Göttinger Wirtschaftsinformatik
Herausgeber: J. Biethahn · M. Schumann

Sebastian Rieger

Einheitliche Authentifizierung in heterogenen IT-Strukturen für ein sicheres e-Science-Umfeld

Band 59

Cuvillier Verlag Göttingen

Göttinger Wirtschaftsinformatik
Herausgeber: J. Biethahn · M. Schumann

Band 59

Sebastian Rieger

Einheitliche Authentifizierung in heterogenen IT-Strukturen für ein sicheres e-Science-Umfeld

CUVILLIER VERLAG

Herausgeber

Prof. Dr. J. Biethahn
Abt. Wirtschaftsinformatik I

Prof. Dr. M. Schumann
Abt. Wirtschaftsinformatik II

Georg-August-Universität
Platz der Göttinger Sieben 5
37073 Göttingen

Bibliografische Information Der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.ddb.de abrufbar.
1. Aufl. - Göttingen : Cuvillier, 2007
Zugl.: Göttingen, Univ., Diss., 2007
ISBN 978-3-86727-329-9

Nonnenstieg 8, 37075 Göttingen
Telefon: 0551-54724-0
Telefax: 0551-54724-21

1. Auflage, 2007
Gedruckt auf säurefreiem Papier

ISBN 978-3-86727-329-9

Einheitliche Authentifizierung in heterogenen IT-Strukturen für ein sicheres e-Science-Umfeld

Dissertation

zur Erlangung des wirtschaftswissenschaftlichen Doktorgrades der

Wirtschaftswissenschaftlichen Fakultät der Universität Göttingen

vorgelegt von

Sebastian Rieger

aus Hannover

Göttingen, 2007

Erstgutachter:	Prof. Dr. Hartmut Koke
Zweitgutachter:	Prof. Dr. Matthias Schumann
Tag der mündlichen Prüfung:	11.7.2007

Vorwort

„Was bedeutet das *sprich, Freund, und tritt ein*?“ fragte Merry. „Das ist doch ganz klar“, antwortete Gimli. „Wenn du ein Freund bist, sage das Losungswort und die Tür wird sich öffnen und du kannst eintreten.“[1]

Authentifizierung ist allgegenwärtig. Überschreitet man eine Landesgrenze, so ist der Besitz eines Ausweises erforderlich, anhand dessen Validität die Identifizierung der zugehörigen Person möglich ist. Kreditkarten, Bankkonten und insbesondere Dienste im Internet erfordern ebenfalls jeweils separat ein eindeutiges Merkmal als Passwort oder PIN, das nur dem Besitzer bekannt ist und ihn daher eindeutig identifiziert. Allerdings haben die Authentifizierungsmerkmale in der Realität ihren Äquivalenten in der Informationstechnologie etwas voraus. Für sie sind im Laufe der Jahre bereits standardisierte Vereinheitlichungsformen entstanden, um uns das Leben zu erleichtern. Pässe werden international akzeptiert, wir benötigen nicht für jedes Land einen neuen Pass. Innerhalb der Europäischen Union wird den Bürgern der Mitgliedsstaaten sogar ohne jegliche Prüfung, vergleichbar den entstehenden Federation-Lösungen, die in Kapitel 3 beschrieben werden, vertraut. Kreditkarten werden von unterschiedlichen Banken angeboten, für Schlösser existieren Generalschlüssel usw.

Verglichen damit steht die Authentifizierung in heterogenen IT-Strukturen noch an ihrem Anfang. Systeme erfordern aufgrund fehlender Kompatibilität oder Absprachen zwischen den Organisationen separate Authentifizierungsmerkmale (z.B. Passwörter). Benutzer können keine alternativen Merkmale für ihre Authentifizierung (wie den Führerschein anstelle des Personalausweises) verwenden. Es ist interessant, wie sehr man plötzlich die Authentifizierung und deren Leichtigkeit in der Realität feststellt, wenn man sich im Rahmen eines Promotionsprojekts zur IT-Sicherheit damit auseinandersetzt. Da ist es erleichternd auch in der Literatur außerhalb des IT-Umfelds ein Zitat wie das obige Zitat aus dem „Herrn der Ringe“ zu lesen und zu entdecken, dass sogar fiktive Charaktere und Zauberer über Authentifizierungsverfahren und zugehörige Merkmale längere Zeit grübeln müssen. Sicherlich ist dem einen oder anderen Leser das Passwort für das obige Rätsel bekannt. „Mellon“, die elbische Übersetzung des Wortes „Freund“, ruft bei mir jedoch noch andere Erinnerungen als das Öffnen einer Tür zu einem Zwergen-Bergwerk hervor.

Gemeint sind all die Freunde, Bekannten und Verwandten, die mir in der Zeit, in der ich nicht immer über die Probleme der Authentifizierung, wie im obigen Fall geschildert, schmunzeln konnte, zur Seite standen. Vielen Dank, ihr Gefährten!

---

[1] TOLKIEN, J. R. R.: Der Herr der Ringe. Band I. Die Gefährten. 23. Aufl., 1995, S. 370.

In erster Linie gilt mein Dank Herrn Prof. Dr. Hartmut Koke, dem ich neben dem Themenbereich der Promotion auch die Möglichkeit verdanke, die Facetten der Authentifizierung im Rahmen einer Anstellung bei der Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG) in der Praxis kennen zu lernen. Durch die Unterstützung von Herrn Prof. Dr. Hartmut Koke konnte ich viele interessante Projekte durchführen, die dafür sorgten, dass neben den theoretischen Betrachtungen der Authentifizierung auch die praxisnahe Anwendung des hier vorgestellten Modells unter Beweis gestellt werden konnte. Für die exzellente Unterstützung durch die Abteilungen Wirtschaftsinformatik I und II sowie die persönliche Beratung möchte ich vor allem Herrn Prof. Dr. Matthias Schumann wie auch Herrn Prof. Dr. Jörg Biethahn danken. Mein Dank gilt auch Herrn Prof. Dr. Bernhard Neumair, der mir den notwendigen Freiraum für die Fertigstellung der Dissertation bei der GWDG gewährte. Auch den Kollegen der GWDG gebührt mein Dank für die zahlreichen anregenden Gespräche zu dem Themenbereich der einheitlichen Authentifizierung, die Kritik und das offene Ohr für meine Ideen. Hervorheben möchte ich Herrn Dr. Wilfried Grieger und Herrn Thorsten Hindermann, mit denen ich gemeinsam an vielen Authentifizierungsprojekten, die mir Anregungen gaben, arbeiten durfte. Über die GWDG hinaus gebührt mein Dank den Teilnehmern des GÖ*-Projekts und der Arbeitsgruppe Identity Management des Landesarbeitskreises Niedersachsen für Informationstechnik / Hochschulrechenzentren (LANIT), mit denen ich die einheitliche Authentifizierung am Wissenschaftsstandort Göttingen vorantreiben durfte. Herrn Prof. Dr. Anatol Badach möchte ich ebenfalls für die Prägung meiner wissenschaftlichen Laufbahn und die Denkanstöße zu meinem Promotionsprojekt danken.

Insbesondere möchte ich mich bei meinen Eltern für die langjährige mentale und finanzielle Unterstützung bedanken. Für die Zuwendung im Alltag danke ich besonders Helen, die in der Zeit meiner Promotion so manche Flaute abfedern und so manche Laune heben konnte. Ihr habe ich zu verdanken, dass der gemeinsame Lebensabschnitt trotz der hohen Belastungen auch immer wieder Rettungsanker als analogen Ausgleich zu meinen zunehmenden digitalen Identitäten bot.

Für das intensive Lektorat und die Korrekturen am Ende meiner Promotionszeit danke ich insbesondere Herrn Georg Tuschinsky. Auch ohne Leif Meier wäre das Lesen dieser Arbeit weniger gut möglich. Ich danke ihm für zeitaufwendiges Korrekturlesen und die zahlreichen Anregungen im Laufe meiner Promotion. Danken möchte ich auch meinen Bachelor-Kandidaten und Diplomanden Marina Pavlova und Jan Mönnich für die gemeinsamen Diskussionen über unzählige Aspekte der Authentifizierung.

Inhaltsübersicht

Inhaltsverzeichnis

1 Einleitung

In den vergangenen Jahren hat die Dezentralität des Zugriffs auf IT-Anwendungen und Ressourcen nicht zuletzt durch die große Verbreitung des World Wide Web mehr und mehr zugenommen. Web-Shops bieten ihren Kunden unabhängig von Ladenschlusszeiten oder dem Ort, an dem diese sich befinden, Dienstleistungen an.[2] Web-Services bieten darüber hinaus die globale Vernetzung von Applikationen und Geschäftsprozessen und reduzieren gleichzeitig die Komplexität von verteilten Anwendungen.[3] Durch Entwicklungen wie Asynchronous JavaScript and XML (AJAX)[4] und Rich Clients[5] entsteht unter dem Begriff „Web 2.0“ eine neue Generation von Web-Diensten, die teilweise nicht von klassischen Desktop-Applikationen zu unterscheiden sind. Sie tragen dazu bei, dass die Dezentralität der Anwendungen weiter zunimmt und sicherlich auch zukünftig noch steigen wird.

Im wissenschaftlichen Umfeld dienen Grid-Initiativen als Motor für die Dezentralisierung. Leistung von Rechenzentren soll gebündelt, verteilte Anwendungen über ihre Grenzen hinweg verknüpft werden. Treiber sind unter anderem Projekte wie der Large Hadron Collider der European Organisation for Nuclear Research (CERN), für dessen Experimente eine Datenmenge von ca. 15 Petabytes (15 Millionen Gigabytes) pro Jahr erwartet wird.[6] Die Analyse der Daten ist hierbei zentral am CERN aufgrund der großen Datenmenge nicht zu bewerkstelligen. Über schnelle Kommunikationsnetze sollen die Daten daher weltweit an Rechencluster verteilt werden, die deren Auswertung unterstützen. Zusätzlich sollen tausende von Wissenschaftlern Zugriff auf die Daten erhalten. Neben der Hochenergiephysik haben auch andere Wissenschaften wie die Medizin oder auch die Philologie und Linguistik die Bedeutung der vernetzten IT-Ressourcen mittels Grid erkannt.[7] „Ökonomische Chancen bieten sich insbesondere in den Bereichen Digitalisierung der Dienstleistungswirtschaft und Digital Manufacturing / Digital Factory, um neue Dienstleistungen zu ermöglichen, Produktionszyklen zu flexibilisieren und zu beschleunigen und dadurch Wachstumskräfte in diesen Märkten mit dynamischem Wachstumspotenzial anzureizen.“.[8]

---

[2] Vgl. BADACH, A.; RIEGER, S.; SCHMAUCH, M.: Web-Technologien, 2003, S. 1.

[3] Vgl. BADACH, A.; RIEGER, S.; SCHMAUCH, M.: Web-Technologien, 2003, S. 312.

[4] Vgl. GARRET, J. J.: Ajax: A New Approach To Web Applications, 2005.

[5] Vgl. DAUM, B.: Rich-Client-Entwicklung mit Eclipse 3.2. 2. Aufl., 2006, S. 1 ff.

[6] Vgl. LCG - LHC Computing Grid Project, 2007.

[7] Vgl. MediGRID GRID-Computing für die Medizin und Lebenswissenschaften, 2007; Vgl. TextGrid Modulare Plattform für verteilte und kooperative wissenschaftliche Textdatenverarbeitung - ein Community-Grid für die Geisteswissenschaften, 2007.

[8] Vgl. BMBF-eScience, 2007.

Über die reine Vernetzung der Rechenleistung bzw. Datenverarbeitung sind daher weitere Anwendungen, z.B. in Form von Web-Portalen erforderlich, die die verteilten Anwendungen nutzbar machen und das Potential des Grid ausschöpfen.[9] Wissenstransfer über schnelle, vernetzte Strukturen wie dem Internet und darauf basierendem World Wide Web sollen neue Formen wissenschaftlichen Arbeitens in sich selbst organisierenden Strukturen realisieren.[10] Man spricht in diesem Zusammenhang auch von „enhanced science“ (kurz: e-Science). Dies umfasst auch die Realisierung der erforderlichen IT-Sicherheit, die u.a. den Schutz vertraulicher Daten bei medizinischen Forschungsprojekten gewährleisten soll. Trotz der Vereinfachung des Zugriffs durch die Dezentralisierung soll der Zugriff durch unberechtigte Dritte in jedem Fall ausgeschlossen werden. Dies erfordert nicht zuletzt den Einsatz einer einheitlich über die gesamte IT-Struktur verwendbaren Authentifizierung.

1.1 Problemstellung und Motivation

Die in der Einleitung erläuterte Dezentralität und damit verbundene Vielfalt der Anwendungen z.B. im World Wide Web führt in Bezug auf die Authentifizierung zu einer Vielzahl von Passwörtern bzw. Authentifizierungsmerkmalen, die die Benutzer für ihre Arbeit mit den Anwendungen legitimieren. Die Verwendung und Verwaltung der Authentifizierungsmerkmale, -verfahren und -systeme sorgt dabei sowohl aufseiten der Benutzer als auch seitens der Organisationen bzw. Betreiber für einen erhöhten Aufwand. Gesteigert wird der Aufwand insbesondere aufgrund der bedingt durch die Dezentralisierung gestiegenen Zahl der Benutzer und zugehörigen Benutzerkonten an den einzelnen Standorten. Nicht nur im e-Science Umfeld wird der erhöhte Aufwand zunehmend zu einem Problem. Nahezu alle Internet-Nutzer spüren mittlerweile den erforderlichen Aufwand für die Verwaltung unterschiedlicher Passwörter, so etwa für verschiedene Web-Shops und Internet-Dienste (beispielsweise Amazon, eBay, GMX, usw.). In einer Studie der Fa. SafeNet aus dem Jahr 2004 gaben 29% der befragten 58.000 Benutzer an, sich sieben Passwörter oder mehr allein für die Arbeit merken zu müssen, bei steigender Tendenz. Lediglich 18%, der aus Deutschland, Frankreich, Großbritannien und den USA stammenden Befragten gaben an sich maximal zwei Passwörter merken zu müssen.[11]

Gleichzeitig steigen die Anforderungen an die IT-Sicherheit für die Firmen. Beispielsweise müssen nach der genannten Studie 83% der Benutzer mindestens einmal im Jahr ihr Kennwort ändern. 27%

[9] Vgl. e-Science-Forum, 2007.

[10] Vgl. BMBF-eScience, 2007.

[11] Vgl. SAFENET: Annual Password Survey Results, 2004, S 1. ff.

dürfen bei der Passwort-Änderung kein altes Passwort erneut verwenden, 30% müssen Zahlen und Sonderzeichen neben Buchstaben in ihrem Passwort vergeben. Um sich ihr Passwort merken zu können, schreiben es allerdings 50% auf, 35% teilen ihr Passwort außerdem Kollegen mit. Die erzielte Sicherheit ist somit trotz der Komplexitätsanforderungen sowie unterbundenen Wiederverwendbarkeit der Passwörter eingeschränkt. Zusätzlich bestätigt die Studie nicht nur die verbundene Minderung der Benutzbarkeit (Usability) durch den Aufwand für die Benutzer, sondern auch die steigenden Kosten für die Organisationen. 9% der Angestellten müssen sich drei- bis viermal im Jahr ihr Passwort zurücksetzen lassen. Insgesamt 47% der Befragten benötigen mindestens einmal pro Jahr eine Rücksetzung. Dabei werden in der Studie Kosten zwischen $30 und $50 für das Rücksetzen angenommen. Einen guten Überblick über ähnliche Statistiken zu dem Aufwand und der erzielten Sicherheit durch Passwörter liefert PasswordResearch.[12] Der zunehmende Aufwand sowie die eingeschränkte Sicherheit durch die anwachsende Diversität bilden die Problemstellung der vorliegenden Arbeit.

Die einheitliche Authentifizierung ermöglicht durch die Reduzierung des Aufwands und die Gewährleistung der erzielten Sicherheit eine Optimierung von heterogenen IT-Strukturen. Dies stellt die Motivation dieser Arbeit dar. Die einheitliche Authentifizierung bildet eine Grundlage für ein sicheres e-Science Umfeld sowie IT-Strukturen im Allgemeinen. Aufgrund dieses Potenzials bieten viele Hersteller Soft- und Hardware-Lösungen für die skizzierte Optimierung an. Häufig weisen diese jedoch Einschränkungen auf. Insbesondere lassen sich die Lösungen nicht für alle Anwendungen in einer heterogenen IT-Struktur einsetzen, ohne hohe Kosten oder Einschränkungen in Kauf zu nehmen. Das Potenzial sowie externe Anforderungen an die IT-Sicherheit sorgen jedoch seit einigen Jahren für einen anhaltenden Hype um das Thema Identity Management und „Single Sign-On“. Diese Arbeit befasst sich im Gegensatz hierzu mit den theoretischen Grundlagen für die Vereinheitlichung der Authentifizierung in heterogenen IT-Strukturen und stellt ein geeignetes Modell vor. Sie baut dabei auf bestehenden Bewertungsmodellen zum Aufwand der IT-Sicherheit und Authentifizierung sowie der erzielten Sicherheit als Nutzen auf. Existierende Lösungen für die Realisierung der einheitlichen Authentifizierung werden bewertet sowie Möglichkeiten und Herausforderungen für zukünftige Lösungen definiert. Zusätzlich werden anhand von Fallstudien Ergebnisse der Anwendung in der Praxis beschrieben.

[12] Vgl. Password Research Institute, 2005.

1.2 Zielsetzung

Ziel dieser Arbeit ist die Minimierung des Aufwands für die Authentifizierung in heterogenen IT-Strukturen bei gleichzeitiger Gewährleistung der durch sie erzielten IT-Sicherheit. Hierfür werden bestehende Ansätze für die Quantifizierung von Aufwand und Sicherheit erweitert und auf ein theoretisches Modell für die einheitliche Authentifizierung in heterogenen IT-Strukturen abgebildet. Dadurch ergeben sich für die Bewertung von Kosten und Nutzen der IT-Sicherheit neue Beiträge.[13] Zusätzlich wird der Einfluss der einheitlichen Authentifizierung auf die Optimierung von IT-Strukturen in Bezug auf den Aufwand bei der Verwendung und Verwaltung bereitgestellter Dienste sowie der erzielten IT-Sicherheit bewertet. Durchgeführte Fallstudien, die die Anwendung des Modells in der Praxis verdeutlichen, liefern zudem Ergebnisse, die für die Vereinheitlichung der Authentifizierung in anderen wissenschaftlichen und betrieblichen heterogenen IT-Strukturen verwendet werden können. Anhand des Modells werden darüber hinaus Probleme identifiziert, die durch bestehende Lösungen für die Realisierung einer einheitlichen Authentifizierung nicht adressiert werden. In dieser Arbeit werden Anforderungen an neue Authentifizierungsverfahren genannt, die diese Probleme adressieren, und prototypische Lösungen diskutiert. Sie dienen dabei als Erweiterung der bestehenden Verfahren für Identity Management[14] sowie in der Entwicklung befindlicher benutzerzentrierter Lösungen.[15]

1.3 Methodik und Aufbau der Arbeit

Zunächst werden in Kapitel 2 die Grundlagen für das Verständnis der zur Authentifizierung zählenden Begriffe und Funktionen erläutert. Kapitel 3 beschreibt die Gründe für den in Abschnitt 1.1 beschriebenen erhöhten Aufwand der Authentifizierung in heterogenen IT-Strukturen. Für die Reduzierung des Aufwands existieren bereits Hard- und Software-Lösungen unterschiedlicher Hersteller, die in Abschnitt 3.2 beschrieben und in Bezug auf ihre Eignung für heterogene IT-Strukturen bewertet werden. Probleme der Lösungen werden abschließend zusammengefasst und in

---

[13] Beispiele für bestehende Bewertungen für Kosten der IT-Sicherheit finden sich in MÖRIKE, M.; TEUFEL S.: Kosten & Nutzen von IT-Sicherheit in: HEILMANN, H. ET AL. (Hrsg.): HMD - Praxis der Wirtschaftsinformatik, Heft 248, 2006; GORDON, L. A.; LOEB, M. P.: Managing Cyber-Security Resources - A cost-benefit analysis, 2005; Economics and Security Resource Page, 2007.

[14] Vgl. KUPPINGER, M.: Trends im Identity Management, Vortrag: IdM Day, 2006.

[15] Beispiele für aktuelle Entwicklungen sind MICROSOFT: Introducing Windows CardSpace, 2007; SXIP identity, 2007; COMMUNICATIONS-ELECTRONICS SECURITY GROUP: ID-PKC: a new approach to Public Key Cryptography, 2007.

Abschnitt 3.3 auf Anforderungen für die optimale Gestaltung von IT-Strukturen durch den Einsatz einheitlicher Authentifizierung abgebildet.

Kapitel 4 benennt die Anforderungen und Ziele für eine einheitliche Authentifizierung in heterogenen IT-Strukturen. Für eine einheitliche Authentifizierung werden in Kapitel 4 sowohl Anforderungen aus wissenschaftlichen als auch aus betrieblichen IT-Strukturen betrachtet, die aufgrund ihrer verschiedenen Charakteristika unterschiedlich von der Vereinheitlichung der Authentifizierung profitieren. Da sich die Authentifizierung in den Aufgabenbereich der IT-Sicherheit einbettet[16], werden in Abschnitt 4.3 Schnittstellen zu nachgelagerten Verfahren, wie der Autorisierung und Abrechnung, genannt.

Kapitel 5 und 6 beinhalten den methodischen Kern der vorliegenden Arbeit. In Kapitel 5 wird das in Abschnitt 2.4.2 eingeführte erweiterte Authentifizierungsmodell für heterogene IT-Strukturen auf ein graphentheoretisches Modell abgebildet, dessen Kantengewichte den erforderlichen Aufwand sowie die durch die Authentifizierung erzielte Sicherheit bilden. Im Folgenden beschreiben die Abschnitte des Kapitel 5 die Faktoren für die Optimierung dieses Graphen hinsichtlich der Anzahl seiner Knoten und Summe der Kantengewichte. Hierfür werden mögliche Vereinheitlichungen definiert und, soweit verfügbar, mit bestehenden Lösungen für eine einheitliche Authentifizierung aus Abschnitt 3.2 in Beziehung gesetzt.

Kapitel 6 überträgt das skizzierte theoretische Modell auf Anforderungen aus der Realität wissenschaftlicher und betrieblicher IT-Strukturen und zeigt eine exemplarische Realisierung einer geeigneten einheitlichen Authentifizierung auf. Basierend darauf wird in Abschnitt 6.2 eine Methodik für die Optimierung des Modells bestimmt. Für die Optimierung werden die anhand des Bewertungsmodells aus Kapitel 5 quantifizierten Werte auf ein Fuzzy-Logic Modell übertragen, um die Unschärfe der Begriffe Aufwand und Sicherheit im Modell abzubilden. Die Anwendung der in Abschnitt 6.3 genannten Lösungen in einem Referenzmodell für die durchgeführten Fallstudien in Abschnitt 6.4 führt schließlich zur Bewertung der Ergebnisse in Abschnitt 6.5. Kern des Referenzmodells für die Implementierung der einheitlichen Authentifizierung stellen dabei die Abgrenzung der Vereinheitlichung in den einzelnen Bereichen des in Abschnitt 6.3.3 eingeführten Ebenenmodells sowie eine stufenweise Integrations- und Migrationsstrategie in Abschnitt 6.3.4 dar.

Kapitel 7 fasst die Ergebnisse zusammen und gibt einen Ausblick auf zukünftige Arbeiten.

[16] Die Authentifizierung sichert die Authentizität, deren Bedeutung in Abschnitt 2.2.5 definiert wird.

2 Grundlagen der Authentifizierung in IT-Strukturen

Die folgenden Abschnitte stellen die Grundlagen, die für eine Authentifizierung in IT-Strukturen benötigt werden, vor. Es wird vorrangig die Authentifizierung von Benutzern bzw. Personen gegenüber einem System oder einer Organisation beschrieben. Für die Gewährleistung der IT-Sicherheit ist insbesondere die gegenseitige Authentifizierung zwischen Systemen, Organisationen und Benutzern erforderlich. Beispielsweise sollen in der Regel nur dann geheime Daten für die Authentifizierung des Benutzers an ein System übermittelt werden, wenn dieses vom Benutzer eindeutig identifiziert und als vertrauenswürdig ermittelt wurde. Ohne eine Authentifizierung des Systems vor der Übermittlung der geheimen Informationen, wie z.B. eines Passwortes, könnten diese Informationen an unberechtigte Dritte gesendet werden, die sie dann ihrerseits für eine erfolgreiche Authentifizierung am eigentlichen System verwenden.

Die hierbei beteiligten Informationen, Verfahren und zugehörigen Begriffe erläutert der nachfolgende Abschnitt.

2.1 Begriffsdefinitionen

Die nachfolgenden Abschnitte definieren die in Bezug auf die Authentifizierung in dieser Arbeit verwendeten Begriffe. Größtenteils finden sich die aufgeführten Begriffe auch in der Fachliteratur zur Authentifizierung bzw. IT-Sicherheit wieder.[17]

2.1.1 Benutzer

Um die Authentizität bzw. die eindeutige Identität einer natürlichen oder juristischen Person oder eines Systems überprüfen zu können, wird diesen ein Kennzeichen als digitale Identität zugewiesen. Dieses Kennzeichen kann ein Benutzername sein. Der Begriff der Identität umfasst hierbei sowohl Personen als auch Systeme oder Endgeräte, die an einer Authentifizierung teilnehmen.[18] Im Folgenden wird aus diesem Grund der Begriff Identität gleichermaßen für Personen und Systeme verwendet. Personen, die Zugriff auf eine Ressource in der IT-Struktur nehmen, werden als Benutzer bezeichnet.

Eine Person oder ein System kann mehrere digitale Identitäten besitzen, die z.B. für unterschiedliche Funktionen oder Zugehörigkeiten genutzt werden. Die Zuordnung erfolgt jedoch in jedem Fall

---

[17] Vgl. ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 437 ff. oder SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002.

[18] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 4 f.

eindeutig. Eine digitale Identität ist genau einer Person oder System zugeordnet, während eine Person oder ein System unterschiedliche digitale Identitäten besitzen kann.

Im Englischen spricht man während der Authentifizierung in Bezug auf die Person häufig von einem Principal (deutsch: Vorsteher oder Auftraggeber), der den Auftrag zu seiner Authentifizierung erteilt.[19] Die Identität wird vom Benutzer in der Regel zusammen mit einem Authentifizierungsmerkmal als Auftrag an das authentifizierende System zur Prüfung übermittelt. Auch der Begriff Supplicant (deutsch: Supplikant oder Bittsteller) ist hierbei gebräuchlich.[20]

2.1.2 Betreiber

Als Betreiber werden im Folgenden Personen bzw. Organisationen bezeichnet, die ein System unterhalten, das eine Authentifizierung erfordert.[21] Dies bezieht auch Administratoren, die Authentifizierungskonten, -merkmale sowie Identitäten betreuen, mit ein. Betreiber können Authentifizierungssysteme für unterschiedliche Gruppen von Identitäten oder verschiedene Organisationen betreiben.

Betreiber sind für die Gewährleistung der IT-Sicherheit gegenüber ihren Benutzern zuständig. Dies bezieht neben der vertraulichen Speicherung der Authentifizierungsmerkmale auch die sorgsame Auswahl und Wartung von Authentifizierungsverfahren mit ein.

2.1.3 Ressource

Eine erfolgreiche Authentifizierung ermöglicht den Zugriff auf eine von dem Benutzer gewünschte Ressource. Unter dem Begriff Ressourcen werden im Folgenden Dienste, Anwendungen und Geräte zusammengefasst, die in einer IT-Struktur bereitgestellt werden (z.B. E-Mail-Konto, Netzwerkfreigaben und -zugänge usw.). Man spricht hierbei auch davon, dass sich der Benutzer für den Zugriff auf diese konkrete Ressource authentifiziert hat. Betreiber setzen eine Authentifizierung für die von Ihnen angebotenen Ressourcen voraus, um so den Zugriff durch unberechtigte Dritte zu unterbinden oder sie allgemein vor Missbrauch zu schützen.

---

[19] Vgl. GARMAN, J.: Kerberos. The Definitive Guide, 2003, S. 17.

[20] Vgl. IEEE: 802.1X Port-Based Network Access Control, 2004, S. 7.

[21] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 73.

2.1.4 Authentifizierung

Die Überprüfung einer Identität[22] anhand eines Authentifizierungsmerkmals durch einen Dritten bezeichnet man aus Sicht des Überprüfenden als Authentifizierung.[23] Im Gegenzug wird der Vorgang aus Sicht des Überprüften im deutschen Sprachgebrauch Authentisierung genannt[24], die englische Bezeichnung „Authentication“ die Sichten beider Beteiligten gleichermaßen umfasst. In den folgenden Abschnitten wird im Regelfall die Sicht der Betreiber eines Dienstes, die Identitäten überprüfen, dargestellt und daher der Begriff der Authentifizierung verwendet. In der deutschen Literatur wird hierfür teilweise synonym der Begriff Authentifikation gebraucht, der jedoch im allgemeinen Sprachgebrauch der IT eine geringere Verbreitung besitzt.[25]

Eine Authentifizierung hat in jedem Fall ein eindeutiges Ergebnis. Sie lässt sich anhand einer zweiwertigen Aussagenlogik beschreiben und führt daher zu genau zwei möglichen Ergebnissen. Entweder ist die Authentifizierung erfolgreich oder nicht erfolgreich.[26]

Im Allgemeinen wird eine Authentifizierung zu Beginn einer Sitzung bzw. eines Vorgangs an IT-Systemen durchgeführt und ist dann bis zu deren Beendigung gültig. Zugriffskontrollen (Autorisierung) und etwaige Abrechnung (Accounting) setzen auf die durch eine erfolgreiche Authentifizierung gesicherte Vertrauensbasis auf. Die Authentifizierung ist nicht nur die Grundlage für nachfolgende Prozesse wie die Prüfung von Berechtigungen; sie ermöglicht etwa durch den Austausch von Schlüsseln beim Authentifizieren auch die Gewährleistung der Vertraulichkeit der übertragenen Informationen während einer Sitzung. Dies unterstreicht nicht zuletzt die hohe Bedeutung der Authentifizierung für die IT-Sicherheit.[27]

2.1.5 Authentifizierungsmerkmal

Die Angabe der Identität eines Benutzers gegenüber einem System reicht nicht aus, um eine Person oder ein System eindeutig identifizieren zu können. Auch ein unberechtigter Dritter, der diese Be-

---

[22] Vgl. Abschnitt 2.1.1.

[23] Vgl. CHESWICK, W. R.; BELLOWIN, S. M., RUBIN, A. D.: Firewalls und Sicherheit im Internet. 2. Aufl., 2004, S. 179.

[24] Vgl. DUDEN: Das Fremdwörterbuch, 7. Aufl., 2001, S. 106.

[25] Vgl. ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 187; DUDEN: Das Fremdwörterbuch, 7. Aufl., 2001, S. 106.

[26] Eine detaillierte Betrachtung zweiwertiger Aussagelogik lässt sich in DÖRFLER, W.; PESCHEK, W.: Einführung in die Mathematik für Informatiker, 1988, S. 83 nachlesen.

[27] Vgl. ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 7, wobei Authentizität als erstes Schutzziel der IT-Sicherheit genannt wird.

zeichnung (z.B. den Benutzernamen) einer Person kennt, kann diese direkt an das System übermitteln und den rechtmäßigen Inhaber der Identität impersonieren. Daher ist für die Gewährleistung der Authentizität[28] ein zusätzliches, eindeutiges Authentifizierungsmerkmal notwendig.[29] Dieses Authentifizierungsmerkmal kann auf einer geheimen Information wie einem Passwort basieren, die nur der berechtigten Person bekannt ist, oder einer Eigenschaft, die die Person eindeutig identifiziert. Somit kann durch die Verwendung oder Überprüfung des geheimen Authentifizierungsmerkmals die Identität der Person gesichert überprüft werden.

Authentifizierungsmerkmale müssen vor dem Zugriff durch unberechtigte Dritte geschützt werden. Erlangt ein unberechtigter Dritter Zugriff auf das Authentifizierungsmerkmal, so kann er die Identität des Inhabers vortäuschen oder übernehmen. Authentizität und Verbindlichkeit der zum Authentifizierungsmerkmal gehörigen Identität wären somit nicht mehr gewährleistet.[30] Authentifizierungsmerkmale werden genau einer Identität zugeordnet.

2.1.6 Authentifizierungsfaktor

Erfordert die erfolgreiche Überprüfung einer Identität eines Benutzers mehrere Authentifizierungsmerkmale (z.B. den Besitz eines Tokens und die Kenntnis eines zugehörigen Passwortes), so spricht man in Bezug auf die Merkmale auch von Authentifizierungsfaktoren.[31] Der Benutzer muss in diesem Fall alle Faktoren eindeutig nachweisen, um seine Identität glaubhaft zu bestätigen. Man spricht in diesem Zusammenhang auch von einer Multi-Faktor-Authentifizierung. Häufig werden für die einzelnen Faktoren unterschiedliche technische Verfahren verwendet. Diese Verfahren basieren in der Regel auf der Kenntnis (etwa einer eine Information, die die Identität kennt), dem Besitz (z.B. ein Gegenstand, den sie besitzt) oder einer eindeutigen Eigenschaft (z.B. ein persönliches bzw. biometrisches Kennzeichen).

2.1.7 Authentifizierungskonto

Um die Authentifizierung durchführen zu können, benötigt die überprüfende Instanz die Bezeichnung der Identität sowie eine Kopie des Authentifizierungsmerkmals. Identität und Authentifizie-

---

[28] Der Begriff der Authentizität wird im folgenden Abschnitt als Grundwert der IT-Sicherheit definiert.

[29] Vgl. „distinguishing characteristic“ in SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 3 f.

[30] Die Identität des Benutzers kann nicht verbindlich nachgewiesen werden. Somit ist die Zuordnung zur realen Person, bzw. die Authentizität nicht gewährleistet. Verbindlichkeit und Authentizität werden im folgenden Abschnitt als Grundwerte der IT-Sicherheit beschrieben.

[31] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 28 ff.

rungsmerkmal werden daher aufseiten des Überprüfenden in einem Authentifizierungskonto (kurz Konto) gespeichert.[32] Dieses Konto ordnet ein Authentifizierungsmerkmal genau einer Identität zu. Umgekehrt kann eine Identität in einem Konto mehrere Authentifizierungsmerkmale zugewiesen bekommen. Ein Konto umfasst die Angabe einer Identität sowie zugehöriger Authentifizierungsmerkmale.

2.1.8 Authentifizierungsverfahren und -sitzung

Die Art und Weise, in der eine Authentifizierung durchgeführt wird, beschreibt ein Authentifizierungsverfahren.[33] Dieses definiert, wie eine Identität das zugewiesene Authentifizierungsmerkmal nachweist und wie dieses eindeutig überprüft werden kann. Authentifizierungsverfahren müssen dabei den Anforderungen an Vertraulichkeit, Integrität und Verbindlichkeit genügen, um eine fälschlicherweise korrekte Authentifizierung von unberechtigten Dritten zu unterbinden.[34] Für eine erfolgreiche Authentifizierung können mehrere Authentifizierungsverfahren parallel oder verkettet eingesetzt werden. Hierbei ist für die Gewährleistung der Authentizität und Verbindlichkeit festzulegen, ob eine erfolgreiche Authentifizierung die erfolgreiche Ausführung mehrerer beteiligter Verfahren oder lediglich eines einzelnen erfordert.

Authentifizierungsverfahren beinhalten häufig eine Unterstützung für die Etablierung einer Authentifizierungssitzung. Innerhalb dieser Sitzung kann die Authentizität der Kommunikationspartner ohne eine erneute Authentifizierung gewährleistet werden. Sofern eine Authentifizierungssitzung für unterschiedliche Anwendungen verwendet werden kann, spricht man in Bezug auf die einmalige Authentifizierung zu Beginn auch von einem „Single Sign-On“.

2.1.9 Authentifizierungssystem

Authentifizierungssysteme verwenden ein oder mehrere Authentifizierungsverfahren, um Identitäten gegen Authentifizierungskonten, die auf den Systemen gespeichert werden, anhand zugehöriger Authentifizierungsmerkmale zu authentifizieren. Authentifizierungssysteme können verschiedene Authentifizierungsverfahren als Alternativen für die Authentifizierung verwenden oder diese verketten und so für eine erfolgreiche Authentifizierung die korrekte Verarbeitung aller beteiligten Verfahren voraussetzen.

---

[32] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 80.

[33] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 2 f.

[34] Die Anforderungen an die Vertraulichkeit, Integrität und Verbindlichkeit werden im folgenden Abschnitt als Grundwerte der IT-Sicherheit beschrieben.

Auch Authentifizierungssysteme selbst können verknüpft werden. Die erfolgreiche Authentifizierung der Identität bedingt hierbei je nach Anforderung an die Authentizität und Verbindlichkeit die korrekte Authentifizierung der Identität an einem einzelnen System oder an mehreren beteiligten Systemen.

2.1.10 Heterogene IT-Strukturen

IT-Strukturen, die auf Hard- und Software unterschiedlicher Hersteller bzw. unterschiedlichen Plattformen (z.B. Windows oder Unix) aufsetzen und an vernetzte Strukturen (wie z.B. dem Internet oder lokalen Netzwerken) angebunden sind, werden im Folgenden unter dem Begriff heterogene IT-Strukturen zusammengefasst. Die Heterogenität kann dabei durch spezielle Anforderungen einzelner Benutzergruppen innerhalb der Strukturen begründet sein, deren Umsetzung spezielle Hard- oder Software erfordert. Außerdem kann sie bei der Entstehung und Weiterentwicklung einer IT-Struktur durch die Integration weiterer Benutzergruppen oder Organisationen im Laufe der Zeit entstehen. Auch Produkteigenschaften oder finanzielle Vorteile (Beschaffungs-, Lizenz- oder Wartungskosten) können dazu führen, dass unterschiedliche Hard- und Software-Lösungen innerhalb einer IT-Struktur verwendet werden. Trotz des höheren Aufwands in Bezug auf die Verwendung und Verwaltung für die Benutzer und Betreiberorganisationen im Vergleich zu homogenen Hard- und Software-Strukturen können Vorteile heterogener Lösungen deren Existenz rechtfertigen. Beispielsweise kann ein Unternehmen entscheiden, unterschiedliche Hard- und Software für die gleichen Aufgaben zu verwenden, um den Schaden, der für die IT-Struktur bei einem Serienfehler oder einer Anfälligkeit von Produkten eines einzelnen Herstellers entsteht, zu vermeiden und so eine höhere Verfügbarkeit zu erzielen.

Bezogen auf die Authentifizierung bedeutet eine heterogene IT-Struktur, dass unterschiedliche Authentifizierungsmerkmale, -verfahren und -systeme berücksichtigt werden müssen. Eine einheitliche Authentifizierung muss daher möglichst viele Plattformen bzw. Hard- und Software-Lösungen innerhalb einer IT-Struktur unterstützen.

2.1.11 Einheitliche Authentifizierung

Die einheitliche Authentifizierung beschreibt die Vereinheitlichung der innerhalb von heterogenen IT-Strukturen verwendeten Authentifizierungssysteme, -verfahren und -merkmale. Im Idealfall wird ein einziges, einheitliches Authentifizierungssystem und -verfahren für alle Ressourcen (Dienste wie E-Mail, Dateifreigaben usw.) innerhalb der gesamten IT-Struktur verwendet. Ein Benutzer kann mit einem einzigen, einheitlichen Authentifizierungsmerkmal und Benutzernamen auf alle Ressourcen innerhalb der IT-Struktur zugreifen.

Aufgrund der unterschiedlichen innerhalb einer heterogenen IT-Struktur verwendeten Hard- und Software kann diese vollständige Vereinheitlichung auf ein einziges Authentifizierungssystem, -verfahren und -merkmal in der Regel nicht erfolgen. Die einheitliche Authentifizierung umfasst daher allgemein die Reduktion der innerhalb der IT-Struktur erforderlichen Authentifizierungssysteme, -verfahren und -merkmale und definiert deren minimal erforderliche Anzahl. Begrenzt wird die Vereinheitlichung durch die erzielte IT-Sicherheit. Werden mehrere separate Authentifizierungssysteme, -verfahren und -merkmale verwendet, so steigt die IT-Sicherheit, da bei einer Kompromittierung eines beteiligten Systems, Verfahrens oder Merkmals nicht die gesamte IT-Struktur betroffen ist. Andererseits bedeutet eine hohe Anzahl von Authentifizierungssystemen, -verfahren und -merkmalen eine Minderung der Benutzbarkeit bzw. einen höheren Aufwand bei der Verwaltung und Verwendung der bereitgestellten Ressourcen. Benutzer müssen sich hierbei z.B. eine große Anzahl unterschiedlicher Passwörter merken. Administratoren müssen unterschiedliche Hard- und Software-Produkte für Authentifizierungsverfahren und -systeme warten. Einheitliche Authentifizierung beschreibt in diesem Zusammenhang auch einen Kompromiss bzw. ein optimales Verhältnis zwischen der Benutzbarkeit bzw. dem Aufwand und der durch die Authentifizierung erzielten IT-Sicherheit.

2.1.12 Reduced- und Single Sign-On

Besitzen die Benutzer im Rahmen einer einheitlichen Authentifizierung ein einziges Authentifizierungsmerkmal, das sie für unterschiedliche Applikationen und Ressourcen verwenden können, ohne erneut eine Authentifizierung zu erfordern, so spricht man in Bezug auf die einmal zu Beginn der Sitzung erforderliche Authentifizierung oder Anmeldung von einem „Single Sign-On“.[35] Single Sign-On bedeutet, dass das Authentifizierungsverfahren anderen nachfolgend gestarteten Applikationen Zugriff auf die bestehende Authentifizierungssitzung erlauben muss. Diese müssen zusätzlich in der Lage sein, die Validität der Authentifizierungssitzung ohne weitere Eingaben des Benutzers zu überprüfen. Der Benutzer muss so beispielsweise nur ein einziges Mal sein Kennwort eingeben und kann im Anschluss alle Applikationen und Dienste ohne eine weitere Anmeldung resp. Authentifizierung verwenden. Da hierfür unterschiedliche Standards existieren, ist ein vollständiges Single Sign-On insbesondere in heterogenen IT-Strukturen mit aktuellen Authentifizierungsverfahren und -systemen nicht realisierbar. Dies ist auch den Software-Herstellern von „Single Sign-On“-Lösungen bekannt. Häufig wird daher bereits lediglich von einer Reduzierung der erfor-

[35] Vgl. WINDLEY, P. J.: Digital Identity, 2005, S. 84 f.; SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 115 f.

derlichen Authentifizierung für unterschiedliche Applikationen und Ressourcen seitens der Benutzer als „Reduced Sign-On“ gesprochen.[36]

2.1.13e-Science

John Taylor definierte „enhanced science“ (kurz: e-Science) als „e-Science is about global collaboration in key areas of science and the next generation of infrastructure that will enable it”.[37] Allgemein beschreibt e-Science die Erweiterung klassischer Wissenschaft um eine technische, vernetzte Infrastruktur für globale Zusammenarbeit. Forschungsprozesse bzw. wissenschaftliche Kommunikation und Kollaboration, Informationsbereitstellung, Datenaustausch und -nutzung sowie das Publizieren von wissenschaftlichen Ergebnissen sollen so erleichtert werden. In Deutschland wird e-Science neben dem von der Max-Planck-Gesellschaft initiierten e-Science-Forum auch durch das Bundesministerium für Bildung und Forschung forciert.[38] Im Vordergrund steht dabei die weltweite Verbindung von Hochleistungsrechnern über Hochgeschwindigkeitsnetzwerke. Das durch die Verbindung dieser Rechner entstehende Grid soll Anwendungen und Informationen schnell und für den Anwender transparent zur Verfügung stellen. Der Begriff Grid stammt hierbei vom englischen Begriff „Power Grid“ für Stromnetz ab und soll damit den einfachen Zugang auf Rechenleistung gleichsam „aus der Steckdose“ unterstreichen.

Nicht zuletzt durch die zunehmende Dezentralität ist die Gewährleistung der IT-Sicherheit und insbesondere der Authentifizierung für Grid-Anwendungen und e-Science allgemein ein entscheidender Faktor. Die Authentifizierung ist daher Kernbestandteil vieler Grid-Projekte. Grid-Authentifizierung basiert dabei international häufig auf X.509-Zertifikaten, deren zugehörige Zertifizierungsstellen in eine gemeinsame internationale Grid Trust Federation integriert wurden.[39] Auf europäischer Ebene koordiniert die EUgridPMA die Aufnahme von regionalen Zertifizierungsstellen in die skizzierte internationale Förderation.[40]

Neben den technischen Vorgaben durch den X.509-Standard werden an die Zertifizierung insbesondere organisatorische Anforderungen wie u.a. die persönliche Identifizierung von Zertifikatnehmern gestellt. Diese sollen die IT-Sicherheit und Authentizität der Benutzer trotz deren zunehmend dezentralen Zugriffs gewährleisten. Um die gewünschte Analogie des Grid mit dem Strom-

---

[36] Vgl. FLEMING GRUBB, M.; CARTER, R.: Single Sign-On and the System Administrator, 1998, S. 81.

[37] TAYLOR, J.: e-Science – First phase of the Programme, 2000.

[38] Vgl. BMBF-eScience, 2007; e-Science-Forum, 2007.

[39] Vgl. International Grid Trust Federation (IGTF): The Grid’s Policy Management Authority, 2007.

[40] Vgl. EUGridPMA: The EUGridPMA - coordinating grid authentication in e-Science, 2007.

netz im Sinne des einfachen und für den Nutzer transparenten Zugriffs auf dezentrale Rechenleistung zu ermöglichen, ohne für jede verwendete Information eine erneute Authentifizierung zu erfordern, ist eine einheitliche Authentifizierung erforderlich. Zusätzlich zu X.509-Zertifikaten werden daher auch Verfahren wie Shibboleth, z.B. im Projekt GridShib, für die Grid-Authentifizierung verwendet, die ein Single Sign-On für Grid-Anwendungen ermöglichen.[41]

2.2 Grundwerte für IT-Sicherheit

IT-Sicherheit beschreibt die kontinuierliche Folge aus Angriffen auf die Sicherheit von Informationen und deren Abwehr durch geeignete Techniken und Mechanismen.[42] Die IT-Sicherheit basiert auf fünf Anforderungen oder Grundwerten, die an einen sicheren Umgang mit Daten bzw. deren Übertragung gestellt werden.[43] Diese umfassen die Gewährleistung der Vertraulichkeit, Integrität, Verfügbarkeit, Verbindlichkeit und Authentizität. In den folgenden Abschnitten werden diese Grundwerte der IT-Sicherheit erläutert.

2.2.1 Vertraulichkeit

Daten, die über unsichere Netze, wie z.B. das Internet, übertragen werden, können auf ihrem Weg zwischen Sender und Empfänger von Dritten abgehört werden. Werden sensible Daten übermittelt, so bedeutet dies einen Verlust der Vertraulichkeit. Die Möglichkeit des Abhörens resultiert aus der öffentlichen und dezentralen Struktur der miteinander verbundenen Internet-Knoten. An jedem Netz-Knotenpunkt, den ein Paket passiert, kann dieses ausgelesen und interpretiert werden. Für die Übertragung von sensiblen Daten können unsichere Netze somit nicht ohne zusätzliche Maßnahmen zur Gewährleistung von deren Vertraulichkeit verwendet werden. Um die Anforderung der IT-Sicherheit nach Vertraulichkeit zu erfüllen, werden die Daten in der Regel vor der Übertragung vom Absender verschlüsselt.[44] Für die Authentifizierung ist hierbei relevant, dass die Daten im Allgemeinen nur von einem vom Sender eindeutig identifizierten resp. authentifizierten Empfänger wieder entschlüsselt werden können sollen.

---

[41] Vgl. GridShib: Integrating federated authorization infrastructure with Grid technology, 2007.

[42] Vgl. BADACH, A.; RIEGER, S.; SCHMAUCH, M.: Web-Technologien, 2003, S. 346 ff.

[43] Vgl. ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 6 ff.

[44] Vgl. ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 97.

2.2.2 Integrität

Erlangt ein unberechtigter Dritter Zugriff auf übertragene Daten, wie im vorherigen Abschnitt beschrieben, so kann er neben der Interpretation und Verwendung der abgehörten Inhalte diese verändern und selbst an den Adressaten weiterleiten. Der ursprüngliche Inhalt und Sinn der übertragenen Informationen würde somit verfälscht. Im Rahmen der IT-Sicherheit spricht man hierbei vom Verlust der Integrität der vom Sender übermittelten Daten.[45]

Manipulierte Informationen können neben den übermittelten Inhalten auch Nachrichten des verwendeten Übertragungsprotokolls sein. Hierbei können z.B. Adressen des Absenders oder Empfängers gefälscht oder der Status der Übertragungssitzung manipuliert werden.

Als Mittel für die Gewährleistung der Integrität werden Daten mit Prüfsummen bzw. digitalen Signaturen ausgestattet. Signaturen und Prüfsummen basieren hierbei häufig auf kryptographischen Hash-Verfahren.[46]

Der Ablauf einer Authentifizierung stellt eine erhöhte Anforderung an die Integrität der übermittelten Authentifizierungsinformationen. Werden diese von Dritten auf ihrem Weg zum Adressaten verfälscht, so kann keine verlässliche Authentifizierung durchgeführt werden.

2.2.3 Verfügbarkeit

Systeme, die Daten verarbeiten, bereitstellen oder übertragen, sollen uneingeschränkt verfügbar sein. Der unterbrechungsfreie Betrieb bzw. die Verfügbarkeit der Systeme wird beispielsweise durch Angriffe auf die verwendeten Hard- und Softwareplattformen gefährdet. Oft bietet ein Angriff auf die Verfügbarkeit zusätzliches Potential für den anschließenden Missbrauch des kompromittierten Systems. Letzteres begründet nicht zuletzt die Relevanz des Kriteriums der Verfügbarkeit für die IT-Sicherheit.[47]

Die Authentifizierung ist von der Verfügbarkeit von Systemen, die für die Prüfung der Identität erforderlich sind, abhängig. Die Authentifizierung sichert ihrerseits, dass nur berechtigte Personen Zugriff zu einem System erlangen. Unberechtigte Dritte, die imstande sind, die Stabilität und damit

---

[45] Vgl. ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 8.

[46] Hash-Verfahren werden beispielsweise in ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 353 ff. erläutert.

[47] Vgl. ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 10.

die Verfügbarkeit des Systems zu mindern, können durch eine vorherige Authentifizierung identifiziert und abgewiesen werden.[48]

2.2.4 Verbindlichkeit

Der Absender bzw. Verfasser einer Nachricht muss dieser eindeutig zugeordnet werden können. Er darf nicht in der Lage sein, den Versand der Nachricht oder deren Inhalt abzustreiten. Innerhalb der IT-Sicherheit spricht man in diesem Zusammenhang von der Verbindlichkeit des Absenders.[49]

Verbindlichkeit ist ebenfalls ein entscheidendes Kriterium für die Authentifizierung. Die Person, die eine Authentifizierung durchführt, darf Ihre Identität während des Vorgangs nicht abstreiten können.

2.2.5 Authentizität

Die Authentizität sichert eine eindeutige, überprüfbare Identität zu. Diese kann sich auf den Absender oder Adressaten beziehen. Während die im vorherigen Abschnitt genannte Forderung nach Verbindlichkeit bereits definiert, dass ein Absender seine Identität nicht abstreiten kann, gewährleistet die Verbindlichkeit noch nicht, welche reale Person sich hinter dieser Identität verbirgt. Die Authentizität sichert daher zusätzlich die eindeutige Identifizierung eines Kommunikationspartners.[50]

In der Regel wird hierbei eine digitale Identität, z.B. in Form von Passwörtern oder Schlüsseln, einer realen Person, einem System oder einer sonstigen realen Identität zugeordnet. Häufig überprüfen die Kommunikationspartner gegenseitig ihre Authentizität, um basierend darauf einen gesicherten Übertragungskanal aufzubauen und unberechtigte Dritte auszuschießen. Der Vorgang der Prüfung der Authentizität wird als Authentifizierung bezeichnet.

---

[48] Risiken in Bezug auf die Verfügbarkeit von IT-Systemen, resultierend aus Angriffen und Abwehrmaßnahmen, werden ausführlich in ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 100 f., und PEIKARI, C.; CHUWAKIN, A.: Kenne Deinen Feind, 2004, S. 189 ff. behandelt.

[49] Vgl. ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 11.

[50] Vgl. ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 7.

2.3 Richtlinien für die Authentifizierung im Rahmen der IT-Sicherheit

Innerhalb der Informationstechnik wird die Authentifizierung dem Bereich der IT-Sicherheit zugeordnet.[51] Sie unterliegt damit den für die IT-Sicherheit geltenden Richtlinien und rechtlichen Vorgaben, die in den folgenden Abschnitten dargelegt werden.

2.3.1 Internationale Richtlinien für IT-Sicherheit und Authentifizierung

Für die formale Einhaltung der IT-Sicherheit existieren international unterschiedliche rechtliche Vorgaben und Richtlinien, die im Folgenden erläutert werden. Hierbei werden insbesondere die Anforderungen an die Authentifizierung als Bestandteil der IT-Sicherheit hervorgehoben.

Als formeller europäischer Standard für IT-Sicherheit existieren seit 1991 die rechtlichen Vorgaben für Information Technology Security Evaluation Criteria (ITSEC)[52], deren funktionale Anforderungen teilweise auf das 1983 veröffentlichte Orange Book bzw. die Trusted Computer Security Evaluation Criteria (TCSEC) zurückgehen.[53] Aus den IT-Sicherheitsstandards unterschiedlicher Länder wie der ITSEC wurden 1996 die gemeinsamen Common Criteria (CC) als internationale Richtlinien für IT-Sicherheit erstellt. Seit 1999 liegen diese in der Version 3.0 vor.[54] Neben unterschiedlichen Sicherheitsstufen (Evaluation Assurance Level, kurz: EAL), die die Höhe der erzielten Sicherheit beschreiben, umfassen die CC unterschiedliche Funktionsklassen, die als Basis für die technischen Anforderungen zur Gewährleistung der IT-Sicherheit dienen.[55]

Für die Authentifizierung ist insbesondere die Klasse FIA (Identifikation und Authentisierung) relevant. Sie beschreibt Anforderungen an Funktionen zu Einrichtung und Verifizierung angegebener Benutzeridentitäten. Zusätzlich umfasst die FIA die Zuordnung der Benutzer bzw. Identitäten zu entsprechenden Berechtigungen (Autorisierung). Die verbindliche Authentifizierung von Absender und Empfänger während einer Übertragung wird in FCO (Kommunikation) beschrieben. Anforderungen an die Authentifizierung stellen überdies die Klassen FPR (Privatheit) in Bezug auf den Datenschutz der Identitätsinformationen (inkl. Authentifizierungsmerkmale) sowie FAU (Sicherheitsprotokollierung) durch die erforderliche Protokollierung und eindeutige Zuordnung einer

---

[51] Vgl. ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 187 ff.

[52] Vgl. ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 384 ff.; COMMISSION OF THE EUROPEAN COMMUNITIES: Information Technology Security Evaluation Criteria (ITSEC): Preliminary Harmonised Criteria, 1991.

[53] Vgl. DEPARTMENT OF DEFENSE: DOD 5200.28-STD. Trusted Computer System Evaluation Criteria, 1983.

[54] Vgl. BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: Common Criteria. Version 2.3, 2006.

[55] Vgl. ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 228 f.

sicherheitsrelevanten Handlung zu einer Person her. Bezogen auf die Funktionsklassen definieren die CC Schutzprofile (protection profiles, kurz: PP). Diese definieren konkrete Sicherheitsanforderungen und -ziele bzw. -maßnahmen innerhalb der Funktionsklassen für die Gewährleistung der IT-Sicherheit. Maß für die Höhe der Gewährleistung ist der im Rahmen einer Evaluierung insgesamt erzielte EAL. EAL werden beispielsweise als Maß der von einem Betriebssystem bzw. einer Software oder Hardware erzielten IT-Sicherheit verwendet.[56] Eine CC-Evaluierung kann in Deutschland durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) erfolgen.[57]

In den USA beschreiben des Weiteren insbesondere die Federal Information Processing Standards (FIPS) Richtlinien für die Authentifizierung.[58] Bereits FIPS 113 (Computer Data Authentication) aus dem Jahr 1985 definiert die allgemeine Authentizität von Daten basierend auf dem symmetrischen Verschlüsselungsstandard Data Encryption Standard (DES) aus FIPS 46.[59] FIPS 140-2 enthält Anforderungen an kryptographische Module[60] wie Tokens und Smart Cards beispielsweise für die Verwendung als Hardware Security Module (HSM) in Zertifizierungsrichtlinien.[61] Der in FIPS 180-2 spezifizierte Secure Hash Algorithm (SHA) wird als kryptographisches Hash-Verfahren etwa für die Authentifizierung mittels X.509-Zertifikaten verwendet.[62] FIPS 181 definiert einen automatischen Generator für sichere Passwörter[63], während FIPS 186-2 den Digital Signature Standard (DSS) als Basis für digitale Signaturen und somit die Authentifizierung des Absenders beschreibt.[64] FIPS 190 beschreibt Auswahlkriterien für fortgeschrittene Authentifizierungsverfahren.[65] Insbesondere werden in FIPS 190 Anforderungen an die Sicherheit von Tokens, Zertifikaten

---

[56] Vgl. ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 225, S. 232 ff.

[57] Vgl. BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: Zertifizierung, 2007.

[58] Vgl. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY: Federal Information Processing Standards Publications, 2007.

[59] Vgl. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY: Federal Information Processing Standards Publication 113 - Computer Data Authentication, 1985.

[60] Vgl. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY: Federal Information Processing Standards Publication 140-2 - Security Requirements for Cryptographic Modules, 1994.

[61] Vgl. Beispiel für die Anwendung in einer Zertifizierungsrichtlinie in DFN-CERT SERVICES: Erklärung zum Zertifizierungsbetrieb DFN-PKI Classic Version 1.1, 2005, S. 28.

[62] Vgl. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY: Federal Information Processing Standards Publication 180-2 - Secure Hash Standard, 2002.

[63] Vgl. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY: Federal Information Processing Standards Publication 181 - Automated Password Generator, 1993.

[64] Vgl. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY: Federal Information Processing Standards Publication 186-2 - Digital Signature Standard, 1994.

[65] Vgl. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY: Federal Information Processing Standards Publication 190 - Guideline for the Use of Advanced Authentication Technology Alternatives, 1994.

und biometrischen Verfahren für deren Verwendung in den USA definiert. Gegenseitige Authentifizierung zweier Kommunikationspartner anhand von Public-Key-Verfahren beschreibt FIPS 196 und liefert damit Sicherheitsanforderungen an zertifikatbasierte Authentifizierungsverfahren bzw. Challenge-Response-basierte Schlüsselaustausch-Verfahren wie Diffie-Hellmann.[66] Erweiterungen des DES spezifiziert der Advanced Encryption Standard (AES) in FIPS-197[67], während FIPS 198 seit 2002 eine Erweiterung von SHA für die Prüfung der Authentizität übermittelter Nachrichten als Keyed-Hash Message Authentication Code (HMAC) definiert.[68] Im März 2006 wurden in FIPS 201-1 zusätzlich Vorgaben für die Authentifizierung amerikanischer Regierungsmitarbeiter, basierend auf Zertifikaten, Tokens und biometrischen Verfahren, festlegt.[69]

2.3.2 Rechtliche Grundlagen der IT-Sicherheit und Authentifizierung

Um die Authentifizierung mittels digitaler Signatur rechtlich mit einer Unterschrift gleichzusetzen existiert in Deutschland das Signaturgesetz (SigG) und die zugehörige Signaturverordnung (SigV).[70] Das Signaturgesetz beschreibt zwei Stufen für die Vertrauenswürdigkeit digitaler Signaturen als Authentifizierungsmerkmal für Personen. Äquivalent zur Unterschrift werden rechtlich qualifizierte digitale Signaturen anerkannt. Diese erfordern beispielsweise den Einsatz von Tokens für die Speicherung der Zertifikate und zugehöriger privater Schlüssel sowie vom BSI bzw. der Bundesnetzagentur akkreditierte Zertifizierungsstellen als Aussteller der Zertifikate.[71] Das BSI fordert für die Akkreditierung neben organisatorischen auch technische Vorgaben von den Zertifizierungsstellen, so z.B. die erforderliche Mindestlänge der digitalen Schlüssel.[72] Ziel des SigG ist die Realisierung einer sicheren und zur Unterschrift äquivalenten Sicherheit für elektronische Vorgänge, z.B. im E-Commerce oder E-Government. Das SigG ist daher Bestandteil des Informations- und Kommunikationsdienste-Gesetz (IuKDG), das Vorgaben für die Sicherheit der wirtschaftlichen

---

[66] Vgl. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY: Federal Information Processing Standards Publication 196 - Entity Authentication Using Public Key Cryptography, 1997.

[67] Vgl. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY: Federal Information Processing Standards Publication 197 - Advanced Encryption Standard, 2001.

[68] Vgl. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY: Federal Information Processing Standards Publication 198 - The Keyed-Hash Message Authentication Code, 2002.

[69] Vgl. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY: Federal Information Processing Standards Publication 201-1 - Personal Identity Verification for Federal Employees and Contractors, 2006.

[70] Vgl. BUNDESMINISTERIUM DER JUSTIZ: Gesetz über Rahmenbedingungen für elektronische Signaturen (SigG), 2001; BUNDESMINISTERIUM DER JUSTIZ: Verordnung zur elektronischen Signatur (SigV), 2001

[71] Vgl. BUNDESNETZAGENTUR: Zertifizierungsdiensteanbieter, 2007.

[72] Vgl. BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: Kryptoalgorithmen, 2007.

Nutzung von IT-Strukturen (u.a. E-Commerce) beinhaltet.[73] Den Schutz der bei der Authentifizierung verwendeten digitalen Identitäten reguliert zusätzlich das Bundesdatenschutzgesetz (BDSG).[74] Dies ist insbesondere für die Aggregation von Daten bei bestehenden Verfahren für eine einheitliche Authentifizierung wie bei Verzeichnisdiensten und Public-Key-Infrastrukturen, relevant.[75]

Neben den genannten Richtlinien werden an Banken und Unternehmen durch den Sarbanes-Oxley Act (SOX) in den USA oder Basel II in Europa Anforderungen an die Gewährleistung der IT-Sicherheit gestellt. SOX soll seit 2002 die Korrektheit wirtschaftlicher Bilanzen und die Auditierbarkeit von Geschäftsprozessen sichern.[76] Seit Juni 2006 gilt dies auch für ausländische Unternehmen, die an der US-Börse vertreten sind. Basel II stellt Eigenkapitalrichtlinien für die Kreditvergabe an Unternehmen dar, die ab 2007 in europäischen Mitgliedstaaten umgesetzt werden müssen. Beide bezwecken ein Risiko Management, das sich auch auf die IT-Strukturen der Firmen auswirkt. Insbesondere stellt das Risiko Management Anforderungen an die Gewährleistung der IT-Sicherheit, die die Risiken innerhalb der IT-Struktur bestimmt. SOX und Basel II stellen damit neben den genannten Richtlinien für IT-Sicherheit Anforderungen an die durch die Authentifizierung zu erzielende IT-Sicherheit in Unternehmen.[77]

2.4 Authentifizierungsmodelle

In den folgenden beiden Abschnitten werden die in den vorherigen Abschnitten genannten Begriffe auf Authentifizierungsmodelle abgebildet. Die Modelle spiegeln dabei die Beteiligten (Benutzer und Betreiber) und deren Authentifizierung für den Zugriff auf Ressourcen wider. Abschnitt 2.4.1 zeigt zunächst ein bestehendes Modell für die Authentifizierung in homogenen IT-Strukturen auf. Dieses Modell wird in Abschnitt 2.4.2 für die Authentifizierung in heterogenen IT-Strukturen als Grundlage der vorliegenden Arbeit erweitert.

---

[73] Vgl. UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN: Die wichtigsten Bestimmungen des Informations- und Kommunikationsdienste-Gesetzes (IuKDG), 2007.

[74] Vgl. BUNDESMINISTERIUM DER JUSTIZ: Bundesdatenschutzgesetz (BDSG), 1990.

[75] Vgl. zur Aggregation von Daten bzw. Datenschutzaspekten BIETHAHN, J.; CVJETKOVIC, D.; ORTHEY, F.; MUCKSCH, H.; NISSEN, V.: Datenschutz, Datensicherheit und gesellschaftliche Auswirkungen der Informationsverarbeitung. 3. Aufl., 2000.

[76] Vgl. UNITED STATES OF AMERICA: One Hundred Seventh Congress of the United States of America - „Sarbanes-Oxley-Act“, 2002; einen Überblick über die Relevanz für die IT-Sicherheit liefert HURLEY, E.: Security and Sarbannes-Oxley, 2003.

[77] Vgl. BUNDESBANK: Basel II - Die neue Baseler Eigenkapitalvereinbarung, 2007; einen Überblick über die Relevanz für die IT-Sicherheit liefert CORPORATE-CONSULTING.NETWORK: IT-Sicherheit als Rating-Faktor, 2006.

2.4.1 Authentifizierung in homogenen IT-Strukturen

In homogenen IT-Strukturen werden die den Benutzern angebotenen Dienste von genau einem Software-Produkt oder einer Plattform (z.B. Windows oder Unix) erbracht. Die einzelnen Software-Produkte für die Dienste stammen dabei häufig von einem einzigen oder wenigen Herstellern. Somit wird eine einheitliche Plattform verwendet, die eine effiziente und kostengünstige Administration erlaubt, aber in Bezug auf die möglichen Dienste keine hohe Flexibilität aufweist. Es können ausschließlich Software-Produkte eingesetzt werden, die kompatibel zur bestehenden Plattform und zu den Software-Komponenten des bevorzugten Herstellers sind. Bei Fehlfunktionen müssen Ausbesserungen des gewählten Herstellers abgewartet werden, sofern dieser keine Standardverfahren verwendet, die auch von Drittherstellern implementiert werden. Die Bindung an den Hersteller kann zudem durch starre Lizenzmodelle oder Serviceverträge zusätzlich verstärkt werden. Neben dem Umstand, dass IT-Strukturen wachsen und somit ohnehin einer kontinuierlichen Veränderung unterliegen[78], sind dies mögliche Ursachen dafür, dass insbesondere in großen IT-Strukturen praktisch keine vollständig homogenen Umgebungen existieren. Als homogene Systeme werden daher im Folgenden Teilbereiche von IT-Strukturen bezeichnet, in denen für die Authentifizierung genau ein Authentifizierungssystem und -verfahren zum Einsatz kommt. Ausschließlich dieses System verwaltet alle für den Teilbereich erforderlichen Identitäten, Authentifizierungsmerkmale und -verfahren. Diese Bedingung erfüllen Authentifizierungsmodelle aus der Literatur zur IT-Sicherheit.[79]

Abbildung 2-1 zeigt das Authentifizierungsmodell nach SMITH. SMITH unterteilt die Authentifizierung in fünf Elemente:

- den Benutzer bzw. die Person (person), die sich authentisiert;
- das Authentifizierungsverfahren (authentication mechanism), welches Verlauf und Ergebnis der Authentifizierung bestimmt;
- ein eindeutiges Merkmal als Authentifizierungsmerkmal (distinguishing characteristic), über welches nur die Person verfügt, die hierdurch eindeutig identifiziert wird;
- eine Zugriffskontrolle (access control), die als Autorisierung nach der Authentifizierung erfolgt und für die Person den Zugriff auf eine Ressource gewährt;

---

[78] Vgl. MOORE, G. E.: Moore's Law, 1965.

[79] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 3 f., BOYD, C.; MATHURIA, A.: Protocols for Authentication and Key Establishment, 2003, S. 3 ff.

- den Besitzer bzw. Betreiber (proprietor) oder Administrator, der das Authentifizierungssystem resp. die verwendeten -verfahren verwaltet.

Die Abbildung zeigt anhand der Pfeile das Zusammenspiel der Komponenten während einer Authentifizierung. Der Benutzer verwendet hierbei ein Authentifizierungsmerkmal (z.B. ein Passwort) in Kombination mit einem Benutzernamen, das anhand eines Authentifizierungsverfahrens geprüft wird, welches damit über den Erfolg der Authentifizierung entscheidet. Die notwendigen Vorgaben für die Prüfung werden bei der Konfiguration des Authentifizierungsverfahrens durch den Betreiber festgelegt. Nach einer erfolgreichen Authentifizierung kann durch eine Zugriffskontrolle geprüft werden, ob der Benutzer berechtigt ist, anschließend Zugriff auf die Ressource zu erlangen.

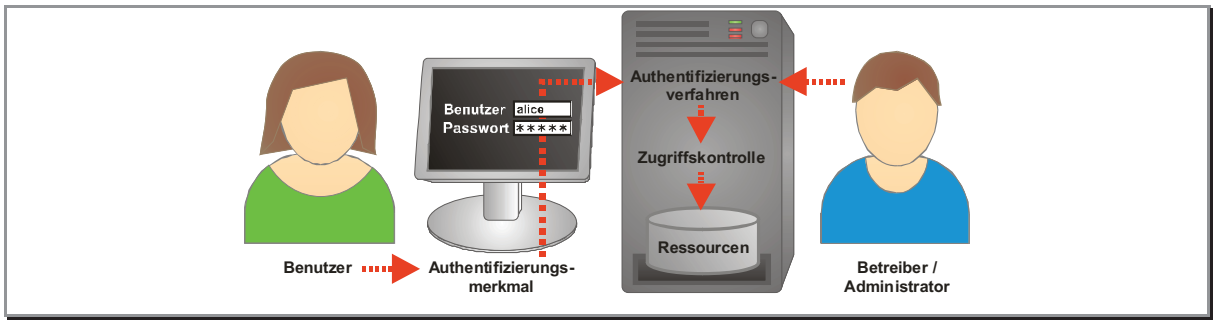

Abbildung 2-1: Authentifizierungsmodell nach SMITH[80]

SMITH bezeichnet dieses einfachste Authentifizierungsverfahren als lokale oder direkte Authentifizierung.[81]

Grenzen des von SMITH aufgezeigten Modells lassen sich beispielsweise an dem Authentifizierungsverfahren Kerberos[82] erkennen, das am Massachusetts Institute of Technologie (kurz MIT) entwickelt wurde. Die Authentifizierung erfolgt bei Kerberos gegenüber einem getrennten Server (Key Distribution Center, kurz KDC) als Authentifizierungssystem, der die vom Benutzer gewünschten Ressourcen nicht selbst bereitstellt. Authentifizierungsmodelle, die genau ein Authentifizierungsverfahren, ein einziges Authentifizierungssystem und ein Authentifizierungsmerkmal pro Benutzer umfassen, können als homogen betrachtet werden. Für die Beschreibung der einheitlichen Authentifizierung in heterogenen e-Science-Umgebungen, in denen stattdessen mehrere Authentifizierungsverfahren und -systeme verwendet werden, ist daher ein erweitertes Modell erforderlich, das im Abschnitt 2.4.2 für die weitere Betrachtung eingeführt wird.

---

[80] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 4.

[81] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 188 ff.

[82] Vgl. GARMAN, J.: Kerberos. The Definitive Guide, 2003, S. 25.

2.4.2 Authentifizierung in heterogenen IT-Strukturen

Die im vorherigen Abschnitt beschriebenen bestehenden Modelle der Authentifizierung beziehen sich nur auf ein vom Benutzer verwendetes Authentifizierungsverfahren, das gegenüber einem Authentifizierungssystem mit genau einem Authentifizierungsmerkmal pro Benutzer durchgeführt wird. Modelle, wie sie im vorherigen Abschnitt beschrieben werden, eignen sich daher nur für die Beschreibung von homogenen Umgebungen, in denen von vornherein eine einheitliche Authentifizierung (mit genau einem einheitlichen Authentifizierungsverfahren, -system und -merkmal pro Benutzer) existiert. Für die im Folgenden beschriebene Betrachtung von heterogenen IT-Strukturen[83] wird daher ein erweitertes Modell eingeführt, das neben den in Abschnitt 2.4.1 genannten Elementen Authentifizierungsmerkmale und -verfahren zusätzlich Authentifizierungssysteme einführt. Die Vielzahl der diversen Systeme, Verfahren und Merkmale resultiert neben der Anzahl der unterschiedlichen Benutzer zusätzlich aus der Anzahl unterschiedlicher Ressourcen innerhalb heterogener IT-Strukturen.[84] Abbildung 2-2 skizziert die entsprechende Erweiterung des in Abschnitt 2.4.1 definierten Authentifizierungsmodells. Die im Kapitel 5 folgende Modellierung einer einheitlichen Authentifizierung für heterogene IT-Strukturen fokussiert daher die Optimierung von Authentifizierungsmerkmalen, -verfahren und -systemen.

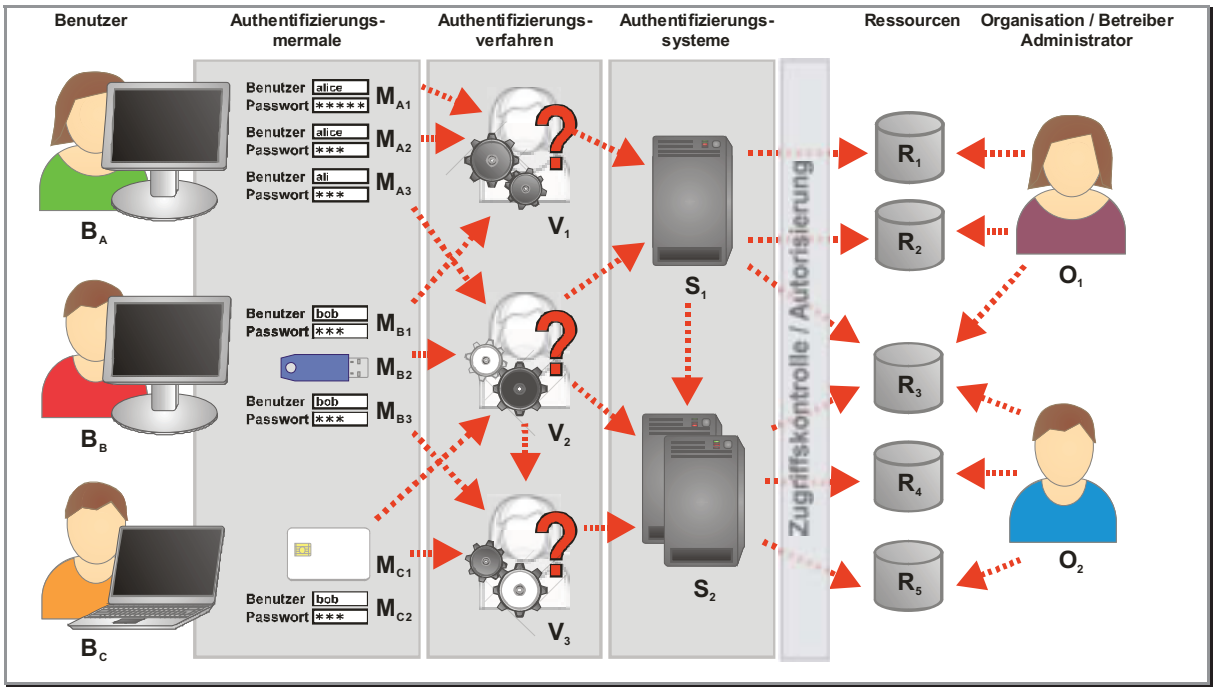

Abbildung 2-2: Authentifizierung als Basis für den Zugriff auf Ressourcen in heterogenen und verteilten IT-Strukturen

[83] Vgl. Abschnitt 2.1.10.

[84] Vgl. Verwendung unterschiedlicher Hard- und Software in heterogenen IT-Strukturen in Abschnitt 2.1.10.

In dem in der Abbildung gezeigten Beispiel besitzt der Benutzer B_B drei unterschiedliche Authentifizierungsmerkmale. M_{B1} und M_{B3} bilden unterschiedliche Passwörter[85], M_{B2} ist ein zusätzliches Token.[86] Der Benutzer kann damit sowohl das Verfahren V_1 und V_2 als auch V_3 für die Authentifizierung verwenden. V_1 könnte eine direkte Authentifizierung am E-Mail-System darstellen, V_3 die Authentifizierung über Kerberos, beispielsweise an einem Active Directory Domänencontroller. So verwendet V_2 ein Zertifikat für die Off-line-Authentifizierung. Wie in der Abbildung dargestellt, kann dies auch über V_3 (Kerberos) erfolgen, womit beide Verfahren verkettet werden.[87] S_2 bildet den Active Directory Domänencontroller, der die Authentifizierungskonten hält. Für die Off-line-Authentifizierung müsste hier zusätzlich noch die Public-Key-Infrastruktur bzw. die Zertifizierungsstelle als Authentifizierungssystem differenziert werden.[88] S_1 bildet das Authentifizierungssystem des Mail-Servers. Dieses könnte, wie in der Abbildung gezeigt, auch das Zertifikat mittels Off-line-Authentifizierung V_2 akzeptieren. Es kann jedoch auch selbst verkettet werden und letztendlich Benutzerkonten des Active Directory Domänencontrollers S_2 für die Authentifizierung der Benutzer verwenden. Zugriffskontrolle bzw. Autorisierung, wie in Abschnitt 2.4.1 genannt, werden in dieser Arbeit und damit im obigen Modell für heterogene IT-Strukturen nicht betrachtet. Die Authentifizierung dient jedoch als Grundlage für die anschließende Autorisierung. Im Folgenden wird für die Vielzahl der innerhalb der IT-Struktur zur Verfügung gestellten Ressourcen, die eine Authentifizierung erfordern, auch die Möglichkeit der Kooperation der Betreiber berücksichtigt. In der Abbildung 2-2 wird die Ressource R_3 kooperativ von O_1 und O_2 angeboten und verwaltet.

In der Praxis kann ein Verfahren mehreren Systemen und ein System unterschiedlichen Verfahren zugewiesen sein. Gleiches gilt für die Beziehungen zwischen Merkmalen und Verfahren. Die theoretische Grundlage für dieses Modell wird in Kapitel 5 detailliert beschrieben. Die Abbildung 2-2 verdeutlicht die Diversität von Authentifizierungsmerkmalen, -verfahren und -systemen. In heterogenen IT-Strukturen werden darüber hinaus deutlich mehr Ressourcen und Benutzer verwaltet als im skizzierten vereinfachten Beispiel.

---

[85] Die Passwörter muss der Benutzer kennen bzw. sich merken.

[86] Das Token muss der Benutzer besitzen.

[87] Dies kann über das Verfahren PKINIT erfolgen, das die Authentifizierung an Kerberos mittels Zertifikat resp. Token erlaubt.

[88] Die Ausstellung von Zertifikaten erfolgt im Rahmen einer Public-Key-Infrastruktur.

2.5 Authentifizierungsmerkmale und -faktoren

Neben den häufig verwendeten Passwörtern existiert eine Vielzahl weiterer Ausprägungen von Authentifizierungsmerkmalen in heterogenen IT-Strukturen. In der Literatur werden diese häufig in die Kategorien Kenntnis („something you know“), Besitz („something you have“) und persönliche Eigenschaft („something you are“) unterteilt.[89] Diese Kategorien werden auch als Authentifizierungsfaktoren bezeichnet. Um eine hohe Sicherheit zu gewährleisten, wird für die erfolgreiche Authentifizierung mancher Verfahren die Überprüfung mehrerer Faktoren erfordert. Dies bezeichnet man auch als Multi-Faktor-Authentifizierung. Die folgenden Abschnitte geben einen Überblick über die einzelnen Faktoren.

2.5.1 Kenntnis einer Information

Passwörter stellen die am weitesten verbreitete Ausprägung von Authentifizierungsmerkmalen dar.[90] Sie bilden die Grundlage für die in den folgenden Abschnitten genannten weiteren Faktoren, die in der Regel ohne Passwort allein nicht eingesetzt werden können.[91] Die Abfrage von Passwörtern kann leicht implementiert werden und ist flexibel anwendbar, da sie ohne spezielle Anforderungen an Rechnern, die über eine Tastatur verfügen, verwendet werden kann. Die Sicherheit von Passwörtern beruht auf der Basis, dass ausschließlich der zu authentifizierende Benutzer Kenntnis über das Passwort hat („something you know“), und somit eindeutig identifiziert werden kann. Gemäß SMITH wird die Verwendung von Passwörtern insbesondere dadurch begrenzt, dass sie einerseits leicht zu merken, andererseits jedoch schwer zu erraten sein sollen.[92]

ANDERSON stellt jedoch fest, dass das Erinnern an komplexe Passwörter (mehr als 12 Zeichen) der häufigste Grund für Beschwerden und Fehler bei dem Design von IT-Sicherheits-Systemen ist.[93] Um die Usability von Passwörtern zu erhöhen, kann die Anforderung an die Komplexität (z.B. die erforderliche Mindestlänge) herabgesetzt werden, sofern die dadurch reduzierte IT-Sicherheit in Kauf genommen werden kann. Zusätzlich können alternativ zu textbasierten auch graphische Passwörter eingesetzt werden. Benutzer merken sich in diesem Fall Bilder oder Bildkombinatio-

---

[89] Vgl. KENT, S. T.; MILLETT, L. I.: Who goes there? Authentication Through the Lens of Privacy, 2003, S. 106 ff. und SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 28 ff.

[90] Gemäß CHESWICK, W. R.; BELLOWIN, S. M., RUBIN, A. D.: Firewalls und Sicherheit im Internet. 2. Aufl., 2004, S. 180 ff.

[91] Vgl. BURNETT, M.; KLEIMAN, D.: Perfect Passwords, 2006, S. 131.

[92] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 157 f.

[93] Vgl. ANDERSON, R.: Security Engineering. A Guide to Building Dependable Distributed Systems, 2001, S. 36.

nen, die aus kognitiver Sicht leichter merkbar sind.[94] Beispiele hierfür sind Passfaces oder inkblots.[95] RENAUD unterteilt daher die Authentifizierung anhand von Kenntnis bzw. erforderlichem Wissen der Benutzer in drei Kategorien:[96]

- Zufällige Passwörter (random passwords), bestehend aus zufälligen Sequenzen von Buchstaben, Ziffern und Zeichen. Passwörter die ausschließlich aus Ziffern bestehen, werden auch als Personal Identification Number (PIN) bezeichnet. Bestehen Passwörter aus mehreren Wörtern, so spricht RENAUD von einer Passphrase. Zufällige Passwörter müssen ohne Hinweis abgerufen werden. Benutzer tendieren daher dazu, einfache Passwörter (einfache Buchstaben- und Ziffernkombinationen geringer Komplexität) zu verwenden.
- Kulturelle Passwörter (cultural passwords), die Hinweise für die Erinnerung bzw. den Abruf der Passwörter liefern. Beispiel hierfür sind Challenge-Response-Verfahren. Hierbei werden Benutzer z.B. nach dem Familiennamen Ihrer Mutter, dem Namen ihres ersten Haustiers oder der Grundschule, die sie besuchten, gefragt. Die korrekten Antworten auf mehrere dieser Fragen bilden das Authentifizierungsmerkmal.
- Auf Erkennung (recognition) basierende Passwörter, wie sie bereits als graphische Passwörter durch Bildfolgen, -positionen oder -strukturen beschrieben wurden.

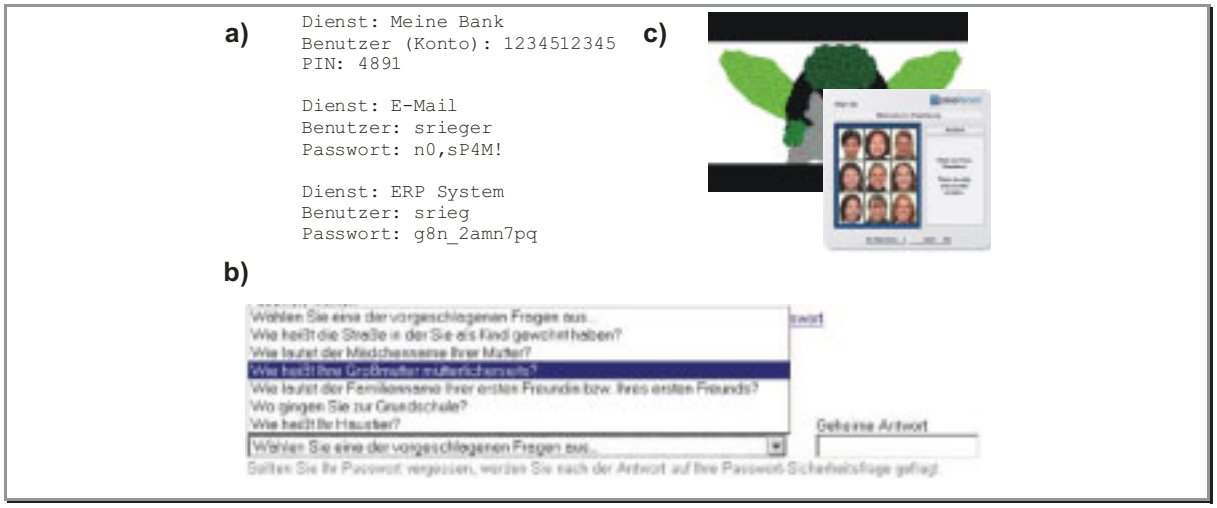

Abbildung 2-3: Beispiele für Kenntnis-basierte Authentifizierungsmerkmale

[94] Vgl. MONROSE, F.; REITER M. K.: Graphical Passwords, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 159.

[95] Vgl. passfaces, 2007; ROSS, S.: Is It Just My Imagination? (Inkblots), 2007.

[96] Vgl. RENAUD, K.: Evaluating Authentication Mechanisms, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 103 ff.

Abbildung 2-3 zeigt unterschiedliche Beispiele für Authentifizierungsmerkmale, die auf Kenntnis basieren. a) zeigt Passwörter und PINs für drei unterschiedliche Dienste. Über b) wird beim Internet-Auktionshaus eBay anhand von kulturellen Passwörtern die Authentifizierung und anschließende Änderung des Passworts ermöglicht, sofern dieses vergessen wurde.[97] Beispiele für graphische Passwörter, z.B. passfaces, das auf der Wiedererkennung von Gesichtern basiert[98], oder Microsofts inkblots, bei denen ein Passwort mit einer Interpretation eines Bildes bzw. Musters verknüpft wird[99], zeigt Abbildung 2-3 c).

2.5.2 Besitz eines Tokens

Insbesondere um die Angriffe durch Abhören der im vorherigen Abschnitt genannten auf Kenntnis basierenden Merkmale zu verhindern, wurden Verfahren entwickelt, die neben der Kenntnis auch den Besitz eines physikalischen Merkmals erfordern. Der Benutzer muss für die erfolgreiche Authentifizierung den Besitz nachweisen („something you have“). Diese physikalischen Merkmale werden als Tokens bezeichnet. Häufig ist für die Verwendung oder Aktivierung des Tokens zusätzlich eine PIN oder ein Passwort, wie im vorherigen Abschnitt geschildert, notwendig. Auf diese Weise ermöglichen Tokens eine auf mehreren Faktoren basierende Authentifizierung (Multi-Faktor-Authentifizierung). SMITH unterscheidet zwischen passiven und aktiven Tokens:[100]

- Passive Tokens übermitteln bei deren Verwendung direkt das erforderliche Merkmal bzw. Geheimnis um die Authentifizierung, basierend auf dem Besitz, durchzuführen. Beispiele sind herkömmliche Schlüssel oder Karten mit Magnetstreifen, die Ihre Informationen direkt zum Zweck der Authentifizierung übertragen.
- Aktive Tokens geben das Merkmal bzw. Geheimnis nicht bei der Authentifizierung preis. Sie verwenden das Merkmal lediglich intern bzw. indirekt, um dessen Besitz nachzuweisen. Beispiele hierfür sind Geräte, die Einmal-Passwörter (One Time Passwords - OTP) erzeugen und auf einem Display darstellen, oder Crypto-Karten (SmartCards) und -USB-Tokens, die einen privaten Schlüssel speichern, der nicht ausgelesen, aber für die Erzeugung einer digitalen Signatur verwendet werden kann. Einmal-Passwörter werden nur für einen einzigen Authentifizierungsvorgang verwendet. Wird das Passwort von einem Dritten abgehört, kann es somit nicht für nachfolgende Authentifizierungen verwendet werden. One-Time-Passwords können in

[97] Vgl. eBay, 2007.

[98] Vgl. passfaces, 2007.

[99] Vgl. ROSS, S.: Is It Just My Imagination? (Inkblots), 2007.

[100] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 257 ff.

Challenge-Response-Verfahren verwendet werden. Ein Beispiel hierfür bildet das S/Key-Verfahren.[101] Auch eine Aushändigung von Einmal-Passwörtern in Form einer Liste (vgl. die Ausgabe von TAN-Listen von Kreditinstituten) ist möglich. Zusätzlich können Einmal-Passwörter direkt mittels aktivem Token nach einem gemeinsamen Verfahren (zähler- oder zeitbasiert) durch die Benutzer und Organisationen dynamisch erzeugt werden. Ein aktives Token kann der Benutzer durch die Eingabe einer PIN oder eines Passworts entsperren. Das Token empfängt daraufhin externe Daten und verschlüsselt diese mit dem nicht auslesbaren privaten Schlüssel. Um zusätzlich das Abhören der PIN für die Aktivierung des Tokens zu vermeiden existieren bereits Lösungen, die u.a. die Eingabe der PIN physikalisch auf dem Token selbst erlauben.[102]

Abbildung 2-4 zeigt Beispiele für aktive Tokens. Im Rahmen dieser Arbeit wurden GPK16000 SmartCards der Fa. GemPlus[103], eToken der Fa. Aladdin[104] sowie SecureID Tokens der Fa. RSA[105] verwendet.

Abbildung 2-4: Beispiele für aktive Tokens

Der Einsatz von physikalischen Authentifizierungsmerkmalen bietet folgende Vorteile:[106]

- Es kann eine Multi-Faktor-Authentifizierung erzielt werden, die den Besitz eines Tokens sowie die Kenntnis einer PIN oder eines Passworts für die Aktivierung des Tokens erfordert.
- Tokens sind schwerer zu duplizieren als Passwörter.
- Der Verlust des Tokens ist für den Benutzer physikalisch feststellbar. Er kann daraufhin den Zugang sperren lassen. Der Verlust eines Passworts durch Abhören kann nicht unmittelbar

[101] Vgl. ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 445 ff.
[102] Vgl. Cypak PIN-on-Card, 2007.
[103] Vgl. GemPlus, 2007.
[104] Vgl. Aladdin eToken, 2007.
[105] Vgl. RSA SecureID, 2007.
[106] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 256.

festgestellt werden. Allerdings ist die Erzeugung eines neuen Tokens schwieriger als die Vergabe eines neuen Passworts.

Neben dem Einsatz von physikalischen Tokens kann der Besitz auch durch Zertifikate und zugehörige private Schlüssel nachgewiesen werden. Das Zertifikat stellt hierbei einen signierten öffentlichen Schlüssel dar, der eindeutig einer Person zugeordnet wird. Der private Schlüssel bildet gewissermaßen ein virtuelles Token, das z.B. durch die Eingabe eines PINs oder Passworts aktiviert wird. Für heterogene IT-Strukturen entsteht hierbei der Vorteil, dass die authentifizierende Instanz nicht das private Authentifizierungsmerkmal resp. den privaten Schlüssel, sondern den öffentlichen Schlüssel bzw. das Zertifikat verwendet. Das eigentliche geheime Authentifizierungsmerkmal in Form des privaten Schlüssels wird somit nicht verteilt und verbleibt ausschließlich bei dessen Besitzer. Zertifikate nach dem X.509-Standard[107] können daher leicht über die heterogene IT-Struktur verteilt und von unterschiedlichen Anwendungen auf unterschiedlichen Plattformen verwendet werden, ohne dass die Sicherheit durch die Hinterlegung oder Verwendung der Authentifizierungsmerkmale gemindert wird.

2.5.3 Biometrische Eigenschaft

Biometrische Eigenschaften bieten sich für die Authentifizierung von Personen an, da jeder Mensch über entsprechende eindeutige Merkmale verfügt. Beispiele sind Fingerabdrücke, Iris-Strukturen, Gesichtsfeld- oder Hand-Geometrien.[108] Für die erfolgreiche Authentifizierung muss der Benutzer das entsprechende persönliche Merkmal vorweisen („something you are“). Auch Pässe sollen durch biometrische Eigenschaften der Person erweitert werden und so eine höhere Sicherheit erzielen.[109] Relativ neu sind in diesem Zusammenhang Verfahren, die Tastendrücke (typing patterns) auf der Tastatur und somit das Tippverhalten der Benutzer als biometrische Eigenschaft für die Authentifizierung nutzen.[110]

---

[107] Vgl. HOUSLEY, R. ET AL.: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 3280), 2002.

[108] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 193 ff. und ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 479 ff.

[109] Vgl. BUNDESMINISTERIUM DES INNEREN: Hintergrundinformationen zum ePass. Technik & Sicherheit, 2007.

[110] Vgl. PEACOCK, A.; KE, X.; WILKERSON, M.: Identifying Users from Their Typing Patterns, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 199 ff.

Während sich biometrische Verfahren leicht durch Personen anwenden lassen, weisen sie entscheidende Nachteile auf:[111]

- Personen mit Behinderungen können durch biometrische Verfahren benachteiligt werden (etwa bei Amputationen). Allgemein können sich biometrische Merkmale einer Person verändern; z.B. kann die Iris während der Schwangerschaft Veränderungen unterliegen.
- Im Gegensatz zu Passwörtern, PINs, Zertifikaten bzw. den in den vorherigen Abschnitten genannten Faktoren können Eigenschaften nicht weitergegeben werden. Soll ein Vertreter beispielsweise bedingt durch Krankheit des Benutzers kurzzeitig dessen Funktion übernehmen, so kann er die biometrischen Verfahren nicht verwenden. Ein Passwort könnte kurzfristig jedoch mitgeteilt und später geändert werden. Diese mögliche Änderung des Authentifizierungsmerkmals ist ein weiterer Nachteil von biometrischen Verfahren. Soll ein Zugang gesperrt werden, da z.B. die Daten des Fingerabdrucks einer Person bei deren Eingabe kopiert wurden, muss der Benutzer zukünftig einen anderen Finger oder die andere Iris für die Authentifizierung verwenden. Dies lässt sich nur begrenzt fortsetzen.
- Maschinen besitzen keine biometrischen Eigenschaften. Die Authentifizierung eines Dienstes oder der Web-Seite eines Kreditinstituts ist somit nicht möglich. Ein einziges einheitliches Authentifizierungsverfahren, das ausschließlich biometrische Merkmale verwendet, ist innerhalb einer heterogenen Umgebung somit nicht sinnvoll (bzw. erlaubt keine Authentifizierung der Clients und Server).

Insgesamt ist die biometrische Authentifizierung in heterogenen IT-Strukturen aufgrund der genannten Nachteile nicht einheitlich anwendbar bzw. für in der Praxis auftretende Fälle wie Vertretung oder Kompromittierung der Merkmale zu unflexibel.[112] Biometrische Verfahren werden daher für die Vereinheitlichung im Folgenden nicht betrachtet.

2.5.4 Lokation, Zeit

Auch die Lokation eines Benutzers kann für die Authentifizierung genutzt werden. In der Realität kann eine fremde Person beispielsweise authentifiziert werden, sofern sie am verabredeten Treff-

[111] Vgl. COVENTRY, L.: Usable Biometrics, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 192 ff. und CHESWICK, W. R.; BELLOWIN, S. M., RUBIN, A. D.: Firewalls und Sicherheit im Internet. 2. Aufl., 2004, S. 90 f.

[112] Vgl. RENAUD, K.: Evaluating Authentication Mechanisms, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 109, 116 f., 120, 122.

punkt erscheint. Neben dem Ort kann auch die gewählte Zeit für die Authentifizierung dienen. Dieses Prinzip wird auch bei Zeitschlössern verwendet.

In IT-Strukturen wird an vielen Stellen eine Authentifizierung basierend auf der aktuellen Adresse (z.B. IP-Adresse im Netzwerk) des Benutzers durchgeführt.[113] Dieses Vorgehen ist für die Authentifizierung jedoch zunehmend ungeeignet, da sich alle gängigen Adressen und Adressierungsverfahren im Netzwerk gleichermaßen fälschen lassen.[114] Genauso können Zeitstempel auch von unbedarften Benutzern leicht gefälscht werden. So kann der Versender einer E-Mail die Absenderadresse in seinem Programm frei wählen und zusätzlich die Uhrzeit vor dem Versenden der Nachricht verstellen. Aufgrund der dadurch reduzierten Sicherheit werden im Folgenden keine Authentifizierungsverfahren basierend auf Lokation oder aktueller Zeit verwendet.

2.6 Kryptographie als Basis für Authentifizierungsverfahren

Authentifizierungsverfahren erfordern eine vertrauliche Übertragung der Daten, wie in Abschnitt 2.2.1 beschrieben, um ein Abhören der Authentifizierungsinformationen durch unberechtigte Dritte zu verhindern. Zusätzlich muss die Integrität und Verbindlichkeit der übertragenen Daten gewährleistet werden, um zu verhindern, dass unberechtigte Dritte die Authentifizierung eines Benutzers übernehmen können. Die Kryptographie beschreibt Verfahren, um die in Abschnitt 2.2 aufgeführten Anforderungen bzw. Grundwerte der IT-Sicherheit zu erfüllen.[115] Die erforderlichen kryptographischen Grundlagen für die Realisierung von Authentifizierungsverfahren werden in den folgenden Abschnitten erläutert.

2.6.1 Symmetrische und asymmetrische Verschlüsselung

Um die Vertraulichkeit der Authentifizierung zu gewährleisten, existieren verschiedene Verschlüsselungsverfahren. Diese lassen sich in symmetrische und asymmetrische Verschlüsselung unterteilen. Symmetrische Verfahren verwenden für die Entschlüsselung den gleichen Schlüssel wie für die Verschlüsselung. Schlüssel können zufällige Bitfolgen sein, die Absender und Adressat bekannt sind und beispielsweise mittels exklusivem Oder (XOR) mit dem Datenstrom verknüpft werden

---

[113] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 232 ff. und CHESWICK, W. R.; BELLOWIN, S. M., RUBIN, A. D.: Firewalls und Sicherheit im Internet. 2. Aufl., 2004, S. 192.

[114] Vgl. PEIKARI, C.; CHUWAKIN, A.: Kenne Deinen Feind, 2004, S. 189 ff.

[115] Insbesondere gewährleistet die Kryptographie die Vertraulichkeit gemäß Abschnitt 2.2.1 durch eine Verschlüsslung von Informationen.

und diesen damit verschlüsseln (Strom- und Blockchiffren).[116] Beispiel bildet der Advanced Encryption Standard (AES), dessen zugrunde liegender Algorithmus Schlüssel mit einer Länge von 256 Bit verwendet.[117] Weitere Beispiele sind die Rivest Cipher 2,4 und 5 (RC2, RC4 und RC5)[118], der Data Encryption Standard (DES) sowie „triple DES" (3DES)[119] und der International Data Encryption Algorithm (IDEA).[120] Symmetrische Verschlüsselung erfordert den vorherigen gesicherten Schlüsselaustausch zwischen den Kommunikationspartnern, ohne dass ein Dritter Zugriff auf den verwendeten Schlüssel erhält. Daher erfolgt bei dem Schlüsselaustausch in der Regel eine vorherige Authentifizierung der Kommunikationspartner.

Asymmetrische Verfahren teilen dieses Vorgehen in einen Schlüssel zum Verschlüsseln und einen Komplementärschlüssel zum Entschlüsseln der Daten auf. Die Schlüssel werden als private und öffentliche Schlüssel (private keys und public keys) bezeichnet. Daten, die mit dem privaten Schlüssel verschlüsselt wurden, lassen sich nur mit dem öffentlichen entschlüsseln und umgekehrt. Der private Schlüssel lässt sich dabei nicht vom öffentlichen ableiten. Um die Gewinnung des Komplementärschlüssels zu verhindern, werden mathematische Probleme wie die Faktorisierung großer Primzahlen beim RSA (Rivest Shamir Adleman)-Verfahren oder die Berechnung eines diskreten Logarithmus bei Diffie-Hellman (als Verfahren für den sicheren Schlüsselaustausch) eingesetzt.[121] Da diese Probleme erst für große Zahlen hinreichend schwer durchzuführen sind, werden für asymmetrische Verfahren in der Regel Schlüssel ab einer Länge von 1024 Bit bzw. 2048 Bit empfohlen.[122] Anders als symmetrische Verfahren erfordern asymmetrische Verfahren keinen vorherigen sicheren Schlüsselaustausch, da der öffentliche Schlüssel frei verteilt werden kann, da nur der Besitzer des zugehörigen privaten Schlüssels in der Lage ist, ihn zu entschlüsseln. Typische asymmetrische Verschlüsselungs- und Schlüsselaustauschverfahren sind Rivest Shamir Adleman (RSA), Diffie-Hellman und ElGamal.[123] Eine detaillierte Beschreibung symmetrischer und asymmetrischer Verschlüsselungsverfahren liefern beispielsweise BIETHAHN ET AL.., BUCHMANN und

---

[116] Vgl. SCHNEIER, B.: Angewandte Kryptographie, 1996, S. 223 ff. sowie BUCHMANN, J.: Einführung in die Kryptographie. 3. Aufl., 2003, S. 68 ff.

[117] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY: Federal Information Processing Standards Publication 197 - Advanced Encryption Standard, 2001.

[118] Vgl. RIVEST, R.: A Description of the RC2(r) Encryption Algorithm (RFC2268), 1998; SCHNEIER, B.: Angewandte Kryptographie, 1996, S. 368 f., 455 f., 397 ff.

[119] Vgl. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY: Federal Information Processing Standards Publication 46-3 - Data Encryption Standard, 1999.

[120] Vgl. SCHNEIER, B.: Angewandte Kryptographie, 1996, S. 370 ff.

[121] Vgl. BUCHMANN, J.: Einführung in die Kryptographie. 3. Aufl., 2003, S. 137 ff., 153 ff.

[122] Vgl. BUNDESNETZAGENTUR: Geeignete Algorithmen, 2006.

[123] Vgl. BUCHMANN, J.: Einführung in die Kryptographie. 3. Aufl., 2003, S. 137 ff., 210 ff.

SCHNEIER.[124] Häufig werden auch hybride Verfahren eingesetzt, um den Geschwindigkeitsvorteil einfacher symmetrischer Verfahren mit der hohen Sicherheit und öffentlichem Schlüsselaustausch über unsichere Netze von asymmetrischen Verfahren zu verknüpfen.

Abbildung 2-5 zeigt ein Beispiel für ein solches hybrides Verschlüsselungsverfahren. Dabei wird der Adressat Bob durch dessen öffentlichen Schlüssel authentifiziert. Alice erzeugt einen zufälligen symmetrischen Sitzungsschlüssel für die spätere Datenübertragung und sendet ihn verschlüsselt mit dem öffentlichen Schlüssel von Bob. Nur Bob ist in der Lage, den Sitzungsschlüssel mit seinem zugehörigen privaten Schlüssel zu entschlüsseln und für die nachfolgende Sitzung zu verwenden. Hybride Verfahren bilden die Basis für Authentifizierungsverfahren wie Secure Sockets Layer (SSL) oder Transport Layer Security (TLS).[125]

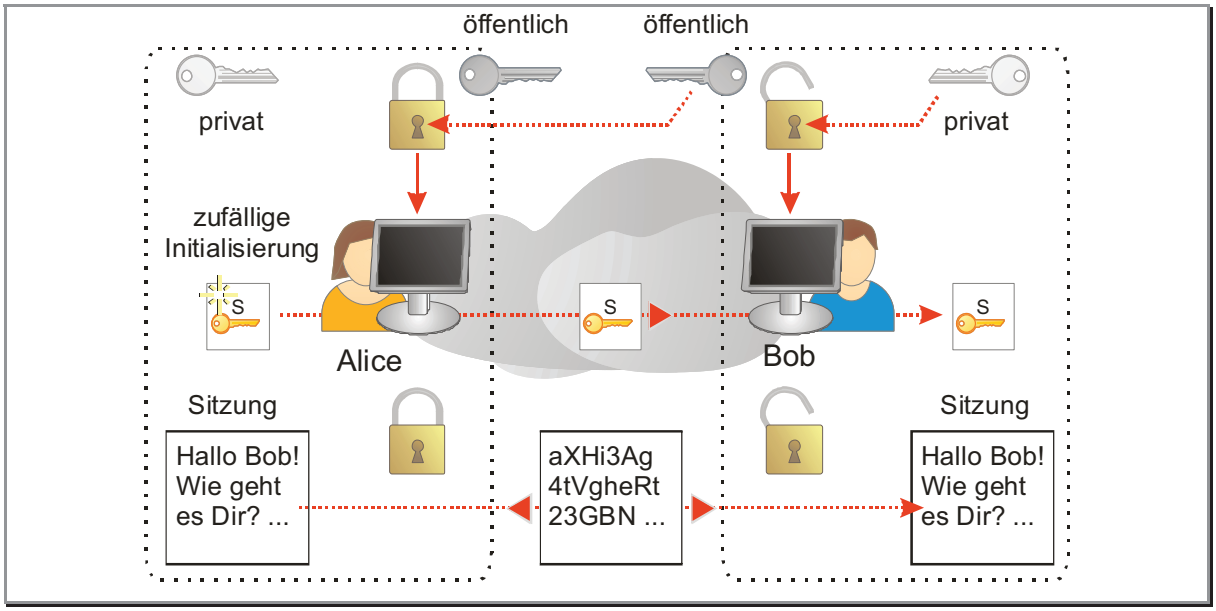

Abbildung 2-5: Hybride Verschlüsselungsverfahren nach BADACH ET AL.[126]

In den vergangenen Jahren sind zunehmend Angriffe auf symmetrische[127] und asymmetrische Verschlüsselungsverfahren[128] bekannt geworden. Für die Erhöhung der Sicherheit der asymmetrischen

[124] Vgl. BIETHAHN, J.; CVJETKOVIC, D.; ORTHEY, F.; MUCKSCH, H.; NISSEN, V.: Datenschutz, Datensicherheit und gesellschaftliche Auswirkungen der Informationsverarbeitung. 3. Aufl., 2000, BUCHMANN, J.: Einführung in die Kryptographie. 3. Aufl., 2003; SCHNEIER, B.: Angewandte Kryptographie, 1996.

[125] Vgl. NETSCAPE: SSL 3.0 Specification, 1996; DIERKS, T.: The Transport Layer Security (TLS) Protocol. Version 1.1 (RFC 4346), 2006.

[126] Vgl. BADACH, A.; RIEGER, S.; SCHMAUCH, M.: Web-Technologien, 2003, S. 363.

[127] Vgl. PELZL, J.; GÖRTZ H.: Cryptoanalysis with a cost-optimized FPGA cluster, 2006.

[128] Vgl. RSA: The RSA Challenge Numbers, 2007.

Verschlüsselung sind auf elliptic curve (EC) basierende Verfahren in der Entwicklung, die eine hohe Sicherheit bei geringerer Schlüssellänge im Vergleich zu RSA erlauben.[129]

2.6.2 Digitale Signaturen und Hash-Verfahren

Damit Alice dem öffentlichen Schlüssel von Bob bzw. dessen Identität vertrauen kann, werden digital signierte öffentliche Schlüssel verwendet. Alice erhält somit einen von einem Aussteller ihres Vertrauens digital unterschriebenen Schlüssel von Bob. Für die digitale Unterschrift (Signatur) verwendet der Aussteller dabei seinen privaten Schlüssel, so dass Alice mit dem zugehörigen öffentlichen Schlüssel eindeutig überprüfen kann, ob die Signatur von der ihr vertrauten Instanz stammt. Der signierte Schlüssel dient als digitaler Ausweis von Bob. In Bezug auf den signierten öffentlichen Schlüssel spricht man von einem Zertifikat, das in aller Regel dem X.509-Standard entspricht.[130] Der Aussteller wird als Zertifizierungsstelle (Trust Center) bezeichnet.

Die Identität vertrauenswürdiger Zertifizierungsstellen (bzw. deren öffentliche Schlüssel in Form von Root-Zertifikaten) wird beispielsweise direkt mit dem Betriebssystem, das Alice verwendet, ausgeliefert.

So werden ein sicherer Schlüsselaustausch und eine Authentifizierung zwischen Alice und Bob möglich, ohne dass diese sich vor der Übertragung persönlich kennen und gegenseitig identifizieren müssen. Die Authentizität wird durch einen vertrauenswürdigen Dritten, der Zertifizierungsstelle gewährleistet.

Die Abbildung 2-6 zeigt die digitale Signatur als Authentifizierung des Absenders durch die Verschlüsselung der Daten mit dessen privatem Schlüssel.

---

[129] Vgl. BUCHMANN, J.: Einführung in die Kryptographie. 3. Aufl., 2003, S. 221.

[130] Vgl. HOUSLEY, R. ET AL.: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 3280), 2002.

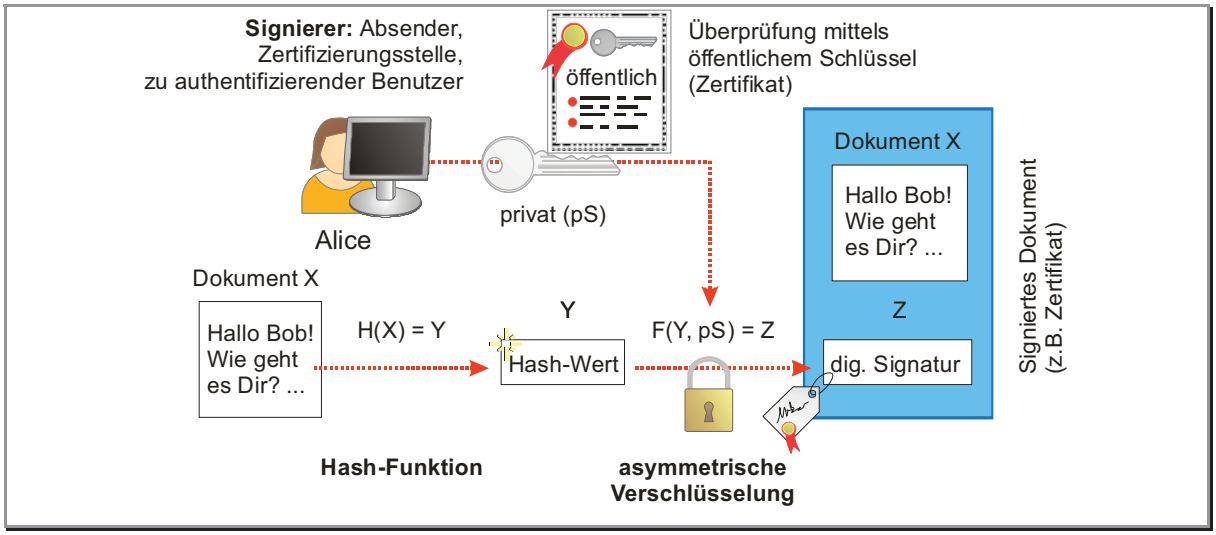

Abbildung 2-6: Digitale Signatur nach BADACH ET AL.[131]

Um nicht die gesamten Daten asymmetrisch verschlüsseln zu müssen, wird zunächst ein eindeutiges Komprimat des Dokuments gebildet. Dieses Komprimat wird durch eine kryptographische Hash-Funktion erzielt, die gewährleistet, dass bereits kleinste Änderungen am Dokument X zu einem abweichenden Hash-Wert Y führen. Man bezeichnet H(X) dabei auch als kollisionsfrei.[132] Zusätzlich sind von Y keine Rückschlüsse auf X möglich. Y wird anschließend vom Signierer mit dessen privatem Schlüssel verschlüsselt und als digitale Signatur Z mit dem Dokument bzw. den Daten übermittelt. Empfänger können den von Alice erzeugten Hash-Wert Y anhand des öffentlichen Schlüssels von Alice (z.B. aus deren Zertifikat) entschlüsseln, selbst H(X) auf das Dokument anwenden und die Ergebnisse vergleichen. Sofern beide übereinstimmen, ist Alice als Absender eindeutig identifiziert resp. authentifiziert.

Hash-Verfahren werden aufgrund der irreversiblen Verschlüsselung bzw. der nicht möglichen Rückgewinnung der ursprünglichen Daten aus dem Komprimat auch für die Speicherung von Passwörtern verwendet. Typische Hash-Funktionen sind Message Digest 4 (MD4)[133], Message Digest 5 (MD5)[134] und der Secure Hash Algorithm 1 (SHA1).[135] In den vergangenen Jahren wur-

[131] Vgl. BADACH, A.; RIEGER, S.; SCHMAUCH, M.: Web-Technologien, 2003, S. 370.

[132] Vgl. BADACH, A.; RIEGER, S.; SCHMAUCH, M.: Web-Technologien, 2003, S. 365 und BUCHMANN, J.: Einführung in die Kryptographie. 3. Aufl., 2003, S. 192.

[133] Vgl. RIVEST, R.: The MD4 Message-Digest Algorithm (RFC 1320), 1992.

[134] Vgl. RIVEST, R.: The MD5 Message-Digest Algorithm (RFC 1321), 1992.

[135] Vgl. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY: Federal Information Processing Standards Publication 180-2 - Secure Hash Standard, 2002.

den zunehmend Angriffe auf die Kollisionsfreiheit von Hash-Funktionen durchgeführt.[136] Daraus wird deutlich, dass die Verschlüsselung allein keine sichere Authentifizierung gewährleisten kann; die Sicherheit des eventuell verwendeten Hash-Verfahrens ist ebenfalls relevant.

2.6.3 Challenge-Response Verfahren

Für die Übertragung der Passwörter bei deren Verwendung bieten Hash-Verfahren allein jedoch keine Sicherheit. Angreifer könnten den Hash-Wert des Passworts gleichermaßen abhören und analog zum Passwort in Klartext verwenden. Als Lösung werden häufig Challenge-Response Verfahren verwendet, sofern Passwörter über einen Übertragungskanal versendet werden, der selbst keine Vertraulichkeit gewährleistet.[137] Bei Challenge-Response Verfahren wird das Passwort um eine zufällige, einmalig verwendete Komponente erweitert, die vom Authentifizierungssystem ausgewählt und an den Benutzer übermittelt wird. Diese zufällig ausgewählte Nummer, die nur ein einziges Mal verwendet wird, bezeichnet man auch als Nonce („number used only once“).

Das Authentifizierungssystem übermittelt hierbei die Nonce als Herausforderung (Challenge) an den Benutzer. Dieser wendet auf die Kombination aus seinem Passwort und Nonce die Hash-Funktion H(X, nonce) an und sendet das Resultat Y als Antwort (Response) an das Authentifizierungssystem. Anschließend überprüft der Server, ob der übermittelte Hash-Wert aus Passwort und gestellter Herausforderung gebildet wurde, indem er ebenfalls H(X, nonce) anwendet und den ermittelten Wert Y mit dem vom Benutzer erhaltenen vergleicht. Während der gesamten Kommunikation wird das eigentliche Authentifizierungsmerkmal (das Passwort) nicht selbst übertragen, so dass ein Abhören nicht möglich ist. Basierend auf dem Prinzip, die eigentliche Authentifizierungsinformation bzw. das Geheimnis nicht für die Authentifizierung zu übertragen, wurden in den vergangenen Jahren darüber hinaus weitere Zero-Knowledge-Verfahren wie das Fiat-Shamir-Verfahren entwickelt.[138]

---

[136] Vgl. WANG, X.; YAO, A. C.; YAO, F.: Cryptoanalysis on SHA-1, 2005.

[137] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 285 ff. und ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 457 ff.

[138] Vgl. ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 462 ff. und BUCHMANN, J.: Einführung in die Kryptographie. 3. Aufl., 2003, S. 230.

2.7 Authentifizierungsverfahren und -systeme

Die folgenden Abschnitte beschreiben Authentifizierungsverfahren und -systeme. SMITH definiert lokale, direkte, indirekte und Off-line-Authentifizierungsverfahren.[139] Lokale Authentifizierung findet beispielsweise unmittelbar am Arbeitsplatzrechner statt und erfolgt nicht über ein Netzwerk. Die Authentifizierung an einem System über ein Netzwerk definiert SMITH als direkte Authentifizierung. Führt das System, das die vom Benutzer gewünschte Ressource anbietet, die Authentifizierung nicht selbst durch, sondern nutzt ein separates Authentifizierungssystem, so bezeichnet SMITH das Verfahren als indirekt. Sofern eine Ressource die Authentizität eines Benutzers überprüfen kann, ohne eine Verbindung zu einem Authentifizierungssystem über das Netzwerk aufzubauen, so bezeichnet SMITH das Verfahren als Off-line-Authentifizierung.

2.7.1 Lokale Authentifizierung

Die einfachste Form der Authentifizierung ist nach SMITH die lokale Anmeldung (resp. lokale Authentifizierung). Sie kann beispielsweise an einem Arbeitsplatzrechner oder einem Personal Digital Assistant (PDA) erfolgen.[140] Das Authentifizierungssystem bzw. -verfahren ist dabei lokal auf dem Gerät installiert. Benutzer verwenden ihr Authentifizierungsmerkmal, um sich anzumelden. Die Verwaltung des zugehörigen Authentifizierungskontos resp. -verfahrens erfolgt individuell für jeden Rechner. Authentifizierung und Autorisierung bzw. Zugriffskontrolle sind auf den lokalen Rechner begrenzt, somit bildet dieser allein den realisierten physikalischen Sicherheits-Perimeter. Die Komponenten einer lokalen Authentifizierung nach SMITH sind in Abbildung 2-7 dargestellt.

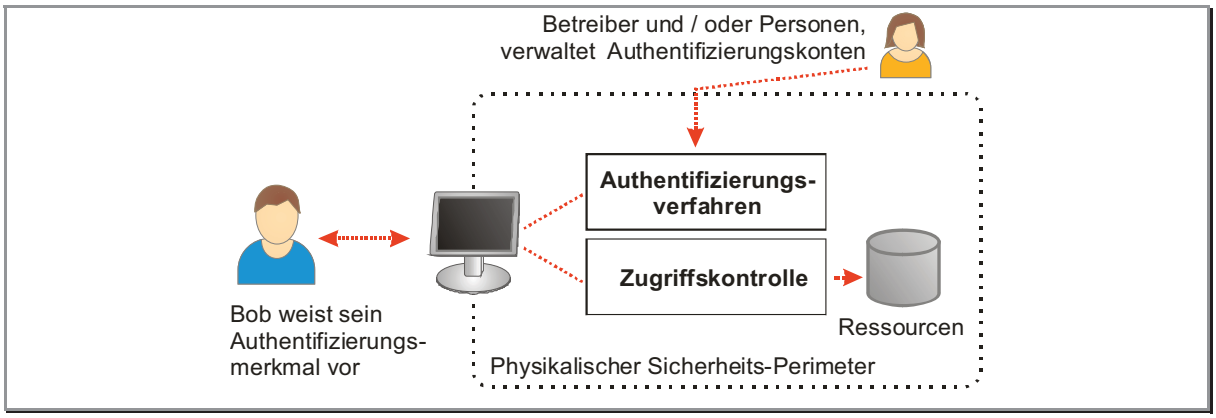

Abbildung 2-7: Lokale Authentifizierung nach SMITH[141]

[139] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 104.

[140] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 133 ff.

[141] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 118.

Ein Beispiel für lokale Authentifizierung stellt die Anmeldung an einem Windows-Rechner, der nicht an einem Netzwerk angeschlossen ist, über die „graphical identification and authentication“ (GINA) dar.[142] Ein weiteres Beispiel bildet die Applikation login oder die lokale Verwendung der „pluggable authentication modules“ (PAM) unter Unix.[143] PAM regelt dabei auch die Sitzungsverwaltung und Zugriffskontrolle, z.B. auf Dateien, die auf dem Rechner lokal gespeichert sind. Auch die Verwendung von lokalen Anwendungen, etwa für die Verschlüsselung von Daten, die eine Authentifizierung erfordern, fällt in die beschriebene Kategorie.

2.7.2 Direkte Authentifizierung

Erfolgt die Authentifizierung nicht lokal am Arbeitsplatz, sondern wird stattdessen beispielsweise eine Client-Anwendung verwendet, die die Authentifizierung an einem entfernen System (Server) durchführt, so bezeichnet SMITH dieses Verfahren als direkte Authentifizierung.[144] Abbildung 2-8 skizziert den Aufbau einer direkten Authentifizierung:

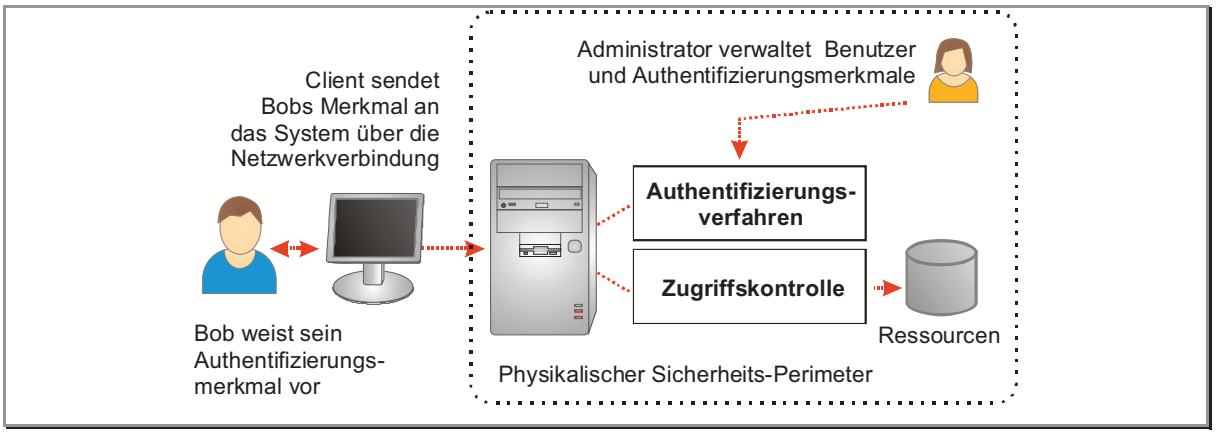

Abbildung 2-8: Direkte Authentifizierung nach SMITH[145]

Authentifizierungsverfahren und -konten werden wie bereits bei der lokalen Authentifizierung, die im vorherigen Abschnitt beschrieben wurde, innerhalb des Servers, der den Zugriff auf die Ressourcen kontrolliert, verwaltet. Somit bildet der Server ein eigenständiges Authentifizierungssystem. Im Gegensatz zur lokalen Authentifizierung können unterschiedliche Clients den Server und das verwaltete Authentifizierungsverfahren verwenden. Beispiele für direkte Authentifizierung

---

[142] Vgl. SCHMIDT, J.: Windows 2000 Security. Kryptographie, Kerberos, Authentifizierung, 2001, S. 112.

[143] Vgl. SAMAR, V.; CHARLIE, L.: Making Login Services Independent of Authentication Technologies (PAM), 1996.

[144] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 313 ff.

[145] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 120.

bilden Anwendungen, die ein eigenes Authentifizierungsverfahren integrieren, wie die direkte Anmeldung an einem Unix-Rechner über Secure Shell (SSH)[146] oder einem E-Mail Server, der eigene Authentifizierungskonten speichert. Auch die Anmeldung an einem Lightweight Directory Access Protocol (LDAP)[147] Verzeichnisdienst zur Abfrage von dort gespeicherten Informationen stellt eine direkte Authentifizierung dar. Wird jedoch ein LDAP-Server von Servern, die ihrerseits Ressourcen anbieten, verwendet, so handelt es sich um eine indirekte Authentifizierung, die im nächsten Abschnitt erläutert wird.

2.7.3 Indirekte Authentifizierung

Wird die Authentifizierung außerhalb des Systems, das die Ressource anbietet oder den Zugriff darauf kontrolliert, durchgeführt, so beschreibt SMITH die Authentifizierung als indirekt.[148] Durch die Realisierung der Authentifizierung in einem separaten System können unterschiedliche Dienste und Ressourcen dieses Authentifizierungssystem gemeinsam verwenden. Auf diese Weise muss jeweils nur ein Konto pro Benutzer bzw. nur ein Authentifizierungsverfahren und -system für die angebotenen Dienste verwaltet werden. Für die Kommunikation zwischen dem System, das den Dienst oder die Ressource anbietet, und dem Authentifizierungssystem kommt in der Regel ein Authentifizierungsprotokoll zum Einsatz, das ein Authentifizierungsverfahren implementiert.[149] Hierbei können Challenge-Response Verfahren, wie sie in Abschnitt 2.6.3 beschrieben wurden, zum Einsatz kommen. Aufbau und Ablauf der indirekten Authentifizierung werden in Abbildung 2-9 verdeutlicht. Bob bzw. sein Client sendet dabei eine Anfrage bzw. Anmeldung an das System, das den gewünschten Dienst zur Verfügung stellt. Bob übermittelt dabei z.B. seinen Benutzername und sein für die Authentifizierung am System erforderliches Authentifizierungsmerkmal. Das System schickt daraufhin eine Authentifizierungsanfrage an das Authentifizierungssystem. In der Antwort wird die Identität von Bob durch das Authentifizierungssystem bestätigt oder abgelehnt. Daraufhin entscheidet das System anhand der Zugriffskontrolle bzw. Autorisierung über die Gewährung des Zugriffs von Bob auf die Ressourcen.

---

[146] Vgl. CHESWICK, W. R.; BELLOWIN, S. M., RUBIN, A. D.: Firewalls und Sicherheit im Internet. 2. Aufl., 2004, S. 92 f.

[147] Vgl. ZEILENGA, K.: Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map (RFC 4510), 2006.

[148] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 104.

[149] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 122 f.

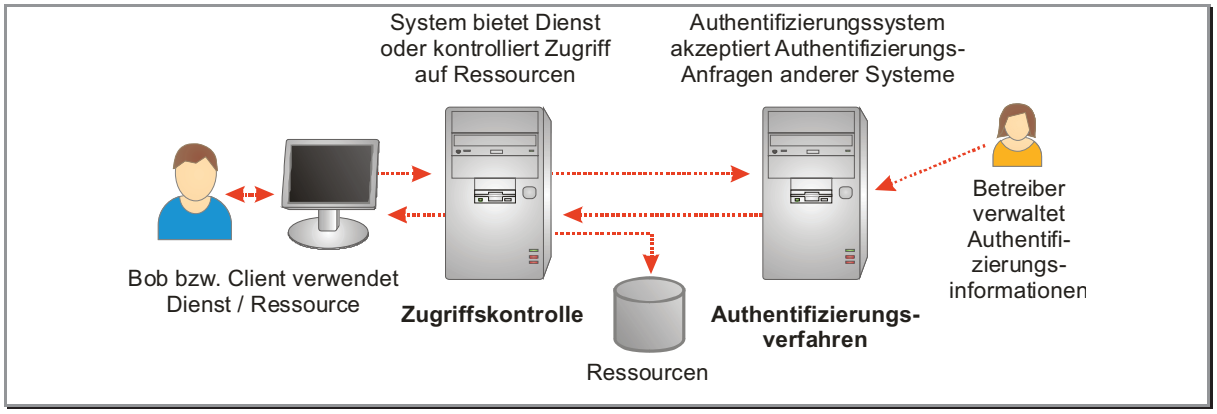

Abbildung 2-9: Indirekte Authentifizierung nach SMITH[150]

Ein Authentifizierungssystem kann unterschiedliche Authentifizierungsverfahren anbieten, die für die Authentifizierung der Benutzer verwendet werden können. Aufgrund der Vereinfachung der Verwaltung und Skalierbarkeit verwenden die meisten aktuellen Authentifizierungsverfahren eine indirekte Authentifizierung.[151] Begrenzt wird die Skalierbarkeit nur für Authentifizierungssysteme, die organisationsübergreifend verwendet werden sollen.[152] Durch Verwendung mehrerer Authentifizierungssysteme kann zudem die Redundanz bzw. Fehlertoleranz durch indirekte Authentifizierung gesteigert werden.[153]

Beispiele für Protokolle, die eine indirekte Authentifizierung realisieren, sind der Remote Authentication Dial In User Service (RADIUS) und Kerberos.[154]

Authentifizierungsprotokolle können unterschiedliche Verfahren verwenden, was beim Extensible Authentication Protocol (EAP)[155] der Fall ist, das unterschiedliche Authentifizierungsverfahren für die Anmeldung an Netzwerk-Ressourcen erlaubt. Es wird beispielsweise vom IEEE Protokoll 802.1X[156] für die Port-basierte Netzwerk-Authentifizierung verwendet. Unter Unix bietet der

[150] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 123.
[151] Vgl SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 124.
[152] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 125.
[153] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 125.
[154] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 313 ff.
[155] Vgl. ABOBA ET AL.: Extensible Authentication Protocol (EAP) (RFC 3748), 2004.
[156] Vgl. IEEE: 802.1X Port-Based Network Access Control, 2004.

Simple Authentication and Security Layer (SASL) unterschiedliche Authentifizierungsverfahren für verschiedene Anwendungen und Dienste.[157]

2.7.4 Off-line-Authentifizierung

Insbesondere für dezentrale, verteilte Anwendungen ist es schwer möglich, ein zentrales Authentifizierungssystem, wie in den vorherigen Abschnitten beschrieben, zu realisieren. Dies begründet sich neben der Komplexität der Anbindung auch mit der Problematik, dass Betreiber in dezentralen Strukturen nicht die Vertrauenswürdigkeit der verteilten Systeme gewährleisten können.[158] Durch die Verwendung auf asymmetrischer Verschlüsselung basierender X.509-Zertifikate[159] lässt sich eine dezentrale Authentifizierung erzielen, die ohne eine Verbindung zum eigentlichen Authentifizierungssystem durchgeführt werden kann. SMITH klassifiziert entsprechende Verfahren als Off-line-Authentifizierung.[160] Beispielsweise wird beim Internet-Banking das Kreditinstitut als Betreiber zunächst durch den Benutzer authentifiziert. Dies geschieht, indem während des Aufbaus der Verbindung (z.B. im Web mittels HTTPS[161]) das Zertifikat des Systems des Kreditinstituts auf dessen Echtheit überprüft bzw. für die Authentifizierung verwendet wird. Erst nach erfolgreicher Prüfung wird die Sitzung verschlüsselt und innerhalb dieser Sitzung die Authentifizierung des Benutzers durchgeführt, beispielsweise mittels Eingabe der Kontonummer und zugehöriger PIN.[162] Abbildung 2-10 zeigt den schematischen Aufbau der Off-line-Authentifizierung: Bob überprüft hierbei die Identität des Systems durch eine Prüfung der Signatur der Nachrichten bzw. des zugehörigen Zertifikats. Er vertraut hierbei der Signatur des Betreibers der Zertifizierungsstelle, die das Zertifikat für das System ausgestellt hat. Dieses Zertifikat, das als Wurzel für die Kette der signierten Zertifikate für die Systeme dient (daher auch als Root-Zertifikat bezeichnet), ist beispielsweise im Betriebssystem oder Web-Browser von Bob vorinstalliert. Das Vertrauen in die Zertifikatkette, Verteilung sowie Verwaltung der Zertifikate als signierte öffentliche Schlüssel ist Aufgabe einer Public-Key-Infrastruktur. Während die Authentifizierung ohne eine Verbindung zur Zertifizie-

---

[157] Vgl. MELNIKOV, A.; ZEILENGA, K.: Simple Authentication and Security Layer (SASL) (RFC 4422), 2006 und CHESWICK, W. R.; BELLOWIN, S. M., RUBIN, A. D.: Firewalls und Sicherheit im Internet. 2. Aufl., 2004, S. 191.

[158] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 125 f.

[159] Vgl. HOUSLEY, R. ET AL.: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 3280), 2002.

[160] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 125 ff.

[161] Vgl. RESCORLA, E.: HTTP over TLS (RFC 2818), 2000.

[162] Der genaue Ablauf der Prüfung des Zertifikats bei der Verwendung von HTTPS ist in BADACH, A.; RIEGER, S.; SCHMAUCH, M.: Web-Technologien, 2003, S. 388 ff. detailliert beschrieben.

rungsstelle als Authentifizierungssystem durch Prüfung der digitalen Signatur (off-line) erfolgt, ist die Autorisierung als Zugriffskontrolle hierbei nach wie vor Aufgabe des Systems. Analog kann die Authentifizierung von Bob anhand seines Zertifikats durch das System ebenfalls off-line erfolgen.

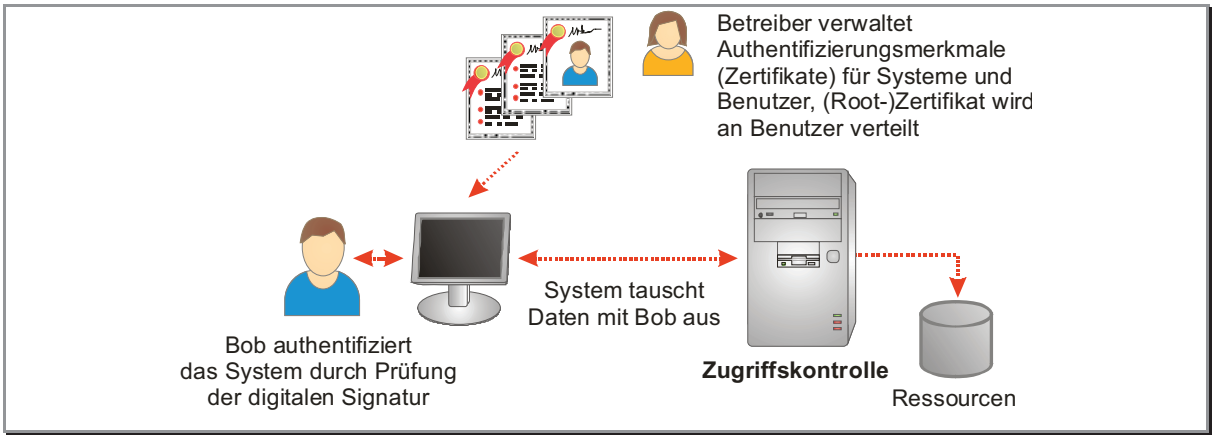

Abbildung 2-10: Off-line-Authentifizierung nach SMITH[163]

Aktuelle Zertifikat-basierte Authentifizierungsverfahren brechen das skizzierte Paradigma der Off-line-Authentifizierung, da hierbei die Validität des verwendeten Zertifikats on-line überprüft wird. Das trifft für das Online Certificate Status Protocol (OCSP)[164] zu, das anstelle einer zwischengespeicherten Sperrliste für die Prüfung der Gültigkeit von Zertifikaten eine direkte Verbindung zur Zertifizierungsstelle aufbaut und den aktuellen Status des Zertifikats verifiziert, bevor die Authentifizierung als erfolgreich bewertet wird.

Typische Authentifizierungsverfahren, die eine Off-line-Authentifizierung realisieren, sind Secure Sockets Layer (SSL) sowie der Internet-Standard Transport Layer Security (TLS).[165] Diese liefern die Grundlage für spezifische Sicherheits-Erweiterungen verschiedener Anwendungsprotokolle, die dadurch Vertraulichkeit, Integrität, Verbindlichkeit und Authentizität erzielen. Beispiele stellen die sichere Version des Hypertext-Transfer-Protokolls HTTPS oder LDAPS für das Lightweight Directory Access Protocol dar. SSL und TLS arbeiten dabei mit dem in Abschnitt 2.6.1 beschriebenen

[163] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 128.

[164] Vgl. MYERS ET AL.: X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol - OCSP (RFC 2560), 1999.

[165] Vgl. die Beschreibung von SSL und TLS im Rahmen der hybriden Verschlüsselungsverfahren in Abschnitt 2.6.1.

hybriden Verschlüsselungsverfahren. Sie bilden eine Sitzung, innerhalb derer die IT-Sicherheit bei der Verwendung der Anwendung garantiert wird.[166]

2.8 Risiken der Authentifizierung

Die Authentifizierung bildet die Grundlage für den sicheren Zugriff auf Ressourcen. Sie steht am Anfang einer Sitzung und ermöglicht durch die eindeutige Identifizierung des Benutzers oder des Systems die Basis für die anschließende Autorisierung oder Abrechnung (Accounting). Für eine fehlerfreie Authentifizierung müssen die Vertraulichkeit, Integrität und Verbindlichkeit als IT-Sicherheitskriterien und Grundwerte gemäß Abschnitt 2.2 gewährleistet werden. Andernfalls ist die Manipulation der Authentifizierung durch Dritte möglich. Risiken, die durch Fehler bei einer Authentifizierung, z.B. durch deren Manipulation, entstehen können, nennen die folgenden Abschnitte. Die Abwägung der im Folgenden aufgezählten Risiken und die Auswahl entsprechend gesicherter Authentifizierungsmerkmale, -verfahren und -systeme bildet die Basis für die durch die Authentifizierung innerhalb einer heterogenen IT-Struktur erzielten Sicherheit.

2.8.1 Sicherheit von Authentifizierungsmerkmalen

Der einfachste Weg für den Einbuch in ein System erfolgt nach CHESWICK ET AL. direkt über eine erfolgreiche Authentifizierung an der regulären Schnittstelle der Anwendung durch Erlangung des erforderlichen Passworts.[167] Sofern der Zugriff auf Authentifizierungsmerkmale somit nicht effizient vor unberechtigten Dritten geschützt ist, können diese eine erfolgreiche Authentifizierung vortäuschen, ohne dass dies vom Benutzer oder Betreiber bemerkt werden kann. Authentifizierungsmerkmale weisen je nach deren Ausprägung, wie in Abschnitt 2.5 beschrieben, unterschiedliche Angriffspotentiale auf. Für Authentifizierungsmerkmale, die auf Kenntnis eines Geheimnisses basieren, z.B. Passwörter, existieren folgende Angriffskategorien, die deren Sicherheit einschränken:

---

[166] Detailliert werden sie in ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 735 ff. und CHESWICK, W. R.; BELLOWIN, S. M., RUBIN, A. D.: Firewalls und Sicherheit im Internet. 2. Aufl., 2004, S. 386 ff. beschrieben.

[167] Vgl. CHESWICK, W. R.; BELLOWIN, S. M., RUBIN, A. D.: Firewalls und Sicherheit im Internet. 2. Aufl., 2004, S. 131.

- **Geringe Passwort-Komplexität**: Häufig basieren Passwörter auf einfachen Wörtern, bestehen ausschließlich aus Buchstaben oder sind zu kurz.[168] Dadurch können Passwörter durch unberechtigte Dritte erraten werden. Für gängige Passwörter wie Vornamen und darauf basierende Kombinationen existieren außerdem spezielle Wörterbücher, die über das Internet auf einfache Weise bezogen werden können.[169]

- **Passwort-Cracking**: Insbesondere aufgrund der geringen Passwort-Komplexität können leicht alle möglichen Kombinationen für ein Passwort vom Angreifer nacheinander ausprobiert werden (sog. „brute-force"-Verfahren).[170] Dies wird als Passwort-Cracking bezeichnet. Werden die Passwörter als Hash-Werte[171] gespeichert und erhält der Angreifer Zugriff auf die entsprechende Datei, so kann er z.B. für alle möglichen alphanumerischen Kombinationen zugehörige Hash-Werte und somit in endlicher Zeit das Passwort ermitteln, das zum jeweiligen Hash-Wert führt. Für diese Aufgabe existieren zusätzlich sog. Rainbow Tables[172], die vorberechnete Hash-Werte für alle möglichen Eingabe-Werte abbilden, und so keine Anwendung langwieriger Hash-Verfahren erfordern. Auch Verfahren für die Ermittlung privater Schlüssel oder die Reduktion der notwendigen Vorgänge für das Ausprobieren möglicher Schlüssel existieren bereits.[173] Diese sind zudem abhängig von der Güte der Zufallszahlen, die beispielsweise für das RSA-Verfahren benötigt werden.[174]

- **Standard-Passwörter**: Einfacher als das Ausprobieren aller möglichen Kombinationen ist das vorherige Testen von Standard-Passwörtern. Häufig besitzen Systeme entsprechende Passwörter in ihrem Auslieferungszustand oder Passwörter neuer Benutzer werden mit deren Geburtsdatum oder Vornamen etc. belegt. In diese Sicherheitslücke fallen auch Passwörter, die ein Benutzer wieder verwendet, z.B. für alle Dienste, die ein Passwort erfordern und damit sein Standard-Passwort bilden.[175]

---

[168] Vgl. RILEY, S.: Password Security: What Users Know and What They Actually Do, 2006 und ADAMS, A.; SASSE, A.: Users Are Not the Enemy. Why Users Compromise Security Mechanisms and How to Take Remedial Measures, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 640 ff.

[169] Vgl. z.B. Word lists, 2007.

[170] Vgl. CHESWICK, W. R.; BELLOWIN, S. M., RUBIN, A. D.: Firewalls und Sicherheit im Internet. 2. Aufl., 2004, S. 402 und SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 51 ff.

[171] Hash-Werte werden durch die in Abschnitt 2.6.2 erläuterten Hash-Verfahren gebildet.

[172] Vgl. OECHSLIN, P.: Making a Faster Cryptoanalytical Time-Memory Trade-Off, 2003.

[173] Vgl. WEISSTEIN, E. W.: RSA-640 Factored, 2005.

[174] Vgl. BUCHMANN, J.: Einführung in die Kryptographie. 3. Aufl., 2003, S. 137 ff., 206 ff.

[175] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 81 f.

- **Passwort-Recherche**: Häufig schreiben Benutzer ihre Passwörter auf Zettel, die sie in unmittelbarer Nähe ihres Arbeitsplatzes leicht zugänglich aufbewahren.[176] Findet ein Angreifer einen solchen Zettel, erhält er unmittelbar Zugriff auf die Authentifizierungsmerkmale. Zettel, auf denen Passwörter notiert wurden, lassen sich auch in Papierkörben der Benutzer finden. Eine weitere Möglichkeit sind Log-Dateien. Teilweise geben Benutzer irrtümlicherweise bei der Anmeldung ihr Passwort anstelle des Benutzernamens ein, das Passwort kann in diesem Fall durch den protokollierten Anmelde-Versuch ermittelt werden.[177]
- **Abhören von Passwörtern**: Passwörter werden während ihrer Verwendung, z.B. bei der Eingabe, offengelegt. Ein Angreifer kann hierbei die Eingaben auf der Tastatur beobachten, was als „shoulder surfing" bezeichnet wird.[178] Ein Abhören (Sniffing) der übertragenen Passwörter ist ebenfalls möglich, sofern das Authentifizierungsverfahren die Information im Klartext versendet.

Authentifizierungsmerkmale, die auf dem Besitz z.B. von Tokens basieren, lassen folgende Angriffe zu:

- **Diebstahl**: Ein Token kann gestohlen werden.[179] Sofern es sich um ein passives Token handelt, kann dies nach dem Diebstahl sofort für die erfolgreiche Authentifizierung eingesetzt werden.
- **Physikalische Analyse**: Für Tokens existieren Angriffe, die es erlauben, das auf ihnen gespeicherte Merkmal, wie etwa den privaten Schlüssel, ohne vorherige Authentifizierung auszulesen. Entweder kann dies durch Beschädigung und anschließendes Auslesen erfolgen oder während der Verwendung des Tokens durch Sekundäranalyse, z.B. Schwankungen in dessen Leistungsaufnahme, bei der Verwendung des privaten Schlüssels.[180]
- **Manipulation der Verwendung**: Wird die zum Token zugehörige PIN über eine Tastatur, z.B. am Rechner, eingegeben, so kann die PIN von einem Programm auf dem Rechner mitgeschnitten werden.[181] Gleiches gilt für das Abfangen eines vom Token erzeugten One Time Passwords, das durch den Angreifer verwendet werden kann, während die eigentliche Sitzung des Benutzers terminiert wird. Auch kann das Token, während es eingesteckt und aktiviert ist,

---

[176] Vgl. CHESWICK, W. R.; BELLOWIN, S. M., RUBIN, A. D.: Firewalls und Sicherheit im Internet. 2. Aufl., 2004, S. 182.

[177] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 18, 77.

[178] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 23 ff.

[179] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 273 ff.

[180] Vgl. ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 469 ff.

[181] Vgl. ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 469 ff.

durch den Angreifer für andere Zwecke missbraucht werden. Ein weiteres Problem bildet die Tatsache, dass der Benutzer nicht sieht, welche Daten er z.B. mit dem privaten Schlüssel auf dem Token signiert. Es kann also durch geeignete Manipulation eine andere Nachricht vom Token signiert werden, als dem Benutzer angezeigt wird.[182]

Biometrische Authentifizierungsmerkmale, die auf physischen Eigenschaften des Benutzers basieren, besitzen folgende Schwachstellen:

- **Unzureichende Genauigkeit**: Aktuelle Verfahren weisen eine hohe Fehlerrate auf. Dabei ist sowohl die Anzahl der fehlerhaft erfolgreich authentifizierten Angreifer (false acceptance rate, kurz: FAR) als auch die Anzahl der fälschlicherweise abgewiesenen legitimen Benutzer (false rejection rate, kurz: FRR) hoch.[183]
- **Fehlende Möglichkeit des Schlüsselwechsels**: Persönliche Eigenschaften wie Fingerabdruck oder Iris sind einmalig. Im Falle einer Kompromittierung können sie nur begrenzt ausgetauscht werden.[184] Beispielsweise sind pro Benutzer nur zwei Authentifizierungsmerkmale über die Iris seiner beiden Augen realisierbar.
- **Datenschutz**: Für eine Authentifizierung, die auf Fingerabdrücken basiert, muss ein Benutzer einen seiner Fingerabdrücke offen legen. Da diese Information über ihn eindeutig ist und ggf. auch für andere Zwecke verwendet wird (seine ungewollte Identifizierung anhand hinterlassener Fingerabdrücke oder für die Strafverfolgung), ist die Offenlegung auch aus Sicht des Datenschutzes relevant, insbesondere wenn der Benutzer nicht über die Verwendung der Daten bestimmen kann.[185]
- **Abhören des Merkmals**: Wird ein persönliches Merkmal wie die Fixpunkte eines Gesichtsfelds während der Anwendung abgehört, so kann es durch erneute Übertragung von einem Angreifer missbraucht werden.[186] In diesem Fall ist das Authentifizierungsmerkmal endgültig kompromittiert, da der Benutzer nur über ein Gesicht verfügt, sofern nicht neue Fixpunkte für die Authentifizierung verwendet werden können.

---

[182] Vgl. ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 469 ff.

[183] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 211 ff.

[184] Vgl. RENAUD, K.: Evaluating Authentication Mechanisms, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 120.

[185] Vgl. RENAUD, K.: Evaluating Authentication Mechanisms, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 122.

[186] Vgl. RENAUD, K.: Evaluating Authentication Mechanisms, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 120 f.

Neben der geeigneten Auswahl der Authentifizierungsmerkmale, basierend auf den genannten Risiken und der gewünschten Sicherheit, lassen sich die skizzierten Schwächen durch die Verwendung mehrerer Authentifizierungsfaktoren adressieren. Beispielsweise kann dies durch die Kombination von Kenntnis und Besitz als Anforderung an die erfolgreiche Authentifizierung in Form eines Tokens mit zugehöriger PIN für dessen Verwendung erfolgen. Stiehlt der Angreifer das Token, so benötigt er zusätzlich die PIN für dessen Aktivierung. Während der Angreifer versucht, diese zu erhalten, kann der Benutzer bereits das Token als Merkmal beim Betreiber sperren lassen.

2.8.2 Angriffe auf Authentifizierungsverfahren

Neben den im vorherigen Abschnitt genannten Angriffen auf Authentifizierungsmerkmale können auch Authentifizierungsverfahren manipuliert werden. Hierbei versucht der Angreifer, durch geeignete Manipulation des Authentifizierungsverfahrens die Authentifizierungssitzung berechtigter Benutzer zu übernehmen, abzuhören oder vorzutäuschen. Folgende Kategorien von Angriffen werden hierbei unterschieden:

- **Ausnutzung von Implementierungsfehlern**: Insbesondere komplexe Authentifizierungsverfahren enthalten Lücken oder Fehler, die für deren Missbrauch verwendet werden können.[187] Beispielsweise ermöglichen ältere Authentifizierungsverfahren wie LANMAN unter Windows NT einen sog. „downgrade attack".[188] Hierbei gibt sich der Angreifer als vermeintlicher Server aus und handelt den Client auf die Übertragung des Passworts in Klartext herunter (downgrade). Eine weitere Möglichkeit sind „back doors" die unberechtigten Dritten z.B. den direkten Zugriff ohne jegliche Authentifizierung erlauben.[189]
- **Abhören der Sitzung**: Informationen, z.B. Merkmale, können während der Übertragung abgehört werden, sofern das Authentifizierungsverfahren keine Vertraulichkeit gewährleistet.[190] Im Anschluss kann der Angreifer versuchen, gewonnene Informationen für eine weitere Authentifizierungssitzung zu verwenden. Einen besonderen Aspekt bildet hierbei die sog. „known plaintext" Attacke, bei der der Angreifer Teile der übermittelten Daten in unverschlüsselter

[187] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 33 f.

[188] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 303.

[189] Vgl. CHESWICK, W. R.; BELLOWIN, S. M., RUBIN, A. D.: Firewalls und Sicherheit im Internet. 2. Aufl., 2004, S. 137 ff.

[190] Vgl. Abhören der Daten, wie in Abschnitt 2.2.1 beschrieben.

Form kennt und so Rückschlüsse auf den verwendeten Schlüssel für das Chiffrat vornehmen kann.[191]

- **Übernahme der Sitzung**: Hört der Angreifer die Sitzung ab, so kann er sie zusätzlich manipulieren, sofern diese nicht die Integrität und Verbindlichkeit gewährleistet.[192] Hierbei kann der Angreifer die Sitzung des Benutzers bei sich terminieren und selbst eine neue Sitzung zum eigentlich Server aufbauen. Anschließend verbindet er die Sitzungen und leitet somit alle Daten zwischen Benutzer und Server selbst weiter. Man spricht hierbei in Bezug auf den Angreifer vom „Man-in-the-Middle".[193] Beispielsweise kann er so die ausgehandelten Sitzungsschlüssel, wie in Abbildung 2-5 für die hybride Verschlüsselung gezeigt, bestimmen und die Daten zwischen Authentifizierungssystem und Benutzer auslesen bzw. die Sitzung übernehmen. Dies ist möglich, sofern keine wechselseitige Authentifizierung (mutual-authentication) erfolgt oder das Authentifizierungssystem nicht vor der Authentifizierung des Benutzers durch diesen selbst eindeutig, z.B. über dessen Zertifikat, identifiziert wird.[194] Auch ein solches Zertifikat kann vorgetäuscht werden, sofern der Benutzer dessen digitale Signatur bzw. die zugehörige evtl. nicht vertrauenswürdige Zertifizierungsstelle unachtsam akzeptiert.[195] In der Vergangenheit sind jedoch auch Fälle bekannt geworden, in denen selbst vertrauenswürdige Zertifizierungsstellen auf falschen Informationen basierende Zertifikate ausgestellt haben, indem sie vom Angreifer bei der Beantragung getäuscht wurden.[196]
- **Manipulation der Sitzung**: Durch Manipulation der Sitzung kann der Angreifer z.B. als „Man-in-the-Middle" auch die für die Authentifizierung ausgetauschten Nachrichten modifizieren. So kann er versuchen, eine Nachricht über den Misserfolg einer Authentifizierung zwischen der Ressource und dem Authentifizierungssystem bei der indirekten Authentifizierung in eine Erfolgsmeldung zu ändern, um so selbst Zugriff auf die Ressource zu erhalten.[197] Der Angreifer kann auch eine alte Nachricht einer erfolgreichen Authentifizierung senden, sofern das

---

[191] Vgl. ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 341 f.

[192] Vgl. Manipulation der Daten in Abschnitt 2.2.2 und Abstreiten der Identität des Absenders in 2.2.4.

[193] Vgl. ANDERSON, R.: Security Engineering. A Guide to Building Dependable Distributed Systems, 2001, S. 19 f.

[194] Vgl. ANDERSON, R.: Security Engineering. A Guide to Building Dependable Distributed Systems, 2001, S. 20.

[195] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 403 ff.

[196] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 403 f.

[197] Vgl. „forged accept" in SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 319.

System die zeitliche Abfolge der Nachrichten nicht berücksichtigt[198]. Einige Protokolle lassen auch Rückschlüsse auf den verwendeten Schlüssel zu, indem der Angreifer die Authentifizierungsanforderung gegen einen ihm bekannten Text austauscht und das Chiffrat, das der Authentifizierungsserver als Antwort sendet, analysiert. Dies wird als „chosen plaintext"-Angriff bezeichnet.[199]

- **Missbrauch von Authentifizierungs-Protokollen**: Authentifizierungsverfahren können allgemein u.a. durch deren Penetration mit nicht vorgesehenen Abläufen und Daten (mittels „brute-force") gebrochen werden.[200] Eine Besonderheit bilden hierbei sog. „race conditions", bei denen ein Teil der Authentifizierung eines legitimen Benutzers abgehört wird. Für den restlichen Teil werden mehrere Verbindungen zum Server aufgebaut und parallel mit allen Möglichkeiten für weitere Eingaben des Benutzers (z.B. den Rest des Passworts) bedient. Sofern die Sitzungen nicht jeweils neue Merkmale erfordern (etwa mittels Challenge-Response) und nur wenige theoretische Kombinationen möglich sind, gewinnt der automatisierte Angriff das Rennen (race) gegenüber den später erfolgenden Eingaben des berechtigten Benutzers.
- **Veränderung des Kontexts**: Authentifizierungsverfahren müssen unabhängig vom Kontext, in dem Sie ausgeführt werden, fehlerfrei funktionieren. Einige Verfahren sind z.B. abhängig vom zeitlichen Kontext, so dass der Angreifer durch Manipulation der Uhrzeit am Client oder der Ressource alte Authentifizierungs-Sitzungen erneut nutzen kann.[201] Häufigste Veränderung des Kontexts zur Vortäuschung einer Identität ist jedoch die Maskierung resp. Manipulation der Absenderadresse (Spoofing) oder der Adressierungsverfahren. Nahezu alle Netzwerkadressen und -adressierungsverfahren lassen sich mit geeigneten Angriffen fälschen.[202]
- **Modifikation des Clients**: Auch durch eine Modifikation des Clients kann der Angreifer Authentifizierungsmerkmale erlangen oder -verfahren manipulieren. Hierfür kann z.B. über einen Virus oder durch Ausnutzung der Leichtgläubigkeit des Benutzers ein Trojaner auf dem Client installiert werden, der das Authentifizierungsverfahren überwacht oder modifiziert.[203]

---

198 Vgl. „replay attack" in SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 327.

199 Vgl. ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 342.

200 Vgl. CHESWICK, W. R.; BELLOWIN, S. M., RUBIN, A. D.: Firewalls und Sicherheit im Internet. 2. Aufl., 2004, S. 402.

201 Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 362 f.

202 Vgl. CHESWICK, W. R.; BELLOWIN, S. M., RUBIN, A. D.: Firewalls und Sicherheit im Internet. 2. Aufl., 2004, S. 45 ff. und PEIKARI, C.; CHUWAKIN, A.: Kenne Deinen Feind, 2004, S. 189 ff.

203 Vgl. ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 50 62 f.

Adressiert werden die genannten Schwachstellen durch die Kopplung mehrer Verfahren. So werden häufig vor der eigentlichen Authentifizierung SSL-Verbindungen[204] aufgebaut, die als Tunnel die eigentliche Übertragung einhüllen und schützen. Dies kann auch durch Verfahren wie IPsec[205] auf dem Layer 3 realisiert werden. Allgemein wird durch diese Sitzungen die Vertraulichkeit, Integrität und Verbindlichkeit, wie in Abschnitt 2.2 definiert, gewährleistet. Die Einhaltung dieser Kriterien bildet die Grundlage für sichere Authentifizierungsverfahren.

2.8.3 Angriffe auf Authentifizierungssysteme

Weitere Risiken entstehen für die Authentifizierung, sofern die Authentifizierungssysteme, die Authentifizierungsverfahren anwenden und Konten speichern, angegriffen werden. Grundsätzlich zielen diese Angriffe auf die anschließende Modifikation der Authentifizierungssysteme bzw. deren Missbrauch im Sinne der Angreifer. Dies gilt insbesondere für lokale Authentifizierung, wie sie in Abschnitt 2.7.1 beschrieben wurde. Hier versucht ein Angreifer die Authentifizierung am lokalen System zu umgehen, um z.B. mit Administrator-Rechten direkten Zugriff auf Ressourcen bzw. Informationen zu erhalten. Angriffe, die auf die Manipulation der Authentifizierungssysteme zielen, lassen sich wie folgt differenzieren:

- **Software-Manipulation**: Durch Hintertüren ("back doors") und Lücken kann ein Angreifer Zugriff auf das Betriebssystem des Authentifizierungssystems erlangen. Erhält er dort Administrator-Rechte, so kann er die installierten Anwendungen, insbesondere die Authentifizierungsverfahren, manipulieren und neue Konten und Authentifizierungsmerkmale installieren.[206] Neben gezielten Angriffen auf Schwachstellen der Software kann der Angreifer unter Umständen auch Standard-Passwörter verwenden, die z.B. bei der Auslieferung der Software vom Hersteller gesetzt und nach der Installation durch den Betreiber nicht geändert wurden.[207] Anschließend kann er das übernommene System als Ausgangspunkt für weitere Angriffe nutzen. Oft kann er dadurch dessen Quell-Adresse im Netzwerk verwenden, um dadurch Schutzmechanismen wie Firewalls[208] für Folgeangriffe zu umgehen. Häufig werden derartige Angrif-

---

[204] Vgl. SSL Verbindungen wurden am Ende des Abschnitts 2.6.1 im Rahmen der hybriden Verschlüsselungsverfahren erläutert.

[205] Vgl. KENT, S.; SEO, K.: Security Architecture for the Internet Protocol, 2005 und ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 708 ff.

[206] Vgl. CHESWICK, W. R.; BELLOWIN, S. M., RUBIN, A. D.: Firewalls und Sicherheit im Internet. 2. Aufl., 2004, S. 137 ff.

[207] Dies wurde bereits unter dem Begriff „Standard-Passwörter" im Abschnitt 2.8.1 beschrieben.

[208] Vgl. CHESWICK, W. R.; BELLOWIN, S. M., RUBIN, A. D.: Firewalls und Sicherheit im Internet. 2. Aufl., 2004, S. 219 ff.

fe über den Arbeitsspeicher realisiert.[209] Gelingt es dem Angreifer, physikalischen Zugriff auf das Authentifizierungssystem zu erhalten, so kann er auch beispielsweise ein alternatives Betriebssystem starten und die Inhalte und Schlüssel des Rechners ohne Zugriffskontrolle kopieren oder manipulieren.[210]

- **Hardware-Manipulation**: Bei physikalischem Zugriff auf das Authentifizierungssystem ist ein Austausch der Hardware oder deren Modifikation möglich. So kann der Angreifer die Festplatte stehlen, um sie in einem anderen Rechner zu analysieren. Auch können I/O Kanäle angezapft und so Informationen und Daten im laufenden Betrieb des Rechners gewonnen werden.[211]

- **Angriffe auf die Verfügbarkeit**: Über den Netzwerk-Anschluss des Authentifizierungssystems, der beispielsweise für die indirekte Authentifizierung verwendet wird, erhält der Angreifer eine Schnittstelle für entfernte Angriffe. Er kann hierbei neben der Suche nach eventuellen Schwachstellen der Software auch einen Stillstand des Systems erzwingen (sog. „Denial of Service“ DoS-Angriff).[212] Während ein DoS-Angriff abgewendet werden kann, indem die Quell-Adresse des Angreifers blockiert wird, sind verteilte DoS-Angriffe (sog. Distributed Denial of Service kurz: DDoS-Angriffe) kaum zu verhindern.[213] Der Angreifer modifiziert hierfür zuvor zahlreiche Rechner, wie etwa über die Verteilung eines Virus oder Nutzung eines Bot-Netzes[214] über das Internet, die später jeweils eigenständig einen DoS-Angriff auf das zu attackierende System auslösen. Die Authentifizierung legitimer Benutzer am System ist durch die Flut an Paketen, die durch DoS- oder DDoS-Angriffe eintreffen, nicht mehr möglich.

---

[209] Vgl. „buffer overflow“ CHESWICK, W. R.; BELLOWIN, S. M., RUBIN, A. D.: Firewalls und Sicherheit im Internet. 2. Aufl., 2004, S. 137.

[210] Vgl. „os substitution“ in SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 109.

[211] Vgl. „I/O access“ in SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 110 ff.

[212] Vgl. „Denial of Service“ in ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 100 ff. und CHESWICK, W. R.; BELLOWIN, S. M., RUBIN, A. D.: Firewalls und Sicherheit im Internet. 2. Aufl., 2004, S. 144 ff.

[213] Vgl. CHESWICK, W. R.; BELLOWIN, S. M., RUBIN, A. D.: Firewalls und Sicherheit im Internet. 2. Aufl., 2004, S. 147 ff.

[214] Vgl. CHESWICK, W. R.; BELLOWIN, S. M., RUBIN, A. D.: Firewalls und Sicherheit im Internet. 2. Aufl., 2004, S. 156 f.

Durch Abschottung der Authentifizierungssysteme, z.B. durch Firewalls[215] oder Intrusion-Prevention-Systeme (IPS)[216] als Netzwerkfilter oder physikalische Sicherung des Zugriffs auf die Systeme, können die genannten Angriffe weitestgehend verhindert werden. Einzig die Abwehr von den skizzierten DDoS-Angriffen ist mit derzeitigen Netzwerk-Protokollen nur schwer möglich.[217]

2.8.4 Social Engineering und Phishing

Schwächstes Glied in der realisierten Sicherheits-Kette zwischen zu schützender Ressource und dem Benutzer ist letzterer selbst.[218] Benutzer können manipuliert werden, um Authentifizierungsmerkmale preiszugeben und Verfahren zu missbrauchen. So können sie gefälschte Zertifizierungsstellen als vertrauenswürdig in ihrem Betriebssystem akzeptieren oder Dritten ihr Passwort aushändigen. So kann ein Angreifer unter einem Vorwand, wie der neuen Installation eines Programms für den Benutzer dessen Passwort per Telefon erfragen. Diese Manipulation der Benutzer, die freiwillig ihr Passwort herausgeben, wird als „Social Engineering“ bezeichnet.[219] Eine spezielle Ausprägung des Social Engineering ist die Fälschung von Nachrichten, in denen Benutzer von einer vermeintlich vertrauten Instanz aufgefordert werden, ihr Passwort einzugeben. Dies kann durch einen Aufruf per E-Mail z.B. über ein angehängtes Programm oder über die Manipulation von Web-Seiten und das Versenden von Verweisen zu diesen erfolgen. Dem Benutzer wird hierbei z.B. die Web-Seite seiner Bank vorgetäuscht. Gibt er auf der gefälschten Seite sein Passwort ein, so wird dies dem Angreifer übermittelt. Sofern die eigentliche Seite keine Sicherheitsmaßnahmen vornimmt, ist sogar die nahtlose Übergabe der Sitzung des Benutzers an die reale Bank möglich.[220] Wird die Leichtgläubigkeit bzw. Täuschung des Benutzers verwendet, um ein Passwort zu erlangen, so bezeichnet man dies auch als „Phishing“[221] oder „Pharming“.[222]

---

[215] Vgl. CHESWICK, W. R.; BELLOWIN, S. M., RUBIN, A. D.: Firewalls und Sicherheit im Internet. 2. Aufl., 2004, S. 219 ff.

[216] CHAPPLE, M.: Intrusion Prevention Systeme sind immer noch ein Muss, 2007.

[217] Vgl. CHESWICK, W. R.; BELLOWIN, S. M., RUBIN, A. D.: Firewalls und Sicherheit im Internet. 2. Aufl., 2004, S. 149.

[218] Vgl. MITNICK, K.: Die Kunst der Täuschung, 2006, S. 19 und SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 19 ff.; GERD TOM MARKOTTEN, D.: Benutzbare Sicherheit in informationstechnischen Systemen, 2003, S. 75.

[219] Vgl. MITNICK, K.: Die Kunst der Täuschung, 2006, S. 376.

[220] Vgl. „Man-in-the-Middle“ Angriff unter „Übernahme der Sitzung“ in Abschnitt 2.8.2.

[221] Vgl. SCHULTZ, A.: Phishing for financial agents oder die Mär vom schnellen Geld, 2006.

[222] Vgl. HERRMANN, V.: Pharming - Phishing mit Schleppnetz, 2007.

Auch Administratoren können manipuliert werden und Authentifizierungsverfahren deaktivieren oder vorgetäuschte neue Benutzerkonten einrichten. Ein Angreifer kann einen Administrator z.B. täuschen, indem er telefonisch vorgibt, gerade nicht am Arbeitsplatz zu sein und dringend Zugriff auf seine Dateien zu benötigen, aber sein Passwort vergessen zu haben. Unter Umständen kann so die Setzung eines neuen Passworts am Telefon erzielt werden.[223] Sogar von Zertifizierungsstellen, die bei der Vergabe von Zertifikaten bzw. der Identifizierung der Zertifikatnehmer auf hohe Sicherheitsanforderungen setzen, sind bereits Fälle bekannt, in denen auf diesem Weg einem unberechtigten Dritten ein offizielles Zertifikat auf den Namen der Fa. Microsoft ausgestellt wurde.[224]

Es ist auch möglich, dass ein Administrator oder legitimer Benutzer die Authentifizierungssysteme aus eigenem Interesse missbraucht. Angriffe, die von Personen innerhalb der Organisation durchgeführt werden, sind nach SMITH häufig.[225] Diese bieten zudem ein hohes Risiko, da die Manipulationen des Administrators oder internen Benutzers schwerer aufgedeckt werden können.[226]

Die Schwachstelle Administrator lässt sich durch die Aufteilung der Authentifizierung bzw. anschließende Berechtigung auf mehrere Administratoren erzielen. Kennt ein Administrator z.B. nur einen Teil des erforderlichen Passworts, so benötigt er für die Manipulation zusätzlich einen anderen Administrator.

Ein Social Engineering, das auf die Leichtgläubigkeit der Benutzer zielt, ist durch geeignete Schulung der Benutzer in Bezug auf die IT-Sicherheit besser verhinderbar. Der Erfolg von Angriffen, in denen ein Benutzer oder Administrator für die Manipulation der Authentifizierung bedroht wird, kann jedoch nicht vollständig ausgeschlossen werden.[227]

---

[223] Vgl. CHESWICK, W. R.; BELLOWIN, S. M., RUBIN, A. D.: Firewalls und Sicherheit im Internet. 2. Aufl., 2004, S. 135.

[224] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 407 f.

[225] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 75.

[226] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 75 ff.

[227] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 77 f.

3 Authentifizierung in heterogenen IT-Strukturen

Heterogene IT-Strukturen umfassen neben der Vielzahl angebotener Ressourcen auch eine Vielzahl Authentifizierungsverfahren und -systeme, die teilweise jeweils eigene Authentifizierungsmerkmale erfordern. Die resultierende Diversität äußert sich für die Benutzer, insbesondere aber für die Betreiber durch einen hohen Aufwand in Bezug auf die Verwaltung und Verwendung der Authentifizierung. In den folgenden Abschnitten wird daher der Ist-Zustand der Authentifizierung in heterogenen IT-Strukturen ermittelt.

3.1 Diversität der Authentifizierung als Grund für deren Vereinheitlichung

Im Abschnitt 2.4.2 wurde bereits die Diversität der Authentifizierung in heterogenen IT-Strukturen anhand der großen Anzahl unterschiedlicher verwendeter Authentifizierungssysteme, -verfahren und -merkmale beschrieben. Durch die Vereinheitlichung soll eine Minimierung des Aufwands bei gleichzeitiger Wahrung der durch die Authentifizierung erzielten Sicherheit erfolgen. Dabei besitzen die Authentifizierungssysteme hinsichtlich der Vereinheitlichung die größte Relevanz für deren Betreiber bzw. Organisationen, da sie unmittelbar mit den zur Verfügung gestellten Ressourcen in Verbindung stehen.[228] Für die Benutzer haben wiederum die Authentifizierungsmerkmale die höchste Relevanz, da sie von diesen unmittelbar mit der Authentifizierung verbunden werden.[229]

Ein Benutzer benötigt für die Ressourcen innerhalb der IT-Struktur viele unterschiedliche Passwörter und Zertifikate. In einer Studie von Forrester Consulting aus dem Jahr 2004 wird die durchschnittliche Anzahl von acht unterschiedlichen Passwörtern eines Benutzers bestimmt.[230] Eine weitere Studie der Fa. RSA Security aus dem Jahr 2006 ermittelt bei 35% der 1.343 Befragten (in Asien, Europa, Latein- und Nordamerika) sogar zwischen sechs und 15 unterschiedliche Passwörter bei steigender Tendenz.[231] Neben dem Aufwand für Verwaltung und Verwendung dieser Passwörter aufseiten der Benutzer entsteht ein erhöhter Aufwand, insbesondere für die Betreiber durch erforderliche Passwort-Rücksetzungen sowie Verwaltung der Authentifizierungsverfahren und -systeme und damit verbundene Kosten. In der genannten RSA-Studie aus dem Jahr 2006 gaben 21% der Befragten an, dass 25-50% der Help-Desk-Anfragen in ihrer Firma Passwort-bezogen

---

[228] Vgl. Relationen zwischen Ressourcen und Authentifizierungssystemen in Abbildung 2-2.

[229] Vgl. RENAUD, K.: Evaluating Authentication Mechanisms, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 104.

[230] Vgl. ENSOR, B.: How Consumers Remember Passwords, 2004.

[231] Vgl. RSA SECURITY INC.: The 2nd Annual RSA Security Password Management Survey, 2006, S. 2.

sind.[232] Die langfristigen Betriebskosten günstiger Passwort-Lösungen sind nach CHESWICK ET AL. weitaus höher als deren initiale Anschaffung und Realisierung.[233] Hinzu kommt die schlechte Skalierbarkeit, z.B. durch unterschiedliche Hash-Verfahren, in denen die Passwörter kodiert und gespeichert werden.[234] Soll etwa eine neue Applikation innerhalb einer heterogenen IT-Struktur angeboten werden, so können Passwörter der bestehenden Benutzer nur dann übernommen werden, sofern die Applikation die existierenden Hash-Werte der Benutzer-Passwörter verwenden kann, da die Hash-Werte nicht invertiert oder konvertiert werden können.

Die Diversität der Authentifizierungsmerkmale wird zusätzlich durch Authentifizierungsverfahren erhöht, die spezielle Merkmale voraussetzen. Beispielsweise erfordern Off-line-Authentifizierungsverfahren den Einsatz von öffentlichen Schlüsseln resp. Zertifikaten[235], während diese für die indirekte, direkte und lokale Authentifizierung nicht erforderlich sind. Unterschiedliche Authentifizierungsverfahren sind auch aufgrund der unterschiedlichen Sicherheitsanforderungen innerhalb einer heterogenen IT-Struktur erforderlich. Spezielle Anwendungsfälle setzen besondere Authentifizierungsverfahren voraus. So muss für die dezentrale Authentifizierung im Netzwerk ein verschlüsseltes Verfahren verwendet werden, das nicht von Dritten abgehört werden kann[236], während eine Authentifizierung am lokalen System insbesondere vor Modifikationen am System selbst geschützt werden muss.[237] Für unterschiedliche Ressourcen sind jeweils eigene Authentifizierungsvorgänge erforderlich. Gegebenfalls muss der Benutzer sogar für die Verwendung ein und derselben Ressource kurz hintereinander erneut sein Merkmal vorweisen. Benutzer wünschen sich daher ein sog. „Single Sign-On“ oder „Reduced Sign-On“, wie in Abschnitt 2.1.12 definiert, das die Anzahl der erforderlichen Authentifizierungsvorgänge innerhalb einer Sitzung minimiert.[238] Während diese Reduzierung des Aufwands insbesondere für Benutzer relevant ist, ist sie auch seitens der Betreiber, z.B. für den kooperativen Betrieb von Ressourcen zwischen mehreren Organisationen erforderlich, um allen Benutzern beider Organisationen Zugriff auf gemeinsame Ressourcen zu gewähren.

---

[232] Vgl. RSA SECURITY INC.: The 2nd Annual RSA Security Password Management Survey, 2006, S. 3.

[233] Vgl. CHESWICK, W. R.; BELLOWIN, S. M., RUBIN, A. D.: Firewalls und Sicherheit im Internet. 2. Aufl., 2004, S. 185 f.

[234] Hash-Funktionen sind Einwegfunktionen. Vom Hash-Wert kann nicht auf den Eingangswert geschlossen werden, vgl. Abschnitt 2.6.2.

[235] Der Einsatz von Zertifikaten wird in Abschnitt 2.7.4 detailliert beschrieben.

[236] Vgl. „Abhören der Sitzung“ in Abschnitt 2.8.2.

[237] Vgl. „Hard- und Software Manipulation“ in Abschnitt 2.8.3.

[238] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 115 f. und WINDLEY, P. J.: Digital Identity, 2005, S. 84 f.

Heterogene IT-Strukturen zeichnen sich durch eine hohe Anzahl unterschiedlicher Ressourcen unterschiedlicher Hersteller aus.[239] Häufig sind Ressourcen zusätzlich an eine bestimmte Plattform (vgl. Windows und Unix-Anwendungen) gebunden und setzen eigene Authentifizierungssysteme ein. Parallel zur Diversität der Authentifizierungssysteme steigt zusätzlich die Diversität zugehöriger Authentifizierungsverfahren. Sollen alle Benutzer gleichermaßen Zugriff auf die einzelnen Ressourcen erhalten oder diese kooperativ mit anderen Organisationen genutzt werden, steigt der Aufwand durch die Pflege der Authentifizierungskonten für alle Benutzer in dem jeweiligen System. Die Verwendung eines einzigen zentralen Systems ist zusätzlich nicht sinnvoll, da es eine zentrale Fehlerquelle hinsichtlich der Authentifizierung darstellt.[240]

3.2 Bestehende Lösungen für einheitliche Authentifizierung

In den folgenden Abschnitten werden bestehende Teillösungen für die Vereinheitlichung der Authentifizierung in heterogenen IT-Strukturen beschrieben. Sie fokussieren die Minderung des Aufwands, der durch die erhöhte Diversität der Authentifizierung in heterogenen IT-Strukturen entsteht, wie im vorherigen Abschnitt beschrieben. Häufig sind die skizzierten Lösungen herstellerspezifisch, plattformgebunden oder bedingen eine Einschränkung der erzielten Sicherheit oder Benutzbarkeit (Usability). Entsprechende Probleme und Grenzen bestehender Verfahren werden daher anschließend in Abschnitt 3.3 geschildert. Basierend auf der Adressierung dieser Probleme des Ist-Zustands und der Fokussierung auf die Anforderungen des Soll-Zustands in Kapitel 4, erfolgt in Kapitel 5 und 6 die Modellierung einer einheitlichen Authentifizierung für heterogene IT-Strukturen, die neben der Auswahl geeigneter Verfahren anhand der Optimierung des Verhältnisses zwischen erforderlichem Aufwand und erzielter Sicherheit als Nutzen der Authentifizierung auch Anforderungen und Implementierungsmöglichkeiten zukünftiger Lösungen für einheitliche Authentifizierung nennt.

3.2.1 Verwendung eines einzigen Authentifizierungsverfahrens und -systems

Die einfachste und umfassendste Form der Vereinheitlichung kann innerhalb einer heterogenen IT-Struktur erzielt werden, indem genau ein Authentifizierungssystem, ein einziges Verfahren und von jedem Benutzer nur ein Authentifizierungsmerkmal verwendet werden. Abbildung 3-1 stellt diese

---

[239] Vgl. Verwendung unterschiedlicher Hard- und Software-Komponenten in heterogenen IT-Strukturen in Abschnitt 2.1.10.

[240] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 128 f.

Vereinheitlichungsform graphisch dar. Hierbei müssen alle Ressourcen, die von O_1 und O_2 betrieben werden, das einheitliche Authentifizierungssystem S_1 unterstützen. Das einheitliche Authentifizierungsverfahren v_1 muss zusätzlich alle möglichen Anwendungsfälle innerhalb der IT-Struktur (z.B. den mobilen Zugriff) erlauben.

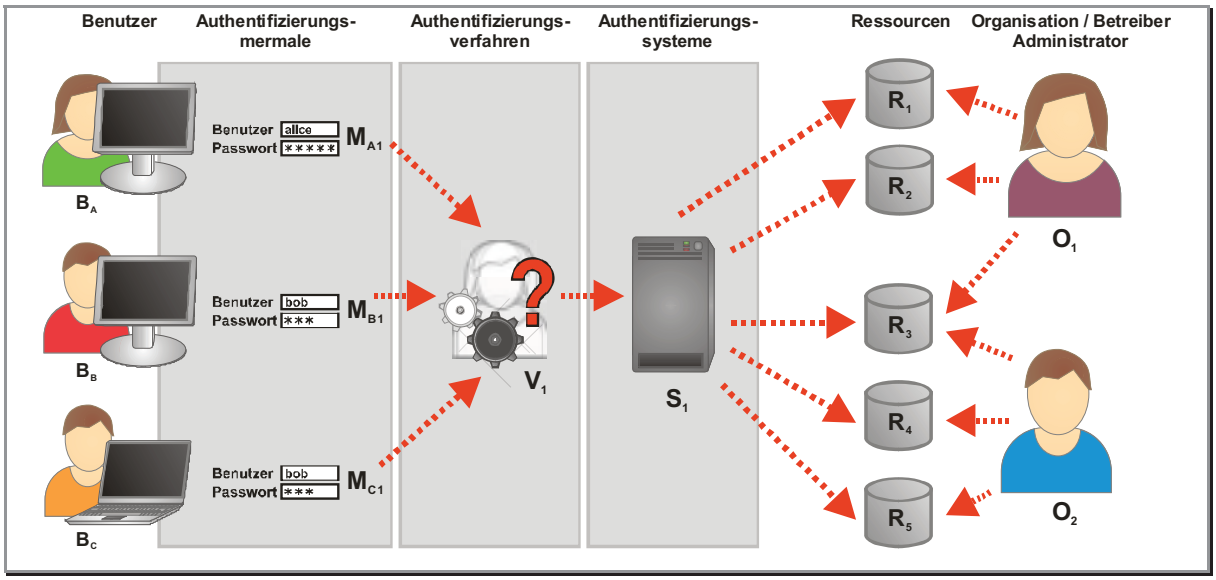

Abbildung 3-1: Vereinheitlichung der Authentifizierung durch Realisierung einer homogenen IT-Struktur

In heterogenen IT-Strukturen lässt sich diese Anforderung, z.B. aufgrund der Plattformabhängigkeit von Authentifizierungssystemen, nicht ohne Einschränkungen erreichen. Eine vollständige Vereinheitlichung der Authentifizierungsmerkmale, -verfahren und -systeme ist nur möglich, wenn auf Anwendungen, die ein eigenes Authentifizierungssystem oder -verfahren erfordern, verzichtet werden kann oder von vornherein eine homogene Struktur betrieben wird.

Auch für die Benutzer ist insbesondere in heterogenen IT-Strukturen die Verwendung eines einheitlichen Authentifizierungsverfahrens nicht ohne Einschränkung möglich. Beispielsweise muss das Authentifizierungsverfahren dezentral an mobilen Endgeräten oder auf Web-Seiten eingesetzt werden können. Dies ist nicht gewährleistet, sofern das einheitliche Verfahren eine bestimmte Hard- oder Software erfordert.

Aufgrund der Heterogenität der betrachteten wissenschaftlichen IT-Strukturen[241] und der in diesem Abschnitt geschilderten Nachteile wird die skizzierte vollständige Vereinheitlichung der Authentifizierung in den folgenden Abschnitten nicht gesondert berücksichtigt. Stattdessen werden Möglichkeiten für die Bestimmung eines optimalen Verhältnisses für die Vereinheitlichung der Authentifizierung innerhalb heterogener IT-Strukturen in Kapitel 6 beschrieben.

[241] Vgl. Eigenschaften heterogener IT-Strukturen in Abschnitt 2.1.10.

3.2.2 Verzeichnisdienste, Meta-Directory und Virtual Directory

Um die Authentifizierung in heterogenen IT-Strukturen zu vereinheitlichen werden im Allgemeinen Verzeichnisdienste verwendet. Diese speichern dabei die erforderlichen Authentifizierungskonten zentral. Verwenden alle Ressourcen den Verzeichnisdienst für die Authentifizierung, so bildet er das alleinige Authentifizierungssystem innerhalb der IT-Struktur. Im Unix-Umfeld wurde zunächst eine lokale oder direkte Authentifizierung mittels passwd bzw. shadow eingesetzt.[242] Später wurde für die vereinfachte Administration und Verwaltung der Authentifizierungskonten der Network Information Service (kurz: NIS, später auch NIS+) basierend auf dem Yellow Pages (yp) Protokoll von Sun Microsystems eingeführt.[243] Benutzer konnten sich dadurch an allen Systemen innerhalb der Unix-Umgebung mit dem gleichen Benutzernamen und Passwort authentisieren.

Auch im Windows-Umfeld wurde zunächst eine lokale oder direkte Authentifizierung eingesetzt. Mit Windows NT wurde schließlich die Domänenstruktur eingeführt, die wie NIS eine vereinfachte Verwaltung der Authentifizierung an mehreren Ressourcen erzielte. Seit Windows 2000 existiert mit Active Directory ein Verzeichnisdienst, der gemeinsam mit Kerberos für die dezentrale Authentifizierung in aktuellen Windows-Umgebungen verwendet wird.[244]

Aufgrund der mangelnden Sicherheit von NIS, die unter anderem durch die unverschlüsselte und ungesicherte Übertragung der Authentifizierungsmerkmale bedingt wird, wurden yp, NIS und NIS+ in aktuellen Unix-Umgebungen, analog zum Active Directory Ansatz von Microsoft, weitgehend durch Lightweight Directory Access Protocol (kurz LDAP) basierte Verzeichnisse abgelöst.[245] LDAP stellt dabei im Gegensatz zum ursprünglichen X.500 Ansatz der International Telecommunication Union (ITU) für Verzeichnisdienste[246] einen schlanken offenen Internet-Standard für den Zugriff auf Verzeichnisse dar, der in RFC 4510 spezifiziert wird.[247]

Das LDAP-Protokoll erlaubt während der Anmeldung am Verzeichnisdienst über die sog. Bindung (bind) eine Authentifizierung und stellt damit auch ein Authentifizierungsverfahren zur Verfügung.

---

[242] Vgl. ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 456.

[243] Vgl. CHESWICK, W. R.; BELLOWIN, S. M., RUBIN, A. D.: Firewalls und Sicherheit im Internet. 2. Aufl., 2004, S. 79 f. und ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 117 f.

[244] Vgl. MICHELA, F.; PALME, M.: Active Directory, 1999, S. 60 f., 126.

[245] Vgl. CHESWICK, W. R.; BELLOWIN, S. M., RUBIN, A. D.: Firewalls und Sicherheit im Internet. 2. Aufl., 2004, S. 96.

[246] Vgl. MICHELA, F.; PALME, M.: Active Directory, 1999, S. 21 ff.

[247] Vgl. ZEILENGA, K.: Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map (RFC 4510), 2006.

Die Übermittlung der Daten kann hierbei mittels LDAPS über eine TLS / SSL Sitzung verschlüsselt erfolgen.[248] Für die eigentliche Authentifizierung mittels Benutzername und Passwort erlaubt LDAP die Verwendung unterschiedlicher Authentifizierungsverfahren wie SASL und GSSAPI, die in Abschnitt 3.2.8 beschrieben werden.

LDAP-basierte Verzeichnisdienste bilden häufig die Grundlage für einheitliche Authentifizierung in bestehenden heterogenen IT-Strukturen. Unterschiedliche Typen von Verzeichnisdiensten können dabei wie in Abbildung 3-2 dargestellt klassifiziert werden.

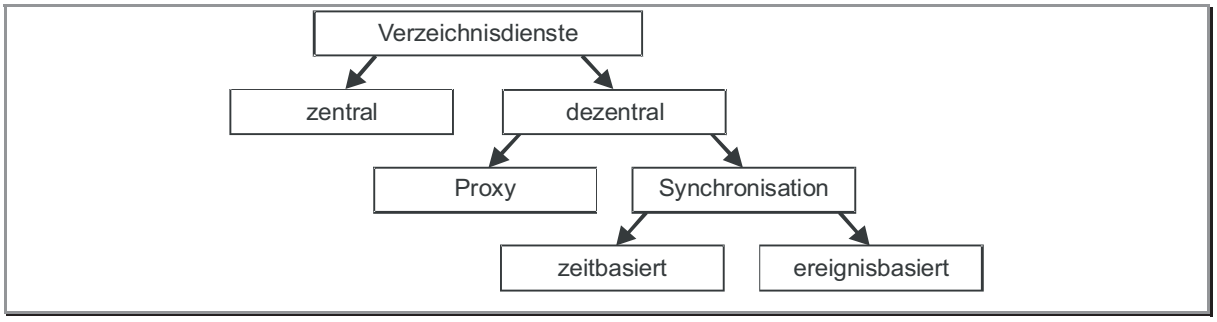

Abbildung 3-2: Klassifizierung von Verzeichnisdiensten

Zentrale Verzeichnisdienste

Wird von allen Ressourcen innerhalb der gesamten IT-Struktur ein einziges zentrales Verzeichnis verwendet, so wird dies als zentrales Authentifizierungssystem, wie in Abbildung 3-3 gezeigt, eingesetzt. Die Ressourcen können beispielsweise über LDAP an das Authentifizierungssystem angebunden werden.

Beispiele für zentrale Verzeichnisdienste bilden Microsoft Active Directory[249], OpenLDAP[250] oder Novell eDirectory.[251] Es existieren auch Erweiterungen für zentrale Verzeichnisdienste, die eine partielle plattformübergreifende Nutzung erlauben. Beispiel hierfür sind AD4Unix und Microsoft Services for Unix, die eine Anbindung von Unix-Rechnern an ein Active Directory erlauben, oder Samba Erweiterungen des OpenLDAP-Schemas für die Anbindung von Windows-Rechnern.[252] In der Regel bieten diese nicht den vollen Funktionsumfang im Vergleich zu einem originär für die jeweilige Plattform vorgesehenen Authentifizierungssystem.

---

[248] SSL, TLS und darauf basierende Verfahren wie LDAPS wurden in Abschnitt 2.6.1 erläutert.

[249] Vgl. MICHELA, F.; PALME, M.: Active Directory, 1999.

[250] Vgl. KLÜNTER, D.; LASER, J.: LDAP verstehen, OpenLDAP einsetzen. Grundlagen, Praxiseinsatz, Single Sign-On Systeme, 2003.

[251] Vgl. Novell Directory Service and Identity Management: eDirectory, 2007.

[252] AD4Unix, 2007; Microsoft Windows Services for UNIX, 2007; BARTLETT, A.: Samba 4 - Active Directory, 2005.

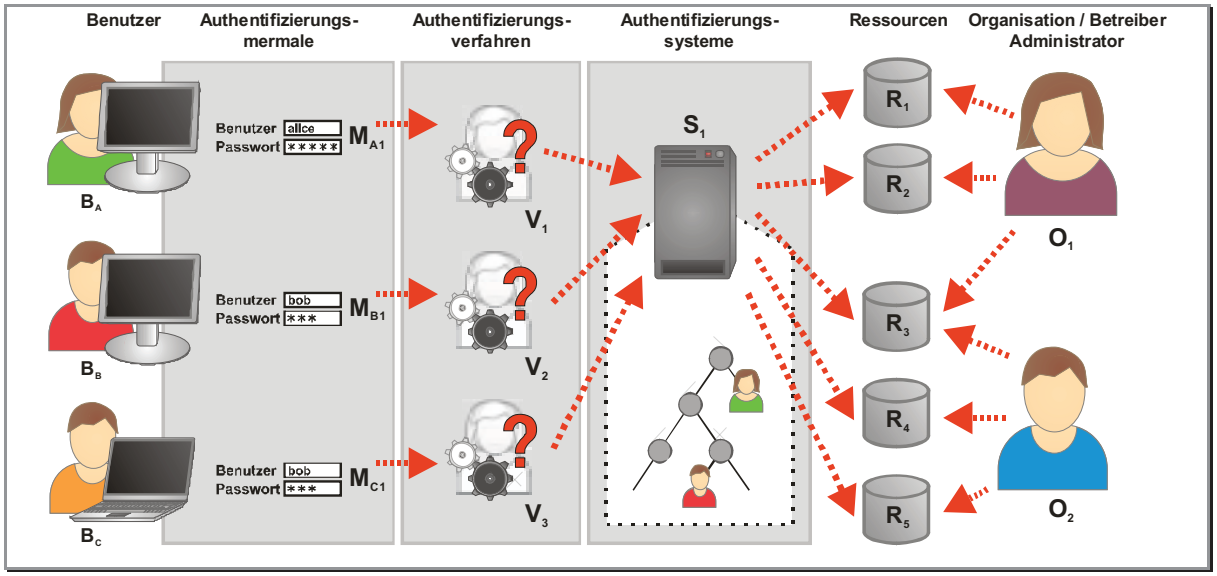

Abbildung 3-3: Verzeichnisdienst als zentrales Authentifizierungssystem

Meta-Directory und dezentrales Identity Management

Zentrale Verzeichnisdienste lassen sich aufgrund der in Abschnitt 3.2.1 genannten Probleme nicht ohne weiteres als alleiniges Authentifizierungssystem in heterogenen IT-Strukturen verwenden. Zudem stellt sich die Frage, wie eine Authentifizierung bzw. Verwaltung der Identitäten über die Grenzen des Verzeichnisses hinweg erfolgen kann. Dies kann erforderlich sein, wenn mehrere Organisationen kooperieren und ihren Benutzern Zugang zu den Ressourcen aller Organisationen ermöglichen wollen. In diesem Fall muss ein organisations-übergreifendes Verzeichnis realisiert werden.

In den vergangenen Jahren haben sich hierfür dezentrale Authentifizierungssysteme bzw. sog. „Identity Management"-Lösungen etabliert, die mehrere Authentifizierungssysteme und deren Konten miteinander verknüpfen. Dezentrale Verzeichnisdienste können hierfür über eine vorgeschaltete Anwendung, die als Proxy unterschiedliche Verzeichnisdienste befragt, oder über eine Synchronisation der in den Konten enthaltenen Informationen resp. Benutzernamen und Authentifizierungsmerkmale verbunden werden.

Die Synchronisation kann dabei zu festen Zeiten (zeitbasiert) bzw. innerhalb bestimmter Intervalle oder ereignisbasiert über ein sog. Meta-Directory, wie in Abbildung 3-4 illustriert, erfolgen.[253] Ein Ereignis beschreibt hierbei eine Änderung, z.B. ein Hinzufügen, Modifizieren oder Löschen eines Authentifizierungskontos, die an andere relevante, ebenfalls an das Meta-Directory angebundene Authentifizierungssysteme ohne zeitliche Verzögerung übertragen werden soll. Relevante Systeme

[253] Vgl. WINDLEY, P. J.: Digital Identity, 2005, S. 85 ff. und POHLMAN, M.: LDAP Metadirectory. Provisioning Methodology, 2003, S. 20 ff.

werden über Filter und Regeln mit den Informationen versorgt, die von den Organisationen entsprechend erstellt werden müssen. Neben dem Vorteil der Meta-Directories durch die flexible Anpassung dieser Regeln für unterschiedliche angebundene Authentifizierungssysteme liegt hier auch ein Nachteil aufgrund des zusätzlichen Implementierungs- und Verwaltungsaufwands des Regelwerks.

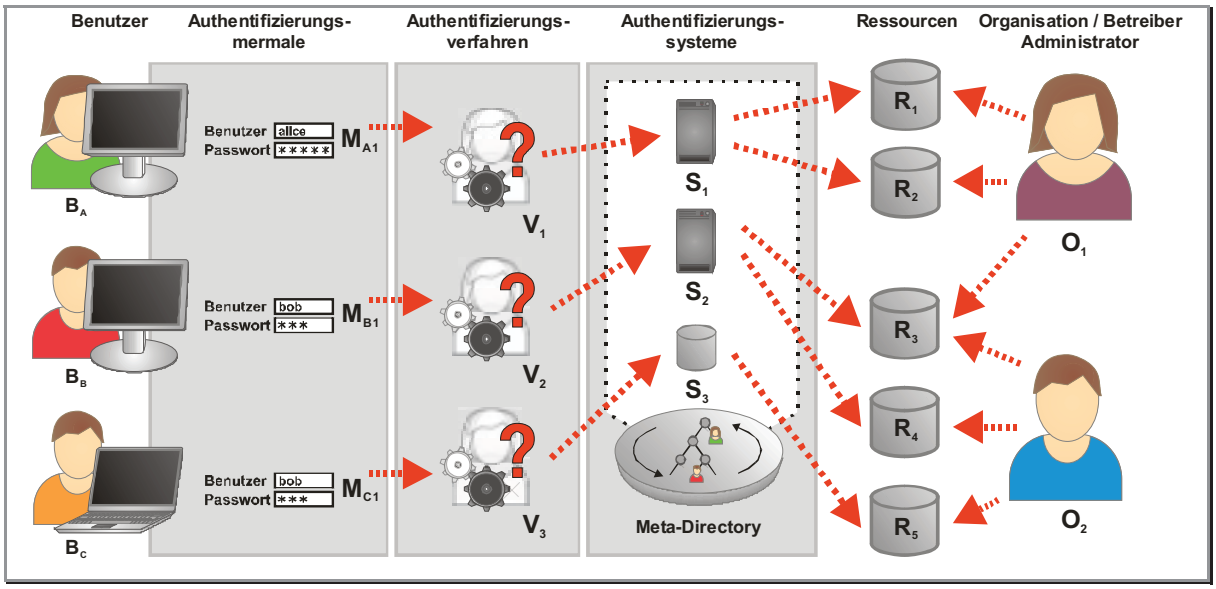

Abbildung 3-4: Abgleich mehrerer Authentifizierungssysteme mittels Meta-Directory

Neben der Synchronisation der Authentifizierungsmerkmale und Identitäten werden Meta-Directories auch für die Synchronisation von Rollen und Rechten für die Autorisierung verwendet. Dies umfasst den Bereich des Access, Security und Digital Rights Management.[254] Dezentrale Verzeichnisdienste versuchen den kompletten Lebenszyklus einer Identität innerhalb einer IT-Struktur zu kontrollieren und so dessen Verwaltung zu vereinfachen.[255] Dies beginnt bei der Anlage aller notwendigen Ressourcen für neue Identitäten (z.B. E-Mail-Adresse, Datei-Freigaben), dem sog. Provisioning, über die individuelle Verteilung der Identität an alle relevanten Authentifizierungssysteme, dem sog. Propagating. Anschließend erfolgt die synchrone Verwaltung der Identität (z.B. Änderung des Nachnamens, Zuweisung von neuen Rollen und Rechten in speziellen Systemen), das sog. Maintaining, bis schließlich eine Löschung oder Sperrung der Identität in der IT-Struktur (z.B. inkl. Archivierung der Daten bestimmter Systeme) erfolgt, was für mehrere Systeme als sog. Deprovisioning bezeichnet wird. Allein die Vereinheitlichung der Verwaltung der Identitä-

[254] Vgl. WINDLEY, P. J.: Digital Identity, 2005, S. 89 ff.
[255] Vgl. WINDLEY, P. J.: Digital Identity, 2005, S. 29 ff.

ten dient bereits als Einsparungs-Potential, z.B. durch die Einführung von Self-Service Portalen für die Passwort-Änderung.[256]

Allgemein können Meta-Directories als Drehscheibe für Informationen unterschiedlicher Datenquellen angesehen werden. Neben Verzeichnisdiensten können diese auch Datenbanken, Dateien usw. darstellen.[257]

Produkte, die zeit- oder ereignisbasierte Meta-Directories implementieren, sind z.B. Microsoft Identity Integration Server (MIIS)[258], Siemens DirX[259] oder Novell Identity Manager.[260]

Virtual Directory

Eine Alternative für die Realisierung dezentraler Verzeichnisse bildet deren Virtualisierung. Anstelle der Synchronisation der Authentifizierungskonten fragen Virtual Directories mehrere Authentifizierungssysteme im Hintergrund ab, um die gewünschte Information zu erhalten.[261] Sie stellen somit einen zentralen Vertreter (Proxy) für die eigentlichen Verzeichnisse bzw. Authentifizierungssysteme bereit.

Abbildung 3-5 zeigt den Einsatz eines Virtual Directorys, das unterschiedliche Authentifizierungsverfahren bietet und unterschiedliche Authentifizierungssysteme anbindet. Virtuelle Verzeichnisse verändern somit die Anfragen von Authentifizierungsverfahren an Authentifizierungssysteme oder deren resultierende Antworten. Vorteil gegenüber Meta-Directories ist, dass nur die gewünschten Informationsflüsse bzw. deren Abfragen in entsprechenden Regeln modelliert werden müssen. Andere Anfragen kann das Virtual Directory ohne Modifikation direkt an das jeweilige Authentifizierungssystem weiterleiten.

---

[256] Vgl. WINDLEY, P. J.: Digital Identity, 2005, S. 54.

[257] Vgl. POHLMAN, M.: LDAP Metadirectory. Provisioning Methodology, 2003, S. 110 ff.

[258] Vgl. Microsoft Identity Integration Server, 2007.

[259] Vgl. Siemens DirX, 2007.

[260] Vgl. Novell Identity Manager, 2007.

[261] Vgl. WINDLEY, P. J.: Digital Identity, 2005, S. 87 f. und POHLMAN, M.: LDAP Metadirectory. Provisioning Methodology, 2003, S. 579 ff.

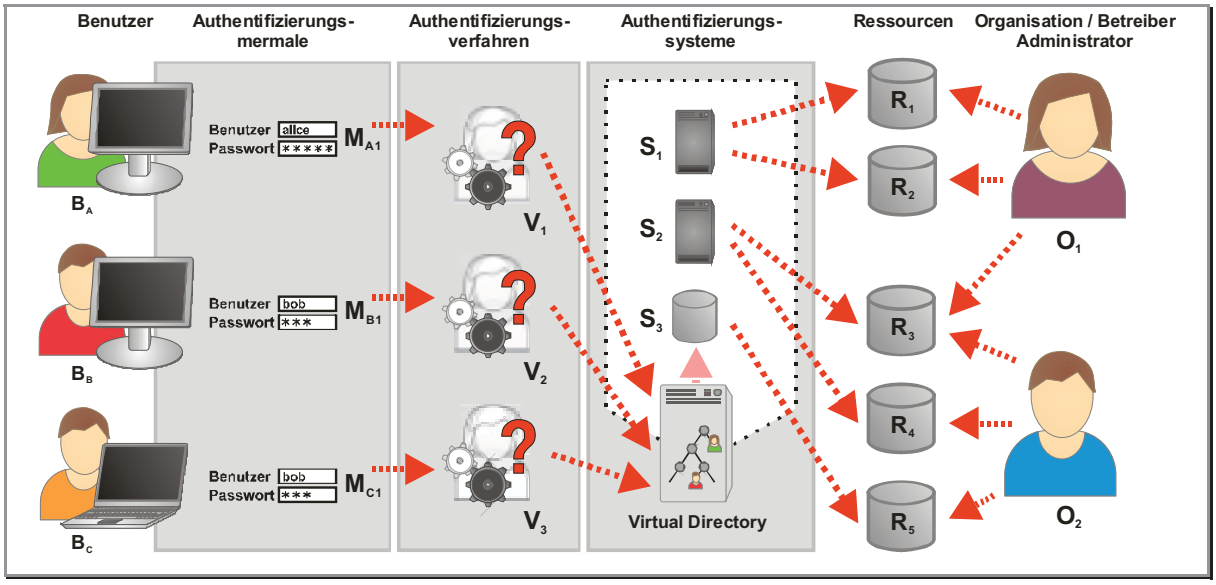

Abbildung 3-5: Verwendung dezentraler Verzeichnisdienste mittels Virtual Directory

Hierdurch ergibt sich für die Authentifizierung jedoch zusätzlich ein Nachteil. Authentifizierungsmerkmale werden von Authentifizierungsverfahren in der Regel als Hash-Wert bzw. nicht invertierbar[262] verschlüsselt übertragen. Virtual Directories können somit entsprechende Authentifizierungsverfahren nur an Systeme weiterleiten, die diese verarbeiten können; eine Übersetzung oder Vermittlung zwischen unterschiedlichen Verfahren ist in der Regel nicht möglich.

Software-Lösungen, die ein Virtual Directory implementieren, sind Penrose[263], Oracle Virtual Directory[264] und Novell Virtual Directory Services.[265]

3.2.3 Kerberos

Die im vorherigen Abschnitt vorgestellten zentralen und dezentralen Verzeichnisdienste erlauben eine Vereinheitlichung der Authentifizierungssysteme. Authentifizierungsverfahren werden hierbei jedoch nicht vereinheitlicht. Um eine sichere Authentifizierung in verteilten IT-Strukturen zu erzielen und gleichzeitig für alle verwendeten Ressourcen nur eine einzige Authentifizierung zu erfor-

[262] Vgl. die fehlende Möglichkeit, vom Hash-Wert auf den Eingangswert zu schließen, wie in Abschnitt 2.6.2 beschrieben.

[263] Vgl. Safehaus penrose, 2007.

[264] Vgl. Oracle Virtual Directory, 2007.

[265] Vgl. Novell Virtual Directory Services, 2007.

dern, wurde am MIT das Kerberos-Verfahren entwickelt.[266] Kerberos ermöglicht ein „Single Sign-On“[267] für alle Ressourcen innerhalb der IT-Struktur. Dies wird durch sog. Tickets erzielt, die als zeitlich begrenzte Authentifizierungsmerkmale von Key Distribution Center (kurz: KDC) innerhalb einer Kerberos-Struktur ausgestellt werden. Die eigentliche Authentifizierung des Benutzers erteilt diesem dabei ein sog. Ticket Granting Ticket (kurz: TGT), das dieser für die Erteilung von Service Tickets, die den Zugriff auf die konkrete Ressource gewähren, verwendet. Aufgrund der Verwendung des TGT, dem der Ticket-Granting-Server für die Vergabe von Service Tickets durch die Verwendung eines gemeinsamen symmetrischen Sitzungsschlüssels (K) vertraut, ist seitens des Benutzers hierbei keine erneute Authentifizierung erforderlich.[268] Den Ablauf einer Kerberos-Sitzung veranschaulicht die Abbildung 3-6.

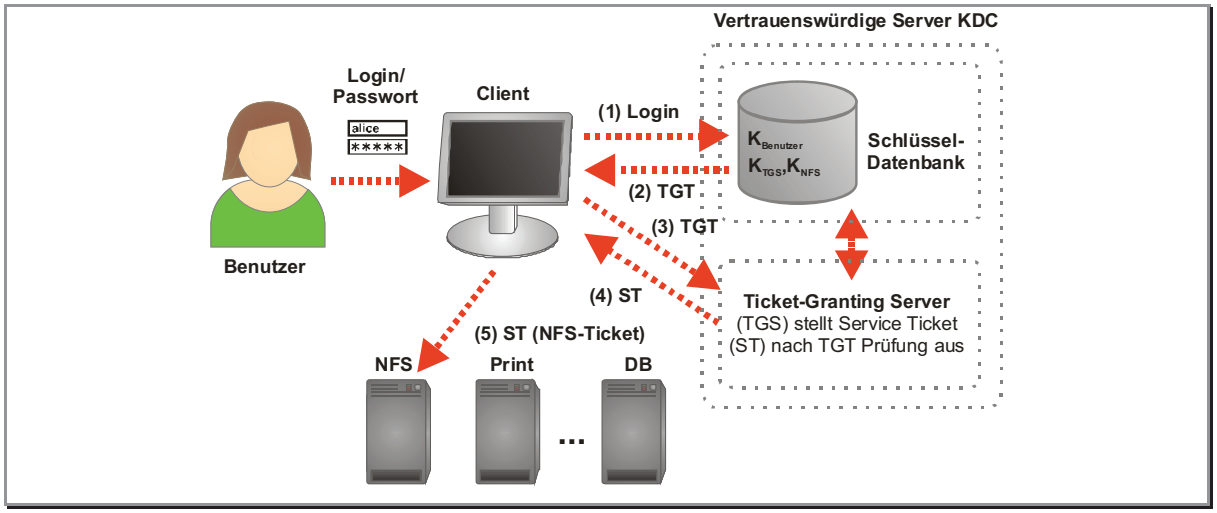

Abbildung 3-6: Einsatz von Kerberos als einheitliches Authentifizierungsverfahren und -system nach ECKERT[269]

Das KDC bildet aufgrund der Schlüssel-Datenbank, die die Authentifizierungsmerkmale der Benutzer und Dienste enthält, ein Authentifizierungssystem. Kerberos bildet somit gleichermaßen ein Authentifizierungsverfahren und -system. KDC sowie zugehöriger Ticket Granting Server (TGS) sind für Dienste innerhalb eines festen Bereichs, bzw. einer IT-Struktur, dem sog. Realm resp. der Domäne, zuständig. Durch Vertrauensstellungen (Trusts), basierend auf der gegenseitigen Akzeptanz der Sitzungsschlüssel, können seit Kerberos Version 5 TGTs an andere KDCs, z.B. einer ande-

---

[266] Vgl. NEUMAN, C. ET AL.: The Kerberos Network Authentication Service (V5) (RFC 4120), 2005; GARMAN, J.: Kerberos. The Definitive Guide, 2003, S. 6 ff.; SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 341 ff.

[267] Wie in Abschnitt 2.1.12 beschrieben.

[268] Vgl. GARMAN, J.: Kerberos. The Definitive Guide, 2003, S. 6.

[269] nach ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 506.

ren Organisation, weitergeleitet werden. Dadurch können Realm- und organisationsübergreifende „Single Sign-On"-Strukturen durch Kerberos ermöglicht werden. Theoretisch ist Kerberos durch die Abbildung der Realms auf Domänen innerhalb des Domain Name System (DNS) dezentral anwendbar, jedoch existieren unterschiedliche Kerberos-Implementierungen, die nicht kompatibel sind. Zusätzlich müssen vertrauenswürdige KDCs explizit innerhalb eines Realms definiert werden.[270]

Kerberos steht für unterschiedliche Plattformen zur Verfügung. Beispielsweise ist es das primäre Authentifizierungsverfahren von Microsofts Active Directory. Für Unix-Umgebungen existiert neben der ursprünglichen Kerberos Implementierung des MIT aus dem Athena-Projekt[271] auch eine freie Implementierung des Royal Institute of Technology in Stockholm (KTH) mit dem Namen heimdal[272] zur Verfügung. Trotzdem ist die Plattformunabhängigkeit von Kerberos begrenzt. So wurde die Kerberos-Implementierung in Microsofts Active Directory neben der Authentifizierung um die Unterstützung von Autorisierungsmerkmalen erweitert. Die resultierenden Tickets sind daher nicht mehr kompatibel mit der ursprünglichen Spezifikation.[273] Insbesondere begrenzt jedoch die Notwendigkeit der Unterstützung von Kerberos durch die Anwendungen die Verwendbarkeit. Nicht für alle Dienste und Anwendungen, die in heterogenen IT-Strukturen eingesetzt werden, existieren entsprechend um die Unterstützung von Kerberos erweiterte (sog. „kerberisierte") Versionen.[274]

Eine Lösung für dieses Problem sollte das Secure European System for Applications in a Multivendor Environment (kurz: SESAME) liefern. Allerdings besitzt dies in IT-Strukturen eine noch geringere Verbreitung als Kerberos.[275]

3.2.4 Public-Key-Infrastrukturen

Eine Möglichkeit, sowohl Authentifizierungsmerkmale als auch -verfahren und -systeme zu vereinheitlichen, stellen X.509-Zertifikate und darauf basierende Public-Key-Infrastrukturen (PKI) dar.[276] Als einheitliches Authentifizierungsverfahren können hierbei zertifikatbasierte Protokolle

---

[270] Vgl. GARMAN, J.: Kerberos. The Definitive Guide, 2003, S. 168 ff.

[271] Vgl. MIHALIK, A. D.: Project Athena, 1999.

[272] Vgl. heimdal, 2007.

[273] Vgl. ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 513 f.

[274] Vgl. GARMAN, J.: Kerberos. The Definitive Guide, 2003, S. 137 ff.

[275] Vgl. GARMAN, J.: Kerberos. The Definitive Guide, 2003, S. 10; What is SESAME, 2007.

[276] Vgl. HOUSLEY, R. ET AL.: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 3280), 2002.

wie SSL oder TLS verwendet werden.[277] Die Public-Key-Infrastruktur dient als Authentifizierungssystem, das die Vertrauenswürdigkeit der Zertifikate gegenüber unterschiedlichen Ressourcen gewährleistet. Durch den X.509 Standard ist die Verwendung von Zertifikaten plattform- und anwendungsunabhängig verwendbar.[278]

X.509-Zertifikate bilden die Grundlage für die meisten Authentifizierungsverfahren, die hohe Sicherheit realisieren sollen. Zertifikate stellen signierte öffentliche Schlüssel dar, die z.B. die Authentizität zweier Kommunikationspartner innerhalb einer SSL- oder TLS-Sitzung gewährleisten. Formal stellt dies eine Off-line-Authentifizierung, wie in Abschnitt 2.7.4 beschrieben, dar. Zertifikate bilden die ideale Basis für einheitliche Authentifizierungsmerkmale. Sie können zum einen für unterschiedliche Verwendungszwecke (Signatur und Verschlüsslung von E-Mails, Authentifizierung von Servern und Clients) eingesetzt werden. Zum anderen kann ein Zertifikat ohne Sicherheitsrisiken auf alle Authentifizierungssysteme kopiert werden, da das Zertifikat lediglich den öffentlichen Schlüssel beinhaltet, der frei zur Verfügung gestellt werden kann. Der zum Zertifikat zugehörige Benutzer authentifiziert sich anhand der Verwendung des passenden privaten Schlüssels, über den nur er verfügt und der auf keinem Authentifizierungssystem benötigt wird.

Für die Verwaltung, z.B. das Ausstellen oder Widerrufen von Zertifikaten, sind Vertrauensstrukturen erforderlich, die als Public-Key-Infrastrukturen bezeichnet werden.[279] An der Spitze dieser Vertrauensstrukturen steht die sog. Root-Zertifizierungsstelle, die Zertifikate für die untergeordneten Zertifizierungsstellen ausstellt. Zertifikate von Root-Zertifizierungsstellen werden bereits mit allen gängigen Betriebssystemen ausgeliefert. Beispiele für Root-Zertifikate, die mit allen Browsern und Betriebssystemen ausgeliefert werden, stellen Zertifikate der Firmen VeriSign[280], Thawte[281] oder TrustCenter[282] dar. Die Abbildung 3-7 zeigt die Hierarchie einer Public-Key-Infrastruktur und die entstehende Zertifikatkette vom Endnutzer zur Root-Zertifizierungsstelle. Benutzer können die Gültigkeit eines Zertifikats prüfen, indem sie die digitale Signatur der Zertifikate über die öffentlichen Schlüssel des Ausstellers überprüfen.

Durch eine Kreuzsignatur zwischen zwei Zertifizierungsstellen (z.B. Root-Zertifizierungsstellen) können zusätzlich, unabhängig von der Hierarchie, bilaterale Vertrauensstellungen realisiert wer-

---

[277] Der Einsatz von SSL und TLS wurde bereits in Abschnitt 2.6.1 erläutert. Den Aufbau von Zertifikaten als signierte öffentliche Schlüssel beschreibt darüber hinaus der Abschnitt 2.6.2.

[278] Vgl. ADAMS, C.; LLOYD, S.: Understanding PKI, 2003, S. 223.

[279] Vgl. ADAMS, C.; LLOYD, S.: Understanding PKI, 2003, S. 28 ff., 273 ff.

[280] Vgl. VeriSign, 2007.

[281] Vgl. Thawte, 2007.

[282] Vgl. TrustCenter, 2007.

den. Dies wird als Cross-Zertifizierung bezeichnet.[283] In diesem Fall vertrauen alle Benutzer beiden Zertifizierungsstellen.

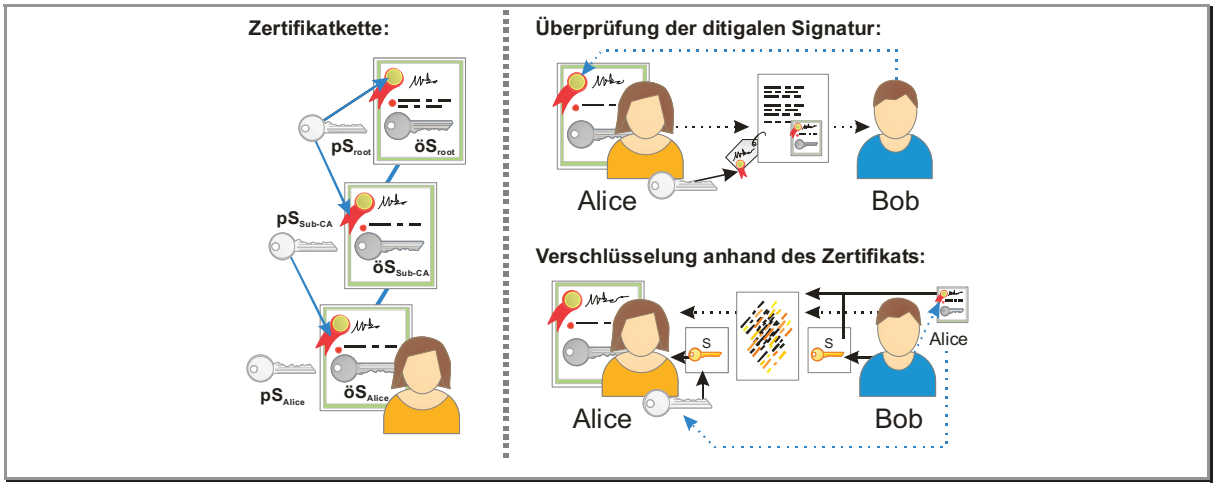

Abbildung 3-7: Zertifikatkette in Public-Key-Infrastrukturen und Anwendung von Zertifikaten

Neben Zertifizierungsstellen (Certification Authority, kurz: CA) können auch Registrierungsstellen (Registration Authority, kurz: RA), die nicht selbst Zertifikate ausstellen, sondern ausschließlich dezentral die Identität der Zertifikatnehmer überprüfen und z.B. mittels digitaler Signatur der Zertifizierungsstelle gegenüber gewährleisten, verwendet werden.

Wie in Abbildung 3-7 illustriert, signiert die Root-Zertfizierungsstelle ihr Zertifikat selbst mit ihrem eigenen privaten Schlüssel (pS_{root}). Die Vertrauenswürdigkeit einer Wurzel-Zertifizierungsstelle hängt von der Art und Weise ab, nach der die Zertifikate ausgestellt werden. Um die Vertrauenswürdigkeit zu gewährleisten, halten sich Zertifizierungsstellen an sog. Zertifizierungsrichtlinien (Certification Policies kurz: CP) und Certificate Practice Statements (kurz: CPS). Benutzer können die Zertifizierungsrichtlinien öffentlich einsehen und so die Vertrauenswürdigkeit der Root-Zertifizierungsstelle überprüfen. Für diese existiert in RFC 3647 ein Rahmenwerk.[284] Um in Deutschland digitale Signaturen als rechtskräftig anzuerkennen und der Unterschrift gleichzustellen, wurde das Signaturgesetz (SigG) erlassen. Dieses definiert ebenfalls Vorgaben für erforderliche Sicherheitsniveaus der CP und CPS[285]. Im e-Science-Umfeld werden dezentrale und eigene Public-Key-Infrastrukturen der Teilnehmer durch eine Policy Management Authority (PMA) zu-

[283] Vgl. ADAMS, C.; LLOYD, S.: Understanding PKI, 2003, S. 28 ff., 273 ff.

[284] Vgl. CHOKANI, S. ET AL.: Internet X.509 Public Key Infrastructure, Certificate Policy and Certificate Practices Framework (RFC 3647), 2003.

[285] Vgl. BUNDESMINISTERIUM DER JUSTIZ: Gesetz über Rahmenbedingungen für elektronische Signaturen (SigG), 2001; BUNDESNETZAGENTUR: Zertifizierungsdiensteanbieter, 2007.

sammengefasst. Eine PMA prüft hierbei die Güte und gegenseitige Akzeptanz der CP und CPS und liefert an die Teilnehmer basierend darauf die akkreditierten Root-Zertifikate aus.[286]

Neben dem Ausstellen von Zertifikaten umfassen die Aufgaben einer PKI auch die Veröffentlichung von Zertifikaten, etwa in öffentlichen Verzeichnisdiensten. Hierzu zählt insbesondere die Veröffentlichung von Sperrlisten widerrufener Zertifikate (Certificate Revocation Lists, kurz: CRL)[287] bzw. die Bereitstellung eines Dienstes zur direkten Überprüfung (online) mittels Online Certificate Satus Protocol (OCSP)[288] oder Simple Certificate Verification Protocol (SCVP).[289] Die Zertifizierungsstelle kann gegebenenfalls auch eine Archivierung der privaten Schlüssel anbieten und diesen nach erfolgreicher Prüfung und Authentifizierung des Besitzers diesem erneut aushändigen.[290]

Zertifikate weisen dem enthaltenen öffentlichen Schlüssel, neben der Identifikation des Inhabers und der Signatur des Ausstellers, auch einen Gültigkeitszeitraum zu, um Schlüsselkompromittierungen zu vermeiden.[291] Daher ist eine regelmäßige Verlängerung der Zertifikate erforderlich. Neben der hohen Sicherheit durch die Verwendung von öffentlichen und privaten Schlüsseln, wie in Abschnitt 2.6.2 erläutert, und der Vereinheitlichung durch Zertifikat-basierte Authentifizierungsverfahren, bedeuten PKI daher einen hohen Verwaltungsaufwand.[292] Public-Key-Infrastrukturen sind daher in der Vergangenheit häufig nur vereinzelt eingesetzt worden[293], obwohl die Mehrzahl der aktuellen Authentifizierungsverfahren, die eine hohe Sicherheit realisieren, auf Zertifikaten basieren. Beispiele sind die Verwendung bei HTTPS für die sichere Übermittlung und Authentifizierung von Web-Seiten oder die Verwendung anderer sicherer Protokolle wie LDAPS oder TLS für SMTP.[294] Auch die digitale Signatur und Verschlüsselung von E-Mails mittels S/MIME[295]

---

[286] In Europa existiert hierfür die EUGridPMA: The EUGridPMA - coordinating grid authentication in e-Science, 2007.

[287] Vgl. HOUSLEY, R. ET AL.: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 3280), 2002.

[288] Vgl. MYERS, M. ET AL.: X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol - OCSP (RFC 2560), 1999.

[289] Vgl. FREEMAN, T.: Server-based Certificate Validation Protocol (SCVP), 2007.

[290] Vgl. ADAMS, C.; LLOYD, S.: Understanding PKI, 2003, S. 28 ff., 97 ff.

[291] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 409.

[292] Vgl. ADAMS, C.; LLOYD, S.: Understanding PKI, 2003, S. 28 ff., 263 ff.

[293] Vgl. ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 401 f.

[294] Vgl. Einsatz von SSL für unterschiedliche Anwendungsprotokolle in BADACH, A.; RIEGER, S.; SCHMAUCH, M.: Web-Technologien, 2003, S. 390 f.

[295] Vgl. DUSSE, S. ET AL.: S/MIME Version 2 Message Specification (RFC 2311), 1998.

bzw. von Dokumenten und allgemeinem Code-Signing[296] stellen eine wichtige Anwendung dar. X.509 Zertifikate werden hierfür von den meisten aktuellen Anwendungen direkt unterstützt.[297] Ein weiteres Anwendungsgebiet stellen Web-Services und XML-basierte Dienste dar, deren Sicherheit ebenfalls über Zertifikate gewährleistet wird.[298]

Um den Verwaltungsaufwand zu minimieren, existieren verschiedene Projekte, die im Wesentlichen die Komplexität der Wartung sowie der Richtlinien gemäß CP und CPS einer PKI vereinfachen.[299]

Beispiele für Produkte, die eine PKI implementieren, sind die in Microsoft Windows Server enthaltenen Zertifizierungsdienste[300] und das quelloffene OpenCA[301] resp. OpenSSL[302].

Häufig werden bei der Einführung von Public-Key-Infrastrukturen auch Tokens, wie in Abschnitt 2.5.2 beschrieben, verteilt.[303] Diese ermöglichen neben den genannten Anwendungsbereichen für Zertifikate auch die Authentifizierung beim Login am Arbeitsplatz-Rechner. Hierfür wird das Crypto USB-Token oder die Smart Card während der Anmeldung verwendet und mittels zugehöriger PIN freigeschaltet.[304] Für Windows- und Unix-Umgebungen kann hierbei eine Erweiterung des Kerberos-Protokolls für die Authentifizierung mittels Zertifikat (sog. PKINIT) verwendet werden.[305] Abbildung 3-8 zeigt die Verwendung von PKINIT.

---

[296] Vgl. KOMAR, B.: Microsoft Windows Server 2003. PKI und Zertifikatsicherheit, 2004, S. 425 ff.

[297] Vgl. z.B. OpenOffice, Microsoft Office, Microsoft Outlook, Thunderbird bzw. Web-Browser, siehe auch GWDG-CA Ebene 2 User-CA. Anleitungen und Download, 2007.

[298] Vgl. SAML in Abschnitt 3.2.7.

[299] Vgl. BALFANZ, D.; DURFEE, G.; SMETTERS, D. K.: Making the Impossible Easy: Usable PKI, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 319 ff.; SPKI (geringe Verbreitung) in ADAMS, C.; LLOYD, S.: Understanding PKI, 2003, S. 28 ff., 228 f.; RIEGER, S. ET AL.: Self-Service PKI-Lösungen für eScience, in Paulsen, C. (Hrsg.): Sicherheit in vernetzten Systemen. 13. Workshop, 2006, S. B-1 ff.

[300] Vgl. KOMAR, B.: Microsoft Windows Server 2003. PKI und Zertifikatsicherheit, 2004, S. 61 ff.

[301] Vgl. OpenCA, 2007.

[302] Vgl. OpenSSL, 2007.

[303] Vgl. CHESWICK, W. R.; BELLOWIN, S. M., RUBIN, A. D.: Firewalls und Sicherheit im Internet. 2. Aufl., 2004, S. 189 f.; BUNDESMINISTERIUM FÜR GESUNDHEIT: Die Gesundheitskarte, 2007.

[304] Die Authentifizierung basiert hierbei auf zwei Faktoren, vgl. Abschnitt 2.5.2.

[305] Vgl. ZHU, L.; TUNG, B.: Public Key Cryptography for Initial Authentication in Kerberos, 2006; Einsatz unter Windows in KOMAR, B.: Microsoft Windows Server 2003. PKI und Zertifikatsicherheit, 2004, S. 293 ff.; Einsatz unter Unix in pkinit for heimdal, 2007.

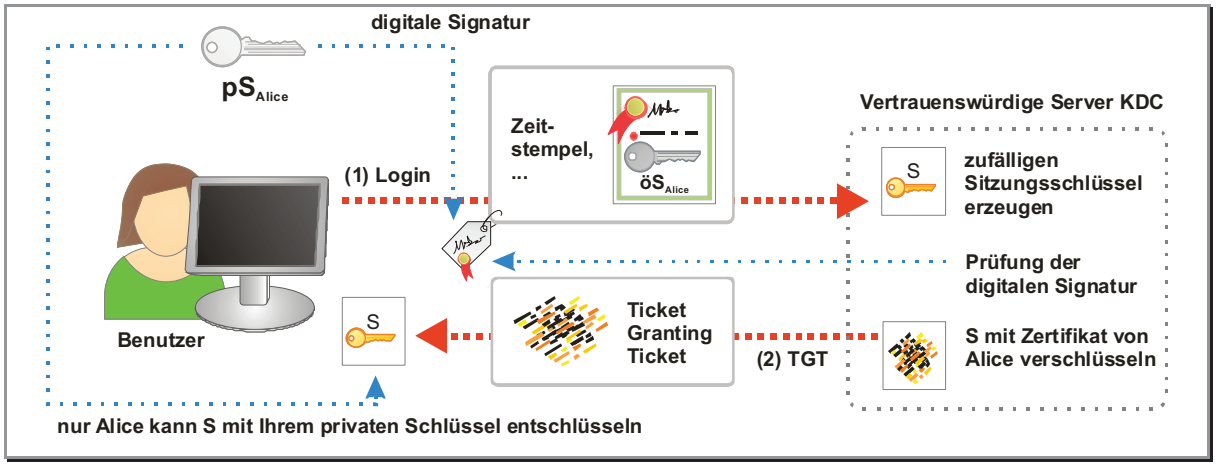

Abbildung 3-8: Verwendung von Zertifikaten bei Kerberos mittels PKINIT nach SMITH[306]

Der Vergleich zwischen Kerberos ohne PKINIT in Abbildung 3-6 und Abbildung 3-8 zeigt, dass bei PKINIT das KDC keine eigenen Schlüssel resp. Konten mehr verwalten muss. Die Verwaltung der Authentifizierungsmerkmale erfolgt somit einheitlich über die PKI. Sofern ein Token[307] für die Authentifizierung verwendet wurde, kann dies nach der Anmeldung für weitere Authentifizierungen z.B. mittels Client- oder Benutzer-Zertifikat einer SSL- oder TLS-Sitzung oder für die Signatur von E-Mails benutzt werden und so ein Single Sign-On unterstützen.

Kerberos basiert, wie in Abschnitt 3.2.3 erläutert, auf zeitlich begrenzt gültigen Tickets. In der Vergangenheit wurde das Kerberos-Verfahren durch die Manipulation der Uhrzeit angegriffen. Zertifikate können hier durch signierte Zeitstempel vertrauenswürdige Gültigkeitszeiträume innerhalb einer IT-Struktur garantieren.[308]

Public-Key-Infrastrukturen und die Verwendung von X.509-Zertifikaten werden aktiv durch unterschiedliche Gremien erweitert. Detaillierte Informationen lassen sich bei der PKIX-Arbeitsgruppe der IETF auffinden.[309]

3.2.5 Netzwerk-Authentifizierungsprotokolle

Netzwerk-Dienste können die in den vorherigen Abschnitten genannten Verfahren wie LDAP, Kerkeros oder SSL und TLS verwenden, um die Authentifizierung der Benutzer durchzuführen. Für den Zugriff auf die Netzwerke selbst, z.B. bei Einwahl-Systemen oder drahtlosen Netzwerken,

---

[306] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 462.

[307] Die Verwendung von Zertifikaten auf aktiven Tokens wurde in Abschnitt 2.5.2 erläutert.

[308] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 363.

[309] Vgl. Public-Key Infrastructure (X.509) (pkix) Charter, 2007.

haben sich jedoch eigene Authentifizierungsverfahren etabliert. Einwahlsysteme basieren häufig auf dem Point-to-Point Protocol (PPP)[310]. Hier wurde zunächst das Password Authentication Protocol (kurz: PAP) und später Challenge Handshake Authentication Protocol (kurz: CHAP) verwendet.[311] Um weitere Netzwerk-Authentifizierungsverfahren und -protokolle unterstützen und diese bei der Einwahl differenzieren zu können, wurde als Erweiterung das Extensible Authentication Protocol (kurz: EAP) in der RFC 3748 definiert.[312] Für EAP existieren verschiedene Erweiterungen, die die konkreten Authentifizierungsverfahren implementieren. EAP-MD5[313] stellt beispielsweise ein auf MD5 basierendes Challenge-Response Verfahren dar. EAP-TLS[314] verwendet TLS für die Authentifizierung von Server und Client mittels X.509-Zertifikat. Die Verfahren EAP-TTLS[315], PEAP[316] sowie EAP-FAST[317] verwenden Challenge-Response-Verfahren innerhalb einer TLS Sitzung (als Tunnel), der die Vertraulichkeit, Integrität und Verbindlichkeit der Übertragung gewährleistet.

Für die Authentifizierung in verteilten Netzwerken wird häufig das Remote Authentication and Dial-In User Service Protokoll (kurz: RADIUS) verwendet.[318] Dabei bildet der RADIUS-Server ein Authentifizierungssystem, das die Konten der Benutzer vorhält oder von anderen Authentifizierungssystemen (z.B. einem Verzeichnisdienst oder einem Kerberos KDC) bezieht. Clients des RADIUS-Servers stellen Netzwerkkomponenten dar, die den Benutzern Zugang zum Netz gewähren (Einwahlsysteme, Access Points). Diese werden als Network Access Service (NAS) bezeichnet. RADIUS übernimmt neben der Authentifizierung (Authentication) auch die Autorisierung (Authorization) und Abrechnung (Accounting). Man bezeichnet es daher in Bezug auf die Anfangsbuchstaben der genannten Aufgaben auch als AAA-Protokoll. Ein RADIUS Server kontrolliert den

---

310 Vgl. BADACH, A.; HOFFMANN, E.: Technik der IP-Netze, 2001, S. 428 ff.; SIMPSON, W.: The Point-to-Point Protocol (PPP) (RFC 1661), 1994.

311 Vgl. BADACH, A.; HOFFMANN, E.: Technik der IP-Netze, 2001, S. 439 f.; LLOYD, B.; SIMPSON, W.: PPP Authentication Protocols (RFC 1334), 1992; SIMPSON, W.: PPP Challenge Handshake Authentication Protocol (RFC 1994), 1996.

312 Vgl. ABOBA, B.: Extensible Authentication Protocol (EAP) (RFC 3748), 2004.

313 Vgl. MD5-Challenge in ABOBA, B.: Extensible Authentication Protocol (EAP) (RFC 3748), 2004.

314 Vgl. ABOBA, B.; SIMON, D.: PPP EAP TLS Authentication Protocol, 1999.

315 Vgl. FUNK, P.; BLAKE-WILSON, S.: EAP Tunneled TLS Authentication Protocol Version 1 (EAP-TTLSv1), 2006.

316 Vgl. JOSEFSSON, S. ET AL.: Protected Extensible Authentication Protocol (PEAP), 2001.

317 Vgl. CAM-WINGET, N. ET AL.: The Flexible Authentication via Secure Tunneling Extensible Authentication Protocol Method (EAP-FAST), 2007.

318 Vgl. ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 494 ff., SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 318 ff.

Zugriff auf eine Netzwerkstruktur, der über dezentrale Zugriffspunkte (z.B. Einwahlnetze oder drahtlose Netzwerke bzw. WLAN) erfolgt.

Da das RADIUS Protokoll keine Nachrichtenverschlüsselung einsetzt bzw. die übertragenen Authentifizierungsmerkmale symmetrisch verschlüsselt versendet und somit z.B. für Known-Plaintext Angriffe[319] anfällig ist, befindet sich dessen Nachfolger DIAMETER bereits in der Entwicklung.[320]

Um eine Authentifizierung direkt am Netzwerkzugang zu erzwingen, bevor der Benutzer jegliche Infrastruktur des Netzwerks nutzen kann, wurde von des Institute of Electrical and Electronics Engineers (IEEE) die Port-basierte Authentifizierung nach dem 802.1X-Standard spezifiziert. Nach 802.1X startet die Netzwerkkomponente (z.B. der Switch im LAN oder Access Point im WLAN) eine Authentifizierung bei einem zugewiesenen RADIUS-Server. Verläuft die Authentifizierung nicht erfolgreich, so wird der Port und somit der Zugang zum Netzwerk für den Benutzer nicht freigeschaltet.[321] Für die Kommunikation mit dem RADIUS Server verwendet 802.1X die bereits erläuterten EAP Protokolle.

Eine einheitliche Authentifizierung kann erfolgen, indem der RADIUS Server seinerseits Verzeichnisdienste oder ein Kerberos KDC als Authentifizierungssystem verwendet. Er dient damit als Vertreter (Proxy) des eigentlichen Authentifizierungssystems. Zusätzlich kann eine einheitliche Authentifizierung und Single Sign-On durch die Verwendung von Zertifikaten unterstützt werden. Hierfür können z.B. EAP-TLS eingesetzt und die Client-Zertifikate von einem Token bei der Anmeldung am Arbeitsplatz[322] für den Zugriff auf das Netzwerk verwendet werden. Netzwerke können hier auch entfernte Strukturen mittels gesichertem Zugriff über Virtual Private Networks (kurz: VPN) darstellen.[323]

Abbildung 3-9 illustriert den Einsatz von Client-Zertifikaten für ein Single Sign-On mittels Zertifikat, z.B. von einem Token des Benutzers.[324] Der RADIUS-Server prüft hierbei die Authentizität des Benutzers anhand dessen Zertifikat, dessen Gültigkeit durch die dem RADIUS-Server vertraute Zertifizierungsstelle gesichert wird. Somit bildet die PKI das eigentliche einheitliche Authentifizierungssystem und -verfahren.

---

[319] Vgl. „Abhören der Sitzung“ in Abschnitt 2.8.2.

[320] Vgl. ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 499.

[321] Vgl. IEEE: 802.1X Port-Based Network Access Control, 2004; ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 835 ff.

[322] Vgl. Abbildung 3-8.

[323] Vgl. BADACH, A.; HOFFMANN, E.: Technik der IP-Netze, 2001, S. 529 ff.

[324] Vgl. Abschnitt 2.5.2.

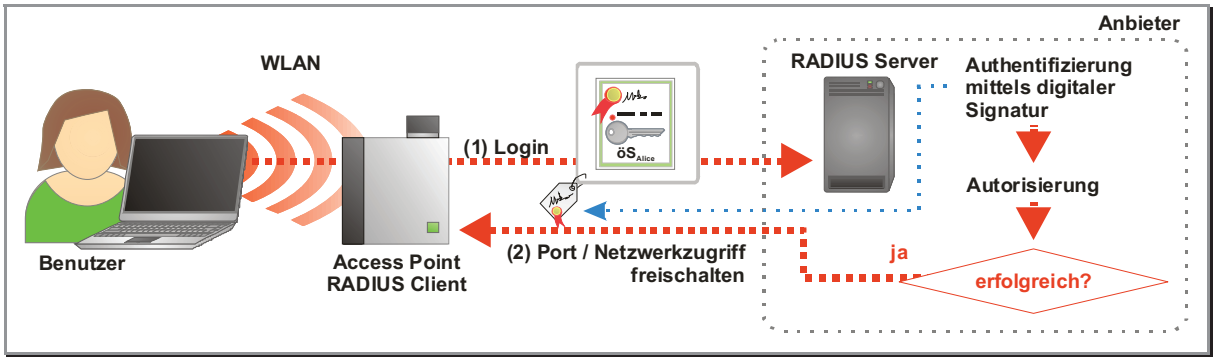

Abbildung 3-9: Verwendung eines RADIUS-Servers mit 802.1X

3.2.6 Web-basierte Authentifizierung

In der Version 1.1 wurden für das Hypertext Transfer Protocol (kurz: HTTP) Möglichkeiten für die Authentifizierung von Benutzern beim Zugriff auf Web-Seiten eingeführt.[325] Diese überlassen die Speicherung der Authentifizierungskonten jedoch individuell dem Web-Server und unterstützen somit keine eigenständige Vereinheitlichung der Authentifizierung. Eine Ausnahme stellt die Unterstützung von Simple and Protected GSSAPI Negotiation Mechanism (SPNEGO)[326] resp. Kerberos und NT LAN Manager (NTLM)[327] als Authentifizierungsverfahren in aktuellen Web-Browsern dar. Auch Web-Server unterstützen als Gegenstück die Verwendung von Kerberos und NTLM.[328] Es ermöglicht die Übermittlung der für die Anmeldung an Windows verwendeten Authentifizierungsmerkmale und somit ein Single Sign-On an Web-Seiten innerhalb einer Domäne. Allerdings muss dies explizit für Domänen im Web-Browser freigeschaltet werden, um Sicherheitsrisiken bei der Übertragung der Authentifizierungsmerkmale zu verhindern.

Das einzige einheitliche Authentifizierungsverfahren, das in allen Web-Browsern implementiert wird und ein Single Sign-On erlaubt, ist die Verwendung von Client-Zertifikaten mittels SSL / TLS.[329] Erfordert die vom Benutzer ausgewählte Web-Seite eine Client-seitige Authentifizierung

---

[325] Vgl. BADACH, A.; RIEGER, S.; SCHMAUCH, M.: Web-Technologien, 2003, S. 77 f.

[326] Vgl. GARMAN, J.: Kerberos. The Definitive Guide, 2003, S. 47, 146; BAIZE, E.; PINKAS, D.: The Simple and Protected GSS-API Negotiation Mechanism (SPNEGO) (RFC 2478), 1998.

[327] Vgl. Mozilla: Integrated Auth, 2005.

[328] Vgl. NTLM auth module for Apache/Unix, 2007; mod_auth_vas - Windows Integrated Authentication for Apache, 2007; SURANTI, S.; MUCKIN, M.: http-Based Cross-Platform Authentication via the Negotiate Protocol, 2002.

[329] Vgl. die Authentifizierung des Adressaten durch Verschlüsselung von Informationen anhand dessen öffentlichem Schlüssel in Abschnitt 2.6.1.

mittels SSL / TLS, so kann der Web-Browser automatisch ein Zertifikat aus seinem Speicher oder angeschlossenem Token[330] auswählen und verwenden.

HTTP wurde als zustandsloses Protokoll konzipiert. Um dennoch aufeinander folgende Anfragen einer eindeutigen Sitzung zuordnen zu können, wurde HTTP um die Unterstützung von Web-Transaktionen erweitert.[331] Diese Sitzungen bilden auch die Grundlage für eine einheitliche Authentifizierung im Web, da hier ebenfalls aufeinander folgende Anfragen ggf. auch an unterschiedliche Web-Seiten ohne erneute Authentifizierung erlaubt werden sollen. Um Web-Transaktionen über unterschiedliche Web-Anfragen und Web-Seiten hinweg zu ermöglichen, werden in der Regel Cookies verwendet. Abbildung 3-10 illustriert den Ablauf bei der Verwendung von Cookies für die Etablierung einer Sitzung mittels HTTP. Dabei setzt der Web-Server in (2) ein Cookie auf der Seite des Clients, das dieser in (3) erneut an den Server sendet, der so den Client zu der zugehörigen laufenden Sitzung zuordnen kann.[332]

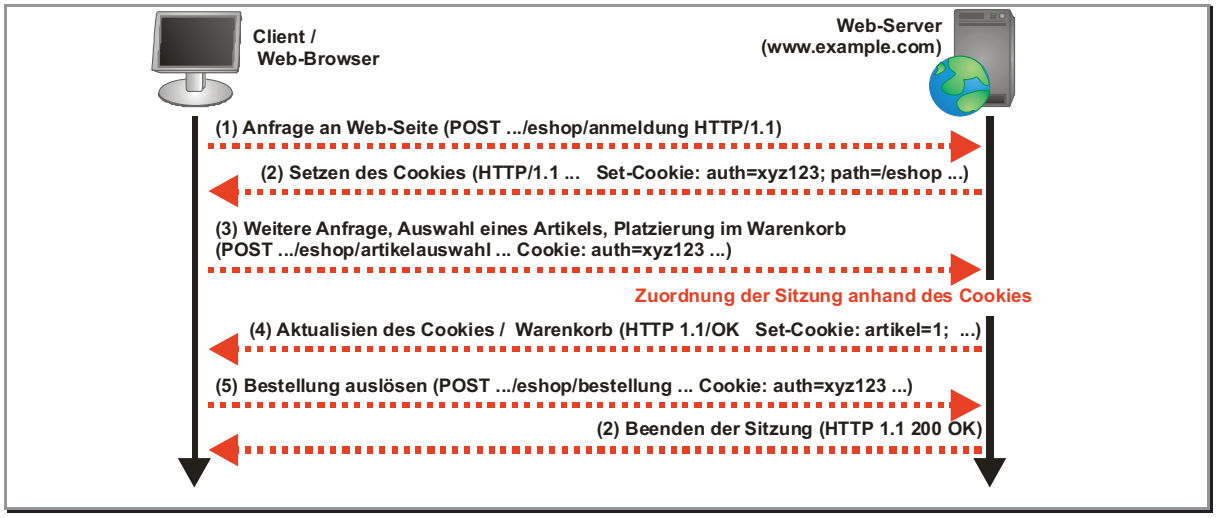

Abbildung 3-10: Verwendung von Cookies für die Realisierung von Web-Transaktionen nach BADACH ET AL.[333]

Für die Authentifizierung kann ein Cookie hierbei auch Authentifizierungsmerkmale wie Sitzungsschlüssel usw. mit begrenzter Laufzeit speichern.[334] Aus Sicherheitsgründen werden Cookies nur an die Domäne übertragen, die sie gesetzt haben. Für ein Single Sign-On an unterschiedlichen Web-Seiten müssen Zugriffe auf diese daher zunächst an einen zentralen Dienst, der das Cookie

---

[330] Vgl. den Einsatz von Zertifikaten auf aktiven Tokens in Abschnitt 2.5.2.

[331] Vgl. BADACH, A.; RIEGER, S.; SCHMAUCH, M.: Web-Technologien, 2003, S. 165 ff.

[332] Vgl. BADACH, A.; RIEGER, S.; SCHMAUCH, M.: Web-Technologien, 2003, S. 173 ff.

[333] Vgl. BADACH, A.; RIEGER, S.; SCHMAUCH, M.: Web-Technologien, 2003, S. 173.

[334] Vgl. WINDLEY, P. J.: Digital Identity, 2005, S. 51 f.

ausstellt, umgeleitet werden. Eine Möglichkeit hierfür sind Web-Proxy-Server auf der Seite der Clients.[335] Da diese jedoch für alle Clients, die die Web-Seite aufrufen, konfiguriert werden müssten, werden in der Regel Reverse Proxies / Caches[336] auf der Seite der Web-Server verwendet, die die Authentifizierung zu Beginn der Sitzung an einen zentralen Authentifizierungsdienst umleiten. Häufig werden diese zentralen Authentifizierungsdienste auch in Web-Portalen integriert, die u.a. den Zugang zu unterschiedlichen Web-Applikationen innerhalb einer Organisation anbieten. Software-Lösungen, die einen solchen Reverse Proxy für ein Single Sign-On realisieren, sind z.B. Sun Java System Access Manager oder Novell Access Manager.[337]

Ein Beispiel für eine zentrale Lösung für Web-basiertes Single Sign-On stellt Microsoft Passport dar, dessen Funktionsweise in Abbildung 3-11 gezeigt wird. Hierbei wird der Zugriff auf die Seite www.example.com (1) an den Passport-Server umgeleitet (2a und 2b). Dieser setzt schließlich ein Cookie (6), das bei zukünftigen Weiterleitungen an den Passport-Server übermittelt wird, und so ein Single Sign-On ermöglicht.[338]

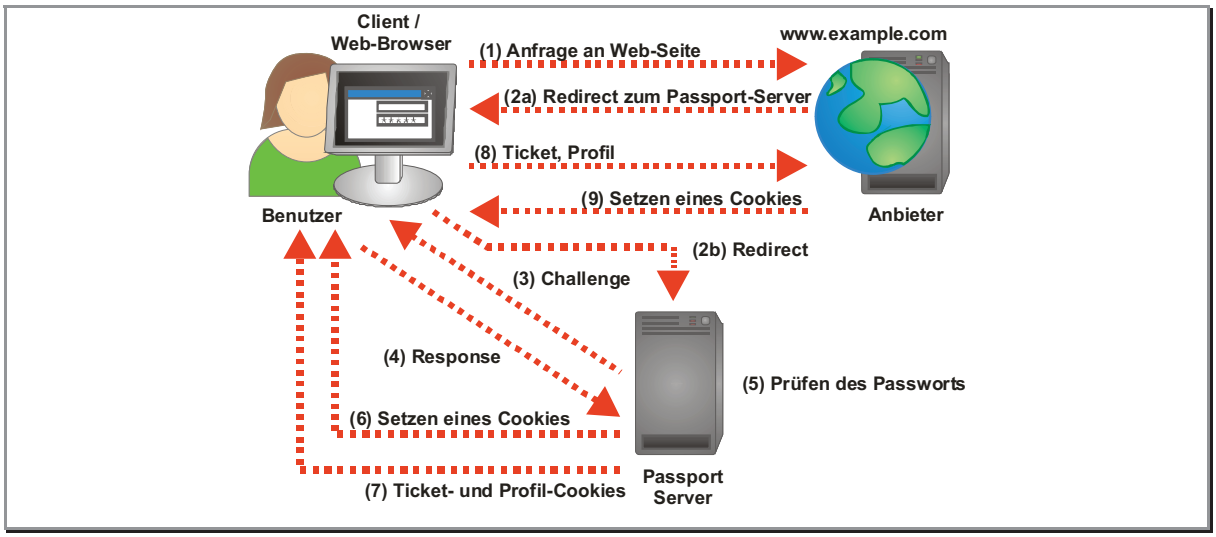

Abbildung 3-11: Microsoft Passport als Beispiel für einen zentralen Single Sign-On Dienst nach ECKERT[339]

Aufgrund der zentralen Lösung bzw. Speicherung der Authentifizierungsmerkmale weist der Passport Dienst jedoch Sicherheitsrisiken auf.[340] Nicht zuletzt aufgrund dieser Risiken werden aktuell

[335] Vgl. BADACH, A.; RIEGER, S.; SCHMAUCH, M.: Web-Technologien, 2003, S. 247 f.
[336] Vgl. BADACH, A.; RIEGER, S.; SCHMAUCH, M.: Web-Technologien, 2003, S. 228 f.
[337] Vgl. Sun Java Access Manager, 2007; Novell Access Manager, 2007.
[338] Vgl. ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 514 ff.
[339] Nach ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 518.
[340] Vgl. ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 520 ff.

dezentrale Authentifizierungssysteme im Web bevorzugt, sofern eine organisationsübergreifende Authentifizierung erzielt werden soll. Diese basieren auf Federations, die im folgenden Abschnitt erläutert werden. Andere Beispiele für zentrale Lösungen sind der Central Authentication Service (CAS)[341] der Yale University oder das ursprüngliche Liberty 1.0 Framework des Liberty Alliance Projects.[342] Zusätzlich fallen alle Web-Anwendungen und -Portale, die auf zentrale Identitätsquellen und Authentifizierungssysteme, wie z.B. Verzeichnisdienste oder Kerberos, zurückgreifen, in die Kategorie der zentralen Lösungen.

3.2.7 Federation-basierte Authentifizierung

Zentrale Authentifizierungssysteme, wie sie in den vorherigen Abschnitten vorgestellt wurden, gelangen bei der Etablierung organisationsübergreifender Vertrauensstellungen an ihre Grenzen. In der Regel endet die einheitliche Authentifizierung bzw. das erzielte Single Sign-On an der Grenze der Organisation.[343] Kooperationen für zentralisierte Authentifizierungssysteme zwischen unterschiedlichen Organisationen skalieren mit zunehmender Anzahl der Partner schlecht, da die Beziehungen zwischen Identitäten in der Realität eine eher Web-ähnliche (vermaschte) Struktur aufweisen, während zentrale Systeme ein strikt hierarchisches Verzeichnis-orientiertes Modell abbilden.[344] Zentrale Systeme erfordern zudem eine einheitliche Spezifikation der Identitäten wie Benutzernamen, auf die sich alle beteiligten Organisationen verständigen. Änderungen an diesen Spezifikationen oder auch einfache Modifikationen der Identitäten (z.B. Hinzufügen, Löschen) haben Auswirkungen auf alle Beteiligten. Zusätzlich ist es nicht praktikabel, dass beispielsweise ein Web-Shop alle Identitäten in das Authentifizierungssystem einer Universität kopiert oder umgekehrt, um für eine Teilmenge der Benutzer eine einheitliche zentrale Authentifizierung zu ermöglichen.[345] Dezentrale Authentifizierungssysteme und -verfahren lösen diese Nachteile im Vergleich zu den bisherigen vorgestellten Lösungen. Sie passen sich zusätzlich den Anforderungen heterogener IT-Strukturen, gemäß Abschnitt 2.1.10, an, indem sie verteilte eigenständige Authentifizierungssysteme unterschiedlicher Anwendungen und Plattformen verknüpfen. Vorteile der dezentralen Architektur, wie sie auch das Internet abbildet, sind:[346]

---

[341] Vgl. JA-SIG Central Authentication Service (CAS), 2007.

[342] Vgl. Liberty: Specifications, 2007.

[343] Vgl. WINDLEY, P. J.: Digital Identity, 2005, S. 118.

[344] Vgl. Veranschaulichung anhand der Kreditkarten Industrie in WINDLEY, P. J.: Digital Identity, 2005, S. 119, 121 f.

[345] Vgl. WINDLEY, P. J.: Digital Identity, 2005, S. 121.

[346] Vgl. WINDLEY, P. J.: Digital Identity, 2005, S. 120.

- Angreifer können die gesamte Struktur nicht durch den Angriff auf ein einzelnes beteiligtes System lahmlegen.
- Dezentrale Strukturen sind weniger anfällig gegen politischen oder kommerziellen Missbrauch der Identitäten (Datenschutz) als zentrale Identitäts-Datenbanken.
- Im Vergleich zu homogenen Systemen, bei denen der Ausfall der zentralen Komponente den Ausfall der gesamten Struktur zur Folge hat, sind dezentrale Architekturen weniger fehleranfällig.

Die Verknüpfung unterschiedlicher Authentifizierungssysteme und -verfahren in einer einheitlichen dezentralen Architektur wird in Bezug auf die Identitäten der Benutzer als Federated Identity bezeichnet. Aufgrund der föderierten Identitäten bezeichnet man die resultierenden Strukturen auch kurz als Federations.[347] Innerhalb einer Federation sind beteiligte Organisationen und deren Authentifizierungssysteme eigenständig.

Obwohl eine Federation für die Benutzer durch das gebotene Single Sign-On in jedem Fall erwünscht ist, können Organisationen als eigentliche Betreiber der Federation unterschiedliche Interessen bei dem Beitritt verfolgen. WINDLEY stellt drei Muster für die Bildung von Federations vor:[348]

- „ad-hoc federation“: bilaterale Beziehungen und Vertrauensstellungen zwischen Organisationen, die ihre Identitäten föderieren möchten;
- „hub-and-spoke federation“: Insellösungen für Federations um große Organisationen;
- „identity federation network“: Etablierung einer unabhängigen, allen Beteiligten gehörenden Institution (z.B. einem Clearinghouse bzw. einer eigenständigen Organisation).

Obwohl diese Muster unabhängig voneinander sind, werden sie bei der Bildung von Federations in der Regel in der genannten Reihenfolge durchlaufen.[349] WINDLEY erläutert dies am Beispiel der Föderation der Kreditkarten-Industrie. Hier wurde für die BankAmericard zunächst auf eine spontane Kooperation („ad-hoc“) zwischen der Bank of America sowie beteiligten Händlern gesetzt, die später von der Bank of America zentral verwaltet („hub-and-spoke“) und nach Unstimmigkeiten

[347] Vgl. WINDLEY, P. J.: Digital Identity, 2005, S. 118.
[348] Vgl. WINDLEY, P. J.: Digital Identity, 2005, S. 125 ff.
[349] Vgl. WINDLEY, P. J.: Digital Identity, 2005, S. 125.

der beteiligten Partner zur Gründung von VISA als unabhängige Organisation bzw. Kreditkarten-Föderation führte.[350]

Eine dezentrale, auf Federations basierende Authentifizierung erfordert Standards, z.B. für den Austausch von temporären Authentifizierungsmerkmalen (auch Tickets, Tokens oder Assertions genannt) oder die verwendeten Authentifizierungsverfahren. Derzeit existieren hierfür die WS-* Standards[351] der Firmen Microsoft und IBM, der Security Assertion Markup Language (SAML) Standard der Organization for the Advancement of Structured Information Standards (OASIS)[352] sowie das Liberty Framework des Liberty Alliance Project.[353] Hervorzuheben ist hierbei, dass alle Standards in der jeweils aktuellen Version mit dem SAML-Standard der OASIS in der Version 2.0, die auch für andere XML-basierte Standards wie SOAP oder WSDL im Web-Service-Umfeld verantwortlich ist, integriert werden können. Somit wird für die folgenden Betrachtungen der SAML 2.0 Standard als Standard verwendet. Beispiel für die Interoperabilität sind die Active Directory Federation Services (ADFS), die durch die Verwendung der WS-* Standards neben Kerberos Tickets auch SAML Assertions akzeptieren und ab Microsoft Windows 2003 Server R2 von Microsoft kostenfrei ausgeliefert werden.

SAML wird auch von dem Shibboleth Projekt[354] des Internet2 für Federations im wissenschaftlichen Bereich verwendet.[355] Shibboleth resp. SAML bildet damit den wichtigsten Federation Ansatz für aktuelle e-Science-Strukturen. Abbildung 3-12 illustriert die Verwendung von Shibboleth und SAML für die Bildung von Federations. In der Version 2.0 unterstützt Shibboleth SAML 2.0 und somit die Integration mit anderen Federation-basierten Lösungen wie WS-Federation[356] (des WS-* Standards) von Microsoft und IBM oder Liberty Phase 3[357] des Liberty Alliance Project.

---

[350] Vgl. WINDLEY, P. J.: Digital Identity, 2005, S. 128.

[351] Vgl. IBM Web Services Security, 2007.

[352] Vgl. OASIS Security Services (SAML), 2007.

[353] Vgl. WINDLEY, P. J.: Digital Identity, 2005, S. 122 ff. und ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 528.

[354] Vgl. Internet 2 Shibboleth, 2007.

[355] Vgl. auch GridShib: Integrating federated authorization infrastructure with Grid technology, 2007.

[356] Vgl. IBM Web Services Security, 2007.

[357] Vgl. Liberty: Specifications, 2007.

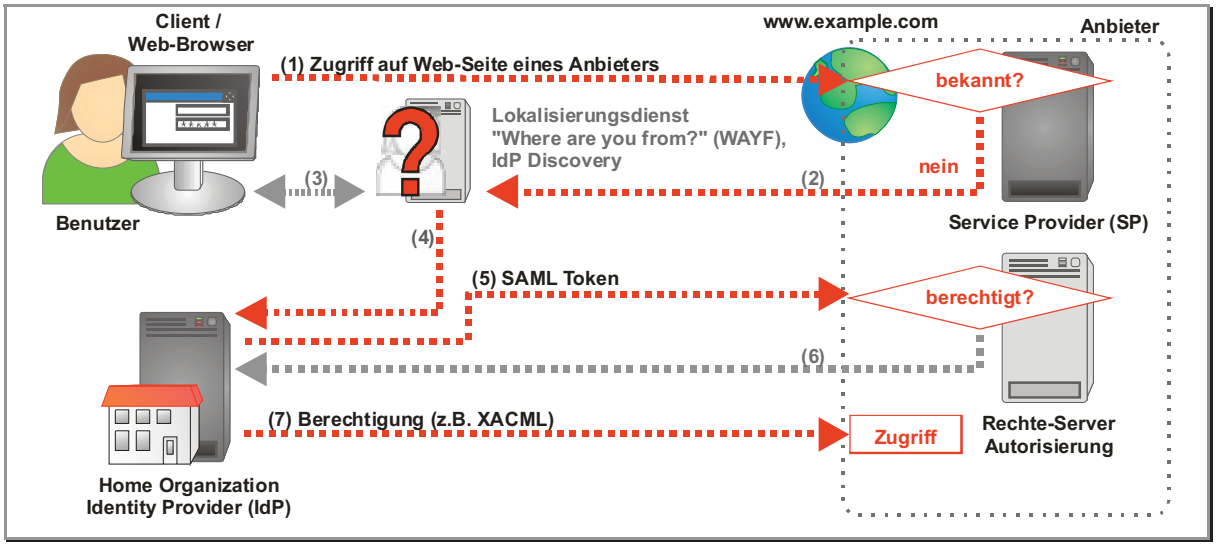

Abbildung 3-12: Verwendung von Shibboleth für Web-basiertes Single Sign-On[358]

In der Abbildung 3-12 möchte der Benutzer eine Web-Anwendung eines externen Anbieters verwenden. Dieser stellt einen Service Provider (SP) zur Verfügung, der den SAML-Standard unterstützt. Verfügt der Benutzer bereits über ein SAML Token, so wird dies als Cookie[359] übermittelt. Sofern das Cookie vom SP akzeptiert wird (Akzeptanz der im Cookie enthaltenen digitalen Signatur vgl. Abschnitt 2.6.2), erfolgt keine erneute Authentifizierung.

Sofern der Benutzer beim SP nicht lokal bekannt ist und kein SAML Token übermittelt hat, wird der für ihn zuständige Identity Provider (IdP) ermittelt. Häufig wird hierfür ein Portal („Where are you from?“, kurz: WAYF-Server) verwendet, auf dem der Benutzer seinen IdP bzw. seine Heimatorganisation (Home Organization) auswählt. Dies ist optional und daher in Abbildung 3-12 als Schritt (3) grau dargestellt.

Der zugehörige IdP wickelt die eigentliche Authentifizierung des Benutzers ab. Hierfür können unterschiedliche Authentifizierungsverfahren verwendet werden. Dem SP übermittelt er jedoch keine persönlichen Daten des Benutzers wie z.B. Authentifizierungsmerkmale, sondern erzeugt ein SAML Token bzw. eine Assertion, die als temporäres Merkmal an den SP übertragen und als Cookie im Web-Browser des Benutzers gespeichert wird. Die Authentifizierung erfolgt somit dezentral beim IdP der Heimatorganisation des Benutzers.

Optional verwenden einige Federations zusätzlich Autorisierungskomponenten, die die Berechtigung des Benutzers in Schritt (6) und (7) prüfen.[360] Für die entsprechende Erweiterung des SAML

---

[358] Nach AAR: Wie funktioniert Shibboleth?, 2006, S. 9.

[359] Wie in Abschnitt 3.2.6 für die Web-basierte Authentifizierung beschrieben.

[360] Vgl. AAR: Wie funktioniert Shibboleth?, 2006, S. 14 ff.

Tokens kann der eXtensible Access Control Markup Language (XACML) Standard verwendet werden.[361] Das SAML Token kann der Benutzer innerhalb dessen Gültigkeitszeitraums für den Zugriff auf weitere SP innerhalb der Federation nutzen, ohne dass eine erneute Authentifizierung erforderlich wird.

Basis für die Authentifizierung am IdP stellt ein existierendes Identity Management[362] der Heimatorganisation dar.[363]

Mit der Unterstützung von SAML 2.0 in Shibboleth 2.0 sind weitere Funktionen realisierbar. Unter anderem wird zugunsten eines IdP Discovery auf die WAYF Funktion verzichtet. IdP und SP können durch Delegation auch nach dem WS-Federation Standard operieren. Durch ShARPE und Autograph[364] wird dem Benutzer des Weiteren ermöglicht selbst zu bestimmen, welche Teile seiner Identität er an den jeweiligen SP übermitteln möchte, womit der Datenschutz verbessert wird. Benutzer übergeben die Informationen zu ihrer Identität hierbei in Form von virtuellen Visitenkarten, wie sie auch bei Microsofts InfoCards bzw. CardSpace[365] als Nachfolger des Passport Diensts zum Einsatz kommen. Auch sind Anwendungen außerhalb des Webs im Fokus der Entwicklung.

Microsofts InfoCards sind Bestandteil des geplanten Identity Metasystem[366], das unterschiedliche Technologien wie Meta-Directory, Digital Rights Management (DRM) und Federations bündelt. Bei dem Identity Metasystem besitzt ein Benutzer bzw. eine Identität unterschiedliche Claims, die sie eigenständig verwalten und für die Authentifizierung verwenden kann.[367] Abbildung 3-13 zeigt die Architektur des Identity Metasystem. Relying Parties haben hierbei die gleiche Funktion wie die bereits genannten Service Provider und zeigen daher, dass beim skizzierten System unterschiedliche Verfahren für IdP (über unterschiedliche Module am Security Token Service) und SP (über unterschiedliche Module am WS-Security Provider) verwendet werden können.

---

[361] OASIS: XACML, 2007.

[362] Als Realisierung eines einheitlichen Authentifizierungssystems für den IdP z.B. anhand eines Meta- oder Virtual Directory, vgl. Abschnitt 3.2.2.

[363] Vgl. AAR: Wie funktioniert Shibboleth?, 2006, S. 7; WINDLEY, P. J.: Digital Identity, 2005, S. 104 f.

[364] Vgl. DFN AAIWiki: ShARPE, 2007.

[365] Vgl. Microsoft Windows CardSpace, 2007.

[366] Vgl. Microsoft: Microsoft's Vision for an Identity Metasystem, 2005.

[367] Vgl. CAMERON, K.: The Laws of Identity, 2005.

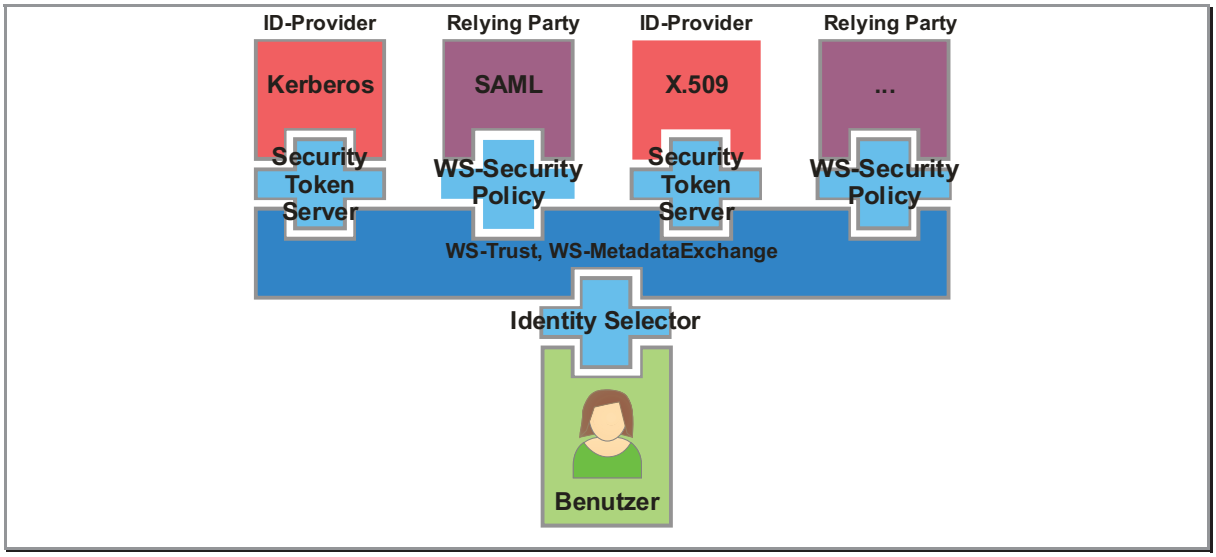

Abbildung 3-13: Architektur des Identity Metasystems von Microsoft nach CAMERON[368]

Für die Abbildung des in Abschnitt 3.2.2 genannten Lebenszyklus des Identity Managements existieren neben SAML weitere XML-Standards für die Realisierung der einzelnen Prozesse. Insbesondere sind hier die eXtensible Access Control Markup Language (XACML) für die einheitliche Beschreibung der Autorisierung und deren Verwaltung sowie die Service Provisioning Markup Language (SPML)[369] für das Provisioning der Identitäten zu nennen.[370]

3.2.8 Modulare Authentifizierungs-Clients und Proxies

Die bisher im Abschnitt 3.2 vorgestellten Lösungen erzielen die Vereinheitlichung von Authentifizierungsverfahren und -systemen aufseiten der Organisationen bzw. Servern. Eine Vereinheitlichung ist jedoch ebenfalls durch eine Modifikation der Clients möglich. Clients werden hierbei auf die Verwendung unterschiedlicher Authentifizierungsverfahren und -systeme umgestellt. Verfahren und Systeme, die im Anschluss nicht mehr benötigt werden, werden reduziert, womit die Authentifizierung insgesamt vereinheitlicht wird.

Insbesondere für eine Migration kann es sinnvoll sein, temporär die Diversifikation der verwendeten Verfahren und Systeme am Client hinzunehmen. Hierdurch können Benutzer nach wie vor die alten Verfahren und Systeme verwenden, während zusätzlich neue zur Verfügung gestellt und die

[368] Nach Microsoft: Microsoft's Vision for an Identity Metasystem, 2005.
[369] OASIS: SPML, 2007.
[370] Vgl. WINDLEY, P. J.: Digital Identity, 2005, S. 98 ff.

alten im Anschluss deaktiviert werden. Dies wird im Rahmen existierender Migrations-Strategien auch als „weiche Migration“ bezeichnet.[371]

Für die Unterstützung unterschiedlicher Authentifizierungsverfahren und -systeme durch die Clients existieren unterschiedliche Frameworks. Ein Beispiel sind die Pluggable Authentication Modules (kurz: PAM), die unter Unix zur Verfügung stehen.[372] PAM übernimmt die Ermittlung der Benutzernamen (account), die verwendbaren Authentifizierungsverfahren (auth), erlaubte Verfahren für die Passwort-Änderung (password) sowie die Verwaltung der Sitzung bzw. Umgebung nach erfolgreicher Anmeldung (session). In jedem dieser Bereiche können mehrere Methoden angegeben und dadurch unterschiedliche Authentifizierungsverfahren und -systeme nacheinander geprüft werden. Eine erfolgreiche Authentifizierung kann entweder die erfolgreiche Prüfung aller dieser Methoden erfordern oder eine einzige. Die Abfolge der verwendeten Authentifizierungssysteme lässt sich in den Bereichen für unterschiedliche Anwendungen (z.B. FTP, SSH) separat definieren. Dadurch wird eine weiche Migration resp. Vereinheitlichung der Authentifizierung, wie eingangs erläutert, vereinfacht. PAM ist Hauptbestandteil der X/Open „Single Sign-On“-Service Spezifikation (kurz: XSSO), die eine Client-seitige Lösung für Single Sign-On in Unix-Betriebssystemen vorsieht.[373] Die Abbildung 3-14 zeigt die Architektur von PAM.

Unter Windows wird die Authentifizierung Client-seitig von der Local Security Authority (kurz: LSA) übernommen.[374] Die Anmeldung des Benutzers erfolgt mittels Graphical Identification and Authentication (kurz: GINA), die unterschiedliche Security Support Provider (kurz: SSP) für die Verwendung verschiedener Authentifizierungsverfahren unterstützt.[375] Diese sind jedoch primär für Verfahren in homogenen Windows-Umgebungen, z.B. Kerberos für die Authentifizierung gegenüber Active Directory, aber nicht ohne zusätzliche Konfiguration für andere Verfahren (wie Kerberos-Implementierungen) vorgesehen. Verschiedene Dritthersteller nutzen die Schnittstelle, um eigene SSP für spezielle Authentifizierungsanforderungen zu realisieren.

---

[371] Vgl. „chicken little“ Strategie in ERDLE, C.: Legacy Migrationsstrategien, 2005.

[372] Vgl. SAMAR, V.; CHARLIE, L.: Making Login Services Independent of Authentication Technologies (PAM), 1996.

[373] Vgl. X/Open Single Sign-on Service (XSSO) - Pluggable Authentication Modules, 1997.

[374] Vgl. MICHELA, F.; PALME, M.: Active Directory, 1999, S. 109.

[375] Vgl. SCHMIDT, J.: Windows 2000 Security. Kryptographie, Kerberos, Authentifizierung, 2001, S. 286.

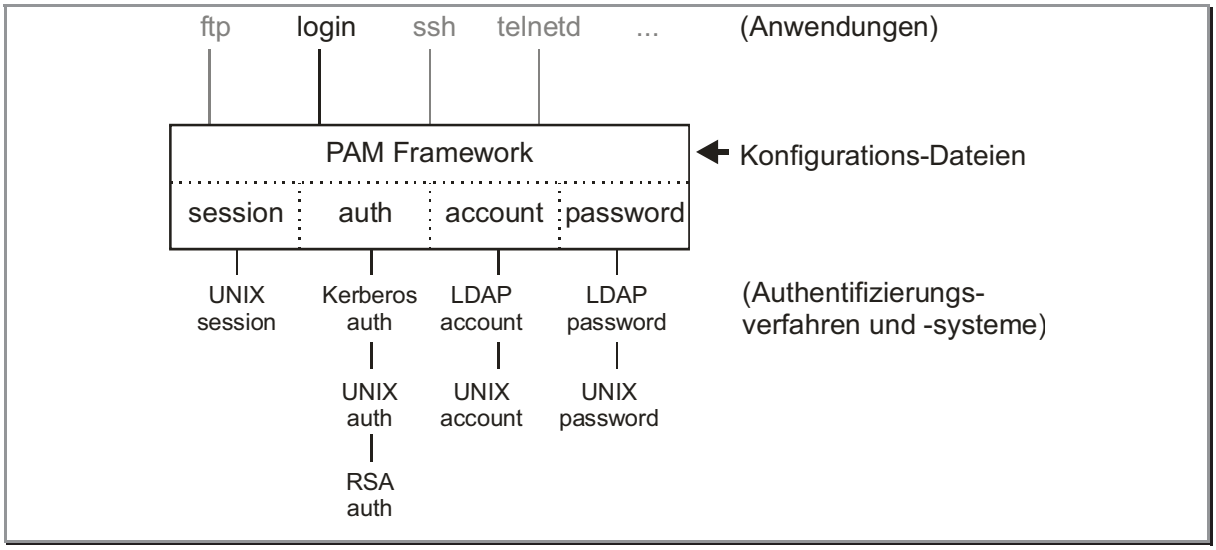

Abbildung 3-14: Verwendung von PAM für unterschiedliche Authentifizierungsverfahren und -systeme[376]

Eine Möglichkeit, die über die Schnittstelle eine PAM Funktionalität für Windows nachbildet, ist die frei verfügbare pGINA-Implementierung, die mehrere Authentifizierungsverfahren und -systeme verwenden kann.[377] pGINA stellt als Alternative zur oben genannten originären GINA von Microsoft einen Authentifizierungs-Proxy auf der Seite des Clients dar. Sie erlaubt beispielsweise eine Authentifizierung alternativ an einem RADIUS-Server, einer Datenbank, einem OpenLDAP-Server zusätzlich zur regulären Authentifizierung am Microsoft Active Directory bzw. lokalen Rechner. Neben weiteren Authentifizierungssystemen unterstützt pGINA dabei auch die Funktion, das Passwort nach erfolgreicher Authentifizierung gegenüber einem alternativen System direkt in das Active Directory zu übernehmen. Sie ermöglicht somit die Vereinheitlichung von Authentifizierungsverfahren und -systemen auf der Seite des Clients. pGINA ermöglicht durch die Verwendung von PAM als Modul die direkte Anmeldung (mittels PAM) in einer Unix-Umgebung an einem Windows Client.[378] Umgekehrt existieren auch Erweiterungen für PAM unter Unix für die Authentifizierung gegenüber Active Directory.[379]

Für die Implementierung von Diensten auf Server-Seite existieren gleichermaßen Frameworks, die unterschiedliche Authentifizierungsverfahren unter einer einheitlichen Schnittstelle zur Verfügung

[376] Nach SAMAR, V.; CHARLIE, L.: Making Login Services Independent of Authentication Technologies (PAM), 1996, S. 5.

[377] Vgl. pGINA, 2007.

[378] Vgl. pGINA PAM, 2007.

[379] Vgl. pam-krb5, 2007; pam_ldap, 2007.

stellen. Beispiele sind der Simple Authentication and Security Layer (kurz: SASL)[380], sowie das Generic Security Services Application Programming Interface (GSSAPI).[381] Für Java wird eine ähnliche Schnittstelle durch den Java Authentication and Authorization Service (kurz: JAAS) realisiert.[382] Auf diese Weise lässt sich die Verwendung unterschiedlicher Authentifizierungsverfahren in Authentifizierungssystemen durch die Verwendung eines der genannten Frameworks vereinheitlichen.

3.2.9 Passwort-Speicher und Authentifizierungsautomatismen

Um den Aufwand durch die Diversität von Authentifizierungsmerkmalen, die auf Kenntnis[383] basieren zu mindern, schreiben sich gemäß einer Studie des Fraunhofer-Institut für Sichere Informations-Technologie 50% der Benutzer allgemein ihre Passwörter auf.[384] Die damit verbundenen Risiken wurden in Abschnitt 2.8.1 erläutert. Sie werden durch spezielle Programme minimiert, die als sicherer Passwort-Speicher fungieren und mehrere Passwörter verschlüsselt durch ein einziges Master-Passwort verwalten. Nur nach erfolgreicher Eingabe des Master-Passworts werden die im Speicher enthaltenen Passwörter dem Benutzer angezeigt. Dies entspricht bedingt einer Vereinheitlichung der Authentifizierungsmerkmale seitens der Benutzer, da sich dieser nur das Master-Passwort merken muss. Allerdings benötigt jede Anwendung nach wie vor ein separates Passwort. Passwort-Speicher bedeuten neben der Vereinfachung allerdings ein zusätzliches Risiko. Erhält ein Dritter Zugriff auf das Master-Passwort oder umgeht er die Sicherheitsmechanismen des Passwort-Speichers, so sind alle Passwörter kompromittiert. Dies kann auch während einer regulären Sitzung erfolgen, sobald der Benutzer den Speicher geöffnet hat und die Passwörter für einen gewissen Zeitraum entschlüsselt angezeigt werden. Daher sind hohe Sicherheitsanforderungen an einen Passwort-Speicher zu stellen. Ein Beispiel für einen Passwort-Speicher bildet der von SCHNEIER empfohlene Password Safe, der die Passwörter nach dem symmetrischen Blowfish Verfahren verschlüsselt.[385] Password Safe stellt eine reguläre Anwendung dar, die einen Rechner erfordert und somit nur bedingt mobil einsetzbar ist.

---

[380] Vgl. CHESWICK, W. R.; BELLOWIN, S. M., RUBIN, A. D.: Firewalls und Sicherheit im Internet. 2. Aufl., 2004, S. 191.

[381] Vgl. CHESWICK, W. R.; BELLOWIN, S. M., RUBIN, A. D.: Firewalls und Sicherheit im Internet. 2. Aufl., 2004, S. 391 f.

[382] Vgl. Sun JAAS, 2007.

[383] Vgl. z.B. Passwörter in Abschnitt 2.5.1.

[384] Vgl. Password Sitter, 2007.

[385] Vgl. Password Safe, 2007.

Neben der Adaption des Programms für mobile Endgeräte[386] existiert im Passwort Sitter eine web-basierte Alternative des Fraunhofer Instituts für Sichere Informations-Technologie (SIT).[387] Der Password Sitter erstellt dabei online auf einer Web-Seite oder off-line auf dem Arbeitsplatz-Rechner des Benutzers zufällige Passwörter für unterschiedliche Dienste nach flexiblen Kriterien anhand des Master-Passworts. Die erzeugten Kennwörter werden nicht gespeichert, sondern bei jedem Zugriff anhand des Master-Passworts, das für die Anmeldung am Password Sitter erforderlich ist, neu berechnet. Durch die Implementierung in Java ist neben der web-basierten Lösung eine Plattform-übergreifende Verwendung auf lokalen Endgeräten möglich.

Häufig verwenden Benutzer die Funktion der Passwort-Speicherung direkt in der Applikation. Aktuelle Browser, wie z.B. Mozilla Firefox, erlauben direkt nach der Eingabe eines Passworts dessen Speicherung, um das entsprechende Anmelde-Formular auf der Web-Seite beim nächsten Zugriff automatisch zu füllen.[388] Auch E-Mail-Anwendungen und andere Netzwerk-Dienste ermöglichen die direkte Speicherung des Passworts. Während die Funktionalität aus Sicht des Benutzers eine Vereinheitlichung des Authentifizierungsmerkmals erlaubt, ist die Sicherheit dieser Funktionalität aus Sicht der Betreiber stark eingeschränkt. Die Passwörter müssen für die Verwendung innerhalb der Applikation symmetrisch und somit reversibel verschlüsselt gespeichert werden. Ähnlich wie beim Password Safe liegen sie in dem Moment, in dem der Anwender die Applikation verwendet, für kurze Zeit im Klartext, im Arbeitsspeicher des Rechners vor. Wird das Passwort von dem Benutzer auch für andere Applikationen verwendet, so bedeutet die unbemerkte Kompromittierung durch das Abgreifen des gespeicherten Passworts ein noch größeres Sicherheitsrisiko. Bei einer Passwort-Änderung müssen zusätzlich alle gespeicherten Passwörter geändert werden. Um die Sicherheit zu erhöhen, sollten entsprechende Funktionalitäten daher vom Betreiber gesperrt oder nur für weniger sicherheitsrelevante Applikationen erlaubt werden.

Die bisher vorgestellten Passwort-Speicher ermöglichen ausschließlich die Vereinheitlichung von Authentifizierungsmerkmalen. Eine Vereinheitlichung der Authentifizierungsverfahren bzw. ein Single Sign-On[389] sind daher (abgesehen von der Speicherung direkt in der Applikation mit den genannten Nachteilen) nicht möglich. Verschiedene Hersteller haben daher die Funktionalität ihrer Passwort-Speicher um die Automatisierung von Authentifizierungsvorgängen erweitert. Beispiele stellen die Client Security Solution (kurz: CSS), die Lenovo Notebooks beiliegt, oder ähnliche

[386] Vgl. PocketPC Version Password Safe, 2007.
[387] Vgl. Password Sitter, 2007.
[388] Vgl. Mozilla Password Manager, 2007.
[389] Vgl. Abschnitt 2.1.12.

Verfahren anderer Notebook-Hersteller wie Dell dar.[390] Diese Verfahren basieren auf der Verwendung des Trusted Platform Module (kurz: TPM) als Bestandteil der Spezifikation der TCG (Trusted Computing Group).[391] Dieser Chip übernimmt die Verschlüsselung der Passwörter und dient als physikalischer Schutz ähnlich einem fest implementierten Token.[392] Neben Passwörtern können TPM zukünftig digitale Schlüssel für die Verwendung digitaler Medien aufnehmen. Dies wird als Digital Rights Management (DRM) bezeichnet.[393]

Die CSS verwenden hierfür eine Applikation, die das Öffnen neuer Anmelde-Dialoge sowie Login-Fenster erkennt und dort automatisch Benutzername und Passwort aufseiten des Clients einträgt. Erforderliche Passwörter werden zuvor aus dem TPM nach dessen Aktivierung durch den Benutzer abgerufen. Risiken können hierbei entstehen, wenn es einem Angreifer gelingt, den Anmelde-Dialog einer Anwendung vorzutäuschen und so automatisiert das Passwort abzugreifen. Zusätzlich befindet sich das Passwort auch während der Eingabe im Klartext im Arbeitsspeicher. Auf die entsprechende Absicherung der Automatisierung der Authentifizierung haben sich spezielle Single Sign-On Clients (kurz: SSO-Clients) fokussiert.

Ein Beispiel hierfür stellt Novell Secure Login dar. Secure Login speichert Passwörter unterschiedlicher Applikationen verschlüsselt in einem zentralen Verzeichnisdienst. Für die Authentifizierung wird das Authentifizierungsmerkmal verschlüsselt an Secure Login übertragen und nach dem bei CSS skizzierten Verfahren in den Anmelde-Dialog eingegeben. Die Abbildung 3-15 zeigt die Verwendung von Novell SecureLogin.[394] Dabei meldet sich der Benutzer zunächst am lokalen SSO-Client an (1), der die Identität gegenüber einem zentralen Verzeichnisdienst überprüft. Startet der Benutzer daraufhin Anwendung A, die eine Authentifizierung erfordert, so kann der SSO-Client das in (3) für die Anwendung erhaltene Passwort in (5) an diese übermitteln und so die Authentifizierung im Hintergrund ohne eine Eingabe des Benutzers realisieren.

Ähnliche SSO-Clients werden von MetaPass oder dem Secure Access Manager von Evidian realisiert.[395]

---

[390] Vgl. Dell IdentiPHI Enterprise Security Solution, 2007; Lenovo ThinkVantage Client Security Solution, 2007.

[391] Vgl. Trusted Computing Group (TCG), 2007.

[392] Vgl. Abschnitt 2.5.2.

[393] Vgl. SCHUMANN, M. ET AL.: Digital Rights Management - Technologien, in Das Wirtschaftsstudium 5, 2004, S. 666 ff.

[394] Vgl. Novell SecureLogin, 2007.

[395] Vgl. MetaPass, 2007; Evidian AccessMaster, 2007.

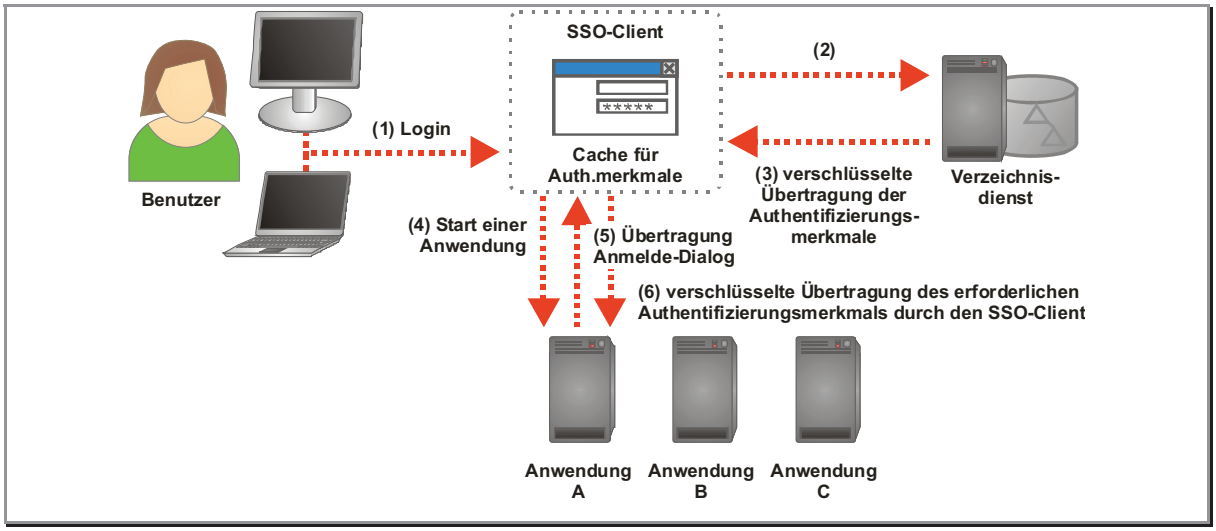

Abbildung 3-15: Funktion von SSO-Clients am Beispiel von SecureLogin[396]

3.3 Probleme bestehender Lösungen für eine einheitliche Authentifizierung

Die im Abschnitt 3.2 vorgestellten bestehenden Verfahren für einheitliche Authentifizierung lassen sich nur bedingt in heterogenen IT-Strukturen einsetzen. Zum einen sind einige der Verfahren auf konkrete Plattformen (z.B. nur Windows- oder nur Unix-Umgebungen) beschränkt, andere lassen sich nicht für alle Anwendungen (z.B. nur im World Wide Web, vgl. Abschnitt 3.2.6 und 3.2.7) verwenden. Die folgenden Abschnitte erläutern die Nachteile bestehender Verfahren und liefern somit die Ausgangslage (Ist-Zustand) für die anschließend im Kapitel 4 definierten Anforderungen an die Auswahl und Implementierung geeigneter Verfahren für eine einheitliche Authentifizierung in heterogenen IT-Strukturen.

3.3.1 Interoperabilität, Flexibilität und Skalierbarkeit

Einige der in Abschnitt 3.2 genannten Verfahren lassen sich nicht in heterogenen IT-Strukturen einsetzen, da sie nicht von allen Ressourcen und Plattformen unterstützt werden. Beispiel ist Kerberos, das eine Anpassung der Applikationen erfordert.[397] Während LDAP-basierte Verzeichnisdienste auf Kerberos als Authentifizierungssystem zurückgreifen können, existiert darüber hinaus umgekehrt keine Erweiterung von Kerberos für die Verwendung eines nachgelagerten Verzeichnisdienstes. Kerberos und Verzeichnisdienste sind somit nicht in beide Richtungen interoperabel.

---

[396] Nach Novell SecureLogin Technical Whitepaper, 2007, S. 11.

[397] Vgl. um Kerberos erweiterte Anwendungen am Ende des Abschnitts 3.2.3.

Auch für die Verwendung von Verzeichnisdiensten ist die Anpassung der Applikationen erforderlich. Eine Lösung stellen Frameworks, wie sie in Abschnitt 3.2.8 vorgestellt wurden, dar, die von Applikationen zur Unterstützung unterschiedlicher Authentifizierungsverfahren genutzt werden können. Eine hohe Interoperabilität kann durch freie Standards in Bezug auf die übertragenen Authentifizierungsmerkmale unabhängig vom konkreten Verfahren erzielt werden. Beispiele sind der XML-basierte SAML-Standard bzw. die WS-* Spezifikationen.[398] Allerdings sind diese aktuell auf Web-Anwendungen beschränkt und können somit nicht für die Authentifizierung an allen Ressourcen und Applikationen verwendet werden.

Dies beschreibt bereits die Problematik der fehlenden Flexibilität. Zusätzlich müssen Verfahren in unterschiedlichen Kontexten und Umgebungen, z.B. mobil im World Wide Web oder an mobilen Endgeräten, einsetzbar sein.[399] Auch ein Roaming muss innerhalb einer Sitzung ohne erneute Authentifizierung möglich sein, was derzeit nur durch Verfahren wie Kerberos oder Federations unterstützt wird. Die Sicherheit darf in drahtlosen Netzwerken nicht eingeschränkter sein als in drahtgebundenen.

Durch den zusätzlichen administrativen Aufwand bei der Vergabe von Zertifikaten skalieren Public-Key-Infrastrukturen schlecht, sofern zeitaufwendige Kontrollen und Abläufe innerhalb der zugehörigen Zertifizierungsrichtlinien gefordert werden. Die schlechte Skalierbarkeit gilt allgemein für zentralisierte Strukturen, sofern diese über mehrere Organisationen ausgedehnt werden.[400] Beispielsweise kann dies durch Kooperationen zwischen einzelnen Organisationen erforderlich werden. Derzeit können hier nur dezentrale Verzeichnisdienste oder Federation-basierte Lösungen eingesetzt werden. Allerdings erfordern auch diese eine zentrale Koordination, die erneut Probleme bei der Spezifizierung der ausgetauschten Information (z.B. die Definition einheitlicher Benutzernamen bzw. Attribute der Identitäten) aufwirft. Insbesondere in e-Science Umgebungen herrscht zudem eine hohe Benutzerfluktuation vor, die durch aufwendige Verfahren oder zeitaufwendige Verwaltung von Authentifizierungsmerkmalen schlecht berücksichtigt werden kann.

3.3.2 Verwaltungsaufwand

Insbesondere dezentrale Verzeichnisdienste und Public-Key-Infrastrukturen erfordern einen hohen Aufwand für ihre Verwaltung seitens der Organisationen als Betreiber. Dezentrale Verzeichnisdienste bieten ein Framework für die Synchronisierung und Vereinheitlichung von Informationen,

---

[398] Beide wurden als Grundlage der Federation-basierten Authentifizierung in Abschnitt 3.2.7 erläutert.

[399] Vgl. HAGENHOFF, S.; SCHUMANN, M.: Mediaconomy - Internetökonomie der Medienwirtschaft, in IT - Information Technology Nr. 48, 2006, S. 219 f.

[400] Vgl. WINDLEY, P. J.: Digital Identity, 2005, S. 119.

wie in Abschnitt 3.2.2 erläutert. Um die Funktionalität dieser dezentralen Verzeichnisse zu realisieren, ist jedoch eine Implementierung der Regeln erforderlich, nach denen z.B. Authentifizierungsmerkmale synchronisiert werden. Dies bedeutet erneut einen zusätzlichen Aufwand. Für Public-Key-Infrastrukturen ist, bedingt durch die Einhaltung der Sicherheitsanforderungen an Zertifizierungsstellen, wie in Abschnitt 3.2.4 erläutert, ebenfalls ein hoher Verwaltungsaufwand erforderlich.

Der Aufwand wird durch die Verwaltung unterschiedlicher Verfahren und Authentifizierungssysteme innerhalb einer heterogenen IT-Struktur zusätzlich verstärkt. Dies gilt insbesondere dann, wenn auch eine hohe Anzahl von Benutzern verwaltet werden muss und sich der Verwaltungsaufwand dadurch vervielfacht.

3.3.3 Sicherheit und Benutzbarkeit

Abgesehen von den in Abschnitt 3.2.9 genannten Risiken der Passwort-Speicherung und der schwachen Verschlüsselung der Authentifizierungsmerkmale bei RADIUS[401] bieten die beschriebenen Verfahren eine hohe Sicherheit bzw. gewährleisten die Vertraulichkeit, Integrität und Verbindlichkeit wie durch die Verwendung von SSL und TLS.[402] Web-Anwendungen, deren Authentifizierungsverfahren in Abschnitt 3.2.6 und 3.2.7 beschrieben wurden, können durch Angriffe auf die verwendeten Cookies beeinträchtigt werden.[403] Zusätzlich können Authentifizierungsverfahren durch Angriffe auf die Web-Anwendungen mittels SQL-Injection[404] oder Cross-Site-Scripting[405] umgangen oder manipuliert werden.

Sicherheitsverfahren wie TLS und SSL auf Server- und Client-Seite steigern die Sicherheit, reduzieren jedoch die Benutzbarkeit (Usability) aufgrund der höheren Komplexität.[406] Ein Problem stellen hier z.B. die Zertifikate dar, die eine Installation im Betriebssystem erfordern. Smart Cards oder Tokens[407] benötigen zudem die Installation spezieller Treiber und das Vorhandensein von Schnittstellen wie Kartenleser oder USB. Authentifizierungsverfahren müssen in allen Anwendun-

---

401 Vgl. Abschnitt 3.2.5.

402 Diese Grundwerte der IT-Sicherheit wurden in den Abschnitten 2.2.1, 2.2.2 und 2.2.4 genannt.

403 Vgl. HUSEBY, S. H.: Sicherheitsrisiko Web-Anwendung, 2004, S. 17 ff.

404 Vgl. HUSEBY, S. H.: Sicherheitsrisiko Web-Anwendung, 2004, S. 30 ff.; PEIKARI, C.; CHUWAKIN, A.: Kenne Deinen Feind, 2004, S. 408 ff.

405 Vgl. HUSEBY, S. H.: Sicherheitsrisiko Web-Anwendung, 2004, S. 111 ff.

406 Vgl. RENAUD, K.: Evaluating Authentication Mechanisms, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 116 ff.

407 Vgl. Abschnitt 2.5.2.

gen und in allen Umgebungen (z.B. an mobilen Endgeräten) verwendbar sein, um eine hohe Benutzbarkeit zu erzielen.

Akzeptieren Benutzer die Komplexität bzw. den Aufwand für die Verwendung der Sicherheitsverfahren und -vorgaben nicht, so versuchen sie, diese zu umgehen. Wird beispielsweise eine hohe Komplexität der Passwörter erfordert sowie eine zyklische Änderung, so beginnen die Benutzer damit das Passwort leicht zugänglich aufzuschreiben und am Arbeitsplatz (z.B. als Zettel am Monitor) zu hinterlegen.[408] Erzwungene regelmäßige Passwort-Änderungen werden auch umgangen, indem der Benutzer zunächst mehrfach zufällige neue Passwörter vergibt, bis die maximale Passwort-Historie erschöpft ist, um schließlich das alte zu vergeben. Eine weitere Möglichkeit ist das simple Anfügen einer Zahl, die bei jeder Änderung hochgezählt wird.[409]

3.3.4 Fehlende Benutzer-Zentrierung und Datenschutz

Die im vorherigen Abschnitt erläuterten Probleme der Benutzbarkeit bestehender Verfahren für einheitliche Authentifizierung werden unter anderem durch die fehlende Ausrichtung auf die Anforderungen des Benutzers (auch als Benutzer-Zentrierung bezeichnet) bedingt. Verfahren wie das im folgenden Abschnitt 3.4 erläuterte SXIP ermöglichen im Gegensatz dazu eine Selbstbestimmung des Benutzers über dessen Identität. Sie erlauben dem Benutzer, Vertrauen, das er bei anderen Partnern gewonnen hat (z.B. durch Transaktionen in Web-Shops oder Reputation in Web-Foren), auf neue Partner und die bei ihnen erforderliche Authentifizierung zu übertragen. Authentizität wird bestimmt durch Vertrauensbekundungen von Dritten, wie z.B. Organisationen oder bekannte Benutzer. Diese vermaschten Beziehungen lassen sich in hierarchischen Vertrauensstrukturen wie Verzeichnisdiensten und Public-Key-Infrastrukturen jedoch nicht abbilden.

Fehlende Selbstbestimmung über die Identität führt insbesondere zu einer Minderung des Datenschutzes. Benutzer können nicht in jeder IT-Struktur über die Verwendung ihrer Daten bestimmen. Durch die zunehmende Dezentralität werden die Daten auch Dritten zugänglich, beispielsweise durch Kooperationen zwischen Web-Anbietern. Durch Verzeichnisdienste kann leicht eine Aggregation der Daten erfolgen, die ohne Zustimmung des Benutzers erfolgt. Eine mögliche Lösung sind separate Authentifizierungsdienste bzw. -dienstleister, die als Vermittler agieren, ohne die Identitätsinformationen zu aggregieren.[410] Effizienter ist jedoch die Zentrierung der Identitätsverwaltung

---

[408] CHESWICK, W. R.; BELLOWIN, S. M., RUBIN, A. D.: Firewalls und Sicherheit im Internet. 2. Aufl., 2004, S. 182; SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 160 ff.

[409] Vgl. YAN, J ET AL.: The Memorability and Security of Passwords, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 132.

[410] Vgl. WINDLEY, P. J.: Digital Identity, 2005, S. 128 f.

auf den Benutzer selbst, der über seine Vertrauensstellungen bestimmt und somit zusätzlich den Aufwand für die Verwaltung seitens der Betreiber mindert.[411]

3.4 Stand der Forschung zu einheitlichen Authentifizierungsverfahren

Während die im den Abschnitt 3.2 beschriebenen bestehenden Lösungsansätze für einheitliche Authentifizierung vorrangig auf zentralen Strukturen wie Verzeichnisdiensten oder festen hierarchischen Modellen wie Public-Key-Infrastrukturen basieren, fokussieren aktuell entwickelte Lösungen die dezentrale Authentifizierung. Dies ermöglicht beispielsweise die dezentrale Administration bzw. Delegierung der Identitätsverwaltung innerhalb einer IT-Struktur. Zusätzlich ermöglicht die dezentrale Verwaltung der Authentifizierungsmerkmale ein hohes Maß an Selbstbestimmung der Benutzer.

Diese Anforderungen fließen sowohl in die Weiterentwicklung von Shibboleth innerhalb des Internet2 als auch in Microsofts Identity Metasystem ein.[412] CAMERON beschreibt für die Anforderungen an Identitätssysteme basierend darauf sieben Regeln als „Laws of Identity“ im Rahmen des Identity Metasystem von Microsoft:[413]

- **User Control and Consent:** „Technical identity systems must only reveal information identifying a user with the user’s consent.“
- **Minimal Disclosure for a Contrained Use:** „The solution which discloses the least amount of identifying information and best limits its use is the most stable long term solution.“
- **Justifiable Parties:** „Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.“
- **Directed Identity:** „A universal identity system must support both “omni-directional” identifiers for use by public entities and “unidirectional” identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.“
- **Pluralism of Operators and Technologies:** „A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers.“

---

411 Vgl. Sxip Networks: SXIP 2.0 Overview, 2007, S. 3.

412 Vgl. AAR: Wie funktioniert Shibboleth?, 2006, S. 22.

413 Die folgenden Regeln sind direkte Zitate aus CAMERON, K.: The Laws of Identity, 2005.

- **Human Integration:** „The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks."
- **Consistent Experience across Contexts:** „The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies."

Aus den genannten Laws of Identity sowie den in Abschnitt 3.2.7 vorgestellten Mustern für Federations lässt sich das Paradigma der Benutzer-Zentrierung ableiten. Zukünftige Ansätze für Identity Management und Authentifizierung orientieren sich vermehrt an den Anforderungen der Benutzer und deren Selbstbestimmung als an hierarchischen Modellen wie Verzeichnisdiensten und PKI. Sie bilden damit Beziehungen und Vertrauensstrukturen realitätsnäher ab, da das Vertrauen zwischen Menschen in der Realität ebenfalls nicht strikt hierarchisch bestimmt wird.[414]

Den Grundsatz der Benutzer-Zentrierung verfolgen auch Ansätze wie OpenID[415] und das Simple Extensible Identity Protocol (kurz: SXIP)[416]. Bei SXIP besitzt jeder Benutzer eine Homesite, die z.B. ein Internet-Anbieter oder eine Web-Community sein kann. Benutzer werden bei OpenID und SXIP anhand einer neutralen URL ihrer Homesite identifiziert, die sie für die Anmeldung bei anderen Web-Seiten, die eine SXIP-Anmeldung gestatten, verwenden. Diese Web-Seiten werden auch als Membersites bezeichnet. Ist der Benutzer bereits bei seiner Homesite angemeldet erfolgt keine erneute Überprüfung des Passworts, so dass zwischen allen vom Benutzer registrierten Membersites ein Single Sign-On möglich ist. Unterschiedliche Identitäten, vergleichbar mit den in Abschnitt 3.2.7 vorgestellten Visitenkarten und InfoCards, werden bei SXIP als Persona bezeichnet. Bei der ersten Anmeldung an einer Membersite entscheidet der Benutzer, welche Informationen (bzw. welche Persona) er für die Anmeldung verwenden möchte.[417] Abbildung 3-16 zeigt Ablauf einer SXIP-Sitzung.

In (1) baut der Benutzer eine Verbindung zur Membersite auf und wählt dort für die Anmeldung das SXIP-Verfahren aus (dies wird als „SXIP-in" bezeichnet). Die Membersite leitet den Benutzer mittels SXIP auf dessen Homesite (2), an der sich der Benutzer authentisiert (3). Nach erfolgreicher Anmeldung entscheidet der Benutzer über Informationen seiner Persona, die er an die Membersite senden möchte. Diese werden an die Membersite übertragen und der Client (Web-Browser) des Benutzers an diese umgeleitet (4). Daraufhin erfolgt die Anmeldung an der Membersite (5).

---

[414] Vgl WINDLEY, P. J.: Digital Identity, 2005, S. 119.

[415] Vgl. OpenID: an actually distributed identity system, 2007, das insbesondere für Blogs verwendet wird.

[416] Vgl. SXIP identity, 2007.

[417] Vgl. Sxip Networks: SXIP 2.0 Overview, 2007, S. 4.

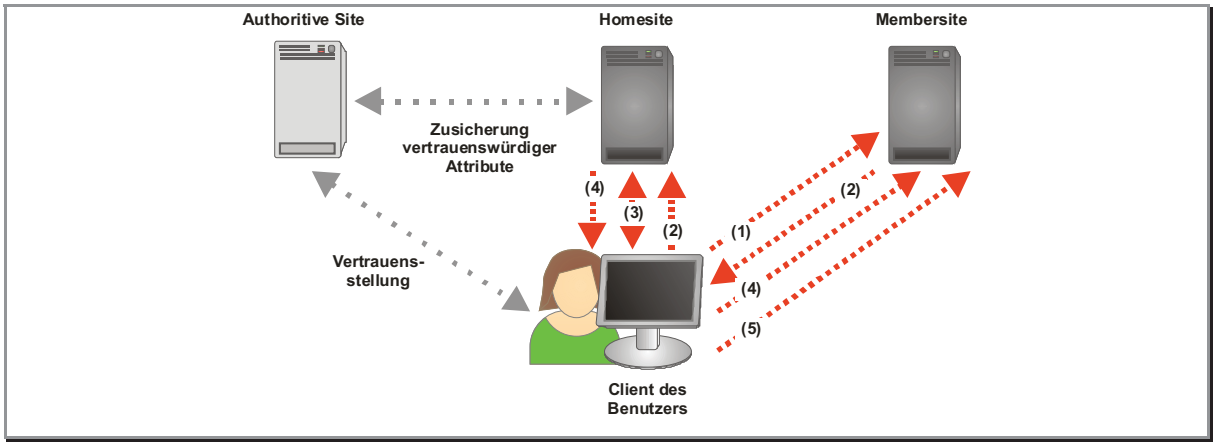

Abbildung 3-16: Dezentraler, Benutzerzentrierter Ansatz am Beispiel von SXIP[418]

Als Erweiterung für die aktuelle SXIP-Version 2.0 existieren sog. Authoritive Sites, die einzelne Informationen zu einer Persona überprüfen und für deren Validität bürgen. Eine Authoritive Site kann eine Behörde sein, die ein Geburtsdatum gewährleistet, oder eine Organisation, die die Zugehörigkeit der Persona (z.B. eines Mitarbeiters) zu ihr bestätigt.[419]

Durch die Benutzer-Zentrierung kann der Benutzer Informationen, die seine Identität und Authentizität bestätigen, gezielt für die Registrierung bei anderen Anbietern verwenden. Die Informationen dienen dabei als Bestätigungen (Bewertungen, Reputation), die andere Organisationen oder Benutzer über den Benutzer treffen (Beispiel: Bewertung in Foren, Web-Shops oder Auktionshäusern). Die Benutzer-Zentrierung wird von HARDT, dem Gründer von SXIP, in Bezug auf den Fortschritt gegenüber den klassischen im Abschnitt 3.2 genannten Verfahren auch als Identity 2.0 bezeichnet.[420]

Während InfoCard bzw. Microsoft Identity Metasystem und SXIP noch vorrangig auf Web-Anwendungen fixiert sind, orientieren sich ähnliche Projekte bereits an der Generalisierung für beliebige Anwendungen und Plattformen. Beispiele sind das Eclipse-basierte Projekt Higgins oder das bandit Projekt.[421] Durch Standards wie SAML und WS-*[422] wird dabei eine zukünftige Interoperabilität der Ansätze angestrebt.

---

[418] Nach Sxip Networks: SXIP 2.0 Overview, 2007, S. 5, 8.

[419] Vgl. Sxip Networks: SXIP 2.0 Overview, 2007, S. 8.

[420] Vgl. HARDT, D.: Identity 2.0, 2007.

[421] Vgl. Higgins Trust Framework Project, 2007; Bandit Project, 2007; OSIS: The Open-Source Identity System, 2007.

[422] Vgl. Abschnitt 3.2.7.

Usability & Security bzw. benutzbare Sicherheit stellt einen weiteren Gegenstand aktiver Forschung dar.[423] Es existieren in diesem Zusammenhang zahlreiche Arbeiten in Bezug auf die Authentifizierung, die auch die Vereinfachung bestehender Verfahren adressieren.[424] Beispielsweise werden Public-Key-Infrastrukturen durch flache Hierarchien vereinfacht und um die automatisierte Ausstellung von Zertifikaten erweitert.[425] Auch die Verknüpfung von Zertifikaten mit Bildern (sog. Logotypes), um eine benutzerfreundliche Überprüfung zu ermöglichen, steht noch am Anfang der Entwicklung.[426] Eine Erweiterung der klassischen Public-Key-Verfahren stellt auch ID-PKC dar, bei dem Public Keys direkt aus allgemeinen Bezeichnern wie E-Mail-Adressen abgeleitet werden.[427] Zusätzlich erhält der Benutzer bei ID-PKC die Möglichkeit, über einen Dienst die Verwendung seiner Signatur bzw. seines Schlüssels selektiv für einzelne Benutzer zu erlauben. Vereinfachungen für die Verwendung von Zertifikaten bieten auch das in RFC 2693 spezifizierte Simple Public Key (SPKI)[428] Zertifikatformat oder die Simple Distributed Security Infrastructure (SDSI)[429], die jedoch in der Praxis nahezu keine Verwendung finden.

Zunehmend werden auch die Kosten bzw. die dem entgegenstehenden Risiken der Authentifizierung bzw. IT-Sicherheit bewertet. Dies wird im Bereich Economics & Security zusammengefasst, der Gegenstand aktiver Forschung ist.[430]

Durch die Bestrebungen der Länder, Pässe mit digitalen Identitätsmerkmalen auszustatten, bieten sich zukünftig neue Möglichkeiten für einheitliche Authentifizierungsmerkmale. Allerdings erfor-

---

[423] Vgl. ADAMS, A.; SASSE, A.: Users Are Not the Enemy. Why Users Compromise Security Mechanisms and How to Take Remedial Measures, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 640 ff.; WITTEN, A.; TYGAR, J. D.: Why Johnny Can't Encrypt, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 669 ff.

[424] Vgl. beispielsweise RENAUD, K.: Evaluating Authentication Mechanisms, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 103 ff.; YAN, J ET AL.: The Memorability and Security of Passwords, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 129 ff.; MONROSE, F.; REITER, M. K.: Graphical Passwords, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 157 ff.

[425] Vgl. SMETTERS, D. K.: Making the Impossible Easy: Usable PKI, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 319 ff.

[426] Vgl. SANTESSON, S.; HOUSLEY, R.; FREEMAN, T.: Internet X.509 Public Key Infrastructure: Logotypes in X.509 Certificates, 2004.

[427] Vgl. ID-PKC, 2007; COCKS, C.: PKC - A Fresh Approach, 2001.

[428] Vgl. ELLISON, C. ET AL.: SPKI Certificate Theory (RFC 2693), 1999.

[429] Vgl. A Simple Distributed Security Infrastructure (SDSI), 2007.

[430] Vgl. Economics & Security, 2007 und MÖRIKE, M.; TEUFEL S.: Kosten & Nutzen von IT-Sicherheit in: HEILMANN, H. ET AL. (Hrsg.): HMD - Praxis der Wirtschaftsinformatik, Heft 248, 2006.

dern diese auch eine hohe Sicherheit und sind aus Sicht des Datenschutzes, bedingt durch die Nachverfolgbarkeit der Benutzer, nicht unbedenklich. Hier bieten die skizzierten Entwicklungen dezentraler Authentifizierung, ggf. mit einer Erweiterung wie den in diesem Abschnitt vorgestellten Authority Sites, eine mögliche Lösung.

4 Anforderungen an eine einheitliche Authentifizierung in heterogenen IT-Strukturen

Insbesondere im Abschnitt 3.3 wurden die Probleme des Ist-Zustands der einheitlichen Authentifizierung in heterogenen IT-Strukturen geschildert. Für die Lösung der genannten Probleme und die Definition eines geeigneten Soll-Zustands werden in diesem Kapitel erforderliche Ziele ermittelt. Die folgenden Abschnitte definieren zusätzlich die in dieser Arbeit für die Vereinheitlichung betrachteten Zielgruppen und beschreiben Schnittstellen der Authentifizierung zu angrenzenden Verfahren wie der Autorisierung. Zusätzlich werden neben den Zielen der einheitlichen Authentifizierung in heterogenen IT-Strukturen auch die Grenzen der Vereinheitlichung genannt.

4.1 Ziele einer einheitlichen Authentifizierung

Die folgenden Abschnitte nennen die Ziele für die Vereinheitlichung der Authentifizierung in heterogenen IT-Strukturen. Sie beschreiben daher auch die Vorteile, die durch eine einheitliche Authentifizierung erzielt werden.

4.1.1 Vereinheitlichung der Authentifizierungselemente

Vorrangiges Ziel für die einheitliche Authentifizierung ist die Reduktion von Authentifizierungsmerkmalen, -verfahren und -systemen. Hierdurch wird eine Minimierung des Aufwands für Benutzer und Organisationen erreicht. Neben der quantitativen Reduktion kann eine Vereinheitlichung auch qualitativ anhand einer Ablösung aufwendiger Merkmale, Verfahren und Systeme durch einfachere Varianten erfolgen.

Die Vereinheitlichung der Authentifizierungsmerkmale wird in Bezug auf die Reduktion von Passwörtern häufig als „Single-Password“ bezeichnet. Benutzer sollen mit einem einzelnen Passwort Zugriff auf unterschiedliche Ressourcen erhalten.

Wird nicht nur die Ausprägung von Authentifizierungsverfahren vereinheitlicht, sondern auch deren Verwendung für unterschiedliche Applikationen innerhalb einer Sitzung, spricht man von „Single-“ oder „Reduced Sign-On“, wie bereits in Abschnitt 2.1.12 definiert. Ziel ist es hierbei den Aufwand für die Verwendung der Authentifizierungsverfahren zu mindern.

Aus Sicht der Organisationen zielt die Vereinheitlichung in erster Linie auf Authentifizierungssysteme. Die angebotenen Ressourcen sollen beispielsweise ein zentrales Authentifizierungssystem (z.B. einen Verzeichnisdienst wie in Abschnitt 3.2.2 beschrieben) verwenden. Auch hier ist das Ziel die Minimierung des Aufwands etwa für Wartung und Betrieb der Systeme seitens der Organisationen.

4.1.2 Steigerung von Benutzbarkeit und IT-Sicherheit

Einheitliche Authentifizierung ermöglicht eine deutliche Steigerung der Benutzbarkeit (Usability[431]) durch den verminderten Aufwand für die Verwendung von Authentifizierungsmerkmalen, -verfahren und -systemen, wie im vorherigen Abschnitt erläutert. Dies zielt auf die Wünsche der Benutzer nach hoher Usability.[432] Eine hohe Usability der Authentifizierung kann auch eine höhere Produktivität der Mitarbeiter erzielen und durch geringeren Verwaltungsaufwand (z.B. Entlastung des Help-Desk durch weniger Passwort-bezogene Anfragen) Einsparungen für die Organisationen erzielen.[433]

Wird die Authentifizierung, bedingt durch hohe Usability, von den Benutzern besser akzeptiert, so steigt auch die IT-Sicherheit. Erachten Benutzer den Aufwand für die Authentifizierung im Gegensatz dazu als zu hoch bzw. die Usability als zu schlecht, so sind sie bestrebt, die Sicherheitsvorkehrungen zu umgehen.[434] Dies gilt für Benutzer wie für Administratoren gleichermaßen. Ziel der einheitlichen Authentifizierung muss es daher sein, die IT-Sicherheit durch Vereinfachung der Verwendung bzw. Minderung des Aufwands der Authentifizierung zu steigern. Allerdings kann die Vereinheitlichung auch eine Minderung der IT-Sicherheit bedeuten. Beispielsweise sinkt die Sicherheit bei der Verwendung eines einzigen Passworts, da bei dessen Kompromittierung alle Systeme betroffen sind. Um die IT-Sicherheit im Rahmen einer einheitlichen Authentifizierung zu gewährleisten und dem genannten Risiko entgegenzuwirken, muss die einheitliche Authentifizierung z.B. eine hohe Komplexität der vereinheitlichten Authentifizierungsmerkmale, -verfahren und -systeme erzielen.

4.1.3 Einheitliches Identity Management

Über die Authentifizierung hinaus sollen durch die Vereinheitlichung definierte Schnittstellen für die Verwaltung von Identitäten geschaffen werden. Dies umfasst auch Schnittstellen zur Autorisie-

---

[431] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 115 f.

[432] Vgl. NIELSEN, J.: Usability Engineering, 1993, S. 23 ff.; GERD TOM MARKOTTEN, D.: Benutzbare Sicherheit in informationstechnischen Systemen, 2003, S. 35 ff., 69 ff.

[433] Vgl. GADATSCH, A.; UEBELACKER, H.: Wirtschaftlichkeitsbetrachtungen für IT-Security-Projekte, in MÖRIKE, M.; TEUFEL S.: Kosten & Nutzen von IT-Sicherheit in: HEILMANN, H. ET AL. (Hrsg.): HMD - Praxis der Wirtschaftsinformatik, Heft 248, 2006, S. 46.

[434] Benutzer beginnen Passwörter leicht zugänglich zu notieren, Administratoren installieren Sonderlösungen für Authentifizierungsverfahren, vgl. BISHOP, M.: Psychological Acceptability Revisited, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 2 ff; SASSE, M. A.; FLECHAIS, I.: Usable Security. Why Do We Need It? How Do We Get It?, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 13 ff.

rung von Benutzern sowie die Abrechnung (Accounting) von deren Sitzungen. Im Rahmen der Autorisierung muss die Authentifizierung die eindeutige Zuweisung einer Identität zu Rollen, Gruppen und Rechten erlauben. Hierfür sind auch einheitliche Benutzernamen für die Identitäten erforderlich.

Allgemein sollen hierbei sämtliche Prozesse der Verwaltung von Identitäten (Identity Management) vereinfacht werden. Ziel ist es den gesamten Lebenszyklus einer Identität in den Organisationen mit einem einheitlichen Werkzeug zu verwalten und zu optimieren. Die Optimierung bezieht sich hierbei z.B. auf die Reduzierung der für die Einrichtung und Löschung neuer Benutzer erforderlichen Zeit. Ein neuer Benutzer soll automatisch und über einheitliche Schnittstellen bei seiner initialen Anlage in alle für ihn relevanten Systeme übertragen werden. Dieser Vorgang wird als Provisioning[435] bezeichnet. Dies umfasst auch die Anlage der Ressourcen des Benutzers wie E-Mail-Adresse und Speicherplatz, Home-Verzeichnis etc. über externe Prozesse. Während der Lebenszeit des Benutzers werden Änderungen an dessen Identität analog in die beteiligten Systeme, die der Benutzer verwendet, verteilt. Am Ende der Lebenszeit der Identität des Benutzers werden oft externe Prozesse verwendet, um die Daten des Benutzers zu archivieren und diesen schließlich in allen Systemen zu löschen (Deprovisioning).

Die Realisierung eines einheitlichen Identity Managements im Rahmen der einheitlichen Authentifizierung bietet somit eine ganzheitliche Lösung für die Optimierung von Prozessen der Benutzerverwaltung.

4.2 Betrachtete Zielgruppen

An die Authentifizierung werden je nach Zielgruppe individuelle Anforderungen gestellt. Beispielsweise kann die mobile Authentifizierung auf Web-Seiten für eine Organisation essentiell sein, während eine andere diese aus Sicherheitsgründen von vornherein ablehnt. Auch Faktoren wie die Fluktuation der Benutzer bzw. Anzahl und Häufigkeit der neu hinzugefügten oder gelöschten Benutzer in einem bestimmten Intervall sind von Organisation zu Organisation verschieden. In dieser Arbeit werden vorrangig die Anforderungen wissenschaftlicher bzw. e-Science-Umgebungen berücksichtigt. Da hier durch die hohe Dezentralität, z.B. von europa- oder weltweiten Forschungsgruppen sowie der hohen Fluktuation (z.B. durch Studierende, wechselnde Hilfskräfte) hohe Anforderungen an die Flexibilität der Authentifizierung gestellt werden, lassen sich die Anforderun-

[435] Vgl. z.B. WALTHER, H.: Identity Management, in SAUERBURGER, H. (Hrsg.): Open-Source-Software in: HEILMANN, H. ET AL. (Hrsg.): HMD - Praxis der Wirtschaftsinformatik, Heft 238, 2004, S. 46; WINDLEY, P. J.: Digital Identity, 2005, S. 30.

gen auch auf betriebliche IT-Strukturen übertragen. Benutzer und Betreiber wissenschaftlicher und betrieblicher IT-Strukturen stellen daher die primär in dieser Arbeit betrachteten Zielgruppen dar.

4.2.1 Wissenschaftliche IT-Strukturen

Die Authentifizierung von Benutzern in wissenschaftlichen IT-Strukturen bzw. e-Science Umgebungen zeichnet sich durch folgende Anforderungen aus:

- Benutzer müssen dezentral authentifiziert werden können. So kooperieren internationale Forschungsgruppen, ohne vorher einen persönlichen Kontakt der beteiligten Benutzer zu erfordern. Die Authentifizierung für den Schutz der gemeinsam verwendeten Ressourcen muss somit auch ohne persönlichen Kontakt zwischen Benutzern und Betreibern ermöglicht werden. Dies ist insbesondere für die Einhaltung von Zertifizierungsrichtlinien für X.509-Zertifikate relevant, die in der Regel eine persönliche Identifizierung der Zertifikatnehmer erfordern. Hierfür müssen dezentrale Registrierungsstellen einander vertrauen, um etwa externen Forschern im europäischen Umfeld Zertifikate für die Nutzung gemeinsamer e-Science- resp. Grid-Ressourcen auszustellen. Um die genannten Anforderungen zu erfüllen, ist ein benutzerzentriertes Idenity Management basierend auf den in Abschnitt 3.2.7 vorgestellten Federation-basierten Lösungen erforderlich.[436] Dabei werden die Identitäten und Authentifizierungsinformationen nicht zentral in einer Vielzahl von Verzeichnissen gespeichert, sondern der Benutzer entscheidet, welche Informationen er preisgibt und welche Vertrauensstellungen er eingeht. Die Authentifizierung erfolgt dezentral am Identity Provider der Heimatorganisation.[437]
- Wissenschaftliche IT-Strukturen erfordern, z.B. auch innerhalb der Max-Planck-Gesellschaft, die vollständige Eigenständigkeit der beteiligten Institute. Es können daher nicht immer zentrale Lösungen forciert werden. Dezentrale Administration von Benutzern oder Lösungen für Federation-basierte Authentifizierung usw. sind erforderlich.
- Bedingt durch kurzzeitige bzw. befristete Mitarbeiter (Hilfskräfte, Doktoranden, Studierende, Gastwissenschaftler usw.) besteht eine hohe Benutzerfluktuation. Benutzer müssen somit schnell Zugriff auf alle für sie relevanten Systeme erhalten. Am Ende der Lebenszeit einer Identität dürfen deren Daten zudem nicht gelöscht werden, sondern müssen ggf. in andere Institute migriert oder archiviert werden. Die Anforderungen an die Restaurierbarkeit der Identitäten können bis in die digitale Langzeitarchivierung, z.B. für die Archivierung von Forschungs-

[436] Wie es in Sxip Networks: SXIP 2.0 Overview, 2007, S. 3 oder Microsoft: Microsoft's Vision for an Identity Metasystem, 2005 vorgestellt wird.

[437] Vgl. Identity Provider und Heimatorganisation in Abschnitt 3.2.7.

ergebnissen oder Patientendaten, hineinreichen. Problemstellung ist hierbei auch der Datenschutz. Beispielweise darf bei der Erstellung eines Zertifikats in der Max-Planck-Gesellschaft aus dessen Gültigkeit kein Rückschluss auf die Dauer des Arbeitsverhältnisses (z.B. von Hilfskräften usw.) möglich sein.

- Innerhalb wissenschaftlicher IT-Strukturen wird eine Vielzahl unterschiedlicher Plattformen (unterschiedliche Betriebssysteme und Hardware-Architekturen) verwendet. Teilweise ist diese Heterogenität durch Vorlieben oder spezielle Anforderungen der Wissenschaftler bedingt, teilweise entsteht sie aus gewachsenen Strukturen. Die Authentifizierung muss somit auch nach einer Vereinheitlichung für eine Vielzahl unterschiedlicher bzw. heterogener Systeme verwendbar sein.

Insbesondere an Forschungsprojekte, die mit sensiblen Daten (z.B. Patientendaten medizinischer Forschungsergebnisse) arbeiten, werden neben den genannten hohen Anforderungen an die Flexibilität zusätzlich hohe Sicherheitsanforderungen gestellt. Beispielsweise gelten für die Forschung an den physikalischen Grundlagen von Fusionskraftwerken des Instituts für Plasmaphysik der Max-Planck-Gesellschaft höhere Sicherheitsanforderungen als für andere Max-Planck-Institute. Basierend auf diesen Sicherheitsanforderungen werden im Grid- bzw. e-Science Umfeld beispielsweise von vornherein Zertifikate für die Authentifizierung eingesetzt.[438]

4.2.2 Betriebliche IT-Strukturen

Auch wirtschaftliche Organisationen können die im vorherigen Abschnitt genannten Anforderungen an die einheitliche Authentifizierung stellen. Allerdings werden hier in der Regel geringere Ansprüche an die Flexibilität gesetzt. Die Eigenständigkeit beteiligter Institutionen bzw. Tochtergesellschaften eines Konzerns usw. ist, im Hinblick auf die Benutzerverwaltung, häufig nicht erforderlich oder nicht sinnvoll. Auch die Fluktuation der Benutzerkonten der Mitarbeiter ist häufig geringer als für die Wissenschaft geschildert. Sofern auch Benutzerkonten für Kunden betrachtet werden, kann sie jedoch auch beträchtlich größer sein. Darüber hinaus stellen wirtschaftliche Organisationen folgende zusätzliche Anforderungen an die einheitliche Authentifizierung:

- Wirtschaftliche Organisationen stellen im Sinne der Kostenminimierung monetäre Anforderungen an die einheitliche Authentifizierung. Die einheitliche Authentifizierung muss wirtschaftlich sein, indem die durch die Reduzierung des Aufwands minimierten Kosten für das Controlling messbar werden. Zusätzliche Hard- und Software Investitionen, z.B. für das Identity Management, müssen sich amortisieren.

---

[438] Vgl. International Grid Trust Federation (IGTF): The Grid's Policy Management Authority, 2007.

- Ziel der einheitlichen Authentifizierung sollte neben der Reduzierung des Aufwands auch die Wahrung oder Steigerung der erzielten IT-Sicherheit sein. Häufig ist die Bestrebung zur Steigerung der IT-Sicherheit Teil eines Risiko-Managements innerhalb der Organisationen bei dem potentielle Schäden bzw. Lücken der IT-Sicherheit bewertet und den Kosten für deren Eindämmung gegenüber gestellt werden. Teilweise besteht auch die explizite Verpflichtung nach einer Einhaltung konkreter IT-Sicherheitsniveaus. Diese können entweder erforderlich sein, um Daten der Kunden oder Partner-Organisationen sicher zu verarbeiten, oder durch gesetzliche bzw. externe wirtschaftliche Vorgaben an die Organisation gestellt werden. Beispiele hierfür sind der Sarbanes-Oxley-Act, Basel II oder auch das Bundesdatenschutz- sowie das Informations- und Telekommunikationsdienstegesetz, die z.B. in Abschnitt 2.3.2 beschrieben wurden.
- Ähnlich der dezentralen Authentifizierung innerhalb wissenschaftlicher IT-Strukturen, wie im vorherigen Abschnitt beschrieben, können auch Kooperationen mit anderen Unternehmen bzw. Partnerorganisationen Anforderungen an die einheitliche Authentifizierung stellen. Kooperiert beispielsweise ein Internet-Auktionshaus mit einem Kreditinstitut, so sollen die Kunden beider Organisationen sich an allen gemeinsamen Ressourcen der Organisationen authentifizieren bzw. ihre Daten verwenden können.

Allgemein stellt die Wahrung der IT-Sicherheit im E-Commerce eine wichtige Anforderung dar, die auch im Informations- und Telekommunikationsdienstegesetz geregelt wird.[439] Beispielsweise ist erst nach einer eindeutigen Authentifizierung der beiden Kommunikationspartner eine sichere Transaktion z.B. über Web-Shops gewährleistet. Der Diebstahl von Identitäten, wie in Abschnitt 2.8.1 beschrieben, stellt hier ein zu vermeidendes Risiko dar.

Auch in betrieblichen Strukturen existieren insbesondere in großen Organisationen die bereits im vorherigen Abschnitt beschriebenen heterogenen Strukturen (z.B. bedingt durch Spezialanwendungen oder um durch unterschiedliche Hard- und Software Lösungen die Fehlertoleranz zu erhöhen), die gleichermaßen vereinheitlicht werden sollen, um den Aufwand und damit die Kosten für deren Betrieb und Wartung zu minimieren.

4.3 Schnittstellen zu nachgelagerten Verfahren

In dieser Arbeit werden vorrangig Verfahren zur Authentifizierung und deren Vereinheitlichung betrachtet. Für die Realisierung der IT-Sicherheit, vgl. deren Grundwerte in Abschnitt 2.2, sind

[439] Vgl. UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN: Die wichtigsten Bestimmungen des Informations- und Kommunikationsdienste-Gesetzes (IuKDG), 2007.

jedoch zusätzliche Verfahren erforderlich, die den Zugriff auf die geschützten Daten nach erfolgreicher Authentifizierung kontrollieren. Die folgenden Abschnitte beschreiben Schnittstellen zu diesen nachgelagerten Verfahren und deren Vereinheitlichung. In Bezug auf die Authentifizierung müssen für die Vereinheitlichung dieser nachgelagerten Verfahren insbesondere einheitliche Benutzernamen etabliert werden, wie sie bereits in Abschnitt 4.1.3 gefordert wurden.

Die Authentifizierung bildet die Grundlage für die IT-Sicherheit, da sie zu Beginn jeder Sitzung insbesondere beim Zugriff auf dezentrale Ressourcen durchgeführt wird. Sie muss daher robust ausgelegt und fehlerfrei realisiert werden, um eine sichere Basis für die nachfolgenden Verfahren zu gewährleisten.

4.3.1 Autorisierung

Während die Authentifizierung die Identität eines Benutzers eindeutig nachweist, kontrolliert sie nicht dessen Berechtigung für den Zugriff auf die Daten. Dies wird von Autorisierungsverfahren basierend auf dem durch die Authentifizierung ermittelten Benutzernamen übernommen. Benutzernamen werden für die Autorisierung beispielsweise auf Gruppen und Rechte abgebildet. Um die Verwaltung dieser Autorisierungsinformationen zu vereinheitlichen, wurde die Abbildung auf Rollen eingeführt. Rechte werden hierbei Rollen zugewiesen, die ihrerseits Benutzern zugeordnet werden. Wird später einem Benutzer eine neue Rolle zugewiesen oder eine seiner Rollen entfernt, so werden alle zugehörigen Rechte im selben Schritt hinzugefügt oder entfernt. Ebenso können einer Rolle neue Rechte, z.B. für eine neue Applikation eingeräumt und dadurch automatisch allen verbundenen Benutzern zugewiesen werden. Für die Implementierung von Rollen existieren verschiedene Lösungen. Als Standard hat sich Role-Based Access Control (RBAC) etabliert.[440] Zusätzlich existiert in der Extensible Access Control Markup Language (XACML) ein XML-basierter Autorisierungsstandard, der vorrangig von Web-Anwendungen verwendet wird.[441] Neben diesen plattform- und herstellerunabhängigen Lösungen für die Vereinheitlichung der Autorisierung bieten zahlreiche Hersteller unterschiedliche proprietäre Lösungen an.[442]

---

[440] Vgl. NIST: Role Based Access Control (RBAC), 2007.

[441] OASIS: XACML, 2007.

[442] Wie z.B. Novell Entitlements, 2007, Siemens DirXMetaRoles in HERWIG, V.; SCHLABITZ, L.: Unternehmensweites Berechtigungsmanagement, in KÖNIG, W. (Hrsg.): Wirtschaftsinformatik, 46. Jahrgang, Heft 4, 2004, S. 289 ff.

4.3.2 Sitzungsverwaltung und Accounting

In der Regel bildet die Authentifizierung nur den Anfang einer anschließenden Sitzung des Benutzers, in der er die geschützte Anwendung bzw. Ressource verwendet. Zum einen müssen über diese Sitzung hinweg Authentifizierungsinformationen zwischengespeichert werden, sofern nicht für jede Funktion innerhalb der Anwendung eine neue Anmeldung erfolgen soll.[443] Dies erfolgt durch die Sitzungsverwaltung. Für bestimmte Nutzungsszenarien, z.B. beim Roaming des Benutzers zwischen unterschiedlichen Dienstleistern, die die Anwendung anbieten, kann auch die Aufrechterhaltung der Authentifizierung ohne erneute Prüfung über Sitzungen hinweg gewünscht sein. Hierfür muss die Sitzungsverwaltung in der Lage sein, die Authentifizierung beim Roaming des Benutzers im Hintergrund automatisch abzuwickeln.

Zum anderen müssen für eine spätere Abrechnung der Sitzung, z.B. der Einwahl in das Netzwerk eines Drittanbieters, Eigenschaften wie Dauer der Sitzung, verwendete Ressourcen etc. ermittelt werden. Dies wird als Accounting bezeichnet. Die Authentifizierung muss eine Schnittstelle für das Accounting bieten. Hierbei wird in der Regel die Identität des Benutzers, z.B. ein Benutzername verwendet, der von der Authentifizierung überprüft und an das Accounting im Rahmen einer Sitzung weitergereicht wird.

4.3.3 Auditing

Werden hohe Anforderungen an die Nachvollziehbarkeit der Authentifizierung oder resultierender Sitzungen, wie im vorherigen Abschnitt beschrieben, z.B. bzgl. der Einhaltung von IT-Sicherheitsrichtlinien, gestellt, so ist die Aufzeichnung von Authentifizierungsvorgängen bzw. deren Erfolg oder Misserfolg erforderlich. Insbesondere in Bezug auf externe Vorgaben an die Organisationen sowie allgemeine Anforderungen an die IT-Sicherheit, z.B. durch den Sarbanes-Oxley-Act[444] oder Basel II[445], wird die Auditierbarkeit bzw. das Auditing immer mehr erforderlich. Die Konformität der eingesetzten Authentifizierungsverfahren sowie deren Gewährleistung durch entsprechendes Auditing werden in Bezug auf diese Richtlinien auch als Compliance bezeichnet. Erneut sichert die Authentifizierung hierbei die Nachvollziehbarkeit der Identität. Sie gewährleistet, dass eine bestimmte Handlung exakt von einem bestimmten Benutzer durchgeführt wurde.

---

[443] Vgl. Single- bzw. Reduced Sign-On in Abschnitt 2.1.12.

[444] Vgl . HURLEY, E.: Security and Sarbannes-Oxley, 2003.

[445] Vgl. BUNDESBANK: Basel II - Die neue Baseler Eigenkapitalvereinbarung, 2007; einen Überblick über die Relevanz für die IT-Sicherheit liefert CORPORATE-CONSULTING.NETWORK: IT-Sicherheit als Rating-Faktor, 2006.

4.4 Begrenzende Faktoren

Durch die Vereinheitlichung der Authentifizierung können Nachteile entstehen. Beispielsweise steigt das Sicherheitsrisiko für die IT-Struktur insgesamt, wenn nur noch ein einziges Authentifizierungssystem, -verfahren und -merkmal verwendet wird.[446] Da die einheitliche Authentifizierung vor allem eine Minderung des Aufwands gemäß Abschnitt 4.1.1 erzielen soll, darf der zusätzliche Aufwand für die Vermeidung der Nachteile nicht größer als die durch die Vereinheitlichung erreichte Minderung des Aufwands sein. Der zusätzliche Aufwand stellt somit eine Begrenzung der sinnvoll realisierbaren Vereinheitlichung dar. Die folgenden Abschnitte zeigen die Risiken und Einschränkungen, die mit zunehmender Vereinheitlichung der Authentifizierung entstehen, im Einzelnen auf.

4.4.1 Homogenität von Authentifizierungsmerkmalen

Den größten Nachteil bildet die mit der Vereinheitlichung zunehmende Homogenität. Obwohl sie für die Minimierung des Aufwands erwünscht ist, wird die erzielbare Sicherheit gesenkt. Für die Authentifizierungsmerkmale bedeutet die Homogenität, dass ein Benutzer im Extremfall nur noch ein einziges Passwort für alle von ihm verwendeten Dienste nutzt. Erlangt ein unberechtigter Dritter Zugriff auf dieses Passwort, so kann er alle Dienste im Namen des impersonierten Benutzers verwenden. Hinzu kommt, dass der Benutzer bei der Verwendung von Passwörtern nicht unmittelbar bemerkt, dass ein Dritter sein Passwort erlangt hat.

Beispielsweise kann ein Administrator eines Web-Shops die Passwörter seiner Kunden während der Eingabe oder Speicherung abgreifen. Werden die Passwörter im Rahmen einer einheitlichen Authentifizierung synchronisiert bzw. verwenden die Kunden in anderen Web-Shops oder Anwendungen, z.B. E-Mail Konten, ERP-Systemen usw., dasselbe Passwort, so kann der Administrator unbemerkt seine Kunden in diesen Systemen impersonieren und beispielsweise in deren Namen Waren erwerben. Auch Szenarien wie Phishing von Passwörtern oder Social Engineering[447] wird durch die Homogenität von Passwörtern eine größere Angriffsfläche bzw. ein größerer Anreiz geboten.

Um derartigen Szenarien vorzubeugen, muss die Sicherheit im Rahmen der Vereinheitlichung zusätzlich gesteigert werden. Beispielsweise können Tokens und eine Multi-Faktor Authentifizierung

---

[446] Wie in Abschnitt 4.1.2 für die Verwendung eines einzigen Passworts geschildert.

[447] Vgl. „Abhören von Passwörtern“ in Abschnitt 2.8.1 und 2.8.4.

eingesetzt werden.[448] In diesem Fall ist für die erfolgreiche Authentifizierung neben der Kenntnis des Passworts auch der physikalische Besitz des zugehörigen Tokens erforderlich.

Insbesondere muss bei der Vereinheitlichung der Authentifizierungsverfahren und -systeme darauf geachtet werden, dass diese nicht kompromittiert werden und so ein Abhören der übermittelten Authentifizierungsmerkmale möglich wird. Dies kann durch kryptographische Verfahren, wie z.B. SSL und TLS, wie sie in Abschnitt 2.6.1 beschrieben wurden, ermöglicht werden. Auch Verfahren zur Offline-Authentifizierung[449] sind für die Minderung des skizzierten Nachteils geeignet.

Zukünftig sollte auf Federation-basierte Lösungen gesetzt werden, da hier die Authentifizierung am Identity Provider der Home Organization durchgeführt wird und somit sämtliche Service Provider keinen Zugriff auf das eigentliche Authentifizierungsmerkmal besitzen.[450] Der Identity Provider kann hierbei mit einem Clearinghouse verglichen werden, das z.B. in Form von Zertifikaten eine sichere Vertrauensstellung zwischen den Service-Providern realisiert und die Authentifizierung der Benutzer (z.B. über Passwörter) eigenständig abwickelt.

Adressiert wird der beschriebene Nachteil auch durch benutzerzentrierte Lösungen, bei denen die Benutzer selbst entscheiden können, welche Authentifizierungsmerkmale und -informationen sie verwenden oder freigeben möchten.

4.4.2 Kompatibilität der angebundenen Ressourcen

Eine Vereinheitlichung der Authentifizierungssysteme ist nur möglich, sofern diese gemeinsame Authentifizierungsverfahren oder standardisierte Schnittstellen verwenden. Zusätzlich müssen sie neben den eingesetzten Authentifizierungsverfahren auch von allen erforderlichen Ressourcen der heterogenen IT-Struktur verwendet werden können. Die Kompatibilität zwischen angebundenen Ressourcen, eingesetzten Authentifizierungsverfahren und -systemen ist somit ein begrenzender Faktor für die einheitliche Authentifizierung. Diese können beispielsweise auf unterschiedliche Hardware- oder Betriebssystem-Plattformen (z.B. Windows, Unix oder Apple Macintosh) aufsetzen. Unterstützt die Vereinheitlichung nicht alle Ressourcen oder Authentifizierungsverfahren durch die verbleibenden Authentifizierungssysteme, so müssen, sofern auf die Ressourcen und Verfahren nicht verzichtet werden kann, separate Authentifizierungssysteme zu Ungunsten der Vereinheitlichung in Kauf genommen werden.

---

[448] Vgl Vorteile beim Einsatz von aktiven Tokens in Abschnitt 2.5.2.

[449] Vgl. Verwendung von Zertifikaten in Abschnitt 2.7.4.

[450] Vgl. Abschnitt 3.2.7.

Durch gezielte Analyse des Ist-Zustands vor der Vereinheitlichung und Ermittlung der Abhängigkeiten z.B. von Authentifizierungssystemen lässt sich die aufgezeigte Grenze für die Vereinheitlichung geeignet erkennen und berücksichtigen. Zusätzlich kann der durch die Vereinheitlichung entstehende Nachteil durch die Fokussierung auf modulare Authentifizierungssysteme verringert werden. Unter modularen Authentifizierungssystemen werden hierbei Systeme verstanden, die unterschiedliche Authentifizierungsverfahren unterstützen oder zwischen diesen vermitteln können. Derartige Systeme setzen in der Regel auf standardisierten Verfahren auf, wie z.B. LDAP, die plattformunabhängig von unterschiedlichen Ressourcen unterstützt werden.[451] Lösungen wie Virtual Directories oder Proxies sind zusätzlich in der Lage, als stellvertretendes Authentifizierungssystem unterschiedliche Authentifizierungsverfahren anzubieten oder im Hintergrund abzubilden.[452]

4.4.3 Portabilität von Authentifizierungsverfahren und -merkmalen

Analog zu dem im vorherigen Abschnitt beschriebenen Nachteil durch die Inkompatibilität von Authentifizierungssystemen ist auch die Vereinheitlichung von Authentifizierungsverfahren begrenzt. Zum einen können diese, wie im vorherigen Abschnitt geschildert, inkompatibel zu den verwendeten Authentifizierungssystemen sein, zum anderen können sie jedoch auch spezielle Authentifizierungsmerkmale voraussetzen. Zusätzlich wird die Verwendung der Authentifizierungsmerkmale für unterschiedliche Authentifizierungsverfahren durch deren Speicherung begrenzt. Passwörter werden in der Regel irreversibel verschlüsselt, in den im Authentifizierungssystem gespeicherten Konten gespeichert. Für die Sicherheit ist dieses Vorgehen vorteilhaft, da kein Dritter, insbesondere kein Administrator, auf die Passwörter der Benutzer zugreifen kann. Allerdings können Administratoren die Passwörter durch geeignete Anpassung der Authentifizierungsverfahren, Log-Dateien usw. ohnehin während der Authentifizierung Zugriff auf die Passwörter erlangen. Für die Verwendung unterschiedlicher Authentifizierungssysteme in heterogenen IT-Strukturen ist somit der Nachteil relevanter, dass Passwörter, die einmal in einem bestimmten irreversiblen Hash-Wert[453] gespeichert wurden, später schlecht in zusätzlich eingeführte Anwendungen, die ein anderes Hash-Verfahren verwenden, übernommen oder konvertiert werden können. Die Synchronisation oder Vereinheitlichung von Hash-Werten und damit die Portabilität von Authentifizierungs-

---

[451] Die Verwendung LDAP-basierter Verzeichnisse wurde in Abschnitt 3.2.2 erläutert.

[452] Virtuelle Verzeichnisse als Server-seitige Proxies nennt der Abschnitt 3.2.2. Client-seitige Authentifizierungsproxies wurden in Abschnitt 3.2.8 beschrieben.

[453] Vgl. Hash-Verfahren in Abschnitt 2.6.2.

merkmalen ist daher abhängig von deren Unterstützung durch die verwendeten Authentifizierungssysteme und -verfahren.

Als Lösung bieten sich Meta-Directories[454] an, die die Passwörter vor der Erzeugung des Hash-Werts aus den Quellsystemen erlangen und z.B. asymmetrisch bzw. reversibel verschlüsseln,[455] um bei Bedarf neue Hash-Werte für zukünftige Anwendungen erzeugen zu können. Eine weitere Möglichkeit sind Initial-Passwörter für Benutzer, die von der vergebenden Organisation im Klartext gespeichert und vom Benutzer anschließend geändert werden. Sie können für spätere Anwendungen und neue Hash-Verfahren erneut genutzt werden. Auch hier bietet sich jedoch insbesondere eine benutzerzentrierte Lösung, z.B. in Form eines Web-Portals, das die Anmeldung an unterschiedlichen Systemen erlaubt und die Hash-Werte zentral erzeugt und verteilt, an. Auch Federation-basierte Lösungen mindern den Einfluss der genannten Grenze, da die Authentifizierungsinformationen zwischen den Service Providern in standardisierter Form (basierend auf XML), unabhängig von der konkreten Ausprägung bei der Authentifizierung am Identity Provider, ausgetauscht werden.[456]

4.4.4 Rechtliche Aspekte

Vor allem bei organisationsübergreifender Authentifizierung spielen externe rechtliche Vorgaben an die Organisationen, wie sie in Abschnitt 2.3.2 beschrieben werden, eine entscheidende Rolle. So können rechtliche Vorgaben aus Sicht des Datenschutzes relevant sein, sofern die zur Authentifizierung verwendeten Informationen auf persönlichen Daten beruhen. Um diese Grenze zu vermeiden, sollte den Benutzern beispielsweise über Web-Portale die Möglichkeit geboten werden, die Verteilung ihrer Authentifizierungsinformationen eigenständig zu steuern. Um die Sicherheit zu steigern und diesbezüglich individuelle Anforderungen an die Organisationen, die eine gemeinsame Authentifizierung betreiben, zu unterstützen, sollten über die Portale auch Partner-Organisationen die Möglichkeit erhalten, ihre Benutzer, etwa im Rahmen eines kooperativen Identity Managements bei dem jeweiligen Partner, zu verwalten. Rechtliche Vorgaben sollten insbesondere an den IT-Sicherheitsrichtlinien der IT-Struktur orientiert oder diesen angepasst werden. Dies kann beispielsweise auch die Vorgabe von getrennten Authentifizierungsmerkmalen für sensible Anwendungen oder spezielle Sicherheitsanforderungen an die Merkmale und Verfahren einschließen.

---

[454] Vgl. die Synchronisation von Attributen (z.B. Passwörtern) über Meta-Directories in Abschnitt 3.2.2.

[455] Vgl. asymmetrische Verschlüsselung in Abschnitt 2.6.1.

[456] Federation-basierte Lösungen wurden in Abschnitt 3.2.7 erläutert.

5 Modellierung und Klassifizierung der Faktoren für eine einheitliche Authentifizierung

Im Kapitel 4 wurden die Ziele für eine einheitliche Authentifizierung genannt. Um die optimale Umsetzung der damit verbundenen Anforderungen zu erreichen, werden in diesem Kapitel die bestimmenden Faktoren für eine Vereinheitlichung bestehender Authentifizierungsstrukturen definiert und bewertet. Die Faktoren werden hierbei auf ein geeignetes Modell für die einheitliche Authentifizierung in heterogenen IT-Strukturen abgebildet und abschließend konkrete Vereinheitlichungspotentiale aufgezeigt und evaluiert. Hierbei werden die in Abschnitt 2.1 definierten Elemente und Beteiligten einer Authentifizierung betrachtet.

Heterogene IT-Strukturen umfassen in der Realität eine Vielzahl von Authentifizierungssystemen und -verfahren.[457] Die resultierende Komplexität der Authentifizierung aus Sicht der Betreiber und Benutzer lässt sich durch Optimierungsverfahren minimieren. Geeignete Optimierungsverfahren werden in Kapitel 6 evaluiert. Optimierungsverfahren als Bestandteil der Operations Research lassen sich jedoch nicht unmittelbar auf reale heterogene IT-Strukturen anwenden. Sie erfordern zunächst ein Modell, das die realen Strukturen formal abbildet.[458] Verfahren zur hierfür erforderlichen Modellierung werden beispielsweise von BIETHAHN ET AL. oder SUHL UND MELLOULI beschrieben.[459] Allgemein bildet der Vorgang der Optimierung den in Abbildung 5-1 illustrierten Ablauf.

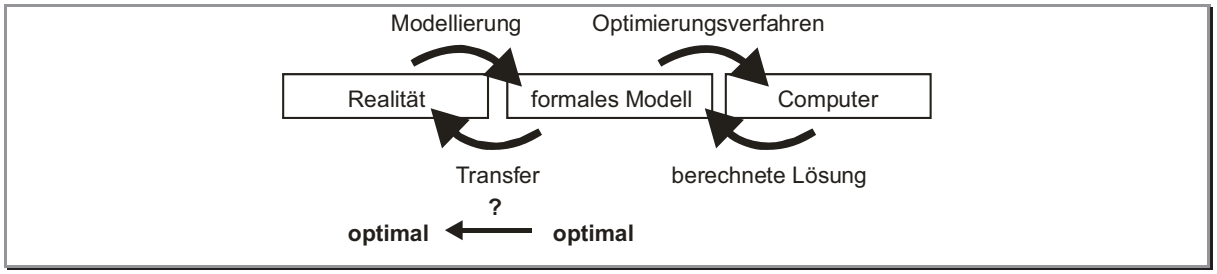

Abbildung 5-1: Ablauf der Modellierung und Optimierung von realen Systemen[460]

Dabei wird die Realität durch Modellierungsverfahren auf ein formales Modell abgebildet, auf das computergestützte Optimierungsverfahren angewendet werden können. Die berechnete Lösung wird für die Verfeinerung des formalen Modells verwendet, das anschließend in die Realität trans-

[457] Vgl. Diversität in Abschnitt 3.1.

[458] Vgl. SUHL, L.; MELLOULI, T.: Optimierungssysteme, 2006, S. 6 f.

[459] Vgl. BIETHAHN, J. ET AL.: Optimierung und Simulation, 2004, S. 5 ff.; SUHL, L.; MELLOULI, T.: Optimierungssysteme, 2006, S. 5 ff.

[460] Nach SUHL, L.; MELLOULI, T.: Optimierungssysteme, 2006, S. 1.

feriert bzw. umgesetzt wird. Abschließend erfolgt die Evaluation des Transfers und bedingt im Falle einer nicht optimalen Umsetzung eine erneute Modellierung resp. Optimierung.

Bestehende Authentifizierungsmodelle[461] lassen sich nicht für die Optimierung von heterogenen IT-Strukturen verwenden, da sie sich auf genau ein System (homogene IT-Struktur) beziehen, das die Authentifizierung bzw. Authentifizierungsverfahren ausführt. Eine einheitliche Authentifizierung in heterogenen IT-Strukturen bedingt, aufgrund der Vielfalt der eingebunden Systeme[462], eine übergreifende Lösung für unterschiedliche innerhalb der IT-Struktur eingesetzte Plattformen (z.B. Windows, Unix), Anwendungen und Ressourcen. Daher wird für die Klassifizierung der Faktoren einer einheitlichen Authentifizierung in heterogenen IT-Strukturen das erweiterte Authentifizierungsmodell aus Abschnitt 2.4.2 verwendet und im folgenden Abschnitt auf ein formales theoretisches Modell abgebildet, das anschließend optimiert wird.

5.1 Formales Modell für die Authentifizierung in heterogenen IT-Strukturen

Basierend auf dem Modell aus Abschnitt 2.4.2 lassen sich die an einer Authentifizierung beteiligten erforderlichen Elemente Benutzer, Betreiber, Ressourcen, Authentifizierungsmerkmale, -verfahren und -systeme unterscheiden.[463] In Anlehnung an bestehende Authentifizierungsmodelle werden diese Elemente, im Folgenden auch als Authentifizierungselemente[464] bezeichnet. Diese Authentifizierungselemente umfassen ihrerseits erneut eine Menge von Unterelementen, die deren konkrete Ausprägungen bzw. Varianten darstellen. Varianten bezeichnen hierbei z.B. unterschiedliche technische Implementierungen von Authentifizierungsverfahren oder verschiedene Authentifizierungsmerkmale.[465] In individuellen IT-Infrastrukturen können diesen Mengen verschiedene Elemente zugeordnet werden. Für die Klassifizierung der Faktoren einer einheitlichen Authentifizierung wird daher im Folgenden ein allgemeines, formalisiertes Modell definiert und verwendet, das in Abbildung 5-2 gezeigt wird. Zur Veranschaulichung wurden den Mengen exemplarische Elemente zugeordnet.

Das Modell umfasst die Menge der Organisationen bzw. Betreiber *O,* die eine Menge von Ressourcen *R* (wie z.B. Rechner-, Speichersysteme) anbieten. Betreiber können hierbei kooperieren, d.h.

---

[461] Wie beispielsweise das Authentifizierungsmodell nach SMITH (vgl. Abschnitt 2.4.1).

[462] Vgl. Diversität von Authentifizierungsmerkmalen, -verfahren und -systemen in Abschnitt 3.1.

[463] Vgl. Begriffsdefinition in Abschnitt 2.1.

[464] Vgl SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 4.

[465] Vgl. Abschnitt 2.7 und Abschnitt 2.5.

Ressourcen gemeinsam verwalten und ihren Nutzern zur Verfügung stellen. Abbildung 5-2 veranschaulicht dies in der Ressource r_k, die sowohl von der Organisation o_1 als auch o_2 betrieben und verwendet wird. Zwischen den Mengen O und R existierende Relationen sind linkstotal und rechtstotal bzw. surjektiv, da alle Ressourcen und Organisation zugeordnet werden. Sie sind jedoch weder rechtseindeutig noch linkseindeutig bzw. injektiv, da eine Ressource von mehreren Organisationen verwaltet werden kann und eine Organisation mehrere Ressourcen verwaltet. Die Relationen zwischen den beiden Mengen gelten formal somit als Abbildungen.[466]

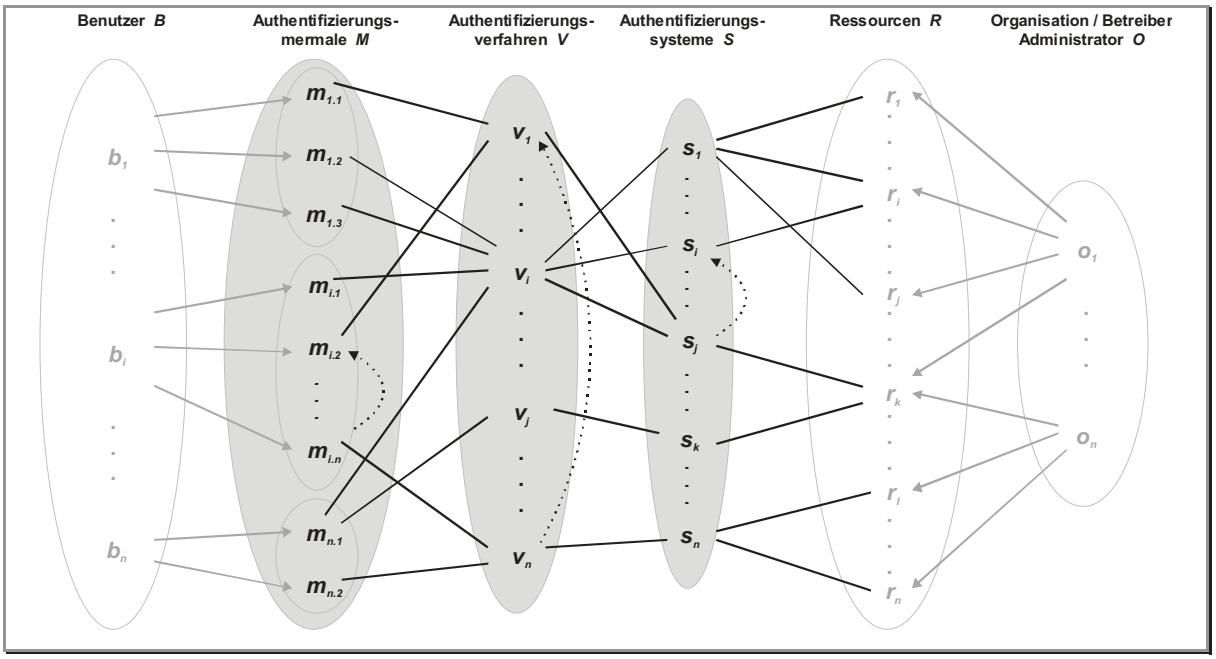

Abbildung 5-2: Formales Modell für die Authentifizierung in heterogenen IT-Strukturen

Um unberechtigten Nutzern den Zugriff auf die Ressourcen der Menge R zu verweigern, setzen die Betreiber eine Menge S von Authentifizierungssystemen ein, die eine Authentifizierung und in der Regel anschließende Zugriffskontrolle bzw. Autorisierung der Benutzer durchführen. Einzelne Systeme können, wie in Abschnitt 2.1.9 beschrieben, verbunden werden. In diesem Fall greift ein System für die Authentifizierung eines Benutzers seinerseits auf ein weiteres System zurück. In der Abbildung 5-2 veranschaulicht dies das System s_j, das auf das System s_i zurückgreift. Um die Administration und Bereitstellung von Ressourcen für die Betreiber zu vereinfachen, werden im Idealfall mehrere Ressourcen einem gemeinsamen System zugewiesen. Benutzer, die die Ressourcen r_1, r_i und r_j verwenden möchten, könnten sich im in Abbildung 5-2 gezeigten Beispiel gegenüber dem System s_1 authentisieren. Es kann jedoch, wie für Ressource r_k in Abbildung 5-2 gezeigt, sinnvoll

[466] Vgl. Surjektivität und Injektivität von Abbildungen in MEYBERG, K.; VACHENAUER, P.: Höhere Mathematik 1, 4. Auflage, 1997, S. 2.

sein, eine Ressource von unterschiedlichen Systemen zugänglich zu machen. Im Folgenden werden ausschließlich Ressourcen betrachtet, für die eine Authentifizierung erfolgen soll. Daher sind die Relationen zwischen den Mengen *R* und *S* linkstotal und rechtstotal. Jede Ressource und jedes Authentifizierungssystem wird zugeordnet. Die Relationen sind jedoch weder linkseindeutig noch rechtseindeutig, da eine Ressource mehreren Authentifizierungssystemen zugeordnet werden kann und ein System für die Verwaltung mehrerer Ressourcen verwendet wird. Relationen zwischen Ressourcen und Authentifizierungssystemen werden somit formal als Abbildungen betrachtet.

Für die Authentifizierung verwenden die Authentifizierungssysteme der Menge *S* Verfahren der Menge *V*. Verfahren können ihrerseits weitere Verfahren für die Authentifizierung verwenden, wie in Abbildung 5-2 durch Verfahren v_n verdeutlicht, das seinerseits v_1 verwendet. Systeme können mehrere Verfahren verwenden (vgl. s_j), ein Verfahren kann jedoch auch mehreren Systemen zugeordnet werden (vgl. v_i). Auch die Relationen zwischen Authentifizierungssystemen und Authentifizierungsverfahren sind somit zwar linkstotal und rechtstotal, aber weder linkseindeutig noch rechtseindeutig. Sie stellen daher ebenfalls formal Abbildungen dar.

Authentifizierungsmerkmale werden als Elemente der Menge *M* klassifiziert. Ein Authentifizierungsmerkmal identifiziert einen Benutzer eineindeutig und ist somit exakt einem Element der Menge Benutzer *B* zugeordnet. Benutzer besitzen ihrerseits mehrere Authentifizierungsmerkmale der Menge *M*. Wie in Abbildung 5-2 illustriert, umfasst die Menge *M* alle Authentifizierungsmerkmale aller Benutzer, da diese insgesamt von Authentifizierungsverfahren und -systemen verwendet werden. Dies entspricht der Sicht der Betreiber resp. Organisationen *O*, die alle Authentifizierungsmerkmale verwalten müssen. Aus der Sicht der Benutzer existieren jedoch innerhalb der Menge *M* Untermengen, die jeweils die Merkmale eines einzelnen Benutzers umfassen. In der Abbildung werden beispielsweise die Merkmale des Benutzers b_1 daher mit m_1 indiziert und dem Benutzer b_1 somit insgesamt $m_{1.1}$, $m_{1.2}$ und $m_{1.3}$ eindeutig zugeordnet. Diese werden daher in Abbildung 5-2 als Untermengen dargestellt. Zwischen den Mengen *B* und *M* existieren Relationen, die linkstotal und rechtstotal sind. Sie sind zusätzlich linkseindeutig, da für die folgenden Betrachtungen vorausgesetzt wird, dass ein Merkmal genau einem Benutzer zugeordnet wird. Dies entspricht den Anforderungen an eine Authentifizierung, wie in Abschnitt 2.1.4 beschrieben, die die Identität eines Benutzers anhand eines Merkmals eindeutig nachweist. Benutzer besitzen jedoch insbesondere in heterogenen Umgebungen eine Vielzahl von Authentifizierungsmerkmalen, so dass die dargestellten Relationen zwischen *B* und *M* nicht rechtseindeutig sind.[467] Mehrere Authentifizierungsmerkmale können miteinander verknüpft bzw. für eine erfolgreiche Authentifizierung ge-

[467] Vgl. Anzahl der Authentifizierungsmerkmale in Abschnitt 2.4.2.

meinsam vorausgesetzt werden.[468] Im Modell in Abbildung 5-2 wird dies durch die Verknüpfung der Merkmale $m_{i.n}$ und $m_{i.2}$ veranschaulicht.

In den folgenden Abschnitten wird die Vereinheitlichung des skizzierten Modells aus zwei Perspektiven betrachtet und bewertet. Zum einen die der Organisationen bzw. Betreiber. Zum anderen die Perspektive der Benutzer. Daher wurden die Relationen zwischen den Mengen *M*, *V*, *S* und *R*, in Abbildung 5-2 ungerichtet dargestellt. Beispielsweise erlaubt ein bestimmtes Authentifizierungsverfahren aus Sicht der Organisationen die Anbindung unterschiedlicher Authentifizierungsmerkmale, z.B. für unterschiedliche Benutzer. Im Gegenzug kann ein Benutzer ein Authentifizierungsmerkmal für unterschiedliche Verfahren (z.B. Kerberos, LDAP usw.) verwenden.

Als Faktoren für eine einheitliche Authentifizierung gelten die Authentifizierungselemente dieses Modells, die eine hohe Diversität und Komplexität aufweisen, die durch geeignete Vereinheitlichung reduziert werden kann. Mit steigender Diversität des jeweiligen Authentifizierungselements steigt dessen Relevanz als Faktor für eine einheitliche Authentifizierung aufgrund des zunehmenden Vereinheitlichungspotentials.

Die Diversität bzw. resultierende Komplexität der einzelnen Elemente wird durch die möglichen Varianten bzw. Anzahl an Unterelementen der Menge und deren Relationen und Abhängigkeiten untereinander bestimmt. Die Reduzierung der Varianten und Relationen beschreibt die Vereinheitlichung des in Abbildung 5-2 gezeigten Authentifizierungsmodells für heterogene IT-Strukturen. Durch die Vereinheitlichung unterschiedlicher Authentifizierungselemente und Relationen entstehen separate Modelle für die einheitliche Authentifizierung, die in den folgenden Abschnitten evaluiert, auf die Realität übertragen und optimiert werden. Hierfür wird ein Bewertungsmodell vorgestellt, das Güte, Aufwand und Nutzen der Vereinheitlichung aus den Perspektiven der Benutzer sowie Organisationen, Betreiber und Administratoren bestimmt.

Die einheitliche Authentifizierung in heterogenen e-Science-Umgebungen kann dabei nicht für alle Authentifizierungselemente sinnvoll umgesetzt werden:

- **Benutzer**: Eine Vereinheitlichung der Benutzer ist nicht zielführend. Sie würde zur Folge haben, dass unterschiedliche Anwender (z.B. Wissenschaftler, vgl. Abschnitt 4.2.1) ein gemeinsames Benutzerkonto resp. Authentifizierungsmerkmal verwenden müssten. Auch wenn dies in einigen wenigen Anwendungsbereichen in der Realität praktiziert wird, wäre hierbei eine vertrauliche Verwendung von Informationen und Daten generell nicht möglich. Die Umsetzung der Anforderungen aus Abschnitt 4.1.2 lässt daher eine Vereinheitlichung der Varianten dieses Authentifizierungselements nicht zu.

[468] Vgl. Multi-Faktor Authentifizierung in Abschnitt 2.5.2.

- **Ressourcen**: Werden den Benutzern weniger Ressourcen angeboten, so verringert sich neben dem Aufwand für deren Administration auch der Aufwand für die zugehörige Authentifizierung und Zugriffskontrolle. Es ist daher betriebswirtschaftlich häufig sinnvoll, mehrere Ressourcen zu integrieren. Redundanzszenarien, verteilte Strukturen und technische Einschränkungen (z.B. die Kompatibilität zu integrierender Ressourcen untereinander) begrenzen diese Integration jedoch. Insbesondere für heterogene IT-Strukturen, wie in Abschnitt 4.1.1 gezeigt, sind für eine einheitliche Authentifizierung somit Lösungen für eine Vielzahl von Ressourcen erforderlich. Die Reduktion der abgebildeten Ressourcen im Authentifizierungsmodell ist daher nicht Bestandteil der folgenden Betrachtungen.
- **Organisationen / Betreiber**: Wie im Abschnitt 4.2.1 ausgeführt, erfordert ein Modell für die einheitliche Authentifizierung besonders in heterogenen e-Science-Umgebungen die Integration unterschiedlicher, dezentraler Betreiber, z.B. in Form von verteilten Instituten, unterschiedlichen Forschungsstandorten oder Kooperationspartnern. Eine Vereinheitlichung der beteiligten Organisationen wird daher nicht betrachtet.

Die genannten Einschränkungen für die Vereinheitlichung der Authentifizierungselemente führen zu folgenden verbleibenden variablen Faktoren für einheitliche Authentifizierungsmodelle, deren Mengen daher in Abbildung 5-2 grau hinterlegt gezeigt sind:

- Authentifizierungsmerkmale
- Authentifizierungsverfahren
- Authentifizierungssysteme

Des Weiteren wird die Vereinheitlichung der Relationen dieser Faktoren bzw. deren Mengen M, V, S und R betrachtet. Es wird vorausgesetzt, dass ein Authentifizierungsmerkmal als Element der Menge M genau einem Benutzer der Menge B zugewiesen ist.[469] Daher ist eine Vereinheitlichung der Relationen zwischen den Mengen B und M nicht möglich. Gemeinsame Ressourcen mehrerer Betreiber können durch die kooperative Administration eine einheitliche Authentifizierung unterstützen. Diese Integration von Ressourcen und Organisationen ist jedoch, wie in diesem Abschnitt geschildert, nicht Bestandteil der vorliegenden Arbeit, daher werden auch die Relationen zwischen den Mengen O und R als fest vorgegeben definiert und ihre Vereinheitlichung nicht evaluiert.

[469] Um diesen gemäß Abschnitt 2.1.4 eindeutig zu identifizieren.

5.2 Integrationsformen der im Modell ermittelten Faktoren

Die in dieser Arbeit verwendeten Verfahren bzw. Formen für die Vereinheitlichung und Integration der in Abschnitt 5.1 ermittelten Faktoren für eine einheitliche Authentifizierung zeigt die Abbildung 5-3. Hierbei wurden exemplarisch Elemente der Menge *M* des in Abbildung 5-2 eingeführten Authentifizierungsmodells für heterogene IT-Strukturen verwendet.

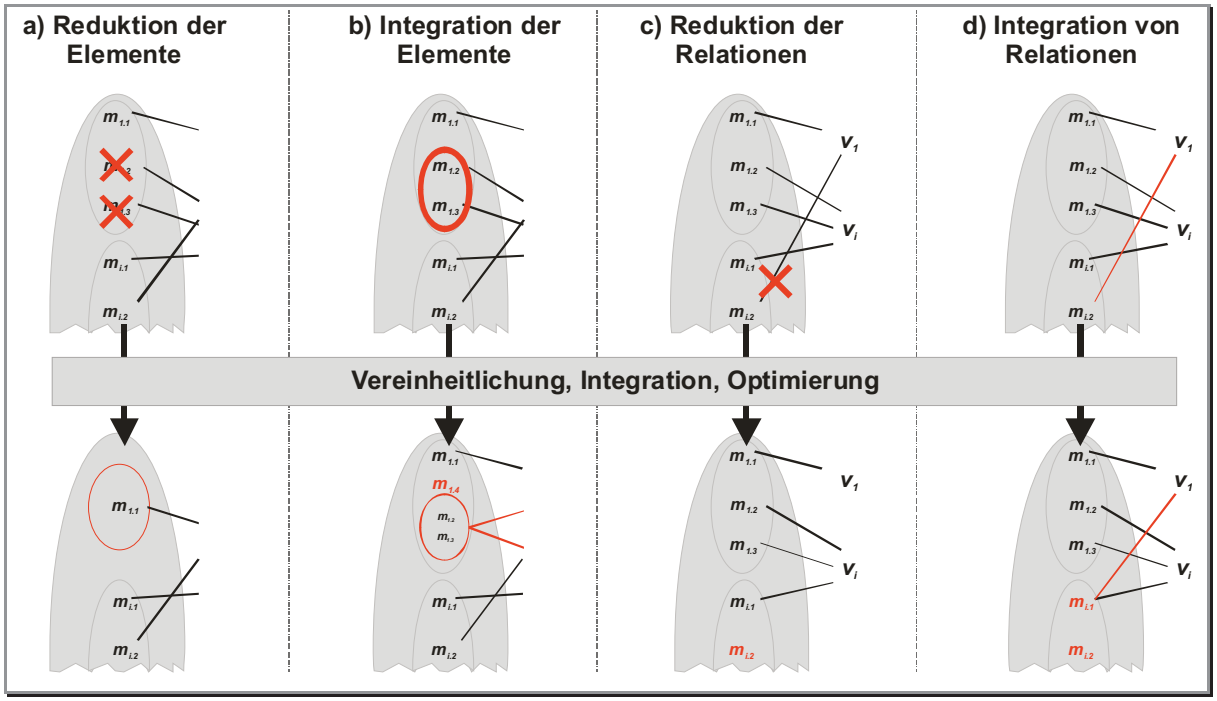

Abbildung 5-3: Integrations- und Vereinheitlichungsformen für die Authentifizierung in heterogenen IT-Strukturen am Beispiel des Modells aus Abbildung 5-2

a) Reduktion der Elemente eines Faktors (Int_a)

Die einfachste Form der Vereinheitlichung bildet die Reduktion der in einer Menge bzw. einem Faktor enthaltenen Elemente. So können etwa Authentifizierungsmerkmale entfernt bzw. reduziert werden, um sowohl die Administration der Identitäten für die Organisation, als auch die Anwendbarkeit der Authentifizierung für die Benutzer zu vereinheitlichen und damit zu vereinfachen. Aufgrund der dadurch reduzierten Komplexität kann dies bereits als Optimierung bezeichnet werden.

b) Integration mehrerer Elemente eines Faktors in einem neuen separaten Element (Int_b)

Neben einer Reduktion der Elemente eines Faktors, wie in a) beschrieben, können auch mehrere Elemente zu einem neuen separaten Element zusammengefasst resp. integriert werden. Dies

kann beispielsweise ein Authentifizierungsmerkmal oder -konto[470] sein, das weitere Authentifizierungsmerkmale eines Benutzers beinhaltet. In der Abbildung 5-3 b) veranschaulicht dies das neue Element $m_{1.4}$. Die Diversität der Authentifizierung wird für den Benutzer durch ein solches Element (im Weiteren auch als Proxy-Element bezeichnet) verringert. Für den Benutzer stellt diese Vereinheitlichung somit eine Vereinfachung dar. Aus Sicht des Betreibers bzw. der Administratoren bildet ein Proxy-Element allerdings ein zusätzliches Merkmal, das verwaltet werden muss. Es handelt sich nur dann auch für die zugehörigen Organisationen um eine Vereinheitlichung bzw. Vereinfachung, wenn durch die Einführung des Proxy-Elements die Administration der beinhalteten Authentifizierungsmerkmale entfällt.

c) Reduktion der Relationen eines Faktors (Int_c)

Elemente besitzen, wie im Abschnitt 5.1 beschrieben, Relationen zu Elementen anderer Mengen. Durch die Reduktion dieser Relationen wird die Komplexität des Modells verringert und damit eine Vereinheitlichung erzielt. Abbildung 5-3 c) zeigt das Entfernen einer Relation des Elements $m_{i.2}$. Dies würde bedeuten, dass der Benutzer *i* dieses Merkmal für das Verfahren v_1 nicht mehr verwenden muss. Nach dem Entfernen der Relation weist das Element $m_{1.2}$ im gezeigten Beispiel keine Relationen mehr auf. Es könnte somit nach dem in a) beschriebenen Verfahren entfernt werden.

d) Integration mehrerer Relationen eines Faktors (Int_d)

Durch das Zusammenfassen bzw. Integrieren mehrerer Relationen wird die Komplexität des Modells zusätzlich verringert. In der Abbildung 5-3 d) wurde die Relation des Merkmals $m_{i.2}$ zum Verfahren v_1 einem anderen Element resp. Authentifizierungsmerkmal $m_{i.1}$ zugewiesen. Es wurde somit eine weitere Relation am Merkmal $m_{i.1}$ integriert. Der Benutzer *i* benötigt somit für die Verwendung beider Verfahren v_1 und v_2 nur noch Merkmal $m_{i.1}$. Auch für die Administration stellt dies eine Vereinheitlichung der Authentifizierung dar, da das Merkmal $m_{i.2}$ nicht mehr für das Verfahren v_1 verwaltet werden muss. Analog zu c) besitzt das Element $m_{i.2}$ im gezeigten Beispiel anschließend keine weiteren Relationen. Es kann somit nach dem in a) beschriebenen Verfahren entfernt werden.

Bei der Vereinheitlichung können ein einzelner Faktor, mehrere oder alle Faktoren betrachtet werden. Die folgenden Abschnitte geben einen Überblick über diesen Umfang der Vereinheitlichung. Als „worst case"-Szenario für die Authentifizierung in heterogenen IT-Strukturen wird die Beibehaltung oder schlimmstenfalls weitere Diversifikation aller Mengen bzw. Faktoren definiert. Hier-

[470] Vgl. Speicherung von Authentifizierungsmerkmal und Benutzername in einem Authentifizierungskonto in Abschnitt 2.1.7.

bei entsteht gemäß den in Abschnitt 4.1.1 genannten Anforderungen der größte Aufwand für die Verwaltung und Verwendung der Authentifizierungsverfahren und -systeme in den IT-Strukturen.

Durch die Gewichtung der Relationen eines Faktors kann die Relevanz der Elemente und Relationen für eine Integration bzw. einheitliche Authentifizierung ermittelt werden. Folgende Kriterien werden bei dieser Gewichtung unterschieden:

- **Kosten und Aufwand *A***

  Eine Authentifizierung stellt in jedem Fall einen zusätzlichen Aufwand im Vergleich zum freien Zugriff ohne Überprüfung der Identität der Benutzer dar. Dieser Aufwand äußert sich für Benutzer in der Verwaltung und Verwendung einzelner Authentifizierungsmerkmale, -verfahren und -systeme. Insbesondere für die Organisationen als Betreiber wirkt sich dieser Aufwand jedoch monetär in Form von Kosten bei Anschaffung und Betrieb aus.[471]

- **Erzielte Sicherheit *S* als Nutzen**

  Durch den Einsatz einer Authentifizierung entsteht für Benutzer und Betreiber ein Nutzen durch die Steigerung der erzielten IT-Sicherheit. Insbesondere die Betreiber können so ihre Ressourcen schützen und durch die Risikominimierung auch Kosten die durch den Missbrauch von Ressourcen entstehen würden, vermeiden. In den betrachteten heterogenen IT-Strukturen existiert in der Regel bereits ein akzeptables Niveau an IT-Sicherheit. Sofern dies der Fall ist, orientiert sich die einheitliche Authentifizierung als Optimierung der Struktur vorrangig an der Minimierung des Aufwands bei gleichzeitiger Gewährleistung der bestehenden IT-Sicherheit.

5.3 Sichtweisen auf das Authentifizierungsmodell

Bei der nachstehenden Vereinheitlichung der in Abschnitt 5.1 klassifizierten Faktoren für eine einheitliche Authentifizierung werden zwei unterschiedliche Sichtweisen auf das Authentifizierungsmodell aus Abschnitt 5.1 unterschieden. Zum einen die Sicht der Benutzer, zum anderen die der Organisationen bzw. Betreiber und deren Administratoren. Diese Sichtweisen werden für die Optimierung der Faktoren der einheitlichen Authentifizierung in heterogenen IT-Strukturen separat betrachtet. Hierbei bringen Organisationen vorrangig wirtschaftliche Optimalitätskriterien (z.B. Steigerung des Return on Investment für die Vereinheitlichung) in die Zielfunktion ein, während aus Sicht der Benutzer vorrangig die Benutzbarkeit der Authentifizierung im Vordergrund steht.

---

[471] Vgl. LUBICH, H. P.: IT-Sicherheit: Systematik, aktuelle Probleme und Kosten-Nutzen-Betrachtungen, in MÖRIKE, M.; TEUFEL S.: Kosten & Nutzen von IT-Sicherheit in: HEILMANN, H. ET AL. (Hrsg.): HMD - Praxis der Wirtschaftsinformatik, Heft 248, 2006, S. 9 ff.

Das Authentifizierungsmodell aus Abbildung 5-2 lässt sich als Netzwerk beschreiben, in dem die Elemente der Mengen die Knoten und die Relationen die Kanten darstellen. Betrachtet man nun das Netzwerk getrennt aus der Richtung der Benutzer sowie der Organisationen, so bildet jede Betrachtung einen gerichteten, zyklenfreien Graphen.[472] Die resultierenden Graphen aus Sicht der Benutzer und Organisationen werden in den folgenden beiden Abschnitten erläutert.

5.3.1 Sicht der Benutzer

Abbildung 5-4 zeigt die Authentifizierung in einer heterogenen IT-Struktur aus Sicht der Benutzer am Beispiel des Benutzers b_i. Hierbei bildet der Benutzer die Quelle des skizzierten Graphen. Wie im Beispiel in Abschnitt 5.1 beschrieben, besitzt der Benutzer b_i drei Authentifizierungsmerkmale ($m_{i.1}$, $m_{i.2}$ sowie $m_{i.3}$), die ihm Zugriff auf Ressourcen der Organisationen, denen er angehört, ermöglichen. Da die Merkmale unterschiedlich hohen Sicherheitsanforderungen[473] genügen können, ist die erzielte Sicherheit S resp. der Nutzen als Gewicht der Kanten zwischen dem Benutzer und seinen Merkmalen variabel. Ebenso bedeutet die Verwendung und Verwaltung des Merkmals für den Benutzer einen unterschiedlich hohen Aufwand[474] und ist daher als variables Kantengewicht A aufgeführt.

Seine Authentifizierungsmerkmale kann der Benutzer b_i im aufgezeigten Beispiel mit den Verfahren v_1, v_i und v_n verwenden, deren Aufwand A und gebotene Sicherheit S ebenfalls als variables Kantengewicht definiert wird. Als Senken des Graphen zeigt die Abbildung 5-4 die Systeme s_1, s_i, s_j und s_n. Auch zwischen den Knoten der Verfahren und Systeme werden variable Kantengewichte für Aufwand A und Sicherheit S definiert.

---

[472] Vgl. TURAU, V.: Algorithmische Graphentheorie, 1996, S. 19, DIESTEL, R.: Graphentheorie, 2. Auflage, 2000, S. 13 ff.

[473] Vgl. Authentifizierungsfaktoren aus Abschnitt 2.1.6, bzw. unterschiedliche Passwort-Längen in Abschnitt 2.5.1.

[474] Vgl. unterschiedliche Authentifizierungsmerkmale in Abschnitt 2.5. Z.B. den höheren Aufwand bei der Verwaltung von Passwörtern im Vergleich zu biometrischen Merkmalen seitens der Benutzer.

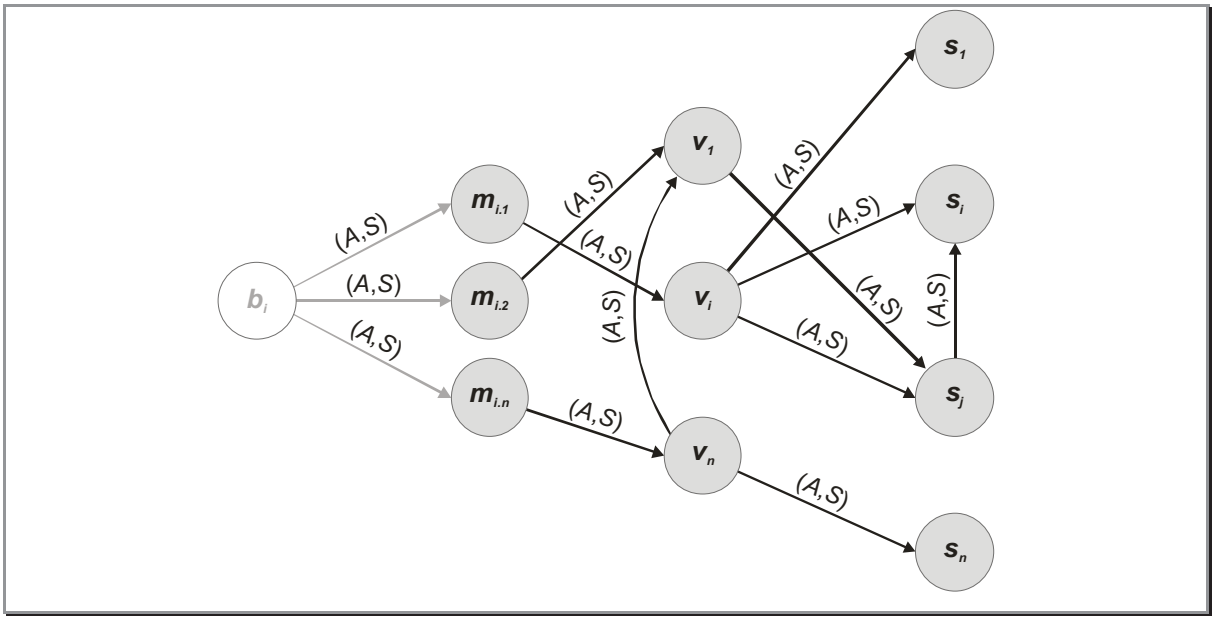

Abbildung 5-4: Authentifizierung in heterogenen IT-Strukturen als gerichteter Graph aus Sicht der Benutzer

Für die Sicht der Benutzer werden die Mengen der Ressourcen *R* sowie die der Organisationen *O* aus Abbildung 5-2 nicht betrachtet, da sie für die Authentifizierung nicht relevant sind. Dies begründet sich damit, dass der Umgang mit den eigentlichen Ressourcen aus Sicht des Nutzers ohne jegliche Authentifizierung identisch zur Verwendung nach erfolgreicher Authentifizierung ist.

Die Authentifizierung kann gemäß dem skizzierten Graphen als Fluss zwischen dem Benutzer, als Quelle über dessen Authentifizierungsmerkmale sowie gemäß den zugewiesenen Authentifizierungsverfahren und den Authentifizierungssystemen als Senke interpretiert werden. Durch den Fluss und die Richtung der Kanten im Graphen wird auch die grundlegende Relevanz der beteiligten Faktoren für die Optimierung vorgegeben. Sie nimmt auf dem Weg von der Quelle zur Senke ab. Authentifizierungsmerkmale erhalten somit aus Sicht der Benutzer die höchste Relevanz für eine Optimierung.

Wird ein Authentifizierungsmerkmal durch eine Vereinheitlichung reduziert, so können evtl. darauf aufbauende Authentifizierungsverfahren oder -systeme ebenfalls reduziert werden, sofern diese von keinem anderen Merkmal des Nutzers referenziert werden. Es wird somit auch die Komplexität der nachfolgenden Faktoren im Graphen reduziert. Dies veranschaulicht die Relevanz der Authentifizierungsmerkmale für die Vereinheitlichung. Zusätzlich wird die Reduktion der betroffenen Kanten bzw. des Authentifizierungsmerkmals für den Benutzer unmittelbar spürbar, da sich durch die Reduktion der betroffenen Kanten für ihn der Aufwand (als Kantengewicht *A*) für die Authentifizierung innerhalb der heterogenen IT-Struktur verringert. Obwohl hierbei auch die Gesamtsumme der Kantengewichte *S* als erzielte Sicherheit verringert wird, kann dies nicht als Minderung der Sicherheit betrachtet werden. Im Folgenden wird als Optimalitätskriterium vielmehr die Einhaltung eines

minimalen Gewichts aller enthaltener Kanten und so eine Gewährleistung der IT-Sicherheit definiert.

Auch die Reduktion der Authentifizierungsverfahren, durch sie ausgelöste Authentifizierungsvorgänge sowie eine verringerte Anzahl von Authentifizierungssystemen verringern die Komplexität für den Benutzer.[475]

Analog zur Darstellung in Abbildung 5-2 wurden die im Folgenden optimierten Faktoren Authentifizierungsmerkmale ($m_{1...n}$), -verfahren ($v_{1...n}$) und -systeme ($s_{1...n}$) in Abbildung 5-4 grau hinterlegt.

5.3.2 Sicht der Organisationen (Betreiber)

Für Organisationen und Betreiber ergibt sich im Vergleich zur im vorherigen Abschnitt beschrieben Sicht einzelner Benutzer ein komplexerer Graph bei der Abbildung der Authentifizierung in heterogenen IT-Strukturen. Abbildung 5-5 zeigt einen exemplarischen Graphen für die kooperierenden Organisationen o_1 und o_n aus Abbildung 5-2, die die Quellen des Graphen bilden. Die Organisation o_1 stellt ihren Benutzern vier Ressourcen (r_1, r_i, r_j und r_k) zur Verfügung. Dabei wird die Ressource r_k gemeinsam mit der Organisation o_n betrieben und angeboten. Organisation o_n bietet in dem in Abbildung 5-5 gezeigten Beispiel drei Ressourcen (r_k, r_l und r_n) an. In Abbildung 5-5 wurden die Kanten zwischen Ressourcen und Authentifizierungssystemen grau dargestellt, da sie für die Vereinheitlichung und Optimierung der Authentifizierung in heterogenen IT-Strukturen nicht betrachtet werden. Vereinheitlicht wird ausschließlich die erforderliche Authentifizierung für die Ressourcen, nicht aber der Betrieb bzw. die Anzahl der angebotenen Ressourcen.

Abbildung 5-5 zeigt die Ressource r_i, die an die Authentifizierungssysteme s_1 und s_i angebunden ist. An den Betrieb der Ressourcen stellen die Organisationen unterschiedliche Sicherheitsanforderungen, die durch das variable Kantengewicht S zwischen Ressourcen und Organisationen dargestellt werden. Um die Sicherheitsanforderungen einzuhalten und umzusetzen, ist hierbei ein zusätzlicher Aufwand beim Betrieb der Ressource erforderlich, der als Kantengewicht A betrachtet wird. Im Gegensatz zu den Kanten zwischen Organisationen und Ressourcen gehen die Kanten zwischen Ressourcen und Authentifizierungssystemen in die folgende Optimierung ein, da sich Aufwand und erzielte Sicherheit hierbei vorrangig auf die Authentifizierung beziehen. Ohne jegliche Authentifizierung würde dieser Aufwand nicht erforderlich, aber auch die erzielte Sicherheit nicht erreicht. Beispielsweise resultiert der Gesamtaufwand für den Betrieb der in Abbildung 5-5 gezeigten Ressource r_i hinsichtlich der Authentifizierung aus dem Aufwand der beiden Kanten zu den Authenti-

---

[475] Vgl. GERD TOM MARKOTTEN, D.: Benutzbare Sicherheit in informationstechnischen Systemen, 2003, S. 76 ff.

fizierungssystemen s_1 und s_i. Authentifizierungssysteme ($s_{1...n}$) setzen wiederum verschiedene Authentifizierungsverfahren ($v_{1...n}$) ein, um die Authentifizierung der Benutzer anhand von deren Authentifizierungsmerkmalen ($m_{1...n}$) durchzuführen. Aufwand und erzielte Sicherheit der Authentifizierungsverfahren und -merkmale werden hierbei erneut als variable Kantengewichte *A* und *S* definiert.

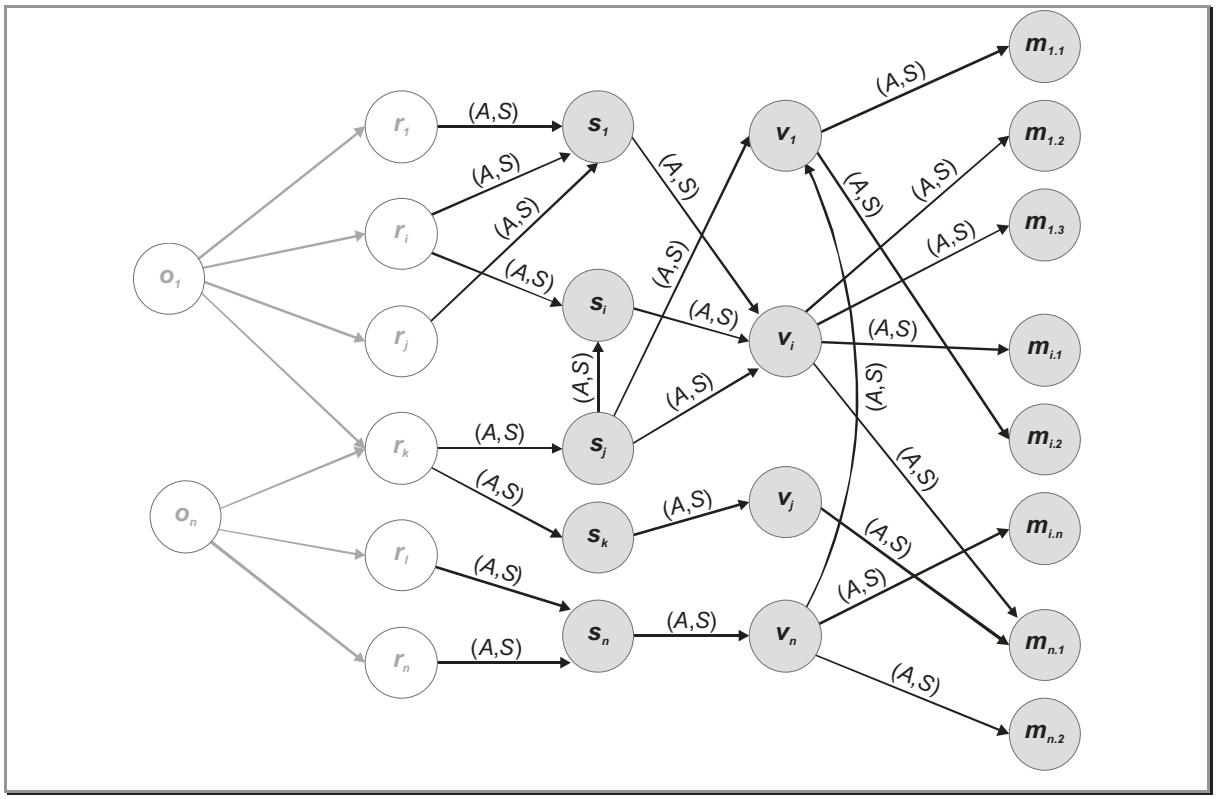

Abbildung 5-5: Authentifizierung in heterogenen IT-Strukturen als gerichteter Graph aus Sicht der Betreiber

Als Senken des in Abbildung 5-5 gezeigten Graphen werden die Authentifizierungsmerkmale betrachtet. Im vorherigen Abschnitt sowie in Abbildung 5-2 wurden diese Authentifizierungsmerkmale zusätzlich Benutzern zugeordnet. Benutzer werden aus Sicht der Organisationen jedoch für die folgende Optimierung vorrangig durch ihre Authentifizierungsmerkmale resp. zugehörige Authentifizierungskonten[476] repräsentiert. Der Aufwand für den Betrieb einer Ressource in Bezug auf die Authentifizierung entsteht hierbei durch die Verwaltung der Authentifizierungsmerkmale der Benutzer; eine Optimierung der Menge der Benutzer beispielsweise durch die Zuweisung eines Authentifizierungsmerkmals zu mehreren Benutzern ist nicht zielführend, da hierbei keine individuelle Sicherheit für die Benutzer sowie keine Unterscheidung der Identitäten möglich ist.[477] Für

[476] Wie sie in Abschnitt 2.1.7 definiert wurden.

[477] Vgl. die in Abschnitt 2.1.4 geforderte eindeutige Identifizierung von Benutzern und Identitäten.

den Betriebsaufwand ist aus Sicht der Organisationen zudem weniger entscheidend, wie viele Authentifizierungsmerkmale ein einzelner Benutzer besitzt, als vielmehr die Anzahl der verwalteten Authentifizierungsmerkmale insgesamt. Als Einschränkung gilt hierbei im Folgenden jedoch die Minderung der Sicherheit, z.B. aufgrund der geringeren Akzeptanz einer hohen Diversität von Authentifizierungsmerkmalen aus Sicht der Benutzer, wie in Abschnitt 4.1.2 dargestellt.

Der in Abbildung 5-5 skizzierte Graph beschreibt die Authentifizierung aus Sicht der Organisationen als Fluss über die angebotenen Ressourcen, notwendigen Authentifizierungssysteme und -verfahren hin zu den Authentifizierungsmerkmalen der Benutzer. Durch die Richtung der Kanten im in Abbildung 5-5 skizzierten Graphen wird die Relevanz der Optimierung beteiligter Faktoren aus Sicht der Organisationen bestimmt. Sie nimmt von den Quellen aus in Richtung der Senken ab. Durch die Reduktion bzw. Integration von Authentifizierungssystemen lassen sich beispielsweise im Idealfall auch verbundene Authentifizierungsverfahren und -merkmale reduzieren. Im Beispiel in Abbildung 5-5 lässt sich dies an der Reduktion des Systems s_j beschreiben, die eine Verringerung des Betriebsaufwands von s_i und v_i sowie zusätzlich eine Reduktion von v_1 und $m_{1.1}$ ermöglicht. Authentifizierungssysteme erhalten somit für die Vereinheitlichung der Authentifizierung aus Sicht der Betreiber bzw. Organisationen eine höhere Relevanz als Authentifizierungsverfahren und -merkmale.

Durch die Reduktion der verwendeten Authentifizierungssysteme, -verfahren und -merkmale verringert sich der Aufwand für den Betrieb der Ressourcen. Im Graphen wird dies durch die resultierende Verringerung der Gesamtsumme der Kantengewichte A deutlich.[478] Während hierbei auch die Gesamtsumme des Kantengewichts S verringert wird, wird dies nicht als Verminderung der erzielten Sicherheit definiert. Vorgabe für die folgenden Optimierungen ist stattdessen die individuelle Maximierung der einzelnen Kantengewichte S oder die Sicherung eines Mindestwertes über alle Flüsse des Graphen. Das maximal erzielbare Sicherheitsniveau wird durch das Minimum der enthaltenen Kantengewichte definiert.[479]

Die im Folgenden optimierten Faktoren Authentifizierungssysteme ($s_{1...n}$), -verfahren ($v_{1...n}$) und -merkmale ($m_{1...n}$) wurden in Abbildung 5-5 analog zu ihrer Darstellung in Abbildung 5-2 grau hinterlegt.

---

[478] Vgl. Summen der Kantengewichte in Abbildung 5-5.

[479] Vgl. GERD TOM MARKOTTEN, D.: Benutzbare Sicherheit in informationstechnischen Systemen, 2003, S. 75, sowie Abschnitt 6.1.2.

5.4 Quantifizierung des Aufwands und der erzielten Sicherheit

Um eine Optimierung anhand der im Abschnitt 5.2 eingeführten Kantengewichte *A* und *S* durchzuführen, müssen diese quantifiziert werden. Für die Quantifizierung der Sicherheit existieren bereits internationale Vorgaben und Richtlinien, wie bereits in Abschnitt 2.3 ausgeführt. Die Quantifizierung des Aufwands ist Gegenstand der aktuellen Forschung im Umfeld der IT-Sicherheit. Im Abschnitt 5.4.1 werden Modelle für die Bewertung genannt, die anschließend im Abschnitt 5.4.2 für die Verwendung hinsichtlich der Bewertung und Optimierung der Authentifizierung in heterogenen IT-Strukturen erweitert werden.

5.4.1 Bestehende Bewertungsmodelle

RENAUD beschreibt ein Bewertungsmodell für Authentifizierungsverfahren, das für die Bewertung von Authentifizierungsmerkmalen und Authentifizierungssystemen erweitert werden kann.[480] Dieser Abschnitt stellt die Dimensionen und Faktoren der Bewertung nach RENAUD vor und bildet damit das Grundgerüst für die Auswahl von Verfahren für die Integration und Vereinheitlichung des in Abbildung 5-2 gezeigten Modells.

Alternativen zur Verwendung des Bewertungsverfahrens nach RENAUD existieren beispielsweise in Evaluationsverfahren für IT-Sicherheit.[481] Kriterien für die Benutzbarkeit von IT-Sicherheit und deren Bewertung beschreiben zusätzlich GERD TOM MARKOTTEN und die von CRANOR UND GARFINKEL vorgestellten Paper zum Thema „Security & Usability".[482] Allgemeine Anforderungen an Bewertungsverfahren für IT-Sicherheit, neben den in Abschnitt 2.3 genannten Vorgaben, beschreibt SCHNEIER.[483] ANDERSON liefert neben der Bewertung IT-Sicherheits-Systemen auch Kriterien zur Wartbarkeit und Wirtschaftlichkeit.[484] Für die allgemeine Bewertung der Qualität von Software und damit auch der Authentifizierung besteht die Norm ISO/IEC 9126, deren Kriterien im nächsten Abschnitt genannt werden. Das enthaltene Kriterium der Benutzbarkeit ist zusätzlich in

---

[480] Vgl. RENAUD, K.: Quantifying the Quality of Web-Authentication Mechanisms. A Usability Perspektive, in Journal of Web Engineering 3(2), 2003, S. 95 ff.

[481] Vgl. NISO: Ranking of Authentication and Access Methods Available to the Metasearch Environment, 2005; BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: Authentifizierung im E-Government, 2005; Future of Identity in the Information Society (FIDIS) Deliverables, 2007.

[482] Vgl. GERD TOM MARKOTTEN, D.: Benutzbare Sicherheit in informationstechnischen Systemen, 2003; CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005.

[483] Vgl. SCHNEIER, B.: Secrets & Lies, 2004, S. 139 ff.; SCHNEIER, B.: Beyond Fear, 2003, 3 ff., 47 ff., 181 ff.

[484] Vgl. ANDERSON, R.: Security Engineering. A Guide to Building Dependable Distributed Systems, 2001, S. 512; Economics and Security Resource Page, 2007.

der Norm DIN EN ISO 9241 Teil 10[485] beschrieben, deren Relevanz GERT TOM MARKOTTEN bewertet und geeignet erweitert.[486]

Für die Bewertung von IT-Sicherheit existieren zusätzlich unterschiedliche Bewertungsverfahren, die bereits in Abschnitt 2.3 vorgestellt wurden. Speziell für die Authentifizierung sieht beispielsweise die Common Criteria Leitlinie den Abschnitt FIA (Identifikation und Authentisierung)[487] vor. Allerdings beziehen sich die in Abschnitt 2.3.1 genannten nationalen und internationalen Richtlinien für IT-Sicherheit nur auf die Bewertung der zu gewährleistenden Sicherheit, nicht aber auf den damit verbundenen Aufwand. Für eine Bewertung der in Abschnitt 5.3 genannten Modelle decken sie somit nur die Kantengewichte *S* für die erzielte Sicherheit ab. Zusätzlich liefern diese Richtlinien keine Quantifizierung oder Metrik, die für die anschließende Optimierung der betrachteten Kantengewichte erforderlich ist.

Das in diesem Abschnitt skizzierte Bewertungsverfahren für Authentifizierungsverfahren nach RENAUD bildet die Grundlage für die folgende Bewertung und Vereinheitlichung der Authentifizierung in heterogenen IT-Strukturen. Es wird jedoch im Abschnitt 5.4.2 erweitert, da RENAUD zum einen ausschließlich die Kriterien aus Sicht der Benutzer (nicht der Organisationen als Betreiber) fixiert, und zum anderen auf oben genannte Kriterien aus Richtlinien und Standards zur IT-Sicherheit und Benutzbarkeit verzichtet.

RENAUD gliedert die Bewertung der Qualität von Authentifizierungsverfahren in vier Kriterien:

- Zugänglichkeit (accessibility)
- Einprägsamkeit (memorability)
- Kosten (cost)
- Sicherheit (security)

Für jedes dieser Kriterien unterscheidet RENAUD verschiedene Dimensionen, die dessen Qualität bestimmen.

---

[485] ISO 9241-11:1998: Ergonomic requirements for office work with visual display terminals (VDTs) -- Part 11: Guidance on usability, 1998; GERD TOM MARKOTTEN, D.: Benutzbare Sicherheit in informationstechnischen Systemen, 2003, S. 47 ff.

[486] Vgl. GERD TOM MARKOTTEN, D.: Benutzbare Sicherheit in informationstechnischen Systemen, 2003, S. 69 ff.

[487] Vgl. BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: Common Criteria. Version 2.3, 2006.

5.4.1.1 Aufwand der Authentifizierung als Defizit

Die Kriterien „Zugänglichkeit", „Einprägsamkeit" und Kosten (cost) des von RENAUD eingeführten Modells lassen sich als für die Authentifizierung erforderlicher Aufwand zusammenfassen. Für die „Zugänglichkeit" (accessibility) definiert RENAUD die Dimensionen als „spezielle Anforderungen" (special requirements), die für die Authentifizierung und deren Verwaltung benötigt werden, die „Bequemlichkeit" (convenience) in Bezug auf die Verwendung und Verwaltung des Authentifizierungsverfahrens sowie dessen „Barrierefreiheit" (inclusivity) bzw. die erfolgreiche Verwendung des Authentifizierungsverfahrens unabhängig von Behinderungen der Benutzer. Je mehr Eigenschaften oder Einschränkungen in den Dimensionen auftreten, desto höher ist gemäß RENAUD das Defizit des Verfahrens in Bezug auf dessen Zugänglichkeit zu bewerten. RENAUD bezieht die Zugänglichkeit des Verfahrens sowohl auf die Benutzer als auch auf die Betreiber bzw. Organisationen, die ihrerseits z.B. spezielle Soft- und Hardware für das Authentifizierungsverfahren anbieten müssen. Die Abbildung 5-6 illustriert die genannten Dimensionen der Zugänglichkeit:

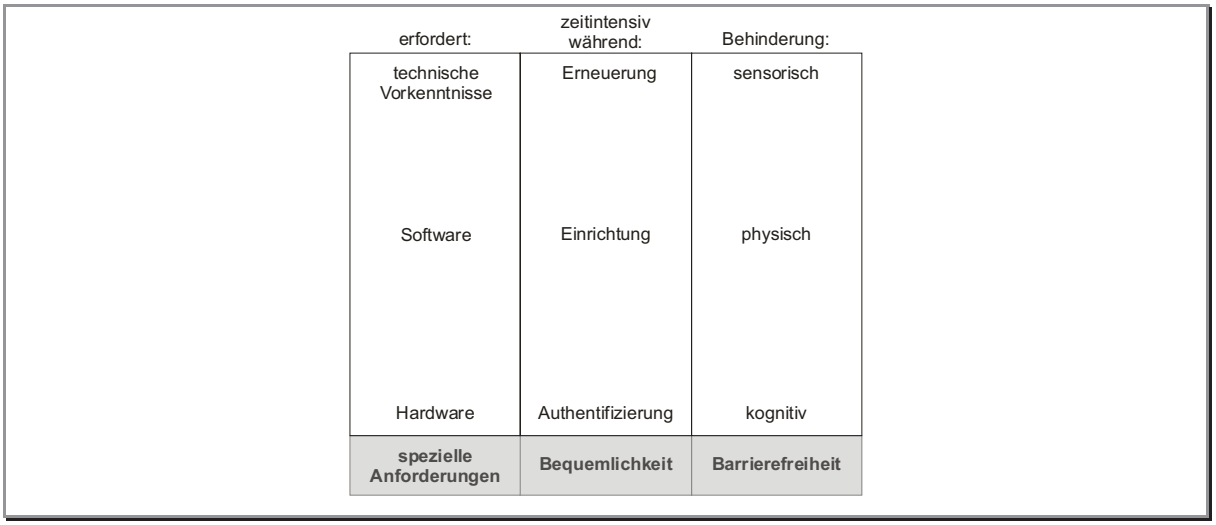

Abbildung 5-6: Zugänglichkeit von Authentifizierungsverfahren[488]

Für die Einprägsamkeit des Authentifizierungsverfahrens bzw. -merkmals nennt RENAUD die Dimensionen „Verarbeitungstiefe" (depth of processing) als Maß für die erforderliche Einprägung des gewählten Authentifizierungsmerkmals während dessen Einrichtung, die „Abrufbarkeit" (retrieval strategy) des gewählten Merkmals bei seiner späteren Verwendung sowie die „Aussagefähigkeit" (meaningfulness) des Merkmals für den Benutzer. Das Defizit in Bezug auf die Einprägsamkeit eines Authentifizierungsverfahrens steigt gemäß der Abbildung 5-7 nach RENAUD mit zunehmender Unzulänglichkeit der skizzierten Dimensionen.

[488] Nach RENAUD, K.: Evaluating Authentication Mechanisms, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 116.

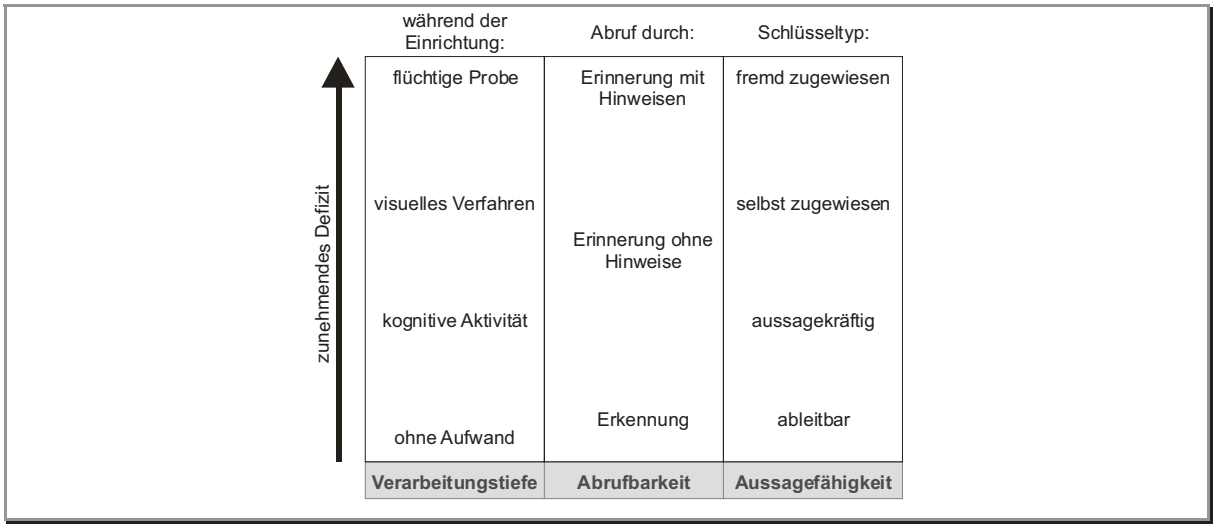

Abbildung 5-7: Einprägsamkeit von Authentifizierungsverfahren[489]

Als generelles Kriterium für die Bewertung von Authentifizierungsverfahren nennt RENAUD die Kosten für Verwendung und Verwaltung des Verfahrens. Die Kosten umfassen dabei folgende Dimensionen:

- Software (z.B. speziell für ein Authentifizierungsverfahren erforderlich)
- Hardware (z.B. speziell für ein Authentifizierungsverfahren erforderlich)
- Einrichtung (von Benutzern und deren Merkmalen)
- Authentifizierung (Kosten des Vorgangs)
- Schlüsselerneuerung (z.B. bei Schlüsselverlust, -verfall)
- Schutz des Schlüssels (vor physikalischem Zugriff durch unberechtigte Dritte)
- Verwaltung (z.B. Backup, Verfall, Widerruf, aber auch des Verfahrens selbst)

5.4.1.2 Sicherheit der Authentifizierung als Defizit

RENAUD bewertet zusätzlich das Kriterium der „Sicherheit“ (security) in Bezug auf das evaluierte Authentifizierungsverfahren. Hierbei werden als Dimensionen die „Vorhersagbarkeit“ (predictability) in Bezug auf das Authentifizierungsmerkmal aus der Sicht Dritter und die „Fülle“ (abundance) unterschieden, die insbesondere eine Aussage über die Anzahl der möglichen Schlüsselwechsel (z.B. Verfall) angibt, bevor erneut ein bereits zuvor genutzter Schlüssel verwendet werden muss. Weiterhin wird die „Offenlegung“ (disclosure) des erforderlichen Schlüssels während nachfolgen-

[489] Nach RENAUD, K.: Evaluating Authentication Mechanisms, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 118.

den Authentifizierungsvorgängen sowie die „Angreifbarkeit“ (breakability and crackability), z.B. durch Schwachstellen im Verfahren, die einen Angriff oder ein simples mehrfaches Probieren sämtlicher möglicher Schlüssel („brute force“) darstellen können, als Kriterium für die Sicherheit beschrieben.

„Datenschutz“ (privacy) als Dimension für die Offenlegung von privaten Daten des Benutzers gegenüber den Organisationen oder Dritten sowie die „Vertraulichkeit“ (confidentiality) in Bezug auf die Offenlegung des erforderlichen Schlüssels während der Authentifizierung bilden die abschließenden Dimensionen des Kriteriums Sicherheit. Analog zur Abbildung 5-7 steigt das Defizit der Dimensionen mit deren zunehmender Unzulänglichkeit, wie Abbildung 5-8 zusätzlich verdeutlicht.

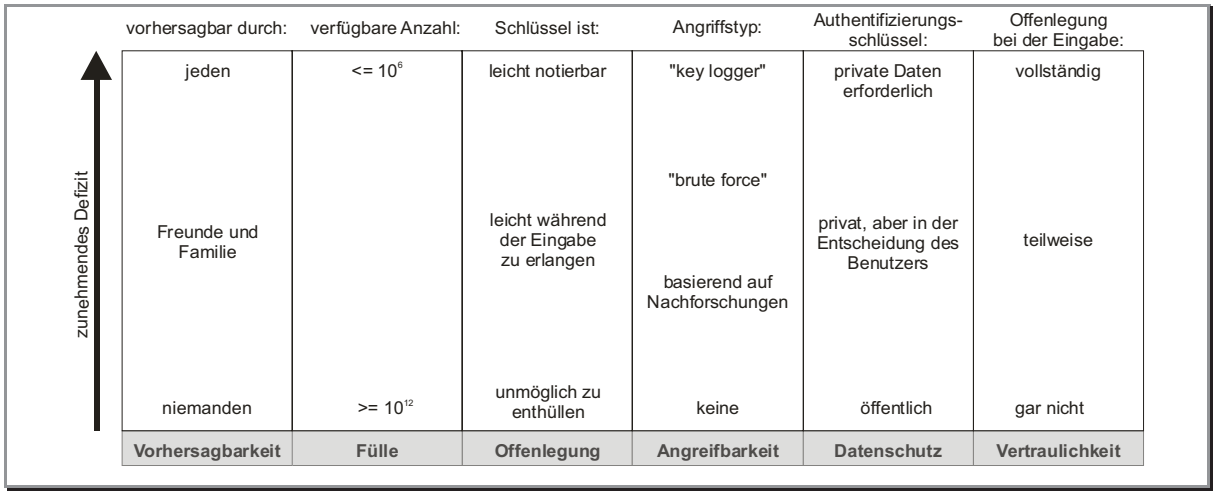

Abbildung 5-8: Sicherheit von Authentifizierungsverfahren[490]

5.4.1.3 Berechnung des Gesamtdefizits

RENAUD berechnet für die Bewertung von Authentifizierungsverfahren das Gesamtdefizit der genannten Kriterien durch die Summierung in den vorherigen beiden Abschnitten genannten Defizite. Diese Defizite werden durch die einzelnen Aspekte, die Bestandteil der betrachteten Dimension eines Kriteriums sind, bestimmt. Beispielsweise kann die Dimension „Spezielle Anforderungen“, wie in Abbildung 5-6 dargestellt, als maximales Defizit den Wert 1 erhalten, sofern alle drei Anforderungen (spezielle technische Vorkenntnisse, Software und Hardware) erforderlich sind. Werden keine speziellen Anforderungen gestellt, so umfasst die Dimension ein Defizit mit dem Wert 0. Dementsprechend entsteht ein Defizit von 0,33 bei einem sowie 0,66 bei zwei erforderlichen Aspekten. Bei der Betrachtung von Einprägsamkeit und Sicherheit entsteht das Defizit nicht durch die

[490] Nach RENAUD, K.: Evaluating Authentication Mechanisms, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 119.

Summe der innerhalb der Dimension betroffenen Aspekte, sondern durch den einzelnen, zutreffenden Aspekt. Ist ein Authentifizierungsmerkmal beispielsweise für niemanden außer dem Benutzer selbst vorhersagbar, so erhält das Defizit der Dimension Vorhersagbarkeit ein Defizit mit dem Wert 0.[491] Ist es für Freunde oder Familienangehörige möglich, die Information vorherzusagen, steigt das Defizit auf den Wert 0,5. Als maximales Defizit entsteht der Wert 1, sofern die Information für jeden Dritten leicht vorhersagbar ist.

Für das Gesamtdefizit der einzelnen Dimensionen ($\overline{n}$) wird folgende Formel verwendet:[492]

$$\overline{n} = \sqrt{x^2 + y^2 + z^2}$$

x, *y* und *z* werden hierbei z.B. beim Kriterium Zugänglichkeit durch die Dimensionen *Spezielle Anforderungen*, *Bequemlichkeit* und *Barrierefreiheit* gebildet, die als maximales Defizit jeweils den Wert 1 aufweisen. Das Maximum für $\overline{n}$ ist somit $\sqrt{3} \approx 1{,}73$. Ein maximales Defizit einer einzelnen Dimension besitzt durch die definierte Formel einen Einfluss von 57,7%, zwei maximal defizitäre Dimensionen einen Einfluss von 81,6% auf das Gesamtergebnis. Dadurch hat bereits ein maximales Defizit einer enthaltenen Dimension größeren Einfluss auf das Gesamtergebnis als mehrere geringfügig defizitäre Dimensionen.[493]

Das Gesamtdefizit der Kriterien und damit des betrachteten Authentifizierungsverfahrens ($\overline{d}$) definiert RENAUD als

$$\overline{d} = ad + md + sd + vd$$

wobei *ad* das Defizit der Zugänglichkeit (*accessibility*) und *md* das Defizit der Einprägsamkeit (*memorability*) angibt. Die in Abbildung 5-8 gezeigten Dimensionen für das Defizit der Sicherheit (security) unterteilt RENAUD für die Berechnung in das Defizit *sd*, das die Dimensionen *Vorhersagbarkeit*, *Fülle* und *Offenlegung* umfasst, sowie das Kriterium Verwundbarkeit (vulnerability) *vd*, das die Dimensionen *Angreifbarkeit*, *Datenschutz* und *Vertraulichkeit* umfasst. Insgesamt ergibt sich durch das oben genannte Maximum für $\overline{n}$ ein maximales Defizit $\overline{d}$ eines betrachteten Verfahrens von $1{,}73 * 4 \approx 6{,}92$.

---

[491] Vgl. zunehmendes Defizit in Abbildung 5-8.

[492] Vgl. RENAUD, K.: Quantifying the Quality of Web-Authentication Mechanisms. A Usability Perspektive, S. 13.

[493] Wie in RENAUD, K.: Quantifying the Quality of Web-Authentication Mechanisms. A Usability Perspektive, S. 13 gefordert.

Zusätzlich definiert RENAUD äußere Faktoren (*environmental factors*), die verstärkend (Faktor 1,5) oder abschwächend (Faktor 0,5) auf die Defizite der Kriterien einwirken können. Daraus ergibt sich abschließend die Formel:[494]

$$\overline{d_{env}} = ad * control + md * freq * renewal + sd * access * motive + vd * audit$$

Hierbei bezieht *control* (in Bezug auf die Zugänglichkeit) die mögliche Kontrolle resp. Absicherung der Umgebung, innerhalb derer die Authentifizierung erfolgt, ein. Unkontrollierte Umgebungen erhalten den Faktor 1,5, kontrollierte den Faktor 1. Die Einprägsamkeit wird durch *freq* (Frequentierung des Verfahrens) und *renewal* (Erzwungene Erneuerung des Authentifizierungsmerkmals) beeinflusst. Tägliche Anwendung der Authentifizierung erhält den Faktor *freq* 0,5, wöchentliche Faktor 1 und monatliche oder größer den Faktor 1,5. Sofern keine regelmäßige Erneuerung der Authentifizierungsmerkmale erforderlich ist, wird der Faktor *renewal* als 1, andernfalls als 1,5 definiert.

Hat ein unberechtigter Zugriff durch Dritte keinen Schaden für den rechtmäßigen Benutzer zur Folge, wird der Faktor *access* mit 0,5 bewertet. Tritt hierbei ausschließlich ein Schaden für den betroffenen Benutzer auf, so wird der Faktor *access* mit 1, bei einem resultierenden Schaden für mehrere Benutzer mit 1,5 belegt. Der Faktor *motive* wird als 1 definiert, sofern Benutzern die Einhaltung von Sicherhaltsvorgaben auferlegt werden kann, andernfalls beträgt der Faktor 1,5.[495]

Die Verwundbarkeit wird durch den Faktor *audit* beeinflusst, der mit dem Wert 1,5 belegt wird, sofern keine Überwachung bzw. Auditierung der Authentifizierung erfolgt und ansonsten den Wert 1 erhält.

5.4.2 Erweiterte Bewertung des Aufwands in heterogenen IT-Strukturen

Im vorherigen Abschnitt wurde das Bewertungsmodell von RENAUD genannt, das sich speziell auf Authentifizierungsverfahren bezieht und eine Quantifizierung von deren Defiziten beinhaltet. Wie im vorherigen Abschnitt erläutert, umfasst das Modell zudem bereits Aspekte zur Bewertung des Aufwands durch die Authentifizierung. Es wird daher als Grundlage für die Bewertung der Faktoren einer einheitlichen Authentifizierung in heterogenen IT-Strukturen verwendet und in diesem Abschnitt entsprechend erweitert.

---

[494] Vgl. RENAUD, K.: Quantifying the Quality of Web-Authentication Mechanisms. A Usability Perspektive, S. 15.

[495] Nach RENAUD, K.: Quantifying the Quality of Web-Authentication Mechanisms. A Usability Perspektive, S. 14.

Wie in Abschnitt 5.3 erläutert, werden für die Bewertung und anschließende Optimierung der Authentifizierung in heterogenen IT-Strukturen der Aufwand und die erzielte Sicherheit als Kantengewichte der Graphen aus Sicht der Benutzer und Betreiber resp. Organisationen definiert.[496] Aufwand entsteht hierbei für Benutzer und Betreiber jeweils bei der Verwendung der Authentifizierung sowie bei der Verwaltung der Authentifizierungsmerkmale, -verfahren und -systeme. Die Verwendung umfasst hierbei den Aufwand, der innerhalb des Zeitraums, in dem die Authentifizierung durchgeführt wird, auftritt. Aufwand, der außerhalb dieses Zeitraums, z.B. für die Speicherung von Authentifizierungsinformationen oder deren Wartung erforderlich ist, wird unter Verwaltung erfasst.

Um eine Bewertung und anschließende Optimierung des Aufwands zu erreichen, müssen die betrachteten Faktoren einer einheitlichen Authentifizierung qualitativ vergleichbar sein. Basis für den Vergleich bildet die Quantifizierung der Qualität von Authentifizierungsmerkmalen, -verfahren und -systemen. Als Maß für die Qualität von Software definiert die ISO/IEC-Norm 9126[497], die auf den Modellen von MCCALL UND BOEHM basiert, sechs Kriterien:[498]

- Funktionalität (Functionality)
- Zuverlässigkeit (Reliability)
- Benutzbarkeit (Usability)
- Effizienz (Efficiency)
- Wartbarkeit (Maintainability)
- Portabilität (Portability)

Ein Modell für die Quantifizierung dieser Kriterien bzw. der Qualität allgemein liefert GILB.[499] GILB regt dabei an, die Quantifizierung auf bestehenden Skalen und Metriken aufzubauen, und diese zu modifizieren bzw. zu erweitern.[500] Skalen umfassen hierbei die eigentliche Quantifizierung (beispielsweise prozentuale Erfüllung einer Anforderung). Metriken beschreiben nach GILB Methoden, um die numerischen Werte innerhalb der definierten Skalen, z.B. für die Qualitätsmessung zu gewinnen. GILB gliedert Skalen und Metriken einer Betrachtung in elementare Aspekte, deren individuelle Skalen in die Gesamtbewertung einfließen. Im Folgenden werden die elementa-

[496] Vgl. auch die Beispiele in Abbildung 5-4 und Abbildung 5-5.

[497] Vgl. ISO 9126: Software Engineering - Product Quality, 2001.

[498] Vgl. FOLMER, E.: Software architecture analysis of usability, 2005, S. 19 ff.

[499] Vgl. GILB, T.: Competitive Engineering, 2005, S. 137 ff.

[500] Beschreibung von Skalen und Metriken vgl. GILB, T.: Competitive Engineering, 2005, S. 137 ff.

ren Aspekte des Aufwands sowie der erzielten Sicherheit in Bezug auf die Authentifizierung in heterogenen IT-Strukturen genannt. Als Grundlage für die Metrik dient das Bewertungsmodell für Authentifizierungsverfahren nach RENAUD. Ziel für die Definition der Metriken bilden die in Abschnitt 4.1 genannten Anforderungen.[501]

In die Bewertung des Aufwands werden zusätzlich die genannten sechs Kriterien für Software-Qualität nach ISO/IEC 9126 integriert.[502] Dabei wird eine qualitative Einschränkung der Kriterien als eine Erhöhung des Aufwands für Benutzer und Organisationen als Betreiber betrachtet. Der Aufwand wird gemäß Abschnitt 5.3 jeweils aus Sicht der Benutzer sowie der Organisationen als Betreiber bewertet. Jede Sichtweise gliedert sich in unterschiedliche Aspekte, die den Aufwand bestimmen. Einzelne Aspekte werden minimal mit einem Aufwand von 0, maximal mit einem Aufwand von 1 bewertet. Den konkreten Wert eines Aspekts definieren dessen Teilaspekte, die entweder in der Summe den Wert 1 ergeben oder einen Bruchteil des Maximalwerts bilden.

5.4.2.1 Aufwand für die Verwendung seitens der Benutzer

Grundlage für die Bewertung des Aufwands während der Verwendung der Authentifizierung durch die Benutzer liefert die Benutzbarkeit.[503] Als Metrik hierfür dienen die bestehenden Aspekte der Zugänglichkeit (Accessibility).[504]

Aspekt: Spezielle Anforderungen ($A_{b.sa}$)

Quantifizierung des Aufwands: Anteil der für die Authentifizierung erforderlichen speziellen Anforderungen ($0 \leq A_{b.sa} \leq 1$)		
Teilaspekte	**Beschreibung**	**Bewertung**
Technische Vorkenntnisse	Erhöhter Aufwand, sofern spezielle technische Kenntnisse für die erfolgreiche Verwendung der Authentifizierung erforderlich sind.	$A_{b.sa}$ + 0,33
Software	Zusätzlicher Aufwand, sofern die Authentifizierung spezielle Software voraussetzt.	$A_{b.sa}$ + 0,33
Hardware	Zusätzlicher Aufwand, sofern die Authentifizierung spezielle Hardware voraussetzt.	$A_{b.sa}$ + 0,33

Tabelle 5-1: Aufwand durch spezielle Anforderungen für die Benutzer[505]

[501] In Anlehnung an GILB, T.: Competitive Engineering, 2005, S. 163 ff.

[502] Vgl. ISO 9126: Software Engineering - Product Quality, 2001.

[503] Vgl. GERD TOM MARKOTTEN, D.: Benutzbare Sicherheit in informationstechnischen Systemen, 2003, S. 35 ff.

[504] Vgl. RENAUD, K.: Evaluating Authentication Mechanisms, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 115 ff.

[505] Basierend auf RENAUD, K.: Evaluating Authentication Mechanisms, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 116.

Aspekt: Bequemlichkeit ($A_{b.beq}$)

Quantifizierung des Aufwands: Anteil der erforderlichen Teilaspekte mit hohem Zeitaufwand ($0 \leq A_{b.beq} \leq 1$)		
Teilaspekte	**Beschreibung**	**Bewertung**
Authentifizierung	Erhöhter Aufwand, sofern der Vorgang der Authentifizierung zeitintensiv bzw. komplex ist.	$A_{b.beq}$ + 0,33
Diversität der Authentifizierung	Zusätzlicher Aufwand, sofern die Authentifizierung keine Integration mit anderen Faktoren (z.B. Authentifizierungsmerkmalen des Benutzers) unterstützt.	$A_{b.beq}$ + 0,33
Diversität der Verwendung	Zusätzlicher Aufwand, sofern die betrachtete Authentifizierung innerhalb einer Sitzung des Benutzers mehrfach erfolgt und keine Integration der Vorgänge (Single Sign-On) unterstützt wird.	$A_{b.beq}$ + 0,33

Tabelle 5-2: Aufwand durch fehlende Bequemlichkeit[506]

Die Teilaspekte *Einrichtung* und *Erneuerung* werden anders als bei RENAUD der Verwaltung durch die Benutzer zugeordnet, da sie keinen Zeitaufwand während der Verwendung zur Folge haben.

Unter dem Teilaspekt Authentifizierung wird ergänzend zur Definition durch RENAUD auch der Aufwand durch komplexe, z.B. auf mehreren Faktoren basierende Authentifizierungsverfahren erfasst.[507] Für die Bewertung des Aufwands in heterogenen IT-Strukturen wurden die Teilaspekte *Diversität des Merkmals* und *Diversität der Verwendung* eingeführt. Unter der Diversität des Merkmals wird die fehlende Integration mit anderen Faktoren des gleichen Typs verstanden. Dies ist beispielsweise der Fall, sofern sich ein Authentifizierungsmerkmal nicht mit anderen Authentifizierungsmerkmalen synchronisieren resp. integrieren lässt bzw. für jede Anwendung und Ressource ein eigenes Passwort erforderlich ist.[508]

Die Diversität der Verwendung stellt ein Defizit dar, sofern das betrachtete Verfahren, Merkmal oder System innerhalb der Sitzung eines Benutzers mehrere Authentifizierungen erfordert bzw. kein „Single Sign-On" bietet.[509] Dieser Aspekt wird auch von SMITH für die Betrachtung des Aufwands der Authentifizierung verwendet.[510]

---

[506] Erweitert basierend auf RENAUD, K.: Evaluating Authentication Mechanisms, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 116 f.

[507] Vgl. Eigenschaften von Authentifizierungsverfahren in Abschnitt 2.1.8.

[508] Vgl. Single-Password in Abschnitt 4.1.1; SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 115 f.

[509] Vgl. Die Definition von Single Sign-On in Abschnitt 2.1.12.

[510] Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 115 ff.

Aspekte: Barrierefreiheit ($A_{b.bar}$)

Quantifizierung des Aufwands: Anteil der nicht berücksichtigten Behinderungen resp. Teilaspekte ($0 \leq A_{b.bar} \leq 1$)		
Teilaspekte	**Beschreibung**	**Bewertung**
Sensorisch	Erhöhter Aufwand, sofern die Authentifizierung nicht mit sensorischen Behinderungen (z.B. Sehstörungen, Taubheit) erfolgreich durchgeführt werden kann.	$A_{b.bar}$ + 0,33
Physisch	Zusätzlicher Aufwand, sofern die Authentifizierung nicht mit physischen Behinderungen (z.B. Amputation, körperliche Einschränkung) erfolgreich durchgeführt werden kann.	$A_{b.bar}$ + 0,33
Kognitiv	Zusätzlicher Aufwand, sofern die Authentifizierung nicht mit kognitiven Behinderungen (z.B. Legasthenie, Vergesslichkeit) erfolgreich durchgeführt werden kann.	$A_{b.bar}$ + 0,33

Tabelle 5-3: Aufwand durch fehlende Barrierefreiheit[511]

5.4.2.2 Aufwand für die Verwendung seitens der Organisationen

Während das Kriterium der Zugänglichkeit sich nach RENAUD vorrangig auf die Verwendung durch den Benutzer bezieht, werden im folgenden Aspekte der Verwendbarkeit aus Sicht der Organisatoren als Betreiber betrachtet. Dabei werden Kriterien der ISO/IEC 9126 für Software-Qualität wie Wartbarkeit, Effizienz und Portabilität integriert.

Aspekt: Spezielle Anforderungen ($A_{o.sa}$)

Quantifizierung des Aufwands: Anteil der für die Authentifizierung erforderlichen speziellen Anforderungen ($0 \leq A_{o.sa} \leq 1$)		
Teilaspekte	**Beschreibung**	**Bewertung**
Kenntnisse	Erhöhter Aufwand, sofern für die Anwendung der Authentifizierung spezielle Kenntnisse der Administratoren erforderlich sind.	$A_{o.sa}$ + 0,25
Software	Zusätzlicher Aufwand, sofern spezielle Software für die Anwendung der Authentifizierung erforderlich ist.	$A_{o.sa}$ + 0,25
Hardware	Zusätzlicher Aufwand, sofern spezielle Hardware für die Anwendung der Authentifizierung erforderlich ist.	$A_{o.sa}$ + 0,25
Proprietäre Lösung	Zusätzlicher Aufwand, sofern die Lösung auf einem proprietären Standard basiert, der nicht von anderen Herstellern unterstützt wird.	$A_{o.sa}$ + 0,25

Tabelle 5-4: Aufwand durch spezielle Anforderungen für die Betreiber[512]

---

[511] Basierend auf „inclusivity“ nach RENAUD, K.: Evaluating Authentication Mechanisms, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 117.

[512] Erweitert basierend auf RENAUD, K.: Evaluating Authentication Mechanisms, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 116.

Durch den Teilaspekt *Proprietäre Lösung* wird die Einschränkung der Flexibilität bewertet, die innerhalb einer heterogenen IT-Struktur auftritt, sofern die Authentifizierungslösung nicht mit zukünftigen Erweiterungen, z.B. Alternativprodukten von Drittherstellern, verwendet werden kann. Diese Anforderung wird nicht nur in heterogenen IT-Strukturen, sondern auch durch das Kriterium *Portabilität* in ISO 9126 gestellt.[513]

Aspekt: Portabilität / Kompatibilität ($A_{o.po}$)

In heterogenen IT-Strukturen müssen Authentifizierungsmerkmale, -verfahren und -systeme auf unterschiedlichen Plattformen eingesetzt werden können, und diese integrieren. Das Kriterium der *Portabilität* aus ISO 9126 bildet daher eine eigene Bewertungsdimension.[514]

Quantifizierung des Aufwands:
Anteil der Teilaspekte, die die Portabilität einschränken ($0 \leq A_{o.po} \leq 1$)

Teilaspekte	Beschreibung	Bewertung
Fehlende Skalierbarkeit	Erhöhter Aufwand, sofern die Komplexität der Authentifizierung schneller als linear (z.B. exponentiell) zur Benutzerzahl wächst.[515]	$A_{o.po}$ + 0,25
Plattformabhängigkeit	Zusätzlicher Aufwand, sofern die Authentifizierung nicht auf allen Plattformen der betrachteten heterogenen IT-Struktur einsetzbar ist.	$A_{o.po}$ + 0,25
Inkompatibilität	Zusätzlicher Aufwand, sofern die Authentifizierung mit anderer innerhalb der heterogenen IT-Struktur eingesetzten Software inkompatibel ist.	$A_{o.po}$ + 0,25
Institutionsabhängigkeit	Zusätzlicher Aufwand, sofern sich die Authentifizierung nur mit hohem Aufwand institutionsübergreifend realisieren lässt.[516]	$A_{o.po}$ + 0,25

Tabelle 5-5: Aufwand durch fehlende Portabilität

Aspekt: Mobilität ($A_{o.mob}$)

Für die Bewertung in heterogenen IT-Strukturen wird die Dimension Mobilität eingeführt, um Roaming und dezentrale Nutzung der angebotenen Ressourcen zu erlauben und zu bewerten.[517] Der Teilaspekt *Eingeschränkte Web-Schnittstelle* bezieht sich beispielsweise auf die mobile Verwendung der Authentifizierung an öffentlichen Internetzugangspunkten (vgl. drahtlose Netzwerke

513 Vgl. FOLMER, E.: Software architecture analysis of usability, 2005, S. 20.

514 Vgl. FOLMER, E.: Software architecture analysis of usability, 2005, S. 20.

515 Vgl. „Multiple points of service" nach SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 117.

516 Vgl. Abschnitt 3.2.7 Federation; Abschnitt 3.2.2 Synchronisation; „Multiple enterprises" nach SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 117.

517 Vgl. Anforderungen an mobile Anwendungen in HAGENHOFF, S.; SCHUMANN, M.: Mediaconomy - Internetökonomie der Medienwirtschaft, in IT -Information Technology Nr. 48, 2006, S. 218 ff.

resp. Hot Spots oder im Internet-Café). Ist die Authentifizierung hier nicht mit Standard-Komponenten, die an jedem Ort verfügbar sind, möglich, so entsteht ein hoher Aufwand für die Verwendung.[518]

Quantifizierung des Aufwands: Anteil der Einschränkungen hinsichtlich der Mobilität ($0 \leq A_{o.mob} \leq 1$)		
Teilaspekte	**Beschreibung**	**Bewertung**
Lokale Anwendung	Erhöhter Aufwand, sofern die Authentifizierung nur lokal erfolgen kann[519]	$A_{o.mob}$ + 0,33
Eingeschränkte Web-Schnittstelle	Zusätzlicher Aufwand, sofern die Authentifizierung nicht auch über Standard Web-Browser erfolgen kann.	$A_{o.mob}$ + 0,33
Fehlende Roaming Unterstützung	Zusätzlicher Aufwand, sofern die Authentifizierung kein Roaming ohne erneute Authentifizierung bietet.	$A_{o.mob}$ + 0,33

Tabelle 5-6: Aufwand durch fehlende Mobilität

5.4.2.3 Aufwand für die Verwaltung seitens der Benutzer

RENAUD beschreibt die Einprägsamkeit (Memorability), die die Speicherung der Authentifizierungsmerkmale aus der Sicht der Benutzer bewertet und den hauptsächlichen Teil des Aufwands für die Verwaltung der Authentifizierung durch die Benutzer umfasst. Zusätzlich wurde die Dimension der Wartbarkeit eingeführt, die den Zeitaufwand für die Einrichtung und evtl. Erneuerung der Authentifizierungsmerkmale und -verfahren bewertet.

Aspekt: Wartbarkeit ($A_{b.war}$)

Quantifizierung des Aufwands: Anteil der Teilaspekte mit hohem Zeitaufwand ($0 \leq A_{b.war} \leq 1$)		
Teilaspekte	**Beschreibung**	**Bewertung**
Einrichtung	Erhöhter Aufwand, sofern die Einrichtung der Authentifizierung für Benutzer zeitintensiv ist.	$A_{b.war}$ + 0,5
Erneuerung	Zusätzlicher Aufwand, sofern die Erneuerung oder Wartung der Authentifizierung für Benutzer zeitintensiv ist.	$A_{b.war}$ + 0,5

Tabelle 5-7: Aufwand durch fehlende Wartbarkeit aus Sicht der Benutzer[520]

[518] Dieser Aspekt wird auch in SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 261 bestätigt.

[519] Vgl. „Single point of service" und „Efficient Administration" nach SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 117.

[520] Erweitert basierend auf RENAUD, K.: Evaluating Authentication Mechanisms, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 123 ff.

Aspekt: Verarbeitungstiefe ($A_{b.vt}$)

Quantifizierung des Aufwands: Grad der initialen Verarbeitung (Erlernen) des Authentifizierungsmerkmals oder -verfahrens als Maß für dessen nachhaltige Speicherung beim Nutzer ($0 \leq A_{b.vt} \leq 1$)		
Grad des Aufwands	**Beschreibung**	**Bewertung**
Flüchtige Probe	Höchster Aufwand, sofern die für die Authentifizierung notwendige Information nur flüchtig vom Benutzer abgefragt wird.	$A_{b.vt} = 1$
Visuelles Verfahren	Hoher Aufwand, sofern die Authentifizierung ausschließlich anhand (ggf. kurzzeitiger) visueller Darstellung durchgeführt wird.	$A_{b.vt} = 0{,}67$
Kognitive Aktivität	Mittlerer Aufwand, sofern die Authentifizierung ggf. durch Wiederholung langfristig im Gedächtnis verankert und erlernt wird.	$A_{b.vt} = 0{,}33$
Ohne Aufwand	Kein Aufwand, sofern kein Erlernen und Speichern erforderlich ist (z.B. Biometrie).	$A_{b.vt} = 0$

Tabelle 5-8: Aufwand für das Erlernen der Authentifizierung[521]

Aspekt: Abrufbarkeit ($A_{b.ab}$)

Quantifizierung des Aufwands: Grad des Zeitaufwand für den Abruf der gespeicherten Information zur Authentifizierung ($0 \leq A_{b.ab} \leq 1$)		
Grad des Aufwands	**Beschreibung**	**Bewertung**
Erinnerung ohne Hinweis	Höchster Aufwand, sofern die für die Authentifizierung erforderliche Information ohne Hinweise auf sie abgerufen werden muss.	$A_{b.ab} = 1$
Erinnerung mit Hinweis	Mittlerer Aufwand, sofern die für die Authentifizierung erforderliche Information mit zugehörigem Hinweis abgerufen wird.	$A_{b.ab} = 0{,}5$
Erkennung	Kein Aufwand, sofern der Abruf der Information durch Wiedererkennen erfolgt (z.B. visuelle Abfrage der Authentifizierungsmerkmale).	$A_{b.ab} = 0$

Tabelle 5-9: Aufwand in Bezug auf die Abrufbarkeit der Authentifizierungsinformation[522]

[521] Basierend auf RENAUD, K.: Evaluating Authentication Mechanisms, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 118 f.

[522] Basierend auf RENAUD, K.: Evaluating Authentication Mechanisms, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 117 f.

Aspekt: Aussagekräftigkeit ($A_{b.aus}$)

Quantifizierung des Aufwands: Grad der Aussagekräftigkeit der Information zur Authentifizierung ($0 \leq A_{b.aus} \leq 1$)		
Grad des Aufwands	**Beschreibung**	**Bewertung**
fremd zugewiesen	Höchster Aufwand, sofern die Information (z.B. Authentifizierungsmerkmal) dem Benutzer zugewiesen wurde.	$A_{b.aus} = 1$
selbst zugewiesen	Mittlerer Aufwand, sofern die Information vom Benutzer selbst gewählt wurde.	$A_{b.aus} = 0{,}67$
aussagekräftig	Geringer Aufwand, sofern die Information aussagekräftig für den Benutzer ist.	$A_{b.aus} = 0{,}33$
ableitbar	Kein Aufwand, sofern die Information für den Benutzer aus anderen Informationen ableitbar ist.	$A_{b.aus} = 0$

Tabelle 5-10: Aufwand in Bezug auf die Aussagekräftigkeit der Authentifizierungsinformation[523]

5.4.2.4 Aufwand für die Verwaltung seitens der Organisationen

Kosten werden von RENAUD, wie in Abschnitt 5.4.1 beschrieben, als separates Kriterium genannt. Allerdings wird deren Anteil am Aufwand (neben evtl. monetären Bedingungen beispielsweise durch Budgets[524]) nicht quantifiziert. Eine Quantifizierung für die Verwendung in der folgenden Optimierung der Authentifizierung in heterogenen IT-Strukturen auf Basis der bereits im vorherigen Abschnitt genannten Dimensionen der Kosten als Kriterium umfasst folgende Aspekte:

Aspekt: Benutzerverwaltung ($A_{o.bv}$)

Für die Verwendung der Authentifizierung müssen von den Betreibern Benutzer und deren Authentifizierungskonten[525] verwaltet werden. Dies bedeutet einen Zeitaufwand, der anhand folgender Teilaspekte bewertet wird:

Quantifizierung des Aufwands: Anteil der Teilaspekte mit hohem Zeitaufwand ($0 \leq A_{o.bv} \leq 1$)		
Teilaspekte	**Beschreibung**	**Bewertung**
Einrichtung	Erhöhter Aufwand, sofern die Einrichtung neuer Benutzer zeitintensiv ist.	$A_{b.bv} + 0{,}33$
Erneuerung	Zusätzlicher Aufwand, sofern die Erneuerung oder Wartung bestehender Benutzer zeitintensiv ist.	$A_{b.bv} + 0{,}33$
Sperrung und Entfernung	Zusätzlicher Aufwand, sofern die Sperrung oder Löschung von Benutzern zeitintensiv ist.	$A_{b.bv} + 0{,}33$

Tabelle 5-11: Aufwand durch Benutzerverwaltung

---

[523] Basierend auf RENAUD, K.: Evaluating Authentication Mechanisms, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 118.

[524] Siehe RENAUD, K.: Evaluating Authentication Mechanisms, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 125 ff.

[525] Vgl. Definition von Authentifizierungskonten in Abschnitt 2.1.7.

Aspekt: Software ($A_{o.sw}$)

Quantifizierung des Aufwands: Anteil der kostenintensiven Teilaspekte der für die Authentifizierung eingesetzten Software ($0 \leq A_{o.sw} \leq 1$)		
Teilaspekte	**Beschreibung**	**Bewertung**
Anschaffung	Erhöhter Aufwand, sofern die Anschaffung der Software für die Authentifizierung mit hohen Kosten verbunden ist.	$A_{o.sw}$ + 0,33
Lizenzen	Zusätzlicher Aufwand, sofern die Software hohe Lizenzkosten beinhaltet.	$A_{o.sw}$ + 0,33
Wartung	Zusätzlicher Aufwand, sofern die Software einen hohen Wartungsaufwand besitzt.	$A_{o.sw}$ + 0,33

Tabelle 5-12: Aufwand für Software-Kosten

Aspekt: Hardware ($A_{o.hw}$)

Quantifizierung des Aufwands: Anteil der kostenintensiven Teilaspekte der für die Authentifizierung eingesetzten Hardware ($0 \leq A_{o.hw} \leq 1$)		
Teilaspekte	**Beschreibung**	**Bewertung**
Anschaffung	Erhöhter Aufwand, sofern die Anschaffung der Hardware für die Authentifizierung mit hohen Kosten verbunden ist.	$A_{b.hw}$ + 0,50
Betrieb / Wartung	Zusätzlicher Aufwand, sofern die Hardware einen hohen Betriebs- oder Wartungsaufwand besitzt.	$A_{b.hw}$ + 0,50

Tabelle 5-13: Aufwand für Hardware-Kosten

Aspekt: Wartbarkeit ($A_{o.war}$)

Quantifizierung des Aufwands: Anteil der Teilaspekte mit einem hohen Zeitaufwand ($0 \leq A_{o.war} \leq 1$)		
Teilaspekte	**Beschreibung**	**Bewertung**
Implementierung	Erhöhter Aufwand, sofern die Implementierung der Authentifizierung mit hohen Kosten verbunden ist.	$A_{o.war}$ + 0,33
Betrieb	Zusätzlicher Aufwand, sofern der Betrieb der Authentifizierung mit hohen Kosten verbunden ist (dies beinhaltet auch notwendige Sicherheitsstrukturen[526]).	$A_{o.war}$ + 0,33
Erneuerung / Wartung	Zusätzlicher Aufwand, sofern die Erneuerung oder Wartung der Authentifizierung mit hohen Kosten verbunden ist.	$A_{o.war}$ + 0,33

Tabelle 5-14: Aufwand durch eingeschränkte Wartbarkeit

[526] Vgl. Schutz der Schlüssel resp. Backup in RENAUD, K.: Evaluating Authentication Mechanisms, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 123.

Kosten werden ausschließlich für ide Organisationen bzw. Betreiber betrachtet. Es wird davon ausgegangen, dass die Betreiber die IT-Struktur für ihre Benutzer bereitstellen[527] und somit auch die Kosten für die zur Authentifizierung der Benutzer benötigte Soft- und Hardware tragen.

5.4.2.5 Berechnung des insgesamt erforderlichen Aufwands

Der insgesamt erforderliche Aufwand ergibt sich durch die Summierung der in den vorherigen Abschnitten quantifizierten Aspekte. Hierbei wird für die Berechnung des Aufwands für die Verwendung der Authentifizierung durch die Benutzrt die Formel zur Berechnung des Defizits $\bar{n}$ nach RENAUD angepasst.[528]

$$A_{b.verwendung} = \sqrt{A_{b.sa}{}^2 + A_{b.beq}{}^2 + A_{b.bar}{}^2}, \qquad 0 \le A_{b.verwendung} \le \sqrt{3} \approx 1{,}73$$

Als maximaler Aufwand für die Verwendung der Authentifizierung durch die Benutzer wird daher $A_{b.verwendung} = \sqrt{3} \approx 1{,}73$ definiert. Dadurch erhalten, wie bei RENAUD beschrieben, einzelne Dimensionen mit maximalem Aufwand (bzw. maximalem Defizit) einen höheren Anteil an der Gesamtbewertung.[529] Eine einzelne Dimension mit maximalem Aufwand führt zu $A_{b.verwendung} = 1$ und erhält so $\frac{1}{1{,}73} \approx 0{,}58$ resp. 58% des maximal möglichen Aufwands.

Für die Berechnung des Aufwands bezüglich der Verwaltung der Authentifizierung seitens der Benutzer wird die Formel nach RENAUD um eine Dimension erweitert:[530]

$$A_{b.verwaltung} = \sqrt{A_{b.war}{}^2 + A_{b.vt}{}^2 + A_{b.ab}{}^2 + A_{b.aus}{}^2}, \qquad 0 \le A_{b.verwaltung} \le \sqrt{4} = 2$$

Der maximale Aufwand für die Verwaltung durch die Benutzer wird somit definiert als $A_{b.verwaltung} = \sqrt{4} = 2$. Durch die Anwendung bzw. Erweiterung der Formel von RENAUD bestimmt eine einzelne Dimension mit maximalem Aufwand ($A_{b.verwaltung} = 1$) bereits 50% des insgesamt maximal möglichen Aufwands für die Verwaltung.

---

[527] Vgl. Zielgruppen in Abschnitt 4.2. Für die Benutzer entstehen keine Kosten in Bezug auf die Authentifizierung.

[528] Vgl. Abschnitt 5.4.1.

[529] Wie in RENAUD, K.: Quantifying the Quality of Web-Authentication Mechanisms. A Usability Perspektive, S. 13 gefordert.

[530] Vgl. RENAUD, K.: Quantifying the Quality of Web-Authentication Mechanisms. A Usability Perspektive, S. 13.

Hinsichtlich der Authentifizierung setzt sich der Gesamtaufwand für die Benutzer aus $A_{b.verwendung}$ und $A_{b.verwaltung}$ zusammen. Analog zur in Abschnitt 5.4.1.3 genannten Formel für die Berechnung des Gesamtdefizits $\overline{d_{env}}$ wirken auch auf den in dieser Arbeit betrachteten Aufwand äußere Einflüsse ein.[531] Diese umfassen bei Betrachtung des Aufwands für die Benutzer den Faktor *control* als Maß für die Kontrolle über die IT-Struktur, in der die Authentifizierung durchgeführt wird. Handelt es sich hierbei um eine kontrollierte Umgebung, in der etwa spezielle Hard- und Software flächendeckend zur Verfügung gestellt werden kann, so erhält der Faktor *control* den Wert 0,5.[532] Diese Reduzierung begründet sich zusätzlich durch den Einfluss auf garantierte Barrierefreiheit oder bereitgestellte Single-Password oder „Single Sign-On"-Lösungen, der innerhalb einer kontrollierten, geschlossenen Umgebung durch die Betreiber ausgeübt werden kann. Sofern eine IT-Struktur betrachtet wird, die z.B. aufgrund einer hohen Dezentralität nicht kontrolliert werden kann, wird der Aufwand durch den Faktor *control* mit dem Wert 1,5 verstärkt.

Auf den Aufwand hinsichtlich der Verwaltung seitens der Benutzer wirkt, analog zu dessen Verwendung, der Faktor *freq*. Dieser wird mit dem Wert 0,5 belegt, sofern die Benutzer die Authentifizierung häufig verwenden und damit einen geringeren Aufwand bei deren Verwaltung benötigen.[533] Sofern die Authentifizierung selten durchgeführt wird, wird *freq* mit 1,5 belegt.

Der von RENAUD verwendete Faktor *renewal* wird in dieser Arbeit in einem erweiterten Kontext *policy* berücksichtigt. Definiert die IT-Struktur, in der die Authentifizierung verwendet wird, spezielle Vorgaben mit hohen Einschränkungen hinsichtlich der Erneuerung (*renewal*), Komplexität oder Verwaltung von Authentifizierungsmerkmalen und -verfahren für die Benutzer, so wird *policy* mit dem Wert 1,5 belegt.[534] Werden keine Einschränkungen in Bezug auf Erneuerung, Komplexität oder Verwaltung seitens der Benutzer erfordert, erhält *policy* den Wert 0,5 und der Aufwand wird entsprechend halbiert.

---

[531] Vgl. „Environmental Considerations" nach RENAUD, K.: Quantifying the Quality of Web-Authentication Mechanisms. A Usability Perspektive, S. 123 ff.

[532] In RENAUD, K.: Quantifying the Quality of Web-Authentication Mechanisms. A Usability Perspektive, S. 13 f. wird der Wert 1,0 für kontrollierte Umgebungen verwendet, in dieser Arbeit wird jedoch auch die Verringerung des Aufwands durch Single-Password und Single Sign-On betrachtet.

[533] In RENAUD, K.: Quantifying the Quality of Web-Authentication Mechanisms. A Usability Perspektive, S. 14 wird 0,5 für tägliche Authentifizierung, 1 für wöchentliche und 1,5 ab monatlicher Authentifizierung verwendet.

[534] Für den Begriff Einschränkungen in diesem Zusammenhang vgl. SASSE, M. A.; FLECHAIS, I.: Usable Security. Why Do We Need It? How Do We Get It?, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 13 ff.; ADAMS, A.; SASSE, A.: Users Are Not the Enemy. Why Users Compromise Security Mechanisms and How to Take Remedial Measures, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 640 ff.

Für die Bewertung des Gesamtaufwands für die Benutzer ergibt sich die Formel:

$$A_b = A_{b.verwendung} * control + A_{b.verwaltung} * freq * policy, \qquad 0 \leq A_b \leq 7{,}1$$

Analog zur Summierung der Aspekte in Bezug auf den Aufwand während der Verwendung der Authentifizierung durch die Benutzer ergibt sich für die Organisationen:

$$A_{o.verwendung} = \sqrt{A_{o.sa}{}^2 + A_{o.po}{}^2 + A_{o.mob}{}^2}, \qquad 0 \leq A_{o.verwendung} \leq \sqrt{3} \approx 1{,}73$$

Der maximale Aufwand wird mit $A_{o.verwendung} = \sqrt{3} \approx 1{,}73$ definiert. Eine einzelne Dimension mit maximalem Aufwand bestimmt analog zur Berechnung von $A_{b.verwendung}$ 58% des maximal möglichen Gesamtaufwands für $A_{o.verwendung}$.

Für die Bewertung des Aufwands für die Verwaltung der Authentifizierung aufseiten der Organisationen als Betreiber wird die Formel analog zur Bewertung des Verwaltungsaufwands seitens der Benutzer erweitert zu:

$$A_{o.verwaltung} = \sqrt{A_{o.bv}{}^2 + A_{o.sw}{}^2 + A_{o.hw}{}^2 + A_{o.war}{}^2}, \qquad 0 \leq A_{o.verwaltung} \leq \sqrt{4} = 2$$

Maximal ergibt sich daher der Aufwand $A_{o.verwaltung} = \sqrt{4} = 2$ für die Verwaltung der Authentifizierung durch die Organisationen als Betreiber. Der Einfluss einer einzelnen Dimension mit maximalem Aufwand auf den Gesamtaufwand für $A_{o.verwaltung}$ liegt, wie bei $A_{b.verwaltung}$, bei 50%.

Der Aufwand für Verwendung und Verwaltung ergibt in der Summe den Gesamtaufwand für die Betreiber A_o. Auf diesen Aufwand wirken, analog zur Berechnung des Aufwands A_b für die Benutzer, äußere Faktoren[535] ein. Als *control* wird dabei der Faktor bezeichnet, der das Maß der durch die Organisationen ausgeübten Kontrolle über die IT-Struktur in Bezug auf die Verwendung der Authentifizierung angibt. Können in der IT-Struktur spezielle Anforderungen (z.B. Hard- und Software) umfassend realisiert und eine homogene Struktur ohne Anforderungen an die Portabilität der Authentifizierung erzwungen werden oder besitzt die Mobilität der Benutzer in der IT-Struktur keine Rolle, so wird *control* mit dem Wert 0,5 als Minderung des Aufwands definiert.[536] Lässt sich

---

[535] Vgl. „Environmental Factoring of the Coefficient" in RENAUD, K.: Quantifying the Quality of Web-Authentication Mechanisms. A Usability Perspektive, S. 13 ff.

[536] in RENAUD, K.: Quantifying the Quality of Web-Authentication Mechanisms. A Usability Perspektive, S. 13 wird hier der Wert 1 verwendet, jedoch wird in dieser Arbeit die Minderung des Aufwands durch erhöhte Portabilität und Mobilität in kontrollierten IT-Strukturen einbezogen.

eine derartige Kontrolle, etwa bedingt durch dezentrale IT-Strukturen, nicht realisieren, so wird der Aufwand durch den Faktor *control* mit dem Wert 1,5 verstärkt.

In Bezug auf die Verwaltung der Authentifizierung durch die Organisationen werden die Faktoren *management* und *self-service* definiert. *Management* wird mit dem Wert 0,5 belegt, sofern die Authentifizierung über zentrale (Identitäts-)Management-Funktionen, z.B. in Form vom Verzeichnisdiensten, Föderationen[537] usw., realisiert wird, die eine zentrale Verwaltung auch bei dezentralen IT-Strukturen (z.B. bestehend aus mehreren Betreibern) erlauben. Sofern kein solches Management realisierbar ist oder der Aufwand für die Verwaltung mit zunehmender Größe der IT-Struktur durch die Vielzahl an Authentifizierungssystemen, -verfahren und -merkmalen nicht linear (sondern beispielsweise exponentiell) ansteigt, so wird *management* mit 1,5 definiert und damit der vergrößerte Aufwand entsprechend berücksichtigt.

Zusätzlich wird in dieser Arbeit der Faktor *self-service* für die Bewertung der Verwaltung der Authentifizierung durch die Organisationen resp. Betreiber eingeführt. *Self-service* wird mit dem Wert 0,5 belegt, sofern die eingesetzte Authentifizierung Möglichkeiten für die Benutzer bietet, ihre verwendeten Authentifizierungsmerkmale und -verfahren teilweise selbst und ohne Aufwand für die Organisationen zu verwalten. Sofern diese Möglichkeiten nicht existieren, wird *self-service* mit dem Wert 1,5 belegt.

$$A_o = A_{o.verwendung} * control + A_{o.verwaltung} * management * self\text{–}service, \qquad 0 \le A_o \le 7{,}1$$

Das Kantengewicht A der Graphen wird somit insgesamt innerhalb dieser Arbeit definiert als:

$$A = A_o + A_b, \qquad 0 \le A \le 14{,}2$$

5.4.3 Erweiterte Bewertung der Sicherheit in heterogenen IT-Strukturen

Während im vorherigen Abschnitt die Bewertung des Aufwands definiert wurde, wird in diesem Abschnitt das Bewertungsverfahren für den durch die Authentifizierung erzielten Nutzen bzw. die erzielte Sicherheit S erläutert.[538] Die Bewertung der Aspekte und Teilaspekte erfolgt hierbei analog zum vorherigen Abschnitt. Auch für die Bewertung der Sicherheit wird das Bewertungsmodell von RENAUD als Grundlage verwendet und für den Einsatz in heterogenen IT-Strukturen entsprechend

[537] Vgl. Federation-basierte Authentifizierung in Abschnitt 3.2.7.

[538] Vgl. Abschnitt 5.2.

erweitert.[539] Die Bewertung der Aspekte in Bezug auf die Verwendung wird im Vergleich zu RENAUD invertiert. Während RENAUD einen Aspekt im Falle des höchsten Defizits resp. der geringsten Sicherheit mit dem Maximalwert 1 belegt, nimmt im Folgenden der Wert der erzielten Sicherheit zu. Dies ist erforderlich, da die spätere Optimierung die Erhöhung der Sicherheit als resultierenden Nutzen aus dem erforderlichen Aufwand *A*, der im vorherigen Abschnitt bewertet wurde, definiert. Ein maximales Defizit (1) nach RENAUD bildet somit in dieser Arbeit die minimal erzielte Sicherheit (0). Umgekehrt erhält eine Lösung, die keine Defizite nach RENAUD (0) aufweist, im Folgenden den Maximalwert für *S* (1).

Als Kriterien für die Definition der Bewertung der erzielten Sicherheit fließen zusätzlich die in Abschnitt 2.3.1 genannten internationalen Kriterien für IT-Sicherheit, insbesondere der Common Criteria als ISO/IEC 15401, ein.[540]

5.4.3.1 Sicherheit der Authentifizierung in heterogenen IT-Strukturen

In die Erweiterung des Bewertungsmodells nach RENAUD fließen hierbei die in Abschnitt 2.3 vorgestellten Richtlinien für IT-Sicherheit, insbesondere die Common Criteria, ein.[541] Für die Gewährleistung der Grundwerte der IT-Sicherheit[542] „Vertraulichkeit", „Integrität", „Verfügbarkeit" und „Verbindlichkeit" wird hierfür die Dimension „Schutzziele" eingeführt und die Dimension „Vertraulichkeit" nach RENAUD in diese übernommen.[543]

Die Sicherheit wird für Benutzer und Organisationen als Betreiber nach gleichen Kriterien berechnet.[544]

---

[539] Vgl. RENAUD, K.: Quantifying the Quality of Web-Authentication Mechanisms. A Usability Perspektive, S. 11 ff.

[540] Vgl. BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: Common Criteria. Version 2.3, 2006.

[541] Vgl. BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: Common Criteria. Version 2.3, 2006.

[542] Vgl. Abschnitt 2.2.

[543] Vgl. „Confidentiality" in RENAUD, K.: Evaluating Authentication Mechanisms, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 121.

[544] Vgl. hierzu auch Vorgaben der Common Criteria BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: Common Criteria. Version 2.3, 2006. Hier erfolgt keine Unterscheidung zwischen Benutzer und Betreiber.

Aspekt: Vorhersagbarkeit (S_{vor})

Quantifizierung des Nutzens / der erzielten Sicherheit: Grad der Minderung durch Vorhersagbarkeit der Authentifizierungsmerkmale ($0 \leq S_{vor} \leq 1$)		
Grad der Sicherheit	**Beschreibung**	**Bewertung**
niemanden	Höchste Sicherheit, sofern das erforderliche Authentifizierungsmerkmal für Dritte nicht vorhersagbar ist.	$S_{vor} = 1$
Freunde und Familie	Mittlere Sicherheit, sofern das Authentifizierungsmerkmal für Freunde und Familie vorhersagbar ist.	$S_{vor} = 0{,}5$
Jeden	Niedrige Sicherheit, sofern das Authentifizierungsmerkmal für Dritte leicht vorhersagbar ist.	$S_{vor} = 0$

Tabelle 5-15: Minderung der erzielten Sicherheit durch Vorhersagbarkeit[545]

Aspekt: Fülle und Ersetzbarkeit (S_{fe})

Quantifizierung des Nutzens / der erzielten Sicherheit: Anzahl der maximal verfügbaren unterschiedlichen Authentifizierungsmerkmale ($0 \leq S_{fe} \leq 1$)		
Grad der Sicherheit	**Beschreibung**	**Bewertung**
$\geq 2^{64}$	Hohe Sicherheit, sofern mehr als 2^{64} Authentifizierungsmerkmale für Einrichtung und Ersatz zur Verfügung stehen.	$S_{fe} = 1$
$\sim 2^{50}$	Mittlere Sicherheit, sofern mehr oder weniger als 2^{50} Authentifizierungsmerkmale für Einrichtung und Ersatz zur Verfügung stehen.	$S_{fe} = 0{,}5$
$< 2^{40}$	Niedrige Sicherheit, sofern weniger als 2^{40} mögliche Authentifizierungsmerkmale für Einrichtung und Ersatz zur Verfügung stehen.	$S_{fe} = 0$

Tabelle 5-16: Erzielte Sicherheit durch ausreichende Fülle und Ersetzbarkeit[546]

Wie RENAUD ausführt, wird die Sicherheit von Fülle und Ersetzbarkeit der Authentifizierungsmerkmale abhängig bewertet. Ersetzbarkeit bezieht sich hierbei auf mögliche Schlüssel bzw. Authentifizierungsmerkmale, die verwendet werden können, sofern der bisher verwendete Schlüssel bzw. das Merkmal kompromittiert wurden. RENAUD nennt als Beispiel für fehlende Ersetzbarkeit biometrische Merkmale (2.5.3), die zwar eine hohe Fülle aufweisen, aber nur begrenzt ersetzbar sind.[547]

---

[545] Basierend auf RENAUD, K.: Evaluating Authentication Mechanisms, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 119.

[546] Vgl. „Abundance“ in RENAUD, K.: Evaluating Authentication Mechanisms, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 120.

[547] Vgl. RENAUD, K.: Evaluating Authentication Mechanisms, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 120.

Aspekt: Offenlegung (S_{of})

Quantifizierung des Nutzens / der erzielten Sicherheit: Grad der Minderung durch Offenlegung der Authentifizierungsmerkmale ($0 \leq S_{of} \leq 1$)		
Teilaspekte	**Beschreibung**	**Bewertung**
unmöglich zu enthüllen	Hohe Sicherheit, sofern das Authentifizierungsmerkmal nicht notiert, kopiert bzw. allgemein enthüllt werden kann.	$S_{of} = 1$
leicht während der Eingabe zu erlangen	Mittlere Sicherheit, sofern das Authentifizierungsmerkmal leicht während der Eingabe durch Dritte abgehört und kopiert werden kann.	$S_{of} = 0{,}5$
leicht notierbar	Niedrige Sicherheit, sofern das Authentifizierungsmerkmal leicht notiert bzw. kopiert werden kann.	$S_{of} = 0$

Tabelle 5-17: Minderung der erzielten Sicherheit durch Offenlegung[548]

Aspekt: Angreifbarkeit (S_{an})

Quantifizierung des Nutzens / der erzielten Sicherheit: Grad der Minderung durch Angreifbarkeit der Authentifizierung ($0 \leq S_{an} \leq 1$)		
Teilaspekte	**Beschreibung**	**Bewertung**
Keine	Höchste Sicherheit, sofern derzeit keine Angriffe auf das Authentifizierungsverfahren bekannt sind.	$S_{an} = 1$
basierend auf Nachforschungen	Hohe Sicherheit, sofern Angriffe auf das Authentifizierungsverfahren Nachforschungen bzw. spezielle technische Kenntnisse erfordern.	$S_{an} = 0{,}67$
„brute force“	Mittlere Sicherheit, sofern Angriffe auf das Authentifizierungsverfahren durch Probieren aller Kombinationen („brute force“) möglich sind.	$S_{an} = 0{,}33$
„key logger“	Niedrige Sicherheit, sofern Angriffe auf das Authentifizierungsverfahren durch Abhören und Speichern z.B. bei der Eingabe („key logger“) erfolgen können.	$S_{an} = 0$

Tabelle 5-18: Erzielte Sicherheit durch Minderung der Angreifbarkeit[549]

[548] Basierend auf „Disclosure“ in RENAUD, K.: Evaluating Authentication Mechanisms, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 120.

[549] Basierend auf „Breakability and crackability“ in RENAUD, K.: Evaluating Authentication Mechanisms, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 122.

Aspekt: Datenschutz (S_{dat})

Quantifizierung des Nutzens / der erzielten Sicherheit: Grad der Minderung durch Missachtung des Datenschutzes ($0 \leq S_{dat} \leq 1$)		
Teilaspekte	**Beschreibung**	**Bewertung**
Öffentlich	Hohe Sicherheit, sofern für die Authentifizierung keine privaten Daten verwendet werden.	$S_{dat} = 1$
Privat, aber in der Entscheidung des Benutzers	Mittlere Sicherheit, sofern für die Authentifizierung private Daten verwendet werden können, dies jedoch vom Benutzer entschieden wird.	$S_{dat} = 0{,}5$
Private Daten erforderlich	Niedrige Sicherheit, sofern die Authentifizierung die Verwendung privater Daten erfordert.	$S_{dat} = 0$

Tabelle 5-19: Minderung der erzielten Sicherheit durch Minderung des Datenschutzes[550]

Aspekt: Schutzziele (S_{sz})

Quantifizierung des Nutzens / der erzielten Sicherheit: Anteil der Teilaspekte zur Gewährleistung der Schutzziele der IT-Sicherheit ($0 \leq S_{sz} \leq 1$)		
Teilaspekte	**Beschreibung**	**Bewertung**
Vertraulichkeit	Erhöhte Sicherheit, sofern für die Authentifizierung relevante Daten während der Verwendung nicht offen gelegt werden.[551]	S_{sz} +0,25
Integrität	Erhöhte Sicherheit, sofern Manipulationen an den zur Authentifizierung übermittelten Daten[552] erkannt und verhindert werden.	S_{sz} +0,25
Verfügbarkeit	Erhöhte Sicherheit, sofern die Authentifizierung redundant ausgelegt ist[553] und eine Fehlertoleranz bietet.[554]	S_{sz} +0,25
Verbindlichkeit	Erhöhte Sicherheit, sofern die Identität des Absenders sowie des Empfängers der Authentifizierung unabstreitbar zugewiesen werden.[555]	S_{sz} +0,25

Tabelle 5-20: Erhöhte Sicherheit durch Garantie von Schutzzielen

---

[550] Basierend auf „Privacy“ in RENAUD, K.: Evaluating Authentication Mechanisms, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 121 f.

[551] Z.B. erreichbar, indem die übermittelten Daten verschlüsselt werden (Abschnitt 2.2.1).

[552] Z.B. durch Man-In-The-Middle Angriffe, vgl. Abschnitt 2.8.2.

[553] Schutz vor Denial-of-Service Angriffen, vgl. Abschnitt 2.8.3.

[554] Vgl. „fault tolerance“ in SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 115 f.

[555] Beispielsweise durch die Verwendung digitaler Signaturen resp. Zertifikate.

Aspekt: Technische Absicherung (S_{aut})

Quantifizierung des Nutzens / der erzielten Sicherheit: Anteil der erfüllten Teilaspekte zur Absicherung der Authentifizierung ($0 \leq S_{aut} \leq 1$)		
Teilaspekte	**Beschreibung**	**Bewertung**
Multi-Faktor Authentifizierung	Erhöhte Sicherheit, sofern die erfolgreiche Authentifizierung die Verwendung mehrerer Faktoren erfordert.[556]	S_{aut} + 0,33
Beidseitige Authentifizierung	Erhöhte Sicherheit, sofern die Authentifizierung für beide Seiten[557] erforderlich ist.	S_{aut} = +0,33
Absicherung der beteiligten Software- und Hardware	Erhöhte Sicherheit, sofern die für die Authentifizierung verwendeten Komponenten (z.B. physikalisch) zusätzlich gegen Missbrauch abgesichert sind.	S_{aut} = +0,33

Tabelle 5-21: Erhöhte Sicherheit durch technische Absicherung der Authentifizierung

5.4.3.2 Berechnung der insgesamt erzielten Sicherheit

Die insgesamt erzielte Sicherheit als Nutzen ergibt sich durch die Summierung der in den vorherigen Abschnitten definierten Aspekte. RENAUD unterscheidet bei der Bewertung der Sicherheit zwischen Sicherheit (security) und Anfälligkeit (vulnerability).[558] In dieser Arbeit wird die Sicherheit jedoch insgesamt als Nutzen bewertet. Dabei wird, wie bereits für die Bewertung des Aufwands in Abschnitt 5.4.2 definiert, zwischen der Sicherheit während der Verwendung und der Sicherheit, die durch entsprechende Verwaltung der Authentifizierung erreicht werden kann, unterschieden. Wählen Benutzer beispielsweise Authentifizierungsmerkmale aus, die leicht vorhersagbar sind, leicht offen gelegt werden können oder nicht die gesamte mögliche Fülle an Merkmalen ausschöpfen, so schränkt dies die Sicherheit bezüglich der Verwendung der Authentifizierung ein. Dies gilt auch aufseiten der Betreiber, sofern etwa Authentifizierungsverfahren oder -systeme verwendet werden, die diese Aspekte einschränken:

$$S_{verwendung} = 1{,}73 - \sqrt{(1 - S_{vor})^2 + (1 - S_{fe})^2 + (1 - S_{of})^2}, \qquad 0 \leq S_{verwendung} \leq 1{,}73$$

Bei der Berechnung des Aufwands $A_{b.verwendung}$ in Abschnitt 5.4.2.5 bestimmte eine einzelne Dimension mit maximalem Aufwand durch die Anwendung der Formel nach RENAUD 58% des insgesamt möglichen Aufwands. Bei der Berechnung von $S_{verwendung}$ hat im Gegensatz dazu eine einzelne Di-

[556] Vgl. Abschnitt 2.1.6, z.B. durch den Einsatz von Tokens vgl. Abschnitt 2.5.2.

[557] Vgl. „mutual authentication" resp. Client- und Server-seitige Authentifizierung in. ANDERSON, R.: Security Engineering. A Guide to Building Dependable Distributed Systems, 2001, S. 20 ff.

[558] Vgl. RENAUD, K.: Quantifying the Quality of Web-Authentication Mechanisms. A Usability Perspektive, S. 12.

mension mit minimaler Sicherheit den größten Einfluss auf die insgesamt erzielte Sicherheit.[559] Es geht daher für jede Dimension deren Differenz zum maximalen Wert 1 ein, wobei innerhalb der Wurzel somit das Sicherheitsdefizit bestimmt wird.[560] Um im Gesamtergebnis trotzdem die erzielte Sicherheit als Nutzen und nicht das Defizit zu betrachten, wird das Ergebnis der Wurzel von dessen Maximum 1,73 (bei $S_{vor} = S_{fe} = S_{of} = 0$) abgezogen.

Durch die Auswahl der für die Authentifizierung verwendeten Verfahren werden die resultierende Angreifbarkeit, der realisierte Datenschutz sowie adressierte Schutzziele bestimmt. Gemeinsam mit der technischen Absicherung des gewählten Authentifizierungsverfahrens oder -systems ergibt sich die Summe der quantifizierten Sicherheitsaspekte für die Verwaltung seitens der Organisationen als Betreiber:

$$S_{verwaltung} = 2 - \sqrt{(1-S_{an})^2 + (1-S_{dat})^2 + (1-S_{sz})^2 + (1-S_{aut})^2}, \qquad 0 \le S_{verwaltung} \le 2$$

Hierbei wird erneut innerhalb der Wurzel aus der erzielten Sicherheit durch dessen Differenz zum maximalen Wert 1 das Sicherheitsdefizit gebildet. Dadurch wird einem einzigen Aspekt mit maximalem Defizit, wie bereits im Abschnitt 5.4.2.5 für den Aufwand $A_{b.verwaltung}$ erläutert, ein Anteil von 50% an der insgesamt erzielten quantifizierten Sicherheit in Bezug auf die Verwaltung zugeordnet. Besitzt ein Authentifizierungsverfahren beispielsweise keine Vorkehrungen für den Datenschutz ($S_{dat} = 0$) und legt private Daten öffentlich frei, so ergibt sich, sofern S_{an}, S_{sz} und S_{aut} maximale Sicherheit erzielen, für $S_{verwaltung}$:

$$2 - \sqrt{(1-1)^2 + (1-0)^2 + (1-1)^2 + (1-1)^2} = 2 - 1 = 1$$

Dabei umfasst der Wert 1 einen Anteil von 50% am Maximalwert 2 und halbiert somit bereits die erzielte Sicherheit verglichen mit dem Maximum.

RENAUD beschreibt für die Sicherheit die äußeren Einflüsse *risk*, *motive* und *audit*, die auf die erzielte Sicherheit einwirken. *Risk* definiert dabei das Risiko, das durch fehlerhafte Authentifizierung entstehen kann. Der Wert 1,5 wird in dieser Arbeit für *risk* verwendet, sofern durch einen Authentifizierungsfehler kein Zugriff auf die Daten des betreffenden Benutzers möglich ist. Wird der unberechtigte Zugriff auf die Daten des Benutzers möglich, wird *risk* mit dem Wert 1 belegt. Ermög-

---

[559] Vgl. GERD TOM MARKOTTEN, D.: Benutzbare Sicherheit in informationstechnischen Systemen, 2003, S. 75.

[560] Vgl. RENAUD, K.: Quantifying the Quality of Web-Authentication Mechanisms. A Usability Perspektive, S. 13.

licht ein Authentifizierungsfehler Zugriff auf die Daten aller Benutzer, so wird *risk* als 0,5 definiert und halbiert damit die erzielte Sicherheit in Bezug auf die Verwendung.[561]

Darüber hinaus beschreibt RENAUD den Faktor *motive*, der den Einfluss der Sicherheitsmotivation seitens der Benutzer einbezieht. Sicherheitsmotivation lässt sich beispielsweise durch die Definition von Richtlinien erreichen, die Sanktionen für die Benutzung definieren, sofern die enthaltenen Vorgaben nicht eingehalten werden. Existieren solche Richtlinien, so wird *motive* mit dem Wert 1 definiert. Sofern keine Sicherheitsvorgaben bzw. -richtlinien in der IT-Struktur bekannt gegeben und die Benutzer nicht über Aspekte der IT-Sicherheit informiert wurden, erhält *motive* den Wert 0,5 und halbiert somit die bei der Verwendung der Authentifizierung erzielte Sicherheit.[562]

Zusätzlich wird die Anfälligkeit (vulnerability) durch eine Überwachung (Auditierung) als Faktor *audit* der Authentifizierung beeinflusst. Dieser Faktor wirkt auch auf die in dieser Arbeit betrachtete erzielte Sicherheit bezüglich der Verwaltung der Authentifizierung ($S_{verwaltung}$). Wird keine Überwachung der Authentifizierung durchgeführt, so erhält *audit* den Wert 0,5 und halbiert die erzielte Sicherheit. Bei einer überwachten Authentifizierung erhält *audit* dagegen den Wert 1.[563] Insgesamt ergibt sich die in dieser Arbeit maximale Quantifizierung der erzielten Sicherheit mit dem Wert 4,6 durch die Formel:[564]

$$S = S_{verwendung} * risk * motive + S_{verwaltung} * audit, \qquad 0 \leq S \leq 4{,}6$$

5.5 Vereinheitlichung von Authentifizierungsmerkmalen

In Abschnitt 5.2 wurden Integrationsmöglichkeiten für die betrachteten Faktoren einer einheitlichen Authentifizierung aus Abschnitt 5.1 genannt. Im Folgenden werden diese Möglichkeiten für eine Vereinheitlichung von Authentifizierungsmerkmalen betrachtet. Zunächst wird in Abschnitt 5.5.1 die Diversität der Authentifizierungsmerkmale in einer heterogenen IT-Struktur aufgezeigt. Hierbei werden vorrangig die Anforderungen vorgestellt, die unterschiedliche Authentifizierungsmerkmale und damit deren Diversifizierung bedingen. Abschnitt 5.5.2 bewertet diese Anforderun-

---

[561] Vgl. RENAUD, K.: Quantifying the Quality of Web-Authentication Mechanisms. A Usability Perspektive, S. 14.

[562] Vgl. RENAUD, K.: Quantifying the Quality of Web-Authentication Mechanisms. A Usability Perspektive, S. 14.

[563] Vgl. RENAUD, K.: Quantifying the Quality of Web-Authentication Mechanisms. A Usability Perspektive, S. 14.

[564] In Anlehnung an RENAUD, K.: Quantifying the Quality of Web-Authentication Mechanisms. A Usability Perspektive, S. 15.

gen aus der Sicht der Benutzer sowie der Betreiber[565] und gibt damit die Relevanz für deren Integration vor. Anforderungen, die aus Sicht der Benutzer oder Betreiber ein höheres Vereinheitlichungspotential aufweisen, werden hierbei bevorzugt in die in Kapitel 6 folgende Optimierung einbezogen. Gemäß dem in Abschnitt 5.3.1 gezeigten Graphen wurde bereits erläutert, dass der Reduzierung bzw. Vereinheitlichung von Authentifizierungsmerkmalen aus Sicht der Nutzer die höchste Relevanz zugeordnet wird.

Konkrete Integrationsansätze gemäß der in Abschnitt 5.2 genannten theoretischen Möglichkeiten nennt der Abschnitt 5.5.3. Da durch die Integration die Homogenität der Authentifizierungsmerkmale zunimmt und damit z.B. Sicherheitsrisiken bei der Kompromittierung eines Merkmals entstehen, zeigt Abschnitt 5.5.4 zusätzlich Grenzen für eine sinnvolle und effiziente Integration auf.

Abschnitt 5.5.5 nennt schließlich resultierende Hypothesen in Bezug auf die Vereinheitlichung von Authentifizierungsmerkmalen in heterogenen IT-Strukturen.

5.5.1 Diversität von Authentifizierungsmerkmalen

Um Potentiale für eine Vereinheitlichung von Authentifizierungsmerkmalen zu bestimmen, wird im Folgenden die Vielfalt bzw. Diversität von Authentifizierungsmerkmalen in heterogenen IT-Strukturen anhand der sie bestimmenden Faktoren beschrieben. Für die Bestimmung der Diversität der Authentifizierungsmerkmale sind die in Abschnitt 5.3 beschriebenen Sichten zu unterscheiden. Wie in Abschnitt 5.1 erläutert, entsteht die Diversität von Authentifizierungsmerkmalen durch die Anzahl der Elemente der Menge *M* der Authentifizierungsmerkmale und deren Relationen zu Authentifizierungsverfahren der Menge *V*. Relationen zur Menge *B* der Benutzer werden nicht betrachtet, da ein Authentifizierungsmerkmal genau einem Benutzer zugewiesen wird.[566]

Die Diversität von Authentifizierungsmerkmalen wird in den in dieser Arbeit betrachteten heterogenen IT-Strukturen vorrangig durch nachstehende Faktoren bestimmt:

a) Unterschiedliche Ressourcen ($Div_{Merkmal.a}$)

Benutzer verwenden unterschiedliche Ressourcen, z.B. in Form von Anwendungen, die unterschiedliche Funktionen bereitstellen. Häufig verwenden diese Ressourcen kein gemeinsames Authentifizierungssystem und erfordern daher separate Authentifizierungsmerkmale. Beispiele für Anwendungen, die unterschiedliche Authentifizierungsmerkmale voraussetzen, können

---

[565] Vgl. die unterschiedlichen Sichtweisen auf das Modell in Abschnitt 5.3.

[566] Ein Authentifizierungsmerkmal kann nicht mehreren Benutzern zugeordnet werden, vgl. 5.1, da es den jeweiligen Benutzer eindeutig identifiziert, vgl. Abschnitt 2.1.4.

E-Mail-Server, Remote-Zugangsdienste[567] und Web-Seiten sein. Anwendungen und Ressourcen, die bereits ein gemeinsames Authentifizierungssystem und damit ein einzelnes gemeinsames Authentifizierungsmerkmal für den jeweiligen Benutzer verwenden, sind z.B. zentrale Verzeichnisdienste[568], wie sie u.a. durch Active Directory von Microsoft oder OpenLDAP unter Unix angeboten werden.[569]

b) Verschiedene Organisationen ($Div_{Merkmal.b}$)

Verwendet ein Benutzer Ressourcen, die von unterschiedlichen Organisationen bereitgestellt werden, so muss er für diese in der jeweiligen Organisation ein separates Passwort vergeben. Dies ist auch dann erforderlich, wenn die Ressource in beiden Organisationen die gleiche Funktion zur Verfügung stellt. Beispielsweise ist dies der Fall für Passwörter, die dem Benutzer den Zugang zu zwei unterschiedlichen Versandhäusern im Web ermöglichen. Beide ermöglichen den Zugriff auf einen ähnlichen Funktionsumfang, müssen aber separat definiert und gepflegt[570] werden, sofern die beiden Organisationen kein gemeinsames Authentifizierungssystem verwenden.

c) Verschiedene Authentifizierungsverfahren ($Div_{Merkmal.c}$)

Je nach technischer Ausprägung, Sicherheitsanforderung und Entwicklungshistorie verwenden verschiedene Ressourcen unterschiedliche Authentifizierungsverfahren, deren unterstützte Authentifizierungsmerkmale nicht immer kompatibel sind. Benutzer müssen somit für die Verwendung der Ressourcen bzw. ihrer Authentifizierungsverfahren unterschiedliche Authentifizierungsmerkmale vorhalten und pflegen. So setzt etwa ein Web-Server für die Authentifizierung eines Benutzers innerhalb einer HTTPS Sitzung[571] nach dem Authentifizierungsverfahren SSL ein Zertifikat als Authentifizierungsmerkmal voraus, während eine andere Web-Seite das in HTTP enthaltene Authentifizierungsverfahren „digest“ verwendet, das ein Passwort als Authentifizierungsmerkmal bedingt.

d) Unterschiedliche Sicherheitsanforderungen und Authentifizierungsfaktoren ($D_{Merkmal.d}$)

Gewährt eine Organisation ihren Benutzern Zugriff auf Ressourcen bzw. Informationen, die unterschiedliche Sicherheitsanforderungen stellen, so äußern sich diese Reglementierungen häufig

---

567 Vgl. Abschnitt 3.2.5.

568 Vgl. RADIUS in Abschnitt 3.2.5.

569 Vgl. MICHELA, F.; PALME, M.: Active Directory, 1999, S. 21 ff.; KLÜNTER, D.; LASER, J.: LDAP verstehen, OpenLDAP einsetzen. Grundlagen, Praxiseinsatz, Single Sign-On Systeme, 2003.

570 Z.B. müssen Passwort Änderungen und Sperrungen an allen Authentifizierungssystemen separat durchgeführt werden.

571 Vgl. Abschnitt 3.2.6.

auch bei Auswahl und Verwendung der Authentifizierungsmerkmale. Im einfachsten Fall bedeutet dies z.B. unterschiedliche Komplexitätsanforderungen an das für die jeweilige Ressource verwendete Passwort. Sensiblere Ressourcen und Informationen können hierbei etwa nur mit einem längeren oder komplexeren Passwort (z.B. Vorraussetzung von Groß-, Kleinbuchstaben, Ziffern und Sonderzeichen als Bestandteil) verwendet werden, als es für weniger sensible Ressourcen und Informationen innerhalb der Organisation erforderlich ist. Für die Benutzer bedeutet dies erneut die separate Pflege unterschiedlicher Authentifizierungsmerkmale für die jeweilige Sicherheitsstufe.

Für die Einhaltung hoher Sicherheitsniveaus wird häufig zusätzlich die Verwendung mehrerer Authentifizierungsfaktoren vorausgesetzt. Ein klassisches Beispiel stellt die Verwendung einer Multi-Faktor-Authentifizierung mit Token oder Smart Card und zugehöriger PIN / Passwort-Kombination dar.[572] In diesem Fall müssen die Benutzer neben dem Passwort bzw. der PIN auch das Token oder die Smart Card vorhalten und verwalten.

Durch verschiedene Ausprägungen der Authentifizierungsmerkmale wie etwa durch die Verwendung von Tokens wird die Diversität zusätzlich durch deren Inkompatibilität erhöht, sofern diese nicht von allen Endgeräten oder allen Authentifizierungsverfahren, die der Benutzer verwendet, unterstützt werden.[573] Im Gegensatz wird die Diversität von Passwörtern in Bezug auf deren Kompatibilität mit unterschiedlichen Endgeräten und Authentifizierungsverfahren nur durch die angebotenen Eingabegeräte und -verfahren (beispielsweise die Unterstützung von internationalen Zeichensätzen usw.) bestimmt.

e) Verschiedene Benutzer ($Div_{Merkmal.e}$)

In erster Linie wird die Diversität der Authentifizierungsmerkmale für die Organisationen durch die Anzahl der Benutzer bestimmt. Sofern die Benutzer sich nicht ein gemeinsames Authentifizierungsmerkmal teilen, was in der Regel zur Gewährleistung der Privatsphäre und Sicherheit der persönlichen Informationen nicht der Fall ist, verfügt jeder Benutzer über ein separates Konto und damit Authentifizierungsmerkmal. Jedes Konto resp. jeder Benutzer und jedes Authentifizierungsmerkmal müssen von der Organisation separat bereitgestellt und verwaltet werden.

f) Verschiedene Authentifizierungssysteme ($Div_{Merkmal.f}$)

Die von einer Organisation angebotenen Ressourcen verwenden insbesondere in heterogenen IT-Strukturen, wie in Abschnitt 2.4.2 beschrieben, verschiedene Systeme für die Authentifizie-

---

[572] Vgl. Multi-Faktor-Authentifizierung in Abschnitt 2.5.2.

[573] Vgl. Abhängigkeit von installierter Software und Endgeräten bei Tokens in Abschnitt 2.5.2.

rung ihrer Benutzer. Dies kann durch technische Inkompatibilität, aber auch durch räumliche und organisatorische Trennung bedingt sein. Um den Benutzern Zugriff auf sämtliche zur Verfügung stehenden Ressourcen zu ermöglichen, muss die Organisation als Betreiber somit separate Konten und Authentifizierungsmerkmale für die unterschiedlichen Authentifizierungssysteme anlegen und verwalten.

g) Verschiedene Formate der Authentifizierungskonten ($Div_{Merkmal.g}$)

Authentifizierungsmerkmale werden von den Organisationen innerhalb entsprechender Konten in einer anderen Form als aufseiten der Benutzer gespeichert. Beispielsweise werden Passwörter in der Regel nicht im Klartext, den sich der Benutzer für die Eingabe des Passworts merkt, gespeichert, sondern als Hash-Wert[574] abgelegt. Dadurch können sie von den Organisationen z.B. nicht durch die Administratoren im Klartext ausgelesen und für eine Authentifizierung bei einer anderen Organisation, bei der der Benutzer das gleiche Passwort verwendet, missbraucht werden. Ferner können die Passwörter auf diese Art und Weise nicht versehentlich durch Angestellte der Organisation wie Administratoren oder Helpdesk-Mitarbeiter unberechtigten Dritten preisgegeben werden. Das Passwort liegt seitens der Organisation aufgrund der Eigenschaften von Hash-Verfahren[575] irreversibel verschlüsselt bzw. als nicht invertierbares Komprimat (Hash-Wert) vor.

Die Speicherung der Authentifizierungsmerkmale in kontenspezifischen Formaten erhöht die Sicherheit gegenüber Missbrauch, aber auch ihre Diversität. Dies resultiert aus der technischen Inkompatibilität der Formate bzw. der fehlenden Invertier- und Konvertierbarkeit. Beispielsweise lässt sich ein als MD5 Hash-Wert gespeichertes Passwort nicht in einen SHA1 Hash-Wert konvertieren. Verwenden Authentifizierungssysteme somit für die Speicherung der Authentifizierungsmerkmale in Konten Formate bzw. Hash-Verfahren, die keine Schnittmenge aufweisen, so müssen die Organisationen für dasselbe Authentifizierungsmerkmal eines Benutzers verschiedene Merkmale erstellen, verwalten und vorhalten.

5.5.2 Bewertung des Vereinheitlichungspotentials

Im vorherigen Abschnitt wurden Faktoren für die Diversität von Authentifizierungsmerkmalen genannt. Um für die Senkung der Diversität von Authentifizierungsmerkmalen durch eine Verein-

[574] Vgl. Hash-Werte als Ergebnis von Hash-Verfahren in Abschnitt 2.6.2.

[575] Vgl. fehlende Möglichkeit vom Komprimat (Hash-Wert) auf den Eingangswert zu schließen in Abschnitt 2.6.2.

heitlichung geeignete Verfahren zu finden, wird zunächst das Vereinheitlichungspotential dieser Faktoren bewertet.

Folgende Vereinheitlichungskriterien werden hierbei unterschieden:

- **quantitative Vereinheitlichung**

  Beschreibt die einfachste Form der Vereinheitlichung durch die Reduktion von Elementen resp. Verminderung der Anzahl von Authentifizierungsmerkmalen gemäß der Verfahren $\mathbf{Int_a}$ und $\mathbf{Int_b}$ in Abschnitt 5.2.

- **qualitative Vereinheitlichung**

  Umfasst die Vereinheitlichung der Authentifizierung durch die Minimierung der Aufwände A_b und A_o, die als Kantengewichte der Relationen mit Authentifizierungsmerkmalen definiert wurden.[576] Die qualitative Vereinheitlichung bezieht sich daher auf die Verfahren $\mathbf{Int_c}$ und $\mathbf{Int_d}$ aus Abschnitt 5.2.

  Wie in Abschnitt 5.2 für die Verfahren $\mathbf{Int_c}$ und $\mathbf{Int_d}$ beschrieben, wird hierbei das Vereinheitlichungspotential zusätzlich erhöht, da, sofern hierdurch alle Relationen des Authentifizierungsmerkmals entfernt wurden, dieses anschließend selbst gemäß $\mathbf{Int_a}$ reduziert werden kann. Qualitative Vereinheitlichungen bilden somit eine Grundlage für eine anschließende quantitative Vereinheitlichung.

Das quantitative Vereinheitlichungspotential wird durch die Menge bzw. Anzahl der Authentifizierungsmerkmale in der betrachteten heterogenen IT-Struktur bestimmt. Wird hier eine hohe Anzahl unterschiedlicher Authentifizierungsmerkmale verwendet, so bietet deren Vereinheitlichung ein hohes Potential. Sofern nur eine geringe Anzahl von Authentifizierungsmerkmalen verwendet wird, sinkt damit das Potential der durch die mögliche Vereinheitlichung erzielten Optimierung. Verfügen Benutzer über eine hohe Anzahl unterschiedlicher Authentifizierungsmerkmale, steigt damit der Aufwand für die Verwaltung seitens der Benutzer. Daher beginnen die Benutzer beispielsweise vermehrt ihre Passwörter aufzuschreiben, weiterzugeben oder unsichere Passwörter zu wählen[577], und die Sicherheit nimmt ab.

Weder für die Benutzer noch für die Organisationen ist eine verallgemeinerte quantitative Vereinheitlichung sinnvoll, da die effizient verwaltbare Anzahl auf beiden Seiten individuell variiert.

---

[576] Vgl. Bewertung der Kantengewichte in Abschnitt 5.4.2.

[577] Vgl. SASSE, M. A.; FLECHAIS, I.: Usable Security. Why Do We Need It? How Do We Get It?, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 16 f.

Während einige Benutzer eine bestimmte Anzahl an Authentifizierungsmerkmalen[578] ohne Einschränkung der Sicherheit verwenden können, beginnen andere bereits, die Passwörter aufzuschreiben und reduzieren damit die Sicherheit durch diese Offenlegung. Überdies ist die maximale quantitative Reduktion auf ein einziges Authentifizierungsmerkmal ebenfalls nicht sinnvoll, da hierdurch ein weiteres Sicherheitsrisiko bei dessen Missbrauch entsteht.[579] Diese Arbeit fokussiert heterogene IT-Strukturen im e-Science-Umfeld und klassifiziert daher Kriterien für eine effiziente Anzahl von Authentifizierungsmerkmalen. Es ist jedoch aufgrund der genannten individuellen Unterschiede nicht sinnvoll, eine allgemeingültige Zahl von Authentifizierungsmerkmalen zu quantifizieren. In einer Studie der Wichita State University wird beispielsweise eine durchschnittliche Anzahl von 8,5 unterschiedlichen Authentifizierungsmerkmalen der 315 befragten Benutzer der Universität genannt.[580] In den betrachteten Anwendungen schreiben dabei 15% ihre Passwörter aufgrund der Menge und Komplexität auf, 28,6% speichern das Passwort direkt nach der Eingabe in der zugehörigen Applikation auf ihrem Rechner und reduzieren so die Sicherheit.[581] Erhält ein Angreifer physikalischen Zugriff auf den Rechner, so kann er in diesem Fall direkt alle gespeicherten Passwörter resp. die zugehörigen Dienste und Ressourcen verwenden.

Eine effiziente Anzahl von Passwörtern wird seitens der Benutzer zusätzlich durch Komplexitätsvorgaben bestimmt. Sind die Benutzer beispielsweise gezwungen, Passwörter nach komplexen Vorgaben (z.B. Länge, Zeichenumfang, Historie) zu wählen, so steigt das qualitative Vereinheitlichungspotential bereits für eine geringe Anzahl von Merkmalen, da der Gesamtaufwand hoch ist. Komplexitätsvorgaben werden durch ihren Einfluss auf den Aufwand für die Benutzer im Folgenden unter der qualitativen Vereinheitlichung erfasst.

Im Folgenden wird daher vorrangig das Potential für qualitative Vereinheitlichungen bewertet, welches als Basis für eine anschließende quantitative Vereinheitlichung dient. Tabelle 5-22 zeigt die qualitative Bewertung des Vereinheitlichungspotentials von Authentifizierungsmerkmalen in einer heterogenen IT-Struktur. Dabei werden die in Abschnitt 5.5.1 genannten Diversitätskriterien ($\mathbf{Div_{Merkmal}}$) anhand der durch sie beeinflussten Bewertungskriterien für Aufwand und Sicherheit[582] bewertet.

---

[578] ohne Aufwand in Bezug auf die „Abrufbarkeit“ vgl. Abschnitt 5.4.1.

[579] Vgl. Verwendung eines einzigen Passworts in Abschnitt 4.1.2.

[580] Vgl. RILEY, S.: Password Security: What Users Know and What They Actually Do, 2006.

[581] Vgl. RILEY, S.: Password Security: What Users Know and What They Actually Do, 2006. Weitere Beispiele bilden die in den Abschnitten 1.1, 3.1 und 3.2.9 genannten Studien.

[582] Wie in den Abschnitten 5.4.2 und 5.4.3 definiert.

Wirkt ein Diversitätskriterium auf alle Kriterien in Bezug auf den Aufwand bei Verwendung und Verwaltung aus Sicht der Benutzer oder Organisationen ein, so besitzt es für diesen eine Relevanz von 100%. Sofern nicht alle Kriterien bei der Bemessung des Aufwands beeinflusst werden, wird deren prozentualer Anteil ermittelt. Die prozentuale Relevanz der resultierenden vier Bereiche des Aufwands wird gemittelt. Anschließend wird die Relevanz für den erzielten Nutzen aufsummiert und der Mittelwert als endgültige Relevanz bzgl. Aufwand und Sicherheit als Erwartungswert für den Nutzen fixiert.

Einfluss auf:	**Aufwand**				**Nutzen**
Diversität der Authentifizierungsmerkmale durch:	**Verwendung Benutzer** (Spezielle Anforderungen, Bequemlichkeit, Barrierefreiheit)	**Verwendung Org.** (Spezielle Anforderungen, Portabilität, Mobilität)	**Verwaltung Benutzer** (Wartbarkeit, Verarbeitungstiefe, Abrufbarkeit, Aussagekräftigkeit)	**Verwaltung Org.** (Benutzerverwaltung, Software, Hardware, Wartbarkeit)	**Sicherheit** (Vorhersagbarkeit, Fülle, Offenlegung, Angreifbarkeit, Datenschutz, Schutzziele, tech. Absicherung)
a) Unterschiedliche Ressourcen	■ Bequemlichkeit	■ Portabilität ■ Mobilität	■ Wartbarkeit ■ Abrufbarkeit	■ Benutzerverwaltung ■ Wartbarkeit	■ Vorhersagbarkeit ■ Fülle ■ Offenlegung ■ Angreifbarkeit
Qual. Relevanz: $(A_a+N_a)/2=53{,}6\%$	$A_a=(33\%+67\%+50\%+50\%)/4=50\%$				$N_a=57{,}1\%$
b) Verschiedene Organisationen	■ Bequemlichkeit	■ Portabilität ■ Mobilität	■ Wartbarkeit ■ Abrufbarkeit	■ Benutzerverwaltung ■ Wartbarkeit	■ Vorhersagbarkeit ■ Fülle ■ Offenlegung ■ Angreifbarkeit ■ Datenschutz
Qual. Relevanz: $(A_b+N_b)/2=60{,}7\%$	$A_b=(33\%+67\%+50\%+50\%)/4=50\%$				$N_b=71{,}4\%$

c) Verschiedene Authentifizierungsverfahren	■ Spezielle Anforderungen ■ Bequemlichkeit ■ Barrierefreiheit	■ Spezielle Anforderungen ■ Portabilität ■ Mobilität	■ Wartbarkeit ■ Verarbeitungstiefe ■ Abrufbarkeit	■ Hardware ■ Software ■ Wartbarkeit	■ Vorhersagbarkeit ■ Fülle ■ Offenlegung ■ Angreifbarkeit ■ Datenschutz ■ Schutzziele ■ Tech. Absicherung
Qual. Relevanz: $(A_c+N_c)/2=93{,}8\%$		$A_c=(100\%+100\%+75\%+75\%)/4=87{,}5\%$			$N_c=100\%$
d) Unterschiedliche Sicherheitsanforderungen und Authentifizierungsfaktoren	■ Spezielle Anforderungen ■ Bequemlichkeit ■ Barrierefreiheit	■ Spezielle Anforderungen ■ Portabilität ■ Mobilität	■ Wartbarkeit ■ Verarbeitungstiefe ■ Abrufbarkeit ■ Aussagekräftigkeit	■ Benutzerverwaltung ■ Hardware ■ Software ■ Wartbarkeit	■ Vorhersagbarkeit ■ Fülle ■ Offenlegung ■ Angreifbarkeit ■ Datenschutz ■ Schutzziele ■ Tech. Absicherung
Qual. Relevanz: $(A_d+N_d)/2=100\%$		$A_d=(100\%+100\%+100\%+100\%)/4=100\%$			$N_d=100\%$
e) Verschiedene Benutzer	- (wird nicht durch Benutzer beeinflusst)	■ Portabilität ■ Mobilität	- (wird nicht durch Benutzer beeinflusst)	■ Benutzerverwaltung ■ Wartbarkeit	■ Vorhersagbarkeit ■ Fülle ■ Offenlegung ■ Angreifbarkeit
Qual. Relevanz: $(A_e+N_e)/2=57{,}7\%$		$A_e=(67\%+50\%)/2=58{,}3\%$			$N_e=57{,}1\%$
f) Verschiedene Authentifizierungssysteme	- (wird nicht durch Benutzer beeinflusst)	■ Spezielle Anforderungen ■ Portabilität ■ Mobilität	- (wird nicht durch Benutzer beeinflusst)	■ Benutzerverwaltung ■ Hardware ■ Software ■ Wartbarkeit	■ Vorhersagbarkeit ■ Fülle ■ Offenlegung ■ Angreifbarkeit ■ Datenschutz ■ Tech. Absicherung
Qual. Relevanz: $(A_f+N_f)/2=92{,}9\%$		$A_f=(100\%+100\%)/2=100\%$			$N_f=85{,}7\%$

g) Verschiedene Formate der Authentifizierungskonten	- (wird nicht durch Benutzer beeinflusst)	■ Spezielle Anforderungen ■ Portabilität ■ Mobilität	- (wird nicht durch Benutzer beeinflusst)	■ Benutzerverwaltung ■ Software ■ Hardware ■ Wartbarkeit	■ Vorhersagbarkeit ■ Fülle ■ Offenlegung ■ Angreifbarkeit ■ Tech. Absicherung
Qual. Relevanz: $(A_g+N_g)/2=85{,}7\%$		$A_g=(100\%+100\%)/2=100\%$			$N_g=71{,}4\%$

Tabelle 5-22: Vereinheitlichungspotential bei Authentifizierungsmerkmalen

Höchste Relevanz für Aufwand und Sicherheit als resultierenden Nutzen besitzt gemäß Tabelle 5-22 $\mathbf{Div_{Merkmal.d}}$ mit 100% Prozent. Die Reduzierung von $\mathbf{Div_{Merkmal.d}}$ setzt sich wie folgt zusammen. Bei der Verwendung unterschiedlicher Sicherheitsanforderungen (z.B. Komplexitätsvorgaben der Passwörter) oder verschiedener Authentifizierungsfaktoren (z.B. Passwörter sowie Zertifikate und Tokens) benötigen die Benutzer für deren Verwendung ggf. spezielle Anforderungen (Umgang mit Zertifikaten, privaten Schlüsseln und Tokens). Die Bequemlichkeit ist ebenfalls eingeschränkt, da z.B. unterschiedliche komplexe Passwörter vorgehalten oder Zertifikate installiert werden müssen. Physikalische Tokens oder biometrische Merkmale schränken die Verwendung durch Personen mit körperlichen Behinderungen ein, Komplexitätsvorgaben bilden eine Barriere für Personen mit Gedächtnisschwäche oder Legasthenie.[583] Dies erhöht auch den Aufwand für deren Verwaltung bzw. Wartung aufseiten der Benutzer. Komplexe Passwörter bedürfen einer hohen Verarbeitungstiefe, z.B. durch wiederholte Eingabe während deren Definition, um sie zu erlernen, und sind deshalb aus psychologischer Sicht schwerer abrufbar[584]. Sofern bestimmte Zeichen oder Vorgaben für die Auswahl der möglichen Passwörter (z.B. Sonderzeichen) erforderlich sind, mindert dies die Aussagekräftigkeit.

Für die Organisationen entstehen bei der Verwendung der Authentifizierungsmerkmale spezielle Anforderungen, etwa durch Zertifikate und Tokens, für deren Verwendung das Personal gesonderte Kenntnisse benötigt. Zusätzliche Hardware (vgl. Tokens) mindert, sofern nicht plattformunabhängig verfügbar, die Portabilität. Hierbei bildet beispielsweise die Zertifikatvergabe zusätzlich einen

583 Vgl. RENAUD, K.: Evaluating Authentication Mechanisms, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 117.

584 Vgl. BISHOP, M.: Psychological Acceptability Revisited, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 4.

hohen Aufwand beim Skalieren für große Benutzergruppen.[585] Biometrische Sensoren, Unterstützung der Tokens bzw. Zertifikate sind häufig nicht ohne zusätzliche Installation möglich, so dass die Mobilität beispielsweise durch eine nicht realisierbare Verwendung im Internet-Café eingeschränkt wird.

Zertifikate oder auch unterschiedliche Passwörter eines Benutzers müssen separat verwaltet werden, so dass der Aufwand für die Benutzerverwaltung steigt. So ist für die Einrichtung von Tokens oder die Erfassung und Speicherung von biometrischen Merkmalen zusätzliche Hard- und Software erforderlich, die inkl. der zur Verfügung gestellten Verfahren darüber hinaus gewartet werden muss.

Andererseits bieten unterschiedliche Sicherheitsanforderungen und Authentifizierungsfaktoren eine höhere Sicherheit als resultierenden Nutzen. Die Vorhersagbarkeit komplexer Passwörter sinkt. Bei Vorraussetzung mehrerer Authentifizierungsfaktoren wird das Risiko der Vorhersagbarkeit zusätzlich reduziert. Komplexe Passwörter (z.B. mit Sonderzeichen oder größerer Länge) bieten eine größere Fülle bei der Wahl der Passwörter. Werden beispielsweise Tokens als zusätzlicher Authentifizierungsfaktor verwendet, so ist die Offenlegung des zugehörigen Passworts allein kein Risiko, da zusätzlich physikalischer Zugriff auf das Token zur erfolgreichen Authentifizierung erforderlich ist, wodurch auch ein Beispiel für die Reduzierung der Angreifbarkeit bzw. der technischen Absicherung gegeben wird. Durch die Speicherung des Authentifizierungsmerkmals auf einem Token bzw. einer Smart Card ist dieses nicht auslesbar, wodurch die Schutzziele Vertraulichkeit und Verbindlichkeit gestärkt werden.

Beispielsweise biometrische Merkmale haben jedoch einen negativen Einfluss auf den Datenschutz, da durch ihre Weitergabe ohne Zustimmung des Benutzers dessen eindeutige Identifikation auch durch Dritte möglich ist. Die genannten Beispiele veranschaulichen die Relevanz unterschiedlicher Sicherheitsanforderungen an Authentifizierungsmerkmale für die einheitliche Authentifizierung.

Für die verbleibende Diversitätskriterien treffen nicht alle qualitativen Kriterien für Aufwand und Sicherheit gemäß der Abschnitte 5.4.2 und 5.4.3 zu, so dass deren Relevanz für die Vereinheitlichung wie folgt abnimmt:

- **DivMerkmal.d** = 100% (Untersch. Sicherheitsanf. u. Authentifizierungsfaktoren)
- **DivMerkmal.c** = 93,8% (Verschiedene Authentifizierungsverfahren)

---

[585] Vgl. RIEGER, S. ET AL.: Self-Service PKI-Lösungen für eScience, in Paulsen, C. (Hrsg.): Sicherheit in vernetzten Systemen. 13. Workshop, 2006, S. B-1 ff.

- **DivMerkmal.f** = 92,9% (Verschiedene Authentifizierungssysteme)
- **DivMerkmal.g** = 85,7% (Verschiedene Formate der Authentifizierungskonten)
- **DivMerkmal.b** = 60,7% (Verschiedene Organisationen)
- **DivMerkmal.e** = 57,7% (Verschiedene Benutzer)
- **DivMerkmal.a** = 53,6% (Unterschiedliche Ressourcen)

5.5.3 Ermittlung geeigneter Integrationsformen

In Abschnitt 5.5.2 wurde das Potential für eine Vereinheitlichung von Authentifizierungsmerkmalen anhand der Diversitätskriterien aus Abschnitt 5.5.1 bestimmt. Quantifiziert wurde das Potential nach den in den Abschnitten 5.4.2 und 5.4.3 genannten Bewertungskriterien, die in Aufwand für die Authentifizierung und erzielte Sicherheit als Nutzen unterschieden werden. Um das Potential freizulegen und den Aufwand für Organisationen und Benutzer zu vermindern bzw. die erzielte Sicherheit zu steigern, werden im Folgenden die in 5.2 vorgestellten Integrationsmöglichkeiten für Authentifizierungsmerkmale beschrieben und, sofern bereits geeignete Verfahren existieren, auf die in Abschnitt 3.2 genannten bestehenden Lösungsansätze für einheitliche Authentifizierung abgebildet.

Für die Bestimmung des Potentials wurde im Abschnitt 5.5.2 zwischen quantitativer und qualitativer Vereinheitlichung unterschieden. Quantitativ ist das Potential von der individuell betrachteten IT-Struktur und der Anzahl der in ihr verwendeten Authentifizierungsmerkmale abhängig. Wie in Abschnitt 5.3.1 für die Sicht der Benutzer beschrieben, ermöglicht die Integration bzw. Reduktion von Authentifizierungsmerkmalen aus Sicht der Benutzer zusätzlich eine mögliche anschließende Reduktion der Authentifizierungsverfahren und -systeme. Aus dem in Abbildung 5-4 skizzierten Graphen ist zusätzlich ersichtlich, dass die Authentifizierungsmerkmale aus Sicht der Benutzer den primären Faktor für die Integration bzw. Vereinheitlichung der Authentifizierung in heterogenen IT-Strukturen darstellen. Sie sind dem Benutzer direkt über eine einzige Kante im Graphen zugeordnet und werden von ihm unmittelbar mit der Authentifizierung in Verbindung gebracht.[586]

Die nachfolgende Abbildung 5-9 zeigt die beschriebene Sicht der Benutzer auf die Authentifizierungsmerkmale. Jedes Merkmal ist dabei in Bezug auf dessen Verwendung und Verwaltung[587] mit einem Aufwand verbunden, der als Kantengewicht *A* in Abschnitt 5.2 definiert und gemeinsam mit der als Nutzen erzielten Sicherheit in Abbildung 5-9 übernommen wurde. Wie in Abschnitt 5.1

[586] Vgl. Relevanz der Authentifizierungsmerkmale für die Benutzer in Abschnitt 2.4.2.

[587] Vgl. Bewertungskriterien aus Abschnitt 5.4.2.

beschrieben, ist ein Authentifizierungsmerkmal genau einem Benutzer zugewiesen.[588] Eine qualitative Vereinheitlichung dieser Kanten[589] ist somit nicht möglich bzw. führt aus Sicht der Benutzer direkt zur Reduktion des zugehörigen Authentifizierungsmerkmals gemäß Int_a. Kantengewichte zwischen Benutzern und Authentifizierungsmerkmalen werden somit lediglich als Auswahlkriterium für die nach Int_a reduzierten Merkmale verwendet, weshalb die zugehörigen Kanten in Abbildung 5-9 grau dargestellt wurden. Eine Optimierung nach Int_b ist für die Benutzer möglich, indem mehrere Authentifizierungsmerkmale zu einem neuen Element zusammengefasst werden.

Organisationen verwalten, insbesondere bei einer hohen Anzahl von Benutzern, separate Authentifizierungsverfahren und -systeme, die jeweils eigene Authentifizierungsmerkmale verwenden. Das resultierende Vereinheitlichungspotential lässt sich durch Int_c und Int_d freilegen, indem Authentifizierungsverfahren und -systeme das jeweilige Authentifizierungsmerkmal nicht länger verwenden oder unterschiedlichen Verfahren dasselbe Merkmal zugewiesen wird. Besitzt das Authentifizierungsverfahren anschließend keine Kante zu einem Authentifizierungsverfahren, so entfällt das Merkmal direkt gemäß Int_a. Int_b wird für die Organisationen möglich, indem mehrere Merkmale zu einem gemeinsamen Merkmal integriert werden. In Abbildung 5-9 wurde die Menge der Authentifizierungssysteme nicht dargestellt, da diese nicht direkt, sondern über ein Authentifizierungsverfahren auf die Authentifizierungsmerkmale zugreifen. Kanten zwischen Organisationen und Verfahren wurden daher gepunktet dargestellt.

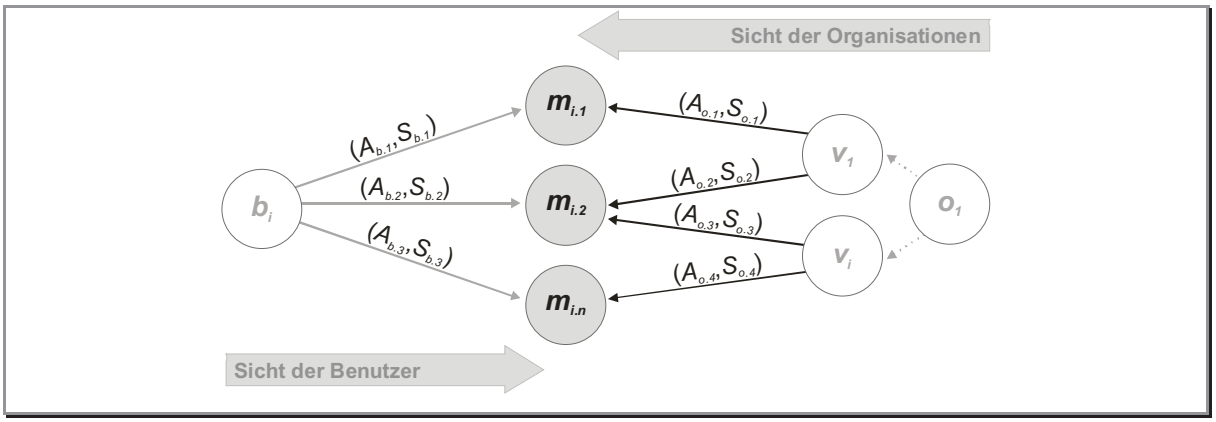

Abbildung 5-9: Sicht der Benutzer und Organisationen auf die Integration von Authentifizierungsmerkmalen

Als generelles Ziel für die Integration und Vereinheitlichung von Authentifizierungsmerkmalen in Bezug auf den Aufwand *A* lässt sich die Reduktion auf ein einziges Merkmal definieren. Diese

[588] Wie in Abschnitt 5.1 beschrieben, wird vorausgesetzt, dass Authentifizierungsmerkmale nicht von mehreren Benutzern gemeinsam verwendet werden.

[589] Gemäß Int_c oder Int_d, in Abschnitt 5.2.

Integration wird im Umfeld der IT-Sicherheit bzw. des Identity Management[590] auch unter dem Begriff „Single Password“ zusammengefasst.[591] Eingeschränkt wird das Erreichen dieser idealen Minimierung des Aufwands *A* jedoch durch die damit verbundene Reduktion der Sicherheit. Als Nebenbedingung gilt daher die gleichzeitige Gewährleistung der erzielten Sicherheit *S*.

Die Sicht der Benutzer sowie der Organisationen lässt sich jeweils als gerichteter Graph anhand der in Abbildung 5-9 gezeigten Kanten auffassen. Aus Sicht der Benutzer entsteht der Gesamtaufwand für die verwendeten und zu verwaltenden Authentifizierungsmerkmale direkt aus der Summe der Kantengewichte *A* zwischen Benutzern und ihren Authentifizierungsmerkmalen.

$$A_{b.merkmal} = \sum_{k=1}^{n} A_{b.k} \quad , \quad 0 \le A_{b.k} \le 7{,}1$$

Hierbei wird vorausgesetzt, dass die Kantengewichte *A* zuvor nach dem in Abschnitt 5.4.2 beschriebenen Verfahren quantifiziert wurden.

Von den Organisationen aus betrachtet, summiert sich der Gesamtaufwand aus den Kantengewichten zwischen Authentifizierungsverfahren und -merkmalen:

$$A_{o.merkmal} = \sum_{k=1}^{n} A_{o.k} \quad , \quad 0 \le A_{o.k} \le 7{,}1$$

Für die nachfolgenden Betrachtungen wird der Aufwand für Benutzer und Organisationen im Gesamtaufwand $A_{merkmal}$ zusammengefasst, wobei gilt:

$$A_k = A_{b.k} + A_{o.k} \quad , \quad 0 \le A_k \le 14{,}2 \quad , \quad A_{merkmal} = \sum_{k=1}^{n} A_k$$

Im Gegensatz zur Berechnung des Gesamtaufwands für Authentifizierungsmerkmale wird die insgesamt erzielte Sicherheit nicht direkt als Summe der Kantengewichte *S* beschrieben. Für die Berechnung der Sicherheit besitzt das Merkmal mit der geringsten Sicherheit ($S\min$) der Menge: $S :\Leftrightarrow \forall s \in S : S\min \le s$ eine hohe Relevanz.[592]

Wird das Merkmal mit der geringsten Sicherheit kompromittiert, so hat dies eine Auswirkung auf die gesamte durch die Authentifizierung erzielte Sicherheit. Das Verhältnis zwischen $S\min$ und dem größtmöglichen Wert 4,6 beschränkt die Summe der erzielten Sicherheit.[593] Die Multiplikati-

---

[590] Vgl. Identity Management z.B. durch Meta-Directories in Abschnitt 3.2.2.

[591] Vgl. die Verwendung eines einzigen Authentifizierungsmerkmals in Abschnitt 2.1.11.

[592] Dieses bestimmt die erzielbare Sicherheit, vgl. GERD TOM MARKOTTEN, D.: Benutzbare Sicherheit in informationstechnischen Systemen, 2003, S. 75.

[593] Vgl. Maximum für S in Abschnitt 5.4.3.

on der Summe der Kantengewichte S mit diesem Verhältnis bewirkt eine insgesamt erzielte Sicherheit von 0, sobald ein einziges Kantengewicht und damit $S\min = 0$ ist.

Allerdings wächst die Sicherheit nicht linear, da eine Steigerung der Sicherheit zusätzlich deren Komplexität erhöht. Mit zunehmender Komplexität lässt sich daher eine geringere Sicherheitssteigerung erzielen.[594] Um diesen Einfluss der Komplexität aus dem Gesamtergebnis herauszurechnen, wird im Folgenden die Wurzel aus der ermittelten Summe gezogen.

$$S_{merkmal} = \sqrt{\frac{S\min}{4{,}6} * \sum_{k=1}^{n} S_k} \quad , \qquad 0 \le S_k \le 4{,}6$$

Diese beschreibt auch die Sicherheitssteigerung, die entsteht, sofern zusätzliche Authentifizierungsmerkmale verwendet werden. Verwendet ein Benutzer z.B. drei Merkmale jeweils mit einer nach Abschnitt 5.4.3 quantifizierten Sicherheit von $S = 4$, so ermittelt sich eine insgesamt erzielte Sicherheit von:

$$S_{merkmal} = \sqrt{\frac{4}{4{,}6} * (4+4+4)} \approx 3{,}23 \quad \text{Sofern ein Merkmal 0 ist: } \sqrt{\frac{0}{4{,}6} * (0+4+4)} = 0$$

Durch die aufgestellte Formel wird auch die Reduktion der Sicherheit durch eine Vereinheitlichung der Authentifizierungsmerkmale beschrieben. Würde ein Merkmal aus dem Beispiel entfernt, und so der Aufwand für die Authentifizierung verringert, so ergibt sich für die erzielte Sicherheit:

$$S_{merkmal} = \sqrt{\frac{4}{4{,}6} * (4+4)} \approx 2{,}64$$

5.5.3.1 Reduktion der Authentifizierungsmerkmale (Int_a)

Am einfachsten lässt sich eine Vereinheitlichung durch die Reduktion der Authentifizierungsmerkmale erreichen. Abbildung 5-10 zeigt die Reduktion des Merkmals $m_{i.1}$, die implizit die Reduktion der Kanten mit $A_{b.1}$ und $A_{o.1}$, die in Abbildung 5-9 dargestellt wurden, zur Folge hat.

Eine solche Reduktion kann nur von den Organisationen aus erfolgen. Würde ein Benutzer auf ein Merkmal verzichten, so könnte er auch die Authentifizierungsverfahren und -systeme sowie damit verbundene Ressourcen nicht mehr verwenden. Ausgenommen wird hierbei der Sonderfall, in dem

[594] Vgl. Einfluss des Elements mit der geringsten erzielten IT-Sicherheit in WINDEMANN, P.; SCHLIENGER, T.; TEUFEL, S.: Messung der Informationssicherheit auf der Ebene der Sicherheitspolitik in MÖRIKE, M.; TEUFEL S.: Kosten & Nutzen von IT-Sicherheit in: HEILMANN, H. ET AL. (Hrsg.): HMD - Praxis der Wirtschaftsinformatik, Heft 248, 2006, S. 53 ff.

ein Benutzer z.B. auf einen separaten Passwort-Speicher[595] verzichtet, der zuvor ein separates Authentifizierungsmerkmal benötigte. Organisationen können eine entsprechende Reduktion beispielsweise durch die Reduktion der Sicherheitsanforderungen oder erforderlicher Authentifizierungsfaktoren[596] erreichen. Dies besitzt, wie in Abschnitt 5.5.2 bewertet, eine Relevanz von 100% für das Vereinheitlichungspotential. Ebenfalls kann durch die Reduktion der notwendigen Formate nach Int_a für die Speicherung der Authentifizierungskonten ($Div_{Merkmal.g}$) seitens der Organisationen eine Vereinheitlichung erzielt werden, welche eine Relevanz von 85,7% besitzt.[597]

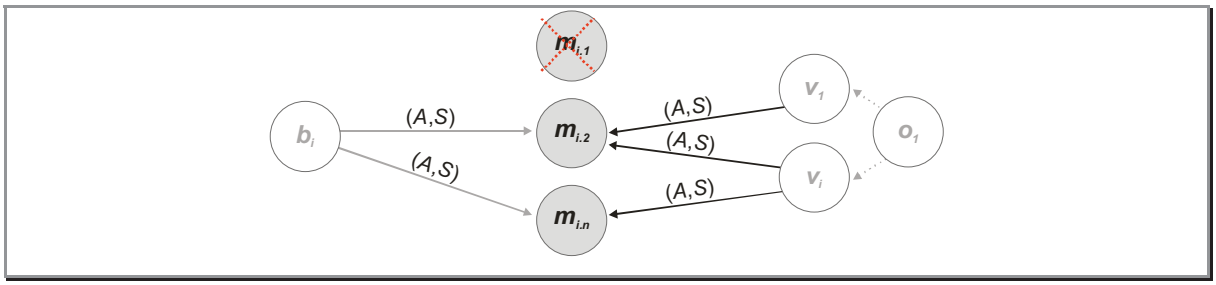

Abbildung 5-10: Reduktion der Authentifizierungsmerkmale

5.5.3.2 Integration der Authentifizierungsmerkmale (Int_b)

Abbildung 5-11 zeigt die Vereinheitlichungsmöglichkeiten durch die Integration mehrerer Authentifizierungsmerkmale zu einem neuen separaten Merkmal.

- In **a)** erfolgt die Integration für den Benutzer. Dies kann im einfachsten Fall bedeuten, dass der Benutzer für unterschiedliche Authentifizierungskonten das gleiche Passwort verwendet, was die insgesamt erzielte Sicherheit reduziert. Auch die Verwendung eines Passwort-Speichers oder eines Tokens zur Speicherung mehrerer Zertifikate fällt unter **a)**.[598] Während die Integration nach **a)** aufseiten der Benutzer eine Vereinheitlichung darstellt, bleibt die Diversität für die Organisationen erhalten, so dass **a)** für Organisationen keine Vorteile in Bezug auf Verwendung und Verwaltung von Authentifizierungsmerkmalen hat.

---

[595] Vgl. Speicherung von Passwörtern in einem Passwort-Speicher anhand eines einzigen Master-Passworts in Abschnitt 3.2.9.

[596] Vgl. $Div_{Merkmal.d}$ in Abschnitt 5.5.1.

[597] Vgl. Abschnitt 5.5.2.

[598] Vgl. Passwort-Speicher in Abschnitt 3.2.9 und die Speicherung von mehreren Merkmalen auf Tokens in Abschnitt 2.5.2.

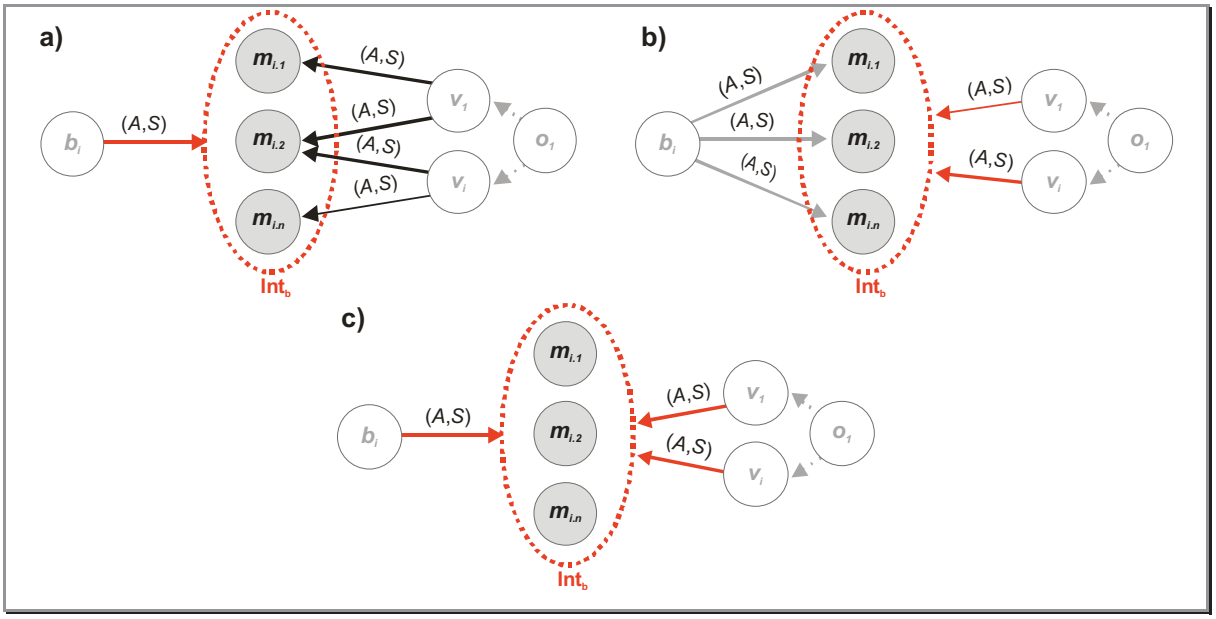

Abbildung 5-11: Integration von Authentifizierungsmerkmalen

- **b)** zeigt die Integration aufseiten der Organisationen, beispielsweise durch die Speicherung verschiedener Authentifizierungsmerkmale in einem Benutzerobjekt eines Verzeichnisdiensts.[599] Für die Benutzer bleibt die Diversität der Authentifizierungsmerkmale unverändert, so dass sich für sie kein Vorteil ergibt.
- Die in **c)** dargestellte Integration erfolgt gleichermaßen für Benutzer und Organisationen. **c)** kann z.B. durch die Realisierung eines Meta-Directorys oder Virtual Directorys erzielt werden.[600] Benutzer können hierbei ihre Passwörter für alle verwendeten Systeme zentral über das Meta-Directory setzen und dadurch ein einheitliches Authentifizierungsmerkmal verwenden. Organisationen können diese Merkmale einheitlich über das Meta-Directory verwalten.

5.5.3.3 Integration und Reduktion der Relationen (Int_c, Int_d)

Eine weitere Möglichkeit zur Vereinheitlichung der Authentifizierungsmerkmale bietet die Integration oder Reduktion von deren Kanten. Abbildung 5-12 zeigt die Reduktion der Kante zwischen b_i und $m_{i.n}$ aus Sicht des Benutzers. Diese führt nach den in Abschnitt 5.5.3.1 genannten Gesichtspunkten implizit zur anschließenden Reduktion des Authentifizierungsmerkmals $m_{i.n}$. Eine Integra-

[599] Vgl. die Speicherung von Authentifizierungskonten in Verzeichnisdiensten gemäß Abschnitt 3.2.2.

[600] Vgl. die Synchronisation von Authentifizierungsmerkmalen als Attribute über Meta-Directories in Abschnitt 3.2.2.

tion der Kanten (Int_d) aus Sicht der Benutzer ist für diese Kante nicht möglich, da ein Merkmal genau einem Benutzer zugewiesen ist.[601]

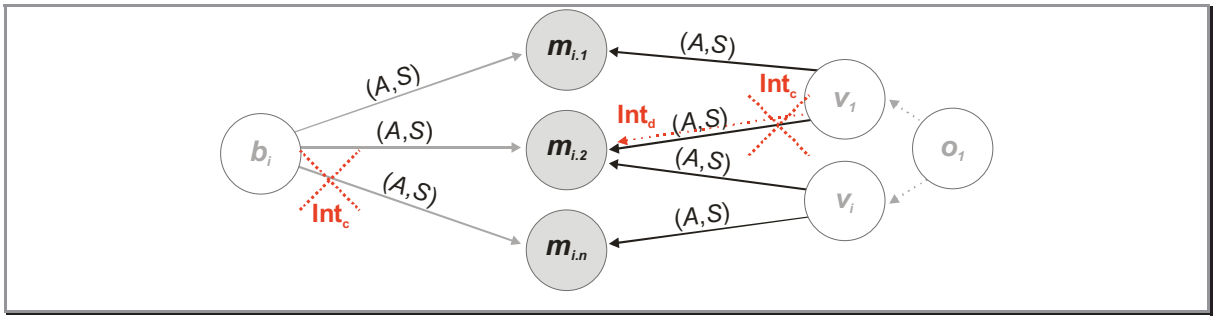

Abbildung 5-12: Integration und Reduktion der Relationen von Authentifizierungsmerkmalen

Organisationen können Verfahren, die unterschiedliche Authentifizierungsmerkmale verwenden, auf die Verwendung eines einzigen Merkmals reduzieren. Dies zeigt die Abbildung 5-12 für die Kante zwischen v_1 und $m_{i.2}$. Dabei kann diese, sofern das Merkmal erhalten bleiben soll, etwa da es eine erhöhte Sicherheit bietet, mit der Kante von v_i nach $m_{i.2}$ integriert werden. Beispielsweise kann ein Passwort, das für eine Web-basierte Authentifizierung sowie für Kerberos genutzt wird, ausschließlich auf die Verwendung in Kerberos umgestellt werden und so eine höhere Sicherheit sowie geringeren Aufwand erzielen.[602]

Sofern die Merkmale $m_{i.1}$ und $m_{i.n}$ keine Vorteile durch niedrigen Aufwand oder hohe Sicherheit aufweisen, bietet sich als Ideallösung die Integration der Kanten zwischen v_1 und $m_{i.1}$ sowie v_i und $m_{i.n}$ an. Dadurch würden anschließend implizit die Merkmale $m_{i.1}$ und $m_{i.n}$ aus Sicht der Organisationen reduzierbar.

5.5.4 Grenzen der Vereinheitlichung

Begrenzt wird die im vorherigen Abschnitt geschilderte Integration bzw. Reduktion von Authentifizierungsmerkmalen durch deren mit sinkender Anzahl der Merkmale zunehmende Homogenität.[603] Wird das Authentifizierungsmerkmal kompromittiert, so sind nach der Integration im Extremfall alle Authentifizierungsverfahren, -systeme und angebundenen Ressourcen gefährdet.

Um diese Problematik zu umgehen, ist es erforderlich parallel zur Reduzierung des Aufwands auch die erzielte Sicherheit zu erhöhen, um die Authentifizierung insgesamt ohne Nachteile durch die Vereinheitlichung zu optimieren.

---

[601] Vgl. die eindeutige Zuweisung der Merkmale zu einem Benutzer in Abschnitt 5.1.

[602] Vgl. Kerberos in Abschnitt 3.2.3 und Web-basierte Authentifizierung in Abschnitt 3.2.6.

[603] Vgl. Abschnitt 4.4.1.

Insbesondere für Authentifizierungsmerkmale, die auf den Faktoren Besitz oder persönliche Eigenschaft beruhen[604], gelten außerdem die in Abschnitt 4.4.2 und 4.4.3 genannten Kriterien Kompatibilität und gewünschte Portabilität als Grenze für die Vereinheitlichung. So müssen alle Authentifizierungsverfahren und -systeme die Verwendung des vereinheitlichten Authentifizierungsmerkmals unterstützen. Diese Einflüsse gehen allerdings bereits in die Bewertung des Aufwands ein.[605]

5.5.5 Resultierende Hypothesen

Aus der in Abschnitt 5.5 betrachteten Vereinheitlichung von Authentifizierungsmerkmalen werden folgende formale Hypothesen abgeleitet, die anschließend deduktiv, verifiziert und präzisiert werden.

H 1: Authentifizierungsmerkmale bilden das größte Potential für die Vereinheitlichung der Authentifizierung aus Sicht der Benutzer. Dabei kommt der Vereinheitlichung von Sicherheitsanforderungen und Authentifizierungsfaktoren die höchste Relevanz zu. Insbesondere für die Organisationen bilden Authentifizierungsmerkmale durch die Abhängigkeit von der Anzahl der Benutzer, der verwendeten Verfahren und Systeme auch das quantitativ größte Vereinheitlichungspotential.

H 2: Der Aufwand für Verwaltung und Verwendung von Authentifizierungsmerkmalen (sowie Authentifizierungsverfahren und -systemen) steigt linear mit deren Anzahl, während die erzielte Sicherheit mit zunehmender Komplexität vergleichsweise geringer ansteigt.

H 3: Die insgesamt erzielte Sicherheit wird maßgeblich durch das Authentifizierungsmerkmal mit der geringsten Sicherheit bestimmt. Dies gilt analog für Authentifizierungsverfahren und -systeme.

H 4: Ein geeignetes Integrationsverfahren für Authentifizierungsmerkmale stellt die Integration mehrerer Elemente (Int_b) dar, sofern diese sowohl seitens der Benutzer als auch für die Organisationen erfolgt.

H 5: Grenze für die Vereinheitlichung von Authentifizierungsmerkmalen (sowie Authentifizierungsverfahren und -systeme) stellt die zunehmende Homogenität dar. Die erzielte Sicherheit muss daher parallel zur Reduktion des Aufwands gesteigert werden. Kompromisslösungen in Bezug auf die Sicherheit können zusätzliche Authentifizierungsmerkmale (oder -verfahren und -systeme) erfordern und den Umfang der Vereinheitlichung begrenzen.

---

[604] Vgl. aktive Tokens in Abschnitt 2.5.2 oder biometrische Eigenschaften in 2.5.3.

[605] Vgl. z.B. Portabilität, Bequemlichkeit, Mobilität in Abschnitt 5.4.2.

5.6 Vereinheitlichung von Authentifizierungsverfahren

In den folgenden Abschnitten werden, analog zur Vereinheitlichung von Authentifizierungsmerkmalen im Abschnitt 5.5, Vereinheitlichungsmöglichkeiten für Authentifizierungsverfahren aufgezeigt. Zunächst wird in Abschnitt 5.6.1 die Diversität von Authentifizierungsverfahren ermittelt, die das in Abschnitt 5.6.2 bewertete Vereinheitlichungspotential bildet. Abschnitt 5.6.3 nennt Integrationsmöglichkeiten, die dieses Potential nutzen, um die Diversität von Authentifizierungsverfahren für Benutzer und Organisationen zu reduzieren. Begrenzt wird die Integration durch die in Abschnitt 4.4 genannten Faktoren. Abschließend werden als Basis für die Vereinheitlichung der Authentifizierung in heterogenen IT-Strukturen in der vorliegenden Arbeit in Abschnitt 5.6.5 Hypothesen für die Vereinheitlichung von Authentifizierungsverfahren aufgestellt.

5.6.1 Diversität von Authentifizierungsverfahren

Wie in Abschnitt 5.5.1 für Authentifizierungsmerkmale beschrieben, werden in diesem Abschnitt Diversitätskriterien von Authentifizierungsverfahren genannt. Die Diversität von Authentifizierungsverfahren wird in den in dieser Arbeit betrachteten heterogenen IT-Strukturen vorrangig durch nachstehende Faktoren bestimmt:

a) Verschiedene Ressourcen ($Div_{Verfahren.a}$)

Ressourcen in heterogenen IT-Strukturen verwenden in der Regel nicht ein gemeinsames bzw. einheitliches Authentifizierungssystem. Da die Authentifizierungssysteme ihrerseits häufig unterschiedliche bzw. inkompatible Authentifizierungsverfahren verwenden, wird so die Diversität von Authentifizierungsverfahren erhöht.

b) Verschiedene Organisationen ($Div_{Verfahren.b}$)

Kooperieren in einer heterogenen IT-Struktur mehrere Organisationen miteinander, so entsteht durch deren individuelle Verwendung von Authentifizierungsverfahren eine entsprechende Diversität. Dies kann auch durch unterschiedliche Authentifizierungssysteme begründet werden, die die einzelnen Organisationen verwenden.

c) Verschiedene Verfahren während einer Sitzung ($Div_{Verfahren.c}$)

Für die Benutzer äußert sich die Diversität von Authentifizierungsverfahren primär während deren Verwendung innerhalb einer Sitzung. Häufig müssen insbesondere in heterogenen Umgebungen durch die Diversität der Authentifizierungsverfahren und Ressourcen mehrfache Authentifizierungsvorgänge durchlaufen werden. Sofern nur ein Authentifizierungsvorgang pro Sitzung bzw. sogar während der gesamten Arbeitszeit benötigt wird, spricht man vom sog. „Single Sign-On“. Der Benutzer muss somit nur ein Authentifizierungsverfahren verwenden. In diesem Fall werden anschließende Authentifizierungsvorgänge nach der einmaligen Eingabe

bzw. dem Bereitstellen durch den Benutzer im Hintergrund und ohne Aufwand für den Benutzer ausgehandelt.

d) Unterschiedliche Sicherheitsanforderungen ($Div_{Verfahren.d}$)

Werden innerhalb der IT-Struktur unterschiedliche Sicherheitsanforderungen an die verwendeten Authentifizierungsverfahren gestellt, so führt dies erneut zu einer Diversität. Beispielsweise ist dies der Fall, wenn für den Zugriff auf sensitive Daten zusätzlich ein Zertifikat oder Token[606] erforderlich ist. Darüber hinaus sind Authentifizierungsverfahren häufig für bestimmte Einsatzgebiete vorgesehen. Ein Verfahren, das eine schwache Verschlüsselung verwendet, kann z.B. innerhalb einer geschlossenen IT-Struktur sicher angewendet werden. Für die Verwendung in dezentralen Strukturen (z.B. drahtlosen Netzwerken) ist jedoch in diesem Fall ein weiteres separates Authentifizierungsverfahren erforderlich, dass sich im Netzwerk dezentral verwenden lässt und zusätzlich die erforderliche Sicherheit der Authentifizierung garantiert.

e) Verschiedene Authentifizierungssysteme ($Div_{Verfahren.e}$)

Authentifizierungssysteme unterstützen in der Regel nur eine begrenzte Anzahl von Authentifizierungsverfahren. Werden von unterschiedlichen Ressourcen innerhalb der heterogenen IT-Struktur unterschiedliche Authentifizierungssysteme vorausgesetzt, so erhöht dies insgesamt die Diversität der verwendeten Authentifizierungsverfahren.

5.6.2 Bewertung des Vereinheitlichungspotentials

Wie im Abschnitt 5.5.2 für Authentifizierungsmerkmale eingeführt, wird in diesem Abschnitt das Potential für die Vereinheitlichung von Authentifizierungsverfahren definiert. Dabei wird, wie schon in Abschnitt 5.5.2 beschrieben, vorrangig das qualitative Vereinheitlichungspotential in der folgenden Tabelle 5-23 genannt. Die quantitativ mögliche Vereinheitlichung ergibt sich aus der Anzahl der innerhalb der heterogenen IT-Struktur verwendeten Authentifizierungsverfahren. Eine optimale Anzahl von Authentifizierungsverfahren kann, abgesehen von dem trivialen Idealfall, in dem genau ein Authentifizierungsverfahren verwendet werden kann, nicht unabhängig von der konkreten Größe und Ausprägung der heterogenen IT-Struktur definiert werden.

[606] Vgl. Authentifizierungsmerkmale basierend auf dem Besitz eines Tokens in Abschnitt 2.5.2.

Einfluss auf:	**Aufwand**				**Nutzen**
Diversität der Authentifizierungsverfahren durch:	**Verwendung Benutzer** (Spezielle Anforderungen, Bequemlichkeit, Barrierefreiheit)	**Verwendung Org.** (Spezielle Anforderungen, Portabilität, Mobilität)	**Verwaltung Benutzer** (Wartbarkeit, Verarbeitungstiefe, Abrufbarkeit, Aussagekräftigkeit)	**Verwaltung Org.** (Benutzerverwaltung, Software, Hardware, Wartbarkeit)	**Sicherheit** (Vorhersagbarkeit, Fülle, Offenlegung, Angreifbarkeit, Datenschutz, Schutzziele, tech. Absicherung)
a) Unterschiedliche Ressourcen	■ Spezielle Anforderungen ■ Bequemlichkeit ■ Barrierefreiheit	■ Spezielle Anforderungen ■ Portabilität ■ Mobilität	■ Wartbarkeit ■ Verarbeitungstiefe	■ Software ■ Hardware ■ Wartbarkeit	■ Offenlegung ■ Angreifbarkeit ■ Schutzziele ■ Tech. Absicherung
Qual. Relevanz: $(A_a+N_a)/2=69{,}2\%$	$A_a=(100\%+100\%+50\%+75\%)/4=81{,}3\%$				$N_a=57{,}1\%$
b) Verschiedene Organisationen	■ Spezielle Anforderungen ■ Bequemlichkeit ■ Barrierefreiheit	■ Spezielle Anforderungen ■ Portabilität ■ Mobilität	■ Wartbarkeit ■ Verarbeitungstiefe	■ Software ■ Hardware ■ Wartbarkeit	■ Offenlegung ■ Angreifbarkeit ■ Datenschutz ■ Schutzziele ■ Tech. Absicherung
Qual. Relevanz: $(A_b+N_b)/2=76{,}3\%$	$A_b=(100\%+100\%+50\%+75\%)/4=81{,}3\%$				$N_b=71{,}4\%$
c) Verschiedene Authentifizierungsverfahren während einer Sitzung	■ Spezielle Anforderungen ■ Bequemlichkeit ■ Barrierefreiheit	■ Spezielle Anforderungen ■ Portabilität ■ Mobilität	■ Wartbarkeit	■ Hardware ■ Software ■ Wartbarkeit	■ Offenlegung ■ Angreifbarkeit ■ Schutzziele ■ Tech. Absicherung
Qual. Relevanz: $(A_c+N_c)/2=66{,}1\%$	$A_c=(100\%+100\%+25\%+75\%)/4=75\%$				$N_c=57{,}1\%$

d) Unterschiedliche Sicherheitsanforderungen	■ Spezielle Anforderungen ■ Bequemlichkeit ■ Barrierefreiheit	■ Spezielle Anforderungen ■ Portabilität ■ Mobilität	■ Wartbarkeit ■ Verarbeitungstiefe	■ Hardware ■ Software ■ Wartbarkeit	■ Offenlegung ■ Angreifbarkeit ■ Datenschutz ■ Schutzziele ■ Tech. Absicherung
Qual. Relevanz: $(A_d+N_d)/2=76,3\%$		$A_d=(100\%+100\%+50\%+75\%)/4=81,3\%$			$N_d=71,4\%$
e) Verschiedene Authentifizierungssysteme	- (wird nicht durch Benutzer beeinflusst)	■ Spezielle Anforderungen ■ Portabilität ■ Mobilität	- (wird nicht durch Benutzer beeinflusst)	■ Benutzerverwaltung ■ Hardware ■ Software ■ Wartbarkeit	■ Offenlegung ■ Angreifbarkeit ■ Datenschutz ■ Schutzziele ■ Tech. Absicherung
Qual. Relevanz: $(A_e+N_e)/2=85,7\%$		$A_e=(100\%+100\%)/2=100\%$			$N_e=71,4\%$

Tabelle 5-23: Vereinheitlichungspotential bei Authentifizierungsverfahren

Das höchste Potential für die Vereinheitlichung von Authentifizierungsverfahren bildet die durch verschiedene Authentifizierungssysteme aufseiten der Organisationen entstehende Diversität ($Div_{Verfahren.e}$) mit 85,7%. Verwendung und Verwaltung durch die Benutzer gehen in die Betrachtung des Potentials nicht ein, da die Authentifizierungssysteme durch die Organisationen betrieben werden.

Die Bewertung der Relevanz von $Div_{Verfahren.e}$ setzt sich wie folgt zusammen: Für die Organisationen kann die Verwendung unterschiedlicher Authentifizierungsverfahren verschiedener Authentifizierungssysteme ($Div_{Verfahren.e}$) spezielle Anforderungen beinhalten. Beispielsweise muss ggf. Personal in Konfiguration und Handhabung der Authentifizierungsverfahren geschult werden. Durch die eingeschränkte Kompatibilität der Authentifizierungsverfahren untereinander wird zusätzlich die Portabilität und Mobilität eingeschränkt.

Separate Authentifizierungsverfahren und -systeme erfordern in der Regel eine separate Benutzerverwaltung. Ebenfalls relevant für den Aufwand hinsichtlich der Verwaltung der Authentifizierungsverfahren sind etwaige zusätzliche Hard- und Software, die von den Verfahren vorausgesetzt wird. Dies bezieht auch deren Anschaffung und Wartung mit ein.

Für die Sicherheit hat die Diversität von Authentifizierungsverfahren durch verschiedene Authentifizierungssysteme einen Einfluss auf die Offenlegung von Informationen während der Authentifizierungsvorgänge. Je nach Sicherheit und Angreifbarkeit der Verfahren können Informationen von

unberechtigten Dritten erlangt werden. Sie sollten daher gängige Schutzziele der IT-Sicherheit (Vertraulichkeit, Integrität, Verfügbarkeit, Verbindlichkeit) adressieren. Einzelne Verfahren können datenschutzrelevante Angaben der Benutzer erfordern. Beispielsweise ist für die Verwendung von biometrischen Authentifizierungsverfahren ggf. die Speicherung bzw. Verwendung eines Fingerabdrucks erforderlich. Authentifizierungsverfahren können durch zusätzliche technische Mittel abgesichert werden. So gibt es spezielle, manipulationssichere Hardware, die die Authentifizierung z.B. in einem geschützten externen Gehäuse durchführt.

Für die verbleibenden Diversitätskriterien treffen weniger qualitative Kriterien für Aufwand und Sicherheit gemäß der Abschnitte 5.4.2 und 5.4.3 zu, so dass deren Relevanz wie folgt abnimmt:

- **DivVerfahren.e** = 85,7% (Verschiedene Authentifizierungssysteme)
- **DivVerfahren.d** = 76,3% (Unterschiedliche Sicherheitsanforderungen)
- **DivVerfahren.b** = 76,3% (Verschiedene Organisationen)
- **DivVerfahren.a** = 69,2% (Verschiedene Ressourcen)
- **DivVerfahren.c** = 66,1% (Verschiedene Authentifizierungsverf. während einer Sitzung)

Auffallend ist hierbei, dass die Diversität durch verschiedene Authentifizierungsverfahren während einer Sitzung, die von „Single Sign-On"-Lösungen[607] adressiert wird, für die Verwendung durch Benutzer und Organisationen zwar vollständig relevant ist, jedoch insgesamt durch den geringen Einfluss auf die Verwaltung und erzielte Sicherheit die geringste qualitative Relevanz aufweist.

5.6.3 Ermittlung geeigneter Integrationsformen

In Abschnitt 5.5.3 wurde die Anwendung der in Abschnitt 5.2 genannten Integrationsverfahren am Beispiel von Authentifizierungsmerkmalen beschrieben. Im Folgenden werden analog Authentifizierungsverfahren integriert und vereinheitlicht. Abbildung 5-13 zeigt die Sicht der Benutzer und Organisationen auf die durch die Vereinheitlichung und Integration ermöglichte Optimierung.

[607] Vgl. Definition von „Single Sign-On" in Abschnitt 2.1.12.

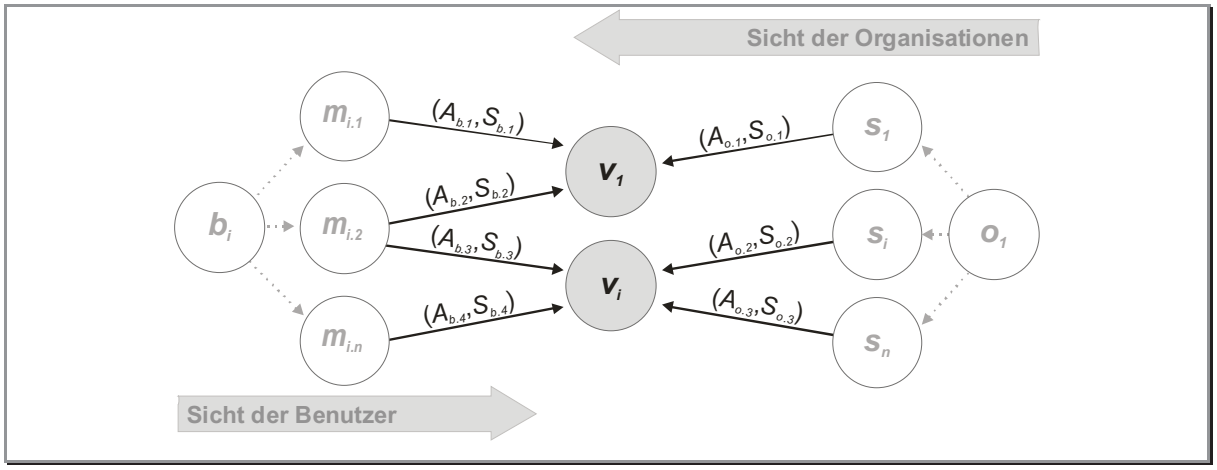

Abbildung 5-13: Sicht der Benutzer und Organisationen auf die Integration von Authentifizierungsverfahren

Bei der Integration der Authentifizierungsverfahren wird neben deren quantitativer Anzahl die Summe der zugehörigen qualitativen Kanten (in Bezug auf Aufwand und Sicherheit) betrachtet. Authentifizierungsverfahren verwenden Authentifizierungsmerkmale der Benutzer für die Authentifizierung, wobei ein Verfahren mehrere Merkmale und ein Merkmal mehrere Verfahren verwenden kann. Aus Sicht der Benutzer sind daher, anders als in Abschnitt 5.5.3 für Authentifizierungsmerkmale beschrieben, neben den Integrationen Int_a und Int_b auch die Integrationen Int_c und Int_d möglich[608].

Aus Sicht der Organisationen werden Authentifizierungsverfahren von unterschiedlichen Authentifizierungssystemen, denen wiederum Ressourcen zugewiesen sind, verwendet. Da ein Verfahren mehrere Systeme und ein System mehrere Verfahren verwenden kann, bieten sich auch hier die Integrationen Int_c und Int_d neben Int_a und Int_b an.

Als generelles Ziel der Optimierung kann die Reduktion auf einziges Authentifizierungsverfahren angenommen werden[609]. Dieses Ziel lässt sich jedoch, nicht zuletzt aufgrund der im nachfolgenden Abschnitt 5.6.4 beschriebenen Grenzen, nicht vollständig erreichen. Hersteller von Produkten und Lösungen in diesem Umfeld haben daher den Terminus für dieses Ziel von „Single Sign-On“ auf „Reduced Sign-On“ gemäß den Grenzen in der Realität angepasst. Häufig spricht man auch von „Single Sign-On“ für einen klar abgegrenzten Bereich als Teillösung innerhalb einer heterogenen IT-Struktur.

Hierfür müssen neben den Authentifizierungsverfahren auch die Authentifizierungsmerkmale integriert werden. Würden die reduzierten Authentifizierungsverfahren weiterhin unterschiedliche

[608] Vgl. die Definition der Integrationsformen in Abschnitt 5.2.

[609] Vgl. Single Sign-On durch die Verwendung eines einzigen einheitlichen Verfahrens in Abschnitt 2.1.12.

Authentifizierungsmerkmale verwenden, müssten diese jeweils während einer Sitzung abgefragt werden. Ein „Single Sign-On“ wäre somit unmöglich.

Analog zur Berechnung des Aufwands von Authentifizierungsmerkmalen in Abschnitt 5.5.3 ergibt sich für den Gesamtaufwand aus Sicht der Benutzer und Organisationen in Bezug auf Authentifizierungsverfahren ($A_{verfahren}$):

$$A_{verfahren} = \sum_{k=1}^{n} A_k \;, \qquad \text{wobei gilt: } 0 \le A_k \le 14{,}2$$

Die insgesamt erzielte Sicherheit aufseiten der Benutzer ($S_{b.verfahren}$) und Organisationen ($S_{o.verfahren}$) ergibt sich durch:

$$S_{verfahren} = \sqrt{\frac{S\min}{4{,}6} * \sum_{k=1}^{n} S_k} \;, \quad \text{wobei gilt: } 0 \le S_k \le 4{,}6$$

5.6.3.1 Reduktion von Authentifizierungsverfahren (Int_a)

Wird auf die Verwendung einzelner Authentifizierungsverfahren verzichtet, so reduzieren sich auch die damit verbundenen Kanten zu Merkmalen und Systemen. Int_a bildet somit ein hohes Vereinheitlichungspotential. Ein Verzicht auf einzelne Authentifizierungsverfahren kann nur aufseiten der Organisationen erfolgen. Benutzer müssen die unterschiedlichen Verfahren der Organisationen in jedem Fall verwenden, sofern sie auf die damit geschützten Ressourcen zugreifen möchten.

Für Organisationen ist die Reduktion nach Int_a, wie in Abbildung 5-14 illustriert, nur dann möglich, wenn kein Merkmal oder System das Verfahren voraussetzt.

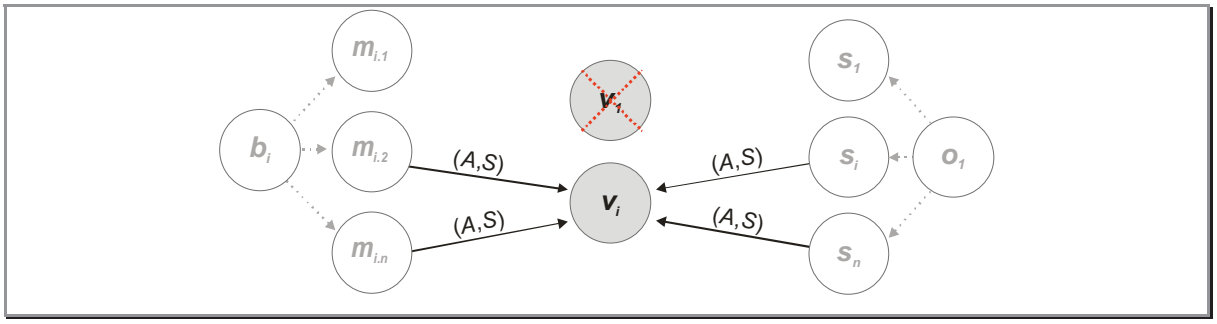

Abbildung 5-14: Reduktion der Authentifizierungsverfahren

Typische Beispiele für die Reduktion der Authentifizierungsverfahren stellen Kerberos und die Verwendung einer Public-Key-Infrastruktur mit X.509 als Authentifizierungsverfahren dar.[610] Beide ermöglichen eine umfassende „Single Sign-On“-Lösung, müssen allerdings von allen Ressour-

[610] Vgl. Kerberos in Abschnitt 3.2.3 und Public-Key-Infrastrukturen in Abschnitt 3.2.4.

cen bzw. Authentifizierungssystemen in der heterogenen IT-Struktur unterstützt werden. Bei X.509 ist zusätzlich die Verwaltung von Zertifikaten als Authentifizierungsmerkmal durch die Benutzer erforderlich.

Aufgrund dieser Einschränkung stellt Int_a eher die Folge aus Int_c und Int_d dar. Als Ausgangspunkt der Integration kann Int_a dann fungieren, wenn beispielsweise auf unterschiedliche Sicherheitsanforderungen ($Div_{Verfahren.b}$), ggf. auch während einer Sitzung ($Div_{Verfahren.c}$), verzichtet wird.[611]

5.6.3.2 Integration von Authentifizierungsverfahren (Int_b)

Mehrere separate Authentifizierungsverfahren können in einem einzigen Verfahren gemäß Int_b, wie in Abbildung 5-15 dargestellt, zusammengefasst werden.

- **a)** zeigt in Abbildung 5-15 die Integration für die Benutzer. Diese kann beispielsweise durch die Installation von modularen Authentifizierungsclients und Proxies erfolgen.[612] Auch die Automatisierung der Authentifizierung aufseiten der Benutzer beinhaltet neben der Integration auf ein Merkmal die Möglichkeit dieses für unterschiedliche Verfahren zu verwenden.[613] Durch die Realisierung von Web-Anwendungen, die im Hindergrund auf unterschiedliche Authentifizierungsverfahren zurückgreifen, ist ebenfalls eine Integration möglich.[614] Wird die Authentifizierung aus Sicht der Benutzer im Hintergrund auf verschiedene Authentifizierungsverfahren abgebildet, z.B. über Virtual Directories, so fällt auch dies unter die in **a)** gezeigte Integration.[615]

---

[611] Vgl. die Definition von $Div_{Verfahren.b}$ und $Div_{Verfahren.c}$ in Abschnitt 5.6.1.

[612] Vgl. modulare Authentifizierungsclients und Proxies in Abschnitt 3.2.8.

[613] Vgl. Authentifizierungsautomatismen in Abschnitt 3.2.9.

[614] Vgl. die Authentifizierung an Web-Seiten, deren Web-Server im Hintergrund unterschiedliche Authentifizierungsverfahren und -systeme verwenden, in Abschnitt 3.2.6.

[615] Vgl. Virtual Directories in Abschnitt 3.2.2.

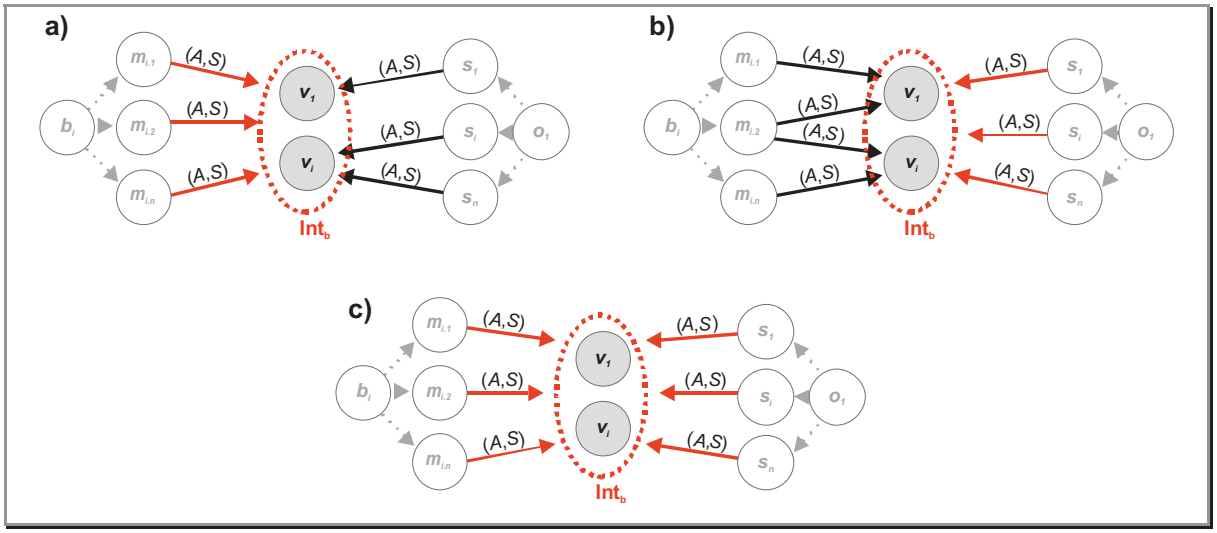

Abbildung 5-15: Integration von Authentifizierungsverfahren

- In **b)** erfolgt die Integration für die Organisationen. Lösungen für eine solche Integration bieten beispielsweise RADIUS als Netzwerk-Authentifizierungsprotokoll. Ein RADIUS-Server kann im Hintergrund unterschiedliche Authentifizierungsverfahren verwenden, um den Benutzern Zugriff auf Netzwerkressourcen zu gewähren.[616] Auch Verzeichnisdienste integrieren in der Regel unterschiedliche Authentifizierungsverfahren.[617]

- Die Integration sowohl aufseiten der Benutzer als auch seitens der Organisationen zeigt **c)**. Diese kann teilweise mit bestehenden Lösungen wie RADIUS als Netzwerk-Authentifizierungsprotokoll und Verzeichnisdiensten realisiert werden.[618] Der Dienst muss in diesem Fall unterschiedliche Authentifizierungsmerkmale der Benutzer (z.B. Passwörter, Zertifikate) unterstützen und diese für die Authentifizierungssysteme über verschiedene Verfahren überprüfen. Integriert wird diese Anforderung in neueren Authentifizierungsverfahren wie SAML und Shibboleth; allerdings adressieren diese primär zunächst Web-Anwendungen.[619] Ein SAML-Token kann unterschiedliche Authentifizierungsmerkmale wie z.B. Challenge-Passwort und unterschiedliche Authentifizierungsverfahren verwenden. Unterschiedliche Systeme, die die Ressourcen bereitstellen, akzeptieren diese Bestandteile des Tokens anschließend für die Authentifizierung.

---

[616] Vgl. Verwendung von RADIUS-Servern in Abschnitt 3.2.5.

[617] Vgl. z.B. LDAP oder Kerberos, wie in Abschnitt 3.2.2 und 3.2.3 beschrieben.

[618] Vgl. die Verwendung von RADIUS-Servern in Abschnitt 3.2.5 oder Verzeichnisdienste in Abschnitt 3.2.2.

[619] Wie in Abschnitt 3.2.7 beschrieben.

5.6.3.3 Integration und Reduktion der Relationen (Int_c, Int_d)

Kann ein Benutzer mit unterschiedlichen Authentifizierungsmerkmalen das gleiche Verfahren und dahinter liegende Systeme und Ressourcen verwenden, so kann, sofern das separate Merkmal nicht beispielsweise eine höhere Sicherheit bietet, auf die Verwendung eines der Merkmale und damit die Relation bzw. Kante zum Authentifizierungsverfahren verzichtet werden. Die Abbildung 5-16 zeigt dies in der Reduktion der Kante zwischen $m_{i.n}$ und v_i gemäß Int_c.

Int_d wird in Abbildung 5-16 für die Integration der Kante s_1, v_1 zur Kante s_1, v_i illustriert. Sie kann z.B. dadurch ermöglicht werden, dass das Authentifizierungssystem s_1 zukünftig auch das Verfahren v_i unterstützt.

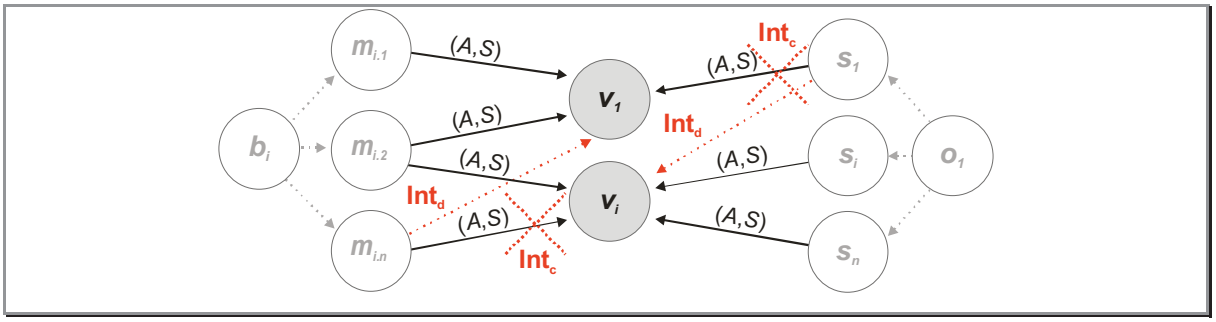

Abbildung 5-16: Integration und Reduktion der Relationen von Authentifizierungsverfahren

Als Beispiel für die Umsetzung von Int_d kann Kerberos herangezogen werden.[620] Hier wird durch die Unterstützung des Standards Kerberos durch unterschiedliche Authentifizierungssysteme eine Integration der Authentifizierungsverfahren möglich. Ähnliches gilt für den LDAP-Standard in Verzeichnisdiensten oder dessen Vorläufer NIS und Yellow Pages (yp).[621] Auch Public-Key-Infrastrukturen (X.509) und Netzwerk-Authentifizierungsprotokolle (wie 802.1X) versuchen eine Unterstützung durch unterschiedliche Authentifizierungssysteme zu erzielen.[622] Allerdings setzen sie damit analog zu Kerberos deren Anpassung explizit voraus.

Im Gegensatz dazu bieten Federation-Lösungen die Unterstützung unterschiedlicher Authentifizierungsverfahren und damit eine flexible Integration nach Int_d, wobei Teile der Authentifizierungssysteme weiter verwendet bzw. von Komponenten der Federation-Lösung genutzt werden können.[623]

---

[620] Vgl. die Verwendung von Kerberos und die Erweiterung bestehender Anwendungen um die Unterstützung von Kerberos in Abschnitt 3.2.3.

[621] Verzeichnisdienste sowie NIS und yp wurden in Abschnitt 3.2.2 beschrieben.

[622] Vgl. Public-Key-Infrastrukturen in Abschnitt 3.2.4 und 802.1X in Abschnitt 3.2.5.

[623] Vgl. Federation-basierte Authentifizierung in Abschnitt 3.2.7.

An die Integration nach Int_c und Int_d kann sich direkt die Reduktion nach Int_a anschließen, sofern durch die Minderung bzw. Änderung der Kanten Knoten entstehen, die keine Kanten mehr zu Authentifizierungsverfahren besitzen.

5.6.4 Grenzen der Vereinheitlichung

Begrenzt wird die Vereinheitlichung der Authentifizierungsverfahren in erster Linie durch deren Kompatibilität mit Authentifizierungssystemen. Nur ein Authentifizierungsverfahren, das alle Authentifizierungssysteme und damit verbundene Ressourcen innerhalb einer heterogenen IT-Struktur unterstützt, lässt sich in dieser effizient als einheitliches Verfahren verwenden. Dieser Aspekt wurde auch bereits in Abschnitt 4.4.2 beschrieben. Abschnitt 4.4.3 nennt zusätzlich die Portabilität resp. Flexibilität der Verfahren als Kriterium bzw. Einschränkung für die mögliche Vereinheitlichung.

Zusätzlich übt die erforderliche Sicherheit einen Einfluss auf die Vereinheitlichung aus. Bietet die erzielte Vereinheitlichung nicht sowohl die Minimierung des Aufwands als auch die Gewährleistung der erforderlichen IT-Sicherheit, so muss für sicherheitskritische Anwendungen ein Kompromiss, z.B. anhand verbleibender zusätzlicher Verfahren mit höherer Sicherheit definiert werden. Wird ein einziges Verfahren für die Authentifizierung verwendet, so ist auch die gesamte durch die Authentifizierung erzielte Sicherheit von diesem und dessen Sicherheitslücken abhängig. Gelingt es einem Angreifer, eine Lücke in dem Verfahren zu nutzen, stehen ihm auf Grund der Vereinheitlichung alle Ressourcen der IT-Struktur zur Verfügung.

Sicherheitsanforderungen können in Bezug auf die Verfahren auch organisatorische Bedeutung haben, beispielsweise wenn eine dedizierte Nutzergruppe keinen Zugriff auf spezielle Ressourcen erlangen soll. Sofern dies nicht allein eine nach der Authentifizierung angeordnete Autorisierung absichern soll, kann durch separate Verfahren und Systeme gewährleistet werden, dass nicht berechtigte Benutzer bereits bei der Authentifizierung abgewiesen werden.

5.6.5 Resultierende Hypothesen

Ergänzend zu den in Abschnitt 5.5.5 genannten Hypothesen für die Vereinheitlichung von Authentifizierungsmerkmalen werden diese für die folgenden Betrachtungen in Bezug auf Authentifizierungsverfahren ergänzt um:

H 6: „Single Sign-On“ besitzt in Bezug auf Aufwand und erzielte Sicherheit eine niedrige Relevanz insbesondere aus Sicht der Organisationen. Für die Umsetzung von „Single Sign-On“

gilt daher das Pareto-Prinzip, das beschreibt, dass 80% des Erfolges (resp. der Vereinheitlichung) durch 20% des Aufwands erzielt werden, während für die Erlangung der restlichen 20% des Erfolgs 80% des Aufwands erforderlich wären („80-zu-20-Regel“).[624] 80% der Systeme in einer heterogenen IT-Struktur lassen sich mit einem einheitlichen Authentifizierungsverfahren verwenden, die restlichen 20% in das „Single Sign-On“-Konzept zu integrieren bedeutet jedoch 80% des Gesamtaufwands.

H 7: Als geeignetes Integrationsverfahren für Authentifizierungsverfahren bietet sich die Integration der Relationen (Int_d) an. Diese kann eine anschließende Reduktion der Elemente (Int_a) zur Folge haben. Für die Integration in heterogenen Umgebungen wäre auch die Integration der Elemente (Int_b) (beidseitig für Benutzer und Organisationen) gut geeignet. Der Aufwand für die Verwaltung ist nach Int_b jedoch in jedem Fall höher als nach einer Vereinheitlichung durch Int_d.

5.7 Vereinheitlichung von Authentifizierungssystemen

Die folgenden Abschnitte beschreiben, analog zu der in Abschnitt 5.5 beschrieben Vereinheitlichung von Authentifizierungsmerkmalen, die Vereinheitlichung von Authentifizierungssystemen in heterogenen IT-Strukturen. Abschnitt 5.7.1 nennt die Faktoren, die zu einer Diversität der Authentifizierungssysteme führen. Diese bilden damit das Potential, das durch eine Vereinheitlichung erzielt werden kann und in Abschnitt 5.7.2 beschrieben wird. Konkrete Vereinheitlichungsmöglichkeiten werden im Abschnitt 5.7.3 aufgezeigt. Begrenzt werden die dort genannten Integrationen und Reduktionen durch die in Abschnitt 5.7.4 geschilderten Aspekte. Abschnitt 5.7.5 ergänzt schließlich die für Authentifizierungsmerkmale und -verfahren postulierten Hypothesen für die weitere Betrachtung in dieser Arbeit.

5.7.1 Diversität von Authentifizierungssystemen

In heterogenen IT-Strukturen kommen in der Regel, wie in Abschnitt 3.1 beschrieben, verschiedene Authentifizierungssysteme zum Einsatz. Die resultierende Diversität wird dabei insbesondere durch folgende Faktoren bestimmt.

a) Verschiedene Organisationen ($Div_{Systeme.a}$)

Benutzer, die Ressourcen unterschiedlicher Organisationen verwenden, oder Organisationen, die kooperieren, müssen in der Regel unterschiedliche Authentifizierungssysteme verwenden.

[624] Vgl. KOCH, R.: Das 80/20 Prinzip. Mehr Erfolg durch weniger Aufwand, 2. Auflage, 2004.

Bedingt wird dies z.B. durch etablierte Strukturen bzw. Software-Lösungen oder Plattformen, die in der jeweiligen Organisation verwendet werden. Da die Authentifizierungssysteme die Konten der Benutzer vorhalten[625], bedeutet deren Diversität für die Benutzer in der Regel einen zusätzlichen Aufwand für die Verwaltung ihrer unterschiedlichen Authentifizierungskonten (z.B. durch unterschiedliche Passwörter). Ändert der Benutzer sein Passwort im Authentifizierungssystem der einen Organisation, so muss er es manuell auch in allen anderen Authentifizierungssystemen setzen, um ein konsistentes Ergebnis zu erzielen.

b) Verschiedene Ressourcen und deren Kompatibilität mit Authentifizierungssystemen ($Div_{Systeme.b}$)

Wie bereits in Abschnitt 5.1 beschrieben, werden Ressourcen Authentifizierungssystemen zugewiesen, die mit der Hilfe von Authentifizierungsverfahren den Zugriff auf die berechtigten Benutzer limitieren. Jede Ressource setzt jedoch in der Regel bestimmte Authentifizierungssysteme voraus oder verwendet sogar ein eigenes separates Authentifizierungssystem. Beispielsweise können Authentifizierungssysteme häufig nicht plattformübergreifend verwendet werden.[626]

c) Verschiedene Sicherheitsanforderungen ($Div_{Systeme.c}$)

An die Authentifizierung werden höhere Anforderungen gestellt, sofern diese sensible Daten schützt. Somit werden häufig unterschiedliche Authentifizierungssysteme für unterschiedliche Sicherheitsanforderungen verwendet. Während die Authentifizierung am lokalen Arbeitsplatzrechner z.B. per Kerberos[627] erfolgt, kann für den Zugriff auf sensible Daten über eine Web-Seite zusätzlich die Eingabe eines One Time Passwords[628] erforderlich sein.

5.7.2 Bewertung des Vereinheitlichungspotentials

Tabelle 5-24 zeigt, wie in Abschnitt 5.5.2 bereits für Authentifizierungsmerkmale beschrieben, das qualitative Vereinheitlichungspotential bezogen auf die im vorherigen Abschnitt genannten Diversitätskriterien. Das quantitative Potential bestimmt sich durch die Anzahl der Authentifizierungssysteme in der jeweiligen betrachteten heterogenen IT-Struktur.

---

[625] Vgl. die Verwendung von Authentifizierungskonten in Abschnitt 2.1.7.

[626] Vgl. die Verwendung unterschiedlicher Plattformen (z.B. Unix und Windows) in heterogenen IT-Strukturen in Abschnitt 2.1.10.

[627] Vgl. die Verwendung von Kerberos in Abschnitt 3.2.3.

[628] Vgl. passive Tokens in Abschnitt 2.5.2.

Einfluss auf:	**Aufwand**				**Nutzen**
Diversität der Authentifizierungssysteme durch:	**Verwendung Benutzer** (Spezielle Anforderungen, Bequemlichkeit, Barrierefreiheit)	**Verwendung Org.** (Spezielle Anforderungen, Portabilität, Mobilität)	**Verwaltung Benutzer** (Wartbarkeit, Verarbeitungstiefe, Abrufbarkeit, Aussagekräftigkeit)	**Verwaltung Org.** (Benutzerverwaltung, Software, Hardware, Wartbarkeit)	**Sicherheit** (Vorhersagbarkeit, Fülle, Offenlegung, Angreifbarkeit, Datenschutz, Schutzziele, tech. Absicherung)
a) Unterschiedliche Ressourcen	- (wird nicht durch Benutzer beeinflusst)	■ Spezielle Anforderungen ■ Portabilität ■ Mobilität	- (wird nicht durch Benutzer beeinflusst)	■ Benutzerverwaltung ■ Software ■ Hardware ■ Wartbarkeit	■ Angreifbarkeit ■ Tech. Absicherung
Qual. Relevanz: $(A_a+N_a)/2=64{,}3\%$		$A_a=(100\%+100\%)/2=100\%$			$N_a=28{,}6\%$
b) Verschiedene Organisationen	- (wird nicht durch Benutzer beeinflusst)	■ Spezielle Anforderungen ■ Portabilität ■ Mobilität	- (wird nicht durch Benutzer beeinflusst)	■ Benutzerverwaltung ■ Software ■ Hardware ■ Wartbarkeit	■ Angreifbarkeit ■ Datenschutz ■ Tech. Absicherung
Qual. Relevanz: $(A_b+N_b)/2=71{,}4\%$		$A_b=(100\%+100\%)/2=100\%$			$N_b=42{,}9\%$
c) Unterschiedliche Sicherheitsanforderungen	- (wird nicht durch Benutzer beeinflusst)	■ Spezielle Anforderungen ■ Portabilität ■ Mobilität	- (wird nicht durch Benutzer beeinflusst)	■ Benutzerverwaltung ■ Hardware ■ Software ■ Wartbarkeit	■ Angreifbarkeit ■ Datenschutz ■ Schutzziele ■ Tech. Absicherung
Qual. Relevanz: $(A_c+N_c)/2=78{,}6\%$		$A_c=(100\%+100\%)/2=100\%$			$N_c=57{,}1\%$

Tabelle 5-24: Vereinheitlichungspotential bei Authentifizierungssystemen

Höchstes qualitatives Vereinheitlichungspotential bildet die Diversität durch unterschiedliche Sicherheitsanforderungen ($Div_{Systeme.c}$) mit 78,6%. Dies resultiert in erster Linie aus der höheren Komplexität durch die speziellen Sicherheitsvorgaben. Authentifizierungssysteme werden von den Benutzern nur indirekt über Authentifizierungsverfahren verwendet, somit wird der Aufwand von Verwendung und Verwaltung auf dieser Seite nicht berücksichtigt. Die Relevanz von $Div_{Systeme.c}$ setzt sich wie folgt zusammen. Für die Organisationen setzen Sicherheitsanforderungen bei ihrer Verwendung spezielle Anforderungen wie z.B. Fähigkeiten oder Qualifikation der Administratoren voraus. Einschränkungen, bedingt durch hohe Sicherheitsanforderungen, wirken sich zudem begrenzend auf Mobilität und Portabilität der Systeme aus.

Separate Systeme mit hohen Sicherheitsanforderungen erfordern unterschiedliche Benutzerverwaltungen, in denen berechtigte Benutzer explizit getrennt verwaltet werden sollen. Diese benötigen unter Umständen separate Software und damit verbundene Lizenzen. Werden die Systeme technisch zusätzlich, z.B. durch die Verwendung von Tokens oder Crypto-Modulen[629] abgesichert, ist für die Verwaltung auch zusätzliche Hardware erforderlich, die ebenfalls gewartet werden muss.

Physikalisch bietet beispielsweise gesonderte Hardware auch eine höhere technische Absicherung, die sich auf die Sicherheit auswirkt, die Angreifbarkeit mindert und Schutzziele wie Vertraulichkeit, Integrität, Verbindlichkeit und Verfügbarkeit realisiert. Aufgrund der Verwaltung der Konten in Authentifizierungssystemen ist insbesondere bei unterschiedlichen Organisationen oder Sicherheitsanforderungen der Datenschutz zu beachten, da es sich bei Identitäten und Kennwörtern um persönliche Daten handelt.

Die Relevanz weiterer Diversitätskriterien nimmt wie folgt ab:

- **DivSysteme.c** = 78,6% (Verschiedene Authentifizierungssysteme)
- **DivSysteme.b** = 71,4% (Verschiedene Organisationen)
- **DivSysteme.a** = 64,3% (Verschiedene Ressourcen)

5.7.3 Ermittlung geeigneter Integrationsformen

Für die in dieser Arbeit betrachtete Optimierung von heterogenen IT-Strukturen in Bezug auf eine vereinheitlichte Authentifizierung ist es erforderlich, die Authentifizierungssysteme zu integrieren, damit den in Abschnitt 5.7.1 genannten Kriterien zu begegnen und die Diversität zu reduzieren. Abbildung 5-17 zeigt analog zur Betrachtung der Integration von Authentifizierungsmerkmalen in Abschnitt 5.5.3 ein Beispiel für die Integration von Authentifizierungssystemen.

[629] Vgl. Abschnitt 2.5.2.

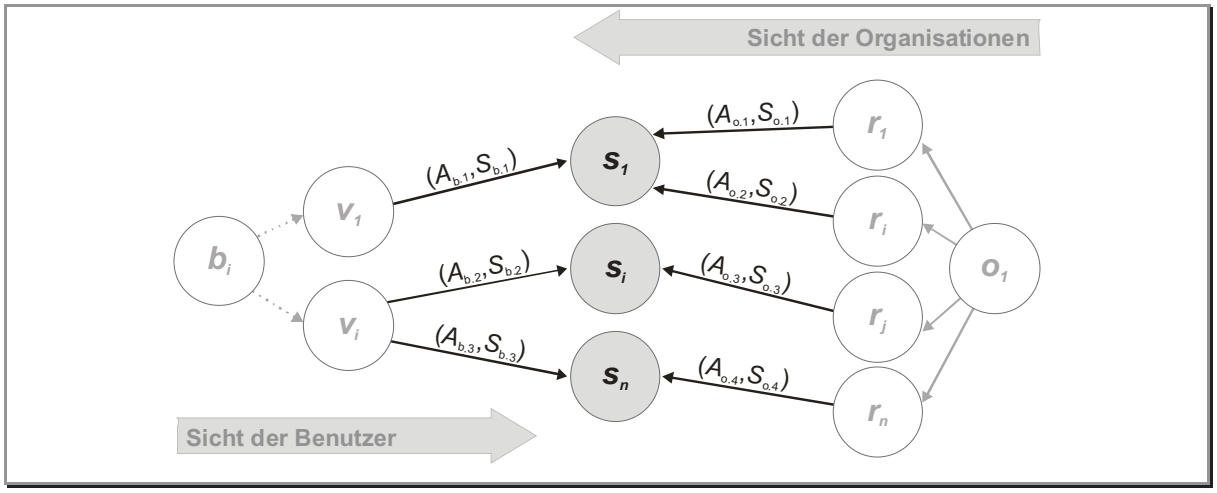

Abbildung 5-17: Sicht der Benutzer und Organisationen auf die Integration von Authentifizierungssystemen

Authentifizierungssysteme besitzen, wie in Abschnitt 5.1 eingeführt, Relationen bzw. Kanten zu Ressourcen, die diese verwenden, sowie Authentifizierungsverfahren, die ihrerseits von den Authentifizierungssystemen angewendet werden. Eine Ressource sowie ein Verfahren kann dabei mehreren Authentifizierungssystemen zu gewiesen sein und umgekehrt. Beispielsweise kann ein Authentifizierungssystem verschiedene Verfahren anbieten oder ein Verfahren bei der Authentifizierung unterschiedliche Authentifizierungssysteme bzw. auf ihm gespeicherte Konten[630] verwenden. Sowohl aus Sicht der Benutzer als auch der Organisationen sind daher die Integrationsformen Int_a, Int_b, Int_c und Int_d möglich.

Häufig besitzen Ressourcen in heterogenen IT-Strukturen eigene separate Authentifizierungssysteme.[631] Allgemeines Ziel der Integration ist es daher, unterschiedliche Ressourcen auf ein gemeinsames Authentifizierungssystem zugreifen zu lassen. Dadurch reduziert sich die Anzahl der Authentifizierungssysteme innerhalb der Organisationen. Eingeschränkt wird die Integration dabei durch die im nachfolgenden Abschnitt 5.7.4 genannten Grenzen.

Die Berechnung des Aufwands erfolgt analog zu den Authentifizierungsmerkmalen in Abschnitt 5.5.3. Für den Gesamtaufwand aus Sicht der Benutzer und Organisationen ergibt sich in Bezug auf Authentifizierungssysteme ($A_{systeme}$):

$$A_{systeme} = \sum_{k=1}^{n} A_k \ , \qquad \text{wobei gilt: } 0 \le A_k \le 14{,}2$$

630 Vgl. Speicherung von Benutzernamen und Authentifizierungsmerkmal in Authentifizierungskonten in Abschnitt 2.1.7.

631 Vgl. die Verwendung unterschiedlicher Plattformen (z.B. Unix und Windows) in heterogenen IT-Strukturen in Abschnitt 2.1.10 sowie das zugehörige Authentifizierungsmodell in Abschnitt 2.4.2.

Als erzielte Sicherheit ergibt sich daher analog zu Abschnitt 5.5.3:

$$S_{systeme} = \sqrt{\frac{S\min}{4{,}6} * \sum_{k=1}^{n} S_k} \quad , \qquad \text{wobei gilt: } 0 \le S_k \le 4{,}6$$

5.7.3.1 Reduktion von Authentifizierungssystemen (Int_a)

Existieren in einer heterogenen IT-Struktur Authentifizierungssysteme, die nicht explizit von einer Ressource oder einem Verfahren vorausgesetzt werden, bzw. werden diese Verfahren oder Ressourcen auf alternative Authentifizierungssysteme umgestellt, so lässt sich das System gemäß Int_a aus der Struktur reduzieren.

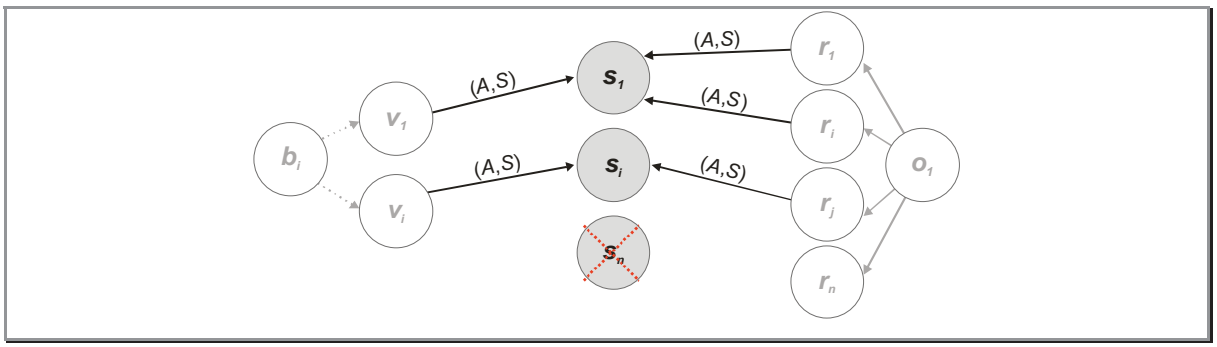

Abbildung 5-18: Reduktion der Authentifizierungssysteme

In dem in Abbildung 5-18 gezeigten Beispiel hätte dies zur Folge, dass die Ressource r_n zukünftig das System s_1 oder s_i für die Authentifizierung verwenden müsste. Ein Beispiel hierfür kann die Anbindung einer Ressource von einem lokalen Authentifizierungssystem[632] mit einer eigenen lokalen Benutzerverwaltung an ein Verzeichnisdienst[633] oder ein Kerberos-System sein. In diesem Fall würde auch das Authentifizierungsverfahren, das zuvor lokal verwendet wurde, reduziert bzw. zukünftig für dieses Authentifizierungssystem nicht länger erforderlich sein.

5.7.3.2 Integration von Authentifizierungssystemen (Int_b)

Int_b beschreibt die Möglichkeit mehrere Authentifizierungssysteme in einem neuen separaten System zu integrieren, ohne die ursprünglichen Systeme und ihre Eigenschaften zu reduzieren. Abbildung 5-19 zeigt drei Ausprägungen dieser Integration, in denen jeweils die Kanten bzw. Relationen der Systeme aus Sicht der Organisationen und/oder Benutzer gebündelt werden.

---

[632] Vgl. lokale Authentifizierungssysteme und -verfahren in Abschnitt 2.7.1.

[633] Vgl. die Verwendung eines zentralen Verzeichnisdienstes für unterschiedliche Ressourcen und Anwendungen in Abschnitt 3.2.2.

- in Abbildung 5-19 erfolgt die Integration in **a)** ausschließlich für die Benutzer. Bestehende Lösungsansätze für einheitliche Authentifizierung decken diese Integrationsform nicht ab. Ausnahme bilden teilweise Federations, bei denen die Benutzer sich an unterschiedlichen Service Providern anmelden, dafür jedoch das Token ihrer virtuellen Organisation verwenden.[634] Allerdings führen Service Provider keine eigenständige Authentifizierung durch, sondern verwenden das vom Identity Provider erstellte Token. Sie bilden somit keine Authentifizierungssysteme.

- **b)** zeigt die Integration für die Organisationen. Beispiele für eine derartige Integration bilden Meta-Directories, sofern diese Authentifizierungsinformationen unterschiedlicher Systeme bzw. Plattformen verwalten.[635] Ein weiteres Beispiel ist die Verwendung von Kerberos mit Zertifikaten.[636] Dabei erfolgt die Authentifizierung am Kerberos-System., die Authentifizierungsinformation wird jedoch integriert in einer Public-Key-Infrastruktur bereitgestellt.[637]

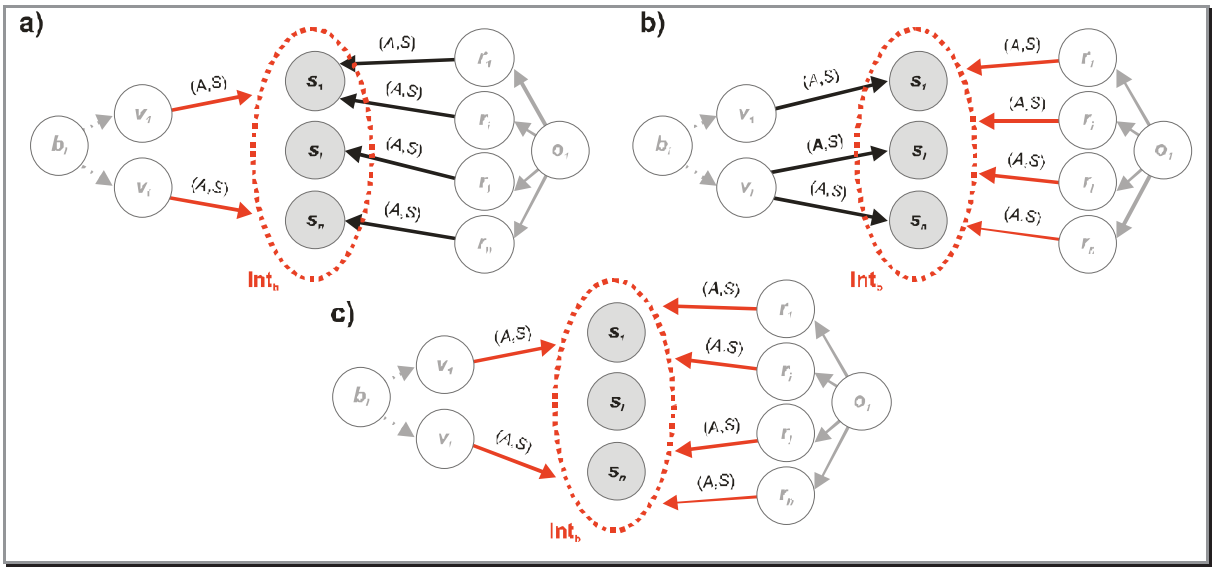

Abbildung 5-19: Integration von Authentifizierungssystemen

- bei **c)** erfolgt die Integration sowohl aufseiten der Benutzer als auch der Organisationen. Dieser Ansatz ist in bestehenden Lösungen nicht umgesetzt. Er lässt sich bedingt durch eine Kombina-

634 Vgl. Federation-basierte Authentifizierung in Abschnitt 3.2.7.

635 Vgl. die Synchronisation von Informationen unterschiedlicher Anwendungen und Plattformen über Meta-Directories in Abschnitt 3.2.2.

636 Vgl. PKINIT, wie in Abschnitt 3.2.4 erläutert.

637 Vgl. die Verwendung von Zertifikaten innerhalb von Public-Key-Infrastrukturen in Abschnitt 3.2.4.

tion der in **a)** genannten Federations sowie der in **b)** genannten Lösungen Meta-Directory, insb. Virtual Directory und Public-Key-Infrastrukturen beschreiben.[638]

5.7.3.3 Integration und Reduktion der Relationen (Int_c, Int_d)

Abbildung 5-20 zeigt die Integration einzelner Kanten eines Authentifizierungssystems. Im illustrierten Beispiel wird z.B. die Ressource r_j vom System s_i entfernt, welches dadurch keine weiteren Relationen zu Ressourcen besitzt und nach Int_a reduziert werden kann. Ermöglicht wird eine solche Integration beispielsweise durch die Unterstützung verschiedener Plattformen eines Authentifizierungssystems. Unterstützt ein Authentifizierungssystem zusätzliche Authentifizierungsverfahren, so kann auch hier eine Integration nach Int_d erfolgen. Beispiel hierfür kann die Unterstützung von Kerberos als gemeinsames Verfahren (hier z.B. v_i) sein.[639]

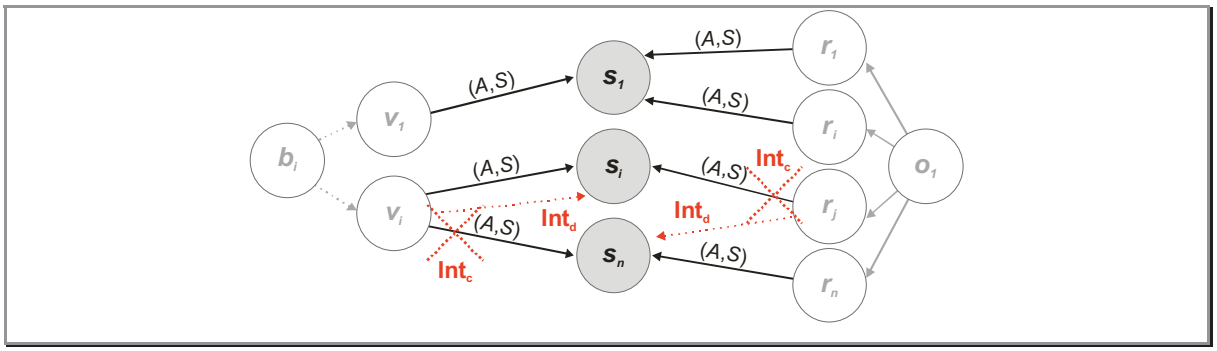

Abbildung 5-20: Integration und Reduktion der Relationen von Authentifizierungssystemen

5.7.4 Grenzen der Vereinheitlichung

In Abschnitt 4.4.2 wurde bereits die Kompatibilität der Systeme mit unterschiedlichen Plattformen, Ressourcen und Authentifizierungsverfahren als Grenze für die Integration genannt. Neben dieser Begrenzung besteht bei einer Reduktion der Systeme, im Extremfall auf ein einziges System, die Gefahr, eine zentrale Fehlerquelle (als „single point of failure“) zu schaffen. Mit zunehmender Reduktion der Systeme müssen somit Redundanzszenarien eingeplant und realisiert werden, um bei einem Ausfall der integrierten Systeme nicht die gesamte Authentifizierung innerhalb der IT-Struktur zu verhindern.

---

638 Vgl. die Verwendung des Identity Providers der Heimatorganisation durch die Benutzer in Abschnitt 3.2.7 sowie die Synchronisation der Informationen innerhalb der Heimatorganisation mittels Meta- oder Virtual Directories, wie in Abschnitt 3.2.2 beschrieben.

639 Vgl. Abschnitt 3.2.3.

5.7.5 Resultierende Hypothesen

Aus den vorherigen Abschnitten ergeben sich folgende Ergänzungen für die in Abschnitt 5.5.5 und 5.6.5 aufgestellten Hypothesen:

H 8: Authentifizierungssysteme stellen in der Regel das kleinste quantitative Vereinheitlichungspotential dar. Ihre Anzahl ist kleiner als die der Authentifizierungsverfahren, da ein System unterschiedliche Verfahren unterstützen kann.

H 9: Die Reduktion auf ein einziges System ist nicht sinnvoll, sofern nicht für entsprechende Redundanz im Falle eines Fehlers gesorgt wurde. Daraus resultiert auch eine geringere Relevanz der vollständigen Integration[640] im Vergleich zur Fokussierung auf die Integration und Reduktion von Authentifizierungsmerkmalen und -verfahren.

H 10: Für die Vereinheitlichung von Authentifizierungssystemen bietet sich die Reduktion der Relationen (Int_c) und Elementen (Int_a) an. Insbesondere Ressourcen, die eigenständige Authentifizierungssysteme erfordern, sollten reduziert werden.

[640] Vgl. die einfachste Form der einheitlichen Authentifizierung in Abschnitt 3.2.1.

6 Realisierung einer einheitlichen Authentifizierung für sichere e-Science-Umgebungen

Kapitel 5 beschreibt ein formales Modell für die Authentifizierung in heterogenen IT-Strukturen anhand der Faktoren Authentifizierungsmerkmale, -verfahren und -systeme. Hierbei werden die Sicht der Benutzer, die authentifiziert werden, und die Sicht der Organisationen, die die Authentifizierung betreiben und gewährleisten wollen, unterschieden. Beide Sichten bilden jeweils formal einen Graphen, dessen Knoten die genannten Faktoren darstellen. Kanten zwischen den Faktoren kennzeichnen deren Verwendung sowie den damit verbundenen Aufwand und die erzielte Sicherheit als Kantengewichte. Die Abschnitte 5.5.3, 5.6.3 und 5.7.3 nennen bereits Möglichkeiten für die Vereinheitlichung der Faktoren, indem einzelne Elemente reduziert oder integriert werden. Einheitliche Authentifizierung wird darauf basierend im Folgenden formal als Folge der Reduktion und Integration von Knoten und Kanten der beschriebenen Graphen definiert. Je mehr Kanten und Knoten reduziert werden, desto höher ist der Grad der Vereinheitlichung. Als Optimalitätskriterium für die Vereinheitlichung gilt zudem die Minimierung der Kantengewichte, die den Aufwand beschreiben, bei gleichzeitiger Wahrung bzw. Gewährleistung der erforderlichen Sicherheit. Sowohl Aufwand als auch Sicherheit wurden in den Abschnitten 5.4.2 und 5.4.3 als scharfe Werte quantifiziert. In diesem Abschnitt gehen sie jedoch als unscharfe Menge in die Bewertung ein, da Aufwand und insbesondere Sicherheit subjektiv bzw. durch von verschiedenen Organisationen individuell bewertet werden.

Betrachtet werden im Folgenden wissenschaftliche IT-Strukturen, wie sie in Abschnitt 4.2.1 genannt wurden. Die zunehmende IT-basierte Vernetzung wissenschaftlicher Strukturen, z.B. für international verteilte e-Science-Anwendungen, stellt hohe Anforderungen an die Authentifizierung und deren Vereinheitlichung.[641]

Durch die im Rahmen der vorliegenden Arbeit durchgeführten Fallstudien wird die Isomorphie des in Kapitel 5 eingeführten formalen Modells insbesondere für die einheitliche Authentifizierung in heterogenen wissenschaftlichen und betrieblichen IT-Strukturen bestätigt.[642] Die Isomorphie des Modells wird daher auch bei der Überprüfung der Hypothesen aus Kapitel 5 am Ende dieses Kapitels berücksichtigt.

---

[641] Vgl. Definition von e-Science und in diesem Rahmen verwendete Anwendungen im Abschnitt 2.1.13.

[642] Vgl. die Abschnitte 4.2.1 und 4.2.2.

6.1 Kriterien für die Optimierung einheitlicher Authentifizierung

Die folgenden Abschnitte fassen die in Kapitel 4 genannten Anforderungen und Ziele zusammen und definieren den Rahmen für die anschließende Optimierung der in Kapitel 5 genannten Faktoren. Sie beschreiben somit die Kriterien für die Optimierung von heterogenen IT-Strukturen durch die Umsetzung einer einheitlichen Authentifizierung. Während in Abschnitt 3.1 bereits der Ist-Zustand der Authentifizierung in heterogenen IT-Strukturen erläutert wurde, beschreiben die nachfolgenden Abschnitte ein geeignetes Konzept für die Optimierung der IT-Strukturen im Hinblick auf den Soll-Zustand, den die Anforderungen des Kapitels 4 beschreiben.

6.1.1 Minimierung des Aufwands für die Betreiber

Wie in Abschnitt 5.4 beschrieben, entsteht für Organisationen als Betreiber ein Aufwand in Bezug auf die Verwaltung und Verwendung der Authentifizierung. Dieser Aufwand äußert sich aus wirtschaftlicher Hinsicht durch Sachkosten für erforderliche Betriebsmittel der Authentifizierung sowie Personalkosten, z.B. bezogen auf die Verwaltung. Kosten werden hierbei nur aus Sicht der Organisationen betrachtet, da vorausgesetzt wird, dass diese eventuelle Sachkosten für die Benutzer (z.B. Mitarbeiter) übernehmen. Personalkosten in Bezug auf die Authentifizierung werden im folgenden Abschnitt durch die Benutzbarkeit bestimmt, die somit ebenfalls Einfluss auf die wirtschaftliche Betrachtung ausübt.

Einen Bestandteil des Soll-Konzepts für einheitliche Authentifizierung in heterogenen IT-Strukturen bildet daher die Minimierung des Aufwands sowie resultierende Personal- und Sachkosten durch die erzielte Vereinheitlichung. Diese bezieht sich auf den Aufwand A in Bezug auf Verwaltung und Verwendung für die Organisationen.[643]

Als Beispiel für den Aufwand bezogen auf die Verwaltung von Authentifizierungsmerkmalen seitens der Organisationen kann das Rücksetzen von Passwörtern im Rahmen der Benutzerverwaltung angesehen werden, das laut einer Studie von Gartner 10 - 30% der Help-Desk-Anfragen darstellt.[644] Gartner ermittelt in der Studie Kosten zwischen $51 und $147, die pro Benutzer und Vorgang des Rücksetzens von Passwörtern in Form von Personalkosten aufgewendet werden müssen. Ein weiteres Beispiel beschreibt die Kostensenkung innerhalb einer Schweizer Bank, die vor der Einführung eines „Single Sign-On“-Systems 30.000 passwortbezogene Anfragen pro Monat bei ihrem Help-Desk verzeichnete, wobei eine durchschnittliche Dauer von 20 Minuten und ein inter-

[643] Gemäß Definition und Quantifizierung des Aufwands als Kantengewicht in Abschnitt 5.4.2.

[644] Vgl. GARTNER: Password Reset: Self-Service That You Will Love, 2002.

ner Stundensatz von 60 Euro angegeben wurde.[645] Dies entspricht den in der Gartner Studie ermittelten Zahlen. Durch die Passwortrücksetzung und integrierte „Single Sign-On"-Lösung konnte die Zahl der passwortbezogenen Anrufe um mehr als ein Drittel gesenkt werden. Das resultierende Einsparungspotential bildet einen hohen Return on Investment (ROI) für die erforderlichen IT-Sicherheitsinvestitionen im Rahmen der einheitlichen Authentifizierung. Innerhalb der Wirtschaftlichkeitsbetrachtungen von IT-Sicherheit, die Gegenstand aktiver Forschung sind[646], wurde hierfür zusätzlich der Begriff Return on Security Investment (ROSI)[647] vorgeschlagen, um z.B. nicht monetäre Vorteile der Erhöhung der IT-Sicherheit (beispielsweise in Bezug auf die erzielte Risikominimierung) zu erfassen. Zusätzlich existiert ein umfassendes Kosten- / Nutzen-Modell von GORDON UND LOEB[648], das jedoch umstritten ist.[649] Die genannten Modelle und Verfahren beinhalten jedoch keine Ansätze für die Abschätzung des effektiven Aufwands, z.B. für die Wartbarkeit und resultierende Personalkosten.

In dieser Arbeit wird für die Quantifizierung der Kosten der Authentifizierung und deren Minimierung im Hinblick auf die wirtschaftliche Optimierung daher der in Abschnitt 5.4.2.5 genannte Aufwand A_o aus Sicht der Organisationen verwendet.

6.1.2 Minimierung des Aufwands für die Benutzer

Während im vorherigen Abschnitt die Minimierung des Aufwands aus Sicht der Organisationen als wirtschaftliche Optimierung genannt wurde, steigert die Reduzierung des Aufwands für die Benutzer die Usability bzw. Benutzbarkeit. Anwender können schneller und unkomplizierter Zugriff auf die eigentliche Applikation oder Ressource nehmen, die durch die Authentifizierung geschützt wird. Die Verwaltung ihrer Authentifizierungsmerkmale wird beispielsweise durch deren Synchro-

---

645 Vgl. GADATSCH, A.; UEBELACKER, H.: Wirtschaftlichkeitsbetrachtungen für IT-Security-Projekte, in MÖRIKE, M.; TEUFEL S.: Kosten & Nutzen von IT-Sicherheit in: HEILMANN, H. ET AL. (Hrsg.): HMD - Praxis der Wirtschaftsinformatik, Heft 248, 2006, S. 46.

646 Diese stehen nach FEDERRATH, H.: Kosten und Nutzen der IT-Sicherheit, in MÖRIKE, M.; TEUFEL S.: Kosten & Nutzen von IT-Sicherheit in: HEILMANN, H. ET AL. (Hrsg.): HMD - Praxis der Wirtschaftsinformatik, Heft 248, 2006, S. 4; LUBICH, H. P.: IT-Sicherheit: Systematik, aktuelle Probleme und Kosten-Nutzen-Betrachtungen, in MÖRIKE, M.; TEUFEL S.: Kosten & Nutzen von IT-Sicherheit in: HEILMANN, H. ET AL. (Hrsg.): HMD - Praxis der Wirtschaftsinformatik, Heft 248, 2006, S. 6 noch an Ihrem Anfang.

647 Vgl. POHLMANN, N.: Wie wirtschaftlich sind IT-Sicherheitsmaßnahmen?, in MÖRIKE, M.; TEUFEL S.: Kosten & Nutzen von IT-Sicherheit in: HEILMANN, H. ET AL. (Hrsg.): HMD - Praxis der Wirtschaftsinformatik, Heft 248, 2006, S. 29 ff.

648 Vgl. GORDON, L. A.; LOEB, M. P.: Managing Cyber-Security Resources - A cost-benefit analysis, 2005, S. 27 ff.

649 Vgl. WILLEMSON, J.: On the Gordon & Loeb Model for Information Security, 2006.

nisation erleichtert (Single Password, Einsatz von Tokens).[650] Lösungen für ein Reduced- bzw. Single Sign-On vermindern zusätzlich die Anzahl der erforderlichen Authentifizierungsvorgänge, wie in Abschnitt 4.1.1 beschrieben.[651]

Sofern die Benutzer Mitarbeiter einer Organisation sind, die die Authentifizierung betreibt, ergibt sich aus der Steigerung der Benutzbarkeit auch eine wirtschaftliche Optimierung. Der Anteil der Arbeitszeit bzw. implizit der Personalkosten, die für Verwendung und Verwaltung der Authentifizierung seitens der Mitarbeiter erforderlich ist, sinkt. Allgemein erhöht sich jedoch insbesondere, auch für Personen, die keine Mitarbeiter des Betreibers der Authentifizierung sind, die Akzeptanz der Authentifizierung, bedingt durch den geringeren Aufwand. Beispielsweise sind Benutzer bereit, ein komplexeres Authentifizierungsmerkmal (z.B. komplexeres Passwort) zu akzeptieren, wenn sie damit verschiedene Dienste verwenden können.[652] Sofern verschiedene komplexe Passwörter erforderlich sind, beginnen die Anwender die Komplexitätskriterien zu umgehen. Beispielsweise werden erzwungene maximale Passworthistorien umgangen, indem die Benutzer zunächst mehrere zufällige Passwörter definieren und anschließend wieder das alte Passwort vergeben.[653] Passwortlänge oder vorgegebene kurze Frequenz der Passwort-Änderung führt des Weiteren dazu, dass Benutzer das Kennwort schlimmstenfalls leicht zugänglich am Arbeitsplatz aufschreiben oder in den Applikationen selbst abspeichern.[654] Als Resultat führen diese oder ähnliche Passwortvorgaben nicht zu einer Steigerung, sondern Minderung der IT-Sicherheit, die im nächsten Abschnitt beschrieben wird.

Die Benutzbarkeit der Authentifizierung und deren Optimierung wird in dieser Arbeit auf die Minimierung des in Abschnitt 5.4.2.5 genannten Aufwands A_b aus Sicht der Benutzer zurückgeführt.

---

650 Vgl. Synchronisation von Informationen und Authentifizierungsmerkmalen anhand eines Meta-Directories in Abschnitt 3.2.2.

651 Weitere Beispiele für Auswirkung der Authentifizierung bzw. IT-Sicherheit auf die Benutzbarkeit finden sich in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005 und GERD TOM MARKOTTEN, D.: Benutzbare Sicherheit in informationstechnischen Systemen, 2003.

652 Vgl. ADAMS, A.; SASSE, A.: Users Are Not the Enemy. Why Users Compromise Security Mechanisms and How to Take Remedial Measures, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 647 f.

653 Vgl. YAN, J ET AL.: The Memorability and Security of Passwords, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 132.

654 Vgl. Speicherung von Passwörtern in Abschnitt 3.2.9.

6.1.3 Gewährleistung der IT-Sicherheit

Über die in den vorherigen beiden Abschnitten genannte Reduzierung des Aufwands hinaus stellt ein zusätzliches Ziel der einheitlichen Authentifizierung die Steigerung der erzielten IT-Sicherheit dar. Mögliche Risiken, die durch den unberechtigten Zugriff auf Informationen entstehen können[655], sollen verhindert bzw. gemindert werden. Risiken z.B. durch die Einschränkung der Vertraulichkeit, Integrität, Verbindlichkeit oder Verfügbarkeit[656] lassen sich durch geeignetes Risiko-Management in Form von Wagniskosten bewerten. Lösungen für eine einheitliche Authentifizierung können erhöhte Sicherheitsmaßnahmen bei gleichzeitiger Reduzierung der Kosten bzw. des Aufwands ermöglichen. Ein Beispiel hierfür bietet die Ablösung unterschiedlicher Passwörter durch Smart Cards bzw. Tokens.[657] Durch die Authentifizierung anhand von zwei Faktoren steigt die Sicherheit, wobei die Integration unterschiedlicher Dienste und Authentifizierungsmerkmale auf dem Token den Aufwand bezogen auf die Verwaltung der Merkmale für die Benutzer senkt. IT-Sicherheit kann auch eine Anforderung sein, die durch Dritte an die Organisationen gestellt wird und im Rahmen einer einheitlichen Authentifizierung berücksichtigt werden muss. Als Beispiel können hier Datenschutzbestimmungen gemäß BDSG oder wirtschaftliche Vorgaben, z.B. in den USA durch den Sarbanes-Oxley Act (kurz: SOX) oder in Europa durch Basel II sein.[658] Beide Regularien beziehen sich auf die Richtigkeit der Finanzdaten von Unternehmen. Die Banken- und Kapitaladäquanzrichtlinie Basel II, die seit 1.1.2007 auch in Deutschland rechtliche Wirkung bei der Kreditvergabe besitzt, bezieht im Rahmen des geforderten Risiko-Managements auch ein aktives IT-Risiko-Management resp. Gewährleistung der IT-Sicherheit ein.[659]

Allgemein bezieht sich die Anforderung, die durch die geschilderte Steigerung der IT-Sicherheit gestellt wird, auf die Gewährleistung der durch die Authentifizierung innerhalb der heterogenen IT-Struktur erzielten Sicherheit *S*.[660]

---

[655] Risiken, die in Zusammenhang mit der Authentifizierung entstehen, wurden in Abschnitt 2.8 genannt.

[656] Vgl. Grundwerte für IT-Sicherheit in Abschnitt 2.2.

[657] Vgl. Authentifizierungsmerkmale basierend auf dem Besitz von Tokens in Abschnitt 2.5.2.

[658] Vgl. BUNDESMINISTERIUM DER JUSTIZ: Bundesdatenschutzgesetz (BDSG), 1990; HURLEY, E.: Security and Sarbannes-Oxley, 2003; BUNDESBANK: Basel II - Die neue Baseler Eigenkapitalvereinbarung, 2007 sowie Abschnitt 2.3.2.

[659] Siehe CORPORATE-CONSULTING.NETWORK: IT-Sicherheit als Rating-Faktor, 2006.

[660] Vgl. Abschnitt 5.4.3.

6.2 Gestaltung des Authentifizierungsmodells für heterogene IT-Strukturen

Anhand der im vorherigen Abschnitt genannten Anforderungen an die Gestaltung einer optimalen Authentifizierung in heterogenen IT-Strukturen werden in den folgenden beiden Abschnitten die in dieser Arbeit verwendete Optimierungsmethodik sowie zu erzielende Optimalitätskriterien definiert. Die Optimierung bezieht sich hierbei auf die geeignete Veränderung des in Kapitel 5 eingeführten formalen Modells zur Minimierung des Aufwands bei gleichzeitiger Gewährleistung der erzielten IT-Sicherheit als Nutzen.

6.2.1 Gestaltung des Verhältnisses zwischen Aufwand und Sicherheit

In Abschnitt 5.2 wurden die in dieser Arbeit betrachteten Möglichkeiten für eine Vereinheitlichung der Authentifizierung in heterogenen IT-Strukturen erläutert. Gemäß der Abschnitte 5.5.3, 5.6.3 und 5.7.3 wurde der Aufwand jeweils für Authentifizierungsmerkmale, -verfahren und -systeme als Summe der jeweils verbundenen Relationen in $A_{merkmal}$, $A_{verfahren}$ und A_{system} definiert und durch die Vereinheitlichung reduziert. Als Maß für die Sicherheit nach Vereinheitlichung wurden $S_{merkmal}$, $S_{verfahren}$ und S_{system} eingeführt, wobei die insgesamt erzielte Sicherheit von dem Element mit der geringsten erzielten Sicherheit abhängt.[661] Zusätzlich steigt die Sicherheit mit zunehmender Komplexität weniger stark an.[662] Für die Vereinheitlichung der Authentifizierung in heterogenen IT-Strukturen ist daher die optimale Gestaltung des Verhältnisses zwischen Aufwand und erzielter Sicherheit erforderlich. Für Aufwand und Sicherheit über k betrachtete Elemente, die vereinheitlicht werden sollen, wurden daher in Abschnitt 5.4 folgende Formeln aufgestellt:

$$A = \sum_{k=1}^{n} A_k \text{ , wobei: } 0 \le A_k \le 14{,}2 \qquad S = \sqrt{\frac{S\min}{4{,}6} * \sum_{k=1}^{n} S_k} \text{ , wobei: } 0 \le S_k \le 4{,}6$$

Aus den genannten Annahmen für die Minderung der Steigung der erzielten Sicherheit bei höherem Aufwand kann umgekehrt gefolgert werden, dass der Aufwand bzw. die Kosten mit zunehmend höherem angestrebtem Sicherheitsniveau kontinuierlich ansteigen. Die Abbildung 6-1 verdeutlicht diese Zusammenhänge.

---

[661] Vgl. den Einfluss des geringsten Kantengewichts S in Abschnitt 5.4.3.

[662] Vgl. Abbildung 6-3.

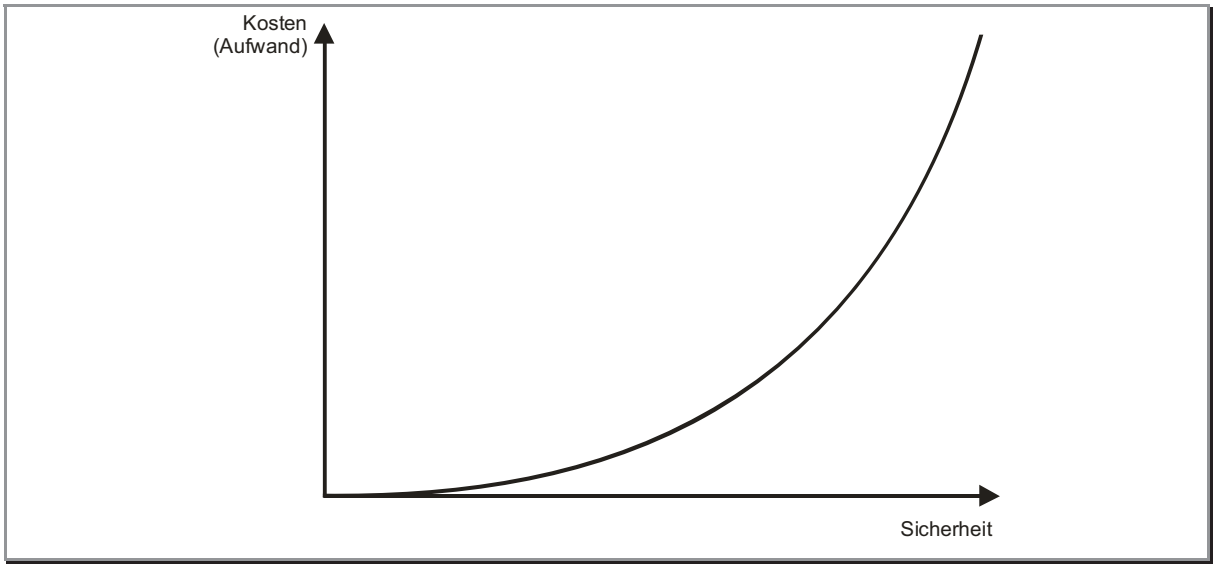

Abbildung 6-1: Abhängigkeit zwischen erzielter Sicherheit und damit verbundenem Aufwand

Auch in anderen Publikationen wird das Verhältnis zwischen Kosten und erzielter IT-Sicherheit analog dargestellt. Abbildung 6-2 zeigt dies als Budget für IT-Sicherheit nach TEUFEL ET AL.[663] TEUFEL ET AL. definiert zusätzlich ein Schadenspotenzial, das die Kosten durch fehlende oder gebrochene Sicherheitsmaßnahmen beschreibt. Das Schadenspotenzial sinkt im Gegensatz zum erforderlichen Budget für höhere Sicherheitsniveaus. Ein optimales Verhältnis zwischen vorgesehenem Budget und möglichem Schadenspotenzial stellt nach TEUFEL ET AL. der Schnittpunkt beider Kurven dar. Vom Ursprung bis zum Optimum ergibt sich in diesem Fall die erzielbare Sicherheit. Darüber hinaus wird das restliche Risiko abgetragen.

[663] Vgl. WINDEMANN, P.; SCHLIENGER, T.; TEUFEL, S.: Messung der Informationssicherheit auf der Ebene der Sicherheitspolitik in MÖRIKE, M.; TEUFEL S.: Kosten & Nutzen von IT-Sicherheit in: HEILMANN, H. ET AL. (Hrsg.): HMD - Praxis der Wirtschaftsinformatik, Heft 248, 2006, S. 53 ff.

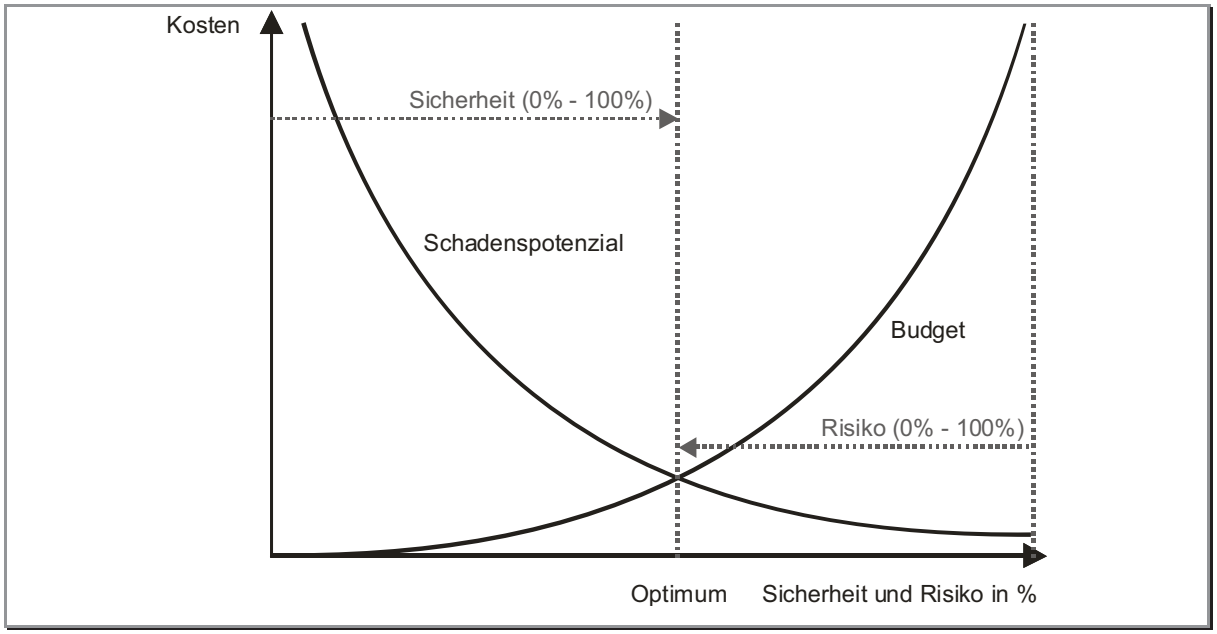

Abbildung 6-2: Erzielte IT-Sicherheit in Abhängigkeit der erforderlichen Kosten.[664]

Während der Gesamtaufwand linear mit der Anzahl der zu vereinheitlichenden Elemente anwächst, wurde für die Sicherheit in Abbildung 6-1 gezeigt, dass diese mit zunehmender Anzahl der Elemente resp. höherem Aufwand weniger stark ansteigt. Dieses Verhältnis bildet die Wurzel in der Formel für *S* ab.

Abschnitt 6.1.2 nennt jedoch weitere Einflussfaktoren auf die erzielte IT-Sicherheit, die durch die Minderung der Benutzbarkeit (bzw. Usability) bei höheren Sicherheitsniveaus begründet sind. Zusätzlich steigen mit zunehmender Komplexität und erzielter Sicherheit auch die möglichen Fehlerquellen der Authentifizierung. Fehler einer Authentifizierung beziehen sich dabei z.B. auf die fehlerhafte eindeutige Identifizierung einer Person. Wird ein unberechtigter Dritter durch einen Fehler als legitimer Benutzer authentifiziert, spricht man von „false acceptance“. Der prozentuale Anteil solcher fälschlicher Akzeptierungen unberechtigter Dritter an den insgesamt durchgeführten Authentifizierungen wird als „false acceptance rate“ (FAR) bezeichnet. Werden berechtigte Benutzer im Gegensatz dazu als vermeintlich unberechtigte Dritte durch die Authentifizierung ausgewiesen, so spricht man von „false rejection“ bzw. in Bezug auf deren Anteil von einer „false rejection rate“ (FRR).[665] Letztere wird insbesondere von den Benutzern als störend empfunden. Abgesehen von

---

[664] Eigene Darstellung nach WINDEMANN, P.; SCHLIENGER, T.; TEUFEL, S.: Messung der Informationssicherheit auf der Ebene der Sicherheitspolitik in MÖRIKE, M.; TEUFEL S.: Kosten & Nutzen von IT-Sicherheit in: HEILMANN, H. ET AL. (Hrsg.): HMD - Praxis der Wirtschaftsinformatik, Heft 248, 2006, S. 54.

[665] Siehe SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 213 ff., sowie FAR und FRR bei biometrischen Merkmalen in Abschnitt 2.5.3.

der biometrischen Authentifizierung ist sie z.B. durch Fehleingaben oder -anwendung seitens der Benutzer möglich.[666] Sie führt jedoch auch dazu, dass Betreiber bzw. Administratoren Fehler der Authentifizierung stillschweigend akzeptieren und so unter Umständen die FAR erhöhen, da sie Zugriffe unberechtigter Dritter für regulär auftretende Fehler halten.[667] Zusammen mit der Minderung der Benutzbarkeit bilden FAR und FRR somit eine Begrenzung der erzielten Sicherheit. In dieser Arbeit wird daher im Folgenden das in Abbildung 6-3 gezeigte Verhältnis zwischen Sicherheit und Aufwand angenommen. Die Sicherheit steigt dabei zunächst analog zur Abbildung 6-1 rapide an, sobald überhaupt Aufwand in ihre Gewährleistung investiert wird. Die Steigung nimmt jedoch bedingt durch die zunehmende Komplexität ab, wie ebenfalls in Abbildung 6-1 im Verhältnis zwischen Aufwand und Sicherheit dargestellt. Durch den genannten Einfluss der Benutzbarkeit, FAR und FRR nimmt sie schließlich ab einer Akzeptanzgrenze für die Benutzer und Administratoren ab, die Sicherheitsmechanismen mit zunehmender Höhe umgehen.[668]

Anders als in Abbildung 6-2, in der als Optimum exakt der Schnittpunkt zwischen Schadenspotenzial und Budget ermittelt werden kann, repräsentiert die Akzeptanzgrenze in Abbildung 6-3 einen Toleranzbereich für die optimal anzustrebende Sicherheit. Im Gegensatz zum Verhältnis zwischen Budget und erwartetem Schaden lässt sich die Grenze nicht scharf bestimmen, da unterschiedliche Benutzer, z.B. abhängig von deren technischem Kenntnisstand, eine individuelle Toleranzgrenze besitzen. Erzielte Sicherheit und erforderlicher Aufwand bilden in Bezug auf die Benutzer und Organisationen als Betreiber eine unscharfe Menge. Verfahren, die aus Sicht der einen Organisation noch ein mittleres Sicherheitsniveau erzielen, können von einem anderen Betreiber bereits mit einer niedrigen Sicherheitsstufe bewertet werden. Merkmale, deren geforderte Komplexität von dem einen Benutzer noch als akzeptabel hingenommen wird, können für andere Benutzer bereits einen inakzeptablen Aufwand darstellen. Dies könnte bedeuten, dass letztere beginnen, Passwörter leicht zugänglich (z.B. direkt am Arbeitsplatz) zu hinterlegen, während erstere aufgrund der höheren Akzeptanzgrenze für IT-Sicherheit bereit sind, auch komplexe Passwörter auswendig zu lernen. Beide Beispiele beschreiben die Unschärfe von Aufwand und Sicherheit.

Allgemein wird definiert, dass mit zunehmendem Aufwand für die Authentifizierung die Flexibilität bzw. Benutzbarkeit sinkt. Sobald die Einschränkung der Flexibilität bzw. Benutzbarkeit ein

---

666 Vgl. Abschnitt 2.5.1.

667 Dies wird auch in SCHNEIER, B.: Beyond Fear, 2003, S. 56, 189 f. und BURNETT, M.; KLEIMAN, D.: Perfect Passwords, 2006, S. 133 beschrieben.

668 Vgl. Abschnitt 6.1.2.

Niveau erreicht hat, das nicht mehr von den Anwendern akzeptiert wird, sinkt auch die durch die Authentifizierung erzielte Sicherheit.[669]

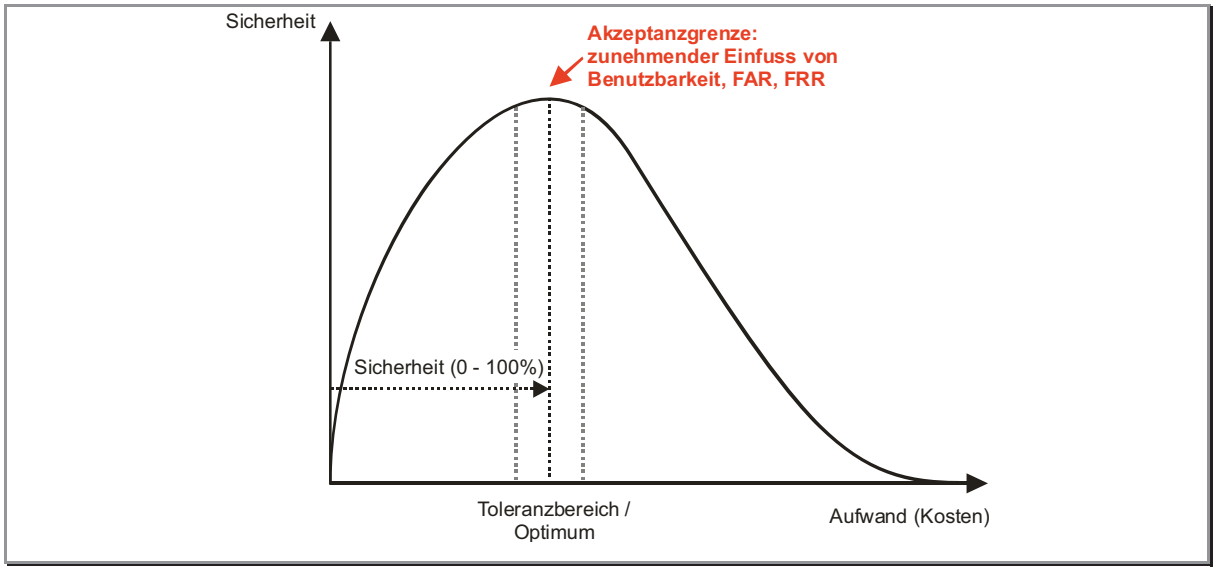

Abbildung 6-3: Erzielte Sicherheit unter Berücksichtigung der Benutzbarkeit

Aufgrund des in Kapitel 5 eingeführten Modells der Authentifizierung in heterogenen IT-Strukturen in Form eines Netzwerks bzw. Graphen aus Sicht der Benutzer und Organisationen bieten sich für die Vereinheitlichung resp. Optimierung der Authentifizierung Verfahren der Netzwerk- bzw. Graphenoptimierung an.[670] Grundsätzlich verfolgen die Netzwerkoptimierungsverfahren die bereits in Abschnitt 5.2 gezeigte Reduktion der Knoten und Kanten. Die in Abschnitt 5.2 beschriebene Vereinheitlichung nach Int_c lässt sich beispielsweise durch minimale Spannbäume[671] aus Sicht der Benutzer oder Organisationen erzielen. Ein Baum bezeichnet dabei einen schleifenfreien, zusammenhängenden Graph. Dieser ist dann ein minimaler Spannbaum, sofern kein weiterer spannender Untergraph existiert, dessen Summe der Kantengewichte kleiner ist.[672] Durch die Anwendung passender Algorithmen wie Prim oder Kruskal lässt sich so eine Minimierung des

---

669 Der geschilderte Zusammenhang zwischen Sicherheit und erforderlichem Aufwand wird auch in SASSE, M. A.; FLECHAIS, I.: Usable Security. Why Do We Need It? How Do We Get It?, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 13 ff und GERD TOM MARKOTTEN, D.: Benutzbare Sicherheit in informationstechnischen Systemen, 2003, S. 143 ff. bestätigt.

670 Entsprechende Verfahren werden beispielsweise in SUHL, L.; MELLOULI, T.: Optimierungssysteme, 2006, S. 163 ff. und HAMACHER, H. W.; KLAMROTH, K.: Lineare Optimierung und Netzwerkoptimierung, 2. Auflage, 2006, S 105 ff. beschrieben.

671 Vgl. SUHL, L.; MELLOULI, T.: Optimierungssysteme, 2006, S. 169 ff.

672 Vgl. HAMACHER, H. W.; KLAMROTH, K.: Lineare Optimierung und Netzwerkoptimierung, 2. Auflage, 2006, S 111.

Gesamtaufwands für die Authentifizierung erzielen.[673] Um die Optimierung zusätzlich neben dem Hinblick auf den Aufwand auch hinsichtlich der gemäß Abschnitt 5.4.3 bewerteten Sicherheit durchzuführen, existieren Verfahren, die minimale Spannbäume für mehrkriterielle Optimierungsverfahren erweitern, diese jedoch als NP-vollständig beschreiben.[674] Für die Reduktion der Knoten (Int_a) oder die Integration der Kanten (Int_d) müssen für die Verwendung von Netzwerkoptimierungsverfahren zunächst alle theoretisch möglichen Kanten zwischen den beiden betrachteten Elementen (z.B. Authentifizierungsverfahren und -systeme) abgebildet und mit Kantengewichten bewertet werden. Anschließend kann analog die Bildung eines minimalen Spannbaums zur Optimierung erfolgen. Für die Integration von Knoten (Int_b) können so jedoch maximal Ansatzpunkte durch eine verbleibende hohe Anzahl von Knoten ermittelt werden. Auch die gegenseitige Abhängigkeit zwischen Aufwand und erzielter Sicherheit sowie die bereits für Abbildung 6-3 beschriebene Unschärfe begründen die eingeschränkte Eignung von Netzwerkoptimierungsverfahren für das skizzierte Modell zur Vereinheitlichung der Authentifizierung.

6.2.2 Unschärfe von Aufwand und Sicherheit im Authentifizierungsmodell für heterogene IT-Strukturen

Für die folgenden Betrachtungen wird neben der Integration von Relationen (Int_c) anhand der Bestimmung von minimalen Spannbäumen, wie im vorherigen Abschnitt beschrieben, ein unscharfes, auf Fuzzy Logic basierendes, Modell für die Bewertung von Aufwand und Sicherheit verwendet. Es erweitert die Bewertung der Kantengewichte innerhalb des im Abschnitt 5.1 eingeführten Authentifizierungsmodells für heterogene IT-Strukturen. Die Unschärfe des Aufwands und der erzielten Sicherheit wurde im vorherigen Abschnitt bereits anhand der Abbildung 6-3 beschrieben. Der „Fuzzy Logic“ Ansatz wurde 1965 von L. A. Zadeh vorgestellt.[675] Er ermöglicht es, verbale, ungenaue Bewertungen mathematisch zu erfassen. Während im Sinne des scharfen Cantorschen Mengenbegriffs jedes Element eindeutig einer zugehörigen Menge zugewiesen ist[676], erlaubt die Fuzzy-Logik eine variable Zugehörigkeit der Elemente zu einer damit unscharfen Menge. In der Aussagenlogik lassen sich beispielsweise Variablen eindeutig in „ja“ und „nein“ differenzieren. Fuzzy-Logik erlaubt hier stattdessen eine variable Zugehörigkeit und ermöglicht damit die Abbildung verbaler Bewertungen wie „eher nicht“ oder „vielleicht“. BIETHAHN ET AL. und ROMMELFANGER

673 Vgl. HAMACHER, H. W.; KLAMROTH, K.: Lineare Optimierung und Netzwerkoptimierung, 2. Auflage, 2006, S 113 ff.

674 Vgl. HAMACHER, H. W.; RUHE, G.: On spanning tree problems with multiple objectives, 2005.

675 Vgl. ZADEH, L. A.: Fuzzy Sets, 1965; ZIMMERMANN, H. J.: Fuzzy set theory and its applications, 1991.

676 Vgl. MEYBERG, K.; VACHENAUER, P.: Höhere Mathematik 1, 4. Auflage, 1997, S. 1 f.

UND EICKEMEIER. beschreiben den Einsatz von Fuzzy-Logik für Optimierungssysteme in den Wirtschaftswissenschaften.[677] Im Vordergrund steht dabei die Entscheidungsfindung bzw. -unterstützung, die dadurch eine Bewertung vager Zusammenhänge und deren Einbindung in den Entscheidungsprozess ermöglicht.[678] Aufwand und Sicherheit werden daher im Folgenden als unscharfe Eingangsvariablen für einen Entscheidungsprozess zur Optimierung der Authentifizierung in heterogenen IT-Strukturen definiert. Die Unschärfe resultiert hierbei neben den in Abbildung 6-3 erläuterten Zusammenhängen auch aus der individuellen Wahrnehmung der Sicherheit und dem damit verbundenen Aufwand. Während die Authentifizierung selbst eine scharfe Ergebnismenge verwendet (die Authentifizierung ist entweder „erfolgreich“ oder „nicht erfolgreich“), stellt die Sicherheit einen abstrakten Begriff dar, der nur bedingt mess- bzw. quantifizierbar ist. Vorgehensweisen, die beispielsweise für den einen Benutzer oder die eine Organisation noch als sicher gelten, können von anderen bereits als inakzeptabel angesehen werden. Genauso kann ein für die Sicherheit erforderlicher Aufwand, z.B. bedingt durch Vorkenntnisse eines Anwenders, als akzeptabel hingenommen werden, während andere Benutzer bereits beginnen, den Aufwand zu umgehen und damit das Sicherheitsniveau zu reduzieren. Abbildung 6-4 zeigt die Zuordnung der in Abschnitt 5.4.2 beschriebenen Bewertung des Aufwands zu einer Fuzzy-Menge. Sie beschreibt daher eine „Fuzzyfizierung“ des Aufwands als ersten Schritt der Erstellung eines Fuzzy-Modells.[679]

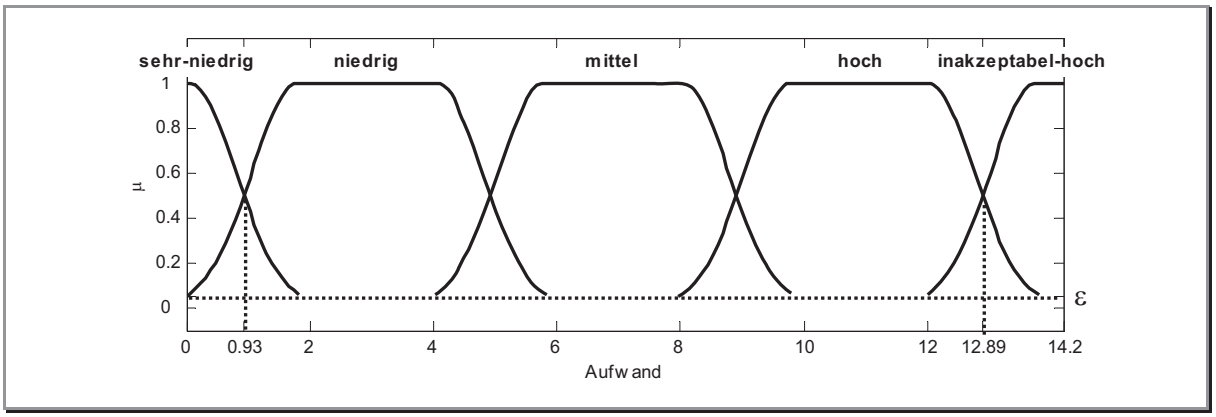

Abbildung 6-4: Fuzzy-Bewertung des Aufwands für die Authentifizierung

677 Vgl. BIETHAHN ET AL.: Methoden der praktischen Entscheidungsfindung, 4. Auflage, 2000, S. 95 ff.; BIETHAHN, J. ET AL.: Fuzzy Set-Theorie in der betriebswirtschaftlichen Anwendung, 1996; ROMMELFANGER, H. J.; EICKEMEIER, S. H.: Entscheidungstheorie. Klassische Konzepte und Fuzzy-Erweiterungen, 2002, S. 173 ff.

678 Vgl. BIETHAHN ET AL.: Methoden der praktischen Entscheidungsfindung, 4. Auflage, 2000, S. 95.

679 Vgl. BIETHAHN ET AL.: Methoden der praktischen Entscheidungsfindung, 4. Auflage, 2000, S. 99 ff. und ROMMELFANGER, H. J.; EICKEMEIER, S. H.: Entscheidungstheorie. Klassische Konzepte und Fuzzy-Erweiterungen, 2002, S. 35 ff.

Als markante untere Grenze wurde der Wert 0,93 definiert. Dieser entsteht für *A*, indem allen in Abschnitt 5.4.2 genannten Kriterien der jeweils kleinste Wert ungleich Null zugewiesen wird ($A_{b.sa}$ = 0,33, $A_{b.beq}$ = 0,33, $A_{b.bar}$ = 0,33, $A_{o.sa}$ = 0,25, $A_{o.po}$ = 0,25, $A_{o.mob}$ = 0,33, $A_{b.war}$ = 0,5, $A_{b.vt}$ = 0,33, $A_{b.ab}$ = 0,5, $A_{b.aus}$ = 0,33, $A_{o.bv}$ = 0,33, $A_{o.sw}$ = 0,33, $A_{o.hw}$ = 0,5, $A_{o.war}$ = 0,33) sowie *control*, *freq*, *policy*, *management* und *self-service* den Wert 0,5 erhalten. Er markiert die Schwelle, ab der der ermittelte Wert für den Aufwand in dieser Arbeit als „niedrig" bewertet wird. Werte unterhalb dieser Schwelle gelten als „sehr niedrig". Der Aufwand für die Authentifizierung wird hierbei vom Benutzer nicht wahrgenommen. ROMMELFANGER UND EICKEMEIER empfiehlt für Zugehörigkeitsfunktionen in den Wirtschaftswissenschaften die Verwendung s-förmiger Funktionen, die sich an der Nutzentheorie orientieren[680], statt der in der Mess- und Regeltechnik üblichen Trapez- und Dreiecksfunktionen. Als Basis für die Zugehörigkeitsfunktion des Aufwands wurde daher die Gaußsche Normalverteilung gewählt. Die Funktionen für die Klassen „sehr-niedrig", „niedrig", „mittel", „hoch" und „inakzeptabel-hoch" stellen dabei eine Kombination aus zwei Gauß-Funktionen dar, deren Steigung so definiert wurde, dass der Schnittpunkt der Zugehörigkeitsfunktionen „sehr-niedrig" und „niedrig" den zuvor genannten Schwellwert für den Aufwand bei 0,93 bildet und ein Aufwand von 0 eine Zugehörigkeit $\mu = 1$ zur Klasse „sehr-niedrig" aufweist. Jede Schwelle ist somit zu jeweils gleichem Anteil ($\mu = 0{,}5$) zugehörig zu beiden angrenzenden Klassen. Von ROMMELFANGER UND EICKEMEIER wird zusätzlich empfohlen, Zugehörigkeitswerte unterhalb eines Mindestniveaus ε zu ignorieren, um eine fehlerhafte Beeinflussung des Entscheidungsprozesses durch die asymptotische Annäherung der Zugehörigkeitsfunktion an den Wert Null zu vermeiden.[681] Es wurde daher $\varepsilon = 0{,}05$ festgelegt.

Als oberer Schwellwert zwischen den Klassen „hoch" und „inakzeptabel-hoch" wurde der Wert 12,89 definiert. Dieser begründet sich durch ($A_{b.sa}$ = 1), wobei sowohl technische Vorkenntnisse als auch spezielle Hard- und Software erforderlich sind.[682] ($A_{b.beq}$ = 0,67). Zwei der Bedingungen zur Bequemlichkeit treffen zu (z.B. die Authentifizierung selbst ist zeitaufwendig und ein Benutzer

---

680 Vgl. ROMMELFANGER, H. J.; EICKEMEIER, S. H.: Entscheidungstheorie. Klassische Konzepte und Fuzzy-Erweiterungen, 2002, S. 178.

681 Vgl. ROMMELFANGER, H. J.; EICKEMEIER, S. H.: Entscheidungstheorie. Klassische Konzepte und Fuzzy-Erweiterungen, 2002, S. 178.

682 Was gemäß RENAUD, K.: Evaluating Authentication Mechanisms, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 116 und PIAZZALUNGE, U.; SALVANESCHI, P.; COFFETTI, P.: The Usability of Security Devices, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 227 ff. geringe Akzeptanz aufseiten der Benutzer bewirkt. Vgl. Bewertung des Aufwands in Abschnitt 5.4.2.

benötigt diverse Authentifizierungsmerkmale).[683] Sowohl kognitiv und physisch als auch sensorisch behinderte Benutzer können die Authentifizierung nicht verwenden ($A_{b.bar} = 1$). Mindestens drei spezielle Anforderungen für die Authentifizierung werden an die Organisationen als Betreiber gestellt ($A_{o.sa} = 0{,}75$) (z.B. spezielle Hardware, Software und technische Vorkenntnisse der Administratoren).[684] Außerdem sind drei der Kriterien hinsichtlich des Aufwands bei der Portabilität der Authentifizierung erfüllt ($A_{o.po} = 0{,}75$) (z.B. schlecht skalierbar für wachsende Benutzerzahlen, inkompatibel mit anderen bestehenden Lösungen und plattformabhängig).[685] Die Lösung ist nicht mobil bzw. nicht ohne Weiteres an unterschiedlichen Arbeitsplätzen verwendbar ($A_{o.mob} = 1$). Sowohl Wartung und Verarbeitungstiefe bei der Einrichtung der Authentifizierung als auch Abrufbarkeit z.B. des erforderlichen Merkmals sind hierbei für die Benutzer mit hohem Aufwand verbunden ($A_{b.war} = 1$), ($A_{b.vt} = 1$) und ($A_{b.ab} = 1$). Allerdings ist das Merkmal nicht fremd zugewiesen ($A_{b.aus} = 0{,}67$), was derzeit gängige Praxis etwa für die Wahl von Passwörtern ist.[686] Für Organisationen wurden zwei der drei Vorgänge (Einrichtung, Erneuerung und Sperrung) mit hohem Aufwand angenommen ($A_{o.bv} = 0{,}67$).[687] Spezielle Hard- und Software mit Anschaffungskosten, laufenden Lizenz- sowie Wartungskosten ist erforderlich ($A_{o.sw} = 1$), ($A_{o.hw} = 1$). Die Wartung für Implementierung, Betrieb und Erneuerung der Authentifizierungsmaßnahmen ist aufwendig ($A_{o.war} = 1$). *control*, *freq*, *policy*, *management* und *self-service* wurden jeweils mit ihrem Maximum 1,5 einbezogen.

Zwischen dem oberen Schwellwert als angenommene Akzeptanzgrenze sowie dem unteren Schwellwert für merklichen Aufwand der Authentifizierung wurden die drei Klassen „niedrig", „mittel" und „hoch" gleichmäßig verteilt. Der Maximalwert für A beträgt 14,2.[688]

Für die Sicherheit wurde ebenfalls eine „Fuzzyfizierung" vorgenommen, die die Abbildung 6-5 illustriert.

---

683 Vgl. negative Bewertung analog zu ADAMS, A.; SASSE, A.: Users Are Not the Enemy. Why Users Compromise Security Mechanisms and How to Take Remedial Measures, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 644 ff.

684 Was auch in RENAUD, K.: Evaluating Authentication Mechanisms, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 116 als inakzeptabel gilt.

685 Vgl. z.B. den Aufwand für die Vergabe von Tokens und deren Plattformabhängigkeit in Abschnitt 2.5.2.

686 Vgl. RILEY, S.: Password Security: What Users Know and What They Actually Do, 2006; BURNETT, M.; KLEIMAN, D.: Perfect Passwords, 2006, S. 6 ff.

687 Vgl. hierzu auch RENAUD, K.: Evaluating Authentication Mechanisms, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 116 f.

688 Vgl. Abschnitt 5.4.2.5.

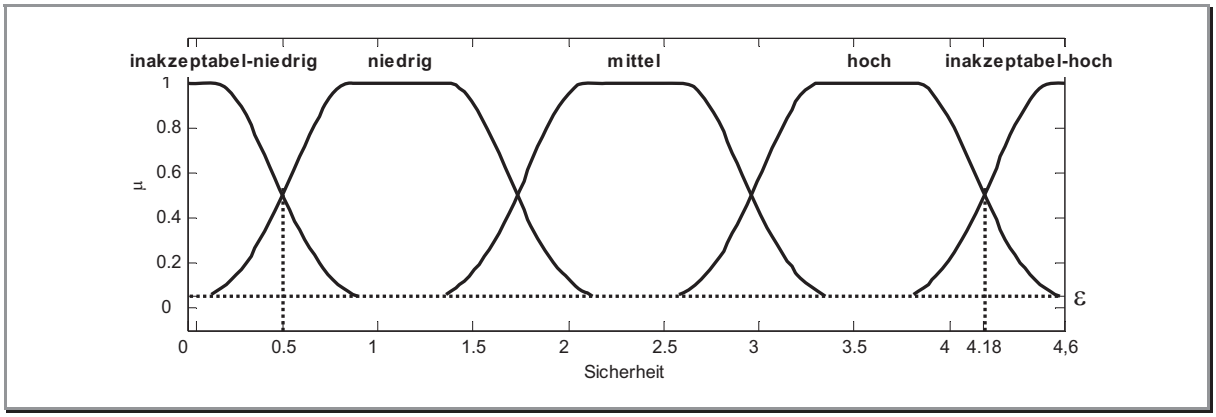

Abbildung 6-5: Fuzzy-Bewertung der Sicherheit als Nutzen der Authentifizierung

Analog zur „Fuzzyfizierung" des Aufwands wurden s-förmige Zugehörigkeitsfunktionen verwendet und ε = 0,05 als Mindestniveau vorgegeben. Untere Schwelle der Sicherheit stellt der Wert 0,5 für *S* dar. S = 0,5 setzt sich dabei zusammen aus S_{vor} = 0,5, S_{of} = 0,5, S_{fe} = 0, S_{an} = 0,33, S_{dat} = 0,5, S_{rz} = 0,25 sowie *risk* = 1, *motive* = 0,5 und *audit* = 0,5. Dabei wurde für die in Abschnitt 5.4.3 genannten Kriterien für *S* eine Passwort-basierte Authentifizierung als einfachstes technisches Mittel mit der größten Verbreitung in der Praxis gewählt.[689] Die Vorhersagbarkeit ist hier bei z.B. häufig auf Namen, Geburtstagen etc. basierenden Passwörtern für Freunde und Bekannte möglich ($\boldsymbol{S_{vor}}$ = 0,5).[690] Passwörter werden während der Eingabe zum Zweck der Authentifizierung offengelegt ($\boldsymbol{S_{of}}$ = 0,5).[691] Ihre Fülle liegt in der Regel unter dem Niveau von FIPS 118, das zehn Zeichen lange, randomisierte Passwörter mit einer resultierenden maximalen Fülle von 2^{40} möglichen Passwörtern vorsieht ($\boldsymbol{S_{fe}}$ = 0).[692]

Passwörter sind durch „brute-force"-Angriffe verletzbar ($\boldsymbol{S_{an}}$ = 0,33).[693] Benutzer können Passwörter in der Regel selbst bestimmen und daher Einfluss auf die in ihnen enthaltenen Daten nehmen ($\boldsymbol{S_{dat}}$ = 0,5). Während der Authentifizierung werden Passwörter in der Regel verschlüsselt resp.

---

689 Vgl. CHESWICK, W. R.; BELLOWIN, S. M., RUBIN, A. D.: Firewalls und Sicherheit im Internet. 2. Aufl., 2004, S. 179.

690 Vgl. BURNETT, M.; KLEIMAN, D.: Perfect Passwords, 2006, S. 17.

691 Passwörter sind in der Regel auch leicht notierbar, die Schwelle zum niedrigen Sicherheitsniveau wird hier jedoch durch die Offenlegung bei der Eingabe bestimmt.

692 Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 99 zur durchschnittlichen Länge siehe RILEY, S.: Password Security: What Users Know and What They Actually Do, 2006.

693 Grundsätzlich ist durch die Offenlegung während der Eingabe auch ein „key-logger" (vgl. „password sniffing" in SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 23 ff.) als Angriff möglich. Als Schwelle zum niedrigen Sicherheitsniveau wird jedoch „brute force" CHESWICK, W. R.; BELLOWIN, S. M., RUBIN, A. D.: Firewalls und Sicherheit im Internet. 2. Aufl., 2004, S. 402 betrachtet.

vertraulich übertragen[694] oder Authentifizierungssysteme werden redundant (verfügbar) ausgelegt (S_{sz} = 0,25). Passwörter weisen in der aktuellen Praxis nur Benutzer gegenüber dem System aus (nicht zusätzlich das System gegenüber dem Benutzer). Sie bilden einen einzelnen Faktor der Authentifizierung und setzen abgesehen von „One Time Password" als passive Tokens[695] keine zusätzliche Hardware zur physischen Absicherung ein (S_{aut} = 0). Für die Beschreibung der Umgebung wurde angenommen, dass Fehler der Authentifizierung nur die Daten des kompromittierten Benutzers selbst offenlegen (*risk* = 1), Benutzer im schlimmsten Fall keine Kenntnis über IT-Sicherheit besitzen (*motive* = 0,5) und keinerlei Überprüfung der IT-Sicherheit durchgeführt wird (*audit* = 0,5).

Als Maximum wurde der Wert 4,18 festgelegt. Dabei wird angenommen, dass die Authentifizierung für niemanden außer dem Benutzer selbst vorhersagbar ist (S_{vor} = 1) und zu keinem Zeitpunkt für die Authentifizierung relevante Informationen offengelegt werden (S_{of} = 1). Eine Fülle oberhalb von 64 Bit ist in der Praxis nur mit kryptographischen Schlüsseln erreichbar[696] (S_{fe} = 1).[697] Es sind keine Angriffe auf das Verfahren bekannt (S_{an} = 1), personenbezogene Daten werden für die Authentifizierung nicht verwendet (S_{dat} = 1). Drei der vier möglichen Schutzziele werden erreicht (S_{sz} = 0,75). Fehlendes viertes Ziel könnte hier z.B. die Verbindlichkeit sein, die Zertifikate[698] bzw. Tokens[699] erfordert und in der Praxis durch Komplexität einen hohen Verwaltungsaufwand bedeutet. Mindestens zwei der Anforderungen an (S_{aut} = 0,67) sind erfüllt. Beispielsweise wird ein Token verwendet, welches eine physikalische Multi-Faktor-Authentifizierung darstellt. Es wurde zusätzlich angenommen, dass hohe Sicherheitsanforderungen an der Schwelle zur Klasse „inakzeptabel-hoch" keinerlei Risiko für den Zugriff auf die durch die Authentifizierung geschützten Daten bilden (*risk* = 1,5). Benutzer werden bzgl. der IT-Sicherheit geschult (*motive* = 1) sowie die IT-Sicherheit fortlaufend überprüft (*audit* = 1).

Die Kombination der „fuzzyfizierten" Eingangsvariablen Aufwand und Sicherheit ergibt (ebenfalls „fuzzyfiziert") die Ausgabevariable, die die realisierte Vereinheitlichung widerspiegelt und in Abbildung 6-6 dargestellt ist. Niedrigerer Aufwand und höhere Sicherheit als vor der Vereinheitli-

---

694 Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 143 ff.

695 Vgl. Abschnitt 2.5.2.

696 Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 99 ein typischen 10-Zeichen Passwort (englischer Text) besitzt eine Fülle von 16 Bit („attack space"). Die FIPS wurden zusätzlich in Abschnitt 2.3.1 genannt.

697 Vgl. SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 98 f.

698 Vgl. Abschnitt 2.6.2.

699 Vgl. Abschnitt 2.5.2.

chung innerhalb einer heterogenen IT-Struktur führen somit zu einer Optimierung. Die Optimalität der Vereinheitlichung wird in die normalverteilten (auf der Gauss-Funktion basierenden) Zugehörigkeitsfunktionen „schlechter-“, „schlechter“, „neutral“, „besser“ und „besser+“ aufgeteilt. Die Spannweite der Funktionen resp. Steigung wurde so definiert, dass die Schnittpunkte der Zugehörigkeit zwischen zwei Klassen bei μ=0,25 liegen, um eine signifikante Zugehörigkeit der Ergebnisse zu den Klassen zu erzielen.

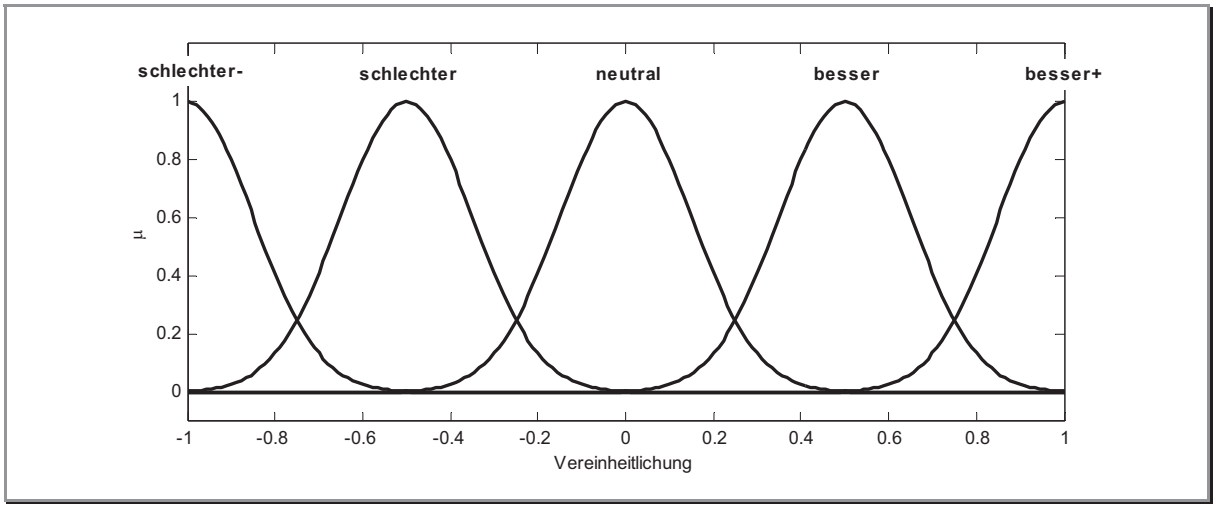

Abbildung 6-6: Fuzzy-Bewertung der Vereinheitlichung der Authentifizierung

Die Verknüpfung zwischen Aufwand und Sicherheit wurde gemäß der in diesem Abschnitt sowie in Abschnitt 6.1 gestellten Anforderungen und unter Verwendung der von CRANOR UND GARFINKEL gesammelten Usability- resp. Benutzbarkeit-Bewertungen wie folgt festgelegt:[700]

Für weitere Betrachtungen in dieser Arbeit sinkt gemäß der Tabelle 6-1 die Vereinheitlichung mit steigendem Aufwand und abnehmender Sicherheit. Ein inakzeptabel hoher Aufwand bei einer inakzeptabel niedrigen erzielten Sicherheit stellt hierbei das untere Ende der Bewertungsskala für die Vereinheitlichung dar. Umgekehrt bildet ein sehr niedriger Aufwand bei hoher erzielter Sicherheit die ideale Vereinheitlichung am oberen Ende der Skala. Inakzeptabel hohe Sicherheit führt jedoch durch die eingangs in diesem Abschnitt bewerteten Effekte in Bezug auf die Akzeptanzgrenze seitens der Benutzer zu einer Minderung der erzielten Vereinheitlichung.

---

[700] Vgl. ADAMS, A.; SASSE, A.: Users Are Not the Enemy. Why Users Compromise Security Mechanisms and How to Take Remedial Measures, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 639 ff.; SASSE, M. A.; FLECHAIS, I.: Usable Security. Why Do We Need It? How Do We Get It?, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 13 ff.; RENAUD, K.: Quantifying the Quality of Web-Authentication Mechanisms. A Usability Perspektive, in Journal of Web Engineering 3(2), 2003, S. 95 ff.

Aufwand	Sicherheit	Vereinheitlichung
sehr-niedrig	inakzeptabel-niedrig	neutral
sehr-niedrig	niedrig	besser
sehr-niedrig	mittel	besser+
sehr-niedrig	hoch	besser+
sehr-niedrig	inakzeptabel-hoch	neutral
niedrig	inakzeptabel-niedrig	schlechter
niedrig	niedrig	neutral
niedrig	mittel	besser
niedrig	hoch	besser+
niedrig	inakzeptabel-hoch	neutral
mittel	inakzeptabel-niedrig	schlechter
mittel	niedrig	schlechter
mittel	mittel	neutral
mittel	hoch	besser
mittel	inakzeptabel-hoch	schlechter
hoch	inakzeptabel-niedrig	schlechter-
hoch	niedrig	schlechter
hoch	mittel	neutral
hoch	hoch	neutral
hoch	inakzeptabel-hoch	schlechter
inakzeptabel-hoch	inakzeptabel-niedrig	schlechter-
inakzeptabel-hoch	niedrig	schlechter-
inakzeptabel-hoch	mittel	schlechter
inakzeptabel-hoch	hoch	neutral
inakzeptabel-hoch	inakzeptabel-hoch	schlechter

Tabelle 6-1: Verknüpfung der Eingangsvariablen Aufwand und Sicherheit zur Ausgangsvariablen Vereinheitlichung

6.2.3 Zielfunktion für die Vereinheitlichung des Authentifizierungsmodells

Die im vorherigen Abschnitt erläuterte Verknüpfung zwischen Aufwand und Sicherheit anhand des skizzierten Fuzzy-Modells führt zu der Zielfunktion, die die Optimalität der Vereinheitlichung der Authentifizierung bestimmt. Die Vereinheitlichung erfolgt hierbei anhand des in Abschnitt 5.1 eingeführten Authentifizierungsmodells. Hierfür wurden die Fuzzy-Mengen Aufwand und Sicherheit anhand der in Tabelle 6-1 getroffenen Vorgaben über den Minimum-Operator verknüpft (z.B. $A = 0{,}93$ und $S = 0{,}5$, $\mathrm{Min}(0{,}93;0{,}5) = 0{,}5$).[701] Für die Bestimmung des Erfüllungsgrades (Implika-

[701] Vgl. BIETHAHN ET AL.: Methoden der praktischen Entscheidungsfindung, 4. Auflage, 2000, S. 102 ff.

tion) und die Zuweisung zur entsprechenden Klasse bzw. Zugehörigkeitsfunktion der Ausgangsvariable Vereinheitlichung wurde die Max-Prod-Inferenz verwendet.[702] Wie von Rommelfanger vorgeschlagen, wurden die resultierenden erfüllten Zugehörigkeitsfunktionen mittels der algebraischen Summe aggregiert.[703] Abbildung 6-7 zeigt die anhand der Schwerpunkt-Methode „defuzzyfizierten" Ergebniswerte des Fuzzy-Modells.[704] Für die Erzeugung der Abbildung wurde das Paket sciFLT des scilab-Projekts verwendet.[705]

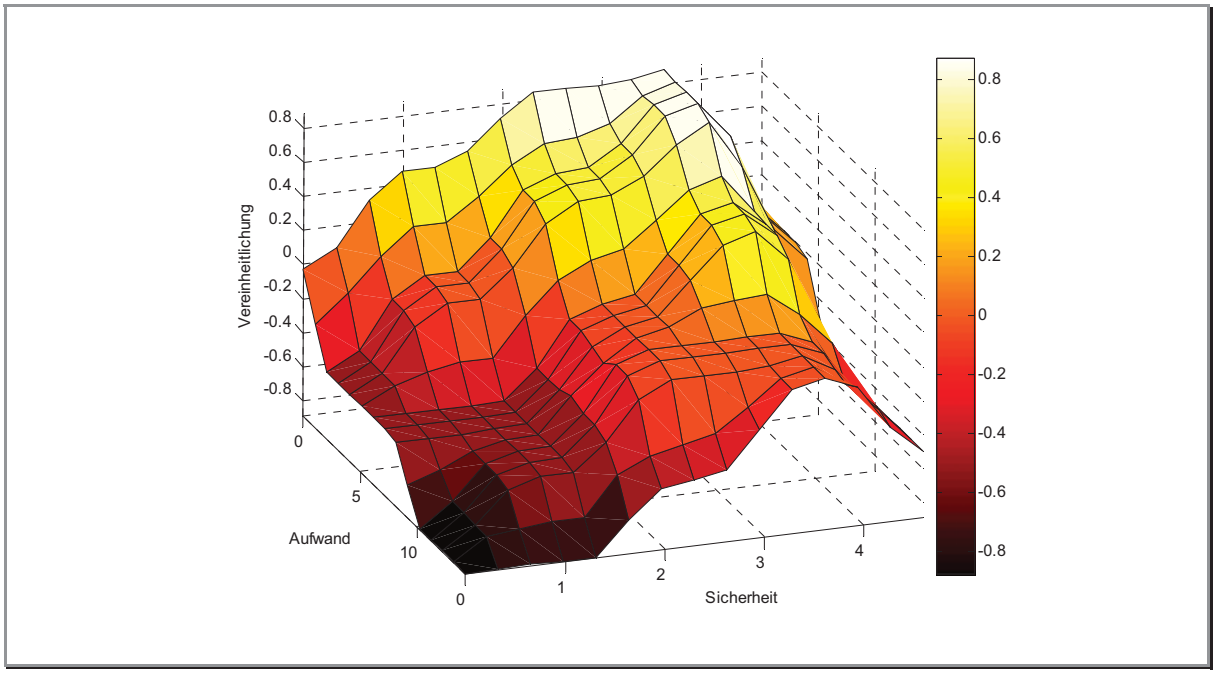

Abbildung 6-7: Zielfunktion und Optimum der Vereinheitlichung

Aus der Abbildung 6-7 lässt sich erkennen, dass die Vereinheitlichung erwartungsgemäß mit steigendem Aufwand sinkt, hingegen mit höherer Sicherheit zunimmt. Sobald Werte des Sicherheitsniveaus „inakzeptabel-hoch" erzielt werden, sinkt die Vereinheitlichung, wie bereits erläutert, ab und spiegelt damit den Einfluss der höheren Komplexität hoher Sicherheitsanforderungen hinsicht-

[702] Vgl. BIETHAHN ET AL.: Methoden der praktischen Entscheidungsfindung, 4. Auflage, 2000, S. 102 ff. und ROMMELFANGER, H. J.; EICKEMEIER, S. H.: Entscheidungstheorie. Klassische Konzepte und Fuzzy-Erweiterungen, 2002, S. 182.

[703] Vgl. ROMMELFANGER, H. J.; EICKEMEIER, S. H.: Entscheidungstheorie. Klassische Konzepte und Fuzzy-Erweiterungen, 2002, S. 182.

[704] Vgl. BIETHAHN ET AL.: Methoden der praktischen Entscheidungsfindung, 4. Auflage, 2000, S. 109 ff.

[705] Vgl. sciFLT, 2007; scilab, 2007.

lich deren Akzeptanz seitens der Benutzer wider.[706] Aufgrund der höheren Komplexität wird die erzielbare Vereinheitlichung hier abgeschwächt.

Das Optimum kann somit für die die Vereinheitlichung V anhand folgender Zielfunktion beschrieben werden:

Maximiere $V = A * S \Rightarrow Max!$

In Abschnitt 5.4.2.5 wurde ein Maximum von 14,2 für den Aufwand A quantifiziert. Als Maximum für die in dieser Arbeit quantifizierte Sicherheit S wurde 4,6 ermittelt. Um für die genannte Zielfunktion das Optimum in Bezug auf A und S zu erzielen, werden die in Abschnitt 5.2 beschriebenen Vereinheitlichungsformen verwendet. Wie für die Integration von Authentifizierungsmerkmalen in Abschnitt 5.5.3 beschrieben, werden hierbei die Kantengewichte der in Abbildung 5-4 und Abbildung 5-5 beschriebenen Graphen aus Sicht der Benutzer und Betreiber in Bezug auf den Aufwand minimiert sowie die erzielte Sicherheit als Nutzen gewahrt. Dabei variiert die Anzahl n der Kanten für die individuellen betrachteten Elemente. Aufwand und Sicherheit wurden jedoch im vorherigen Abschnitt sowie in der Lösungsmenge der Zielfunktion, wie in Abbildung 6-7 gezeigt, auf eine einzelne Kante mit den Maximalwerten 14,2 für den Aufwand sowie 4,6 für die erzielte Sicherheit normiert. Folgende Optimierungsbetrachtungen verwenden in Bezug auf das Fuzzy-Modell daher ein relativiertes Verhältnis zwischen maximal möglichem Aufwand bzw. erzielter Sicherheit und den jeweiligen nach der Optimierung erzielten Werten aller betrachteten Kanten.

Der relative Gesamtaufwand wird aus dem Verhältnis zwischen ermitteltem und maximalem Aufwand für n vor der Optimierung existierende Kanten definiert als:

$$A_{gesamt} = \frac{\sum_{k=1}^{n} A_k}{14{,}2 * n} * 14{,}2 = \frac{\sum_{k=1}^{n} A_k}{n}, \qquad \text{wobei: } 0 \le A_{gesamt}, A_k \le 14{,}2$$

Dabei bezieht sich die Summe über A_k auf die Kantengewichte nach der Vereinheitlichung. A_{gesamt} bildet somit den Durchschnitt des Aufwands bezogen auf die ursprünglich zwischen den Elementen existierenden Kanten.

Analog ergibt sich für die Kantengewichte, die die Sicherheit beschreiben, das Verhältnis zwischen erzielter Sicherheit und maximal für n existierende Kanten erreichbarer Sicherheit relativ zum Maximalwert 4,6:

[706] Vgl. Beschreibung der Akzeptanzgrenze in Abbildung 6-3.

$$S_{gesamt} = \frac{\sqrt{\frac{S\min}{4{,}6} * \sum_{k=1}^{n} S_k}}{\sqrt{4{,}6n}} * 4{,}6 = \frac{\sqrt{4{,}6n} \cdot \sqrt{\frac{S\min}{4{,}6} * \sum_{k=1}^{n} S_k}}{n} \text{ , wobei: } 0 \le S_{gesamt}, S_k \le 4{,}6$$

Die erzielte Sicherheit erfüllt somit für *n* Kanten die in Abschnitt 5.4.3 geforderten Kriterien. Sie hängt in verstärktem Maße von dem kleinsten enthaltenen Kantengewicht als minimales Sicherheitsniveau ab. Bedingt durch die zunehmende Komplexität wächst die insgesamt erzielte Sicherheit nicht linear mit der Anzahl der Kanten *n*.[707]

Durch die Bewertung der Optimierung anhand der gegebenen Zielfunktion bzw. dem Ergebnis *V* können geeignete Vereinheitlichungsformen aus dem Abschnitt 5.2 ausgewählt werden. Im Folgenden wird durch die Bewertung konkreter Fallstudien dadurch eine Überprüfung der Hypothesen aus Kapitel 5 anhand der Erkenntnisse aus der exemplarischen Übernahme des Modells aus Abschnitt 5.1 in die Praxis heterogener IT-Strukturen möglich.

6.3 Implementierung eines Referenzmodells

Während in den vorherigen Abschnitten die theoretischen Grundlagen der einheitlichen Authentifizierung definiert wurden, liefern die folgenden Abschnitte hierauf basierend Lösungen für die praktische Umsetzung einheitlicher Authentifizierung sowie die Erweiterung der in Abschnitt 3.2 vorgestellten bestehenden Verfahren. Diese bestätigen die Isomorphie des theoretischen Modells für die Übernahme in reale heterogene IT-Strukturen. Dadurch werden auch Ansatzpunkte für die Transformation der Ergebnisse der im Abschnitt 6.2 erläuterten Optimierung auf bestehende IT-Strukturen beschrieben.

6.3.1 Kombination bestehender Verfahren für eine einheitliche Authentifizierung

Existierende Verfahren für die einheitliche Authentifizierung wurden bereits in Abschnitt 3.2 beschrieben. Basierend auf den aufgestellten Hypothesen werden für die weitere Betrachtung in diesem Abschnitt zunächst bestehende Ansätze für die Vereinheitlichung von Authentifizierungsmerkmalen, -verfahren und -systemen in heterogenen IT-Strukturen ausgewählt und in nachfolgenden Abschnitten erweitert.

[707] Vgl. Zunahme der Sicherheit in Abbildung 6-1 und Abbildung 6-3.

Geeignete Verfahren für die Vereinheitlichung von Authentifizierungsmerkmalen

Eine Reduktion von Authentifizierungsmerkmalen (Int_a) wäre ausschließlich aufseiten der Organisation durch einen Verzicht z.B. auf Sicherheitsanforderungen möglich. Für Benutzer würde ein Verzicht bedeuten, auch die zugehörigen Authentifizierungsverfahren und -systeme und damit verbundene Ressourcen nicht mehr verwenden zu können. Die Reduktion der Relationen zu Authentifizierungsverfahren (Int_c) würde ebenfalls einen Verzicht bedeuten. Eine Integration (Int_d) ist für die Organisationen nur bedingt möglich, da Authentifizierungsmerkmale in der Regel als nicht invertier- resp. konvertierbarer Hash-Wert gespeichert werden.[708] Hypothese H4 aus Abschnitt 5.5.5 nennt daher die Integration von Authentifizierungsmerkmalen (Int_c) als ideale Form der Vereinheitlichung sowohl für die Benutzer als auch für die Organisationen.

Die Integration der Authentifizierungsmerkmale (Int_b) seitens der Benutzer und Organisationen als ideale Vereinheitlichung wird ermöglicht durch die bestehenden Verfahren:

- **Meta-Directory und Virtual Directory**[709]

  Authentifizierungsmerkmale resp. -konten werden im Meta-Directory oder Virtual-Directory zusammengefasst und zentral administriert bzw. synchronisiert.

- **Public-Key-Infrastruktur**[710] **und Einsatz von Tokens**[711]

  Unterschiedliche Authentifizierungsmerkmale (Passwörter, Zertifikate) werden auf einem Token integriert. Ggf. wird hierbei schrittweise die Migration von Passwörtern zu Zertifikaten auf dem Token vollzogen.

Es ist anzumerken, dass durch die Integration mehrerer Authentifizierungsmerkmale in einem neuen Element zunächst zusätzlicher Aufwand entsteht. Bedingt durch die nicht mögliche Konvertierung von Hash-Werten[712] und deren verbreitete Verwendung bei der Speicherung von Passwörtern kann jedoch nur auf diese Weise eine weiche Migration zu neuen Authentifizierungsmerkmalen, -verfahren und -systemen erfolgen. Eine Reduktion der Authentifizierungsmerkmale ist nur möglich, sofern die dadurch geschützten Ressourcen über die unterstützten Verfahren und Systeme auch andere bzw. alternative Merkmale nutzen können.

---

[708] Vgl. $Div_{Merkmal.g}$ in Abschnitt 5.5.1.

[709] Vgl. die Synchronisation von Informationen in Verzeichnisdiensten über Meta- oder Virtual Directories in Abschnitt 3.2.2.

[710] Vgl. den Aufbau von Public-Key-Infrastrukturen in Abschnitt 3.2.4.

[711] Vgl. den Einsatz von Tokens als Authentifizierungsmerkmal in Abschnitt 2.5.2.

[712] Vgl. fehlende Invertierbarkeit von Hash-Verfahren in Abschnitt 2.6.2.

Geeignete Verfahren für die Vereinheitlichung von Authentifizierungsverfahren

Eine Reduktion von Authentifizierungsverfahren (Int_a) oder zugehörigen Relationen (Int_c) wäre analog zu den Authentifizierungsmerkmalen nur durch die Organisationen möglich. In jedem Fall bedeutet die einfache Reduktion einen Verzicht, der nur dann akzeptabel ist, sofern die Authentifizierungsmerkmale und -systeme auch andere Authentifizierungsverfahren als die reduzierten unterstützen bzw. ein einzelnes einheitliches Authentifizierungsverfahren verwendet werden kann. Zusätzlich bedeutet die Reduktion auch eine Minderung der erzielten Sicherheit. Die Integration mehrerer Authentifizierungsverfahren in einem separaten Element (Int_b) bedeutet hingegen zusätzlichen Verwaltungsaufwand für das neue Element und sollte daher vermieden werden.[713] Sofern ein Element bereits mehrere Verfahren unterstützt und somit bereits Int_b realisiert[714], kann dies direkt für die Integration der Relationen (Int_d) verwendet werden. Die Hypothese H7 nennt daher die Integration der Relationen (Int_d) zwischen Authentifizierungsmerkmalen und -verfahren als ideale Vereinheitlichungsform.[715]

Folgende bestehende Verfahren erlauben die Integration der Relationen von Authentifizierungsverfahren (Int_d):

- **Kerberos[716], Verzeichnisdienste resp. LDAP[717]**

  Kerberos oder LDAP können als zentrales Authentifizierungsverfahren verwendet werden. Innerhalb der IT-Struktur müssen die Clients jedoch diese Verfahren unterstützen oder entsprechend erweitert werden. Kerberos bietet derzeit den besten Kompromiss zwischen Aufwand und Sicherheit insbesondere für die Realisierung eines Single Sign-On. Public-Key-Infrastrukturen ermöglichen ebenfalls Single Sign-On, bedeuten aber einen höheren Aufwand.[718] Authentifizierungsclients bzw. -automatismen realisieren Single Sign-On nur zu dem Preis einer reduzierten Sicherheit.[719]

---

713 Z.B. sollte für den langfristigen Einsatz auf modulare Authentifizierungs-Clients (vgl. Abschnitt 3.2.8) aufgrund des zusätzlichen Wartungsaufwands verzichtet werden.

714 Vgl. z.B. 802.1X als Verfahren für Netzwerk-Authentifizierung (Abschnitt 3.2.5) oder SAML-basierte Federations (Abschnitt 3.2.7).

715 Vgl. Abschnitt 5.6.5.

716 Vgl. Verwendung und Funktion von Kerberos in Abschnitt 3.2.3.

717 Vgl. LDAP als Authentifizierungsverfahren bei der Verwendung von Verzeichnisdiensten in Abschnitt 3.2.2.

718 Vgl. den Aufbau von Public-Key-Infrastrukturen in Abschnitt 3.2.4.

719 Vgl. Passwort-Speicher in Abschnitt 3.2.9.

Auch ohne die Realisierung von „Single Sign-On“-Lösungen kann z.B. durch die Verwendung von Verzeichnisdiensten[720], die in der Regel LDAP als Authentifizierungsverfahren verwenden, bereits eine Vereinheitlichung der Authentifizierungsverfahren erzielt werden.

- **Federation-basierte Verfahren z.B. SAML**[721]

  Zukünftig ermöglichen Federation-basierte Lösungen nicht nur eine organisationsübergreifende Authentifizierung, sondern implizit auch eine ideale Vereinheitlichung der Authentifizierungsverfahren. Allerdings sind Federation-basierte Lösungen derzeit auf Web-Anwendungen begrenzt.

Generell können Web-Anwendungen als ideale Plattform für einheitliche Authentifizierungsverfahren und Single Sign-On angesehen werden. Die Authentifizierung erfolgt hier innerhalb von Standard-Web-Browsern, ohne dass Benutzer spezielle Software oder Kenntnisse benötigen. Durch oben genannte Federation-basierte Lösungen sowie weitere in Abschnitt 3.2.7 genannte Verfahren können zusätzlich „Single Sign-On“-Funktionalitäten realisiert werden.

Geeignete Verfahren für die Vereinheitlichung von Authentifizierungssystemen

Setzt eine Ressource explizit ein spezielles eigenes Authentifizierungssystem voraus, das von keiner anderen Ressource verwendet wird, so sollte die Ressource auf ein alternatives, gemeinsam verwendetes System umgestellt werden (Int_a). Gleiches gilt für Authentifizierungsverfahren, die ein spezielles oder eigenes Authentifizierungssystem voraussetzen. Sofern technisch möglich, kann auch die Integration mehrerer Authentifizierungssysteme in ein anderes System erfolgen (Int_b). Hierbei können beispielsweise die Authentifizierungskonten des alten Systems für den Zeitraum einer Migration im neuen System hinzugefügt werden. Zur Minderung des Aufwands ist langfristig jedoch Int_c anzustreben. Neben der Reduktion und Integration der Systeme muss zusätzlich auf Redundanz geachtet werden, um trotz der Konzentration auf wenige oder ein einziges Authentifizierungssystem keine zentrale Fehlerquelle („single point of failure“) zu erzeugen. Als ideale Vereinheitlichungsform für Authentifizierungssysteme nennt Hypothese H10 daher in Abschnitt 5.7.5 die Reduktion von Relationen (Int_c) zu Authentifizierungsverfahren und Ressourcen.

Folgende bestehende Verfahren unterstützen die Vereinheitlichung nach Int_c:

---

[720] Vgl. Abschnitt 3.2.2.

[721] Vgl. Federation-basierte Lösungen in Abschnitt 3.2.7.

- **Verzeichnisdienste und Virtual Directory**[722]

  Verwenden Ressourcen oder Authentifizierungsverfahren einen zentralen Verzeichnisdienst, so löst dieser individuelle separate Authentifizierungssysteme ab. Auch die Authentifizierung gegen ein Virtual Directory als Bündelung verschiedener Verzeichnisse oder Datenquellen ist möglich. Authentifizierungskonten werden so zentral administrierbar bzw. die Verwaltung der Authentifizierungssysteme durch deren reduzierte Anzahl vereinfacht.

- **Public-Key-Infrastrukturen**[723]

  Public-Key-Infrastrukturen bieten eine drastische Vereinheitlichung der Authentifizierung, da keine Konten verwaltet werden müssen. Benutzer erhalten ein Zertifikat, dessen Verifizierung die Authentizität gewährleistet, ohne dass alle Zertifikate der Benutzer vorgehalten werden müssen. Lediglich Zertifikate der vertrauenswürdigen Zertifizierungsstellen müssen im Authentifizierungssystem gespeichert werden, um die digitale Signatur und somit die Authentizität prüfen zu können. Auch wenn die einzelnen Zertifikate der berechtigten Benutzer im Authentifizierungssystem gespeichert werden, kann dies ohne Probleme erfolgen. Zertifikate beinhalten ausschließlich öffentliche Schlüssel und können somit leicht unverschlüsselt[724] verteilt werden. Durch die Verteilung der Zertifikate von Zertifizierungsstellen werden zusätzlich Federations ermöglicht.[725] Allerdings bedeuten Public-Key-Infrastrukturen neben erhöhter Sicherheit auch einen erhöhten Aufwand, wie in Abschnitt 3.2.4 beschrieben.

Nachfolgend werden Passwort-Speicher und Authentifizierungsautomatismen, wie sie in Abschnitt 3.2.9 erläutert wurden, nicht betrachtet. Dies resultiert aus den in Abschnitt 3.2.9 beschriebenen Nachteilen für die Sicherheit. Modulare Authentifizierungsclients, Proxies und andere Client-seitige bzw. Frontend-Lösungen werden nur für die Migration beschrieben. Es wird vorausgesetzt, dass die Anzahl der Clients in heterogenen IT-Strukturen größer ist als die der Server und somit der Aufwand für die in Abschnitt 3.2.8 aufgezeigten Authentifizierungsclients und Proxies insbesondere langfristig größer ist als Server-seitige bzw. Backend-Lösungen. In Abschnitt 3.2.5 beschriebene Verfahren und Protokolle für die einheitliche Authentifizierung in Netzwerkstrukturen werden in Bezug auf die Vereinheitlichung von Authentifizierungsverfahren mit berücksichtigt.

---

[722] Vgl. Abschnitt 3.2.2.

[723] Vgl. Abschnitt 3.2.4.

[724] Im Vergleich zu Passwörtern entfällt die Speicherung in unterschiedlichen Hash-Verfahren wie in Abschnitt 5.5.1 beschrieben.

[725] Vgl. Federation-basierte Lösungen in Abschnitt 3.2.7.

6.3.2 Erweiterung bestehender Lösungen

Die folgenden Abschnitte zeigen praktische Möglichkeiten für die Erweiterung der in Abschnitt 3.2 genannten bestehenden Lösungsansätze auf. Sie werden anschließend im Rahmen der im nachfolgenden Abschnitt 6.4 erläuterten Fallstudien bei der Umsetzung der in dieser Arbeit vorgestellten theoretischen Konzepte verwendet.

6.3.2.1 Skalierbares Identity Management

In den vergangenen Jahren sind in der Wissenschaft und Wirtschaft viele Projekte zur Verwaltung von Identitäten gestartet worden. Diese Projekte bezogen sich im Kern zumeist auf die Einführung von Meta- und Virtual Directories oder zentralen Verzeichnisdiensten, wie sie in Abschnitt 3.2.2 beschrieben wurden. Zusammen mit „Single Sign-On"-Lösungen und Autorisierungsverfahren, z.B. der Implementierung von Rollen, werden die Projekte im Bereich Identity Management zusammengefasst. Allerdings umfassten die Projekte nicht nur die Verwaltung von Identitäten, sondern allgemein den Abgleich verschiedener Informationen im Unternehmen. Unterschiedliche Datenquellen und -senken sollen so integriert oder synchronisiert werden.

Viele große Projekte im Umfeld des Identity Management (kurz: IDM) sind in den letzten Jahres gescheitert.[726] Es liegt die Vermutung nahe, dass dies nicht zuletzt durch die hohe Komplexität der Lösungen bedingt ist.[727] Diese wird zusätzlich durch die häufig angestrebte vollständige Integration aller Systeme von Beginn des Projekts an verstärkt.

Durch die pragmatische Umsetzung von „Identity Management"-Projekten, wobei zunächst bewusst nur wenige ausgewählte Systeme angebunden werden, lässt sich der Aufwand minimieren. Dieses Vorgehen wird im Folgenden als skalierbares Identity Management beschrieben. Ein weiterer Vorteil dieser Herangehensweise besteht darin, im Vorlauf des Projekts bei der Integration zusätzlicher Systeme anhand der gewonnenen Erfahrungen abzuwägen, ob eine Reduktion des Systems mittel- bis langfristig effektiver ist als die Integration. Datenquellen, die zu Beginn des „Identity Management"-Projekts noch als essentiell angesehen wurden, werden so im weiteren Verlauf durch bereits integrierte vollständig ersetzt. Bei der Abwägung bietet sich zudem die Integration unterschiedlicher „Identity Management"-Lösungen an. Häufig zentrierten sich IDM-Projekte auf genau eine Implementierungsform (z.B. Meta-Directory oder Virtual Directory).[728] Es kann jedoch

---

[726] Vgl. KUPPINGER, M.: Das erfolgreiche Identity Management-Projekt, 2005, GRAVES, M.: Why Identity Management Projects Fail, 2006.

[727] Vgl. Aufwand für die Implementierung von Regeln in Abschnitt 3.2.2 und die Komplexität von Public-Key-Infrastrukturen in Abschnitt 3.2.4.

[728] Vgl. WINDLEY, P. J.: Digital Identity, 2005, S. 85 ff.

im Verlauf der pragmatischen Umsetzung des Projekts durchaus sinnvoll sein, ein spezielles System, das Identitäten verschiedener Quellen benötigt, über ein zusätzliches Virtual Directory zu versorgen, ohne die Identitäten in den einzelnen Systemen über ein bestehendes Meta-Directory mit zusätzlichem Aufwand bzgl. der Implementierung zu synchronisieren. Dies kann insbesondere für e-Science Umgebungen mit hoher Dezentralität oder Benutzerfluktuation sinnvoll sein, in denen nicht alle Benutzer an jedem Standort, sondern nur für gelegentliche Zugriffe einheitlich zur Verfügung stehen müssen.[729]

Bei einer skalierbaren, phasenweisen Umsetzung des Identity Management muss auch die Einbindung externer Prozesse berücksichtigt werden. Nicht nur die Authentifizierung ist relevant, sondern auch die Verfügbarkeit der Dienste in einheitlicher Form nach erfolgreicher Authentifizierung. Werden daher Benutzer über ein Identity Management zentral verwaltet und synchronisiert, müssen auch ihre Berechtigungen und Daten[730] geeignet verfügbar sein. In Bezug auf die initiale Bereitstellung[731] aller Identitäten und benötigten Dienste eines Benutzers müssen externe Prozesse transaktionssicher realisiert werden. Die Synchronisation darf erst dann erfolgreich abgeschlossen werden, wenn alle Systeme und externen Prozesse vollständig abgearbeitet wurden. Gleiches gilt für die zentrale Löschung von Identitäten.[732]

6.3.2.2 Web-basierte „Identity Management"-Portale

Hersteller von „Identity Management"-Lösungen, wie sie in Abschnitt 3.2.2 beschrieben wurden, setzen in bestehenden Produktreihen vermehrt auf Web-Portale für die Administration der Identitäten. Häufig können Benutzer neben ihrem Passwort in diesen Web-basierten IDM-Portalen auch weitere Merkmale ihrer Identität selbständig (als „Self-Service") verwalten. Die Verwaltung z.B. der Authentifizierungsmerkmale durch die Organisationen wird dabei insbesondere für deren dezentrale Administration vereinfacht, während die Verwendung und Verwaltung aufseiten der Benutzer durch den zentralen Zugriff über das Portal ebenfalls erleichtert wird.[733] Einige Hersteller beginnen zusätzlich Workflow-Komponenten z.B. für die Abwicklung von Bestellvorgängen oder die Einrichtung von Berechtigungen in ihre IDM Portale zu integrieren. Dabei stehen insbesondere

---

[729] Vgl. die Verwendung dezentraler Ressourcen in wissenschaftlichen IT-Strukturen in Abschnitt 4.2.1.

[730] Vgl. hierzu auch an die Authentifizierung angrenzende Verfahren in Abschnitt 4.3.

[731] Dies wird auch als Provisioning (Provisionierung der Identität) bezeichnet vgl. WINDLEY, P. J.: Digital Identity, 2005, S. 30.

[732] Was häufig als „Deprovisioning" (Deprovisionierung der Identität) bezeichnet wird.

[733] Beispiele für entsprechende Portale existieren in JBoss-Portal, 2007 und Novell-UserApplication, 2007.

neue Benutzer im Fokus, die Zugang zu relevanten Systemen und Arbeitsmaterialien benötigen.[734] Für die Definition von Workflows über die Grenzen des Portals hinweg, insbesondere für die Anbindung der Geschäftslogik, dienen hierbei Web-Services.[735]

Speziell für wissenschaftliche Anforderungen ergibt sich jedoch bereits bei der initialen Anmeldung am Portal ein Problem. Die Hersteller bestehender IDM-Lösungen vergeben für die initiale Anmeldung in der Regel Standard-Passwörter (z.B. den Nachnamen der Benutzer). Während diese Praxis in Unternehmen, bei denen neue Mitarbeiter in der Regel sofort ihr Benutzerkonto verwenden, akzeptabel sein kann, entsteht beispielsweise durch die Verwendung des Nachnamens als Passworts bei Studierenden und Wissenschaftlern aufgrund der Dezentralität der Benutzergruppe sowie deren hoher Fluktuation ein inakzeptables Sicherheitsrisiko. Nachnamen von Studierenden lassen sich leicht ermitteln und so die bereitgestellten Authentifizierungskonten missbrauchen. Auch die Aushändigung randomisierter Passwörter kann aufgrund der Dezentralität im e-Science-Umfeld als inakzeptabel angesehen werden, da diese den z.B. über internationale Forschungsgruppen verteilten Benutzern schwer sicher mitgeteilt werden können. Ein direkter Import bestehender Passwörter der Benutzer ist aufgrund der verschiedenen Hash-Verfahren[736] nicht möglich. Die Portale müssen daher entsprechend erweitert werden, um unterschiedliche Hash-Werte für die Prüfung des Passworts zu erlauben. Neben der Speicherung dieser Werte im Verzeichnisdienst besteht die Möglichkeit, auf der Hauptseite des Portals eine Funktion (z.B. ein Portlet[737]) zu realisieren, die eine Anmeldung gegen verschiedene bestehende Verzeichnisse, Datenbanken usw. erlaubt. Nach erfolgreicher Authentifizierung gegenüber diesen Systemen wird das eingegebene Passwort in das Portal bzw. das dahinter liegende Verzeichnis resp. IDM übernommen und der Benutzer angemeldet. Abbildung 6-8 illustriert den Ablauf einer Anmeldung an einem solchen Portlet.

---

[734] Vgl. hierzu auch Novell-UserApplication-Workflow, 2007.

[735] Vgl. SCHUMANN, M. ET AL.: Spezifikation und Abwicklung von Workflows auf Basis von Web-Services, in FRÖSCHLE, H. P.: Kosten & Nutzen von IT-Sicherheit in: HEILMANN, H. ET AL. (Hrsg.): HMD - Praxis der Wirtschaftsinformatik, Heft 234, 2003, S. 63 ff.

[736] Vgl. Abschnitt 5.5.1 f).

[737] Als dynamischer, vom Benutzer konfigurierbarer Bereich einer Web-Seite, vgl. Java JSR-168 Portlet Definition in Sun JSR-168, 2003 oder Microsoft WebParts, 2007.

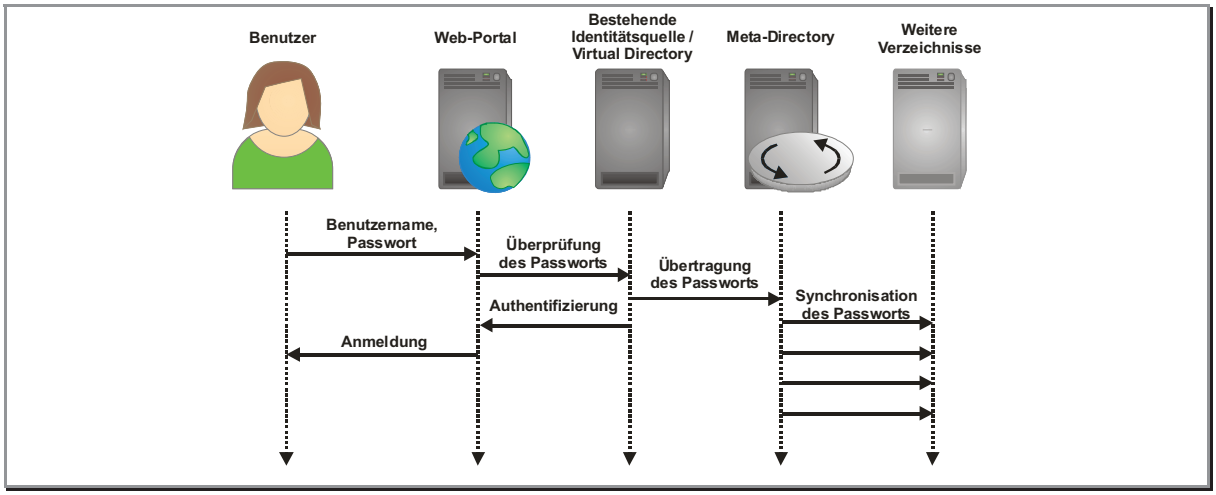

Abbildung 6-8: Portlet für die Übernahme von bestehenden Passwörtern in „Identity Management"-Portale

Weitere Portlets können für die Prüfung der Funktionalität des Benutzerkontos realisiert werden. Der Benutzer kann mit ihnen nach der Eingabe seines Passworts überprüfen, welche Systeme er verwenden kann und eventuelle Fehler, z.B. bei dem Zugriff auf Dateien, Überschreitung von Quotierungen auf Datenträgern usw. selbst diagnostizieren. Dies ermöglicht eine gezielte Unterstützung des Help-Desk-Personals bei der Lösung eventueller Probleme. Innerhalb des Portlets können dabei auch Self-Service-Funktionen für die direkte Behebung der Probleme (z.B. Beantragung von zusätzlichem Speicherplatz, Einspielen von Backups, usw.) realisiert werden.

Benutzer können so ihre Identität und zugehörige Daten im Identity Management selbständig beeinflussen. Es wird nicht fremd über ihre Identitäten bestimmt, sondern sie sind in der Lage, selbst zu bestimmen, in welche Systeme welche Informationen über sie vermittelt werden. Dies ist insbesondere für Federations[738] wichtig, in denen Benutzerkonten resp. zugehörige Informationen, dezentral über verschiedene Service Provider verteilt, verwendet werden können.

6.3.2.3 Self-Service PKI-Lösungen für e-Science

Während Zertifikate eine Lösung beispielsweise für übergreifende „Reduced Sign-On"-Lösungen darstellen, gestaltet sich die Realisierung und Verwendung von Public-Key-Infrastrukturen für Benutzer und Administratoren gleichermaßen komplex.[739] Insbesondere dezentrale und virtualisierte IT-Strukturen wie e-Science Umgebungen erfordern jedoch vielfach gerade die erhöhte Sicherheit für Authentifizierungs- und Verschlüsselungsmechanismen und somit den Einsatz von digita-

[738] Vgl. Abschnitt 3.2.7.

[739] Vgl. die Komplexität von Public-Key-Infrastrukturen in Abschnitt 3.2.4.

len Zertifikaten. Eine Lösung für die Reduzierung des durch die Komplexität erhöhten Aufwands bieten Self-Service-PKI-Lösungen für e-Science, wie sie in RIEGER ET AL. vorstellt wurden.[740]

e-Science-Umgebungen stellen in erster Linie Anforderungen durch die hohe Benutzerfluktuation und die räumliche Verteilung an bestehende PKI-Lösungen. Diesen Anforderungen kann durch folgende Erweiterungen begegnet werden:

- mobile Vergabe von Zertifikaten, z.B. vor Ort in Instituten oder auf Tagungen, ohne Wartezeit. Zertifikate mit begrenzter Gültigkeit sind hierbei sofort verfügbar.
- Eigenständige Verlängerung und Sperrung von Zertifikaten durch den Besitzer bzw. Zertifikatnehmer. Keine erneute persönliche Identifizierung - schlanker Beantragungsprozess.
- Eigenständige Beantragung von zusätzlichen Zertifikaten (z.B. für Server, neue E-Mail-Adressen etc.), ohne erneute persönliche Identifizierung bei der Zertifizierungsstelle.
- Etablierung von Registrierungsstellen in den Instituten, schnelle Vergabe von Zertifikaten bzw. Identifizierung neuer Zertifikatnehmer vor Ort.

Des Weiteren lässt sich eine allgemeine Steigerung der Benutzbarkeit (Usability) von e-Science-PKI-Lösungen erzielen durch:

- Optionale Verteilung der Zertifikate inkl. privaten Schlüssels, um Fehler bei der Verknüpfung von privatem Schlüssel und Zertifikat zu vermeiden und den Beantragungsvorgang zu vereinfachen.
- Optionale Archivierung der an die Zertifikatnehmer ausgehändigten privaten Schlüssel, um den Schaden bei versehentlicher Löschung des privaten Schlüssels zu reduzieren.

Abbildung 6-9 illustriert den Ablauf einer Verlängerung bzw. Beantragung weiterer Zertifikate für die Benutzer anhand einer bestehenden digitalen Signatur ohne erneute persönliche Identifizierung. Hierfür können bestehende Signatur-Lösungen in gängigen Web-Browsern verwendet werden, um die Zertifikate z.B. in „Identity Management"-Web-Portalen zu beziehen.[741] Neben der Verwaltung der Zertifikate sowie der Beantragung neuer Zertifikate für weitere Organisationen oder Verwendungszwecke ist auch deren Sperrung über zentrale Web-Portale möglich.

---

[740] Vgl. RIEGER, S. ET AL.: Self-Service PKI-Lösungen für eScience, in Paulsen, C. (Hrsg.): Sicherheit in vernetzten Systemen. 13. Workshop, 2006, S. B-1 ff.

[741] Vgl. hierzu auch RIEGER, S. ET AL.: Self-Service PKI-Lösungen für eScience, in Paulsen, C. (Hrsg.): Sicherheit in vernetzten Systemen. 13. Workshop, 2006, S. B-1 ff.

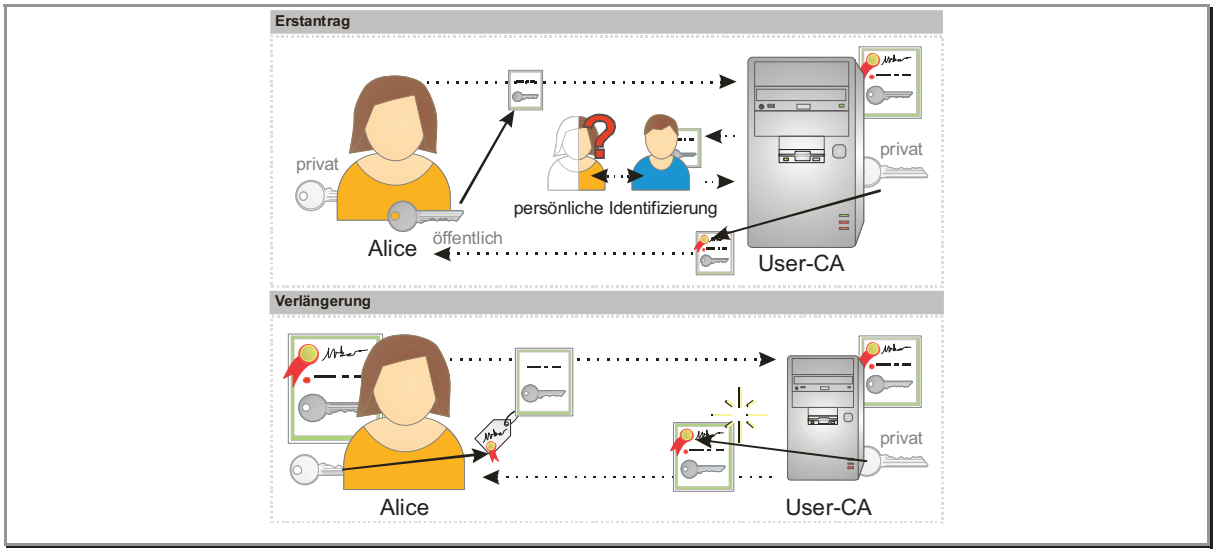

Abbildung 6-9: Verlängerung und Beantragung neuer Zertifikate im Self-Service anhand digitaler Signaturen

6.3.2.4 Integration Federation-basierter Authentifizierung in Desktop-Anwendungen

Im vorherigen Abschnitt wurde bereits die erweiterte Fokussierung auf den Benutzer beschrieben. Häufige Anforderung der Benutzer neben der einfachen Verwaltung ihrer Identitäten ist insbesondere die Vereinfachung der Verwendung der Authentifizierung resp. Single Sign-On.[742] Als bestehende Lösung für Desktop-Anwendungen bietet sich hierfür, wie in Abschnitt 3.2.3 beschrieben, nur Kerberos an, das Single Sign-On z.B. in „Microsoft Active Directory"-Umgebungen und Unix-Umgebungen bietet. Jedoch unterstützen nicht alle Anwendungen den Kerberos-Standard, so dass in heterogenen Umgebungen unterschiedliche Authentifizierungsverfahren[743] verwendet werden. Zudem ist auch Kerberos nicht für alle Plattformen einsetzbar, bedingt durch proprietäre Erweiterungen.[744] Automatisierungslösungen, wie sie in Abschnitt 3.2.9 beschrieben wurden, versuchen zwar eine allgemeine Lösung für Single Sign-On zu finden, schränken dabei jedoch die erzielte Sicherheit ein.

Für das World Wide Web existieren bereits effektivere „Single Sign-On"-Lösungen, wie sie in Abschnitt 3.2.7 in Form von Federation-Lösungen vorgestellt wurden. Durch deren Erweiterung für die Verwendung in Desktop-Anwendungen kann eine plattform- und herstellerunabhängige XML-

[742] Vgl. Single- bzw. Reduced Sing-On in Abschnitt 2.1.12.

[743] Vgl. Abschnitt 3.1.

[744] Vgl ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 513 f.

basierte Implementierung zukünftig eine hohe Integration erzielen.[745] Auch die Nutzung von Zertifikaten ermöglicht anhand verschiedener Vertrauensstellungen[746] sowie der Verwendung von Tokens als Speicher für unterschiedliche Zertifikate ein Single- bzw. Reduced Sign-On.[747] Während in den letzten Jahren viele Desktop-Anwendungen durch geeignete Web-Anwendungen ergänzt oder ersetzt wurden[748], können verbleibende Desktop-Applikationen analog durch Federation-Lösungen erweitert werden. Dies ermöglicht trotz der Verwendung einer zentralen „Identity Management"-Lösung innerhalb der Organisationen, als Vereinheitlichung der Verwaltung, eine dezentrale Authentifizierung und Gewährleistung der IT-Sicherheit über Organisationsgrenzen hinweg.[749] Diese Erweiterung der bestehenden Verfahren wird im Folgenden als Integration Federation-basierter Authentifizierung in Desktop-Anwendungen bezeichnet. Hierfür würde sich ein universeller TCP/IP-basierter „Reduced Sign-On"-Dienst auf dem Arbeitsplatz-Rechner anbieten, um applikations- und plattformunabhängiges Reduced Sign-On zu erlauben. Der Dienst kann direkt bei der ersten Anmeldung am Rechner über den Identity Provider der Home Organization des Benutzers initialisiert werden.[750] Über Attribute der Assertion des Identity Providers lassen sich zudem weitere Authentifizierungsmerkmale (z.B. Kerberos Tickets resp. Sitzungsschlüssel) transportieren und auf dem Client hinterlegen. Für mobile Anwendungen lässt sich der Dienst z.B. als Web-Service[751] realisieren, ohne Netzwerk-Verbindung zum Identity Provider hingegen kann er als Cache fungieren. Analog zu der Verwaltung der Identitäten im Web-Portal im vorherigen Abschnitt entscheidet der Benutzer hierbei, z.B. durch explizite Freigabe, welche Informationen an die jeweiligen Service Provider und Authentifizierungsverfahren weitergereicht werden. Damit bestimmt der Benutzer in Bezug auf die Übertragung und Speicherung der Authentifizierungsmerkmale auch die gewünschte Sicherheit.

Abbildung 6-10 zeigt eine Möglichkeit für eine entsprechende Erweiterung der Desktop-Anwendungen und Betriebssysteme um einen „Reduced Sign-On"-Dienst. Dieser Dienst besitzt dabei einen zentralen Speicher für Sitzungsschlüssel. Sofern das Sicherheitsrisiko akzeptabel ist,

---

[745] Vgl. Integrationsproblematik in SCHUMANN, M.; RAWOLLE, J.; ADE, J.: Informationen im Internet: XML als Integrationstechnologie, in Das Wirtschaftsstudium Nr. 8-9, 2002, S. 1119 f.

[746] Vgl. Vertrauen in Root-Zertifikate in Abschnitt 3.2.4.

[747] Vgl. die Verwendung von Tokens für die Speicherung unterschiedlicher Authentifizierungsmerkmale in Abschnitt 2.5.2.

[748] Vgl. BADACH, A.; RIEGER, S.; SCHMAUCH, M.: Web-Technologien, 2003, S. XV ff.

[749] Wie in HAGENHOFF, S.; GOOS, P.; SCHMALTZ, R.: Sicherheitsmodelle für Kooperationen, in: FERSTL, O. K. (Hrsg.): Wirtschaftsinformatik 2005, 2005, S. 1247 ff. gefordert.

[750] Vgl. den Ablauf der Authentifizierung bei Federation-basierten Lösungen in Abschnitt 3.2.7.

[751] Vgl. BADACH, A.; RIEGER, S.; SCHMAUCH, M.: Web-Technologien, 2003, S. 311 ff.

kann, analog zur Verfahrensweise in aktuellen Betriebssystemen (vgl. Microsoft Windows), das bei der Anmeldung eingegebene Passwort ebenfalls zwischengespeichert werden. Durch geeignete Anpassung der Desktop-Anwendungen können diese für nachfolgende Authentifizierungsverfahren zunächst geeignete bestehende Sitzungsschlüssel über den Dienst erlangen, ohne dass der Benutzer erneut eine Authentifizierung durchführen muss. Langfristig können passende Authentifizierungsmerkmale auch über Assertions und zugehörige Attribute ermittelt werden, wie sie in Abschnitt 3.2.7 beschrieben wurden.[752]

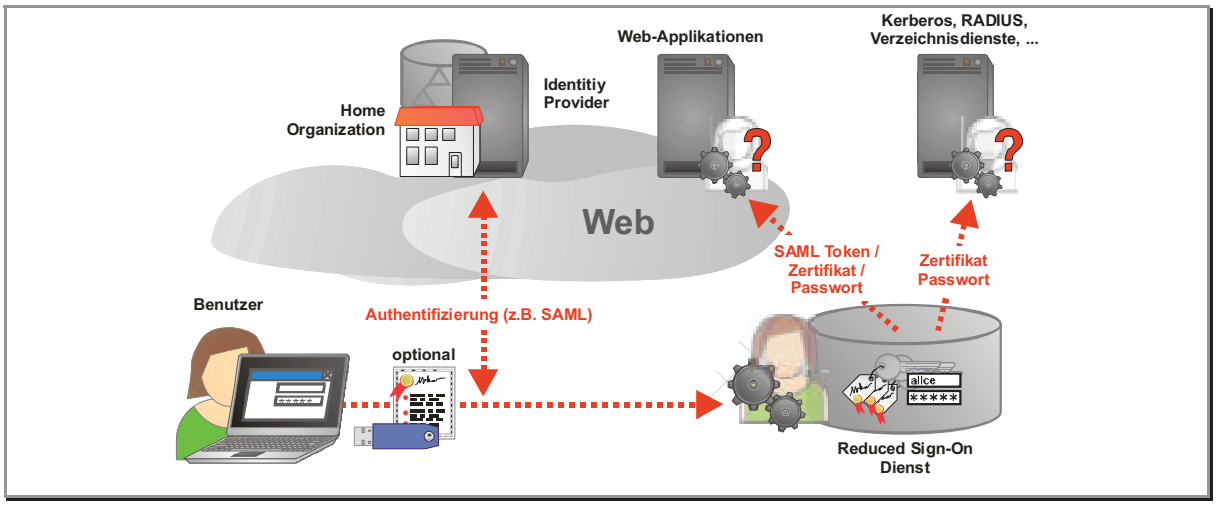

Abbildung 6-10: Erweiterung bestehender Desktop-Anwendungen um Federations und Reduced Sign-On

Um Sicherheitsrisiken beim automatisierten Austausch von Passwörtern zu umgehen, bietet sich die Ablösung von Passwörtern z.B. durch X.509-Zertifikate an.[753] Der öffentliche Schlüssel kann hierbei ohne das Risiko einer Kompromittierung an die einzelnen Authentifizierungssysteme verteilt werden. Diese können anhand der Signatur des Zertifikats dessen Authentizität überprüfen. Authentifizierungsvorgänge des Benutzers kann dieser über eine digitale Signatur mit seinem zugehörigen privaten Schlüssel durchführen.[754] Viele Authentifizierungssysteme wie Verzeichnisdienste, Kerberos oder Web-Anwendungen unterstützen bereits die Verwendung von Zertifikaten zur Authentifizierung. Werden die zugehörigen privaten Schlüssel auf einem Token gehalten, kann dieses beispielsweise einmalig zu Beginn der Sitzung über eine zugehörige PIN aktiviert werden.[755] Nachfolgende Authentifizierungsvorgänge erfolgen ohne weitere Eingabe der PIN. Auch

[752] Hierfür ist jedoch zunächst eine Erweiterung der Anwendungen um die Funktionalität eines Service Providers erforderlich.

[753] Vgl. die Verwendung von Zertifikaten in Public-Key-Infrastrukturen in Abschnitt 3.2.4.

[754] Vgl. Prüfung digitaler Signaturen in Abschnitt 2.6.2.

[755] Vgl. die Verwendung von aktiven Tokens in Abschnitt 2.5.2.

hier kann der Benutzer mehrere Zertifikate für unterschiedliche Organisationen und Verwendungszwecke auf dem Token halten und die gewünschte Sicherheit, beispielsweise durch eine erforderliche zusätzliche PIN für gewisse Schlüssel, selbst bestimmen.[756]

Allerdings wird durch die Verwendung von Tokens und deren fehlende Unterstützung z.B. in Internet-Cafés die Mobilität eingeschränkt.[757] Dies ließe sich durch eine internationale umfassende Standardisierung für den Token-Zugriff (Erweiterung bzw. Verallgemeinerung von PKCS#11 und PKCS#15) erreichen.[758] Allerdings existieren aktuell bereits verschiedene Standards, die (vgl. PKCS#11) überdies trotzdem auf den Endgräten jeweils spezielle Treiber-Software erfordern. Ein möglicher Lösungsansatz könnte daher ein Software-Token, z.B. in Form des genannten „Reduced Sign-On"-Dienstes bzw. einer Web-Anwendung sein.

6.3.2.5 Flexible Trust-Modelle

Neben den im vorherigen Abschnitt genannten Einschränkungen für die Benutzbarkeit von Public-Key-Infrastrukturen ergibt sich auch durch deren strikt hierarchisches Modell ein Nachteil in e-Science-Umgebungen. Wissenschaftliche Benutzer können unterschiedlichen Organisationen angehören und ihre Zugehörigkeit mehrfach wechseln (so werden aus Studierenden Alumni oder Tutoren bzw. Mitarbeiter). Für die Public-Key-Infrastrukturen bedeutet dies, dass Benutzer unterschiedliche Zertifikate benötigen bzw. häufig neue Zertifikate ausgestellt werden müssen. Für Grid-Umgebungen haben sich hierfür die in RIEGER ET AL. erläuterten Proxy-Zertifikate etabliert.[759] Jedoch weisen diese nur eine kurze Gültigkeit auf, sind ebenfalls an eine Organisation gebunden und reduzieren die Sicherheit durch die zusätzliche Übertragung der privaten Schlüssel. Eine Erweiterung des X.509-Standards um multiple Signaturen, ähnlich dem PGP Standard[760], kann die Zugehörigkeit zu unterschiedlichen Organisationen ermöglichen. Dies kommt auch Vertrauensstellungen in der Realität näher, die neben dem hierarchischen Vertrauen, z.B. in Ausstellungsbehörden auch ein individuelles, wechselseitiges Vertrauen direkt zwischen unterschiedlichen

---

[756] Auch eine Verwendung der in den Zertifikaten enthaltenen öffentlichen Schlüssel z.B. für Secure Shell Anwendungen (SSH) CHESWICK, W. R.; BELLOWIN, S. M., RUBIN, A. D.: Firewalls und Sicherheit im Internet. 2. Aufl., 2004, S. 92 f. ist realisierbar.

[757] Vgl. Anforderungen an mobile Anwendungen in HAGENHOFF, S.; SCHUMANN, M.: Mediaconomy - Internetökonomie der Medienwirtschaft, in IT -Information Technology Nr. 48, 2006, S. 218 ff.

[758] Vgl. PKCS#11 und PKCS#15 auf RSA: Public-Key Cryptography Standards (PKCS), 2007.

[759] Vgl. RIEGER, S. ET AL.: Self-Service PKI-Lösungen für eScience, in Paulsen, C. (Hrsg.): Sicherheit in vernetzten Systemen. 13. Workshop, 2006, S. B-1 ff.

[760] Vgl. ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 758 ff.

Benutzern, erlaubt. Derzeit wird dies nur von Cross-Zertifizierungen nach X.509 unterstützt.[761] Eine Erweiterung des Standards erlaubt ein flexibles Signaturfeld mit Signaturen unterschiedlicher Aussteller innerhalb der Zertifikate bzw. einer XML-Struktur, das als Ergänzung von den Benutzern übermittelt werden kann.

Auch bei Federation-basierten Lösungen, deren Vertrauensverhältnis zwischen Service- und Identity Provider über Zertifikate bestimmt wird, könnten so beispielsweise Benutzern unterschiedliche Identity Provider zugeordnet werden.[762] Es wird ebenfalls eine Erweiterung um kurzfristige Förderationen denkbar, in denen multilaterale Beziehungen zwischen verschiedenen Föderationen oder Institutionen erlaubt werden. Diese könnten auch von den Benutzern über die in Abschnitt 6.3.2.2 genannten „Identity Management"-Portale selbständig beantragt und verwaltet werden. Hierfür wäre die Definition maschinell interpretierbarer Zertifizierungsrichtlinien, z.B. basierend auf XML, erforderlich, um beispielsweise den Benutzern einer Föderation über das Portal multilaterale Inter-Föderations-Beziehungen mit gleichem Sicherheitsniveau in Bezug auf die Vergabe der Zertifikate zu erlauben.

6.3.3 Ebenenmodell für einheitliche Authentifizierung

Im Abschnitt 6.3.2 wurden Erweiterungen bestehender Verfahren vorgestellt, die eine Minimierung des Aufwands sowie Erhöhung der erzielten Sicherheit durch einheitliche Authentifizierung ermöglichen. Dabei wurden die Bedürfnisse des Benutzers in den Mittelpunkt gestellt. Im Folgenden wird ein Modell vorgestellt, das als Basis für den Kompromiss zwischen Aufwand und Sicherheit in heterogenen IT-Strukturen verwendet werden kann und die in Abschnitt 6.1 genannten Anforderungen adressiert. Es orientiert sich an den Anforderungen der Benutzer, den Aufwand möglichst gering zu halten, sowie an der Sicht der Organisationen, die eine möglichst hohe Sicherheit erzielen wollen.

Authentifizierungsmerkmale existieren nicht nur in heterogenen IT-Strukturen, sie bestimmen viele alltägliche Bereiche, in denen eine Handlung eindeutig einer Identität zugeordnet werden soll.[763] Die Authentifizierung erfolgt außerhalb der IT-Strukturen z.B. durch Kreditkarten, PINs, Codes, Ausweise oder auch den Besitz eines herkömmlichen Schlüssels. Ihr Zweck ist die Absicherung

---

[761] Vgl. ADAMS, C.; LLOYD, S.: Understanding PKI, 2003, S. 28 ff., 273 ff.

[762] Vgl. die starre Zuweisung von Identity Providern zu einer Heimatorganisation in Abschnitt 3.2.7.

[763] Herkömmliche Schlüssel dienen z.B. gleichzeitig für die Autorisierung und Authentifizierung, vgl. hierzu Abschnitt 4.3.1.

einer nachfolgenden Autorisierung über eine eindeutige Zurechnung.[764] Dabei haben sich im Laufe der Jahre für die Verwendung dieser Authentifizierungsmerkmale Standards etabliert, die eine Vereinheitlichung bzw. Minderung des Aufwands bei Gewährleistung oder Steigerung der Sicherheit erlauben. Beispielsweise wird für die Authentifizierung einer natürlichen Person in Europa einheitlich der Personalausweis akzeptiert. Für spezielle Anforderungen gibt es zusätzliche Merkmale wie etwa den Reispass oder Führerschein, die die Funktion eines Ausweises besitzen, jedoch andere Informationen beglaubigen. Teilweise lassen sich diese auch alternativ verwenden (z.B. der Führerschein als Ersatz für den Personalausweis). In Bezug auf den Gültigkeitsbereich des jeweiligen Nachweises lassen sich die Bereiche als Ebenen z.B. mit unterschiedlich gewährleistetem bzw. erforderlichem Sicherheitsniveau beschreiben.

Während Ausweise in der Regel durch Institutionen vergeben werden, lassen sich ähnliche Vereinheitlichungen von Authentifizierungsmerkmalen, initiiert durch die Benutzer, im Alltag ermitteln. Die Verwendung von gleichen Schlüsseln für unterschiedliche Schlösser bzw. Generalschlüssel stellt ein Beispiel dar, das den Aufwand der Verwendung von Authentifizierung und Autorisierung minimiert. Dabei wird das erhöhte Risiko im Falle eines Verlusts des Schlüssels als Kompromiss zwischen Aufwand und Sicherheit in Kauf genommen. Auch hier sorgen separate zusätzliche Schlüssel für unterschiedliche Sicherheitsniveaus bzw. Ebenen.

Die Verwendung ein und desselben Ausweises oder Schlüssels für unterschiedliche Zwecke ist somit in der Realität nicht ungewöhnlich. Soll die damit verbundene Minderung der Sicherheit kompensiert werden, werden zusätzliche Schlösser oder neue Ausweise etabliert.

[764] Vgl. hierzu die Autorisierung als an die Authentifizierung angrenzendes Verfahren in Abschnitt 4.3.1.

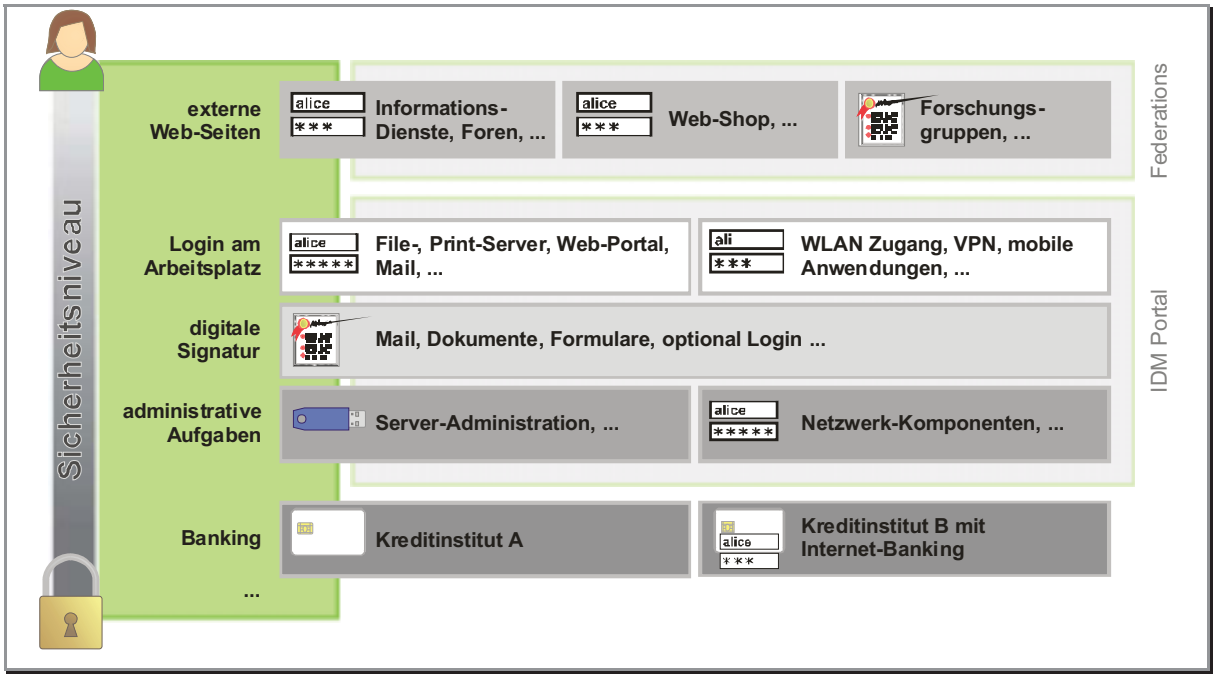

Abbildung 6-11: Beispiel für einheitliche Authentifizierung auf unterschiedlichen Sicherheitsebenen

Abbildung 6-11 zeigt die Realisierung unterschiedlicher Sicherheitsebenen bzw. die Verwendung gleicher Merkmale für unterschiedliche Anwendungen. So kann z.B. ein einfaches Passwort für Informationsdienste im World Wide Web verwendet werden, ein weiteres für Web-Shops.[765] Um dem Problem der Homogenität von Passwörtern insb. bei externer Speicherung[766] entgegenzuwirken, bietet sich der Einsatz von Zertifikaten oder Federation-basierter Lösungen an, bei denen die Authentifizierung ausschließlich über die Home Organization des Benutzers erfolgt. [767]Die Erweiterung der Federations oder selbständige Verwaltung durch die Benutzer wurde in den Abschnitten 6.3.2.4 und 6.3.2.5 bereits beschrieben.

Dabei muss optional auch eine Verwendung unterschiedlicher Authentifizierungsmerkmale durch die Benutzer auf einer Ebene erlaubt werden. Dies bedeutet z.B. für die Realisierung von Meta-Directories, dass Passwörter nicht generell an jedes angeschlossene System verteilt werden. Getrennte Merkmale für die angeschlossenen Systeme können z.B. vom Benutzer innerhalb von IDM Portalen[768] verwaltet werden. So bietet es sich für die Benutzer an, für die mobile Verwendung von

---

[765] Die Homogenisierung unterschiedlicher Passwörter auf einer niedrigen Sicherheitsebene wird auch in CHESWICK, W. R.; BELLOWIN, S. M., RUBIN, A. D.: Firewalls und Sicherheit im Internet. 2. Aufl., 2004, S. 182 vorgeschlagen.

[766] Vgl. den Missbrauch durch Administratoren externer Organisationen in Abschnitt 4.4.1

[767] Vgl. Home Organization resp. Heimatorganisation in Abschnitt 3.2.7.

[768] Vgl. Abschnitt 6.3.2.2.

Diensten seiner Organisation von außerhalb, z.B. für den Zugang zu Web-Anwendungen oder virtuellen privaten Netzwerken (VPNs), unterschiedliche Merkmale, ggf. auch mit höherem Sicherheitsniveau, zu verwenden. Sofern für alle erforderlichen Dienste Zertifikate als Authentifizierungsmerkmal eingesetzt und mehrere Zertifikate, z.B. auf Tokens verwendet werden können[769], wird durch den Verzicht auf Passwörter diese Trennung zunehmend weniger erforderlich.

Risiko und Kosten, wie sie in Abschnitt 6.1.1 betrachtet wurden, werden getrennt für die einzelnen Ebenen betrachten. Auf jeder Ebene wird innerhalb einzelner Blöcke, wie in Abbildung 6-11 illustriert, ein Single-Password bzw. soweit möglich basierend darauf Reduced Sign-On realisiert. Dabei werden in der Abbildung externe Web-Seiten, z.B. über Federations vereinheitlicht. Alle betrieblich genutzten Ressourcen werden von einem zentralen IDM Portal erfasst. Vollständiges Single Sign-On über alle Ebenen ist nicht realistisch, da dies ein einheitliches Sicherheitsniveau bedingen würde. Beispielsweise wird ein Tresor-Schlüssel in der Realität kaum gleichzeitig als Autoschlüssel dienen sollen bzw. ein Benutzer aus eigenem Interesse für den Zugang zu seinem Bankkonto ein anderes Passwort als für einen gemeinsam mit anderen Personen verwendeten PC verwenden.

Vorrangig sollte daher die Vereinheitlichung der Form der Merkmale, z.B. auf Zertifikate bzw. der Authentifizierungsverfahren angestrebt werden. Unterschiedliche Zertifikate (unterschiedlicher Zertifizierungsstellen) resp. zugehörige private Schlüssel können dann einheitlich z.B. in Form von Tokens verwaltet werden.

Die in Abbildung 6-11 gezeigte Differenzierung der Ebenen resp. Sicherheitsniveaus in Anwendungsbereiche kann analog auch auf unterschiedliche Netzwerkbereiche etc. verteilt werden.

6.3.4 Integrationsstrategie für einheitliche Authentifizierung

In Abschnitt 6.3.2.1 wurden bereits Ansätze für ein skalierbares Identity Management genannt. Für die konkrete Umsetzung eines skalierbaren „Identity Management"-Projekts in heterogenen IT-Strukturen stellt dieser Abschnitt ein Phasenmodell als Integrationsstrategie vor. Wie bereits in Abschnitt 6.3.2.1 erläutert, bietet sich eine stufenweise Migration der zu vereinheitlichenden Authentifizierungsmerkmale, -verfahren und -systeme an. Klassische „Identity Management"-Projekte, die in der Regel die Vereinheitlichung von Authentifizierungsmerkmalen und -systemen fokussieren, werden dagegen häufig in einem großen finalen Schritt migriert. Dies wird auch als „Big Bang" Strategie bezeichnet.[770] Die Ablösung sämtlicher Authentifizierungssysteme und damit

[769] Vgl. Verwendung mehrerer Zertifikate auf aktiven Tokens in Abschnitt 2.5.2.

[770] Vgl. ERDLE, C.: Legacy Migrationsstrategien, 2005.

verbundener Merkmale ist auf diese Weise wesentlich komplexer bzw. weitaus schlechter planbar.[771]

Für die Realisierung der Vereinheitlichung in der vorliegenden Arbeit werden daher die in Abbildung 6-12 gezeigten Integrationsschritte bzw. Phasen verwendet:

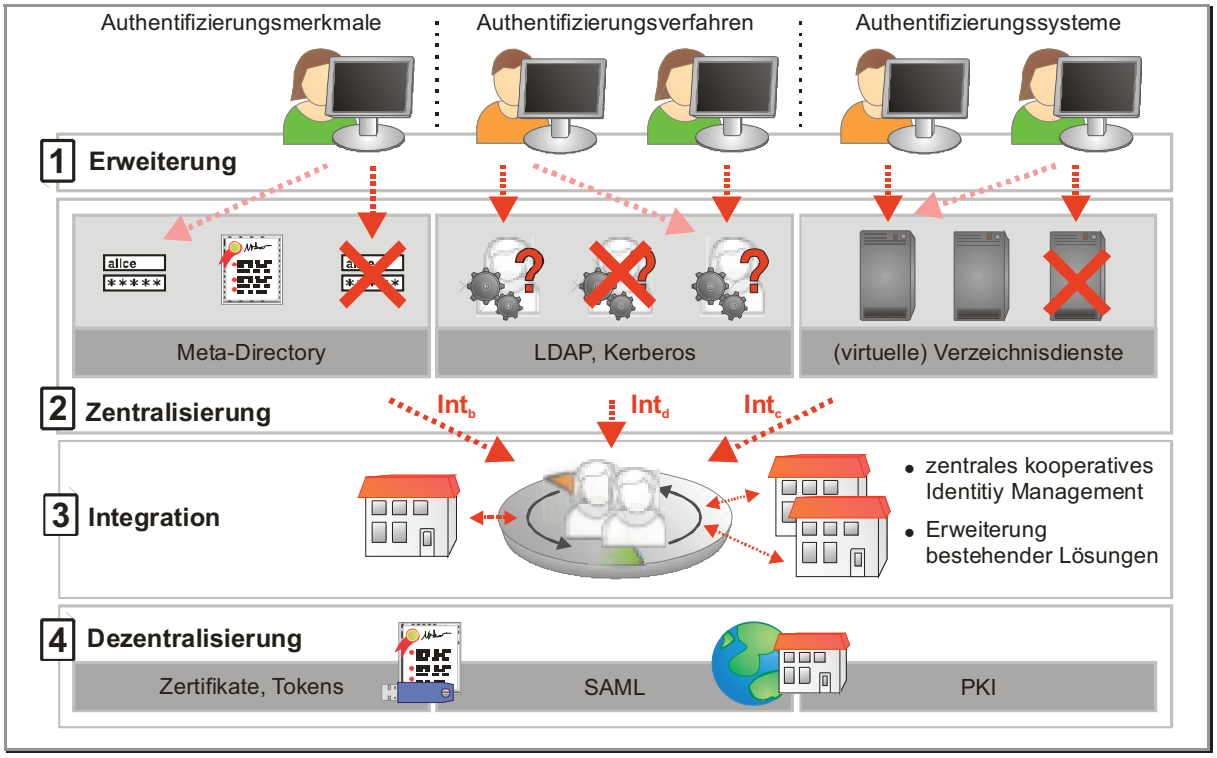

Abbildung 6-12: Phasenweise Vereinheitlichung der Authentifizierung in heterogenen IT-Strukturen

1. Die erste Phase beschreibt die Erweiterung bestehender Clients um zusätzliche Authentifizierungsverfahren, -merkmale und -systeme. Beispielweise können in dieser Phase die in Abschnitt 3.2.8 vorgestellten modularen Authentifizierungsclients und Proxies verwendet werden. Obwohl die Diversität durch die Verwaltung der unterschiedlichen Verfahren für die Clients zunächst ansteigt, kann durch die Erweiterung im Anschluss eine weiche Migration zu zentralen Authentifizierungssystemen erfolgen. Clients werden zunächst auf die Verwendung unterschiedlicher Authentifizierungssysteme umgestellt, von denen dann eines als späteres zentrales System ausgewählt wird. Auf diese Weise können Benutzer unterschiedlicher Authentifizierungssysteme die Ressource verwenden. Zusätzlich können zunächst unterschiedliche Authentifizierungsverfahren für den Zugang angeboten werden.

[771] Vgl. ERDLE, C.: Legacy Migrationsstrategien, 2005.

2. Im zweiten Schritt werden die Authentifizierungsmerkmale, -verfahren und -systeme zentralisiert. Ziel ist dabei eine Reduktion der Elemente. Beispielsweise kann ein zentrales Authentifizierungssystem für unterschiedliche Ressourcen ausgewählt werden. Für Authentifizierungsmerkmale bietet sich, wie in Abschnitt 6.3.1 erläutert, die Synchronisation über ein Meta-Directory an.[772] Mehrere Authentifizierungsmerkmale (z.B. Passwörter) werden durch das Meta-Directory synchronisiert und zentral anhand des virtuellen Merkmals im Meta-Directory verwaltet. Dies führt zu einer Integration nach Int_b.[773]

   Authentifizierungsverfahren können gemäß Abschnitt 6.3.1 durch LDAP und Kerberos integriert werden.[774] Hierbei wird die Authentifizierung an bestehenden Applikationen auf die Verwendung von LDAP umgestellt. Andere, z.B. lokale oder separate Authentifizierungsverfahren der Applikationen bzw. Authentifizierungssysteme, werden hierbei zur Minderung des Aufwands deaktiviert, was einer Integration nach Int_d entspricht.

   Durch Zentralisierung der Authentifizierungssysteme lässt sich ein hohes Maß an Vereinheitlichung erreichen. Bereits seit mehreren Jahren dienen hier zentrale Verzeichnisdienste auf unterschiedlichen Plattformen für die integrierte Authentifizierung. Für dezentrale Lösungen bieten sich vermehrt Erweiterungen wie z.B. virtuelle Verzeichnisdienste an.[775] Ressourcen, die separate Authentifizierungssysteme erfordern, werden, sofern dies keine Sicherheitsminderung bedeutet, außer Betrieb genommen bzw. durch Alternativen ersetzt. Dies entspricht einer Integration nach Int_c. Somit sinkt der Aufwand für die Verwaltung.

   Die Abwägung der Optimalität der Zentralisierung bzw. Integration der Merkmale, Verfahren und Systeme erfolgt anhand der in Abschnitt 6.2.3 eingeführten Zielfunktion. Dabei wird neben der Minimierung des Aufwands auch die Gewährleistung der durch die Authentifizierung erzielten Sicherheit angestrebt.

3. Nach der Zentralisierung der Authentifizierungselemente in einer Organisation erfolgt deren Integration in einem zentralen Identity Management. Dieses Identity Management kann z.B. auf einem zentralen Meta- oder Virtual Directory basieren, das unterschiedliche Authentifizierungsmerkmale und -verfahren unterstützt. Diese Komponente dient hierbei als Drehscheibe für die Authentifizierungsinformationen unterschiedlicher Applikationen. Sie ist zugleich

---

[772] Vgl. Synchronisation von Informationen über ein Meta-Directory in Abschnitt 3.2.2.

[773] Vgl. die Integration der Authentifizierungsmerkmale aufseiten der Benutzer und Organisationen in Abschnitt 5.2.

[774] Vgl. Verwendung von LDAP als Authentifizierungsverfahren in Abschnitt 3.2.2 und Kerberos in Abschnitt 3.2.3.

[775] Vgl. Virtual Directories in Abschnitt 3.2.2.

Schnittstelle für die Integration zusätzlicher Organisationen. So können die Identitäten unterschiedlicher Organisationen synchronisiert werden, um z.B. den gemeinsamen Betrieb von Applikationen für unterschiedliche Benutzergruppen zu erlauben. Hierbei können die einzelnen Organisationen jeweils ein eigenständiges Identity Management betreiben und selbst definieren, welche Informationen durch Partner-Organisationen verwendet werden dürfen. Hierfür bietet sich auch die in Abschnitt 6.3.2.2 beschriebene Erweiterung um Web-basierte „Identity Management"-Portale an.

4. Während die Zentralisierung und Integration der Authentifizierung in den Phasen 2 und 3 insbesondere für die Organisationen eine Minimierung des Aufwands erlaubt, wird die Flexibilität der Verwendung hierbei durch die Fokussierung auf zentrale Komponenten stark eingeschränkt. Somit kann der Aufwand für die Verwendung insbesondere seitens der Benutzer gleich bleiben. Ein Single Sign-On bietet beispielsweise nur die in Abschnitt 6.3.1 empfohlene Ausrichtung auf den Kerberos Standard, der jedoch nicht von allen Anwendungen unterstützt wird. Um die dezentrale Verwendung der Identitäten einer Organisation unabhängig vom zentralen Identity Management zu erlauben, erfolgt in der vierten Phase die Erweiterung um dezentrale Verfahren. So kann im Idealfall eine Public-Key-Infrastruktur[776] als einheitliches Rückrat für die Authentifizierung etabliert werden, die durch digitale Signaturen bzw. Zertifikate auch eine dezentrale Authentifizierung unabhängig vom zentralen Identity Management System erlaubt. Benutzer können unterschiedliche Zertifikate für mehrere Organisationen und Verwendungszwecke sowie Passwörter auf Tokens[777] für eine sichere, auf zwei Faktoren basierende Authentifizierung verwenden. Die Sicherheit der Authentifizierungsmerkmale wird durch den Einsatz von Zertifikaten bzw. die Aufteilung in privaten und öffentlichen Schlüssel im Vergleich zu Passwörtern deutlich gesteigert, während die Verwaltung durch die freie Verteilung des öffentlichen Schlüssels erleichtert wird. Die Minderung des erhöhten Aufwands durch die Verwendung von Zertifikaten und Public-Key-Infrastrukturen wurde in Abschnitt 6.3.2.3 vorgestellt.

   Federation-Lösungen bieten zusätzlich die dezentrale und einmalige Authentifizierung (resp. Single Sign-On) für unterschiedliche Organisationen und Applikationen; sie wurden in Abschnitt 3.2.7 erläutert. Die zusätzliche Erweiterung des Identity Managements um Federation-Lösungen für Desktop-Anwendungen wurde in Abschnitt 6.3.2.4 beschrieben. Durch die Er-

[776] Vgl. Aufbau von Public-Key-Infrastrukturen in Abschnitt 3.2.4.

[777] Vgl. Beschreibung von Tokens in Abschnitt 2.5.2.

weiterung wird eine zentrale Verwaltung der Identitäten unabhängig von deren dezentraler Verwendung über unterschiedliche Organisationen hinweg ermöglicht.[778]

Auch bei der Auswahl dezentraler Authentifizierungsmerkmale, -verfahren und -systeme bietet sich die Bewertung anhand der in Abschnitt 6.2 definierten Methodik in Bezug auf Relationen und Elemente gemäß des in Kapitel 5 eingeführten theoretischen Modells an. Durch die Bewertung kann analog zur Zentralisierung in Phase 2 die Optimalität der erzielten Vereinheitlichung in Bezug auf Aufwand und erzielte Sicherheit ermittelt werden.

6.4 Fallstudien im Kooperationsprojekt GÖ*

Im Rahmen dieser Arbeit wurden Fallstudien innerhalb des GÖ*-Projekts[779] durchgeführt. Zentraler Inhalt von GÖ* ist das integrierte Informationsmanagement im heterogenen e-Science Umfeld. Beteiligte des GÖ*-Projekts sind die Georg-August-Universität Göttingen, die Max-Planck-Gesellschaft sowie vier IT-Dienstleister des Wissenschaftsstandorts Göttingen. Zu diesen IT-Dienstleistern gehören der Geschäftsbereich 3-7 IT (GB 3-7 IT) des Bereichs Humanmedizin der Universität Göttingen der klinische Anwendungen für das Universitäts-Klinikum bereitstellt, die Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG) als Rechenzentrum für die Max-Planck-Gesellschaft und die Universität Göttingen, die Datenverarbeitung der Niedersächsischen Staats- und Universitätsbibliothek Göttingen sowie die Datenverarbeitung der Universität Göttingen.

Über den Wissenschaftsstandort Göttingen erstreckt sich eine heterogene IT-Struktur, die somit eine ideale Basis für die in dieser Arbeit vorgestellten Vereinheitlichungsansätze darstellt. Unterschiedliche Applikationen, Plattformen und Benutzergruppen mit verschiedenen Sicherheitsanforderungen (z.B. im wissenschaftlichen oder patientenbezogenen Umfeld des Universitätsklinikums) stellen eine Vielzahl von Authentifizierungssystemen und -verfahren für die Verwendung der Ressourcen am Standort. Applikationen und Ressourcen, die im Zuge der Kooperation gemeinsam von unterschiedlichen Organisationen und Benutzergruppen verwendbar sein sollen, benötigen in diesem Umfeld eine einheitliche Authentifizierung. Darüber hinaus sind für ein integriertes Informati-

---

[778] Vgl. Anforderungen in HAGENHOFF, S.; GOOS, P.; SCHMALTZ, R.: Sicherheitsmodelle für Kooperationen, in: FERSTL, O. K. (Hrsg.): Wirtschaftsinformatik 2005, 2005, S. 1247 ff.

[779] Vgl. KOKE, H. (Hrsg.): GÖ* - Integriertes Informationsmanagement im heterogenen eScience-Umfeld: GÖ*-Vorantrag für die DFG-Förderinitiative „Leistungszentren für Forschungsinformation“, 2004 und KOKE, H. (Hrsg.): GÖ* - Integriertes Informationsmanagement im heterogenen eScience-Umfeld: GÖ*-Hauptantrag für die DFG-Förderinitiative „Leistungszentren für Forschungsinformation“, 2004.

onsmanagement weitere Lösungen, z.B. gemeinsame SAN-Strukturen oder ein gemeinsames System-Management erforderlich.[780]

Im Verlauf des Projekts wurden Ergebnisse dieser Arbeit im technischen Teilvorhaben „Einheitliche Authentifizierung" erarbeitet, evaluiert und umgesetzt.[781] Zusätzlich konnten Ergebnisse für die Durchführung des kundenspezifischen Vorhabens GÖ*-Portal gemäß den in 6.3.2.2 skizzierten Web-Portal-Lösungen realisiert werden.[782]

Die Anforderungen an die Vereinheitlichung gehen hierbei auch über die Grenzen Göttingens hinaus. Beispielsweise erfordert ein standortübergreifendes E-Learning die Authentifizierung an landesweiten Lernmanagementsystemen oder den Zugriff auf Material externer Verlage. Innerhalb der Max-Planck-Gesellschaft mit ihren 80 Forschungsinstituten werden für zentrale web-basierte Benutzer-Portale zusätzlich Landesgrenzen überschritten. Die entstehenden Anforderungen an einheitliche Authentifizierung wurden im Verlauf dieser Arbeit auch mit externen Arbeitskreisen wie dem „Landesarbeitskreis Niedersachsen für Informationstechnik" (LANIT)[783] innerhalb der Arbeitgruppe IDM sowie dem „E-Learning Academic Network Niedersachsen" (ELAN)[784] mitgestaltet. Ergebnisse dieser Arbeit sind hierbei in die Konzeption und Einführung einer niedersachsenweiten Federation-Lösung als Niedersächsische Authentifizierungs- und Autorisierungs-Infrastruktur (NDS-AAI) eingeflossen.

Auch aus der Teilnahme am Arbeitskreis IDM der „Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung e.V." (ZKI)[785] sowie der Arbeitsgruppe Portale der Deutschen Initiative für Netzwerkinformation e.V. (DINI)[786] bestätigt sich die allgemeine Forderung nach Identity Management für e-Science-Umgebungen, das den Aufwand für Verwaltung und Verwendung der Identitäten reduziert und die Sicherheit gleichermaßen steigert.

---

[780] Diese werden in KOKE, H. (Hrsg.): GÖ* - Integriertes Informationsmanagement im heterogenen eScience Umfeld: GÖ*-Hauptantrag für die DFG-Förderinitiative „Leistungszentren für Forschungsinformation", 2004, S. 106 ff. detailliert beschrieben.

[781] Vgl. KOKE, H. (Hrsg.): GÖ* - Integriertes Informationsmanagement im heterogenen eScience Umfeld: GÖ*-Hauptantrag für die DFG-Förderinitiative „Leistungszentren für Forschungsinformation", 2004, S. 107 ff.; KOKE, H.: HRK-Guidelines for Strategies to the Information and Communication Structure at Universities, in LILLEMAA, T. (Hrsg.): Proceedings of the 12th International Conference of European University Information Systems, 2006.

[782] Vgl. hierzu auch das GÖ*-Portal in KOKE, H. (Hrsg.): GÖ* - Integriertes Informationsmanagement im heterogenen eScience Umfeld: GÖ*-Hauptantrag für die DFG-Förderinitiative „Leistungszentren für Forschungsinformation", 2004, S. 67 ff.

[783] Vgl. LANIT, 2007.

[784] Vgl. ELAN, 2007.

[785] Vfg. ZKI, 2007.

[786] Vgl. DINI, 2007.

In den folgenden zwei Abschnitten werden zwei Projekte, die als Fallstudien sowohl Ergebnisse für diese Dissertation geliefert haben als auch basierend auf Ergebnissen dieser Arbeit realisiert wurden, vorgestellt.

6.4.1 Identity Management am Wissenschaftsstandort Göttingen

Am Standort Göttingen existieren aufgrund seiner heterogenen IT-Landschaft und der Vielzahl wissenschaftlicher IT-Dienstleister viele separate Verzeichnisse für die Verwaltung von Benutzerkonten bzw. Identitäten. Für die Integration und Synchronisation dieser Identitäten (als Bestandteil des Identity Managements) wird eine Meta-Directory-Lösung eingesetzt. Synchronisiert werden unterschiedliche Active Directory Forests, OpenLDAP Systeme, Datenbanken sowie extern angebundene Prozesse. Externe Prozesse umfassen hierbei beispielsweise das Anlegen von Benutzer-Verzeichnissen bei Vergabe neuer Identitäten, die Archivierung beim Entfernen sowie die Verwaltung zugehöriger E-Mail-Konten.

Insgesamt werden 68.469 Identitäten aus 16 Systemen synchronisiert.[787] Führende Identitätsquelle für Studierende ist das HIS-System der Universität Göttingen. Identitäten der Mitarbeiter werden zukünftig aus dem SAP-System der Universität in angebundene Identitätssenken synchronisiert. Die Synchronisation umfasst hierbei neben der selektiven Replikation der Identitäten insbesondere Konvertierung und Adaption der zugehörigen Informationen zwischen den unterschiedlichen Quell- und Ziel-Systemen. Auch Kontext-Informationen wie Transaktionsnummern (TAN) werden vom Meta-Directory zwischen unterschiedlichen Applikationen übermittelt.

Die Abbildung 6-13 zeigt ein Beispiel für die Synchronisation der Identitäten am Wissenschaftsstandort Göttingen. In der Abbildung wird eine Identität in einem Active Directory Forest des Geschäftsbereichs 3-7 (GB 3-7 IT) des Universitäts-Klinikums erzeugt und über das gemeinsam im GÖ*-Projekt betriebene Meta-Directory selektiv synchronisiert. Hierbei wird für den neuen Benutzer, sofern freigeschaltet, z.B. ein E-Mail-Konto im Exchange System der GWDG (getrennte eigenständige Active Directory Forests) angelegt oder der Benutzer innerhalb des GB 3-7 IT provisioniert bzw. in weiteren Systemen angelegt. Hierfür wurde eine transaktionsorientierte Verarbeitung externer Prozesse entwickelt. So können beispielsweise erst nach erfolgreicher Archivierung der Daten aus allen Systemen Identitäten gelöscht werden. Sperrattribute und die Definition von separaten Identitäts-Containern für den Austausch ermöglichen zusätzlich die selektive Synchronisation, ohne eine Zentralisierung der Daten innerhalb des Meta-Directorys zu erfordern.

[787] Stand: 19.12.2006.

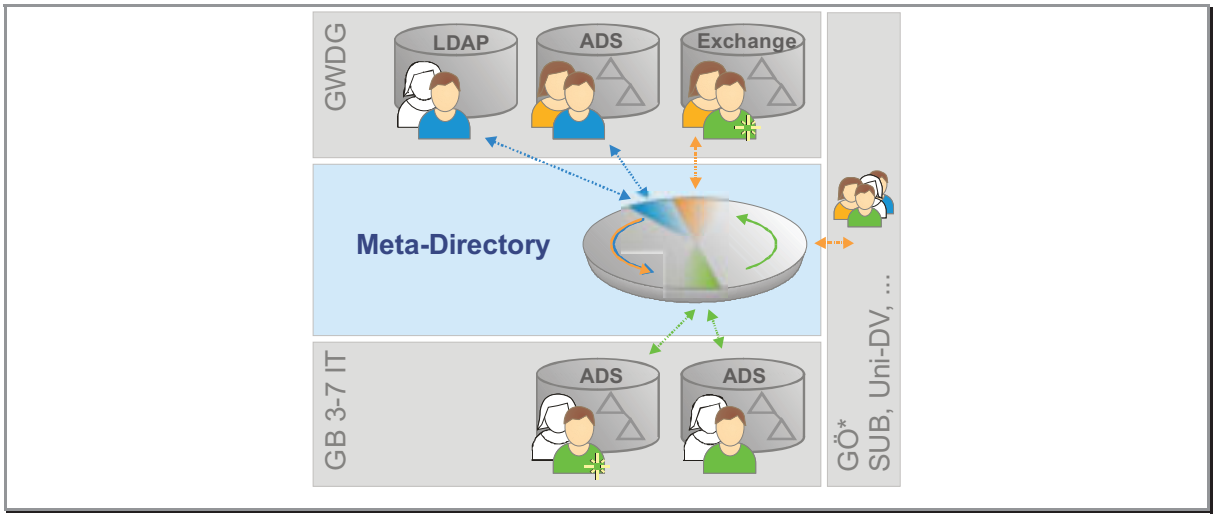

Abbildung 6-13: Kooperatives Identity Management am Standort Göttingen

Im Rahmen des GÖ*-Projekts wird eine pragmatische Umsetzung des Identity Managements (IDM) vorangetrieben.[788] Neben dem Meta-Directory dienen weitere IDM-Ansätze wie z.B. Virtual Directories als zentrale Schnittstelle für die sukzessive Integration weiterer Systeme. Viele IDM-Projekte in Wissenschaft und Wirtschaft konnten in der Vergangenheit unter anderem aufgrund der von vornherein vollständigen Integration aller Systeme und der damit verbundenen Komplexität nicht gänzlich umgesetzt werden. Durch die schrittweise Umsetzung des IDM in GÖ* kann im Gegensatz dazu auf bestehende Lösungen bei der Integration zusätzlicher Systeme zurückgegriffen werden.[789] Insbesondere kann dabei entschieden werden, ob die Funktion der zusätzlichen Systeme von bereits integrierten übernommen werden kann. Der Aufwand für die Anbindung an das Meta-Directory entfällt in diesem Fall von vornherein. Stattdessen wird das System zu Gunsten eines zentralen Verzeichnisses oder Virtual Directorys reduziert.[790] Virtual Directories bietet zusätzlich die Anbindung externer Organisationen (z.B. externer Max-Planck-Institute) an eine zentrale Authentifizierung, ohne dabei deren Benutzerdaten zentral zu speichern. Dies bietet neben Vorteilen für den Datenschutz auch Vorteile für die Eigenständigkeit der Institute.[791]

Im Zentrum des IDM stehen nicht die Verzeichnisse und technischen Lösungen, sondern die Benutzer selbst. Sie können z.B. ein einziges synchronisiertes Passwort für die integrierten Anwendungen verwenden („Single Password“) sowie einzelne Anwendungen durch einmalige Anmeldung nutzen („Single Sign-On“). Durch die Integration eines Web-Portals wird ihnen eine zentrale

[788] Vgl. skalierbares IDM in Abschnitt 6.3.2.1 sowie das Phasenmodell in Abschnitt 6.3.4.

[789] Gemäß Abschnitt 6.3.2.1.

[790] Vgl. Abschnitt 3.2.2.

[791] Vgl. Eigenständigkeit von Instituten als Anforderung in Abschnitt 4.2.1.

Möglichkeit für die Verwaltung von Passwörtern sowie weiterer identitätsbezogener Prozesse geboten.[792] Benutzer können hierbei nicht nur bestimmen, in welche Systeme ihre Identität sowie z.B. ein zugehöriges Passwort synchronisiert werden, sondern auch Workflows (beispielsweise für die Beantragung weiterer E-Mail-Adressen, von zusätzlichem Speicherbereich etc.) auslösen.

Für neu angelegte Benutzer-Konten wird innerhalb des IDM bereits ein eindeutiger Name (sog. GÖ*-ID) vergeben. Diese bildet die Basis für die einheitliche Vergabe von Benutzernamen in allen angeschlossenen Systemen. Eindeutige Benutzernamen stimmen hierbei mit dem in der E-Mail-Adresse verwendeten Namen überein, um die Benutzbarkeit zu erhöhen und gleichzeitig den Aufwand für die Administration zu senken.

Eine weitere Steigerung der Benutzbarkeit innerhalb des GÖ*-Umfelds sowie darüber hinaus bietet die bestehende Integration eines Identity Providers[793], der es Göttinger Identitäten ermöglicht, ohne weitere Anmeldung gemäß Single Sign-On auf Web-Inhalte über den Standort Göttingen hinaus (beispielsweise von Verlagen) zuzugreifen. Durch Integration der zugrunde liegenden Federation-Lösungen (vgl. SAML bzw. konkret Shibboleth) in Desktop-Anwendungen außerhalb des World Wide Web werden neben bestehenden Grid- und Bibliotheks-Anwendungen (vgl. Shibboleth) zukünftig umfassende Reduced- und „Single Sign-On“-Lösungen realisierbar.[794]

6.4.2 PKI für die Max-Planck-Gesellschaft und Universität Göttingen

Dezentrale und virtualisierte IT-Strukturen wie beispielsweise e-Science Umgebungen erfordern vielfach eine erhöhte Sicherheit für Authentifizierungs- und Verschlüsselungsmechanismen und somit den Einsatz von digitalen Zertifikaten sowie Public-Key-Infrastrukturen (PKI) für deren Verwaltung.[795] Um die Verwendung zertifikat-basierter Verfahren zu vereinfachen, sind Lösungen erforderlich, die organisatorische Vorgaben innerhalb einer PKI nutzerorientiert abbilden und den durch die Komplexität erhöhten Aufwand reduzieren, ohne hierbei die erzielte IT-Sicherheit zu mindern.

Eine Realisierung dieser Anforderungen bietet die Integration von Web-Portal-Lösungen, die den Benutzern ein eigenständiges Beantragen und Verwalten von Zertifikaten („Self-Service“) erlauben, wie sie bereits in Abschnitt 6.3.2.3 erläutert wurden. Dieser web-basierte Self-Service bietet nicht nur für die Benutzer als Zertifikatnehmer, sondern auch für die zuständigen Zertifizierungs-

---

[792] Gemäß Abschnitt 6.3.2.2.

[793] Basierend auf SAML vgl. Abschnitt 3.2.7.

[794] Vgl. Abschnitt 6.3.2.4.

[795] Vgl. Aufbau von Public-Key-Infrastrukturen in Abschnitt 3.2.4.

stellen eine nachhaltige Vereinfachung der notwendigen Abläufe für die Verwaltung und Nutzung einer PKI. Die dargestellten Prozesse werden in der Praxis für die PKI der Max-Planck-Gesellschaft und der Universität Göttingen, betrieben durch die Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG), angewendet.

Die Zertifizierungsstellen (CA) der GWDG (GWDG-CA und MPG-CA) sind seit Ihrer Inbetriebnahme im Juni 2004 (MPG-CA September 2004) Bestandteil der Public-Key-Infrastruktur des DFN-Vereins (DFN-PCA).[796] Im Juni 2005 wurden beide Zertifizierungsstellen als „Piloten“ in den Aufbau der neuen DFN-PKI integriert. Hierbei sind auch Anforderungen dieser Arbeit in die neuen Zertifizierungsrichtlinien des DFN-Vereins eingeflossen.[797] PKI-Leistungen der GWDG, die auf den erläuterten web-basierten Self-Service Portalen basieren, werden derzeit von verschiedenen Max-Planck-Instituten, dem Rechenzentrum Garching, der Universität Göttingen sowie der Stadt Göttingen für die Vergabe von X.509-Zertifikaten genutzt. Die PKI der GWDG bietet damit die digitale Vertrauensstruktur für das GÖ*-Projekt.

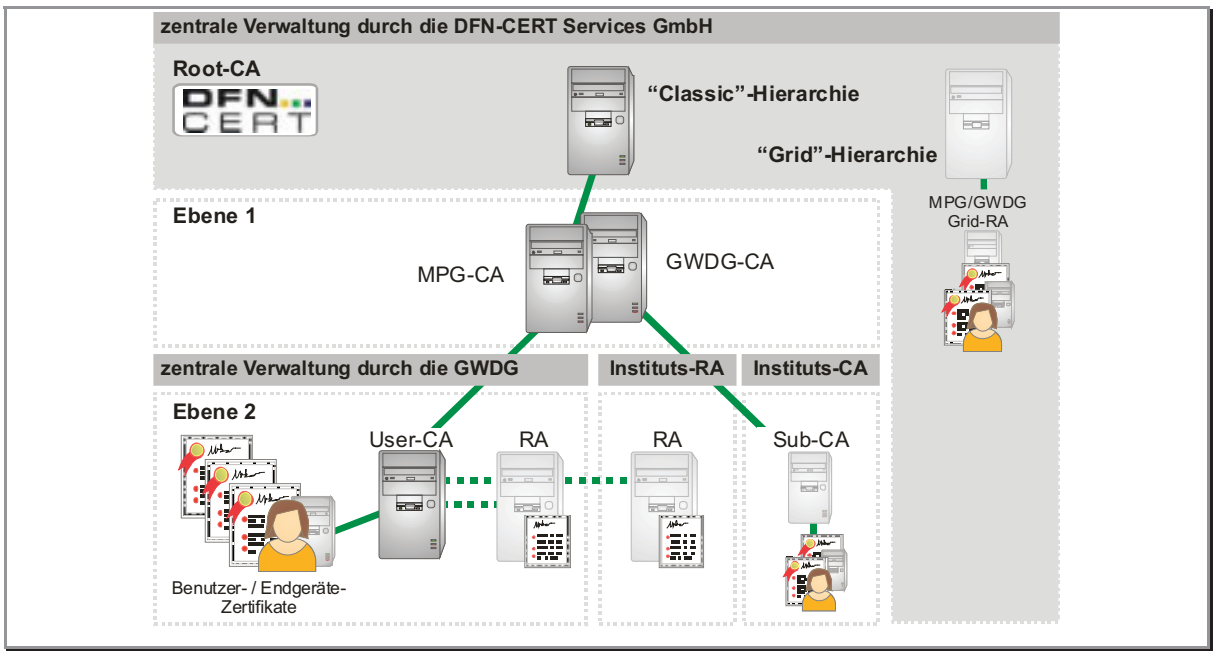

Abbildung 6-14: Struktur der Zertifizierungsstellen für Max-Planck-Gesellschaft und Universität Göttingen

Die Abbildung 6-14 zeigt die schematische Eingliederung der GWDG- und MPG-CA in die PKI des DFN-Vereins. In der Abbildung sind zwei Hierarchien (bzw. Root-CAs) der DFN-PKI darge-

[796] Vgl. DFN-PCA, 2007.

[797] Vgl. Abschnitt 6.3.2.3; Beispielsweise die Möglichkeit neue Anträge und Verlängerungen basierend auf bestehenden digitalen Signaturen zu verwenden, siehe DFN-CERT SERVICES: Zertifizierungsrichtlinie DFN-PKI Classic Version 1.1, 2005, S. 13.

stellt. Auf der rechten Seite die von der EUGridPMA[798] akkreditierte „Grid"-Hierarchie in die GWDG Registrierungsstellen (RA) betreibt, sowie die „Classic"-Hierarchie auf der linken Seite. Für interessierte Institute bietet die GWDG hierbei drei Betriebsmodelle an. Das Institut kann eine zentral von der GWDG betriebene CA oder für das Institut verwaltete RA verwenden oder selbst eine RA resp. CA realisieren.

Wissenschaftliche Nutzergruppen zeichnen sich im Vergleich mit anderen Nutzergruppen durch eine hohe Fluktuation der Mitglieder und eine große räumliche Verteilung der Beteiligten aus. Diese Eigenschaften wurden im Rahmen der Realisierung einer bundesweiten PKI für die Max-Planck-Gesellschaft spürbar. Ihre Berücksichtigung wurde nicht zuletzt von Administratoren interessierter Institute als unmittelbare Anforderung an die Realisierung und damit die Akzeptanz der zugehörigen PKI gestellt. Wird diese Anforderung nur ungenügend adressiert, verzichten Institutsangehörige auf die Steigerung der IT-Sicherheit durch Zertifikate zu Gunsten einer höheren Flexibilität, z.B. durch die Verwendung von ungesicherten Kommunikationsverfahren oder Passwörtern. [799]

Die hohe Benutzerfluktuation bedeutet für die Vergabe von Zertifikaten resp. PKI-Leistungen, dass innerhalb eines Monats eine Vielzahl von Zertifizierungs- und Sperrungsanträgen bearbeitet werden muss. Anders als bei geschlossenen und statischen Nutzergruppierungen können Zertifikate somit nicht einmalig gesammelt erstellt und für eine Laufzeit von mehreren Jahren verteilt werden. Zertifikate müssen kontinuierlich ausgestellt, verwaltet und zurückgezogen werden, da beispielsweise Gastforscher, Tutoren und Dozenten häufig ihre Institutszugehörigkeit wechseln oder mehreren Instituten oder Forschungsgruppen neu zugeordnet werden.[800]

Durch die räumliche Verteilung der Zertifikatnehmer werden Anforderungen an die organisatorischen Vorgaben und Abläufe einer PKI gestellt. Dies äußert sich insbesondere bei der eindeutigen, erstmaligen Identifizierung der Teilnehmer für die Überprüfung eines Zertifizierungsantrags. Einen Angehörigen eines Max-Planck-Instituts, der als Externer an einem Institut im Ausland forscht, ausschließlich durch persönlichen Kontakt mit dem Betreiber der PKI zu identifizieren ist beispielsweise nicht immer leicht durchführbar. Die Problematik wird durch zunehmend internationale Forschungsverbünde und -kooperationen verstärkt. Dies gilt insbesondere auch für Prozesse wie die Verlängerung bestehender Zertifikate oder die Beantragung zusätzlicher Zertifikate (z.B. weite-

---

[798] Vgl. EUGridPMA: The EUGridPMA - coordinating grid authentication in e-Science, 2007.

[799] Vgl. KOKE, H.: HRK-Guidelines for Strategies to the Information and Communication Structure at Universities, in LILLEMAA, T. (Hrsg.): Proceedings of the 12th International Conference of European University Information Systems, 2006; RIEGER, S. ET AL.: Self-Service PKI-Lösungen für eScience, in Paulsen, C. (Hrsg.): Sicherheit in vernetzten Systemen. 13. Workshop, 2006, S. B-1 ff.

[800] RIEGER, S. ET AL.: Self-Service PKI-Lösungen für eScience, in Paulsen, C. (Hrsg.): Sicherheit in vernetzten Systemen. 13. Workshop, 2006, S. B-1 ff.

re E-Mail-Adressen oder Endgeräte bzw. Server oder Clients des Zertifikatnehmers). Eine erneute persönliche Identifizierung durch den PKI-Betreiber ist hier ebenfalls weder im Interesse des Anwenders noch der Administratoren noch der Direktoren der Institute, denen sie angehören. [801]

Die herausgestellten Anforderungen durch Benutzerfluktuation und räumliche Verteilung an die Akzeptanz einer PKI bzw. von Zertifikat-basierten Authentifizierungsverfahren sind nicht nur für wissenschaftliche Nutzergruppen relevant. Sie gehören zu allgemeinen Anforderungen an die Anwendbarkeit (Usability), Barrierefreiheit bzw. die Akzeptanz von Authentifizierungsverfahren, wie sie von CRANOR UND GARFINKEL beschrieben werden.[802] Nutzer sind demnach nur dann bereit, Zertifikate als sicheres Authentifizierungsmerkmal im Vergleich zu simplen Passwörtern zu verwenden, wenn ihre Anwendbarkeit in einem akzeptablen Verhältnis zu der für sie erkennbaren Sicherheitsanforderung ist. Lösungsansätze, die bei der Realisierung der PKI für Max-Planck-Gesellschaft und Universität Göttingen verwendet wurden, beschreibt der Abschnitt 6.3.2.3.

6.4.3 Zusammenfassung der Ergebnisse der Fallstudien

Bereits am Ende des Kapitels 5 wurden in den Abschnitten 5.5.5, 5.6.5 sowie 5.7.5 hypothetische Aussagen über die Vereinheitlichung der Authentifizierung in heterogenen IT-Strukturen anhand des skizzierten theoretischen Modells getroffen. Durch die vorgestellten Fallstudien lassen sich die getroffenen Hypothesen überprüfen und verfeinern. Die Ergebnisse der Fallstudien dienen somit als Experimente für die Verifizierung der in dieser Arbeit getroffenen Aussagen über einheitliche Authentifizierung in heterogenen IT-Strukturen, so dass sich das in Abbildung 6-15 gezeigte hypothetisch-deduktive Modell ergibt.

Im Folgenden werden die Ergebnisse der Fallstudien für die Prüfung der anhand des theoretischen Modells gewonnenen Hypothesen verwendet. Die resultierenden endgültigen Hypothesen dieser Arbeit bilden daher die Zusammenfassung der Ergebnisse und Fallstudien.

---

[801] RIEGER, S. ET AL.: Self-Service PKI-Lösungen für eScience, in Paulsen, C. (Hrsg.): Sicherheit in vernetzten Systemen. 13. Workshop, 2006, S. B-1 ff.

[802] Vgl. CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 101 ff.

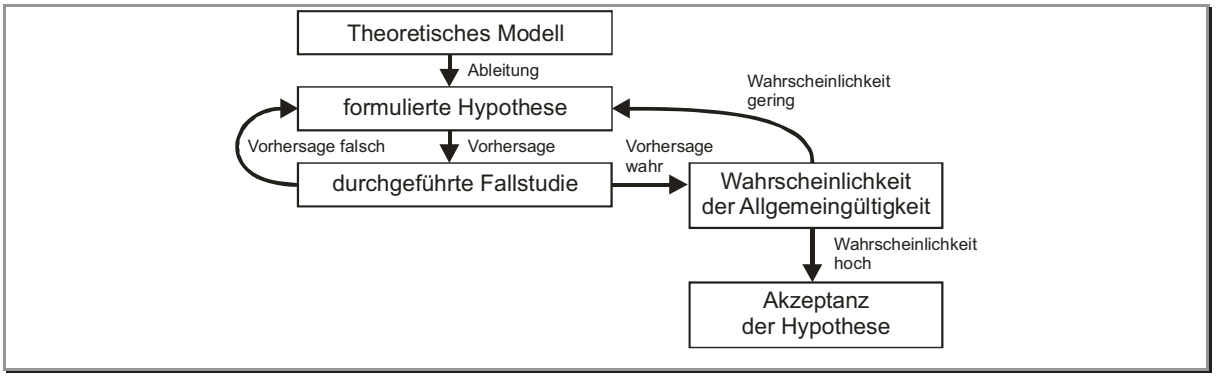

Abbildung 6-15: Hypothetisch-deduktives Modell der Beweisführung

Hypothese H1 aus Abschnitt 5.5.5 wird durch die Fallstudie zum Identity Management am Wissenschaftsstandort Göttingen nur teilweise bestätigt. Benutzer verstehen unter der Authentifizierung vorrangig ein Authentifizierungsmerkmal (z.B. Passwort) für den Zugriff auf die verwendeten Ressourcen. Die Einführung eines „Identity Management"-Portals[803] mit Möglichkeiten zur Synchronisation bzw. Verwaltung der Passwörter findet breite Akzeptanz unter den Benutzern. Ausnahmen stellen technisch versierte Anwender dar, die bewusst getrennte Passwörter bevorzugen.[804] Jedoch ist die Vereinheitlichung von Sicherheitsanforderungen weniger relevant für die Benutzer als die Anzahl der Authentifizierungsmerkmale. Benutzer sind durchaus bereit, für zwei Applikationen, deren Sicherheitsniveau sie unterschiedlich bewerten, unterschiedlich komplexe Passwörter zu definieren. Für Organisationen bilden Authentifizierungen zudem nicht das in H1 als hoch definierte Vereinheitlichungspotential. Systeme wie Verzeichnisdienste skalieren auch ohne größere Einschränkungen für die Verwaltung großer Mengen an Authentifizierungsmerkmale. Relevanter ist hier die Anzahl der erforderlichen Systeme selbst.

Darauf aufbauend ergibt sich die zusätzliche Relevanz der Anzahl im Vergleich zur Komplexität in Hypothese H2. Nicht nur mit zunehmender Komplexität, auch mit zunehmender Anzahl beginnen Benutzer beispielsweise Passwörter direkt im Programm abzuspeichern oder leicht zugänglich zu notieren.[805] Daraus folgt, dass die Hypothese H3 nicht bestätigt werden kann. Zwar bilden das

---

[803] Vgl. Abschnitt 6.3.2.2.

[804] Diese Ergebnisse bestätigten auch die Erkenntnisse aus RILEY, S.: Password Security: What Users Know and What They Actually Do, 2006 und ADAMS, A.; SASSE, A.: Users Are Not the Enemy. Why Users Compromise Security Mechanisms and How to Take Remedial Measures, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 639 ff.

[805] Dies wird auch in RILEY, S.: Password Security: What Users Know and What They Actually Do, 2006 und ADAMS, A.; SASSE, A.: Users Are Not the Enemy. Why Users Compromise Security Mechanisms and How to Take Remedial Measures, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, 2005, S. 639 ff. bestätigt.

Merkmal, das Verfahren oder das System, das die schwächste Sicherheit realisiert, das höchste Risiko, andererseits schützen aber insbesondere in heterogenen IT-Strukturen die einzelnen Merkmale und Verfahren unterschiedliche Ressourcen. Somit kann dies nur als Bewertungskriterium für die erzielte Sicherheit, nicht aber für die Vereinheitlichung allgemein beschrieben werden.

Bestätigt wird die Hypothese H4, die als ideale Integrationsform für Authentifizierungsmerkmale die Integration mehrerer Elemente (Int_b) nennt. Durch die Integration in einem Meta-Directory konnten auch in der Fallstudie zum GÖ* Identity Management Probleme, z.B. durch unterschiedliche Hash-Verfahren bei der Speicherung der Authentifizierungsmerkmale umgangen werden. Für Benutzer verringert sich der Aufwand durch die Verwaltung des zentralen Passworts im Meta-Directory mittels Web-Portal. Für die Administratoren sinkt der Aufwand durch die automatische Synchronisation der Authentifizierungsmerkmale durch das Meta-Directory. Um trotz einheitlichem Authentifizierungsmerkmal zusätzlich eine höhere Sicherheit zu erzielen, wurde mit dem Einsatz von USB Crypto-Tokens, z.B. für die Authentifizierung von Administratoren an deren Servern eine entsprechende Möglichkeit realisiert.

Diese adressiert auch die Hypothese H5, die eine Grenze für die Vereinheitlichung durch zunehmende Homogenität der Authentifizierungsmerkmale definiert. Neben der Verwendung von Zertifikaten und Tokens als Minderung dieser Problematik wurden in dem in Abschnitt 6.3.2.2 vorgestellten Web-Portal auch Möglichkeiten für die getrennte Vergabe bzw. Sperrung der Synchronisation von Passwörtern für die Benutzer realisiert. Allerdings wird diese Funktion nur von einem geringen Bruchteil der Benutzer verwendet bzw. gewünscht. Die Begrenzung gilt auch für die Vereinheitlichung von Authentifizierungssystemen insbesondere in Bezug auf deren Verfügbarkeit.[806]

Die Hypothese H6 aus Abschnitt 5.6.5 muss für aktuelle heterogene IT-Strukturen noch weiter eingeschränkt werden. Single Sign-On kann nur in Teilbereichen, z.B. mittels Kerberos oder für Web-Anwendungen, z.B. mittels SAML realisiert werden. Sofern keine Verfahren verwendet werden, die eine Speicherung bzw. automatische Übermittlung der Authentifizierungsmerkmale verwenden, schränken Reduced- und „Single Sign-On"-Lösungen die Sicherheit nicht ein.[807] Es konnte jedoch auch keine Steigerung der Sicherheit ermittelt werden. Die Reduktion des Aufwands durch einheitliche Authentifizierungsverfahren (z.B. LDAP, Kerberos) allgemein, wie in Hypothese H7 genannt, ist signifikanter als die durch den Teilaspekt „Single Sign-On" realisierte.

Für Organisationen besitzt in der Realität die Vereinheitlichung von Authentifizierungssystemen die höchste Relevanz. Kann ein System abgelöst werden, so entfällt der Aufwand für Verwaltung

[806] Vgl. H9 in Abschnitt 5.7.5.

[807] Vgl. die Nachteile durch die Speicherung von Passwörtern in Abschnitt 3.2.9.

und Verwendung sämtlicher damit verbundener Verfahren und Merkmale. Hypothese H8 muss daher neu formuliert werden. Innerhalb der heterogenen IT-Struktur im betrachteten GÖ*-Projekt existierten und existieren Ressourcen, die, z.B. bedingt durch gewachsene Strukturen, eigenständige separate Authentifizierungssysteme verwenden. Sie sollten, wie in H10 in Abschnitt 5.7.5 gefordert, auf gemeinsame Authentifizierungssysteme migriert oder außer Betrieb genommen werden.

Als finale Hypothesen nach Überprüfung durch die in diesem Abschnitt vorgestellten Fallstudien verbleiben:

H 1: Authentifizierungsmerkmale bilden, insbesondere durch deren Anzahl, das größte Potential für die Vereinheitlichung der Authentifizierung aus Sicht der Benutzer. Ein geeignetes Integrationsverfahren für Authentifizierungsmerkmale stellt die Integration mehrerer Elemente (Int_b) dar.

H 2: Der Aufwand für Verwaltung und Verwendung von Authentifizierungsmerkmalen (sowie Authentifizierungsverfahren und -systemen) steigt linear mit deren Anzahl. Während die erzielte Sicherheit mit zunehmender Anzahl und Komplexität weniger ansteigt.

H 3: Grenze für die Vereinheitlichung von Authentifizierungsmerkmalen (sowie Authentifizierungsverfahren und -systeme) bildet die zunehmende Homogenität und damit verbundene Minderung der erzielten Sicherheit.

H 4: „Single Sign-On“ besitzt in Bezug auf die erzielte Sicherheit eine niedrige, bezogen auf den Aufwand aus Sicht der Benutzer jedoch hohe Relevanz. In heterogenen IT-Strukturen sollte für die Umsetzung das Pareto-Prinzip („80-zu-20-Regel“) beachtet und nur in Teilbereichen ein „Single Sign-On“ angestrebt werden. Geeignetes Integrationsverfahren für Authentifizierungsverfahren bietet die Integration der Relationen (Int_d).

H 5: Authentifizierungssysteme stellen aus Sicht der Organisationen das höchste Vereinheitlichungspotential dar. Für die Vereinheitlichung von Authentifizierungssystemen bietet sich die Reduktion der Relationen (Int_c) und Elemente (Int_a) an. Insbesondere Ressourcen, die eigenständige Authentifizierungssysteme erfordern, sollten reduziert werden.

6.5 Bewertung des Realisierungsansatzes

Die im vorherigen Abschnitt vorgestellten Ergebnisse der Fallstudien dieser Arbeit unterstreichen die Relevanz der einheitlichen Authentifizierung für die Gestaltung zukünftiger IT-Strukturen. Aufgrund der Heterogenität, in wissenschaftlichen und betrieblichen IT-Strukturen gleichermaßen, ist eine Balance zwischen Aufwand und Sicherheit erforderlich, um eine effiziente Authentifizierung zu gewährleisten. Die genannten Hypothesen geben hierfür einen Handlungsrahmen vor. Die

innerhalb des GÖ*-Projekts gewonnenen Erkenntnisse können dabei auch auf andere Projekte übertragen werden. Aus der im Abschnitt 6.4 genannten Zusammenarbeit mit anderen Gruppen (LANIT, ZKI) und zahlreichen Diskussionen über die Abwägung des Aufwands der Authentifizierung für Benutzer und Administratoren mit den Teilnehmern wird dies ebenfalls deutlich. Dabei ist ein ganzheitlicher Ansatz erforderlich, der auch Schnittstellen zu den in Abschnitt 4.3 genannten angrenzenden Themen der IT-Sicherheit definiert. Durch die zunehmend dezentralen IT-Strukturen, wie am Beispiel des GÖ*-Projekt erläutert, stellt die Authentifizierung eine wichtige Grundvoraussetzung für den Betrieb verteilter Anwendungen und Netzwerke dar. Authentifizierung dient jedoch nicht dem Selbstzweck, sondern dem Schutz der eigentlich von ihr gesicherten Anwendungen und Ressourcen. Um daher den Aufwand in Relation zur erzielten Sicherheit zu halten, wurden in 5.4 geeignete Bewertungsmodelle vorgestellt. Im folgenden Abschnitt wird die quantitative Bewertung von Aufwand und Sicherheit vor und nach entsprechender Vereinheitlichung der Authentifizierung exemplarisch an den Fallstudien des GÖ*-Projekts gezeigt.

6.5.1 Quantifizierung der erzielten Vereinheitlichung

Neben der im Abschnitt 6.4.1 genannten quantitativen Reduktion der Authentifizierungssysteme, -verfahren und -merkmale lässt sich anhand der Fallstudie zum Identity Management am Wissenschaftsstandorts Göttingen auch die qualitative Vereinheitlichung der Authentifizierung ermitteln. Hierfür wird das in den Abschnitten 5.4.2 sowie 5.4.3 eingeführte und in Abschnitt 6.2 erweiterte Bewertungsmodell verwendet.

6.5.1.1 Bewertung der Ausgangssituation

Die Tabelle 6-2 zeigt die im Rahmen der Fallstudie ermittelte Quantifizierung des Aufwands sowie der erzielten Sicherheit der Authentifizierung vor der Vereinheitlichung durch das Identity Management. Benutzer benötigten keine speziellen Anforderungen ($A_{b.sa} = 0$), da überwiegend Standard-Authentifizierungsverfahren der Systeme verwendet wurden. Als Merkmale kamen nahezu ausschließlich Passwörter zum Einsatz. Aufgrund der hohen Anzahl bzw. der Begrenzung auf die konkreten Systeme entstand jedoch eine hohe Diversität der Authentifizierung (Anzahl der Passwörter und Anzahl der Authentifizierungsvorgänge pro Sitzung), daher wird $A_{b.beq}$ mit 0,67 bewertet. Benutzer mit kognitiven Einschränkungen wurden z.B. durch die Diversität der Passwörter benachteiligt ($A_{b.bar} = 0{,}33$). Mehrere passwortbezogene Anfragen oder Änderungen beim Help-Desk waren täglich zu verzeichnen. Sofern Benutzer ihr Passwort ändern wollten, mussten sie es in allen unterschiedlichen verwendeten Systemen tun, dies galt auch für die initiale Einrichtung des Benutzerkontos ($A_{b.war} = 1$). Da nahezu ausschließlich konventionelle, in der Regel alphanumerische Passwörter verwendet wurden, erfordert das Erlernen des Passworts, das auf einem initialen Brief vermerkt wird, bis zur evtl. Änderung ausschließlich kognitive Aktivität ($A_{b.vt} = 0{,}33$). Auf Erinne-

rungsfunktionen an das Passwort wurde aufgrund der hohen Fluktuation z.B. bei Studierenden, die zudem leicht Details ihrer Kommilitonen für den Rückschluss auf den Passwörter hätten verwenden können, verzichtet ($A_{b.ab}$ = 1). Allen Benutzern wurde nach der Aushändigung des initialen Passworts eine Passwort-Änderung empfohlen, so dass $A_{b.aus}$ = 0,67 bewertet wird.

$A_{b.sa}$	$A_{b.beq}$	$A_{b.bar}$	$A_{b.war}$	$A_{b.vt}$	$A_{b.ab}$	$A_{b.aus}$	$A_{o.sa}$	$A_{o.po}$	$A_{o.mob}$	$A_{o.bv}$	$A_{o.sw}$	$A_{o.hw}$	$A_{o.war}$
0	0,67	0,33	1	0,33	1	0,67	0	1	0,67	1	0,33	0,5	0,67
control = 1,5 , freq = 0,5 , policy = 1,5 , control = 1,5 , manage = 1,5 , self-service = 1,5												**A = 7,15**	
S_{vor}		S_{fe}		S_{of}		S_{an}		S_{dat}		S_{sz}		S_{aut}	
0,5		0,5		0,5		0		0,5		0,25		0	
risk = 1 , motive = 1 , audit = 1												**S = 1,19**	
Insgesamt: V = -0,5													

Tabelle 6-2: Ausgangssituation für die Fallstudie Identity Management am Wissenschaftsstandort Göttingen

Aufseiten der Organisationen waren für die bestehenden Systeme hinsichtlich der Authentifizierung keine speziellen Anforderungen erforderlich ($A_{o.sa}$ = 0). Die Authentifizierung war, obgleich teilweise wartungsintensiv, direkter Bestandteil der individuellen Anwendungen bzw. betriebenen Systeme selbst. Betrachtet auf die gesamte IT-Struktur war kein Merkmal, Verfahren oder System in der Lage, als alleiniges Element für die gesamte heterogene Struktur zu operieren. Dies resultiert teilweise aus Plattformabhängigkeit der Lösungen, Inkompatibilitäten oder fehlender Skalierbarkeit. Hierdurch war auch die in Abschnitt 6.4.1 geforderte kooperative Bereitstellung von Anwendungen durch die Institutsabhängigkeit eingeschränkt. $A_{o.po}$ wurde daher mit 1 bewertet. Aus den genannten Einschränkungen resultiert auch das eingeschränkte Roaming. Ebenfalls waren nicht für alle Anwendungsfälle Web-Schnittstellen für die dezentrale Authentifizierung und Verwaltung von Authentifizierungsinformationen verfügbar ($A_{o.mob}$ = 0,67). Sollten Benutzer über die gesamte IT-Struktur eingerichtet, erneuert, gesperrt oder entfernt werden, so war dies mit großem (da manuellem) Aufwand verbunden ($A_{o.bv}$ = 1). Aus der Diversität der Hard- und Software für Authentifizierungsverfahren und -systeme resultiert auch der Aufwand für deren Wartung ($A_{o.sw}$ = 0,33) und Betrieb ($A_{o.hw}$ = 0,5). Wartung für eine Erneuerung der Systeme, Verfahren und Merkmale war jedoch, ausgenommen der Passwort-Änderungen durch das Help-Desk, nicht gesondert erforderlich ($A_{o.war}$ = 0,67).

In der heterogenen IT-Struktur am Wissenschaftsstandort arbeiten unterschiedliche Benutzergruppen an unterschiedlichen Instituten und Orten; eine vollständige Kontrolle der Benutzer ist, z.B. allein durch die Fluktuation von Gast-Wissenschaftlern, Hilfskräften etc. nicht denkbar (*control = 1,5*). Da die Authentifizierung von Standard-Anwendungen wie E-Mail oder File-Zugriff betrachtet wurde, kann die Frequenz der Verwendung jedoch als hoch bewertet werden (*freq* = 0,5). Durch die Einführung einer Sicherheitsleitlinie der Universität Göttingen sowie den damit verbundenen Bestrebungen der ansässigen Institute kann *policy* = 1,5 angenommen werden. Eine zentrale Ver-

waltung aller Authentifizierungssysteme resp. -verfahren und -merkmale innerhalb der heterogenen IT-Struktur war nicht gegeben (*manage* = 1,5). Benutzer hatten daher auch keine Möglichkeit, zentral ihre Authentifizierungsinformationen zu verwalten (*self-service* = 1,5).

Es kann nicht ausgeschlossen werden, dass die verwendeten Passwörter am Standort nicht für Freunde und Verwandte der Benutzer vorhersagbar waren, da teilweise Passwörter mit weniger als acht Zeichen und ausschließlich basierend auf Buchstaben verwendet wurden (S_{vor} = 0,5). Aufgrund der Limitierung einiger Systeme auf eine maximale Passwortlänge von 8 Zeichen kann S_{fe} = 0,5 angenommen werden.[808] Die Passwörter konnten leicht während der Eingabe oder teilweise auch über das Netzwerk abgehört werden (S_{of} = 0,5). Auch Fälle, in denen eingeschleuste Programme Kennwörter der Administratoren abgehört hatten[809], waren bekannt (S_{an} = 0). Benutzer hatten die Möglichkeit für ihre Passwörter private Informationen zu verwenden (S_{dat} = 0,5). Geschützt wurden die Vertraulichkeit der übermittelten und gespeicherten Authentifizierungsinformationen oder auch deren Verfügbarkeit (z.B. durch Firewalls oder redundante Systeme) (S_{sz} = 0,25). Unterschiedliche Authentifizierungsfaktoren bzw. Hard- und Software wurden nicht verwendet, beidseitige Authentifizierung nur vereinzelt (S_{aut} = 0).

Sofern ein Angreifer Zugriff z.B. auf das Authentifizierungsmerkmal eines Benutzers erlangen konnte, wären ausschließlich die Daten dieses Benutzers offengelegt worden (*risk* = 1).[810] Aufgrund regelmäßiger, freiwilliger IT-Sicherheits-Schulungen am Wissenschaftsstandort Göttingen wird motive mit 1 bewertet. Die IT-Sicherheitsbeauftragten am Standort tragen auch zu einer regelmäßigen Kontrolle der Authentifizierungsvorgänge der wichtigsten Systeme bei (*audit* = 1). Insgesamt führt dies zur Ausgangssituation V = -0,5, wie in Tabelle 6-2 gezeigt.

6.5.1.2 Bewertung nach der Realisierung eines Identity Managements

Durch ein zentrales Identity Management, wie in Abschnitt 6.4.1 beschrieben, konnte die Diversität der Authentifizierungsmerkmale und -verfahren reduziert werden ($A_{b.beq}$ = 0,33 sowie *manage* = 0,5). Die Realisierung einheitlicher Passwörter mindert den Einfluss von kognitiven Einschränkungen ($A_{b.bar}$ = 0). Einrichtung und Erneuerung werden über ein zentrales Web-Portal im Self-Service (*self-service* = 0,5) erleichtert ($A_{b.war}$ = 0). Im skizzierten Portal werden zusätzlich Hilfen für die Erinnerung an das vergebene Passwort integriert ($A_{b.aus}$ = 0,33). Jedoch erfordert die Realisierung des Identity Management bzw. der erforderlichen Software und deren Anschaffung ($A_{o.sw}$ = 0,33) spezielle Kenntnisse aufseiten der Organisationen ($A_{o.sa}$ = 0,25). Das zentrale Management der

[808] Vgl. Fülle in SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 98 f.

[809] Vgl. "password sniffing" in SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 23 ff.

[810] Ausgenommen dem Zugriff auf Authentifizierungsmerkmale der Administratoren.

Identitäten über System- und Plattformgrenzen hinweg erlaubt die Reduktion von $A_{o.po}$ in der betrachteten IT-Struktur auf 0. Zusätzlich erleichtert es die Administration bzw. Benutzerverwaltung ($A_{o.bv}$ = 0, $A_{o.war}$ = 0,33). Die Einführung eines Web-Portals für das Identity Management reduziert zudem $A_{o.mob}$ auf 0,33.

Einfluss auf die erzielte Sicherheit nimmt das Identity Management z.B. durch die einheitliche Vorgabe von Komplexitätsrichtlinien für Passwörter (S_{an} = 0,67). Zusätzlich wird bei der Zentralisierung der Authentifizierungssysteme und -verfahren auf den verschlüsselten Austausch der Authentifizierungsinformationen (beidseitige Authentifizierung zwischen Benutzer und System S_{aut} = 0,33) geachtet. Die Verfahren kontrollieren hierbei auch die Integrität der übermittelten Daten. Redundante und gesicherte Authentifizierungssysteme[811] wie z.B. Verzeichnisdienste erlauben insgesamt eine Bewertung mit S_{sz} = 0,75.

$A_{b.sa}$	$A_{b.beq}$	$A_{b.bar}$	$A_{b.war}$	$A_{b.vt}$	$A_{b.ab}$	$A_{b.aus}$	$A_{o.sa}$	$A_{o.po}$	$A_{o.mob}$	$A_{o.bv}$	$A_{o.sw}$	$A_{o.hw}$	$A_{o.war}$
0	**0,33**	**0**	**0**	0,33	1	**0,33**	**0,25**	**0**	**0,33**	**0**	**0,33**	0,5	**0,33**
control = 1,5 , freq = 0,5 , policy = 1,5 , control = 1,5 , manage = **0,5** , self-service = **0,5**													**A = 2,11**
S_{vor}		S_{fe}		S_{of}		S_{an}		S_{dat}		S_{sz}		S_{aut}	
0,5		0,5		0,5		**0,67**		0,5		**0,75**		**0,33**	
risk = 1 , motive = 1 , audit = 1													**S = 1,93**
													Insgesamt: V = 0,41

Tabelle 6-3: Bewertung der Vereinheitlichung der Authentifizierung durch zentrales Identity Management

Die Änderungen wurden in Tabelle 6-3 farblich sowie fett hervorgehoben. Insgesamt ergibt sich aus dem fuzzyfizierten Bewertungsmodell eine im Vergleich zur Ausgangssituation in Tabelle 6-2 deutlich gesteigerte Vereinheitlichung von V = 0,41. Bedenkt man, dass nach wie vor durch die unterschiedlichen Authentifizierungsvorgänge eine Diversität existiert sowie die Sicherheit in wissenschaftlichen IT- resp. e-Science-Strukturen nicht in allen Einzelheiten (z.B. die Fluktuation neuer Studierender, Hilfskräfte etc.) kontrolliert werden kann, erscheint das Bewertungsverfahren auch für andere IT-Strukturen außerhalb des betrachteten Wissenschaftsstandorts Göttingen tragfähig.

[811] Vgl. Firewall in CHESWICK, W. R.; BELLOWIN, S. M., RUBIN, A. D.: Firewalls und Sicherheit im Internet. 2. Aufl., 2004, S. 219 ff. und Intrusion Prevention in STROBEL, S.: Intrusion Detection und Intrusion Prevention, in MÖRIKE, M.: Kosten & Nutzen von IT-Sicherheit in: HEILMANN, H. ET AL. (Hrsg.): HMD - Praxis der Wirtschaftsinformatik, Heft 236, 2004, S. 86 ff.

6.5.1.3 Bewertung nach der Realisierung exemplarischer „Single Sign-On"-Lösungen

Durch die Realisierung von „Single Sign-On"-Lösungen lässt sich die erzielte Vereinheitlichung weiter steigern. Tabelle 6-4 zeigt jedoch erwartungsgemäß[812] den geringen Einfluss von „Single Sign-On"-Lösungen auf das Gesamtergebnis der Vereinheitlichung. Während die Sicherheit durch Single Sign-On nicht verändert wird, wird der Aufwand für die Benutzer durch die reduzierten Authentifizierungsvorgänge gemindert ($A_{b.beq}$ = 0). „Single Sign-On"-Verfahren sind im Gegensatz zum skizzierten Idealmodell in Abschnitt 6.3.2.4 in der Praxis häufig auf spezielle Software angewiesen (z.B. auf Web-Anwendungen[813]) oder auf einzelne Plattformen beschränkt ($A_{o.po}$ = 0,5). Innerhalb dieser Strukturen wird jedoch von den Lösungen auch ein Roaming erlaubt ($A_{o.mob}$ = 0). Insgesamt ergibt sich insbesondere aus Sicht der Betreiber eine minimale Steigerung der Vereinheitlichung auf V = 0,42. Es ist anzumerken, dass die Reduktion der Authentifizierungsvorgänge jedoch seitens der Benutzer eine höhere Akzeptanz der Authentifizierungsverfahren zur Folge hat, die auch das Erzielen einer höheren Sicherheit ermöglichen kann. Dieser Effekt konnte jedoch in den durchgeführten Fallstudien nicht signifikant quantifiziert werden.

$A_{b.sa}$	$A_{b.beq}$	$A_{b.bar}$	$A_{b.war}$	$A_{b.vt}$	$A_{b.ab}$	$A_{b.aus}$	$A_{o.sa}$	$A_{o.po}$	$A_{o.mob}$	$A_{o.bv}$	$A_{o.sw}$	$A_{o.hw}$	$A_{o.war}$
0	**0**	0	0	0,33	1	0,33	0,25	**0,5**	**0**	0	0,33	0,5	0,33
control = 1,5 , freq = 0,5 , policy = 1,5 , control = 1,5 , manage = 0,5 , self-service = 0,5												**A = 1,84**	
S_{vor}		S_{fe}		S_{of}		S_{an}		S_{dat}		S_{sz}		S_{aut}	
0,5		0,5		0,5		0,67		0,5		0,75		0,33	
risk = 1 , motive = 1 , audit = 1												**S = 1,93**	
Insgesamt: V = 0,42													

Tabelle 6-4: Erweiterung des Identity Managements um „Single Sign-On"-Lösungen

6.5.1.4 Bewertung nach der Realisierung einer Public-Key-Infrastruktur

Um die Vereinheitlichung noch weiter zu erhöhen, ist die Steigerung der erzielten Sicherheit erforderlich. Eine Möglichkeit hierfür wurde durch die Verwendung von X.509-Zertifikaten für Authentifizierungsmerkmale und -verfahren innerhalb der Fallstudie zur Public-Key-Infrastruktur (PKI) für Max-Planck-Gesellschaft und Universität-Göttingen skizziert.[814] In Tabelle 6-5 werden die Ergebnisse der Fallstudie anhand der in Abschnitt 6.2 vorgestellten Methodik bewertet. Zertifikate erfordern in Bezug auf ihre Verwendung beim Benutzer spezielle Kenntnisse sowie Software ($A_{b.sa}$ = 0,67). Allerdings können Sie für „Single Sign-On"-Lösungen verwendet werden und so die Di-

[812] Vgl. H3 in Abschnitt 6.4.3.

[813] Vgl. Abschnitt 3.2.7.

[814] Vgl. die Fallstudien in Abschnitt 6.4.2.

versität von Authentifizierungsmerkmalen und -verfahren reduzieren ($A_{b.beq}$ = 0). Physisch oder sensorisch behinderte Benutzer können jedoch Zertifikate bzw. die verbundenen privaten Schlüssel ggf. nur mit Hilfestellung beantragen oder installieren ($A_{b.bar}$ = 0,33). Auch für andere Benutzer bedeutet die Einrichtung der Zertifikate einen Mehraufwand, auch wenn für die Erneuerung ein Web-Portal, wie in Abschnitt 6.3.2.3 skizziert, eingeführt wurde ($A_{b.war}$ = 0,5 sowie $A_{o.bv}$ = 0,67).

Organisationen benötigen speziell geschultes Personal für den Betrieb der Public-Key-Infrastrukturen sowie spezielle Software ($A_{o.sa}$ = 0,5) resp. deren Anschaffung und Wartung ($A_{o.sw}$ = 0,67). Zertifikate können durch die Verteilung der Root-Zertifikate leicht in unterschiedlichen Institutionen und plattformunabhängig verwendet werden. Allerdings skaliert die Vergabe von Zertifikaten aufgrund des höheren Aufwands im Vergleich zu Passwörtern schlechter ($A_{o.po}$ = 0,25). Nicht alle Web-Anwendungen lassen sich mittels Zertifikat, beispielsweise in Internet-Cafés etc. verwenden. Auch für das Roaming existiert kein allgemeiner Standard ($A_{o.mob}$ = 0,67).[815] Insgesamt bedeutet die Implementierung und Wartung der Public-Key-Infrastruktur für die Organisationen trotz der innerhalb der Fallstudie verwendeten Realisierung der Self-Service-Portale[816] bei Implementierung, Betrieb und Erneuerung einen höheren Aufwand im Vergleich zur Passwort-basierten Authentifizierung ($A_{o.war}$ = 1).

Durch die Verwendung von Zertifikaten resp. öffentlichen und privaten Schlüsseln wird die Sicherheit jedoch nachhaltig gesteigert. Authentifizierungsmerkmale sind nicht vorhersagbar (S_{vor} = 1), durch Schlüssellängen oberhalb von 1024 Bit kann S_{fe} = 1 angenommen werden. Schlüssel sind öffentlich (S_{dat} = 1) und können daher ohne Sicherheitsrisiko während der Verwendung offengelegt werden (S_{of} = 1). Durch die digitale Signatur innerhalb der Authentifizierungsvorgänge wird auch eine Verbindlichkeit und somit insgesamt S_{sz} = 1 erreicht.

Trotz des gesteigerten Aufwands von 3,70, der aufgrund der Verdopplung im Vergleich zur Verwendung von Passwörtern in Tabelle 6-3 als realistisch angesehen werden kann, ermöglicht die Steigerung der erzielten Sicherheit auf 2,98 eine Steigerung der Vereinheitlichung auf 0,65. Dies resultiert auch aus der impliziten Realisierung von „Single Sign-On“-Lösungen bzw. Vereinheitlichungen der Authentifizierungsmerkmale und -verfahren beim einheitlichen Einsatz von Zertifikaten.

$A_{b.sa}$	$A_{b.beq}$	$A_{b.bar}$	$A_{b.war}$	$A_{b.vt}$	$A_{b.ab}$	$A_{b.aus}$	$A_{o.sa}$	$A_{o.po}$	$A_{o.mob}$	$A_{o.bv}$	$A_{o.sw}$	$A_{o.hw}$	$A_{o.war}$
0,67	**0**	**0,33**	**0,5**	0,33	1	0,33	**0,5**	**0,25**	**0,67**	**0,67**	**0,67**	0,5	**1**
control = 1,5 , freq = 0,5 , policy = 1,5 , control = 1,5 , manage = 0,5 , self-service = 0,5												**A = 3,70**	

[815] Z.B. als Erweiterung für SSL vgl. Abschnitt 2.6.1.

[816] Vgl. Web-basierte Portale in Abschnitt 6.3.2.3.

S_{vor}	S_{fe}	S_{of}	S_{an}	S_{dat}	S_{sz}	S_{aut}
1	1	1	0,67	1	1	0,33
risk = 1 , motive = 1 , audit = 1						**S = 2,98**
						Insgesamt: V = 0,65

Tabelle 6-5: Erhöhung der Vereinheitlichung durch Steigerung der erzielten IT-Sicherheit mittels PKI

6.5.1.5 Bewertung nach der exemplarischen Verwendung von Tokens

Um die Sicherheit über die in Tabelle 6-5 betrachtete Fallstudie zur Publik Key Infrastruktur für Universität-Göttingen und Max-Planck-Gesellschaft zusätzlich zu steigern, wurde innerhalb der Fallstudie die Vergabe von USB Crypto-Tokens getestet. Derzeit werden diese Tokens nur für Administratoren im Windows- bzw. „Microsoft Active Directory"-Umfeld der GWDG verwendet. Benutzer benötigen zusätzlich das Token als spezielle Hardware ($A_{b.sa}$ = 1), was die Verwendung für sensorisch und physisch behinderte Benutzer einschränkt ($A_{b.bar}$ = 0,67). Auch für die Anwendungen und Systeme, die die Benutzer verwenden, müssen spezielle Software-Komponenten installiert werden ($A_{o.sw}$ = 1). Für die Initialisierung der Tokens ist ggf. spezielle Hardware (z.B. für Smart-Cards) erforderlich ($A_{o.sa}$ = 1).

Für die Mehrzahl der getesteten Token-Lösungen ist derzeit kein Angriff bekannt[817] (S_{an} = 1). Die Authentifizierung erfolgt durch das Token und ein für dessen Verwendung erforderliches Passwort anhand zweier Authentifizierungsfaktoren (S_{aut} = 1).

Die Tabelle 6-6 zeigt trotz leicht gestiegenem Aufwand im Vergleich zur PKI resp. Einführung von Zertifikaten in Tabelle 6-5 eine insgesamt höhere Vereinheitlichung von V = 0,89. Es ist jedoch zu bemerken, dass die erzielte Sicherheit von 3,73 bereits kurz vor der in dieser Arbeit in 6.2.2 Schwelle zur Klasse „inakzeptabel-hoch" liegt. Aufgrund der Tatsache, dass für die Verwendung der Tokens, z.B. unter Windows spezielle Software erforderlich ist (für Unix, Linux ist eine Unterstützung durch OpenSC[818] erforderlich), kann dieses Ergebnis als realistisch angesehen werden. Auch die Tatsache, dass die Erhöhung des Aufwands durch den Einsatz von Zertifikaten höheren Einfluss auf den Aufwand als die zusätzliche Verwendung von Tokens hat, kann auf andere Projekte übertragen werden.

$A_{b.sa}$	$A_{b.beq}$	$A_{b.bar}$	$A_{b.war}$	$A_{b.vt}$	$A_{b.ab}$	$A_{b.aus}$	$A_{o.sa}$	$A_{o.po}$	$A_{o.mob}$	$A_{o.bv}$	$A_{o.sw}$	$A_{o.hw}$	$A_{o.war}$
1	0	0,67	0,5	0,33	1	0,33	1	0,25	0,67	0,67	1	0,5	1
control = 0,5 , freq = 0,5 , policy = 1,5 , control = 1,5 , manage = 0,5 , self-service = 0,5												**A = 3,77**	

[817] Allerdings gibt es allgemeine theoretische Ansätze vgl. ECKERT, C.: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., 2004, S. 469 ff.

[818] Vgl. OpenSC, 2007.

S_{vor}	S_{fe}	S_{of}	S_{an}	S_{dat}	S_{sz}	S_{aut}
1	1	1	**1**	1	1	**1**
risk = 1 , motive = 1 , audit = 1						**S = 3,73**
						Insgesamt: V = 0,89

Tabelle 6-6: Zusätzliche Steigerung der IT-Sicherheit durch den Einsatz von Tokens

Im Rahmen der durchgeführten Fallstudie konnte auch ermittelt werden, dass die Handhabung der Zertifikate auf Tokens durch die nicht erforderliche Installation in sämtlichen Anwendungen resp. Registrierung usw. sogar erleichtert wird.

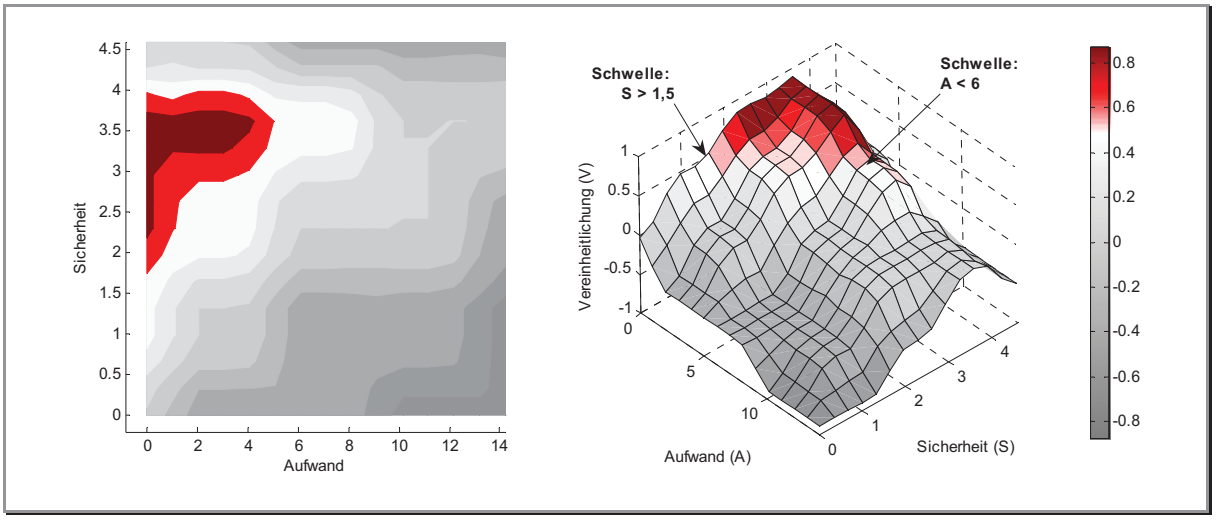

Abbildung 6-16: Schwellwerte der in dieser Arbeit betrachteten Vereinheitlichung der Authentifizierung

Allgemein können aus dem methodischen Ansatz für die Bewertung der Vereinheitlichung der Authentifizierung Schwellwerte für maximalen Aufwand und minimal zu erzielende Sicherheit ermittelt werden, ab denen eine Vereinheitlichung effizient ist. Abbildung 6-16 zeigt diese Schwellwerte anhand des Fuzzy-Modells aus Abschnitt 6.2.2. In der Skala ist der Farbraum für die Werte V > 0,5 markiert. Als minimaler Wert für die Sicherheit ab dem V > 0,5 angenommen werden kann, kann aus den Ergebnissen dieser Arbeit 1,5 angenommen werden. Der maximal mögliche Aufwand, der noch zu V > 0,5 führt, wird als 6 ermittelt. Die Vereinheitlichung der Authentifizierung in heterogenen Umgebungen sollte somit in Bezug auf die in dieser Arbeit betrachteten Faktoren einen Aufwand A < 6 sowie eine erzielte Sicherheit S > 1,5 erzielen, um als optimal (V > 0,5) zu gelten. Steigt das Sicherheitsniveau auf S > 4,0 so sinkt die Vereinheitlichung aufgrund der zunehmenden Komplexität, wie in Abschnitt 6.2.1 beschrieben. Die Schwellen wurden für die in dieser Arbeit betrachteten heterogenen IT-Strukturen anhand der in Abschnitt 6.2.2 definierten Grenzen bestimmt. Sie können für andere IT-Strukturen analog, basierend auf dem formalen Bewertungsmodell aus den Abschnitten 5.4.2 und 5.4.3, ermittelt werden.

Wie bereits in 6.1 erläutert, lassen sich als Zielvorgabe für den Aufwand die Reduzierung der damit verbundenen Kosten sowie für die Sicherheit die Minderung des Risikos definieren.[819] Kosten entstehen für die Organisationen durch den Aufwand für die Authentifizierung. Aus den Fallstudien wird deutlich, dass die Reduzierung der Kosten insbesondere durch eine Minimierung des Verwaltungsaufwands für die Organisationen ($A_{o.verwaltung}$ vgl. Abschnitt 5.4.2.5) erfolgen kann. Die Tabelle 6-3 zeigt die Reduzierung dieser Einflussfaktoren auf die Kosten durch $A_{o.bv}$, $A_{o.sw}$, $A_{o.hw}$ und $A_{o.war}$.

Die Sicherheit wird im Gegensatz dazu maßgeblich durch die Benutzer bestimmt. Aufgrund der hohen Anzahl von Benutzern, insbesondere in den betrachteten e-Science-Umgebungen, ist es erforderlich, dass ein einheitlicher Sicherheitsstandard realisiert wird. Eine hohe Anzahl von Benutzern kann zu unsicheren Lösungen verleiten, um den Aufwand klein zu halten. Insbesondere die unsichere Verwendung der Authentifizierung $S_{verwendung}$[820] bzw. $A_{b.verwendung}$[821] kann zur Kompromittierung, z.B. durch Abhören der Übertragung von Passwörtern durch Dritte führen. Für die Minderung des Risikos sollte daher die Maximierung von $S_{verwendung}$ angestrebt werden. Die Minimierung von $A_{b.verwendung}$ unterstützt daneben die Steigerung der Sicherheit durch hohe Akzeptanz der Authentifizierung auf der Seite der Benutzer.

6.5.2 Abgrenzung zu homogenen IT-Strukturen

Eine triviale Möglichkeit der vollständigen Vereinheitlichung der Authentifizierung stellt die Reduktion auf ein einziges Authentifizierungssystem -verfahren und -merkmal dar.[822] Beispielsweise könnten dies Active Directory, Kerberos und ein zugehöriges Passwort oder OpenLDAP, LDAP und ein zugehöriges Passwort bilden. In den in Abschnitt 6.4 aufgeführten Fallstudien wurde jedoch deutlich, dass diese Homogenisierung der IT-Strukturen in den betrachteten e-Science-Umgebungen nicht realisierbar ist, da es derzeit in der Praxis kein System oder Verfahren gibt, dass von allen Anwendungen und Ressourcen in der betrachteten heterogenen IT-Struktur unterstützt wird, wie bereits in Abschnitt 2.1.10 erläutert. Ansätze für mögliche zukünftige Verfahren werden in Abschnitt 6.3.2.3 und 6.3.2.5 beschrieben. Zusätzlich gelten für vollständig homogene Strukturen die in Abschnitt 4.4 genannten Nachteile. Homogene Authentifizierungsmerkmale öffnen unberechtigten Dritten im Falle einer Kompromittierung alle Ressourcen und Anwendungen der IT-Struktur. Insbesondere die Homogenität von Authentifizierungsverfahren und -systemen bildet

[819] Vgl. auch Abschnitt 5.4.2.

[820] Vgl. Abschnitt 5.4.3.

[821] Vgl. Abschnitt 5.4.2.

[822] Wie in Abschnitt 3.2.1 beschrieben.

durch ihre Anfälligkeit, z.B. bei einem Fehler der eingesetzten Software, ein hohes Risiko, während in heterogenen Strukturen im Falle eines Fehlers nur die an das jeweilige System angebundenen Ressourcen betroffen sind.[823]

Federation-basierte Lösungen, wie sie in Abschnitt 6.3.2.4 vorgestellt wurden, können diese Nachteile einer homogenen Authentifizierung in heterogenen IT-Strukturen zukünftig ausgleichen, sofern die in Abschnitt 4.4 geschilderten Grenzen berücksichtigt werden.

[823] Vgl. „fault tolerance“ bzw. “single point of failure” in SMITH, R. E.: Authentication. From Passwords to Public Keys, 2002, S. 115.

7 Fazit und Ausblick

In den folgenden Abschnitten werden die Ergebnisse dieser Arbeit abschließend zusammengefasst. Zusätzlich werden aktuelle Entwicklungen im Umfeld der Authentifizierung, der Stand der Forschung sowie Ansatzpunkte für zukünftige Arbeiten beschrieben.

7.1 Zusammenfassung der Ergebnisse

Die in Abschnitt 6.5.1 vorgestellte Bewertung der Ergebnisse der Fallstudien[824] belegt die Eignung des in Abschnitt 5.1 eingeführten Modells für die Authentifizierung in heterogenen IT-Strukturen. Aus den verbleibenden fünf Hypothesen des Abschnitts 6.4.3 lässt sich für die optimale Gestaltung von IT-Strukturen ableiten, dass für eine Vereinheitlichung zunächst Authentifizierungsmerkmale und -systeme betrachtet werden sollten. Dabei sollten Authentifizierungssysteme zunächst reduziert werden, während sich für Merkmale eine Integration, z.B. durch deren Synchronisation über mehrere Systeme, anbietet. Erst im zweiten Schritt besitzt die Vereinheitlichung von Authentifizierungsverfahren bzw. die Realisierung von Reduced- oder „Single Sign-On"-Lösungen eine Relevanz. Die Vereinheitlichung wird nach unten und oben durch die erzielte Sicherheit begrenzt. Werden keine Ansätze zur Vereinheitlichung verfolgt, so sorgt die in Abschnitt 3.1 beschriebene Diversität in heterogenen IT-Strukturen für einen hohen Aufwand, der nach Abschnitt 6.2.1 zu einer Verminderung der Sicherheit führt. Eine vollständige oder zu hohe Vereinheitlichung beschränkt ebenfalls die erzielte Sicherheit, z.B. durch die zunehmende Homogenisierung der Authentifizierungsmerkmale.[825] Zusätzlich wird die Vereinheitlichung durch die Kompatibilität der Systeme oder auch rechtliche Aspekte (wie den Datenschutz) begrenzt.[826] Eine vollständige Homogenisierung großräumiger bzw. verteilter heterogener IT-Strukturen ist somit, wie in Abschnitt 6.5.2 erläutert, nicht durchführbar.

Um das optimale Verhältnis zwischen Aufwand und Sicherheit der Authentifizierung in heterogenen IT-Strukturen zu finden, kann das theoretische Vergleichsmodell aus Abschnitt 5.1 gemäß der Zielfunktion aus Abschnitt 6.2.3 verwendet werden. Anhand des Modells kann die Eignung bestehender Verfahren für einheitliche Authentifizierung[827] evaluiert werden. Aus den in Kapitel 5 aufgestellten Hypothesen ergibt sich für die einheitliche Authentifizierung in e-Science-Umgebungen die Verwendung von Meta- und Virtual Directories für die Vereinheitlichung von Authentifizie-

[824] Vgl. Abschnitt 6.4.
[825] Vgl. Abschnitt 4.4.1.
[826] Vgl. Abschnitt 4.4.
[827] Vgl. Abschnitt 3.2.

rungsmerkmalen, sofern der Aufwand für die Verwendung von Zertifikaten resp. einer Public-Key-Infrastruktur zu hoch ist. Im Idealfall sind Zertifikate durch den höheren Sicherheitsstandard, z.B. in Kombination mit Tokens, die eine einfache Verwendung erlauben, zu favorisieren. Authentifizierungsverfahren sollten, sofern Single- oder Reduced Sign-On realisiert werden soll, auf Kerberos fokussiert werden. Als Übergang ist auch eine Authentifizierung mittels LDAP gegenüber zentralen oder dezentralen Verzeichnisdiensten sinnvoll. Für Web-Anwendungen sollten bereits Federation-basierte Lösungen favorisiert werden, basierend auf dem SAML 2.0 Standard der OASIS.[828] Es ist zu erwarten, dass Federation-basierte Verfahren zunehmend auch für Authentifizierungsverfahren außerhalb des World Wide Web Verwendung finden werden. Für Authentifizierungssysteme bietet sich derzeit deren Reduktion durch Verzeichnisdienste an, sofern nicht Public-Key-Infrastrukturen eingesetzt werden.

Für eine optimale Vereinheitlichung der Authentifizierung ist jedoch neben der Auswahl der bestehenden Lösungen auch deren Erweiterung erforderlich, um die in Abschnitt 3.3 genannten Probleme bestehender Verfahren zu kompensieren. Hierfür wird in Abschnitt 6.3.4 ein Migrationsmodell beschrieben, dass die Vereinheitlichung in drei Phasen einteilt.[829] Zunächst erfolgt eine bewusste Diversifikation der Authentifizierung durch die Erweiterung der Clients um die Verwendung alternativer Authentifizierungsverfahren und -systeme. Die anschließende Zentralisierung der Verfahren und Systeme dient als Grundlage für die Etablierung von dezentralen und plattform- sowie anwendungsunabhängigen Lösungen wie Federation-basierte Verfahren[830] und flexible Vertrauensstellungen.[831] In jedem Fall wird hierbei die Verwaltung der Identität zukünftig mehr und mehr selbständig durch den Benutzer durchgeführt. Dies ermöglicht eine Verringerung der Verwaltungskosten aufseiten der Betreiber bei gleichzeitiger Erhöhung des Datenschutzes bzw. der Selbstbestimmung durch den Benutzer. Dieser kann dadurch seine Identität für unterschiedliche Organisationen und Anwendungsfälle verwenden. Durch Trust-Modelle, wie sie in Abschnitt 6.3.2.5 erläutert werden, ist hierbei auch eine Verwendung bestehender Vertrauensstellungen für neue Anwendungen möglich. Beispielsweise kann ein Benutzer seine Anerkennung und Glaubwürdigkeit in Form einer Bewertung bei einem Web-Shop, Internet-Auktionshaus oder Forum für den Nachweis seiner Vertrauenswürdigkeit und Authentizität bei einer neuen Organisation wieder verwenden.[832] Um den Benutzern diese Optionen zu eröffnen, sind Web-Portale, wie sie in Abschnitt 6.3.2.2 vorge-

---

[828] Vgl. OASIS Security Services (SAML), 2007.

[829] Vgl. auch skalierbares Identity Management in Abschnitt 6.3.2.1.

[830] Vgl. Verwendung von Federation-basierten Verfahren für Desktop-Anwendungen in Abschnitt 6.3.2.4.

[831] Vgl. Abschnitt 6.3.2.5.

[832] Vgl. benutzerzentrierte Verfahren wie SXIP in Abschnitt 3.4.

stellt werden, eine Grundbedingung. Für die Verwendung von Zertifikaten innerhalb einer Public-Key-Infrastruktur sind diese durch Self-Service-Funktionen, wie sie in Abschnitt 6.3.2.3 beschrieben werden, zu erweitern. Hierdurch werden die in Kapitel 4 und Abschnitt 6.1 erläuterten Anforderungen an die Vereinheitlichung der Authentifizierung in heterogenen wissenschaftlichen und betrieblichen IT-Strukturen optimal umgesetzt.

Ein optimales Maß für die Vereinheitlichung der Authentifizierung bietet dabei das in Abschnitt 6.3.3 vorgestellte Ebenenmodell. Es teilt die Vereinheitlichung auf unterschiedliche Sicherheitsniveaus auf, die vom Benutzer bestimmt werden. Dieses Modell kann als Grundlage für die Verwaltung der Authentifizierungsmerkmale im Web-Portal dienen. Benutzern wird so die Abwägung zwischen Aufwand und Sicherheit vermittelt und ermöglicht.

Das in Kapitel 5 definierte theoretische Modell für die Authentifizierung in heterogenen IT-Strukturen kann auch für die Bewertung zukünftiger Authentifizierungsmerkmale, -verfahren und -systeme als Erweiterung der in Abschnitt 3.2 genannten bestehenden Lösungsansätze für einheitliche Authentifizierung verwendet werden. Mögliche zukünftige Anwendungen und Erweiterungen werden im folgenden Abschnitt aufgezeigt.

7.2 Zukünftige Arbeiten

Im Abschnitt 3.4 wurden bereits aktuelle Entwicklungen für eine einheitliche Authentifizierung in Web-Anwendungen beschrieben. Diese beschreiben beispielsweise in den sieben Identity Laws von CAMERON eine Zentrierung der Authentifizierung und Identitätsverwaltung auf den Benutzer.[833] Basierend auf diesen Entwicklungen ist die Betrachtung von Federation-basierten Verfahren für Anwendungen außerhalb des World Wide Web in zukünftigen Arbeiten relevant. Sie würden auch die in Abschnitt 3.3 genannten Defizite bestehender Verfahren adressieren und eine Homogenisierung der Authentifizierungsverfahren ohne Einschränkung der IT-Sicherheit erlauben. Der Benutzer kann hierbei selbständig entscheiden, für welche Bereiche, Anwendungen und Organisationen er eine einheitliche Authentifizierung verwenden möchte und welche ein separates Sicherheitsniveau erfordern.[834] Hierfür wäre die Erweiterung der Federation-Lösungen um die selbständige Verwaltung der Identität durch die Benutzer erforderlich. Dies umfasst die Integration der in dieser Arbeit ausgegrenzten Verfahren zur Autorisierung und Abrechung sowie dem Auditing.[835] Basis für die Erweiterung könnte ein neues Authentifizierungsverfahren bilden, das auch in hetero-

[833] Vgl. CAMERON, K.: The Laws of Identity, 2005.

[834] Vgl. Ebenenniveau in Abschnitt 6.3.3.

[835] Vgl. Abschnitt 4.3.3.

genen IT-Strukturen und organisationsübergreifend einsetzbar ist. Dieses könnte auch die Auswertung von Vertrauensstellungen, z.B. durch die maschinelle Verarbeitung von Zertifizierungsrichtlinien, wie in Abschnitt 6.3.2.5 beschrieben, realisieren. Die durch Maschinen interpretierbare Definition von Zertifizierungsrichtlinien wäre ebenfalls Gegenstand potenzieller zukünftiger Arbeiten. Auch die Definition von Anforderungen an die Gestaltung von Web-Portalen hinsichtlich der in Abschnitt 6.3.2.2 genannten Kriterien bietet sich für zukünftige Arbeiten an.

Die Bewertung und Quantifizierung von Sicherheit und dem damit verbundenen Aufwand bietet ebenfalls weiteren Raum für die Forschung. Nachfolgende Arbeiten können hierfür auf dem in Kapitel 5 skizzierten Modell aufbauen und dessen Optimierung erweitern.

Abbildungsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

A Simple Distributed Security Infrastructure (SDSI) [SDSI, 2007]: http://theory.lcs.mit.edu/~cis/sdsi.html, abgerufen am: 21.01.2007.

AAR: Wie funktioniert Shibboleth? [AAR-Shib, 2006]: Wie funktioniert Shibboleth? Ein technischer Überblick, Vortrag: 3. AAR Workshop, http://aar.vascoda.de/docs/workshop_20061010/AAR_20061010_Einfuehrung.pdf, abgerufen am: 21.01.2007.

ABOBA ET AL. [EAP, 2004]: Extensible Authentication Protocol (EAP) (RFC 3748), ftp://ftp.rfc-editor.org/in-notes/rfc3748.txt, abgerufen am: 21.01.2007.

ABOBA, B. [EAP, 1996]: Extensible Authentication Protocol (EAP) (RFC 3748), ftp://ftp.rfc-editor.org/in-notes/rfc3748.txt, abgerufen am: 21.01.2007.

ABOBA, B.; SIMON, D. [EAP-TLS, 1999]: PPP EAP TLS Authentication Protocol, ftp://ftp.rfc-editor.org/in-notes/rfc2716.txt, abgerufen am: 21.01.2007.

AD4Unix [AD4Unix, 2007]: AD4Unix, http://sourceforge.net/projects/ad4unix/, abgerufen am: 21.01.2007.

ADAMS, A.; SASSE, A. [Users-Not-Enemy, 2005]: Users Are Not the Enemy. Why Users Compromise Security Mechanisms and How to Take Remedial Measures, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, O'Reilly, Sebastopol, 2005.

ADAMS, C.; LLOYD, S. [PKI, 2003]: Understanding PKI, Addison-Wesley, Boston et al., 2003.

Aladdin eToken [Aladdin, 2007]: Authentisierung digitale Signaturen und Zertifikate PKI - eToken, http://www.aladdin.de/produkte/usbtoken_esecurity/etoken_uebersicht.html, abgerufen am: 21.01.2007.

ANDERSON, R. [Sec-Engineering, 2001]: Security Engineering. A Guide to Building Dependable Distributed Systems, Wiley, New York et al., 2001.

BADACH, A.; HOFFMANN, E. [Technik-der-IP-Netze, 2001]: Technik der IP-Netze, Carl-Hanser Verlag, München, 2001.

BADACH, A.; RIEGER, S.; SCHMAUCH, M. [Web-Technologien, 2005]: Web-Technologien, Carl-Hanser Verlag, München, 2003.

BAIZE, E.; PINKAS, D. [SPNEGO, 1998]: The Simple and Protected GSS-API Negotiation Mechanism (SPNEGO) (RFC 2478), ftp://ftp.rfc-editor.org/in-notes/rfc2478.txt, abgerufen am: 21.01.2007.

BALFANZ, D.; DURFEE, G.; SMETTERS, D. K. [Usable-PKI, 2005]: Making the Impossible Easy: Usable PKI, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, O'Reilly, Sebastopol, 2005.

Bandit Project [Bandit, 2007]: http://www.bandit-project.org/index.php/Welcome_to_Bandit, abgerufen am: 21.01.2007.

BARTLETT, A. [Samba-Active-Directory, 2005]: Samba 4 - Active Directory, http://samba.org/samba/news/articles/abartlet_thesis.pdf, abgerufen am: 21.01.2007.

BIETHAHN ET AL. [Fuzzy-Sets, 1965]: Methoden der praktischen Entscheidungsfindung, 4. Auflage, Skripten der Abteilung Wirtschaftsinformatik I, Göttingen, 2000.

BIETHAHN, J. ET AL. [Fuzzy-Set-BWL, 1996]: Fuzzy Set-Theorie in der betriebswirtschaftlichen Anwendung, Franz Vahlen, München, 1996.

BIETHAHN, J. ET AL. [Optimierung-Simulation, 2004]: Optimierung und Simulation, Oldenbourg, München, 2004.

BIETHAHN, J.; CVJETKOVIC, D.; ORTHEY, F.; MUCKSCH, H.; NISSEN, V. [Datenschutz, 2000]: Datenschutz, Datensicherheit und gesellschaftliche Auswirkungen der Informationsverarbeitung. 3. Aufl., Göttingen, 2000.

BISHOP, M. [Usability-Psychology, 2005]: Psychological Acceptability Revisited, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, O'Reilly, Sebastopol, 2005.

BMBF-eScience [BMBF-eScience, 2007]: BMBF: eScience, http://www.bmbf.de/de/298.php, abgerufen am 21.01.2007.

BOYD, C.; MATHURIA, A. [Boyd-Authentication, 2003]: Protocols for Authentication and Key Establishment, Springer, Heidelberg, 2003.

BUCHMANN, J. [SHA1, 2005]: Einführung in die Kryptographie. 3. Aufl., Springer, Berlin et al., 2003.

BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK [BSI-Kryptoalgorithmen, 2007]: Kryptoalgorithmen, http://www.bsi.bund.de/esig/basics/techbas/krypto/index.htm, abgerufen am: 21.01.2007.

BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK [BSI-Zertifizierung, 2006]: Zertifizierung, http://www.bsi.bund.de/zertifiz/zert/index.htm, abgerufen am: 21.01.2007.

BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK [CC, 2006]: Common Criteria. Version 2.3, http://www.bsi.bund.de/cc, abgerufen am: 21.01.2007.

BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: Authentifizierung im E-Government [E-Government-Auth, 2005]: http://www.bsi.bund.de/fachthem/egov/download/4_Authen.pdf, abgerufen 21.01.2007.

BUNDESBANK [Basel-II, 2007]: Basel II - Die neue Baseler Eigenkapitalvereinbarung, http://www.bundesbank.de/bankenaufsicht/bankenaufsicht_basel.php, abgerufen am: 21.01.2007.

BUNDESMINISTERIUM DER JUSTIZ [BDSG, 1990]: Bundesdatenschutzgesetz (BDSG), http://www.gesetze-im-internet.de/bdsg_1990/index.html , abgerufen am: 21.01.2007.

BUNDESMINISTERIUM DER JUSTIZ [SigG, 2001]: Gesetz über Rahmenbedingungen für elektronische Signaturen (SigG), http://www.gesetze-im-internet.de/sigg_2001/index.html, 21.01.2007.

BUNDESMINISTERIUM DER JUSTIZ [SigV, 2001]: Verordnung zur elektronischen Signatur (SigV), http://www.gesetze-im-internet.de/sigv_2001/index.html, abgerufen am: 21.01.2007.

BUNDESMINISTERIUM DES INNEREN [BMI, 2007]: Hintergrundinformationen zum ePass. Technik & Sicherheit, http://www.bmi.bund.de/cln_012/nn_122688/Internet/Content/Themen/Informationsgesellschaft/Einzelseiten/ePass__Biometrie/Hintergrundinfo__ePass.html, abgerufen am: 21.01.2007.

BUNDESMINISTERIUM FÜR GESUNDHEIT [GK, 2007]: Die Gesundheitskarte, http://www.die-gesundheitskarte.de, abgerufen am: 21.01.2007.

BUNDESNETZAGENTUR [BNetzA-Algorithmen, 2006]: Geeignete Algorithmen, http://www.bundesnetzagentur.de/media/archive/5951.pdf, 2006.

BUNDESNETZAGENTUR [BNetzA-Zert, 2007]: Akkreditierung, http://www.bundesnetzagentur.de/enid/392e9e4d807582f10d29cfd8afb6c1c6,0/Elektronische_Signatur/Zertifizierungsdiensteanbieter_ph.html, abgerufen am: 21.01.2007.

BURNETT, M.; KLEIMAN, D. [Passwords, 2006]: Perfect Passwords, Syngress, Rockland, 2006.

CAMERON, K. [Laws-of-Identity, 2005]: The Laws of Identity, http://www.identityblog.com/stories/2004/12/09/thelaws.html, abgerufen am: 21.01.2007.

CAM-WINGET, N. ET AL. [EAP-FAST, 2006]: The Flexible Authentication via Secure Tunneling Extensible Authentication Protocol Method (EAP-FAST), ftp://ftp.rfc-editor.org/in-notes/internet-drafts/draft-cam-winget-eap-fast-06.txt, abgerufen am: 21.01.2007

CHAPPLE, M. [IPS, 2007]: Intrusion Prevention Systeme sind immer noch ein Muss, http://www.searchsecurity.de/themenkanaele/netzwerksicherheit/intrusionmanagement/networkintrusiondetection/articles/50599/, abgerufen am: 21.01.2007.

CHOKANI, S. ET AL. [PKI-Policy, 2003]: Internet X.509 Public Key Infrastructure, Certificate Policy and Certificate Practices Framework (RFC 3647), ftp://ftp.rfc-editor.org/in-notes/rfc3647.txt, abgerufen am: 21.01.2007.

COCKS, C. [PKC, 2001]: PKC - A Fresh Approach, http://www.cesg.gov.uk/site/ast/idpkc/media/idpkcho.pdf, abgerufen am: 21.01.2007.

COMMISSION OF THE EUROPEAN COMMUNITIES [ITSEC, 1991]: Information Technology Security Evaluation Criteria (ITSEC): Preliminary Harmonised Criteria, http://www.ssi.gouv.fr/site_documents/ITSEC/ITSEC-uk.pdf, abgerufen am 21.01.2007.

COMMUNICATIONS-ELECTRONICS SECURITY GROUP [ID-PKC, 2007]: ID-PKC: a new approach to Public Key Cryptography, http://www.cesg.gov.uk/site/ast/index.cfm?menuSelected=3&displayPage=3, abgerufen am: 21.01.2007.

CORPORATE-CONSULTING.NETWORK [Basel-II-IT-Sec, 2006]: IT-Sicherheit als Rating-Faktor, http://www.basel-ii.info/print-pdf.php?sid=76, abgerufen am: 21.01.2007.

COVENTRY, L.: Usable Biometrics, in CRANOR, L. F.; GARFINKEL, S. [Usable-Biometrics, 2005]: Security and Usability. Designing Secure Systems That People Can Use, O'Reilly, Sebastopol, 2005.

CRANOR, L. F.; GARFINKEL, S. [Security-and-Usability, 2005]: Security and Usability. Designing Secure Systems That People Can Use, O'Reilly, Sebastopol, 2005.

Cypak PIN-on-Card [Cypak, 2007]: PIN-on-Card, http://www.cypak.com/index.php?a=products&b=sc&page=products_sc, abgerufen am: 21.01.2007.

DAUM, B. [Rich-Client, 2006]: Rich-Client-Entwicklung mit Eclipse 3.2, 2. Aufl., dpunkt, Heidelberg, 2006.

Dell IdentiPHI Enterprise Security Solution [IdentiPHI, 2007]: http://www.dell.com/content/topics/topic.aspx/global/shared/sitelets/pub_solutions/hied/Security?c=us&l=en&s=gen&~page=4, abgerufen am: 21.01.2007.

DEPARTMENT OF DEFENSE [TCSEC, 1983]: DOD 5200.28-STD. Trusted Computer System Evaluation Criteria, http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html, abgerufen am: 21.01.2007.

DFN AAIWiki: ShARPE [ShARPE, 2007]: https://wiki.aai.dfn.de/wiki/index.php/ShARPE, abgerufen am: 21.01.2007.

DFN-CERT SERVICES [DFN-CP, 2005]: Zertifizierungsrichtlinie DFN-PKI Classic Version 1.1, 2005, http://www.pca.dfn.de/dfn-pki/certification/cp/classic/x509/dfn-pki-cp-classic-1.3.6.1.4.1.22177.300.1.1.1.1.1.pdf, abgerufen am: 21.01.2007.

DFN-CERT SERVICES [DFN-CPS, 2005]: Erklärung zum Zertifizierungsbetrieb DFN-PKI Classic Version 1.1, http://www.pca.dfn.de/dfn-pki/certification/cps/classic/x509/dfn-pki-cps-classic-1.3.6.1.4.1.22177.300.2.1.1.1.1.pdf, abgerufen am: 21.01.2007.

DFN-PCA [DFN-PCA, 2007]: http://www.pca.dfn.de, abgerufen am: 21.01.2007.

DIERKS, T. [TLS, 2006]: The Transport Layer Security (TLS) Protocol. Version 1.1 (RFC 4346), ftp://ftp.rfc-editor.org/in-notes/rfc4346.txt, abgerufen am: 21.01.2007.

DIESTEL, R. [Graphentheorie, 2000]: Graphentheorie, 2. Auflage, Springer, Berlin, 2000.

DINI [DINI, 2007]: http://www.dini.de, abgerufen am: 21.01.2007.

DÖRFLER, W.; PESCHEK, W. [Math-Informatik, 1988]: Einführung in die Mathematik für Informatiker, Carl-Hanser Verlag, München, 1988.

DUDEN [Duden-Fremdwörter, 2001]: Das Fremdwörterbuch, 7. Aufl., Dudenverlag, Mannheim, 2001.

eBay [eBay, 2007], eBay Passwort vergessen?, http://cgi4.ebay.de/ws/eBayISAPI.dll?ForgotYourPasswordShow, abgerufen am: 21.01.2007.

ECKERT, C. [IT-Sicherheit, 2004]: IT-Sicherheit Konzepte. Verfahren - Protokolle. 3. Aufl., Oldenbourg Wissenschaftsverlag, München, 2004.

Economics & Security [EcoSec, 2007]: Economics and Security Resource Page, http://www.cl.cam.ac.uk/%7Erja14/econsec.html, abgerufen am: 21.01.2007.

Economic-Security [Economic-Security, 2007]: Economics and Security Resource Page, http://www.cl.cam.ac.uk/%7Erja14/econsec.html, 2007.

ELAN [ELAN, 2007]: http://www.elan-niedersachsen.de, abgerufen am: 21.01.2007.

ELLISON, C. ET AL. [SPKI, 1999]: SPKI Certificate Theory (RFC 2693), ftp://ftp.rfc-editor.org/in-notes/rfc2693.txt, abgerufen am: 21.01.2007.

ENSOR, B. [Consumers-Passwords, 2004]: How Consumers Remember Passwords, http://www.forrester.com/Research/Document/Excerpt/0,7211,34566,00.html, abgerufen am: 21.01.2007.

ERDLE, C. [Migrationsstrategien, 2005]: Legacy Migrationsstrategien, Hauptseminar: Management von Softwaresystemen an der TU-München, http://www4.in.tum.de/lehre/seminare/hs/WS0506/mvs/files/Ausarbeitung_Erdle.pdf, abgerufen am: 21.01.2007.

e-Science-Forum [e-Science-Forum, 2007]: e-Science-Forum: Grids, http://www.e-science-forum.de/de/77.php, abgerufen am 21.01.2007.

EUGridPMA [EUGRIDPMA, 2007]: The EUGridPMA - coordinating grid authentication in e-Science:, http://www.eugridpma.org , abgerufen am: 21.01.2007.

Evidian AccessMaster [AccessMaster, 2007]: http://www.evidian.com/security/index.htm, abgerufen am: 21.01.2007.

FEDERRATH, H. [Kosten-Nutzen-IT-Sicherheit, 2006]: Kosten und Nutzen der IT-Sicherheit, in MÖRIKE, M.; TEUFEL S.: Kosten & Nutzen von IT-Sicherheit in: HEILMANN, H. ET AL. (Hrsg.): HMD - Praxis der Wirtschaftsinformatik, Heft 248, dpunkt, Heidelberg, 2006.

FLEMING GRUBB, M.; CARTER, R.: Single Sign-On and the System Administrator, in Proceedings of the Twelfth Systems Administration Conference (LISA ‘98), Boston, 1998, http://www.usenix.com/publications/library/proceedings/lisa98/full_papers/grubb/grubb.pdf, abgerufen am: 21.01.2007.

FOLMER, E. [Software-Usability, 2005]: Software architecture analysis of usability, University Library Groningen, Groningen, 2005.

FREEMAN, T. [SCVP, 2007]: Server-based Certificate Validation Protocol (SCVP), ftp://ftp.rfc-editor.org/in-notes/internet-drafts/draft-ietf-pkix-scvp-31.txt, abgerufen am: 21.01.2007.

FUNK, P.; BLAKE-WILSON, S. [EAP-TTLS, 2006]: EAP Tunneled TLS Authentication Protocol Version 1 (EAP-TTLSv1), http://tools.ietf.org/wg/eap/draft-funk-eap-ttls-v1-01.txt, abgerufen am: 21.01.2007.

Future of Identity in the Information Society (FIDIS) Deliverables [FIDIS, 2007]: http://www.fidis.net/fidis-del, abgerufen am: 21.01.2007.

GADATSCH, A.; UEBELACKER, H. [Benutzbare-Sicherheit, 2004]: Wirtschaftlichkeitsbetrachtungen für IT-Security-Projekte, in MÖRIKE, M.; TEUFEL S.: Kosten & Nutzen von IT-Sicherheit in: HEILMANN, H. ET AL. (Hrsg.): HMD - Praxis der Wirtschaftsinformatik, Heft 248, dpunkt, Heidelberg, 2006.

GARMAN, J. [Kerberos, 2003]: Kerberos. The Definitive Guide, O'Reilly, Sebastopol, 2003.

GARRET, J. J. [Ajax, 2005]: Ajax: A New Approach To Web Applications, http://www.adaptivepath.com/publications/essays/archives/000385.php, abgerufen am 21.01.2007.

GARTNER: Password Reset: Self-Service That You Will Love [Gartner-Pwd-Reset, 2002]: http://www.gartner.com/DisplayDocument?ref=g_search&id=354760, http://www.passwordresearch.com/stats/study76.html, abgerufen am: 21.01.2007.

GEMPLUS [GEMPLUS, 2007]: ID and Security Solutions from Gemplus, http://www.gemplus.com/pss/id_security/enterprise/safesite/safesite_smartcards.html, abgerufen am: 21.01.2007.

GERD TOM MARKOTTEN, D. [Benutzbare-Sicherheit, 2004]: Benutzbare Sicherheit in informationstechnischen Systemen, RHOMBOS, Berlin, 2003.

GILB, T. [Competitive-Engineering, 2005]: Competitive Engineering, Elsevier, Burlington, 2005.

GORDON, L. A.; LOEB, M. P. [Cyber-Security, 2005]: Managing Cyber-Security Resources - A cost-benefit analysis, McGraw-Hill, New York et al., 2005.

GRAVES, M. [IDM-Failure, 2006]: Why Identity Management Projects Fail, http://sdiam.blogspot.com/2006/10/why-identity-management-projects-fail.html, abgerufen am: 21.01.2007.

GridShib [GridShib, 2007]: Integrating federated authorization infrastructure with Grid technology, http://gridshib.globus.org , abgerufen am: 21.01.2007.

GWDG-CA Ebene 2 User-CA. Anleitungen und Download [User-CA, 2007]: http://ca3.gwdg.de/download, abgerufen am: 21.01.2007.

HAGENHOFF, S.; GOOS, P.; SCHMALTZ, R. [Sicherheitsmodelle-Kooperationen, 2006]: Sicherheitsmodelle für Kooperationen, in: FERSTL, O. K. (Hrsg.): Wirtschaftsinformatik 2005, Physica-Verlag, Heidelberg, 2005.

HAGENHOFF, S.; SCHUMANN, M. [Mediaconomy, 2006]: Mediaconomy - Internetökonomie der Medienwirtschaft, in: IT -Information Technology Nr. 48, Oldenbourg, München, 2006.

HAMACHER, H. W.; KLAMROTH, K. [Netzwerkoptimierung, 2006]: Lineare Optimierung und Netzwerkoptimierung, 2. Auflage, Vieweg, Wiesbaden, 2006.

HAMACHER, H. W.; RUHE, G. [Multi-Criteria-Spanning-Tree, 1994]: On spanning tree problems with multiple objectives, in Annals of Operations Research, Springer, Berlin et al., 1994, http://www.springerlink.com/content/r81g0gvkw32wu841/fulltext.pdf, abgerufen am: 21.01.2007.

HARDT, D. [Identity20, 2007]: Identity 2.0, http://identity20.com, abgerufen am: 21.01.2007.

heimdal [heimdal, 2007]: http://www.pdc.kth.se/heimdal/, abgerufen am: 21.01.2007.

HERRMANN, V. [Pharming, 2007]: Pharming - Phishing mit Schleppnetz, http://www.aufrecht.de/4346.html, abgerufen am: 21.01.2007

HERWIG, V.; SCHLABITZ, L. [DirXMetaRole, 2004]: Unternehmensweites Berechtigungsmanagement, in KÖNIG, W. (Hrsg.): Wirtschaftsinformatik, 46. Jahrgang, Heft 4, Vieweg, Wiesbaden, 2004.

Higgins Trust Framework Project [Higgins, 2007]: http://www.eclipse.org/higgins, abgerufen am: 21.01.2007.

HOUSLEY, R. ET AL. [X509, 2002]: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 3280), ftp://ftp.rfc-editor.org/in-notes/rfc3280.txt, abgerufen am: 21.01.2007.

HURLEY, E. [SOX-IT-Sec, 2007]: Security and Sarbannes-Oxley, http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci929451,00.htm, abgerufen am 21.01.2007.

HUSEBY, S. H. [Web-Sicherheit, 2004]: Sicherheitsrisiko Web-Anwendung, dpunkt, Heidelberg, 2004.

IBM Web Services Security [WS-Sec, 2007]: http://www-128.ibm.com/developerworks/library/ws-secroad, abgerufen am: 21.01.2007.

ID-PKC [ID-PKC, 2007]: http://www.cesg.gov.uk/site/ast/index.cfm?menuSelected=3&displayPage=31, abgerufen am: 21.01.2007.

IEEE [8021X, 2004]: 802.1X Port-Based Network Access Control, New York, 2004.

International Grid Trust Federation (IGTF) [GRIDPMA, 2007]: The Grid's Policy Management Authority, http://www.gridpma.org, abgerufen am 21.01.2007.

Internet 2 Shibboleth [Shibboleth, 2007]: http://shibboleth.internet2.edu, abgerufen am: 21.01.2007.

ISO 9126 [ISO-9126, 2001]: Software Engineering - Product Quality, 2001, http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=22749&ICS1=35&ICS2=80&ICS3=, abgerufen am: 21.01.2007.

ISO 9241-11:1998 [ISO-9241-11, 1998]: Ergonomic requirements for office work with visual display terminals (VDTs) -- Part 11: Guidance on usability, 1998, http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=16883&showAllRelItems=y, abgerufen am: 21.01.2007.

JBoss-Portal [JBoss-Portal, 2007]: http://labs.jboss.com/portal/jbossportal, abgerufen am: 21.01.2007.

JOSEFSSON, S. ET AL. [PEAP, 2001]: Protected Extensible Authentication Protocol (PEAP), http://tools.ietf.org/html/draft-josefsson-pppext-eap-tls-eap-01, abgerufen am: 21.01.2007.

KENT, S. T.; MILLETT, L. I. [Privacy, 2003]: Who goes there? Authentication Through the Lens of Privacy, The National Academy Press, Washington D.C., 2003.

KENT, S.; SEO, K. [IPsec, 2005]: Security Architecture for the Internet Protocol, ftp://ftp.rfc-editor.org/in-notes/rfc4301.txt, abgerufen am: 21.01.2007.

KLÜNTER, D.; LASER, J. [OpenLDAP, 2003]: LDAP verstehen, OpenLDAP einsetzen. Grundlagen, Praxiseinsatz, Single Sign-On Systeme, dpunkt, Heidelberg, 2003.

KOCH, R. [Pareto-80-20, 2004]: Das 80/20 Prinzip. Mehr Erfolg durch weniger Aufwand, 2. Auflage, Campus Verlag, Frankfurt, 2004.

KOKE, H. (Hrsg.) [GÖ*-Hauptantrag, 2006]: GÖ* - Integriertes Informationsmanagement im heterogenen eScience-Umfeld: GÖ*-Hauptantrag für die DFG-Förderinitiative „Leistungszentren für Forschungsinformation“, GWDG, Göttingen, 2004.

KOKE, H. (Hrsg.) [GÖ*-Vorantrag, 2006]: GÖ* - Integriertes Informationsmanagement im heterogenen eScience-Umfeld: GÖ*-Vorantrag für die DFG-Förderinitiative „Leistungszentren für Forschungsinformation“, GWDG, Göttingen, 2004.

KOKE, H. [HRK, 2006]: HRK-Guidelines for Strategies to the Information and Communication Structure at Universities, in LILLEMAA, T. (Hrsg.): Proceedings of the 12th International Conference of European University Information Systems, University of Tartu, Tartu, 2006.

KOMAR, B. [MS-PKI, 2004]: Microsoft Windows Server 2003. PKI und Zertifikatsicherheit, Microsoft Press, Unterschleißheim, 2004.

KUPPINGER, M. [IDM-Erfolg, 2005]: Das erfolgreiche Identity Management-Projekt, Vortrag: IdM Day 2005, http://www.iam-wiki.org/Technologien%2C_Architekturen_und_Projektdurchf%C3%BChrung?action=AttachFile&do=get&target=IAM_ProjekteRichtigUmsetzen.pdf, abgerufen am: 21.01.2007.

KUPPINGER, M. [IDM-Trends, 2006]: Trends im Identity Management, Vortrag: IdM Day, 2006, http://www.iam-wiki.org/Der_Markt_des_Identity_Managements?action=AttachFile&do=get&target=KCP_Martin_Kuppinger_TrendsimIdM.pdf, abgerufen am 21.01.2007.

LANIT [LANIT, 2007]: http://soi.lanit-hrz.de/cms/de/lanit, abgerufen am: 21.01.2007.

LCG [LCG, 2007]: LCG - LHC Computing Grid Project, http://lcg.web.cern.ch/LCG, abgerufen am 21.01.2007.

Lenovo ThinkVantage Client Security Solution [Lenovo-CSS, 2007]: http://www.pc.ibm.com/europe/think/de/security.html?de&cc=de, abgerufen am: 21.01.2007.

Liberty: Specifications [Liberty, 2007]: http://www.projectliberty.org/liberty/specifications__1, abgerufen am: 21.01.2007.

LLOYD, B.; SIMPSON, W. [PPP-Authentication, 1992]: PPP Authentication Protocols (RFC 1334), ftp://ftp.rfc-editor.org/in-notes/rfc1334.txt, abgerufen am: 21.01.2007.

LUBICH, H. P. [Kosten-Nutzen-IT-Sicherheit, 2006]: IT-Sicherheit: Systematik, aktuelle Probleme und Kosten-Nutzen-Betrachtungen, in MÖRIKE, M.; TEUFEL S.: Kosten & Nutzen von IT-Sicherheit in: HEILMANN, H. ET AL. (Hrsg.): HMD - Praxis der Wirtschaftsinformatik, Heft 248, dpunkt, Heidelberg, 2006.

MediGRID [MediGRID, 2007]: MediGRID GRID-Computing für die Medizin und Lebenswissenschaften, http://www.medigrid.de, abgerufen am 21.01.2007.

MELNIKOV, A.; ZEILENGA, K. [SASL, 2006]: Simple Authentication and Security Layer (SASL) (RFC 4422), ftp://ftp.rfc-editor.org/in-notes/rfc4422.txt, abgerufen am: 21.01.2007.

MetaPass [MetaPass, 2007]: http://www.metapass.com/metapass, abgerufen am: 21.01.2007.

MEYBERG, K.; VACHENAUER, P. [Höhere-Mathematik-1, 1997]: Höhere Mathematik 1, 4. Auflage, Springer, Berlin, 1997.

MICHELA, F.; PALME, M. [Active-Directory, 1999]: Active Directory, Microsoft Press, Unterschleißheim, 1999.

MICROSOFT [CardSpace, 2007]: Introducing Windows CardSpace, http://msdn2.microsoft.com/en-us/library/aa480189.aspx, abgerufen am: 21.01.2007.

Microsoft Identity Integration Server [MIIS, 2007]: http://www.microsoft.com/windowsserversystem/miis2003/default.mspx, abgerufen am: 21.01.2007.

Microsoft WebParts [WebParts, 2007]:
http://www.microsoft.com/sharepoint/server/downloads/webparts/applications.asp, abgerufen am: 21.01.2007.

Microsoft Windows CardSpace [Microsoft-CardSpace, 2007]: http://cardspace.netfx3.com, abgerufen am: 21.01.2007.

Microsoft Windows Services for UNIX [SFU, 2007]: Microsoft Windows Services for UNIX, http://www.microsoft.com/technet/interopmigration/unix/sfu/default.mspx, abgerufen am: 21.01.2007.

Microsoft: Microsoft's Vision for an Identity Metasystem [Identity-Metasystem, 2005]:
http://msdn2.microsoft.com/en-us/library/ms996422.aspx, abgerufen am: 21.01.2007.

MIHALIK, A. D. [Athena, 1999]: Project Athena, http://www-tech.mit.edu/V119/N19/history_of_athe.19f.html, abgerufen am: 21.01.2007.

MITNICK, K. [Kunst-der-Täuschung, 2006]: Die Kunst der Täuschung, REDLINE, Heidelberg, 2006.

mod_auth_vas - Windows Integrated Authentication for Apache [VAS, 2007]:
http://rc.vintela.com/topics/mod_auth_vas/, abgerufen am: 21.01.2007.

MONROSE, F.; REITER M. K. [Graphical-Passwords, 2005]: Graphical Passwords, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, O'Reilly, Sebastopol, 2005.

MONROSE, F.; REITER, M. K. [Graphical-Passwords, 2005]: Graphical Passwords, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, O'Reilly, Sebastopol, 2005.

MOORE, G. E. [Moore, 1965]: Moore's Law,
http://www.intel.com/technology/mooreslaw/index.htm, abgerufen am: 21.01.2007.

MÖRIKE, M.; TEUFEL S. [HMD, 2006]: Kosten & Nutzen von IT-Sicherheit in: HEILMANN, H. ET AL. (Hrsg.): HMD - Praxis der Wirtschaftsinformatik, Heft 248, dpunkt, Heidelberg, 2006.

Mozilla Password Manager [Password-Manager, 2007]: http://www.mozilla.org/projects/security/pki/psm/help_21/using_priv_help.html, abgerufen am: 21.01.2007.

Mozilla: Integrated Auth [Mozilla-NTLM, 2005]: Integrated Auth, http://www.mozilla.org/projects/netlib/integrated-auth.html, abgerufen am: 21.01.2007.

MYERS ET AL. [OCSP, 1999]: X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol - OCSP (RFC 2560), ftp://ftp.rfc-editor.org/in-notes/rfc2560.txt, abgerufen am: 21.01.2007.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY [FIPS, 2007]: Federal Information Processing Standards Publications, http://www.itl.nist.gov/fipspubs, abgerufen am: 21.01.2007.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY [FIPS113, 1985]: Federal Information Processing Standards Publication 113 - Computer Data Authentication, http://www.itl.nist.gov/fipspubs/fip113.htm, abgerufen am: 21.01.2007.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY [FIPS140-2, 1994]: Federal Information Processing Standards Publication 140-2 - Security Requirements for Cryptographic Modules, http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf, abgerufen am: 21.01.2007.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY [FIPS180-2, 2002]: Federal Information Processing Standards Publication 180-2 - Secure Hash Standard, http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf, abgerufen am: 21.01.2007.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY [FIPS181, 1993]: Federal Information Processing Standards Publication 181 - Automated Password Generator, http://www.itl.nist.gov/fipspubs/fip181.htm, abgerufen am 21.01.2007.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY [FIPS186-2, 1994]: Federal Information Processing Standards Publication 186-2 - Digital Signature Standard, http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf, abgerufen am 21.01.2007.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY [FIPS190, 1994]: Federal Information Processing Standards Publication 190 - Guideline for the Use of Advanced Authentication Technology Alternatives, http://www.itl.nist.gov/fipspubs/fip190.htm, abgerufen am: 21.01.2007.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY [FIPS196, 1997]: Federal Information Processing Standards Publication 196 - Entity Authentication Using Public Key Cryptography, http://csrc.nist.gov/publications/fips/fips196/fips196.pdf, abgerufen am: 21.01.2007.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY [FIPS197, 2001]: Federal Information Processing Standards Publication 197 - Advanced Encryption Standard, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, abgerufen am: 21.01.2007.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY [FIPS198, 2002]: Federal Information Processing Standards Publication 198 - The Keyed-Hash Message Authentication Code, http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf, abgerufen am: 21.01.2007.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY [FIPS201-1, 2006]: Federal Information Processing Standards Publication 201-1 - Personal Identity Verification for Federal Employees and Contractors, http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf, abgerufen am: 21.01.2007.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY [FIPS46-3, 1999]: Federal Information Processing Standards Publication 46-3 - Data Encryption Standard, http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf, abgerufen am: 21.01.2007.

NETSCAPE [SSL, 1996]: SSL 3.0 Specification,http://wp.netscape.com/eng/ssl3, abgerufen am: 21.01.2007.

NEUMAN, C. ET AL. [Kerberos, 2005]: The Kerberos Network Authentication Service (V5) (RFC 4120), ftp://ftp.rfc-editor.org/in-notes/rfc4120.txt, abgerufen am: 21.01.2007.

NIELSEN, J. [Usability-Engineering, 1993]: Usability Engineering, Academic Press, San Diego, 1993.

NISO: Ranking of Authentication and Access Methods Available to the Metasearch Environment [NISO, 2005]: http://www.niso.org/standards/resources/MI-Access_Management.pdf, abgerufen am: 21.01.2007.

NIST: Role Based Access Control (RBAC) [RBAC, 2007]: http://csrc.nist.gov/rbac, abgerufen am: 21.01.2007.

Novell Access Manager [Novell-Access-Manager, 2007]: http://www.novell.com/products/accessmanager, abgerufen am: 21.01.2007.

Novell Directory Service and Identity Management: eDirectory [eDirectory, 2007]: http://www.novell.com/products/edirectory/, abgerufen am: 21.01.2007.

Novell Entitlements [Entitlements, 2007]: http://www.novell.com/documentation/idm/index.html?page=/documentation/idm/admin/data/am46smm.html, abgerufen am: 21.01.2007.

Novell Identity Manager [IDM, 2007]: http://www.novell.com/products/identitymanager/, abgerufen am: 21.01.2007.

Novell SecureLogin [SecureLogin, 2007]: http://www.novell.com/products/securelogin, abgerufen am: 21.01.2007.

Novell SecureLogin Technical Whitepaper [SecureLogin-Whitepaper, 2007]: http://www.novell.de/prodinfos/pdf/secure_login_tech_wp_e.pdf, abgerufen am: 21.01.2007.

Novell Virtual Directory Services [NVDS, 2007]: http://www.novell.com/collateral/4621416/4621416.pdf, abgerufen am: 21.01.2007.

Novell-UserApplication [UserApplication, 2007]: http://www.novell.com/products/identitymanager, abgerufen am: 21.01.2007.

Novell-UserApplication-Workflow [UserApp-Workflow, 2007]: http://www.novell.com/products/identitymanager/features.html, abgerufen am: 21.01.2007.

NTLM auth module for Apache/Unix [Apache-NTLM, 2007]: http://modntlm.sourceforge.net, abgerufen am: 21.01.2007.

OASIS Security Services (SAML) [SAML, 2007]: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security, abgerufen am: 21.01.2007.

OASIS: SPML [SPML, 2007]: http://www.oasis-open.org/home/index.php, abgerufen am: 21.01.2007.

OASIS: XACML [XACML, 2007]: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml, abgerufen am: 21.01.2007.

OECHSLIN, P. [RainbowTables, 2003]: Making a Faster Cryptoanalytical Time-Memory Trade-Off, Vortrag: Advanced in Cryptology – CRYPTO 2003, http://lasecwww.epfl.ch/~oechslin/publications/crypto03.pdf, abgerufen am: 21.01.2007.

OpenCA [OpenCA, 2007]: http://www.openca.org, abgerufen am: 21.01.2007.

OpenID: an actually distributed identity system [OpenID, 2007]: http://openid.net, abgerufen am: 21.01.2007

OpenSC [OpenSC, 2007]: http://www.opensc-project.org, abgerufen am: 21.01.2007.

OpenSSL [OpenSSL, 2007]: http://www.openssl.org, abgerufen am: 21.01.2007.

Oracle Virtual Directory [OVDS, 2007]: http://www.oracle.com/technology/products/id_mgmt/ovds/index.html, abgerufen am: 21.01. 2007.

OSIS: The Open-Source Identity System [OSIS]: http://osis.netmesh.org/wiki/Main_Page, abgerufen am: 21.01.2007.

pam_ldap [pam_ldap, 2007]: http://www.padl.com/OSS/pam_ldap.html, abgerufen am: 21.01.2007.

pam-krb5 [pam-krb5, 2007]: http://sourceforge.net/projects/pam-krb5, abgerufen am: 21.01.2007.

passfaces [passfaces, 2007]: passfaces, http://www.realuser.com, abgerufen am: 21.01.2007.

Password Safe [Password-Safe, 2007]: http://passwordsafe.sourceforge.net, abgerufen am: 21.01.2007.

Password Sitter [Password-Sitter, 2007]: http://www.passwordsitter.de, abgerufen am: 21.01.2007.

Password-Research-Institute [Password-Research-Institute, 2005] Password Research Institute, http://www.passwordresearch.com/about.html, abgerufen am 21.01.2007.

PEACOCK, A.; KE, X.; WILKERSON, M. [Typing, 2005]: Identifying Users from Their Typing Patterns, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, O'Reilly, Sebastopol, 2005.

PEIKARI, C.; CHUWAKIN, A. [SecurityWarrior, 2004]: Kenne Deinen Feind, O'Reilly, Köln, 2004.

PELZL, J.; GÖRTZ H. [Crypto-FPGA, 2006]: Cryptoanalysis with a cost-optimized FPGA cluster, Vortrag: UCLA IPAM Workshop IV, http://www.copacobana.org/paper/IPAM2006_slides.pdf, abgerufen am: 21.01.2007.

pGINA [pGINA, 2007]: http://www.pgina.org, abgerufen am: 21.01.2007.

pGINA PAM [pGINA-PAM, 2007]: http://www.pgina.org/?page_id=8, abgerufen am: 21.01.2007.

PIAZZALUNGE, U.; SALVANESCHI, P.; COFFETTI, P. [Usability-Token, 2005]: The Usability of Security Devices, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, O'Reilly, Sebastopol, 2005.

pkinit for heimdal [pkinit-heimdal, 2007]: http://people.su.se/~lha/patches/heimdal/pkinit, abgerufen am: 21.01.2007.

POHLMAN, M. [Metadirectory, 2003]: LDAP Metadirectory. Provisioning Methodology, iUniverse, Lincoln, 2003.

Public-Key Infrastructure (X.509) (pkix) Charter [pkix, 2007]: http://www.ietf.org/html.charters/pkix-charter.html, abgerufen am: 21.01.2007.

RENAUD, K. [Eval-Authentication, 2005]: Evaluating Authentication Mechanisms, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, O'Reilly, Sebastopol, 2005.

RENAUD, K. [Quantify-Authentication-Quality, 2003]: Quantifying the Quality of Web-Authentication Mechanisms. A Usability Perspektive, in: Jounal of Web Engineering 3(2), Rinton Press, 2003, http://www.dcs.gla.ac.uk/~karen/Papers/j.pdf, Abgerufen am: 21.01.2007.

RESCORLA, E. [HTTPS, 2000]: HTTP over TLS (RFC 2818), ftp://ftp.rfc-editor.org/in-notes/rfc2818.txt, abgerufen am: 21.01.2007.

RIEGER, S. ET AL. [Self-Service-PKI, 2007]: Self-Service PKI-Lösungen für eScience, in Paulsen, C. (Hrsg.): Sicherheit in vernetzten Systemen. 13. Workshop, DFN-CERT, Hamburg, 2006.

RILEY, S. [Pwd-Security, 2006]: Password Security: What Users Know and What They Actually Do, http://psychology.wichita.edu/surl/usabilitynews/81/Passwords.htm, abgerufen am: 21.01.2007.

RIVEST, R. [MD4, 1992]: The MD4 Message-Digest Algorithm (RFC 1320), ftp://ftp.rfc-editor.org/in-notes/rfc1320.txt, abgerufen am: 21.01.2007.

RIVEST, R. [MD5, 1992]: The MD5 Message-Digest Algorithm (RFC 1321), ftp://ftp.rfc-editor.org/in-notes/rfc1321.txt, abgerufen am: 21.01.2007.

RIVEST, R. [RC2, 1998]: A Description of the RC2(r) Encryption Algorithm (RFC2268), ftp://ftp.rfc-editor.org/in-notes/rfc2268.txt, abgerufen am: 21.01.2007.

ROMMELFANGER, H. J.; EICKEMEIER, S. H. [Entscheidungsfindung, 2002]: Entscheidungstheorie. Klassische Konzepte und Fuzzy-Erweiterungen, Springer, Berlin et al., 2002.

ROSS, S. [inkblots, 2007]: Is It Just My Imagination? (Inkblots), http://research.microsoft.com/displayArticle.aspx?id=417, abgerufen am: 21.01.2007.

RSA [RSA-Challenge, 2007]: The RSA Challenge Numbers, http://www.rsasecurity.com/rsalabs/node.asp?id=2093, abgerufen am: 21.01.2007.

RSA SecureID [RSA, 2007]: RSA SecureID Authentication, http://www.rsasecurity.com/node.asp?id=1156, abgerufen am: 21.01.2007.

RSA SECURITY INC. [RSA-Passwords, 2006]: The 2nd Annual RSA Security Password Management Survey, http://www.rsasecurity.com/node.asp?id=3124, abgerufen am: 21.01.2007.

RSA: Public-Key Cryptography Standards (PKCS) [PKCS, 2007]: http://www.rsasecurity.com/rsalabs/node.asp?id=2124, abgerufen am: 21.01.2007.

Safehaus penrose [penrose, 2007]: http://docs.safehaus.org/display/PENROSE/Home;jsessionid=864377D9232CB9CDEB3D7CBEE0BA6A22, abgerufen am: 21.01.2007.

SafeNet [SafeNet, 2004]: Annual Password Survey Results, http://www.safenet-inc.com/pwsurvey04, abgerufen am 21.01.2007.

SAMAR, V.; CHARLIE, L. [PAM, 1996]: Making Login Services Independent of Authentication Technologies (PAM), http://www.sun.com/software/solaris/pam/pam.external.pdf , abgerufen am: 21.01.2007

SANTESSON, S.; HOUSLEY, R.; FREEMAN, T. [Logotypes, 2004]: Internet X.509 Public Key Infrastructure: Logotypes in X.509 Certificates, ftp://ftp.rfc-editor.org/in-notes/rfc3709.txt, abgerufen am: 21.01.2007.

SASSE, M. A.; FLECHAIS, I. [Usable-Security, 2005]: Usable Security. Why Do We Need It? How Do We Get It?, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, O'Reilly, Sebastopol, 2005.

SCHMIDT, J. [Windows-Sec, 2001]: Windows 2000 Security. Kryptographie, Kerberos, Authentifizierung, Markt+Technik, München, 2001.

SCHNEIER, B. [Beyond-Fear, 2003]: Beyond Fear, Copernicus Books, New York, 2003.

SCHNEIER, B. [Schneier-Crypto, 1996]: Angewandte Kryptographie, Addison-Wesley, Bonn et al., 1996.

SCHNEIER, B. [Secrets-And-Lies, 2004]: Secrets & Lies, Wiley, Indiana, 2004.

SCHULTZ, A. [Phishing, 2006]: http://www.medien-internet-und-recht.de/volltext.php?mir_dok_id=314, Phishing for financial agents oder die Mär vom schnellen Geld, abgerufen am: 21.01.2007.

SCHUMANN, M. ET AL. [DRM, 2004]: Digital Rights Management - Technologien, in Das Wirtschaftsstudium Nr. 5, 2004.

SCHUMANN, M. ET AL. [Workflow-Web-Services, 2003]: Spezifikation und Abwicklung von Workflows auf Basis von Web-Services, in FRÖSCHLE, H. P.: Kosten & Nutzen von IT-Sicherheit in: HEILMANN, H. ET AL. (Hrsg.): HMD - Praxis der Wirtschaftsinformatik, Heft 234, dpunkt, Heidelberg, 2003.

SCHUMANN, M.; RAWOLLE, J.; ADE, J. [XML, 2002]: Informationen im Internet: XML als Integrationstechnologie, in Das Wirtschaftsstudium Nr. 8-9, 2002.

sciFLT [sciFLT, 2007]: http://es.geocities.com/jaime_urzua/sciFLT/sciflt.html, abgerufen am: 21.01.2007.

scilab [scilab, 2007]: http://www.scilab.org, abgerufen am: 21.01.2007.

Siemens DirX [DirX, 2007]: http://www.siemens.com/index.jsp?sdc_p=ft3ml0s4u0o1181191i1345494pHPcz3&sdc_bcpath=1180841.s_4,&sdc_sid=2450758676&, abgerufen am: 21.01.2007.

SIMPSON, W. [CHAP, 1996]: PPP Challenge Handshake Authentication Protocol (RFC 1994), ftp://ftp.rfc-editor.org/in-notes/rfc1994.txt, abgerufen am: 21.01.2007.

SIMPSON, W. [PPP, 1994]: The Point-to-Point Protocol (PPP) (RFC 1661), ftp://ftp.rfc-editor.org/in-notes/rfc1661.txt, abgerufen am: 21.01.2007.

SMITH, R. E. [Authentication, 2002]: Authentication. From Passwords to Public Keys, Addison-Wesley, Boston et al., 2002.

STROBEL, S. [IPS, 2004]: Intrusion Detection und Intrusion Prevention, in MÖRIKE, M.: Kosten & Nutzen von IT-Sicherheit in: HEILMANN, H. ET AL. (Hrsg.): HMD - Praxis der Wirtschaftsinformatik, Heft 236, dpunkt, Heidelberg, 2004.

SUHL, L.; MELLOULI, T. [Optimierungssysteme, 2006]: Optimierungssysteme, Springer, Berlin, 2006.

Sun JAAS [JAAS, 2007]: http://java.sun.com/products/jaas, abgerufen am: 21.01.2007.

Sun Java Access Manager [Sun-Access-Manager, 2007]: http://www.sun.com/software/products/access_mgr, abgerufen am: 21.01.2007.

Sun Java System Directory Server Enterprise Edition [Sun-Directory, 2007]: http://www.sun.com/software/products/directory_srvr_ee/index.xml , abgerufen am: 21.01.2007.

Sun JSR-168 [JSR-168, 2003]: http://jcp.org/en/jsr/detail?id=168, abgerufen am: 21.01.2007.

SURANTI, S.; MUCKIN, M. [MS-SPNEGO, 2002]: http-Based Cross-Plattform Authentication via the Negotiate Protocol, http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnsecure/html/http-sso-1.asp, abgerufen am: 21.01.2007.

SXIP [SXIP, 2007], Sxip Identity, http://www.sxip.com; http://www.sxip.org, abgerufen am 21.01.2007.

Sxip Networks [SXIP-2, 2007]: SXIP 2.0 Overview, http://www.sxip.net/downloads/sxip2-overview.pdf, 21.01.2007.

TAYLOR, J. [e-Science, 2000]: e-Science – First phase of the Programme, http://www.rcuk.ac.uk/escience/news/firstphase.htm, abgerufen am: 21.01.2007.

TextGrid [TextGrid, 2007]: TextGrid Modulare Plattform für verteilte und kooperative wissenschaftliche Textdatenverarbeitung - ein Community-Grid für die Geisteswissenschaften, http://www.textgrid.de, abgerufen am 21.01.2007.

Thawte [Thawte, 2007]: http://www.thawte.com, abgerufen am: 21.01.2007.

TrustCenter [TrustCenter, 2007]: http://www.trustcenter.de, abgerufen am: 21.01.2007.

Trusted Copmputing Group (TCG) [TCG, 2007]: https://www.trustedcomputinggroup.org/home, abgerufen am: 21.01.2007.

TURAU, V. [Graphentheorie, 1996]: Algorithmische Graphentheorie, Addison-Wesley, Bonn et al., 1996.

UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN [IuKDG, 2007]: Die wichtigsten Bestimmungen des Informations- und Kommunikationsdienste-Gesetzes (IuKDG), http://www.datenschutzzentrum.de/material/themen/multimed/index.htm#3, abgerufen am: 21.01.2007.

UNITED STATES OF AMERICA [SOX, 2002]: One Hundred Seventh Congress of the United States of America - „Sarbanes-Oxley-Act“, http://www.law.uc.edu/CCL/SOact/soact.pdf, abgerufen am: 21.01.2007.

VeriSign [VeriSign, 2007]: http://www.verisign.com, abgerufen am: 21.01.2007.

Vgl. DUSSE, S. ET AL. [S/MIME, 1998]: S/MIME Version 2 Message Specification (RFC 2311), ftp://ftp.rfc-editor.org/in-notes/rfc2311.txt, abgerufen am: 21.01.2007.

Vgl. JA-SIG Central Authentication Service (CAS) [CAS, 2007]: http://www.ja-sig.org/products/cas/index.html, abgerufen am: 21.01.2007.

WALTHER, H. [Identity-Management, 2006]: Identity Management, in SAUERBURGER, H. (Hrsg.): Open-Source-Software in: HEILMANN, H. ET AL. (Hrsg.): HMD - Praxis der Wirtschaftsinformatik, Heft 238, dpunkt, Heidelberg, 2004.

WANG, X.; YAO, A. C.; YAO, F. [SHA1, 2005]: Cryptoanalysis on SHA-1, Vortrag: NIST Hash Function Workshop. First Workshop, http://csrc.nist.gov/pki/HashWorkshop/2005/Oct31_Presentations/Wang_SHA1-New-Result.pdf, abgerufen am: 21.01.2007.

WEISSTEIN, E. W. [RSA-640, 2005]: RSA-640 Factored, http://mathworld.wolfram.com/news/2005-11-08/rsa-640, abgerufen am: 21.01.2007.

What is SESAME [SESAME, 2007], https://www.cosic.esat.kuleuven.ac.be/sesame/html/sesame_what.html, abgerufen am: 21.01.2007.

WILLEMSON, J. [Gordon-Loeb-Schwächen, 2006]: On the Gordon & Loeb Model for Information Security, Vortrag: The Fifth Workshop on the Economics of Information Security (WEIS 2006), http://weis2006.econinfosec.org/docs/12.pdf, abgerufen am: 21.01.2007.

WINDEMANN, P.; SCHLIENGER, T.; TEUFEL, S. [Messung-Informationssicherheit, 2006]: Messung der Informationssicherheit auf der Ebene der Sicherheitspolitik in MÖRIKE, M.; TEUFEL S.: Kosten & Nutzen von IT-Sicherheit in: HEILMANN, H. ET AL. (Hrsg.): HMD - Praxis der Wirtschaftsinformatik, Heft 248.

WINDLEY, P. J. [Digital-Identity, 2005]: Digital Identity, O'Reilly, Sebastopol, 2005.

Word lists [word-list, 2007]: http://www.word-list.com, abgerufen am: 21.01.2007.

X/Open Single Sign-on Service (XSSO) - Pluggable Authentication Modules [XSSO, 1997]: http://www.opengroup.org/onlinepubs/008329799/front.htm, abgerufen am: 21.01.2007.

YAN, J ET AL. [Memorability-Passwords, 2005]: The Memorability and Security of Passwords, in CRANOR, L. F.; GARFINKEL, S.: Security and Usability. Designing Secure Systems That People Can Use, O'Reilly, Sebastopol, 2005.

ZADEH, L. A. [Fuzzy-Sets, 1965]: Fuzzy Sets, http://www-bisc.cs.berkeley.edu/zadeh/papers/Fuzzy%20Sets-1965.pdf, abgerufen am: 21.01.2007.

ZEILENGA, K. [LDAP, 2006]: Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map (RFC 4510), ftp://ftp.rfc-editor.org/in-notes/rfc4510.txt, abgerufen am: 21.01.2007.

ZHU, L.; TUNG, B. [PKINIT, 2006]: Public Key Cryptography for Initial Authentication in Kerberos, ftp://ftp.rfc-editor.org/in-notes/rfc4556.txt, abgerufen am: 21.01.2007.

ZIMMERMANN, H. J.; LEHMANN, I.; WEBER, R. [Fuzzy-Set-Theory, 1991]: Fuzzy set theory, in OR Spectrum, Springer, Berlin et al., 1991, http://www.springerlink.com/content/q63np6p5v613v262/fulltext.pdf, abgerufen am: 21.01.2007.

ZKI [ZKI, 2007]: https://www.zki.de, abgerufen am: 21.01.2007.

Göttinger Wirtschaftsinformatik

Herausgeber: Prof. Dr. J. Biethahn • Prof. Dr. M. Schumann

Band 31: Dr. rer. pol. Christian Stummeyer
Integration von Simulationsmethoden und hochintegrierter betriebswirtschaftlicher PPS-Standardsoftware im Rahmen eines ganzheitlichen Entwicklungsansatzes
ISBN 3-89712-874-8

Band 32: Dr. rer. pol. Stefan Wegert
Gestaltungsansätze zur IV-Integration von elektronischen und konventionellen Vertriebsstrukturen bei Kreditinstituten
ISBN 3-89712-924-8

Band 33: Dr. rer. pol. Ernst von Stegmann und Stein
Ansätze zur Risikosteuerung einer Kreditversicherung unter Berücksichtigung von Unternehmensverflechtungen
ISBN 3-89873-003-4

Band 34: Dr. rer. pol. Gerald Wissel
Konzeption eines Managementsystems für die Nutzung von internen sowie externen Wissen zur Generierung von Innovationen
ISBN 3-89873-194-4

Band 35: Dr. rer. pol. Wolfgang Greve-Kramer
Konzeption internetbasierter Informationssysteme in Konzernen
Inhaltliche, organisatorische und technische Überlegungen zur internetbasierten Informationsverarbeitung in Konzernen
ISBN 3-89873-207-X

Band 36: Dr. rer. pol. Tim Veil
Internes Rechnungswesen zur Unterstützung der Führung in Unternehmensnetzwerken
ISBN 3-89873-237-1

Band 37: Dr. rer. pol. Mark Althans
Konzeption eines Vertriebscontrolling-Informationssystems für Unternehmen der liberalisierten Elektrizitätswirtschaft
ISBN 3-89873-326-2

Band 38: Dr. rer. pol. Jörn Propach
Methoden zur Spielplangestaltung öffentlicher Theater
Konzeption eines Entscheidungsunterstützungssystems auf der Basis Evolutionärer Algorithmen
ISBN 3-89873-496-X

Cuvillier Verlag Göttingen

Nonnenstieg 8 • 37075 Göttingen

Göttinger Wirtschaftsinformatik

Herausgeber: Prof. Dr. J. Biethahn • Prof. Dr. M. Schumann

Band 39: Dr. rer. pol. Jochen Heimann
DV-gestützte Jahresabschlußanalyse
Möglichkeiten und Grenzen beim Einsatz computergeschützter Verfahren zur Analyse und Bewertung von Jahresabschlüssen
ISBN 3-89873-499-4

Band 40: Dr. rer. pol. Patricia Böning Spohr
Controlling für Medienunternehmen im Online-Markt
Gestaltung ausgewählter Controllinginstrumente
ISBN 3-89873-677-6

Band 41: Dr. rer. pol. Jörg Koschate
Methoden und Vorgehensmodelle zur strategischen Planung von Electronic-Business-Anwendungen
ISBN 3-89873-808-6

Band 42: Dr. rer. pol. Yang Liu
A theoretical and empirical study on the data mining process for credit scoring
ISBN 3-89873-823-X

Band 43: Dr. rer. pol. Antonios Tzouvaras
Referenzmodellierung für Buchverlage
Prozess- und Klassenmodelle für den Leistungsprozess
ISBN 3-89873-844-2

Band 44: Dr. rer. pol. Marina Nomikos
Hemmnisse der Nutzung Elektronischer Marktplätze aus der Sicht von kleinen und mittleren Unternehmen eine theoriegeleitete Untersuchung
ISBN 3-89873-847-7

Band 45: Dr. rer. pol. Boris Fredrich
Wissensmanagement und Weiterbildungsmanagement
Gestaltungs- und Kombinationsansätze im Rahmen einer lernenden Organisation
ISBN 3-89873-870-1

Cuvillier Verlag Göttingen

Nonnenstieg 8 • 37075 Göttingen

Göttinger Wirtschaftsinformatik

Herausgeber: Prof. Dr. J. Biethahn • Prof. Dr. M. Schumann

Band 46: Dr. rer. pol. Thomas Arens
Methodische Auswahl von CRM Software
Ein Referenz-Vorgehensmodell zur methodengestützten Beurteilung und Auswahl von Customer Relationship Management Informationssystemen
ISBN 3-86537-054-3

Band 47: Dr. rer. pol. Andreas Lackner
Dynamische Tourenplanung mit ausgewählten Mataheuristiken
Eine Untersuchung am Beispiel des kapazitätsrestriktiven dynamischen Tourenplanungsproblems mit Zeitfenstern
ISBN 3-86537-084-5

Band 48: Dr. rer. pol. Tobias Behrensdorf
Service Engineering in Versicherungsunternehmen
unter besonderer Berücksichtigung eines Vorgehensmodells zur Unterstützung durch Informations- und Kommunikationstechnologien
ISBN 3-86537-110-8

Band 49: Dr. rer. pol. Michael Range
Aufbau und Betrieb konsumentenorientierter Websites im Internet
Vorgehen und Methoden unter besonderer Berücksichtigung der Anforderungen von kleinen und mittleren Online-Angeboten
ISBN 3-86537-490-5

Band 50: Dr. rer. pol. Gerit Grübler
Ganzheitliches Multiprojektmanagement
Mit einer Fallstudie in einem Konzern der Automobilzulieferindustrie
ISBN 3-86537-544-8

Band 51: Dr. rer. pol. Birte Pochert
Konzeption einer unscharfen Balanced Scorecard
Möglichkeiten der Fuzzyfizierung einer Balanced Scorecard zur Unterstützung des Strategischen Managements
ISBN 3-86537-671-1

Cuvillier Verlag Göttingen

Nonnenstieg 8 • 37075 Göttingen

Göttinger Wirtschaftsinformatik

Herausgeber: Prof. Dr. J. Biethahn • Prof. Dr. M. Schumann

Band 52: Dr. rer. pol. Manfred Peter Zilling

Effizienztreiber innovativer Prozesse für den Automotive Aftermarket

Implikationen aus der Anwendung von kollaborativen und integrativen Methoden des Supply Chain Managements

ISBN 3-86537-790-4

Band 53: Dr. rer. pol. Mike Hieronimus

Strategisches Controlling von Supply Chains

Entwicklung eines ganzheitlichen Ansatzes unter Einbeziehung der Wertschöpfungspartner

ISBN 3-86537-799-8

Band 54: Dijana Bergmann

Datenschutz und Datensicherheit unter besonderer Berücksichtigung des elektronischen Geschäftsverkehrs zwischen öffentlicher Verwaltung und privaten Unternehmen

ISBN 3-86537-894-3

Band 55: Jan Eric Borchert

Operatives Innovationsmanagement in Unternehmensnetzwerken
Gestaltung von Instrumenten für Innovationsprojekte

ISBN 3-86537-984-2

Band 56: Andre Daldrup

Konzeption eines integrierten IV-Systems zur ratingbasierten Quantifizierung des regulatorischen und ökonomischen Eigenkapitals im Unternehmenskreditgeschäft unter Berücksichtigung von Basel II

ISBN 978-3-86727-189-9

Cuvillier Verlag Göttingen

Nonnenstieg 8 • 37075 Göttingen

Göttinger Wirtschaftsinformatik

Herausgeber: Prof. Dr. J. Biethahn • Prof. Dr. M. Schumann

Band 57: Thomas Diekmann

Ubiquitous Computing-Technologien im betrieblichen Umfeld

Technische Überlegungen, Einsatzmöglichkeiten und Bewertungsansätze

ISBN 978-3-86727-194-3

Band 58: Lutz Seidenfaden

Ein Peer-to-Peer-basierter Ansatz zur digitalen Distribution wissenschaftlicher Informationen

ISBN 978-3-86727-329-9

Cuvillier Verlag Göttingen

Nonnenstieg 8 • 37075 Göttingen