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.