Ein Architektur-Modell für anonyme Autorisierungen und Überwachungsdaten *

Ulrich Flegel
Universität Dortmund
D-44221 Dortmund
ulrich.flegel@udo.edu

Zusammenfassung: Eine digitale Welt benötigt Systeme, welche die Sicherheitsanforderungen von Dienstleistern und Nutzern gleichermaßen berücksichtigen. Dieser Beitrag betrachtet bei sicheren Autorisierungen die Anforderungen hinsichtlich Zurechenbarkeit und Anonymität mit Bezug auf eine Sicherheitsüberwachung bei der Diensterbringung. Hierfür wird ein Architektur-Modell für sichere anonyme Autorisierungen entwickelt, anhand dessen Eigenschaften konkreter Anonymitäts-Technologien systematisch vergleichbar werden. Es zeigt sich, daß Anonymität und Zurechenbarkeit bei der Sicherheitsüberwachung mit technischer Zweckbindung praktikabel nur durch die Pseudonymisierung bereits erhobener Überwachungsdaten machbar ist. Bekannte Ansätze für die Anonymisierung von Überwachungsdaten werden vorgestellt und verglichen.

1 Vom Realen des Digitalen

Sicherheitsmaßnahmen in der digitalen Welt sind häufig bereits vorhandenen Sicherheitsmaßnahmen der realen Welt nachempfunden. Das mag daran liegen, daß Vertrauen letztlich stets in der realen Welt gegründet ist und Sicherheitsmaßnahmen gerade bei fehlendem Vertrauen der Akteure notwendig sind. Die Betrachtung von Vertrauensverhältnissen und Sicherheitsmaßnahmen in der realen Welt hilft uns im Folgenden, die vorgeschlagenen Modelle zu verstehen. Die Modelle wiederum helfen uns, vorhandene Technologien einzuordnen, sie gegeneinander abzugrenzen und auf ihre Eigenschaften zu schließen. Der Bogen wird hier bewußt weit gespannt, aber die Modelle, ihre Eigenschaften und die Technologien werden im Folgenden stets im Hinblick auf Überwachungsdaten und deren Anonymisierung betrachtet.

1.1 Ein Besuch im Zoo

Wie wir in der realen Welt mit Vertrauen umgehen, läßt sich am Beispiel eines Studierenden zeigen, der den Zoo besuchen möchte. Der Zoo tritt hier als Dienst(leister) auf und bietet Studierenden kostenlosen Eintritt. Nicht-Studierende könnten versuchen, sich einen geldwerten Vorteil zu verschaffen, indem sie an der Zoo-Kasse lügen und sich in ihrer Eigenschaft als *Studierende* vorstellen. Der Vorteil des Kunden ist gleichzeitig der nachteilhafte Ausfall seines Eintrittsgeldes für die Zoo-Kasse. Daher wird an der Zoo-Kasse den potentiellen Kunden hinsichtlich der Aussage über die Eigenschaft *Studierender* nicht vertraut. Es reicht an der Zoo-Kasse daher nicht, zu sagen man habe die Eigenschaft *Studierender*. Der Besitz dieser Eigenschaft kann vom Kassenpersonal nicht vor Ort geprüft werden. Stattdessen wird verlangt, den Studierenden-Ausweis vorzuzeigen. Der Studierenden-Ausweis fungiert als beglaubigte Eigenschaftsaussage, indem er den Namen des Aussage-Subjekts der Eigenschaft *Studierender* zuordnet. Als beglaubigenden und verantwortlichen Agenten für eine korrekte Zuordnung vermerkt die Eigenschaftsaussage den Namen der Universität. Das eingebettete Lichtbild beweist, daß

*Die beschriebenen Arbeiten werden derzeit zum Teil von der Deutschen Forschungsgemeinschaft gefördert unter Bi 311/10-2.

der Subjekt-Name tatsächlich die an der Zoo-Kasse stehende Person bezeichnet. Schließlich enthält die Eigenschaftsaussage noch Informationen zur Gültigkeit, etwa nahezu unfälschbare Echtheitsmerkmale und eine Geltungsdauer. Die Zoo-Kasse akzeptiert diese beglaubigte Eigenschaftsaussage, wenn gilt: Es wurde beschlossen, der vermerkten Universität als Agent für solche Beglaubigungen zu vertrauen, das Lichtbild "paßt" zur vorlegenden Person, der Studierenden-Ausweis ist noch nicht abgelaufen und sieht "echt" aus.

Wenn die Zoo-Kasse den Studierenden-Ausweis akzeptiert, autorisiert sie die vorlegende Person, den Zoo-Eingang zu passieren. Die Person erhält damit die dienstspezifische Eigenschaft *Zoo-Eintritts-Berechtigter*. Am Zoo-Eingang reicht es aber nicht zu sagen, man habe die Eigenschaft *Zoo-Eintritts-Berechtigter*. Das fehlende Vertrauen ist hier dadurch begründet, daß man sich durch Lügen den Eintritt erschleichen könnte. Deswegen stellt die Zoo-Kasse eine Autorisierung in Form eines Eintritts-Tickets aus. Diese Autorisierung enthält eine dem Kunden zugeordnete Ticket-Nummer, es ist vermerkt, daß die Autorisierung zum *Zoo-Eintritt berechtigt*, von welcher Kasse sie ausgestellt wurde, und sie trägt Gültigkeitsinformationen wie eine Geltungsdauer sowie schwer fälschbare Echtheitsmerkmale[1]. Am Zoo-Eingang wird das Eintritts-Ticket akzeptiert, wenn gilt: Der aufgedruckten Kasse wird vertraut, Tickets nur an Berechtigte auszustellen, die Ticket-Nummer "sieht plausibel aus", das Ticket berechtigt zum Zoo-Eintritt, ist noch nicht abgelaufen und sieht "echt" aus. Da das Ticket keine Information zur Authentisierung des Zoo-Eintritts-Berechtigten enthält, ist es prinzipiell übertragbar. Weitere Betrugsmöglichkeiten sind an den oben durch Hochkommata ("...") markierten Stellen denkbar.

Wenn am Zoo-Eingang das Eintritts-Ticket akzeptiert wurde, kann der Studierende in den Zoo eintreten. Gleich ganz vorn springt ihm ein Schild ins Auge, auf dem steht, welches Verhalten im Zoo untersagt ist, gemäß der Politik des Zoos. Vor allem soll man die Affen nicht ärgern, wohl weil die sich mit Bananenschalen-Geschossen rächen könnten. Der Zoo wird vermutlich niemanden finden, der ihm vorher verantwortlich zusichert, daß der Studierende sich im Zoo anständig verhalten wird, er also die Eigenschaft *politik-konform* besitzt. Deswegen muß der Zoo zunächst darauf vertrauen, daß die Zoo-Besucher sich an die Regeln halten. An kritischen Stellen (bei den Affen) kann der Zoo einen Wächter postieren, der dem munteren Treiben der Zoo-Besucher zusieht und bei entdeckten Regel-Verstößen sinnvoll reagiert.

1.2 Von Vertrauen und Kontrolle

In Abschnitt 1.1 sind zwei Situationen dargestellt, in denen dienstspezifische *Geber* (Zoo-Kasse, Zoo-Eingang) etwas geben (Eintritts-Ticket, Eintritt in den Zoo). An das Geben ist entsprechend der Politik des Dienstes eine Bedingung über Eigenschaften geknüpft (*Studierender*, *Zoo-Eintritts-Berechtigter*). Wenn der *Nehmer* zum Nachteil des Gebers über den Besitz der geforderten Eigenschaft lügen kann, vertraut der Geber nicht den diesbezüglichen Eigenschaftsaussagen des Nehmers. Deswegen möchte der Geber die Eigenschaften des Nehmers gern selbst prüfen. Er weiß dann, ob die Eigenschaften vorliegen und kann die Zuordnung zum Nehmer selbst vornehmen. Wenn er diese Prüfung nicht selbst durchführen kann, muß er einer dritten Partei vertrauen (Universität, Zoo-Kasse), die diese Prüfung für ihn vornimmt und die entsprechende Eigenschaftsaussage dem Nehmer zuordnet und mit unfälschbaren Echtheitsmerkmalen versieht (Studierenden-Ausweis, Eintritts-Ticket), sie also verantwortlich beglaubigt. Die Dritte Partei, welcher der Geber vertraut, kann die Prüfung und Beglaubigung über mehrere Schritte mittels entsprechender Eigenschaftsaussagen an andere Parteien delegieren, denen sie dafür vertrauen muß. Die sogenannte Delegation und Lizensierung sollen hier nicht betrachtet werden, integrieren sich aber nahtlos mit den vorgestellten Modellen [BK02, BK03, Kar02].

Da der Nehmer ein Interesse daran haben könnte, diesen Vorgang zu korrumpieren, darf der Nehmer keine Kontrolle über die dritte Partei haben. Insbesondere darf nur die dritte Partei die Fähigkeit besitzen, die Eigenschaftsaussage mit unfälschbaren Echtheitsmerkmalen zu versehen. Sind diese Voraussetzungen erfüllt, kann der Geber darauf vertrauen, daß die Eigenschaft vorliegt und dem Nehmer korrekt zugeordnet wurde.

Sind derartige präventive Eigenschaftsprüfungen nicht vorgesehen oder aufgrund der Art der geforderten Eigenschaft nicht möglich (z.B. ein Verhalten nach bestimmten Regeln über einen längeren Zeitraum), wird das

[1] Der Aufwand zur Fälschung der Echtheitsmerkmale übersteigt den Eintrittspreis.

Nehmen bei Nicht-Vorliegen der Eigenschaft (*politik-konform*) untersagt und sanktioniert. Der Geber muß also darauf vertrauen, daß beim Nehmer die von der Nehmer-Politik geforderte Eigenschaft vorliegt und kann an kritischen Stellen (Affen) versuchen zu entdecken (Wächter), ob dies nicht der Fall ist.

1.3 Das Digitale zum Realen

In der digitalen Welt entsprechen die präventiven Eigenschaftsprüfungen auf der Basis von beglaubigten Eigenschaftsaussagen den Zugriffskontrollen, z.B. basierend auf einer Public-Key-Infrastructure (PKI). Auch in der digitalen Welt lassen sich nicht alle Eigenschaften präventiv sinnvoll prüfen oder beglaubigen, wie etwa das Verhalten der Nutzer von IT-Systemen. Das IT-System kann das Verhalten als Überwachungsdaten aufzeichnen und diese können hinsichtlich Politik-Verletzungen analysiert werden, z.B. automatisiert durch ein Intrusion-Detection-System (IDS) [McH01, ACF+00, Axe99].

1.4 Beitrag und Überblick

Abschnitt 1 illustriert, wie Autorisierungsstrukturen unserem Sicherheitsbedürfnis Rechnung tragen. Diese Strukturen wurden auf die digitale Welt übertragen. Sie stärken dabei aber meist einseitig die Sicherheitsinteressen der Dienstleister in ihrer Funktion als Geber. Der Schutz der Dienste kommt sicherlich zum Teil auch den Dienstnutzern zugute. Dienstnutzer treten zwar hinsichtlich der Dienstleistung einerseits als Nehmer auf, andererseits aber hinsichtlich der Datenspuren bei der Dienstnutzung als Geber. Da die Speicherung und Verarbeitung von Datenspuren in der digitalen Welt um ein vielfaches einfacher ist als in der realen Welt, rückt das Interesse der Dienstnutzer am Schutz ihrer informationellen Selbstbestimmung zunehmend in den Vordergrund. Verschiedene Systeme zum Schutz der informationellen Selbstbestimmung etwa durch Anonymisierung wurden vorgeschlagen und werden zunehmend verfügbar. Die von diesen Systemen hergestellte Anonymität ist mitunter so stark, daß eine Verfolgung bei Mißbrauch im Ausnahmefall nahezu unmöglich ist.

Gesucht sind also Systeme, welche die Sicherheitsanforderungen sowohl der Dienstleister als auch der Nutzer berücksichtigen. Eine dahingehende Bewertung verfügbarer Systeme mußte bisher durch eine Analyse der einzelnen Systeme erfolgen. In diesem Beitrag wird ein Architektur-Modell für anonyme Autorisierungen entwickelt, anhand dessen Eigenschaften konkreter Anonymitäts-Technologien erkennbar und verschiedene anonyme Autorisierungs-Architekturen im Hinblick auf anonyme Überwachungsdaten systematisch vergleichbar werden. Das Modell wird in drei Schritten entwickelt:

1. Ein PKI-basiertes Architektur-Modell für Autorisierungen [BK02, BK03, Kar02] wird verallgemeinert, indem von der PKI-Technologie abstrahiert wird (Abschnitt 2). Dieses Modell berücksichtigt zunächst vorrangig die Sicherheits-Interessen der Dienstleister.
2. Bestehende gesetzliche Verpflichtungen der Dienstanbieter zum Schutz der informationellen Selbstbestimmung der Dienstnutzer erschweren die überwachungsgestützte Absicherung von Diensten (Abschnitt 3). Es wird ein Ansatz zum Interessenausgleich von Überwachung und Anonymität entwickelt, der auf Pseudonymen basiert (Abschnitt 4). Die Begriffswelt der Pseudonymität [PK00] wird um die Konzepte der organisatorischen und der technischen Zweckbindung erweitert, welche für den angestrebten Interessenausgleich eine zentrale Bedeutung haben (Abschnitt 5).
3. Die Pseudonymitäts-Konzepte aus Abschnitt 5 werden mit dem Modell aus Abschnitt 2 integriert zu einem Architektur-Modell für anonyme Autorisierungen. Kriterien für den Vergleich von Architekturen für anonyme Autorisierung und Überwachung werden erarbeitet und im Modell angewandt. Einige konkrete Architekturen werden in das Modell eingeordnet (Abschnitt 6).

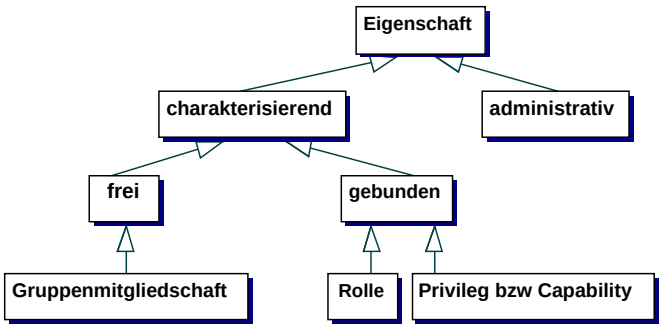


Abbildung 1: Klassifizierung von Eigenschaften (vgl. Abb. 5)

Mit dem Blick auf eine Sicherheitsüberwachung bei der Diensterbringung zeigt sich, daß ein Interessenausgleich insbesondere unter der hierfür spezifischen Anforderung der technischen Zweckbindung praktikabel nur durch die Pseudonymisierung bereits erhobener Überwachungsdaten machbar ist. Bekannte Ansätze für die Pseudonymisierung von Überwachungsdaten werden vorgestellt und verglichen (Abschnitt 7).

2 Ein Architektur-Modell für Autorisierungen

Im Folgenden wird ein Architektur-Modell für Autorisierungen vorgestellt. Das Modell verallgemeinert ein hybrides PKI-Modell [BK02, BK03, Kar02], indem es von der PKI-spezifischen Technologie abstrahiert. Die Darstellung konzentriert sich auf die Parteien, mit denen der Dienst-Nutzer direkt kommuniziert. Die Lizensierung, die Delegation und die verschiedenen Betriebsmodi der einzelnen Entitäten werden nicht dargestellt, funktionieren jedoch analog zum hybriden PKI-Modell [BK02, BK03, Kar02]. Das Modell ist bereits für die Erweiterung um Anonymität vorbereitet.

In der digitalen Welt sind weder die entsprechenden Entitäten der realen Welt noch deren Eigenschaften sichtbar. Deswegen werden *Entitäten* der realen Welt in der digitalen Welt durch sog. *Prinzipale* sichtbar dargestellt und ihre realen *Eigenschaften* in digitalen *Attributen* sichtbar kodiert. Die Beziehung zwischen einer Entität und ihren Eigenschaften soll in digital sichtbaren *Eigenschaftsaussagen* ausgedrückt werden, wobei die Sicherheit der Bindung des entsprechenden Prinzipals an die entsprechenden Attribute auf Kryptographie und privaten Parametern des für die Beglaubigung *verantwortlichen Agenten* beruht. Die Übereinstimmung des *Subjekts* einer Eigenschaftsaussage mit deren vorlegenden Partei wird mittels Kryptographie und privaten Parametern des Subjekts geprüft. Ob eine digitale Eigenschaftsaussage tatsächlich die Eigenschaften der beschriebenen Entität in der realen Welt abbildet, bleibt letztlich eine Frage des individuell subjektiven *Vertrauens*, das in den verantwortlichen Agenten gesetzt wird. Die skizzierten Beziehungen zwischen der realen und der digitalen Welt werden in Abb. 2 dargestellt und im Folgenden genauer beschrieben.

Entitäten und Eigenschaften: Im Modell werden Individuen, Rechner und andere Akteure eines verteilten IT-Systems als *Entität*en bezeichnet. Ein *Prinzipal* ist ein Bit-String, der in seinem Anwendungsbereich eindeutig genau einer Entität als deren Surrogat zugeordnet ist. Eine Entität kann *Eigenschaft*en haben, die in Sicherheitspolitiken als Entscheidungsbedingungen formuliert sind. Biskup und Karabulut unterscheiden charakterisierende und administrative Eigenschaften [BK02, Kar02] (s. Abb. 1). Während erstere die Nutzer charakterisieren, beschreiben letztere die verantwortlichen Agenten und werden für die Lizensierung und Delegation benötigt und sind bei der Vertrauensevaluierung von entsprechender Bedeutung. Administrative Eigenschaften und die zugehörigen Attribute und Eigenschaftsaussagen werden hier nicht betrachtet, da sie sich in das hier vorgestellte Modell integrieren, wie von Biskup und Karabulut beschrieben [BK02, BK03, Kar02].

Beglaubigung und Autorisierung: Charakterisierende Eigenschaften werden nach freien und gebundenen Eigenschaften unterschieden (s. Abb. 1). *Freie Eigenschaft*en sind auf Entitäten und nicht auf Dienste bezogen, z.B. personenbezogene Daten, technische Merkmale, Fähigkeiten, (Gruppen-)Mitgliedschaften, etc. Eine freie Eigenschaft impliziert demnach per se keine spezifische Dienstnutzungs-Autorisierung. Der Begriff *Beglaubigung* bezeichnet im Modell den Vorgang und das Resultat, wenn ein verantwortlicher Agent als *Beglaubiger* eine Aussage über freie Eigenschaften beglaubigt. Als Beispiel für die beglaubigte Aussage über die freie Eigenschaft *Studierender* trat in Abschnitt 1.1 der Studierendenausweis als Beglaubigung auf. *Gebundene Eigenschaft*en sind Ausdruck einer Erlaubnisbeziehung zwischen einer Entität und einem spezifischen Dienst, z.B. die Zoo-Eintritts-Berechtigung. Gebundene Eigenschaften sind demnach dienstbezogen und implizieren eine spezifische Dienstnutzungs-Erlaubnis, z.B. über eine Rolle. Der Begriff *Autorisierung* bezeichnet im Modell den Vorgang und das Resultat, wenn ein verantwortlicher Agent als *Autorisierer* eine Aussage über gebundene Eigenschaften beglaubigt. Als Beispiel für die beglaubigte Aussage über die gebundene Eigenschaft *Zoo-Eintritts-Berechtigter* trat in Abschnitt 1.1 das Eintritts-Ticket als Autorisierung auf.

2.1 Eigenschaftsaussagen

Eigenschaften werden einer *Subjekt*-Entität meist von einer anderen Entität, dem *verantwortlichen Agenten* zugeordnet (s. Abschnitt 1.2, hier Universität oder Zoo-Kasse), indem der Agent eine Aussage über die Zuordnung eines Prinzipals des Subjekts zu Attributen, welche die Eigenschaften repräsentieren, unter einem seiner eigenen Prinzipale beglaubigt. Die Zuordnung des Subjekt-Prinzipals zur vorlegenden Entität wird mittels Authentisierungswerten verifizierbar gemacht. Die Eigenschaftsaussage enthält zusätzlich verifizierbare, unfälschbare Angaben zur Gültigkeit, die ausschließlich vom verantwortlichen Agenten aufgebracht werden können. Beglaubigte Eigenschaftsaussagen können in verschiedenen Formen auftreten, etwa als statisches Dokument (z.B. Zertifikate [BK02]) oder als interaktiver Protokollablauf (z.B. anonyme Credentials [CL01b]). Die *Komponenten* einer Eigenschaftsaussage sind im einzelnen (s. Abb. 2 und Abb. 3):

verantwortlicher Agent: ein Prinzipal der Entität, die dafür verantwortlich ist zu prüfen, daß die Subjekt-Entität das Eigenschaftsbündel aufweist und der Subjekt-Prinzipal zur Subjekt-Entität gehört. Diese Komponente zeigt dem Empfänger den verantwortlichen Agenten an. Vertraut der Empfänger diesem Agenten (s. Vertrauens-Ausdruck in Abb. 7), kann er darauf vertrauen, daß dieser folgende Zuordnungen korrekt vorgenommen hat:

- der Prinzipal ist korrekt einer Entität zugeordnet;
- diese Entität besitzt die von den Attributen beschriebenen Eigenschaften.

Zusätzlich fungiert diese Komponente als Referenz auf Eigenschaftsaussagen über den verantwortlichen Agenten. Diese sind im Fall von Lizensierung und Delegation zur Verifikation hinzuzuziehen [BK02]. Diese Komponente kann fehlen, wenn der verantwortliche Agent bekannt ist, etwa wenn die Eigenschaftsaussage direkt von ihm über einen authentisierten Kanal bezogen wird, z.B. bei A4 in Abb. 9 und A3 in Abb. 12, sowie C1 in Abb. 10, B3 in Abb. 11 und C1 in Abb. 12.

Validität: unter Verwendung privater Parameter berechnete öffentliche Werte. Diese Komponente dient der Verifikation der Gültigkeit der Eigenschaftsaussage und deren technischer Merkmale (s. Abschnitt 5.1.3), wie etwa garantierte Einzigartigkeit, Übertragbarkeit, Aufdeckbarkeit, etc. Die Verifikation kann entweder zeitnah über ein online-Protokoll geschehen, oder offline wie etwa bei referenzierten Eigenschaftsaussagen. Bei der Berechnung der Validitäts-Komponente müssen private Parameter des verantwortlichen Agenten so eingehen, daß die Komponente ausschließlich von ihm gebildet werden kann. Diese Komponente kann fehlen, wenn die Eigenschaftsaussage direkt vom verantwortlichen Agenten über einen authentisierten und sicheren Kanal bezogen wird, z.B. bei A4 in Abb. 9 und A3 in Abb. 12, sowie C1 in Abb. 10, B3 in Abb. 11 und C1 in Abb. 12.

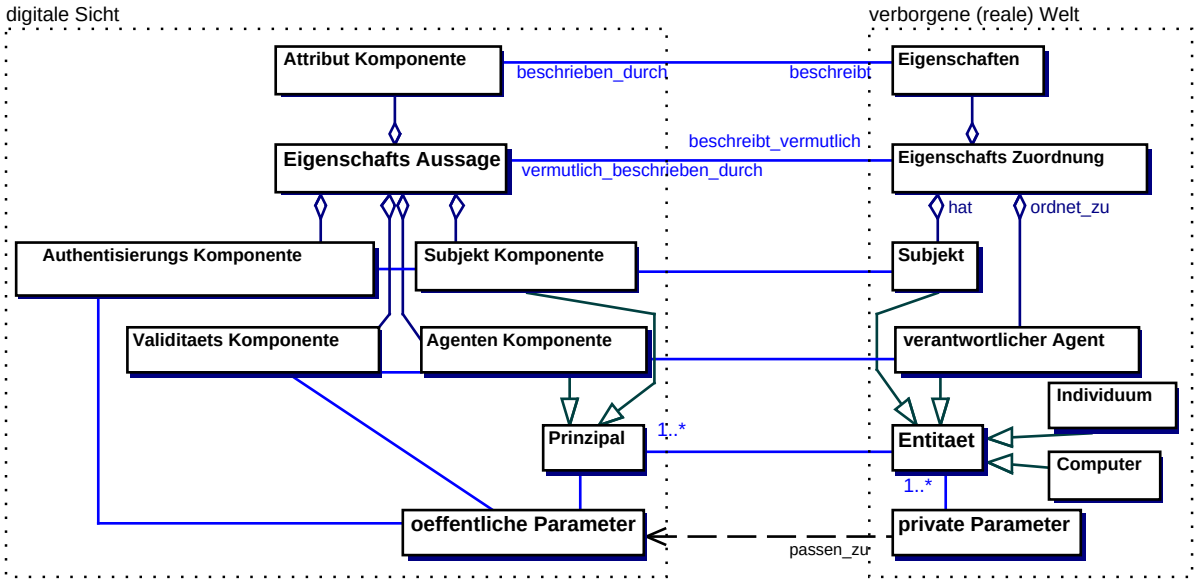


Abbildung 2: Beziehungen von Eigenschaftsaussagen und Entitäten

Authentisierung: unter Verwendung privater Parameter berechnete öffentliche Werte. Diese Komponente dient dem Nachweis, daß die Eigenschaftsaussage der vorlegenden Entität zugeordnet ist. Der Nachweis wird stets zeitnah über ein online-Protokoll erbracht. Bei der Berechnung der Authentisierungskomponente müssen private Parameter der Subjekt-Entität und frische Herausforderungs-Werte so eingehen, daß die Komponente ausschließlich von der Subjekt-Entität als Antwort auf die Herausforderungs-Werte gebildet werden kann. Die Komponente kann fehlen, wenn ein verantwortlicher Agent die vorlegende Entität bereits authentisiert hat und die Eigenschaftsaussage zusammen mit der Dienst-Anfrage in Richtung Dienst über einen sicheren Kanal zustellt, wie etwa bei C1 in Abb. 10 und 12. Der Dienst vertraut dem verantwortlichen Agenten dann zusätzlich hinsichtlich der korrekten Authentisierung der vorlegenden Entität.

Attribute: das Eigenschaftsbündel der Subjekt-Entität, über das eine Aussage gemacht wird. Diese Komponente dient der Entscheidungsfindung auf Basis der Sicherheitspolitik des Empfängers (s. Attribut-Ausdruck in Abb. 7). Sie kann fehlen, wenn bekannt ist, daß der verantwortliche Agent immer dasselbe Eigenschaftsbündel beglaubigt.

Subjekt: ein Prinzipal der Subjekt-Entität (auch Subjekt-Prinzipal). Dient der Verkettbarkeit von Transaktionen zu dieser Eigenschaftsaussage (s. Anfrage-Kontext in Abb. 8), etwa um Reputation unter diesem Prinzipal zu etablieren. Diese Komponente ist immer vorhanden, wenn die Eigenschaftsaussage über eine Eigenschaftsreferenz verkettet werden soll. Sie kann fehlen, wenn die Eigenschaftsaussage nicht verkettet werden soll, also nicht bei A4 in Abb. 9 und B3 in Abb. 11.

Bei der Bildung der Authentisierungs- und Validitäts-Komponenten gehen private Parameter verschiedener Parteien ein, die bereits geeignet verteilt und geschützt wurden. Analoges gilt für die öffentlichen Parameter für die Verifikation dieser Komponenten.

2.2 Architekturen und Kontrollverhältnisse

Aus Abschnitt 2.1 geht hervor, daß die Komponenten beglaubigter Eigenschaftsaussagen vorrangig Sicherheitsziele im Sinne der Dienste unterstützen. Zusammen mit den Folgerungen aus Abschnitt 1.2 ergibt sich, daß die

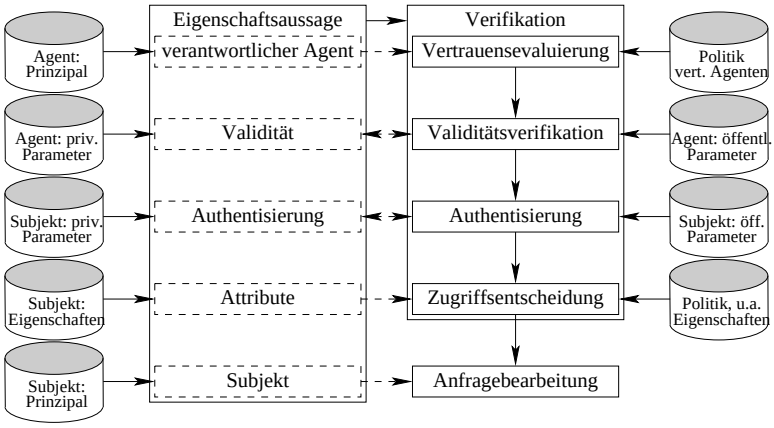


Abbildung 3: Verifikation von Eigenschaftsaussagen

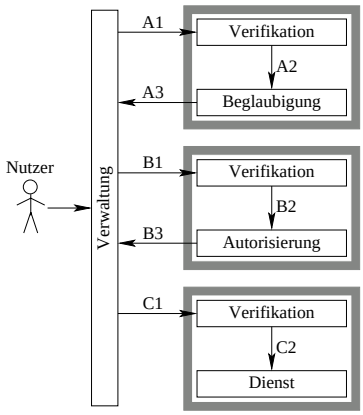


Abbildung 4: Grundmodell

Nutzer als Subjekt-Entitäten keine Kontrolle über Beglaubiger, Autorisierer und Dienste haben dürfen. Dementsprechend stehen die in den Abb. 4 und Abb. 9 bis Abb. 12 hellgrau umrahmten Bereiche für die Durchsetzung der primär dienstbezogenen Sicherheitsziele und damit außerhalb der Kontrolle des Nutzers. In Abb. 4 und Abb. 9 bis Abb. 12 zeigen die Pfeile die Flußrichtung beglaubigter bzw. nachgewiesener Aussagen über Eigenschaften bzw. entsprechender Referenzen an[2]. Die Pfeile werden im Text mittels ihrer Bezeichner referenziert (hier: A1 bis C2).

Verifikation: Im Grundmodell (s. Abb. 4) wird bei der Verifikation beglaubigter Eigenschaftsaussagen durch deren Empfänger (s. Verifikation in Abb. 4) zunächst der verantwortliche Agent (s. Beglaubigung bzw. Autorisierung in Abb. 4) anhand der gleichnamigen Komponente ermittelt. Der Empfänger entscheidet zunächst darüber, ob er dem Agenten hinsichtlich der Prüfung der in der Attribut-Komponente beschriebenen Eigenschaften und deren korrekter Zuordnung zum Prinzipal der korrekten Entität vertraut (s. Vertrauensevaluierung in Abb. 3 und Vertrauensbasis in Abb. 7). Anschließend wird anhand der Validitäts-Komponente festgestellt, ob die Eigenschaftsaussage gültig ist (s. Validitätsverifikation in Abb. 3). Dann prüft der Empfänger mittels der Authentisierungs-Komponente, ob die vorlegende Entität der Subjekt-Komponente entspricht (s. Authentisierung in Abb. 3). Schließlich interpretiert der Empfänger die Attribute entsprechend seiner eigenen Politik (s. Zugriffsentscheidung in Abb. 3 und Attribut-Konvertierung in Abb. 7)).

[2]Da die Antworten des Dienstes keine Aussagen über Eigenschaften des Nutzers enthalten, sind sie im Modell nicht zu sehen.

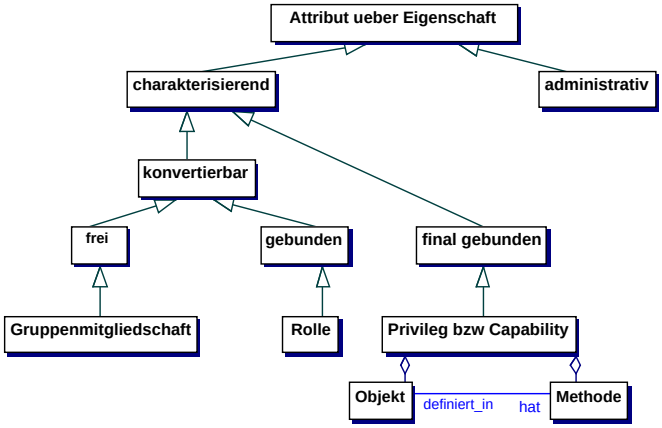


Abbildung 5: Klassifizierung von Attributen über Eigenschaften (vgl. Abb. 1)

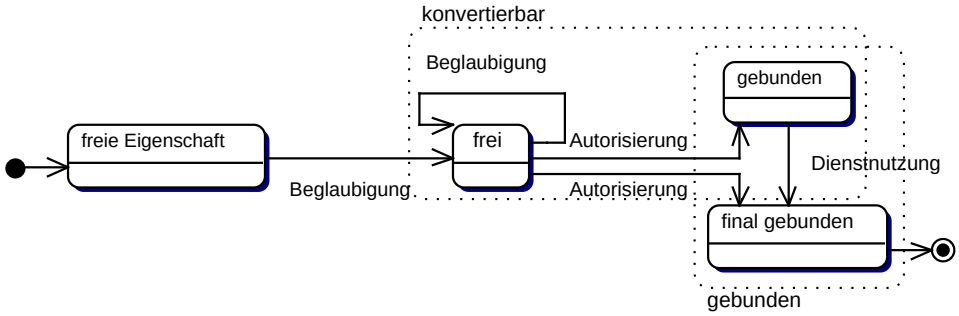


Abbildung 6: Mögliche Konvertierungen von Attributen über Eigenschaften (s. Abb. 5)

Referenzen auf Eigenschaftsaussagen: Bei den in Abb. 9 und Abb. 11 dargestellten Modellvarianten erhält der Nutzer nur eine Referenz auf eine Eigenschaftsaussage (s. A3 in Abb. 9 und B4 in Abb. 11), die er an den Empfänger leitet (s. B1 in Abb. 9 und C1 in Abb. 11). Sie enthält folgende Komponenten:

Subjekt: Subjekt-Prinzipal der zugehörigen Eigenschaftsaussage.

Bezug: Information, von wo die zugehörige Eigenschaftsaussage bei Bedarf bezogen werden kann. Diese Komponente kann fehlen, wenn der Bezugspunkt bekannt ist.

Der Empfänger erhält die referenzierte Eigenschaftsaussage vom verantwortlichen Agenten (s. A4 in Abb. 9 und B3 in Abb. 11). Erhält der Empfänger die Eigenschaftsaussage über einen authentisierten und sicheren Kanal und vertraut der Empfänger in die Sicherheit des verantwortlichen Agenten bzw. des Bezugspunkts, können die Komponenten zum verantwortlichen Agenten und zur Validität fehlen (s. A4 in Abb. 9 und A3 in Abb. 12, sowie C1 in Abb. 10, B3 in Abb. 11 und C1 in Abb. 12).

Nutzungsphasen und Attributkonvertierung: Die in den Abb. 4 und Abb. 9 bis Abb. 12 gezeigten Akteure sind die Verwaltung, ein Beglaubiger, ein Autorisierer und ein Dienst. Die Dienst-Nutzung verläuft in drei Phasen: 1) Der Nutzer läßt seine relevanten Eigenschaften beglaubigen (s. A1, A2 und A3 in Abb. 4). 2) Der Nutzer wird auf Vorlage der relevanten Beglaubigungen für die Dienst-Nutzung autorisiert (s. B1, B2 und B3 in Abb. 4). 3) Bei Vorlage dieser Autorisierungen kann der Nutzer den Dienst-Server in Anspruch nehmen (s. C1 und C2 in Abb. 4). Dieser Ablauf kann auch als mehrstufige Konvertierung von Attributen in Eigenschaftsaussagen betrachtet werden (s. Abb. 6). Dementsprechend werden Attribute analog zu Abb. 1 klassifiziert, jedoch werden zusätzlich konvertierbare und final gebundene Attribute unterschieden (s. Abb. 5).

Verwaltung: Die Verwaltung wird vom Nutzer kontrolliert. Sie tritt mit den anderen Akteuren in Kontakt und wählt auf Grundlage der Politik des Nutzers und der Anforderungen des Dienstes bzw. verantwortlichen Agenten (s. Politiken bei der Verifikation in Abb. 3 sowie Attribut-Ausdruck und Vertrauens-Ausdruck in Abb. 7) die für die jeweiligen Interaktionen zum Versand geeigneten Eigenschaftsaussagen und Informationen aus.

Beglaubiger: Der Beglaubiger agiert üblicherweise unabhängig von Diensten. Er ordnet dem Nutzer freie Eigenschaften durch das Ausstellen von Beglaubigungen zu (s. Attribut über freie Eigenschaft in Abb. 7). Die Politik des Beglaubigers formuliert die an die Beglaubigung geknüpften Bedingungen, die der Nutzer zu erfüllen hat (s. Attribut-Ausdruck in Abb. 7). Einerseits kann der Beglaubiger sich durch eine Prüfung des Nutzers in der realen Welt selbst davon überzeugen, daß dieser die zu beglaubigende(n) Eigenschaft(en) besitzt (s. freie Eigenschaft in Abb. 6). Andererseits kann der Beglaubiger eine von einem anderen Beglaubiger ausgestellte Beglaubigung (s. Attribut über freie Eigenschaft in Abb. 7) akzeptieren und daraus ableiten (s. Attribut-Konvertierung in Abb. 7), daß der Nutzer die zu beglaubigende(en) Eigenschaft(en) besitzt. Der Beglaubiger stellt eine Beglaubigung aus (s. mit Beglaubigung bezeichnete Pfeile in Abb. 6), die nicht notwendigerweise digital vorliegen muß. Das Subjekt erhält ggf. lediglich eine Referenz auf die Beglaubigung (s. Abb. 9).

Autorisierer: Der Autorisierer ordnet dem Nutzer im Auftrag des Dienstes dienstspezifische Autorisierungen zu (s. Attribut über (final) gebundene Eigenschaft in Abb. 7). Demgemäß wird die Beziehung vom Dienst zum Autorisierer meist enger sein, als zu Beglaubigern. Die Politik des Autorisierers formuliert die an die Autorisierung geknüpften Bedingungen, die der Nutzer zu erfüllen hat (s. Attribut-Ausdruck in Abb. 7). Einerseits kann der Autorisierer Beglaubigungen über freie Eigenschaften akzeptieren [3] (s. Attribut über freie Eigenschaft in Abb. 7). Andererseits kann er Autorisierungen über an andere Dienste gebundene Eigenschaften aus der Sicht seines Dienstes als freie Eigenschaften interpretieren und akzeptieren. Der Autorisierer konvertiert (s. Attribut-Konvertierung in Abb. 7) die akzeptablen Attribute über freie bzw. gebundene Eigenschaften wahlweise in Attribute über dienstspezifisch gebundene Eigenschaften [4], z.B. Rollen, die vom Dienst noch final an an Privilegien gebunden werden, oder in bereits final gebundene Privilegien in Form von Capabilities. Anschließend stellt der Beglaubiger eine Autorisierung aus (s. mit Autorisierung bezeichnete Pfeile in Abb. 6) [5], die notwendigerweise digital vorliegt, damit der Dienst sie digital prüfen kann. Das Subjekt erhält ggf. lediglich eine Referenz auf die Autorisierung (s. Abb. 11).

Falls allerdings alle geforderten beglaubigten Eigenschaftsaussagen digital vorliegen und die Autorisierungsentscheidung anhand der Politik digital gefällt werden kann, kann der Autorisierer die Autorisierung zusammen mit der Dienstanfrage des Nutzers direkt über einen sicheren und authentisierten Kanal dem Dienst zusenden (s. C1 in Abb. 10 und 12). Vertraut der Dienst dem Autorisierer hinsichtlich der korrekten Nutzerauthentisierung, so kann zusätzlich zu den Validitäts- und Agenten-Komponenten auch die Authentisierungs-Komponente des Autorisierers fehlen. Aus Nutzersicht verschmelzen damit Autorisierer und Dienst.

[3] Vgl. Interaktionen II und IV sowie entsprechende Protokollskizze in [BK03].

[4] Vgl. [BK03, Kar02].

[5] Ein Autorisierer kann zwar Attribute über gebundene Eigenschaften als Attribute über freie Eigenschaften interpretieren und in Attribute über (final) gebundene Eigenschaften konvertieren. In Abb. 6 werden die zu konvertierenden Attribute aus der Sicht der konvertierenden Entität interpretiert. Dementsprechend existiert kein Autorisierungs-Pfeil in Abb. 6, der von Attributen über gebundene Eigenschaften ausgeht, da diese bei der Autorisierung als Attribute über freie Eigenschaften interpretiert werden.

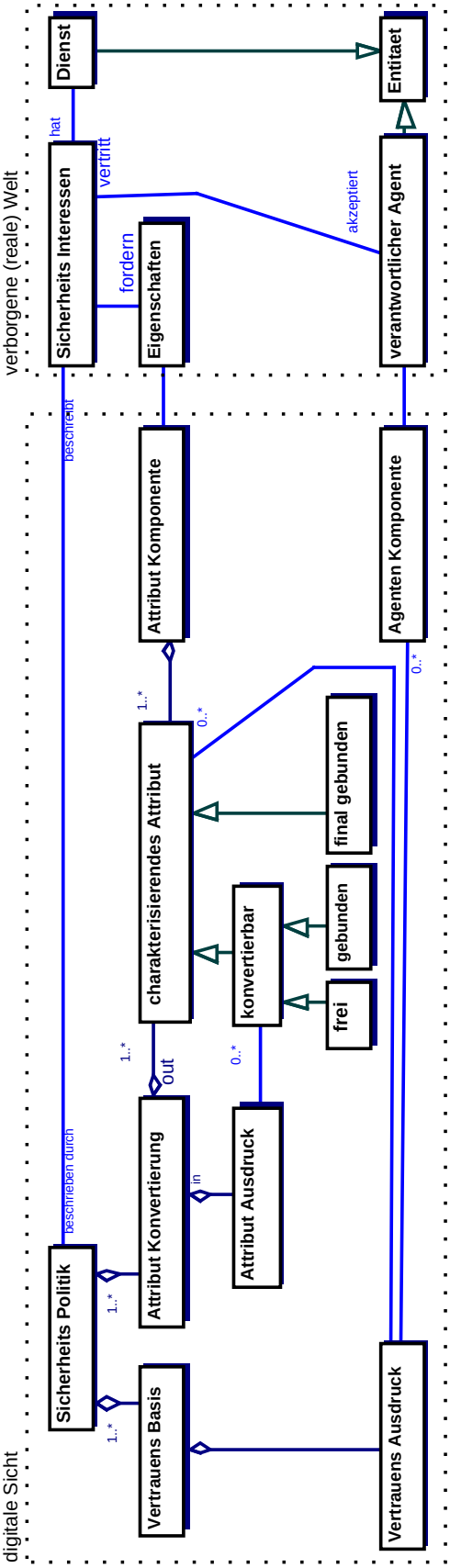


Abbildung 7: Beziehungen von Sicherheitsinteressen und Attributen

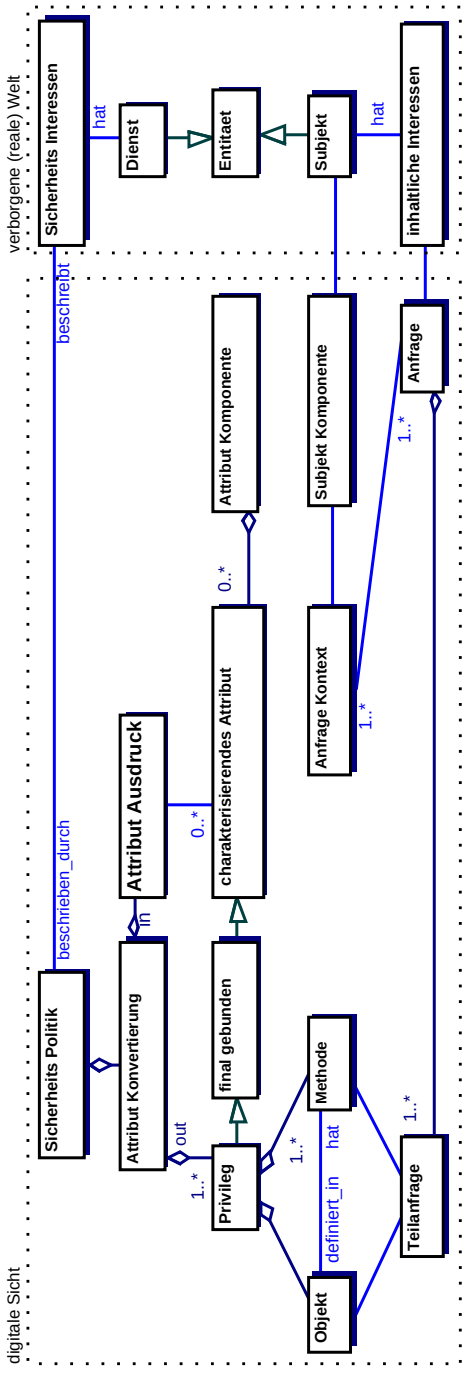


Abbildung 8: Beziehungen von Subjekt, dessen Interessen und Privilegien zur Laufzeit

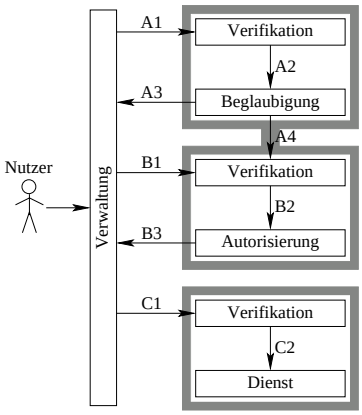


Abbildung 9: Der Autorisierer bezieht zu einer Referenz eine Eigenschaftsaussage

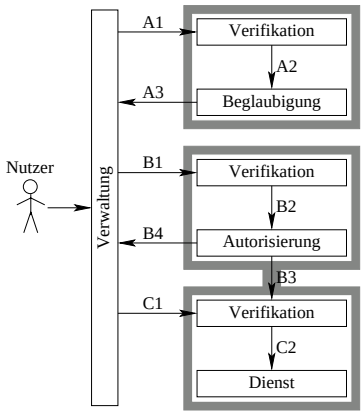


Abbildung 11: Der Autorisierer sendet dem Dienst eine referenzierbare Autorisierung

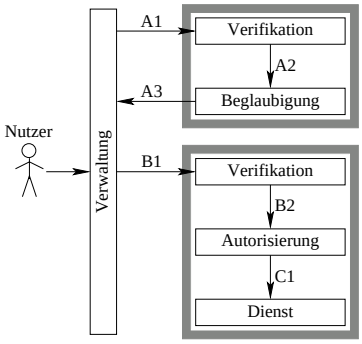


Abbildung 10: Der Autorisierer sendet dem Dienst die Dienst-Anfrage nebst Autorisierung

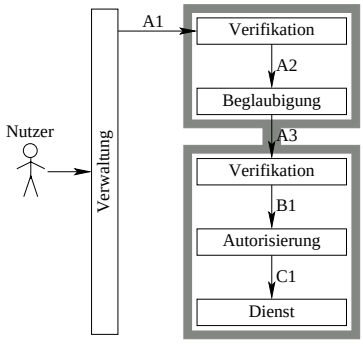


Abbildung 12: Der Beglaubiger sendet dem Autorisierer die Dienst-Anfrage nebst Beglaubigung

Dienst: Der Dienst erhält die Autorisierung und die Anfrage (s. Attribut-Komponente und Anfrage in Abb. 8) simultan oder zu verschiedenen Zeitpunkten. Die Politik des Dienstes formuliert die an die Diensterbringung geknüpften Bedingungen, die der Nutzer zu erfüllen hat. Der Dienst akzeptiert (digitale) Autorisierungen [6] und kann zusätzliche Bedingungen prüfen, die nicht von den Autorisierungen ausgedrückt werden, z.B. bzgl. des Empfangszeitstempels der Anfrage. Die Autorisierungen liegen in der Form von Capabilities bzw. Privilegien vor (s. Attribut über final gebundene Eigenschaft in Abb. 7) die der Dienst mit den angefragten Zugriffsprivilegien vergleicht (s. Privileg und Teilanfrage in Abb. 8). Alternativ erhält der Dienst dienstspezifische Attribute über gebundene Eigenschaften (s. charakterisierendes Attribut in Abb. 8), die er gemäß seiner Politik in entsprechende Privilegien (s. Privileg in Abb. 8) konvertiert (s. Attribut-Konvertierung in Abb. 8).

2.3 Beispiele

Das in Abb. 4 dargestellte Grundmodell modelliert z.B. die Autorisierungs-Architektur von Kerberos [Gol99]: Die Verwaltung entspricht dem Client, der Beglaubiger dem *Authentication-Server*, der Autorisierer dem *Ticket-Granting-Server* und der Dienst dem Dienst-Server.

[6] Vgl. Interaktion V und entsprechende Protokollskizze in [BK03].

Den im oberen Teil von Abb. 9 dargestellten Fall des nachträglichen Bezugs einer Beglaubigung findet man etwa in der Situation, in der ein Email-Client das zur Verifikation einer digitalen Signatur benötigte öffentliche Signaturverifikations-Schlüssel-Zertifikat von einem PKI-Verzeichnis anfordert (s. A4 in Abb. 9). Der Beglaubiger-Teil der Variante in Abb. 9 kann in Kombination mit den Varianten in Abb. 10 und Abb. 11 auftreten.

In Abb. 10 verschmelzen Autorisierer und Dienst. Der Nutzer liefert seine Anfrage zusammen mit der notwendigen Beglaubigung an den Autorisierer/Dienst[7] (s. B1 in Abb. 10). Dies modelliert etwa die Informationsquellen eines Multimedia-Mediators [BK02].

Abb. 11 modelliert z.B. die übliche paßwortbasierte Autorisierungs-Praxis. Aufgrund der Beglaubigung seiner Organisationszugehörigkeit (s. B1 in Abb. 11) erhält der Nutzer vom Administrator in seiner Funktion als Autorisierer als Referenz für seine Autorisierungen eine Kontokennung (s. B4 in Abb. 11). Die eigentliche Autorisierung, bestehend aus Subjekt-, Authentisierungs- und Attribut-Komponente, bringt der Administrator direkt in das IT-System ein (s. B3 in Abb. 11). Als zugehörigen privaten Authentisierungsparameter hat der Nutzer ein Paßwort.

Bei der Variante in Abb. 12 modelliert der Beglaubiger etwa einen IPSEC-Knoten, der vom Nutzer IP-Pakete erhält (Dienst-Anfrage) und diese mit einem Authentisierungs-Header versieht, bestehend aus Agenten-, Validitäts- und Subjekt-Komponente. Der IPSEC-Knoten beglaubigt damit, daß die Anfrage aus einem seiner IP-Adreßbereiche kommt.

3 Datenschutz-Anforderungen

Die Darstellung in den vorangegangenen Abschnitten hatte vorrangig die Schutzziel-Anforderungen der Dienstanbieter im Blick. Zwar liegt die Gewährleistung dieser Schutzziele zum Teil auch im Interesse der Nutzer. So profitieren insbesondere auch die Nutzer von einer hohen Verfügbarkeit der Dienste. Die Perspektive wird im Folgenden hinsichtlich der Nutzeranforderungen um Datenschutz, insbesondere um Anonymität erweitert, die dem Schutz des Grundrechts auf *informationelle Selbstbestimmung* dienen.

Die mit dem Datenschutz einhergehenden Schutzziel-Anforderungen gewinnen in der digitalen Welt zusätzlich an Gewicht. Im Gegensatz zu Pauschal- bzw. Bündelangeboten legen bedarfsorientierte Dienstangebote die Interessen ihrer Nutzer offen. Im Vergleich zu traditionellen Geschäftsvorfällen sind in der digitalen Welt neue bzw. mehr Parteien an Transaktionen beteiligt, die dadurch Rückschlüsse auf die Nutzer ziehen können. Auch unbeteiligte Parteien können über die Nutzer Informationen erlangen, wenn sie die Möglichkeit haben, das System zu beobachten. Digitale Information läßt sich beliebig speichern, effizient verarbeiten und mit Informationen anderer Parteien zusammenführen und korrelieren. Schon heute hinterlassen Internet-Nutzer eine Vielzahl von Spuren bei der Nutzung von Diensten [Spi03a]. Eine Massenüberwachung ist im Gegensatz zur realen Welt mit deutlich geringerem Aufwand verbunden. Manche Parteien wie etwa Netzzugangs-Dienstleister und Web-Email-Dienstleister können bereits heute Daten über eine große Anzahl von Nutzern sammeln.

Es besteht ein grundlegender Unterschied zwischen traditionellen Schutzziel-Anforderungen wie Vertraulichkeit oder Integrität und datenschutzbezogenen Anforderungen. Dieser Unterschied wird deutlich beim Versand einer Nachricht durch einen Sender an einen Empfänger[8]. Traditionelle Schutzziele konzentrieren sich auf dritte Angreiferparteien, die in der Regel keine Beziehungen zum Nachrichten-Sender und -Empfänger bzw. -Verwender unterhalten. In diesem Angreifer-Modell geht man davon aus, daß der Angreifer insbesondere den Opfern unbekannt bleibt. Demgegenüber werden personenbezogene Daten in der Regel im Rahmen einer Dienstnutzung (ggf. notwendigerweise) offenbart. In diesem Fall schließt das Angreifer-Modell auch den Empfänger der personenbezogenen Daten ein, der dem Sender bekannt ist.

[7] Vgl. Interaktion I in [BK03] und das entsprechende Protokoll in [ABFK03].

[8] Das Nachrichtenszenario ist geeignet, um viele Datenverarbeitungssituationen zu simulieren.

Die präventive Wirkung von Gesetzen auf unbekannte Angreifer oder auf Angreifer, die kein eigenes Interesse an der Aufrechterhaltung von Beziehungen mit dem Sender oder Empfänger haben, wird in der Regel als gering angenommen. Eine entsprechend hohe Bedeutung wird technischen Schutzmaßnahmen eingeräumt, die unter der Kontrolle der potentiellen Opfer stehen. Zwar sind derartige Maßnahmen für den Schutz personenbezogener Daten ebenfalls von Vorteil. Zusätzlich ist jedoch zu berücksichtigen, daß manche Dienstleistungen inhärent die Preisgabe personenbezogener Daten erfordern und sie damit in die Hand des Empfängers, also eines potentiellen Angreifers geben. Dieser hat in diesem Fall jedoch ein vorwiegendes Interesse daran, die Beziehungen zum Sender nicht durch sein eigenes Fehlverhalten zu beeinträchtigen. Zudem ist der Empfänger bzw. Angreifer namentlich bekannt, wodurch das gesetzliche, präventive Moment an Bedeutung gewinnt.

Der legitime Empfänger personenbezogener Daten ist also im Interesse guter Beziehungen und zur Vermeidung zu erwartender Sanktionen von rechtlicher Seite motiviert, seinerseits Datenschutz zu gewährleisten. Beim Empfänger lokalisierte technische Datenschutzmaßnahmen sind daher notwendig, obwohl sie aus Sendersicht einen schwächeren Schutz gewährleisten als allein senderkontrollierte Maßnahmen. Im Vergleich der Maßnahmen zeigt sich, daß empfängerkontrollierte Maßnahmen spezifische Vorteile aufweisen, etwa eine einfache Umsetzung (s. Abschnitt 6.3).

Neben der Erhaltung guter Beziehungen zu Kunden, stellen die Datenschutzgesetze also eine erhebliche Motivation der Dienstanbieter dar, sich mit technischen Datenschutzmaßnahmen auseinanderzusetzen. Beide Seiten werden daher im Folgenden beleuchtet. Inbesondere bei den juristischen Aspekten geschieht dies stets aus technischer Sicht und kann nicht eine Rechtsberatung ersetzen.

3.1 Nutzererwartungen

In der realen Welt finden wir diverse gesellschaftlich akzeptierte anonyme Dienstangebote, wie etwa anonyme Hotlines für die Seelsorge und Problemberatung, anonyme Wahlen, anonyme Telefonate mittels Bargeld oder Prepaid-Karte (Telefonzelle) und schließlich den anonymen Warenerwerb mittels Bargeld. Die Menschen erwarten, daß entsprechende Aktivitäten in der digitalen Welt ebenfalls anonym durchführbar sind. Studien zeigen, daß Internetnutzer- und -käufer auch in der digitalen Welt großen Wert auf die Wahrung ihrer Privatsphäre legen [New01, Pro00, ACR99, Inc99, R+98, CDT02].

Das Fehlen anonymer Nutzungsmöglichkeiten kann Nutzer von der Inanspruchnahme von Diensten abhalten. Die Mehrzahl der Kunden würde neue Technologien nicht nutzen, wenn dabei zu befürchten wäre, daß Daten zu ihrer Person für andere als für die von ihnen zugestimmten Zwecke erhoben und verarbeitet würden [dMiWuG98]. Eine weitere Studie kommt zu dem Schluß, daß beim Angebot der Nutzug unter Pseudonym erwartet werden kann, daß mehr Nutzer kommerzielle Transaktionen durchführen [HNP99].

Der Begriff *Anonymität im Internet* ist bei den Nutzern überwiegend positiv besetzt und wird mit Persönlichkeitsschutz und Freiheit assoziiert [BJR+03]. Dies spiegelt sich auch in der starken Besorgnis um die Gefahr der Beobachtung durch Unbekannte und der Profilbildung durch Dritte wider [Pro00, BJR+03]. Dennoch nutzen lediglich 4-5% der jeweils Befragten einen Anonymisierungsdienst. Dies sei auf mangelnde Informationen zurückzuführen [BJR+03, Pro00]. Der Anteil der Nutzer die einen Anonymisierungsdienst nutzen würden, stieg bei der erstgenannten Umfrage auf 76%, nachdem die Nutzer sich im Rahmen der Umfrage mit dem Thema auseinander gesetzt hatten [BJR+03]. Ein andere Studie zeigt, daß Nutzer durch die Anwendung von Anonymitätsdiensten insbesondere die Profilbildung durch Dienstbetreiber vermeiden wollen und daß die Anonymitätsdienstnutzung überwiegend bereits ein Bestandteil der täglichen Routine ist [Spi03b].

3.2 Gesetzliche Anforderungen

Nach deutschem Datenschutz-Recht unterliegt die Erhebung, Speicherung und Verarbeitung personenbezogener Daten einem Erlaubnisvorbehalt. Liegt ein gesetzlicher Erlaubnistatbestand oder die Einwilligung des Betroffe-

nen vor, hat der Datenverwender weitreichende Pflichten gegenüber dem Betroffenen, u.a. die Zweckbindung, die Unterrichtungs-, Lösch- und Meldepflicht [RS00].

Je nach der Art eines Dienstes gelten bei der Verarbeitung personenbezogener Daten ein oder mehrere Datenschutzgesetze, die im Detail verschiedene Forderungen und Sanktionen vorsehen. Beispielsweise ist ein Email-Dienst ein Teledienst, während ein WWW-Dienst sowohl ein Tele- als auch ein Mediendienst ist. [Jae00, Bun02]

Die Datenschutzgesetze unterscheiden je nach der Art der personenbezogene Daten Bestands-, Nutzungs- und Abrechnungsdaten. Die Nutzung von *Bestandsdaten* unterliegt keiner zeitlichen Beschränkung [Jae00]. In diese Kategorie fallen z.B. die oben dargestellten Autorisierungen.

Zu den *Nutzungsdaten* gehören die personenbezogenen Anfragen, die der Nutzer an den Dienst stellt. Ihre Erhebung, Verarbeitung und Nutzung ist "[...] nur soweit dies zur Inanspruchnahme des Teledienstes notwendig ist und nur solange die Nutzung andauert [...]" gestattet. Der Personenbezug ist meist gegeben, z.B. wenn die Anfrage die IP-Adresse des Dienst-Nutzers oder seine Nutzerkonto-Kennung enthält [Gol03, RRSCI02, RSCI01, Jae00, Köh00, Bun02, SFHR97].

Insofern ist die von vielen Dienstanbietern angewandte Praxis der Speicherung von Nutzungsdaten in Form von Überwachungs-, Log- bzw. Audit-Daten problematisch [Gol03]. Im Folgenden wird stets der Begriff *Audit-Daten* verwendet. Er bezeichnet die vom Dienst erhobenen Daten über Ereignisse im System, die häufig in ihrer Gesamtheit den Verlauf der Dienstnutzung dokumentieren, also auch das Verhalten der Nutzer. Audit-Daten werden auf Vorrat erhoben, gespeichert und analysiert mit dem Ziel, Mißbrauch zu entdecken und zwecks Rechtsverfolgung dem Urheber zuzurechnen [RSCI01] (vgl. Abschnitte 1.1 bzw. 1.3: Wächter bzw. Intrusion-Detection). Diese wichtige Sicherheitsmaßnahme kann sich auf Audit-Daten stützen, die an verschiedenen Stellen im Modell erhoben werden können. Hier werden ausschließlich die vom Dienst erhobenen Audit-Daten betrachtet.

Als *Abrechnungsdaten* werden die Daten bezeichnet, die der Dienstanbieter unmittelbar zur Abrechnung seiner Leistungen benötigt. Sie sind also die abrechnungsrelevante Untermenge der Nutzungs-Audit-Daten. Das Abrechnungsmodell bestimmt, welche Daten erhoben, gespeichert und verarbeitet werden dürfen [Gol03]. In der Regel wird abrechnungsseitig keine Notwendigkeit vorliegen, vollständige Nutzungsverläufe personenbezogen zu erheben. Damit sind Abrechnungsdaten i.a. für Intrusion-Detection nicht geeignet. Sind die Abrechnungsdaten personenbeziehbar, unterliegen sie einer kurzen Löschfrist [Jae00].

Organisationen stellen ihren Mitarbeitern häufig Dienste für betriebliche bzw. dienstliche Zwecke zur Verfügung. Insbesondere wenn dabei eine private Nutzung geduldet wird, kann durch Audit-Daten das Recht der Mitarbeiter auf informationelle Selbstbestimmung verletzt werden. Zusätzlich hat der Betriebs- bzw. Personalrat nach deutschem Recht ein Mitbestimmungsrecht bei der Einführung von Technologien, die zur Überwachung der Mitarbeiterleistung geeignet sind [Bun02, Sob99]. Die Erhebung und Speicherung von Audit-Daten bzw. Nutzungsdaten durch die den Mitarbeitern zur Verfügung gestellten Dienste ermöglicht vielfältige Analysen, auch im Hinblick auf die Arbeitsleistung.

Aufgrund der komplexen rechtlichen Situation und den datenschutz-gesetzlichen Einschränkungen bei der Erhebung, Speicherung und Verarbeitung personenbezogener Daten gestaltet sich der gesetzeskonforme Einsatz von Audit-Daten-gestützten Schutzmaßnahmen wie etwa Intrusion-Detection für viele Dienstanbieter äußerst schwierig.

Im Folgenden werden die Begriffe, Konzepte und Prinzipien kurz eingeführt, die für Entwurf von Systemen für den technischen Datenschutz relevant sind, insbesondere mit dem Blick auf anonyme Autorisierungen und Audit-Daten.

Das Recht auf informationelle Selbstbestimmung: Die erste bekannte Begriffsbestimmung eines Rechts auf *Privacy* stammt von Warren und Brandeis: "the right to be alone" [WB91]. Die heute geläufige Definition stammt von Alan Westin und weist bereits auf ein Recht auf informationelle Selbstbestimmung hin: "Privacy is the claim of individuals [...] to determine for themselves, when, how and to what extent information about them is communicated to others" [Wes87]. Hier wird nur der informationelle Aspekt von Privacy betrachtet, insbesondere wie er

in Deutschland durch das sog. Volkszählungsurteil des Bundesverfassungsgerichts als Recht auf informationelle Selbstbestimmung postuliert wurde [dB84].

Das Recht auf informationelle Selbstbestimmung ist von den Grundrechten auf Menschenwürde ([GG:49] Art. 1 (1)) und auf freie Entfaltung der Persönlichkeit ([GG:49] Art. 2 (1)) abgeleitet (s. C II 1a in [dB84]) und gehört damit verfassungsrechtlich zu einem der höchsten Werte. Es erlaubt den Bürgern, prinzipiell selbst über die Offenbarung von Informationen zu ihrer Person zu bestimmen.

Fundamentale Datenschutz-Konzepte: Das Grundrecht auf informationelle Selbstbestimmung kann nicht als unbegrenzt oder absolut betrachtet werden, da es mit anderen Rechten und Werten in Konflikt stehen kann (s. Abschnitt 4). Überdies ist eine volle Teilnahme an der Gesellschaft ohne Preisgabe personenbezogener Daten kaum möglich. Dem Rechnung tragend sind Ausnahmen für *legale Zwecke* im überwiegenden Allgemeininteresse zulässig. Ausnahmen stellen Einschränkungen des Rechts auf Informationelle Selbstbestimmung dar (s. C II 2 in [dB84]) und bedürfen einer gesetzlichen Grundlage, welche nach dem *Rechtsstaatsprinzip* der *Normenklarheit* und der *Verhältnismäßigkeit* genügt (s. C II 1b in [dB84]).

Das bedeutet, daß Maßnahmen, die eine solche Einschränkung umsetzen, hinsichtlich ihrer *Voraussetzungen* und ihres *Umfangs* klar und verständlich zu definieren sind. Zudem müssen einschränkende Maßnahmen hinsichtlich des verfolgten Zwecks *erforderlich*, *geeignet* und *verhältnismäßig* sein. Ob eine Maßnahme für einen Zweck verhältnismäßig ist, kann anhand der Sensitivität der betroffenen personenbezogenen Daten bestimmt werden. Das Bundesverfassungsgericht hat klargestellt, daß es a priori keine nicht-sensitiven personenbezogenen Daten gibt (s. C II 2 in [dB84]). Vielmehr ergibt sich die *Sensitivität* aus der Art der Maßnahme und dem verfolgten *Zweck*, also aus *Art* und *Umfang* der erhobenen Daten, deren Verarbeitbarkeit (bzw. Verkettbarkeit), den *Resultaten* der Verarbeitung und deren *Empfängern*. Um also die Verhältnismäßigkeit einer Maßnahme zu beurteilen, ist zunächst die Datensensitivität festzustellen und zu fixieren. Dies geschieht, indem die obigen Einflußfaktoren offengelegt und festgeschrieben werden, insbesondere der verfolgte Zweck. Dementsprechend spricht man dabei von der *Zweckbindung*.

Weitere im Volkszählungsurteil zu findende Datenschutz-Konzepte sind die Transparenz, die informationelle Gewaltenteilung und die Forderung nach der Um- und Durchsetzung der Konzepte. Mittels der *Transparenz* werden den Betroffenen umfassende Rechte auf Information und auf den Zugriff auf die eigenen Daten zugesichert. Die *informationelle Gewaltenteilung* soll eine Zusammenführung personenbezogener Daten verhindern, welche an verschiedenen Stellen erforderlicherweise vorliegen. Schließlich fordert das Bundesverfassungsgericht *angemessene organisatorische und technische Maßnahmen* zur Durchsetzung der informationellen Selbstbestimmung. Abb. 13 veranschaulicht grob, wie die Konzepte zueinander in Beziehung stehen.

Prinzipien bei der technischen Umsetzung: Für den Schutz der informationellen Selbstbestimmung formulieren nationale Datenschutzgesetze (z.B. das deutsche Datenschutzrecht), internationale Datenschutzrichtlinien (z.B. die EU-Datenschutzrichtlinie) sowie Selbstverpflichtungs-Richtlinien und Ethik-Grundsätze (UN, OECD) diverse Prinzipien für den Umgang mit personenbezogenen Daten. Die gemeinsamen Prinzipien werden im Folgenden kurz eingeführt, soweit sie für eine technische Umsetzung der informationellen Selbstbestimmung relevant sind.

Die Erhebung und Verarbeitung personenbezogener Daten soll nach gesetzlichen Vorgaben und fair durchgeführt werden. Die *Fairness* umfaßt die Aspekte der Transparenz, der Datenrichtigkeit und des Erlaubnisvorbehalts. Die *Transparenz* bei der Erhebung und bei der Verarbeitung läßt sich durch umfassende *Information* bzw. *Benachrichtigung* der Betroffenen herstellen, z.B. durch Hinweis auf den Verarbeiter, Umfang, Zweck, Empfänger, Zugriffs- und Korrekturrechte sowie auf automatisierte Entscheidungsprozesse. Die Transparenz dient auch der *Datenrichtigkeit*. Die Betroffenen müssen Daten einsehen und im Bedarfsfall unrichtige oder unrechtmäßig erhobene Daten *korrigieren*, *löschen* oder *sperren* (lassen) können.

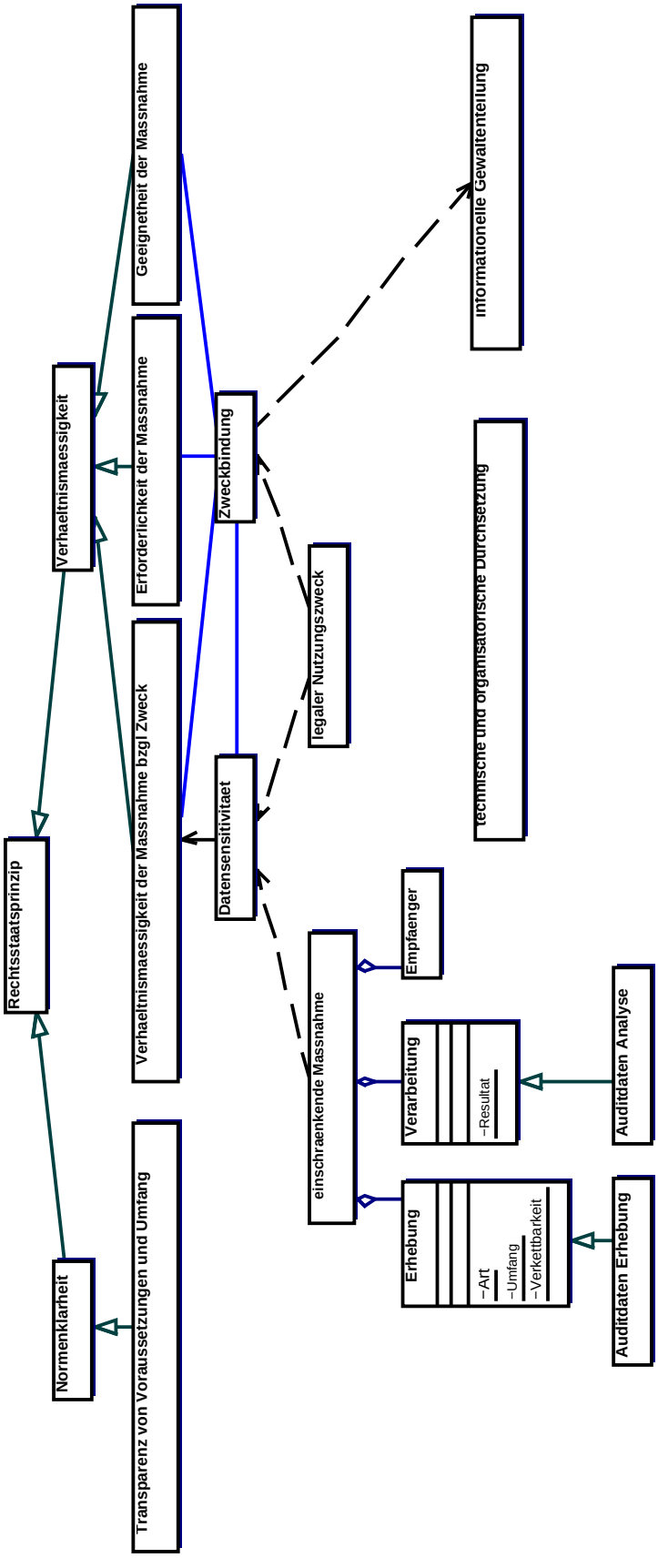


Abbildung 13: Konzepte aus dem Volkszählungsurteil des Bundesverfassungsgerichts [dB84]

Wenn Daten vom System eines Nutzers über ihn gespeichert werden, die später weitergegeben werden könnten, sollten diese Möglichkeiten bereits lokal im Nutzersystem vorgesehen werden, z.B. im Modell in der Verwaltung des Nutzers. In diesem Fall kann eine automatisierte, aber situationsbezogene und konfigurierbare Freigabe von Daten den Nutzer unterstützen (vgl. informationelle Gewaltenteilung). Aufgrund des prinzipiellen *Erlaubnisvorbehalts* bei der Erhebung personenbezogener Daten ist, sofern keine Erlaubnis *gesetzlich vorgesehen* ist, eine *Einwilligung des Betroffenen* erforderlich, welche vorab die Transparenz voraussetzt. Digitale Einwilligungen sollten rechtsgültig vom System der Datenverwender verwaltet werden.

Die technische Umsetzung der beschriebenen Fairnessaspekte wird im Weiteren nicht betrachtet. Vielmehr liegt in diesem Text das Augenmerk auf den Aspekten der *Datenqualität*. Diese subsumiert die oben eingeführten Konzepte der Erforderlichkeit und der Zweckbindung. Aus dem Grundsatz, daß nur für den Verarbeitungszweck erforderliche Daten verarbeitet werden dürfen, folgt, daß sofern möglich eine anonyme Verarbeitung bzw. Diensterbringung und ggf. Bezahlung zur Verfügung zu stellen ist und darüber zu informieren ist. Im Idealfall ist diese Variante bereits die Grundvorgabe für den Nutzer. Die Erforderlichkeit beinhaltet die Prinzipien der *Datenvermeidung* und der *nachträglichen Datenreduktion*. Während sich letztere durch Datenaggregation, -vergröberung, -anonymisierung oder -löschung nach Zweckerfüllung bzw. nach mandatorischen Fristen umsetzen läßt, können personenbezogene Daten vermieden werden, wenn sie gar nicht, nur im erforderlichen Umfang und/oder anonymisiert bzw. pseudonymisiert erhoben werden (s. Abschnitt 4.1). Die *Zweckbindung* läßt sich umsetzen, indem der legale bzw. eingewilligte Zweck fixiert wird und die mögliche Verarbeitung und deren Resultate technisch an diesen Zweck gebunden werden (s. Abschnitt 5.1.1). Ebenfalls ist eine technische Kontrolle bei der Erhebung der personenbezogenen Daten möglich (vgl. Verwaltung im Modell).

Zu den technisch umsetzbaren Prinzipien gehört des weiteren der Einsatz geeigneter *Sicherheitsmaßnahmen* zur Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit personenbezogener Daten. Abb. 14 soll grob veranschaulichen, wie die Prinzipien zueinander in Beziehungen stehen. Gesetzliche Vorgaben und Hinweise zu deren Umsetzung sind beispielsweise für Webseiten von Tele- und Mediendiensten beim Hamburgischen Datenschutzbeauftragten zu finden [SM02].

Ambivalenz von Sicherheitsmaßnahmen: Während Sicherheitsmaßnahmen dem Datenschutz dienen sollen, können sie gleichzeitig dazu im Konflikt stehen. Die mittels Sicherheitsmaßnahmen zur Verfügung gestellten personenbezogenen Daten können auch für Ziele genutzt werden, die über die mit den Maßnahmen ursprünglich verfolgten Zielen hinausgehen. Dieser Konflikt wird im Folgenden anhand von Beispielen aufgezeigt und für Audit-Daten ausführlicher beschrieben.

Eigenschaftsaussagen, deren Subjekt-Komponenten Nutzer identifizieren, offenbaren bei ihrer Nutzung und Authentisierung die Präsenz und ggf. den Aufenthaltsort der Nutzer. Diese Daten könnten innerhalb eines Betriebs etwa für die Erstellung von Bewegungsprofilen genutzt werden, welche Aufschluß über die Arbeitsleistung der Mitarbeiter geben können. Die Attribut-Komponenten zuordenbarer Eigenschaftsaussagen beschreiben die Eigenschaften von Nutzern und deren Erlaubnisse im IT-System. Die Attribute sind oft für große, ggf. nicht autorisierte, Nutzerkreise einsehbar. Die Datenverfügbarkeit wird in der Regel auch mittels Backup-Lösungen gewährleistet. Im Backup gesicherte personenbezogene Daten entsprechen u.U. nicht mehr dem aktuellen Stand. Dennoch werden sie häufig nicht der Möglichkeit der Nutzer-Korrektur unterworfen, wodurch die Rechte der Nutzer beeinträchtigt werden. Das Beispiel von Audit-Daten z.B. für Intrusion-Detection zeigt, daß einerseits das Schutzziel Integrität unterstützt wird, während andererseits die Audit-Daten Personenbezüge beinhalten und damit die informationelle Selbstbestimmung derjenigen Nutzer beeinträchtigen, die keine Schutzzielverletzungen hervorrufen. Da sich nahezu alle Nutzer regelkonform verhalten, sind fast alle Nutzer von dieser Einschränkung betroffen. Audit-Daten können etwa für eine kontinuierliche Leistungsüberwachung, Tätigkeitsanalysen und Persönlichkeitsprofile genutzt werden [Sob99]. Die Kenntnis derartiger Maßnahmen kann bei den Nutzern zu einer Zunahme der Streßbelastung, einer Abnahme der Produktivität bei sowie der Zufriedenheit mit der Arbeit führen [IHS86].

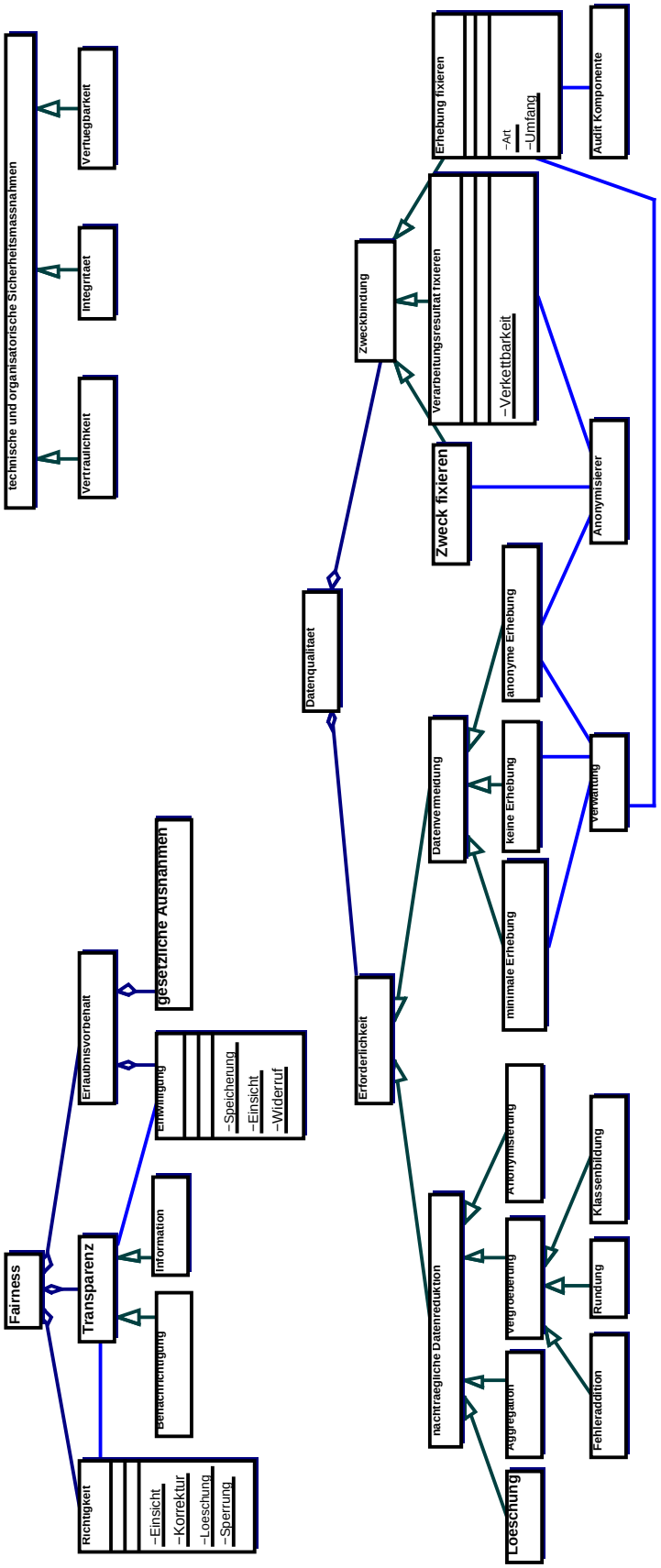


Abbildung 14: Prinzipien des technischen Datenschutzes

Eine Studie der US National Science Foundation hat die Praxis der Nutzung von Audit-Daten an akademischen Einrichtungen und die Ambivalenz von Audit-Daten im Hinblick auf den Datenschutz studentischer personenbezogener Daten zum Gegenstand [RRSCI02, RSCI01]. Die hier relevanten Ergebnisse der Studie werden im folgenden zusammenfassend dargestellt.

Audit Daten werden an den untersuchten Einrichtungen mit den Zielen erhoben und analysiert, einen sicheren (44%), effizienten und stabilen Betrieb zu gewährleisten. Nahezu an allen Einrichtungen wurden für diese Zwecke Audit-Daten erhoben (96%) und mehr als die Hälfte der Betreiber würde gern mehr Audit-Daten als bisher erheben (59%). Die aus Betreibersicht überwiegenden Gründe, die gegen eine Verstärkte Erhebung sprechen, sind Zeitmangel (57,7%), mangelnde technische Ausstattung (50%), und andere Faktoren (38,5%), aber nur in geringem Maße Verarbeitungsrichtlinien der Einrichtung (11,5%), persönliche ethische Grundsätze (9,6%) und Gesetze (7,7%). Die Audit-Daten-Erhebung wird von den meisten Betreibern mit den o.g. Zielen auf die lokalen Bedürfnisse beim Suchen in oder regelbasierten Auswertung von Audit-Daten zugeschnitten (82%).

Nahezu die Hälfte der Betreiber hat bei Verdacht auf Mißbrauch eine Verhaltensüberwachung von Nutzern durchgeführt (42%), ohne die Nutzer darüber zu benachrichtigen oder deren Erlaubnis einzuholen. Für forensische Zwecke und zur Gewährleistung der Systemstabilität werden von fast allen Betreibern die erhobenen Audit-Daten archiviert (82%), von einem Viertel dieser Betreiber sogar über einen Zeitraum von länger als zwei Monaten (22%).

Die Studie zeigt, daß die System-Administratoren (Betreiber) im Hinblick auf die Erlaubnis systemtechnischer Handlungen eine zu technische Sichtweise verfolgen. In der Regel nehmen die Administratoren an, daß alle Handlungen, die Ihnen im System technisch möglich sind, die also vom System autorisiert sind, ihnen auch erlaubt sind. Die zur Gewährleistung eines stabilen und sicheren Betriebs erforderlichen und technisch durchgesetzten Autorisierungen gehen meist jedoch weit über die im Zusammenhang mit dem Datenschutz gewünschten Erlaubnisse hinaus. Datenschutzziele bleiben damit in der Regeln im nichttechnischen Bereich in Form von Richtlinien, Gesetzen und Nutzererwartungen. Die Diskrepanz bei Autorisierungen zwischen technisch nicht durchgesetzten Datenschutzanforderungen und technisch durchgesetzten Stabilitäts- und Sicherheitsanforderungen gewinnt durch folgende weitere Faktoren an Bedeutung. Die technisch durchgesetzten Autorisierungen erlauben es den Administratoren, die mit einem Audit-Datensatz in Zusammenhang stehenden Personen im Mittel in lediglich 1,6 Arbeitsschritten zu identifizieren. Als Administratoren fungiert nicht nur langjährig erfahrenes Personal, sondern beispielsweise auch studentische Hilfskräfte. Administratoren wechseln ihre Rollen und Verantwortlichkeiten, aber die Autorisierungen werden im technischen Bereich oft nicht aktualisiert bzw. entzogen. Bei einem Wechsel unterbleibt häufig eine Einweisung über die nicht technisch durchgesetzten Autorisierungbeschränkungen für den Datenschutz. Oftmals liegen auch keine schriftlichen Richtlinien über diese Autorisierungsbeschränkungen vor.

In der Studie werden alle direkten Unteraspekte der drei Hauptprinzipien *Fairness*, *Datenqualität* und *Sicherheitsmaßnahmen* für die technischen Umsetzung des Datenschutzes als gefährdet identifiziert (s. Prinzipien in der zweiten Ebene in Abb. 14). Für die Fairness wird zunächst die Transparenz vorausgesetzt, und die Studie zeigt, daß diese häufig nicht hergestellt wird. Ohne Transparenz läßt sich wiederum die Datenrichtigkeit nicht umsetzen. Da die Administratoren häufig nicht realisieren, daß Audit-Daten personenbezogene Daten sind und unter Schutz stehen, kommt der Erlaubnisvorbehalt in der Praxis nicht zum Zug. Aufgrund oftmals fehlender Verarbeitungsrichtlinien wird die Zweckbindung nicht umgesetzt. Zeit- und Personalmangel führt in der Regel dazu, daß Audit-Daten auf Vorrat erhoben und archiviert, nicht aber zeitnah analysiert werden. Dies läuft dem Prinzip der Erforderlichkeit zuwider, insbesondere dem Prinzip der nachträglichen Datenreduktion. Schließlich greifen technische Sicherheitsmaßnahmen nicht, da die technisch durchgesetzten Autorisierungen der Administratoren ein Unterlaufen von Vertraulichkeit, Integrität und Verfügbarkeit ermöglichen. Fehlende Richtlinien stellen nicht klar, wo die erlaubten Grenzen der Administratoren innerhalb der technischen Autorisierungen liegen.

Die Ambivalenz der Audit-Daten-gestützter Sicherheitsmaßnahmen wird in der Studie wie folgt formuliert. Es wird geschlossen, daß neue Formen der Überwachung zu erwarten sind, wenn damit die Hoffnung einhergeht, dem Mißbrauch entgegenzutreten. Sowohl Sicherheitsbedenken hinsichtlich IT-Systemen als auch die Tendenz, Technologien soweit wie möglich auszunutzen, werden als treibende Kräfte für die Entwicklung von Technologien für eine zunehmende Überwachung identifiziert [RSCI01].

Europäische Harmonisierung: Das Ziel der EU-Direktive 95/46/EC [95/95] ist der Datenschutz als Grundrecht. Sie fordert von den Mitgliedsstaaten einen hohen Datenschutz-Mindeststandard, um einen Fluß personenbezogener Daten zwischen den Mitgliedsstaaten zu ermöglichen, der für einen europäischen Handel erforderlich ist (s. Erwägungen 3, 5, 7–9 in [95/95]). Dementsprechend konnte eine Harmonisierung der nationalen Gesetzestexte der meisten Mitgliedsstaaten erreicht werden. Der geforderte Datenschutz orientiert sich an einer Kombination der oben genannten Datenschutz-Prinzipien, die aus den Datenschutzgesetzen verschiedener Mitgliedsstaaten stammen und insbesondere vom deutschen System geprägt sind.

Die in Artikel 25 der Direktive festgelegten Restriktionen des Datentransfers üben auf Drittstaaten ökonomischen Druck aus, ein adäquates Datenschutz-Niveau herzustellen. Dennoch ist eine vollständig internationale Harmonisierung aufgrund kultureller, politischer und geschichtlicher Unterschiede nicht zu erwarten [FH01]. Als Beispiel kann hier der Ansatz der USA dienen, der anstatt umfassender Datenschutzgesetze die Selbstregulierung und privatsektorspezifische Gesetze vorsieht. Eine Selbstregulierung bleibt jedoch oft unangemessen, da es an Kontroll- und Durchsetzungsmöglichkeiten fehlt [FH01].

3.3 Notwendigkeit der technischen Durchsetzung

Digital vorliegende Information läßt sich leicht speichern und aggregieren oder mit anderen Informationen zusammenführen. Der Nutzer merkt in der Regel nicht, wenn seine Daten kopiert und weitergegeben werden. Ein Nachweis über Mißbrauch ist im Nachhinein sehr schwierig oder unmöglich zu führen. Auch wenn dies gelingt, kann ein irreparabler Schaden entstehen, da einmal veröffentlichte Daten faktisch nicht mehr zurückgenommen werden können. Schließlich können Datenflüsse im Transit auch das Hoheitsgebiet von Datenschutz-Gesetzen mit hohem Schutzniveau verlassen. Abschnitt 3.2 hat gezeigt, daß eine globale Harmonisierung der Datenschutz-Gesetze nicht zu erwarten ist.

Auch wenn die Daten von IT-Systemen vertrauenswürdiger Personen gespeichert und verarbeitet werden, können diese Personen praktisch nicht ausschließen, daß ihr IT-System verdeckte Komponenten enthält, die personenbezogene Daten an unautorisierte Dritte weiterleiten (Trojanische Pferde). Überdies können IT-Systeme bislang unbekannte Verwundbarkeiten aufweisen, die unautorisierten Dritten den Zugriff auf personenbezogene Daten ermöglichen.

Die genannten Schwierigkeiten zeigen, daß Gesetze allein nicht ausreichen können, um personenbezogene Daten effektiv zu schützen. Daraus motiviert sich die Notwendigkeit technischer Datenschutz-Maßnahmen, die idealerweise unter der Kontrolle der Betroffenen stehen. Dennoch ist für deren Einsatz die Einbettung in einen gesetzlichen Rahmen unabdingbar. Nach wie vor ist der Datenverwender in der Pflicht, die Datenschutzgesetze einzuhalten. Denn nutzerkontrollierte Datenschutz-Maßnahmen wirken zwar meist gegen starke Angreifer, ein alleiniger Verweis der Nutzer auf diese Technologien würde jedoch obiges Prinzip verletzen und die die Verantwortung zum Datenschutz allein den Nutzern aufbürden.

4 Die Herausforderung: Technische Durchsetzung mehrseitiger Sicherheit

Es besteht ein Spannungsfeld zwischen dem Interesse einzelner Nutzer an Datenschutz und Anonymität einerseits und der Zurechenbarkeit andererseits, um im Mißbrauchsfall die Interessen anderer beteiligter Parteien schützen zu können. Die einfachste Lösung besteht darin, eine der beiden Anforderungen zugunsten der anderen vollständig aufzugeben.

Werden nur die Schutz-Anforderungen des Dienstanbieters durchgesetzt, gilt dies auch bei der Beglaubigung und Autorisierung unter Ausschluß der Kontrolle durch den Nutzer (s. Abb. 4 und Abb. 9 bis Abb. 12). Schließlich unterstützen alle Komponenten der beglaubigten Eigenschaftsaussagen die Schutzziele des Dienstanbieters. In diesem Szenario kann nutzerseitig kein Vertrauen hinsichtlich der Wahrung der Nutzeranonymität bei der

Beglaubigung und Autorisierung aufgebaut werden, insbesondere wenn deren Subjekt-Komponente einen personenbezogenen Prinzipal enthält. Der Nutzer wird diese Beglaubigungen und Autorisierungen je nach Art des Diensten mehr oder weniger ungern für dessen Nutzung verwenden (s. Abschnitt 3.1).

Setzt man nur die Anonymitäts-Anforderung der Nutzer durch, so gilt dies auch bei der Beglaubigung und Autorisierung unter Ausschluß der Kontrolle durch den Dienstanbieter. In diesem Szenario kann seitens des Dienstanbieters kein Vertrauen hinsichtlich der vollständigen Wahrung seiner Schutzziele bei der Beglaubigung und Autorisierung aufgebaut werden. Die Akzeptanz dieses Risikos durch den Anbieter wird stark von der Art des Dienstes bestimmt.

So können leicht Szenarien entstehen, in denen keine Interaktion zwischen Nutzer und Dienst stattfinden werden. Wie etwa die Diskussion in [Fie01, Roß02, Fie02] deutlich macht, kann eine für die beteiligten Parteien zufriedenstellende Lösung i.a. eben nicht darin bestehen, eine der beiden Anforderungen zugunsten der anderen vollständig aufzugeben.

Vielmehr scheint ein fairer Ausgleich der Interessen aller beteiligter Parteien unter Berücksichtigung der jeweiligen Anwendungssituation erstrebenswert. IuKT-Technologien, die anwendungsspezifisch eine ebensolche Balance widerstreitender Sicherheits-Interessen erreichen oder zumindest Transparenz hinsichtlich der durchsetzbaren Sicherheits-Interessen herstellen, werden als Technologien zur Herstellung *mehrseitiger Sicherheit* bezeichnet [RPM99, Pfi01].

4.1 Ein Lösungsansatz durch Pseudonyme

Der auf Pseudonymen beruhende Lösungsansatz wurde in seiner jursitischen Dimension von Roßnagel und Scholz [RS00] sowie Jaeger [Jae00] motiviert und fundiert. Die relevanten Ergebnisse werden hier zusammengefaßt und interpretiert. Der Ansatz wird in den folgenden Abschnitten in seiner technischen Dimension betrachtet.

“§3 Abs. 4 TDDSG und §12 Abs. 5 MDStV: fordern ‘Gestaltung und Auswahl technischer Einrichtungen für Tele(Medien)Dienste an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen.’ Diese Anforderung wird durch die in §4 Abs. 1 TDDSG und §13 Abs. 1 MDStV enthaltene Verpflichtung der Diensteanbieter konkretisiert, die Inanspruchnahme von Telediensten und Mediendiensten sowie ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist.” [RS00]. Anonymität und Pseudonymität dienen als Mittel zur Umsetzung von System- und Selbstdatenschutz, indem sie Datenvermeidung, Datensparsamkeit und informationelle Selbstbestimmung realisieren [RS00].

Der in diesem Zusammenhang zentrale Begriff des *Personenbezug*s ist relativ, da die Personenbeziehbarkeit einer Information vom jeweiligen Zusatzwissen zum jeweiligen Zeitpunkt abhängt. Dementsprechend gelten die Datenschutzgesetze nur für diejenigen Datenverwender, die durch Zusatzwissen den Bezug der Daten zum Betroffenen herstellen können. Somit kann der in Abschnitt 4 beschriebene Zielkonflikt zwischen Zurechenbarkeit und Anonymität durch die Dienstnutzung unter Pseudonymen fair gelöst werden, indem über die Kontrolle von Zusatzwissen zwischen Regelfall (keine Zurechenbarkeit) und Ausnahmefall (Zurechenbarkeit möglich) unterschieden wird. [RS00]

Mittels Pseudonymen werden personenbezogene Daten so verändert, daß sie ohne Kenntnis der zugehörigen Zuordnungsregel nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zuordenbar sind, für den Ausnahmefall aber mittels der Zuordnungsregel die Identifizierung der Person ermöglichen. Für Kenner der Zuordnungsregel sind die pseudonymen Daten personenbeziehbar, für diejenigen, die die Zuordnungsregel nicht kennen, sind sie praktisch anonym. [RS00]

Da für die Parteien, welche die Zuordnungsregel nicht kennen, die Daten praktisch anonym bzw. nicht personenbezogen sind, fallen die Daten für diese Parteien nicht unter die Datenschutzgesetze. Für diese Parteien entfallen dementsprechend der generelle Erlaubnisvorbehalt, sowie die mit der Verarbeitung verbundenen weitreichenden Pflichten gegenüber den Betroffenen (s. Abschnitt 3). [RS00]

Damit stellen Pseudonyme ein Schlüsselkonzept für den mehrseitig sicheren Umgang mit Audit-Daten dar, ja sie ermöglichen in vielen Umgebungen erst die gesetzeskonforme Erhebung und Speicherung von Audit-Daten.

Im Normalfall sind die Daten für eine Partei nur solange anonym, bis die enthaltenen Pseudonyme ihr gegenüber mit Hilfe der Zuordnungsregel aufgedeckt wurden. Damit die wieder personenbeziehbaren Daten ab diesem Zeitpunkt nicht unter die Datenschutzgesetze fallen, ist der Aufdeckungszweck geeignet einzuschränken und der Aufdeckungszeitpunkt daran auszurichten.

"Falls Angriffe bzw. Sicherheitsverletzungen mit dem Charakter von Straftaten oder Ordnungswidrigkeiten durch das IDS erkannt werden, dürfen gemäß [BDSG] §14(2) die aufgezeichneten Daten zu deren Verfolgung genutzt werden." [Bun02] "[...] wenn bereits während der Nutzung vorauszusehen ist, daß gerade diese Daten für die Strafverfolgung erforderlich sind, käme die Ausnahme in §6(3) TDDSG zum Zuge [...]" [Jae00], so daß Mißbrauchsverläufe mittels personenbezogener Daten zugerechnet werden können. Daneben führt "[...] das TDDSGÄndG [...] §6 Abs. 8 ein, der es dem Teledienstanbieter erlaubt, personenbezogene Daten desjenigen Nutzers zu speichern, der seinen Teledienst mißbraucht. Die Anhaltspunkte, die zu der Annahme eines solchen Mißbrauchs geführt haben, sind vor der Speicherung [der personenbezogenen Daten] genau zu dokumentieren. Zu Zwecken der Rechtsverfolgung darf der Diensteanbieter diese personenbezogenen Daten auch über die Speicherfristen hinaus verarbeiten und nutzen. Da das bisherige Gesetz dem Teledienstanbieter generell verbietet, [personenbezogene] Daten zu erheben und zu speichern, wenn nicht einer der wenigen Erlaubnistatbestände vorlag, wäre es dem Teledienstanbieter heute nicht möglich, den Verursacher des Mißbrauchs durch Recherche in seinen Log-Dateien festzustellen." [Jae00]

Es sollte also erlaubt sein, anonyme Anhaltspunkte zu im voraus definierten Mißbräuchen während deren Verlauf zu speichern, da die anonymen Anhaltspunkte keine personenbezogenen Daten enthalten. In Anlehnung an die obigen Zitate kann man davon ausgehen, daß es erlaubt ist, die Anhaltspunkte eines Mißbrauchsverlaufs mittels Aufdeckung der enthaltenen Pseudonyme zurechenbar zu machen, sobald der anonyme Verlauf so weit voranschreitet, daß ein hinreichender Anfangsverdacht für einen Mißbrauch vorliegt. Wird die beschriebene Aufdeckungsbedingung technisch unumgehbar durchgesetzt, sprechen wir von *technischer Zweckbindung* (s. Abschnitt 5.1.1).

Für den Fall der Pseudonym-Aufdeckung sind geeignete Vorsorgeregelungen vorzusehen [RS00]. Dazu gehört u.a. die Herstellung von Transparenz gegenüber dem Nutzer, z.B. darüber, daß seine Anonymität bei Mißbrauch aufgehoben wird. Desweiteren sind Maßnahmen zur Sicherung der Pseudonymitätseigenschaft vorzusehen. In diesem Kontext sind die Ausführungen im Abschnitt 6.2 über die Kontrolle der Zuordnungsregel zu sehen.

5 Pseudonyme

Für die Definition von Pseudonymen werden die in [PK00] vorgeschlagenen Definitionen für die Unverkettbarkeit, die Anonymität und die Anonymitätsmenge verwendet.

Zwei Objekte sind *unverkettbar* bezüglich eines Angreifers, wenn die Wahrscheinlichkeit, daß beide Objekte zueinander in Beziehung stehen, vor und nach jeder dem Angreifer möglichen Beobachtung gleich ist. Zwei Objekte stehen dann zueinander in Beziehung, wenn sie im Hinblick auf ein Merkmal korrelieren, z.B. in Inhalt, Größe oder Zeitstempel übereinstimmen. Eine *ID* ist ein Prinzipal, der eine Entität eindeutig identifiziert, z.B. eine Person. Basierend darauf ist ein gegebenes Objekt *anonym*, wenn es mit keiner ID verkettbar ist. Entsprechend ist eine ID anonym, wenn sie mit keinem Objekt verkettbar ist. Ein Objekt ist *zurechenbar*, wenn es mit einer ID verkettbar, also nicht anonym ist. Ein Objekt ist z.B. ein Ereignis. Die *Anonymitätsmenge* bezüglich eines anonymen Ereignisses ist die Menge der Subjekte, die das Ereignis ausgelöst haben können. Je mächtiger die Anonymitätsmenge zu einem anonymen Ereignis ist, desto aufdeckungsresistenter ist es [9].

[9] Idealerweise soll die Anonymitätsmenge so mächtig sein, daß eine Deanonymisierung aller Teilnehmer dem Angreifer keinen größeren Vorteil verschafft im Vergleich zum Nachteil, der dem Angreifer durch die Deanonymisierung erwächst [PWP00].

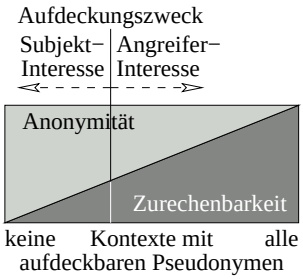


Abbildung 15: Interessenkonflikt und Zweckbindung bei der Pseudonym-Aufdeckbarkeit im Hinblick auf die kontrollierte Aufdeckbarkeit

Ein *Pseudonym* ist ein Prinzipal, der per se ungeeignet ist, die zugeordnete Entität zu identifizieren. Ein Objekt ist *pseudonymisierbar*, wenn es nach der Entfernung jener enthaltenen Prinzipale, die mit IDs übereinstimmen, anonym ist. Die *Pseudonymisierung* bezeichnet den Vorgang der Ersetzung ebendieser Prinzipale durch Pseudonyme gemäß einer Zuordnungsregel, anstatt ihrer Entfernung. Die *Zuordnungsregel* ordnet jedem verwendeten Pseudonym eindeutig die dadurch ersetzte ID zu[10]. Eine ID kann durch verschiedene Pseudonyme ersetzt werden. Nach der Pseudonymisierung enthält das Objekt keine Prinzipale, die mit einer ID verkettbar sind. Das *pseudonymisierte* bzw. *pseudonyme* Objekt ist anonym gegenüber Entitäten, welche die Zuordnungsregel nicht kennen. Für eine Entität, welche die zugehörige Zuordnungsregel kennt, sind die in einem Objekt enthaltenen Pseudonyme *aufdeckbar*. Die *Aufdeckung* eines Objekts besteht in dessen Verkettung mit der Zuordnungsregel. Das Objekt wird *reidentifiziert*, indem jedes Pseudonym durch die ihm von der Zuordnungsregel zugeordnete ID ersetzt wird. Nach der *Reidentifizierung* ist das Objekt wieder zurechenbar.

5.1 Pseudonym-Eigenschaften

In Abschnitt 4.1 wurde ein Ansatz vorgestellt, um mittels Pseudonymen einen fairen Ausgleich der konfligierenden Schutzziele Anonymität und Zurechenbarkeit herzustellen. Beide Schutzziele sind unmittelbar mit der kontrollierten Aufdeckbarkeit von Pseudonymen verbunden. Die andere Dimension von Pseudonymen ist ihre Verkettbarkeit, ohne die viele Dienste nicht möglich wären. Auch setzen viele Verfahren zur Analyse von Audit-Datensätzen deren Verkettbarkeit voraus. Die beiden Dimensionen Aufdeckbarkeit und Verkettbarkeit sind nicht voneinander unabhängig, wie die Definition von Anonymität zeigt.

5.1.1 Aufdeckbarkeit (kontrollierte)

Die *kontrollierte Aufdeckbarkeit* von Pseudonymen stellt eine kontrollierte Möglichkeit dar, pseudonymisierte Objekte von ihrem anonymen Zustand in einen zurechenbaren Zustand zu überführen. Diese Möglichkeit wird über die Kenntnis der Zuordnungsregel kontrolliert.

Die Entität, deren Eigeninteresse das Schutzziel Anonymität ist, wird als *IA* bzw. Subjekt bezeichnet. Analog heißt der Interessenträger für die Zurechenbarkeit *IZ* bzw. Angreifer (im Hinblick auf die Anonymität). Eine Entität, der *IA* dafür vertrauen kann, daß sie *IA*'s Anonymität schützt, trägt die Bezeichnung *VA* bzw. Agent. Analoges gilt für die Entität *VZ* im Hinblick auf die Zurechenbarkeit. Schließlich bezeichnet *VAZ* eine Entität, der *IA* und *IZ* vertrauen können, ihrer beider Interessen entsprechend einem Zweck fair auszugleichen.

organisatorische Zweckbindung: Die Entität, welche die Zuordnungsregel verwaltet, ist in der Verantwortung, die Reidentifizierung nur für legitime Zwecke und im Auftrag berechtigter Entitäten durchzuführen. Wenn

[10] Bei *Gruppenpseudonymen* ordnet die Zuordnungsregel jedem Gruppenpseudonym alle dadurch ersetzten IDs zu. Gruppenpseudonyme werden hier nicht weiter betrachtet.

die Verantwortung über den Umgang mit der Zuordnungsregel einer Person übertragen wird, findet bei der Reidentifizierung eine *organisatorische Zweckbindung* statt. Die korrekte Zweckbindung sorgt für einen fairen Ausgleich zwischen den Schutzzielen Anonymität und Zurechenbarkeit im Sinne mehrseitiger Sicherheit. Abb. 15 zeigt den Interessenkonflikt von Subjekt *IA* und Angreifer *IZ* hinsichtlich der Aufdeckbarkeit. Der durch Zweckbindung zu wahrende Aufdeckungszweck bestimmt in welchen Kontexten Pseudonyme aufdeckbar sein müssen, hier dargestellt durch die senkrechte Linie, die andeutet, innerhalb wie vieler Kontexte gemäß Aufdeckungszweck Pseudonyme aufdeckbar sind. Eine korrekte organisatorische Zweckbindung ist aber nur dann verläßlich möglich, wenn die reidentifizierende Entität kein überwiegendes Eigeninteresse an nur einem der beiden Schutzziele hat. Damit scheiden *IA* und *IZ* hierfür aus. Stattdessen können *IA* und *IZ* der Entität *VAZ* vertrauen, daß sie den Interessenkonflikt zweckgemäß löst. Alternativ kann das Vertrauen nach dem Vier-Augen-Prinzip auf zwei Entitäten *VA* und *VZ* verteilt werden, z.B. mittels Schwellenwert-Kryptosystemen [DF89]. Bei der Aufdeckung unter organisatorischer Zweckbindung muß *IZ* mit *VAZ* bzw. mit *VA* und *VZ* interagieren, damit diese für ihn pseudonymisierte Daten reidentifizieren.

technische Zweckbindung: Der Zweck der Aufdeckbarkeit kann auch bereits in die Erzeugung der Pseudonyme eingehen, indem man die Zuordnungsregel in geschützter Form den pseudonymisierten Daten beifügt. Der Zweck bestimmt, unter welchen Bedingungen dieser Schutz unwirksam ist und die Zuordnungsregel zur Reidentifizierung genutzt werden kann. Sind die Bedingungen nicht erfüllt, so sind die Pseudonyme nicht aufdeckbar. Paßt man die Zuordnungsregel bei der Pseudonym-Erzeugung kryptographisch diesen Bedingungen an, erhält man Pseudonyme mit unumgehbar *technisch zweckgebundene*r Aufdeckbarkeit. Gegenüber der organisatorischen Zweckbindung fließt der Zweck in technisch implementierte Bedingungen sein, d.h. die Bedingungen und die Verkettbarkeit sind in der Regel applikationsspezifisch zu formulieren. Da die technische Zweckbindung über die Bedingungen gesteuert wird, dürfen diese nur von einer Entität kontrolliert werden, der die Interessenträger vertrauen, die konfligierenden Interessen dem Zweck entsprechend fair auszugleichen: *VAZ*. Bei der technischen Zweckbindung kann *IZ* die pseudonymisierten Daten ohne weitere Interaktion und zeitnah selbst reidentifizieren, sobald die Bedingungen erfüllt sind.

Kombination von organisatorischer und technischer Zweckbindung: Stellt sich im nachhinein heraus, daß die Bedingungen nicht vollständig den intendierten Zweck modellieren, müßten alle Pseudonyme entsprechend der neuen Parameter angepaßt werden. Dies ist i.a. nicht praktikabel. Wenn es in dieser Situation dennoch notwendig ist, die Pseudonyme aufzudecken, kann parallel zur technischen Zweckbindung das Verfahren für die organisatorische Zweckbindung zum Einsatz kommen. So ermöglicht die technische Zweckbindung im Normalfall eine zeitnahe Reidentifizierung, während in Ausnahmesituationen die langsamere organisatorische Zweckbindung zum Einsatz kommen kann.

Vorgehensweise bei unzweckmäßiger Aufdeckung: Mittels zusätzlicher organisatorischer Zweckbindung läßt sich zwar das Problem bei der technischen Zweckbindung kompensieren, daß Daten aufgrund einer unvollständigen Modellierung nicht aufdeckbar sind (Fehlerklasse 1) [11]. Jedoch kann eine fehlerhafte Modellierung auch dazu führen, daß die technische Zweckbindung eine kontrollierte Aufdeckung von Pseudonymen erlaubt, die tatsächlich keinen Anfangsverdacht für Mißbrauch erfüllen (Fehlerklasse 2) [12]. Deswegen wird folgende organisatorische Vorgehensweise bei der Aufdeckung von Pseudonymen unter technischer Zweckbindung vorgeschlagen.

Jede Pseudonym-Aufdeckung durch *IZ* wird zusammen mit der zweckorientierten Begründung und den Daten protokolliert, die zur Beurteilung der Validität der Aufdeckung notwendig sind. Jede protokollierte Aufdeckung sollte dem jeweils betroffenen Nutzer (*IA*) zur Kenntnis gebracht werden. Dies ließe sich so realisieren, daß jeder so erzeugte Aufdeckungs-Datensatz nach seiner Erzeugung zeitnah von *IZ* abgearbeitet werden muß, indem

[11] Die Fehlerklasse 1 entspricht bei der Entdeckung von Schutzzielverletzungen durch Intrusion-Detection-Systeme einem falschen Negativ-Bericht, also dem Ausbleiben eines Alarms trotz eines vorliegenden Anfangsverdacht für Mißbrauch.

[12] Die Fehlerklasse 2 entspricht bei der Entdeckung von Schutzzielverletzungen durch Intrusion-Detection-Systeme einem falschen Positiv-Bericht, also einem falschen Alarm, obwohl kein Anfangsverdacht für Mißbrauch vorliegt.

entweder *IA* oder *VA* über die Aufdeckung informiert wird. Ergibt die Untersuchung der Aufdeckungs-Audit-Daten durch *IZ*, daß ein Fehler der Klasse 2 vorliegt, kann *IA* umgehend direkt informiert werden. Besteht jedoch der begründete Verdacht, daß tatsächlich ein Mißbrauch durch *IA* vorliegt, kann es kontraproduktiv sein, *IA* umgehend zu informieren. *IZ* kann in diesem Fall die Informierung von *IA* für die Dauer der Klärung des Mißbrauchs-Vorfalls unter Angabe von Gründen zurückstellen. Im Gegenzug kann *IA*'s Interessenvertreter *VA* alle zurückgestellten Aufdeckungs-Datensätze nebst Begründung einsehen und so eine Kontrollfunktion ausüben (organisatorische Zweckbindung).

Beispiele für die Implementierung der Zuordnungsregel: Die Zuordnungsregel kann auf verschiedene Weise implementiert werden. Wird sie als eine Tabelle implementiert, ist diese Tabelle geeignet zu schützen. Die Aufdeckung geschieht durch Suchen des Pseudonyms in der Tabelle, welchem die fragliche ID zugeordnet ist. Wird die Zuordnungsregel als eine parametrisierbare kryptographische Funktion implementiert, kann die Funktion offengelegt werden, die gewählten Parameterwerte sind zu schützen. Beispielsweise läßt sich eine technische Zweckbindung durch kryptographische Geheimnisteilung erreichen. Die Funktion kann eine kryptographische Dechiffrierfunktion sein, so daß die Aufdeckung durch Berechnung der Funktion unter der Eingabe des Pseudonyms und der Parameterwerte die ID ergibt. Die Pseudonyme werden dementsprechend durch Chiffrieren der ID mit der korrespondieren Chiffrierfunktion und den korrespondierenden Parameterwerten gebildet.

Eine Variante der Pseudonymbildung verwendet eine kryptographische kollisionsresistente (parametrisierbare) Hashfunktion anstatt einer Chiffrierfunktion (s. Jaeger-Anonymisierer in Abschnitt 6.4). In diesem Fall läßt sich die Hashfunktion nicht umkehren, so daß nach der hier verwendeten Definition keine Zuordnungsregel für die geordnete Aufdeckung existiert. Eine Aufdeckung der in Objekten enthaltenen Pseudonyme kann dennoch durchgeführt werden, sofern die Parameterwerte und alle fraglichen IDs bekannt sind. Dann können alle fraglichen IDs in Pseudonyme überführt und diese mit Pseudonymen in den Objekten abgeglichen werden. Alternativ läßt sich ein Verdachtsmoment über eine ID zu einem Pseudonym in einem Objekt bestätigen, indem die verdächtigte ID in ihr Pseudonym überführt wird und mit dem Pseudonym im Objekt verglichen wird.

Verfügbarkeit der Zuordnungsregel: Die Zuordnungsregel und die entsprechenden pseudonymisierten Daten, die beim Kenner der Zuordnungsregel gespeichert sind, sind für diesen personenbezogene bzw. personenbeziehbare Daten und unterliegen dem Datenschutz [RS00]. Der Kenner muß also entsprechende Schutzmaßnahmen ergreifen. Im Folgenden werden die möglichen Kenner der Zuordnungsregel genannt [PK00, RS00]. Für die Reidentifizierung benötigt *IZ* bei der organisatorischen Zweckbindung die Kooperation des Kenners. Bei der technischen Zweckbindung benötigt *IZ* bei erfüllten Bedingungen hierfür nur die pseudonymisierten Daten. Bei jedem Kenner ist vermerkt, ob die pseudonymisierten Daten für den Datenverwender *IZ* personenbeziehbar sind, ob mehrseitige Sicherheit oder nur einseitige Sicherheit hinsichtlich eines Schutzziels erreichbar ist, und ob *IZ* für die Reidentifizierung mit einem Kenner interagieren muß bzw. eigenständig reidentifizieren kann.

öffentlich: personenbeziehbar; einseitig (Zurechenbarkeit); eigenständig

Datenverwender (*IZ*): personenbeziehbar (nicht personenbeziehbar gegenüber Dritten); einseitig (Zurechenbarkeit); eigenständig

Agent (*VAZ* bzw. *VA* und *VZ*): nicht personenbeziehbar; mehrseitig wenn der/die Agent(en) vertrauenswürdig sind, sonst einseitig; Kooperation des/der Agenten

Daten: nicht personenbeziehbar; mehrseitig wenn der pseudonymisierende Agent *VAZ* vertrauenswürdig ist, sonst einseitig; eigenständig

Subjekt (*IA*): nicht personenbeziehbar; einseitig (Anonymität); Kooperation des Subjekts

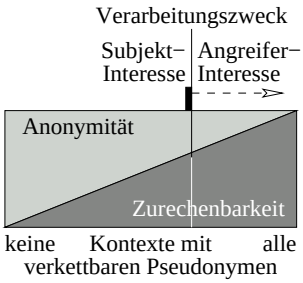


Abbildung 16: Interessenkonflikt und Zweckbindung bei der Pseudonym-Verkettbarkeit im Hinblick auf die unkontrollierte Aufdeckbarkeit

5.1.2 Verkettbarkeit

Aus der Definition der Anonymität folgt der Einfluß der Verkettbarkeit auf die Anonymität eines Objekts [SK03]. Je häufiger und in je mehr verschiedenen Kontexten ein Pseudonym verwendet wird, desto mehr Objekte sind direkt und transitiv mit dem Pseudonym verkettbar. Damit ist die Chance größer, daß sich darunter ein zurechenbares Objekt befindet, das eine *unkontrollierte Aufdeckung* der mit dem Pseudonym verkettbaren Objekte ermöglicht. Ein Pseudonym sollte daher möglichst selten und in möglichst wenigen verschiedenen Kontexten verwendet werden, etwa durch häufigen Pseudonymwechsel. Entsprechend kann man Pseudonyme nach den Kontexten klassifizieren, in denen sie verwendet werden. In [PK00] werden Kontexte vorgeschlagen, in denen ein entsprechendes Pseudonym ausschließlich verwendet wird. Die entsprechenden Pseudonyme heißen bei steigender Aufdeckungsresistenz:

Subjekt-Pseudonym: in jedem Kontext

Rollen-Pseudonym: im Kontext einer spezifischen Rolle

Beziehungs-Pseudonym: im Kontext einer spezifischen Kommunikations-Beziehung

Rollen-Beziehungs-Pseudonym: im Kontext einer spezifischen Rolle bei einer spezifischen Kommunikations-Beziehung

Transaktions-Pseudonym: im Kontext einer spezifischen Transaktion

Analog zur Zweckbindung bei der Pseudonym-Aufdeckung kann auch der Zweck der Verarbeitung der pseudonymisierten Daten bei der Pseudonym-Erzeugung in deren Verkettbarkeit eingehen. Der Verarbeitungszweck bestimmt die Parameter des Verarbeitungs-Algorithmus und damit in welchen Kontexten die Pseudonyme eines Subjekts verkettbar sein müssen. Im Gegensatz zur Zweckbindung der Aufdeckung wird bei der *Zweckbindung der Verkettbarkeit* den Pseudonymen keine geschützte Information beigefügt. Erfordert die Verarbeitung in einem spezifischen Kontext es, werden die Pseudonyme eines Subjekts so erzeugt, daß sie unmittelbar verkettbar sind. Andernfalls sind die Pseudonyme des Subjekts unverkettbar. Da die Verarbeitung der pseudonymen Daten sowohl im Interesse des Subjekts als auch des Datenverwenders liegt, besteht hinsichtlich der Verkettbarkeit per se kein Interessenkonflikt. Die Verkettbarkeit hat jedoch Einfluß auf die unkontrollierte Aufdeckbarkeit und berührt so die Interessen von *IA* und *IZ*. Folglich muß die Pseudonym-Erzeugung analog zur Zweckbindung der Aufdeckbarkeit von *VAZ* kontrolliert werden, damit der für die Verarbeitung im beidseitigen Interesse notwendige Trade-Off zwischen Verkettbarkeit und Aufdeckbarkeit nicht zu Ungunsten der Anonymität ausgeweitet wird. Abb. 16 zeigt den Interessenkonflikt von Subjekt *IA* und Angreifer *IZ* hinsichtlich der unkontrollierten Aufdeckbarkeit. Der durch Zweckbindung zu wahrende Verarbeitungszweck bestimmt, in welchen Kontexten Pseudonyme verkettbar sein müssen, hier dargestellt durch die senkrechte Linie, die andeutet, innerhalb wieviele r Kontexte gemäß Verarbeitungszweck Pseudonyme verkettbar sind. Das kleine schwarze Rechteck deutet die im Interesse des Subjekts liegende Anzahl von Kontexten mit verkettbaren Pseudonymen an. Dementsprechend möchte *IA* nicht mehr und nicht weniger Kontexte mit verkettbaren Pseudonymen als vom Verarbeitungszweck

vorgegeben, während der Angreifer zwecks unkontrollierter Aufdeckung möglichst viele Kontexte mit verkettbaren Pseudonymen anstrebt.

5.1.3 Weitere Eigenschaften:

In der Literatur sind Verfahren zur Gewährleistung zusätzlicher Eigenschaften von Pseudonymen und den zugehörigen Eigenschaftsaussagen dokumentiert [PK00, KB00] auf die an dieser Stelle nicht vertiefend eingegangen wird:

- die mandatorische Beteiligung spezifizierter verantwortlicher Agenten bei der Beglaubigung einer Eigenschaftsaussage oder der Bildung der Pseudonyme;
- die Übertragbarkeit des Pseudonyms mit/ohne Preisgabe wertvoller Geheimnisse bei Gewährleistung der Authentisierung der vorlegenden Partei;
- die Veränderbarkeit des Pseudonyms bei Gewährleistung der Validität der Eigenschaftsaussage;
- die Beschränkung der Anzahl der Pseudonyme je Subjekt;
- die Beschränkung der Anzahl der möglichen Nutzungen; [13]
- die Beschränkung der Geltungsdauer;
- die Möglichkeit, jederzeit die Gültigkeit zu widerrufen bzw. die Eigenschaftsaussage zu sperren.

5.2 Unbeobachtbarkeit anonymer Ereignisse

Zusätzlich zur Anonymität von Ereignissen durch deren Pseudonymisierung kann man die Unbeobachtbarkeit von Ereignissen betrachten. Die Definition und die Maßnahmen zur Unbeobachtbarkeit stehen orthogonal zur Definition und zu Maßnahmen der Pseudonymisierung.

Ein Ereignis ist *unbeobachtbar* bezüglich eines Angreifers, wenn die Eintritts-Wahrscheinlichkeit nach jeder dem Angreifer möglichen Beobachtung gleich ist. Eine Standardmaßnahme um die Eintritts-Wahrscheinlichkeit eines Ereignisses aus der Sicht des Unbeobachtbarkeits-Angreifers konstant zu halten, ist, Ereignisse regelmäßig auszulösen. Werden also keine echten Ereignisse ausgelöst, werden stattdessen Strohmann-Ereignisse ausgelöst, die für den Unbeobachtbarkeits-Angreifer nicht von echten Ereignissen unterscheidbar sind.

Handelt es sich bei dem Ereignis um das Senden einer Nachricht, so gibt es zwei Empfänger des Ereignisses: den Unbeobachtbarkeits-Angreifer und den legitimen Ereignis-Empfänger. Strohmann-Ereignisse dürfen den legitimen Ereignis-Empfänger nicht stören. Die Nachrichten müssen also eine neutrale Wirkung auf ihn haben. Dies ist realisierbar, wenn der legitime Ereignis-Empfänger über einen Ereignis-Filter verfügt, der alle Strohmann-Ereignisse verwirft. Sind der legitime Ereignis-Empfänger und der Angreifer verschiedene Entitäten, können Strohmann-Ereignisse bei ihrer Auslösung ausschließlich für den legitimen Ereignis-Empfänger als solche erkennbar gekennzeichnet werden.

Wenn Angreifer und legitimer Ereignis-Empfänger jedoch dieselbe Entität sind, könnte der Angreifer die Strohmann-Ereignisse als solche erkennen. Verfügt der Angreifer unabhängig von Strohmann-Ereignissen bereits über einen Ereignis-Filter, der auch legitime Ereignisse verwirft, könnten Ereignisse dieser Sorte unbeobachtbar gemacht werden, indem Strohmann-Ereignisse der selben Sorte ausgelöst werden. Diese Strohmann-Ereignisse verwirft der Angreifer, ohne wissen zu müssen, daß es Strohmann-Ereignisse sind. Beim Entwurf ist zu entscheiden, ob es lohnt, gerade jene Ereignisse unbeobachtbar zu machen, die der Angreifer nicht weiter verarbeitet (s. Abschnitt 6.3).

[13] In Abschnitt 7.2 wird die Beschränkung der Anzahl der Pseudonymnutzungen zur Realisierung der technischen Zweckbindung der Aufdeckbarkeit eingesetzt.

6 Ein Architektur-Modell für anonyme Autorisierungen

In diesem Abschnitt wird das in Abschnitt 2 eingeführte Modell um pseudonymbasierte Anonymität erweitert. Zunächst werden die Eigenschaftsaussagen aus Abschnitt 2.1 in Abschnitt 6.1 im Hinblick auf Pseudonyme interpretiert, die in Abschnitt 2.2 dargestellten Architekturen in Abschnitt 6.2 um Reidentifizierung, Audit-Daten-Erhebung, und -Verarbeitung erweitert und die Kontrollverhältnisse in Bezug auf Anonymität von Dienst-Audit-Daten verfeinert. Schließlich werden die einzelnen Anonymisierungsebenen in Abschnitt 6.3 vergleichend untersucht. Abschnitt 6.4 zeigt, wie das Modell zur Klassifizierung von Anonymitäts-Technologien verwendet werden kann.

6.1 Anonyme Eigenschaftsaussagen

Die Verifizierer beglaubigter Eigenschaftsaussagen benötigen in vielen Fällen keine IDs für ihre Tätigkeit [vRGB+95]. Für sie ist lediglich wichtig, daß die enthaltenen Attribute authentisch der vorlegenden Entität zugeordnet sind, daß die Eigenschaftsaussage von einem Agenten beglaubigt wurde, dem sie vertrauen, und daß die Aussage gültig ist. Beispielsweise enthält das Zoo-Eintritts-Ticket aus Abschnitt 1.1 nicht den Namen des Inhabers, sondern nur eine ihm eindeutig zugeordnete Ticket-Nummer, die als Inhaber-Pseudonym interpretiert werden kann.

Sind in einem Autorisierungsszenario keine IDs notwendig, können Eigenschaftsaussagen und ihre Referenzen anonymisiert werden, indem der Subjekt-Prinzipal durch ein Pseudonym mit geeigneten Eigenschaften ersetzt wird (s. Abschnitt 5). Das deutsche Signaturgesetz sieht bereits entsprechende Beglaubigungen vor (§7 Abs. 1-3 SigG) [RS00]. Ebenfalls ist sicherzustellen, daß auch die anderen Eigenschaftsaussage-Komponenten keine IDs der Subjekt-Entität enthalten oder aufgrund ihrer Einzigartigkeit Rückschlüsse auf die Subjekt-Entität zulassen. Zusätzlich wird im Modell eine Annahme dahingehend gemacht, daß die Empfänger der Eigenschaftsaussage keine Beobachtungen machen können, nach denen das Pseudonym mit einer ID der Subjekt-Entität verkettbar ist. Mit der Ausnahme der kontrollierten Aufdeckung durch den Agenten bleibt die Eigenschaftsaussage den Empfängern gegenüber anonym.

So ist es etwa an der Zoo-Kasse nicht notwendig, den Namen des Studierenden zu erfahren. Wichtig ist nur, daß die Eigenschaft *Studierender* an die Person gebunden ist, die einen gültigen Studierenden-Ausweis vorlegt, und daß dieser von einem vertrauenswürdigen Agenten ausgestellt wurde. Dementsprechend könnte der Studierenden-Ausweis anonym ausgelegt werden, indem in die Subjekt-Komponente statt des Namens die Matrikel-Nummer des Studierenden eingetragen würde.

Der Agent ist nun einerseits im Interesse der Zurechenbarkeit den Verwendern der Eigenschaftsaussage gegenüber zusätzlich dafür verantwortlich, daß er entsprechend seiner im voraus festgelegten Politik zu spezifischen Zwecken gegenüber spezifischen Entitäten mittels der Zuordnungsregel Pseudonyme aufdeckt. Andererseits ist der Agent im Interesse der Anonymität den Subjekt-Entitäten gegenüber dafür verantwortlich, die Zuordnungsregel zu schützen und hinsichtlich der Aufdeckbarkeit und Verkettbarkeit der Pseudonyme seine dem Subjekt bekannte Politik einzuhalten.

Geeignete Pseudonyme: Hinsichtlich beider Dimensionen – (kontrollierte) Aufdeckbarkeit und Verkettbarkeit – sind die Eigenschaften der Pseudonyme zu bestimmen, die für anonyme beglaubigte Eigenschaftsaussagen geeignet sind.

Zuordnungsregeln, die öffentlich oder nur dem Datenverwender bekannt sind, sind für anonyme Eigenschaftsaussagen ungeeignet, da mit ihnen nur einseitig die Zurechenbarkeit der Pseudonyme realisiert werden kann, aber keine Anonymität. Entsprechend kommen ausschließlich der Subjekt-Entität bekannte Zuordnungsregeln für Eigenschaftsaussagen nicht ein Betracht, da mit ihnen nur einseitig Anonymität realisiert werden kann, aber keine verläßliche Zuordnung der Subjekt-Eigenschaften möglich ist. Übrig bleiben Zuordnungsregeln, die Agenten

bekannt sind. Er kann die Pseudonym-Aufdeckung mittels der Zuordnungsregel entweder organisatorisch oder technisch an den in seiner Politik formulierten Aufdeckungszweck binden.

Der Agent kann entsprechend seiner Politik die Nutzbarkeit eines Pseudonyms auf spezifische Kontexte einschränken. Hier ist das ganze Spektrum zwischen Subjekt- und Transaktions-Pseudonymen möglich. Kommen allerdings Referenzen auf beglaubigte Eigenschaftsaussagen zum Einsatz, sind aufgrund des fehlenden Synchronismus zwischen den Subjekt-Komponenten von Eigenschaftsaussage und deren Referenz keine Transaktions-Pseudonyme möglich. Dementsprechend setzt der Einsatz von Transaktions-Pseudonymen anonyme beglaubigte Eigenschaftsaussagen voraus, die der Agent dem Subjekt zur Nutzung zur Verfügung stellt.

6.2 Architekturen und Kontrollverhältnisse

Der durch die Anwendung von Pseudonymen erreichbare Grad der Anonymität sollte proportional zum Risiko durch Datenerhebung und -verarbeitung sowie dem Aufwand eines Angreifers sein. Um den von einem System für anonyme Autorisierungen gewährleisteten Grad an Anonymität zu bestimmen, ist eine systemspezifische Analyse der Möglichkeiten eines Angreifers hinsichtlich Verkettbarkeit bzw. Aufdeckbarkeit notwendig [SK03]. Eine genaue Aussage über den erreichbaren Grad an Anonymität einer gegebenen Architektur ist also nur bei genauer Analyse des einzelnen implementierenden Systems hinsichtlich eines definierten Angreifers möglich. Bei identischem Angreifer-Modell sind Systeme, die Architekturen für anonyme Autorisierungen implementieren, vergleichbar.

Allerdings lassen sich auch ohne eine genaue Bestimmung des erreichbaren Grads der Anonymität Eigenschaften von Architekturen für anonyme Autorisierungen identifizieren, welche Aufschluß über die Möglichkeiten eines Angreifers im Hinblick auf die Anonymität bzw. Verkettbarkeit sowie über die Sicherheit der Autorisierungen und die Praktikabilität der Architektur geben (s. Abschnitt 6.3).

Das *Angreifer-Modell* spezifiziert, welche möglicherweise kollaborierenden Parteien welche personenbezogene Daten erheben und korrelieren können (s. Abschnitt 6.2.1). Eine Architektur für anonyme Autorisierungen gibt an, *wann* und *wo* personenbezogene Daten im System pseudonymisiert werden, und gibt damit vor, gegen welche Angreifer-Modelle es schützen kann. Je früher im Datenpfad die personenbezogene Daten pseudonymisiert werden, desto größere Bereiche dürfen Anonymitäts-Angreifer kontrollieren, ohne daß der Grad an Anonymität beeinträchtigt wird. Dementsprechend kann bei gegebenem Angreifer-Modell eine geeignete Architektur ausgewählt werden (s. Abschnitt 6.2.2). Dabei ist zu beachten, daß je nach Angreifer-Modell, der Angreifer Zugriff auf Daten in verschiedenen Schichten des OSI-Referenzmodells haben kann. Die Semantik der Autorisierungen und der in Anspruch genommene Dienst sind nicht auf die Anwendungs-Schicht beschränkt, sondern sind für jede Schicht geeignet zu bestimmen. Für jede Schicht, in der der Angreifer Daten einsehen kann, ist eine geeignete Architektur für die Pseudonymisierung zu wählen.

Beim Entwurf von Architekturen für anonyme Autorisierungen sind mit dem Blick auf geeignete Angreifer-Modelle weitere Faktoren zu berücksichtigen. Betrachtet man im Sinne mehrseitiger Sicherheit zusätzlich zur Anonymität die Zurechenbarkeit, so ergibt sich, daß sowohl die Pseudonymisierung, als auch die kontrollierte Aufdeckung von Pseudonymen nicht allein von einer Partei durchführbar sein darf, welche ein überwiegendes Interesse an nur einer der beiden Anforderungen hat. Die Kontrollbereiche aller beteiligten Parteien sind entsprechend zu definieren und nach Möglichkeit technisch, sonst organisatorisch, voneinander abzuschotten (s. Abschnitt 6.2.2). Das Verfahren für die Pseudonymisierung und für die kontrollierte Pseudonym-Aufdeckung bestimmt die erforderliche Kooperation und Anzahl der dabei beteiligten Parteien und ist geeignet auszuwählen (s. Abschnitte 5.1.1 und 6.2.3). Lassen sich Aufdeckbarkeit und Verkettbarkeit parametrisieren, so sollen die Parameter so gewählt werden, daß sie einen fairen Ausgleich erlauben. Die gewählten Parameter sollen allen beteiligten Interessenvertretern bekannt sein.

6.2.1 Anwendungsszenario und Angreifer-Modell

Bei der Betrachtung anonymer Architekturen ist das Angreifer-Modell ein wichtiger Bezugspunkt, da es die notwendigen Kontrollverhältnisse bestimmt und festlegt, in welcher Phase Pseudonyme spätestens eingeführt werden müssen. Die Einführung von Pseudonymen muß geschehen, bevor der Angreifer Beobachtungen machen kann, die ihm die Verkettung der Pseudonyme mit IDs der Subjekt-Entität ermöglichen. Folgend werden auf Abschnitt 2.2 basierend Architekturen vorgestellt, die Nutzer-Anonymität gegenüber den *Sicherheits-Administratoren* eines Dienstes herstellen, welche Beobachtungen ausschließlich auf der Basis der vom Dienst gelieferten Audit-Daten machen können (s. Abb. 18 bis Abb. 21). Die Audit-Daten werden von der *Audit-Komponente* des Dienstes erhoben und der *Audit-Analyse* der Sicherheits-Administratoren des Dienstes verfügbar gemacht (s. E1 in Abb. 17). Diese erzeugt entsprechend des *Analyse-Zwecks Einzelberichte* und sendet sie an die *Antwort-Einheit* (s. E2 in Abb. 17), welche wiederum geeignet auf die Einzelberichte reagiert, z.B. indem sie den Sicherheits-Administrator unterrichtet und ihm Handlungsvorschläge macht. Ein Einzelbericht kann einen *Analyse-Kontext* enthalten, der eine Untermenge der Audit-Daten ist. Eine konkrete Instanz dieses Szenarios wäre ein Intrusion-Detection-System, dessen Analyse-Zweck das Entdecken bekannter und durch die Dienstnutzer verursachter Anfangsverdachte für *Schutzzielverletzungen* bzw. Mißbräuche ist. Ein Einzelbericht ist ein *Alarm*, der als Analyse-Kontext etwa die *Anhaltspunkte* für den Anfangsverdacht in der Form von *Audit-Datensätzen* enthält, die den Verlauf der Schutzzielverletzung dokumentieren, um weitere Untersuchungen zu unterstützen (s. Abschnitt 4.1). Hier werden also Architekturen betrachtet, die Pseudonyme einführen, bevor die Audit-Daten die Audit-Analyse erreichen, welche den Sicherheits-Administratoren Beobachtungen des Nutzerverhaltens ermöglicht. Dementsprechend unterliegen die Sicherheits-Administratoren im Hinblick auf die pseudonymen Audit-Daten keinen Verarbeitungsbeschränkungen durch die Datenschutzgesetze [RS00]. Das kommt der hier gemachten Annahme entgegen, daß die Sicherheits-Administratoren hinsichtlich der Wahrung der Nutzer-Anonymität nicht das Vertrauen der Nutzer genießen, also aus Nutzersicht potentielle Angreifer der Nutzer-Anonymität sind.

6.2.2 Architekturen

Die Abb. 18 bis Abb. 21 zeigen die dem Modell aus Abb. 4 entsprechenden anonymen Versionen, bei denen eine Entität Anonymität der Dienst-Nutzer gegenüber den Sicherheits-Administratoren herstellt, indem sie ein Nutzer-Pseudonym erstmalig einführt. Einerseits lassen sich die anonymen Versionen kombinieren, so daß mehrere Entitäten Pseudonyme einführen. Andererseits existieren für die Varianten in Abb. 9 bis Abb. 12 ebenfalls entsprechende anonyme Versionen. Die Eigenschaften der anonymen Varianten und der Kombinationsmöglichkeiten sind im einzelnen nicht Gegenstand der Betrachtung.

In den Abbildungen zeigen die *durchgezogenen Pfeile* die Flußrichtung zurechenbarer und beglaubigter bzw. nachgewiesener Aussagen über Eigenschaften bzw. deren Referenzen an. Die *gestrichelten Pfeile* zeigen die Flußrichtung der anonymen und ggf. beglaubigten Aussagen über Eigenschaften bzw. deren Referenzen an. Schließlich zeigen die *gepunkteten Pfeile* die Flußrichtung der Zuordnungsregel an. Jede fette graue Umrahmung schließt einen Bereich ein, in dem die Interessen einer Entität durchgesetzt werden. Gemäß Abschnitt 1.2 dürfen in diesem Bereich jene Entitäten keine Kontrolle ausüben, deren Interessen mit den im Bereich durchgesetzten Interessen im Konflikt stehen. Dabei stehen die dunkelgrauen Umrahmungen für das Nutzerinteresse Anonymität und die hellgrauen Umrahmungen für das Interesse der Sicherheits-Administratoren an Zurechenbarkeit. Dunkel ausgefüllte Kästen realisieren gemeinsam mehrseitige Sicherheit. Sie befinden sich gerade in den doppelt umrahmten Bereichen, also dort, wo konfligierende Interessen durchgesetzt werden.

In diesem Szenario mit konfligierenden Interessen verschiedener Entitäten ist es einfach, einseitige Sicherheit zu erreichen, indem man alle mit den Interessen einer Partei in Konflikt stehenden Interessen vollständig aufgibt. Entsprechend Abschnitt 1.2 zeigt Abb. 17, wie zugunsten der Zurechenbarkeits-Anforderung der Sicherheits-Administratoren Nutzer-Anonymität unmöglich wird. Die Sicherheits-Administratoren müssen hier dem Beglaubiger, dem Autorisierer und dem Dienst hinsichtlich Zurechenbarkeit vertrauen. Da der Nutzer ein mit der Zurechenbarkeit konfligierendes Interesse an Anonymität hat, können die Sicherheits-Administratoren ihm nicht vertrauen, Eigenschaftsaussagen verläßlich zu reidentifizieren.

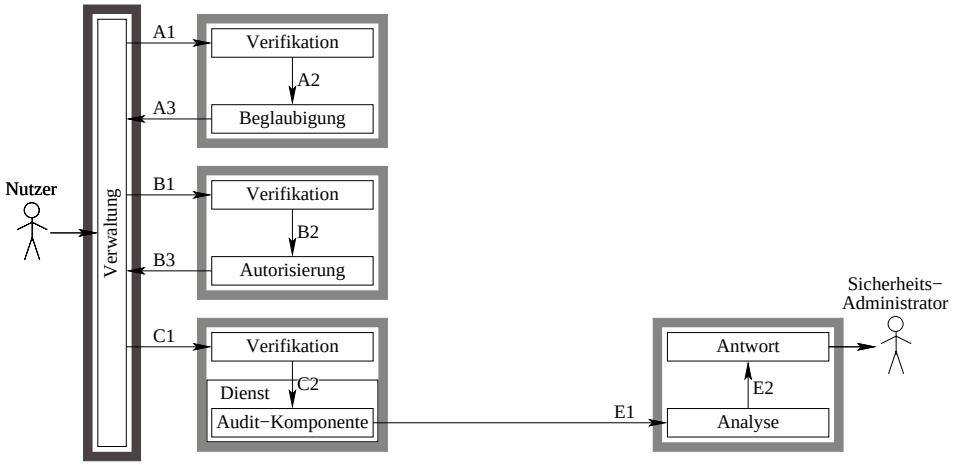


Abbildung 17: Einseitig sicher: Zurechenbarkeit

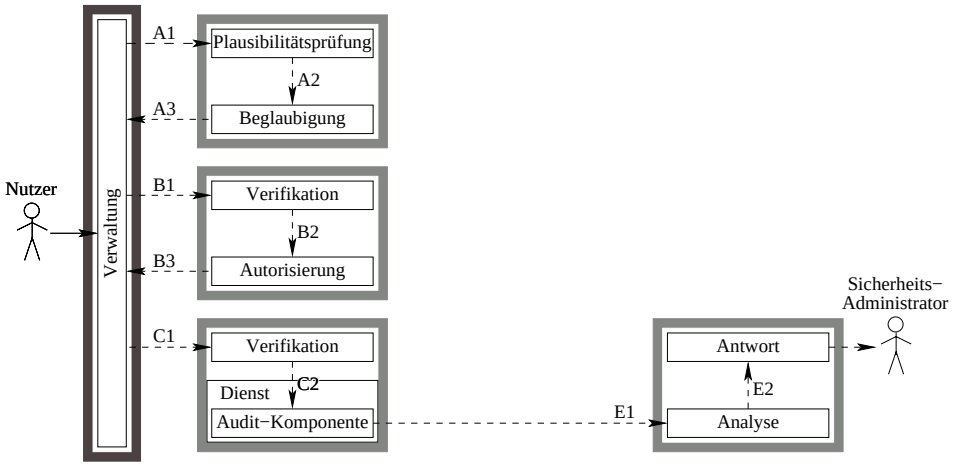


Abbildung 18: Einseitig sicher: Anonymität durch die Verwaltung

Aufgrund desselben Arguments kann im Szenario einseitige Sicherheit zugunsten der Anonymität entstehen, wenn der Beglaubiger die von der Verwaltung des Nutzers ausgewählten Subjekt-Prinzipale nicht daraufhin prüft, daß sie tatsächlich IDs des Nutzers sind. Wenn er solche Eigenschaftsaussagen akzeptiert, ließen diese sich nicht verläßlich aufdecken, weil die zugehörige Zuordnungsregel unter der Kontrolle der Verwaltung des Nutzers steht, dem die Sicherheits-Administratoren nicht hinsichtlich Zurechenbarkeit vertrauen (s. Abb. 18, vgl. Abschnitt 6.1).

Ebenfalls einseitige Sicherheit hinsichtlich Anonymität wird erreicht, wenn eine Entität, die anonyme beglaubigte Eigenschaftsaussagen ausstellt, die Zuordnungsregel nicht für die Reidentifizierung zur Verfügung stellt, d.h. bei dieser Entität wird die Herstellbarkeit von Zurechenbarkeit unterbrochen. Demnach können die Sicherheits-Administratoren dieser Entität nicht hinsichtlich Zurechenbarkeit vertrauen. In Abb. 19 bis Abb. 21 würde bei der Entität, welche die Anonymität herstellt, entsprechend die hellgraue Umrahmung, der gepunkteten Pfeil sowie die Reidentifizierung fehlen. Authentisierung und Beglaubigung wären nicht dunkel ausgefüllt.

Die Versionen für einseitige Sicherheit sind einfacher zu realisieren, weil die Entität, deren Schutzziel durchgesetzt wird, nur Agenten benötigt, die lediglich ihr Schutzziel durchsetzen, die also nicht in einem Interessenkonflikt stehen.

Da in mehrseitig sicheren Versionen gegenläufige Interessen mehrerer Entitäten berücksichtigt werden sollen, führt dies gemäß Abschnitt 1.2 und Abschnitt 6.2 zum Ausschluß der Kontrolle eben dieser Entitäten über die

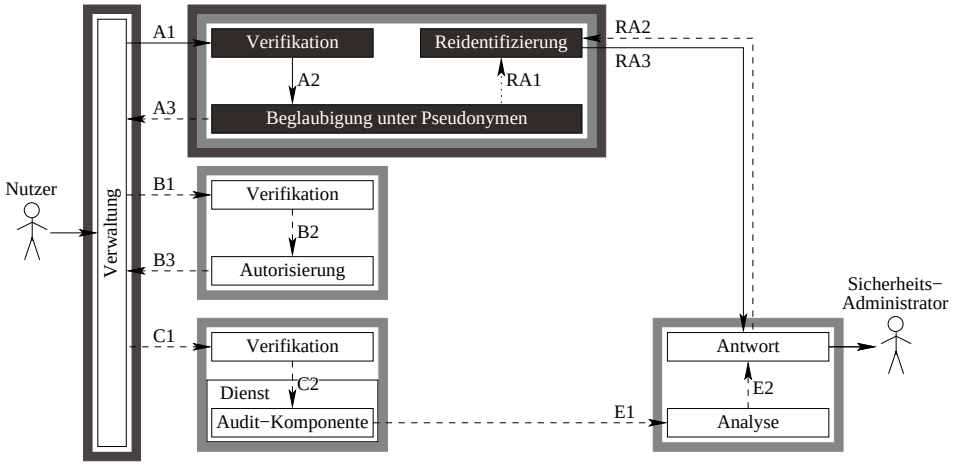


Abbildung 19: Mehrseitig sicher: Anonymität und Zurechenbarkeit durch den Beglaubiger

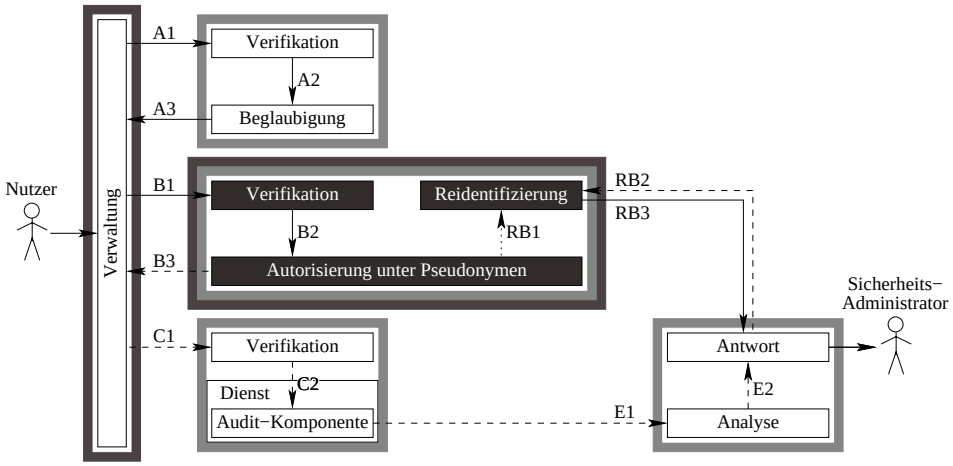


Abbildung 20: Mehrseitig sicher: Anonymität und Zurechenbarkeit durch den Autorisierer

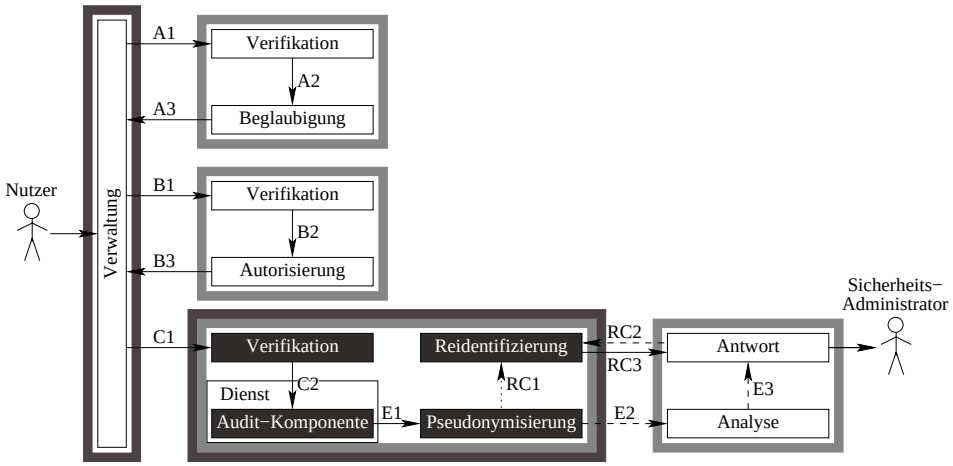
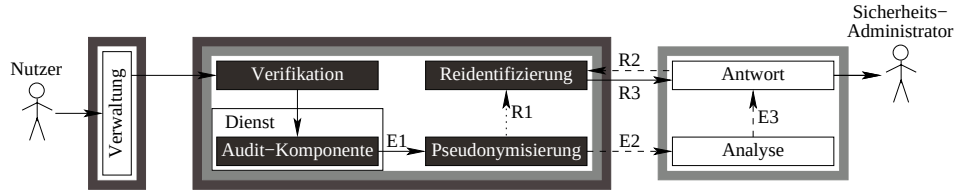
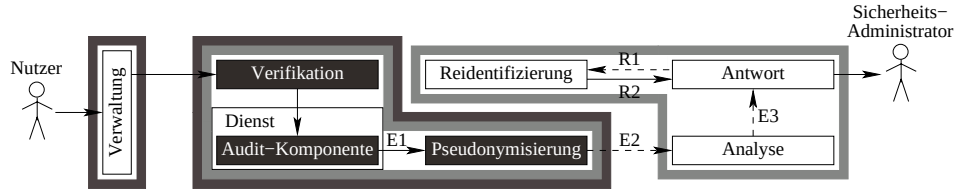


Abbildung 21: Mehrseitig sicher: Anonymität und Zurechenbarkeit durch den Dienst



(a) organisatorische Zweckbindung



(b) technische Zweckbindung

Abbildung 22: Zweckbindung der kontrollierten Aufdeckbarkeit

Interessenobjekte, also die Pseudonyme in den Eigenschaftsaussagen. Entsprechend Abschnitt 6.1 ist für mehrseitige Sicherheit die Zuordnungsregel von Agenten zu kontrollieren, denen auch nach Abschnitt 1.2 die Interessenträger vertrauen müssen. Diese Situation ist in Abb. 19 bis Abb. 21 dargestellt. Die jeweilige Entität, die Zurechenbarkeit und Anonymität der Eigenschaftsaussagen verantwortet, genießt das Vertrauen beider Interessenträger unter Ausschluß deren Kontrolle. Die dunkel gefüllten Funktionskomponenten realisieren zusammen die mehrseitige Sicherheit für die Interessenträger.

Die mehrseitig sicheren Versionen sind schwieriger zu realisieren, da beide Interessenträger Agenten finden müssen, denen sie gemeinsam vertrauen können, den Interessenkonflikt gemäß dem in der Politik formulierten Aufdeckungs- und Verarbeitungszweck zu lösen. Je nach Agent ist dieser Interessenkonflikt verschieden kritisch (s. Abschnitt 6.3). Um dieses Problem zu lösen, können Agenten in mehrere Sub-Agenten zerlegt werden, so daß ein Ergebnis nur bei Kooperation einer geeigneten Menge von Subagenten erreichbar ist. Dies kann etwa durch Überschlüsseln wie in Mix-Netzen [FH01] oder mittels Schwellenwert-Kryptosystemen [SS00, DF89] erreicht werden. Diese Vorgehensweise wird hier nicht betrachtet.

6.2.3 Zweckbindung

In Abb. 19 bis Abb. 21 sind nur Architekturen für Pseudonyme mit organisatorischer Zweckbindung und die dafür notwendigen Kontrollverhältnisse dargestellt. Abb. 22 zeigt am Beispiel eines Dienstes mit einem Pseudonymisierer, wie der Einsatz der technischen Zweckbindung für die kontrollierte Aufdeckbarkeit die notwendigen Kontrollverhältnisse vereinfacht. Bei der technischen Zweckbindung der Aufdeckbarkeit wird den Pseudonymen die zweckgebunden geschützte Zuordnungsregel beigefügt (s. E2 in Abb. 22b), so daß diese nicht mehr direkt dem Reidentifizierer übermittelt werden muß (vgl. R1 in Abb. 22a). Die Reidentifizierung ist so unumgehbar nur noch entsprechend dem Zweck der kontrollierten Aufdeckung möglich. Demgemäß muß der Nutzer derjenigen Entität, welche die Reidentifizierung kontrolliert, nicht mehr vertrauen. Da also die Sicherheits-Administratoren nicht mehr von der Kontrolle des Reidentifizierers ausgeschlossen sind, können sie die Reidentifizierung selbst kontrollieren und unverzüglich durchführen, sobald der entsprechende Zweck vorliegt. Die in Abschnitt 5.1.1 beschriebene organisatorische Vorgehensweise zur Handhabung von Aufdeckungsfehlern der Klasse 2 könnte zwar technisch unterstützt werden. Sie basiert bei den vorgeschlagenen Kontrollverhältnissen allerdings auf dem Vertrauen darin, daß kein Sicherheits-Administrator diese Maßgaben umgeht. Im Modell ist eine technische Zweckbindung analog für Autorisierer und Beglaubiger möglich (s. Abb. 19 und Abb. 20), aber unterschiedlich sinnvoll (s. Abschnitt 6.3).

Tabelle 1: Übersicht über die Eigenschafts-Kriterien, gruppiert nach inhaltlichem Bezug zu Vertrauen, operationaler Sicherheit, Praktikabilität. Kriterium ist: ‘ $\surd$’=erfüllt, ‘$-$’=nicht erfüllt, ‘%’=gegenstandslos

Eigenschafts-Kriterien	Pseudonym-ausgebende Entität			
	Verwaltung	Beglaubiger	Autorisierer	Dienst
Mehrseitige Sicherheit	$-$	$\surd$	$\surd$	$\surd$
Dienst-Unabhängigkeit	$\surd$	$\surd$	$-$	$-$
Vertrauenswürdige Attributzuordnung	$-$	$\surd$	$\surd$	%
Technische Zweckbindung	$-$	$-$	$\surd$	$\surd$
Pseudonymverifikation vor Zugriff	$\surd$	$\surd$	$\surd$	$-$
Nutzer-Unabhängigkeit	$-$	$-$	$-$	$\surd$
Infrastruktur-Unabhängigkeit	$\surd$	$-$	$-$	$\surd$

6.3 Architekturen für anonyme Autorisierungen im Vergleich

Die Abb. 18 bis Abb. 21 zeigen die verschiedenen Entitäten, die Pseudonyme einführen können, so daß die Audit-Analyse nur anonyme Audit-Daten erhält. Dabei hat das Einführen der Pseudonyme bei jeder Entität spezifische Vor- und Nachteile, welche im Folgenden diskutiert und in Tab. 1 zusammengefaßt werden.

Mehrseitige Sicherheit: Mehrseitige Sicherheit kann mit Hilfe jener Entitäten erreicht werden, die nicht selbst Träger der konfligierenden Interessen sind. Diese Entitäten sind der Beglaubiger, der Autorisierer und der Dienst (s. Dienst-Unabhängigkeit). Bei entsprechender Politik können diese Entitäten auch stets einseitig zugunsten eines Interesses handeln. Demgegenüber handeln Entitäten, die Träger nur eines Interesses sind, immer einseitig zugunsten dieses Interesses. Dazu gehört im Modell die Verwaltung.

Dienst-Unabhängigkeit: Auch wenn die Entität kein Interessenträger ist, so kann doch die Organisation, der sie angehört, Träger eines Interesses sein. Da die Entität von der Organisation abhängig ist, könnte sie sich parteiisch zugunsten dieses Interesses verhalten. Dies läßt sich bei der Wahl des Beglaubigers vermeiden. Da der Autorisierer aber aufgrund seiner Aufgabe mit dem Dienst assoziiert ist, könnte er parteiisch handeln. Selbiges gilt auch für den Dienst selbst. Man versucht in der realen Welt durch organisatorische Maßnahmen parteiisches Verhalten zu vermeiden, indem es eine Person in der Organisation gibt, welche die Aufgabe hat, das Nutzerinteresse zu vertreten. Diese Aufgabe fällt meist dem Datenschutzbeauftragten zu. Der Grad der Abhängigkeit der Person von der Organisation bestimmt, zugunsten wessen Interessen sie sich parteiisch verhalten wird. Besteht die beschriebene Abhängigkeit, wird der Nutzer der Entität (Autorisierer, Dienst) hinsichtlich der Wahrung seines Interesses an Anonymität weniger Vertrauen entgegenbringen können. Besteht keine Abhängigkeit, kann der Nutzer der Entität vertrauen (Verwaltung, Beglaubiger).

Vertrauenswürdige Attributzuordnung: Ob die hinter einer pseudonymen Eigenschaftsaussage verborgene Person tatsächlich die angegebenen Eigenschaften besitzt, hängt davon ab, welche Entität für die Eigenschaftsaussage verantwortlich ist. Ist es ein Agent, der auch die Interessen des Dienstes wahrt, ist die Eigenschaftszuordnung vertrauenswürdig. Ist die Verwaltung verantwortlich, ist gemäß Abschnitt 1.2 zu folgern, daß die Eigenschaftszuordnung nicht vertrauenswürdig ist. Da bei der Pseudonymisierung durch den Dienst keine Eigenschaften zugeordnet werden, ist dieses Kriterium beim Dienst gegenstandslos.

Technische Zweckbindung: Wie bei Diensten ist eine technische Zweckbindung analog für Autorisierer möglich (s. Abschnitt 6.2). Da Beglaubigungen zur Erlangung von Autorisierungen für viele verschiedene Dienste geeignet sind, müßten entsprechend viele Verarbeitungs-Zwecke antizipiert und berücksichtigt werden. Da dadurch

eine massive Erosion der Anonymität der Beglaubigungen zu erwarten ist, erscheint eine technische Zweckbindung durch Beglaubiger nicht sinnvoll. Schließlich sind Eigenschaftsaussagen, für welche die Verwaltung verantwortlich ist, nicht verläßlich dem Subjekt zuordenbar, wodurch sich jedwede Zweckbindung erübrigt.

Pseudonymverifikation vor Zugriff: Werden Pseudonyme im Modell noch vor der dritten Phase des Dienst-Zugriffs eingeführt, kann der Dienst die Gültigkeit der Autorisierungen sowie der Pseudonym-Eigenschaften noch vor dem Zugriff prüfen. Anfragen mit ungültigen Autorisierungen können abgewiesen und somit Schaden vermieden werden. Werden Pseudonyme erst während oder nach dem Zugriff im Dienst durch einen Pseudonymisierer eingeführt, der nicht Teil der Zugriffskontroll-Komponente des Dienstes ist, können ungültige Pseudonyme auftreten, ohne daß der damit verbundene Zugriff blockiert werden kann. Dieses Kriterium ist komplementär zum Kriterium *Nutzer-Unabhängigkeit*.

Nutzer-Unabhängigkeit: Wenn die Entität, welche die Pseudonyme einführt, auf ein entsprechendes Software-Gegenstück beim Nutzer oder auf die korrekte Bedienung durch den Nutzer angewiesen ist, findet die Herstellung der Anonymität nicht nutzer-unabhängig statt. Einerseits eröffnet dies durch Fehlbedienung Risiken für die Anonymität. Andererseits hat der Dienst entsprechend Abschnitt 3 ein Interesse daran, daß die Audit-Daten anonym vorliegen, um nicht die gesetzlichen Datenschutz-Anforderungen erfüllen zu müssen. Nutzer-Unabhängigkeit ist daher beidseitig von Vorteil. Dieses Kriterium ist komplementär zum Kriterium *Pseudonymverifikation vor Zugriff*.

Infrastruktur-Unabhängigkeit: Kommen in der Modell-Variante beglaubigte Eigenschaftsaussagen zum Einsatz, erfordert dies eine Infrastruktur, mittels derer sich die Nutzer bei den Agenten registrieren können. Der zum Aufbau einer solchen Infrastruktur erforderliche Aufwand und die Rahmenbedingungen haben einen beträchtlichen Einfluß darauf, in welchem Zeitrahmen die Infrastruktur auf breiter Basis zur Verfügung gestellt werden kann. Die Erfahrungen, die bei der Etablierung von Infrastrukturen für anonyme Kommunikation und elektronische Münzen im großen Rahmen gemacht wurden, bestätigen dies [Gol02]. Infrastruktur-Unabhängigkeit ist im Interesse einer raschen Implementierung von Anonymität.

Unbeobachtbarkeit: Aufgrund der Vielzahl der an dieses Kriterium geknüpften Bedingungen wird es nicht in der Übersicht dargestellt. Zwar können in den verschiedenen Modell-Varianten in den Abb. 4 und Abb. 9 bis Abb. 12 die einzelnen Entitäten Strohmann-Ereignisse auslösen. Für die Verwaltung, den Beglaubiger und den Autorisierer macht dies jedoch wenig Sinn. Entweder ist der Dienst in der Lage, Strohmann-Ereignisse als solche zu erkennen und zu verwerfen; d.h. die Strohmann-Ereignisse erscheinen als solche in den Audit-Daten oder sie werden gar nicht gespeichert. So kann den Sicherheitsadministratoren gegenüber keine Unbeobachtbarkeit hergestellt werden. Idealerweise sind die Strohmann-Ereignisse aus der Sicht der Diensterbringung neutrale Ereignisse. In diesem Fall bestimmt das Analyse-Verfahren, ob Unbeobachtbarkeit erreicht werden kann, oder ob es zu Störungen kommt.

Der Pseudonymisierer des Dienstes kann leicht Strohmann-Datensätze in die Audit-Daten einbringen. Da die Analyse-Einheit als Empfänger der Audit-Daten gleichzeitig vom Angreifer auf die Unbeobachtbarkeit kontrolliert wird, müssen die Strohmann-Datensätze so beschaffen sein, daß sie von der Analyse-Einheit verworfen werden, ohne als Strohmann-Datensätze erkannt zu werden.

Basiert die Analyse auf Modellen über die normale Dienstnutzung[14], würden die Strohmann-Datensätze die Analyse stören, sofern sie nicht verworfen werden. Sind die verworfenen Strohmann-Datensätze für den Unbeobachtbarkeits-Angreifer von Interesse, könnten sie unbeobachtbar gemacht werden.

[14] Bei der Entdeckung von Schutzzielverletzungen durch Intrusion-Detection-Systeme wird die auf Modellen über normale Dienstnutzung basierende Analyse auch als *Anomaly-Detection* bezeichnet [McH01].

Wenn die Analyse auf Modellen über Mißbrauchsverhalten basiert [15], werden Datensätze verworfen, die normales Nutzungsverhalten repräsentieren. Daher kann normales Nutzungsverhalten unbeobachtbar gemacht werden, indem durch Strohmann-Datensätze mindestens eine Filterbedingung der Analyse erfüllt wird. Die Bedingung, die ungefährliche Ereignis-Typen verwirft, kann zustandslos, also einfach erfüllt werden. Alle anderen Bedingungen wirken kontextabhängig und wären pseudonymisiererseitig nur unter großem Aufwand erfüllbar. Mithin ist es aufwendig, das gesamte normale Nutzungsverhalten unbeobachtbar zu machen, für eine spezifische Teilmenge ist es jedoch einfach.

6.4 Beispiele existierender Architekturen für anonyme Autorisierungen

Für jede pseudonym-ausgebende Entität in Tab. 1 werden im Folgenden beispielhaft datenschutzfördernde Technologien angegeben, die Anonymität in der Rolle dieser Entität implementieren. Die Auswahl erhebt nicht den Anspruch, einen repräsentativen Überblick über die vorhandene Literatur zu verschiedenen datenschutzfördernden Technologien und deren Implementierungen zu geben. Die Betrachtung von anonymen Eigenschaftsaussagen erlaubt die Klassifizierung von Autorisierungssystemen, umfaßt aber nicht sämtliche Möglichkeiten für anonymes Handeln in verteilten Systemen. Folgende Anwendungen werden daher im Folgenden nicht weiter betrachtet: anonymes Publizieren [SDDW+01, Gol02], anonyme Wahlen [SDDW+01], anonyme Auktionen [SDDW+01], anonyme Tauschbörsen [DNC+02], Private Information Retrieval (PIR) [CGKS98] und dessen Anwendungen wie etwa gezielte Werbung [Jue01].

In der Literatur sind drei Ansätze zu finden, die alle Entitäten des Modells abdecken. Die Korrespondenzen zwischen unserem Modell und diesen Ansätzen werden bei den Beispielen aufgeführt. Alamäki et al. definieren verschiedene funktionale Komponenten (*Profile Broker, Identity Broker, Authenicator*), die für Architekturen anonymer Autorisierungen benötigt werden, und geben verschiedene Architekturen an [ABD+02], ohne jedoch deren Eigenschaften gegeneinander abzugrenzen und die erforderlichen Kontrollverhältnisse anzugeben.

Die niederländische Datenschutzbehörde *Registratiekamer* hat zusammen mit dem Informations- und Datenschutzbeauftragten der Provinz Ontario (Kanada) ein Modell für Informationssysteme angegeben [vRGB+95, Bor96]. Basierend auf diesem Modell wird der Vorgang von Autorisierungen inklusive Audit-Daten analog zur Modell-Variante in Abb. 11 beschrieben, d.h. es wird zunächst von lokal beim Dienst vorgehaltenen Eigenschaftsaussagen ausgegangen, die aufgrund der lokalen Speicherung keiner Agenten- und Validitäts-Komponenten bedürfen. Der Nutzer erhält dementsprechend nur Referenzen auf die ihn betreffenden Eigenschaftsaussagen. An verschiedenen Stellen des Modells kann ein *Identity Protector* plaziert werden. Er fungiert als eine pseudonymeinführende Entität, die also die Domänen, in denen IDs bekannt sind von denjenigen Domänen trennt, in denen mit Pseudonymen gearbeitet wird. Die sich ergebenden Architekturen werden beschrieben, ohne deren Eigenschaften gegeneinander abzugrenzen und die erforderlichen Kontrollverhältnisse anzugeben. Die mit unserem Modell korrespondierenden Stellen werden unten bei den entsprechenden Entitäten aufgeführt. Eine spätere Studie beschäftigt sich mit dem Datenschutz in Systemen mit intelligenten Software-Agenten und zeigt in diesem Szenario die Einsatz- und Implementierungsmöglichkeiten für den Identity Protector auf [BvES99]. Die Studie weist darauf hin, daß bei hohen Anforderungen an den Datenschutz die folgenden Merkmale von Agenten-Systemen nicht in Anspruch genommen werden können: Mobilität von Nutzeragenten, Klonen von Nutzeragenten, von Dritten zur Verfügung gestellte Nutzeragenten.

Der dritte Ansatz dient dem *datenschutzfördernden Identitätsmanagent*. Dabei soll der Nutzer selbst bestimmen können, wer welche Daten über ihn erhält, und er soll verschiedene Lebensbereiche bei Bedarf trennen können, so daß verschiedene Adressaten einen ganz unterschiedlichen Blick auf die jeweilige Teilidentität der Person haben können [Han03]. Das Identitätsmanagementsystem umfaßt dabei die Applikationen, die Middleware und die Kommunikationsinfrastruktur. Auf Applikationsebene werden die Anforderungen an die Teilidentitäten, welche durch Eigenschaftsaussagen repräsentiert werden, ausgehandelt und festgelegt. Dies geschieht zwischen dem

[15] Bei der Entdeckung von Schutzzielverletzungen durch Intrusion-Detection-Systeme wird die auf Modellen über Mißbrauchsverhalten basierende Analyse auch als *Misuse-Detection* bezeichnet [McH01].

Identitätsmanager des Nutzers (Verwaltung) und dem Dienstanbieter (Dienst). Der Ansatz befaßt sich nicht nur mit anonymen Autorisierungen, sondern soll auch den anonymen elektronischen Behördengang und den anonymen elektronischen Handel ermöglichen. Datenschutzförderndes Identitätsmanagement stützt sich daher nicht nur auf Beglaubiger und Autorisierer (s.u.) mit kontrollierter Aufdeckbarkeit sowie auf eine Infrastruktur für anonyme Kommunikation (s.u. Anonymität von Sender und/oder Empfänger) ab, sondern erfordert weitere Mediatoren bzw. Treuhänder für den digitalen Güteraustausch, für den Ausgleich von Verbindlichkeiten, für elektronische Zahlungen (s.u. elektronische Münzen) und schließlich für die Auslieferung von Gütern in der realen Welt. [CK01, CPHVH02]

6.4.1 Verwaltung

Identity Protector: Die Verwaltung entspricht dem Identity Protector, wenn dieser nutzerseitig zwischen der Repräsentation des Nutzers und des Dienstes implementiert wird [vRGB+95, Bor96]. In Agenten-Systemen entspricht dies der Integration mit dem bzw. dem Wrapping des Nutzeragenten [BvES99].

Identity Broker: Alamäki et al. definieren Identity Broker als Entitäten, die Pseudonyme einführen (vgl. Trusted Mobile Terminal in [ABD+02]).

Profile Broker: Alamäki et al. definieren Profile Broker als Zugangspunkte zu Nutzerprofilen, deren Inhalte den Attributen von Eigenschaftsaussagen entsprechen [ABD+02]. Profile Broker können um Contract Broker erweitert werden, welche die gegenseitigen Anforderung von Nutzern und Diensten hinsichtlich der Offenlegung von Nutzerprofilen nachweisbar aushandeln. (vgl. Trusted Mobile Terminal in [ABD+02])

Identitätsmanagement: Einerseits gehen Menschen in der realen Welt, die den Einzelnen heute immer wieder vor die Aufgabe einer Neuorientierung und Selbstordnung stellt, mit Teilidentitäten ganz selbstverständlich und natürlich um. Es hat sich jedoch gezeigt, daß der explizite Umgang mit verschiedenen Teilidentitäten in der digitalen Welt Nutzer häufig überfordert [Kum03]. Es ist daher erforderlich, den Nutzer beim Einsatz und der Verwaltung seiner Teilidentitäten und deren Verkettbarkeit [HR03] zu unterstützen. Auf dem Nutzer-Endgerät installierte Identitätsmanager unterstützen den Nutzer bei der Erstellung und Auswahl seiner Teilidentitäten bzw. Identitätsprofile, welche die Eigenschaftsaussagen beinhalten [SP98, DPR99].

Diese Funktionalität läßt sich anstatt direkt beim Nutzer auch bei einer Partei, sog. Infomediary, implementieren, welcher der Nutzer vertraut, oder auch auf mehrere solcher Parteien verteilen [GGK+99b, GGK+99a, GGMA97]. Ebensolche Implementierungen sind beispielsweise [Cra99, CK01]: Proxymate bzw. Lucent Personalized Web Assistant (LPWA)[16], digitalme[17] von Novell, SuperProfile von Lumeria[18], iPrivacy[19], PrivacyBank[20], Persona von Privaseek[21], v-GO von Passlogix[22] und die Freedom[23] Security and Privacy Suite.

Die Verwaltung kann jede Preisgabe von Eigenschaftsaussagen nachhalten [KB00, Brü03] und den Nutzer bei der Beurteilung des aktuellen Grades an Anonymität unterstützen. Die Selektierung der zu übertragenden Eigenschaftsaussagen, z.B. gemäß P3P [CLM+01], geschieht durch Abgleich der Anforderungen und Datenschutz-Politik des Dienstes bzw. verantwortlichen Agenten und der vom Nutzer definierten Identitätsprofile und die mit ihnen verknüpften Datenschutz-Anforderungen des Nutzers unter Einbeziehung der aktuellen Situation, in welcher der Nutzer agiert [CK01, CPHVH02, KB00, JGtM01, GtMJ01]. Analog zur

[16] http://www.bell-labs.com/project/lpwa

[17] http://www.digitalme.com

[18] http://www.lumeria.com

[19] http://www.iprivacy.com

[20] http://www.privacybank.com

[21] http://www.privaseek.com

[22] http://www.passlogix.com

[23] http://www.freedom.net

Vertrauensevaluierung seitens der Dienste bzw. verantwortlichen Agenten, findet eine Vertrauensevaluierung hinsichtlich deren Datenschutz-Politik bei der Verwaltung statt.

6.4.2 Beglaubiger

Identity Protector: Der Beglaubiger entspricht dem Identity Protector, wenn dieser als dritte Partei zwischen der Repräsentation des Nutzers und des Dienstes implementiert wird [vRGB+95, Bor96]. In Agenten-Systemen entspricht der Beglaubiger der nächsten vertrauenswürdigen Partei, die der Agent aufsuchen kann, damit diese durch Mediation den Datenschutz für den Agenten gewährleistet [BvES99].

Identity Broker: s.o. (vgl. Physical Separation of Identity and Profile in [ABD+02])

Authenticator: Alamäki et al. definieren einen Authenticator als eine Entität, welche die Authentisierung von Nutzern durchführt. Im Modell ist dies Teil der Verifikation (s. Abb. 3).

Identitätsmanagement: Das Identitätsmanagement stützt sich auf anonymen Credentials ab (s.u.).

Anonymität von Sender und/oder Empfänger: Um Anonymität effektiv zu gewährleisten, müssen in verteilten Systemen personenbezogene Daten auf allen Schichten des OSI-Referenzmodells vermieden werden. Daher erfordern Anonymitätsdienste in der Applikationsschicht zusätzlich Dienste, die eine anonyme Kommunikation gestatten. Einseitig sichere Anonymisierungsdienste unterstützen keine kontrollierte Aufdeckbarkeit [BFK00b]. Sie entsprechen meist der Architektur-Variante in Abb. 12. Dabei verteilen z.B. Mix-Systeme das Vertrauen, das der Nutzer hinsichtlich seiner Anonymität in den Beglaubiger haben muß, auf mehrere unabhängige Parteien. Es existieren verschiedene Implementierungen von Mix-Systemen: Onion Routing, Hordes, Freedom Network, JAP, Babel und Mixmaster-Remailer. Crowds und Cypherpunk-Remailer basieren auf ähnlichen Konzepten. Einfachere implementierte Systeme, die das notwendige Vertrauen nicht auf mehrere Parteien verteilen sind z.B. Anonymizer.com, Anonymouse und Anon.penet.fi. Einen Überblick über diese Technologien geben diverse Autoren [EP01, FH01, BFK00a, SDDW+01, Gol02, GWB97]. Es existieren Konzepte, die nachweisbar Sender-Anonymität herstellen, z.B. DC-Netze, oder Empfänger-Anonymität, z.B. mittels Broadcast-Übertragung [FH01, dKdDdBudL97]. Diese Konzepte sind aber nicht in allen Umgebungen effizient umsetzbar.

Anonyme Credentials: Anonyme Credentials sind die in Abschnitt 6.1 beschriebenen Beglaubigungen [Cha86, CE87, Cha87, Cha90, VH00, Bra00, GGLS01, SS00, CL01b, CL01a, LRSW99]. Sie sind als Beglaubigungen und als Autorisierungen einsetzbar. Eine einfache Konstruktion basierend auf einem beliebigen Signatursystem und einem Kommunikationsystem, das Senderanonymität gewährleistet, ist ebenfalls möglich [PWP00]. Ein Verfahren mit beweisbarer Sicherheit existiert, ist aber für praktische Anwendungen zu ineffizient [Dam88]. Beim Einsatz von Referenzen auf anonyme Eigenschaftsaussagen (s. Abb. 9 und Abb. 11) kann die Beobachtung der Abrufe zugehöriger Eigenschaftsaussagen zu Nutzungprofilen führen. Ein erster Ansatz soll dies vermöge PIR lösen [IS03].

Anonyme Authentisierung: Die Verifikation anonymer Eigenschaftsaussagen umfaßt unter anderem die anonyme Authentisierung der Partei, welche die Eigenschaftsaussage vorlegt (s. Authentisierungs-Komponente in Abschnitt 2.1). Hierfür existieren in der Literatur diverse Ansätze mit kontrollierter Aufdeckbarkeit [SPH99, GMI+01, HY01] oder aber auch ohne eine solche, dann aber mit einem starken Mechanismus zur Demotivation der unautorisierten Übertragung bzw. Weitergabe von anonymen Eigenschaftsaussagen [Han00]. Die Anonyme Authentisierung wird vorwiegend mittels Gruppensignaturen durchgeführt [CS97, KP98, KP97, BF99].

Elektronische Münzen: Faire elektronische Offline-Münzen bieten in der Regel eine technisch zweckgebundene, kontrollierte Aufdeckbarkeit, wenn jemand versucht, zweimal mit derselben Münze zu bezahlen [Neu03, SDDW+01, Pet97, DFTY97, CMS96, CPV99, Poi00, NHS99]. Dabei kommen vorwiegend Gruppensignaturen [DWND+01, Tra99, MB01], Magic Ink Signaturen [Jak97] oder faire blinde Signaturen [SPC95] zum Einsatz. Aber auch anonyme Credentials, deren Attribute einen finanziellen Wert kodieren und die nur beim ersten Vorzeigen gültig sind, könnten benutzt werden, um elektronische Münzen zu implementieren.

ANIDA-Kerberos (1): Für das Intrusion-Detection-System ANIDA wurde der *Kerberos-Authentication-Server* konzeptionell um Pseudonyme mit organisatorisch zweckgebundener Aufdeckbarkeit erweitert [BK99]. Eine Implementierung des Datenschutzkonzepts ist in der Literatur nicht dokumentiert.

6.4.3 Autorisierer

Identity Protector: s.o. beim Beglaubiger.

Identity Broker: s.o. beim Beglaubiger.

Identitätsmanagement: s.o. beim Beglaubiger.

Anonyme Credentials: s.o. beim Beglaubiger.

Anonyme Authentisierung: s.o. beim Beglaubiger.

ANIDA-Kerberos (2): Das Datenschutz-Konzept zu ANIDA kennt eine Variante, für die der *Kerberos-Ticket-Granting-Server* um einen mehrseitig sicheren Mix erweitert wird [BK99]. Diese Architektur entspricht der Variante in Abb. 10.

Unverkettbare serielle Transaktionen: Die vollständig unverkettbare Autorisierung serieller Transaktionen kann mittels lediglich einmal nutzbarer Credentials gewährleistet werden, deren Validität jeweils nach einer Nutzung für eine weitere Nutzung verlängert wird [SSG99].

Anonyme Internet-Anmeldung: Basierend auf fairen elektronischen Münzen [CFN88] kann die anonyme Anmeldung der Nutzer bei ihrem Internet Service Provider durchgeführt werden [Cha99].

Nutzerkonto unter Pseudonym: Die Bezeichner von Nutzerkonten können bei entsprechenden organisatorischen Voraussetzungen als Rollen-Pseudonyme genutzt werden [FH01, vRGB+95] (s. Architektur-Variante in Abb. 11, vgl. Abschnitt 2.3).

6.4.4 Dienst

Identity Protector: Ein Audit-Daten-Anonymisierer entspricht dem Identity Protector, wenn dieser dienstseitig zwischen der Repräsentation des Dienstes und den Audit-Daten implementiert wird [vRGB+95, Bor96].

Identitätsmanagement: Der Dienst muß die Autorisierung auf der Basis anonymer Eigenschaftsaussagen vorsehen und der Verwaltung des Nutzers gemäß der Sicherheitspolitik des Dienstes die Anforderungen über akzeptierte Eigenschaftsaussagen nennen bzw. mit ihm aushandeln [CK01, CPHVH02].

Die allgemeine Verarbeitung personenbezogener Daten sowohl des Nutzers als auch anderweitig Betroffener unterliegt der Zweckbindung. Analog zum Schutzziel Vertraulichkeit kann das Schutzziel Anonymität hinsichtlich bereits erhobener Daten lokal durch geeignete Zugriffskontrollen hergestellt werden. Ein entsprechendes Zugriffskontroll-Modell hat sich an den Aufgaben des Verarbeitenden zu orientieren und wurde von Fischer-Hübner formalisiert und implementiert [FH01]. Andererseits können Daten anonymisiert werden, wobei die Zweckbindung etwa mit kryptographischen Mitteln durchgesetzt wird. Im Folgenden wird der Schutz personenbezogener Daten von Nutzern und andereren Betroffenen durch Anonymisierung von Audit-Daten in den Blick genommen.

Eine zentrale Anforderung bei der Analyse von Audit-Daten hinsichtlich Anhaltspunkten für Mißbrauch ist die zeitnahe Pseudonym-Aufdeckbarkeit zwecks Zurechenbarkeit. Unter dem Gesichtspunkt der Praktikabilität sind die Unabhängigkeit der Lösung vom Nutzer und die Unabhängigkeit von aufwendigen Infrastrukturen entscheidend. Tab. 1 zeigt, daß diese Anforderungen gemeinsam nur auf Dienstebene erfüllbar sind. Die hierfür bekannten Ansätze werden im Folgenden vorgestellt und in Abschnitt 7 miteinander verglichen.

Intrusion Detection and Avoidance (IDA): Mit diesem nur teilweise implementierten Forschungs-System wurde das Konzept der Intrusion-Detection-Analyse auf anonymen Audit-Daten eingeführt [FH93, FH01, SFHR97, FHB89].

Adaptive Intrusion Detection (AID): Dieses Forschungs-System greift das mit IDA eingeführte Konzept der Analyse anonymer Audit-Daten auf, wobei sich die Architekturen von AID und IDA stark voneinander unterscheiden. AID wurde vollständig implementiert [MH00, Sob99, FH01, SFHR97, SRK96, Sob95].

Lundin Firewall Audit Anonymisierer: Lundins Anonymisierer ist ein Forschungs-System für die Anonymisierung der Audit-Daten einer spezifischen Proxy-Firewall. Auf den anonymisierten Daten wurden Intrusion-Detection-Experimente durchgeführt [LJ00, LJ99b, LJ99a].

Jaeger-Anonymisierer: Jaegers Anonymisierungs-Konzept bietet verkettbare Pseudonyme, die nicht kontrolliert aufgedeckt werden können. Sie können aber zur Bestätigung eines konkreten Verdachts zu einer ID dienen [Jae00].

WebWasher: Das kommerzielle Content-Filter-System WebWasher kann seine Audit-Daten bzw. Berichte anonymisieren. Zur Funktionsweise der Anonymisierung ist nur bekannt, daß die organisatorische Zweckbindung bei der kontrollierten Aufdeckung das 4-Augen-Prinzip anwendet [wA03].

BSMpseu: Das frei verfügbare Forschungs-System BSMpseu anonymisiert Solaris-BSM-Audit-Daten mittels verkettbarer Pseudonyme ohne Möglichkeit zur kontrollierten Aufdeckung. Auf den anonymisierten Daten wurden Intrusion-Detection-Experimente durchgeführt [Rie03].

Anonymouse: Der Anonymouse-Log-File-Anonymizer ist als kurzes Perl-Skript implementiert, das Web-Server-Audit-Daten anonymisiert. Dabei werden nur die Top-Level-Domains der Nutzer-Adressen beibehalten, so daß ggf. eine spezifische Top-Level-Domain vielen Nutzern zugeordnet ist. Demnach ist die Top-Level-Domain ein Gruppen-Pseudonym (vgl. Abschnitt 5). Eine kontrollierte Aufdeckung ist nicht möglich [EP01].

Pseudonymization with Conditional Reidentification (Pseudo/CoRe): Das frei verfügbare, portierbare Forschungs-System Pseudo/CoRe anonymisiert Audit-Daten im Sinne mehrseitiger Sicherheit. Dabei unterliegen die Pseudonym-Nutzungskontexte, der Pseudonym-Wechsel und die kontrollierte Pseudonym-Aufdeckung der technischen Zweckbindung [Fle03c, BF02, Fle03b, Fle02b, Fle02a, BF00b, BF00c, BF00a].

7 Anonyme Audit-Daten

Das nachträgliche Pseudonymisieren von Audit-Daten erzielt eine vergleichbare Wirkung wie die Dienstnutzung mittels pseudonymer Autorisierungen [RS00]. Allerdings stellt die spezifische Anwendungssituation andere Anforderungen an das Konzept und die Implementierung der Pseudonym-Erzeugung.

Die erste Anforderung betrifft die Performanz der Pseudonym-Erzeugung. Je nach Sorte des Dienstes, der die Audit-Daten erzeugt, kann ein extrem hohes Aufkommen zu bewältigen sein, insbesondere beim Dienst Betriebssystem, wenn es für Intrusion-Detection Systemrufe als Audit-Datensätze speichert. Die Pseudonym-Erzeugung findet idealerweise on-the-fly statt und sollte daher einen dem Datenaufkommen angemessenen Durchsatz erreichen. Im Idealfall findet die Anonymisierung von Audit-Daten dort statt, wo die Audit-Daten erhoben werden, nämlich auf dem Gerät, das die Nutzeranfragen zur Diensterbringung verarbeitet. Damit der Dienst nicht ausgebremst wird, ist es wichtig, daß die Pseudonym-Erzeugung nicht den überwiegenden Teil der Prozessor-Ressourcen bindet. Aufwendige kryptographische Verfahren scheiden daher für die Pseudonym-Erzeugung für einen dienst-lokalen on-the-fly-Einsatz aus.

Die zweite Anforderung betrifft den Verwendungszweck der pseudonymisierten Audit-Daten. Erfordert der Zweck eine rasche kontrollierte Aufdeckbarkeit, läßt sich dies nur mittels technischer Zweckbindung erreichen.

Im Gegensatz dazu erfordert die organisatorische Zweckbindung bei der kontrollierten Aufdeckbarkeit die Kooperation eines oder mehrerer Agenten. In der Regel findet die Zweckprüfung manuell statt, so daß sich die Aufdeckung verzögert, wenn die verantwortliche Person nicht verfügbar ist.

7.1 Audit-Daten-Anonymisierer im Vergleich

Die in Abschnitt 6.4 vorgestellten Ansätze für anonyme Audit-Daten werden im Folgenden anhand der Eigenschaften ihrer Pseudonyme (s. Abschnitt 5.1) und den notwendigen Kontrollverhältnissen (s. Abschnitt 6.2) in Tab. 2 verglichen. Alle betrachteten Ansätze berücksichtigen die in Abschnitt 7 formulierte Performanz-Anforderung. Einen detaillierteren Überblick zu den Systemen *Lundin Firewall Audit Anonymizer*, *IDA*, *AID* und *ANIDA* bieten [BF00a, BF00c]. Die Vergleichskriterien sind im einzelnen:

Pseudonym-Aufdeckbarkeit: Sind die verwendeten Pseudonyme gegenüber dem Sicherheits-Administrator aufdeckbar (s. Abschnitt 5.1.1)?

- **Zuordnungsregel:** Welche Art von Zuordnungsregel wird für die Pseudonym-Erzeugung verwendet?
- **Zweckbindung:** Welche Art von Zweckbindung wird für die kontrollierte Aufdeckung verwendet (technisch/organisatorisch)? Welche Art von Schutz wird bei der technischen Zweckbindung verwendet?
- **Kontrolle:** Welche Entität hat die Kontrolle über die Zuordnungsregel? Diese Entität führt die Zweckbindung für die kontrollierte Aufdeckung durch: für die technische Zweckbindung bei der Pseudonymisierung bzw. für die organisatorische Zweckbindung bei der Aufdeckung.

Pseudonym-Verkettbarkeit: Sind die verwendeten Pseudonyme verkettbar? Welche Pseudonym-Sorte wird verwendet (s. Abschnitt 5.1.2)?

- **Pseudonym-Wechsel:** Wie werden zusätzliche Pseudonym-Wechsel unabhängig von der Pseudonym-Sorte durchgeführt?
- **Zweckbindung:** Wird technische Zweckbindung für die Verkettbarkeit verwendet?
- **Kontrolle:** Welche Entität hat Kontrolle über die (technische Zweckbindung der) Verkettbarkeit der Pseudonyme?

Architektureigenschaften: Welche Eigenschaften hat die Architektur des Verfahrens, insbesondere das Verfahren zur Durchsetzung der organisatorischen Zweckbindung. Liegen die notwendigen Kontrollverhältnisse vor?

In diesem Bereich liegen die größten Probleme der ursprünglich für mehrseitige Sicherheit ausgelegten Ansätze. Entweder wurden die Vertrauensbeziehungen und Kontrollverhältnisse beim Entwurf nicht vollständig berücksichtigt, so daß der Sicherheits-Administrator unter Umgehung der Zweckbindung direkten Zugriff auf die Zuordnungsregel erlangen kann. Oder es wurde ein ungeeignetes Verfahren zur Implementierung des 4-Augen-Prinzips gewählt, so daß der aufgeteilte Dechiffrier-Schlüssel nach der ersten Aufdeckung zumindest einer der beiden Entitäten bekannt ist. Für die Implementierung der Mehrparteien-Dechiffrierung ohne Offenlegung des Dechiffrier-Schlüssels sind beispielsweise Schwellenwert-Kryptosysteme geeignet [DF89].

Tabelle 2: Übersicht über die Eigenschaften der Ansätze für anonyme Audit-Daten. ‘$\surd$’=Kriterium erfüllt, ‘–’=Kriterium nicht erfüllt, ‘%’=fehlende Information zum Ansatz, ‘(?. . . ?)’=Vermutung.

Ansatz (Verfügbarkeit)	Aufdeckung möglich	Verkettung möglich · Pseudonym-Sorte
	Art der Zuordnungsregel	zusätzliche Pseudonym-Wechsel
	Art der Zweckbindung · Schutz	technische Zweckbindung
	Kontrolle der Zweckbindung	Kontrollierende Entität
	Architektureigenschaften: Ursache	
Anonymouse Log File Anonymizer (Forschung)	–	–
	Vergröberung	–
	–	–
	–	Datenschützer
	einseitig, Anonymität: keine Aufdeckbarkeit	
BSMpseu (Forschung, frei)	–	$\surd$ · Subjekt-Pseudonyme
	Zufall	–
	–	–
	–	Datenschützer
	einseitig, Anonymität: keine Aufdeckbarkeit	
Jaeger-Anonymisierung (Konzept)	–	$\surd$ · Subjekt-Pseudonyme
	Einwegfunktion (Hash)	–
	–	–
	–	Datenschützer
	einseitig, Anonymität: keine Aufdeckbarkeit	
Lundin Firewall Audit Anonymizer (Forschung)	$\surd$	$\surd$ · Subjekt-Pseudonyme
	Zähler / Vergröberung	Zuordnung vergessen
	–	–
	Sicherheits-Admin	Datenschützer
	einseitig, Zurechenbarkeit: Angreifer kennt die Zuordnungsregel	
WebWasher (kommerziell)	$\surd$	% (?$\surd$ · Subjekt-Pseudonyme?)
	% (?Chiffrieren?)	%
	organisatorisch (?nur einmal?)	% (?–?)
	% (?Datenschützer?)	% (?Datenschützer?)
	% (?ggf. einseitig, Zurechenbarkeit: 4-Augen-Prinzip umgehbar?)	
IDA – Intrusion Detection and Avoidance (Konzept)	$\surd$	$\surd$ · Subjekt-Pseudonyme
	symmetrisches Chiffrieren	Schlüssel-Wechsel
	organisatorisch (nur einmal)	–
	Datenschützer	Datenschützer
	ggf. einseitig, Zurechenbarkeit: 4-Augen-Prinzip umgehbar	
AID – Adaptive Intrusion Detection (Forschung)	$\surd$	$\surd$ · Subjekt-Pseudonyme
	symmetrisches Chiffrieren	Schlüssel-Wechsel
	– / organisatorisch	–
	– / Datenschützer	Datenschützer
	einseitig, Zurechenbarkeit: Angreifer kennt die Zuordnungsregel	
Pseudo/CoRe – Pseudonymization with Conditional Reidentification (Forschung, frei)	$\surd$	$\surd$ · Rollen-Pseudonyme
	symmetrisches Chiffrieren	Timeout oder Verdachtsabbruch
	techn. + org. · Geheimnisteilung	–
	Datenschützer	Datenschützer
	mehrseitig, Anonymität und Zurechenbarkeit	

7.2 Pseudo/CoRe

Der Vergleich der Ansätze in Tab. 2 zeigt, daß nur der Pseudo/CoRe-Ansatz in der Lage ist, Audit-Daten im Sinne mehrseitiger Sicherheit bei technischer Zweckbindung zu anonymisieren. Dazu tragen die klar definierten und umsetzbaren notwendigen Vertrauens- und Kontrollverhältnisse beim Einsatz von Pseudo/CoRe bei [Fle02b, Fle03c].

Pseudo/CoRe ist auch der einzige Ansatz, der die technische Zweckbindung konsequent durchsetzt. Diese gilt nicht nur für die kontrollierte Pseudonym-Aufdeckung, sondern auch für die automatischen Pseudonym-Wechsel. Erstens definiert der Aufdeckungszweck verschiedene Mißbrauchs-Szenarien. In jedem besitzt ein Nutzer ein anderes Pseudonym [BF00b]. Zweitens werden Pseudonyme automatisch unaufdeckbar, wenn die mit ihnen verbundenen Verdachtsmomente sich nicht bestätigen. Optional wird ebenfalls eine organisatorische Zweckbindung bei der kontrollierten Pseudonym-Aufdeckung unterstützt.

Fazit

Anhand der vorgestellten Modelle lassen sich Eigenschaften existierender Architekturen für anonyme Autorisierungen bestimmen und vergleichen. Die gesetzlichen Einschränkungen entfallen bei der Nutzung von anonymen Audit-Daten [RS00]. Auf Ebene des Dienstes läßt sich dies praktikabel durch Audit-Daten-Anonymisierer erreichen. Beim Entwurf bzw. bei der Auswahl von Audit-Daten-Anonymisierern ist besonderes auf die notwendigen Kontrollverhältnisse und die Mechanismen für die Durchsetzung der Zweckbindung bei der Pseudonym-Aufdeckung zu achten.

Literaturverzeichnis

[95/95] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L 281, October 1995. `http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html`.

[ABD+02] T. Alamaki, M. Björksen, Gripenberg C. Dornbach, P., N. Györbíró, G. Márton, Z. Németh, T. Skyttä, and M. Tarkiainen. Privacy Enhancing Service Architectures. In Dingledine and Syverson [DS02], pages 99–109.

[ABFK03] Christian Altenschmidt, Joachim Biskup, Ulrich Flegel, and Yücel Karabulut. Secure Mediation: Requirements, Design and Architecture. *Journal of Computer Security*, 11(3):365–398, June 2003.

[ACF+00] J. Allen, A. Christie, W. Fithen, J. McHugh, P. Pickel, and E. Stoner. State of the Practice of Intrusion Detection Technologies. Technical Report CMU/SEI-99-TR-028, ESC-99-028, Carnegie Mellon University, Software Engineering Institute, January 2000.

[ACR99] Mark S. Ackerman, Lorrie F. Cranor, and Joseph Reagle. Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences. In *Proceedings of the 1st ACM conference on Electronic Commerce*, pages 1–8, Denver, Colorado, USA, 1999.

[Axe99] Stefan Axelsson. Research in Intrusion Detection Systems: A Survey. Technical Report 98-17, Department of Computer Engineering, Chalmers University of Technology, Sweden, August 1999. Revised version.

[BF99] Dan Boneh and Matt Franklin. Anonymous Authentication With Subset Queries. In *Proceedings of the 6th ACM Conference on Computer and Communications Security*, pages 113–119, Kent Ridge Digital Labs, Singapore, November 1999. ACM SIGSAC, ACM Press.

[BF00a] Joachim Biskup and Ulrich Flegel. On Pseudonymization of Audit Data for Intrusion Detection. In Federrath [Fed00], pages 161–180.

[BF00b] Joachim Biskup and Ulrich Flegel. Threshold-based Identity Recovery for Privacy Enhanced Applications. In Sushil Jajodia and Pierangela Samarati, editors, *Proceedings of the 7th ACM Conference on Computer and Communications Security*, pages 71–79, Athens, Greece, November 2000. ACM SIGSAC, ACM Press.

[BF00c] Joachim Biskup and Ulrich Flegel. Transaction-Based Pseudonyms in Audit Data for Privacy Respecting Intrusion Detection. In Hervé Debar, Ludovic Mé, and S. Felix Wu, editors, *Proceedings of the Third International Symposium on Recent Advances in Intrusion Detection (RAID 2000)*, number 1907 in Lecture Notes in Computer Science, pages 28–48, Toulouse, France, October 2000. Springer.

[BF02] Joachim Biskup and Ulrich Flegel. Ausgleich von Datenschutz und Überwachung mit technischer Zweckbindung am Beispiel eines Pseudonymisierers (in German). In Sigrid Schubert, Bernd Reusch, and Norbert Jesse, editors, *Informatik bewegt, Proceedings of the 32nd Annual GI Conference on Informatik (Informatik 2002) (in German)*, number P-19 in Lecture Notes in Informatics, pages 488–494, Dortmund, Germany, October 2002. Gesellschaft für Informatik e.V.(GI), Köllen Verlag.

[BFK00a] Oliver Berthold, Hannes Federrath, and Marit Köhntopp. Project "Anonymity and Unobservability in the Internet". In *Proceedings of the Workshop on Freedom and Privacy by Design / Conference on Freedom and Privacy*, pages 57–65, Toronto, Canada, April 2000. ACM.

[BFK00b] Oliver Berthold, Hannes Federrath, and Stefan Köpsell. Web MIXes: A System for Anonymous and Unobservable Internet Access. In Federrath [Fed00], pages 115–129.

[BJR+03] Thomas Butzlaff, Florian Jäger, Björn Röber, David Weber, and Andreas Wilms. Marktchancen von Anonymisierung (in German). *Datenschutz und Datensicherheit*, 27(3):146–149, March 2003.

[BK99] Roland Büschkes and Dogan Kesdogan. Privacy Enhanced Intrusion Detection. In Müller and Rannenberg [MR99], pages 187–204.

[BK02] Joachim Biskup and Yücel Karabulut. A Hybrid PKI Model with an Application for Secure Meditation. In *Proceedings of the Annual IFIP WG 11.3 Working Conference on Data and Application Security*, Cambridge, England, July 2002.

[BK03] Joachim Biskup and Yücel Karabulut. Mediating Between Strangers: A Trust Management Based Approach. In *Proceedings of the 2nd Annual PKI Research Workshop* [NIS03].

[Bor96] John Borkin. Der Identity Protector (in German). *Datenschutz und Datensicherheit*, 20(11):654–658, November 1996.

[Brü03] Lars Brückner. Aktiver Datenschutz mit DataJournals (in German). *Datenschutz und Datensicherheit*, 27(5):300, May 2003.

[Bra00] Stefan A. Brands. *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy*. MIT Press, Cambridge, Massachusetts, 2000.

[Bun02] Bundesamt für Sicherheit in der Informationstechnik, Godesberger Allee 185-189, 53133, Bonn, Germany. *Einführung von Intrusion-Detection-Systemen – Rechtliche Aspekte (in German)*, October 2002. `http://www.bsi.de/literat/studien/ids02/dokumente/Rechtv10.pdf`.

[BvES99] J. J. Borking, B. M. A. van Eck, and P. Siepel. Intelligent Software Agents and Privacy. Technical report, Registratiekamer Netherlands and Information and Privacy Commissioner Ontario, Canada, Achtergrondstudies en Verkenningen 13, The Hague, 1999.

[CDT02] Privacy Survey Results, January 2002. `http://www.cdt.org/privacy/survey/findings/`.

[CE87] D. Chaum and J.-H. Evertse. A secure and privacy-protecting protocol for transmitting personal information between organizations. In A. M. Odlyzko, editor, *Proceedings of the Conference on Advances in Cryptology (CRYPTO'86)*, number 263 in Lecture Notes in Computer Science, pages 118–167, Santa Barbara, California, USA, August 1987. Springer.

[CFN88] David Chaum, Amos Fiat, and Moni Naor. Untraceable Electronic Cash. In Goldwasser [Gol88], pages 319–327.

[CGKS98] D. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan. Private Information Retrieval. *Journal of the ACM*, 45(6):965–982, November 1998.

[Cha85] David Chaum. Security without Identification: Transaction Systems to make Big Brother Obsolete. *Communications of the ACM*, 28(10):1030–1044, October 1985.

[Cha86] David Chaum. Showing Credentials without Identification – Signatures Transferred between Unconditionally Unlinkable Pseudonyms. In *Advances in Cryptology – EUROCRYPT 1985*, number 219 in Lecture Notes in Computer Science, pages 241–244, Linz, Austria, April 1986. Springer.

[Cha87] David Chaum. Security without Identification – Card Computers to make Big Brother Obsolete. `http://www.chaum.com/articles/Security_Wthout_identification.htm`, 1987. Extended version of [Cha85].

[Cha90] David Chaum. Showing Credentials without Identification: Transferring Signatures between Unconditionally Unlinkable Pseudonyms. In J. Seberry and J. Pieprzyk, editors, *Proceedings of the Conference on Advances in Cryptology (AUSCRYPT'90)*, number 453 in Lecture Notes in Computer Science, pages 246–264, Sydney, Australia, January 1990. Springer.

[Cha99] Yuen-Yan Chan. On Privacy Issues of Internet Access Services via Proxy Servers. In Rainer Baumgart, editor, *Proceedings of the Congress on Secure Networking – CQRE[Secure]'99*, number 1740 in Lecture Notes in Computer Science, pages 183–191, Düsseldorf, Germany, November 1999. secunet, Springer.

[CK01] Sebastian Clauß and Marit Köhntopp. Identity management and its support of multilateral security. *Computer Networks*, 37(2):205–219, 2001.

[CL01a] Jan Camenisch and Anna Lysyanskaya. Efficient Revocation of Anonymous Group Membership Certificates and Anonymous Credentials. `http://eprint.iacr.org/2001`, December 2001.

[CL01b] Jan Camenisch and Anna Lysyanskaya. An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. In B. Pfitzmann, editor, *Advances in Cryptology – EUROCRYPT 2001*, number 2045 in Lecture Notes in Computer Science, pages 93–118, Austria, May 2001. Springer.

[CLM+01] Lorrie Cranor, Marc Langheinrich, Massimo Marchiori, Martin Presler-Marshall, and Joseph Reagle. The Platform for Privacy Preferences 1.0 (P3P1.0) Specification, September 2001. `http://www.w3.org/TR/2001/WD-P3P-20010928/`.

[CMS96] J. Camenisch, U. Maurer, and M. Stadtler. Digital Payment Systems with Passive Anonymity-Revoking Trustees. In E. Bertino, H. Kurth, G. Martella, and E. Montolivo, editors, *Proceedings of the 4th European Symposium on Research in Computer Security (ESORICS'96)*, number 1146 in Lecture Notes in Computer Science, pages 33–43, Rome, Italy, September 1996. Springer.

[CPHVH02] Sebastian Clauß, Andreas Pfitzmann, Marit Hansen, and Els Van Herreweghen. Privacy-Enhancing Identity Management. In *IPTS Report Vol. 67*, pages 8–16. Institute for Prospective Technological Studies (IPTS) of the Joint Research Center (JRC) of the European Commission, Seville, September 2002. `http://www.jrc.es/pages/iptsreport/vol67/english/IPT2E676.html`.

[CPV99] J. Claessens, B. Preneel, and J. Vandewalle. Anonymity Controlled Electronics Payment Systems. In *Proceedings of the 20th Symposium on Information Theory in the Benelux*, pages 109–116, Haasrode, Belgium, May 1999.

[Cra99] Lorrie F. Cranor. Agents of Choice: Tools that Facilitate Notice and Choice about Web Site Data Practices. In *Proceedings of the 21st International Conference on Privacy and Personal Data Protection*, pages 19–25, Hong Kong SAR, China, September 1999.

[CS97] Jan Camenisch and Markus Stadtler. Efficient Group Signature Schemes for Large Groups. In B. S. Kaliski, editor, *Proceedings of the Conference on Advances in Cryptology (CRYPTO'97)*, number 1294 in Lecture Notes in Computer Science, pages 410–424, Santa Barbara, California, USA, August 1997. Springer.

[Dam88] I. Damgard. Payment Systems and credential mechanisms with provable security against abuse by individuals. In Goldwasser [Gol88], pages 328–335.

[dB84] Erster Senat des Bundesverfassungsgerichts. Urteil vom 15. Dezember 1983 zum Volkszählungsgesetz - 1 BvR 209/83 u.a. (in German). *Datenschutz und Datensicherheit*, 84(4):258–281, April 1984. `http://www.datenschutz-berlin.de/gesetze/sonstige/volksz.htm`.

[DF89] Yvo Desmedt and Yair Frankel. Threshold Cryptosystems. In G. Brassard, editor, *Proceedings of the Conference on Advances in Cryptology (CRYPTO'89)*, number 435 in Lecture Notes in Computer Science, pages 307–315, Santa Barbara, California, USA, August 1989. Springer.

[DFTY97] George Davida, Yair Frankel, Yiannis Tsiounis, and Moti Yung. Anonymity Control in E-Cash Systems. In Hirschfeld [Hir97], pages 1–16.

[dKdDdBudL97] Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder. Datenschutzfreundliche Technologien in der Telekommunikation, October 1997. Überarbeitete Fassung.

[dMiWuG98] Enquete-Kommission "Zukunft der Medien in Wirtschaft und Gesellschaft". Deutschlands Weg in die Informationsgesellschaft (Schlussbericht). Bundestags-Drucksache 13/11004, June 1998.

[DNC+02] C. Díaz, V. Naessens, J. Claessens, B. De Win, S. Seys, B. De Decker, and B. Preneel. Anonymity and Privacy in Electronic Services (APES) Deliverable 5 – Tools for Technologies and Applications. Technical report, K. U. Leuven, November 2002.

[DP01] Michel Dupuy and Pierre Paradinas, editors. *Proceedings of the IFIP TC11 16th International Conference on Information Security (IFIP/Sec'01)*, Paris, France, June 2001. IFIP, Kluwer Academic Publishers.

[DPR99] H. Damker, U. Pordesch, and M. Reichenbach. Personal Reachability and Security Management. In Müller and Rannenberg [MR99], pages 95–111.

[DS02] R. Dingledine and P. Syverson, editors. *Proceedings of the International Workshop on Privacy Enhancing Technologies*, number 2482 in Lecture Notes in Computer Science, San Francisco, California, USA, April 2002. Springer.

[DWND+01] B. De Win, V. Naessens, C. Díaz, S. Seys, C. Goemans, J. Claessens, B. De Decker, J. Dumortier, and B. Preneel. Anonymity and Privacy in Electronic Services (APES) Deliverable 3 – Technologies Overview. Technical report, K. U. Leuven, November 2001.

[EP01] Claudia Eckert and Alexander Pircher. Internet Anonymity: Problems and Solutions. In Dupuy and Paradinas [DP01], pages 35–50.

[Fed00] Hannes Federrath, editor. *Proceedings of the International Workshop on Design Issues in Anonymity and Unobservability*, number 2009 in Lecture Notes in Computer Science, Berkeley, California, July 2000. ICSI, Springer.

[FH93] Simone Fischer-Hübner. *IDA (Intrusion Detection and Avoidance System): Ein einbruchsentdeckendes und einbruchsvermeidendes System (in German)*. Reihe Informatik. Shaker, 1993.

[FH01] Simone Fischer-Hübner. *IT-Security and Privacy: Design and Use of Privacy-Enhancing Security Mechanisms*. Number 1958 in Lecture Notes in Computer Science. Springer, 2001.

[FHB89] Simone Fischer-Hübner and Klaus Brunnstein. Opportunities and Risks of Intrusion Detection Expert Systems. In *Proceedings of the International IFIP-GI-Conference Opportunities and Risks of Artificial Intelligence Systems ORAIS'89*, Hamburg, Germany, July 1989. IFIP.

[Fie01] Herbert Fiedler. Der Staat im Cyberspace (in German). *Informatik Spektrum*, 24(5):309–314, 2001.

[Fie02] Herbert Fiedler. Cyber-libertär (in German). *Informatik Spektrum*, 25(3):215–219, 2002.

[Fle02a] Ulrich Flegel. Pseudonymizing Unix Log Files. Technical report, Dept. of Computer Science, Chair VI Information Systems and Security, University of Dortmund, D-44221 Dortmund, May 2002. Extended version of [Fle02b]. `http://ls6-www.cs.uni-dortmund.de/issi/archive/literature/2002/Flegel:2002a.pdf`.

[Fle02b] Ulrich Flegel. Pseudonymizing Unix Log Files. In George Davida, Yair Frankel, and Owen Rees, editors, *Proceedings of the Infrastructure Security Conference (InfraSec2002)*, number 2437 in Lecture Notes in Computer Science, pages 162–179, Bristol, United Kingdom, October 2002. Springer.

[Fle03a] Ulrich Flegel. Anonyme Audit-Daten im Überblick (in German). *Datenschutz und Datensicherheit*, 27(5):278–281, May 2003.

[Fle03b] Ulrich Flegel. Evaluating the Design of an Audit Data Anonymizer Using Basic Building Blocks for Anonymity. Technical report, Dept. of Computer Science, Chair VI Information Systems and Security, May 2003. `http://ls6-www.cs.uni-dortmund.de/issi/archive/literature/2003/Flegel:2003c.pdf`.

[Fle03c] Ulrich Flegel. Praktikabler Datenschutz für Log-Daten (in German). In Rolf Schaumburg and Marco Thorbrügge, editors, *Proceedings of the 10th DFN-CERT Workshop on Sicherheit in vernetzten Systemen*, DFN-CERT publications, pages F1–F20, Hamburg, Germany, February 2003. DFN-CERT, Books on Demand.

[Fra00] Y. Frankel, editor. *Proceedings of the 4th International Conference on Financial Cryptography (FC'00)*, number 1962 in Lecture Notes in Computer Science, Anguilla, British West Indies, February 2000. Springer.

[GG:49] Grundgesetz für die Bundesrepublik Deutschland (in German), May 1949. http://www.datenschutz-berlin.de/recht/de/gg/index.htm.

[GGK+99a] E. Gabber, P. Gibbons, D. Kristol, Y. Matias, and Mayer. A. Consistent, yet anonymous, web access with LPWA. *Communications of the ACM*, 42(2):42–47, February 1999.

[GGK+99b] E. Gabber, P. Gibbons, D. Kristol, Y. Matias, and Mayer. A. On Secure and Pseudonymous Client-Relationships with Multiple Servers. *ACM Transactions on Information and System Security*, 2(3):390–415, November 1999.

[GGLS01] Ariel Glenn, Ian Goldberg, Frédéric Légaré, and Anton Stiglic. A Description of Protocols for Private Credentials. http://eprint.iacr.org/2001, October 2001.

[GGMA97] E. Gabber, P. Gibbons, Y. Matias, and Mayer. A. How o make personalized web browsing simple, secure and anonymous. In Hirschfeld [Hir97], pages 17–32.

[GMI+01] Dimitris Gritzalis, Konstantinos Moulinos, John Iliadis, Costas Lambrinoudakis, and Steven Xarhoulakos. PyTHIA: Towards Anonymity in Authentication. In Dupuy and Paradinas [DP01], pages 1–17.

[Gol88] S. Goldwasser, editor. *Proceedings of the Conference on Advances in Cryptology (CRYPTO'88)*, Lecture Notes in Computer Science, Santa Barbara, California, August 1988. Springer.

[Gol99] Dieter Gollmann. *Computer Security*, chapter 10.2.1 Kerberos, pages 168–171. John Wiley & Sons, Inc. 1999.

[Gol02] Ian Goldberg. Privacy-Enhancing Technologies for the Internet, II: Five Years Later. In Dingledine and Syverson [DS02], pages 1–12.

[Gol03] Claudia Golembiewski. Das Recht auf Anonymität im Internet (in German). *Datenschutz und Datensicherheit*, 27(3):129–133, March 2003.

[GtMJ01] Daniela Gerd tom Markotten and Uwe Jendricke. Identitätsmanagement im E-Commerce. *it+ti Informationstechnik und Technische Informatik*, 43(5):236–245, October 2001.

[GWB97] Ian Goldberg, David Wagner, and Eric Brewer. Privacy Enhancing Technologies for the Internet. In *Proceedings of the COMPCON'97*, San Jose, February 1997. IEEE. http://www.cs.berkeley.edu/~daw/privacy-compcon97-www/privacy-html.html.

[Han00] Ben Handley. Resource-Efficient Anonymous Group Identification. In Frankel [Fra00], pages 295–312.

[Han03] Marit Hansen. Identitätsmanagement (in German). *Datenschutz und Datensicherheit*, 27(5):306, May 2003.

[Hir97] R. Hirschfeld, editor. *Proceedings of the First International Conference on Financial Cryptography (FC'97)*, number 1318 in Lecture Notes in Computer Science, Anguilla, British West Indies, February 1997. Springer.

[HNP99] D. L. Hoffman, T. P. Novak, and M. A. Peralta. Information Privacy in the Marketspace: Implications for the Commercial Uses of Anonymity on the Web. *The Information Society*, 15(2):129–140, April 1999. http://elab.vanderbilt.edu/research/papers/html/manuscripts/anonymity/anonymity2_nov10.htm.

[HR03] Marit Hansen and Martin Rost. Nutzerontrollierte Verkettung (in German). *Datenschutz und Datensicherheit*, 27(5):293–296, May 2003.

[HY01] Shouichi Hirose and Susumu Yoshida. A User Athentication Scheme with Identity and Location Privacy. In Varadharajan V. and Y. Mu, editors, *Proceedings of the 6th Australasian Conference on Information Security and Privacy (ACISP 2001)*, number 2119 in Lecture Notes in Computer Science, pages 235–246, Sydney, Australia, July 2001. Springer.

[IHS86] R. H. Irving, C. A. Higgins, and F. R. Safayeni. Computerized Performance Monitoring Systems: Use and Abuse. *Communications of the ACM*, 29(8):794–801, 1986.

[Inc99] Louis Harris & Associates Inc. IBM Multi-National Consumer Privacy Survey. Technical Report 938568, IBM Global Services, 1999.

[IS03] Alex Iliev and Sean Smith. Privacy-enhanced credential services. In *Proceedings of the 2nd Annual PKI Research Workshop* [NIS03].

[Jae00] Stefan Jaeger. Verbotene Protokolle (in German). *Zeitschrift für Kommunikations- und EDV-Sicherheit (KES)*, 2000(5):6–12, 2000.

[Jak97] Björn Markus Jakobsson. *Privacy vs. Authenticity*. PhD thesis, University of California San Diego, 1997.

[JGtM01] Uwe Jendricke and Daniela Gerd tom Markotten. Identitätsmanagement: Einheiten und Systemarchitektur. In Dirk Fox, Marit Köhntopp, and Andreas Pfitzmann, editors, *Proceedings of Verläßliche IT-Systeme - Sicherheit in komplexen Infrastrukturen*, DuD-Fachbeiträge, pages 77–85, Wiesbaden, Germany, September 2001. GI, Vieweg.

[Jue01] Ari Juels. Targeted Advertising . . . And Privacy Too. In D. Naccache, editor, *Proceedings of The Cryptographers' Track at RSA Conference 2001 - Progress in Cryptology (CT-RSA 2001)*, Lecture Notes in Computer Science, pages 408–424, San Francisco, CA, USA, April 2001. Springer.

[Kar02] Yücel Karabulut. *Secure Mediation Between Strangers in Cyberspace*. PhD thesis, University of Dortmund, Dortmund, Germany, September 2002.

[KB00] Marit Köhntopp and Oliver Berthold. Identity Management Based on P3P. In Federrath [Fed00], pages 141–160.

[Köh00] Marit Köhntopp. Technischer Datenschutz in offenen Netzen. In *Proceedings of the 7th DFN-CERT Workshop on Sicherheit in vernetzten Systemen*, DFN-Bericht, Hamburg, Germany, March 2000. DFN-CERT.

[KP97] Joe Kilian and Erez Petrank. Identity Escrow. Theory of Cryptography Library, August 1997. `http://theory.lcs.mit.edu/pub/tcryptol/97-11.ps`.

[KP98] Joe Kilian and Erez Petrank. Identity Escrow. In H. Krawczyk, editor, *Proceedings of the Conference on Advances in Cryptology (CRYPTO'98)*, number 1462 in Lecture Notes in Computer Science, pages 196–185, Santa Barbara, California, USA, August 1998. Springer.

[Kum03] Christel Kumbruck. Verwirrungen um die Identität beim pseudonymen elektronischen Einkaufen (in German). *Datenschutz und Datensicherheit*, 27(5):287–292, May 2003.

[LJ99a] Emilie Lundin and Erland Jonsson. Privacy vs. Intrusion Detection Analysis. In *Proceedings of the Second International Symposium on the Recent Advances in Intrusion Detection (RAID'99)*, West Lafayette, Indiana, September 1999. Purdue University, CERIAS.

[LJ99b] Emilie Lundin and Erland Jonsson. Some Practical and Fundamental Problems with Anomaly Detection. In *Proceedings of NORDSEC'99*, Kista Science Park, Sweden, November 1999.

[LJ00] Emilie Lundin and Erland Jonsson. Anomaly-based intrusion detection: privacy concerns and other problems. *Computer Networks*, 34(4):623–640, October 2000.

[LRSW99] Anna Lysyanskaya, Ronald L. Rivest, Amit Sahai, and Stefan Wolf. Pseudonym Systems. In Howard Heys and Carlisle Adams, editors, *Proceedings of the 6th Annual International Workshop on Selected Areas in Cryptography (SAC'99)*, pages 184–199, Kingston, Ontario, Canada, August 1999. Springer.

[MB01] Greg Maitland and Colin Boyd. Fair Electronic Cash Based on a Group Signature Scheme. In S. Qing, T. Okamoto, and J. Zhou, editors, *Proceedings of the Third International Conference on Information and Communications Security (ICICS 2001)*, number 2229 in Lecture Notes in Computer Science, pages 461–465, Xian, China, November 2001. Springer.

[McH01] John McHugh. Intrusion and Intrusion Detection. *International Journal of Information Security*, 1(1):14–35, 2001.

[MH00] Michael Meier and Thomas Holz. Sicheres Schlüsselmanagement für verteilte Intrusion-Detection-Systeme (in German). In Patrick Horster, editor, *Systemsicherheit*, DuD-Fachbeiträge, pages 275–286, Bremen, Germany, March 2000. GI-2.5.3, ITG-6.2, ÖCG/ACS, TeleTrusT, Vieweg.

[MR99] Günter Müller and Kai Rannenberg, editors. *Multilateral Security in Communications*. Information Security. Addison Wesley, 1999.

[Neu03] Heike Neumann. Anonyme Zahlungssysteme (in German). *Datenschutz und Datensicherheit*, 27(5):270–273, May 2003.

[New01] Heise Newsticker. 13. WWW-Benutzer-Analyse von Fittkau & Maaß. http://www.ct.heise.de/newsticker/data/anw-26.11.01-001/, November 2001.

[NHS99] Toru Nakanishi, Nobuaki Haruna, and Yuji Sugiyama. Unlinkable Electronic Coupon Protocol with Anonymity Control. In M. Mombo and Y. Zheng, editors, *Proceedings of the Second International Workshop on Information Security (ISW'99)*, number 1729 in Lecture Notes in Computer Science, pages 37–46. Springer, November 1999.

[NIS03] NIST. *Proceedings of the 2nd Annual PKI Research Workshop*, Gaitherburg, Maryland, USA, April 2003.

[Pet97] Holger Petersen. Faires elektronisches Geld (in German). In *Mit Sicherheit in die Informationsgesellschaft*, pages 427–444, Bonn, Germany, April 1997. Bundesamt für Sicherheit in der Informationstechnik, SecuMedia Verlag, Ingelheim.

[Pfi01] Andreas Pfitzmann. Multilateral Security: Enabling Technologies and Their Evaluation. In R. Wilhelm, editor, *Informatics: 10 Years Back. 10 Years Ahead.*, number 2000 in Lecture Notes in Computer Science, pages 50–62. Springer, 2001.

[PK00] Andreas Pfitzmann and Marit Köhntopp. Anonymity, Unobservability, and Pseudonymity – A Proposal for Terminology. In Federrath [Fed00], pages 1–9.

[Poi00] David Pointcheval. Self-Scrambling Anonymizers. In Frankel [Fra00], pages 259–275.

[Pro00] Pew Internet & American Life Project. Trust and Privacy Online: Why Americans Want to Rewrite the Rules. http://www.pewinternet.org/reports/pdfs/PIP_Trust_Privacy_Report.pdf, August 2000.

[PWP00] Birgit Pfitzmann, Michael Waidner, and Andreas Pfitzmann. Secure and Anonymous Electronic Commerce: Providing Legal Certainty in Open Digital Systems Without Compromising Anonymity. Technical Report RZ 3232 (#93278) 05/22/00, IBM Zurich Research Lab, May 2000.

[R+98] Jarek Rossignac et al. GVU's 10th WWW User Survey, December 1998. http://www.cc.gatech.edu/gvu/user_surveys/survey-1998-10/graphs/graphs.html#privacy.

[Rie03] Konrad Rieck. *Konzept zur datenschutzorientierten Verarbeitung von Solaris-BSM-Audit-Daten (in German)*. Fachbereich Mathematik und Informatik, Institut für Informatik, Freie Universität Berlin, January 2003. http://www.roqe.org/bsmpseu.

[Roß02] Alexander Roßnagel. Freiheit im Cyberspace (in German). *Informatik Spektrum*, 25(1):33–38, 2002.

[RPM99] Kai Rannenberg, Andreas Pfitzmann, and Günter Müller. IT Security and Multilateral Security. In Müller and Rannenberg [MR99], pages 21–29.

[RRSCI02] Virginia E. Rezmierski, Marshall R. Reese, and Nathaniel St. Clair II. University systems security logging: who is doing it and far can they go. *Computers & Security*, 21(6):557–564, 2002.

[RS00] Alexander Roßnagel and Philip Scholz. Datenschutz durch Anonymität und Pseudonymität (in German). *Zeitschrift für Informations-, Telekommunikations- und Medienrecht (MMR)*, 2000(12):721–732, 2000.

[RSCI01] Virginia E. Rezmierski and Nathaniel St. Clair II. Final Report NSF-Lamp Project: Identifying Where Technology Logging and Monitoring for Increased Security End and Violations of Personal Privacy and Student Records Begin. Technical Report CSD1702, American Association of Collegiate Registrars and Admissions Officers, 2001. http://www.aacrao.org/publications/catalog/NSF-LAMP.pdf.

[SDDW+01] S. Seys, C. Díaz, Bart De Win, V. Naessens, C. Goemans, J. Claessens, W. Moreau, B. De Decker, J. Dumortier, and B. Preneel. Anonymity and Privacy in Electronic Services (APES) Deliverable 2 – Requirement Study of Different Applications. Technical report, K. U. Leuven, May 2001.

[SFHR97] Michael Sobirey, Simone Fischer-Hübner, and Kai Rannenberg. Pseudonymous Audit for Privacy Enhanced Intrusion Detection. In L. Yngström and J. Carlsen, editors, *Proceedings of the IFIP TC11 13th International Conference on Information Security (SEC'97)*, pages 151–163, Copenhagen, Denmark, May 1997. IFIP, Chapman & Hall, London.

[SK03] Sandra Steinbrecher and Stefan Köpsell. Modelling Unlinkability. In *Proceedings of the International Workshop on Privacy Enhancing Technologies*, Lecture Notes in Computer Science, Dresden, Germany, March 2003. Springer. To appear.

[SM02] Peter Schaar and Frank Möller. Was bei der Gestaltung von Webseiten zu beachten ist – Orientierungshilfe Tele- und Mediendienste. Der Hamburgische Datenschutzbeauftragte, January 2002.

[Sob95] Michael Sobirey. Aktuelle Anforderungen an Intrusion Detection-Systeme und deren Berücksichtigung bei der Systemgestaltung von AID^2 (in German). In Hans H. Brüggemann and Waltraud Gerhardt-Häckl, editors, *Proceedings of Verläßliche IT-Systeme*, DuD-Fachbeiträge, pages 351–370, Rostock, Germany, April 1995. GI, Vieweg.

[Sob99] Michael Sobirey. *Datenschutzorientiertes Intrusion Detection (in German)*. DuD-Fachbeiträge. Vieweg, 1999.

[SP98] Michael Schneider and Ulrich Pordesch. Identitätsmangement. *Datenschutz und Datensicherheit*, 22(11):645–649, 1998.

[SPC95] M. Stadtler, J.-M. Pivetau, and J. Camenisch. Fair Blind Signatures. In F. Pichler, editor, *Advances in Cryptology – EUROCRYPT 1995*, number 219 in Lecture Notes in Computer Science, pages 209–219, Linz, Austria, April 1995. Springer.

[SPH99] Stuart Schechter, Todd Parnell, and Alexander Hartemink. Anonymous Authentication of Membership in Dynamic Groups. In M. Franklin, editor, *Proceedings of the Third International Conference on Financial Cryptography (FC'99)*, number 1648 in Lecture Notes in Computer Science, pages 184–195, Anguilla, British West Indies, February 1999. Springer.

[Spi03a] Gerald Spiegel. Spuren im Netz (in German). *Datenschutz und Datensicherheit*, 27(5):265–269, May 2003.

[Spi03b] Sarah Spiekermann. Die Konsumenten der Anonymität (in German). *Datenschutz und Datensicherheit*, 27(3):150–154, March 2003.

[SRK96] M. Sobirey, B. Richter, and H. König. The Intrusion Detection System AID – Architecture and Experiences in automated audit trail analysis. In P. Horster, editor, *Proceedings of the IFIP TC6/TC11 International Conference on Communications and Multimedia Security*, pages 278–290, Essen, Germany, September 1996. IFIP, Chapman & Hall, London.

[SS00] Stuart G. Stubblebine and Paul F. Syverson. Authentic Attributes with Fine-Grained Anonymity Protection. In Frankel [Fra00], pages 276–294.

[SSG99] Stuart G. Stubblebine, Paul F. Syverson, and David M. Goldschlag. Unlinkable Serial Transactions: Protocols and Applications. *ACM Transactions on Information and System Security*, 2(4):354–389, November 1999.

[Tra99] Jaques Traoré. Group Signatures and Their Relevance to Privacy-Protecting Offline Electronic Cash Systems. In J. Pieprzyk, R. Safavi-Naini, and J. Seberry, editors, *Proceedings of the 4th Australasian Conference on Information Security and Privacy (ACISP'99)*, number 1587 in Lecture Notes in Computer Science, pages 228–243, Wollongong, NSW, Australia, April 1999. Springer.

[VH00] Els Van Herreweghen. Secure Anonymous Signature-Based Transactions. In G. Goos, J. Hartmanis, and J. van Leeuwen, editors, *Proceedings of the 6th European Symposium on Reserach in Computer Security (ESORICS 2000)*, number 1895 in Lecture Notes in Computer Science, pages 55–71, Toulouse, France, October 2000. Springer.

[vRGB$^+$95] H. van Rossum, H. Gardeniers, J. Borking, et al. Privacy-Enhancing Technologies: The Path to Anonymity, Volume II. Technical report, Registratiekamer Netherlands and Information and Privacy Commissioner Ontario, Canada, Achtergrondstudies en Verkenningen 5B, Rijswijk, August 1995.

[wA03] webwasher.com AG. Den Überblick behalten, Reporting mit WebWasherEE (in German). `http://www.webwasher.com/product_pdf/deutsch/Produktblatt_Reporting.pdf`, January 2003.

[WB91] S. D. Warren and L. D. Brandeis. The Right To Privacy. *Harvard Law Review*, (5):193–220, 1890-91.

[Wes87] Alan Westin. *Privacy and Freedom*. Bodley Head, New York, 1987.