Beitrag zur Sommerakademie 2000, Kiel

Identitätsmanagement

Oliver Berthold
TU Dresden, Fakultät Informatik,
Institut für Systemarchitektur
oliver.berthold@gmx.de

Hannes Federrath
International Computer Science
Institute, Berkeley
hannes@icsi.berkeley.edu

Einführung

Identitätsmanagement in Computernetzen soll einen Benutzer in die Lage versetzen, persönliche Merkmale nur gezielt und bewußt weiterzugeben. Identitätsmanagement dient also dem Schutz personenbezogener Daten. Hierzu benötigen die Benutzer eine bewußte Kontrolle über die Information, mit deren Hilfe in unterschiedlichen Situationen weitergegebene personenbezogenen Daten verknüpft werden können. Mit dem Begriff **persönliches Merkmal** ist in diesem Papier in erster Linie ein Kennzeichen für eine Person gemeint, das für sich allein meist keinen eindeutigen Personenbezug darstellt, aber in der **Verkettung** mit mehreren persönlichen Merkmalen zu einem identifizierenden Computerdatensatz wird und die Identität einer Person bestimmt. Beispiele für solche persönlichen Merkmale sind Geburtsdatum, Wohnort, Staatsangehörigkeit, Beruf oder die später noch ausführlich erläuterten **Pseudonyme**. In manchen Fällen wird vom Kommunikationspartner ein Nachweis über eine vorhandene Eigenschaft gefordert, z.B. das Erreichen eines bestimmten Alters zum Abschluß von Geschäften im Internet. In machen Fällen wird ein von einem Computer generierter Datensatz zu einem persönlichen Merkmal, wie z.B. Cookies[1] in einem Web-Browser.

Natürlich ist der Name einer Person ein persönliches Merkmal und in vielen Fällen bereits ein identifizierendes Merkmal. Im wirklichen Leben empfinden wir es als durchaus normal, uns gegenseitig mit Namen vorzustellen, und im Normalfall wickeln wir Geschäfte auch unter unserem Namen ab. Ein davon abweichendes Verhalten wird berechtigterweise als sonderbar empfunden. Bei genauerem Hinsehen zeigt sich aber, daß es sehr viele **Ausnahmefälle** gibt, bei denen die bewußte **Anonymität**, d.h. das Verbergen der eigenen Identität, der akzeptierte Regelfall ist, z.B. telefonische Beratung, Schaufenster-Shopping[2], Bezahlen von Waren mit Bargeld. Vergleichbare Handlungen im Internet sollten ebenfalls anonym möglich sein. Eine Handlung, die man zwar nicht anonym, aber geheim durchführt, sind z.B. Wahlen. Man erlangt eine Berechtigung zum Wählen; der abgegebene Stimmzettel darf aber nicht verkettbar sein mit der Identität der Person, die den Stimmzettel abgegeben hat.

---

[1] Cookies sind kleine Datensätze (wenige Byte), die im Rechner des Benutzers abgespeichert werden. Sie ermöglichen dem Betreiber des Webservers, für den das Cookie generiert wurde, den Benutzer zu verfolgen, solange bzw. sooft er sich auf den Webseiten dieses Webservers aufhält. Im Beitrag von Thomas Roessler in diesem Band wird auf solche und andere „Datenspuren“ ausführlich eingegangen.

[2] auch mit Betreten des Ladens…

Die Benutzer neuer Medien haben bewußt oder unbewußt in Kauf genommen, daß die Kommunikationskultur der alten Medien (Brief, Telefon) nicht beibehalten werden kann und sich neue Ausdrucksformen gesucht.[3] Bezogen auf das Fordern und die Preisgabe persönlicher Merkmale hat sich allerdings eine Kultur etabliert, die noch weit entfernt von einem gesellschaftlichen Konsens ist. Zwei Beispiele sollen das verdeutlichen: **1.** Heute arbeitet nahezu jede kommerzielle Website mit Cookies, obwohl für die Anzeige der Webseiten überhaupt keine Cookies erforderlich sind. Inzwischen sind einige Anbieter von virtuellen Warenhäusern dazu übergegangen, die Warenkörbe ihrer Kunden ohne Cookies zur realisieren, obwohl Cookies ursprünglich hierfür gedacht waren. Mehr und mehr Kunden konfigurieren jedoch ihre Browser so um, daß Cookies generell abgelehnt werden. **2.** Viele Anbieter von Dienstleistungen fordern von ihren Kunden die Angabe von E-Mail-Adressen, obwohl für den Kunden überhaupt nicht einsichtig ist, warum dies beispielsweise beim legalen Download von frei verfügbarer Musik zwingend nötig ist. Ob der Kunde seine korrekte E-Mail-Adresse angibt oder nicht, ändert am Download meist nichts. Allerdings beeinflußt er die Anzahl eingehender Werbemails an ihn deutlich.

Dieses Papier versucht im folgenden, die technischen Möglichkeiten des Identitätsmanagements in Computernetzen darzustellen. Wir beschreiben in den Abschnitten 2 und 3 eines der wichtigsten Konzepte des Identitätsmanagements, die sog. Pseudonymität, die es ermöglicht, ohne das Offenlegen der eigenen Identität Aktionen durchzuführen und die Verkettbarkeit zu anderen Aktionen eines Benutzers gezielt zu steuern. Im Abschnitt 4 werden Verfahren beschrieben, mit denen man persönliche Eigenschaften nachweisbar machen kann. Im Abschnitt 5 folgen einige Bemerkungen zur Verwaltung von Pseudonymen in einem persönlichen Endgerät. Abschnitt 6 beschreibt an einem Fallbeispiel, wie ein Identitätsmanagement in Ansätzen für das Internet realisiert wurde. Das Papier schließt mit einer Zusammenfassung ab.

Pseudonymität

1.1 Pseudonymitätsstufen

Pseudonyme können nach dem Grad der erreichbaren Anonymität eingeteilt werden.[4] Bezogen auf die Gegebenheiten heutiger Computernetze werden im folgenden die drei wichtigsten Pseudonymitätsstufen erläutert.[5] Jede Stufe wird am Beispiel von E-Mail-Adressen erläutert.

---

[3] Als bekanntestes Beispiel gelten die Smileys in E-Mails.

[4] siehe hierzu Birgit Pfitzmann, Michael Waidner, Andreas Pfitzmann: Rechtssicherheit trotz Anonymität in offenen digitalen Systemen. Datenschutz und Datensicherung DuD 14/5-6 (1990) 243-253, 305-315.

[5] Pseudonyme werden von Pfitzmann et. al. 1990 zunächst in Personenpseudonyme und Rollenpseudonyme eingeteilt, die ihrerseits noch einmal unterteilt werden. Personenpseudonyme werden unterteilt in öffentliche Personenpseudonyme, nichtöffentliche Personenpseudonyme und anonyme Personenpseudonyme. Motiviert war die Einteilung nach öffentlich und nichtöffentlich durch die damals noch vorherrschende Telekommunikationsinfrastruktur (insbesondere für Telefonie) des Staates. Unter den Gegebenheiten der Liberalisierung der Telekommunikationsmärkte und der globalen Kommunikationsstruktur des Internets paßt die

Personenpseudonyme. Wird von einer Person über einen längeren Zeitraum und in vielen Kommunikationsbeziehungen mit unterschiedlichen Kommunikationspartnern das gleiche Pseudonym verwendet, spricht man von einem Personenpseudonym. Ein typisches Beispiel ist die E-Mail-Adresse einer Person, so wie wir sie heute vorfinden (z.B. oliver.berthold@gmx.de und hannes@icsi.berkeley.edu). Ein Personenpseudonym stellt also ein potentielles Personenkennzeichen dar, selbst dann, wenn die Zeichenkette, die das Pseudonym repräsentiert, auf den ersten Blick keinen direkten Personenbezug aufweist.

Geschäftsbeziehungspseudonym. Wählt sich eine Person für die Kommunikation mit einem bestimmten Kommunikationspartner jeweils ein neues, dann aber gleichbleibendes Pseudonym (z.B. eine neue E-Mail-Adresse), das keinen direkten Personenbezug aufweist (z.B. 1182643@hotmail.com), und verwendet sie das Pseudonym in keiner Kommunikationsbeziehung mit anderen Kommunikationspartnern, dann handelt es sich um ein Geschäftsbeziehungspseudonym.

Transaktionspseudonym. Falls sich eine Person entscheidet, jeweils für jede Transaktion ein neues Pseudonym einzusetzen (z.B. heute 3735428@yahoo.com und morgen jazzfan@hotmail.com beim Herunterladen von Musik von ein und demselben MP3-Server), dann spricht man von einem Transaktionspseudonym. Ein Transaktionspseudonym wird also nach Beendigung der Transaktion von diesem Teilnehmer nie wieder verwendet.

1.2 Verkettbarkeit von Pseudonymen

Personen-, Geschäftsbeziehungs- und Transaktionspseudonyme unterscheiden sich in der Verkettbarkeit der jeweiligen Kommunikationsereignisse. Nachrichten mit Transaktionspseudonymen sind mittels diesen überhaupt nicht verkettbar. Mit Geschäftsbeziehungspseudonymen gesendete Nachrichten sind für den Geschäftspartner verkettbar. Wenn jedoch zwei Geschäftspartner ihre Datenbanken abgleichen, lassen sich über die Pseudonyme keine Verkettungen zwischen ihren Kunden vornehmen. Bei Personenpseudonymen ist dies selbstverständlich möglich.

Leider sind die vorangegangenen Bemerkungen noch größtenteils Theorie, wenn man sich heutige Kommunikationsbeziehungen im Internet betrachtet. **1.** Man muß heute bei kostenpflichtigen Diensten praktisch immer seine Identität angeben, damit die Kosten per Rechnungsstellung oder Kreditkartenzahlung ausgeglichen werden. Anonyme Vorauszahlung von kostenpflichtigen Dienstleistungen hilft nur, wenn man bereits weiß, daß man etwas kaufen möchte und der Dienstleister anonyme Vorauszahlung überhaupt anbietet. **2.** Man sollte daran denken, daß in den heutigen Kommunikationsnetzen die Kommunikationsbeziehungen über die stets in einer Nachricht mitgesendete Absenderadresse (hier ist z.B. die IP-Adresse gemeint) verkettet werden können. Je nach Art des Zugangs zum

---

Unterscheidung nach öffentlichen, nichtöffentlichen und anonymen Personenpseudonymen nicht mehr ganz, bzw. es fällt schwer, ein konkretes Szenario in eine der drei Pseudonymitätsstufen einzuteilen. Die Unterschiede verschwimmen gewissermaßen. Rollenpseudonyme werden in Geschäftsbeziehungspseudonyme und Transaktionspseudonyme unterschieden.

Kommunikationsnetz (z.B. mit fest zugewiesener IP-Adresse oder mit dynamischer Adreßvergabe) ist die Benutzung eines Geschäftsbeziehungs- oder Transaktionspseudonyms ohne das zusätzliche Verbergen von Adreßinformation (z.B. durch sog. Mix-Netze oder Benutzen öffentlicher Zugangsnetze ohne Identitätsabfrage) unnütz. **3.** Bei keiner Form von Pseudonymverwendung sollte der Benutzer jemals seine Identität offenlegen, da andernfalls alle unter dem jeweiligen Pseudonym stattgefundenen Kommunikationsbeziehungen nachträglich zu seiner Identität verkettet werden können.

Es versteht sich von selbst, daß man ein Transaktionspseudonym verwenden sollte, wann immer es möglich ist.

Pseudonyme, mit denen man Aktionen einer Identität verketten kann

Ziel ist es, daß eine Person ohne Aufdecken ihrer Identität **mehrere Aktionen** (z.B. Versenden von E-Mails, Teilnahme in einem Chat-Room, Kauf von Waren in einem Online-Shop) ausführt und dabei bewußt wiedererkannt werden möchte. Dies ist der typische Anwendungsfall für Pseudonyme. Im Gegensatz zur Anonymität sollen Aktionen eines Teilnehmers miteinander **verkettbar** sein. Praktische Anwendungen könnten z.B. sein:

– die Fortsetzung eines Online-Gesprächs zwischen Personen, die sich nur online kennen und ihre Identität nicht voreinander preisgeben möchten,
– die Nutzung von Treuerabatten und individuell zugeschnittenen Angeboten in Online-Shops, in denen die „Ware“ ebenfalls digital ist, d.h. auf die Angabe einer Lieferadresse verzichtet werden kann.

Im folgenden werden typische Implementierungen für Pseudonyme beschrieben, mit denen man Aktionen einer Identität verketten kann.

1.3 Vom Teilnehmer selbst gewählte Zeichenketten, die keinen Bezug zu seiner Identität besitzen

Solche Pseudonyme (z.B. Petty Champagner, Veuve Cliquot) sind sehr einfach und intuitiv zu bilden, haben aber den Nachteil, daß mehrere Personen zufällig das gleiche Pseudonym wählen könnten. Außerdem wäre es einem bösartigen Teilnehmer möglich, absichtlich das Pseudonym eines fremden Teilnehmers anzunehmen. Dies ist nicht gleichzusetzen damit, daß er die Identität des echten Benutzers des Pseudonyms kennt.

1.4 Große Zufallszahlen (z.B. 150 Bit lang, d.h. mit etwa 45 Dezimalstellen)

Bei der Verwendung von großen Zufallszahlen (z.B. 15627384662036271…) treten zufällige Gleichheiten zwischen Pseudonymen nur noch mit verschwindend geringer Wahrscheinlichkeit auf. Ein bösartiger Teilnehmer könnte aber immer noch ein fremdes Pseudonym mißbrauchen. Außerdem lassen sich Zahlen mit 45 Dezimalstellen nicht mehr leicht merken, was die technisch unterstützte Speicherung der eigenen Pseudonyme auf einem

persönlichen Gerät nahelegt. Da man typischerweise mehrere Pseudonyme für unterschiedliche Kommunikationsbeziehungen verwendet, kommt man in der Praxis um ein solches Gerät nicht herum. Je nach Ort und Art der Pseudonymverwendung könnten die Pseudonyme im Personalcomputer, einem kleinen Persönlichen Digitalen Assistenten (PDA) oder einer Chipkarte gespeichert sein.

1.5 Öffentliche Testschlüssel eines Signatursystems

Verwendet man als Pseudonym den öffentlichen Testschlüssel eines Signatursystems, dann ist es erstens ebenfalls sehr unwahrscheinlich, daß mehrere Personen versehentlich das gleiche Pseudonym wählen, und außerdem wird es einem bösartigen Teilnehmer unmöglich gemacht, ein Pseudonym zu mißbrauchen. Jede pseudonym zu sendende Nachricht wird mit dem privaten Signierschlüssel digital signiert. Der Empfänger und alle Außenstehenden können überprüfen, daß eine Nachricht tatsächlich vom Pseudonym-Inhaber (hier: dem Eigentümer des öffentlichen Testschlüssels) stammt, da nur er den passenden Signierschlüssel besitzt. Der Vorteil dieser Sicherheit kann jedoch je nach Anwendung auch ein Nachteil sein: Für den Pseudonym-Inhaber ist es nicht mehr möglich, eine gesendete Nachricht gegenüber Dritten abzustreiten, da jeder Außenstehende die Signatur mit Hilfe des öffentlichen Testschlüssels überprüfen kann. Insbesondere dann, wenn zu einem späteren Zeitpunkt die Identität des Pseudonym-Inhabers öffentlich wird (aus Unachtsamkeit oder absichtlich) kann dies von Bedeutung sein.

Im kommerziellen Einsatz von Pseudonymen kann man die Überprüfbarkeit der Nachricht durch Dritte praktisch nutzen, um im **Streitfall eine Kommunikationsbeziehung aufdecken** zu können. Hierzu meldet sich ein Teilnehmer bei der vertrauenswürdigen Zertifizierungsstelle (Trusted Third Party) unter seiner Identität an und läßt sich seine Pseudonyme (d.h. seine öffentlichen Testschlüssel) zertifizieren. Das Zertifikat wird dann einen Datensatz enthalten, an dem der Prüfer feststellen kann, daß ein Aufdecken im Streitfall möglich ist. Die Zertifizierungsstelle merkt sich, welchem Teilnehmer sie welchen Schlüssel zertifiziert hat. Ein Beispiel ist in der Abbildung 1 dargestellt.

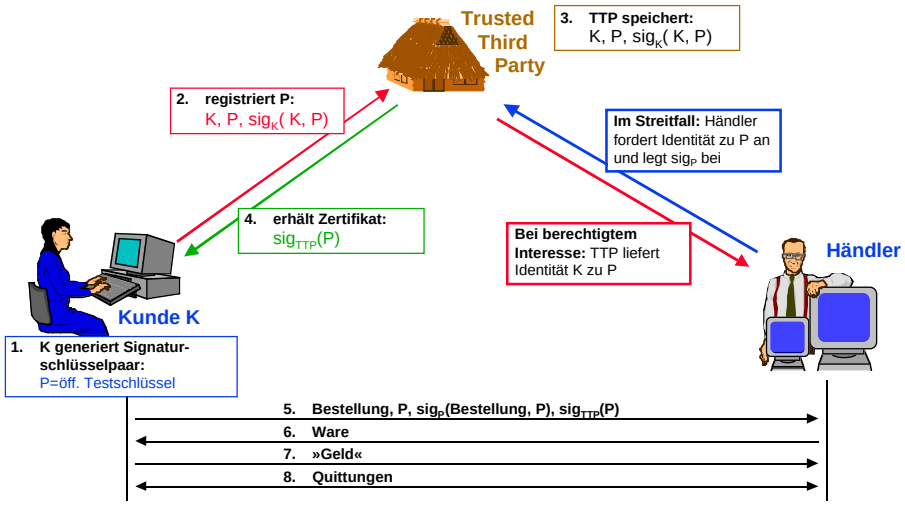

Abbildung 1: Ausstellen, Benutzen und Aufdecken eines Pseudonyms

Dieses Verfahren läßt sich auch derartig dezentralisieren, daß die Zuordnung eines Pseudonyms zu einer Identität nur unter Zusammenarbeit mehrerer Zertifizierungsstellen möglich ist, um das mögliche Fehlverhalten einer Zertifizierungsstelle zu tolerieren. Hierzu läßt man sich beispielsweise von einer Zertifizierungsstelle Z_1 ein Pseudonym P_1 zertifizieren, zu dem sie die Identität kennt. Von einer weiteren Zertifizierungstelle Z_2 läßt man sich ein Zertifikat über ein Pseudonym P_2 ausstellen, zu dem Z_2 bestätigt, daß es das Pseudonym P_1 kennt, das von der Zertifizierungsstelle Z_1 bestätigt wurde u.s.w. Der Benutzer benutzt das letzte ausgestellte Pseudonym. Im Streitfall muß die Verkettung rückwärts unter Mitarbeit aller beteiligten Zertifizierungsstellen aufgelöst werden.

Pseudonyme zur Bestätigung von Eigenschaften

Neben der Verkettung von Aktionen eines Teilnehmers, der seine Identität geheimhalten möchte, gibt es viele Anwendungsfälle, in denen der Kommunikationspartner das Vorhandensein einer ganz bestimmten Eigenschaft überprüfen können soll. Dies könnte der Nachweis über die Zugehörigkeit zu einer bestimmten Altersgruppe (z.B. „über 18 Jahre alt“) sein oder die Bestätigung einer Bank über einen bestimmten Kreditrahmen. Unsere digitale Identität wird durch einen Vektor solcher Attribute gebildet. Neben eindeutig identifizierenden Merkmalen (z.B. Personalausweisnummer) gibt es in der Mehrzahl Attribute, die auf eine Gruppe gleichermaßen zutreffen (z.B. Geburtsjahr, Geschlecht, Wohnort). Häufig genügt es dem Kommunikationspartner, daß er eine bestimmte Eigenschaft sicher überprüfen kann (z.B. Nachweis der Geschäftsfähigkeit bei Online-Geschäften), aber weitere Eigenschaften vor ihm verborgen bleiben.

1.6 Ein sehr einfaches Verfahren

Eine sehr einfache Möglichkeit zur Zertifizierung von Eigenschaften besteht darin, daß eine Zertifizierungsstelle den öffentlichen Testschlüssel des Pseudonyms zusammen mit der nachzuweisenden Eigenschaft zertifiziert.

```
BEGIN ZERTIFIKAT
Pseudonym: 304526342723466234249872413 75
Öffentlicher Testschlüssel des Pseudonyms:
h833hd38dddajscbicme098342k236egfkw74h5445
84hdbscldmrtpofjrkt0jshuedagaszw12geb3u4b=
Bestätigte Eigenschaften:
Der Inhaber ist über 18 Jahre alt.
Der Inhaber ist deutscher Staatsbürger.
Datum: 19.03.2000
Gültig bis: 18.03.2001
Aussteller: Einwohnermeldeamt Dresden
Signatur des Ausstellers:
23j423vdsaz345kj435ekji3u4z2983734ijo23i72
kj867wdbez2o074j5lkdmcdkki1237t3rgbdvbwdj=
END ZERTIFIKAT
```

Der Teilnehmer signiert seine Nachricht mit dem privaten Signierschlüssel seines Pseudonyms. Der Kommunikationspartner benötigt zum Nachweis der Echtheit der Nachricht den Testschlüssel und das Zertifikat. Falls mehrere Eigenschaften in ein Zertifikat aufgenommen werden, reduziert das zwar die Anzahl auszustellender Zertifikate, jedoch liefert der Teilnehmer dem Kommunikationspartner möglicherweise mehr Information, als dieser fordert. Weiterhin kennt die Zertifizierungsstelle im Regelfall die Zuordnung zwischen Identität, Pseudonym und den zertifizierten Eigenschaften. Ein solches System ist also noch verbesserungswürdig. Man möchte im Idealfall ein System, mit dem ein Teilnehmer beweisen kann, daß er eine in dem jeweiligen Kontext geforderte Eigenschaft besitzt, ohne ungewollt alle oder zumindest eine Vielzahl weiterer Eigenschaften über sich offenzulegen. Weiterhin möchte man nicht, daß die Vorlage derselben Eigenschaft an anderer Stelle mit der bei einer vorherigen Stelle verkettbar ist. Außerdem soll vor der Zertifizierungsstelle das Pseudonym verborgen bleiben, für das sie ein Zertifikat mit einer bestimmten Eigenschaft ausstellt.

1.7 Blenden des Pseudonyms vor dem Zertifizieren

Wenn man verhindern möchte, daß die Zertifizierungsstelle die Zuordnung von Identität und Pseudonym kennt, kann man folgendes Verfahren anwenden: Der Teilnehmer blendet das Pseudonym mit einer Zufallszahl, die sich nach der Zertifizierung des Pseudonyms wieder entfernen läßt, ohne das Zertifikat zu zerstören. Ein kryptographisches Verfahren, mit dem so etwas erreicht werden kann, ist als **Blinde Signatur**[6] bekannt.

Die Zertifizierungsstelle bestätigt gewissermaßen eine Eigenschaft einer Person, deren Pseudonym die Zertifizierungsstelle nicht kennt. Da die Zertifizierungsstelle nichts über den Inhalt (hier: das Pseudonym) erfährt, den sie digital signiert, kann die Eigenschaft auch nicht in das Zertifikat selbst kodiert werden, wie dies z.B. beim Zertifikat in Abschnitt 4.1 der Fall

[6] David Chaum: Blind Signature System. Crypto '83, Plenum Press, New York 1984, 153.

war. Stattdessen wird die Eigenschaft fest mit dem jeweiligen Schlüssel assoziiert, den die Zertifizierungsstelle verwendet. Für jede zu zertifizierende Eigenschaft besitzt sie ein eigenes Schlüsselpaar.

1.8 Secret-Key-Zertifikate

Geblendete Zertifikate aus dem vorangegangenen Abschnitt haben in der Praxis verschiedene Nachteile:

- Es ist der Zertifizierungsstelle unmöglich, in das Zertifikat ein Ausstellungs- oder Verfallsdatum hineinzukodieren.
- Die Anzahl der Eigenschaften wird bestimmt durch die Anzahl der Schlüsselpaare der Zertifizierungsstelle. Zu jeder Eigenschaft muß der zu dieser Eigenschaft assoziierte öffentliche Testschlüssel im Voraus bekannt sein, damit man die Blendung des Pseudonyms durchführen kann.
- Ein Teilnehmer könnte sich eine Eigenschaft bestätigen lassen und das Zertifikat dann unbemerkt weitergeben oder verkaufen.

Mit sogenannten Secret-Key-Zertifikaten[7] sollen sich diese Nachteile beseitigen lassen. Bei allen bisher beschriebenen Zertifikaten handelt es sich um Echtheitsnachweise des öffentlichen Testschlüssels eines Signatursystems. In den Echtheitsnachweis werden dann ggf. zusätzliche Eigenschaften mit aufgenommen. Mit den patentierten Secret-Key-Zertifikaten soll man von vielen innerhalb eines Zertifikats vorhandenen zertifizierten Eigenschaften je nach Bedarf eine Untermenge aufdecken können, während andere Eigenschaften verdeckt bleiben. Damit wäre im Extremfall nur noch ein Zertifikat nötig, in dem sich der Teilnehmer eine Vielzahl von Eigenschaften bestätigen läßt. Die Überprüfung der Eigenschaft erfolgt in einem interaktiven Verfahren mit der Zertifizierungsstelle.

Identitätsverwaltung im lokalen Gerät

Wie bereits in Abschnitt 3.2 erwähnt, wird man in der Praxis um die technisch unterstützte Speicherung der Pseudonyme nicht herumkommen. Da man für die Digitale Signatur zukünftig sowieso ein persönliches Gerät besitzen wird, bietet es sich an, auch das **Identitätsmanagement**, d.h. die **Pseudonymverwaltung** darauf vorzunehmen, soweit dies technisch möglich ist.[8]

Ein solches Gerät sollte:

- vertrauenswürdig sein, d.h. zumindest nicht manipulierbare Hardware, ein vertrauenswürdiges Betriebssystem und strikte Prozeß- und Speichertrennung besitzen,
- ausreichende Rechenleistung für asymmetrische Kryptographie, d.h. digitale Signatur und Public-Key-Verschlüsselung, besitzen,

[7] Stefan Brands: Rethinking public key infrastructures and digital certificates — building in privacy. http://www.xs4all.nl/~brands/.

[8] Zu den Anforderungen des Identiätsmanagements im Endgerät siehe Marit Köhntopp: Generisches Identitätsmanagement im Endgerät. http://www.koehntopp.de/marit/publikationen/idmanage/.

– eine geeignete Benutzungsschnittstelle bereitstellen, die tatsächlich das anzeigt, was signiert werden soll,
– eine autonome Energieversorgung und eigene Uhr besitzen, um Angriffe über Energie- oder Zeitverbrauch auszuschließen.

Für einen Benutzer, der Pseudonyme intensiv nutzt, stellt sich möglicherweise irgendwann einmal die Frage „Welches Pseudonym hatte ich damals für die Kommunikation mit … verwendet?“. Ein Identitätsmanager muß den Benutzer dabei unterstützen, für jede Kommunikationsbeziehung das „richtige“ Pseudonym auszuwählen.

Folgende Regeln bzw. Funktionen sollte ein Identitätsmanager dabei implementieren:
– Wann immer es möglich ist, sollte der Teilnehmer **anonym und unbeobachtbar kommunizieren** können. Ausnahmen von dieser Grundregel bestimmt der Benutzer.
– Grundsätzlich sollte für jede Kommunikationsbeziehung ein eigenes Pseudonym benutzt werden. Das bedeutet, jede neue Kommunikationsbeziehung beginnt mit dem **Generieren eines neuen Pseudonyms**, solange der Benutzer nichts anderes bestimmt.
– Normalerweise ist es erwünscht, vom Kommunikationspartner wiedererkannt zu werden (gleiches Pseudonym). Ausnahmen (verschiedene Pseudonyme gegenüber dem gleichen Partner) müssen dann als **verschiedene eigene Rollen** definiert werden können.
– Eine Person kann ein Pseudonym dazu verwenden, um eine **Eigenschaft beweisen** zu können, ohne die Identität preisgeben zu müssen: Beispielsweise könnte sich ein Arzt seinen Beruf bescheinigen lassen.
– Der Identitätsmanager sollte es seinem Benutzer ermöglichen, **selektiv Informationen mit einem Pseudonym verknüpfen**: Name, Adresse, Alter, Beruf, Hobbies, Freundeskreis etc.
– **Monotonie:** Informationen, die bezüglich eines Pseudonyms verkettet wurden, sind nicht mehr entfernbar. Es ist nur noch möglich, ein neues Pseudonym zu wählen. Man muß jedoch aufpassen, daß zusammen mit dem neuen Pseudonym nicht zu viele Informationen preisgegeben werden, weil es sonst über die Gleichheit der Eigenschaften mit dem alten verkettbar wird.
– Wann immer der Benutzer es wünscht, sollte er eigene **Pseudonyme für den Kommunikationspartner miteinander verkettbar** machen können. Welcher Informationsgewinn dadurch beim Kommunikationspartner entsteht, sollte durch den Identitätsmanager sichtbar gemacht werden.

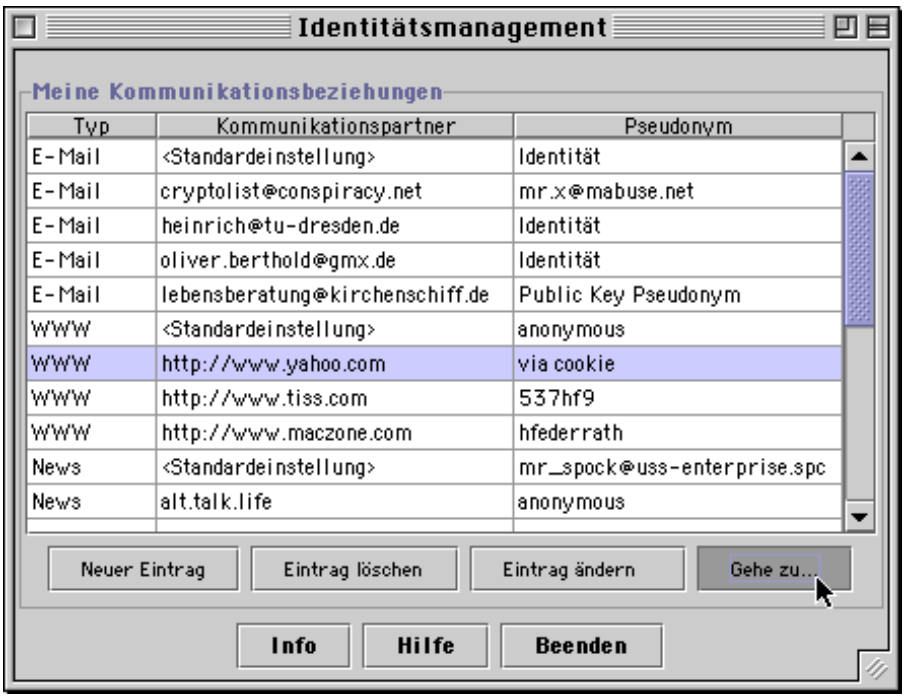

Abbildung 2: Beispiel einer Oberfläche eines Identitätsmanagers

Um den Benutzer nicht mit dem Management der eigenen Pseudonyme zu überfordern, sollte eine möglichst einfache **persönliche Managementzentrale** der Ausgangspunkt aller anonymen bzw. pseudonymen Kommunikationsbeziehungen sein. In der Abbildung 2 ist ein Vorschlag hierfür dargestellt. Der Benutzer wählt seinen Kommunikationspartner aus, indem er auf die Zeile in der Tabelle klickt. Im entsprechenden Kommunikationsprogramm (Mailprogramm, Browser, News-Reader) wird dann automatisch das entsprechende Pseudonym gewählt und die Kommunikationsverbindung entsprechend hergestellt. Dabei können die Einzelheiten des Pseudonymaufbaus vor dem Benutzer verborgen bleiben, sofern die interne Repräsentation des Pseudonyms sowieso nur aus Zufallszahlen bzw. sinnlosen Zeichen (z.B. Cookies) oder öffentlichen Testschlüsseln besteht.

Fallbeispiel: Das Pseudonymkonzept von Freedom

Freedom ist ein von der kanadischen Firma Zero-Knowledge Systems (ZKS) Inc. angebotener Service, der es Internetnutzern ermöglicht, mehrere verschiedene Internetdienste anonym zu nutzen. Die Anonymität wird dadurch gewährleistet, daß die Kommunikationsbeziehung zwischen dem Rechner des Teilnehmers und dem jeweiligen Internetserver über eine Anzahl von anonymisierenden Zwischenknoten, die sog. Freedom-Server, geleitet wird. Da diese Knoten gleichzeitig die Kommunikationsbeziehungen vieler Teilnehmer vermitteln, kann ein externer Beobachter die Zuordnung zwischen eingehenden und ausgehenden Nachrichten nicht mehr ermitteln. Für einen Angreifer, der nicht alle diese Knoten kontrolliert, ist somit die Kommunikationsbeziehung eines Teilnehmers unbeobachtbar.

Völlige Anonymität ist jedoch nur für Kommunikationsbeziehungen möglich, die in einem Kommunikationsschritt abgewickelt werden können. Ein Beispiel hierfür wäre das anonyme Versenden einer E-Mail. Sobald jedoch für einen Dienst mehrere Kommunikationsschritte erforderlich sind, muß jeder der Teilnehmer einen Schritt des anderen zu dessen vorherigen Schritten verketten können. Normalerweise erfolgt diese Verkettung entweder über die Identität oder Adresse des jeweiligen Teilnehmers. Bei einer anonymen Nutzung eines solchen Dienstes ist dafür ein **Pseudonym** nötig, welches je nach Art des Dienstes über unterschiedlich lange Zeiträume gültig sein muß. Eine Reply-Adresse in einer pseudonym gesendeten E-Mail sollte beispielsweise einige Tage wenn nicht gar dauerhaft gültig, d.h. in der Lage sein, an sie gesendete E-Mails unbeobachtbar an den eigentlichen Teilnehmer weiterzuleiten.

Aus diesen Gründen wurde in Freedom folgendes Pseudonymkonzept[9] integriert.

1.9 Pseudonymkonzept

Jeder Teilnehmer erhält eine Anzahl Pseudonyme, die bei Freedom „Nyms“ genannt werden. Der Teilnehmer kann nun einem Internetdienst unter diesem Pseudonym gegenübertreten. So wird z.B. für jedes Nym eine E-Mail-Adresse bereitgestellt, unter der der Teilnehmer Nachrichten empfangen und senden kann. Beim Senden einer E-Mail über das Freedom-Netz wird die E-Mail-Adresse des jeweils ausgewählten Nyms als Absenderadresse eingetragen.

Momentan wird das Nym-Konzept nur für E-Mails konsequent angewendet. Für andere Anwendungen wird das Nym nur verwendet, um die Berechtigung des Benutzers zur Nutzung des Freedom-Netzes zu beweisen. Das Nym wird vom letzen Freedom-Server aus der zu sendenden Nachricht entfernt, bevor die Nachricht an die Zieladresse weitergeleitet wird.

Solange ein Nutzer Nachrichten unter dem gleichen Nym durch das Freedom-Netz schickt, sind alle gesendeten **Nachrichten** zu dem Nym **verkettbar**. Jedoch bleibt die Identität des Absenders geschützt.

Das Haupteinsatzgebiet der Nyms dürfte bis auf weiteres das pseudonyme Senden und Empfangen von E-Mail sein. Darauf basiert auch das Geschäftsmodell von Freedom. Während kurzfristig gültige (30 Tage) Nyms kostenlos erhältlich sind, muß man Nyms mit längerer Gültigkeit kostenpflichtig mieten. Dabei kauft man sich jeweils ein Nutzungsrecht für 5 Nyms für den Zeitraum von 6 Monaten zum derzeitigen Preis von 49,90 US Dollar. Die Pseudonyme können nach Ablauf dieser Zeitspanne verlängert werden.

1.10 Nymerzeugung

Ein Nym ist in erster Linie ein Kennzeichen, daß es einem Teilnehmer ermöglicht, mehrere über ein anonymes Netz gesendete Nachrichten gegenüber einer anderen Station als zusammengehörig zu kennzeichnen. Die Erzeugung eines solchen Nyms ist sehr einfach: Der

[9] Russel Samuels: Untraceable Nym Creation on the Freedom Network. Whitepaper, November 1999, http://www.freedom.net/.

Teilnehmer wählt einfach eine **sehr große Zufallszahl** (mit ca. 128 Bit bzw. 40 Dezimalstellen), die er später in jeder Nachricht mitsendet. Ein solches Pseudonym ist, wenn man dem benutzten anonymen Kommunikationsnetz vertrauen kann, grundsätzlich unverkettbar zu dem Teilnehmer, da er es selbst ohne Dritte erzeugt. Bei Freedom hat ein Pseudonym jedoch noch weitere Funktionen. So soll z.B. durch den Verkauf von Nyms eine **Abrechnung der Dienstleistung** ermöglicht werden.

Die existierenden Zahlungssysteme haben jedoch den Nachteil, daß der Teilnehmer beim direkten Kauf eines Nyms über das Internet (z.B. mittels einer Kreditkarte) identifiziert wird und somit das Nym, das ja die Preisgabe der Identität verhindern soll, wertlos wäre. Um die Unverkettbarkeit von Identität und Nym beim Kauf sicherzustellen, wird ein interaktives Protokoll unter Zuhilfenahme mindestens eines vertrauenswürdigen Dritten abgearbeitet.

Um einer solchen Partei nicht vollständig vertrauen zu müssen, sind bei Freedom an den Nymerzeugungungsprozeß mehrere Parteien so beteiligt, daß im Idealfall die Unverkettbarkeit des Pseudonym bereits dann garantiert ist, wenn eine der Parteien vertrauenswürdig ist. Man muß somit nicht mehr einer einzigen Partei vertrauen.

Der Nymerzeugungsprozeß (siehe Abbildung 3) läuft in 3 Stufen unter Einbeziehung von 4 Parteien ab:

1. Der Nutzer erwirbt vertraulich von einem sog. **WWW-Shop**, einem Server von ZKS, eine Seriennummer, die ihn zum Erwerb eines sog. **Nym-Tokens** berechtigt. Den Preis für diese Transaktion kann er per Kreditkarte oder per Postbrief bezahlen. Die Seriennummer wird in einer zentralen Datenbank von Freedom gespeichert und freigeschaltet, sobald der Geldbetrag dem WWW-Shop gutgeschrieben wurde.
2. Der Nutzer baut eine unbeobachtbare Verbindung zu einem **Token-Server** auf und übermittelt die im ersten Schritt erhaltene Nummer. Der Token-Server, der von einer vertrauenswürdigen Dritten Partei betrieben wird, überprüft die Gültigkeit der Seriennummer durch Abfragen der Datenbank und übermittelt dem Nutzer bei erfolgreicher Überprüfung ein oder mehrere **Nym-Token**. Diese Nym-Token sind vom Token-Server signierte Berechtigungsmarken zur Erzeugung eines Nyms.
3. Mit Hilfe des Nym-Tokens kann der Nutzer später auf einem zentralen **Nym-Server**, der von ZKS betrieben wird, jeweils ein **Nym** (d.h. eine pseudonyme E-Mail-Adresse) erstellen.

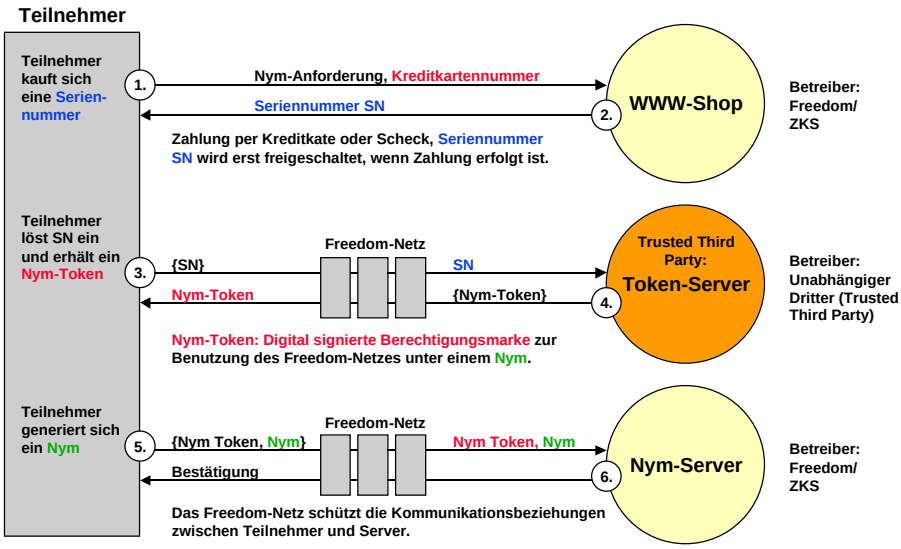

Abbildung 3: Nymerzeugung bei Freedom

Wenn man darauf vertraut, daß eine Verbindung über das Freedom-Netz unbeobachtbar ist, dann kann ein Nym nur dann mit der Identität des Teilnehmers verkettet werden, wenn alle oben genannten Server zusammenarbeiten. Zurzeit wird allerdings höchstens der Token-Server nicht direkt von ZKS betrieben. Später soll u.U. auch der WWW-Shop an andere Anbieter ausgelagert werden, während der Nym-Server stets von ZKS betrieben wird.

1.11 Pseudonymverwaltung

Bei der Verwaltung seiner pseudonymen Identitäten wird der Nutzer momentan fast nicht unterstützt. Er muß vor der Nutzung eines Internetdienstes angeben, unter welchem Pseudonym dies geschehen soll.

Bei E-Mail erscheint dann beispielsweise als Absenderadresse das aktuell ausgewählte Nym des Teilnehmers. Eine etwaige Rückantwort auf eine unter einem bestimmten Nym gesendete E-Mail wird dem Teilnehmer zugestellt, sobald er wieder unter dem Nym aktiv wird.

Die Nymverwaltung beim WWW verfügt zumindest über folgendes Feature. Durch die Cookie-Funktion der WWW-Browser wird den WWW-Servern eine Verkettung von mehrere Zugriffen eines Teilnehmers ermöglicht. Im Prinzip ist ein solcher Cookie nichts anderes als ein Pseudonym. Würden die Cookies einfach an den Browser weitergeleitet, könnten die WWW-Server bzw. der jeweilige letzte Freedom-Server verschiedene Nyms verketten, wenn der Teilnehmer den entsprechenden Internetserver unter verschiedenen Pseudonymen besucht. Aus diesem Grund werden die übermittelten Cookies von Freedom gefiltert und auf Wunsch unter dem benutzen Pseudonym abgespeichert. Eine Verkettung mehrerer Nyms über die Cookies ist somit ausgeschlossen.

Insgesamt würde man sich eine intelligentere Pseudomverwaltung wünschen, die für jedes Pseudonym eine Nutzungshistorie erstellt, so daß dem Nutzer für eine bestimmte

Kommunikationsbeziehung das passende Pseudonym vorgeschlagen und vor möglichen ungewollten Verkettungen gewarnt werden kann.

In Zukunft plant ZKS das Nym-Konzept zu erweitern. So soll es z.B. möglich sein, daß ein Teilnehmer bzw. ein Nym verschiedene Eigenschaften gegenüber anderen Stationen nachweisen kann. Der wesentliche Fortschritt dabei ist, daß der Teilnehmer entsprechend der Situation auswählen kann, welche zertifizierten Eigenschaften der Kommunikationspartner erfahren soll. Zusätzlich soll ein anonymes Zahlungssystem integriert werden. Basis für diese Erweiterungen sind die Patente von Stefan Brands.

Zusammenfassung

Anonymität, Pseudonymität und Identitätsmanagement sind stark miteinander verflochten. Dabei bilden Anonymität und Identität die Pole eines „Pseudonymitätsfeldes“. Privatheit, d.h. im Kontext dieses Papiers Anonymität und Unbeobachtbarkeit kann der Benutzer nur verlieren: Jemals preisgegebene Informationen können nicht zurückgezogen werden. Deshalb sollte, wann immer es möglich ist, anonym kommuniziert werden. Wo Verkettbarkeit gefordert wird, sollten zunächst Transaktionspseudonyme eingesetzt werden, bevor die Verkettbarkeit weiter erhöht und die Anonymität weiter reduziert wird. Die pseudonyme Zertifizierung von Eigenschaften einer Person ist insbesondere bei der kommerziellen Nutzung von Dienstleistungen in Computernetzen hilfreich, da sie dem Dienstleister Sicherheiten gibt, aber dem Benutzer trotzdem Anonymität gewährt.

Für Hinweise, Kritik und Korrekturlesen geht ein herzlicher Dank an Marit Köhntopp, Andreas Pfitzmann und Thomas Roessler.