Seminar Secure Web Application Engineering
Stefan Richter/734347

Identitätsmanagement

„Who is the Dick on your site?“

Inhaltsverzeichnis

1. Einleitung

Das Identitätsmanagement ist eines der aktuellen, wichtigen Themen in der Systemverwaltung und den Internet-Technologien. Wie soll ein Mensch möglichst einfach und zugleich sicher mit seinen (vielfältigen) Identitäten umgehen? Welche Anforderungen stellt er an ein System, dass ihm dabei helfen soll? Und welche Unterschiede bestehen zwischen abgeschlossenen Organisationen, wie zum Beispiel Universitäten, und dem Internet? Viele Fragen und die vielleicht wichtigste fehlt noch: Was ist „Identität“ eigentlich? Auf die meisten davon ist noch keine endgültige Antwort gefunden worden, aber es gibt bereits interessante Konzepte und Ideen.

Dazu zuerst ein kleiner Exkurs zur Bestimmung der Eigenschaften einer Identität und in wie weit auf diese in IT-Systemen Rücksicht genommen werden müssen. Aufbauend werden dann die Variationen des Identitätsmanagements dargestellt und einige, damit im Zusammenhang stehende, technische Grundbegriffe betrachtet. Bevor man die innovativen, neuen Entwicklungen Einschätzen kann, sollte man sich die bereits etablierten Technologien betrachten. Zu guter Letzt sollen dann noch zwei Vertreter dieser neuen Technologien kurz vorgestellt werden.

2. Eigenschaften einer Identität

Als grundlegende Frage beim Thema Identitätsmanagement stellt sich: Was ist eigentlich Identität und sind alle Identitäten gleich(-wertig)? Als wichtigste aller Identitäten hat jeder Mensch eine physische Identität, sozusagen sein selbst. Durch ihre schlechte Fassbarkeit ist diese für die Verwendung in IT-Systemen ungeeignet. Aus diesem Grund haben die meisten Menschen in unserer Umgebung noch eine oder mehrere digitale Identitäten, zum Beispiel in Form ihres eMail-Accounts oder einer persönlichen Website. Mit der Weiterentwicklung der Technik ist dabei in den letzten Jahren noch eine besondere Art der digitalen Identität entstanden: die virtuelle Identität. In virtuellen Welten wie „World of Warcraft“ oder „Second Life“ wird der digitalen Identität noch eine bessere graphische Ausdrucksmöglichkeit eingeräumt: die Avatare. Diese Unterscheidung spielt im Kontext des Identitätsmanagement aber nur eine untergeordnete Rolle.

Neben dieser Unterscheidungsweise kann man Identitäten noch nach ihrer Herkunft unterscheiden: individuelle Identität vs. Organisations-Identität. Die individuelle Identität entspricht weites gehend dem allgemeinen Verständnis von Identität. Die organisatorische Identität dagegen, ist die Rolle einer Person oder einer Sache in einem Unternehmen und damit die häufigste Form der digitalen Identität innerhalb von Firmen.

Bei so vielen verschiedenen Arten von Identitäten stellt sich die Frage nach den Gemeinsamkeiten und damit nach einer einheitlichen Definition. Ganz allgemein ist eine Identität „die völlige Übereinstimmung einer Person oder Sache mit dem, was sie ist oder als was sie bezeichnet wird“(Prof. Zorn; Hasso-Plattner-Institut Potsdam). Der erste Teil dieser Definition ist die für physische Identitäten selbstverständliche. Leider lässt sich diese nur schlecht auf digitale Identitäten übertragen, für diese verwendet man dann einen zumeist Namen. Dabei folgt aus der Definition sofort eine Frage: wie stellt man diese Übereinstimmung fest?

Um dieses Problem zu lösen, klärt man die Frage, wie der Mensch Übereinstimmungen zwischen einem Objekt und seiner Erinnerung an das Objekt feststellt. Das Gehirn speichert von einem Objekt einen Satz von Merkmalen, wie zum Beispiel das Bild oder die Haptik.

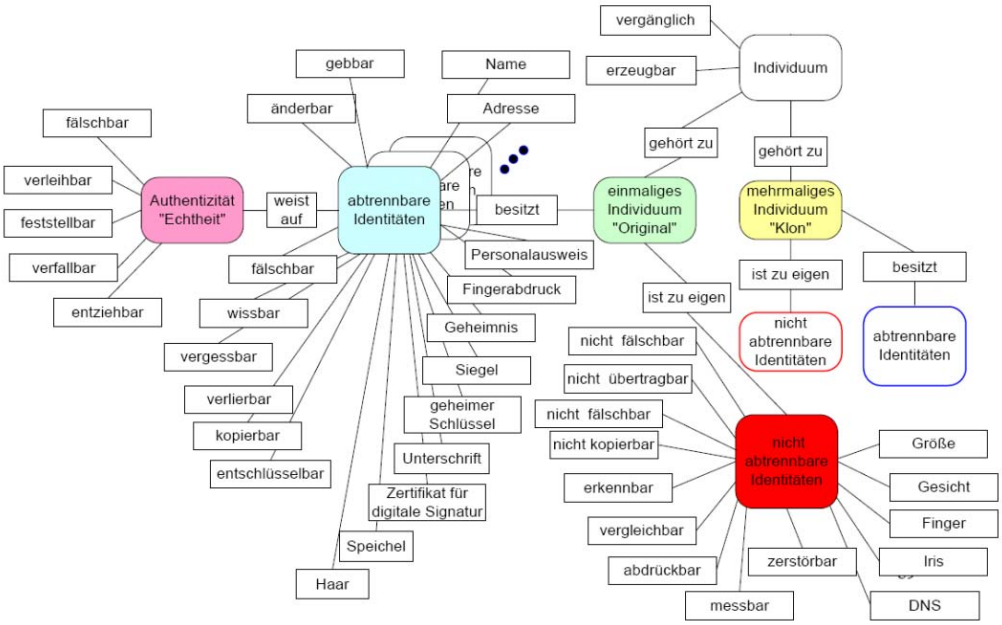

Abbildung 1: abtrennbare und nicht abtrennbare Identitäten

Dabei kann man diese Eigenschaften in zwei Kategorien einteilen: abtrennbare und nicht abtrennbare. So kann ein Mensch zum Beispiel seinen Personalausweis ändern, eine abtrennbare Eigenschaft, aber nicht seine DNS, eine nicht abtrennbare Eigenschaft. So wird offensichtlich, dass eine Identität, deren Eigenschaftssatz nur aus abtrennbaren Eigenschaften besteht, relativ einfach zwischen Menschen übertragen werden kann. Daher muss bei diesen Identitäten in der Echtheitsprüfung auf besondere Sorgfalt geachtet werden. So ergibt sich als verbesserte Definition für die Identität: völlige Übereinstimmung der überprüfbaren Eigenschaften eines Individuums mit dessen unverwechselbaren Eigenschaften. Aus diesen verschiedenen Teilmengen der Menge aller Eigenschaften des Menschen bzw. Objektes ergeben sich damit auch verschiedene Teilidentitäten.

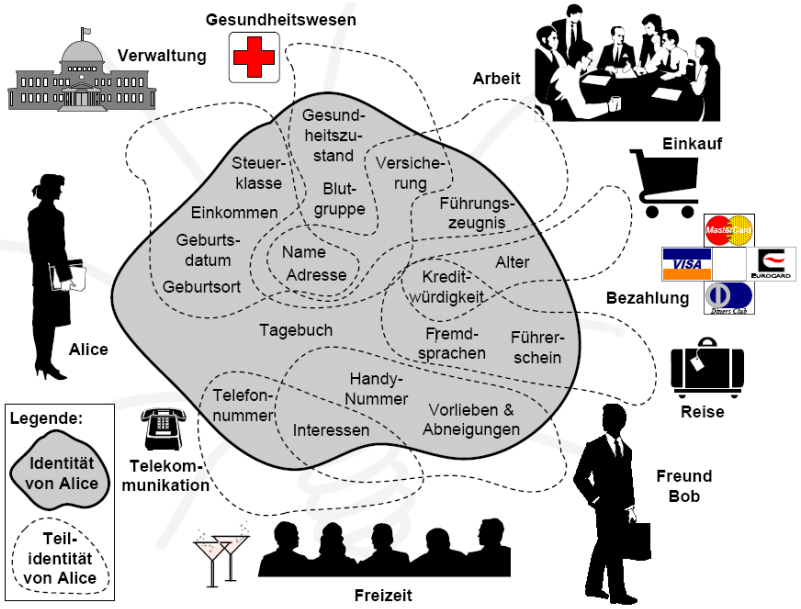

Abbildung 2: Teilidentitäten

So ist für das Gesundheitswesen zum Beispiel nicht von Interesse welche Fremdsprachen Alice spricht, welche Blutgruppe sie hat dagegen schon. Aus dieser Vielfalt von Teilidentitäten ergibt sich der Bedarf für ein adäquates Identitätsmanagement.

3. Verwaltung von Identitäten

Aufgrund Vielzahl der verschiedenen Teilidentitäten wäre ein übersichtliches Identitätsmanagement für die Endbenutzer von großem Nutzen. Dabei werden prinzipiell zwei Definitionen von Identitätsmanagement unterschieden:

- „Als Identitätsmanagement (IdM) wird der zielgerichtete und bewusste Umgang mit Identität, Anonymität und Pseudonymität bezeichnet.“(Wikipedia) bzw.
- „Der Zweck des Identity and Access Management (IAM) ist die Vielzahl der Kennungen und personenbezogenen Informationen welche die Anwender für den Zugriff auf Applikationen, Ressourcen und IT-Systeme benötigen, zu reduzieren und nach Möglichkeit in einer einzigen digitalen Identität zusammenzufassen.“(Prof. Zorn; Hasso-Plattner-Institut).

Die erste Definition geht in Richtung des benutzerzentrischen Identitätsmanagement das später noch besprochen wird. Die zweite Definition ist die in der Organisations-IT übliche Interpretation. Direkt daraus leiten sich auch die beiden Arten des Identitätsmanagement ab: Account Management und

benutzerzentrisches Identitätsmanagement. Während das erste zugewiesene Identitäten verwaltet, wählt sich der Benutzer beim letzteren eine eigene Identität und muss diese auch (mit Hilfe eines Dienstleisters) selbst verwalten. Dabei kann man auch eine technologische Weiterentwicklung feststellen, von fremdverwalteten Accounts zu selbstverwalteten, digitalen Identitäten.

4. Digitale Identitäten

Dabei stellt sich natürlich die Frage: wozu braucht man (s)eine (Teil-)Identität? Die mit Abstand wichtigste Verwendung für digitale Identitäten ist der Zugriff auf Ressourcen und Services. Um diesen Zugriff zu erlangen, bedarf es zweier Dinge: Authentifizierung und Autorisierung. Zunächst muss die Echtheit der vorgezeigten Identität bewiesen werden. Dies geschieht in der realen Welt zumeist mit einer Unterschrift oder einem Foto auf einem vertrauenswürdigem Dokument (Bsp.: Personalausweis, Führerschein). Diese Wege sind in der digitalen Welt nicht möglich, der hier gebräuchliche, aber auch unbequeme und damit unsichere Weg, ist ein Passwort. Die klassische Technologie im Internetumfeld ist dabei die HTTP-Basic-Authentifikation.

Der zweite Teil des Zugangsprozesses prüft, ob der authentifizierte Benutzer die angeforderte Ressource überhaupt benutzen darf. Der einfachste und gebräuchlichste Weg dafür ist die Verwaltung der Rechte mit Hilfe von „Access Control Lists“. Dabei steht in der Liste für jeden Benutzer implizit oder explizit wie er die aktuelle Ressource nutzen darf (Bsp.: Leserecht auf eine Datei).

5. Aktuelle Technologien

Anfänglich gab es einfache Benutzerlisten auf abgeschlossenen Maschinen, dann begann sich jedoch der Wunsch zu regen nur eine einzige Identität in einer Organisation zu besitzen und, je nach Rechten, diese überall einsetzen zu können. Doch dazu waren neue Ansätze und Technologien nötig, welche das Identitätsmanagement vereinfachten und zentralisierten.

5.1. Verzeichnisdienste

Als zentraler Verwaltungs- und Aufbewahrungsort für Identitäten haben sich Verzeichnisdienste etabliert. Auf Basis des Telefonbuchkonzeptes haben die Telefonkonzerne das Zentralisierungsproblem durch die Einführung von hierarchisch gegliederten, zentralen Verzeichnissen in Angriff genommen. Der allgemeine Durchbruch dieser Technologie vollzog sich allerdings erst nach der Entwicklung eines einfach Zugriffsprotokolls: LDAP(Lightweight Directory Access Protocol). In LDAP-basierten Verzeichnisdiensten sind die Objekte in hierarchisch Strukturierten „organisatorischen Einheiten“(OU) geordnet. Neben einem eindeutigen Namen(basierend auf der Position im Baum) zeichnet sich ein Element hierbei noch durch die Realisierung einer oder mehrerer Objektklassen(objectclass) aus. Dabei ermöglichen die Objektklassen dem Element noch verschiedene Attribute zu tragen. Dieses Konzept unterstützt gut die direkte Umsetzung einer rollenbasierten Autorisierung. Verzeichnisdienste stehen heute hinter allen großen Identitätsmanagementsystemen.

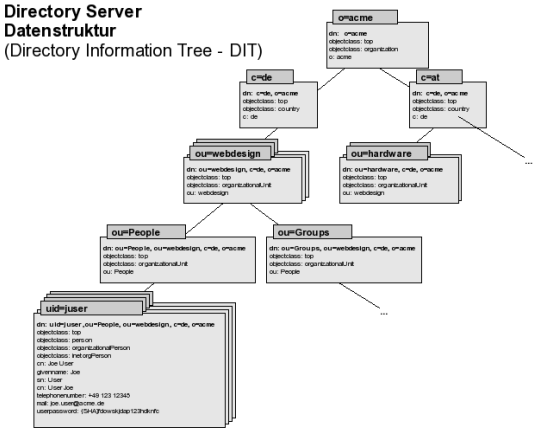

Abbildung 3: LDAP-Verzeichnisdienst

Die bekanntesten Vertreter sind dabei das Microsoft Active Directory, Novells eDirectory und das freie OpenLDAP.

5.2. Verteilte Authentifizierung

Nach der Einführung einer zentralen Identität, welche auf allen Systemen verwendet werden kann, war die Vereinfachung und Zentralisierung der Authentifizierungs-Infrastruktur nur der nächste logische Schritt. Dabei sollte sich der Benutzer nur ein einziges Mal pro Arbeitstag an seinem Rechner anmelden müssen und fortan auf allen vertrauenden Rechner als authentifiziert gelten (Single Sign On; SSO). Zur Erreichung dieses Ziels wurde in den 1980er Jahren am MIT, im Rahmen des Projektes Athena, Kerberos (von Cerberus, griechische Mythologie) entwickelt. Kerberos ist ein Ticket-basiertes Authentifizierungssystem bei dem der Benutzer einem Dienst ein passendes Ticket übermittelt, woraufhin ihm die Nutzung einer Ressource gestattet oder verboten wird (siehe Autorisierung). Dabei wird dem Benutzer nach der ersten Authentifizierung ein so genanntes „Ticket Granting Ticket“ ausgestellt, mit dessen Hilfe er Session Tickets erzeugen lassen kann, ohne sich neu authentifizieren zu müssen. Diese Session Tickets verwendet er nun, bei der Kommunikation mit dem Service bzw. der Ressource. Durch die nur noch einmalige Anmeldung und die durchgehende Verwendung von Verschlüsselung, ermöglicht Kerberos ein sicheres und bequemes Authentifizierungssystem. Kerberos wird heute von allen wichtigen Betriebssystemen von Haus aus unterstützt und ist seit Windows 2000 bzw. unter Mac OS X sogar das Standard-System.

5.3. Role Based Access Control

Durch die zentralisierte Benutzerverwaltung hat sich die Vergabe von Rechten teilweise stark verändert. Diesen Veränderungen Rechnung tragend, wurde die rollenbasierte Rechtevergabe entwickelt. Dabei ist der Gedanke dahinter genauso einfach wie praktisch. Statt den einzelnen Benutzern direkt Rechte zu zuordnen, ordnet man den Benutzern verschiedene Rollen, wie zum Beispiel Sekretärin oder Musketier, zu. Diesen Rollen wiederum gestattet man die Nutzung von Diensten und Ressourcen. Dieses Konzept wird auch direkt durch das Konzept der Objektklassen in LDAP unterstützt, welche neben den Rollenzugehörigkeit auch die nötigen Attribute fordern können.

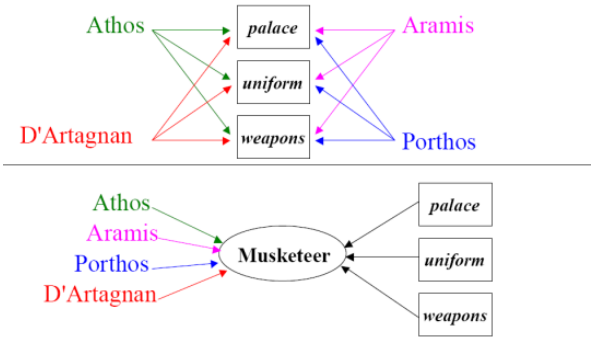

Abbildung 4: Rollenbasierung der Musketiere

6. Wünsche für die Zukunft

Im Internet herrscht leider bis heute der Zustand der Identitätsinseln vor, da bisher der Prozess der Identitätsintegration, wie innerhalb der Organisationen, nicht vollzogen wurde. Dies liegt hauptsächlich an dem Fehlen einer zentralen Instanz. Microsoft Passport war ein Versuch eine zentrale Instanz unter der Herrschaft eines einzelnen Unternehmens zu schaffen und hat die ganze Komplexität der Problematik direkt offenbart. Auf der anderen Seite hat die in Teilbereichen kriminalisierte Nutzung des Internets den Bedarf nach einem verlässigen Identitätsmanagement weiter verstärkt. Auf Basis dieser Entwicklung und der Betrachtung der vorhandenen Identitätssysteme hat James Cameron, Architect of Identity and Access (Microsoft Corp), die „Laws of Identity“ entwickelt:

1. User Control and Consent

2. Limited Disclosure for Limited Use
3. The Law of Fewest Parties
4. Directed Identity
5. Pluralism of Operators and Technologies
6. Human Integration
7. Consistent Experience Across Contexts

Diese beschreiben ein „Identity Metasystem“, welches eben keine konkrete Technologie im Hintergrund hat, sondern eine große Vielfalt von Technologien unterstützen soll(Gesetz 5). Dabei steht der Benutzer, ganz im Sinne des „Identity 2.0“, im Zentrum. So spielt sowohl die Bedienbarkeit (Gesetz 6) als auch die Kontrolle der übermittelten Claims (Gesetz 2) eine wichtige Rolle.

7. Föderierung von Identitäten

Innerhalb bestehender Organisation hat das Konzept der „federated Identities“ viele Anhänger. Föderierte Identitäten bedeutet in diesem Kontext, entweder die virtuelle Integration mehrerer Identitätsmanagement-Systeme oder bezeichnet den Prozess der Benutzeranmeldung über verschiedene IT-Systeme (Wikipedia). Insgesamt werden dabei die Grenzen zwischen den Identitätssilos einzelner Unternehmen aufgeweicht und redundante Datenhaltung vermieden, indem sich die Benutzer der einen Firma auch an Systemen der anderen Firma mit ihren „Heimat-Accounts“ authentifizieren können. Die Hauptmotivation ist dabei die engere Zusammenarbeit von Unternehmen mit Partnern und Sub-Unternehmern. Bekannte Vertreter dieser Kategorie sind Shibboleth und die Active Directory Federation Services.

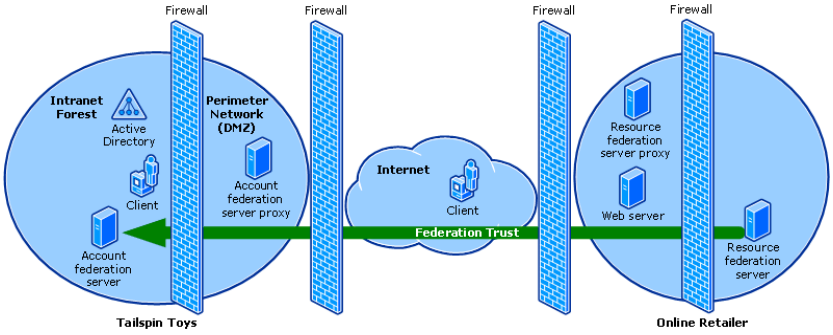

Abbildung 5: federeted Identity mit Active Directory

8. Benutzerzentrisches Identitätsmanagement

Nach Dick Hardts (CEO von Sxip) legendärer Präsentation auf der OSCON 2005 ist der Begriff „Identity 2.0“ wohl in jedem Munde. Aber was ist das „Identity 2.0“? Prinzipiell wird darunter eine benutzerzentrierte Identitätsinfrastruktur für das Internet verstanden, welche den Gedanken der federated Identity weiterführt, die Macht über die Identitäten allerdings in Benutzerhand legt. Im speziellen werden im Folgendem zwei Aspiranten betrachtet, welche sich anschicken den Benutzer bei der Verwaltung seiner Identitäten zu unterstützen und so die „Identity 2.0“ Realität werden zu lassen.

8.1. OpenID

OpenID ist der heute am weitesten verbreitete, dezentrale, föderierte Identity-Provider. Dabei besteht Unterstützung für ein HTTP-basiertes Single Sign-On sowie Integration in Firefox v3 und Vista (durch ein Update). Das besondere an OpenID ist die Einfachheit und die große Freiheit, sowohl technologisch als auch organisatorisch. So kann man seine Identität auf prinzipiell jedem Rechner

hosten und findet auch für die allermeisten Plattformen einsatzbereite, freie Implementierungen. Durch die starke Dezentralisierung des gesamten System ist das Ausscheiden beteiligter Firmen kein Problem und hat nur geringen Einfluss auf das Gesamtsystem: "OpenID does not crumble if any one company turns evil of goes out of business." (Brad Fitzpatrick; Erfinder des LiveJournal). Als typisches Open Source Projekt wurde auch der Entwicklungsprozess sehr offen gestaltet. So kann jeder seine Ideen einbringen und bei der Entwicklung mitarbeiten. Durch diese Offenheit und die Benutzerfreundlichkeit erfüllt OpenID auch alle „Laws of Identity“.

Technologisch basiert OpenID auf URLs, daher jede Identität entspricht einer URL. Diese verweist meistens auf die Website bzw. Blog des Inhabers oder ein Profil in einer Social-Community-Plattform. Mittels Yadis werden dann die zur Authentifizierung notwendigen Informationen, derzeit nur der Authentifizierungsserver (der Identity Provider), bestimmt, woraufhin dieser die Authentizität der Identität bestätigen muss. Hat sich der Benutzer an dem Identity-Provider-Dienst noch nicht angemeldet, so muss er dies nun nachholen. Danach muss der Nutzer noch die Übertragung der Daten gestatten und kann daraufhin den ursprünglich angeforderten Dienst (Relying Party) nutzen.

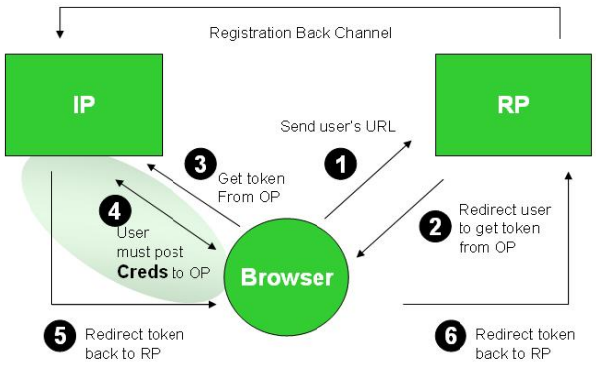

Abbildung 6: OpenID-Architektur

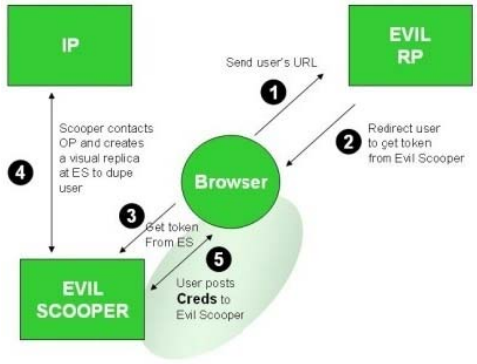

Abbildung 7: Phishing mit OpenID

Aus diesem Aufbau folgt auch direkt der größte Nachteil von OpenID: es ist Anfällig für Phishing-Angriffe. Der Angreifer baut dabei einen bösen Dienstanbieter auf, welcher, statt den Benutzer korrekt weiterzuleiten, den Benutzer auf eine gefälschte Identity-Provider-Seite leitet. Dort meldet sich dann das Opfer an und der Dieb hat alle notwendigen Informationen, und damit die Identität, gestohlen.

8.2. Information Cards

Information Cards ist ein von Microsoft maßgeblich mitentwickelter Teil des Identity Metasystems, welche speziell für die Realisierung der „Laws of Identity“ entworfen wurde. Dabei wurden aus den sieben Regeln vier Design-Ziele formuliert:

- Unterstützung für jedes Identitätsmanagementsystem
- durchgehende Benutzerkontrolle
- Ersatz für Passwörter
- Erhöhung der Benutzerzufriedenheit

Diese Ziele sind zwar hochgesteckt, versprechen aber ein brauchbares System.

Wie werden diese Ziele nun technisch erreicht? Das gesamte Identity Metasystem basiert auf den offenen Standard-Web-Service-Protokollen der WS-Familie. Dabei wird allerdings aus Sicherheitsgründen eine verschlüsselte Kommunikation standardmäßig vorausgesetzt. Um nicht die Ermittlung von Surfgewohnheiten zu ermöglichen, gibt es keine direkte Kommunikation zwischen Identitätsanbieter und Dienstanbieter. Beide kennen nur den Benutzer, welcher damit auch alle ausgetauschten Daten kontrollieren kann. Diese Architektur ist der von OpenID sehr ähnlich. Zusätzlich werden für die Kommunikation mit verschiedenen Dienstanbietern auch verschiedene Kommunikationsschlüssel eingesetzt, sodass auch ein Dienstleister, welcher mehrere Webseiten besitzt, nicht so einfach feststellen kann, ob zwei Benutzer derselben Person entsprechen. Auch die Art in der die Identität vorliegt ist unbeschränkt, so kann das System mit X.509-Zertifikaten genauso gut umgehen, wie mit klassischen Passwörtern. Der große Vorteil liegt bei der Verwendung von Information Cards mit Passwörtern gegenüber normalen Passwörtern in der Abstraktion von dem konkreten Passwort, da der Benutzer nur eine Information Cards auswählt, in der das Passwort enthalten ist. So kann auch Phishing gut verhindert werden, da der Benutzer keine Informationen einfach herausgeben kann: die Information Cards sind nur verschlüsselt übertragbar und die Identität der Gegenseite wird mit Hilfe von High-Assurance-Zertifikaten geprüft. Diese besonderen Zertifikate enthalten dabei mehr Informationen über die Gegenseite, wie zum Beispiel ein Firmenlogo sowie eine Anschrift, und bedürfen einer stärkeren Überprüfung bei der Ausstellung.

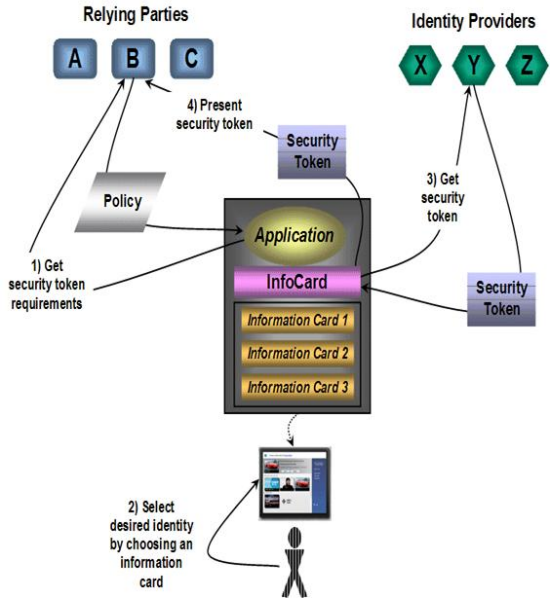

Abbildung 8: Information Cards-Architektur

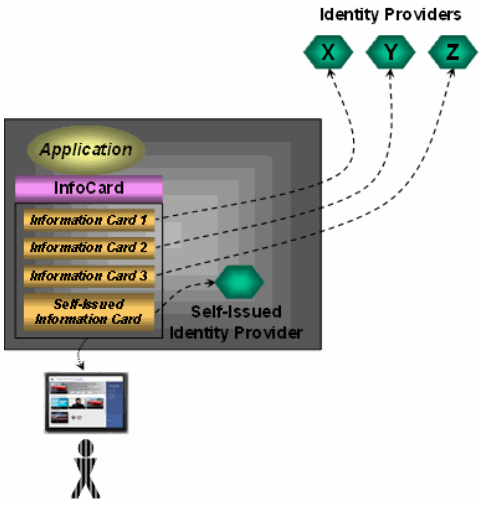

Abbildung 9: Self-issued Identity Provider

Eine Besonderheit hat das Information Cards-Konzept allerdings: so genannte „Self-issued Information Cards“. Diese kann sich der Benutzer selbst ausstellen ohne einen „normalen“ Identity Provider und sollen für Authentifizierung, zum Beispiel, bei Foren genügen, welche nur geringe Ansprüche an die Korrektheit der übermittelten Claims stellen. Dabei ist in der Client-Implementierung ein einfacher Identity Provider eingebaut, welcher diese Information Cards ausstellt. Dies erhöht wiederum die Benutzerzufriedenheit, da es den Aufwand für die Erstellung einfacher Identitäten stark verringert.

9. Fazit

Insgesamt sieht man, dass das Identitätsmanagement schon einen langen Weg seit den Anfängen im rein maschinenzentrierten Account-Management zurück gelegt hat. Mit Verzeichnisdiensten und verteilten Authentifizierungs-Mechanismen ist heute eine stabile Basis für ein sicheres und benutzerfreundliches Identitätsmanagement innerhalb geschlossener Organisationen gegeben. Aber mit den

Möglichkeiten wachsen natürlich, wie überall, die Wünsche. Federated Identity ist hier eine vielversprechende Lösung für die Zusammenarbeit über Firmengrenzen hinweg. Allerdings sind die Identitätsprobleme im Internet teilweise ganz anderer Natur. Besonders die Vielfalt der Identitätsanbieter und Technologien macht eine vernünftige Lösung aufwendig und politisch nicht einfach. Die hier vorgestellten Lösungen sind beide vielversprechend, gehen technisch allerdings meist getrennte Wege. Während OpenID hauptsächlich auf die Authentizität einer Identität ausgelegt ist, konzentriert sich Information Cards auf die Absicherung beliebiger Claims und ist damit allgemeiner, allerdings auch wesentlich komplexer. Die Zeit wird dabei zeigen, welcher Ansatz zum Erfolg führt.

Besonders interessant dabei sind die Integrationsversuche beider Technologien: am OpenID-Identitätsanbieter anmelden mit einer Information Card. Dieser Ansatz macht hoffentlich Schule und die Parteien arbeiten zusammen, anstatt sich in sinnlose Grabenkämpfe aufzubrauchen.

Quellen

- Vorlesung Kommunikationssystem I
- http://(en|de).wikipedia.org
- https://www.prime-project.eu/prime_products/presentations/idmanage-berlin-20060913.pdf
- http://blog.thomasbiesenbach.de/uploads/diverses/SL_biesi_14062007_1_300.jpg
- http://www.opengroup.org/security/heron.pdf
- http://www4.informatik.uni-erlangen.de/ Lehre/SS02/PS_KVBK/talks/folien_guido.pdf
- http://oskorei.motpol.nu/?p=127
- http://www.ericom.com/kerberos.asp
- http://www.identityblog.com/
- http://blogs.zdnet.com/digitalID/?p=78