

Identity Management Identitätskrisen in der IT

Identity Management Systeme könnten die Lösung darstellen, um einen „Identitätskollaps“ bezogen auf zu viele Identitäten/Passwörter, Sicherheitsprobleme und hohe Kosten im Internet zu vermeiden. Dazu bedarf es einer neuen Organisation der Nutzermerkmale und Nutzerdaten, sowie neuer Identifikations- und Authentifikationslösungen. Zusätzlich können so zukünftig neue Geschäftsfelder für unsere Wissens- und Informationsgesellschaft erschlossen werden.

Probleme ergeben sich auf Seiten der Nutzer und der Anbieter. Die Nutzer sind nicht mehr in der Lage, ohne Hilfe ihre stetig wachsende Anzahl von Zugangsdaten (Identifikationen und Passwörter) sicher zu verwalten, und auf der Anwenderseite werden Unmengen an Benutzerdaten doppelt gespeichert oder gehalten, obwohl sie nicht mehr aktiv genutzt werden. Benutzerdaten liegen in verschiedenen Aktualitäten vor und können nicht synchronisiert werden. Wenn keine geeigneten Identity Management Systeme gefunden werden, ist in der Zukunft eine Art Kollaps durch Passwörter, ausufernde Accountmengen, Dateileichen, fehlende Übersicht usw. zu erwarten, verbunden mit einem enorm steigenden Verlust an Sicherheit und an der Nutzung von Diensten. Es steht nicht nur die Lösung vorhandener Probleme im Vordergrund, sondern auch das Erreichen eines Mehrwerts durch höhere Benutzerfreundlichkeit und die Erschließung neuer Geschäftsfelder durch neue integrierbare Technologien, wie zum Beispiel Web Services.

Was ist eine Identität?

Im realen Leben besitzen wir als Person eine eindeutige Identität durch unseren Vornamen, Nachnamen, Geburtstag und Geburtsort die durch die Standesämter verwaltet werden. Überprüft werden, kann unsere Identität durch unseren Personalausweis, der von den Einwohnermeldeämtern gemanagt wird. Wir sind in der realen Welt durch dieses Prinzip eindeutig identifizierbar.

Digitale Identitäten sind Datensätze die Objekte in der IT-Welt repräsentieren. Sie bestehen aus einer Sammlung verfügbarer personen- oder objektbezogener Attribute. In der IT-Welt sind dies zurzeit in der Regel ein Benutzername und ein Passwort. Weitere Attribute dieser Identität sind zum Beispiel Adress- oder Bankdaten.

Diese Objekte sind nicht zwangsläufig natürlichen Personen zugeordnet. Auch juristische Personen, Systemkomponenten (Geräte und Hardwaremodule), Anwendungen

und Services, respektive Webservices, können durch diese Objekte abgebildet werden. Grundsätzlich hat zurzeit jede Person mehrere Identitäten, da die einzelnen Systeme/Dienste voneinander unabhängig betrieben werden.

Entwicklung vom Intranet zum Internet

Innerhalb von Firmen und Organisationen werden Identity Management Systeme bereits vielfach erfolgreich eingesetzt. Sicherheit und Kostenersparnis sind die treibenden Faktoren zum Einsatz solcher Identity Management Systeme. Die größte Menge an Identitäten findet sich jedoch nicht in den Netzen der Firmen und Organisationen sondern im Internet. Außerdem sollten Identitäten nicht nur firmenintern, sondern auch firmenübergreifend genutzt werden können. Es gibt bisher nur wenige Ansätze, die wirklich das Potenzial besitzen, ein Identity Management System für das Internet darzustellen.

RoSI – Return on Security Investment

Selbstverständlich werden Identity Management Systeme nicht nur eingesetzt, um den Benutzern das Leben zu vereinfachen. Abgesehen davon, dass ganz massive Sicherheitsprobleme gelöst werden, bietet sich im Bereich Identity Management ein beträchtliches Return on Investment Potenzial, begründet in der Kostenreduktion, der Produktivitätssteigerung und in der Erhöhung der Sicherheit. Allein für die Kostenreduktion wird nach Angaben der Gartner Group, führender Anbieter in Forschung und Analyse in der globalen IT-Industrie, das Einführen von Identity Management Systemen sinnvoll.

Jede relevante Firma/Organisation betreibt in der Regel ein Helpdesk für ihre Internet- und Intranetressourcen. Diese Helpdesks verwenden einen Großteil ihrer Zeit auf passwortbezogene Anfragen, wie z.B. die Rücksetzung nach vergessenem oder kompromittiertem Passwort. Eine Firma/Orga-

nisation mit 10.000 Anwendern und zwölf Applikationen würde, in einem Zeitraum von drei Jahren rund 3,5 Millionen Dollar sparen, unter der Annahme, dass die IT-Abteilung ca. 14.000 Stunden für Zugangsbelege ihrer Anwender aufbringt, wenn sie eine entsprechende Identity Management Lösung nutzen würden [Gart05]. Dieses Thema wird auch auf dem IT-Security-Forum 2005 der IIR, 08.-10. November 2005, in Frankfurt behandelt.

Ansätze: Microsoft .Net Passport und Liberty Alliance

Identity Management im Internet wird bisher nur von wenigen Systemen unterstützt. Im Folgenden werden zwei unterschiedliche Ansätze beschrieben.

Microsoft schickte das .Net Passport System ins Rennen. Dieses System ist ausschließlich darauf ausgerichtet, ein Single-Sign-On durchzuführen. Single-Sign-On bedeutet eine einmalige Identifizierung und Authentifikation eines Benutzers an einem System, die es erlaubt weitere Dienste, für die der Benutzer berechtigt ist, ohne erneuten Nachweis der Identität, zu nutzen.

Beispielsweise war die Firma „ebay“ Nutzer der Passport-Technologie. Nachdem sich ein User an einem Passport-Server durch Benutzernamen und Kennwort angemeldet hatte, konnte bei „ebay“ mitgesteuert werden, ohne erneut eine Authentifizierung durchzuführen.

Das Passport-System ist bereits im WWW gescheitert und wird nur noch für microsoft-eigene Dienste genutzt. Grund hierfür ist der zentrale Aufbau des Systems, denn die Passport-Server speicherten sämtliche Identitäten und Passwörter der Benutzer. Auch die Weitergabe der Benutzerdaten an angeschlossene Server wurde ohne explizite Zustimmung des Nutzers durchgeführt. Somit konnte das System weder eine ausreichende Vertrauenswürdigkeit noch den Anspruch an ein entsprechendes Sicherheitsniveau erreichen.

Der Ansatz der Liberty Spezifikation ist im Gegensatz zum Microsoft „.Net Passport“

System eine dezentrale Lösung. Das LibertyAlliance Projekt (www.projectliberty.org) ist eine Vereinigung von mehr als 160 Firmen wie AOL, Mastercard, Sun Microsystems, RSA Security, ..., aus der ganzen Welt. Ein so genannter Identity Provider, den sich der Benutzer selber aussuchen kann, speichert dessen Authentifizierungsdaten. Der Benutzer besitzt im Gegensatz zur Passport Technologie die Entscheidungsgewalt über jeglichen Umgang mit seinen Benutzerdaten. Die Weitergabe der Adressinformationen an einen angeschlossenen Service Provider (reiner Dienstanbieter) ist beispielsweise ein Vorgang, der nur vom Benutzer selbst initiiert werden kann.

Die Liberty Alliance Idee basiert auf der Föderation von Benutzer-Accounts. Das bedeutet, dass die angeschlossenen Server nicht die Benutzerdaten untereinander austauschen, sondern lediglich über ein Pseudonym eine Zuordnung der Benutzer-Accounts etabliert wird. Der Benutzer selbst bestimmt, welche Provider einer Identität zugeordnet werden. Dieser Zusammenschluss wird als Circle of Trust bezeichnet. Er beinhaltet mindestens einen Identity Provider. Innerhalb dieses Kreises (Circle of Trust) werden Single-Sign-On-Funktionalitäten und der Austausch von Autorisierungs-, Authentifizierungs- und Benutzerprofil-Informationen in drei Entwicklungsstufen ermöglicht.

Voraussetzung ist ein einheitliches Netzwerk (Circle of Trust) auf Basis der Liberty Alliance Technologie. Die Anbieter müssen sich vertraglich zusammenschließen, um einen gemeinsamen, identischen Standard und klare rechtliche Verhältnisse zu erlan-

gen. Dies bedarf einer pragmatischen Vorgehensweise, um die Ziele schnell und nachhaltig umsetzen zu können [Gebe05].

Beispielprojekt des Instituts für Internet-Sicherheit

Ziel des Beispielprojektes des Instituts für Internet-Sicherheit ist die Umsetzung der ersten Phase der Liberty Alliance Spezifikation, eingeschlossen der Möglichkeit, mittels mobiler Zertifikate, eine starke Authentifizierung durchzuführen zu können. Diese soll durch die Einbindung eines XKMS (XML Key Management Specification) Service [BPP04] und einer angeschlossenen PKI (Public Key Infrastructure) vom Institut angeboten und realisiert werden. Die mobile Speicherung von Zertifikaten wird beispielhaft durch den USB-Token „mIdentity“ der Firma Kobil realisiert.

Der XKMS Server wird im Institut für Internet-Sicherheit betrieben. Einfach ausgedrückt bietet dieser Service durch die Web Services Technologie den gesamten Funktionsumfang einer PKI basierend auf XML. Außerdem ist der Anschluss mehrerer PKIs an einen XKMS Server möglich. Mit Hilfe des XKMS Dienstes können die Zertifikate sehr einfach verifiziert und validiert werden. Zur Anwendung kommt das System auf den Webseiten des Instituts für Internet-Sicherheit und des TeleTrust Vereins. Den autorisierten Besuchern dieser Webseiten soll das System zur Demonstration angeboten werden, um die Vorteile der Liberty Alliance Technologie zu entdecken und eine Sensibilisierung der Nutzer für förderierte Identitäten zu erreichen. Zusätzlich wird die Vorteilhaftigkeit der starken Authentifizierung präsentiert [Linn05].

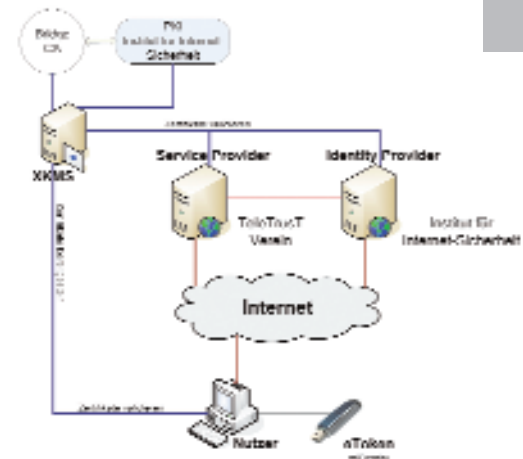


Abbildung 2: Projekt Schema

Identity Management Anwendung im Bereich Automotive

Durch die Verbreitung von Medien und Diensten über das Internet in allen Bereichen des Lebens gewinnt Identity Management in neuen Geschäftsbereichen stark an Bedeutung. Der Bereich Automotive ist ein gutes Beispiel für den sinnvollen Einsatz von Identity Management und im Besonderen der Liberty Alliance Spezifikation.

Das Radio mit Kassettenteil oder CD galt lange Jahre als Begleiter des Autofahrers. Durch neue, schnellere Übertragungstechniken, wie beispielsweise UMTS drängen neue Medien in den Automotiv-Bereich vor. Musikdaten und Radiosender können direkt aus dem Internet geladen werden, ebenso Filme für die Kinder auf der Rückbank oder Navigationsdaten, für das Navigationssystem, um schnell ans Ziel zu gelangen. Voice over IP wäre im Auto ebenso denkbar.

Für Geschäftsleute wäre es möglich Dienste zu etablieren, die durch ein An- und Abmelden bei Fahrtantritt und Fahrende beispielsweise dem E-Mail-Programm des Fahrers ein Signal senden. Dieses Signal könnte beispielsweise veranlassen, dass wichtige E-Mails, die während der Fahrtzeit eintreffen direkt mit der Information beantwortet werden, dass die E-Mail frühestens zum Zeitpunkt X (Fahrende) beantwortet werden kann. Ebenso wäre denkbar, dass die E-Mail dann im Auto vorgelesen wird, da das E-Mail-Programm durch das Signal realisiert hat, dass sich der Fahrer im Auto befindet. Üblicherweise ist eine Anmeldung für jeden einzelnen dieser Dienste

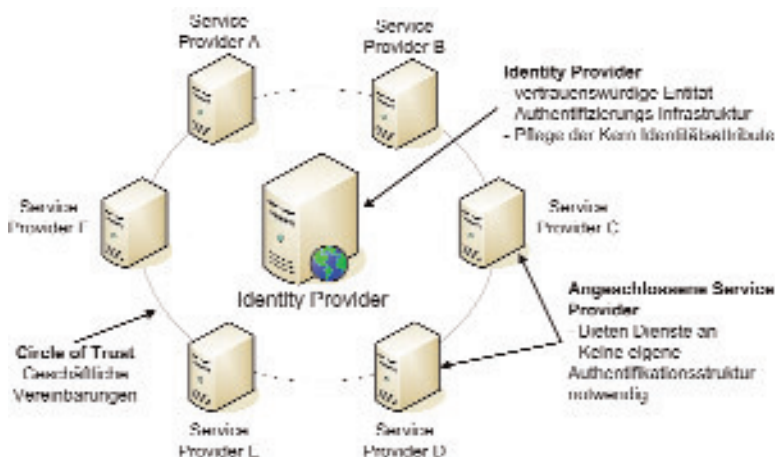


Abbildung 1: Circle of Trust

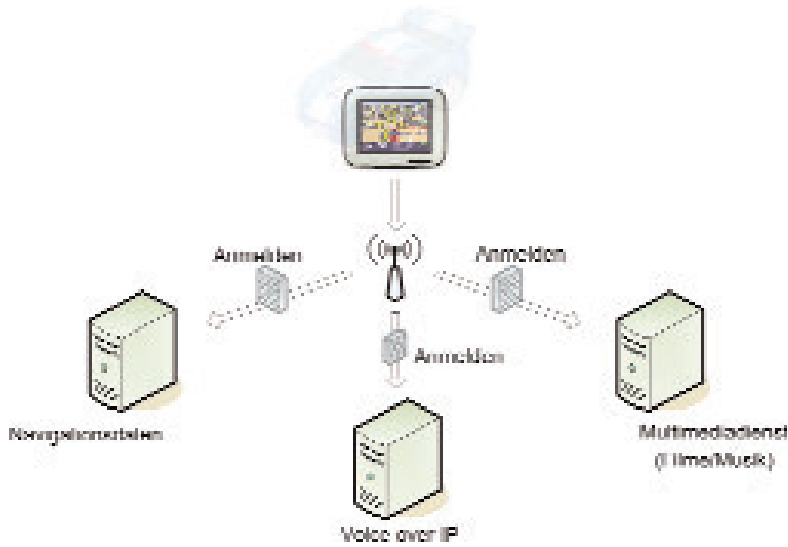


Abbildung 3: Anmeldung an verschiedenen Systemen

notwendig, da sie von unterschiedlichen Anbietern erbracht werden. Abbildung 3 stellt dieses Szenario dar.

Aber wer möchte in sein Auto einsteigen und vor Fahrtantritt erst einmal fünf Authentifizierungsvorgänge mit verschiedenen Daten durchführen? Ideal wäre ein einmaliges Anmelden bei Antritt der Fahrt. An dieser Stelle findet wieder das Identity Management seinen Einsatz. In der dritten Phase der Liberty Alliance Spezifikation finden sich bereits Dienste, die das vorher erwähnte Szenario realisieren.

Die Abbildung 4 zeigt den wünschenswerten Zustand als Liberty Alliance Umsetzung. Die verschiedenen Dienste werden in einem Circle of Trust an eine Identität gebunden.

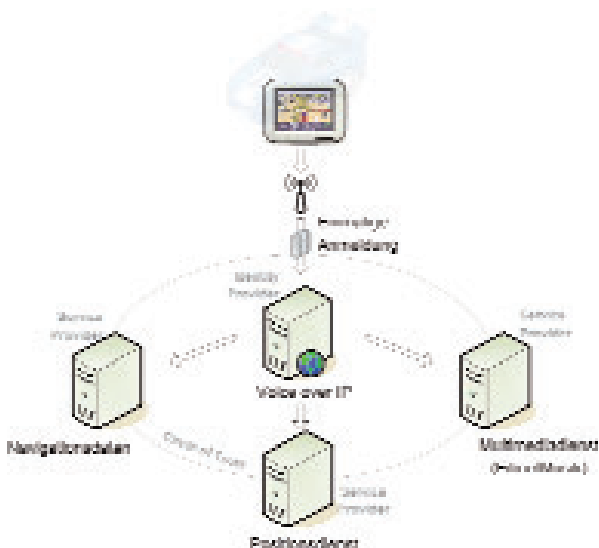


Abbildung 4: Single Sign On über die Liberty Spezifikation

Identity Management ist also nicht nur eine Technologie, um in einem Unternehmen die Arbeit der Administratoren zu erleichtern, Kosten zu sparen oder die Systeme sicherer zu machen. Ganz neue Geschäftsfelder werden erschlossen, hier am Beispiel des Automobilbereiches.

Ausblick

Der Liberty Alliance Ansatz wird vielseitig unterstützt und bietet in der zweiten und dritten Phase der Spezifikation enormes Potenzial für zukunftsorientierte Anwendungen. Allerdings basiert der Ansatz auf Absprachen zwischen den Anbietern. Nur mit deren Bereitschaft zur Kooperation hat die Technologie eine Chance im Internet umfänglich umgesetzt zu werden.

Identity Management ist aufgrund der Entwicklung des Internets und der Bedeutung überbetrieblicher Kommunikation eine unausweichliche Entwicklung, um einen hohen Grad an Sicherheit und eine gleichzeitige Kostenreduzierung zu erreichen. Die zertifikatsbasierte Authentifizierung legt einen Grundstein für sichere Authentifizierungen.

Das Institut Internet-Sicherheit verknüpft das Identity Management System mit neuen Technologien, wie XML Key Management Specifica-

tion (XKMS), Web Services und Trusted Computing.

Durch diese Kombination entstehen neue Geschäftsfelder und die Möglichkeit zukünftige und bereits existierende Anwendungen sicher, vertraulich, kostengünstig und benutzerfreundlich zu gestalten.

Dipl.-Inform. (FH) Markus Linnemann
 markus.linnemann@internet-sicherheit.de
 Prof. Dr. Norbert Pohlmann
 norbert.pohlmann@informatik.fh-gelsenkirchen.de
 Institut für Internet-Sicherheit
 Fachhochschule Gelsenkirchen
 www.internet-sicherheit.de

[BPP04] D. Bär, A. Philipp, N. Pohlmann: „Web Service Security - XKMS“, in „ISSE 2005 - Securing Electronic Business Processes - Highlights of the Information Security Solutions Europe 2004 Conference“, Hrsg.: S. Paulus, N. Pohlmann, H. Reimer, Vieweg-Verlag, Wiesbaden 2004

[Gart05] Network Computing (pm), Roter Teppich ins Netz. Identity- und Access-Management, Network Computing, Heft 18, 2004

[Gebe05] G. Gelel: „Federated Identity: A Progress Report“, in „ISSE 2005 - Securing Electronic Business Processes - Highlights of the Information Security Solutions Europe 2005 Conference“, Hrsg.: S. Paulus, N. Pohlmann, H. Reimer, Vieweg-Verlag, Wiesbaden 2005

[Linn05] M. Linnemann: „Identity Management“, Diplomarbeit, Institut für Internet-Sicherheit, FH-Gelsenkirchen 2005