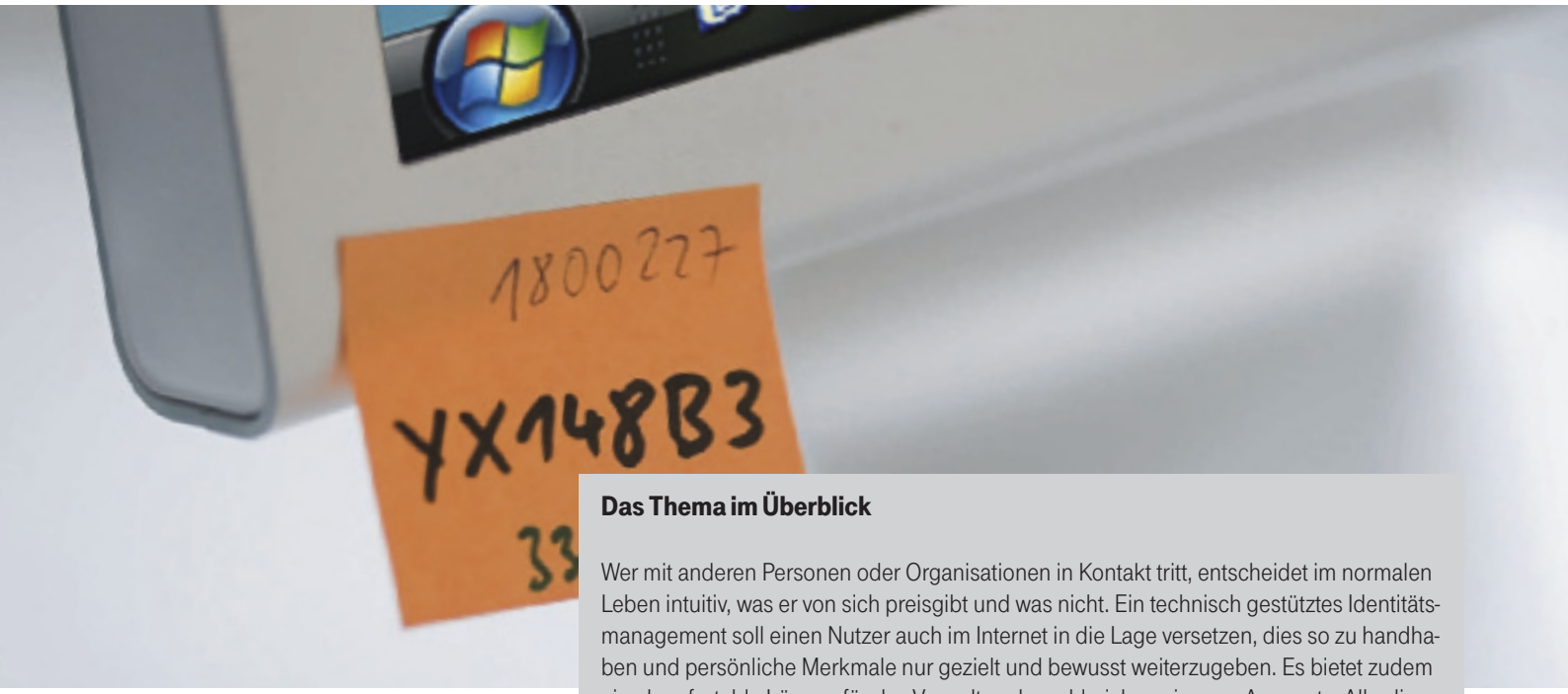
WissenHeute Jg. 61 6/2008



Das Thema im Überblick

Wer mit anderen Personen oder Organisationen in Kontakt tritt, entscheidet im normalen Leben intuitiv, was er von sich preisgibt und was nicht. Ein technisch gestütztes Identitätsmanagement soll einen Nutzer auch im Internet in die Lage versetzen, dies so zu handhaben und persönliche Merkmale nur gezielt und bewusst weiterzugeben. Es bietet zudem eine komfortable Lösung für das Verwalten der zahlreichen eigenen Accounts. Allerdings hängt die System-Akzeptanz der Nutzer von der Benutzerfreundlichkeit und auch vom Vertrauensmodell ab.

Identitätsmanagement – vereinfachte Handhabung von Internet-Zugangsdaten

Fast täglich melden sich Internetnutzer bei neuen Online-Dienstleistern mit den jeweils dort geforderten Zugangsdaten an. Für die Nutzer entsteht dadurch mit der Zeit eine „Sammlung" von Zugangsdaten und Passwörtern, die stetig ergänzt wird und sie immer öfter vor Probleme stellt. So ist es z.B. schwierig, den Überblick zu wahren und vor allem auch die Verwendung der eingegebenen Daten beim Anbieter zu kontrollieren. In diesem Beitrag werden Lösungskonzepte des Identitätsmanagements beschrieben, mit denen die Benutzerfreundlichkeit erhöht und den Nutzern die Kontrolle ihrer persönlichen Daten erleichtert werden.

Die Autoren

Dipl.-Ing. Stefanus Römer ist als Projektleiter für mobile Datendienste bei T-Mobile Deutschland tätig.

Dipl.-Inform. Dietmar Krüger ist als Projektleiter und Senior-Experte im „Overarching AAA" Projektfeld der Deutsche Telekom Laboratories tätig.

Hintergrund

Als Identitätsmanagement (IDM, Identity Management) wird beispielsweise im Online-Lexion Wikipedia[1] der zielgerichtete und bewusste Umgang mit Identität, Anonymität und Pseudoanonymität bezeichnet. Durch die zunehmende Internetvernetzung und die Übertragung vieler Aspekte aus der „realen" Welt in die Online-Welt, hat auch die Frage von bewusster Anonymität und dem bewussten Umgang mit Teilen der eigenen Identität im Internet eine neue und besondere Bedeutung erlangt.

In der sich ausbreitenden digitalen Welt werden für die Anwender viele neue Dienste und Anwendungen verfügbar. So kaufen z.B. schon viele Menschen ganz selbstverständlich im Internet ein. Doch wenn sie die Dienste nutzen wollen, ist es auch notwendig, dass sie den Anbietern dieser Dienste persönliche Daten bekannt geben und sich registrieren. Und bei fast jeder Registrierung werden immer wieder die gleichen persönlichen Daten (z.B. Name, Adresse und Geburtsdatum) erhoben.

Allzu oft werden auch Angaben verlangt, die zur Erbringung der jeweiligen Dienstleistung unerheblich sind. Viele Menschen sind den-

[1] www.wikipedia.de

noch bereit, auf vielen Internetseiten beliebige persönliche Angaben zu machen, ohne genau zu wissen, wer diese Angaben verlangt und zu welchem Zweck sie erhoben werden. Dabei ist es fast unmöglich, den einzelnen Online-Dienstleister bei der Verwendung der registrierten persönlichen Daten zu kontrollieren. Deshalb ist es besonders wichtig, sich die Konsequenzen der Herausgabe seiner Daten in der digitalen Welt bewusst zu machen, beispielsweise die Folgen der

- unbegrenzten Speicherung persönlicher Daten, unabhängig vom ursprünglichen Zweck,
- Erfassung, Auswertung und Weitergabe von Nutzerprofilen sowie der
- nicht autorisierten Weitergabe persönlicher Daten.

Hieraus ergeben sich die Anforderungen der Nutzer an den Umgang mit ihren Identitäten im Internet: Sie möchten sich nicht mehr bei jedem neuen Online-Anbieter einzeln und mit immer den gleichen Daten registrieren. Sie wollen sich zudem möglichst zu Beginn einer Internet-Sitzung einmalig anmelden und danach ohne jede weitere Anmeldung alle ihre registrierten Dienste sofort nutzen können (Single Sign On). Sie möchten auch nicht mehr persönliche Informationen preisgeben, als unbedingt erforderlich sind. Sie wollen zudem jederzeit die volle Kontrolle über ihre eingegebenen Daten haben und jederzeit bestimmen, an wen sie herausgegeben werden und was damit geschieht. Das Ziel ist es daher, ein technisch gestütztes Identitätsmanagement einzurichten, das diese Ansprüche der Nutzer erfüllt.

Bisher bietet das Internet hierzu keine einheitliche Lösung. So besteht oft keine Möglichkeit der gegenseitigen Identifizierung der Kommunikationsteilnehmer und für die Nutzer auch keine umfassende Kontrolle der weiteren Verwendung ihrer persönlichen Daten. Mit der Zeit hat sich eine unüberschaubare Zahl verschiedenartiger und proprietärer Insellösungen zur Registrierung und Authentisierung[2] herausgebildet, die die Interessen der Nutzer jedoch selten hinreichend berücksichtigen. Zudem bieten sie nicht immer ausreichenden Schutz vor kriminellen Angriffen oder Missbrauch. Inzwischen haben sich jedoch verschiedene Konzepte und Standards von Anbietern herausgebildet, die Abhilfe anbieten können. Ein mögliches Anwendungsszenario sieht beispielsweise wie folgt aus:

- Nutzer A verbindet seinen Laptop mit dem Internet und besucht die Startseite seiner Bank.
- Sobald er sich anmelden möchte, wird er jedoch zunächst automatisch auf die Login-Seite seines IDM-Dienstleisters geleitet, um sich dort mit seinen Zugangsdaten zu authentisieren.
- Das IDM überprüft die Zugangsdaten und leitet den Browser dann zurück zu der Bankseite, wo der Nutzer A direkt auf seiner persönlichen Startseite landet. Dort kann er dann sofort seine Bankgeschäfte erledigen.
- Anschließend möchte der Nutzer A den aktuellen Stand seiner Online-Auktionen bei eBay verfolgen und wechselt zu seiner persönlichen Mein-eBay-Startseite. Statt sich nun erneut authentisieren zu müssen, erhält er sofort Einblick in seine laufenden Auktionen. Dies ist möglich, weil sich im Hintergrund der eBay-Server und das IDM, ohne weitere Interaktion mit dem Nutzer, über die bereits gültige Authentisierung ausgetauscht haben.

Die zurzeit bestehenden Konzepte und Standards solcher IDM-Systeme werden im Folgenden genauer beschrieben.

Begriffe

Der wichtigste Begriff des IDM ist der der **Netzidentität**. Die Fachwelt definiert den Begriff – nach Liberty Alliance – als Menge aller Attribute der verschiedenen Benutzerkonten (Accounts) eines Nutzers. Ein **Attribut** ist dabei eine Eigenschaft, die ein Nutzer während der Registrierung bei dem jeweiligen Service Provider (**SP**) in seinem Benutzerkonto angibt. Es obliegt dem Service Provider, die einzelnen Attribute im Rahmen des Registrierungsprozesses auf ihre Gültigkeit zu überprüfen. Zurzeit sind die Netzidentitäten der Nutzer mit vielen Unstimmigkeiten und Doppelangaben über das gesamte Internet verstreut und werden nur durch die Nutzer selbst zusammengehalten.

Eine **Teilidentität** (oder Pseudonym) ist abhängig vom Kontext[3], in dem sie benötigt wird und entspricht heute der Teilmenge der Attribute, die in einem der vielen verschiedenen Benutzerkonten enthalten sind. Es wird unterschieden in

- omni-direktionale Teilidentitäten, die in jedem Kontext gültig sind (z.B. universell einsetzbare benutzerzentrische Kennungen wie OpenID), und
- uni-direktionale (gerichtete) Teilidentitäten, die nur in einem einzigen Kontext genutzt werden können (z.B. providerzentrische Kennung wie im Online-Handel bei eBay oder innerhalb eines Unternehmensnetzes).

Von großer Bedeutung ist im IDM auch der Begriff der **Reputation**. Die Reputation gibt Auskunft über die Glaubwürdigkeit eines Nutzers. Sie kann entweder implizit[4] an die jeweilige Teilidentität gebunden sein oder als explizite[5] Kenngröße angeben werden, wie z.B. in Form von Bewertungen durch andere Nutzer. Die Reputation wird zunehmend wichtiger für die Benutzerautorisierung. Sie dient dazu, in Abhängigkeit vom jeweiligen Wert einem Nutzer bestimmte und besondere Rechte einzuräumen. Beispielsweise können eBay-Nutzer ab der zehnten positiven Bewertung durch andere Nutzer ihre Waren auch ohne Versteigerung im Sofortkauf anbieten.

Eine eher theoretische Möglichkeit, zu einer integrierten (umfassenden und einzigen) Netzidentität zu gelangen, ist die Verknüpfung

[2] Siehe hierzu den Beitrag „Authentifizierung, Autorisierung und Accounting in IP-Netzen“, WissenHeute Nr. 5/2005, S. 232 ff.

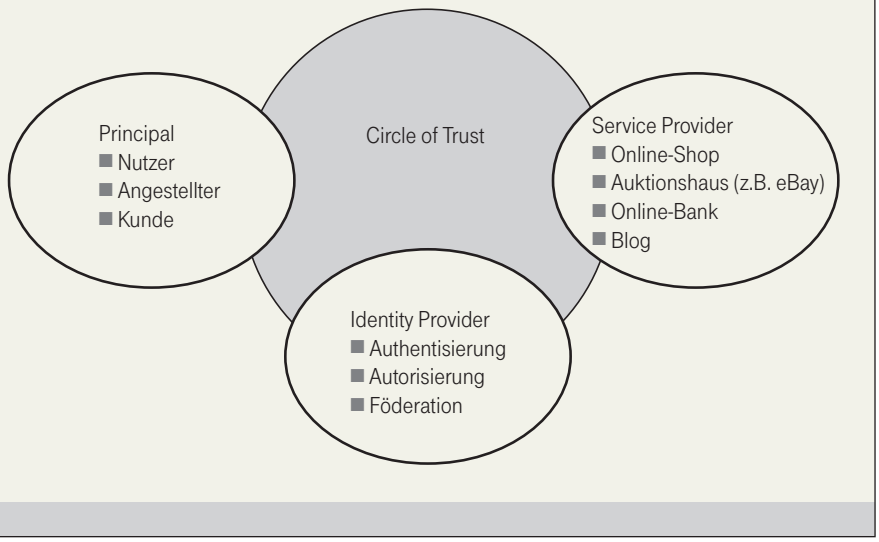
[3] **Kontext:** Der inhaltliche (Gedanken-, Sach-)Zusammenhang, in dem eine Äußerung steht, und der Sach- und Situationszusammenhang, aus dem heraus sie verstanden werden muss.

[4] **implizit:** mit enthaltend, mit gemeint, aber nicht ausdrücklich gesagt.

[5] **explizit:** ausdrücklich, deutlich.

der einzelnen Teilidentitäten eines Nutzers. Die technische Verknüpfung verschiedener Teilidentitäten wird als **Föderation** bezeichnet. Eine vollständige Föderation der Teilidentitäten eines Nutzers stellt auf Grund der hohen Zahl von Service Providern ein technisches und organisatorisches Problem dar. Die Föderation von Identitäten zwischen Service Providern erfordert, dass ein konkretes geschäftliches Interesse an der Zusammenarbeit und eine entsprechende vertragliche Grundlage bestehen. Kooperierende Service Provider verwenden deshalb in der Regel einen gemeinsamen Identity Provider (**IDP**) zur Verwaltung der gemeinsam benötigten Identitäten.

Bild 1 **Circle of Trust**



Service Provider und Identity Provider bilden dabei einen so genannten „Circle of Trust". Ein **Circle of Trust** ist eine Gruppe von Service Providern und Identity Providern, die sich gegenseitig hinsichtlich der Authentisierung und Autorisierung von Nutzern vertrauen (Bild 1).

Der Circle of Trust kann darüber hinaus auch für den Austausch von Identitätsmerkmalen in Form von Attributen genutzt werden. So kann ein Service Provider innerhalb des Circle of Trust zu einem Nutzer, der durch den zugehörigen Identity Provider authentisiert wurde, weitere Attribute abfragen (z.B. Nachname oder Anschrift). Die Informationen werden mit Hilfe so genannter **Security Tokens** ausgetauscht. Diese Security Tokens werden auch zum Austausch von Informationen über den Authentisierungs- oder Autorisierungsstatus verwendet.

Universell verfügbares IDM

Obwohl in vielen Fällen eine universell verfügbare Netzidentität wünschenswert wäre, ist nicht davon auszugehen, dass sich ein einziges weltweites IDM-System herausbilden wird oder eine einzige digitale Identität für jeden Kontext ausreichen wird.

Bereits vorhandene digitale Identitäten sind für jedes Unternehmen auch wichtige Größen. Es wird wahrscheinlich kein Unternehmen bereit sein, seine Bestandsdaten einem zentralen IDM-System, und damit anderen Unternehmen, zur Verfügung zu stellen.

Wie in der „realen" Welt wird es deshalb auch in der Online-Welt abhängig vom jeweiligen Kontext weiterhin unterschiedliche Teilidentitäten geben. Statt eines einzigen zentralen Systems mit einer universellen Identität müssen die Konzepte in Richtung eines Identitäts-Metasystems gehen (ein System von Systemen wie Microsoft es im Identity Metasystem beschrieben hat), das die einzelnen IDM-Systeme mit ihren Teilidentitäten und die Service Provider über standardisierte Schnittstellen lose miteinander verbindet (Loosely Coupled) und nach außen einen universellen Service anbietet.

Anforderungen

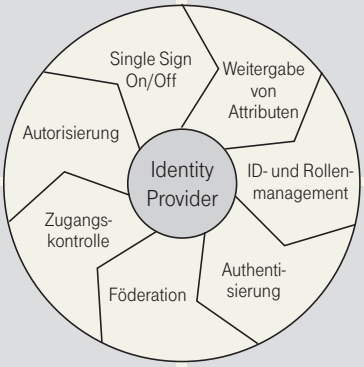
Die Grundlage der Anforderungen für ein benutzerzentriertes IDM-Metasystem bilden die folgenden „Sieben Gesetze des Identitätsmanagements[6]" (Seven Laws of Identity) von Kim Cameron[7]. Sie haben in der Fachwelt weite Akzeptanz gefunden:

- Zentrale Nutzerkontrolle (User Control and Consent): Der Nutzer muss jederzeit die volle Kontrolle über seine persönlichen Daten und deren Verwendung behalten.
- Minimalprinzip bei der Preisgabe persönlicher Daten: An einen Service Provider werden nicht mehr Informationen weitergeben, als zur Erbringung der geforderten Dienstleistung unbedingt erforderlich sind.
- Berechtigung: Persönliche Daten werden nur an berechtigte Parteien (Justifiable Parties) weitergegeben.
- Unterstützung von omni- und uni-direktionalen Teilidentitäten (Directed Identity): Ein IDM muss abhängig vom jeweiligen Zusammenhang spezielle Teilidentitäten unterstützen.
- Offene Schnittstellen (Pluralism of Operators and Technolgies): Ein weltweites IDM-Metasystem wird nur Akzeptanz finden, wenn es auf offenen Standards aufbaut und die Integration verschiedener Technologien und IDP ermöglicht.
- Benutzerintegration (Human Integration): Um ein hohes Sicherheitsniveau zu erzielen, ist es unerlässlich, Mechanismen zu finden, um in jeder Situation eine eindeutige Kommunikation zwischen IDM-System und Nutzer zu ermöglichen.
- Einfache und konsistente Nutzererfahrung (Consistent Experience Across Contexts): Der Nutzer benötigt eine einfache, intuitive und gleichbleibende Nutzerschnittstelle.

[6] http://blues.inf.tu-dresden.de/prime/EUT_Tutorial_V0/german/german/PRIME_nm.htm

[7] **Cameron:** Amerikanischer Softwarearchitekt für Identitäts- und Zugriffslösungen bei Microsoft. Startete auf seinem Blog eine Diskussion über die von ihm so bezeichneten „Identitätsgesetze".

Bild 2 **Dienste eines Identity Providers**



ID Identity

Bild 3 **Sicherheitsanforderungen an IDM-Systeme**

	Inhalt der Kommunikation	Kontext der Kommunikation
unberechtigter Zugriff auf Informationen	■ Vertraulichkeit ■ Verschleierung	■ Anonymität ■ Unverbindbarkeit (Unlinkability) ■ Unbeobachtbarkeit
unberechtigte Veränderung von Informationen	■ Datenunversehrtheit (Integrität)	■ Verantwortlichkeit, Haftung
unberechtigter Entzug von Ressourcen	■ Verfügbarkeit	

Quelle: Deutsche Telekom Laboratories

Funktionen eines IDP

Typische Grundfunktionen eines IDP sind:

- Nutzerauthentisierung mit unterschiedlichen Authentisierungsverfahren: Beispielsweise ist ein automatisches Login auf Grundlage des genutzten Zugangsnetzes oder mit Hilfe von Benutzername und Kennwort möglich.
- Single Sign On/Off: Über ein Sitzungsmangement wird sichergestellt, dass sich der Nutzer zu Beginn einer Internet-Sitzung nur einmal anmelden muss und danach innerhalb dieser Sitzung ohne erneutes Anmelden unterschiedliche Dienste desselben Circle of Trust nutzen kann. Sobald sich der Nutzer bei einem der Service Provider innerhalb des Circle of Trust abmeldet, wird gleichzeitig die gesamte Sitzung beendet (Single Sign Off oder Global Logout).
- Nutzerautorisierung: Aufbauend auf bestimmten Attributen (z.B. Reputation oder Alter) eines Nutzers werden ihm besondere Rechte bei der Dienstnutzung eingeräumt.
- Kontextabhängiges Rollenmanagement basierend auf Teilidentitäten: Entsprechend des Minimalprinzips kann der Nutzer kontextabhängig Teilidentitäten oder Pseudonyme festlegen, die außerhalb des jeweiligen Kontextes keine Rückschlüsse auf seine wahre Identität oder sein Nutzerverhalten ermöglichen.
- Föderation von Teilidentitäten: Innerhalb desselben Circle of Trust kann der Nutzer Teilidentitäten weiterer Service Provider mit seiner Netzidentität föderieren.
- Weitergabe von Attributen an verschiedene Dienste: Der Nutzer kann festlegen, welche Attribute (z.B. Alter und Geschlecht oder Reputation) innerhalb des Circle of Trust zwischen den Service Providern weitergegeben werden können.

Ein Beispiel zu den angebotenen Diensten eines Identity Providers ist in Bild 2 dargestellt.

Sicherheitsanforderungen

Ein IDM-System muss ein hohes Sicherheitsniveau bieten, denn der Zugriff auf Netzidentitäten ist in vielfacher Hinsicht besonders kritisch und ein lohnendes Angriffsziel für einen Missbrauch. Folgende Sicherheitsanforderungen (Bild 3) sind daher zu erfüllen:

- **Vertraulichkeit**
  Es muss sichergestellt sein, dass Unbefugte weder auf die gespeicherten Daten zugreifen können, noch während einer Datenübertragung einen Zugriff auf persönliche Daten erhalten. Dies umfasst insbesondere einen Schutz vor Phishing[8] und Identitätsdiebstahl.
- **Integrität**
  Daten dürfen während einer Datenübertragung nicht verfälscht werden können (Datenunversehrtheit).
- **Verfügbarkeit**
  Benötigte Ressourcen müssen einem autorisierten Nutzer unabhängig vom genutztem Endgerät und Zugangsnetz (Device Agnostic) jederzeit zur Verfügung stehen.
- **Anonymität**
  Ein Nutzer kann eine Ressource oder einen Dienst in Anspruch nehmen, ohne seine Identität preisgeben zu müssen.
- **Unverbindbarkeit (Unlinkability)** durch Nutzung von **Pseudonymity**
  Eine mehrfache Nutzung der gleichen Ressource oder des gleichen Dienstes kann durch das genutzte System nicht in Verbindung gebracht werden.
- **Unbeobachtbarkeit**
  Ein Nutzer kann eine Ressource oder einen Dienst in Anspruch nehmen, ohne dass andere bemerken, dass diese Ressource oder dieser Dienst genutzt wird.

[8] **Phishing:** Das Stehlen von Kontodaten, speziell über gefälschte Bank-Webseiten und E-Mails. Siehe hierzu den Beitrag „Computerviren – vom Ärgernis zur ernsthaften Bedrohung“, WissenHeute Nr. 8/2004, S. 420 ff.

- **Verantwortlichkeit** (Accountability, Legal Enforcement)
  Keine der an einer Transaktion beteiligten Parteien darf im Nachhinein ihre Beteiligung an der betreffenden Transaktion erfolgreich abstreiten dürfen. Ein IDM-System muss die Möglichkeit bieten, in bestimmten Fällen die Anonymität eines Nutzers aufzuheben, um eine Strafverfolgung zu ermöglichen.

Klassifizierung

Digitale IDM-Systeme werden schon seit den 1980er Jahren genutzt. Sie werden immer dann eingesetzt, wenn es darum geht, den Zugang zu kritischen informationstechnischen Ressourcen, z.B. Rechner, Daten oder Anwendungen, zentral zu kontrollieren. Die Deutsche Telekom Laboratories haben im Rahmen der so genannten IDM & AAA Referenzarchitektur (Identity Management & Authentisierung, Autorisierung und Accounting) eine Übersicht über wichtige IDM-Konzepte erstellt (Bild 4). Die Unterscheidungsdimensionen sind der Gültigkeitsbereich und die Verfügbarkeit:

- **Provider-zentrische** IDM-Systeme verwalten ausschließlich Identitäten für einen begrenzten Gültigkeitsbereich (z.B. innerhalb eines Unternehmensnetzes oder eines Circle of Trust).
- **Benutzer-zentrische** IDM-Systeme stellen den einzelnen Nutzer in den Mittelpunkt – und zwar unabhängig vom jeweiligen Kontext oder von einem bestimmten Service Provider. Sie sind universell verfügbar, sofern die Service Provider die jeweiligen Benutzer-zentrischen IDM-Systeme akzeptieren.

Provider-zentrische IDM-Systeme:
Das klassische Konzept, wie es üblicherweise in Unternehmensnetzen zum Einsatz kommt, beruht auf einem netzinternen Domain-Controller, der zentral alle Anmeldungsvorgänge bearbeitet und den einzelnen Nutzern bestimmte Berechtigungen zuweist (Bild 5). Ein typisches Beispiel ist die Anmeldung an einem Unternehmensnetz und der anschließende Zugriff auf den zentralen Mailserver (z.B. Microsoft Exchange) ohne wiederholte Anmeldung.

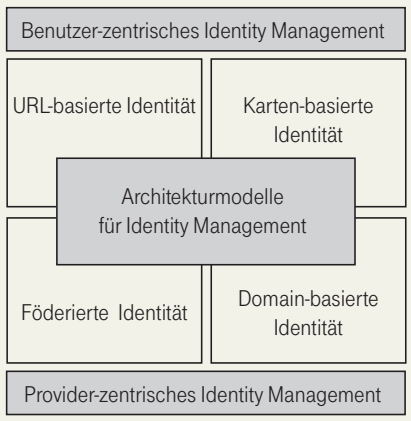
Zur Klasse der Provider-zentrischen IDM-Systeme zählen auch föderierte Multi-Domain IDM-Systeme verschiedener Identity Provider (Bild 6). Beispiele für solche Systeme sind Föderationen nach Liberty Alliance ID-FF (Identity Federation Framework) oder SAML (Security Assertion Markup Language) der OASIS (Organization for the Advancement of Structured Information Standards). Solche Systeme zeichnen sich durch einen Circle of Trust aus, der den Gültigkeitsbereich der föderierten Identitäten festlegt. Innerhalb dieses Bereiches akzeptiert jeder Provider alle Nutzerauthentisierungen, die durch die anderen Provider vorgenommen werden.

Das IDM-Konzept des Liberty Alliance Projects ist in der Fachwelt wegweisend und wesentliche Elemente des Ansatzes wurden von anderen IDM-Konzepten übernommen. Daher wird das Konzept des Single Sign On mit HTTP-Redirect (Hypertext Transfer Protocol) im Folgenden anhand eines einfachen Nutzungsszenarios beispielhaft vorgestellt. Die Voraussetzungen für die Nutzung eines IDM-Systems nach Liberty Alliance sind:

- Bestehender Circle of Trust zwischen Service Provider und Identity Provider.
- Erfolgreiche Föderierung der Zugangsdaten beim Service Provider und Identity Provider durch den Nutzer.

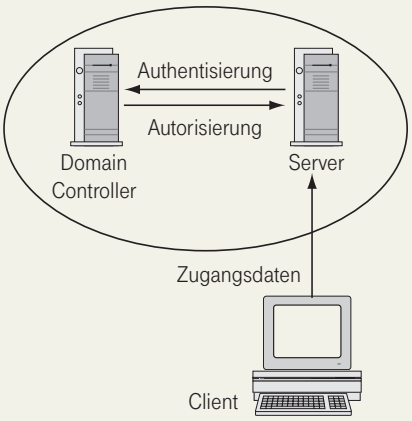
Ein Circle of Trust basiert auf einer geschäftlichen Vereinbarung zwischen SP und IDP und legt unter anderem die technische Schnittstelle fest, wonach z.B. die Security Tokens der Nutzer während des Anmeldevorgangs ausgetauscht werden. Um die Zugangsdaten des IDP auch für die Anmeldung beim SP nutzen zu können, muss der Nutzer zuvor einmalig beide Benutzerkonten miteinander föderieren. Hierzu meldet er sich zunächst bei seinem IDP an, wählt die Option zur Föderation mit weiteren SP aus dem Circle of Trust und authentisiert sich schließlich mit den Zugangsdaten des betreffenden SP.
Es folgt ein Beispiel, in dem ein Anmeldevorgang über den IDP mit Hilfe von HTTP-Redi-

Bild 4 Klassifizierung von IDM-Systemen



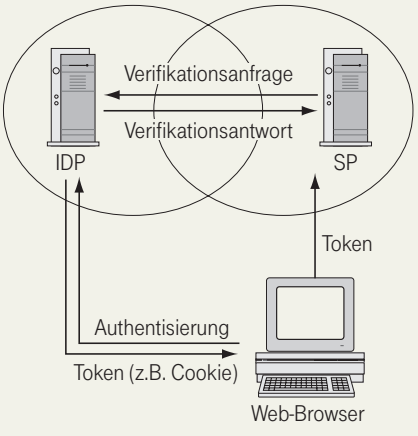
URL Uniform Resource Locator
Quelle: Deutsche Telekom Laboratories

Bild 5 Domain-basiertes IDM



Quelle: Deutsche Telekom Laboratories

Bild 6 Föderierte Multi-Domain IDM-Systeme



IDP Identity Provider
SP Service Provider
Quelle: Deutsche Telekom Laboratories

Bild 7 **Benutzerauthentisierung mit Web-Redirection über den Browser**

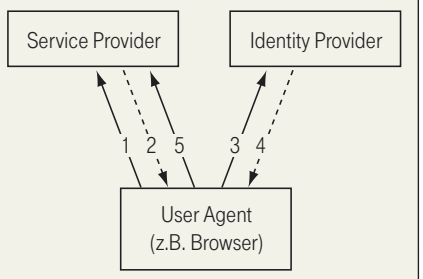
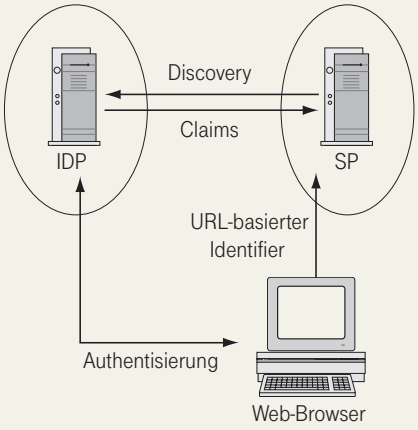
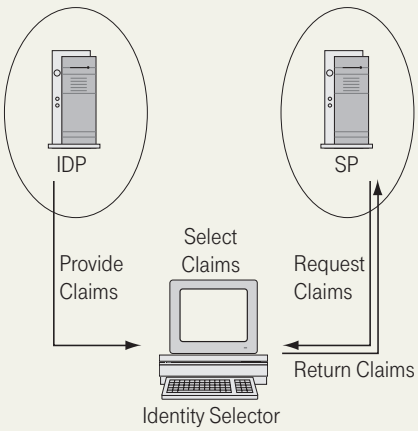


Bild 8 **URL-basierte IDM-Systeme**



IDP Identity Provider
SP Service Provider
URL Uniform Resource Locator
Quelle: Deutsche Telekom Laboratories

Bild 9 **Kartenbasierte IDM-Systeme**



IDP Identity Provider
SP Service Provider
Quelle: Deutsche Telekom Laboratories

rect vorgestellt wird. Die Technik des HTTP-Redirect wird genutzt, um über den Browser des Nutzers einen Kommunikationskanal zwischen IDP und SP bereitzustellen. Das Verfahren ist auch in Bild 7 dargestellt:

- Der Nutzer gibt die URL (Uniform Resource Locator) des gewünschten SP in seinem Browser ein (1).
- Der SP antwortet mit einer HTTP-Redirect-Nachricht unter Angabe einer neuen URL des IDP und einer Rücksprung-URL auf die personalisierte Startseite des jeweiligen Nutzers (2).
- Der Browser sendet automatisch eine HTTP-Anfrage zur vom SP in Schritt 2 angegebenen URL und landet auf einer Anmeldeseite des IDP, wo der Nutzer aufgefordert wird, seine Zugangsdaten einzugeben. Mit dieser HTTP-Anfrage wird gleichzeitig die Rücksprung-URL des SP geliefert (3).
- Bei erfolgreicher Authentisierung leitet der IDP mit einem HTTP-Redirect den Browser über die Rücksprung-URL. Gleichzeitig wird auf dem Rechner des Nutzers ein Session-Cookie mit einer Session-Nummer oder -Handle abgelegt, das auf eine aktive Nutzer-Sitzung auf Seiten des IDP referenziert und somit ein Single Sign On ermöglicht (4).
- Der Browser sendet automatisch unter Angabe der Session-Nummer eine HTTP-Anfrage zur vom IDP in Schritt 3 angegebenen Rücksprung-URL (5), wo der Nutzer seine persönliche Startseite wiederfindet. Anhand der Session-Nummer kann der SP über eine direkte Schnittstelle zum IDP das Ergebnis der Authentisierung überprüfen und gegebenenfalls weitere Nutzerattribute erfragen.

Wechselt der Nutzer nach einer erfolgreichen Anmeldung den Service Provider, indem er z.B. vom Webservice seiner Bank zu eBay geht, erkennt das IDM-System anhand des Session-Cookies automatisch, dass bereits eine aktive Session besteht. Statt dem Nutzer erneut eine Login-Seite anzuzeigen, wird sein Browser sofort zur jeweiligen Rücksprung-URL des neuen Service Providers umgeleitet.

Benutzer-zentrische IDM-Systeme

Wichtige Benutzer-zentrische IDM-Systeme sind URL-basierte Systeme, z.B. das aus der OpenSource-Bewegung stammende und immer häufiger genutzte OpenID (Bild 8), oder kartenbasierte IDM-Systeme (z.B. Cardspace von Microsoft). Das OpenID ist ein dezentrales Verfahren zur Nutzer-Authentisierung für Internet-Dienste. Dabei legt der Nutzer einmalig bei einem OpenID-Provider ein Benutzerkonto an, das anschließend über eine bestimmte URL verfügbar ist. Sobald ein Nutzer einen Internet-Dienst aufruft, der das Verfahren nach OpenID unterstützt, und dort seine OpenID-Kennung eingibt, wird sein Browser automatisch auf seine korrespondierende URL umgeleitet, wo die eigentliche Authentisierung vorgenommen wird. Bei einer positiven Authentisierung wird sein Browser anschließend automatisch wieder zurückgeleitet.

Die Idee bei Microsoft Cardspace (Bild 9) besteht darin, das Konzept der Identitätskarten aus der realen Welt in die Online-Welt zu übertragen. Statt Kundenkarten, Kreditkarten oder Ausweisen stehen dem Nutzer in einer speziellen Anwendung von Microsoft (Cardspace) unterschiedliche virtuelle Identitätskarten verschiedener IDP zu Verfügung. Mit jeder virtuellen Identitätskarte zertifiziert der IDP eine Teilidentität zusammen mit zugehörigen Attributen. Wenn der Nutzer nun einen Internet-Dienst in Anspruch nehmen möchte, kann er, ähnlich wie in der realen Welt, aus der Liste der akzeptierten Identitätskarten auswählen, mit welcher er sich ausweisen möchte. Sofern er sich für den jeweiligen Dienst authentisieren muss, geht in einer gesicherten Umgebung innerhalb des Betriebssystems Windows Vista automatisch ein neues Pop-up-Fenster auf, in dem alle akzeptierten persönlichen Identitätskarten angezeigt werden. Wenn der Nutzer eine Karte auswählt, wird vom zugehörigen IDM-Provider ein verschlüsseltes Security Token mit den entsprechenden Attributen (z.B. Name und Adresse) generiert und dem Nutzer angezeigt. Sofern er der Weitergabe dieser Attribute zustimmt, wird das Security Token an den gewünschten Dienst (Relying Party) geschickt und der Nutzer kann den Dienst starten.

Der Vorteil eines Benutzer-zentrischen IDM-Konzeptes ist, dass der Nutzer seine Teilidentitäten an zentraler Stelle auf seinem Rechner selber verwalten und im Rahmen einer vorgegebenen Auswahl frei entscheiden kann, mit welcher Identitätskarte er sich im Einzelfall ausweisen möchte. Damit hat er innerhalb gewisser Grenzen die freie Entscheidung, welche Teilidentität er mit welchen Informationen von sich preisgeben möchte.

Microsoft Cardspace ist ein so genannter Identity Selector für Microsoft Windows mit einer intuitiven Benutzeroberfläche. Das zu Grunde liegende Konzept baut auf offenen Standards auf, so dass auch andere Hersteller kompatible Identitätsselektoren für ihre Betriebssysteme erstellen können.

Ausblick

Obwohl provider-zentrische IDM-Modelle wie beispielsweise von Liberty Alliance seit vielen Jahren bekannt sind und sich grundlegende Mechanismen, z.B. HTTP-Redirect, durchgesetzt haben, blieb ihre Anwendung bisher auf wenige, isolierte Organisation begrenzt. Neue, benutzerorientierte IDM-Modelle (z.B. OpenID und Cardspace) erfordern demgegenüber keine enge Kooperation zwischen verschiedenen Organisationen und haben daher das Potenzial, sich als universelles IDM zu verbreiten.

Anbieter von Telekommunikationsdiensten sind auf Grund ihres umfassenden Marktzugangs, ihrer vorhandenen Authentisierungsmöglichkeiten und ihres engen Vertrauensverhältnisses zu ihren Kunden in besonderer Weise geeignet, sich als IDM-Anbieter zu positionieren. Das Vertrauen der Nutzer ist eine wichtige Grundlage eines IDM und somit ein Alleinstellungsmerkmal, das man nicht kaufen kann. Besonders für Mobilfunknetzbetreiber ist es von besonderem Interesse, die vorhandene SIM-Karte (Subscriber Identity Module) ihrer Kunden als universelles Authentisierungsmittel einzuführen.

Vor dem Hintergrund der rasanten Entwicklung in Richtung Web 2.0[9] wird es zunehmend wichtig, webbasierte Authentisierungsverfahren dahingehend zu unterstützen, dass netzbasierte Authentisierungen im Rahmen sicherer Multifaktor-Authentisierungen im Internet mitgenutzt werden können. Nur so kann die aktuelle Situation verbessert und eine Zunahme der Betrugs- und Missbrauchsdelikte verhindert werden, die das Vertrauen in das wichtige Medium Internet grundlegend erschüttern würde. *(J)*

Verwendete Abkürzungen

HTTP	Hypertext Transfer Protocol
ID-FF	Identity Federation Framework
IDM	Identity Management
IDP	Identity Provider
OASIS	Organization for the Advancement of Structured Information Standards
SAML	Security Assertion Markup Language
SIM	Subscriber Identity Module
SP	Service Provider
URL	Uniform Resource Locator

Internetadressen

www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf

www.prime-project.eu/prime_products/whitepaper/

www.projectliberty.org/resource_center/specifications/liberty_alliance_id_ff_1_2_specifications

[9] Siehe hierzu den Beitrag „Web 2.0 – Trends der Internetnutzung“, WissenHeute Nr. 3/2008, S. 15 ff.