Stand des Indentity Management

The actual status of the Identity Management

Definition, Historie, neuere Entwicklungen

Horst Walther SiG Software Integration GmbH, Hamburg[1]

erschienen in IM Information Management & Consulting Heft 19, (2/2004), Mai 2004, Seite 48

Stichworte

Digitale Identität, Identitäts-Management, Identitäten Föderierung, Föderiertes Identitäts-Management, Verzeichnisdienste, Metaverzeichnisdienste, Virtuelle Verzeichnisdienste, User Provisioning.

Keywords

Digital Identity, Identity Management, Identity Federation, Federated Identity Management, Directory Service, Meta Directory Service, Virtual Directory Service, User Provisioning.

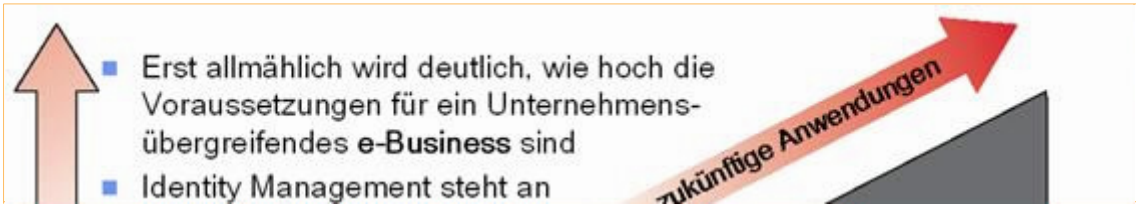
Zusammenfassung

Die Nutzung des Internets macht Unternehmensgrenzen durchlässig. Ein ganzheitliches Identity Management wird daher erforderlich. Unternehmensübergreifende Geschäftsprozesse werden derzeit am besten durch das Modell des Federated Identity Management unterstützt. Im Gegensatz zur Technik für die Unterstützung eines zentralen wie auch eines unternehmensübergreifenden Identity Management befindet sich der rechtlichgeschäftliche Rahmen noch in der Anfangsphase. Vorreiter eines Federated Identity Management sind zunächst große Unternehmen. Erst wenn die Marktteilnehmer genügend Zutrauen in die Verlässlichkeit dieser Disziplin entwickelt haben, wird sich e-Business in seiner vollen Breite und Tiefe verwirklichen lassen.

Summary

Using the Internet makes companies perimeters porous. Thus a holistic approach to identity management is required. Intercompany business processes are at present best supported by the federated identity management model. Unlike the technology for implementing company-wide and federated identity Management the complementary legal and business framework is still in its infancy. Thus federated identity management will be implemented within large corporations first. Only after the participants will have gained sufficient confidence in the reliability and trustworthiness of this business discipline, they will take e-business to its full possible extension.

1. Einführung ↑



Die

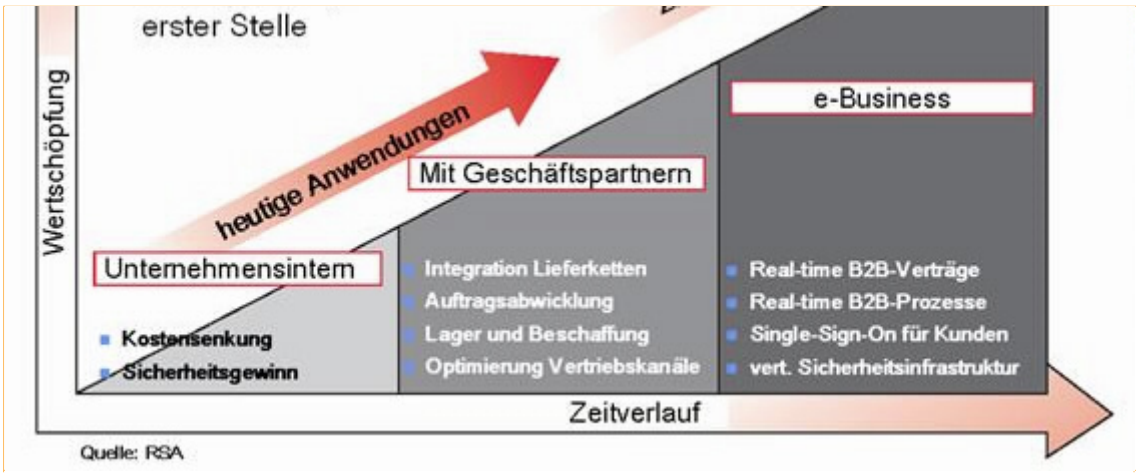


Abbildung 1: Die zunehmende Bedeutung des Identity Management

Verwaltung von Identitäten wird erst seit etwa drei Jahren als einheitliche Management-Disziplin betrachtet. Neu sind dabei nicht die zu bewältigenden Aufgaben. Schon davor musste für große und kleine Organisationen, wie kommerzielle Unternehmen, der Zutritt von Mitarbeitern und anderen Personen, wie Kunden oder Geschäftspartnern, und deren Zugriff auf Unternehmensressourcen geregelt und überwacht werden. Seit der Einführung von Computern fiel auch deren Nutzung darunter. Sinnvollerweise wurde das auch wieder auf elektronischem Wege vollzogen. Neu ist vielmehr, dass diese zuvor auf Personalmanagement, Kunden Management, User Management und andere Unternehmensfunktionen aufgeteilten Aufgaben, als Ausprägungen einer einheitlichen Disziplin gesehen werden, dem Identitätsmanagement, Identity Management oder Identity und Access Management. Im Folgenden wird einheitlich von Identity Management gesprochen.

Dieser Wandel der Wahrnehmung hat sich schleichend vollzogen. Die Gründe sind:

- Das Denken in kompletten **Geschäftsprozessen** fordert auch von der zugrundegelegten Infrastruktur eine einheitliche Organisation. Isoliert auf der Ebene einzelner Anwendungen definierte Benutzeridentitäten und Zugriffsrechte behindern deren Implementierung. Andererseits ist eine Definition von Zugriffsrechten nach einem rollenbasierten Berechtigungssystem erst mit vertretbarem Aufwand möglich, wenn diese aus den Geschäftsrollen der Geschäftsprozessdefinitionen abgeleitet werden können.
- **Der logischen Vernetzung**, die als Folge einer Reduktion der Fertigungstiefe einzelner Unternehmen zugunsten eines Netzwerkes von Lieferanten und Abnehmern entstand, folgt nun die elektronische Vernetzung. Die Versprechen des e-Business lassen jedoch sich nur erfüllen, wenn die Unternehmen ihr Inneres buchstäblich nach außen kehren und externe Partner direkt an bisher interne Geschäftsprozesse anschließen. Damit **verschwimmen** die ehedem festgefugten **Grenzen** zwischen der (geschützten) internen und der (gefahrvollen) externen Unternehmenswelt. Eine Klassifizierung der Kommunikationsinfrastruktur in Intranet, Extranet und Internet wir den geänderten Anforderungen nicht mehr gerecht. Vielmehr ist eine "feinkörnigere" Struktur der Berechtigungsdomänen gefordert, die einerseits im Innern Zonen unterschiedlichen Schutzbedarfes abbildet und andererseits externen Partnern einen gesteuerten Zugriff auf unternehmenseigene Ressourcen gestattet.
- **Unternehmensübergreifende** Zusammenarbeit in automatisierten Prozessen lässt sich nicht mehr mit unternehmensweiten technischen Lösungen unterstützen. Nur

über standardisierte Formate, Protokolle und Verfahren lässt sich der notwendige minimale Satz an Zugriffsrechten verlässlich über Unternehmensgrenzen hinweg weiter reichen. Sollen automatisierte unternehmensübergreifende Geschäftsprozesse auch in kurzfristig aufgebauten Geschäftsbeziehungen möglich werden, wird darüber hinaus eine Clearing Infrastruktur gefordert. Wie hoch die Anforderungen an ein realtime-eBusiness sind, wird erst allmählich deutlich (s. Abb. 1).

- **Ressourcenvirtualisierungen**, wie sie bei Hardware durch die Grid-Computing Initiative oder bei Anwendungen durch Web-Services erreicht werden, verleihen der Notwendigkeit, digitale Identitäten und ihren Unternehmenskontext effektiv zu verwalten, effizient zu transportieren und transformieren und automatisiert für Rechteprüfungen zu nutzen, weitere Bedeutung.
- Durch die **steigende Dynamik** der Wirtschaft wird der Wechsel zum Normalzustand. Mitarbeiter bleiben für kürzere Zeit als früher mit einer Geschäftsrolle verknüpft. Sie wechseln Abteilungen, arbeiten in Projekten oder gehen für einige Wochen zu einer Niederlassung. Normal ist auch der zeitweilige Einsatz externer Kräfte, die meist Zugriff auf bestimmte interne Ressourcen benötigen. Um hierbei Sicherheitsrisiken durch überzählige Zugriffsrechte oder Produktivitätsverluste aufgrund mangelnder Zugriffsrechte auszuschließen, bedarf es einer Automatisierung der zugrundeliegenden Verwaltungsprozesse.

Abbildung 2: Die Schalen der digitalen Identität
Quelle: Burton Group

- Erfahrungen mit den **Gefahren des Internet**, die allgemein hohe IT Abhängigkeit und nicht zuletzt das aktuelle Weltgeschehen haben zu einem erhöhten Sicherheitsbewusstsein (*Security Awareness*) geführt. Früher übliche *workarounds* wie Benutzerkonten auf Vorrat oder die leihweise Überlassung von Kennwörtern werden heute nicht mehr akzeptiert.
- Die **elektronische Verkettung** von Geschäftsprozessen zu einem Online Business birgt Risiken. Behördliche Regelungen nehmen sich immer intensiver dieser Risiken an und definieren entsprechende Anforderungen. Beispielsweise müssen sich Banken nach den Plänen des Basel Accord II darauf einrichten, für die operativen Risiken (*operational risks*) ihrer internen Abläufe Rückstellungen zu bilden. Diese lassen sich nur dann reduzieren, wenn nachgewiesen werden kann, dass die internen Abläufe geringere Risiken bergen, als pauschal unterstellt wird. International operierende Unternehmen sind darüber hinaus in vielen Staaten

verschärften Sicherheitsauflagen ausgesetzt. Beispiele sind die US-Amerikanischen Regularien wie der Sarbanes-Oxley Act, der Health Insurance Portability and Accountability Act (HIPAA), der Gramm-Leach-Bliley Act (GLBA), der Federal Information Security Management Act (FISMA), beschränkt auf Kalifornien der Security Breach Information Act (SB1386) oder in Kanada der Personal Information Protection and Electronic Documents Act (PIPEDA).

2. Die digitale Identität

Im Zentrum der Überlegungen zur Definition des Identity Management steht das Konzept der digitalen Identität. Darunter wird allgemein das Informationsabbild eines Individuums im Kontext spezifischer Informationsanforderungen verstanden. Darüber hinaus existiert noch keine einheitliche Definition. Sowohl die Strukturierung wie die Benennung Ihrer Komponenten in der Fachwelt werden noch diskutiert. Ihre Struktur wird häufig durch ein Schalenmodell beschrieben (s. Abb. 2):

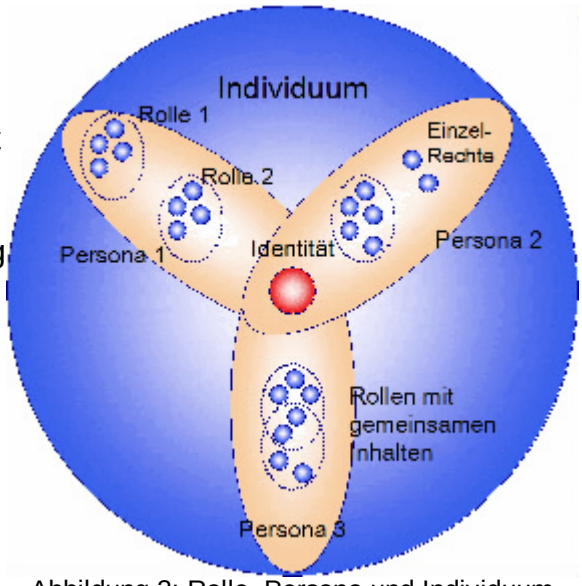


Abbildung 3: Rolle, Persona und Individuum

- **Identifikation** - Der Kern ist eine im Gültigkeitsbereich eindeutige Identifikation. Das ist die "ID", der Name oder eine Nummer einer natürlichen oder juristischen Person, einer Anwendung oder einer Hardwarekomponente. Sie sollte eine mindestens gleiche Gültigkeitsdauer haben, wie das Objekt, das sie repräsentiert.
- **Zertifikate** - Die erste Schale bilden die Zertifikate, mit je nach Anforderung, unterschiedlich starker Aussagefähigkeit bis hin zur qualifizierten digitalen Signatur nach dem Signaturgesetz.
- **Beschreibung** - Die zweite Schale machen nach diesem Modell rollenunabhängige gemeinsame Attribute aus, wie etwa die Adressinformationen oder weitere charakteristische Merkmale.
- **Kontext** - In der dritten Schale finden sich die volatilsten, aber praktisch bedeutsamsten, Merkmale wieder: die von der Rolle des Inhabers abhängigen Berechtigungen. Diese sind unterschiedlich, ob eine natürliche Person beispielsweise als Kunde, Mitarbeiter, Lieferant oder Gesellschafter oder einer Kombination davon auftritt. Vergleichbar ist die digitale Identität damit in der uns bekannten, analogen Welt mit einem Reisepass mit darin enthaltenen Visa für den Grenzübertritt in die entsprechenden Staaten.

2.1 Feinstruktur der Identität

Sollten einmal alle wesentlichen Belange beruflichen und privaten Lebens über IT gestützte Dienste abgewickelt werden, würde eine so definierte digitale Identität vielfältige

und im Zweifel brisante Informationen über das referenzierte Individuum tragen. In der Praxis würde jedoch jeweils nur ein Teil dieser Informationen für Zwecke der Identifizierung, Authentisierung, Autorisierung oder für administrative Prozesse benötigt. In der Fachwelt wird daher eine Feinstruktur diskutiert. Diese sei an Beispielen verdeutlicht:

Abbildung 4: Der Lebenszyklus einer digitalen Identität

Es ist schon erwähnt worden, dass Zugriffsrechte zu Rollen zusammengefasst werden können. So kann in einer Kfz-Werkstatt eine Person gleichzeitig die Rolle eines Meisters, die Rolle des Geschäftsführers und die eines Teilhabers einnehmen. Der Mitarbeiter einer Großbank mag gleichzeitig die Rolle eines Abteilungsleiters wahrnehmen, zusätzlich Prokura besitzen und Mitglied des Betriebsrates sein. Im Regelfalle ist er noch zusätzlich Kunde seines eigenen Unternehmens. Nach einem neueren Vorschlag bilden all diese Rollen zusammen eine "persona", zu Deutsch etwa ‚Persönlichkeit', in diesem Falle die Business-Persona. Im realen Leben hat diese Person allerdings nicht nur ihre Geschäfts-Persönlichkeit, unter der sie ihr Arbeitgeber kennt, sondern ggf. zusätzlich ihre Persönlichkeiten als Familienvater / -mutter, vielleicht als Fußballtrainer, Globetrotter oder Buchautor etc.. Dabei kann nicht unterstellt werden, dass diese Persönlichkeiten a priori miteinander über eine gemeinsame Identität verlinkt sind. Das liegt in vielen Fällen auch nicht im Interesse der abgebildeten Person. Eine mögliche Zusammenführung, etwa durch Meta-Verzeichnisdienste, oder auch nur eine Föderierung wird zusätzlich durch ihre unterschiedlichen Lebensdauern erschwert. Die Frage, wie die Summe all dieser Persönlichkeiten zu nennen ist, bewegt die Fachwelt noch. Für eine Fraktion ist das die Identität. Andere nennen sie Individuum. Für sie ist die Identität eher mit einer OID, Object ID, einem eindeutigen Identifikator eben, in Abb. 2 Existenz genannt, zu vergleichen, der in verschiedenen Inkarnationen vorkommen kann (Name, Personalnummer, Kundennummer, Steuernummer, Führerscheinnummer, ...).

Zusammengefasst: Die Abbildung einer Person ist das Individuum, die sich in verschiedene Persönlichkeiten aufspaltet, von denen jede verschiedene Rollen ausüben kann, die wiederum jeweils mit einem Satz an Rechten und Privilegien verbunden sind (s. Abb. 3).

Der Begriff der virtuellen Identität' geht noch einen Schritt weiter und postuliert, dass auf elektronischen Ausweisen auch nur dieser eindeutige Identifikator, begleitet von entsprechenden bestätigenden Zertifikaten, gespeichert wird. Jede weitere Information wird, in einer weitgehend vernetzten Umgebung, zum Bedarfzeitpunkt vom Individuum oder einer beauftragten Stelle (Hausarzt, Einwohnermeldestelle, Arbeitgeber, ...) abgerufen. Soweit nicht behördlich geregelt, obliegt es danach der Person die Nutzung seiner persönlichen Daten zu autorisieren oder zu untersagen. Die Diskussion mag etwas ‚akademisch' anmuten. In einer weitgehend digitalisierten Berufs- und Lebensumwelt aber kann die diskutierte Strukturierung erhöhte Bedeutung erlangen - damit nicht am Ende die eigene Hausbank zur Absicherung einer Kreditvergabeentscheidung die Liste der, zu medizinischen Zwecken gespeicherten, eigenen Vorerkrankungen heranzieht.

3. Identity Management

Noch hat sich in der Fachwelt keine einheitliche Auffassung darüber durchgesetzt, was unter Identity Management zu verstehen ist. In einer "natürlichen" Definition lässt sich darunter jedoch die ganzheitliche Behandlung von digitalen Identitäten verstehen, also die Disziplin, die sich mit den Prozessen von digitalen Individuen im Laufe ihres Lebenszyklus befasst.

Das Identity Management befasst sich mit dem Erzeugen / Ändern / Registrieren, dem Verteilen / Bereitstellen / Integrieren / Transformieren, der Verwendung und dem Terminieren / Archivieren von digitalen Identitäten (s. Abb. 4).

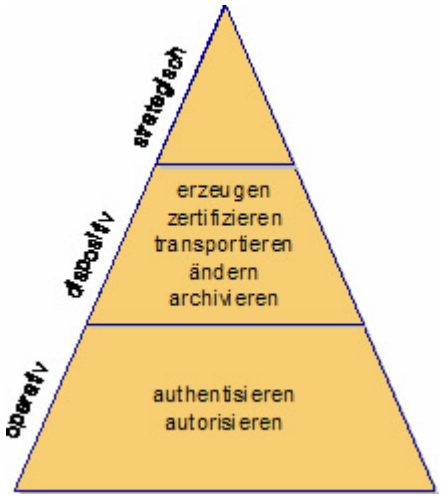


Abbildung 5: Unternehmensfunktionen

Weitere Gliederungsmöglichkeiten sind:

- organisatorisch in (*dispositive*) Prozesse der Verwaltung der Existenz, ihrer Zertifikate, Rollen und Berechtigungen und in (*operative*) Prozesse der Verwendung während der Authentisierung und der Autorisierung (s. Abb. 5). Zu der zweiten Gruppe zählt auch die Funktion Single Sign On (SSO).
- in **fachlich** erforderliche (verwalten und verwenden) und *physikalisch* durch die technische Implementierung notwendige Prozesse (integrieren, transportieren, synchronisieren, transformieren und publizieren).
- nach den "Schalen" der digitalen Identität (*Existenz*, *Zertifikat*, *Beschreibung* und *Kontext*), die jeweils verwaltet und verwendet oder integriert, transportiert, transformiert und publiziert werden.

4. Identity Federation

Unternehmensübergreifenden Beziehungen laufen heute bereits großenteils direkte elektronische Kommunikation. Für deren Absicherung werden sinnvoll die von den Unternehmen festgelegten Identitäten, Rollen und Berechtigungen verwendet. Schon in großen Unternehmen mit wirtschaftlich selbständig agierenden Substrukturen oder räumlich getrennten Niederlassungen ist es jedoch häufig schwierig, eine einzige zentrale Stelle führend mit der Definition von unternehmensweit gültigen Identitäten zu betrauen. Leichter durchsetzbar und flexibler in der Abwicklung ist hingegen die wechselseitige Anerkennung autonom in selbständigen Geschäftsbereichen definierter Identitäten, sogenannter föderierter Identitäten (Federated Identities). Im unternehmensübergreifenden Geschäftsverkehr bildet sich diese Form der Zusammenarbeit immer mehr als Methode der Wahl heraus (s. Abb. 7).

Auslöser und minimale Anforderung sind die Realisierung eines Single-Sign-On für den gesamten Geschäftsprozess über alle Partner hinweg. Der Anstoß kam denn auch nicht aus dem Unternehmens-Identity Management, sondern ist durch das Erscheinen von Microsofts Web-AuthentisierungsTools Passport ausgelöst worden, das eine portable Identity-Definition und -Implementierung für das Single Sign On für B2CAnwendungen im Web (Web-SSO) ermöglicht.

Auch von den Befürwortern eines Federated Identity Management wird nicht bestritten, dass durch eine zentral, etwa durch staatliche Stellen, vergebene und universell

nutzbare Identität keine Föderierung erforderlich würde und uns die damit verbundenen zusätzliche Komplexität erspart werden könnten. Es ist vielmehr wirtschaftlicher Pragmatismus, der sich von einer lose gekoppelten Föderation die größten Realisierungschancen verspricht. Als Konsequenz sind die beteiligten Unternehmen allerdings gezwungen, sich mit neuen Herausforderungen zu beschäftigen: mit der Zuweisung und Verteilung der damit verbundenen Verantwortlichkeiten, Risiken und Kosten.

Kosten, die zusätzlich zu einer Implementierung einer zentralen Identity Management Lösung entstehen sind:

- Kosten für das Aushandeln und Schließen formaler Vereinbarungen mit den Partnern im elektronischen Handel (inklusive operationalisierter Durchführungsbestimmungen für den Informationsaustausch, für Verantwortungsübernahme, Konfliktlösung, Datenschutz und Überprüfung der Regenkonformität),
- Kosten für die Einführung neuer technischer Lösungen und
- Kosten für die Einhaltung eines Soll-Niveaus für die operative Qualität, insbesondere der Sicherheitsanforderungen. (Alternativ die Kosten von Qualitätsverletzungen, inklusive der Sicherheitsvorfälle.)

Die wichtigsten Parteien in einen föderierten

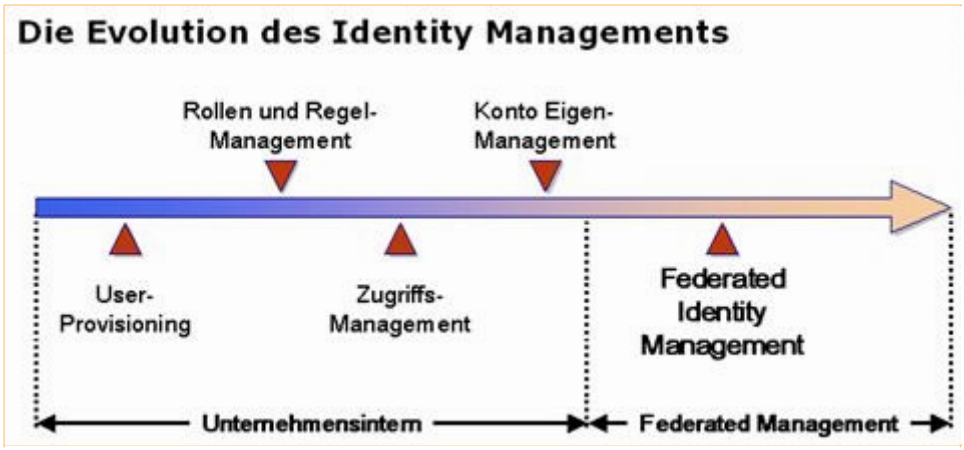


Abbildung 7: Quelle André Durand [Durand]

Identitäten-Netzwerk sind nach [Durand 2003] ...

- *Identity Principal* - Die Person, die über die behandelte Identität referenziert wird.
- *Primary Authenticator* - Die Stelle, die den *Identity Principal* authentifiziert, in das Identitäten Netzwerk einführt und den vertrauenden Teilnehmern zusichert (*assert*).
- *Identity Provider* - Die Stelle (*asserting party*), die die zur Identität gehörende Persönlichkeit (*persona*) speichert und auf Anforderung an Form einer Zusicherung (*assertion*) herausgibt.
- *Service Provider* - Als Gegenpol zum *Identity Provider* ist der Service Provider der Abnehmer (*relying party*) der Zusicherung. Er vertraut auf die Gültigkeit der Zusicherung.
- *Identity Network Operator* - Betreiber des Identitätsaustausch-Netzwerkes, eine Clearing-Stelle, der ein vertragliches Regelwerk bereitstellt und mit den Teilnehmern vereinbart. Er ermöglicht es ihnen auf diese Weise einen *circle of trust* zu bilden, wie er in den technischen Umsetzungskonzepten wie dem der *Liberty Alliance* vorgesehen ist.

In den technisch dominierten Umsetzungskonzepten der nachfolgend genannten Organisationen werden die Funktionen Primary Authenticator und Identity Network Operator als außerhalb des Betrachtungsrahmens liegende Voraussetzungen gesehen.

Heute sind vier wesentliche Organisationen damit befasst, Konzepte für Federation-Standards auszuarbeiten: Die Organization for the Advancement of Structured Information Standards (OASIS) , die Liberty Alliance, ein von Microsoft und IBM angeführtes Hersteller-Konsortium und das Shibboleth-Projekt

Das OASIS Security Services Technical Committee (SSTC) hat die Security Assertion Markup Language (SAML) in der Version 1.1 als Standard publiziert und seine Pläne zur Definition von SAML 2.0 vorgelegt. SAML bietet einen grundlegenden Austauschmechanismus für Authentisierungs- und Autorisierungsinformationen. SAML 2.0 soll vor allem die Lücken in SAML 1.1 füllen, wie das fehlende Session Management und Single Logout und darüber hinaus SAML mit dem Liberty Alliance Identity Federation Framework [Wason 20031, für das anwendergesteuerte Verknüpfen ("opt-in") von Benutzerkonten über Standorte und Unternehmen hinweg verschmelzen.

Derweil arbeitet ein anderes Technical Committee, das OASIS eXtensible Access Control Markup Language TC an der eXtensible Access Control Markup Language (XACML). Dieses TC hat die Aufgabe übernommen, ein XML-Schema und einen entsprechenden Namensraum für die Abbildung von Berechtigungsregeln zu definieren. Die XACML-Version 1.0 ist OASIS-Standard, Version 1.1 liegt als Entwurf (*draft*) vor. An Version 2.0 wird bereits gearbeitet.

Die Liberty Alliance ist mit ihren Spezifikationen am weitesten fortgeschritten. Sie hat kürzlich ihre Phase 2 Spezifikationen [Fontana 2003] für den zustimmungsgesteuerten Zugriff auf Benutzerattribute veröffentlicht. Phase 3 soll sich mit identitätsabhängigen Diensten befassen wie der Ermittlung des Anwesenheitsstatus oder Kalenderfunktionen. Die Liberty Alliance mit heute über 150 Mitgliedsunternehmen hat sich ursprünglich, vom Microsoft-Konkurrenten SUN Microsystems initialisiert als Gegenbewegung zu Microsofts Passport entwickelt.

Das von Microsoft und IBM angeführte Hersteller-Konsortium konzentriert sich zwar darauf Web-Services operativ nutzbar zu machen. Der Ansatz erscheint in seiner Breite jedoch sehr umfassend zu sein. Es arbeitet an einem verbesserten Web Services Framework (WS-*). Die darin enthaltenen Konzepte WS-Trust und WS-Federation basieren ebenfalls auf SAML, sind aber vorerst nicht mit den Arbeiten der Liberty Alliance vereinbar [Kearns 2003]. Dem Shibboleth-Projekt der Internet2-Gemeinde (Internet2/MACE), das seine Spezifikationen und auch bereits Implementierungen in der Version 1.1 vorgestellt hat, wird von Beobachtern der Bewegung eine Marktwirkung noch abgesprochen. Von Datenschützern hervorgehoben wird dessen vorbildliche Steuerungsmöglichkeit der persönlichen Informationen durch die betroffene Person selber.

Ungeachtet aller immer wieder aufkommenden Unstimmigkeiten zwischen diesen unterschiedlichen Organisationen scheint sich SAML 2.0 als Basis für die Implementierung von Identity Management Verfahren, unabhängig von einer möglichen Föderierung, zu empfehlen. Weiter findet die zur Abbildung von Policies entwickelte Darstellungssprache XACML immer mehr Zuspruch.

Damit die portable digitale Identität verwendet werden kann, sind neben der

Spezifikation technischer und organisatorischer Lösungen, drei weitere Voraussetzungen zu erfüllen. Es ist eine multiprotokollfähige, robuste Referenzimplementierung einer Zugangssoftware bereit zu stellen, ein rechtlicher Rahmen und eine verteilte Infrastruktur zu schaffen, die von den Beteiligten genutzt werden kann.

Es ist bemerkenswert und möglicherweise für den Erfolg entscheidend, dass sich dieser Aufgabenstellungen keines der großen und etablierten Unternehmen, sondern eine kleine Neugründung, die Ping Identity Corporation (PingID), aus Denver, CO, USA (www.ping1D.com) angenommen hat. PingID vertreibt die entsprechende Federation-Software SourcelD und stellt sie gleichzeitig als Open-Source über die nonprofit Organisation SourcelD (www.sourceid.org) zum kostenlosen Download bereit. Das Open-Source Toolkit SourcelD vl.1 unterstützt SAML und Liberty Alliance Protokoll 1.1, ist für Java & NET erhältlich und soll über Identity Federation eine unternehmensübergreifende Sicherheitslösung unter Partnern bereitstellen.

Um der Forderung nach einem rechtlichen Rahmen zu begegnen, hat PingID das PingID Network ins Leben gerufen. Es soll durch seine Mitglieder getragen werden, sich technologieneutral verhalten und das Regelwerk für mit der Föderierung von Identitäten verbundenen rechtlichen Fragen erarbeiten. Ausdrücklich ist auch der für jegliche Akzeptanz wichtige Schutz personenbezogener Daten in den Geschäftszielen genannt.

Bewusst sollen die aus dem Interbankenverkehr bekannten Clearing-Häuser wie Plus, Star und Cirrus oder auch Visa als Vorbild dienen. Wenn auch nur bedingt vergleichbar, soll doch von der Analogie gelernt werden. Schließlich kann hier ein Kunde über einen beliebigen Bankautomaten das Geld von einer beliebigen Bank abheben. Noch keine befriedigende Lösung ist allerdings für die Verteilung der Verantwortung in Schadensfalle in Sicht. Das ist für kritische Transaktionen nicht tolerierbar. Kritiker eines Weiterreichens der Verantwortung im Schadensfalle [Benson 2003] über eine Prozesskette sehen hier keine bisher keine Lösung.

Über das PingID Network soll auch der dritten Forderung begegnet werden, der Schaffung einer Clearing-Infrastruktur für die engagierten Parteien.

5. Technische Komponenten ↑

So wie fachlich das Identity Management erst seit kurzer Zeit als einheitliche Disziplin betrachtet wird, sind auch die unterstützenden Verwaltungssysteme und operativen Komponenten unabhängig voneinander und ohne Rücksichtnahme aufeinander entwickelt worden.

Historisch lassen sich drei große Entwicklungen ausmachen:

- Die Idee einer public key infrastructure (**PKI**) für eine auf Zertifikaten basieren de starke Authentisierung lässt sich bis in das Jahr 1976 zurück verfolgen,
- Die **CCITT** und heutige ITU-T kam schon 1988 mit der ersten Spezifikation eines Verzeichnisdienstes nach dem X.500- Standard heraus. Noch heute sind die gängigen (LDAP-) Verzeichnisdienste von diesen Entwicklungen geprägt.
- Etwa fünf Jahre später begann das **NIST** mit seinen Arbeiten über rollenbasierte Zugriffssteuerung. Darauf basieren alle späteren Zugriffsverfahren über Rollen-Mechanismen.

Dadurch weisen die so entstandenen Systeme eine hohe funktionale Überlappung auf und lassen sich nicht problemlos zu einer vollständigen Identity Management Infrastruktur zusammenstellen. Die wichtigsten dieser Komponenten einer Identity Management Infrastruktur sind: Verzeichnisdienste - Verzeichnisdienste (Directory Services) sind üblicherweise das Kernelement einer Identity Management Infrastruktur. Auf die Speicherung großer Mengen kurzer Datensätze und häufige Lesezugriffe optimiert, organisiert nach einem hierarchischen Schema und mit einem standardisierten (LDAP-) Zugriff versehen, dienen sie heute im Regelfalle als Identitätsspeicher.

- **Metaverzeichnisdienste** - sind Integrationskomponenten, die digitale Identitäten aus Verzeichnissen und anderen Informationsquellen auslesen, regelbasiert konsolidieren und in einem Zielverzeichnis ablegen. Sie werden erforderlich, wenn die Vielzahl an verteilten Identity-Informationen heutiger Großunternehmen vereinheitlicht werden soll.
- **Virtuelle Verzeichnisdienste** - Sie positionieren sich als leichtgewichtige Alternative zu Metaverzeichnisdiensten, um unterschiedliche Verzeichnisse konsolidieren. Sie erzeugen jedoch, im Unterschied zu diesen die Ergebnismenge zur Laufzeit und liefern typischerweise an eine Anwendung zurück, die eigentlich einen LDAP-Verzeichnisdienst erwartet. Damit vermeiden sie Konflikte um die Hoheit über autoritative Daten.
- **PKI**-Komponenten - Sie dienen als Werkzeuge, wenn eine starke Authentisierung gefordert wird. Die Verwaltungsprozesse, die für den Betrieb einer PKI notwendig sind, gelten als aufwändig und haben einen breiten Durchbruch bisher verhindert. EAM-Komponenten - Extranet Access Management - Tools sind ursprünglich für Web-Applikationen entwickelte Autorisierungs-Komponenten. Häufig bieten sie weitere Funktionen des Identity Managements, um so als eigenständige Komponenten einsetzbar zu sein.
- **SSO**-Tools - Single Sign On-Systeme sind eher eine Hilfskonstruktion. Sie dienen der Synchronisation der Passwörter unterschiedlicher Systeme und deren Weiterleitung, sodass ein Anwender sich idealerweise nur einmal anmelden muss, um auf alle für ihn freigeschalteten Systeme zugreifen zu können. Da SSO in sich neue Sicherheitsrisiken birgt, kann mit einem Reduced Sign On ein sinnvoller Kompromiss erreicht werden.
- **User Provisioning**-Systeme sind die jüngste Entwicklung. Sie automatisieren die Prozesse der Beantragung, Vergabe und des Entzugs von Berechtigungen. Sie bieten Reporting-Funktionen, um den Berechtigungszustand zu einen beliebigen Zeitpunkt revisionssicher zu dokumentieren. Über Konnektoren können sie die Benutzerberechtigungen direkt in die zu versorgenden Zielsysteme einspeisen und zu Kontrollzwecken wieder auszulesen. Um aus diesen Teil-Systemen und Einzelkomponenten ein reibungslos zusammen arbeitendes System für das unternehmensweite Identity Management zusammenstellen zu können, beginnen die Anbieter mit jeweils unterschiedlichen Ausgangspositionen ihr Portfolio zu erweitern, um sich, über Eigenentwicklungen, Akquisitionen oder Partnerschaften als Komplettanbieter im Identity Management-Markt zu positionieren.

Die anwendenden Unternehmen verlangen hingegen zunehmend danach, sich eine Infrastruktur für das Identity Management aus best-of-breed-Komponenten zusammenstellen zu können.

Dadurch erhalten die vielfältigen Bemühungen über SPML, SAML, DSML oder XCAML, einen standardisierten Informationsaustausch von Identity Informationen zu ermöglichen,

eine Schlüsselrolle für die erfolgreiche Etablierung eines unternehmensweiten Identity Management.

6. Ausblick

Steigender Aufwand bei der Verwaltung von Benutzern und Zugriffsrechten bei weiter anhaltendem Druck zu Senkung von Verwaltungskosten unter gleichzeitiger Wahrung eines angemessenen Sicherheitsniveaus, werden weiterhin gute Gründe für die Beschäftigung mit Identity Management Systemen liefern.

Dabei lassen Amortisationsdauern die, beispielsweise bei der Einführung von moderneren prozessorientierten Systemen, wie User Provisioning Systemen, unter zwei Jahren liegen, Investitionen in derartige Systeme auch in wirtschaftlich schwierigen Zeit als sinnvoll erscheinen.

Für Unternehmen, die planen, effiziente und sichere internetbasierte Unternehmensprozesse, z. B. über Webservices, einzuführen, wird darüber hinaus die effektive Beherrschung der Infrastrukturdisziplin Identity Management zu einem erfolgskritischen Schlüsselfaktor werden.

Während die Technik für die Unterstützung eines zentralen, wie auch eines unternehmensübergreifenden (federated) Identity Management, wie zum Beispiel Verzeichnisdienste, bereits eine gute Reife aufweist oder, wie bei der Entwicklung von Austauschformaten für Sicherheitsinformationen oder Geschäftsregeln, absehbar entsteht, befindet sich der rechtlich, geschäftliche Rahmen noch in der Anfangsphase. Verfahren, Abwicklungsstellen und eine Vertrauen schaffende, weithin geübte "gute Praxis" werden jedoch nicht "über Nacht" entstehen. So wird das Federated Identity Management zunächst erst innerhalb großer Unternehmen implementiert. Unternehmen mit traditionell enger partnerschaftlicher Zusammenarbeit, wie etwa zwischen Automobil-Herstellern und deren Zulieferern, werden vermutlich den nächsten Schritt tun. Erst darauf wird sich genügend Zutrauen in die Verlässlichkeit dieser Disziplin entwickelt haben, damit die in Abb. 1 postulierte Stufe 3 des e-Business mit realtime-B2B-Verträgen und nachfolgenden realtime-B2B-Prozessen verwirklicht werden kann.

Glossar

CCITT	Comite Consultatif Internationale de Télégraphie et Téléphonie
DSML	Directory Services Markup Language, eine XML Spezifikation für die Darstellung von Verzeichnisdienstinformationen
ITU	international Telecommunications Union-Telecommunication
LDAP	Lightweight Directory Access Protocol
NIST	National Institute of Standards & Technology
RABC	Role Based Access Control
SAML	Security Assertion Mark-up Language, eine XML Spezifikation für den Austausch von Authentisierungs- und Autorisierungsinformationen
SPML	Service Provisioning Markup Language, eine XML Spezifikation für den Austausch von User provisioning Informationen

XACML	eXtensible Access Control Markup Language, eine XML Spezifikation für die Darstellung von Unternehmensregelungen für den Informationszugriff über das Internet

Literaturverzeichnis

- [Microsoft 2000] Microsoft Corporation, "**Enterprise Identity Management, Strategy White Paper**", 2000
- [Durand 2002] Norlin, E., Durand, A., "**Towards Federated Identity Management**", 2002
- [Durand 2003] Norlin, E., Durand, A., "**Identity Networks: Role of the Primary Authenticator**", 11.01.2003
- [Wason 2003] Wason T., "**Liberty ID-FF Architecture Overview**", 2003
- [Fontana 2003] Fontana, J., "**Liberty completes Phase 2 of its identity work**", Network World Fusion, 12.11.2003
- [Kearns 2003] Kearns, D., "**Liberty Alliance vs. WS-Federation: Should we care?**", Network World Identity Management Newsletter, 03.11.2003
- [Benson 2003] Benson C., "**Liability and Federated Identity: Much Ado About Nothing?**", 12/2003.

Autoreninformation

[1]Dr. Horst Walther ist Geschäftsführer der SiG Software Integration GmbH in Hamburg:

Dr. Horst Walther
SiG Software Integration GmbH
Chilehaus A * Fischertwiete 2
D-20095 Hamburg
Fon: 040/32005 439
Fax & Voice-Mail: 040/8708306 8
Mobil & Voice Box: 0171 2145502
E-Mail: Horst.Walther@Si-G.com
http://www.si-G.com
Dr. Horst Walther

Horst Walther, Hamburg, 04. August 2005

home < Drucken