Identity Management

Definition, Status, Trend

Dr. Horst Walther[1]

1. Zusammenfassung

Der Begriff Identity Management scheint sich zu etablieren. Treiber ist die Absicht vieler Unternehmen, automatisierte Geschäftsprozesse mit dem Internet als Trägermedium zu etablieren. Damit entspricht die dualistische Einteilung der Netzwelt in internes Intranet und externes Internet – mit speziellen Extranets als Behelfskonstrukt für die externe Kommunikation – nicht mehr den Anforderungen. Vielmehr bedarf es der Implementierung eines ganzheitlichen Identity Managements, um so eine sichere und feingranulare Zugriffssteuerung zu erreichen. Unternehmensübergreifende Geschäftsprozesse werden am besten durch das Modell des *Federated Identity Management* unterstützt. Der mit dem Überschreiten der Unternehmensgrenzen erforderliche Austausch standardisierter Sicherheitsinformationen stellt neue Herausforderungen. Aktuelle Bestrebungen zur Ressourcenvirtualisierung wie Web-Services oder Grid-Computing erhöhen den Handlungsdruck weiter. Parallel dazu haben viele Marktangebote eine für einen unternehmensweiten Einsatz hinreichende Reife erlangt. Amortisationsdauern, beispielsweise bei der Einführung von User Provisioning Systemen, die unter zwei Jahren liegen, lassen Investitionen in bestimmte Systeme auch in wirtschaftlich schwierigen Zeit als sinnvoll erscheinen.

2. Die Ausgangslage

Neue Begriffe kommen und gehen. Daran haben wir uns gewöhnt. Identity Management scheint zu den Kreationen zu gehören, die uns einige Zeit begleiten werden. Vor etwa drei Jahren tauchte diese Bezeichnung für ein Aufgabegebiet auf, das bereits lange zu den notwendigen Verwaltungsaufgaben im Unternehmen zählte, bis dahin jedoch nicht als einheitliche Disziplin gesehen wurde.

Dem Wandel der Wahrnehmung von Unternehmensaufgaben folgend, ist die Dienstleistung der Verwaltung von Zugriffsberechtigungen neuen Anforderungen ausgesetzt:

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.

Der logischen Vernetzung, die als Folge einer Reduktion der Fertigungstiefe einzelner Unternehmen zugunsten eines Netzwerkes von Lieferanten und Abnehmern entstand, folgt nun die elektro-

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

nische Vernetzung. Die Versprechen des e-Business lassen 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 festgefügten ***Grenzen*** zwischen der (geschützten) internen und der (gefahrvollen) externen Unternehmenswelt.

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.

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.

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. Ein "*Leih' mir 'mal Dein Passwort*!" wird 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.

3. Die digitale Identität

Wenn diesen fundamentalen Herausforderungen begegnet werden soll muss als Grundlage eine eindeutige und übergreifend gültige digitale Identität verwendet werden.

Die digitale Identität lässt sich gut mit einem Schalenmodell beschreiben.

- ***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 die Objekte, die 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 Adress-

Abbildung 1: Die Schalen der digitalen Identität

informationen 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.

4. Prozesse des Identity Managements

In der Fachwelt hat sich zwar noch 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. Das ist die Disziplin, die sich mit den Prozessen einer digitalen Identität im Laufe ihres Lebenszyklus befasst.

Das Identity Management befasst sich also mit dem Erzeugen / Ändern / Registrieren, dem Verteilen / Bereitstellen / Integrieren / Transformieren, der Verwendung und dem Terminieren / Archivierenvon digitalen Identitäten (s. Abb. 1).

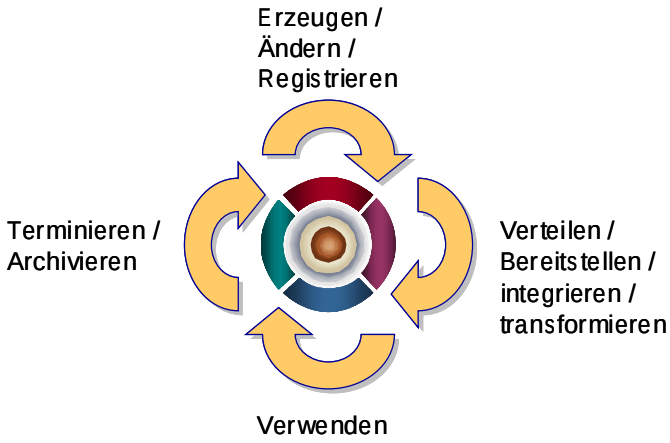

Abbildung 2: Der Lebenszyklus einer digitalen Identität

Die Prozesse des Identity Management lassen sich außer nach dem Lebenszyklus gruppieren:

- 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.
- in **fachlich** erforderliche (verwalten und verwenden) und **physikalisch** durch die technische Implementierung notwendige Prozesse (integrieren, transportieren, 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.

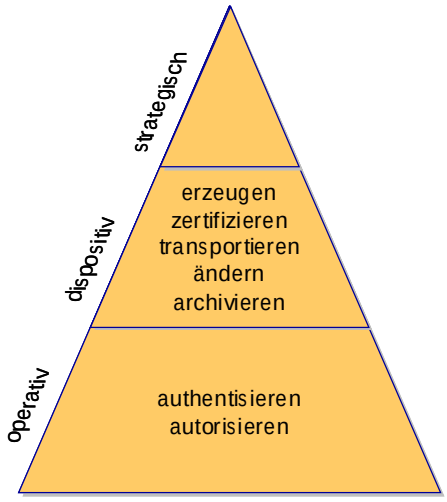

Abbildung 3: Unternehmensfunktionen

Eine eigenwillige, aber wegen der Geschlossenheit ihrer Darstellung interessante, fachliche Klassifizierung stammt von der Fa. Microsoft [Microsoft 2000]. Das Identity Management lässt sich danach in drei Gruppen von Prozessen gruppieren, die der Bearbeitung der digitalen Personenidentität dienen:

Identity Administration – Verwalten von digitalen Personenidentitäten, ihren Beziehungen zur Organisationseinheit und die Zuweisung von Ressourcen.

Community Management – Authentisierung, Bereitstellen / Publizieren und Autorisierung von Personen gemäß ihren digitalen Personenidentitäten.

Identity Integration - Mechanismen für die Aktualisierung und Synchronisation von digitalen Personenidentitäten, die verteilt und teilweise redundant gehalten werden.

Abbildung 4: Prozesse des Identity Managements (Quelle: Microsoft)

Die erste Prozessgruppe repräsentiert also dispositive Prozesse, die zweite die operativen Prozesse und die dritte Gruppe die physikalisch erforderlichen, fachlich aber trivialen Integrationsprozesse. Damit spannt diese Definition den maximalen Rahmen für die Prozesse des Identity Management auf.

5. Komponenten des Identity Management

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 basierende starke Authentisierung lässt sich bis in das Jahr 1976 zurück verfolgen,

Die CCITT[2] und heutige ITU-T[3] kam schon 1988 mit der ersten Spezifikation eines Verzeichnisdienstes nach dem X.500- Standard heraus. Noch heute sind die gängigen Verzeichnisdienste von diesen Entwicklungen geprägt.

Etwa 5 Jahre später begann das NIST[4] mit seinen Arbeiten über rollenbasierte Zugriffssteuerung[5]. 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 zusammen stellen.

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[6]-) 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 – 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,

---

[2] Comite Consultatif Internationale de Télégraphie et Téléphonie

[3] International Telecommunications Union-Telecommunication

[4] National Institute of Standards & Technology

[5] RABC: Role Based Access Control

[6] Lightweight Directory Access Protocol

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[7], SAML[8], DSML[9] oder XCAML[10], einen standardisierten Informationsaustausch von Identity Informationen zu ermöglichen, eine Schlüsselrolle für die erfolgreiche Etablierung eines unternehmensweiten Identity Management.

6. *Federation*, der nächste Schritt

Da das Wesen wirtschaftlichen Handelns in der geschäftlichen Interaktion zwischen Partnern liegt, enden viele Geschäftsprozesse nicht an der Unternehmensgrenze. Diese unternehmensübergreifenden Beziehungen laufen heute bereits großenteils direkte elektronische Kommunikation. So ist es auch nur folgerichtig, dass die von den Unternehmen festgelegten Identitäten, Rollen und Berechtigungen auch für unternehmensübergreifende Prozesse verwendet werden.

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.

Dennoch beginnt hier technologisches, organisatorisches und rechtliches Neuland. Für den Schritt des Identity Management über die Unternehmensgrenze hinaus, sind einige zusätzliche Vorkehrungen zu treffen.

[7] Service Provisioning Markup Language, eine XML Spezifikation für den Austausch von User provisioning Informationen

[8] Security Assertion Markup Language, eine XML Spezifikation für den Austausch von Authentisierungs- und Autorisierungsinformationen

[9] Directory Services Markup Language, eine XML Spezifikation für die Darstellung von Verzeichnisdienstinformationen

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

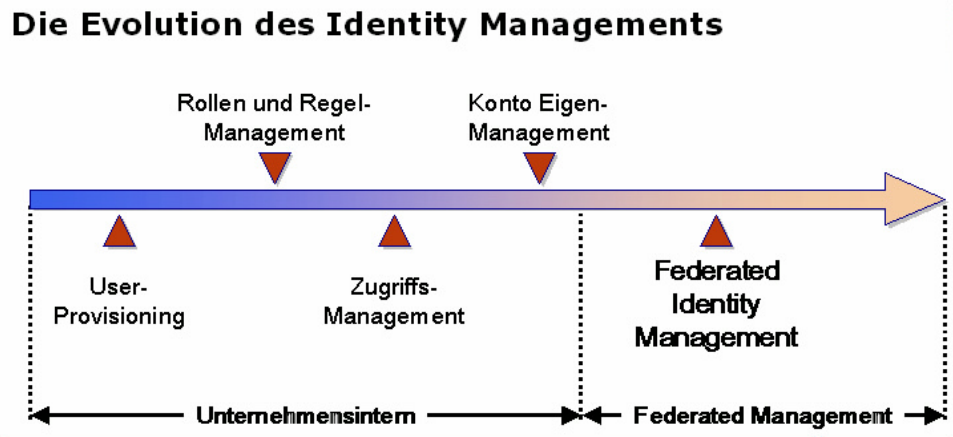

Abbildung 5: Quelle: Andre Durand [Durand 2002]

Interessanterweise ist der Anstoß zur Entwicklung dieser *Federated Identity Management* genannten Disziplin nicht aus dem Unternehmens-Identity Management gekommen, sondern durch das Erscheinen von Microsofts Web-Authentisierungs-Tools *Passport* ausgelöst worden.

Der Vorstoß von Microsoft, mit dem Produkt Passport eine portable Identity-Definition und –Implementierung auszuliefern, die das *Single Sign On* speziell für B2C-Anwendungen im Web (Web-SSO) ermöglicht, hat nach anfänglicher „Schreckstarre“ zu erheblichen Diskussionen im Markt und auf der politischen Ebene geführt. Vom Konkurrenten SUN Microsystems initialisiert, hat sich daraufhin die Liberty Alliance mit heute über 150 Mitgliedsunternehmen geformt, die mit Gegenspezifikationen für alternative Produkte der übrigen Hersteller begann.

Trust (Vertrauen) ist das Schlüsselwort des Federated Identity Management. Im Deutschen Sprachgebrauch treffen die Begriffe „Verlässlichkeit“ oder „Zuverlässigkeit“ die geforderten Qualität der Information besser, als die direkte Übersetzung als „Vertrauen“. Hier ist den im Unternehmenskontext üblichen Prüfprozessen noch die Überprüfung der Zuverlässigkeit der zugrunde liegenden Informationen vorgeschaltet:

- Trust → Identify → Authenticate → Authorize → Access.

In den Umsetzungskonzepten wird die Bereitstellung des fachlichen Dienstes durch einen *Service Provider* von der des davon unabhängigen Identitätsdienstes durch einen *Identity Provider* unterschieden. In sogenannten *Circles of Trust* werden die Identitäten, begleitet von Verlässlichkeitsaussagen (*trust*) und Anwendungsregeln (*policies*), unter diesen Partnern weitergegeben.

Heute sind vier wesentliche Organisationen damit befasst, Konzepte für Federation-Standards auszuarbeiten: Die Organization for the Advancement of Structured Information Standards (OASIS)[11], die Liberty Alliance[12], ein von Microsoft und IBM angeführtes Hersteller-Konsortium[13] und das Shibboleth-Projekt[14]:

Das **OASIS** Security Services Technical Committee (SSTC[15]) 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 Authentisie-

[11] http://www.oasis-open.org

[12] http://www.projectliberty.org/

[13] http://www-106.ibm.com/developerworks/webservices/library/ws-fedworld/

[14] http://shibboleth.internet2.edu/

[15] http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

rungs- 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 2003], für das anwendergesteuerte („opt-in“) Verknüpfen 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)[16]. 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.

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 dieser unterschiedlichen Organisationen scheint sich SAML 2.0 als solide Basis für die Implementierung von Identity Management Verfahren, ob *federated* oder nicht, zu empfehlen. Weiter findet die zur Abbildung von *Policies* entwickelte Darstellungssprache XACML immer mehr Zuspruch.

Damit die portable digitale Identity 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.pingID.com) angenommen hat.

[16] http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

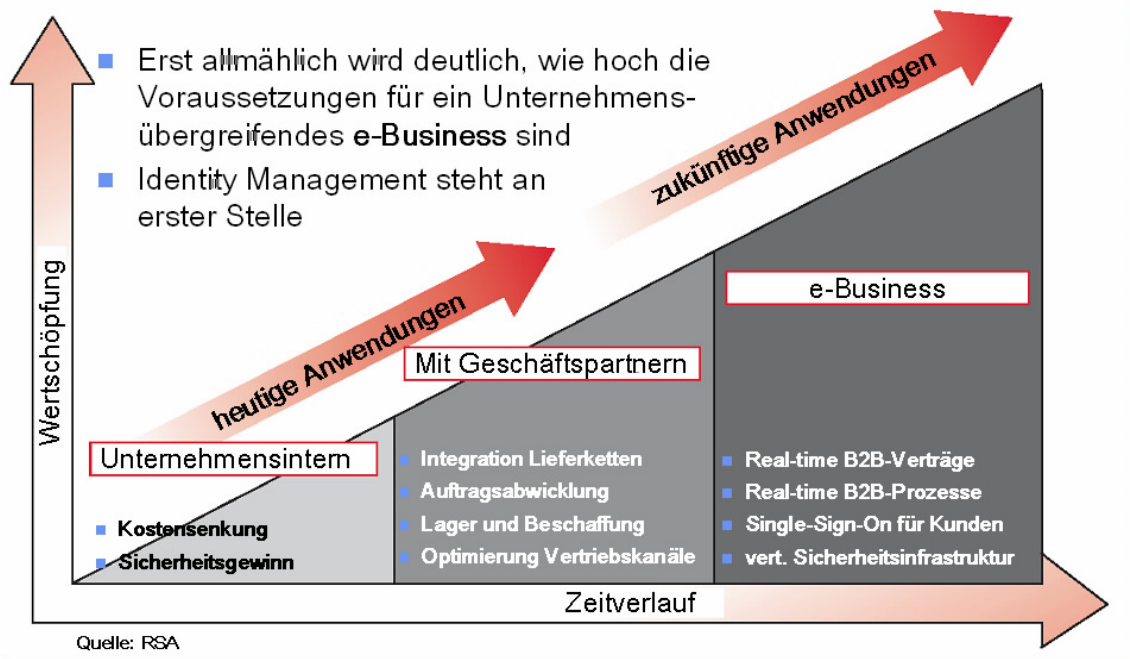

Abbildung 6: Die zunehmende Bedeutung des Identity Management

PingID vertreibt die entsprechende Federation-Software SourceID und stellt sie gleichzeitig als Open-Source über die non-profit Organisation SourceID (www.sourceid.org) zum kostenlosen Download bereit. Das Open-Source Toolkit **SourceID v1.1** unterstützt SAML und Liberty Alliance Protokoll 1.1, ist für Java & .NET erhältlich und soll über Identity Federation eine unternehmens-übergreifende 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 über die Verteilung der Verantwortung in Schadensfalle in Sicht, ein Umstand der für kritische Transaktionen nicht tolerierbar ist. Kritiker eines Weiterreichens der Verantwortung im Schadensfalle [Benson 2003] über eine Prozesskette hinweg sind jedenfalls noch nicht glaubhaft widerlegt worden.

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

7. 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 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 einzuführen, wird darüber hinaus die effektive Beherrschung der Infrastrukturdisziplin Identity Management zu einem erfolgskritischen Schlüsselfaktor werden.

Um technisch auf eine systemgestützte unternehmensübergreifende Zusammenarbeit, z. B. über Webservices, vorbereitet zu sein, empfiehlt es sich, die Implementierung einzelner Lösungen in eine offene und an Standards orientierte Gesamtarchitektur einzubetten und in Risiko begrenzenden Stufen zu realisieren. Denn in Form der Beherrschung des *Federated Identity Management* wartet die nächste Aufgabe auf ihre Bewältigung.

Wichtiger noch als die technisch organisatorischen Ansätze, wird hierbei, der Weg sein, über den die ersten anwendenden Unternehmen in der Öffentlichkeit, ob Unternehmen oder private Konsumenten, ein angemessenes Vertrauen in die Verlässlichkeit der Prozesse aufbauen und pflegen. Das Teilnehmervertrauen der privaten Verbraucher im B2C-Bereich wird sich möglicherweise über einen Wettbewerb konkurrierender Systeme in einem allmählichen Gewöhnungsprozess bei langsam steigender Bedeutung der Transaktionen herausbilden.

Von den Unternehmen erfordert das eine explizite Marktkommunikation in Sachen Schutz der persönlichen Daten (Privacy) und ein glaubwürdiges, schlüssiges und mit dem globalen Markenimage harmonisiertes Handeln. Wenn das gelingt, wird das Identity Management endgültig die Hinterzimmer der Systemadministratoren verlassen und seinen Platz auf Unternehmensführungsebene eingenommen haben.

Ob es gelingen wird, werden die nächsten 2 – 3 Jahre zeigen.

8. Literatur

- [Microsoft 2000] *Microsoft Corporation,* “Enterprise Identity Management”, Strategy White Paper, www.microsoft.com/windows2000/docs/eim.doc, 2000
- [Durand 2002] Norlin, E., Durand, A., “Towards Federated Identity Management”, http://discuss.andredurand.com/stories/storyReader$320, 2002
- [Wason 2003], Wason T., “Liberty ID-FF Architecture Overview”, http://www.projectliberty.org/specs/liberty-idff-arch-overview-v1.2.pdf, 2003
- [Fontana 2003] Fontana, J., “Liberty completes Phase 2 of its identity work”, Network World Fusion, http://www.nwfusion.com/news/2003/1112liberty.html, 12.11.2003
- [Kearns 2003], Kearns, D., “Liberty Alliance vs. WS-Federation: Should we care?”, Network World Identity Management Newsletter, *http://www.nwfusion.com/newsletters/dir/2003/1103id1.html*, 03.11.2003
- [Benson 2003] Benson C., “Liability and Federated Identity: Much Ado About Nothing?”, http://magazine.digitalidworld.com/Nov03/Page70.pdf, 12/2003.

10 Seiten, 3017 Wörter, 21799 Zeichen