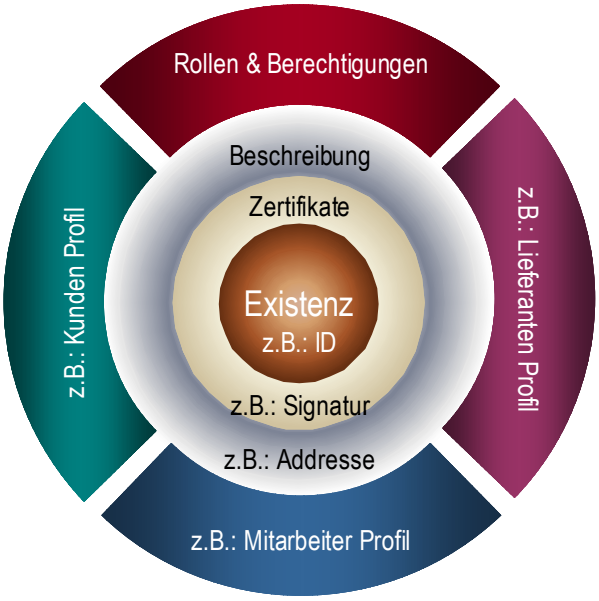
Identity Management

Dr. Horst Walther und Manfred Härtel[1, 2]

Der Begriff Identity Management scheint sich zu etablieren. Treiber ist die Absicht vieler Unternehmen, automatisierte und unternehmensübergreifende Geschäftsprozesse über Internet abzuwickeln. Für die sichere Organisation der Zugriffsberechtigungen brauchen sie ein ganzheitliches Identity Management.

Grundlage des Identity Managements ist eine eindeutige und übergreifend gültige digitale Identität.

Sie lässt sich gut mit folgendem Schalenmodell beschreiben.



- ***Identifikation*** - Der Kern ist eine im Gütigkeitsbereich 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 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 je nachdem, ob eine natürliche Person beispielsweise Kunde, Mitarbeiter, Lieferant oder Gesellschafter oder eine Kombination davon ist.

Vergleichbar ist die digitale Identität mit einem Reisepass mit darin enthaltenen Visa für die entsprechenden Staaten.

Prozesse des Identity Managements

In der Fachwelt hat sich zwar noch keine einheitliche Auffassung 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, also mit dem Erzeugen, Ändern, Registrieren, Verteilen, Bereitstellen, Integrieren, Transformieren, der Verwendung und dem Terminieren sowie Archivieren von digitalen Identitäten (s. Abb. 1).

[1] Manfred Härtel ist Regional Sales Director der Burton Group für Mittel- und Südeuropa.

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

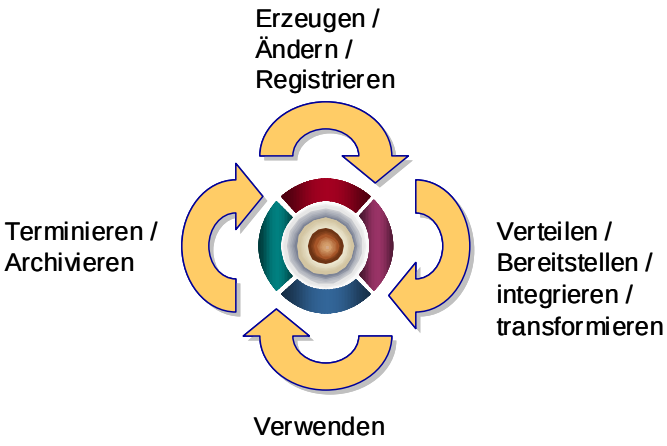
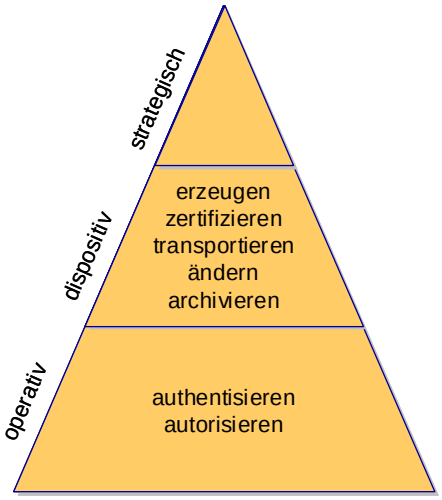


Abbildung 1: Der Lebenszyklus einer digitalen Identität

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 die (**operativen**) Prozesse der Verwendung während der Authentisierung und der Autorisierung.
- in **fachlich** erforderliche (verwalten und verwenden) und **physisch** 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.



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 identifizieren:

Die Idee einer *Public Key Infrastructure* (PKI) für eine auf Zertifikaten basierende starke Authentisierung lässt sich bis in das Jahr 1976 zurückverfolgen. Die CCITT[3] und heutige ITU-T[4] 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 fünf Jahre später begann das NIST[5] mit seinen Arbeiten über rollenbasierte Zugriffssteuerung[6]. 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 Infrastruktur für das Identity Management zusammenstellen.

Wesentliche Komponenten einer Identity Management Infrastruktur sind:

[3] Comité Consultatif Internationale de Télégraphie et Téléphonie

[4] International Telecommunications Union-Telecommunication

[5] National Institute of Standards & Technology

[6] RABC: Role Based Access Control

- ***Verzeichnisdienste*** – (Directory Services) sind das Kernelement jeder Identity Management Infrastruktur. Auf die Speicherung großer Mengen kurzer Datensätze und häufige Lesezugriffe optimiert, organisiert nach einem hierarchischen Schema und mit einem standardisierten (LDAP[7]-) 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*** – positionieren sich als leichtgewichtige Alternative zu Metaverzeichnisdiensten, um unterschiedliche Verzeichnisse konsolidieren. Sie liefern jedoch, im Unterschied zu diesen, zur Laufzeit typischerweise die Ergebnismenge an eine Anwendung zurück, die eigentlich einen LDAP-Verzeichnisdienst erwartet.
- ***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 isolierte Tools einsetzbar zu sein.
- ***SSO-Tools*** – *Single Sign On*-Systeme sind eher eine Hilfskonstruktion. Sie dienen der Synchronisation der Passwörter unterschiedlicher Systeme und deren Weiterleitung, so dass 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, stellt Reduced Sign On einen vernünftigen Kompromiss dar.
- ***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 einem beliebigen Zeitpunkt revisionssicher zu dokumentieren. Über Konnektoren können sie die Benutzerberechtigungen direkt in die zu versorgenden Zielsysteme einspeisen.

Ausblick

Systeme wie Metaverzeichnisdienste, virtuelle Verzeichnisdienste und User Provisioning Systeme wurden zu unterschiedlichen Zwecken entwickelt, ihre Funktionen überlappen sich jedoch zunehmend. Entsprechend beginnen die Anbieter mit jeweils unterschiedlichen Ausgangspositionen ihr Portfolio zu erweitern, um sich, teilweise 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[8], SAML[9], DSML[10] oder XCAML[11], die einen standardisierten Informationsaustausch von Identity Informationen ermöglichen, eine Schlüsselrolle für die erfolgreiche Etablierung eines Identity Managements im Unternehmen.

[7] Lightweight Directory Access Protocol

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

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

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

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

Für Unternehmen, die effiziente internetbasierte Unternehmensprozesse einführen wollen, wird die effektive Beherrschung der Infrastrukturdisziplin Identity Management zu einem erfolgskritischen Schlüsselfaktor werden.

Zusätzlich lassen Amortisationsdauern die, beispielsweise bei der Einführung von User Provisioning Systemen, unter zwei Jahren liegen, Investitionen in derartige Systeme auch in wirtschaftlich schwieriger Zeit als sinnvoll erscheinen. Dennoch ist es ratsam die Implementierung einzelner Lösungen in eine Gesamtarchitektur einzubetten. Dies gilt vor allem vor dem Hintergrund der Unterstützung künftiger Entwicklungen, wie z.B. Webservices.