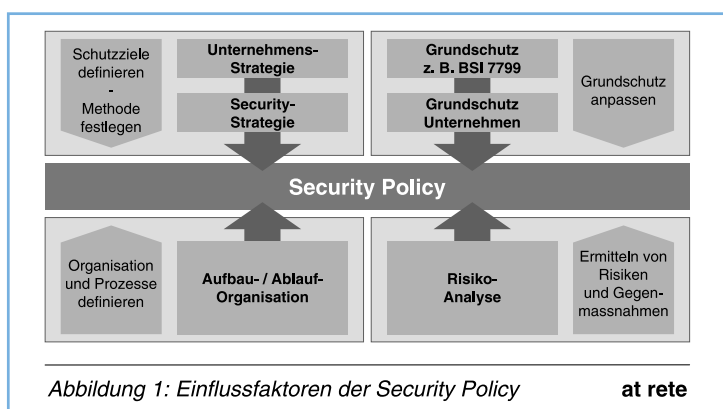


Identity Management: Hype oder Realität?

Der Nutzen einer digitalen Identität ist unbestritten: Benutzern wird ermöglicht, auf digitale Ressourcen zuzugreifen und Anbieter können die Ressourcen den Berechtigten gezielt zuweisen und – als wohl wichtigster Punkt – die Nutzung ihrer Ressourcen verrechnen. Die digitale Identität ist somit Grundvoraussetzung für funktionierende Geschäftsmodelle im digitalen Zeitalter. Wie aber werden digitale Identitäten verwaltet? In unserer vernetzten Welt würde man ohne weiteres erwarten, dass eine derart zentrale Funktion auch zentral gelöst wird. Die Realität aber zeigt, dass jede Applikation und jede Organisation das Problem der Identität individuell angeht. Wo also liegt das Problem? Der Artikel zeigt, was unter Identity Management zu verstehen ist, mit welchen Problemen organisationsübergreifende Identity Management Systeme konfrontiert sind und weist – anhand einer Initiative von SWITCH¹ – darauf hin, welche Lösungen heute in der Praxis erprobt werden.

von Anton Klee und André Redard

Wer kennt das Problem nicht: Obschon physisch eine Person und durchaus identifizierbar, müssen wir uns elektronisch laufend identifizieren. Sei es am Arbeitsplatz mit Passwort und User ID, am Telearbeitsplatz zu Hause zusätzlich mit einer Smart Card oder beim e-banking mit Passwort, User ID und Streichliste. Und das Einkaufen über das Internet verlangt selbstverständlich ebenfalls Passwort und Kundennummer.



at rete

Es liegt auf der Hand, dass es einfacher wäre – zumindest für Organisationen, die eng zusammenarbeiten – die Benutzer und deren Identitäten nur einmal zu registrieren und zu verwalten. Die Vorteile sind klar: Die Benutzer müssen sich lediglich einmal registrieren und die angeschlossenen Organisationen greifen bei Bedarf gegenseitig auf die registrierten digitalen Identitäten zu. Den in einem solchen Verbund registrierten Benutzern können die von den jeweiligen Organisationen autorisierten Ressourcen – im kommerziellen Umfeld sprechen wir von Angeboten – zugewiesen werden. In Summe wird folglich ein derart gestaltetes Identity Management für alle Beteiligten zum Vorteil gereichen.

Es zeigt sich nun aber, dass vor allem zwei Aspekte die Akzeptanz und die Verbreitung von organisationsübergreifenden Identity Management Systemen hemmen. Es sind dies:

- Die Autonomie der einzelnen Organisationen
- Die Heterogenität der involvierten IT-Systeme

Autonomie der einzelnen Organisationen

Diese drückt sich – aus der für uns relevanten Sicherheits-Perspektive – darin aus, dass jede Organisation eine eigenständige Ausprägung ihrer IT-Security Policy hat. Diese umfasst neben den organisationspezifischen Risikobetrachtungen und den zugehörigen Schutzmassnahmen auch organisatorische Belange, insbesondere die Ausgestaltung der Ablaufprozesse in der Organisation. Abbildung 1 zeigt die Zusammenhänge dieser Elemente:

Identity Management und damit die Art der Authentifizierung von IT-Benutzern ist Teil der IT-Security und findet ihre Begründung letztlich in der jeweiligen Security Policy. Aufgrund der Verankerung der Security Policy in der Unternehmensstrategie und – was sich noch stärker auswirkt – in der Aufbau- und Ablauforganisation, ist unschwer ersichtlich, dass jede Organisation in diesem Bereich möglichst autonom sein will.

Heterogenität der involvierten IT-Systeme

Organisationsübergreifendes Identity Management verlangt, dass die involvierten IT-Security Systeme aufeinander abgestimmt sind und dass sich das Identity Management nahtlos in die bereits existierenden Systemlandschaften integrieren lässt. Auf der technischen Ebene bedeutet IT-Security, dass jede Organisation – unter anderen – Systeme zur Bewältigung des AAA-Problems (Authentifizierung / Autorisierung / Accounting) im Einsatz hat. Angesprochen werden hier Themen wie:

- Tokenbasierte Authentifizierung
- Zertifikatsbasierte Authentifizierung (PKI)
- Directory (X.500, LDAP)
- Single Sign On
- LDAP, Radius, TACACS, Kerberos

Typischerweise wählt jede Organisation die für ihre Bedürfnisse passende Ausprägung der obigen Systemlandschaft. Eine Vereinheitlichung zum Zwecke eines übergreifenden Identity Managements ist aufwändig und mit bedeutenden Kosten verbunden. Letzteres bringt – in der heutigen Zeit der sich nahtlos aneinanderreihenden IT-Budgetkürzungsrunden – jedes entsprechende Projekt auf die «watch-list» der CIOs.

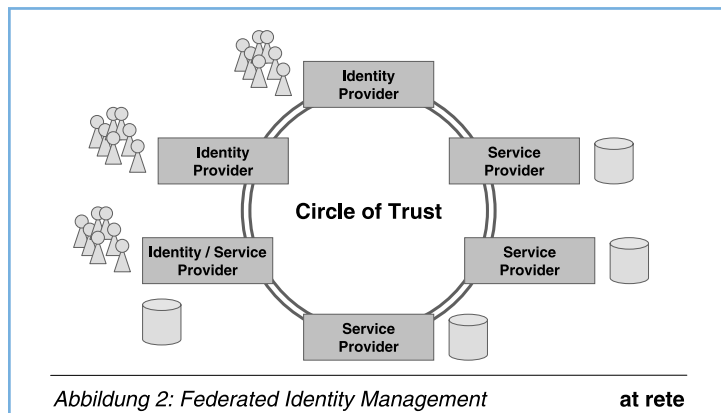
Was also bietet sich als Erfolg versprechender Ansatz zur Überwindung der gezeigten Hemmnisse an?

Federated Identity Management als

Lösungsansatz

Der Schlüssel zum Erfolg liegt, wie so oft, in der richtigen Kombination von Technologie und Organisation. Wir sprechen damit das unter dem Namen «Federated Identity Management» bekannte Modell an. Der föderative Gedanke kommt in der Tatsache zum Tragen, dass die Autonomie der einzelnen Organisationen möglichst weitgehend erhalten bleibt und gleichzeitig aber die bestehenden Vertrauensverhältnisse zwischen Benutzern und ihren individuellen Organisationen auf die Gemeinschaft, also die Föderation, übertragen werden.

Mit dieser Übertragung von Vertrauensverhältnissen gelingt es auf elegante Weise den Zwang zur Harmonisierung der IT-Security Systeme auf ein Minimum zu beschränken. Wie in Abbildung 2 dargestellt, beschränkt sich die Harmonisierung auf die Schnittstellen der einzelnen Identity Provider und Service



Provider sowie auf die Kommunikationsprotokolle zwischen diesen Akteuren.

Die Liberty Alliance (www.projectliberty.org), ein Zusammenschluss von über 150 Unternehmungen, hat eine solche Architektur sowie die erforderlichen Kommunikationsprotokolle definiert und bereits entsprechende Produkte auf den Markt gebracht.

Die Praxis: Federated Identity Management bei den Schweizer Hochschulen

Einem echten Praxistest wird dieser Ansatz gegenwärtig bei SWITCH, dem «Swiss Education & Research Network», unterzogen. Den Anfang der entsprechenden Initiative markiert das Bologna Protokoll, mit welchem die Mobilität der Studierenden gefördert werden soll. Ein weiterer Treiber sind die von mehreren Hochschulen gemeinsam angebotenen e-Learning Applikationen. Die Summe dieser treibenden Kräfte gipfelt in der Vision «Enabling E-Academia» – und das konkrete Resultat ist, dass die Schweizer Universitäten und Fachhochschulen unter der Federführung von SWITCH zurzeit im Begriffe sind eine föderalistische Authentifizierungs- und Autorisierungsinfrastruktur (AAI) zu etablieren.

Die Funktionsweise der SWITCH AAI ist in Abbildung 3 dargestellt und wird im folgenden erläutert.

Um zu verhindern, dass jede Applikation ihre Benutzer selber registriert und mit einer digitalen Identität versieht, erfolgt die Registrierung nur durch jene Hochschule (Identity Provider), an welcher die Studierenden immatrikuliert beziehungsweise die wissenschaftlichen Mitarbeitenden oder Dozenten und Dozentinnen angestellt sind. Bevor Hochschulangehörige den Service einer anderen Hochschule (Ser-

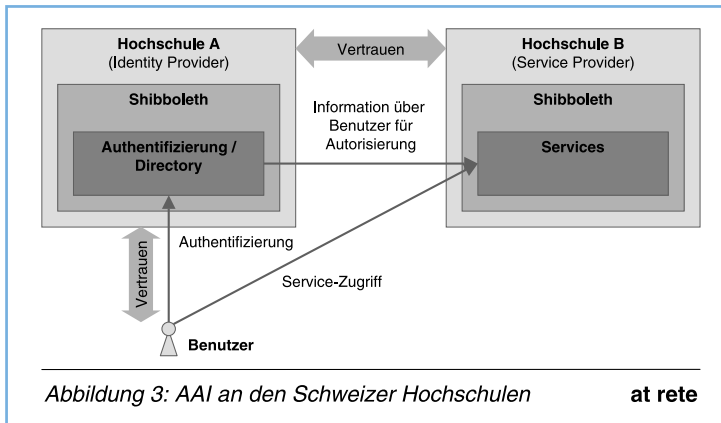


Abbildung 3: AAI an den Schweizer Hochschulen **at rete**

vice Provider) nutzen können, müssen sie sich gegenüber ihrer eigenen Hochschule authentifizieren. Diese – als Identity Provider - sendet anschliessend die Authentifizierungsbestätigung zusammen mit Zusatzinformationen über die Rolle des Benutzers an den Service Provider. Das Autorisierungssystem des Service Providers kann aufgrund dieser Information entscheiden, ob und in welcher Art der Benutzer den Service nutzen kann. Der Service Provider behält damit die vollständige Hoheit über seinen Service. Gleichzeitig wird das Vertrauensverhältnis zwischen

Am asut-Seminar vom 12. Juni 2003 in Bern wird Christoph Graf, Head of Network Security SWITCH und AAI Projektleiter, einen Vortrag halten mit dem Thema «Identity-Management Projekt der Schweizer Hochschulen – Gibt es ein Leben nach PKI?»

den Hochschulangehörigen und ihrer Hochschule, wie auch zwischen den Hochschulen untereinander auf die Beziehung zwischen allen beteiligten Hochschulangehörigen und jeder beteiligten Hochschule ausgedehnt.

Die SWITCH AAI basiert auf dem von amerikanischen Hochschulen entwickelten System Shibboleth (shibboleth.internet2.edu). Als Protokoll zwischen Identity und Service Provider wird SAML eingesetzt (Security Assertion Markup Language). Ausschlaggebend für diese Architektur waren einerseits der dezentrale Ansatz und andererseits der Erhalt der vollständigen Autonomie der Heimorganisation in der Wahl ihrer bevorzugten Authentifizierungsmethode. Da die Übertragung von Informationen vom Identity Provider an den Service Provider auf das für die Autorisierung benötigte Minimum beschränkt werden kann, sind auch die Rahmenbedingungen des Datenschutzgesetzes erfüllt. □

¹ SWITCH, The Swiss Education & Research Network, www.switch.ch

Anton Klee, lic.rer.pol., dipl. Ing. ETH, ist CEO und Partner bei at rete ag, Zürich.
André Redard, Dipl. Math. ETH, ist Senior Consultant und Partner bei at rete ag, Zürich.