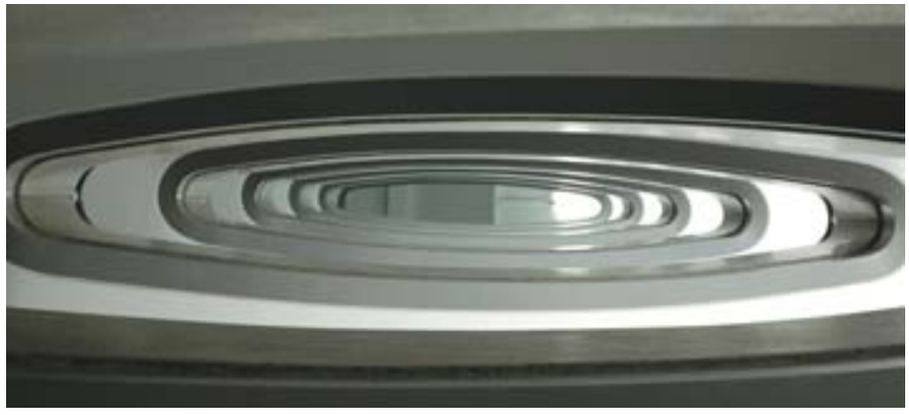
Das Dilemma mit den digitalen Identitäten

Von Daniel Muster*

Digitale Identitäten sind wegen des Datenschutzes verpönt. Jedoch vermögen sie die IT-Sicherheit und folglich auch den Datenschutz zu verbessern.



R. Künzler, Hochschule für Technik Zürich

Ein Symbol für die Angst: die endlos erscheinende Flucht eines Treppenhauses.

Grundsätzlich wird eine systematische Erfassung und Sammlung von Personenattributen in einer zentralen oder in verschiedensten Datenbanken gefürchtet, sei dies auch nur zur Identifikation der Kommunikationsteilnehmer. Daten, welche der Identifikation dienen, sind zum Beispiel Passfoto, Postanschrift, Nummer der Identitätskarte und des Passes oder die Sozialversicherungsnummer.

Allein die Erfassung der Daten, sofern sie keinen Rückschluss auf die Gesundheit, auf die Persönlichkeit oder Privatsphäre erlauben, fürchtet man weniger. Mehr Angst herrscht gegenüber dem mit der Datensammlung verbundenen Missbrauchspotenzial. Missbräuchlich wäre zum Beispiel, wenn man mit Hilfe der digitalen Identitäten alle gesammelten Daten einer Person zentral zusammenziehen und in einer einzigen, zentral administrierten Datenbank speichern und dann gezielt auswerten würde. Dabei würden auch Rückschlüsse gezogen, welche für die Betroffenen einschneidende Auswirkungen im Bereich ihres sozialen Umfeldes und ihres Alltags haben könnten. Zudem birgt die zentralisierte Datensammlung ein Klumpenrisiko bezüglich Verlust und Bekanntgabe der Daten an unberechtigte Dritte.

Die Ängste sind berechtigt und bestehen auch vor der systematischen Sammlung von DNA-Daten oder anderen ärztlichen Analyseergebnissen, welche Rückschlüsse auf Erbkrankheiten oder auf andere Gebrechen erlauben, die bei einer normalen Arztuntersuchung nicht zum Vorschein kämen.

Die Ängste vor der systematischen Sammlung von Personendaten beruhen unter anderem auch auf der bestehenden Ausgestaltung des Versicherungsvertraggesetzes (VVG). Verschweigt der Versicherungsnehmer eine bestehende, ihm bekannte Gefahr beim Antrag eines Versicherungsvertrages, so begeht er eine Anzeigepflichtverletzung. Der Versicherer hat dann das Recht den Versicherungsvertrag innerhalb von 4 Wochen nach Kenntnisnahme der Anzeigepflichtverletzung zu kündigen (Art. 6, Abs.1 und 2 VVG). Zudem kann er die Leistung bei Eintreten des damit kausal verbundenen Versicherungsereignisses verweigern (Art. 6, Abs. 3 VVG). Verschweigt der Versicherungsnehmer die Risiken nicht, hat er aber mit einer Ablehnung des Antrags, mit einer eingeschränkten Versicherungsdeckung oder mit höheren Versicherungsprämien zu rechnen.

Mangel an Regelung

Heute fehlt es beim elektronischen Geschäftsverkehr mit den Behörden (eGovernment) noch an einer einheitlich vorgeschriebenen Methode, welche Daten einer Person wie zu erfassen sind, damit man die Personen im Dschungel der Datenkommunikation identifizieren kann. Der Mangel an einer eindeutigen Identitätskennung und an einem einheitlichen Verfahren zur Bestimmung der Kommunikationsteilnehmer birgt aber das Risiko, dass jemandem irrtümlich vertrauliche und unter Umständen delikate Personendaten zugeordnet werden, welche ei-gentlich einer anderen Person hätten zugeschrieben werden müssen.

Erst eine eindeutige Identifikation ermöglicht eine vertrauliche Kommunikation. Nachrichten können zwar heute mit den bestehenden technischen Mitteln bezüglich Vertraulichkeit geschützt (verschlüsselt) übermittelt werden. Dies allein genügt jedoch nicht. Bevor vertrauliche Daten verschickt werden, ist es unerlässlich, den Empfänger zuerst zuverlässig zu identifizieren. Ansonsten riskiert man, eine vertrauliche Nachricht zwar verschlüsselt, aber an einen Unbekannten zuzustellen. Die Wichtigkeit der Identifikation wird nicht selten vergessen und schlägt sich auch in den meisten Klassifikationsschemata von Informationen nieder. Oft wird die Information nur anhand der Vertraulichkeit, nicht aber bezüglich Authentizität (Echtheit oder Richtigkeit, von wem sie stammt) eingestuft.

Ausgewogenheit technischer Mittel

Bei der Wahl der technischen Mittel zur Realisierung der Aufgaben im Identity-Management (vgl. Kasten) sollte beachtet werden, dass eine gut gesicherte Authentisierung eine sorgfältige und entsprechend gesicherte Administration der Identitätskennungen voraussetzt. Eine gesicherte Zuteilung der Rechte setzt aber vernünftigerweise wiederum eine ebenso gesicherte Authentisierung voraus. Ist die Person vorgängig nicht sorgfältig authentisiert worden, macht eine ausgeklügelte und äussert gesicherte Zuteilung der Rechte wenig Sinn.

Die eingesetzten Sicherheitstechnologien sollten auf die Sicherheitsanforderungen angepasst und in ihrer Funktionalität und in ihrem Schutzpotenzial unter den verschiedenen

R. Künzler, Hochschule für Technik Zürich

Verbindung von Digitaler ID (6), Person und Zugang.

Aufgabenbereichen abgestimmt sein. Ansonsten besteht die Gefahr, dass der Einsatz der Technologien eher unökonomisch ist.

Risiken von digitalen Identitäten

Identifizieren bedeutet eigentlich das Feststellen der Identität oder der Ablauf zur Bestimmung der Identität. Die Identität ist das Unverwechselbare und Einzigartige eines Lebewesens oder eines Objektes, wodurch es sich von allem Anderen unterscheidet.

Im Unterschied zur reellen (physischen) Welt besteht aber in der virtuellen Welt der Informatik und Datenkommunikation die Möglichkeit der Übertragung oder des Austausches von digitalen Identitäten. Also können die Geheimnisse, welche für die Authentisierung benötigt werden, und die dazu passenden Identitätskennungen an jemanden anderen übertragen oder von einem unberechtigten Dritten entwendet werden. Folglich kann nicht mehr eindeutig festgestellt werden, mit wem man wirklich kommuniziert. Ein Identifizieren (Feststellen der Identität) ist in der digitalen Welt folglich gar nicht möglich. Dies stellt wohl das fundamentalste Risiko im Bereich des Identity Managements dar.

Wegen der Übertragbarkeit der digitalen Identitäten bedeutet in der digitalen Welt die Identifikation nicht das Feststellen einer Identität, sondern das Zuordnen der Verantwortlichkeit. Deswegen sollte in einem Unternehmen auch der Umgang mit den digitalen Identitäten und die Handhabung derer Geheimelemente zur Authentisierung entsprechend in einer Richtlinie geregelt und festgehalten werden. Im elektronischen Geschäftsverkehr

Identity Management

Identity Management ist heute das Schlagwort rund um das Thema der digitalen Identitäten. Identity Management befasst sich hauptsächlich mit folgenden Aufgaben und Themen:

- Die **Administration der Identitätskennungen** beinhaltet unter anderem das Definieren der Attribute, welche für die Identifikation verwendet werden sollen, deren Prüfung, das Erfassen, Speichern in einer Datenbank und das Warten dieser Datenbank. Werden die Daten einzig für die Sicherung der Kommunikation im Privaten (zum Beispiel in einem Unternehmen) verwendet, dann stellt die Wahl der Identitätskennungen weniger ein Problem dar. Das Unternehmen kann ja grundsätzlich (im Rahmen der bestehenden Gesetze) selber bestimmen, welche Attribute wie Foto und Personalnummer sie verwenden will. Im öffentlichen Sektor (zum Beispiel im eGovernment) fehlt es jedoch an einer klaren Regelung, welche Nummern und Kennungen zu verwenden sind. Zur Verfügung stünden zum Beispiel die AHV-Nr., die ID-Nr. des Passes oder der Identitätskarte. Die bestehende AHV-Nr. hat den Nachteil, dass sie nicht eindeutig einer Person zugeordnet werden kann. Dies sollte eine neue Sozialversicherungsnummer jedoch beheben. In der heutigen Zeit bedarf es aber nicht nur einer klaren Regelung der Identitätskennungen für natürliche Personen, sondern auch einer für Server und IT-Dienste von juristischen Personen. Im Rahmen der Gesetzgebung zur elektronischen Signatur (ZertES) hätte man zumindest die verbindliche Kommunikation zu und von Servern regeln können. Diese Chance wurde aber vom Gesetzgeber damals leider verpasst.
- **Authentisierung** bedeutet den Vorgang der Identifizierung der an der Kommunikation beteiligten Partner. Diese wird meist mit Hilfe von Identitätskennungen und eines oder mehreren Geheimnissen vorgenommen. Als Identitätskennung werden Attribute bezeichnet, welche die Identifikation ermöglichen; Identifikatoren sind Attribute, die für sich allein ausreichen, damit eine Authentisierung vorgenommen werden kann.
- **Access Control** beschäftigt sich damit, wer, wie und welche Befugnisse in dem betreffenden IT-System erhält.
- **Audit** bedeutet in diesem Zusammenhang Nachvollziehbarkeit, nicht eine interne oder externe Prüfung. Zum Beispiel bei Finanztransaktionen oder bei der Buchhaltung ist es wichtig, dass zu einem späteren Zeitpunkt nachvollziehbar ist und geprüft werden kann, wer welche Transaktionen oder Buchungen wann und wie durchgeführt hat.

Wegen der Übertragbarkeit der digitalen Identitäten bedeutet in der digitalen Welt die Identifikation nicht das Feststellen einer Identität, sondern das Zuordnen der Verantwortlichkeit.

lassen sich erste Ansätze in den Haftungsbestimmungen Art. 59a OR und in den Bestimmungen im Umgang mit den Geheimelementen (Art. 11 VZertES) finden.

Fazit

Im elektronischen Geschäftsverkehr mit den Behörden (eGovernment) bedarf es einer Regelung, welche digitalen Identitäten wie einzusetzen sind und wie diese zu prüfen sind. Von der Regelung sollten nicht nur natürliche Personen erfasst werden, sondern auch die IT-Dienste und Server von juristischen Personen. Die Basis jeder Sicherheitsarchitektur in einem dezentralen Netz ist das Identity Management, wobei die Administration der digitalen Identitäten eine zentrale Rolle zukommt. ■

** Daniel Muster, Dipl. Physiker und NDS ETHZ, Hochschule für Technik Zürich (HSZ-T), Zürich*

Quellenverweis:

– *D. Muster, Digitale Unterschriften und PKI, März 2006, ISBN 3-9522387-3-3, HSZ-T*
– *OR, Schweizerisches Obligationenrecht vom 30. März 1911 betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (SR 220)*
– *VVG, Bundesgesetz vom 2. April 1908 über den Versicherungsvertrag (SR 221.229.1)*
– *VZertES, Verordnung vom 3. Dezember 2004 über Zertifizierungsdienste im Bereich der elektronischen Signatur (SR 943.032)*
– *ZertES, Bundesgesetz vom 19. Dezember 2003 über Zertifizierungsdienste im Bereich der elektronischen Signatur (SR 943.03)*