

EINLEITUNG UND ZUSAMMENFASSUNG

Die Aufgabe: Elektronisches Identitätsmanagement für alle

Immer häufiger wird von Bürgern und Verbrauchern der Nachweis ihrer Identität in elektronischen Prozessen benötigt, etwa bei Einkäufen im Internet oder beim Onlinebanking. Im "realen Leben" geschieht der Identitätsabgleich über lang etablierte persönliche Identitätskarten (Personalausweis, Reisepass, Führerschein ...) oder auch einfach durch Leisten einer i.d.R. nicht immer nachgeprüften Unterschrift.

Das Identitätsmanagement im virtuellen Raum steht dagegen noch ganz am Anfang. Dabei ist es angesichts immer wieder aufgedeckter Fälle von Datenmissbrauch – häufig trotz der Nutzung von Sicherungssystemen mit PINs und/oder Passwörtern – eine drängende Notwendigkeit, Transparenz über die Identität von Privatpersonen, aber auch von Dienstleistern aus Privatwirtschaft und Verwaltung zu schaffen und dafür eine geeignete Infrastruktur zur Verfügung zu stellen. Transparenz bedeutet dabei nicht notwendig vollständige Transparenz, sondern die Identifikation in dem Ausmaß, das für die betreffenden Anwendungen erforderlich ist.

Identitätsmanagement: Anwendungen, Funktionen und Ziele

Das Identitätsmanagement betrifft grundsätzlich zwei Bereiche:

- ¶ Erstens hochgradig sicherheitsrelevante Anwendungen innerhalb der Kernprozesse der öffentlichen Verwaltung. Hierzu gehört z.B. die sichere Identifizierung von Personen beim Grenzübertritt, bei der auch moderne biometrische Technologien zum Einsatz kommen.
- ¶ Zweitens Anwendungen im nicht hochsicherheitsrelevanten Bereich, der die meisten privatwirtschaftlichen Transaktionen und auch die meisten Interaktionen im E-Government-Bereich umfasst.

In diesem Dokument geht es ausschließlich um Identitätsmanagement im nicht hochsicherheitsrelevanten Bereich; der hoheitliche Bereich der öffentlichen Verwaltung wird bewusst ausgeklammert.

Die Funktionen des Identitätsmanagements können am Beispiel des in Deutschland für das Jahr 2010 geplanten elektronischen Personalausweises erläutert werden. Der elektronische Personalausweis wird grundsätzlich drei Funktionen zur Verfügung stellen:

1. Identifikation auf Basis biometrischer Merkmale durch ein gespeichertes Foto und (optional) Fingerabdrücke,
2. Identitätsnachweis durch elektronische Authentisierung und
3. Einsatz einer qualifizierten elektronischen Signatur.

Die beiden letztgenannten Funktionen – deren Freischaltung der Nutzer zustimmen bzw. selbst betreiben muss – betreffen den Inhalt dieses Dokuments, wobei der Schwerpunkt auf der elektronischen Authentisierung liegt. Dieser Begriff bezeichnet den Vorgang des Nachweises der Identität *beider* Partner einer Transaktion.

Das elektronische Identitätsmanagement verfolgt drei Ziele:

1. Die Authentisierung im Netz muss für alle Anwender einfach möglich sein.
2. Bürger und Verbraucher sollten die Hoheit über die Preisgabe ihrer Daten haben.
3. Die Sicherheit der Authentisierung im Netz wird immer wichtiger und muss daher verbessert werden.

Unser Diskussionsbeitrag: Acht Thesen

Mit dem vorliegenden Whitepaper stellen wir acht Thesen zum elektronischen Identitätsmanagement zur Diskussion, die das Erreichen der genannten drei Ziele im Blick haben. Das Papier liefert allerdings keine fertigen Lösungen. Unsere Absicht ist vielmehr, Stoßrichtungen für weitere Entwicklungen im elektronischen Identitätsmanagement aufzuzeigen und den Raum für Entscheidungen in Politik und Privatwirtschaft abzustecken.

Zu den wesentlichen Erkenntnissen, die wir durch unsere Analysen gewonnen haben, zählen die folgenden:

- ¶ Welche Instrumente und Infrastrukturen für das elektronische Identitätsmanagement letztlich auch ausgewählt werden, wichtig ist, dass die Bürger und Verbraucher ihnen vertrauen, sonst wird ihre weite Verbreitung an der mangelnden Akzeptanz scheitern. Außerdem müssen sie sicher und ihre Nutzung einfach sein. Essenziell ist zudem, dass sie eine breite Palette von Anwendungen abdecken. Serviceanbietern müssen sie zudem attraktive Geschäftsmodelle ermöglichen. Wo das Investment nicht lohnt, wird sich die Privatwirtschaft nicht engagieren.
- ¶ Der elektronische Personalausweis kann, muss aber nicht, eine zentrale Rolle im Identitätsmanagement übernehmen. Er könnte als Vertrauensanker für die Bürger und Konsumenten fungieren, dafür muss er aber die im erstgenannten Punkt enthaltenen Anforderungen erfüllen.
- ¶ Die entstehende Infrastruktur für das Identitätsmanagement sollte im Zielzustand grenzüberschreitend funktionieren können, damit sie den erwünschten größtmöglichen Nutzen erzielt. Nischenlösungen oder isolierte Lösungen, die sich an rein nationalen Anforderungen orientieren, helfen mittel- bis langfristig nicht weiter.
- ¶ Alle Beteiligten (u.a. Regulatoren, Datenschützer, die Industrie, Endnutzer und Nichtregierungsorganisationen) müssen bei der Einführung eines einheitlichen Identitätsmanagements an einem Strang ziehen und in institutionalisierter Form zusammenarbeiten. Erfolgskritisch für die Einführung ist außerdem der absolute Wille von Staat und Privatwirtschaft, das Projekt zum Erfolg zu führen, sowie "Leuchtturmanwendungen", anhand derer der Nutzen des elektronischen Identitätsmanagements aufgezeigt werden kann. Die Einführung sollte in jedem Fall von einer Informationskampagne begleitet werden.

Entscheidend bei all diesen Überlegungen ist die Dringlichkeit des Themas. Es darf in keinem Fall sich selbst überlassen bleiben; auch darf seine Bearbeitung nicht in die unbestimmte Zukunft verschoben wer-

den. Durch den Beschluss zur Einführung des elektronischen Personalausweises und die aktuelle Sensibilisierung der Öffentlichkeit für Themen der elektronischen Identität hat sich ein geeignetes Zeitfenster geöffnet, das es zu nutzen gilt.