ISPRAT
Interdisziplinäre Studien zu Politik, Recht, Administration und Technologie e.V.

ELEKTRONISCHES IDENTITÄTSMANAGEMENT

Mehr Einfachheit, Datenhoheit und Datensicherheit in unserer virtualisierten Welt

ISPRAT Whitepaper

Herausgeber:

Matthias Kammer (Dataport, Vorstandsvorsitzender von ISPRAT), **Marie-Therese Huppertz** (SAP, Stellvertretende Vorstandsvorsitzende von ISPRAT), **Staatssekretär Horst Westerfeld** (CIO des Bundeslandes Hessen , Geschäftsführer von ISPRAT,)

Autoren:

Dr. Dirk Graudenz (McKinsey & Company) mit Beiträgen von **Jens Fromm** (Fraunhofer FOKUS), **Michael Grözinger** (Microsoft Deutschland GmbH), **Willi Kaczorowski** (Cisco), **Dr. Anika D. Luch, Dr. Sönke E. Schulz** (Lorenz-von-Stein-Institut für Verwaltungswissenschaften an der CAU Kiel), **Andreas Pohler** (IBM Deutschland), **Dr. Angelika Steinacker** (CSC) und **Thomas Walloschke** (Fujitsu Siemens)

INHALT

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.

ELEKTRONISCHES IDENTITÄTSMANAGEMENT – NUTZEN UND NOTWENDIGKEIT

Das heutige elektronische Identitätsmanagement ist nicht mehr adäquat für die fortgeschrittene Virtualisierung der Welt

In der für die modernen Industrienationen charakteristischen Wissensgesellschaft entwickelt sich das Netz immer stärker zu einem eigenen Lebens-, Wirtschafts- und Sozialraum. Ermöglicht wird die Virtualisierung, d.h. die Verfügbarkeit von Services entkoppelt von Raum und Zeit, durch elektronische Netzwerke. Ein einfaches Beispiel für die mühelose Überwindung von Entfernungen ist der Austausch von E-Mails, ein komplexeres Beispiel sind internationale Handelsplattformen für industrielle Güter. Für die Nutzer hat die Virtualisierung viele Vorteile; dies zeigt sich nicht nur am fortschreitenden Volumen des internetbasierten Handels und Onlinebankings, sondern auch (und viel mehr) an dem Erfolg und der stetig weiteren Verbreitung von *social networking sites* wie Facebook, MySpace und Xing. Weltweit ist bereits jeder fünfte Mensch online, und dieser Anteil wird zukünftig weiter – und schnell – steigen. Die Virtualisierung zeigt sich auch darin, dass Fahrkarten durch elektronische Instrumente ersetzt werden, siehe z.B. die Oyster Card für den Nahverkehr in London. Auch der öffentliche Sektor macht immer stärker von elektronischen Transaktionen Gebrauch, sowohl bei der Kommunikation mit Privatpersonen als auch mit der Privatwirtschaft. Folgende Fakten illustrieren die aktuelle Entwicklung schlaglichtartig:

- **Hohes Volumen des Onlinehandels:** Im Jahr 2006 belief sich das Volumen des Onlinehandels in Deutschland bereits auf knapp 7% der gesamten Handelsumsätze. Mittlerweile wird hierzulande ein Drittel des Versandhandels online abgewickelt.
- **Steigendes Volumen des Internetbankings:** In Deutschland hat der Nutzerkreis des Onlinebankings im Zeitraum von 2003 bis 2007 von 21% auf 35% aller Kontoinhaber zugenommen.
- **Zunehmende Verlagerung von Dienstleistungen des öffentlichen Sektors ins Internet:** Ein Beleg dafür ist die regelmäßige

Untersuchung des Beratungsunternehmens Capgemini für die Europäische Kommission. Laut den aktuellen Ergebnissen ist die Online-Verfügbarkeit von E-Government-Services in Deutschland von 47% im Jahr 2006 auf 75% im vergangenen Jahr angestiegen.

- **Wachsendes Volumen und zunehmende Bedeutung elektronischer Transaktionen:** Neue Geschäftsmodelle (B2C und B2B), eine höhere Bereitschaft der jüngeren Generationen zu virtuellen Interaktionen und die weiter zunehmende Verbreitung mobiler Endgeräte treiben die Virtualisierung zusätzlich voran.
- **Sorgloser Umgang mit eigenen persönlichen Daten und Identitäten:** Trotz der öffentlichen Datenschutzdebatte scheint der Umgang der Anwender mit ihren persönlichen Daten und Identitäten außerordentlich unbefangen zu sein.
- **Keine anwendungsübergreifende elektronische Identität verfügbar:** Selbst verantwortungsvolle Netzbenutzer haben es schwer, sich zweifelsfrei zu authentisieren und die Vielzahl ihrer elektronischen Identitäten sicher, konsistent und datensparsam zu verwalten und nachzuweisen. Durch widersprüchliche Identitäten geht man von Wirtschaftseinbußen weltweit in Milliardenhöhe aus.

Die personenbezogenen Datenbestände wachsen kontinuierlich

Parallel zu der Virtualisierung unseres Lebensumfelds werden fortschreitend größere und detailliertere Datenbestände, die zudem immer größere Zeiträume umfassen, auf staatlicher Seite, aber auch und gerade in der Privatwirtschaft gehalten. Im Prinzip erlauben es diese Informationen, ein immer genaueres Bild des Lebens von Bürgern und Verbrauchern zu zeichnen. Kundenkarten, die mittlerweile von vielen Einzelhändlern ausgegeben werden, sind nur ein Beispiel für diese Entwicklung.

Drei Konsequenzen aus den aktuellen Trends

Aus der zunehmenden Virtualisierung und den wachsenden Datenbeständen ergeben sich drei Schlussfolgerungen:

1. **Die Authentisierung im Netz muss für alle Anwender einfach möglich sein:** Das Netz muss auch für diejenigen erschlossen werden, die es heute wegen zu hoher Komplexität oder fehlenden Vertrauens noch nicht nutzen. Da immer mehr Transaktionen ins Internet verlagert werden, sind einfache Authentisierungsverfahren erforderlich.

2. **Bürger und Verbraucher sollten die Hoheit über die Preisgabe ihrer Daten haben:** Datenhoheit ist praktizierte informationelle Selbstbestimmung und ermöglicht Datensparsamkeit, d.h. die kontrollierte Preisgabe von persönlichen Informationen. Datenhoheit schließt das Recht auf Datenfreigiebigkeit ein, selbst wenn die Offenbarung (zu) vieler Details von anderen als "unvernünftig" empfunden wird. Datenhoheit heißt auch, dass Bürger und Verbraucher ihre Instrumente des Identitätsmanagements frei wählen können. Zukünftiges elektronisches Identitätsmanagement ist eine Voraussetzung für Datenhoheit in der virtuellen Welt.

3. **Die Sicherheit der Authentisierung im Netz wird immer wichtiger und muss daher verbessert werden:** Internetkriminalität beruht häufig darauf, dass sich Kriminelle mangels eines wirksamen elektronischen Identitätsmanagements als vertrauenswürdige Institution ausgeben können. Mittelbar steigt die Online-Kriminalität, vor allem durch unerwünschte E-Mails ("Spam"). Weltweit hat der Anteil von Spam an allen E-Mails zwischen 2003 und 2007 von 33% auf 42% zugenommen – da das E-Mail-Volumen stetig wächst, entspricht dies absolut gesehen einem Faktor von 2,4. "Phishing", das Abgreifen von online eingegebenen Daten mit Hilfe falscher Internetseiten, erfolgt im Wesentlichen durch das Versenden von Spam-E-Mails. Konsequenz sind z.B. illegale "Botnets" – PCs, die ohne Wissen ihrer Eigner in Netzwerken zusammengeschaltet und für ungesetzliche Aktivitäten verwendet werden. Das "Threat Assessment 2007" von Europol zeichnet ein klares Bild: Der Anteil der Botnet-infizierten PCs steigt kontinuierlich, und Berichte über Phishing-Angriffe häufen sich. Die Angriffe werden überdies zunehmend geschickter und schwerer abzuwehren. Das gilt auch für den in Einzelfällen unternehmensintern veranlassten Missbrauch von Daten, die dem Unternehmen – z.B. in Form von Kundeninformationen – vorliegen.

8 THESEN

Auf der Grundlage der vorangegangenen Überlegungen zu den aktuellen Trends haben wir acht Thesen formuliert:

1. Moderne Industrienationen benötigen eine neue Infrastruktur für ein besseres Management von elektronischen Identitäten. Diese Infrastruktur eröffnet Chancen für Bürger, Verbraucher, Wirtschaft und Verwaltung und verringert die Sicherheitsrisiken der virtualisierten Welt.

2. Bürger und Verbraucher können nur dann für das elektronische Identitätsmanagement gewonnen werden, wenn die Nutzung der Infrastruktur einfach ist und die Verbraucher den betreffenden Instrumenten und Infrastrukturanbietern vertrauen.

3. Die Infrastruktur muss verschiedene Grade der Sicherheit und der Anonymität darstellen können.

4. Erfolgreiche Lösungen für das elektronische Identitätsmanagement basieren auf mehreren aufeinander abgestimmten Instrumenten und auf Infrastrukturfunktionen, die diesen Instrumenten zugrunde liegen. Der elektronische Personalausweis kann dabei als Katalysator eine wesentliche Rolle spielen. Das Zusammenspiel der Instrumente kann in Form eines regulierten Marktes organisiert werden.

5. Die Einführung des Identitätsmanagements kann in der Breite nur dann ein Erfolg werden, wenn es ausreichend viele öffentliche und privatwirtschaftliche Anwendungen und Geschäftsmodelle gibt, die auf der geschaffenen Infrastruktur aufbauen. Dies gilt auch für ein Identitätsmanagement auf Basis des elektronischen Personalausweises.

6. Die Infrastruktur sollte national und international interoperabel sein, damit sie den größtmöglichen Nutzen erzielt.

7. Die Zusammenarbeit der verschiedenen Stakeholder sollte, um die notwendige Verbindlichkeit zu schaffen, in einer Initiative "Vertrauen im Netz" (Arbeitstitel) institutionalisiert werden.

8. Für die Einführung erfolgskritisch sind politisches und privatwirtschaftliches Commitment, "Leuchtturmanwendungen" und eine gute Kommunikation.

These 1: Moderne Industrienationen benötigen eine neue Infrastruktur für ein besseres Management von elektronischen Identitäten. Diese Infrastruktur eröffnet Chancen für Bürger, Verbraucher, Wirtschaft und Verwaltung und verringert die Sicherheitsrisiken der virtualisierten Welt.

In der industrialisierten Welt mit der ihr eigenen Mobilität der Bürger kommt es häufig vor, dass eine Person die Leistung eines Anbieters in Anspruch nimmt, ohne dass sie ihm persönlich bekannt ist. Deshalb muss sich die Person gegenüber dem Anbieter ausweisen. In den vergangenen Jahrzehnten haben sich eine Reihe von Dokumenten für diesen Zweck etabliert: Der Blick in typische Brieftaschen fördert Führerscheine, Mitgliedsausweise, Kredit- und Bankkarten und nicht zuletzt Personalausweise zu Tage, die alle dazu dienen, die Identität einer Person in einer bestimmten Situation nachzuweisen.

Identitätsnachweise heute und morgen

Ob als Bürger oder Verbraucher – immer häufiger wird der Nachweis der Identität in elektronischen Prozessen benötigt. Während Identitätsmanagement in der dinglichen Welt über die genannten gut etablierten persönlichen Identitätskarten oder auch einfach über soziale Konventionen (z.B. durch Leisten einer i.d.R. nicht nachgeprüften Unterschrift) fest etabliert ist, steckt das Identitätsmanagement im virtuellen Raum noch in den Kinderschuhen. Um die eingangs genannten drei Ziele Einfachheit, Datenhoheit und Sicherheit der Authentisierung zu erreichen, ist es erforderlich, Möglichkeiten für das Management der elektronischen Identitäten von Bürgern und Verbrauchern – aber auch von Dienstleistern aus Privatwirtschaft und Verwaltung – zu schaffen und dafür eine geeignete Infrastruktur zur Verfügung zu stellen.

Einige Staaten haben die Herausforderungen und Chancen des Identitätsmanagements bereits erkannt und damit begonnen, geeignete Instrumente einzuführen bzw. deren Einführung zu planen.

- Österreich beispielsweise hat die e-card in Form einer Bürgerkartenfunktion der elektronischen Gesundheitskarte eingeführt, die bereits über 130.000 Bürgern eine Authentisierungs- und Signaturfunktion zur Verfügung stellt.

- In Belgien besitzen (Stand 2007) rund die Hälfte aller Bürger, die älter als zwölf Jahre sind, eine nationale eID-Karte.
- In Großbritannien soll ab 2009/10 ein System für das Identitätsmanagement etabliert werden. Im Jahr 2006 wurde bereits der "Identity Card Act" verabschiedet.
- Südkorea hat den "i-Pin"-Service zur elektronischen Authentisierung auf Webseiten eingeführt. Grund für die Einführung war die hohe Zahl von Fällen von Identitätsdiebstahl aufgrund der bisherigen Nutzung der "Citizen Registration Number".

Auch Deutschland treibt das Thema des elektronischen Identitätsmanagements mit Nachdruck voran. Mit dem Handlungsdruck aus der fortschreitenden Virtualisierung, den Anforderungen an die Online-Sicherheit, die sich in den vergangenen Jahren stetig erhöht haben, und der jüngst vom Bundeskabinett beschlossenen Einführung des elektronischen Personalausweises hat sich ein Zeitfenster geöffnet, innerhalb dessen dieses Ziel erreicht werden kann.

Welche Funktionen muss das Identitätsmanagement bieten?

Identitätsmanagement besteht aus Verfahren und Werkzeugen zur Verwaltung von personenbezogenen Daten, mit denen ein zweckmäßiger Austausch von Informationen zur Feststellung und Prüfung der Identität ermöglicht wird.

Unterstützt wird dies durch Prozesse für das Identifizieren und Registrieren von Nutzern sowie für das nachfolgende Management der Nutzeridentitäten und Berechtigungen. Schaubild 1 zeigt am Beispiel des elektronischen Personalausweises, welche Funktionen die Infrastruktur des Identitätsmanagements erfüllen muss. Grundsätzlich muss eine sichere Prozesskette vom Token (z.B. der Chipkarte), den der Benutzer hält, über die Anwendung bzw. Middleware auf Nutzerseite und die Geschäfts-/-Sicherheitslogik auf Seiten des Diensteanbieters bis zum "eID-Server" geknüpft werden. Eingebunden sind dabei Zertifizierungsdiensteanbieter (ZDAs, auch "Trustcenter" genannt), die das Authentisierungszertifikat ausgeben und prüfen oder die qualifizierte elektronische Signatur erzeugen. Wichtig ist auch die Zertifizierung der Middleware auf Seiten des

Nutzers und der Software für den eID-Server, und zwar um die Einhaltung der Sicherheitsstandards zu garantieren. Die Kommunikationsinfrastruktur wird über verschlüsselte Datenverbindungen abgesichert.

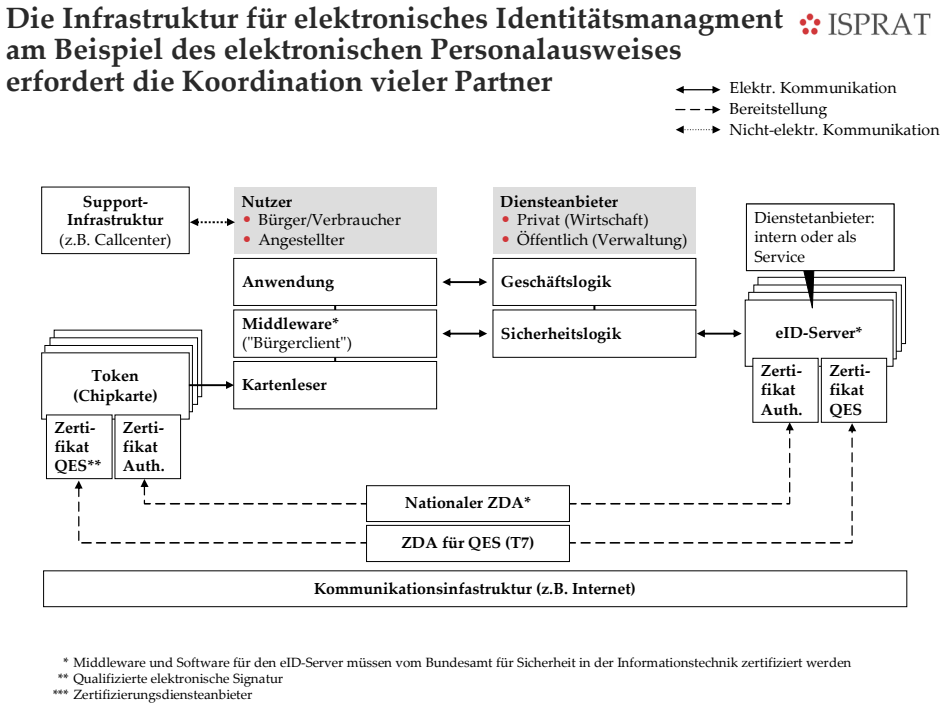

Schaubild 1: Infrastruktur für das elektronische Identitätsmanagement

Umfassende Verbesserungen dank der neuen Infrastruktur

Mit den Funktionen, die eine Infrastruktur für das elektronische Identitätsmanagement bietet, können Verbesserungen in vier Dimensionen erreicht werden:

1. **Effizienz:** Bestehende Dienste können effizienter angeboten werden; man denke nur an die Vereinfachung von Transaktionen der Verbraucher mit der Privatwirtschaft (z.B. Online-Eröffnung von Bankkonten) oder der Bürger mit der Verwaltung (E-Government-Lösungen).

2. **Qualität:** Neuartige Leistungen können angeboten werden, die einen sensiblen Umgang mit Identitäten erfordern, z.B. personalisierte Services. Bestehende Leistungen können dank der Infrastruktur in einer Form angeboten werden, die deren Nutzung

stark vereinfacht, beispielweise durch Verringerung der heute verwirrend hohen Zahl von Benutzernamen und Passwörtern.

3. **Kostenreduktion:** Bei entsprechender Vereinheitlichung der Infrastruktur oder tieferer Durchdringung der Kundenbasis aufgrund von Skalenvorteilen können Transaktionskosten vermindert werden.

4. **Risikoreduktion:** Das Risiko von Online-Transaktionen verringert sich. Hier sind zwei Aspekte relevant: Transaktionen erhalten per se eine höhere Sicherheit in dem Sinne, dass sie schwerer zu fälschen oder "abzuhören" sind. Und durch Möglichkeiten der Anonymisierung hinterlassen Bürger und Verbraucher eine geringere Datenspur – das Paradoxon ist ja gerade, dass ein hochsicheres Instrument, das zur Authentisierung dient, gleichzeitig über geeignete Verschlüsselungsverfahren auch für die Anonymisierung geeignet ist.

These 2: Bürger und Verbraucher können nur dann für das elektronische Identitätsmanagement gewonnen werden, wenn die Nutzung der Infrastruktur einfach ist und die Verbraucher den betreffenden Instrumenten und Infrastrukturanbietern vertrauen.

Das elektronische Identitätsmanagement wird nur dann Anklang finden, wenn zwei Bedingungen erfüllt sind: Der Nutzen muss offensichtlich sein, und es dürfen – gerade vor dem Hintergrund der aktuellen Diskussionen über den Datenschutz – keine Ängste bestehen, dass es ausgenutzt wird, um den gläsernen Bürger/Verbraucher Realität werden zu lassen. Der Nutzen des elektronischen Identitätsmanagements ist wiederum zweifach: Es vereinfacht die Prozesse und erhöht die Sicherheit. Spontan als besonders positiv wahrgenommen wird vermutlich die Vereinfachung von Prozessen (schnellerer Online-Einkauf o.Ä.). Der Sicherheitsnutzen dagegen ist zwar unbestritten, wird aber zu selten wirklich als offensichtlich wahrgenommen.

Einfache Nutzung

Die Einfachheit der Nutzung bezieht sich sowohl auf das unkomplizierte Beschaffen des Instruments als auch auf den möglichst geringen Aufwand bei der Durchführung von Transaktionen. Die Authentisierungs- und Signaturfunktionen des in Deutschland geplanten elektronischen Personalausweises könnten geeignet sein, um eine weite Verbreitung des Identitätsmanagements sicherzustellen und den Zusatzaufwand für die Beschaffung der Sicherheitszertifikate bei den Trustcenters zu minimieren. Transaktionen können dadurch vereinfacht werden, dass die Vielzahl verschiedener Identitäten, die der durchschnittliche Verbraucher "managen" muss, durch Nutzung einer einheitlichen Infrastruktur verringert wird.

Vertrauen der Nutzer

Die Vertrauensbildung auf Seiten der Bürger ist essenziell. Wichtig ist hierbei insbesondere, dass sie die volle Kontrolle über die Freigabe ihrer Daten erhalten und ausgeschlossen ist, dass Dritte ohne explizite Einwilligung oder Wissen der Nutzer Bewegungs-, Tätigkeits- oder Konsumprofile erstellen können. Vorkehrungen hierfür sollten in mehreren Dimensionen getroffen werden, d.h.

- **regulatorisch** durch Gesetze (in Deutschland und ggf. EU-weit) und Zertifizierungen,
- **prozessual** durch eine verteilte Datenhaltung und durch die explizite Entscheidung des Nutzers, welche Daten er freigibt,
- **wirtschaftlich** durch geeignete Betreibermodelle für Infrastruktur (Netzwerke, Trustcenter und Mehrwertdienste jeweils öffentlich, privat oder als Public-Private-Partnership) und
- **technologisch** im erforderlichen Umfang durch kryptographische Verfahren (Verschlüsselungsverfahren) zur Anonymisierung.

Zwei Dinge erscheinen bei der Vertrauensbildung von herausragender Wichtigkeit: Um Vertrauen zu bilden, sollte es einen partizipativen Prozess geben, der die wesentlichen Stakeholder einbezieht (z.B. Innen-/Justizministerium, Bürger, Datenschützer, ggf. NGOs). Vertrauen für ein Instrument kann vom Staat nur in einem Prozess eingeworben und aufgebaut werden. Zur Sicherstellung höchstmöglicher Transparenz und Nutzbarkeit sollte die Infrastruktur des elektronischen Personalausweises als offene (d.h. dokumentierte und zur Nutzung freigegebene) Plattform zur Verfügung stehen.

Regulatorischer Rahmen

Der regulatorische Rahmen kann von einer freiwilligen Zertifizierung von Serviceanbietern über eine Akkreditierungspflicht bis hin zu einer staatlichen Zulassung reichen, wobei in Abhängigkeit von den unterschiedlichen Sicherheitsanforderungen bestimmter Bereiche Mischformen vorzuziehen sind. In Anlehnung an die verschiedenen Sicherheitsstufen der elektronischen Signatur sind zumindest für besonders sensible Bereiche (Bankgeschäfte, Transaktionen mit dem Staat etc.) Mindestvoraussetzungen für den Datenschutz und die Datensicherheit zu definieren. Daneben kann ein nicht regulierter Markt bestehen bleiben, der es Anbietern und Nutzern ermöglicht, je nach persönlichem Bedürfnis "weniger sichere" Kommunikationswege zu wählen. Ähnlich wie im Kontext der elektronischen Signatur erscheint zumindest eine EU-weite, kompatible Regelung wünschenswert.

These 3: Die Infrastruktur muss verschiedene Grade der Sicherheit und der Anonymität darstellen können.

Wie in der realen Welt gibt es bei Transaktionen im Netz zwei wesentliche unabhängig voneinander auszubalancierende Dimensionen: *Sicherheit vs. Aufwand* und *Anonymität vs. Transparenz.* Sinnvoll ist es, Methoden der Authentisierung mit abgestuften Sicherheits- und Anonymitätsgraden anzubieten.

Dimension 1: Sicherheit vs. Aufwand

Unterschiedliche Sicherheitsgrade (d.h. die "Authentisierungsqualität") bedeuten einen unterschiedlichen Aufwand, sowohl zeitlich als auch finanziell – diese Form des Abwägens (Trade-off) ist aus den Wirtschaftswissenschaften wohlbekannt. Beispielsweise wird das Leisten einer justiziablen elektronischen Unterschrift aus gutem Grund als aufwendiger wahrgenommen als eine Authentisierung für den Zugriff auf ein E-Mail-Konto. Der Grundsatz sollte hier sein: So sicher wie nötig, so einfach wie möglich.

Dimension 2: Anonymität vs. Transparenz

In konkreten Anwendungen kann es genügen, bei der Authentisierung die Identität des Nutzers dem Diensteanbieter nicht vollständig preiszugeben, z.B. bei gesetzlich vorgeschriebenen Altersprüfungen für bestimmte Produkte. In anderen Fällen genügt es, die Identität zum Nutzer einer früheren Transaktion nachzuweisen, ohne die Identität selbst preiszugeben. Viele Transaktionen in der realen Welt können völlig anonym durchgeführt werden, und es gibt keinen Grund, warum dies nicht in vielen Fällen auch im Netz möglich sein sollte.

These 4: Erfolgreiche Lösungen für das elektronische Identitätsmanagement basieren auf mehreren aufeinander abgestimmten Instrumenten und auf Infrastrukturfunktionen, die diesen Instrumenten zugrunde liegen. Der elektronische Personalausweis kann dabei als Katalysator eine wesentliche Rolle spielen. Das Zusammenspiel der Instrumente kann in Form eines regulierten Marktes organisiert werden.

Eine wichtige Frage ist, wie viele verschiedene Instrumente für das elektronische Identitätsmanagement benötigt werden. Hier ist prinzipiell ein breites Spektrum von Varianten denkbar, vom Ansatz "one size fits all" bis hin zu minimaler Interoperabilität.

Anforderungen an die Authentisierungsverfahren

Folgende Anforderungen müssen alle Verfahren zur elektronischen Authentisierung erfüllen:

1. Alle Nutzer (d.h. Bürger/Konsumenten, Privatwirtschaft und der öffentliche Sektor) sollten den Verfahren **Vertrauen** entgegenbringen können.
2. Die Nutzung sollte **einfach** sein, idealerweise einfacher als die etablierten Methoden der Authentisierung im Netz.
3. Der Einsatz sollte **kostengünstig** sein, um auch bei häufiger Nutzung eine weite Verbreitung sicherzustellen und kein Instrument für die Nischennutzung zu schaffen.
4. Die Instrumente sollten technisch und prozessual eine **große Bandbreite** von Anwendungen abdecken können.
5. Die Instrumente sollten **sicher** sein, und diese Sicherheit sollte für bestimmte Anwendungen justiziabel sein.
6. Die Instrumente sollten Serviceanbietern **ausreichend viele Anwendungen und insbesondere attraktive Geschäftsmodelle** ermöglichen.

Inwiefern Szenarien diese Anforderungen erfüllen, lässt sich für die meisten dieser Kriterien anhand systematischer technischer oder betriebswirtschaftlicher Analysen beantworten – das gilt vor allem für die technische

Eignung, die Sicherheit, die Kosten und die Einfachheit. Die größte Hürde für den Einsatz eines elektronischen Identitätsmanagements dürfte jedoch die Akzeptanz seitens der Bürger sein, und damit insbesondere die Frage des Vertrauens.

Der elektronische Personalausweis als Vertrauensanker

Der elektronische Personalausweis, der zurzeit vom Bundesministerium des Innern entwickelt wird, kann im Zusammenhang mit einer universellen Lösung für das Identitätsmanagement prinzipiell eine wichtige Rolle spielen. Sein Einsatz im Identitätsmanagement setzt allerdings voraus, dass er die oben genannten Anforderungen erfüllt. Entscheidend ist auch hier die Akzeptanz der Nutzer – und sie ist nicht selbstverständlich, auch wenn die codierten biometrischen Merkmale und die hier diskutierten Authentisierungs- und Signaturfunktionen voneinander unabhängig sind. Diese Akzeptanz zu erreichen, ist eine hochgradig anspruchsvolle Aufgabe, von deren Lösung es abhängt, ob der elektronische Personalausweis ein wichtiges Instrument für das Identitätsmanagement wird oder sein Einsatz auf die Ausweisfunktion beschränkt bleibt.

Lösungsansätze im elektronischen Identitätsmanagement – vier Szenarien

Um den Lösungsraum zu beschreiben, werden im Folgenden vier Grobszenarien beschrieben und bewertet:

1. **Fokussierung auf den E-Personalausweis ("one size fits all"):** Der E-Personalausweis ist das Authentisierungsinstrument für alle Anwendungen von der rechtsverbindlichen Signatur bis hin zum Nahverkehrsticket.

   Bewertung: Die Authentisierungsfunktion des elektronischen Personalausweises ist durch die Einführung von dienste- und bereichsspezifischen Kennzeichen technisch so konstruiert, dass prinzipiell keine Tätigkeits- und Bewegungsprofile erstellt werden können. Dies wird auch dadurch unterstützt, dass bei der Verwendung des Instruments die Kommunikation direkt zwischen dem Chip des Personalausweises und dem eID-Server stattfindet, ohne "Umweg" über eine alle Diensteanbieter umfassende zentrale Infrastruktur. Unabhängig von der technischen Unmöglichkeit der Pro-

filerstellung gibt es jedoch mit hoher Wahrscheinlichkeit psychologisch erklärbare Bedenken gegen die Verwendung nur eines Instruments für alle Identitätsmanagementfunktionen im virtuellen Raum. Schon die Angst vor Verlust des in diesem Szenario einzigen Zugangs zu allen Diensten ist hoch. Dieser Themenkomplex könnte im Rahmen einer Marktforschung weiter geklärt werden.

2. **Unabhängige ID-Karte:** Eine vom E-Personalausweis unabhängige ID-Karte wird auf Wunsch der Bürger/Verbraucher zusätzlich ausgegeben; sie bietet alle unter 1. genannten Funktionen. Bürger/Verbraucher haben die Wahl, welches der beiden Instrumente – E-Personalausweis oder ID-Karte – sie nutzen.

Bewertung: Aus einem ähnlichen Grund wie 1. ist auch die Realisierung von 2. eher unwahrscheinlich, da für einen zentraler Anbieter – unabhängig davon, ob es sich dabei um die öffentliche Verwaltung oder ein privates Unternehmen handelt – eine Argumentation analog zu der nach Szenario 1 gelten dürfte.

3. **E-Personalausweis als Katalysator:** Der E-Personalausweis dient u.a. als Instrument, um andere Authentisierungsinstrumente zu erstellen/erstellen zu lassen. Ein mögliches Szenario ist, dass man sich gegenüber dritten Dienstleistern, die ggf. eigene Trustcenter betreiben, über den E-Personalausweis ausweist, um für spezifische Anwendungen jeweils eine personalisierte ID-Karte mit eingeschränkten Merkmalen erstellen zu lassen, z.B. eine Karte, die neben dem Namen lediglich einen Altersnachweis "18 Jahre oder älter" trägt, oder eine solche, die mit einem RFID-Chip ausgestattet ist und "anonyme Tokens" für Einmaltransaktionen wie Fahrten mit dem Nahverkehr oder Eintrittskarten enthalten kann. Die dritten Dienstleister hätten insbesondere die Möglichkeit des Brandings der Karten bzw. könnten für die von ihnen erstellten Karten Mehrwertleistungen anbieten. Dieses Szenario könnte in der Hinsicht erweitert werden, dass Bürger/Verbraucher den elektronischen Personalausweis freiwillig als universell einsetzbares Instrument verwenden können, sofern die betreffenden Dienstanbieter dies ermöglichen.

Bewertung: Dieses Szenario ist denkbar. Es umgeht die Schwierigkeiten aus 1. und 2. durch die Vielzahl von "dezentralen Anbietern". Die Branding-Möglichkeiten und Personalisierungen könnten attraktive Geschäftsmodelle eröffnen.

4. **Unkoordiniertes Vorgehen:** Es werden lediglich Standards für die technische Infrastruktur definiert. Der "Wert" eines bestimmten Instruments entscheidet sich in diesem Szenario im Laufe der Zeit am Markt. Insbesondere die Einschätzung der Qualität der Authentisierungen läge ausschließlich in der Verantwortung der Serviceanbieter. Der elektronische Personalausweis wäre nur ein Instrument unter vielen.

Bewertung: Auch dieses Szenario ist denkbar. Dieses Szenario ist das wahrscheinlichste, wenn keine weiteren substanziellen Anstrengungen unternommen werden. Damit würden allerdings einige der Chancen des elektronischen Personalausweises vergeben.

Zusammenspiel der Instrumente in einem regulierten Markt

"Regulierung" bedeutet, dass ein Markt von außen geprägte Grundregeln besitzt. Das können Gesetze oder Verordnungen sein oder auch Regeln, die eine geeignete steuernde Institution dem Markt vorgibt. Die Stakeholder in Szenario 3 können im Rahmen eines "regulierten Marktes" zusammenarbeiten. "Markt" bedeutet dabei: Das Gut "Identitätsmanagement" wird den Mechanismen von Angebot und Nachfrage unterworfen. Anbieter bringen Lösungen für das Identitätsmanagement (beispielsweise verschiedene Arten von Chipkarten) in Umlauf, und Nachfrager (Serviceanbieter, Bürger/Verbraucher) nutzen diese Lösungen (Schaubild 2). Die verschiedenen Leistungsmerkmale (z.B. Servicelevel und Preise) sind differenzierende Produktmerkmale.

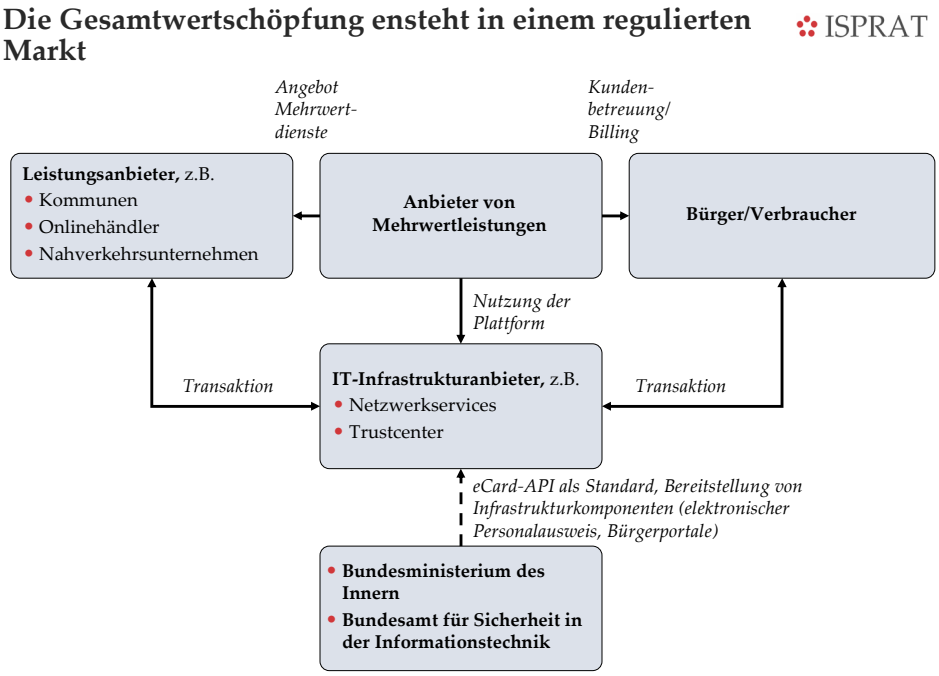

Schaubild 2: Zusammenspiel der Stakeholder im regulierten Markt

Auch Infrastrukturfunktionen können auf einem Markt angeboten werden. So können beispielsweise die bei der Beschreibung der Infrastruktur bereits genannten eID-Server von verschiedenen privaten Anbietern eingerichtet werden. Diese stellen kleineren Unternehmen, die aus Kostengründen keinen eigenen eID-Server vorhalten können, gegen geringe Transaktionskosten Authentisierungsfunktionen zur Verfügung. Analog ist es denkbar, dass zentrale Anbieter für die in Szenario 3 genannten anderen Authentisierungsinstrumente Infrastrukturleistungen zur Verfügung stellen.

These 5: Die Einführung des Identitätsmanagements kann in der Breite nur dann ein Erfolg werden, wenn es ausreichend viele öffentliche und privatwirtschaftliche Anwendungen und Geschäftsmodelle gibt, die auf der geschaffenen Infrastruktur aufbauen. Dies gilt auch für ein Identitätsmanagement auf Basis des elektronischen Personalausweises.

E-Government alleine ist kein tragfähiges Geschäftsmodell für elektronisches Identitätsmanagement: Der Erfolg des Einsatzes elektronischer Identitäten steht und fällt mit der Zahl der Nutzungen, sowohl auf der Seite der Bürger/Verbraucher als auch auf der Seite der Infrastrukturanbieter. Der Bundesbürger interagiert pro Jahr im Durchschnitt drei- bis viermal mit der Verwaltung. Eine so geringe Zahl der Interaktionen rechtfertigt nicht den Aufwand, um Millionen von Bürgern mit einem elektronischen Instrument zur Authentisierung auszustatten, so wünschenswert dies auch aus Sicht der Verwaltung und unter dem Aspekt der Effizienzerhöhung wäre. Zum Vergleich: Bankkunden führen pro Jahr durchschnittlich 70 Transaktionen mit ihren Bankkarten aus.

Nutzen der elektronischen Identitäten für die Privatwirtschaft

Für die Privatwirtschaft sind elektronische Identitäten nur dann interessant, wenn sie Geschäftsmodelle profitabler machen oder neue Geschäftsmodelle ermöglichen. Eine Profitabilisierung ist denkbar über eine Ertragssteigerung (z.B. durch höhere Transaktionszahlen), eine Kostenreduktion (z.B. durch Wegfall von proprietärer Infrastruktur zur Authentisierung) und eine Verringerung des Transaktionsrisikos. Neue Geschäftsmodelle sind beispielsweise dadurch denkbar, dass mittels elektronischen Identitätsmanagements die Identität von Verkäufern auf Handels- und Auktionsplattformen eindeutig festgestellt werden kann und die Plattformen dadurch ggf. ein Alleinstellungsmerkmal erlangen.

Erfolgsfaktor Staat

Neben der Zahl der Nutzungen bei prospektiven Anwendungen des elektronischen Personalausweises ist ein starkes Commitment seitens des Staates allerdings ein wichtiger Erfolgsfaktor. Die derzeit laufende Evaluierung für Pilotanwendungen des elektronischen Personalausweises, die vom Bundesministerium des Innern durchgeführt wird, ist dafür ein Beleg. Dank dieses Verfahrens könnten rechtzeitig zum Einführungstermin des

elektronischen Personalausweises wesentliche Erkenntnisse zu den Erfolgsfaktoren des neuen Ausweises vorliegen.

Darüber hinaus ist es möglich, durch entsprechende Kampagnen schon früh eine hohe Akzeptanz in der Bevölkerung zu erreichen. Auch bei den E-Government-Anwendungen kann der Staat Zeichen setzen. Ein Beispiel für eine erfolgreiche Einführung einer E-Government-Anwendung ist "Elster" für die elektronische Steuererklärung.

These 6: Die Infrastruktur sollte national und international interoperabel sein, damit sie den größtmöglichen Nutzen erzielt.

Infrastrukturen, die auf Standards beruhen, besitzen für die meisten Beteiligten große Vorteile. Der wesentliche Vorteil sind die Netzwerkeffekte, die sich aus der Interoperabilität ergeben, wie ein Blick auf andere Infrastrukturen zeigt: Auch die Protokollstandards des Internets, die Mobiltelefonie auf GSM-Basis in Europa, die weltweite Logistik mit normierten Containern auf dem Seeweg sowie der europäische Transport auf einem Schienennetz mit weitgehend konstanter Spurbreite basieren auf der Möglichkeit der Interoperabilität durch etablierte Standards. Standards etablieren sich im Laufe der Zeit von selbst als De-facto-Standard, werden von einem Industriekonsortium eingeführt oder von einem Gremium festgelegt.

Status quo: Einzellösungen im Identitätsmanagement

Infrastruktur besitzt den höchsten Wert, wenn sie interoperabel ist – dies gilt umso mehr, je mehr Nutzer die Infrastruktur hat. Die Lösungen, die heute schon im Identitätsmanagement eingesetzt werden, wirken dagegen eher wie Insellösungen. Das Instrumentarium ist groß – mit der Konsequenz, dass das Identitätsmanagement in Identitätssilos zersplittert ist. Hier seien nur einige Beispiele genannt:

- Fast ohne Authentisierung kommen **Kreditkarten** zum Einsatz. Hier genügen Name, Kreditkartennummer, Verfallsdatum und ggf. eine Unterschrift. Alle diese Informationen sind auf der Karte unverschlüsselt zugänglich.
- Wohl fast jeder benutzt für finanzielle Transaktionen eine **elektronische Bankkarte,** die in der Regel (aber nicht notwendigerweise, wie das Beispiel von Kreditkarten zeigt) mit einer PIN gesichert ist.
- Im Onlinebanking bzw. beim Zugriff auf andere E-Commerce-Benutzerkonten wird in der Regel eine Kombination aus **Benutzername, Passwort und** (bei Bankgeschäften) **TAN** verwendet.

- Zugang zum privaten Webmail-Account verschafft man sich in der Regel durch eine **Kombination des Namens und eines Passworts.**

- Schließlich ist beabsichtigt, durch die Einführung des **E-Personalausweises in Deutschland ein offizielles Identifikationsdokument** mit der Möglichkeit der elektronischen Authentisierung und elektronischen Signatur auszustatten. Weitere elektronische Kartenprodukte des Bundes, z.B. die elektronische Gesundheitskarte, sollen dabei technisch interoperabel sein, wie dies in den vom Bundeskabinett am 9. März 2005 verabschiedeten "Eckpunkten für eine gemeinsame eCard-Strategie" beschlossen worden ist.

Diese Zersplitterung, die sich im Laufe der Zeit ergeben hat, ist Folge der Notwendigkeit, die Anforderungen Sicherheit und Aufwand auszubalancieren, und des Fehlens einer geeigneten Infrastruktur zur Zeit, als die genannten Mechanismen eingeführt wurden.

Vorteile der Interoperabilität

Neben den positiven Netzwerkeffekten hat die Interoperabilität den Vorteil, dass Elemente der Infrastruktur wiederverwendet werden können. So sollte es beispielsweise möglich sein, dass Chipkarten von privatwirtschaftlichen Anbietern die Middleware, die in Endgeräten (in der Regel ein PC und ein Kartenleser) zwischen Chipkarte und Anwendung bzw. Chipkarte und eID-Server vermittelt, ebenso nutzen können wie dies der elektronische Personalausweis tut. Dies setzt das Einhalten von Hardware- und Protokollstandards bei den Zusatzkarten und den entsprechenden "alternativen" eID-Servern voraus. Die Wiederverwendung von Infrastruktur berührt allerdings auch den Grad des Vertrauens der Bürger/Verbraucher; hier ist eine sorgfältige Abwägung vonnöten.

Für internationale Interoperabilität ist eine Verzahnung mit bestehenden europäischen Initiativen wie STORK, PRIME und i2010 sinnvoll; diese sollte aber nicht zu Lasten einer ehrgeizigen Einführung in Deutschland gehen.

These 7: Die Zusammenarbeit der verschiedenen Stakeholder sollte, um die notwendige Verbindlichkeit zu schaffen, in einer Initiative "Vertrauen im Netz" (Arbeitstitel) institutionalisiert werden.

Die Akteure und ihre Rollen

Die Einführung eines koordinierten elektronischen Identitätsmanagements wird nur dann erfolgreich sein, wenn alle Beteiligten an einem Strang ziehen. Unter einem einheitlichen Identitätsmanagement verstehen wir ein System, in dem auf Basis von Standards die Interoperabilität verschiedener Verfahren sichergestellt wird. Insbesondere bedeutet dies, dass beispielsweise mit dem E-Personalausweis sowohl E-Government-Services in Anspruch genommen als auch sichere Online-Transaktionen mit der Privatwirtschaft getätigt werden können. Dazu müssen alle Stakeholdergruppen systematisch zusammenarbeiten. Denn obwohl es in der Regel nur zwei bis drei Hauptakteure bei jeder konkreten Transaktion gibt (beispielsweise ein Kunde, ein Serviceanbieter und ein Trustcenter), existiert im vollständigen Bild elektronischer Identitäten ein kompliziertes Geflecht von Stakeholdern, die in einer ersten Näherung acht verschiedenen Stakeholdergruppen mit nicht notwendigerweise vollständig kongruenten Zielen zugeordnet werden können: Regulatoren, Beauftragte für den Datenschutz, Standardsetzer, Infrastrukturanbieter, Endgeräte- und Softwareanbieter, Serviceanbieter, Endnutzer und NGOs (Schaubild 3). Einige der Akteure übernehmen dabei auch mehrere Rollen; der Staat beispielsweise tritt als Regulator, Standardsetzer und Serviceanbieter auf.

Schaubild 3: Landkarte der Stakeholder für elektronische Identitäten

Zusammenarbeit von Staat und Wirtschaft

Eine der wichtigsten zu schlagenden Brücken ist die zwischen öffentlichem Sektor und Privatwirtschaft: Nur durch ein Zusammenwirken können für alle Teilnehmer (öffentlicher Sektor, Privatwirtschaft und Bürger/Verbraucher) auf den elektronischen Transaktionsmärkten Verbundeffekte *(economies of scope)* realisiert werden. Das setzt einen Dialog auf allen Ebenen voraus, mögliche Themen sind dabei:

- Auf technologischer Seite muss sichergestellt werden, dass die wichtigsten Nutzungsszenarien unterstützt werden, z.B. eine einfache Form der Authentisierung mit einem hohen Grad der Anonymität bis hin zum Leisten einer rechtsverbindlichen Signatur mit einem hohen Sicherheitsgrad und dann notwendigerweise geringerer/fehlender Anonymität.
- Für den wirtschaftlichen Betrieb der Infrastruktur kann es geboten sein, dass rechtliche Regelungen den Betrieb der entsprechenden Netzwerke und Rechenzentren durch die Privatwirtschaft bzw. durch Public-Private-Partnerships zulassen.
- Zur Sicherung der Qualität, d.h. beispielsweise des Grades der Systemverfügbarkeit, der Güte der Kundenbetreuung, der Vertraulichkeit von Daten und des Niveaus der garantierten Sicherheit, ist eine unabhängige Instanz, die die Steuerung übernimmt, vorteilhaft.

Als derartige Instanz/Institution wäre für den regulierten Bereich ein Beirat o.ä. bei der zuständigen Regulierungsbehörde denkbar, um die technische und wirtschaftliche Realisierbarkeit der ggf. vom Gesetz- oder Verordnungsgeber vorgegebenen unterschiedlichen Sicherheitsniveaus sicherzustellen. Daneben könnte für den freien Markt ein Betreiberkonsortium in privatrechtlicher Rechtsform, u.U. unter Einbindung der öffentlichen Hand, Maßnahmen zur Standardisierung und Interoperabilität ergreifen und dort eine Selbstregulierung sicherstellen.

These 8: Für die Einführung erfolgskritisch sind politisches und privatwirtschaftliches Commitment, "Leuchtturmanwendungen" und eine gute Kommunikation.

Politisches und privatwirtschaftliches Commitment

Wie bei allen Infrastrukturen, die auf Netzwerkeffekten beruhen, besteht bei der Einführung grundsätzlich ein "Henne-Ei-Problem": Die verschiedenen Stakeholder im politischen und privatwirtschaftlichen Bereich warten darauf, dass der jeweils andere den ersten Zug macht – ohne akzeptable Geschäftsmodelle kein Grund zum Aufbau der Infrastruktur und ohne Infrastruktur keine Möglichkeit zur Realisierung von profitablen Geschäftsmodellen. Was die Infrastruktur angeht, sind die Voraussetzungen für das elektronische Identitätsmanagement gut, denn benötigt werden lediglich eine Chipkarte, ein Trustcenter und ein Netzwerk. Mit dem ab 2010 bei den Bürgerinnen und Bürgern eingeführten elektronischen Personalausweis kann im Prinzip innerhalb von wenigen Jahren einem signifikanten Teil der Bevölkerung eine Chipkarte zur Verfügung gestellt werden. Trustcenter sind in Deutschland in ausreichender Zahl vorhanden, und Zugang zum Internet ist hierzulande nahezu überall gegeben. Der Preis für ein Endverbraucherzertifikat für eine qualifizierte elektronische Signatur dürfte (sehr grob geschätzt) im Bereich von 15 bis 25 EUR p.a. liegen; hinzu kämen noch die einmaligen Kosten für ein Kartenlesegerät. Obwohl die laufenden Kosten lediglich 5 bis 10% des Betrags ausmachen, den Verbraucher durchschnittlich pro Jahr für ihren Internetzugang ausgeben (ca. 240 bis 360 EUR p.a.), werden Zertifikate nur dann weit verbreitet sein, wenn sie einen deutlichen Mehrwert gegenüber dem aktuellen Verfahren mit Nutzernamen und Passwort erkennen lassen.

Komplexer wird die Situation, wenn man sich die vorgeschlagene Infrastruktur vor Augen führt. Wie im Abschnitt zur These 4 (Szenarien) diskutiert, ist es unwahrscheinlich, dass die Bereitstellung nur eines Instruments ausreicht. Die Verzahnung verschiedener Instrumente erfordert allerdings die Orchestrierung verschiedener Anbieter. Unterstützt werden kann dies durch das klare Commitment seitens der Politik und der Privatwirtschaft, das Thema zum Erfolg führen zu wollen.

Leuchtturmanwendungen

Ideal wären frühzeitige und weit verbreitete "Leuchtturmanwendungen", die den Nutzen eines elektronischen Identitätsmanagements demonstrieren, d.h. in Bereichen mit sehr hohen Transaktionszahlen anzusetzen.

Zu den regelmäßigen Authentisierungen, die von Verbrauchern vorgenommen werden, gehören neben dem Einsatz der Bankkarte das Einloggen in Webmail-Programme und der Kauf von Fahrkarten für den öffentlichen Nahverkehr. Im Großraum Hamburg mit einem Einzugsgebiet von ca. 3,3 Mio. Einwohnern werden z.B. für immerhin 16% der jährlich ca. 840 Mio. Fahrten, das sind mehr als 130 Mio. Fahrten, Einzelfahrscheine gelöst. Es wäre eine spürbare Vereinfachung, wenn die jeweilige Authentisierung (Nachweis des Besitzes einer gültigen Fahrkarte) durch einfaches Auflegen einer Karte stattfinden könnte. Beim Einloggen in Webmailer sollte idealerweise eine PIN genügen. Im Bereich der öffentlichen Verwaltung könnten für die internetaffine junge Generation Services rund um das Studium interessant sein: BaföG-Beantragung, Einschreibung und Rückmeldung an Universitäten sowie Ausleihe in Universitätsbibliotheken. Nützlich wären auch Anwendungen im Kontext der EU-Dienstleistungsrichtlinie, die ein anspruchsvolles elektronisches Identitätsmanagement voraussetzt – die elektronische Antragstellung durch Dienstleistungserbringer bei den in der EU-Dienstleistungsrichtlinie vorgesehenen einheitlichen Ansprechpartnern erfordert einen Mechanismus zur einfachen Bereitstellung elektronischer Daten und Dokumente. Für typische E-Commerce-Anwendungen wie Onlinehändler und -Auktionshäuser sowie für *social networking sites* wäre zu prüfen, inwieweit hier die Transaktionsanzahl bzw. der von den Verbrauchern "gefühlte Mehrnutzen" ausreichend hoch ist; hier stellt sich auch die Frage, inwiefern ein Interessenkonflikt zwischen der Transparenz und Nutzbarkeit der Daten für die Diensteanbieter und der Privatsphäre der Verbraucher besteht.

Kommunikation

Die Einführung eines elektronischen Identitätsmanagements sollte von einer Informationsinitiative begleitet werden, bei der wesentliche Stakeholdergruppen mit den für sie entscheidenden Themen erreicht werden. Für private Anwender, Datenschützer und NGOs wären dies Themen wie Nutzungsmöglichkeiten, Sicherheit und Schutz der Privatsphäre, für Infra-

strukturanbieter, Endgeräte- und Softwareanbieter sowie Serviceanbieter die Chancen, die sich durch neue Geschäftsmodelle eröffnen.

SCHLUSSWORT

Die Privatwirtschaft und der Staat müssen das Thema elektronisches Identitätsmanagement *gemeinsam* und *umgehend* vorantreiben. Denn aktuell ist das Zeitfenster dafür aufgrund des deutlich wahrnehmbaren Handlungsdrucks aus der fortschreitenden Virtualisierung und den stetig wachsenden Anforderungen an die Online-Sicherheit sowie aufgrund der beschlossenen Einführung des elektronischen Personalausweises noch weit geöffnet. Sollte es sich schließen, bevor eine koordinierte Lösung gefunden ist, wäre die weitere Zersplitterung der Angebote kaum mehr aufzuhalten.