Digitale Identitäten

Positionspapier des Dachverbandes ICTswitzerland

1. Ausgangslage in der ‚analogen' Welt

Bürgerinnen und Bürger, Einwohnerinnen und Einwohner unseres Landes weisen sich gegenüber Behörden, Amtspersonen oder im Bedarfsfall gegenüber Geschäftspartnern (wie beispielsweise Schweizer Banken anlässlich der Aufnahme einer Geschäftsbeziehung) traditionell dadurch aus, dass sie der entsprechenden Behörde oder Person einen dokumenten- oder kartenbasierten Ausweis (Pass, Identitätskarte) oder eine amtlich ausgestellte und/oder notariell beglaubigte Ausweisschrift vorlegen.

Dieser Sachverhalt trifft unter anderem auch dann zu, wenn wir uns in traditionellen ‚Netzwerken' (wie z.B. im Eisenbahn- oder Strassenverkehrsnetz) bewegen und unsere Identität und Berechtigung fallweise, z.B. bei Kontrollen, nachzuweisen haben. Am Umstand, dass wir im Zuge solcher Kontrollen regelmässig unsere Identität ‚preisgeben', stört sich niemand, der nicht unlauteren Grund dazu hätte.

Diese Ausweise repräsentieren einerseits die Inhaberin/den Inhaber des Ausweises als Individuum und andererseits die ihre/seine Identität beschreibenden Daten und Informationen, welche in den entsprechenden Registern des Bundes, der Kantone und Gemeinden eingetragen sind und dort ordnungsgemäss geführt werden. Dasselbe trifft auf beglaubigte Auszüge aus dem Handelsregister für darin eingetragene Organisationen (z.B. juristische Personen) sowie für die Handlungs- und Zeichnungsbefugnis ihrer entsprechend registrierten Exponentinnen/Exponenten und Bevollmächtigten zu.

2. Problemstellung in der ‚digitalen' Welt

Mit der Verbreitung von Videotex, des Internet (besonders des World Wide Web) und der Mobilgeräte sowie der Nutzung netzbasierter Informationen und Dienste hat sich mit zunehmender Dringlichkeit die Frage gestellt, ob, wann und wie sich die verschiedenen Akteure (Anbieter, Intermediäre, Anwender) in Online-Interaktionen sicher und einwandfrei identifizieren (können, sollen, müssen). Dabei stand nicht die Online-Identifikation neuer, noch nicht identifizierter Kunden im Vordergrund, sondern stets nur die sichere Authentisierung und Autorisierung bestehender, d.h. bereits ‚analog' identifizierter Kunden.

In Anwendungsbereichen, welche aufgrund der Natur des Geschäftes hohe Anforderungen an Sicherheit und Überprüfbarkeit stellen (z.B. Telebanking mit Schweizer Banken), wurden diese Prozesse von Beginn weg klar geregelt. Die dafür eingesetzten Mittel und Verfahren konnten die Erwartungen der Kunden nicht immer befriedigen und wurden seither laufend verbessert. Heute gelten die meist proprietären Lösungen führender Institute als ausgesprochen sicher, robust und resistent gegen Attacken.

Für Akteure, die sich via elektronische Kanäle und in Online-Interaktionen erstmals begegnen und nicht bereits aufgrund traditioneller Ausweise oder Verfahren vorgängig identifiziert worden sind, treffen diese Feststellungen nicht zu. Um in solchen Situationen bei Bedarf oder von Gesetzes wegen trotzdem eine sichere und eindeutige Identifikation zu gewährleisten, sind entsprechende Instrumente, Mittel und Verfahren sowie allenfalls gesetzliche Grundlagen zu schaffen und Lösungen rasch bereitzustellen.

Da viele Akteure diese ‚Online-Welten' als einen *neuen und weitgehend rechtsfreien Aktionsraum* interpretieren, stören sie sich – aus welchen Gründen auch immer – am legitimen Bedürfnis der Interaktionspartner, ihre (wahre) Identität im Bedarfsfall auch in den elektronischen Netzwerken zweifelsfrei feststellen zu können (vgl. oben, Eisenbahn- und Strassenverkehrsnetz). Das Bedürfnis nach – oder gar der Anspruch auf – Anonymität oder Pseudonymität erleben mit den elektronischen Kanälen eine *gesellschaftliche Hausse*, deren Gründe zu untersuchen bleiben.

3. Digitale Identitäten in Online-Interaktionen

Um die Akteure (oder allgemeiner: die interagierenden Entitäten) in elektronischen Kanälen und Online-Interaktionen von Gesetzes wegen oder bei Bedarf eindeutig und sicher identifizieren zu können, sind *grundlegende Fragen zu klären* und *Vorkehrungen zu treffen*.

3.1 Wer bzw. was interagiert mit wem bzw. was?

- *Natürliche Personen*, also Bürgerinnen und Bürger, Einwohnerinnen und Einwohner
- *Organisationen*, z.B. juristische Personen, Unternehmen und Unternehmer, öffentlich-rechtliche Stellen, Institutionen, sowie die für sie handelnden natürlichen Personen (Exponentinnen und Exponenten, Bevollmächtigte; vgl. Ausführungen unter Kapitel 3.4 zum Thema Trust Directory)
- *Tiere*, z.B. Haustiere, die sich via Chip-Implantat und dem Animal Identity Service ANIS bei Kontrollen ausweisen lassen
- *Sachen*, z.B. Güter, die sich via passive oder aktive RFID-Chips an Lesegeräten z.B. in Transport- und Logistikprozessen ausweisen lassen
- *Elektronische Dienste*, z.B. Web Services in elektronischen Datenflüssen, die entlang digitalisierter Prozesse organisationsübergreifend miteinander interagieren

Generell ist davon auszugehen, dass in vernetzten Umgebungen moderner Informationsgesellschaften die digitale Identifikation innert Kürze zum Default der anfallenden Interaktionen wird.

3.2 Wie werden interagierende Entitäten identifiziert?

- Mit *ihnen unverwechselbar zuordnungsfähigen (eineindeutigen) Merkmalen und Informationen*, z.B. DNA-Proben, biometrische Merkmale, charakteristische Eigenheiten. Deren ‚Eineindeutigkeit' über längere Zeiträume wird von Experten unter Umständen in Zweifel gezogen, z.B. bei Mutation des Erbgutes, Umwandlung des Geschlechts, Wechsel sozialer Kontexte, Doppelbürgerschaft usw.
- Mit *Daten- und Informationssätzen, welche diese Identifikationsmerkmale und -informationen beschreiben*. Solche Datensätze können zumindest theoretisch auch ‚redundant', aber trotzdem verschieden sein, z.B. bei Doppelbürgerschaft.
- Mit *Einträgen in amtlichen Registern (Datenbanken), welche solche identitätsbeschreibende Daten- und Informationssätze enthalten und bei Bedarf ausweisen*.
- Mit *Devices* (z.B. *SmartCards, USB Tokens* etc.), auf welchen solche *identitätsbeschreibende Daten- und Informationssätze ganz, teilweise oder angereichert enthalten* sind (z.B. Bürgerkarte).
- Mit *Interfaces* (z.B. *Lese- und Eingabegeräte* z.B. an PCs oder Notebooks), welche solche *Devices* bzw. *die darauf enthaltenen Daten und Informationen lesen* können, sofern die entsprechenden Zugriffsregeln korrekt eingehalten werden.
- Mit *zusätzlichen Diensten und Verfahren* (z.B. PKI, digitale Zertifikate, digitale Signatur), welche die *identifizierte Online-Interaktion* (z.B. sichere und signierte Datenübertragung via e-Mail) gemäss Gesetz und Verordnung (z.B. ZertES) *zusätzlich (qualifiziert) sichern und ausweisen*.

3.3 Wer stellt die Infrastruktur und den Betrieb sicher?

- Die *‚ab-initio'-Feststellung der Identitäten* von natürlichen Personen (Bürgerinnen und Bürger, Einwohnerinnen und Einwohner) und von Organisationen (juristische Personen, Unternehmen und Unternehmer, Institutionen usw.), welche im Staatsgebiet der Schweiz domiziliert sind, ist eine *nicht delegierbare Aufgabe unseres Staatswesens*.
- Dies trifft auch auf die Erfassung, Führung und Bewirtschaftung der diese Identitäten beschreibenden *Daten- und Informationssätze* in den entsprechenden *Registern des Bundes, der Kantone und Gemeinden* zu. Die Harmonisierung dieser Register, Vereinheitlichung der Prozesse und Integrati-

on der Dienste in organisationsübergreifenden Abläufen ist eine dringende und prioritäre Aufgabe im Rahmen der Umsetzung der neuen E-Government-Strategie Schweiz.

- Ebenso hat das Staatswesen dafür zu sorgen, dass diese *identitätsbeschreibenden Daten und Informationen* in der Form entsprechender *Ausweise* (z.B. Pass, Identitätskarte, Handelsregisterauszug) *ausgegeben und in elektronischen Umgebungen nutzbar gemacht* werden können. Im Rahmen der Umsetzung der E-Government-Strategie Schweiz erachten wir es als dringlich und prioritär, sämtliche im Umlauf befindlichen Identitätskarten per Verfalldatum *automatisch* durch *neue ‚intelligente' Ausweise* (z.B. *SmartCards*, analog der österreichischen Bürgerkarte) zu ersetzen.
- Die Produktion und der Vertrieb solcher SmartCards kann, wie in der Privatwirtschaft üblich, durch *spezialisierte Unternehmen nach den Vorgaben und unter Kontrolle der zuständigen Bundesstellen* nach marktüblichen Tarifen erfolgen. Dasselbe gilt für Lese- und Eingabegeräte, sofern und soweit sie die entsprechenden Spezifikationen und Standards nachweislich einhalten.
- Der faktische Einsatz und die Nutzung digitaler Identitäten (oder Identifizierungsmerkmalen in Registern und auf Datenträgern) misst sich nicht an Gesetzen, Verordnungen oder am Vorhandensein von SmartCards und Interfaces, sondern an der *Verfügbarkeit nützlicher, häufig anfallender und einfach zu bedienender Dienste (Services) in den Bereichen e-Government, e-Democracy, e-Health, e-Learning sowie in anderen wichtigen Handlungskontexten* einer modernen Informations- und Wissensgesellschaft. Solche Dienste bereitzustellen oder zumindest klare Anreize für deren Bereitstellung zu schaffen, ist dringliche und prioritäre Aufgabe der Öffentlichen Hand im Rahmen der Umsetzung der bundesrätlichen Strategie für eine Informationsgesellschaft in der Schweiz.
- Der Betrieb von PKI-Lösungen und den damit verbundenen Diensten, Prozessen und Verfahren soll den dafür qualifizierten und zertifizierten Organisationen überlassen werden. Hingegen verbleibt die *Governance*, d.h. die *Überwachung der Einhaltung (adherence) der für einen einwandfreien, vertrauenswürdigen und sicheren Online-Verkehr nötigen Rahmenbedingungen durch die Akteure*, eine nicht delegierbare Aufgabe der Behörden (vgl. Sarbanes-Oxley Act sowie vergleichbare Regelungen).

3.4 Welche konkreten Entscheide sind in der Wintersession 06/07 zu treffen?

- Festlegung der *Zuständigkeiten, Aufgaben, Kompetenzen und Verantwortlichkeiten*, soweit nicht bereits geschehen, für die *Umsetzung der bundesrätlichen Strategie für eine Informationsgesellschaft in der Schweiz* (sieben thematische Dossiers, unter Befolgung der sieben Grundsätze) sowie für die *Umsetzung der neu formulierten E-Government-Strategie Schweiz* durch die dafür vorgesehenen Instanzen (Landesregierung, Departemente, Bundesämter, Steuerungsorgan, Federführer, Geschäftsstelle etc.).
- Erfassung der *neuen Sozialversicherungsnummer für natürliche Personen ab 2007* in den Registern und *automatische Ausgabe ab 2007/2008 als eindeutige digitale Identitäten in geeigneter Form auf elektronischen Identitätskarten (SmartCards)*, wie in diesem Positionspapier ausgeführt.
- Festlegung der *elektronischen Unternehmens-Identität (UID)* für Organisationen (juristische Personen, Unternehmen und Unternehmer, Institutionen usw.) *als CH-Nummern im elektronischen Handelsregister (zefix)*; laufende Nacherfassung der heute noch nicht im HR eingetragenen Entitäten (z.B. Freiberufliche, Ärzte, Landwirte) gemäss BUR (Betriebs- und Unternehmens-Register des BFS) im elektronischen HR als CH-Nummern.
- *Auslösung, Bereitstellung und operative Führung* (z.B. durch Swisscom Directories, Orell Füssli/ Teledata usw.) *eines elektronischen Trust Directory für Organisationen und deren Bevollmächtigte* (Detailkonzept liegt seit 2005 vor).
- *Information und Kommunikation* im Rahmen der Umsetzung der E-Government-Strategie Schweiz, insbesondere via eCH (Standards, Hilfsmittel, Best Practices) und eVanti.
- *Schulung, Motivation und Change Management der Leitenden und Angestellten* der Verwaltung, damit sie diese Massnahmen nicht nur ‚ertragen', sondern als Herausforderung annehmen und sich in deren rascher und kompetitiver Umsetzung – und den damit verbundenen Erfolgen – messen.

Für weitere Auskünfte und für Präsentationen stehen wir gerne zur Verfügung.

Kontaktadresse:

Markus Fischer, MF Consulting, 1789 Lugnorre FR
markus-fischer@bluewin.ch, +41 79 600 0412

Vorstandsmitglied ICTswitzerland
Mitglied Expertenausschuss eCH
Wissenschaftlicher Beirat SATW