Identity Managament und Trust
SATE-Workshop 2./3.11.2006

Prof. Dr. Reinhard Posch,
CIO des Bundes, Österreich
Wissenschaftlicher Gesamtleiter A-SIT

Identity Management ist ein zentraler Aspekt jeder automatischen Verwaltung. Verwaltung auf allen Ebenen, aber auch die Industrie hat sich des Themas in besonderer Weise angenommen. Dabei werden die unterschiedlichsten Ansätze verfolgt.

1. In punkto Sicherheit:
Hier reichen die Ansätze von Benutzerkennung und Passwort bis hin zur Chipkarte.

2. In punkto Einsatz:
Hier wird elektronische Identität in Form der elektronischen Pässe, also in passiver Weise, aber auch als aktives Element der Authentifikation genutzt.

3. In punkto Technologie:
Vom proprietären System bis zum standardorientierten Ansatz sind derzeit verschiedenste Lösungen anzutreffen. Dennoch ist das Thema wesentlich zu komplex, als dass es durch den Normalbenutzer verstanden oder durchschaut werden könnte. Der Benutzer sieht nicht ein, warum er komplexe Technologien einsetzten sollte. Er versteht auch nicht, was die Technologie überhaupt leistet und er kann nicht abschätzen, ob dadurch die behauptete Sicherheit gegeben ist.

Auch in der Industrie hat sich in diesem Bereich noch nicht wirklich eine Orientierung durchgesetzt und es erinnert die Situation in vielen Fällen an eine Art Goldgräberstimmung, wo es um Quick Wins geht, die Systematik und Nachhaltigkeit aber in vielen Fällen erst in zweiter Linie betrachtet werden.

Schließlich tragen auch die Presse und die Öffentlichkeitsarbeit durch ein Vermischen der unterschiedlichsten Facetten zusätzlich zur Desorientierung bei.

Europa benötigt einen strategischen Ansatz.

Mit dem Programm E 2010 wurde auf europäischer Ebene das „Was“ festgestellt. Das „Wie“ wird noch durch besondere Anstrengungen klarzustellen sein und wird sich in Normen, Technologien und Best Practices erst niederschlagen müssen.

Elektronische Reisedokumente sind (noch) keine elektronische Identifikation im Sinne einer eID.

Zur Darstellung von Synergien wird der elektronische Pass oft als Kernelement von elektronischer Identifikation hingestellt, und die ID-Karten werden mit elektronischen Identitäten gleichgesetzt oder zumindest gleichzeitig erwähnt und damit fast unverweigerlich verwechselt.

Dieses Umfeld benötigt daher eine nachhaltige Klärung. Identitätsdokumente sind hochwertige Mechanismen, die die Kontrolle der Identität durch die Organe ermöglichen. Sie bauen auf qualifizierter Identifikation und auf qualitätsvollem Enrollment auf. Sie sind per se aber noch keine elektronische Identifikation. Elektronische Identifikation erfordert Mechanismen, die der Benutzer zur Authentifizierung verwenden kann. In diesem Sinne sind elektronische Identifikation und die zugehörige Authentifikation etwas Aktives und nicht etwas, was durch eine dritte Person, also passiv aus der Sicht des Eigentümers der Identifikation durchgeführt wird.

Eine Synergie durch Nutzung der gleichen Hardware kann sehr sinnvoll sein, hängt aber von der Verwaltungskultur und von der Einstellung der Bürger ab. So kann etwa das Vorhandensein von biometrischen Kenngrößen wie etwa dem Fingerabdruck bereits zu einer Ablehnung der Nutzung in einigen Bereichen (z. B. im Bereich der Privatwirtschaft) führen, auch dann, wenn diese Kenngrößen im konkreten Einsatz gar nicht verwendet werden können.

eID braucht einen Träger!

Ansätze in Europa haben uns gezeigt, dass eID als Stand-alone-Technologie des E-Government nicht den notwendigen Verbreitungsgrad erreichen kann. Man muss sich eines geeigneten Trägers bedienen, der eine Basis der Installation sicherstellt, die dann elektronische Identifikation für das E-Government und in der weiteren Folge auch für die Privatwirtschaft ermöglicht. Solche Träger einer Zwei-Komponenten Authentifizierung können z. B. sein:

1. eine Identitätskarte, wenn sie entsprechend mit einem Chip ausgerüstet wird

2. eine Versicherungskarte mit der entsprechenden Chip- und Identifikationstechnologie

3. das Mobiltelefon, das mit der SIM-Karte bereits die wesentlichen Elemente der elektronischen Identifikation beinhaltet

4. eine Bankkarte, die die elektronische Identifikation dem Benutzer auch bewusst macht, die aber in vielen Fällen eine breite Palette der Identifikationstechnolgien von sehr schwachen (z.B. Magnetstreifen) bis qualitativ hochwertigen Technologien in sich vereint.

eID muss Nutzen bei Bürger und Verwaltung schaffen.

Elektronische Identifikation bedeutet „Technolgie“ und ist als solche ein Werkzeug, das den Einsatz ohne geeignete Maßnahmen an sich eher schwieriger als erleichternd erscheinen:

- *Es werden zusätzlich Hardware und Software benötigt.* Dadurch ist an sich schon eine Hürde, etwa durch den Kartenleser oder durch die entsprechenden Kartenlesertreiber und die Software, die die Karte anspricht, gegeben.

- *Es werden zusätzliche Skills benötigt.* Dies ist eine noch wesentlich größere Hürde, weil bei an sich sehr niedrigen Frequenzen im Rahmen des E-Government[1] ein Unterrichten und damit ein Erwerben derartiger Skills eine Herausforderung darstellt.

- *Technologie und Anwendung müssen aufeinander abgestimmt sein.* Damit ist eine weitere Hürde gegeben, weil die Zahl der Anwendungen in Gruppen zerfällt, die auf die entsprechenden Technologien abgestimmt sind oder aber die Anwendungen durch Unterstützung einer Vielzahl von Technologien komplexer werden.

- *eID bedeutet schließlich auch Kosten.* Diese vordergründig entstehenden Kosten sind in vielen Fällen die sichtbarste, aber in der Praxis die am wenigsten bedeutsamste Hürde.

Alle diese Hürden müssen eine geeignete Kompensation finden. Als geeignete Elemente zur Kompensation derartiger Hürden bieten sich an:

- *Erhöhen des Komforts der Anwendungen*. Dadurch, dass man sich etwa nicht pro Anwendung User-ID und Passwort merken muss, ist eine unmittelbare Steigerung des Komforts gegeben.

[1] In Österreich sind das durchschnittlich 1,7 Verwaltungskontakte pro Bürger und Jahr.

- *Steigerung der Effizienz.* Wegen der bereits angesprochenen Frequenz ist die Steigerung der Effizienz vor allem ein Element, das seitens der Verwaltung, aber kaum seitens des Bürgers als eine Bedeutung wahrgenommen werden wird.

- *Kompensation bzw. Anreizsysteme*. Die finanziellen bzw. sonstigen Mehraufwendungen müssen deutlich sichtbar und für den Benutzer einsichtig durch Vorteile kompensiert werden, damit die freiwillige und positive Entscheidung, die eine Grundvoraussetzung für einen breiten Einsatz darstellt, ermöglicht wird.

- *Sicherheit:* Wegen der Unsichtbarkeit des Elementes Sicherheit erfordert dieses in der Praxis wahrscheinlich wesentlichste Element eine besondere Anstrengung bei der Verbreitung und beim Bewusstmachen auf der Seite der betroffenen Bürger.

- *Erweiterte Funktionalität:* Hier kann man sich beispielsweise vertretungsweises Einschreiten für ältere Personen oder auch für Bekannte und Verwandte als eine wünschenswerte Funktionserweiterung sehr leicht vorstellen und auf diese Wiese auch das Thema positiv vermitteln. Es muss auch angemerkt werden, dass eID eine Fülle von Anwendungen (z.B. elektronische, nachweisliche Zustellung, sicherheitskritischere Anwendungen wie etwa den Strafregisterauszug etc.) überhaupt erst für das E-Government erschließt.

- *Flexibilität:* Bei geeigneten Strukturen ist die Flexibilität der Identifikationstechnologie wesentlich höher als die von anderen Mechanismen und es ist damit bereits ein erster Beitrag im Zusammenhang Interoperabilität auf nationaler, regionaler und internationaler Ebene gegeben.

Da Technologie im allgemeinen und in diesem speziellen Fall wertneutral ist, muss sich der Vorteil beim Benutzer und bei der Verwaltung darstellen lassen.

Sicherheit und Flexibilität sind Enabler für Komfort und Effizienz. Die Kombination mit Datenschutz und Datensicherheit kann dabei ein besonderes Grundelement sein, das zu einer speziellen Ausprägung der elektronischen Identitäten führt. Ohne in diesen Ausführungen weiterzugehen, lässt sich konkludent festhalten, dass elektronische Identifikation nur eingebettet in einer strategischen und übergreifenden planerischen Situation erfolgreich sein kann.

Dieser Schluss ist nicht nur auf nationaler Ebene, sondern auch im europäischen Umfeld zu ziehen.

Damit sind aber augenscheinlich die Aspekte der Sicherheit, der Standards und der Interoperabilität mit zu Beginn des Einsatzes von elektronischen Identifikationen Strategieanforderungen, die jedenfalls zu berücksichtigen sind.

Basierend auf derartigen Überlegungen wurde im Rahmen des Programms E 2010 die Aktivität „Large Scale Pilots“ begonnen. Als übergreifende Aktivität wird sie im CIP-Programm der EU-Kommission betreut und gefördert.

7 - 10 Mitgliedstaaten sollen einen richtungsweisenden Pilotversuch umsetzen.

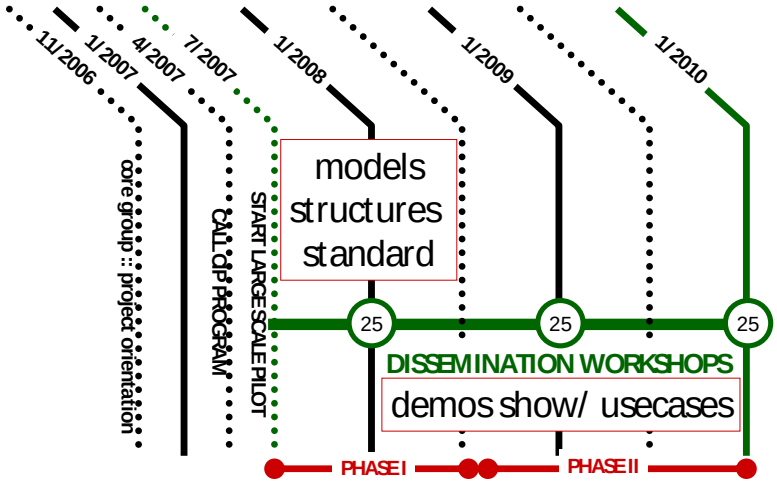
Diese Projektaktivität ist insoweit einzigartig, als die Verwaltungen nicht einfach Prototypen umsetzen können (wie das etwa im Forschungsumfeld ohne weiteres möglich ist), sondern dabei die rechtlichen und organisatorischen, aber auch die politischen Randbedingungen beachten müssen.
Aufgrund der Verwaltungskultur wird ein derartiger Pilot nicht nur die Eigenheiten eines Mitgliedstaates sondern wegen der Anforderungen an Interoperabilität auch die Besonderheiten mehrerer wenn nicht überhaupt aller Mitgliedstaaten mit ins Kalkül ziehen müssen bzw. Schritt für Schritt in diese Richtung erweitert werden. In der Praxis wird man also in einer kleinen Gruppe beginnen können und dann die weiteren Hürden in anderen Verwaltungssystemen erarbeiten und erforschen. Dabei sind folgende Bausteine von Bedeutung:

- *Das Modell der Zusammenarbeit:* Zum einen ist ein Modell, wo Interoperabilität auf der Ebene der Middleware in der Benutzerumgebung stattfindet, denkbar und erfüllt dieses auch die Anforderungen des Datenschutzes. In einem anderen Extrem kann aber auch ein System von Intermediates eine sinnvolle Lösung bieten. Langfristig - sofern man auf einen gemeinsamen europäischen Standard zuarbeitet - ist dieses Proxymodell nur eine Zwischenstufe, während das Modell der Berücksichtigung der Anforderungen in der Middleware auf der Seite des Benutzers eine umfassende Lösung darstellt.

- *Das Modell Datenschutz:* Wir haben in Europa unterschiedlichste Anforderungen. Von der einen flachen Identifikation etwa in den nordischen Staaten bis hin zur völligen Trennung der Bereiche etwa in Frankreich sind verschiedenste Ausprägungen anzutreffen. Jedenfalls müssen die national vorgegebenen Randbedingungen eingehalten werden, weil wir hier wie auch in anderen Fällen vermeiden müssen, dass Technologie die Gesellschaft prägt, sondern eher davon auszugehen haben, dass die Gesellschaft die Technologie prägen soll.

- *Elektronische Dokumente:* Die Umsetzung elektronischer Identifikation und die Integration in Verwaltungssystemen wird auch Aussagen zu elektronischen Dokumenten und zur Anerkennung bzw. zur automatisierten Verarbeitbarkeit derartiger Dokumente treffen müssen.

- *Standards:* Die wesentliche Komponente dabei werden auch das offene Umsetzen von offenen Standards und der Ausblick auf neue Technologien und auf zukünftig zu erwartende Entwicklungen sein müssen. Diese Herausforderung ist besonders schwierig zu befriedigen, da die Wege der Zukunft in der Technologie immer nur sehr unspezifisch vorhergesagt werden konnten.



Möglicher Zeitablauf der Pilotprojekte

Schließlich muss noch kurz auf die weiteren Aufgaben im Bereich Interoperabilität und eID eingegangen werden. Im Laufe des Jahres 2006 sollen jedenfalls noch die Arbeitspakete und die ins Auge gefassten Showcases bzw. Usecases unter den Mitgliedstaaten, die Interesse haben, an einem derartigen Large Scale Pilot mitzumachen, zusammengefasst werden. Zur Zeit haben sich etwa sieben Mitgliedstaaten klares Interesse signalisiert; darunter Belgien, die Niederlande, Portugal, Polen, Italien, Malta und als Präsidentschaftsland zu dem Zeitpunkt, wo die grundlegenden Überlegungen zu dieser Aktivität durchgeführt worden sind, Österreich. Weiters wird die Rolle der Industrie im Rahmen derartiger Umsetzung definiert werden müssen.