

Identity Management for e-government Use Case

1. Background

Historically, government-issued identification documents (identity cards, passports, driver's licenses, social security and medical insurance cards, etc.) started as paper-only documents. They were hard to fake because very few people had the necessary technology to manufacture, cut, print, and certify such paper documents. Over time, as forgers gained access to the necessary technologies and became more adept at falsifying papers, these documents became more and more sophisticated, resorting to special materials, filigree, watermarks, holograms, magnetic stripes, and other such harder-to-duplicate features. Today, the most advanced government identification documents contain embedded smartcards with access controls [BAC], [EAC], cryptographic functions and biometrics records. So far, the vast majority of such cards have always been and still are used exclusively "off-line", i.e. they are meant to be presented at designated service and controls points for obtaining passage or services unrelated to any on-line transactions. With suitable card readers, smartcards may be recognized and used as indices into back-end government databases for logging or verifying information. They are also, in some countries, a tool for digitally signing documents. They are also starting to be used to grant card holders access to general-purpose IT systems or applications.

At the same time, IT has become a reality that has penetrated deep into the operational infrastructure of industrial societies: activities that people used to simply do with their own physical and mental capabilities (e.g. reading a public announcement on a municipality's blackboard or buying a newspaper) are now mediated by ICT. This has led to the situation where people wishing to access information or initiate transactions via ICT systems or applications need to identify themselves in order to gain on-line access to the desired facility or service. This applies to government-provided IT facilities and services as well as to simple and complex commercial transactions.

Yet such identification happens most of the time via user-IDs and passwords that have nothing to do with existing smartcard-based electronic identification documents. Even in cases where more sophisticated and secure identification means are deployed on the IT side, (e.g. tokens, smartcard, or biometrics means,) these usually have nothing to do with already existing government identification cards. An example of an exception is the Finnish Citizen Certificate [Fin 2009], that can come in the form of a "software certificate" and can be attached to a GSM SIM card or to a government ID card. In both cases the certificate makes available a rather long list of government and non-government applications [Fin 2006]. However, such examples are rare at this point in time.

For a number of reasons government identification cards and IT system authentication mechanisms have evolved both in parallel and in isolation from one another, such that the designs supported by IT systems are simply unable to leverage existing government

identification cards. These have not been designed for that purpose and are usually owned and controlled by completely different state organizations.

2. Vision

Therein lays a shortcoming and a major opportunity, which is the foundation for the following vision: what if IT authentication systems and government-issued identification credentials were designed to serve both purposes, so that the latter could be leveraged to gain secure access to the former? What if government employees could gain access to government IT systems using their government-issued credentials to identify themselves to those systems? What if new technologies for identifying citizens could support off-line as well as internet identification, thereby allowing accountability while protecting privacy? In fact, what if consumers and employees of non-governmental organizations could use their government-issued credentials to access their employers' IT systems or any commercial e-business transaction system on the internet?

The challenge has several facets: IT systems and government-issued credentials would need to be modified to work with one another; and non-government IT systems would need to honour government-issued credentials. The former is a technical issue; the latter a trust policy issue. One element of it is referred to as identity federation; another element is the balance between governments, private enterprises and citizens. For instance, users registering at a hotel are used to presenting their government-issued IDs at check-in to gain trust from the hotel and to enable it to fulfil its legal obligations for registration. They would, however, be quite astonished if the hotel receptionist would not be able to accept their ID documents on their own merit and needed to verify them online.

Unlike government-issued credential systems, which were mostly designed and deployed from the top down, IT-based identification systems were usually designed and deployed bottom-up. Thus, national credential systems are honoured (trusted) across entire countries, or even across boundaries in the case of passports, ID cards issued in Europe, and some driver's licenses. By contrast, until a few years ago, most IT credentials were honoured (trusted) only by the organization that issued them. It has only been in recent years, in the mobile communications industry and its (GSM) roaming concepts, that the notion of federating identity systems emerged; i.e. honouring (trusting) credentials issued by one organization within another organization.

The problem is that such federation – the degree of trust across organizations – rapidly decreases with the size and heterogeneity of the federation. That is, with the number and reputation of the member organizations that decided to join together into a federation: your friends' friends are not necessarily your friends.

3. Roadmap

The challenge is, thus, to take the world from where it stands today – a mix of systems in a spectrum from global but insecure or somewhat trustworthy but non-federated IT identification systems – to where the foregoing vision would like it to be: globally

federated IT identification systems, which provide high trustworthiness through leveraging national identification systems while still respecting privacy and data protection. This can be achieved in several steps:

1) Associating electronic IT credentials with government ID documents

Firstly, electronic credentials could be associated with government-issued identification documents in such a way that they can be used for on-line identification with IT systems – initially probably government IT systems and eventually, through federation, any other IT systems. Such credentials would essentially be “software” artefacts stored on citizens’ desktops, laptops, handhelds or other portable, mobile devices such as SIM cards in a mobile phone.

2) Extending electronic IT credentials to objects and legal entities

In a second step, such credentials could be extended from people to legal entities (enterprises, organizations, etc.) and even beyond e-ID cards to “things” (sensors, devices, servers, services, etc.) representing or belonging to actual persons or legal entities. Governments already maintain registers of companies and associations, which could serve as the foundation for such purposes. Governments also usually maintain registers of cars (mobile IP carrying “things”) corresponding to car IDs, that are starting to be supported by IT. This example, especially, can serve as a major case study for examining the privacy issues.

3) Locating electronic IT credentials ON government ID documents

In a parallel step, beyond being merely associated with government-issued identification documents, such credentials could be made to reside on those documents themselves, (e.g. stored on smartcard-based ID cards, passports, driver’s licenses, insurance cards, etc.). This would make the association explicit and would ease the issuance process by avoiding the parallel issuance of software artefacts and physical documents. Obviously, experiences with the rise in complexity through these initiatives need to be considered; as does the relevance of the research needed.

4) Adding user-centric privacy-enhancing technology to government IDs

A large challenge in the above steps is the protection of citizens’ privacy. Indeed, existing government identification documents reveal much information about their holders, without allowing an opportunity to control how much data could be revealed, to whom, and/or in which circumstances. So, for instance, a typical identification document, beyond bearing an identification number and giving a person’s name, will typically provide also their birth date and place of birth, their address, and maybe even their profession; it will in fact typically display their picture and imply their gender, and implicitly suggest their nationality, etc.

As long as such documents were purely paper artefacts, a government official or anyone else presented with one could see all such information but hardly remember any of the details, especially after checking hundreds such documents in a day. With the spread of copy machines and now electronic identification documents, anyone presented with such a document can easily make a (paper or electronic) copy of it, thus leaving a detailed trace of the holder’s passage or action after the event. Access to the information on an

electronic ID card is controlled [through BAC or EAC]. However, such control is often of an all-or-nothing nature. If a person or device is authorized to read the content of such a card, they will usually be able to read all of it.

Using such electronic credentials in IT settings would be just as bad without additional controls: any IT system authorized to verify the identity of the holder of an electronic government-issued credential in the normal course of operation could potentially read and log all the personal details of that holder in the absence of additional controls. Technologies such as Microsoft's **UProve** [UProve] and IBM's **Identity Mixer** [IDMX] are emerging to restrict this potential for abuse. These schemes are user-centric, in that they are designed with the credential holder in mind rather than just the credential issuer: the holder has a means to express and limit how much information from her credential should be disclosed in any transaction with any party who requests that credential for identification. Thus, for instance, many transactions could be conducted just based on the nationality, the place of residence, the age, or the gender of a credential holder, without ever revealing her name, address, social security number or other uniquely identifying information. This preserves anonymity while guaranteeing a minimal amount of authentication based on non-unique identification attributes.

Thus, in parallel to taking the steps suggested above to leverage government-issued credentials for IT identification purposes, measures need to be taken to ensure that the privacy of citizens is adequately protected. As part of such an effort, privacy and identity governance policies must be defined and deployed to enable citizens to control what happens to their information, who can use it, for what purpose, what guarantees they have that proper controls are enforced, and what means they have to detect violations and demand damages if and when needed. A particular challenge along these lines is that defining, communicating, and agreeing/disagreeing with such policies are complex tasks, currently beyond the understanding of average citizens. Great care will have to be deployed to make such technologies practically useful and manageable by ordinary people. This will be a serious challenge beyond merely implementing the basic technologies.

5) Need for an identification meta-system

Under the assumption that there would be as many different varieties of national and state-issued electronic credentials as there are varieties of physical documents today, there is a manifest need for some standardization to ensure interoperability. This in turn suggests a need for designing a global identification meta-system; i.e. a framework (similar to the BAC and EAC standards for electronic identification cards) profiting from experience in systems for passport interoperability or GSM roaming as well as from standardisation efforts like the European Citizen Card (ECC), within which individual governments can plan and deploy their own systems, knowing that these will be able to interoperate and be federated with other systems. This is the only way to ensure that the different attributes on an electronic ID document issued by one state will be readable and understandable by card readers, computers and applications in another state.

6) Developing policy support for relying parties

Identification systems offering privacy choices are, of necessity, more complex than today's systems that do not support such functions. Specifically, such systems will

typically require interactive protocols for users and service providers to agree on the quality of identification information required for any given transaction. Thus, service providers will need to define policies, which balance the data-describing identity they require against the data or services requested. Commercial entities, (e.g. mail order houses) are used to work with available identification and authorization information and to react accordingly based on a risk assessment. This kind of experience can and will need to be expanded to other application areas where government will need to restrict requirements to the minimum necessary identification information.

The above – not necessarily sequential – six steps constitute the required foundation for a comprehensive solution to use a single set of technologies both for ID documents and IT identification purposes, thus leveraging their security and trustworthiness to enable secure and, at the same time, globally federated IT identification systems. A high level of technology neutrality is also needed, since current and future technologies will eventually be outdated and need replacement within some general framework.

Appendix A: References

[BAC] <http://eprint.iacr.org/2005/095.pdf>

[EAC] http://www.bsi.de/literat/tr/tr03110/TR-03110_v111.pdf

[Fin 2006]

www.vaestorekisterikeskus.fi/vrk/fineid/home.nsf/pages/5982EEE5795622DEC225709700387995

[Fin 2009]

www.vaestorekisterikeskus.fi/vrk/fineid/home.nsf/pages/261234746AEDB771C2257054002DB790

[IDMX]

Idemix (Identity Mixer),

<http://www.zurich.ibm.com/security/idemix/rentAcarScreenshotsAnnotated.pdf>

Jan Camenish and Anna Lysyanskaya, “Efficient non-transferable anonymous multi-show credential system with optional anonymity revocation” in EUROCRYPT 2001, vol. 2045 of LNCS, pp. 93-118, Springer Verlag 2001

Jan Camenisch and Els van Herreweghen, “Design and implementation of the idemix anonymous credential system”, in CCS ’02: Proceedings of the 9th ACM conference on Computer and communications security, 2002, ISBN 1-58113-612-9, pages 21-30 ACM, New York, NY, USA

“Made in IBM labs: IBM software to safeguard consumer identity on the web with idemix”, http://www-05.ibm.com/de/pressroom/presseinfos/2007/01/26_1.html

PRIME – Privacy and Identity Management for Europe, <https://www.prime-project.eu/>

PrimeLife - Bringing sustainable privacy and identity management to future networks and services, <http://www.primelife.eu/>

[U-Prove]

Stefan Brands, “Rethinking Public Key Infrastructures and Digital Certificates”, The MIT Press, ISBN 0-262-02491-8, first edition, August 2000, see also (http://www.credentica.com/the_mit_pressbook.html)

Stefan Brands, “Secret-key Certificates”, CWI (Centre for Mathematics and Computer Science), Amsterdam, The Netherlands, 1995

Stefan Brands, “Restrictive blinding of secret-key certificates”, CWI (Centre for Mathematics and Computer Science), Amsterdam, The Netherlands, 1995

U-Prove technology, <http://www.credentica.com/>

U-Prove SDK, http://www.credentica.com/u-prove_sdk.html

U-Prove – Unique Features, http://www.credentica.com/unique_features.html

U-Prove – Patent Portfolio, http://www.credentica.com/patent_portfolio.html