Electronic Identity Cards …

… (eID) have already been introduced in a number of countries and more are planned. Belgium and Austria, for instance, have deployed a first version of a national eID card. France, Switzerland and others are in the planning phase. Beyond eID cards, other forms of official electronic cards are also being deployed, for instance electronic drivers’ licenses in the UK.

Secondary Use

Such eID and similar cards offer not only higher security and more expedient verification in whatever scenarios they are designed for (identification or license). They also offer great potential for what is termed “secondary use”, the possibility for third parties to use them for identification or authorization in scenarios unrelated to their primary (official) intent.

eID cards could, for instance, be used by commercial enterprises, off-line or over the Internet or mobile phones, to control access to restricted facilities or services based on age, e.g. denying youth access to adult movies, DVD rentals, liquor or tobacco stores, or on the contrary denying adult access to teenagers social networking web sites, or again granting elderly people discounted access to certain facilities, such as public transportation, shows, or on-line commerce and service sites.

Privacy Threats

The uncontrolled deployment of eID or similar cards in secondary use scenarios does however present serious threats to privacy. Without remedies to these threats, public adoption of such technologies in secondary use scenarios will not happen as people will not trust the systems. In fact some of the early eID card deployments met with significant resistance from users or even criticism by the very governments that deployed them because these cards released full personal details about their users to vendors accepting them for secondary use. Released data included far more than merely the age range or other attribute that would have been sufficient. Sometimes such eID cards communicated to the vendor the owner’s national identification number, thus making it possible to track and link a consumer across multiple transactions with the same or different vendors. In some countries having deployed such eID cards, secondary use scenarios or at least use of national identification numbers in secondary use scenarios had to be legally forbidden.

If all that is necessary in some transaction is knowledge of a consumer’s age or age range or some such attribute, then that is all that should be communicated even though an eID card clearly contains much more personal information.

When a student shows an identification card to a bar tender to prove that she is old enough to buy an alcoholic beverage, the bar tender only looks at the picture and the birth date, and does not record anything. However if that same student presented her eID card as it is to order the same beverage on line, the vendor processing the order could very well not just look at and verify but even log all of the student’s personal details as they appear on her card, even though that is totally unnecessary in this particular scenario.

Protecting consumers’ privacy in secondary use scenarios will be increasingly essential because threats to privacy will be pervasive in the upcoming information age. Indeed today’s information society is less and less forgiving and forgetful. Not too long ago, the personal details that one organization could collect about one individual would typically “age out and die” as generations of applications and information systems succeeded one another. Today however society’s dependence on digital information is such that data increasingly persists through application and system migration. Information about individuals has become cumulative and it has, for instance, become practically impossible to erase or even reduce the information about oneself that is publicly discoverable through Google, much less privately held in enterprise back-end databases.

Not only does the volume of information collected about any individual accumulate but the number of systems involved in storing and processing such information is increasing, so that it becomes ever harder to keep track of where this information lives and ensure that it is properly secured against abuse by hackers or insiders determined to commit identity theft or crimes.

Finally these many systems are increasingly interconnected so that the information they contain can be linked to draw conclusions that would not have been possible without today’s degree of networking. Even when enterprises do their best to protect private consumer information, “linkability” is unavoidable: whether resulting from legitimate business needs, explicit mergers and acquisitions or otherwise desirable federation of identification systems, uneven or incomplete regulations in trans-border data flows, or accidental leaks, private individual information is and will continue to be increasingly linked in unexpected ways.

As a result it is becoming increasingly easy – legitimately or not – to track individuals through their many transactions in life. And even when individuals have nothing to hide from the Law, such linking and tracking can lead to obnoxious, indulgent, or downright criminal abuse.

Privacy Requirements

Threats to privacy are perceived differently by different cultures and civilizations. However while there is a clear global trend towards increased surveillance on one hand, there is also a clear concern about ensuring some level of privacy on the other hand. Policy makers all over the world, particularly in Europe, have started recognizing citizens’ right to privacy and
enacting corresponding privacy laws.

Governments are showing increasing interest in privacy-enhancing technologies (PETs) and starting to mandate their use in many types of applications and scenarios. Regulations in this space have become so strict that compliance can often not be achieved without resorting to PETs. Even where they are not mandated or de facto required these technologies have the potential to significantly reduce an enterprise’s exposure to accidental or malicious abuse. At the very least the deployment of PETs will be essential to ensure citizens’ confidence in information technology that is often already starting to erode.

PETs give people a choice, a means to control how much information about themselves they are willing to reveal, to whom, for what purposes and with what usage, lifetime, or other restrictions. Successful deployment of PETs does however require user education and natural, self-explanatory, user interfaces.

At the same time, one must underline that PETs are not about allowing private citizens to hide from the Law. PETs that would prevent governments – under legitimate and justified (e.g. notarized) conditions – to track people suspected of wrongdoing are doomed from their inception. The sole purpose of deploying privacy enhanced (PE) eID cards is to enable PE secondary use in legitimate circumstances, not to prevent legitimate use in legitimate circumstances. PETs are not about allowing private wrongdoing to be concealed, but rather to enable the legitimate use of personal attributes, which are not intended to be concealed.

PETs give people a choice, a means to control how much information about themselves they are willing to reveal, to whom, for what purposes and with what usage, lifetime, or other restrictions. Successful deployment of PETs does however require user education and natural, self-explanatory, user interfaces.

Privacy Solutions

The Prime Project includes in its toolbox technologies that will enable high-trust, high-security, government-issued eID cards to be leveraged in secondary use scenarios while protecting citizens’ privacy.

Using such technologies, a government-issued identification certificate guaranteeing the validity of all the personal attributes of a citizen could be safely stored onto that citizen’s eID card for PE secondary use, next and in addition to whatever restricted government information might be there for primary use.

A government itself might leverage its eID cards in primary – but privacy requiring – scenarios, e.g. elections, referendum, polls or opinion surveys in which citizenship, age, area of residence or other attributes such as gender or profession may be relevant whereas personal details such as name, national identification number, exact address or phone number are precisely not wanted.

These technologies can be seen as a complementary to existing national eID schemes and could enhance them by providing several potential forms of PE secondary use: a minimal one, a soft-extensible one, and a hard-extensible one. With the minimal solution, the stored certificate could be leveraged to allow the citizen to prove that she has any of the attributes guaranteed by the government without revealing anything about her that she did not want to in any transaction. This way no transaction would be linkable to any past or future transactions of this citizen with the same or another vendor. However only personal attributes guaranteed by the government in the original certificate can be asserted. The eID card is a read-only device in this basic scenario.

In the soft-extensible scenario, the government-issued certificate can be “federated” with other certificates issued by third parties able to vouch for other user attributes than those guaranteed by the main government-issued certificate. This would for instance allow banks or credit card organizations to certify that the citizen holds a proper bank account or credit line (without necessarily giving away the bank account or credit card number). It could also allow an employer to certify where the user works or merely that she is regularly employed. It might also enable a public transportation authority to certify that the user is entitled to board any vehicle circulating within a certain geographical region, or it may be leveraged by a wireless service provider to warrant the user access to any hot spot of a certain brand or in a certain area, etc. In this soft-extensible scenario any additional certificate delivered for such secondary use is cryptographically linked to the original government certificate in that it is guaranteed to relate to the same person. However it is not stored on the eID card. It is merely saved on some other card, cell phone, other mobile device, or even desktop station owned by the user. It is simply not possible to use such secondary certificates without presence of the original eID card in or near the device hosting them.

The hard-extensible scenario is functionally identical to the soft-extensible one, except for the fact that some number of additional secondary-use certificates may even be stored on the eID card itself, next to the original one, thus offering enhanced security and ease of use. The eID card is then a read-write card.