

# Complexity is the Achilles Heel of eID

## The Swedish eID system

Fredrik Ljunggren



Over a decade ago it became evident that there was a need emerging for secure and reliable identification of individuals over open networks, such as the Internet. Trade and services over the Internet would soon become multi-billion Euro markets. Authorities and financial and health-care institutions also realised that there were huge rationalisations to be made by handling information electronically, which required a high level of security.

To facilitate this, many people became involved in creating an electronic analogue to the physical way of signing documents and identifying oneself. These methods were laid out and standardised by the European Telecommunications Standards Institute (ETSI). The analogue builds upon the use of the X.509 standard for Public Key Infrastructure (PKI), and implies the use of X.509 digital certificates. In some parts of almost every country's legislation there are requirements relating to hand-written signatures. In these cases, legislation would have to be extended if electronic signatures are to have legal effect.

In the spirit of this, Directive 1999/93/EC of the European Parliament was produced to co-ordinate the legal status of electronic signatures across the European Union (EU). The Directive defines a framework for electronic signatures within the European Community. The extraordinary thing about this Directive is that it identifies the methods, instead of the results, which is a contradiction in the very definition of an EU directive. In the ever-changing world of computing, one can expect the methods and requirements for electronic signing and authentication to change almost constantly.

This Directive, which is mandatory for all of the Member States, has found its way into

national legislation. This was the easy part. To actually issue and use these electronic identities has proved to be much harder.

What is often overlooked is that the real-world need for electronic signatures is actually marginal. What really matters is to identify people in a safe manner. With identification we can perform the vast majority of all day-to-day business, including the offering and acceptance of contracts enforceable in a court of law – without the need for any legislation of the methods used.

When we write our final will, take out a loan or sell our house, we can still use the old fashioned way of handwriting and witnessing. With basic risk analysis, it is evident that the requirements for everyday identification are very different from those for producing advanced electronic signatures.

Unfortunately, our efforts so far have been focused on designing a universal solution to meet the most demanding requirements. The problem we were trying to solve initially stalled because we were aiming too high. The goal of reliable identification has been marginalised in favour of something we do not really need.

### The standards

The basic idea behind the X.509 PKI is to have cryptographically sound security mechanisms for authentication, signing and non-repudiation. Every individual entity in the PKI has its own key pairs (public-private), often several pairs for the different operations. For protection of the private keys, there must be 'secure signature-creation devices'. This usually implies having smart cards and using secure smart card readers.

The methods employed are those typically used within a financial institution, the military or even parts of a large private enterprise – where there is very strict control of the complete technical environment coupled with proper education of the end-users and support.

However, these methods do not work in our open Internet-based world, where security starts and ends with the end-users – the citizens and their PCs. The resulting complexity leads to services being less attractive to use. Traditional pen and paper is easier and less obstructive than the technology designed to facilitate that very service.

### A national perspective

The result of the legislation is that it has actually prevented the adoption of electronic identification instead of promoting it.

The failure is evident by looking at what has been achieved so far. After 10 years of intense bureaucracy and tens of millions of Euros, we have still not been able to implement a national eID scheme in Sweden. Even though there is a Swedish national ID card (NIDEL) capable of holding an electronic ID, it is empty. The card is basically a brick! Essentially we are at the same point now as we were a decade ago. It is clear that something is fundamentally wrong.

In the end, it is always a question of resources. What prevents the national eID scheme from being deployed on a large scale is the unreasonably high cost per operation, in relation to the benefit. The high costs preventing the adoption of the solution stem from:

- the technical complexity which calls for extensive end-user education and roll-out of special purpose end-user hardware and software
- substantial help desk costs to support end-users
- the tailoring of solutions for the single purpose of citizen-to-authority communication; relatively few operations will ever be made per eID
- the huge legal liabilities associated with the issuing of identities
- the high integration costs for the relying parties
- poor user experience – the security mechanisms are inherently insecure as people make mistakes – cases of fraud will have to be handled appropriately.

A provider of electronic identities will have to transfer all these costs, via the relying parties, to the end-users. The scheme will only be viable if these costs can be recovered from end-users.

In the current proposal for a national eID scheme in Sweden the state would perform a co-ordinating function for the authorities by purchasing the services of issuing identities from private corporations. This service is unlikely to be cheap, which would prevent any commercial application. End-users would have to pay for it with higher taxes.

In reality, therefore, the practical use of electronic identification will only happen when the tools for supporting it are significantly simplified.

### Privacy concerns

Technical complexity is not the only concern with PKI. Even if every single European citizen had his or her own national eID with three individual key pairs, an individual 'secure signature-creation device' and the education to handle it, it would be unacceptable to use it for any other purpose than in communicating with financial institutions and authorities, because of the privacy concerns it raises.

The X.509 certificate carries all the information associated with the identity, and is easily copied into a database in every imaginable situation. It can be looked up in directories, it can be eavesdropped or cross-referenced with other databases, and there is no way of selectively hiding information.

Engineers have been trying to compensate for these concerns with complicated cryptographic schemes built into the smart cards. But the functions do not fulfil their purpose; if it is not evident for the card-holders how or even if their identities are protected, then the function is not useful.

The holders of identity cards must be in control of the mechanisms that allow them to use the identification service in a safe manner. It must be evident what actually happens, what information is revealed, to whom and when. The user must be given a chance to cancel the operation before the information is revealed and, in the case of accepting an agreement or signing, to see what is actually going to be signed or agreed. These safety controls should be fulfilled by any national eID scheme.

### The way forward

Fundamentally, there needs to be a cost-benefit analysis of eID, where the costs in complexity are compared with the risks we are trying to mitigate, i.e., the benefits of a security mechanism.

In some sectors, strong cryptography, legislation and cryptographic signatures are necessary – where there are substantial risks involved that justify the use of this technology, and where the inertia and stability of a strictly controlled environment are advantages rather than deficiencies, such as in the financial sector.

However, in almost every other case, the risks do not in any way justify the costs of the qualified certificates. Given this, it would be better to design an entry-level solution for eID, which is:

- cheaper and suitable for all applications – authorities, commercial and non-profit
- easier to use and deploy
- and allows for protection of our personal data.

A good solution is to build upon the concept of identity providers – a broker of identity information which performs the identification process and relays relevant information to the relying parties. Upon successful identification in a particular context, the identity provider would issue electronic tickets for this specific context, assuring the identity of the holder, and would attach the relevant identity information. There is a unique identifier for each relationship, which cannot be cross-referenced with other relationships.

The identity provider would also be able to collect meta-information related to the subjects, such as if they are the authorised signatory for an organisation, have a medical license or are a student, or even to include a private name space for the corporation where they are currently employed. This system would allow for much greater flexibility than having separate identities for each context, as proposed by others.

Before a successful identification the user would be presented with the information agreed to be released to the relying party. At this point the user would have the option to accept or cancel, which makes it easy to fulfil legislative requirements such as Directive 95/46/EC on the protection of personal data.

Several independent identity providers can interoperate within a federation. The federation would establish policies under which identity providers should issue and handle identities. Identities within the federation would be interoperable and only the data exchange protocols would have to be co-ordinated. Such protocol already exists, e.g., the Security Assertion Markup Language (SAML) version 2, as standardised by the Organisation for the Advancement of Structured Information Standards (OASIS).

The means for users to identify themselves could vary. Different situations may require different assurance levels, which would allow users to select the technical solution that best fits their needs in every situation.

National eIDs, in the rare cases they actually exist, could be used as one. Arbitrary security tokens could also be used as long as they comply with the policy for that assurance level within the federation.

This would enable all existing and future technical solutions for identifying ourselves to be deployed, to protect an individual's identity information and preserve anonymity, while also enforcing legal responsibility for actions taken online. Both the qualified certificates and other means for identification would also be held in the same infrastructure.

Accepting agreements and contracts could be achieved by having a trusted third party, an electronic variant of notarius publicus, signing the document while asserting both parties have accepted the content. The environment provided by the trusted third party would be harder to manipulate than the end-user's PC, and would also provide a better user experience by presenting the exact contents of the agreement.

### Start simple

We should try to start simple and solve the most urgent problems first. Solutions must be designed to meet demands from all sectors and to provide the usability and protection of personal data as needed for everyday use.

Basic cost-benefit analysis can identify which technical solutions are feasible and justified. However, it is important to understand that the concept of identity providers is not mutually exclusive with the use of national eID, which would enable us to move forward in a rational way, fulfilling all the requirements for a sound and reliable solution for identification.

The certificates in a national eID scheme may be used just as any other reliable means of identification to the identity provider. End-users' methods for identification are totally transparent to the relying parties, and are therefore irrelevant. The identity provider will supply the proper protection of personal data.

Let's move forward in this rational way.

Fredrik Ljunggren ([fredrik@kirei.se](mailto:fredrik@kirei.se)) is an IT security advisor and co-founder of Kirei AB in Gothenburg, Sweden.