



More About eID Systems

Niels J Bjergstrom

Editor

If you still haven't gotten around to reading LSE's report into the UK government's Identity Project you can fetch it here:

<http://is.lse.ac.uk/idcard/identityreport.pdf>

It's a bit over 300 pages long and fascinating reading. It concludes – like earlier editorials in ISB – that the proposed project is *not feasible*, saying that the proposals are *too complex, technically unsafe, overly prescriptive* and *lack a foundation of public trust and confidence*. LSE's report also concludes that *the risk of failure in the current proposal is therefore magnified to the point where the scheme should be regarded as a potential danger to the public interest and to the legal rights of individuals*.

I will add to this that the proposals are particularly unimaginative. Given a blank slate for such a fascinating potentially future-shaping project, is this really the best vision politicians and government employees can come up with?

The whole approach to this project is reactive rather than forward-looking and proactive. The justifications for introducing a national identity system in the Bill include 'the interest of national security', 'the enforcement of prohibitions on unauthorised working', 'enforcement of immigration controls' and 'prevention and detection of crime'.

These goals seem to be missing: 'enabling and facilitating a society based on e-commerce', 'increasing individual freedom by enhancing anonymity and privacy', 'enabling irrefutable authentication of humans to machines' and 'providing individuals with transactional security'. These are some of the *positive* drivers of an eID system, some of the drivers that will actually be able to underpin the acceptance by the public and justify the huge expenses initially associated with establishing and not least running an eID system. I also think that the positive drivers are better predictors of a positive ROI of such a project. In fact I think it will be quite easy to demonstrate a high likelihood of a positive ROI if you follow the path of analysing the potential benefits of an eID system rather than focussing on the preventive measures you can tie to such a system like the legislation does.

For a moment, let us look at the concept of *identity*. What is an identity? Well, a person normally has a whole range of different identities: the 'IT trouble-shooter' on the job, the 'regional champion' in the go-kart club, 'Mrs. Smith' in the GP's office, etc. Thus, identities are *context-specific*. They are maintained by individuals as social and economic players in society.

How can one substantiate a claim to a particular identity? By having an employee badge at the job, a membership card in the go-kart club and a National Security card at the medical centre, for example. In other words, by authenticating yourself. An identity can only be substantiated through authentication. This again implies some sort of enrollment process: in order to acquire an identity in a given context you need to enroll. In the UK most identities are based on being able to show documents such as a driving license or utility bills, i.e. resting on an earlier enrollment and its ensuing identity. At the bottom of this hierarchy somebody witnesses a birth and testifies to the fact: Mrs Jones has had a baby girl (who later married Mr. Smith but that is an added complication). Somebody issues a birth certificate, which is recorded by the local registrar of births.

EDITORIAL

In the 21st century this is of limited use. Even if someone carries her birth certificate it suffers from two problems:

- the carrier of the document can't prove the connection between the piece of paper and herself
- machines are not very good at reading paper documents, so authenticating on the basis of a birth certificate always requires human intervention (a man-in-the-middle) and at the end of the day, some other kind of authentication

In a digital world what we need is an irrefutable electronically readable document that can serve as a 'digital birth certificate', without the problems of the paper one, in other words, a *Root Identity*.

This, I would argue, should be the main line of thought when designing an eID system. The eID must serve as a Root Identity.

If you adopt this line of reasoning you find that in order to function in this capacity the eID must have some specific properties:

- it must be able to bind out to other processes
- it must specifically be able to facilitate an irrefutable link between its user and itself.
- it must be able to participate in *authorisation* procedures, in my view without leaking any identity information – helping to answer the question: *is this individual allowed to do this in this context?* In most cases you do not need *identification* to answer this type of question.
- it should be able to facilitate *authentication* processes without compromising identity – allowing anonymity or pseudonymity most of the time is a fundamental requirement of any eID system in a free society
- it should be able to uniquely represent the legitimate holder (and only the legitimate holder) in public key cryptographic protocols – a consequence of the two above
- it should be able to participate in identification processes if identification is required and legitimate
- it must not depend on irreplaceable personal characteristics, in the sense that the system as such must be able to cope with the problem of compromised characteristics
- the token containing the eID must be replaceable without unwanted consequences, or as a corollary, theft or loss of a token must not enable impersonation
- all its functions, including any disclosure of information in the token, must be fully controlled by the owner

There are more necessary factors but I don't have space to write a book about it here.

Several problems are in evidence here. The issue of irrefutability is not easy. It basically implies that a given token can only function in connection with one particular individual on the planet, and it must not be able to function unless it is provably authorised to do so by that individual.

The system must not rely so heavily on any particular personal characteristic that a compromise or loss of

that characteristic (amputation of a finger for example) makes it impossible for the individual to participate.

Both these two problems point at biometric solutions and how these are used. The thing is that unless the token and the person can be irrefutably tied together, an eID is no worse and not much better than a birth certificate and the whole exercise a waste of time and money. To create this tie you need to use some suitable biometric. There are not many of those – universally usable across races, constant with age, replaceable in case of compromise or loss – in fact I can only think of one: DNA. If you want to know more about how DNA can be used as the basis of eIDs without leaking information or compromising personal details, look at the presentation/paper I gave at InfoSeCon 2005 in Dubrovnik last June. There is no real alternative.

Don't get me wrong here. Using DNA analysis on a day-to-day basis is not technically feasible, not desirable. However, for an eID to really constitute a Root Identity DNA must be included (establishing a correct database begins at birth and takes a generation). I suggest this be used mainly in case an individual needs other types of biometrics updated or installed on her eID. This information should not be stored in any database and it doesn't have to be. It is sufficient to store a cryptographic value derived from the information.

The whole system must be as decentralised as possible, building on information inside the eID token. Implementations interfacing to the eID system must be subject to strict risk analysis, so that the level of credential asked for is proportional to the risk involved per transaction. Otherwise it gets far too expensive because in many cases multiple biometrics must be used.

With regard to the UK bill I am not going to argue with it here although technical issues aside – it certainly is an obnoxious piece of legislation, moving the relationship between state and citizen several hundred years back, introducing important components of a totalitarian state by stealth – the ID card part is in a way the least important. It is a piece of legislation that does not belong in a democratic country.

Technically, it builds on a range of false assumptions, including the pie-in-the-sky idea that technologies to solve these issues exist and can be deployed. This is not the type of project you can simply give to a vendor or two and expect them to be able to deliver. More than anything I can recall ever seeing, this project requires a top-down architectural design process. It is not a vendor-problem that you can throw existing components at. This problem is so complex that it requires close co-operation between scientists, government and vendors. It will take a small extremely competent work group at least a year to identify possible solutions and consequences.

Unfortunately the current bill is so poorly drafted that it can't form the basis for discussion and amendment – back to square one. Normally that would make me complain bitterly over waste of my tax money but in this case there are only a handful of people in the world competent to do it right. Those are the individuals the UK government needs to find.

I think I know the people who can design and produce most of the deliverables but who asks the old editor?

For further light reading, see <http://www.idcorner.org>