National e-ID Card Schemes: An Overview

The UK is one of a few countries that does not have a national ID card scheme. This thesis takes a closer look at why.

BY SIDDHARTHA ARORA AND DR. MICHAEL GANLEY

Royal Holloway
University of London

Produced by the Information Security Group at Royal Holloway, University of London in conjunction with TechTarget.

SUMMARY BOX

- Supporting digital signatures and e-Government applications are the key drivers for e-ID card schemes across Europe (UK being an exception)
- e-ID card schemes across Europe differ significantly in implementation, primary motivations and policy drivers
- Barriers to significant adoption include lack of support and participation by the private sector
- Interoperability between schemes is an unaddressed technical and policy challenge
- Human error remains the greatest risk associated with vulnerabilities of e-ID card schemes

Siddhartha Arora

Information Security Group, Royal Holloway, Egham, Surrey, U.K.

Dr. Michael Ganley

Information Security Group, Royal Holloway, Egham, Surrey, U.K.

National e-ID Card Schemes: An Overview

National identity cards, most notably e-ID cards, are getting of lot of press coverage at the moment. But what is the motivation for these cards being implemented across Europe? How important is it to have a unique card? What role does a national e-ID card have in the private sector? Are e-ID cards already finding any application usage? What risks exist and what future areas of e-ID cards need to be addressed?

This paper is the result of an Information Security MSc thesis project recently completed at Royal Holloway, University of London. The objective of the project was to take a closer look at electronic identity (e-ID), especially in the context of national e-ID card schemes across Europe. While the main focus of the project was to better understand the meaning of the national e-ID card and the main (policy) drivers and objectives, together with their present key applications and those in the future, the most interesting outcome of

This article was prepared by students and staff involved with the award-winning M.Sc. in Information Security offered by the Information Security Group at Royal Holloway, University of London. The student was judged to have produced an outstanding M.Sc. thesis on a business-related topic. The full thesis is available as a technical report on the Royal Holloway website http://www.ma.rhul.ac.uk/tech.

For more information about the Information Security Group at Royal Holloway or on the M.Sc. in Information Security, please visit http://www.isg.rhul.ac.uk.

the project was to identify some of the key lessons learned from today's e-ID card schemes – their present shortcomings as well as some success stories.

The UK and Ireland are the only countries in the European Union without a national identity card scheme, and the rest of Europe is still at a very early stage of development, and despite numerous initiatives, there is no coordinated effort across Europe to implement e-ID cards. This has led to a heterogeneous collection of scheme types, leading to a general lack of interoperability between schemes.

ELECTRONIC IDENTITY

Before the internet became widely used by the general public, *The New Yorker* magazine published a cartoon by Peter Steiner of two dogs sitting in front of a computer workstation. One dog says to the other *"On the Internet, nobody knows you're a dog."* It is an example illustrating the challenges facing proving one's identity in a distributed systems environment. In today's context, e-ID cards are seen as a mechanism to address some of these challenges.

One of the earliest references to basic e-ID functions was made by Fiat and Shamir at the CRYPTO '86 conference [1], where they illustrated the limitations of not using e-ID technology. These were:

- Passports could be photocopied by hostile governments
- Credit card numbers could be copied
- Passwords would be vulnerable to hackers and wire-tappers

Fiat and Shamir were the first to define[1] what are now commonly understood as the three basic forms of protection to be offered by e-ID cards: I-A-S

Identification (I)	A can prove to B that he is A, but someone else can not prove to B that he is A.
Authentication (A)	A can prove to B that he is A, but B can not prove to someone else that he is A.
Signature (S)	A can prove to B that he is A, but B can not prove to himself that he is A.

Source: [1]

There seem to be three key drivers why e-ID cards have recently received prominent attention:

- **E-Passports** - There are political and legal pressures to implement electronic passports, also known as e-Passports, which are considered next-generation passports. They are mandated by the UN's International Civil Aviation Organisation (ICAO) Document 9303, which defines how smart cards and biometrics should be integrated into the e-Passport to make them even more machine-readable and secure than today.

- **EU Electronic Signatures Directive** - The 1999 European Directive on Electronic Signatures has led to various initiatives both at pan-European and national levels to enable this directive to be realised. Specifically, an e-ID card with a built-in smart card can act as a Secure Signature Creation Device (SSCD).

- **Extend existing ID cards to support new functions** - National initiatives to define and deploy more advanced and secure identity cards (independent of the EU directive) have led many governments to review their existing ID cards with the aim of adding features to make it meet more of the I-A-S functions.

An occurrence of all the policy drivers at the same time has caused some confusion with the realisation of their objectives. In fact, whilst some of the base technology, such as smart cards, is the same, the challenges and primary functions of passports are from the onset very different to those of identity cards. Passports are primarily seen as a border control document, while the national identity card has multiple identification purposes, including being used for authentication and signature purposes. Hence, this paper will focus only on the e-ID card in a national identity card context, and not address the e-Passport.

In general, the e-ID cards are designed by various government ministries, with limited participation from the private sector. One might think that using a national e-ID card, for example for digital signing purposes, might be a useful application for the private sector. The designers of today's national e-ID cards do not necessarily see this to be the case. A list of supported applications (almost always e-government applications) is proof of this. An example of where a national e-ID card from the initial design phase had private-sector participation was the Malaysian e-ID card. The private-sector participation in the design helped in supporting non-e-government applications from the beginning. As a result, the adoption and

In general, the e-ID cards are designed by various government ministries, with limited participation from the private sector.

general usage of the e-ID cards was higher, hence providing a greater utility to the general public.

Even within a pan-European context, the e-ID card is seen as a driver to address government, rather than private-sector objectives. Common objectives for an e-ID card include:

- Address common and global identity fraud
- Address national and pan-European anti-terrorism measures
- Build a more “inclusive” European society (creating a European Identity)
- Stimulate the emergence of new “intra-European” services to reduce costs of infrastructure (efficiency gains)

The limited private sector participation might be explained by a lack of government policies to involve them in the design and deployment. However, this might change, as various countries start rolling out their e-ID cards and the private sector finds innovative means to use the cards for secondary use scenarios.

E-ID CARDS AND PRIVACY

In an identity management context, privacy can be seen to address four characteristics, discussed in more detail by Pfitzman and Hansen[2] and defined in the ISO 15408 standard[3]:

Anonymity	Ensures a user may use a resource or service without disclosing the user's identity.
Unlinkability	Ensures a user may make multiple uses of resources or services without others being able to link these uses together.
Unobservability	Ensures a user may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used.
Psydonymity	Ensures a user may use a resource or service accountable for that use.

Source: [3]

The legal and policy drivers of addressing privacy for e-ID cards tend to focus on existing data protection and retention laws. These ensure that the repositories of e-ID and personally identifiable information (PII), be they in a centralised system, or on the card itself, are adequately protected from various vulnerabilities. With the exceptions of the Austrian scheme that explicitly addressed unlinkability as a design requirement, no other card design schemes put emphasis on privacy beyond data protection and retention. With the exception of describing some aspects of the Austrian scheme, this paper will not discuss debates around privacy.

IDENTITY, NATIONALITY & CITIZENSHIP

The scope of this paper is the *national e-ID card*. It is worth taking a step back to define what is understood by identification (ID). One classical definition was given by Clarke[4], as *"human identification is the association of data with a particular human being."* This data can come in different forms, but generally includes aspects such as the following:

The national identity card is a tangible device which attempts to represent the above forms of identification. It is perhaps also worthwhile taking a closer look at what is understood by nationality and how it differs from citizenship. Prior to the concepts of citizenship and nationality, in ancient times, allegiance was the general concept that defined what today may be better understood as nationality or citizenship. "You had a king, you owed allegiance to him. It was as simple as that"[5].

In Roman times, law defined the terms of citizenship, which ultimately defined to whom you paid your taxes. Citizenship could

Means of Identification	Clarke's Definition	Examples
Appearance	How the person looks	Use of photographs on identity documents, facial biometrics
Social behaviour	How the person interacts with others	Education records, mobile phone records, credit card statements, video surveillance data
Names / Codes	What the person is called by other people or by an organisation	Name listed in national registry, on passports, birth certificates, ID card numbers, social security numbers, etc.
Knowledge	What the person knows	Passwords, PINs
Tokens	What the person has	Smart cards, Secure ID cards
Bio-dynamics	What the person does or is	Most forms of biometrics: fingerprint, iris, retina, etc.
Imposed physical characteristics	What the person is now	Height, weight

Source: [4]

be obtained by enemy aliens through defection and collaboration. With the rights to citizenship, also came certain duties beyond paying taxes, most notably military service. A refusal to partake in the service would mean a revocation of the citizenship. Likewise, Romans would automatically lose their citizenship if they became prisoners of war[5]. Today, e-IDs can be similarly revoked (e.g. through published Certificate Revocation Lists)[6] though their motivation tends to be to due a change in the status of the card or contents as opposed to a revocation of citizenship.

Unlike citizenship, the concept of nationality is a more modern one. In fact it is not until the early nineteenth century that one seems to find initial references to nationality in the English language. It is likely that the English borrowed the term from the French *principe des nationalités*[5]. This term had its origins in revolutionary theory that "persons having a common language and culture form a nation and, as such, ought to be entitled to self-government as a state." While this definition may seem to make sense, it caused confusion especially in Britain where having a British passport did not necessarily imply that the holder had British citizenship.

Lloyd[5] has pointed out that "the passage of time has somehow fused and confused the ideas of allegiance, nationality and citizenship". This fusion and confusion is increased further when incorporating the concepts of e-ID and e-ID cards, especially when pertaining to national e-ID cards, which imply nationality, but not necessarily citizenship.

E-ID CARD APPLICATIONS

Almost all application areas of today's e-IDs revolve around government services, most notably the enablement of e-Government applications. The ones that seem to be considered most effective are those that generate some form of income to government agencies (e.g. tax-collection related). Other e-Government applications include:

- Age verification
- Personal data (national registry) verification
- e-voting (trials already performed in Estonia)
- Secure e-mail (in Estonia each citizen is given an e-mail address along with their electronic identity).

Estonia is an interesting example where

Almost all application areas of today's e-IDs revolve around government services, most notably the enablement of e-Government applications.

despite deploying an advanced e-ID card with a high penetration level, 65% of the population declare their taxes online using secure e-banking applications rather than with their national e-ID card. This has to do with the fact that banks rolled-out a secure online infrastructure (e.g. PKI) to enable e-filing of taxes before the national e-ID card was introduced.

Currently, the use of e-ID cards in non-Government sectors within Europe come in two forms:

- Use of e-ID cards as an SSCD to digitally and electronically sign documents with legal validity.
- Collaboration with financial institutions to share authentication infrastructure (e.g. PKI). This seems popular in some Nordic countries.

Some future uses of e-ID card applications include:

- Access to Public Wireless LANs / Metronets
- Age verification for services such as online gambling
- Anonymous credential systems[8] to address privacy concerns
- Encryption

While the use of smart cards for encryption is an easy extension, we have not seen this use of e-ID cards for a number of reasons:

- Requires an additional (encryption) certificate – this requires an additional (certificate) management task.
- No mandating legislation is in place (unlike electronic signatures).
- The demand does not seem to exist – conventional alternatives are already present.
- While privacy is being dealt with, mainly from a data retention perspective, the encryption of communications does not crop up in existing e-ID card literature.

NATIONAL E-ID CARDS IN EUROPE: AUSTRIA, BELGIUM & THE UNITED KINGDOM

While countries in Europe are at different stages of deploying national e-ID cards, the following three examples are illustrative of the variety of implementation mechanisms. Most notably, one can see the different underlying motivations and technical implementations. While at a national level the schemes might operate as initially designed, attempting to use e-ID cards to address cross-border functions (see pan-European

While countries in Europe are at different stages of deploying national e-ID cards, the following three examples are illustrative of the variety of implementation mechanisms.

drivers above), has proved to be nearly impossible. The Austrians have made an initial attempt to demonstrate interoperability through a Proof-of-Concept (PoC)[9], but otherwise interoperability of national e-ID cards remains an unaddressed functionality.

THE AUSTRIAN BÜRGERKARTE (CITIZENS CARD)

There are four unique aspects to the Austrian Bürgerkarte, which are worth highlighting:

(i) Multiple tokens (e-IDs):

The Austrian e-ID, unlike many other initiatives around Europe, is not focused on being a *single* card. Hence physical tokens may be found in the form of a government-issued identity card, but also all Austrian bank-issued ATM cards are legally valid e-ID cards (SSCDs), and even one of the telecom providers issues SIM cards that comply with Austrian legislation for serving as an e-ID "card".

(ii) Two forms of identity:

While in other national schemes there tends to only be a single (unique) identity, the Austrians legally define [9] two forms of acceptable identity:

Unique Identity	Designation of a specific person by means of one or more features enabling that data subject to be unmistakably distinguished from all other data subjects.
Recurring Identity	Designation of a specific person in a way which, while not ensuring unique identity, enables this person to be recognised by reference to a previous event, such as an earlier submission.

Source:[9]

Some advantages of legally defining and accepting the Recurring Identity include:

- Enabling multiple parties to generate their own e-ID tokens for the same unique identity
- Ability to integrate foreign e-IDs into the Austrian scheme

(ii) Unlinkability:

While there is no legal driver for preventing linkability as a privacy protection mechanism, the Austrians make it a point to highlight this aspect of their card. The motivation behind this feature is to address a privacy concern by making sure that when an identifier is used by one government organisation (e.g. national health insurance), another government agency would be required to use a different identifier (e.g. tax authorities). While technically speaking an elegant solution is provided, the Austrian's ability to truly address unlinkability fails on two counts:

- There is no legal requirement to address unlinkability. Hence, unlike clearly defined data retention laws, this privacy feature lacks any legal definition or ability to assure compliance.
- The use of other data to identify a citizen (e.g. name and date of birth) quickly shows that, for practical purposes, citizens can still be "linked". This is especially the case in a relatively small country as Austria with around 8 million citizens.

(iv) Interoperability:

The Austrians have been one of the few implementers of a national e-ID scheme that have made an attempt, through a PoC [9], to illustrate the interoperability of a foreign e-ID with their national scheme. The ability to perform such a function is possible due to the Austrian definition of the *Recurring Identity*. As an example, certificate serial numbers from a Finnish e-ID card are used to identify such cards, and tax ID numbers on the Italian e-ID card are used to uniquely identify Italian card holders. Using these foreign identifiers as inputs, the Austrians illustrated in their PoC the ability to generate an Austrian e-ID. This ability to "accept" a foreign e-ID is only one illustration of interoperability in an e-ID scheme. The level of acceptance is still limited in that it still requires an Austrian e-ID to be generated (using the foreign identifier as a seed identifier). Functionality, such as using a foreign-issued e-ID directly to conduct a transaction has not yet been a design requirement. As an example, an Italian wishing to file a case online with an Austrian public authority would be unable to do so with their Italian e-ID card. Other forms of interoperability between schemes are common practice in other domains, such as the ability to use an ATM card at foreign banks, authentication to a mobile phone network when roaming or the use of a driver's licence to prove one's right to operate vehicles even when abroad.

As a result of the Austrian's design objectives and legal definition of e-ID, it has allowed for a much wider deployment of national e-IDs than in other parts of Europe. While not having a single e-ID card, Austrian legislation has allowed a nationally valid e-ID to be issued on multiple form factors:

- National e-ID card
- Banking/ATM cards
- SIM cards
- USB fobs

Functionality, such as using a foreign-issued e-ID directly to conduct a transaction has not yet been a design requirement.

Belgian Personal Identity Card (BELPIC)

BELGIQUE CARTE D'IDENTITE
BELGIË IDENTITEITSKAART
BELGIEN PERSONALAUSWEIS
BELGIUM IDENTITY CARD
Nom / Name
Prénoms / Given names
Lieu et date de naissance / Place and date of birth
Sexe / Sex
Nationalité / Nationality
N° carte / Card No
Valide du - au / Valid from - until
Signature du titulaire / Holder's signature
N° d'identification du Registre national / Identification number of the National Register
Lieu de délivrance / Place of issue
Autorité / Authority
I<BEL0000000000<<<<<<<<<<<<
5001013F0806017BEL<<<<<<<<<<
VAN<PASSEL<<MICHAEL<<<<<<<<<

Source: [6]

The objectives of the BELPIC have been to accomplish the following functions[7]:

- Citizen identification
- Data capture
- Authentication
- Digital signature
- Access control (e.g. to municipal services such as library, swimming pool…)

In order to perform the above, it was decided to use three key pairs [6] for the following purposes:

- **Citizen authentication** – using an authentication certificate
- **Advanced electronic signature** – using a qualified certificate to produce digital signatures compliant with the EU Directive 1999/93/EC
- **e-ID card authentication** – the national registry knows the respective key for a given e-ID card

The first two cases each use X.509 v3 certificates to store keys on the card. X.509 is a standard certificate format which is also used by the Estonian and Finnish e-ID cards. While only a single aspect of commonality between the card schemes, the use of the same certificate format is an example where interoperability between card schemes becomes easier to implement (though presently not done).

Unlike the Austrian e-ID, which from the onset has attempted to be privacy-friendly through the use of unlinkability schemes, the

Belgian e-ID card has not addressed any aspects of privacy.

Also unlike the Austrian model described above, interoperability is still an issue not completely addressed by the BELPIC. The present focus is on interoperability of e-IDs across different administrative units within Belgium (federal, regional, community and municipality). There has not been any work on interoperability activities with regards to foreign e-ID cards[10].

UNITED KINGDOM IDENTITY CARD

As mentioned at the start of this paper, the UK is one of the few countries without an existing national identity card scheme. As a result, considerable debate has revolved more around whether and how the UK should adopt an identity-card scheme, than addressing aspects such as digital signature creation or increasing the security of an existing identity card.

Rather than attempt to provide the latest status of the UK Identity Card, which seems to be a continually moving target, there are a few key aspects which make the UK card scheme unique in Europe:

Identity checking services

While all e-ID schemes surveyed across Europe were focused on enablement of e-Government applications, the UK scheme set itself apart by focusing heavily on providing online identity checking services[11]. An example could be a bank seeking to verify the identity of a new account holder. There are specifically two aspects of these services which set the UK apart from the other schemes:

- The attempt to generate income from identity checking services
- The use of existing "Chip and PIN" infrastructure

While other European schemes see e-ID as an enabler to better collect revenue from existing government schemes (such as tax collection), none of them have as a stated goal to generate new revenue from the scheme itself. The use of "Chip and PIN" would allow UK e-ID cards to be used by a conventional payment card reader to verify the card holder's identity. While use of such infrastructure is technically possible, it poses some interesting questions regarding the use of the card reader technology for an unintended purpose (i.e. identification as opposed to payment authorisation).

The UK is one of the few countries without an existing national identity card scheme.

The S (Signature) part of the I-A-S model is clearly missing from the UK scheme

Despite considerable debate and activities around the use of e-ID cards to act as an SSCD across Europe, this discussion has not been conducted in the Strategic Action Plan for the National Identity Scheme [11], which is the officially mandated roadmap for the UK e-ID card. In fact, while the role of PKI is emphasised as a form to ensure card and back-end security, this infrastructure is not seen as an enabler to digitally sign electronic documents.

Biometrics

The UK identity card is also unique in the emphasis on usage of biometrics for verification purposes. Other e-ID card schemes do not capture biometric enrolment and verification beyond the printing of a facial photograph (or laser image in the case of the Italian e-ID).

RISKS

As with any large-scale IT implementation risks are omnipresent. National e-ID cards are just as vulnerable to attack as any other IT system, especially when one considers e-ID cards and their respective infrastructure as a form of *critical national infrastructure*. Hence, aspects such as Denial of Service attacks – both in the traditional sense, as well as intentional denial of acceptance when a card acceptor/user does not wish for the card to be recognised, the breaking or failure of underlying PKI infrastructure, or physical attacks to smart cards – all need to be considered when conducting a risk assessment of national e-ID card schemes.

Probably the vulnerability with the greatest threat to e-ID card schemes is human error. This is amply illustrated by the chaotic handling of all kinds of personal (and sensitive) data by various UK Government agencies during late 2007. Human error can take place at any stage where humans interact with the scheme. For example, during the enrolment processing, data may be incorrectly entered leading to confusion once the identity card has been issued. This is especially true with seed documents whose validity is less likely to be questioned (e.g. birth certificates). Likewise during enrolment, biometrics can be poorly captured leading to a higher level of false rejects.

CONCLUSION

The development of national e-ID card schemes is far from complete. The study

National e-ID cards are just as vulnerable to attack as any other IT system, especially when one considers e-ID cards and their respective infrastructure as a form of *critical national infrastructure.*

that was conducted in conjunction with this paper came to the conclusion that for many purposes a national e-ID card was not important, but rather the e-ID in itself sufficed. Probably the best illustration of this observation can be seen from the Austrian e-ID, where a single identity card is not the only way forward.

The Austrians also illustrated, by developing a Proof-of-Concept, the possibility of interoperability between schemes, albeit in a limited fashion. As the need grows of claiming social services across borders, the need to address interoperability issues becomes more critical. As an example, Poles working in the UK claiming retirement pensions after returning to Poland or British pensioners claiming social benefits from a retirement home in Bulgaria are just a few sample scenarios where e-Government applications need to be reviewed to ensure the requirements of e-Government applications are met in a Europe that is more and more operating without national borders. Purely for such scenarios where people are far away from their local public administrations, an interoperable e-ID card would be valuable to both citizens and governments alike.

Finally, there is potential for the private-sector to play a more active role in using the national e-ID cards. Today there is a lack of third-party (i.e. non-Government) applications for e-ID cards (an exception being the Austrians where there is not a single e-ID "card" issued per person). This limitation can be attributed to two reasons. First, there is a lack of participation of the private sector in the design of e-ID schemes. Hence, use-cases that could be of interest to non-Government institutions are not adequately addressed. Secondly, as we saw in the case of Estonians using pre-existing e-Banking authentication infrastructure to file their taxes, the functionality of the government e-ID schemes have in some cases already been addressed by other schemes and hence additional value to the public is not being created.*

Ron Condon

UK bureau chief
searchsecurity.co.UK

Ron Condon has been writing about developments in the IT industry for more than 30 years. In that time, he has charted the evolution from big mainframes, to minicomputers and PCs in the 1980s, and the rise of the Internet over the last decade or so. In recent years he has specialized in information security. He has edited daily, weekly and monthly publications, and has written for national and regional newspapers, in Europe and the U.S.

REFERENCES

[1] A. Fiat and A. Shamir, “How to Prove Yourself: Practical Solutions to Identification and Signature Problems,” in Advances in Cryptology - CRYPTO '86: Springer Berlin / Heidelberg, 1988.

[2] A. Pfitzman, M. Hansen, “Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – A consolidated Proposal for Terminology”, Draft v0.28, May 2007.

[3] “ISO/IEC 15408-2:2005 Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements”, International Organization for Standardization, 2005.

[4] R. Clarke, “Human Identification in Information Systems: Management Challenges and Public Policy Issues,” Information Technology & People, vol. 7, pp. 6-37, December 1994.

[5] M. Lloyd, The Passport. Sparkford, England: Sutton Publishing, 2005.

[6] D. D. Cock, “Belgian eID Card Technicalities,” Heverlee, Belgium: Katholieke Universiteit Leuven, 2006.

[7] D. D. Cock, C. Wolf, and B. Preneel, “The Belgian Electronic Identity Card (Overview),” in 3rd Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik: Bonner Köllen Verlag, 2006.

[8] J. Camenisch, D. Sommer, and R. Zimmermann, “A General Certification Framework with Application to Privacy-Enhancing Certificate Infrastructures,” in SEC 2006: Springer-Verlag, 2006.

[9] A. Hayat, R. Posch, and T. Rössler, “Giving an Interoperable Solution for Incorporating Foreign eIDs in Austrian E-Government,” in IDABC-Conference 2005: Cross-Border e-Government Services for Administrations, Businesses and Citizens Brussels, Belgium, 2005.

[10] “The Status of Identity Management in European eGovernment Initiatives,” DG Information Society and Media, European Commission 6 June 2006.

[11] “Strategic Action Plan for the National Identity Scheme Safeguarding your identity “ UK Home Office Ref. No. 278283, December 2006.