consult hyperion

white paper

Top ten barriers to eID in EU

A Consult Hyperion white paper,

Version 1, June 2006

CONTENTS

Abstract..... 2

Typology and overview 2

Our top ten issues..... 3

About the authors 12

Our business..... 13

Abstract

Consult Hyperion has been asked by IPTS to write a 5-10 page paper on the top 10 issues we consider to be barriers to the adoption of eID in Europe. These are either the most important or the most challenging for the digital ID sector.

Space and time do not allow for a detailed analysis. This analysis will be done during the project which includes a workshop (in conjunction with the annual Consult Hyperion Digital Identity Forum, www.digitalidforum.com) where eID experts will engage in a facilitated debate.

Our analysis in this paper draws on our own extensive experience of eID issues in the public and private sectors, as well as several key sources of recent eID work funded by the EU:

- MODINIS
- GUIDE
- IPTS study by Consult Hyperion and ILS on 'EU eID Management: Analysis of 25+ Member States' Systems'

Typology and overview

A typology of issues is proposed as follows with our top-ten barriers assigned to one of the categories:

- Legal
    - Mandatory unique identifiers disallowed in some Member States
    - Matching 'standard' technical security solutions to diversity of legal frameworks
- Technical
    - Legacy 'transaction-centric' systems dominate
    - Too many standards, no commonly accepted standard

- Economic
    - Initial investments needed are high.
    - Multitude of digital IDs
- Social
    - Trust: data sharing and federation
    - Cultural and social attitudes to data sharing
- Organisational
    - Lack of agreed semantic understanding
    - High inertia: change is disruptive and these systems are often mission critical

It should be noted that these categories are not mutually excusive, but rather they represent different aspects of the same barriers.

All of these barriers interlock to hamper interoperability in Europe, so efforts to single out and dismantle individual barriers seem likely to meet with limited success. Perhaps a more fruitful direction forward is to begin to create an environment where specific industry sectors tackle the barriers in a more "localised" way to overcome them (eg, SAFE in the pharmaceutical sector, IdenTrust in the financial sector) and then interlink through sharing or genuine federation.

In an international or cross-sector context, specific attention needs to be paid to the organisational and social issues. These are less amenable to analysis and action plan than technical, business or economic issues. This means that even sectors that a quite limited in scope will find them difficult to overcome: at a low level, SAFE and IdenTrust "dictionaries" may either have words in them that mean different things or have no equivalents.

Our top ten issues

For each of the issues that we consider should make the top ten, we present the reasons why and at least one relevant example.

Unique identifiers

From a technical point of view, the use of a single unique identifier per person might seem desirable and some national ID schemes are taking this approach. However, there are reasons why this approach might not be considered desirable and there are also reasons why this approach cannot work on an international level. One such reason is that some countries have legislation that disallows the compulsory allocation of a unique identifier to each person.

Therefore there is a wide variation in the approaches taken in different countries:

- Germany forbids the obligatory assignment of unique identifiers to citizens
- Belgium issues mandatory identifiers to citizens
- Ireland issues multiple identifiers for different services (though this is likely to change)

Consequently, the cross-border use of unique identifiers needs to comply with the applicable legal framework.

Matching 'standard' technical security solutions to diversity of legal frameworks

There is a mis-match between technical actions (e.g. digital signature) and the legal equivalent (handwritten signature). Clearly digital signature has a lot more to offer than handwritten signatures (e.g. potentially strong non-repudiation if implemented well). But how do you measure that the implementation is appropriate and correct and feed this into any legal processes?

Another example is in the area of authorisation. It is technically simple to authorise someone to act on your behalf, for example, your tax accountant might submit your tax return for you. But what if they fail to do so? The legal frameworks involved somehow need to associate appropriate liabilities to such authorisations. The common solution is to force users to accept End User Licence Agreements to establish a conventional legal framework. However, when operating internationally, these can be more difficult to enforce. The solution here might have to be 'legal federation' where the user accepts the legal framework provisions of the service provider, regardless of their actual needs.

Legacy 'transaction-centric' systems dominate

The majority of legacy systems, especially within government departments are transaction-centric (or 'case-centric'), rather than person-centric. This makes it extremely difficult to track identities across interactions with government. It allows for persons to have multiple identities fraudulently, as well as for poor data quality to propagate throughout systems, inadvertently creating multiple identities.

Continued degradation in departmental data quality from use of a case-centric model will ensure that person-centric records needed for Identity Management become increasingly hard to locate. Just as it is hard and expensive to retrofit security, it is hard to add an identity layer to existing systems. It is not clear how to encompass legacy systems (largely case-centric and with inflexible architectures) into a modern Identity Management Service and further work needs to be started in this area.

Too many standards, no commonly accepted standard

The saying goes – 'The great thing about standards is that there are so many to choose from.' There have been many attempts at standardisation in the field of eID that do not seem to have not yet led to practical interoperability, but may in the future:

- Under the mandate of the Hague Program, launched in 2004 to set migration and asylum polices for the EU25, the European Council, and the Commission have been invited to elaborate minimum security standards for electronic ID cards including biometrics. The Commission is due to publish a report, describing not only the standards, but also the state of electronic ID card programs and plans in the Member Countries. The European Commission's Article 6 Committee is charged with drafting common security standards for national identity cards, in particular the use of biometrics.

- The more informal Porvoo Group—an international cooperative network whose primary goal is to promote a trans-national, interoperable electronic identity in order to help ensure secure public and private sector e-transactions in Europe. The Group also promotes the introduction of interoperable data specifications, the mutual, cross-border acceptance of authentication mechanisms, as well as cross-border, on-line access to administrative services. The Porvoo Group believes Belgium, Estonia and Finland, and perhaps Italy and Spain, could have interoperable digital credentials one day, and plans a demonstration project.
- The UK Presidency of the Council of the European Union has put forward a proposal that all ID cards in the EU should have biometrics to meet the International Civil Aviation Organization (ICAO) standards for travel documents.

We have seen that setting standards is not enough and driving through to the point of rollout of significant numbers of eIDs is the only way forward. A good case in point is the US Personal Identification and Verification (PIV) card standardised as FIPS 201. In a very short space of time, they have written a specification (based on relevant standards and bridging the gaps). They have also set up accreditation and interoperability laboratories that will ensure that there is a list of off-the-shelf products in 2007. This has only been possible because the suppliers are prepared to make significant effort because they know there will be a significant market for many years to come.

Initial investments needed are high

The levels of investment required to create fully interoperable digital IDs are naturally high because of the complexity of creating international infrastructure. While individual banks, government departments, companies and other organisations might benefit greatly from the use of interoperable digital IDs, none of them would be prepared to fund the entire infrastructure. It is obvious, for example, that (as part of initiatives associated with SEPA and other pan-European banking directions) EU banks would save a lot of money if they could accept a variety of other EU identities—perhaps digital certificates on smart ID cards, for example—rather than traditional, paper identification documents, yet no government would expect banks to pay for the cost national smart identity cards.

Multitude of digital IDs

Investigation is needed into best architectural practice for minimising persons having multiple IDs across government. Seeing as we cannot expect to have biometrics registered for all those encountered in the foreseeable future, this might need to be as simple and pragmatic as a linked numbering schemes across department systems.

Rather than replace existing and planned identity systems with a single system, an Identity *metasystem* is needed in addition, constructed in such a way as to allow IdM best practice to emerge, evolve, be guided and partly self organise as we have seen happen with the Internet.

We can list the following desired characteristics of the metasystem as depicted in Figure 1:

- Controlled simplified access to the identification services of multiple ID providers, as well as private sector and international partners.
- Authentication to the *services* of multiple Relying Parties such as potentially all government department and agencies, as well as private sector and international partners.
- ID providers have strong registration processes supported by biometric technologies – in order to reduce the possibility of multiple identities for a single person.
- Encourage the re-use of existing identification tokens/identifiers thereby providing efficiencies and allowing IdM to be done by parties that would otherwise not be able to afford to contemplate it.
- A reduced set of identifying tokens/identifiers resulting from increased use of trusted national ID tokens such as driving license, passport and potentially ID card.
- Support for federation of locally held attributed and biographical information based on a minimal disclosure model that enhances the privacy of the individual while streamlining their interactions with government.
- Provide an encapsulating protocol allowing systems to share information and queries that is independent of technologies chosen by individual systems. It is not feasible to try to mandate particular technologies since IdM requires co-operation with parties across the globe.

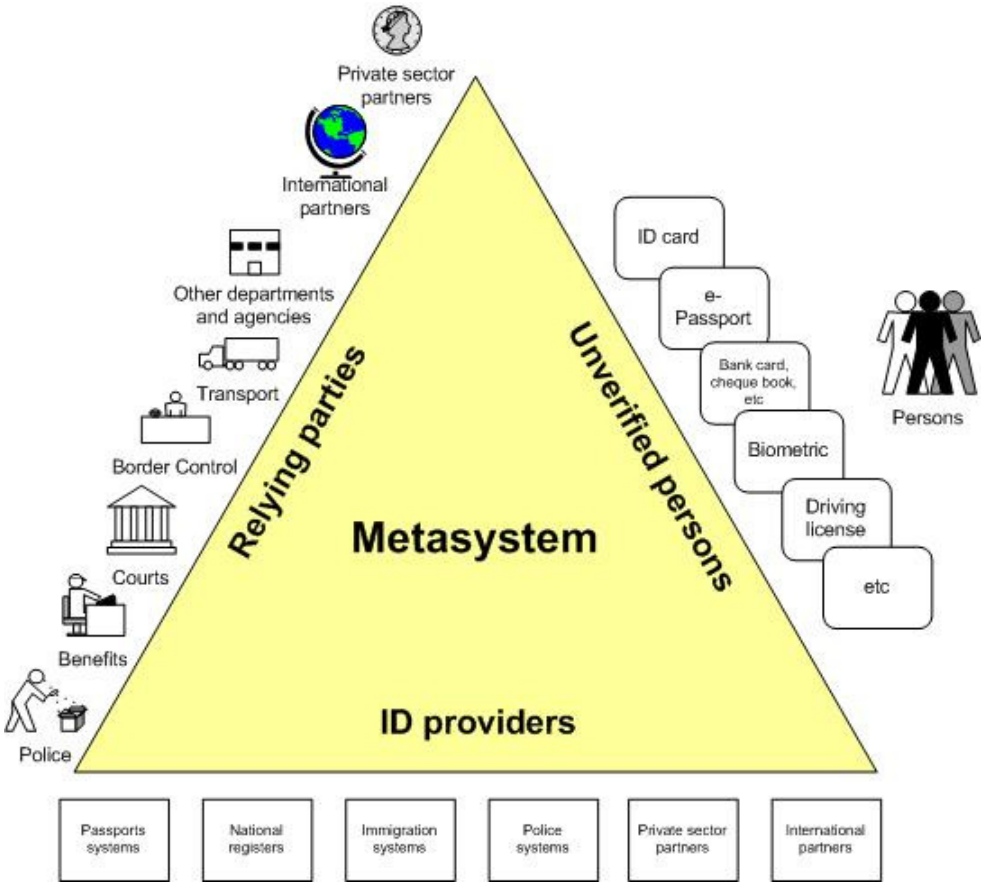

Figure 1: Metasystem overview

A Federated Identity approach is probably the way forward since IdM can only be realised by the co-operation of multiple systems. There is also an argument that smaller federated databases will perform more accurate and faster matching than a monolithic one.

For these reasons, we expect to see a 'Federation of Federations' [GUIDE] emerging across the globe over the next decade and it will be important for the UK government to be ready to integrate with this in order to co-operate and maximise benefits to accurate person-based IdM.

An example of broad forward thinking is the EU funded GUIDE research project which is entering phase 2 of its funding. By the end of the project several countries will have linked their population databases to GUIDE in proof-of-concept form. At the moment the following countries will probably be participating in the trials with twice as many again as observers: UK, France, Spain, Italy, Belgium, Netherlands, Estonia and Austria. The aim is to try to reach critical mass. Each of these countries will have had a GUIDE gateway with the Identity Services installed. It should be noted though that these gateways are prototype only and are not for full production usage, they will allow the governments to see the concept working with real data.

Governments should work closely with international partners to determine how federation is best applied in the light of most recent research and good practice across the globe including US initiatives and EU research such as GUIDE and MODINIS.

Trust: data sharing and federation

Identification processes are varied and often disconnected. For example, the identification records (e.g. photograph, fingerprint, attributed data) created by one organisation typically remains unused by partner organisation, perhaps allowing for undetected person substitution or other crimes. Current sharing between organisations is severely limited by system capacity and availability of proprietary links.

Each Identity system deals with its own 'population' of persons. Each has its own purpose and legislative domain. The Venn diagram below shows how identities can move across legislative populations over time.



Figure 2: Single ID for individuals migrating between populations

An asylum seeker might be granted refugee status, become a British citizen and go on to gain a criminal record. It is important that these overlapping populations, managed by different business area systems, are able to be managed in a co-operative manner (to minimise multiple IDs for one person) while remaining within legislative constraints.

Thus data sharing between systems is imperative if we are to achieve effective person IdM across government. Recent experience in the USA indicates that there is considerable benefit to law enforcement officers having access to person records including unpaid fines, cautions, etc. The US has a 'zero tolerance' approach and they will not agree to share registrations of trusted travellers with other countries until they use fingerprinting to check for all such outstanding records. There is a tension here that needs to be resolved.

Controlled and justified sharing of identity data is key to good IdM practice. When unverified people are met and they appear not to have been encountered before ('unknowns'), then we have no records and need to record an instance of a new identity. Everyone has some sort of social or biographical footprint in some domain or other. The way to access this information is by sharing data with other systems inside and outside of government.

Other barriers to data sharing include:

- ***Plurality of operators and technologies:*** The fact that IdM is immature and that there are so many partners that UK government will potentially need to work with in this field (national and international; public and private sectors) means that interoperability if hard to achieve. There are competing technologies (e.g. SAML; Liberty Alliance). Systems often operate from different Legislative domains with different trust models. All this gives rise to the following:
    - *A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers.*

- ***Unready partners***: Partners whose data we wish to share might not be in a position to co-operate due to lack of connectability of old systems or simply having insufficient system capacity to cope with escalating external requests.

It is necessary to determine the best way to migrate legacy systems to balance person-centric views at the heart of current thinking on Identity Management while retaining those elements of case-centric approach which are key to business needs. This should be a key part of the requirements of the IdM procurements since this is the best data currently available for IdM systems to use.

Data cleansing is also key. It is not clear how to do this and how the metadata relating to quality will be transmitted between departments. Another element to be factored into the government-wide IdM governance framework is the recognition that bad quality data (or partially inaccurate and context-dependent data – e.g. information from informants) will continue to be used for the foreseeable future, and processes will be needed to deal with this on an ongoing basis.

Data warehousing and data mining need to be investigated as partial solutions to data cleansing and providing person-centricity in the future.

Cultural and social attitudes to data sharing

There is much confusion around the issue of privacy, especially with the introduction of smart ID card and biometric systems at the national level.

When we are dealing with government-wide IdM, we must remember the view-point of the citizen: privacy is desirable. The following are privacy good practice considerations:

- "Minimal disclosure for a constrained use". Some applications might only require an entitlement to be verified rather than a person's name (e.g. "is over 18" rather than revealing their date of birth. c.f. EURODAC only returns yes/no to the questions "have these fingerprints been recorded from a current asylum seeker").
- "Justifiable parties". Design should be such that disclosure of identifying information is limited to parties having a necessary and justifiable place in an identification relationship.

Connection is easy (networks, IP, etc), disconnection is harder. Hence the need for disconnection technologies which are currently less well exploited: PKI, smart cards, biometrics. For example, the US has recently mandated smart ID cards for all Federal staff ID.

Lack of agreed semantic understanding

Our simple framework for interoperability that we used in our previous work for IPTS is adequate for examining and exploring the relevant issues of interoperable eID across domains (Figure 3). It is based on three levels: the strategy level, the procedural level and the systems level. While the technical complexity around interoperability is greatest at the bottom of the pyramid, technical interoperability problems (once they have been identified) are, in principle, possible to overcome. Conversely, at the top of the pyramid there may be great complexity in achieving "political" interoperability.

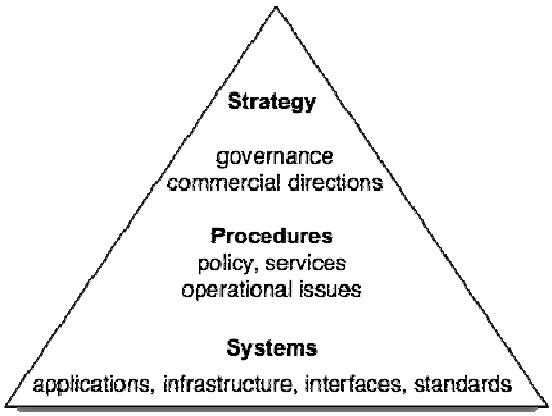

Figure 3: Presumed Interoperability Framework

To show how these interoperability levels related to inter-domain eID, consider a straightforward example: the use of bank-issued eID by eGoverment services (as illustrated in Figure 4). In this example, the technical standards required for interoperability are well-known and well-established and at least one set of appropriate procedural standards for interoperability already exist (in this case, the Identrus set developed by a consortium of international banks).

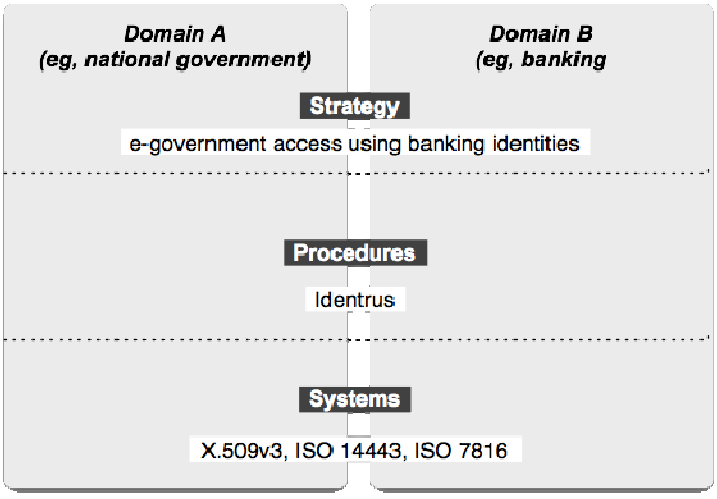

Figure 4: Inter-Domain Interoperability within Framework

This simple and clear approach to interoperability highlights the role of interoperability as a driver to development: not at the technical level, but at the strategic level, resulting in procedural interoperability. Technical interoperability is not a driver: the technical fact that one government's eID cards can be read by another country's eHealth readers is not, in itself, a driver that will pressure the development of procedures.

One of the key barriers to the progression of eID across the globe is the lack of agreed terminology with which to debate the eID frameworks. The problem is not a lack of suggested common nomenclatures (one of the most recent has been provided by MODINIS), but rather ones of agreement and thereafter correct usage.

This is not merely an academic issue, but rather one that strikes at the root of achieving eID interoperability. For example, what do we mean by the basic terms identity, identifier, identification, verification, token, authorisation, authentication, to name just a few. The solution to this barrier is not clear, but what is for sure is that it is not to build another glossary!

High inertia: change is disruptive and these systems are often mission critical

The systems that provide the possibility of interoperable eID are often mission critical. This is particularly true at government level where they tend to be associated with such 'businesses areas' as immigration control, criminal justice and national ID. Therefore, there is reluctance to introduce change because of the associated risks to impacting mission-critical procedures, such as passport production.

Passports are a good case in point. Some EU government had been considering the use of biometrics and smart cards for several years before US mandated them for members of their Visa Waiver Programme. It likely that nothing would have happened for many more years if it were not for the US mandate.

References

[GUIDE] Identity Interoperability Services Report: Core Services Descriptions, v2, 30 September. Available from http://istrg.som.surrey.ac.uk/projects/guide/

[LAWS-ID] Kim Cameron, *The Laws of Identity*, Microsoft Corporation, 11 May 2005. Available from http://www.identityblog.com/stories/2004/12/09/thelaws.html

[MODINIS] *Common Terminological Framework for Interoperable Electronic Identity Management*, Consultation Paper, MODINIS, v 2.01, 23 November 2005. Available from https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/GlossaryDoc

About the authors



David G.W. Birch is a Director of Consult Hyperion—the IT management consultancy that specialises in electronic transactions—which he helped found after several years working as a consultant in Europe, the Far East and North America. A physicist by training, Dave has lectured on the impact of new communications technologies to MBA level. He is European correspondent for the *Journal of Internet Banking and Commerce*, a member of the editorial advisory the *European Business Review* and is a European Commission expert reviewer in the field of mobile commerce. Described in *The Independent* in 2004 as a "grade-A geek", he has written for publications ranging from *The Guardian* to the *Parliamentary IT Review* and is a media commentator on electronic business issues.



John Elliott is a Principal Consultant with Consult Hyperion, a UK IT management consultancy specialising in digital identity and digital money. He has a PhD from the University of Edinburgh and is a Chartered Engineer with over ten years IT industry experience. John has worked for Consult Hyperion since 1998 and is recognised internationally as an expert on multi-application smart cards, PKI and biometrics.

Recent work John has undertaken includes:

- Security assessment and tender specification for the Hong Kong National ID card
- Biometrics framework for the UK Home Office, Immigration and Nationality Directorate.
- Biometric technology roadmap for UK Police IT Organisation
- Contactless smart card strategy for the Malaysian national ID card

Our business

Consult Hyperion is an independent management consultancy with a global client base. We help organisations to reap tangible benefits from technological change in the field of secure electronic transactions. These transactions support applications ranging from payments to passport control and from mobile phone top-up to TV shopping. We work to:

- Evaluate new business concepts;
- Develop new products and services;
- Manage the evolution of complex systems.

Our aim is to assist our clients in reaching their goals in a timely and cost-effective way. We work in four main sectors:

- Financial services;
- Public sector;
- Retail;
- Telecommunications, media and technology (TMT).

We support the deployment of practical solutions using the most appropriate technologies. We have world-class expertise at every step in the transaction value chain:

- Authentication, such as smart cards, RFID and biometrics;
- Access Devices, such as set-top boxes, PCs and mobile phones;
- Digital Networks, such as digital TV, the Internet and GSM;
- Transaction services, founded on the concepts of digital money and digital identity;
- Applications ranging from customer service to electronic voting.

Consult Hyperion
Tweed House, 12 The Mount, Guildford, Surrey GU2 4HN, England
t: +44(0)1483 301793 f: +44(0)1483 561657 e: info@chyp.com w: www.chyp.com