JRC Scientific and Technical Reports

Overcoming Barriers In the EU Digital Identity Sector

Editors: Ioannis Maghiros and Boris Rotenberg
Authors: John Elliott, Dave Birch, Margaret Ford, and Andrew Whitcombe

EUR 23046 EN - 2007

JRC EUROPEAN COMMISSION

ipts Institute for Prospective Technological Studies

The mission of the IPTS is to provide customer-driven support to the EU policy-making process by researching science-based responses to policy challenges that have both a socio-economic and a scientific or technological dimension.

European Commission
Joint Research Centre
Institute for Prospective Technological Studies

Contact information
Address: Edificio Expo. c/ Inca Garcilaso, s/n. E-41092 Seville (Spain)
E-mail: jrc-ipts-secretariat@ec.europa.eu
Tel.: +34 954488318
Fax: +34 954488300

http://www.jrc.es
http://www.jrc.ec.europa.eu

JRC40719

EUR 23046 EN
ISBN 978-92-79-07818-7
ISSN 1018-5593
DOI: 10.2791/70350

Luxembourg: Office for Official Publications of the European Communities

Printed in Spain

Acknowledgements

Editors:
Ioannis Maghiros, European Commission – DG JRC – IPTS
Boris Rotenberg, European Commission – DG JRC – IPTS

Authors:
John Elliott, Consult Hyperion, UK
Dave Birch, Consult Hyperion, UK
Margaret Ford, Consult Hyperion, UK
Andrew Whitcombe, Consult Hyperion, UK

Workshop participants:
Caspar Bowden, Microsoft
Clive Reedman, Identity Solutions Ltd
Dave Engberg, CoreStreet
Angela Sasse, University College London
Mike Butler, US Department of Defence
John Browning, The Economist
Dieter Sommer IBM Research
Peter Brown, CEN eGovernment Focus Group
Bart Preneel, Katholieke Universiteit Leuven
Niall Barry, Irish Department of Social and Family Affairs
Mart Parve, Look@World Foundation
Martin Meints, Independent Centre for Privacy Protection
Stefan Brands, Credentica

Table of Contents

Executive Summary

1. Research question

Digital identity entails critical technology, business and policy issues which, nowadays, affect practically every user, industry and government. Digital identities—the collection of digital information associated with an individual, organisation or entity—exist in a wide array of forms and formats, such as combinations of user-ids and passwords, PIN numbers, etc. Many people equate digital identity (eID) with government-issued identity cards sometimes containing a chip. However, digital identities are routinely created by users for a great many online transactions that are not government-related. Similarly, there are many applications such as e-health, e-government, identity brokering, digital rights management, electronic payments, and e-banking, where efficient identity management is essential. Market actors responsible for implementing and supporting these services are now experiencing barriers impeding growth in this area.

There are many different barriers to the adoption of digital identity systems, for example:

- social barriers such as the culture of distrust, the loss of anonymity, or possible role conflict.
- potential economic barriers such as increased transaction costs or the high investment costs associated with the move to an increasingly digital economy.
- technical barriers such as the existing proprietary standards and risks of lock-in, the lack of interoperability, and the legacy problems.
- organisational barriers such as the lack of internal capacity of some corporations for addressing this complex problem, or the aversion to change.
- legal barriers such as the multiplication of legal requirements, of corporate ID policies, and of national laws impacting identity.

The purpose of this project was to identify the most important and/or most challenging technical, organisational and legal barriers to EU-wide deployment of digital identity technologies across both private and public sectors. After prioritising the barriers according to their importance and the ease with which they can be addressed, the study aimed to identify appropriate policy options in order to remove these barriers. The overall goals of the study have certainly been achieved. The study contributes significantly to a deeper understanding of the challenges, opportunities and threats in overcoming barriers to the EU market for eID. It also helps in raising awareness and promoting an advanced understanding of the eID research and policy climate.

2. Overall conclusion

A lot of ground was covered as a result of in-depth discussions during the project and at the prioritisation workshop. Although the experts were not able to reach consensus on a list of the most important and/or challenging barriers with a view to prioritising them, a number of important insights emerge from this report. As regards methodology, the study made clear that the technical, social, economic and legal aspects of problems facing digital identity are so inter-twined that it would be ill-advised to analyse these aspects separately. In order to draw clear policy conclusions, it soon became obvious that policy making in this field is in need of a more compelling taxonomy or classification that would allow for a more thorough cross-disciplinary analysis. Only after such a classification has been agreed on, can the various barriers listed in the report be tackled.

The report analyses these barriers according to the scale on which the issue is considered most important and/or challenging (individual, systems, or project level). This is interesting as a classification because the focus on the scale at which the problem is faced inherently points to the type of policy lever (technological, economic, or legal regulatory) that may be used to remove the particular barrier, as well as the level of decision making at which this may be done.

The report acknowledges the fact that there is such a strong inter-relationship between the issues faced at the individual, systems or project level, that it is sometimes hard to draw firm conclusions for each of these levels. Besides including a clear definition of the three levels, the report therefore

analyses most of the barriers from the 'individual' point of view, which is considered the dominant or default category. Remaining problems are analysed from the systems or project angle only when it is clear that the individual dimension is not central to the issue at stake. Second, though the classification does not specifically spell out the internal market dimension of the various barriers to deployment of digital identity systems, the report highlights the role of European Union policy making in overcoming barriers at various stages, and makes it clear when there is a genuine need to understand better the specifically European dimension of a particular barrier to digital identity.

3. Study insights

3.1 Foster inter-disciplinary research and discussion

Nevertheless, a number of interesting insights can be garnered from the report. For a start, the discussions in the experts' workshop made clear how sharp the divides are across the various disciplines. For instance, the inability to communicate effectively between the technical discipline and the policy discipline (private sector and government) is a particularly devastating obstacle. This could affect both the quality of public procurement and the prosperity of the eID sector. Semantic difficulties are viewed by many as one of the most critical barriers. Despite the repeated production of glossaries in relation to identity projects, at present there is no commonality of discourse around eID.

Taking this insight at the level of the study, the participants failed to agree on which barriers were the most important and/or most challenging, because experts across disciplines had different understandings of key policy determinants such as the "important" or "challenging" nature of a particular barrier, and of key concepts such as "trust." This strongly suggests there is a need to support more inter-disciplinary research and discussions in the field of digital identity.

3.2 Strive for flexibility at all levels

The uncertain nature and degree of a number of supposed barriers demands a cautious approach, in which maximum flexibility is guaranteed. This flexibility appears to be necessary at a number of levels. Neither industry nor users have shown any clear enthusiasm for a standard government-issued digital identity. From the user's point of view, it has also become clear that different demographics require different solutions. Good policy consequently supports maximum user choice and flexibility. There is great value to be gained from offering flexibility in the types of virtual digital identity adopted by users and the types of physical medium on which they can be stored. This permits individuals to choose the physical format which is most convenient or familiar to them, while still enabling organisations to issue a standard set of digital credentials which addresses security and privacy requirements.

Likewise, a flexible approach to standards is vital to the effective interaction of identity systems across the region. Current standards regulation, based around older technologies like X.509, appears to be stifling the market for newer, more flexible solutions. The ideal would be to have a standardised technical core surrounded by varying optional elements, as implemented, for instance, in the US PIV programme.[1]

There is also general recognition of the importance of interregional intransposability: i.e. the success of a system in one region does not automatically make it appropriate elsewhere. Local cultural issues are a vital consideration. The starting point is thus to limit the scale of the pilot projects before starting roll-out. Only such a flexible approach may eventually lead to successful EU-wide implementations. This view seems to be supported by the fact that smaller countries such as Austria and Belgium have been able to co-operate more effectively on digital ID than larger countries such as France and Germany.

[1] *See* http://csrc.nist.gov/piv-program/

3.3 Use widest array of policy tools

The report offers a range of policy recommendations. This approach is useful with a view to tailoring the policy measure to the perceived seriousness of the problem at hand. The policy recommendations offered by the authors may be sub-divided into research recommendations, and soft, hard, and institutional solutions. Examples of soft law are guidelines, best practices; hard law takes the form of directives and regulations; institutional solutions are about the creation of a specific entity or authority in order to solve certain perceived problems.

(i) Research recommendations

Most of the research recommendations relate to users, and the problems they face when confronted with digital identity systems. The most pressing problem concerns data protection. The study reveals a need for closer investigation into the economic and social implications of data protection and profiling across the EU. This would also provide the opportunity to investigate the degree to which the laws are, in fact, enforced and whether penalties provide an adequate deterrent. The remainder of the research recommendations concern the social aspects of identity systems, where investigation is considered to be more urgent and complex than many of the remaining technical problems. Examples include research into improving user experience, the human aspects of security, regarding the different mechanisms for building assurance and trust into identity systems, or seeking to identify the influence of demographics on individuals' choices of identity tokens (i.e. preferences regarding storing credentials on cards, mobile phones, key fob tokens, etc.).

(ii) Soft measures

The report also points to a need to increase soft measures in the digital identity sector. A first type of soft measures consists in the mere coordination of existing industry efforts, or industry commitments. These could relate to *(a)* initiatives to encourage industry co-operation in making data protection a key focus, *(b)* support for initiatives which strive to develop a global data protection culture, such as the International Conference of Data Protection and Privacy Commissioners, or *(c)* incentivising industry efforts to develop effective technical mechanisms to control the use of information once it has been collected. Other examples relate to technical implementation and standardisation. A commitment by industry to put user experience at the heart of their identity systems, perhaps in association with standards bodies such as the ISO, may equally be useful. Given the potential for damage to reputation, prosperity and health from failures in identity systems, the highest standards in engineering for safety should be mandatory in their design.

A second type of soft measure is the drafting of formal guidelines or an industry code of conduct on given eID-related issues. A framework could be developed, governing the interaction between hardware devices and soft identity credentials, to ensure that both flexibility and security are respected during the design process. A layered model, similar to the OSI networking model, would appear to be the most practical way of approaching this. Similarly, industry could be asked to develop a formal scheme for certifying the strength of enrolment for different levels of functional credentials. The existing 'tScheme' might serve as a model for this.[2] This would provide a greater level of certainty when dealing with the wide variety of ID credentials across the region. Industry could also be asked to develop a standard code of conduct for electronic identity transactions, in order to clarify the responsibilities of the end user. If implemented correctly, this could have a major impact on the amount of fraud due to phishing attacks. Finally, it might be helpful for industry to promote its own guidelines regarding revocation. At present, significant effort is expended on the design process, in order to give users access to a system. However, the reverse process of terminating access at the appropriate stage is often given a lower priority though it is necessary in order to secure the long-term integrity of identity systems.

The most far-reaching soft measure is the centralisation of knowledge on particular issues. There is a wealth of experience available regarding the implementation of large-scale identity projects in both the public and commercial sectors in Europe. Unfortunately, this experience is not particularly easily accessible, neither is it necessarily applied to subsequent projects. It would be good to make the knowledge widely available. One such instance might be the creation of a central log of large-

[2] *See* http://www.tscheme.org/

scale government identity projects across the EU region, with open and unbiased reporting of the lessons, both positive and negative, to be learned from these projects. Where possible, details of relevant, international projects should be included. An example of this might be the implementation of Chip and PIN in the banking sector. The log should be openly accessible and give the option for regular moderated updates by interested parties, as well as comments and cross-referencing. Another example relates to standards, with the creation of an accessible framework of standards relating to identity, with annual updates, in order to assist with implementation projects. The ECRYPT yearly report on algorithms and key sizes might serve as a model for this.[3]

(iii) Hard measures

The report identified two potential areas for hard law measures. The first such area is data protection law. The report points out that profiling is flourishing in both government and commercial contexts. This presents many ethical issues relating to privacy and the manipulation of personal data in order to influence individuals, even potentially in ways which they themselves may not fully comprehend. As a result of the EU legislation in the field, data protection already has a strong basis within the EU. There are, however, considerable differences in practice between the levels of protection offered in countries across the community. The report advocates the need for legal measures to ensure that 'personal information' is understood in effectively the same sense in each jurisdiction. Additional measures may include *(a)* legal controls on the sale of personal information to third parties, *(b)* the promotion of privacy-enhancing technologies which offer unlinkability and would bring clear benefits, or *(c)* industry oversight by data protection authorities of the justification for their identification, authentication, authorisation and retention policies.

The second area is standardisation. At present, each country makes its own standards, and there are even struggles for standards regionally within countries, resulting in a global explosion of standards. This is a very clear barrier to integration at the most basic technical level. EU-wide regulatory guidelines at the meta-level for building digital identity systems would be a positive step. These should be less prescriptive than current regulations. Member State governments could learn from the example of the US PIV implementation, by specifying a standard core for all of their identity requirements, but at the same time leaving scope for customisation around that core.

(iv) Institutional solutions

Finally, on a number of issues, there may be a need to reconsider the institutional configuration surrounding digital identity. This may include extending the responsibilities of existing authorities to include wider usability issues, the formation of an institution to raise standards in implementations relating to user experience across the EU, or support to existing initiatives to increase the understanding of identity across the EU, possibly through the creation of a non-profit organisation on the model of the US Interagency Advisory Board.[4]

---

[3] *See* http://www.ecrypt.eu.org/

[4] *See* http://www.smart.gov/iab/

About the eID Barriers Study

This report is the result of a study on barriers to digital identity, commissioned by the Institute of Prospective Technology Studies (IPTS).[5] The objective of the study is to inform the policy process within the European Union on the socio-economic and technological developments taking place with respect to digital identity. Promoting an efficient identity management framework is a vital ingredient in achieving a European knowledge society, which is itself a target of the i2010 policy initiative and the Lisbon process.

The study analyses technological, economic, social and legal barriers to the EU-wide deployment of digital identity technologies, as well as their broader implications. The main challenge of the study is thus to offer a detailed report on barriers to the EU-wide deployment of digital identification technologies, detailing the issues at stake for Europe. The study seeks to help achieve a deeper understanding of the challenges, opportunities and threats in overcoming identified barriers to the EU market for eID from the point of view of the European policy-maker. Furthermore, it aims at raising awareness, with a view to promoting an advanced understanding of the eID research and policy climate.

The scope and detailed specification of research has been prepared by IPTS. The study has been performed by Consult Hyperion in cooperation with IPTS, between October 2006 and June 2007. Many persons have contributed to make this report possible. The report was written by Dave Birch, Margaret Ford, John Elliott from Consult Hyperion. It was validated at a workshop by an interdisciplinary and international group of experts on 28th February-1st March 2007. The results of the validation workshop have been used to enrich and complement the report. Throughout the work process towards the final result, it was thoroughly reviewed and edited by Ioannis Maghiros and Boris Rotenberg from IPTS. We are most grateful to everyone who contributed to this study (see acknowledgments).

Structure of the report

The report that follows is composed of four parts. The first part considers the digital identity barriers that are most relevant from the individual users' point of view. The second part analyses the issues at the system-level. The third part discusses the digital identity barriers from a more macro perspective, namely from the project level. The final part analyses the situation and presents recommendations for further initiatives in Europe, focusing on each of the three levels identified and discussed in the previous parts. The contents of the first four parts are presented in more detail below.

Section 1: Individual-level barriers

This section is dedicated to the investigation of issues relating to the integration of digital identity which have the greatest effect at an individual or personal level. As one might expect from discussions surrounding identity, all related issues could be considered as relating to the 'individual'. However, where there are also significant systems or project elements, the relevant issues have been assigned to those sections. The content of this section is as follows:

- User-centricity
- Data sharing and data protection
- Profiling

[5] IPTS is one of the 7 research institutes of the European Commission's Joint Research Centre.

Section 2: Systems-level barriers

This section is dedicated to the investigation of issues relating to the integration of digital identity which have the greatest effect at a systems level. The study finds that a number of problems become more apparent at this level, and consequently analysing it from this angle may help devising appropriate solutions. The content of this section is as follows:

- Lack of semantic understanding
- Physical/logical separation – demographics
- Identification, authentication and authorisation
- Appropriate use of standards

Section 3: Project-level barriers

This section is dedicated to the investigation of issues relating to the integration of digital identity which have the greatest effect at a project level. The study finds that a number of barriers transpire from a closer look at this level, and consequently that this is the level from which these need to be addressed. The content of this section is as follows:

- Learning from mistakes – start with small scale pilots
- Interregional intransposability

Section 4: Conclusions and policy recommendations

This section proposes a series of policy recommendations and options. It follows the structure of the report in that the recommendations are sub-divided in three levels: individual, systems, and project level.

Annexes

The report includes the following in annex:

- Appendix A: List of references.
- Appendix B: List of acronyms (Glossary).
- Appendix C: Results of the validation workshop survey.

1 INTRODUCTION

1.1 Objective

The purpose of this project is to identify the technical, organisational and legal barriers to EU-wide deployment of digital identity technologies. With the aim of removing these barriers, we consider a range of policy options.

As a result of the high quality discussions at the expert workshop held in London in February 2007, the final list of barriers has evolved considerably since the interim version of the report.

The dedicated weblog for this project has also supported ongoing discussions amongst the project team and invited experts, providing further input to this report.

1.2 Scope

The scope of this final synthesis report is to determine:

- Barriers to the EU-wide deployment of digital identification technologies across both private and public sectors.
- The economic, legal and social significance of these barriers, means of eliminating them through policy making and the likely timeframes for achieving this.

Figures estimating the relative importance and ease of resolution for each barrier were collected at the expert workshop, with the aim of making the most important and most easily resolved barriers the earliest subjects of policy making initiatives. (See Appendix C).

1.3 Audience

- IPTS
- All workshop participants
- Ultimately for wider publication.

2 Overview

This section sets the scene from which we can consider the barriers from different perspectives. Section 2.1 defines important concepts and terms used in this study. Section 2.2 explains the structure of the report.

2.1 Terms and definitions

For the purposes of this study, we have used the definition of digital identity (eID) proposed by the Modinis IDM Project [MOD]:

> 'A digital identity is a partial identity in digital form: For any given entity, there will typically exist many digital identities which may be unique or non-unique. A digital identity can be created on the fly when a particular identity transaction is desired.
>
> 'A digital identity is, by definition, a subset of the identity and can in effect be considered a manifestation of an entity's presence in an electronic Identity Management (IdM) system (i.e. it is the subset of attributes belonging to an entity that is accessible through a specific IdM system).'

According to Philip Windley [WIND], identities can be classified into tiers:

1. **Abstract Identity**: timeless and unconditional traits or features of a subject, e.g. eye colour
2. **Shared Identity**: attributes assigned to subjects by other subjects, e.g. your employee id card — which is shared between you and your employer and is temporary in nature
3. **Abstracted Identity**: used to identify groups, e.g. the group of people who when shopping at a supermarket also regularly buy petrol

Tier 1 identities are the innate characteristics which form the basis for biometrics.

Tier 2 identities are the domain in which *digital* identities operate.

Tier 3 identities have practical uses, e.g. data mining customer behaviour, and are relevant to this study due to privacy concerns resulting from profiling.

This report therefore investigates all three of these tiers. The term 'eID' is deliberately used in a broad sense, in order to encompass many different forms of digital identity across all sectors. Whilst traditional government-issued identification clearly forms part of this debate, it is not intended to be our main focus.

Whilst identity is considered in fairly broad terms in this report, the term 'identification' is used specifically to denote 'unique identification of an individual'.

In our investigations, we treat 'integration' as an increase in mobility within the sector, whether this stems from social, political, legal, market, technical or potentially other types of development. Whilst clearly the prosperity of the sector is a vital element of this, the potential for harmonisation is also a strong priority.

In investigating the barriers to the integration of digital identity, we define a 'barrier' as anything which blocks, limits, complicates or delays the development of a harmonised EU-wide digital identity sector. The elimination of these barriers should be understood as a drive to allow the "basic movement" provisions of the EU to take effect: free movement of services (both eID services, and the services which depend upon eID), free movement of persons (especially in a cross-border context). This in no way implies enforced uniformity. Indeed, the dangers of over-integration are clearly recognised (see Section 3.2).

2.1 Approach

Originally, our report [INTERIM] segregated barriers into 'legal, market, technical and social' categories, which made a useful starting point for discussions at the workshop. In practice, however, discussions constantly ranged across all of these areas, due to the complexity of the subject matter. It was therefore agreed to restructure this report in order to reflect the shape of those discussions, whilst keeping the technical, organisational and legal implications in view.

The concept of user-centricity dominated the workshop, from the opening comments to the final conclusions. The central position of user experience within identity management is illustrated in **Figure 1** below. The EU-funded PRIME project, with its central focus on the user experience, was repeatedly referenced by the expert delegates. Consequently, 'individual' presented as the dominant category. As one might expect from discussions surrounding identity, all of the key findings could be considered as relating to the 'individual'. However, where there are also significant systems or project elements those categories have been assigned.

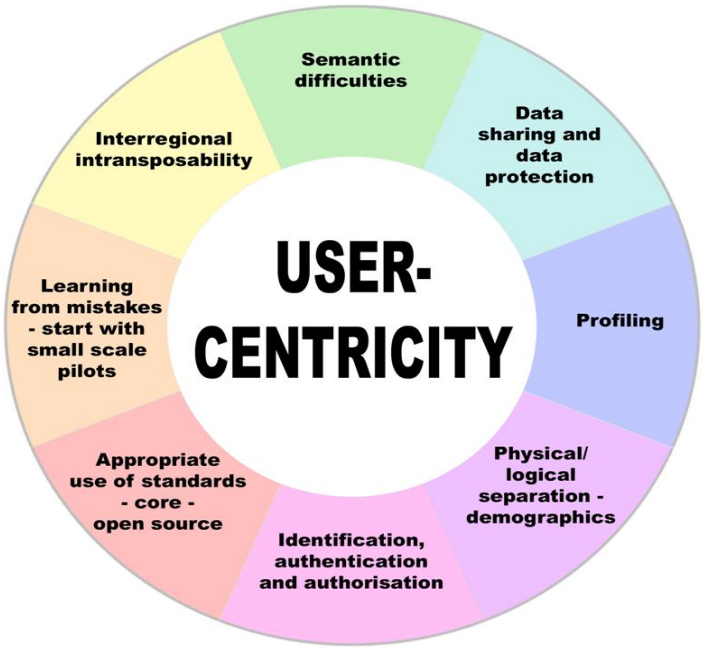

Figure 1 - User-centricity

In principle, the individual level could encompass all the issues identified. There are, however, also significant implications relating to the framework within which the technology is implemented, which clearly ties many of the issues to the 'systems' category. When looking at the implementation of the technology, it also became clear that certain points should be considered at each individual implementation. These were categorised as 'project' issues. Following the workshop, it became clear that the key issues could best be categorised in the following way:

- Individual – most applicable at an individual/personal level
- Systems – most applicable when considering systems design
- Project – most applicable to project management/implementation

3 Individual level

This section is dedicated to the investigation of issues relating to the integration of digital identity which have the greatest effect at an individual or personal level. As one might expect from discussions surrounding identity, all related issues could be considered as relating to the 'individual'. However, where there are also significant systems or project elements, the relevant issues have been assigned to those sections.

The content of this section is as follows:

- User-centricity
- Data sharing and data protection
- Profiling

3.1 User-centricity

3.1.1 User interface

While the ID credential itself is relatively trivial, the user experience has immense power to act as a boost or a barrier to the integration of digital identity. It is the user interface which defines the experience: a strong connection between an ID credential and its context is vital. J.C.R. Licklider, an ARPA psychologist and computer scientist, credited with envisioning the internet in the 1960s, described an 'on-line interactive vicarious expediter and responder' [OLIVER] in 1968, in order to highlight the potential for human-computer interaction:

> 'At your command, your OLIVER will take notes (or refrain from taking notes) on what you do, what you read, what you buy and where you buy it. It will know who your friends are, your mere acquaintances. It will know your value structure, who is prestigious in your eyes, for whom you will do what and with what priority, and who can have access to which of your personal files. It will know your organization's rules pertaining to proprietary information and the government's rules relating to security classification.' Importantly, Licklider recognised that people and machines possess diverse aptitudes: 'certain genotypic differences in capability between men and computers do stand out, and they have a bearing on the nature of possible man-computer symbiosis and the potential value of achieving it.'[SYMBIOSIS]

It is essential to appreciate the intrinsic qualities of both people and computers and to design the interface between the two so that it plays to the strengths of each. As Donald Norman argues:

> 'Because humans and computers are such different kinds of systems, it should be possible to develop a symbiotic, complementary strategy for cooperative interaction…People excel at qualitative considerations, machines at quantitative ones. As a result, for people, decisions are flexible because they follow qualitative as well as quantitative assessment, modified by special circumstances and context. For the machine, decisions are consistent, based upon quantitative evaluation of numerically specified, context-free variables. Which is to be preferred? Neither: we need both.'[ANALOG]

Fitting technology to its human operator is the only practical alternative to the techno-centric 'blame and train' cycle: a failure occurs, the operator is blamed, then trained but the failures continue because the system is designed around machine-based technology and not around its human user.

Historically, user interfaces have tended to be developed around particular processes, rather than the person accessing those processes. Even some of the most popular graphical user interfaces still rely heavily on text-based menu items. In order for systems to be truly effective, it is vital that their interface should be as accessible and intuitive as possible.

The PRIME project is a strong example of user-centric design. The PRIME user interface is very graphical, as compared with the traditional process of selecting a context from a text-based list. It uses a city as a metaphor within the interface, including pictures of a bank building and an industrial park. This type of approach shows considerable promise for the future.

3.1.2 Accessibility and e-inclusion

In looking at user experience, it is essential to recognise that individual user capabilities and therefore experiences will vary in many different ways. There is much talk of the 'digital divide'. In fact there are many different types of digital divide: educational, financial, within nations, between nations, as well as areas of disability, where accessibility is traditionally considered. There is also the 'digital drop-out' to be considered, who may previously have participated in society in a digital sense, but now chooses not to [POLITICS].

To underline its commitment to inclusion and accessibility, the European Commission has designated 2007 as the 'European Year of Equal Opportunities for All'[6]. Clearly, from a commercial point of view, it is desirable to include as many people as possible into any given eID scheme. Also, there is a legal aspect, since there are laws in member states (e.g. the UK's Disability Discrimination Act [DDA]) requiring reasonable efforts to be made to be inclusive and accessible when offering services.

Consult Hyperion's work for the Irish Government's National Disability Agency (NDA) has raised the following issues relating to integrating technical eID systems:

- No technology can include everyone. For example for every biometric chosen, there will be people who, for one reason or another, cannot conveniently supply that biometric (e.g. those without fingers cannot provide fingerprints; some cannot remember PINs).
- There are standards created by the European Committee for Standardization (CEN) for encoding preferences of a token holder for how terminals interact with them (e.g. large, high-contrast print for the partially sighted; induction loops or higher volumes for the hard of hearing) [CEN].
- Retrofitting accessibility is hard to do, so scheme providers need to think of it from the beginning (e.g. in the UK, the Post Office installed chip-card readers that were fixed in a position that was too high for wheelchair users to reach).

A prime example of the Commission's commitment to equality is the eInclusion@EU project,[7] with its aim to support ICT policy making in this area.

As noted in the blog for this project by Mart Pave of the Look@World Foundation, Estonia has placed great emphasis on inclusion:

- 'National ID-cards issued to over 75% of the population.
- Fully functional Digital Signature Act and numerous e-services provided by both the private and public sector.
- Parliamentary elections at the end of February with electronic voting, using digital signatures based on the ID-card's certificates.

---

6 http://equality2007.europa.eu

7 http://www.einclusion-eu.org/

- In April 2009 a service called Mobile-ID will be launched, which allows the use of eID via cellphone (certificates are stored in SIM cards, WPKI).

The Look@World Foundation, which is in fact a third sector organization, is renowned for having dramatically decreased the digital divide in Estonia through its efforts. From a population of around 1.4 million, it has provided basic computer tuition free of charge to over 100,000 people and installed over 500 Public Internet Hotspots, for the benefit of those who do not own their own PC. It is social campaigns such as these which can really contribute to widespread acceptance of digital ID.'

3.2 Data sharing and data protection

The concepts of data sharing and data protection are at the centre of an emerging conflict within the digital identity arena: we want interoperable standards in order to permit the free flow of data globally, while also requiring strict privacy restrictions in order to control that same data flow. Technology is generally intended to enable its users, however security technology has a preventive role. It is this juxtaposition which makes the management of data protection particularly challenging.

Sharing of identity data across organisations in the private sector is a thriving business area[8]. It is of great value to an organisation providing goods or services to understand its customer, and there has long been a practice of buying and selling personal data between private organisations. Such data sharing is tightly controlled in the EU by data protection legislation, requiring permission to be obtained from individuals before any such sharing can take place. The EU Data Protection Directive 1995 was enacted in order to provide a standardised regime across the region. A central stipulation of the Directive is that anyone storing personal data about an individual is required to register with the Information Commissioner within their own member state. It also clearly defines acceptable and unacceptable uses of data and limits on data export. This has provided a strong framework around which expectations of data protection can be measured. However, standards of data protection still vary considerably between member states. For example, the UK Data Protection Commissioner has made efforts to highlight the levels of abuse resulting from inadequate penalties and to ensure that appropriate penalties are imposed [PRIVACY]. In contrast, Belgium is recognised by a recent EC report as having a very strong data protection culture, which is very closely aligned with the original intentions of the Directive.[9]

Although historically the US has not had a strong data protection culture, Senate Bill 1386, introduced in California in July 2003 [SB1386] is proving very effective in highlighting the issue of privacy. This legislation requires that any potential disclosure of unencrypted personal information about Californian residents should automatically be notified to the individuals concerned. This has had the effect of increasing the visibility of data protection nationally, with the result that many other states have enacted similar laws. The public humiliation of having to publish details of breaches and the cost of notification has led to a greater level of security awareness, with organisations increasingly encrypting their data.[10]

3.2.1 The risks of linking identities

An important element of this discussion is the way in which identity in the physical world has traditionally been fragmented, providing individuals with the ability to maintain a sense of privacy in different spheres of life. Perhaps perversely, lack of semantic understanding (see Section 4.1) can even be regarded as providing a kind of practical benefit in this respect. If this

[8] http://www.192business.com/files/imagemanagermodule/@random43463ce8b4e6b/192_GlobalUS_release_160506.pdf

[9] http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/consultation/technical-annex_en.pdf

[10] http://www.boston.com/business/globe/articles/2007/01/18/firms_face_pressure_to_encrypt_data/

issue were to be resolved, and all the diverse identity links joined up, this could pose a major risk to privacy. As highlighted by Caspar Bowden of Microsoft in the blog for this project:

> 'EU Data Protection authorities have expressed concern that adopting a technology policy goal of ensuring that biometric templates are interoperable between disparate systems could have the effect of lowering barriers to inappropriate adoption of biometrics in applications where they would "over-identify" the individual, and unnecessarily erode the individual's sense of autonomy.'

3.2.2 Data Sharing in the Public Sector

In the public sector 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.

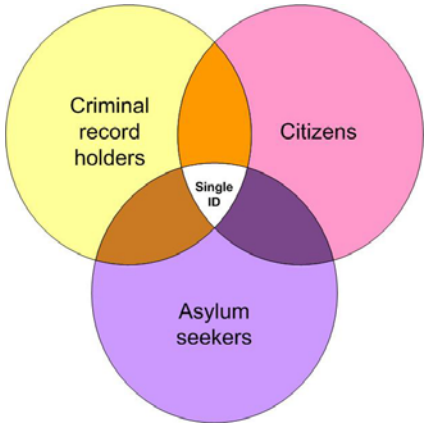

Figure 2 - Single ID for individuals migrating between populations

An asylum seeker might be granted refugee status, become a citizen of a particular nation and then go on to acquire 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 some data sharing between systems is required if we are to achieve effective person IdM across government. 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 no record of them may be found and it is necessary to record an instance of a new identity. This is extremely inefficient if, in fact, the individual in question does already have a relationship with the organisation, or a wider structure within which the organisation belongs (e.g. a government or retail consortium). 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 within suitable data protection controls (e.g. obtaining permission from the individual).

Some interesting work is being done in this area by the EU-funded GUIDE project, researching the potential for data sharing across European borders. This will eventually culminate in a 'real-world "proof of concept"'.[11]

3.2.3 Case study: Austrian Citizens' Card

Widely regarded as an example of best practice in the implementation of digital identity, the Austrian Bürgerkarte scheme[12] provides extensive functionality across a range of applications,

[11] http://istrg.som.surrey.ac.uk/projects/guide/faqs.html

both public and private sector. Based upon firm open standards principles, it underlines a strong regard for inclusion, security, usability, interoperability and efficiency at all levels.

Having initially been used for providing electronic membership cards for the Austrian Computer Society and service cards for civil servants and students, the scheme now includes the following extensive functionality:[13]

- Health insurance card for every citizen
- ID capabilities included in all bank cards
- Digital signature to enable mobile phones to work as a citizen card

The Austrian e-government strategy, which was initiated in 2000, was strongly reinforced by the 2004 'E-Government Act', with the aim of actively promoting the widespread use of digital ID at all levels (local, municipal, provincial and national) across the country. With support at the very highest level of government, the scheme has always aimed to guide and encourage the gradual and realistic adoption of a wide range of interoperable IDs, rather than imposing a strict structure. Indeed, their stated principles are:[14]

- Proximity to citizens
- Convenience through efficiency
- Confidence and security
- Transparency
- Accessibility
- Usability
- Cooperation
- Sustainability
- Interoperability
- Technological neutrality

Fundamental to the success of the scheme has been continued government support at the highest levels, which has even extended to funding the building blocks of the system, in order to encourage early and widespread take-up. Digital signatures, as defined by the 1999 EU Directive, are now implemented widely both in bank cards and ID cards. As an example of platform independence, they are even made available in mobile phones. Whilst all this functionality is offered to citizens via ID cards, it is the choice of the individual whether to activate the electronic signature associated with their ID and so activate an identity link.

The commitment of Austria to digital interoperability is equally noticeable at an international level. They have worked directly with other European countries where digital ID is also widely accepted, such as Belgium, Italy and Estonia, in order to integrate their respective ID capabilities. Equally here, a non-intrusive approach is taken, simply adding the foreign citizen to the Supplementary Register and creating an identity link from an identifier on their foreign eID.

Perhaps this case study shows an unusually rosy picture of government eID implementation. Another perspective, suggested by Niall Barry of the Irish Government's Department of Social and Family Affairs in the blog for this project is more pragmatic:

> *'Standard IdM wisdom such as Kim Cameron's Seven Laws [LAWS] is fine from a private sector perspective, but modifications need to be made somewhere when integrating them into the public sector thinking. The first law states:*

---

12 http://www.buergerkarte.at

13 https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/AustrianProfile

14 http://www.egovmonitor.com/node/1523

1. User Control and Consent: *Technical identity systems must only reveal information identifying a user with the user's consent.*

Governments tend to take a very different stance: you will give us the following information and you have no choice about what that information is and how it is used if you want to be part of the society we run. Indeed some governments, such as the UK, plan to go further and make the user liable to a fine if the information changes (e.g. address) and the user does not inform the government within a given time period. Maybe this is a form of 'user control'.

3.3 Profiling

Profiling involves the collection and analysis of data, providing an insight into individual attributes and behaviour. Very closely linked to data sharing and data protection, it poses such an immediate threat to privacy in its own right that it merits separate discussion here. Beyond privacy considerations and the potential for price discrimination, it may also give rise to redlining: a practice whereby whole geographical areas are marked out for economic exclusion (circled with a 'red line' on the map to mark their boundaries).

The development of data mining technologies has increased capabilities for organisations to analyse personal information at a group level and also potentially at an individual level. The type of very detailed personal data gleaned from loyalty card records can be valuable as a commodity in its own right and is readily sold to third parties at considerable prices. This has become particularly visible in the USA, where controls on this type of activity have historically been relatively relaxed.[15] Indeed, it was recently reported that ISPs are selling details of individual users' click streams to third parties, in order to raise extra revenue.[16]

Price differentiation has long been associated with the rail and air transport industries, with their complex ticketing structures and large variations in price for apparently similar journeys. The sophistication of advanced processing techniques is now making this type of differentiation viable in a wider range of market areas, including consumer electronics, book sales.

It is important to recognise that the economic effects of increased processing power are not entirely one-sided, as auction sites and shopping agents give the consumer greater power to identify the best deal available on a particular purchase [PRIVECON]. Equally, many would argue that profiling offers the potential for improved customer service, if used appropriately.

3.3.1 Case study – Harrah's Casinos

With advanced analysis and marketing techniques increasingly being used to drive sales, the associated 'Business Intelligence' industry is thriving. Harrah's Casinos, based in the US, is a prime example of the business benefits to be derived from this approach. Starting from a relatively weak position around 2000, they have increased their market value from $3m to $17m over the past seven years. Under the leadership of Gary Loveman, a Harvard Business School professor, they have relentlessly followed a policy of deep data mining, in order to gain a detailed understanding of their customers' preferences and habits. Much of this analysis is carried out in real time, in order to provide an environment which will encourage gamblers not to leave the casino:

> 'Analysis of gambling patterns in the Teradata database showed that most customers have a "pain threshold" beyond which they will not bet. When losses reach that point, they may become disillusioned and leave the casino. Harrah's now uses software... to anticipate dissatisfaction and intervene before it happens. If the computer flags that Betty is about to reach a level of losses at which she usually quits, for example, she will

[15] http://www.epic.org/privacy/profiling/
[16] http://internet.seekingalpha.com/article/29449

> be offered a free meal or a ticket to a show to keep her happy and keep her in the casino.'[17]

While offering the ability to provide exceptional levels of customer satisfaction, this degree of intervention could have the potential to undermine an individual's self-determination. Indeed, no doubt aware of these potential criticisms, Harrah's has a very strict 'responsible gaming' code of conduct. Their personnel are trained to recognise problem gambling situations and there are policies in place which permit a person to choose to be removed from the casino company's marketing database and even be excluded from their premises:

> 'Our "self-restriction" program allows a person to request not to receive direct marketing by Harrah´s owned, managed, or operated properties, as well as be denied credit and check cashing privileges. Our "self-exclusion" program allows a guest to request to have all privileges, including play privileges denied at all Harrah's owned, managed, or operated properties.'[18]

With 15% of the US population signed up to Harrah's reward programme, the Gold, Platinum and Diamond cards are influential tokens. By offering different incentives to different customers according to their previous spending habits, the company is able to increase revenues.

3.3.2 Profiling in an international context

The exact value of an individual's personal data varies according to context: as the level of privacy increases, so any available data increases in value. Similarly, there are variances in levels of data protection from one country to another, which will affect the availability and thus the value of personal data. A key principle in controlling profiling is purpose limitation, which implies that data may only be used for the specific purpose for which they were collected.

Technical means, such as the mechanisms being developed around contextual integrity,[19] are being explored as a means of providing this protection to personal data. This would appear to be a positive way of controlling access, providing a lighter touch than legal measures. However, following the uproar surrounding Sony's introduction of insecure DRM software,[20] very strong assurances surrounding the security implications of any such initiative will be required.

Data protection is taken very seriously in Germany but less so in other areas of Europe and still less in the US, where data mining is increasingly widespread. The Safe Harbor framework was introduced by the US Department of Commerce[21] in order to enable US-based companies to self-certify their compliance with the requirements of the EU Data Protection Directive 1995 [DPDIR]. Without this compliance, they are not permitted to process personal data originating from within the EU. Safe Harbor itself strictly limits the uses which can be made of these data. Consequently, standard US data protection statements found on many global e-commerce sites (effectively 'use my data as you wish') can not be enforced in EU member states.

Some interesting work is being undertaken by MIT, in investigating the potential for controlling data use, rather than data collection, on the basis that information is now so freely dispersed, that it is largely impossible to control availability. This work places a very strong emphasis on policies governing the actions which may be performed on data and maintenance of a detailed audit trail, in order to provide transparency in verifying that those policies have not been contravened. [TRANS]

3.3.2.1 Case study – the SWIFT network

A recent statement by the European Data Protection Supervisor concerning provision of financial data to the US Treasury from the Belgium-based SWIFT network (Society for

---

17 http://www.information-age.com/article/2007/january_2007/nothing_left_to_chance
18 http://www.harrahs.com/harrahs-corporate/about-us-responsible-gaming.html
19 http://michaelzimmer.org/2007/01/11/economist-on-contextual-integrity/
20 http://www.washingtonpost.com/wp-dyn/content/article/2005/11/02/AR2005110202362.html
21 http://www.export.gov/safeharbor

Worldwide Interbank Financial Telecommunication), demonstrates the complexity of privacy in a cross-border context:

'In the aftermath of the terrorist attacks of 11 September 2001, the United States Treasury ("UST") addressed multiple subpoenas to the SWIFT operation centre in the US. SWIFT did not oppose the subpoenas, but privately negotiated with the UST an arrangement on how to comply with them. Personal data were therefore communicated by the SWIFT US operating centre to the UST through a "black box" construction, which first permits a massive transfer of data from the SWIFT database to the "black box", owned by the UST, and in a second time, allows for a focused search by the UST.' [EURODP]

A number of data protection principles, which the European Central Bank, as data controller, is responsible for upholding, were highlighted in relation to this transfer:

- Purpose limitation - the data were supplied in order to carry out a financial transaction and should not be used for any other purpose.
- Information to the data subject – the data subject has the right to know how his data is being used and by whom and to take corrective action where appropriate.
- Transborder data flows – appropriate protection must be provided to data being transferred to countries beyond the European Community.
- Notification and independent supervision – data controllers have an obligation to notify the Data Protection Officer of their activities and involve the European Data Protection Supervisor, where appropriate.

The statement strongly underlines the principle that, even under extreme circumstances, it is vital that data protection policies are respected. It is interesting to compare this with a statement by the Canadian Information Commissioner about this same incident:

'The Commissioner determined that SWIFT was subject to the Personal Information Protection and Electronic Documents Act. She…determined that SWIFT had not contravened the Act when it disclosed personal information to the UST. The Act allows for an organization such as SWIFT to be able to abide by the legitimate laws of other countries in which it operates, and an organization may disclose personal information without knowledge or consent in response to a subpoena issued by a court, person or body with jurisdiction to compel the production of information.'[22]

Although the Canadian Commissioner affirms her solidarity with her European colleagues at the end of this statement, there is a clear difference between their legal positions: The use of subpoenas by the US to demand the transfer of data relating to Canadian citizens from an international organisation such as SWIFT is recognised as acceptable within the law. Clearly, more open and visible means of sharing information are preferred, but in principle this type of transfer could still take place.

In contrast, European data protection controls make this type of transfer unacceptable. For international organisations, this makes the requirements for regulating the sharing of personal data extremely complex. A particular example of this is the conflict between the 'whistleblower' requirements of the US Sarbanes Oxley Act of 2002 and French data protection laws.[23]

On a practical level, the 'black box' scenario as described above can be considered the least desirable situation. Where information is requested, it is always preferable to query one's own data in order to provide a response. Once the entire database has been provided to a third party, all control is lost and the data may be used freely for potentially unspecified purposes from then onwards.

---

22 http://www.privcom.gc.ca/cf-dc/2007/swift_exec_070402_e.asp

23 http://www.globalcompliance.com/pdf/SOXComplianceEUDataPrivacyLabor.pdf

4 SYSTEMS LEVEL

This section is dedicated to the investigation of issues relating to the integration of digital identity which have the greatest effect at a systems level. Although clearly these could all be considered as relating to the 'individual' they also have significant systems elements which justify their inclusion in this section.

The content of this section is as follows:

- Lack of semantic understanding,
- Physical/logical separation – demographics,
- Identification, authentication and authorisation,
- Appropriate use of standards.

4.1 Lack of semantic understanding

4.1.1 Terminology

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 the Modinis IDM Project [MOD]), but rather one of agreement and thereafter correct usage. For example, in the EMV (smart card credit/debit) payment specifications, the PIN entry stage of a chip and PIN transaction is referred to as Card Holder Verification (CHV). Similar steps in other industries are often referred to as authentication, a term which, in EMV, refers specifically to the cryptographic checks carried out to ensure that a card (not necessarily the cardholder) is genuine.

This is not merely an academic issue, but rather one that strikes at the root of achieving eID interoperability. The solution to this barrier is not clear, but what is for sure is that it is not to build another glossary, rather a consensus of definition is required to enable integration to be discussed between partners from a foundation of common understanding.

The FIDIS (Future of Identity in the Information Society) Network of Excellence has, in working with the International Standards Organisation (ISO), taken a considerable step forward in producing a 'framework for the definition of identity and the secure management of identity information''.[24] Its stated aim is 'to provide to both the experts and the non-expert a common and explicit understanding of the identity domain, facilitating the comprehension and the sharing of knowledge on this subject' [FIDIS]. However, there are still more fundamental semantic difficulties at the very heart of any discussion of electronic identities (see Section 4.1.1.1). This is not only a technical domain but also one with profound social implications: For any implementation to be successful, these considerations must be central to the design process from the outset. It is not sufficient to attempt to bolt on security after the main thrust of development has taken place.

4.1.1.1 Trust

A particularly interesting example of semantic differences at the most basic level is the divide between social science and technical science over the definition of trust (a concept central to any IdM discussion) [TRUST]. This concept was explored in some depth by Angela Sasse at the project workshop:

[24] http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=2145

Trust is clearly only required in situations of risk and uncertainty. From the social perspective, in the first instance, one is aware of being vulnerable but expects to derive some gain from the act of trusting. This is the reason for accepting the risk of trusting in that situation.

As this trusting relationship continues and becomes habitual, one becomes reliant on the other party and the concept of risk becomes more remote. If the trusting party suffers an abuse of their trust (e.g. a phishing attack) at this later stage, there is a tendency for them to become angry and withdraw from the situation on a permanent basis. The long-term implications of this for e-commerce are potentially devastating.

Consequently, it is essential to provide incentives for a trustee to be more trustworthy (perhaps through codes of conduct), rather than looking for ways to encourage users of a service to be more trusting. Given the potential for opportunistic crime,[25] it is important not to create opportunities for abuse, nor to force people to trust a system, nor to create symbols of trust (e.g. a brand), as these could all increase the user's vulnerability and ultimately rejection of the system.

It is more productive to focus on symptoms of trust. In the physical world, these might be a clean, well-presented shop with contented-looking customers at the counter. In the digital world, the equivalent might be reviews on Amazon, which reassure us that other people similar to ourselves have bought and enjoyed the kind of books which we are interested in. In this context, the term 'assurance' is often used to denote a level of confidence and trustworthiness. The cost of countermeasures in a low trust environment is considerable. Although in principle everyone is economically better off in a high trust environment, a low trust environment is considerably less damaging if breached.

4.1.2 Federation

While trust is well known to be a thorny subject, which has perplexed philosophers over the centuries,[26] even recently designated and apparently rigid technical terms can prove similarly problematic. The topic of identity 'federation' was continually discussed at the expert workshop for this project and, perhaps surprisingly, also offers scope for misunderstanding:

The definition provided by Computer Associates appears quite neutral: 'Identity federation provides a foundation for validating users (or services) from various organizations that are part of a network of business partners. In this way, users (or services) can seamlessly access resources provided by those trusted partners.' [CA]

However, when viewed from another perspective, federation can start to appear less benign: 'At its worst, user-centrism does nothing for data subjects but greatly extend the reach of unintended cross-domain sharing of identity data about them, resulting in the creation of a common identifier with each and every user-centric data transfer; in this scenario, the data subject is in essence contributing to "super-federation." Once previously unlinked accounts are linked, the data subject is powerless: from here on, organizations can reliably exchange data about the user directly among themselves.'[CREDENTICA]

As a result of the workshop, it became clear that the term 'federation' is widely used to imply authentication carried out on-the-fly, as a result of the once-only provision of specific individual credentials from one system to another with the user's assent, as well as the more traditional definition involving the creation of permanent links. The former model offers considerably greater protection for privacy and so the distinction in this case is particularly important.

In the implementation of federated systems, unlinkability (the separation between identities used by an individual in different contexts, so that one identity can not effectively be associated with another) is a central concept, which requires detailed definition and merits legal protection.

---

[25] http://www.privacyrights.org/ar/onlinepubrecs.htm
[26] http://www.open2.net/trust/

In order to protect this unlinkability at the application layer, a substrate of anonymity is required at the transport layer.

4.2 Physical/logical separation - demographics

4.2.1 Physical/logical separation

Firstly, we must be sure to differentiate between the physical device (such as a phone, laptop, smart card, key ring with secured memory) and the digital identity credentials which may be electronically loaded onto that device and later erased from it. These credentials have no physical existence in themselves, being composed of electronic encoding of personal data. The relationship between the two could be compared to a pair of glasses, in which the frames play only a supporting role to the lenses. This type of relationship will be familiar to many from the standard OSI networking model.

From a security perspective, clear means of separation are required to ensure that multiple digital identities retain their integrity within a single selector [MANAGING IS]. An adaptable identity selector controlled by the user could provide the required versatility, although user education would be essential in promoting its use. As an example of this functionality in practice, the EU Framework 6 'InspireD' programme has developed a tamper-resistant personal authentication device (Trusted Personal Device), which permits its holder to collect and use soft credentials in the course of their daily activities.[27] This may not be available for immediate adoption, but offers considerable promise for the future of high security credentials.

4.2.2 Demographics

As different social groups tend to favour different forms of connectivity (desktop computer – home user, laptop – business user, mobile phone - teenager, public kiosks – casual user), these preferences and their potential successors should be accommodated when designing identity solutions in both public and private sectors. These factors are important to bear in mind before expecting, for example, a single national (or indeed international) eID from government to be accepted, trusted and used by all groups for all manner of transactions.

The digital identity sector is best served by retaining maximum flexibility in the range of devices supported and the types of virtual identity which can be loaded onto those devices. Therefore, it is essential that we are not tied down to any fixed expectations of formats. The overlap between the worlds of brand (and marketing) and identity may be at the core of the future eID business model. The idea that identity can be branded is hardly revolutionary (in a world where Aussie football players change their names to Coke and Whiskas) but the ramifications of 'tribal' branding go well beyond anything we may have seen to date: it may be very uncool for a teenager to log in to a chat room using an e-government ID rather than a Nike ID and hence the interoperability of private IDs would be more important to them.

It is certainly the case that the absence of brand in the first wave of digital ID deployment contributed to poor market traction: Brands like Verisign were not recognised by consumers and so they were not readily accepted. The role of brands in the identity management value network therefore deserves further investigation. The future consumer, doing business online, may well find that a virtual identity with a good eBay reputation is a more attractive trading partner than a real identity with a government badge. If this sounds far-fetched, note that under the recent agreement between PayPal and GE Consumer Finance to create the PayPal Buyer Credit product, eBay sellers with high approval ratings can offer interest-free payment periods on goods over $199 or low interest rates on purchases over $1,000.

[27] http://www.inspiredproject.com/

4.2.2.1 Case study – France's Minitel Service

France's legacy videotex information service, Minitel, provides an interesting historical view on the way that different formats can appeal to different demographics over time. Launched by France Télécom in 1982, it achieved widespread popularity long before the Internet was widely accessible and boasted over 20,000 active sites and six million dedicated terminals by its height at the end of the 1990s. The immensely popular home shopping and 'Minitel Rose' adult services were widely used across all age groups and throughout the country.

In its latter years, Minitel is now largely the preserve of the older generation, with many middle-aged people using a mixture of Minitel and Internet and the younger generation using only the Internet for information searches and transactions.[28] Although it is now in decline with a residue of 5,000 services (maintained by 1,500 providers), the simplicity and familiarity of the interface is cited by many as the reason that as much as 16% of the French population still has access to Minitel.

Some legacy applications, such as placing orders on the Interflora floristry network, are still handled exclusively through the Minitel platform. Services such as online banking also still form a significant percentage of traffic, due to the perceived security of this technology developed before the age of PC viruses.

Amongst other services, people regularly use their terminals in order to check:

- Directory services e.g. yellow pages
- Business information in a commercial context
- Daily information updates such as the weather forecast or sports results.[29]

These services are now also offered through a version of Minitel accessible via the Internet, with a similar charging structure to the legacy service. Service providers have been understandably reluctant to lose the commercial model behind Minitel, by which content is chargeable. This commercial influence has provided a clear disincentive for providers to move exclusively to the Internet, where the expectation is normally that information is free.[30]

Although the demise of Minitel seems inevitable, France Telecom's campaign, 'Et-hop Minitel', has served to slow this a little by making web content available via Minitel devices.[31] This may only be a short-term solution, but may provide a means for entrenched Minitel users to become accustomed to experiencing the Internet in a 'safe' environment.

4.3 Identification, authentication and authorisation

In order to design effective IdM systems, it is vital to recognise the essential differences between identification, authentication and authorisation. For the purposes of this report, we will consider identification as the association of an identity with an entity (human or machine), authentication as the validation of a credential and authorisation as the granting of rights.[32]

Clearly, the three are very closely linked and may often need to be implemented in combination. However, this should never be assumed without first considering the system design requirements.

4.3.1 Identification

It is particularly important to draw a distinction between identification and authentication, as confusing the two carries considerable risks (see Section 4.3.2). It may be helpful to consider

---

28 http://www.nytimes.com
29 http://www.leskiosques.com/V3/solutions/minitel/breve15_03_2007.php4
30 http://www.leskiosques.com/V3/solutions/minitel/doc/article_minitel_AFP_100307.pdf
31 http://www.leskiosques.com/V3/solutions/minitel/doc/bilan_minitel_2006.pdf
32 http://www.dcoce.ox.ac.uk/glossary/

the traditional context for identification: meeting people. On first meeting a person, we learn their name and associate that name with them. This is the basis of identification.

When we subsequently meet the same person, we are able to identify them. We are also able to authenticate them as being the same person that we met previously. This does not imply any particularly strong authentication: the authentication is as trustworthy as the person who originally introduced us. If we introduced ourselves, then any subsequent authentication is based on observed information: physical characteristics, associations, behaviour (see Section 4.1.1.1).

Enrolment and revocation are both critical considerations relating to identification in IdM systems. A system is only as secure as its weakest link and this could be the enrolment process. The process of enrolment is responsible for providing a degree of confidence that the person accessing the system has the entitlements which they claim to have. The process of authentication then seeks to provide a degree of confidence that the person seeking access is the same as the person who originally enrolled. In some systems such as national identity systems, this might involve claiming an absolute identity. If a fraudster succeeds in breaking the enrolment process then they will be able to authenticate as a legitimate user with impunity. A strong revocation process is therefore vital for correcting a situation such as this.

Clear consensus was reached at the project workshop that identification for its own sake is undesirable within a system. The less we implement identification, the more privacy will be protected. However, according to Clive Reedman, one scenario where it may be necessary to employ an element of identification is in a large scale eID system in order to ensure that a 'clean' database exists.

4.3.1.1 Legal definition of identification

It is interesting to note the variation in definitions of identification between different legal systems. As a result of national legislation based on the Data Protection Directive 1995, most EU countries (apart from the UK and Ireland[33]) count indirectly identifying data such as ISP IP logs as personal data and hence provide it with considerable legal protection. The Irish[34] and British[35] transpositions comprehend this only if the data directly identify the subject (or potentially if the data identify the subject with other information already in the public domain). The indirect sense of identification is not recognised. This is clearly important when considering the scope of profiling (see Section 3.3).

According to Dieter Sommer revocable anonymity, which is possible in a strong trust model without involving any new parties in the transactions, might prove an effective way of limiting identification if legal steps are taken to reduce the use of unconditional anonymity in particular scenarios. Credential systems which can provide this type of functionality often have the benefit of a formal security proof and are technically mature. However, it can take time for decision makers in industry and government to acknowledge this and progress from older standards (see Section 4.4).

4.3.2 Authentication

Traditionally user authentication is considered as a means of validating an identity, and consists of up to three factors [AUTH]:

1. Something the user has (such as a token or smart card)
2. Something the user knows (such as a PIN or password)
3. Something the user is (biometrics – such as fingerprint, iris or voice)

---

[33] http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/consultation/technical-annex_en.pdf
[34] Data Protection (Amendment) Act 2003, Section 1(1)
[35] Data Protection Act 1998, Section 1(1)

A clear example of the dangers of confusing authentication with identification is the inappropriate selection of credentials: information such as 'mother's maiden name' is freely available from public information sources. It would be very easy for a fraudster to gain access to this information and use it to 'authenticate' himself as a chosen target.

Similarly, passwords and PINs which provide the authentication in a conventional computer system are easily broken. For this reason, they should be chosen carefully with minimum strength requirements, as well as regular changes being enforced. For any system requiring a reasonably strong level of authentication, it is wise to consider certificates, smart cards and possibly also biometrics. The key consideration is that the means of authentication should not be freely available to a third party.

Connection technologies are well understood and easy to implement (networks, IP, etc). However, disconnection (i.e. ensuring that data cannot be accessed by those without permission to do so) is harder: end users may not appreciate the security provided to their data by particular security architectures. Equally, organisations may put too much trust in end-technologies such as smart cards and biometrics, without designing effective security into the wider system. 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 (see Section 4.4.2). This gives them much greater control over the types of access made available, who has this access and it also allows for quick and effective disconnection where necessary.

However, sometimes only a much broader level of authentication may be required. As Peter Brown states in the blog for this project:

'in many situations we don't really need to 'identify' the person as such, but only some property relevant to a particular situation: "Sorry, women aren't allowed into the sauna until 12 today; men only" or "There's no way he is 18 years old, I'm not selling alcohol to him".'

The following are privacy good practice considerations [LAWS-ID]:

- "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.

It is important to remember that privacy is not necessarily achieved at the expense of security [RAENG]. Indeed, often attempts to trade one for the other would point to design issues. Privacy-enhancing technologies are a very powerful tool against the insider threat, which is very hard both to detect and to defend against. According to a recent survey, 63 per cent of global technology companies who responded are very confident that they are protected against external attacks, whereas only 47 per cent have the same level of confidence in their protection against internal attacks.[36]

Mutual authentication (where both the entity connecting to the system and the system itself provide authentication credentials) was highlighted at the project workshop as having a huge contribution to make towards increasing the global level of security, without any loss of privacy. At present, it is usual for a party connecting to a system to provide credentials, but rare for that system to provide credentials in return. For example, an ATM machine will authenticate a card being used to withdraw money but the card has no mechanism for verifying the authenticity of the ATM machine.

[36] http://www.deloitte.com/dtt/cda/doc/content/dtt_DR_ProtectingDigitalAssets_062106.pdf

Common frauds, such as phishing attacks, rely on this lack of verification and the introduction of checks to ensure that both the entity initiating the connection and the entity receiving the connection are valid, would greatly improve the level of trust within the online environment. There are, however, substantial cost implications, which may limit the implementation of these types of checks in the short term.

4.3.3 Authorisation

As mentioned by Martin Meints at the workshop, in practice identity tokens are normally selected with a particular type of authorisation in mind (for example a credit card or club membership card). An important consideration here is that while cards may be technically similar, if they have significantly different enrolment requirements, integration is unlikely to viable. For instance, a supermarket may require no proof of ID to enrol for its loyalty scheme, just name and address details taken at face value. A bank, however, will have an enrolment process that requires multiple proofs of ID and residency (such as passports, driving licence, utility bills etc.).

Both the bank and the supermarket may issue eID tokens according to technically similar specifications. However, the bank will not accept authorisation on the strength of credentials provided by the supermarket loyalty card. This is not due to issues with the eID token itself, or the level of security provided by the authentication token, but because of differing requirements in the enrolment process. In order to overcome this barrier, there needs to be a common means of securely identifying the extent to which a user's identity was verified at registration, such as the registration levels defined by tScheme.[37] There then needs to be a technical and secure means of sharing this level of registration between integrated eID schemes.

On a practical level, individuals do not appear to want to be identified unless there is a very clear reason for it, as Angela Sasse pointed out at the project workshop. For example, paying congestion charges by token is much more acceptable than being tracked according to time, date and location by a central identifying system. The token solution provides authorisation, without the unnecessary extra identification processes.

Similarly, the use of blind signatures for paid video downloads is an interesting example of using the minimum necessary credentials for a purpose. There is no social or commercial need to identify the person paying for this legitimate downloaded material, so it is implemented on the basis of minimal authentication and authorisation.

4.4 Appropriate use of standards

The saying goes – 'The great thing about standards is that there are so many to choose from.' According to Bart Preneel, standards are proliferating across Europe, as each country creates its own standards and even within small countries such as Belgium, struggles are emerging between regional standards. It is important to take a long view, creating a global vision before ever-increasing divergence leads to extreme fragmentation. Most of all we need a framework for components, rather than simply producing specifications.

The 'pyramid' framework for integration (**Figure 3 - Presumed Integration Framework**) clearly highlights the relevant issues of integrated eID across domains. It is based on three levels: the strategic level, the procedural level and the systems level. While the technical complexity around integration is greatest at the bottom of the pyramid, technical integration 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 regulatory integration.

An example of the way in which technical requirements may be overcome was provided by Martin Meints at the workshop: In Germany the handling of data had historically been very distributed. However, last year last year it became clear that data exchange between the

[37] http://www.tscheme.org/

different regions would be required. Within one year this has been achieved through the implementation of an XML scheme. Once the requirements were identified, the implementation was relatively quick and clean.

A positive lesson can also be learned from the implementation of a national travel card in the Netherlands. A requirement for the tender was that the card specification should subsequently be published as open source. This seems like a potentially fruitful way forward, preventing a single supplier from completely dominating individual markets.

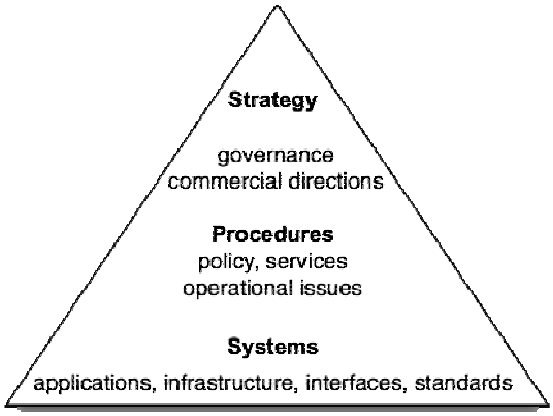

Figure 3 - Presumed Integration Framework

4.4.1 Legal implications

Organisations need legal certainty in order to transact. Where this legal certainty is provided by contract (e.g. credit cards) then there is not a problem but where this certainty is going to be provided by national laws within an EU framework, first it is necessary to identify the competent authorities and how they might, in practice, achieve interoperability.

For the past decade, public key infrastructure (PKI) has been heralded as the ideal solution for electronic identification in both the public and private sector, but it is only now starting to reach the market sizes predicted for it over 10 years ago. User interface issues have been a key contributing factor to this lack of success for large user bases. Smart cards and PKI may be more secure than username and password for user security but, if the systems are significantly more complex for users to master, they are unlikely to be accepted.

When looking to integrate different eID solutions, the issues relating to user interface are multiplied further. Users may have adjusted to the user interface of one eID system, but this may not necessarily mean that they adapt well to the interface provided by another. For instance, if an individual tries to use their bank ID to access e-government services and is presented with a significantly different user experience to that which they are used to when interacting with their bank, this may well act as a barrier to the customer's use of integrated eID, even if the technical infrastructure is in place.

The key to overcoming this barrier is in seeking to integrate not only the identification credentials, but also the identification process (e.g. providing a cross-organisational 'single-sign-on' experience for users). A standard code of conduct across all banks for carrying out transactions online was proposed by Angela Sasse at the workshop. This might prove effective in countering phishing and consequently might also make it possible to hold an individual personally liable for fraud resulting from actions which contravene the agreed process.

4.4.2 Case study – the US PIV card

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 existing 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 considerable efforts, on the understanding that there will be a significant market for many years to come. A bottom-up approach has enabled key users of the system to contribute to its development. In the US individual firemen and police officers are feeling motivated to contribute towards the development of their own ID solution.

Mike Butler of the US Department of Defence provides an insight into the driving force behind the introduction of the US PIV card in the blog for this project:

'The United States Federal Sector, at the direction of the President, undertook the ambitious goal of creating a common Federal credentialing standard as directed in Homeland Security Presidential Directive (HSPD) 12. The Presidential mandate entails the definition of a new technical standard, revisiting 50 years of policies on vetting and suitability, and has an aggressive timeline for activation. From the signing of the directive, it has now been 26 months and massive business changes are soaking into the infrastructure of our Federal Agencies…

'Popular lore has it that when Hernán Cortés reached the New World, he burned his ships. Ultimately, he sent a message to his men and his adversaries that he was committed to success. Likewise, in order for HSPD-12 to be successful, it has been necessary for many different groups to make commitments and sacrifices. The goals of HSPD-12 are set in information sharing across networks, information assurance via secure smart credentials, yet also true to the concepts of federation which allows different business lines to adapt their unique needs. However, to reach these goals 'vertical market industries' have had to adapt product lines and marketing strategies to fit into a world where 'interoperability' among credentials is the overarching goal.

'Computer middleware, driver software, smart cards, physical security systems, and all of their associated business lines are being shocked out of the past 20 years of comfortable proprietary supply chains. We have seen rewards already in those agencies (such as the Department of Defence and the Department of State) who have long standing smartcard and PKI implementation that common credentials, secure computer log-on, Public Key enablement to enhance self service, and new physical security systems and business lines based on these tools are just emerging. The application of these technologies and common secure credentials is just opening a door to new opportunities to dramatically change past business processes'.

Although there is still a variation in the extent to which the CAC specification is implemented between different US government departments, the effect of a presidential mandate has been greatly to increase the urgency with which the specifications have been adopted and the degree of homogeneity across departments. Momentum is clearly a vital factor in ensuring the implementation of standardised systems, requiring co-operation across a wide range of industry and government groups.

5 PROJECT LEVEL

This section is dedicated to the investigation of issues relating to the integration of digital identity which have the greatest effect at a project level. Although clearly these could all be considered as relating to the 'individual' they also have significant project-related elements which justify their inclusion in this section.

The content of this section is as follows:

- Learning from mistakes – start with small scale pilots
- Interregional intransposability

5.1 Learning from mistakes – start with small scale pilots

Both the degree of innovation around the digital identity sector and the fact that the technology is so profoundly personal imply that eID implementations carry very high levels of risk. Good quality risk models are required. These will need to be highly qualitative, due to the sensitivity of the risks involved:

'Attitudes to risk vary across individuals, and may be different at different levels of an organisation. Risk attitudes or appetites may also vary across different aspects of the same risk, may in reality not correspond to any stated appetite and may change with new or better information. Policy-makers seeking to aggregate these views therefore face many difficulties. Not least is the problem of knowing which public understandings of risk to take seriously and which not. In some cases, the public may understand risk issues very clearly.' [RISK]

It is important to remember that the risks relating to identity extend far beyond monetary considerations. Crimes such as identity fraud can damage a person's reputation and standing within the community. Where identity systems holding health information (for instance cards stating blood group and allergies) are compromised, the results can even be life-threatening. Whether the effect is financial, social or physical, in many cases it can cause lasting damage.

Most of all, it is vital for the sector as a whole to learn collectively from experience (both positive and negative). The US PIV implementation offers us many lessons (see Section 4.4.2). Similarly, there are many lessons to be learned within the EU.

5.1.1 Digital signatures

It was agreed at the workshop that digital signatures are effective within a single-domain model i.e. within a closed environment such as a corporate system or Identrust in the banking arena. Given that the aim of the 1999 EU Directive on electronic signatures is to provide a firm basis for legal non-repudiation in a wider digital context, significant progress is still required. We are not aware of any examples of eID signature non-repudiation actually being upheld in law. Indeed, according to John Browning, repudiation as a legal concept may be considered to be beyond the scope of technical solutions, for example: an accused person may claim that an action is performed under duress or on the basis of incorrect information having been provided to them.

As Dave Engberg pointed out at the workshop, many points made relating to eID are in fact orthogonal to whether ID is electronic or paper-based. Because eID is regarded as a new concept, there is a tendency for it to be surrounded by unrealistically high expectations, in a way that may not apply to its paper-based equivalent. There is a mismatch between technical actions (e.g. digital signature) and the legal equivalent (handwritten signature). Clearly, digital signature can have a lot more to offer than handwritten signatures (e.g. potentially strong non-

repudiation within agreed communities such as IdenTrust). But how do you measure that the implementation is appropriate and correct and feed this into any legal processes?

There are effectively two approaches: to assert that a digital signature has the same status as a hand-written signature (this is a quicker solution but potentially unpredictable). However, the alternative is to alter all existing legislation which requires an agreement to have a particular form e.g. 'in writing'. This is clearly too great a task to be practicable.

There is already a considerable history of legislation relating to Digital Signatures:

- Utah Digital Signature Statute (1995)
- ABA Digital Signature Guidelines (1996)
- UNCITRAL Model Law (1996)
- EU Directive on a common framework for electronic signatures (1999)

The directive has subsequently led to the introduction of local laws within members states, such as (taking the UK as an example):

- UK Electronic Communications Act (2000)
- The Electronic Signatures Regulations (2002)

Unfortunately, there are many concerns remaining over the effective use of digital signatures under the law, especially in a cross-border scenario. On a practical level, both within the EU and elsewhere, questions are increasingly being asked regarding the credibility of archived material which has been digitally signed. With the progress of cryptographic technologies, credible attacks to the MD4/MD5 and SHA-0/SHA-1 families of hashing algorithms are being published [HASH]. As a result their reliability is being called into question. Since these have both historically been used as part of the digital signing process, this is of considerable concern.

A particular threat is posed by Quantum Computing (QC).[38] This is an emerging technology, which could potentially increase processing capabilities to such an extent that exhaustive key search attacks on cryptographic algorithms become very much faster. While this is not capable of much at present, it is perfectly possible that this technology will become disruptive through some leap of discovery and it could undermine existing encryption and digital signature technologies, many of which rely on key searches taking an unfeasibly large amount of time.

5.1.1.1 Practical measures for working with digital signatures

Authoritative advice on the appropriate use of cryptography for longer term storage is available from the ECRYPT European Network of Excellence in Cryptology [KEYSIZE].

One response to the issue of non-repudiation in relation to archived material is the German eWitness programme:

A document is signed with a device which is known to be secure at the time of signing. This is then sent to a Trusted Third Party archive. In 10 years' time, it will be possible to retrieve the archived document from the Trusted Third Party and compare it to the original, to confirm whether it has been tampered with. Although this is working successfully within Germany, this may be because German law is stronger than elsewhere. It fundamentally depends on the reliability of the Trusted Third Party and does not resolve the underlying cryptographic vulnerabilities.

Another helpful approach, highlighting the importance of digital signing being a conscious act by the individual is provided by Ueli Maurer: As a practical measure, Digital Declarations (possibly based on voice or video) are suggested as a means of an individual confirming that they actively intended to sign a document, 'due to this guaranteed awareness, the denial of having signed a document is a precise and meaningful claim, equivalent to the (serious) claim that the signature is forged.' [DIGIDEC]

[38] http://cam.qubit.org/

With regard to non-repudiation, it is interesting to note that biometrics can present similar issues to digital signatures, as Clive Reedman points out in the blog for this project:

> *'Consider a conventional physical signature; it is real and has substance, whereas a Biometric signature rarely uses more than a digital interpretation. Usually in a Biometric application the raw image of the physical or behavioural characteristic is discarded. Where does this leave us if somebody insists that they did not in fact supply the reference?'*

5.2 Interregional intransposability

At its most extreme, diversity in the networked world can be characterised by the following quote:
"The international nature of the Internet will continue to be a persistent problem. Differences in laws among various countries can even lead to a high-tech form of jurisdiction shopping." [BEYOND]

The diversity of legal frameworks across the EU and other countries can indeed act as a barrier to integration in several ways. Harmonisation has an important role to play: clearly, the cost of getting into new regional markets is increased as schemes have to be adapted to fit each new set of regulations (see Section 4.4). Equally, the additional work required to extend an already-established domestic scheme abroad may discourage investment outside of the native region.

When considering matters of best practice and regulation, it is however essential to be aware of which elements of any system are truly transferable and which may potentially have local cultural implications. The 'principle of subsidiarity', which states that any decisions should be taken as closely as possible to the individual citizen, is legally and politically central to this debate. In deciding whether legislation should be enacted at the civic, regional, national or cross-border level, it also requires legislators to take into account the benefits of the action, effect on individual freedoms and whether it is genuinely possible to legislate at a more local level.

Some inventive approaches are already being taken to cope with these situations and it is expected that these will increase (see Section 3.2.3). The clear consequence of this is the need for a strong yet flexible legal structure, if it is to encompass the eID needs of the entire EU region.

In this respect the key principle cited by the Modinis Project[39] is 'the principle of interregional intransposability', which states that, given that cultural matters are central to acceptance, it cannot be assumed that a system which is hugely successful in one region will automatically be successful or even acceptable if implemented in the same form in another location.

Whilst integration may appear to be an admirable aim, it is only really meaningful where the underlying non-digital systems are sufficiently similar. For example, according to Martin Meints, although in principle the French and German health cards could be made to interoperate, the actual health systems behind them are so diverse as to make this a purely technical exercise.

[39] https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi

6 POLICY RECOMMENDATIONS

6.1 Individual level

It is essential that identity implementations offer a very good user experience, in order that the technology can play its vital role in protecting both people and assets. This experience encompasses a range of requirements, including safety, ease of use, privacy, inclusion and accessibility. A number of different measures could be undertaken to support this aim:

- Formation of an institution to raise standards in implementations relating to user experience across the Community.
- Consideration of extending the responsibilities of existing authorities to include wider usability issues.
- Investment by member states into research to improve the user experience of eID systems.
- A commitment by industry to put user experience at the heart of their identity systems, perhaps in association with standards bodies such as the ISO. Given the potential for damage to reputation, prosperity and health from failures in identity systems, the highest standards in engineering for safety should be mandatory in their design [SAFEWARE].

As a result of the EU Data Protection Directive 1995, data protection already has a strong basis within the EU. There are, however, considerable differences in practice between the levels of protection offered in countries across the community. Some possible approaches to correcting this situation are:

- Legal measures to ensure that 'personal information' is understood in effectively the same sense in each jurisdiction.
- A closer investigation of the economics of data protection across the region. This would give the opportunity to investigate the degree to which the laws are in fact enforced and whether penalties provide an adequate deterrent.
- Initiatives to encourage industry co-operation in making data protection a key focus. Perhaps the commercial benefits of assurance could be highlighted in this connection. The promotion of privacy-enhancing technologies which offer unlinkability[40] would bring clear benefits. Equally the risks and benefits of disclosure could be explored.

With the advent of data mining technologies, new issues are arising around the use of personal data. There are several relevant initiatives which could be considered in this respect:

- Legal controls on the sale of personal information to third parties, even if this information was lawfully collected.
- Support for initiatives which strive to develop a global data protection culture, such as the International Conference of Data Protection and Privacy Commissioners.[41]
- Investigation into the social implications of profiling – contrasting the potential for providing outstanding customer service, with the dangers of encouraging compulsive habits in vulnerable individuals. (See Section 3.3.1)
- Incentives for industry to develop effective technical mechanisms to control the use of information once it has been collected.

[40] http://www.jrc.es/home/report/english/articles/vol67/IPT2E676.htm
[41] http://www.privacyconference2007.gc.ca/Terra_Incognita_home_E.html

6.2 Systems level

The lack of semantic understanding between the social and technical disciplines involved in identity, is both one of the most important barriers to integration and one of the hardest to resolve (see **Figure 6 - Barrier Overview**). There are, however, several steps which could be taken in order to mitigate this situation:

- Support could be given to initiatives to increase the understanding of identity across the EU, possibly through the creation of a non-profit organisation. The US Interagency Advisory Board might serve as a model for this.[42]
- Human aspects of security are widely recognised as being more influential and harder to manage than technical aspects. Initiatives to include social modules in technical education courses could lay a firm foundation for the future.
- Research into different mechanisms for building assurance into identity systems should be carried out, underlining the importance of offering reasons to trust in the digital environment.

There is great value to be gained from offering flexibility in the types of virtual digital identity held and the types of tokens on which they can be stored. This permits individuals to choose the physical format which is most convenient or familiar to them, while still enabling organisations to issue a standard set of digital credentials. In order to support this flexibility, the following options could be considered:

- A framework should be developed, governing the interaction between hardware devices and soft identity credentials, to ensure that both flexibility and security are respected during the design process. A layered model, similar to the OSI networking model, would appear to be the most practical way of approaching this.
- A study could be carried out in association with key industry organisations, in order to identify the influence of demographics on individuals' choices for identity tokens. (i.e. preferences regarding storing credentials on cards, mobile phones, key fob tokens).

The key processes which may be required of an identity scheme are identification, authentication and authorisation. In order to establish the scheme, enrolment is required and a clear process for revocation is required, in order to ensure the integrity of the scheme over time. There are many possible approaches to achieving these aims, some of which are detailed below:

- A formal scheme for certifying the strength of enrolment for different levels of functional credentials should be developed. The existing tScheme[43] might serve as a model for this. This would provide a greater level of certainty when dealing with the wide variety of ID credentials across the region.
- Prior to building any system involving directly or indirectly identifying personal data, there should be a requirement to justify Identification, Authentication, Authorisation and Retention policies in writing, with a clear explanation of the motivation behind these system design decisions. The existing data protection authorities might be well placed to oversee this mechanism.
- Greater emphasis should be placed on the revocation process, in order to secure the long-term integrity of identity systems. At present, significant effort is expended on the design process, in order to give users access to a system. However, the reverse process of terminating access at the appropriate stage is often given a lower priority. It might be helpful for the industry to promote its own guidelines for this purpose.

Standards are vital to the effective interaction of identity systems across the region. Their effective use could be promoted in a number of different ways:

---

[42] http://www.smart.gov/iab/
[43] http://www.tscheme.org/

- An accessible framework of standards relating to identity could be maintained, with annual updates, in order to assist with implementation projects. The ECRYPT yearly report on algorithms and key sizes [KEYSIZE] might serve as a model for this.
- Member State governments could learn from the example of the US PIV implementation, by specifying a standard core for all of their identity requirements, whilst still leaving scope for customisation around that core.
- Organisations within industry could promote the use of open source, which ultimately provides increased opportunities for interoperability, flexibility and innovation.

6.3 Project level

There is a wealth of experience available regarding the implementation of large scale identity projects in both the public and commercial sectors. Unfortunately, this experience is not particularly easily accessible, neither is it necessarily applied to subsequent projects. Given that many identity projects are carried out on a very large scale, especially in the public sector, it would seem reasonable to take certain precautions:

- A central log should be set up of large scale government identity projects across the EU region, with open and unbiased reporting of the lessons, both positive and negative, to be learned from these projects. Where possible, details of relevant, international projects should be included. An example of this might be the implementation of Chip and PIN in the banking sector.
- The log should be openly accessible and give the option for regular moderated updates by interested parties, as well as comments and cross-referencing.
- As mentioned above, justification should be provided for system design decisions.
- In order to limit the costs associated with huge roll-outs, industry guidelines should be drawn up, enabling implementers to gain the fullest benefit from risk assessments and pilot implementations, prior to making any large scale commitments.
- A standard code of conduct for electronic identity transactions should be developed, in order to clarify the responsibilities of the end user. If implemented correctly, this could have a major impact on the amount of fraud due to phishing attacks.

Perhaps the most striking issues relating to identity arise from cultural differences at both a national and regional level. It is important to recognise the impact that these differences can have and to draw up appropriate measures to manage them:

- Legal harmonisation has a great deal to offer in opening up the market.
- Initiatives which permit integration without a high level of technical interoperability have a great deal to offer. This principle, used successfully in the Austrian citizens' card programme for accommodating foreign IDs, could usefully be emulated elsewhere.

APPENDIX A REFERENCES

This section lists the references used in this study used in this report.

[ANALOG] Donald A. Norman, *Being Analog*, originally published as Chapter 7 of _The Invisible Computer, MIT Press, 1998. Available from: http://www.jnd.org/dn.mss/being_analog.html

[AUTH] *White Paper, Advanced Authentication*, Thales e-Security. Available from: http://www.thales-esecurity.com/Whitepapers/documents/Advanced_Authentication_.pdf

[BARRIERS] Rebecca Eynon, *Breaking Barriers to eGovernment: Overcoming obstacles to improving European public services*, Modinis study for the European Commission, Oxford Internet Institute, April 2007.

[BEYOND] Bruce Schneier, *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*, Copernicus Books, September 2003.

[CA] *Identity Federation: Concepts, Use Cases and Industry Standards*, Computer Associates, January 2007. Available from: http://www3.ca.com/Files/WhitePapers/identity_federation_white_paper.pdf

[CEN] *CEN/CENELEC Guide 6 Guidelines for standards developers to address the needs of older persons and persons with disabilities*, European Committee for Standardisation, January 2002. Available from: http://www.cen.eu/boss/supporting/reference+documents/cclcgd006.pdf

[CREDENTICA] *Government Online, a Credentica White Paper*, Credentica Inc, February 2007. Available from: http://www.credentica.com/whitepapers/GovOnline.pdf

[DDA] *The UK Disability Discrimination Act 1995, Chapter 50*, Office of Public Sector Information. Available from: http://www.opsi.gov.uk/acts/acts1995/95050--c.htm#19)

[DIGIDEC] Ueli Maurer, *New Approaches to Digital Evidence*, Proceedings of the IEEE, Vol. 92, No. 6, June 2004. Available from: ftp://ftp.inf.ethz.ch/pub/crypto/publications/Maurer04.pdf

[DIGILIFE] *digital.life ITU Internet Report*, International Telecommunication Union, December 2006. Available from: http://www.itu.int/osg/spu/publications/digitalife/docs/digital-life-web.pdf

[DIGISIG] Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures, Commission of the European Communities, March 2006. Available from: http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/com/2006/com2006_0120en01.pdf

[DPDIR] *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.*

[DPCOM] *Communicating Data Protection and Making It More Effective*, 28th International Conference of Data Protection and Privacy Commissioners, October 2006. Available from: http://ico.crl.uk.com/files/Communicating%20data%20protection%20and%20making%20it%20more%20effective%20-%2020%20October%202006%20(E).pdf

[ECONOM] *Complying with rules for identity management*, Economist Intelligence Unit briefing paper sponsored by IdenTrust, December 2006. Available from: http://graphics.eiu.com/files/ad_pdfs/eiu_ComplyingwithRulesForIdentityManagement.pdf

[EURODP] Peter Hustinx, European Data Protection Supervisor, *EDS opinion on the role of the European Central Bank in the SWIFT case*, February 2007. Available from: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Inquiries/07-02-01_Opinion_ECB_role_SWIFT_EN.pdf

[FIDIS] *D 2.1: Inventory of Topics and Clusters*, FIDIS Network of Excellence, September 2005. Available from: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp2-del2.1_Inventory_of_topics_and_clusters.pdf

[FINN] Patrick Wauters, Graham Colclough, *Online Availability of Public Services: How is Europe Progressing? Web Based Survey on Electronic Public Services, Report of the 6th Measurement. Cap Gemini, June 2006. Available from:* http://ec.europa.eu/information_society/eeurope/i2010/docs/benchmarking/online_availability_2006.pdf

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

[HASH] Carlos Cid, *Recent developments in cryptographic hash functions: Security implications and future directions*, Information Security Technical Report, Volume 11, Issue 2, June 2006, Pages 100-107. Available from: http://www.sciencedirect.com

[INTERIM] John Elliott, Dave Birch, Margaret Ford, Andrew Whitcombe, *Barriers to the integration of the EU digital identity sector – Interim Report*, Consult Hyperion, February 2007.

[INTEROP] Mary Rundle and Paul Trevithick, *Interoperability In the New Digital Identity Infrastructure*, Harvard Law School, January 2007. Available from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=962701

[KEYSIZE] European Network of Excellence in Technology, *ECRYPT Yearly Report on Algorithms and Key Sizes (2006)*, January 2007. Available from: http://www.ecrypt.eu.org/documents/D.SPA.21-1.1.pdf

[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

[LSE PIM] London School of Economics & Political Science, *The Identity Project: An assessment of the UK Identity Cards Bill & its implications*, Interim Report, March 2005. Available from: http://www.lse.ac.uk/collections/pressAndInformationOffice/PDF/IDreport.pdf

[MANAGING IS] Steve Purser, *A Practical Guide to Managing Information Security*, Artech House, March 2004

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

[MS ID META] *The Identity Metasystem: Towards a Privacy-Compliant Solution to the Challenges of Digital Identity*, Microsoft, October 2006.

[OLIVER] J.C.R. Licklider, *The Computer as a Communication Device*, Science and Technology, April 1968

[PRIVACY] *What price privacy now? The first six months progress in halting the unlawful trade in confidential personal information*, UK Information Commissioner's Office, December 2006. Available from: http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/ico-wppnow-0602.pdf

[PRIVECON] Andrew Odlyzko, *Privacy, Economics and Price Discrimination on the Internet*, University of Minnesota, July 2003. Available from: http://www.dtc.umn.edu/~odlyzko/doc/privacy.economics.pdf

[POLITICS] Andrew Chadwick, *Internet Politics: States, Citizens, and New Communication Technologies*, Oxford University Press, March 2006

[RAENG] *Dilemmas of Privacy and Surveillance, Challenges of Technological Change*, The Royal Academy of Engineering, March 2007. Available from: http://www.raeng.org.uk/policy/reports/pdf/dilemmas_of_privacy_and_surveillance_report.pdf

[RISK] Michael Power, *The Risk Management of Everything, Rethinking the Politics of Uncertainty*, Demos, June 2004. Available from: http://www.demos.co.uk/files/riskmanagementofeverything.pdf

[SAFEWARE] Nancy Leveson, *Safeware: System Safety and Computers*, Addison-Wesley, 1995

[SB1386] *SB 1386, Peace. Personal information: privacy*, Bill Number 1386 Chaptered: Bill Text, California Senate, 26 September 2002. Available from: http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

[SHARE] *Information sharing vision statement*, UK Government Department for Consitutional Affairs, September 2006.

[SYMBIOSIS] J.C.R. Licklider, *Man-Computer Symbiosis*, IEEE Transactions on Human Factors in Electronics, volume HFE-1, pages 4-11, March 1960

[TRANS] Daniel J. Weitzner, Harold Abelson, Tim Berners-Lee, Chris Hanson, James Hendler, Lalana Kagal, Deborah L. McGuinness, Gerald Jay Sussman, K. Krasnow Waterman, *Transparent Accountable Data Mining: New Strategies for Privacy Protection*, Massachusetts Institute of Technology, January 2006. Available from: http://www.w3.org/2006/01/tami-privacy-strategies-aaai.pdf

[TRUST] Jens Riegelsberger, M. Angela Sasse, John D. McCarthy, *The Mechanics of Trust: a Framework for Research and Design*, International Journal of Human-Computer Studies 62 (2005), pages 381 – 422. Available from: http://www.elsevier.com/locate/ijhcs

[WIND] Philip J. Windley, *Digital Identity*, O'Reilly Media Inc., August 2005.

APPENDIX B GLOSSARY

The table below defines the terms and abbreviations used within this document.

Abbreviation or Term	Definition
2FA	Two-factor Authentication
CAC	(US) Common Access Card
CEN	European Committee for Standardization
CHV	Card Holder Verification (method such as PIN entry)
DoD	(US) Department of Defence
eID	Electronic ID
EMV	Chip and PIN smart credit/debit card standard
EU	European Union
FIPS	(US) Federal Information Processing Standards
GSM	Global System for Mobile (international standards for digital mobile phones)
ICAO	International Civil Aviation Organisation
ID	Identity
IdM	Identity Management
IMS	Identity Management System
IP	Internet Protocol
IPTS	Institute for Prospective Technology Studies
ISO/IEC	International Standards Organisation
LSE	London School of Economics
MRTD	Machine Readable Travel Document
NDA	(Irish) National Disability Authority
NFC	Near Field Communications
NIST	(US) National Institute for Science and Technology
OASIS	Organisation for the Adoption of Structured Information Standards
PIN	Personal ID Number
PIV	Personal Identity Verification (FIPS 201)
PKI	Public Key Infrastructure
PSE	Payment Systems Environment (EMV)
SAFE	Secure Access For Everyone
SAML	Security Assertion Markup Language
SEPA	Single Euro Payment Area
SSL	Secure Sockets Layer

Abbreviation or Term	Definition
UK	United Kingdom
US	United States
USA	United States of America
VWP	(US) Visa Waiver Programme
XML	Extensible Markup Language

Table 1: Terms and abbreviations

APPENDIX C WORKSHOP SURVEYS

An expert workshop, to validate the findings of the Interim Report for this study [INTERIM], was held at the Holiday Inn London Bloomsbury in the UK on the afternoon of 28 February and the morning of 1 March. It was attended by international experts specialising in economic, legal, social and technical aspects of Digital Identity (the focus of the Interim Report).

Two surveys were completed at the workshop, in order to rate the importance and ease of resolution of each barrier. Ratings were collected from the expert participants both prior to the discussions (**Figure 4 - Initial Barrier Ratings**) and then again following the discussions (**Figure 5 - Final Barrier Ratings**). It should be noted that although these results from the expert workshop are of interest, the sample group is not large enough to be scientifically representative. The results of these surveys are shown in the following two charts:

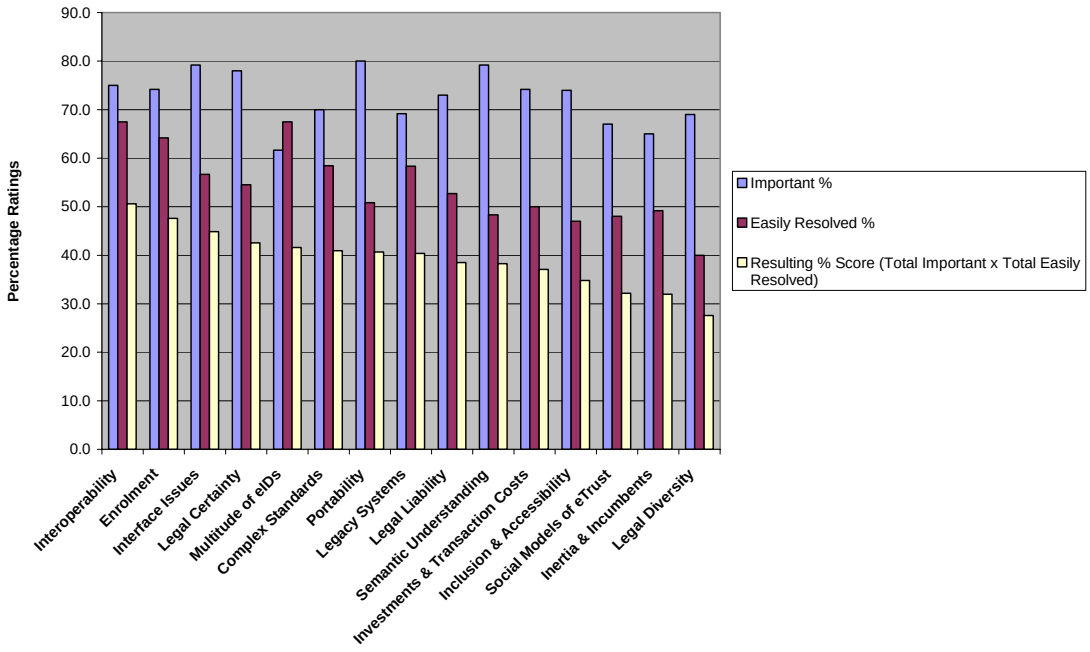

Figure 4 - Initial Barrier Ratings

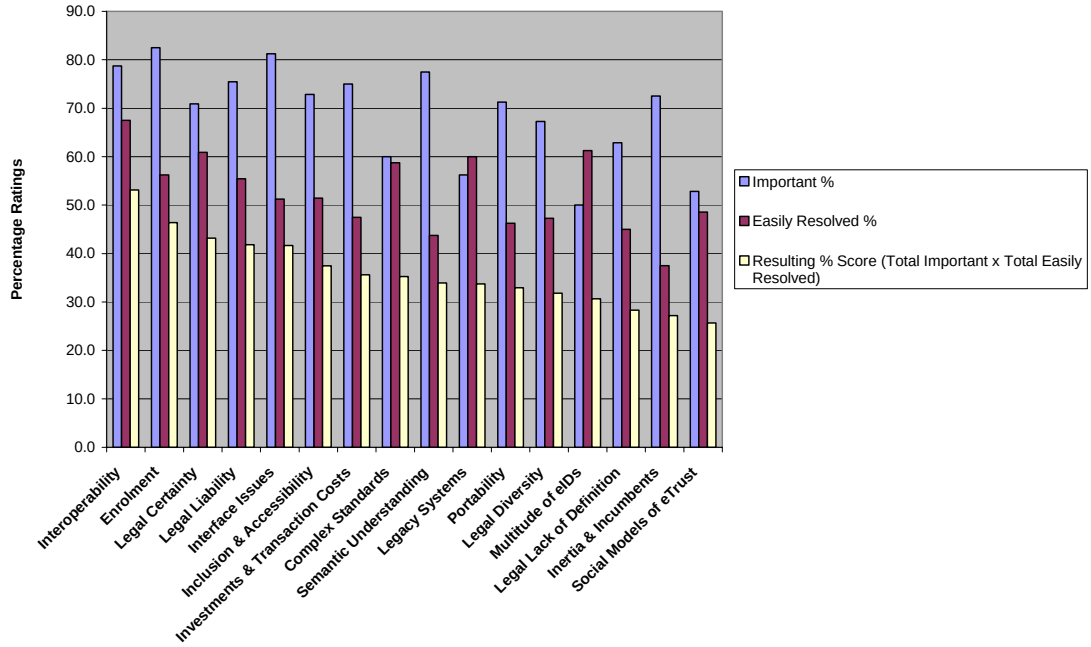

Figure 5 - Final Barrier Ratings

Findings from each of the two surveys appear to be relatively stable: 'interoperability', 'enrolment', 'interface issues' and 'legal certainty' were the top four barriers in the first survey and still within the top five in the final survey. Perhaps surprisingly, 'Multitude of eIDs' was rated quite highly initially but, following discussions, was even suggested as a benefit by one participant. Also, semantic understanding has very high importance ratings but low ratings for ease of resolution, which might suggest a high level of persistence. 'Legal lack of definition' only occurs in the final survey, as it was proposed as an extra barrier at the workshop.

The following slide is included in order to give a simple overview of the relative ease of solution and importance ratings given by workshop delegates to each barrier identified in the interim report:

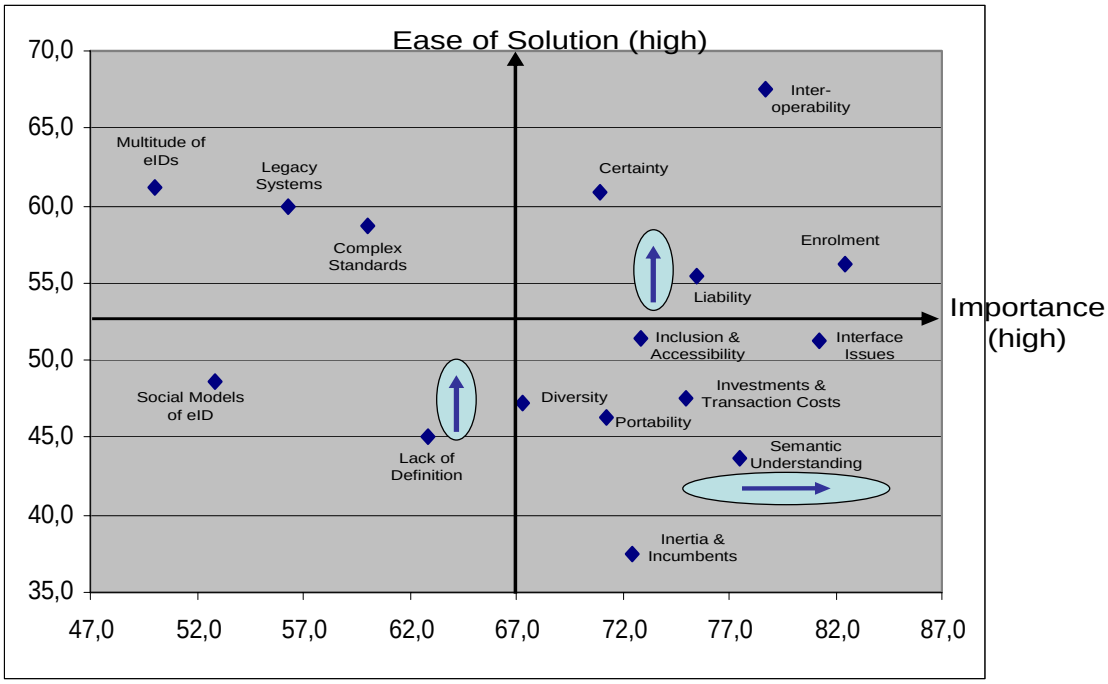

Figure 6 - Barrier Overview

Analysis of these results would appear to indicate that interoperability, enrolment, interface issues and legal certainty are the areas in which greatest progress can be made most quickly. Our policy recommendations have been made on the basis of these findings from the workshop, however further research would be required to confirm this.

The final barriers identified by the experts at the workshop are aligned with the survey ratings in the following way:

Barrier	Relationship to survey
1. Lack of user-centricity	Encompasses many top-ranking barriers, including 'interoperability', 'enrolment' and 'interface issues'.
2. Semantic difficulties	Encompasses 'interface issues' and 'legal certainty', as well as several other market and technical barriers.
3. Conflict between data sharing and data protection	Encompasses 'interoperability', 'enrolment' and 'social models of eTrust'.
4. Profiling	Encompasses 'enrolment' and 'social models of eTrust'.
5. Single format ID card inflexible, unattractive	Encompasses 'interoperability', 'interface issues' and 'portability'.
6. Confusion over Identification, Authentication and Authorisation	Encompasses 'interface issues', 'semantic understanding', 'complex standards', 'legacy systems' and 'social models of eTrust'.
7. Inappropriate use of standards	Encompasses 'interface issues', 'interoperability', 'complex standards', 'legacy systems' and 'portability'.
8. Persistent project failure	Encompasses 'inertia and incumbents', 'investments and transaction costs', 'legacy systems' and 'social models of eTrust'.
9. Interregional intransposability	Encompasses 'interoperability', 'enrolment', 'legal diversity', 'lack of semantic understanding', 'social models of eTrust', as well as several technical barriers.

European Commission

EUR 23046 EN – Joint Research Centre – Institute for Prospective Technological Studies
Title: **Overcoming Barriers in the EU Digital Identity Sector**
Editors: Ioannis Maghiros and Boris Rotenberg
Authors: John Elliott, Dave Birch, Margaret Ford, and Andrew Whitcombe
Luxembourg: Office for Official Publications of the European Communities
2007
EUR – Scientific and Technical Research series – ISSN 1018-5593
ISBN 978-92-79-07818-7
DOI: 10.2791/70350

Abstract

Digital identity is widely considered to be a key enabling technology for successful deployment of the information society. The world of digital identity is still in transition from the era of trials, pilots and closed systems to an era of local and national roll-out, interoperability and open systems. For the EU, there is a need to understand to what extent European integration of the identity sector has been achieved and/or is desirable in order to support this transition, and what are the main technical, organisational and legal barriers that might need to be overcome. The purpose of this project was to identify the most important and/or most challenging barriers to EU-wide deployment of digital identity technologies across both private and public sectors, to enable prioritisation and policy making. In line with the findings from the expert workshop, the categorisation of issues concentrates on the level at which they are most effective. The report finds that barriers arise at three distinct levels: individual level (most applicable at an individual or personal level), systems level (most applicable when considering systems design), and project level (most applicable to project management or project implementation). In the final part, the likely role of Europe is presented, as are policy options for removing the barriers found and for further initiatives at each of the three levels identified in the report.

The mission of the JRC is to provide customer-driven scientific and technical support for the conception, development, implementation and monitoring of EU policies. As a service of the European Commission, the JRC functions as a reference centre of science and technology for the Union. Close to the policy-making process, it serves the common interest of the Member States, while being independent of special interests, whether private or national.

JRC
EUROPEAN COMMISSION

LF-NA-23046-EN-C

ISBN 978-92-79-07818-7