E-identification technologies for e-government interoperability in the EU

Elias Pimenidis*

School of Computing and Technology, University of East London, UK
E-mail: e.pimenidis@uel.ac.uk
*Corresponding author

Ioannis Savvas

Informatics Laboratory, Agricultural University of Athens, Greece
E-mail: jsav@aua.gr

Abstract: The EU commission has set the Pan-European Interoperability of secure authentication and authorisation systems for access to e-government services as a priority target for 2010. To this effect a large number of EU member states have implemented e-identification schemes. These are at varying stages of completion and use a range of technologies. All of them though aim at meeting the above target for interoperability while at the same time securing their home e-government services thus making them more attractive to their citizens. The number of states reviewed here and the state of the technologies used is not exhaustive but provides a good representation across the EU. This work is ongoing as are the initiatives and pilot schemes studied here.

Keywords: e-identification; digital identities; e-government; e-government interoperability; digital identity technologies; citizen card; EU digital identification initiatives.


Biographical notes: Elias Pimenidis is a Senior Lecturer at the University of East London in the UK. The core of his research work focuses on e-business and e-government development projects. Recently, he has taken an interest in security issues in terms of online transactions and in particular, on the effect, these could have on e-government implementations. His other research interests include the evaluation of web services, knowledge management systems and the use of computer games for educational purposes. He is also a visiting Lecturer at the Informatics laboratory of the Agricultural University of Athens, Greece.

Ioannis Savvas is an employee in one of the 13 regional government Directorates in Greece. He is involved in projects exploring the potential of e-government implementations in improving the Greek public administration’s efficiency, focusing in particular, on back office procedures and applications. This is also the focus of his Doctoral research currently undertaken at the
1 Introduction: the need for e-identification

Enterprises, government agencies, healthcare organisations, professional services and organisations all need to exchange valuable or confidential information, while the ordinary citizen is constantly challenged to communicate and transact with all of the above online. The dramatic rise in cyber crime and the emergence of new legislative requirements point to the need for better means to protect digital information and ensuring privacy. Citizens using e-government applications assume that electronic administrative procedures are just as secure and reliable as the classic visit to an office. The public administration is expected to guarantee a high level of data protection and to handle data in a responsible manner. Appropriate measures must be taken in order to ensure that this existing confidence in the authorities is maintained in the context of e-government.

Secure online procedures and network and information security are guaranteed by the use of a variety of methods and mechanisms. Security is increasingly becoming one of the fundamental challenges of our time. Given its increasingly widespread availability, e-government is becoming a critical part of the infrastructure and is therefore, particularly deserving of protection. Particular attention must be paid to central components such as registers and directories. Even small-scale attacks can give rise to uncertainty amongst users, which can adversely affect confidence in electronic administrative services. An adequately secure and protected system can counteract such fears and lead to wider acceptance.

On the 25th of April 2006, the EU commission adopted the e-Government action plan recognising the need for interoperable pan-European e-IDM. Under this action plan EU governments have agreed to facilitate, as a matter of high priority, the establishment for mutual recognition of national electronic identities for public administration websites and services. The action plan foresees full implementation by 2010 (Graux, 2007).

Electronic identities are fundamental for securing access to and convenient use of e-government services in Europe. Prior to the above date, a number of Member States have introduced electronic ID (e-ID) card schemes, whilst others are in various stages of implementation and planning. In researching the different approaches from governments and agencies across the continent and in particular, the EU, it appears that there are a number of different technologies used to allow secure access to government services (Savvas et al., 2006). In order to prevent these developments from creating new digital barriers across borders, a set of minimum requirements and common standards must be agreed to enable European e-ID solutions to interoperate.

One of the biggest challenges for e-government is the diverse number of agencies involved. Not only are citizens and local firms customers, but in many cases, the agencies can be seen as customers as well. But not all customers are equal with respect to level of information sharing; information sharing across networks between the police department and a city operated water department may be done at a different level than the police department and the public citizens of the area. It is important to look at each of
these potential interactions as communication channels that need to be defined in terms of trust, and content. These different entities each have a role in the community’s response to a cyber-security event, and the exercise is structured to explore this aspect of emergency operations. Managing these multiple independent relationships is a challenge that grows exponentially with the number of channels. Thus, the issue of creating a secure and interoperable e-IDM infrastructure becomes more complex (Conklin and White, 2006).

E-schemes need to be able to authenticate users and to support a digital signature facility that can be consistent in an e-transaction process. e-ID cards can incorporate advanced security features (such as biometric identifiers) for convenient proof of identity of a person. For governments, e-ID is therefore, both a secure replacement for paper-based identity schemes and a reliable key to identify and authenticate users of e-enabled public services.

Similarly, as companies and organisations grow, they have multiple systems for managing and using digital identities. The complexities that result from having multiple identity systems generate high costs, management overheads and security vulnerabilities; e-ID can solve the identity and access management challenges, control environments and reduce complexity. However, the road to success is not an easy one.

This paper proceeds by examining the key principles behind the attempt to establish a pan-European e-IDM system. In doing so, the authors review a selection of good practice cases by looking at the technologies used, the penetration achieved and the potential of extending the use of such technologies across domain and potentially national boundaries to achieve the interoperability sought after by the EU commission.

2 E-identification and associated technologies in use

An e-identification is an e-ID document that an individual can use as identification on the Net. It generally contains the information required to identify an individual electronically, such as name, personal identity number, period of validity of the identification, etc. These details do not need to be stored in the e-ID document, but can also be supplied by the issuer in response to an inquiry about the owner of a unique e-ID document. In this instance, the ID document contains a unique designation that can be securely linked to a person. The common denominator for all e-identifications is that they are based on a Public Key Infrastructure (PKI), which can briefly be described as an encryption system, in which the sender and recipient each have an encryption key – a private and a public key (The Swedish 24/7 Agency Delegation, 2005).

In attempting to apply the above principles, many organisations and countries have invested considerable research effort, money and other resources in producing solutions that respond to the above requirements. To be able to expand the application of any technical solution to meet the requirements of a pan-European interoperable e-IDM infrastructure one must consider the following functionalities and whether any of the technologies applied in the cases reviewed here can respond to the challenges posed by differences in language, culture, national infrastructures and customary practices across the different EU Member States. The desirable functionalities are: mutual recognition, identification, authorisation, authentication, electronic documentation and ease of use, security, economy of scale, reducing fraud and ensuring privacy.
In addition to the above in assessing the potential of any solution discussed here the following have to be considered:

1. Usage – How many persons/business have used it and the lessons learnt from such use

2. Common architecture – is there any that can be derived from the cases and how can this be used in a large scale pilot scheme?

3. Are the common lessons learnt and how can these be utilised further to support the common cause of interoperability? (Varghese, 2007).

2.1 The right to a digital identity

The most common technology used in the applications reviewed is that of e-ID cards. The basic concept of the e-ID card was introduced by TeleTrust in the TeleTrust Token 20 years ago. Since then advances have been made, but the basic concept remains: the e-ID card is designed to identify the cardholder, to create a digital signature and to support routines for confidentiality. The card has two key pairs and certificates stored on the chip that forms the primary physical security feature of it (EEMA, 2006). The card is of familiar appearance and usage to most residents of the Member States of the EU, as its features and use are similar to those of a common credit or debit (charge) card that millions across the EU use in their everyday transactions with stores and services.

Recent research has demonstrated that identity cards had historically tended to be introduced by authoritarian regimes and were viewed as a repressive measure. As such, they have been resisted by countries such as the UK and the US (EEMA, 2006). Such fears on the historical use of identity cards have been combined by the considerable cost of introducing, maintaining and operating such schemes (LSE, 2005) that led the UK Government to recall its original plans and reconsider the whole scheme. This decision in relation to the e-ID scheme proposed for the UK is also compatible with the approach adopted by the UK towards e-government projects, where the aim is to develop cost efficient systems that would achieve value adding improvements to the services offered both to the government and the user (Savvas et al., 2007).

However, nowadays the original purpose of identity cards (authoritarian government use) has been lost and they are becoming a useful tool in the battle against organised criminal activities. Since the tragic events of the 11th September 2001, resistance to the ID card in the US had diminished and so has in the UK, since July 2005 following the London Underground bombings. The US is moving ahead with an e-ID card scheme that would provide a single, secure credential that would be tamperproof and hard to forge, and could be used for physical and logical access. A recent example of the usefulness of such an id is at the crisis of hurricane Katrina when it struck the city of New Orleans. At that time 6000 medical personnel wanted to go and help, but were unable to do so because no one knew who they were.

Thus, the concept of a pan-European e-IDM card scheme might sound more plausible and more useful, than ever before, since the need for instant and tamper proof identification is increasing and is embracing issues beyond those of the use of the internet and support services.

The EU and the USA are not the only places in the world that explore single point e-ID systems. Korea for example is trying to explore e-IDM systems to decongest its public services. The example of the Supreme Court where citizens can access documents electronically is a creditable case.
A hardware security module generates an electronic signature with the Supreme Court’s PKI certificate. The secure document generation server delivers this data, as well as an appropriate 2D bar code and a digital watermark, with the certificate to the user’s computer through the web server. The user can then print a legally valid document. This system employs print control and DRM technologies to protect the document’s contents, including the bar code and watermark, during delivery to the user (Kim et al., 2006). This appears a more ‘democratic’ approach to e-ID, but the extent of its usage has not been tested appropriately to lead to conclusions as to whether it can replace e-ID cards.

3 Good practices across the EU

The sections in this part of this paper discuss individual countries and the technological solutions they have implemented in seeking the roadmap towards a pan-European e-IDM Interoperable framework. These are not the only applications, but the ones that have been identified as good practices at a recent evaluation exercise across the EU. There are many other smaller pilot schemes that are expected to deliver creditable results and hopefully valuable conclusions as to the potential of European integration in the area of e-IDM. Table 1 summarises the current state of facts as presented here.

<table>
<thead>
<tr>
<th>Country</th>
<th>Purpose</th>
<th>Technology</th>
<th>Services</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malta</td>
<td>All Citizens</td>
<td>User Name, Password and Activation Pin</td>
<td>One e-government Services Portal</td>
<td></td>
</tr>
<tr>
<td>The Netherlands</td>
<td>All Citizens</td>
<td>Authentication of user through a third party agency</td>
<td>Access to e-government Services – no one point entry</td>
<td>3 million (February 2007)</td>
</tr>
<tr>
<td>Finland</td>
<td>All Citizens</td>
<td>‘KATSO’ outsourcing IDM system</td>
<td>e-government and private sector eServices</td>
<td>100,000 organizations. Citizens to follow</td>
</tr>
<tr>
<td>Ireland</td>
<td>All Citizens</td>
<td>e-passport</td>
<td>No direct purpose</td>
<td>Potentially all citizens</td>
</tr>
<tr>
<td>Belgium</td>
<td>All Citizens</td>
<td>Chip Technology</td>
<td>Services and General Identification purposes</td>
<td>2 million (February 2007)</td>
</tr>
<tr>
<td>Austria</td>
<td>All Citizens</td>
<td>Chip and PIN</td>
<td>Authentication and Identification Potential of Integrating Foreign e-IDs</td>
<td>Most of population by November 2005</td>
</tr>
<tr>
<td>Sweden</td>
<td>All Citizens</td>
<td>Smart card</td>
<td>e-government</td>
<td>500,000 slow uptake</td>
</tr>
</tbody>
</table>

3.1 The Austrian citizen card

Austria has experimented with the issue of e-identification since 1999 and has been one of the pioneering member states in the EU. The name given to the implemented solution is ‘citizen card’ might appear a bit confusing. One might assume a single class of smart-card like devices which is specified in a high grade of details. This in fact, is not
the case; the Austrian citizen card is rather a concept that will show a variety of appearances. The health insurance card rolled-out to each Austrian citizen in 2005 is one of these appearances. The public identity card available as a smart-card in 2002 is another one. Further examples of the citizen cards are member cards of the Austrian computer society, or SSCDs shipped by CSPs that issue qualified certificates. Also bank cards for automated teller machines are following the citizen card concept since May 2005 (Leitold et al., 2002; Rossler and Leitold, 2007).

The citizen card provides electronic signature for authentication and electronic identity for identification and the principle can be applied to any smart card supported by a chip and PIN mechanism issued by any authorised organisation in Austria. The authorities use different personal identifiers derived from the source PIN of the natural person concerned and from the relevant procedural sector. This is an irreversible cryptographic derivation, which is used only once. This means that the source PIN cannot be retraced from the derived identifier. Similarly, it is impossible to derive a new identifier for another sector from an existing derivation (Hollosi and Hörbe, 2004).

Furthermore, Austria has gone a step further into integrating foreign e-IDs into its system by supplying a ‘Substitutional Source PIN’ for foreign identity cards. This has so far been successfully implemented for the identity cards of Italy, Belgium and Finland (Rossler and Leitoldm, 2007).

3.2 Belgium

The key driver for implementing the e-ID card scheme in Belgium was to give Belgian citizens an electronic identity card enabling them to authenticate themselves towards diverse applications and to put digital signatures Proof (Strickx, 2007). At the time of writing, there are more than 4.5 million e-ID cards activated in Belgium. The needs are both political and social. Within the e-government context, the Belgian government aims at offering solutions for strong authentication of citizens accessing online services such as income tax returns, to health services. This is considered crucial as government data is highly critical and should not fall into the wrong hands. Furthermore, e-IDs can be used for authentication in securing chat room use for teenagers as the problems with paedophiles committing crimes online have shaken society in Belgium far too often, in the past.

The country has invested in the strongest form of identification world-wide: a smart-card-based identification. Introducing this to the public was not a problem as Belgium has a long history of identity cards: only the introduction of the chip was a real challenge. However, the issue of usage has been the stronger challenge yet, as it required considerable effort to make people use the e-IDs.

3.3 Finland

Finland have experimented with smart card solutions in the past, but these have proved of little value and have since been abandoned for what appears to be a much more popular and effective system. KATSO is a nationwide solution for outsourcing identity management, authentication (SSO) and authorisation for organisations. This is currently in progress and once complete, it will support,

1 e-government services
2 e-services for the private sector.
Expected users will be all government agencies (e-services) and organisations in Finland (users of e-services). There is a very large user base already with over 100,000 organisations involved. It is expected that this will evolve as the defacto identity management, authentication and authorisation solution for organisations in Finland in particular those involved in Business to Government (B2G) services (Ihalainen, 2007).

3.4 Sweden

The Swedish have opted for a smart-card-based e-ID scheme which is proving quite successful in terms of the level of security provided and ease of use. Under the Swedish National ID card with Electronic Identification (NIDEL) model, the user can download an e-ID certificate from any authorised issuer of e-ID certificates, or from any authorised issuer of role certificates; the chip can be activated any time during the life of the chip (5 years); it is built to Swedish and international standards; it allows for openness and freedom and it provides an easy way to convert from e-ID on files to tokens and cryptographic keys in hardware.

The issue with usage though remains a challenge for the Swedish government. Despite the large number of e-ID cards that have been issued to date, there are 10 times as many e-IDs on software files. The government has been devising incentives to promote the use of e-IDs. One such incentive was introduced in 2004, when those submitting a tax rebate using the e-ID received it three months earlier than usual (The Swedish 24/7 Agency Delegation, 2005).

The Swedish government sees the uptake and use of e-IDs as an essential element of ensuring the efficiency of e-services offered by the state. The public sector has more than three million unique visitors to its websites each month. Many of them perform the services over the net that are offered by the public sector. To enable public players to offer e-services, solutions are required for electronic identification and signatures. Naturally, it is easier for individuals if they are only required to use one type of e-identification, whether they are customers of a company using private e-services or citizens using public e-services. Both the government and citizens believe that the confidence issue is of crucial importance for the use of e-services. For example, a citizen must have confidence that the information and documentation supplied to or received from public authorities over the internet are handled in a secure and correct manner. It should be possible for both authorities and the public to convey information electronically with the same confidence and legal effect as sending information in the form of documents with hand-written signatures.

3.5 Slovenia and Malta

Smaller states and newcomers in the EU have each put in place their own initiatives in implementing e-ID applications.

Slovenia has targeted e-IDs as a means of securing access to government files and services for civil servants only so far. This is a limited application based on the use of smart cards. By the end of 2006 the rate of penetration of the use of e-ID cards had been more than 40% amongst government employees. The scheme is part of the country’s
efforts in improving the efficiency of government services and promoting e-government by achieving the following (Sel, 2007):

- reduction of paperwork
- faster operation of public administration
- accurate and timely data at all offices
- improved and transparent processes
- prevention of abuse
- cost efficient administrative procedures.

Malta has launched its e-ID scheme in 2004 in response to the need for one secure and trusted gateway to government e-services (Pisani, 2007). Currently, this is based on username and password plus activation PIN – similar to the system used in the UK for tax services. E-ID is offered to natural persons only and not companies and is open to all Maltese citizens. The e-ID application process is handled by an independent registration authority. One of the good technical characteristics is that this scheme can be adapted to support any other member states’ own e-ID system, thus accommodating the need for interoperability. The whole system is at pilot state yet and the inclusion of companies is an ongoing phase of the project.

3.6 The Netherlands

Holland has approached the issue of e-ID as a single trustworthy system for communication with the government. This falls in line with the government’s strategic objective of 65% of all public services (at national, regional and local authority level) to be provided electronically by the end of 2007 (Stempels, 2007).

The ‘DigiD’ is capable of proving three levels of security in its objective of supporting an one submission registration for government services. Currently, at middle level it uses the following data:

- **Citizens:** social security number/A-number
  - *Later in 2007:* ‘Citizen Service Number’
  - *Registration only:* date of birth, address data from Key register of natural persons
  - activation letter is sent to the address as known in register.

- **Enterprises:** sector number registers
  - business service number
  - agriculture sector number
  - other sector numbers.

In terms of usage, the uptake has been quite impressive, despite the fact that the required legislation is not complete. The number of registered DigiD users was at 3 million in February 2007 and is expected to rise to 5 million by April 2007. This is quite impressive considering that the total population 16 million and the tax paying part of the population which is most likely to use the e-government services is 9 million.
4 The current status of implementation of e-IDs

Despite the above creditable efforts, the target of interoperability currently appears to be untenable, at least in the scale envisaged originally. It is not a question of availability of technologies and applications, but an issue of readiness and coordination of efforts. Across the currently 27 member states, there is great disparity in terms of strategies, plans, uses, extent of implementation and level of readiness as to e-identification status across the state. Thus, less than 3 years away from the target date, it appears that the interoperability for e-government purposes will only be achieved partially or more precisely through a selection of cases amongst the most advanced countries in terms of implementation (Austria, Italy, Finland) or amongst those who have the highest incentives for doing so (Belgium).

Table 2 presents the summary of the current status of e-identification implementations across not only the 27 member states, but including others that have close associations with the EU (Norway and Iceland) or are candidate members (Turkey). A total of 30 countries have been reviewed. The numbers in each case are divided into two categories, those that have implemented on the basis of four different technological formats and those that intend to do so. A fifth category shows the number of countries that have no central e-identification strategy or infrastructure in place and their plans as to future implementations are either not clear at the time of writing or focus on partial implementations and pilot runs. The graph shown in Figure 1 has been compiled using data drawn from the European Unions official portal on e-government progress, monitoring the events and progress across 32 European countries (epractice.eu, 2007).

<table>
<thead>
<tr>
<th>Timeline</th>
<th>Technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Chip and pin cards</td>
</tr>
<tr>
<td>Present</td>
<td>5</td>
</tr>
<tr>
<td>Future plans</td>
<td>4</td>
</tr>
</tbody>
</table>

Table 2 e-Identification status across Europe

Figure 1 Current status of e-ID implementations and future plans
What is most alarming in this figure is that there are still countries that do not even have a national strategy for e-identification or have not planned for central e-identification infrastructure. These are not just the poorest newcomers to the EU, but include some of the older member states such as Germany and Greece. Amongst the currently predominant implementations are those based on chip and pin cards, while there is a large group of countries using electronic signatures, which are monitored and distributed at national level. Chip and pin identification cards appear to be a current favourite, but also feature well in plans for implementation in the near future, while identification cards based on plastic cards containing software codes appear to be gaining ground in future plans for implementation. Finally, the use of electronic signatures over the internet appears to be losing its appeal in future plans despite its strong presence in current applications.

On 12 September 2007 the e-ID Interoperability for Pan European E-Government Services Draft Common Specifications were presented during the 2nd IDABC e-IDM Interoperability Workshop (Graux and van der Maren, 2007). However, there is no information as to any successful implementation on the basis of these proposed specifications yet and their acceptance and adoption has not been finalised yet.

5 Conclusion

Various Member States have put forward a variety of e-identification schemes ranging as to the objectives, the technology used, application domain and extent of usage. Almost all of them aim at facilitating secure access to e-government services expecting to make these more attractive to citizens and to reap the benefits of more effective public administration. The most common technology encountered is that of smart cards. These appear to be a more attractive solution, especially when combined with the concept of national or local identification cards. Although the issue of identification cards is still the cause for social concerns across some of the Member States, the example of the Austrian Citizen card has demonstrated considerable advantages. This being the most advanced scheme so far across the EU appears to provide a viable solution both in terms of supporting secure access to national e-government applications and facilitating the interoperability features that have been set as a priority by the EU commission. Despite the differences in technologies used, it appears that most of the member states aim at developing applications that would allow them to participate in large pilot schemes that would cross national borders and would eventually lead to a Pan-European Interoperability of e-government services.

References


