# Identifying Obstacles in moving towards an Interoperable Electronic Identity Management System

Amir Hayat*, Reinhard Posch, Herbert Leitold
*Institute for Applied Information Processing and Communication, Tech. Univ. Graz, Austria*
*Tel: +43-316-873-5581, FAX: +43-316-873-5520*
*(amir.hayat, reinhard.posch, herbert.leitold)@iaik.at*

**Abstract:** In this paper we have identified all possible hurdles and obstacles in finding a Pan European interoperable electronic identity management solution. We have also given a brief overview of the existing electronic identity projects. This paper examines technical, social and political issues that are to be considered before we can reach such an interoperable solution.

## 1. Introduction:

In European Union, member states (MS) are working hard for the formation of an information society. MS are working for developing modern public services and a dynamic environment for e-business through widespread availability of broadband access and a secure information infrastructure. A hot issue related to the information society is the electronic identification and authentication of citizens through the use of electronic identity (e-ID). The definition of e-ID as given by the Electronic Identity White Paper is "*A smart card based token, containing private keys and corresponding public key certificates. Optionally, the card may also incorporate a visual identity document*"[1]. The use of e-ID is not only limited to e-government (e-Gov) but also encompass e-Payment, e-Healthcare and e-Transport etc. In the future, an e-ID can be used to vote or declare your taxes via the Internet, act as a travel document, a health insurance card or a purse for securely paying online, and more. Such an e-ID will also offer the option of electronic signature (e-Sig) which is equivalent to handwritten signature according to the Electronic Signature Directive (e-sig) [2].

The electronic identity in Europe was first introduced in 1999 when Finland introduced its first e-ID card. Since then several MS started similar projects. Italy issued its first e-ID card in March 2001- the Carta d'Identità Electtronicà, while Belgium started the distribution of e-IDs in April 2003 [3]. In Sweden more than 100,000 cards have been issued so far, the infrastructure, however is mainly provided by private sector [4]. In less than three years Estonia has equipped 45% of its population with e-ID cards. In year 2005, Austria is planning to roll out the medical insurance cards which will also work as e-ID card. Further, its banking sector will also incorporate the e-ID functionality in their bank cards in the same year. Although e-ID cards have been rolled out in some MS and few others are planning to follow suit, one can observe that interoperability (IOP) of the e-ID has not been given due importance while developing individual systems. Thus a citizen can no longer use his e-ID card for identification, authentication and e-sig with government and private sector as soon as he enters another MS which is also a part of EU. This happens mainly because the electronic identification system in one MS does not recognize the e-ID issued by another MS. Further, as noted in report [5] the lack of IOP, both at national and cross-border level, is a big obstacle for market acceptance and the proliferation of electronic signatures. It has resulted in many

* The work described in this paper has been partially funded by the Higher Education Commission (HEC), Pakistan.

isolated ‘islands’ of electronic signature application, where certificates from only one Certification Authority (CA) can be used for an application.

Various organizations across Europe are making efforts to solve this issue of IOP at political, legal and technological fronts. EUCLID (European initiative for a Citizen digital ID solution), eEpoch, eESC (eEurope Smart Card Initiative), PRIME (Privacy and Identity Management for Europe) and GUIDE are the main organizations working in this domain [6]. In addition to these projects, the EESSI (European Electronic Signature Standardisation Initiative) was launched in 1998 to identify technical requirements and provide related standards.

In the past several studies have also been carried out, from different perspectives, to determine the factors important for bringing about such an interoperable system [5][7][12][5]. However, such studies highlighted one or the other issue but were deficient in bringing the broad picture into light. It is important that for MS who already have introduced e-ID and those who are in the process, the obstacles hindering the way of an IOP solution should be obvious so that a thorough methodology may be adopted to address this issue. Therefore, in this paper we identity all the obstacles hindering the way towards having a Pan European interoperable electronic identity management system. This paper will help the MS who already have their e-ID systems and now are looking at the IOP issues. It will also help the MS who are in the initial stages of their e-ID project as they can design their systems from the IOP perspective.

The concept of electronic identification may apparently seem to be more of a technical issue, yet the social and political dimensions of this issue cannot be overlooked. Therefore we broadly divide the obstacles in technical and social categories. We limit the scope to only identifying the obstacles and not proposing solutions for them. We also limit our discussion to countries within EU. We talk about the e-ID concept in general, however since most of the countries are implementing e-ID using smart cards, therefore we keep that in perspective while discussing different issues.

## 2. Technical Issues

### 2.1. Certification Authority (CA):

In the electronic identification systems, a citizen proves his identity using the digital certificate issued by a CA. However, the CA also needs to be authenticated. The CA authentication and certificate validation process is relatively simple within the MS where it was issued, however it is rather complex when we consider it on a Pan European scale. Consider a typical scenario where a citizen moves from a MS A to the MS B and uses his/her e-ID card for an electronic service. How will the electronic identification system of MS B authenticate the CA of MS A and how can it trust the certificate?

The e-Sig Directive in its article 4 has laid down the basis for the acceptance of advanced electronic signatures based on a qualified certificate throughout EU [2]. However, the practical problem of establishing trust by the authentication of the CA and the validation of the certificate still exists. This issue of mutual recognition and establishment of trust between the CAs has been highlighted in a feasibility report for a Bridge CA by the European Commission [7]. In this report various solutions have been considered for resolving the issue of CA-CA IOP. The solution recommended in this report is the Modified BCA PKI model.

However, the feasibility report also acknowledges that establishing a Pan European BCA is not easy and would not succeed without a strong political support. Further, such effort would have to take into account the policy, legal, organizational and technical issues and would have to reach a minimum IOP basis at the network and protocols levels. Besides these two points, currently there is only one MS having an existing national BCA which indicates that if a BCA will be established, many CAs would have to be interconnected from each MS.

### 2.2. Issues with Digital Signatures:

Practical implementations of digital signature schemes raise a number of issues. When the certificate is installed on a computer, the private key is stored on the hard disk which performs the calculations of the algorithm on behalf of the user. Given the well known threats of viruses, Trojan horses and worms and facing the unreliability of present personal computers it is very hard to make sure that the computer applies this algorithm only when the user directs the machine to do so. There is also no guarantee that the algorithm is applied only to the document presented to the user on the computer screen and in exactly the form as it appears on that computer screen. Schemes to protect the private key are reliable only if the entire hardware, software, operating system and the firmware can be fully trusted, a goal which cannot practically be achieved on a personal computer. Another issue is, if the pair of keys is stored on the computer then how will the citizen carry the e-ID if he/she is travelling to another MS? Copying it on a portable media and carrying it along may compromise the secrecy of private key. Although most of the countries have overcome this issue by using cryptographic smart cards, however the countries which will choose the PC implementation of electronic identity will have to address these issues.

### 2.3. Standardization:

Organizations working across EU for forming standards on electronic identification and authentication include the WS eAuthentication and TC224 working group of the CEN/ISSS and Open Smartcard Infrastructure for Europe (OSCIE). Further, in 1992 EUCLID published the electronic identity white paper laying down the minimum requirements for implementing e-ID systems based on PKI [1]. The e-Sig Directive on electronic signatures has proven to be the legal basis for acceptance of e-Sig across EU. The EESSI (European Electronic Signature Standardization Initiative) programme has developed few standards to assist the implementation of the e-Sig Directive. Although, because of the delay in publishing these standards, several MS had already developed their own technical interpretations of the Directive [5].

However, much work still remains to be done. As mentioned in the International Porvoo Group Conference in Tallinn [8], when developing a Pan European electronic identity, attention must be paid to organizing the deployment, legal issues and standardization. Regulation is needed regarding e.g. the procedures when issuing electronic identity, the issues related to data contents of certificates, data protection and liability. Furthermore, although legislations have been based on technology neutrality, standardization takes a firm stance in favour of PKI [9]. Since technology changes may occur in future thus if applications are not neutral at the level of design requirements there may be problems in incorporating new technologies. Furthermore, MS have varying implementation levels of Annex II of e-sig directive "Requirements for certification-service-providers issuing qualified certificates" which means that the establishment and running of a Certification Service Provider (CSP) will differ considerably [5]. Thus a CSP establishing business in several MS must therefore adapt itself to different requirements and procedures. Product vendors will also have difficulties building products for this fragmented market.

### 2.4. Unique Identification Number (UIN):

In order for governments to provide online service to its citizens and to protect electronic communications, it is imperative that it identifies each citizen uniquely; which brings the issue of UIN. Such a UIN is needed to prove the involvement of a citizen in a particular transaction and to eliminate chances of non-repudiation. Some MS already have such UIN for

their citizens while some other MS are introducing it. For e.g. Austria has established the Austrian Central Residents Register which issues a unique number called CRR to each citizen. Similarly Italy, Belgium, Finland also issue a unique number to every citizen.

In a survey conducted by authors, it was found out that about 11 MS issue UIN to their citizens. On the contrary some MS do not have any plan to introduce such a UIN. Partly it is because of the privacy concerns of a large population of these MS. This is because such a UIN may be used for profiling hence some organizations understandably are against its use. Some countries have constitutional problems for e.g. in Germany the Constitutional Court of Karlsruhe has ruled against having a single identity number for each citizen. The absence of UIN can create an obstacle since the implementation of the electronic signature, creation of public key infrastructures (PKI) and the networking of all public databases has to be based to a large extent on the widespread use of the UIN. The question is that in the countries where such a UIN does not exist, what would be used as unique personal identifier? And how will this issue be resolved at Pan European level?

### 2.5. Public Key Infrastructure (PKI):

E-ID cards are used in the PKI environment. In terms of the promotion of Pan European PKI framework, however, there is a need to ensure that parties in different PKI domains can interoperate. It is necessary for cross border initiatives to be formed to ensure that the different PKI structures and practices are examined and deliberated to develop a mutually agreed inter-working PKI framework. In order to have an IOP system, the White Paper on Electronic Identity sets it as a minimum requirement to have an established PKI [1]. In our opinion since the e-sig Directive has not laid down such a restriction so MS may use the services of any accredited service provider in another MS. But in either case, every MS needs to have a system to identity and authenticate the e-ID cards.

The technical specification by ETSI [10] provides the guidelines in establishing a PKI and specifies policy requirements relating to certification authorities (CAs) issuing qualified certificates. However it may take a while before we see interoperable PKIs established throughout Europe. Further, some MS believe that using the existing authentication systems like password and PIN, they can still manage the security challenges so there is no need to invest in establishing PKI. In a study carried out in 2001, some MS were of the opinion that about 80% of electronic services currently provided by the public sector can be sufficiently protected using a password or a PIN [12]. For the remaining more sensitive services that require strong authentication, these MS believe that a system where electronic certificates are issued by accredited CAs will suffice. Thus these MS believe that they do not have to involve in large-scale, complex and costly procedure of creating a material object like an identity card with a chip and distributing it to all citizens.

Furthermore, the strong technical complexity in the combination of PKI and smartcards for identification purposes features hot spots in the installations of the smartcards and the signature software [11].

### 2.6. Availability of Information:

Currently there are about nine EU member states that already have or are in the process of introducing e-ID. As these MS are making progress, they are generating useful information and 'Best Practises' regarding all the aspects of setting up the infrastructure for an electronic identification system. However not all of this information is accessible by the specific e-ID websites. A survey of such websites, dedicated to the electronic identity, reveal that either the web site is only in the native language or if there is another version of it then it just provides general information and is not as comprehensive as the actual web site. The translation of this information in other EU official languages or at least in the most widely spoken languages has

not been done. Any attempt to create a Pan European IOP electronic identification system will certainly need the details about each individual system. The limited availability of this information will not make the job any easier.

### 2.7. Limited Availability of Electronic Services:

Citizens in MS are not motivated to get an e-ID since there aren't enough electronic services available. On the other hand the vendors are reluctant to invest in an electronic service since there aren't many users with e-IDs to use it. This dilemma similar to Chicken and Egg conundrum is hindering the progress of e-ID projects. Finland may be taken as an example, it was the first country to introduce e-ID cards yet those who possess this cards use it rarely. This can be explained by the still limited types of transactions with the administrations, for which a citizen can use the e-ID cards [12]. This is also the overall condition in EU. The report [5] has posed the question about the current utilization of electronic signatures in Europe and has noticed that there is currently no natural market demand for qualified certificates. The largest application area in Europe for e-Sig is generally linked to e-banking applications in a closed user environment. Within the scope of the e-sig Directive, very few applications are in use today and they are almost completely limited to e-gov.

### 2.8. Hardware and Software Issues:

Depending on the requirements of MS for their e-ID projects, one can observe a range of applications from vendor specific to open source. For e.g. Malta is using the Microsoft solution[13], Italy is using the Baltimore Technologies solution [14] and Estonia is using DigiDoc based on open source OpenXades [15]. When an IOP system will be tried, the incompatibility issues of these heterogeneous platforms may pose some hurdles. MS with an existing e-ID project have their proprietary applications used to interact with e-ID cards. However, when such an application will have to interact with e-IDs from other MS, it will have special requirements like specific APIs and drivers which may or may not be available. This may create acceptability problems of e-ID outside one MS.

A further issue that is starting to emerge is IOP between authentication technologies and other technologies used in the process of generating, transmitting or receiving a transaction. There are already instances where authentication technologies can be rendered ineffective by other technologies [16]. For example firewalls and gateways can reject digital signatures or encrypted messages as they could possibly be maleficent code or contain viruses.

A large number of smart cards from different vendors are not IOP and therefore must use specific software and smart card readers. The e-ID cards issued by an organization may not be read by all card readers even in the same MS. From EU perspective, the problem will further aggravate since there will be a greater number of smart card and card reader manufacturers. The Finnish e-ID project has tested 50 card readers from 14 vendors for the Finnish e-ID and approximately 60% of them have a major or minor issue [18].

## 3. Social and Political Issues

### 3.1. Is e-ID really Required:

From the overall situation of e-ID in EU, it appears as if few MS are still asking this question. While some MS are eager to adopt an e-ID solution for the digital age yet there are a number of MS who do not see a need for such an electronic identity and at the moment do not have any plan to introduce it. Currently Finland, Belgium, Italy, Austria, Estonia, Spain and Sweden are already issuing e-ID cards at big or small level. Three other countries Netherlands, France and Slovenia have already made decision to introduce such an electronic card. Malta has also introduced the e-ID although not in the form of smart cards.

The other 14 countries of the Union do not have any plans for a national roll out of an electronic identity card. Whether the roots of such delay, towards a digital identity, lies in the public hostility towards such an e-ID card, the high cost of PKI setup, or because of the underestimations of its potential usefulness by the government, this will cause a big obstacle towards a Pan European interoperable electronic identification system.

### 3.2. Legal Aspect of E-Sig law:

Most of the MS have implemented the e-sig Directive in their law. However, care must be observed while making laws. As found in report [16] the biggest danger to the IOP of electronic authentication schemes is overly specific legislation or regulation. Schemes that mandate particular approaches to the exclusion of all others, be they technical, legal or procedural, will not be able to accept authenticators from schemes that do not adopt the same approach. This will disadvantage schemes that adopt the mandatory approach in terms of electronic commerce. Thus, overly legislative environment may establish barriers to Pan European wide IOP.

Furthermore, although a legal framework on the European level for the electronic signatures is well in place, there is also the need for a European legal system for cross-border recognition of electronic identities in addition to the e-sig Directive.

Another observation made in report [5] with respect to certification authorities is that some MS have established supervision schemes that are very close to prior authorization, and are possibly infringing provisions of the e-sig Directive. There are important divergences between the various supervision schemes in the MS. Although the effect of these divergences remains limited, since most of the CSPs still operate exclusively in their home country, the divergences will begin to show a negative impact once European or non-European providers start to launch more cross-border certification services across the EU.

### 3.3. Privacy:

It is important to address the privacy concerns of citizens for the e-ID to be popular across European Union. The sensitivity to the issue of privacy varies among the citizens of different MS and unless a majority of population in every MS is convinced, the chances of an e-ID to be popular across EU are limited. While issuing an e-ID card it will be necessary to collect, store and process personal data on various steps. This data on card whether processed on card or outside card will lead to processing of personal data by automatic means. Confidentiality of the personal data while processed is a must. Using a smart card for the data processing with its many technical options and in geographically dispersed locations is a challenge. Although EU has an advanced regulatory framework for protecting personal data and has passed several Directives [19] to safeguard against any misuse, however citizens from different MS may not get the same level of data protection pursuant to the e-sig Directive.

The civil liberty unions are concerned about this issue of ‘Big Brother is Watching’. There are fears that citizen’s privacy may be violated by linking different databases using the UIN. The issues of identity and anonymity are even more important for them as the dangers are not only of a monetary nature but personal freedom, civil and democratic rights may be at stake. To date consumer requirements have only marginally been taken into account although the risks for consumers using a complex technology such as electronic signatures are far greater than the risks businesses face [17].

### 3.4. Multi Application e-ID Card:

An e-ID card can be useful in many different fields of life, such as health insurance, social security, financial transactions etc.. Every MS issuing e-ID cards has to make a decision

whether to restrict the e-ID card for identification, authentication and e-Sig or use it for other applications as well. Some MS are planning that additional data or applications may be chosen by the card holder and stored in the on-board memory of the card. However, who will bear the responsibility for the contents and security of the card if different applications are on the same card is not yet clear. Further, for a multi application card, if a citizen from one MS moves to another MS and needs to have an application installed from an organization in the second MS, will it be possible to get an application installed on the e-ID card from another MS or does the citizen have to apply for a new e-ID in the other MS? Another concern is that if such a card containing various applications is lost, the citizen will temporarily loose his privileges to use all the relevant electronic services till another e-ID is produced. Reconstructing such a multi-application e-ID will take some time since the information in the e-ID will come from several different databases.

### 3.5. Mandatory versus Optional:

Should an e-ID card be mandatory or optional for the citizens? MS have varying policy on this issue. Making it mandatory may not be possible for all MS considering the fact that in countries like UK, Austria etc. citizens are not bound to carry even paper based IDs. However, keeping it optional poses the threat that citizens may not take interest in using the e-IDs, something similar to what happened in Finland. In Finland, for the first 5 years only 5000 people obtained the e-IDs, the figure till March 2004 was 26,000 which is not a very positive indicator. Whether the e-ID is made mandatory or optional, what is important is the widespread use of this technology by the citizens.

### 3.6. Awareness

Electronic identification and authentication are still emerging disciplines. The level of awareness of these technologies and their use is patchy and in many cases fraught with misconceptions. This is particularly the case in respect of the security and reliability of the technologies and their implementation. It has been noted that there is a lack of awareness among government policy makers, business managers and individual users [16]. Government policy makers shape the framework within which electronic identification will be used. In doing so they need to be aware of the national and Pan European environment in which the technology will be used. Governments will not be able to develop user confidence unless they are successful in convincing their citizens that they have the necessary awareness of the issues and have developed appropriate responses.

It is important that businesses also recognizes the advantages of the new technologies and have the confidence to use them. Regarding end users, there is still considerable apprehension and misconception on the subject of electronic identification, authentication and e-sig. Much of this relates to the security of their personal information and transactions. Citizens are more concerned about e-ID since the consequences of misuse of e-ID are much severe compared to a credit card as the abuse of former, in some circumstances, can put one in a legally binding contract. Further, there are also concerns about the security of smart card itself. Various attacks are known for smart cards for e.g. timing attacks, differential and simple power-analysis attacks, and differential and simple electromagnetic-analysis attacks. The old smart cards were vulnerable to such attacks. If the currently deployed smart cards yield to such attacks then the level of user confidence on e-ID using smart cards will further reduce

### 3.7. Financial Investment

Rolling out e-ID cards is not only complex but also bears significant financial burden on State and up to some extent on the citizens. This is also one reason why some MS do not want to

start this kind of project and would rather prefer the security provided by PIN or Password. The electronic identification system using smart cards involve smart cards itself which consists of the plastic body and a microprocessor, the physical security features related to the card, card readers, relevant documentation, developing specific applications, distribution system, a registration authority, PKI, Cross-certification, Time stamping, and Client-side software interacting in a consistent, trustworthy manner. Establishing this infrastructure needs substantial investment. Although such an investment is worthwhile, as is the belief of many, yet it will be a long way to convince every MS to believe the same. Thus till the time that all EU member states are convinced to spend in establishing the infrastructure, an IOP Pan European e-ID is difficult to achieve.

**Conclusion:**

Numerous projects on electronic identification are in progress in several member states. With the rollout of hundreds of thousands of e-ID cards in MS, the issue of interoperability is getting broader attention. In this paper we have examined the obstacles that a Pan European solution would have to overcome. The interoperability of e-ID seems to be a technical issue considering unique identification, certification authority, electronic signatures, hardware and software issues just to name a few. However, several important social and political issues like privacy, legal aspects, financial investment, public awareness etc. will need an equal attention. We have discussed the technical and social/political issues in detail and have highlighted the important questions. This paper paves the way towards a Pan European interoperable identity management solution by pin pointing the core issues that will have to be addressed.

**References**


[1] EUCLID. Electronic identity white paper. Smart Cards / Trailblazer1 :Public Identity, V 1.0.
[2] EU Signature Directive 1999: Directive 1999/93/EC. Official Journal L13/12, 1999.
[3] Europa News. Belgium close to solving electronic ID cards distribution deadlock, Sep 2004.
[4] EU aims at pan-European electronic public identity. Finnish news agency STT, 4 2002.
[5] Jos Dumortier et. al. The legal and market aspects of electronic signatures. Study for the European Commission - DG Information Society: Service Contract Nr. C 28.400.
[6] A. Hayat, R. Posch, T. Rössler, 'Giving an Interoperable Solution for Incorporating Foreign e-IDs in Austrian E-Government.', IDABC Conference 2005
[7] EC Enterprise DG. A bridge CA for Europe's public administrations. Feasibility Study, 07/02.
[8] Int. Porvoo Group. Pan-European e-ID becoming a reality. Press Release 23/06/04.
[9] Trailblazer 2 on Identification. Identification and authentication in e-government, Nov. 2002.
[10]ETSI. Policy requirements for CAs issuing qualified certificates. ETSI TS 101 456.
[11]A. Mitrakas. Citizen centric ID management-chip tricks. Network Security V. 2000, 07/02.
[12]Dr. Jean-Michel Eymeri. The electronic identification of citizens and organisations in the European union: State of affairs. Doc. number B 2001 DG.3.1, 2001 Nov.
[13]MS Corp. Electronic identity solution ensures public trust in e-government. CS, 12/03.
[14]Baltimore Technologies. The Italian electronic identity card. Case Study, 2003.
[15]AS Sertifitseerimiskeskus. The Estonian certification authority website. Retrieved 11/04.
[16]E-security Task Group-APEC. Electronic authentication issues relating to its selection and use. APEC#202-TC-01.2, 2002.
[17]J. Kaufman. Couriers without luggage: Negotiable instruments and digital signatures. 1998
[18]Population Register Centre Finland. Finnish e-ID website, Retrieved Oct 2004.
[19]Directive 94/46/EC on protection of individuals with regards to the processing of personal data and 01/497/EC on the free movement of such data.