Proposed Framework for an Interoperable Electronic Identity Management System

Amir Hayat[1], Thomas Rössler[1]

Several Member States in the European Union (EU)have rolled out electronic identity (eID) tokens for their citizens. The main objective of these eID tokens is to equip citizens with a tool for Identification, Authentication and electronic Signatures (IAS) for online transactions. Member States have invested heavily in building the infrastructure and the e-government services supporting eID tokens are on the rise. At the same time, the electronic identity management systems of Member States are acting as silos, lacking the desired interoperability aspect. The eID tokens are useful only within the jurisdiction of issuing Member State and the concept of pan European eID does not exist. In this paper we have identified the core issues hindering the way to an interoperable system and discussed a framework that can solve the eID interoperability issues. Our framework is based on federated identity management concept relying on open standards. Our proposed solution solves the interoperability issue while addressing the relevant security and privacy concerns.

1 Introduction

The electronic identity tokens are being issued by several Member States in the European Union (EU) to provide secure means of identification and authentication in e-Government transactions. In the internet world the phenomenon of phising and identity theft is all too common and because of growing number of incidents, the trust in the online transactions is declining [1]. The issuance of electronic identity tokens is an effective way to protect both citizens and governments on the internet . Mostly Member States have issued these eID tokens as smartcards using the Public Key Infrastructure (PKI) while few of them are also using mobile phones. The number of issued eID tokens are already in millions. Finland was the first country to issue an eID token. Since then Austria, Belgium, Italy, Estonia and Sweden have followed the suit. In Finland, Belgium, Italy and Estonia, the state is issuing these eID tokens. In Sweden, banks issue the eID tokens which are used for both internet banking and e-government services. In Austria, both state and private organizations are issuing the eID tokens. In addition to these Member States, Germany has announced to rollout the eID tokens by 2008 [2], where as Spain and France are also in the planning phase.

All these countries have developed their national identity management systems to incorporate eID tokens for the e-government processes. Member States have developed their systems with

[1]Institute of Applied Information Processing and Communication, Graz University of Technology. Inffeldgasse 16a, 8010, Graz, Austria,{amir.hayat, thomas.roessler}@iaik.tugraz.at

different goals and objectives, and with varying levels of expectations. Some Member States have chosen to use eID token only for identification e.g. Italian CIE card (Carta d'Identità Elettronica) [3] while others are using it as a multi application token e.g. Estonian eID card [4]. Further, the sensitivities with regards to privacy issues related to eID tokens are also not the same across EU, thus some solutions incorporate higher level of privacy protection than others. In addition to these factors, the interoperability of these national solutions was not conceived in the design phase. The national systems have been developed in silos and optimised considering domestic requirements; not surprisingly we have several good solutions, yet alien to each other. The eID tokens issued by one Member State are not functional in another Member State.

The EU is giving considerable attention to electronic identity and related interoperability issues. In the i2010 initiative [5], which has preceded the eEurope 2005 action plan, it is stated that '*Member States will, over the period 2006-2010, work towards the mutual recognition of national electronic identities by testing, piloting and implementing suitable technologies and methods..*'. A similar policy statement was issued in the meeting of ministers of the G5 countries stating that the eID tokens issued by these countries would be compatible and interoperable [6]. These and similar other initiatives indicate the strong need for an effective and interoperable eID management system across EU.

Several projects have been funded by EU for the concrete implementation of a pan European eID concept. The eEurope Smart Card (eESC) Charter was launched in Dec. 1999 to address issues of interoperability and security with regard to the deployment of smart cards across Europe [7]. The project delivered the technical specifications in 2003 to European Committee for Standardisation [8] and the standard for European Citizen Card (ECC) is expected to come out in the third quarter of 2006. However, while long term interoperability may be better achieved through standardization efforts, the fact is that half a dozen Member States have already rolled out their solutions. Further, the EC treaty [9] keeps the Identity cards outside the scope of EU, thus despite having a standard for eID tokens, it may not be possible to make it mandatory for the Member States. Another organization working for creating a European Identity Management Architecture for eGovernment is GUIDE (Government User IDentity for Europe) [10]. Guide is currently running a trial of their proposed system which essentially is a middle tier between the national identity management systems of the Member States. Guide has, however, left unresolved the issue of how eID tokens are used for Identification and Authentication, which is an important part of an interoperable system [11]. Another important project under the Modinis program is the Modinis Identity Management Initiative which is supposed to submit its recommendations about an interoperable framework by early 2007[12]. An informal working group, InteropEID, composed of members from several Member States is also working on to provide a software solution addressing eID interoperability issues [13]. FIDIS (future of identity in the information society) is another important project to develop a deeper understanding of how identities and identity management shall be handled in the future European information society [14]. These organisations are the key players in the field of identity management across EU and are paving the way towards a future interoperable solution.

2 Overview of Existing System:

Currently seven Member States are issuing eID tokens. Every Member State who has issued eID tokens has also developed the client and server side components. The client or more precisely the middleware, comprising of multiple interacting software components, serves two purposes. Firstly, it provides a graphical user interface for user to perform tasks like reading data stored on the token, electronically signing a document etc. Secondly this middleware acts as a bridge

between the eID token and the server side component and facilitates in remote identification and authentication. Without having a functional middleware on the host machine, the server side component alone cannot achieve the objective of IAS.

Consider a simple scenario to elaborate some of the main interoperability issues. A Citizen A of Member State X accesses an online public service offered by another Member State Y. The citizen uses its eID token for Identification and Authentication. We have used the term foreign service provider for the foreign e-Government service. An ideal situation would be one, where irrespective of geographical boundaries, a citizen can deal with any public administration across EU using its eID token. The real life situation is, however, quite in contrast to this depicted ideal situation. Although not all transactions require Identification and Authentication of the user, we assume that for this particular e-government transaction, the citizen has to be Identified and Authenticated.

- The identification takes place through credentials like name, date of birth, a unique identifier etc. stored in the chip of eID token.
- authentication takes place when the user authenticates itself to the eID token, by entering a personal identification number (PIN) or using biometrics, and the microprocessor then performs a signature on behalf of the user.

In the real life situation where the web service attempts to communicate with the foreign eID token, the communication fails since there is no common interface through which communication between the two components can take place. In short, no 'universal' middleware exists that can bridge this divide between national e-government applications and foreign eID tokens. The eID tokens have a domestic application installed on them, have a certain file layout and they communicate through certain APDUs (Application Protocol Data Units). While ISO 7816 standards govern certain characteristics of smartcards, the file format and how these are retrieved is still issuer dependent. Therefore the web service does not know how to communicate with this foreign eID tokens and to place request for the desired data in the absence of having a middleware which understands the eID token. Figure 1 depicts, at an abstract level, how different components of an electronic identity management system work together.

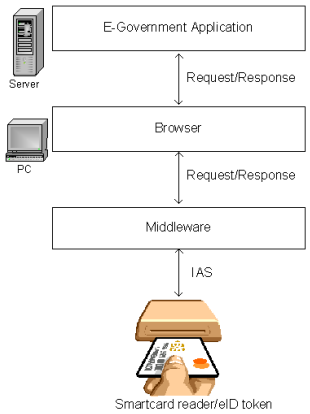

Figure 1: Communication between e-government application and eID token at an abstract level

For identification, the web service needs to extract the unique identifier of the user or a possible combination of user attributes that can uniquely identify her. The user's attributes can be stored in several files and in different formats. Austria, for example, stores a derived form of this unique identifier in an XML file, separate from the electronic certificate. Italy, Belgium and Estonia

store this unique identifier on the electronic certificate itself. Whether the unique identifier is stored on the certificate or in a separate file, it may still be difficult to retrieve it in the absence of having a middleware that understand the eID token. Even when the unique identifier is stored on electronic certificate, it may not be known as to which attribute refers to it which makes it's retrieval difficult. Another issue is the validation of a foreign Certification Authority (CA) across EU [15]. A public administration may not accept a certificate when the CA is not known and its authenticity cannot be checked. These are some of the main hurdles that any identity management system has to come across for providing interoperability. Our proposed framework mainly deals with technical issues, however, where required, we have highlighted the organizational, social and legal issues as well.

3 Proposed Framework

An interoperable solution would gather public acceptance only if it meets some basic requirements. The solution should be able to provide improved security without compromising on citizen's privacy. The electronic identity management systems pose a possible threat of 'Big Brother' attitude from public and private sector and unless legal and technical means are adopted to address this issue, citizens would remain suspicious of eID tokens. Secondly, the solution has to be such that it is 'mutually inclusive' of the existing independent solutions and deployments rather than trying to replace them. Member States have already invested heavily in building their infrastructures for eID management, it would be impractical to ask them for replacing it with another solution. Further, some Member States are already using multiple level authentication services which has to be taken into account. Last but not the least, any proposed solution should be user centric and the user should be in control of revealing its information to a particular organization for a particular transaction.

The issue of interoperability in electronic identity domain cannot be handled through a purely technical approach. It involves organizational, legal and social issues that have to be addressed equally. An interoperable solution would need coordination between different national organizations, has to meet different Member State's legal requirements, has to attend to the privacy concerns of citizens across EU, and has to accommodate different technical implementations already in place. Looking at the afore mentioned challenges, the best available choice is to have a federated identity management system between Member States. Federated identity system means where organizations in different Member States agree on a set of identifiers and/or attributes to use to refer to any user [16] despite using their national solutions. This federated system should be capable of incorporating existing national identity management systems and deployments as part of the solution. This solution on one hand would keep the control with respective Member States and would not disturb their existing identity management solutions. On the other hand, it would provide an interoperable solution that gives the desired level of security and privacy.

We have proposed that in electronic transactions the responsibility of Identification and Authentication should be borne by the eID issuer rather than a foreign e-Government service. By making this shift in responsibilities, we can eliminate most of the complexities identified earlier. The relying Member State shall believe in the assertion provided by the eID issuing Member State. The trust in such an assertion is comparable to the implicit trust in passports, driving licenses, National Identity Cards etc. issued by any Member State and accepted throughout EU. Building such a trust relationship would need bilateral agreements at Member States level to build the inter-institutional trust.

Consider a scenario similar to the one mentioned earlier. A citizen A of Member State X requests

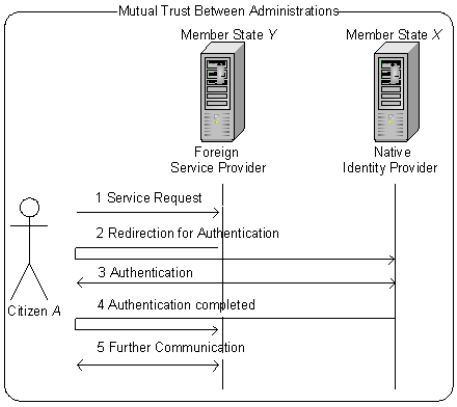

Figure 2: Citizen authentication at foreign service provider through the native identity provider

for a service in the Member State *Y*. The citizen *A* accesses the foreign web service. The web service needs to authenticate the citizen before the request is entertained. Here we introduce another entity called the identity provider. An identity provider is an organization in the home Member State of the citizen which has the means to Authenticate the citizen (ref. section 3.1). Since the foreign public administration is incapable of authenticating the foreign citizen (ref. section 2), it therefore redirects the request to the requester's native identity provider. The citizen authenticates herself at the native identity provider service using the eID token and the corresponding middleware required for the communication between identity provider and the eID token. The native identity provider is the suitable entity for authentication as it has necessary means to communicate with the middleware which understands the directory structure, file formats, number and location of files, can extract the required information and execute the requested operations. Further, the identity provider can validate the native Certification Authority (CA) and can check the certificate status with ease. The identity provider thus authenticates the user and sends the SAML assertion [16] to the requesting foreign web service. The assertion is signed by the identity provider and it holds some unique identifier of the citizen (ref. section 3.2). After the assertion is transmitted to the foreign service provider, the citizen is considered to be authenticated at the foreign web service. Based on this authentication assertion, the foreign web service can further conduct the transaction.

3.1 Role of Identity Provider

In our framework, the native identity provider is responsible for identification and authentication instead of foreign public administration. We suggest that in order to build trust on this entity, it should be kept in the public sector. The assertion provided by the identity provider can be compared to the assertion provided by Governments on citizen's passports or similar documents. Passports, driving licenses, national identity cards etc. are all acceptable throughout EU largely because they are issued by the Governments and not by the private sector.

In some Member States one good candidate for being an identity provider is the Population Register Center which maintains information for all citizens. Member States, which do not have a central Population Register, can use the services of a similar organization. What is important is, that the identity provider should have access to high quality data in a manner where chances of error are minimal. The role of identity provider is central for all communication taking place between the public administrations. Before such a system can be functional, it is vital that identity providers and foreign public administrations make mutual agreements to build trust and agree on the mode of communication.

3.2 Privacy

One important privacy concern with respect to eID tokens is the usage and storage of a unique identifier. Various civil liberty groups are critical of the issuance, usage and storage of a unique identifier, which can be abused by public and private sectors. It is important for Governments to uniquely identify the person conducting a transaction, however, the risk that these Unique Identifiers can be abused for citizen profiling through linking various databases is certainly present. Specially if the eID token has to be used in cross border transactions, it is all the more important to adopt measures that eliminate the possibility of such profiling. Austrian approach to protect user's privacy using unique identifier is a best practice case [17] [18]. In our proposed framework we have expanded on Austrian approach to address privacy concerns at a pan European level. We consider each public sector - across all the Member States - as one specific sector, and the unique identifier is used and stored in each sector in a fashion that no cross-linking is possible. We use a three steps processing of Unique Identifiers as shown in figure 3.

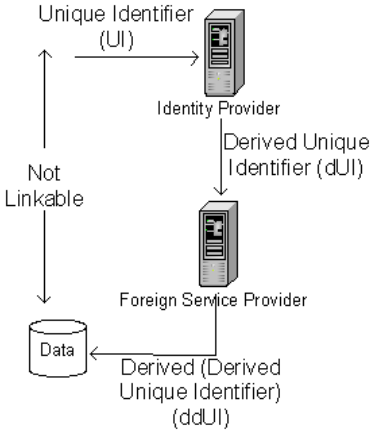

Figure 3: Depicting the process to eliminate cross linking using unique identifier

The state issued unique identifier is stored in the eID token. This unique identifier can either be stored as is e.g. Belgian, Estonian etc. or a cryptographically derived value is stored on the eID token e.g. Austria. To avoid possibility of citizen profiling between cross border organizations, the identity provider does not send the actual unique identifier to the foreign service provider. Rather, a derived value, using one-way hash function, is sent.

dUI= Hash Function (Unique Identifier, Country Identifier)

However, it is important that irrespective of which identity provider generates this derived unique identifier (dUI), the value should remain the same for a particular service provider. It is also suggested that service providers in a Member State may not store this dUI per se in their systems, as there still would be the possibility of linking different databases. Therefore each foreign administration (or service provider) should store a further derivative of this dUI, using a one-way hash function on dUI and the sector identifier of each public administration as double derived unique identifier (ddUI).

ddUI = Hash Function (Derived Unique Identifier (dUI), Sector Identifier)

Using the above mentioned method, it would not be possible to derive the unique identifier from the dUI or ddUI or link ddUI across different public sectors for the same user. For protecting citizen's privacy, in addition to such technical measures, legal means should also be adapted.

In Belgium for example, it is illegal for any person or private organization to store the unique identifier of a citizen.

Furthermore, to protect user's privacy, it is important to have several identity providers e.g. national population register, national tax authority, social security etc. To keep a citizen centered approach, the citizen should have the right to select a particular identity provider for her authentication.

3.3 Electronic Identity Token in Alien Environment:

The discussion so far has focused on remote access of the foreign e-government service by a citizen. In remote access, it is easy to assume that theuser has the middleware component needed for the interaction with her native identity provider. Another situation could be, which is rather complex, that the citizen uses its eID token at a physical site in a foreign Member State where it has no control on software/hardware environment. In this situation user has to rely on the host environment for her Identification and Authentication and the required middleware for communication with the native identity provider may not be available. For our proposed framework to work, a middleware on the host machine that can bridge between identity provider service and eID token is required. If the application cannot recognize the foreign eID token then the eID token would merely act as an ordinary plastic identification card since the chip would be dysfunctional. Examining the current diverse situation across EU, there are three main possibilities to solve this issue of communication between foreign application and the eID token. We assume that the eID card's origin is determined either through ATR (Answer To Reset) or by using a suitable manual method.

The first option is that all the different middlewares (client side applications) from various Member States are put together as one module and installed on the host machine. Once the application recognizes the origin of eID token, it invokes the corresponding middleware developed for this particular eID token. The middleware is then functional and may help in Identifying and Authenticating the user at the Identity Provider's end as explained in our proposed architecture. The second option is that the support for all the foreign eID tokens can be built in the domestic middleware of every Member State. Austria has demonstrated this approach and one of the main implementations of the Austrian security layer concept [19], the TrustDesk client [20], does provide a limited support for Estonian, Finnish, Italian (CNS card) and Belgian eID tokens [17]. The third solution is having one universal middleware that can communicate with all the eID tokens. Currently there is no standard that defines such a pan European middleware interface. However, in the open source software, a good example is that of OpenSC [21], which is already being used by Belgium and supports the eID tokens of Finland and Estonia. There are pros and cons associated with each of these three options, however, due to space restrictions we do not discuss them any further.

From this discussion we can observe that the issue of supporting eID token in an alien environment is a complex task. We have different options, yet no straight forward solution to this issue. While use of eID tokens to access foreign web services is achievable using the proposed framework, the task of using eID tokens in alien environment may take longer.

4 Conclusion:

Governments across Europe are issuing electronic identity (eID) tokens to their citizens and consider them to be the future communication tools between citizens and public sector. The corresponding identity management systems, however, are not interoperable and this issue is

hindering the way of micro and macro benefits of having a pan European interoperable eID. In this paper we have highlighted the main issues hindering the way towards an interoperable solution and have proposed a framework that can achieve the desired goal. Our proposed federated identity managements system is based on collaboration between the existing national systems using open standards. The framework suggests concrete steps to protect citizen's privacy while providing better security.

Acknowledgements

The work has been partially funded by the Higher Education Commission (HEC), Pakistan.

References

[1] Gartner. Gartner survey on consumer trust in online commerce, 06/2005.

[2] Andreas Reisen. Travel and ID Documents of a new Kind: The German ePass. NetID06.

[3] Carta d'identità Elettronica. http://www.anci.it/cie/index.html.

[4] Estonian Electronic ID Card. http://www.id.ee.

[5] i2010 Initiative. Ministerial declaration Manchester UK, 11/2005.

[6] Meeting of the Ministers of the Interiors of G5. Operational Conclusions. Evian, 7/2005.

[7] IDABC Quarterly Issue 3. Towards interoperable eid:, 07/2005.

[8] European Committee for Standardization. CEN TC224 WG15. http://www.cenorm.be.

[9] Treaty of Nice 10/03/2001. Article 18.3. http://www.cenorm.be.

[10] GUIDE. http://istrg.som.surrey.ac.uk/projects/guide/.

[11] GUIDE. Identity interoperability services report:core services descriptions v2.0, Oct 2005.

[12] eEurope 2005 Modinis Program. Modinis-IDM. Common Terminological Framework for Interoperable Electronic Identity Management.

[13] Working group on interoperability of eid cards world-wide. http://www.comune.grosseto.it/interopEID/.

[14] FIDIS. http://www.fidis.net/.

[15] Christian Rechberger Amir Hayat. Interoperable Certification Authorities In The European Union: A Practical Solution. Fourth Internationl eGovernment Conference, Denmark, 2005.

[16] SAML Glossary. http://www.oasis-open.org/.

[17] R. Posch A. Hayat, T. Rössler. Giving an Interoperable Solution for Incorporating Foreign e-IDs in Austrian E-Government . IDABC Conference Feb 2005.

[18] Data Protection Agency of the community of Madrid (DPACM). 2nd european seminar on data protection best practices in european public services. Madrid, Dec 2005.

[19] H. Leitold, A. Hollosi, R. Posch. Security Architecture of the Austrian Citizen Card Concept. Security Applications Conference, Dec 2002.

[20] IT Solution. Trustdesk application. http://www.itsolution.at//.

[21] OpenSC. http://www.opensc-project.org.