Setting Processes for Electronic Signature

Dr. Joachim Schiff
On behalf of the SPES Consortium Workgroup
City of Saarbruecken IKS
Nell-Breuning-Allee 1
D-66115 Saarbruecken
Germany
Tel. 0049 681 905 5000
Fax 0049 681 905 5191
Joachim.schiff@saarbruecken.de

Abstract :

Digital signature PKI security solutions, based on smart cards, are emerging as a key component in providing advanced citizen services on the Internet and in public terminals. However this new technology is not without complications and one of the most pressing challenges is ensuring that citizens in one country, using a digital signature solution from one Certification Authority, can access services in another country using a digital signature solution from another Certification Authority. Needless to say this challenge covers a wide range of technical, legal and organizational aspects. This presentation will focus on the aspect of interoperability and how this challenge has been solved in the SPES project.

1. Introduction

In recent years many countries have adopted a regulatory framework with the aim of introducing the use of digital signature technologies into document exchange and at the same time a large number of local, national and international smart card schemes have been launched.

Thanks to this process for introducing the digital signature, and other practical applications using the same base technology, smart cards have become more commonplace for citizens and digital signature PKI security solutions based on smart cards are thus emerging as a key component in providing advanced citizen services on the Internet and in public terminals. Digital signatures allow citizens to sign e-mails and electronic forms, and provide strong authentication for secure access to sensitive personal information. They are a perfect “access token” to enable personalized use of public terminals for those without PCs. However, with this success the problem of interoperability between local solutions becomes more and more important.

The challenges of interoperability between smart card schemes includes a wide range of aspects, but this paper will focus on the challenge of ensuring interoperability between the digital certificates stored on smart cards. This means that the interoperability solutions presented in this paper, whilst primarily aimed at smart card schemes, are not limited to

such schemes, but also address interoperability between digital signatures in general. To simplify, the question is: "How do we make sure that citizens in one country using a PKI solution from one Certification Authority (CA) can access services in another country using a PKI solution from another CA?"

1.1 – The technical challenges to PKI interoperability

Although the European Commission has adopted a specific Directive [1] to harmonize the national regulations in this field, many technical differences still remain in the various implementations of the supporting tools for digital signature and/or strong authentication.

Many international projects have been launched in recent years with the aim of clearly identifying and providing a definitive solution to this difficult problem of interoperability. But, due to the great variety in implementations, it will take a long time before a unique "standard" solution will be adopted in this market sector. Nevertheless every on-line service developing team has to find a technical solution in order to start using these emerging security technologies in their web sites.

1.2 – The SPES response to the PKI interoperability challenge

The eTEN supported SPES project www.spesproject.org (Setting the Processes for Electronic Signature in European Cities) was launched late 2002 and will be running until the end of 2004. With partner cites of Bologna and Prato (Italy), Naestved (Denmark) Saarbrücken (Germany) and Sheffield (UK), one of the aims of the project was to explore ways of achieving technical interoperability between PKI solutions in different countries.

As we have already discussed no "standard" solution exists to this challenge and the SPES partners came up with the pragmatic solution presented in this paper. The solution consists of a number of tools, which we will describe in the sections below. Special emphasis however will be put on the development of a scalable open source software module, which enables the acceptance of digital signatures from all partners.

2. Objectives

The overall objective of this paper is to show how to practically integrate the usage of digital certificates (mainly, but not exclusively, stored in smart cards) into interactive on-line services, where the exchange and the management of signed electronic documents is necessary, and/or the strong identification of the service users is mandatory.

The emphasis of the proposed practical solution is on flexibility and it can, in principle, be integrated into any modern web service development environment and is developed in order to be suitable for many of the application server environments in most common use.

The final objective of the proposed technical approach is to allow the introduction of an on-line service with the ability to accept digital certificates issued by different European CAs and to uniquely associate the provided digital certificate with the real physical identity of the service user.

3. Methodology

To understand the methodology for arriving at the solution presented in this paper it is necessary to understand that conditions for the development team in SPES differ significantly from those of normal development projects. SPES is a deployment project and not a development project and as such, a solution to the interoperability problem was not the only goal of the project. Market research has been carried out, but it has been aimed at

the overall sustainability of the solutions in the individual partner cities and thus covering more ground than just the interoperability side of the project.

That said, it must be stressed that all partners in the project have extensive knowledge of smart card and digital signature schemes and from the beginning of the project it was the common belief that the interoperability question is of great and growing importance, which we will return to when covering the "Business benefits".

The interoperability solution was arrived at as a result of a number of technical meetings between the partners in SPES and the selected certificate issuers (CAs) in the partner cities. It quickly became evident that the models for interoperability described in market sector publications would be far too complex to be implemented within a realistic timescale.

The solution to the challenge became the set of tools described in the following sections. Actual development was undertaken by the City of Prato in close cooperation with the certificate issuers in the partner cities.

4. Technology Description

SPES is fully based on current open standards, in line with EESSI (European Electronic Signature Standardisation Initiative):

- Communication relies on *TCP/IP* networks and *Internet* technologies;
- Encryption exploits *public key cryptography* (*RSA* and *DES* algorithms);
- Data authenticity and privacy is achieved by means of *PKCS#11* compliant devices;
- Certificates are compliant with the X.509 standard;
- Certification is managed by means of *Certification Authority Hierarchies* and *LDAP* services;
- Information is delivered as a multimedia resource in *HTML and XML*
- Necessary software is platform independent and distributed as *Java applets*.

The X.509 standard has been largely adopted in SPES.

As other standards largely adopted in SPES we can mention:

- HTML - HTTP / HTTS for server – client browser interaction
- XML / SOAP for information transport among the different parts of the implemented systems
- PC/SC standard interface for interaction between user platforms and smart cards.
- ISO7816 -1(2/3/4/5/6/), ISO 7811 1-3, ISO 7811 4-6 for smart card physical characteristics .
- PKCS#7 for digital signature envelope.

5. Developments

To understand the importance of the developments in the SPES project it is first necessary to understand that PKI interoperability is associated with many problems – so many in fact that it is only possible to scratch the surface in this paper. Unfortunately the EU regulations that are currently in force do not always solve these problems as is clearly reported by a recent study promoted by the European Commission [2]. If we are to arrive at a "here and now" solution to the PKI interoperability problem these challenges must be dealt with in a pragmatic and practical manner. The challenges are of a technical, procedural and legal nature.

5.1 The problem of the digital signature in e-services implementation

In many e-service implementations the problem of the authentication of users has to be linked with the handling of digital signatures (the digital signature is another application of the PKI technology), and in all digital signature solutions, the interoperability problems represent a key area to be addressed. This is true for the following reasons:

a) The existence of different hardware devices suitable for cryptographic operations.
b) Differences in national regulations.
c) The insufficient standardisation of the file formats adopted to contain digitally signed electronic documents.

5.2 Interoperability problems

Below are listed some main critical points, which must be addressed in order to solve the interoperability problems in digital signature applications:

a) Interoperability between the different cryptographic devices, at one side, and software packages for digital signature creation, at the other side.
b) The file formats used to store a digitally signed file often come from specific proprietary standards defined by the software providers, that are not disclosed to other subjects.
c) Different options adopted by a software kit producer in the creation/manipulation of X.509 certificates are not always fully documented. One of the more crucial elements of a digital certificate is the Distinguished Name component that must used to uniquely identify the person to which the certificate belongs.
d) Differences in the digital certificate management policies that lead to difficulties in accepting them in other contexts.

As far as the strong authentication scenario is concerned, some problems to be faced in order to achieve complete interoperability among PKI modules coming from different vendors, are very similar to that focused upon within the digital signature scenario. However this problem would appear to be easier to solve than that in the digital signature context due to the following opportunities:

a) The existence of the common standard (HTTPS) provides a uniform way to establish a link between the user client (PC or workstation) and the servers hosting the target e-services. This is true no matter what the hosting environment is and what the client browser is.
b) The wide availability of software module/library suitable for the e-service developers to interact with the HTTPS parameters and functionalities in all the market platforms.

However, the different options adopted by a software kit producer in the creation/manipulation of X.509 certificate exchanged also in HTTPS connections, are again one of the more critical issues to be addressed in strong authentication interoperability.

There are many active projects with the aim of analysing and solving the technical problems related to the interoperability issues in the field of PKI. The theoretical results of these projects will be practically suitable only when the PKI market adopts the proposed standards. In the meantime all interoperability schemes must adopt other ways of dealing

with the challenge. The approach of SPES in the adoption of a number of tools, can be summarised as follows:

a) Ignoring the issue of interoperability between the client software, for digital signature creation, and cryptographic devices on the user platform.
b) Avoiding the management of digital signature creation via web based applications.
c) The development of an "interoperable" software module for digital signature verification (returning later to the important definition of "interoperable" in this context).
d) A centralisation of strong authentication in a dedicated portal.
e) Adoption of a general framework for the acceptance of digital certificates coming from different CAs. (Memorandum of Agreement)

The decision to ignore interoperability among different cryptographic devices on the user platform - point a) above – is justified by the fact that the e-services are mainly accessed by users using their own computer which is already equipped for the use of a specific cryptographic device and its related software. With this approach the "avoided" problem remains to be faced in the "public" stations (e.g. kiosks, public internet access points) in order to allow occasional users to utilise these devices with their personal cryptographic instruments. At the moment this problem can only be solved by installing on the public platforms as large a number as possible of commercial software products for PKI support.

The centralisation of the authentication function facilitates the setting up of a specialised application server environment equipped with all software modules and correctly configured to accept as large a number of digital certificates as possible. This reduces dramatically the efforts needed to manage a large number of different server hosting platforms.

The adoption of a general framework for the acceptance of digital certificates coming from different CAs consists of the following actions:

a) To perform an analysis of all the potentially acceptable CAs policies of digital certificate management in order to decide if the level of security can be considered appropriate for the specific e-service utilisation.
b) To make available, in the easiest possible way, all the necessary software modules for managing the digital signature lifecycle with all the instructions for installing and maintaining these modules.
c) To develop a general procedure, which will allow for the unique definition of the identity of an e-service user, based on the presented digital certificate.

In SPES this framework will be developed by means of the following actions:

a) Utilization of the project web site to maintain the list of "recognised" CAs based on specific analysis performed by the project team on the CA management policies.
b) Maintenance, again on the SPES web site, of all the proprietary software modules released by the "selected" and "accepted" CAs.
c) Signature of a Memorandum of Agreement between the SPES project team and all the selected CAs in order to allow the information exchange necessary to maintain the level of trust in the CAs certificates and to continue to accept them in SPES implemented e-services.
d) Development of an Identity Management module to be integrated both in the strong authentication portal and in the implemented e-services.

As far as strong authentication is concerned, the availability of modules supporting the usage of smart cards inside the most common browser software is largely ensured by the market.

It is evident that while the focus in this paper is the development of the interoperable software module it must be emphasised that this is only one part of the combined SPES solution to deal with the interoperability challenge. It is however one of the most innovative parts of the SPES project and merits special attention.

5.3 The" interoperability" module

The "interoperable" module for digital signature verification has been developed by the City of Prato and produced as a PC SW module that will be distributed via the SPES web server to all the end users (citizens and/or civil servants). While this solution may seem cumbersome the reality is that only relatively few workstations will have to install the software – mostly civil servants.

The module will be maintained and updated from time to time by adding the capability to recognize new certificate issuers (CA's) accepted by the SPES team.
The module operations during verification of a digital signature can be described as follows:

a) After the file format has been identified (either automatically or via a dialog with the user) the signature data is extracted from the file.
b) Based on the information collected by means of the framework established within SPES and maintained in the web site, the software performs the signature verification.
c) Accessing via the network, all the revocation lists, it verifies the validity of the certificate.
d) At the end of the process a summary of the verification activity is reported to the user specifying the level of trust of the signature based on the EU Directive prescriptions.

Via the Memorandum of Agreement signed by the involved CA's, the SPES partners can have access to all the necessary information to perform the digital signature verification as described above.

6. Results

The SPES project is still running and the final results will only be known after the termination of the project at the end of 2004. The project has however already achieved some significant results - chiefly a practical approach to the PKI interoperability challenge.

The contribution of SPES to PKI interoperability is not so much any single components of the solution - although the most innovative part has been the open source scalable interoperability module - but in the total set of tools / approaches to the interoperability problem. Most of the technological components used in SPES are standard tools, which could be made to interoperate if the will and overall guidelines were in place. The real challenge to PKI interoperability is not so much technology but cooperation – cooperation between CA's who are reluctant to accept signatures from other CA's – not the least CA's from other countries.

The challenge for the SPES Consortium has been to arrive at a solution, which achieve interoperability while requiring as little as possible of the CA's. Central to the solution to this problem is the development of the interoperability module (see above), which ensures that only two things are required of the participating CA's:

- They must provide a description of the components of their X.509 certificates, which can be programmed into the interoperability module thus allowing the module to perform the verification of digital signatures from all CA's participating in SPES.
- They must sign a memorandum of agreement accepting the signatures from the other CA's.

While this is no small thing to demand from a CA it is far easier to achieve than to ask the CA to make changes to their own applications allowing the verification of signatures from other CA's. This possibility is simply not realistic at this moment in time. The SPES solution is not the definite solution to the interoperability problem but it is a practical workable solution to achieve interoperability here and now.

7. Business Benefits

The potential business benefits of the SPES solution to the interoperability challenge are considerable. The SPES project is a deployment project and the primary focus during the application and early phases of the project has naturally been to focus the market research on the viability of the solutions in the sites. Systematic market research on the market for a solution to the interoperability challenge has been outside the scope of SPES.

We have however strong indications from a number of sources that the need for input to solving or a solution to the interoperability challenge is becoming increasingly necessary. From the membership of organisations such as Tele Cities and Major Cities the partners have received many expressions of interest. This has also been the feedback from the Commission. More and more smart card schemes are being launched in many different settings and with that comes the need to address the interoperability challenges. Also, it must be stressed that the market for a pragmatic solution is not limited to international interoperability but will also be applicable for national solutions. In SPES for example, the solution is to use both internationally between countries: Germany, Italy and UK but also internally between regions (cities) Bologna and Prato. Interoperability will pave the way to successful cooperation between schemes and thus extending the scale for potential revenue generating activity at higher levels above the local.

While the SPES project is still running the plan to market the results has been drafted. It includes the continuation of the cooperation between the sites - ensuring that interoperability continues - and the invitation to other sites in other countries to join. This will be ensured by the creation of a Memorandum of Agreement which will identify the roles of the service Companies, identifying and detailing their agreement in terms of rights, responsibilities and reservations for applying cross certification and interoperability of services.

Whilst the Directive has set the framework for the acceptability of electronic signatures, the market has still to respond fully. By taking the user more into account, as SPES does with a strong focus upon e.Inclusion, and by stimulating and contributing to standardisation, the promise of "authentication" becoming the "killer application" within a multi-application smart card scheme is more likely to be realised. The product is in fact a key to releasing the potential of other products. The business case rests upon the daily needs of the common user, which have often been ignored in the past. These needs will be fulfilled in an increasingly heteregeneous and complex market, which will evolve from the stimulation of networking activity to ensure the major stakeholders in a complex process are brought together to fully realise the benefits of this "new" technology.

8. Conclusions

The SPES project is continuing and while much still needs to be done, much has been achieved. The main achievement from a European perspective is the addressing of the interoperability challenge. SPES has addressed this real challenge by focusing on a pragmatic solution:

- Ignoring the issue of interoperability between the client software, for digital signature creation, and cryptographic devices on the user platform.
- Avoiding the management of digital signature creation via web based applications
- The Development of a “interoperable” software module for digital signature verification
- A centralisation of strong authentication in a dedicated portal
- The adoption of a general framework for the acceptance of digital certificate coming from different CAs.

The solution will be tested in real life during the remainder of the project and the final results will be included in a “lessons learned” document. It will also form the basis for a decision on if and how to market the interoperability solution. However the plan to market the results has been drafted. It includes the continuation of the cooperation between the sites - ensuring that interoperability continues - and the invitation to other sites in other countries to join.

References

[1] - DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Community framework for electronic signatures.
[2] J. Dumortier, S. Kelm, H. Nilsson, G. Skouma, P.V.Eecke – “The legal and market aspects of electronic signatures” – Study for the European Commission – DG Information Society – 2004.