

eEpoch

(eEurope Smart Card Charter proof of concept and
holistic solution)

Action Research Document: How to Implement eServices with Interoperable eID

Luis Mengibar / Raul Sanchez-Reillo
GUTI – University Carlos III of Madrid

Project Funded by
European Commission
Information Society
IST-2001-37936

Version 1.0
Public
10/05/04

eEpoch
WP 1 – Action Research Responsible
Raul Sanchez-Reillo
GUTI – University Carlos III of Madrid
e-mail: rsreillo@ing.uc3m.es

Action Research Document

Document Control Sheet	
Work package 1 Chair	Theo van Sprundel (Axalto, a Schlumberger Company)
Responsible Author(s):	Luis Mengibar / Raul Sanchez-Reillo (GUTI – UC3M)
Organization:	University Carlos III of Madrid
Subject / Title of Document:	Exploitation and Dissemination plan
Related Task('s):	WP 1, WP 5
Deliverable No.	How to Implement eServices with Interoperable Eid
Save Date of File:	14/05/04
Version Number:	1.0
Ref./File Name	ImplementingServicesWitheID.doc
Number of Pages	18
Distribution Category: (P/R/I)*	P
Nature of the Deliverable (T/M/W/R/O)**	T
Target Date	26/05/04

*Type: **P**: Public, **R**: Restricted, **I**: Internal

Nature: **T: Technical, **M**: Management, **W**: working document, **R**: Review, **O**: Other

Document Distribution			
Member type	Organisation	Name	Distributed
Webpage			
Contractors / Partners	All eEpoch Participants		
European Commission			
Additional			

Change Control Sheet

Date	Issue	Affected Sections	Author / Reference Comments

Review and Approval of the Document

Organisation Responsible for Review	Affected Sections	Approval / Comments	Date

Contents

1.	Introduction	5
1.1	Context within eEpoch European Project.....	5
1.2	Structure of this Document	5
2.	Requirements for eID in eServices.....	7
2.1	User Oriented Services.....	7
2.2	Different Levels of Security.....	7
2.3	Interoperability Needs.....	8
2.4	Service Continuity	10
2.5	User Reactions	10
3.	eID Implementation Alternatives.....	12
3.1	Belonging of an ID Token	12
3.2	Based on Certificates.....	12
3.3	Aided with Biometrics	15
4.	Steps to Implement eServices with eID.....	17

1. Introduction

This document is intended as a guideline of items to be considered with trying to implant an Electronic Service (eService) with user identification, which is supposed to be done electronically (eID – electronic IDentity). Specially important is when the eServices is expected to be able to use infrastructure from other services, so interoperability is a need. The other services could come from the same service provider, from other service provider that belongs to the same environment (business sector, country, etc.), or from one not having any initial relationship. This different kind of relationships will lead to fully different situations to be considered in building an eService with interoperable eID.

Many of the issues reflected in this document could be considered as common-practice, but unfortunately some of them are systematically not considered in the implementation of new eServices. Also, most of this work would not be necessary whether the different organizations and institutions will agree in a “common-understanding” infrastructure. Except for some particular cases (such as the GSM mobile infrastructure definition), eService designer has to cover different approaches at all levels in order to achieve an interoperable product, being most of the major discussions decided at a political level, instead of a technical one.

1.1 Context within eEpoch European Project

This document is considered as a report, result of the work being carried on in the Action Research Activity in eEpoch. Action Research is a methodology based in implementing designs by a dynamical study of its viability and performance, being able to make changes as first results comes out from the design.

Action Research is considered inside eEpoch in its Work Package 1, and it is at the service of all partners in eEpoch Consortium as an aid for any potential problem that they consider it can arise. Some issues has been located, being decided to submit two documents based in two different targets. One of those documents is the one presented here. The other one is about how to understand ISO 7816 security specifications, in order to achieve a trustable eID product.

1.2 Structure of this Document

This document is structured as follows. After this initial introduction, a set of requirements to get eServices with eID will be presented. This section should centre the designer in which is the

problem, where it is really needed to get (which level of interoperability), in order to decide how to implement each situation.

Then a section will cover the different ways the ID could be performed, taking in consideration all different implementation issues that could arise. This document will end with a set of conclusions derived from the document.

2. Requirements for eID in eServices

In this section, the different requirements that a system designer could find when developing an eService with eID, will be given.

2.1 User Oriented Services

The first requirement that a system designer can find when developing an eService, is the need to provide a service personalized for a determined user. For example, giving the user accessing the service, information relevant to him (which could be of no use to other users). This is the initial situation where identifying the user is requested. Depending on the information to be provided, and the kind of user accessing the eService, this could be handle in a variety of ways. In many cases this information is not confidential, identification is only intended to attract the attention of the user to that part of the eService that he can find more useful. In other cases, the information is personal or confidential, so protection to the user privacy is requested.

2.2 Different Levels of Security

In the above section, two different situation have been presented. These two different situations have relevant conditioning to the security requirements. In the first case, only and identification is needed to provide personalized information, but without privacy connotations. In that case, eID has to provide only a link about user interests and the eServices available. It is not really important whether another user gets that same information, or if the right user gets other information sporadically. Therefore the security requirements are minimal, and ID could be handled in a great variety of ways, being more important easiness and cost than security.

On the other hand, the other case involves the situation of being, the information exchanged between the eService and the user, personal and confidential data. In this case, the identification process should be aware that having a security hole, could lead the user to some personal inconveniences and even legal problems, which could therefore be re-directed to the Service Provider. In these case, much more important than easiness and cost, is the security achieved with the identification process.

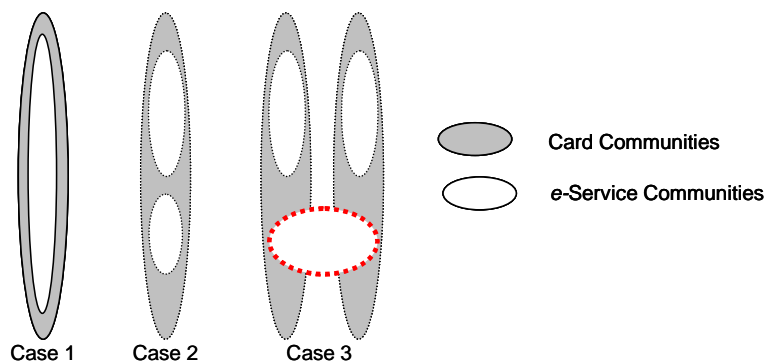
In this last case, security could be considered depending on the sensibility of the information exchanged, specially related to the time validity of such information. For example, if in a payment system all operations are consolidated 3 months after their date of issuing, then if a hacker gets that information after 4 or 5 months, is of no use for him, neither a problem for the user. If, for example, the information exchanged, is related to a serious illness of the user (for example in a

health care system), after a certain time, that information will still be valid, so any security hole could compromise the user's privacy, and extreme care should be placed.

2.3 Interoperability Needs

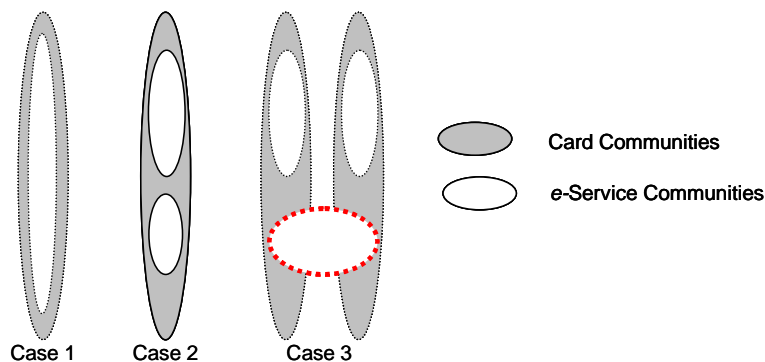
When several service providers want to share the same infrastructure or a single service provider wants to be operative with different infrastructures, then interoperability is requested to allow the usage of such services. In that sense, when considering electronic ID as the infrastructure to be used by the service providers, then different situations can be faced (as stated in "Global Interoperability Framework (GIF) for Identification, Authentication and Electronic Signature (IAS)" documents from eEurope Smart Card Charter), considering the ID as being in a smart card:

Case 1: The Basic Situation – 1 card issuer / 1 service provider



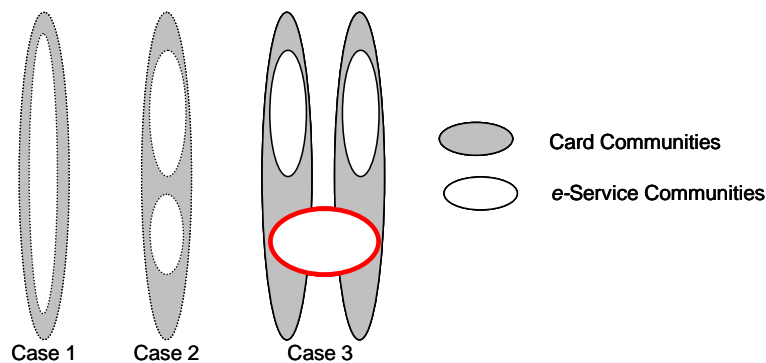
In those cases, there is a strong binding between card issuer and service provider, who generally happen to be the same legal entity. In this case, interoperability is not demanding.

Case 2: Multi-application Frameworks – 1 card issuer / N-service providers



These frameworks enable a smart card community to support multiple e-service communities but their design does not necessarily facilitate e-service communities spanning multiple smart card communities. Therefore, these frameworks do not generally make use of IAS interoperability. Instead they adopt a multi-application smart card approach, in which additional card applications are loaded on the same card, each with its own (possibly proprietary) IAS scheme instead of relying on a common one.

Case 3: Scheme Recognition – N card issuers / N service providers



This is the case where groups of service providers agree to mutually recognize each others cards independently of the card issuers involved. This can be achieved on a “one to one” basis between service providers or by the definition of a common scheme within a specific industry. This case typically enables e service communities to span several distinct card communities.

Scheme interoperability is usually achieved by multiplying the off-card applications supported by each service provider, so that they will recognize and operate with the proprietary card application corresponding to a given scheme.

When interoperability is requested, it can be achieved at different levels:

- Application Level: which provides a common interface to share services across different Service Providers
- Card Level: providing a standardized interface between the terminal and the smart card
- Platform Level: applying a standardized platform-independent interface between the terminal and the smart card
- Public Key Infrastructure (PKI) Level: enabling the deployment of cards and terminals over different certification authorities.

2.4 Service Continuity

In some situations there is the extra requirement that Interoperability is going to be implanted in a system where services are already running. Those services are requested to go on providing its use to the customers. This makes the requirement of allowing a transition time for moving from the isolated-framework, to the interoperability-framework, which, sometimes, make the service provider having two different systems running in parallel.

2.5 User Reactions

A typically forgotten requirement in an eID system, from the technical point of view, is the reaction the user can have to the new system. Far away from what it could seem, this is one of the most determining requirements that a system could have. No matter how technically good is the project, the broad the interoperability is achieved, if the user rejects the system, all previous work is useless.

Users reactions to a new eID system can vary greatly from one community to other (even without geographical or sociological relationships):

- Some users can fully reject the system because they are not used to the need of being identified.
- Also, some users can reject the system because they do not trust the service provider, the card issuer or the PKI owner.
- Other users can accept an eID system as far as it is not related to governmental or legal bodies. When they suspect than a police body could be related, they could reject the system.
- Depending on the way the system is promoted and the community targeted, users can accept the system without worrying about any kind of double meaning or double use of their identity.
- Finally some users could request an eID system with all legal background to warranty some of their daily operations.

So it can be seen the great variety of situations a system designer have to cope with. A deep study should be taken before any further investment, in order to analyze how to approach the new system to the users.

3. eID Implementation Alternatives

This section is dedicated to show the different alternatives for providing eID for different services. Different approaches will be followed, from the common belonging of an ID Token (physical or electronic), to the futuristic Biometrics-based solution.

3.1 Belonging of an ID Token

The most antique and common way to provide an ID to achieve access to a determined service is the belonging of an ID Token, such as a passport, National ID Card, magnetic stripe card, smart card, etc. Obviously, for the scope of eEpoch project, non electronic ID media is not covered, and the common need of having more than a service related to the same ID media, pushes to talk about the use of smart cards.

To provide eID, a smart card can be used at different levels, both regarding interoperability and security:

- Smart cards can be used as if a magnetic stripe card is considered, i.e. having only an ID number that will be processed by an external system to provide the access to the requested service.
- Also, smart cards can be used to authenticate the user, so the card can allow the user to access a single service included in that same card.
- Then, whether different service providers agree, it can be used to authenticate the cardholder, so with a single ID, the user can access more than one service included in the card.
- Additionally, the smart card can authenticate the card holder to allow other identification methods, such as the access to PKI data, and enabling stronger security methods.

3.2 Based on Certificates

When talking about electronic transactions, identity must be granted by a service provider located remotely. This means that the warranty about the identity of the user must be transferred to the service provider, and then he should be able to verify such identity. Years ago, the only way to

perform this kind of operations is by transferring confidential information ciphered with secret key algorithms. This kind of solutions brings some problems, especially when the need of sharing confidential information is requested by a large number of users. The emerging of Public Key Cryptography, has given a solution to this kind of problems. By building a Public Key Infrastructure, a large number of users can perform transactions with:

- **Confidentiality:** ciphering the information with the public key of the receiver, make this information opaque to the rest of the users.
- **Authentication:** ciphering the information with the private key of the emitter, let everybody check the identity of the emitter.
- **Message Integrity:** using other kind of algorithms, a hashing of the message could be generated, in the way that, if someone wants to change a single char of the message, the hashing do not correspond to the initial one. If this is performed together with authentication mechanisms, then an **electronic signature** of the document is generated.
- **Non-repudiation:** or how to reach a point of no return, from which none of the actors in the transaction can deny the commitment of such a transaction.

Using this kind of mechanisms, a new way of identifying electronically a user is developed. Creating a certificate for each user, this certificate can be used to identify the user in any transaction. This certificate must be built in a way that:

- No two users have the same certificate
- It identifies the entity that has generated the certificate
- It grants that the certificate has not been manipulated, or generated by another entity
- It gives some information about the user

Therefore, certificates can be used to sign all transactions and identifying all actors in all communications. Having installed a PKI, then many services can use its certificates and reach interoperability in the way the user is identified.

Unfortunately this interoperability is not always possible, mainly due to the lack of agreements for using the same PKI (PKIs have created a full new business, and many PKIs exist in the same environment). In such cases, when it is not possible to use a single PKI, a solution should be

provided to allow interoperability at the certificate level. In this line, several solutions can be approached:

- **Hierarchical:** where different PKIs are located under the umbrella of a higher level one, so that if a user from one PKI wants to communicate with other from another PKI, the communication will flow through the higher level one. This hierarchy can be developed in the number of levels desired.
- **Certificate Trust Lists (CTL):** where the PKI has a list of the Certification Authorities (CA) that are designated as being trustworthy for a designated purpose.
- **Cross Certification:** where two CAs establish trust by issuing certificates to each other, so two certificates are involved (forward and reverse). It has the problem of increasing greatly the number of certificates when the number of CAs increases.
- **Bridge CA:** creating artificial CAs that serves as a gateway among other CAs. This presents some challenges, such as the cross certification criteria, the validation of certificate paths, the complex signature validation, the distribution and status of certificates, etc.

Depending mainly on the environment, the approach chosen will be defined. Some of the approaches lead to serious political problems, and to question the independency of the CAs. When a common agreement is found, this kind of problems could be solved.

An additional issue to be considered when talking about using a eService with certificates, is where is the user's certificate stored. Depending on the implantation several options can be used:

- **A file in the hard disk of the user's computer:** which stores the user's certificate. This option has the inconvenience than a physical or logical access to the user's computer, can compromise the security of the user's identity. The main advantage is that it is not necessary any infrastructure (readers, devices, etc.) extra, in open networks environments.
- **A file in a removable and conventional computer media,** such as a floppy disk, a CD-ROM or a USB Token. In this case the user can carry his certificate with him, so if an intruder access the user's computer, no fake identity could be used. "The inconvenience is that, typically, this approach is done without authenticating the identity of the media-holder (via a PIN or some other authentication mechanism), so if the media is stolen, the user's identity is once again compromised.

- **A file in a secure media**, such as a smart card, or a tamper-proof device. Usually this will need a holder authentication before accessing the information of the user's certificate. This increase security, although, as seen in the following section, it also has some inconveniences. Additionally, some of these solutions do need an extra hardware/infrastructure (reader, token, etc.) to get the system working, which leads to distribution problems that have to be solved.

3.3 Aided with Biometrics

As seen in the previous sections, to perform the user identification, different automatic approaches can be found, such as the ones based on the belonging of an object, as a card or a token, or based on testing of a knowledge the allowed user should possess. But all of them solve the recognition problem considering something the user has. However this belonging carries some problems that affect the security of the whole system. A potential lost of the token can provide not-authorized users the possibility of being allowed to access to the service protected. Most of the people use words or dates related to their personal life as a password difficult to forget it, which makes the password easily guessed by intruders. These situations induce to develop new security systems, considering that probably one of the safest way of perform the identification is the one done by a person; such a policeman compares a photograph of the password with the person the password belongs to.

But not in all situations it could be a person that can perform this verification, especially in eServices, and therefore the use of biometrics becomes a recommended (if not mandatory). Biometrics identifies the user considering physical or behavioral characteristics of the human being. These technologies are based on something the person is, not something he/she has, not allowing the lost or the transfer to any other user, which increases the security rate of the whole system.

When implementing a biometric system different approaches could be followed. One of the main classifications of these systems can be done: centralized or distributed system. A centralized system is the one that use a database to store the user data and it is consulted each time an identification process take place. On the other hand, a distributed system stores the user data in different means allowing each user to carry his/her data. These distributed systems are safer than the centralized one, where the information stored in the database should be protected of a possible attack, and avoid a possible "big brother" effect.

Although Biometrics is recommended, it does not say that the other approaches have to be forgotten. Really far from that idea, biometrics can be complementary to other techniques, such as the approaches based on certificates. In fact, biometrics could be used to authenticate the user in order to grant the access to his certificate, and after that, being able to perform the eID using all PKI mechanisms available.

4. Steps to Implement eServices with eID

Once studied the different approaches that exist for implementing eID for eServices, it is interesting to enumerate the steps required by a service provider, to be able to implement an eService using eID. This is only a proposal, which, depending on the situation could suffer a great series of changes. Some of them will be enumerated in the document, but many other constraints could appear at any moment.

Step 1: Define the eService relationship with the user

System designer should be aware of the really need of identifying the user, and the level of identification requested. For example:

- is really necessary to identify the user for the service given?
- that necessity is for the user's profit, or for the service provider profit?
- should it be a legal identification, or just an identification of being a client of the service provider?

Step 2: Model the characteristics of the community of users

The community of user could apply a series of technical restrictions. For example, if the users are located in a determined geographical area, they could share the same identification scheme, but when users are located in different areas many other challenges appear. Also, users can be reluctant to the idea of being identified, or to the use of some biometric technique.

Step 3: Define the Interoperability desired/required

In this step, with the information from the previous ones, interoperability needs should be defined. When the relation is fully local, and users are not expected to access the service outside of their local environment, then there is no need to worry about interoperability issues. But in other cases, it should be defined whether this is needed among different PKIs in the same environment, or in different ones (e.g. in different countries). Also, the level of interoperability should be defined, so if it is going to be at application level, or at eID service level, or even at infrastructure level.

Step 4: Decide the way the eID will be implemented

With all results from previous steps, the way eID will be implemented could be handled, so as if it is going to be done with the physical verification of the Token, or via PKI with the user certificate stored in a smart card, which authenticate the card-holder using biometrics, or any of the other intermediate solutions.

Step 5: Define all technical issues related to the previous decisions

For example, if a PKI approach is decided, then having a look to the environment requirements, define the way the interoperability is achieved (hierarchical, bridge, cross certification, CTL, etc.). Also, if a smart card is going to be used, which kind of card will be required, if it is going to be compatible, or the system will try to handle all different cards.

Step 6: Develop the eService

Once the design has been done, the development will start (which can also introduce some modifications to the initial decisions).

Step 7: Implant the eService

An of course, finally, once the development is finished, the implantation has to be done in an efficient way, showing the users how it works, its benefits, and solving all their relevant questions.