

Which services are to be prepared for connection to Interoperable eID?

eEpoch 2nd Conference

Issy-les-Moulineaux

24th September 2003

Vicente Sebastián

(ETRA I+D)

 eEpoch



Content

- Context of eEpoch
- IOP specifications
- Non-technological approach
- Technological approach
- How IOP will be demonstrated in practice

 eEpoch



Context of eEpoch

Context of eEpoch

- eEpoch aims at being the proof of concept of the results of the work done by the the eEurope Smart Card Charter on Global Interoperability Framework for IAS with SmartCards.
- eEpoch is a complete test field because the presence of:
 - Industry
 - Governments / Administrations
 - Service providers

Context of eEpoch

- There is a common intention to carry out trials to face the actual constraints and problems to guarantee IOP at pan-European scale from all the points of view.
- eEpoch has two complementary working lines to address all the necessary aspects:
 - Non-technical specifications
 - Technical specifications

The process in eEpoch

- We are following a progressive approach throughout series of meetings with pilots and technical partners.
- In those meetings all the aspects that can be related with the IOP of the e-services are analyzed and compared:
 - Applications and existing services
 - Architectures
 - Technologies
 - Actors and stakeholders
 - Legal restrictions
 - ...

IOP specifications

GIF input

- The scope of eEpoch is with regards IAS.
- The work for IOP Specifications uses as inputs the GIF that *provides both smart card communities and e-service communities with the necessary concepts and guidance on the tools required for access to e-services and for security of transactions over the Internet where special "high-end" requirements must be fulfilled concerning identification, authentication (tokens and persons), non-repudiation (by electronic signature), encryption and integration with other applications.*

GIF references

- GIF Part 1: Contextual and conceptual modelling:
 - An in depth modelling of the smart card, its environment and interoperability issues with regards to identification, authentication and electronic signature;
- GIF Part 2: Requirements for IAS functional interoperability
 - A list of functional requirements and interoperability prerequisites to be used together with Part 1 for establishing a set of specifications for interoperability at IAS level

GIF references

- GIF Part 3: Recommendation for IOP specifications
 - guidance for enabling, implementing and operating IAS inter-operability;
- GIF Part 4: Deployment strategies for generic IAS
 - an overview of business plan elements, organisational issues, and system development processes for mass deployment strategies.

Non-technological approach

Assumed interoperability architecture

- The interoperability is projected on a 4-layer architecture, in which is
 - card: smartcard containing the EID/IAS application
 - Infrastructure: terminals and network, connecting cards, EID/IAS application, E-service and PKI
 - E-service: web based or web-emulated front office application, containing any e-service that requires strong authentication and/or qualified electronic signature
 - Certificate: PKI

Methodology

- Based on the methodology of “on-us” “not-on-us” used in the GIF.
- The attribute is assigned to each item according it is used/owned in/by the pilot or not.
- The following situations are presented by the eEpoch pilots.

eEpoch map

Situation	Cards	Infrastructure	e-service	certificate
0	On-us	On-us	On-us	On-us
1	Not-on-us	On-us	On- us	Not-on-us
2	Not-on-us	On-us	Not-on-us	Not-on-us
3	On-us	On-us	Not-on-us	On us
4	Not-on-us	Not-on-us	On-us	Not-on-us
5	On-us	Not-on- us	On- us	On-us

The card interoperability means the capability to handle on-us and not-on-us cards and to make the connections

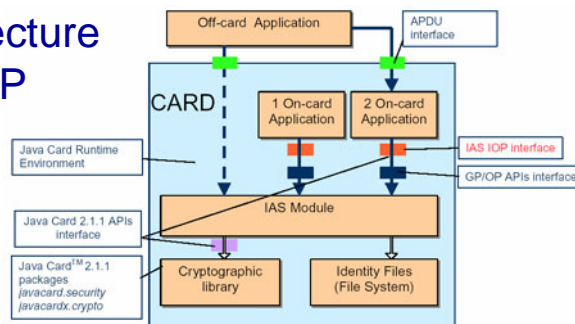
Technological approach

Identification Autentication & Signature IOP

- Functional Mapping of GIF on E-Sign K
 - Part 2 – Requirements for IAS Functional Interoperability
 - GIF Part 3: Recommendation for IOP specifications
 - Part 1 – Basic Requirements. Application Interface for Smartcards used as Secure Signature Creation Devices, CEN/ISSS WS/E-Sign Group K Draft CWA

Card IOP

- Specifications apply to Native cards and Open Platforms (like JavaCards)
- It is being specified a new architecture to support IOP



eEpoch



Certificate IOP

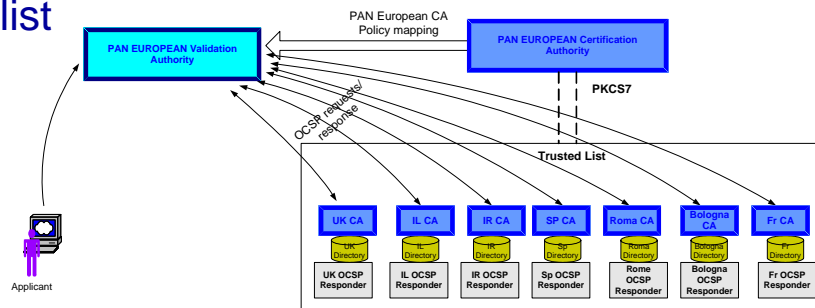
- Classical approach: CA-CA cross certification
 - Appropriate for a reduced and defined group of actors
 - Inappropriate for a large and flexible group:
Cross certifying n [6] pilot site CAs requires $n(n-1)/2$ [15] mutual cross-certification and $n(n-1)$ [30] certificates to install in browsers.

eEpoch



Certificate IOP

- The eEpoch PKI model will be structured as a list of trusted CAs. A CA known as “Pan European CA” will certify the trusted list



eEpoch



eEurope
SmartCards

How IOP will be demonstrated
in practice

eEpoch



eEurope
SmartCards

Interoperability Matrix

To/From	Bologna	Issy	Israel	Rome	Sheffield	Spain
Bologna						
Issy						
Israel						
Rome						
Sheffield						
Spain						

IOP Offer	
No information	

Bologna

- Bologna offers for the pilot two browser based services:
 - A service for entrepreneurs wanting to establish a company in Bologna,
 - A service for owners of actual properties in Bologna, wanting to handle their local taxes.
- Accepted by
 - Spain
 - Rome
 - Issy

Issy-les-Moulineaux

- The e-service that is offered by Issy is on 'e-ticketing'. Announcements of cultural events takes place via internet technology. It requires authentication and qualified signature when e-payment.
- Accepted by
 - Bologna
 - Spain

 eEpoch



 eEurope
SmartGrids

Rome

- Rome offers for the pilot that authenticated citizens, who use the service of INSP online access to their data in the INSP database
- Accepted by
 - Bologna
 - Israel

 eEpoch



 eEurope
SmartGrids

Israel

- Israel offers three services
 - National Insurance Form, to be signed by on-us cards via not-on-us infrastructure
 - Tourist application, with order to be signed, by not on us cards via not-on-us infrastructure
 - E-voting, with e-authentication to prevent double voting per person, for on-us and not-on-us cards, via on-us and not-on-us infrastructure
- Accepted by
 - Rome
 - Spain

 eEpoch



 eEurope
SmartCards

Spain

- Spain makes a browser based document available to formalise denounces, and offers that it will be signed with not-on-us certificate.
- Accepted by
 - Bologna
 - Issy
 - Rome

 eEpoch



 eEurope
SmartCards

Conclusions

- The specification for the IOP of eServices in eEpoch is addressing all the actual problems and constraints.
- Some barriers are out of the scope of eEpoch
- The conclusions based on the analysis of the e-services offered in eEpoch will be of reference for new services.

**More info in
www.eepoch.net**