

# **eEpoch**

## **3rd Open Conference**

# **Preview of Pan-European Interoperability of eID**

7<sup>th</sup> June 2004 Landesversicherungsanstalt  
(LVA) Rheinprovinz

Düsseldorf  
GERMANY

# Relevance of eEpoch Project

Antonio Marqués  
eEpoch Project Director  
ETRA I+D



# Contents

- Need of eEpoch
- Objectives of eEpoch
- How eEpoch objectives will be reached
- eEpoch Results

# Context

- Identity is inherent to the individuals.
- Individual identity is the same from local to European scope.
- When an individual wants to authenticate himself in other region, there are physical documents that are accepted because of the confidence and arrangements among governments.
- When we move to the context of EID, the Interoperability means the capability to permit the IAS of an individual by electronic means.

# The need for IOP eID

- The need and use for electronic identity is broadly shared all over the world.
- We are 25 Member States at the European Union. It is necessary to ensure a successful scalable deployment of PKI and SmartCards in the public ID.
- It is the need for the implementation of trusted interoperable e-government and e-administration services in Europe to gain citizens confidence on the use of Internet and Information Technologies.

# eEpoch Relevance

- It provides a representative and heterogeneous test field to check the pan-European dimension of the IOP, maintaining also the local constraints and requirements.
- It demonstrates the smart card technology capability of implementing a solution for secure and authenticated digital identity.
- It demonstrates the interoperability of the services and solutions according to the requirements of the users and the legal frameworks.
- It proposes solutions to harmonise smart card infrastructures to support the interoperability across sectors and countries

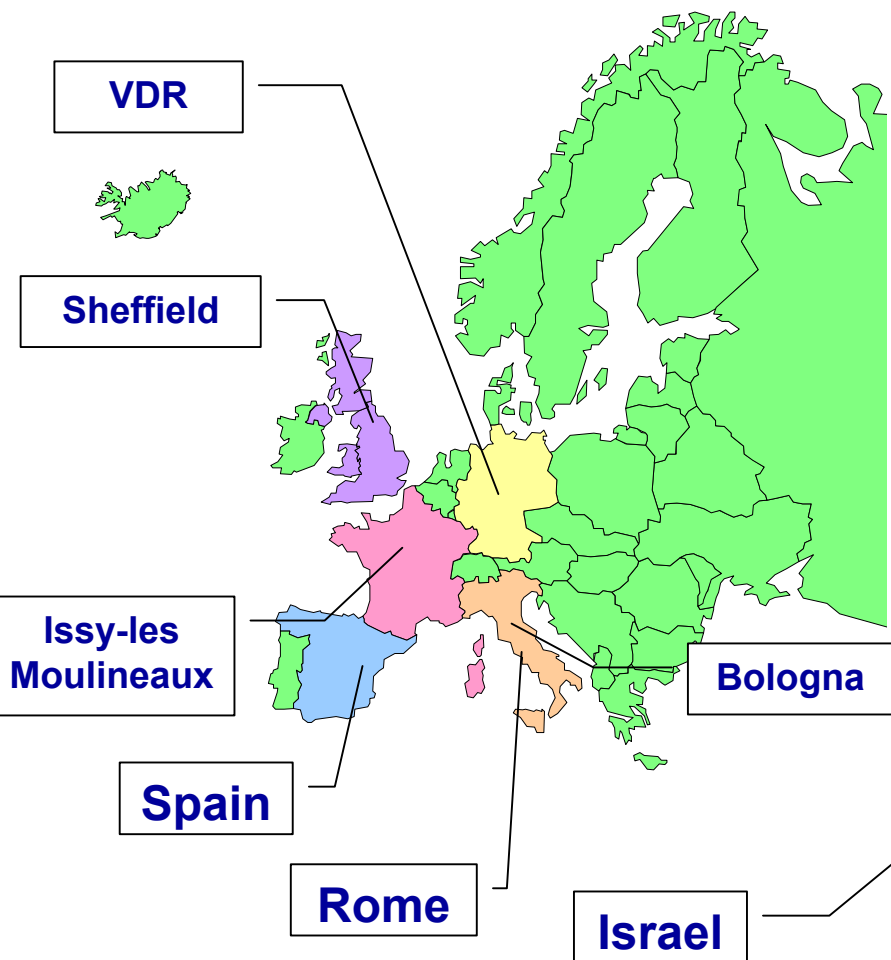
# eEpoch Participants

**16 Organizations**

**7 Pilots**

ETRA INVESTIGATION Y DESAROLLO, S.A.	E	Comune di Bologna	I
SCHLUMBERGER/SEMA	F	Laboratori Fondazione Guglielmo Marconi	I
GlobalSign	B	Istituto Nazionale della Previdenza Sociale	I
Safelayer	E	FINSIEL S.p.A.	I
GIESECKE & DEVRIENT	D	POSTECOM S.p.A.	I
SEM ISSY MEDIA	F	Direccion General de la Policia	E
VDR	D	Sheffield City Council	UK
Ministry of Finance - Israel	IL	Universidad Carlos III	E

# eEpoch Pilots



- Seven Pilots
- Pilots have autonomy for defining the service/application area, but...
  - Common nucleus for identification and authentication based on GIF
  - Interoperability will be demonstrated
  - Sites will contribute to Knowledge research and transfer
- Evaluation by comparison of best practices and benchmarks

# Steps to reach IOP

- Understanding IOP
- Harmonising information -> PKI
- Defining realistic IOP levels

# Understanding IOP



Phase 1: accepting interoperability

*‘from “on-our-own” to pan european’*

Phase 2: preparing for interoperability

*‘from models to reality’*

Phase 3: implementing interoperability

*‘from first experience to stability’*

Phase 4: learning from interoperability

*‘taking advantages of other experiences’*

# Harmonising information

- Definition of a subset of the E-Sign K specification
- Specification of an IAS IOP Interface for Java cards based on the functional mapping of the eEurope GIF documents on the E-SIGN K specification
- Specification of a set of requirements related to the design of a PKI platform that takes into account eEpoch objectives and details the eEpoch certificate structuring.

# eEpoch IOP levels

- ***IOP at Certification Level***
  - Central CA to spread trust through CTL's
  - Validation Services – OCSP based (Online Certificate Status Protocol)
- ***IOP at Application Level***
  - Web Services
  - Email Exchange
- ***IOP at Card Level***
  - IOP at PKCS#11 Compliant Level
  - IOP at MUSCLE Compliant Level
  - IOP at eEpoch Card Level

# IOP at Certification Level (I)

- A Certification Authority able to retrieve “CA certificates” from the different PKI Pilots and responsible to issue a CTL (Certificate Trust List) to spread trust through the different pilot applications.
- A Validation Authority based on an OCSP Responder that collect the status of the certificates issued by the different pilots through their published CRL’s and/or their own OCSP servers.

# IOP at Certification Level (II)

- Citizen certificates: All pilote site use two certificates:
  - Most of them use the qualified certificate for signature.
  - Most of them use classical X.509 certificate for authentication.
  - Only Spanish pilot uses biometrics.

# IOP at Application Level

- WEB Services:
  - formalization of crime reporting to the police via Internet (Spain)
  - INPS Italian Services
  - INPS Foreign Services
  - ICIWeb (Bologna)
  - Ludothèque server (Issy Le Moulineaux)
  - eTendering (Sheffield)
- Email Exchange

# IOP at Card Level

- IOP at PKCS#11 Compliant Level
  - To maintain existing & proprietary services
  - This enables the use different kind of cards, from different vendors or even eEpoch compliant cards, on Pilot applications
- IOP at MUSCLE Compliant Level
  - Open Source that provides a common base for different Java Cards (Axalto, Gemplus, etc) on different platforms (Windows, Solaris, Linux, MacOS).
  - It provides interface to PKCS#11.
- IOP at eEpoch Card Level
  - The most innovative.
  - To be implemented in Open Source by Sheffield.

# Conclusion

- eEpoch provides to the European Society:
  - Technical Specifications for eID IOP at different levels.
  - Input to the European standardization committees on e-ID
  - Lessons learned on the actual implementation of IOP on eID based on eEpoch PKI Architecture.

**Thank you.**

[www.eepoch.net](http://www.eepoch.net)