

# Policy and Guidelines to reach Interoperability

1st eEpoch conference  
February 13, 2003. Madrid  
Hubert VIGNERON  
Schlumberger

## Agenda

1. Interoperability issues: focus
2. Objectives
3. eEpoch policy
4. IAS and card specification
5. Guidelines
6. Considerations and References
7. Questions to be answered
8. The French government case

# Glossary

- Application:
  - a software program (an applet) which execute a function or a set of functions
- Function
  - A basic functionality of the card which can be used in various services: *authentication,...*
- Service
  - A set of functions which allow a service to be filled for the benefit of the cardholder

# Interoperability issues

- Operational
  - Services
- Functional: IAS
  - Identification
  - Authentication
  - Signature
- Technical
  - Cards
  - Infrastructure

## eEpoch main objectives

- To specify how to achieve interoperability (technical and functional) of smart card based Identification, strong Authentication and Qualified Electronic Signature using IAS
- To demonstrate interoperability of these core functions between European member states through their implementation in the card schemes of pilot cities

## Additional objectives

- To prepare the implementation of pan European services using these functions: service, business requirements, security policy...
- To define card scheme specifications that allow various security levels including PKI
- To encourage convergence of the specifications in the implementation of the pilot sites

## eEpoch policy: free choice

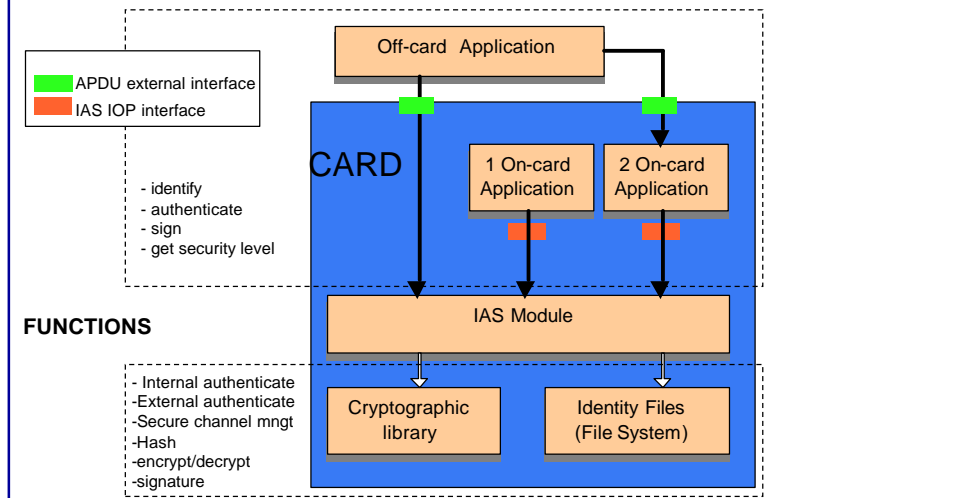
- Pilots sites are free to choose:
  - The services to connect with IAS
  - The card platform technology: open or other
  - The terminal and related infrastructure
  - The card issuance and management process
  - The PKI infrastructure
  - The level of security

but with some conditions.....

## eEpoch card specifications

- What WP3 will provide:
  - The specification of a card able to support the IAS application. It will be possible for both on card and off card applications (services) to access the IAS.
  - These specifications will be based on the merge of various recommendations, schemes or standardization initiatives:
    - GIF part 3, ISO7816-4/8, PKCS#15, JC2.1, OP2.1, ESIGN, CWA 14169,.....

# Generic IAS functional overview



eEpoch

ist

eEurope

## eEpoch guidelines

- Pilots sites should consider to:
  - Implement cards complying with WP3 technical specifications (or at least show where to use them in the roadmap): for example
    - The Card File System should be structured according to PKCS#15
    - An Application Directory should be allocated to store only the identification data representing the cardholder (photo, address, marital status...).
  - Choose a terminal and a card issuance and management system compatible with eEpoch card specifications

eEpoch

ist

eEurope

# eEpoch guidelines

- File system content: personal ID data
  - Identifiers based on standard data elements: social security nb, driving license nb,...
  - Private keys
  - Certificates
    - Related to National directives / Laws or existing data bases
    - Related to European directives or data bases
- Pan European interoperable service supported by IAS (option)

Decisions should be taken before Conference 2

# eEpoch policy: to be considered

- An Open Platform will enable
  - post-issuance personalization so that new Service Providers (eGov institutions) may have their respective services installed on card during the life cycle of the card (life of the card can reach 10 years).
  - service providers to implement their services regardless of the underlying low-level procedures dealing with security and cryptography (to get benefit from those pre-built standardized functions).
- An Open Platform will leverage the e-Gov business model

# References for policy statements

- References:
  - Electronic Signature Directive 1999/93/EC
  - Application interface for smart Cards used as Secure Signature Creation Devices (12 march 2002)
  - EESSI deliverable: CWA
- Additional references
  - Electronic Identity Whitepaper ([www.europe-smartcards.org](http://www.europe-smartcards.org)) final release: march 2003
  - GIF part 2, chapter 3.3 :”Requirements for stakeholders roles” ([www.europe-smartcards.org](http://www.europe-smartcards.org)) final release march 2003.
  - National standards for ID: Spain, France, Italy, Finland,...
  - Directive relating to European driving licenses 96/47/EC

# Reference to ID programs in progress

	Nat. ID	Pin / biom	PKI	Rollout
• Austria	y	p	y	started
• Baltics	y	p	y	started
• Belgium	y	p nb	y	pilot
• Czech rep.	Y	p	y	preparation
• Denmark	p			
• Finland		p nb		started
• France	p			
• Germany	p			
• Greece	y	p	y	
• Ireland	y			
• Italy	y	p b	y	started
• Netherlands	y	p b	y	
• Norway				
• Portugal	y			
• Slovenia				preparation
• Spain	y	p b		preparation
• Sweden	y	p nb	y	started
• UK	p			

# Questions to be answered for 2nd conference

- What is your interest in IAS ?
- What basis do you take for the personal data ? What is/are the identifier(s) and certificate (s) you use for identification on a local and national basis ?
- In your project what is your priority (main service to be filled) and what are the most important functions within IAS:
  - Identification (for ex: Binding the person to the identification data of the card)
  - Strong authentication
  - Electronic signature based on qualified certificates
- What are the services you connect to the 'IAS' and which ones are worth to become interoperable at European level ?

# French government policy.....

“ Titre fondateur”