

2nd eEpoch Open Conference (24.09.03)

eEpoch (eEurope Smart Card Charter proof of concept and holistic solution) General Architecture of a System with interoperable IAS

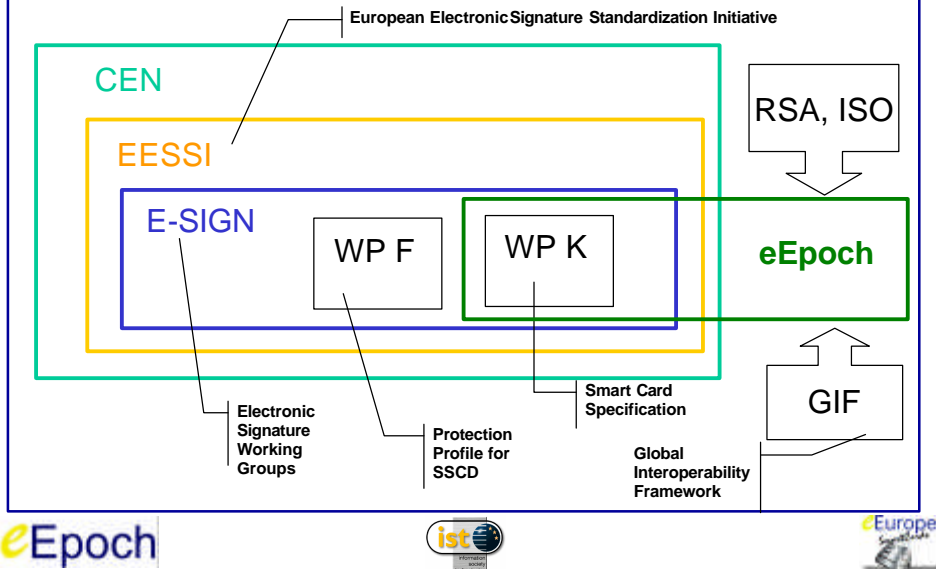
Mourad Faher
axalto A Schlumberger company
mourad.faher@louveciennes.sema.slb.com



Topics

1. Standardization Bodies overview
2. Tasks and Work Packages organization
3. Participants, expected services/deployment
4. Core Application and related Java Card Architecture
5. Comparison: Native Platform versus Open Platform
6. IAS-enabled card personalization
7. Foreseen Business Model(s) and interoperability
8. Conclusion

1. Standardization Bodies overview



2. Tasks and WP organization 1/2

- Task 3.1 Input from the existing national/eGov ID services. Directives and legal aspects.
 - Task 3.2 Definition of IOP specification. Contribution of GIF as follows :
 - Part 1 : Contextual and conceptual Modelling, High level design
 - Part 2 : Requirements for IAS (Ident., Authentication, Signature)
 - Part 3 : Recommendation for IOP Specification
- Mapping of GIF Part 3 to E-SIGN K functionality. E-SIGN K used to describe APDU command set.
- Task 3.3 Definition of test specification for Pilot sites

2. Tasks and WP organization 2/2

- WP1 : Knowledge Base
- WP2 : Knowledge Transfer, Dissemination
- WP3 : Determination of IOP, Specification
- WP4 : IOP Demonstration



3. Participants, expected services

➤ eEpoch WP3 members:

- Schlumberger, Giesecke & Devrient, Ubizen (formerly GlobalSign).

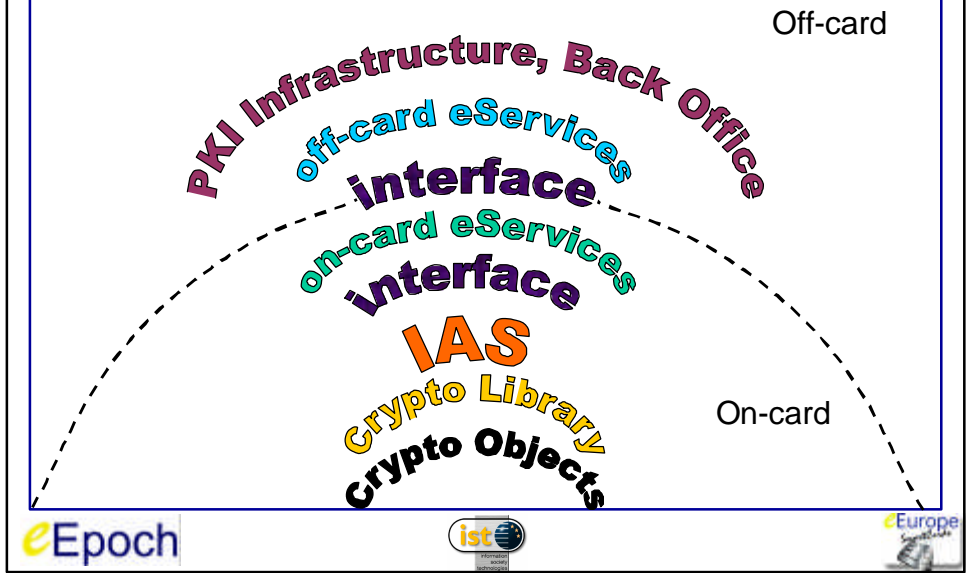
➤ Project Coordination:

- ETRA (Spain)

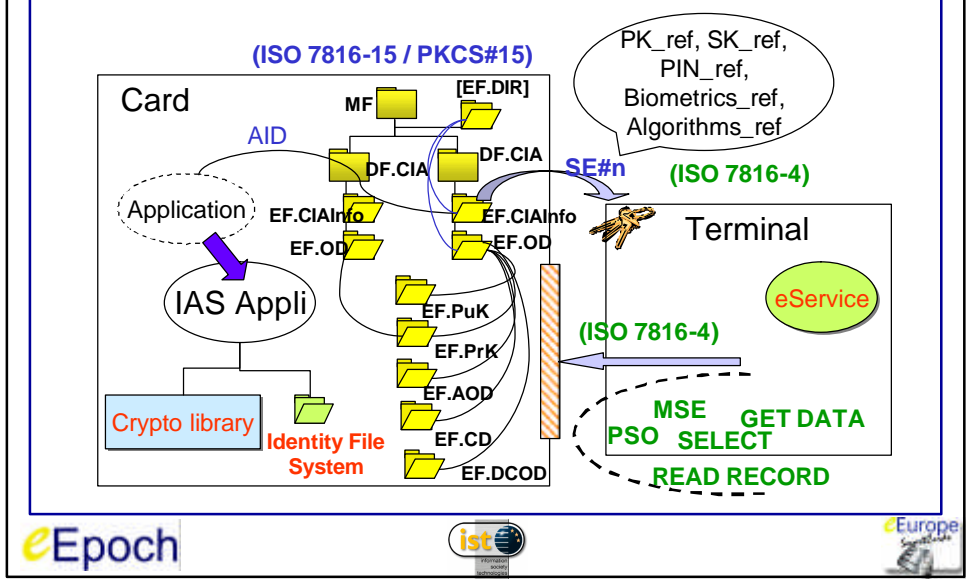
➤ Pilot sites:

- Spain (Dirección General de la Policía) : cross border access for ID Card / eforum ...
- Italy (Bologna & Roma): employees insurance document / game / social security forms / local taxes payment from abroad, applications to sign remotely over Internet...
- France (Issy): CVQ (Daily Life Card)
- Israel (Jerusalem): National insurance form filled out by people located in Italy or Spain / tourism application (booking hotels) / eVote (prevent from giving their opinion twice)
- Britain (Newcastle left the Consortium), may be replaced by Bremen (GE)

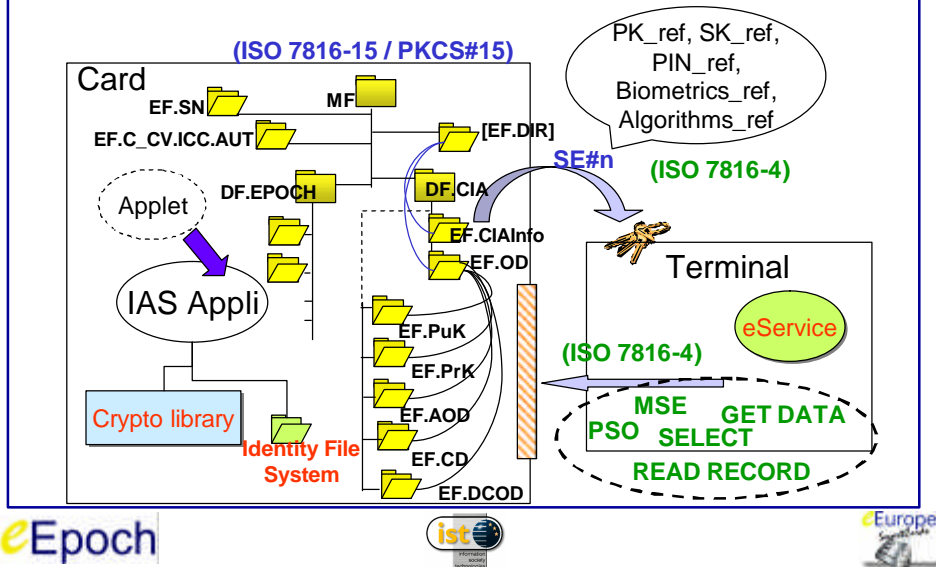
4.Core Application concept 1/5



4.Core Application & Architecture 2/5



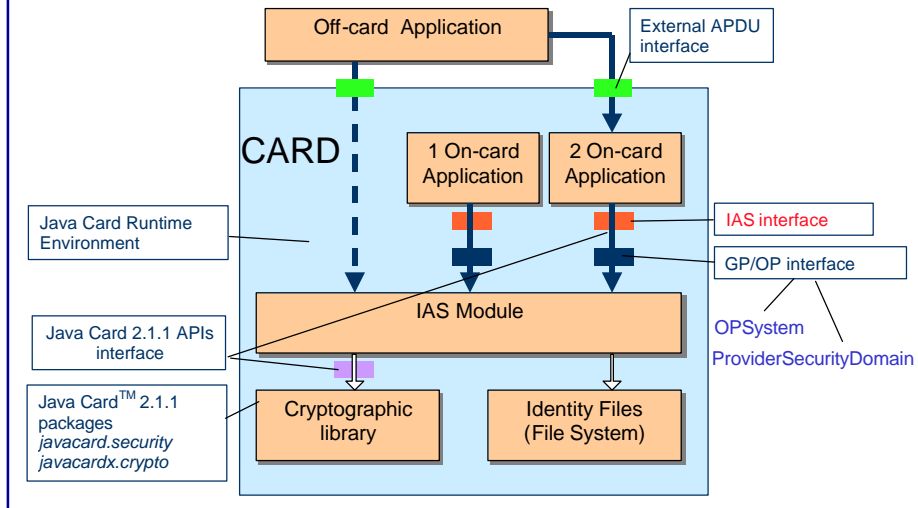
4.Core Application & Architecture 3/5



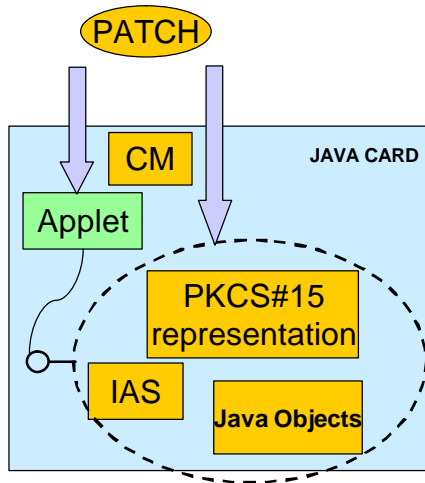
4.Core Application & Architecture 4/5

- Additional Functionality
 - **Read Signed data:** Proprietary command adopted from Tachograph System (Commission Regulation (EC) N° 1360/2002)
 - **Retrieval of Public Key:** after Key Pair generation
 - Two export methods
 - READ BINARY
 - GET DATA

4. Core Application & Architecture 5/5

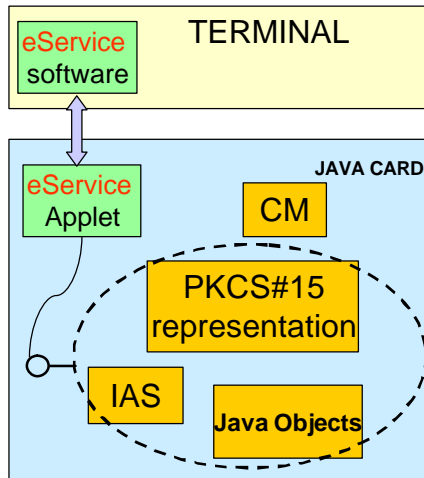


5. Comparison: Native OS vs OP_{1/2}



The patching for application upgrade purposes is not available for native OS.

5. Comparison: Native OS vs OP_{2/2}



eService functions and logic shared between the terminal and the card application.

The Applet may alleviate the terminal software and participate to the interoperability.

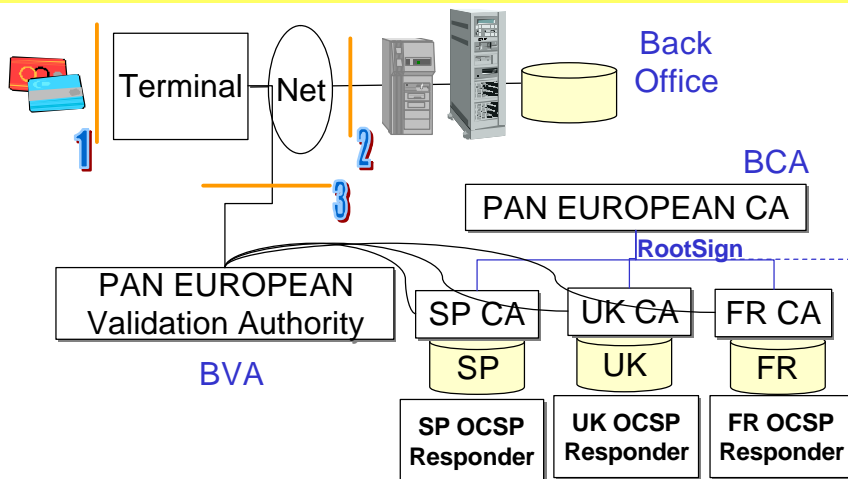
6. IAS-card Personalization

- Pre-personalization
 - load of applets byte code
- Personalization
 - Load / generation of Key Pair
 - Load of the certified PuK
 - Installation of cryptographic objects according to ISO 7816-15

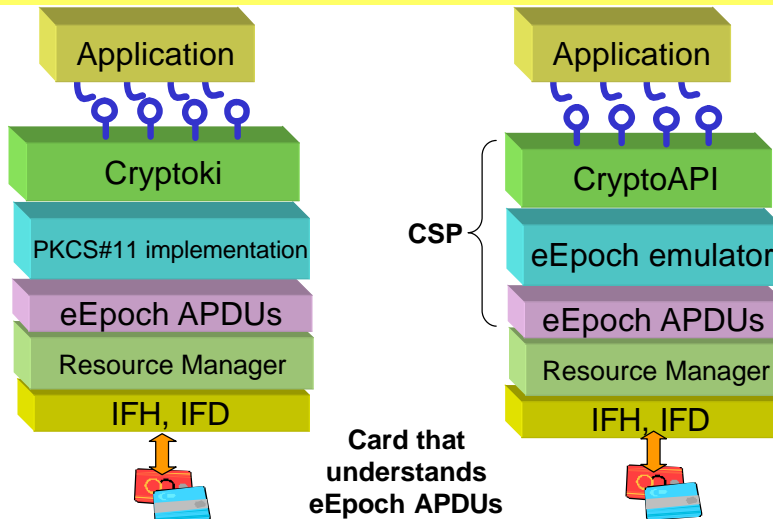
7. Business Model & Interoperability^{1/3}

- Three levels of interoperability
 - Command level: External APDU interface (ISO)
 - Application level: cross border agreement between Service Providers
 - Public Key Infrastructure level: certificate validation

7. Business Model & Interoperability^{2/3}



7. Business Model & Interoperability_{3/3}



8. Conclusion

- eEpoch Platform
 - Java Card being not File System oriented, a convergence between PKCS#15 scheme and Global Platform OP specification is useful.
- eEpoch deployment
 - According to their own policy, the Pilots sites are currently determining their eServices and their business model to foresee future extension from demonstrator to the field.

2nd eEpoch Open Conference (24.09.03)

eEpoch
(eEurope Smart Card Charter proof of
concept and holistic solution)
General Architecture of a System with
interoperable IAS

Mourad Faher
axalto A Schlumberger company
mourad.faher@louveciennes.sema.slb.com

