



Spain Pilot

eEpoch 1st Conference on Policy Statements, Business Cases & Management Guidelines

Manuel Torres
Profesional Services Manager
mtorres@safelayer.com



Spanish ID Card



No need to evangelise about Id Card Benefits

People require same level of privacy in the Net than in real world



eEpoch Spanish Framework

- DGP has already an official Electronic ID Card project for Spanish citizens which “is not” included within the eEpoch framework.
- The DGP participation on eEpoch has an aim to look for interoperability trials and evidences that could be used on its Electronic ID Card Project (eDNI) with similar initiatives around EU community.

The ID Card Project

1. More than 5 M DNI (Id Cards) issued every year
2. Population target is 40.000.000 users
3. The features provides by the new Spanish ID Card must be divided into two functionalities:
 1. Physical Security.
 2. Electronic Security.
4. Provision of Validation Services based on OCSP.
5. No need to publish citizens certificates into a repository but CRL's & ARL's.
6. Be able to provide third parties entities of the public administration with the relevant tools.
7. The certificates issued should be for authentication and Non-Repudiation.
8. Qualified Certificates following CEN CWAs, following EU standards initiatives.
9. Several and distributed Registration centers to issue ID Card, having in mind many operators .
10. The overall time to issue the new ID Card “MUST BE” 10 minutes.

System Requirements

- **Availability**
 - The system must be 24x7x365.
 - MUST BE multi-technology
- **Performance**
 - 120 certification request per second, each request will contain two keys per request.
 - 1.000 OCSP transactions per second
 - 1.400 cryptographic operations per second for the HSM's components.
 - 1.200 concurrent users
 - 100 concurrent users from unattended services points
 - Revocation status updated in less than 15 seconds
- **Security**
 - CA facilities is a Bunker with more than 9 security levels
 - Logical security on every PKI component
 - Business continuity plan on place.
 - Continuous monitoring of the system

SC (chip) Requirements

- Compliant CC EAL4+ or higher.
- File system defined following PKCS#15, including biometrics extensions
- Keys must be generated by the microchip in front of the citizen.
- Keys protected by a strong PIN (pass phrase, not only digits), choose by citizen.
- Keys must be RSA 1024 or higher
- Issued the card, it must be impossible to modify the contents of microchip but PIN update and certificate renew.
- Private key always in microchip, never go out.
- Citizen can at anytime change PIN, unblock cards and renew certificates at Police Stations by using fingerprint on unattended but controlled kiosks.

SC Requirements

Material

Due to the ID card act like an official travel document it must be necessary a secure support.

Polycarbonate (PC) as been chose since it guarantee a good durability and it's the best material for using with laser engraving.

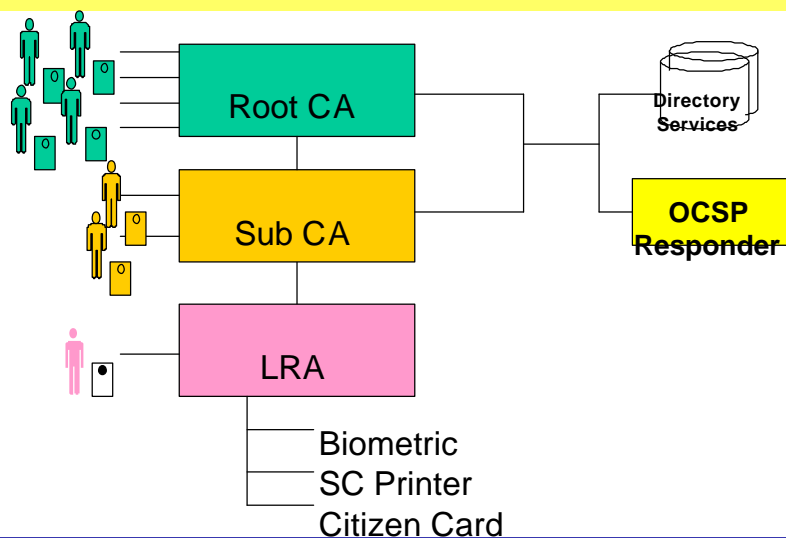
Initiative supporters

- **There are some legal initiatives promoted from central and regional governments to support and to guarantee the complete successful of the Spanish ID Card, such as:**
 - A Virtual Registration office will be created so citizens will be able to carry out any kind of transaction with the PA through it.
 - The CSI (Consejo superior de Informática) will promote and will recommend the use of DNI for all authenticated communications.
 - Citizens will have an unique e-mail address.
 - DNI will be used by private entities.
 - Other TTPs will be able to use DNI to support their registration process

The eEpoch Pilot

- **Technologies:**
 - **PKI: Safelayer**
 - **LDAP: iPlanet**
 - **Smart Cards: TBD**
 - **OS: Solaris and Windows**
 - **SGBD: Oracle, Informix.**
 - **Biometrics: TBD**

eEpoch Architecture (Spain)



eEpoch Project Tasks (Spain)

- **T4.9 Spain Demonstration.** This task is scheduled in the following main phases
 - T4.9.1 Usability Scenarios specification.
 - T4.9.2 System Specification.
 - T4.9.3 Integration Test procedures specifications.
 - T4.9.4 PKI components integration.
 - T4.9.5 Installation and start up of the trial PKI.
 - T4.9.6 Test system analysis.

eEpoch “Deliverables” (Spain)

- As main deliverable of task 4.9 will be produced a technical sub-deliverable that will compile the following technical notes:
 - TN 4.9.1 Usability Scenarios
 - TN 4.9.2 Technical System Specification
 - TN 4.9.3 Integration Test procedures
 - TN 4.9.4 PKI components installation & integration
 - TN 4.9.5 Installation & Configuration specification
 - TN 4.9.6 Test system Report

What we are looking?

International Civil Aviation Organisation

**US “Enhanced Border Security and Visa Entry Reform Act”
SEC. 303. Machine Readable, Tamper Resistant Entry and Exit Documents.**

“(c) (1) Not later than October 26, 2004, the government of each country that is designated to participate in the visa waiver program ... shall certify ... that it has a program to issue to its nationals machine readable passports that are tamper resistant and incorporate biometric and document authentication identifiers that comply with application biometric and document identifying standards established by the **International Civil Aviation Organisation.**”

ICAO have already published 2nd Edition of 9303 3 Size 1 and Size 2 Machine Readable Official Travel Documents.

What we are looking?

- ISO SC37 “First Report of JTC1 SC37 Biometrics”
- ISO SC17 “CARDS AND PERSONAL IDENTIFICATION”
- ISO SC27 “IT Security Techniques”
- Porvoo
- CEN / ETSI
- Others ???

What we expect ?

Interoperability framework

Interoperability trial

Interoperability evidences

Be a testbed for the real system