

European Electronic Identity Practices

Country Update of Portugal

Speaker: Anabela Pedroso

anabela.pedroso@umic.pt

Date: 3 November 2006

1. Status of National legislation on eID

- Are eID specific regulations enacted and in place?

Almost! Currently the new Law for Portuguese Citizen Card is on Portuguese Parliament for discussion and approval

2. CA organisation

- **Responsible CA organization:** Ministry of Justice – Information Technology Institute for Ministry of Justice (ITIJ)
- **The background of the organization:** Public Organization responsible for implementing and running IT in Ministry of Justice
- **Card/ Certificate issuer:** Ministry of Justice – Portuguese Registration Centre for Citizens and Enterprises (DGRN- Direcção-Geral de Registos e Notariado)
- **No. of certificates stored on the eID chip:** 2 certificates are available for the citizen (authentication and signature)
- **What access mechanism is used for each private key:** Private key is stored in the chip, in a high secure environment. The chip is in a EAL5+ certification process

3. Status of National deployment of eID

- Is the eID card obligatory: **yes**
- Number of inhabitants: **10 millions**
- Number of eID cards issued as of October 2006: **0**
- Number of certificates activated: **0**
- Yearly growth rate (percentage): **N/A**
- The expected number of eIDcards by the end of 2007: **200.000**

3. Status on National deployment of eID

- Basic functionalities of the eID card:
 - Official national ID document? Yes
 - European travel document? Yes
 - eServices? Authentication and signature
 - Other?
 - Authentication through multiple channels (using one-time-password application)
 - Match-on-the-card application
 - Offline data transfer (some are PIN protected – e.g., address)

- Validity period of the card/certificates:
 - 5 years

3. Status of national deployment of eID

- The price of the card in euros:
 - for the citizen: In study
 - for the card issuer: In study
 - price for the card reader and software: In study
 - any additional costs for the user/relying party:
In study
- From whom and how can the citizen obtain the end/user packages:
 - In 2007: only the State will provide these packages (in Identification Registration Offices, Ministry of Justice)
 - After 2007: these packages will be available in retail stores (e.g., supermarkets, ...)

3.1. Portuguese eID Citizen Card



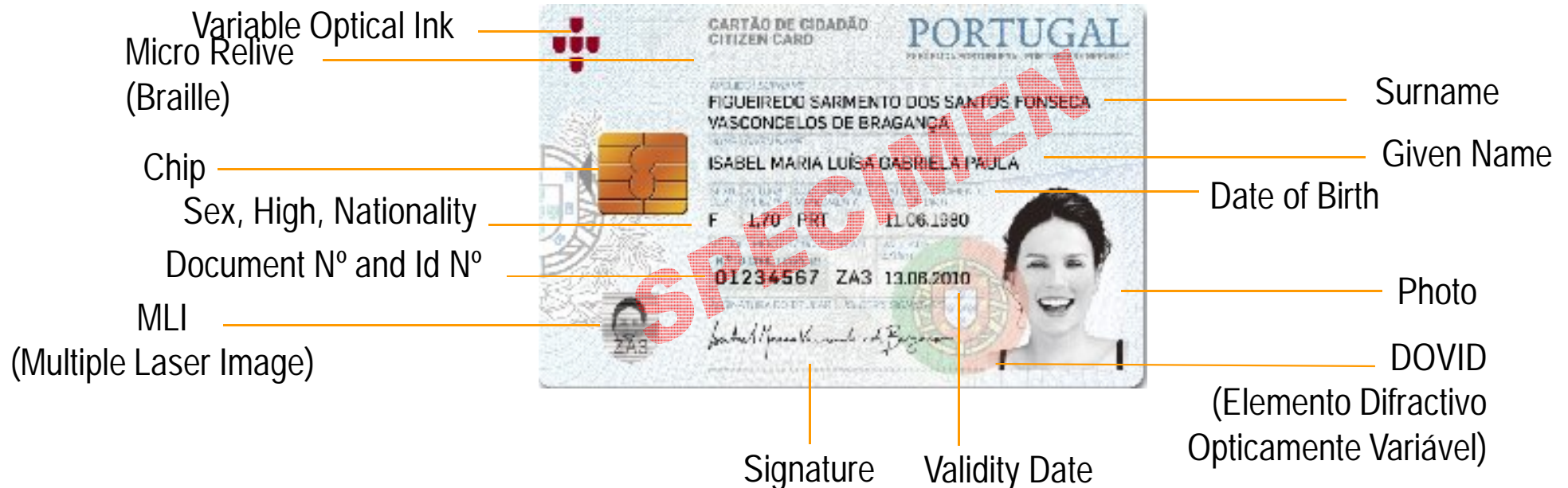
Substitutes 5 National Id Cards

- Identity Card
- Tax Card
- Social Security Card
- Health Services User Card
- Voters Card

Citizen Card

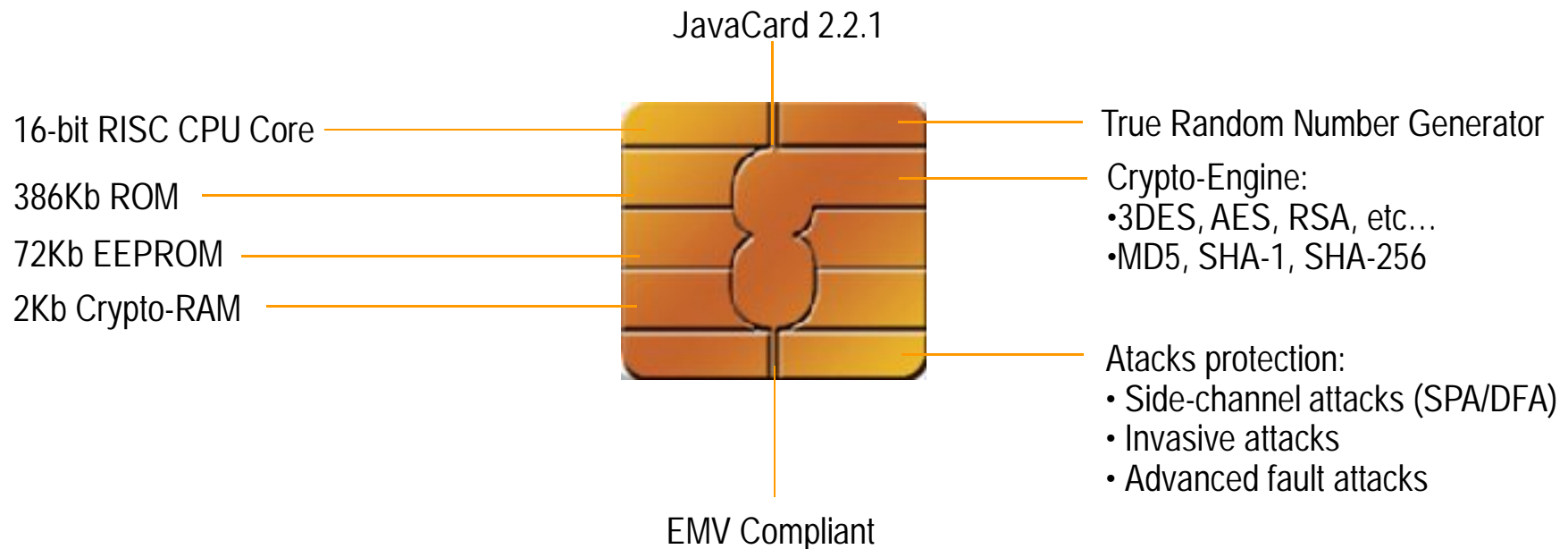
Front

- Physical support (ID-1 format) in polycarbonate with several physical security mechanisms (3 levels of control)
- The front of the Card holds specific information about the identification of the citizen



Citizen Card *Chip*

- *Chip JavaCard*, Philips, 72Kb EEPROM for applications and data.
- Several security mechanisms, in the algorithm and encryption and in the protection against attacks (EAL5+ certification , based in *International Common Criteria standard*)
- EMV compliant (partnership with Banks in the distribuiton of comun readers to the citizens)



4. Interoperability issues

- What is the level of Current Compliance with each of the following international standards or group activities (in Full / Planned / None):
 - CWA 15264 (eAuthentication): Compliant
 - CWA 14890 (eSign) : Compliant
 - CEN/TS 15480 1,2 (European Citizen Card): Compliant
 - ISO 19794 Biometric Data Interchange Format
Part 2: Finger Minutiae Data: Compliant
 - ISO 24727 1,2,3 (ICC programming interfaces): Compliant
 - ICAO 9303 (travel documents): Compliant, where mandatory – e.g., Portuguese Citizen Card does not have Radio Frequency interface

4. 1 Citizen Card Use of Standards

- Besides ECC *standards* ECC, The Citizen Card follows the best practices in eID:

Card:

- ISO/IEC 9798 (device-authentication/Secure messaging);
- ISO 7810;
- ISO 7811;
- ISO 7811;
- ISO 7816;
- ISO 10373;
- ISO/IEC 10373;
- EN 742:1993;
- CECC 90000;
- MIL STD-883C;
- Pr CEN/TS 15480 1,2 (European Citizen Card - draft);
- ICAO 9303 (travel documents);

Chip:

- ISO/IEC 7810
- ISO 7816;
- ISO/IEC 14443;
- Java Card/GP (suporte de Java cards, ISO/IEC 7501-3 (ICAO))
- CEN / TC 2254;
- CWA 15264;
- CWA 14890;
- ISO/IEC 19794-2: Finger Minutiae data;
- ISO/IEC 19794-4,5 : Finger Image data;
- ISO/IEC 19784 - BioAPI;
- ISO/IEC 19785 - CBEFF;
- ISO/IEC 24727
- EMV

Biometria:

- ISO/IEC/JTC 1 SC 37;
- ISO/IEC 7816-11;
- ISO/IEC FCD 19794-2 (*fingerprint minutiae*);
- ISO/IEC 19784-1 BioAPI;
- ISO/IEC 19785-1 *Common Biometric Exchange formats (CBEFF) - Part 1: Data Element Specification.*

PKI, Certificados e

Assinaturas Digitais:

- ISO/IEC 7816-15;
- CWA 14890 - CEN/ISSS *Workshop on the electronic signature (Area K)*;
- CWA 15264 (eAuthentication);
- CWA 14167 (Multipart);
- PKCS#1, PKCS#3 , PKCS#7, PKCS#8, PKCS#10, PKCS#11, PKCS#12, PKCS#15.

5. eAuthentication cross border usage and harmonisation

- Are there agreements with other national smart card issuers (either per country or bi-lateral) for mutual recognition of cards?
Status and targets of these agreements and timetable how to proceed:
 - Currently we are on informal contacts with several countries

6. Next steps in your country?

- **January 2007:** Pilot Phase of Portuguese Citizen Card (in Azores islands)
- **Summer/Autumn 2007:** Project Roll-out beginning in other municipalities
 - 2007: **PORVOO 11 in Portugal!!!**
- **During 2008:** All country and portuguese consulates around the world

Cartão de Cidadão

The Chip: Internal Applications and Data

- Principal “resident” applications:
 - IAS – Responsible for the operations of authentication and electronic signature
 - EMV-CAP – Responsible for the generation of *one-time-passwords* for alternative communications channels (e.g., telephone)
 - Match-on-Card – Responsible for the biometric verification of the finger tips

Applications

IAS

EMV-CAP

Match-On-Card

Citizen Data

Biometric Template of Fingertip

Photo

Adress

Identification data of the Citizen
(the same as the visible data on the card)

Area for personal use of the Citizen

Digital Certificate for Signature

Digital Certificate for Authentication

Legend:

PIN Protection

Public Access

Not Accessible



7. Future of eID

- **What is expected of the eID in the future?**

Catalyst for the complete availability of e-services to the citizen and enterprises:

Eg. in the near futur:

- Change of address
- Medical Doctor Appointment scheduling
- Bank account subscription
- Enterprise creation
- Apply for the University

7. Future of eID

- What is expected from the Porvoo Group in the future? (Cooperation with groups, permanent workinggroups within Porvoo Group etc.)
 - Cooperation with Interoperability Groups
 - Cooperation in Pan-European public services

8. More information

- **Web-pages on eID issues:**
www.cartaodocidadao.pt
www.ucma.gov.pt
www.umic.pt
- **email: anabela.pedroso@umic.pt**

Thank You!

Next Porvoo Meeting

Portugal
City of Coimbra
Spring 2007



**Coimbra, capital of portuguese knowledge.
3th ancient University in
Europe**



European Electronic Identity Practices

Country Update of Portugal

Speaker: Anabela Pedroso

anabela.pedroso@umic.pt

Date: 3 November 2006