

Spain's strategy on eID

Miguel Álvarez Rodríguez

Ministry of Public Administration of Spain

Current national scenario on eID

- ❖ PKI digital certificate is the most common solution for eID, as well as for digital signatures
- ❖ Lively market for CAs: 12 recognised CSPs by the Ministry of Industry as QC issuers
- ❖ Important uptake in the usage of QC in recent years: more than 7 million QC already issued
- ❖ Since 2006: Issuing of a National eID smart card
- ❖ Killer application since 2000 is the Tax declaration. Early return of payments if submitted over the internet (10 days)

An insight to accredited CSP in the country

❖ Public CAs

❖ Royal Mint: More than 2M certificates issued



❖ Police Directorate: National eID card: More than 4M cards issued and expected to reach the whole population over the next few years

❖ Regional PKIs: Set-up by the Governments of Catalonia, the Basque Country and Valencia

❖ Issuance fee is mostly free for the holder



Autoritat de Certificació de la Comunitat Valenciana



Agència Catalana de Certificació

❖ Private CAs



❖ Mainly focused on Professional Bodies: Lawyers, Chambers of Commerce, Public Notaries, Enterprise Certificates, Civil Servant Bodies...

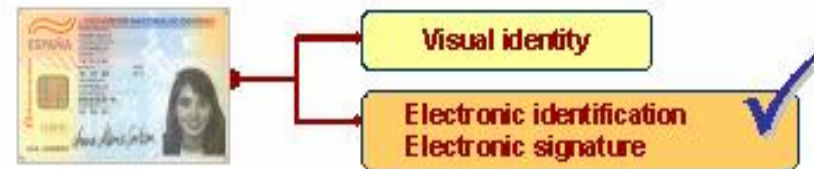


❖ The issuance cost is supported either by the holder of the certificate or by the Professional Body



The national eID card. The main PKI in the country

- National eID (DNle) is the way forward from the traditional paper-based National Identity Card.
- Universal and mandatory Spanish identification card since 1937 and Schengen Territory Travel Document. There is no social rejection to its use
- 97% of the Spanish electronic records with personal data include the ID number of the DNI as the primary citizen identifier.
- Two digital certificates inside the chip:
 - ✓ One for authentication
 - ✓ One for electronic signature
- The roll-out phase has recently finished and reached more than 240 Police offices. In fact, 500K cards monthly issued in the country



The national eID card. A SSCD

- The card has been evaluated following CC standards and accredited as CWA 14169 compliant by the National Certification Authority. “DNle exceeds CWA 14169, EAL4+, as required by EU for SSCD”
- The Certification Authority is the Police Directorate, dependant on the Ministry of Interior Affairs
- The Registration Authorities and issuing points are the Police Stations around the country. Real-time issuing service: Less than 15 minutes to generate the certificates and the printing of the card at the RA (decentralised model)

- Expected more that 6 million cards to have been issued by the end of the year.
- 12 million available eID cards next year..... By 2014 the eID card will have reached the whole population over 14 years old



Editor's Choice 2007

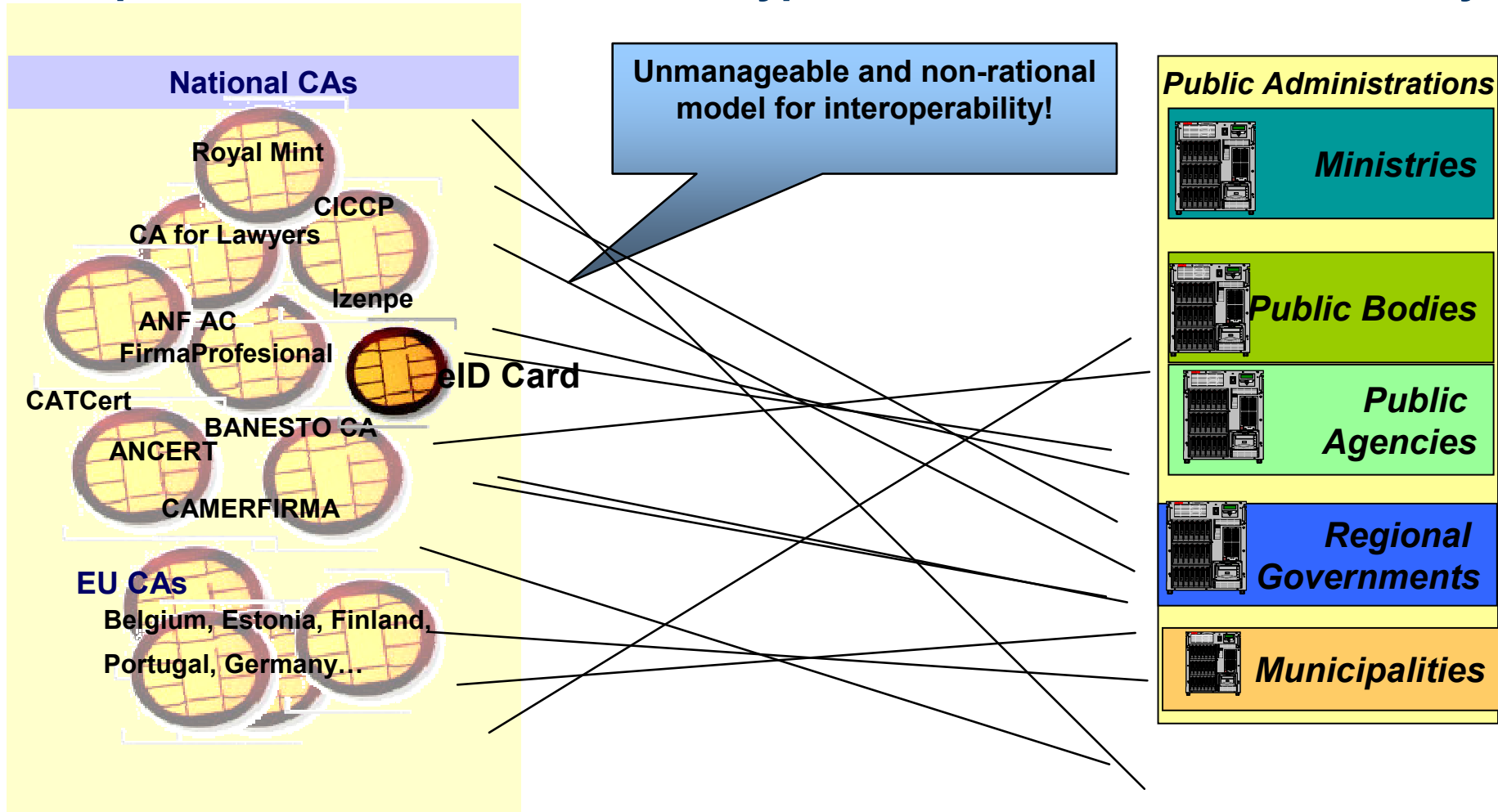


Best Practice Label 2009



The challenge: multiple scenario for PKI infrastructures

As a summary, important uptake of QC in Spain. This leads to a complex scenario of more than 70 types of QC available in the country



The challenge: technicalities.

■ Technical challenges

- Accept certificates from many CAs
- Install and maintain software for
 - validation of the authenticity and integrity of the certificate
 - interpretation of the content of the certificate
 - verification of digital signatures (crypto verification)

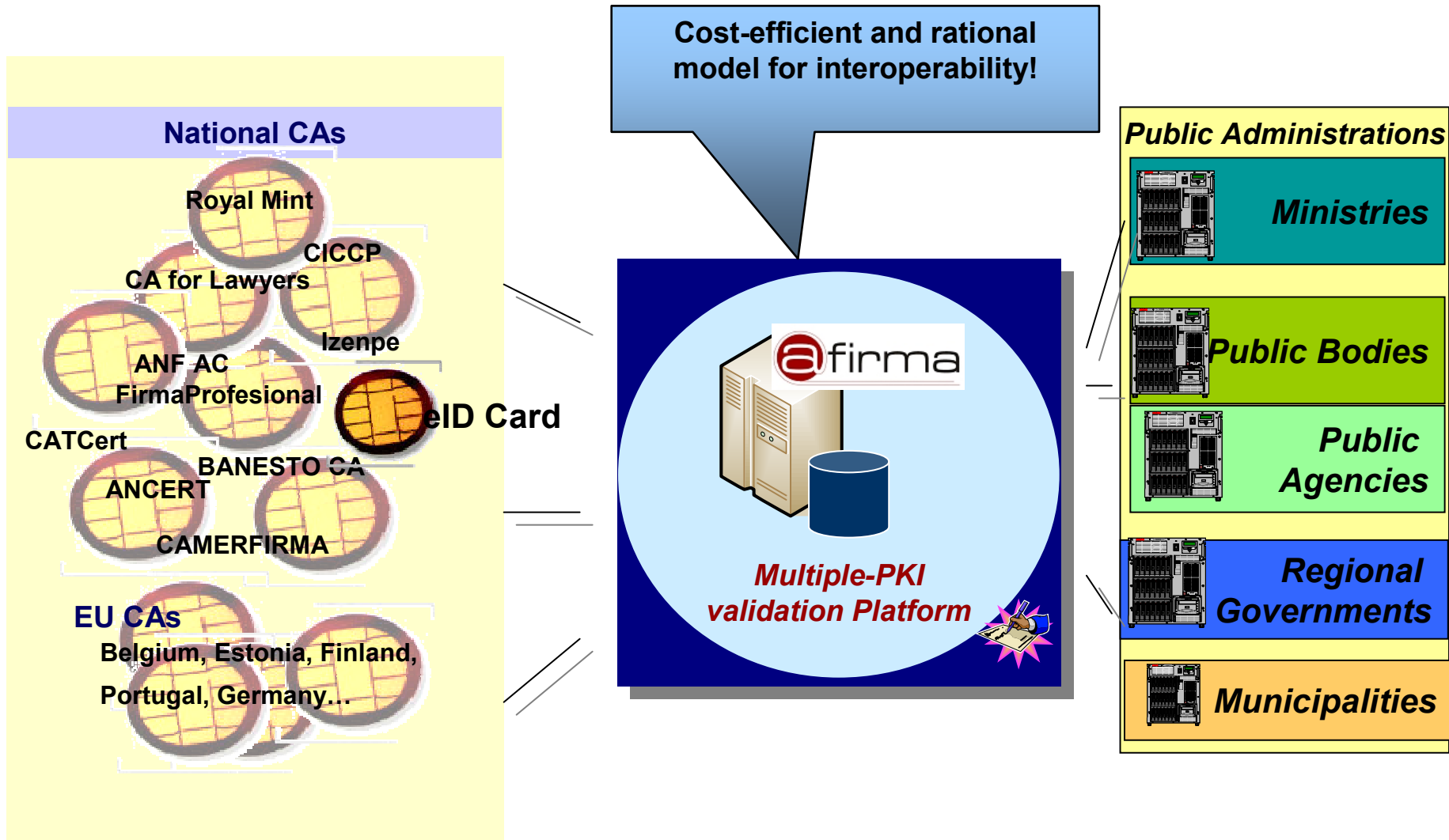
■ The technical complexity increases as the number of CAs increases

■ The number of integration software components needed to process the certificates increases accordingly

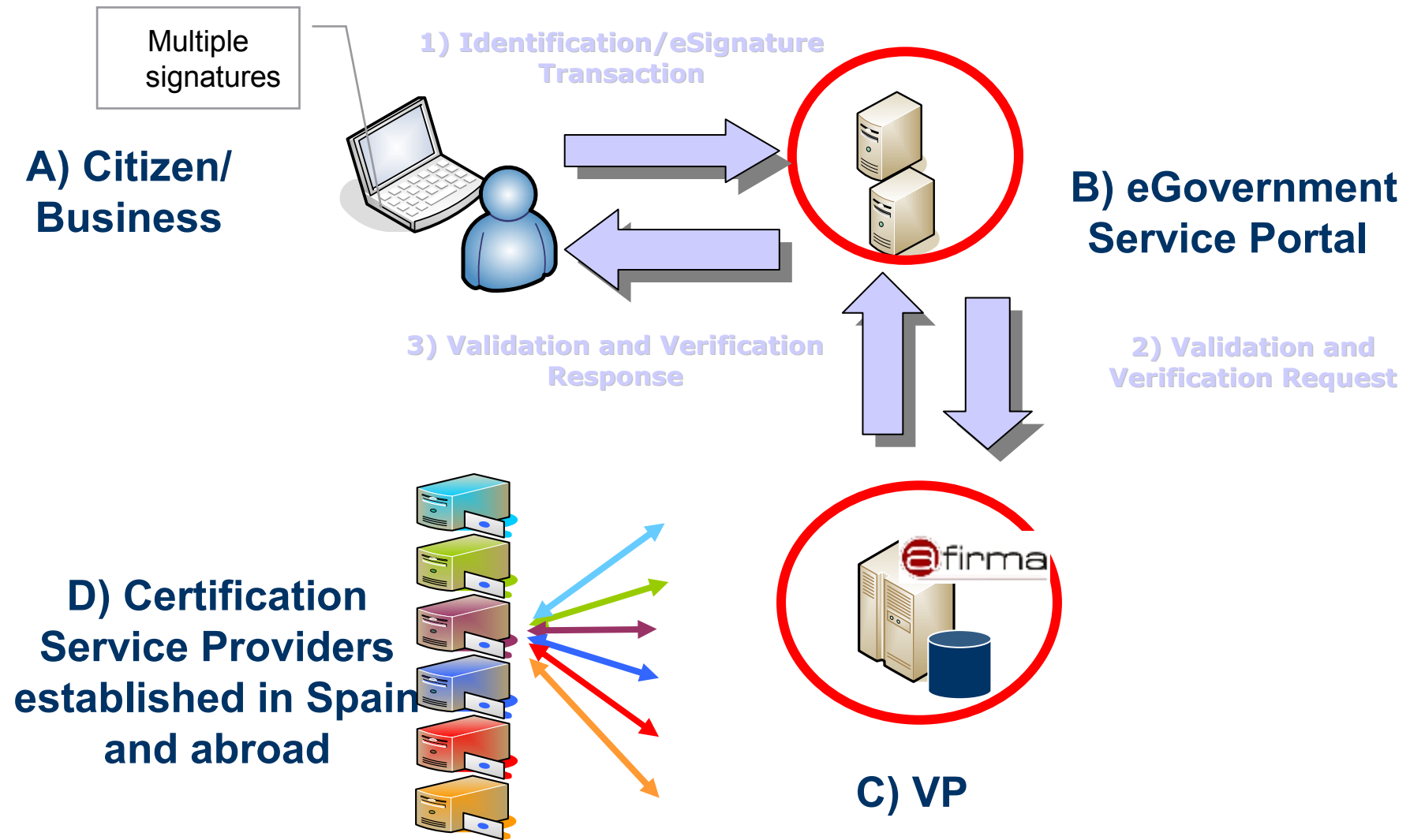
4. Launch of the national Multiple-PKI Validation in goals

- Since eID and digital signatures are key enablers to establish secure eGOV services, the aim was to create a Broker of CAS or Validation Platform (VP) that allows eGovernment Applications to verify the status of all the qualified certificates and eSignatures created in the country
- The Validation Platform is the core element to facilitate among Public Administrations the use of the same digital signature formats and higher levels of trust for eID: Interoperability of different PKI solutions
- The connection to the service provides immediate eID and eSignature Features to eGovernment Portals for all the Qualified Certificates issued in the country (Multiple-PKI Platform)

The national Multiple-PKI Validation Platform: An essential element to develop interoperability on eID and QS



The national Multiple-PKI Validation Platform: interconnection scheme



Services offered by the VP (Sept 2008)

- 1. Certificate validation services for all the QC issued in Spain: Use of OCSP and WS protocols. Integrity /quality, validity and revocation checking of the whole CA chain and the issued QC
- If required, most relevant fields of the QC are extracted in order to compose an easily interpretable XML scheme that is sent back along with the validation response
- 2. Signature verification service: Verification of PKI-based digital signatures
 - Acceptance of various European standards: CMS, PKCS#7, XADES- BES, XADES-T, CADES-BES, CADES-T, ODF, PDF
- 3. Client component (applet) for signature creation

Main eGOV application using the VP services

- **The Tax Agency and Social Security Department run their own VP due to the large amount of monthly transactions performed (millions of QC validations/ QS verification)**
- **The vast majority of Public Sector eGOV services in the country are users of the MPA VP**
- **Ranking of main users (in terms of the highest number of transactions performed against the VP):**
 - **On-line request service for unemployment benefits**
 - **On-line verification service of personal address and checking of driving offence points**
 - **Announcement of movement service**
 - **On-line purchase of treasury bonds**

Lessons learned from the VP

- 1) The VP is a cost-efficient and time-saving service providing eID and electronic signature features in a simple way. In fact, it prevents Public Bodies from investing in validation SW modules and other communications-related infrastructures needed to interconnect eGOV systems to every qualified CA verification service
- 2) The uptake in the use of digital certificates in the public sector is encouraging the private sector to provide secure services based on the national eID card (i.e.: 12 banking entities already incorporating the eID card at on-line banking services
- 3) Spain is also taking part in the Large Scale Pilots on eIDM within the CIP initiative (STORK Consortium) and will integrate this national infrastructure to the future interoperability framework for eID to accept other EU eIDs

More Information

- On the national eID card:
 - <http://www.dnielectronico.es/>
- On the Multiple PKI Validation Platform
 - <http://www.csi.map.es/csi/pg5a12.htm>
 - http://www.dnielectronico.es/seccion_aapp/platform.html
 - <http://www.epractice.eu/cases/1984>



Thank you!

miguel.alvarez@map.es

Dirección para el Impulso de la Administración Electrónica

Ministry of Public Administration of Spain

<http://www.map.es/>

