



*Conference on
Cryptography and Digital
Content Security*

Barcelona, May 16th 2007



The New Spanish Electronic Identity Card: DNI-e

Javier Espinosa-García

Senior Consultant – IT Security

PRICEWATERHOUSECOOPERS 

**connectedthinking*

*contents

Introduction

Goals

Physical Support

Logical Support

Introduction

- **Information Technologies** are growing inside common society, and it means that new user's requests frequently appear.
- Some of those aims are to give the necessary resources and ensure that these **guarantee people privacy, freedom and rights** within a democratic framework.
- Personal electronic identification is a challenge that the Spanish Government faced up to by means of a new identification mechanism based on the traditional **Spanish Identity Card (Documento Nacional de Identidad: DNI)**.

Introduction (II)

- The **DNI** is a document issued by the Spanish Government (Spanish Police, DGP, to be precise) that **authenticates its holder** as genuine and justifies the holder's identity.
- Since it was developed (more than 50 years ago), the DNI has been an **essential document** to officially justify, per se and inside Spain (and in the European Union), holder's identity.
- Furthermore, the DNI guarantee the personal details showed on the card and that its holder has the **Spanish citizenship**.

Goals

1. To provide a **physical and electronic** holder's **identification mechanism**.
2. To make **electronic signature** possible by identification, authentication and digital signature protocols.
3. To promote citizens' confidence in the Information Society and new digital context by providing a suitable mechanism that ensures citizens' identity, privacy and basic rights.
4. To **cooperate** with different European projects related to digital identity.
5. To keep its characteristics and functions as a **travel document**.

Physical Support

- The DNI-e card is a **polycarbonate support** whose durability has been estimated for at least 10 years.
- The size of this card is **similar to any credit card** or smart card we can find today.



Physical Support: Security Level 1

Level 1 is made up of elements that can be observed with the **naked eye**:

- Hologram or kinegram protected by a 100 nm. overlay.
- Optically variable inks.
- Changing laser Image.
- Touch detectable letters.
- Embossed surface structures



Physical Support: Security Level 2

Level 2 is characterized by marks that are just noticeable with **electronic and mechanical**:

- Security background: guilloches graphics that can have logotypes.
- Ultraviolet or infrared visible inks and fluorescent inks.
- Subject's picture is laser recorded at card background and counterfeit protected.



Physical Support: Security Level 3

Level 3 consists of elements that only can be detected at **laboratory**:

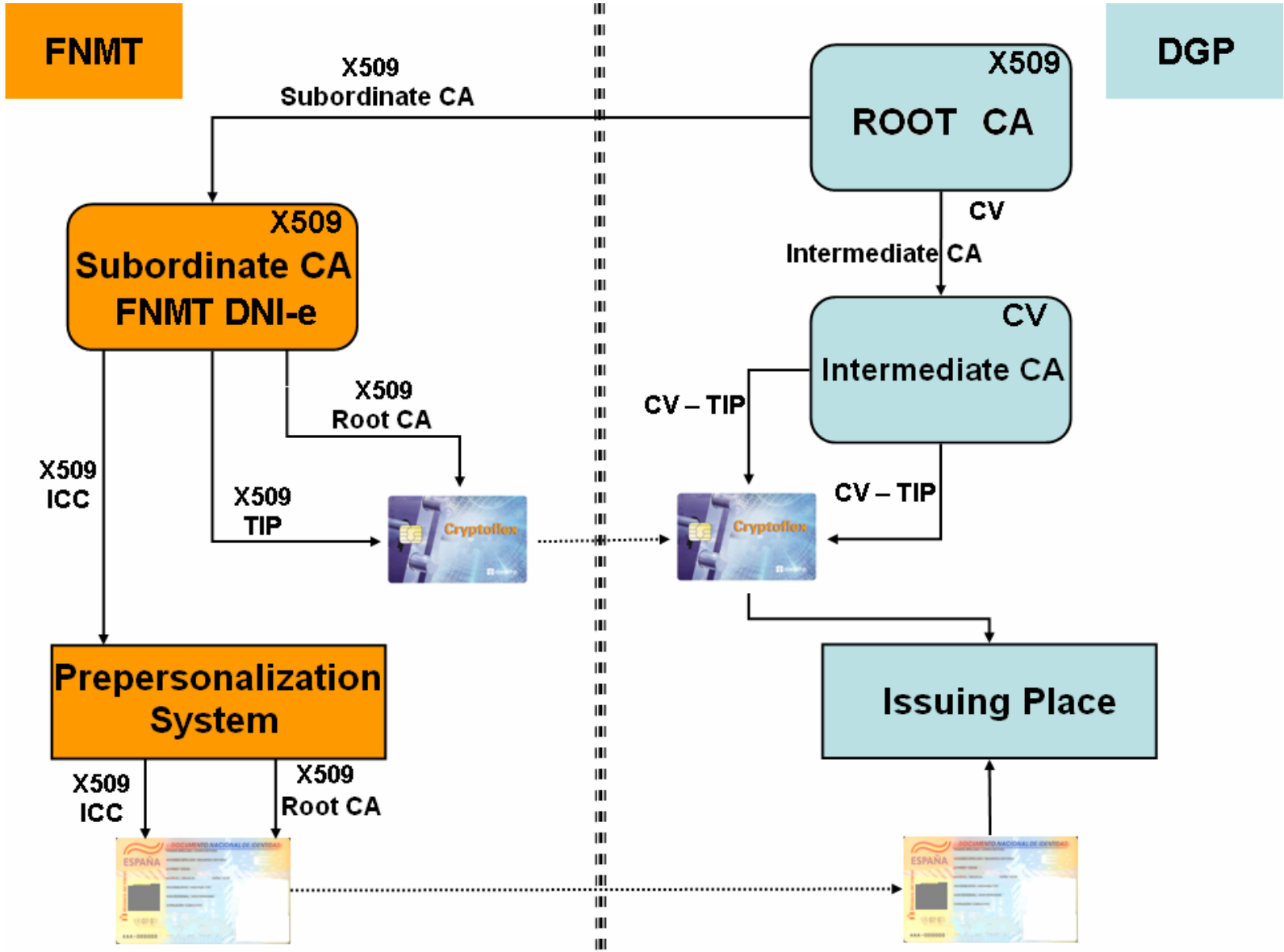
- Personal citizen details.
- Digitalized citizen's photo.
- Digitalized citizen's handmade signature.
- Fingerprint template.
- Cryptographic data.
- Biometric data.
- A “match on card” application.
- A cryptographic processor that ensures private key will not be exported from the card.
- An authentication certificate, X509v3.
- A signature (non repudiation) certificate, X509v3.
- The issuer CA certificate.

Physical Support: Chip

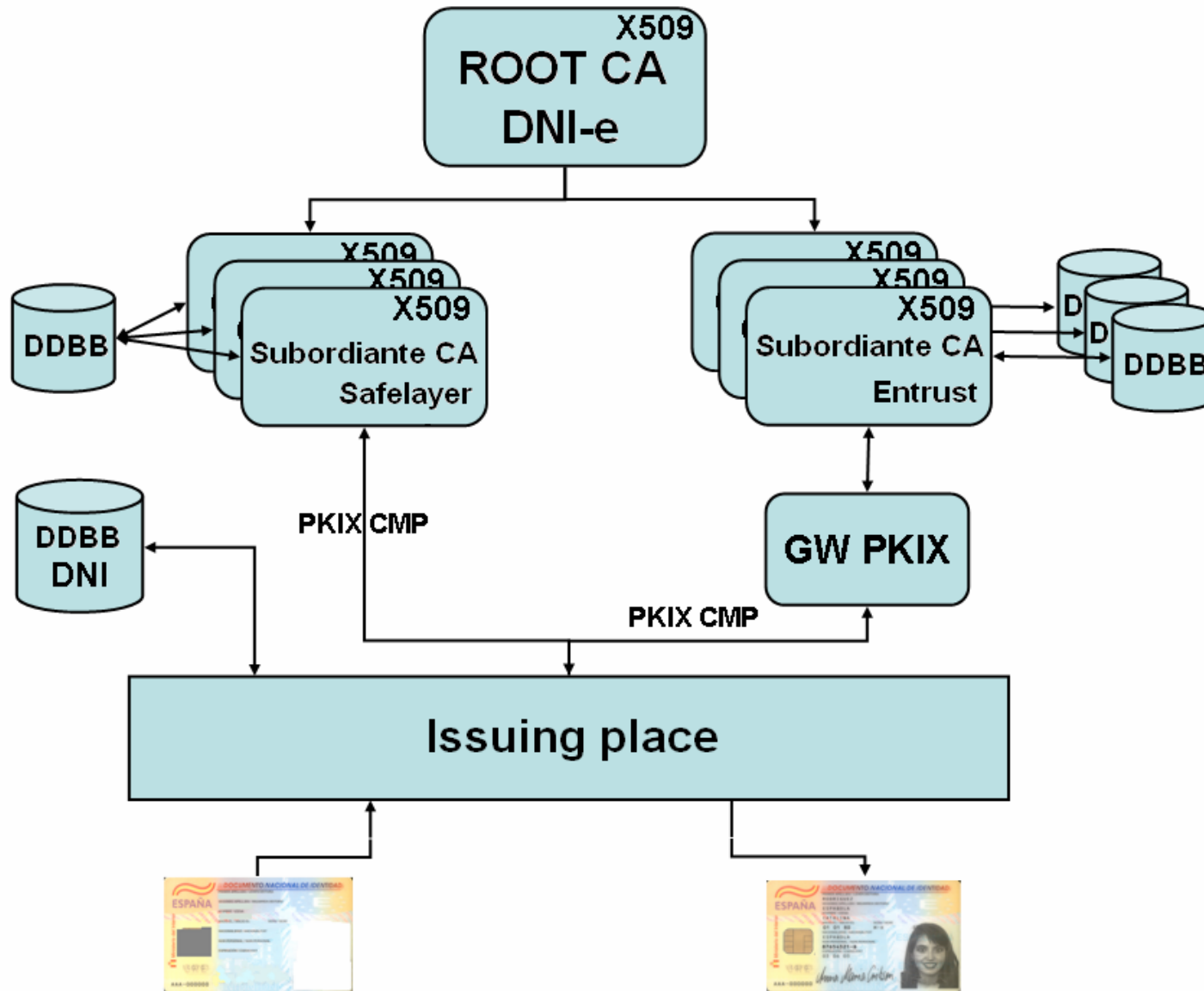
Areas:

1. The first one contains **citizen's certificates**, and, if its holder wants, it can be accessed via PKCS#11.
2. The second area contains **citizen's fingerprint**, and it can be accessed only by authorized Spanish Security Forces and Corps personnel.
3. The last area has all **personal details**, and it can be accessed only by authorized Spanish Security Forces and Corps personnel too.

Logical Support: Pre-personalization



Logical Support: Personalization



PRICEWATERHOUSECOOPERS 

ΣΥΜΒΟΥΛΕΥΤΙΚΗ ΕΠΙΧΕΙΡΗΣΙΑ