



Belgian eID Cards Introduction

Danny De Cock

Danny.DeCock@esat.kuleuven.be

Katholieke Universiteit Leuven/Dept. Elektrotechniek (ESAT)

Computer Security and Industrial Cryptography (COSIC)

Kasteelpark Arenberg 10

B-3001 Heverlee

Belgium

Overview of eID Card Types

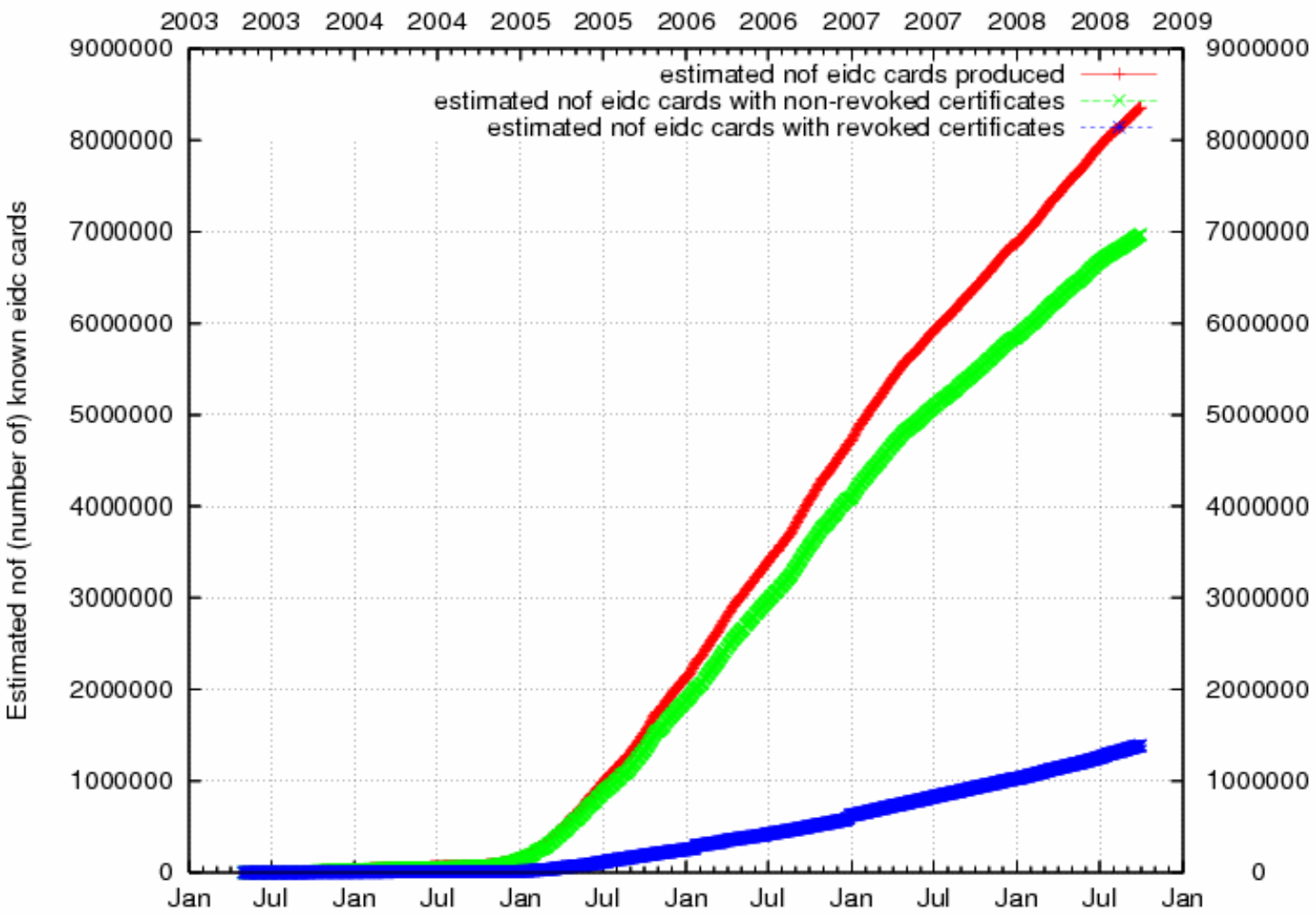
Belgian Citizens

1. Belgian kids:
 - Kids card with two revoked certificates, age < 6
 - Kids card with valid authentication & revoked non-repudiation certificate, $6 \leq \text{age} < 12$
2. Belgian youngster:
 - eID card with valid authentication & revoked non-repudiation certificate, $12 \leq \text{age} < 18$
3. Belgian adults:
 - eID card with two valid certificates, $18 \leq \text{age}$

Aliens ☺

4. Foreign kids:
 - Kids card with two revoked certificates, age < 6
 - Kids card with valid authentication & revoked non-repudiation certificate, $6 \leq \text{age} < 12$
5. Foreign youngster:
 - eID card with valid authentication & revoked non-repudiation certificate, $12 \leq \text{age} < 18$
6. Foreign adults:
 - eID card with two valid certificates, $18 \leq \text{age}$

Belgium issuing eID cards



- 1 Million cards produced and issued in 6 months
- All 589 municipalities issue eID cards

Graph generation: Mon Oct 13 09:53:40 2008. Source: <http://godot.be/eidgraphs>



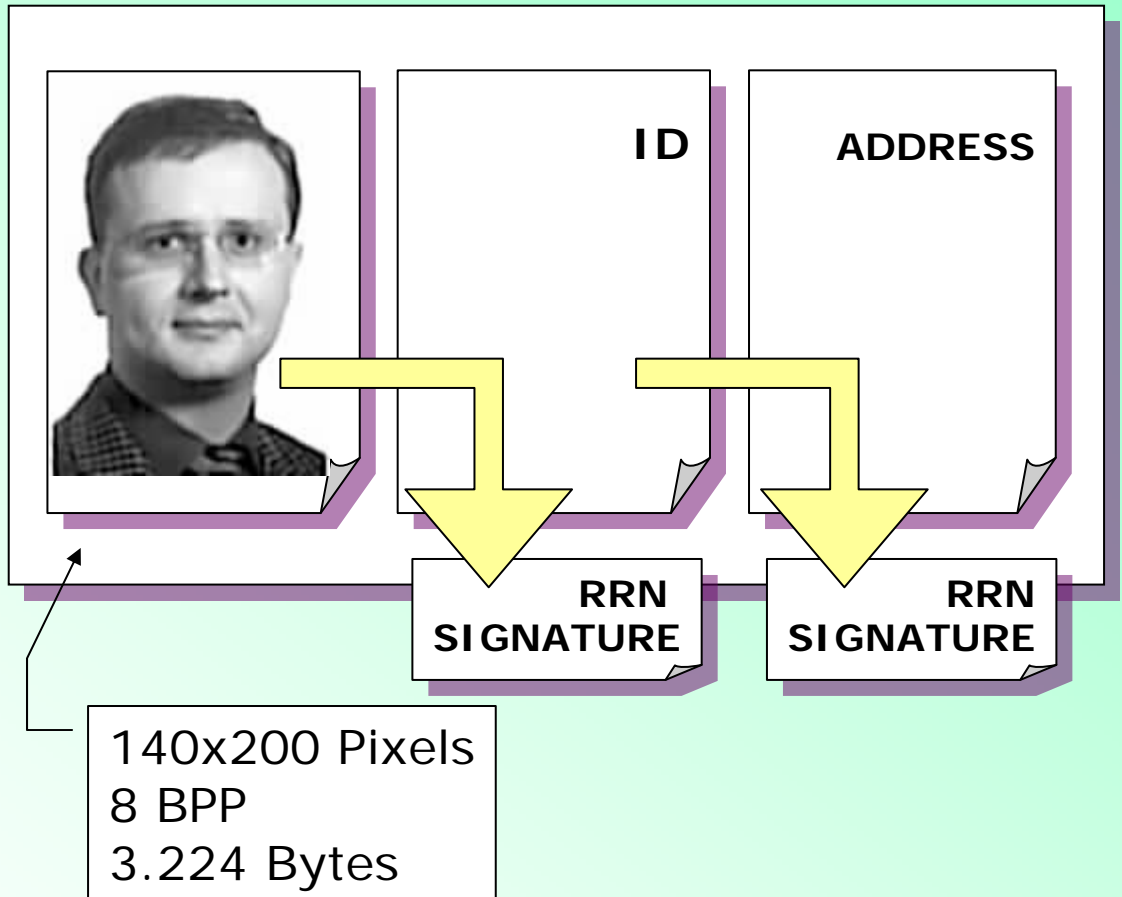
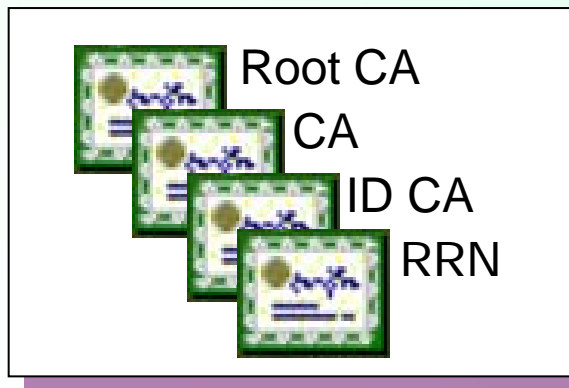
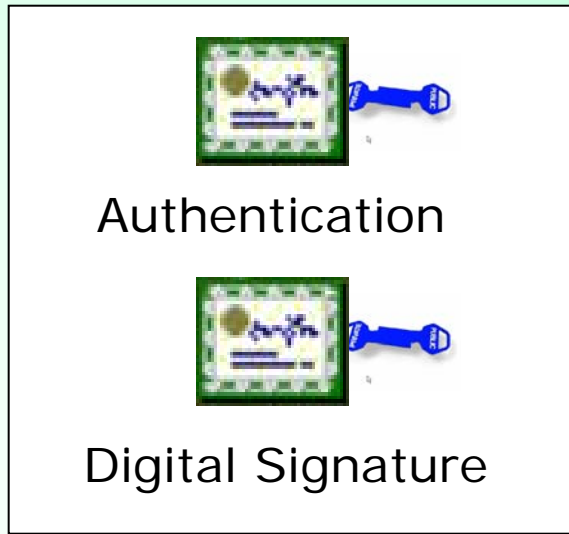
eID Card = 4 Functions

- Non-electronic
 1. Visible identification
- Electronic
 2. Digital identification
 - Data capture
 3. Prove your identity
 - Authentication
 4. Digitally *sign* information
 - Non-repudiation signature
- Inherent to ID card
 - Reason of its existence
- Inherent to eID card
 - Privacy-risky
 - User consent?
 - (Trans)actional activities
 - Consequence of PKI
 - Long-term relations
 - Mandatory

eID Card Content

PKI

Citizen Identity Data



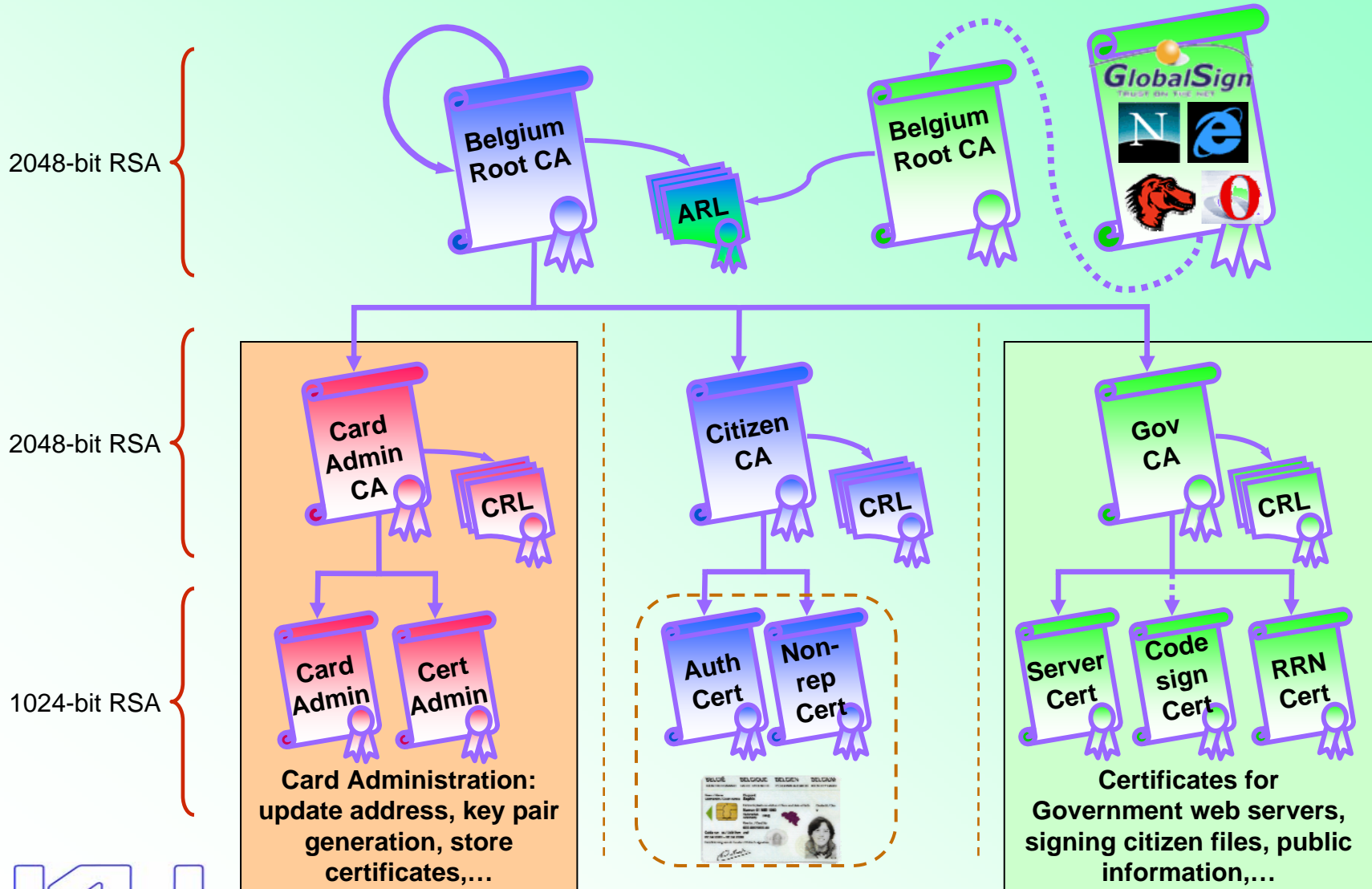
RRN = National Register

Signing Keys & Certificates

- 2 key pairs for the citizen:
 - Citizen-authentication
 - X.509v3 **authentication certificate**
 - Advanced electronic (non-repudiation) signature
 - X.509v3 **qualified certificate**
 - Can be used to produce digital signatures equivalent to handwritten signatures, cfr. European Directive 1999/93/EC
- 1 key pair for the card:
 - eID card authentication (basic key pair)
 - **No corresponding certificate**: RRN (**Rijksregister/Registre National**) knows which public key corresponds to which eID card



eID Certificates Hierarchy



eGovernment's Basic Concepts

- Federated architecture
 - Each sector operates autonomously
 - Interfaces with other sectors through bus system
- Built around authentic sources
 - Master copy of data is available at exactly one repository
 - Master copy = authoritative source
- Maximal reuse of information
 - No data replication
 - Administrations are forbidden to re-request data already available in an authentic source
- Integrated system for user and access management
 - Citizens, professionals and companies are equipped with necessary credentials
 - Each actor manages its own access policies

Service Oriented eGovernment Services

