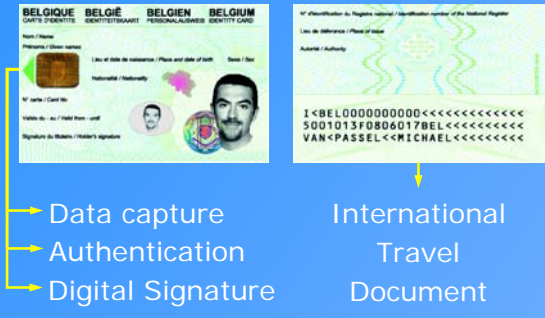
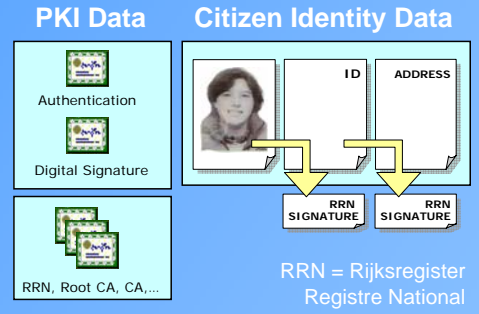


Belgian Electronic Identity Cards

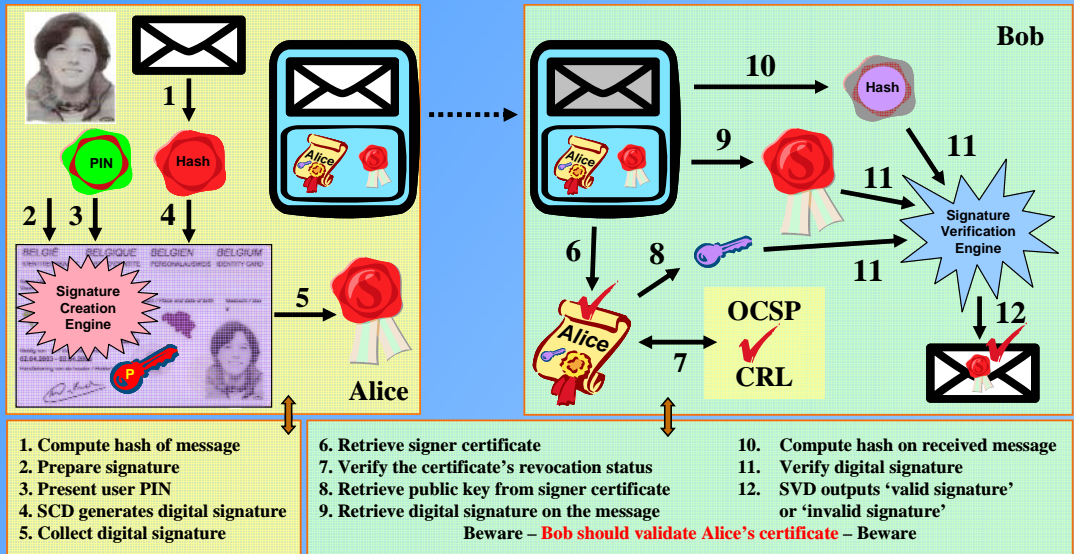
eID Card Functions



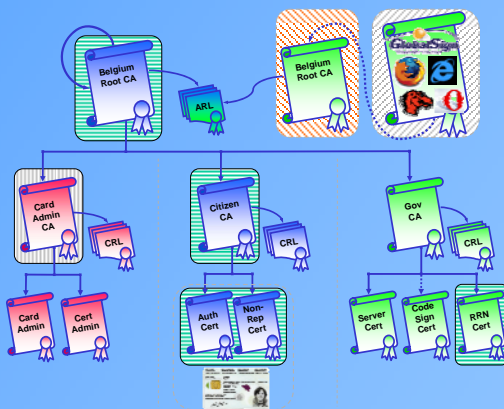
Chip Content



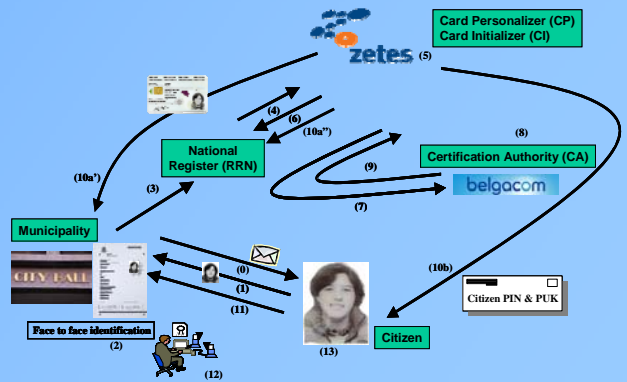
Signature Generation/Verification



Certificate Hierarchy



Issuing Process



Why Introducing an eID Card?

- **Every Belgian citizen gets a tool to**
 - Authenticate him/herself via email, SSL/TLS,...
 - Create digital signatures equivalent with handwritten signatures, e.g., to sign contracts electronically
- **Benefits**
 - Nation-wide PKI reduces need to deploy closed user group PKIs
 - Avoids updating legislation referring to handwritten signatures
 - Improved security and confidence in remote transactions
 - Simplification of administrative tasks through
 - Faster data capture
 - Home-government: consult your own files with the government, fill out tax declarations,...
 - Digital signatures protect electronic content
 - Certificates link digital signatures to citizens
 - The new EID card is smaller than the previous ID card
 - Address changes do not necessitate a issuing a new eID card
- **Risks**
 - Privacy
 - Market distortion
 - Interoperability at European level



Quick Summary Belgian eID

- **Initiated in 1999**
 - Massive rollout started end of October 2004
 - Currently about 1.4 million cards produced
 - About 1 million eID cards activated
- **588 of the 589 municipalities** already activate eID cards
- **eID card can be used to**
 - Authenticate the cardholder
 - Create digital (non-repudiation) signatures
 - Capture citizen data electronically
 - Visually identify the citizen
- Chip contains **administrative data** (photo, address, cardholder identity, national number,...)
- **Card is valid for 5 years after production**
- All Belgian citizens (+12 years) will have obtained an eID card by **end of 2009**

Who Gets an eID Card?

- **A new eID card is issued to**
 - New inhabitants
 - Every youngster at the age of 12
 - People changing from one address to another in the local municipality
 - Replace a lost, stolen, damaged or expired (e)ID card
 - Adjust the citizen's picture
 - Every citizen who asks to replace his/her old ID card
 - Every citizen who changes his/her name, gender,...
- **Target groups**
 - Medical doctors, lawyers, eID software companies,...

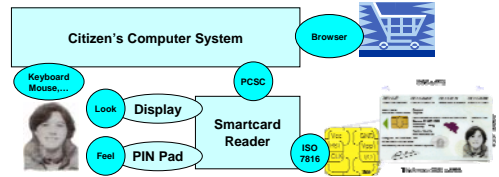
The Belgian eID Card...

- Uses **On-board key pair generation**
 - Private keys cannot leave the eID card
 - Key pair generation is activated during the initialization of the eID card
- Uses **JavaCard technology**
- Can be used using software/middleware – free of charge – provided the Government
- Can only be **managed by the Belgian government**
 - Citizen identity/address data is read/write for the National Registry
 - eID card refuses update attempts from other parties than the government

References...

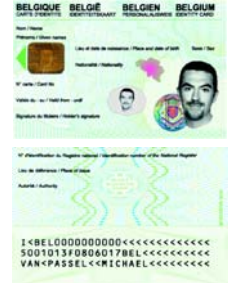
- <http://www.fedict.be>
- <http://www.riksregister.fgov.be>
- <http://eid.belgium.be>
- <http://www.eid-shop.be>
- <http://godot.be/eidforum>

Typical Smartcard Architecture



Visual Identity Information

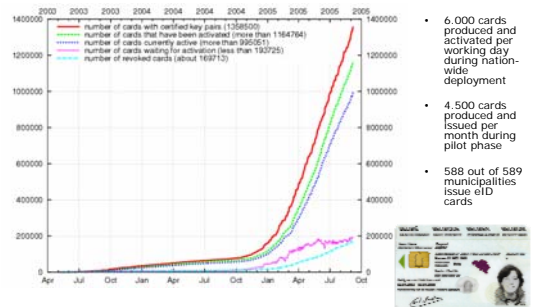
- Front:**
- Name
 - First two names
 - First letter of 3rd name
 - Title
 - Nationality
 - Birth place and date
 - Gender
 - Card number
 - Photo of the holder
 - Begin and end validity dates of the card
 - Hand written signature of the holder
- Back:**
- Place of delivery of the card
 - National Register identification number
 - Hand written signature of the civil servant
 - Main residence of the holder (cards produced before 1/1/2004)
 - ICAO (cards produced since 1/1/2005)



PKI Content – 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

Belgium Issuing eID Cards



Citizen Certificate Details

Citizen Qualified certificate (~1000 bytes)	Citizen Authentication certificate (~980 bytes)
Version: 3 (0x2) Serial Number: 10 00 00 00 00 00 8d 8a fa 33 d3 08 f1 7a 35 b2 Signature Algorithm: sha1WithRSAEncryption (1024 bit) Issuer: O=BE, CN=Citizen CE Not valid before: Nov 12 22:41:00 2003 GMT Not valid after: Nov 12 22:41:00 2008 GMT Subject: CN=BE, CN=Sophie Dupont (Signature), SN=Dupont, GN=Sophie, Nickname/serialNumber=40021404665 Subject Public Key Info: RSA Public Key: (Modulus (1024 bit), 4b: e5: 7e: de: ... 86: 17, Exponent: 65537 (0x10001)) X509v3 extensions: Certificate Policies: Policy: 2.5.6.1.1.1.2.1 Key Usage: critical, Non-Repudiation Authority Key Identifier: (D1:13: ... FF:AF:10) CRL Distribution Points: URI: http://crl.eid.belgium.be/oid0002.crl Network Cert Type: 0x00 Authority Information Access: CA Issuers: URI: http://crl.eid.belgium.be/oid0002.crl OCSP: URI: http://ocsp.eid.belgium.be OCSP: URI: http://ocsp.eid.belgium.be Signature: [74:ac:10: ... c0:91]	Version: 3 (0x2) Serial Number: 10 00 00 00 00 00 0a 5d 9a 91 b1 21: a5 00: a2: 7a Signature Algorithm: sha1WithRSAEncryption (1024 bit) Issuer: O=BE, CN=Citizen CE Not valid before: Nov 12 22:40:52 2003 GMT Not valid after: Nov 12 22:40:52 2008 GMT Subject: CN=BE, CN=Sophie Dupont (Authentication), SN=Dupont, GN=Sophie, Nickname/serialNumber=40021404665 Subject Public Key Info: RSA Public Key: (Modulus (1024 bit), cf: ca: 7a: 77: ... 5c: c5, Exponent: 65537 (0x10001)) X509v3 extensions: Certificate Policies: Policy: 2.5.6.1.1.1.2.2 Key Usage: critical, Digital Signature Authority Key Identifier: (D1:13: ... FF:AF:10) CRL Distribution Points: URI: http://crl.eid.belgium.be/oid0002.crl Network Cert Type: 0x00 Authority Information Access: CA Issuers: URI: http://crl.eid.belgium.be/oid0002.crl OCSP: URI: http://ocsp.eid.belgium.be Signature: [10:ac:04: ... e9:04]