Belgian eID Card
Detailed Overview

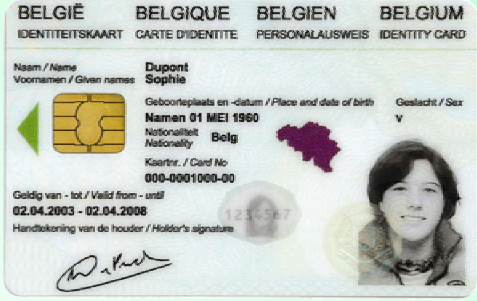
Danny De Cock
Danny.DeCock@esat.kuleuven.ac.be
Katholieke Universiteit Leuven/Dept. Elektrotechniek (ESAT)
Computer Security and Industrial Cryptography (COSIC)
Kasteelpark Arenberg 10
B-3001 Heverlee
Belgium

Why Introducing an eID card?

- **Every Belgian citizen gets a tool to**
  - Authenticate him/herself via email, SSL,…
  - 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

In short – What is an eID card?

- **The digital version of the previous ID card**
- **Bank card-sized plastic card depicts the citizen’s**
  - Photo, Full name, Gender, Handwritten signature, Nationality, Place and Date of birth, Card and National Number,…
- **The chip on the eID card contains the citizen’s**
  - Identity data and address
  - Identity and signing certificates (and key pairs),…
- **The chip can be used to**
  - Authenticate information (e.g., for invoices)
  - Generate digital signatures equivalent to handwritten signatures (e.g., for contracts)
- **The card is valid for 5 years**



BELGIË IDENTITEITSKAART
BELGIQUE CARTE D'IDENTITE
BELGIEN PERSONALAUSWEIS
BELGIUM IDENTITY CARD

Naam / Name: Dupont
Voornamen / Given names: Sophie

Geboorteplaats en -datum / Place and date of birth: Namen 01 MEI 1960
Geslacht / Sex: V
Nationaliteit / Nationality: Belg
Kaartnr. / Card No: 000-0001000-00

Geldig van - tot / Valid from - until: 02.04.2003 - 02.04.2008
Handtekening van de houder / Holder's signature

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
  - Produce a lost, stolen, damaged ID or eID card
  - Replace an expired non-eID 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,…
- **Specific groups who requested a priority:**
  - Medical doctors, lawyers, software companies,…

eID card issuing procedure

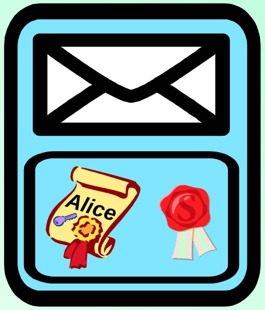
- The citizen receives a convocation letter or presents him/herself spontaneously to the municipality
  - He/she goes to the municipality to sign the eID request form (basisdocument)
    - The citizen brings his/her own picture and 12 euro to the municipality
  - The card manufacturer produces a new eID card an initializes it with all necessary information
  - After 2-3 weeks, the citizen receives a letter with his/her personal identification number (PIN) and card activation code (PUK1)
    - If the citizen receives this letter, the citizen can go and collect his/her eID card
  - The citizen brings his/her current ID card together with the letter with the citizen's PIN and PUK
  - The eID card is activated using the citizen's PUK1 and the government's PUK2
    - If the card is activated, the citizen generates his/her PIN to generate two test signatures: one identity and one qualified signature to prove the proper functioning of the eID card
  - The activation of an eID card takes about 15 minutes

What if …?

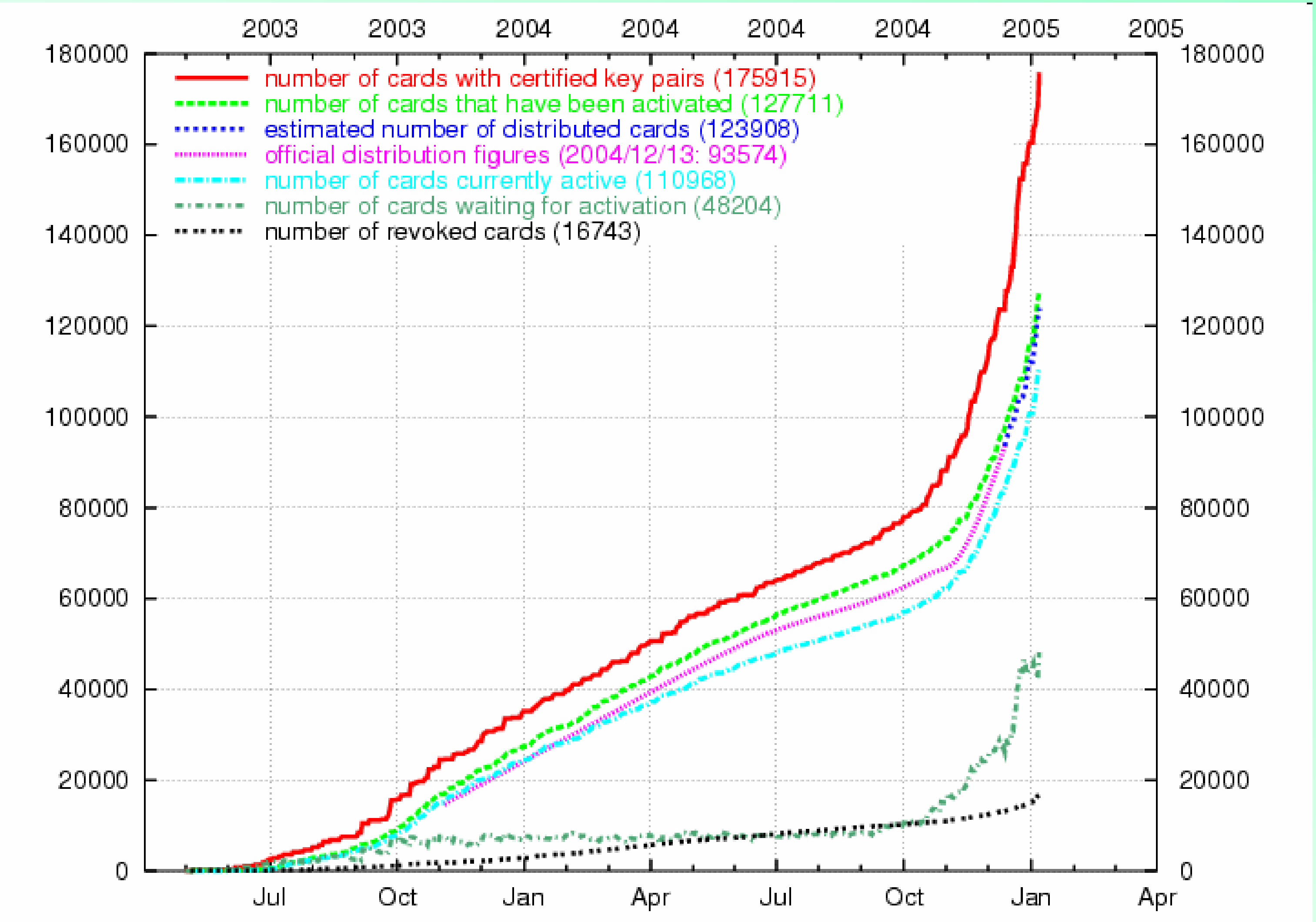
- Your eID card is lost, stolen,…
  - Declare the loss or theft immediately with the police or the municipality nearby
    - eID card stop: +32 (2) 210.21.16 or 210.21.17
  - To avoid any possible abuse of the eID card, the electronic functionalities of the eID card must be suspended
    - If the card is recovered within 7 days after the suspension, the eID card can be re-activated
    - If the card cannot be recovered within 7 days after the suspension, the card renewal procedure is started
      - The old card is revoked and invalidated forever
      - If the card is recovered after it has been revoked and invalidated, it must be returned to the municipality for immediate destruction

Example – How does it work?

- **Case study: Alice uses her eID card to generate a qualified signature on a file contract.doc with Bob**
  - Alice’s computer application asks her whether she wishes to digitally sign the document
  - If she approves, she inserts her eID card in the computer’s smartcard reader
  - She enters her PIN to authorize the generation of a qualified signature
  - Bob receives from Alice:
    - The document contract.doc
    - The digital signature
    - Alice’s qualified certificate



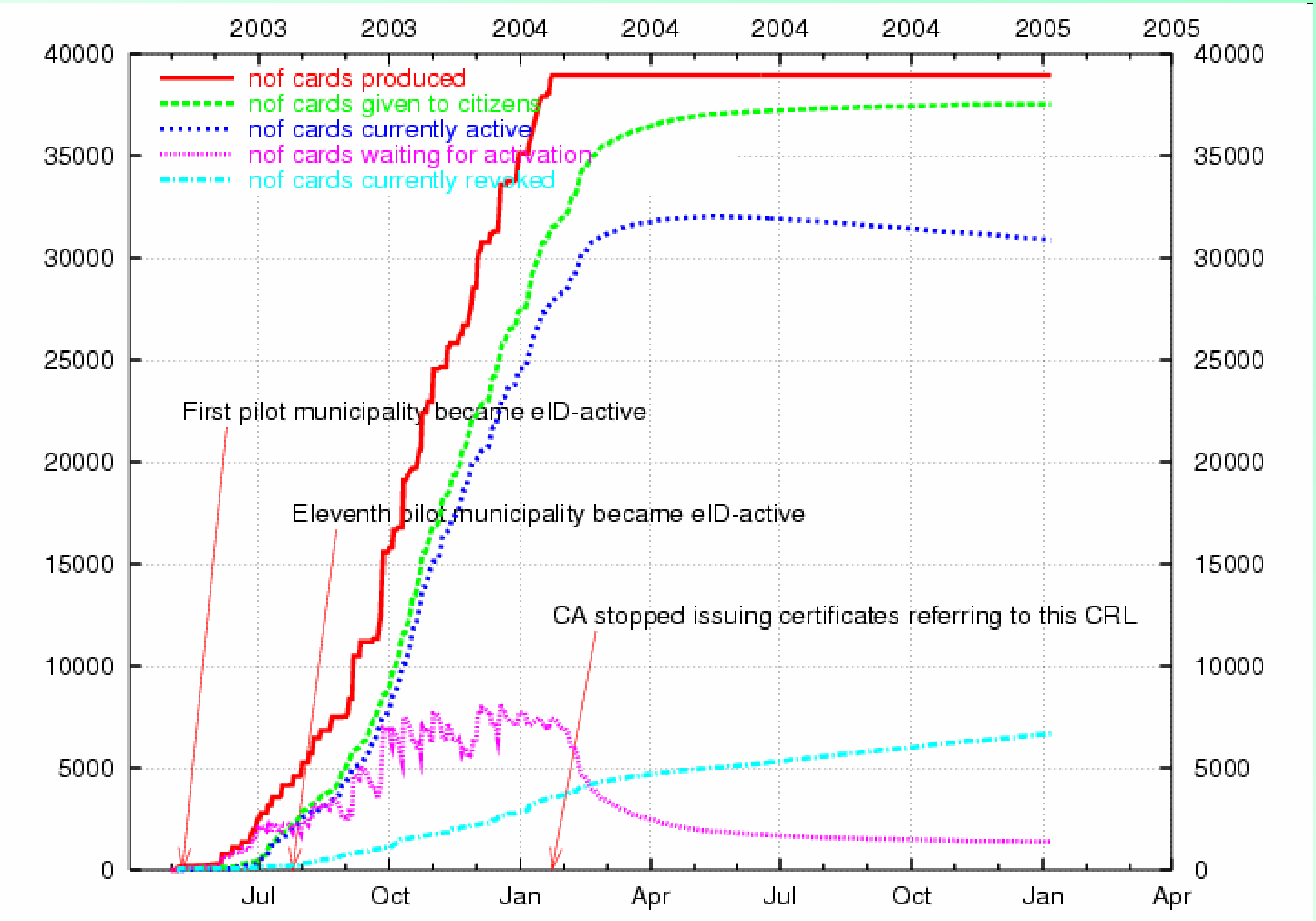
eID Card Distribution Status



- More than 1500 cards produced and activated per working day during nation-wide deployment
- 4500 cards produced and issued per month during pilot phase
- 10% of the pilot citizens do not want any eID functionality
- Already more than 75% of all 589 municipalities issue eID cards

Frequently updated graphs available at http://www.godot.be/site/EidCards/belpic/index.html

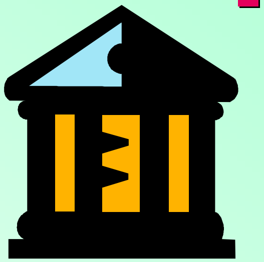
Typical evolution of an eID CRL



- CRLs follow the lifecycle of the eID cards they cover
- The CA stops issuing certificates referring to a particular CRL if it becomes too large
- The graph reflects the evolution of the eID cards following a CRL for which no new certificates are issues

Today’s eID Card Applications

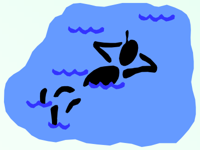
- eGovernment
  - Official document requests
    - Marital status, Birth certificate,…
  - Access to RRN database
  - Online voting



- eTax
  - Tax form declaration

- eJustice
  - Electronic submission of conclusions in court cases

- eAccess
  - Client authentication for web servers
  - Access control, e.g., container park, library, swimming pool,…



- eCommerce
  - Online opening of new account
  - Digital Rights Management
  - Qualified signature
    - Contract signing

Trust²

- eBanking
  - Online mortgage request
- eMail
  - Registered mail
  - Authenticated email

- eAdministration
  - Data capture
  - Car registration

WebDIV.be

TAX-on-web

K.U. LEUVEN

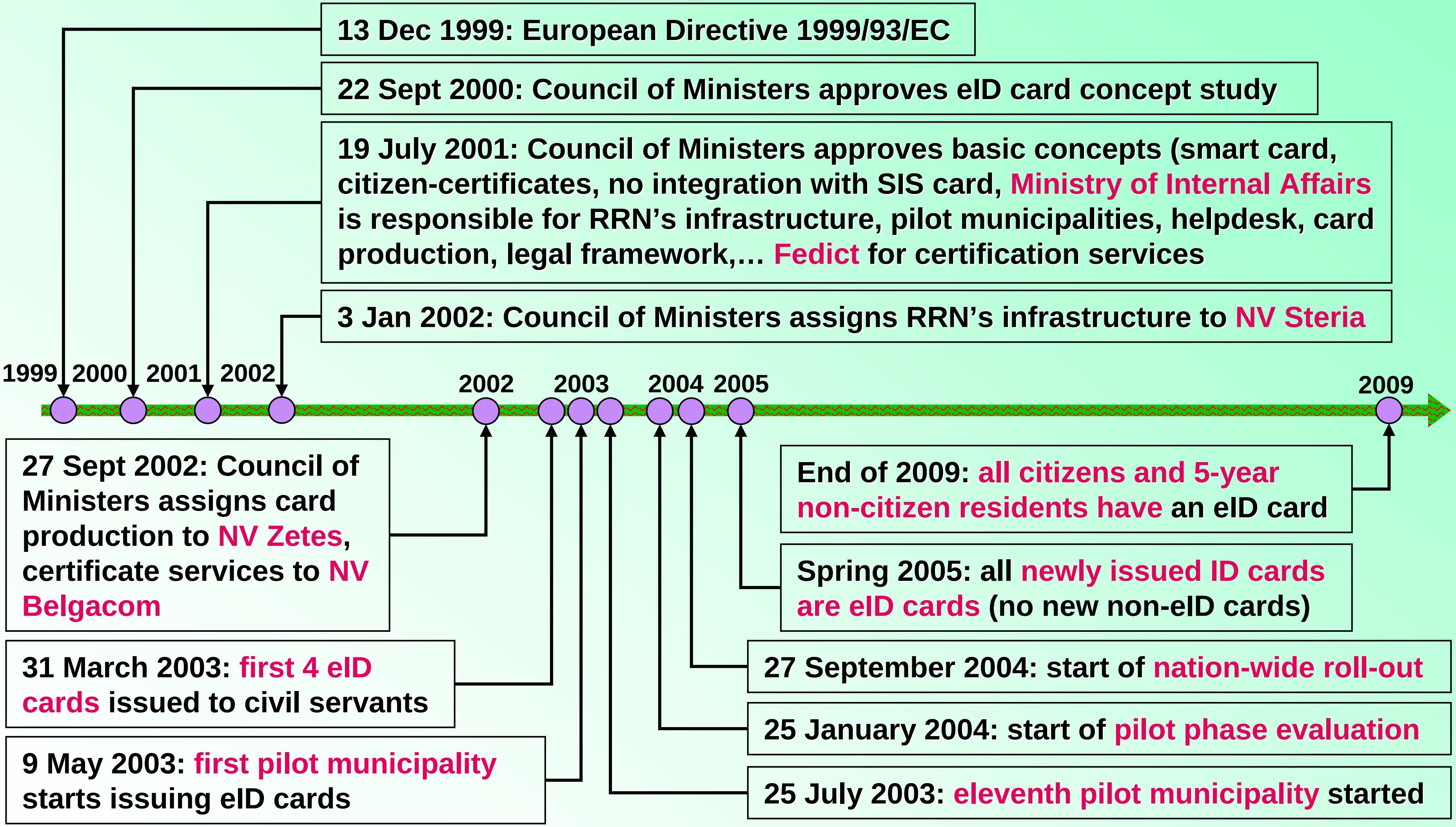
Good To Know (1/2)

- An eID card is **valid for 5 years**
- **Signing** functions of an eID card issued to **minors** (<18 years) is **not activated**
- Any citizen can ask to deactivate the authentication and signature functions
  - **Once deactivated, always deactivated**
- Professional groups can request an eID card, even before their local municipality has become eID-enabled
- 24/7 **helpdesk** is available
  - In case of loss, theft or destruction of an eID card
  - An eID card is first suspended before it is irreversibly revoked
  - Phone: 02/518.21.17 (Dutch), 02/518.21.16 (French)
  - Fax: 02/518.25.21
  - Email: helpdesk@rrn.fgov.be

Good To Know (2/2)

- All electronic signatures can be used as an alternative for a handwritten signature, given that one can prove that the signature corresponds to something which only the author of the content to be signed could create
- The qualified electronic signature is the only type of signature that will automatically be given the same legal value as a handwritten signature
    - A qualified signature is an advanced electronic signature based on a qualified certificate and produced by a secure signature creation device

Belgian eID Project Time line



13 Dec 1999: European Directive 1999/93/EC

22 Sept 2000: Council of Ministers approves eID card concept study

19 July 2001: Council of Ministers approves basic concepts (smart card, citizen-certificates, no integration with SIS card, Ministry of Internal Affairs is responsible for RRN's infrastructure, pilot municipalities, helpdesk, card production, legal framework,… Fedict for certification services

3 Jan 2002: Council of Ministers assigns RRN's infrastructure to NV Steria

27 Sept 2002: Council of Ministers assigns card production to NV Zetes, certificate services to NV Belgacom

31 March 2003: first 4 eID cards issued to civil servants

9 May 2003: first pilot municipality starts issuing eID cards

25 July 2003: eleventh pilot municipality started

25 January 2004: start of pilot phase evaluation

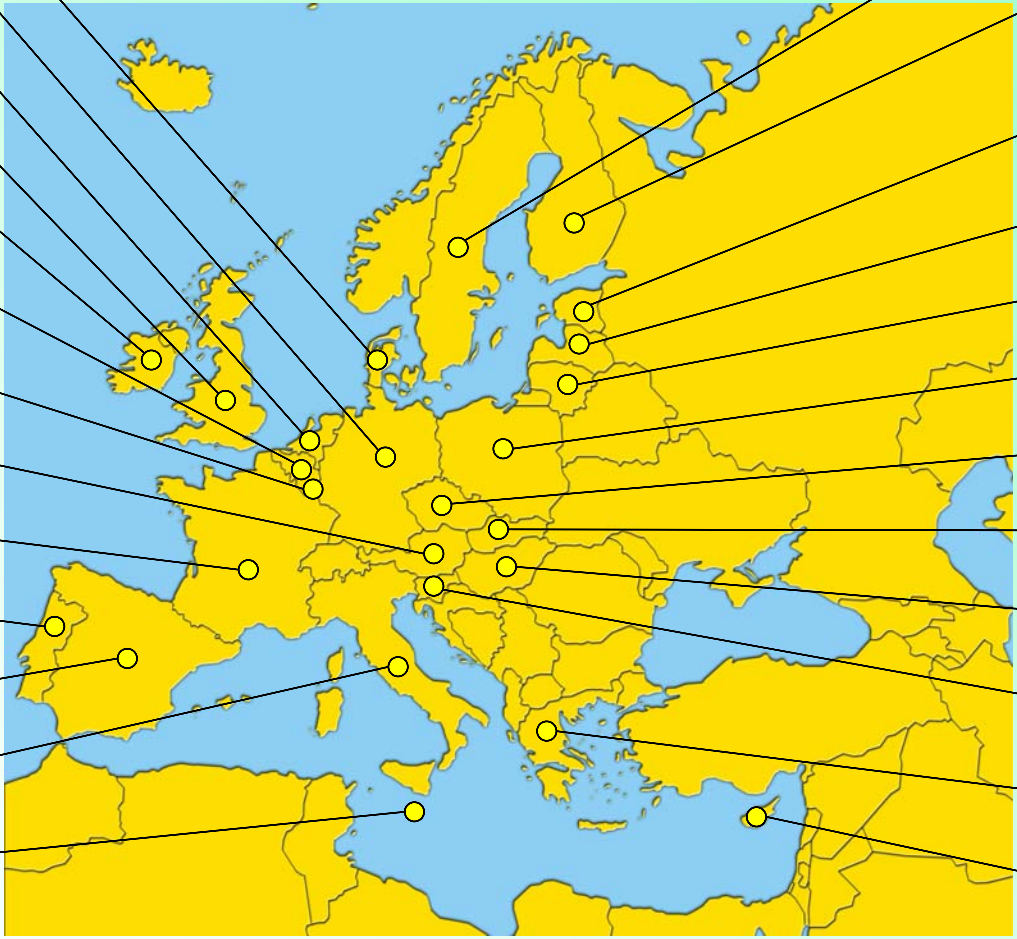
27 September 2004: start of nation-wide roll-out

Spring 2005: all newly issued ID cards are eID cards (no new non-eID cards)

End of 2009: all citizens and 5-year non-citizen residents have an eID card

eID Cards In Europe

eID cards In Europe



Denmark

Germany

The Netherlands

United Kingdom

Ireland

Belgium
> 80.000 in 1.5 years

Luxembourg

Austria

France

Portugal

Spain

Italy

Malta

Sweden

Finland
< 30.000 in 5 years

Estonia
> 500.000 in 2.5 years

Latvia

Lithuania

Poland

Czech Republic

Slovakia

Hungary

Slovenia

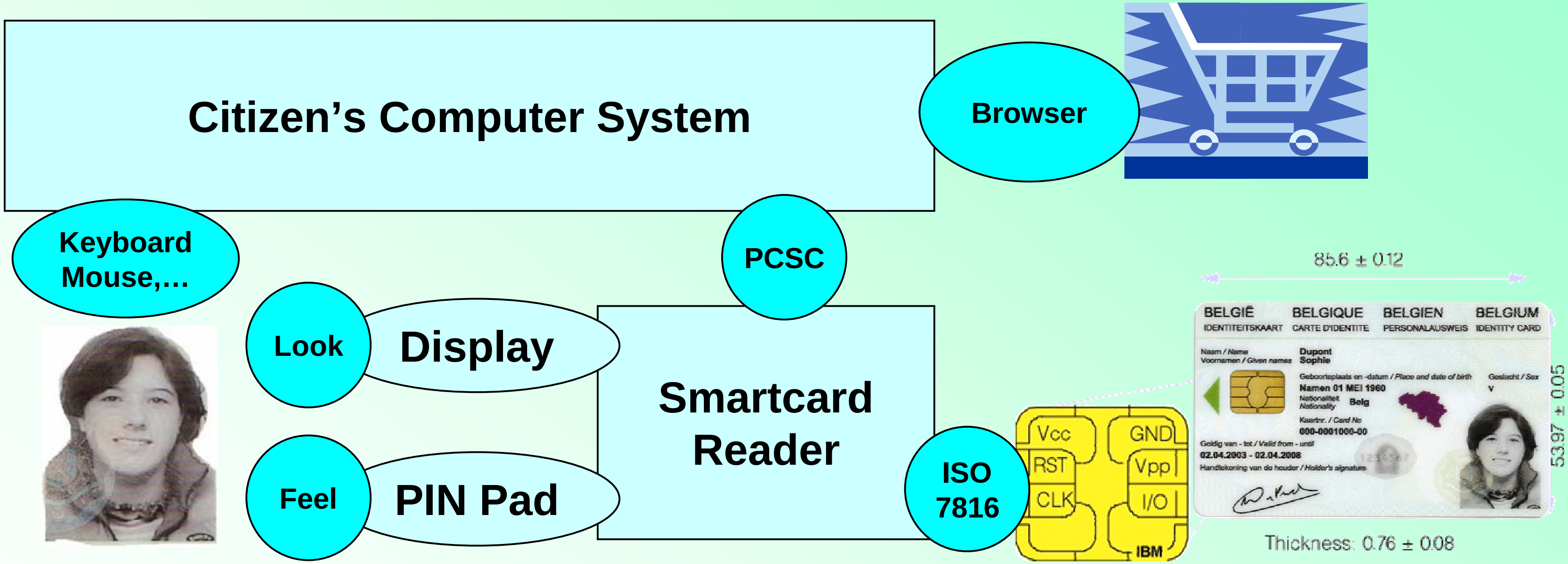
Greece

Cyprus

Citizen can pull an eID card	Government pushes eID cards	Issues eID cards in a pilot phase	Plans to Issue eID cards	No plans to issue eID cards	Not compliant With Directive 1999/93/EC	Plans To issue ID cards	Unknown Status

eID Card Operating System, Drivers & Middleware

Typical Smartcard Architecture



Citizen’s Computer System

Browser

Keyboard Mouse,…

PCSC

Look

Display

Feel

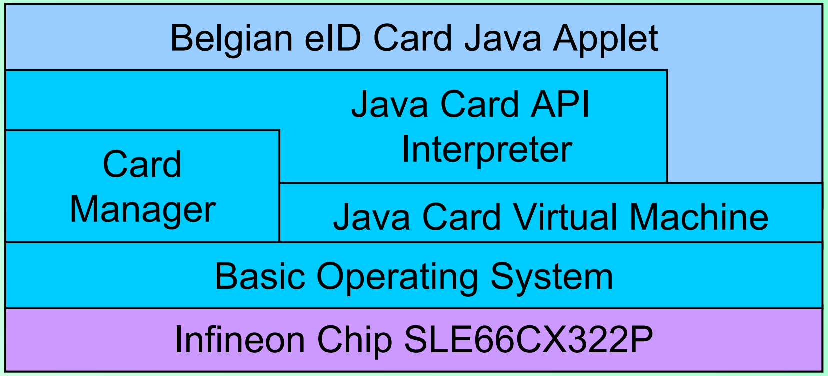
PIN Pad

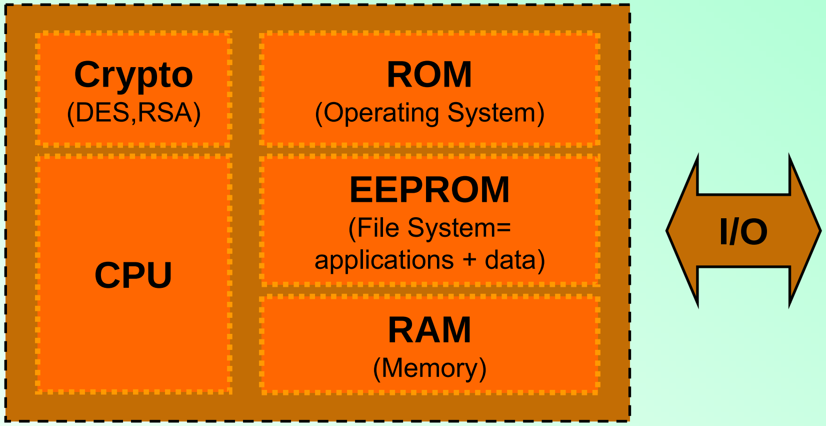
Smartcard Reader

ISO 7816

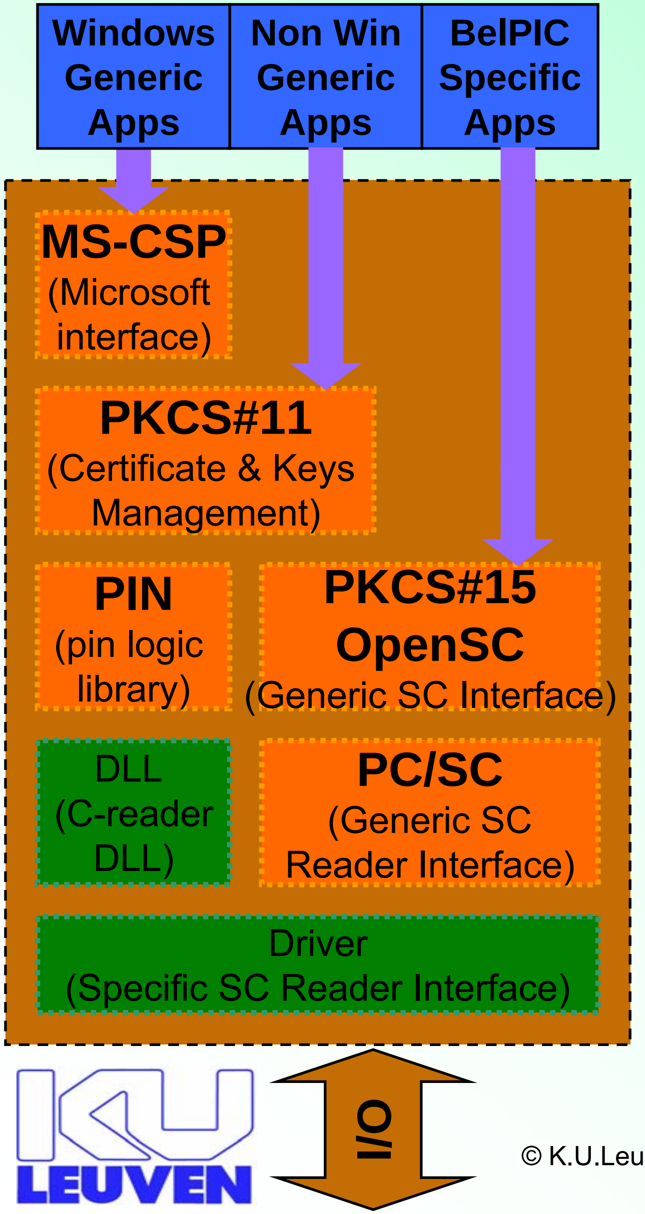
eID Card Chip Specifications

- Cryptoflex JavaCard 32K
  - CPU (processor): 16 bit Microcontroller
  - Crypto-processor:
    - 1100 bit Crypto-Engine (RSA computation)
    - 112 bit Crypto-Accelerator (DES computation)
  - ROM (OS): 136 kB (GEOS Java Virtual Machine)
  - EEPROM (Application + Data): 32 KB (Cristal Applet)
  - RAM (memory): 5 KB
- Standard - ISO/IEC 7816
  - Format & Physical Characteristics ⇔ Bank Card (ID1)
  - Standard Contacts & Signals ⇔ RST, GND, CLK, Vpp, Vcc, I/O
  - Standard Commands & Query Language (APDU)


Belgian eID Card Java Applet
Java Card API Interpreter
Card Manager
Java Card Virtual Machine
Basic Operating System
Infineon Chip SLE66CX322P



eID Card Middleware

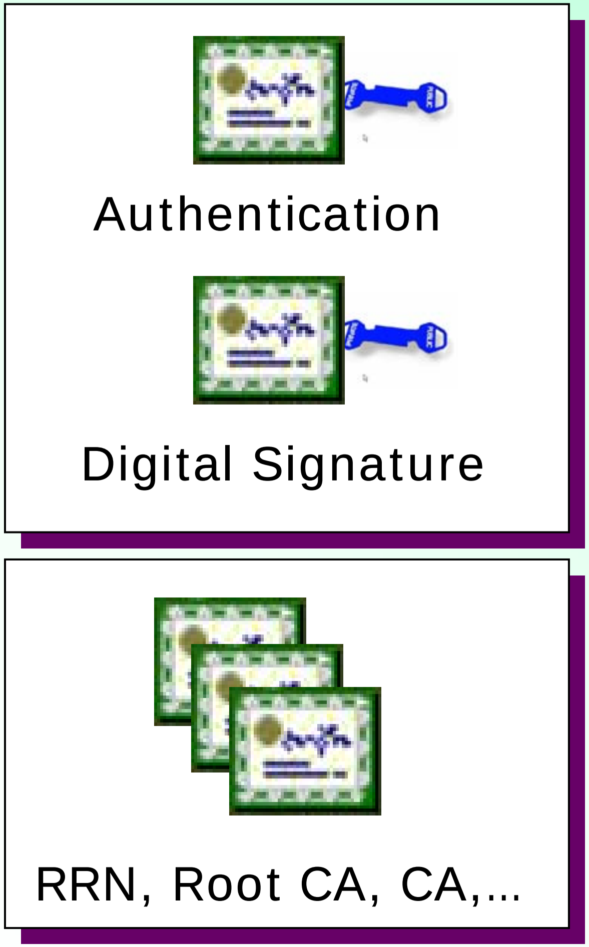


- PKCS#15 file system for ID applications
  - All eID-related data (certificates, photo, address, identity files,…)
  - No key management
- PKCS#11 standard interface to crypto tokens
  - Abstraction of signing functions (authentication, digital signatures)
  - Access to certificates
  - Available for Unix, Windows, MacOSX,…
- CSP for Microsoft Platforms
  - Only keys & certificates available via MSCrypto API
  - Allows authentication (& signature)
  - For Microsoft Explorer, Outlook,…

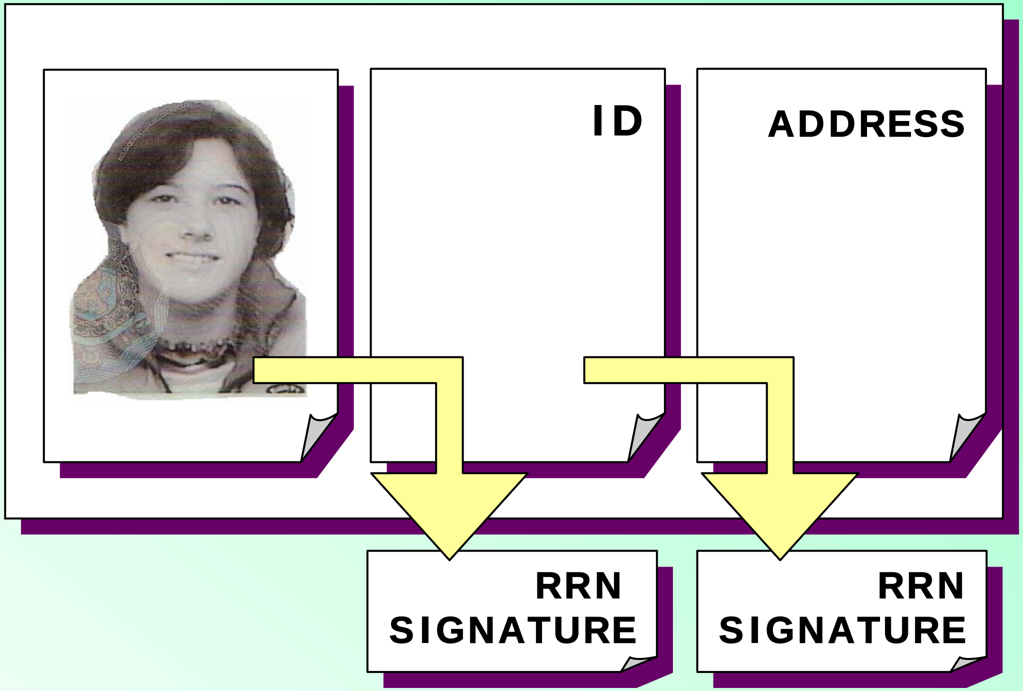
eID Card Content

eID Card Content

PKI



Citizen Identity Data



RRN = National Register

Identity Files Content

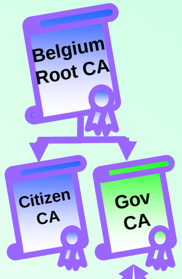
- Identity file (~160 bytes)
  - Chip-specific:
    - Chip number
  - Citizen-specific:
    - Name
    - First 2 names
    - First letter of 3rd first name
    - RRN identification number
    - Nationality
    - Birth location and date
    - Gender
    - Noble condition
    - Special status
    - SHA-1 hash of citizen photo
  - Card-specific:
    - Card number
    - Validity's begin and end date
    - Card delivery municipality
    - Document type
- Digital signature on identity file issued by the RRN

- Citizen's main address file (~120 bytes)
  - Street + number
  - Zip code
  - Municipality
- Digital signature on main address and the identity file issued by the RRN
- Citizen's JPEG photo ~3 Kbytes

King, Prince, Count, Earl, Baron,…

No status, white cane (blind people), yellow cane (partially sighted people), extended minority, any combination

Belgian citizen, European community citizen, non-European community citizen, bootstrap card, habilitation/machtigings card



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

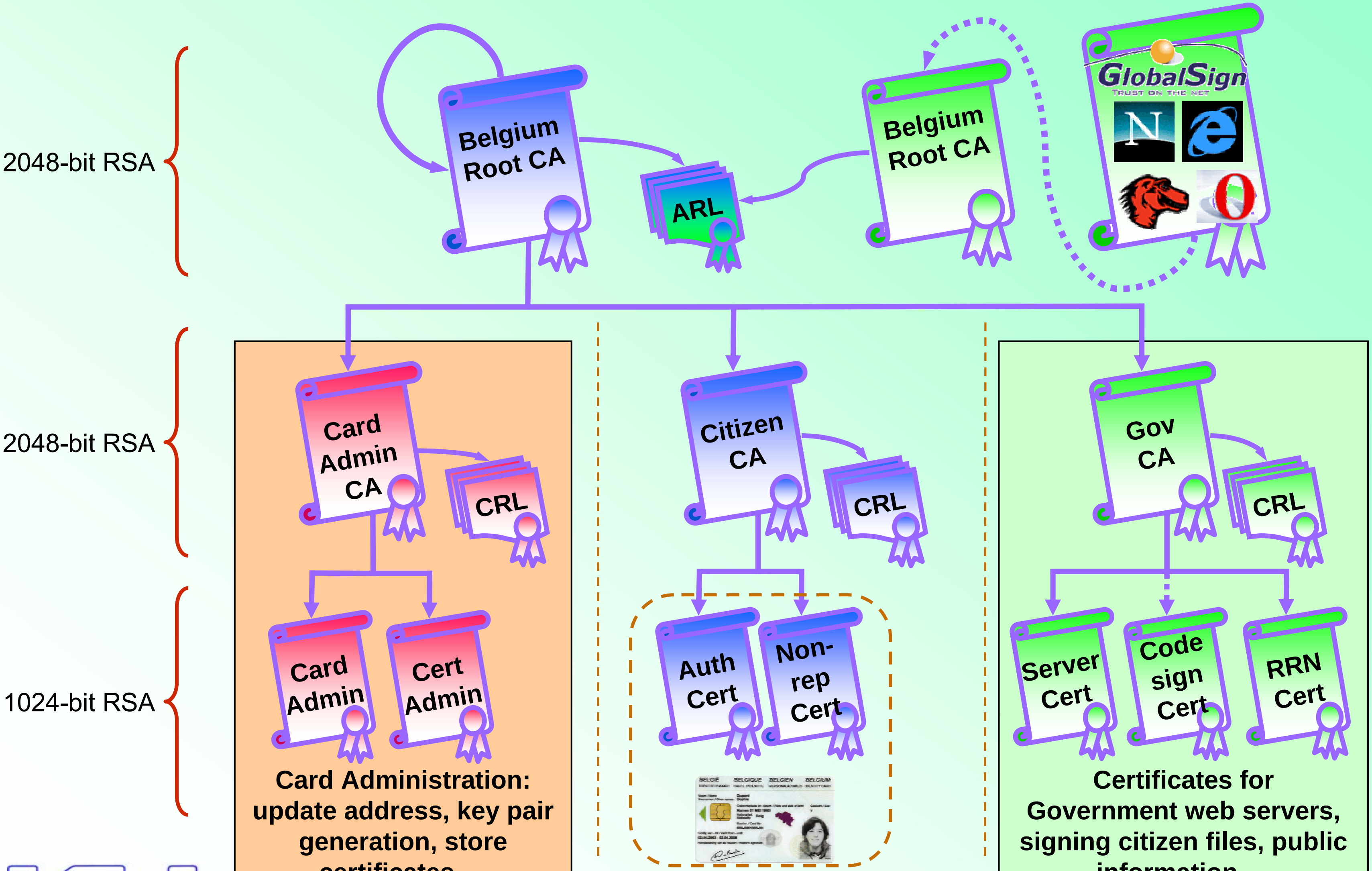
BELGIË BELGIQUE BELGIEN BELGIUM
IDENTITEITSKAART CARTE D'IDENTITE PERSONALAUSWEIS IDENTITY CARD
Naam / Name Dupont
Voornamen / Given names Sophie
Geboorteplaats en -datum / Place and date of birth Namen 01 MEI 1960
Geslacht / Sex V
Nationaliteit / Nationality Belg
Kaartnr. / Card No 000-0001000-00
Geldig van - tot / Valid from - until 02.04.2003 - 02.04.2008
Handtekening van de houder / Holder's signature

Certificate Hierarchy

&

Certificate Details

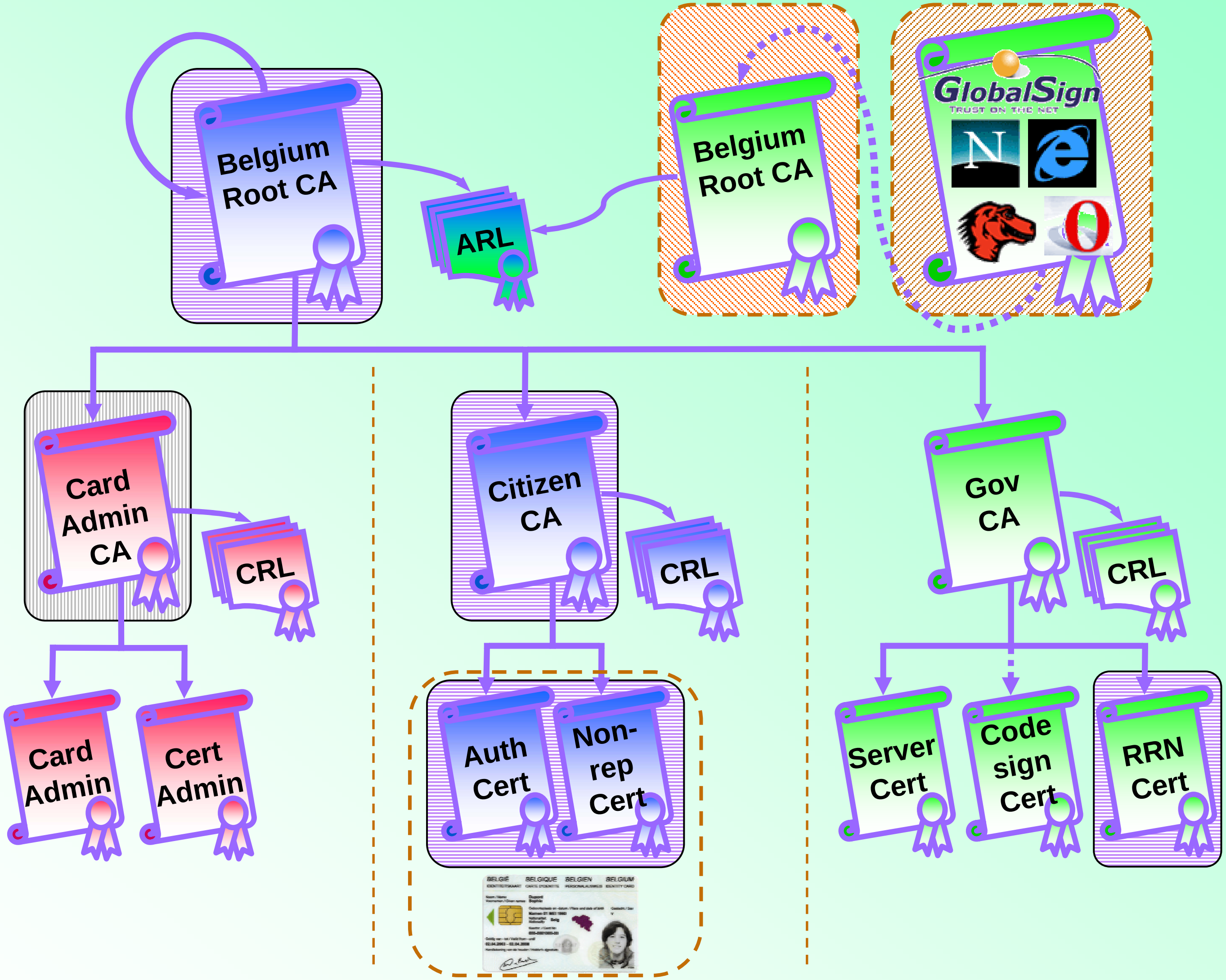
eID Certificates Hierarchy



Card Administration: update address, key pair generation, store certificates,…

Certificates for Government web servers, signing citizen files, public information,…

Location of the Certificates



Certificate embedded in most commercial browsers

Certificate obtained by applications using eID cards

Certificate stored in full in every eID card

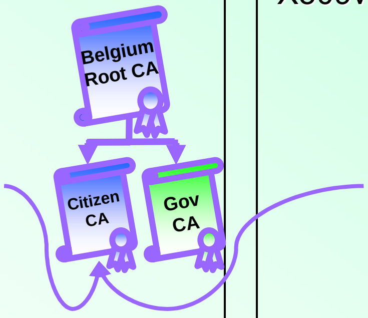
Public key of this certificate is stored in every eID card

Citizen Certificate Details

Citizen Qualified certificate (~1000 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: C=BE, CN=Citizen CA
Not valid before: Nov 12 22:41:00 2003 GMT
Not valid after: Nov 12 22:41:00 2008 GMT
Subject: C=BE, CN=Sophie Dupont (Signature), SN=Dupont, GN=Sophie Nicole/serialNumber=60050100093
Subject Public Key Info:
RSA Public Key: [Modulus (1024 bit): 4b:e5:7e:6e: … :86:17, Exponent: 65537 (0x10001)]
X509v3 extensions:
Certificate Policies:
Policy: 2.16.56.1.1.1.2.1
CPS: http://repository.eid.belgium.be
Key Usage: critical, Non Repudiation

Authority Key Identifier: [D1:13: … :7F:AF:10]
CRL Distribution Points:
URI:http://crl.eid.belgium.be/eidc0002.crl
Netscape Cert Type: S/MIME
Authority Information Access:
CA Issuers - URI:http://certs.eid.belgium.be/belgiumrs.crt
OCSP - URI:http://ocsp.eid.belgium.be
Qualified certificate statements: [00......F..]
Signature: [74:ae:10: … :e0:91]



Citizen Authentication certificate (~980 bytes)

Version: 3 (0x2)
Serial Number:
10:00:00:00:00:00:0a:5d:9a:91:b1:21:dd:00:a2:7a
Signature Algorithm: sha1WithRSAEncryption (1024 bit)
Issuer: C=BE, CN=Citizen CA
Not valid before: Nov 12 22:40:52 2003 GMT
Not valid after: Nov 12 22:40:52 2008 GMT
Subject: C=BE, CN=Sophie Dupont (Authentication), SN=Dupont, GN=Sophie Nicole/serialNumber=60050100093
Subject Public Key Info:
RSA Public Key: [Modulus (1024 bit): cf:ca:7a:77: … :5c:c5, Exponent: 65537 (0x10001)]
X509v3 extensions:
Certificate Policies:
Policy: 2.16.56.1.1.1.2.2
CPS: http://repository.eid.belgium.be
Key Usage: critical, Digital Signature

Authority Key Identifier: [D1:13: … 7F:AF:10]
CRL Distribution Points:
URI:http://crl.eid.belgium.be/eidc0002.crl
Netscape Cert Type: SSL Client, S/MIME
Authority Information Access:
CA Issuers - URI:http://certs.eid.belgium.be/belgiumrs.crt
OCSP - URI:http://ocsp.eid.belgium.be

Signature: [10:ac:04: … :e9:04]

CA Certificate Details

Root CA certificate (920 bytes)

```
Version: 3 (0x2)
Serial Number:
        58:0b:05:6c:53:24:db:b2:50:57:18:5f:f9:e5:a6:50
Signature Algorithm: sha1WithRSAEncryption (2048 bit)
Issuer: C=BE, CN=Belgium Root CA
Not valid before: Jan 26 23:00:00 2003 GMT
Not valid after : Jan 26 23:00:00 2014 GMT
Subject: C=BE, CN=Belgium Root CA

Subject Public Key Info:
        RSA Public Key: [Modulus (2048 bit): 00:c8:a1:71: … :b0:6f,
              Exponent: 65537 (0x10001)]
X509v3 extensions:
        Certificate Policies:
                Policy: 2.16.56.1.1.1
                CPS: http://repository.eid.belgium.be
        Key Usage: critical, Certificate Sign, CRL Sign
        Subject Key Identifier: [10:F0: … :8E:DB:E6]
        Authority Key Identifier: [10:F0: … :8E:DB:E6]


        Netscape Cert Type: SSL CA, S/MIME CA, Object Signing CA
        Basic Constraints: critical, CA:TRUE




Signature: [c8:6d:22: … :43:2a]
```

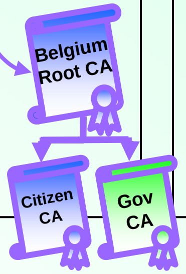
CA certificate (975 bytes)

```
Version: 3 (0x2)
Serial Number:
        6f:77:79:33:30:25:e3:cf:92:55:b9:7a:8a:0b:30:e5
Signature Algorithm: sha1WithRSAEncryption (2048 bit)
Issuer: C=BE, CN=Belgium Root CA
Not valid before: Apr 10 12:00:00 2003 GMT
Not valid after : Jun 26 23:00:00 2009 GMT
Subject: C=BE, CN=Citizen CA

Subject Public Key Info:
        RSA Public Key: [Modulus (2048 bit): 00:c9:ae:05: … :cb:71,
              Exponent: 65537 (0x10001)]
X509v3 extensions:
        Certificate Policies:
                Policy: 2.16.56.1.1.1.2
                CPS: http://repository.eid.belgium.be
        Key Usage: critical, Certificate Sign, CRL Sign
        Subject Key Identifier: [D1:13: … :7F:AF:10]
        Authority Key Identifier: [10:F0: … :8E:DB:E6]
        CRL Distribution Points:
                URI:http://crl.eid.belgium.be/belgium.crl
        Netscape Cert Type: SSL CA, S/MIME CA, Object Signing CA
        Basic Constraints: critical, CA:TRUE, pathlen:0




Signature: [b2:0c:30: … :18:6e]
```



Government Certificate Details

Government CA certificate (~979 bytes)

Version: 3 (0x2)
Serial Number:
99:6f:14:78:8e:ea:69:6a:3d:2e:93:42:81:2b:66:f0
Signature Algorithm: sha1WithRSAEncryption (2048 bit)
Issuer: C=BE, CN=Belgium Root CA
Not valid before: Jan 27 00:00:00 2003 GMT
Not valid after: Jan 27 00:00:00 2009 GMT
Subject: C=BE, CN=Government CA

Subject Public Key Info:
RSA Public Key: [Modulus (2048 bit): 00:ac:c9:a0: … :89:13,
Exponent: 65537 (0x10001)]
X509v3 extensions:
Certificate Policies:
Policy: 2.16.56.1.1.1.3
CPS: http://repository.eid.belgium.be
Key Usage: critical, Certificate Sign, CRL Sign
Subject Key Identifier: [F5:DB: … :D1:8B:D6]
Authority Key Identifier: [10:F0: … :8E:DB:E6]
CRL Distribution Points:
URI:http://crl.eid.belgium.be/belgium.crl
Netscape Cert Type: SSL CA, S/MIME CA, Object Signing CA
Basic Constraints: critical, CA:TRUE, pathlen:0

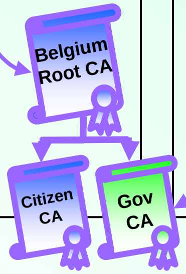
Signature: [a0:53:21: … :1d:c9]

RRN certificate (~808 bytes)

Version: 3 (0x2)
Serial Number:
01:00:00:00:00:00:f8:20:18:9e:17
Signature Algorithm: sha1WithRSAEncryption (1024 bit)
Issuer: C=BE, CN=Government CA
Not valid before: Oct 9 09:06:09 2003 GMT
Not valid after: Jan 26 09:06:09 2009 GMT
Subject: C=BE, CN=RRN, O=RRN

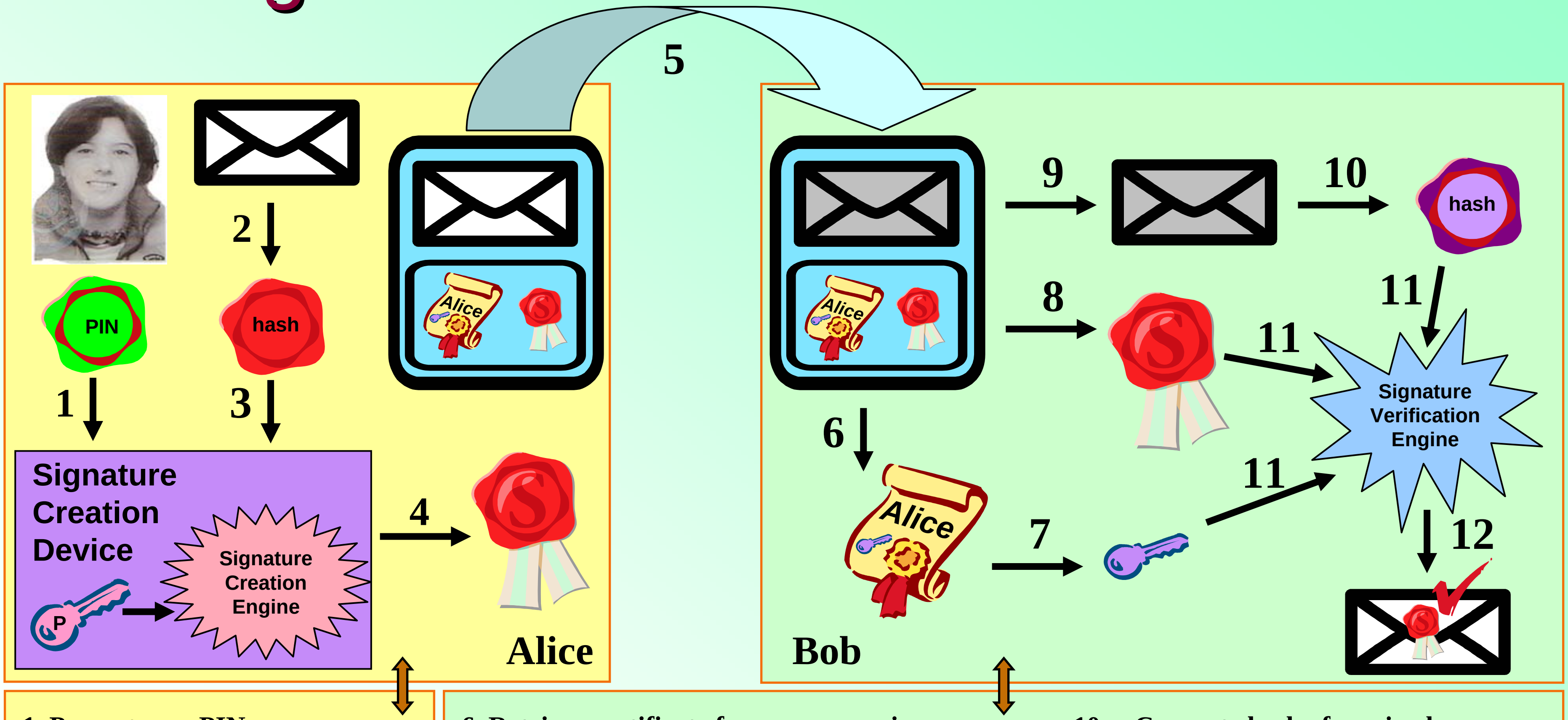
Subject Public Key Info:
RSA Public Key: [Modulus (1024 bit): 00:db:72:4d: … :80:0d,
Exponent: 65537 (0x10001)]
X509v3 extensions:
Certificate Policies:
Policy: 2.16.56.1.1.1.3.1
CPS: http://repository.eid.belgium.be
Key Usage: critical, Digital Signature, Non Repudiation
Subject Key Identifier: [09:22: … :30:01:37]
Authority Key Identifier: [F5:DB: … :D1:8B:D6]
CRL Distribution Points:
URI:http://crl.eid.belgium.be/government.crl

Signature: [12:89:cd: … :ca:2a]



Using Signing Key Pairs

Signature Generation/Verification



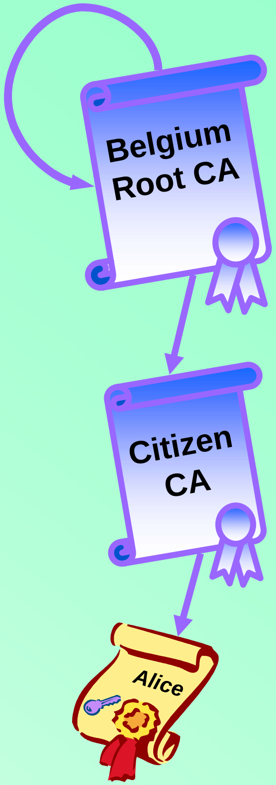
1. Present user PIN
2. Compute hash of message
3. SCD generates digital signature using private key and hash
4. SCD outputs digital signature

6. Retrieve certificate from message signer
7. Retrieve public key from signer certificate
8. Retrieve digital signature from signed message
9. Retrieve received message

10. Compute hash of received message
11. Verify digital signature
12. SVD outputs ‘valid signature’ or ‘invalid signature’

Beware – Bob should also validate Alice’s certificate – Beware

Archiving Signed Data



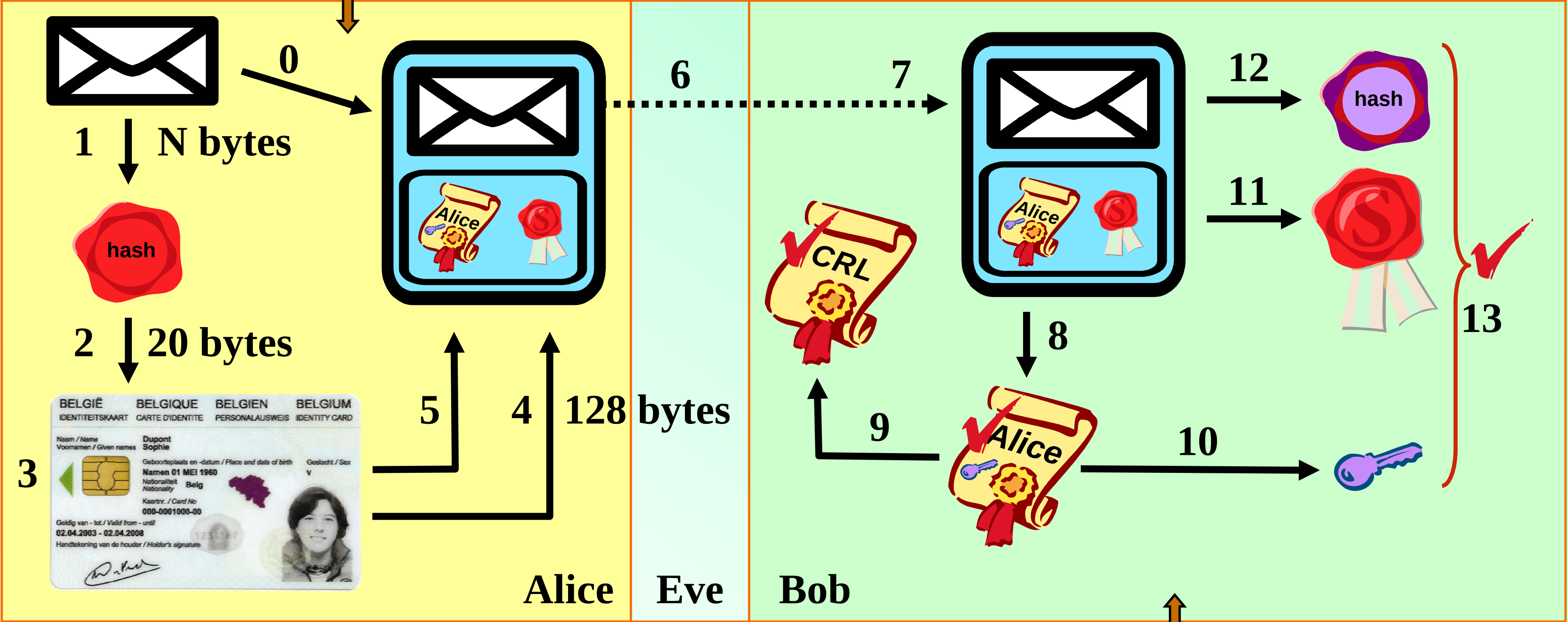
- Digital signatures *remain valid <u>forever</u>* if one stores:
  - The digitally signed data
  - The digital signature on the data
  - The signer's certificate
  - A proof of validity of the signer's certificate
  - The verification timestamp of the signature
- Bottom line:
  - The integrity of this data should be protected!
  - There is no need to retrieve the status of a certificate in the past!

Signing Key Pair Properties

- Private signing key only available to the signer
  - **Signer explicitly authorizes** the Signature Creation Engine to generate a digital signature with the signing key, e.g., by presenting a PIN (personal identification number, cfr. Bank cards)
  - **Signer protects** the hash of his/her message with his/her signing key
  - **Verifier recovers** this hash correctly only if the right verification key is used
- Private signing key corresponds to the public verification key
  - If the Signature Verification Engine (SVE) outputs 'valid signature', the verification key corresponds to the signing key
  - If the SVE outputs 'invalid signature' the triplet (message, digital signature, verification key) does not match:
    - The message may have been *altered*
    - The *verification key may be wrong*, i.e., does not correspond to the signing key
    - The *certificate* of the signer *may have been revoked* (or suspended)
- Private signing key is kept in a secure location, e.g., smartcard
- Public verification key is usually sent along with the digital signature
  - Integrity of the verification key is protected through the signer's certificate

Typical Data Signing Scenario

1. Compute data hash
2. Present PIN
3. Compute signature
4. Collect signature
5. Collect certificate
6. Send message



7. Decompose message
8. Check certificate
9. Check CRL
10. Retrieve public key
11. Retrieve signature
12. Compute hash
13. Verify signature

Validity of Signatures

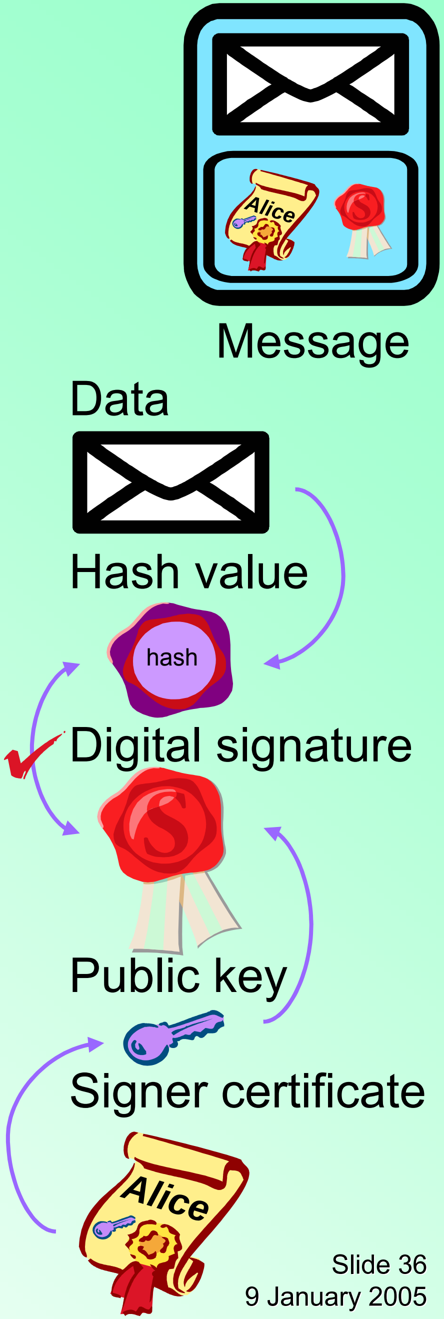
Signature Validation

- A digital signature protects the integrity of information

- A digital signature computed on some data is valid if and only if
  - The signature verification engine confirms that the hash value computed on the data matches the digital signature when applying the signature verification mechanism using the public key found in the corresponding certificate
  - The certificate is valid (cfr. next slide)
  - All the key usage and certificate policies of the certificates in the certificate chain match the context wherein the data is used (e.g., code signing, client authentication, server authentication,…)

- Caveat: When was this signature computed?
- Revoked ≠ Invalid
  - Keep a log of valid signatures

- Features of a hash function useful for cryptographic applications:
  - Given a hash value *H(x)*: hard to find an input *x* which produces *H(x)*
  - Given *x* and *H(x)*: hard to find *y* so that *H(x)=H(y)* and x≠y
  - Hard to find any *x* and *y* so that x≠y and *H(x)=H(y)*



Message

Data

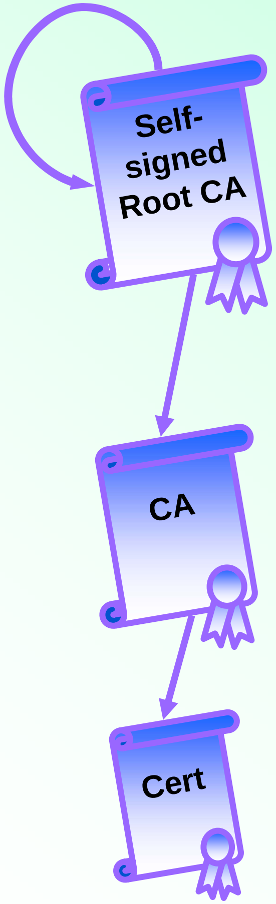
Hash value

Digital signature

Public key

Signer certificate

Certificate (Chain) Validation



- A certificate protects the identity of the holder of the corresponding private key

- Given a self-signed certificate Root CA protects the CA certificate which is used to validate a non-CA certificate

- A certificate Cert is valid if and only if
  - The certificate's digital signature is (cryptographically) valid given the certificate issuer's certificate (CA certificate)
  - The certificate issuer's certificate is valid (using that certificate's issuer certificate. This may be the same certificate if self-signed)
  - The time of certificate validation lies within the validity period of all these certificates
  - All certificate extensions must match the respective profiles and key usages
  - None of these certificates is known as invalid, i.e.,
    - Their serial numbers have not been revoked

- Check the revocation status of a certificate using CRLs or OCSP
  - Depending on the required security level, one may decide to rely on the OCSP, or on a local CRL copy, or on a local CRL copy in combination with a recent Delta CRL
  - Offline validation is possible using CRL, preferably combined with Delta CRL
  - OCSP (Online Certificate Status Protocol) requires a live network connection

- Valid ≠ Trustworthy
  - One should check whether the self-signed (Root CA) certificate can be trusted

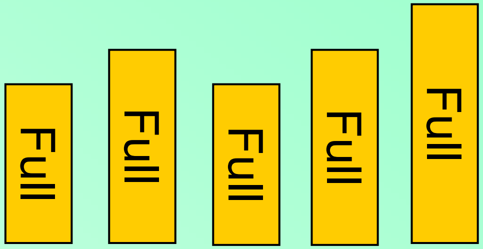
OCSP vs. CRLs – "Is the certificate valid?"

- Two options to make this business decision:
  - Do it yourself and use CRLs and Delta-CRLs
  - Trust a third party using OCSP
- Use the Online Certificate Status Protocol (OCSP) where a trusted OCSP Responder answers the question with either "yes", "no", or "I do not know"
  - Remaining issues:
    - An OCSP Responder may use the most recent certificate status information (CSI)
      - An OCSP Responder does not have to use the most recent CSI!
      - The Responder typically uses CRLs to produce its answers
    - How to trust the OCSP Reponse?
  - Ideal for a few situations:
    - If only a few certificates per time unit must be validated
      - E.g., for citizens who wish to validate a certificate "from time to time"
    - To authenticate high-impact transactions
      - E.g., cash withdrawal, account closure, physical or electronic access control
- Certificate Revocation Lists (CRLs)
  - The digital signature verifier collects the (most recent) CRLs for the certificates in the certificate chain
    - These CRLs may become very large (e.g., several megabytes) ⇨ Delta-CRLs
    - Delta-CRLs may be very large (e.g., half a megabyte) ⇨ Delta-Delta CRLs
      - Note: Delta-Delta-CRLs are not standard (e.g., a few kilobytes each)

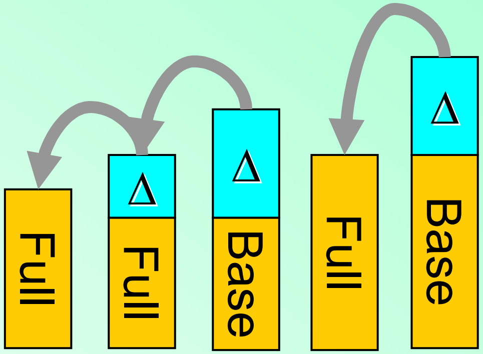
Certificate Revocation Lists

Certificate Revocation Lists (CRLs)

- Complete CRL
  - Enumerates all certificate serial numbers that should not be trusted
  - Typically (very) large, e.g., >>500 Kbytes
  - Validity expires 7 days after creation
  - Certificates of new eID cards
    - Appear as on hold
    - Disappear when activated
  - Suspended certificates appear as on hold for up to 7 days
  - Items without reason code remain revoked forever
  - One complete CRL is referred to as the Base CRL
- Delta CRL
  - Lists all differences between the current complete CRL and the current Base CRL
  - Typically small, e.g., <500 Kbytes
  - Validity expires 7 days after creation
  - Reason codes:
    - On hold — newly issued eID card certificate is not yet activated, or has been suspended
    - Remove from CRL — eID card certificate has been activated
    - None — eID card certificate has been revoked
- Delta-Delta CRLs
  - Lists all differences between the current complete CRL and a Delta CRL
  - Typically very small, e.g., <25 Kbytes
  - Important note: Delta-Delta CRLs are not standardized

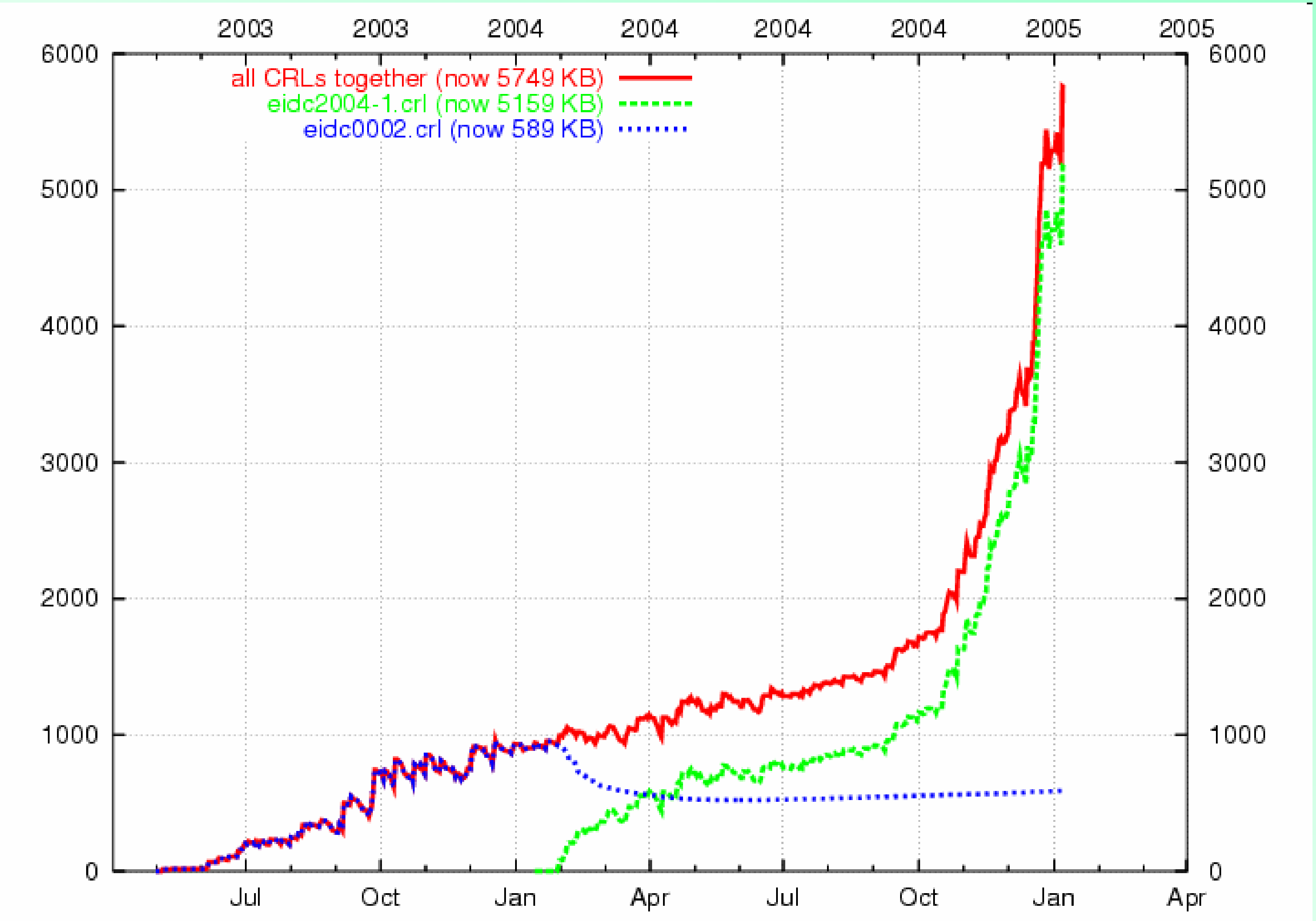


Complete CRLs



Delta CRLs vs. Base CRL

Current eID full CRL sizes



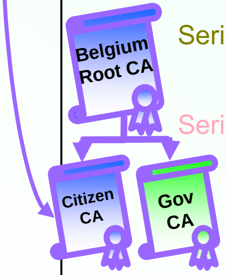
- A CRL is valid for seven days after it is issued
- A new CRL is issued together with a new Delta CRL
- A Delta CRL refers to a particular Base CRL which is always younger than 7 days
- OCSP queries the database with the most recent certificate status information
- OCSP = Online Certificate Status Protocol

Frequently updated graphs available at http://www.godot.be/site/EidCards/belpic/index.html

Certificate Revocation List details

Citizen CRL (+500 Kbyte)

Version 2 (0x1)
Signature Algorithm: sha1WithRSAEncryption (2048 bit)
Issuer: C=BE, CN=Citizen CA
Creation date: Apr 6 15:19:23 2004 GMT
Next update: Apr 13 15:19:23 2004 GMT
CRL extensions:
    Authority Key Identifier: [D1:13: ... :7F:AF:10]
    CRL Number: 4294995040
Revoked Certificates:
    Serial Number: 100000000000000004B823FAE7B1BB44B1
        Revocation Date: Jan 14 12:56:50 2004 GMT
        CRL Reason Code: Certificate Hold
    Serial Number: 1000000000000000062F6A1BB1431902D4
        Revocation Date: Oct 23 23:15:11 2003 GMT
        CRL Reason Code: Certificate Hold
    Serial Number: 10000000000001243778BEFF61123DE
        Revocation Date: Jan 12 10:19:24 2004 GMT
    Serial Number: 10000000000000125DC2DF2031534033
        Revocation Date: Sep 5 09:49:44 2003 GMT
    Serial Number: 1000000000000091ACC84FC377F8A6ECE
        Revocation Date: Dec 16 17:24:15 2003 GMT
        CRL Reason Code: Certificate Hold
    Serial Number: 1000000000000092135CE8FB8F0D66093
        Revocation Date: Nov 13 17:18:49 2003 GMT



Signature: [95:19:b2: ... :21:31]

Citizen Delta CRL (~15 Kbyte)

Version 2 (0x1)
Signature Algorithm: sha1WithRSAEncryption (2048 bit)
Issuer: C=BE, CN=Citizen CA
Creation date: Apr 8 17:43:14 2004 GMT
Next update: Apr 15 17:43:14 2004 GMT
CRL extensions:
    Authority Key Identifier: [D1:13: ... :7F:AF:10]
    CRL Number: 4294995072
    Delta CRL Indicator: critical, 4294995040
Revoked Certificates:
    Serial Number: 10000000000007E5B11506303959320
        Revocation Date: Apr 8 16:33:23 2004 GMT
        CRL Reason Code: Certificate Hold
    Serial Number: 1000000000000091ACC84FC377F8A6ECE
        Revocation Date: Apr 8 16:55:14 2004 GMT
        CRL Reason Code: Remove From CRL
    Serial Number: 100000000000127BE2DA18842E8A7BAC
        Revocation Date: Apr 8 15:20:13 2004 GMT
        CRL Reason Code: Remove From CRL
    Serial Number: 100000000000001902ECF11657FE2813A5
        Revocation Date: Apr 8 16:29:54 2004 GMT
    Serial Number: 100000000000FDFF72C4E59AD46AFC21
        Revocation Date: Apr 8 17:33:31 2004 GMT
        CRL Reason Code: Remove From CRL
    Serial Number: 100000000000FE6A4ACD4ECF04233442
        Revocation Date: Apr 8 15:32:38 2004 GMT
    …

Signature: [64:20:22: ... :c3:5e]

Signature & Certificate Lifecycle

Summary on Validity Statuses

- Digital signature
  - Valid
  - Invalid

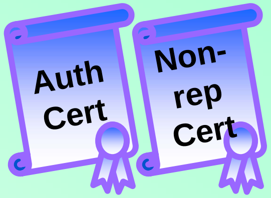
- Signature creation device
  - Valid
  - Invalid
    - Suspended
    - Revoked
    - Expired

BELGIË BELGIQUE BELGIEN BELGIUM
IDENTITEITSKAART CARTE D'IDENTITE PERSONALAUSWEIS IDENTITY CARD

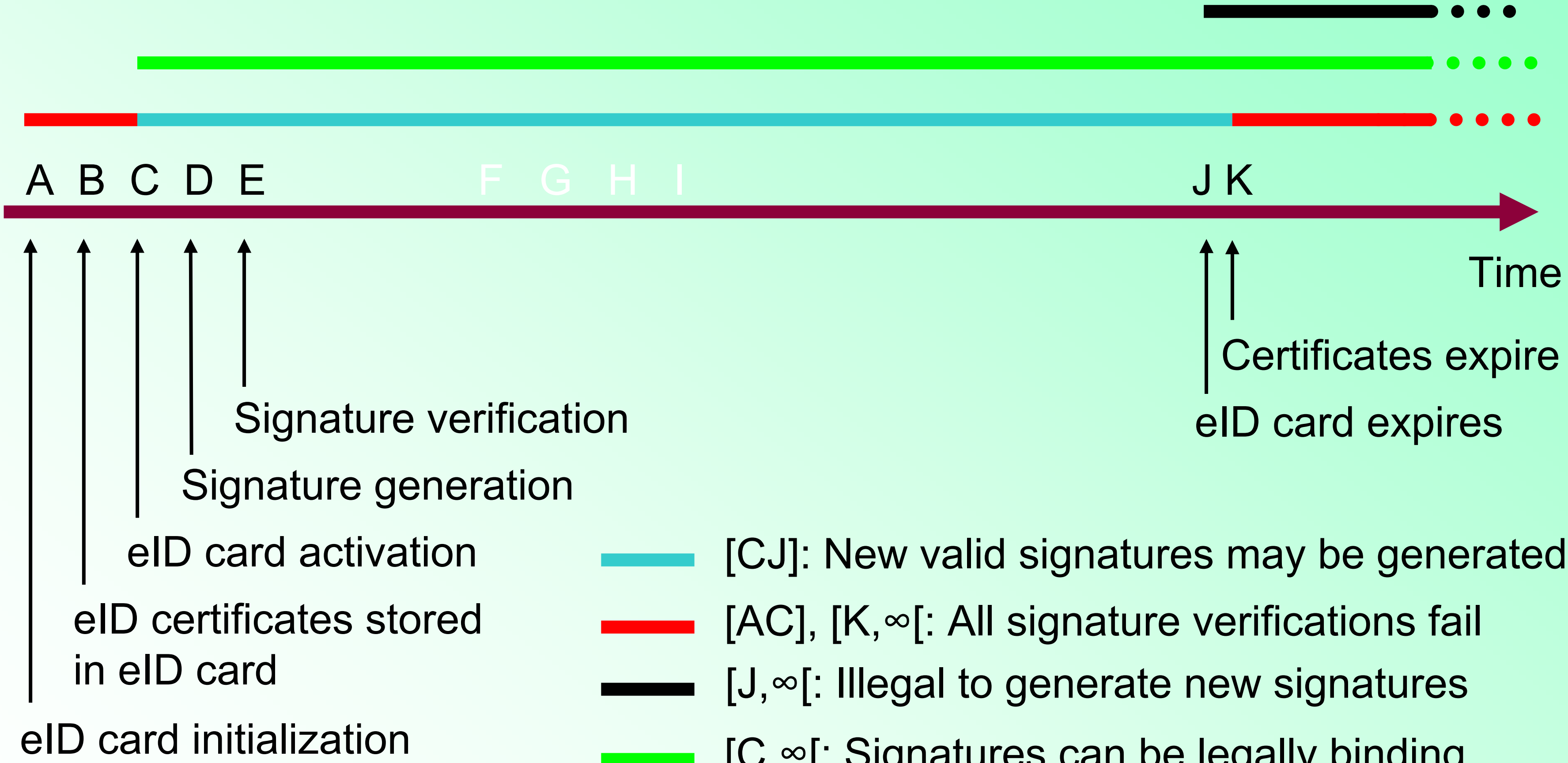
Naam / Name Dupont
Voornamen / Given names Sophie
Geboorteplaats en -datum / Place and date of birth
Namen 01 MEI 1960
Geslacht / Sex
V
Nationaliteit / Nationality Belg
Kaartnr. / Card No
000-0001000-00
Geldig van - tot / Valid from - until
02.04.2003 - 02.04.2008
Handtekening van de houder / Holder's signature

- CRL, OCSP Response
  - Valid
  - Invalid
  - Expired

- Certificate
  - Valid
  - Invalid
    - Suspended
    - Revoked
    - Expired
  - Unknown



Signature Validity



Certificates expire

eID card expires

Signature verification

Signature generation

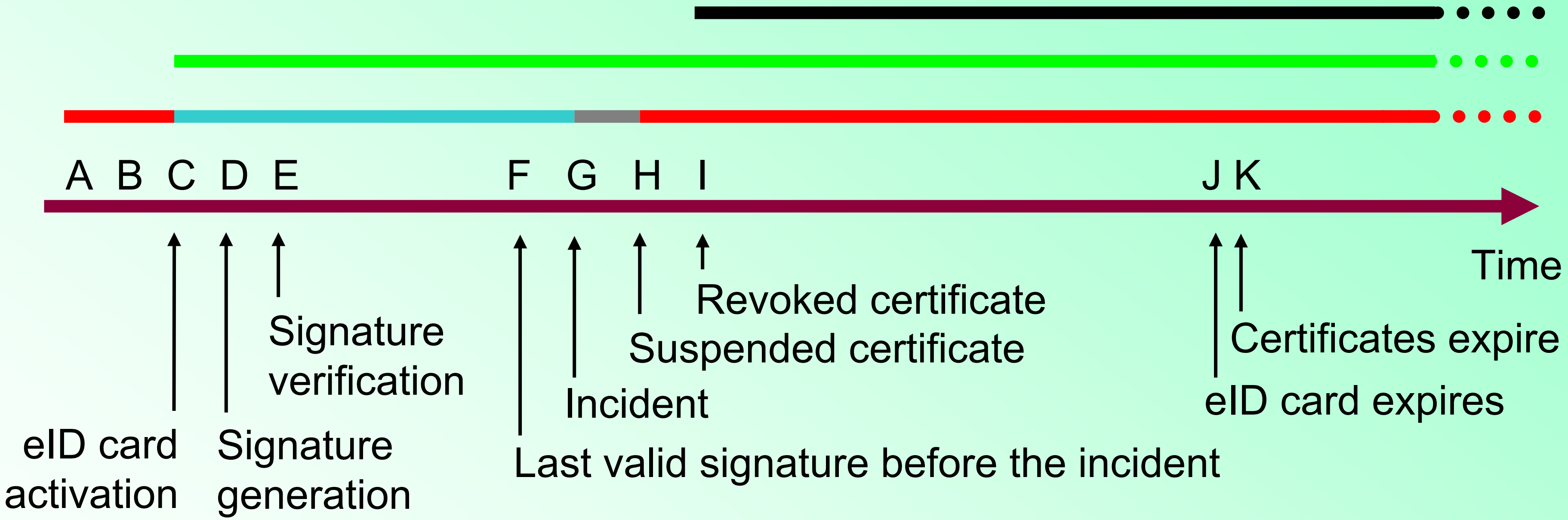
eID card activation

eID certificates stored
in eID card

eID card initialization

🟦	[CJ]: New valid signatures may be generated
🟥	[AC], [K,∞[: All signature verifications fail
⬛	[J,∞[: Illegal to generate new signatures
🟩	[C,∞[: Signatures can be legally binding if verified in [CJ[

Signature Validity with Revocation



A B C D E F G H I J K

Time

eID card activation

Signature generation

Signature verification

Last valid signature before the incident

Incident

Suspended certificate

Revoked certificate

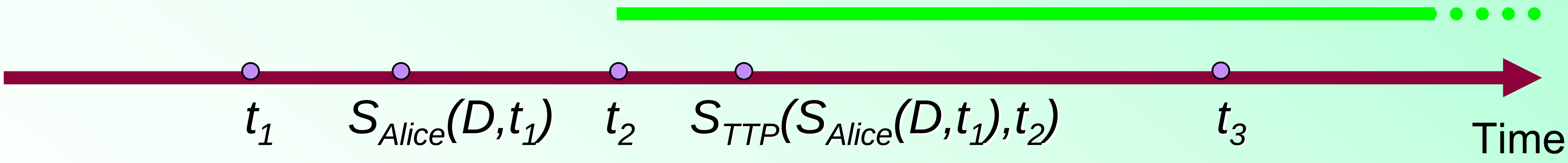
eID card expires

Certificates expire

- ▨ [GH]: Signatures created in [GI] should be invalid, H may be equal to I
- ⬛ [I,∞[: Illegal to generate new signatures
- 🟦 [CG[: New valid signatures may be generated
- 🟥 [AC], [H,∞[: Signature verification returns invalid
- 🟩 [CF]: Signatures validated before F may be valid forever

Long Term Signatures

- Alice produces a digital signature on data *D* that will resist time:
  - Alice collects a time stamp t_1 from a trusted third party *(TTP)*
  - Alice produces a digital signature $S_{Alice}(D,t_1)$ on the time stamp t_1 and the data *D*
  - *TTP* validates a digital signature $S_{Alice}(D,t_1)$ at time t_2
  - *TTP* computes a digital signature $S_{TTP}(S_{Alice}(D,t_1),t_2)$ if and only if the *TTP*
    - Has validated Alice’s digital signature, and
    - Confirms that the signature and Alice’s full certificate chain was valid at time t_2
  - Alice can now indefinitely rely on $S_{TTP}(S_{Alice}(D,t_1),t_2)$, even if her certificate must be revoked, e.g., at time t_3 (after t_2), or if her certificate expires

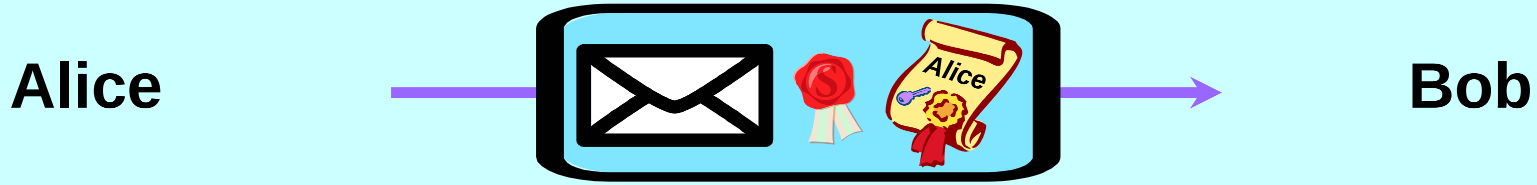


- Note: This procedure assumes that no cryptographic weaknesses are discovered in the signature generation and validation algorithms and procedures

Decryption Procedures

No encryption certificates!

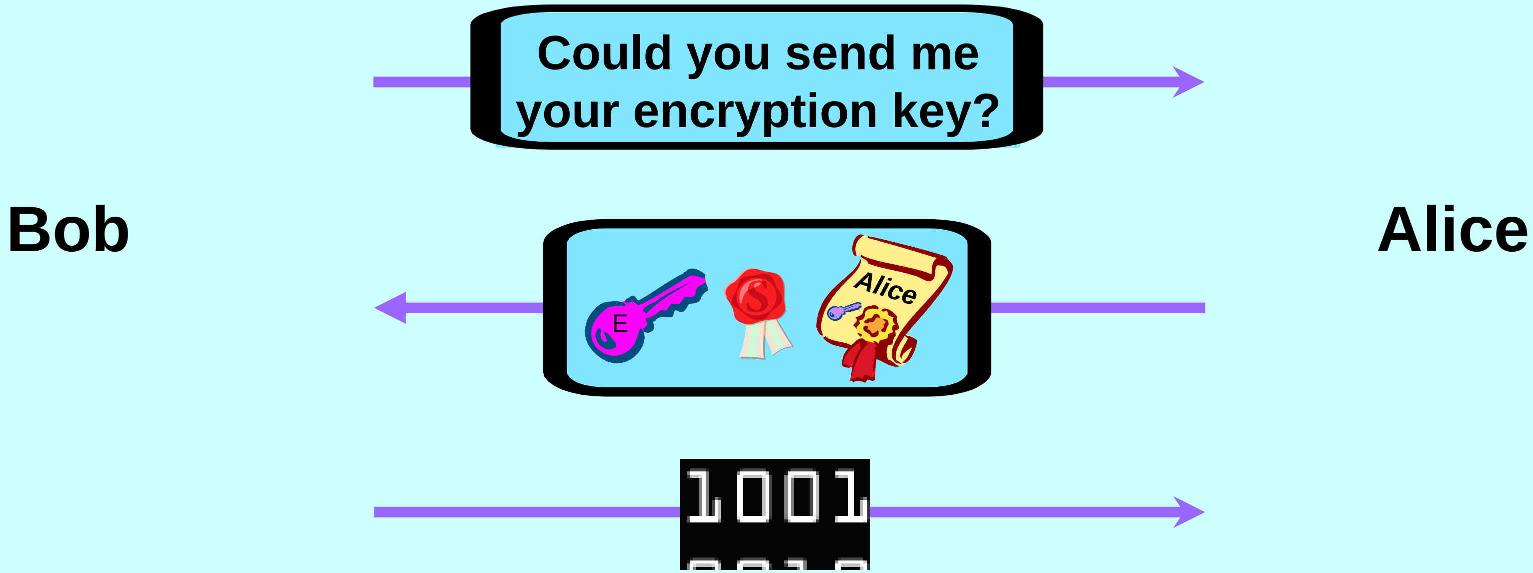
Alice sends a digitally signed message to Bob



Alice

Bob

Alice receives an encrypted message from Bob

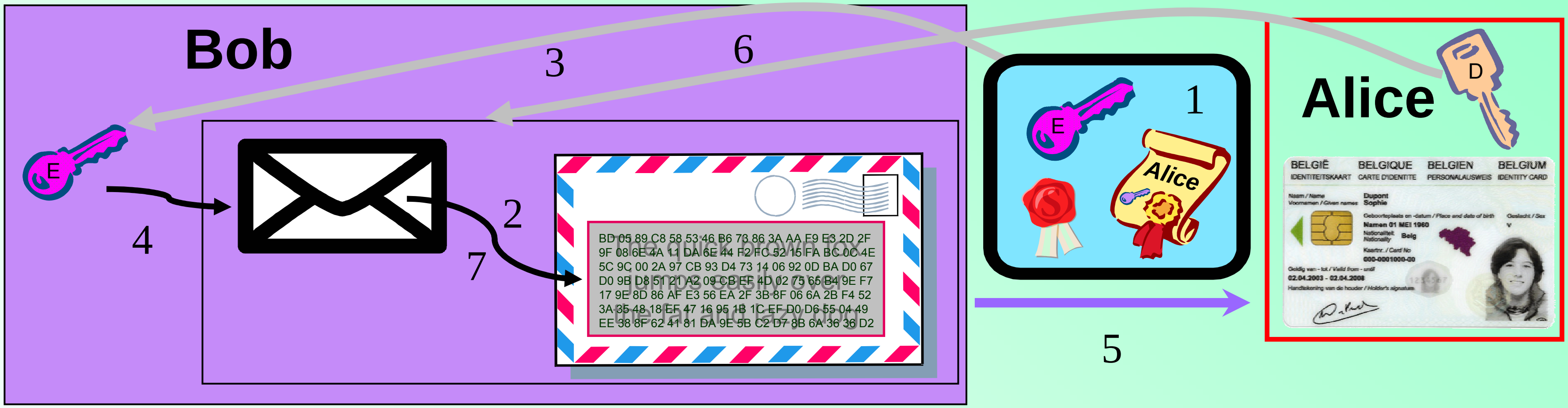


Could you send me your encryption key?

Bob

Alice

Typical Data Decryption Scenario


Bob
3
6
1
Alice
D
E
E
Alice
4
2
7
5
BD 05 89 C8 58 53 46 B6 73 86 3A AA F9 E3 2D 2F
9F 08 6E 4A 11 DA 6E 44 F2 FC 52 15 FA BC 0C 4E
5C 9C 00 2A 97 CB 93 D4 73 14 06 92 0D BA D0 67
D0 9B D8 51 21 A2 09 CB EF 4D 02 75 65 B4 9E F7
17 9E 8D 86 AF E3 56 EA 2F 3B 8F 06 6A 2B F4 52
3A 35 48 18 EF 47 16 95 1B 1C EF D0 D6 55 04 49
EE 38 8F 62 41 81 DA 9E 5B C2 D7 8B 6A 36 36 D2
The quick brown fox
jumps easily over
the fat and lazy dog
BELGIË
BELGIQUE
BELGIEN
BELGIUM
IDENTITEITSKAART
CARTE D'IDENTITE
PERSONALAUSWEIS
IDENTITY CARD
Naam / Name
Voornamen / Given names
Dupont
Sophie
Geboorteplaats en -datum / Place and date of birth
Namen 01 MEI 1960
Geslacht / Sex
V
Nationaliteit
Nationality
Belg
Kaartnr. / Card No
000-0001000-00
Geldig van - tot / Valid from - until
02.04.2003 - 02.04.2008
Handtekening van de houder / Holder's signature

Alice

1. Digitally signs her public encryption key and publishes it on her web site

Bob

2. Encrypts his message for Alice using a random session key
3. Downloads Alice's encryption key (and validates its authenticity)
4. Encrypts the session key with Alice's public encryption key
5. Sends the encrypted message to Alice

Alice

6. Decrypts the session key with her eID card
7. Decrypts the message with the session key

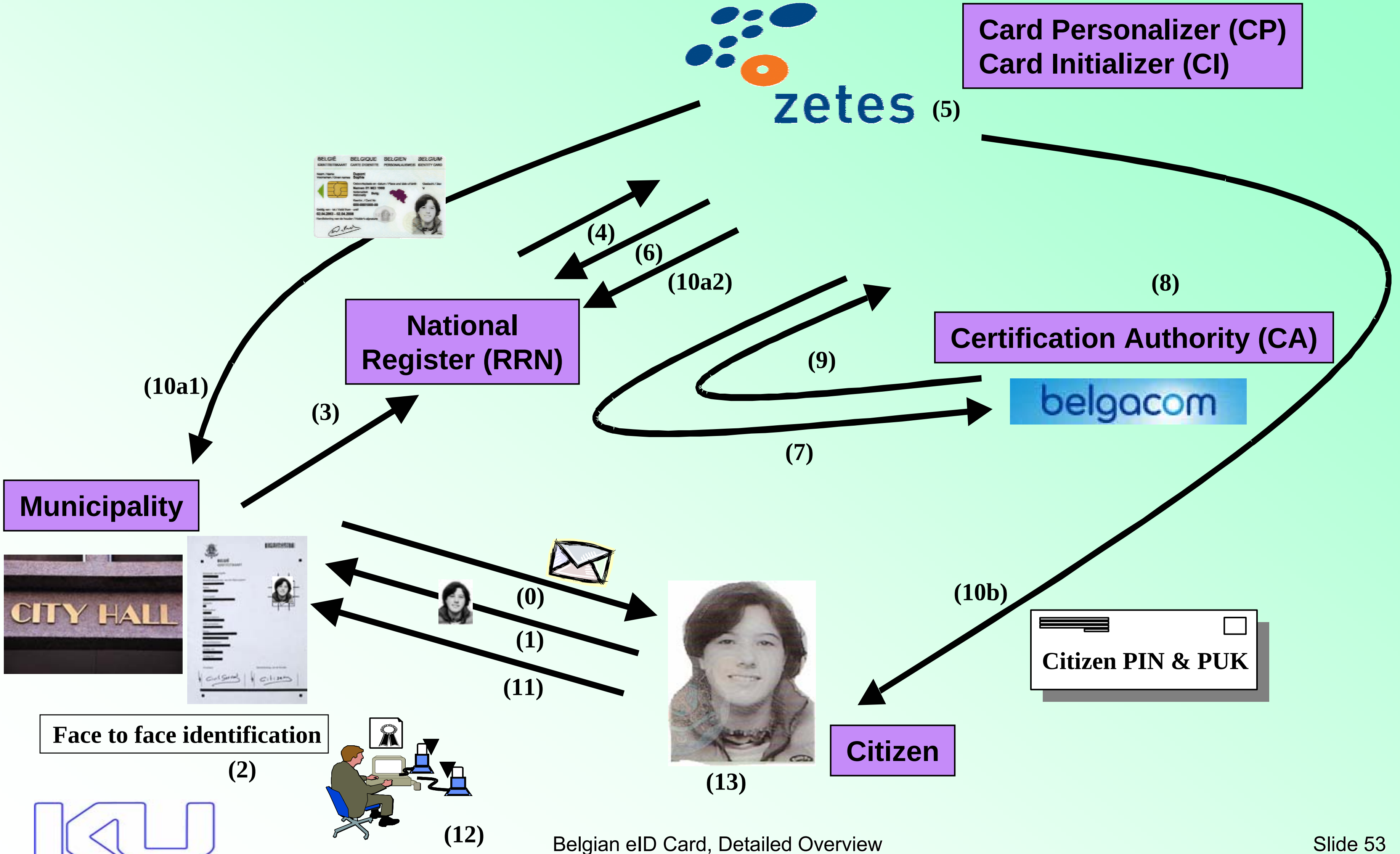
Decryption vs. Signing

- Decryption scenarios:
  - Do **not** require encryption certificates
  - An eID card does **not** support decryption functionality
  - Encryption key management is totally different from signing key management:
    - Lost or damaged eID card
      - ⇨ impossible to access encrypted data
    - Signing certificates are pushed to the message receiver
    - Encryption keys are pulled from the message receiver

	Key pair generation	Private key operation	Certificate distribution	Private key archival
Authentication	On-card	Sign	Signer sends certificate	Impossible
Non-repudiation	On-card	Sign	Signer sends certificate	Impossible
Confidentiality	Software	Decrypt	Encrypter obtains encryption key	Necessity or Key escrow

eID Card Issuing Procedure

eID Card Issuing Procedure (1/2)



Card Personalizer (CP)
Card Initializer (CI)

National Register (RRN)

Certification Authority (CA)

Municipality

Citizen

Citizen PIN & PUK

Face to face identification

eID Card Issuing Procedure (2/2)

0: Citizen receives a convocation letter or takes the initiative

1: Visit municipality with photo

2: Formal eID request is signed

3,4: CP receives eID request via RRN

5: CP prints new eID card, CI starts on-card key pairs generation

6: RRN receives part of the eID card activation code PUK1

7: CA receives certificate requests

8: CA issues two new certificates and issues new CRLs

9: CI stores these certificates on the eID card

10a: CI writes citizen data (ID, address,…) to the card, deactivates the card

10b: CI sends invitation letter with citizen's PIN and activation code PUK2

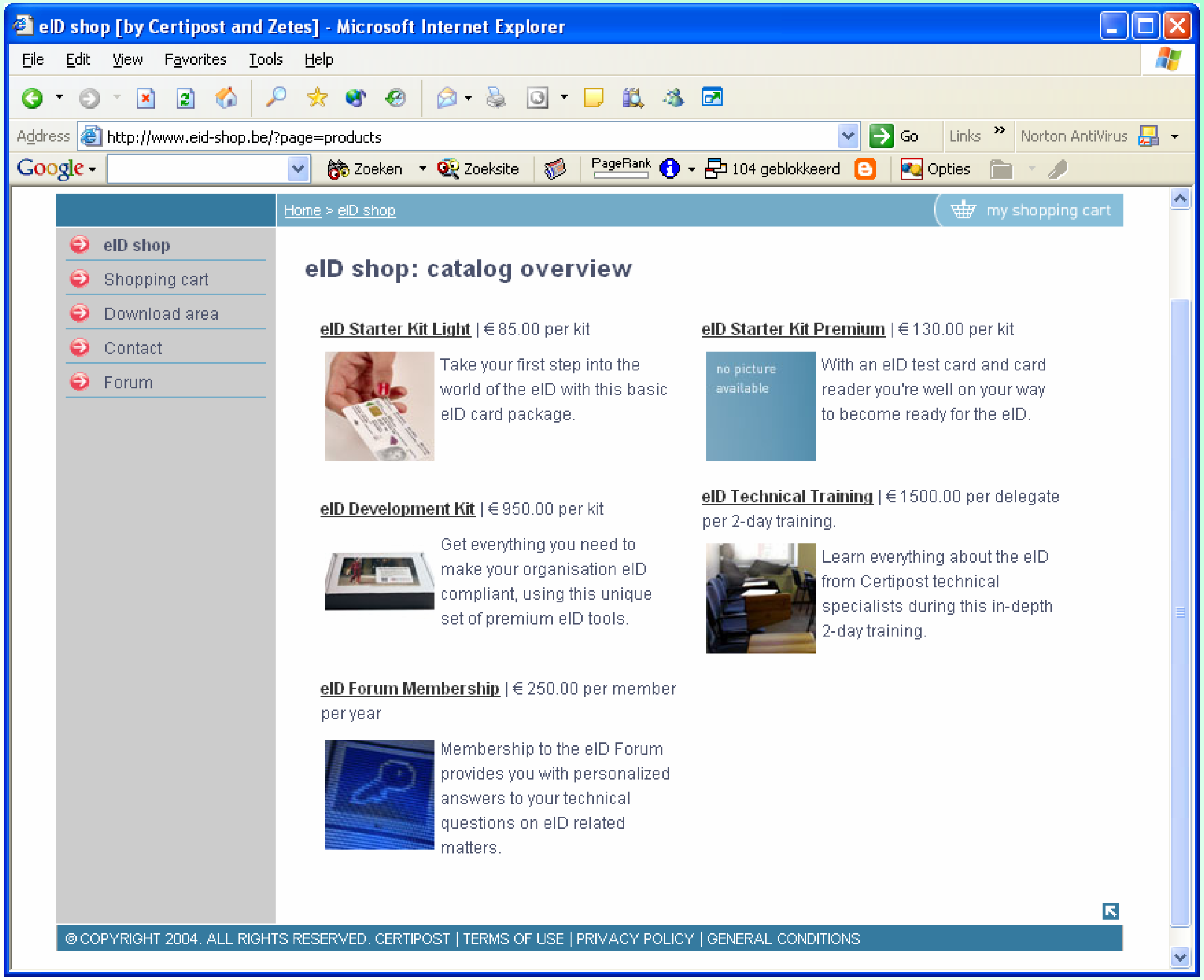
11: Citizen receives invitation letter

12: Civil servant starts eID card activation procedure

13: eID card computes a signature with each private key, CA removes certificates from CRL

eID Test Cards & Shop

eID Shop (1/2)


eID shop [by Certipost and Zetes] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://www.eid-shop.be/?page=products
Go Links Norton AntiVirus
Google Zoeken Zoeksite PageRank 104 geblokkeerd Opties
Home > eID shop
my shopping cart
eID shop
Shopping cart
Download area
Contact
Forum

eID shop: catalog overview

eID Starter Kit Light | € 85.00 per kit

Take your first step into the world of the eID with this basic eID card package.

eID Starter Kit Premium | € 130.00 per kit

no picture available

With an eID test card and card reader you're well on your way to become ready for the eID.

eID Development Kit | € 950.00 per kit

Get everything you need to make your organisation eID compliant, using this unique set of premium eID tools.

eID Technical Training | € 1500.00 per delegate per 2-day training.

Learn everything about the eID from Certipost technical specialists during this in-depth 2-day training.

eID Forum Membership | € 250.00 per member per year

Membership to the eID Forum provides you with personalized answers to your technical questions on eID related matters.

© COPYRIGHT 2004. ALL RIGHTS RESERVED. CERTIPOST | TERMS OF USE | PRIVACY POLICY | GENERAL CONDITIONS

http://www.eid-shop.be

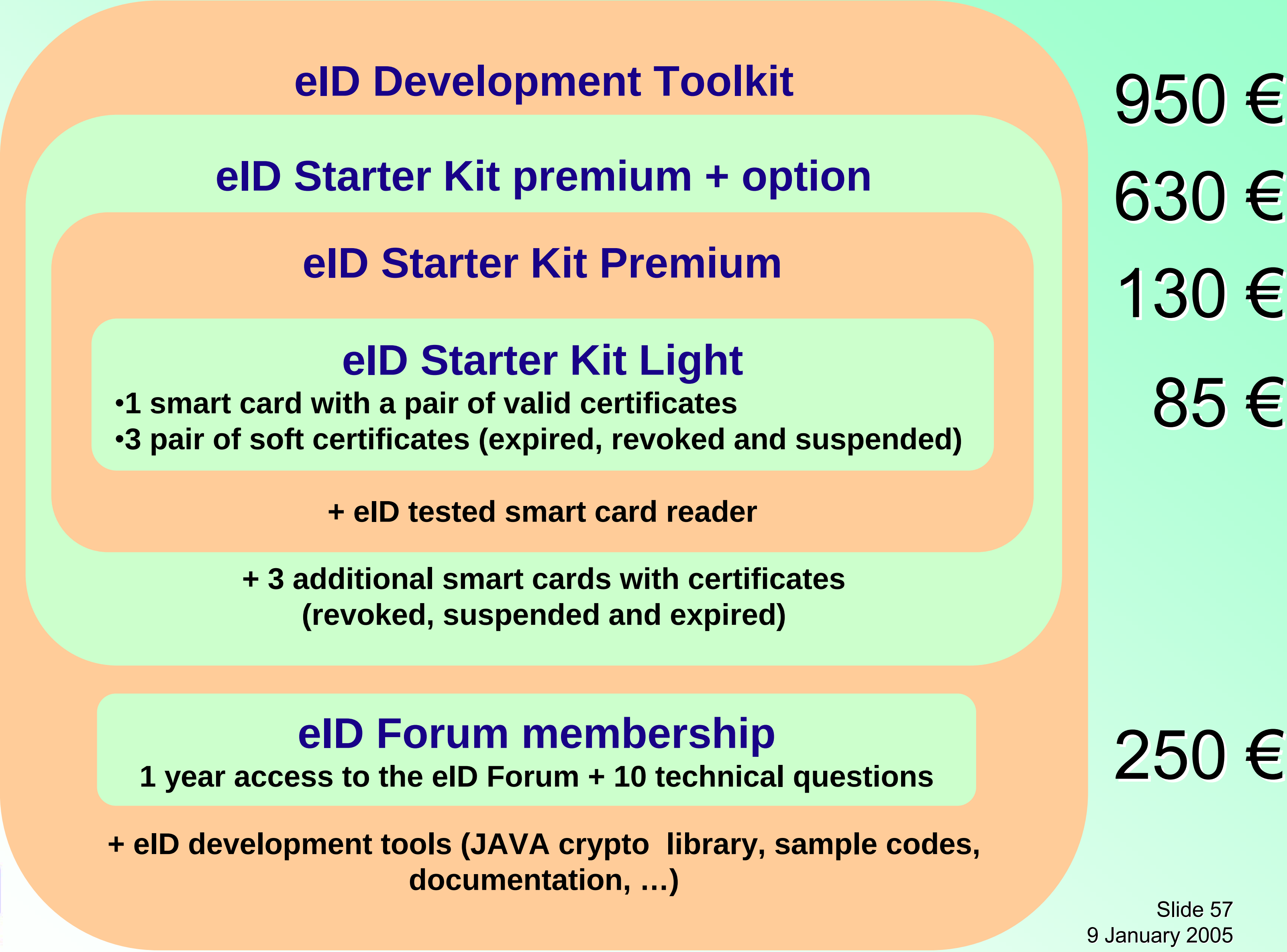
fedict e-gov

National Register
Rijksregister
Registre national

certipost
By Belgacom & De Post - La Poste

ZETES

eID Shop (2/2)



eID Development Toolkit 950 €

eID Starter Kit premium + option 630 €

eID Starter Kit Premium 130 €

eID Starter Kit Light 85 €

•1 smart card with a pair of valid certificates

•3 pair of soft certificates (expired, revoked and suspended)

+ eID tested smart card reader

+ 3 additional smart cards with certificates (revoked, suspended and expired)

eID Forum membership 250 €

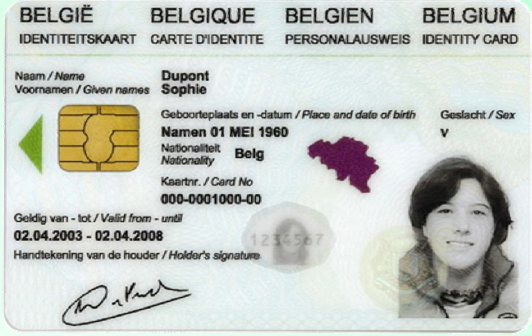
1 year access to the eID Forum + 10 technical questions

+ eID development tools (JAVA crypto library, sample codes, documentation, …)

Data used without explicit authorization from Certipost/Zetes

eID Cards vs. Bank Cards

Comparing eID and Bank Card Functionalities



BELGIË BELGIQUE BELGIEN BELGIUM

IDENTITEITSKAART CARTE D'IDENTITE PERSONALAUSWEIS IDENTITY CARD

Naam / *Name* Dupont

Voornamen / *Given names* Sophie

Geboorteplaats en -datum / *Place and date of birth* Namen 01 MEI 1960

Geslacht / *Sex* V

Nationaliteit / *Nationality* Belg

Kaartnr. / *Card No* 000-0001000-00

Geldig van - tot / *Valid from - until* 02.04.2003 - 02.04.2008

Handtekening van de houder / *Holder's signature*

1234567

- Citizen Identification
- Data Capture
- Strong Authentication
  - Authentication
  - Digital Signatures
  - eID Card
- Access Control
  - Container Park, Swimming Pool, Library,…

- Customer Identification
- Data Capture
- Authentication
  - Electronic Transactions
  - ATM Transactions
  - Electronic Purse
- Access Control
  - Self-Bank

eID & Bank Cards Crypto

- 2 Citizen Key Pairs
  - 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 eID Card-specific Key Pair
  - eID card authentication (basic key pair)
    - No corresponding certificate: RRN (Rijksregister/Registre National) knows which public key corresponds to which eID card

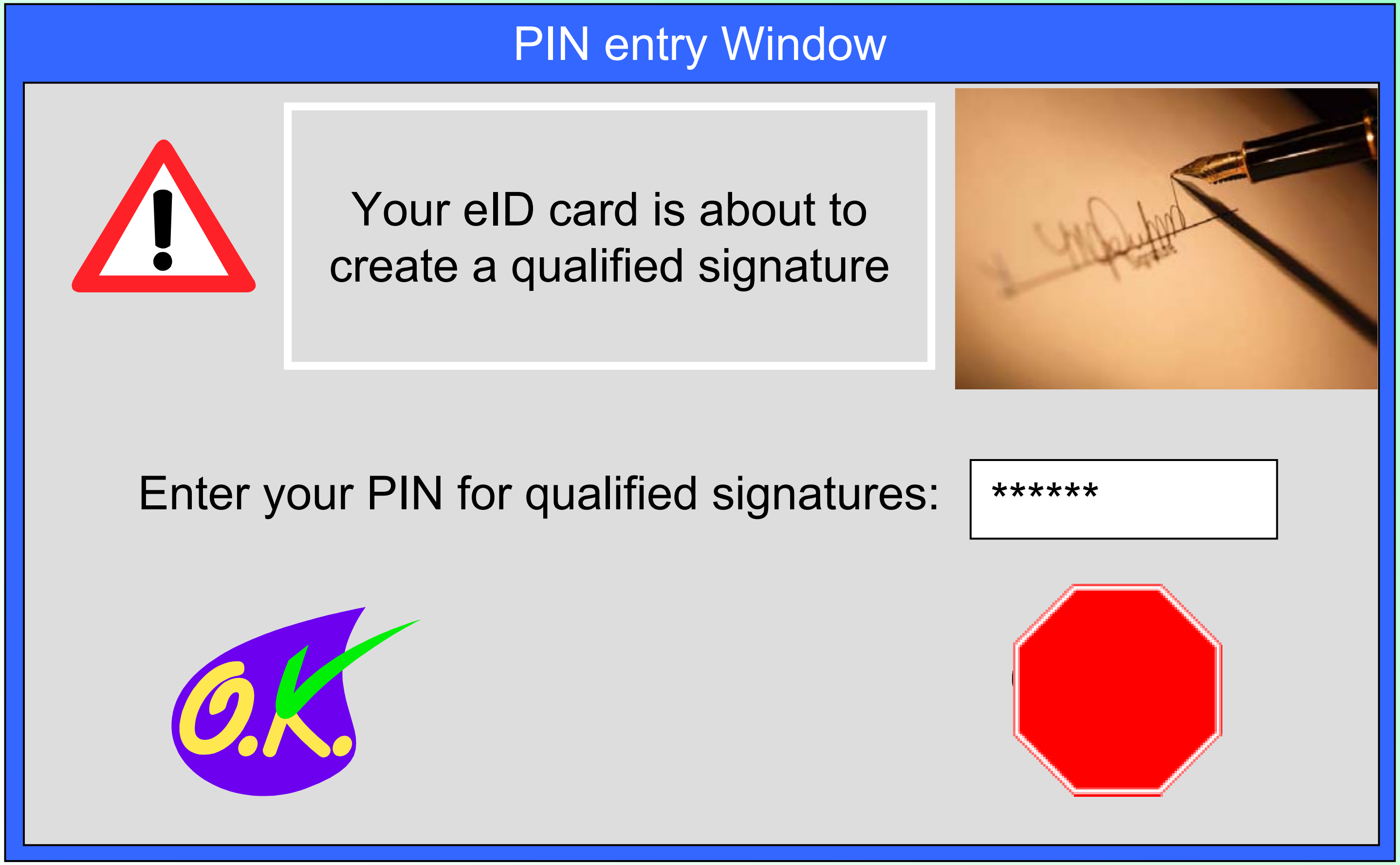
- Transactions with vending machines, ATMs, phone booths, parking meters,…
  - MAC-based use chip card
- Home banking
  - MAC-based
    - Family of secret master keys
    - Uses chip card or Digipass
    - MAC authenticates login, transaction
  - PKI-based
    - Closed user group PKI
    - Key pair stored in key file or smart card
    - Banking organization issues certificate
    - Digital signature authenticates login, transaction

Functionalities Overview

	eID	Credit	Debit	Digipass
Visual functions				
Identification	✓	Some	Some	✗
Card holder signature	✓	✓	✓	✗
Card holder picture	✓	Some	Some	✗
Electronic functions				
Data Capture	✓	✓	✓	✗
Physical Access Control	✓	✓	✓	✗
Challenge Response Authentication	✓	Some	Some	✓
Transaction Authentication	✓	✓	✓	✓
Authentication Requires	PIN	PIN	PIN	PIN
Purse Loading	NA	NA	PIN	NA
Relies on Card Reader	✓	✓	✓	Some
Cryptographic functions				
Digital Signatures	✓	Some	Some	✗
Advanced Electronic Signatures	✓	✗	✗	✗
MAC Calculation	✗	Some	✓	✓
En/Decryption	Not Yet	✗	✗	✗

Legend	
✓	Common Practice
✗	No
NA	Not Applicable

Terrifying Window

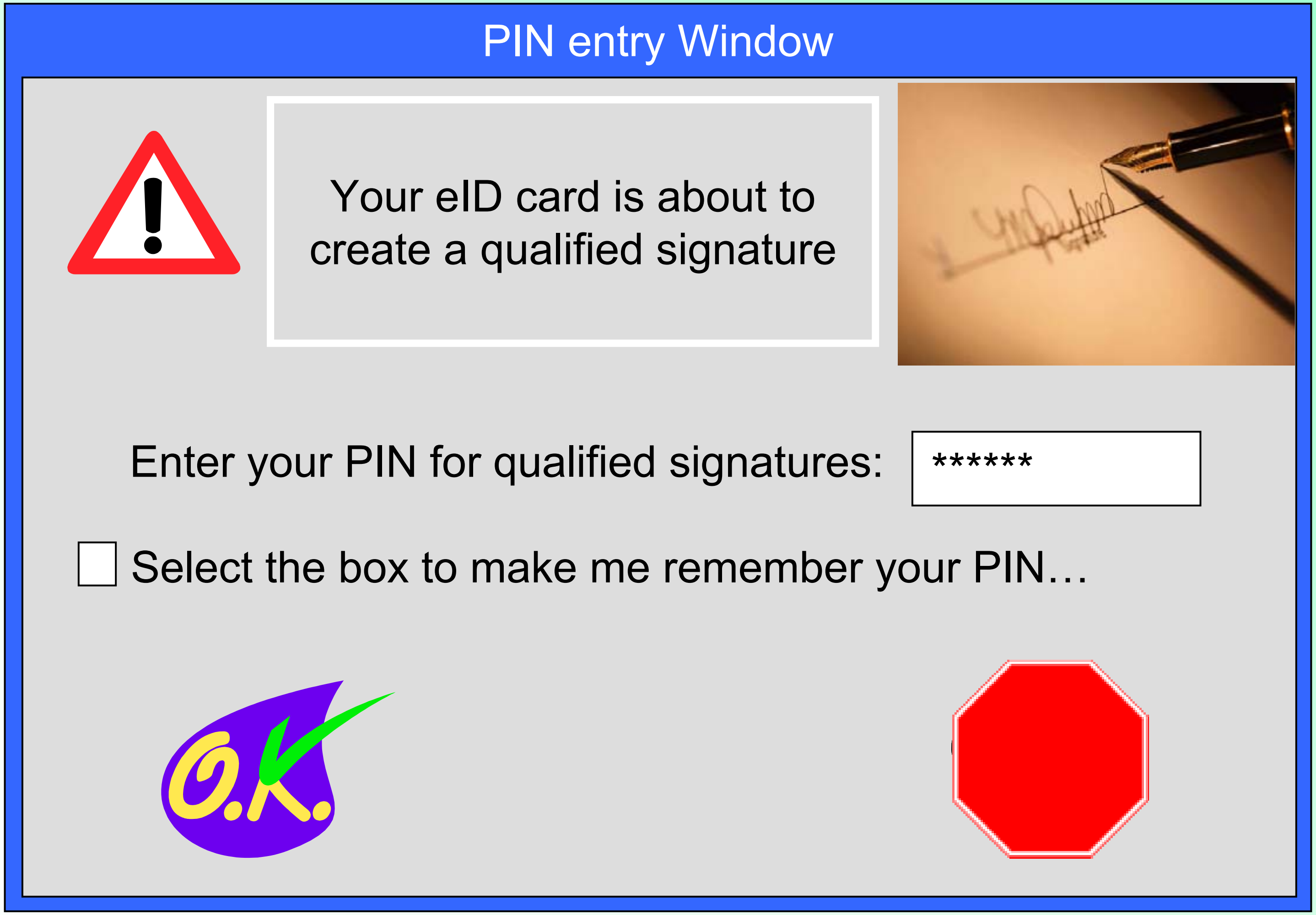


PIN entry Window

Your eID card is about to create a qualified signature

Enter your PIN for qualified signatures: ******

Most Terrifying Window



PIN entry Window

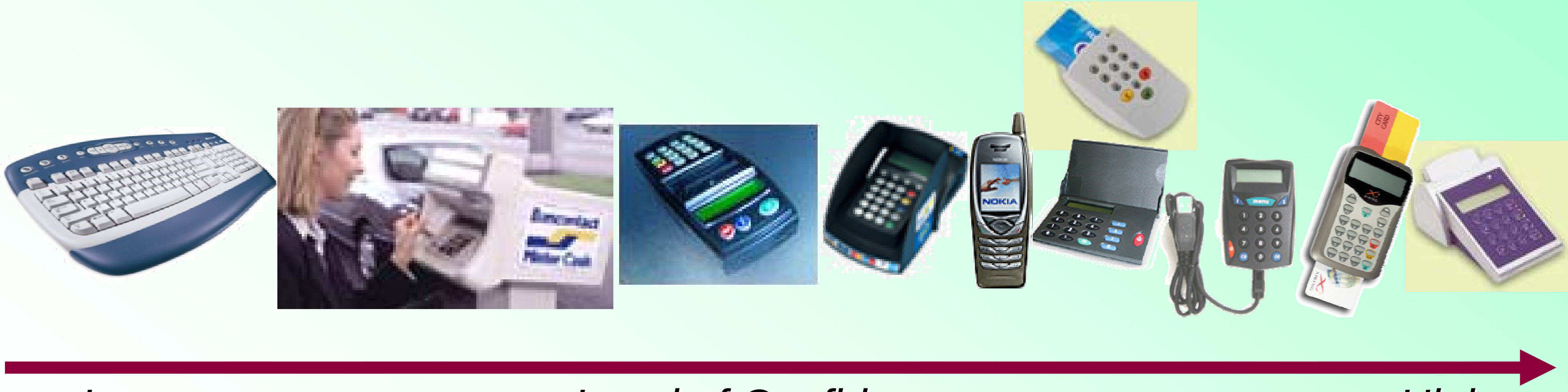
Your eID card is about to create a qualified signature

Enter your PIN for qualified signatures: ******

□ Select the box to make me remember your PIN…

Various Authentication Interfaces

- Authentication of a transaction, client authentication, digital signature,… requires a PIN to be presented to reflect the cardholder's consent



Low *Level of Confidence* *High*

Secure PIN Entry

- Advantages of a secure PIN entry device over a simple smartcard reader:
  - Citizen's PIN cannot easily be intercepted by a PC application
- Simply relying on a secure PIN entry device is not enough:
  - The text displayed on the device during a "Verify PIN" command is usually specified by the PC application
  - WYSIWYS: The cardholder does not know which data and commands are sent to the card
- Accepting a cardholder PIN through the PC keyboard should be avoided!!

WYSIWYS: what you see is what you sign

European Directive 1999/93/EC

European Directive 1999/93/EC

- Intention
- Definitions
- Requirements
  - Annex I — qualified certificates
  - Annex II — certificate service provider
  - Annex III — secure signature creation device
- Recommendations
  - Annex IV — signature verification

Directive – Intention

1. An advanced electronic signature (i.e., a signature which is linked to (s)he who created it using a signature creation device which only (s)he can control) satisfies the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and is admissible as evidence in legal proceedings
   - ⇨ Legislation on handwritten signatures can easily be recycled!!
2. An electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:
   1. in electronic form, or
   2. not based upon a qualified certificate, or
   3. not based upon a qualified certificate issued by an accredited certification-service-provider, or
   4. not created by a secure signature-creation device

Directive – Definitions

- Electronic signature: data in electronic form attached to or logically associated with other electronic data and which serve as a method of authentication
- Advanced electronic signature: an electronic signature which meets the requirements that
  1. it is uniquely linked to the signatory
  2. it is capable of identifying the signatory
  3. it is created using ***means that the signatory can maintain under his sole control***, and
  4. it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable
- Signatory: a person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents
- Signature-creation data: unique data, such as private cryptographic keys, which are used by the signatory to create an electronic signature
- Signature-creation device: configured software or hardware to produce the signature-creation data
- Secure-signature-creation device: a signature-creation device which meets the requirements specified in Annex III
- Signature-verification-data: data, such as public cryptographic keys, which are used for the verification of an electronic signature
- Certificate: an electronic attestation which links signature-verification data to a person and confirms the identity of that person
- Qualified certificate: a certificate which meets the requirements in Annex I and is provided by a certification-service-provider who fulfils the requirements in Annex II
- Certification-service-provider: an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures

Annex I – Qualified Certificates Conditions

Requirements for qualified certificates

- Qualified certificates must contain:
  1. an indication that the certificate is issued as a qualified certificate
  2. the identification of the certification-service-provider and the State in which it is established
  3. the name of the signatory or a pseudonym, which shall be identified as such
  4. provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended
  5. signature-verification data which correspond to signature-creation data under the control of the signatory
  6. an indication of the beginning and end of the period of validity of the certificate
  7. the identity code of the certificate
  8. the advanced electronic signature of the certification-service-provider issuing it
  9. limitations on the scope of use of the certificate, if applicable; and
  10. limits on the value of transactions for which the certificate can be used, if applicable

Annex II – CA Requirements

Requirements for certification-service-providers issuing qualified certificates

- Certification-service-providers must:
  1. demonstrate the reliability necessary for providing certification services
  2. ensure the operation of a prompt and secure directory and a secure and immediate revocation service
  3. ensure that the date and time when a certificate is issued or revoked can be determined precisely
  4. verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued
  5. employ personnel who possess the expert knowledge, experience, and qualifications necessary for the services provided, in particular competence at managerial level, expertise in electronic signature technology and familiarity with proper security procedures; they must also apply administrative and management procedures which are adequate and correspond to recognized standards
  6. use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them
  7. take measures against forgery of certificates, and, in cases where the certification-service-provider generates signature-creation data, guarantee confidentiality during the process of generating such data
  8. maintain sufficient financial resources to operate in conformity with the requirements in the Directive, in particular to bear the risk of liability for damages, for example, by obtaining appropriate insurance
  9. record all relevant information concerning a qualified certificate for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings. Such recording may be done electronically
  10. not store or copy signature-creation data of the person to whom the certification-service-provider provided key management services
  11. before entering into a contractual relationship with a person seeking a certificate to support his electronic signature inform that person by a durable means of communication of the precise terms and conditions regarding the use of the certificate, including any limitations on its use, the existence of a voluntary accreditation scheme and procedures for complaints and dispute settlement. Such information, which may be transmitted electronically, must be in writing and in readily understandable language. Relevant parts of this information must also be made available on request to third-parties relying on the certificate
  12. use trustworthy systems to store certificates in a verifiable form so that:
      - only authorized persons can make entries and changes,
      - information can be checked for authenticity,
      - certificates are publicly available for retrieval in only those cases for which the certificate-holder's consent has been obtained, and
      - any technical changes compromising these security requirements are apparent to the operator

Annex III – SSCD Requirements

Requirements for secure signature-creation devices:

1. Secure signature-creation devices (SSCD) must, by appropriate technical and procedural means, ensure at the least that the signature-creation data used for signature generation:
   1. can practically occur only once, and that their secrecy is reasonably assured
   2. cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology
   3. can be reliably protected by the legitimate signatory against the use of others
2. Secure signature-creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process

Annex IV – Verification Recommendations

Recommendations for secure signature verification:

- During the signature-verification process it should be ensured with reasonable certainty that:
  1. the data used for verifying the signature correspond to the data displayed to the verifier
  2. the signature is reliably verified and the result of that verification is correctly displayed
  3. the verifier can, as necessary, reliably establish the contents of the signed data
  4. the authenticity and validity of the certificate required at the time of signature verification are reliably verified
  5. the result of verification and the signatory's identity are correctly displayed
  6. the use of a pseudonym is clearly indicated; and
  7. any security-relevant changes can be detected

That’s it…

Questions?

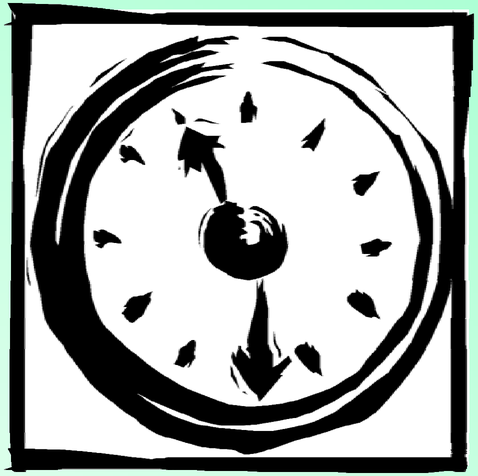
Belgian eID card information on the Internet

http://www.rijksregister.fgov.be
http://www.fedict.be
http://www.belgium.be

Google™ keywords: “godot eID”

Test cards can be ordered at

http://www.eid-shop.be



Myself Danny.DeCock@esat.kuleuven.ac.be
http://www.esat.kuleuven.ac.be/~decockd

Yourself http://www.mijndossier.rrn.fgov.be
http://www.mondossier.rrn.fgov.be
http://www.meindossier.rrn.fgov.be