WiFi Security

Danny De Cock
KU Leuven ESAT/COSIC

For Your Information ☺

- The copyright holder of this information is Danny De Cock (email: godot@godot.be), further referenced as the author
- The information expressed in this document reflects the author's personal opinions and do not represent his employer's view in any way
- All information is provided as is, without any warranty of any kind
- Use or re-use of any part of this information is only authorized for personal or not-for-profit use, and requires prior permission by the author

Typical Network Communication

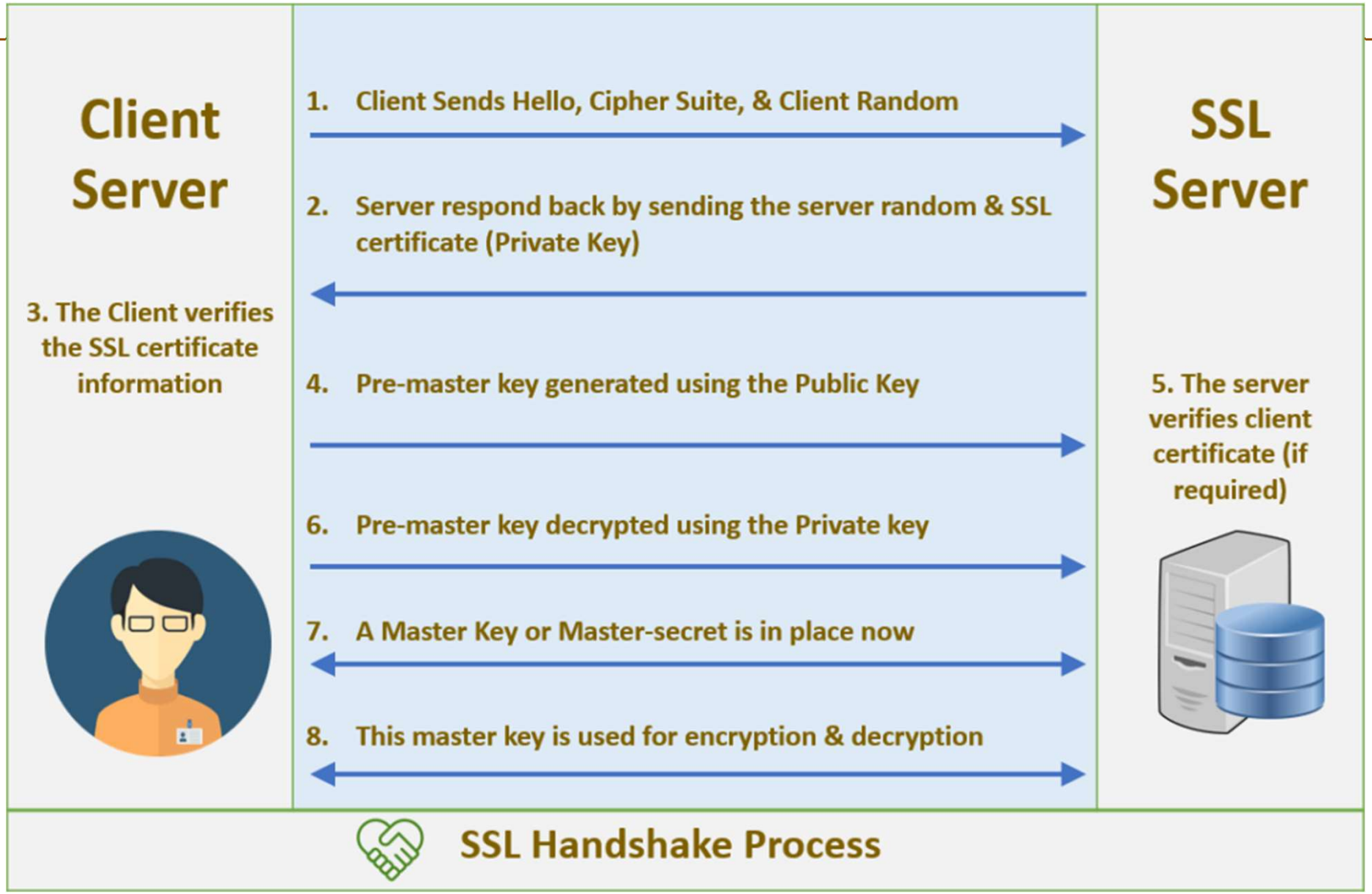
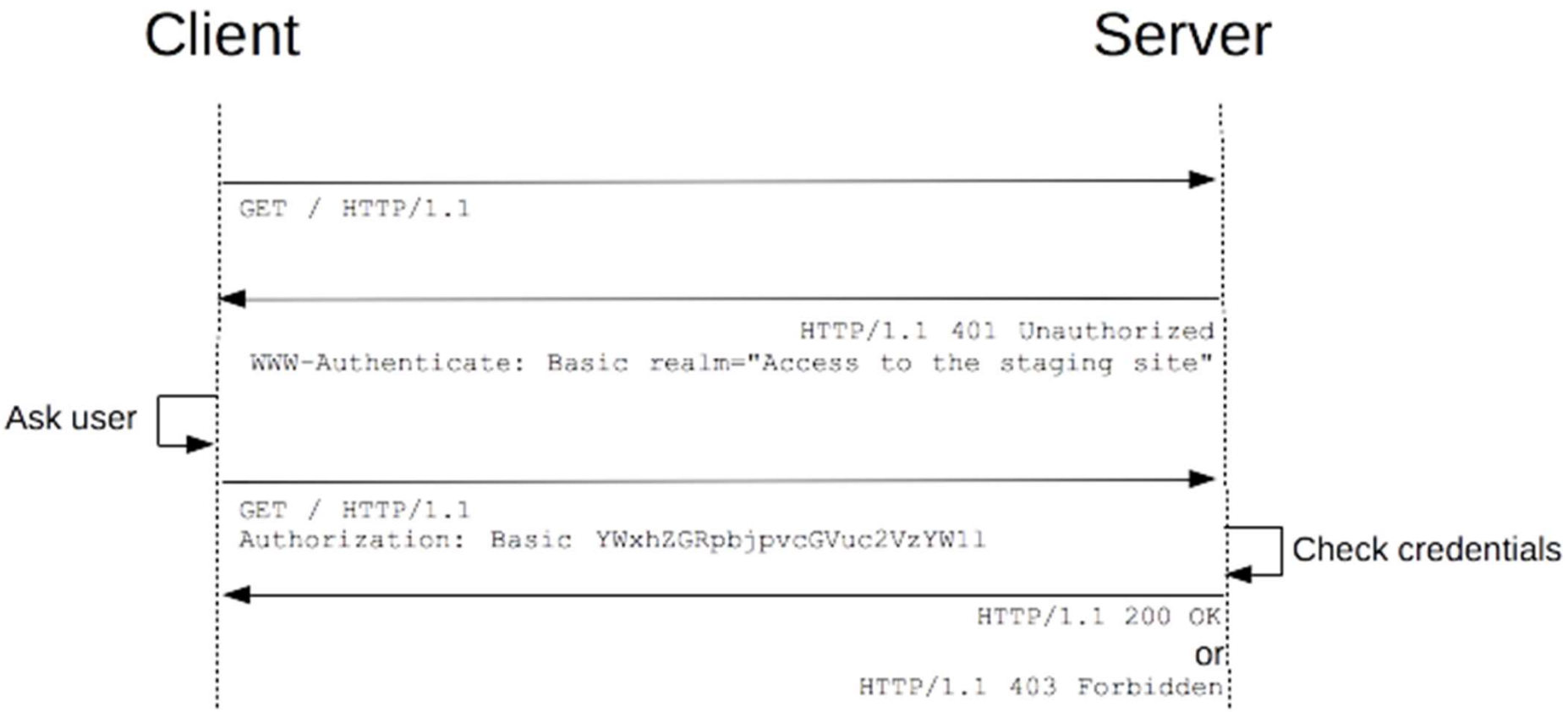


Image credits: SavvySecurity

HTTP Basic Authentication UID/PWD

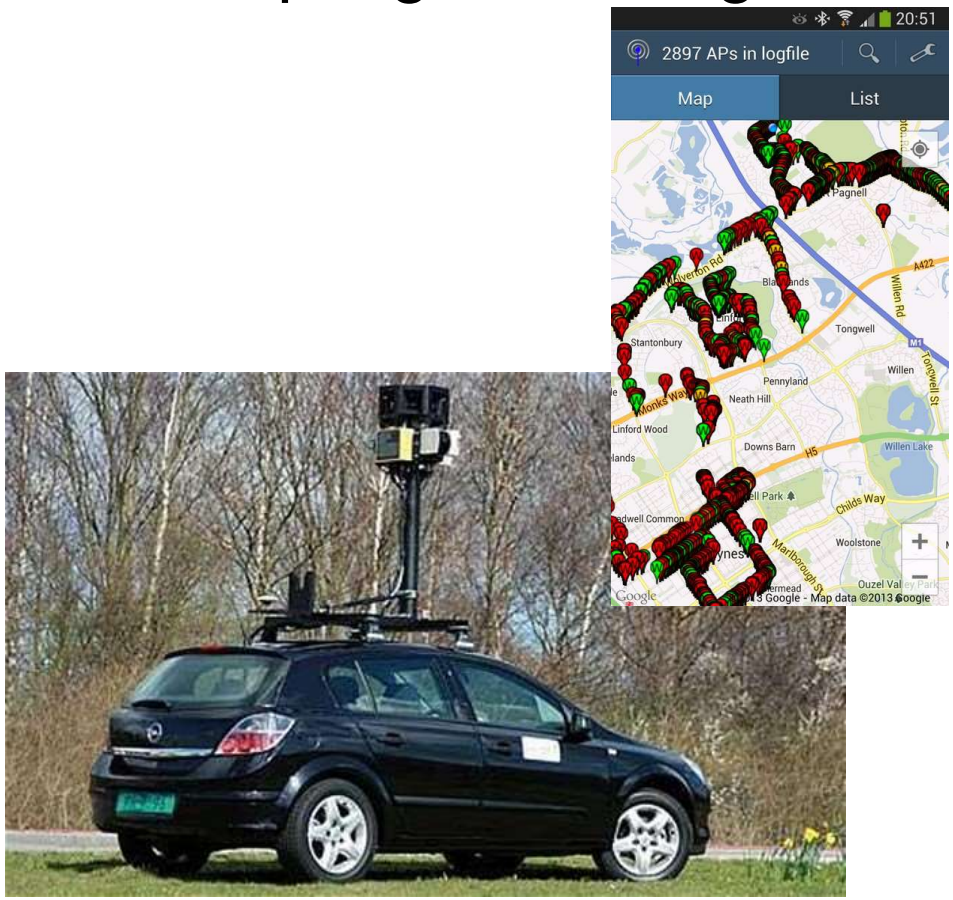



```
$ echo YWxhZGRpbjpvcGVuc2VzYW1l|base64.exe -d
aladdin:opensesame
```

Image credits: Mozilla.org

Sniffing Techniques

- Intercepting Radio Signals



- Active WiFi MITM Devices

Image credits: Google Street View Car, WiFi Pineapple Mark VII+AC Tactical

Software-only WiFi Sniffing

1. Using WireShark (win/lin/mac)
2. Using SSLsplit (lin/mac)
3. Using protocol weaknesses
    1. KRACK – broken WPA encryption
    2. Triggering four-way handshake
        1. Access point + client independently verify PSK
        2. Four-way handshake creates new encryption key
        3. Resetting nonce values fixes encryption key value
    3. Impact: sniffing the wireless wire

Belgian eID cards & ePassports

Slides available from //godot.be/slides

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

For Your Information ☺

- The copyright holder of this information is Danny De Cock (email: godot@godot.be), further referenced as the author
- The information expressed in this document reflects the author's personal opinions and do not represent his employer's view in any way
- All information is provided as is, without any warranty of any kind
- Use or re-use of any part of this information is only authorized for personal or not-for-profit use, and requires prior permission by the author

eID Evolutions

- 18xx: Napoleon introduces citizen and property registers
- 1995-: eIDs introduced in Denmark, Finland, Estonia…
- 1999: European Directive Electronic Signatures 1999/93/EC
- 1999: Belgium introduces eID, first cards issued in 2003

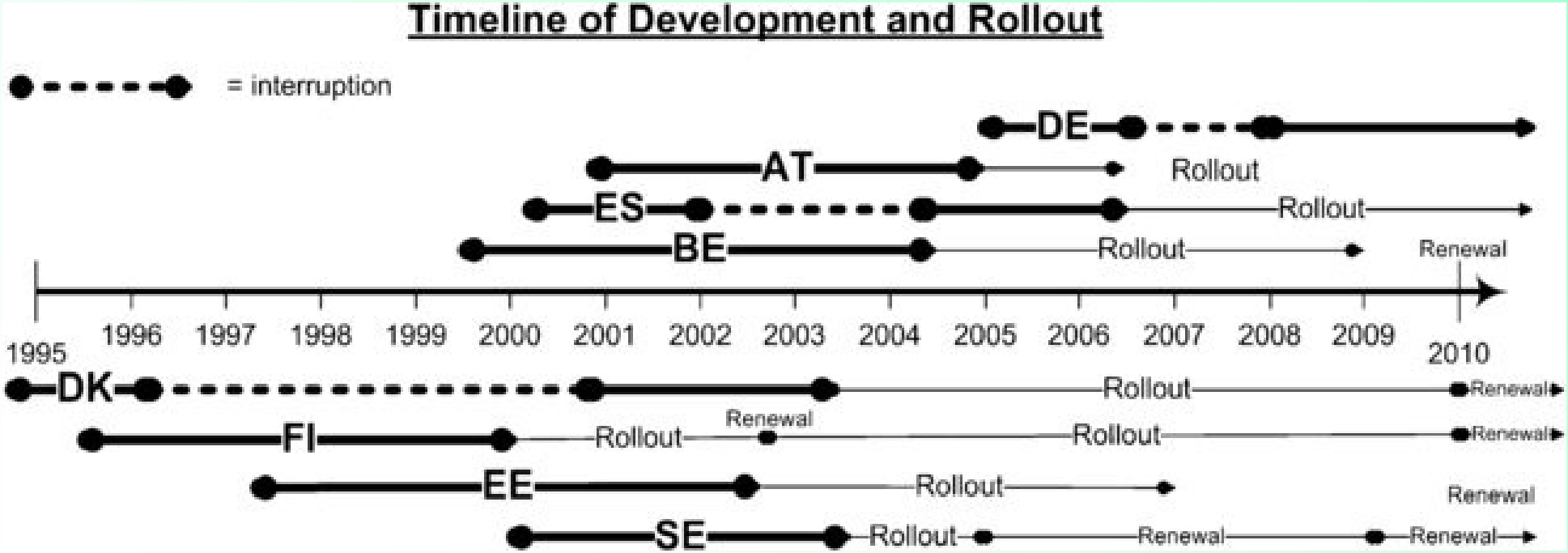
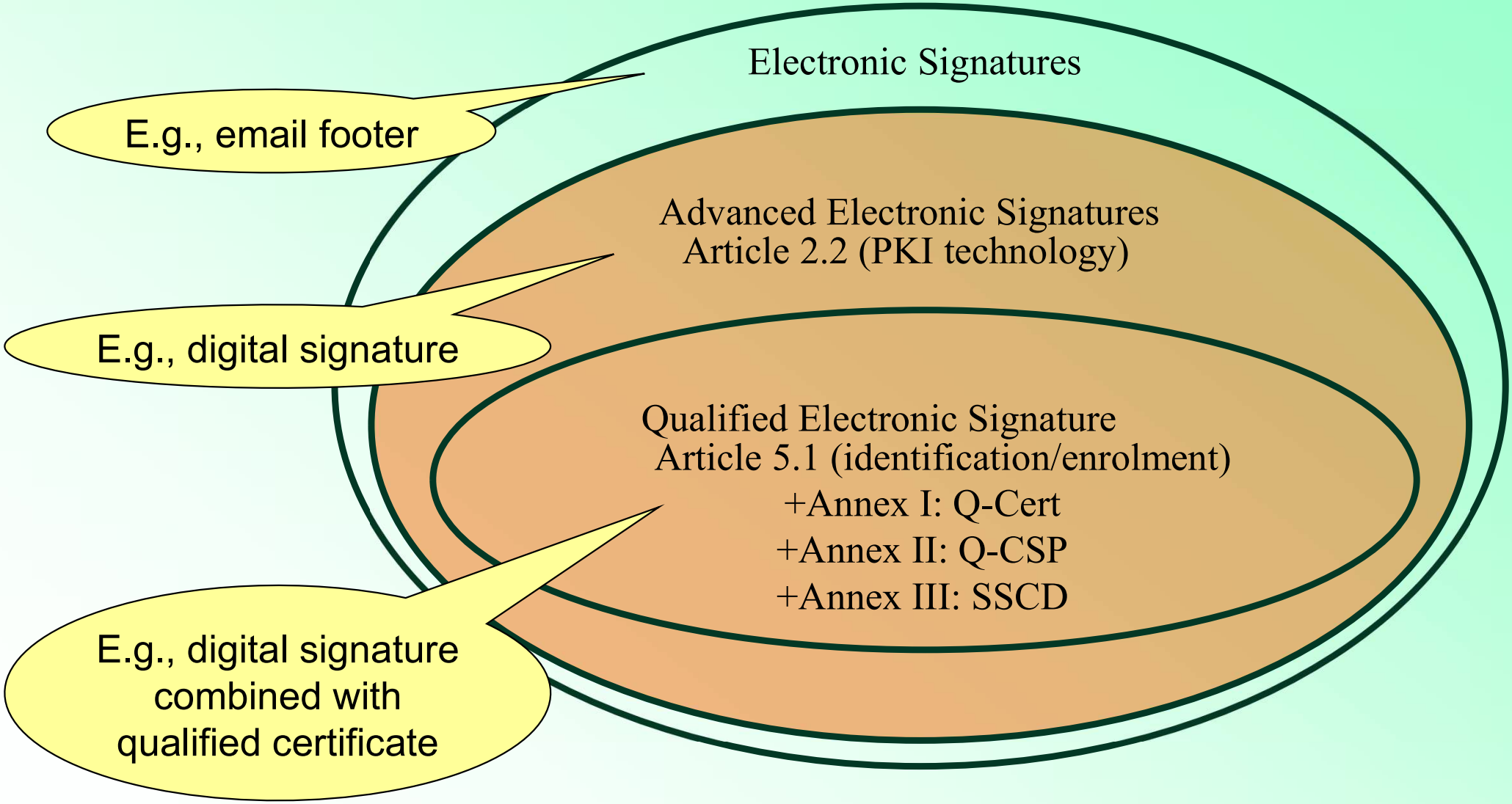


Image credits: Herbert Kubicek

eID to Digital Wallet Evolution

- 1999: European Directive Electronic Signatures 1999/93/EC
- 2014: eIDAS Regulation – interoperability framework for electronic identification, authentication and trust services
  - eID concept broadened covering people and e-services
  - Trust services, electronic signatures, qualified signatures, electronic seals, timestamps, proof of authentications…
- 2018: General Data Protection Regulation (GDPR)
- 2020: Announcement of EU Digital Identity, personal digital wallet for EU citizens, residents and businesses enabling confirmation of the right to reside, work, study…
  - Requesting birth certificates, medical certificates, opening bank account, filing tax returns, applying for university, storing medical prescriptions, proving your age, renting a car using digital driving licence, checking in to a hotel, applying for a bank loan
- 2023: Digital wallet will allow users to open bank accounts, make payments, hold digital documents like personal certificates and travel tickets
  - Ref: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_5651

Signature Types – EU Directive 1999/93/EC



Who gets an eID card?

Citizens

Kids

Aliens

eID card | Kids-ID | Foreigners' card

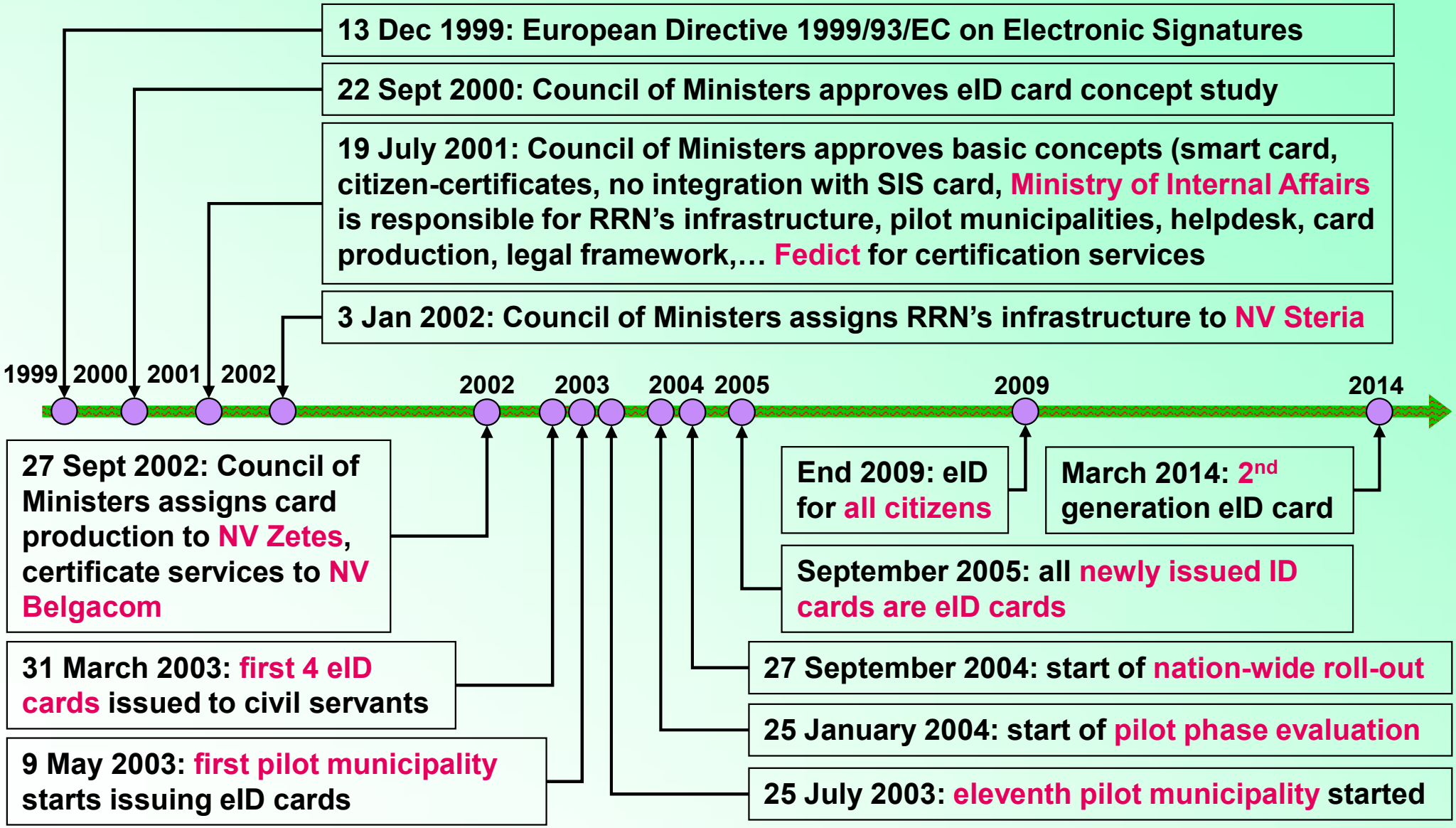
Top row: original eID card layout since 2002
Bottom row: New layout since 14 january 2020

Overview of eID Card Types

1. Belgian Kids:
   - Kids card with two revoked certificates, age < 6
   - Kids card with valid authentication & revoked non-repudiation certificate, 6 ≤ age < 12
2. Belgian youngster:
   - eID card with valid authentication & revoked non-repudiation certificate, 12 ≤ age < 18
3. Belgian adults:
   - eID card with two valid certificates, 18 ≤ age
4. Foreign youngster:
   - eID card with valid authentication & revoked non-repudiation certificate, 12 ≤ age < 18
5. Foreign adults:
   - eID card with two valid certificates, 18 ≤ age

KU LEUVEN

Belgian eID Project Time line



Visual Aspects of a Belgian eID card

Front:

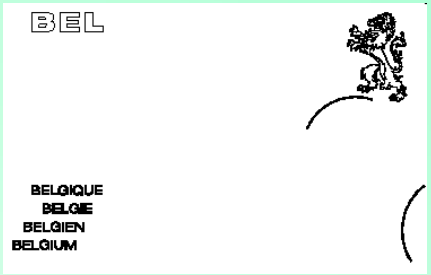
- Name
- First two names
- First letter of 3rd name
- Title
- Nationality
- Birth date
- Birth place (until 2020)
- Gender
- Card number
- Photo of the holder
- Begin and end validity dates of the card
- Hand written signature of the holder

Back side:

- Place of delivery of the card
- National Register identification number
- Handwritten signature of the civil servant (until 2020)
- Citizen's address (until 1/1/2004)
- International Civil Aviation Organization (ICAO)-specified zone (cards produced since 1/1/2005)
- QR-code: national number, card number, expiration date, birth date

Visual Security Mechanisms

- Rainbow and guilloche printing
- Changeable Laser Image (CLI)
- Optical Variable Ink (OVI)
- Alpha gram
- Relief and UV print
- Laser engraving



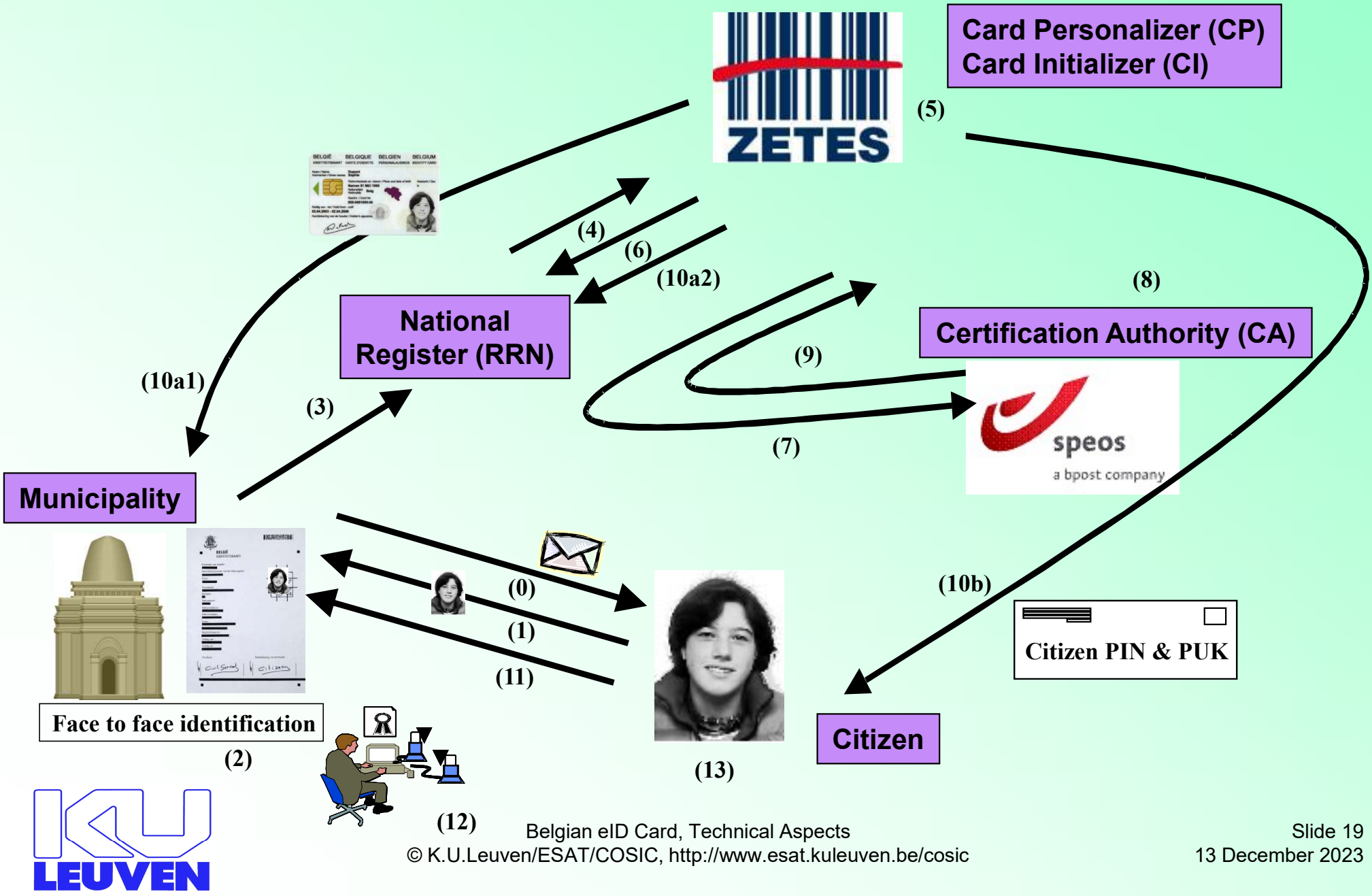
Manny Different Versions in the Field

- eID card valid for 10 years
  - Fingerprints in ICAO chip
  - All cards issued since 1 March 2014
    - Used to be 5 years
  - Now: all certificates (Root, CA, RRN, citizen): secp384r1
    - Used to be Citizen CA certificates with 4096-bit RSA key pairs
    - Used to be 1024-bit and 2048-bit RSA for first eID cards
  - Cards will be used more – increased uptake
    - More prone to physical damage to the card & chip
- Migration with Social Security Identification card?
  - No migration with SIS card
  - SIS card data fetched online
  - eID card = identification token

eID Card with Fingerprints

- eID cards issued since 2020
  - Supports ECDSA 256/384/512, GF(p)
- Nation wide issuing since 2021
  - Use: secp384r1 with NIST-curve P-384
  - Hash function: SHA-384
- European regulation 2019/1157, 20 June 2019
  - Identity cards MUST contain fingerprints
  - Identity fraud protection
- ICAO compatible chip
  - Fingerprints
  - Visual image of card holder
  - Machine Readable Zone must be read to get access to chip

eID Card Issuing Procedure (1/2)



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

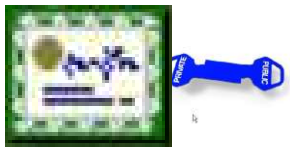
11: Citizen receives invitation letter

12: Civil servant starts eID card activation procedure

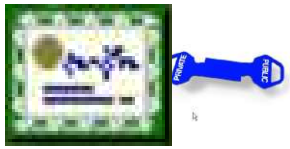
13: eID card computes a signature with each private key, CA removes certificates from CRL

eID Card Content Structure since 2002

PKI



Authentication



Signature

Root CA

CA

RRN

Citizen Identity Data

ID

ADDRESS

RRN SIGNATURE

RRN SIGNATURE

140x200 Pixels
8 BPP
3.224 Bytes

RRN = National Register

eID cards 2002-2020: Digital Identification – Identity Files

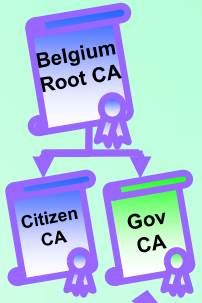
- Identity file (~160 bytes)
  - Chip-specific:
    - Chip number
  - Citizen-specific:
    - Name
    - First 2 names
    - First letter of 3rd first name
    - RRN identification number
    - Nationality
    - Birth location and date
    - Gender
    - Noble condition
    - Special status
    - SHA-1 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/kid, European community citizen/kid, non-European community citizen/kid, bootstrap card, habilitation/machtigings card



eID cards since 2020, applet 1.8v5

File contents and format

Tag (decimal)	Tag (hexadecimal)	Current max. # bytes (decimal)	Data	Encoding type	Default value	Envisioned max. # bytes (decimal)	eID	Foreigner
0	0	2	File structure version	Binary	N/A	2	✓	✓
1	1	12	Card Number	ASCII	M	12	✓	✓
2	2	16	Chip Number	Binary	M	16	✓	✓
3	3	10	Card validity date begin: ***DD.MM.YYYY***	ASCII	M	10	✓	✓
4	4	10	Card validity date end: ***DD.MM.YYYY***	ASCII	M	10	✓	✓
5	5	(42) *47	Card delivery municipality	UTF-8	M	80	✓	✓
6	6	11	National Number	ASCII	M	11	✓	✓
7	7	(62) *90	Name	UTF-8	M	110	✓	✓
8	8	(52) *75	2 first given names	UTF-8	""	95	✓	✓
9	9	3	First letter of 3rd given name	UTF-8	""	3	✓	✓
10	0A	(50) *65	Nationality	UTF-8	M	85	✓	✓
11	0B	(40) *60	Birth location	UTF-8	M	80	✓	✓
12	0C	12	Birth date: ***DD mmmm YYYY*** or ***DD.mmm.YYYY*** (German)	UTF-8	M	12	✓	✓
13	0D	1	Sex ***M***: man ***F/V/W***: woman	ASCII	M	1	✓	✓
14	0E	(21) *30	Noble condition	UTF-8	""	50	✓	✓
15	0F	2	Document type: ***1***: eID ***6***: Kids ID (< 12 years) ***7***: Bootstrap card ***8***: "Habilitation/machtigings" card ***11***: A-card ***12***: B-card ***13***: C-card ***14***: D-card ***15***: E-card ***16***: E+-card ***17***: F-card ***18***: F+-card ***19***: H-card ***20***: I-card [c] ***21***: J-card [c] ***22***: M-card [d] ***23***: N-card [d] ***27***: K-card[f] ***28***: L-card[f] ***31***: EU-card ***32***: EU+-card ***33***: A-card[f] ***34***: B-card[f] ***35***: F-card[f] ***36***: F+-card[f] ***61*** : kids Foreigner Card EU ***62*** : kids Foreigner Card EU+ ***63*** : kids Foreigner Card A ***64*** : kids Foreigner Card B ***65*** : kids Foreigner Card K ***66*** : kids Foreigner Card L ***67*** : kids Foreigner Card F ***68*** : kids Foreigner Card F+ ***69*** : kids Foreigner Card M	ASCII	M	2	✓	✓
16	10	1	Special status: 0: No status 1: White cane (blind people) [a] 2: Extended minority [a] 3: White cane + extended minority [a] 4: Yellow cane (partially sighted people) [a] 5: Yellow cane + extended minority [a]	ASCII	0	2	✓	✓

eID cards since 2020, applet 1.8v5 (ctd)

17	11	48	Hash of EF(Photo)	Binary (SHA-384)	M	48	✓	✓
18	12	2	Duplicate	ASCII	0	2		✓
19	13	1	Special organisation: *1*: SHAPE [a] *2*: NATO [a] *4*: Old European blue card *5*: Researcher	ASCII	""	1		✓
20	14	0	Member of family	Boolean	absent			✓
21	15	13	Date and country of protection dd.MM.yyyy-A2[g]	ASCII	""	13		✓
22	16	1	Mentions: *7*: Labour market : unlimited [c] *8*: Labour market : limited [c] *9*: Labour market : no [c] ~~*A*: Seasonal worker~~ [c]	ASCII	""	1		✓
23	17	13	VAT number [c] xxxx.xxx.xxx	ASCII	""	13		✓
24	18	13	VAT number [c] xxxx.xxx.xxx	ASCII	""	13		✓
25	19	18	Regional file number [c]	ASCII	""	18		✓
26	1A	48	Hash of EF(Puk#1 Basic)	Binary SHA-384	M	48	✓	✓
27	1B	1	Mention: [d] **B** :Article 18(1) Agreement	ASCII	""	1		✓
28	1C	1	Mention: [d] **C** : Séjour permanent	ASCII	""	1		✓
29	1D	1	Mentions: **A:** Seasonal worker [c] **D:** Student [b,c] **E:** School pupil [b,e] **F:** Trainee [b,e] **G:** Volunteer [b,e] **H:** Au pair [b,e] **I:** Researcher [b,e] **J:** Job search [b,e]	ASCII	""	1		✓
30	1E	1	Mention: **K** : Mobility program [b,e]	ASCII	""	1		✓
31	1F	10	Date d'enregistrement (EU) / Date du séjour permanent (EU+) [h]: **DD.MM.YYYY**	ASCII	M	10		✓

[a] Present on existing cards, but not used on new cards anymore.

[b] Directive (EU) 2016/801/EU

[c] Directive 2011/98/EU

[d] Brexit withdrawal agreement

[e] Only for A-card

[f] Council Regulation (EC) 1030/2002

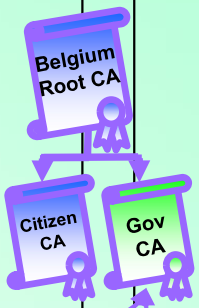
[g] A2 = Alpha-2 country code (ISO 3166)

[h] Directive 2004/38/CE

Integrity of Citizen Data

Citizen Address File (~120 bytes)

- Citizen's main address:
  - Street + number
  - Zip code
  - Municipality
- Digital signature issued by RRN

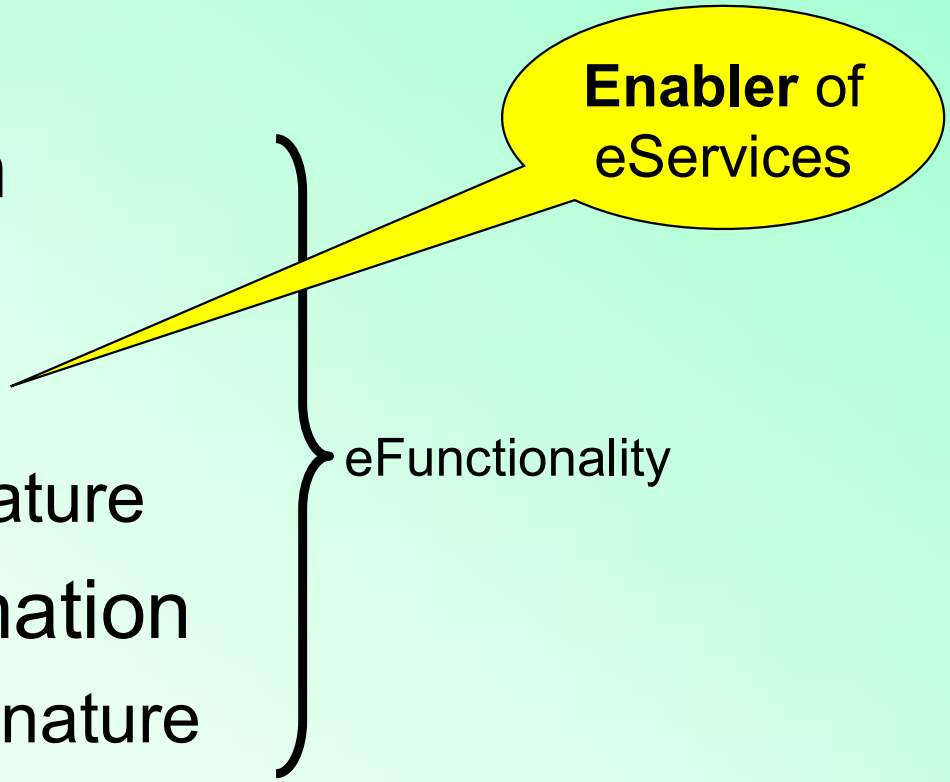


Citizen Identity File (160-752 bytes)

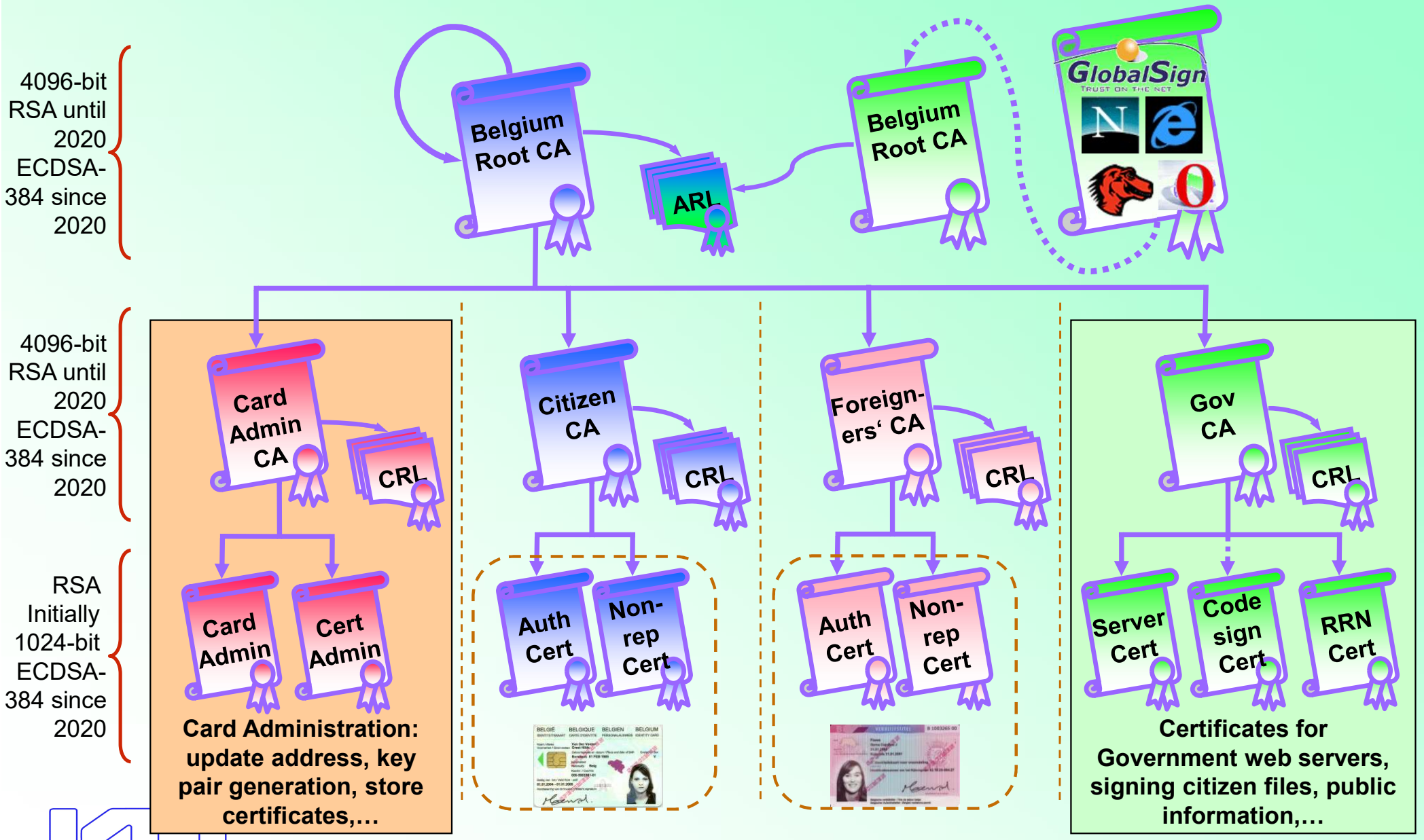
- Content:
  - Chip number
  - Name
  - First 2 names
  - First letter of 3rd first name
  - RRN identification number
  - Nationality
  - Birth location and date
  - Gender
  - Noble condition
  - Special status
  - SHA-1 or SHA-384 hash of citizen photo
  - Special organization, labor market, VAT number, cardholder type, permanent registration date
  - Card number
  - Validity's begin and end date
  - Card delivery municipality
  - Document type
- Digital signature issued by RRN
- Citizen's JPEG photo ~ 3 Kbytes

eID Card = 4 Functions

- Non-electronic
  1. Visible Identification of a person
- Electronic
  2. Digital identification
     - Data capture
  3. Prove your identity
     - Authentication signature
  4. Digitally sign information
     - Non-repudiation signature



eID Certificates Hierarchy



Certificates – Linking public keys to entities

- How does Bob know that a *public* key belongs to Alice?
- Belgian government issues a statement "this *public* key belongs to Alice"
  - Statement is called a "certificate"
  - One certificate per key pair
  - *Private* key only known to certified entity

The Belgian eID card…

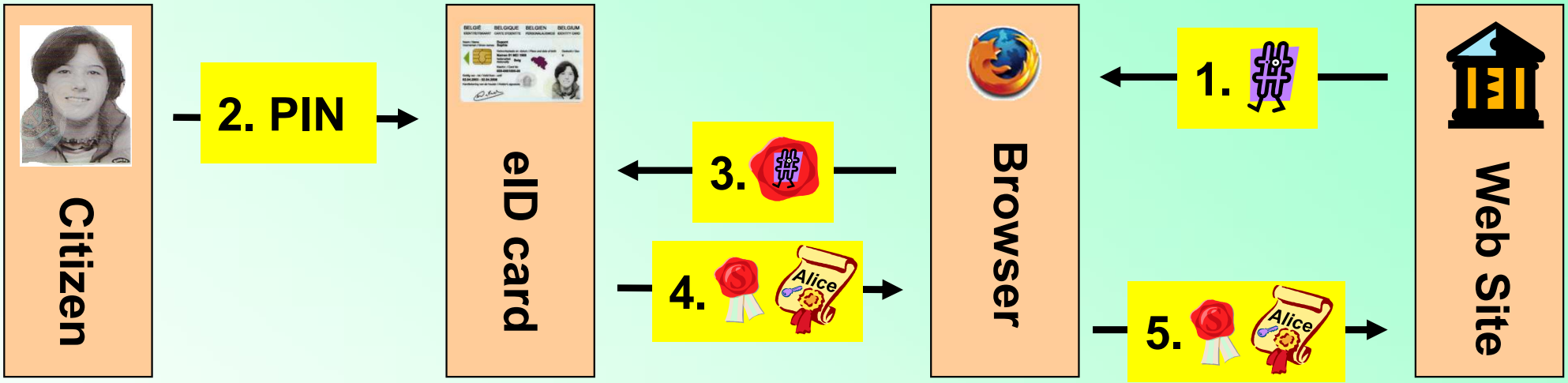
- Uses On-board key pair generation
  - Private keys cannot leave the eID card
  - Key pair generation is activated during the initialization of the eID card
- Uses JavaCard technology
- Can be used using software/middleware – free of charge – provided the Government
- Can only be managed by the Belgian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

Signing Keys & Certificates

- Citizen-authentication
  - X.509v3 authentication certificate
- Advanced electronic signatures
  - X.509v3 qualified certificate
  - Can be used to produce digital signatures equivalent to handwritten signatures, cf. European Directive 1999/93/EC
- eID card authentication
  - No corresponding certificate
  - Used for eID card administration

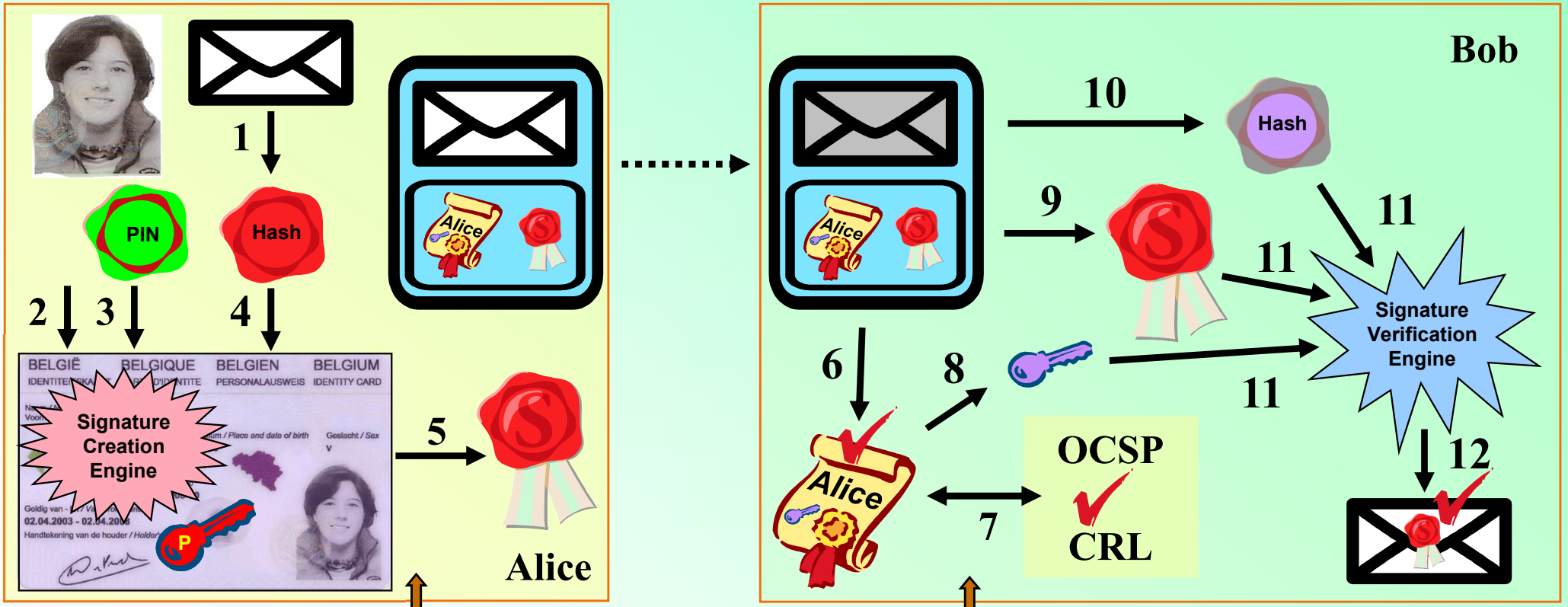
Using an Authentication Certificate

Case study: Alice visits a website which uses client authentication



1. The web server Alice visits sends a random challenge to her browser
2. Alice confirms she wants to log in on the web site by presenting her PIN to her eID card and authorizes the signature generation
3. The browser sends the hashed challenge to Alice's eID card to sign it
4. The browser retrieves the signature and Alice's certificate from her eID card
5. The web server receives Alice's signature and certificate

Signature Generation/Verification

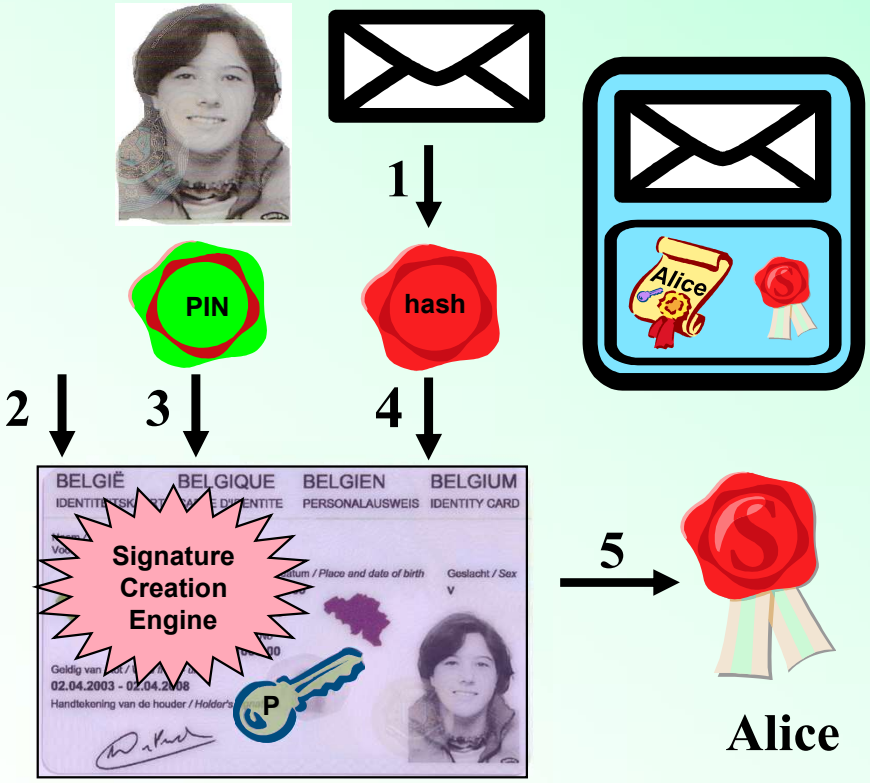


1. Compute hash of message
2. Prepare signature
3. Present user PIN
4. SCD generates digital signature
5. Collect digital signature

6. Retrieve signer certificate
7. Verify the certificate's revocation status
8. Retrieve public key from signer certificate
9. Retrieve digital signature on the message
10. Compute hash on received message
11. Verify digital signature
12. SVD outputs 'valid signature' or 'invalid signature'

Beware – Bob should validate Alice's certificate – Beware

Signature Generation Steps



Alice's application

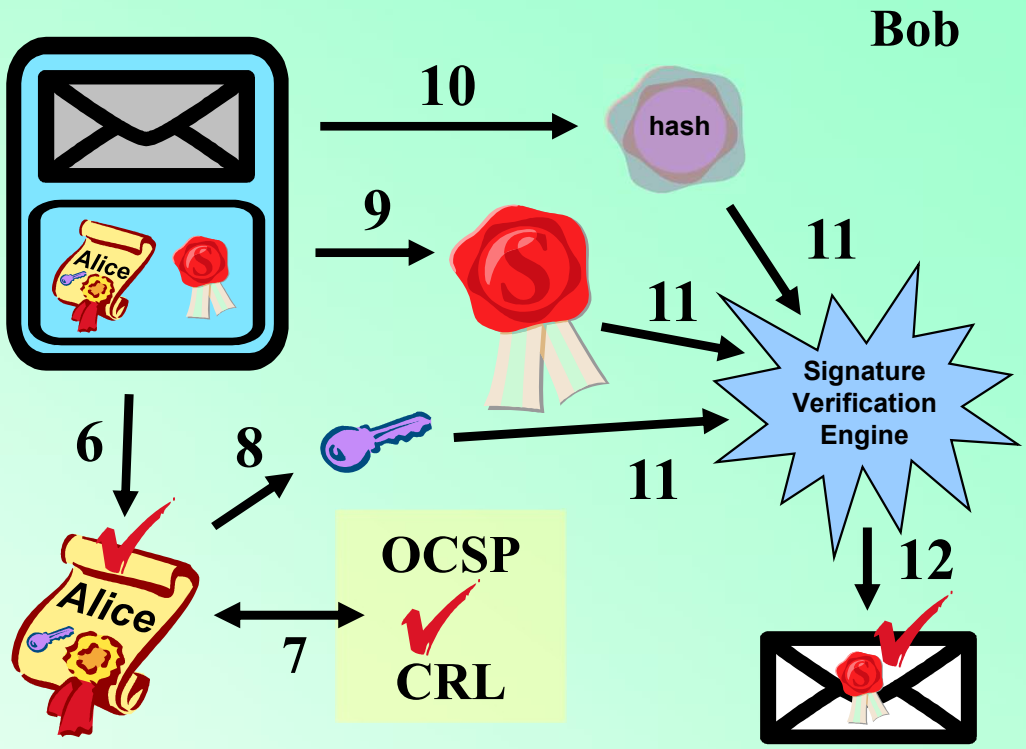
1. Calculates the cryptographic hash on the data to be signed
2. Prepares her eID card to generate an authentication signature or to generate a non-repudiation signature
3. Alice presents her PIN to her eID card
4. Her card generates the digital signature on the cryptographic hash
5. The application collects the digital signature from her eID card

Bob receives an envelope with a digitally signed message and a certificate

Signature Verification Steps

Bob

6. Retrieves the potential sender's certificate
7. Verifies the certificate's revocation status
8. Extracts Alice's public key from her certificate
9. Retrieves the signature from the message
10. Calculates the hash on the received message
11. Verifies the digital signature with the public key and the hash
12. If the verification succeeds, Bob knows that the eID card of Alice was used to produce the digital signature



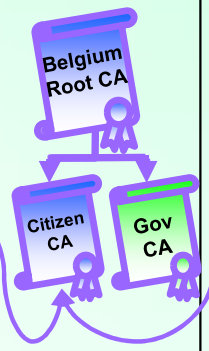
"*The message comes from Alice*" is a business decision

Original 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, SN=200501
Not valid before: Apr 2 22:41:00 2005 GMT
Not valid after: Apr 2 22:41:00 2010 GMT
Subject: C=BE, CN=Sophie Dupont (Signature), SN=Dupont, GN=Sophie Nicole/ serialNumber=60050100295
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, SN=200501
Not valid before: Apr 2 22:40:52 2005 GMT
Not valid after: Apr 2 22:40:52 2010 GMT
Subject: C=BE, CN=Sophie Dupont (Authentication), SN=Dupont, GN=Sophie Nicole/ serialNumber=60050100295
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]

Original 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

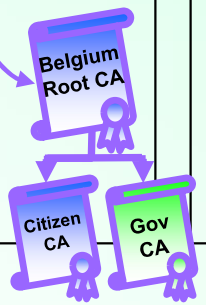
Signature: [c8:6d:22: … :43:2a]

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: 2.16.56.1.1.2
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]



Original 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

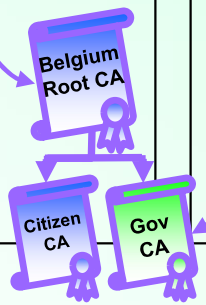
Signature: [a0:53:21: … :1d:c9]

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]



Root and Citizen CA Certificates since 2020

```
Belgium Root CA6 Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
71:8b:57:ff:6b:69:3e:5a:1c:23:5e:d8:87:a3:ef:51:f4:01:0f:26
        Signature Algorithm: ecdsa-with-SHA384
        Issuer: C = BE, L = Brussels, O = Kingdom of Belgium -
Federal Government, OU = FPS Home Affairs - BIK-GCI (NTRBE-
0362475538), OU = FPS Policy and Support - BOSA (NTRBE-0671516647),
CN = Belgium Ro
ot CA6
        Validity
            Not Before: Jun  3 10:01:31 2020 GMT
            Not After : Jun  3 10:01:31 2040 GMT
        Subject: C = BE, L = Brussels, O = Kingdom of Belgium -
Federal Government, OU = FPS Home Affairs - BIK-GCI (NTRBE-
0362475538), OU = FPS Policy and Support - BOSA (NTRBE-0671516647),
CN = Belgium R
oot CA6
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (384 bit)
                pub:
                    04:79:df:60:11:68:b5:6c:3d:27:f9:3f:3f:7e:6f:
                    91:ef:68:15:cf:d2:d8
                ASN1 OID: secp384r1
                NIST CURVE: P-384
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:1
            X509v3 Authority Key Identifier:
keyid:2E:A0:88:B0:0B:0D:62:89:EC:1D:3F:D4:9F:CC:92:44:8E:48:69:46
            X509v3 Subject Key Identifier:
      2E:A0:88:B0:0B:0D:62:89:EC:1D:3F:D4:9F:CC:92:44:8E:48:69:46
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
    Signature Algorithm: ecdsa-with-SHA384
         30:66:02:31:00:b7:67:b6:bd:51:b8:fd:a3:23:22:89:1b:41:
         80:5d:28:ed:67:30:ef:eb:41:17:ee:67:bd:35
```

```
Citizen CA Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
76:c9:b9:b2:bc:ed:be:91:08:77:b5:9b:c3:53:d8:e4:a2:c5:ba:89
        Signature Algorithm: ecdsa-with-SHA384
        Issuer: C = BE, L = Brussels, O = Kingdom of Belgium -
Federal Government, OU = FPS Home Affairs - BIK-GCI (NTRBE-
0362475538), OU = FPS Policy and Support - BOSA (NTRBE-0671516647),
CN = Belgium Root CA6
        Validity
            Not Before: Dec  7 13:03:35 2022 GMT
            Not After : Dec  7 13:03:35 2034 GMT
        Subject: C = BE, L = Brussels, O = Kingdom of Belgium -
Federal Government, OU = CA/RA: FPS Home Affairs - BIK-GCI (NTRBE-
0362475538), OU = QTSP: FPS Policy and Support - BOSA (NTRBE-
0671516647), serialNumber = 202301, CN = Citizen CA
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (384 bit)
                pub:
                    04:7b:ca:2c:89:9e:1c:ba:c5:77:d9:f7:25:f2:49:
                ASN1 OID: secp384r1
                NIST CURVE: P-384
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Authority Key Identifier:
keyid:2E:A0:88:B0:0B:0D:62:89:EC:1D:3F:D4:9F:CC:92:44:8E:48:69:46
            Authority Information Access:
                CA Issuers -
URI:http://crt.eidpki.belgium.be/eid/brca6.crt
                OCSP - URI:http://ocsp.eidpki.belgium.be/eid/brca6
            X509v3 Certificate Policies:
                Policy: X509v3 Any Policy
                  CPS: https://repository.eidpki.belgium.be/eid
            X509v3 Extended Key Usage:
                TLS Web Client Authentication, E-mail Protection
            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://crl.eidpki.belgium.be/eid/brca6.crl
            X509v3 Subject Key Identifier:

A2:DD:73:1F:DD:E0:22:26:19:95:F4:80:4C:6D:A7:C3:81:EC:DA:B8
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
    Signature Algorithm: ecdsa-with-SHA384
         30:65:02:30:1a:86:6e:f5:1d:af:a9:c9:ff:06:e5:d7:26:c5:
         c0:14:f2:ab:10:ba:1d:19:70:0b:5c:8d:8d
```

Citizen Authentication and Signature Certificates since 2020

```
Authentication Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
10:00:00:00:00:00:1b:d8:26:6e:f2:c8:16:39:42:4a
        Signature Algorithm: ecdsa-with-SHA384
        Issuer: C = BE, L = Brussels, O = Kingdom of Belgium -
Federal Government, OU = CA/RA: FPS Home Affairs - BIK-GCI (NTRBE-
0362475538), OU = QTSP: FPS Policy and Support - BOSA (NTRBE-
0671516647), serialNumber = 202301, CN = Citizen CA
        Validity
            Not Before: Oct  3 16:04:27 2023 GMT
            Not After : Oct  2 16:59:59 2033 GMT
        Subject: C = BE, SN = Familienaam, GN = Voornaam,
serialNumber = 66091411253, CN = Voornaam Familienaam
(Authentication)
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (384 bit)
                ASN1 OID: secp384r1
                NIST CURVE: P-384
        X509v3 extensions:
            X509v3 Authority Key Identifier:
            Authority Information Access:
                CA Issuers -
URI:http://crt.eidpki.belgium.be/eid/eidc202301.crt
                OCSP - URI:http://ocsp.eidpki.belgium.be/eid/0
            X509v3 Freshest CRL:
                Full Name:
URI:http://crl.eidpki.belgium.be/eid/eidcd202301.crl
            X509v3 Certificate Policies:
                Policy: 2.16.56.13.6.1.1.1000
                  CPS: https://repository.eidpki.belgium.be/eid
                Policy: 0.4.0.2042.1.2
            X509v3 Extended Key Usage:
                TLS Web Client Authentication
            X509v3 CRL Distribution Points:
                Full Name:
URI:http://crl.eidpki.belgium.be/eid/eidc202301.crl
            X509v3 Subject Key Identifier
            X509v3 Key Usage: critical
                Digital Signature
    Signature Algorithm: ecdsa-with-SHA384
```

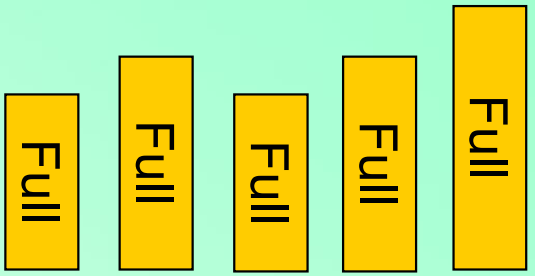
```
Signature Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
10:00:00:00:00:00:64:8c:57:e4:4d:49:01:a3:e4:6e
        Signature Algorithm: ecdsa-with-SHA384
        Issuer: C = BE, L = Brussels, O = Kingdom of Belgium -
Federal Government, OU = CA/RA: FPS Home Affairs - BIK-GCI (NTRBE-
0362475538), OU = QTSP: FPS Policy and Support - BOSA (NTRBE-
0671516647), serialNumber = 202301, CN = Citizen CA
        Validity
            Not Before: Oct  3 16:04:27 2023 GMT
            Not After : Oct  2 16:59:59 2033 GMT
        Subject: C = BE, SN = Familienaam, GN = Voornaam,
serialNumber = 66091411253, CN = Voornaam Familienaam (Signature)
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (384 bit)
                ASN1 OID: secp384r1
                NIST CURVE: P-384
        X509v3 extensions:
            X509v3 Authority Key Identifier:
            Authority Information Access:
                CA Issuers -
URI:http://crt.eidpki.belgium.be/eid/eidc202301.crt
                OCSP - URI:http://ocsp.eidpki.belgium.be/eid/0
            X509v3 Freshest CRL:
                Full Name:
URI:http://crl.eidpki.belgium.be/eid/eidcd202301.crl
            X509v3 Certificate Policies:
                Policy: 2.16.56.13.6.1.2.1000
                  CPS: https://repository.eidpki.belgium.be/eid
                  User Notice:
                    Explicit Text: De gekwalificeerde verlener van
vertrouwensdiensten is FOD BOSA / Le prestataire de services de
confiance qualifié est SPF BOSA / Den qualifizierten
Vertrauensdiensteanbieter ist FÖD BOSA
                Policy: 0.4.0.194112.1.2
            X509v3 Extended Key Usage:
                E-mail Protection
            qcStatements:
0e0.....F..0.....F..0.....F..0.....F...0:.....F..000..(https://
repository.eidpki.belgium.be/eid..en
            X509v3 CRL Distribution Points:
                Full Name:
URI:http://crl.eidpki.belgium.be/eid/eidc202301.crl
            X509v3 Subject Key Identifier:
                DC:0D:46:…59:47
            X509v3 Key Usage: critical
                Non Repudiation
    Signature Algorithm: ecdsa-with-SHA384
```

RRN Certificate since 2020

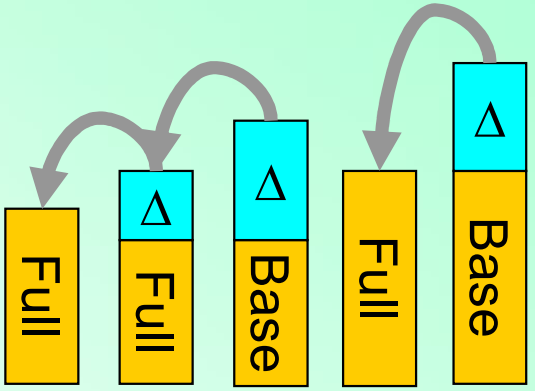
```
RRN Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 0e:67:83:42:e4:40:c9:9a:cf:fd:18:20:f2:59:8e:9b:37:b4:ce:51
    Signature Algorithm: ecdsa-with-SHA384
    Issuer: C = BE, L = Brussels, O = Kingdom of Belgium - Federal Government, OU = FPS Home Affairs -
BIK-GCI (NTRBE-0362475538), OU = FPS Policy and Support - BOSA (NTRBE-0671516647), CN = Belgium Root CA6
      Validity Not Before: Dec  7 13:08:05 2022 GMT, Not After : Dec  7 13:08:05 2034 GMT
      Subject: C = BE, O = RRN, CN = RRN
      Subject Public Key Info:
        Public Key Algorithm: id-ecPublicKey
        Public-Key: (384 bit)
          pub: 04:ae:3a:a7:c8:d5:5b:63:88:9f:24:e9:41:53:00:…:43:99:8d:f2:bb:f5:d5
          ASN1 OID: secp384r1
          NIST CURVE: P-384
      X509v3 extensions:
          X509v3 Basic Constraints: critical
              CA:FALSE
          X509v3 Authority Key Identifier:
              keyid:2E:A0:88:B0:0B:0D:62:89:EC:1D:3F:D4:9F:CC:92:44:8E:48:69:46
          X509v3 Certificate Policies: Policy: 2.16.56.13.6.0.1
              CPS: https://repository.eidpki.belgium.be/eid
          X509v3 CRL Distribution Points: Full Name: URI:http://crl.eidpki.belgium.be/eid/brca6.crl
          X509v3 Subject Key Identifier: 89:21:D1:D4:83:A4:E4:B8:AF:C0:8D:95:5F:37:F6:86:B5:72:6E
          X509v3 Key Usage: critical
              Digital Signature, Non Repudiation
    Signature Algorithm: ecdsa-with-SHA384
         30:65:02:30:77:2f:8d:9a:cf:76:71:8d:c5:57:36:2f:e8:d5:…:ec:ad:cf:ac:b8:16:ac:31:cc:30:c0:9e
```

Certificate Revocation Lists (CRLs)

- Complete CRL
  - Enumerates all certificate serial numbers that should not be trusted
  - Typically (very) large, e.g., >500 Kbytes
  - Reason codes:
    - On hold — newly issued eID card certificate is not yet activated, or has been suspended
    - None — eID card certificate has been revoked
  - Validity period expires 7 days after creation
  - 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., <20 Kbytes
  - 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
  - Validity period expires 7 days after creation



Complete CRLs

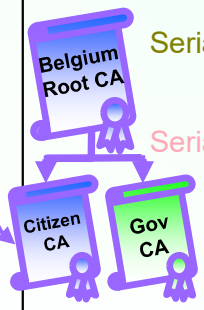


Delta CRLs vs. Base CRL

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: 1000000000000004B823FAE7B1BB44B1
Revocation Date: Jan 14 12:56:50 2004 GMT
CRL Reason Code: Certificate Hold
Serial Number: 10000000000000062F6A1BB1431902D4
Revocation Date: Oct 23 23:15:11 2003 GMT
CRL Reason Code: Certificate Hold
Serial Number: 100000000000001243778BEFF61123DE
Revocation Date: Jan 12 10:19:24 2004 GMT
Serial Number: 10000000000000125DC2DF2031534033
Revocation Date: Sep 5 09:49:44 2003 GMT
Serial Number: 100000000000091ACC84FC377F8A6ECE
Revocation Date: Dec 16 17:24:15 2003 GMT
CRL Reason Code: Certificate Hold
Serial Number: 10000000000092135CE8FB8F0D66093
Revocation Date: Nov 13 17:18:49 2003 GMT



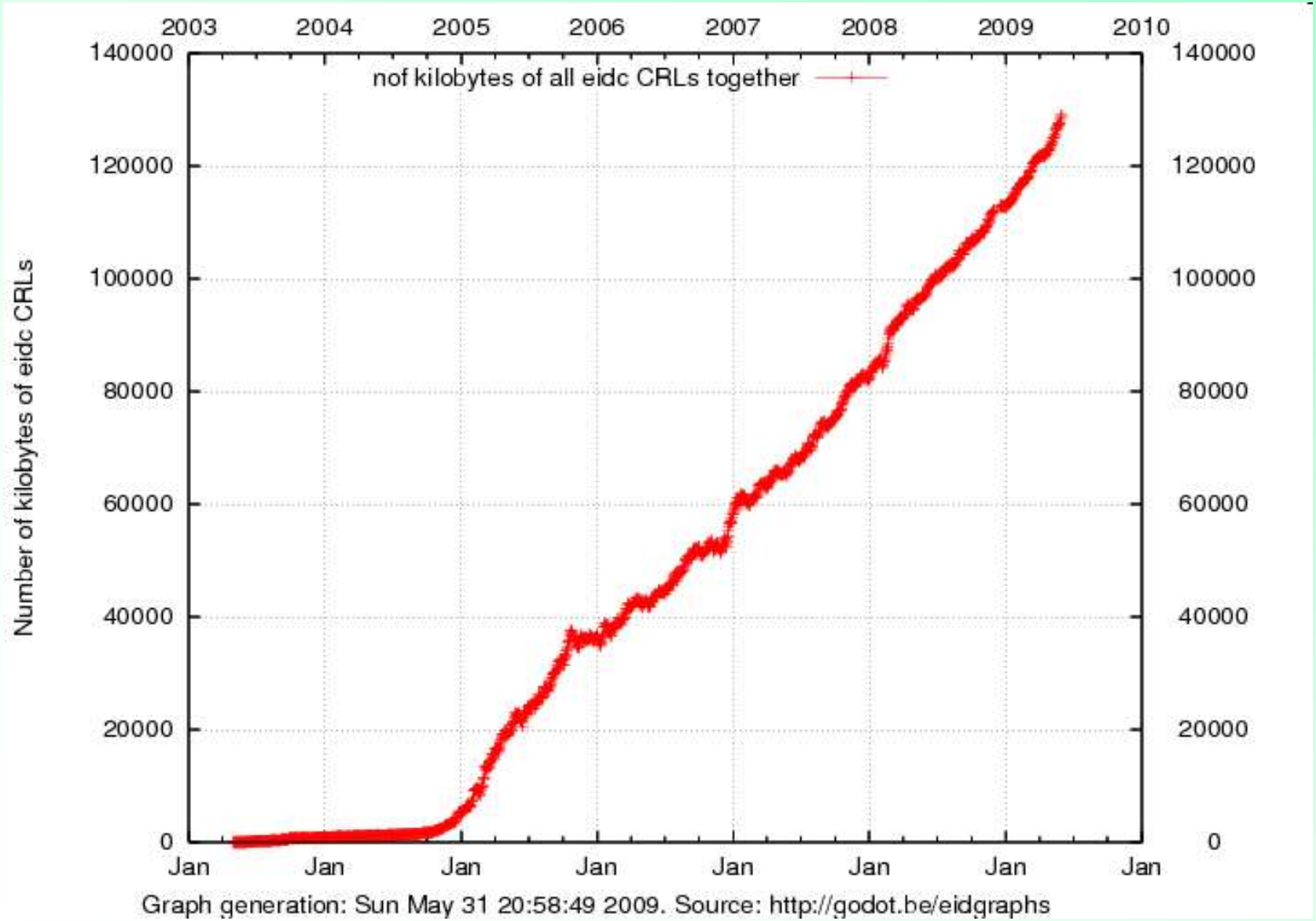
Signature: [95:19:b2: ... :21:31]

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: 100000000000007E5B11506303959320
Revocation Date: Apr 8 16:33:23 2004 GMT
CRL Reason Code: Certificate Hold
Serial Number: 100000000000091ACC84FC377F8A6ECE
Revocation Date: Apr 8 16:55:14 2004 GMT
CRL Reason Code: Remove From CRL
Serial Number: 10000000000127BE2DA18842E8A7BAC
Revocation Date: Apr 8 15:20:13 2004 GMT
CRL Reason Code: Remove From CRL
Serial Number: 1000000000001902ECF11657FE2813A5
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]

eID full CRL sizes

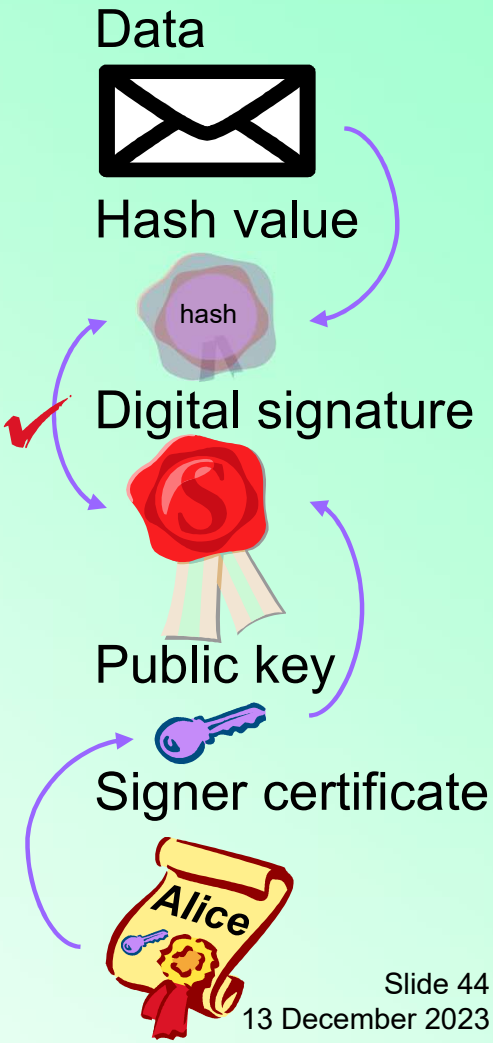


- A CRL is valid for seven days after it is issued
- A new CRL is issued together with a new Delta CRL
- A Delta CRL refers to a particular Base CRL which is always younger than 7 days
- OCSP queries the database with the most recent certificate status information
- OCSP = Online Certificate Status Protocol

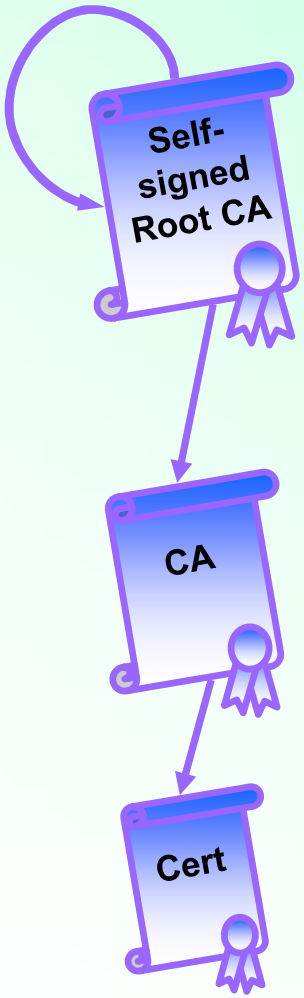
Signature Validation

- 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
- Hash function features:
  - Given a hash value of a document: hard to find a document with that hash value
  - Given a document and its hash value: hard to find a second document with the same hash value
  - Hard to find two distinct documents that have an identical hash value

Message

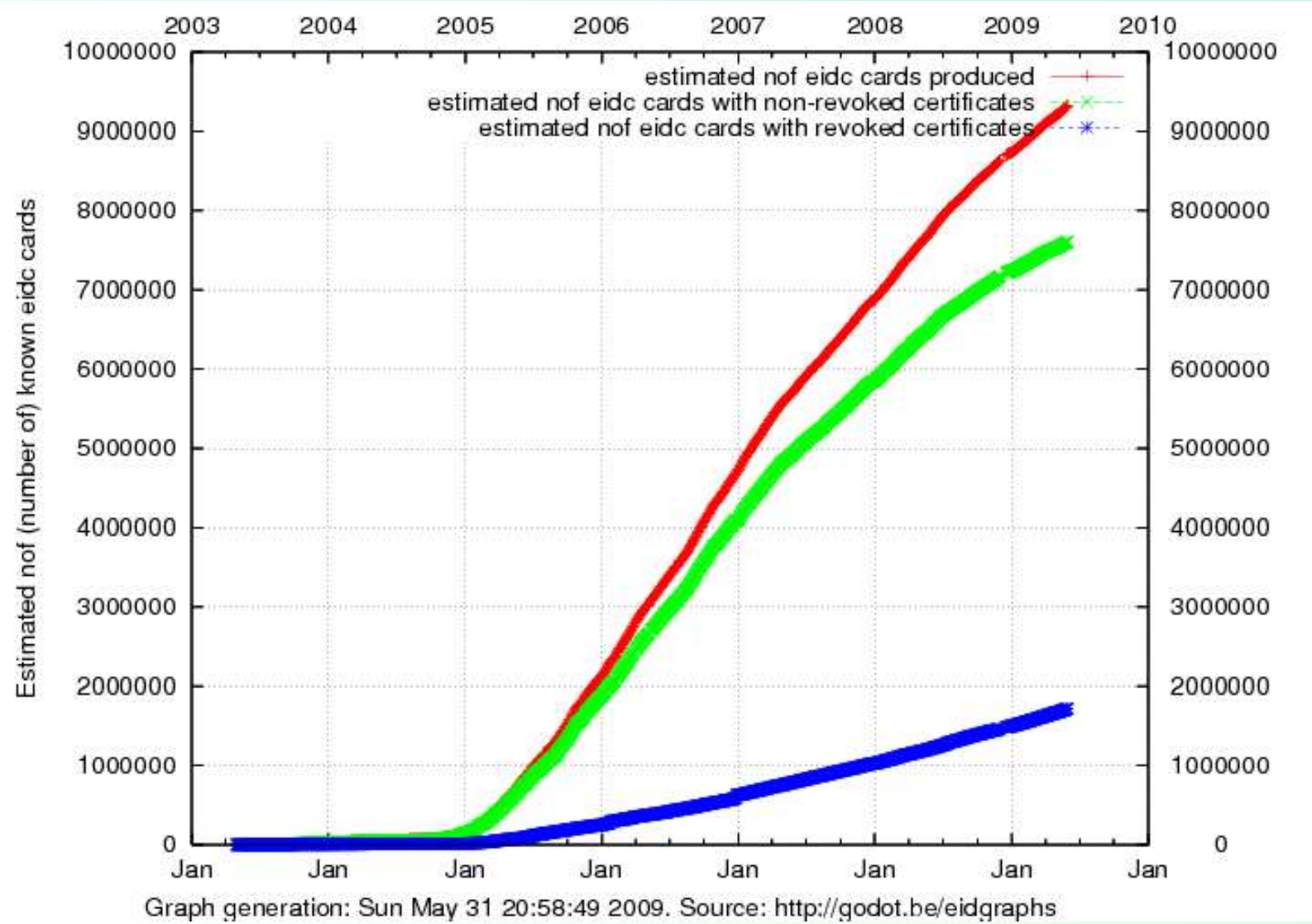


Certificate (Chain) Validation



- 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
- Certificate chain is linked with the CRLs through the Authority Key Identifier
- Valid ≠ Trustworthy
  - One should check whether the self-signed (Root CA) certificate can be trusted

eID Dissemination



- Each month: +5000 new cards produced and issued
- 10% of all citizens revoke their certificates immediately
- Majority of pilot citizens collect their eID card 1 to 3 weeks after its production
- 1/30 eID cards requested without convocation letter
- +200.000 eID card requests by citizens of a non-pilot municipality

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

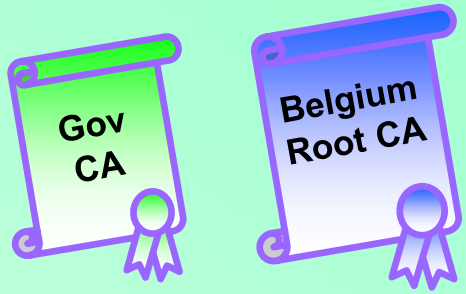
- Two options to make this business decision:
  - Do it yourself and use CRLs and Delta-CRLs
  - Trust a third party and use OCSP
- Use the Online Certificate Status Protocol (OCSP) where a trusted OCSP Responder answers the question with either "yes", "no", or "I do not know"
  - Remaining issues:
    - 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 Response?
  - 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 extremely 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 typically a few kilobytes each, but there is no standard…

About Validity Statuses…

- Digital Signature
  - Valid
  - Invalid

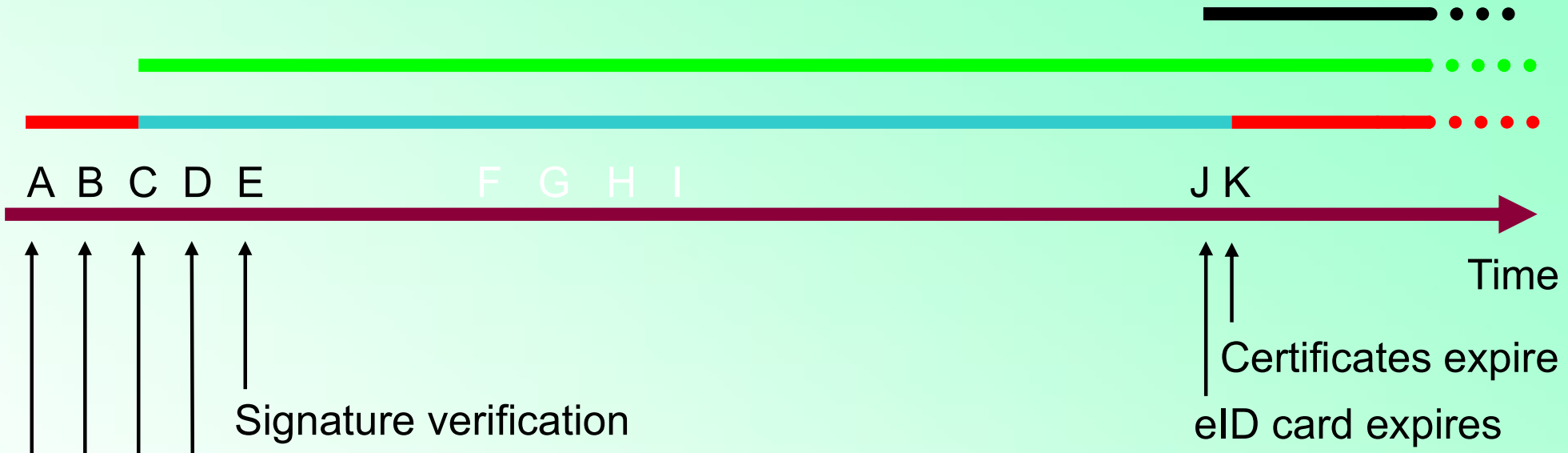
- eID Card (Signature Creation Device)
  - Valid
  - Invalid
    - Suspended
    - Revoked
    - Expired

- CRL, OCSP Response
  - Valid
  - Invalid
  - Expired



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

Signature Validity



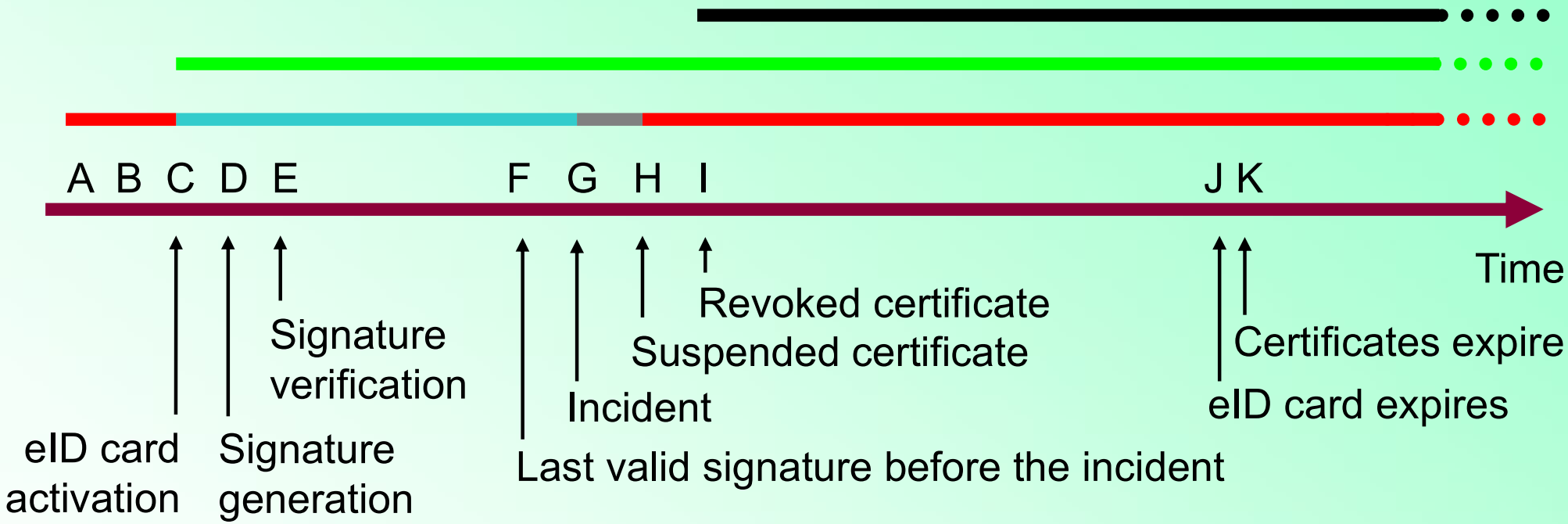
[CJ]: New valid signatures may be generated

[AC], [K,∞[: All signature verifications fail

[J,∞[: Illegal to generate new signatures

[C,∞[: Signatures can be legally binding if verified in [CJ[

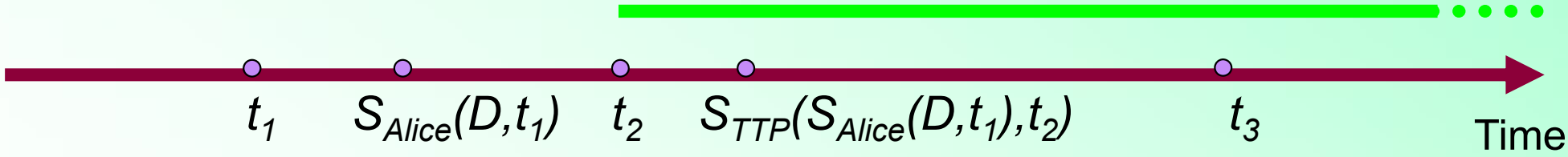
Signature Validity with Revocation



- [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

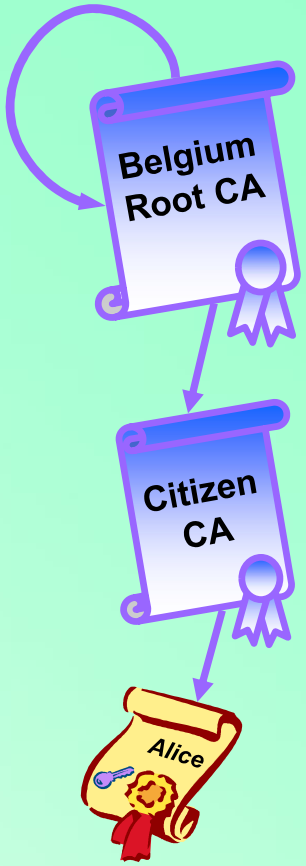
- Alice produces a digital signature on data *D* that will resist time:
  - Alice collects a time stamp t_1 from a trusted third party *(TTP)*
  - Alice produces a digital signature $S_{Alice}(D,t_1)$ on the time stamp t_1 and the data *D*
  - *TTP* validates a digital signature $S_{Alice}(D,t_1)$ at 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

Archiving Signed Data

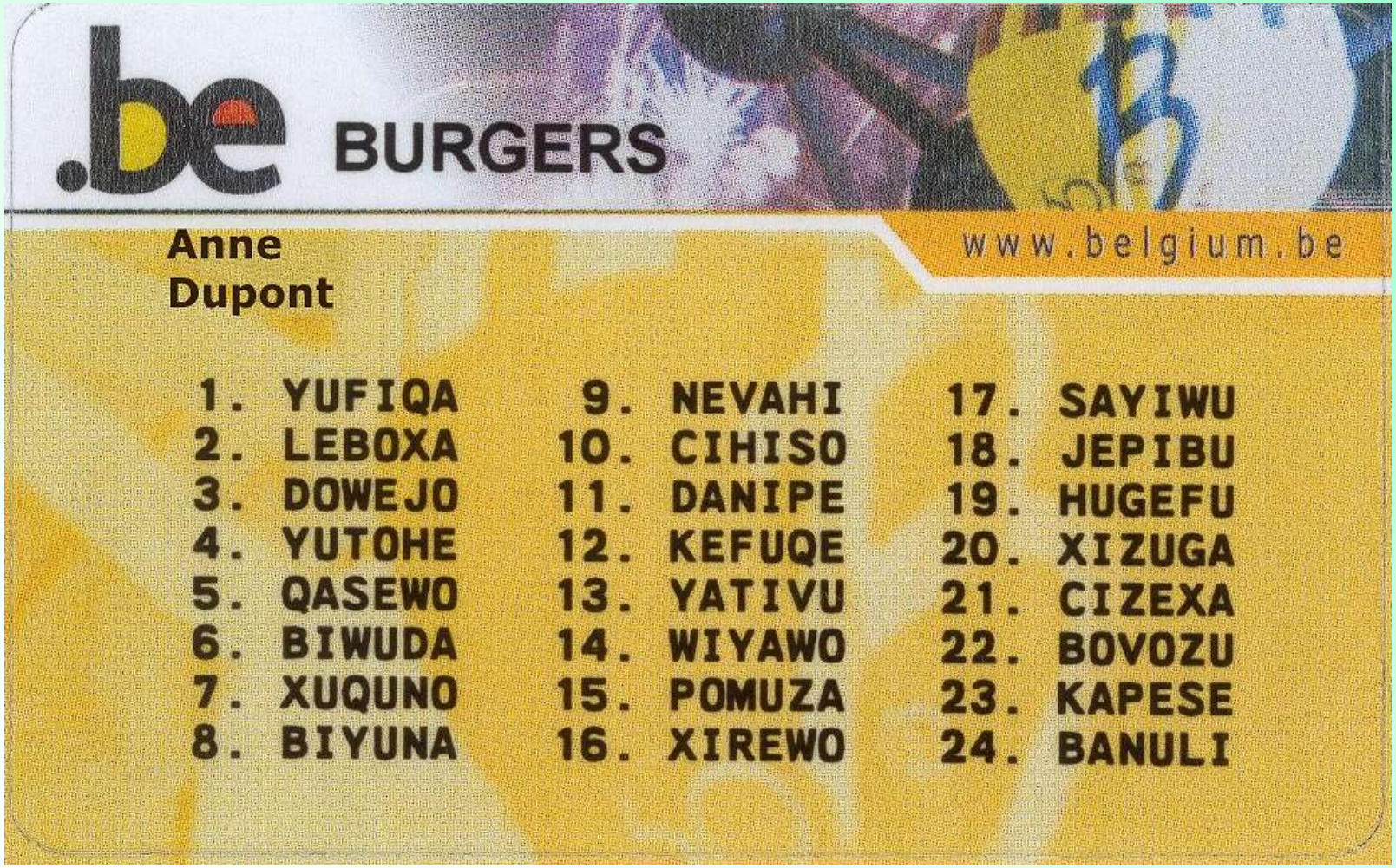
- Digital signatures *remain valid forever* if one stores:
  - The digitally signed data
  - The digital signature on the data
  - The signer's certificate
  - A proof of validity of the signer's certificate
  - The verification timestamp of the signature
- Bottom line:
  - The integrity of this data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



eID – Level 3 + 4

KU LEUVEN

Citizen's Paper Token – Level 2



KU LEUVEN

ePassports

Danny De Cock
K.U.Leuven ESAT/COSIC

For Your Information ☺

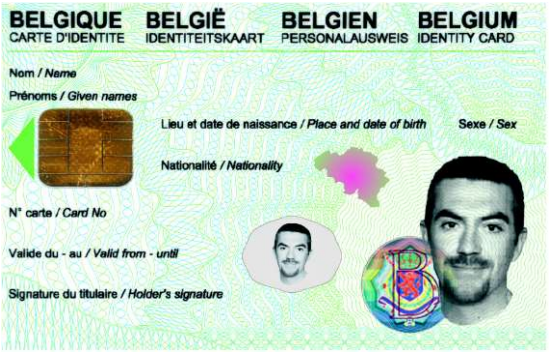
- The copyright holder of this information is Danny De Cock (email: godot@godot.be), further referenced as the author
- The information expressed in this document reflects the author's personal opinions and do not represent his employer's view in any way
- All information is provided as is, without any warranty of any kind
- Use or re-use of any part of this information is only authorized for personal or not-for-profit use, and requires prior permission by the author

Identification & Authentication Chips & Tokens

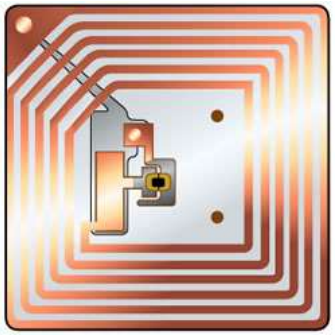
- Identification
  - Requires passive interaction
    - Visually – Eyes
    - Wireless – RFID
- Authentication
  - Requires active interaction
    - Challenge-response
    - Approve actions
      - Knowledge, biometry
- Chip
  - Tamper evident device
- Identity verification
  - Physical identification
    - Opening bank account
    - Access control
- Electronic transactions
  - 2-factor authentication
    - SSL/TLS
    - Control sign/file access
      - PIN, fingerprint, iris,…
- Smartcard = Token
  - Advanced/qualified signatures

Typical examples

RFID-Chip Smartcard
Access Control



eID Card
Contact-based
Strong Authentication



RFID-Tag
Product identification
One-time Deactivation

RFID-based Passport
Contactless Identification
Anti-cloning

eID Card = 4 Functions

- Non-electronic
  1. Visual Identification
- Electronic
  2. Digital identification
     - Data capture
  3. Prove your identity
     - Authentication signature
  4. Digitally sign information
     - Non-repudiation signature

ePassports = 3 Functions

- Non-electronic
  1. Visual Identification
- Electronic
  2. Digital identification
     - Data capture
  3. Document authenticity
     - Anti-cloning

} Focus of this talk

Visual Identification – Passports

- Physical Document – Booklet
  - Data page
    - Name, first name, gender
    - Digital photo, nationality
    - Place of issue, birth
    - Document number, validity
  - Machine-Readable Zone
    - Document type, number, validity
    - Name, gender, birth date
    - Checksums
  - Physical security features
- Digital Document – RFID Chip
  - Storage media
  - Cryptographic coprocessor
  - Biometrics
  - Cryptographic security features
- ICAO standardizes (e)Passports

ePassports Security Requirements

- Unforgeability
  - Digital content of the chip
- Copy protection
  - Copies of the digital document must be detectable
- Access control
  - Unauthorized reading of personal data must be prevented

ICAO Recommendations

- International Civil Aviation Organization
  - ICAO is a UN organization
  - Specifies technical recommendations for passports
- ePassport Technical Reports
  - Deploy biometrics
  - Logical data structure
  - Digital signatures
  - PKI & Security

Passport Protection Systems

- Passive authentication
  - Protects security objects (SO) and logical data structures (LDS) with biometrics and other data
- Comparing printed MRZ and digitally stored MRZ
  - Protects physical link between document and chip
- Active authentication and chip authentication
  - Prevents copying security objects to alien chip
- Basic Access Control system and Password authenticated connection establishment (PACE)
  - Protects against eavesdropping on communication, skimming and misuse of static information
- Terminal authentication
  - Prevents unauthorized access to sensitive data such as fingerprints and other biometrics
- Data encryption
  - Secures additional biometrics

ICAO Logical Data Structure (LDS)

- ePassport Application
  - DG1: Machine readable zone (MRZ) (mandatory)
  - DG2: Facial Image (JPEG encoded) (mandatory)
  - DG3: Fingerprint (no specific encoding) (optional)
  - DG4: Iris (no specific encoding) (optional)
  - DG5: Displayed portrait (JPEG encoded) (optional)
  - DG6: RFU
  - DG7: Displayed signature (JPEG encoded) (optional)
  - DG8: Data features (optional)
  - DG9: Structure features (optional)
  - DG10: Substance features (optional)
  - DG11: Additional personal details (optional)
  - DG12: Additional document details (optional)
  - DG13: Optional details (optional)
  - DG14: RFU
  - DG15: Active Authentication Public Key (optional)
  - DG16: Persons to notify (optional)
  - DG17: Automated Border Clearance Details (optional)
  - DG18: Electronic Visas (optional)
  - DG19: Travel Record Details (optional)
  - SOD: Document Security Object (mandatory)
    - PKCS#7 signed data
    - Protects integrity of all DGs

DG = Data Group
SOD =
RFU = Reserved for Future Use

Passive Authentication

- PKI for passports
  - Country Signing CA – National (Passport) Root CA
  - Document Signer(s) – Passport manufacturer

Algorithm	Country Signing CA	Document Signer
RSA/DSA	3072	2048
ECDSA	256	224

- Certificate revocation
  - Digital documents become less trustworthy
  - Physical documents remain entirely valid

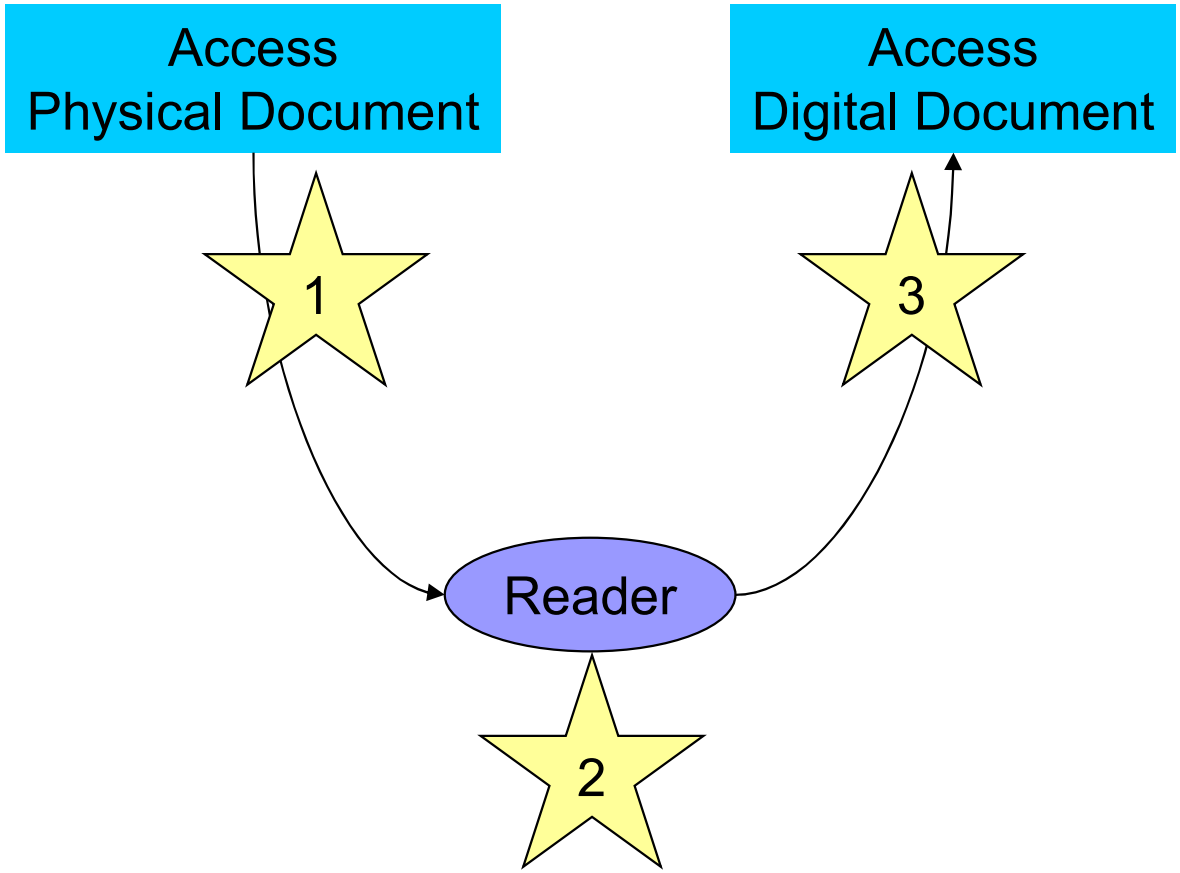
Active Authentication

- Every passport has its own key pair
  - Public key stored in digital document DG15
  - Private key is stored in secure memory of the chip
- Challenge-Response Protocol
  - Terminal challenges passport chip
  - Chip digitally signs the challenge
- Possible problems
  - Chip in the middle attacks
  - Replay of Challenges – request & forward signature from genuine passport

Accessing Information in ePassport

- Sensitivity of (biometric) data
  - Face – MRZ (less-sensitive)
    - Can be obtained easily from other sources
    - Required for global border crossing
    - Requires Basic Access Control
  - Fingerprints, Iris (sensitive)
    - Difficult to obtain from other sources (at a large scale)
    - Only used for national/bilateral purposes
    - Requires Extended Access Control (unspecified)

Basic Access Control – Principle



1. Read MRZ optically
2. Calculate Access Key
3. Authenticate + Read

Basic Access Control – Details

RF Chip

3. Generate Challenge C
4. Generate Key C

9. Decrypt Ciphertext
10. Verify Challenge C
11. Encrypt Challenge R, C + Key C

Inspection System

1. Read MRZ
2. Calculate Access Key K

5. Obtain Challenge C
6. Generate Challenge R
7. Generate Key R
8. Encrypt Challenges C, R + Key R

12. Decrypt Ciphertext
13. Verify Challenge R

After successful authentication:
Secure Messaging + Access to less-sensitive data

Basic Access Control – Security

- Entropy of the access key
  - Approx. 56 bits if passport number is numeric
  - Approx. 73 bits if passport number is alphanumeric
- Goal – anti-skimming protection
  - 40 bits or more provide good protection
- Goal – anti-eavesdropping protection
  - At least 56 bits are necessary for less-sensitive data
  - At least 112 bits are required for sensitive data

Extended Access Control

- Why do fingerprints need additional protection?
  - Fake fingers (silicone, gummy,…) are easy to produce
  - Can be used to circumvent biometrics
  - Criminal investigation…
- Solution: extended access control
  - Only authorized readers are able to access sensitive data
  - “Recently” standardized by ICAO…

Terminal Authentication

- Challenge-response protocol
  - Strong authentication of
    - The terminal's identity and access rights
    - The terminal's ephemeral public key
  - PKI must be in place
    - Chip must be able to verify terminal certificates
    - Terminal certificates must be distributed to chips
    - Challenge:
      - How to revoke terminal certificates?

Supplemental Access Control (SAC)

- Uses Password Authenticated Connection Establishment (PACE) protocol
  - EU passports support SAC since end 2014
- Prevents
  - Online attack to read RFID chip without physical access and without holder's approval
  - Eavesdropping with secure communication stonger than BAC
    - BAC only uses MRZ
    - PACE also allows card access numbers printed on document, e.g., PIN

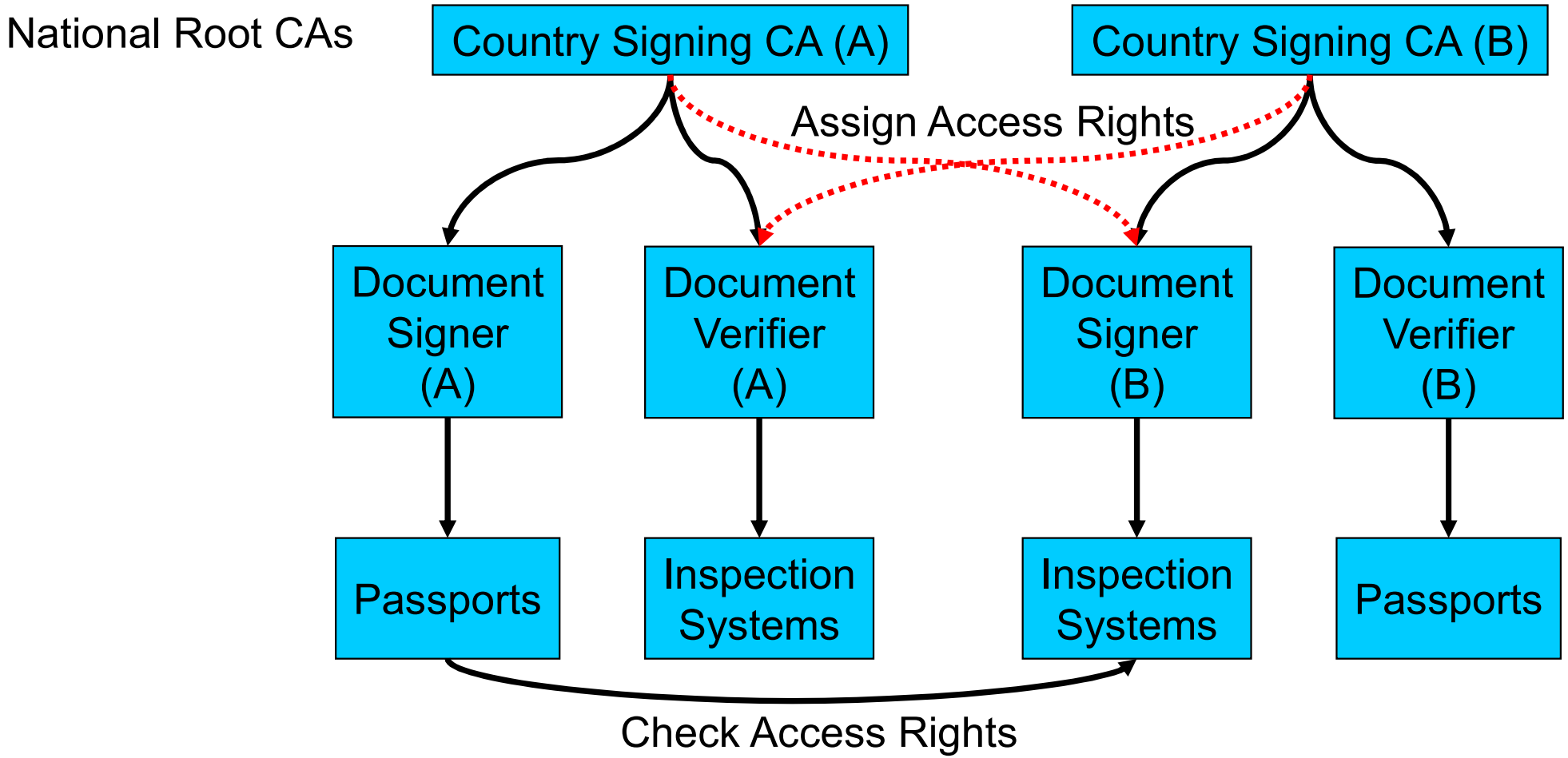
Complete Inspection – Procedure

- Basic Access Control
  - Secure messaging is enabled (medium/strong encryption)
  - Chip grants access to less-sensitive data
  - Read document's security object (SOD)
- Extended access control
  - Chip authentication
    - Secure messaging is restarted (strong encryption)
    - Read less-sensitive data (face)
    - Verify genuineness of chip with active authentication
  - Terminal authentication
    - Chip grants access to sensitive data
    - Read sensitive data (fingerprints, iris,…)

Extended Access Certificates

- Every reader (or group) has its own certificate
  - Certificates are issued by a document verifier
  - Certificates must be parsed by the chip – CV Certificates
  - Certificate holder authorization
    - Requires flexible access right management
    - Reader-specific access to fingerprint, iris,…

PKI for Extended Access Certificates



Terminal Revocation

- Problem – Lost/Stolen inspection systems
  - Unauthorized access to sensitive data
  - Basic access control reduces the problem
- Solution – Certificate revocation
  - Not trivial: chip has no online connection
  - Certificate effective data
  - Certificate expiration date

Practical Session ☺

1. Connect the smartcard reader
2. Go to https://godot.be/cc13
   - download golden.reader.2.9.4.windows.tgz or golden.reader.2.9.4.windows.zip
3. Unpack/install the file
4. Run the application & feed it with data from MRZ
   - Open normal text editor with fixed size font
   - Type 2 first lines of the MRZ into the text editor
   - Click “Autodetect”
   - Paste the two lines of the MRZ, press OK
   - Put your passport on the reader, press OK

Practical Session

- Go to https://godot.be/cc13
  - Install middleware
  - Read eID card
  - Inspect your own certificates
  - Fetch eID CRL
  - Perform OCSP query
    - openssl ocsp -CAfile root.pem -issuer ca.pem –cert cert.pem -url http://ocsp.eid.belgium.be -resp_text

ePassports Exercise

1. Save the data from your passport on disk
   - Click “Write to Disk”
   - Enter the directory where the data should be saved
   - Paste the MRZ,…
2. Examine the information that was saved
   - Which data groups have been saved?
   - What does the certificates contain?
   - Does the picture match your face? ☺
3. Compare the certificate with the eID certificate details of a Belgian eID card

Thank you for your attention!

Email: godot@godot.be

Slides: godot.be/slides