



e ID

Jan Janssens, Driss Kaddouri, Tim Langens, Jef Neefs,
Maarten Van Genechten

History

- Started at the end of 2002
- Generalization decided in March of 2004
- Middle of 2005 passed the milestone of one million
- The end of 2009 more than 8 millions

Objective of the eID

- part of e-Government
- simplify the administration
- modernize the public services



Visible data

- name, first name, gender, nationality, place and date of birth, signature, national number and period of validity of the card
- These are also electronically contained in the card

Electronic data

- The same informations as the one that are visible on the card (including the picture)
- The address of the card owner;
- The identity and signature keys;
- The identity and signature certificates;
- The service provider of the certification

Electronic data (2)

- The information necessary for the authentication of the card;
- The information necessary for the for the protection of the electronically visible data That are encrypted on the card;
- The information necessary for the use of the corresponding qualified certificates

What can be done already.

- ordering a licence plate for your car
- multifunctional tax return
- reporting of labour accidents
- VAT return
- starting an enterprise
- online election results

What can be done in the future.

- digitally signing contracts
- demanding birth certificates for new born children
- instead of buying expensive foreign travel passports just ticking your card at a terminal in the airport
- internet security (secure chat rooms etc)
- banc account access for online trade
- ...

Microsoft™

- Outlook 2003

Know who mailed you with certainty

- Word 2003

Sign letters and even contracts with the same legal value as a normal signature

- MSN Messenger™

Secure Chatrooms know who you are really chatting with or have age controlled chatrooms



Big Brother?

- “Big Brother is watching us”-feeling is not justified
- eID card contains only the same information as your old ID card
- eID gives you access to information on e-government sites
- You can always check when, whom accessed your information.

Middleware

- Software placed between the application (digital signatures) and the device (the smartcard).
- Two independent interface implementations :

Interfaces

- Microsoft CryptoAPI enables authentication, encoding, and encryption of Win32-based applications.
- The PKCS#11 or cryptoki interface provides an abstract interface to the smartcard for non-Microsoft applications like Mozilla.

PIN / PUK Security

- Readers with a PIN-pad must implement all commands needing a PIN input without transmitting the PIN outside the reader.
- Software compatibility with the middleware.

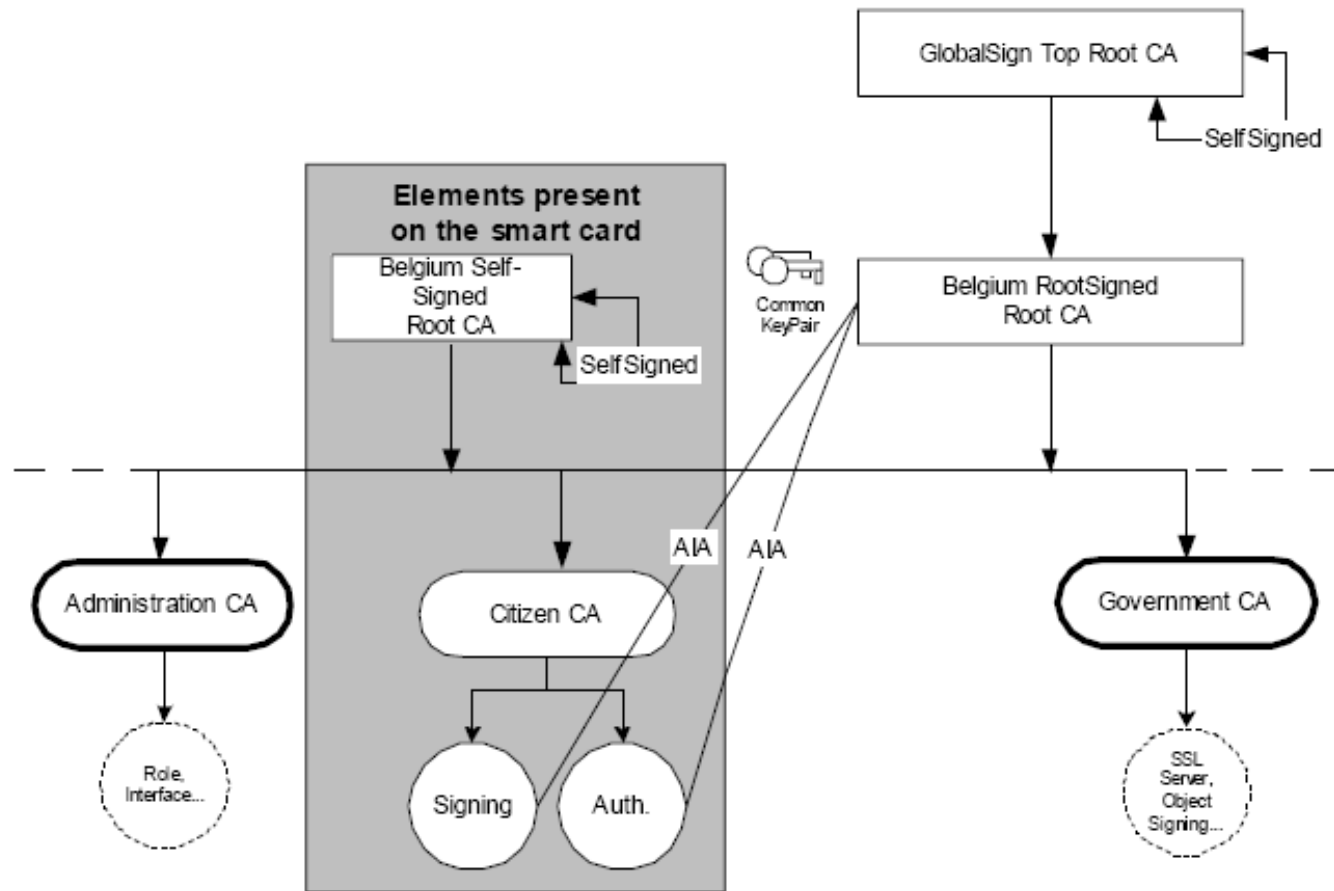
Integration with middleware

- Reader provider must develop for each target OS a DLL implementing :
 - SCR_Init()
 - SCR_VerifyPIN()
 - SCR_ChangePIN()
- Written in C

Structure and Organisation

- dedicated PKI infrastructure
- three levels:
 - The first level is the Belgium Root CA;
 - The second level contains the eID operation CAs (including the citizen CA),
 - the third level concerns the end entities (citizens).

Structure and Organisation



Signature Algorithm

- Key Pairs
 - RSA cryptographic algorithm
 - 2048 bits

To do this	Use whose	Kind of key
Send an encrypted message	Use the receiver's	Public key
Send an encrypted signature	Use the sender's	Private key
Decrypt an encrypted message	Use the receiver's	Private key
Decrypt an encrypted signature (and authenticate the sender)	Use the sender's	Public key

Hashing

- It should accept any length message as input.
- It should produce a small fixed-size output (~ 100 bits).
- It should be easy and fast to compute h for any input.
- It should be a one-way function-hard or impossible to invert.

Hashing (2)

- It should be resistant to weak collisions.
- It should be resistant to strong collisions
- SHA-1

Certificate Profiles

- X.509 version 3
- CRL
- OCSP
- Serial number



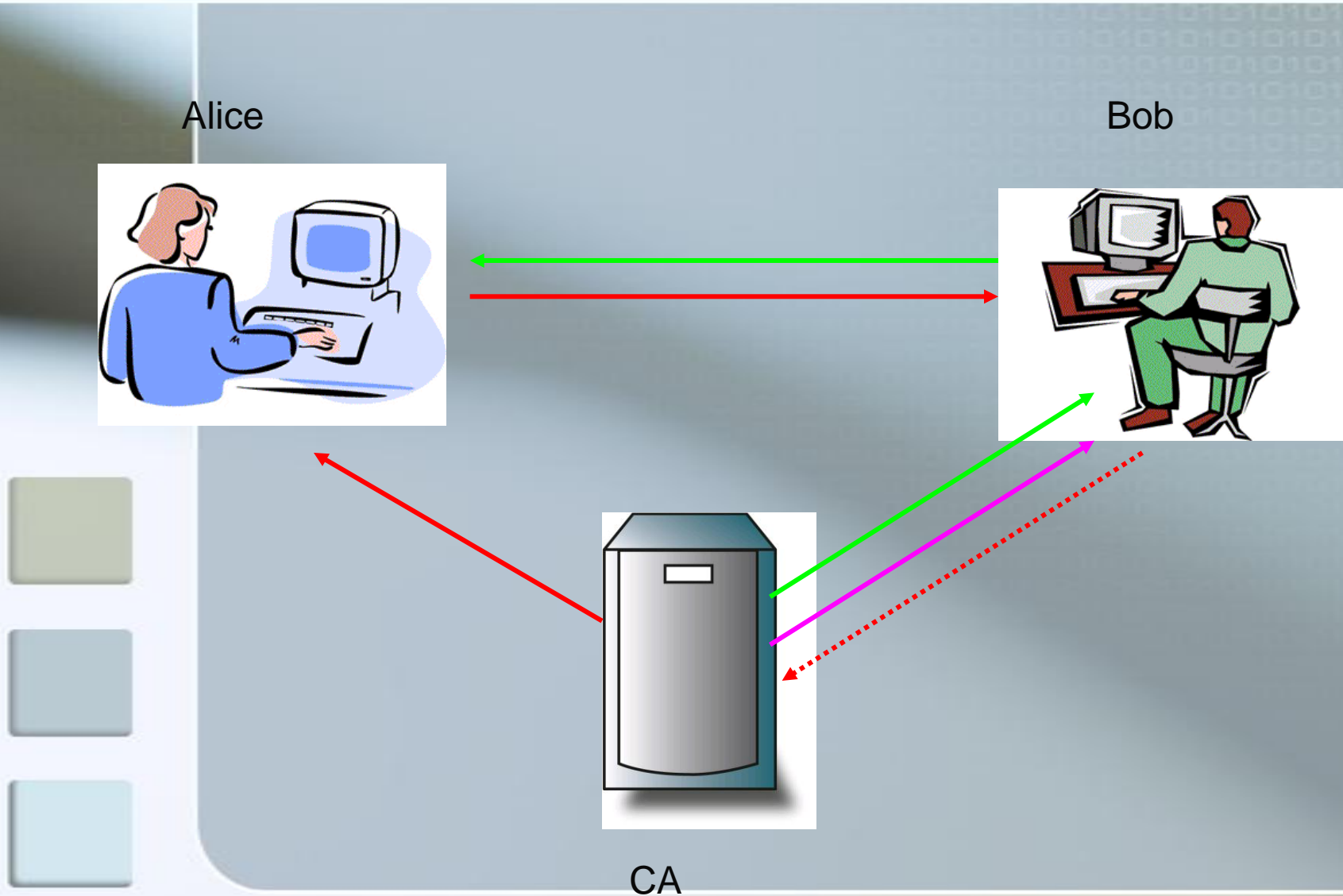
Certificate fields

- Signature field
- Issuer field
- Validity field
- Subject field
- Subject Public Key Info field
- Key Usage extension field
- NetscapeCertType
- ...

OCSP certificate

- Online Certificate Status Protocol
- Obtains the revocation status of a X.509 digital certificate
- Messages sent over OCSP are encoded in the Abstract Notification Standard (ASN 1)
- Alternative to the Certificate Revocation List (CRL)

Basic PKI implementation



Protocol details

- OCSP Response
 - Good
 - Revoked
 - Unknown
 - Error
- Resistant to replay attacks
 - ⇒ Minor Threat

Replay Attacks?

- Capture the traffic and subsequently replay that traffic,
- Capture the status of a certificate whose status is about to change and
- Conduct a transaction requiring the status of that certificate within the time frame of the validity of the response.

OCSP and EID

- Shared key pair
- Multiple OCSP certificates
- Due to the restraint of shared infrastructure, sender and response certificate profile must be identical

What is CRL

- Certificate Revocation List
 - ⇒ List of revoked certificate serial numbers
- Created after a predefined time frame or every time a certificate is revoked



Problems with all CRLs

- Each certificate must be checked, which negates with PKI (works with self authentication)
- Administrator needed to enforce policy
- Solution OCSP

OCSP Advantages over CRL

- OCSP can provide more timely information regarding the revocation status of a certificate.
- OCSP removes the need for clients to retrieve the (sometimes very large) CRLs themselves, leading to less network traffic and better bandwidth management.
- Using OCSP, clients do not need to parse CRLs themselves, saving client-side complexity.

OCSP Advantages over CRL

- An OCSP responder may implement billing mechanisms to pass the cost of validation transactions to the seller, rather than buyer.
- CRLs may be seen as analogous to a credit card company's "bad customer list" -- an unnecessarily public exposure.
- To a degree, OCSP supports trusted chaining of OCSP requests between responders. This allows clients to communicate with a trusted responder to query an alternate responder, saving client-side complexity.

CRL and EID

■ CRL Profile

Version	v2
Signature	sha1RSA
Issuer	<subject CA>
ThisUpdate	<creation time>
NextUpdate	<creation time> + 7 days
RevokedCertificates	
UserCertificate	<certificate serial number>

Delta CRL Profile

Version	v2
signature	sha1RSA
Issuer	<subject CA>
thisUpdate	<creation time>
nextUpdate	<creation time> + 7 days
RevokedCertificates	
userCertificate	<certificate serial number>
revocationDate	<revocation time>
crlEntryExtensions	
CRL Reason Code	certificateHold(6) (for suspended certificates) removeFromCrl(8) (to unsuspend certificates) Note: otherwise not included
crlExtensions	
Authority Key Identifier	non-critical <subject key identifier CA>
CRL Number	non-critical <The CA operator assigned unique number>
Delta CRL Indicator	critical <base CRL Number>

LDAP Scheme

- LDAP node definition:
dc=eid dc=belgium dc=be
- Flat file structure
- Contains:
 - Certificate, Subject Distinguished Name information, CRL and Delta CRL