eID Security

Frank Cornelis
Architect eID
The eID Project

> Provides Belgian Citizens with an electronic identity card.
> Gives Belgian Citizens a device to claim their identity in the new digital age.
eID Partners

Certipost
By Belgacom & De Post - La Poste

Fedict e-gov

Zetes

FOD Binnenlandse Zaken

Spf Intérieur
eID Functionalities

- Visual Identification
- Identification
- Authentication
- Electronic signature

© fedict 2008. All rights reserved
Overview eID Functionality

- Visual Identification
- Identification
- Authentication
- Electronic Signature
From a visual point of view the same information is visible as on a regular identity card:

- the name
- the first two Christian names
- the first letter of the third Christian name
- the nationality
- the birth place and date
- the sex
- the place of delivery of the card
- the begin and end data of the validity of the card
- the denomination and number of the card
- the photo of the holder
- the signature of the holder
- the identification number of the National Register
> Non-electronic functionality is equivalent to regular identity card functionality.
> Non-electronic functionality is equivalent to electronic functionality.
Security Aspects

> Outside

- Rainbow and guilloche printing
- Changeable Laser Image (CLI)
- Optical Variable Ink (OVI)
- Alphagram
- Relief and UV print
- Laser engraving
Chip specifications

> Chip characteristics: Cryptoflex JavaCard 32K
  - **CPU (processor):** 16 bit Micro-controller
  - **Crypto-processor:**
    - 1100 bit Crypto-Engine (RSA computation)
    - 112 bit Crypto-Accelerator (DES computation)
  - **ROM (OS):** 136 kB (GEOS JRE)
  - **EEPROM (Applic + Data):** 32 KB (Belpic Applet)
  - **RAM (memory):** 5 KB
Overview eID Functionality

- Visual Identification
- Identification
- Authentication
- Electronic Signature
From an **electronic** point of view the chip contains the same information as printed on the card, filled up with:

- the identity and signature keys
- the identity and signature certificates
- the accredited certification service furnisher
- information necessary for authentication of the card and integrity protection of the data
- the main residence of the holder

**Electronic identification**

of the holder

- No encryption certificates
- No biometric data
- No electronic purse
- No storage of other data
eID Identification Advantages

- Time consuming
- Inefficient
- Error-prone

- Fast
- Efficient
- Accurate
eID Authentication

- Confirming the identity of the person

**Real world**

- Hi Alice!
- Hi Bob!

**Digital world**

- Log on to web sites
- Container park
- Library

© fedict 2008. All rights reserved
PKI

“PIN protected”

digital signature

authentication

Identity

Use without PIN

ID

ADDRESS

RRN SIGN

RRN SIGN
Data Specifications

> Directory Structure (PKCS#15)

- **Dir (BelPIC):**
  - certificates & keys (PIN code protected)
    - private and public key CA: 2048 bits
    - private and public key citizen: 1024 bits
    - Signatures put via RSA with SHA-1
    - all certificates are conform to X.509 v3
  - standard format (to be used by generic applications)
    - Microsoft CryptoAPI (⇔ Windows)
    - PKCS#11 (⇔ UNIX/Linux & MacOS)
- **Dir (ID):**
  - contains full identity information
    - first name, last name, etc.
    - address
    - picture
    - etc.
  - proprietary format (to be used by dedicated applications only)
Public-key Cryptography

> Asymmetric cryptography: public key and private key

> eID cryptographic algorithm: RSA
Cryptographic Operations

> Encryption

Bob

Hello Alice! -> Encrypt -> Alice's public key

6EB69570 08E03CE4

Alice

Hello Alice! -> Decrypt -> Alice's private key

> Signing

Alice

I will pay $500 -> Sign (Encrypt) -> Alice's private key

DFCD3454 BBEA788A

Bob

I will pay $500 -> Verify (Decrypt) -> Alice's public key

Problem: which key belongs to Alice?
X509 Certificate

> Is a signed digital statement.
> Links a person to a key via a trusted party (CA)

Signed by the CA that issued the certificate.
eID Certificates

- Auth + Sign Key pairs
- 1024 bits
- Private key (inside the chip)
- Public key (inside the certificate)
Web Authentication

1. Validate Server Certificate
2. User Identity
3. "Challenge" to verify Client Identity
4. Encrypt "Challenge" with eID Private Key
5. Decrypt "Challenge" with Public Key from Authentication Certificate
6. If/When "Challenge" match access granted

© fedict 2008. All rights reserved
Overview eID Functionality

- Visual Identification
- Identification
- Authentication
- Electronic Signature
eID electronic signature can have the same legal value as a handwritten signature.
eID Electronic Signature

1. Compose message
2. Compute hash
3. Generate signature
4. Collect signature
5. Collect certificate
6. Send message
7. Compute reference hash
8. Hash, signature, public key match?

Matching triplet?

Alice

Eve

Bob

1. Receive message
2. Inspect certificate
3. Check CRL
4. Check certificate
5. Fetch public key
6. Fetch signature
7. Compute reference hash
8. Hash, signature, public key match?
## Authentication vs. Signatures

<table>
<thead>
<tr>
<th>Authentication</th>
<th>Signatures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature with the key corresponding with the authn</td>
<td>Signature with the key corresponding with the non-</td>
</tr>
<tr>
<td>certificate.</td>
<td>repudiation certificate.</td>
</tr>
<tr>
<td>Liability is application specific.</td>
<td>Liability is regulated by law.</td>
</tr>
<tr>
<td>Lifecycle of authn session is short.</td>
<td>Long-term lifecycle: required storage of revocation data.</td>
</tr>
<tr>
<td>Signature consumer same as signature requestor.</td>
<td>Signature verification by 3th party (e.g. court expert)</td>
</tr>
<tr>
<td>Synchronous by nature.</td>
<td>Creation can be postponed.</td>
</tr>
</tbody>
</table>
The features of a non-repudiation signature drives the need for open signature standards.

- PDF signatures
- ODF signatures
- XAdES signatures
Overview eID Functionality

- Visual Identification
- Identification
- Authentication
- Electronic Signature

© fedict 2008. All rights reserved
Fedict eID Middleware

> Software for using the eID card on a PC
  • Identification (GUI tool + SDK)
  • Authentication/Signature modules:
    • PKCS#11
    • CSP
    • tokenD

> Platforms:
  • Windows: XP, Vista
  • Linux: Fedora, OpenSUSE, Debian
  • Mac
Fedict Reverse Proxy

Used to authenticate a person via eID towards a web application using SSL.
eID Applications

- Student cards
- Healthcare
- Driver’s license
- Home banking
- SSO, ...
- Proof of membership
- E-commerce

© fedict 2008. All rights reserved
More Information?

www.eid.belgium.be
Questions & Answers

Q & A

Thank you!