De Belgische Electronische Identiteitskaart

Bart SIJNAVE
Vlaams Parlement

Brussel, 7 oktober 2004

fedict e-gov

e-government

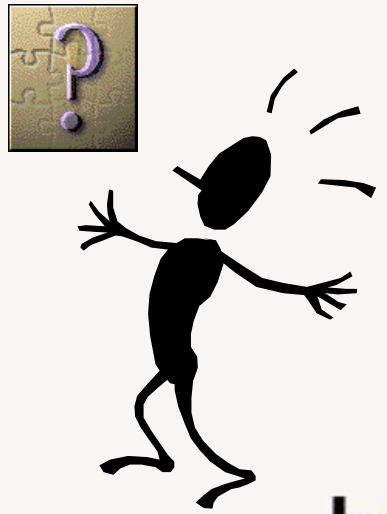
.be

Wat is e-Government ?

NIET : over ‘overheden’

WEL : over ‘de klanten van de overheid’ :

- ✓ burgers
- ✓ ondernemingen
- ✓ ambtenaren



e-Government principles

- totaal-oplossing
- transparantie (verbergen van interne complexiteit)
- “I will say it only once” – eenmalige gegevensinzameling
- beperken van administratieve formaliteiten
- geen extra kost
- privacy
- vermijden van de digitale kloof

Architectuur & bouwstenen

SECURITY & PRIVACY

ANDERE INSTELLINGEN

PORTAAL

www.belgium.be

UME

FEDMAN

AUTHENTIEKE BRONNEN

FPS

FPS

FPS

FPS

ANDERE OVERHEDEN

Connected government

eID - basis

A new ID-card with the format of a bank card and a powerful chip

Doel eID project

Proof of identity

- Elke burger een electronische identiteitskaart geven die moet toelaten om zich te authentificeren en digitale handtekeningen te plaatsen

Signature tool

Welke informatie ?

Visuele identificatie van de houder

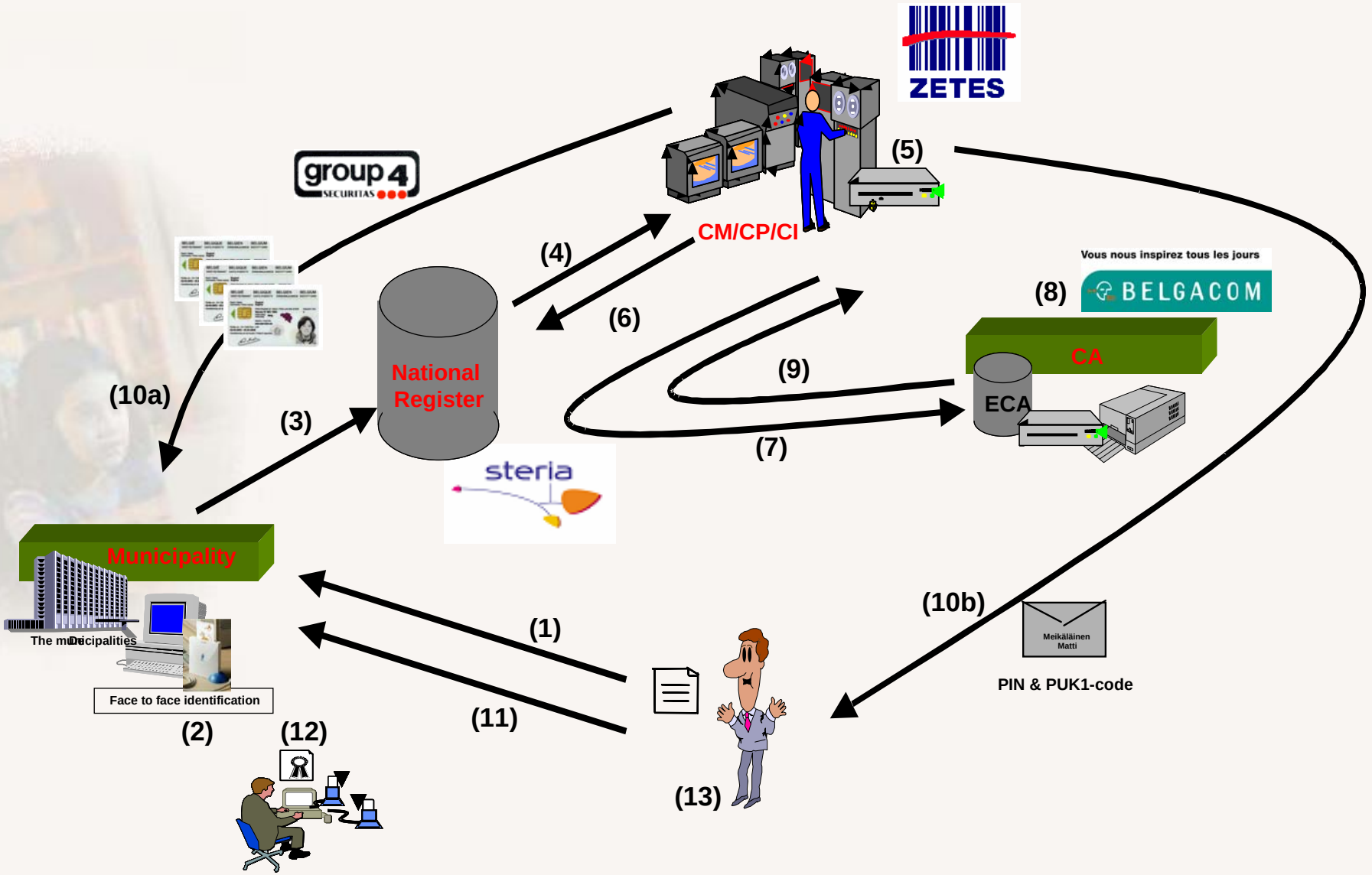
- Visueel is de volgende informatie zichtbaar :
  - naam
  - de eerste twee voornamen
  - de eerste letter van de derde voornaam
  - de nationaliteit
  - de geboorteplaats en -datum
  - het geslacht
  - plaats van afgifte van de kaart
  - geldigheidsdata van de kaart
  - naam en nummer van de kaart
  - foto van de houder
  - handtekening van de houder
  - het identificatie nummer van het Rijksregister
- Analoge functionaliteit als huidige identiteitskaart

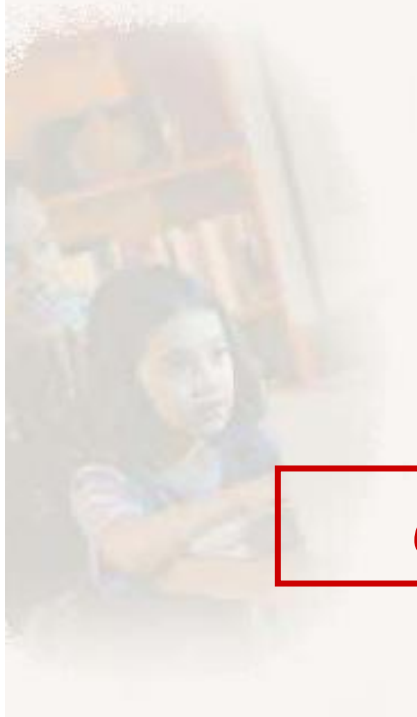
Welke informatie ?

Electronische identificatie
van de houder

- Vanuit electronisch oogpunt zal de chip dezelfde informatie bevatten als gedrukt op de kaart, aangevuld met:
  - identiteits- and handtekening sleutels
  - identiteits- en handtekening certificaten
  - de geaccrediteerde certificatiedienstverlener
  - informatie noodzakelijk voor de authentificatie van de kaart en beveiliging van de elektronische data
  - de hoofdverblijfplaats van de houder
- (momenteel) geen encryptie-certificaten
- (nog) geen biometrische gegevens
- geen opslag van andere gegevens

Verdeling eID : hoe en waar ?





eID – chip

eID, welcome to the e-world !

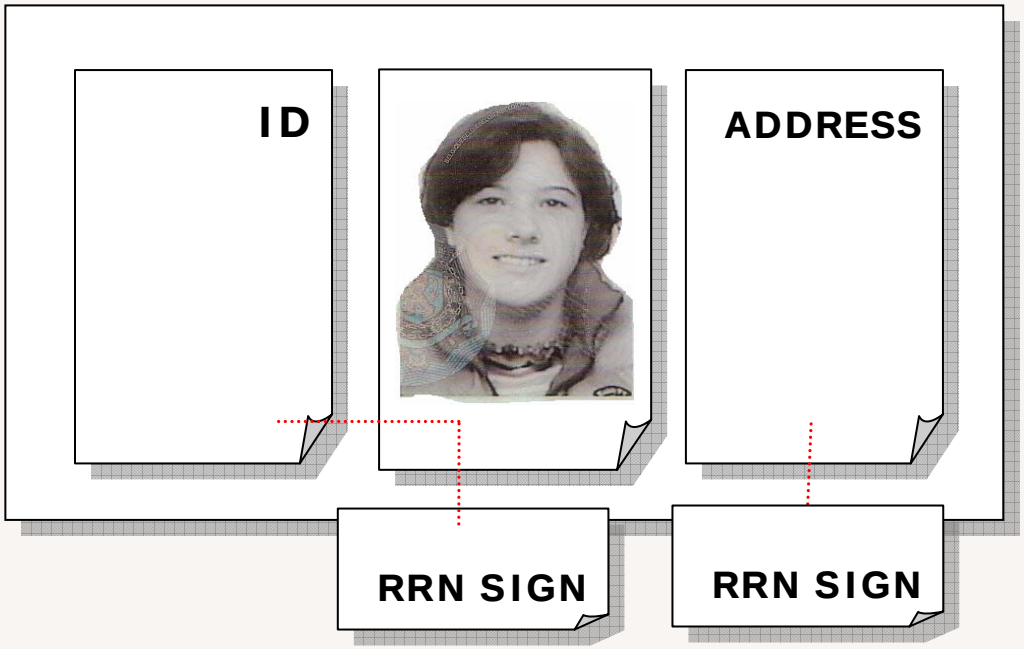
Inhoud van de chip

PKI

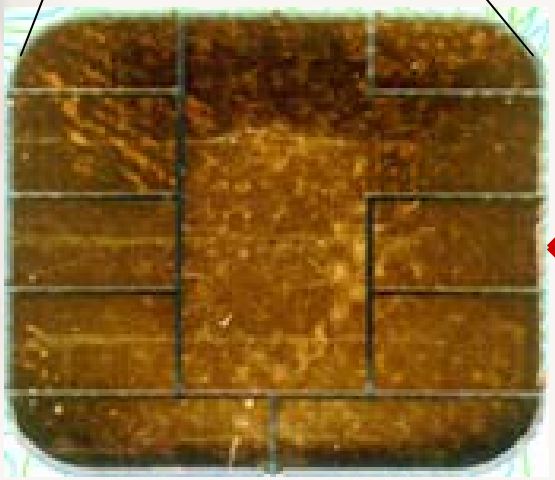
authentication

digital signature

IDENTITY



eID : de e-functionaliteiten

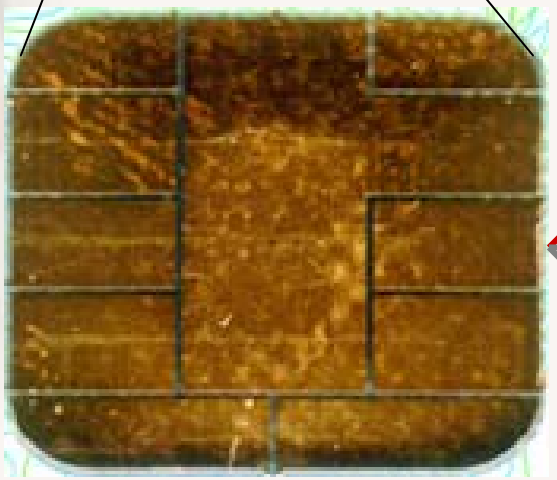


data capture

authentificatie

digitale handtekening

eID : de e-functionaliteiten



data capture

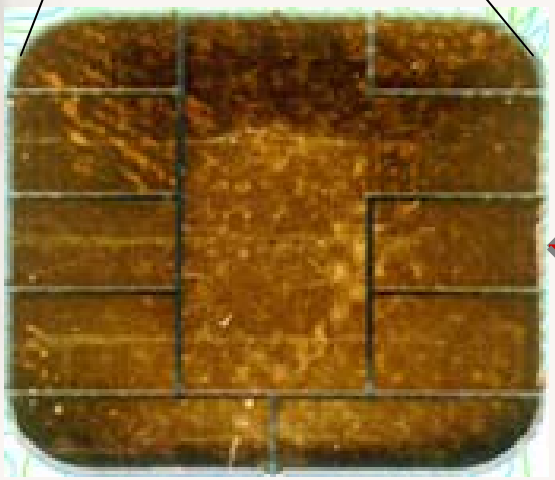
authentificatie

digitale handtekening

Data capture

- **faster** data capture
  - data can be read directly from the card and stored in a particular system
- **more accurate** data capture
  - no more manual re-entrying → less error-prone process
- **more efficient** data capture
  - faster processing of information

eID : de e-functionaliteiten

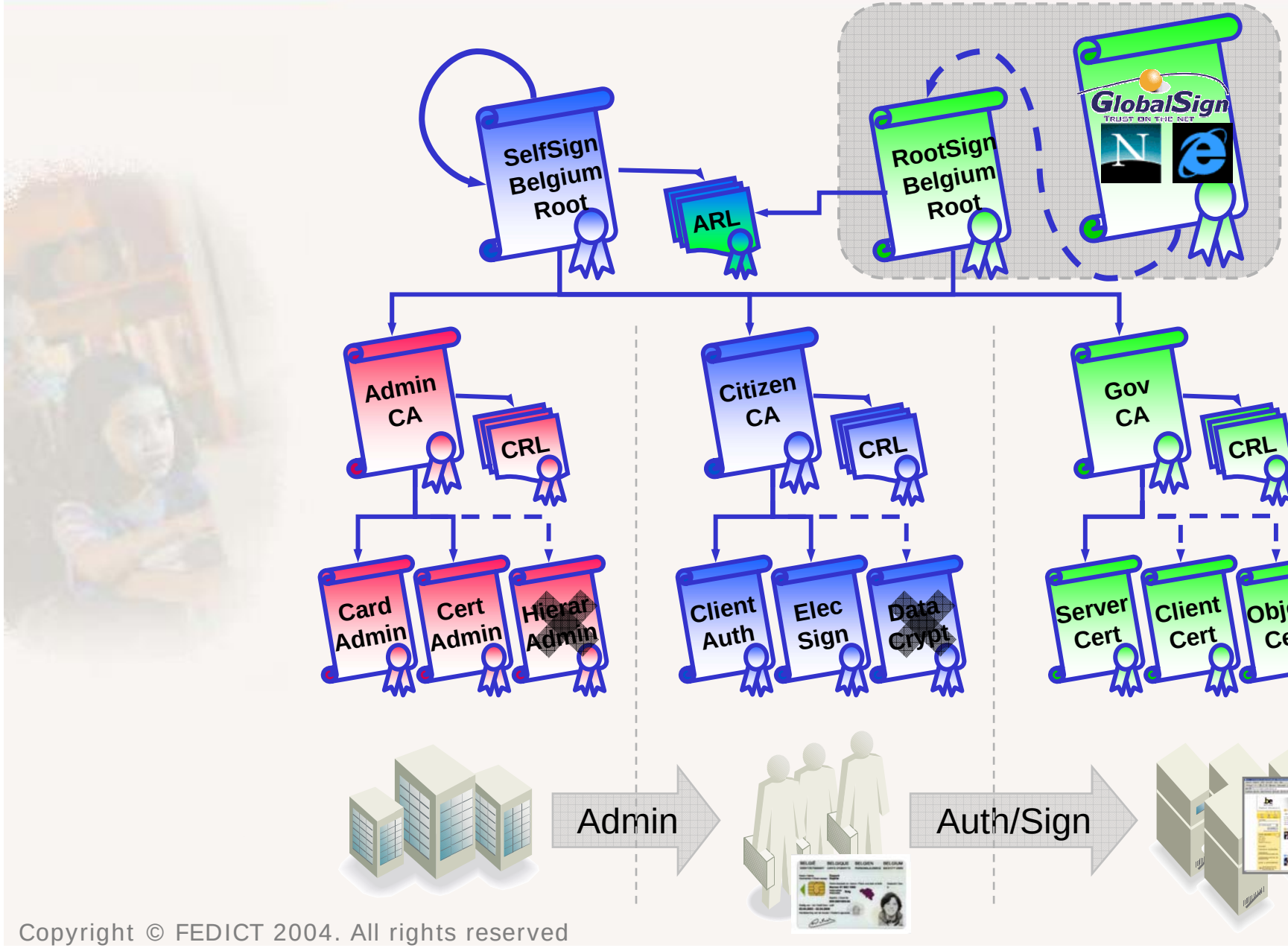


data capture

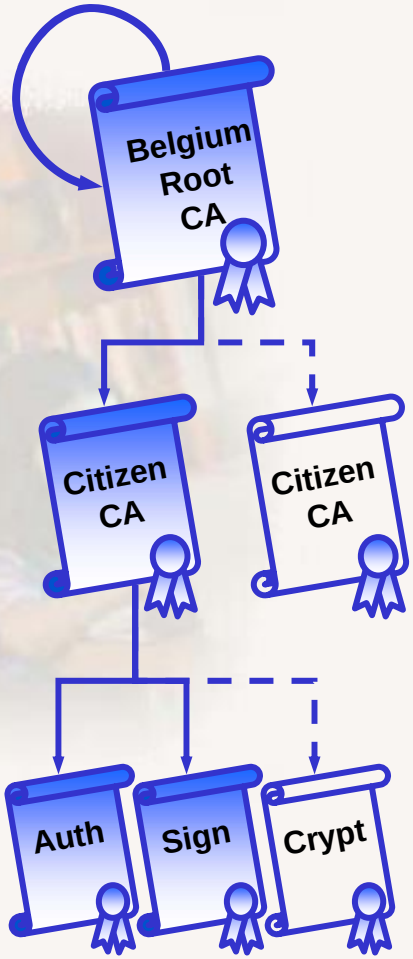
authentificatie

digitale handtekening

Vertrouwenshiërarchie

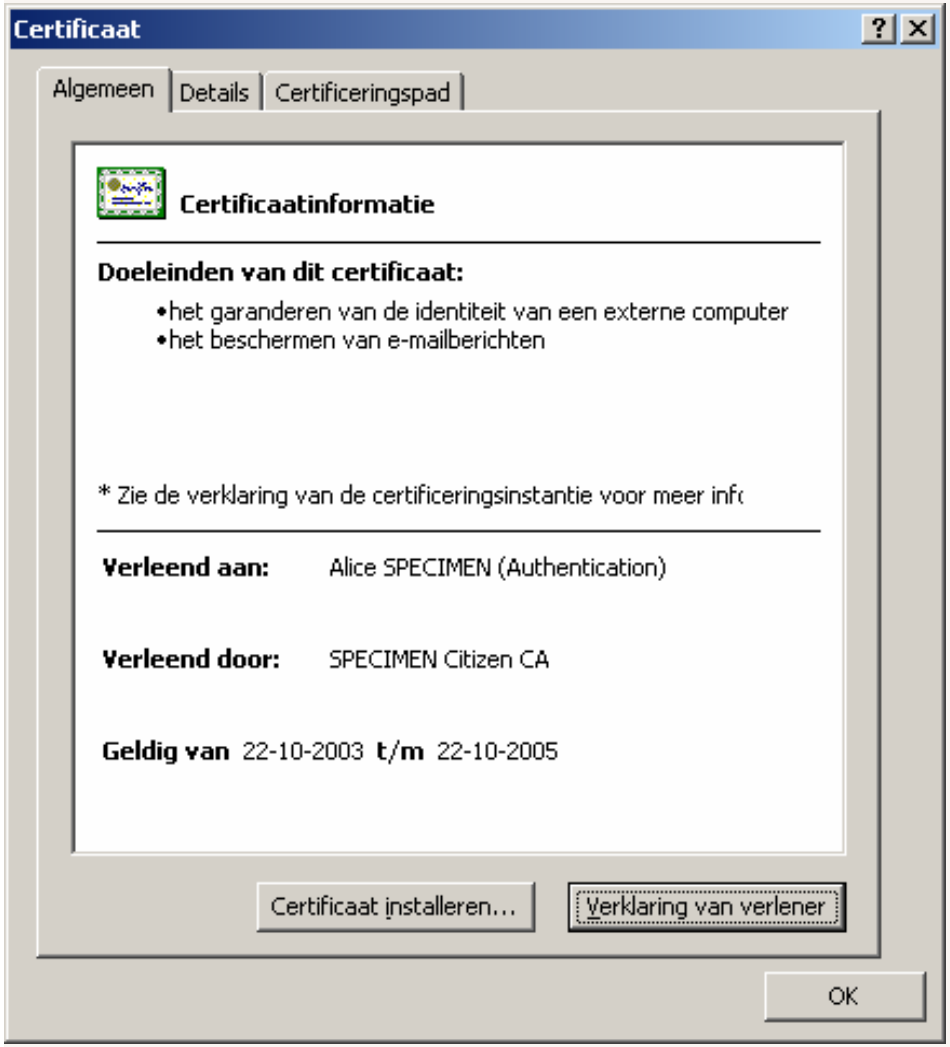


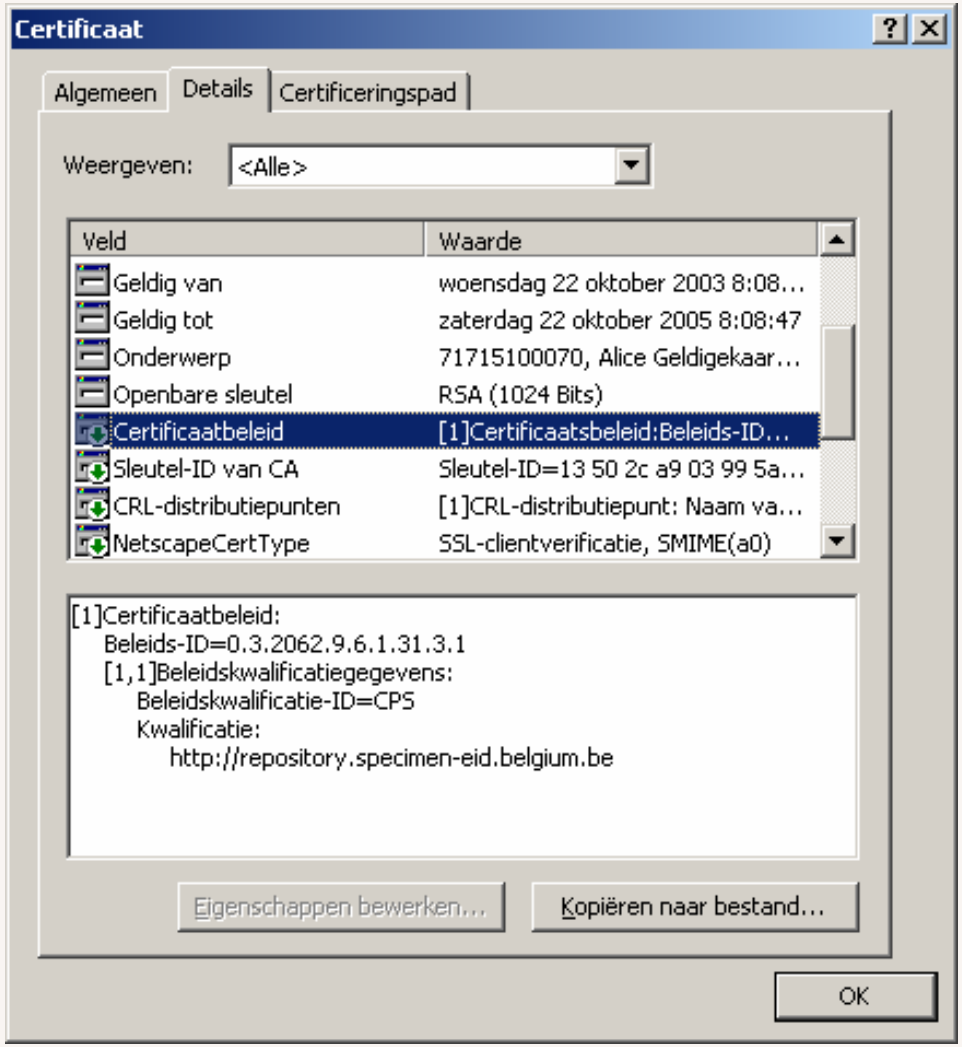
Certificaten



- Burgercertificaten & -sleutels
  - **Authentificatie-**certificaat & sleutelpaar (1024 bits)
    - voorziet in sterke authentificatie
      - web site authentication
      - single sign-on (login)
      - etc.
  - **Handtekening-**certificaat & sleutelpaar (1024 bits)
    - voorziet in niet-weerlegbaarheid (electronische handtekening equivalent aan handgeschreven handtekening)
      - Ondertekenen van documenten
      - Ondertekenen van formulieren
      - etc.
  - (**Encryptie-** certificaat & sleutelpaar)
    - voorzien in een later stadium
    - backup/archivering van privé-sleutels

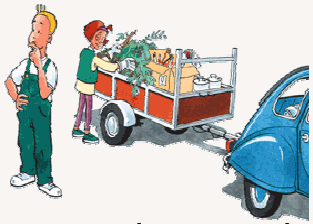
Certificaat





Authentificatie

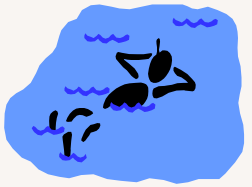
log on to web sites (SSO)



container park

bibliotheek

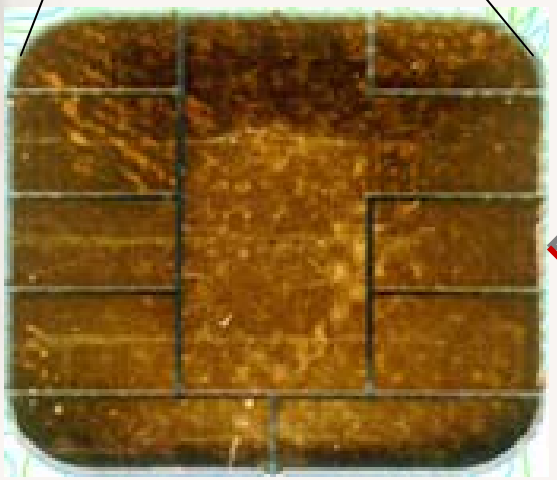
toegangscontrole



zwembad

...

eID : the main e-functionalities



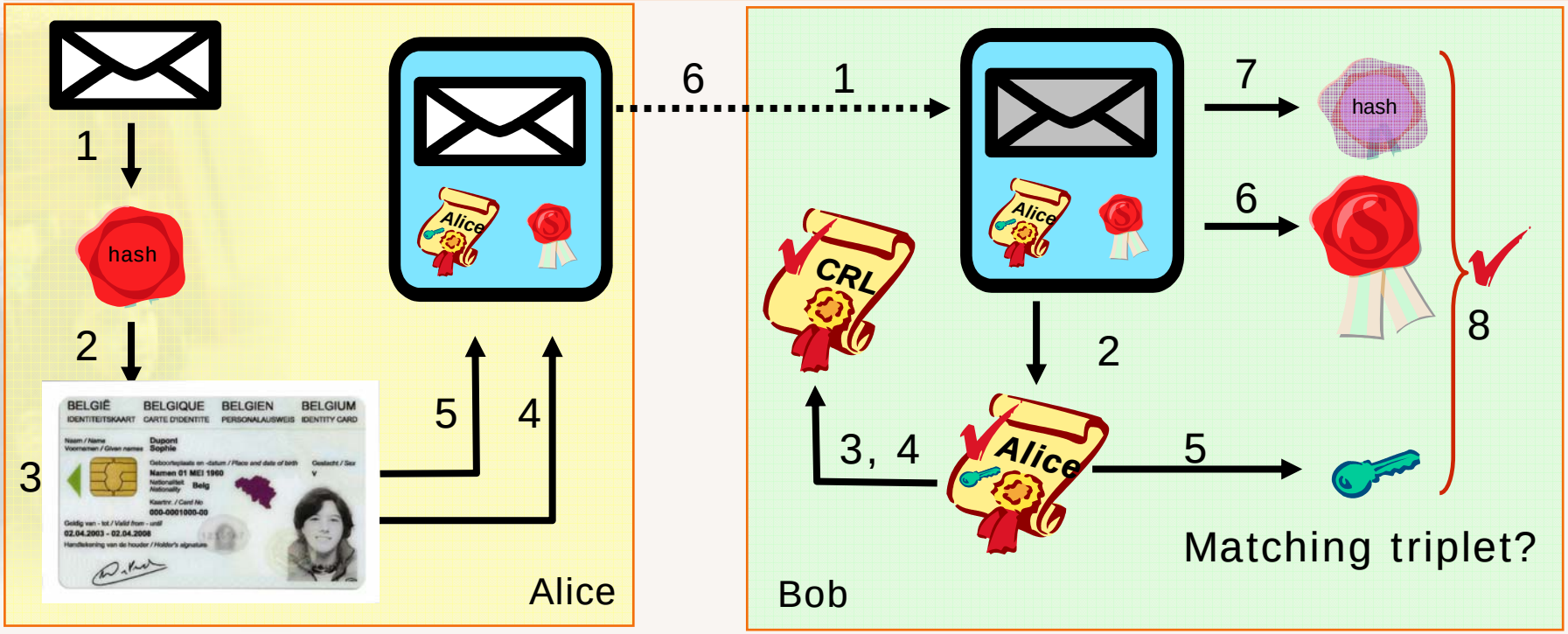
data capture

authentificatie

digitale handtekening

Handtekening

1. Compose message
2. Compute hash
3. Generate signature
4. Collect signature
5. Collect certificate
6. Send message



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

fedict e-gov

eID - toolkits

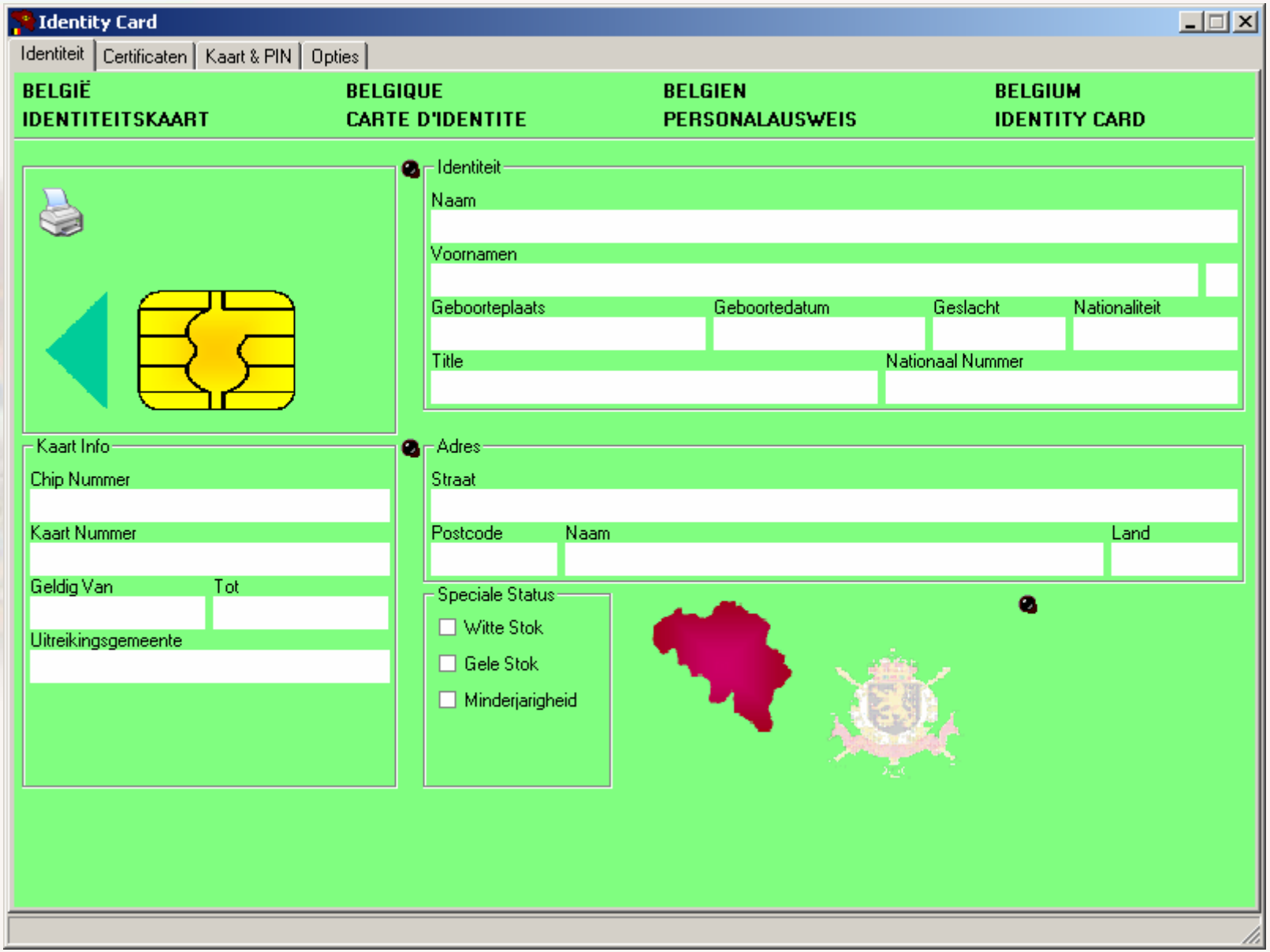
Let's make use of the power of eID !

.be

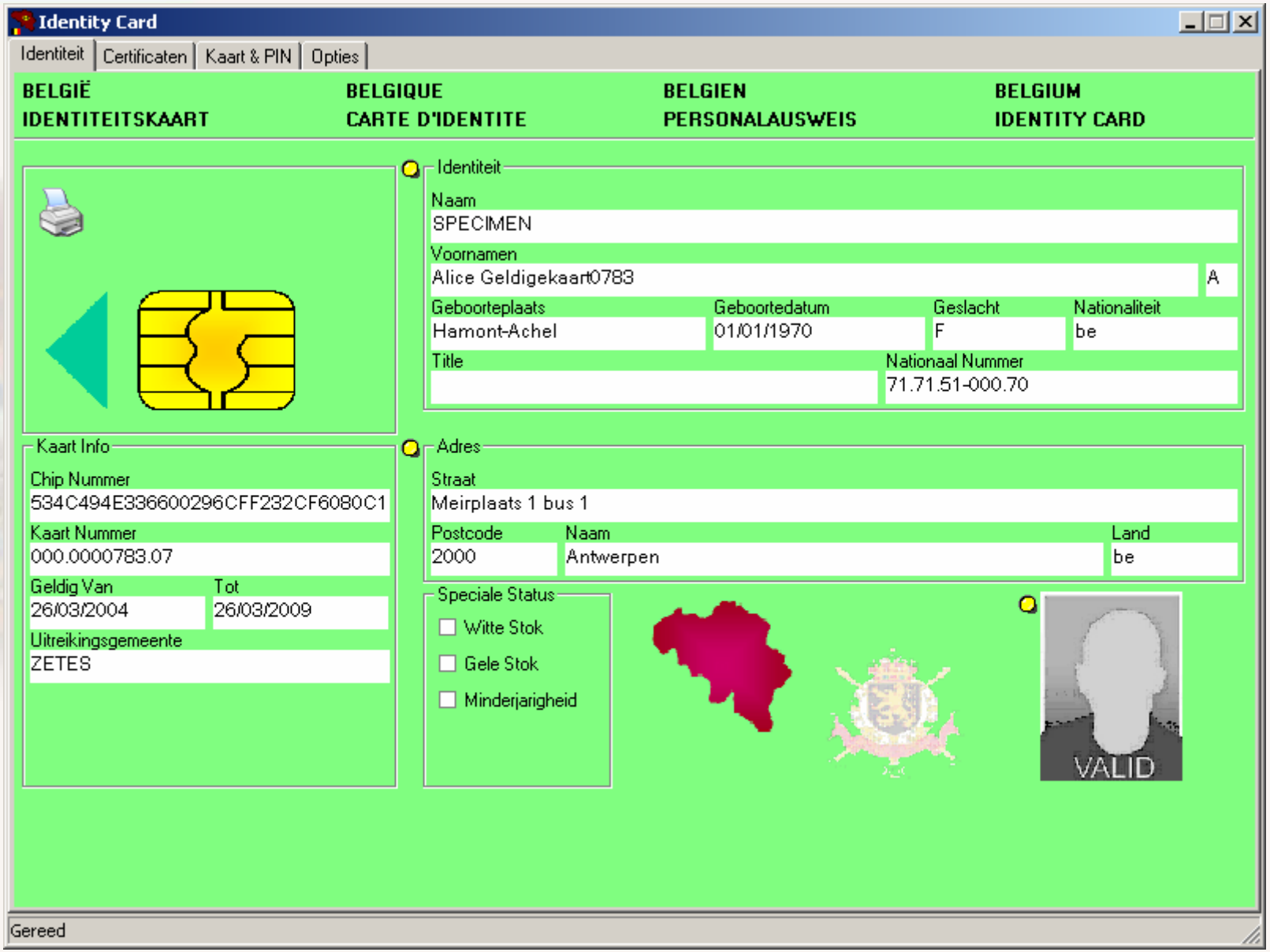
eID-toolkits

- Twee toolkits zijn in testfase :
  - ✓ GUI + PKCS#11 libraries : lezen, afdrukken, valideren en visualiseren van de inhoud van de eID chip
  - ✓ authentication proxy : eenvoudige authentificatie op verschillende platformen
- Doel : verbergen interne kaartwijzigingen
- Labeling quasi vanzelfsprekend bij gebruik van toolkits
- Beide toolkits zijn gratis
- Verdeling via het federale portaal (http://www.belgium.be/fedict → Projecten → eID)

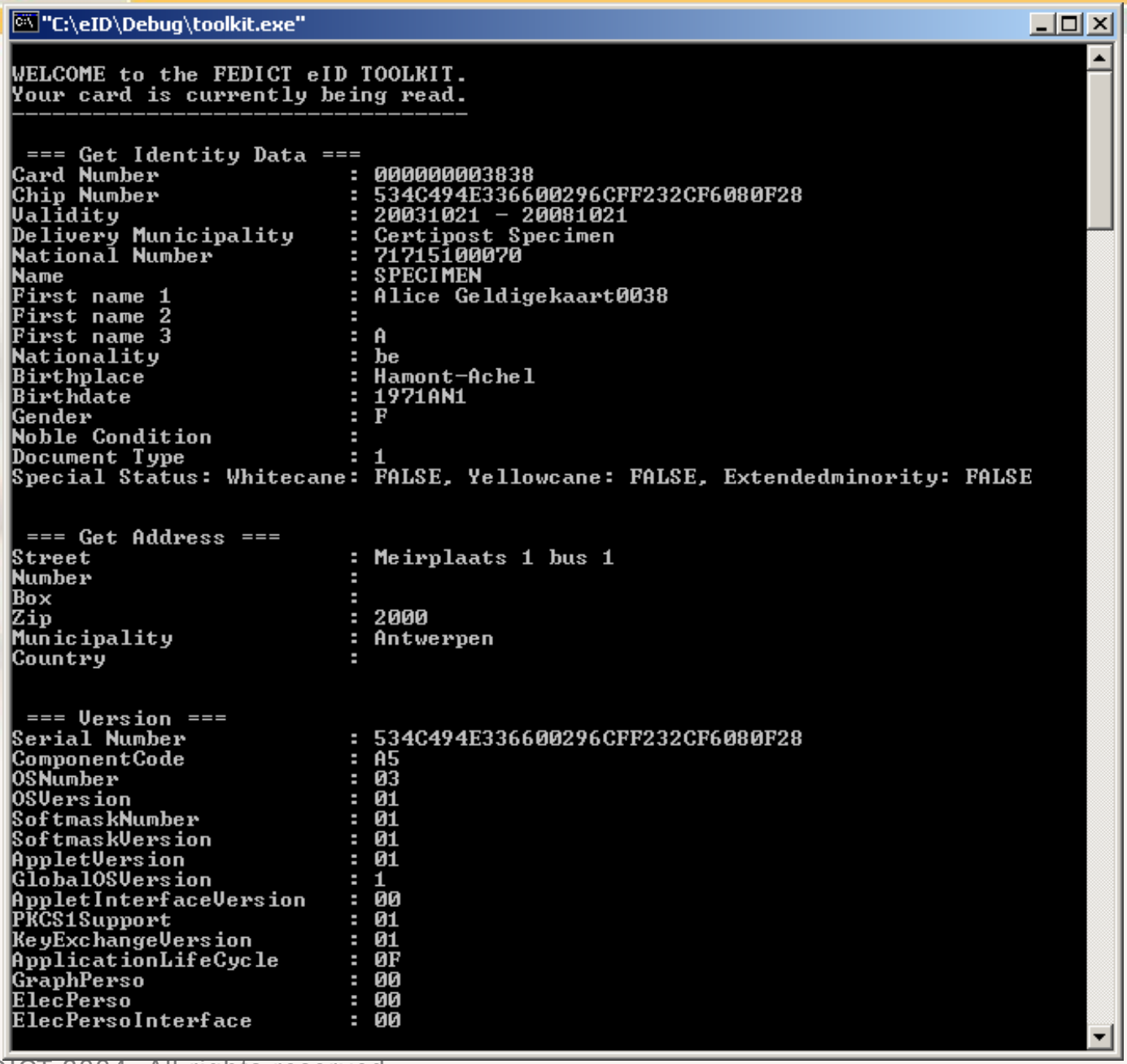
eID-toolkits



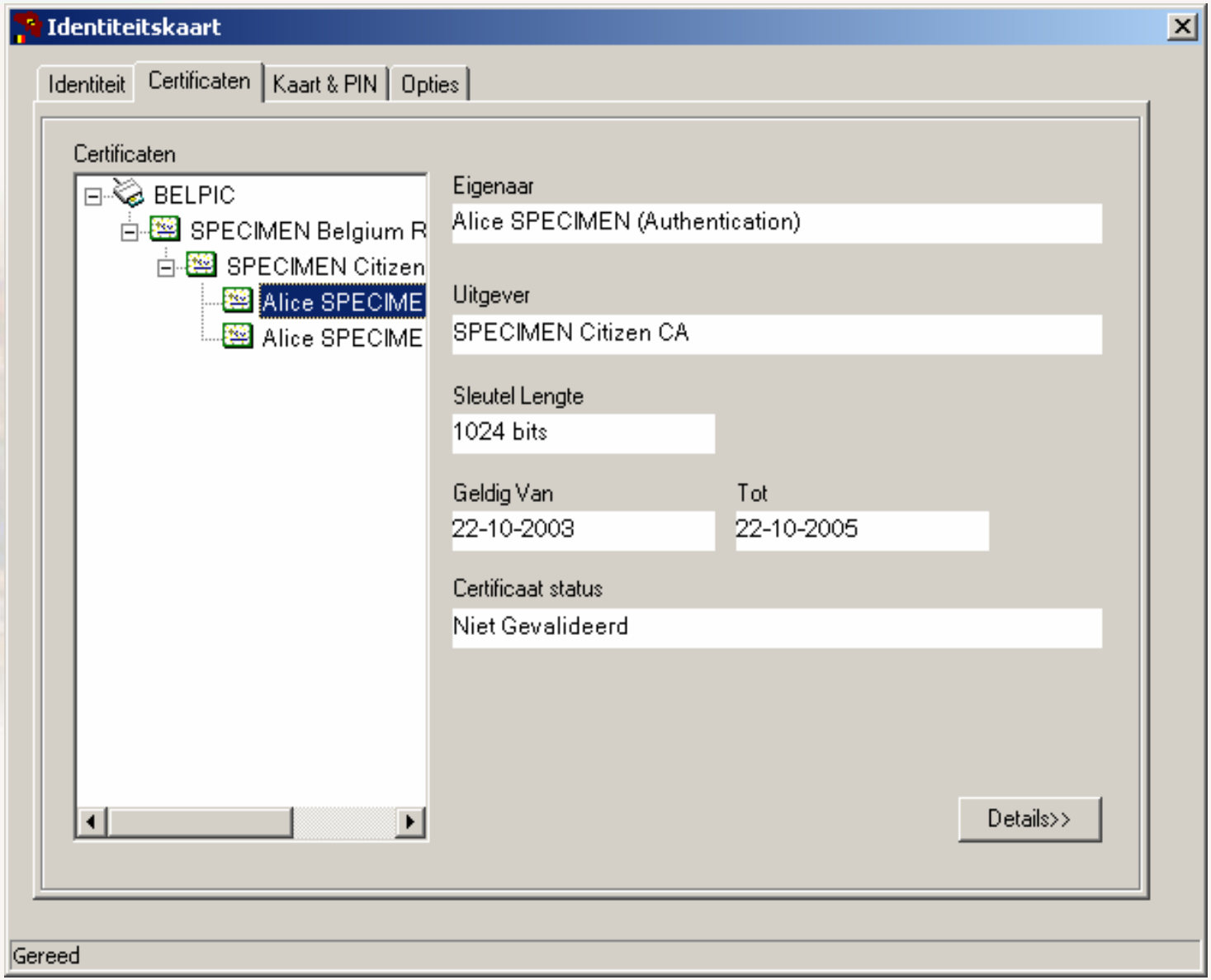
eID-toolkits : Identiteit



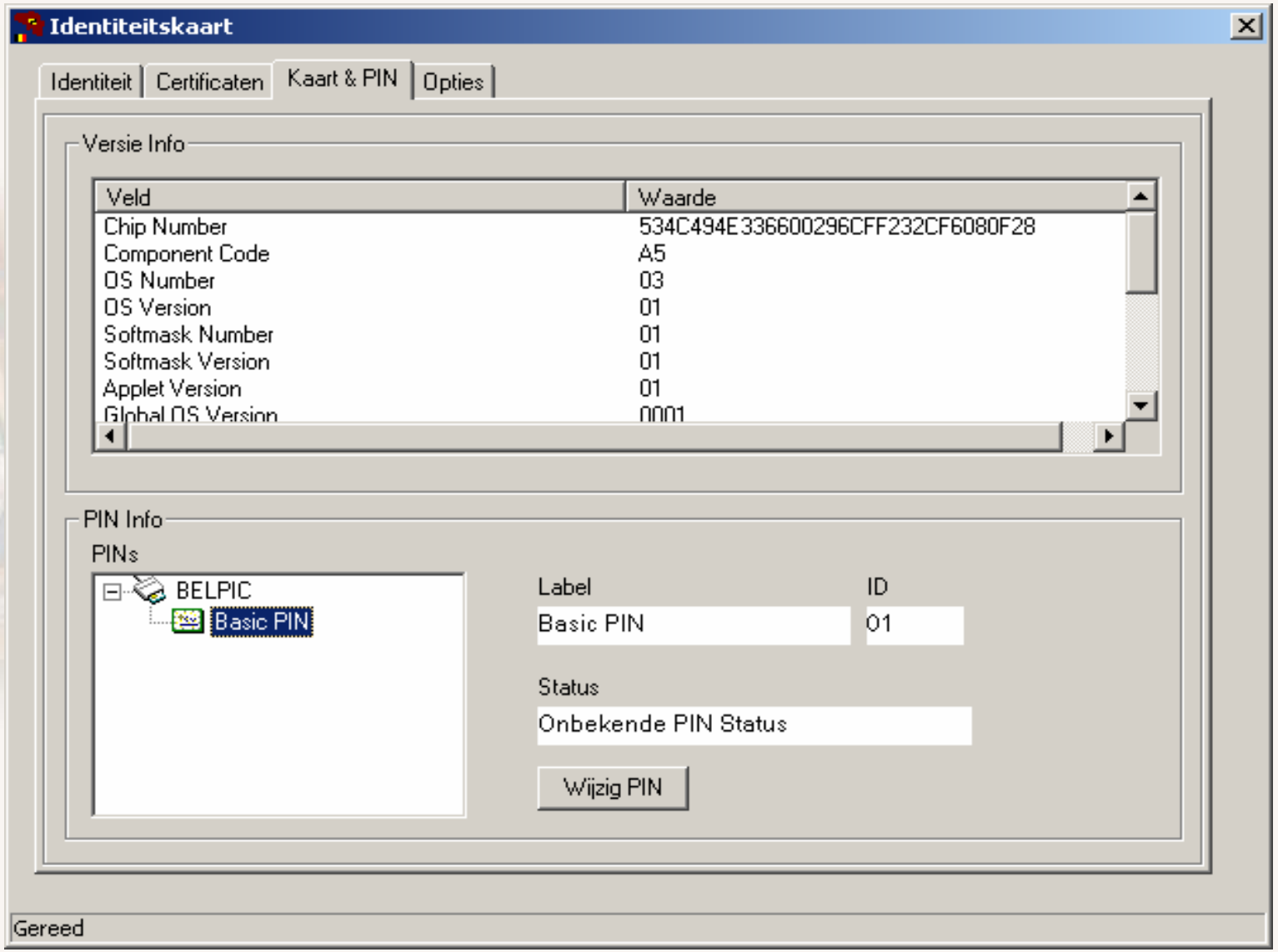
eID-toolkits : library



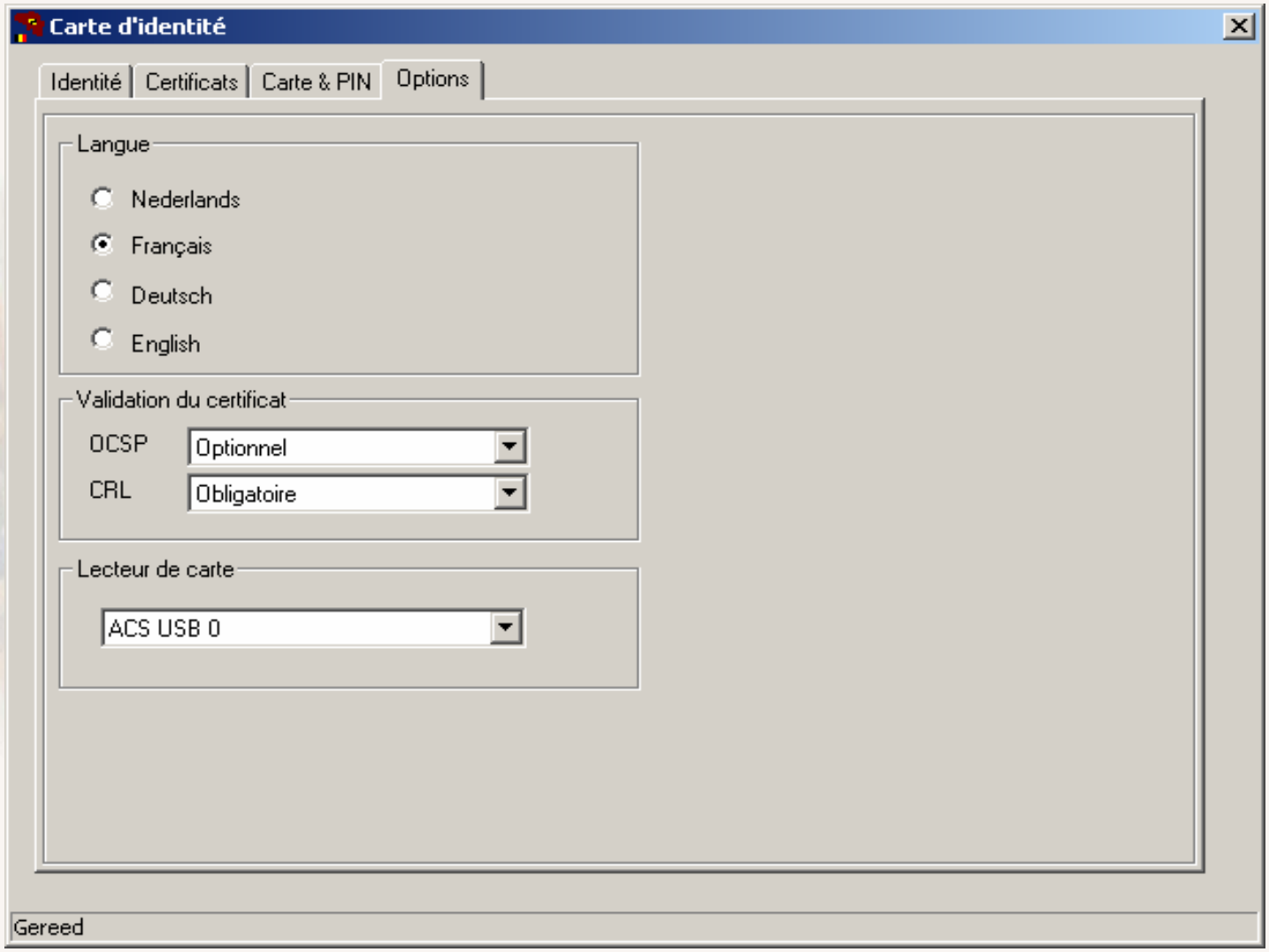
eID-toolkits : Certificaten



eID-toolkits : Kaart & PIN

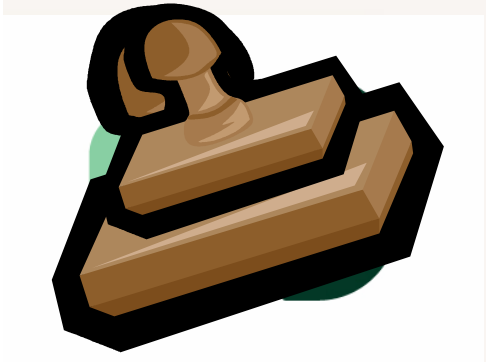


eID-toolkits : Opties



eID - labeling

eID compliance label



- Vereisten:
  - Voor burgers: vertrouwen krijgen in aanbieders van diensten met eID
  - Voor dienstverleners: aantonen dat de 'best practices' effectief zijn toegepast inzake eID gebruik (bv. anti-fraude maatregelen)

- Geïnspireerd door twee two industrie standaarden
  - WebTrust : eCommerce sites
  - SysTrust : eTransaction systems

  Trust Services

  ⇨ Veel auditors beschikbaar
    - Dienstverleners: eenvoudig om een WebTrust/SysTrust accreditatie uit te breiden tot 'eID compliancy'
    - Auditors: eenvoudig om een WebTrust/SysTrust licentie uit te breiden om een eID compliance agent te worden

  ⇨ Snel & Redelijk goedkoop

  ⇨ Niet verplichtend

eID - applicaties

Only the developers' creativity will limit the usage of the eID card.

Een kaart... en dan ?

e-Government applicaties :

- On-line belastingsaangifte www.taxonweb.be
- Inschrijving voertuigen (WEBDIV)
- e-Voting
- Applicaties op gemeentelijk vlak
  - container park (Sint-Pieters-Woluwe)
  - e-loket (Seraing)
  - ...

Een verticale view (sectoren)

- Huis & Werk
- Administratie
- Telecom
- Financiële sector
- Gezondheidszorg
- Transport
- Specifieke groepen

Huis & Werk

Office tools

- ✓ e-mail
- ✓ login (locale PC & netwerk)
- ✓ logon (andere diensten)
- ✓ data & programma confidentialiteit
- ✓ formulieren
- ✓ ...

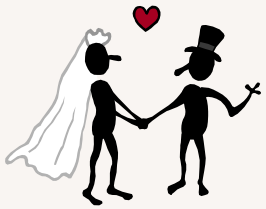
Administratie

Federaal

- ✓ TAX-ON-WEB
- ✓ VAT
- ✓ DIV
- ✓ ...

Gemeentes

- ✓ huwelijk
- ✓ huis
- ✓ kinderen
- ✓ school
- ✓ bibliotheek
- ✓ zwembad
- ✓ container parken
- ✓ ...



Telecom

Telefonie

- ✓ herlaadbare kaarten
- ✓ GSM kaarten ==> UMTS/i-mode

Televisie

- ✓ Pay-TV
- ✓ decryptie-kaarten

Post

- ✓ aangetekende e-mail

Internet

- ✓ VOIP (voice over IP)
- ✓ i-mode

Financiële sector

Identificatie

- ✓ netbanking (userID/Tokens)
- ✓ loket (bank agency)
- ✓ verzekeringscontract (handtekening)

Betalingen

- ✓ credit cards
- ✓ debit cards
- ✓ electronic purse

Gezondheidszorg

Verzekering

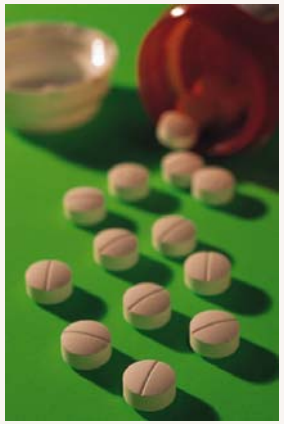
- ✓ MediCard (contract)

Hospitaal

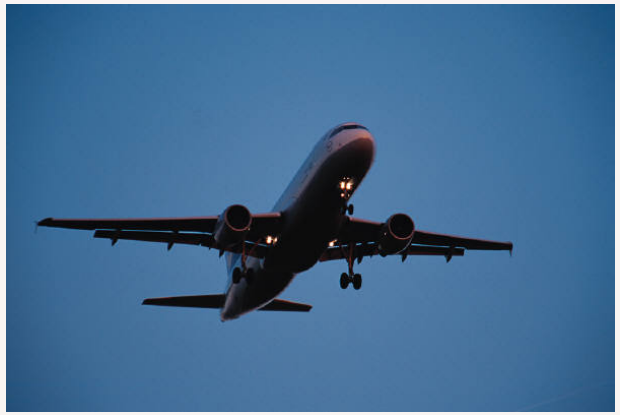
- ✓ privé-gegevens (hospital card, etc)
- ✓ health/emergency data (blood group, etc)

Terugbetaling

- ✓ SIS-kaart
- ✓ apotheek
- ✓ artsen



Transport



Publiek transport

- ✓ ticketing
- ✓ entertainment tijdens vlucht

Parking

- ✓ toegang
- ✓ betaalsystemen

Tankstations

- ✓ tankkaarten
- ✓ getrouwheidskaarten

Specifieke groepen

- Overheid
  - ✓ eProcurement
  - ✓ eSecurity

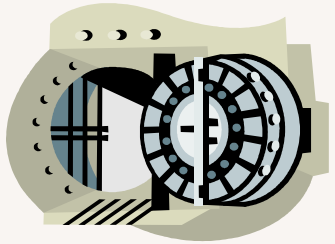
- Universiteiten
  - ✓ resto
  - ✓ boekenwinkel
  - ✓ fotokopieën
  - ✓ bibliotheken

- Administratie

The sky is the limit !

rijbewijs

gezondheidszorg



thuisbankieren, online openen van rekeningen, ...

studentenkaarten, e-learning, ...

...

bewijs van lidmaatschap

SSO, ...

e-commerce

fedict e-gov

eID – vandaag & morgen

.be

Planning

Q1 2004 | Q2 2004 | Q3 2004 | Q4 2004 | Q1 2005

20/3

Piloot fase
Doelgroepen
Evaluatie van piloot fase

BESLISSING

Onder-handelingen

Installatie in gemeentes (578)

Graduele uitrol eID

Continuous advise from and support to enterprises, citizens and authorities

Volgende versies van de eID kaart

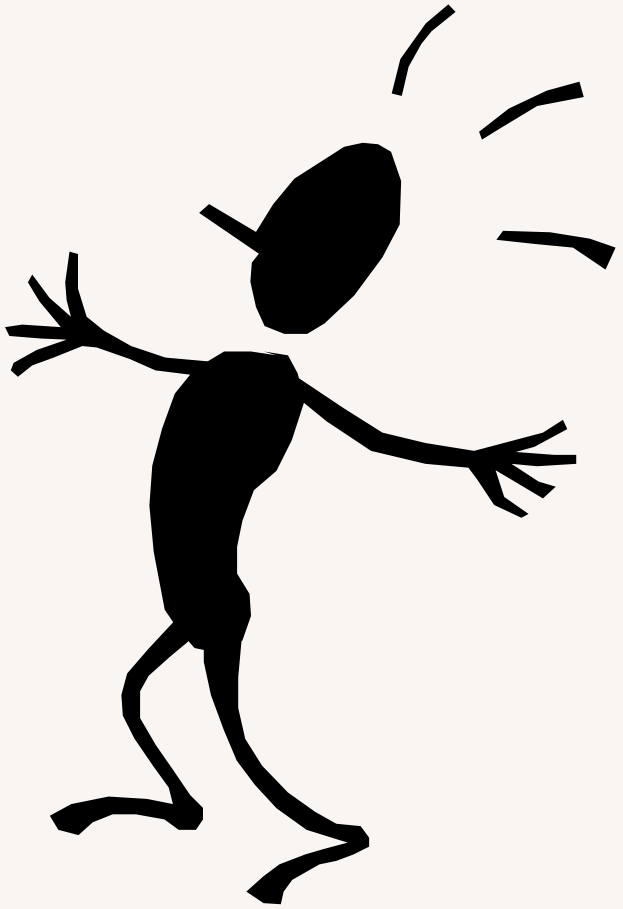
Korte termijn :

- ✓ aanbieden van de mogelijkheid tot het gebruik van twee verschillende PINs voor authentificatie en digitale handtekening
- ✓ integreren van de latest state-of-the art RSA algoritmes
- ✓ gebruik van internationale gegevensformaten
- ✓ offering a more advanced status check
- ✓ providing a structure for using the free space on the chip

Long term :

- ✓ biometrie
- ✓ encryptie certificaten
- ✓ integratie van de SIS kaart
- ✓ integratie van rijbewijs
- ✓ ...

Q&A



Meer informatie

D@nkuwel !

Meer informatie op

www.fedict.be

.be