

De Belgische Electronische Identiteitskaart

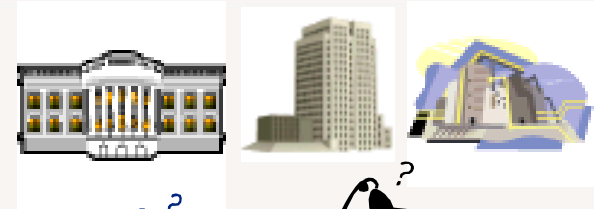
Bart SIJNAVE
Vlaams Parlement

Brussel, 7 oktober 2004

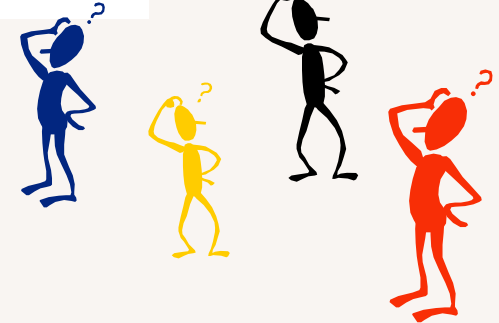


e-government



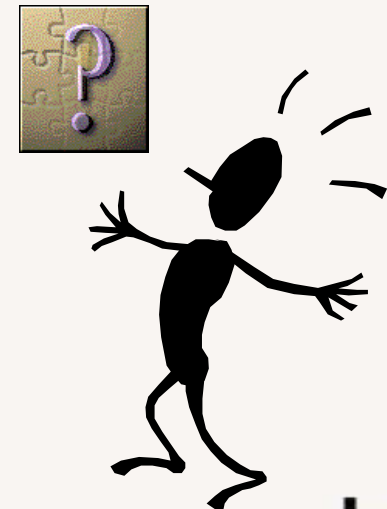



NIET : over 'overheden'

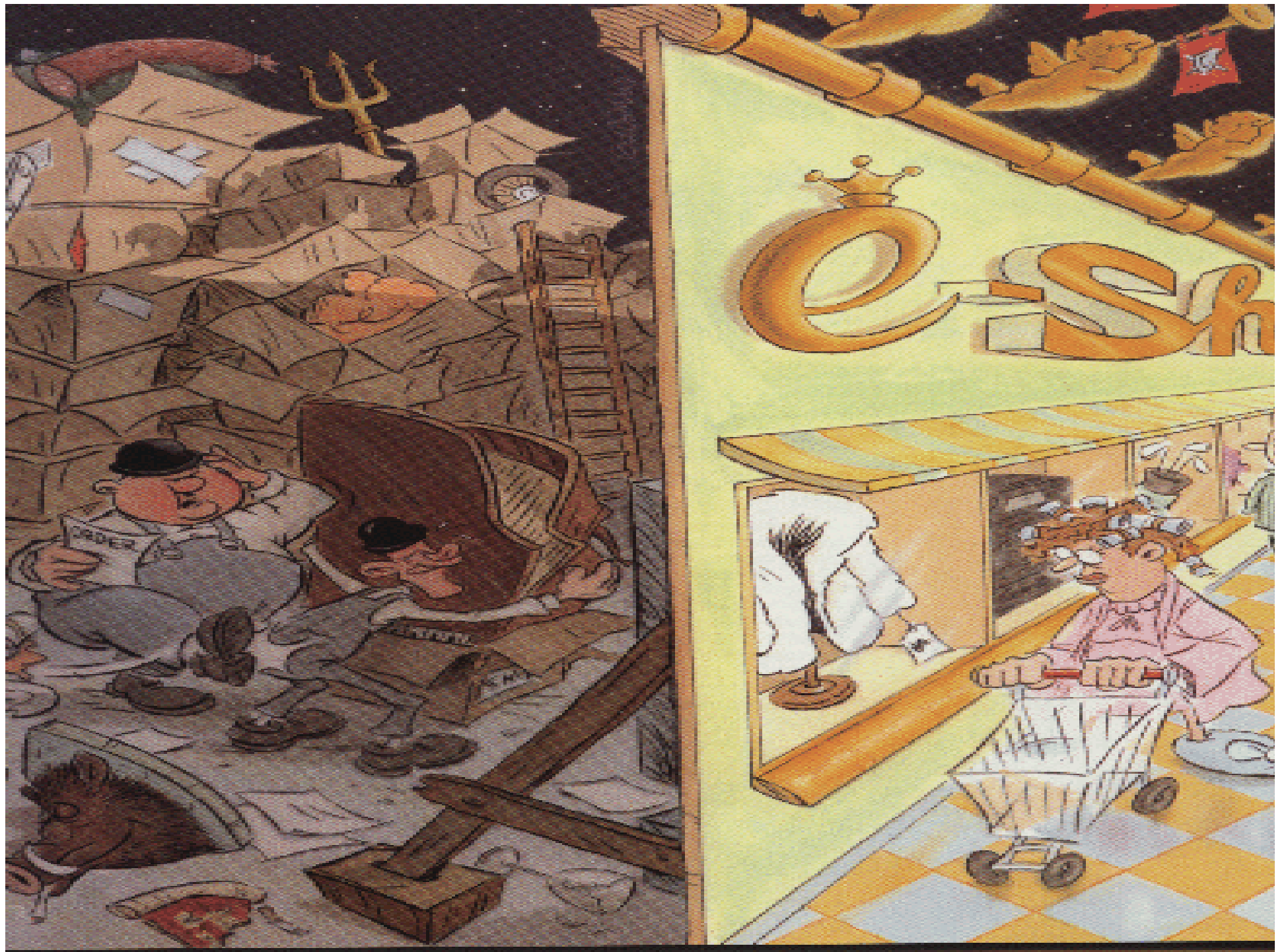


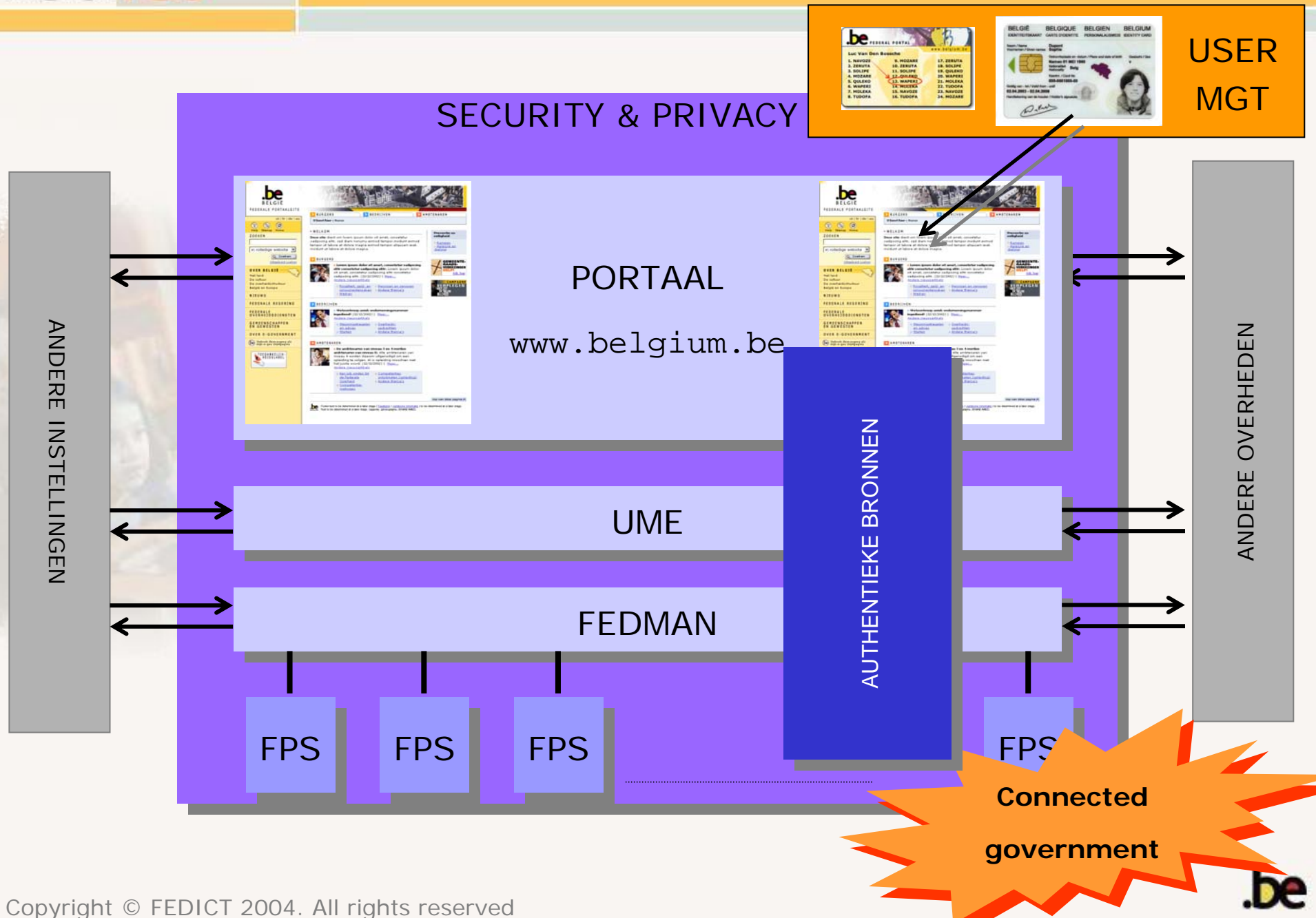
WEL : over 'de klanten van de overheid' :

- ✓ burgers
- ✓ ondernemingen
- ✓ ambtenaren



- 
- ▶ 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





eID - basis

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



Proof of identity

- ▶ Elke burger een elektronische identiteitskaart geven die moet toelaten om zich te **authenticeren** en **digitale handtekeningen te plaatsen**

Signature tool



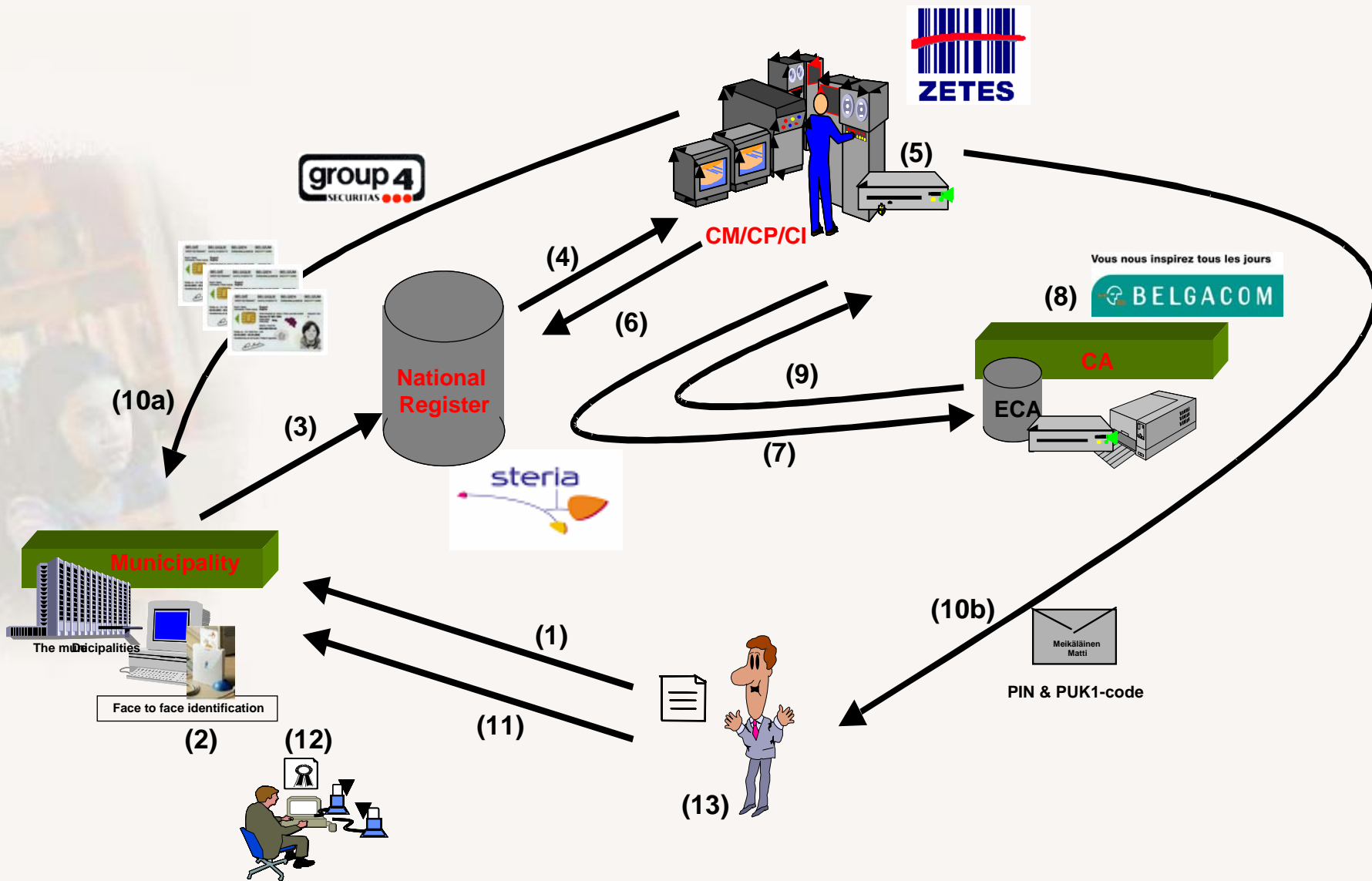
**Visuele
identificatie**
van de houder

- ▶ **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



**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 certificatedienstverlener
 - ◆ informatie noodzakelijk voor de authenticatie 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



eID – chip

eID, welcome to the e-world !

PKI

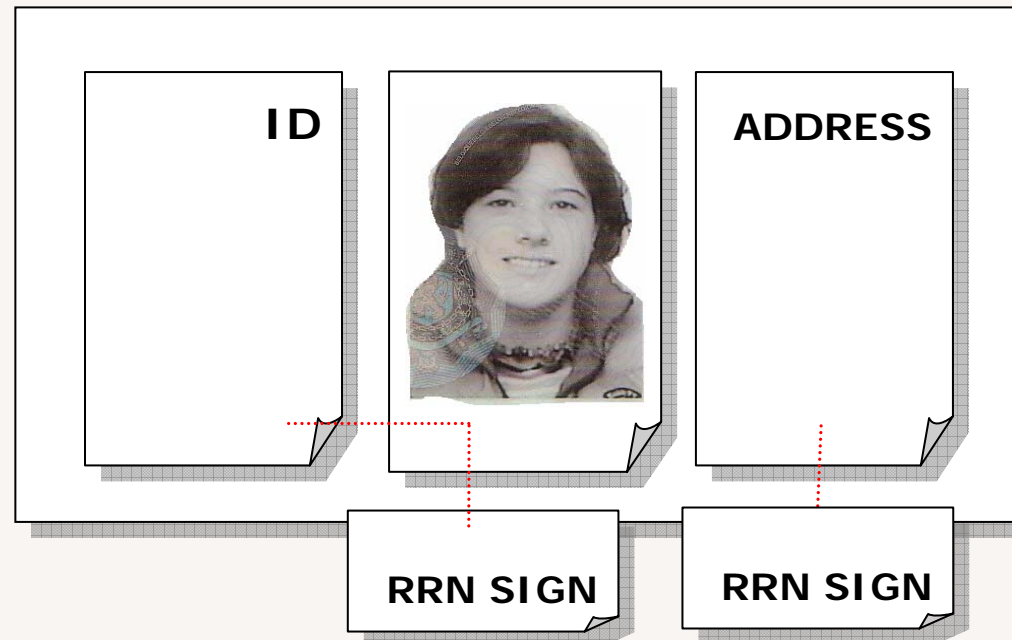


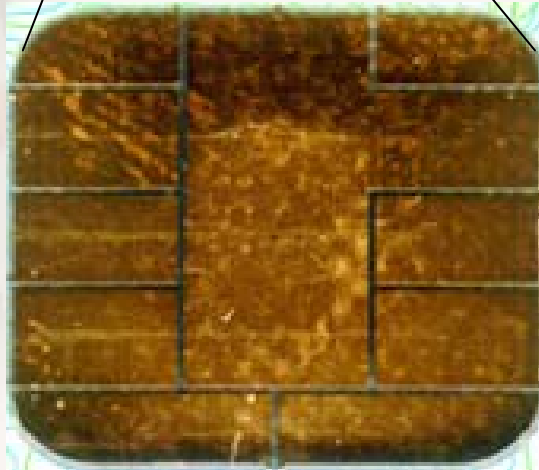
authentication



digital signature

IDENTITY

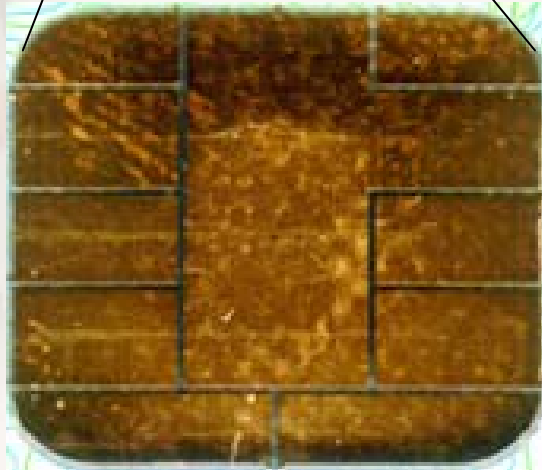




data capture

authenticatie

digitale
handtekening



data capture

authenticatie

digitale

handtekening

▶ faster data capture

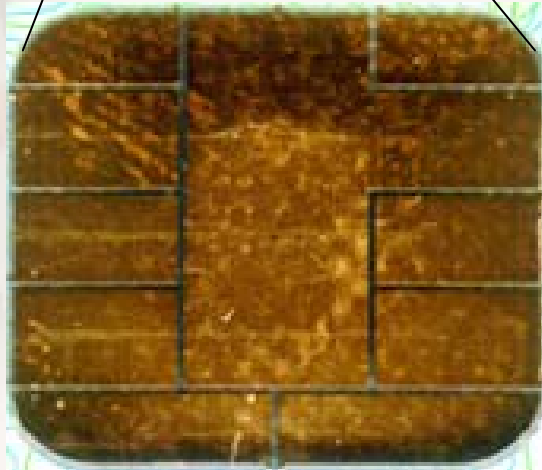
data can be read directly from the card and stored in a particular system

▶ more accurate data capture

no more manual re-entering → less error-prone process

▶ more efficient data capture

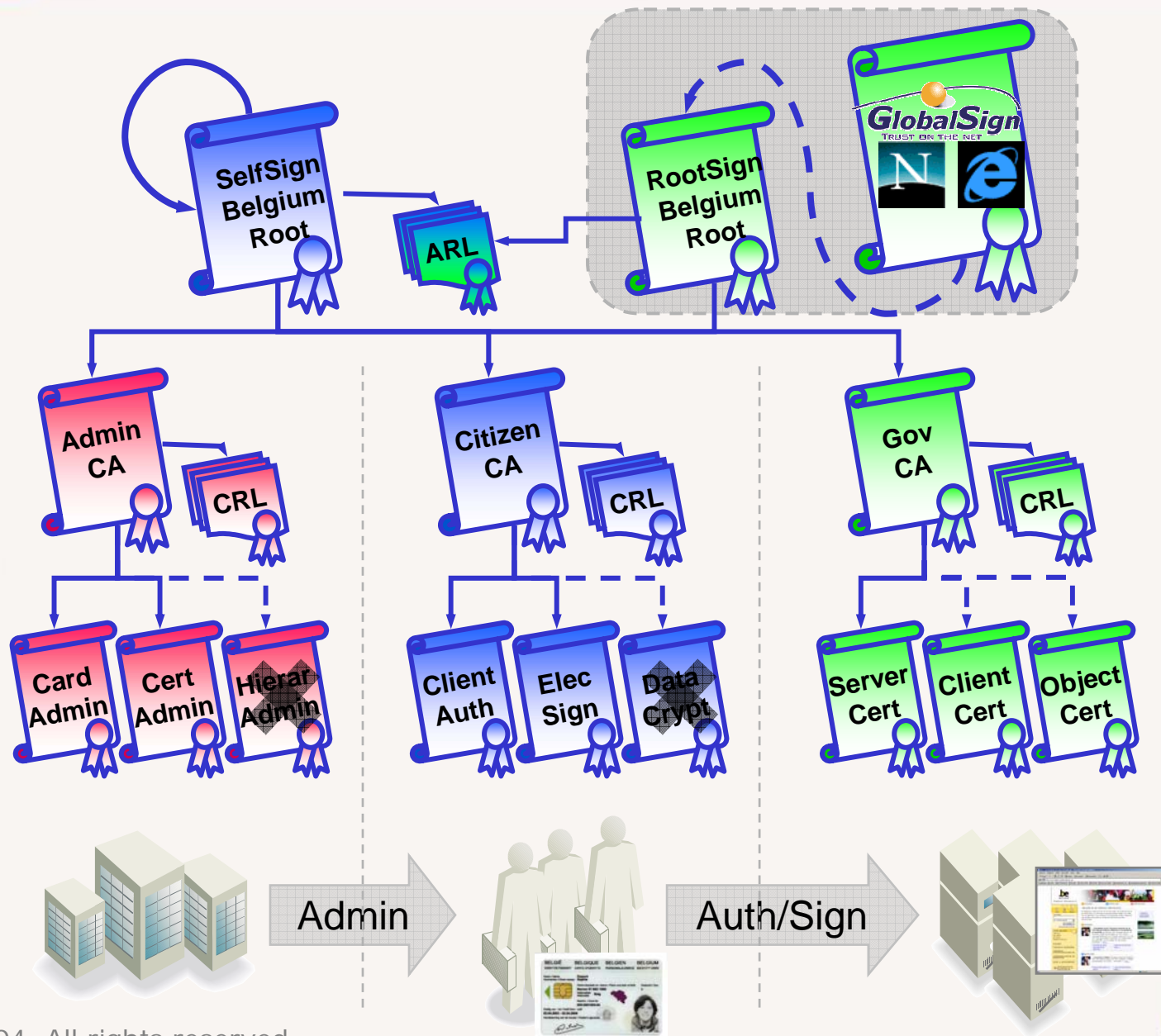
faster processing of information



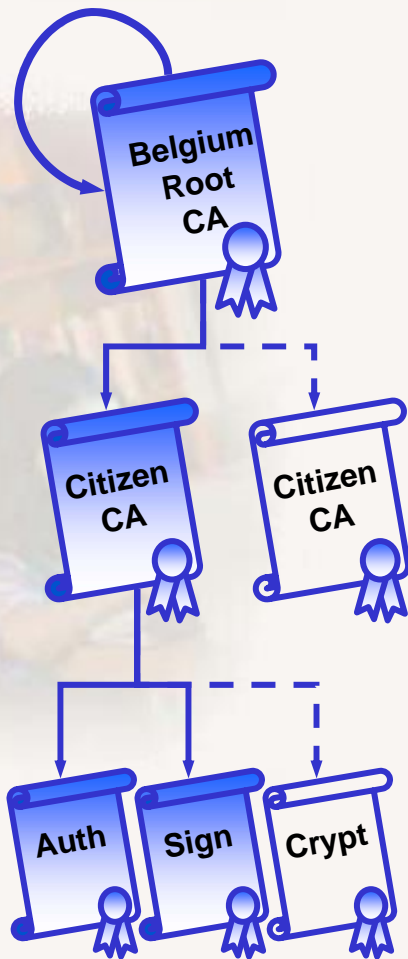
data capture

authenticatie

digitale
handtekening




► Burgercertificaten & -sleutels



- ◆ **Authenticatie**-certificaat & sleutelpaar (1024 bits)
 - voorziet in sterke authenticatie
 - 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 [? X]

Algemeen | Details | Certificeringspad

 **Certificaatinformatie**

Doelinden van dit certificaat:

- het garanderen van de identiteit van een externe computer
- het beschermen van e-mailberichten

* Zie de verklaring van de certificeringsinstantie voor meer info

Verleend aan: Alice SPECIMEN (Authentication)

Verleend door: SPECIMEN Citizen CA

Geldig van 22-10-2003 **t/m** 22-10-2005

Certificaat installeren... Verklaring van verlener

OK

Certificaat [? X]

Algemeen | Details | Certificeringspad

Weergeven: <Alle>

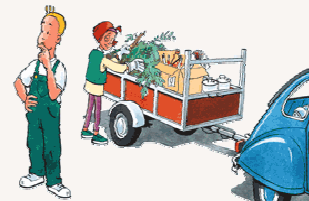
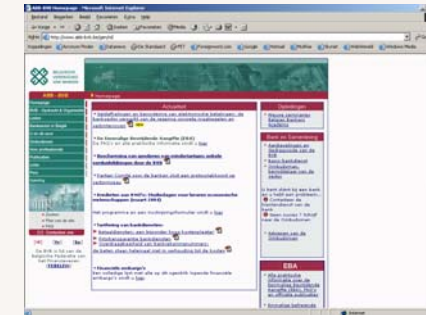
Veld	Waarde
Geldig van	woensdag 22 oktober 2003 8:08...
Geldig tot	zaterdag 22 oktober 2005 8:08:47
Onderwerp	71715100070, Alice Geldigekaar...
Openbare sleutel	RSA (1024 Bits)
Certificaatbeleid	[1]Certificaatsbeleid:Beleids-ID...
Sleutel-ID van CA	Sleutel-ID=13 50 2c a9 03 99 5a...
CRL-distributiepunten	[1]CRL-distributiepunt: Naam va...
NetscapeCertType	SSL-clientverificatie, SMIME(a0)

[1]Certificaatbeleid:
 Beleids-ID=0.3.2062.9.6.1.31.3.1
 [1,1]Beleidskwalificatiegegevens:
 Beleidskwalificatie-ID=CPS
 Kwalificatie:
<http://repository.specimen-eid.belgium.be>

Eigenschappen bewerken... Kopiëren naar bestand...

OK

log on to web sites (SSO)



container park



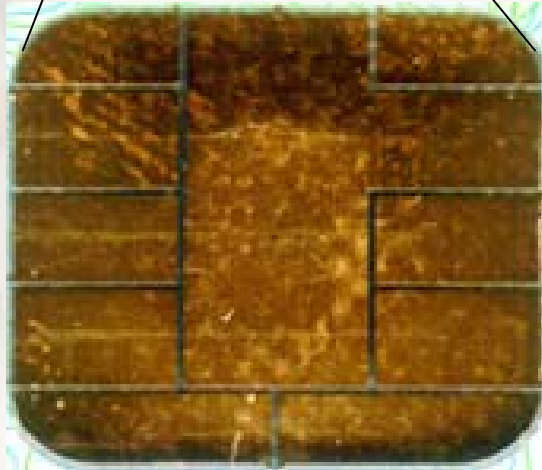
bibliotheek

toegangscontrole



zwembad

...

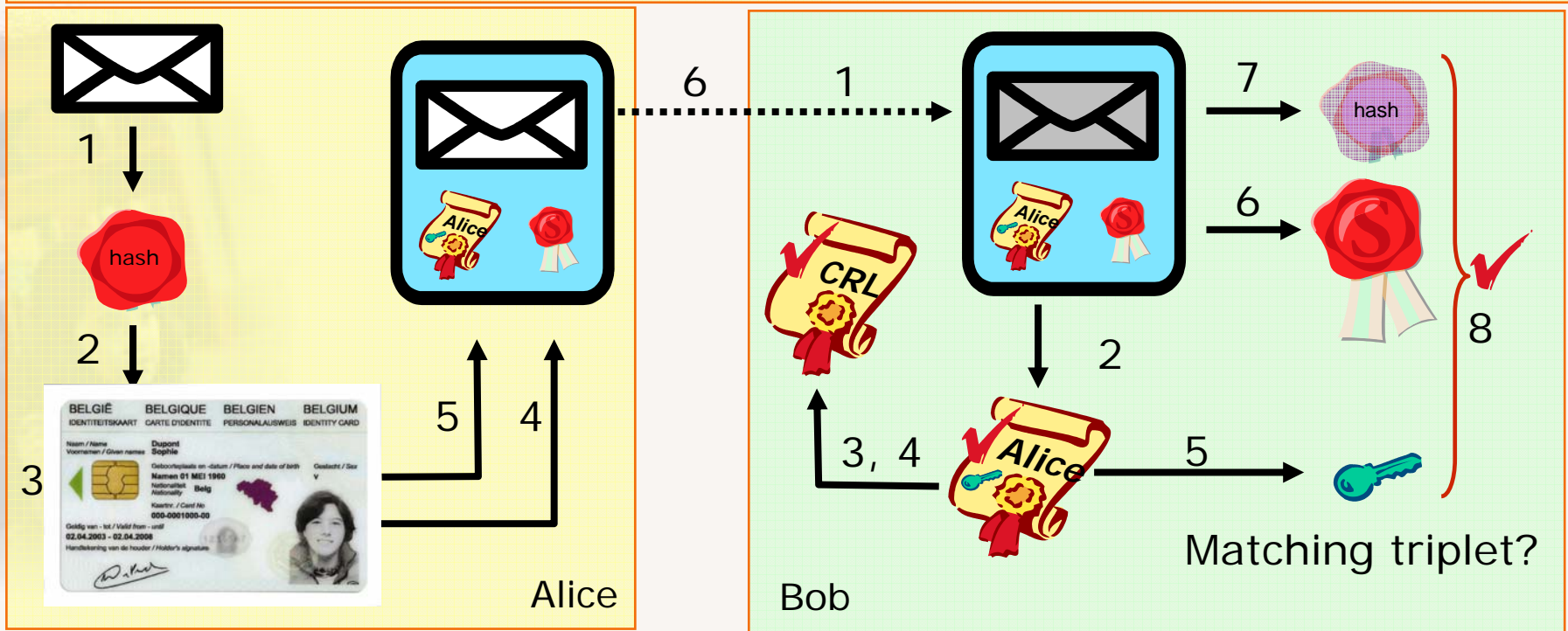


data capture

authenticatie

**digitale
handtekening**

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



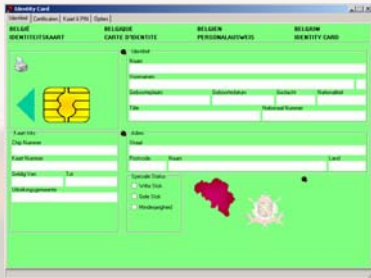
- | | | | |
|------------------------|----------------------|---------------------|---------------------------------------|
| 1. Receive message | 3. Check CRL/OCSP | 5. Fetch public key | 7. Compute reference hash |
| 2. Inspect certificate | 4. Check certificate | 6. Fetch signature | 8. Hash, signature,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

eID - toolkits

Let's make use of the power of eID !

▶ Twee toolkits zijn in testfase :

- ✓ GUI + PKCS#11 libraries : lezen, afdrukken, valideren en visualiseren van de inhoud van de eID chip
- ✓ authentication proxy : eenvoudige authenticatie 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)

Identity Card
_ □ ×

Identiteit | Certificaten | Kaart & PIN | Opties

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

Identiteit

Naam

Voornamen

Geboorteplaats <input style="width: 95%;" type="text"/>	Geboortedatum <input style="width: 95%;" type="text"/>	Geslacht <input style="width: 95%;" type="text"/>	Nationaliteit <input style="width: 95%;" type="text"/>
Title <input style="width: 95%;" type="text"/>		Nationaal Nummer <input style="width: 95%;" type="text"/>	

Kaart Info

Chip Nummer

Kaart Nummer

Geldig Van <input style="width: 95%;" type="text"/>	Tot <input style="width: 95%;" type="text"/>
---	--

Uitreikingsgemeente

Adres

Straat

Postcode <input style="width: 95%;" type="text"/>	Naam <input style="width: 95%;" type="text"/>	Land <input style="width: 95%;" type="text"/>
---	---	---

Speciale Status

Witte Stok

Gele Stok


Minderjarigheid

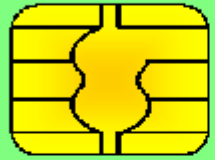
Copyright © FEDICT 2004. All rights reserved

Identity Card
_ □ ×

Identiteit | Certificaten | Kaart & PIN | Opties

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





Identiteit

Naam
SPECIMEN

Voornamen
Alice Geldigekaart0783 A

Geboorteplaats	Geboortedatum	Geslacht	Nationaliteit
Hamont-Achel	01/01/1970	F	be

Title Nationaal Nummer

71.71.51-000.70

Kaart Info

Chip Nummer
534C494E336600296CFF232CF6080C1

Kaart Nummer
000.0000783.07

Geldig Van	Tot
26/03/2004	26/03/2009

Uitreikingsgemeente
ZETES

Adres

Straat
Meirplaats 1 bus 1



Postcode	Naam	Land
2000	Antwerpen	be

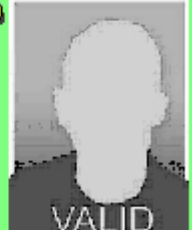
Speciale Status

Witte Stok

Gele Stok

Minderjarigheid



VALID

Gereed

```
C:\eID\Debug\toolkit.exe
WELCOME to the FEDICT eID TOOLKIT.
Your card is currently being read.
-----
=== Get Identity Data ===
Card Number      : 0000000003838
Chip Number      : 534C494E336600296CFF232CF6080F28
Validity         : 20031021 - 20081021
Delivery Municipality : Certipost Specimen
National Number  : 71715100070
Name             : SPECIMEN
First name 1     : Alice Geldigekaart0038
First name 2     :
First name 3     : A
Nationality      : be
Birthplace       : Hamont-Achel
Birthdate        : 1971A01
Gender           : F
Noble Condition  :
Document Type    : 1
Special Status: Whitecane: FALSE, Yellowcane: FALSE, Extendedminority: FALSE

=== Get Address ===
Street           : Meirplaats 1 bus 1
Number          :
Box             :
Zip             : 2000
Municipality     : Antwerpen
Country         :

=== Version ===
Serial Number    : 534C494E336600296CFF232CF6080F28
ComponentCode    : A5
OSNumber         : 03
OSVersion        : 01
SoftmaskNumber   : 01
SoftmaskVersion  : 01
AppletVersion    : 01
GlobalOSVersion  : 1
AppletInterfaceVersion : 00
PKCS1Support     : 01
KeyExchangeVersion : 01
ApplicationLifeCycle : 0F
GraphPerso       : 00
ElecPerso        : 00
ElecPersoInterface : 00
```

Identiteitskaart [X]

Identiteit | **Certificaten** | Kaart & PIN | Opties

Certificaten

- [-] BELPIC
 - [-] SPECIMEN Belgium R
 - [-] SPECIMEN Citizen
 - Alice SPECIME**
 - Alice SPECIME

Eigenaar
Alice SPECIMEN (Authentication)

Uitgever
SPECIMEN Citizen CA

Sleutel Lengte
1024 bits

Geldig Van	Tot
22-10-2003	22-10-2005

Certificaat status
Niet Gevalideerd

Details>>

Gereed

Identiteitskaart [X]



Identiteit | Certificaten | **Kaart & PIN** | Opties

Versie Info

Veld	Waarde
Chip Number	534C494E 336600296CFF232CF6080F28
Component Code	A5
OS Number	03
OS Version	01
Softmask Number	01
Softmask Version	01
Applet Version	01
Global OS Version	0001

PIN Info

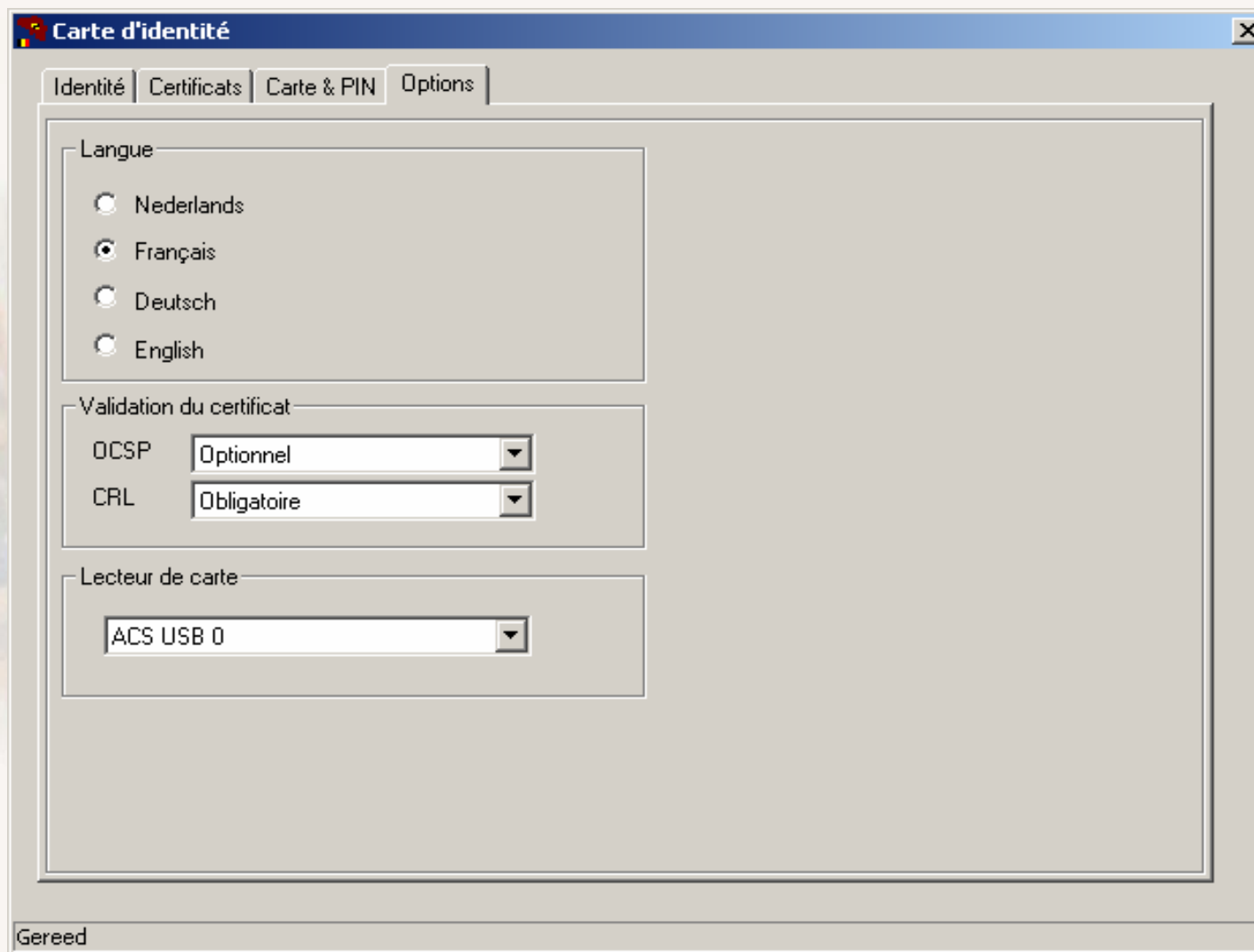
PINs

 BELPIC
 Basic PIN

Label	ID
Basic PIN	01
Status	Onbekende PIN Status

Wijzig PIN

Gereed

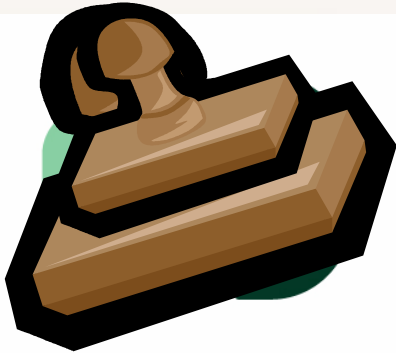


The screenshot shows a software window titled "Carte d'identité" with a close button in the top right corner. The window has four tabs: "Identité", "Certificats", "Carte & PIN", and "Options", with "Options" being the active tab. The main content area is divided into three sections:

- Langue:** A group box containing four radio buttons: "Nederlands", "Français" (which is selected), "Deutsch", and "English".
- Validation du certificat:** A group box containing two dropdown menus: "OCSP" set to "Optionnel" and "CRL" set to "Obligatoire".
- Lecteur de carte:** A group box containing a dropdown menu set to "ACS USB 0".

At the bottom left of the window, the text "Gereed" is displayed.



eID - labeling



▶ 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 twee industrie standaarden

- ◆  : eCommerce sites
 - ◆  : 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.

e-Government applicaties :

- ◆ On-line belastingaangifte
- ◆ Inschrijving voertuigen (WEBDIV)
- ◆ e-Voting
- ◆ Applicaties op gemeentelijk vlak
 - container park (Sint-Pieters-Woluwe)
 - e-loket (Seraing)
 - ...



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

▶ **Office tools**

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



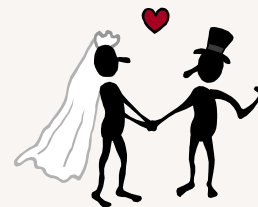
▶ **Federaal**

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



▶ **Gemeentes**

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



▶ **Telefonie**

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



▶ **Televisie**

- ✓ Pay-TV
- ✓ decryptie-kaarten

▶ **Post**

- ✓ aangetekende e-mail

◆ **Internet**

- ✓ VOIP (voice over IP)
- ✓ i-mode



► Identificatie

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



► Betalingen

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



▶ **Verzekering**

- ✓ MediCard (contract)



▶ **Hospitaal**

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

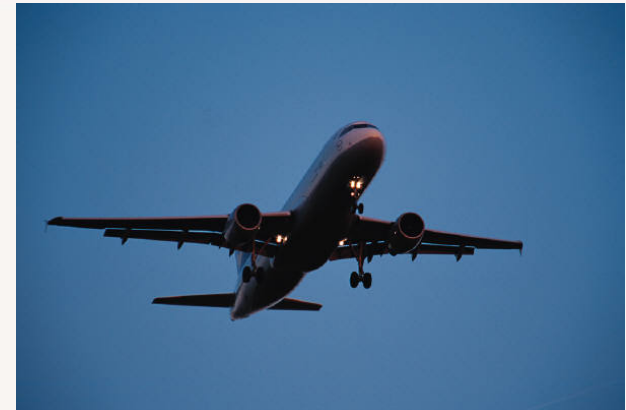
◆ **Terugbetaling**

- ✓ SIS-kaart
- ✓ apotheek
- ✓ artsen



▶ **Publiek transport**

- ✓ ticketing
- ✓ entertainment tijdens vlucht



▶ **Parking**

- ✓ toegang
- ✓ betaalsystemen

▶ **Tankstations**

- ✓ tankkaarten
- ✓ getrouwheidskaarten



▶ **Overheid**

- ✓ eProcurement
- ✓ eSecurity

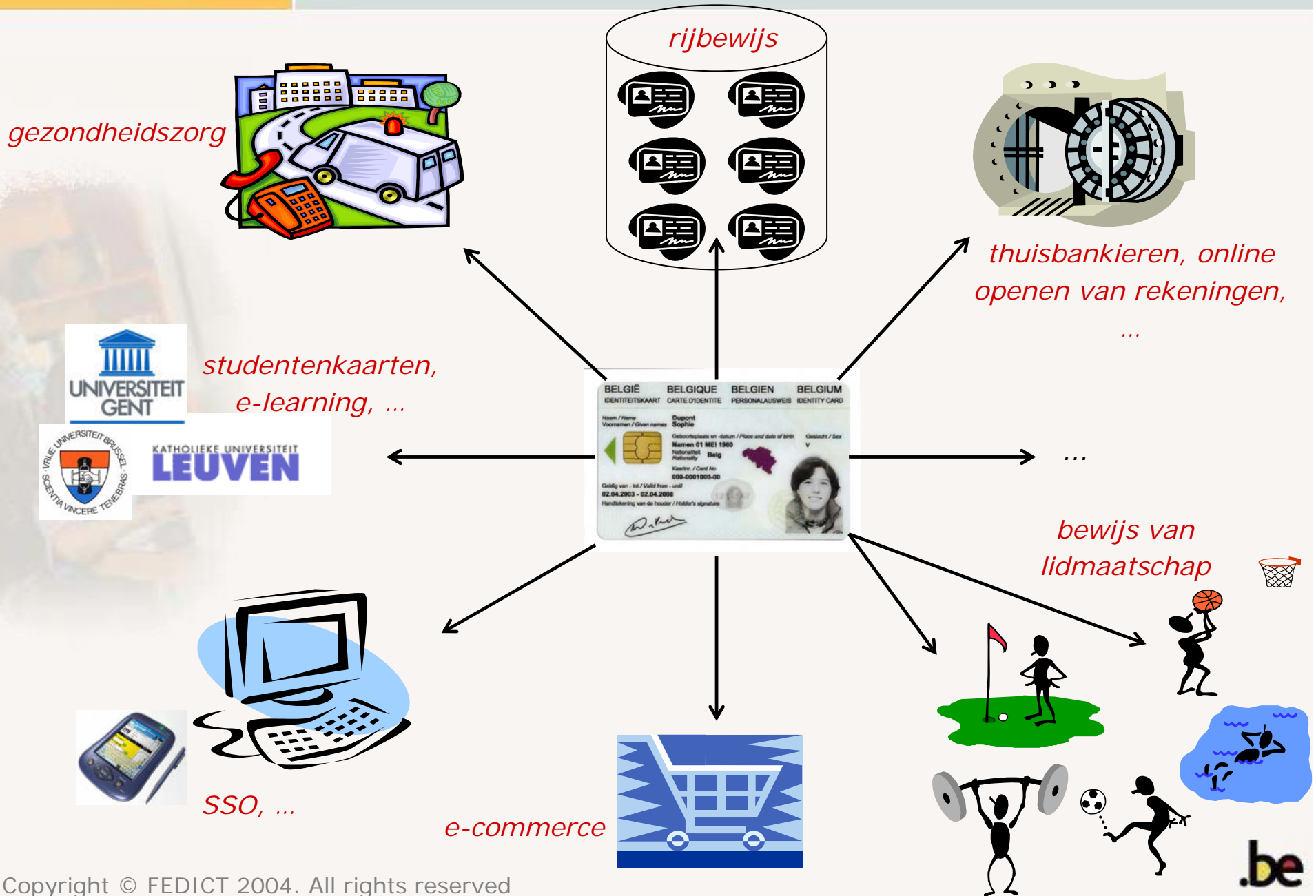


▶ **Universiteiten**

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



▶ **Administratie**





eID – vandaag & morgen

Q1 2004 Q2 2004 Q3 2004 Q4 2004 Q1 2005

20/3

Piloot fase
Doelgroepen
Evaluatie van
piloot fase

B
E
S
L
I
S
S
I
N
G

Onder-
handelingen

Installatie in gemeentes (578)

Graduele uitrol eID

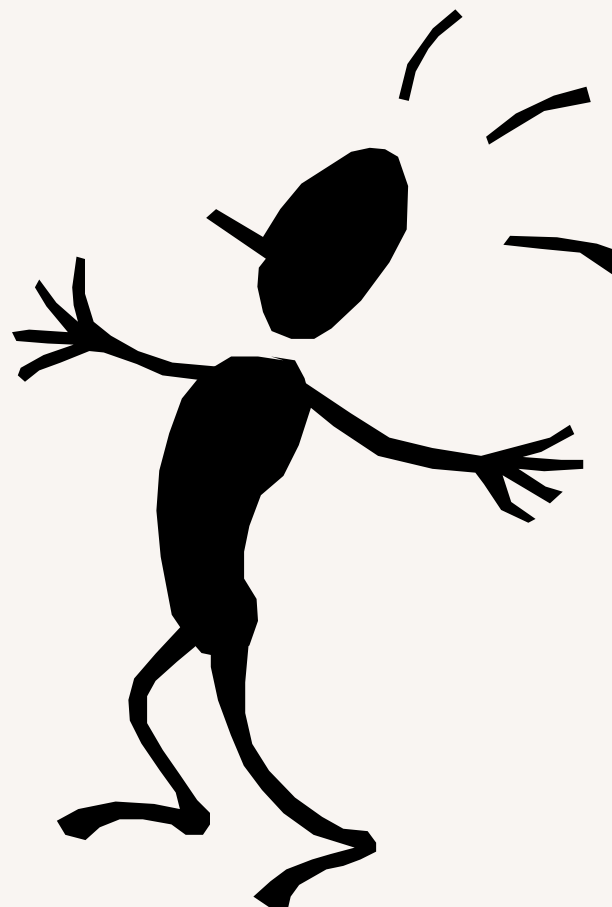
Continuous advise from and support to enterprises, citizens
and authorities

Korte termijn :

- ✓ aanbieden van de mogelijkheid tot het gebruik van twee verschillende PINs voor **authenticatie** 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
- ✓ ...



D@nkuwel !

Meer informatie op

www.fedict.be