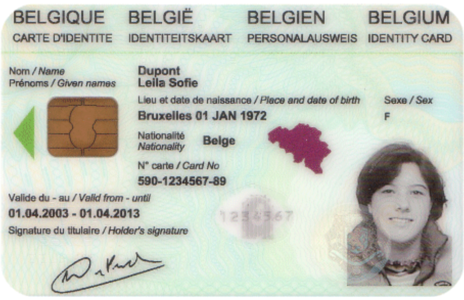
The Belgian eID card

Physical and Optical Security Features

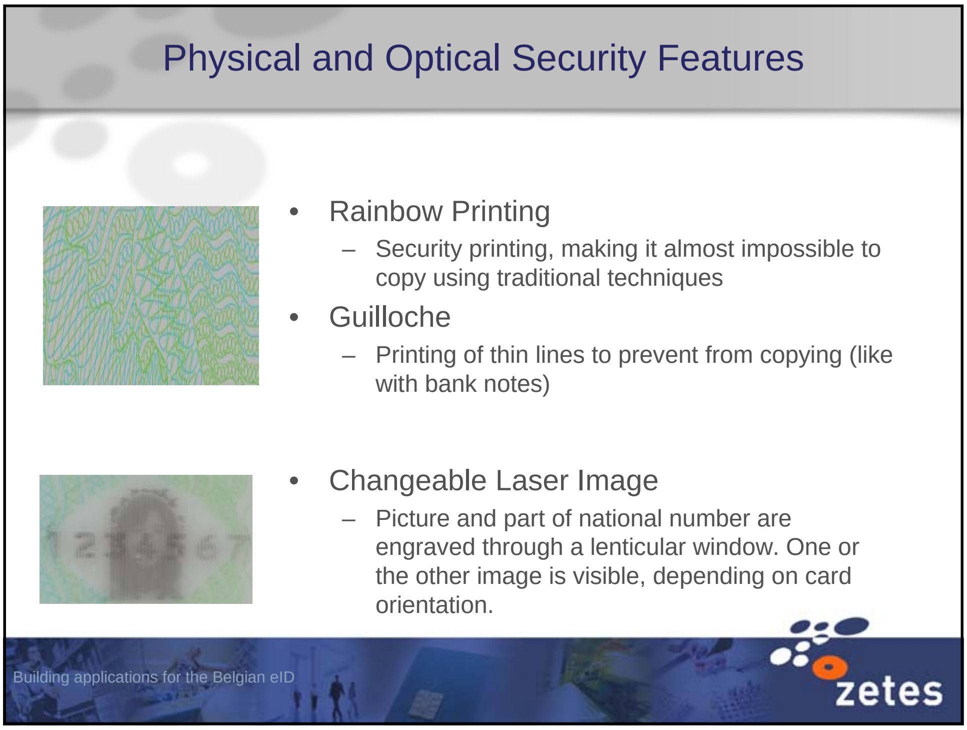
Physical elements



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

Nom / *Name*: Dupont
Prénoms / *Given names*: Leila Sofie
Lieu et date de naissance / *Place and date of birth*: Bruxelles 01 JAN 1972
Sexe / *Sex*: F
Nationalité / *Nationality*: Belge
N° carte / *Card No*: 590-1234567-89
Valide du - au / *Valid from - until*: 01.04.2003 - 01.04.2013
Signature du titulaire / *Holder's signature*

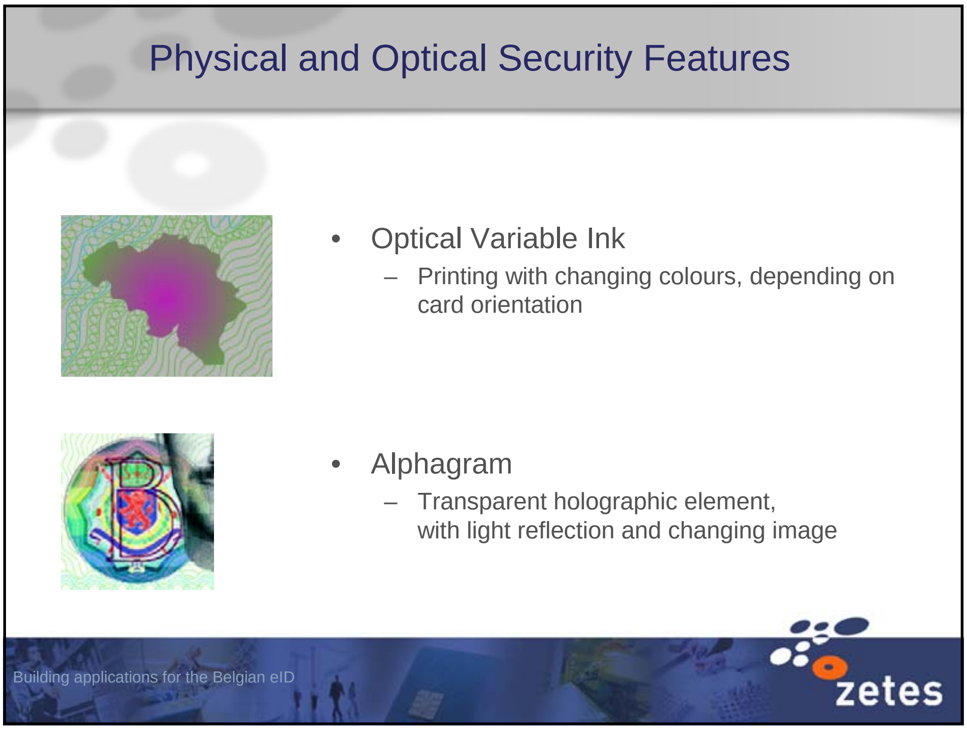
- Card made of durable polycarbonat
- Standard bank card format (ISO)
- Very rich set of physical security elements



Physical and Optical Security Features

- Rainbow Printing
  - Security printing, making it almost impossible to copy using traditional techniques
- Guilloche
  - Printing of thin lines to prevent from copying (like with bank notes)

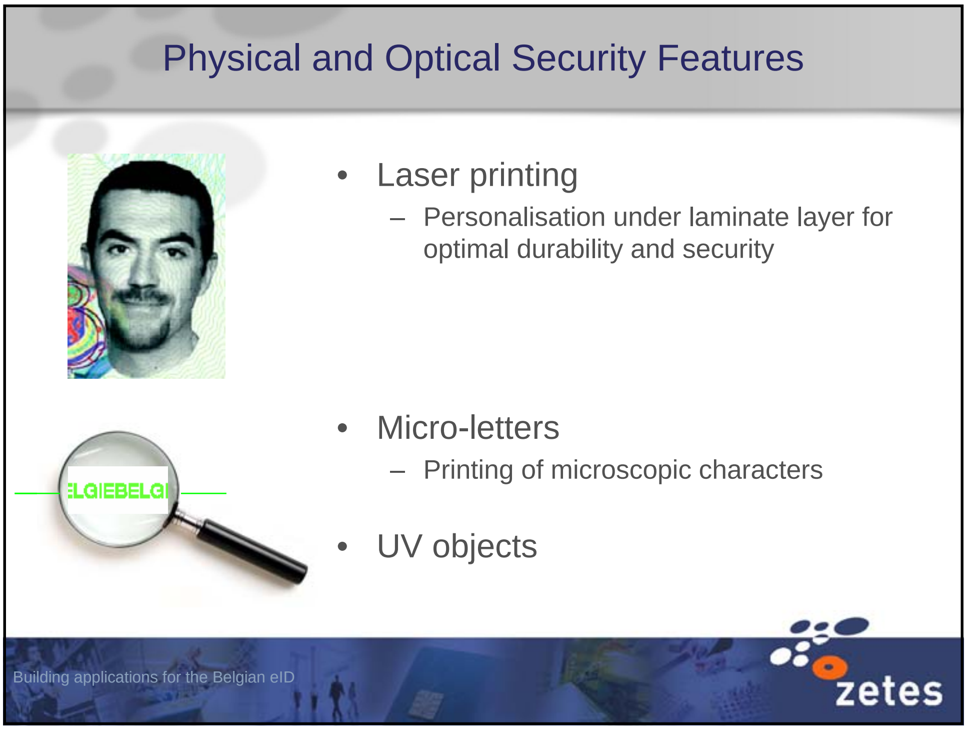
- Changeable Laser Image
  - Picture and part of national number are engraved through a lenticular window. One or the other image is visible, depending on card orientation.



Physical and Optical Security Features

- Optical Variable Ink
  - Printing with changing colours, depending on card orientation

- Alphagram
  - Transparent holographic element, with light reflection and changing image

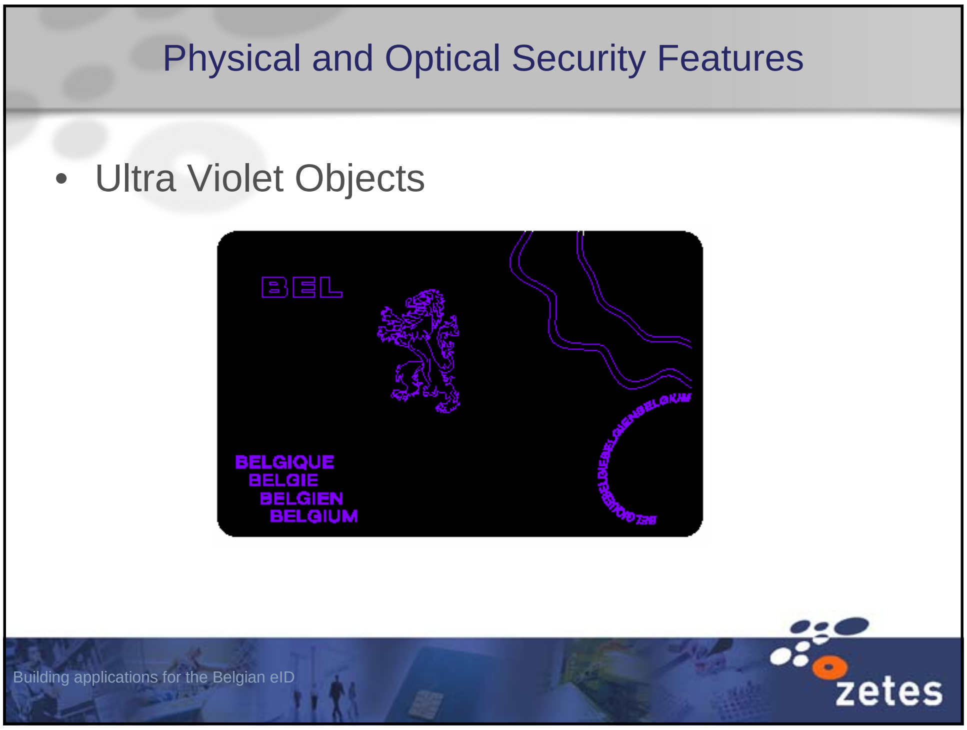


Physical and Optical Security Features

- Laser printing
  - Personalisation under laminate layer for optimal durability and security
- Micro-letters
  - Printing of microscopic characters
- UV objects

Building applications for the Belgian eID

zetes

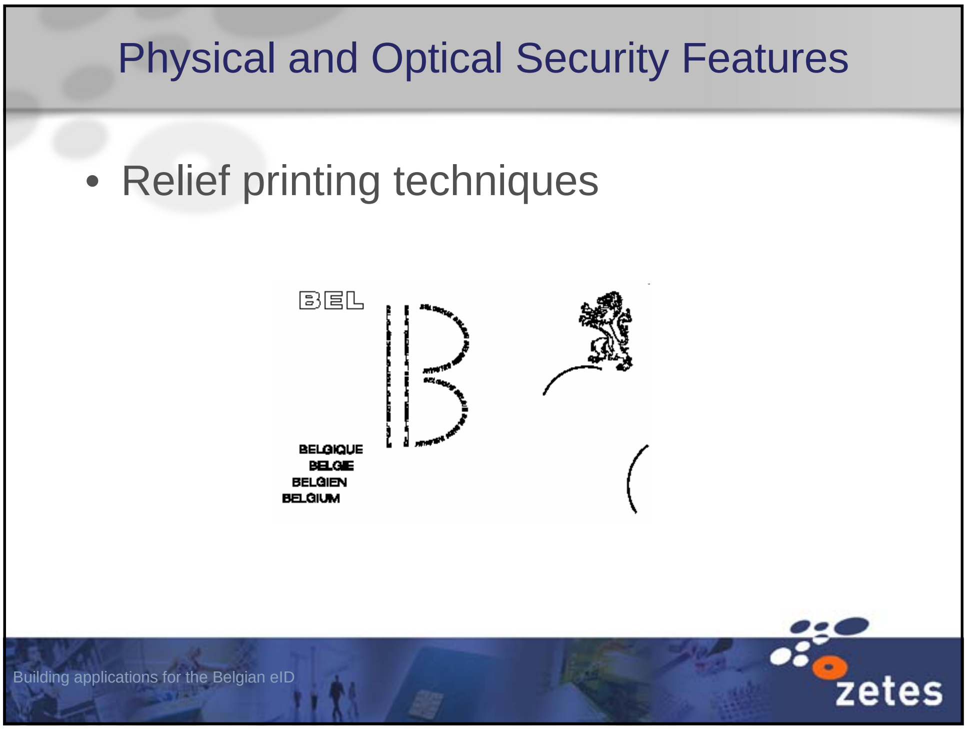


Physical and Optical Security Features

- Ultra Violet Objects

Building applications for the Belgian eID

zetes



Physical and Optical Security Features

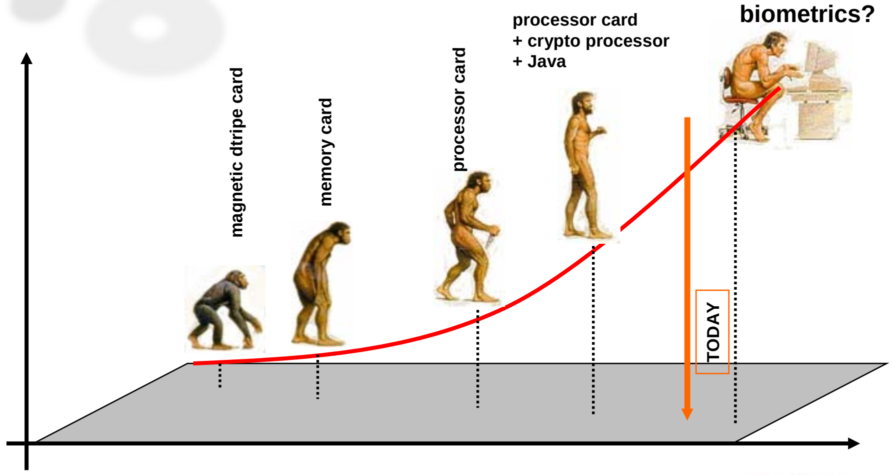
- Relief printing techniques

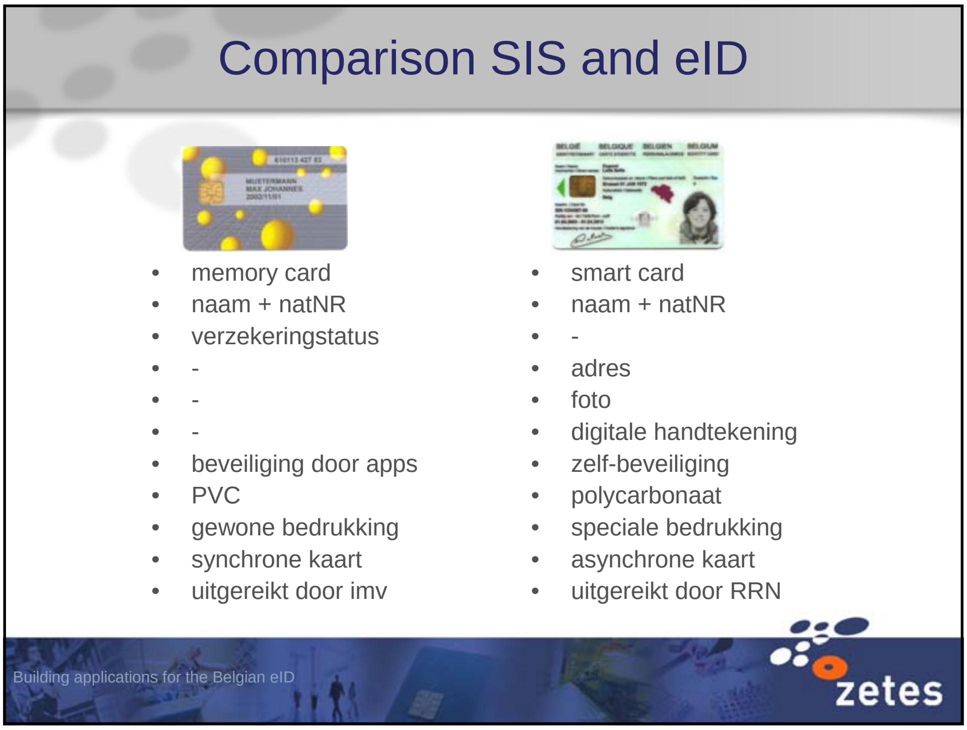
Building applications for the Belgian eID

Belgian eID card

Electronic Functions

Evolution



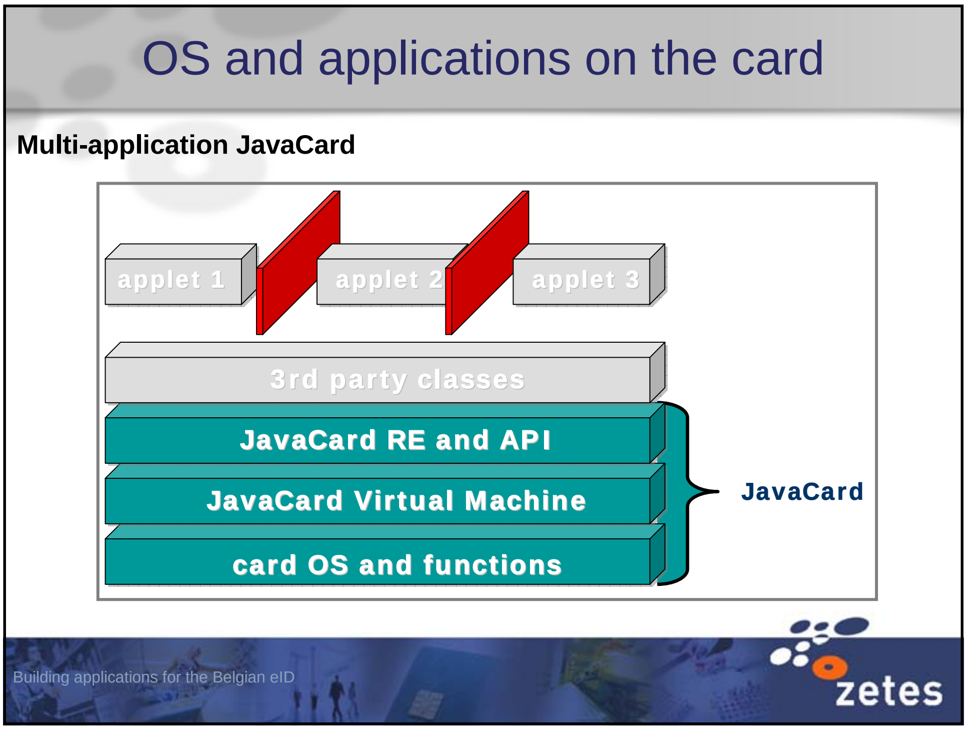


Comparison SIS and eID

memory card	smart card
naam + natNR	naam + natNR
verzekeringstatus	-
-	adres
-	foto
-	digitale handtekening
beveiliging door apps	zelf-beveiliging
PVC	polycarbonaat
gewone bedrukking	speciale bedrukking
synchrone kaart	asynchrone kaart
uitgereikt door imv	uitgereikt door RRN

Building applications for the Belgian eID

zetes



OS and applications on the card

Multi-application JavaCard

applet 1

applet 2

applet 3

3rd party classes

JavaCard RE and API

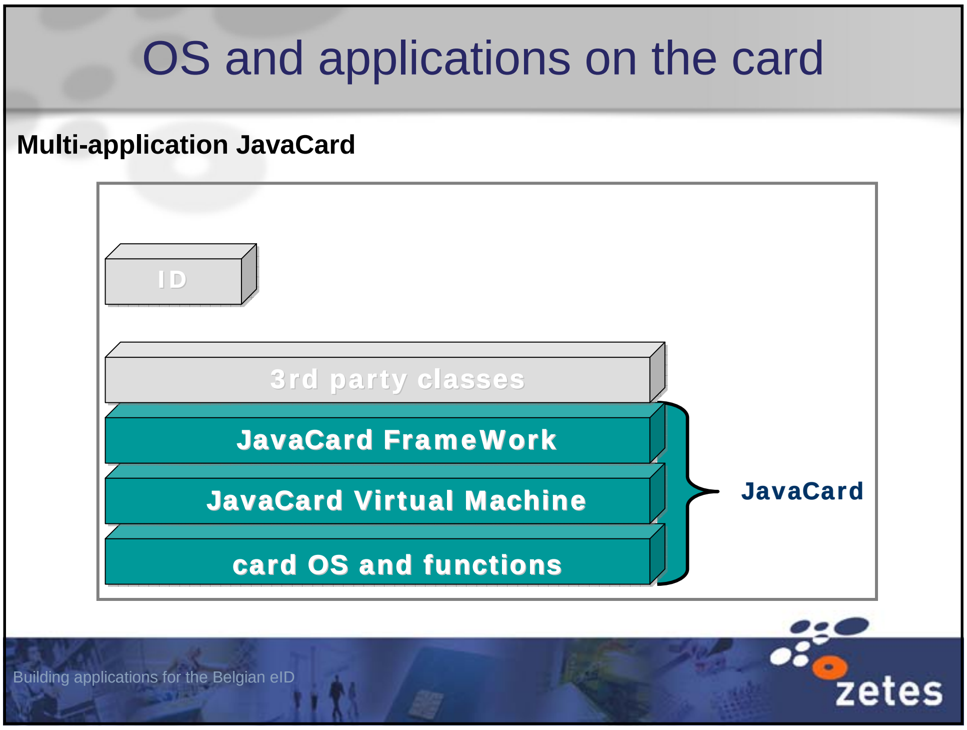
JavaCard Virtual Machine

card OS and functions

JavaCard

Building applications for the Belgian eID

zetes



OS and applications on the card

Multi-application JavaCard

ID

3rd party classes

JavaCard FrameWork

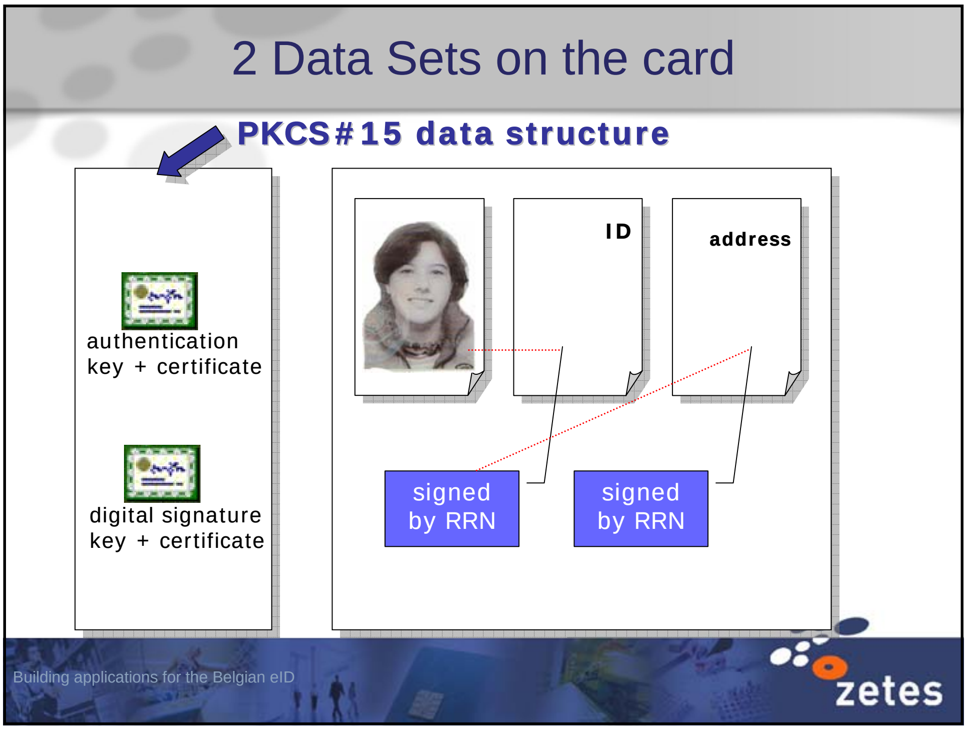
JavaCard Virtual Machine

card OS and functions

JavaCard

Building applications for the Belgian eID

zetes



2 Data Sets on the card

PKCS#15 data structure

authentication key + certificate

digital signature key + certificate

ID

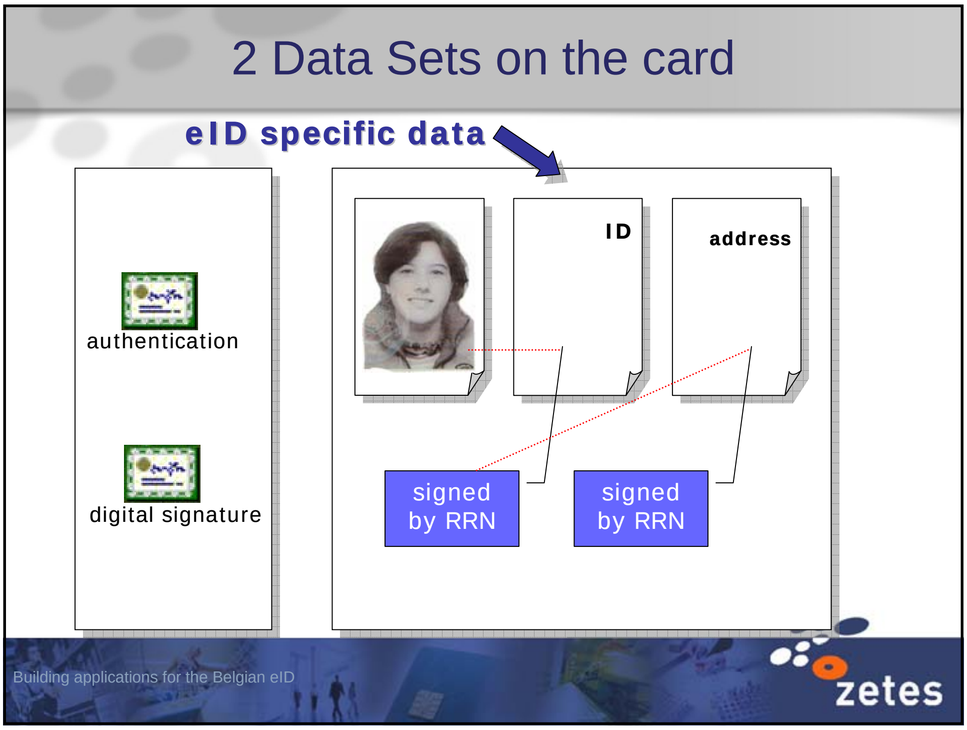
address

signed by RRN

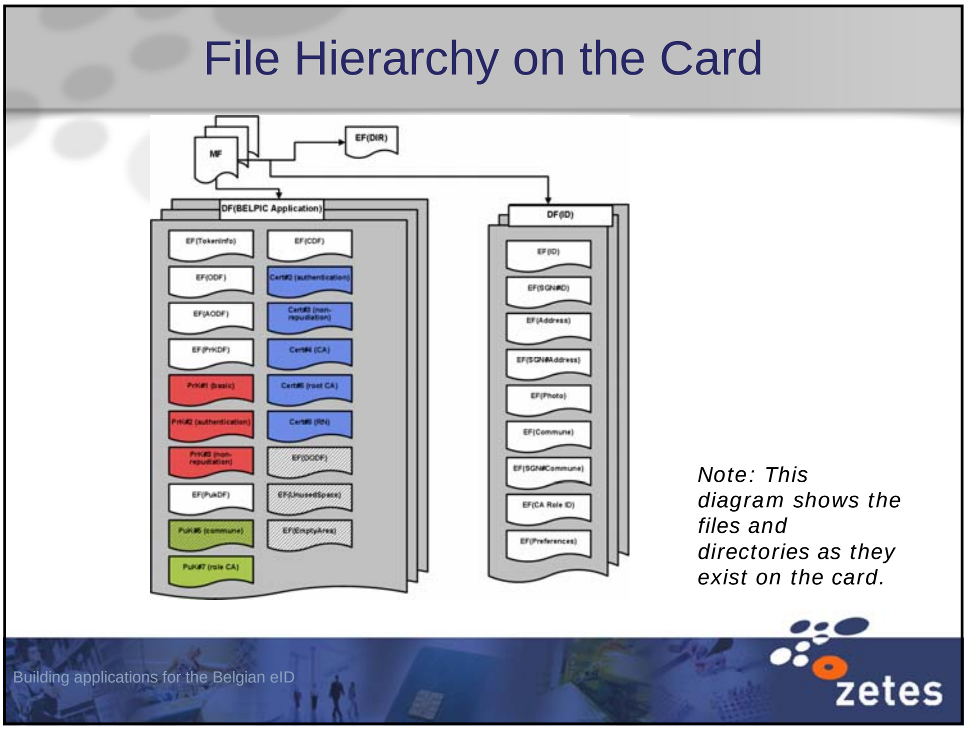
signed by RRN

Building applications for the Belgian eID

zetes

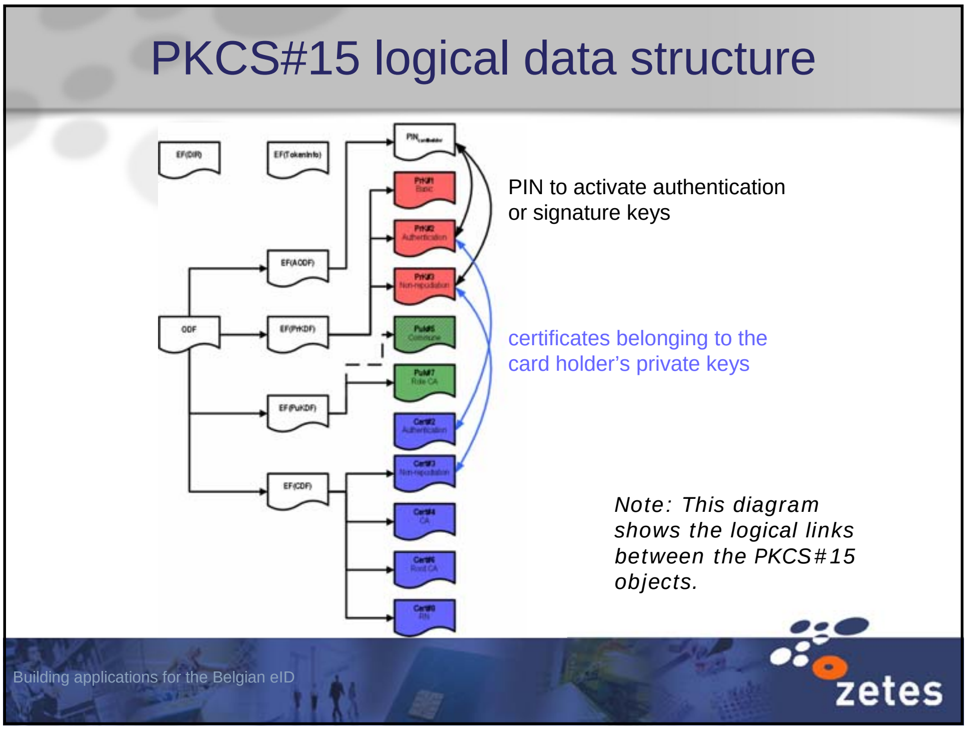


2 Data Sets on the card



File Hierarchy on the Card

Note: This diagram shows the files and directories as they exist on the card.

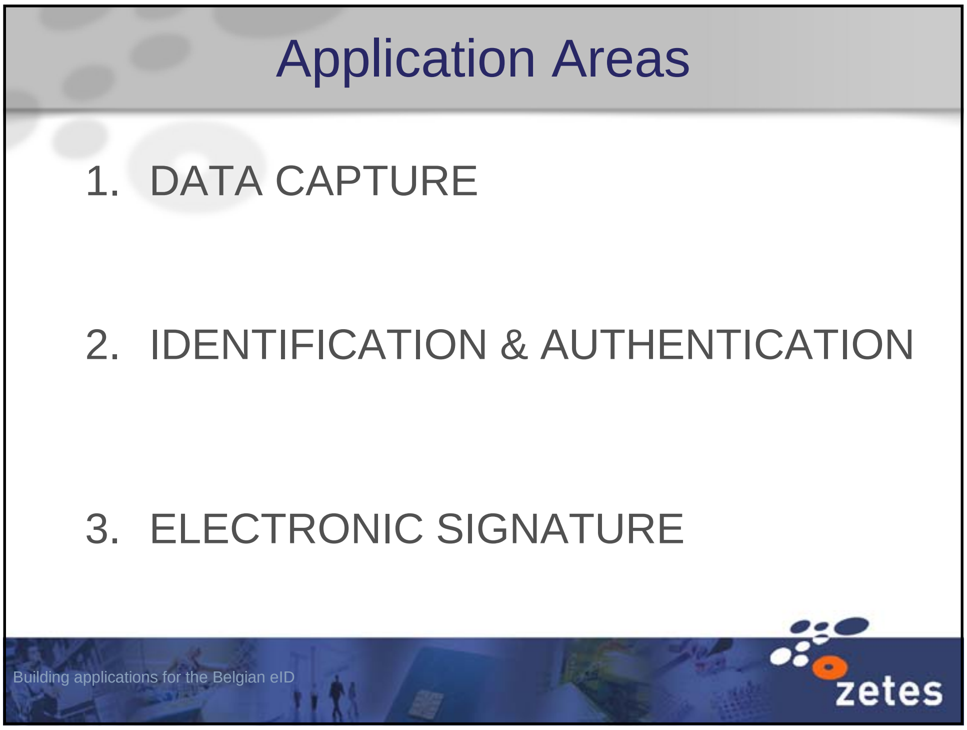


PKCS#15 logical data structure

PIN to activate authentication or signature keys

certificates belonging to the card holder's private keys

Note: This diagram shows the logical links between the PKCS#15 objects.



Application Areas

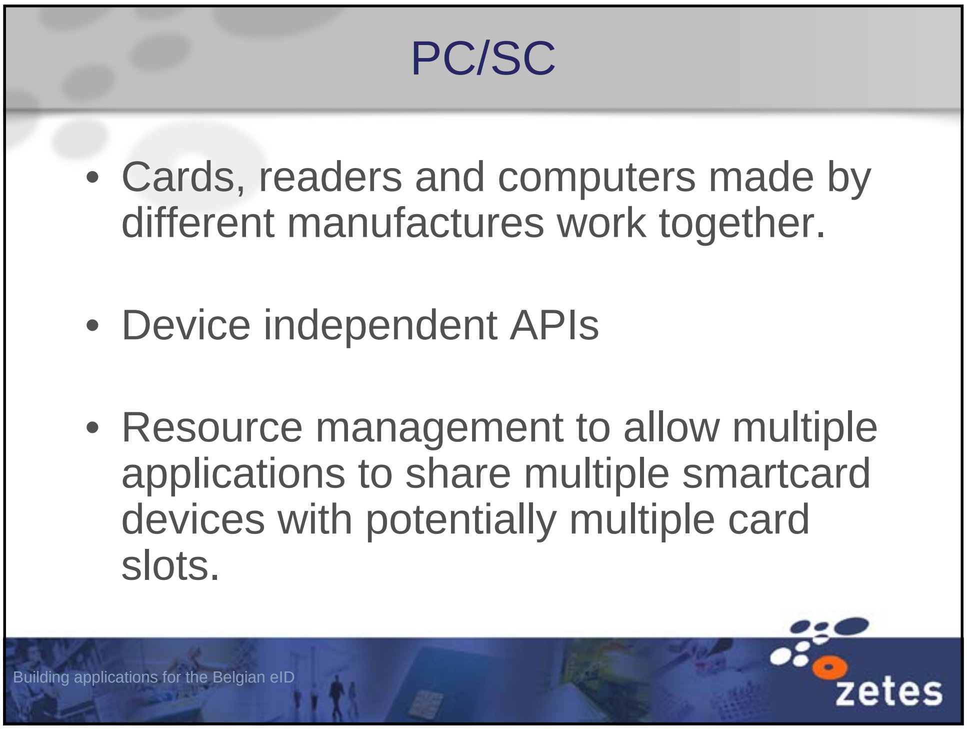
1. DATA CAPTURE

2. IDENTIFICATION & AUTHENTICATION

3. ELECTRONIC SIGNATURE

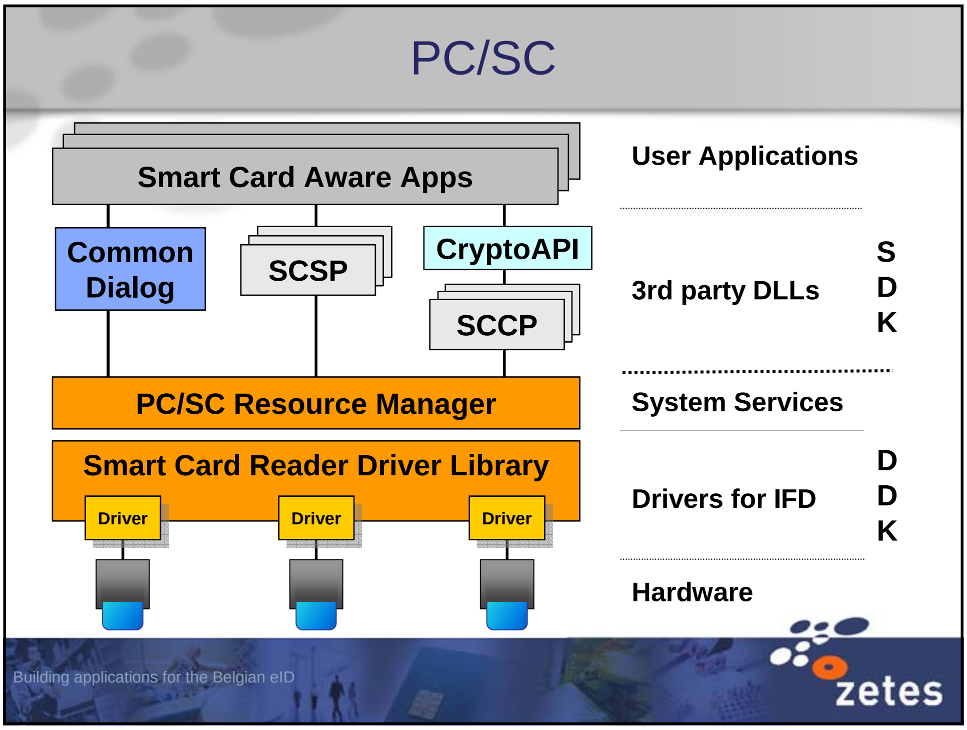
Building Applications for the Belgian eID card

Card Readers and Terminals



PC/SC

- Cards, readers and computers made by different manufactures work together.
- Device independent APIs
- Resource management to allow multiple applications to share multiple smartcard devices with potentially multiple card slots.



PC/SC

Smart Card Aware Apps

Common Dialog

SCSP

CryptoAPI

SCCP

PC/SC Resource Manager

Smart Card Reader Driver Library

Driver

Driver

Driver

User Applications

3rd party DLLs

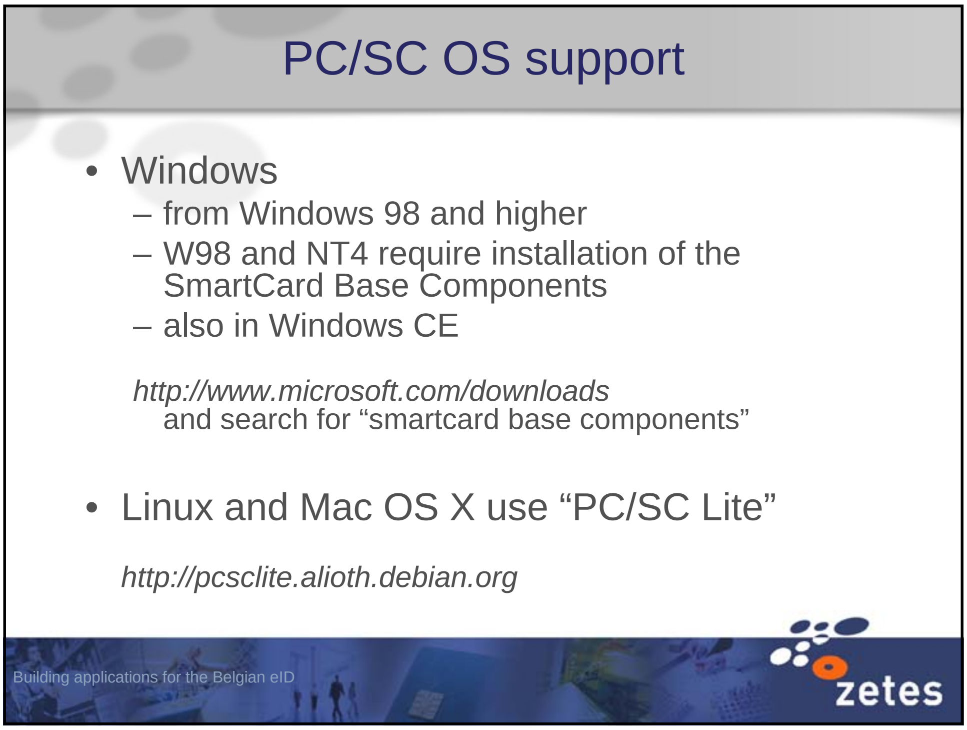
SDK

System Services

Drivers for IFD

DDK

Hardware



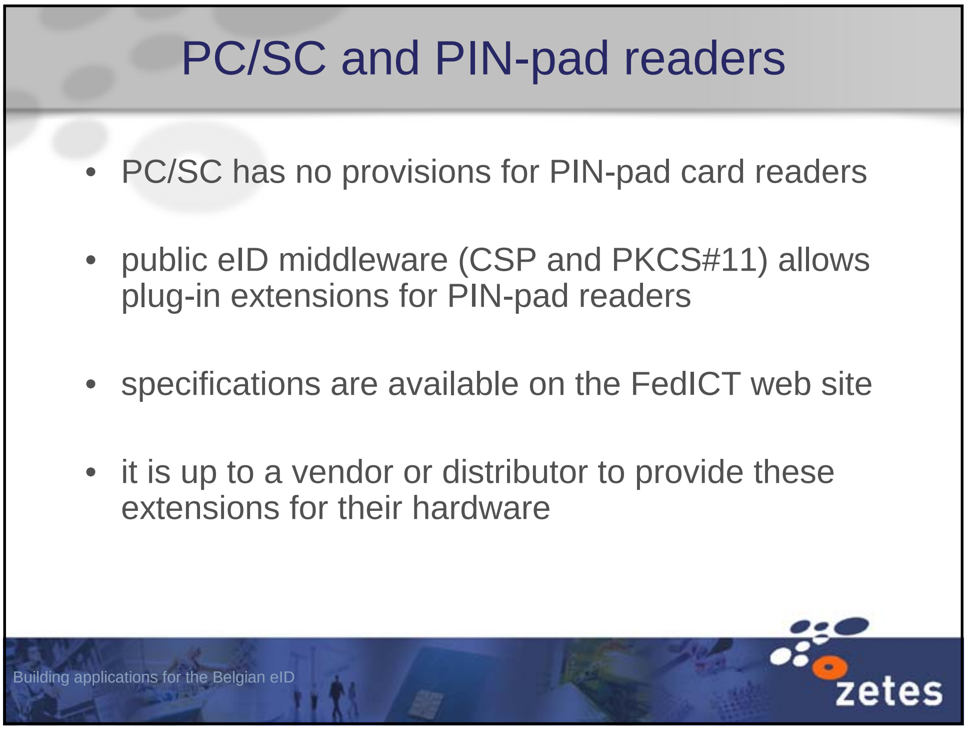
PC/SC OS support

- Windows
  - from Windows 98 and higher
  - W98 and NT4 require installation of the SmartCard Base Components
  - also in Windows CE

  http://www.microsoft.com/downloads
  and search for “smartcard base components”

- Linux and Mac OS X use “PC/SC Lite”

  http://pcsclite.alioth.debian.org

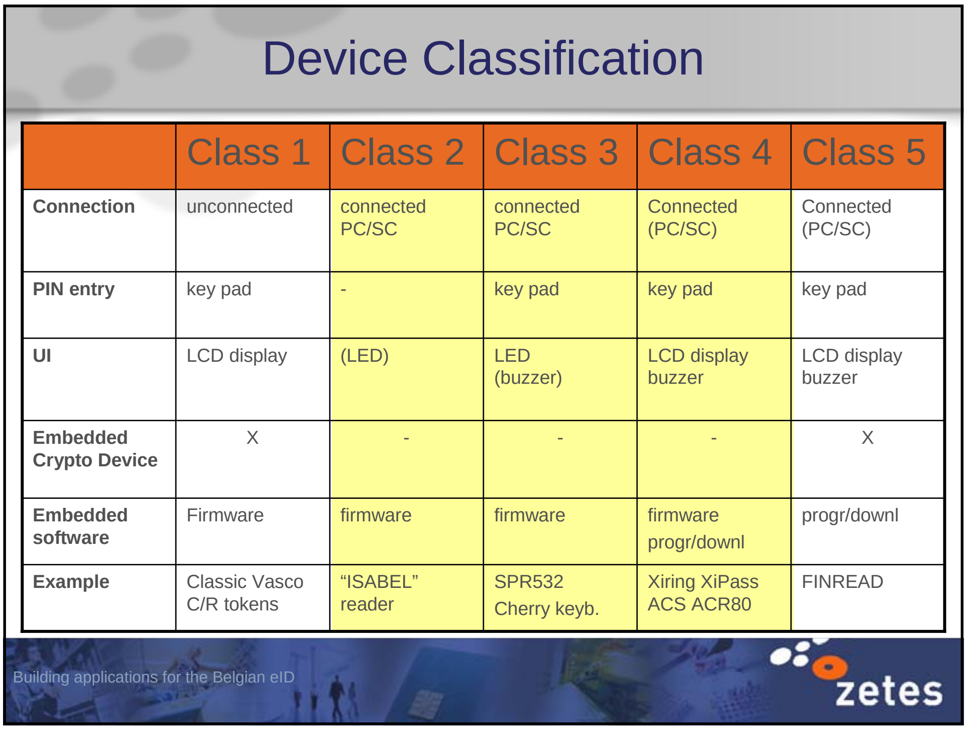


PC/SC and PIN-pad readers

- PC/SC has no provisions for PIN-pad card readers
- public eID middleware (CSP and PKCS#11) allows plug-in extensions for PIN-pad readers
- specifications are available on the FedICT web site
- it is up to a vendor or distributor to provide these extensions for their hardware

Building applications for the Belgian eID

zetes

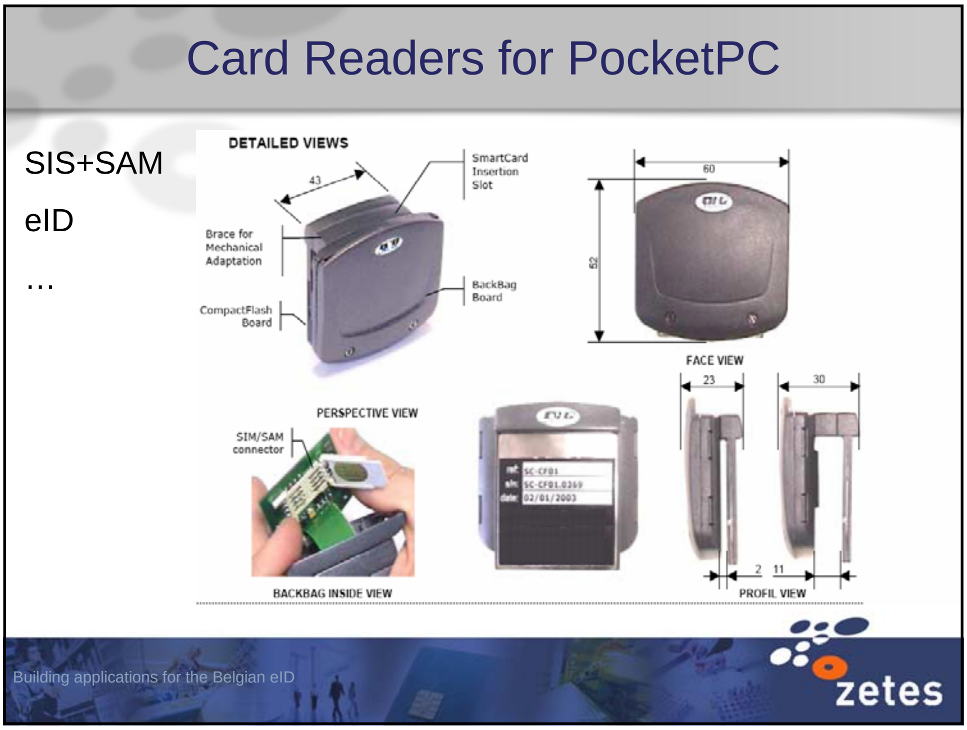


Device Classification

	Class 1	Class 2	Class 3	Class 4	Class 5
Connection	unconnected	connected PC/SC	connected PC/SC	Connected (PC/SC)	Connected (PC/SC)
PIN entry	key pad	-	key pad	key pad	key pad
UI	LCD display	(LED)	LED (buzzer)	LCD display buzzer	LCD display buzzer
Embedded Crypto Device	X	-	-	-	X
Embedded software	Firmware	firmware	firmware	firmware progr/downl	progr/downl
Example	Classic Vasco C/R tokens	"ISABEL" reader	SPR532 Cherry keyb.	Xiring XiPass ACS ACR80	FINREAD

Building applications for the Belgian eID

zetes



Card Readers for PocketPC

SIS+SAM

eID

…

Building applications for the Belgian eID

zetes

Mobile/Standalone Card Reader

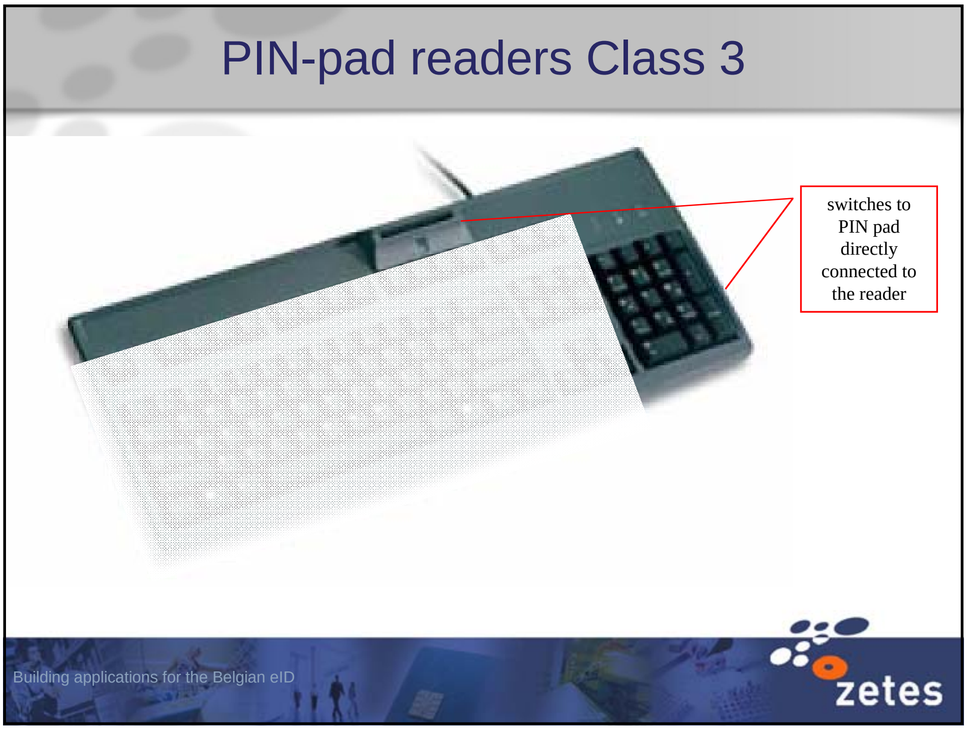
- Compact 12,5 x 7,5 x 1,5 cm
- Light 123 gram
- Non-Volatile Memory read/store/synchronize
- Connects to any PC
- 2 AAA batteries
- programmable in C
- SIS approved

Building applications for the Belgian eID

zetes

Low-cost SIS+SAM /eID reader

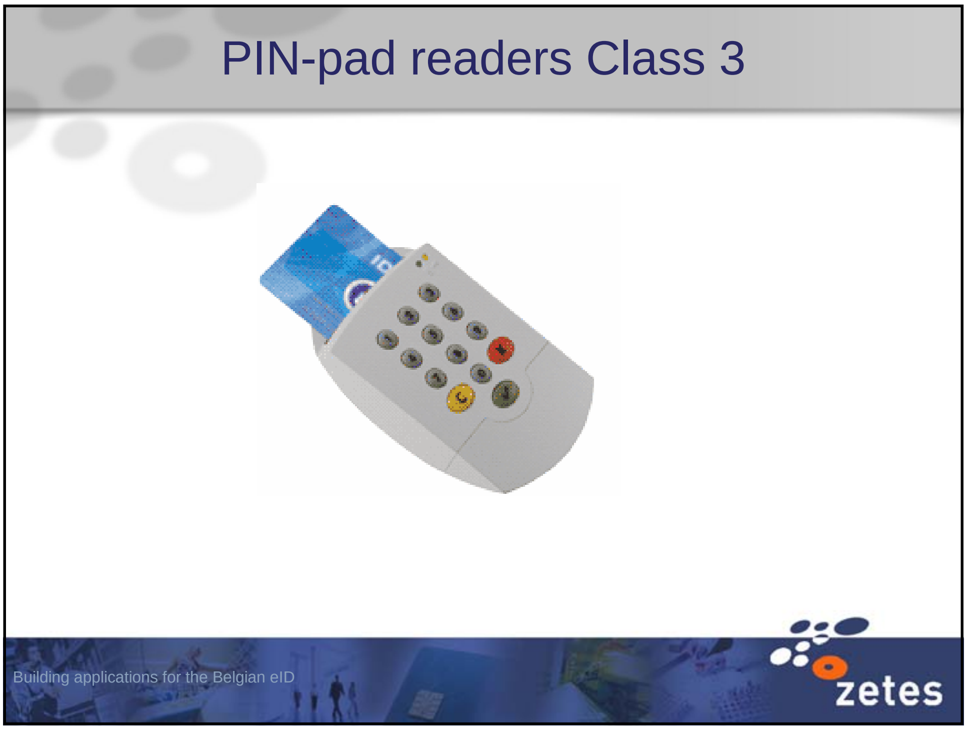
Simple card readers (class 2)



PIN-pad readers Class 3

switches to PIN pad directly connected to the reader

Building applications for the Belgian eID



PIN-pad readers Class 3

Building applications for the Belgian eID

PIN-pad readers Class 4

Ruggedized Mobile Terminal

- water/weather proof
- GSM/GPRS/WiFi
- Bluetooth
- barcode & MRZ scanner
- fingerprint sensor
- contact/contactless card reader
- PocketPC/Windows CE

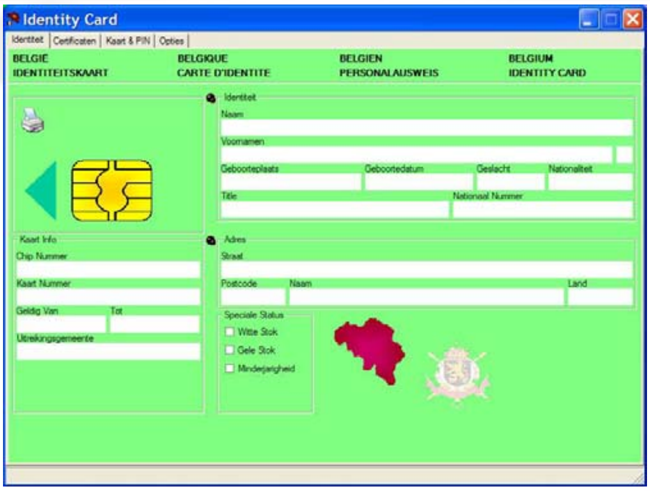
The Belgian eID card

Building Applications
Software Development Kit

FedICT eID software

- Microsoft Windows
  - CryptoAPI CSP for Internet Explorer, Outlook, .NET, …
- OS neutral standards
  - PKCS#11 for Linux, MacOSX, Windows and Sun Solaris
- Java OpenCard Framework

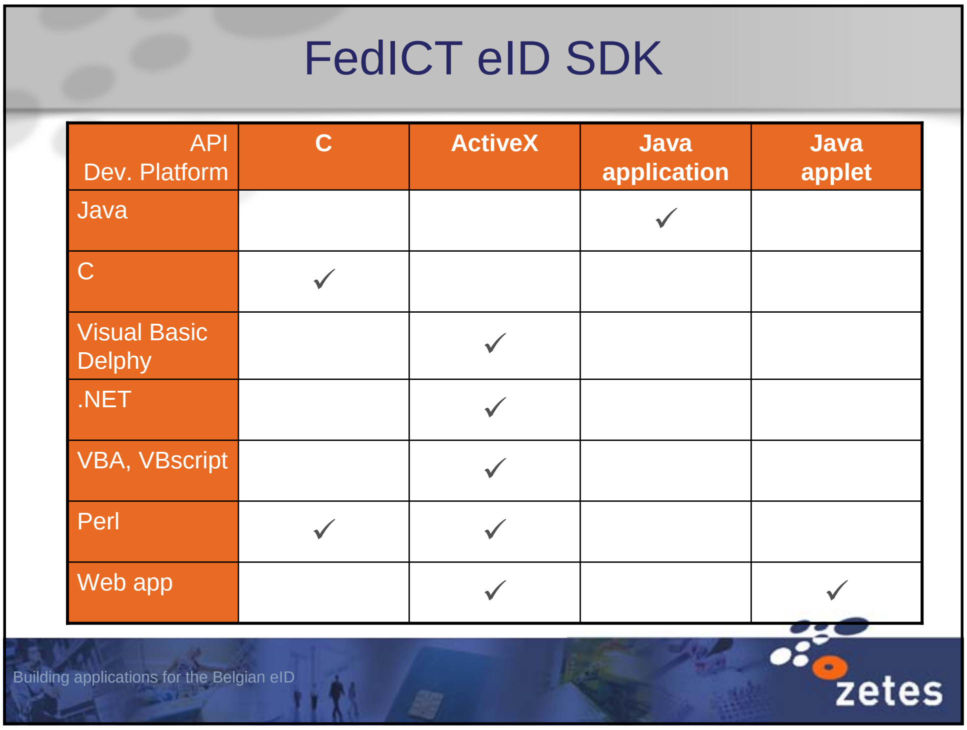
FedICT eID software



FedICT eID SDK

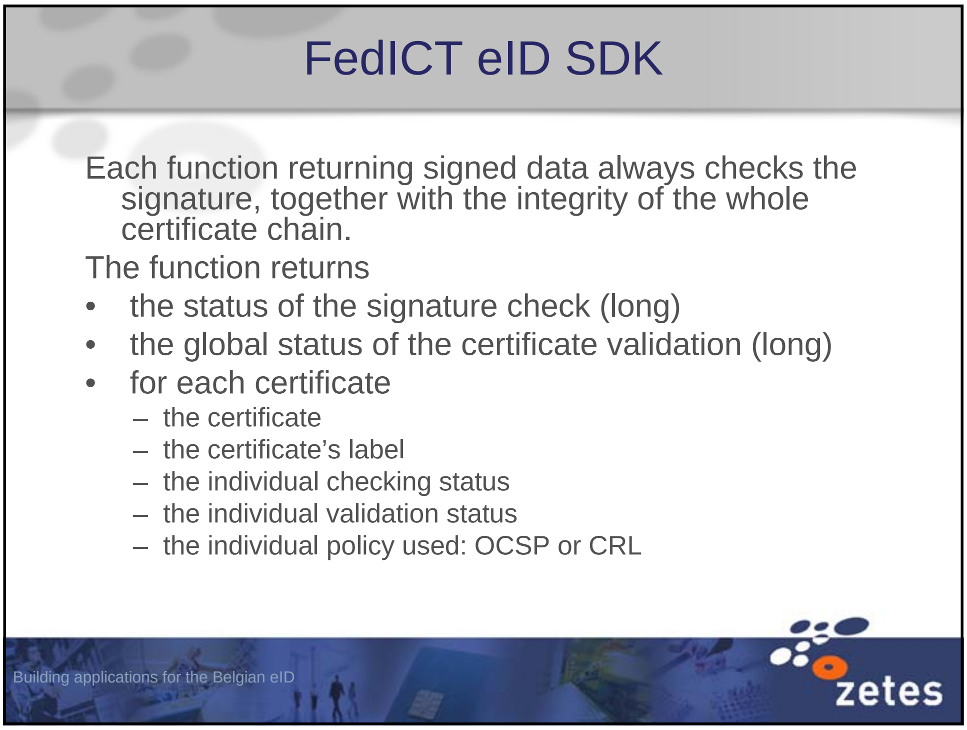
The main goals of the FedICT eID SDK are:

- To provide an easy way to retrieve the identity information from any version of a Belgian Identity Card
- To automate and hide all validation mechanisms
- To provide an easy to use interface to reduce the integration time in applications
- self-sufficient; as an example, all identity functions will automatically
  - select the right application before reading the identity file
  - ensure they are not interrupted in the middle of a file read
  - interpret the contents of a file based on the card version



FedICT eID SDK

API Dev. Platform	C	ActiveX	Java application	Java applet
Java			✓	
C	✓			
Visual Basic Delphy		✓		
.NET		✓		
VBA, VBscript		✓		
Perl	✓	✓		
Web app		✓		✓

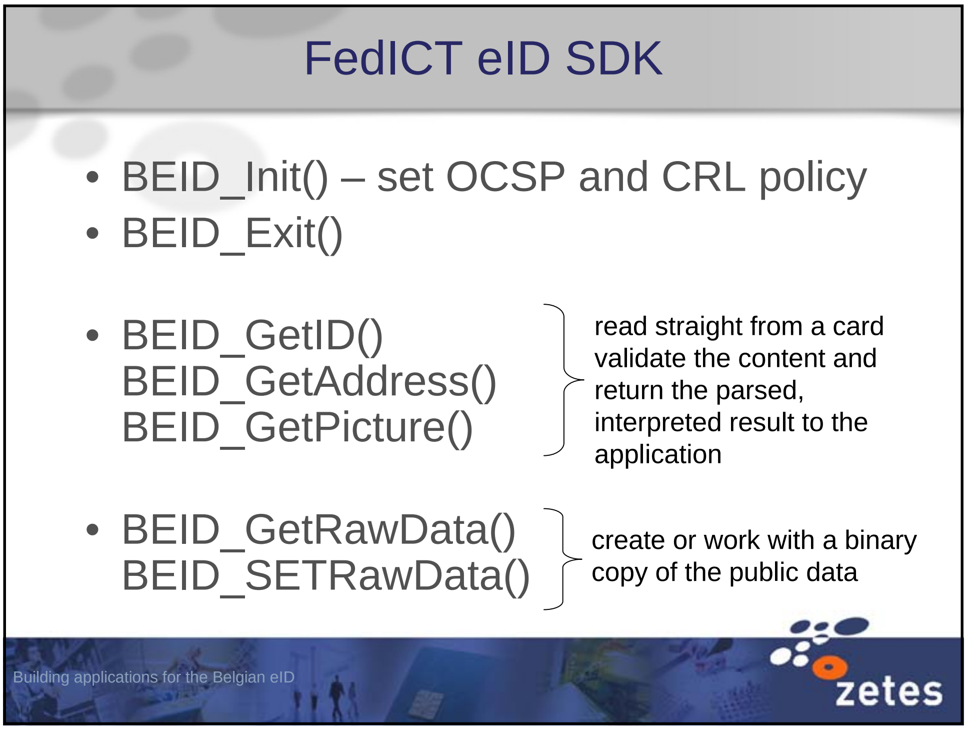


FedICT eID SDK

Each function returning signed data always checks the signature, together with the integrity of the whole certificate chain.

The function returns

- the status of the signature check (long)
- the global status of the certificate validation (long)
- for each certificate
  - the certificate
  - the certificate’s label
  - the individual checking status
  - the individual validation status
  - the individual policy used: OCSP or CRL



FedICT eID SDK

- BEID_Init() – set OCSP and CRL policy
- BEID_Exit()
- BEID_GetID()
  BEID_GetAddress()
  BEID_GetPicture()

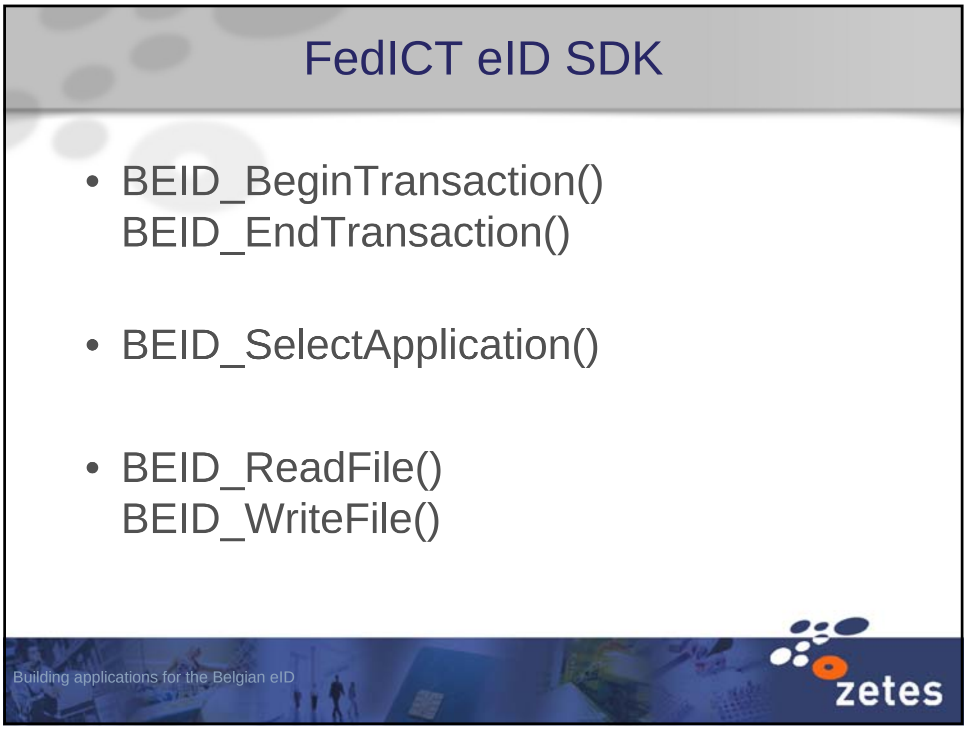
read straight from a card validate the content and return the parsed, interpreted result to the application

- BEID_GetRawData()
  BEID_SETRawData()

create or work with a binary copy of the public data

Building applications for the Belgian eID

zetes

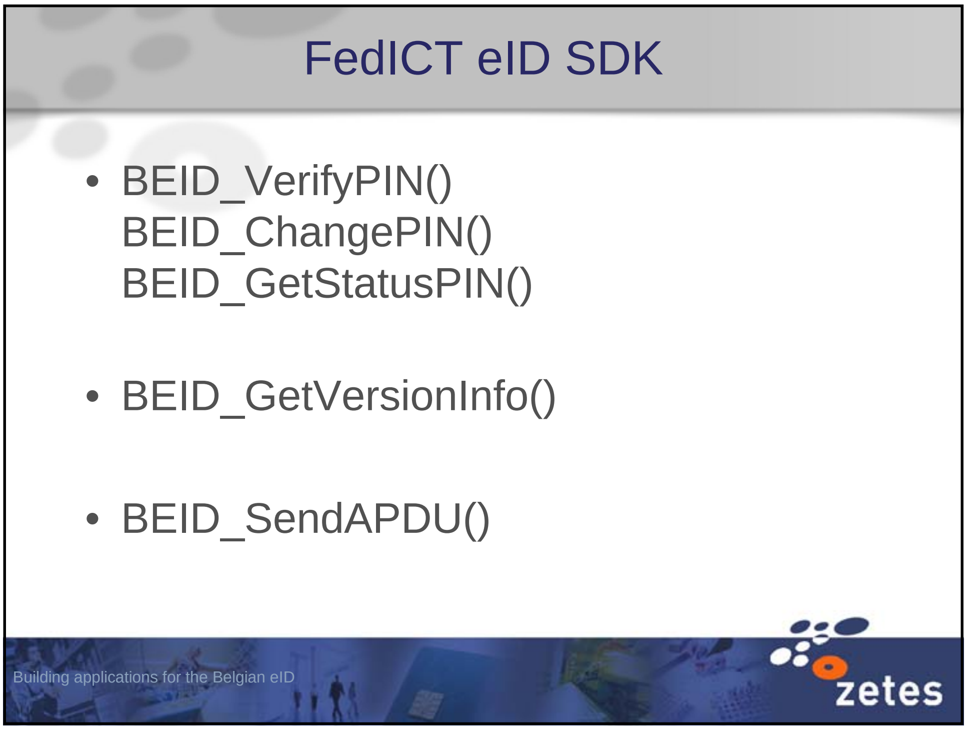


FedICT eID SDK

- BEID_BeginTransaction()
  BEID_EndTransaction()
- BEID_SelectApplication()
- BEID_ReadFile()
  BEID_WriteFile()

Building applications for the Belgian eID

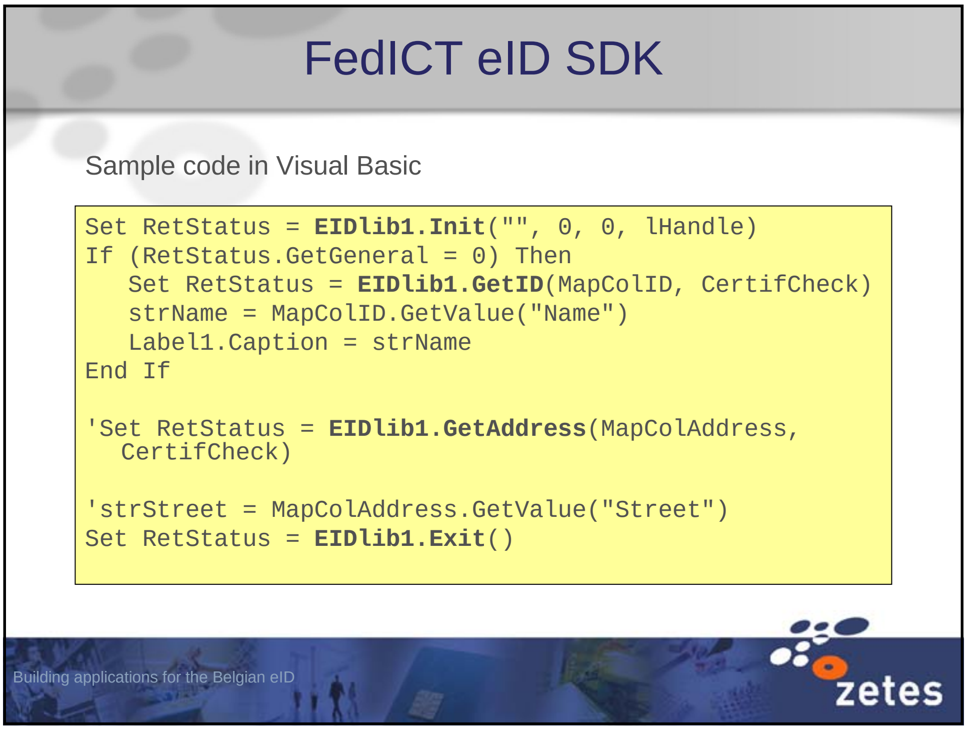
zetes



FedICT eID SDK

- BEID_VerifyPIN()
  BEID_ChangePIN()
  BEID_GetStatusPIN()
- BEID_GetVersionInfo()
- BEID_SendAPDU()

Building applications for the Belgian eID



FedICT eID SDK

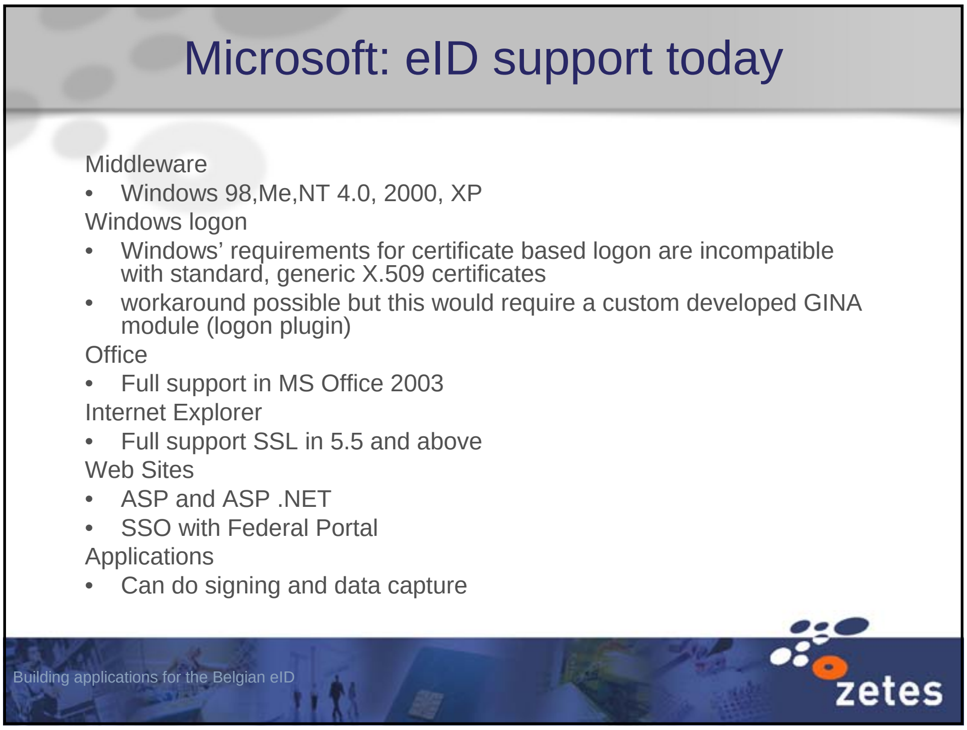
Sample code in Visual Basic

```
Set RetStatus = EIDlib1.Init("", 0, 0, lHandle)
If (RetStatus.GetGeneral = 0) Then
   Set RetStatus = EIDlib1.GetID(MapColID, CertifCheck)
   strName = MapColID.GetValue("Name")
   Label1.Caption = strName
End If

'Set RetStatus = EIDlib1.GetAddress(MapColAddress,
   CertifCheck)

'strStreet = MapColAddress.GetValue("Street")
Set RetStatus = EIDlib1.Exit()
```

Building applications for the Belgian eID



Microsoft: eID support today

Middleware

- Windows 98,Me,NT 4.0, 2000, XP

Windows logon

- Windows' requirements for certificate based logon are incompatible with standard, generic X.509 certificates
- workaround possible but this would require a custom developed GINA module (logon plugin)

Office

- Full support in MS Office 2003

Internet Explorer

- Full support SSL in 5.5 and above

Web Sites

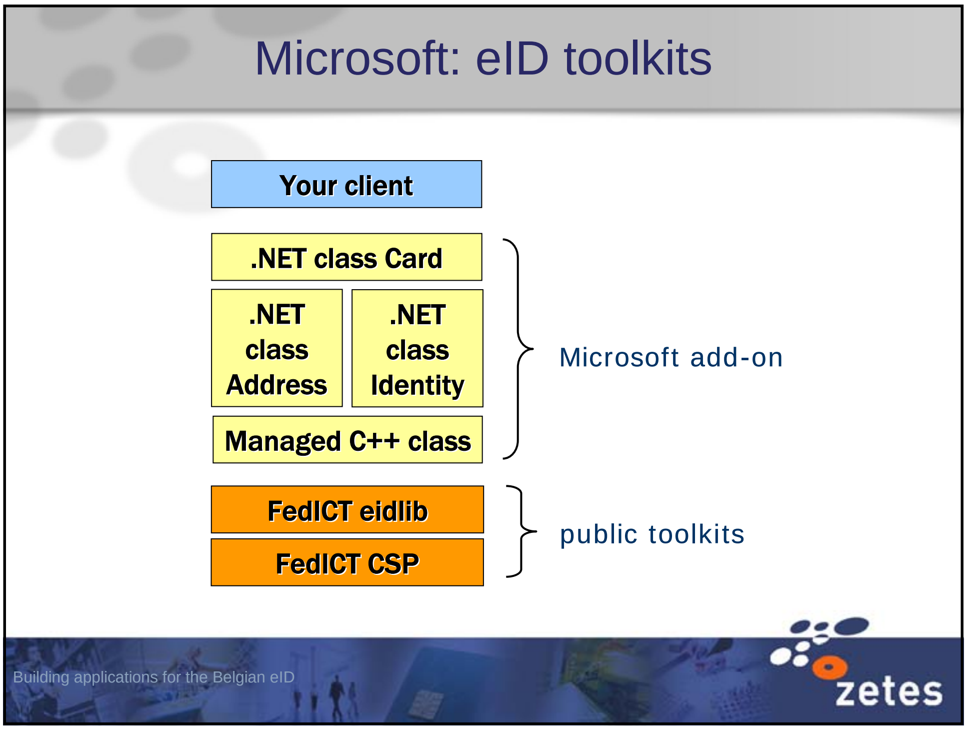
- ASP and ASP .NET
- SSO with Federal Portal

Applications

- Can do signing and data capture

Building applications for the Belgian eID

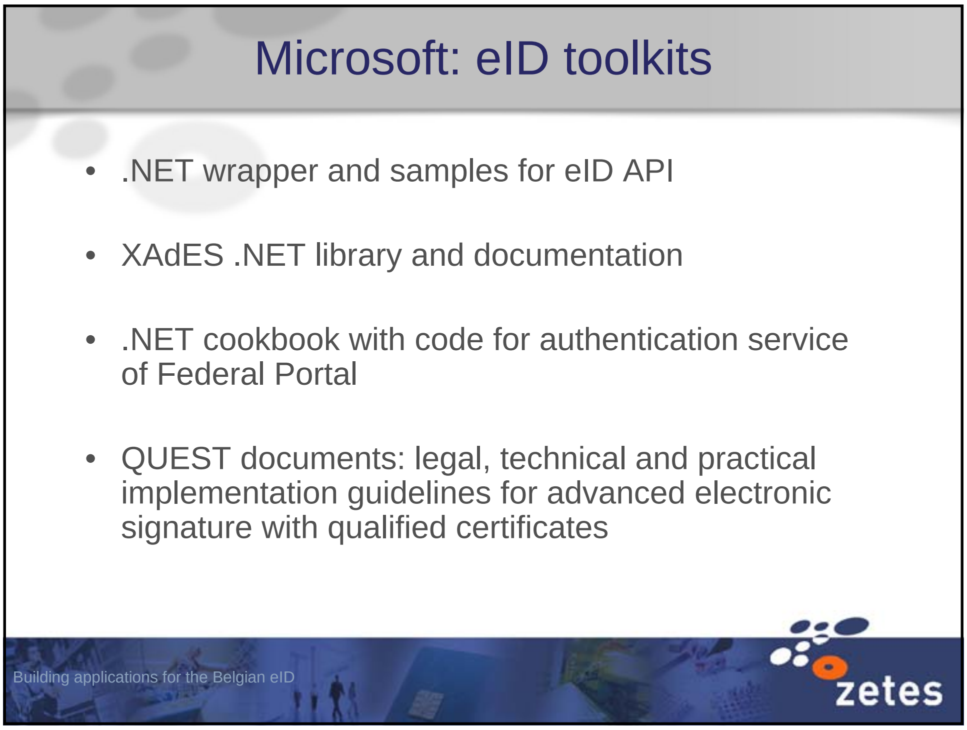
zetes



Microsoft: eID toolkits

Building applications for the Belgian eID

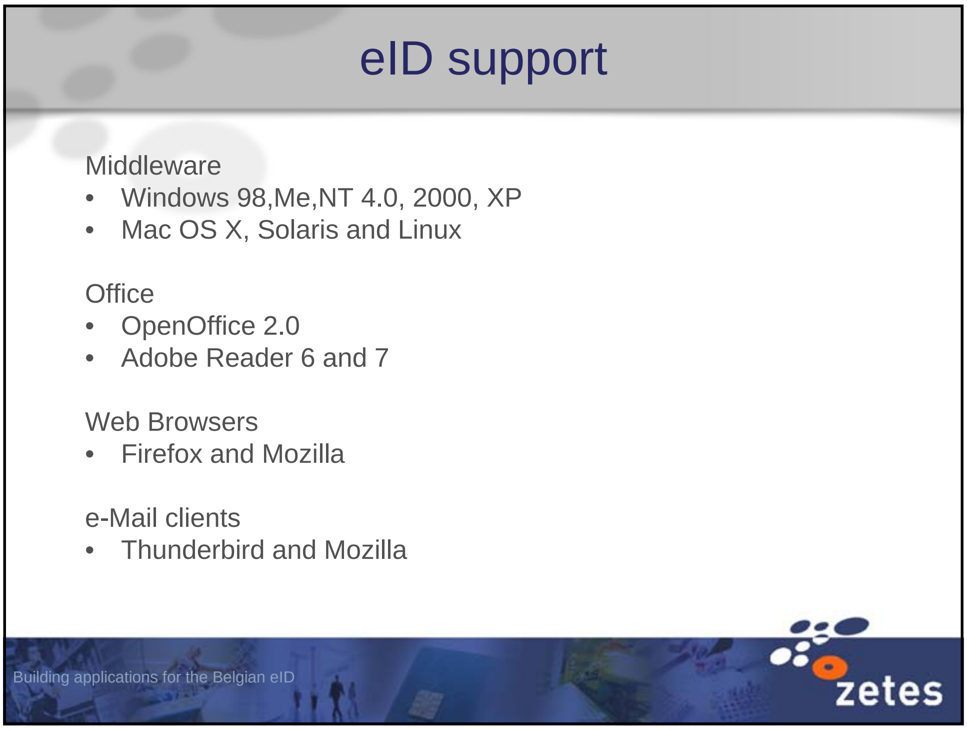
zetes



Microsoft: eID toolkits

- .NET wrapper and samples for eID API
- XAdES .NET library and documentation
- .NET cookbook with code for authentication service of Federal Portal
- QUEST documents: legal, technical and practical implementation guidelines for advanced electronic signature with qualified certificates

Building applications for the Belgian eID



eID support

Middleware
- Windows 98,Me,NT 4.0, 2000, XP
- Mac OS X, Solaris and Linux

Office
- OpenOffice 2.0
- Adobe Reader 6 and 7

Web Browsers
- Firefox and Mozilla

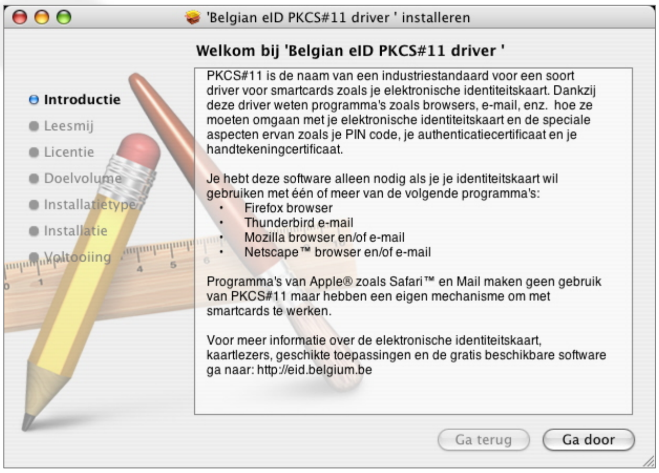
e-Mail clients
- Thunderbird and Mozilla

Building applications for the Belgian eID

eID on the Mac

- smart card support only available on Mac OS X
- no smart card support on MacOS 9
- federal government supplies PKCS#11 for Mac OS X 10.2.8 and higher
- Mac OS X 10.4 is the first OS with built in recognition of the Belgian eID

eID on the Mac



Welkom bij 'Belgian eID PKCS#11 driver '

PKCS#11 is de naam van een industriestandaard voor een soort driver voor smartcards zoals je elektronische identiteitskaart. Dankzij deze driver weten programma's zoals browsers, e-mail, enz. hoe ze moeten omgaan met je elektronische identiteitskaart en de speciale aspecten ervan zoals je PIN code, je authenticatiecertificaat en je handtekeningcertificaat.

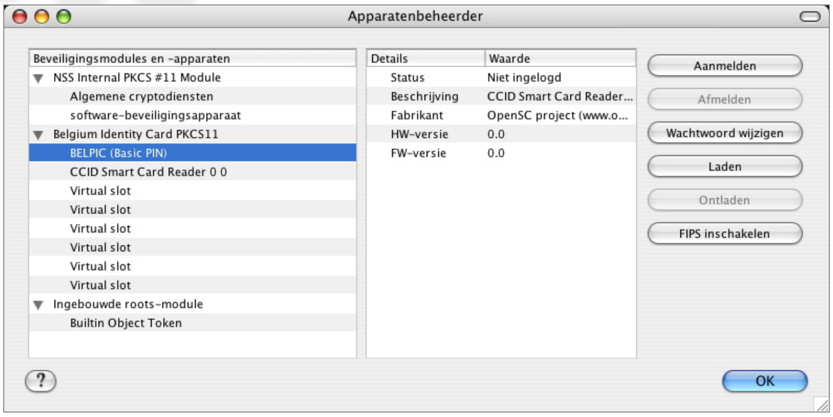
Je hebt deze software alleen nodig als je je identiteitskaart wil gebruiken met één of meer van de volgende programma's:

- Firefox browser
- Thunderbird e-mail
- Mozilla browser en/of e-mail
- Netscape™ browser en/of e-mail

Programma's van Apple® zoals Safari™ en Mail maken geen gebruik van PKCS#11 maar hebben een eigen mechanisme om met smartcards te werken.

Voor meer informatie over de elektronische identiteitskaart, kaartlezers, geschikte toepassingen en de gratis beschikbare software ga naar: http://eid.belgium.be

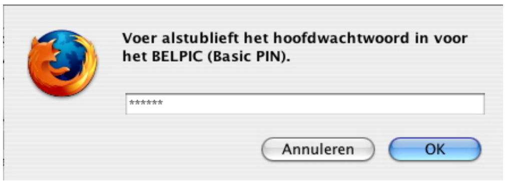
eID on the Mac



Beveiligingsmodules en -apparaten
- NSS Internal PKCS #11 Module
  - Algemene cryptodiensten
  - software-beveiligingsapparaat
- Belgium Identity Card PKCS11
  - BELPIC (Basic PIN)
  - CCID Smart Card Reader 0 0
  - Virtual slot
  - Virtual slot
  - Virtual slot
  - Virtual slot
  - Virtual slot
  - Virtual slot
- Ingebouwde roots-module
  - Builtin Object Token

Details	Waarde
Status	Niet ingelogd
Beschrijving	CCID Smart Card Reader...
Fabrikant	OpenSC project (www.o...
HW-versie	0.0
FW-versie	0.0

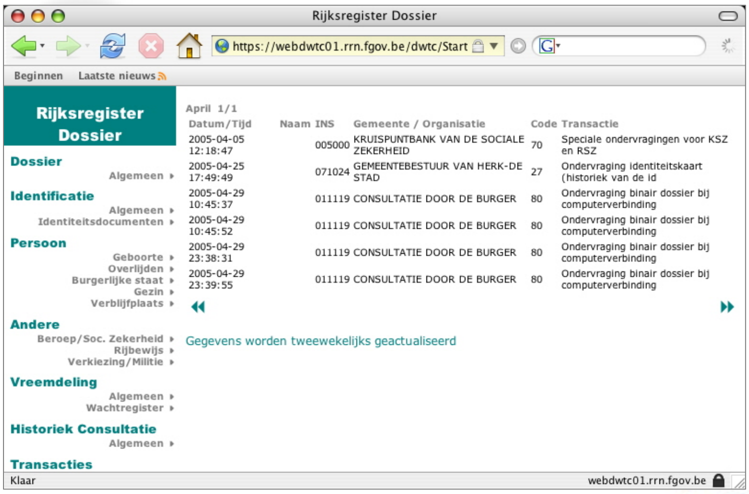
eID on the Mac



Voer alstublieft het hoofdwachtwoord in voor het BELPIC (Basic PIN).

******

eID on the Mac



Rijksregister Dossier

https://webdwtc01.rrn.fgov.be/dwtc/Start

Rijksregister Dossier

Dossier
Algemeen ▸

Identificatie
Algemeen ▸
Identiteitsdocumenten ▸

Persoon
Geboorte ▸
Overlijden ▸
Burgerlijke staat ▸
Gezin ▸
Verblijfplaats ▸

Andere
Beroep/Soc. Zekerheid ▸
Rijbewijs ▸
Verkiezing/Militie ▸

Vreemdeling
Algemeen ▸
Wachtregister ▸

Historiek Consultatie
Algemeen ▸

Transacties

April 1/1

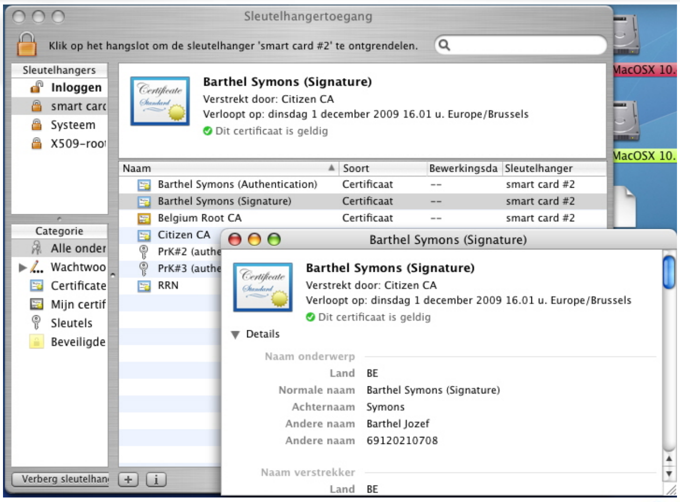
Datum/Tijd	Naam INS	Gemeente / Organisatie	Code	Transactie
2005-04-05 12:18:47	005000	KRUISPUNTBANK VAN DE SOCIALE ZEKERHEID	70	Speciale ondervragingen voor KSZ en RSZ
2005-04-25 17:49:49	071024	GEMEENTEBESTUUR VAN HERK-DE STAD	27	Ondervraging identiteitskaart (historiek van de id
2005-04-29 10:45:37	011119	CONSULTATIE DOOR DE BURGER	80	Ondervraging binair dossier bij computerverbinding
2005-04-29 10:45:52	011119	CONSULTATIE DOOR DE BURGER	80	Ondervraging binair dossier bij computerverbinding
2005-04-29 23:38:31	011119	CONSULTATIE DOOR DE BURGER	80	Ondervraging binair dossier bij computerverbinding
2005-04-29 23:39:55	011119	CONSULTATIE DOOR DE BURGER	80	Ondervraging binair dossier bij computerverbinding

Gegevens worden tweewekelijks geactualiseerd

Klaar

webdwtc01.rrn.fgov.be

eID on the Mac



Sleutelhangertoegang

Klik op het hangslot om de sleutelhanger 'smart card #2' te ontgrendelen.

Barthel Symons (Signature)
Verstrekt door: Citizen CA
Verloopt op: dinsdag 1 december 2009 16.01 u. Europe/Brussels
Dit certificaat is geldig

Naam	Soort	Bewerkingsda	Sleutelhanger
Barthel Symons (Authentication)	Certificaat	--	smart card #2
Barthel Symons (Signature)	Certificaat	--	smart card #2
Belgium Root CA	Certificaat	--	smart card #2
Citizen CA			
PrK#2 (authe			
PrK#3 (authe			
RRN			

Barthel Symons (Signature)

Barthel Symons (Signature)
Verstrekt door: Citizen CA
Verloopt op: dinsdag 1 december 2009 16.01 u. Europe/Brussels
Dit certificaat is geldig

▼ Details

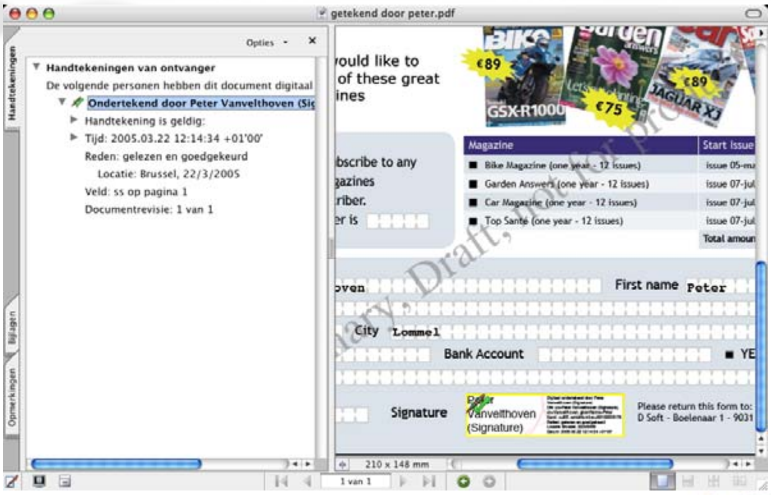
Naam onderwerp

Land	BE
Normale naam	Barthel Symons (Signature)
Achternaam	Symons
Andere naam	Barthel Jozef
Andere naam	69120210708

Naam verstrekker

Land	BE

eID on the Mac



getekend door peter.pdf

Opties ▾ ✕

- ▼ Handtekeningen van ontvanger
  - De volgende personen hebben dit document digitaal
    - ▼ Ondertekend door Peter Vanvelthoven (Sig
      - ▶ Handtekening is geldig:
      - ▶ Tijd: 2005.03.22 12:14:34 +01'00'
      - Reden: gelezen en goedgekeurd
      - Locatie: Brussel, 22/3/2005
      - Veld: ss op pagina 1
      - Documentrevisie: 1 van 1

ould like to
of these great
ines

bscribe to any
azines
riber.
er is

Magazine	Start Issue
■ Bike Magazine (one year - 12 issues)	issue 05-ma
■ Garden Answers (one year - 12 issues)	issue 07-jul
■ Car Magazine (one year - 12 issues)	issue 07-jul
■ Top Santé (one year - 12 issues)	issue 07-jul
	Total amoun

oven First name Peter

City Lommel

Bank Account ■ YE

Signature Peter Vanvelthoven (Signature)

Please return this form to:
D Soft - Boelenaar 1 - 9031

zetes