



# Challenges for Securing Mobile eID

Slides available at <http://godot.be/slides>

**Danny De Cock**

Danny.DeCock@esat.kuleuven.be

Katholieke Universiteit Leuven/Dept. Elektrotechniek (ESAT)

Computer Security and Industrial Cryptography (COSIC)

Kasteelpark Arenberg 10

B-3001 Heverlee

Belgium

# For Your Information ☺

- The copyright holder of this information is Danny De Cock (email: [godot@godot.be](mailto:godot@godot.be)), further referenced as the author
- The information expressed in this document reflects the author's personal opinions and do not represent his employer's view in any way
- All information is provided as is, without any warranty of any kind
- Use or re-use of any part of this information is only authorized for personal or not-for-profit use, and requires prior permission by the author

# Outline

- Belgian eID cards
- From Smart Cards to Smart Devices
- Proof-of-concept with Smart Phone
- Challenges & Concerns



# eID Card = 4 Functions

- Non-electronic
  1. Visible Identification of a person
- Electronic
  2. Digital identification
    - Data capture
  3. Prove your identity
    - Authentication signature
  4. Digitally sign information
    - Non-repudiation signature

**Enabler of  
eServices**

eFunctionality

# 1. Visual Aspects of a Belgian eID card

## Front:

- Name
- First two names
- First letter of 3rd name
- Title
- Nationality
- Birth place and date
- Gender
- Card number
- Photo of the holder
- Begin and end validity dates of the card
- Hand written signature of the holder



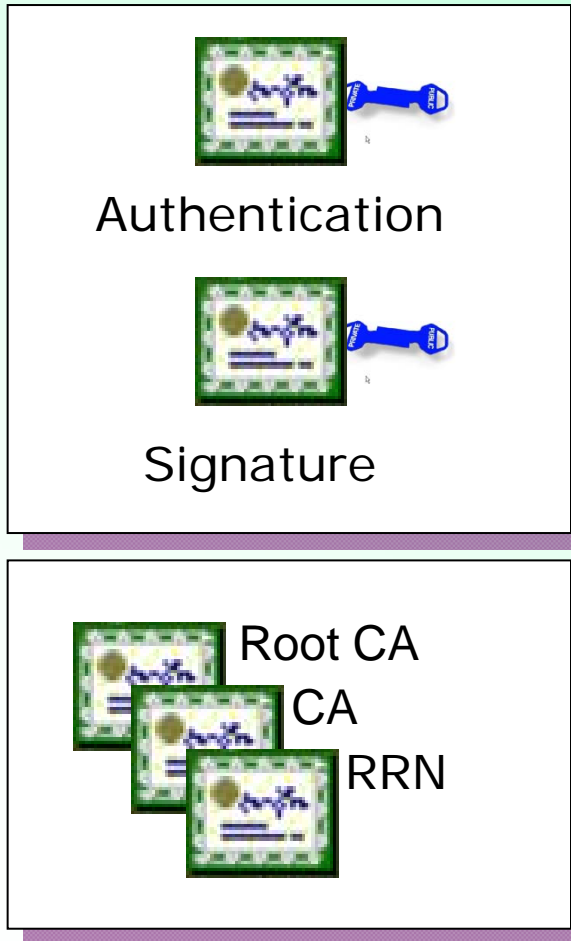
## Back side:

- Place of delivery of the card
- National Register identification number
- Hand written signature of the civil servant
- Main residence of the holder (cards produced before 1/1/2004)
- International Civil Aviation Organization (ICAO)-specified zone (cards produced since 1/1/2005)

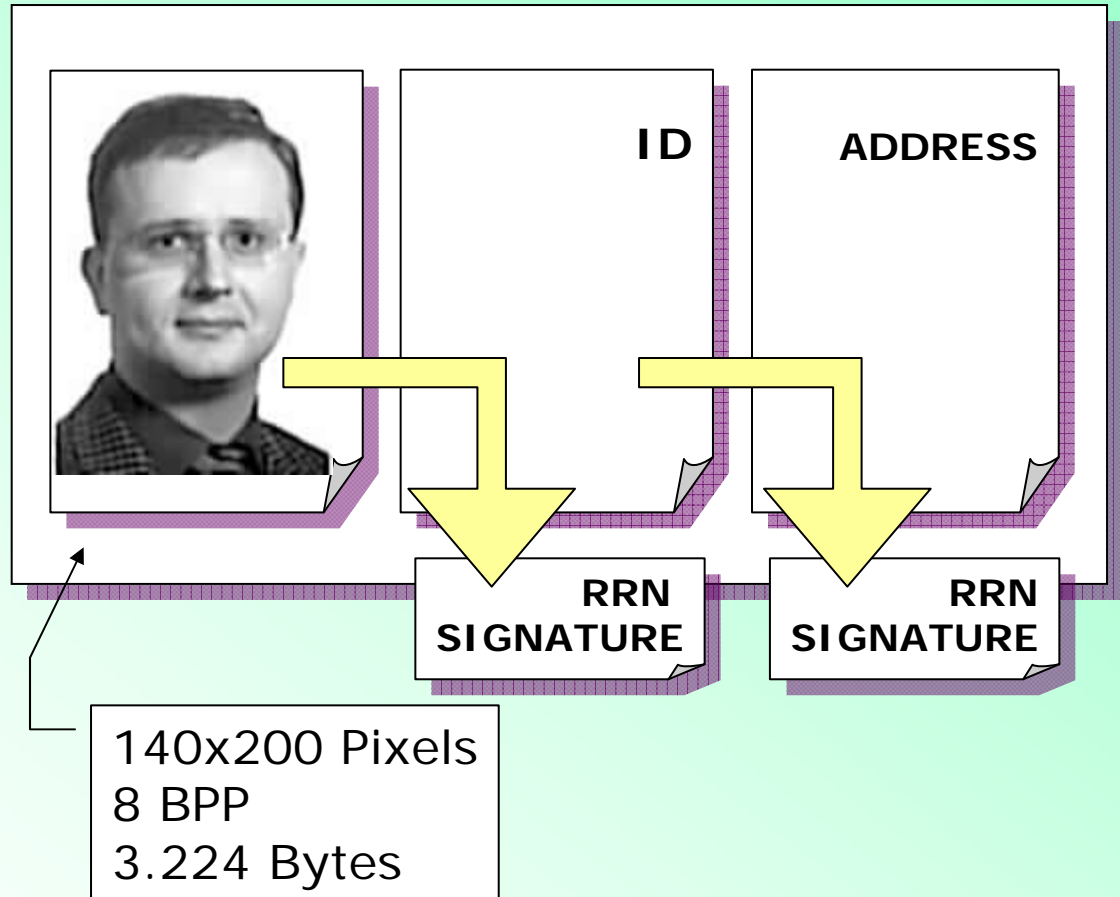


# 2. eID Card Content

## PKI



## Citizen Identity Data



RRN = National Register

# 3. & 4. Signing Keys & Certificates

- Citizen-authentication
  - X.509v3 authentication certificate
- Advanced electronic signatures
  - X.509v3 qualified certificate
  - Can be used to produce digital signatures equivalent to handwritten signatures, cf. European Directive 1999/93/EC
- eID card authentication
  - No corresponding certificate
  - Used for eID card administration



# Problems with Current Smartcards

- Typical application:
  - Smartcard uses its secret or private key
    - E.g., creation of digital signatures, decrypting information...
- ***Trust & What-You-See-Is-What-You-Sign:***
  - Can the user trust her smartcard?
  - Can the user trust her smartcard does what she intends?
  - Is the reader trustworthy?
  - Is the software using the smartcard trustworthy?
  - Can the user verify what the card has done?
    - Phishing, Trojan horses

# Solving these Problems Requires...

- More on-card computing power
  - Multi-threaded
- More on-card storage capacity
  - Interoperable means many trustees & configurations
- On-card user interface
  - Display, PIN pad, OK/Cancel-buttons
- Online connectivity
  - Verifying other party, reader, user
- Sound certification
  - Fundamental to enhance overall trust perception

# Proof-of-concept with Smartphone

- Smartcard → Smartcard Device
  - Device = smartcard + reader + user interface
  - ☺ Solves all issues, but...
  - ☹ Not cheap...
- Open source implementation of JavaCard applet
  - Functionally equivalent with Belgian eID card
  - <http://code.google.com/p/eid-quick-key-toolset/>
- Applied to Android phone
  - Using secure microSD card
  - Exact Copy of eID card files
  - Same signing functions
  - eID card keys cannot be copied



# Challenges & Concerns...

- Linking device to user
  - Reliable registration
- Impossible to implement visual security measures
  - eID card contains visual security measures
- What about malware on phone's OS?