Security and Privacy of Smartcard-based e-Identity

Lejla Batina, Bart Jacobs, Wojciech Mostowski, Erik Poll, and Pim Vullers

Digital Security Group, Radboud University Nijmegen

http://www.ru.nl/ds/

Motivation

Smartcards are the standard technology for e-Identity:

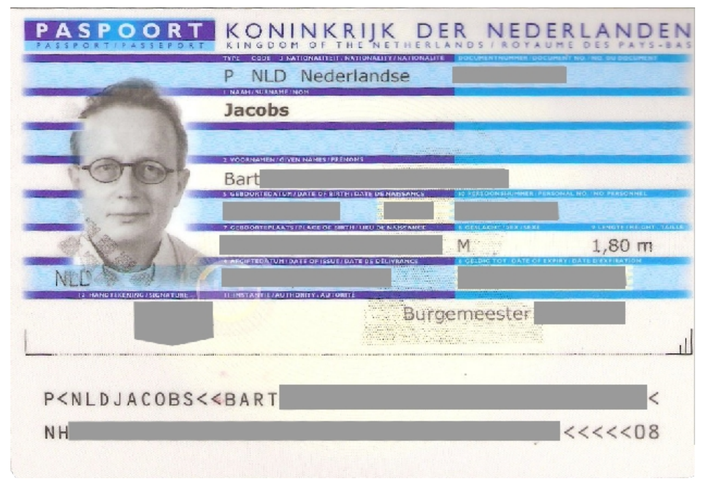
- Bank cards, Biometric passports, ID cards, OV-chipkaart

The use of ID cards will increase, including on-line and for digital signatures.

The Digital Security Group:

- studies existing smartcard solutions
- investigates improved solutions for the future, in theory and in practice

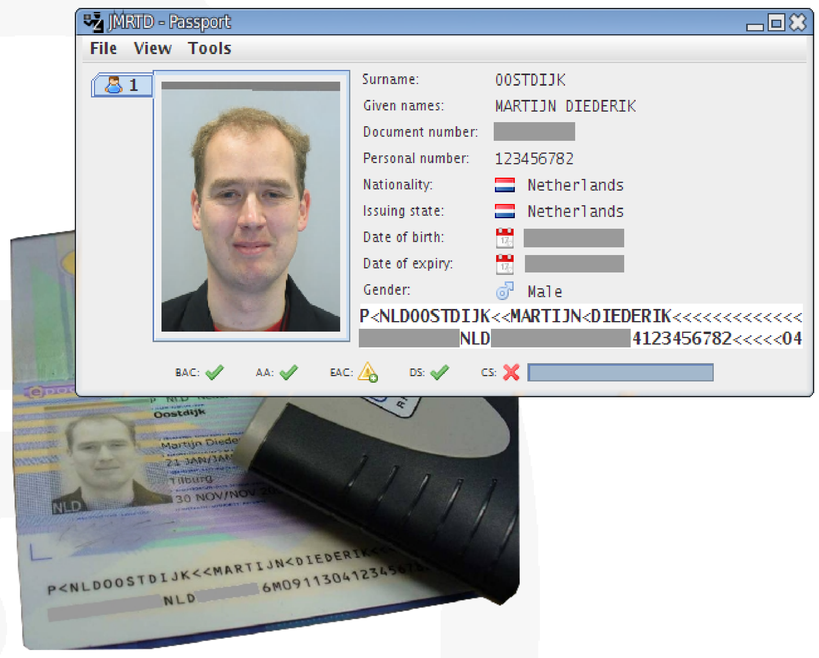
Central concerns: security, privacy, and correctness

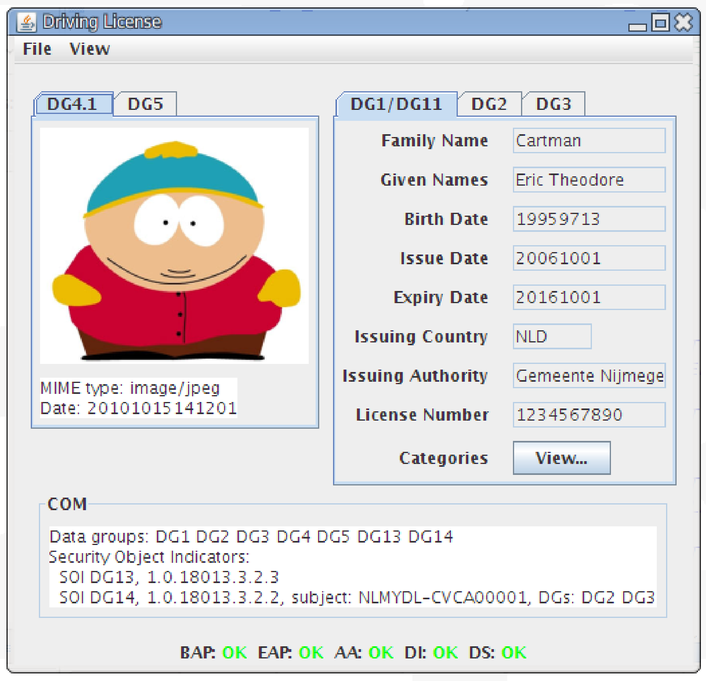


e-Passports

EU passports (and Dutch ID cards) contain RFID chip since 2006, with fingerprint info since 2009:

- Investigation of e-Passport protocols, including possible information leakage
- Security evaluation of e-Passports
- Automated compliance tests using formal models in collaboration with ESI

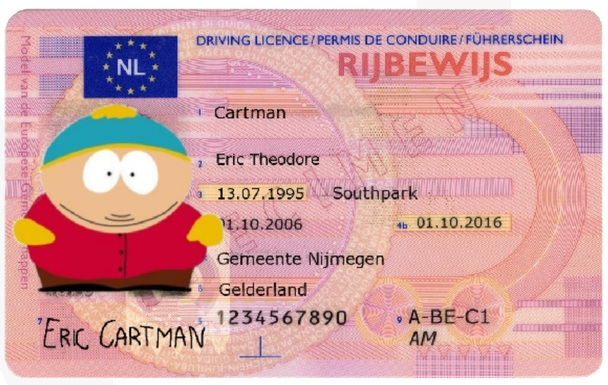




e-Driving License

Driving license may also be equipped with a chip. For RDW we developed:

- The first implementation of ISO18013 Electronic Driving License:
  - Using Java Card
  - Open Source
- With added digital signature functionality for on-line use, e.g. for registering cars



OV Chip 2.0

Privacy friendly solutions for smartcards of the future:

- Basis: Elliptic Curve Cryptography with bilinear pairings
- Blinded signature to provide tokens a.k.a. attributes, e.g.
  - "Over 18" or "Ticket valid in 2010"
- Attribute features: Anonymous, Unlinkable, Unforgable
- Applicable in e-Transport (e-Ticketing) and e-Identity

Results

- Solid and comprehensive overview of security and privacy issues in electronic based identity products
- State-of-the-art protocols for anonymous attributes to protect privacy
- Several prototypes and open source implementations to back up research results

Literature

1. Lejla Batina, Jaap-Henk Hoepman, Bart Jacobs, Wojciech Mostowski, and Pim Vullers. **Developing efficient blinded attribute certificates for smart cards via pairings**. In *Smart Card Research and Advanced Application Conference CARDIS 2010, Proceedings, Passau, Germany*, LNCS 6035, pages 209-222. Springer, April 2010.
2. Jaap-Henk Hoepman, Bart Jacobs, and Pim Vullers. **Privacy and security issues in e-ticketing – Optimisation of smart card-based attribute-proving**. In *Workshop on Foundations of Security and Privacy, FCS-PrivMod 2010, Proceedings*, Edinburgh, U.K., July 2010.
3. Wojciech Mostowski and Erik Poll. **Electronic Passports in a Nutshell**. Technical Report ICIS-R10004, Radboud University Nijmegen, June 2010.
4. Wojciech Mostowski, Erik Poll, Julien Schmaltz, Jan Tretmans, and Ronny Wichers-Schreur. **Model-based testing of electronic passports**. In *Formal Methods for Industrial Critical Systems 2009, Proceedings*, LNCS 5825, pages 207-209. Springer, November 2009.

TU/e Technische Universiteit Eindhoven University of Technology
stw SENTINELS
nlnet FOUNDATION
Trans Link Systems
RDW Collis