Security and Privacy of Smartcard-based e-Identity

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

Digital Security, Radboud University Nijmegen
{lejla,bart,woj,erikpoll,pim}@cs.ru.nl

Keywords: smartcards, e-passports, security, privacy, Java Card

The aim of this poster presentation is to give an overview of research into smartcards for e-identity at the Radboud University. It could be accompanied by demonstrations of the e-passport and our own smartcard solutions.

Abstract

Different kinds of smartcards have "sneaked" into our everyday life over the last decade. Most countries, including all EU countries, now introduced biometric passports (or e-passports) – passports with an embedded contactless smartcard that store biometric data. In many countries contactless smartchips or RFID tags are used in public transport, e.g. the OV-chip card in the Netherlands or the Oyster card in London. Many countries also started issuing electronic ID cards that let citizens digitally sign data (e.g. documents or e-mails) or securely prove their identity over the Internet.

Such technologies and applications naturally raise concerns about security and privacy. The Digital Security group at Radboud University has been conducting research into existing smartcard-based solutions for e-identity and exploring possibilities for new, more privacy-friendly alternatives.

A central case study in research on existing solutions has been the e-passport, where both the protocols as laid down in international standards [3] and security aspects of actual implementations were investigated. This for instance resulted in advanced techniques for the automated and rigorous testing of e-passports, using model-based testing [4]. Also, a substantial amount of open source software was developed, for reading out and for producing e-passports, which provided the basis for a first pilot implementation of a new electronic driving license for the Ministry of Transport.

Work on exploring more privacy-friendly alternatives was started in the OV-chip 2.0 project, funded by Stichting NLNet. Here the aim is to push the boundaries of what modern smartcards are capable of, and implement truly privacy-friendly smartcard protocols for public transport or other e-identity applications using Elliptic Curve Cryptography [1, 2].

Much of the work mentioned above has its roots in the Sentinels funded PinPas Java Card project, which investigated security of the Java Card platform. Java Card provides an open, Java-based environment for programming smarts cards, and has been used in all of our projects to prototype and test our ideas.

Acknowledgments This research been supported by the NWO/STW/EZ research program Sentinels (through the project PINPAS JC), Stichting NLnet, and Trans Link Systems.

References

1. Lejla Batina, Jaap-Henk Hoepman, Bart Jacobs, Wojciech Mostowski, and Pim Vullers. Developing efficient blinded attribute certificates on smart cards via pairings. In *Smart Card Research and Advanced Application Conference CARDIS 2010, Proceedings, Passau, Germany*, volume 6035 of *LNCS*, 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 Veronique Cortier, Mark Ryan, and Vitaly Shmatikov, editors, *Workshop on Foundations of Security and Privacy, FCS-PrivMod 2010, Edinburgh, UK, July 14-15, 2010. Proceedings*, July 2010.
3. Wojciech Mostowski and Erik Poll. Electronic Passports in a Nutshell. Technical Report ICIS–R10004, Radboud University Nijmegen, June 2010. Available at `https://pms.cs.ru.nl/iris-diglib/src/getContent.php?id=2010-Mostowski-ElectronicNutshell`.
4. Wojciech Mostowski, Erik Poll, Julien Schmaltz, Jan Tretmans, and Ronny Wichers Schreur. Model-based testing of electronic passports. In María Alpuente, Byron Cook, and Christophe Joubert, editors, *Formal Methods for Industrial Critical Systems 2009, Proceedings*, volume 5825 of *LNCS*, pages 207–209. Springer, November 2009.

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:

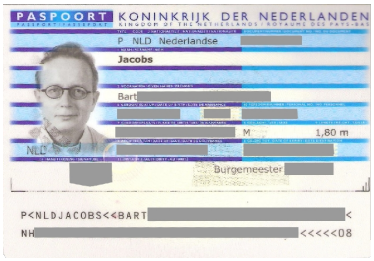
- Bank cards, Biometric passports, ID cards, OV-chipkaart

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

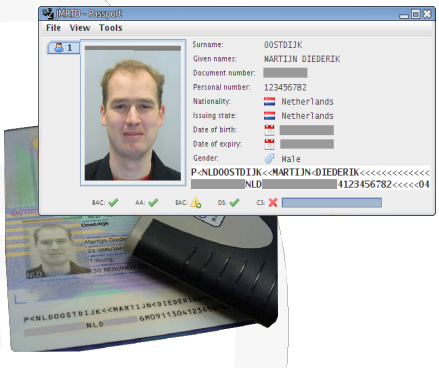
Central concerns: security, privacy, and correctness

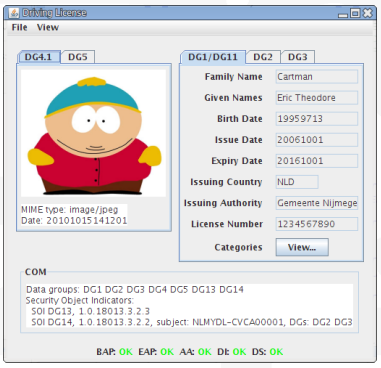


e-Passports

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

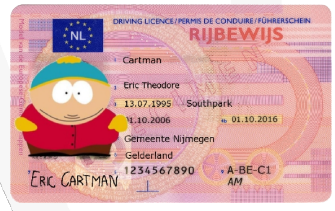




e-Driving License

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

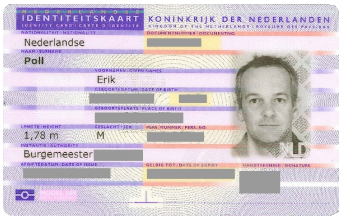
- The first implementation of ISO18013 Electronic Driving License:
  - Using Java Card
  - Open Source
- With added digital signature functionality for on-line use, e.g. for registering cars



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.