OV-chip 2.0: “Applet-based e-ticketing”

Pim Vullers MSc
p.vullers@cs.ru.nl

Institute for Computing and Information Sciences
Radboud University Nijmegen

e-Transport Forum
16th September 2009
Who am I

Pim Vullers MSc
p.vullers@cs.ru.nl

2004 – 2007 Bachelor Student – Computer Science
Eindhoven University of Technology

Kerckhoffs Institute: Eindhoven University of Technology,
University of Twente and Radboud University Nijmegen.

Master Project:
“Secure Ownership and Ownership Transfer in RFID Systems”
University of Luxembourg

2009 – … PhD Student – Digital Security
Institute for Computing and Information Sciences:
Radboud University Nijmegen

OV-chip 2.0: “Applet-based e-ticketing”
What has been done

- Development of privacy-friendly protocols
  - Attributes instead of identity
  - Selective disclosure
  - Using RSA cryptography
  - Using EC cryptography

- Implementation on (JavaCard) smartcards (for RSA)
  - Communication framework
  - Cryptographic primitives
  - Performance tests
  - Prototype OV-chip applet

- Implementation on (NFC-enabled) mobile phones (for RSA)
  - Communication framework
  - Cryptographic primitives (based on JavaCard)
  - Performance tests (based on JavaCard)
How to proceed

“open” work, publication oriented

- Development of privacy-friendly protocols
  - Attributes instead of identity
  - Selective disclosure
  - Using EC cryptography
- Implementation on (JavaCard) smartcards (for EC)
  - Performance tests
  - Prototype OV-chip applet
- Implementation on (NFC-enabled) mobile phones (for EC)
  - Performance tests (based on JavaCard)
  - Prototype OV-chip applet (based on JavaCard)
  - Possibilities of mobile phone compared to smartcard
How to proceed (cont’d)

- New TLS OV-chipkaart (confidential, background work)
  - Analysis of specifications
  - Analysis of TLS prototype(s)
  - Performance / conformance tests
  - Investigate migration issues / feedback
    (depending on TLS input / wishes)
- Development of open source RU prototype(s)
- Study possible integration with other card functionality
  (signing, e-cash, driving license, id card)
- Coordination with Tilburg
- …