Attribute-proving for Smart Cards

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

Institute for Computing and Information Sciences – Digital Security
Radboud University Nijmegen

8th July 2011
Context

*Smart cards are “Big Brother’s little helper”* (Stefan Brands)

**e-Ticketing**

- The OV-chipkaart stores your *identity*
- With a OV-chipkaart you tell . . .
  - when (date and time),
  - how (bus, train, metro, . . . ), and
  - where (precisely at which stop)

  . . . you travel

- This data is stored for several years; Serious privacy concerns!

**Detailed profiles**

. . . can be composed by *both* legitimate and *and* malicious parties.
Anonymous Credentials

Possible solution

- Attribute-based authorisation
- Anonymous credentials: card only says “I’m a first class year pass valid in 2011”
- Subtle point: attribute may be non-identifying, but the digital signature may be used for tracing cards/individuals

Why anonymous credentials?

- Identity-based solutions violate their users’ privacy (and increase identity-fraud risk)
- Anonymous credentials provide the same level of security
- Attributes provide all the system needs to know
Broader Context

**e-Identity**

- Electronic passport and identity cards
- Storing (sensitive) personal information: your identity
- Newest features:
  - e-Signature application
  - On-line authorisation (DigiD)
  - (Attributes)

**Beyond the government...**

Use of verified attributes by commercial parties can easily result in undesired traceability by both the government and third parties.
Introduction
Self-blindable certificates
U-Prove
Idemix
Conclusion

Privacy and Smart Cards

Protection against outsiders
- Random UID
- Reader authentication
- Secure messaging
- Problem: performance

Protection against insiders
- Harder problem
- Zero-knowledge proofs or blinding of identifiable information
- Practical implementations are rare
- Bad performance
Outline

Introduction

Self-blindable certificates

U-Prove

Idemix

Conclusion
Self-blindable certificates (Verheul, Radboud University)

- Main ingredient: Attribute certificate
  - Single attribute
  - Issuer’s signature
  - Prover’s public key
- Issuance
  - Issuer learns the public key
  - Strongly identifying
- Attribute proving
  - Fresh blinding of certificate and public key for each session
  - Untraceable

Performance
Keep smart card implementation in mind while designing.
Self-blindable certificates (Verheul, Radboud University)

Results

- Good performance:
  - Batina et al. (2010): 1.5 seconds (for 1 attribute)
  - Hoepman, Jacobs and Vullers (2010): 0.6 seconds (for 1)
- Anonymous credentials on smart cards are becoming possible

Issues

- This protocol proves only a single attribute (efficiency)
- Attributes do not have values
- Revocation is not supported by the current protocol
- Major bottleneck is the limited access to the cryptographic coprocessor of the Java Card smart card
Outline

Introduction

Self-blindable certificates

U-Prove

Idemix

Conclusion
U-Prove (Brands, Microsoft)

- Main ingredient: U-Prove token
  - Multiple attributes
  - Token’s public key
  - Issuer’s signature
- Blind issuance
  - Issuer does not learn the public key, only the attribute values
  - Issuer unlinkability
- Selective disclosure
  - Prover can decide which (properties of) attributes to show
  - Data minimisation

Traceability
Public key and signature can be used as a pseudonym.
U-Prove (Brands, Microsoft)

Results

• Previous Java Card implementation: Tews and Jacobs (2009)
  • 5 seconds (for 2 attributes), 8 seconds (for 4)
• Efficient MULTOS impl.: Mostowski and Vullers (2011)
  • 0.5 seconds (for 2), 0.8 seconds (for 5)
• Compatible with U-Prove SDK (only smart card limitations)

Issues

• The token serves as a pseudonym (multi-show linkability)
• Microsoft pursues a different smart card approach
• Advanced features (derived attributes) are costly
• Our MULTOS cards have little RAM and limited cryptography
Idemix (Camenisch & Lysyanskaya, IBM Research Zürich)

Components
- Pseudonyms
- Camenisch-Lysyanskaya signatures
  - blind signature scheme
  - self-blindable signatures
- Zero-knowledge proofs

Features
- Both issuer and multi-show unlinkability
- Efficient attributes encoding

Complexity
The many zero-knowledge proofs make it hard to understand and lead to a high computational complexity.
Idemix (Camenisch & Lysyanskaya, IBM Research Zürich)

Results

- Direct Anonymous Attestation
  - Commercial use of anonymous credentials
  - Anonymous authentication of a TPM
  - No attributes
- Java Card implementations (of DAA):
  - Bichsel et al. (2009): 7.5 seconds
  - Sterckx et al. (2009): 3 seconds

Issues

- Complexity (steep learning curve)
- Only smart card implementations for DAA
Conclusion

- Anonymous credentials on smart cards are becoming possible
- Our results are in line with previous work
- Major bottleneck:
  - Java Cards: limited access to the cryptographic coprocessor
  - MULTOS: little RAM and limited cryptography (RSA $> 1024$, ECC) support

Challenges for future research

- Implementing Idemix on MULTOS
- Dealing with smart card platform shortcomings
- Adoption (ongoing project with Novay)