U-Prove on a smart card

Smart card implementation of Microsoft U-Prove on MultOS

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

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

e-Transport Forum
9th March 2011
History

Aug 2000  "Rethinking Public Key Infrastructures and Digital Certificates; Building in Privacy" by Stefan Brands
Jan 2002  Brands founded Credentica to implement U-Prove
Feb 2007  U-Prove technology first released by Credentica

Mar 2008  Microsoft acquires Credentica
Mar 2010  Microsoft published U-Prove protocol specification under the Open Specification Promise with open source reference toolkits in C# and Java
Feb 2011  Release 1.1 of the specification and toolkits
U-Prove token

The ideas

- Pseudonyms
- Attributes
- Selective disclosure

U-Prove token

- Attributes
- Token information
- Prover information
- Token’s public-key
- Issuer’s signature
U-Prove features

**Implemented features**
- Blind issuing
- Selective disclosure
- Device-protected tokens (new in version 1.1)
- Proving attribute properties (interval proof by Pieter Rogaar)

**Unimplemented features**
- Privacy-preserving revocation
- Proving attribute properties
- Limited-use tokens
- Token recertification and updating
- ...
Design of the smart card implementation

- CardService translates U-Prove commands and data types into APDU commands for smart card communication
- MultOS implementation, limited by smart card characteristics, is 90-95% compatible with U-Prove SDK
Results

Performance

- Card setup: 4.6 sec
- Issuing 5 attributes: 2.7 + 1.9 sec
- Disclosing 2 out of 5 attributes: 2.9 sec

Demonstration

- Work in progress
- Currently only command-line applications
- Demo application is under development

Thanks to:

- Wojciech Mostowski (RU)
- Pieter Rogaar (RU and KPMG)