

ADAPID: ADVANCED APPLICATIONS FOR E-ID CARDS

Claudia Diaz
K.U.Leuven / COSIC

L-SEC Identity Management and e-ID Conference
February 28, 2008

ADAPID General Info

- ▣ Duration: July 2005 to June 2009
- ▣ Funded by IWT under SBO program
- ▣ Partners:
 - KULeuven/COSIC (coordinator)
 - KULeuven/DistriNet
 - KULeuven/ICRI
 - McGill University
 - Intesi Group Belgium
 - L-SEC

ADAPID User Group

▣ Goals

- ▣ Fine-tuning of the priorities in the work plan; this is particularly relevant for the work focused on applications
- ▣ Exploring valorization opportunities, such as funded research projects (IWT, EU) or development of commercial solutions
- ▣ Technology transfer of selected results developed in the project towards the key actors in the government and non-profit sector

▣ Requirements

- ▣ Letter expression of intention
- ▣ NDA
- ▣ Attend two meetings a year and project workshops (once a year)

▣ To apply

- ▣ Send email to: claudia.diaz@esat.kuleuven.be

User Group current members

- ▣ NXP Semiconductors
- ▣ Weblications
- ▣ The eID Company
- ▣ Nexus Technology
- ▣ Deloitte & Touche
- ▣ dZine
- ▣ Zetes
- ▣ Vasco Data Security
- ▣ GlobalSign
- ▣ Fedict
- ▣ Verizon
- ▣ Marijke De Soete
- ▣ Ubizen
- ▣ L-SEC
- ▣ Integri

ADAPID Goals

- ▣ Developing a framework for secure and privacy-preserving applications based on the Belgian e-ID card
- ▣ Focusing mainly on **e-government**, **e-health** and **secure archiving** applications, and taking into account both **technical** and **legal** aspects
- ▣ Investigating technologies for future enhanced generations of the e-ID card

ADAPID Research

- ▣ More than 40 publications on:
 - Digital (anonymous) credentials
 - Anonymity metrics
 - Anonymous communication
 - Trust distribution primitives
 - Private database operations
 - Long-term secure archives
 - Modeling methodologies
 - Data protection
 - Policies and Digital Rights Management (DRM)
 - Legal aspects of trust and evidence trails

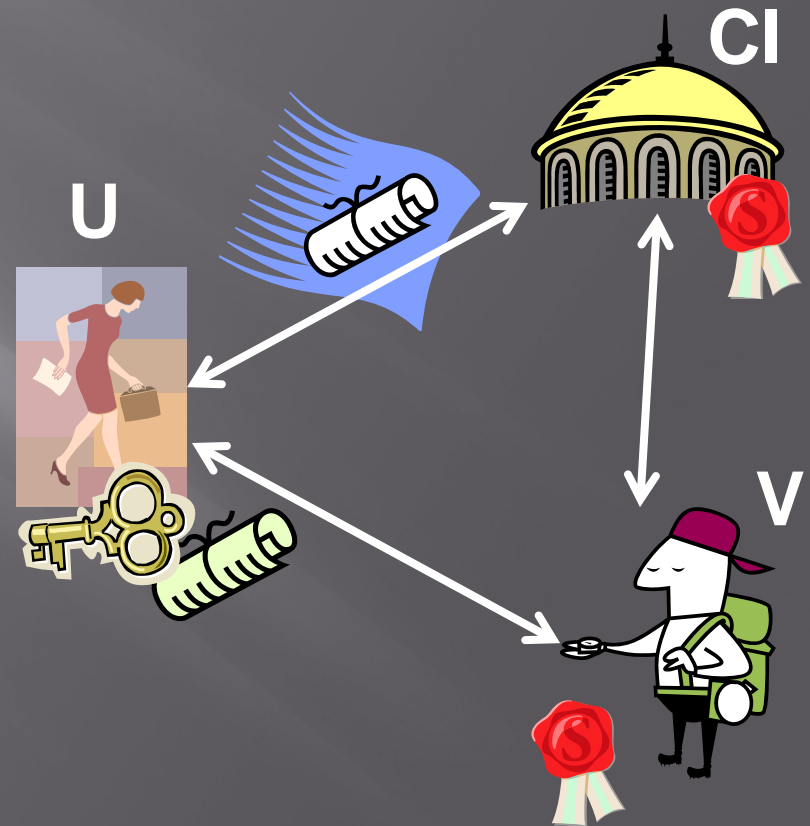
- ▣ Deliverable Basic Research available in our website

Anonymous credentials

- ▣ Privacy risks of ubiquitous use of PKI-based e-IDs
 - Excessive personal information available in certificate
 - Unique identifiers: linkability, tracking
 - Lack of flexibility for use of e-ID outside well-defined interactions with the Government (tax, registry, benefits)
- ▣ Privacy friendly alternative to PKI credentials
 - Based on cryptographic protocols and Zero-Knowledge proofs to reduce to the bare minimum the amount of information disclosed
 - Flexible protocols, many options possible (possession of multiple credentials, de-anonymization,)
 - Implementation by IBM Research, tackled by EU Prime/PrimeLife

Anonymous credentials: example

1. CI issues a credential to U that encodes U's age
2. U can prove to V that her age is above/below a threshold
3. V does not learn U's exact age
4. V can check that this is certified by CI
5. Even if CI and V collude they cannot link U's credential issue and show interactions (1 and 2)



ADAPID Applications

- ▣ Applications first two years of the project:
 - E-Government: Privacy-enhanced e-petitions
 - E-Health: Issuing and handling e-prescriptions
 - Trusted Archives: Design and implementation of long-term secure archives
- ▣ Deliverables e-Government, e-Health, and Archiving available in our website
- ▣ Proof-of-concept demonstrators for these applications

Next ADAPID Workshop

- ▣ Date: July 22, 2008 (half day)
- ▣ Place: Faculty of Law (Ladeuzeplein, Leuven)
- ▣ We will present our latest research results and will have one/two invited speakers

- ▣ Co-Located with
 - EU FP6 PRIME (Privacy and Identity Management for Europe) final workshop on July 21, 2008
 - WOTE (Workshop on Trustworthy Elections) on July 22-23, 2008
 - 8th PETS (Privacy Enhancing Technologies Symposium) on July 23-25, 2008

... for more information

- ▣ ADAPID website:
 - ▣ <https://www.cosic.esat.kuleuven.be/adapid/>
- ▣ ADAPID docs and deliverables available at:
 - ▣ <https://www.cosic.esat.kuleuven.be/adapid/documents.html>
- ▣ Send us an email to:
 - ▣ Claudia.Diaz@esat.kuleuven.be