GOETHE UNIVERSITÄT FRANKFURT AM MAIN

www.goethe-universitaet.de

Evaluation of Privacy-ABC technologies

Fatbardh Veseli
Chair of Mobile Business and Multilateral Security
Goethe University Frankfurt, Germany
fatbardh.veseli@m-chair.de

Oslo, May 3, 2017

Overview

- Myself
- Research projects
- Own research focus – Privacy-ABC technologies
- (Chosen) Results
- Conclusion and future work

About myself

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Studies

- BSc. Computer Science, BSc. Management & Iformatics @Uni Prishtina (2004-2008)
- MSc. Informaton Security @Gjovik University College (Norway) and @Ruhr University Bochum (Germany) (2009-2011)
- PhD Candidate, Research & Teaching Assistant @Goethe University Frankfurt (2011-ongoing)

General Research Interests:

- Privacy enhancing technologies
- User-centric identity management
- Security and privacy evaluation

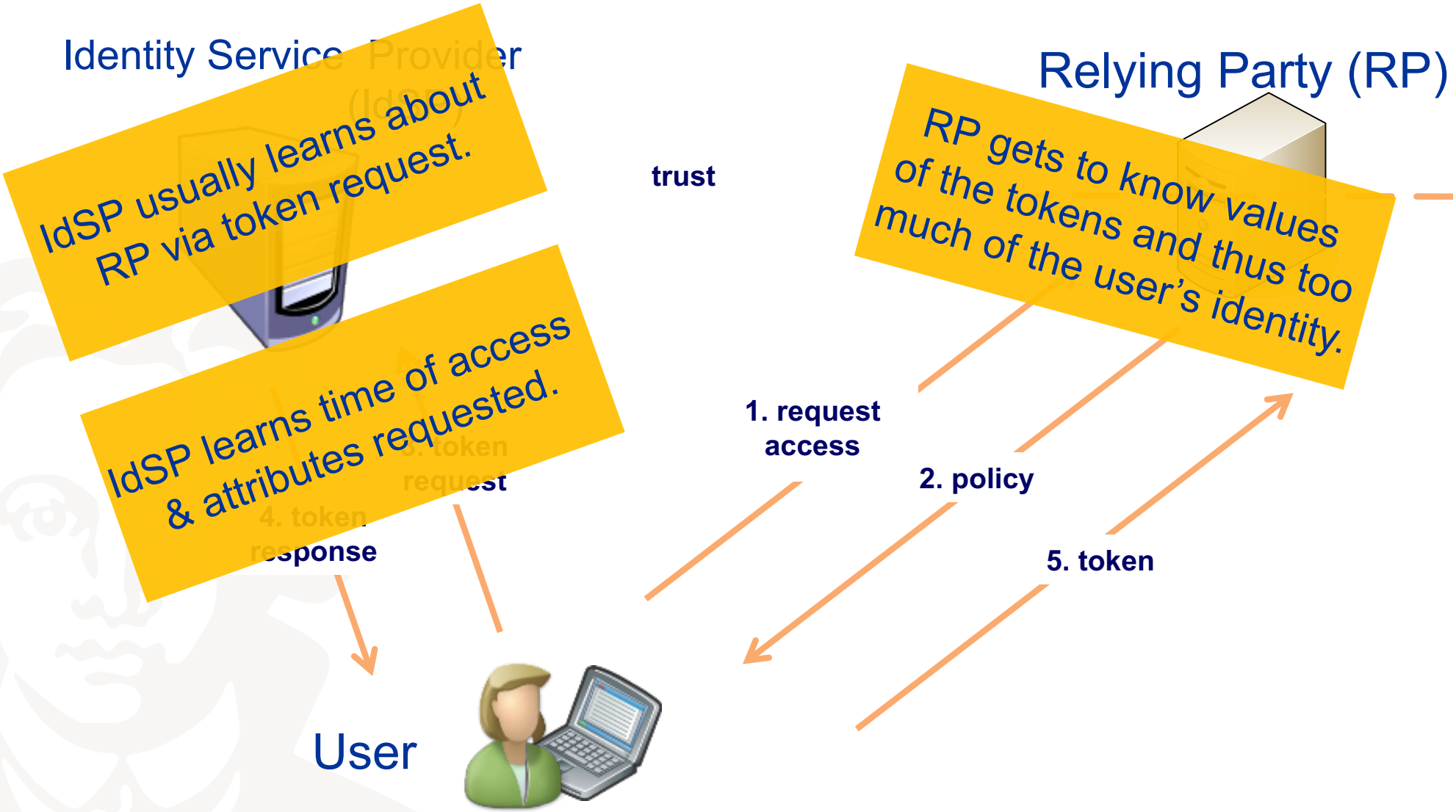
ABC4TRUST

CREDENTIAL

Overview

- Myself
- Research projects
- Own research focus – Privacy-ABC technologies
- (Chosen) Results
- Conclusion and future work

Privacy (and security) issues of typical federated IdM architectures



ABC4Trust
Overview and Goals

- Attribute-based Credentials for Trust (ABC4Trust)
- Nov. 2010 till Feb. 2015
- Objectives:
  - Abstraction of concepts of privacy-ABCs & unification of features
  - A common unified architecture
    - Independent from the specific technologies
    - Enabling the federation of privacy-ABC Systems based on different technologies
    - Enabling interoperability between different privacy-ABC technologies
- Avoid lock-in into one specific system
- Raise trust in privacy-ABC technologies

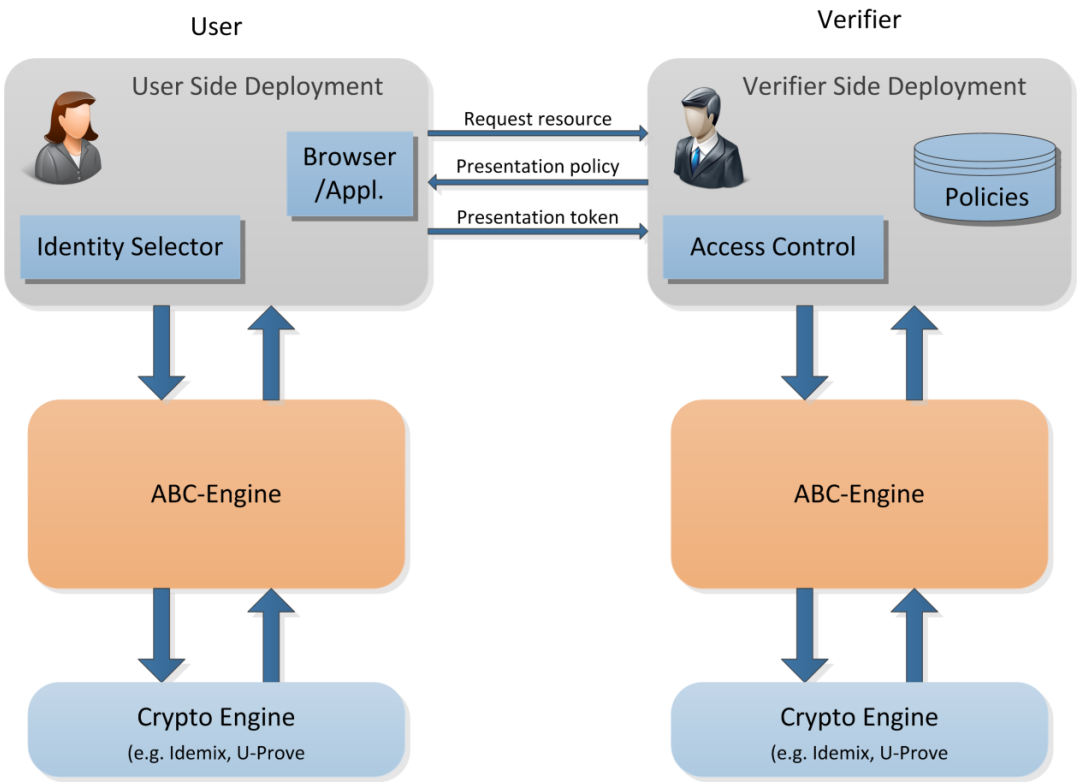
ABC4Trust receives research funding from the 7th Research Framework Program (FP7) of the EU as part of the Trust & Security Program.

ABC4Trust
Architecture goals

Reference implementation with ABC functionality
- coded in the ABC-Engine,
- exposed to the application layer
- as web-services,
- as open source.

For developers
- Easier application development
- Cryptographic operations are abstracted away from.

For users
- Only need to install a browser plug-in



mobile business

CREDENTIAL
Overview and Vision

Key administrative info:
Duration: since October 2015 for 3 years
Coord.: Austrian Institute of Technology GmbH

Vision: develop, test, and **showcase innovative cloud-based services** for storing, managing, and sharing **digital identity information** and other highly critical **personal data** with a demonstrably **higher level of security** than other current solutions.

- Secure, user-friendly, cloud-based identity management solution
- Open, portable and broadly interoperable architecture

Piloting in different domains

- e-government,
- e-health, and
- e-business

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Atos

IAIK TU Graz

KARLSTADS UNIVERSITET

klughammer

Fraunhofer FOKUS

OTE

LOMBARDIA INFORMATICA

CREDENTIAL
Foundations and specific goals

- **Proxy cryptography** for secure and privacy preserving information sharing in the cloud:
  - It shall be guaranteed that identity data in the cloud maintains confidentiality, integrity and authenticity.
  - Personal data are stored in encrypted form at the cloud service provider.
  - Cloud service provider can "re-encrypt" the data without having access to the plaintext.
  - Users get full control over their data via selective management of access rights.
- Strong hardware-based **multi-factor authentication** with **end-to-end encryption.**
- **User-friendliness** shall be ensured without lowering security requirements.

Overview

- Myself
- Research projects
- Own research focus – Privacy-ABC technologies
- (Chosen) Results
- Conclusion and future work

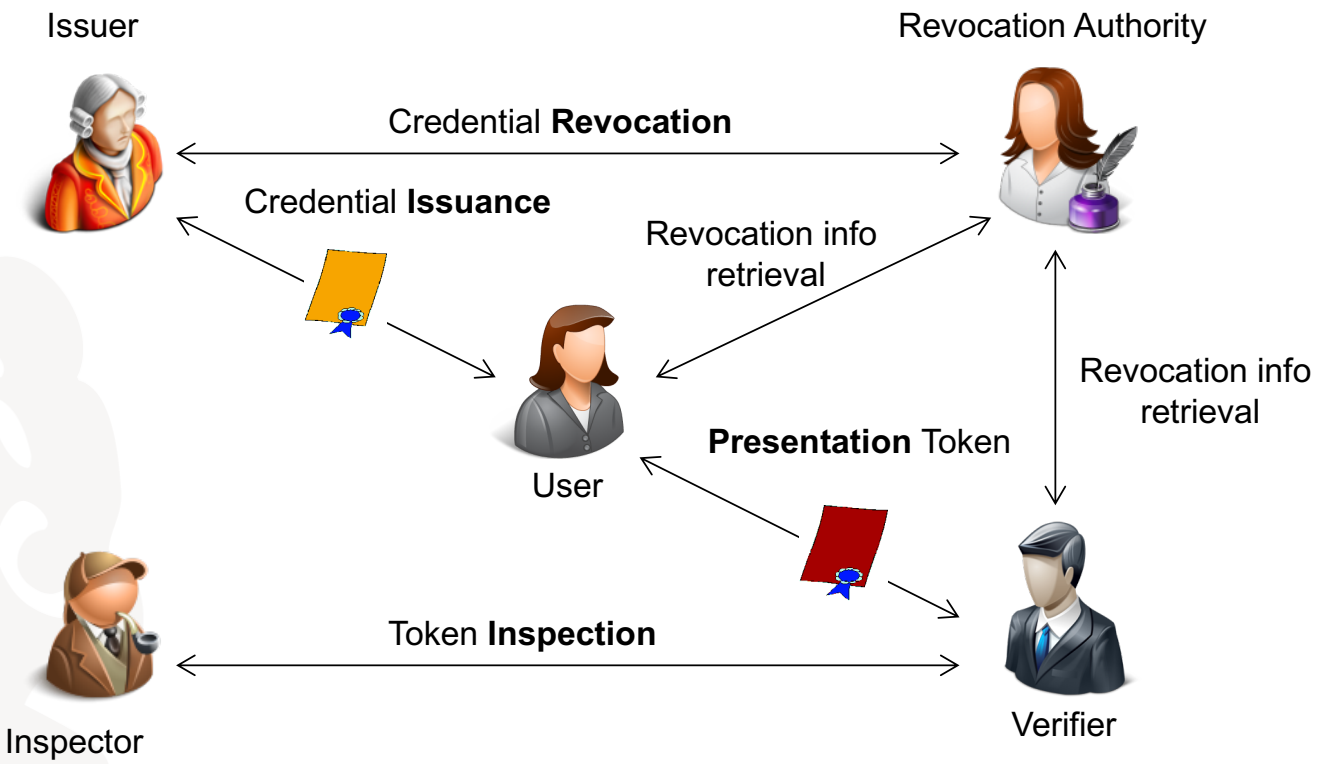
Intro to Privacy-ABC technologies

- AKA “Anonymous credentials”, the original concept dates back to David Chaum’s pseudonymous system (1985)
- Privacy-ABC – Privacy-enhancing attribute-based credentials
- Container of issuer-certified attributes, e.g. university can certify a student credential with student name, date of birth, address, student ID, etc.
- Provide a comparable security assurance to “traditional” PKI + privacy

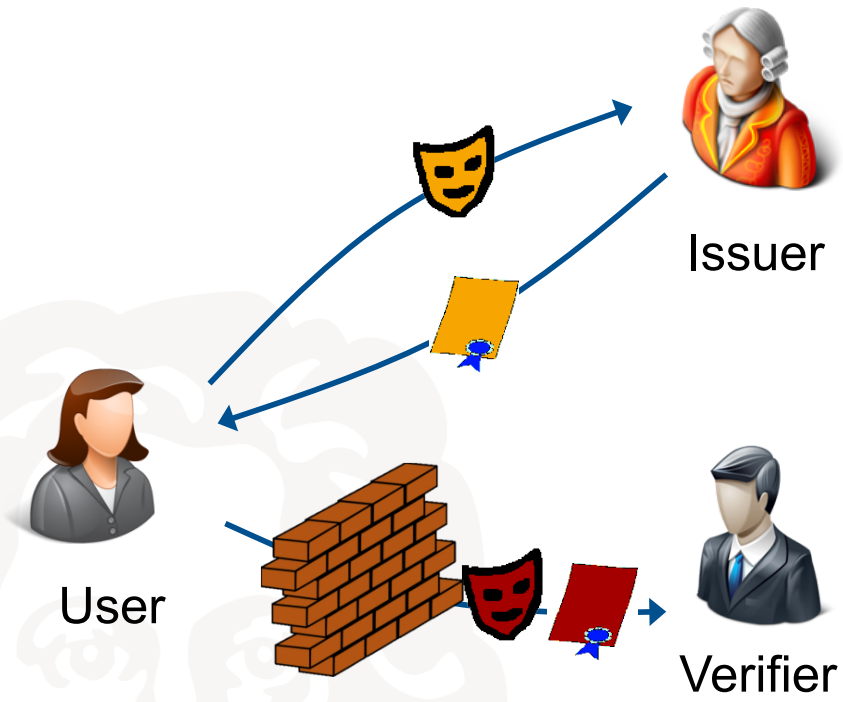
(David Chaum. 1985. Security without identification: transaction systems to make big brother obsolete. *Commun. ACM* 28, 10 (October 1985), 1030-1044. DOI=http://dx.doi.org/10.1145/4372.4373)

A high level overview of Privacy-ABC system

Entities and their interactions

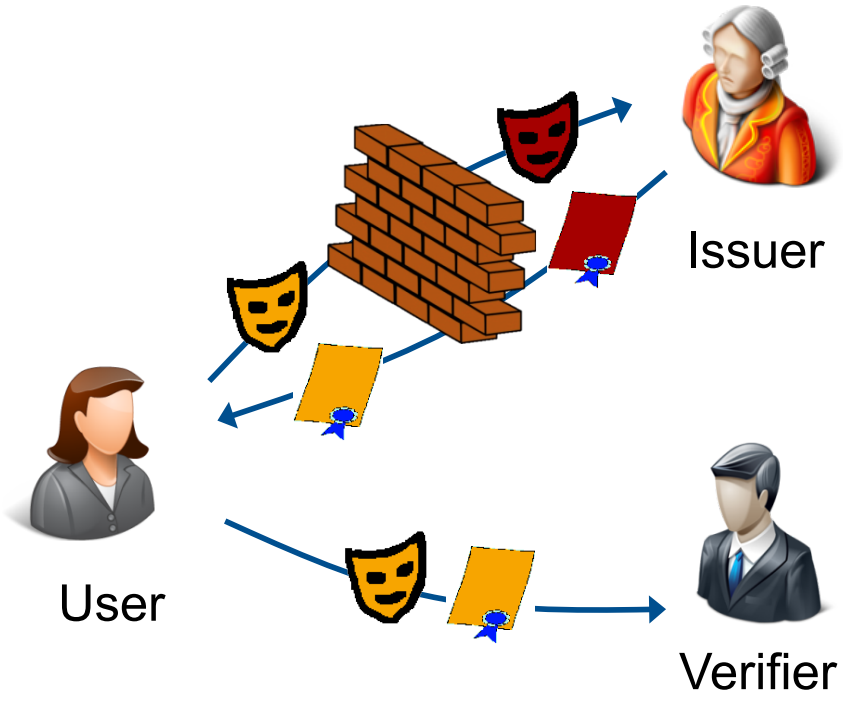


Prominent examples of Privacy-ABC technologies



IBM's Idemix (Identity Mixer)

Damgard, Camenisch & Lysyanskaya
Strong RSA, pairings (LMRS, q-SDH)



Microsoft's U-Prove

Chaum, Brands et al.
Discrete Logs, RSA,…

Key innovative (privacy) properties of Privacy-ABC technologies

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

- Issuance
  - *Carry-over attributes*
  - *Key binding*
  - *Pseudonyms*
- Presentation: proving (User) + verification (Verifier)
  - *Selective disclosure* of attributes -> disclose only a subset of attributes
  - *Untraceability* of presentation to issuance
  - *Unlinkability** between different different presentations
  - *Pseudonyms*
  - *Predicates over attributes*, e.g. “prove” being over 18 without disclosing date of birth.
  - *Inspection* or conditional accountability
  - *Revocation* and *non-revocation proof* (preserving unlinkability)

Research goals

- Provide a common set of criteria for evaluating different Privacy-ABC technologies
- Understand differences between prominent Privacy-ABC technologies
- Help service providers to select the most suitable Privacy-ABC technology for a given service
- Assess the actual impact of individual factors on the overall evaluation of Privacy-ABC technologies

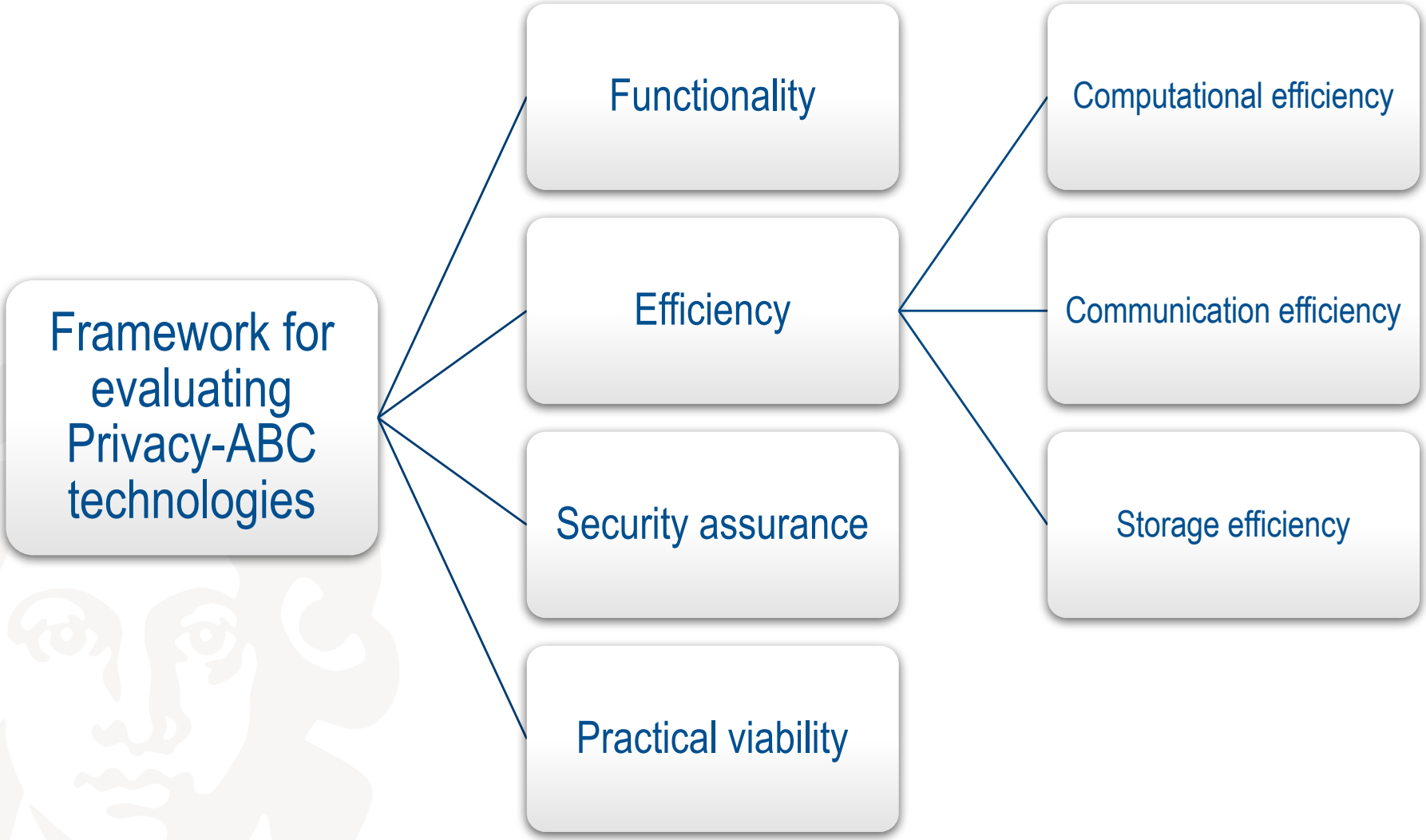
Research questions

- How can we evaluate different Privacy-ABC technologies?
- Which are the common factors that influence a concrete evaluation of different Privacy-ABC technologies?
- How do these factors influence respective evaluations of Privacy-ABC technologies?

Overview

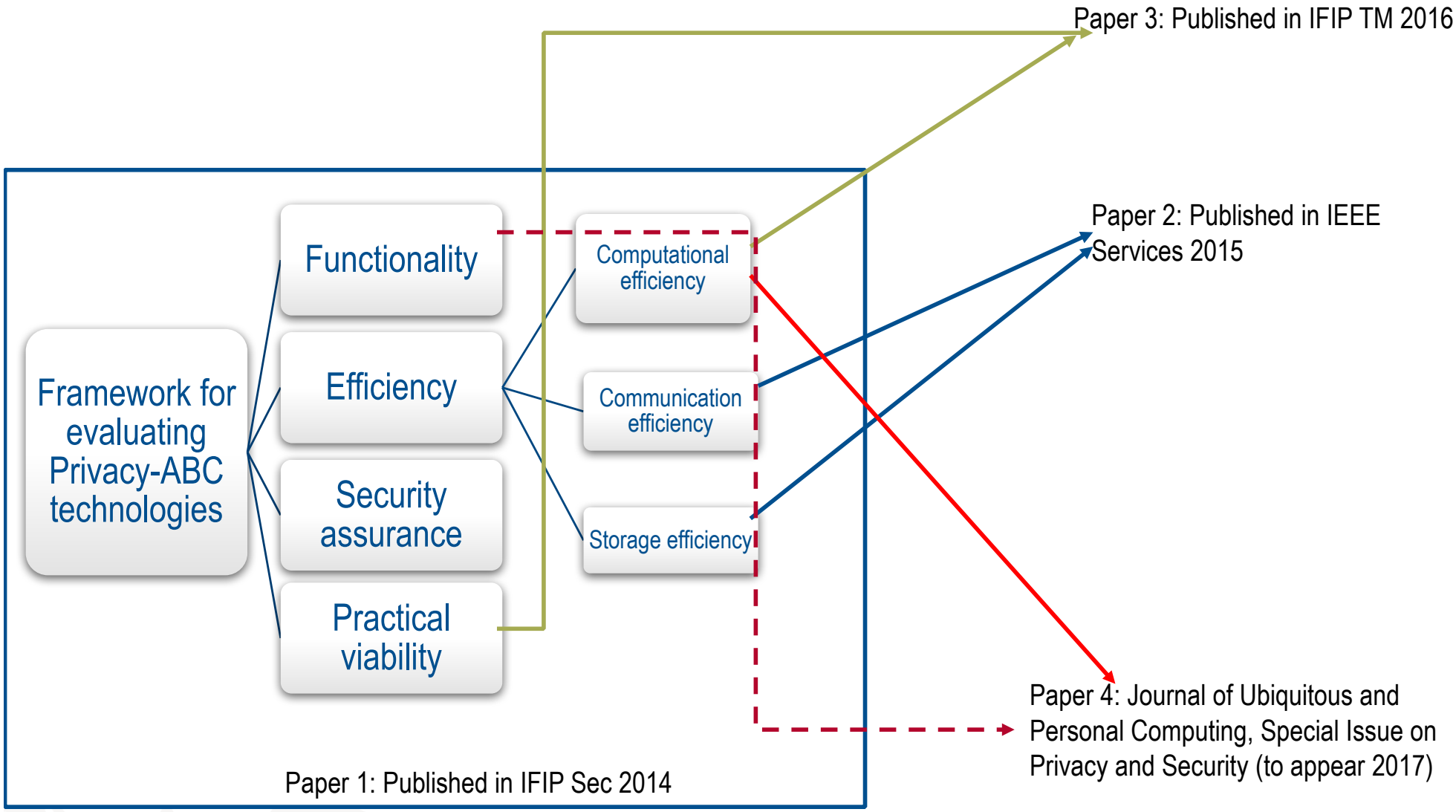
- Myself
- Research projects
- Own research focus – Privacy-ABC technologies
- (Chosen) Results
- Conclusion and future work

A framework for evaluating Privacy-ABC technologies



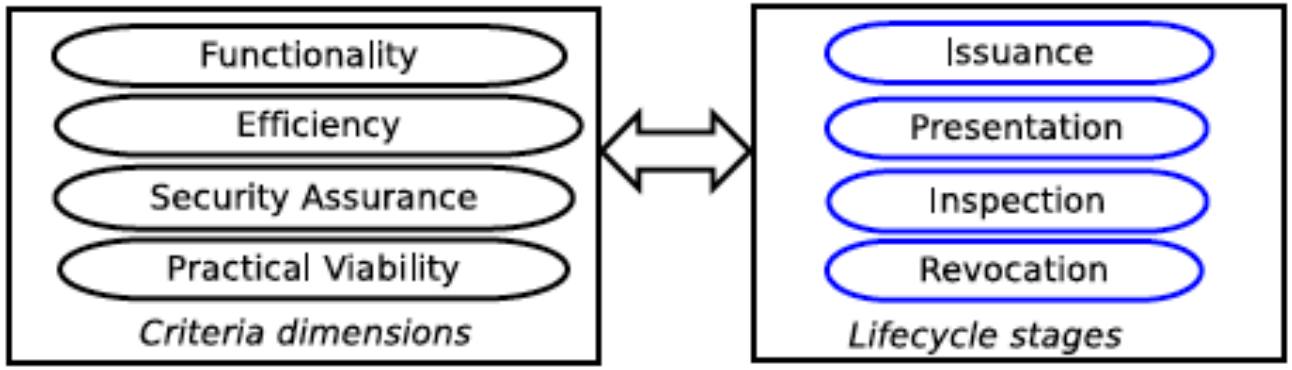
F. Veseli, T. Vateva-Gurova, I. Krontiris, K. Rannenberg, and N. Suri. Towards a Framework for Benchmarking Privacy-ABC Technologies. In N. Cuppens-Boulahia, F. Cuppens, S. Jajodia, A. Abou El Kalam, and T. Sans, editors, *ICT Systems Security and Privacy Protection*, volume 428 of *IFIP Advances in Information and Communication Technology*, pages 197–204. Springer Berlin Heidelberg, 2014.

(Dissertation) Building blocks



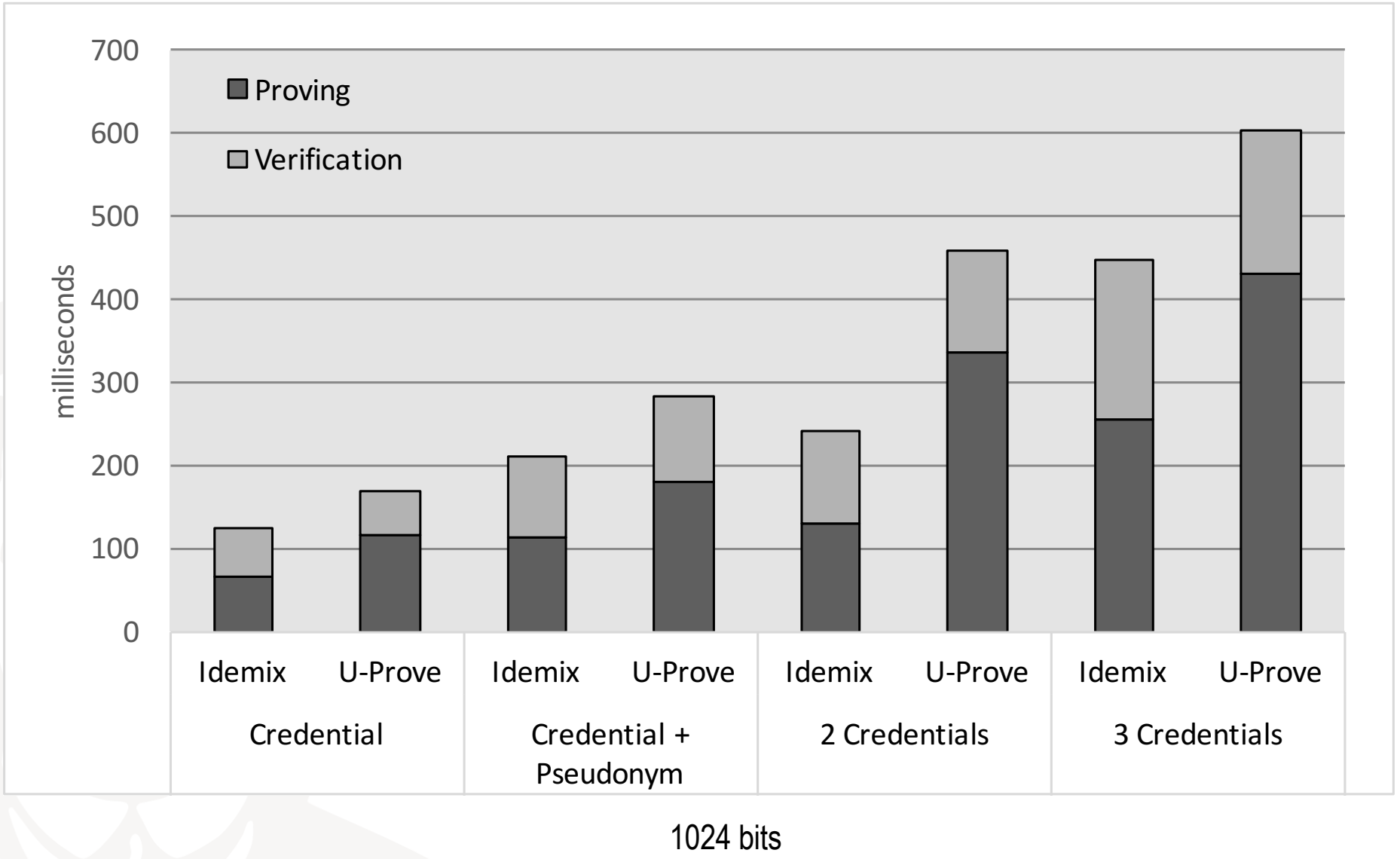
High level overview Organization of the framework Paper 1

- (optional) Further sub-dimensions
- Individual evaluation criteria for each (sub) dimension



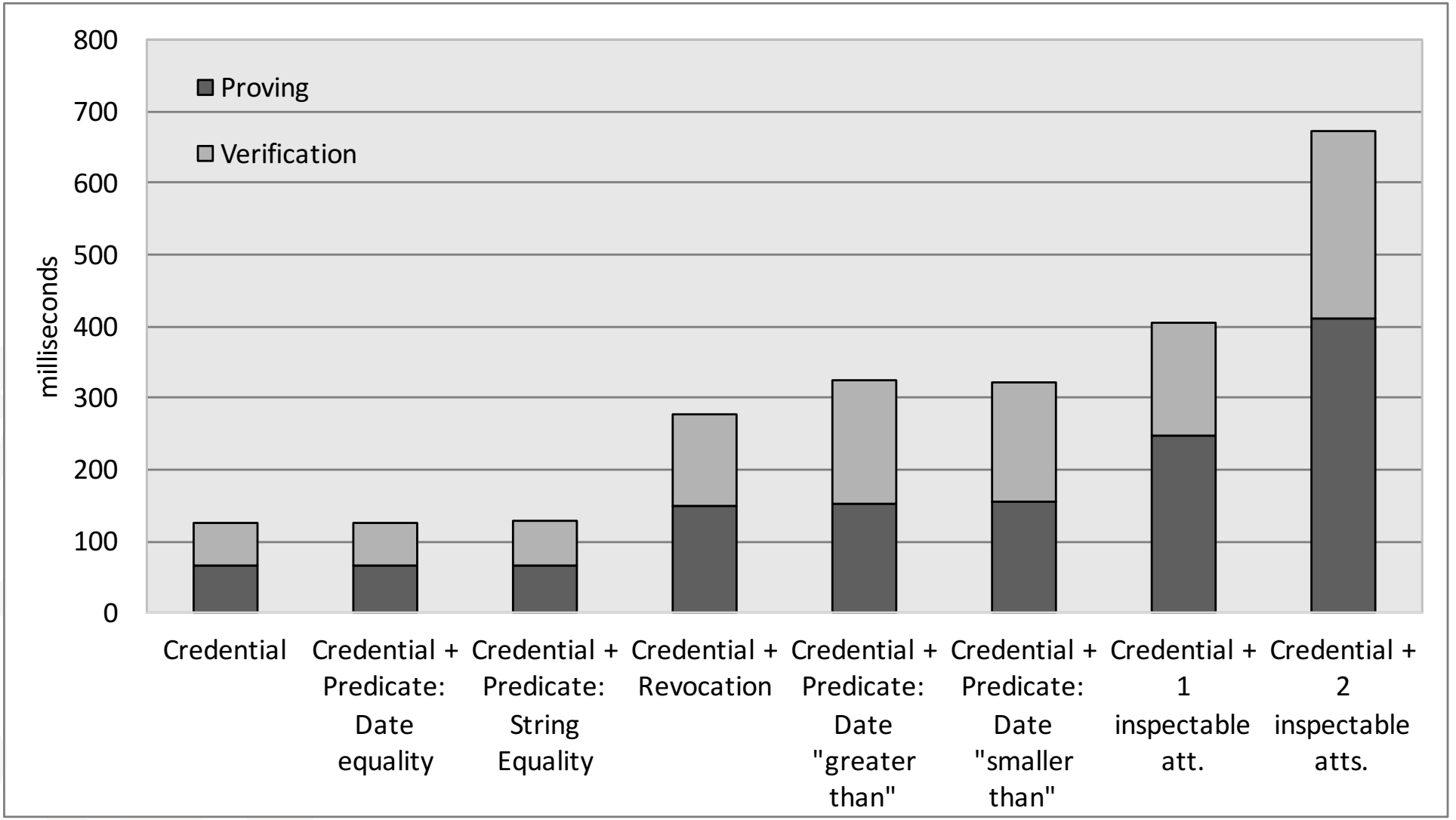
Computational efficiency of presentation

Paper 3



Computational efficiency of presentation

Evaluating the impact of common factors for both technologies - Paper 3



Results shown for Idemix with 1024 bits

Computational efficiency comparison between three Privacy-ABC technologies
Paper 4

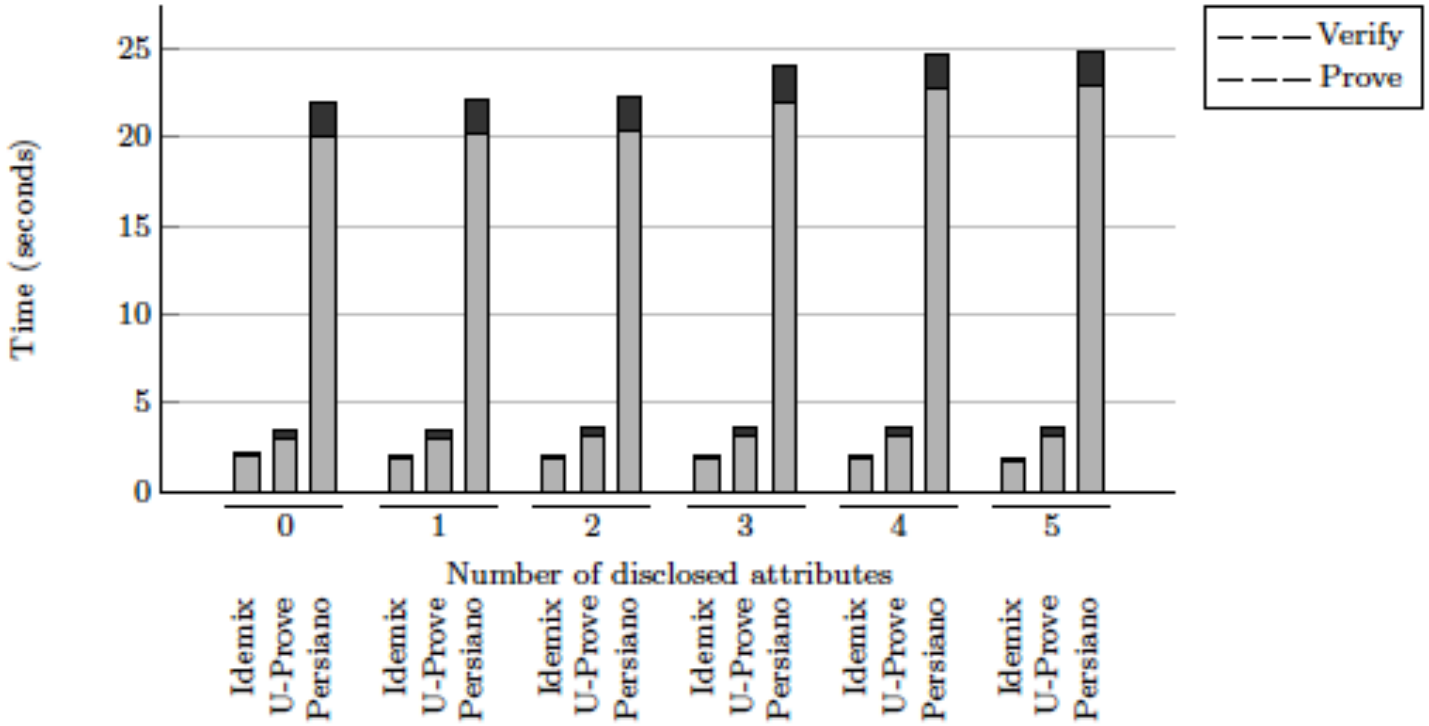


Fig. 8 Evaluation fo the impact of the selective disclosure on the time efficiency of presentation. Results based on the key size of 2048 bits and a credential with 5 attributes for all three technologies.

Overview

- Myself
- Research projects
- Own research focus – Privacy-ABC technologies
- (Chosen) Results
- Conclusion and future work

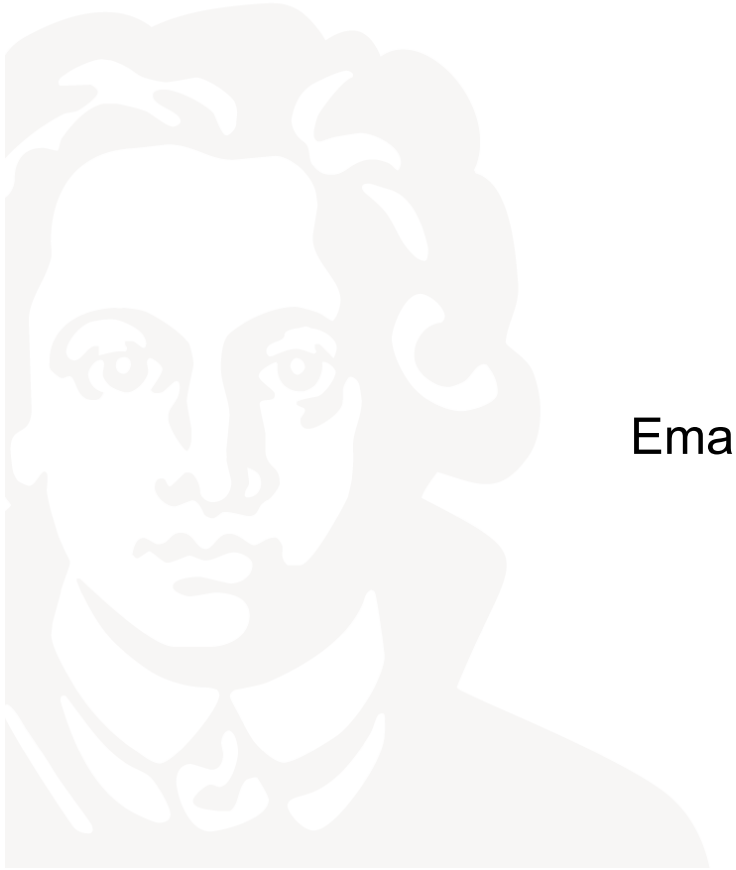
Conclusion

- Privacy-ABC technologies are a crypto innovation that need to be better understood
- The evaluation framework useful to compare different Privacy-ABC technologies
- Service providers can use the evaluations in order to
  - Decide which Privacy-ABC better fulfills their needs
  - Tune-up different properties / functionalities of particular Privacy-ABC technology to better meet the evaluation targets / goals, e.g. performance (efficiency)

- Challenges (and idea for future work):
  - Improving performance and availability of Privacy-ABC enabled infrastructures
    - Combination of different revocation mechanisms
  - Balancing trust and any-time access (mobility)
    - Credential storage on smart cards vs. cloud

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Thank you!



Email: Fatbardh.Veseli@m-chair.de
Twitter: @fatbardhi