Privacy engineering: positive sum or zero sum? Challenges of PETs for mobility

Dr. Fatbardh Veseli
Security Architect (Capgemini) / Senior Lecturer (Riinvest College)

Guest Lecture for „Mobile Business II: Application Design, Applications, Infrastructures and Security“

Goethe Universität Frankfurt am Main, 14 June 2020

Capgemini

Agenda

- Myself
- Motivation – Privacy issues in IdM
- Privacy by Design (PbD)
- Evaluation criteria for PETs
- Example PET: Privacy-enhanced attribute-based credentials (Privacy-ABC)
- Evaluation of Privacy-ABC technologies
- Use cases: Privacy-ABC technologies and smart city
- Example PET: Tor
- Conclusion

Myself

Dr. Fatbardh Veseli

Senior Cybersecurity Consultant
Local Business Security Manager
& Data Protection Champion

Languages: Albanian, English, German

Education & Competences

2020	*Dr. rer. nat*. (Doctor of natural sciences) – Computer Science, Faculty of Computer Science and Mathematics, Goethe University Frankfurt, Germany Thesis title: *A framework for evaluating privacy-enhancing attribute-based credential systems*
2011	*M.Sc. Information Security*, Faculty of Computer Science and Media, Gjovik University College, Norway
2010	*B.Sc. Mathematics – Computer Science*, Faculty of Mathematics and Natural Sciences, University of Prishtina, Kosovo
2009	*B.Sc. Economics – Management* & Informatics, Faculty of Economics, University of Prishtina, Kosovo

Certifications

- CISSP, TOGAF Certified, Prince2 Practitioner, SAFe 5 Agilist, ITIL v4, Certified Architect (L1), Professional Scrum Master (PSM) 1, Microsoft Certified: Azure Fundamentals (AZ900), ISO 27001 Lead Auditor

More than 13 years professional experience (research and industry)

- Technical / management roles in research and innovation projects
- Consultancy in cybersecurity in private and public sector in Germany
- Member and Rapporteur of the ENISA WG on Privacy Engineering
- Member of the WG on Cyber Security & Critical Infrastructure (Rep. Of Kosovo)
- More than 13 semesters teaching experience
  - *Information and communication security* (Master), Goethe University Frankfurt
  - *Mobile Business I: Technology, Markets, Platforms & Business Models,* Goethe University Frankfurt
  - *Mobile Business II: Application Design, Applications, Infrastructures and Security,* Goethe University Frankfurt
  - Supervised over 20 Master, Bachelor, and seminar theses
  - Data Security, Advanced Protocols and Network Security @Riinvest College, Kosovo

Which privacy enhancing technologies do you know of?

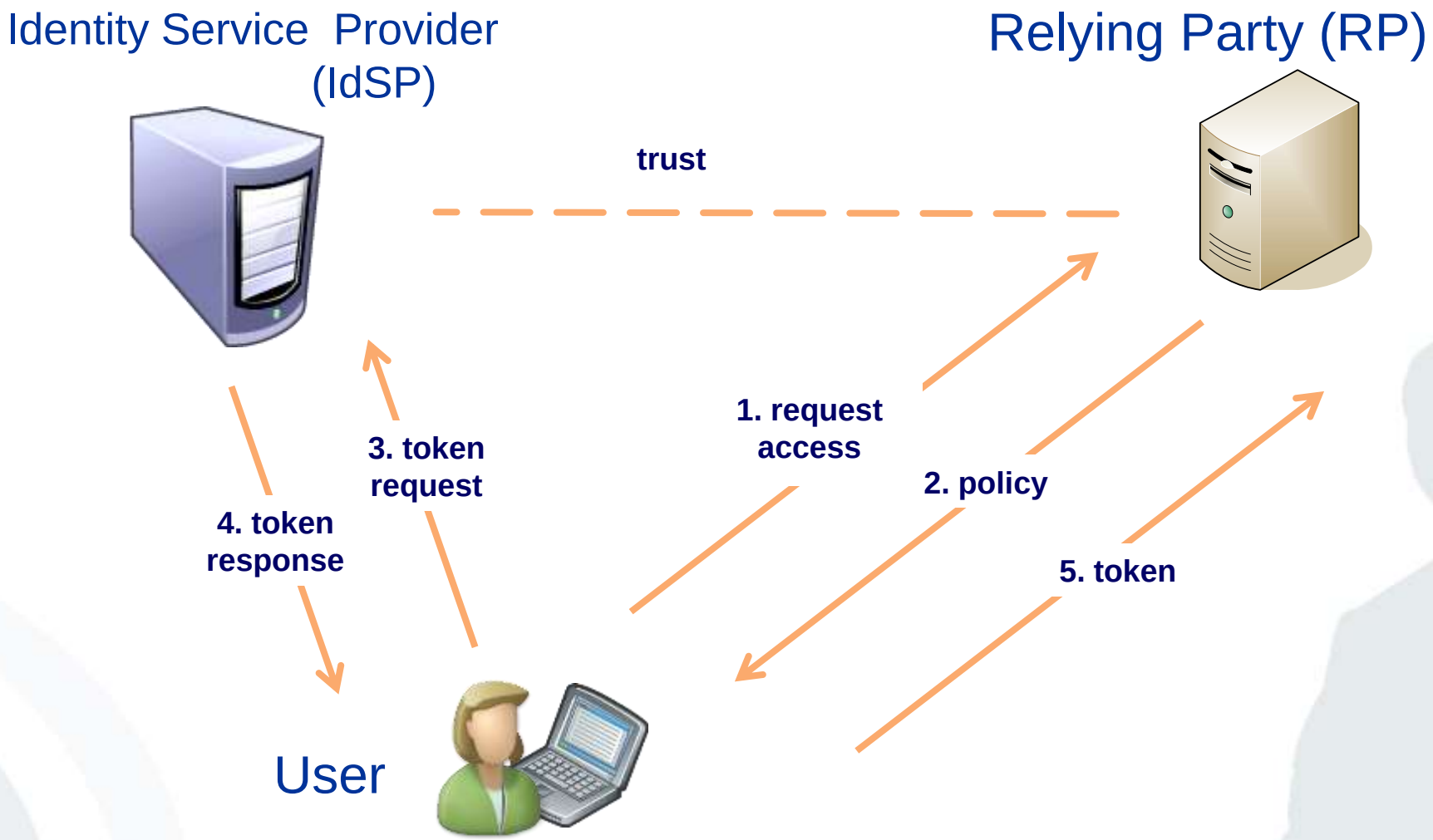
Which privacy enhancing technology do you use?

Motivation – Privacy issues in IdM

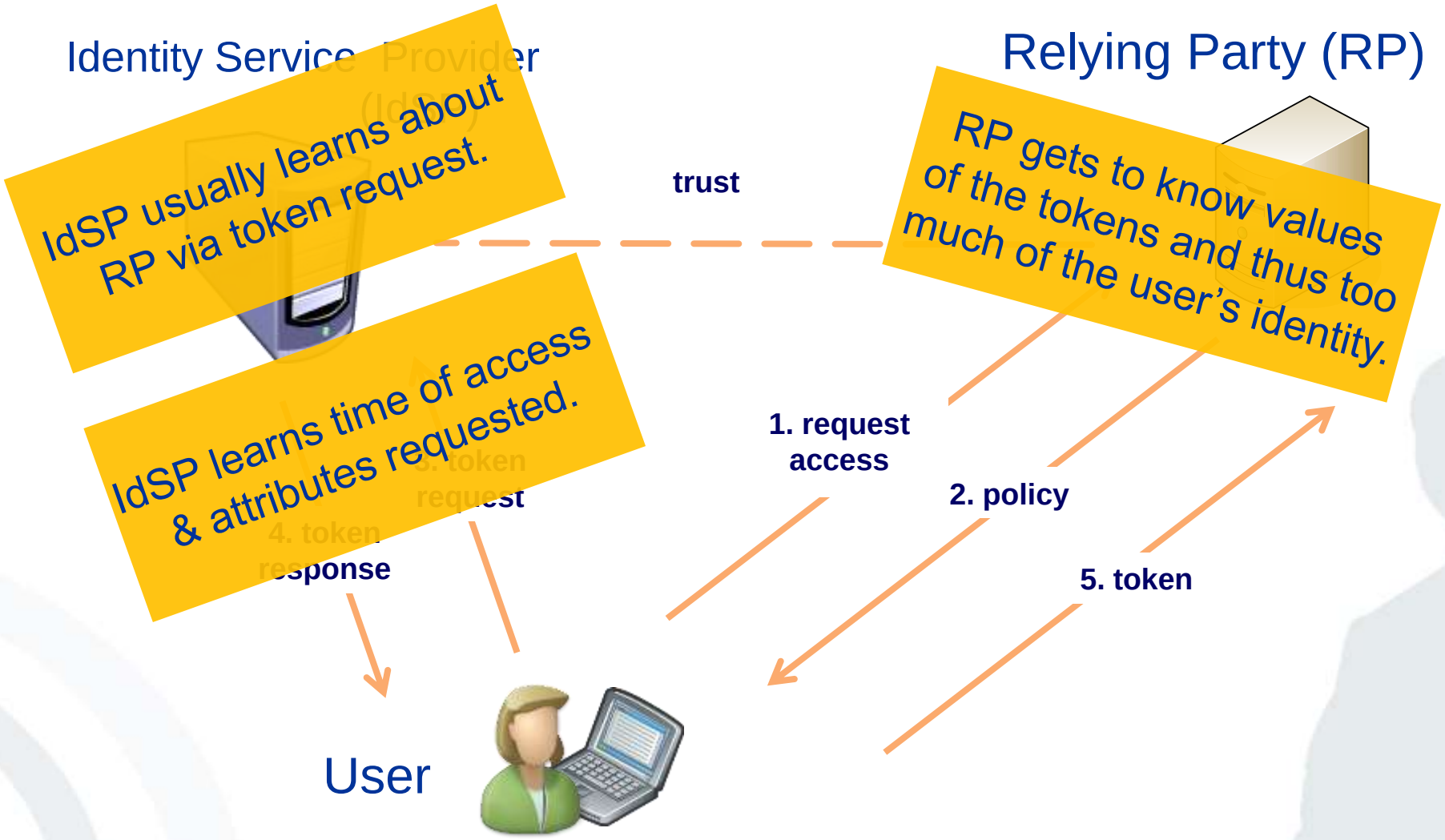
What do these tools have in common?

Source and Copyright: https://raw.githubusercontent.com/MichalSzorad/react-social-login-buttons/master/examples/simple/screenshot1.jpg

Overview of a typical federated IdM architecture



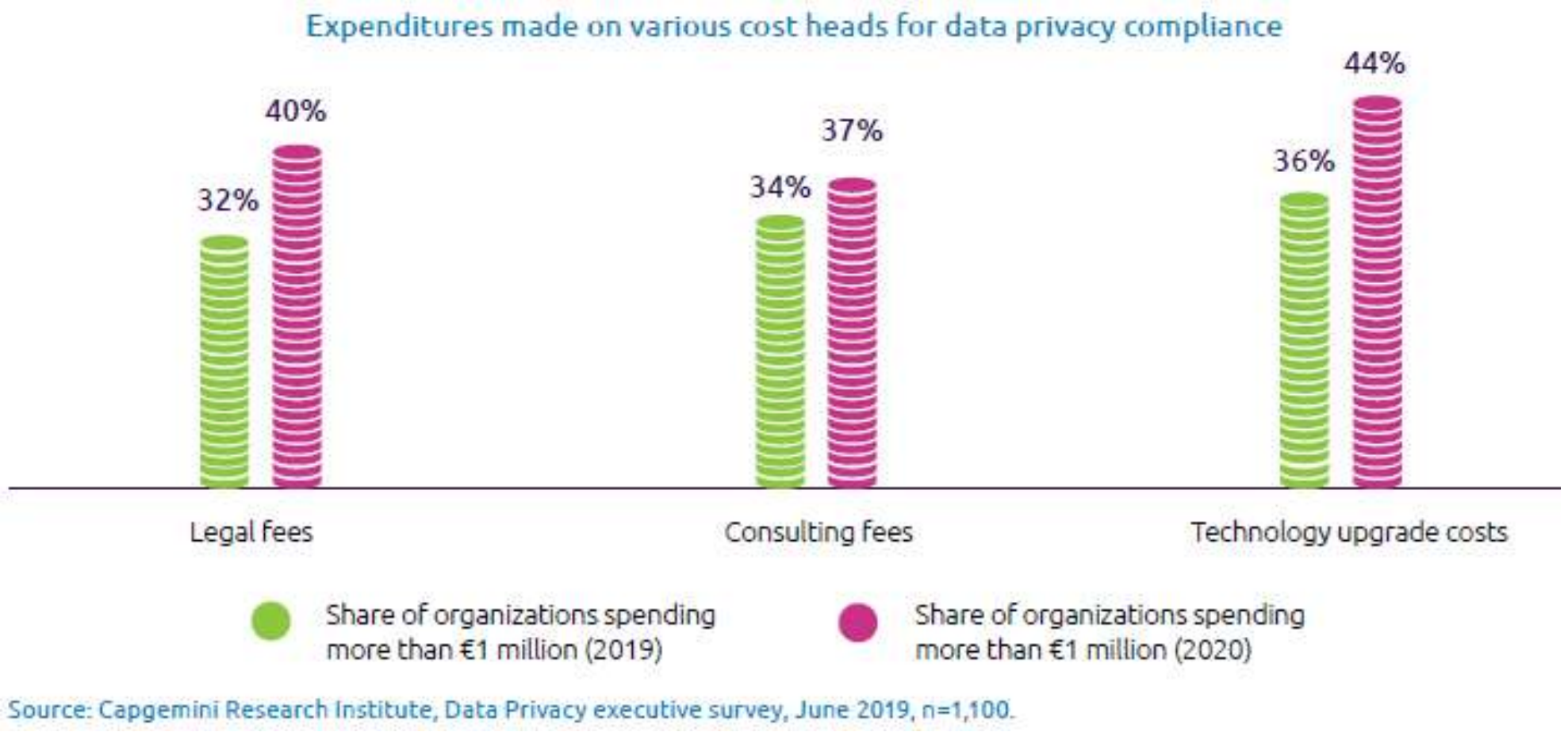
Privacy (and security) issues of typical federated IdM architectures



Privacy market and the GDPR

Global privacy market growth

Through 2022, privacy-driven spending on compliance tooling will rise to **$8 billion** worldwide. (Gartner, 2020)



Companies perceive benefit from GDPR

Source: Capgemini Research Institute, Data Privacy executive survey, June 2019, n=1,039. GDPR Executive Survey, March–April 2018, n=1,000.

Positive impacts of GDPR on companies

Executives were asked to rate these dimensions on a scale of 1–7, where 1=decreased significantly and 7=increased significantly

Source: Capgemini Research Institute, Data Privacy executive survey, June 2019, n=1,039.

Complexity is seen as a barrier for compliance

Source: Capgemini Research Institute, Data Privacy executive survey, June 2019, n=1,039. GDPR Executive Survey, March–April 2018, n=1,000.

Recommendations for improving GDPR-compliance

Study by Capgemini Research Institute: *Championing Data Protection and Privacy*, a source of competitive advantage in the digital century, 2019

1

Privacy by Design

Embed data protection and privacy principles in the organizational culture

2

Privacy enhancing technologies

Assess how new data anonymization techniques and technologies can expand your data-sharing opportunities

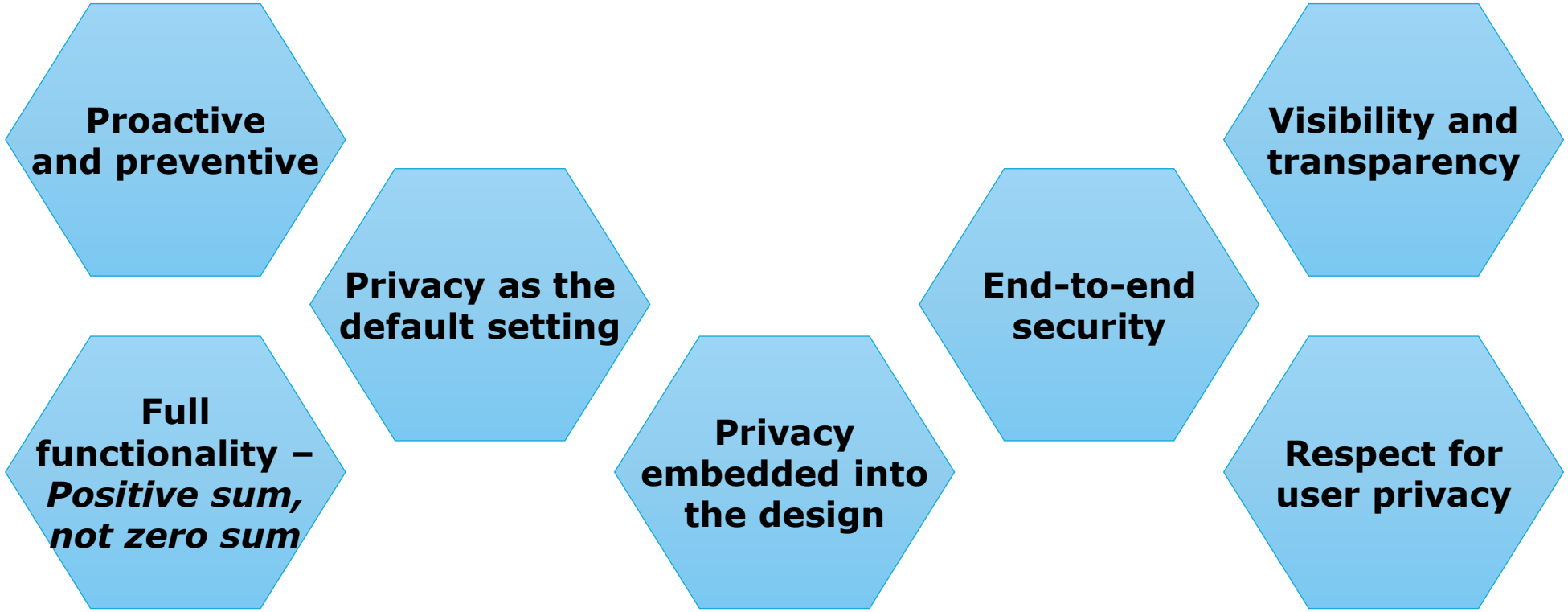
3

Privacy Impact Assessment

Establish and integrate governance, risk, and compliance (iGRC) to build robust protection and privacy capability

Privacy by Design (PbD)

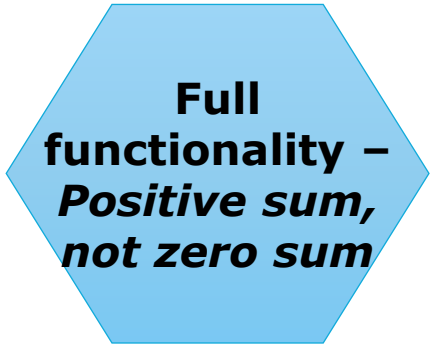
Ann Cavoukian's "privacy-by-design" principles



Ann Cavoukian, "7 Foundational Principles of Privacy by Design", https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

Full functionality: Positive sum, not zero sum

- "Privacy by Design seeks to accommodate all legitimate interests and objectives
  - in a positive-sum "win-win" manner,
  - not through a dated, zero-sum approach, where unnecessary trade-offs are made.
- Privacy by Design avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both."



Ann Cavoukian, "7 Foundational Principles of Privacy by Design", https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

GDPR – Data protection by design (Art. 25)

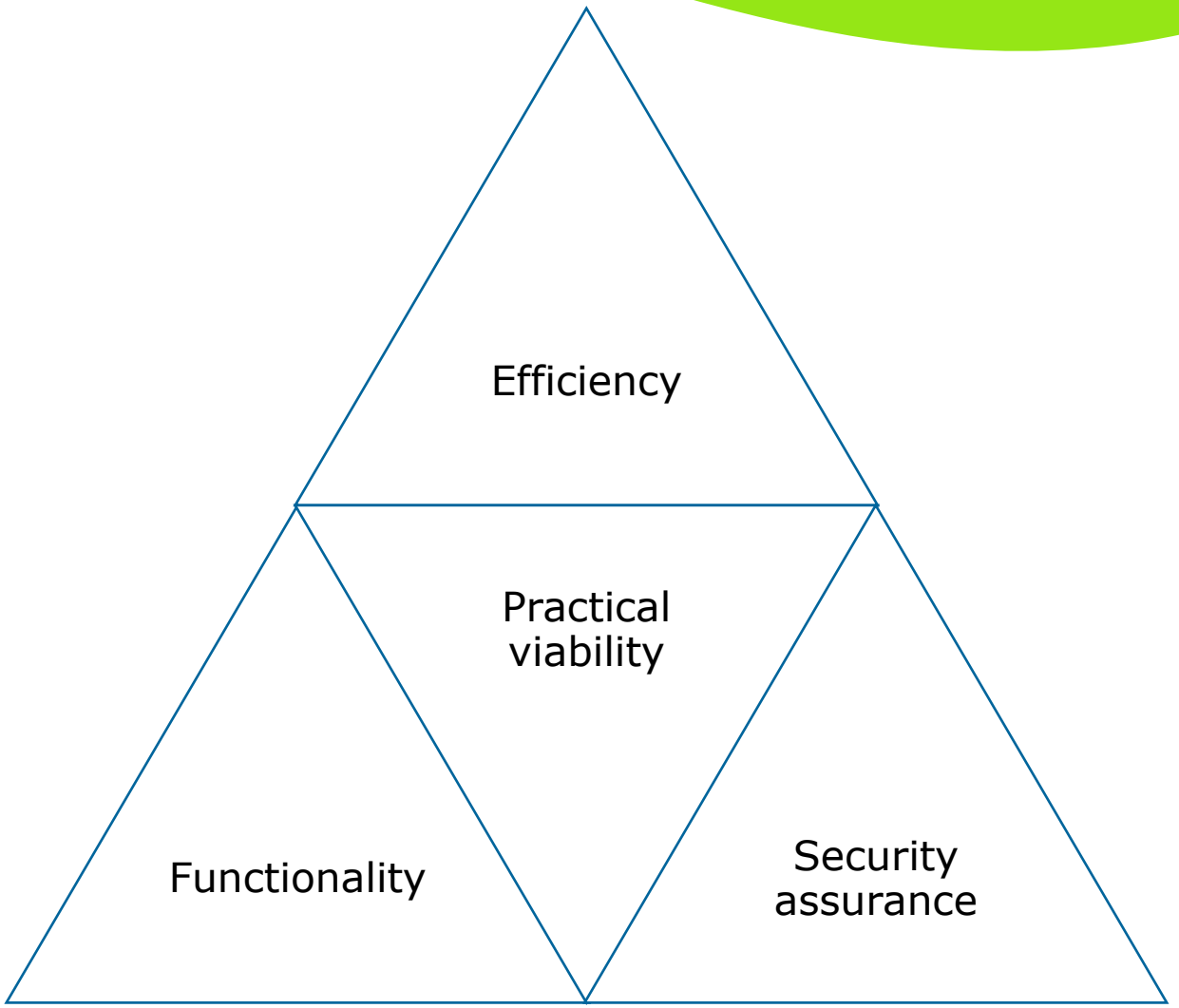
- *„…implement appropriate technical and organisational measures, such as **pseudonymisation**, which are designed to implement data-protection principles, such as **data minimization**"*

Privacy by Design – Challenges

- **Concrete implementation remains unclear** at the present moment.
- "**Limitations of awareness** and **understanding** of *developers and data controllers* as well as **lacking tools** to realise privacy by design" (ENISA, 2014)
- Privacy perceived as "an ***abstract problem***, *not* an *immediate* problem, *not a problem at all* (*firewalls and cryptography would take care of it*), *not their problem* (one for politicians, lawmakers, or society), or simply ***not part of the project deliverables***." (Lahlou *et al*., 2005)

Evaluation criteria for PETs

Competing goals?
Evaluation criteria for PETs



Latency as an aspect of efficiency

- Latency and acceptance
  - How long are Web users willing to wait?
  - Answer: ~2s

  (Nah, F. (2004), A study on tolerable waiting time: how long are Web users willing to wait? Behaviour & Information Technology)

- Time latency => Intention to re-use a service

  ("Customer evaluation of Internet-based service quality and intention to re-use Internet-based services", Sohn, Chang Soo, Southern Illinois University at Carbondale ProQuest Dissertations Publishing, 2000)

How long is adequate?

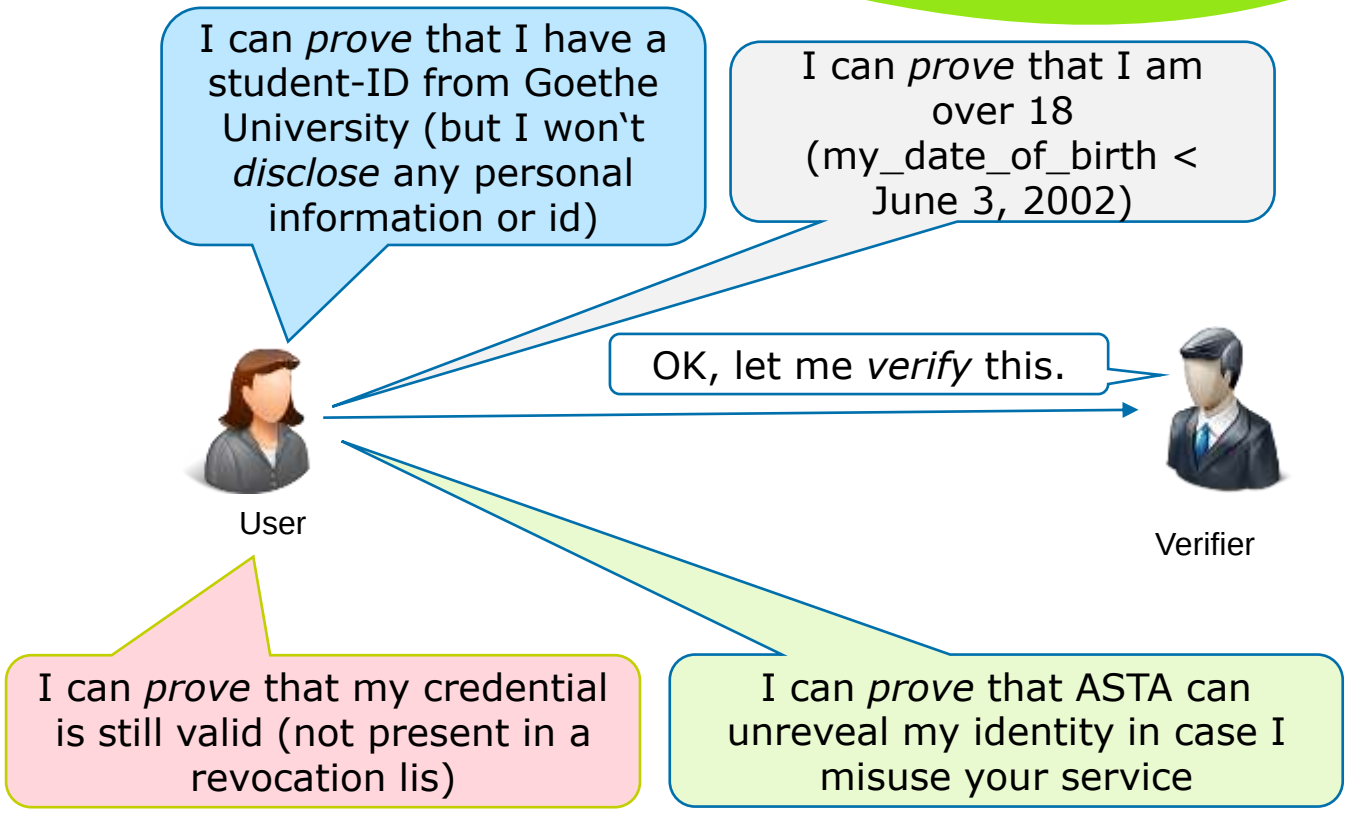
Author	Critical Latency Thresholds (s)	Description	Year	Source Classification
Tolia [32]	1	Thin client response time—annoying	2006	Journal
Nah [33]	2	For simple information retrieval tasks	2004	Journal
Tolia [32]	2	Thin client response time—unacceptable	2006	Journal
Tolia [32]	5	Thin client response time—unusable	2006	Journal
Accounting-WEB [34]	8	Optimal web page waiting time	2000	Practical advise
Bhatti [35]	8.57	Average tolerable delay (but high standard deviation of 5.85)	2000	Conference
Selvidge [36]	10	Tolerable delay by users	1999	Practical advise
Nielson [28]	10	Optimal web page waiting time	1999	Practical advise
Galetta [37]	12	Start of significant decrease in user satisfaction	2004	Journal
Nah [33]	15	Free user from physical and mental captivity	2004	Journal
Ramsay [38]	41	Suggestion as cut-off for long delays	1998	Journal

(Müller *et al.,* Distributed Performance Measurement and Usability Assessment of the Tor Anonymization Network, May 2012, Future Internet 4(2):488-513, DOI:10.3390/fi4020488)

Example PET: Privacy-enhanced attribute-based credentials (Privacy-ABC)

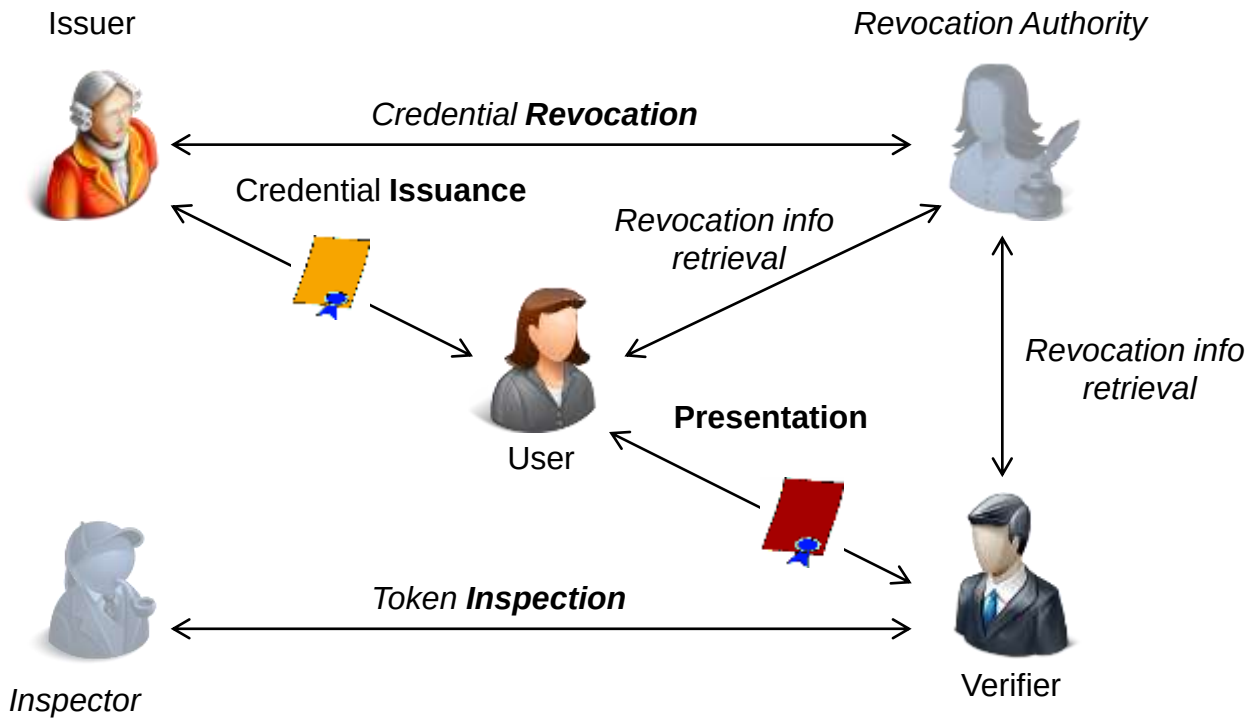
Privacy-enhanced attribute-based credentials (Privacy-ABCs)

- Identity attributes signed by a trusted entity (authenticity)
- Pseudonymous, direct authentication
- Long-lived credentials
- Predicate proofs
- Prove non-revocation
- Inspection



Privacy-ABC system architecture

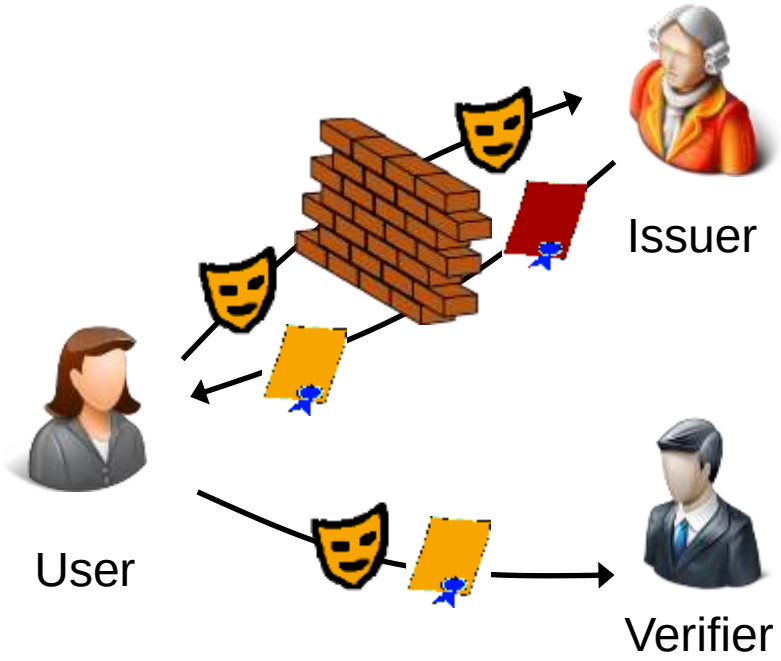
Entities and their interactions



Based on Bichsel *et al.* (2014)

Examples of Privacy-ABC technologies

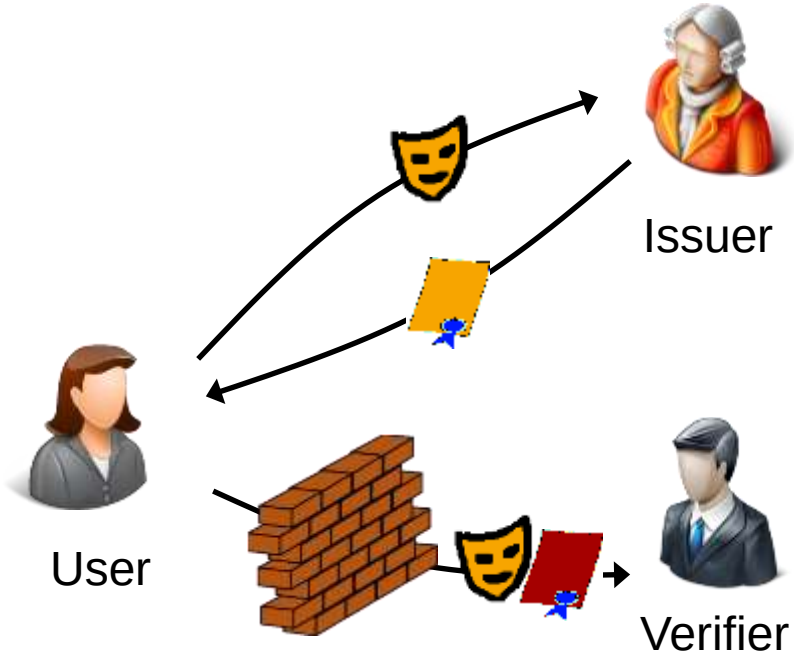
Blind Signatures



U-Prove

Brands, Paquin et al.
Discrete Logs, RSA,..

Zero-Knowledge Proofs



Idemix (Identity Mixer)

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

Privacy features

Minimal disclosure

(zero-knowledge)

Selective disclosure
(by design)

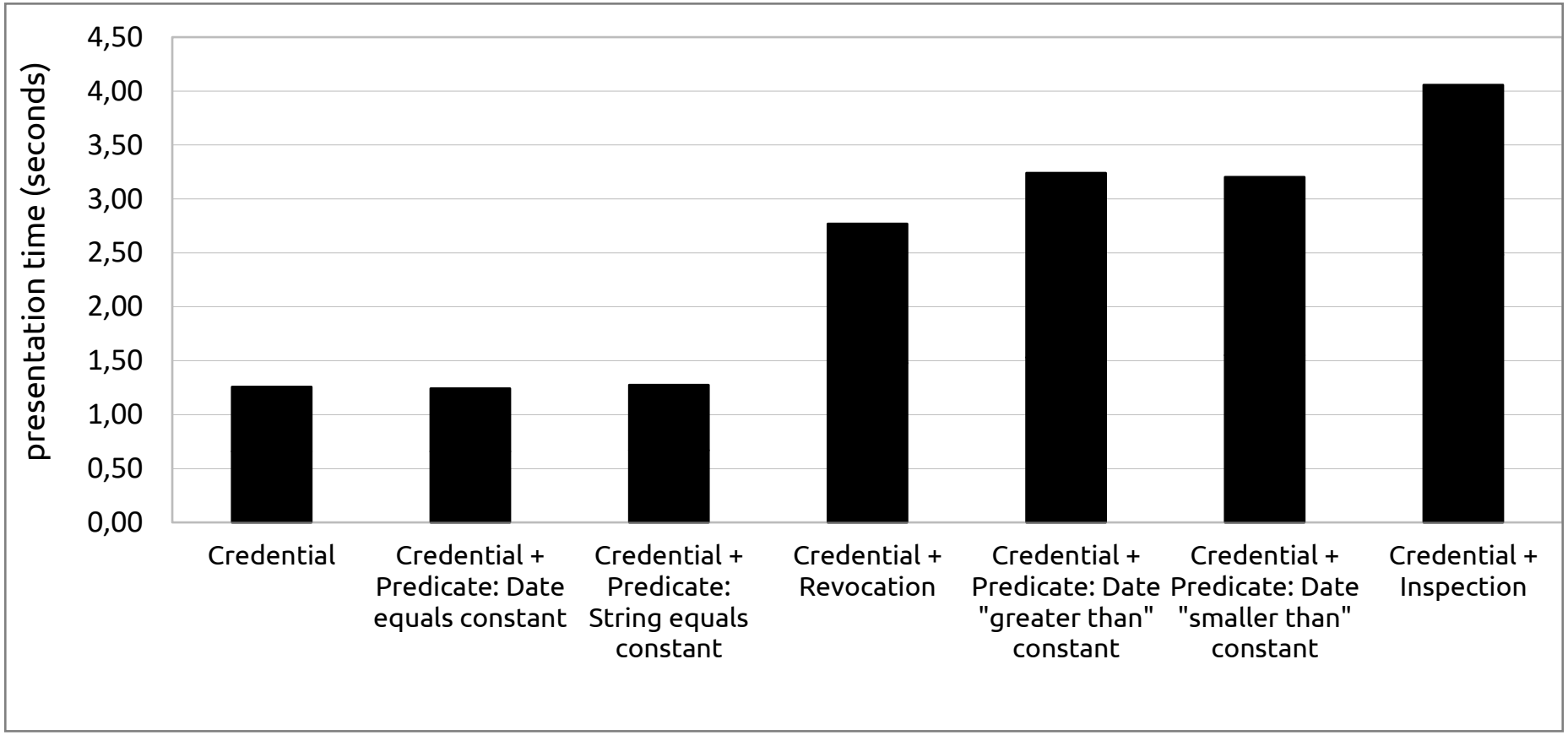
Untraceability of
presentation to issuance

Unlinkability between
different different
presentations

Pseudonymous authentication

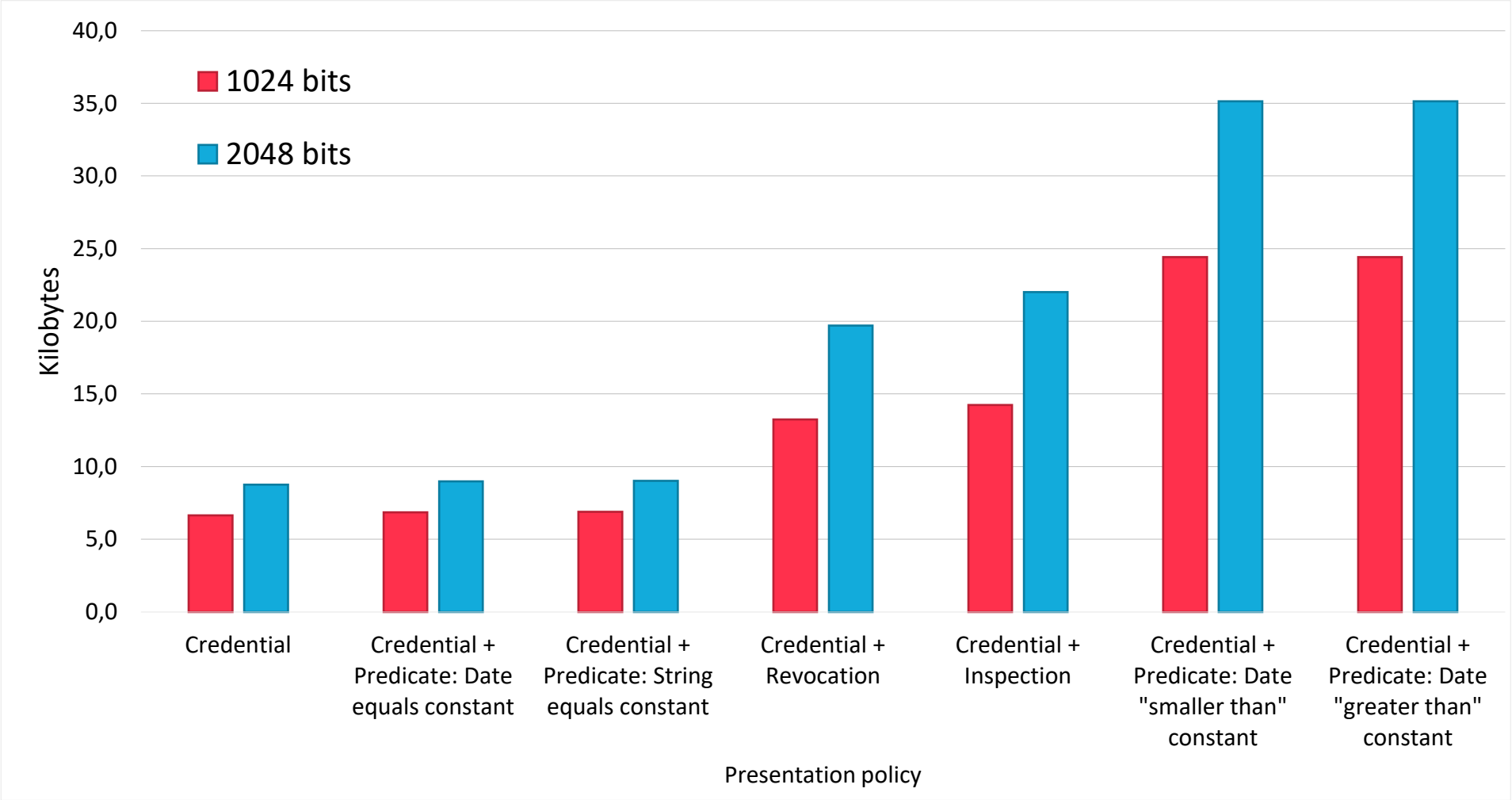
Evaluation of Privacy-ABC technologies

Privacy-ABC technology
Functionality vs. Time Efficiency



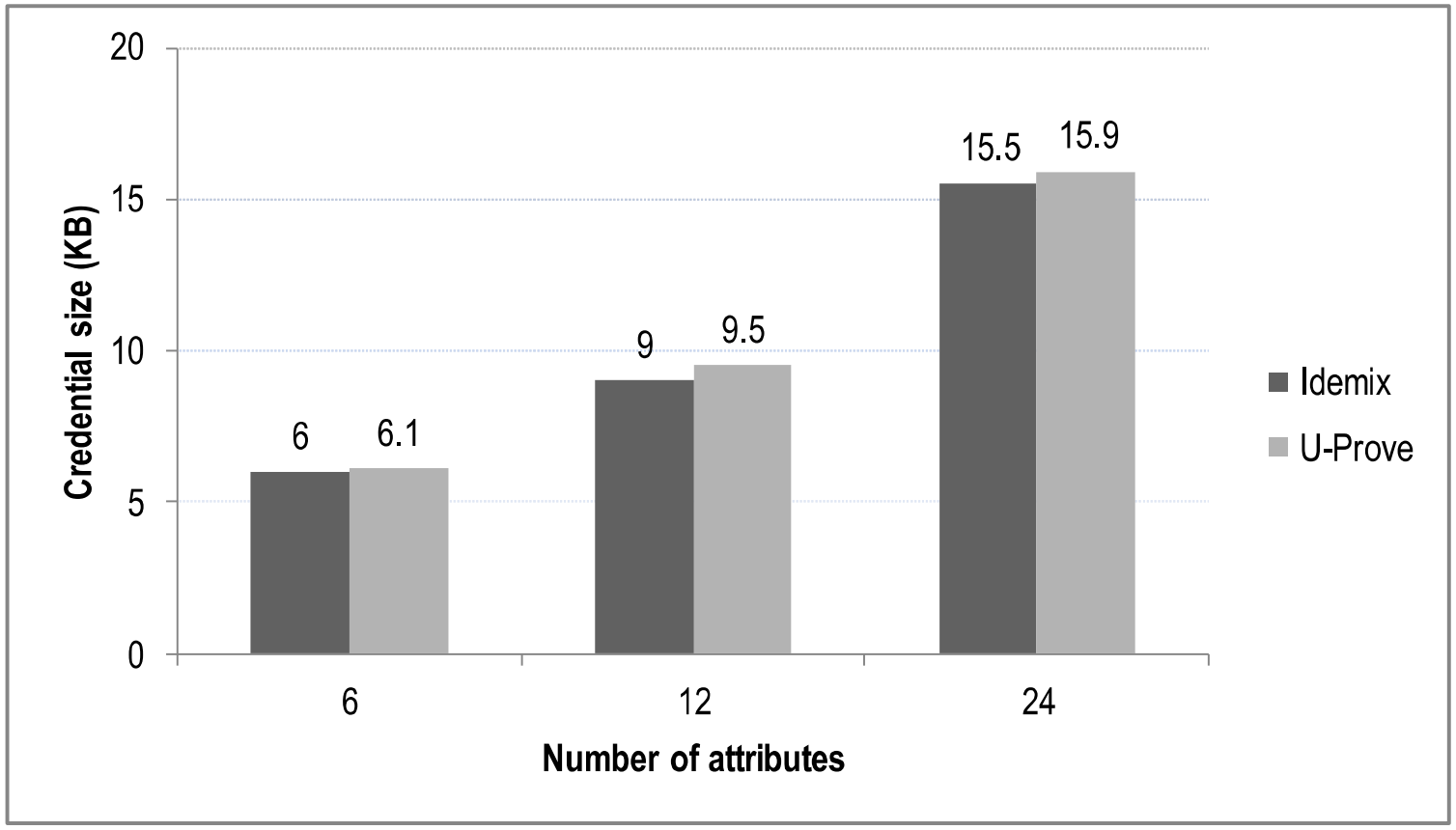
(Idemix, 1024 bits)

Privacy-ABC technology
Functionality vs. Space Efficiency (token sizes)



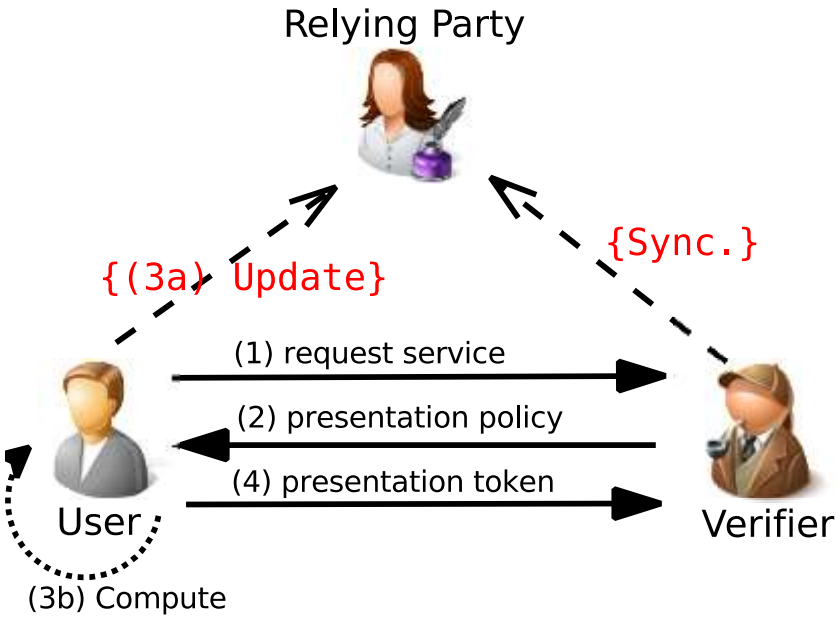
**Results shown here for Idemix. Impact identical for U-Prove.*

Privacy-ABC technology
Number of attributes vs. Space Efficiency (credential sizes)



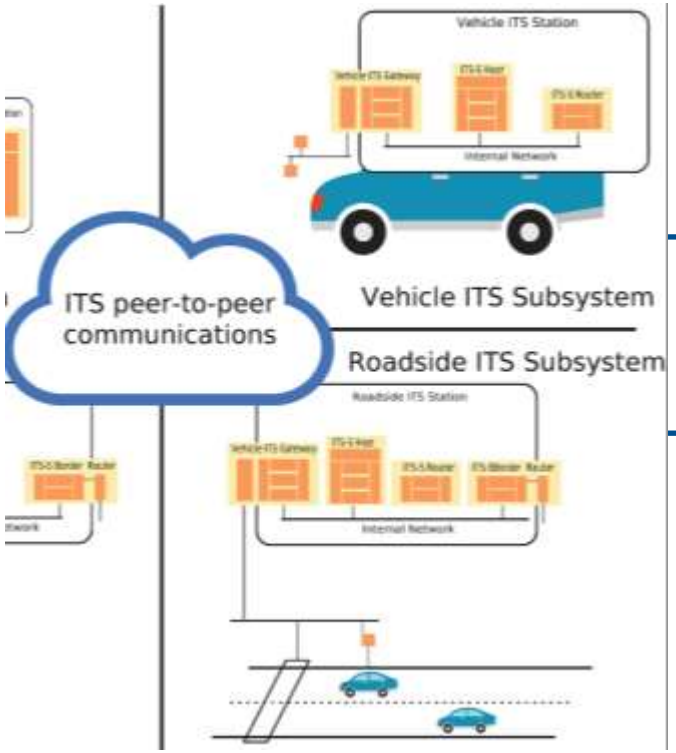
Challenges for Privacy-ABC technologies

- Changes in the identity infrastructure of service providers
- Data-centric business models
- Functionality at the cost of Efficiency
- Direct, non-interactive revocation
- Mobility / Practical viability: smart cards
  - *Do all my credentials fit in one smart cards?*
  - *Can my smart card efficiently make the required proof?*
  - *Can I access my credentials from all my devices (cloud)?*
  - *How long will it take for me to log in with this technology?*



Use cases: Privacy-ABC technologies and smart city

Mobility: Privacy-ABC technologies for Intelligent Transport Systems (ITS) in a smart city



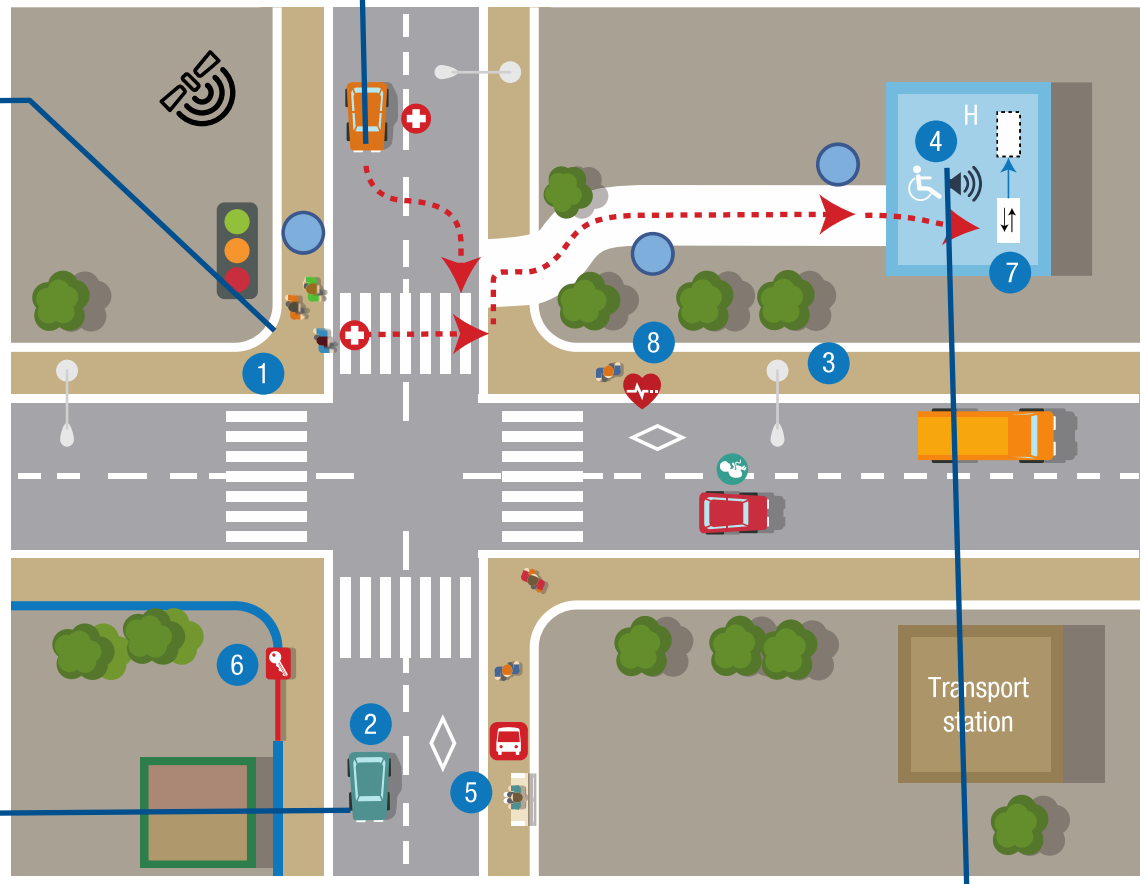
On-Board Units (OBUs) – mounted in vehicle

Road-Side Units (RSUs) – acting as interceptors / sensors

Use cases set 1 - Provision of adapted services

Energy: Adaptive lightning
(e.g. increase for PRV)

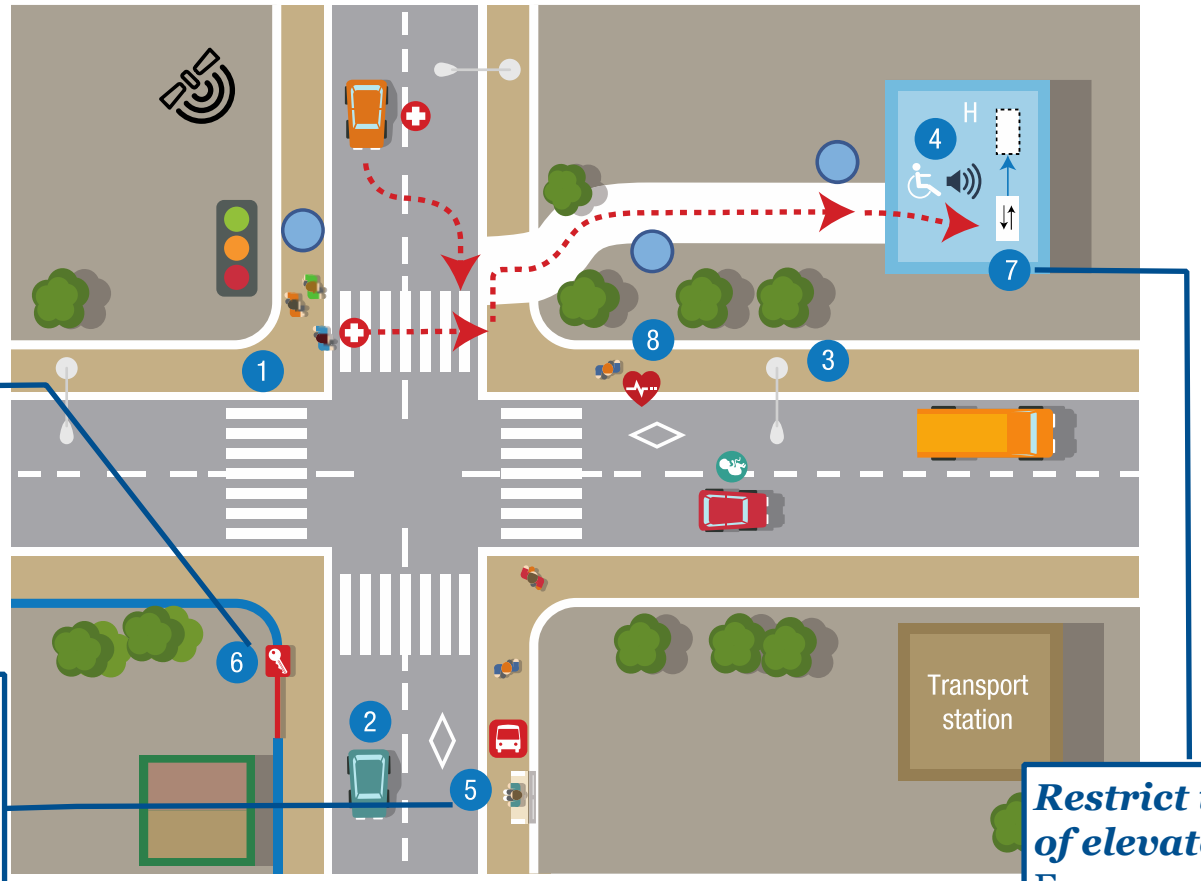
Mobility: Adaptive pedestrian crossing time
- People crossing with children (PCC)
- People with reduced mobility (PRM)
- People with reduced vision / auditory (PRV / PRA)



Mobility: Adaptive directions
-PRM, PRV, PCC or Persons with Cognitive Problems -(PCP): avoid huge crowds, e.g. stadiums during matches

Accessability: Adaptive on-screen text size
(e.g. in the elevator, increase for PRA)

Use cases set 2 – Clearance to use services



Conditional access to residential area

Allow driving on the bus lane

- Pregnant Woman (PW)
- Urgent Assistance Professionals (UAP)

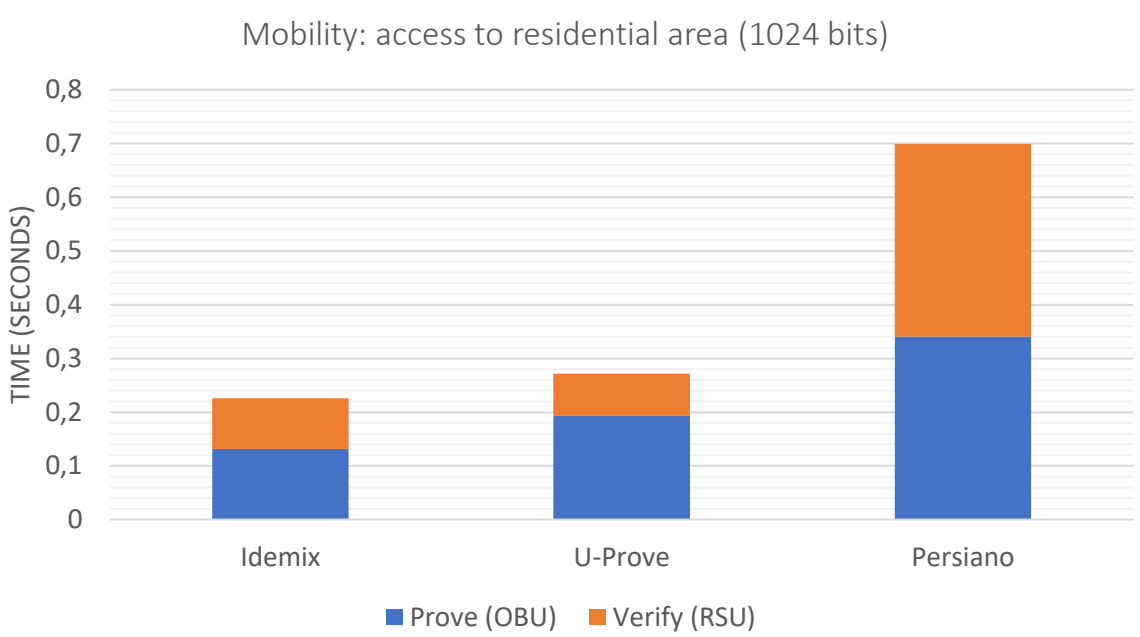
Restrict the use of elevator

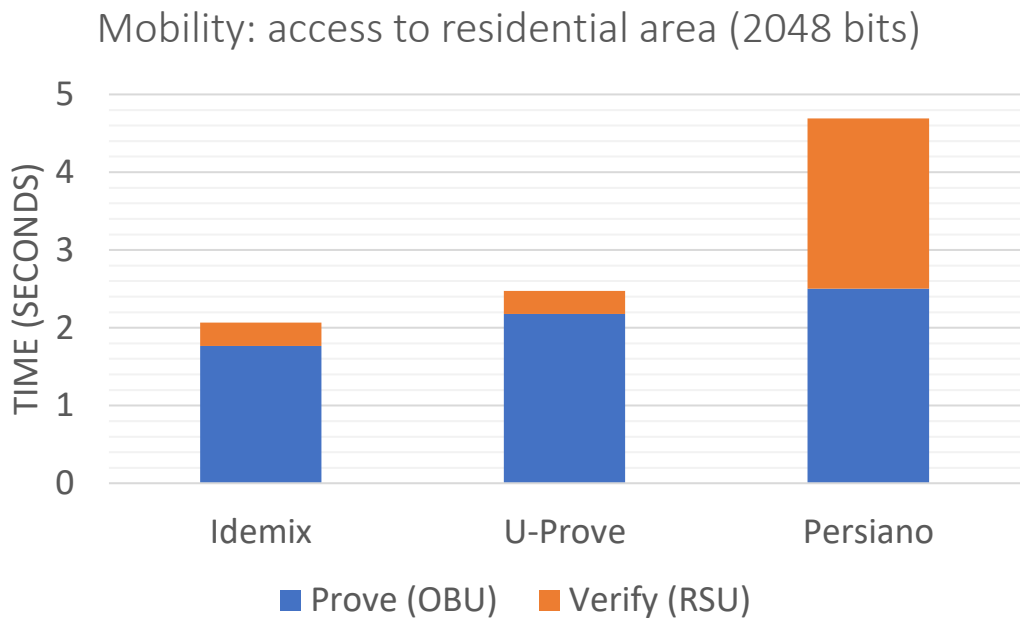
For persons with certain disease(s)

Challenge: Can the car complete the authentication in time?

- Considering a car traveling speed of 150 km/h (42 m/s), the vehicle will move a total of
  - 102m with U-Prove
  - 18.1m with Idemix
- **300 m** is considered as an effective communication range for DSRC (dedicated short-range communication)
- However, this is using a key size 1024 bits => not secure enough
- For higher security, 2048 bits, Persiano would become unfeasible (over 1 km)

Efficiency evaluation, key size and device





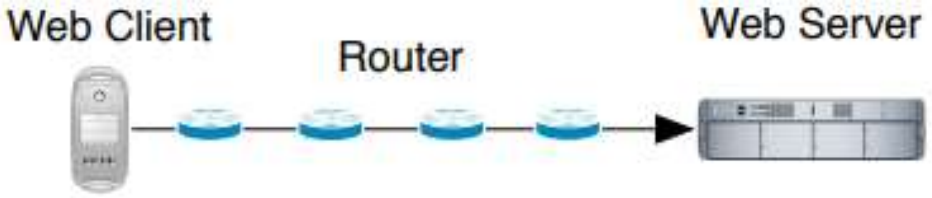
OBU = On-Board Unit

RSU = Road-Side Unit

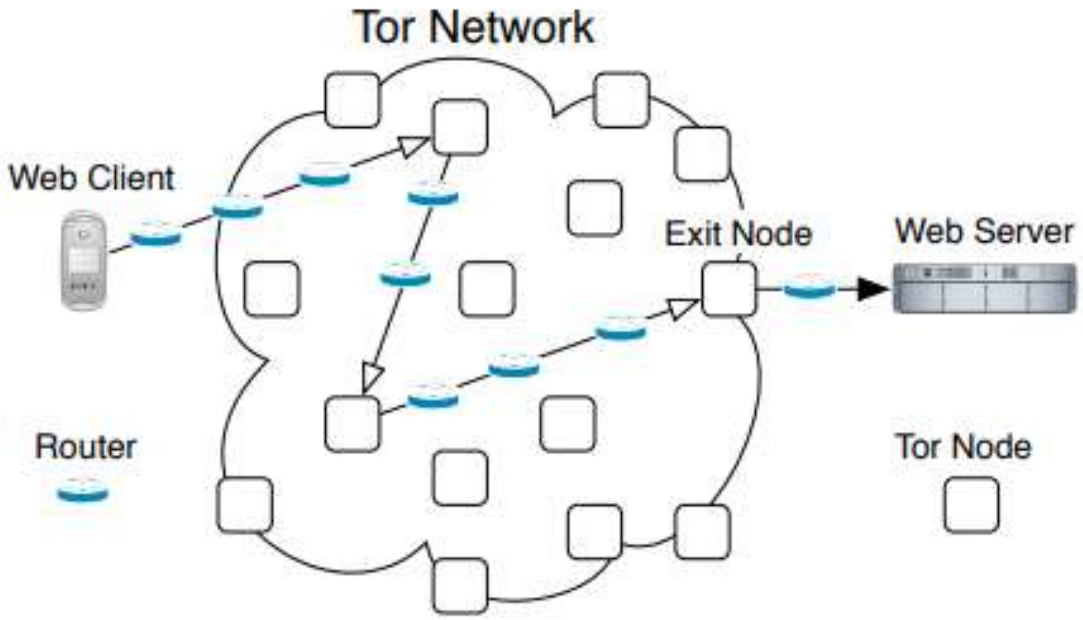
Example PET: Tor

Tor – with and without

Without using Tor („normal“ web usage)



Using Tor („anonymous“ mode)

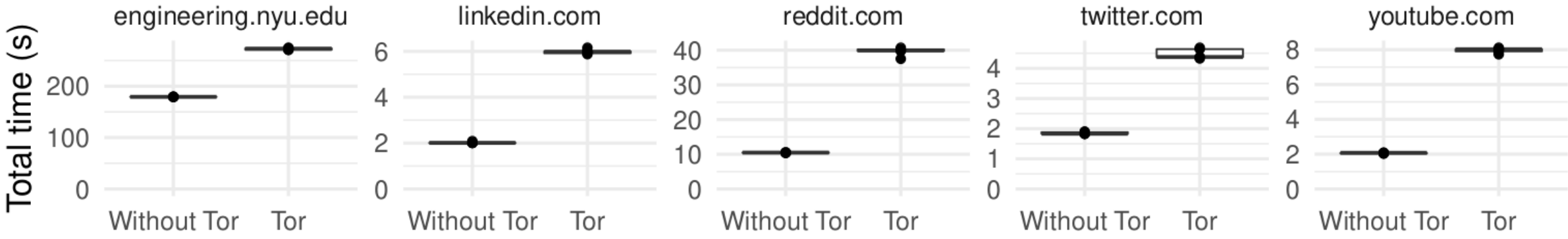


Tor and latency (1)

…”Internet anonymization software such as Tor is an important instrument to protect online privacy. However, due to the performance overhead caused by Tor, many Internet users refrain from using it. This causes a negative impact on the overall privacy provided by Tor, since it depends on the size of the user community and availability of shared resources.”

(Müller *et al.,* Distributed Performance Measurement and Usability Assessment of the Tor Anonymization Network, May 2012, Future Internet 4(2):488-513, DOI:10.3390/fi4020488)

Tor and Latency (2)



(Bintia Keita, Experimental evaluation of the impact of Tor latency on web browsing, January 2021 (Last accessed 13.6.2022))

What is in your view the reason for this challenge?

Conclusion

Conclusion and Outlook

- Privacy-enhanced technologies as an enabler for privacy-friendly information systems
  - PETs should be made less complex and consider user-acceptance
  - Practically viable, but with technical challenges for mobility
- Challenges
  - Latency important
  - practical viability (functionality, storage, etc.)
- Zero sum or positive sum?

Thank you!

Contact:
Dr. Fatbardh Veseli
Fatbardh.veseli@capgemini.com

Capgemini