The complexity of privacy: regulation, market, technology and mobility – chances and challenges

Dr. Fatbardh Veseli

fatbardh.veseli@capgemini.com

Guest Lecture Goethe Universität Frankfurt am Main

Course: **Mobile Business II: Application Design, Applications, Infrastructures and Security**

3 Juni 2020

Agenda

01 About

02 Background

03 Privacy regulation and market

04 Pseudonymization technologies for privacy - challenges for mobility

05 Conclusion and outlook

Agenda

01 About

02 Background

03 Privacy regulation and market

04 Pseudonymization technologies for privacy - challenges for mobility

05 Conclusion and outlook

Who am I?

2009

B.Sc. Management Information Systems
University of Prishtina,
Kosovo

2010

B.Sc. Mathematics – Computer Science
University of Prishtina,
Kosovo

2011

M.Sc. Information Security
Gjovik University College,
Norway

2020

Dr. rer. nat. / Informatik
Goethe University
Frankfurt, Germany

Education

2007 Corporate Client Advisor
ProCredit Bank Kosovo

2008 Software Developer
Komtel p.e. Kosovo

2010 Software Developer
Capesso, Norway

2011 Research Assistant
Security & privacy projects
Goethe University Frankfurt,
Germany

2017

Senior Cybersecurity Consultant
Capgemini

Work

Hobbies

Agenda

01 About

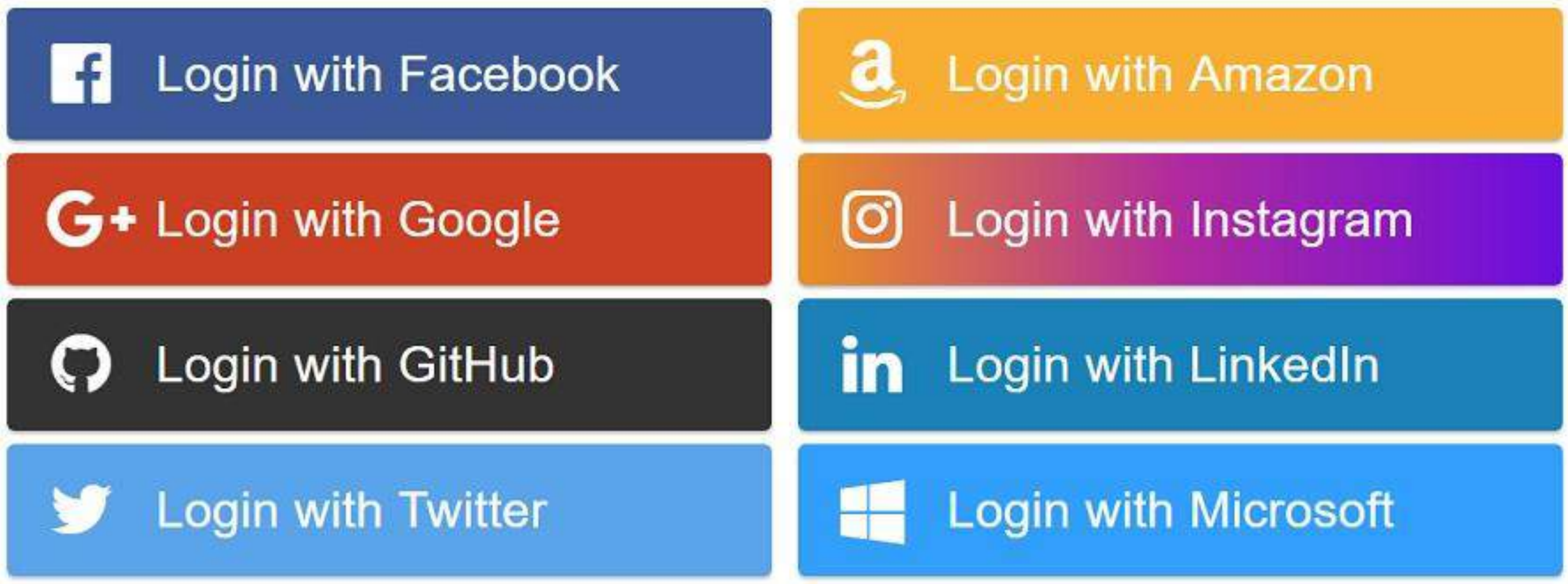
02 Background

03 Privacy regulation and market

04 Pseudonymization technologies for privacy - challenges for mobility

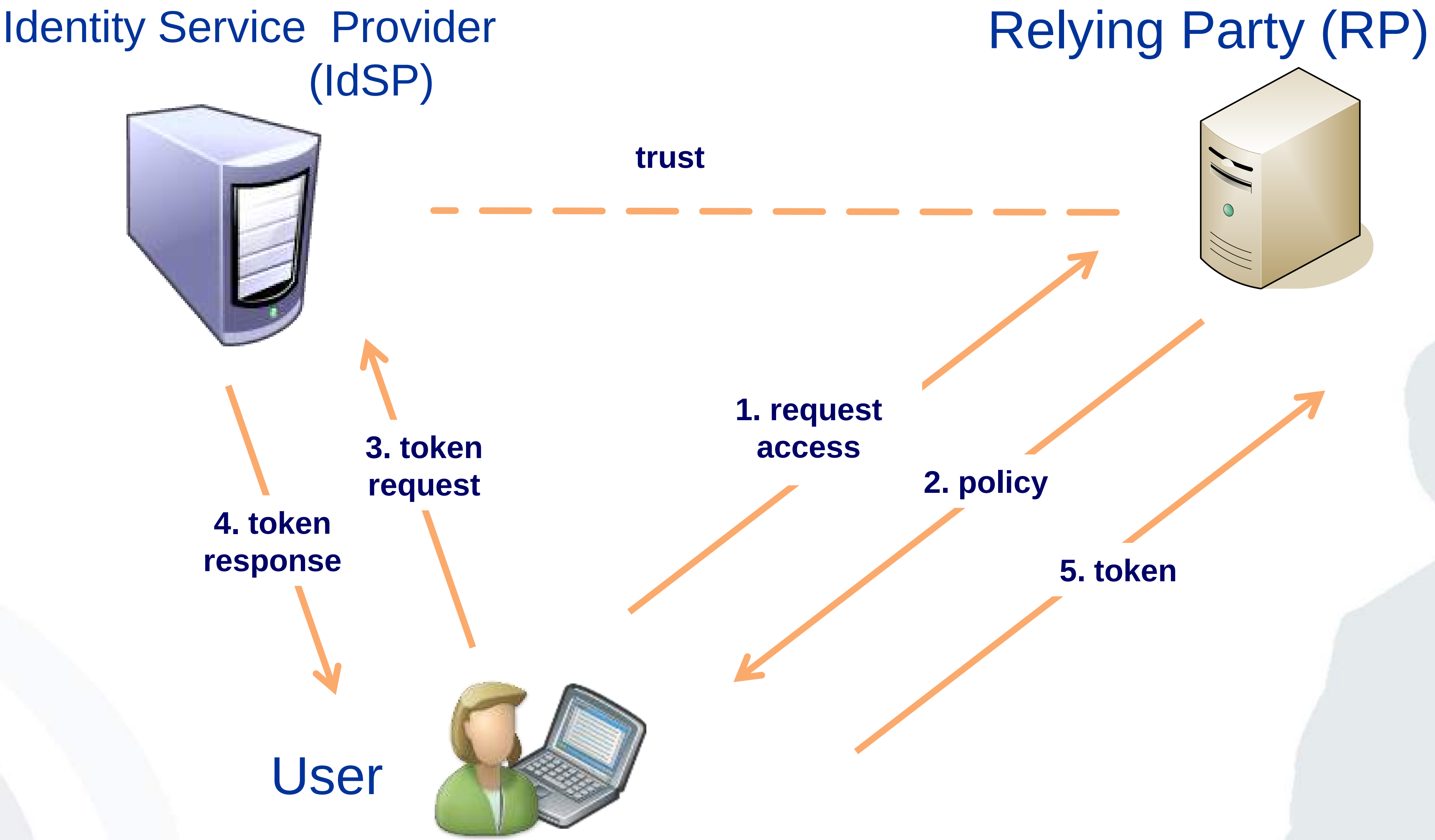
05 Conclusion and outlook

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



Identity Service Provider (IdSP)

Relying Party (RP)

trust

1. request access

2. policy

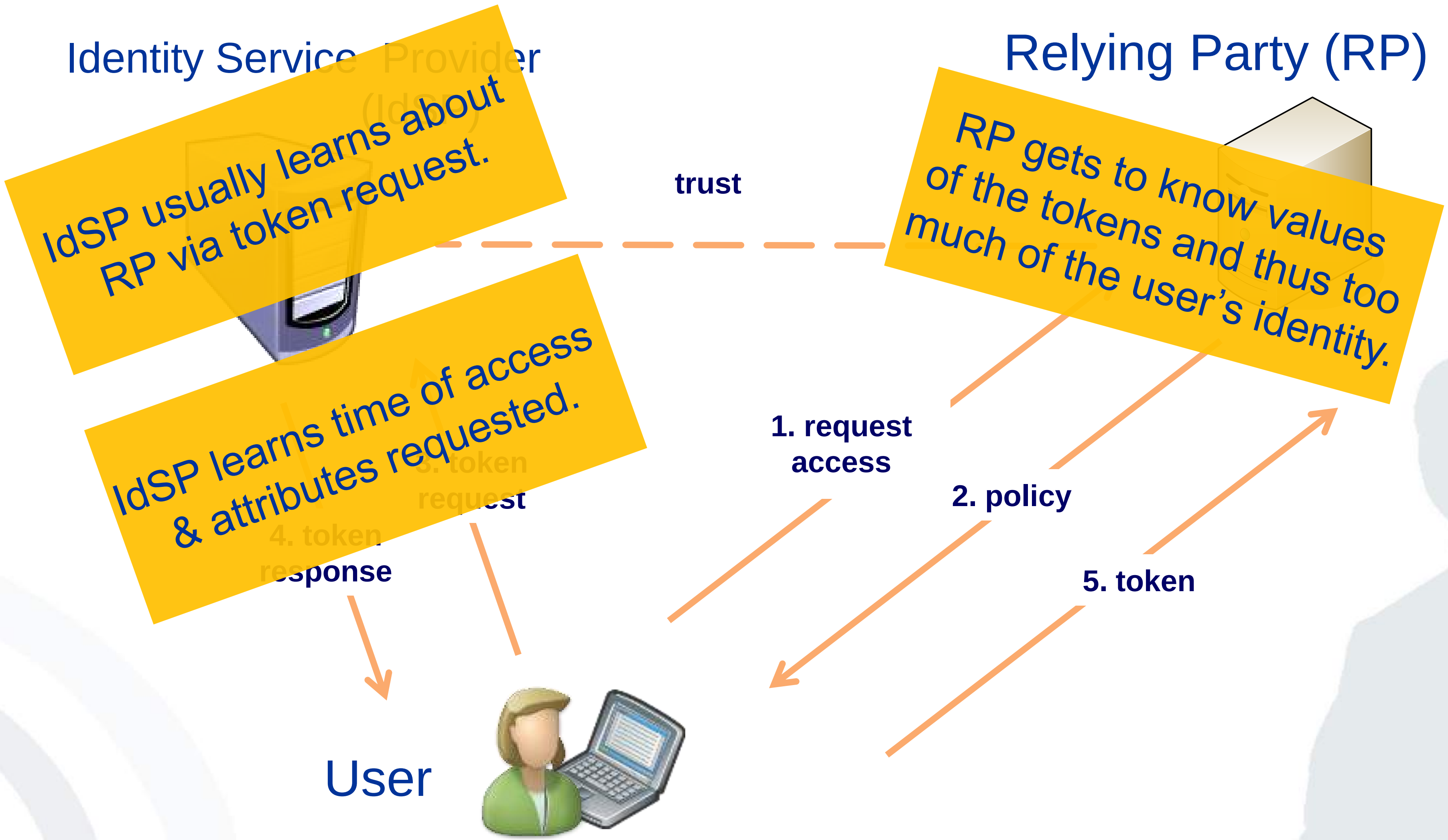
3. token request

4. token response

5. token

User

Privacy (and security) issues of typical federated IdM architectures



IdSP usually learns about RP via token request.

IdSP learns time of access & attributes requested.

RP gets to know values of the tokens and thus too much of the user's identity.

Cryptographic solutions for privacy

- **Blind signature** – A special form of a digital signature in which the content of a message is disguised (blinded) before it is signed
- **Zero-Knowledge Proof** – A protocol, by which you „convince“ (prove) another party that you know a certain secret, without revealing the secret itself or any information about it.
- **Committment** – a binding protocol by which one party „committs“ to a certain value, which can later be „revealed“ but not changed.
- **Accumulator** – cryptographic scheme that enables queries to prove that a certain element belongs or not in a list of „accumulated“ values without disclosing any of the elements (membership proof)
- **Range Proof** – protocols that enable to prove that a certain value lies within a given range or interval
- **Verifiable encryption** – a special form of encryption, where it is possible to verify that the encrypted value is indeed contained certain conditions, without revealing the encrypted value itself.

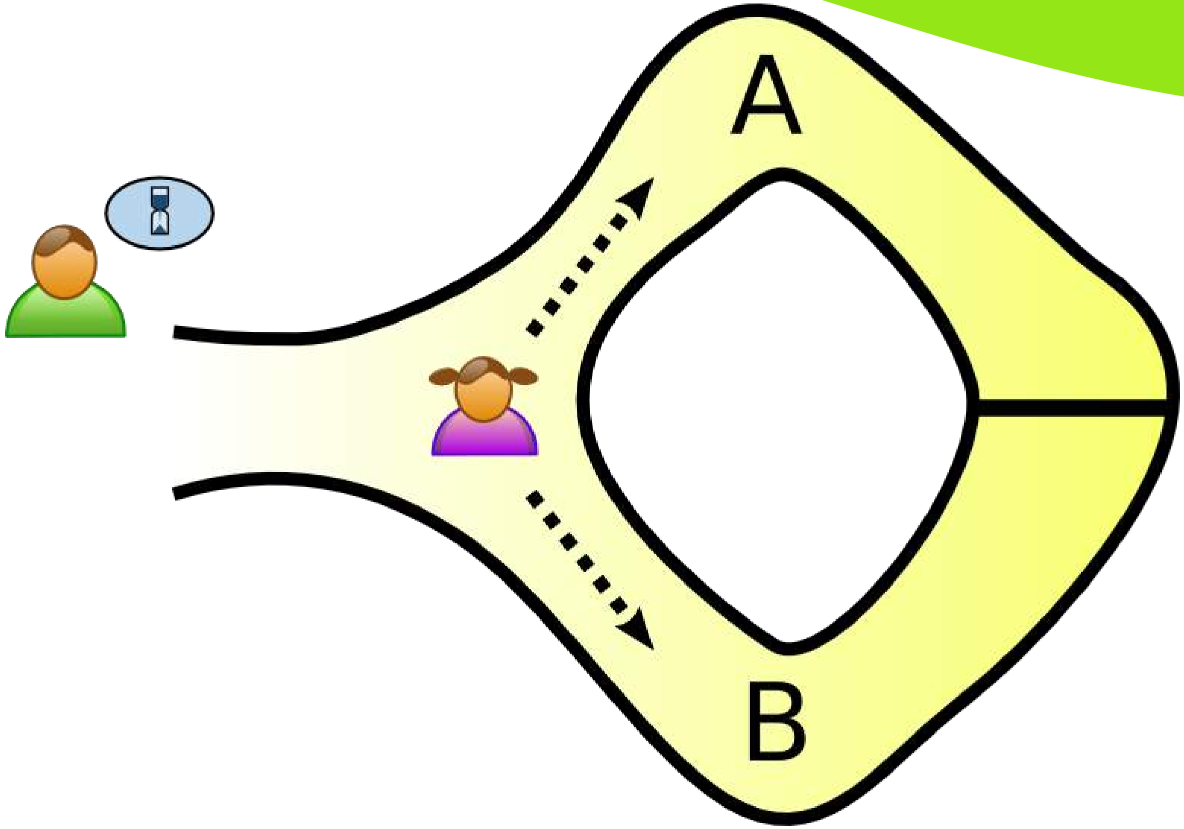
Source: Markus Rückert, https://www.yumpu.com/en/document/view/9256142/lattice-based-blind-signatures-markus-ruckert-technische-

HOW CAN PEGGY PROVE TO VICTOR THAT SHE KNOWS THE SECRET TO A PATH WITHOUT DISCLOSING THE SECRET?

1
1

Zero Knowledge Proofs with Peggy and Victor

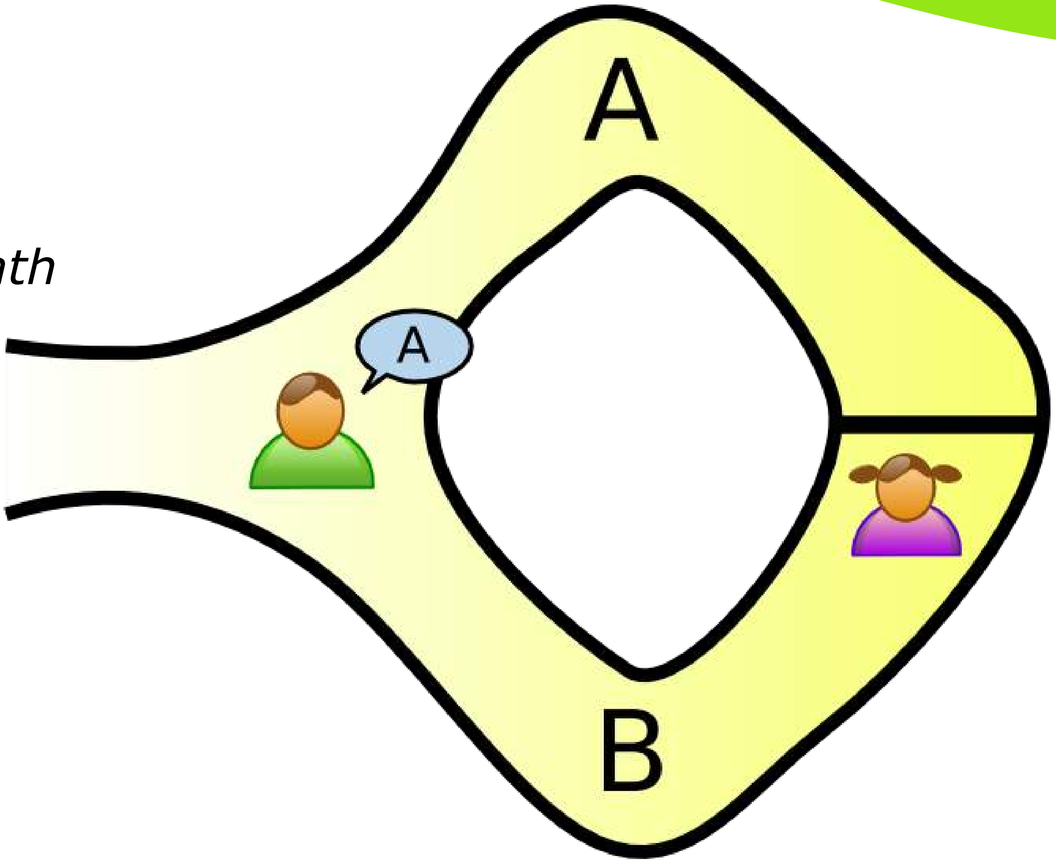
1) Peggy randomly takes either path A or B, while Victor waits outside



Source: Wikipedia, https://en.wikipedia.org/wiki/Zero-knowledge_proof

Zero Knowledge Proofs with Peggy and Victor

Victor chooses an exit path:
“Peggy, come out through path A!”



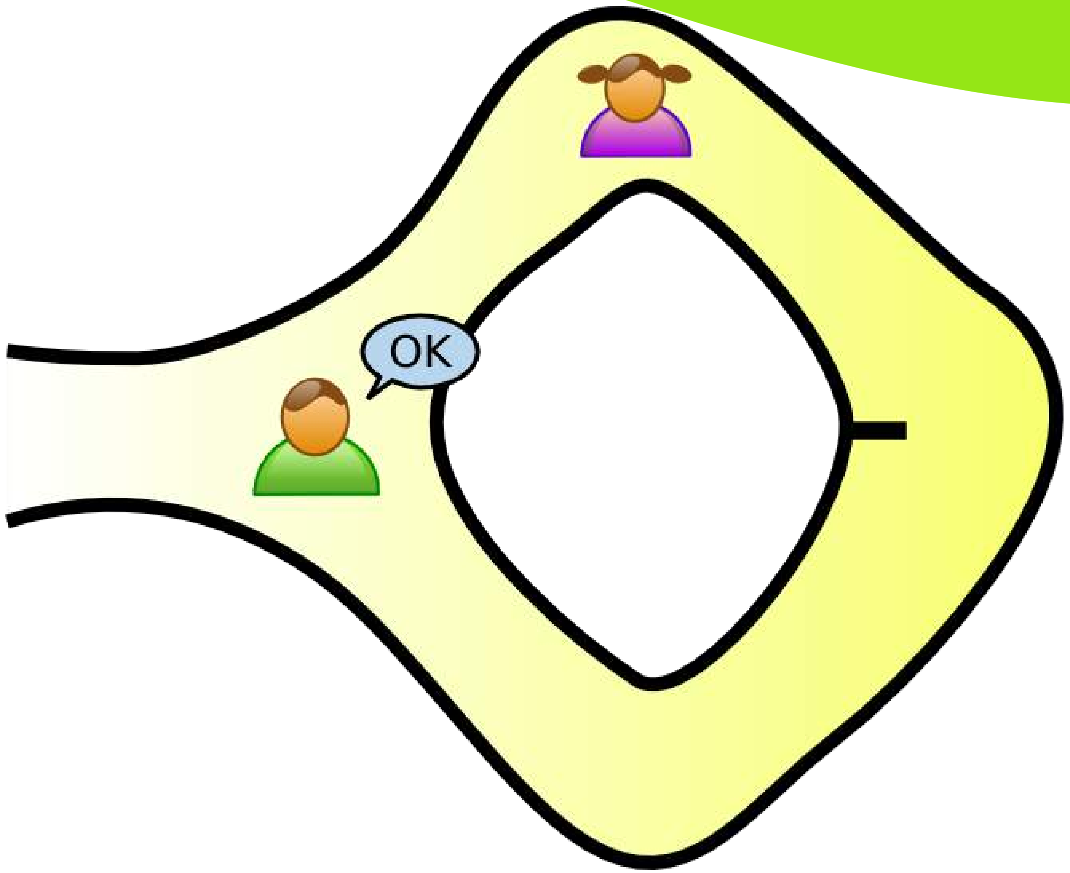
Source: Wikipedia, https://en.wikipedia.org/wiki/Zero-knowledge_proof

Zero Knowledge Proofs with Peggy and Victor

- Peggy reliably appears at the exit Victor names.

The probability of Peggy coming through the right path without knowing the secret is *1/2*

If we repeat this test, say 20 times, this probability becomes very small. Exactly: *~1/1.05 million*



Source: Wikipedia, https://en.wikipedia.org/wiki/Zero-knowledge_proof

Agenda

01 About

02 Background

03 Privacy regulation and market

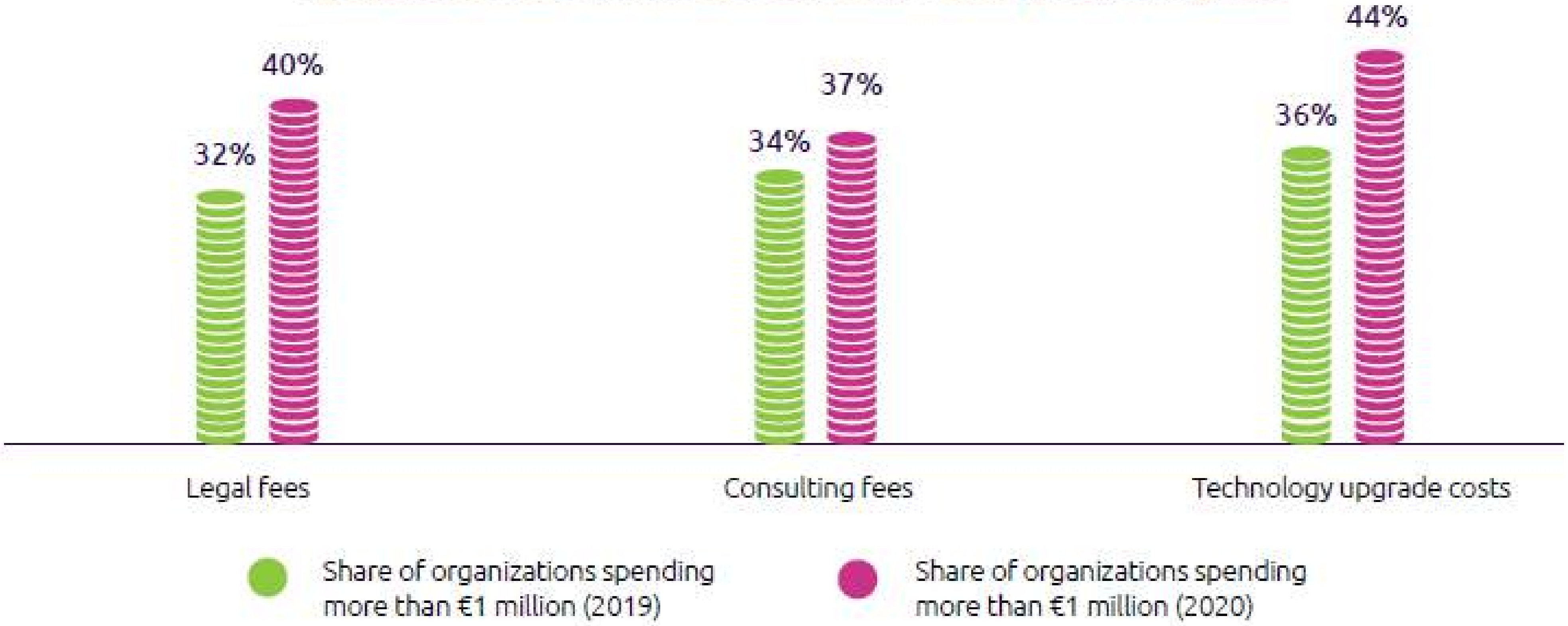
04 Pseudonymization technologies for privacy - challenges for mobility

05 Conclusion and outlook

Global privacy market growth

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

Expenditures made on various cost heads for data privacy compliance



Source: Capgemini Research Institute, Data Privacy executive survey, June 2019, n=1,100.

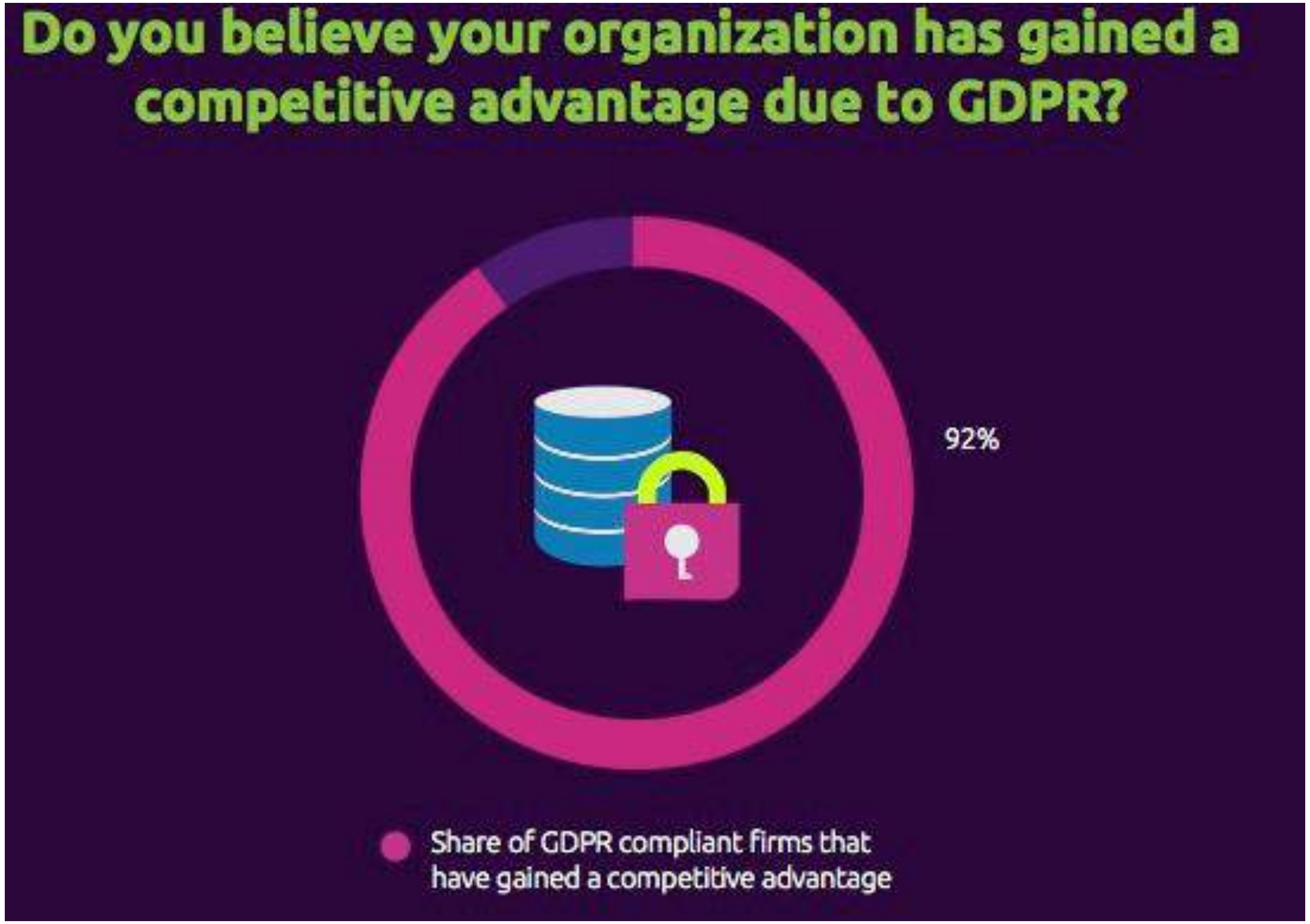
What does privacy and environmental sustainability have in common?

WHAT DOES THE ABBREVIATION GDPR STAND FOR?

What are the consequences of not complying with GDPR

- Whichever is higher:
  - 20 mill. EUR, or
  - 4% firm’s worldwide annual revenue from the preceding financial year
- Examples:
  - British Airways: **204,600,000** EUR (Art. 32: Insufficient TOMs to ensure information security)
  - Marriott International, Inc: **110,390,200** EUR (Art. 32: Insufficient TOMs to ensure information security)
  - Google Inc.: **50,000,000** (Art. 13 GDPR, Art. 14 GDPR, Art. 6 GDPR, Art. 5 GDPR: Insufficient legal basis for data processing)
  - Deutsche Wohnen SE: **14,500,000** EUR (Art. 5, 25: Non-compliance with general data processing principles)
  - 1&1 Telecom GmbH: **9,550,000** EUR (Art. 32, Insufficient technical and organisational measures to ensure information security)

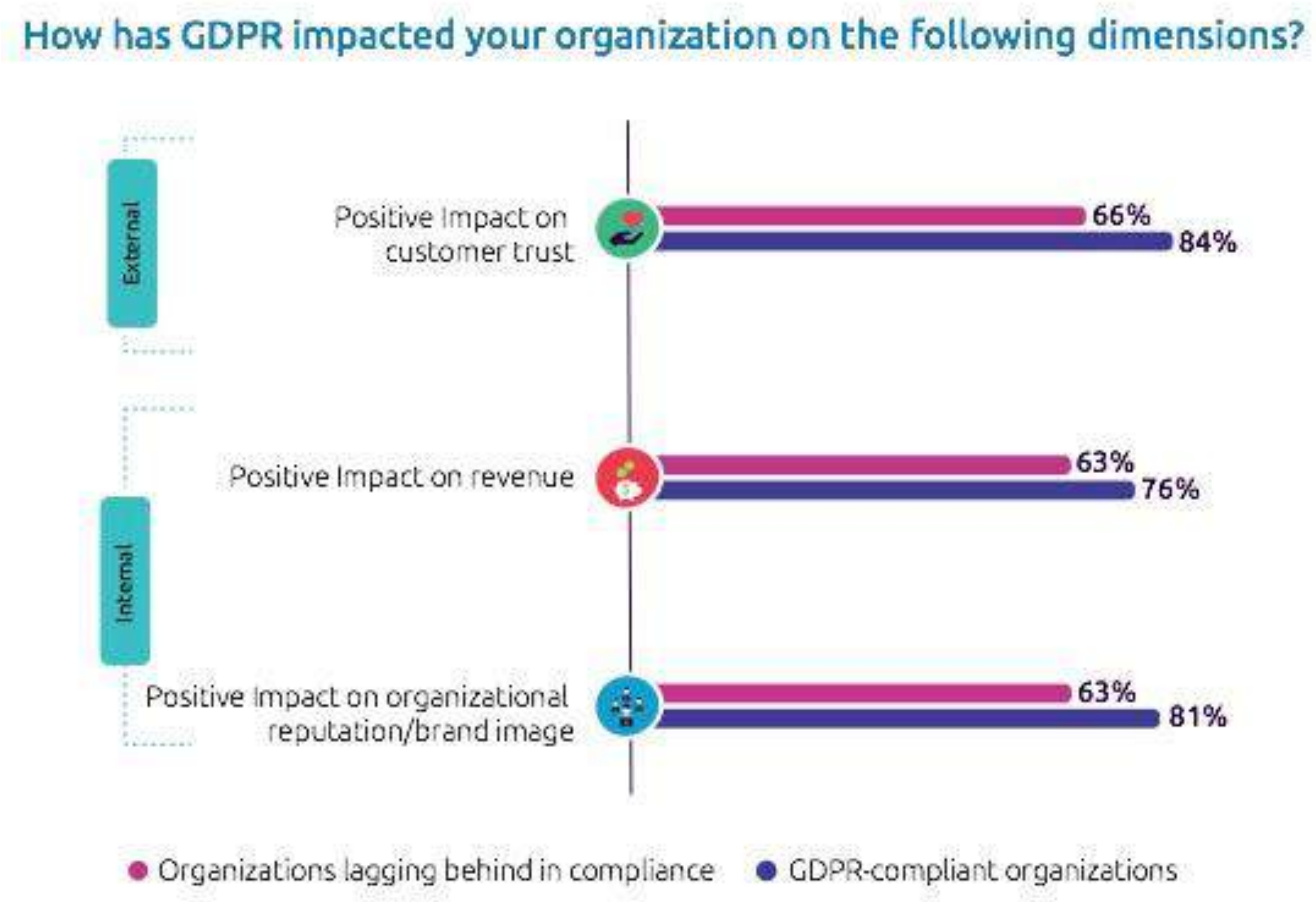
Companies perceive benefit from GDPR



Do you believe your organization has gained a competitive advantage due to GDPR?

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

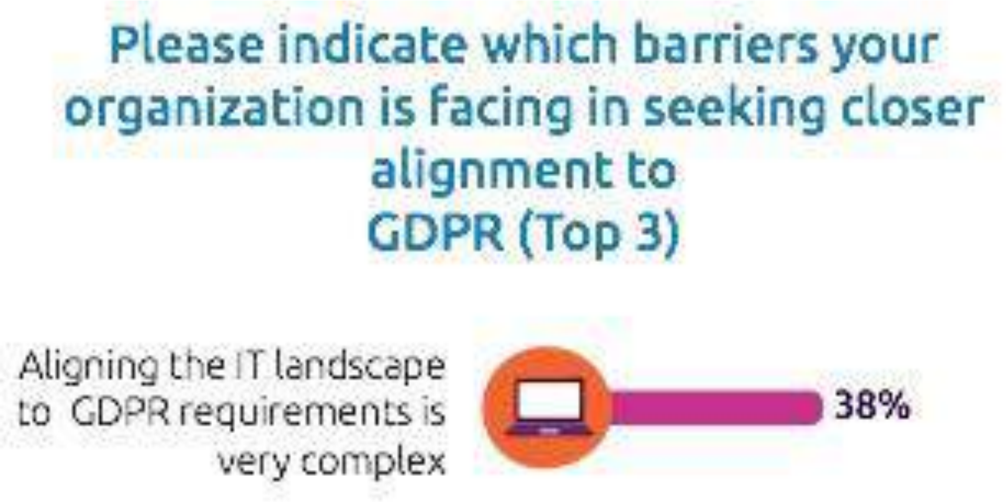
Positive impacts of GDPR on companies



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



Please indicate which barriers your organization is facing in seeking closer alignment to GDPR (Top 3)

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

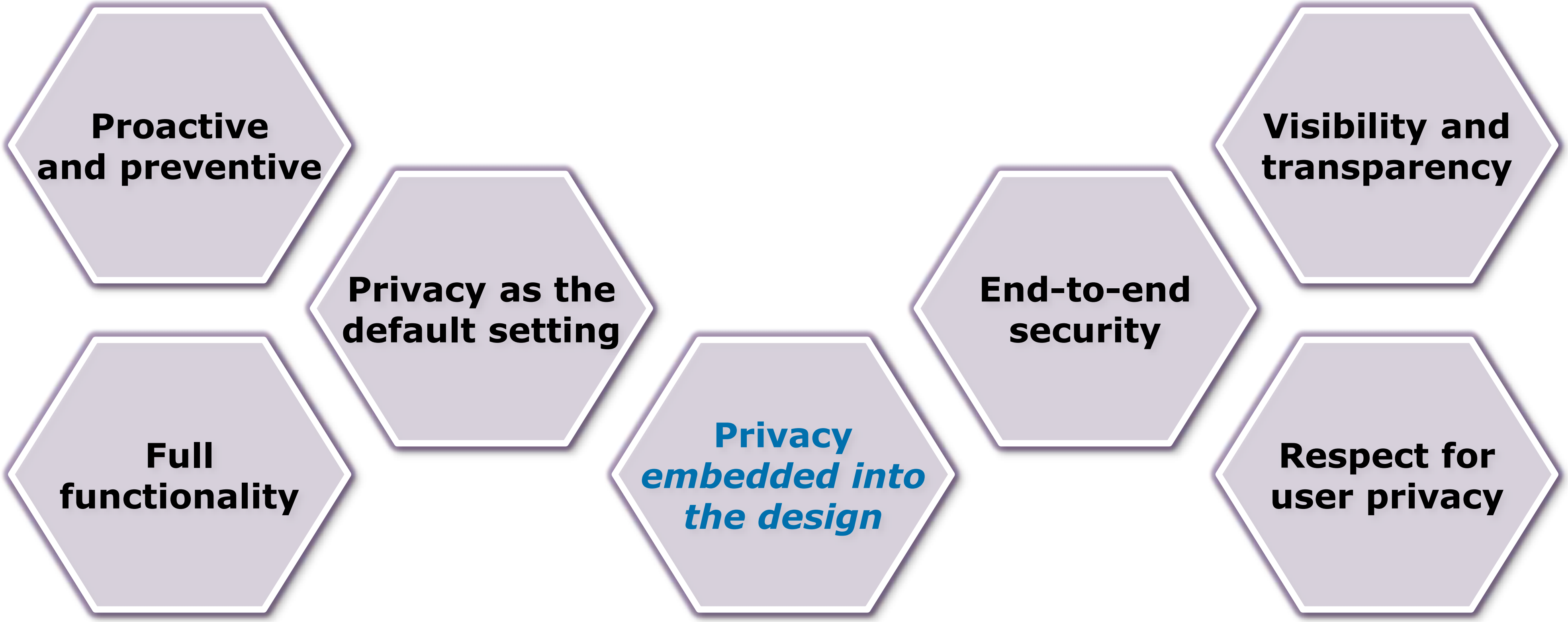
Assess how new data anonymization techniques and technologies can expand your data-sharing opportunities

3

Privacy Impact Assessment

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

Ann Cavoukian’s “privacy-by-design” principles



Proactive and preventive

Privacy as the default setting

Full functionality

Privacy embedded into the design

End-to-end security

Visibility and transparency

Respect for user privacy

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****"*

Privaby by Design – Challenges

- **Concrete implementation remains unclear** at the present moment.

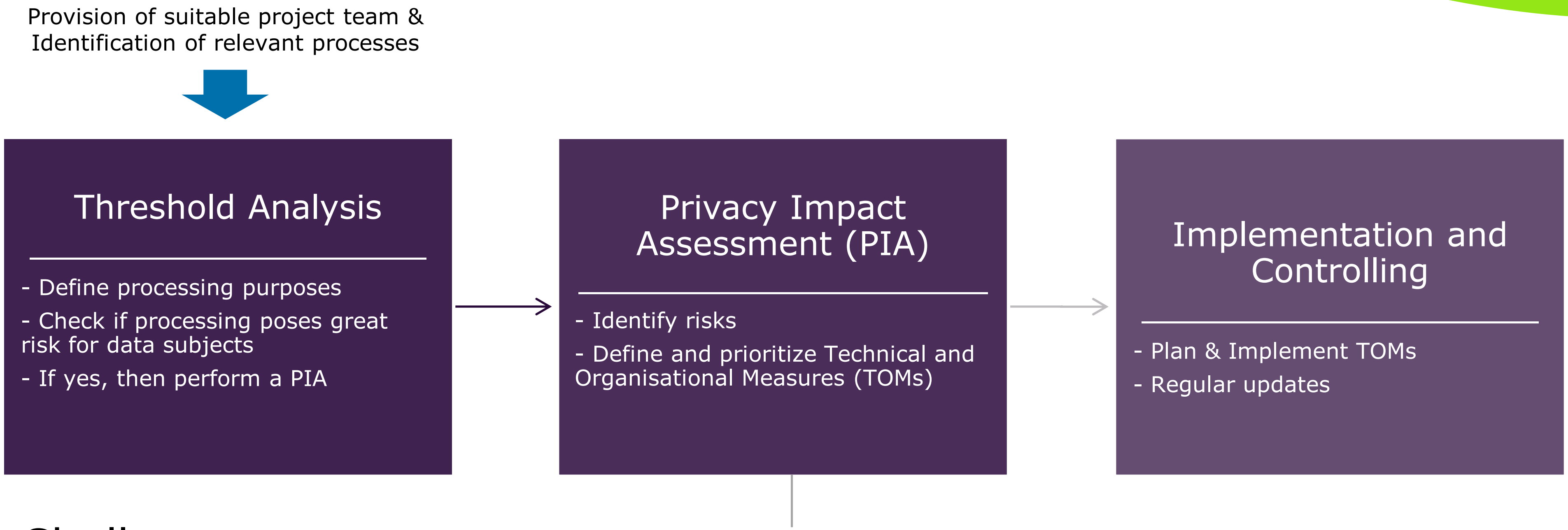
- "**Limitations of awareness** and **understanding** of *developers and data controllers* as well as **lacking tools** to realise privacy by design" (ENISA, 2014)

- 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)

GDPR – Privacy Impact Assessment (PIA) (Art. 35)

- *"Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing,* ***is likely to result in a high risk to the rights and freedoms of natural persons****, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data."*
- If required, then:
  - …"an assessment of the risks to the rights and freedoms of data subjects" …
  - "the measures envisaged to address the risks" (so-called Technical and Organisational Measures (TOMs))

Privacy Impact Assessment (PIA) – Approach & Challenges



Provision of suitable project team & Identification of relevant processes

Threshold Analysis

- Define processing purposes
- Check if processing poses great risk for data subjects
- If yes, then perform a PIA

Privacy Impact Assessment (PIA)

- Identify risks
- Define and prioritize Technical and Organisational Measures (TOMs)

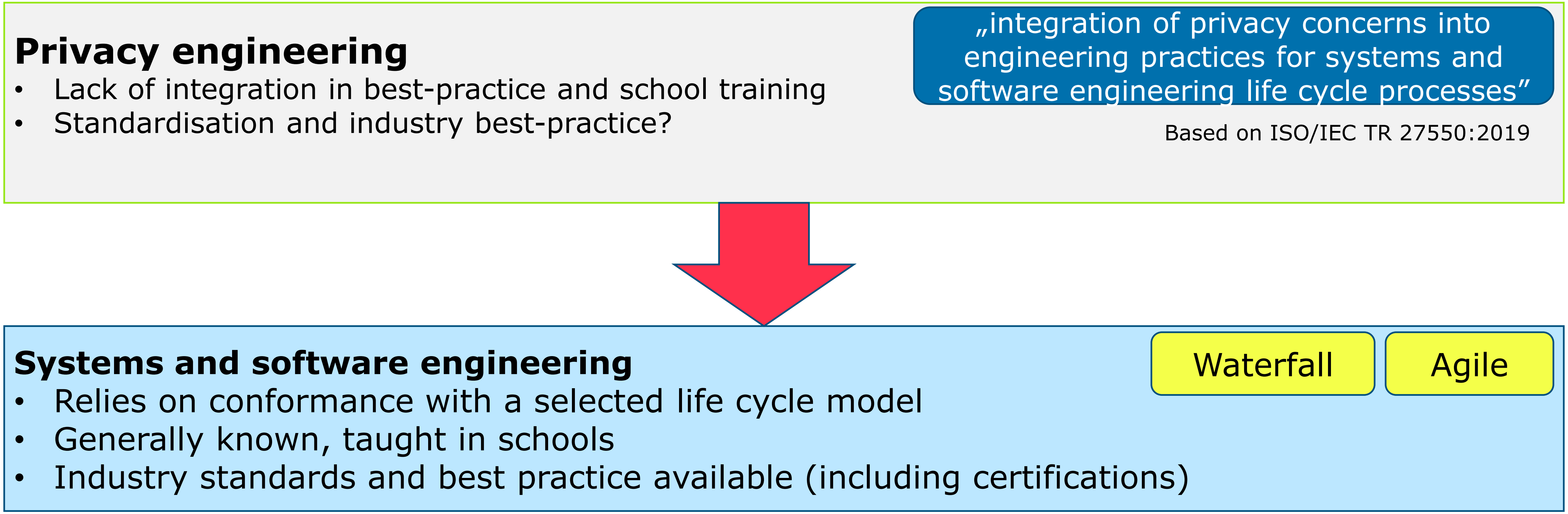
Implementation and Controlling

- Plan & Implement TOMs
- Regular updates

Challenges:

- Lack of know-how in projects
- Variety of stakeholders involved (IT, Business, Risk Management)
- Project deadlines and unawareness
- Lack of integration in software development frameworks

Privacy engineering



Privacy engineering

- Lack of integration in best-practice and school training
- Standardisation and industry best-practice?

„integration of privacy concerns into engineering practices for systems and software engineering life cycle processes"

Based on ISO/IEC TR 27550:2019

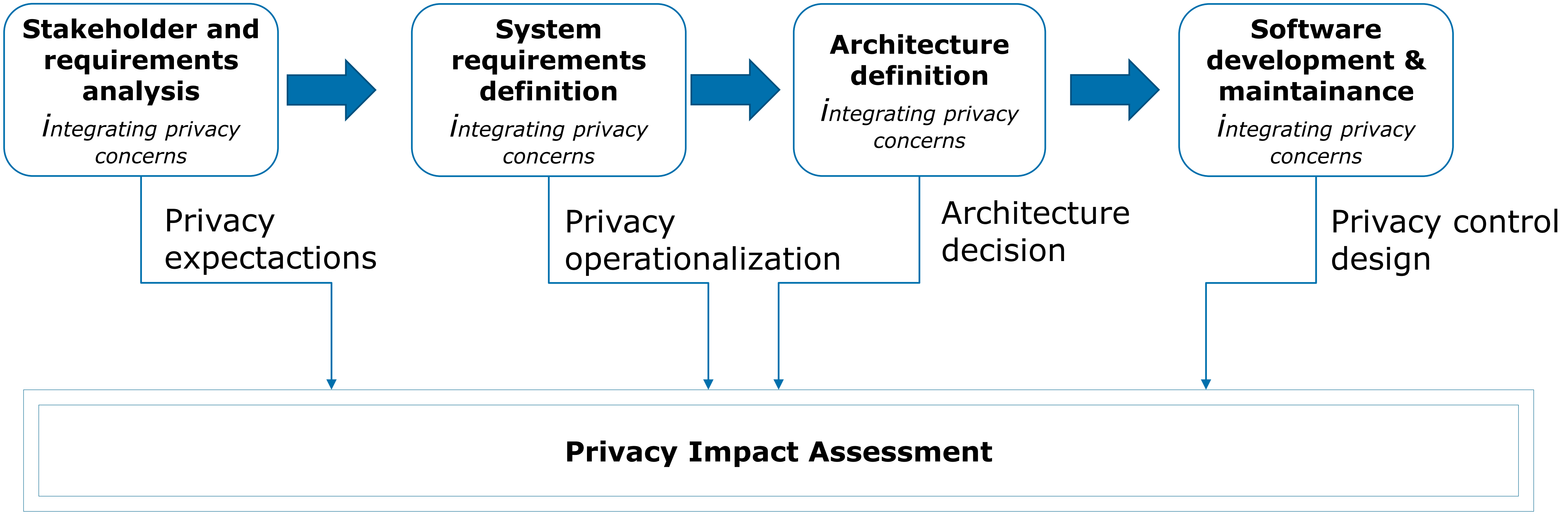
Systems and software engineering

- Relies on conformance with a selected life cycle model
- Generally known, taught in schools
- Industry standards and best practice available (including certifications)

Waterfall

Agile

Privacy Engineering and Privacy Impact Assessment



Stakeholder and requirements analysis

Integrating privacy concerns

System requirements definition

Integrating privacy concerns

Architecture definition

Integrating privacy concerns

Software development & maintainance

Integrating privacy concerns

Privacy expectations

Privacy operationalization

Architecture decision

Privacy control design

Privacy Impact Assessment

Adapted from ISO/IEC TR 27550:2019

Agenda

01 About

02 Background

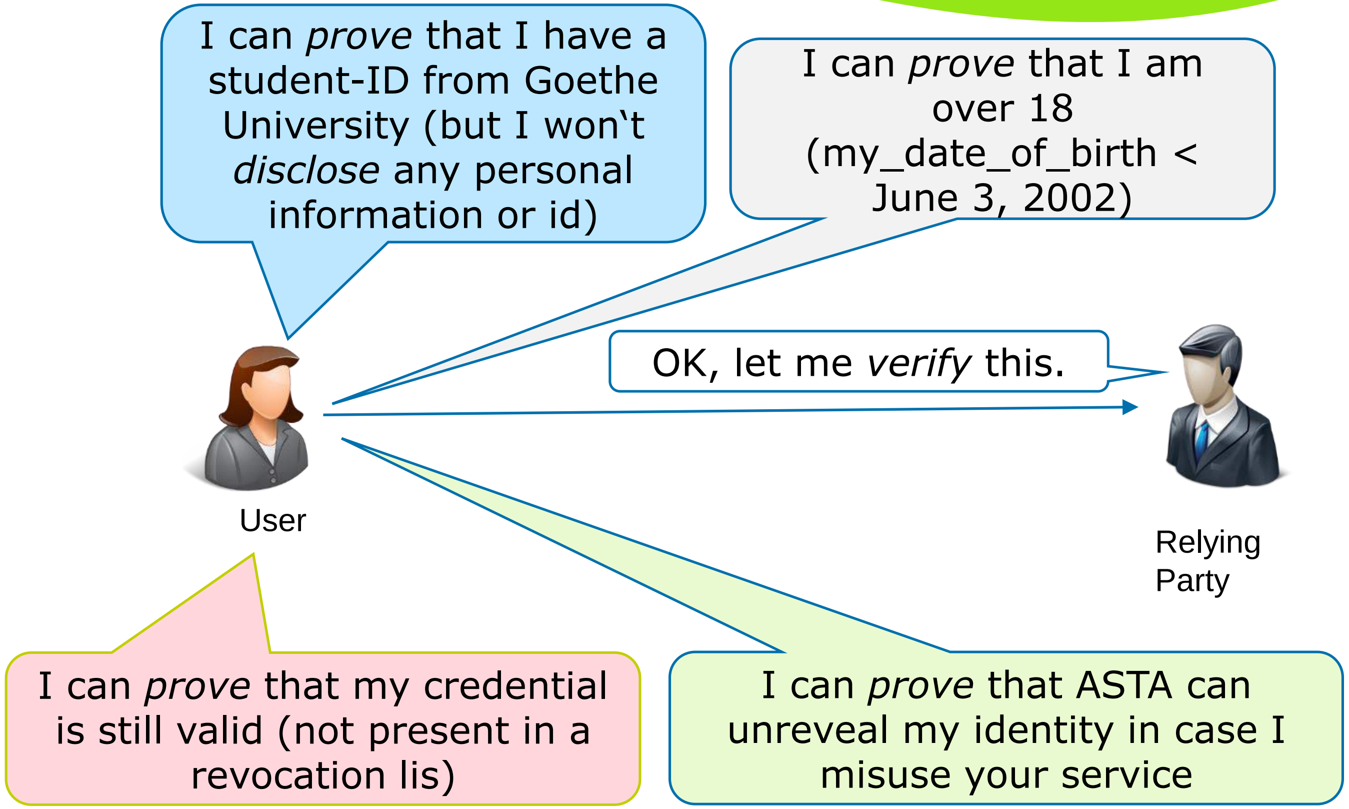
03 Privacy regulation and market

04 Pseudonymization technologies for privacy - challenges for mobility

05 Conclusion and outlook

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



I can *prove* that I have a student-ID from Goethe University (but I won't *disclose* any personal information or id)

I can *prove* that I am over 18 (my_date_of_birth < June 3, 2002)

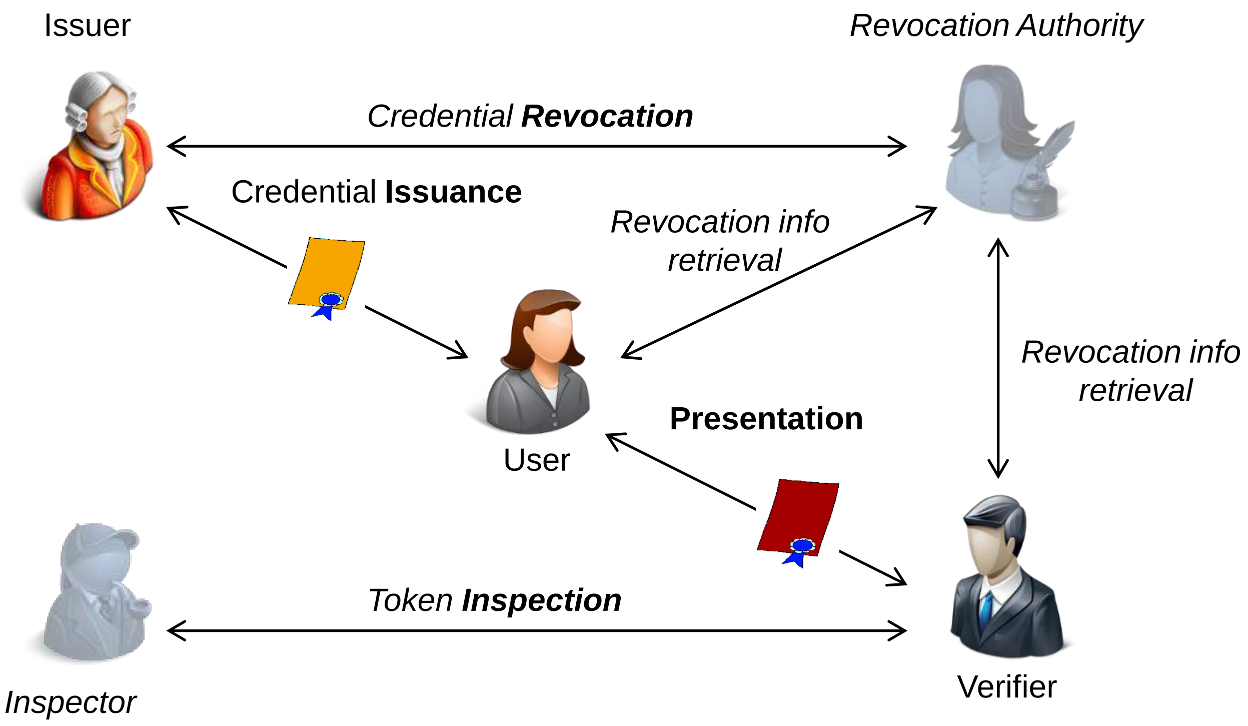
OK, let me *verify* this.

I can *prove* that my credential is still valid (not present in a revocation lis)

I can *prove* that ASTA can unreveal my identity in case I misuse your service

Privacy-ABC system architecture

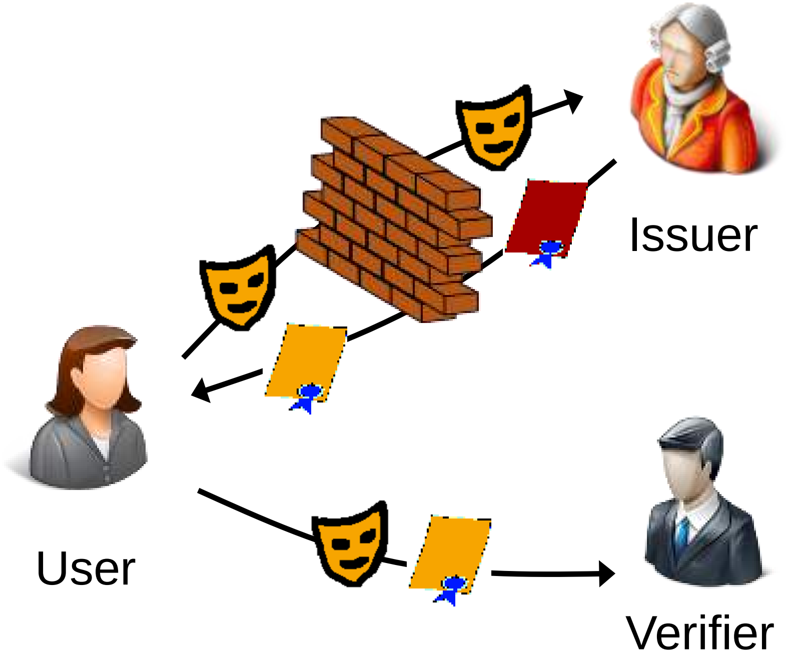
Entities and their interactions



Based on Bichsel *et al.* (2014)

Examples of Privacy-ABC technologies

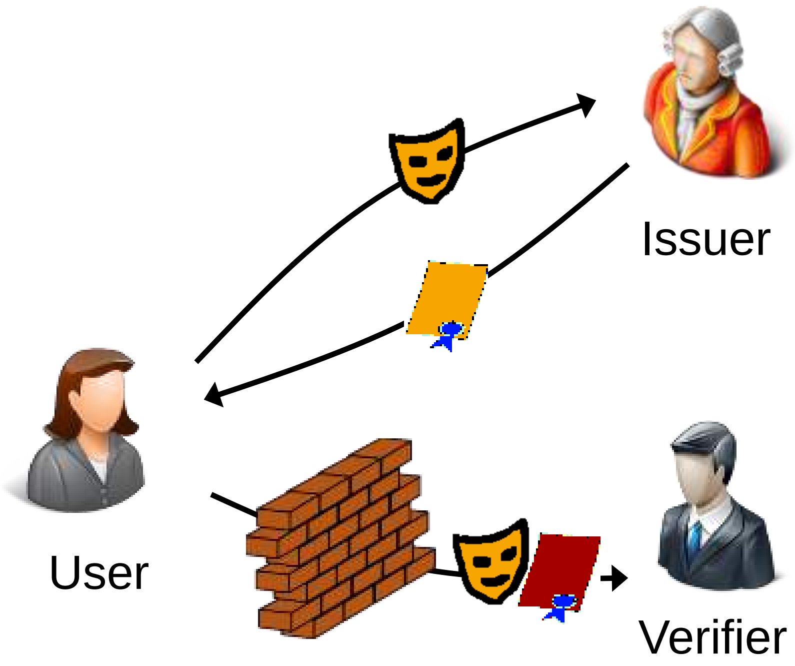
Blind Signatures


Issuer
User
Verifier

U-Prove

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

Zero-Knowledge Proofs


Issuer
User
Verifier

Idemix (Identity Mixer)

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

Privacy features

Minimal disclosure

(zero-knowledge)

Selective disclosure

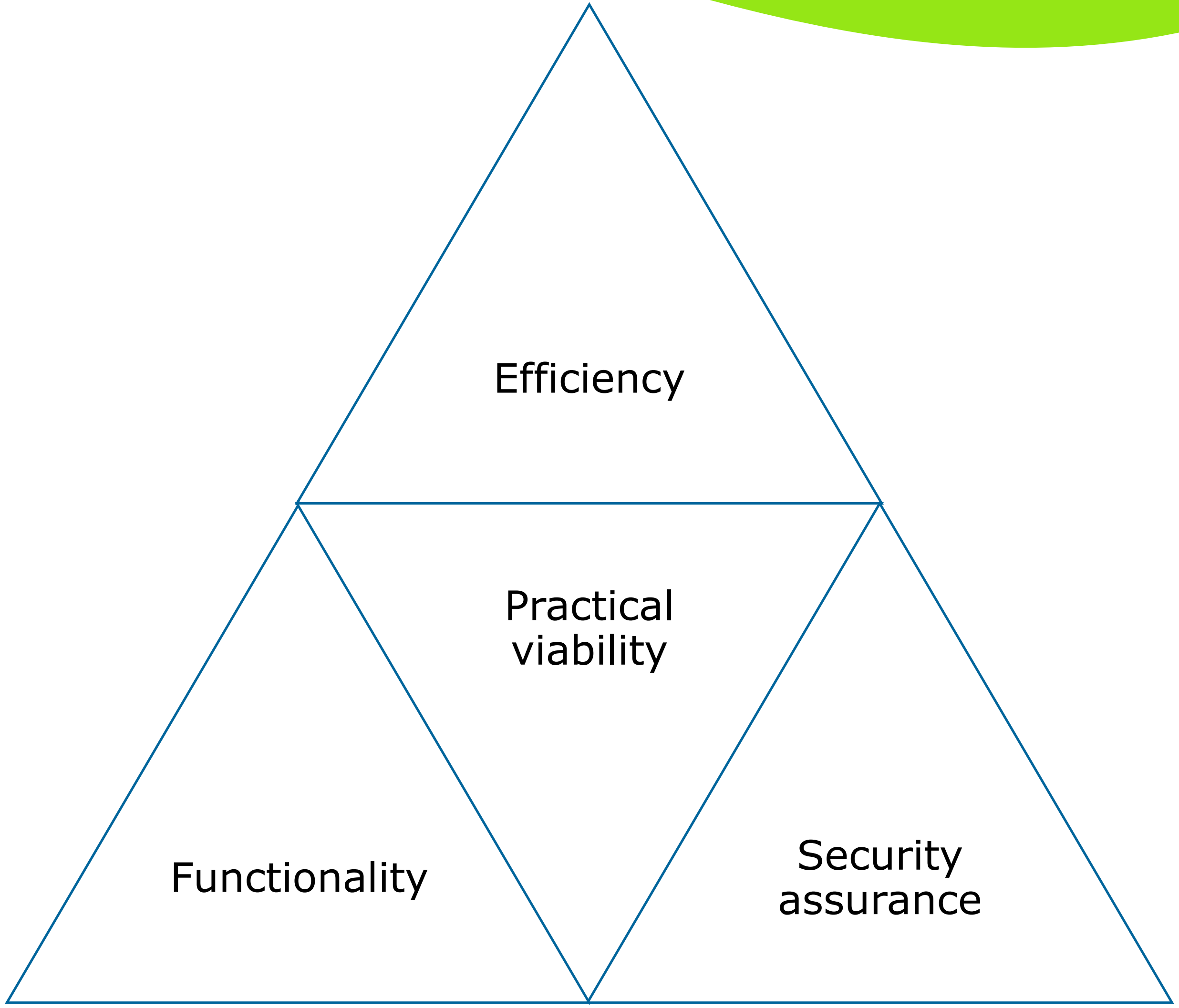
(by design)

Untraceability of presentation to issuance

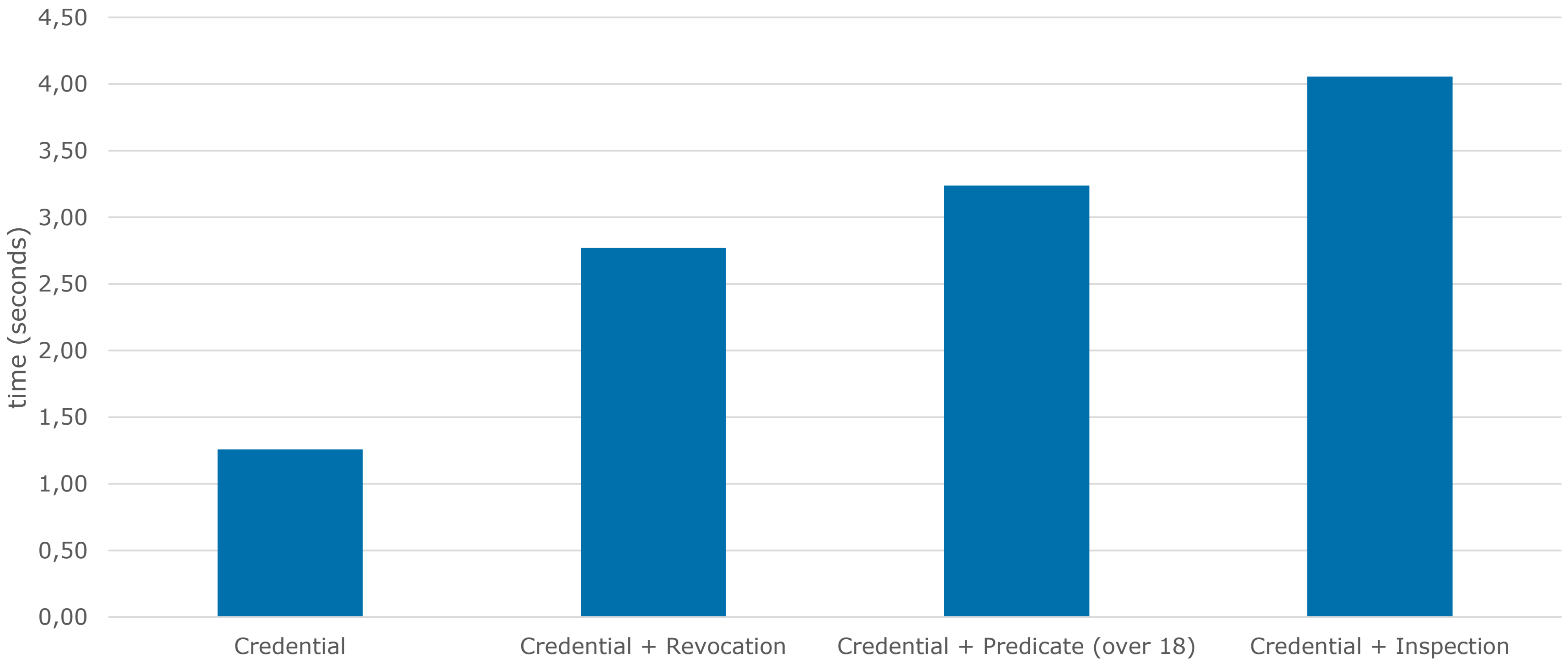
Unlinkability between different different presentations

Pseudonymous authentication

Competing goals?
Evaluation criteria for PETs



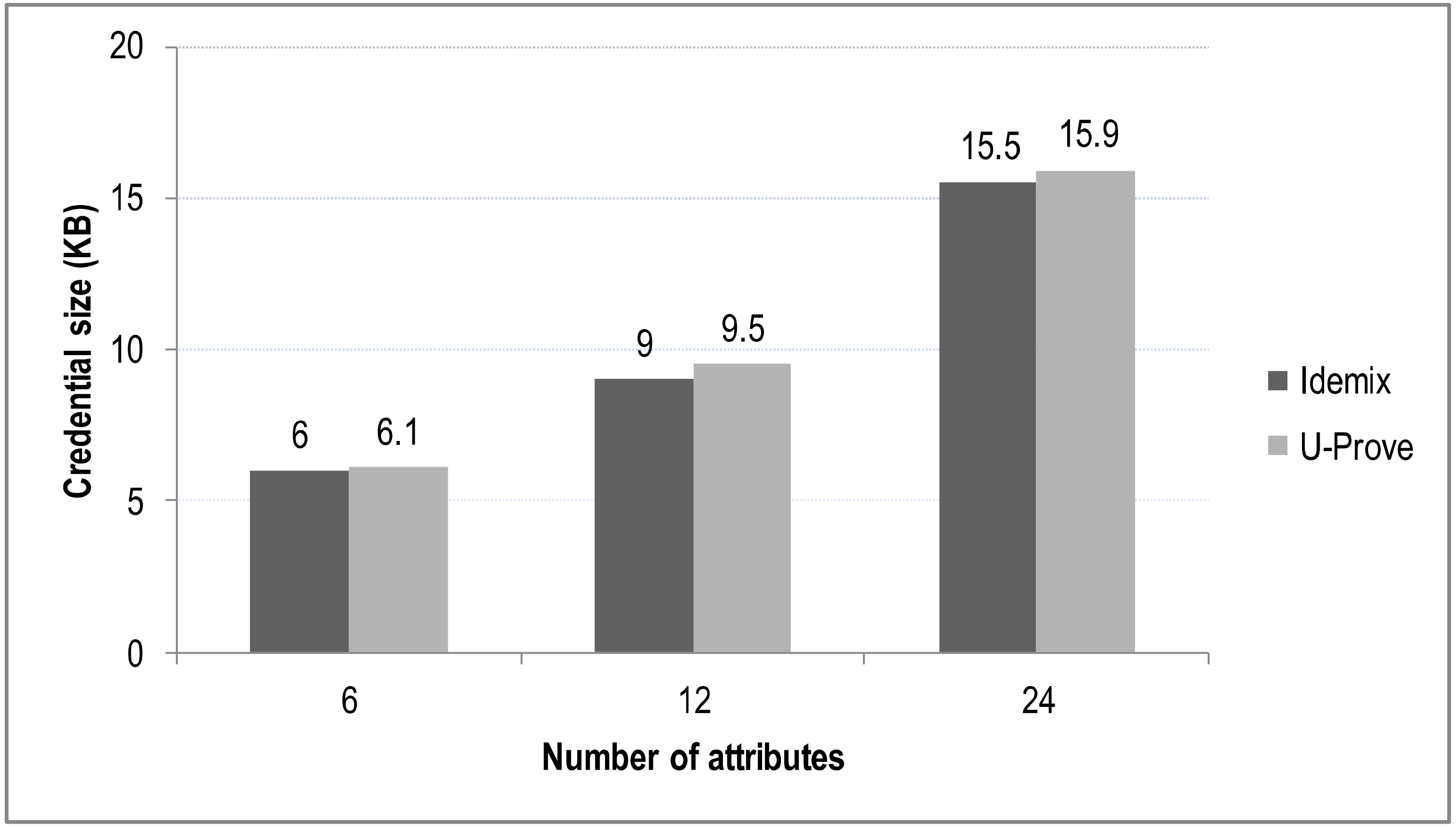
Functionality vs. efficiency



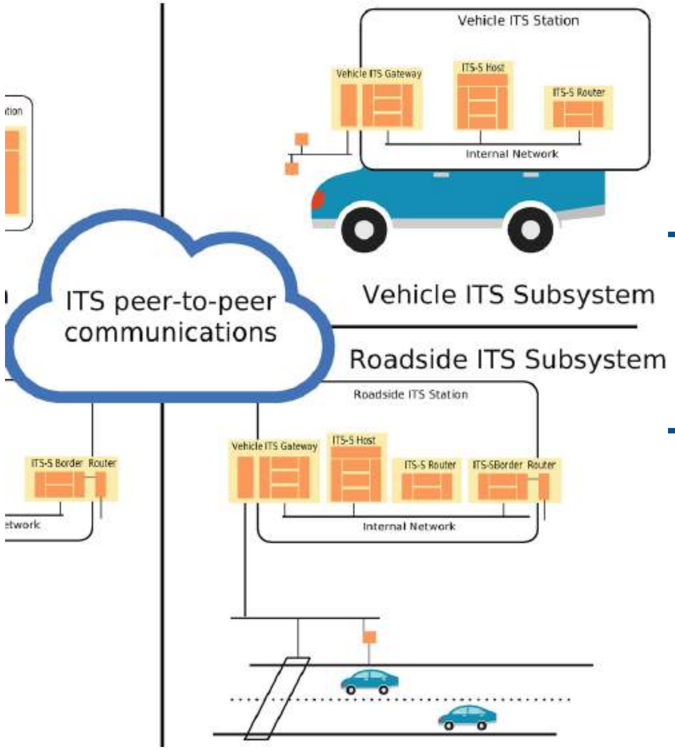
(Idemix, 1024 bits)

Challenges for Privacy-ABC technologies

- Changes in the identity infrastructure of service providers
- Data-centric business models
- 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)?*



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

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, key size is small (1024 bits) => not secure enough.
- For higher security, 2048 bits, Persiano would become unfeasible (over 1 km)

Agenda

01 About

02 Background

03 Privacy regulation and market

04 Pseudonymization technologies for privacy - challenges for mobility

05 Conclusion and outlook

Conclusion and Outlook

- Privacy has gained attention in the industry (regulation)
- Compliance with GDPR challenging in practice, but also a chance for businesses
- Systematic application of GDPR principles „Privacy by Design" and „Privacy Impact Assessment" challenging in practice
- Privacy-enhanced technologies, such as Privacy-ABC, are 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
- Addressing privacy requires changes to existing
  - Infrastructure (information systems)
  - Mindsets
  - Frameworks, best practices, standards, and training curricula

Thank you!

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

Backup slides

Presentation on Capgemini

Who we are

Capgemini is made up of almost **220,000 women and men** in over **40 countries**, who work with **world-renowned clients** to find solutions to their most demanding challenges. As a global leader in consulting, technology services, and digital transformation – with unrivaled sectorial expertise – we enable our clients to **design and build tomorrow’s businesses**, make the most of the opportunities offered by technology, and **boost their competitiveness and agility**.

A Leader for Leaders

2019 full-year results

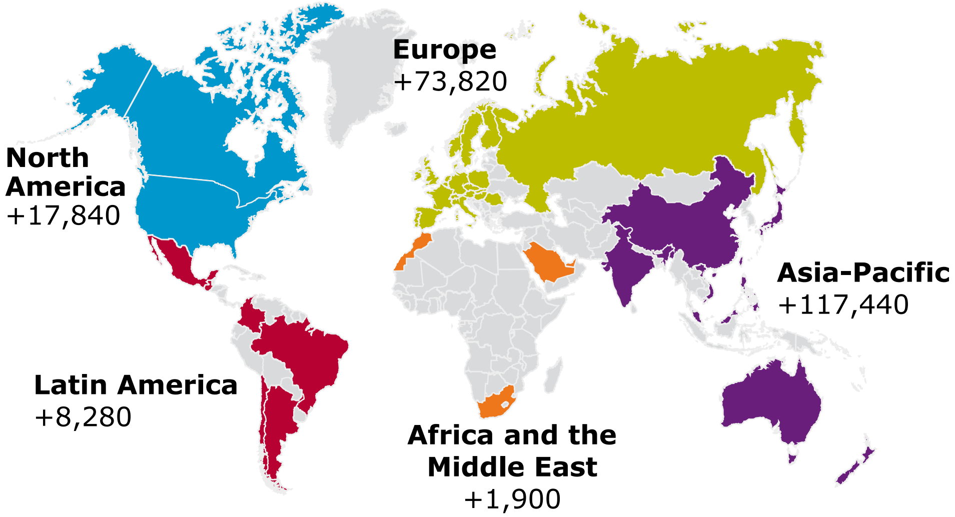
€14.1 bn
revenue
with an operating margin of 12.3%

220 000
people
with more than 110,000 in India alone

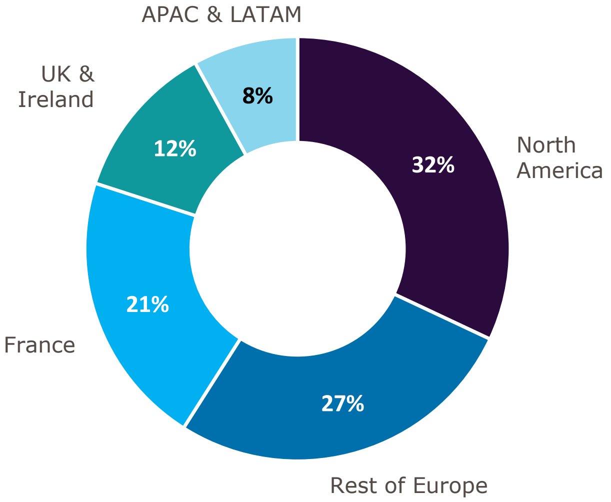
+40
countries
with more than 120 nationalities

33
average age
of our people

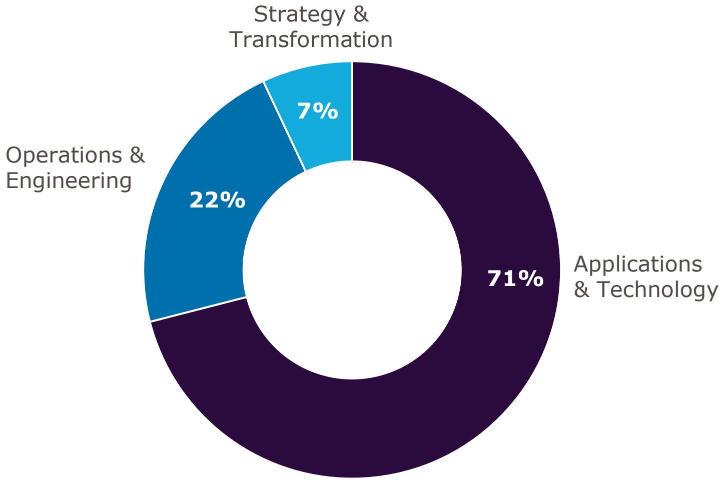
International footprint



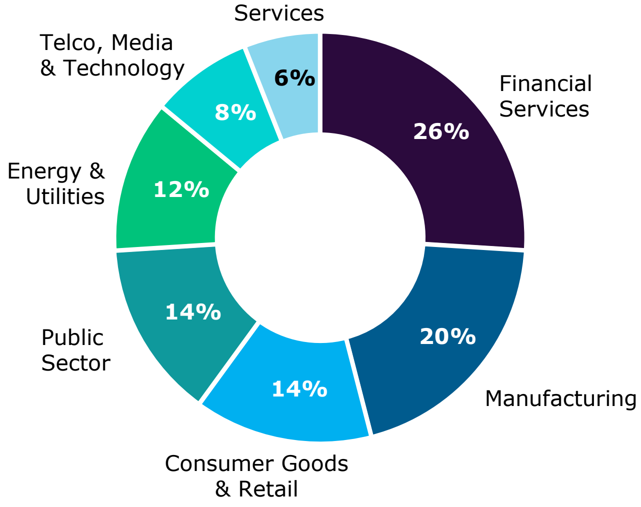
Revenue by region



Revenue by business



Revenue by sector



Einstieg für Studenten

Sammle neben dem Studium Praxiserfahrung:

Praktikum

Werkstudententätigkeit

Abschlussarbeit

Berufsbegleitendes Masterstudium

Duales Studium

Deine Vorteile:

- Praxiserfahrung sammeln
- Einblick in die Projektarbeit
- Fachliche und persönliche Weiterentwicklungsmöglichkeiten durch den praxisnahen Einstieg
- Weiterentwicklung von Soft Skills

Das duale Studium der Informatik oder Wirtschaftsinformatik bietet die ideale Mischung aus Theorie und Praxis.