mobile business

Lecture 9

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Information & Communication Security (WS 18/19)

Privacy Protection II

Prof. Dr. Kai Rannenberg
Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt
www.m-chair.de

Agenda

- Data Protection and Privacy
  - Origin and definition
  - Law, Technology, Standardization
- Technical Privacy Protection
  - Communication systems
  - Transaction systems
- Concepts of Privacy Protection
  - Privacy by Design (PbD)
  - Privacy Engineering
  - Transparency
  - Usability
- Integrated Privacy Protection
  - PRIME LBS
  - ABC4Trust
  - Privacy Advisor
  - Privacy Risk Communication and Mitigation

mobile business

Transaction systems

- Reachability management
- Credential technologies
  - U-Prove

    www.microsoft.com/uprove
  - Idemix

    www.zurich.ibm.com/security/idemix

Identity Management as part of Reachability Management

Statement of urgency

"It is really urgent!"

Specification of a function

"I am your boss!"

Specification of a subject

"Let's have a party tonight."

Presentation of a voucher

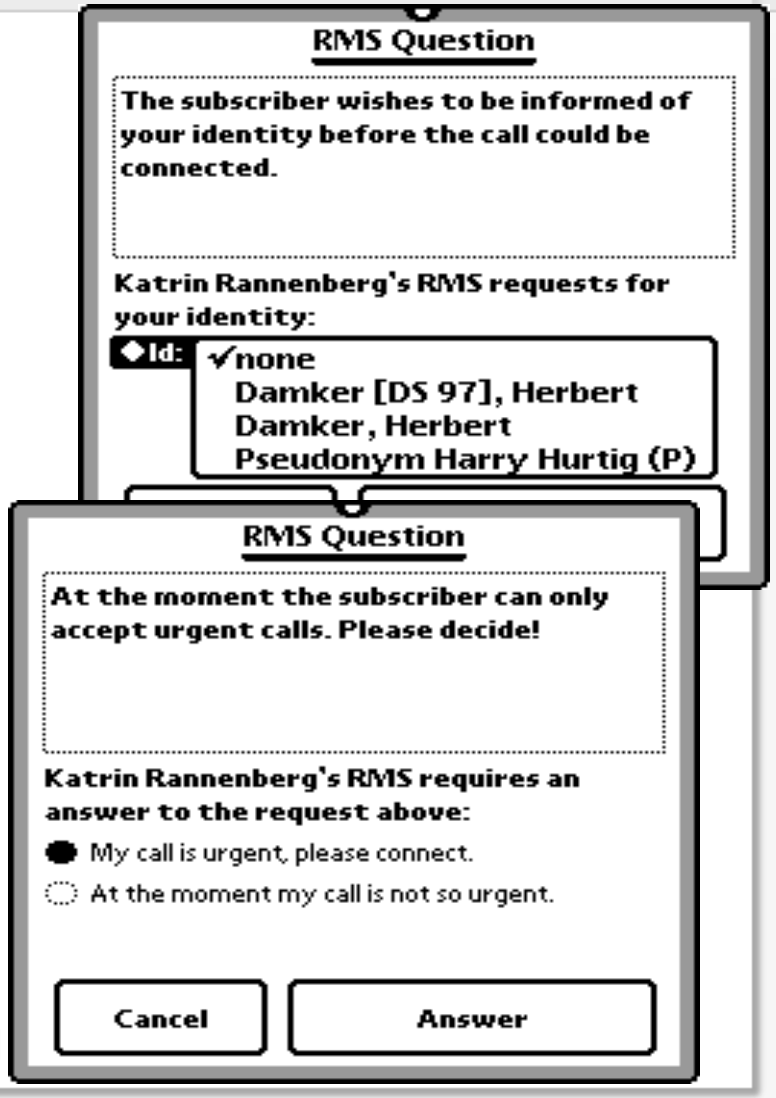
"I welcome you calling back."

Provision of a reference

"My friends are your friends!"

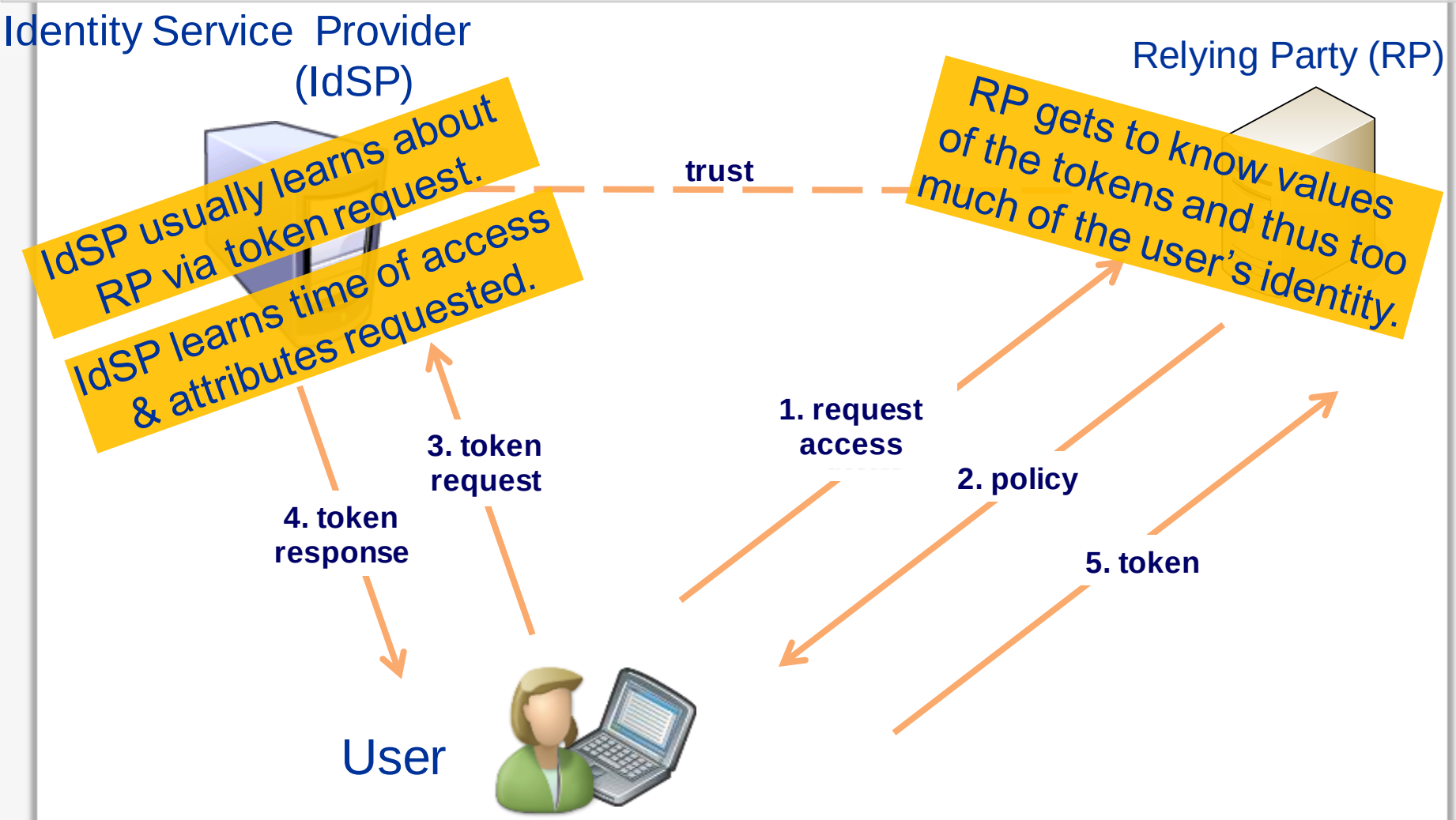
Offering a surety

"Satisfaction guaranteed or this money is yours!"



[Rannenberg2000]

Privacy (and security) issues of typical federated IdM architectures



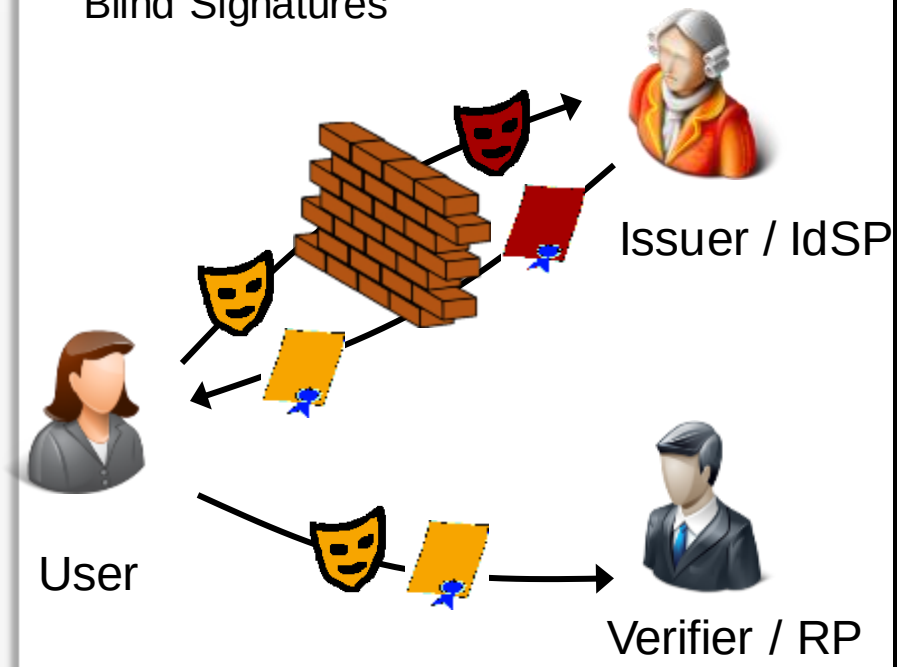
Credential Systems

Privacy-enhancing Attribute-based Credentials (Privacy-ABCs)

- Privacy features:
  - Different levels of pseudonymity
  - Selective (minimal) disclosure of attributes (attribute hiding)
  - Unlinkability of user's transactions
- Additional features are possible:
  - Prove age without disclosing birthday, e.g. for buying alcohol, showing being over 18
  - Proving of not being revoked, without disclosing the serial number in the credential
  - Predicates over attributes (no disclosure) with a constant value or another attribute
    - Inequality of attributes
    - Equality of attributes
    - Value belonging to a certain interval
  - Controlled linkability, e.g. avoid voting more than once
  - Conditional accountability, when needed

Two approaches for Privacy-ABCs

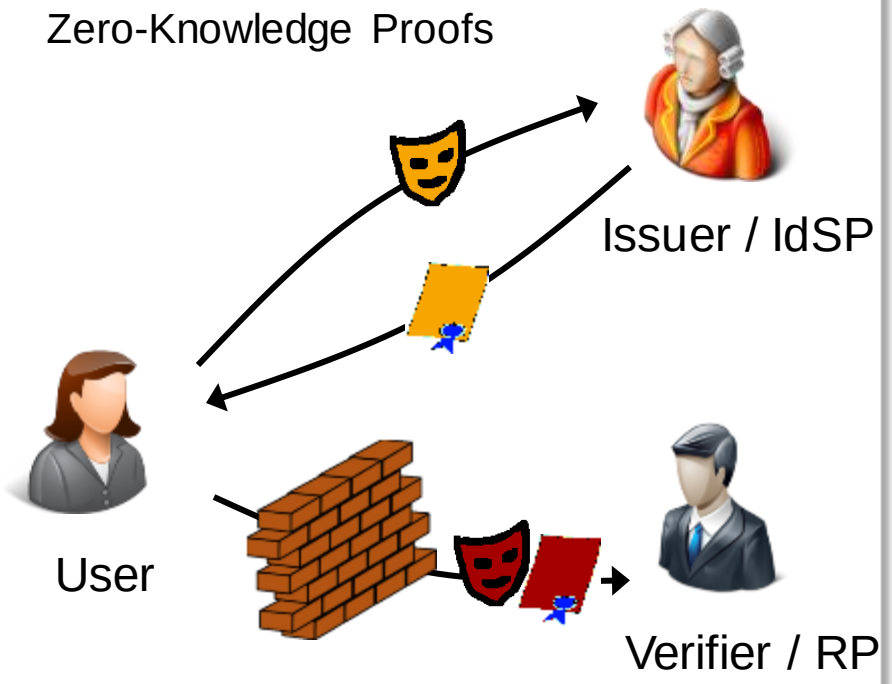
Blind Signatures



U-Prove

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

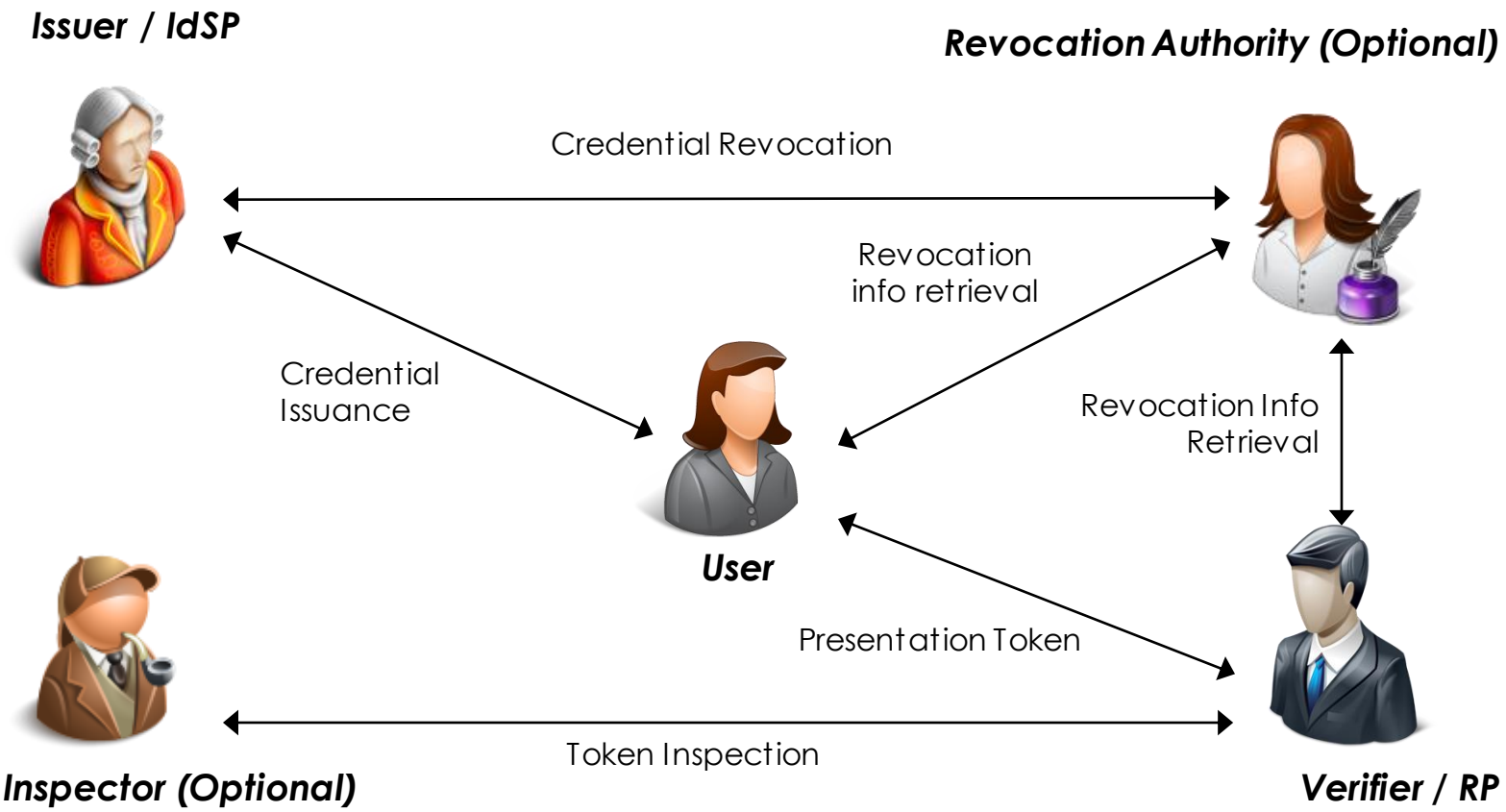
Zero-Knowledge Proofs



Idemix (Identity Mixer)

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

ABC4Trust architecture
High level view



PETs alone are not sufficient

- Anonymization and Pseudonymization
  - Mix-Master, Onion Routing, Anonymous Payment, Anonymous Credentials
  - A myriad of techniques and algorithms
- Playing Cat and Mouse with Big Brother
  - Best example is Cookie Cooker
  - But many people do not have the time.
- Good pragmatic tool, but still no success
  - ⇨ Integrated privacy protection,
    - ⇨ Into business processes
    - ⇨ Into user interfaces

Agenda

- Data Protection and Privacy
  - Origin and definition
  - Law, Technology, Standardization
- Technical Privacy Protection
  - Communication systems
  - Transaction systems
- Concepts of Privacy Protection
  - Privacy by Design (PbD)
  - Privacy Engineering
  - Transparency
  - Usability
- Integrated Privacy Protection
  - PRIME LBS
  - ABC4Trust
  - Privacy Advisor
  - Privacy Risk Communication and Mitigation

Privacy by Design (PbD)

- PbD refers to the philosophy and approach of embedding privacy into the design specifications of various technologies.
- The concept is an example of value sensitive design, i.e., to take human values into account in a well defined matter throughout the whole process.

[Cavoukian2009]

Privacy-by-design
7 Foundational Principles

- Proactive not reactive
- Privacy as the Default setting
- Privacy Embedded into the Design
- Full Functionality
- End-to-End Security
- Visibility and Transparency
- Respect for User Privacy

[Cavoukian2009]

Adoption of Privacy by Design in regulation

- 2010: The International Conference of Data Protection and Privacy Commissioners unanimously endorsed PbD.
- 2012: The Federal Trade Commission (FTC) in the US, proposed a framework for business and policymakers with PbD as a core value.
- 2014: The European Commission announced that: 'Privacy by Design' and 'privacy by default' will become essential principles in EU data protection rules.
- 2016: EU GDPR published including Article 25 "Data protection by design and by default"
- 2018: GDPR to be implemented

[based on CPDP2014]

GDPR Article 25
Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, **both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures,** such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
2. The controller shall implement appropriate technical and organisational measures for ensuring that, **by default, only personal data which are necessary for each specific purpose of the processing are processed**. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.
3. An **approved certification mechanism** pursuant to Article 42 may be used as an element **to demonstrate compliance** with the requirements set out in paragraphs 1 and 2 of this Article.

[EU2016]

GDPR Article 25 (1)
Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, **both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures,** such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

GDPR Article 25 (2) & (3)
Data protection by design and by default

2. The controller shall implement appropriate technical and organisational measures for ensuring that, **by default, only personal data which are necessary for each specific purpose of the processing are processed**. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.
3. An **approved certification mechanism** pursuant to Article 42 may be used as an element **to demonstrate compliance** with the requirements set out in paragraphs 1 and 2 of this Article.

GDPR Recital 78

- The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met.
- In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default.
- Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features.
- When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.

[EU2016]

Privacy-by-design 7 Foundational Principles (in a bit more detail)

- **Proactive not Reactive:**
  - anticipates and prevents privacy invasive events before they happen
- **Privacy as the Default Setting:**
  - seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice
- **Privacy Embedded into Design:**
  - embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact
- **Full Functionality — Positive-Sum, not Zero-Sum:**
  - Privacy by Design avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.
- **End-to-End Security — Full Lifecycle Protection:**
  - having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish.
- **Visibility and Transparency — Keep it Open:**
  - seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.
- **Respect for User Privacy — Keep it User-Centric:**
  - PbD requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

Privacy-by-design 7 Foundational Principles (in a bit more detail)

- **Proactive not Reactive:**
  - anticipates and prevents privacy invasive events before they happen
- **Privacy as the Default Setting:**
  - seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice
- **Privacy Embedded into Design:**
  - embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact
- **Full Functionality — Positive-Sum, not Zero-Sum:**
  - Privacy by Design avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.
- **End-to-End Security — Full Lifecycle Protection:**
  - having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish.
- **Visibility and Transparency — Keep it Open:**
  - seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.
- **Respect for User Privacy — Keep it User-Centric:**
  - PbD requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

Privacy-by-design Principle 4

- **Full Functionality — Positive-Sum, not Zero-Sum:**
  - Privacy by Design avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.

Privacy-by-design Principle 4

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.

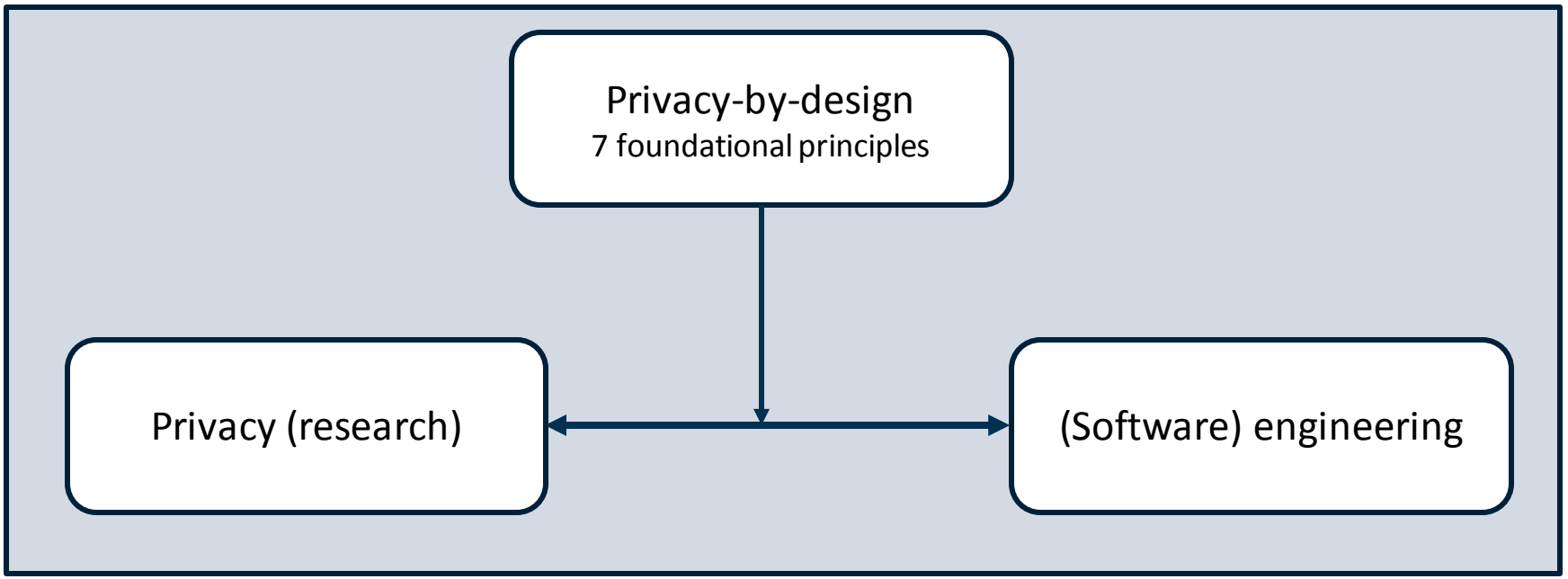
[Cavoukian2009]

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 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*** often possible to have a combination of both.

Privacy engineering I

- Privacy engineering is aimed to fill the gap between research and practice (between privacy and software engineering).



[Gürses2016]

Privacy engineering II

- Field of research and practice that **designs**, **implements**, **adapts**, and **evaluates** methods, techniques, and tools:
  - Methods are approaches for systematically capturing and addressing privacy issues.
  - Techniques are procedures, possibly with a prescribed language, to accomplish privacy-engineering tasks or activities.
  - Tools are means that support privacy engineers during part of a privacy engineering process.

[Gürses2016]

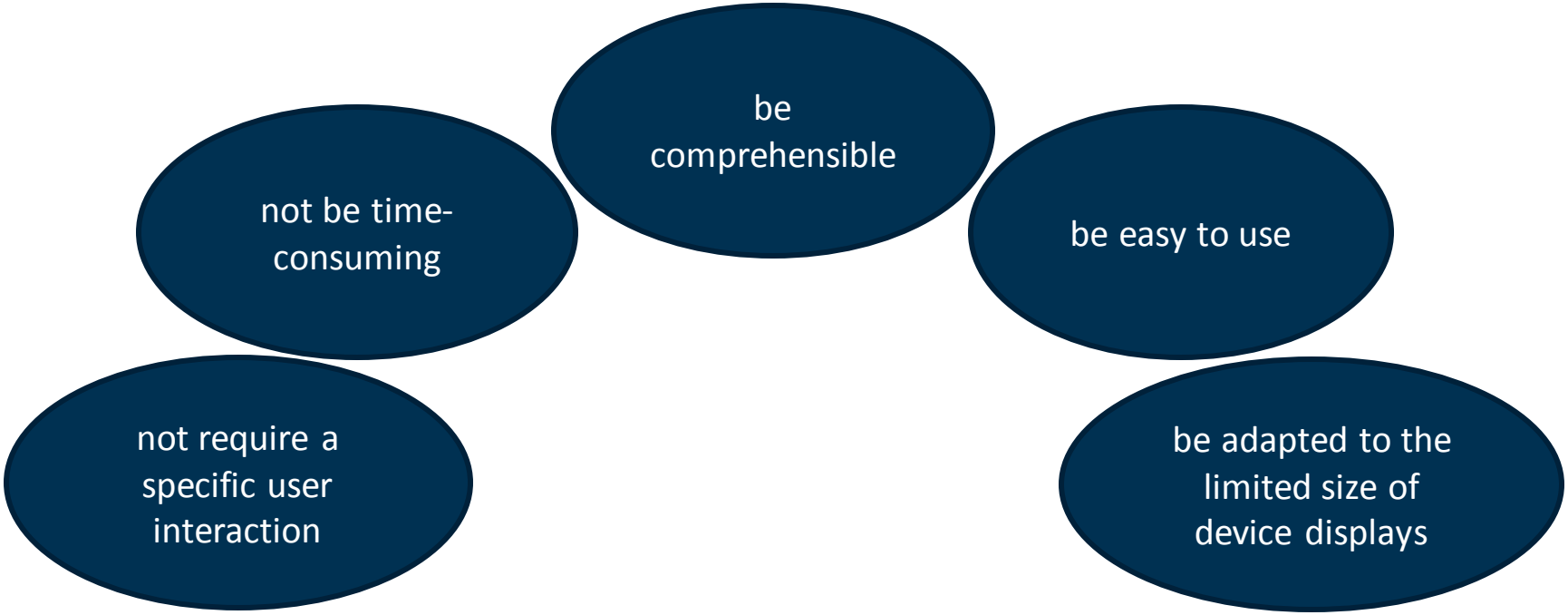
Transparency I

- A basic principle that users must be informed about **how much** and **to which level**, and **by whom** their information is being accessed
- Users must be informed **before**, **during** and **after** the processing takes place, thus it has to cover:
  - not only the actual processing, but also
  - the planned processing (ex-ante transparency) and
  - the time after the processing has taken place to know what exactly happened (ex-post transparency)

[Danezis2014]

Transparency II

- The solutions for providing transparency should have some important features. They should:



[Danezis2014]

mobile business

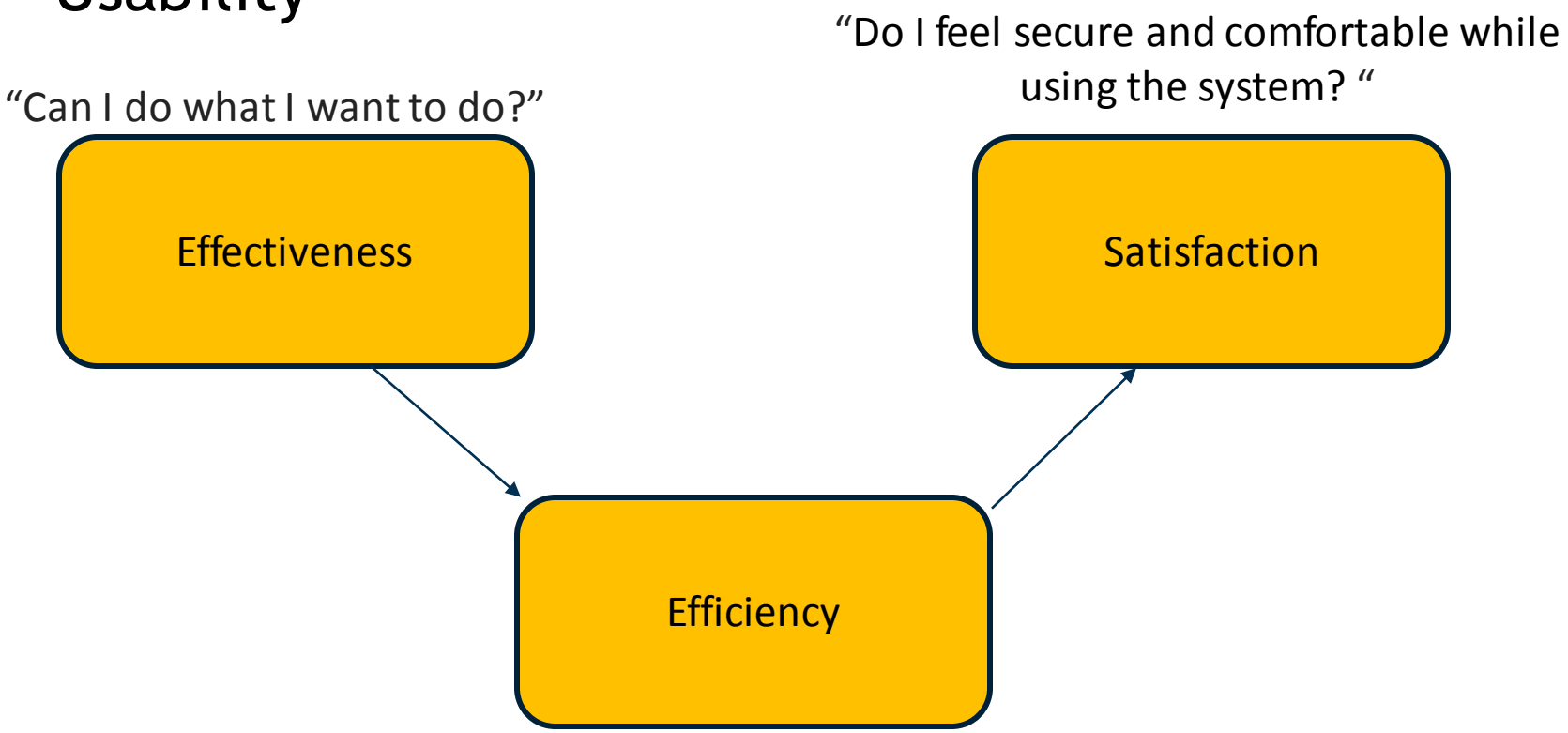
Usability I

- Usability is defined as the **extent** to which a **system**, **product** or **service** can be used by **specified users** to achieve **specified goals** with **effectiveness**, **efficiency**, and **satisfaction:**
  - Effectiveness: The user is able to achieve his/her goal.
  - Efficiency: The user reaches the goal with minimal effort.
  - Satisfaction: The user reaches the goal without dissatisfaction.

[NationalAcademy2010] based on [ISO 9241-11:2018]

Usability II

- Usability



[NationalAcademy2010] based on [ISO 9241-11:2018]

Agenda

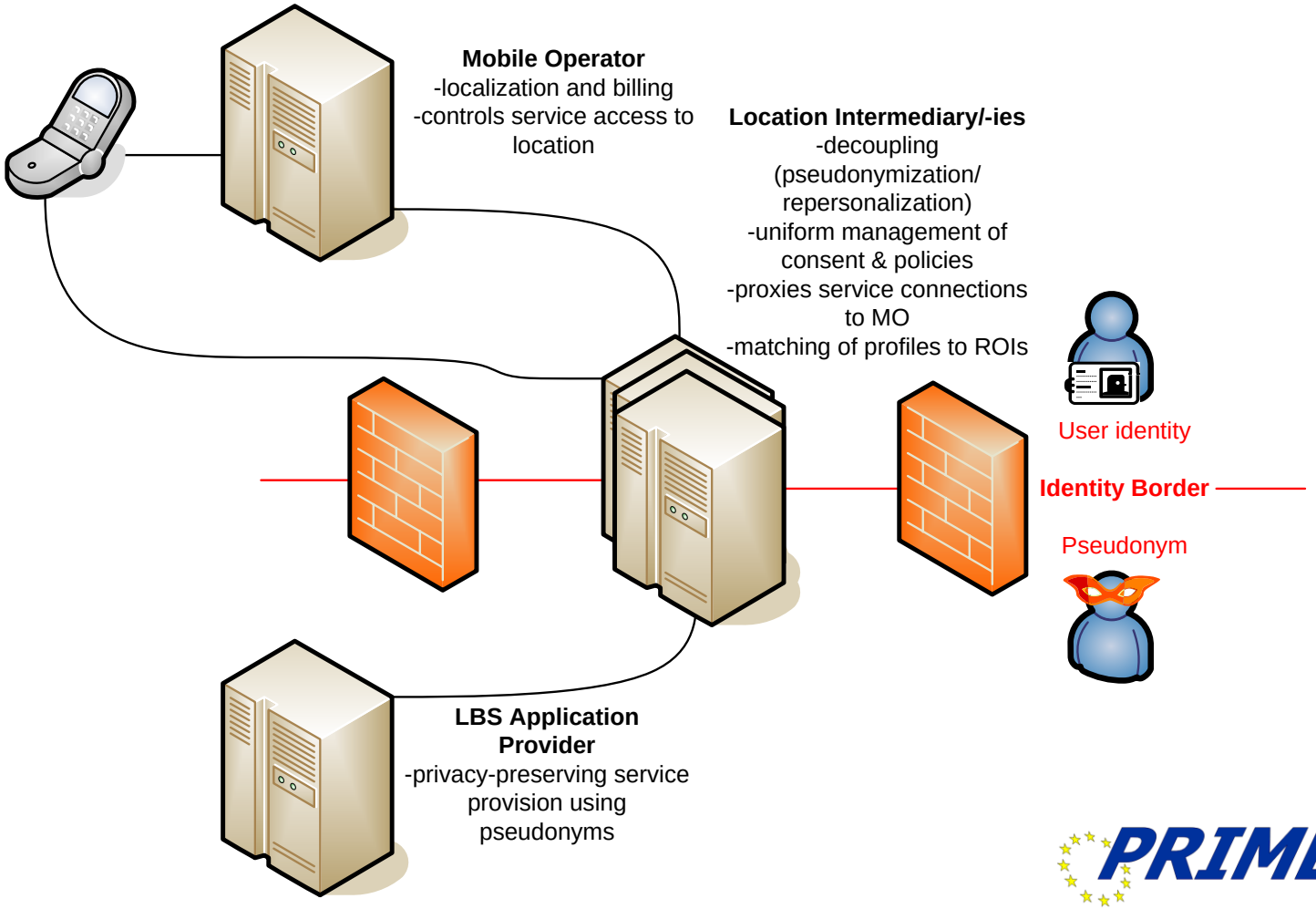
- Data Protection and Privacy
  - Origin and definition
  - Law, Technology, Standardization
- Technical Privacy Protection
  - Communication systems
  - Transaction systems
- Concepts of Privacy Protection
  - Privacy by Design (PbD)
  - Privacy Engineering
  - Transparency
  - Usability
- Integrated Privacy Protection
  - PRIME LBS
  - ABC4Trust
  - Privacy Advisor
  - Privacy Risk Communication and Mitigation

PRIME LBS Application Prototype

- Enhance privacy for typical LBS
  - Pharmacy search (“pull”)
  - Pollen warning (“push”)
- Address wide user range by making only few requirements on the existing infrastructure
  - Simple WAP mobile phone (Version 1), Java phone (Version 2)
- Several challenges
  - Privacy problems
  - Regulation, e.g. of the handling of personal information (and mobile services in general)
  - Business constraints
    - Easy integration into existing infrastructure
    - Applicability to a wide range of business models
    - Adaptability for different market structures

PRIME LBS Application Prototype Intermediary Approach

Architecture Overview

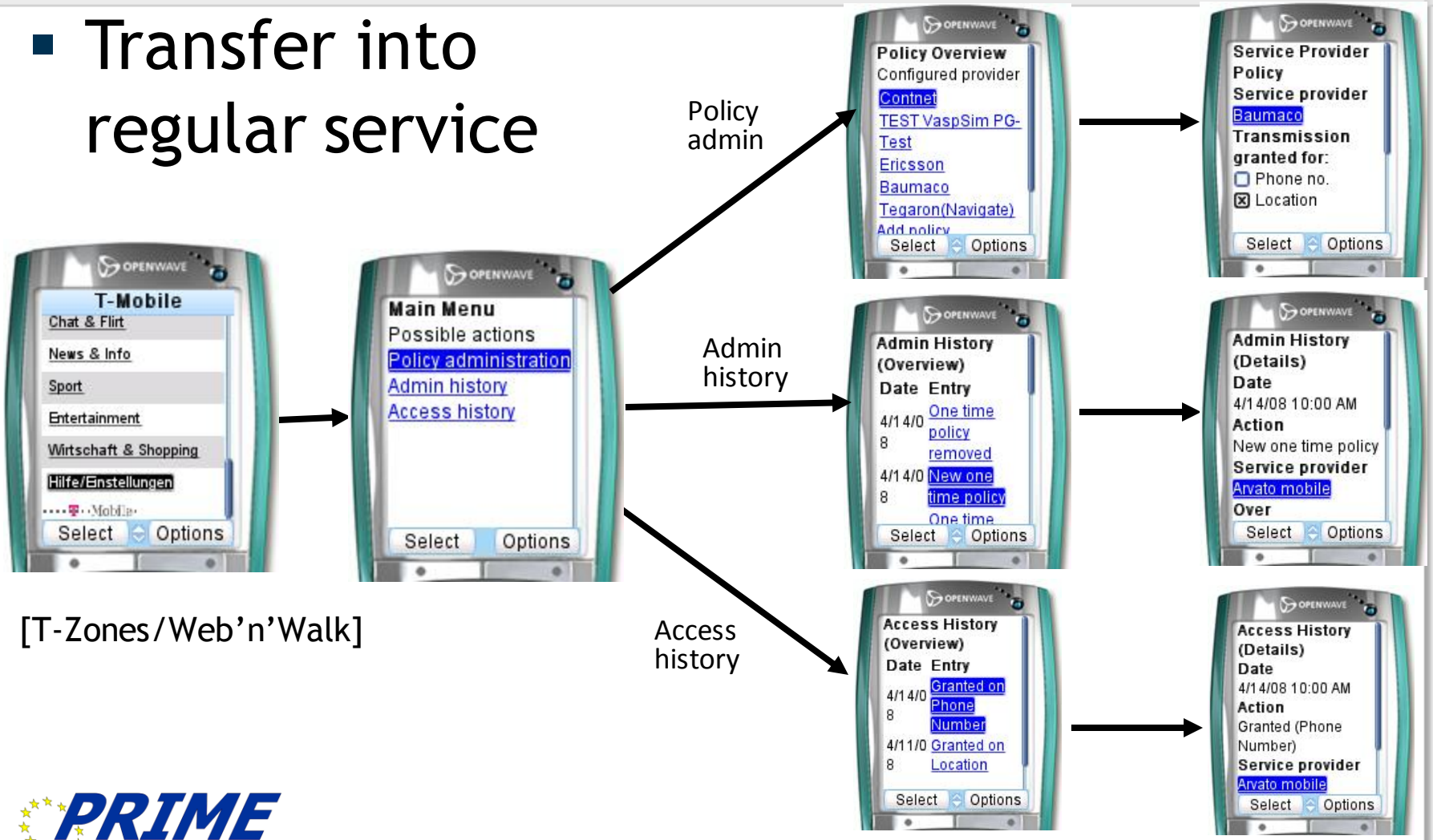


Privacy Gateway

- First transfers into the “real world”
  - „Privacy Gateway“ infrastructure component deployed at T-Mobile Germany and then Deutsche Telekom
  - Allows subscribers to set
    - Which application provider gets data?
    - On which days and times?
- Request for more power on the device for e.g. maintaining one’s own policies
- Computers reflect even closer one’s mind, e.g. one’s trust relations.

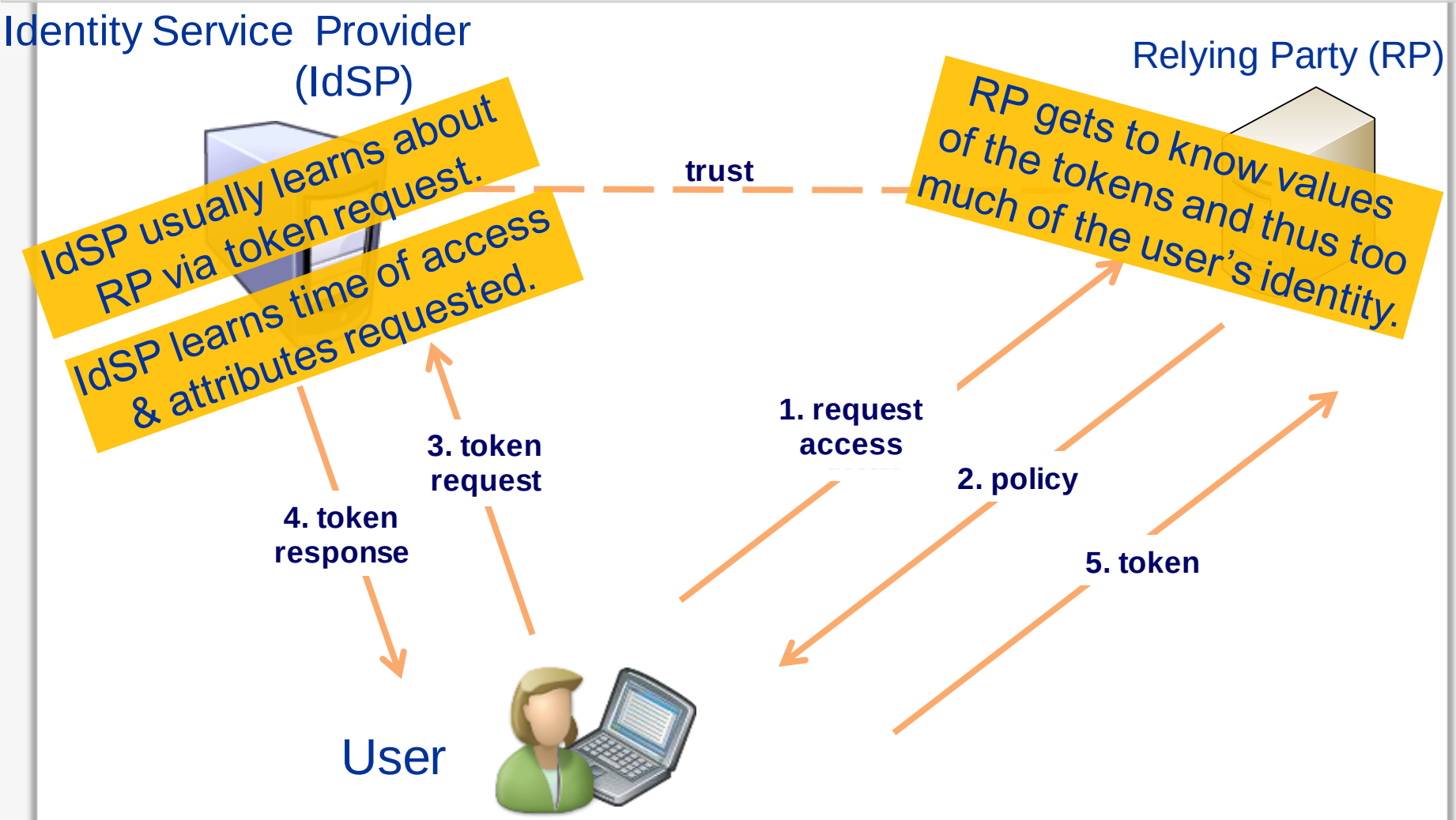
Privacy Gateway - User interface

- Transfer into regular service



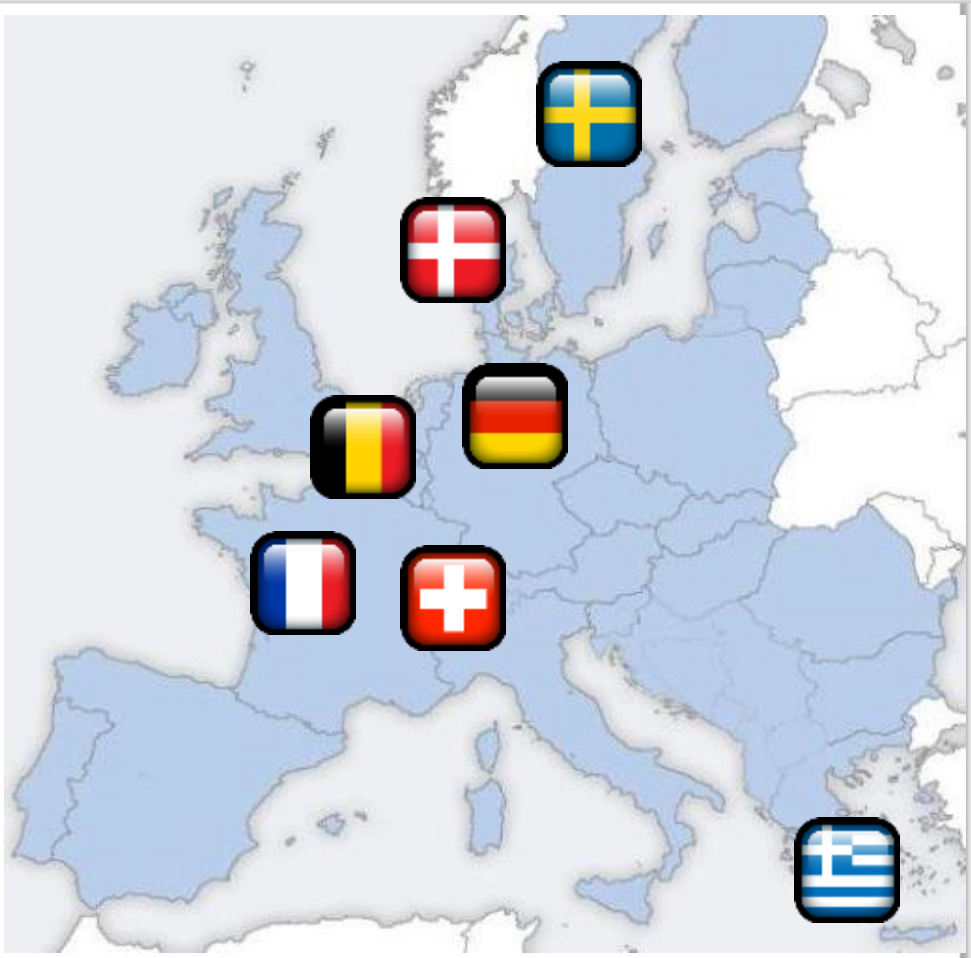
[T-Zones/Web'n'Walk]

Privacy (and security) issues of typical federated IdM architectures

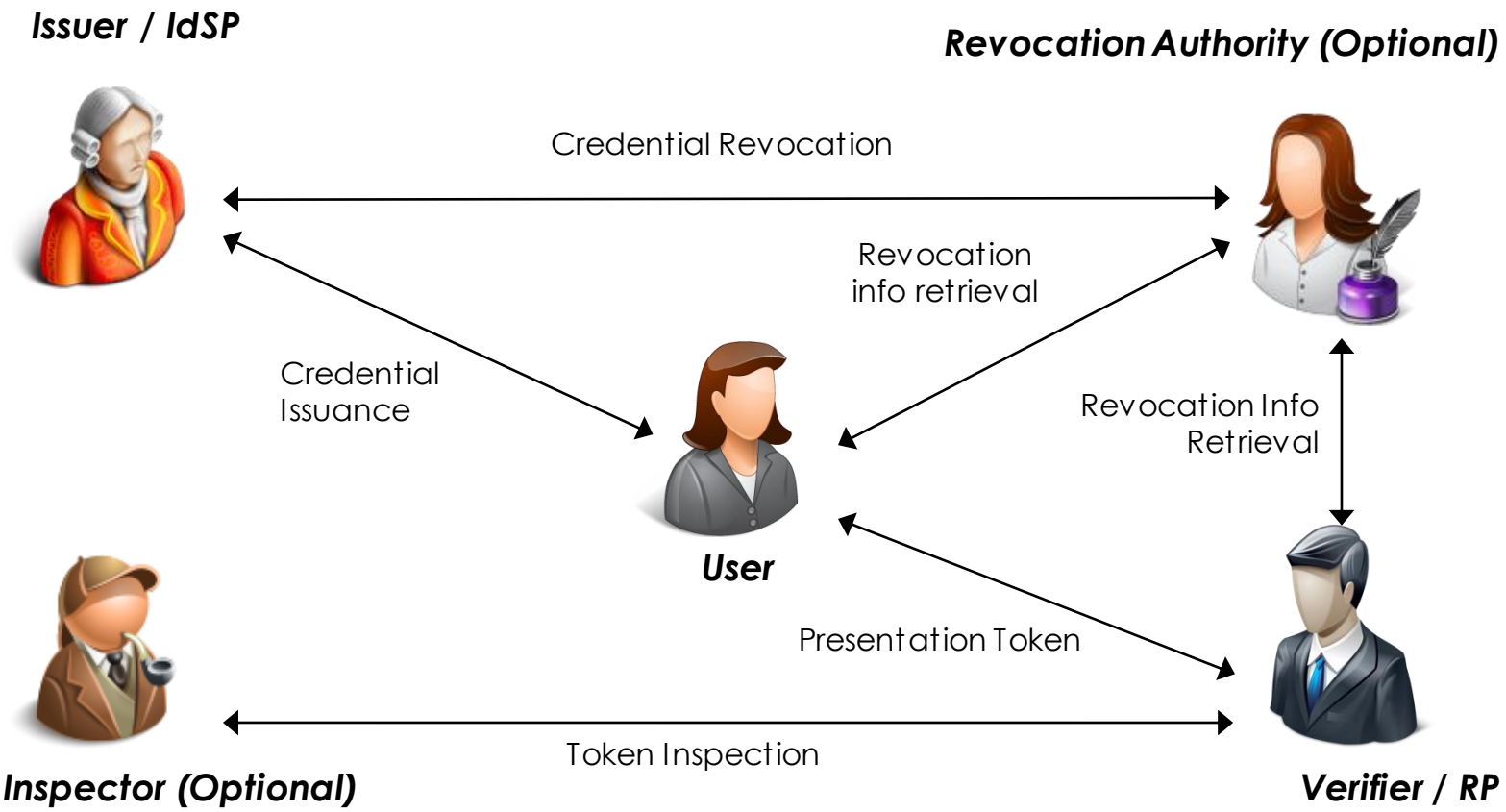


ABC4Trust

- Attribute-Based Credentials for Trust: https://www.abc4trust.eu
- Coordinated by Goethe University Frankfurt
- 12 partners from 7 countries.
- Objectives:
  - to define a common, unified architecture for ABC systems to allow comparing their respective features and combining them on common platforms, and
  - to deliver open reference implementations of selected ABC systems and deploy them in actual production pilots allowing provably accredited members of restricted communities to provide anonymous feedback on their community or its members.



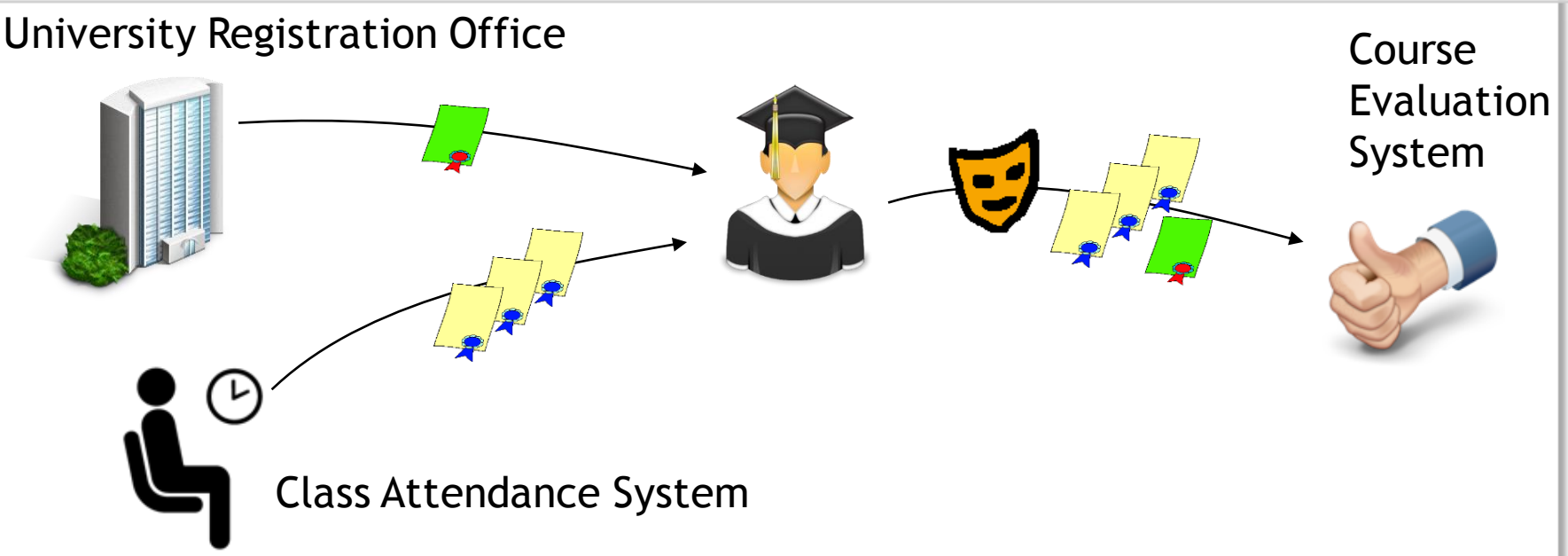
ABC4Trust architecture
High level view



ABC4Trust pilots

- ABC4Trust tested the technology in two pilots:
  - Anonymous course evaluation in the University of Patras, Greece.
    - Students used smartcards to collect credentials for the courses they are attending.
    - At the end of semester they were able to evaluate the course if they had attended a sufficient number of lectures.
    - Their votes will not be linkable to their identity while the technology prohibits them from voting multiple times.
  - Privacy preserving school community platform in Söderhamn, Sweden.
    - Providing online services such as chat rooms, consultations, advices, etc.
    - Pupils satisfying certain policies based on their attributes can access certain services, e.g. based on age, classroom, level, etc.

Anonymous course evaluation

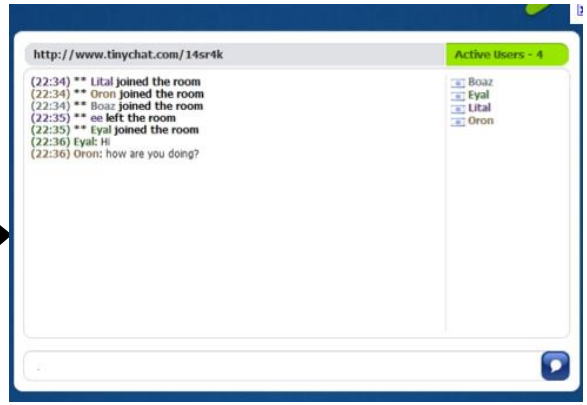


① The students receive a credential when they enrol in a course.
② The students anonymously collect credentials for attending each lecture of the courses.
③ At the end of semester they can prove that they have taken the course and participated at a sufficient number of lectures to be able to evaluate the course without disclosing their identity.

Privacy preserving school community platform

name = Kari Johannson
Grade= 5
Class = 5A
Gender = F

name = ?
Grade = 5
Class = ?



Privacy Advisor on top of Privacy-ABCs

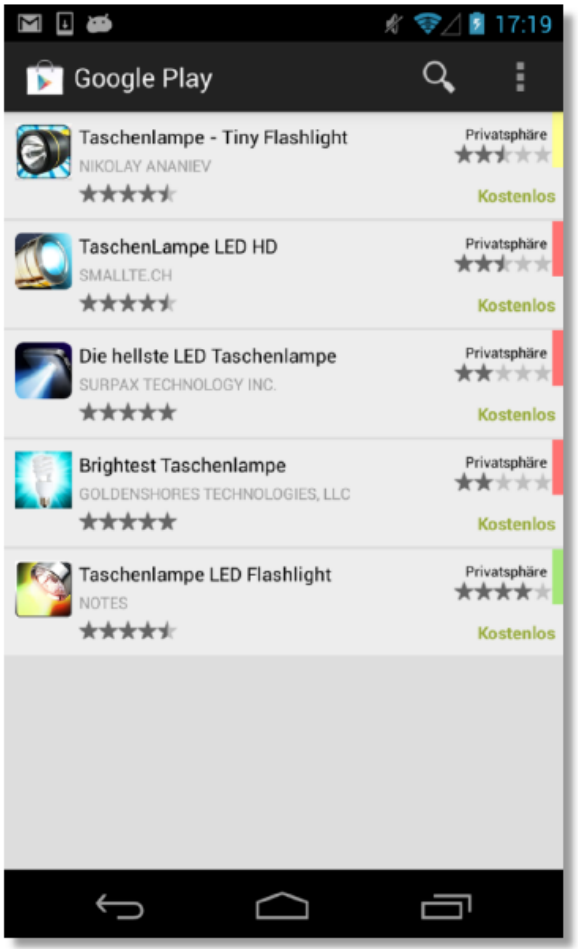
- Privacy advisor that helps users against potentially identity revelations while using privacy-preserving systems
- Automatic detection of privacy sensitive data
- Risk analysis
- Effective communication of the risk to users

Styx: Privacy risk communication method for smartphones

- **Styx Log.**
  - Information about information flows will be stored here. The monitoring component is responsible for creating new log entries.
- **Styx Pattern Collection.**
  - Since privacy impacts are modeled as behavioral patterns of apps. Styx must have access to a set of such privacy-impacting behavioral patterns in order to match application behavior with privacy impacts. Pre-defined patterns are stored in the pattern collection database.
- **Styx Pattern Detection.**
  - The actual matching between observed app behavior and PIBPs is performed by the Styx Pattern Detection engine. This component is triggered by the monitoring component after a new entry has been stored in the log.
- **Styx Notification.**
  - This component is responsible for notifying the user about matches that have been identified by the pattern detection.

Benefits of privacy risk communications

- An improved privacy-risk communication leads to:
  - increased privacy and risk awareness,
  - better comprehension of risks,
  - better comparison of apps,
  - privacy as a stronger decision factor,
  - safer app choices.



References I

[AbLa2007] Timothy G. Abbott, Katherine J. Lai, Michael R. Lieberman, Eric C. Price Browser-Based Attacks on Tor. In 7th International Symposium, PET 2007 Ottawa, Canada, June 20-22, 2007 Revised Selected Papers, pp 184-199.

[Allen2016] Allen & Overy: The EU General Data Protection Regulation is finally agreed, www.allenovery.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf

[BlaBorOlk2003] G. W. Blarkom, John J. Borking, and J.G. Olk. Handbook of Privacy and Privacy-Enhancing Technologies - PISA Privacy Incorporating Software Agent. The Hague, 2003.

[BVG83] Bundesverfassungsgericht: Entscheidung BVerfGE 65, 1 – Volkszählung; Urteil des Ersten Senats vom 15.12.1983 auf die mündliche Verhandlung vom 18. und 19. Oktober 1983 - 1 BvR 209, 269, 362, 420, 440, 484/83 in den Verfahren über die Verfassungsbeschwerden, www.datenschutz-berlin.de/gesetze/ sonstige/volksz.htm, accessed 2007-03-02.

[Cavoukian2009] Privacy by Design The 7 Foundational Principles, https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

[Chaum1981] David Chaum: *Untraceable Electronic Mail, Return addresses, and Digital Pseudonyms*; Communications of the ACM February 1981 Volume 24 Number 2

[CPDP2014] Privacy by Design: Effective Privacy Management in the Victorian public sector, Commissioner for Privacy and Data Protection (CPDP), 2014.

[Danezis2014] Privacy and Data Protection by Design – from policy to engineering, 2014.

References II

[Europe2006] European Parliament and the Council: Directive 2006/24/EC of the European Parliament and of the council; https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF

[EU2016] European Union: REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); Official Journal of the European Union L 119/1, 4.5.2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

[Gürses2016] Privacy Engineering: Shaping an Emerging Field of Research and Practice, IEEE Symposium on Security and Privacy, 2016.

[ISO 9241-11:2018] Ergonomics of human-system interaction — Part 11: Usability: Definitions and concepts

[ISO/IEC 29100:2011] Information technology – Security techniques – Privacy framework; http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

[NationalAcademy2010] Steering Committee on the Usability, Security, and Privacy of Computer Systems: "Toward Better Usability, Security, and Privacy of Information Technology: Report of a Workshop", Report of a Workshop in July 2009, The National Academy Press, Washington DC, 2010, http://www.stern.nyu.edu/networks/Toward_Better_Usability_Security_and_Privacy_of_Information_Technology.pdf

[Rannenberg2000] Kai Rannenberg: Multilateral Security – A concept and examples for balanced security; Pp. 151-162 in: Proceedings of the 9th ACM New Security Paradigms Workshop 2000, September 19-21, 2000 Cork, Ireland; ACM Press; ISBN 1-58113-260-3