mobile business

Lecture 8

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Information & Communication Security (SS 16)

Privacy Protection

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
- Integrated Privacy Protection
  - Privacy by Design (PbD)
  - PRIME LBS
  - ABC4Trust
  - Privacy Advisor
  - Privacy Risk Communication and Mitigation

Data Protection and Privacy

- Both terms are related but not synonymous and have many definitions.
- 2 popular ones:
  - **Data protection** is the protection from harmful and unsolicited usage of data linked to the personal sphere of a person.
  - **Privacy** is the right to be left alone, e.g. to be unwatched or anonymous [WaBr1890].
- More work needed on a complete understanding of privacy
- Nevertheless the topic is important, as one can see from related incidents and activities to address the issue.

The Origin of Data Protection?

- The term "Privacy" ('the right to be left alone') originates from Warren & Brandeis [WaBr1890].
- Data protection in Germany ("Datenschutz") originates from concerns over too much information and power in the hands of large (governmental) institutions ("**Big Brother**").
- Nowadays Data protection and Privacy in Germany are based on the right of informational self determination derived from the constitution in the "Volkszählungsurteil" [BVG1983]).
- ***Germany has one of the most advanced infrastructures for Privacy*** but still no established German language term for Privacy beyond the (misleading) "Datenschutz".
- Some (more or less established) related terms are:
  - Privatheit
  - Privatsphäre
  - Schutz der Privatsphäre

EU General Data Protection Regulation (GDPR)

- The EC adopted a new EU legal framework on the protection of personal data.
- The regulation will enter into force on 24 May 2016, it shall apply from 25 May 2018.
- The European Commission says that the regulation “puts the citizens back in control of their data, notably through”:
  - A right to be forgotten: Users will have the right to demand that data about them be deleted if there are no "legitimate grounds" for it to be kept.
  - People will have easier access to their own data, and will find it easier to transfer it from one service provider to another.
  - Putting people in control
    - Organizations must notify the authorities about data breaches as early as possible, "if feasible within 24 hours”.
    - In cases where consent is required organizations must explicitly ask for permission to process data, rather than assume it.
  - Privacy by design and by default – privacy friendly default settings to be the norm.

[EU2016]

GDPR Principles I

- **Lawfulness, fairness and transparency:** personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.
- **Purpose limitation:** personal data must collected for specified explicit and legitimate purposes.
- **Data minimisation:** personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- **Accuracy:** personal data must accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

[EU2016]

GDPR Principles II

- **Storage limitation:** personal data must kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- **Integrity and confidentiality:** personal data must be processed in a way that ensures appropriate security of the personal data.
- **Accountability:** The controller shall be responsible for and be able to demonstrate compliance to the principles mentioned above.

[EU2016]

mobile business

Principle of Accountability in the GDPR

- The controller shall be responsible for and be able to demonstrate compliance to the regulation to:
  - maintain certain documentation,
  - conduct a data protection impact assessment for more risky processing (data controllers should compile lists of what is caught), and
  - implement data protection by design and by default, e.g., data minimisation.

[EU2016] [Allen2016]

Law Alone is not Sufficient

- The increased usage of IT systems and networks leads to
  - huge amounts of data
  - easily searchable data
  - automatic analysis,
  - and knowledge extraction
- Data protection / Privacy law alone not sufficient
  - Not all processing can be controlled (e.g. every network node).
  - Deliberate breaking and bending of law (different legislations on the internet)
  - Economic pressure can force customers to give consent to almost any kind of ‘privacy’ policy (e.g. selling privacy for “peanuts”).
- Slow pace of privacy self-regulation in the US, Focus on self-help
  - Self regulation by sustaining user ignorance
  - Enforcing norms may violate anti-trust.
  - Being a good actor (e.g. by exposing privacy practices) increases liability.
  - Legal compliance and related business processes (deemed) expensive

[Reagle1998, SelfReg1999, Bell2001, Hoofnagle2005]

⇨ Technical Privacy Protection
⇨ Standardization

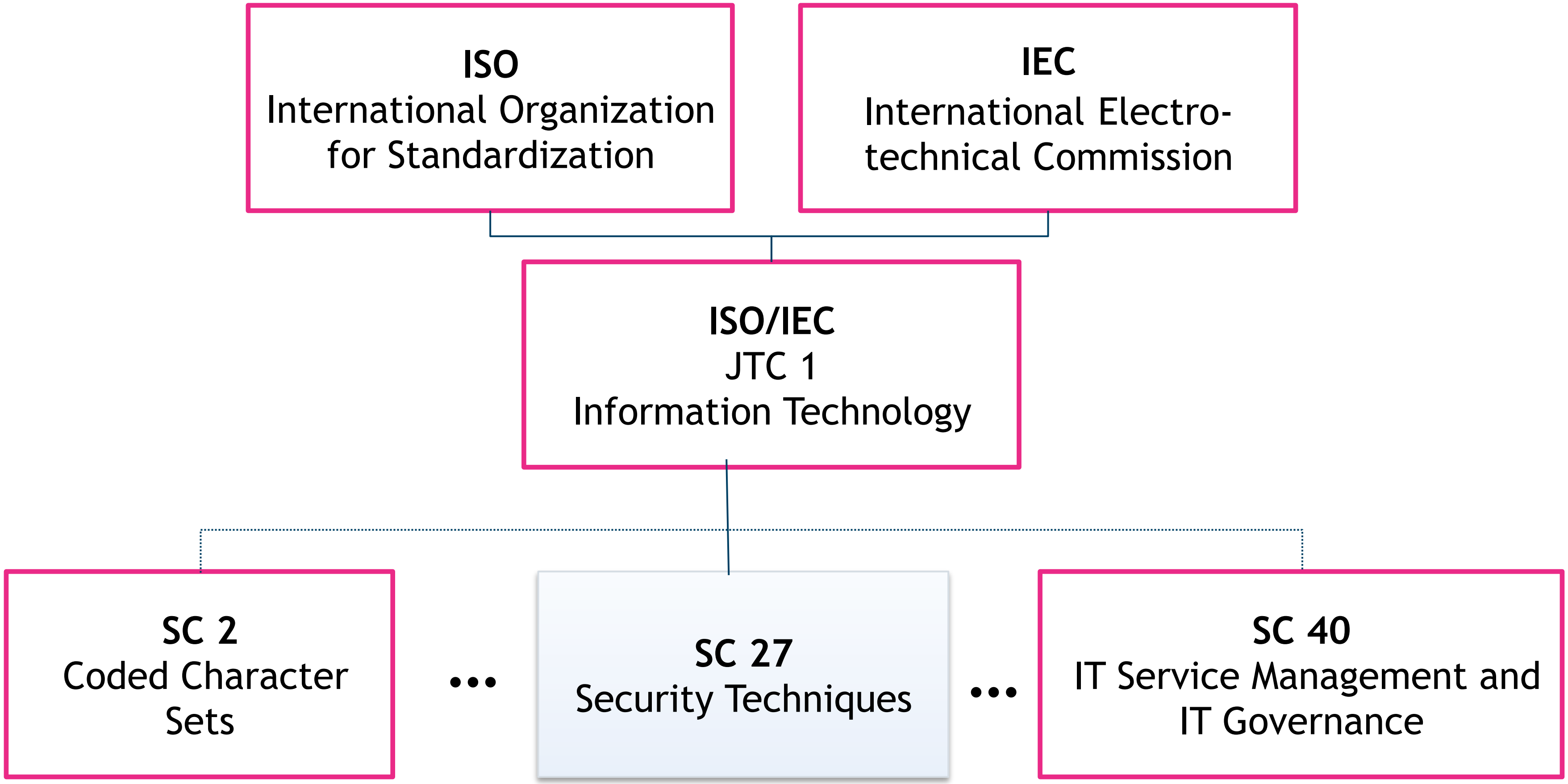
Privacy principles and standardization

ISO/IEC IS 29100:2011 Privacy Framework defines the following privacy principles:

1. Consent and choice
2. Purpose legitimacy and specification
3. Collection limitation
4. Data minimization
5. Use, retention and disclosure limitation
6. Accuracy and quality
7. Openness, transparency and notice
8. Individual participation and access
9. Accountability
10. Information security
11. Privacy compliance

[ISO/IEC 29100:2011]

SC 27 “IT Security Techniques” within ISO/IEC JTC1



ISO
International Organization for Standardization

IEC
International Electrotechnical Commission

ISO/IEC
JTC 1
Information Technology

SC 2
Coded Character Sets

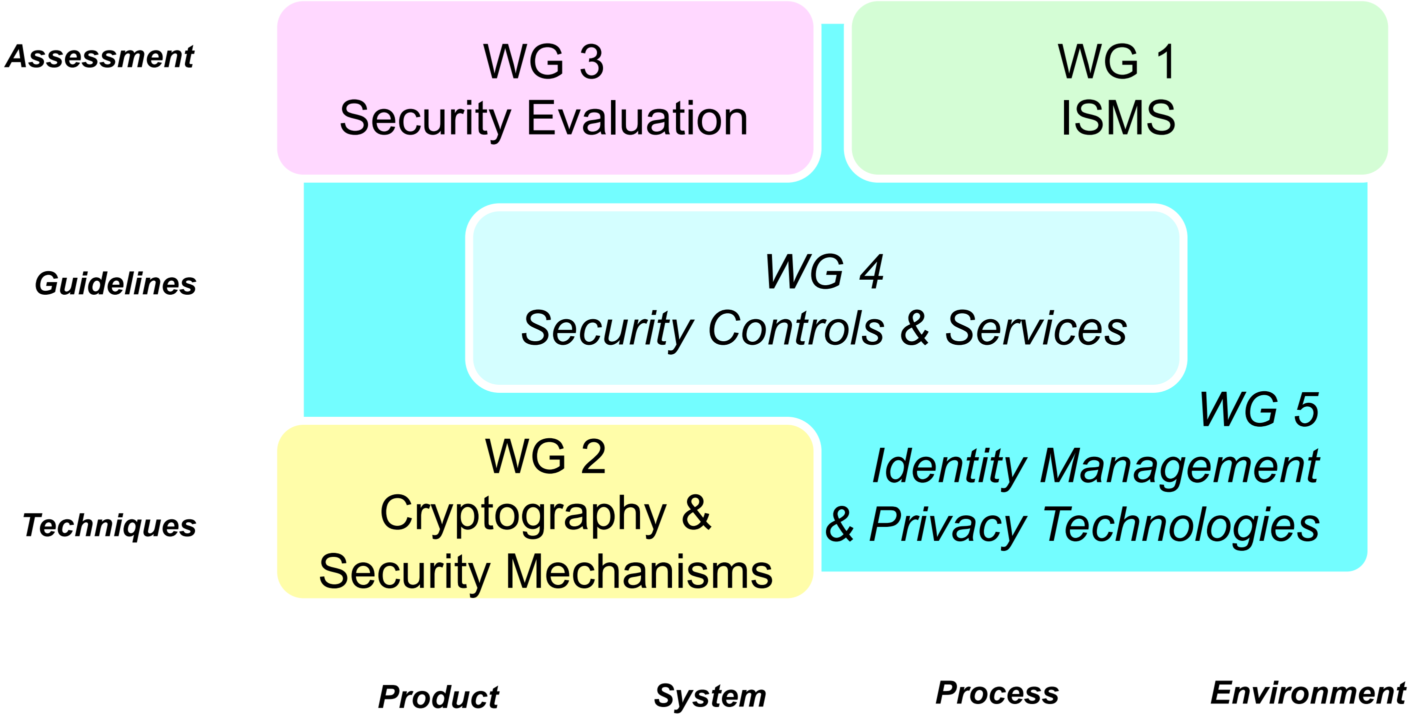
•••

SC 27
Security Techniques

•••

SC 40
IT Service Management and IT Governance

WGs within ISO/IEC JTC 1/SC 27 – IT Security Techniques



Assessment

WG 3
Security Evaluation

WG 1
ISMS

Guidelines

WG 4
Security Controls & Services

WG 5
Identity Management
& Privacy Technologies

Techniques

WG 2
Cryptography &
Security Mechanisms

Product

System

Process

Environment

WG 5 Identity Management & Privacy Technologies Programme of Work (2008-04)

Frameworks & Architectures

- A Framework for Identity Management (ISO/IEC 24760, WD)
- A Privacy Framework (ISO/IEC 29100, WD)
- A Privacy Reference Architecture (ISO/IEC 29101, WD)
- A Framework for Access Management (ISO/IEC 29146, WD)

Protection Concepts

- Biometric template protection (ISO/IEC 24745, WD)
- Access Control Mechanisms (Study Period)

Guidance on Context and Assessment

- Authentication Context for Biometrics (ISO/IEC 24761, FDIS)
- Entity Authentication Assurance (ISO/IEC 29115, WD)
- Privacy Capability Maturity Models (Study Period)

WG 5 Identity Management & Privacy Technologies
Programme of Work (2010-10)

Frameworks & Architectures

- A Framework for Identity Management (ISO/IEC 24760, FCD, WD, WD)
- Privacy Framework (ISO/IEC 29100, FCD)
- Privacy Reference Architecture (ISO/IEC 29101, CD)
- Entity Authentication Assurance Framework (ISO/IEC 29115 / ITU-T X.eaa, CD)
- A Framework for Access Management (ISO/IEC 29146, WD)

Protection Concepts

- Biometric information protection (ISO/IEC 24745, FDIS)
- Requirements for partially anonymous, partially unlinkable authentication (ISO/IEC 29191, CD)

Guidance on Context and Assessment

- Authentication Context for Biometrics (ISO/IEC 24761, IS)
- Privacy Capability Assessment Model (ISO/IEC 29190, WD)

WG 5 Identity Management & Privacy Technologies Programme of Work (2012-05)

Frameworks & Architectures

- A Framework for Identity Management (ISO/IEC 24760, IS, WD, WD)
- Privacy Framework (ISO/IEC 29100, IS)
- Privacy Architecture Framework (ISO/IEC 29101, CD)
- Entity Authentication Assurance Framework (ISO/IEC 29115 / ITU-T X.1254 (formerly X.eaa), DIS)
- A Framework for Access Management (ISO/IEC 29146, WD)
- Telebiometric authentication framework using biometric hardware security module (ITU-T X.bhsm | ISO/IEC 17922, WD)

Protection Concepts

- Biometric information protection (ISO/IEC 24745, IS)
- Requirements for partially anonymous, partially unlinkable authentication (ISO/IEC 29191, CD)

Guidance on Context and Assessment

- Authentication Context for Biometrics (ISO/IEC 24761, IS)
- Privacy Capability Assessment Model (ISO/IEC 29190, WD)
- Code of practice for data protection controls for public cloud computing services (ISO/IEC 27018, WD)
- Identity Proofing (NWIP)
- Privacy impact assessment – methodology (NWIP)

WG 5 Identity Management & Privacy Technologies Programme of Work (2014-10)

Frameworks & Architectures

- A Framework for Identity Management (ISO/IEC 24760, IS, FDIS, CD)
- Privacy Framework (ISO/IEC 29100, IS)
- Privacy Architecture Framework (ISO/IEC 29101, IS)
- Entity Authentication Assurance Framework (ISO/IEC 29115, IS)
- A Framework for Access Management (ISO/IEC 29146, CD)
- Telebiometric authentication framework using biometric hardware security module (ITU-T X. 1085 | ISO/IEC 17922, CD) (formerly X.bhsm)

Protection Concepts

- Biometric information protection (ISO/IEC 24745, IS)
- Requirements for partially anonymous, partially unlinkable authentication (ISO/IEC 29191, IS)

Guidance on Context and Assessment

- Authentication Context for Biometrics (ISO/IEC 24761, IS)
- Privacy Capability Assessment Model (ISO/IEC 29190, IS)
- Code of practice for PII protection in public clouds acting as PII processors (ISO/IEC 27018, IS)
- Identity Proofing (ISO/IEC 29003, WD)
- Privacy impact assessment – Methodology (ISO/IEC 29134, WD)
- Code of practice for the protection of personally identifiable information (ISO/IEC 29151, WD)

WG 5 Identity Management & Privacy Technologies Programme of Work (2016-05)

Frameworks & Architectures

- A framework for identity management (ISO/IEC 24760 (Parts 1-3), IS:2011, IS:2015, FDIS approved, publication being prepared)
- Privacy framework (ISO/IEC 29100, IS:2011)
- Privacy architecture framework (ISO/IEC 29101, IS:2013)
- Entity authentication assurance framework (ISO/IEC 29115, IS:2013)
- A framework for access management (ISO/IEC 29146, FDIS approved, publication being prepared)
- Telebiometric authentication framework using biometric hardware security module (ITU-T X.1085 | ISO/IEC 17922, DIS) (formerly X.bhsm)

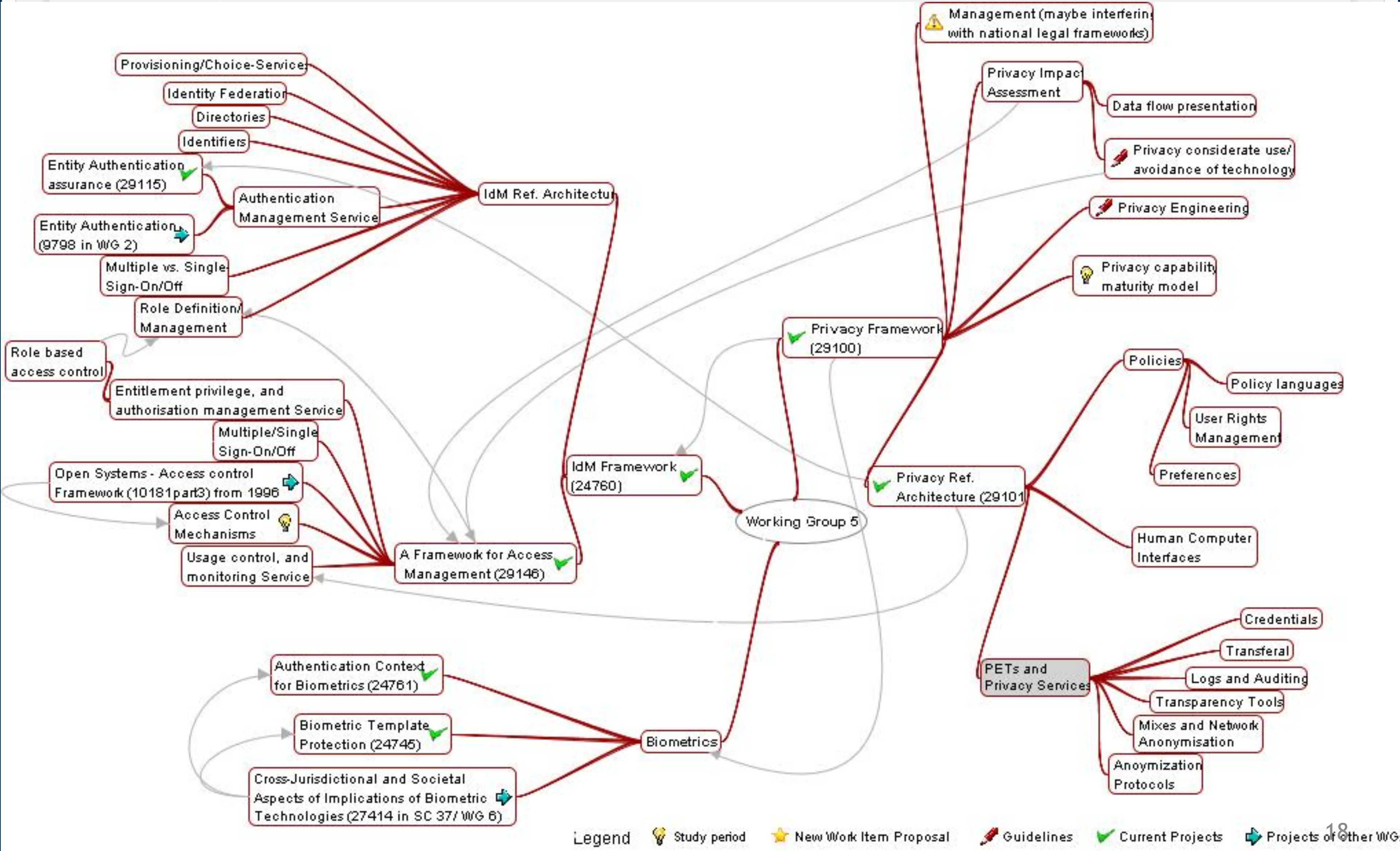
Protection Concepts

- Biometric information protection (ISO/IEC 24745, IS:2011)
- Requirements for partially anonymous, partially unlinkable authentication (ISO/IEC 29191, IS:2012)

Guidance on Context and Assessment

- Authentication context for biometrics (ISO/IEC 24761, IS:2009/Cor 1:2013, Revision WD)
- Privacy capability assessment model (ISO/IEC 29190, IS:2015)
- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors (ISO/IEC 27018, IS:2014)
- Identity proofing (ISO/IEC 29003, CD)
- Privacy impact assessment – methodology (ISO/IEC 29134, DIS)
- Code of practice for PII protection (ITU-T X.gpim | ISO/IEC 29151, DIS)
- Privacy enhancing data de-identification techniques (ISO/IEC 20889, WD)
- Guidelines for online privacy notice and consent (ISO/IEC 29184, WD)

WG 5 Identity Management & Privacy Technologies Roadmap (2008-04)



Working Group 5

IdM Ref. Architectur

Provisioning/Choice-Service

Identity Federatior

Directories

Identifiers

Authentication Management Service

Entity Authentication assurance (29115) ✓

Entity Authentication (9798 in WG 2) ⇨

Multiple vs. Single-Sign-On/Off

Role Definition/ Management

Role based access control

IdM Framework (24760) ✓

A Framework for Access Management (29146) ✓

Entitlement privilege, and authorisation management Service

Multiple/Single Sign-On/Off

Open Systems - Access control Framework (10181part3) from 1996 ⇨

Access Control Mechanisms 💡

Usage control, and monitoring Service

Privacy Framework (29100) ✓

⚠ Management (maybe interfering with national legal frameworks)

Privacy Impact Assessment

Data flow presentation

Privacy considerate use/ avoidance of technology

Privacy Engineering

💡 Privacy capability maturity model

Privacy Ref. Architecture (29101 ✓

Policies

Policy languages

User Rights Management

Preferences

Human Computer Interfaces

PETs and Privacy Services

Credentials

Transferal

Logs and Auditing

Transparency Tools

Mixes and Network Anonymisation

Anoymization Protocols

Biometrics

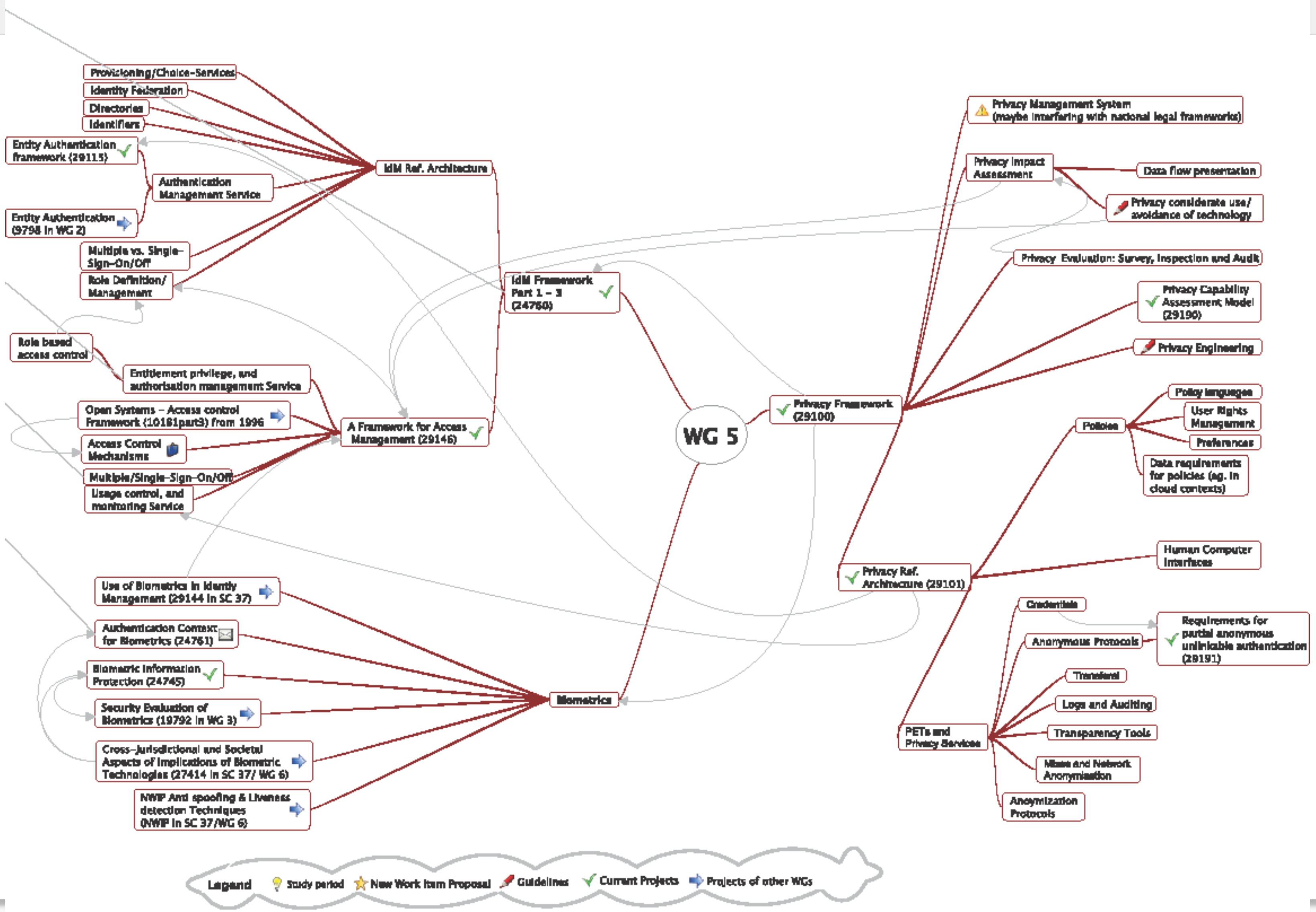
Authentication Context for Biometrics (24761) ✓

Biometric Template Protection (24745) ✓

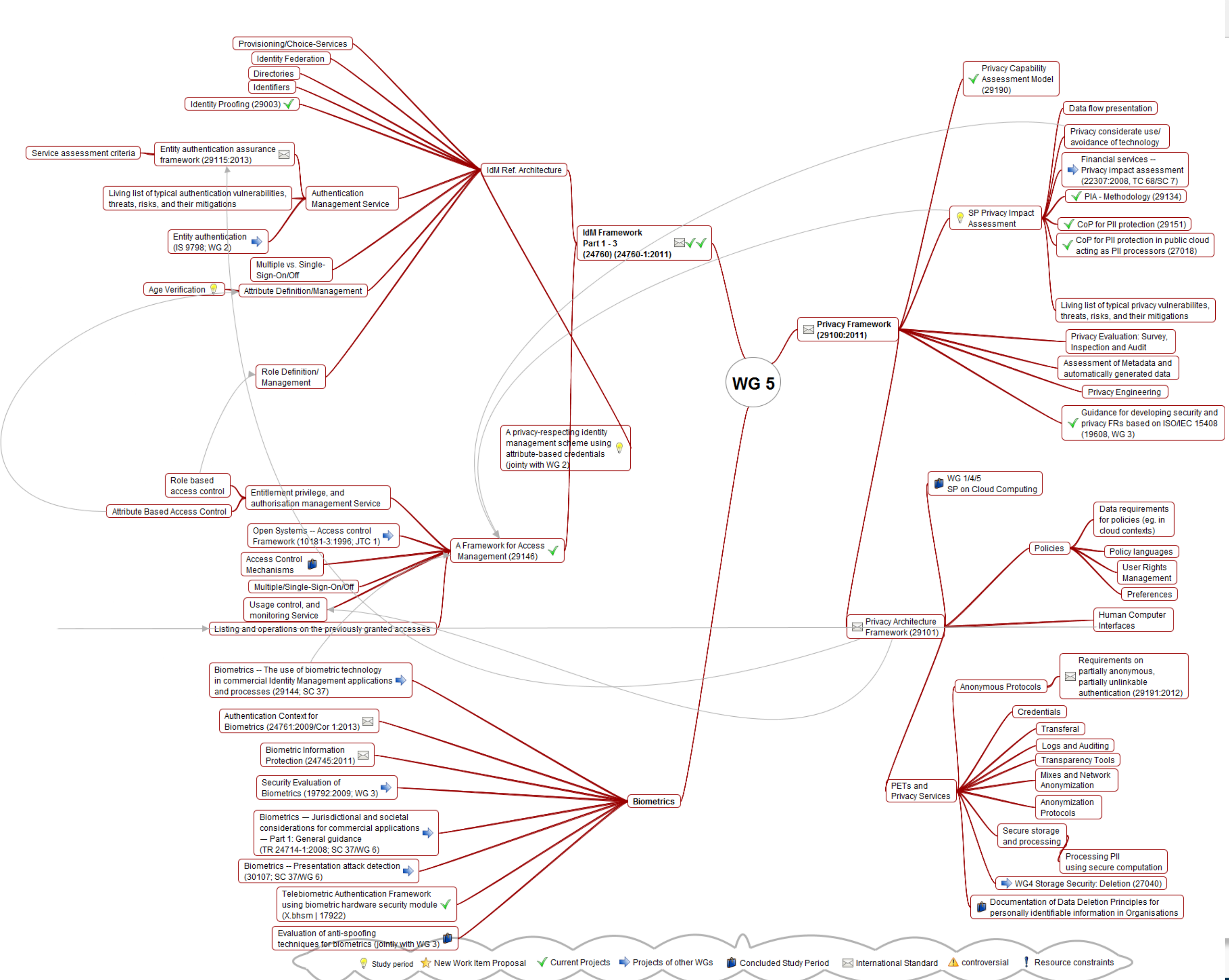
Cross-Jurisdictional and Societal Aspects of Implications of Biometric Technologies (27414 in SC 37/ WG 6) ⇨

Legend 💡 Study period ⭐ New Work Item Proposal Guidelines ✓ Current Projects ⇨ Projects of other WG

WG 5 Identity Management & Privacy Technologies Roadmap (2010-10)


WG 5
IdM Ref. Architecture
Provisioning/Choice-Services
Identity Federation
Directories
Identifiers
Entity Authentication framework (29115) ✓
Authentication Management Service
Entity Authentication (9798 in WG 2)
Multiple vs. Single-Sign-On/Off
Role Definition/ Management
IdM Framework Part 1 – 3 (24760) ✓
Role based access control
Entitlement privilege, and authorisation management Service
Open Systems – Access control Framework (10181part3) from 1996
Access Control Mechanisms
Multiple/Single-Sign-On/Off
Usage control, and monitoring Service
A Framework for Access Management (29146) ✓
Biometrics
Use of Biometrics in Identity Management (29144 in SC 37)
Authentication Context for Biometrics (24761)
Biometric Information Protection (24745) ✓
Security Evaluation of Biometrics (19792 in WG 3)
Cross-Jurisdictional and Societal Aspects of Implications of Biometric Technologies (27414 in SC 37/ WG 6)
NWIP Anti spoofing & Liveness detection Techniques (NWIP in SC 37/WG 6)
Privacy Framework (29100) ✓
Privacy Management System (maybe interfering with national legal frameworks)
Privacy Impact Assessment
Data flow presentation
Privacy considerate use/ avoidance of technology
Privacy Evaluation: Survey, Inspection and Audit
Privacy Capability Assessment Model (29190) ✓
Privacy Engineering
Policies
Policy languages
User Rights Management
Preferences
Data requirements for policies (eg. in cloud contexts)
Privacy Ref. Architecture (29101) ✓
Human Computer Interfaces
PETs and Privacy Services
Credentials
Anonymous Protocols
Requirements for partial anonymous unlinkable authentication (29191) ✓
Transferal
Logs and Auditing
Transparency Tools
Mixes and Network Anonymisation
Anonymization Protocols
Legend
Study period
New Work Item Proposal
Guidelines
✓ Current Projects
Projects of other WGs

WG 5 Identity Management & Privacy Technologies Roadmap (2014-09)



WG 5

IdM Ref. Architecture
Provisioning/Choice-Services
Identity Federation
Directories
Identifiers
Identity Proofing (29003) ✓
Authentication Management Service
Entity authentication assurance framework (29115:2013)
Service assessment criteria
Living list of typical authentication vulnerabilities, threats, risks, and their mitigations
Entity authentication (IS 9798; WG 2)
Multiple vs. Single-Sign-On/Off
Attribute Definition/Management
Age Verification
Role Definition/ Management

IdM Framework Part 1 - 3 (24760) (24760-1:2011) ✓✓

A privacy-respecting identity management scheme using attribute-based credentials (jointly with WG 2)

A Framework for Access Management (29146) ✓
Role based access control
Attribute Based Access Control
Entitlement privilege, and authorisation management Service
Open Systems -- Access control Framework (10181-3:1996; JTC 1)
Access Control Mechanisms
Multiple/Single-Sign-On/Off
Usage control, and monitoring Service
Listing and operations on the previously granted accesses

Biometrics
Biometrics -- The use of biometric technology in commercial Identity Management applications and processes (29144; SC 37)
Authentication Context for Biometrics (24761:2009/Cor 1:2013)
Biometric Information Protection (24745:2011)
Security Evaluation of Biometrics (19792:2009; WG 3)
Biometrics — Jurisdictional and societal considerations for commercial applications — Part 1: General guidance (TR 24714-1:2008; SC 37/WG 6)
Biometrics -- Presentation attack detection (30107; SC 37/WG 6)
Telebiometric Authentication Framework using biometric hardware security module ✓ (X.bhsm | 17922)
Evaluation of anti-spoofing techniques for biometrics (jointly with WG 3)

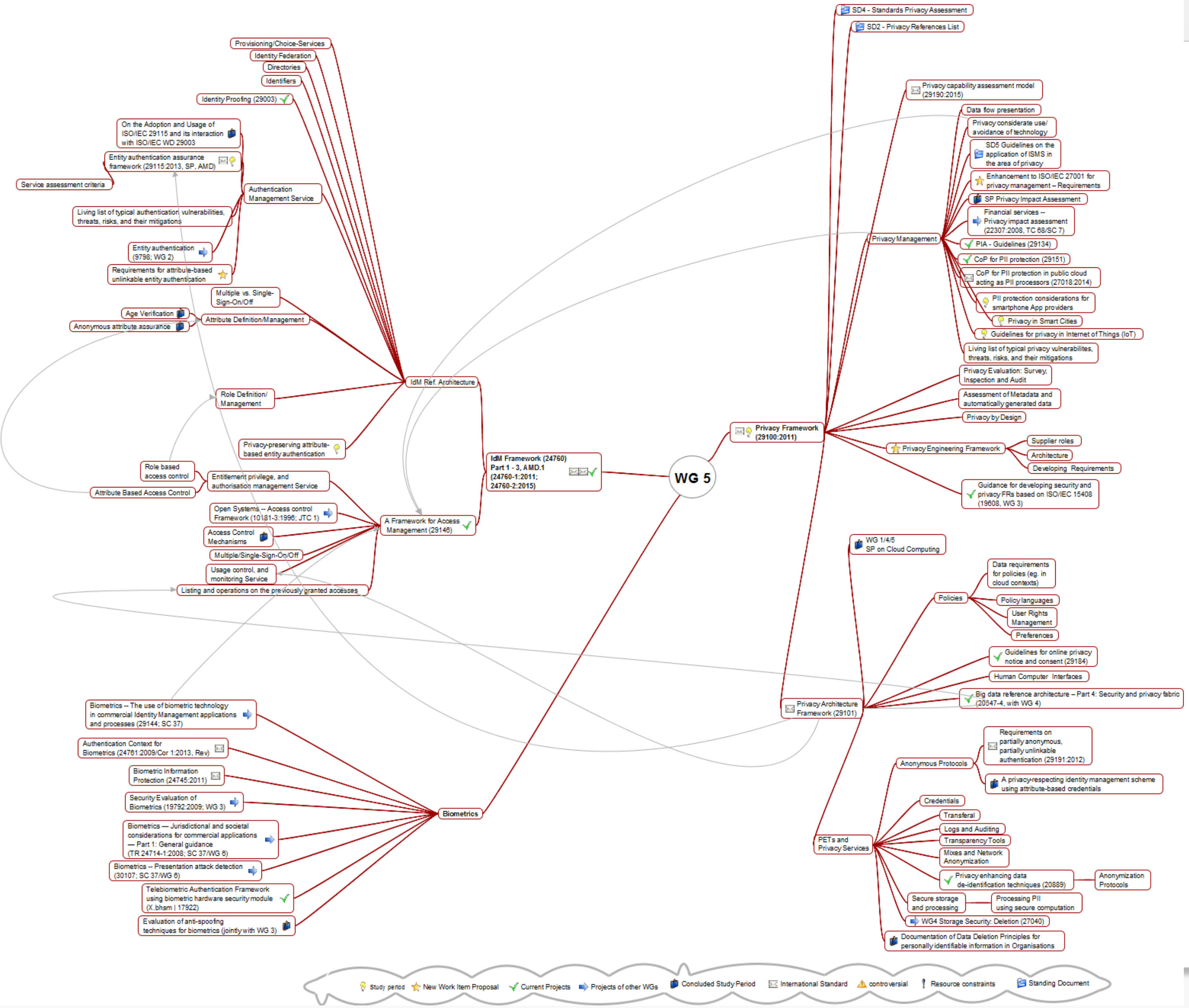
Privacy Framework (29100:2011)
Privacy Capability Assessment Model (29190) ✓
SP Privacy Impact Assessment
Data flow presentation
Privacy considerate use/ avoidance of technology
Financial services -- Privacy impact assessment (22307:2008, TC 68/SC 7)
✓ PIA - Methodology (29134)
✓ CoP for PII protection (29151)
✓ CoP for PII protection in public cloud acting as PII processors (27018)
Living list of typical privacy vulnerabilites, threats, risks, and their mitigations
Privacy Evaluation: Survey, Inspection and Audit
Assessment of Metadata and automatically generated data
Privacy Engineering
✓ Guidance for developing security and privacy FRs based on ISO/IEC 15408 (19608, WG 3)

Privacy Architecture Framework (29101)
WG 1/4/5 SP on Cloud Computing
Policies
Data requirements for policies (eg. in cloud contexts)
Policy languages
User Rights Management
Preferences
Human Computer Interfaces

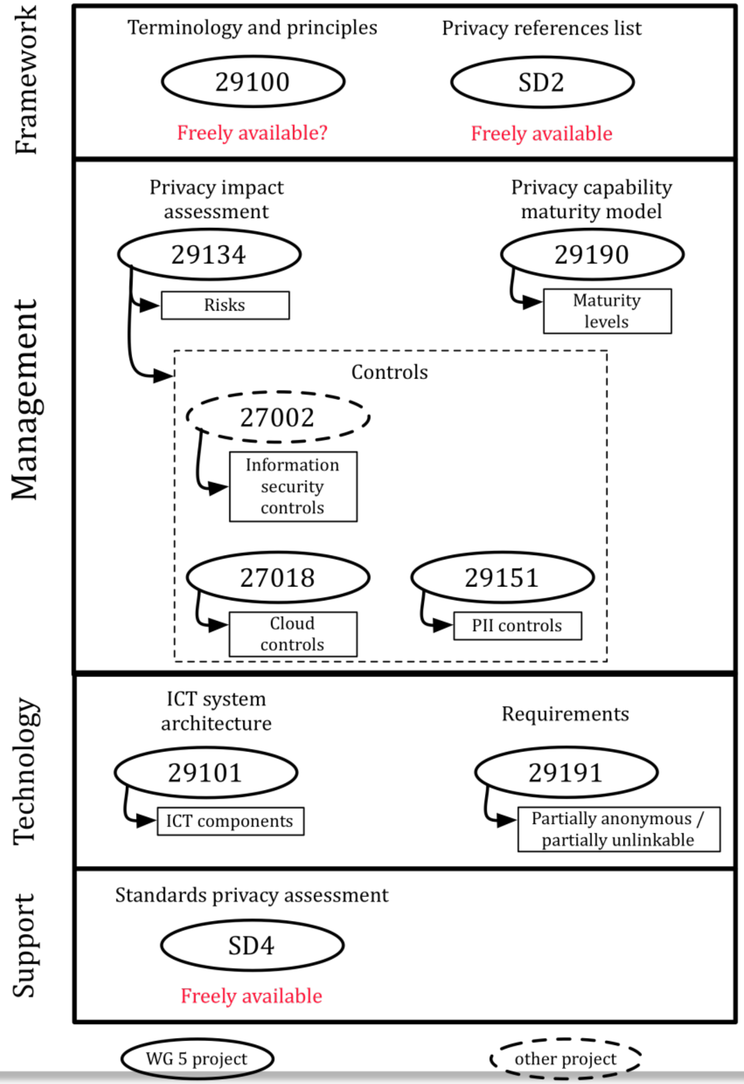
PETs and Privacy Services
Anonymous Protocols
Requirements on partially anonymous, partially unlinkable authentication (29191:2012)
Credentials
Transferal
Logs and Auditing
Transparency Tools
Mixes and Network Anonymization
Anonymization Protocols
Secure storage and processing
Processing PII using secure computation
WG4 Storage Security: Deletion (27040)
Documentation of Data Deletion Principles for personally identifiable information in Organisations

Study period ☆ New Work Item Proposal ✓ Current Projects ➡ Projects of other WGs Concluded Study Period ✉ International Standard ⚠ controversial ! Resource constraints

WG 5 Identity Management & Privacy Technologies
Roadmap (2016-05)


WG 5
IdM Framework (24760) Part 1 - 3, AMD.1 (24760-1:2011; 24760-2:2015)
IdM Ref. Architecture
Provisioning/Choice-Services
Identity Federation
Directories
Identifiers
Identity Proofing (29003)
Authentication Management Service
On the Adoption and Usage of ISO/IEC 29115 and its interaction with ISO/IEC WD 29003
Entity authentication assurance framework (29115:2013, SP, AMD)
Service assessment criteria
Living list of typical authentication vulnerabilities, threats, risks, and their mitigations
Entity authentication (9798; WG 2)
Requirements for attribute-based unlinkable entity authentication
Multiple vs. Single-Sign-On/Off
Attribute Definition/Management
Age Verification
Anonymous attribute assurance
Role Definition/ Management
Privacy-preserving attribute-based entity authentication
A Framework for Access Management (29146)
Entitlement privilege, and authorisation management Service
Role based access control
Attribute Based Access Control
Open Systems -- Access control Framework (10181-3:1996; JTC 1)
Access Control Mechanisms
Multiple/Single-Sign-On/Off
Usage control, and monitoring Service
Listing and operations on the previously granted accesses
Biometrics
Biometrics -- The use of biometric technology in commercial Identity Management applications and processes (29144; SC 37)
Authentication Context for Biometrics (24761:2009/Cor 1:2013, Rev)
Biometric Information Protection (24745:2011)
Security Evaluation of Biometrics (19792:2009; WG 3)
Biometrics — Jurisdictional and societal considerations for commercial applications — Part 1: General guidance (TR 24714-1:2008; SC 37/WG 6)
Biometrics -- Presentation attack detection (30107; SC 37/WG 6)
Telebiometric Authentication Framework using biometric hardware security module (X.bhsm | 17922)
Evaluation of anti-spoofing techniques for biometrics (jointly with WG 3)
Privacy Framework (29100:2011)
SD4 - Standards Privacy Assessment
SD2 - Privacy References List
Privacy Management
Privacy capability assessment model (29190:2015)
Data flow presentation
Privacy considerate use/ avoidance of technology
SD5 Guidelines on the application of ISMS in the area of privacy
Enhancement to ISO/IEC 27001 for privacy management – Requirements
SP Privacy Impact Assessment
Financial services -- Privacy impact assessment (22307:2008, TC 68/SC 7)
PIA - Guidelines (29134)
CoP for PII protection (29151)
CoP for PII protection in public cloud acting as PII processors (27018:2014)
PII protection considerations for smartphone App providers
Privacy in Smart Cities
Guidelines for privacy in Internet of Things (IoT)
Living list of typical privacy vulnerabilites, threats, risks, and their mitigations
Privacy Evaluation: Survey, Inspection and Audit
Assessment of Metadata and automatically generated data
Privacy by Design
Privacy Engineering Framework
Supplier roles
Architecture
Developing Requirements
Guidance for developing security and privacy FRs based on ISO/IEC 15408 (19608, WG 3)
Privacy Architecture Framework (29101)
WG 1/4/5 SP on Cloud Computing
Policies
Data requirements for policies (eg. in cloud contexts)
Policy languages
User Rights Management
Preferences
Guidelines for online privacy notice and consent (29184)
Human Computer Interfaces
Big data reference architecture – Part 4: Security and privacy fabric (20547-4, with WG 4)
PETs and Privacy Services
Anonymous Protocols
Requirements on partially anonymous, partially unlinkable authentication (29191:2012)
A privacy-respecting identity management scheme using attribute-based credentials
Credentials
Transferal
Logs and Auditing
Transparency Tools
Mixes and Network Anonymization
Privacy enhancing data de-identification techniques (20889)
Anonymization Protocols
Secure storage and processing
Processing PII using secure computation
WG4 Storage Security: Deletion (27040)
Documentation of Data Deletion Principles for personally identifiable information in Organisations
Study period
New Work Item Proposal
Current Projects
Projects of other WGs
Concluded Study Period
International Standard
controversial
Resource constraints
Standing Document

Privacy/PII Standards and Projects in SC 27, mainly WG 5 (2013-07)



Framework

Terminology and principles

29100

Freely available?

Privacy references list

SD2

Freely available

Management

Privacy impact assessment

29134

Risks

Privacy capability maturity model

29190

Maturity levels

Controls

27002

Information security controls

27018

Cloud controls

29151

PII controls

Technology

ICT system architecture

29101

ICT components

Requirements

29191

Partially anonymous / partially unlinkable

Support

Standards privacy assessment

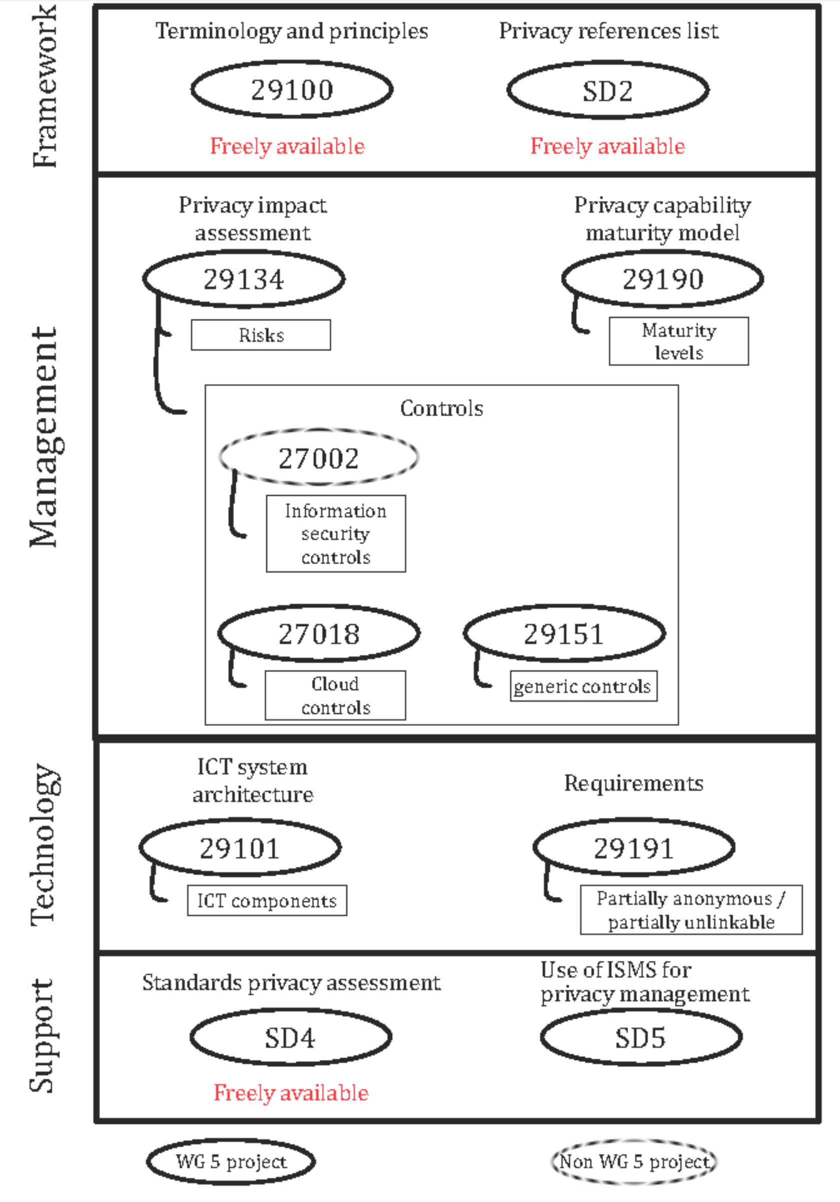
SD4

Freely available

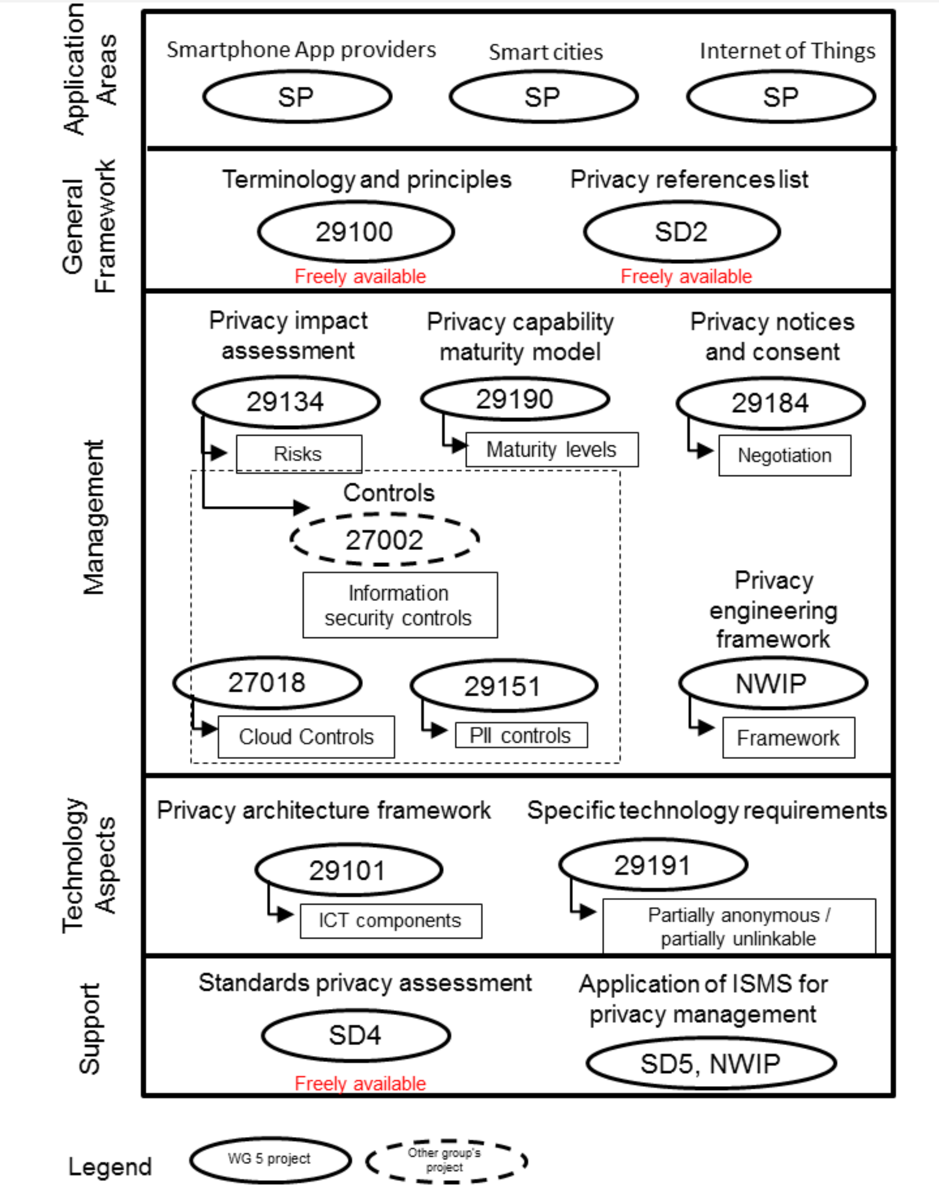
WG 5 project

other project

Privacy/PII Standards and Projects in SC 27, mainly WG 5 (2014-12)



Privacy/PII Standards and Projects in SC 27, mainly WG 5 (2016-05)



Application Areas

Smartphone App providers: SP

Smart cities: SP

Internet of Things: SP

General Framework

Terminology and principles: 29100 (Freely available)

Privacy references list: SD2 (Freely available)

Management

Privacy impact assessment: 29134 → Risks

Privacy capability maturity model: 29190 → Maturity levels

Privacy notices and consent: 29184 → Negotiation

Controls: 27002, Information security controls

27018 → Cloud Controls

29151 → PII controls

Privacy engineering framework: NWIP → Framework

Technology Aspects

Privacy architecture framework: 29101 → ICT components

Specific technology requirements: 29191 → Partially anonymous / partially unlinkable

Support

Standards privacy assessment: SD4 (Freely available)

Application of ISMS for privacy management: SD5, NWIP

Legend: WG 5 project; Other group's project

Agenda

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

Technical Privacy Protection

- Individuals
  - want to control the amount of identity information visible from the outside.
  - consider what personal information they reveal to whom.
- Typical protection techniques are:
  - Anonymization and identity management tools
  - Spontaneous switching between different levels of anonymity and pseudonymity depending on the context

Privacy-X Technologies

- Privacy-enhancing technologies
- Privacy-friendly technologies
- Privacy-preserving technologies
- Privacy-protecting technologies
- Privacy-respecting technologies

Building Blocks and Approaches for Privacy Technologies

- Strong privacy requirements:
  - No trust in the system operator, and
  - No trust into one centralized entity.
- Most common methods consider:
  - Communication systems, or
  - Transactions systems

Communication Systems

- The Anonymizer

  www.anonymizer.com

- Mixmaster – Anonymous Remailer

  http://mixmaster.sourceforge.net

- Onion Routing: Tor Network

  http://tor.eff.org/

- Java Anonymous Proxy (JAP)

  http://anon.inf.tu-dresden.de

- Cookie Cooker

  www.cookiecooker.de

- P3P – Platform for Privacy Preferences

  www.w3.org/P3P

Transaction Systems

- Reachability management
- Credential technologies
  - U-Prove

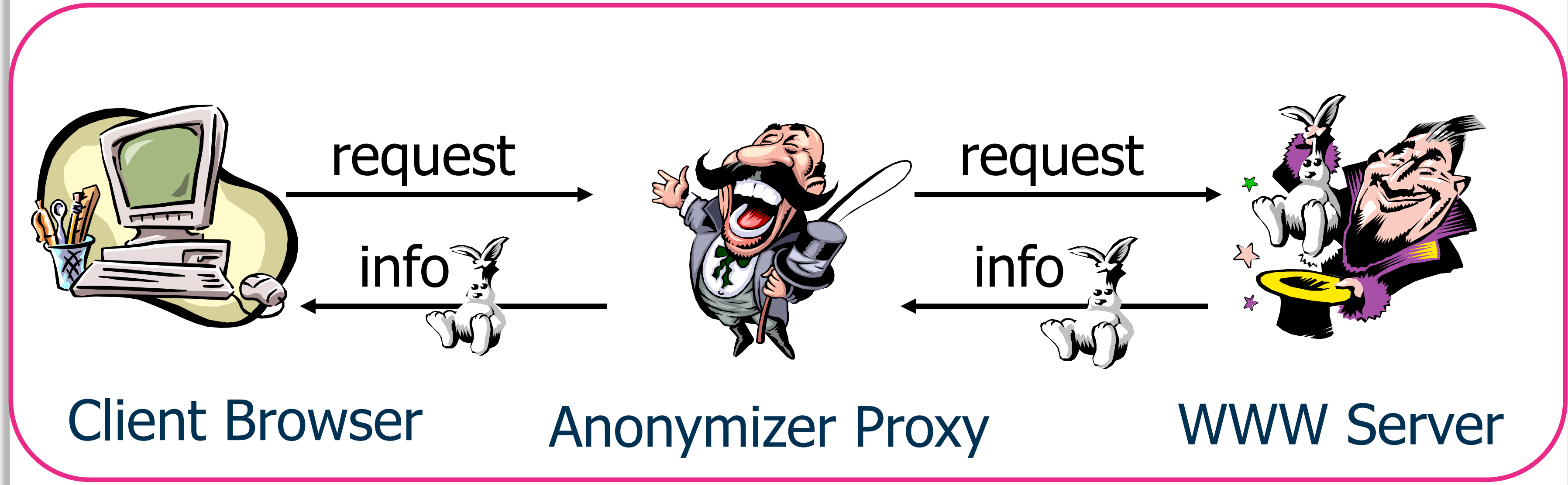
    www.microsoft.com/uprove
  - Idemix

    www.zurich.ibm.com/security/idemix

Agenda

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

www.anonymizer.com



request

info

request

info

Client Browser

Anonymizer Proxy

WWW Server

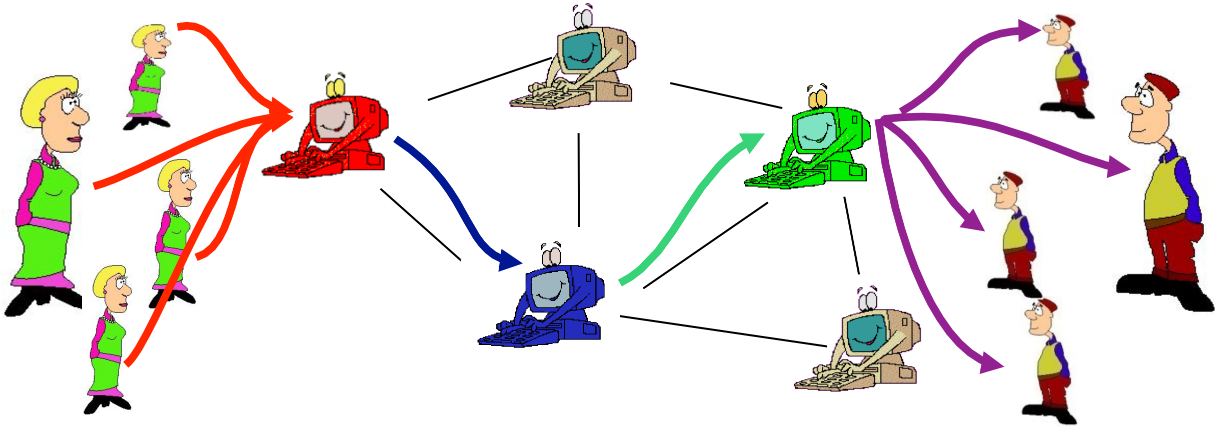
www.anonymizer.com

↑ Client (anonymity) is protected in an “**anonymity set**” of all possible proxy clients.

↓ Anonymizer learns about client’s activities / interests.

↓ No protection against attackers with global view.

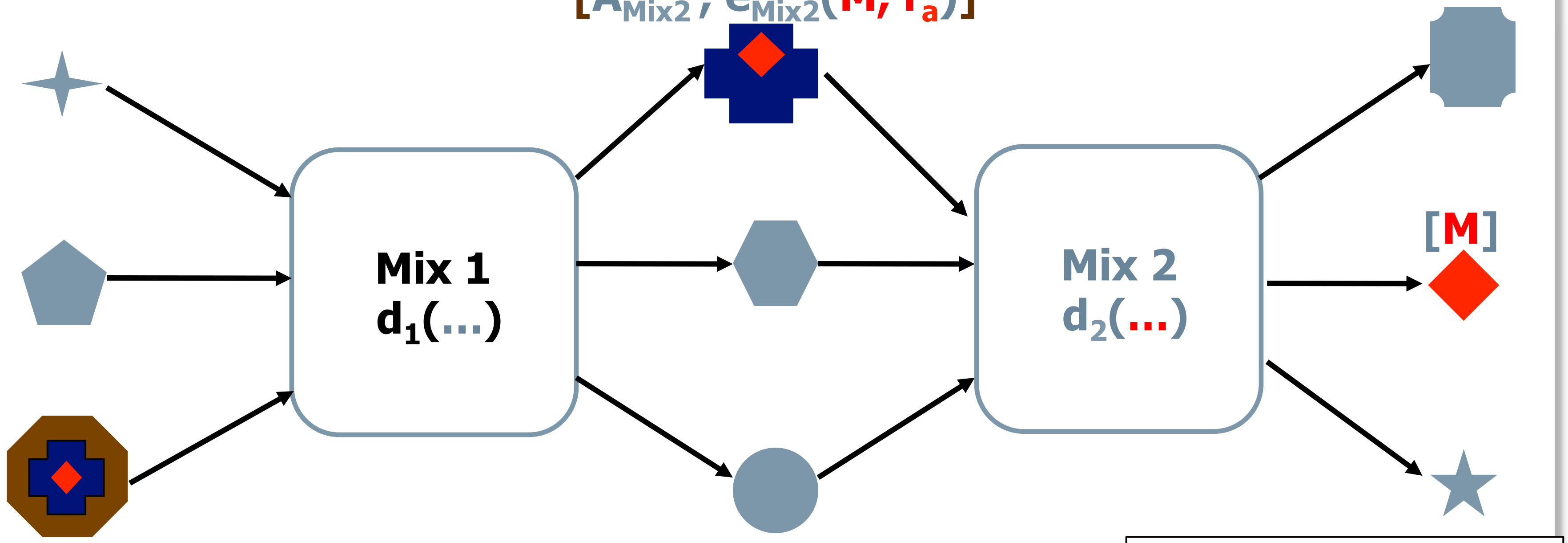
Mixes and Onion Routing



- *Communication is anonymized by multiple mix servers, also called onion routers.*
    - *Both onion routing and JAP are based on the same Mix concept.*

Mixes

$[A_{Mix2}, e_{Mix2}(M, r_a)]$



$[A_{Mix1}, e_{Mix1}(A_{Mix2}, e_{Mix2}(M, r_a), r_b)]$

- Decode, buffer, reorder, and resend incoming messages
- Protect **unlinkability** of input / output messages
- Protect **unobservability** of connections and relations
- No single point of trust / failure

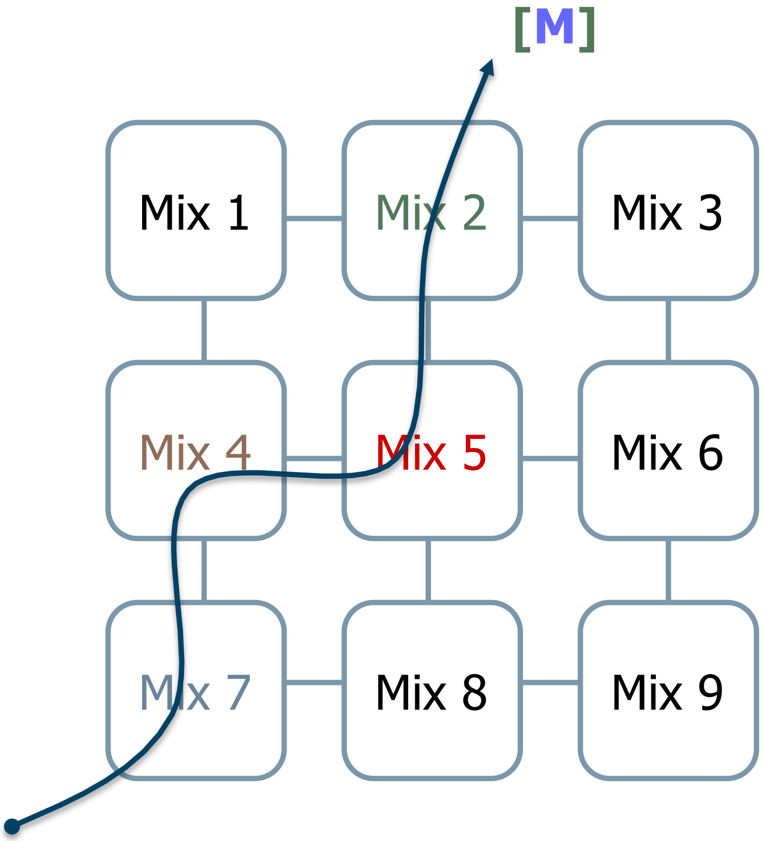
Symbols:

A	**a**ddress
e()	**e**ncryption function
d()	**d**ecryption function
M	core **m**essage
r	**r**andom value
[]	message boundary

[Chaum1981]

Mix Network

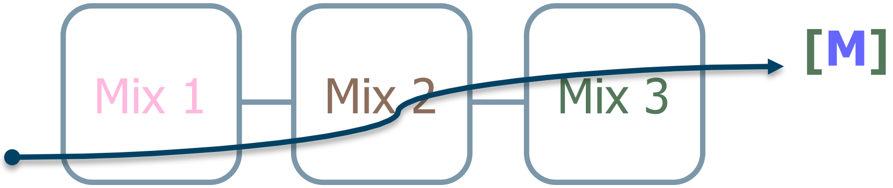
- Choose the way of your message through the mixes!
- Protection guaranteed as long as one chosen mix withstands attacks.
- Free path results in additional confusion, but smaller anonymity set.



$[A_{Mix7}, e_{Mix7}(A_{Mix4}, e_{Mix4}(A_{Mix5}, e_{Mix5}(A_{Mix2}, e_{Mix2}(M, r_a), r_b), r_c), r_d)]$

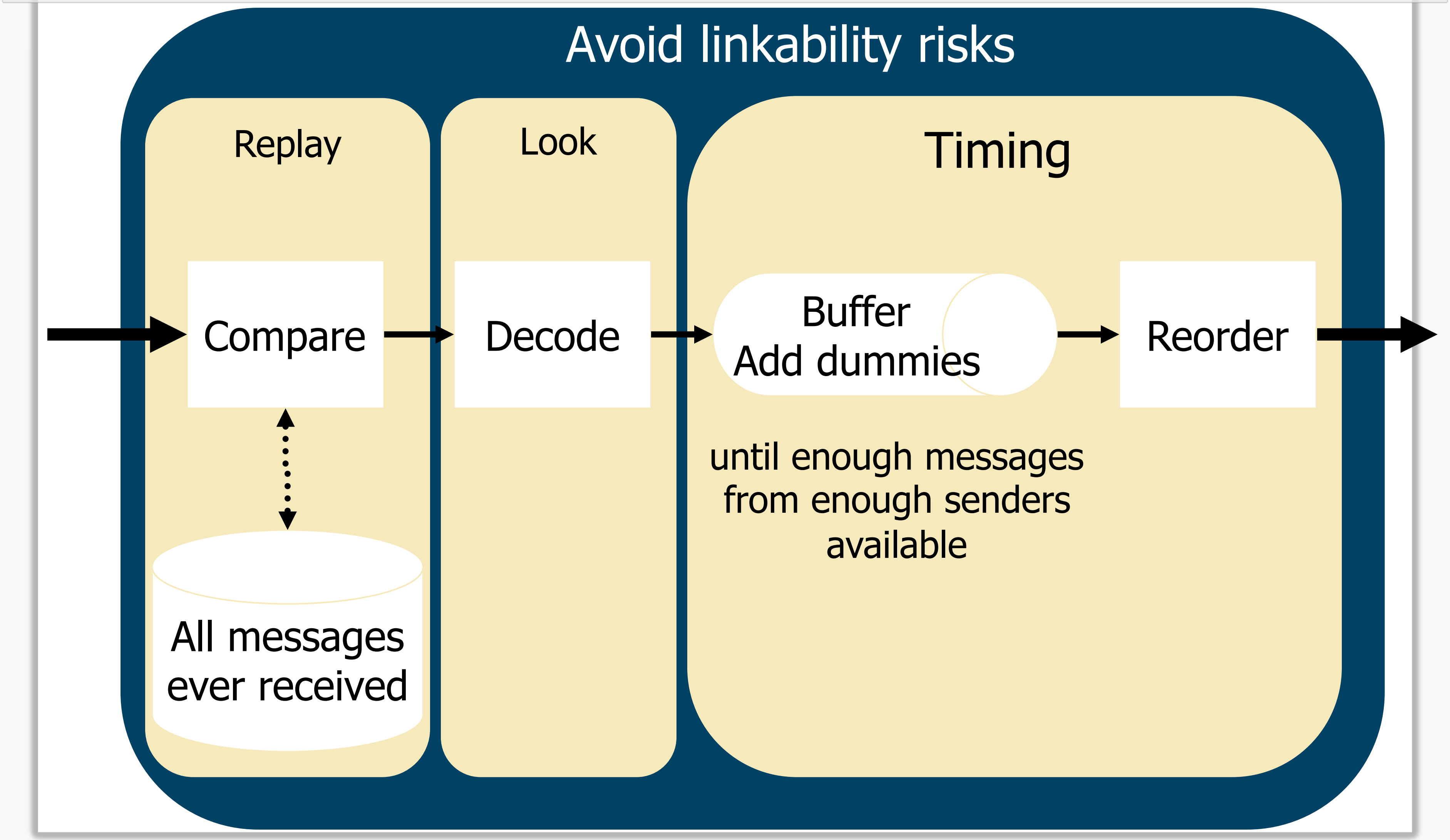
Mix Cascade

$[e_{Mix1}(e_{Mix2}(e_{Mix3}(M, r_a), r_b), r_c)]$



- Fixed Path through the network
- No mix addresses required in messages
- All traffic flows over the same mixes.
- Protection guaranteed as long as one mix withstands attacks

Mixes – Internally



Avoid linkability risks

Replay

Look

Timing

Compare

Decode

Buffer
Add dummies

Reorder

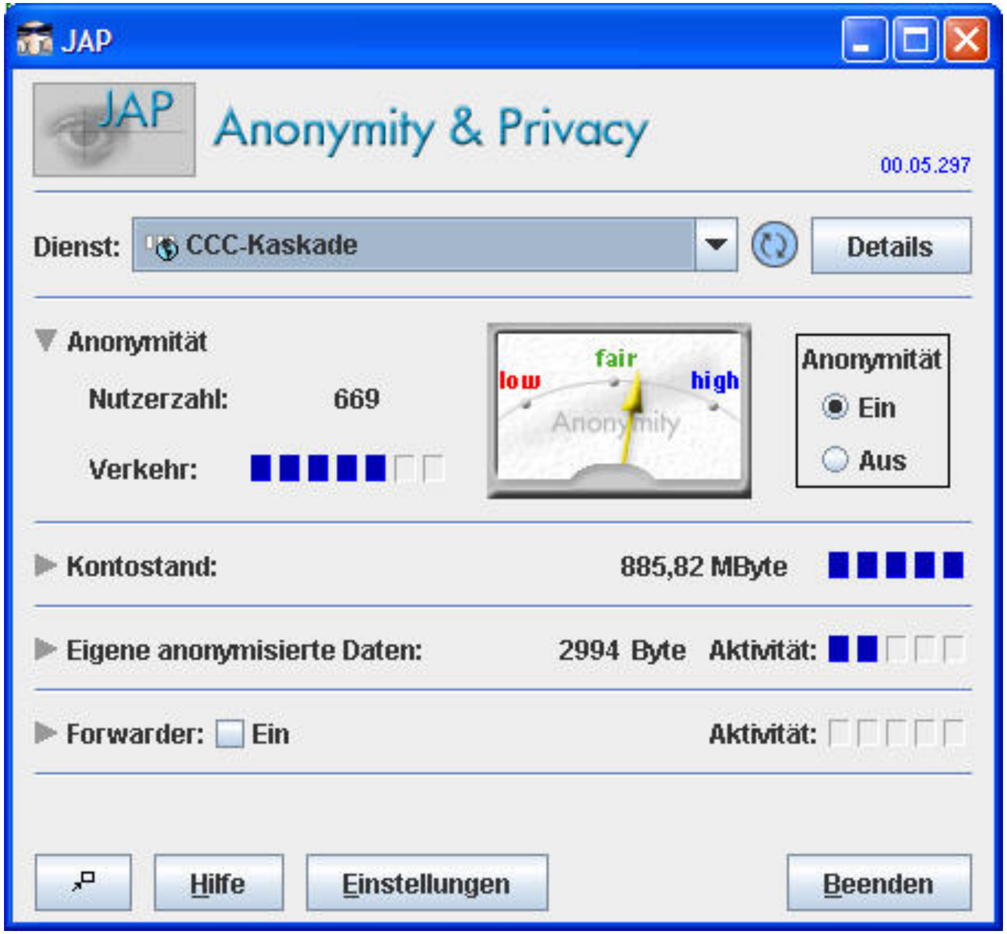
All messages
ever received

until enough messages
from enough senders
available

Java Anonymity Proxy (JAP)

- Users can choose between multiple mix-cascades
- Number of active users is a heuristic for level of anonymity achieved
- Current version does not achieve security against a global attacker but can protect against local attackers
  - your boss
  - your provider
  - operator of a mix

http://anon.inf.tu-dresden.de



JAP

JAP Anonymity & Privacy 00.05.297

Dienst: CCC-Kaskade

Anonymität

Nutzerzahl: 669

Verkehr: ■■■■■□□

Anonymität ● Ein ○ Aus

Kontostand: 885,82 MByte ■■■■■

Eigene anonymisierte Daten: 2994 Byte Aktivität: ■■□□□

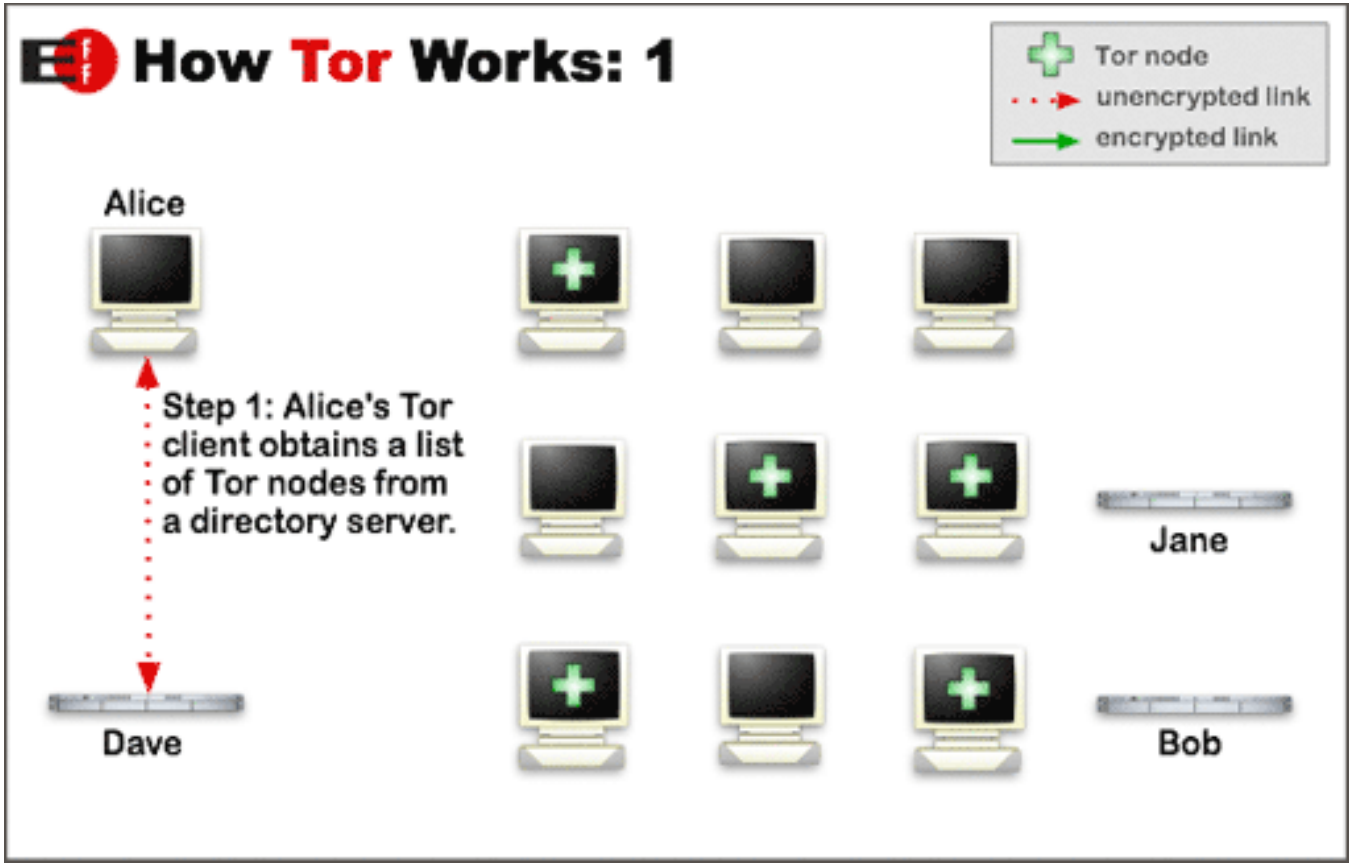
Forwarder: □ Ein Aktivität: □□□□□

Tor Network

- Tor is a network of virtual tunnels that allows people and groups to improve their privacy and security on the Internet
- Distributed anonymous network
- Tor allows users to change circuits during sessions
  - ➢ Aims to minimize linkability of actions
- May be affected by the data retention directive (as well as JAP)
  - ➢ Anonymity and data logs?

[Europe2006]

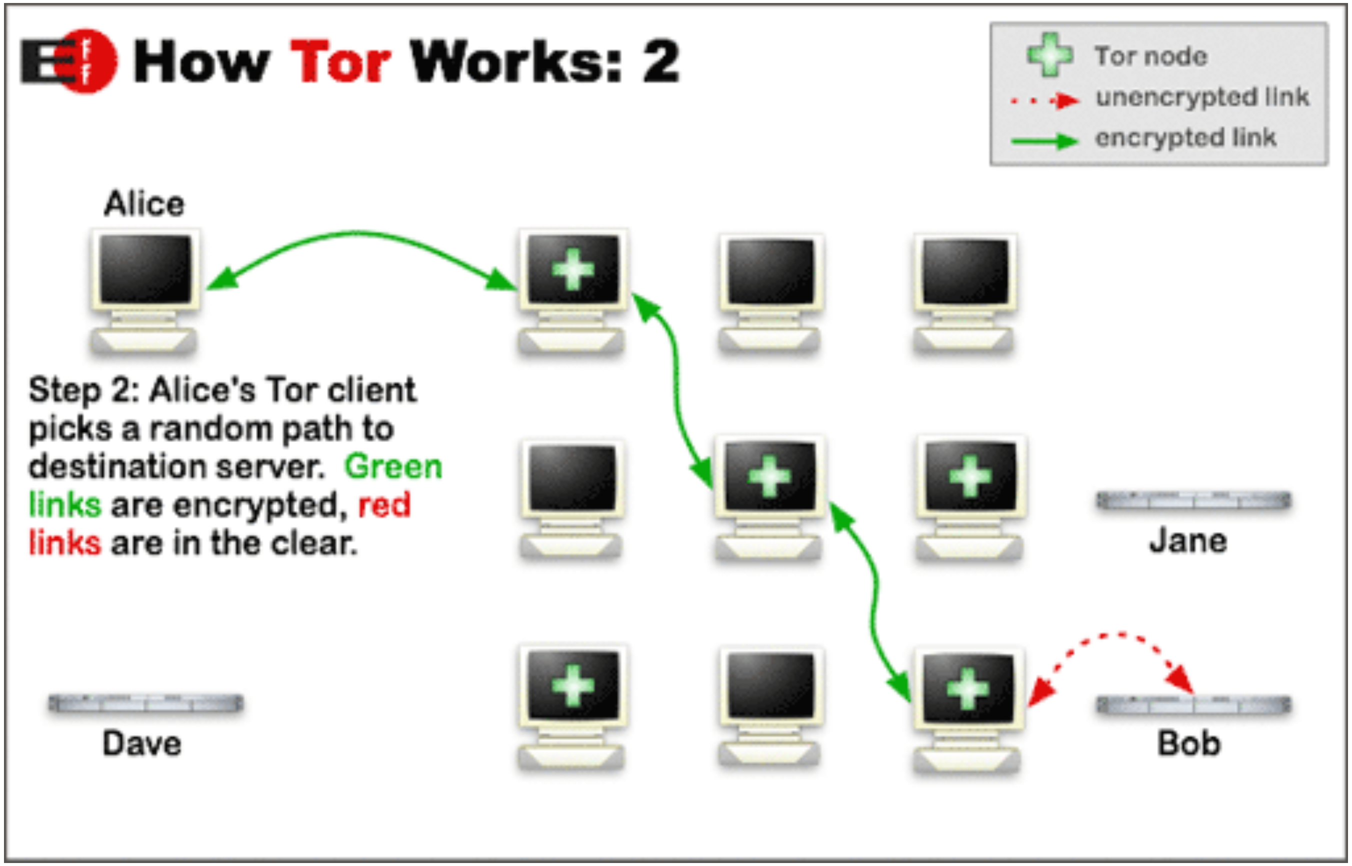
How Tor Works I



How Tor Works: 1
Tor node
unencrypted link
encrypted link
Alice
Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.
Jane
Dave
Bob

http://tor.eff.org

How Tor Works II

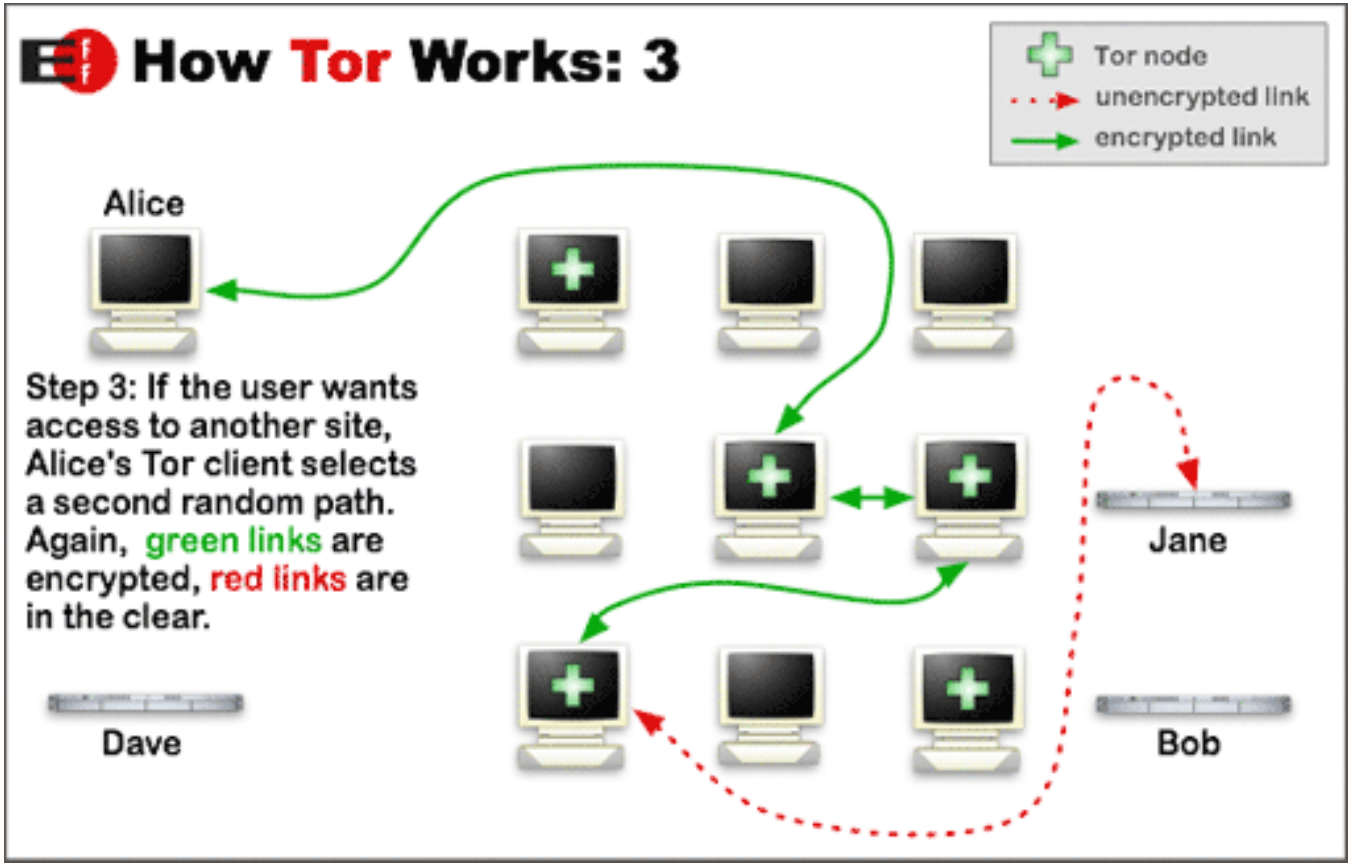


How Tor Works: 2

Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.

http://tor.eff.org

How Tor Works III



How Tor Works: 3

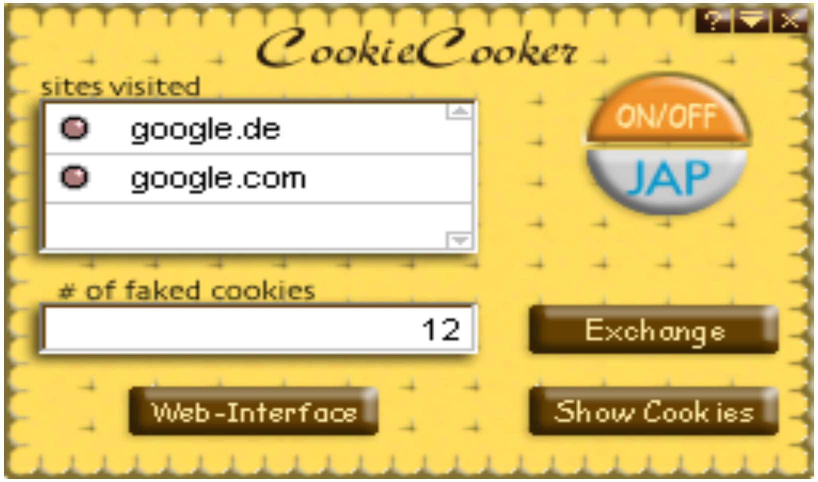
Step 3: If the user wants access to another site, Alice's Tor client selects a second random path. Again, green links are encrypted, red links are in the clear.

http://tor.eff.org

CookieCooker

- Confuse data collectors
  - Exchange of cookies between users
  - Exchange of identities
  - Use of „faked“ data
- User-defined identity management
  - Assistance for the registration
  - Application of „real“ and „faked“ data
- Spam protection through disposable email addresses
- Ad blocking
- Integrated with JAP Anonymizer

Nowadays only disposable email addresses


CookieCooker

sites visited

google.de

google.com

# of faked cookies

12

Platform for Privacy Preferences (P3P)

- Standard of declaring privacy preferences in a standardized way
  - snapshot of how a web site handles personal information about its users
  - P3P enabled browsers can "read" this snapshot and compare it to the consumer's set of privacy preferences.
- P3P aimed at enhancing user control by
  - putting privacy policies where users can find them,
  - in a form users can understand, and
  - enables users to act on what they see. [W3C P3P]
- Unfortunately this promise has not yet been fulfilled.

Agenda

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

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

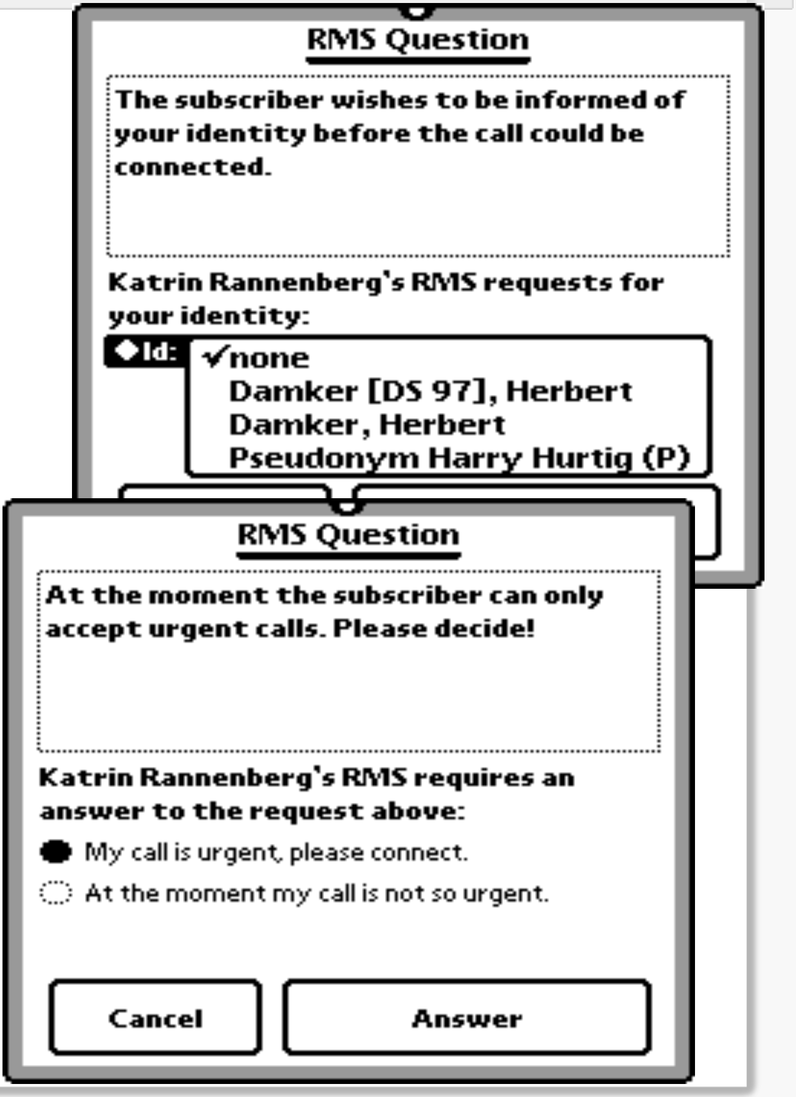
“I welcome you calling back.”

Provision of a reference

“My friends are your friends!”

Offering a surety

“Satisfaction guaranteed
or this money is yours!”



RMS Question

The subscriber wishes to be informed of your identity before the call could be connected.

Katrin Rannenberg's RMS requests for your identity:

✓none
Damker [DS 97], Herbert
Damker, Herbert
Pseudonym Harry Hurtig (P)

RMS Question

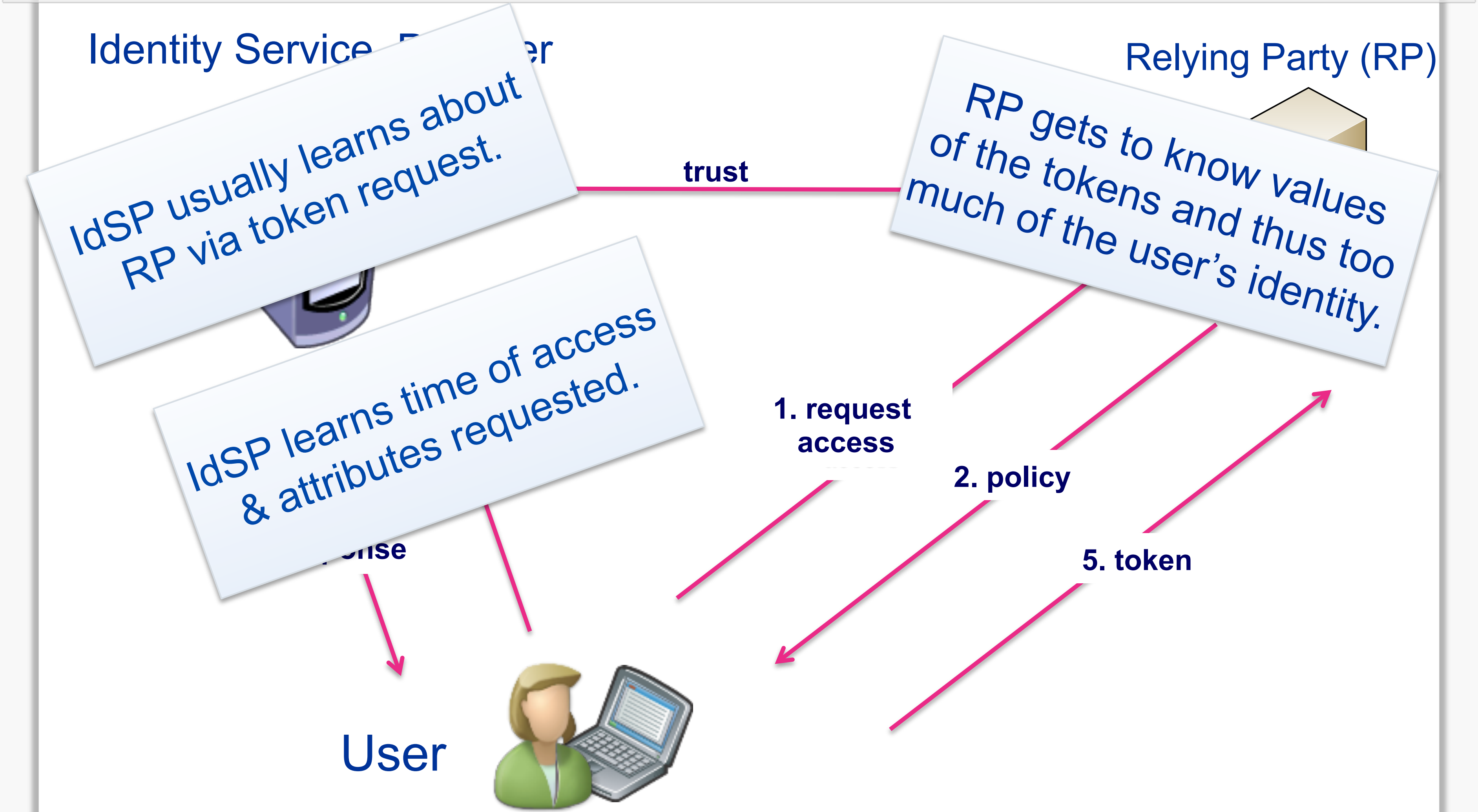
At the moment the subscriber can only accept urgent calls. Please decide!

Katrin Rannenberg's RMS requires an answer to the request above:

● My call is urgent, please connect.
○ At the moment my call is not so urgent.

[Rannenberg2000]

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.

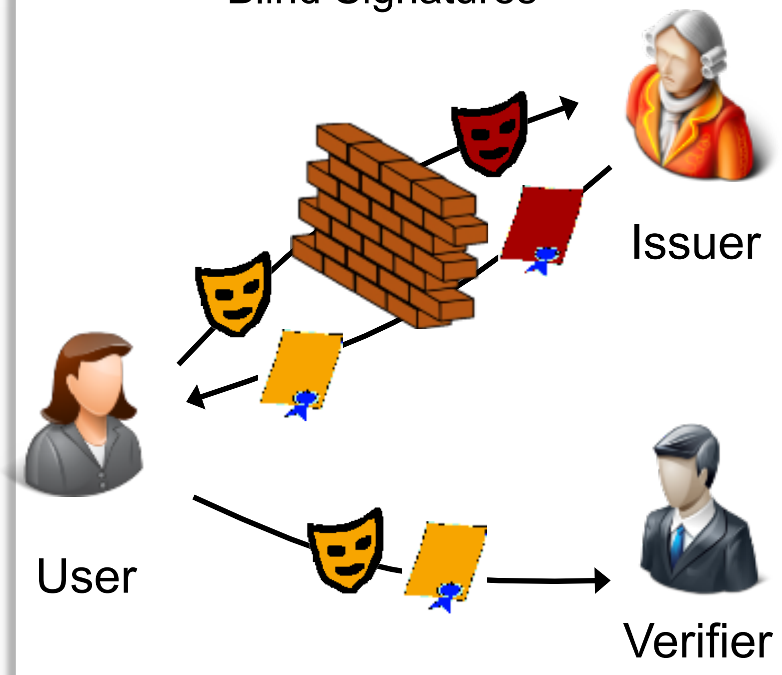
Credential Systems

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



Issuer

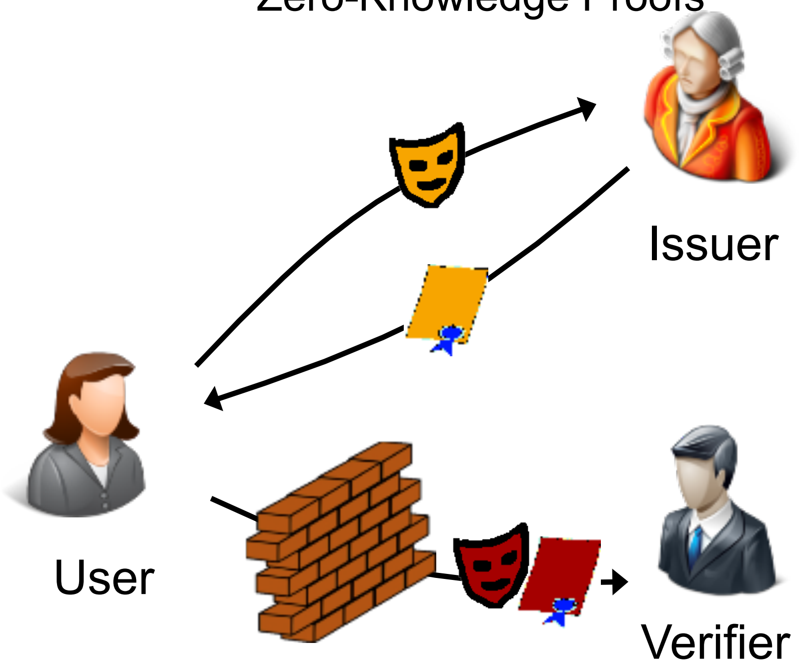
User

Verifier

U-Prove

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

Zero-Knowledge Proofs



Issuer

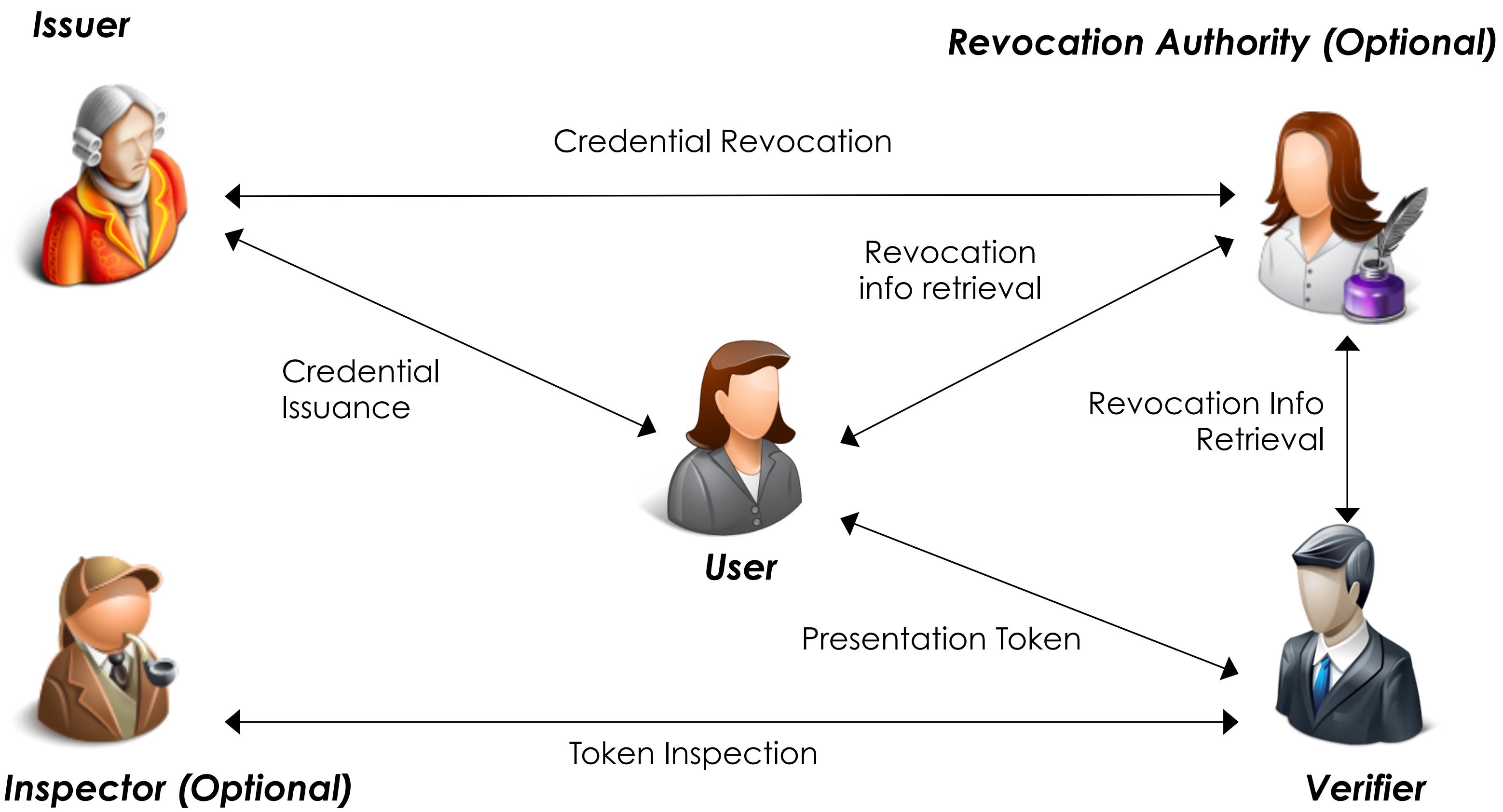
User

Verifier

Idemix (Identity Mixer)

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

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
  - Privacy Enhancing Technologies (PETs)
- Integrated Privacy Protection
  - Privacy by Design (PbD)
  - 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]

The 7 Foundational Principles of PbD

- **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.

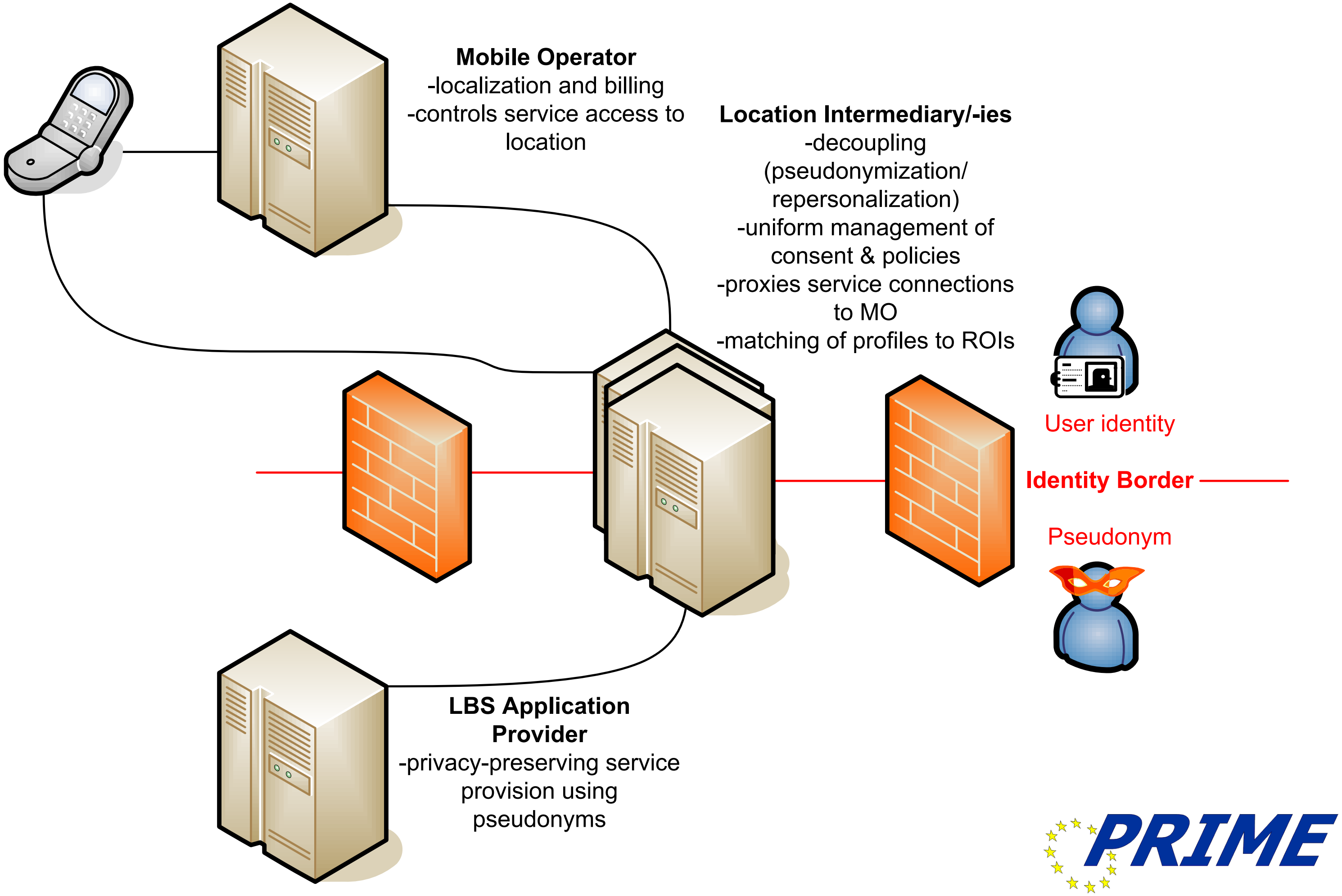
[Cavoukian2009]

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



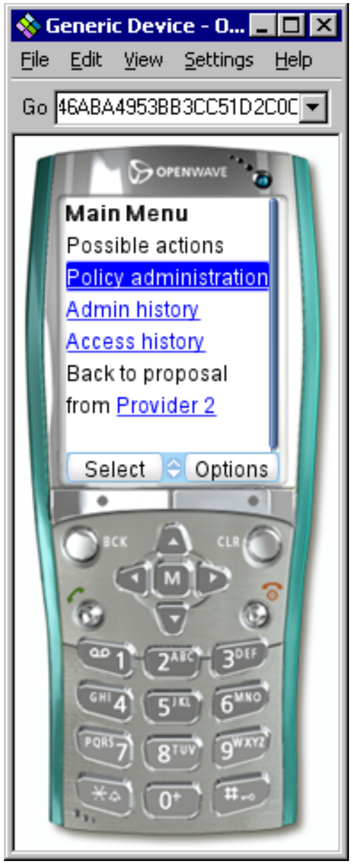
Mobile Operator
-localization and billing
-controls service access to location

Location Intermediary/-ies
-decoupling (pseudonymization/ repersonalization)
-uniform management of consent & policies
-proxies service connections to MO
-matching of profiles to ROIs

LBS Application Provider
-privacy-preserving service provision using pseudonyms

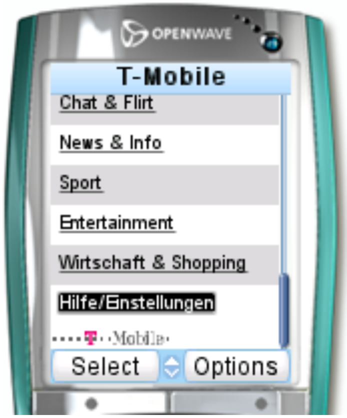
Privacy Gateway

- 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-Mobile

Chat & Flirt

News & Info

Sport

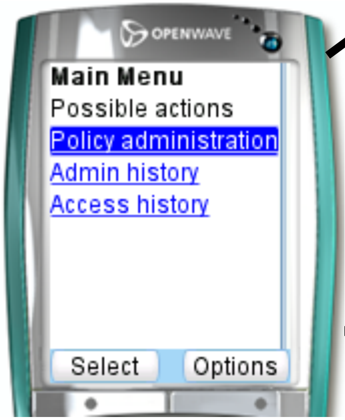
Entertainment

Wirtschaft & Shopping

Hilfe/Einstellungen

T··Mobile·

[T-Zones/Web'n'Walk]



Main Menu

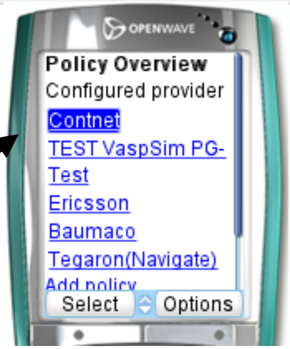
Possible actions

Policy administration

Admin history

Access history

Policy admin



Policy Overview

Configured provider

Contnet

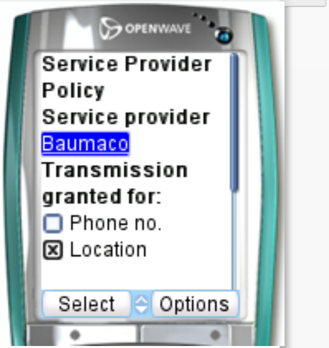
TEST VaspSim PG-Test

Ericsson

Baumaco

Tegaron(Navigate)

Add policy



Service Provider Policy

Service provider

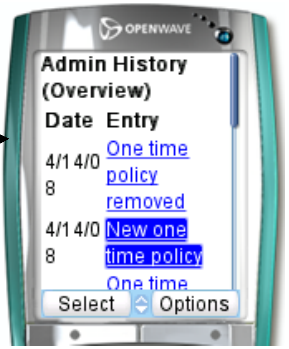
Baumaco

Transmission granted for:

□ Phone no.

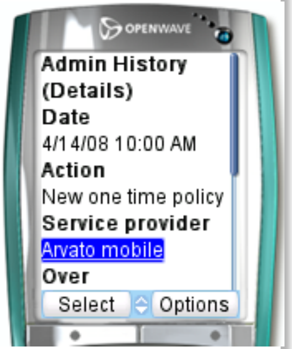
☒ Location

Admin history



Admin History (Overview)

Date	Entry
4/14/08	One time policy removed
4/14/08	New one time policy
	One time



Admin History (Details)

Date

4/14/08 10:00 AM

Action

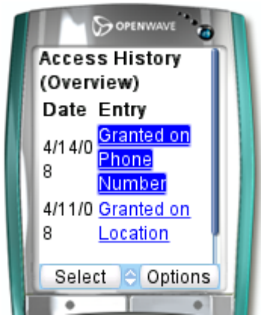
New one time policy

Service provider

Arvato mobile

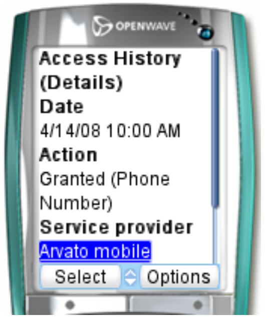
Over

Access history



Access History (Overview)

Date	Entry
4/14/08	Granted on Phone Number
4/11/08	Granted on Location



Access History (Details)

Date

4/14/08 10:00 AM

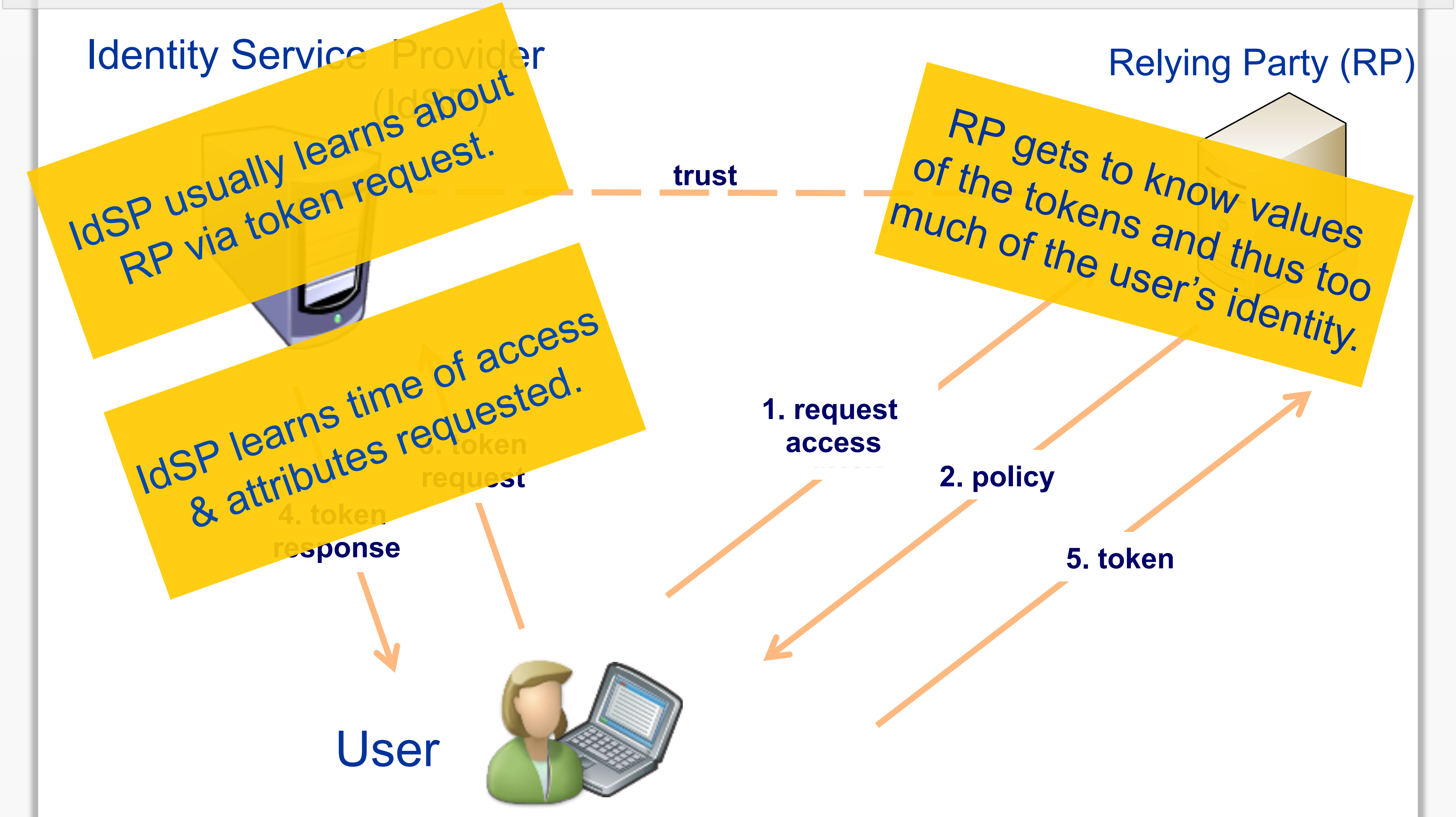
Action

Granted (Phone Number)

Service provider

Arvato mobile

Privacy (and security) issues of typical federated IdM architectures



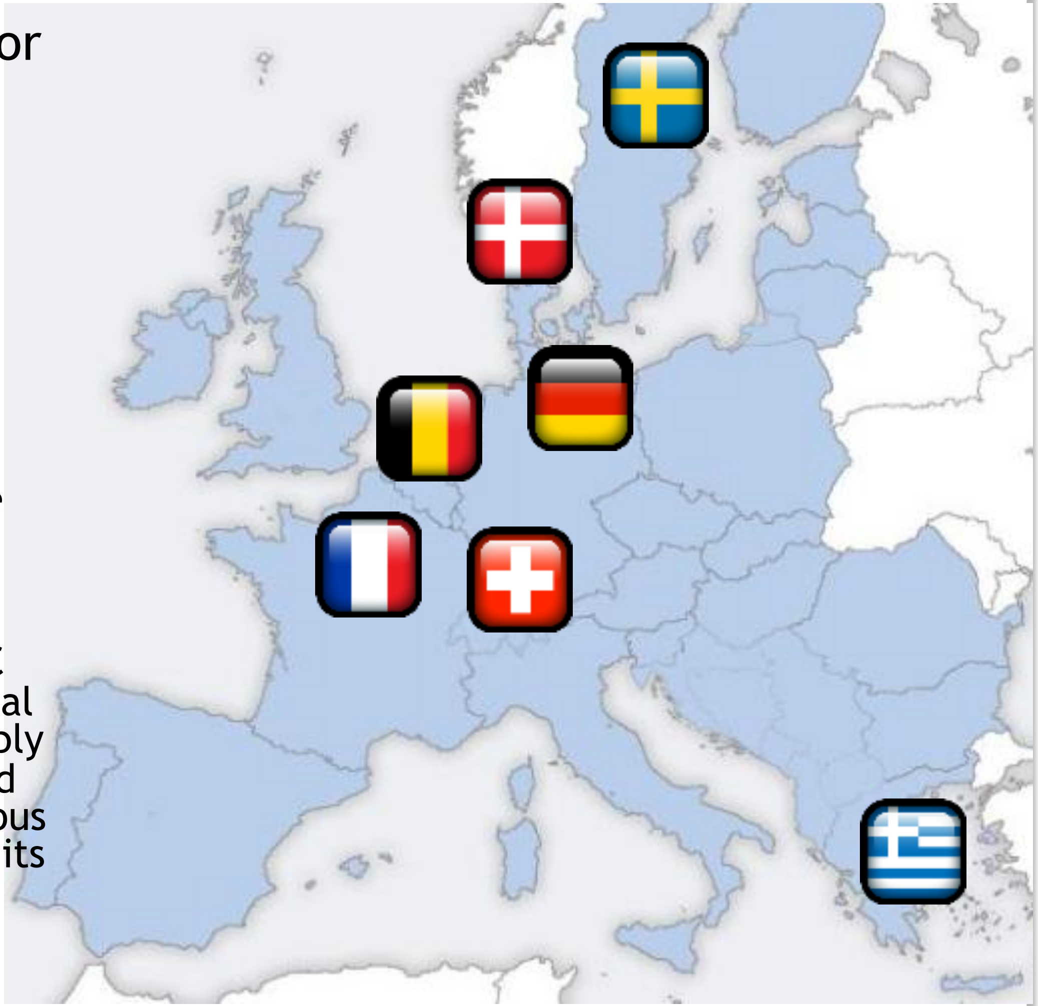
IdSP usually learns about RP via token request.

IdSP learns time of access & attributes requested.

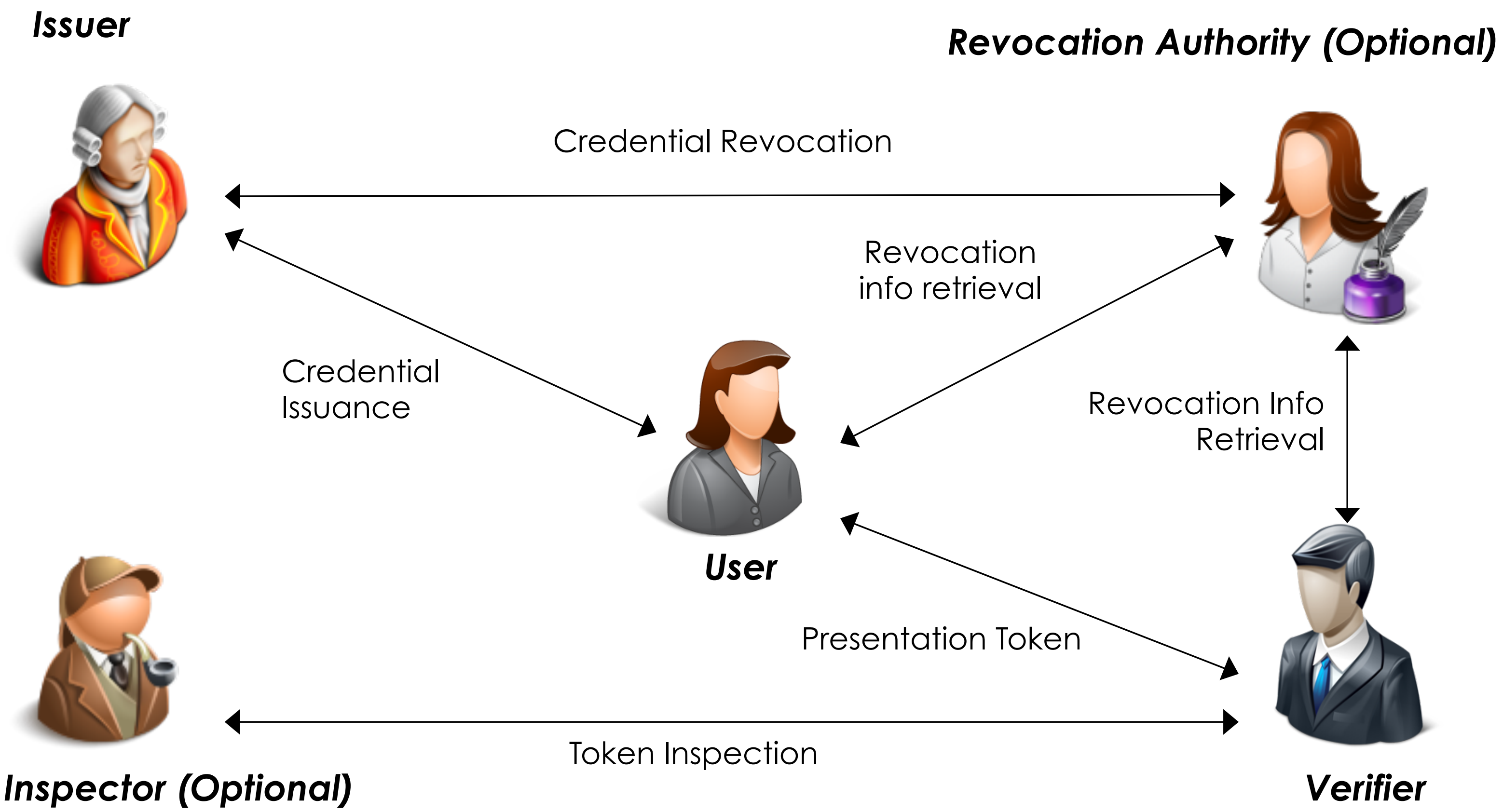
RP gets to know values of the tokens and thus too much of the user's identity.

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.



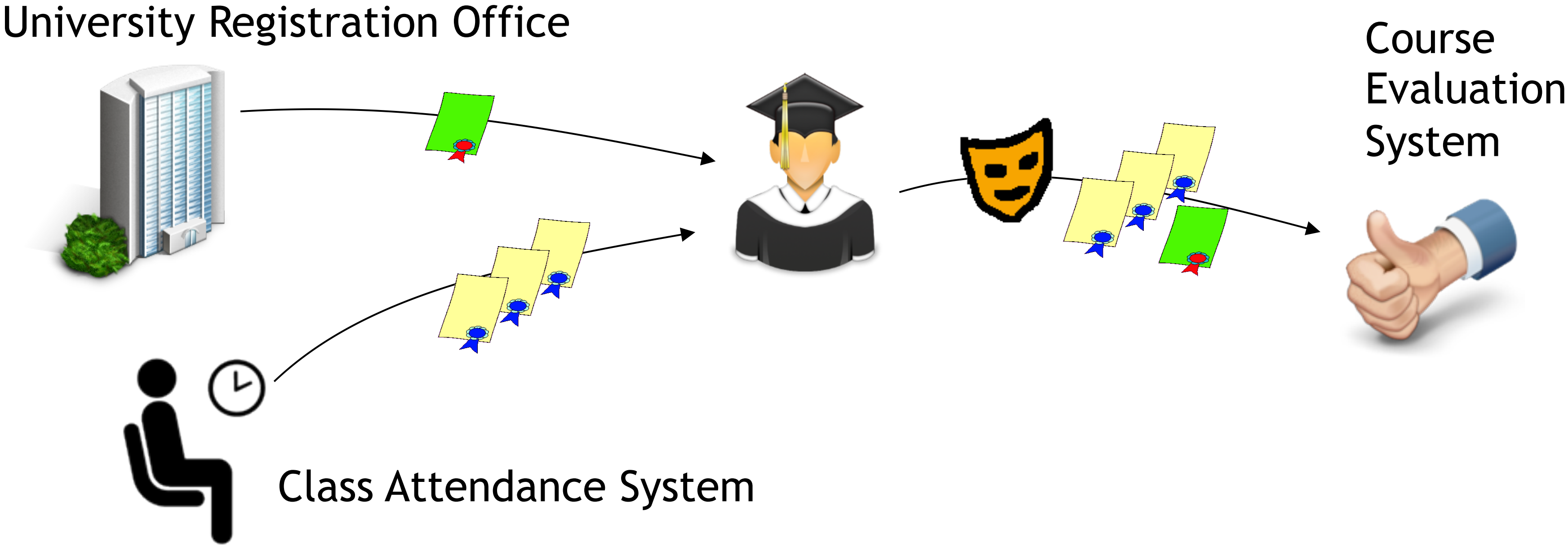
ABC4Trust Architecture High Level View



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 have attended enough 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

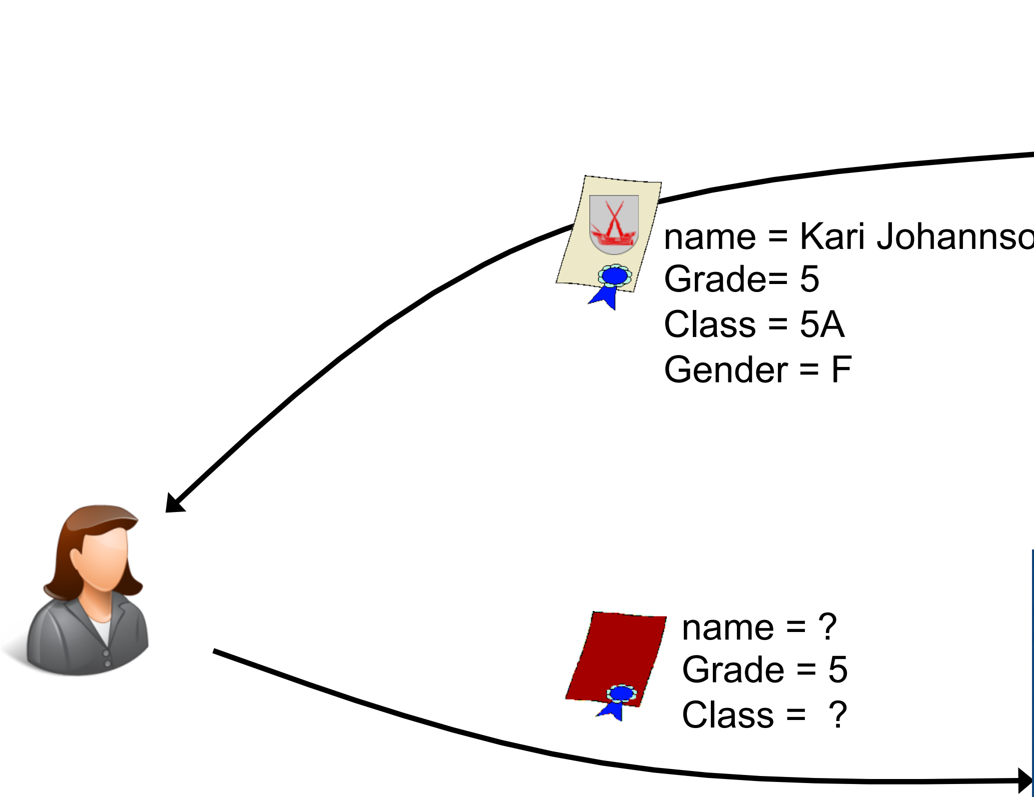


① The students receive a credential when they enrol in a course.

② The students anonymously collect credentials for attending each lecture of the courses.

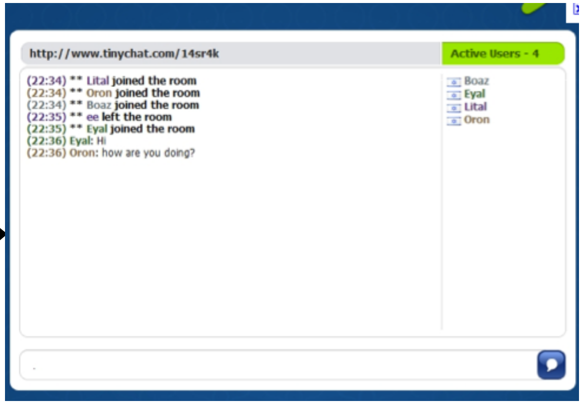
③ At the end of semester they can prove that they have taken the course and participated at enough lectures to be able to evaluate the course without disclosing their identity.

Privacy preserving school community platform



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

name = ?
Grade = 5
Class = ?



http://www.tinychat.com/14sr4k

Active Users - 4

(22:34) ** Lital joined the room
(22:34) ** Oron joined the room
(22:34) ** Boaz joined the room
(22:35) ** ee left the room
(22:35) ** Eyal joined the room
(22:36) Eyal: Hi
(22:36) Oron: how are you doing?

Boaz
Eyal
Lital
Oron

Privacy Advisor on Top of Privacy-ABCs

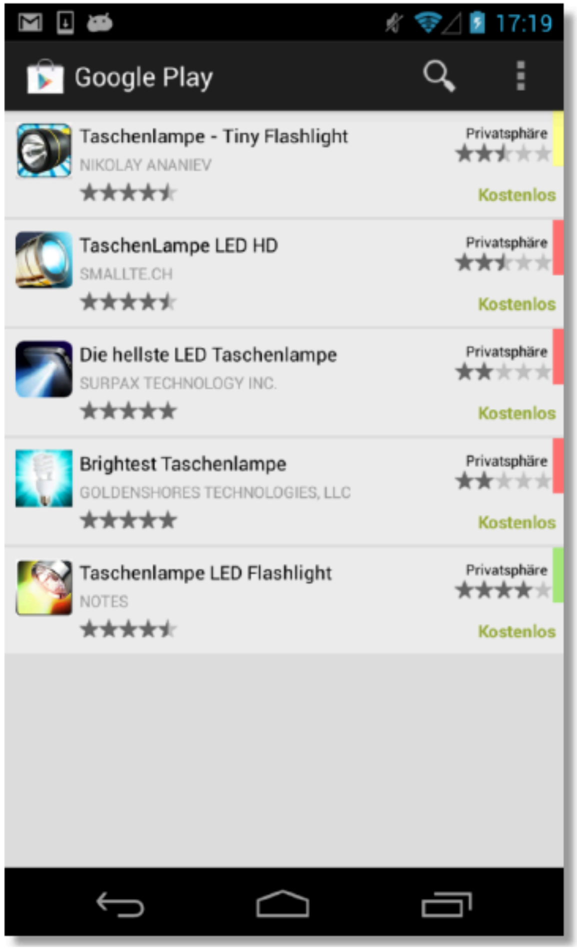
- Privacy advisor that helps users against potentially identity revelations while using privacy-preserving systems
- Automatic detection of privacy sensitive data
- Risk analysis
- Effective communication of the risk to users

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.



17:19

Google Play

Taschenlampe - Tiny Flashlight
NIKOLAY ANANIEV
Privatsphäre
Kostenlos

TaschenLampe LED HD
SMALLTE.CH
Privatsphäre
Kostenlos

Die hellste LED Taschenlampe
SURPAX TECHNOLOGY INC.
Privatsphäre
Kostenlos

Brightest Taschenlampe
GOLDENSHORES TECHNOLOGIES, LLC
Privatsphäre
Kostenlos

Taschenlampe LED Flashlight
NOTES
Privatsphäre
Kostenlos

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

[Bell2001] Tom W. Bell, Internet Privacy and Self-Regulation: Lessons from the Porn Wars, Cato Institute Briefing Papers, No 65., 2001, www.cato.org/pubs/briefs/bp65.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.

[BVwG2003] Bundesverwaltungsgericht: Entscheidung BVerwG 6 C 23.02; www.bundesverwaltungsgericht.de/enid/d90753334a813794b15cc66003046de0,0976e07365617263685f646973706c6179436f6e7461696e6572092d0933353031/8o.html

[Cavoukian2009] Privacy by Design The 7 Foundational Principles, https://www.ipc.on.ca/images/resources/7foundationalprinciples.pdf

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

[Durand2003] Andre Durand, Three Phases of Identity Infrastructure Adoption, http://discuss.andredurand.com/stories/storyReader$343

References II

[Europe2006] European Parliament and the Council: Directive 2006/24/EC of the European Parliament and if the council; www.ispai.ie/DR%20as%20published%20OJ%2013-04-06.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 http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

[Hoofnagle2005] Chris Jay Hoofnagle, Privacy Self Regulation: A Decade of Disappointment, 2005, www.epic.org/reports/decadedisappoint.html

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

[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

[Reagle1998] Joseph M. Reagle Jr., Boxed In: Why US Privacy Self Regulation Has Not Worked, Berkman Center for Internet & Society, Harvard Law School, 1998, http://cyber.law.harvard.edu/people/reagle/privacy-selfreg.html

[SelfReg1999] Self-Regulation: Regulatory Fad or Market Forces? Paper prepared for Cato Roundtable „Privacy vs. Innovation“ by Solveig Singleton, May 7, 1999, www.cato.org/pubs/wtpapers/990507report.html

[W3C P3P] Platform for Privacy Preferences (P3P) Project, W3C, www.w3.org/P3P

[WaBr1890] Samuel D. Warren, Louis D. Brandeis: The Right to Privacy, Harvard Law Review; Vol. IV; December 15, 1890, No. 5; http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html