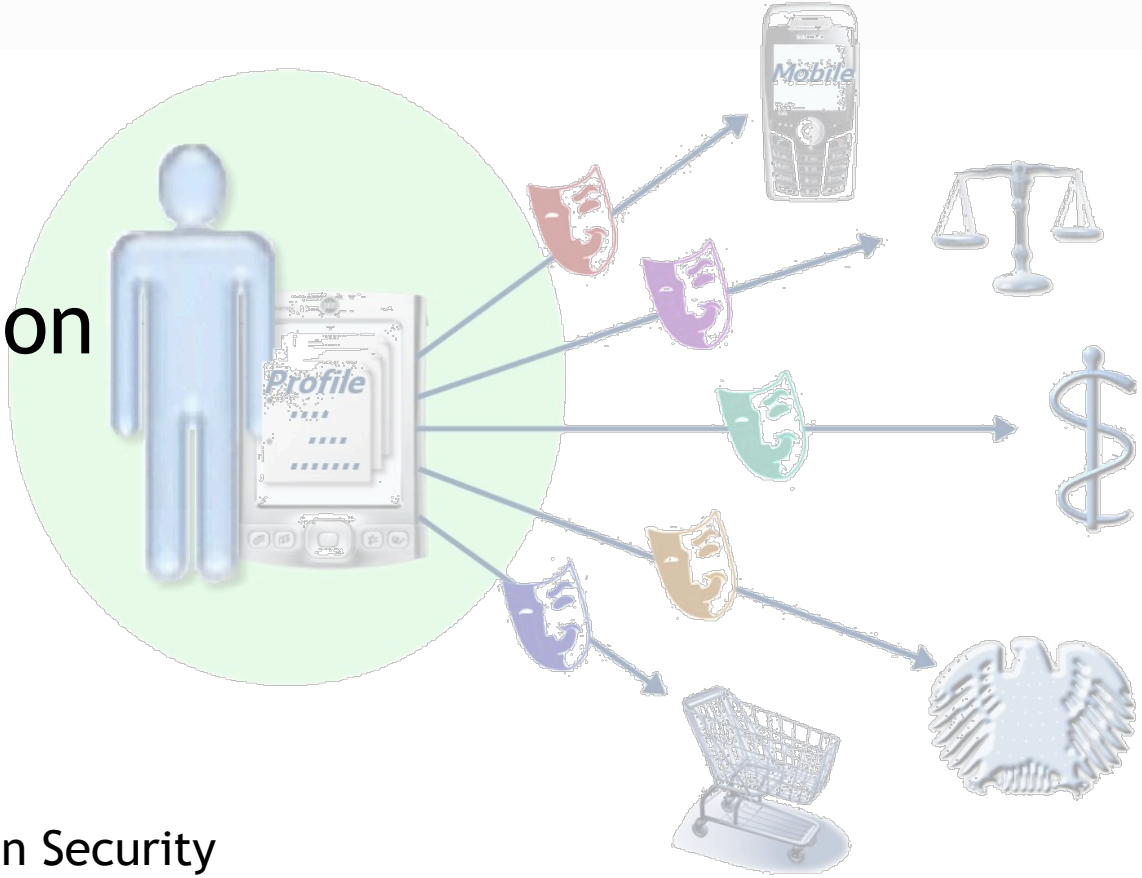
mobile business

Lecture 8

Privacy Protection



Information & Communication Security
(WS 2014/15)

Prof. Dr. Kai Rannenberg

Deutsche Telekom Chair of Mobile Business & Multilateral Security
Goethe-University Frankfurt a. M.

mobile business

Agenda

- Data Protection and Privacy
  - Origin and definition
  - Law, Technology, Standardization
- Technical Privacy Protection
  - Privacy Enhancing Technologies (PETs)
  - Deficiencies
- Integrated Privacy Protection
  - PRIME LBS Application Prototype
  - Privacy Gateway
  - ABC4Trust

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 [WaBr 1890].
- 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“ [BVG 1983]).
- 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

mobile business

9 Principles of EU Privacy Law I

1. **Intention and notification:** The processing of personal data must be reported in advance to a Data Protection Authority.
2. **Transparency:** The person involved must be able to see who is processing her data for what purpose.
3. **Finality principle:** Personal data may only be collected and processed for specific, explicit and legitimate purposes.
4. **Legitimate grounds of processing:** The processing of personal data must be based on a foundation referred to in legislation, such as permission, agreement, and such.
5. **Quality:** Personal data must be as correct and as accurate as possible.

[BlaBorOlk2003]

9 Principles of EU Privacy Law II

6. **Data subject's rights:** The parties involved have the right to take cognisance of and to update their data as well as the right to raise objections.
7. **Processing by a processor:** This rule states that, with the transfer of personal data to a processor, the rights of the data subject remain unaffected and that all restrictions equally apply to the processor.
8. **Security:** A controller must take all meaningful and possible measures for guarding the personal data.
9. **Transfer of personal data outside the EU:** The traffic of personal data is permitted only if that country offers adequate protection.

[BlaBorOlk2003]

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

mobile business

The Montreux Declaration

- 27th International Conference of Data Protection and Privacy Commissioners
- 2005-09-14/16 in Montreux, Switzerland
- “The protection of personal data and privacy in a globalised world: a universal right respecting diversities” [ICDPPC 2005]
- 11 principles

mobile business

11 Principles of the Montreux Declaration

- Lawful and fair data collection and processing,
- Accuracy,
- Purpose-specification and -limitation,
- Proportionality,
- Transparency,
- Individual participation and in particular the guarantee of the right of access of the person concerned,
- Non-discrimination,
- Data security,
- Responsibility,
- Independent supervision and legal sanction,
- Adequate level of protection in case of transborder flows of personal data.

mobile business

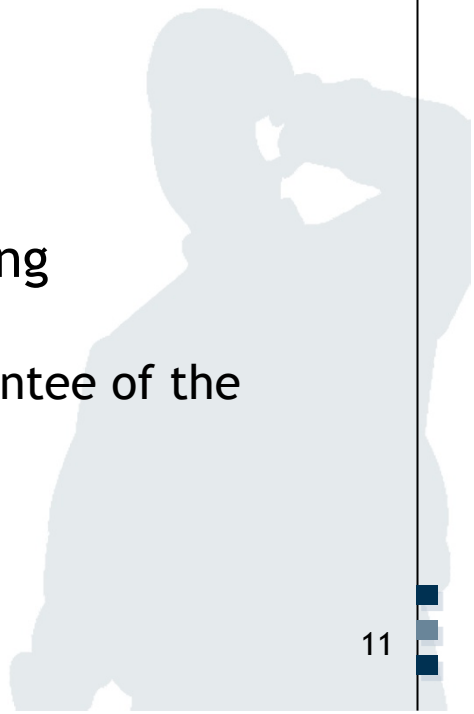
11 Principles of the Montreux Declaration

- Lawful and **fair data collection and processing**,
- Accuracy,
- **Purpose-specification and -limitation,**
- **Proportionality,**
- Transparency,
- **Individual participation and in particular the guarantee of the right of access of the person concerned,**
- Non-discrimination,
- Data security,
- **Responsibility,**
- Independent supervision and legal sanction,
- Adequate level of protection in case of transborder flows of personal data.

mobile business

Data scarcity and Control by the user

- **Data scarcity**
  - Only collect and process data that are needed for the service/ process
  - Use/Develop technologies that provide the service using less data.
  - derived from
    - Fair data collection and processing,
    - Purpose-specification and –limitation,
    - Proportionality
- **Control by the User**
  - Let users decide, when and where data are flowing
  - Derived from
    - Individual participation and in particular the guarantee of the right of access of the person concerned
    - Responsibility



EC Data Protection Law Proposal 2012

- In 2012, the EC proposed a major reform of the EU legal framework on the protection of personal data.
- The European Commission says that the new proposed 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.

[EC2014]

Protection of personal data

[EC-Prot-2014]

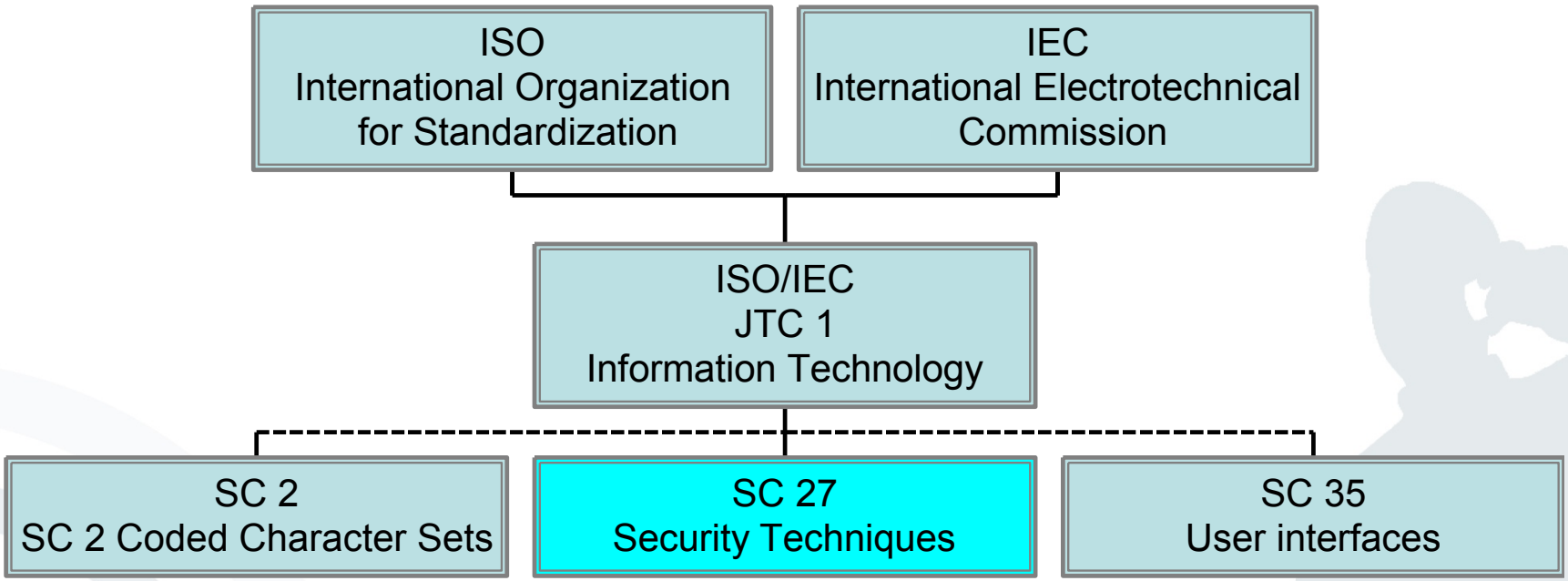
Privacy principles and standardization

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

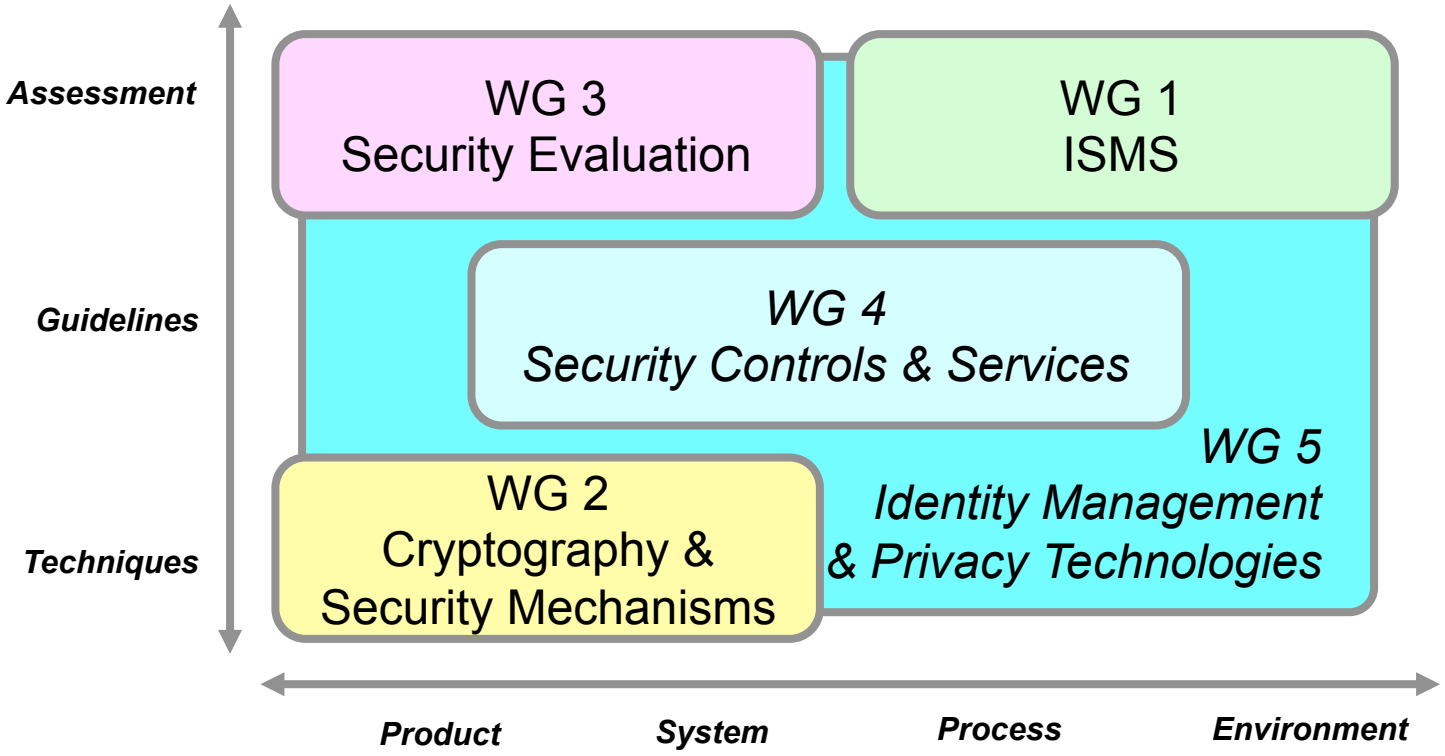
1. Consent and choice
2. Purpose legitimacy and specification
3. Collection limitation
4. Data minimization
5. Use, retention and disclosure limitation
6. Accuracy and quality
7. Openness, transparency and notice
8. Individual participation and access
9. Accountability
10. Information security
11. Privacy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

[ISO29100]

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



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



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

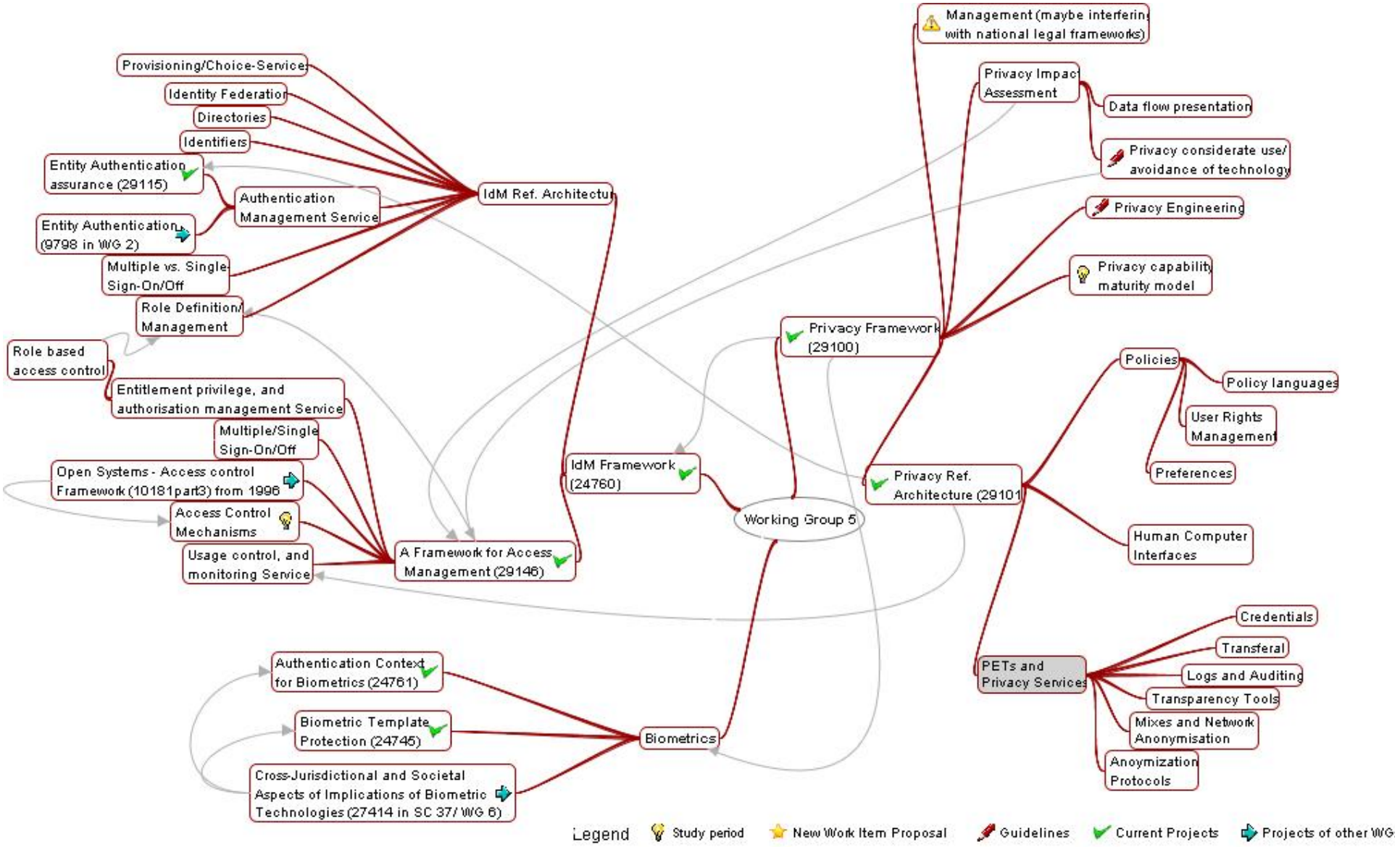
- Biometric information protection (ISO/IEC 24745, IS)
- Requirements for partially anonymous, partially unlinkable authentication (ISO/IEC 29191, IS)

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)

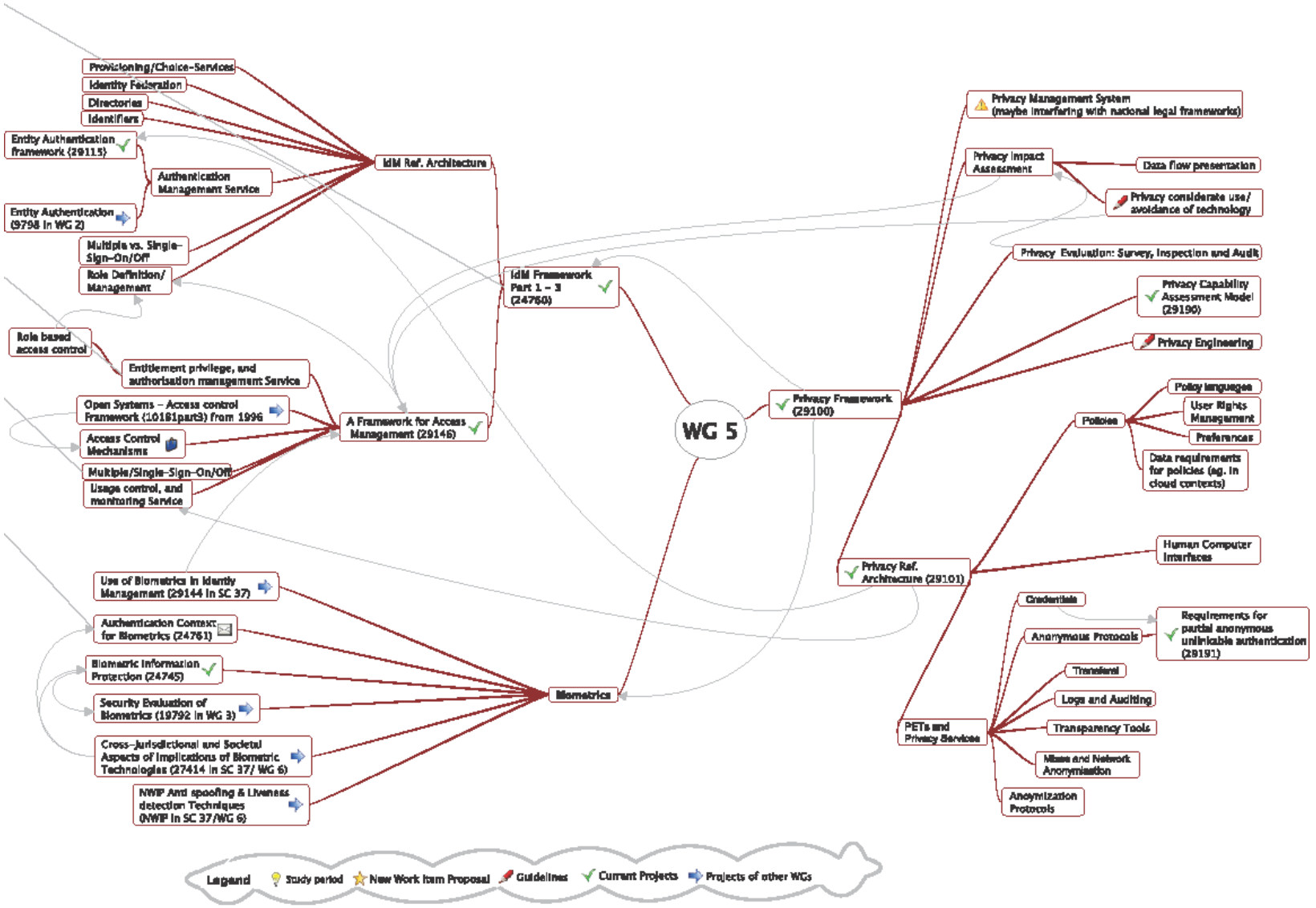
WG 5 Identity Management & Privacy Technologies Roadmap (2008-04)

ISO/IEC JTC 1/SC 27/WG 5 Identity Management & Privacy Technologies



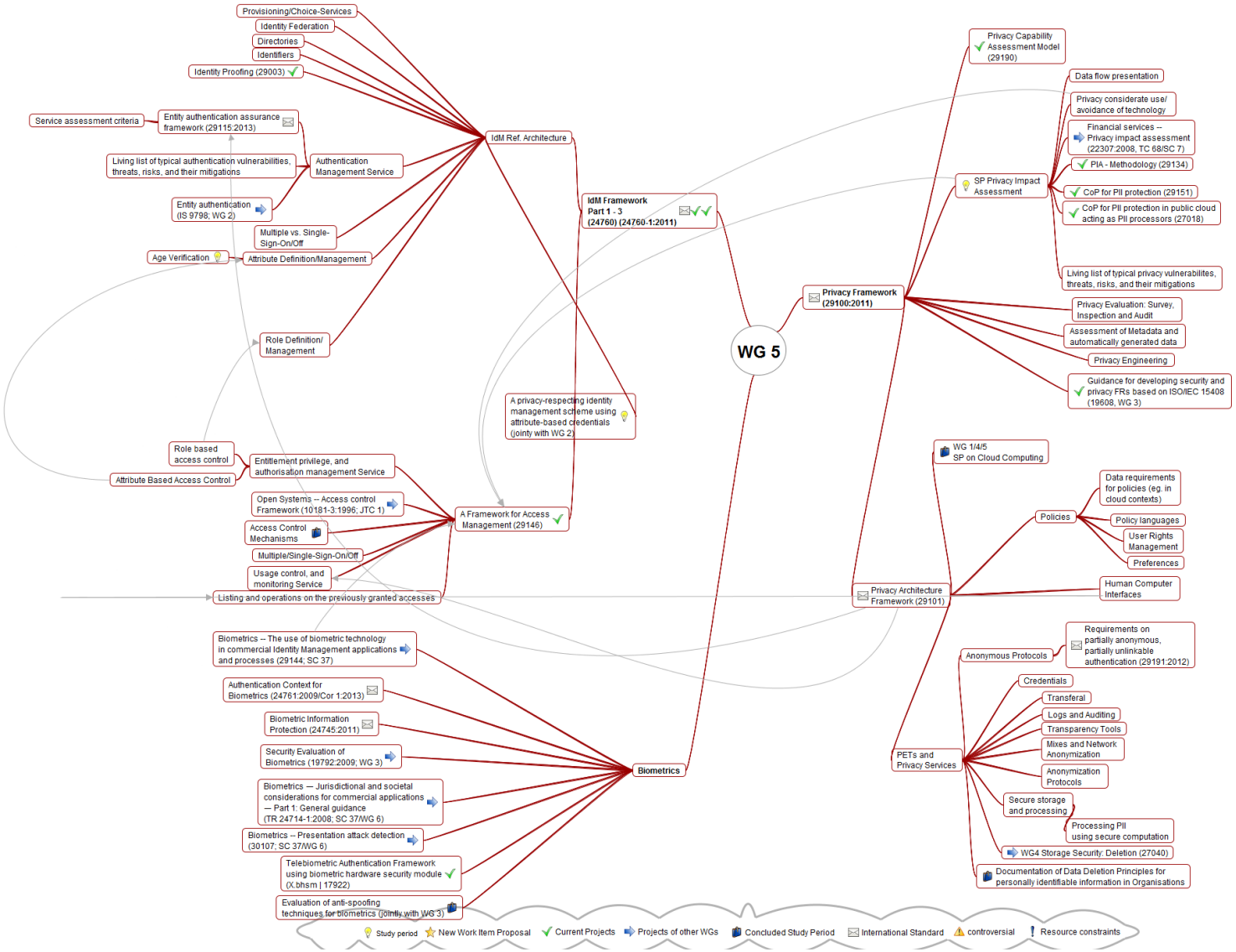
WG 5 Identity Management & Privacy Technologies Roadmap (2010-10)

ISO/IEC JTC 1/SC 27/WG 5 Identity Management & Privacy Technologies



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

ISO/IEC JTC 1/SC 27/WG 5 Identity Management & Privacy Technologies



mobile business

Agenda

- Summary of previous lecture
- Data Protection and Privacy
  - Origin and definition
  - Law, Technology, Standardization
- Technical Privacy Protection
  - Privacy Enhancing Technologies (PETs)
  - Deficiencies
- Integrated Privacy Protection
  - PRIME LBS Application Prototype
  - Privacy Gateway
  - ABC4Trust

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

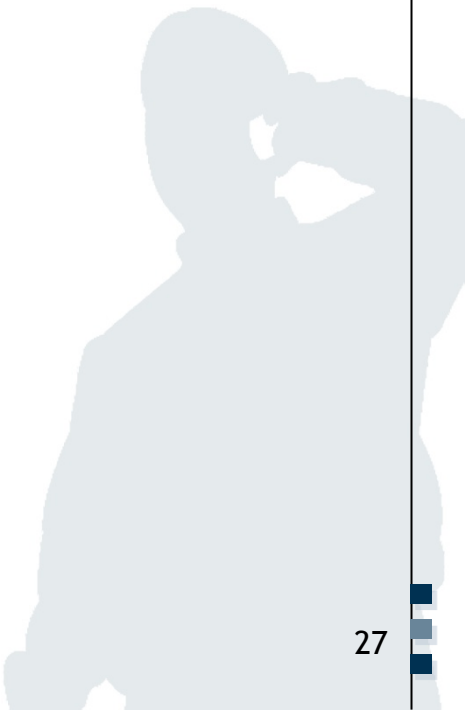
Building blocks and approaches for privacy technologies

- Strong privacy requirements:
  - No trust in the network operator, and
  - No trust into one centralized station.
- Most common methods consider:
  - Privacy-preserving communication systems, or
  - Privacy-preserving transactions

[Federath-2005]

Privacy-preserving 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

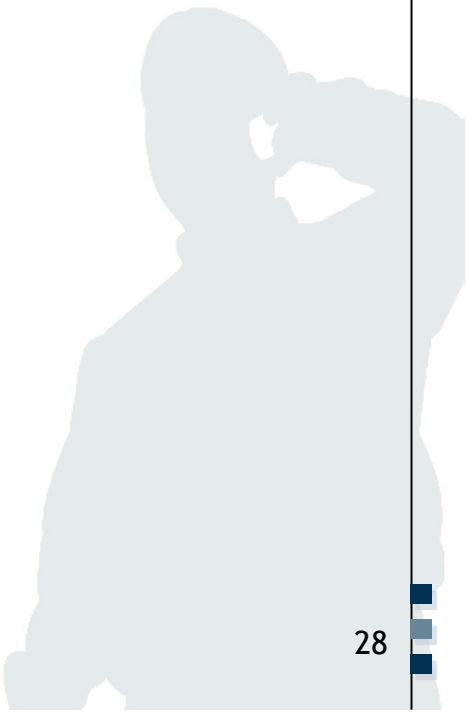


Privacy-preserving transaction systems

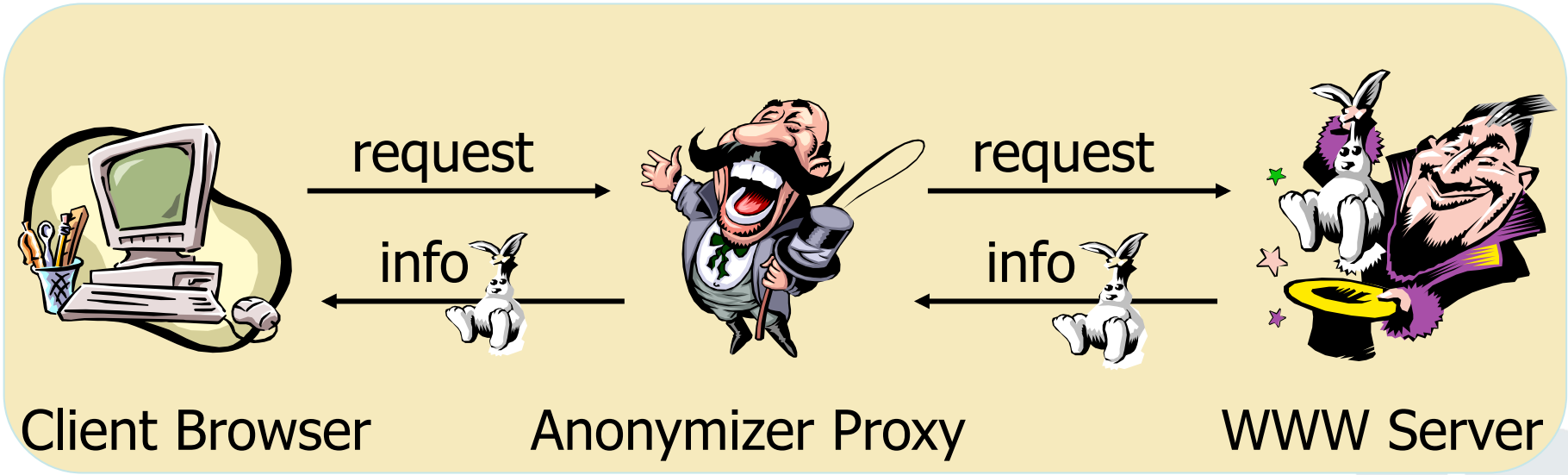
- Reachability Management
- Credential technologies
  - U-Prove

    www.microsoft.com/uprove
  - Idemix

    www.zurich.ibm.com/security/idemix



www.anonymizer.com



www.anonymizer.com

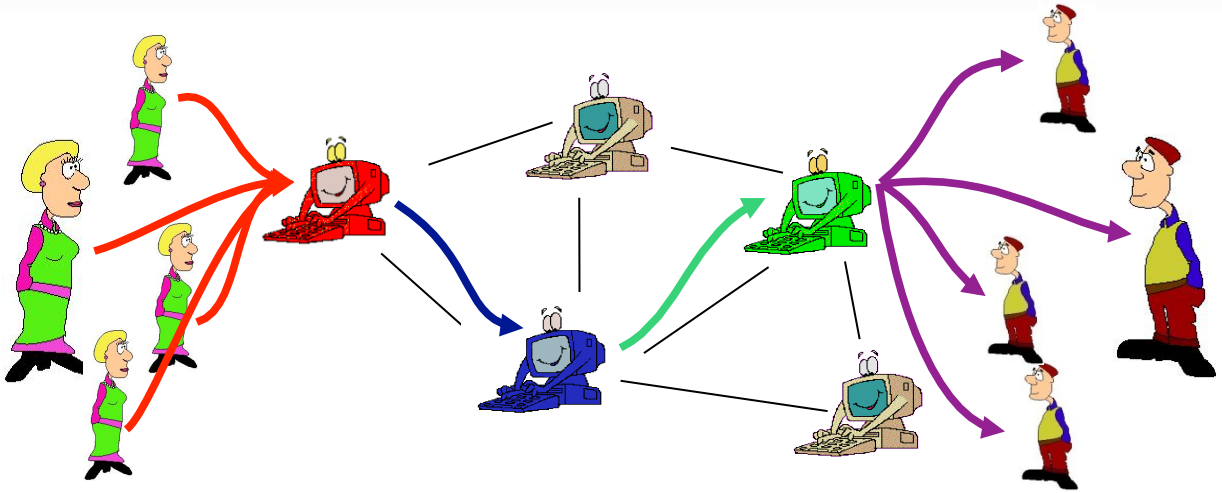
↑ Client (anonymity) is protected in an "**anonymity set**" of all possible proxy clients.

↓ Anonymizer learns about client's activities / interests.

↓ No protection against attackers with global view.

mobile business

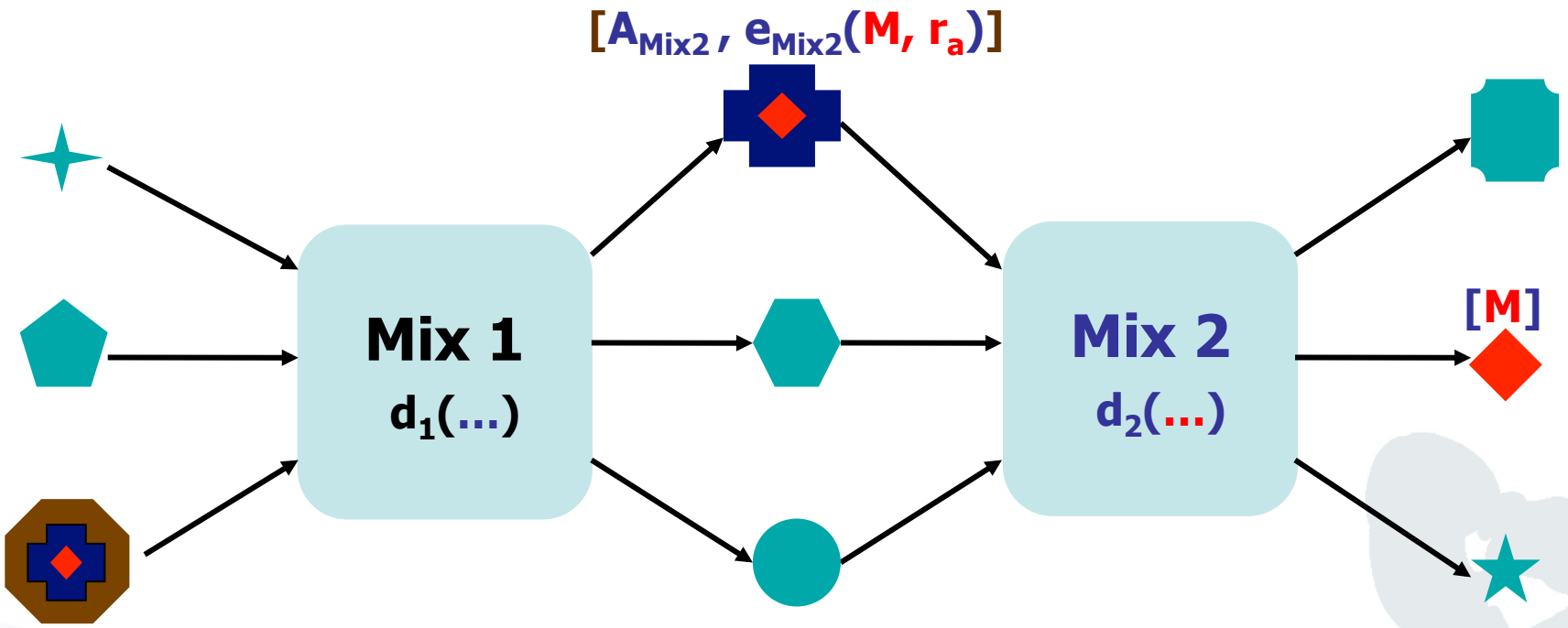
Mixes and Onion Routing



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

mobile business

Mixes



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

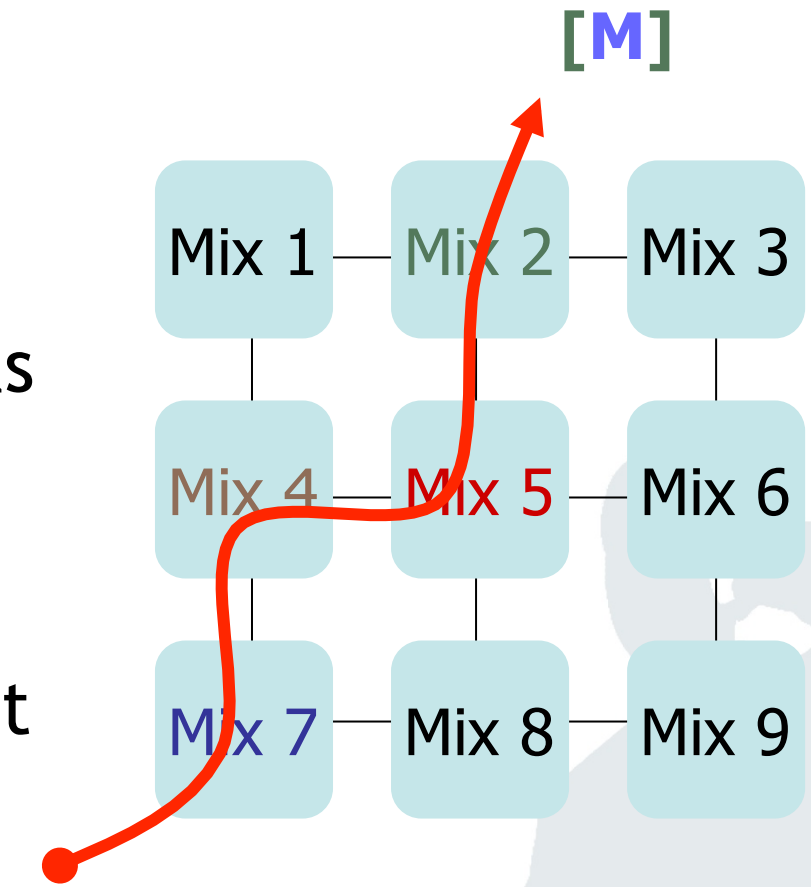
- Decode, buffer, reorder, and resend incoming messages
- Protect **unlinkability** of input / output messages
- Protect **unobservability** of connections and relations
- No single point of trust / failure [Chaum1981]

Symbols:
A address
e() encryption function
d() decryption function
M core message
r random value
[] message boundary

mobile business

Mix network

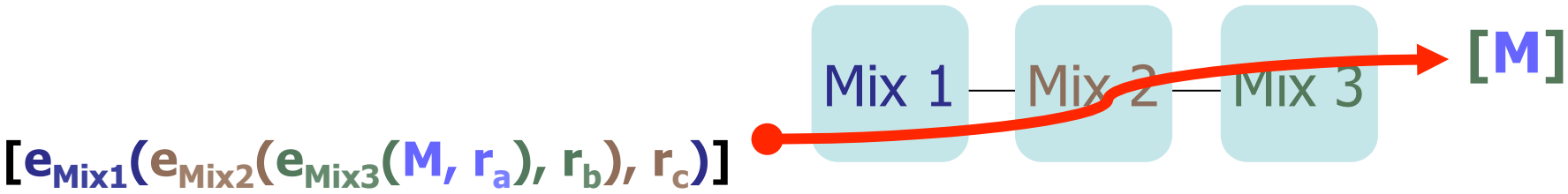
- Choose the way of your message through the mixes!
- Protection guaranteed as long as one chosen mix withstands attacks.
- Free path results in additional confusion, but smaller anonymity set.



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

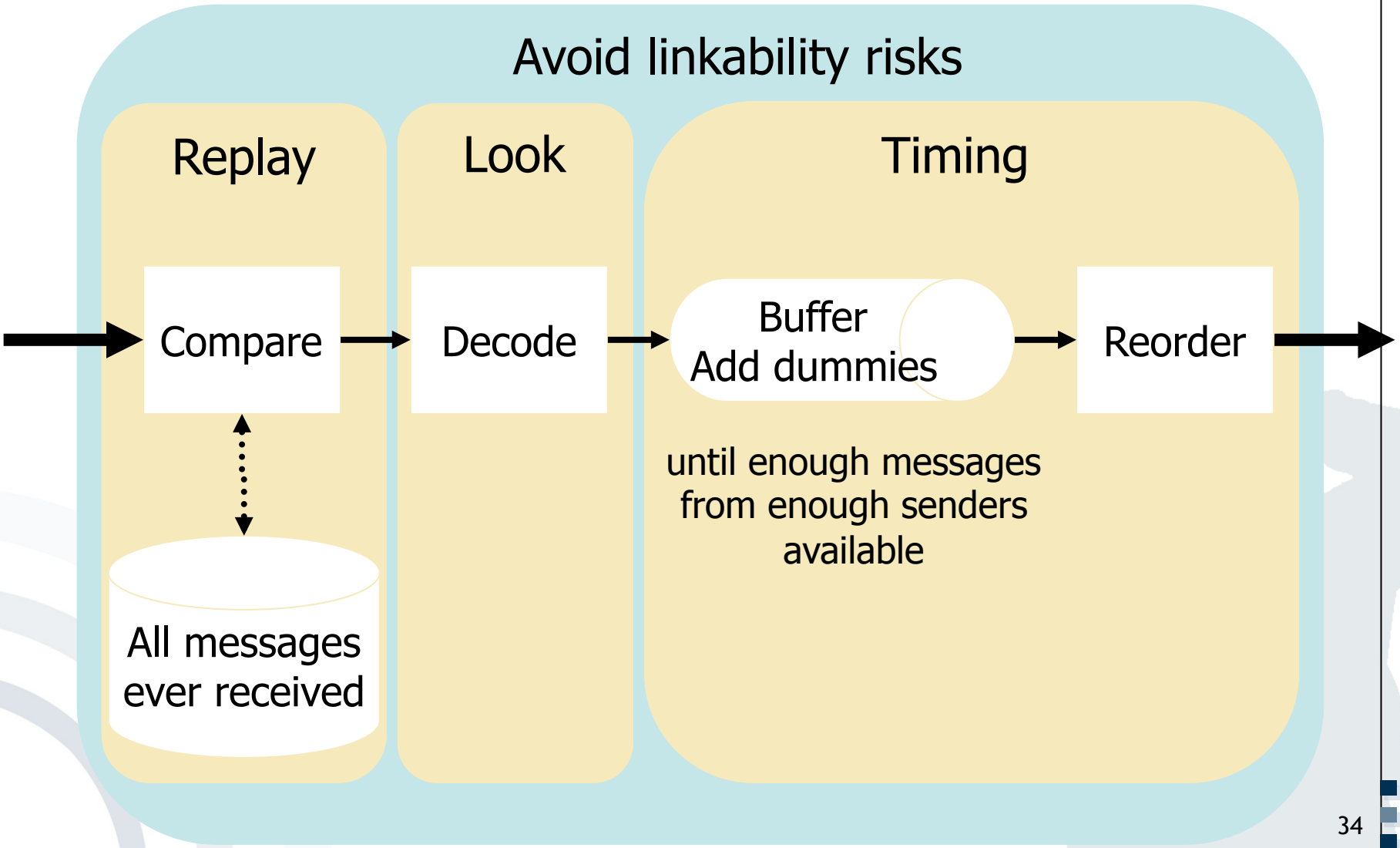
mobile business

Mix cascade



- 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

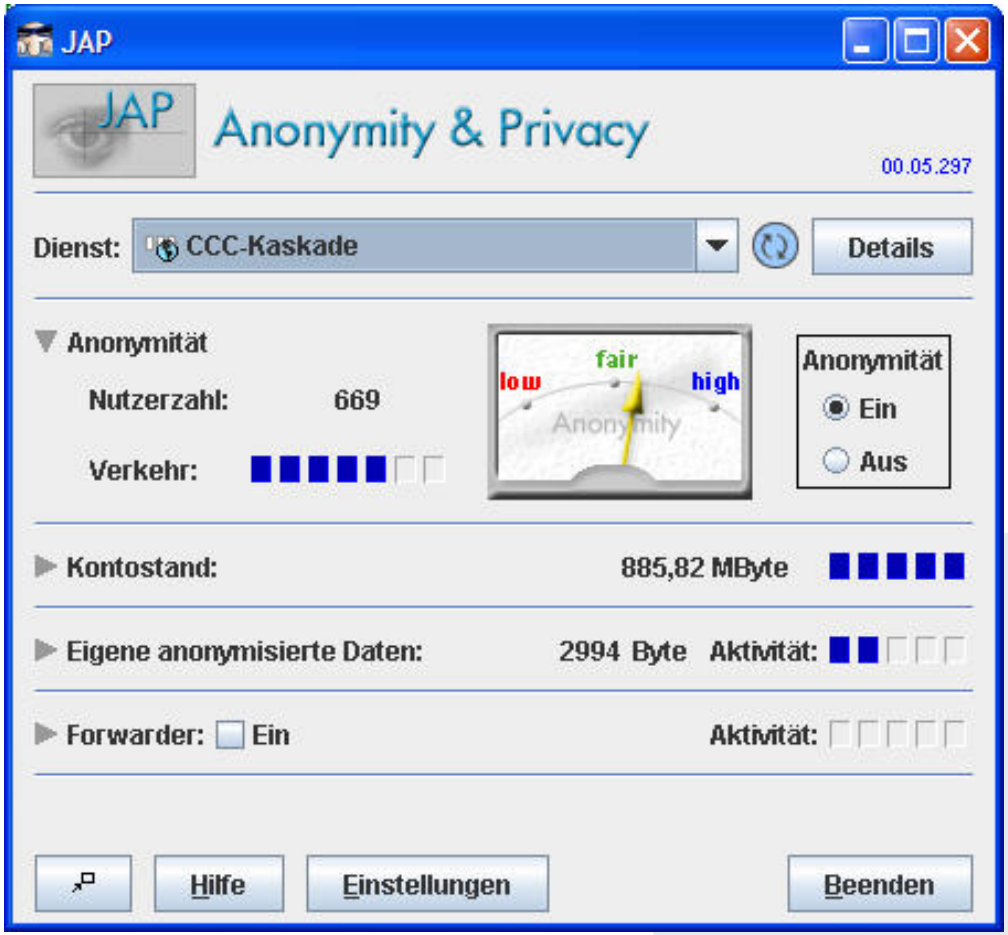
Mixes - Internally



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



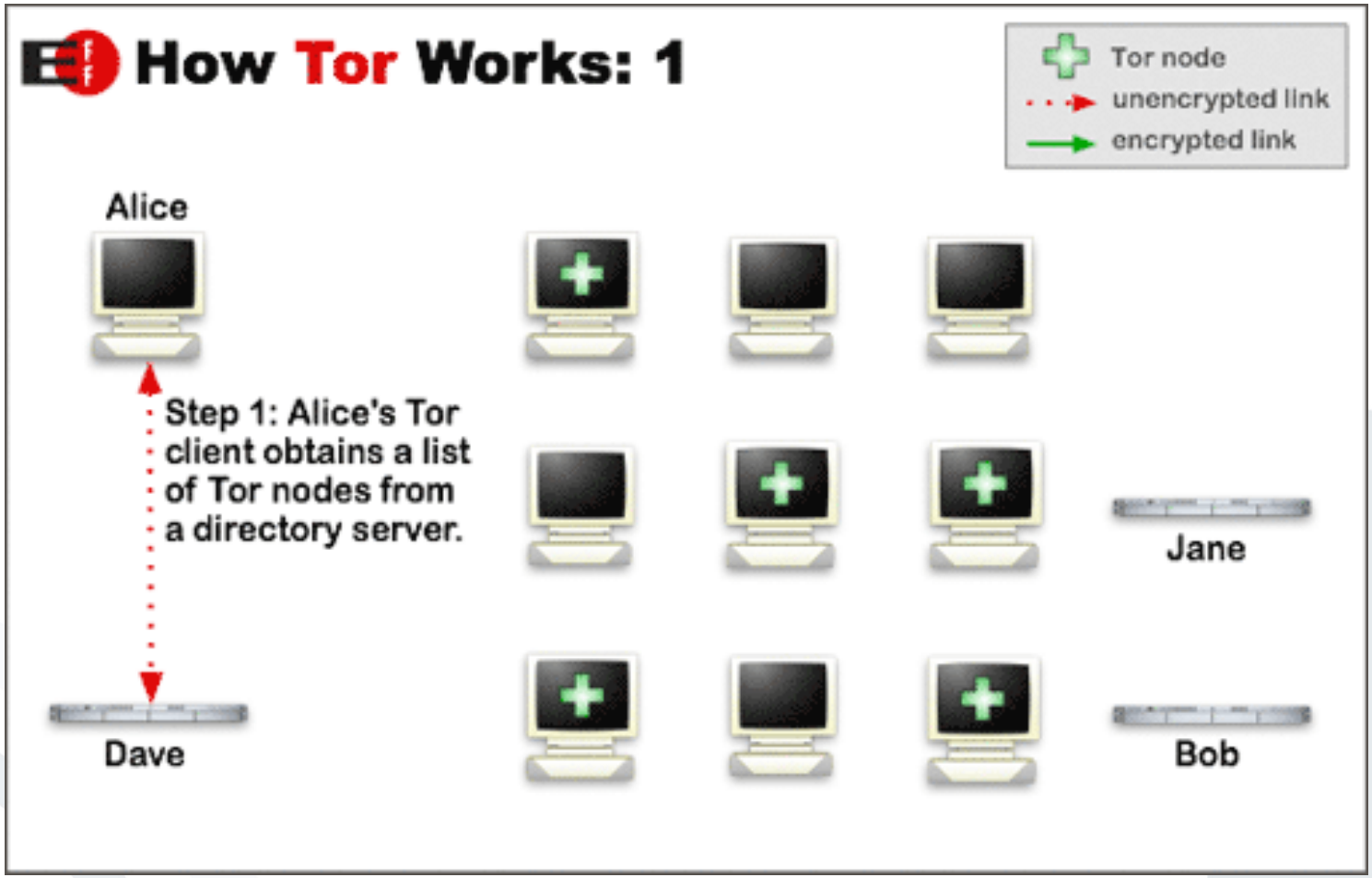
Tor network

- 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]

mobile business

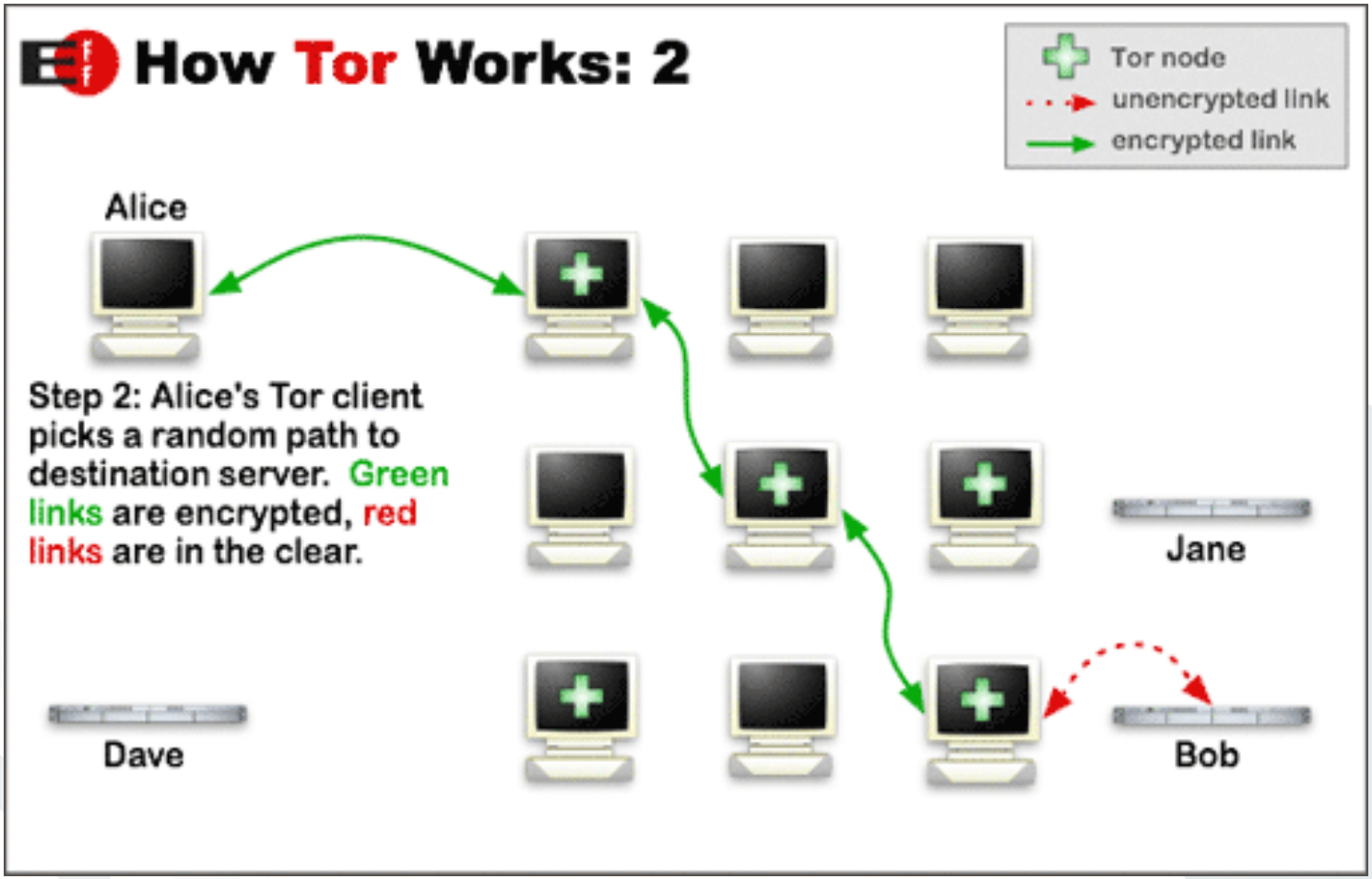
How Tor works I



http://tor.eff.org

mobile business

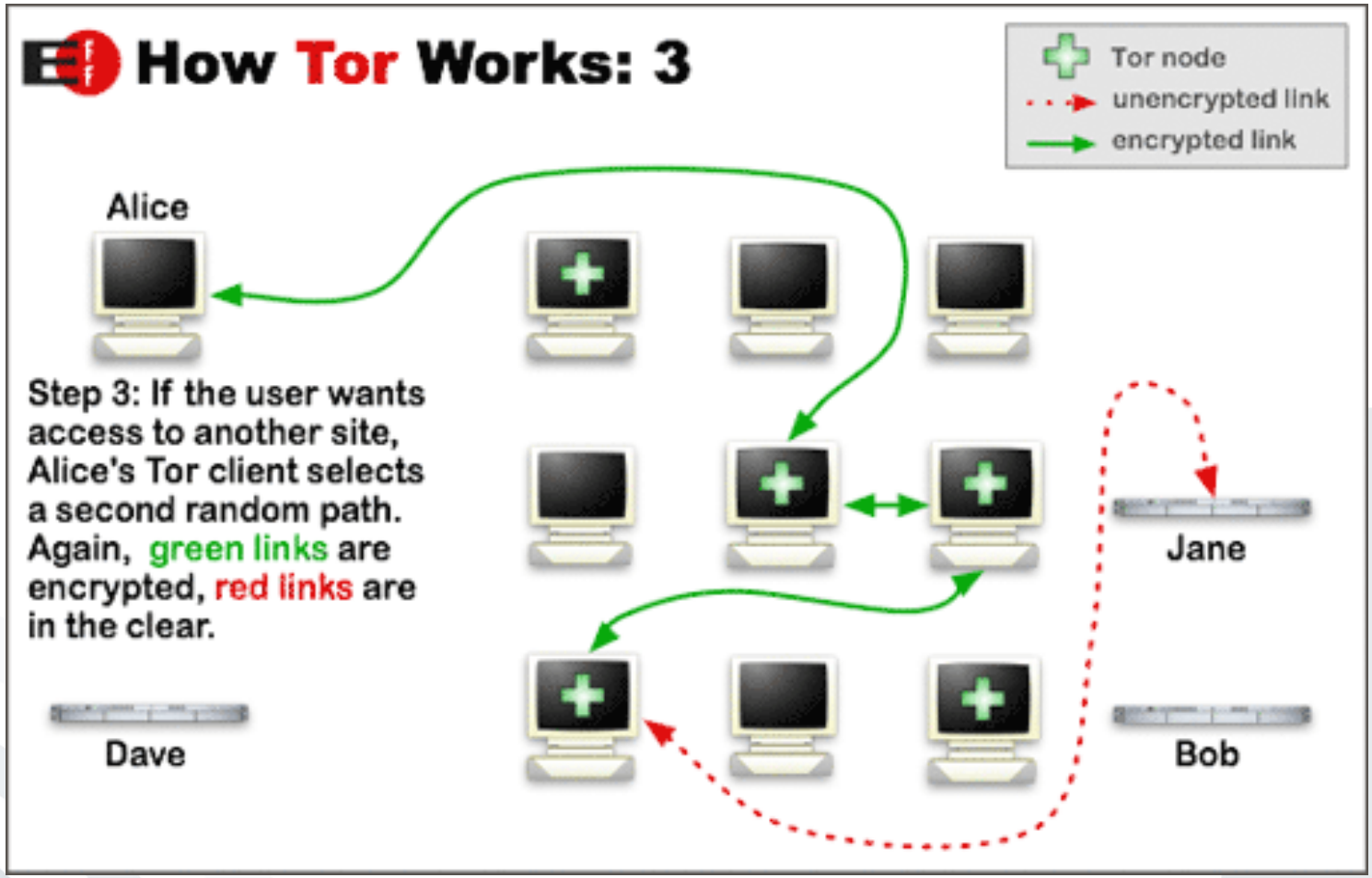
How Tor works II



http://tor.eff.org

mobile business

How Tor works III



http://tor.eff.org

Attacks on Tor

Evil Exit Node

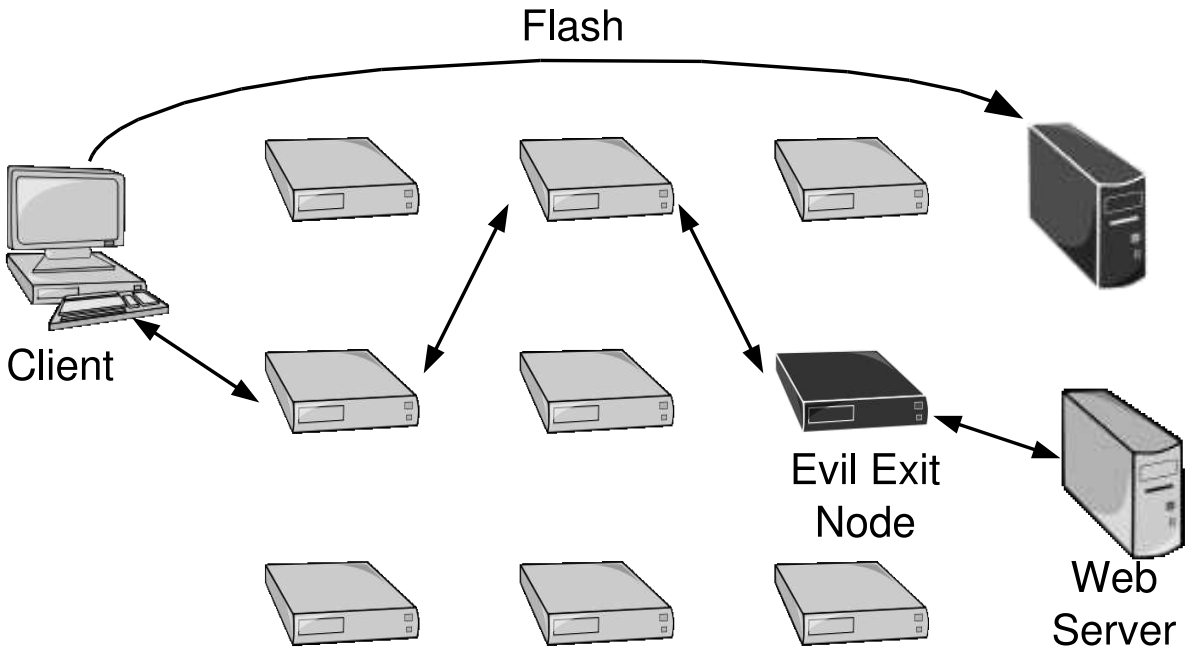


Fig. 3. A browser attack executed by an exit node. The client's web browser executes a Flash program inserted into a webpage by the exit node, which opens a direct connection to a logger machine.

[AbLa2007]

Attacks on Tor

Evil Exit Node attack materialized

- Almost 20 exit relays in the Tor anonymity network that attempted to spy on users' encrypted traffic using man-in-the-middle techniques.
- Exit relays detected sniffing the traffic (both HTTP and SSL sniffing attacks)

WIRED GEAR SCIENCE ENTERTAINMENT BUSINESS SECURITY DESIGN OPINION MAGAZINE

THREAT LEVEL | anonymity | russia | Tor

Russian Spy Nodes Caught Snooping on Facebook Users

BY KEVIN POULSEN 01.21.14 | 5:52 PM | PERMALINK

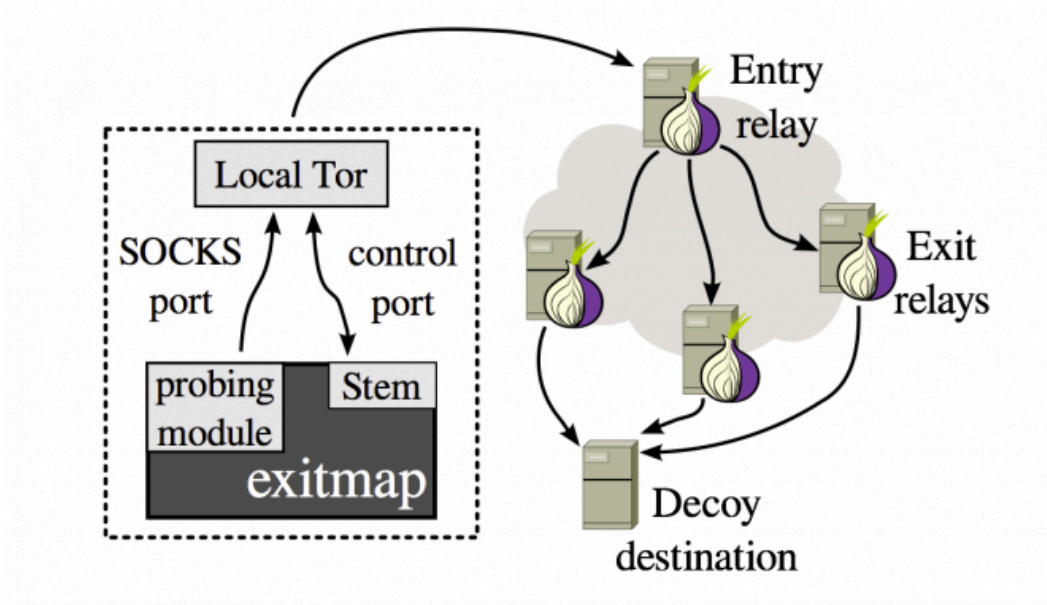


Image courtesy of Philipp Winter and Stefan Lindskog

[http://www.wired.com/2014/01/russia-tor-attack/, 21.1.2014]

Attacks on Tor

Evil Web Server

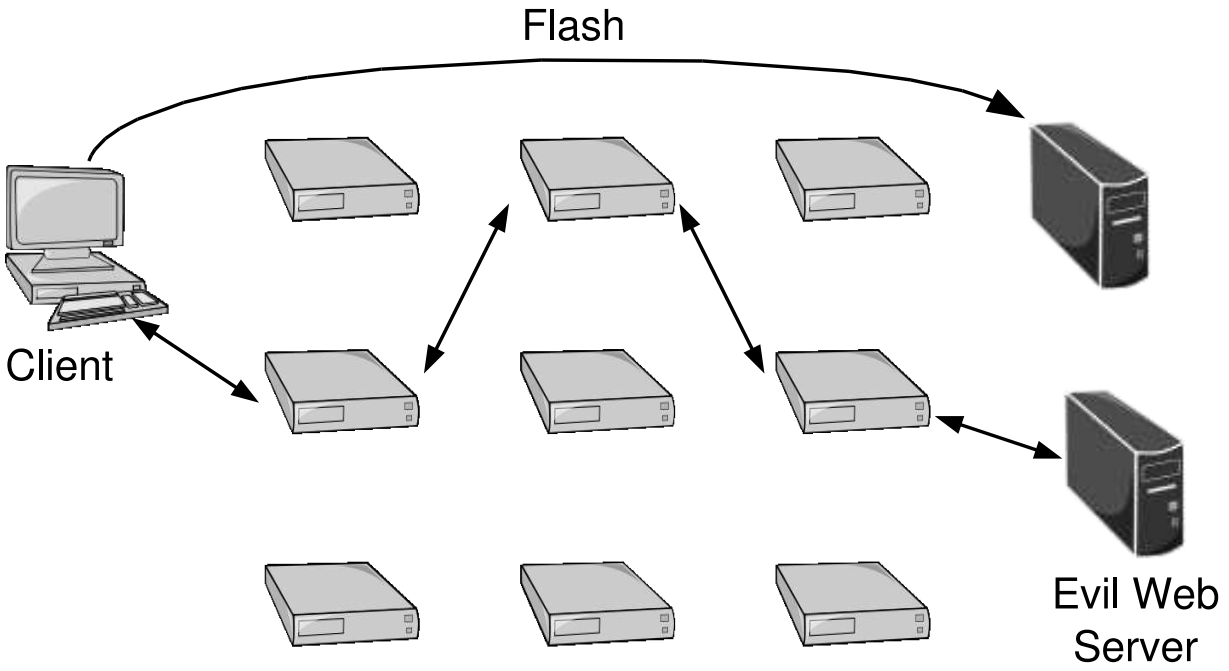


Fig. 2. A browser attack using Flash included in a website. The client's web browser executes a Flash program, which then opens a direct connection to a logger machine, compromising the client's anonymity.

[AbLa2007]

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

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.

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

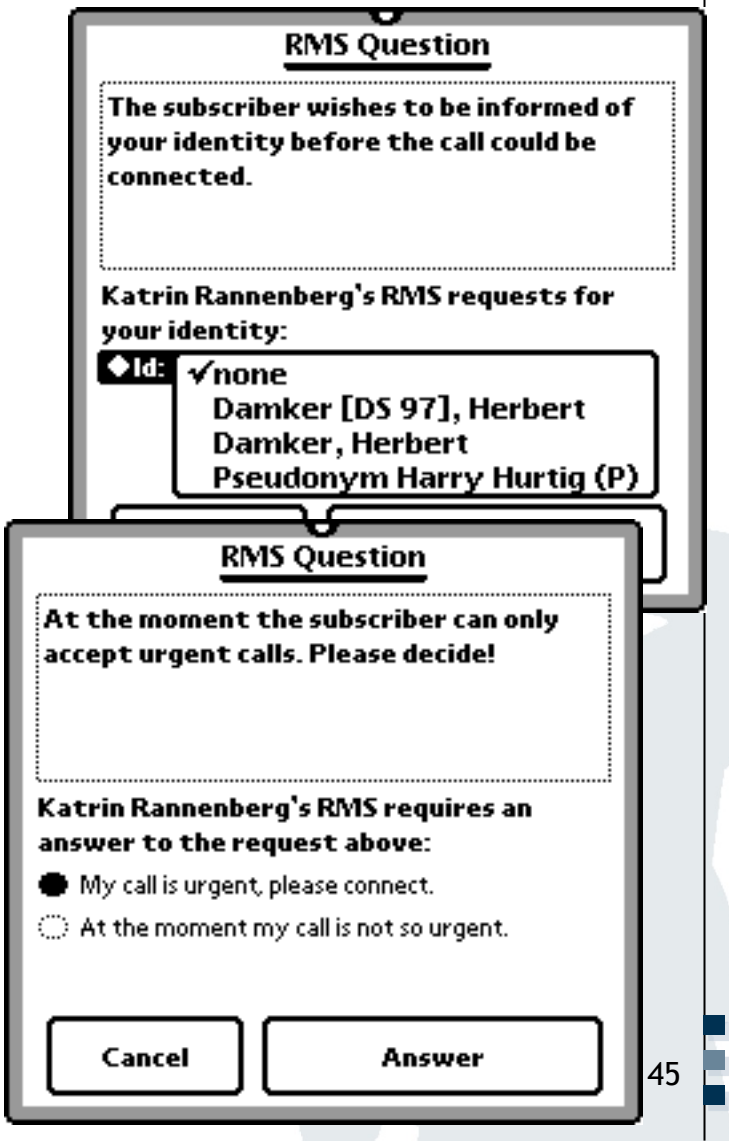
"I welcome you calling back."

Provision of a reference

"My friends are your friends!"

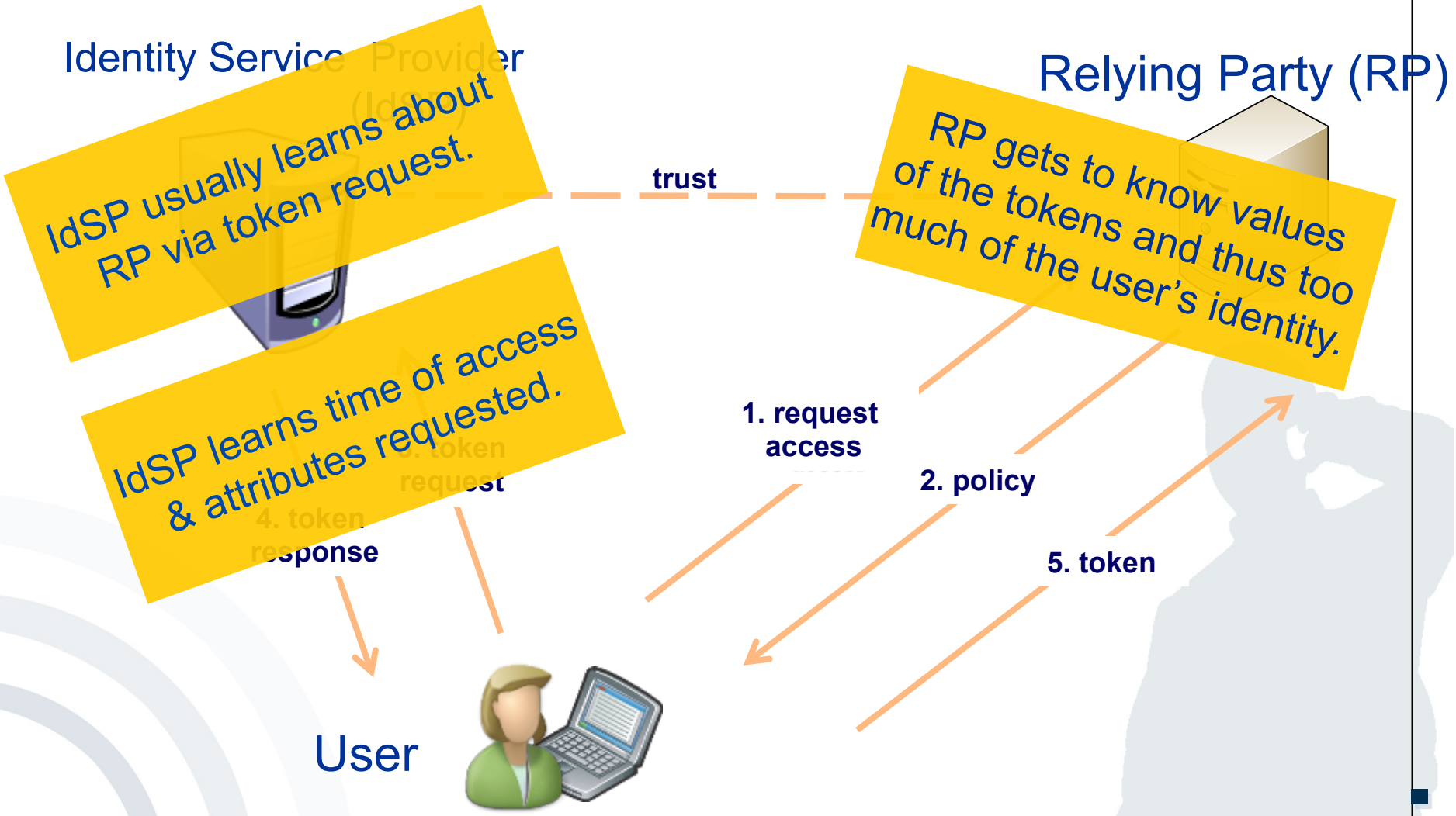
Offering a surety

"Satisfaction guaranteed
or this money is yours!"



[Rannenberg2000]

Privacy (and security) issues of typical federated IdM architectures



mobile business

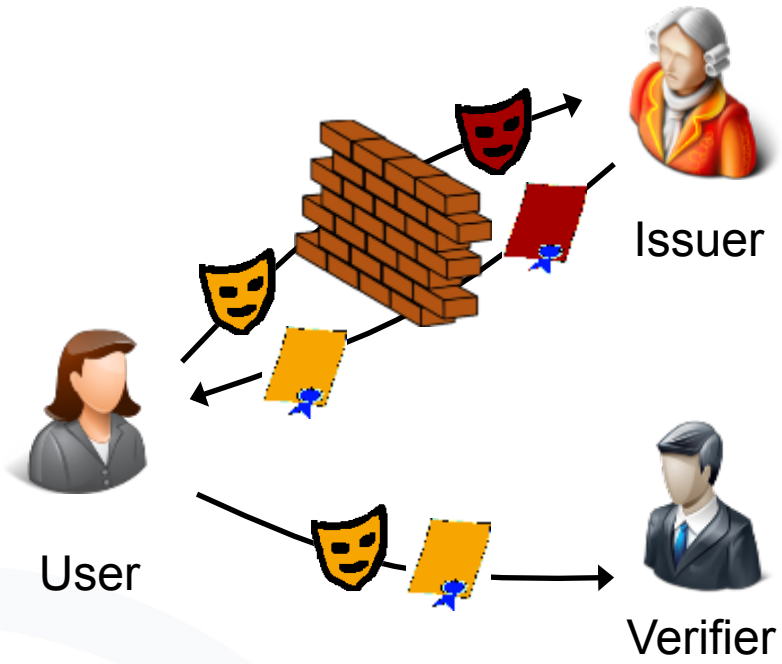
Credential Systems

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

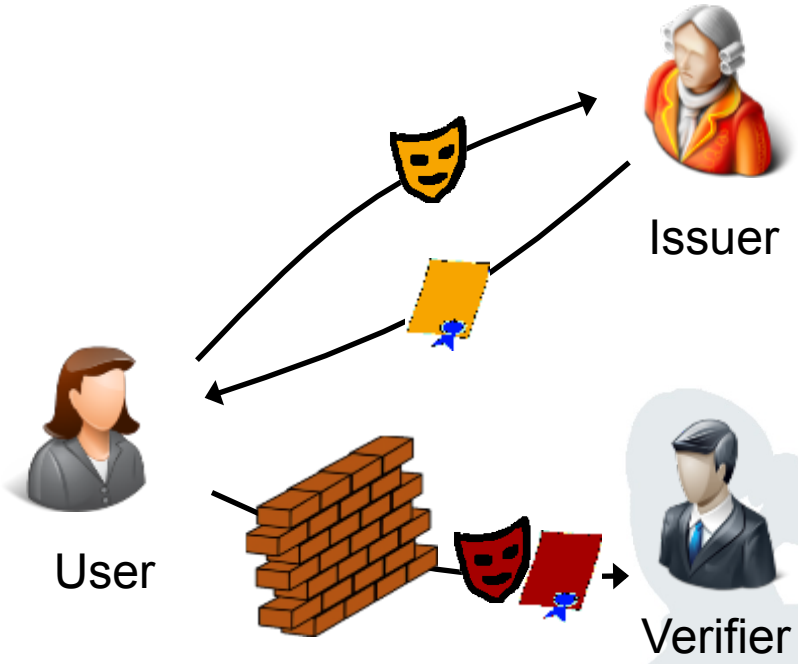
Blind Signatures



U-Prove

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

Zero-Knowledge Proofs

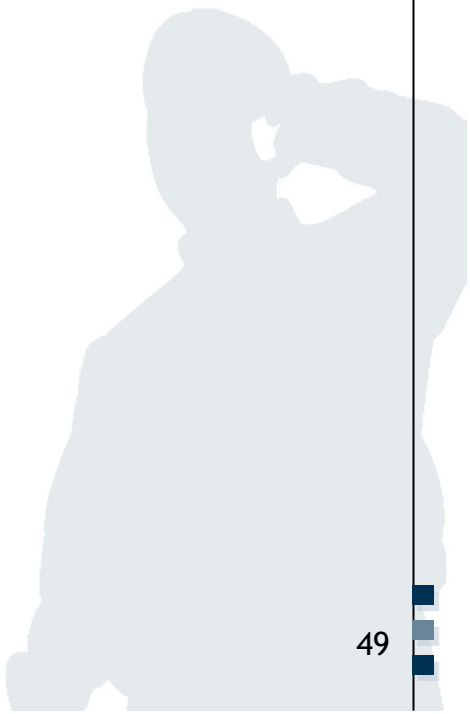


Idemix (Identity Mixer)

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

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



mobile business

Agenda

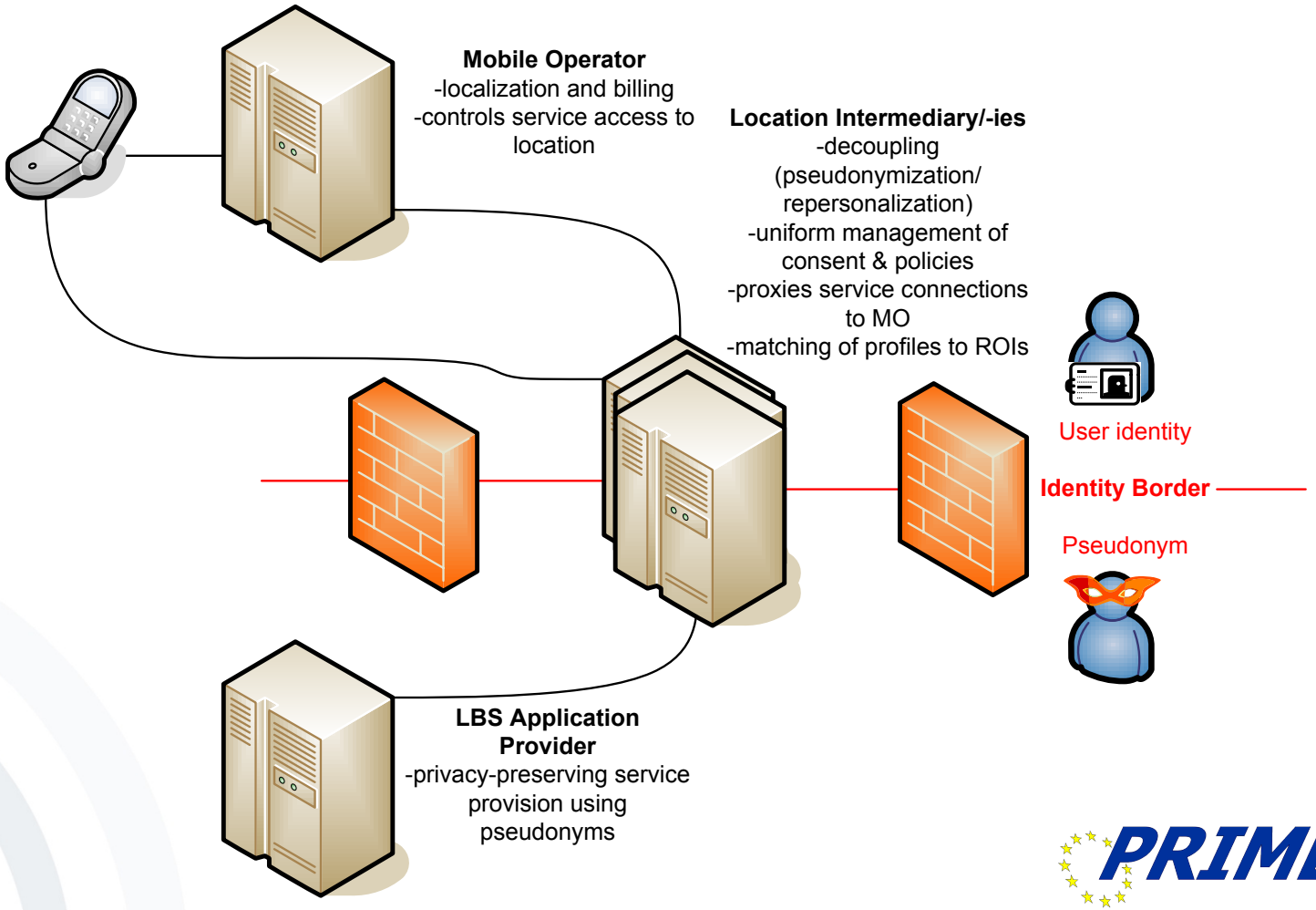
- Data Protection and Privacy
  - Origin and definition
  - Law, Technology, Standardization
- Technical Privacy Protection
  - Privacy Enhancing Technologies (PETs)
  - Deficiencies
- Integrated Privacy Protection
  - PRIME LBS Application Prototype
  - Privacy Gateway
  - ABC4Trust

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

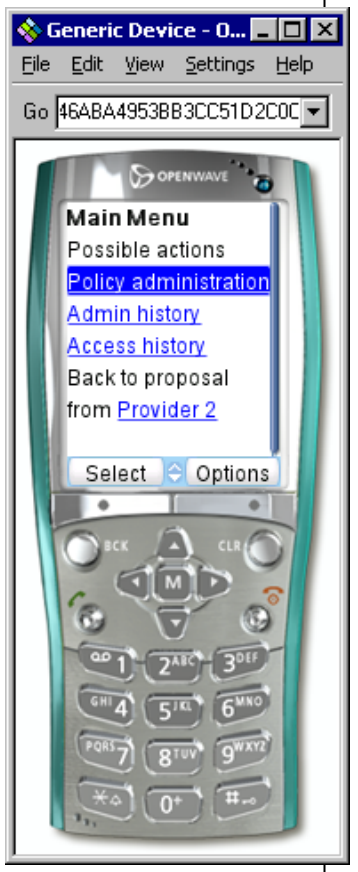
PRIME LBS Application Prototype Intermediary Approach

Architecture Overview



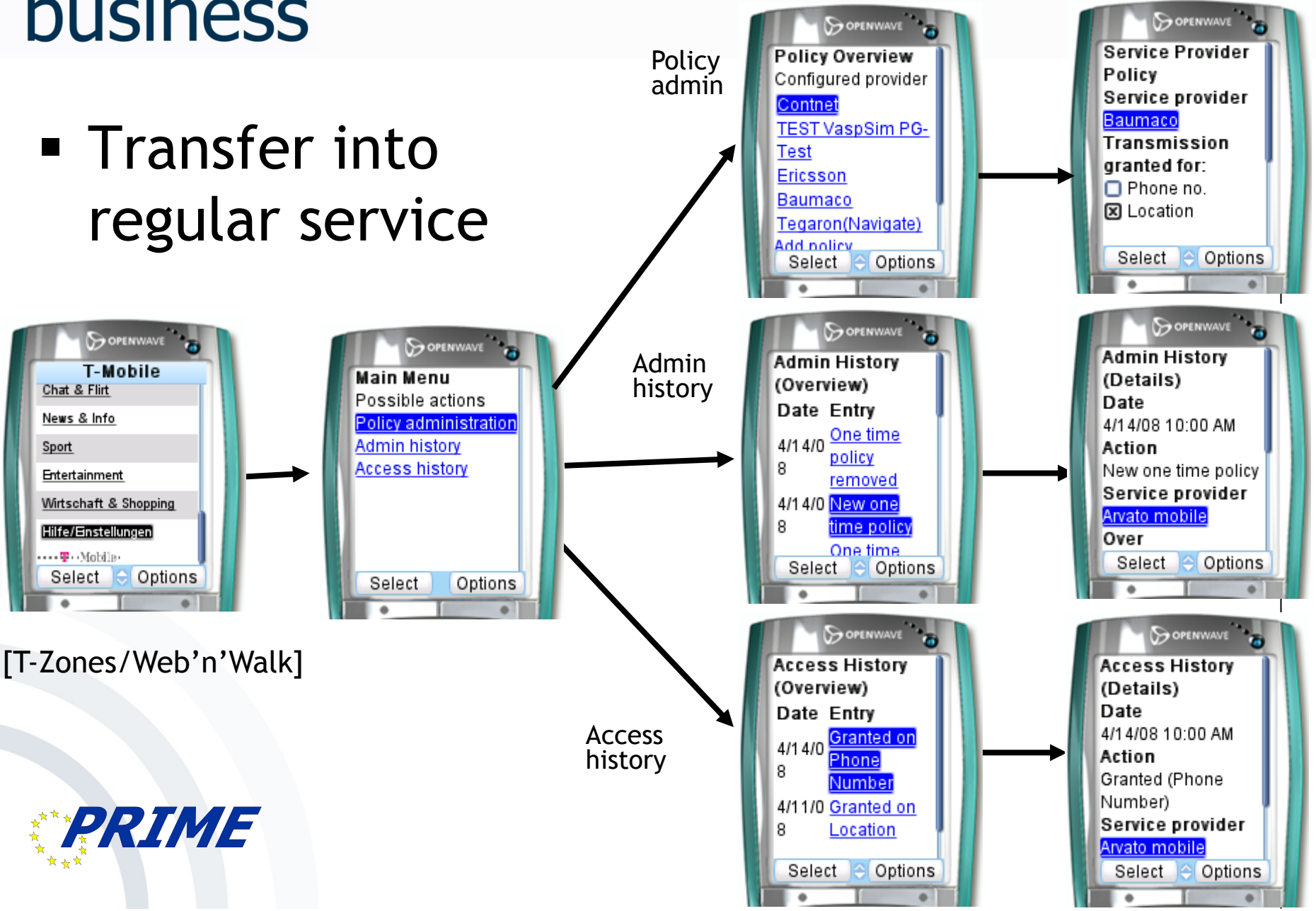
Privacy Gateway

- 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

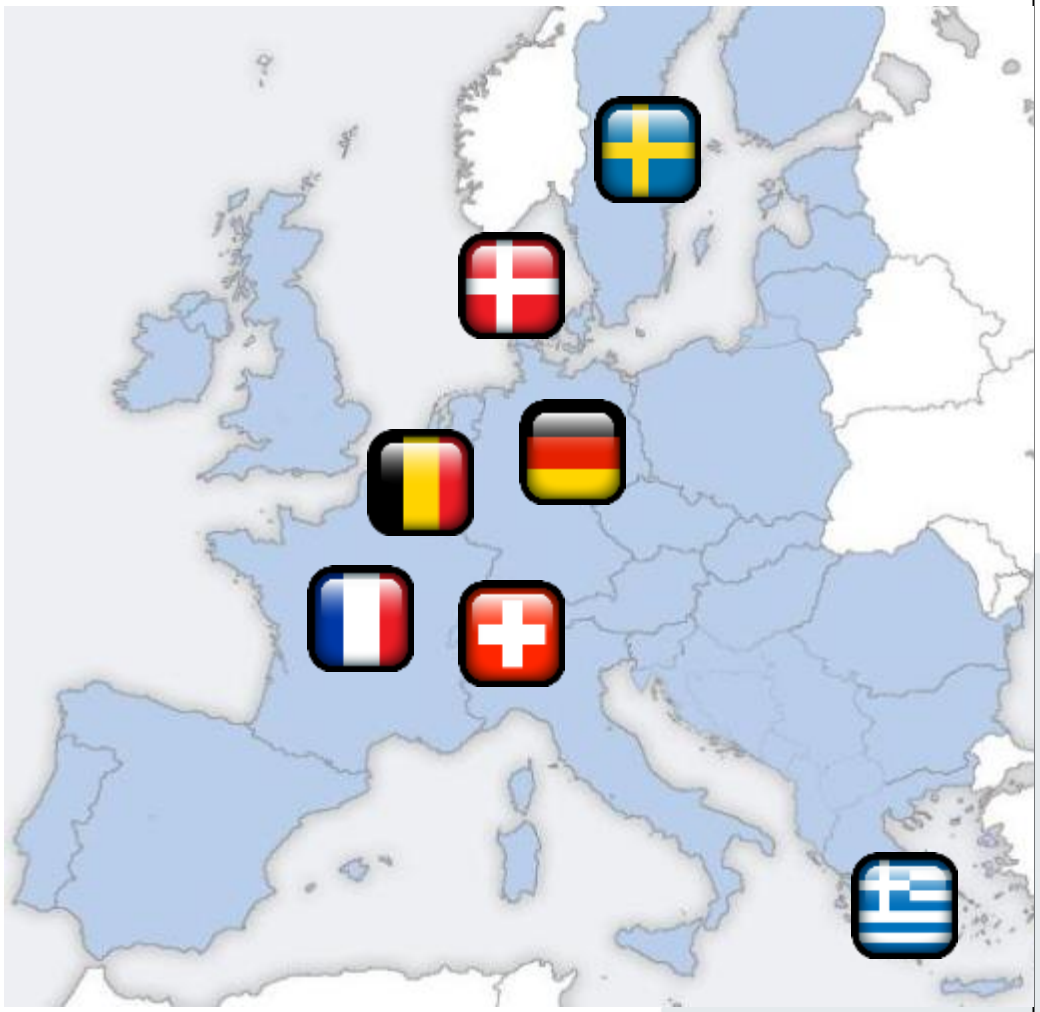
- Transfer into regular service



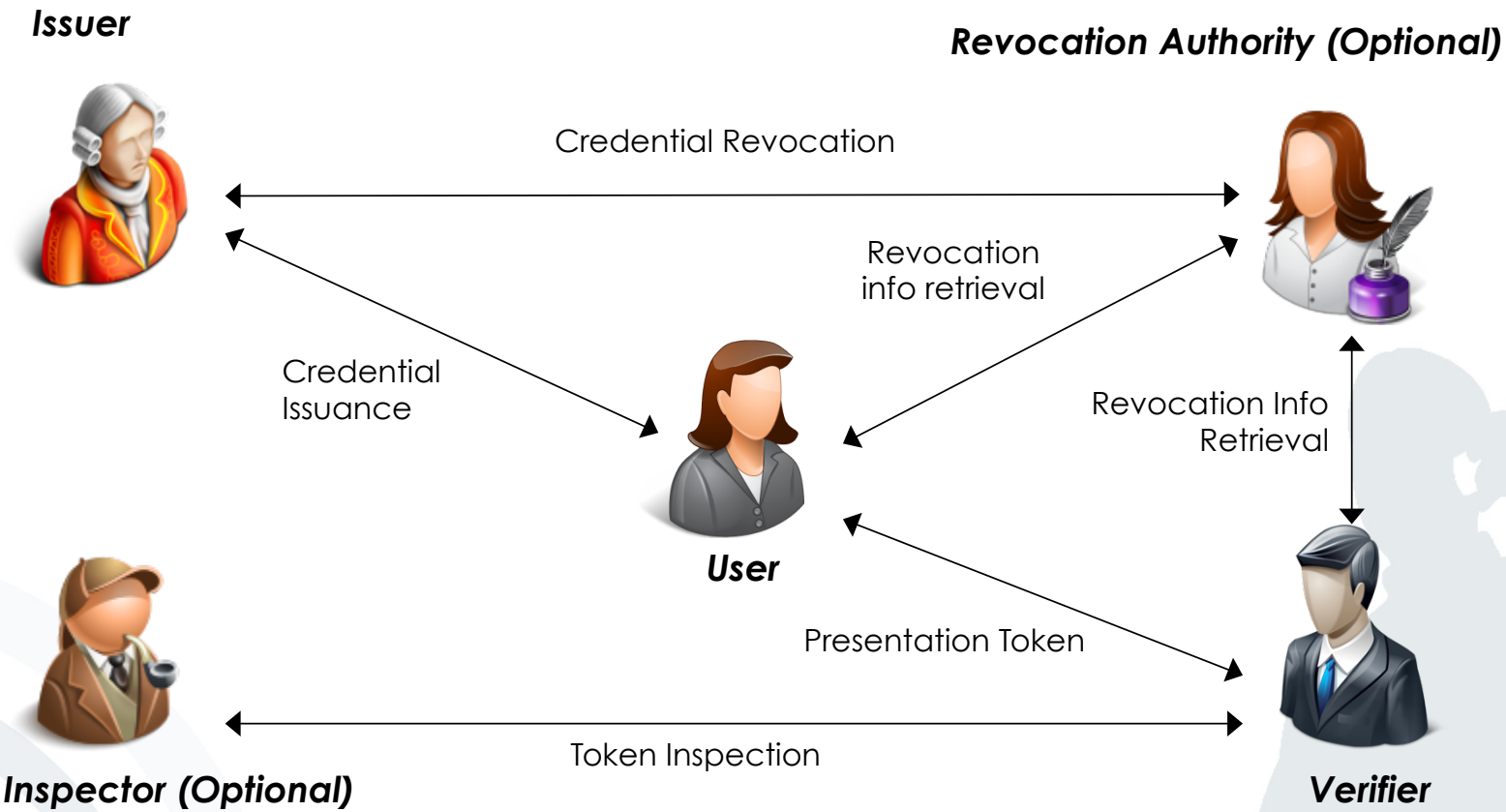
[T-Zones/Web'n'Walk]

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.



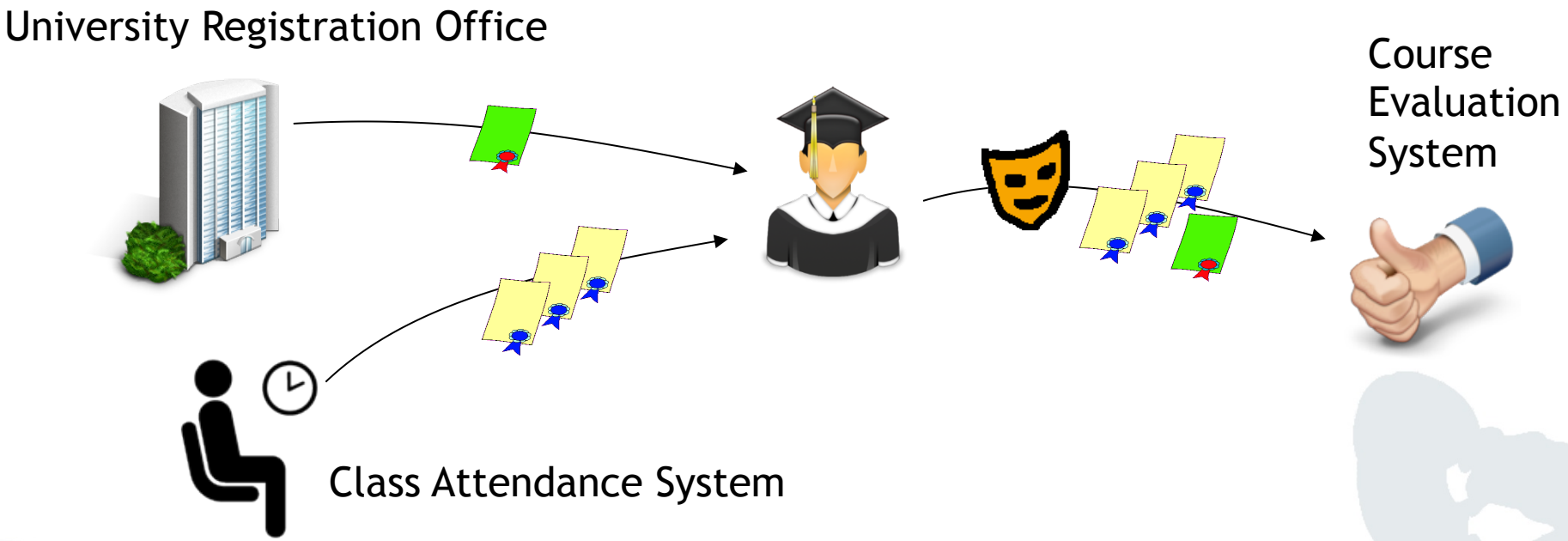
ABC4Trust Architecture High Level View



ABC4Trust Pilots

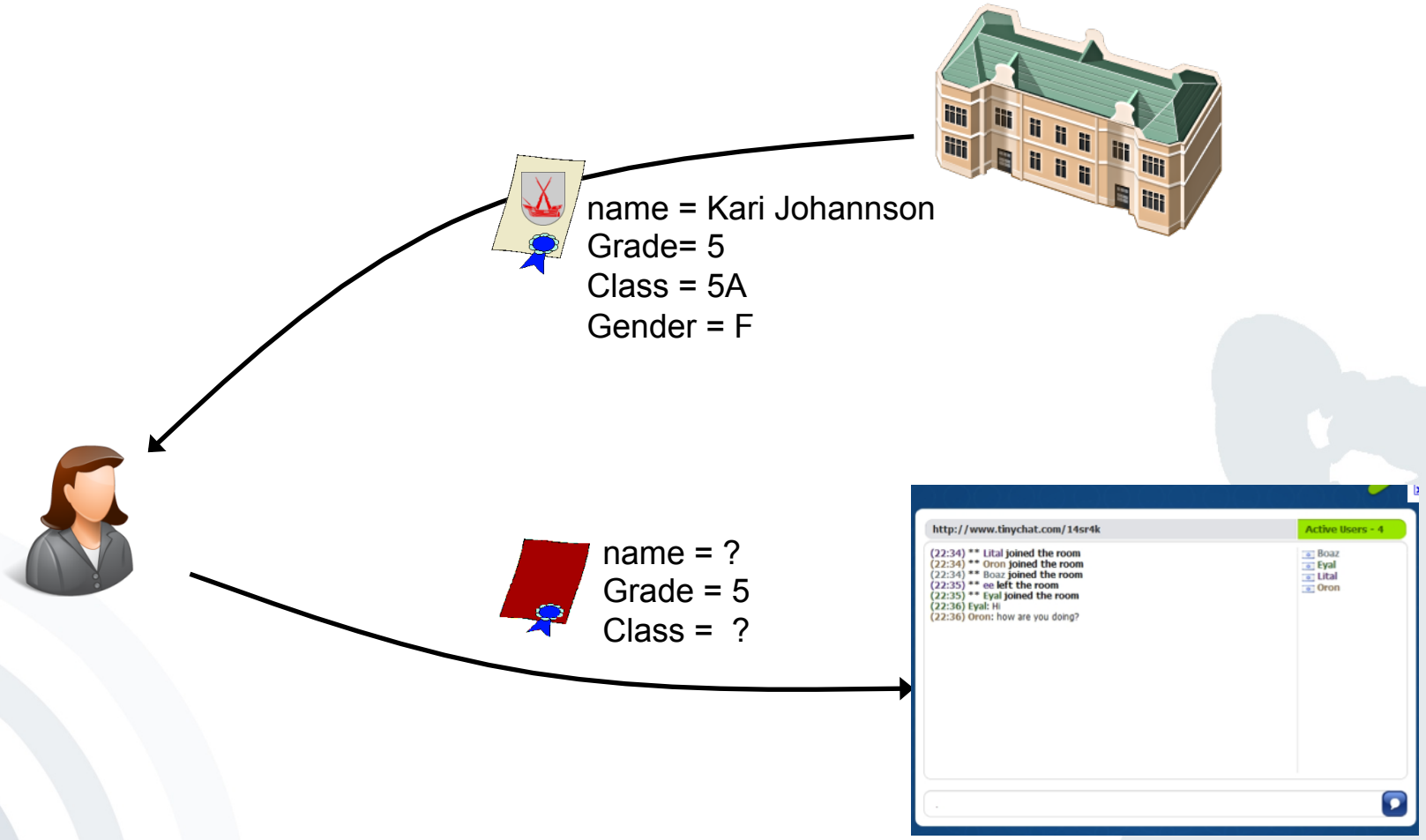
- ABC4Trust tested the technology in two pilots:
  - Anonymous course evaluation in the University of Patras, Greece.
    - Students used smartcards to collect credentials for the courses they are attending.
    - At the end of semester they were able to evaluate the course if they have attended enough 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



mobile business

References

[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.

[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.

[BVwG2003] Bundesverwaltungsgericht: Entscheidung BVerwG 6 C 23.02; www.bundesverwaltungsgericht.de/enid/d90753334a813794b15cc66003046de0,0976e0736561726368 5f646973706c6179436f6e7461696e6572092d0933353031/8o.html

[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

[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

[EC2014] Progress on EU data protection reform now irreversible following European Parliament vote. Accessed at http://europa.eu/rapid/press-release_MEMO-14-186_en.htm on 12.11.2014.

[EC-Prot-2014] European Commission: Protection of personal data: http://ec.europa.eu/justice/data-protection/index_en.htm

[Federath-2005] Hannes Federrath: Privacy Enhanced Technologies: Methods - Markets - Misuse. Proc. 2nd International Conference on Trust, Privacy, and Security in Digital Business (TrustBus '05). LNCS 3592, Springer-Verlag, Heidelberg 2005, 1-9.

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

[ICDPPC 2005] The 27th International Conference of Data Protection and Privacy Commissioners: “The protection of personal data and privacy in a globalised world: a universal right respecting diversities (The Montreux Declaration)”, 2005-09-14/16; Montreux, Switzerland; www.privacyconference2005.org/fileadmin/PDF/montreux_declaration_e.pdf

[ISO29100] ISO/IEC: ISO/IEC 29100:2011 – Information technology – Security techniques – Privacy framework, 2011.

[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