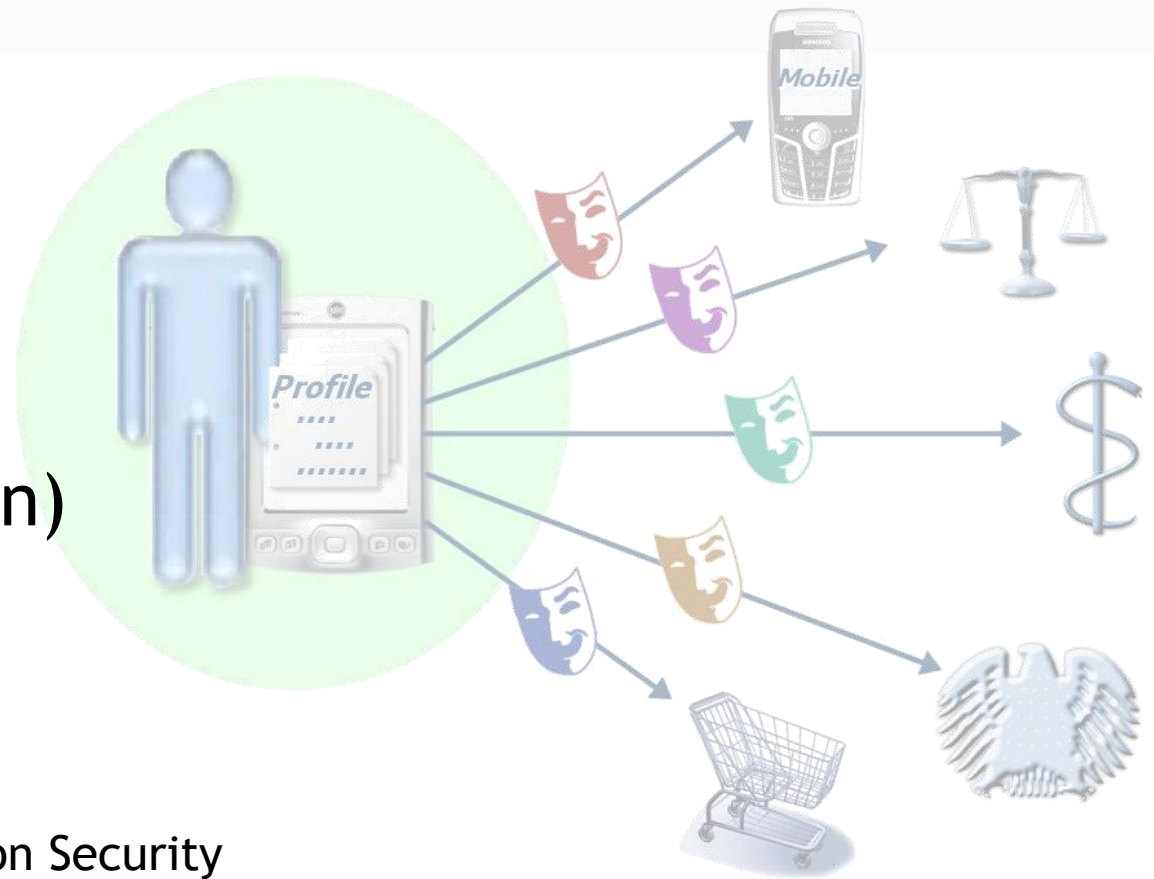


Lecture 8

Identity Management II (Privacy Protection)



Information & Communication Security
(WS 2010/11)

Prof. Dr. Kai Rannenber

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

- Summary of previous lecture
- Data Protection and Privacy
 - Origin and definition
 - Law, Technology, Standardisation
- Technical Privacy Protection
 - Privacy Enhancing Technologies (PETs)
 - Deficiencies
- Integrated Privacy Protection
 - Personal Identity Management
 - PRIME
 - Integrated Solutions, e.g. for LBS

- Introduction
- Identity
- Identity Management
 - Functions
 - Systems
 - Types
 - Account Management
 - Single Sign On
 - Federated Identity Management
 - Profiling,
 - Examples from CRM and the Internet
 - Dataveillance
 - Personal Identity Management
 - Privacy Enhancing Technologies

Type 1



Type 2



Type 3



Account Management:
assigned identity
(= Tier 2)

Profiling:
derived identity
abstracted identity
(= Tier 3)

Management of
own identities:
chosen identity
(= Tier1)

by organisation

by organisation

by user himself
supported by
service providers

➔ There are hybrid systems
that combine characteristics

- Summary of previous lecture
- Data Protection and Privacy
 - Origin and definition
 - Law, Technology, Standardisation
- Technical Privacy Protection
 - Privacy Enhancing Technologies (PETs)
 - Deficiencies
- Integrated Privacy Protection
 - Personal Identity Management
 - PRIME
 - Integrated Solution, e.g. for LBS

- 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 [WaBr1890].
- Data protection in Germany (“Datenschutz”) originates from concerns over too much information und 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

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

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.

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
- ⇒ Standardisation

- 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

- 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.

- 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.

- **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

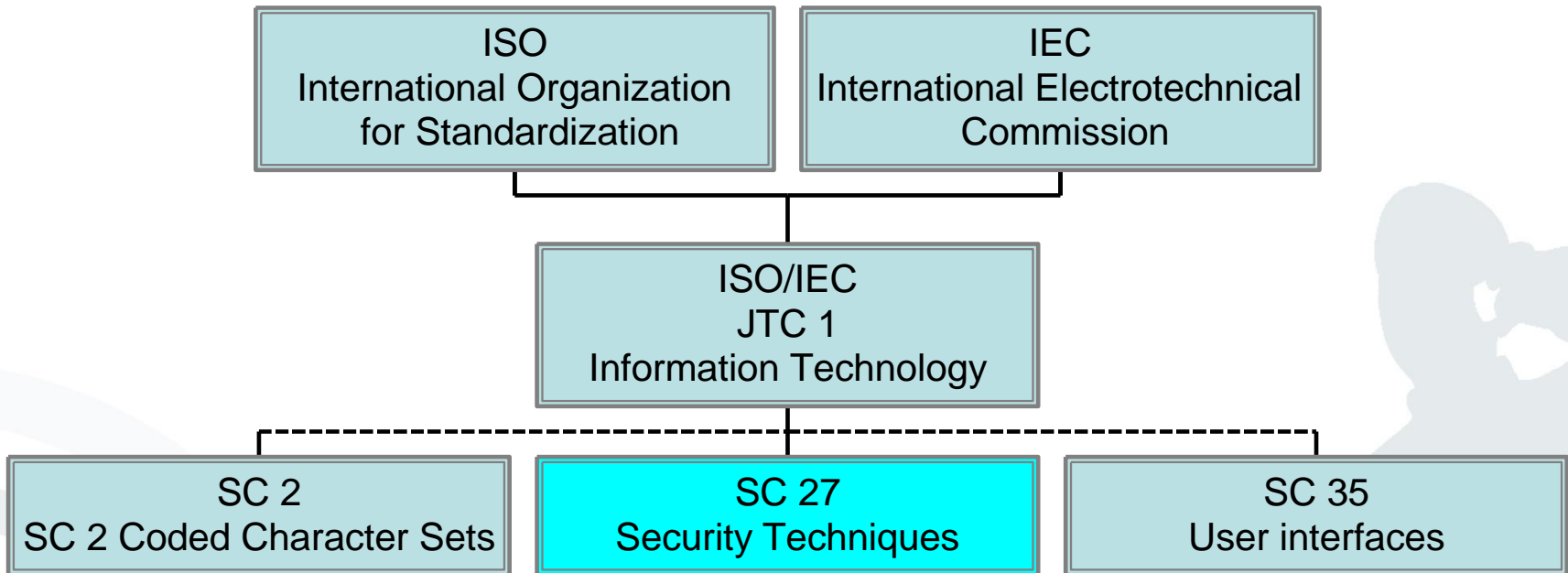
- **Control by the User**

- 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

Some Privacy (related) work in ISO standardisation (ISO/IEC JTC 1)

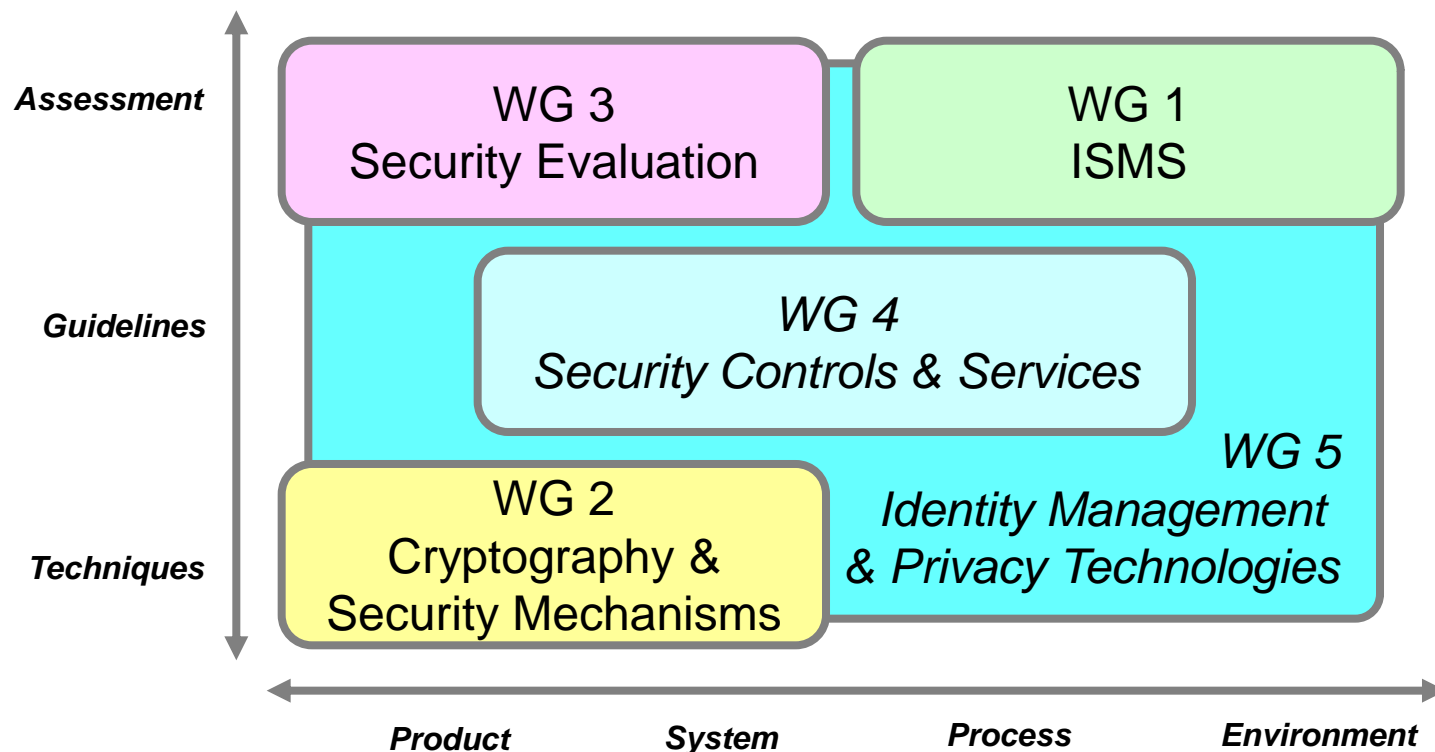
- 1990es: Privacy mentioned in at least one SC 27 standards and drafts, e.g. **ISO/IEC 15408 “Evaluation Criteria for IT Security”**
- **2003/04: JTC1 Privacy Technology Study Group**
 - After intensive discussion recommendation to position the topic to SC 27
 - “Having reviewed and discussed the report of the Privacy Technology Study Group contained in document JTC 1 N 7634, JTC 1 resolves that, for the time being, any new NPs that may arise related to privacy technology, not related to ongoing activities in other SCs, are assigned to SC 27.” [Resolution 13 of the October 2004 JTC 1 Plenary]
 - Study group disbanded [Resolution 20 of the October 2004 JTC 1 Plenary]
- **2004: ISTPA Privacy Framework**
 - submitted as a PAS specification to JTC1
 - **withdrawn after considerable uproar** in the privacy field (too much focussed on processing data, not enough consideration of avoiding/reducing data by design)

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



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

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



- **2004/06: SC 27 Study Period on Identity Management**
 - Decision at October 2004 SC 27 Head of Delegation meeting, Co-Rapporteurs Phil Griffin, Kai Rannenberg, Christophe Stenuit
 - Final report for **May 2006 SC 27 Plenary**
- **2005: New project ISO/IEC 24760: *A framework for identity management***
- **2005/06: SC 27 Study Period on Privacy**
 - Decision at April 2005 SC 27 Plenary, Rapporteur Kai Rannenberg
 - Final report to **May 2006 SC 27 Plenary**
- **May 2006: SC 27 starts new WG 5 “Identity Management and Privacy Technologies” based on work of the Study Groups.**
 - New Projects on
 - A Privacy Framework (ISO/IEC 29100)
 - A Privacy Reference Architecture (ISO/IEC 29101)



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

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

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)

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

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

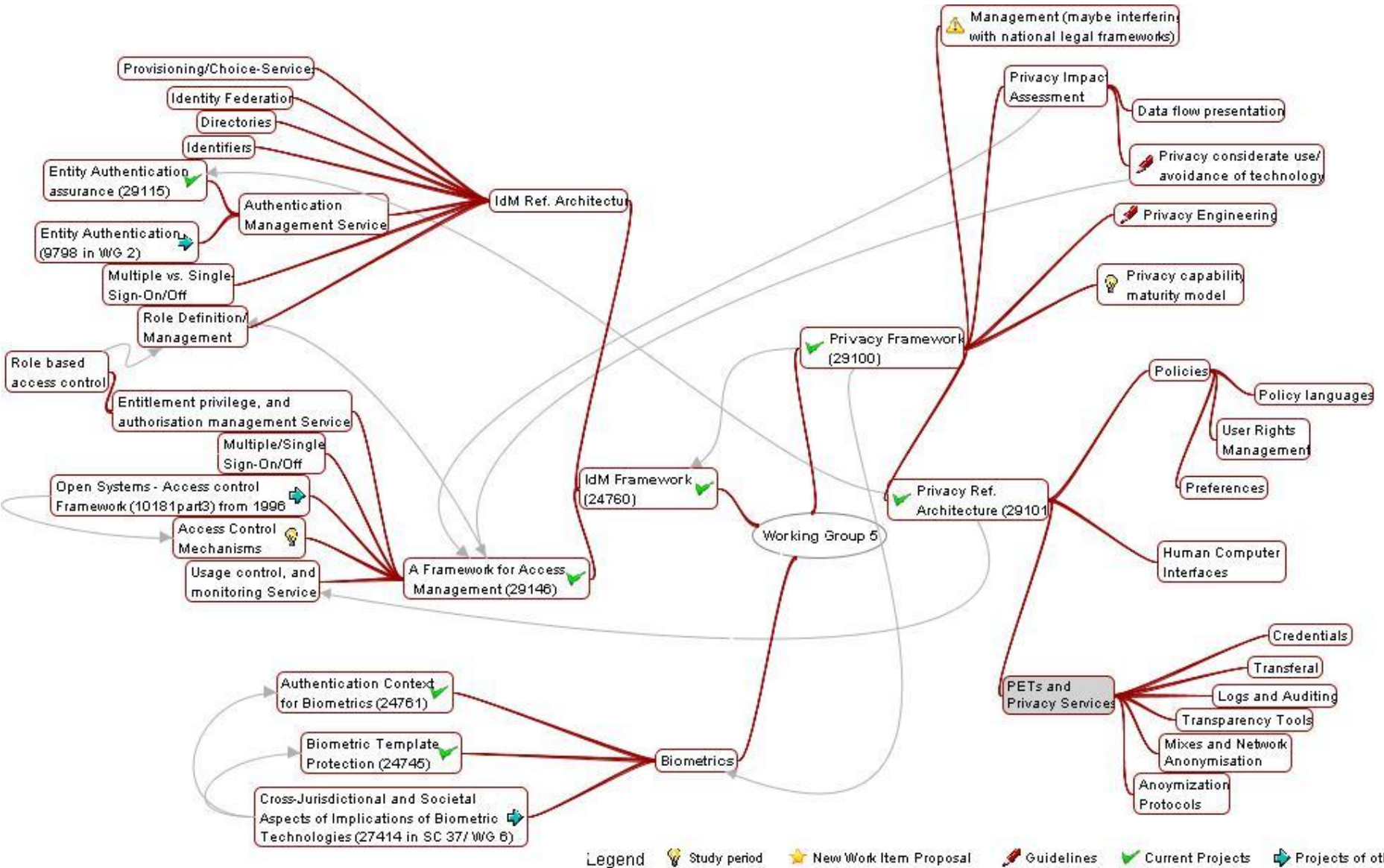
- Biometric information protection (ISO/IEC 24745, FDIS)
- Requirements for partially anonymous, partially unlinkable authentication (ISO/IEC 29191, CD)

Guidance on Context and Assessment

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

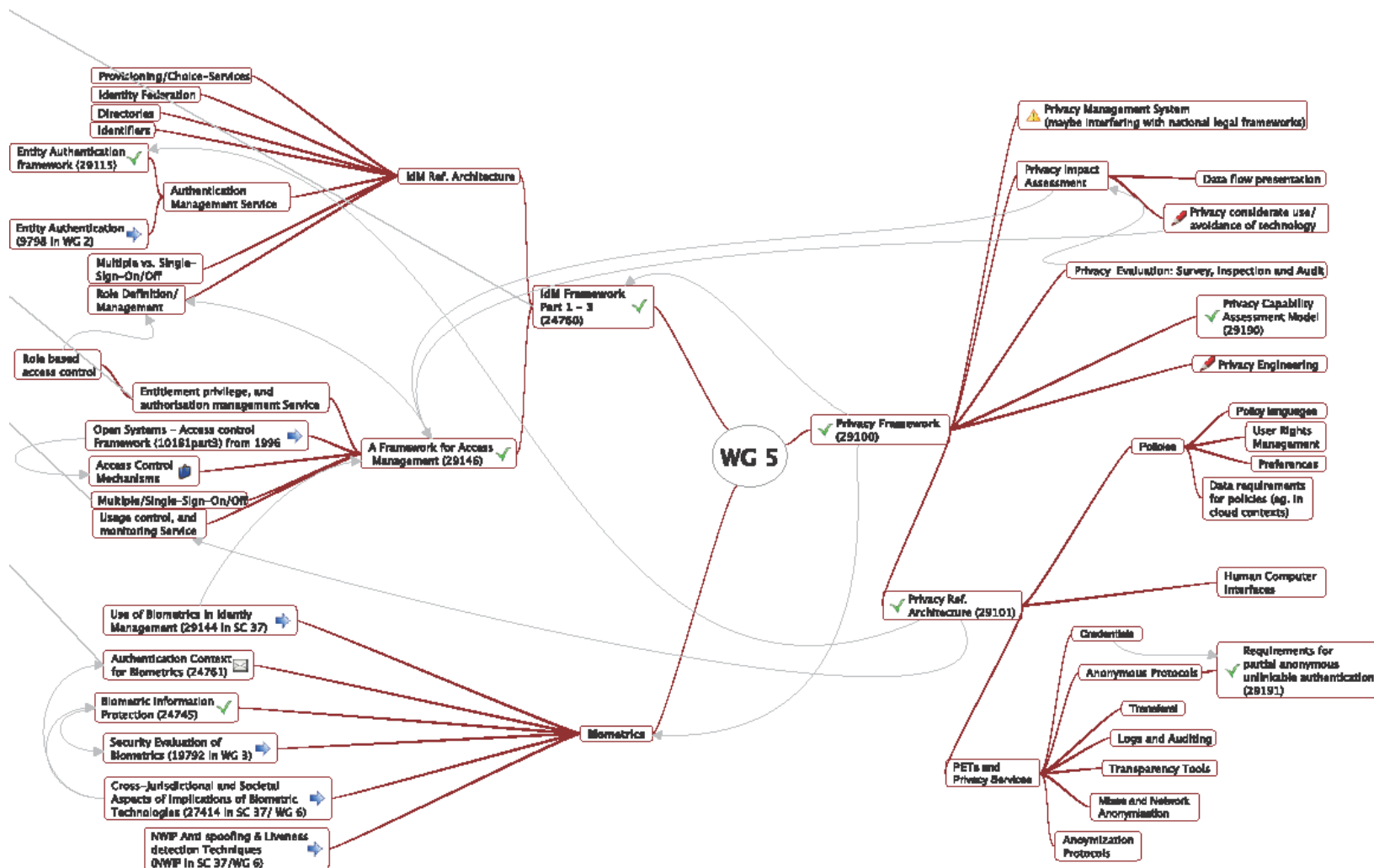
WG 5 Identity Management & Privacy Technologies Roadmap (2008-04)

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



Legend: Study period, New Work Item Proposal, Guidelines, Current Projects, Projects of other WGs

- Summary of previous lecture
- Data Protection and Privacy
 - Origin and definition
 - Law, Technology, Standardisation
- Technical Privacy Protection
 - Privacy Enhancing Technologies (PETs)
 - Deficiencies
- Integrated Privacy Protection
 - Personal Identity Management
 - PRIME
 - Integrated Solution, e.g. for LBS

- 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

- **The Anonymizer**
www.anonymizer.com
- **Mixmaster – Anonymous Remailer**
<http://mixmaster.sourceforge.net>
- **Onion Routing**
www.freehaven.net/tor
- **Java Anonymous Proxy (JAP)**
<http://anon.inf.tu-dresden.de>
- **Tor Network**
<http://tor.eff.org/>

- **Cookie Cooker**

www.cookiecooker.de

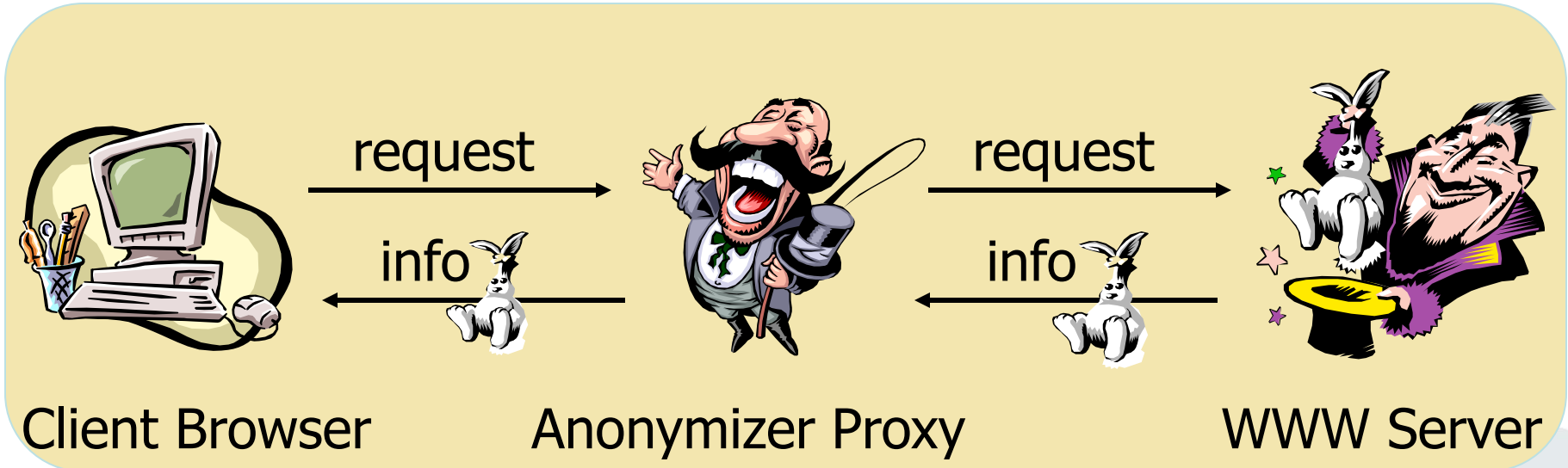
- **P3P - Platform for Privacy Preferences**

www.w3.org/P3P

- **Reachability Management**

- **Idemix**

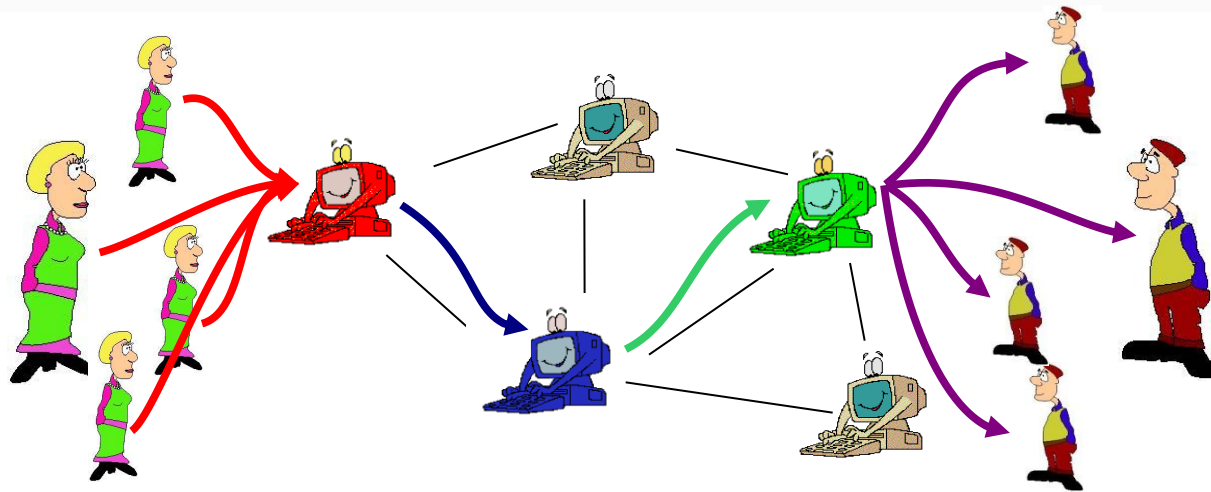
www.zurich.ibm.com/security/idemix



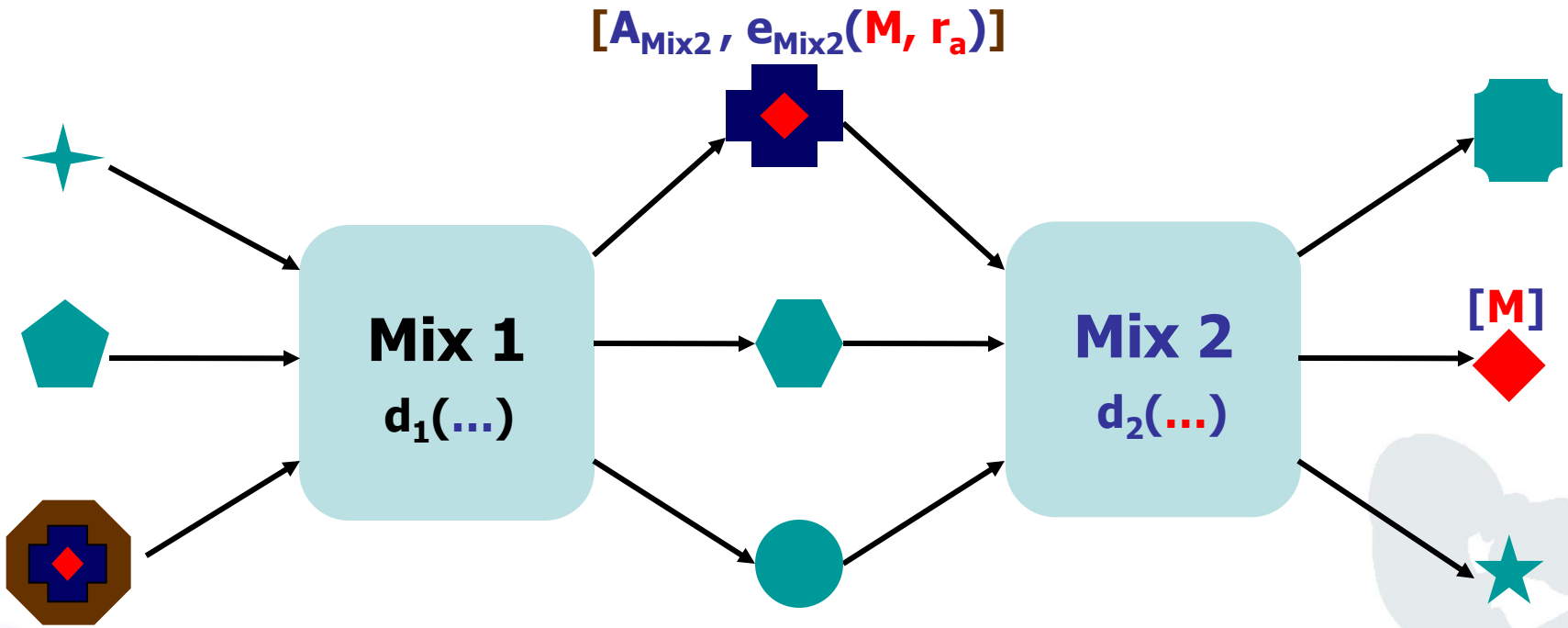
www.anonymizer.com

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

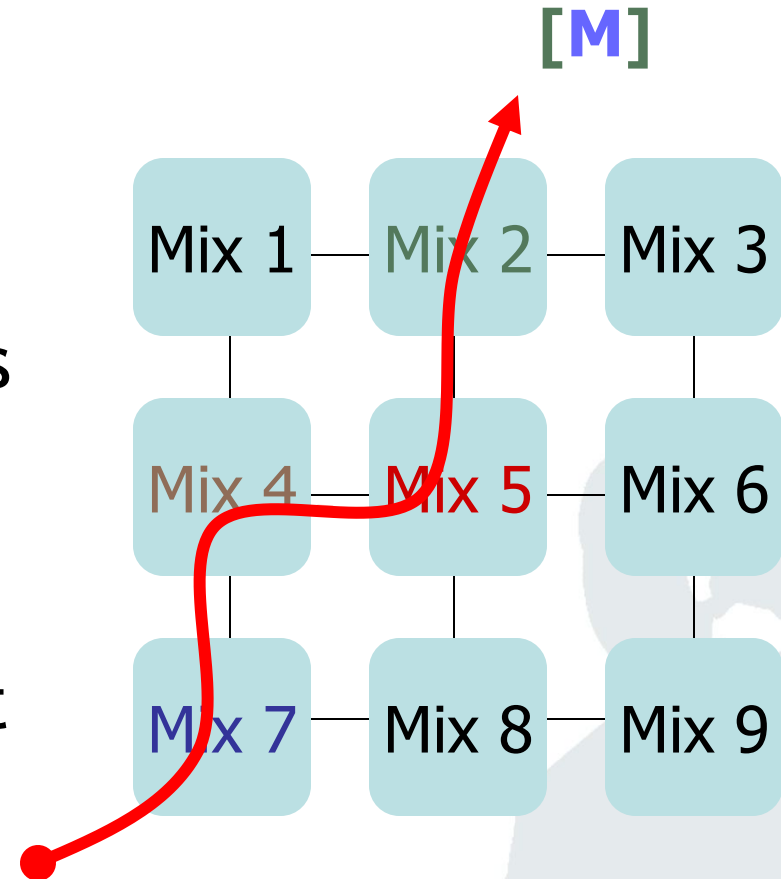


$$[A_{\text{Mix1}}, e_{\text{Mix1}}(A_{\text{Mix2}}, e_{\text{Mix2}}(M, r_a), r_b)]$$

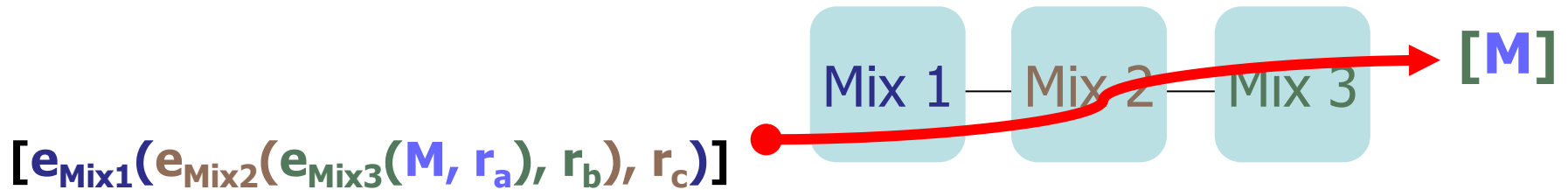
- Decode, buffer, reorder, and resend incoming messages
- Protect **unlinkability** of input / output messages
- Protect **unobservability** of connections and relations
- No single point of trust / failure [Chaum1981]

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

- 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.

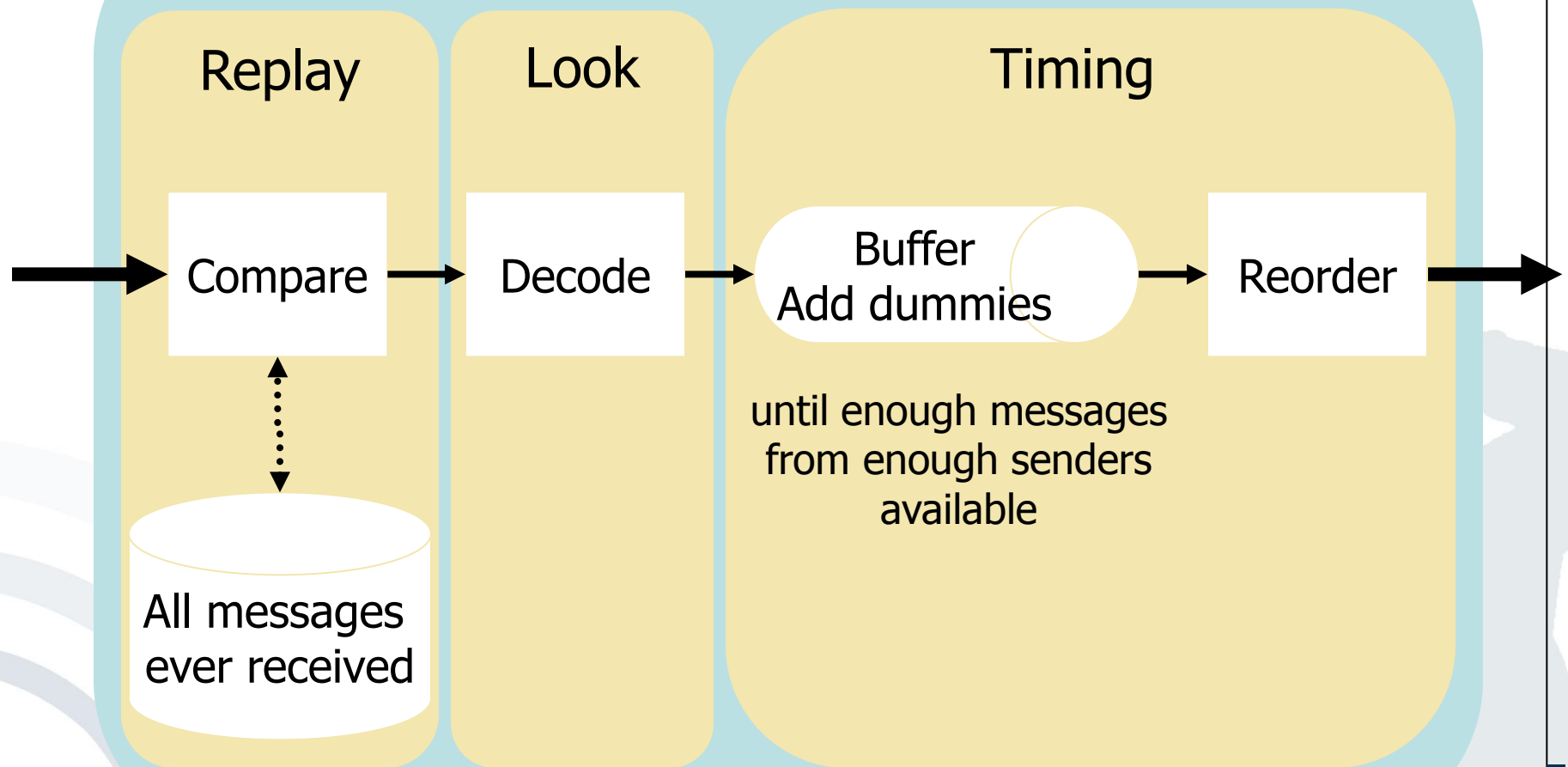


$$[A_{\text{Mix7}}, e_{\text{Mix7}}(A_{\text{Mix4}}, e_{\text{Mix4}}(A_{\text{Mix5}}, e_{\text{Mix5}}(A_{\text{Mix2}}, e_{\text{Mix2}}(M, r_a), r_b), r_c), r_d)]$$



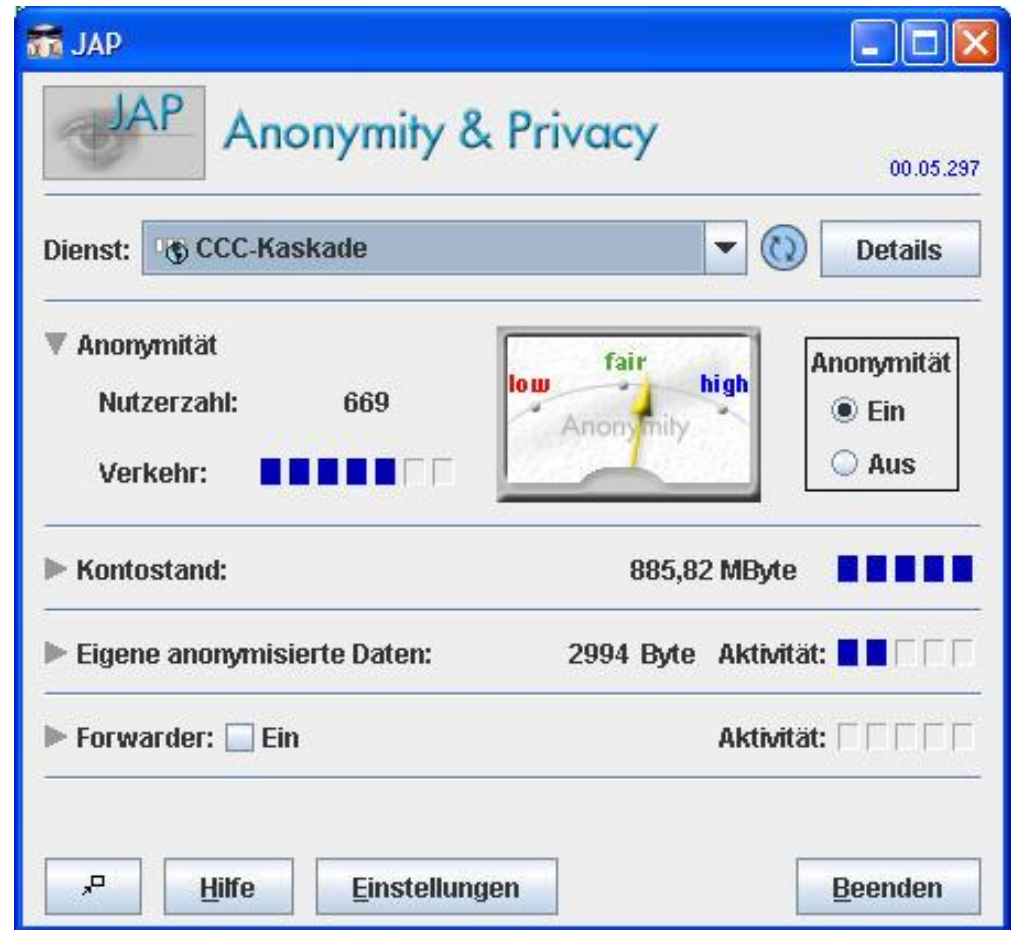
- Fixed Path through the network
- No mix addresses required in messages
- All traffic flows over the same mixes.
- Protection guaranteed as long as one mix withstands attacks

Avoid linkability risks



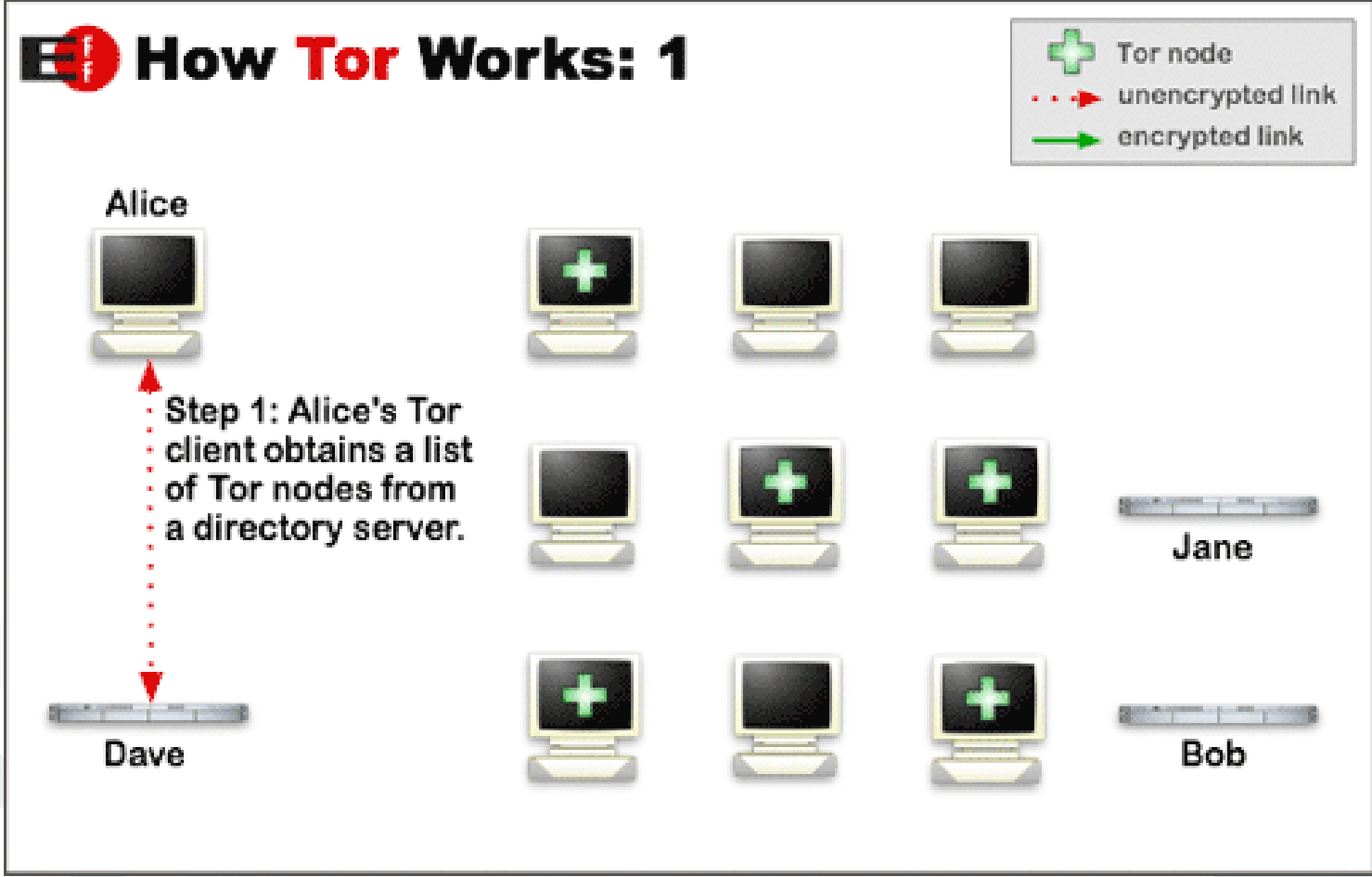
- Users can choose between multiple mix-cascades
- Number of active users is a heuristic for level of anonymity achieved
- Current version does not achieve security against a global attacker but can protect against local attackers
 - your boss
 - your provider
 - operator of a mix

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



- Tor 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?

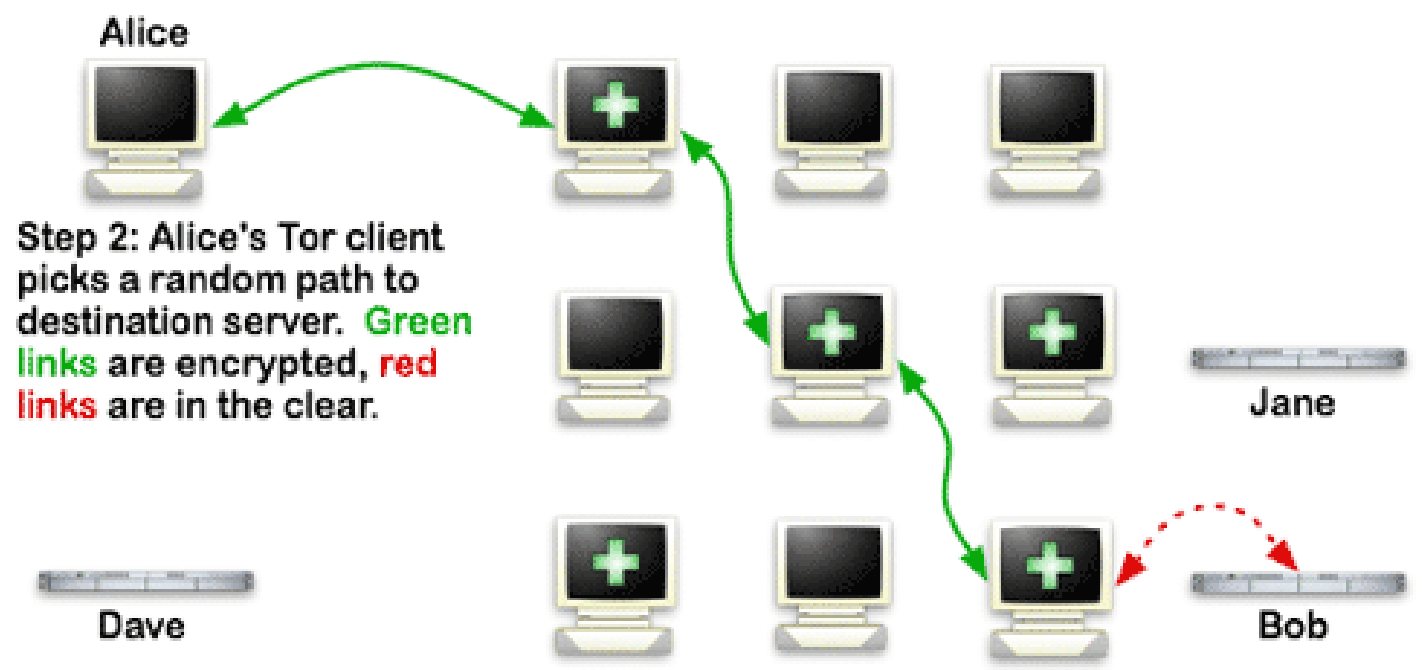
[Europe2006]

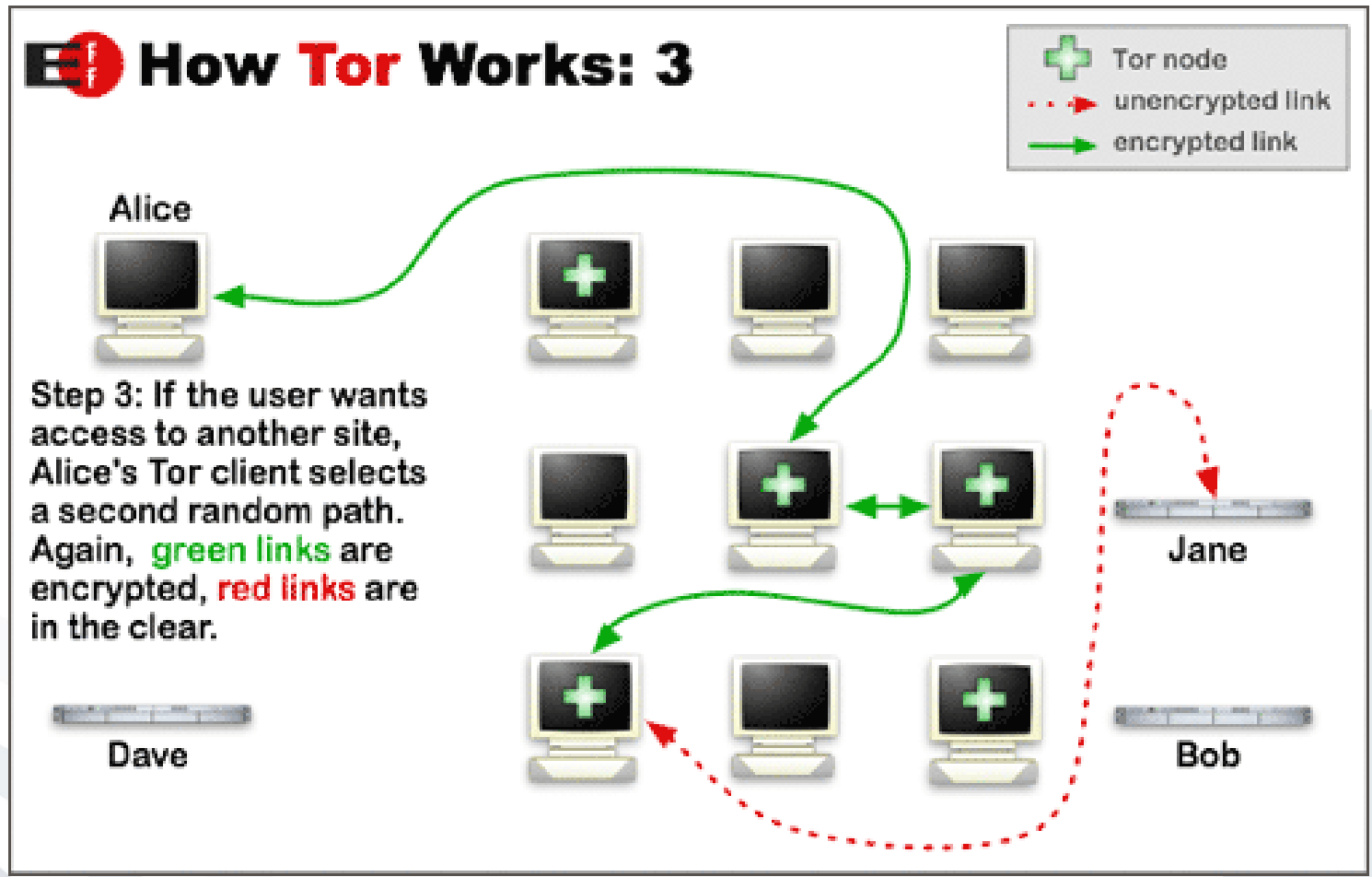


EFF How Tor Works: 2

Legend:

-  Tor node
-  unencrypted link
-  encrypted link





- 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



- 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 enhances 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.

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

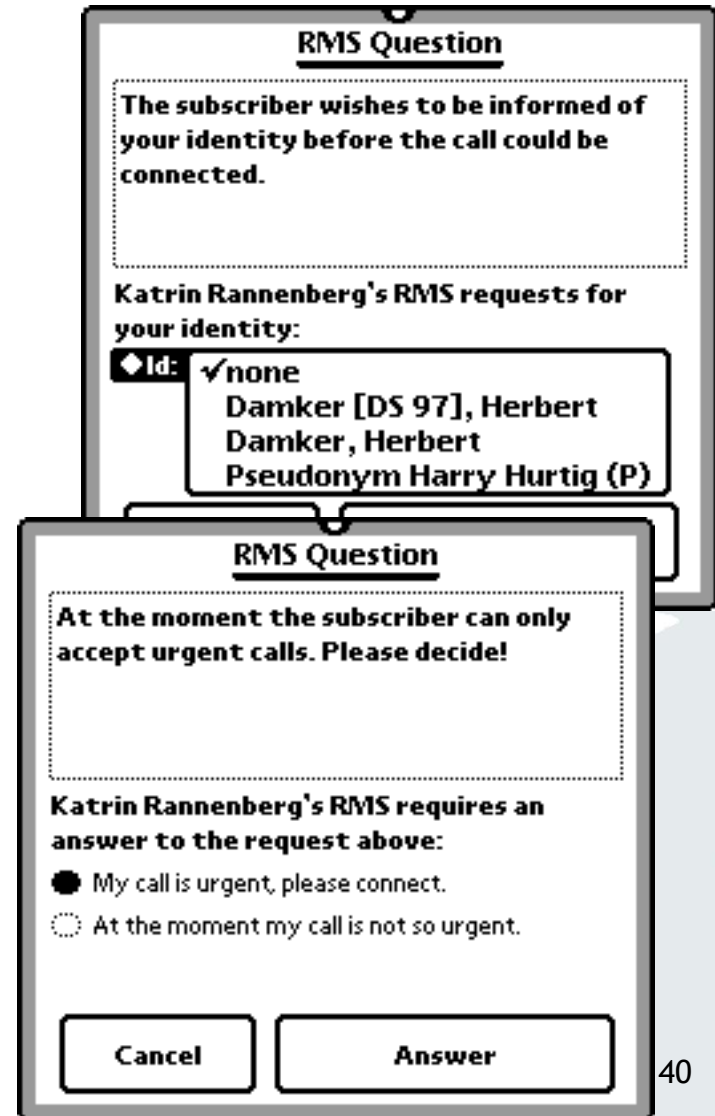
“I welcome you calling back.”

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:

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

RMS Question

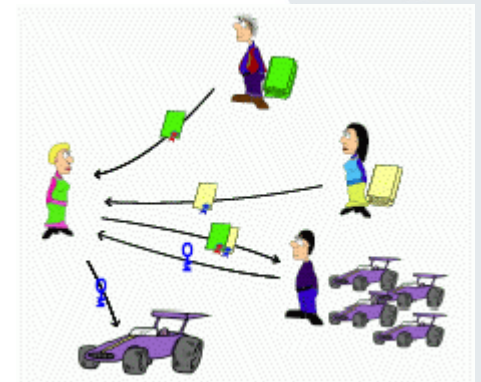
At the moment the subscriber can only accept urgent calls. Please decide!

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

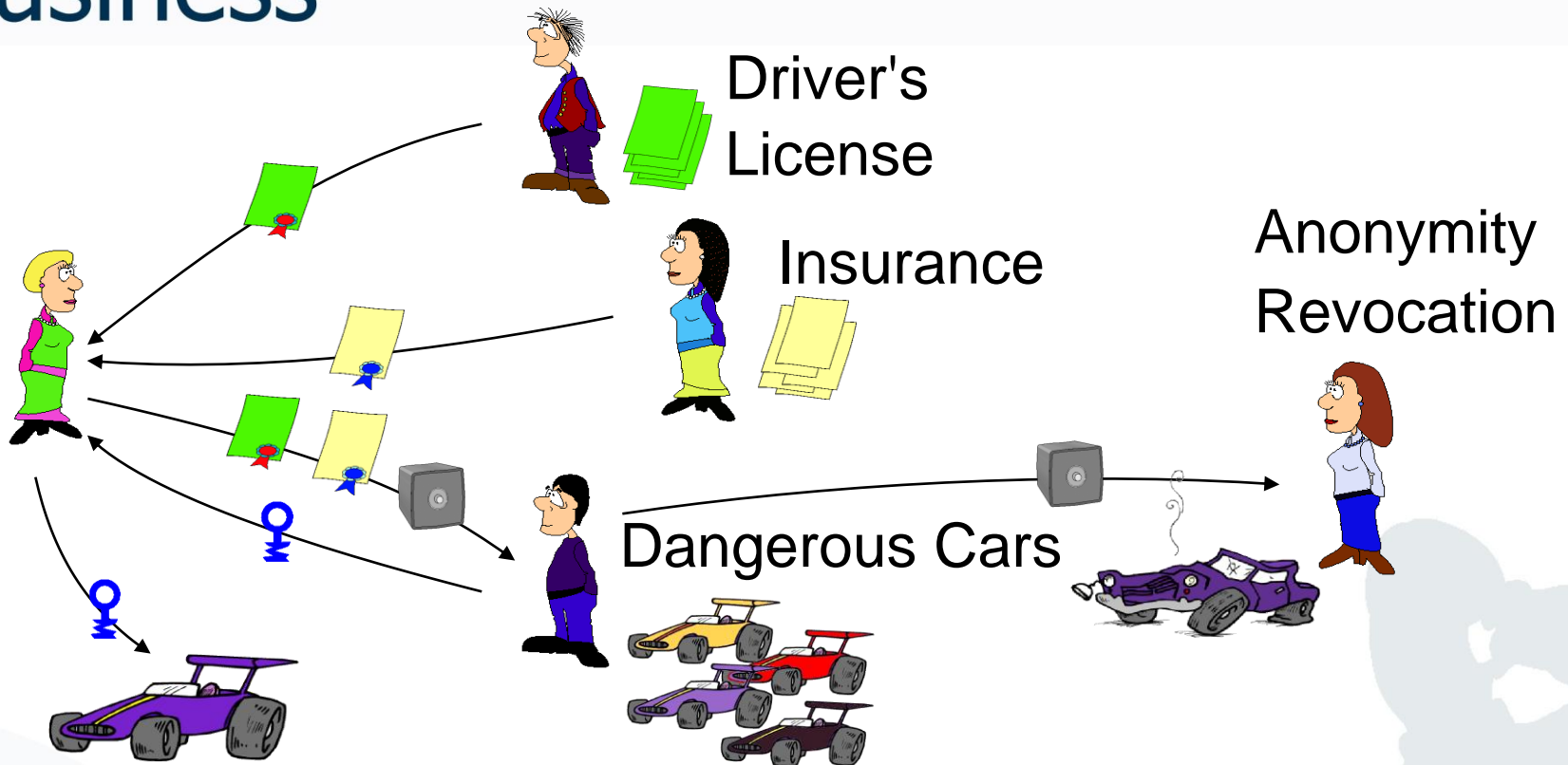
My call is urgent, please connect.
 At the moment my call is not so urgent.

Cancel Answer

- Anonymous Credentials are used to prove privileges or attributes of their owner without revealing its identity, e.g. to prove, that
 - a device contains an unrevoked Trusted Platform Module (TPM); this is also called Direct Anonymous Attestation
 - the owner possesses a subscription and is of the required age, e.g. for an identity management system supporting anonymous video download
- Such a system needs to have the following properties:
 - Unforgeability of credentials
 - Unlinkability of credentials
 - No credential sharing
 - Consistency of credentials



Idemix: Car Example



- What happens if a user exchanges information with multiple parties?
- The user has different pseudonyms with different parties.
- The user uses credentials to prove that he has a driver's license and an insurance.

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

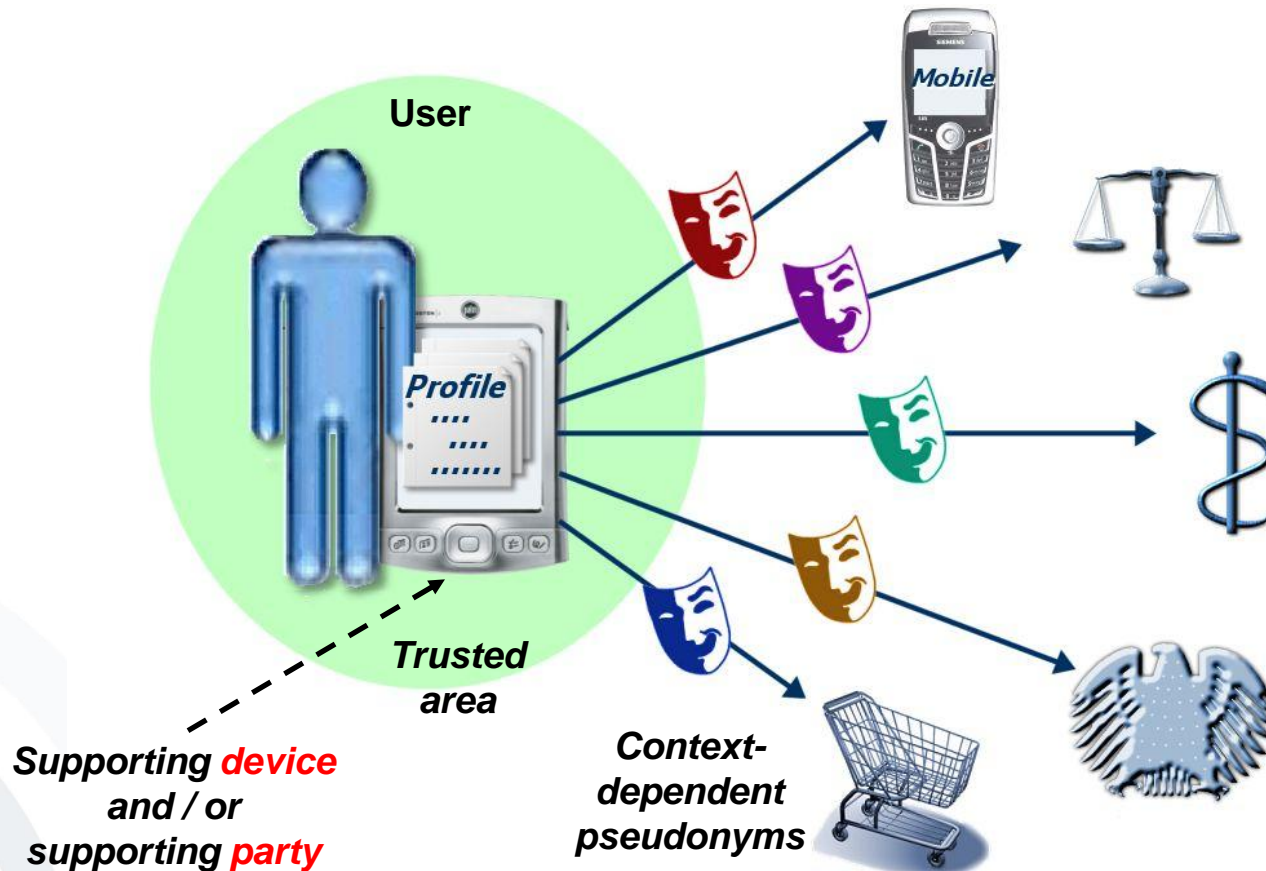
- To provide a reference between
 - the several features and technologies
 - their relations in information and communication systems
- To position privacy-related standards to be developed
- To form a basis from which standardisation work items relevant to privacy can be defined, proposed, voted upon, and developed.
- To cover the various stages in data life cycle management and the required privacy functionalities for PI data in each data life cycle, as well as positioning the roles and responsibilities of all involved parties.
- Relevant input from e.g.
 - 11 principles addressed by the "Montreux Declaration", published by the International Conference of Data Protection and Privacy Commissioners
 - Relevant EC Directives
 - the architecture documents of the project PRIME
 - Further considerations on architecture elements
 - ...
- Begin of work May 2006
- Editor: Stefan Weiss

- One type of architecture elements to cover **privacy functionalities**, such as
 - Private (unobservable, anonymous) and secure communication;
 - Credentials (to gain credibility);
 - Negotiation protocols to transfer information if needed
 - Data objects to describe data handling policies
- 2nd type of architecture elements to cover the **stages in data handling and data lifecycle management** such as
 - Collection/delivery
 - Storage
 - Processing
 - Transfer
 - Destruction of several kinds of data
- 3rd type of architecture elements to cover the **roles of persons and institutions** being involved with the data, e.g.
 - Persons, whose data are being collected and processed, e.g. consumers
 - Entities processing the data
 - Interested parties to whom data may or may not be forwarded

- Summary of previous lecture
- Data protection and Privacy
 - Origin and definition
 - Law, Technology, Standardisation
- Technical Privacy Protection
 - Privacy Enhancing Technologies (PETs)
 - Deficiencies
- Integrated Privacy Protection
 - Personal Identity Management
 - PRIME
 - Integrated Solution, e.g. for LBS

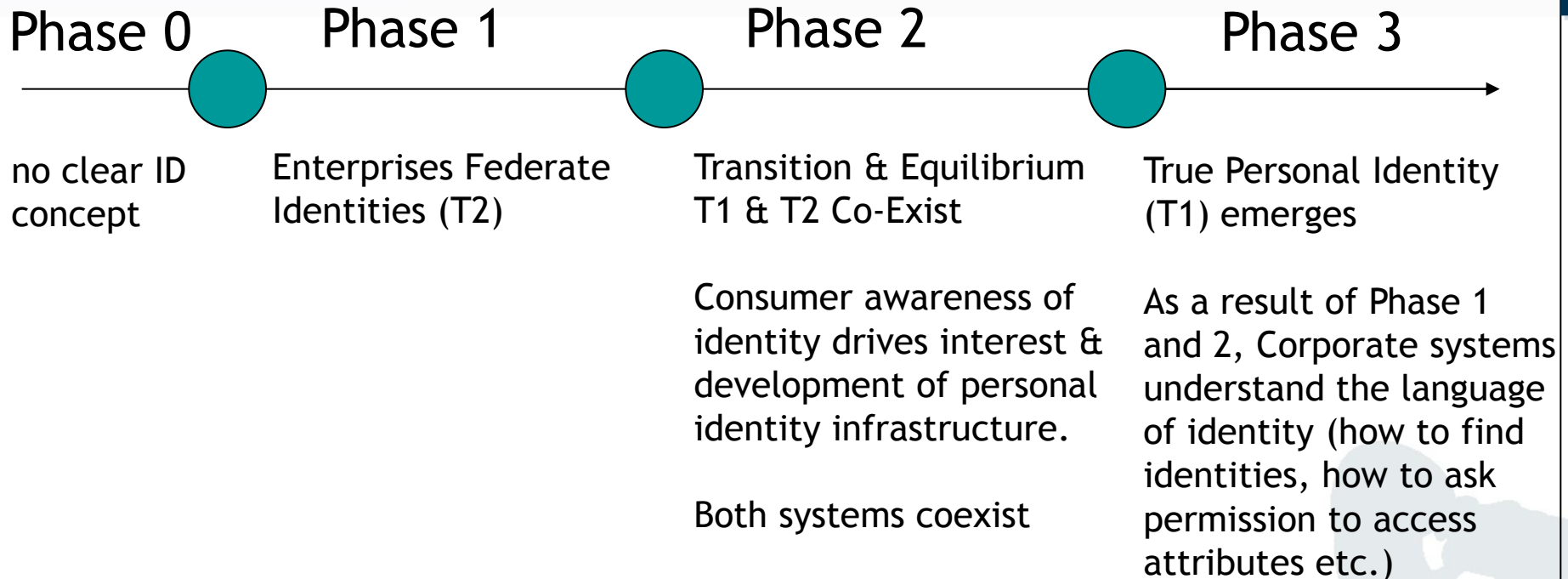
“Management of own identities”

- User controls both identification and his representation („**idem**“) as well as his virtual/online self-designation („**ipse**“)



- Attempt to integrate existing PET systems
 - Uses mix like concepts for anonymisation
 - Based on Idemix for Anonymous Credentials
 - Based on DRIM for Client Side Identity Management Interface
 - Builds on P3P experiences for policy management
- Develops new IdM technology
 - Obligations
 - Attribute based access control
 - Use of semantic web and ontology technology for negotiation
- Considers different application scenarios
- While PRIME is a very ambitious project, Personal Identity Management may arrive in stages.

Phases of IdM deployment



Tier 1: True (,My') Identity - A T1 identity is my true and personal digital identity and is owned and controlled entirely by me, for my sole benefit. T1 identities are both timeless & unconditional.

Tier 2: Assigned (,Our') Identity - A T2 (assigned) identity refers to our digital identities that are assigned to us by corporations (e.g. our 'customer accounts').

- our title (assigned to us by our employer),
- our cell phone number (assigned to us by our mobile phone operator),
- our United Mileage Plus number (assigned to us by United Airlines),
- our social security number (assigned to us by the Government),
- our credit card number (assigned to us by our credit card companies)

- Often applications require “hand crafted” privacy solutions, e.g.
 - Location Based Services (LBS)
 - Airport identification Systems
 - Hospital and medical lab IT systems,due to special requirements such as privacy or security.
- Such solutions can be
 - implemented as stand alone systems
 - integrated into general privacy management frameworks, e.g. PRIME

- *Location based services* (LBS) can pose a privacy risk by collecting and using data against a user's intention.
- Most LBS are provided by mobile communications providers that measures a user's whereabouts by localizing his mobile device.
- Can LBS be developed in a privacy-respecting way, and still be profitable applications on the commercial market of online-services?
- How does a privacy-respecting architecture look like?

- Enable established business models on a secure, privacy-friendly architecture
- Ensure efficiency & economy of the solution
- Enable users to manage policies & their ‘online’ identities for each service provider and for each usage cycle
- No processing of localizations violates a user’s consent
- Hide service usage patterns from observers & infrastructure providers
- Protect confidentiality of communication content against observers & infrastructure

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**
 - Version 1 simple WAP mobile phone
 - Version 2 Java phone
- **Considering B2B scenarios in the value chain**



The issues in a bit more detail

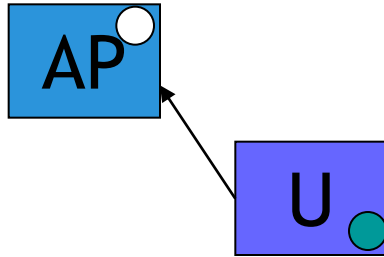
- **Location-based services are a promising business**
 - **Market penetration of GPS phones still limited**
 - **Mobile operator may step in based on Cell ID information**
- **Several challenges**
 - **Privacy problems**
 - **Regulation, e.g. of the handling of personal information (and mobile services in general)**
 - **Business constraints**
 - **Easy integration into existing infrastructure**
 - **Applicability to a wide range of business models**
 - **Adaptability for different market structures**



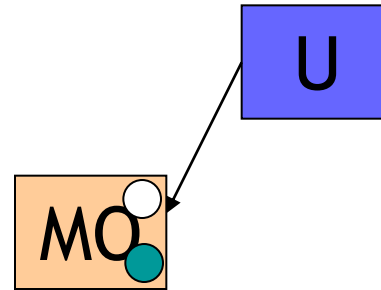
- AP** Location-Based Service Application Provider, a special type of value adding service provider in mobile networks
- U** User, usually a person, but could also be a business entity, or even a vehicle or container
- LI** Location Intermediary, a Party with the business of mediating between LBS provider and operators, it can also perform privacy functionality.
- MO** Operator of a mobile network, that uses it's infrastructure to localize users.

LBS Background Information

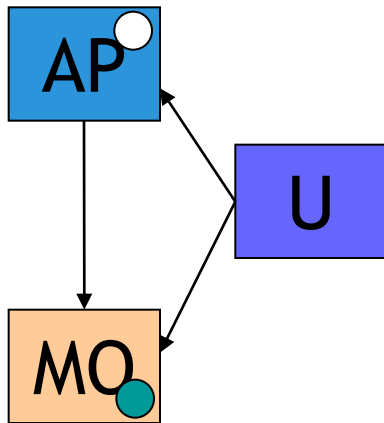
Four Different Business Models



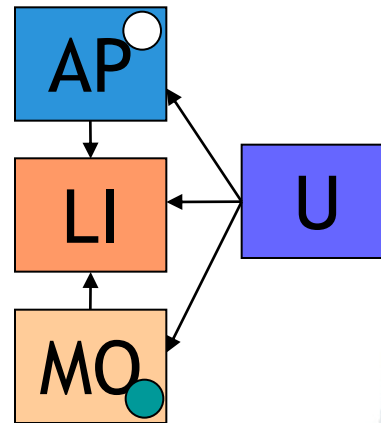
1. Direct localization scenario



2. Operator-portal scenario



3. Application provider scenario

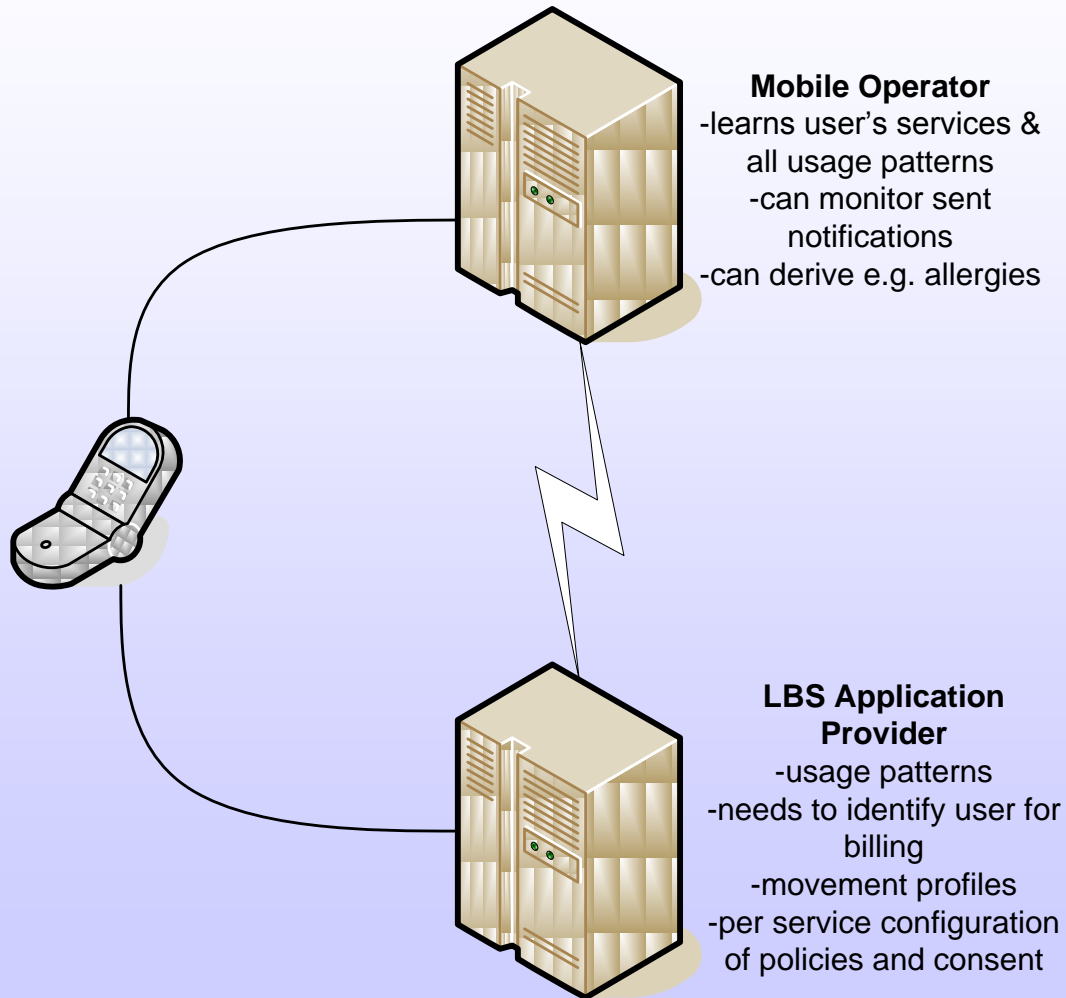


4. Intermediary scenario

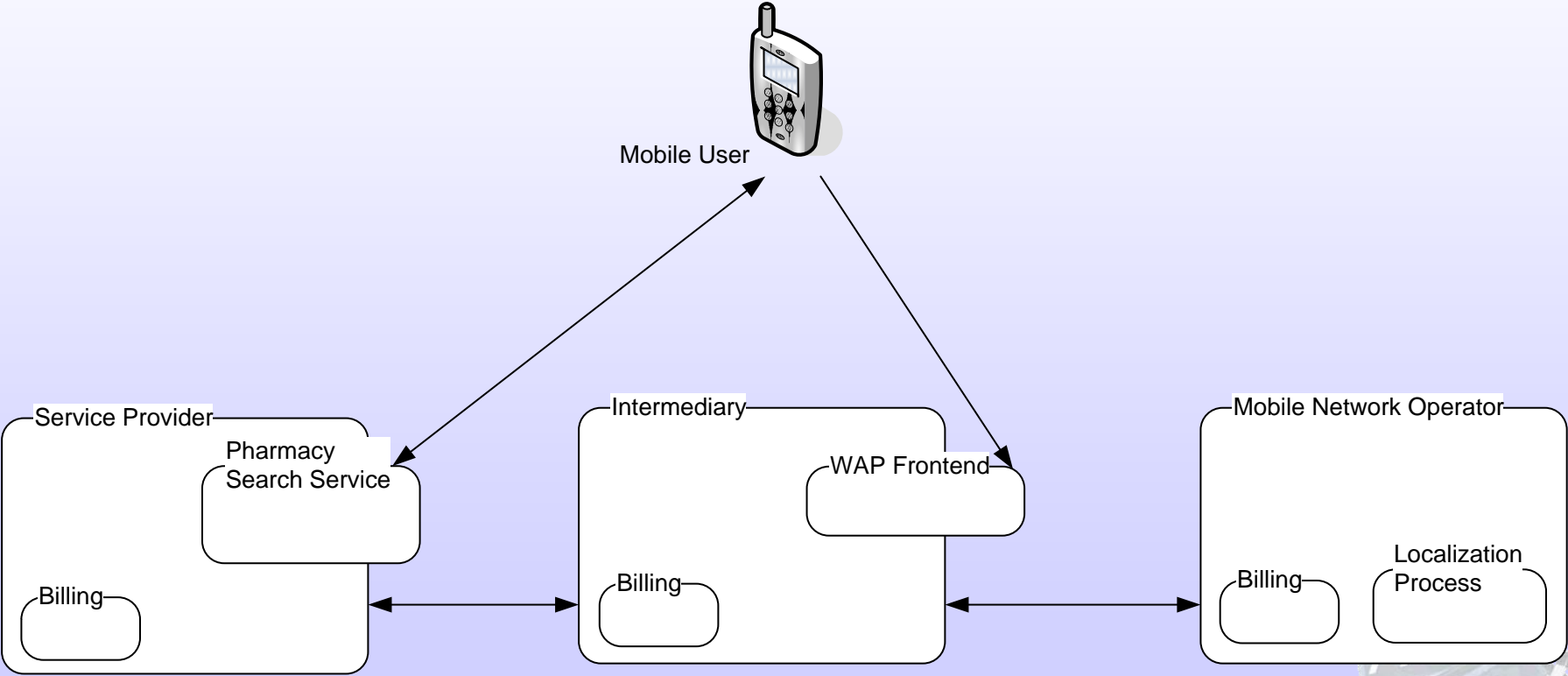
○ Service

● Location Source

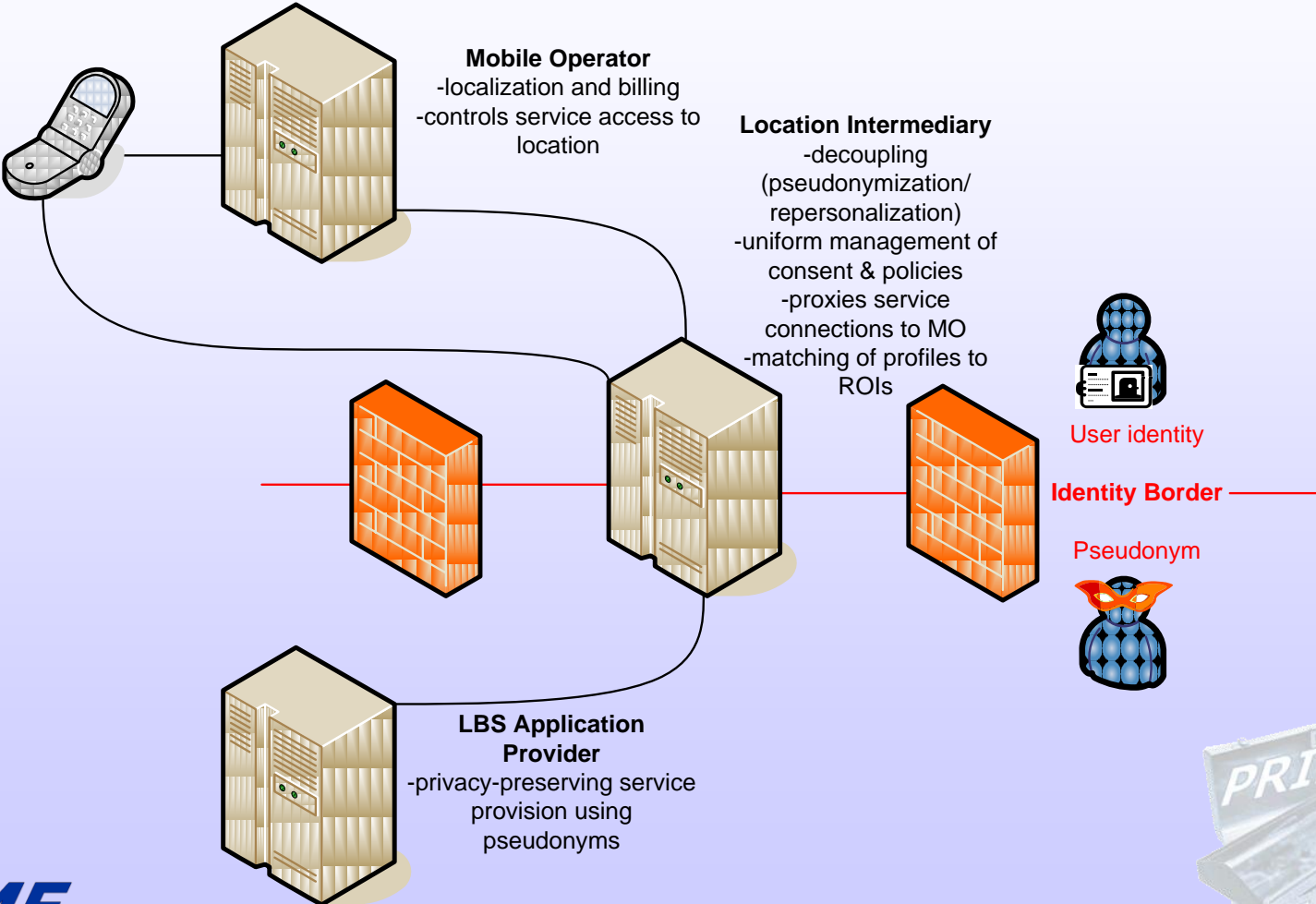
Conventional LBS Deployment



Solution Approach Intermediary

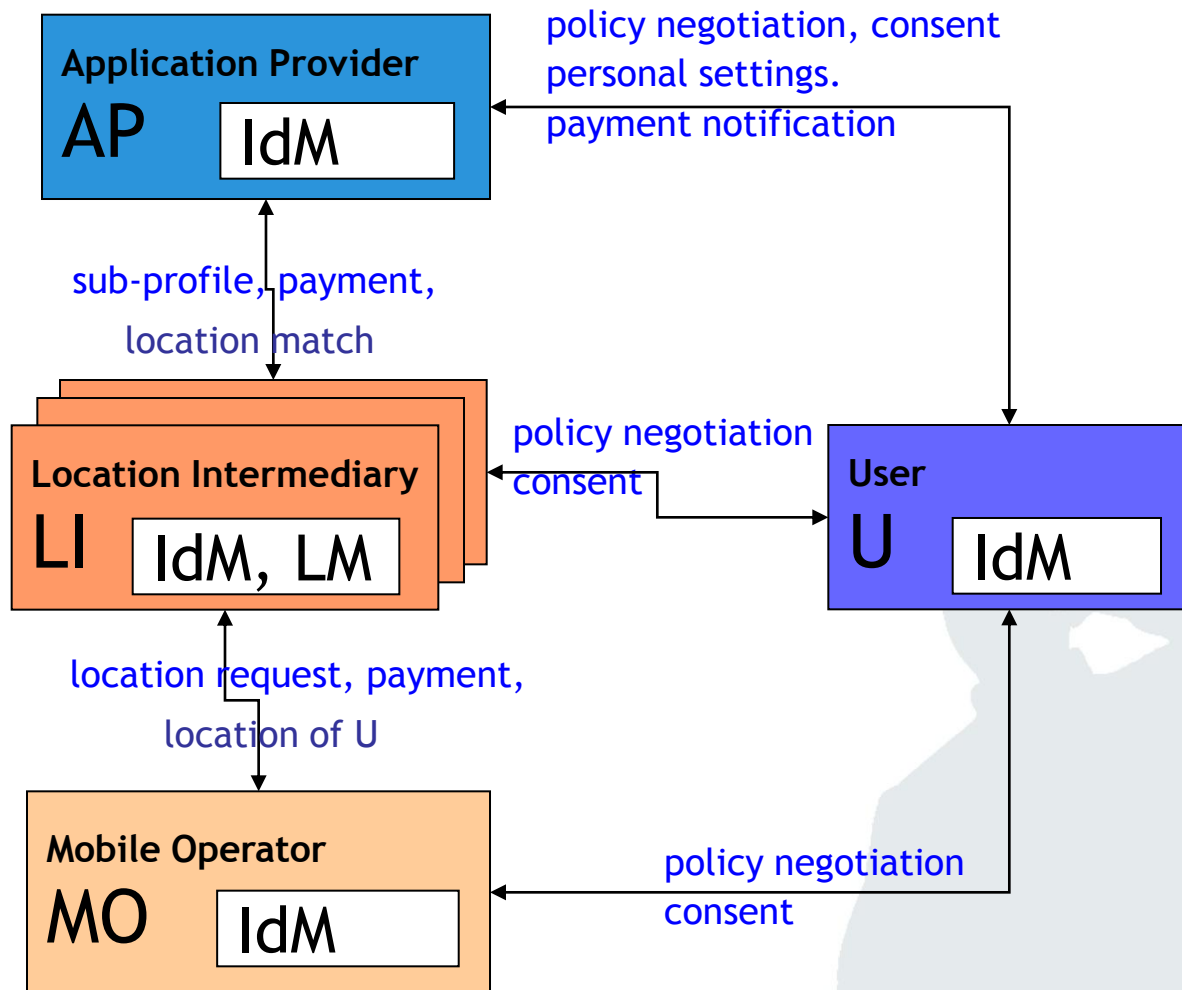


Intermediary Approach Architecture Overview



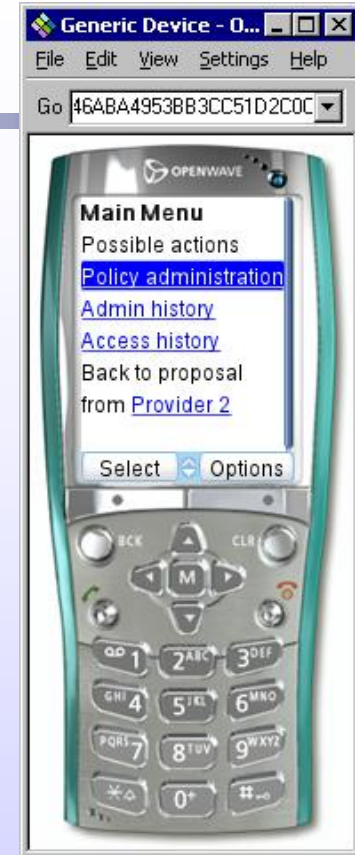
Intermediary Functions

- Identity management (IdM)
 - Providing users with unlinkable pseudonyms for different business partners
- Location matching (LM)
 - Providing AP with location info only when needed, e.g. for a push services



PRIME LBS Application Prototype Summary

- **Evaluation of prototype assures**
 - **Legal compliance**
 - **Economic benefits**
 - **Technical feasibility**
- **First transfers into the real world**
 - **„Privacy Gateway“ infrastructure component deployed at T-Mobile Germany**
 - **Allows subscribers to set**
 - **Which application provider gets data?**
 - **On which days and times?**



- [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/d90753334a813794b15cc66003046de0,0976e07365617263685f646973706c6179436f6e7461696e6572092d0933353031/8o.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](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%20J%2013-04-06.pdf
- [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
- [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; www.lawrence.edu/fac/boardmaw/Privacy_brand_warr2.html