Security, Privacy and Trust in Emerging Technologies
Project Seminar Kick-off

2015-10-20, Frankfurt, Germany

Dr. Jetzabel Serna-Olvera and MSc. Welderufael Tesfay
project.seminar@m-chair.de
Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt

Agenda

- Data Protection and Privacy
- Origin and definition
  - Law, Technology, Standardization
- Technical Privacy Protection
  - Privacy Enhancing Technologies (PETs)
  - Privacy by Design (PbD)
- Integrated Privacy Protection
  - ABC4Trust
  - Privacy Risk Communication and Mitigation
  - Privacy by Default

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

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

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

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]

eIDAS Regulation

- REGULATION on electronic identification and trust services for electronic transactions in the internet market.

- **Objective:**
  - Boosting TRUST and CONVENIENCE in secure and seamless cross-border electronic transactions by promoting the widespread use and uptake of electronic identification and trust services (eIDAS services).
  - Public administration, businesses and citizens will regularly use eIDAS services;
  - Users will demand more and innovative eIDAS services and new services/apps will emerge on the market;
  - eIDAS will be turned into a source of growth and jobs, supporting both the internal and global markets;
  - eIDAS regulatory framework, standards and technologies will influence international dialogues and trade negotiations, thus broadening the economies of scale for eIDAS services and increasing the global competitiveness of European businesses and private sector.

[Electronic identification and trust services (eIDAS): regulatory environment and beyond, ec.europa.eu]

Agenda

- Data Protection and Privacy
- Origin and definition
  - Law, Technology, Standardization
- Technical Privacy Protection
  - Privacy Enhancing Technologies (PETs)
  - Privacy by Design (PbD)
- Integrated Privacy Protection
  - ABC4Trust
  - Privacy Risk Communication and Mitigation
  - Privacy by Default

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
- P3P – Platform for Privacy Preferences

  www.w3.org/P3P

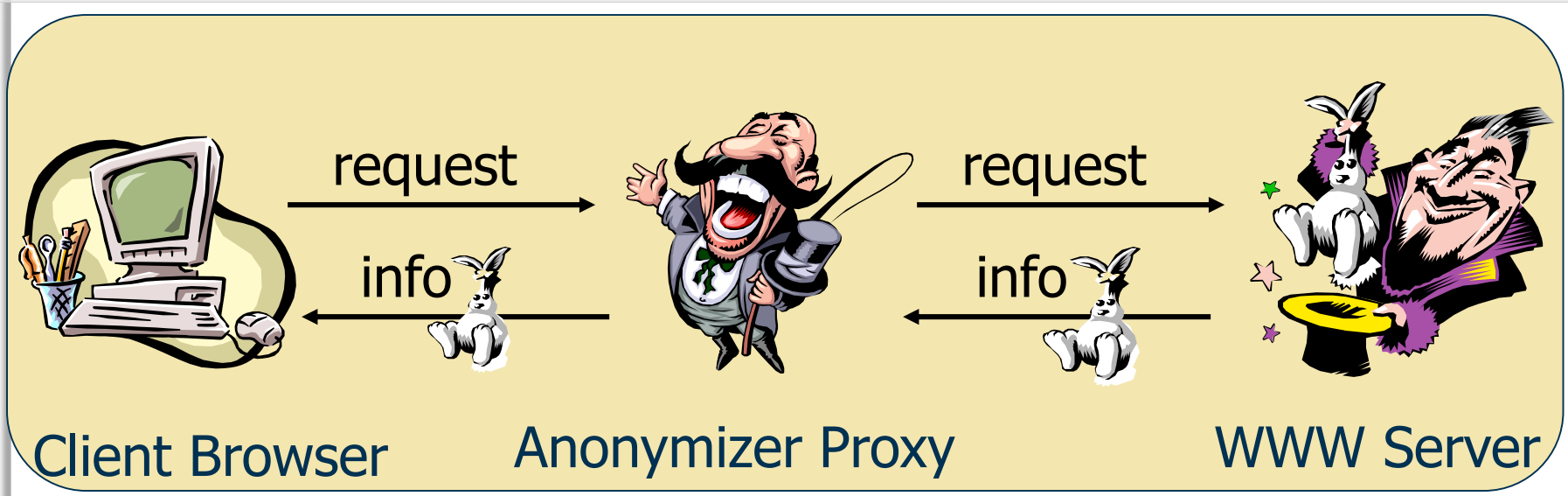
Privacy-preserving Transaction Systems

- Reachability Management
- Credential technologies
  - U-Prove

    www.microsoft.com/uprove
  - Idemix

    www.zurich.ibm.com/security/idemix

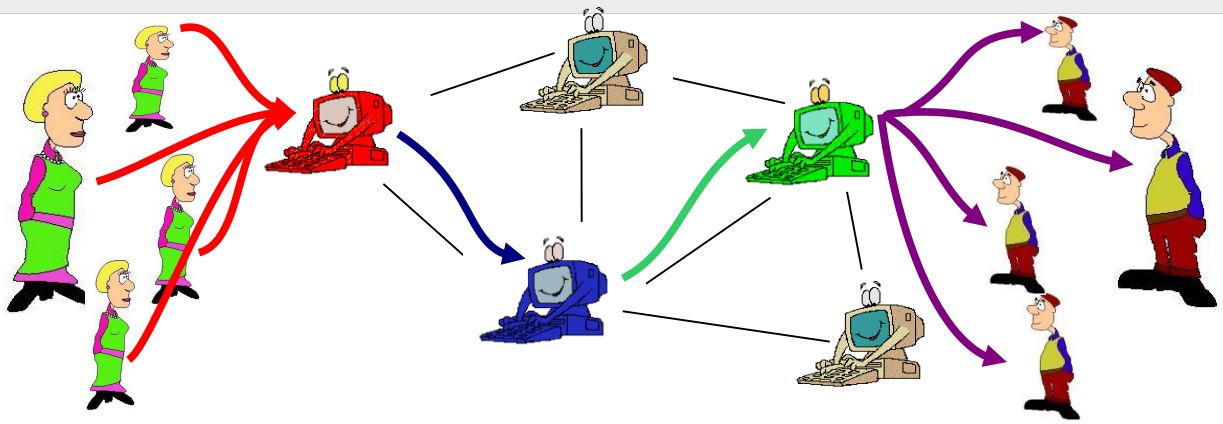
www.anonymizer.com



www.anonymizer.com

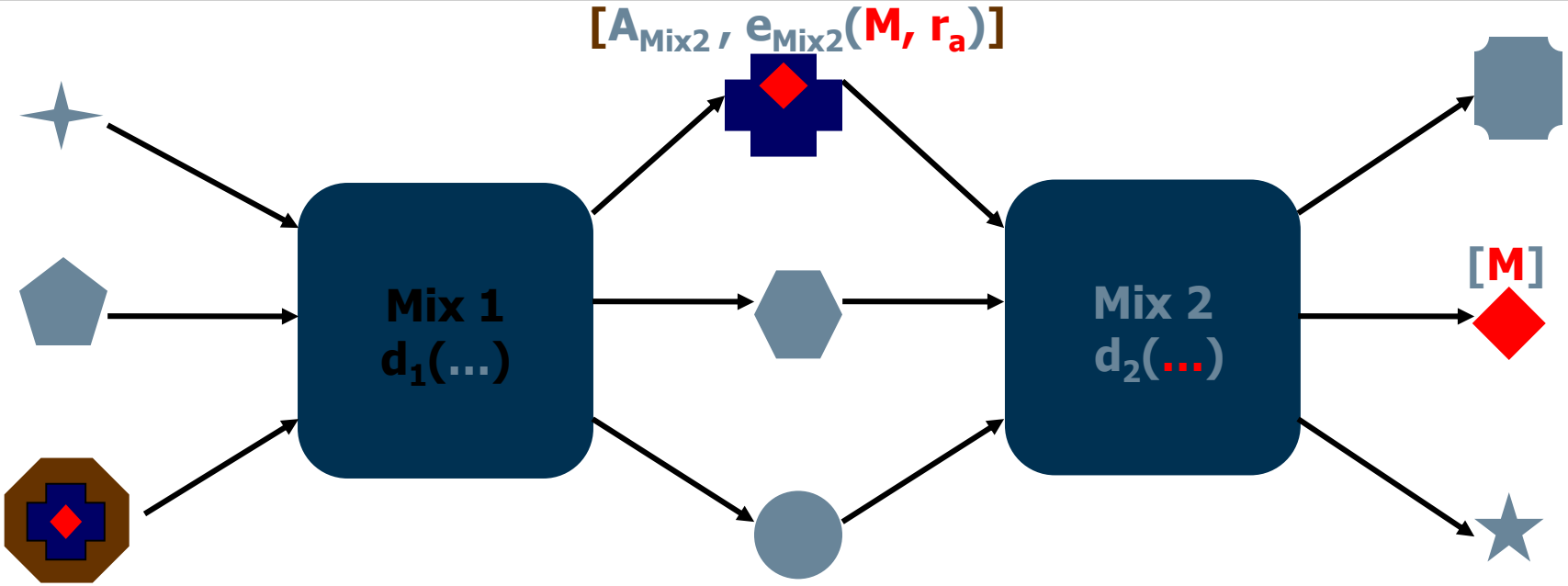
- ↑ Client (anonymity) is protected in an "**anonymity set**" of all possible proxy clients.
- ↓ Anonymizer learns about client's activities / interests.
- ↓ No protection against attackers with global view.

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.*

Mixes

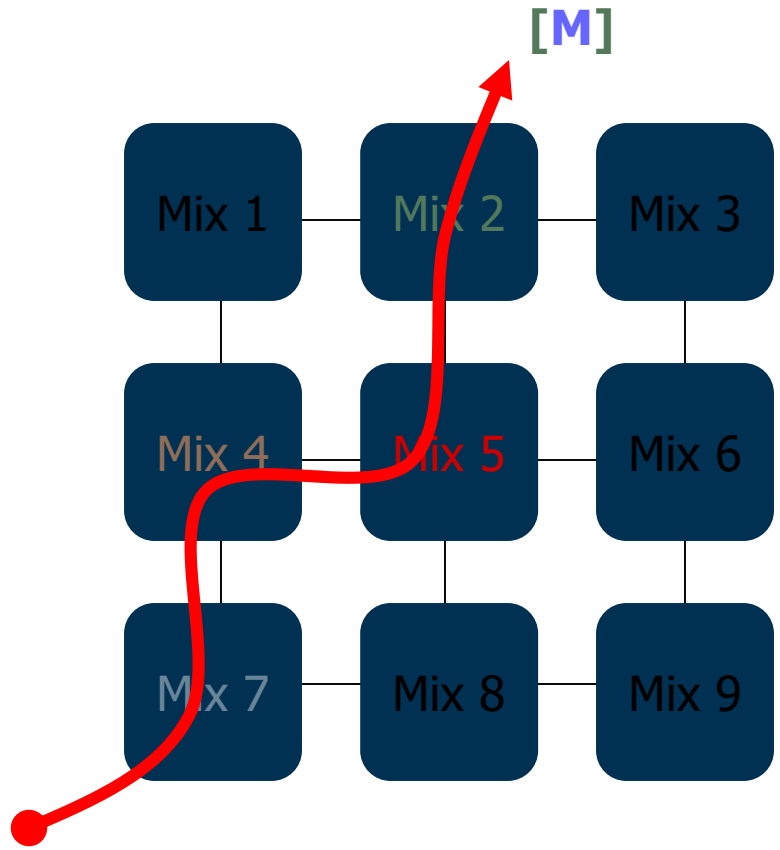


- Decode, buffer, reorder, and resend incoming messages
- Protect **unlinkability** of input / output messages
- Protect **unobservability** of connections and relations
- No single point of trust / failure [Chaum1981]

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

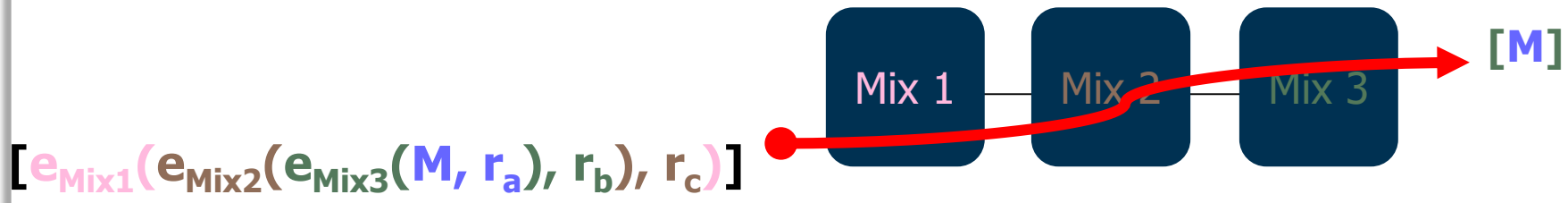
Mix Network

- 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

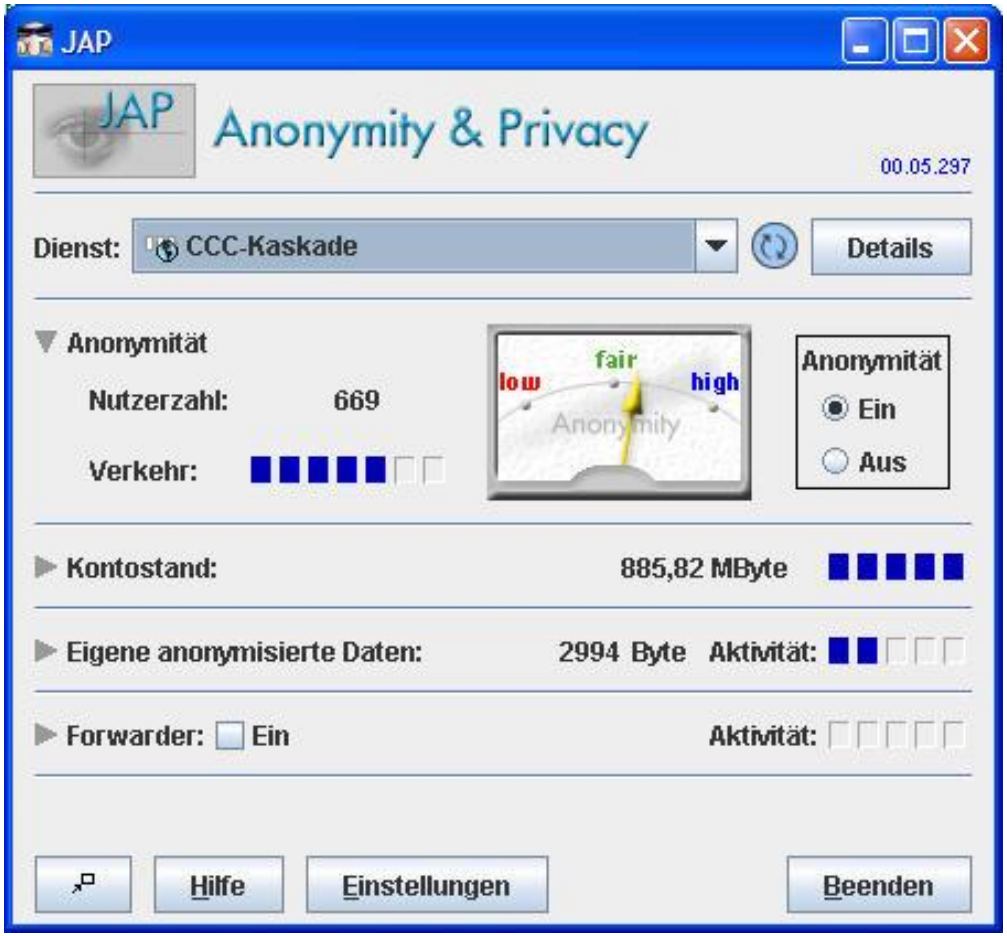


- Fixed Path through the network
- No mix addresses required in messages
- All traffic flows over the same mixes.
- Protection guaranteed as long as one mix withstands attacks

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

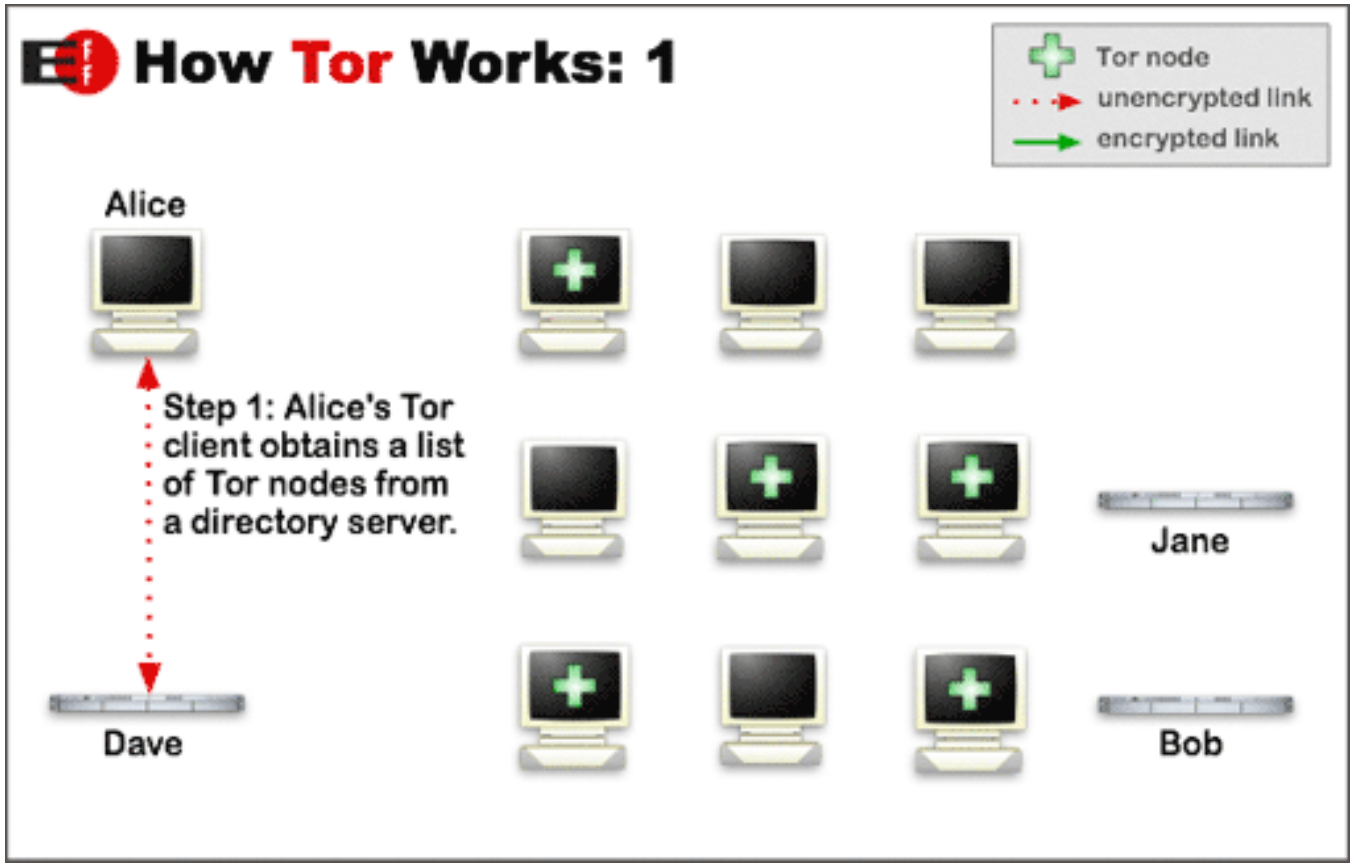


Tor Network

- 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

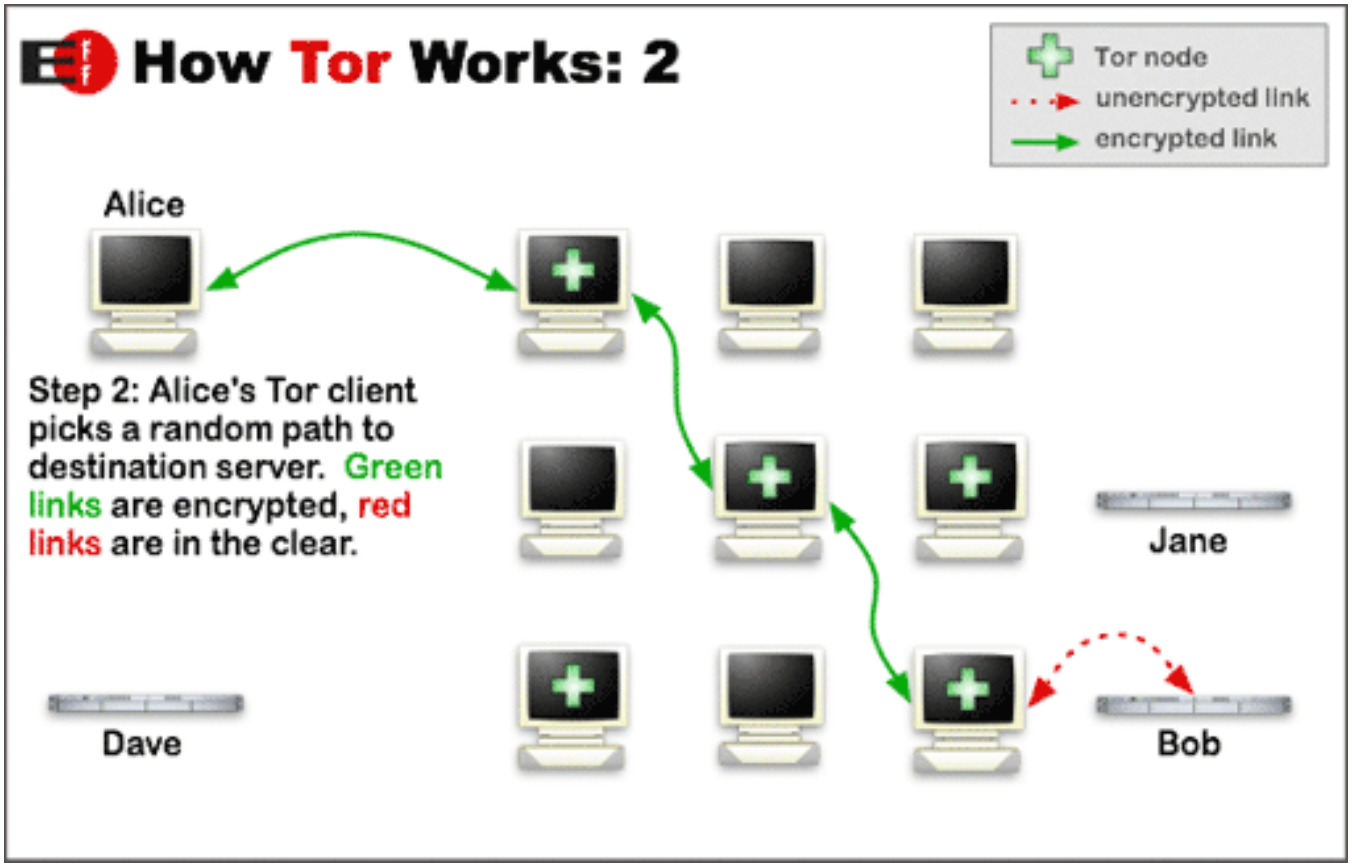
[Europe2006]

How Tor Works I



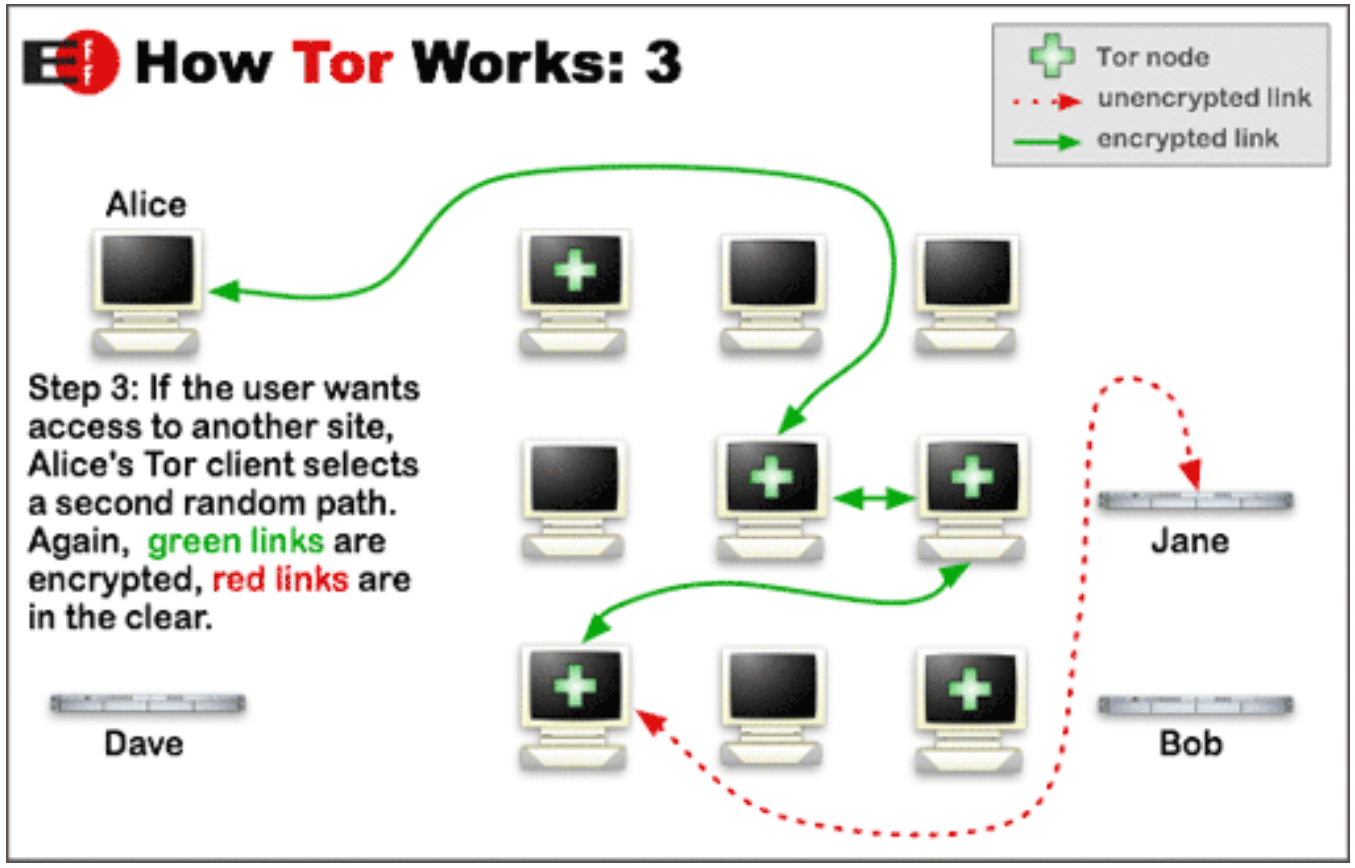
http://tor.eff.org

How Tor Works II



http://tor.eff.org

How Tor Works III



http://tor.eff.org

Attacks on Tor

Evil Exit Node

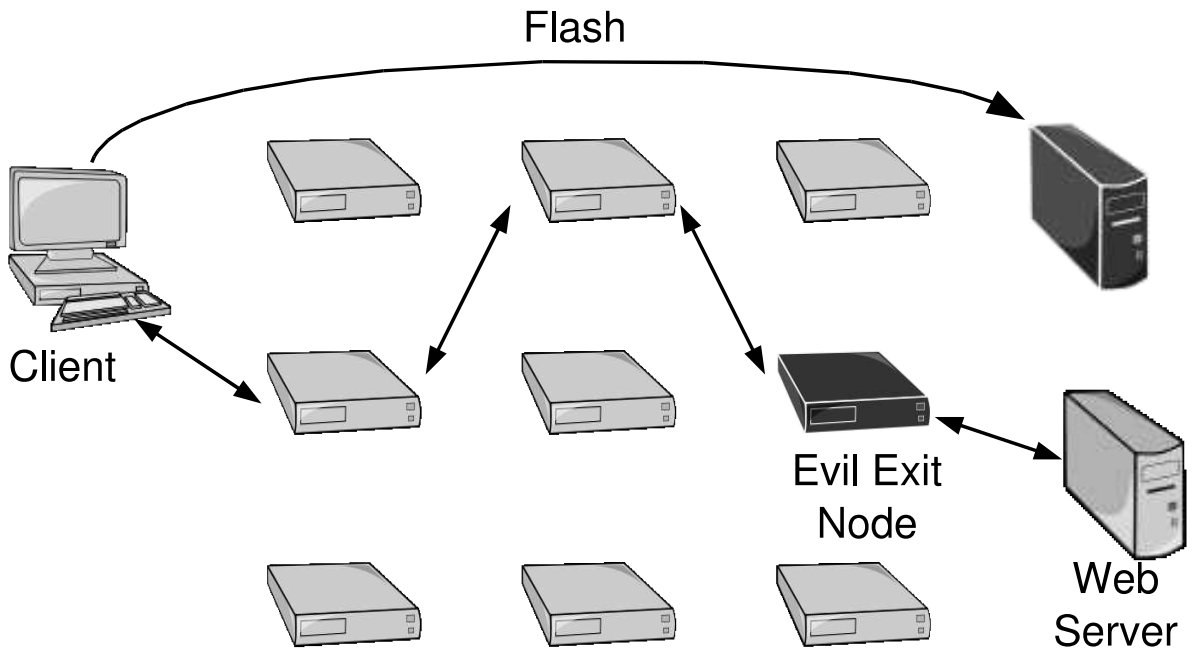


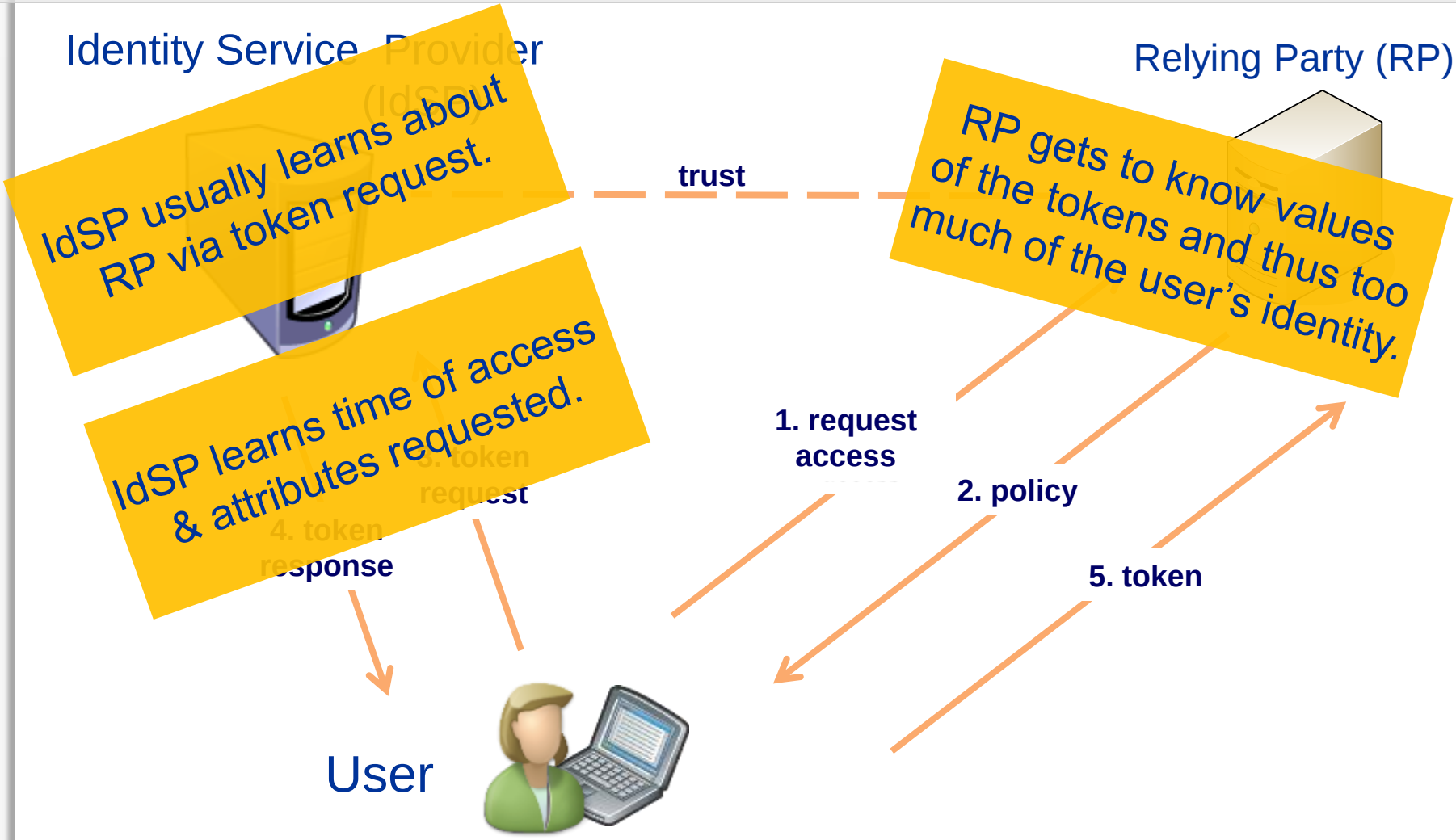
Fig. 3. A browser attack executed by an exit node. The client's web browser executes a Flash program inserted into a webpage by the exit node, which opens a direct connection to a logger machine.

[AbLa2007]

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.

Privacy (and Security) Issues of Typical Federated IdM Architectures



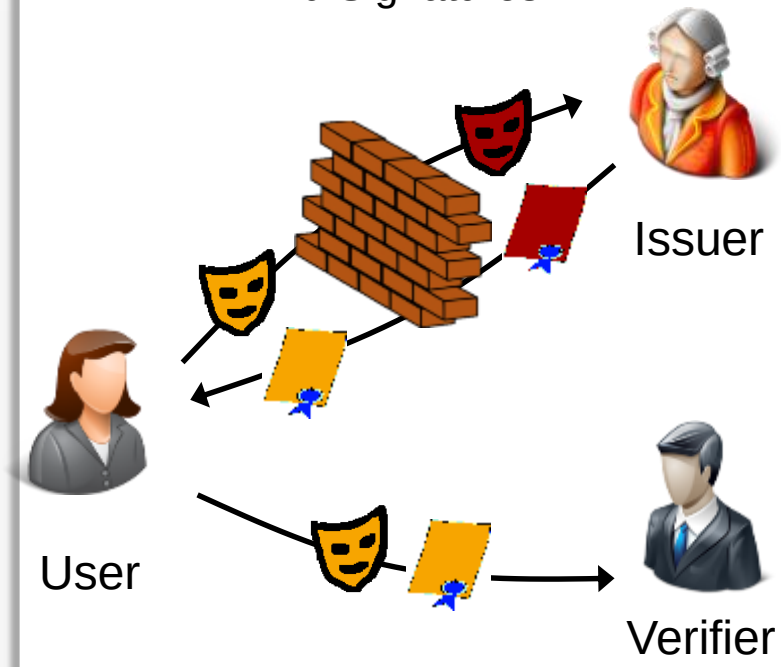
Credential Systems

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

- Privacy features:
  - Different levels of pseudonymity
  - Selective (minimal) disclosure of attributes (attribute hiding)
  - Unlinkability of user's transactions
- Additional features are possible:
  - Prove age without disclosing birthday, e.g. for buying alcohol, showing being over 18
  - Proving of not being revoked, without disclosing the serial number in the credential
  - Controlled linkability, e.g. avoid voting more than once
  - Conditional accountability, when needed

Two Approaches for Privacy-ABCs

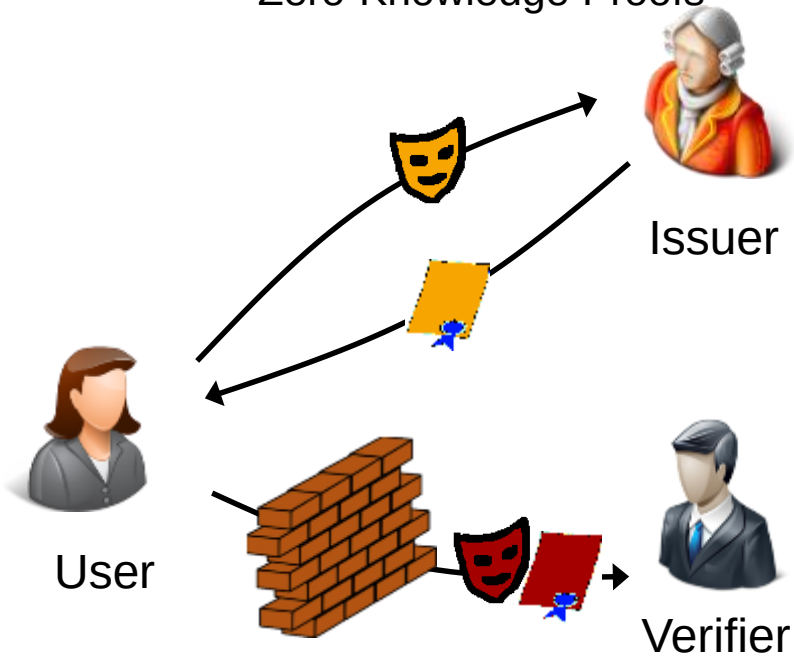
Blind Signatures



U-Prove

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

Zero-Knowledge Proofs



Idemix (Identity Mixer)

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

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.

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.

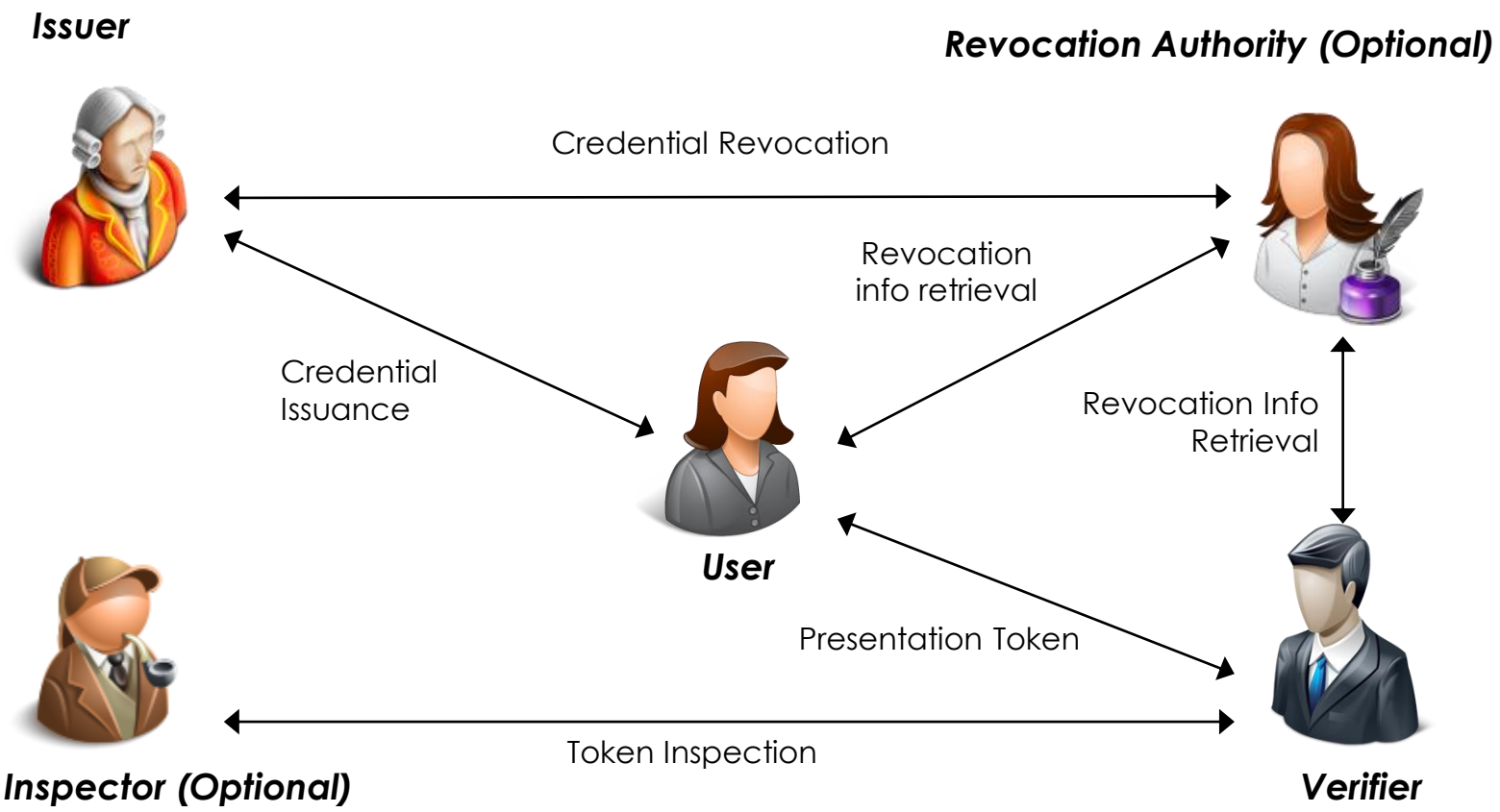
[Cavoukian, A. (2009).]

mobile business

Agenda

- Data Protection and Privacy
- Origin and definition
  - Law, Technology, Standardization
- Technical Privacy Protection
  - Privacy Enhancing Technologies (PETs)
  - Privacy by Design (PbD)
- Integrated Privacy Protection
  - ABC4Trust
  - Privacy Risk Communication and Mitigation
  - Privacy by Default

ABC4Trust Architecture High Level View



Privacy Advisor on Top of Privacy-ABCs

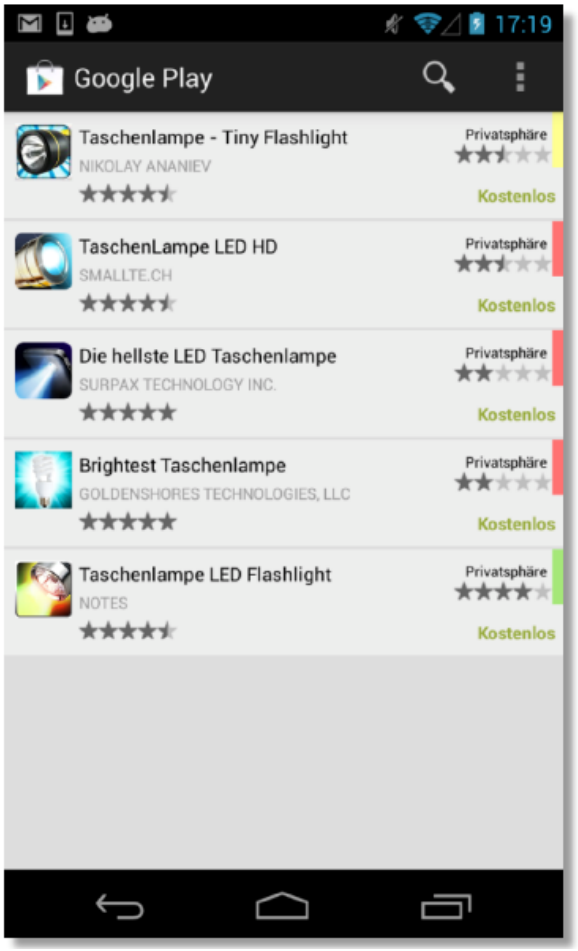
- Privacy advisor that helps users against potentially identity revelations while using privacy-preserving systems.
- Automatic detection of privacy sensitive data.
- Risk analysis.
- Effective communication of the risk to users.

Styx: Privacy Risk Communication Method for Smartphones

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

Benefits of Privacy Risk Communications

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



References

[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