Privacy-respecting Identity Management

Introduction to ABC4Trust

Kai Rannenberg (Kai.Rannenberg@m-chair.de)
Deutsche Telekom Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt, Germany
www.m-chair.de

A research project funded by the European Commission's 7th Framework Programme

Agenda

- Identity Management
- Some Privacy Problems in Identity Management and Assurance
  - Identity Management and Overidentification
  - Identity Assurance and the “Calling Home” Problem
- Attribute Based Credentials
- The ABC4Trust Project
  - The Trials
  - The Architecture
- Today’s Meeting Agenda
- Concluding Remarks

ABC4TRUST

Agenda

- Identity Management
- Some Privacy Problems in Identity Management and Assurance
  - Identity Management and Overidentification
  - Identity Assurance and the “Calling Home” Problem
- Attribute Based Credentials
- The ABC4Trust Project
  - The Trials
  - The Architecture
- Today’s Meeting Agenda
- Concluding Remarks

ABC4TRUST

Identity Management (IdM)
An early approach

- „Fear not, for I have redeemed you;
  I have called you by name: you are mine.”
  [Isaiah 43:1]
- „Var inte rädd, för jag har betalat lösen för dig.
  Jag har kallat dig vid namn, och du är min.”
  [Jesaja 43:1]
- „Μη φοβου· διοτι εγω σε ελυτρωσα,
  σε εκαλεσα με το ονομα σου· εμου εισαι“
  [Ησαιαν 43:1]
- „No temas, porque yo te he redimido,
  te he llamado por tu nombre; mío eres tú.“
  [Isaías 43 [1]]
- „Fürchte dich nicht, denn ich habe dich erlöst;
  ich habe dich bei deinem Namen gerufen; du bist mein!“
  [Jesaja 43,1]

ABC4TRUST

Identity Management (IdM)
2 sides of a medal with enormous economic potential

- **Organisations** aim to sort out
  - User Accounts in different IT systems
  - Authentication
  - Rights management
  - Access control
- **Unified identities** help to
  - ease administration
  - manage customer relations
- **Identity management systems**
  - ease single-sign-on by unify accounts
  - solve the problems of multiple passwords

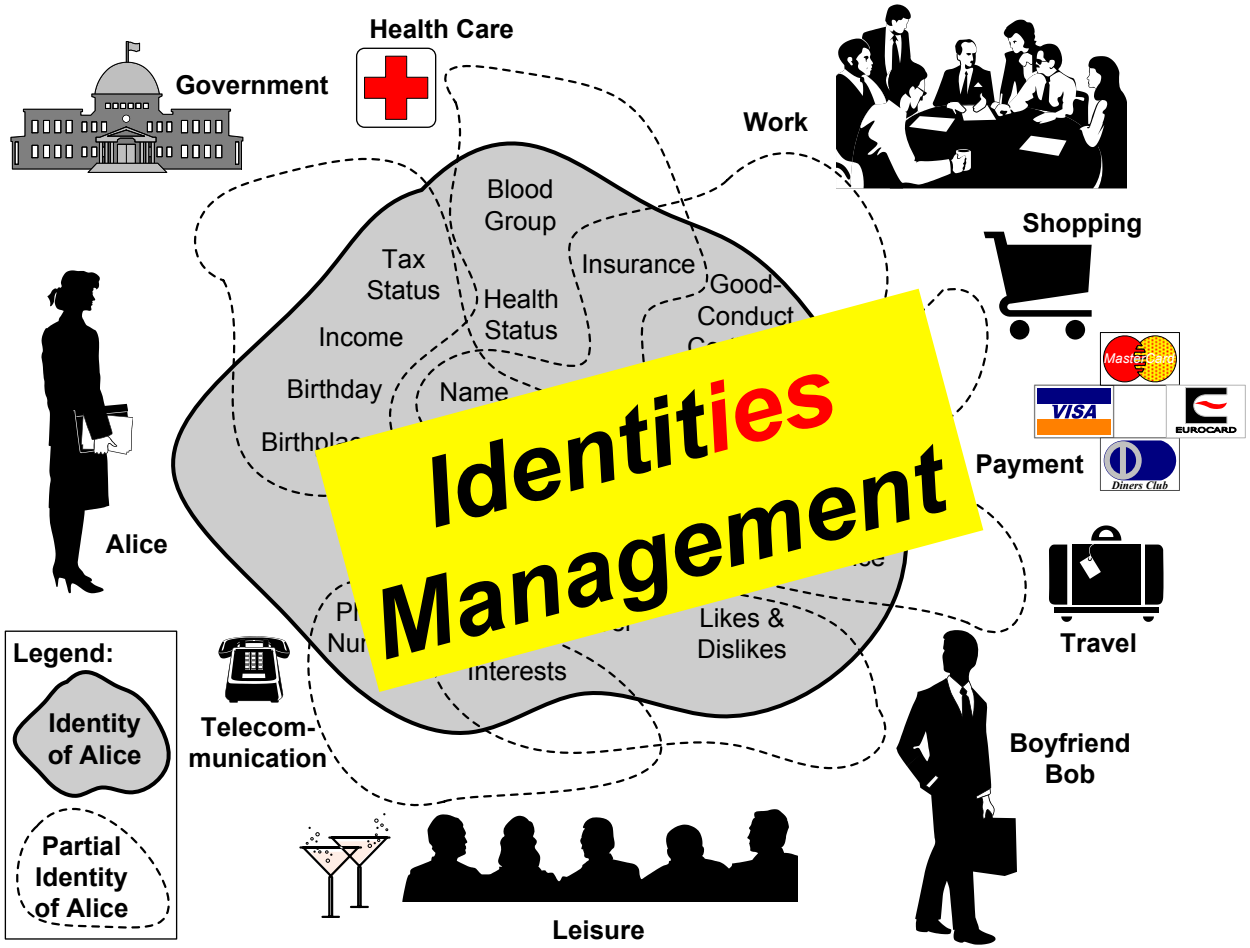
- **People** live their life
  - in different roles (professional, private, volunteer)
  - using different identities (pseudonyms): email accounts, SIM cards, eBay trade names, chat names, Facebook names, …)
- **Differentiated identities** help to
  - protect
    - privacy, especially anonymity
    - personal security/safety
  - enable reputation building at the same time
- **Identity management systems**
  - support users using role based identities
  - help to present the “right” identity in the right context

Identity Management (IdM)
2 sides of a medal with enormous economic potential

- **People** live their life
  - in different roles (professional, private, volunteer)
  - using different identities (pseudonyms): email accounts, SIM cards, eBay trade names, chat names, Facebook names, …)
- **Differentiated identities** help to
  - protect
    - privacy, especially anonymity
    - personal security/safety
  - enable reputation building at the same time
- **Identity management systems**
  - support users using role based identities
  - help to present the “right” identity in the right context

- **Organisations** aim to sort out
  - User Accounts in different IT systems
  - Authentication
  - Rights management
  - Access control
- **Unified identities** help to
  - ease administration
  - manage customer relations
- **Identity management systems**
  - ease single-sign-on by unify accounts
  - solve the problems of multiple passwords

Partial Identities



Based on [Clauß, Köhntopp 2001]

Identity Management (IdM)
One of many definitions

An integrated concept of
processes, policies and **technologies**
that enable
organizations and **individual entities**
to facilitate and control
the
use of identity information
in **their** **respective relations**

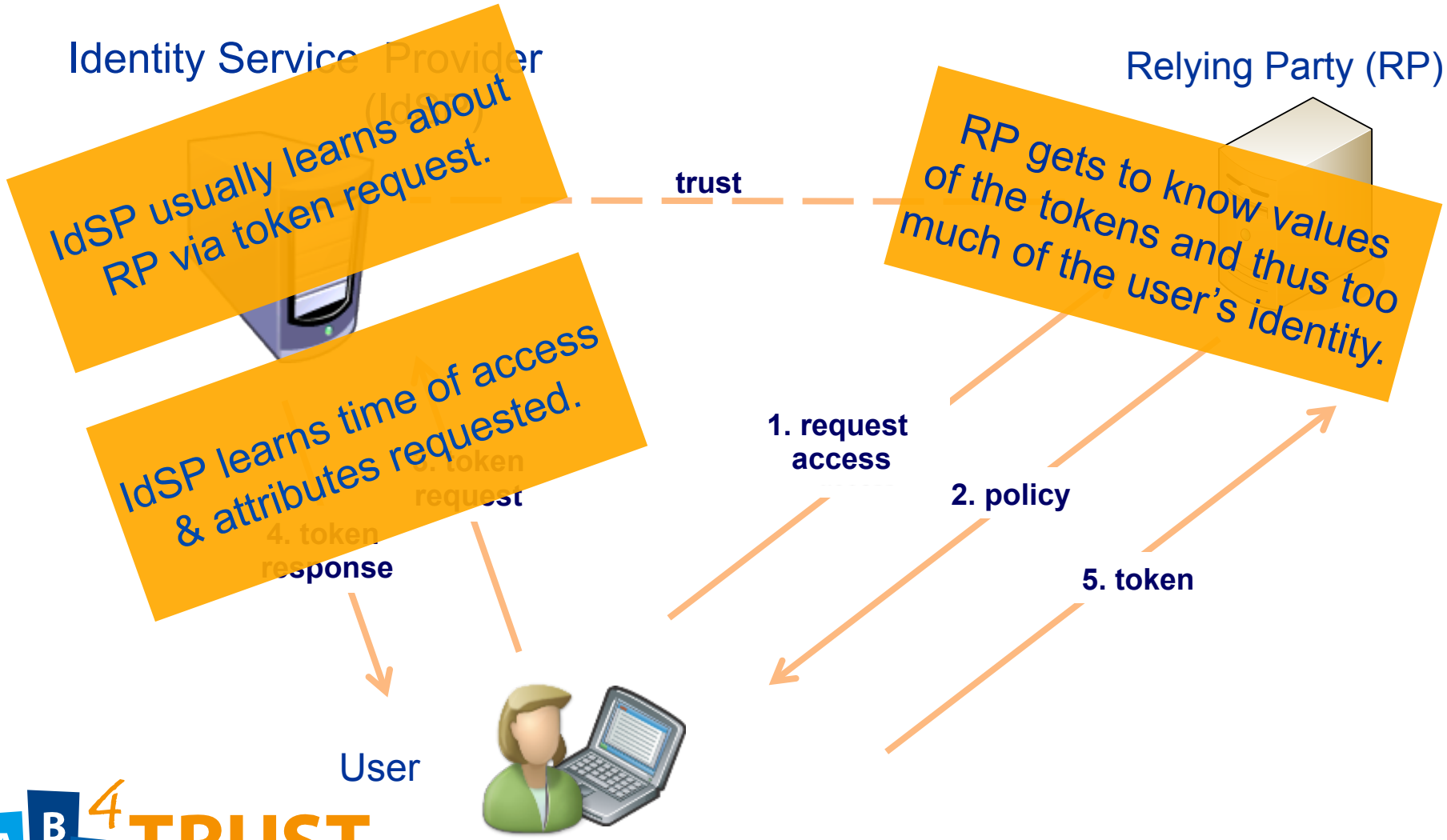
ABC4TRUST

Agenda

- Identity Management
- Some Privacy Problems in Identity Management and Assurance
  - Identity Management and Overidentification
  - Identity Assurance and the “Calling Home” Problem
- Attribute Based Credentials
- The ABC4Trust Project
  - The Trials
  - The Architecture
- Today’s Meeting Agenda
- Concluding Remarks

ABC4TRUST

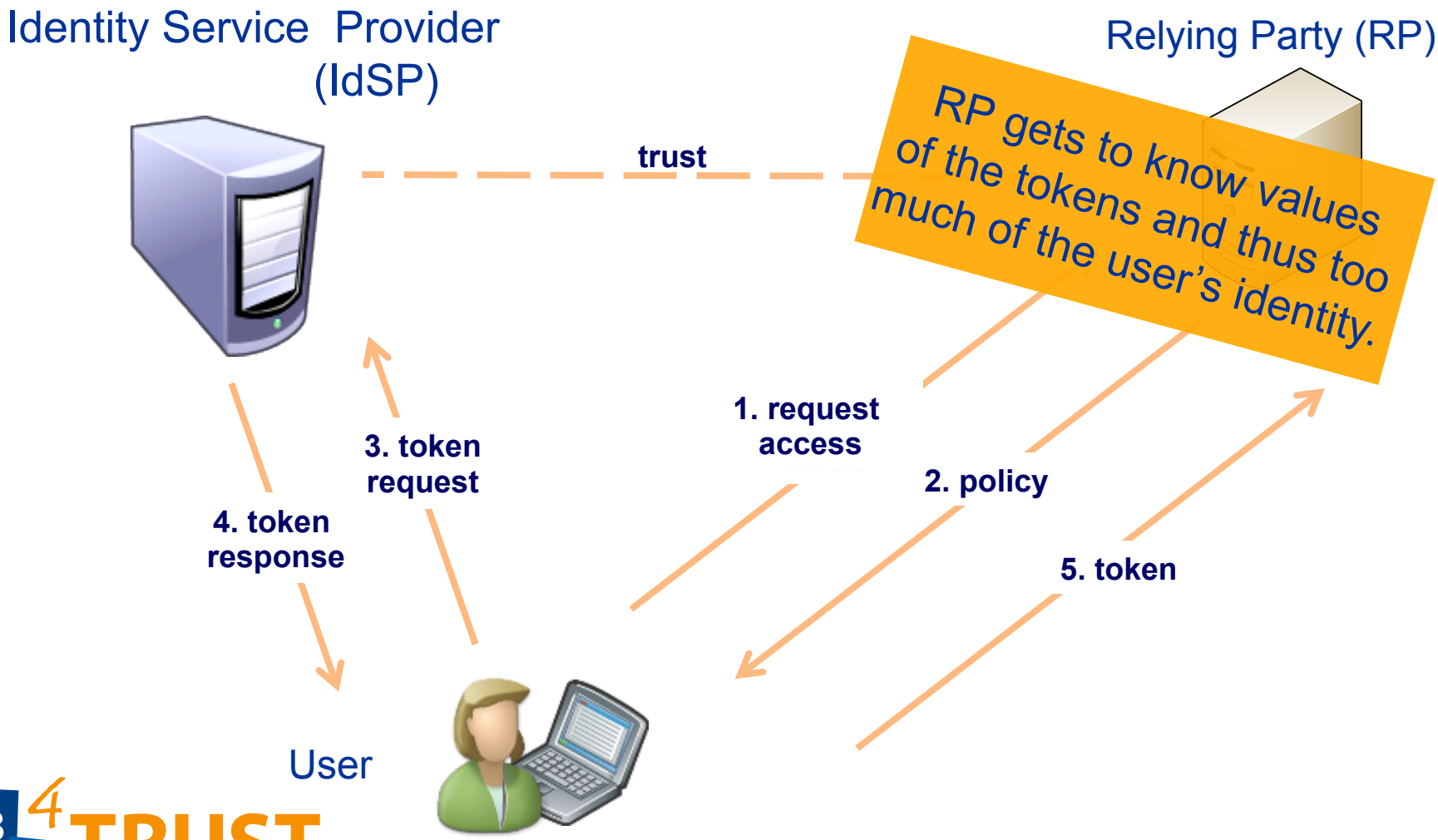
Privacy (and security) issues of typical federated IdM architectures



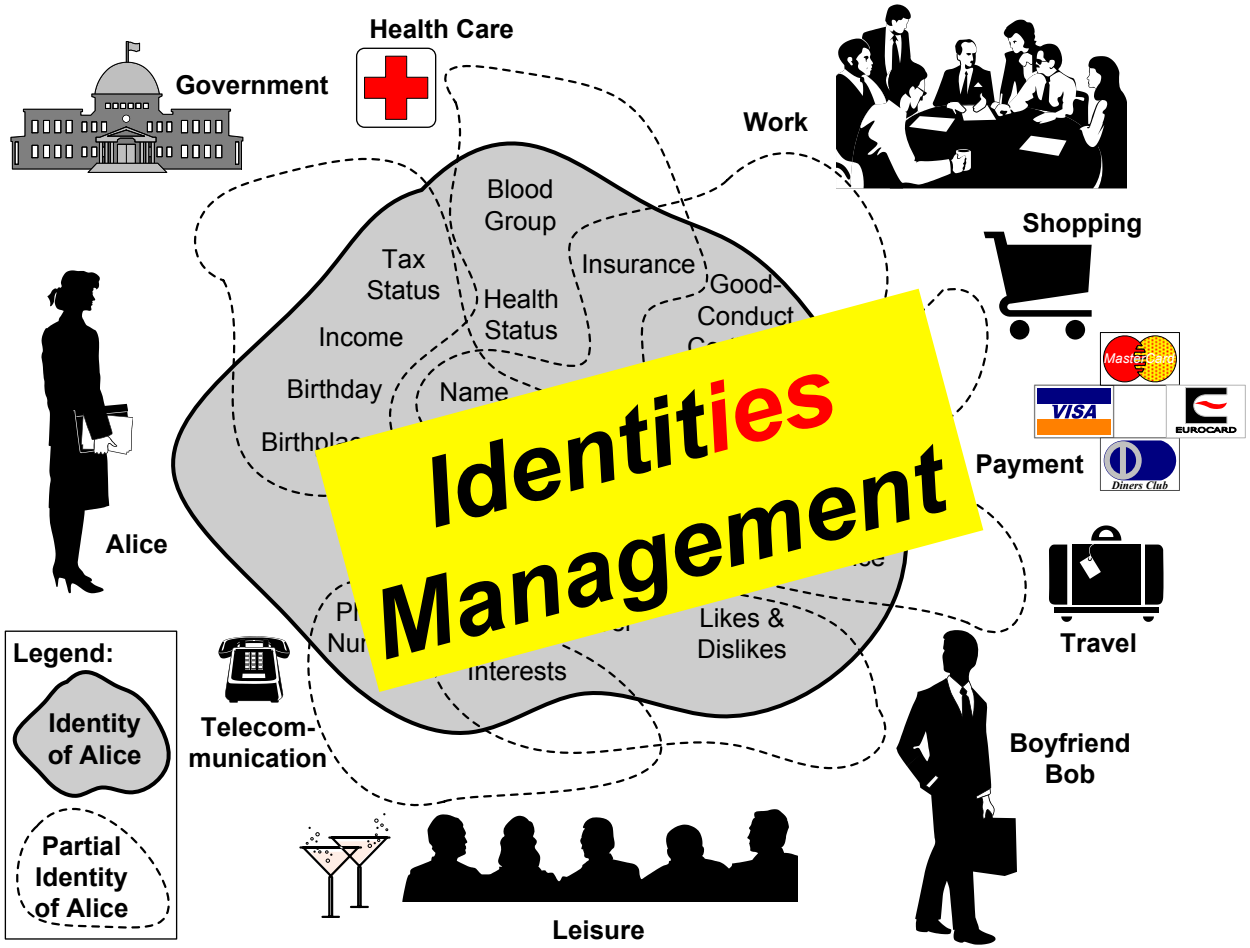
Agenda

- Identity Management
- Some Privacy Problems in Identity Management and Assurance
  - Identity Management and Overidentification
  - Identity Assurance and the “Calling Home” Problem
- Attribute Based Credentials
- The ABC4Trust Project
  - The Trials
  - The Architecture
- Today’s Meeting Agenda
- Concluding Remarks

Identity Management and Overidentification



Partial Identities needed



Based on [Clauß, Köhntopp 2001]

Identity Definition in ISO/IEC 24760 to reduce the risk of Overidentification

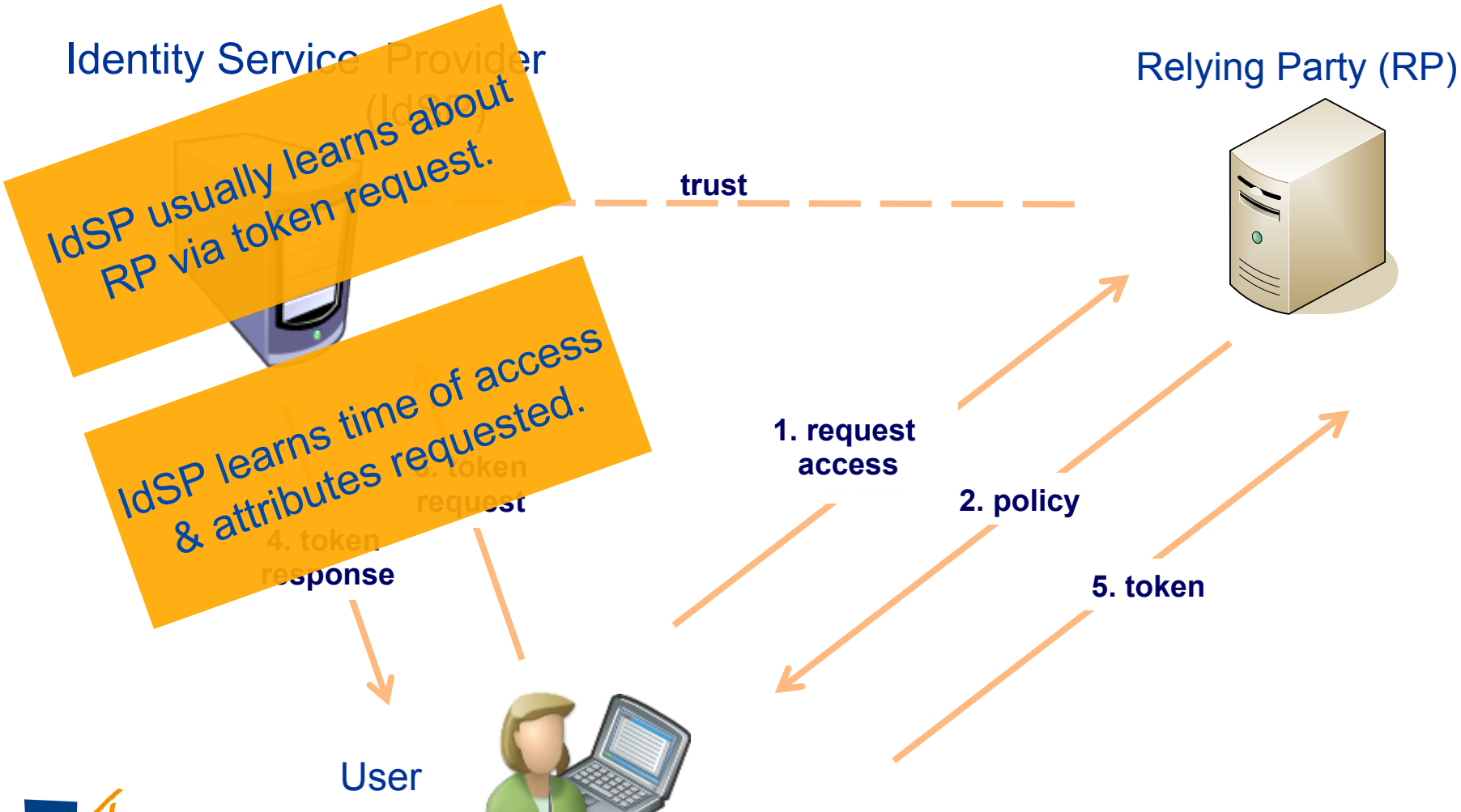
- **Identity** (partial identity):
  - "Set of **attributes** related to an **entity**"
  - From "A Framework for Identity Management" (ISO/IEC 24760)
    - **Part 1: Terminology and concepts (IS:2011)**
    - Part 2: Reference framework and requirements (FDIS)
    - Part 3: Practice (CD)

[standards.iso.org/ittf/PubliclyAvailableStandards/index.html, www.jtc1sc27.din.de/en]

Agenda

- Identity Management
- Some Privacy Problems in Identity Management and Assurance
  - Identity Management and Overidentification
  - Identity Assurance and the “Calling Home” Problem
- Attribute Based Credentials
- The ABC4Trust Project
  - The Trials
  - The Architecture
- Today’s Meeting Agenda
- Concluding Remarks

The “Calling Home” Problem



Agenda

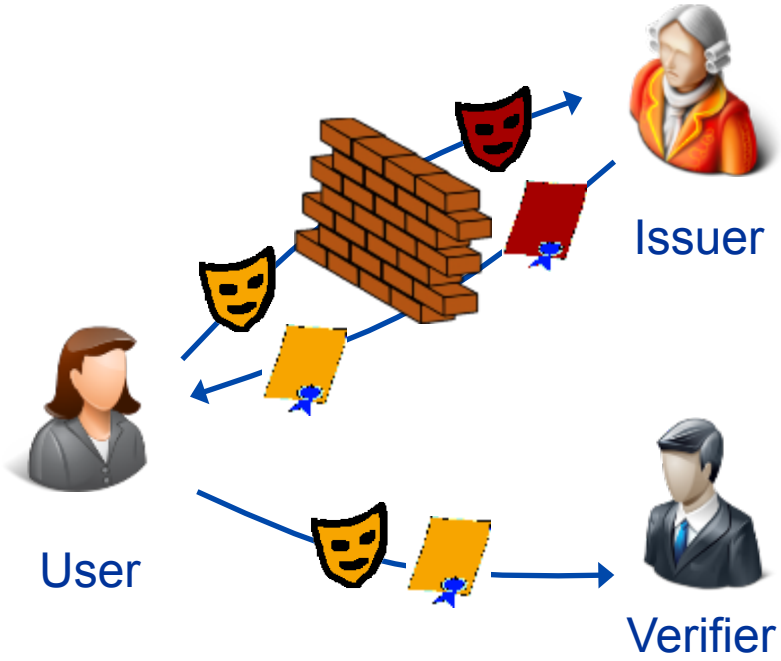
- Identity Management
- Some Privacy Problems in Identity Management and Assurance
  - Identity Management and Overidentification
  - Identity Assurance and the “Calling Home” Problem
- Attribute Based Credentials
- The ABC4Trust Project
  - The Trials
  - The Architecture
- Today’s Meeting Agenda
- Concluding Remarks

Attribute Based Credentials (Privacy-ABCs)

- Certifying **relevant attributes**
- Token issuance and presentation **unlinkable**
  - Rather “coins” (that cannot be distinguished) than “bank notes” (that have a serial number)
- Users can disclose (minimal) **subsets** of the encoded **claims**
  - To respond to unanticipated requests of RPs
  - Without invalidating the token integrity
  - E.g. Certificate for birth date -> Claim for being over 21
- Two major **approaches** and **technologies**
  - U-Prove (Credentica -> Microsoft)
  - Idemix (IBM)

Two approaches for Privacy-ABCs

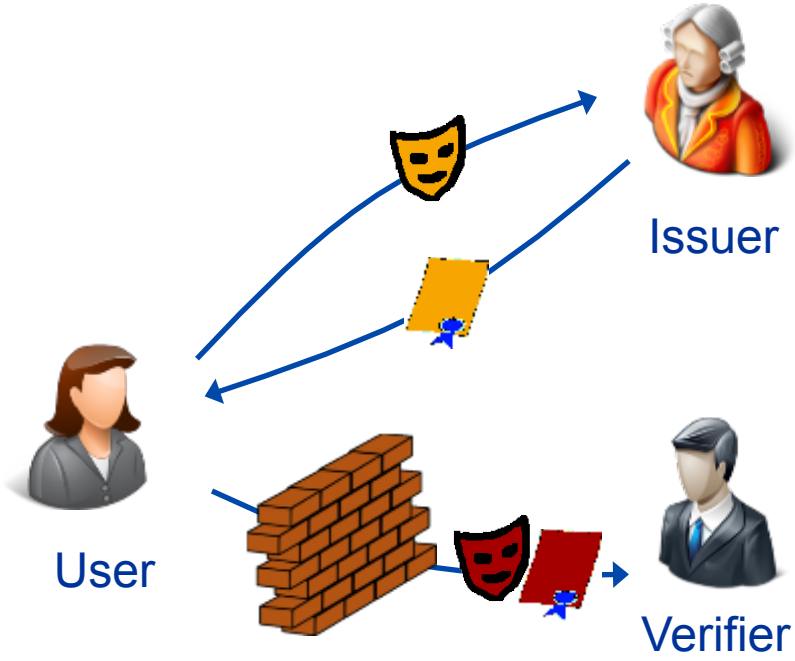
Blind Signatures



U-Prove

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

Zero-Knowledge Proofs



Idemix (Identity Mixer)

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

ABC4TRUST

Agenda

- Identity Management
- Some Privacy Problems in Identity Management and Assurance
  - Identity Management and Overidentification
  - Identity Assurance and the “Calling Home” Problem
- Attribute Based Credentials
- The ABC4Trust Project
  - The Trials
  - The Architecture
- Today’s Meeting Agenda
- Concluding Remarks

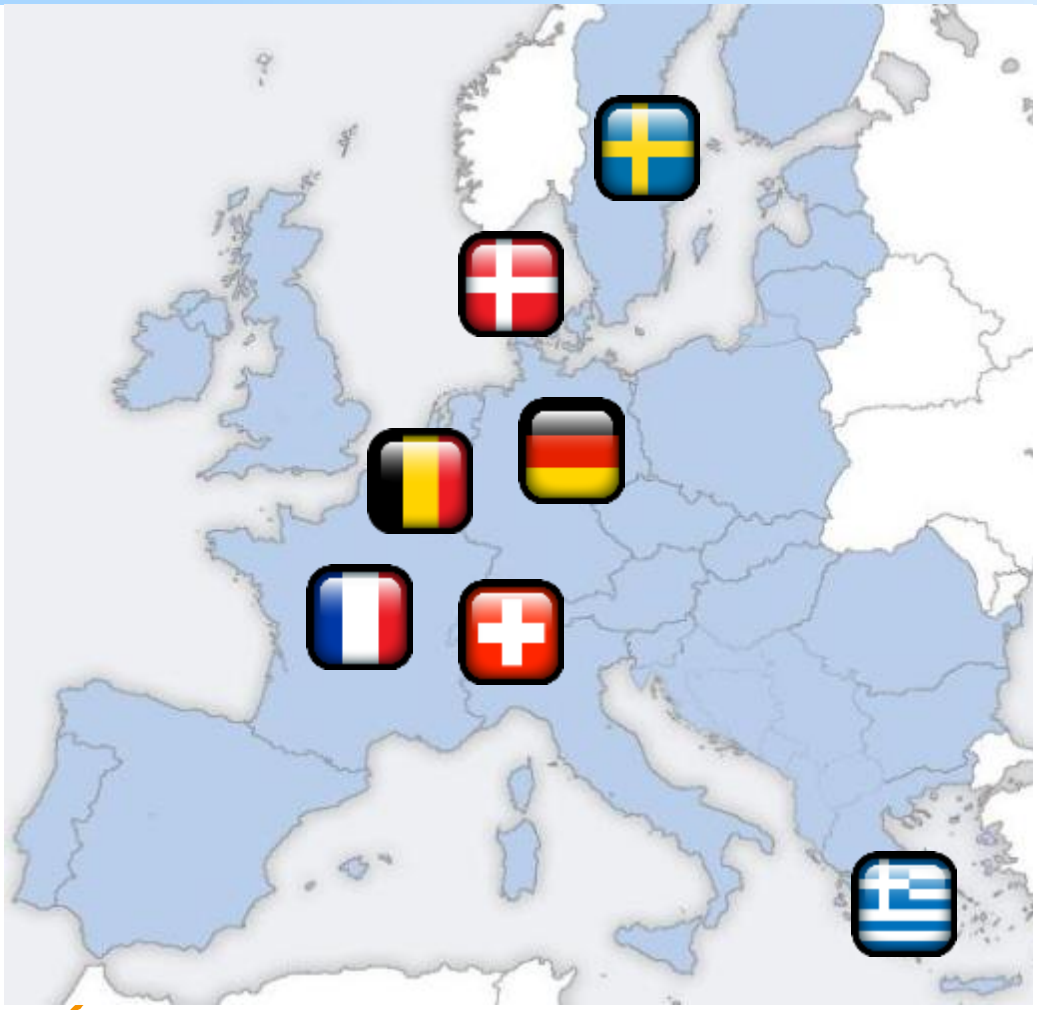
ABC4Trust Objectives

- A common, unified architecture for ABC systems to enable
  - Comparing their respective features
  - Combining them on common platforms
  - “Lock-In” free usage of Privacy-ABC systems
- Open reference implementations of selected ABC systems
- Deployments in actual production enabling
  - Minimal disclosure
  - Provision of pseudonymous/anonymous feedback to a community to one is accredited as a member
- Relevant Standards
  - e.g. in ISO/IEC JTC 1/SC 27/WG 5 “Identity Management and Privacy Technologies”

SEVENTH FRAMEWORK PROGRAMME

ABC4TRUST

ABC4Trust Partners



Johann Wolfgang Goethe-Universität Frankfurt, DE

Alexandra Institute AS, DK

Computer Technology Institute & Press – "DIOPHANTUS", GR

IBM Research - Zurich, CH

Miracle A/S, DK

Nokia, DE

Technische Universität Darmstadt, DE

Unabhängiges Landeszentrum für Datenschutz, DE

Eurodocs AB, SE

CryptoExperts SAS, FR

Microsoft NV, BE

Söderhamn Kommun, SE

ABC4TRUST

Agenda

- Identity Management
- Some Privacy Problems in Identity Management and Assurance
  - Identity Management and Overidentification
  - Identity Assurance and the “Calling Home” Problem
- Attribute Based Credentials
- The ABC4Trust Project
  - The Trials
  - The Architecture
- Today’s Meeting Agenda
- Concluding Remarks

ABC4Trust Pilot Trial: Course Rating

Computer Technology Institute & Press – “Diophantus”
Patras, Greece

- Course ratings conducted anonymously without lecturers knowing participants’ identities
- Conduct polls based on attendance
- Issue multiple credentials (student cards, course enrolment)
- Verify with anonymous proofs towards “untrusted” infrastructure
- Privacy-friendly rewarding process

ABC4TRUST

ABC4Trust Pilot Trial: Community Interaction

Norrtullskolan School
Söderhamn, Sweden

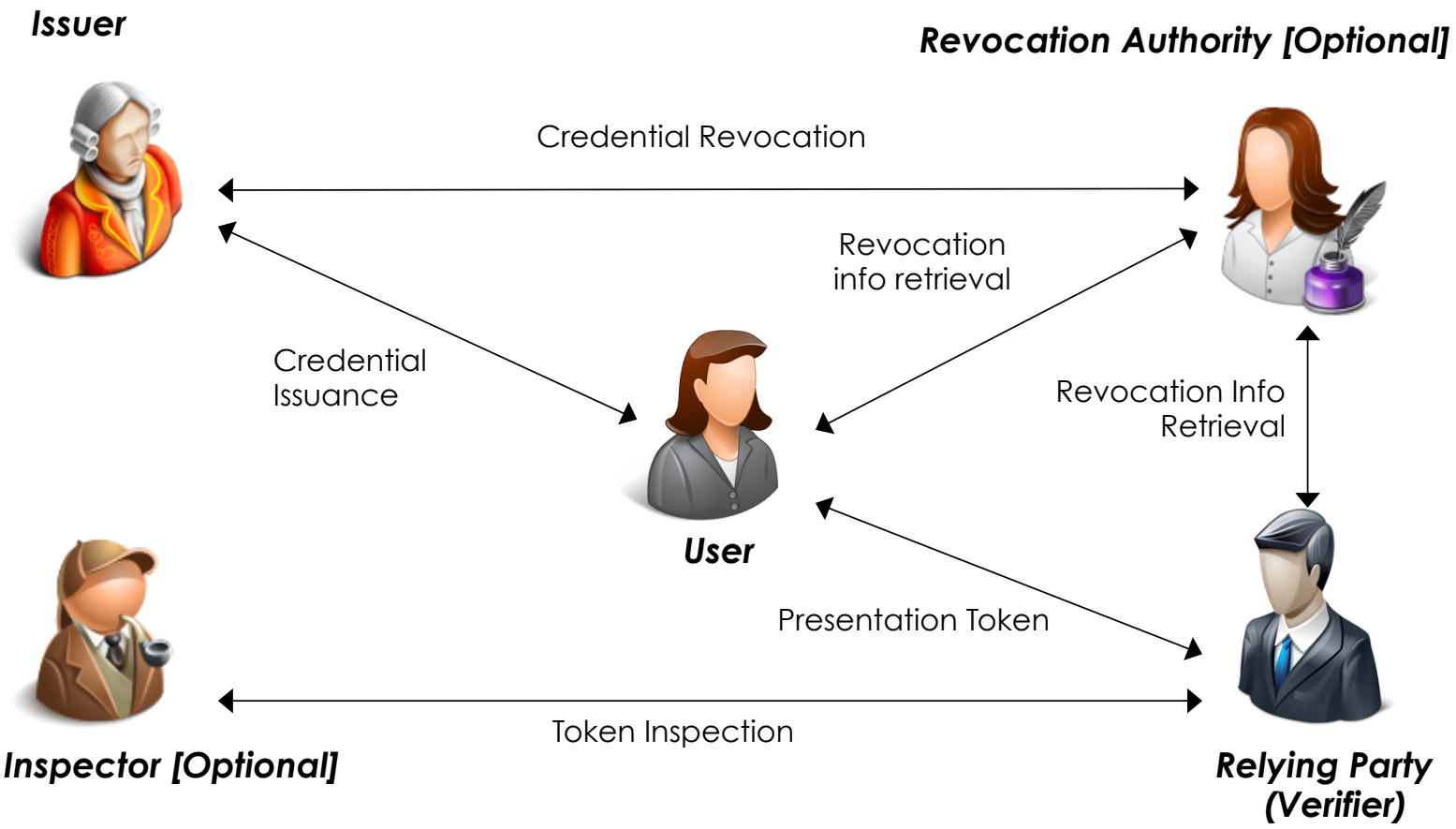
- School internal social network for communication among pupils, teachers, and personnel
- Provide trusted authentication while protecting pseudonymity/ anonymity
- Usability: make privacy technology usable for non-technical users (e.g. pupils)

ABC4TRUST

Agenda

- Identity Management
- Some Privacy Problems in Identity Management and Assurance
  - Identity Management and Overidentification
  - Identity Assurance and the “Calling Home” Problem
- Attribute Based Credentials
- The ABC4Trust Project
  - The Trials
  - The Architecture
- Today’s Meeting Agenda
- Concluding Remarks

ABC4Trust Architecture
High Level View



The ABC4Trust Architecture Characteristics

- Unification of features
  - ***Selective disclosure***, ***pseudonymity***, ***unlinkability***, …
  - XML specification of the data exchange between e.g. Issuer, User, Verifier, Revocation Authority
- Crypto Architecture
  - Allows ***seamless integration*** of cryptographic primitives
  - Encapsulated in components with common interfaces, allowing the rest of the cryptographic layer to be implementation-agnostic
- Users can
  - obtain credentials for more than one Privacy-ABC technology and
  - use them on the same hardware and software platforms.
- Service providers and Identity Service Providers can
  - adopt whatever Privacy-ABC technology best suits their needs.
- Open source implementation available on Github

➢ ***Avoid technology lock-in***

➢ ***Raise trust in Privacy-ABC technologies***

ABC4TRUST

Agenda

- Identity Management
- Some Privacy Problems in Identity Management and Assurance
  - Identity Management and Overidentification
  - Identity Assurance and the “Calling Home” Problem
- Attribute Based Credentials
- The ABC4Trust Project
  - The Trials
  - The Architecture
- Today’s Meeting Agenda
- Concluding Remarks

Summit event agenda I

Time	Agenda Item	
09:30	Opening & Welcome Friedrich von Heusinger (Director of the Representation of the State of Hessen to the EU) Prof. Dr. Birgitta Wolff (President of Goethe University Frankfurt)	
	"EU funded research is keeping up trust in digital society" Rafael Tesoro Carretero (European Commission Directorate-General for Communications Networks, Content and Technology Trust and Security	
	“Privacy-respecting Identity Management - Introduction to ABC4Trust” Prof. Dr. Kai Rannenberg (Goethe University Frankfurt)	
10:30	The Patras Pilot	“ePolls and evaluations” Prof. Dr. Yannis Stamatiou (Computer Technology Institute & Press - DIOPHANTUS)
		“Architecture: Mandatory roles and features” Ahmad Sabouri (Goethe University Frankfurt)
		Demo Prof. Dr. Yannis Stamatiou (Computer Technology Institute & Press - DIOPHANTUS)
11:20	Coffee Break	
11:50	The Söderhamn Pilot	“Community interaction platform” Souheil Bcheri (Eurodocs AB)
12:40	“Architecture layers” Ahmad Sabouri (Goethe University Frankfurt)	
13:00	Lunch break	

Summit event agenda II

14:00	Greeting Address from the European Parliament Jan Albrecht (MEP, Greens/EFA, EP Rapporteur General Data Protection Regulation)	
14:15	"NSTIC at 4: Putting an ecosystem into operation" Michael Garcia (Deputy Director National Strategy for Trusted Identities in Cyberspace, National Institute of Standards and Technology, U.S. Department of Commerce - NIST)	
15:00	"The ABC4Trust Reference implementation" Dr. Michael Østergaard (Miracle A/S)	
15:25	"ABC4Trust on smart cards" Dr. Pascal Paillier	
15:45	"Privacy-ABC technology on mobile phones" Gert Læssøe Mikkelsen (Alexandra A/S)	
16:05	"A movie streaming application & ABC4Trust as services on the cloud" Dr. Anja Lehmann (IBM Research Zurich)	
16:25	Coffee Break	
16:45	Panel discussion	"Global and European Identity Initiatives (and ABC4Trust)"
		Chair: Marit Hansen (Deputy Chief of the Independent Centre for Privacy Protection Schleswig-Holstein, ULD)
		Panellists: Ronnny Bjones (Microsoft); Neil Clowes (EC - eIDAS Task Force); Michael Garcia (NIST); Achim Klabunde (EDPS); Kai Rannenberg (Goethe University Frankfurt)
	Greeting Mark Weinmeister (State Secretary of European Affairs at the Hessian State Chancellery)	
18:15	Reception; introducing the "ABC4Trusters"	

Agenda

- Identity Management
- Some Privacy Problems in Identity Management and Assurance
  - Identity Management and Overidentification
  - Identity Assurance and the “Calling Home” Problem
- Attribute Based Credentials
- The ABC4Trust Project
  - The Trials
  - The Architecture
  - Benefits
- Today’s Meeting Agenda
- Concluding Remarks

ABC4TRUST

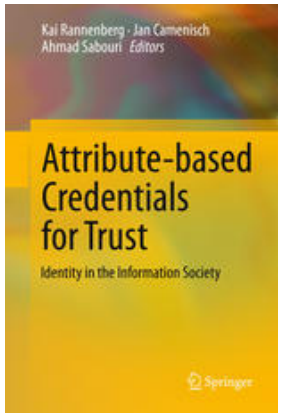
Benefits from ABC4Trust

- Security and privacy hand in hand
  - The excuse that secure but pseudonymous authentication is impossible does not hold anymore.
  - Accountability: if identification is needed only for cases that went wrong, inspection provides a solution.
  - "Lock-In" free usage of Privacy-ABC systems
  - A basis for "Privacy by design" in citizen cards and other identity platforms

Conclusions & Outlook

- ICT and related services are coming ever closer to people.
- A more privacy friendly Internet requires:
  - Partial Identities and Identifiers
  - Minimum Disclosure
  - Attribute Based Credentials
  - Strong Sovereign Assurance Tokens (smart cards, mobile devices, …)

- ABC4Trust Book
- www.abc4trust.eu



- www.jtc1sc27.din.de/en
- www.fidis.net
- www.picos-project.eu
- www.primelife.eu
- www.prime-project.eu

- www.m-chair.de, Kai.Rannenberg@m-chair.de

ABC4TRUST

Back up

The ABC4Trust Architecture Characteristics

- Abstraction of concepts of Privacy-ABCs
- Unification of features
  - specification of the data artefacts exchanged between the entities (i.e. issuer, user, verifier, revocation authority, etc.)
- Crypto Architecture
  - Modularized design.
  - Allows the implementation of additional features, such as predicate for checking linear combinations among attributes.
- Users will be able to
  - obtain credentials for many Privacy-ABC technologies and
  - use them on the same hardware and software platforms
  - without having to consider which Privacy-ABC technology has been used.
- Service providers and Identity Service Providers will be able to
  - adopt whatever Privacy-ABC technology best suits their needs.
- Avoid technology lock-in
- Raise trust in Privacy-ABC technologies

ABC4TRUST

Crypto Architecture

- Provide a truly plug-and-play architecture that allows the seamless integration of cryptographic primitives e.g.:
  - Privacy-ABC signatures: Idemix and Uprove
  - Predicate Proofs
- Move away from the "bridging" approach between several incompatible crypto engines
- Encapsulated in components with common interfaces, allowing the rest of the cryptographic layer to be implementation-agnostic

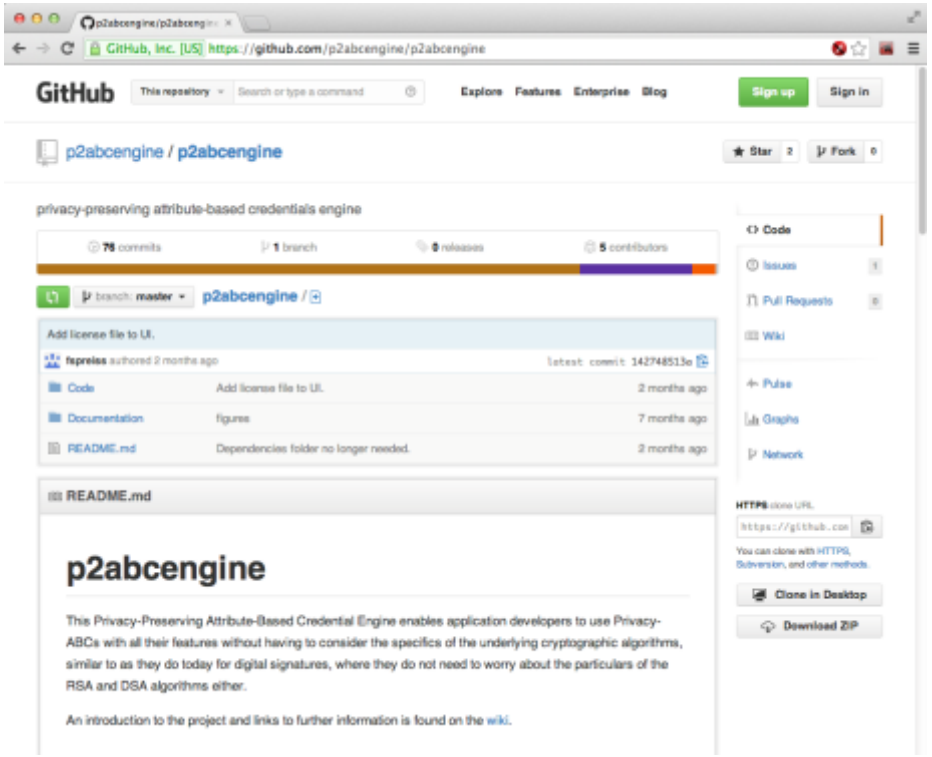
Agenda

- Identity Management
- Some Privacy Problems in Identity Management and Assurance
  - Identity Management and Overidentification
  - Identity Assurance and the “Calling Home” Problem
- Attribute Based Credentials
- The ABC4Trust Project
  - The Trials
  - The Architecture
  - Open Source Reference Implementation
  - ABC4Trust in Perspective
- Conclusions & Outlook

ABC4TRUST

ABC4Trust @GitHub

- https://github.com/p2abcengine/
- Source codes available under Apache license
- Documentation, installation guide and wiki pages



Agenda

- Identity Management
- Some Privacy Problems in Identity Management and Assurance
  - Identity Management and Overidentification
  - Identity Assurance and the “Calling Home” Problem
- Attribute Based Credentials
- The ABC4Trust Project
  - The Trials
  - The Architecture
  - Open Source Reference Implementation
  - ABC4Trust in Perspective
- Conclusions & Outlook

ABC4TRUST

General Challenges & Potential Identity Management

- Considering
  - the views of the respective stakeholders (Multilateral Security)
  - separations of domains that had been natural “before”
- Enabling users to manage their identities and IDs
- Frameworks and reference architectures
  - Along the value chain (with appropriate incentives)
  - For business processes and applications
  - For new communities and networks
- Globally standardized (e.g. in ISO/IEC JTC 1/SC 27/WG 5 “Identity Management and Privacy Technologies” & OpenID Foundation)

The ABC4Trust Architecture Characteristics

- Abstraction of concepts of Privacy-ABCs
- Unification of features
  - XML specification of the data exchange between e.g. issuer, user, verifier, revocation authority
- Crypto Architecture
  - Allows the seamless integration of cryptographic primitives e.g.:
    - Privacy-ABC signatures
    - Predicate Proofs
  - Encapsulated in components with common interfaces, allowing the rest of the cryptographic layer to be implementation-agnostic
- Users are able to
  - obtain credentials for many Privacy-ABC technologies and
  - use them on the same hardware and software platforms
  - without having to consider which Privacy-ABC technology has been used.
- Service providers and Identity Service Providers are able to
  - adopt whatever Privacy-ABC technology best suits their needs.
- Open source implementation available on Github
- Avoid technology lock-in
- Raise trust in Privacy-ABC technologies

ABC4TRUST