



Impulse aus ABC4Trust für besseren Datenschutz bei der Kommunikation im Gesundheitswesen

e-health-Gesetz: Durchbruch für Interoperabilität?

Workshop DIN NIA

2015-03-31

Berlin



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

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
- ABC4Trust & Health Telematics
- Concluding Remarks

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
- ABC4Trust & Health Telematics
- Concluding Remarks

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 43¹]
- „Fürchte dich nicht, denn ich habe dich erlöst;
ich habe dich bei deinem Namen gerufen; du bist mein!“
[Jesaja 43,1]





Identity Management (IdM)

2 sides of a medal with enormous economic potential

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

- **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



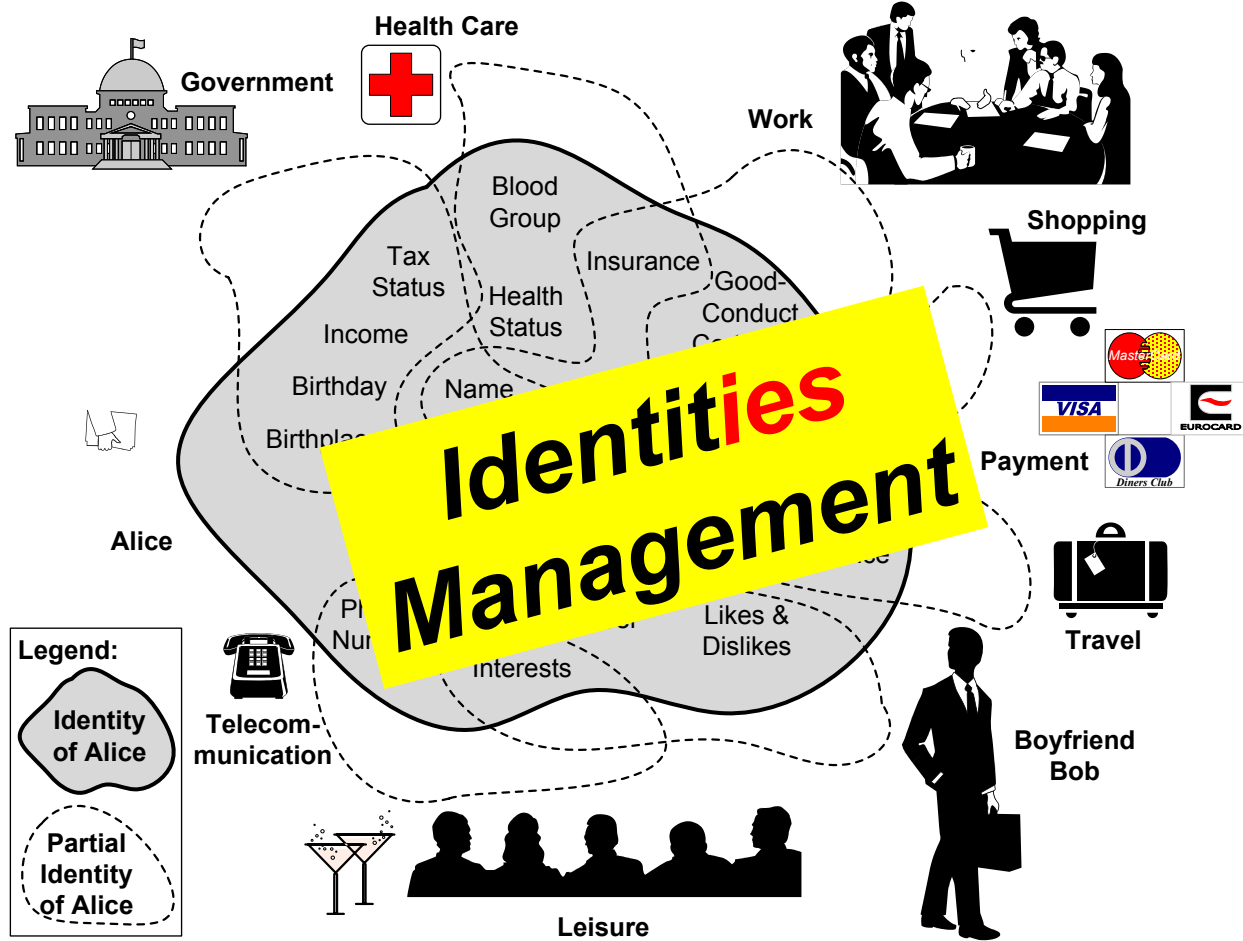
Identity Management (IdM)

2 sides of a medal with enormous economic potential

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

- **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



Identity Management (IdM)

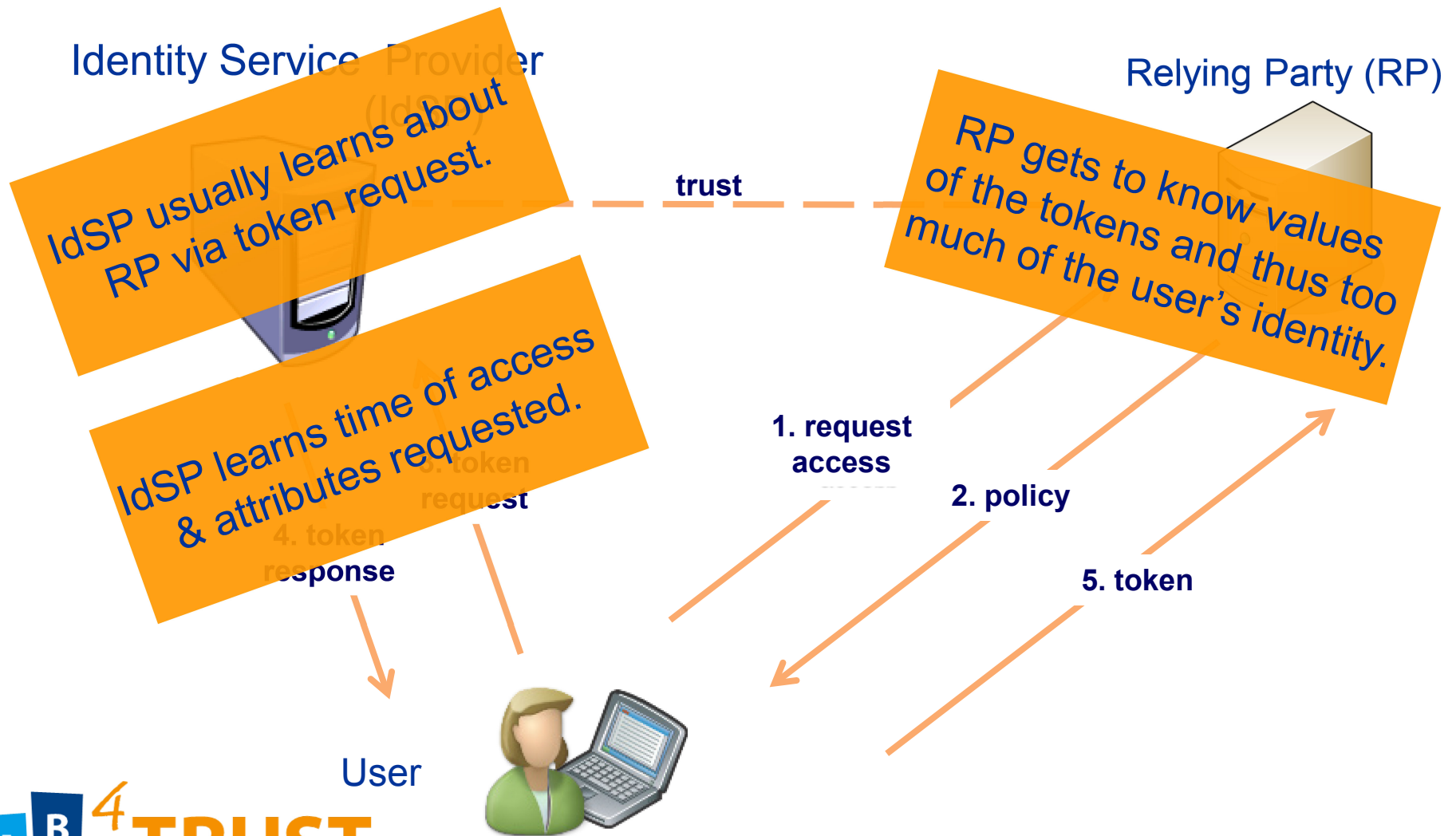
One of many definitions

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**

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
- ABC4Trust & Health Telematics
- Concluding Remarks

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
- ABC4Trust & Health Telematics
- Concluding Remarks

Identity Management and Overidentification

Identity Service Provider (IdSP)

Relying Party (RP)



trust

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

4. token response

3. token request

1. request access

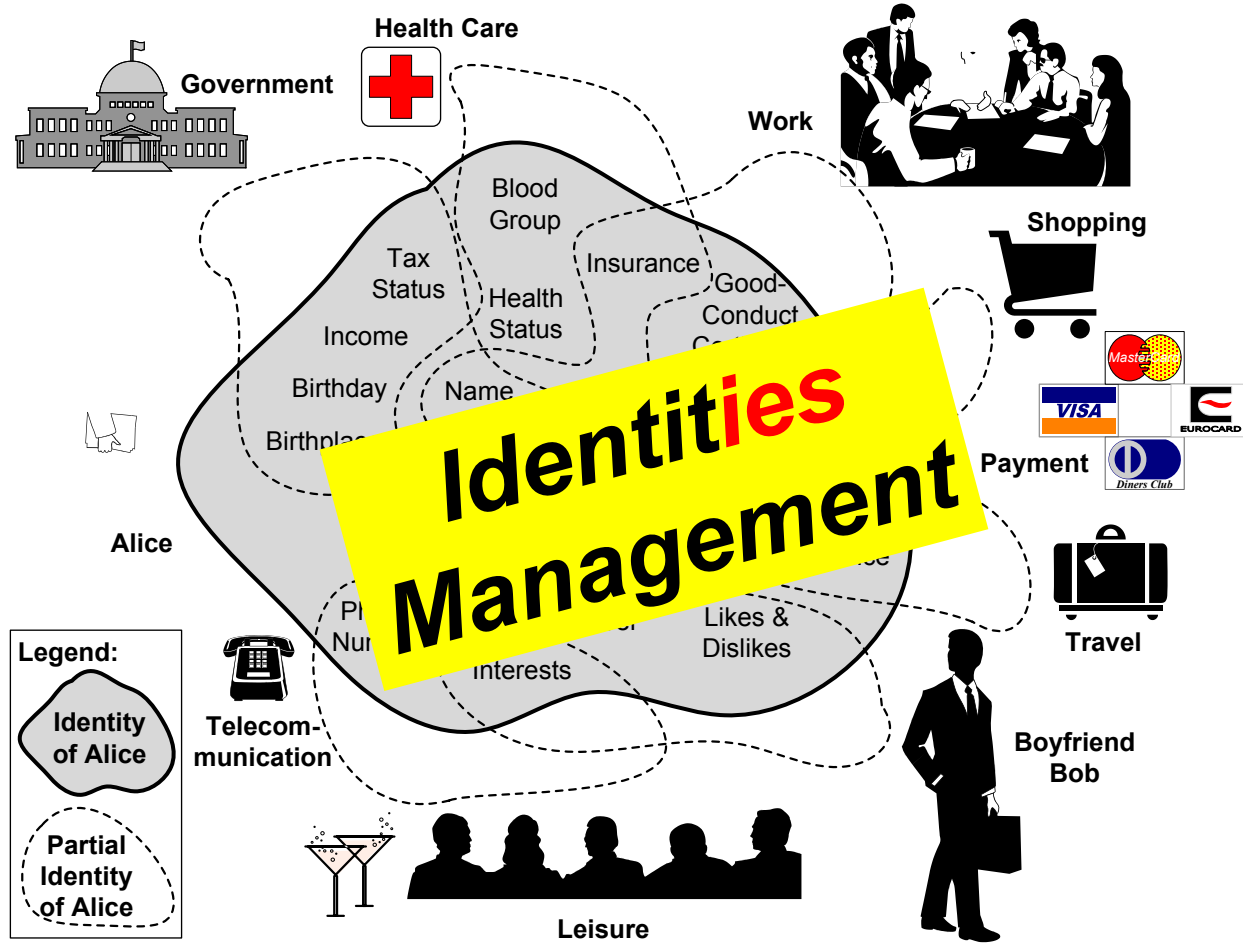
2. policy

5. token

User



Partial Identities needed



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

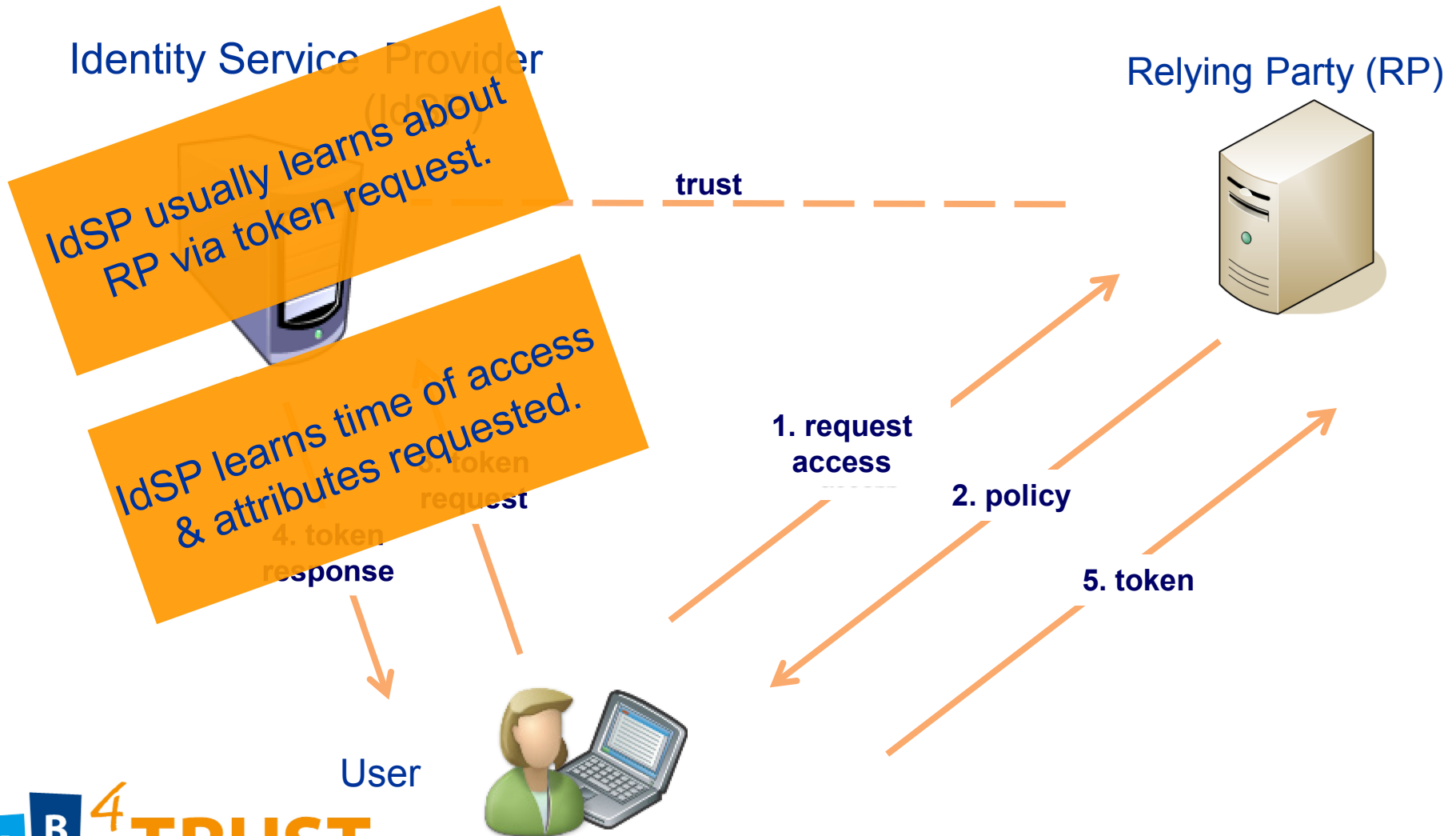
- **Identity** (partial identity):
 - “Set of **attributes** related to an **entity**”
 - From “A Framework for Identity Management” (ISO/IEC 24760)
 - **Part 1: Terminology and concepts (IS:2011)**
 - Part 2: Reference framework and requirements (FDIS)
 - Part 3: Practice (CD)

[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
- ABC4Trust & Health Telematics
- Concluding Remarks

The "Calling Home" Problem



Agenda

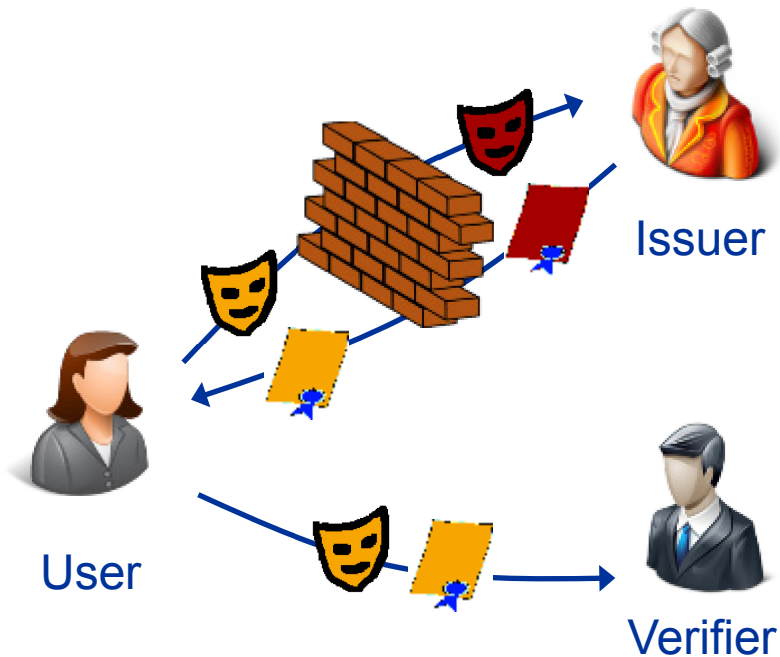
- Identity Management
- Some Privacy Problems in Identity Management and Assurance
 - Identity Management and Overidentification
 - Identity Assurance and the “Calling Home” Problem
- Attribute Based Credentials
- The ABC4Trust Project
 - The Trials
 - The Architecture
- ABC4Trust & Health Telematics
- 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

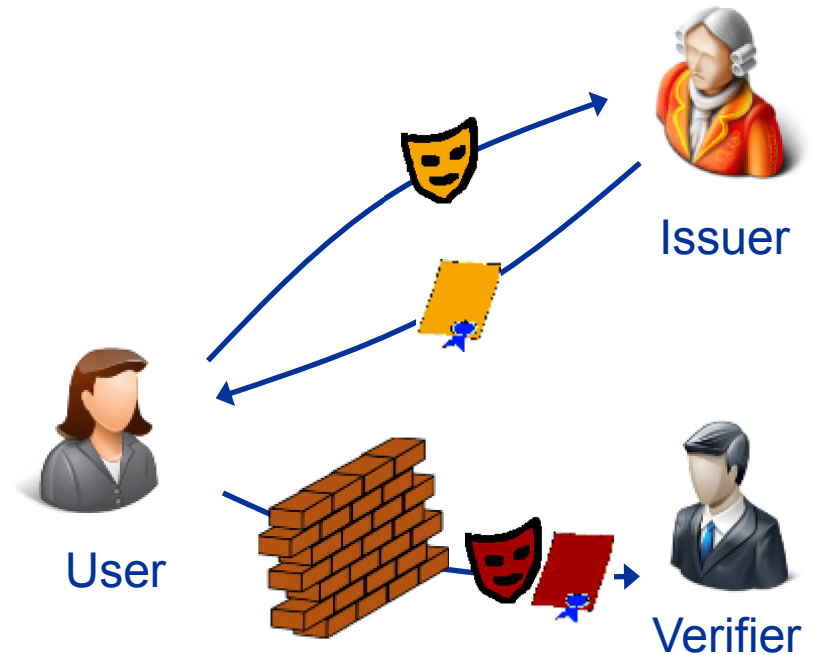
Blind Signatures



U-Prove

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

Zero-Knowledge Proofs



Idemix (Identity Mixer)

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

Agenda

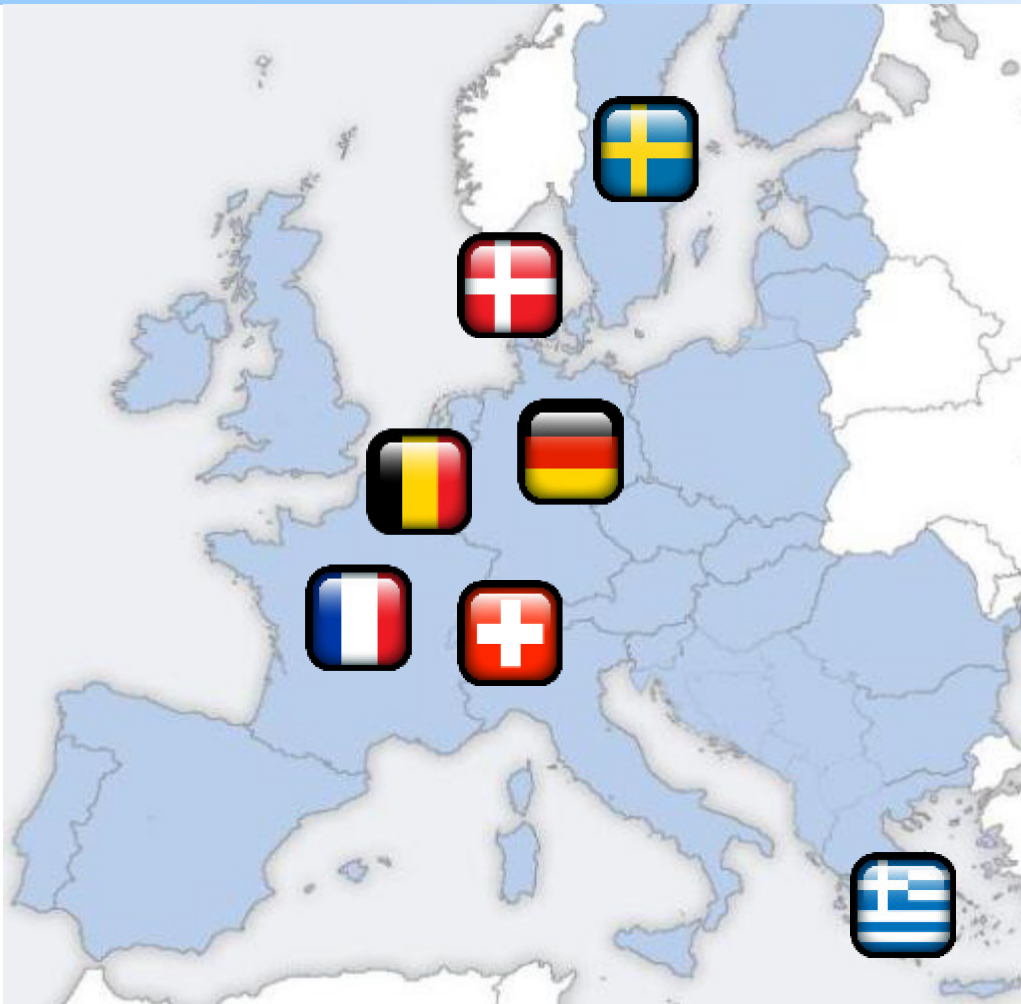
- Identity Management
- Some Privacy Problems in Identity Management and Assurance
 - Identity Management and Overidentification
 - Identity Assurance and the “Calling Home” Problem
- Attribute Based Credentials
- The ABC4Trust Project
 - The Trials
 - The Architecture
- ABC4Trust & Health Telematics
- 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”



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

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
- ABC4Trust & Health Telematics
- 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 Pilot Trial: Community Interaction



Norrtullskolan School
Söderhamn, Sweden

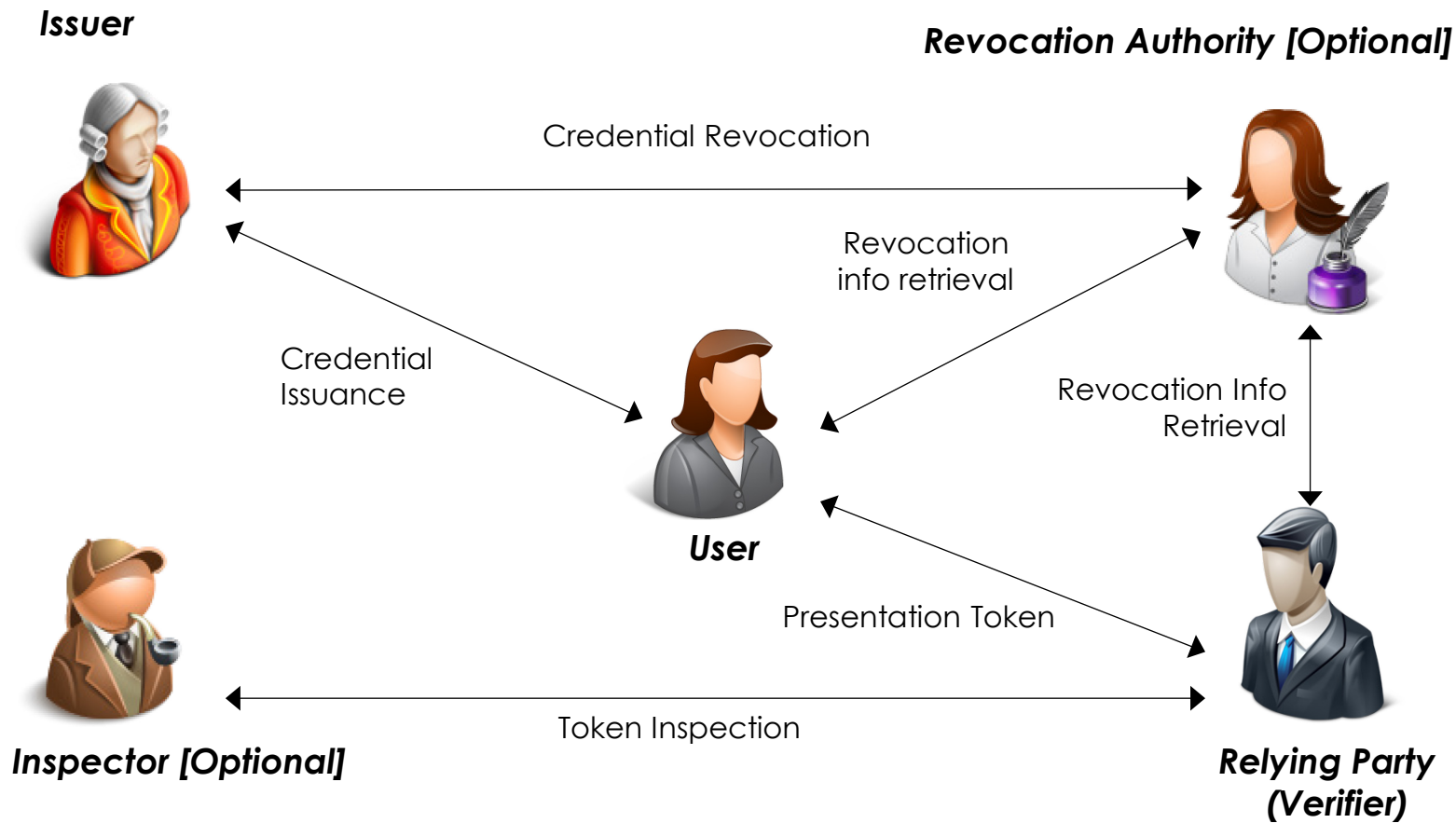
- School internal social network for communication among pupils, teachers, and personnel
- Provide trusted authentication while protecting pseudonymity/anonymity
- Usability: make privacy technology usable for non-technical users (e.g. pupils)

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
- ABC4Trust & Health Telematics
- 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**

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
- ABC4Trust & Health Telematics
- Concluding Remarks

ABC4Trust & Health Telematics

- Health data are often especially sensitive:
 - Health discussions can endanger careers
 - Too much information in the hand of an insurer may lead to disadvantages for individuals, e.g. higher fees.
- Even healthcare meta data are sensitive:
 - Participation in a virtual discussion group for parents of children with specific problems (psychological problems, drug abuse) ...
- **ABC assure specific attributes, but avoid overidentification**

Application scenarios for ABCs in Healthcare

- Anonymous or pseudonymous usage of self-care or discussion groups sharing experiences
 - Living with a family member abusing drugs
 - Experiences with medical or nursing services
 - Doctors reporting and discussing maltreatment and how to avoid it in future
- Pseudonymous signing of documents in patient records
 - To avoid quantitative pseudo-analysis of doctor's performances
- Certified attributes in patient records
 - To avoid overidentification towards experts, that are analysing single cases or groups of cases

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
- ABC4Trust & Health Telematics
- Concluding Remarks

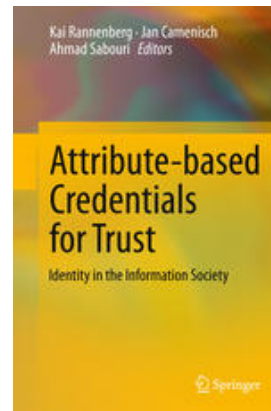
Benefits from ABC4Trust

- 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, ...)
- ISO/IEC (DIN) Standardisation can deal with complex requirements.

- 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

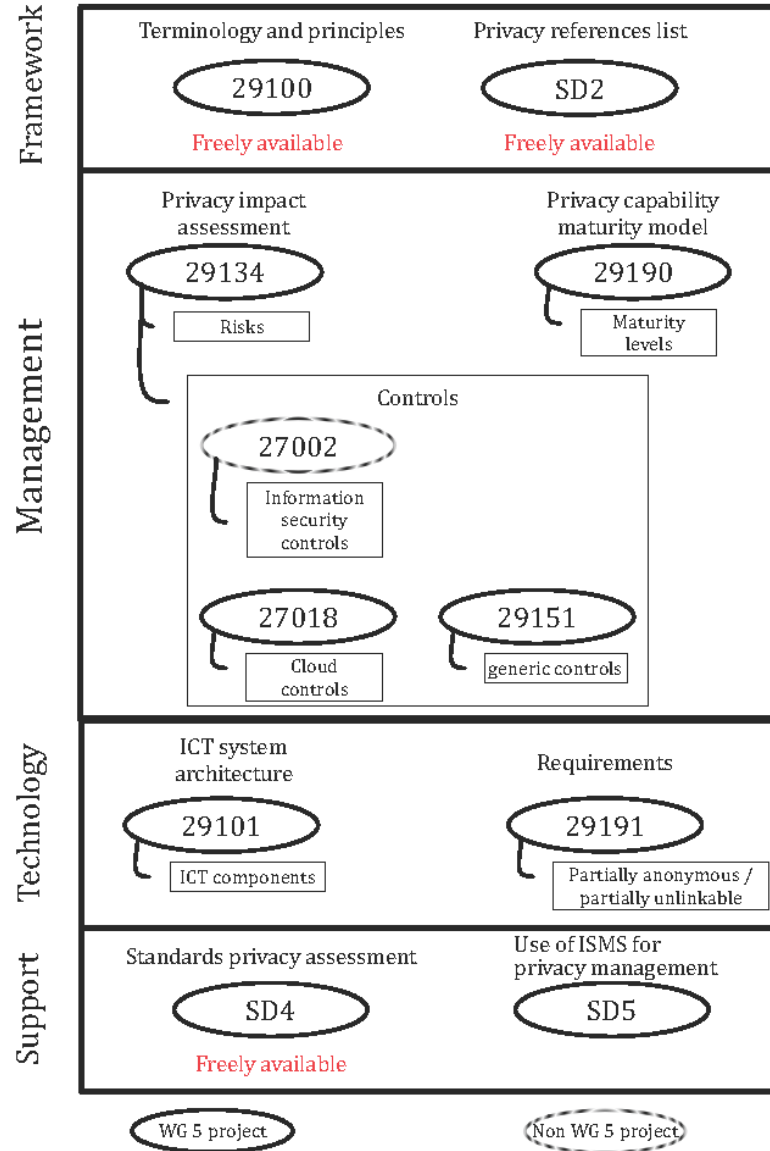




WG 5 Identity Management & Privacy Technologies

Privacy/PII standards in SC 27/WG 5 and elsewhere

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





WG 5 Identity Management & Privacy Technologies Further Reading

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

- www.jtc1sc27.din.de/en
 - SD6 Glossary of IT Security Terminology
 - SD7 Catalogue of SC 27 Standards & Projects
 - WG 5/SD2 Privacy Documents References List
- www.iso.org/obp/ui
 - ISO Online Browsing Platform (OBP)
- <http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html>
 - Freely available standards, e.g. ISO/IEC 24760-1:2011 “A framework for identity management -- Part 1: Terminology and concepts”

Kai.Rannenberga@m-chair.de

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

Crypto Architecture

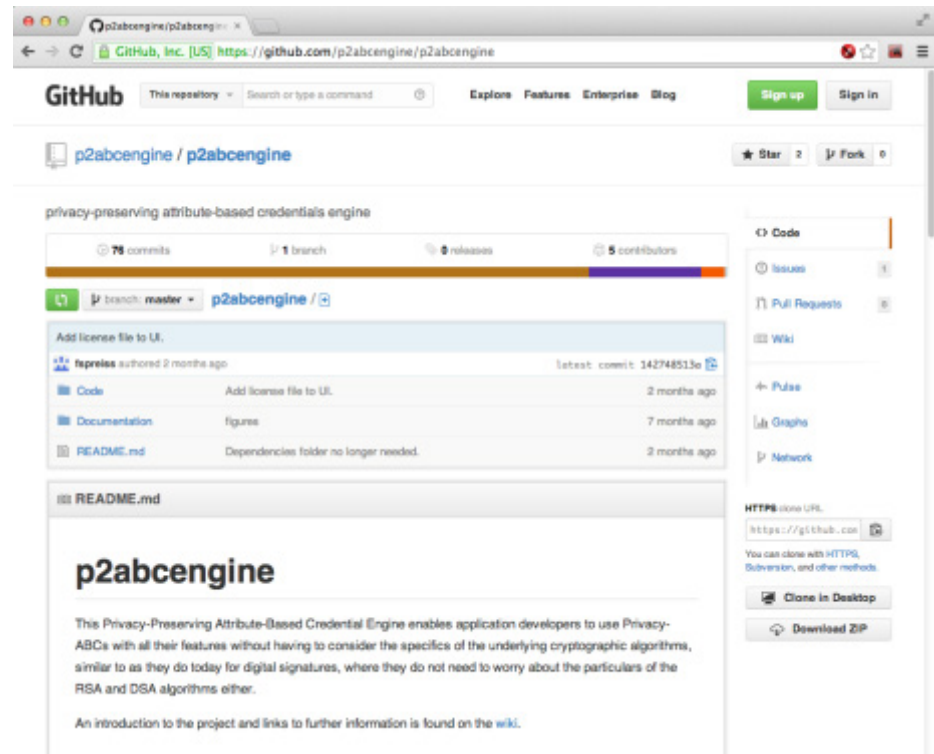
- Provide a truly plug-and-play architecture that allows the seamless integration of cryptographic primitives e.g.:
 - Privacy-ABC signatures: Idemix and Uprove
 - Predicate Proofs
- Move away from the "bridging" approach between several incompatible crypto engines
- Encapsulated in components with common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

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