Privacy-respecting Identity Management

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
  - Open Source Reference Implementation
  - ABC4Trust in Perspective
- Conclusions & Outlook
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
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]
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

Legend:
- Identity of Alice
- Partial Identity of Alice

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.
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
Privacy (and security) issues of typical federated IdM architectures

Identity Service Provider (IdSP)

1. request
2. policy
3. token
4. token
5. token

Relying Party (RP)

1. request access
2. policy
5. token

User

IdSP usually learns about RP via token request.

IdSP learns time of access & attributes requested.

RP gets to know values of the tokens and thus too much of the user’s identity.
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
Identity Management and Overidentification

Identity Service Provider (IdSP)

Relying Party (RP)

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

1. request
2. policy
3. token request
4. token response
5. token

User
Partial Identities needed

Legend:
- Identity of Alice
- Partial Identity of Alice

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 (DIS)
    - Part 3: Practice (CD)

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
The “Calling Home” Problem

Identity Service Provider (IdSP)

1. Identity Service Provider (IdSP) usually learns about the Relying Party (RP) via a token request.
2. IdSP learns the time of access and attributes requested.

Relying Party (RP)

1. request access
2. policy
3. token request
4. token response
5. token

User

trust
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
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
    - Open Source Reference Implementation
    - ABC4Trust in Perspective
- Conclusions & Outlook
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 ABC systems
- Open reference implementations of selected ABC systems
- Deployments in actual production enabling
  - Minimal disclosure
  - Provision of 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
  - Open Source Reference Implementation
  - ABC4Trust in Perspective
- Conclusions & Outlook
ABC4Trust Pilot Trial: Course Rating

- 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

Computer Technology Institute & Press – “Diophantus” Patras, Greece
ABC4Trust Pilot Trial: Community Interaction

- 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)

Norrtullskolan School
Söderhamn, Sweden
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
The ABC4Trust Architecture

Objectives

- Abstraction of concepts of Privacy-ABCs & unification of features
- A common unified architecture
  - That is independent of the specific technologies
  - Federation of Privacy-ABC Systems based on different technologies
  - Interoperability between different Privacy-ABC technologies

- Avoid technology lock-in
- Raise trust in Privacy-ABC technologies

- 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.
ABC4Trust Architecture
High Level View

Issuer

Credential Issuance

Credential Revocation

Revocation Authority [Optional]

Revocation info retrieval

Revocation Info Retrieval

User

Presentation Token

Token Inspection

Inspector [Optional]

Relying Party (Verifier)
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)
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
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, …)

- 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
Announcement

• ABC4Trust Summit Event
  - January 20th, 2015
  - Venue: The Representation of the German federal state of Hessen in Brussels, 21 rue Montoyer.
  - The date conveniently allows interested privacy experts to attend the Summit Event in connection with their travel to attend the Computers, Privacy and Data Protection Conference 2015 (CPDP)