Privacy-ABCs
Features and Architecture

Ahmad Sabouri (ahmad.sabouri@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
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

• 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

• How do we achieve this?
  ▪ System Architecture and components for handling privacy-ABCs
  ▪ Unified and technology agnostic APIs
  ▪ XML specification of all data formats, covering the full life-cycle of credentials
Goal of the Presentation

• We aim to:
  
  ▪ give an impression of the features and concepts of the Privacy-ABCs to all the audiences.
  
  ▪ introduce the architecture, processes, and the artifacts to application and infrastructure developers.
Example Scenario

Name: Alice
Birthdate: 02.05.1986

Identity Service Provider
requirement = Name?
untraceable

Service Provider #1
requirement = Name?
unlinkable

Service Provider #2
requirement = Age > 18

User
Birthdate < 02.09.1996
Features Privacy-ABCs

• Credential issuance

  ▪ list of pairs (attribute, value)
  ▪ certified by issuer
  ▪ key-bound to prevent sharing credentials
  ▪ advanced issuance:
    • blindly issued attributes
    • carried-over attributes (e.g. transfer an identifier to a tombola credential)
Features Privacy-ABCs (2)

• Presentation
  ▪ selected attributes from selected credentials
  ▪ predicates over attributes
    • \( \text{attribute1} =,>,< \text{attribute2} \text{ or constant} \)

• Pseudonyms
  ▪ equivalent to unlinkable public keys for user’s secret key
  ▪ controlled linkability (e.g., account creation)
  ▪ scope-exclusive pseudonym: unique per scope, unlinkable across different scopes
• Inspection
  - attribute value encrypted to trusted Inspector
  - token bound to inspection grounds: conditions to decrypt
  - e.g., de-anonymization in case of abuse

• Revocation
  - credentials’ validity
  - e.g., credential compromise, changed attributes
Interactions and Entities

- **Issuer**
- **User**
- **Verifier**
- **Inspector**

**Credential Issuance**

**Revocation Authority**

**Revocation Info Retrieval**

**Token Presentation**

**Token Inspection**

**Credential Revocation**
High-level view (user)

- Technology-agnostic credential & policy handling
- Unified and technology-independent APIs

 Diagram:

- **ABCE** (Attribute-based Credentials Engine)
- Crypto Engine (e.g. Idemix, U-Prove)
- KeyManager
- Revocation Proxy
- Ext. Device Interface
- Identity Selector
- Browser/Application
High-level view (presentation)

Language framework covering the full life-cycle of credentials and support all concepts.

User Side Deployment:
- User
- Identity Selector
- Policy-Credential Matcher
- Evidence Generation Orchestration
- Credential Manager
- Crypto Engine (e.g. Idemix, U-Prove)

Verifier Side Deployment:
- Verifier
- Policy-Token Matcher
- Evidence Verification Orchestration
- Token Manager
- Crypto Engine (e.g. Idemix, U-Prove)

Request resource via presentation policy, then presentation token.
<?xml version="1.0" encoding="UTF-8"?>

<presentationPolicy xmlns:schema="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xml="http://www.w3.org/2001/XMLSchema"
xmlns:xenc="http://www.w3.org/2001/XMLSchema"
xmlns:xs="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:urn="urn:oasis:names:tc:xacml:1.0:assertion:binding">
  <presentationPolicyPolicyUID="policy1" EnforceSameUserBinding="true" EnforceSameDeviceBinding="false">
    <message>
      <Nonce>aDk3UEm2OTNj0T1cmZH210U0c==</Nonce>
    </message>
    <credential Alias="id">
      <credentialSpecAlternatives>
        <credentialSpecUID>urn:sweden:id</credentialSpecUID>
      </credentialSpecAlternatives>
      <issuerAlternatives>
        <IssuerParametersUID>urn:sweden:id:issuer</IssuerParametersUID>
      </IssuerAlternatives>
      <disclosedAttribute AttributeType="urn:sweden:id:city"/>
    </credential>
    <attributePredicate Function="urn:oasis:names:tc:xacml:1.0:assertion:binding:date-less-than">
      <attribute CredentialAlias="id" AttributeType="urn:sweden:id:birthdate">
        <constantValue>1994-01-20</constantValue>
      </attribute>
    </attributePredicate>
  </presentationPolicyPolicy>
</presentationPolicyPolicyAlternatives>
ABC4Trust Crypto Architecture (1)
ABC4Trust Crypto Architecture (2)
In the architecture WP, we produced a set of benchmarking criteria allowing comparison of different Privacy-ABC technologies based on:

1. **Efficiency**
   - Theoretical vs. practical
   - Computational vs. communication vs. storage

2. **Functionality**: The supported functionalities, privacy features, and other practical considerations/implications

3. **Security**:
   - Security assumptions: (i) *information theoretic*, (ii) *computational* or (iii) *without security reduction/proof*.
   - Mechanisms in place to fulfill different security requirements

4. **Legal**: Legal criteria regarding user’s privacy, and requirements for the other entities

5. **Economic viability**: Key issues that impact the economical value of a choice of a certain combination of technologies
Summary

- ABC4Trust produced a generic and layered architecture for Privacy-ABCs:
  - Defining features, processes, and artifacts
  - Enabling the Reference Implementation and the Pilots
  - Preventing lock-in situations

- The architecture is more privacy-friendly than the available alternatives, e.g. STORK, which is important for the eIDAS discussion.

- The ABC4Trust Crypto Architecture enables modular instantiation of new Privacy-ABC technologies.
Questions?

Thanks for Your Attention

coord-abc4trust@m-chair.de