Privacy-ABCs
Features and Architecture

Attribute-based Credentials for Trust

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
SEVENTH FRAMEWORK PROGRAMME

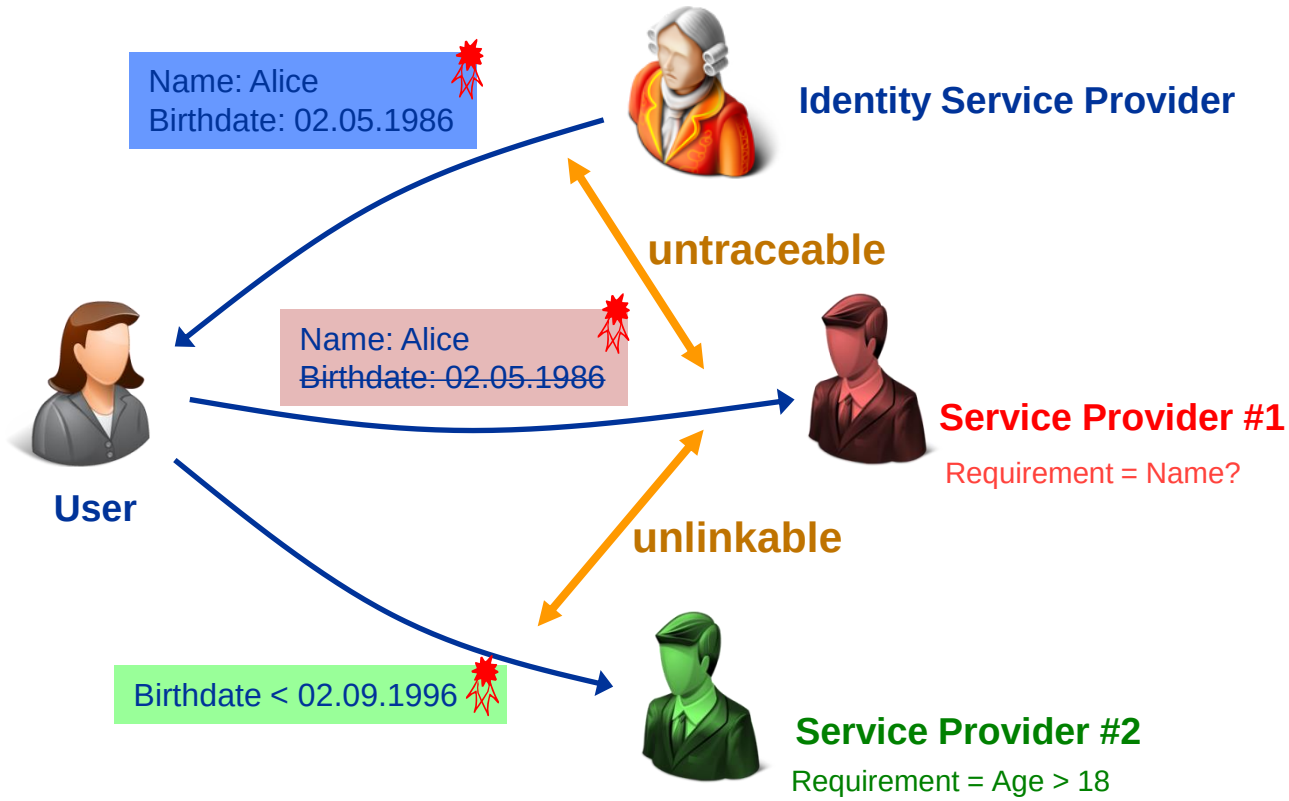
The ABC4Trust Architecture Objectives

- 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



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)

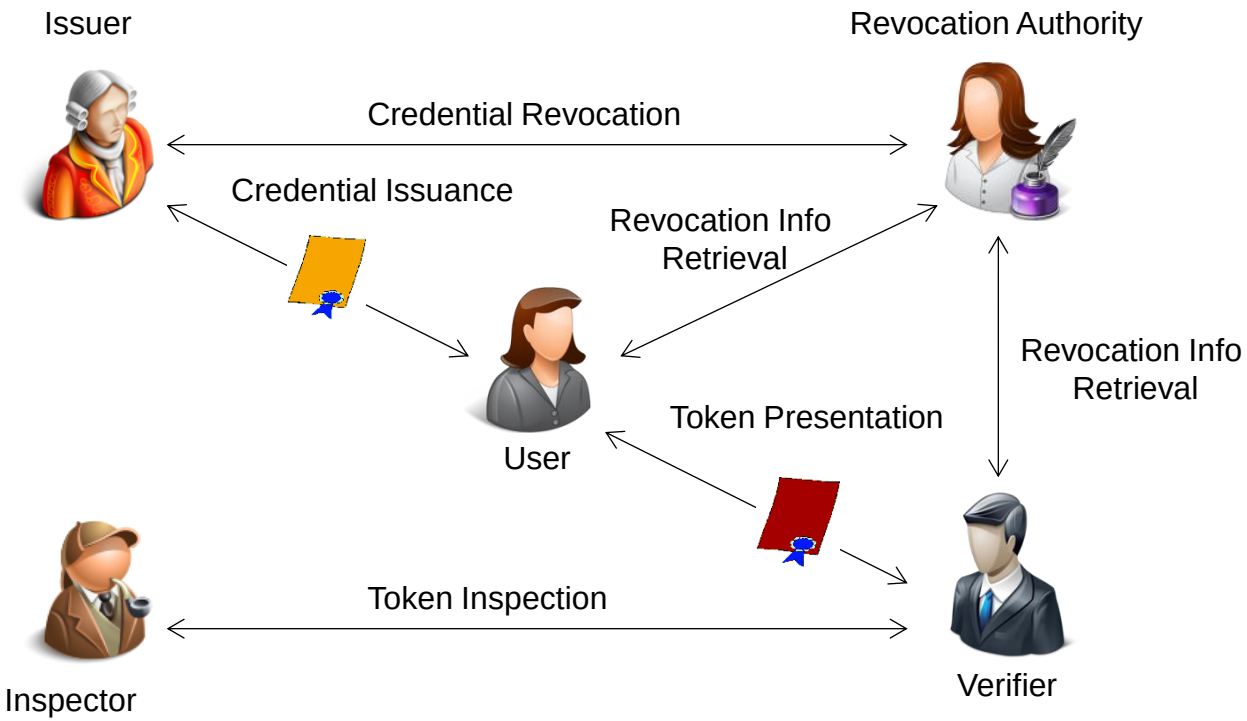
Features Privacy-ABCs (2)

- Presentation
  - selected attributes from selected credentials
  - predicates over attributes
    - attribute1 =,>,< attribute2 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

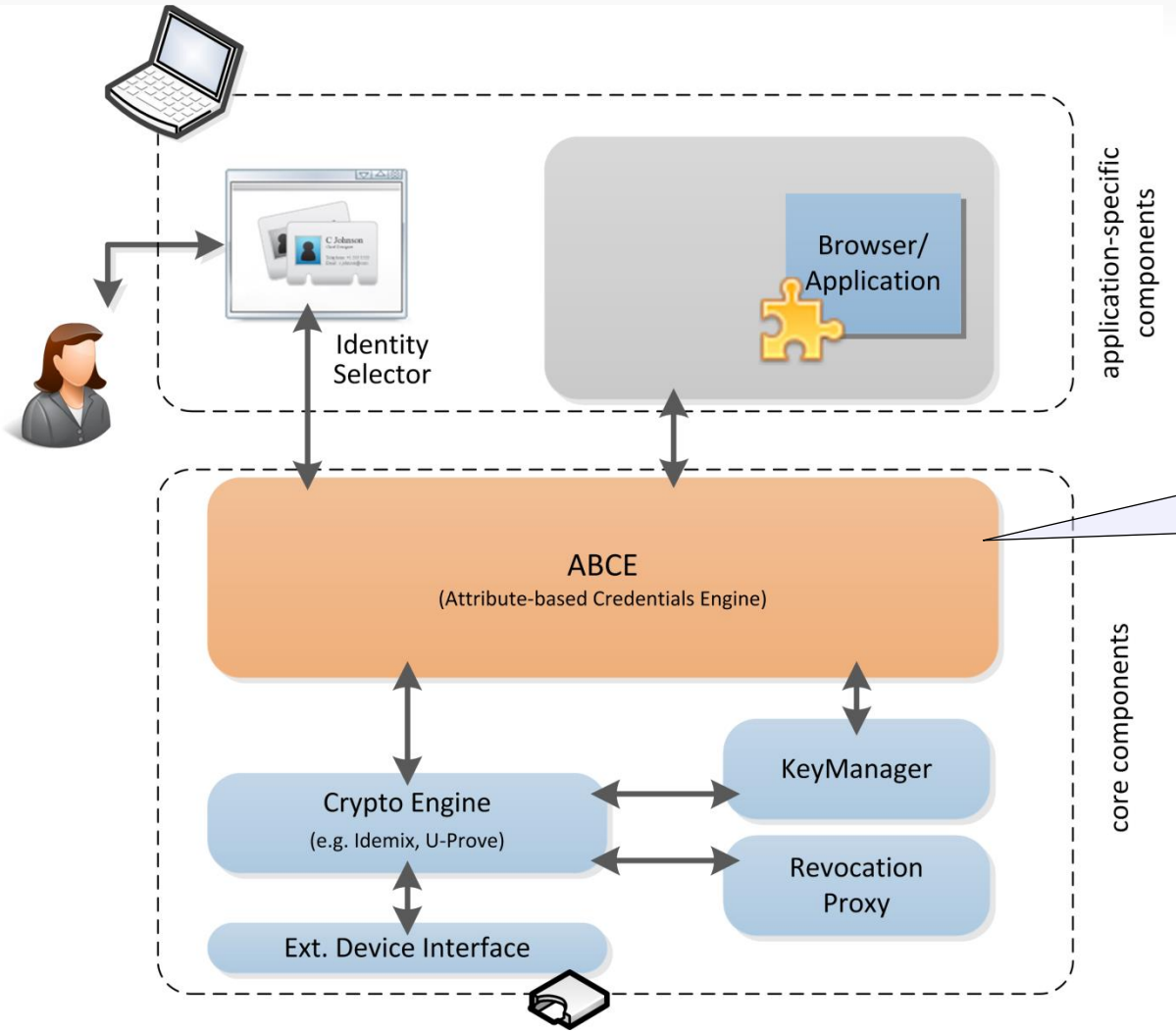
Features Privacy-ABCs (3)

- 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

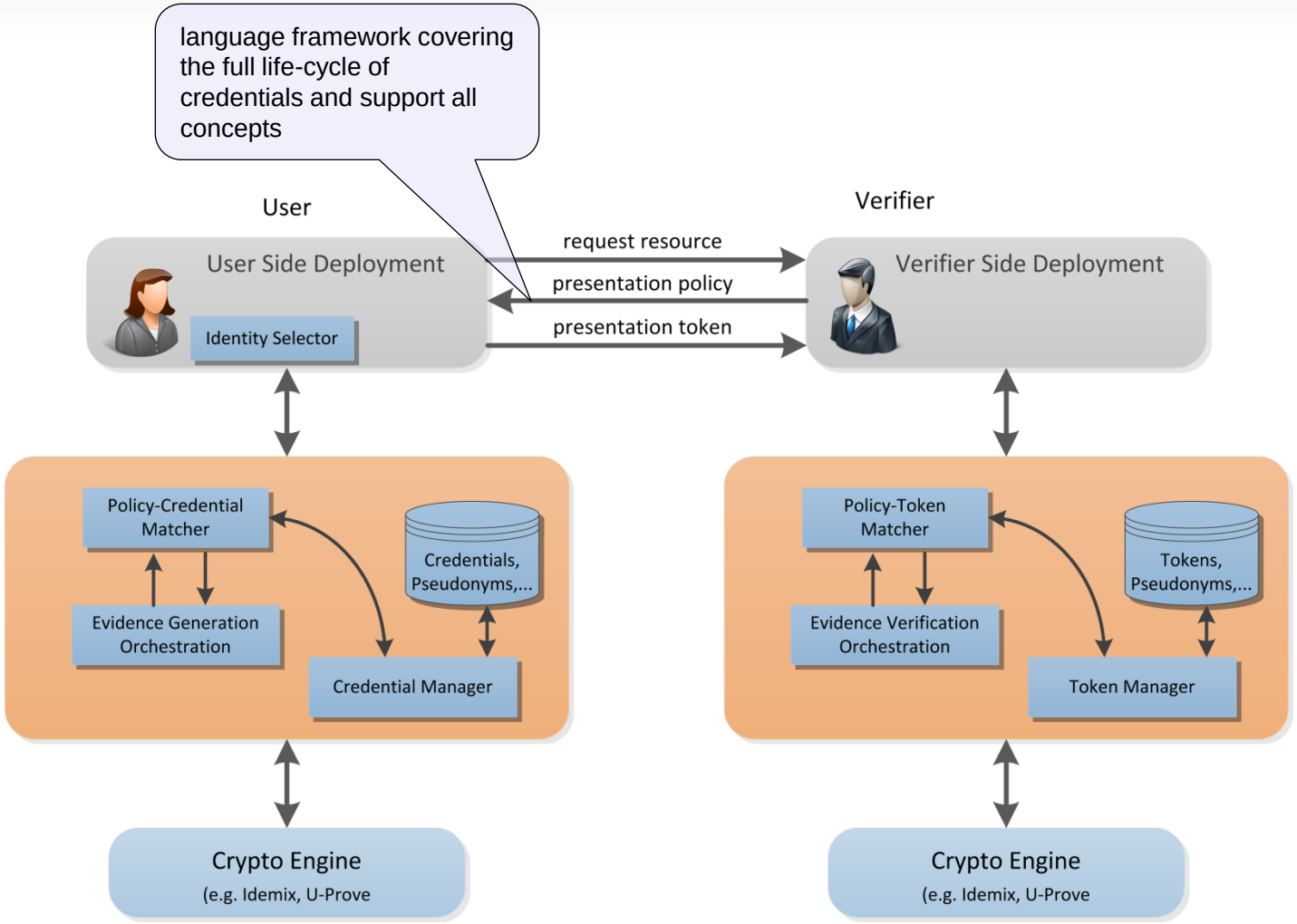


High-level view (user)



- technology-agnostic credential & policy handling
- unified and technology-independent APIs

High-level view (presentation)



Presentation Policy

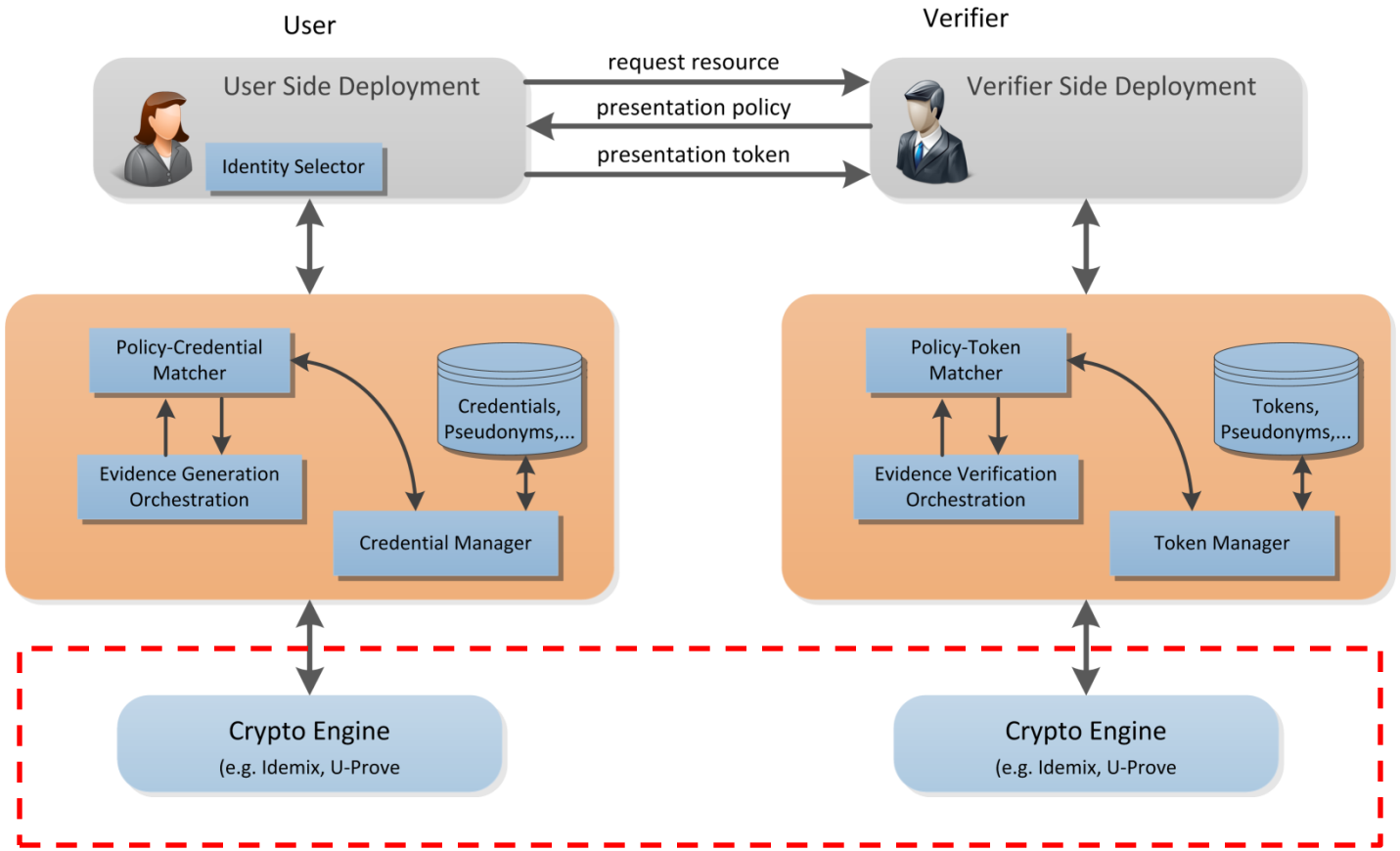
```xml
<?xml version="1.0" encoding="UTF-8"?>

<PresentationPolicyAlternatives xmlns="http://abc4trust.eu/wp2/abcschemav1.0"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:xenc="http://www.w3.org/2001/04/xmlenc"
    xsi:schemaLocation="http://abc4trust.eu/wp2/abcschemav1.0 schema.xsd"
    Version="1.0">
<PresentationPolicy PolicyUID="policy1" EnforceSameUserBinding="true" EnforceSameDeviceBinding="false">

    <Message>
        <Nonce>aDk3UEMzOTNjOTl1cmZHQ210U0c=</Nonce>
    </Message>
    <Pseudonym Alias="nym" Scope="http://sweden.gov/poll0105" Exclusive="true"/>
    <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:function:date-less-than">
        <Attribute CredentialAlias="id" AttributeType="urn:sweden:id:bdate"/>
        <ConstantValue>1994-01-20</ConstantValue>
    </AttributePredicate>

</PresentationPolicy>
</PresentationPolicyAlternatives>
```

ABC4Trust Crypto Architecture (1)



ABC4Trust Crypto Architecture (2)

Benchmarking Criteria

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