Architecture for Privacy-ABCs

Ioannis Krontiris
Goethe University Frankfurt

1st Reference Group Meeting
2012-02-13
Rüschlikon, Switzerland

ABC4TRUST
A research project funded by the European Commission's 7th Framework Programme.
SEVENTH FRAMEWORK PROGRAMME

Overview

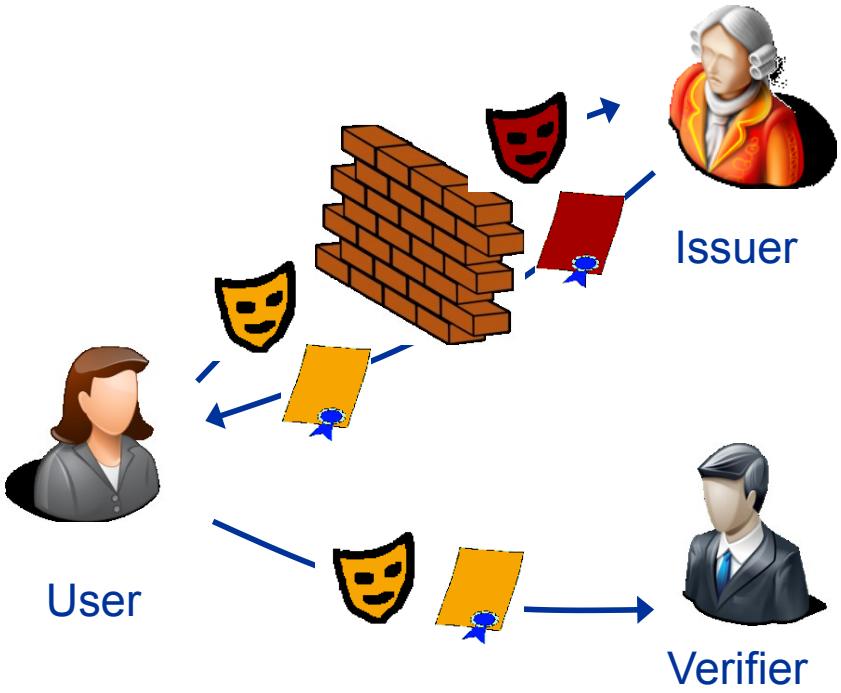
- WP2 Objectives
- Architecture
  - Roles
  - Design Approach
  - Components and their interaction
  - Protocol message flow
  - Data formats
- Future work

Key Messages

- High-level features and concepts of privacy-ABCs defined
- XML specification of all data formats defined
- System Architecture and components for handling privacy-ABCs defined
- Component APIs defined
- Reference implementation started

Two approaches for privacy-ABCs

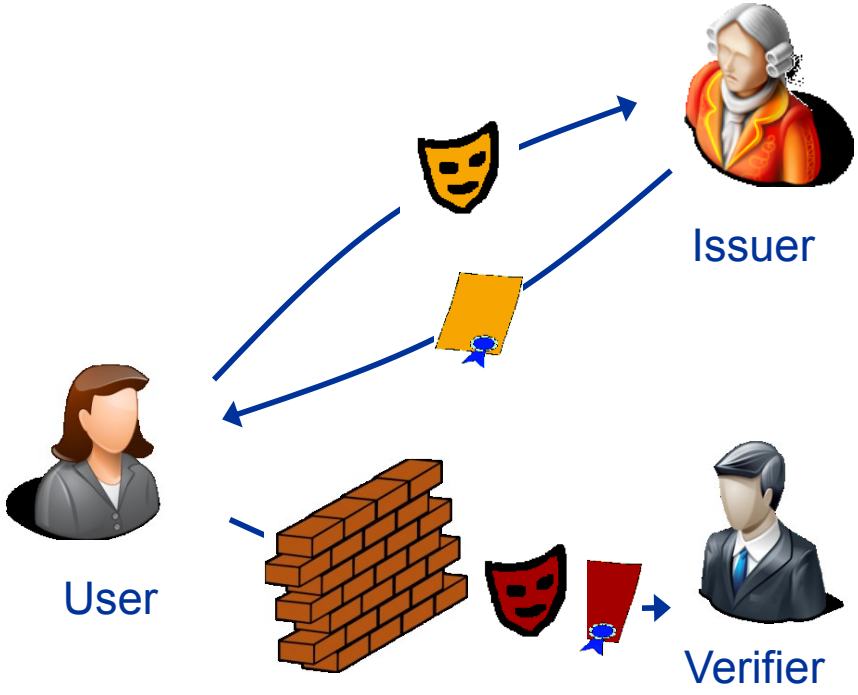
Blind Signatures



U-Prove

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

Zero-Knowledge Proofs



Idemix (Identity Mixer)

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

Different concepts, terminology, interfaces

WP2 Objectives

- Abstraction of concepts of privacy-ABCs & unification of features

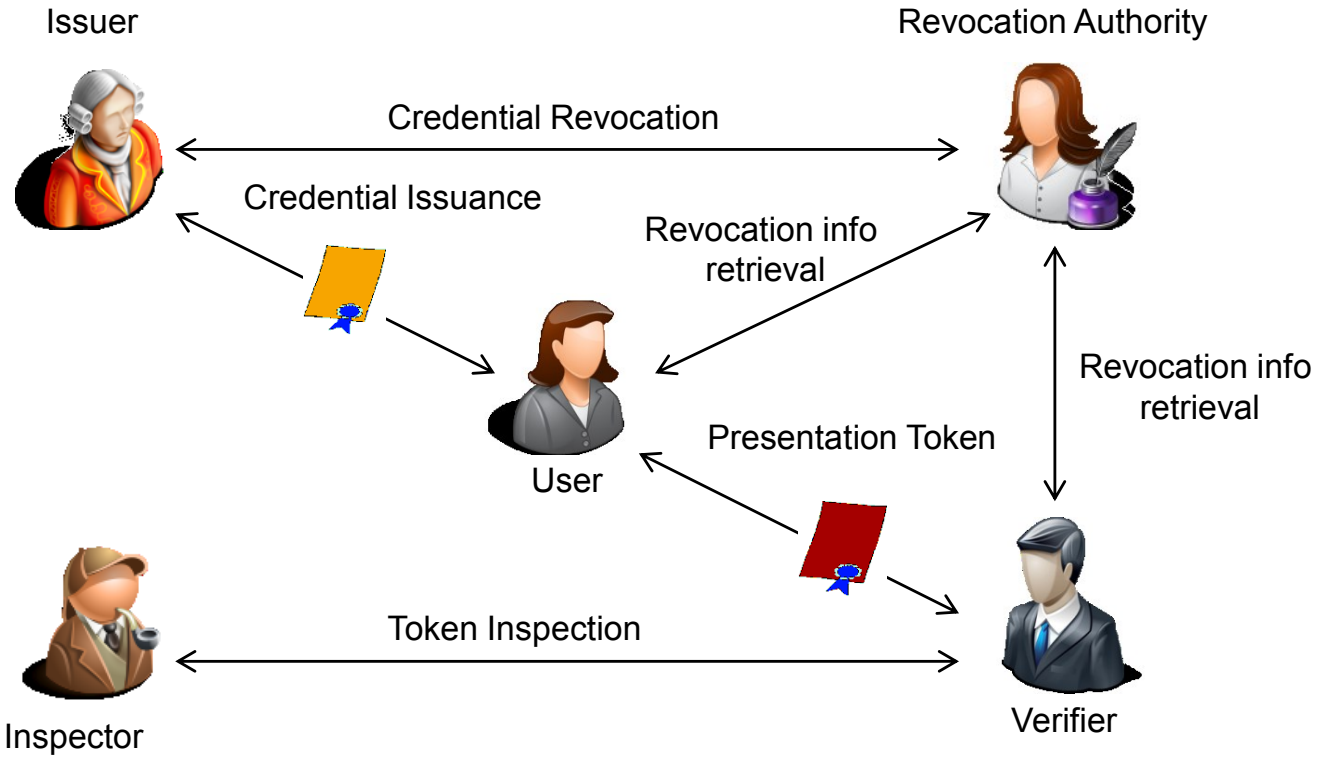
- A common unified architecture
  - That is independent of the specific technologies
  - Federation of privacy-ABC Systems based on different technologies
  - Interoperability between different privacy-ABC technologies

➢ 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.

Interactions and Entities

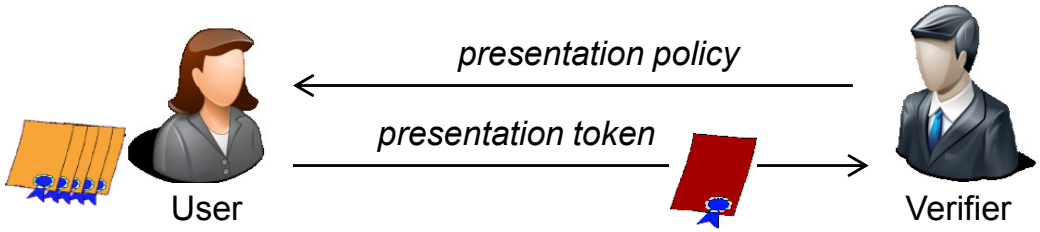


Defined Concepts

- Credentials
  - List of attributes, encoding, etc.

- User binding and device binding
- Issuance policies
- Pseudonyms
  - Verifiable, certified, scope-exclusive
- Inspection + Revocation

Presentation



- Presentation Policy
  - which (combination of) credentials from which issuer
  - which attributes or attribute predicates to reveal
- Presentation token
  - *description*: mechanism-agnostic revealed information
  - *evidence*: mechanism-specific crypto blobs
  - untraceable and unlinkable by default,
    traceable and linkable when so desired

Presentation Policy

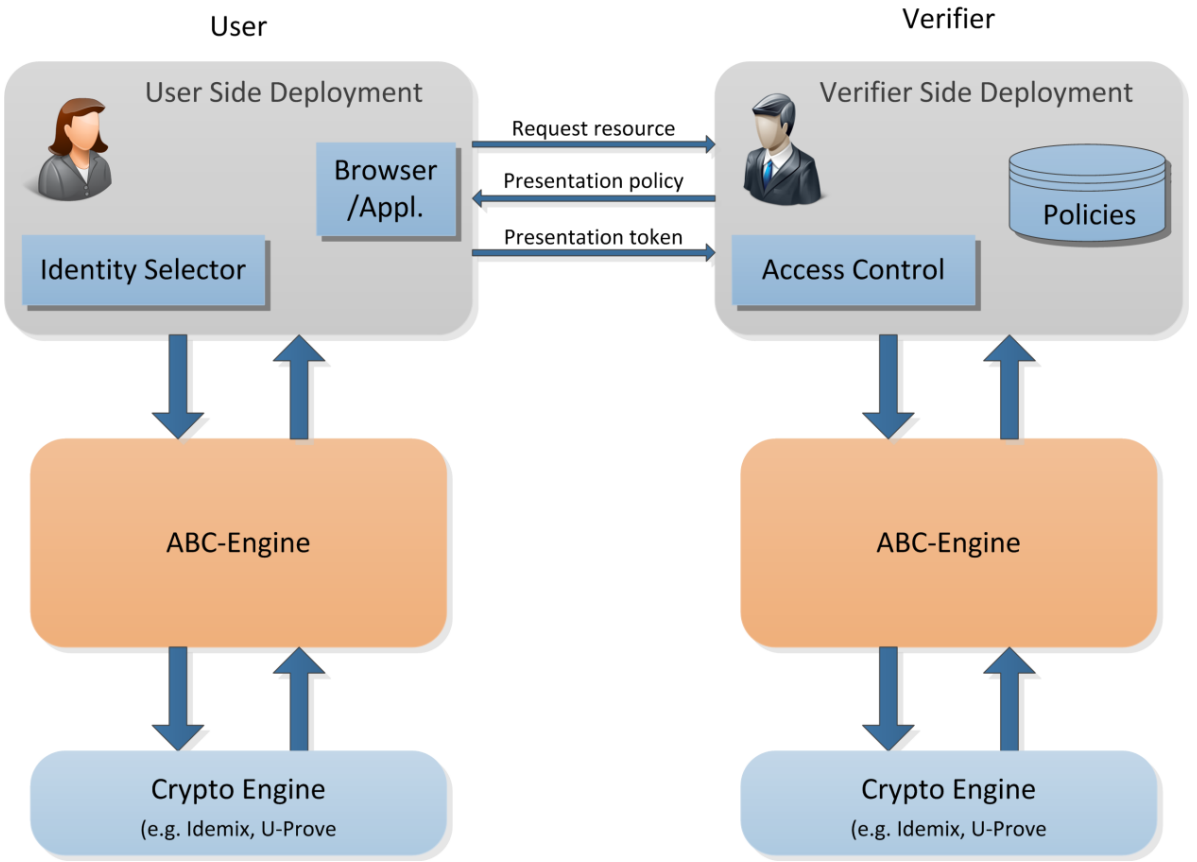
```
<?xml version="1.0" encoding="UTF-8"?>

<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>
```

Presentation Token

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

<PresentationToken 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">

    <PresentationTokenDescription PolicyUID="policy1" EnforceSameUserBinding="true"
EnforceSameDeviceBinding="false">
        <Message>
            <Nonce>aDk3UEMzOTNjOTl1cmZHQ210U0c=</Nonce>
        </Message>
        <Pseudonym Alias="nym" Scope="http://sweden.gov/poll0105" Exclusive="true">
            <PseudonymValue>MER2VXpyR0VaOW51YXdVNHRISHI=</PseudonymValue>
        </Pseudonym>
        <Credential Alias="id">
            <CredentialSpecUID>urn:sweden:id</CredentialSpecUID>
            <IssuerParametersUID>urn:sweden:id:issuer</IssuerParametersUID>
            <DisclosedAttribute AttributeType="urn:sweden:id:city">
                <AttributeValue>          </AttributeValue>
            </DisclosedAttribute>
        </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>
    </PresentationTokenDescription>

    <CryptoEvidence> ... </CryptoEvidence>

</PresentationToken>
```

High-level view of Architecture

- Contains all mechanism-agnostic components of Privacy-ABC systems

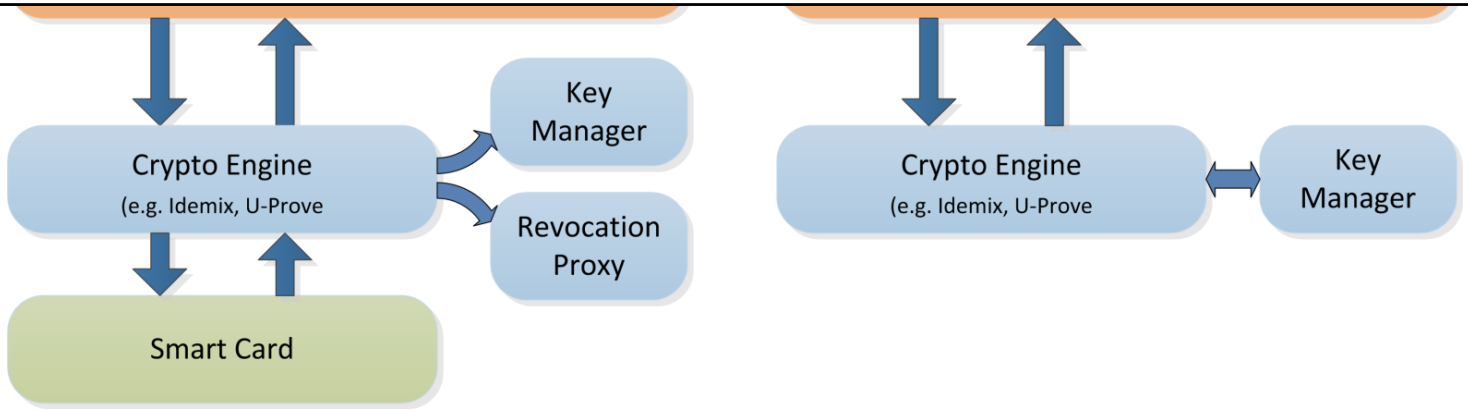


ABCE Components - Presentation

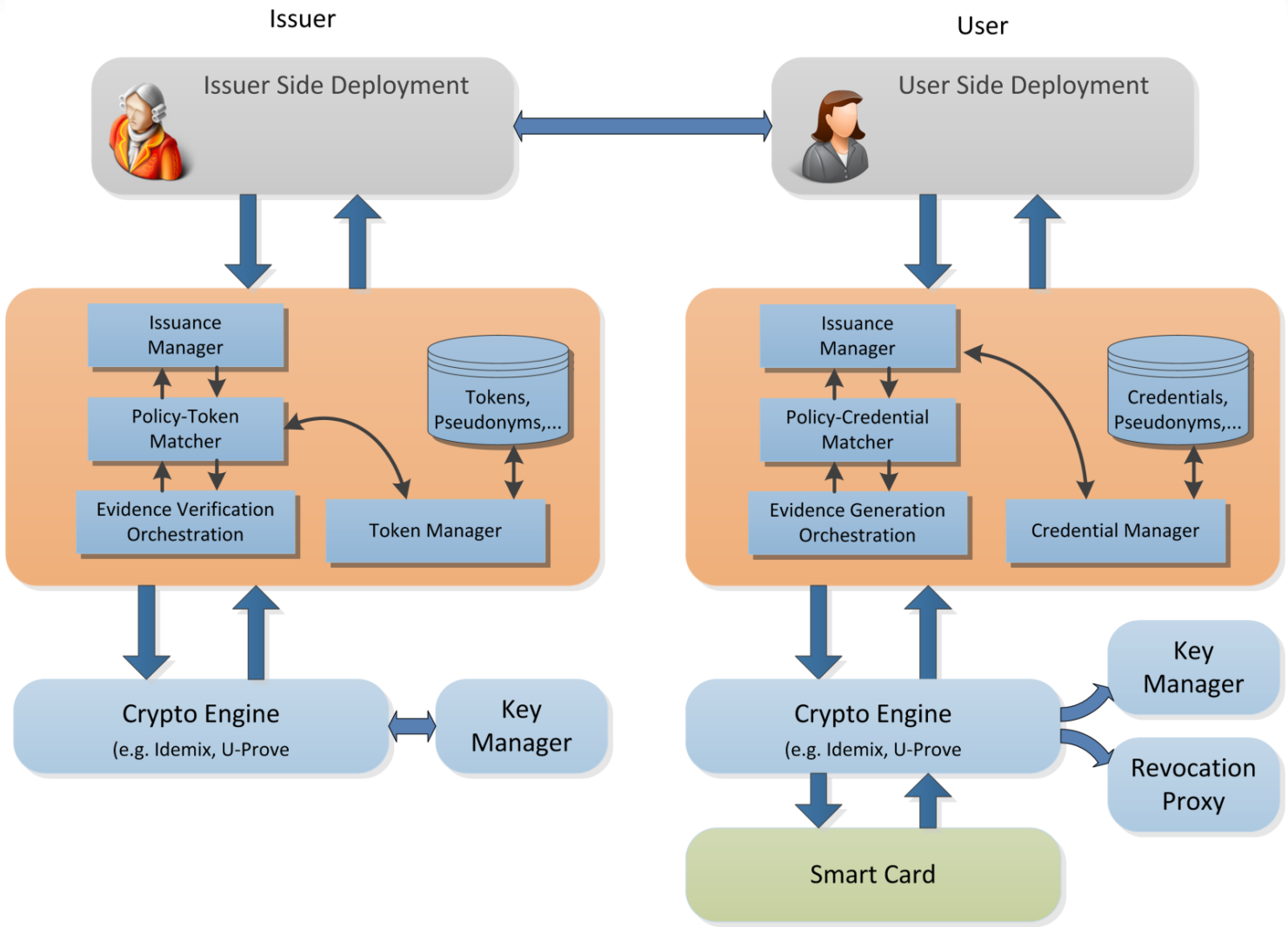
User

Verifier

- `canBeSatisfied(p:PresentationPolicyAlternatives) → boolean`
- `createPresentationToken(p:PresentationPolicyAlternatives) → PresentationToken`
- `createIssuanceToken(m:IssuanceMessage, atts:Attribute[]) → IssuanceMessage`
- `issuanceProtocolStep(m:IssuanceMessage) → IssuanceMessage or CredentialDescription`
- `updateNonRevocationEvidence()`
- `listCredentials()→ anyURI[]`
- `getCredentialDescription(creduid:anyURI) → CredentialDescription`
- `deleteCredential(creduid:anyURI) → boolean`



ABCE Components - Issuance



Looking ahead

- D2.1: Architecture for Attribute-based Credential Technologies – Version 1 (Nov. 2011)
- D2.2: Architecture for Attribute-based Credential Technologies – Version 2 (Jan. 2014)
- D2.3: Benchmarking criteria (Nov. 2013)

- [D8.4: Architecture for Standardization (Feb. 2012)]
- Architecture - Version 2
  - Advanced features to be supported (limited spending, inspection of proofs)
  - Extend the XML schema
  - Architecture of Crypto Engine
  - Incorporate feedback from Pilots

Key Messages

- ✓ High-level features and concepts of privacy-ABCs defined
- ✓ XML specification of all data formats defined
- ✓ System Architecture and components for handling privacy-ABCs defined
- ✓ Component APIs defined
- ✓ Reference implementation started

Thank you!

Legal considerations

Limiting processing to necessary data is supported by Privacy- ABCs with:

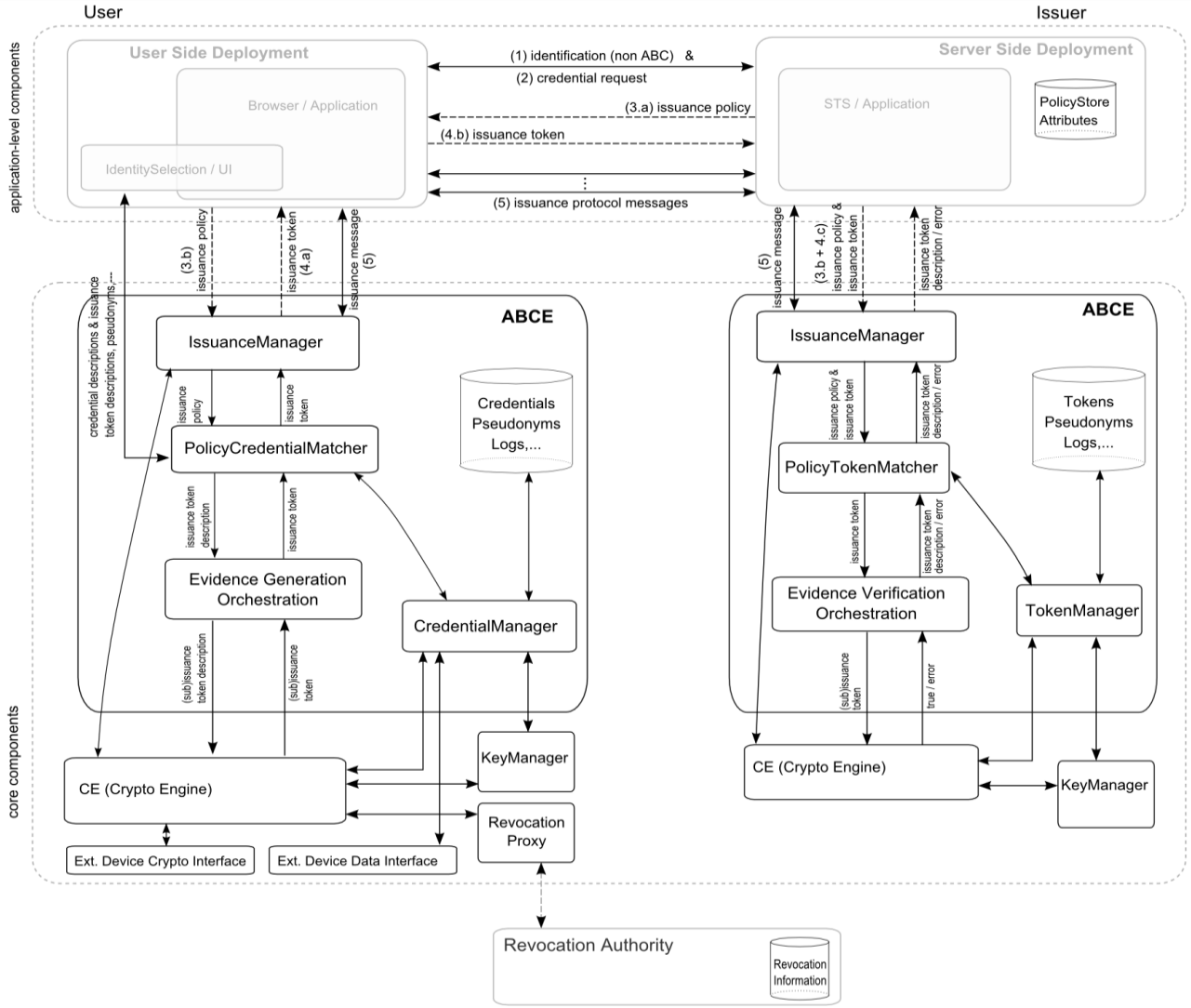
- **Selective disclosure** of attribute-values out of a certificate and
- **Inspection** allowing conditional disclosure of data once this is really necessary.

D2.1 Legal considerations

Purpose binding is supported by Privacy-ABCs as

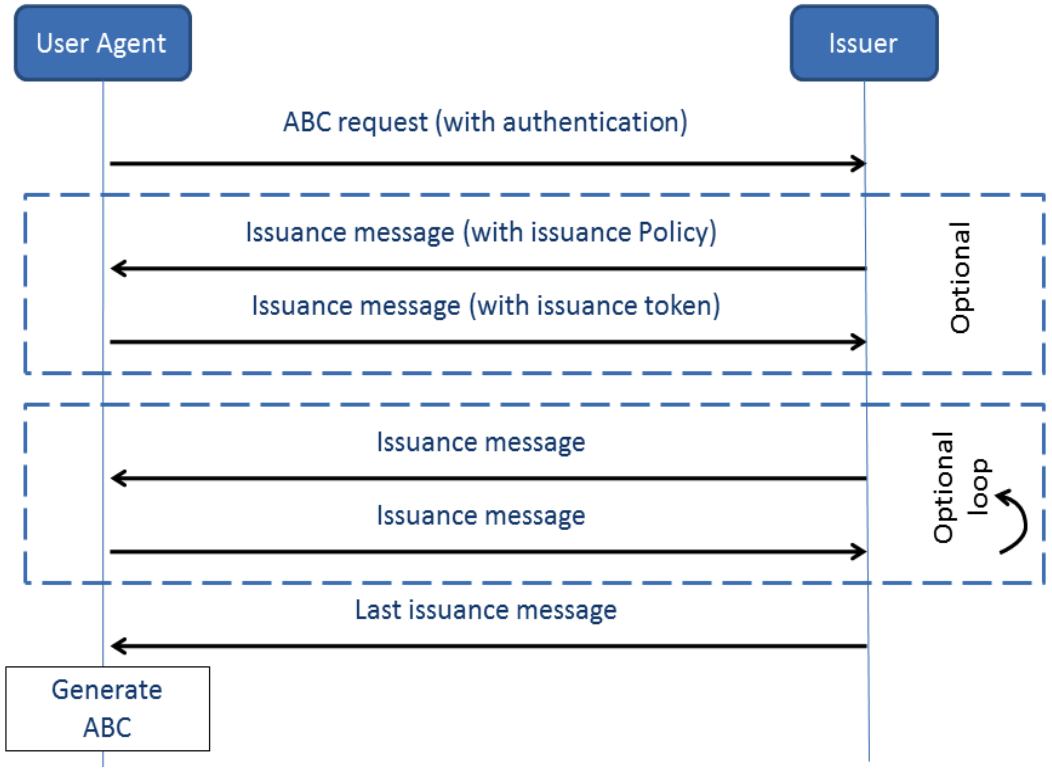
- Unlinkability between presentation tokens prevents mixing of purposes and profiling
- Unlinkability requires separate storage of tokens and related data for each incident

Zoom-in: Issuance



Protocol Message Flow

- E.g. Issuance



Stored and Exchanged Date formats

- Data formats in XML
  - Credential Specification
  - Parameters
  - Issuance/Presentation Policy
  - Issuance/Presentation Token
  - Messages
  - ….

```
<abc:CredentialSpecification Version="1.0" UserBinding="xs:boolean"
DeviceBinding="xs:boolean" Revocable="xs:boolean">
<abc:SpecificationUID>xs:anyURI</abc:SpecificationUID>
<abc:AttributeDescriptions MaxLength="xs:unsignedInt">
<abc:AttributeDescription Type="xs:anyURI"
DataType="xs:anyURI" Encoding="xs:anyURI"/>*
</abc:AttributeDescriptions>
</abc:CredentialSpecification>
```

WP2 Contribution

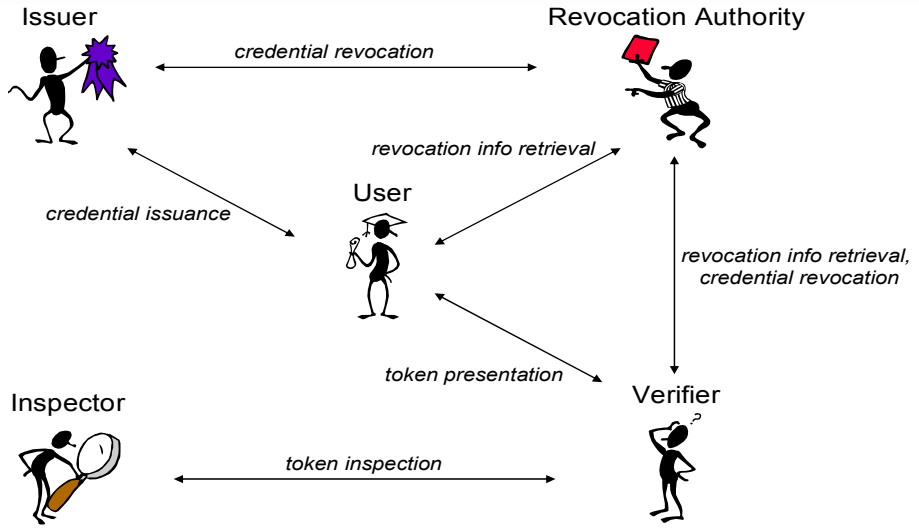
Building the architecture requires defining the

- Components in different layers
- Interfaces and APIs
  - External APIs
  - Internal Interfaces between the components
- Data formats
  - Credential formats
  - …
- Protocol Specification
  - Message formats
  - …

Interactions and Entities

There are 5 types of entities:

- User
- Issuer
- Verifier
- Revocation Authority
- Inspector



The entities can be involved in the followings steps:

- Setup
- Issuance
- Presentation
- Revocation
- Inspection