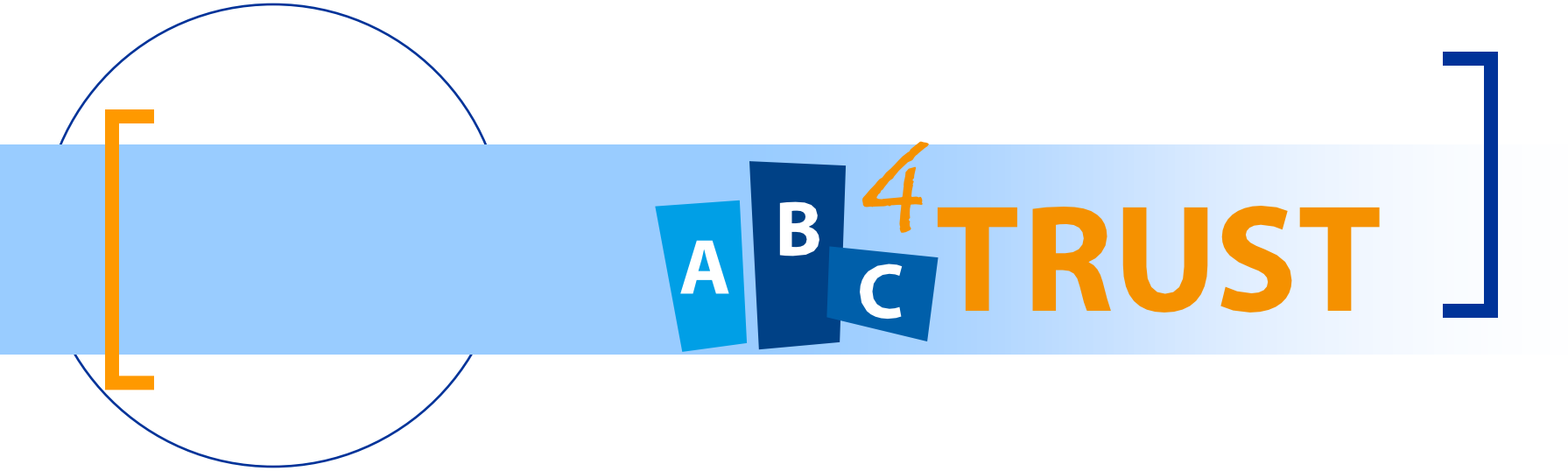


ABC4Trust XML Artefacts

Gregory Neven (IBM Research – Zurich)

ABC4Trust 1st Reference Group Meeting, Zurich, February 13, 2011

SEVENTH FRAMEWORK PROGRAMME

XML Artefacts in D2.1

Technology-agnostic XML schemas for “external” artefacts, including:

- Credential specification
- Issuer parameters
- Presentation policies
- Presentation tokens
- Issuance policies
- …

Söderhamn pilot

- High school pupils with access to “restricted zones”
  - Private document management
  - Anonymous discussion boards
  - Consulting by professionals

- Authorities can lift anonymity in case of emergency, e.g.,
  - Child abuse
  - Threats of violence

Use case: private documents

- Each pupil gets school credential containing
  - First and last name
  - Civic number (= birthdate + 4 digits)
  - Gender
  - School name

- Access private documents by revealing civic number

Credential specification

School credentials

```
1  <CredentialSpecification Version="1.0" KeyBinding="true" Revocable="true">
2
3      <SpecificationUID>http://abc4trust.eu/wp6/credspec/credSchool</SpecificationUID>
4
5      <AttributeDescriptions MaxLength="32">
6          <AttributeDescription Type="http://abc4trust.eu/wp6/credspec/credSchool/firstName"
            DataType="xs:string" Encoding="abc:sha256"/>
7          <AttributeDescription Type="http://abc4trust.eu/wp6/credspec/credSchool/lastName"
           DataType="xs:string" Encoding="abc:sha256"/>
8          <AttributeDescription Type="http://abc4trust.eu/wp6/credspec/credSchool/civicNr"
           DataType="xs:integer" Encoding="abc:plain"/>
9          <AttributeDescription Type="http://abc4trust.eu/wp6/credspec/credSchool/gender"
           DataType="xs:boolean" Encoding="abc:zero-one"/>
10         <AttributeDescription Type="http://abc4trust.eu/wp6/credspec/credSchool/school"
           DataType="xs:string" Encoding="xenc:sha256"/>
11     </AttributeDescriptions>
12
13 </CredentialSpecification>
```

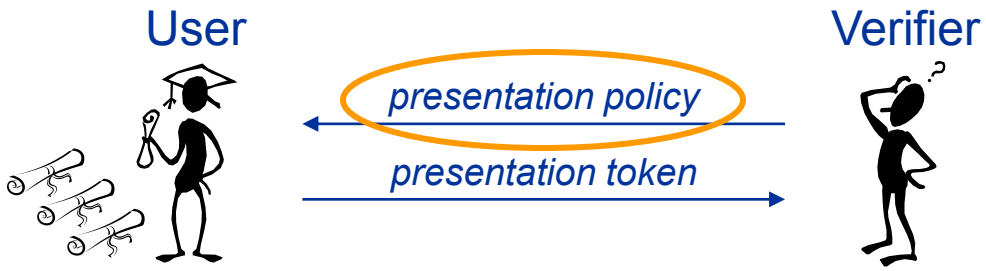
Issuer parameters

```
<IssuerParameters>

    <ParametersUID>http://abc4trust.eu/wp6/soderhamn/IssParams/school</ParametersUID>
    <AlgorithmID>urn:com:microsoft:uprove</AlgorithmID>
    <SystemParameters>...</SystemParameters>
    <CredentialSpecUID>http://abc4trust.eu/wp6/credspec/credSchool</CredentialSpecUID>
    <HashAlgorithm>http://www.w3.org/2001/04/xmlenc#sha256</HashAlgorithm>
    <CryptoParams>...</CryptoParams>
    <KeyBindingInfo>...</KeyBindingInfo>
    <RevocationParametersUID>http://abc4trust.eu/wp6/soderhamn/RevParams/school
    </RevocationParametersUID>

</IssuerParameters>
```

Presentation policy

"reveal civic number from school credential"

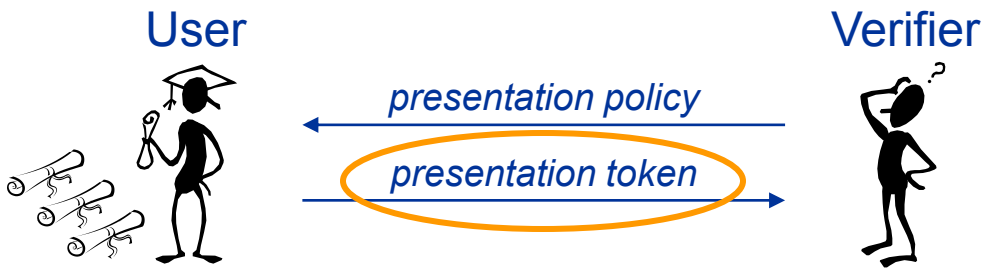
```
<PresentationPolicyAlternatives>
    <PresentationPolicy PolicyUID="revealCivicNr">
        <Message>
            <Nonce>bkQydHBQWDR4TUZzbXJKYUphdVM=</Nonce>
        </Message>
        <Credential Alias="schoolcred">
            <CredentialSpecAlternatives>
                <CredentialSpecUID>http://abc4trust.eu/wp6/credspec/credSchool
                </CredentialSpecUID>
            </CredentialSpecAlternatives>
            <IssuerAlternatives>
                <IssuerParametersUID>http://abc4trust.eu/wp6/soderhamn/IssParams/school
                </IssuerParametersUID>
            </IssuerAlternatives>
            <DisclosedAttribute AttributeType=
            "http://abc4trust.eu/wp6/credspec/credSchool/civicNr"/>
        </Credential>
    </PresentationPolicy>
</PresentationPolicyAlternatives>
```



Presentation token

"reveal civic number from school credential"

```
<PresentationToken>
    <PresentationTokenDescription PolicyUID="revealCivicNr">
        <Message>
            <Nonce>bkQydHBQWDR4TUZzbXJKYUphdVM=</Nonce>
        </Message>
        <Credential Alias="schoolcred">
            <CredentialSpecUID>http://abc4trust.eu/wp6/credspec/credSchool
            </CredentialSpecUID>
            <IssuerParametersUID>http://abc4trust.eu/wp6/soderhamn/IssParams/school
            </IssuerParametersUID>
            <DisclosedAttribute AttributeType=
            "http://abc4trust.eu/wp6/credspec/credSchool/civicNr">
                <AttributeValue>199802251234</AttributeValue>
            </DisclosedAttribute>
        </Credential>
    </PresentationTokenDescription>
    <CryptoEvidence>
        ...
    </CryptoEvidence>
</PresentationToken>
```



Use case: discussion boards

- Each pupil gets course credential for each course taken
  - Attribute course subject
  - Bound to same key as school credential

- Access anonymous discussion board for
  - Boys older than 12 taking English
  - Civic number recoverable by school inspector

Credential specification

Course credentials (one per pupil and per course)

```
<CredentialSpecification KeyBinding="true" Revocable="true">

    <SpecificationUID>http://abc4trust.eu/wp6/credspec/credSubject</SpecificationUID>

    <AttributeDescriptions MaxLength="32">
        <AttributeDescription Type="http://abc4trust.eu/wp6/credspec/credSubject/subject"
        DataType="xs:string" Encoding="xenc:sha256"/>
    </AttributeDescriptions>

</CredentialSpecification>
```

Issuance policy

Carry over key from school credential to course credential

```
<IssuancePolicy>
    <PresentationPolicy PolicyUID="revealCivicNr">
        <Credential Alias="schoolcred">
            <CredentialSpecAlternatives>
                <CredentialSpecUID>http://abc4trust.eu/wp6/credspec/credSchool
                </CredentialSpecUID>
            </CredentialSpecAlternatives>
            <IssuerAlternatives>
                <IssuerParametersUID>http://abc4trust.eu/wp6/soderhamn/IssParams/school
                </IssuerParametersUID>
            </IssuerAlternatives>
        </Credential>
    </PresentationPolicy>
    <CredentialTemplate SameKeyBindingAs="schoolcred">
        <CredentialSpecUID>http://abc4trust.eu/wp6/credspec/credCourse
        </CredentialSpecUID>
        <IssuerParametersUID>http://abc4trust.eu/wp6/soderhamn/IssParams/course
        </IssuerParametersUID>
    </CredentialTemplate>
</IssuancePolicy>
```

Presentation policy

- Boys older than 12 taking English
- Civic number recoverable by school inspector

```
<PresentationPolicyAlternatives>
    <PresentationPolicy PolicyUID="existing">
        <Message>
            <Nonce>bkQydHBQWDR4TUZzbXJKYUphdVM=</Nonce>
        </Message>
        <Pseudonym Scope="http://soderhamn.se/highschool/discuss" Established="true"/>
    </PresentationPolicy>

    <PresentationPolicy PolicyUID="new">
        <Message>
            <Nonce>bkQydHBQWDR4TUZzbXJKYUphdVM=</Nonce>
        </Message>
        <Pseudonym Scope="http://soderhamn.se/highschool/discuss" Alias="nym"/>
        <Credential Alias="school" SameKeyBindingAs="nym">
            <CredentialSpecAlternatives>
                <CredentialSpecUID>http://abc4trust.eu/wp6/credspec/credSchool</CredentialSpecUID>
            </CredentialSpecAlternatives>
            <IssuerAlternatives>
                <IssuerParametersUID>http://abc4trust.eu/wp6/soderhamn/IssParams/school</IssuerParametersUID>
            </IssuerAlternatives>
            <DisclosedAttribute AttributeType="http://abc4trust.eu/wp6/credspec/credSchool/civicNr">
                <InspectorPublicKeyUID>http://abc4trust.eu/wp6/soderhamn/SchoolInspector</InspectorPublicKeyUID>
                <InspectionGrounds>Concrete safety threat.</InspectionGrounds>
            </DisclosedAttribute>
        </Credential>
```

Presentation policy (cont.)

- Boys older than 12 taking English
- Civic number recoverable by school inspector

```
26      <Credential Alias="subject" SameKeyBindingAs="school">
27          <CredentialSpecAlternatives>
28              <CredentialSpecUID>http://abc4trust.eu/wp6/credspec/credSubject</CredentialSpecUID>
29          </CredentialSpecAlternatives>
30          <IssuerAlternatives>
31              <IssuerParametersUID>http://abc4trust.eu/wp6/soderhamn/IssParams/subject</IssuerParametersUID>
32          </IssuerAlternatives>
33      </Credential>
34      <AttributePredicate Function="urn:oasis:names:tc:xacml:1.0:function:boolean-equal">
35          <Attribute CredentialAlias="school" AttributeType=
            "http://abc4trust.eu/wp6/credspec/credSchool/gender"/>
36          <ConstantValue>false</ConstantValue>
37      </AttributePredicate>
38      <AttributePredicate Function="urn:oasis:names:tc:xacml:1.0:function:integer-less-than">
39          <Attribute CredentialAlias="school" AttributeType=
            "http://abc4trust.eu/wp6/credspec/credSchool/civicNr"/>
40          <ConstantValue>200002139999</ConstantValue>
41      </AttributePredicate>
42      <AttributePredicate Function="urn:oasis:names:tc:xacml:1.0:function:string-equal">
43          <Attribute CredentialAlias="subject" AttributeType=
            "http://abc4trust.eu/wp6/credspec/credSubject/subject"/>
44          <ConstantValue>English</ConstantValue>
45      </AttributePredicate>
46    </PresentationPolicy>
47  </PresentationPolicyAlternatives>
```

Conclusion

Not in these examples but also defined

- Issuance tokens
- Cross-credential attribute predicates
- Revocation

ABC4Trust XML schema

- Common format for credential specifications, policies, …
- Technology-agnostic: crypto hidden in dedicated elements
- Easy to switch between U-Prove and Identity Mixer
- Even support mixed-technology tokens