Authentication Context Extension

MAPPING CERTIFICATE IDENTITY TO A SAML AUTHENTICATED IDENTITY

STEFAN SANTESSON

Draft:

Authentication Context Certificate Extension
draft-santesson-auth-context-extension-04

http://tools.ietf.org/html/draft-santesson-auth-context-extension

Federated identity in an EU context

Identity attribute mapping

STORK PEPS

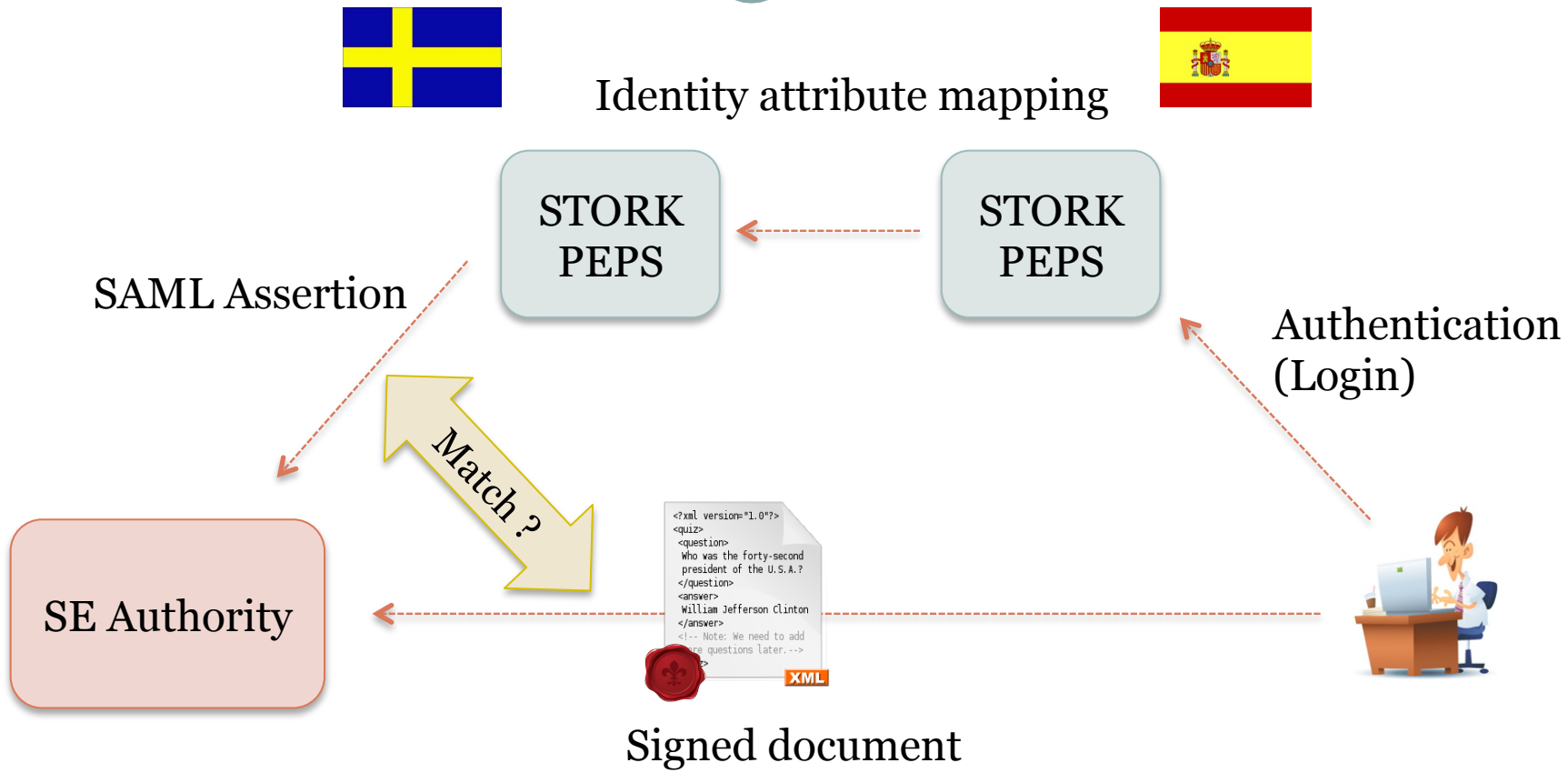
STORK PEPS

SAML Assertion

Authentication (Login)

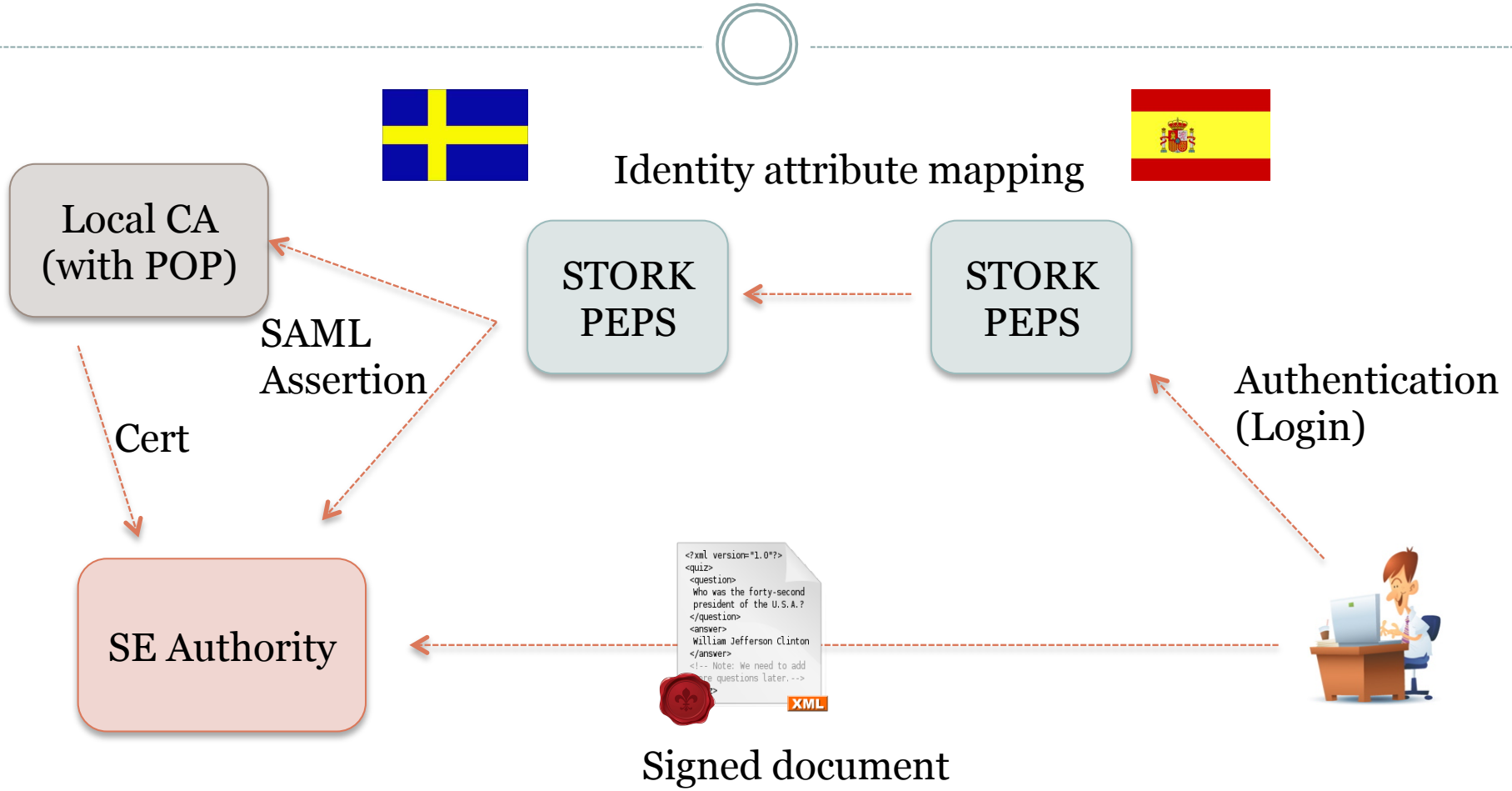
SE Authority

Mapping signature and federated identity



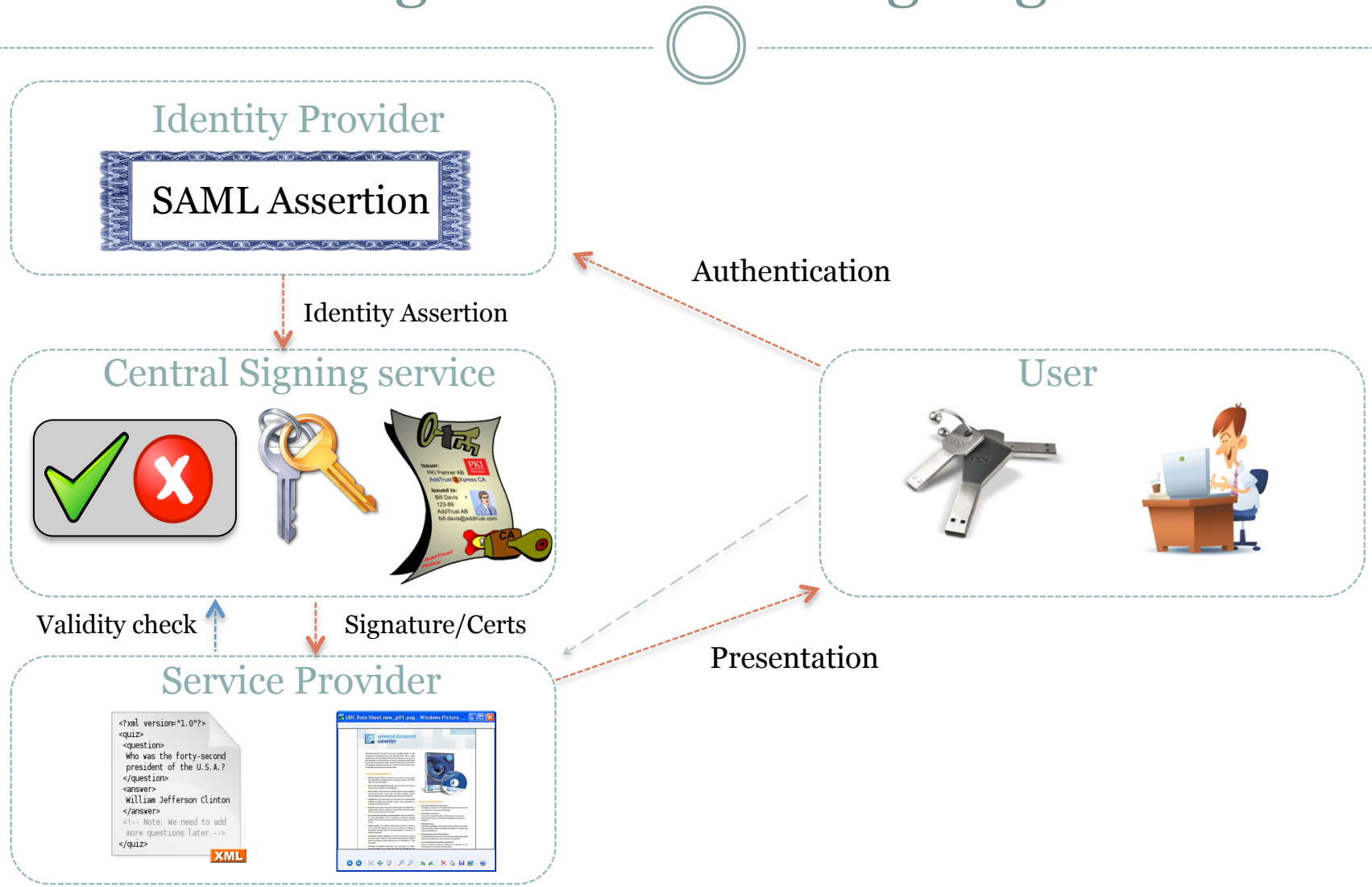
Question: Is the person who logged in also the signer?

Mapping signature and federated identity



Solution:
Verifying signature with local cert

Signing service
Issuing certificates at signing time



Auth context extension

- Provides the missing piece of information in certs in these use cases
- Allow the RP to map the subject identity in the cert to be understood within the originating;
  - SAML attribute context, and;
  - SAML Authentication context
- Allows the certificate subject identity to conform to any cert profile or standard (e.g. RFC 3739).
- Allows expression of implicit and explicit context and mapping information.

Structure

- SEQUENCE of AuthenticationContext
- AuthenticationContext ::=
  - SEQUENCE
    - contextType (holds a URI identifier)
    - contextInfo (Optional XML data according to URI identifier)
- Works very similar to SAML AuthnContextClassRef and AuthnContextDecl:
  - contextType URI identifies an XML Schema for providing contextInfo
  - A contextInfo is optional allowing declaration of implicit rules by ID.

SAML Auth Context type

- The draft provides one contextType for SAML based authentication contexts.
- Holds 2 elements:
  - AuthContextInfo
    - Holding info about a SAML Authentication instant
      - IdP, Date and Time, Assertion Ref, LoA, Verifier
  - IdAttributes
    - Mapping information for present cert attributes and name forms
      - Cert name type
      - Cert name ref (Attribute OID, SAN type)
      - SAML attribute

Example - AuthContextInfo

```
<saci:AuthContextInfo
        AssertionRef="_71b981ab017eb42869ae4b62b2a63add"
        IdentityProvider="https://idp-test.nordu.net/idp/shibboleth"
        AuthenticationInstant="2013-03-05T22:59:57.000+01:00"
        AuthnContextClassRef="http://id.elegnamnden.se/loa/1.0/loa3"/>
```

Example – Mapping info

```
<saci:IdAttributes>
       <saci:AttributeMapping Type="rdn" Ref="2.5.4.5">
           <saml:Attribute
               FriendlyName="Personal ID Number"
               Name="urn:oid:1.2.752.29.4.13">
               <saml:AttributeValue xsi:type="xs:string"
                   >200007292386</saml:AttributeValue>
           </saml:Attribute>
       </saci:AttributeMapping>
       <saci:AttributeMapping Type="rdn" Ref="2.5.4.3">
           <saml:Attribute
               FriendlyName="Display Name"
               Name="urn:oid:2.16.840.1.113730.3.1.241">
               <saml:AttributeValue xsi:type="xs:string"
                   >John Doe</saml:AttributeValue>
           </saml:Attribute>
       </saci:AttributeMapping>
       <saci:AttributeMapping Type="san" Ref="1">
           <saml:Attribute
               FriendlyName="E-mail"
               Name="urn:oid:0.9.2342.19200300.100.1.3">
               <saml:AttributeValue xsi:type="xs:string"
                   >john.doe@example.com</saml:AttributeValue>
           </saml:Attribute>
       </saci:AttributeMapping>
   </saci:IdAttributes>
```

Example – Just mapping. No attr vals

```
<saci:SAMLAuthContext
    xmlns:saci="http://id.elegnamnden.se/auth-cont/1.0/saci"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
    <saci:IdAttributes>
        <saci:AttributeMapping Type="rdn" Ref="2.5.4.6">
            <saml:Attribute Name="urn:oid:2.5.4.6"/>
        </saci:AttributeMapping>
        <saci:AttributeMapping Type="rdn" Ref="2.5.4.5">
            <saml:Attribute Name="urn:oid:1.2.752.29.4.13"/>
        </saci:AttributeMapping>
        <saci:AttributeMapping Type="rdn" Ref="2.5.4.42">
            <saml:Attribute Name="urn:oid:2.5.4.42"/>
        </saci:AttributeMapping>
        <saci:AttributeMapping Type="rdn" Ref="2.5.4.4">
            <saml:Attribute Name="urn:oid:2.5.4.4"/>
        </saci:AttributeMapping>
        <saci:AttributeMapping Type="rdn" Ref="2.5.4.3">
            <saml:Attribute Name="urn:oid:2.16.840.1.113730.3.1.241"/>
        </saci:AttributeMapping>
        <saci:AttributeMapping Type="san" Ref="1">
            <saml:Attribute Name="urn:oid:0.9.2342.19200300.100.1.3"/>
        </saci:AttributeMapping>
    </saci:IdAttributes>
</saci:SAMLAuthContext>
```

DEMO

Swedish National Signing Service

https://eid2cssp.3xasecurity.com/login/

Questions

Stefan Santesson

sts@aaa-sec.com