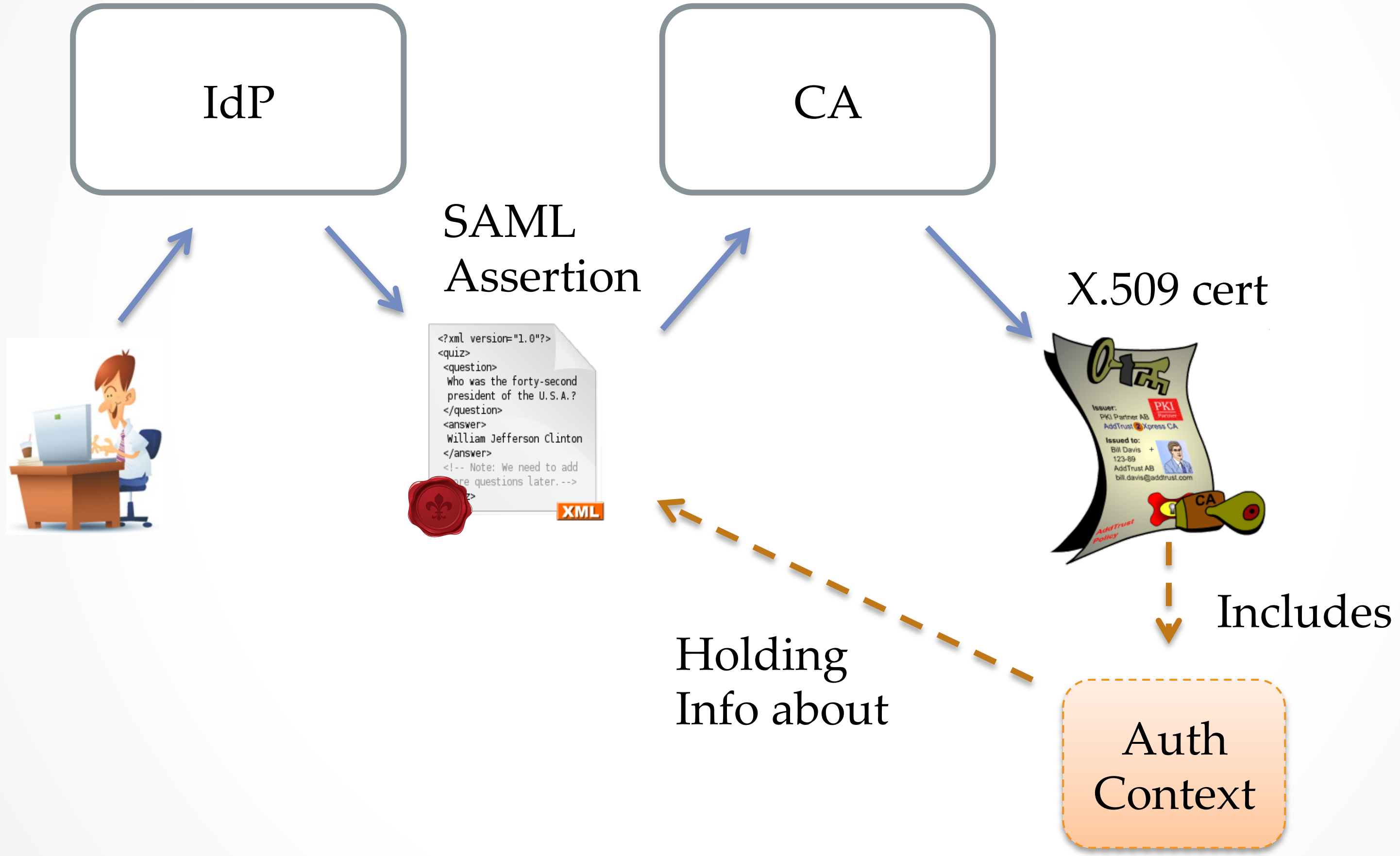
Authentication Context QC Statement

Stefan Santesson, 3xA Security AB
stefan@aaa-sec.com

The use case and problem

- User identities and user authentication is managed through SAML assertions.
- Some applications need certificates that are issued on the basis of a SAML assertion (or other approved authentication technique)
- The SAML attribute profile and the certificate attribute profile is NOT an exact match (e.g. due to RFC 3739 requirements)
- Users of the certificate need the underlying SAML authentication context
- HOW STORE IT IN THE CERT?

Authentication Context



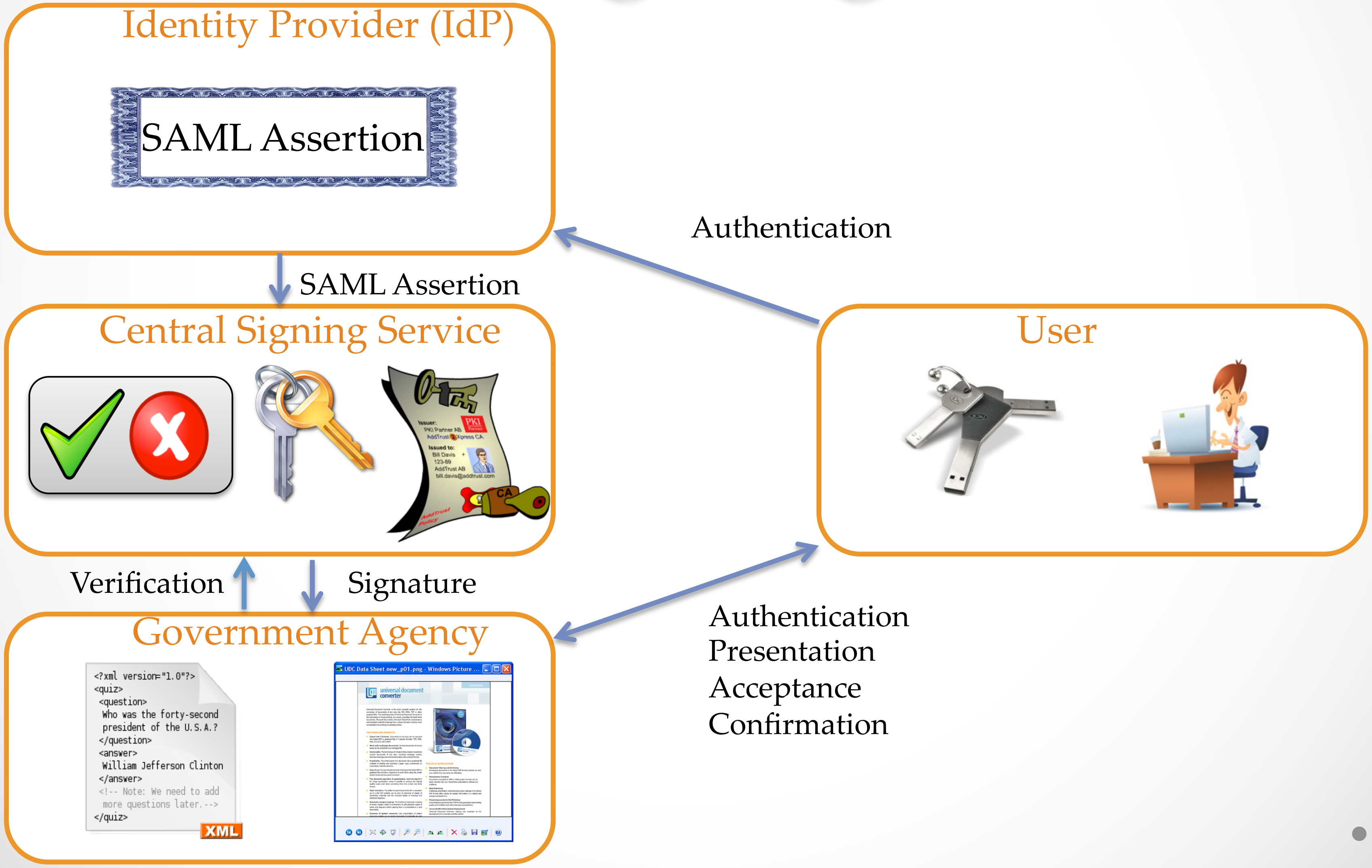
```
<?xml version="1.0"?>
<quiz>
 <question>
  Who was the forty-second
  president of the U.S.A.?
 </question>
 <answer>
  William Jefferson Clinton
 </answer>
 <!-- Note: We need to add
   ore questions later.-->
   z>
```

Use Case
Electronic Signatures

Authentic Swedish e-gov use case

- Users don't have PKI credentials
  - OTP tokens
  - Mobile credentials (e.g. Google authenticator)
  - Etc
- The infrastructure needs user's electronic signature
- A central signing service generates user PKI credentials based on SAML assertions
- The relying party trust the SAML federation and understands the federation attribute profile
- The relying party needs to compare user ID in certs with user ID in SAML assertions

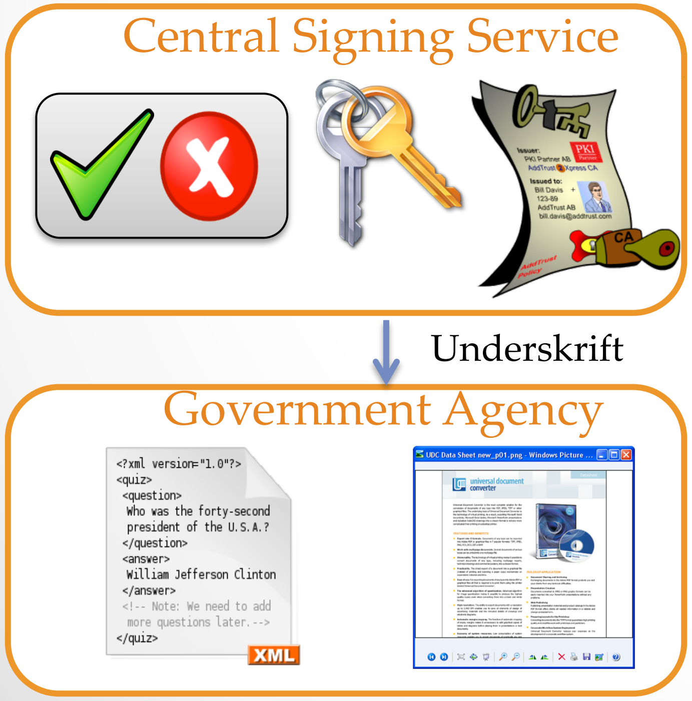
Central Signing Service



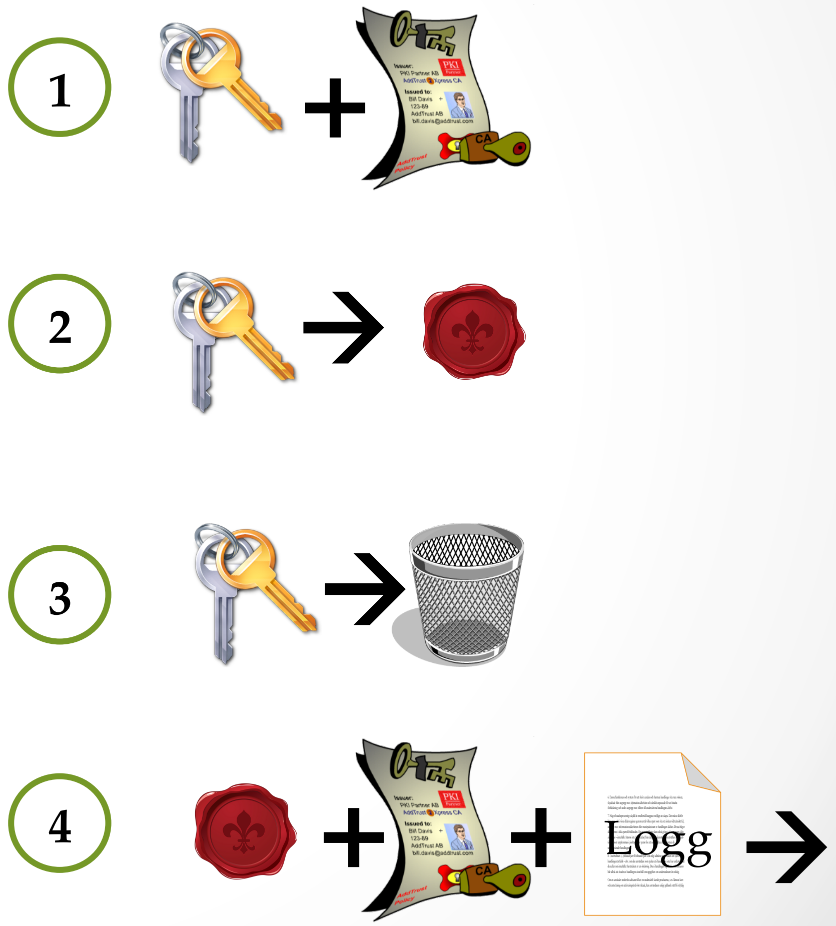
```
<?xml version="1.0"?>
<quiz>
 <question>
  Who was the forty-second
  president of the U.S.A.?
 </question>
 <answer>
  William Jefferson Clinton
 </answer>
 <!-- Note: We need to add
  more questions later.-->
</quiz>
```

Signing process

1. Generate keys and certificate
2. Sign
3. Destroy private key
4. Send signature info



```
<?xml version="1.0"?>
<quiz>
 <question>
  Who was the forty-second
  president of the U.S.A.?
 </question>
 <answer>
  William Jefferson Clinton
 </answer>
 <!-- Note: We need to add
  more questions later.-->
</quiz>
```



Current solution
new QC Statement (RFC 3739)

```
AuthContextQCStatement ::= SEQUENCE {
      authContextType       OBJECT IDENTIFIER,
      authContext           AuthContext }

AuthContext ::= SEQUENCE {
     contentType            PrintableString,
     authContextInfo        IA5String }
```

- contentType holds a mimeType
- authContextInfo stors base64 encoded data.
  - JSON, XML, DER etc

Demo

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

Use Idp named: Testbädd Referens Idp
User name: vlindeman
Password: hemligt

Alternatives

- Why not store the whole SAM Assertion in the cert?
  - Exploding the size of a cert
  - Includes information we may not want to reveal to the public
  - Relying party system is often SAM unaware
  - Note that you CAN store a full SAML assertion using current structure (But you don't have to)
- Why use a typed hole?
  - There will allways be a use case we never thought about
  - Standardizing the data content will require an extremely complex structure to meet all possible needs
  - Local context need to decide data format (XML, JSON, DER etc)

Way ahead

- Could this merit an amendment to RFC 3739?
- Should it go into a new extension?
- Is there a better solution out there?

Questions
Comments

Stefan Santesson
3xA Security AB
stefan@aaa-sec.com