Real World Case Study
Presentations and Mapping to SAML/Liberty Specifications

Context 6, Austria

Thomas Rössler, EGIZ
About EGIZ…

- Austria
  - EU member state
  - approx. 8 mio. citizens
About EGIZ…

- **E-Government Innovation Center – EGIZ**

The E-Government Innovation Center is a joint initiative of the Austrian Federal Chancellery and the Graz University of Technology:

- Research and Innovation
- Supporting the further Development of the IT-Strategy of the Austrian Federal Chancellery
- Design and Specification
There are two issues within the Austrian E-Government identity management which use **SAML / Liberty Alliance**:  

- **Structure of the Identity-Link**  
- Identification/Authentication of citizens through a **server side identification module** (MOA-ID, a kind of „Identity Provider“)

Since Austria is a pioneer in the field of E-Government and identity management, the development of national profiles and interfaces has been started in 2001+. Thus, national profiles and interfaces base on an early version of SAML.
Identity Link

- Structure of the **Identity-Link**
- Identification/Authentication of citizens through **MOA-ID**

Citizen Card

Identity Link

Public Key

Source PIN

Governmental Application

Sector Specific PIN

- Citizen is **identified** uniquely (ssPIN)
- and **authenticated** by applying electronic signatures
Contents

- The Identity Link
  - Server Side Modules for Identification
    - Future Developments
Contents

- The Identity Link
  - Server Side Modules for Identification
  - Future Developments
Identity Link

- For Identification: **Identity Link**
- For Authentication: **Electronic Signatures**

Citizen Card

- **Public Key Source PIN**

Identity Link

Request

Governmental Application

- **Sector Specific PIN**

Citizen is **identified** uniquely (ssPIN)

and **authenticated** by applying electronic signatures
The Identity-Link is created as a **SAML-Assertion**:

```xml
  <saml:AttributeStatement>
    <saml:Subject>
      <saml:SubjectConfirmation>
        <saml:ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:sender-vouches</saml:ConfirmationMethod>
        <saml:SubjectConfirmationData>
          <pr:Person si:type="pr:PhysicalPersonType">
            <pr:Identification>
              <pr:Value>07rCkadqGadWrwSWQdBy/Bg==</pr:Value>
              <pr:Type>urn:publicid:gv.at:baseid</pr:Type>
            </pr:Identification>
            <pr:Name>
              <pr:GivenName>Thomas Gert</pr:GivenName>
              <pr:FamilyName primary="undefined">Rössler</pr:FamilyName>
            </pr:Name>
            <pr:DateOfBirth>1976-08-23</pr:DateOfBirth>
          </pr:Person>
        </saml:SubjectConfirmationData>
      </saml:SubjectConfirmation>
    </saml:Subject>
  </saml:AttributeStatement>
</assertion>
```
Contents

- The Identity Link
- Server Side Modules for Identification
- Future Developments
Austria provides free software components for application developers and service providers in order to enforce diversification of E-Government.

**Modules for Online-Applications:**
- MOA–SS: server-signatures
- MOA–SP: signature-validation
- MOA–ID, MOA-wID: Identification
- MOA–ZS: electronic delivery
- MOA–VV: mandates, representation
MOA-ID for Citizen Identification

- Online Application
- MOA ID Auth
  - Signature Verification
  - Prove of Identity-Link
- Webbrowser
- Citizen Card

(SL)
MOA-ID for Citizen Identification

- Follows Browser/Artifact Profile according to SAML 1.0
Full SAML-Response from MOA-ID to the Application:

```
    <samlp:Status>
        <samlp:StatusCode Value="samlp:Success"/>
        <samlp:StatusMessage>Anfrage erfolgreich beantwortet</samlp:StatusMessage>
    </samlp:Status>
    <saml:Assertion AssertionID="7479969116368580400" IssueInstant="2007-04-19T16:18:02+02:00" Issuer="https://demo.egiz.gv.at:443/moa-id-auth/" MajorVersion="1" MinorVersion="0">
        <saml:AttributeStatement>
            <saml:Subject>[..]
            <saml:Attribute AttributeName="PersonData">[..]
            <saml:Attribute AttributeName="isQualifiedCertificate">[..]
            <saml:Attribute AttributeName="bkuURL">[..]
            <saml:Attribute AttributeName="SignerCertificate">[..]
            <saml:Attribute AttributeName="Vollmacht">[..]
        </saml:AttributeStatement>
    </saml:Assertion>
</rsmp:Response>
```
Personal Information of the Citizen:
- Last Name, First Name
- Date of Birth
- unique Identifier (source-PIN or sector specific PIN)
- the signature provided by the citizen in order to access MOA-ID
MOA-ID for Citizen Identification

- Information whether the citizen has provided a qualified certificate or not
  - this is important in governmental applications due to the legal implications (1999/93/EC)
MOA-ID for Citizen Identification

This attribute provides the full X509-Certificate of the citizen used to access MOA-ID

- the certificate is taken from the citizen’s Citizen Card
In the event of representation, this means that a citizen acts in the name of another person, an additional attribute contains the electronic mandate provided by the representative:

- Austria introduced electronic mandates which are legally accepted
- electronic mandates are intended to be used in connection with MOA-ID
Contents

- The Identity Link
- Server Side Modules for Identification
- Future Developments
Future Developments

- We are working on further developments of MOA-ID
- We aim to extend MOA-ID being a full Identity Provider
  - e.g. to be used in local networks and/or to realize real Single Sign On
- We aim to update the interfaces according to the current specifications of SAML and Liberty Alliance

- To mention one of our newest developments: “Citizen Card activated SSL-Client-Certificates”
  - the user’s SSL-client certificate becomes active after she has been authenticated by MOA-ID
  - MOA-ID triggers an OCSP-responder
  - Assertion Query/Request Profile of SAML2.0
Future Developments

E.g. Citizen Card activated SSL-Client-Certificates:

Association Module

Authentication Store

Revocation Status Provider

Identity Provider

Application

Revocation Status ?

+ Authentication Information

+ eldentity

+ eldentity
Thank you for your attention…

The E-Government Innovation Center is a joint initiative of the Austrian Federal Chancellery and the Graz University of Technology.

Thomas Gert RÖSSLER
thomas.roessler@egiz.gv.at