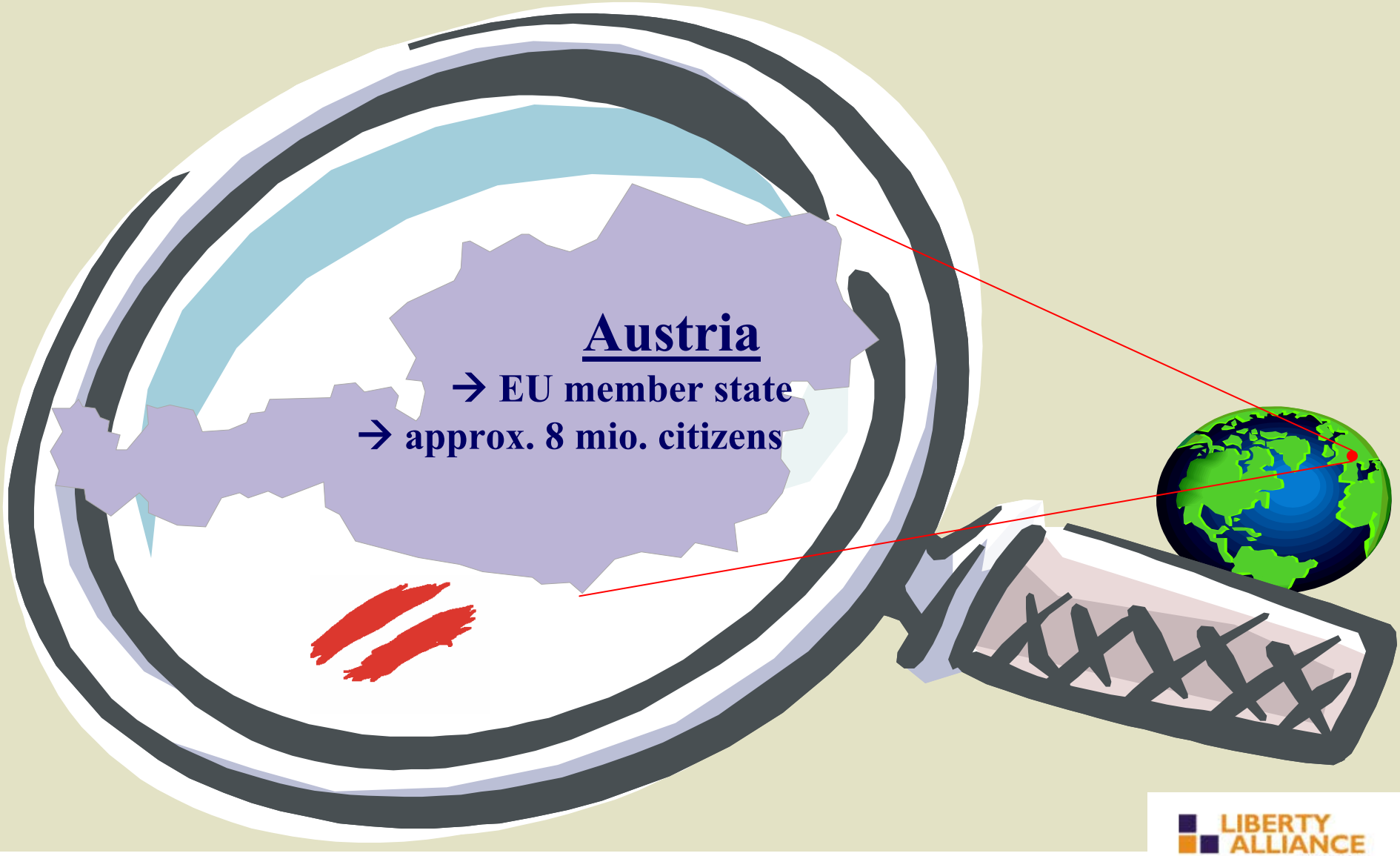
LIBERTY ALLIANCE PROJECT

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

Context 6, Austria

Thomas Rössler, EGIZ

About EGIZ…



LIBERTY ALLIANCE PROJECT

About EGIZ…

- **E**-**G**overnment **I**nnovation **C**enter – 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

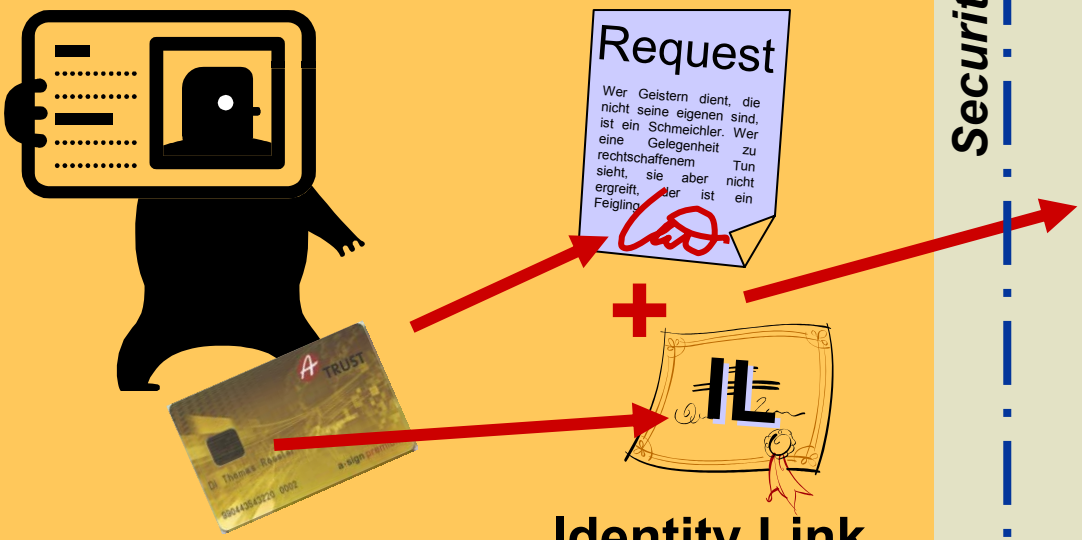
SAML/LA related Issues

- 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.

LIBERTY ALLIANCE PROJECT

Identity Link

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



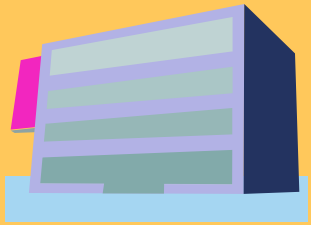
Citizen Card

Identity Link

- Public Key
- Source PIN

Security Layer

Governmental Application

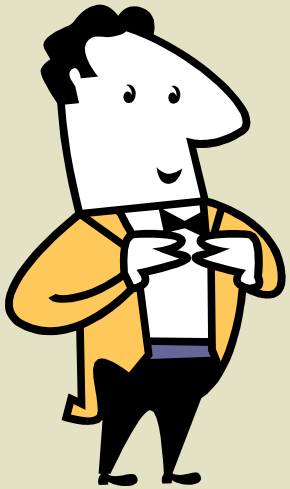


Sector Specific PIN

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

Contents

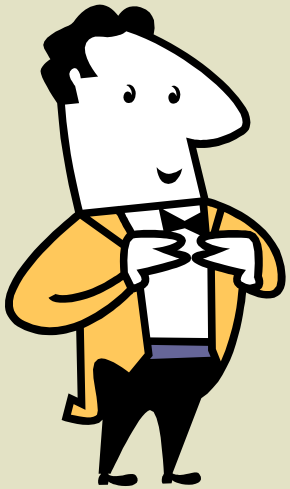
- The Identity Link
  - Server Side Modules for Identification
    - Future Developments



LIBERTY ALLIANCE PROJECT

Contents

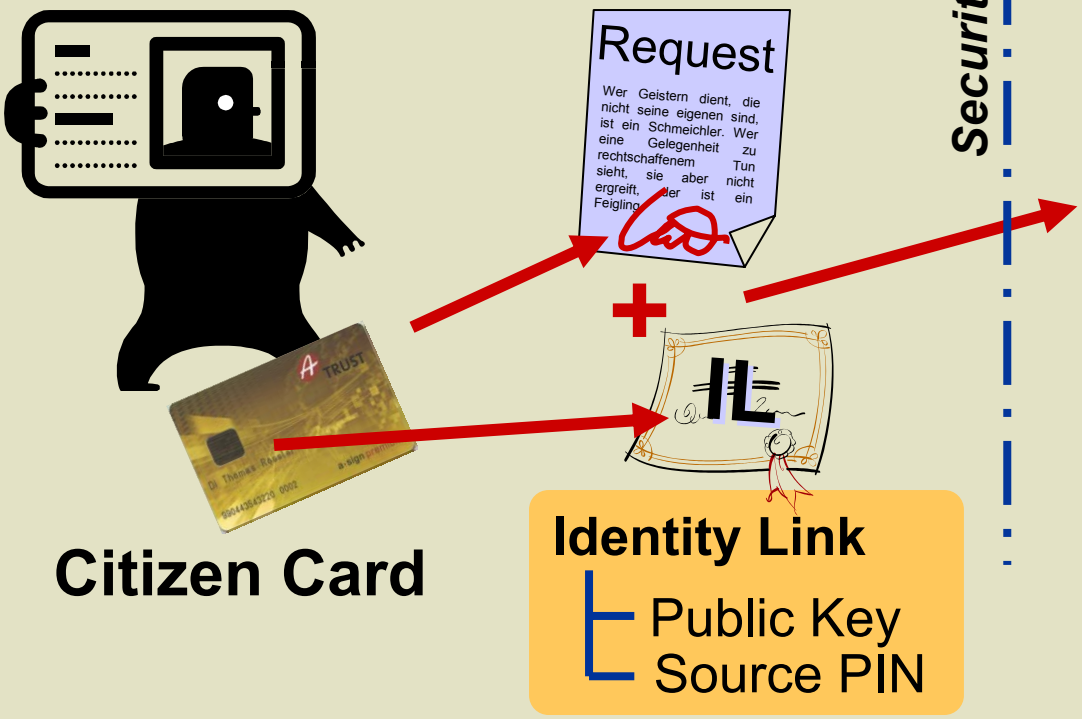
- **The Identity Link**
  - Server Side Modules for Identification
    - Future Developments



LIBERTY ALLIANCE PROJECT

Identity Link

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



LIBERTY ALLIANCE PROJECT

Identity-Link

Identity Link
- Public Key
- Source PIN

- The Identity-Link is created as a **SAML-Assertion**:

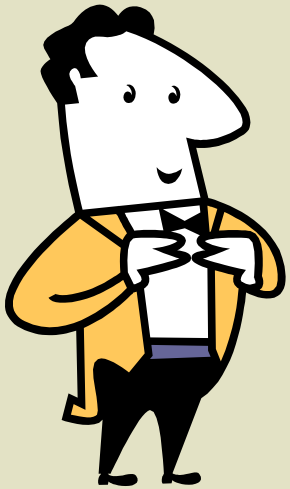
```
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion" AssertionID="szr.bmi.gv.at-
AssertionID108910863604510" IssueInstant="2004-07-06T10:10:36+01:00"
Issuer="http://portal.bmi.gv.at/ref/szr/issuer" MajorVersion="1" MinorVersion="0">
  <saml:AttributeStatement>
    <saml:Subject>
      <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> [..]
```

Personal Information

LIBERTY ALLIANCE PROJECT

Contents

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

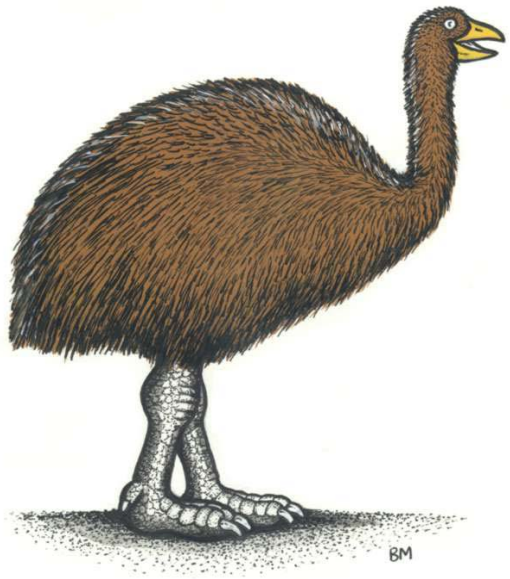


LIBERTY ALLIANCE PROJECT

Server Side Authentication Module

- Austria provides free software components for application developers and service providers in order to enforce diversification of E-Government.

- **M**odules for **O**nline-**A**pplications:
  - MOA–SS: server-signatures
  - MOA–SP: signature-validation
  - MOA–ID, MOA-wID: Identification
  - MOA–ZS: electronic delivery
  - MOA–VV: mandates, representation



LIBERTY ALLIANCE PROJECT

MOA-ID for Citizen Identification

Online Application

Webbrowser

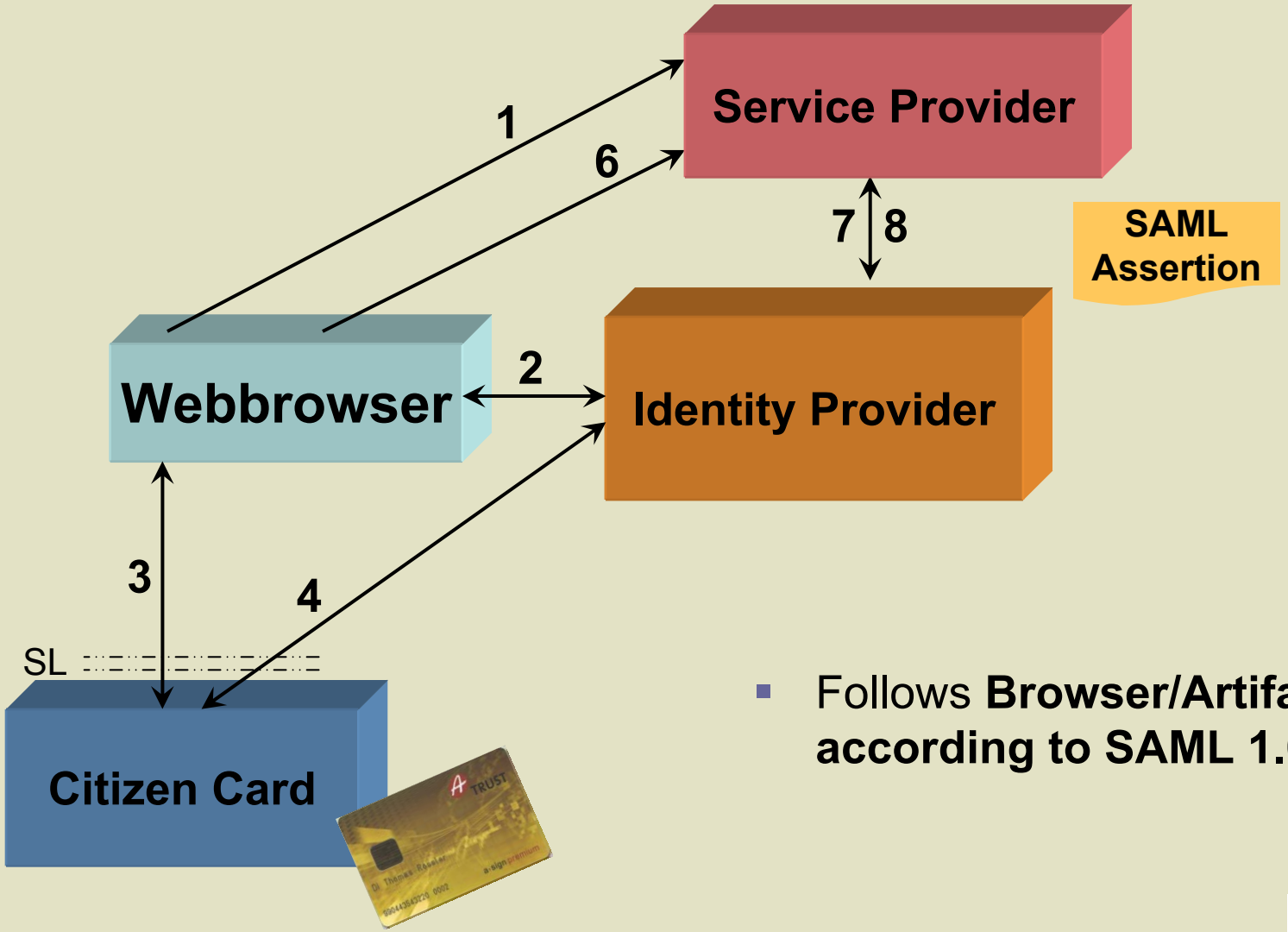
MOA ID Auth
Signature Verification
Prove of Identity-Link

SL

Citizen Card

LIBERTY ALLIANCE PROJECT

MOA-ID for Citizen Identification



- Follows **Browser/Artifact Profile according to SAML 1.0**

LIBERTY ALLIANCE PROJECT

MOA-ID for Citizen Identification

- Full SAML-Response from MOA-ID to the Application:

```
<samlp:Response InResponseTo="" IssueInstant="2007-04-19T16:18:38+02:00" MajorVersion="1"
MinorVersion="0" ResponseID="6365967710943240368" xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol">
        <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>
</samlp:Response>
```

MOA-ID for Citizen Identification

```
<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>
```

- 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

LIBERTY ALLIANCE PROJECT

MOA-ID for Citizen Identification

```
<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>
```

- 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

```
<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>
```

- 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

LIBERTY ALLIANCE PROJECT

MOA-ID for Citizen Identification

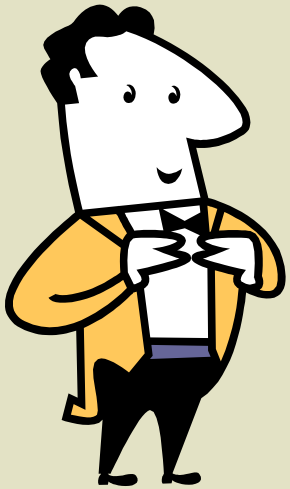
```
<saml:AttributeStatement>
        <saml:Subject>[..]
        <saml:Attribute AttributeName="PersonData" >[..]
        <saml:Attribute
AttributeName="isQualifiedCertificate" > [..]
    <saml:Attribute AttributeName="bkuURL"> [..]
    <saml:Attribute AttributeName="SignerCertificate" > [..]
    <saml:Attribute AttributeName="Vollmacht" >[..]
        </saml:AttributeStatement>
```

- 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

LIBERTY ALLIANCE PROJECT

Contents

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



LIBERTY ALLIANCE PROJECT

Future Developments

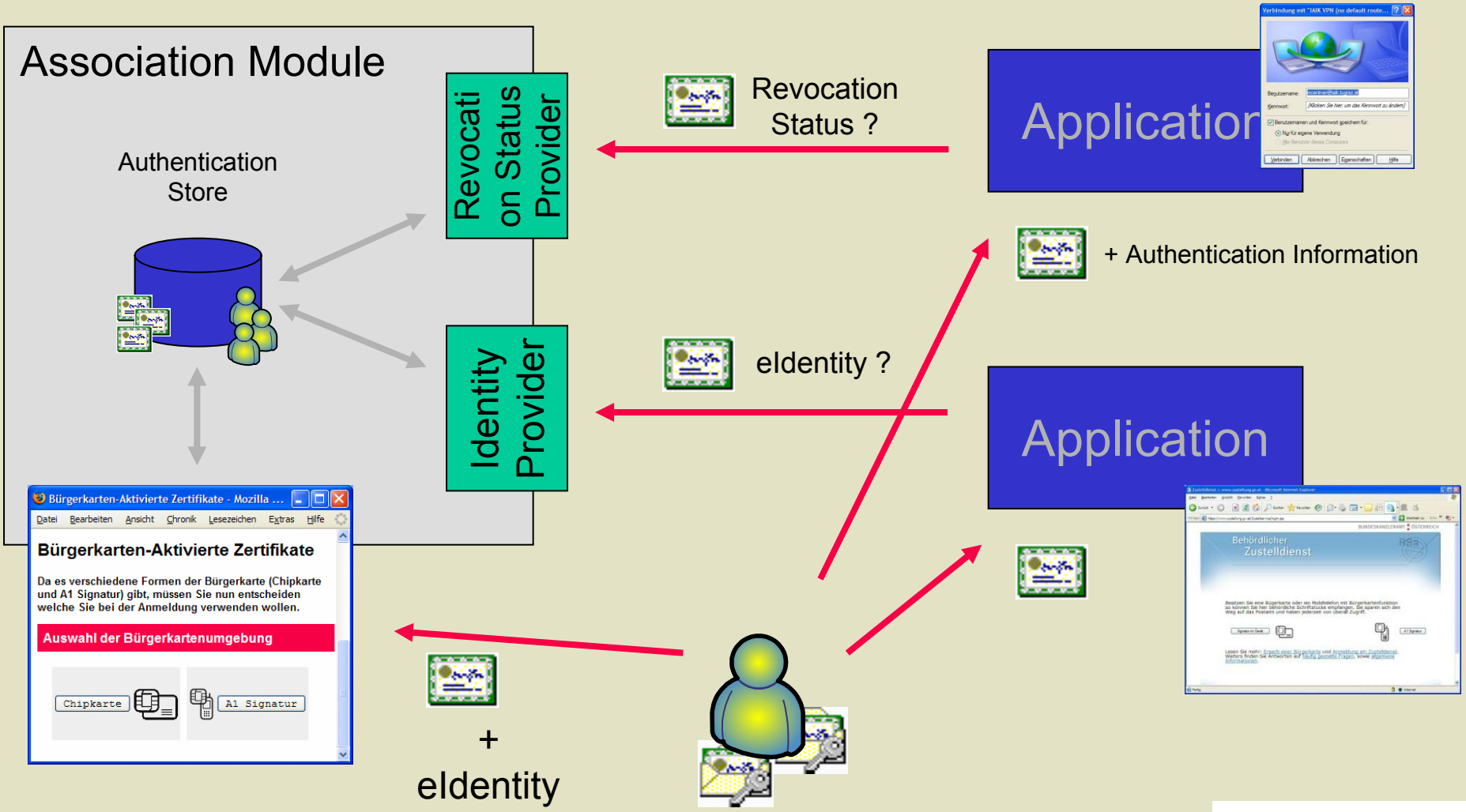
- We are working on further developments of MOA-ID
- We aim to extend MOA-ID being a full Identity Provider
  - e.g. to be used in local networks and/or to realize real Single Sign On
- We aim to update the interfaces according to the current specifications of SAML and Liberty Alliance

- 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**

LIBERTY ALLIANCE PROJECT

Future Developments

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



LIBERTY ALLIANCE PROJECT

Thank you for your attention…

EGIZ E-Government Innovationszentrum

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

TU Graz BUNDESKANZLERAMT ÖSTERREICH

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