Identity Trends in e-Government: Business

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
Contents

- Austrian Identification System
- Austrian Citizen Card Concept
- The Identity-Link
Contents

- Austrian Identification System
  - Austrian Citizen Card Concept
  - The Identity-Link
Each resident has a unique number „ZMR-Zahl“ in the Central Register of Residents (CRR)
The Austrian Identification System

- Identification is based on unique identification numbers taken from Austria’s base registers:
  - e.g. Central Residents Register (CRR), etc.
- Every person in Austria is registered with such a base register
- Even foreigners living in Austria can be registered with the so called Supplementary Register (SR)

Every person gets assigned a unique personal identification number, the so called **Source-PIN**
The Austrian Identification System

- Source PIN
  - ... is **unique**
  - ... in contrast to other base identifiers, it is under the **sole control** of the citizen
  - ... it **must not** be stored by any governmental or private party
- Due to privacy reasons, the **Source PIN** is not used to identify persons in E-Government processes

For Identification in E-Government Processes, we use **Sector Specific-PINs** (ssPIN)
Each governmental sector (i.e. different areas of the public administration) is assigned a specific alphanumeric code, the sector code.

For each of these sectors, the Austrian e-ID concept foresees a separate unique identifier, which is called the **Sector Specific PIN (ssPIN)**.

The Sector Specific PIN is derived from the person’s **Source PIN** by applying a cryptographic one-way function (Hash-function).

Each ssPIN is different and it is neither possible to calculate the underlying sourcePIN nor any other sector’s ssPIN from a given ssPIN.
The Austrian Identification System

For Example:

- **sourcePIN**
  - Add Sector Identifier (SA) to the sourcePIN (Concatination)
  - One Way Function HASH-Function (SHA-1)
  - ssPIN for Sector SA

- **sourcePIN**
  - Add Sector Identifier (GH) to the sourcePIN (Concatination)
  - One Way Function HASH-Function (SHA-1)
  - ssPIN for Sector GH

**Sector**
- "Taxes and Duties"
  - SA
- "Social Security"
  - GH
Contents

- Austrian Identification System
  - Austrian Citizen Card Concept
  - The Identity-Link
Citizen Card

- Citizen Card holds...
  - electronic signatures → Authentication
  - electronic identity → Identification
Austrian Citizen Card Concept

- For Identification: **Source PIN → Sector Specific PIN**
- For Authentication: **Electronic Signatures**

Governmental Application

Sector Specific PIN

Citizen is identified uniquely (ssPIN)

and authenticated by applying electronic signatures
The Identity-Link binds:
- the citizen’s unique Identifier (Source-PIN) to
- the citizen’s public keys used for electronic signatures

thus it contains the following information of a citizen:
- First Name, Last Name, Date of Birth, Source-PIN

the Identity-Link is a **SAML 1.0 Assertion** which is electronically signed by a governmental authority
The Identity-Link is created as a **SAML-Assertion**:

```xml
  <saml:AttributeStatement>
    <saml:Subject>
      **Person Data: First Name, Last Name, Date of Birth, Source-PIN**
    </saml:Subject>
    <saml:Attribute AttributeName="CitizenPublicKey" AttributeNamespace="urn:publicid:gv.at:namespaces:identitylink:1.2">
      <saml:AttributeValue>
        <dsig:RSAKeyValue>
          <dsig:Modulus>yf...RM=</dsig:Modulus>
          <dsig:Exponent>A..B</dsig:Exponent>
        </dsig:RSAKeyValue>
      </saml:AttributeValue>
    </saml:Attribute>
  </saml:AttributeStatement>
  <dsig:Signature>[..]</dsig:Signature>
</saml:Assertion>
```
The Identity-Link is created as a **SAML-Assertion**:

```xml
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>
          <person si:type="pr:PhysicalPersonType">
            <identification>
              <value>07rCkadqGadWrwSWQdBy/Bg==</value>
              <type>urn:publicid:gv.at:baseid</type>
            </identification>
            <name>
              <givenName>Thomas Gert</givenName>
              <familyName primary="undefined">Rössler</familyName>
            </name>
            <dateOfBirth>1976-08-23</dateOfBirth>
          </person>
        </saml:SubjectConfirmationData>
      </saml:SubjectConfirmation>
    </saml:Subject>
  </saml:AttributeStatement>
</assertion>
```
Security-Layer: a high-level interface

- Simple XML requests via Web browser

```xml
<?xml version="1.0" encoding="UTF-8"?>
<CreateXMLSignatureRequest xmlns="http://www.cio
<KeyboxIdentifier>SecureSignatureKeypair</K
<DataObjectInfo Structure="enveloping">
  <sl10:DataObject>
    <sl10:XMLContent>Data to be signed</sl10:XMLContent>
  </sl10:DataObject>
  <sl10:TransformsInfo>
    <sl10:FinalDataMetaInfo>
      <sl10:MimeType>text/plain</sl10:MimeType>
    </sl10:FinalDataMetaInfo>
  </sl10:TransformsInfo>
</DataObjectInfo>
</CreateXMLSignatureRequest>
```
Citizen Card is a „Concept“!

- Citizen Card can be and is realised through various technologies:
  - Signature-Card
  - Bank-Cards
  - Health-Card
  - Student-Cards
  - Employee-ID
  - Mobile Phone
Thank you for your attention…