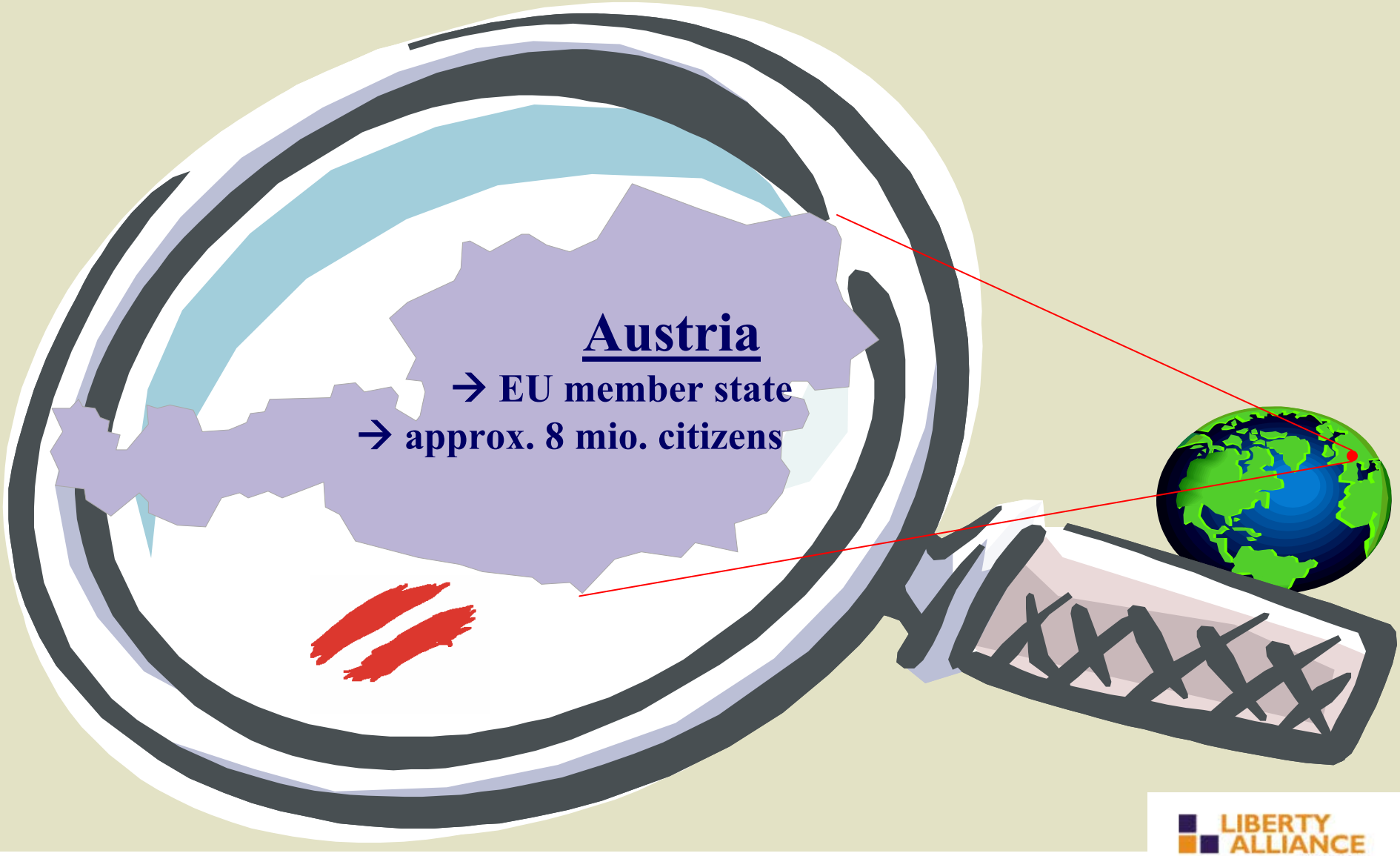
LIBERTY ALLIANCE PROJECT

Identity Trends in e-Government: Business

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

LIBERTY ALLIANCE PROJECT

Contents

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

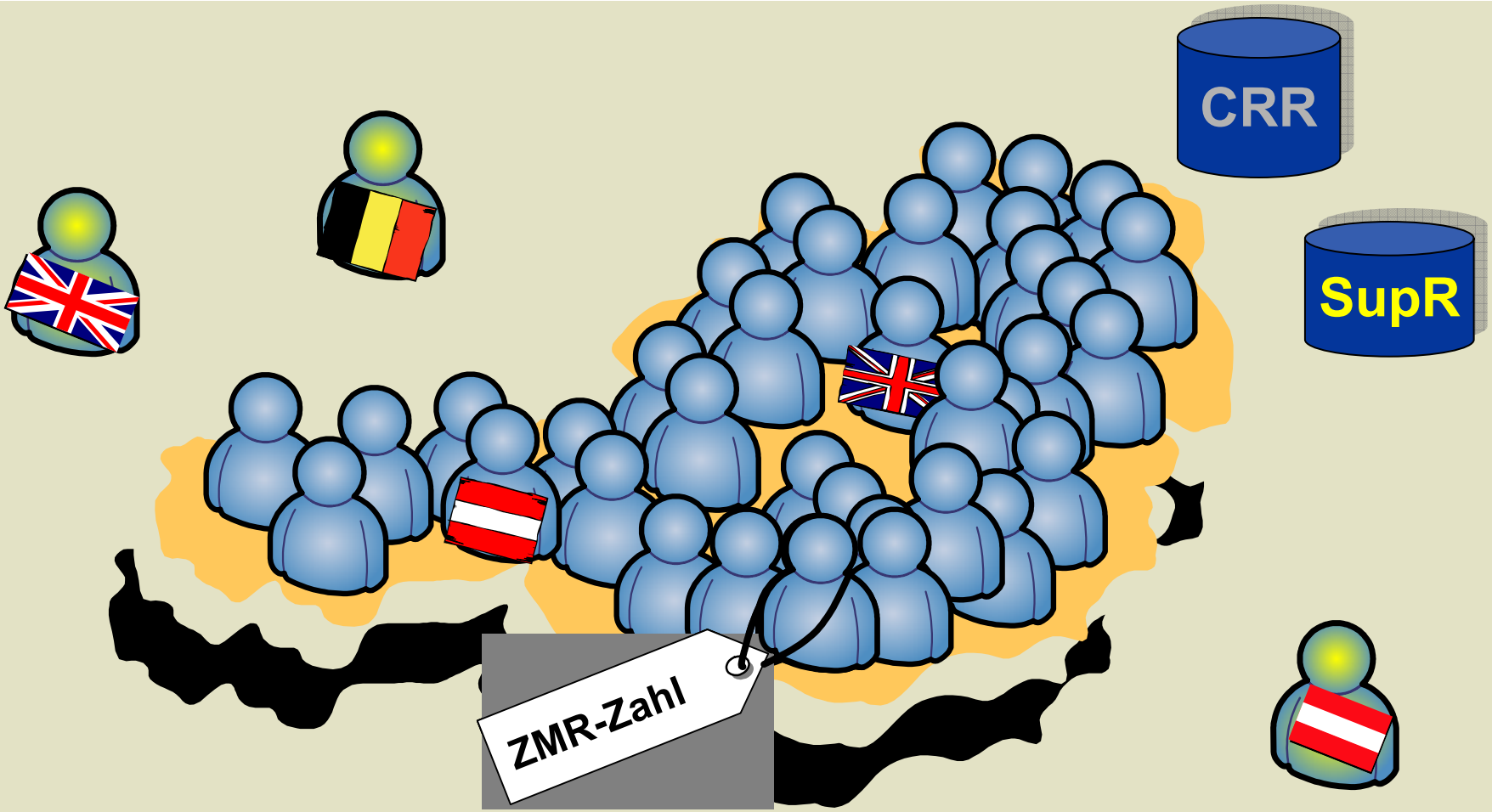
LIBERTY ALLIANCE PROJECT

Contents

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

LIBERTY ALLIANCE PROJECT

Central Register of Residents



Each resident has a unique number „ZMR-Zahl“
in the Central Register of Residents (CRR)

LIBERTY ALLIANCE PROJECT

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)

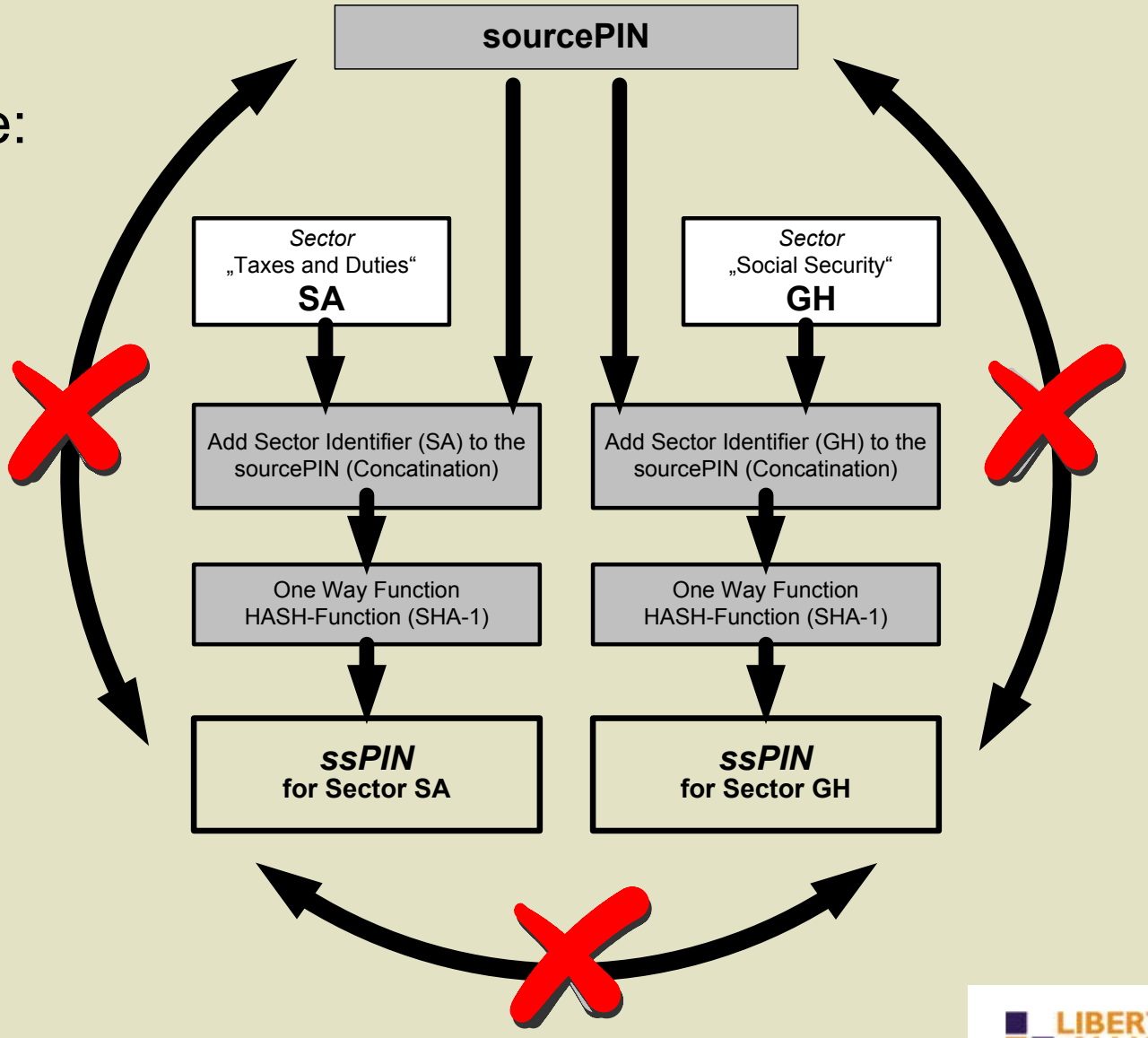
The Austrian Identification System

- 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:



LIBERTY ALLIANCE PROJECT

Contents

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

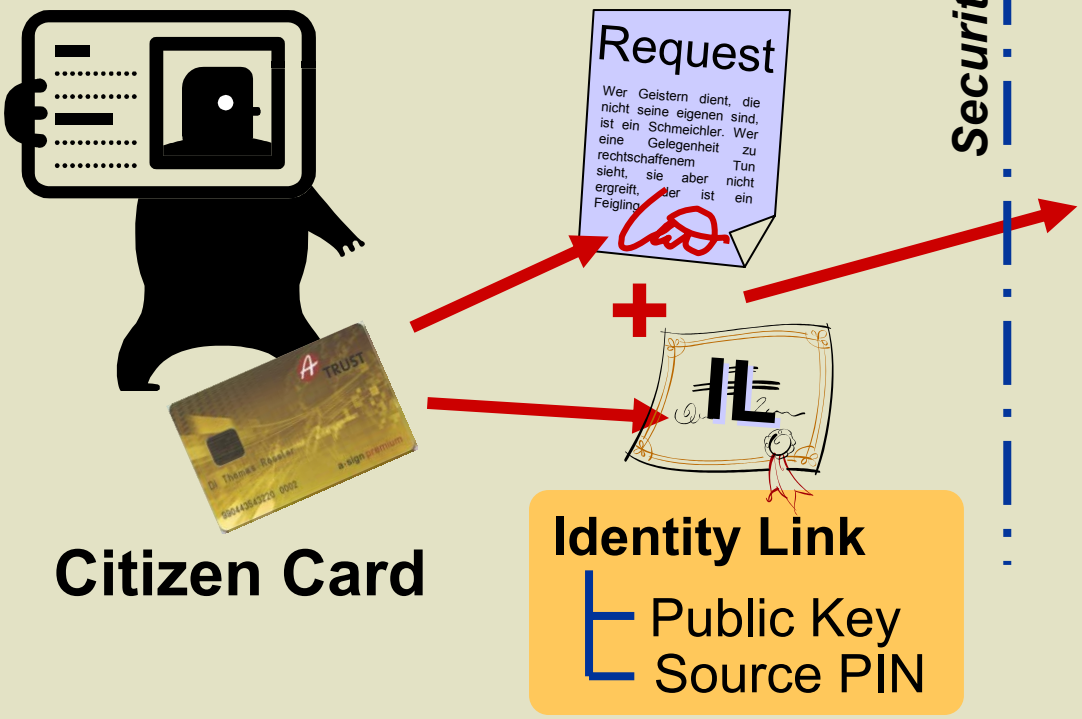
LIBERTY ALLIANCE PROJECT

Citizen Card

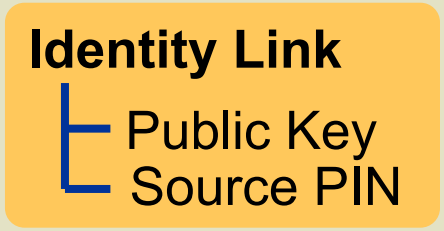
- Citizen Card holds…
  - electronic signatures → **Authentication**
  - electronic identity → **Identification**

Austrian Citizen Card Concept

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



Identity-Link



- 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

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>
      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>
```

Personal Information

+

Citizen‘s Public Key Information

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

Security-Layer: a high-level interface

Open Interface Security Layer

- Simple XML requests via Web browser

```
<?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:Mim
          </sl10:FinalDataMetaInfo>
        </sl10:TransformsInfo>
     </DataObjectInfo>
</CreateXMLSignatureRequest>
```

LIBERTY ALLIANCE PROJECT

Citizen Card is a „Concept“!

- Citizen Card can be and is realised through various technologies:

Signature- Card

Student-Cards

Health-Card

Employee-ID

Bank-Cards

Mobile Phone

LIBERTY ALLIANCE PROJECT

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