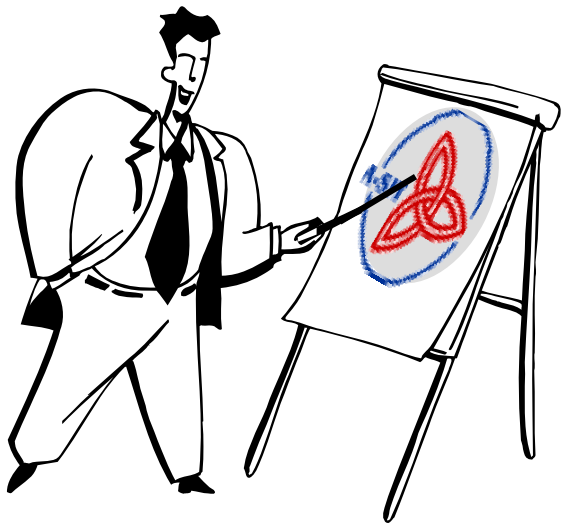
The Austrian Citizen Card

Interoperability and Integration of Technologies

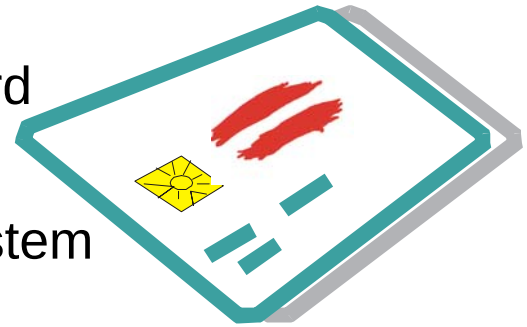
Herbert.Leitold@a-sit.at

Table of Contents



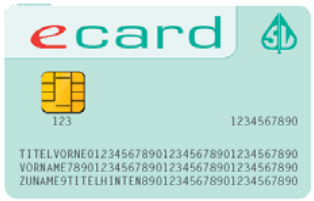
Milestones

- November 2000: Austrian Cabinet Council decision
  … to employ chip-card technology to improve citizen's access to public services; to supplement the planned health insurance card with electronic signatures
- February 2003: 1st Citizen Card
  - Austrian Computer Society membership card
- March 2004: E-Government Act
  - Legal basis of the Identity Management System
- 2005 - 2006
  - several private- and public-sector borne Citizen Card initiatives
  - foreign eID integration (Austrian Presidency event February 2006)



Major initiatives – Citizen Cards

Bank cards (ATM cards)
Each bank card issued since March 2005 is also an SSCD (as of 1999/93/EC)



Health insurance cards:
SSCD, Rollout Mai-Nov. 2005
100 % coverage (8 Mio.) reached end of Nov. 2005

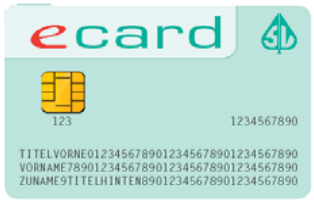
Mobile phones:
each mobile phone
(since March 2004)

Further initiatives:
- CSP signature cards
- Public servant service card
- Student service cards, etc.

ID Cards?

Challenges: Different technologies

Chip-OS: ACOS
Crypto: 192 Bit ECC + 1024 Bit RSA
CA: A-TRUST



Chip-OS: STARCOS
Crypto: 192 Bit ECC for both key-pairs
CA: Main Assoc. of Social Security Organisations

Chip-OS: n/a
Crypto: 2048 Bit RSA
CSP: A1 / A-Trust

Chip-OS: CardOS, STARCOS
Crypto: e.g. 1024 Bit RSA
CSP: A-Trust

Status of foreign eID integration

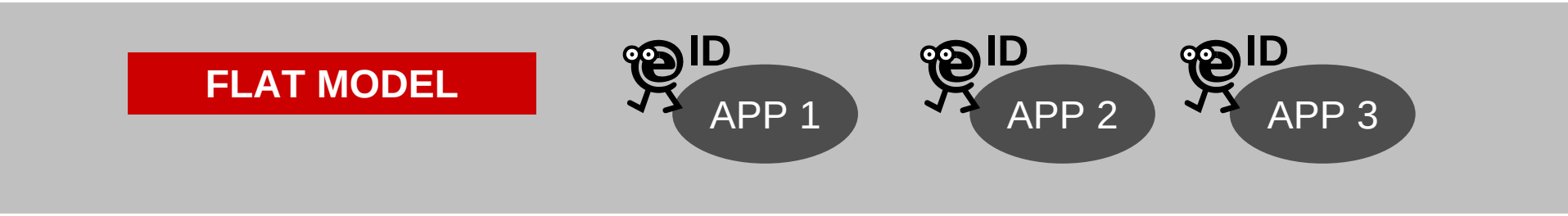
- Integration of foreign eID
  - Belgian, Estonian, Finish, Italian cards already integrated into the IDM concept
  - service started in 02/2006

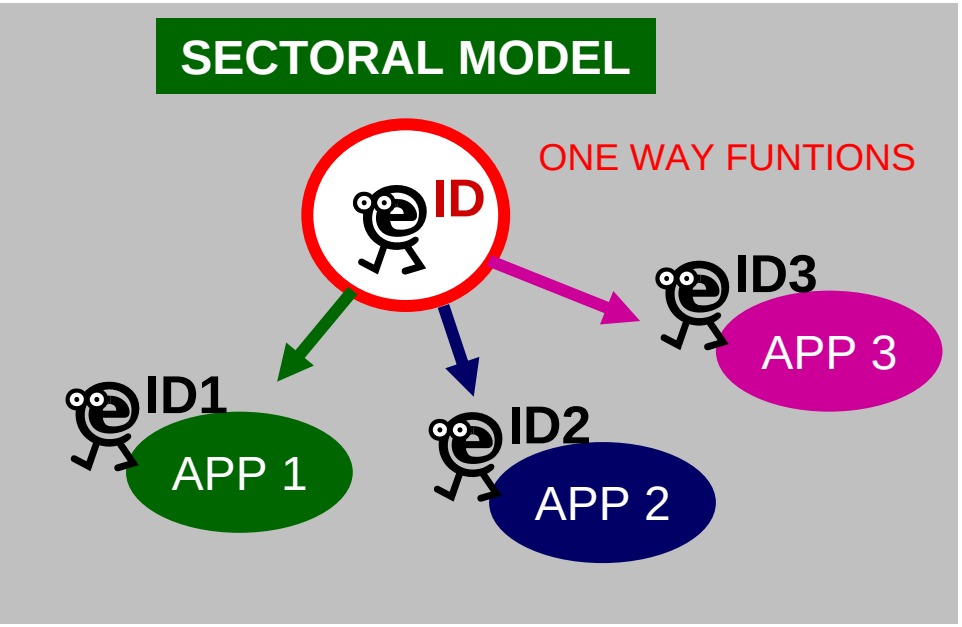
details follow …

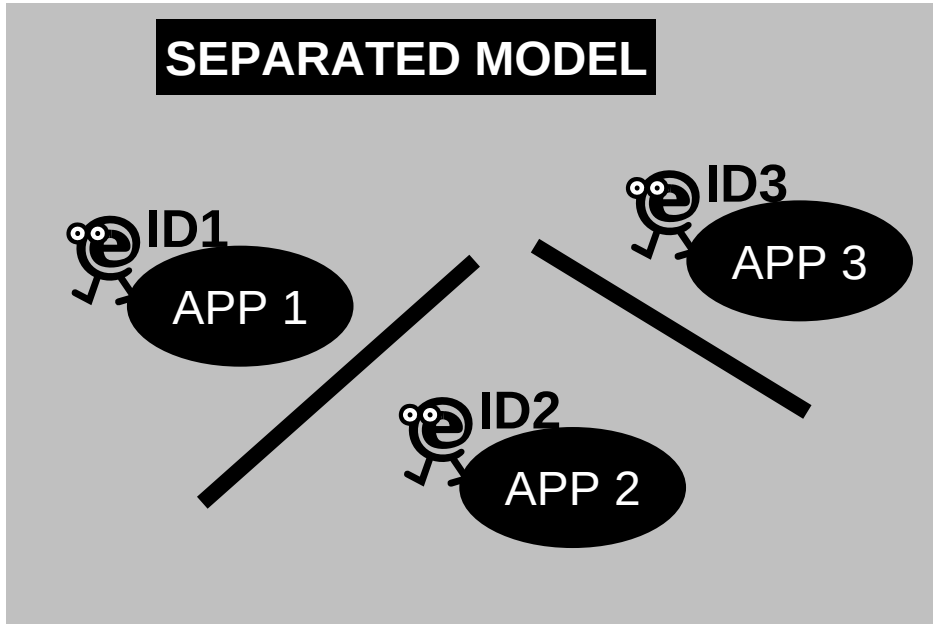
Identification

- IDM models
- eGovernment Registers in Austria
  - Central Register of Residents
  - Supplementary Register
- Sector specific PINs
- Identity Link
  - ID under citizen's control

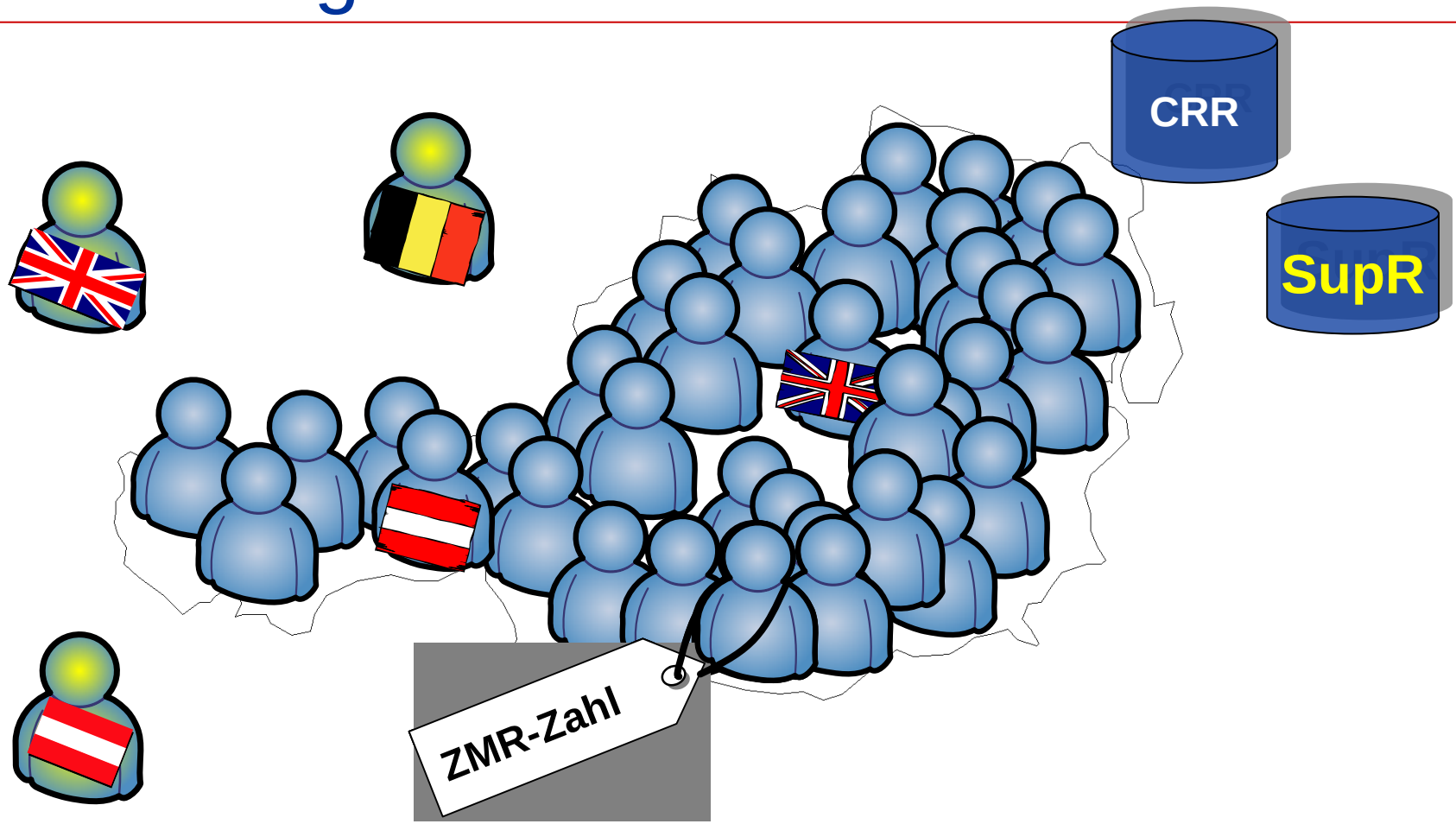
Identity Management Models





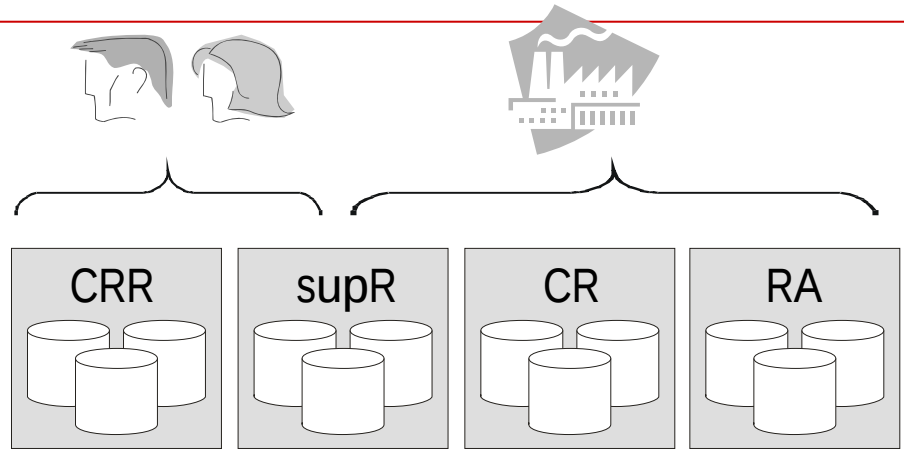


Central Register of Residents



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

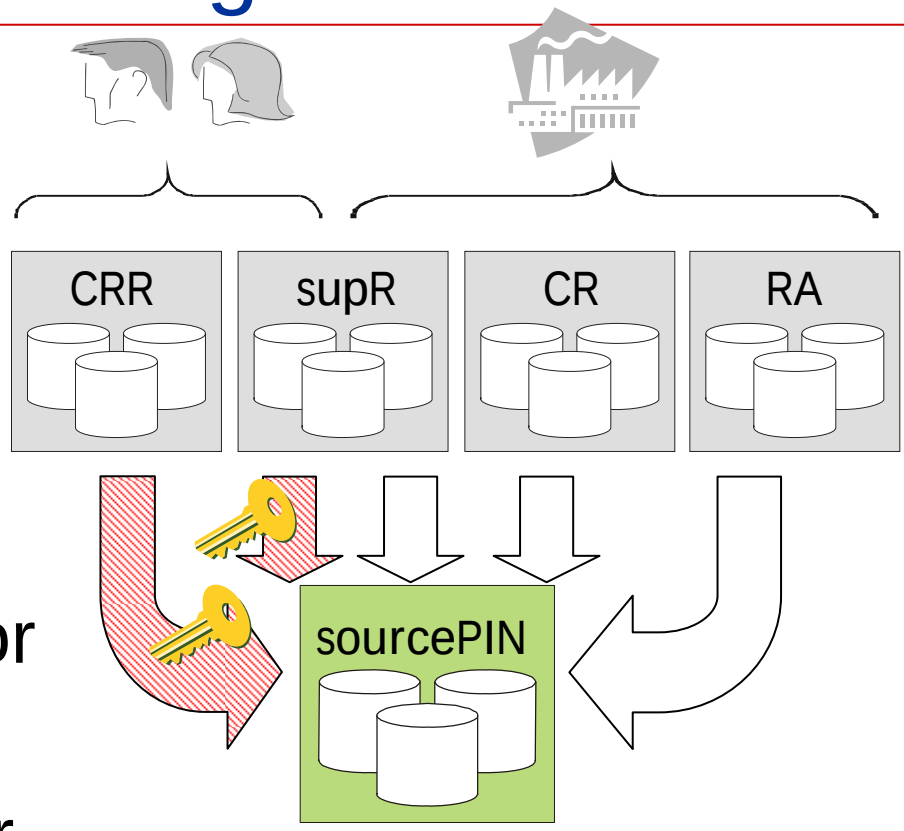
Unique identifiers



- Various unique IDs
  - Central Register of Residents (CRR)
  - Commercial Register (CR)
  - Register of Associations (RA)
  - Supplemental Registers (supR)
    - citizens not enrolled in CRR (e.g., expatriates, foreigners)
    - other concerned parties
- To be combined to a homogeneous system
  - Data-protection to be considered

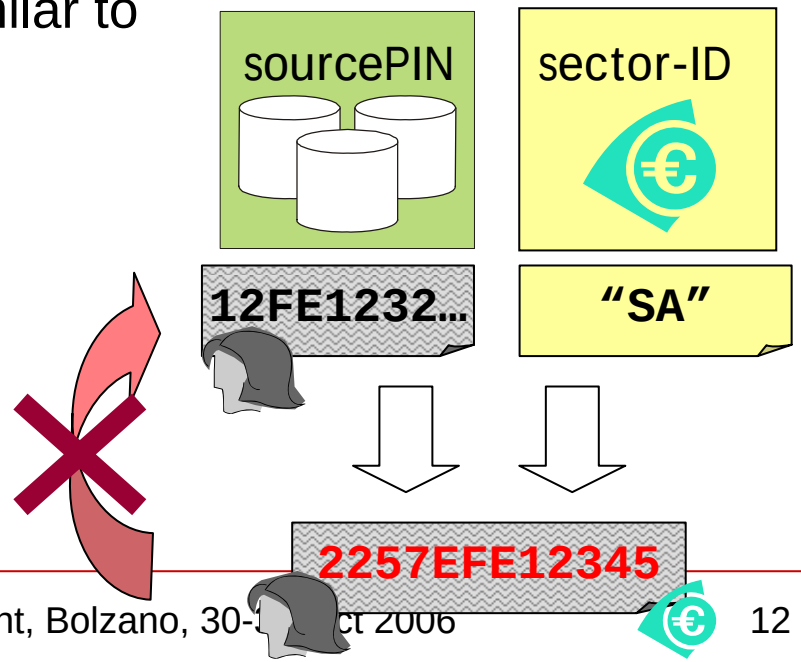
Principal eGovernment registers

- sourcePIN
  - derived from unique IDs
  - strong encryption for physical persons
  - SourcePIN Register Authority is the Data-Protection Commission



Sector-specific personal identifier

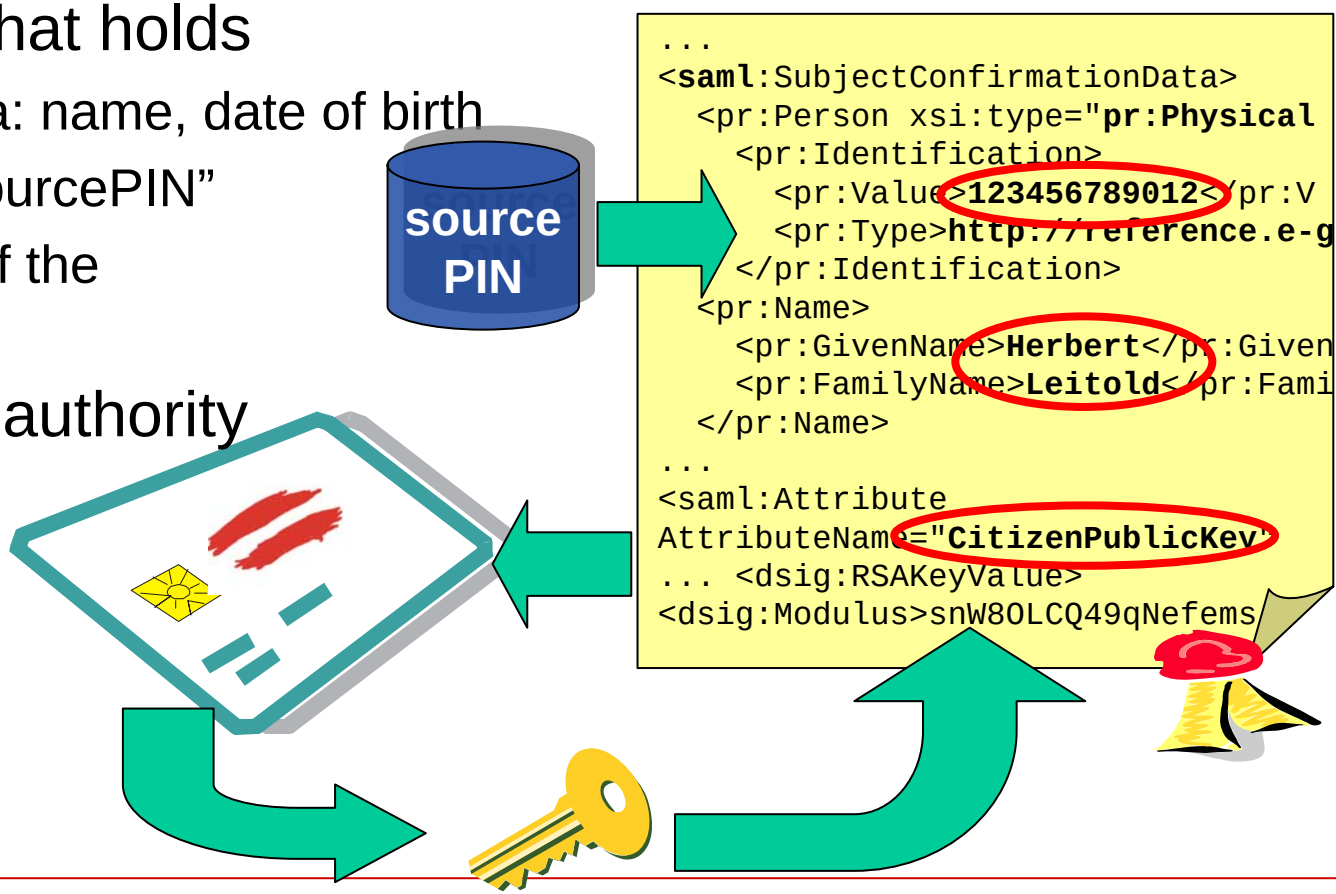
- SourcePIN combined with sector-identifier
  - Citizen uniquely defined within a sector
  - Cryptographic hash-functions
    - one-way function
    - no “back-conversion”
  - Sector-specific IDs (ssPIN) similar to
    - tax number in treasury
    - social security number in health care, etc.
- Cross-search prevented
  - lawful generation of ssPIN possible (SourcePIN Register)



Identity Link

- XML data structure stored in the Citizen Card that holds
  - personal data: name, date of birth
  - unique ID “sourcePIN”
  - public keys of the certificates

  signed by the authority
- Based on SAML



ssPIN calculation example

SourcePIN: **MDEyMzQ1Njc4OWFiY2RlZg==**

ssPIN Taxes

Sector: SA
Hash-Inpput: MDEyMzQ1Njc4OWFiY2RlZg==+urn:publicid:gv.at:cdid+SA
ssPIN (HEX) : 4f 2d 1c f2 c4 4c a4 b3 9c 1a 66 85 5b 2d e2 24 f7 bb c5 97
ssPIN (Base64): **Ty0c8sRMpLOcGmaFWy3iJPe7xZc=**

ssPIN Construction and living

Sector: BW
Hash-Inpuit: Qq03dPrgcHsx3G0lKSH6SQ==+urn:publicid:gv.at:cdid+BW
ssPIN (HEX) : 8f f3 71 75 14 21 a7 eb 4d c8 4f 56 84 77 41 49 8b b2 de 10
ssPIN (Base64): **j/NxdRQhp+tNyE9WhHdBSYuy3hA=**

Integration of technologies

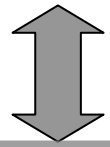
- Definitions
  - Security Layer
  - Citizen Card Environment
- Basic Functions
  - Major standards

Two definitions

- **Security Layer:**
  An interface that provides a logical view to the Citizen Card

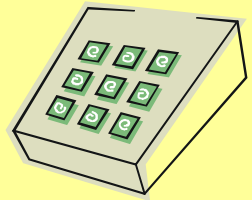
- **Citizen Card Environment:**
  Implementation of the interface
  - Usually a combination of software and hardware elements
  - clear responsibility / liability (signature law)

Security layer



Open Interface Security Layer

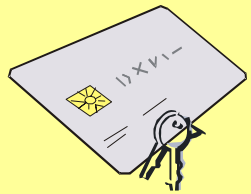
PIN pad

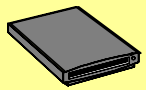


Hash function

trustw. viewer

card-interface (e.g. PKCS#11)

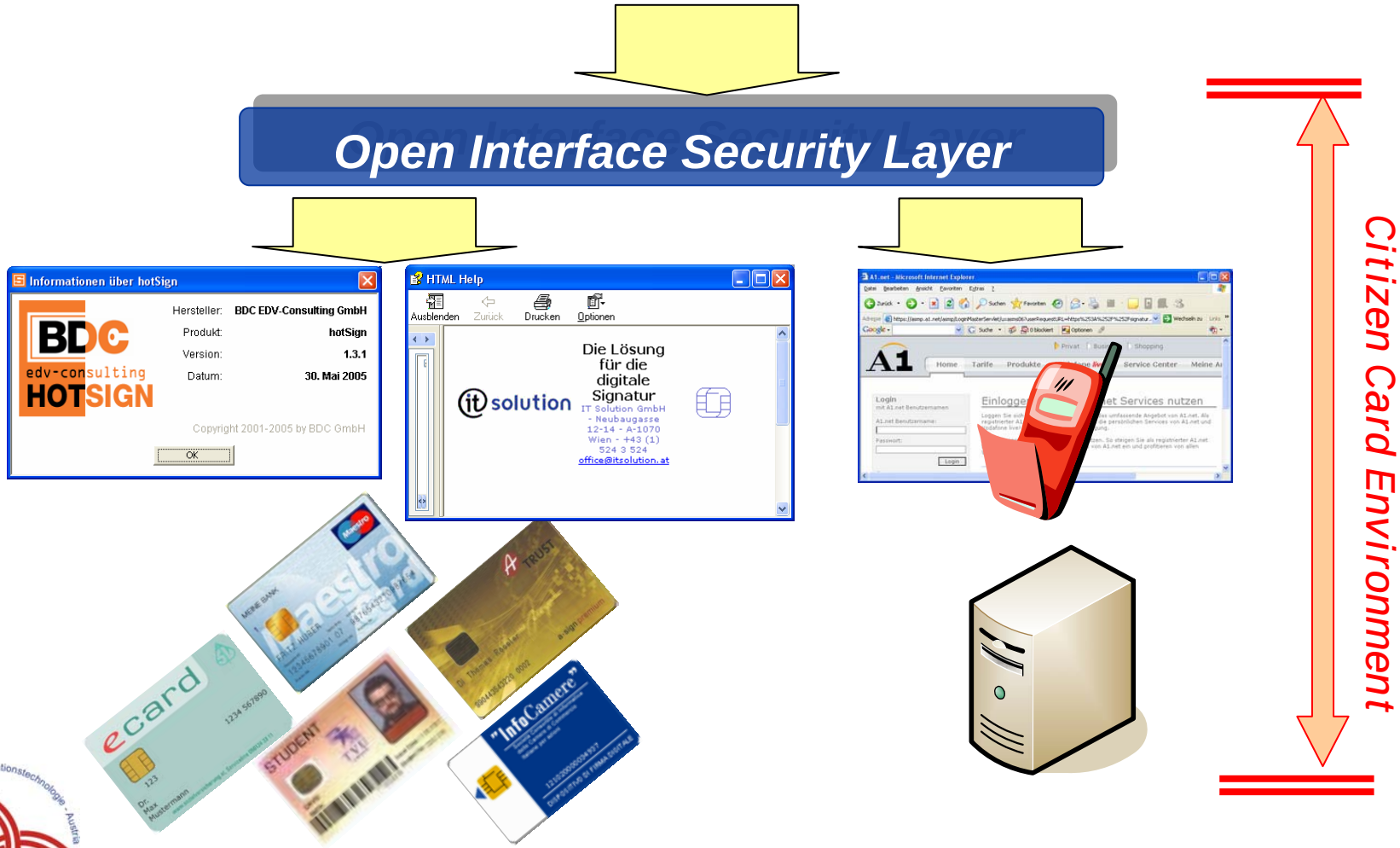




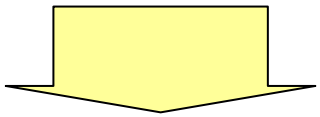
add. memory

Citizen Card Environment

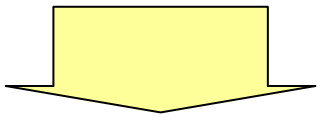
Integration of Technologies

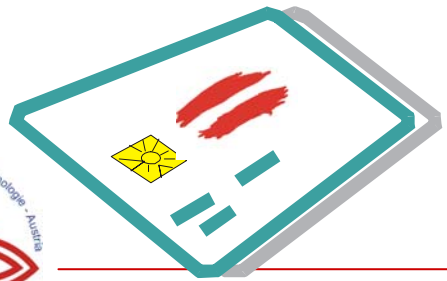


High-level interface



Open Interface Security Layer





- Simple XML requests via Web browser

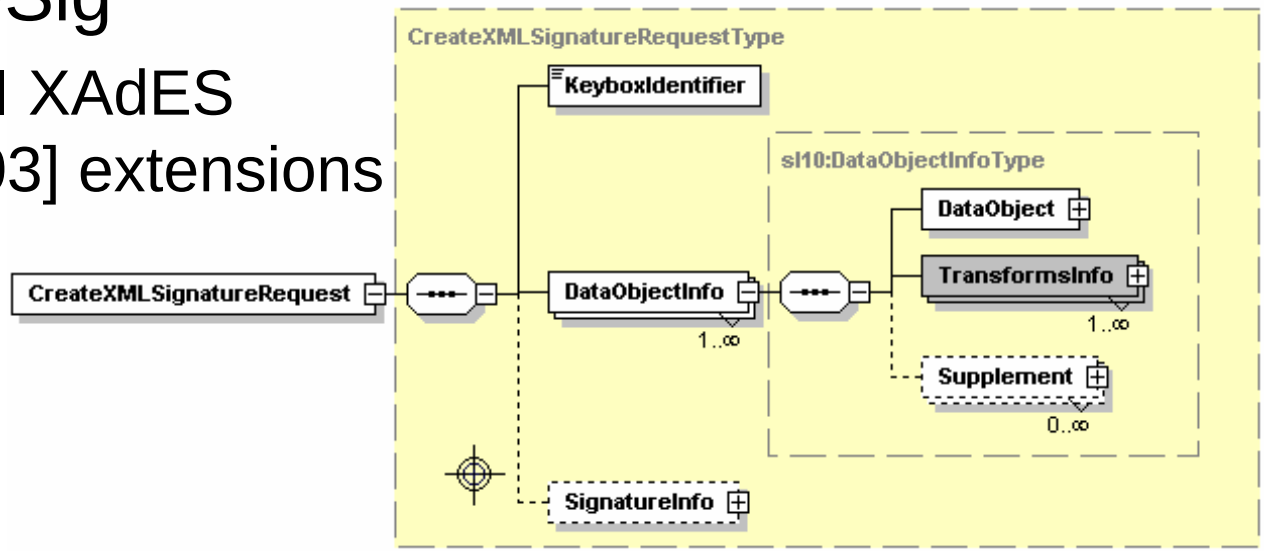
```
<?xml version="1.0" encoding="UTF-8"?>
<CreateXMLSignatureRequest xmlns="http://www.cio
     <KeyboxIdentifier>SecureSignatureKeypair</K
     <DataObjectInfo Structure="enveloping">
          <sl10:DataObject>
             <sl10:XMLContent>Data to be signed
             </sl10:XMLContent>
      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

Citizen Card functions

- Citizen Card defines general requirements
  - secure electronic signatures
    - i.e., legal equivalence to handwritten signatures
  - additional key-pairs
    - ‘general signatures’, encryption
  - info-boxes to store data
    - identity link, certificates, mandates/representation
    - access control to info-boxes

Example electronic signatures

- Signature-creation and validation
  - CMS [RFC3389, PKCS#7]
    - Some ETSI CAdES [TS 101733] extensions
  - W3C XMLDSig
    - some ETSI XAdES [TS 101903] extensions



Alien eID integration

- Austrian Approach
  - Definitions
  - Recurring Identity
  - Substitute SourcePIN

Definitions of Identity

- Austrian E-Government Act

"**Unique identity**": designation of a specific person (data subject, No 7) by means of one or more features enabling that data subject to be unmistakably distinguished from all other data subjects;

"**Recurring identity**": designation of a specific person in a way which, while not ensuring unique identity, enables this person to be recognised by reference to a previous event, such as an earlier submission;

Substitute sourcePIN

- Legal basis in SourcePIN Authority Regulation
  - Requires advanced electronic signature
- Signed request containing
  - Name, date of birth, address
  - Serial Number of the certificate
- “Substitute SourcePIN” calculated from
  - either: name, DOB, address, cert.-serial number
  - or: foreign identity number

Demonstrator available for ...

- Finish eID

serial number + name + DOB

SHA-1

FI:KLFGd24563...

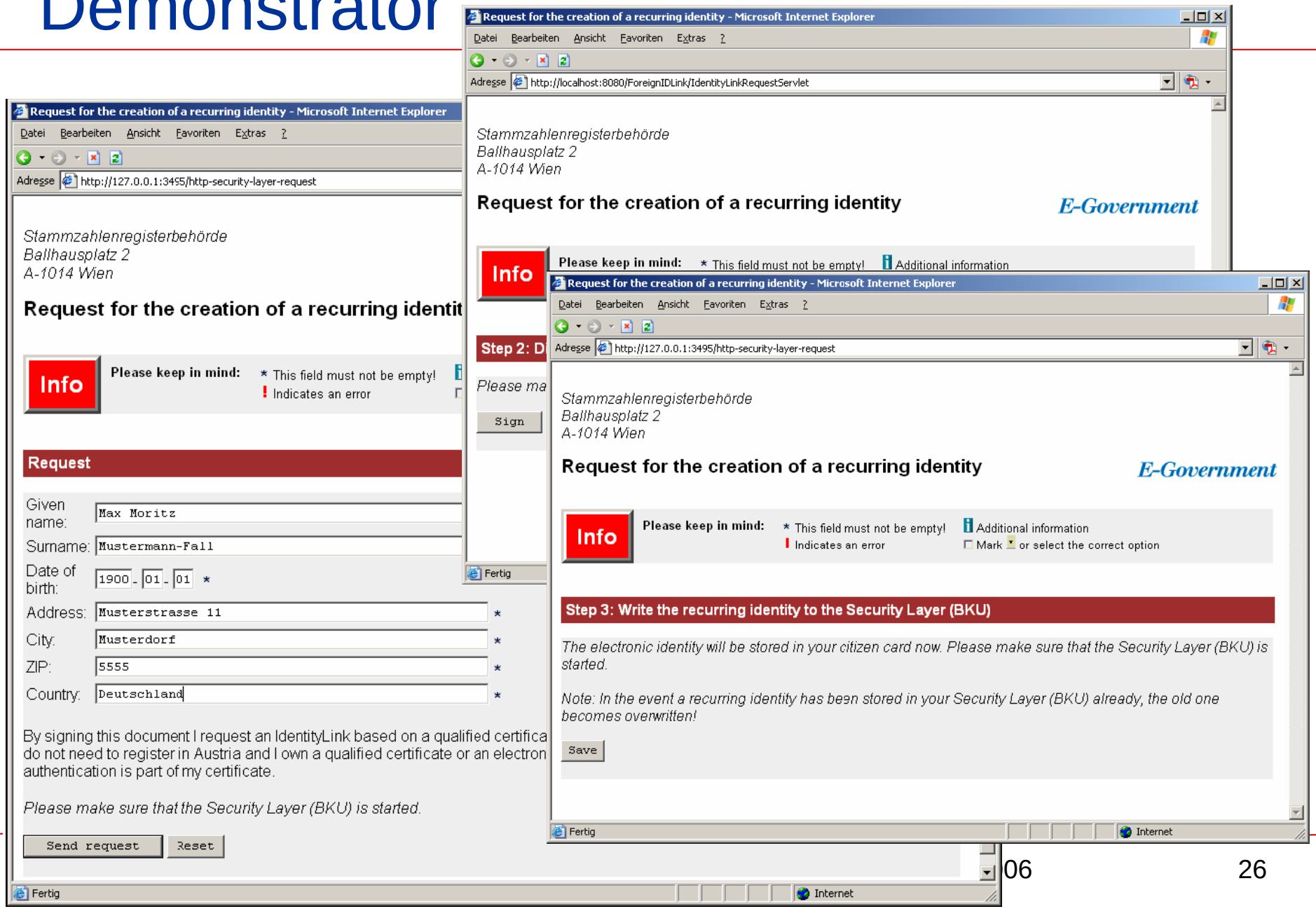
- InfoCamere

codice fiscale

SHA-1

IT:98RDsTf12h..

Demonstrator



Modules for Online-Applications (MOA)

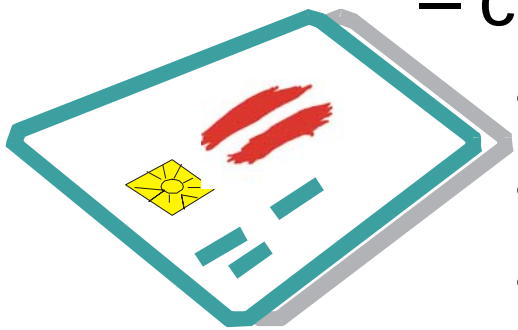
- Open Source Modules
  - MOA–ID, MOA-wID: Identification
  - MOA–SS: server-signatures
  - MOA–SP: signature-validation
  - MOA–ZS: electronic delivery
  - MOA–VV: mandates, representation

for server-side integration

Conclusions

Austrian Citizen Card

- follows technology-neutral approach
- combines basic functions
  - identification
  - authentication
  - mandates
  - identity link
  - electronic signature



- data protection maintained using sector-specific fractional PINs
- demos for alien eID integration

Thank you for Your attention!

http://www.a-sit.at
http://www.buergerkarte.at

Herbert.Leitold@a-sit.at