eID in Austria

THE CITIZEN CARD

Adaptive Organization for a Change
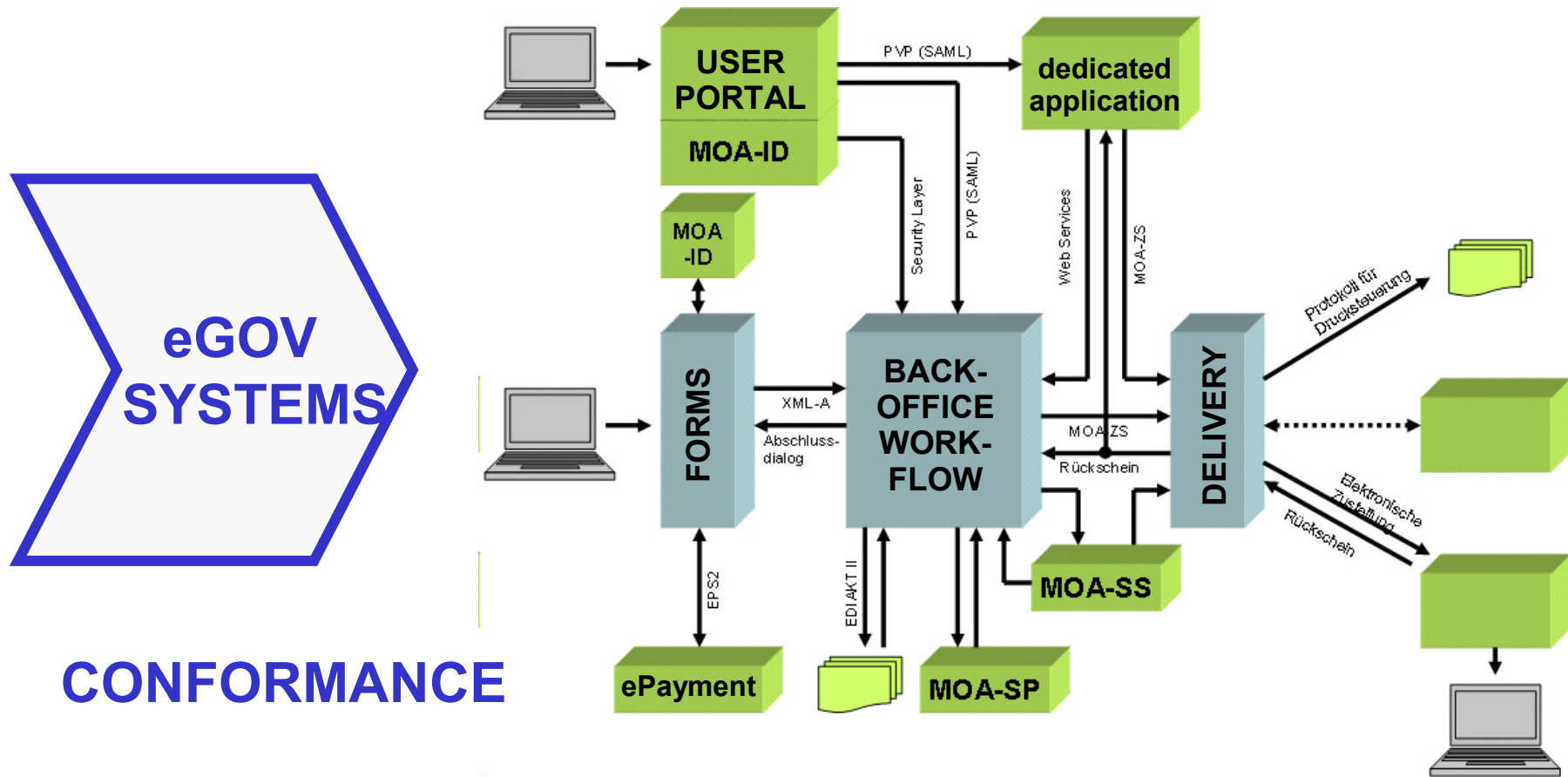
**ORGANISATION FOR
A TRANSFORMATION**

① ② ④

European cooperation

strategy: CIO for the federal government

RESULT

ICT – Federal Level

implementation:
executive secretary

⑪ **cooperation with regional and local level and with industry**

⑬

**ICT
2005+**

2001 → 2002 → 2003 → 2004 → 2005 → 2006 →
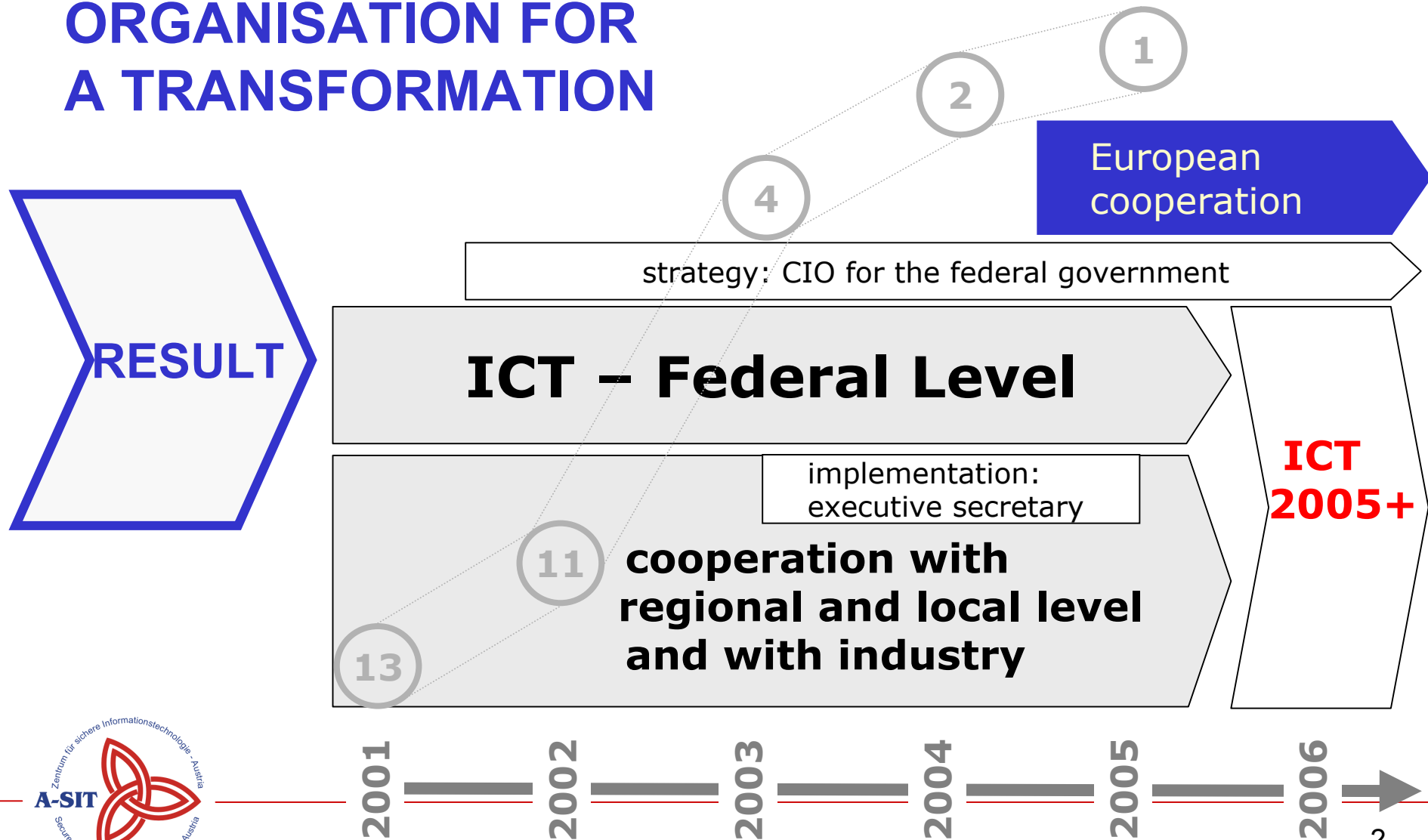
Consolidated Result of ICT - Strategy

Platform
Digital Austria

Federal
CIO

PEOPLE

FEDERAL
ICT-Strategy

Public
Relations

Law, Organization;
International relations

Program-
Project management

ICT-Infrastructure

EGIZ
eGovernment
innovation center
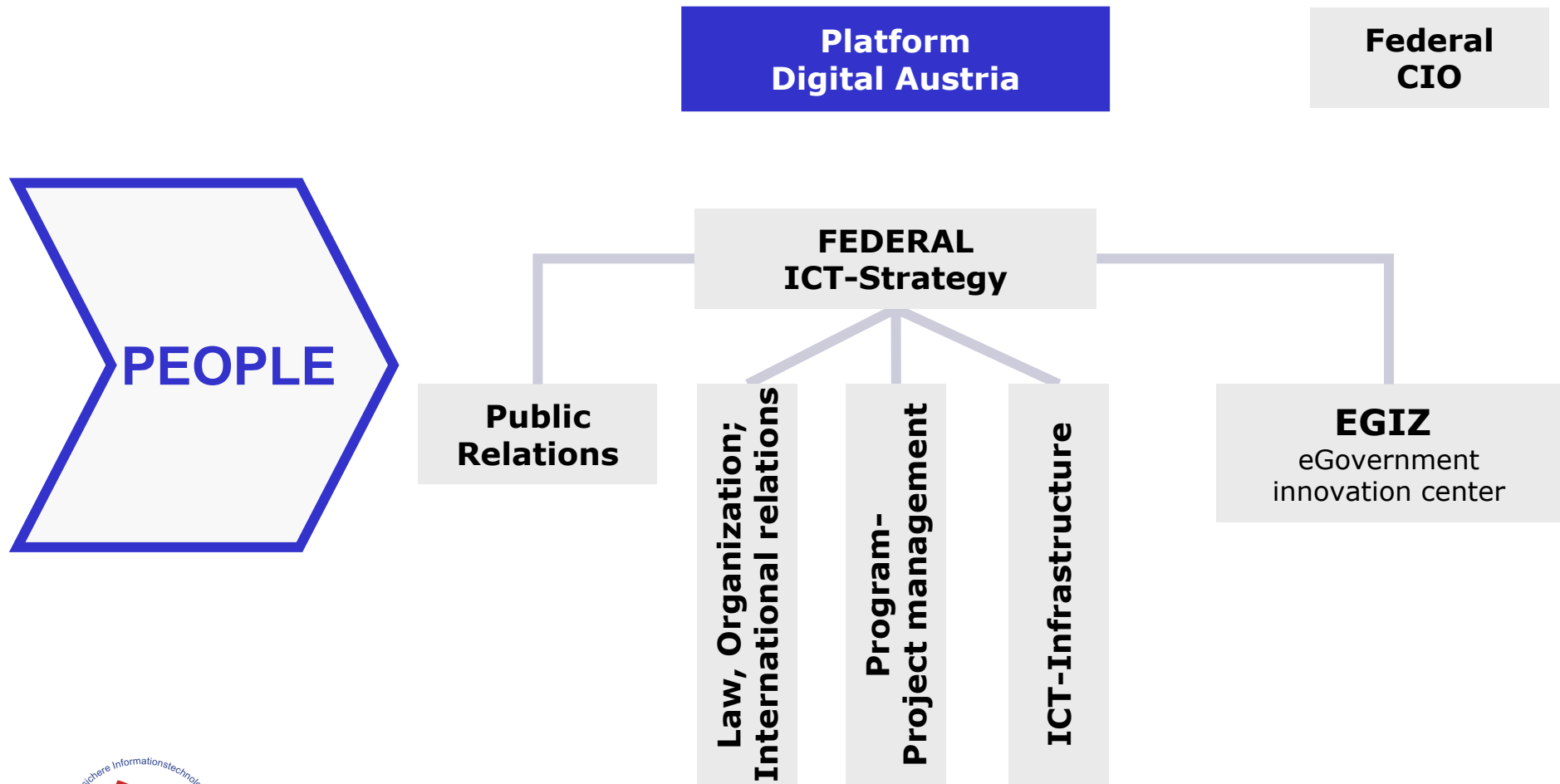
Transparent Overall Structure

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
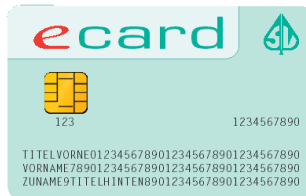 - foreign eID integration (Austrian Presidency event February 2006)
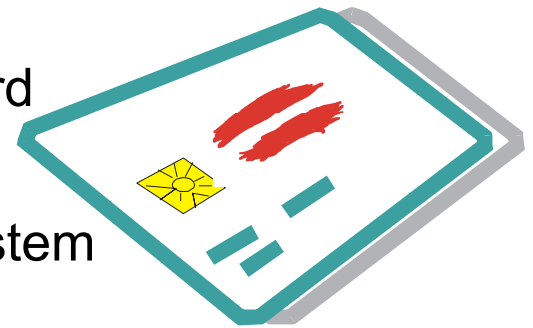
Major initiatives – Citizen Cards

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?

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

Identification

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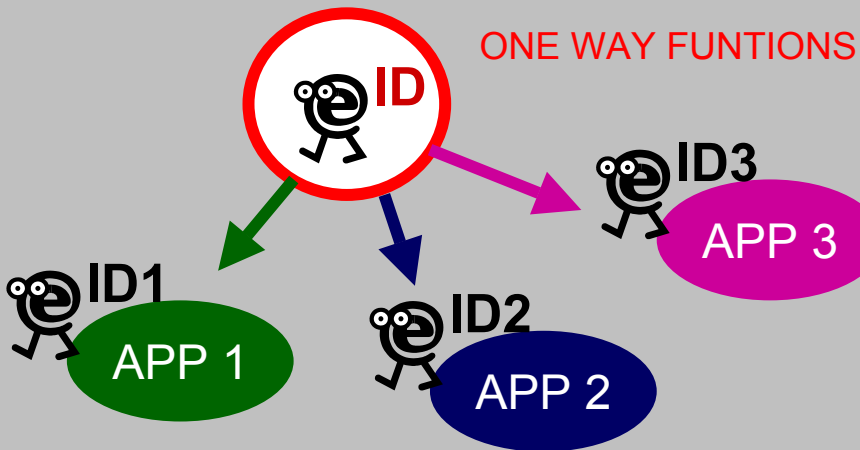- Identity Link
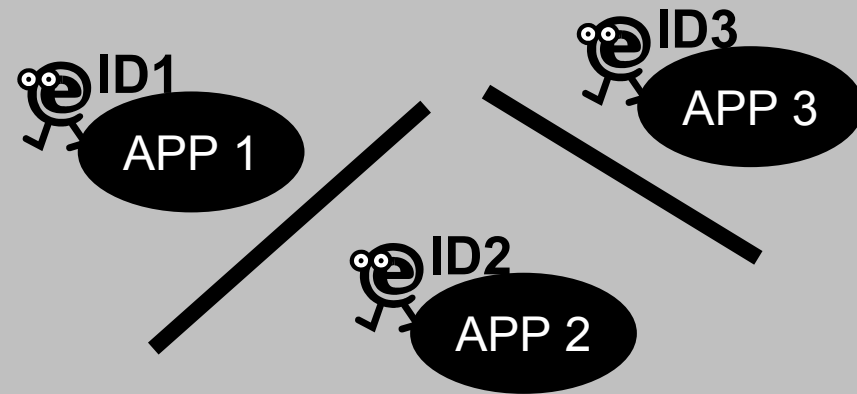 - ID under citizen's control

Identity Management Models

FLAT MODEL

ID APP 1
ID APP 2
ID APP 3

SECTORAL MODEL

ONE WAY FUNTIONS

ID

ID3 APP 3

ID1 APP 1

ID2 APP 2

SEPARATED MODEL

ID1 APP 1

ID3 APP 3

ID2 APP 2
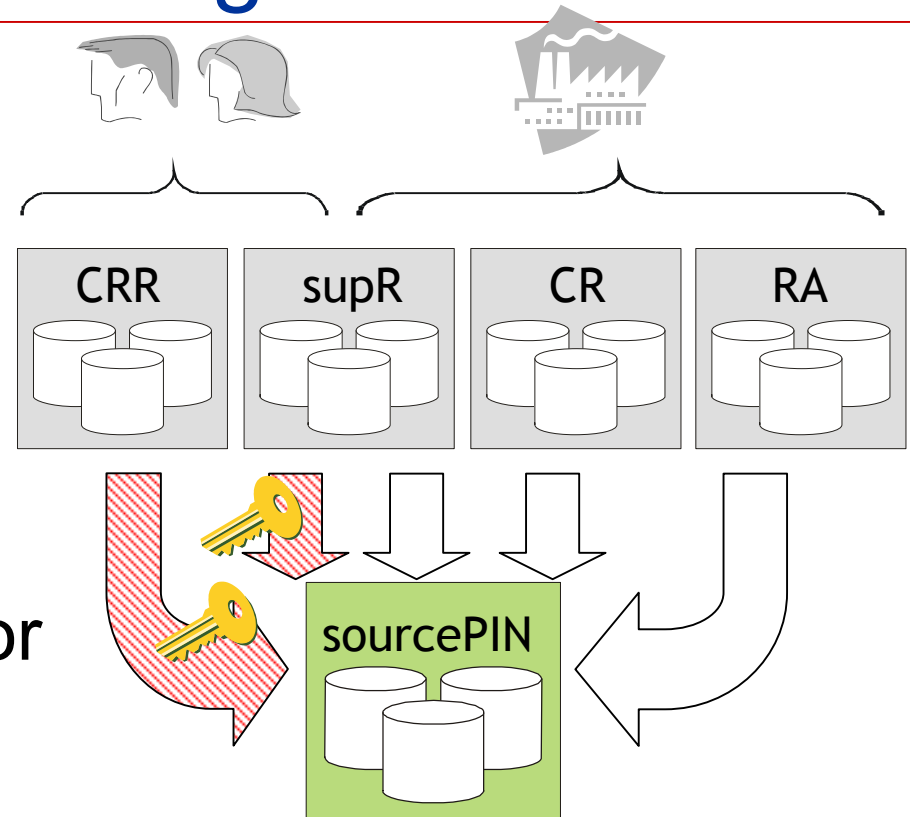
Principal eGovernment registers

- **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)

sourcePIN

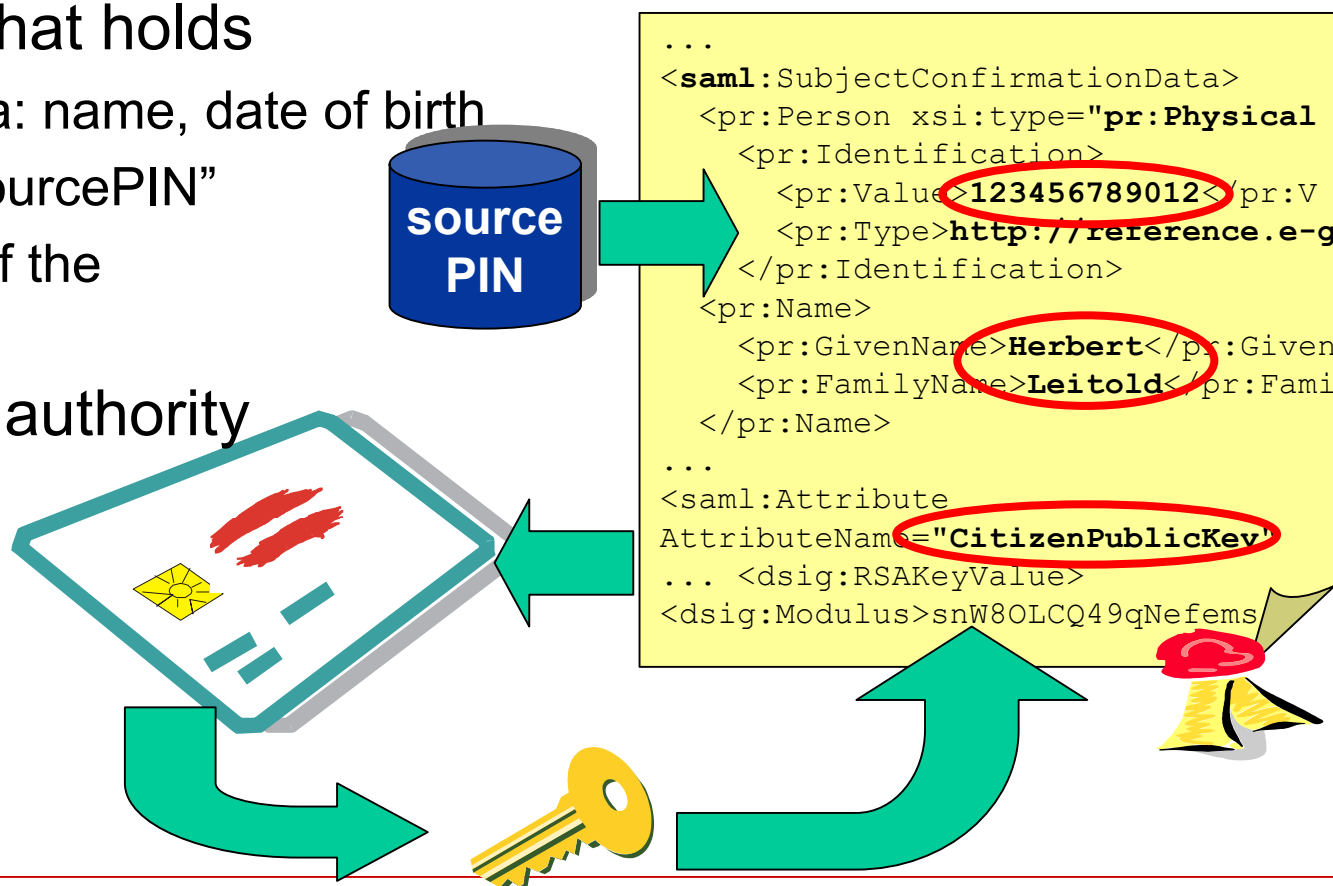sector-ID

`12FE1232…`

`"SA"`

`2257EFE12345`
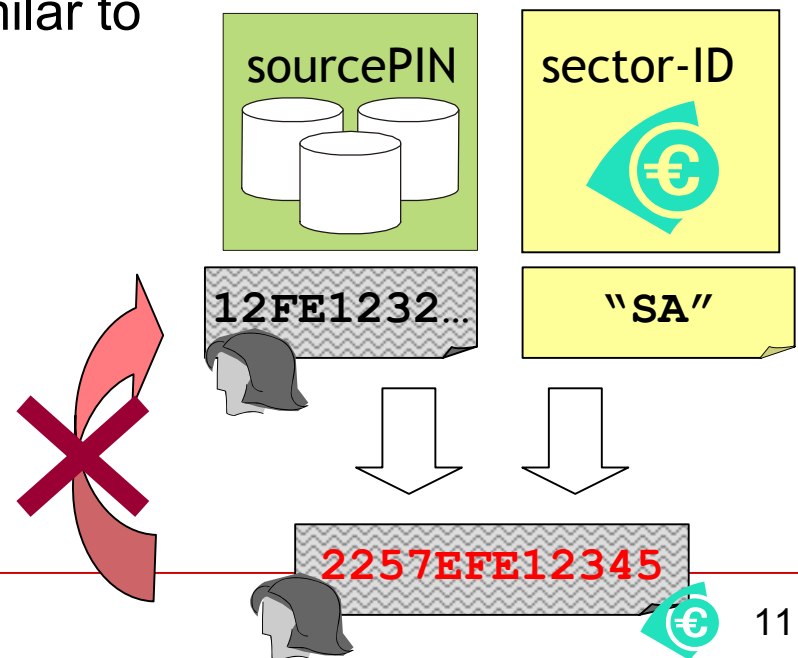
Identity Link

- 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

sourcePIN

```
...
<saml:SubjectConfirmationData>
  <pr:Person xsi:type="pr:Physical
    <pr:Identification>
      <pr:Value>123456789012</pr:V
      <pr:Type>http://reference.e-g
    </pr:Identification>
  <pr:Name>
    <pr:GivenName>Herbert</pr:Given
    <pr:FamilyName>Leitold</pr:Fami
  </pr:Name>
...
<saml:Attribute
AttributeName="CitizenPublicKey"
... <dsig:RSAKeyValue>
<dsig:Modulus>snW8OLCQ49qNefems
```

A-SIT
Zentrum für sichere Informationstechnologie Austria
Secure Information Technology Center - Austria
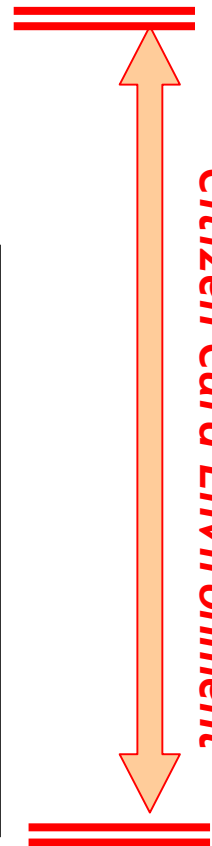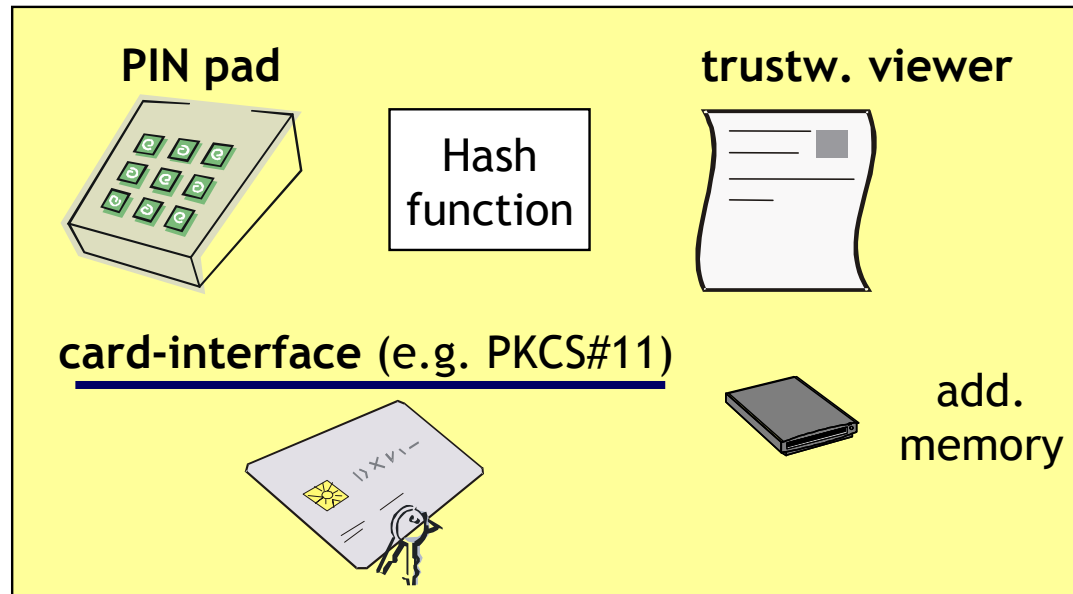
Integration of technologies

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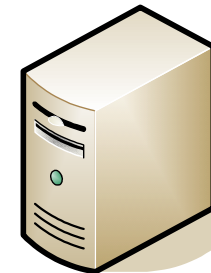- Basic Functions
  - Major standards

Security layer

Open Interface Security Layer

PIN pad

Hash function

trustw. viewer

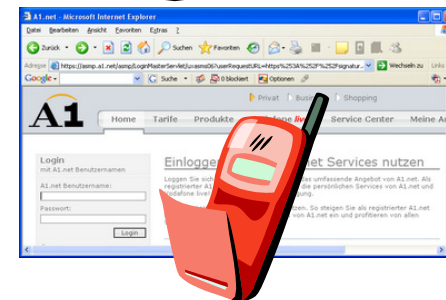**card-interface** (e.g. PKCS#11)

add. memory

Citizen Card Environment

Integration of Technologies

Open Interface Security Layer

Citizen Card Environment

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
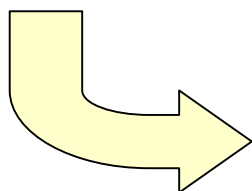   - access control to info-boxes

Alien eID integration

- **Austrian Approach**
  - Definitions
  - Recurring Identity
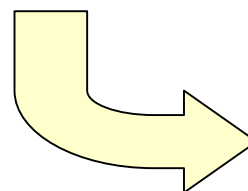 - Substitute SourcePIN

Demonstrator available for …

- Finish eID
- InfoCamere

serial number + name + DOB
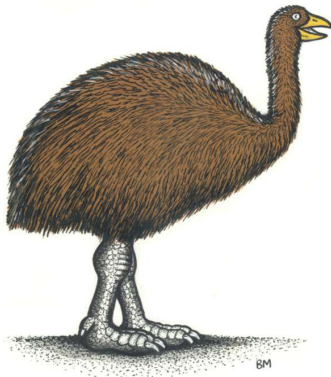
SHA-1

FI:KLFGd24563...

codice fiscale

SHA-1

IT:98RDsTf12h..

Modules for Online-Applications (MOA)
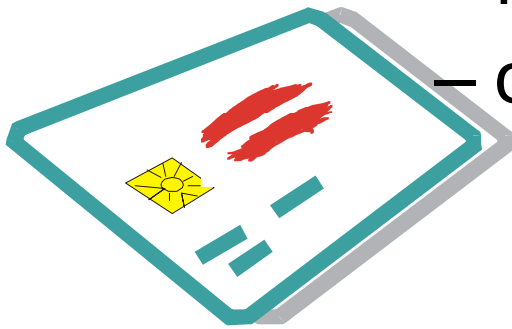

- Open Source Modules
  - MOA–ID, MOA-wID: Identification
  - MOA–SS: server-signatures
  - MOA–SP: signature-validation
  - MOA–ZS: electronic delivery
  - MOA–VV: mandates, representation

  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
- **STRATEGY IS KEY**

A-SIT
Zentrum für sichere Informationstechnologie - Austria
Secure Information Technology Center - Austria