



**Zentrum für sichere Informationstechnologie – Austria**  
**Secure Information Technology Center - Austria**

A-1040 Wien, Weyringergasse 35  
Tel.: ++43 1 – 503 19 63 – 0  
Fax: ++43 1 – 503 19 63 – 66

A-8010 Graz, Inffeldgasse 16a  
Tel.: ++43 316 – 873 5514  
Fax: ++43 316 – 873 5520



# eID – the future in Europe?

Prof. Dr. Reinhard Posch

# eID and the business

- We need an model accepted throughout Europe
- Data protection versus identification
- Availability
- Legal certainty
- Ease of use



# Who should provide eID

**PUBLIC  
SECTOR**

**PRIVATE  
SECTOR**

**IDENTITY BASE**



The Identity base has to be provided or recognized by the authority.

Methods and tools for authentication (proof of identity) can be supplied by the public sector or the private sector.

**CLEARLY DISINGUISH IDENTIFICATION -- AUTHENTICATION**

# Use of eID

## Within administration:

- in order to provide more efficient procedures and to avoid extensive data to be collected

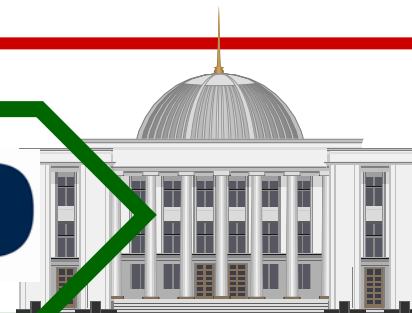


@ID



## Access to e-gov:

- in order to facilitate e-government and transformation (automated procedures)



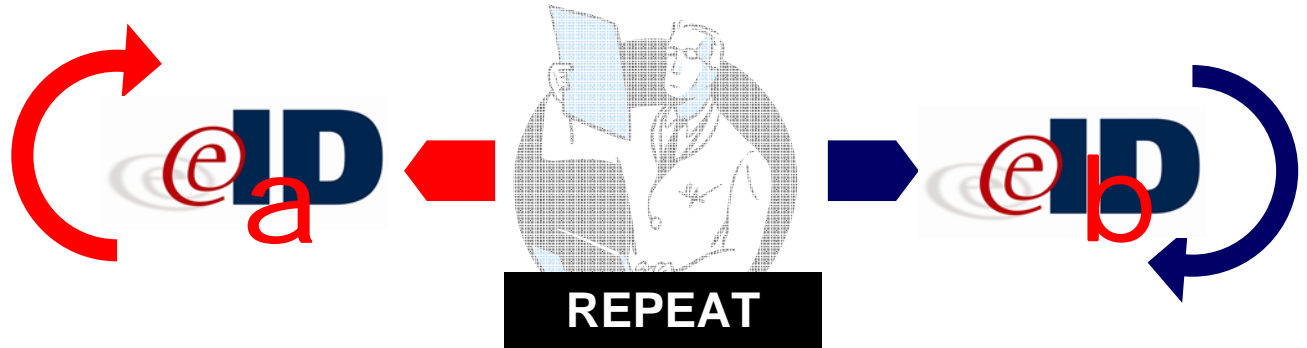
## Access to e-business:

- in order to raise quality trust and security by profiting from public sector

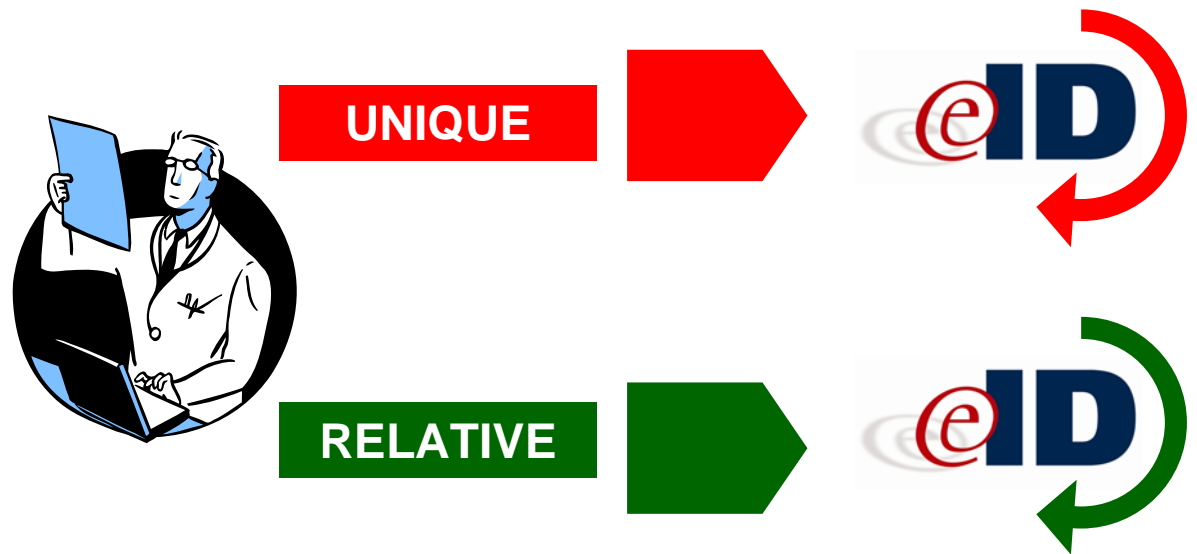


# Use of eID

Use of an eID to proof that the same entity is acting again.  
**E.G. BUSINESS APPLICATION**



Use of an eID to proof that the this is the very person.  
**E.G. SENSITIVE INFORMATION**



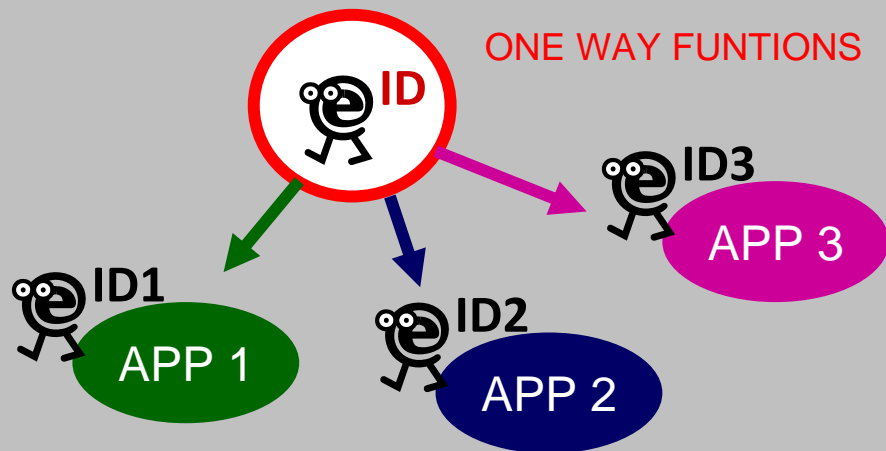
Use of an eID in a given context  
**E.G. WITHIN A MEMBERSTATE**

# eID and Data Protection

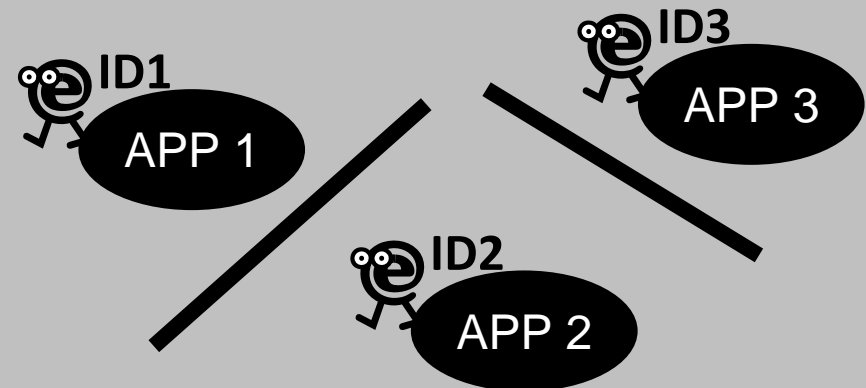
## FLAT MODEL



## SECTORAL MODEL



## SEPARATED MODEL



A European eID model must coexist with all three models not :: compromising privacy

**eID MUST NOT ADD ADDITIONAL PRIVACY RISKS TO EXISTING APPLICATIONS**

# we need an interoperability model

## FLAT MODEL

to preserve the  
simplicity of applications



## SECTORAL MODEL

to ensure the functionality  
and the data protection  
features



## SEPARATED MODEL

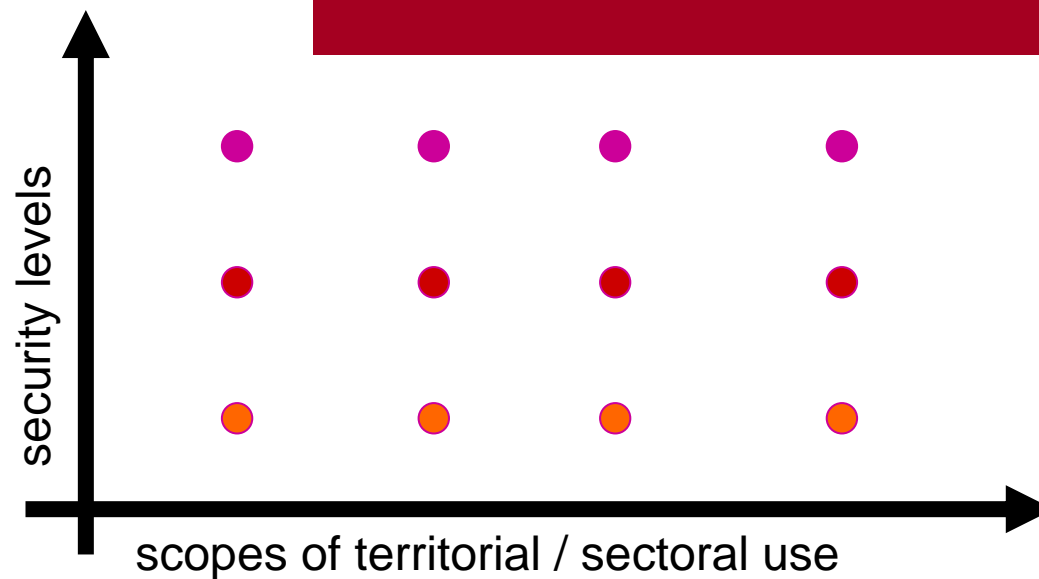
not to infringe with  
the data protection  
through interoperation



**INTEROPERABILITY IS KEY :: IT COMPRISES eID AND eDOCs  
e.g. eProcurement**

# Levels & scope of eID

To decrease barriers and to increase acceptance and use different levels might be helpful



Increasing either dimension might make interoperability more unlikely

We have to develop local views on the identification model to make interoperability happen



# Interoperability and functional inheritance

- We need to benefit from a federated system in many administrative procedures
  - passports
  - documents
  - number plates
  - drivers license
  - ..

**To ensure success of  we must yield maximum benefit through inheritance in terms of functionality and trust**

# Technology is a question of secondary order

- Smart cards
- Mobile phones
- Special tokens (e.g. RSA)
- Several technology avenues to ensure sustainability with rapid innovation

*duration of identity exceeds  
lifetime of tokens and technologies  
there might be several physical  
representations of an identity in question*

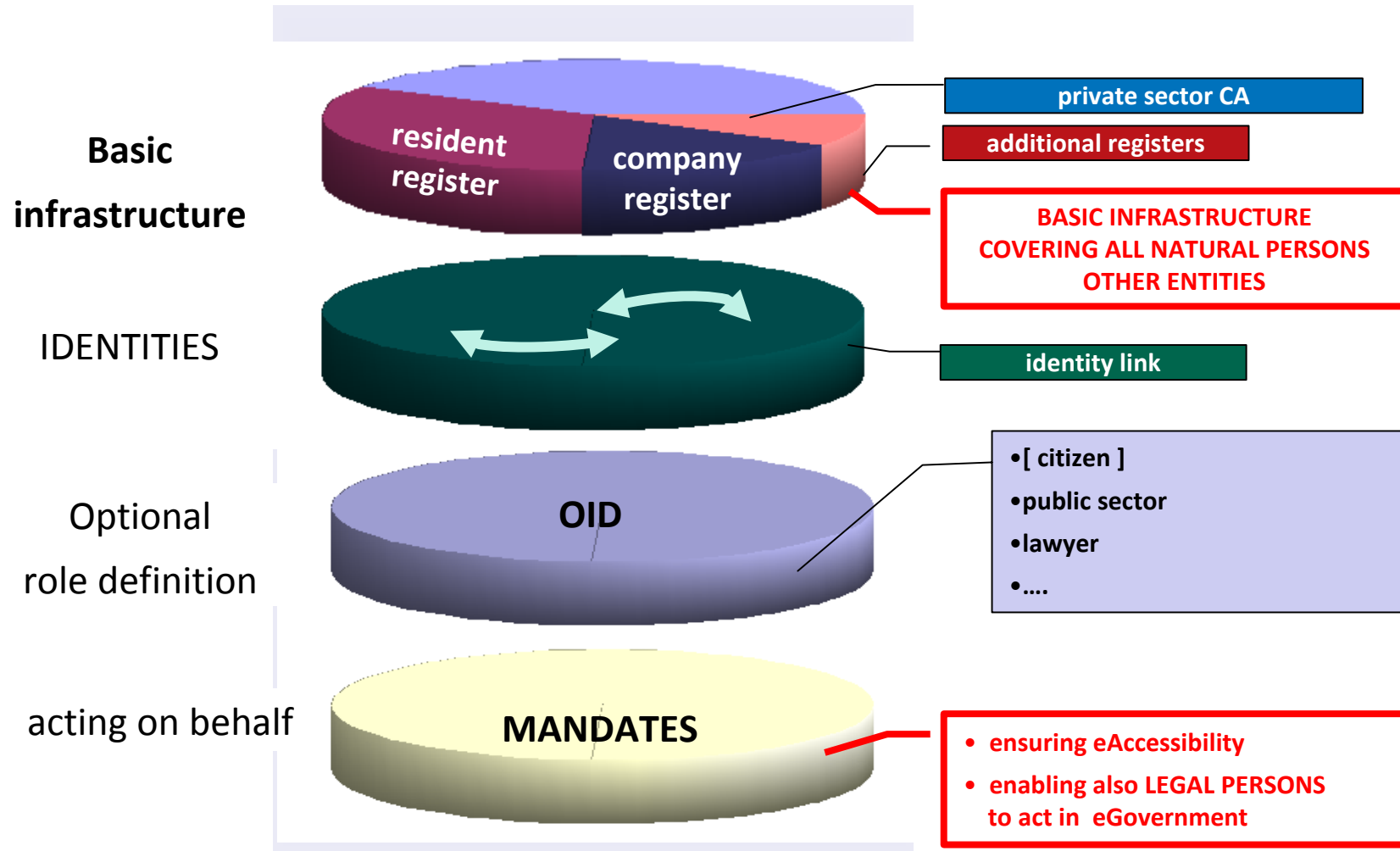
**eID may or may not be combined with ID cards**

**national identities focus on controlled and attended physical environment**

**e.g. border control**

**eID is prely unattended and non physical**

# eIdentity in AT eGovernment

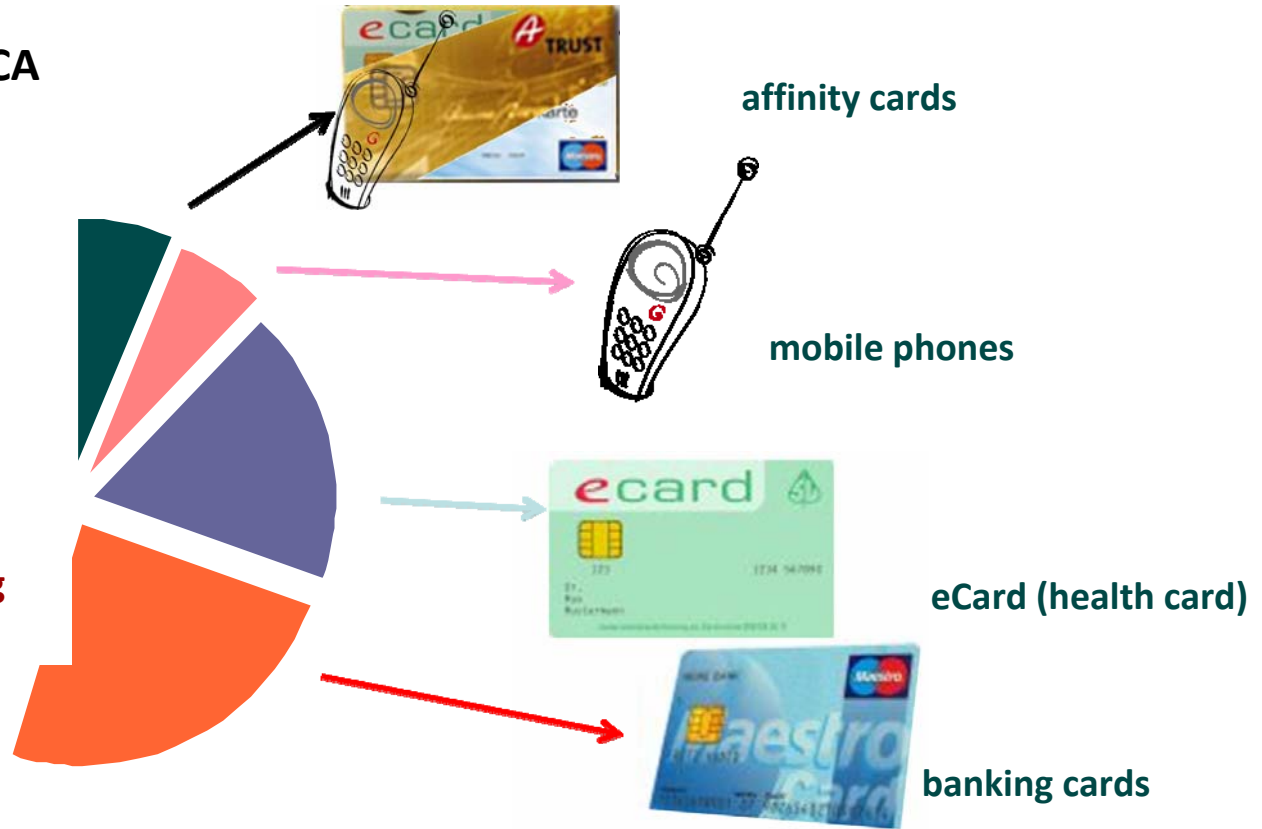


eID and signature covering 100% of services by medical doctors (2005)

# various instances of eID

## PRIVATE SECTOR CA

- validity according to signature law
- revocation following signature law

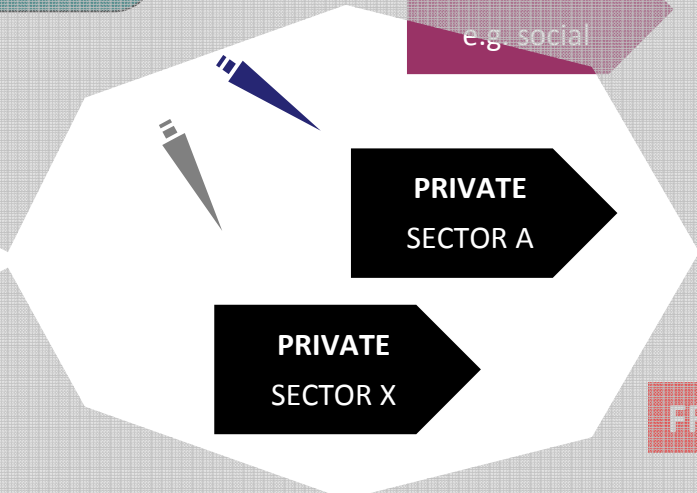
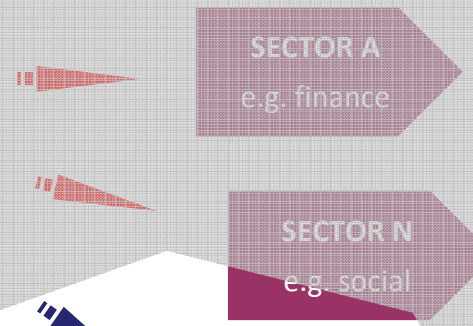


**INHERITING SECURITY AND LEGAL RECOGNITION FROM SIGNATURES**



# sectors and businesses

CONCEPT CITIZEN CARD SOURCE PIN → FRACTIONAL PIN



one way hash

sector oriented id

sectoral id per business

inclusion of businesses

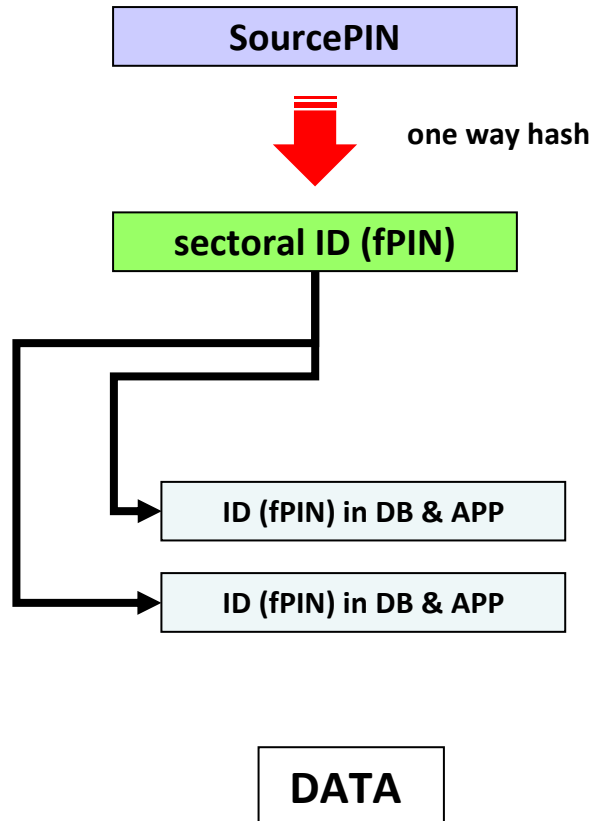
FRACTIONAL PIN :: SECTORAL ID

Cryptography: strong link to eID & separation of sectors  
NO ADDITIONAL PRIVACY RISK



# eID and authentication

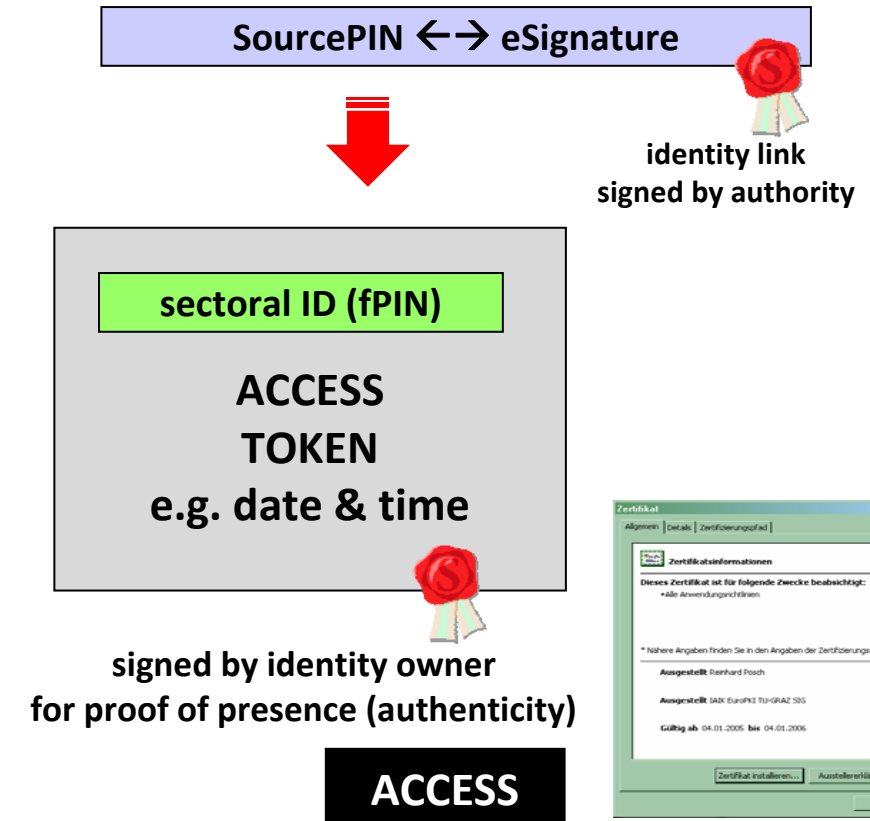
eID



NATURAL AND NON-NATURAL ENTITIES

NATURAL PERSONS ONLY

eAuthentication



# eID multiple access

provider A



provider B



=

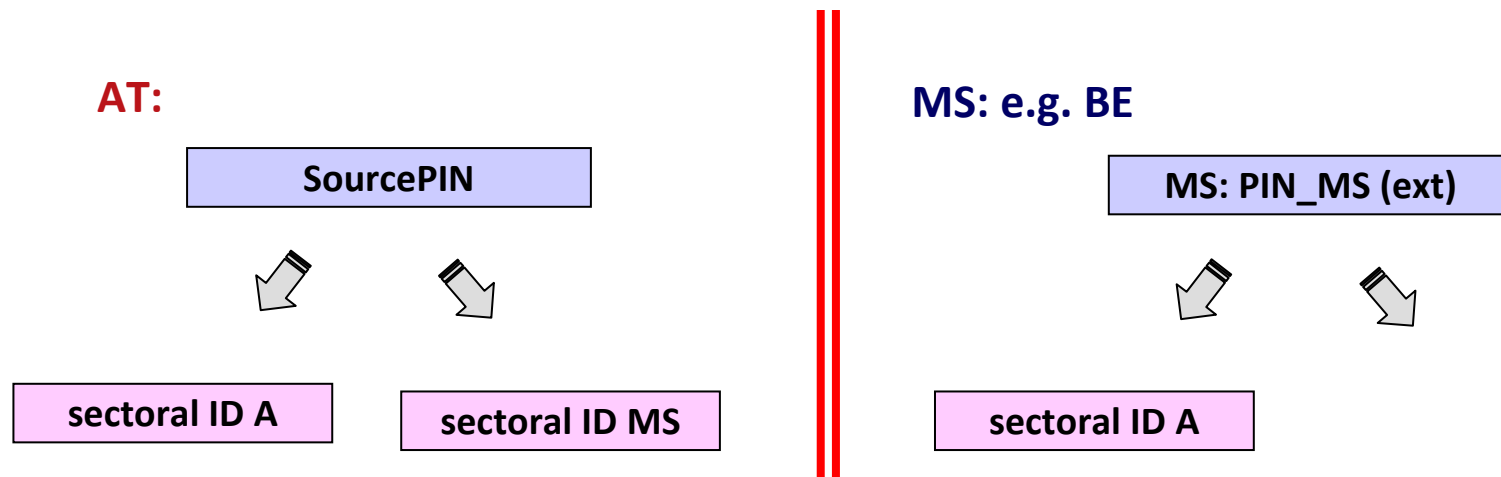



identity link

identity link

- Management & Revocation
- Multi channel / Multi technology
- Separation of DATA & ACCESS
- ENABLE TECHNOLOGY ADVANCES

# AT: eID & interoperability



- USAGE MS: id does not reveal MS:PIN\_MS within AUSTRIA
- USAGE of AT-PIN in MS (fPIN:MS) according to MS rules does not compromise AT schema
- NO ADDITIONAL PRIVACY RISK
- IN PLACE WITH  FROM BE, IT, FI, EE







**Zentrum für sichere Informationstechnologie – Austria**  
**Secure Information Technology Center - Austria**

A-1040 Wien, Weyringergasse 35  
Tel.: ++43 1 – 503 19 63 – 0  
Fax: ++43 1 – 503 19 63 – 66

A-8010 Graz, Inffeldgasse 16a  
Tel.: ++43 316 – 873 5514  
Fax: ++43 316 – 873 5520

**thank you for your  
attention**

[reinhard.posch@a-sit.at](mailto:reinhard.posch@a-sit.at)

