The Office for Personal Data Protection of the

SLOVAK REPUBLIC

E- government, E- health, E- databases…

Personal Data Protection Perspective

Odborárske námestie 3
817 60 Bratislava 15
Tel.:+421 2 502 39 418
Fax: +421 2 502 39 441
STATNY.DOZOR@PDP.GOV.SK
WWW.PDP.GOV.SK

Daniel Valentovič
Tel.: +421 2 50239428
Mob.: +421 903454017
Daniel.Valentovic@pdp.gov.sk

Mrs. Waltraut Kotchy,
Data Protection Commissioner
Oestereichische
Datenschutzkommission,
Ballhausplatz,
1 A - 1014 WIEN
Tel 43/1/531.15.25.25
Fax. 43/1/531.15.26.90
e-mail: dsk@dsk.gv.at

What do we mean by „Personal Data Protection Perspective“ ?

- Definition Personal data

- **Section 3 of the ACT 428/2002 Coll. on Personal Data Protection**

Personal data shall mean any information relating to an identified or identifiable natural person, while such person is one who can be identified, directly or indirectly, in particular by reference to a identifier of general application or by reference to one or more factors specific to his physical, physiological, psychic, mental, economic, cultural or social identity.

We have Personal Data or

Special Categories of Personal Data

- revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, membership in political parties or movements, trade-union membership, and the processing of data concerning health or sex life

Some Legislation on Personal Data :

- EU:
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)
- Additional protocol to Convention 108 regarding supervisory authorities and transborder data flows (ETS No. 181)
- Dir 95/46/EC on Data Protection
- Dir.2002/58/EC on privacy and electronic communications

- SR:
- Constitution of the Slovak Republic , Article19 and 22
- Act 428/2002 Coll. on Personal Data Protection as am.
- Act 610/2003 Coll. on Electronic Communications as am.
- Special acts

E- gov data – protection – security

Types of data contained in E-systems:

- Public or published with the data subject consent
- **Personal data** **(in EC : Article 29 WP of the Dir 95/46/EC on Data Protection)**
  - Ordinary , Special category personal data
- Classified information /data
  - Top secret, Secret, Confidential, Restricted
- Confidential data – internal, strategic, politically sensitive ...

- How to guatrantee security and protection of all these data within SR and with >25 EU countries in future?

- Answer : use synergy of both the :
  - Legal instruments (if we have not a releveant e-gov security legislation in power, there are no budgets available for any technical investment into a really secure & reliable e-gov , e- health solutions)
  - Technical instruments (criminals do not respect law if we do not have technical measures, legal ones alone might not work at all)

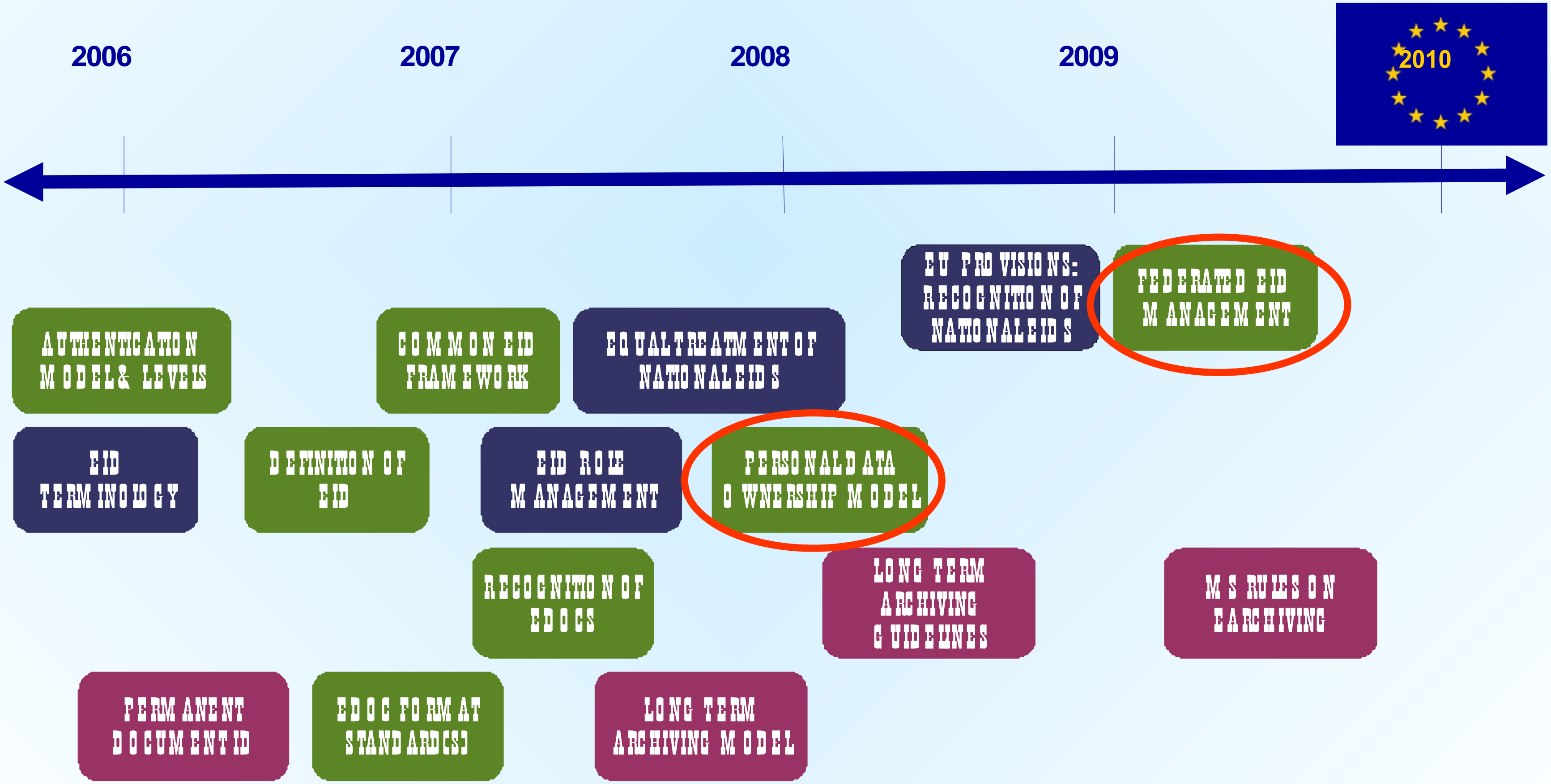
- Security costs some money – but it prevents big losses and problems as well
- Secure Identification and autentication of data subject or data user is a common problem of all of them. Encryption of e-traffic is not a problem.

How to handle the problem of the secure EU E-GOV communication within EU technically

- In principle we will have several major entities for communication:
  - All EU Member states
    - Governments
      - State administrations
      - Municipal administrations
      - Police and customs officials,
      - Law enforcement authorities
    - Hospitals, health professionals, insurance companies , patients, Emergency services,
    - E- banking , E – money ....
    - Other sectors e.g. E-services & E- business, Third sector non profit organisations
    - **Citizens – Data Subjects**
    - **...**
- **How to guarantee a secure communication almost „any-to-any“ of the above data users ?** **Again by :**
  - **Proper legislation in power** – enables R&D and implementation budgets for a GOOD E-gov **solution**
  - **Proper technical solutions implemented** **-** UNIFIED / INTEROPERABLE ID MANAGEMENT & RELIABLE ENCRYPTION QUALITY OF DATA TRAFFIC („co-ordinated technical IT / IS Security of all EU E-gov systems “) **-** criminals do not respect law – PD&privacy must be protected by technical security - really implemented

i2010 signposts

ADAPTING THE INFRASTRUCTURE



AUTHENTICATION MODEL & LEVELS

COMMON EID FRAMEWORK

EQUAL TREATMENT OF NATIONAL EIDS

EU PROVISIONS: RECOGNITION OF NATIONAL EIDS

FEDERATED EID MANAGEMENT

EID TERMINOLOGY

DEFINITION OF EID

EID ROLE MANAGEMENT

PERSONAL DATA OWNERSHIP MODEL

RECOGNITION OF EDOCS

LONG TERM ARCHIVING GUIDELINES

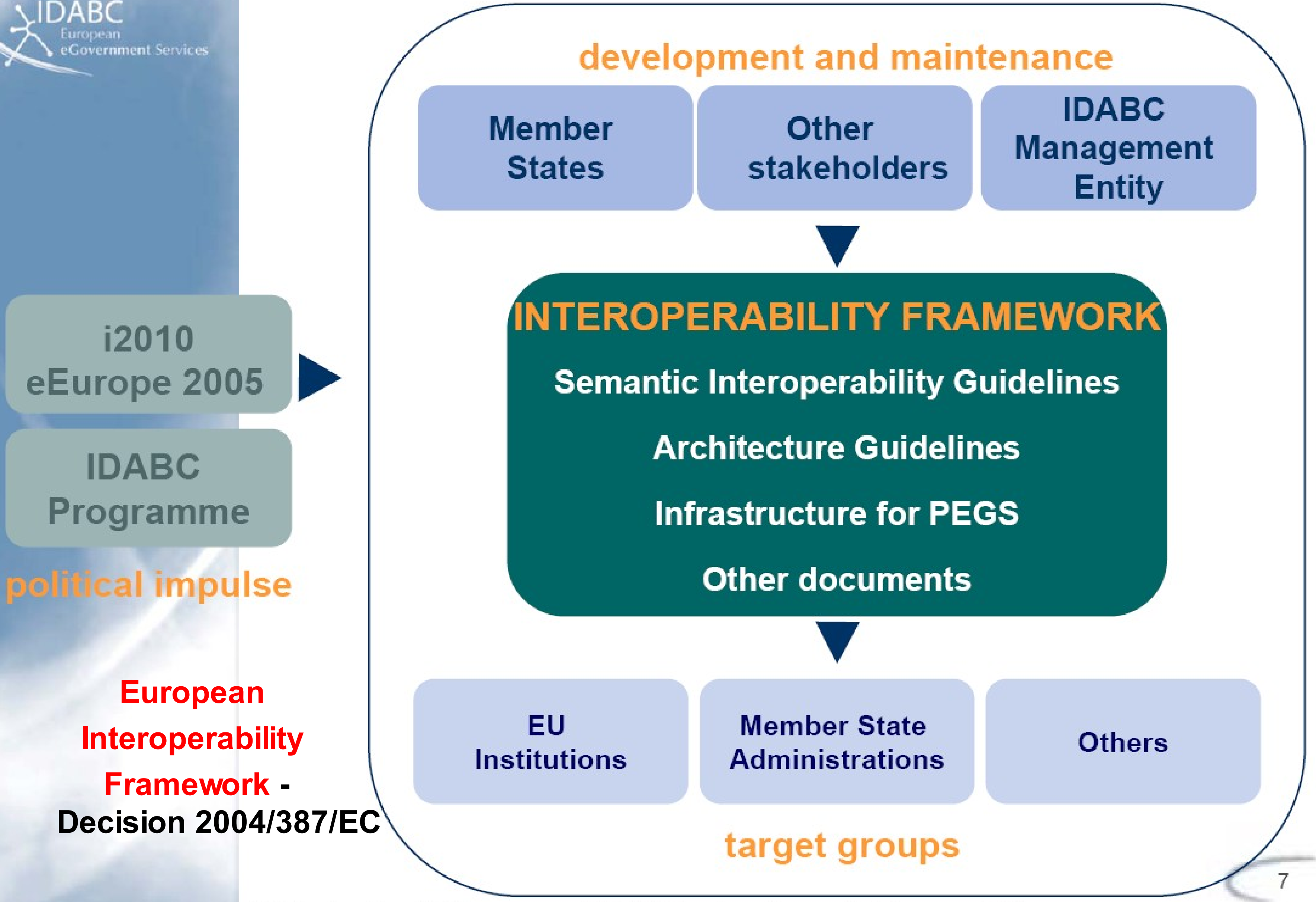
MS RULES ON EARCHIVING

PERMANENT DOCUMENT ID

EDOC FORMAT STANDARD(S)

LONG TERM ARCHIVING MODEL

Interoperability Guidelines



development and maintenance

Member States

Other stakeholders

IDABC Management Entity

INTEROPERABILITY FRAMEWORK

Semantic Interoperability Guidelines

Architecture Guidelines

Infrastructure for PEGS

Other documents

EU Institutions

Member State Administrations

Others

target groups

i2010 eEurope 2005

IDABC Programme

political impulse

European Interoperability Framework - Decision 2004/387/EC

EU perspective of e-systems of EU MS :

After 2009 - EU Federated e-ID, integrated EU solutions – e- gov , e-health, e- call ....

Interoperability is a KEY

Personal data protection and privacy protection of European citizens is guaranteed by EU and Slovak law ...

Data security & privacy protection is a MUST

BUT is it really guaranteed by technical security of data and privacy protection in ever more complex ubiquitous computing ? („Bad guys“ do not respect law and they ACT if the technology alows them to do it)

Is the data&privacy protection possible or impossible in principle?
(all we know that 100% security does not exist)

Do we know a reliable concept of e-gov NOW or not?
Answ.: **YES it exists – it is implemented**

Example of already existing solution

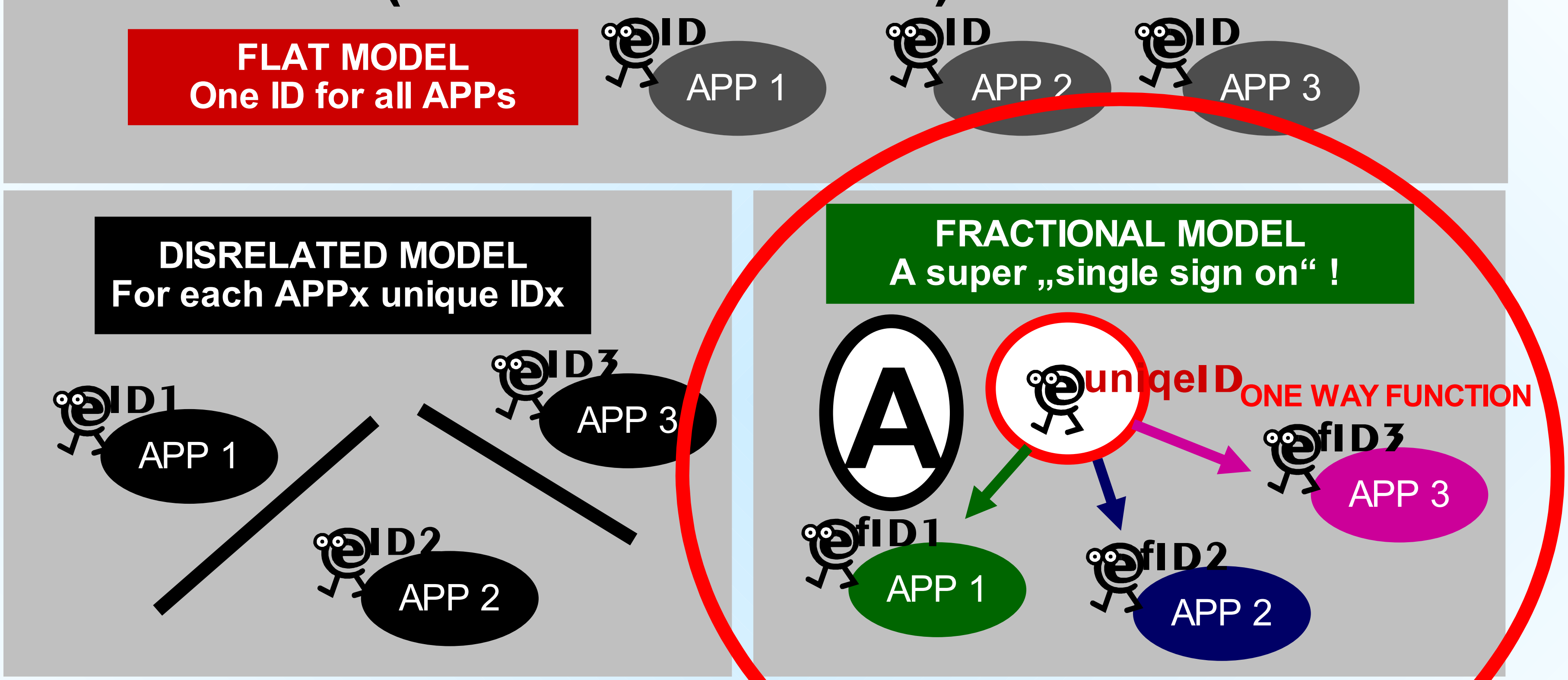
Analysis from a data protection point of view

E- gov & E-health iniciatives in Austria

Slides made in co-operation with

Mrs Waltraut Kotschy
Austrian Data protection Commissioner
Executive Member of the
Austrian Data Protection Commission and
E-Government Register Authority
waltraut.kotschy@dsk.gv.at
Austrian Data Protection Authority

-eID and Data Protection – models in place (eIDx= PINx below)



FLAT MODEL
One ID for all APPs

DISRELATED MODEL
For each APPx unique IDx

FRACTIONAL MODEL
A super „single sign on“ !

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

eID MUST NOT ADD ADDITIONAL PRIVACY RISKS TO EXISTING APPLICATIONS

All Austrian E- government, E- health
... solutions have the same **CONCEPT**

as concerns the identity management

ALL Austrian E- gov solutions
ARE TECHNOLOGICALLY NEUTRAL
i.e. THEY DEPEND ON MATHEMATICAL FORMULAS ONLY,

and do not depend on supliers, nor on pure technical standards.

So sub-systems of e-gov may be supplied by independent suppliers

Legal basis for e-planning – budgeting of E- Gov, e- health...R&D and implementation .

- Relevant legal provisions in Austria:
  - The Austrian E-Government Act **- Federal Act on Provisions Facilitating Electronic Communications with Public Bodies** Nr. 10/2004, entered into force on 1 March 2004
  - Special Acts e.g.:
    - Law on documentation in the health sector (745/1996)
    - Law on Health Telematics:
      - Art. 9 of the Health Reform Law (179/2004)

Problems E-goverment sectors

- National public budgets are seriously affected by **costs**
- **Quality of governmental decisions and services** needs better control, monitoring and evaluation

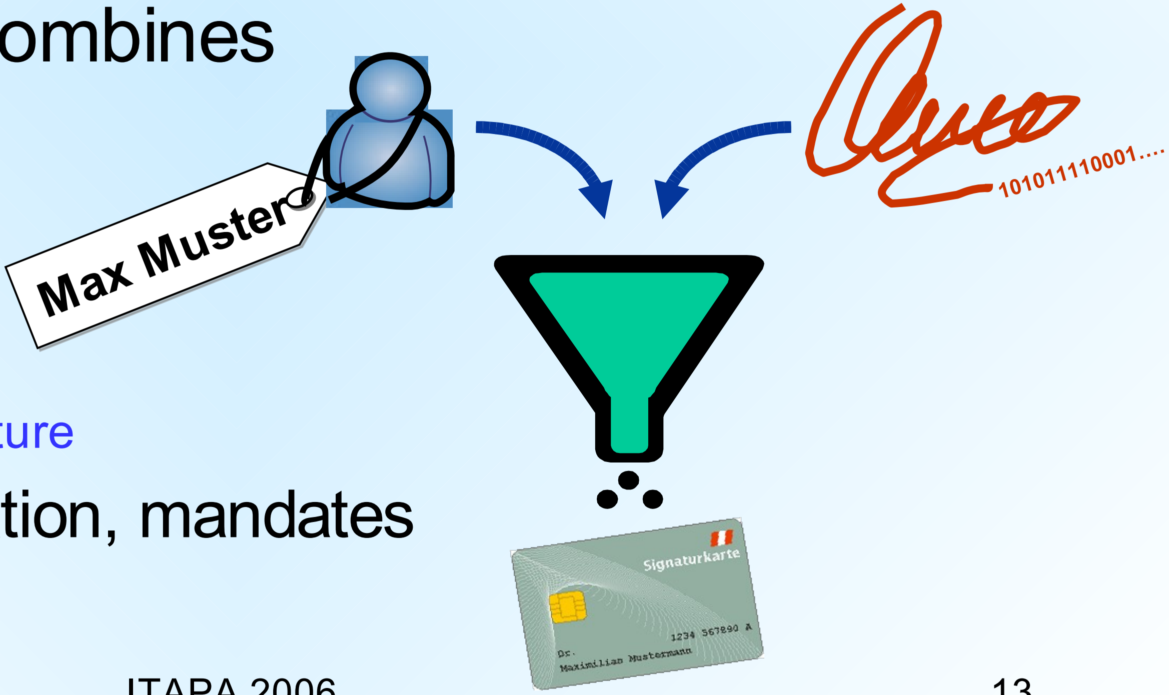
Solutions ?

- **Introduction of telematics** services for better
  - **E-communication** between professionals and data subjects :
    - E.g. Insurance companies, hospitals, doctors, ... parties involved ..
  - **E-controlling** for use of funds in the public sector
  - **E-planning** for future requirements:
    - Government and state administration bodies need accurate and up-to-date information to gain a reliable knowledge from all E-gov systems*

*(data => information =>knowledge. KNOWLEDGE MEANS THE POWER . If a democratic government is really knowledgeable and powerful, the country is led effectively , safely and reliably).

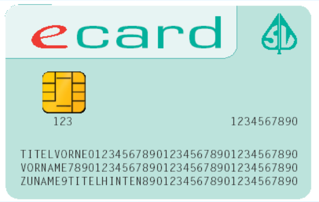
Identity management

- The Austrian Citizen Card is a concept, not a specific technology
- The Citizen Card combines
  - – electronic identity
    - ***Identification***
      - *Source PIN*
    - ***Authentication***
      - – electronic signature
  - – data on representation, mandates



Major initiatives – Citizen Cards

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


ecard
123
1234567890
TITELVORNE01234567890123456789012345678901234567890
VORNAME78901234567890123456789012345678901234567890
ZUNAME9TITELHINTEN890123456789012345678901234567890

Health insurance cards:
Rollout Mai-Nov. 2005, ~70.000 cards/day
100 % coverage (9 Mio.) reached end of Nov.

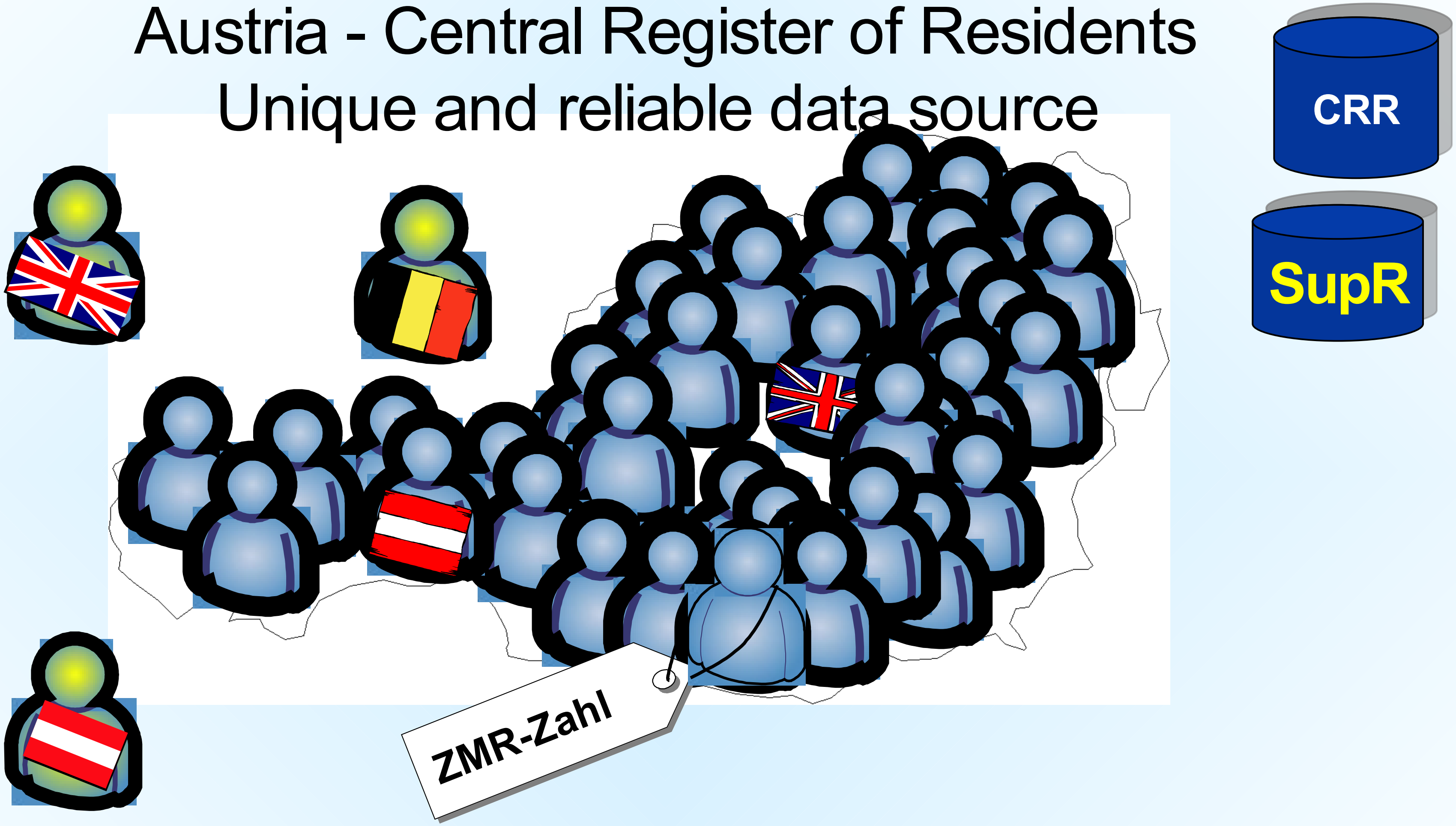
Mobile phones:
each mobile phone (capable of receiving SMS) (since March 2004)

Further initiatives:

- CSP signature cards
- Student service cards, etc.

ID Cards?

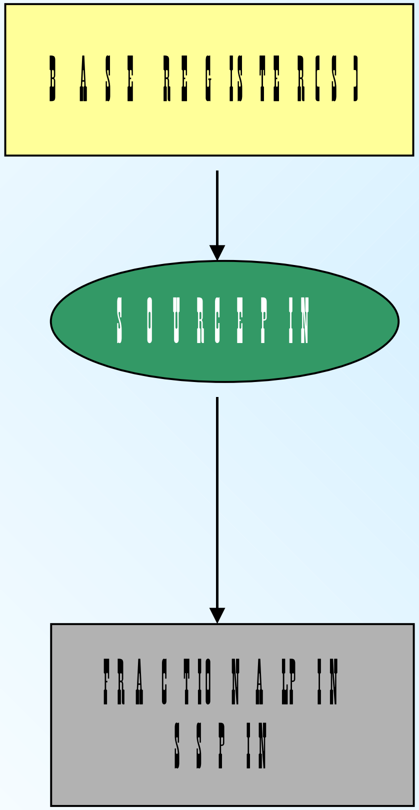
Austria - Central Register of Residents
Unique and reliable data source



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

Fractional approach in Austria

Austrian *e*Government Act:



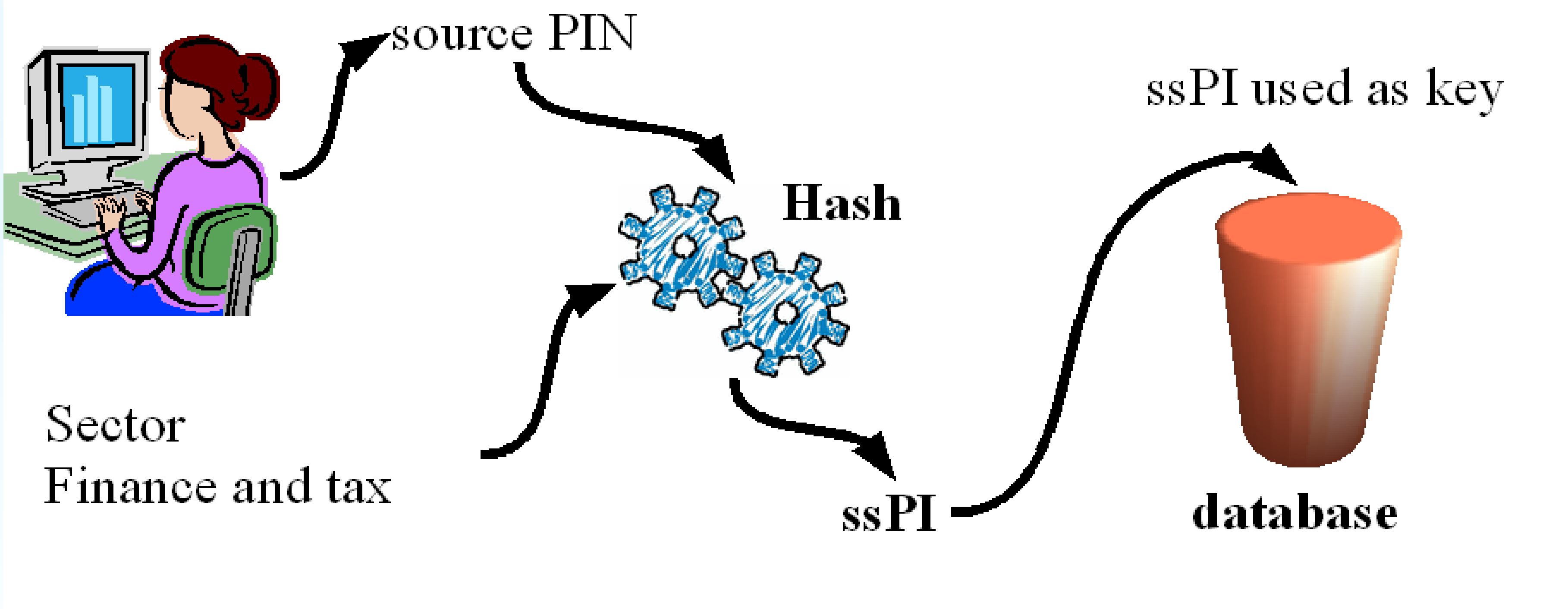
THE BASE REGISTERS OF RESIDENTS PROVIDE FOR UNIQUE IDENTIFICATION

THE SOURCEPIN REPRESENTS THE UNIQUELY IDENTIFIED PERSON; IT IS A **hidden number, stored only in the Citizen Card**, WHICH IS IN THE POSSESSION OF THE DATA SUBJECT AND AUSTRIAN DPA **only**

IN GOVERNMENT DATA BASES ONLY THE APPROPRIATE FRACTIONAL PIN — SSPIN APPEARS FOR IDENTIFYING DATA SUBJECTS. (DIFFERENT FOR THE SAME INDIVIDUAL AT DIFFERENT MINISTRIES AND STATE AUTHORITIES)

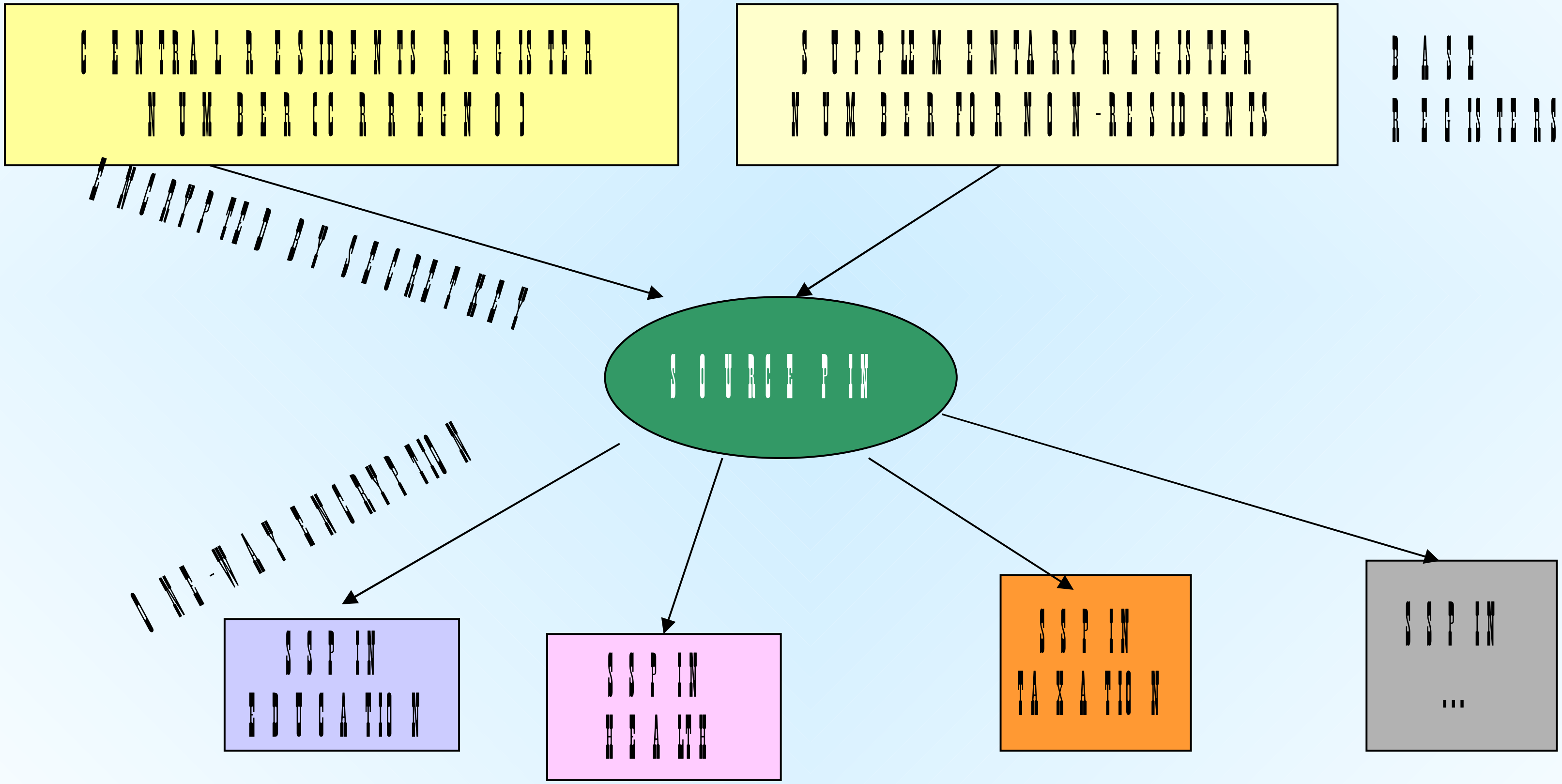
Data Protection / Privacy

- Persons uniquely identified (source PIN)
- ID in applications (fPIN = ssPI= ssPIN= sectoral eID)



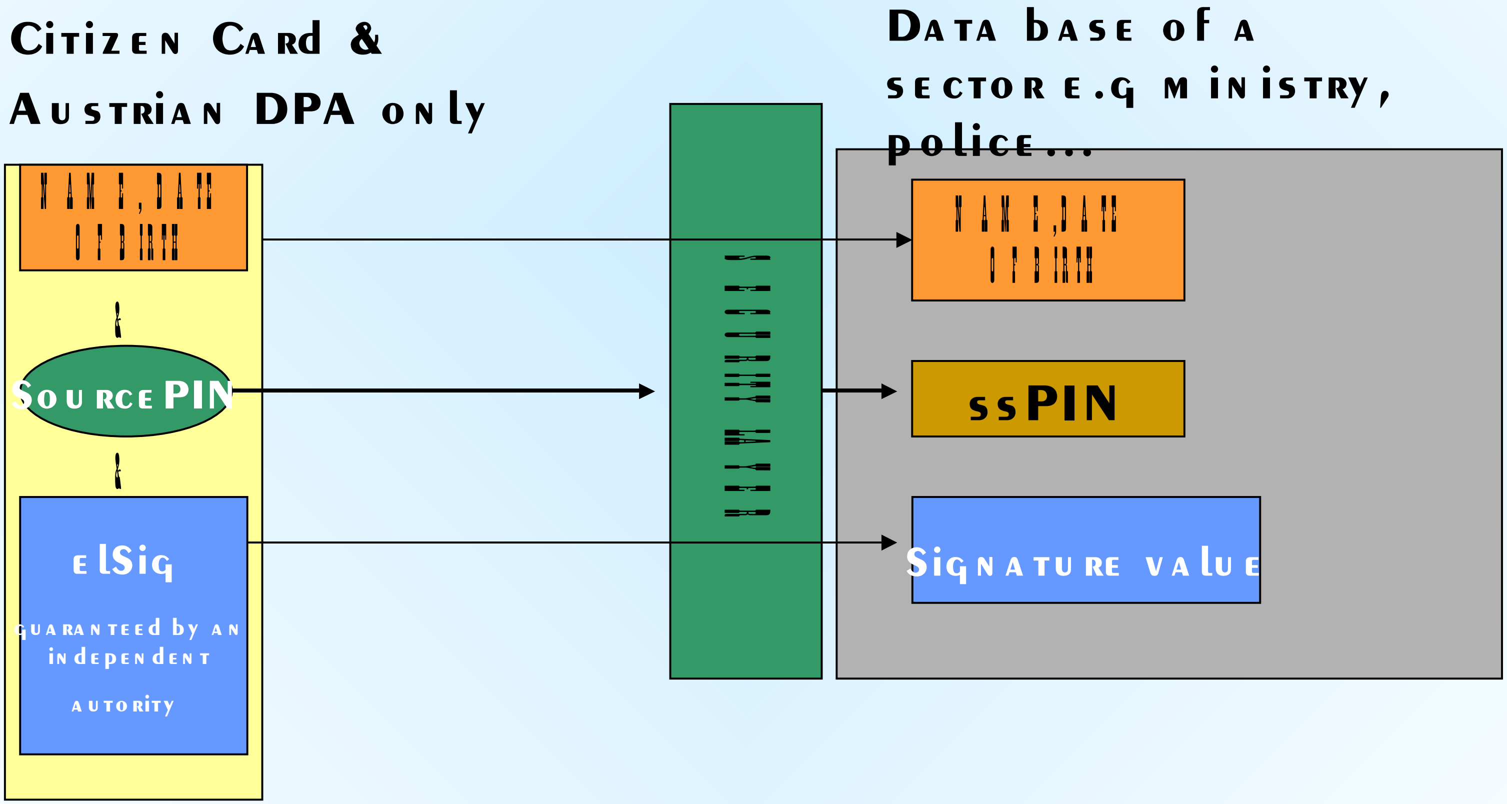
Electronic identity of natural persons

Fractional PIN = sector specific PIN (ssPIN)



How does it work?

- Using the Citizen Card:



Citizen Card &
Austrian DPA only

Data base of a
sector e.g ministry,
police...

NAME, DATE
OF BIRTH

Source PIN

elSig
guaranteed by an
independent
autority

[illegible]

NAME, DATE
OF BIRTH

ssPIN

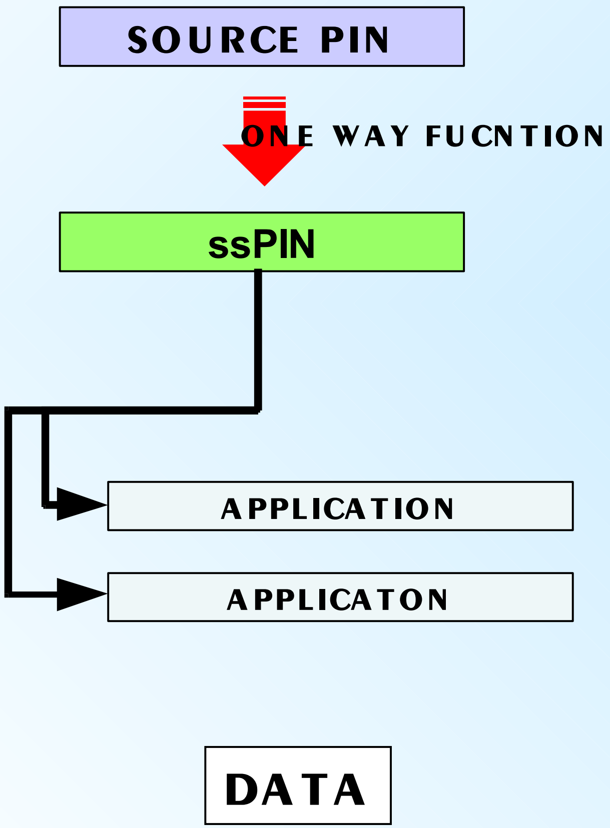
Signature value

IDENTIFICATION
AUTHENTICATION

NATURAL AND NON NATURAL PESONS

NATURAL PERSONS ONLY

eID



SOURCE PIN

ONE WAY FUCNTION

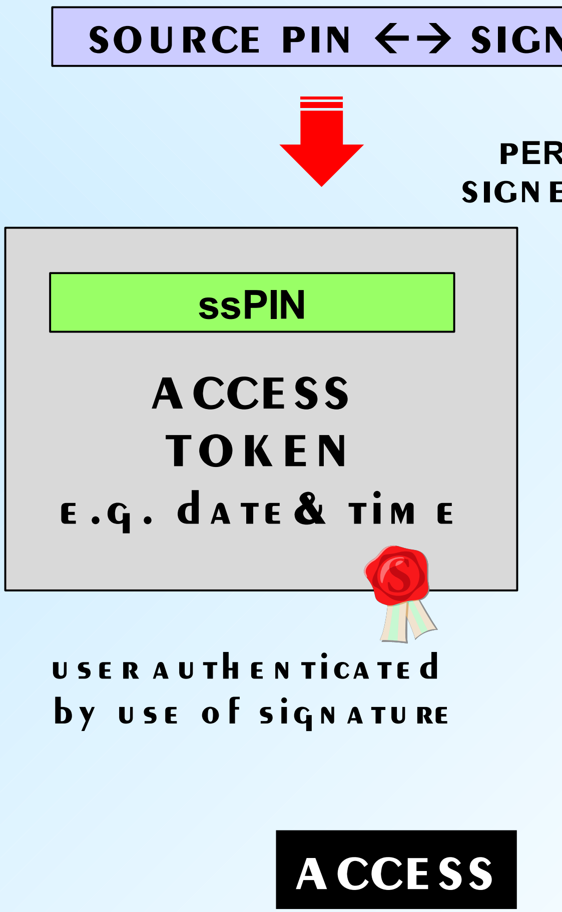
ssPIN

APPLICATION

APPLICATON

DATA

eAuthentication



SOURCE PIN <-> SIGNATURE

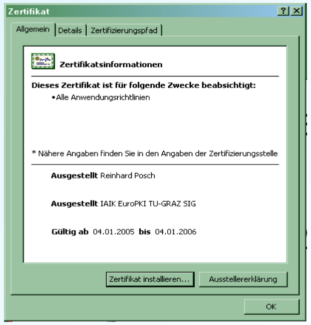
PERSON A BINDING
SIGNED BY Sign. Autority

ssPIN

ACCESS
TOKEN
e.g. date & time

user authenticated
by use of signature

ACCESS



Zertifikat

Zertifikatsinformationen

Dieses Zertifikat ist für folgende Zwecke beabsichtigt:
- Alle Anwendungsrichtlinien

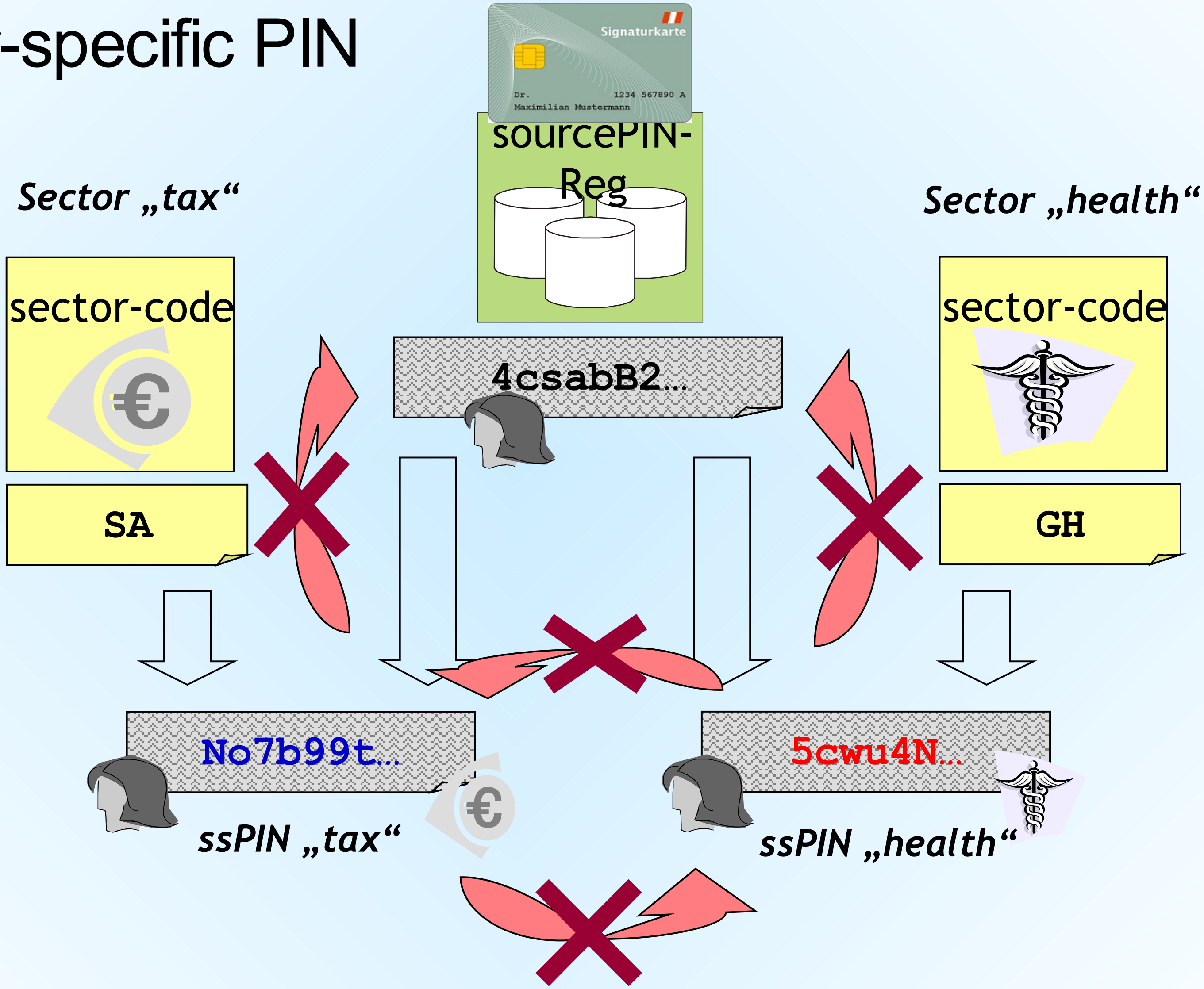
* Nähere Angaben finden Sie in den Angaben der Zertifizierungsstelle

Ausgestellt Reinhard Posch

Ausgestellt IAIK EuroPKI TU-GRAZ SIG

Gültig ab 04.01.2005 **bis** 04.01.2006

Sector-specific PIN



Private sector-specific PIN (pssPIN) (Sect. 14 E-GovAct)

= private sector-specific personal identifier pssPIN

✂ → electronic communication in the private sector (e-Business)

- sector code: controllers´ SourcePIN

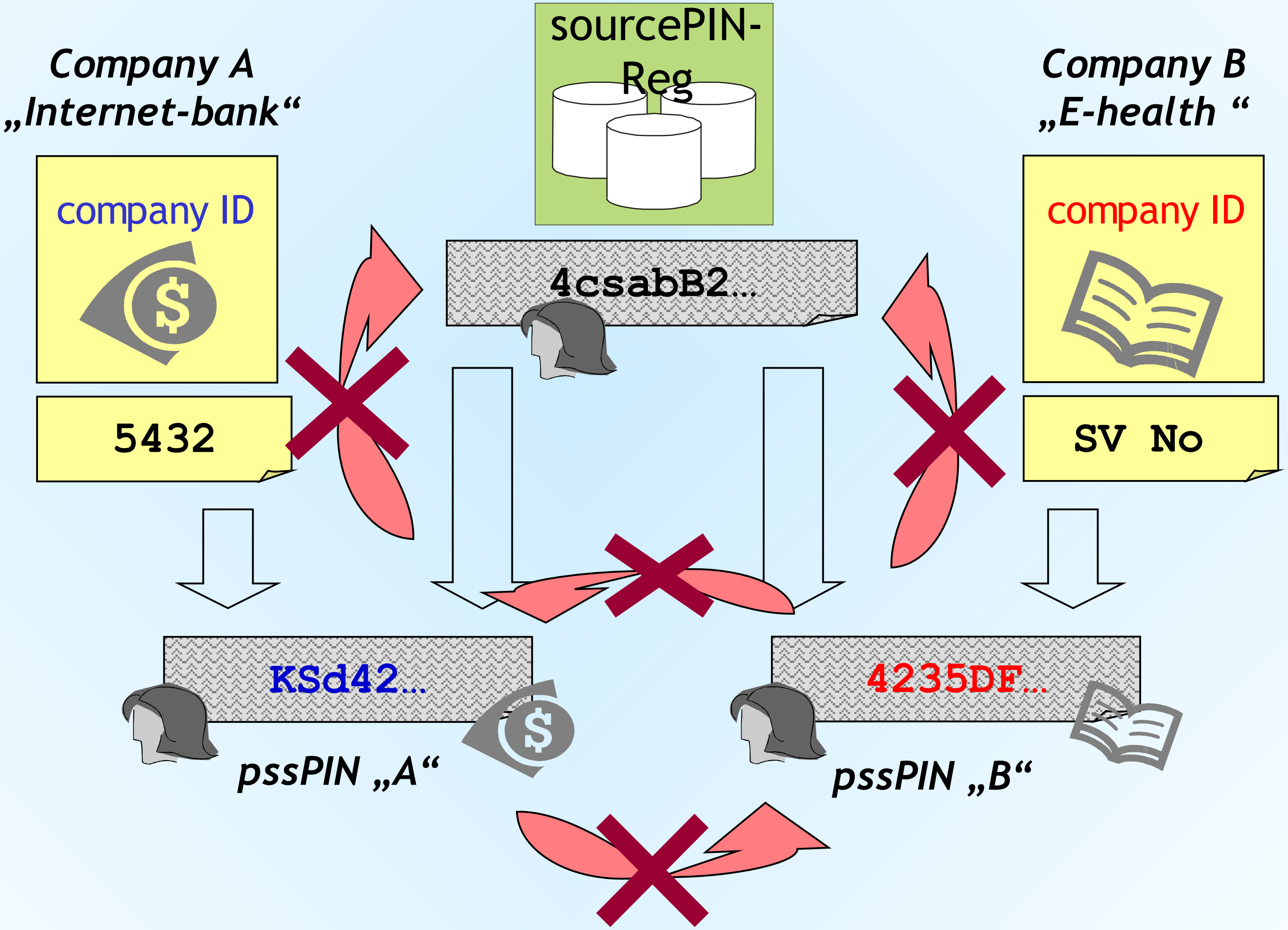
(instead of the identifier used for administration procedures- but derived by the same principle as in e-gov)

- Data controller only may store such pssPINs

A visible PIN

- For data protection reasons the use of fPINs/ssPINs outside the data applications of the public authorities (outside e-gov) is forbidden
- Therefore the health and social security sector uses a sectoral PIN („SV-number“ Social Versicherung Nu), which can be used openly between controllers of the public and the private sector
- The number is not mathematically related to the sourcePIN, but the quality of identification is correlated to a respective sector

Private sector-specific PINs



Company A „Internet-bank“

company ID

5432

KSd42…

pssPIN „A“

sourcePIN-Reg

4csabB2…

Company B „E-health “

company ID

SV No

4235DF…

pssPIN „B“

Restrictions on the use of ffPINs

- **fPINs of another government sector (ffPINs)** may only be stored **in encrypted form only** :

  (sourcePIN + „foreign“ sector1Code) Hash → ffPIN1]

  encrypted

- Encryption is done by means of the public key of the government body asked for the transmission of data

What about security ?

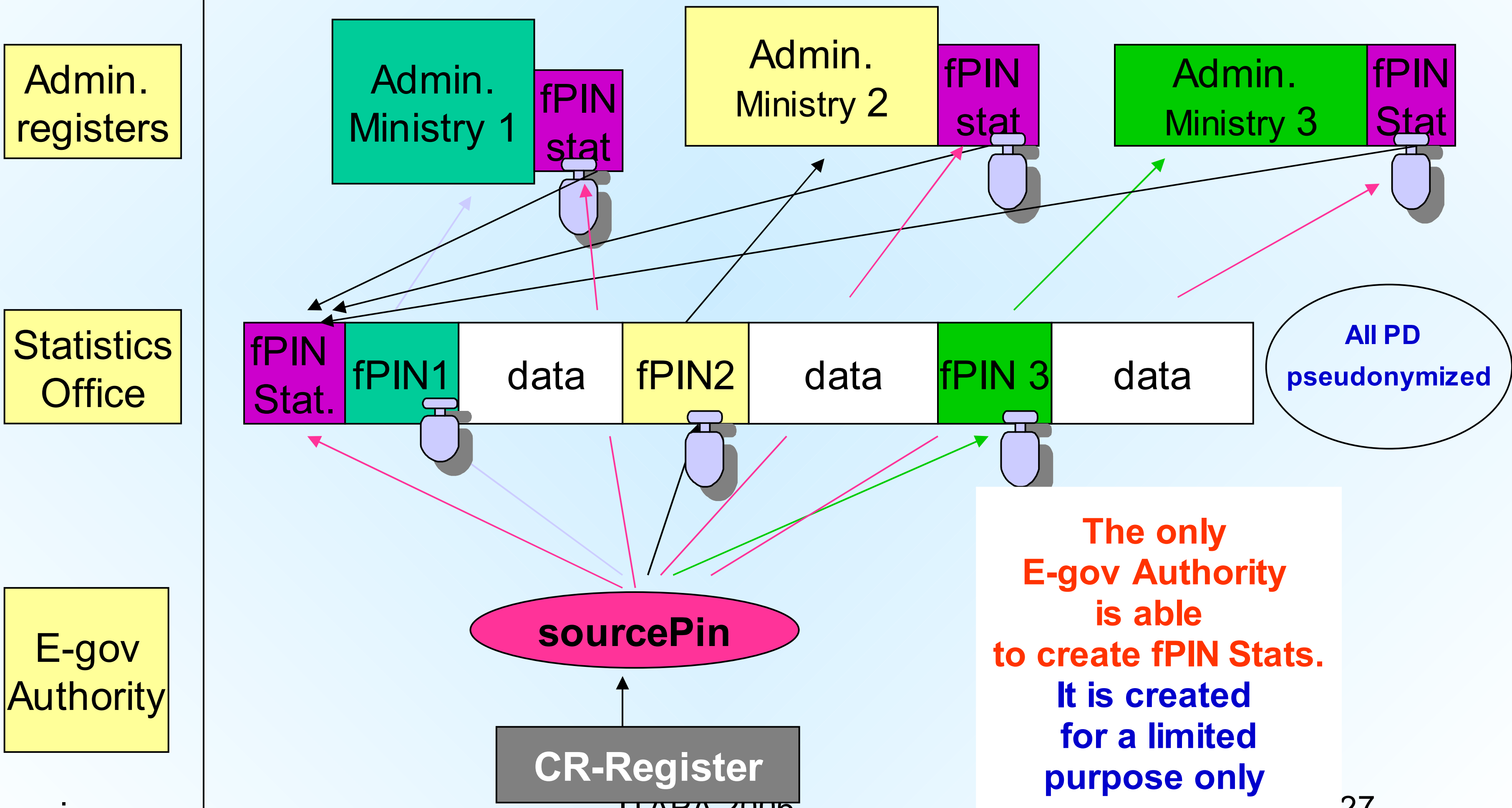
- Every citizen has a unique = different from other citizen :
  - 1Source PIN + many ssPINs + SV-number + (pssPINs) + e-signature (+ Citizens Card reader´s PIN)

- Each of the ssPINs is deleted after an access (they are not stored or stored in the eccrypted form ffPINs by sector „s" only)
- Each citizen 20 totally different e-IDS in e- government only derived from a single Source PIN:
  - Try to crack 100 million totally different eIDs to get access to complete e-goverment info. I one ssPIN is cracked the PD info about one person is available – from a single sector only

- How to use so many access eIDs ? Is it possible to manage it? – YES – and quite simply
  - it is not necessary to store them, they are conmputed from Source PIN if necessary by the authorised authority only
  - Stored in encraptewd for ffPIN by a sector only
- if not stored or stored in encrypted form ssPINs cannot be stolen!

- How to use multisource info ? Is it possible with such a complicated system of the access eIDs? YES and quite simply =>

Collecting and checking data for census/statistics in Austria



Admin. registers

Statistics Office

E-gov Authority

Admin. Ministry 1

fPIN stat

Admin. Ministry 2

fPIN stat

Admin. Ministry 3

fPIN Stat

fPIN Stat.	fPIN1	data	fPIN2	data	fPIN 3	data

All PD pseudonymized

sourcePin

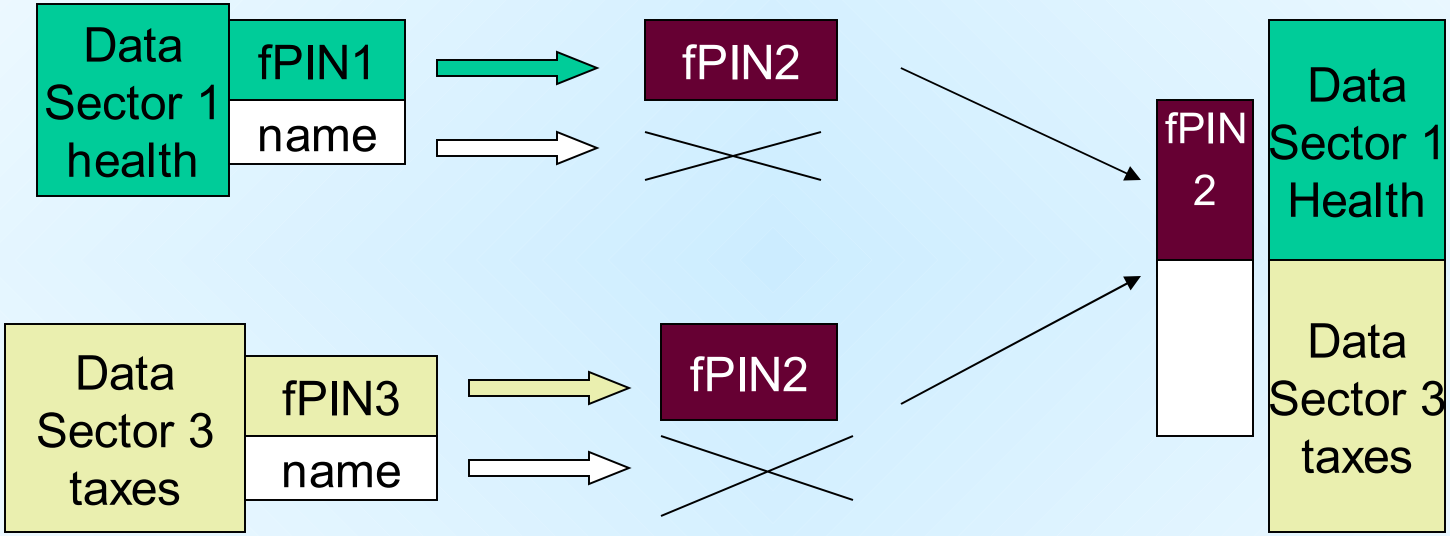
CR-Register

The only E-gov Authority is able to create fPIN Stats.

It is created for a limited purpose only

Individualisation without identification

- Administrative Registers Statistics



E- health & the ecard

- About 8 million people living in Austria are in possession of an ecard (everybody who has social insurance)
- The card contains only
  - the name and
  - the social security number (SV-number)
  - and an electronic signature for electr. communciations with soc. sec. bodies

Identities in E-health

- Of patients:
  - **SV-number** (for open use)
  - fPIN „health“
  - fPIN „social security“
- Of health care professionals:

Register of health care professionals

(Physicians, Hospitals, Laboratories, etc.)

Uses fPIN „health“ for nat. persons – sourcePIN for legal persons

Proving identities E-health

- The doctor (or his staff) prove their „identity“ in the social security e-communication system (*ELSY*) by an „**office card**“

- The patient proves in *ELSY* his identity and his status as socially insured at the hospital, at the doctor by showing his **ecard**

- The full – open E-health record is available if both: the doctor´s **office card & ecard of patient** are inserted into reader at the same time.

E-planning and e-controlling – in general

What sort of data are needed?

- Accurate and up-to-date data are necessary for successful controlling and planning
- These data need not to be personalized, HOWEVER,

  if they are collected from

  - different sources or
  - different times

  correct linkage to the same statistical unit (=individual) is necessary

E-planning and e-controlling – E-health

Where do the data come from?

- Special registers, e.g.
  - Tumor Register
  - Drug addicted persons Register
  - Contagious diseases Register
  - ...
- Data at various Government bodies
- Documentation at the health care professionals
  - Traditional documentation
  - **ELHFs - Electronic Lifelong Health Files in future?**
- etc.

All Austrian E- government , E-health, E-privateSector solutions have the same features

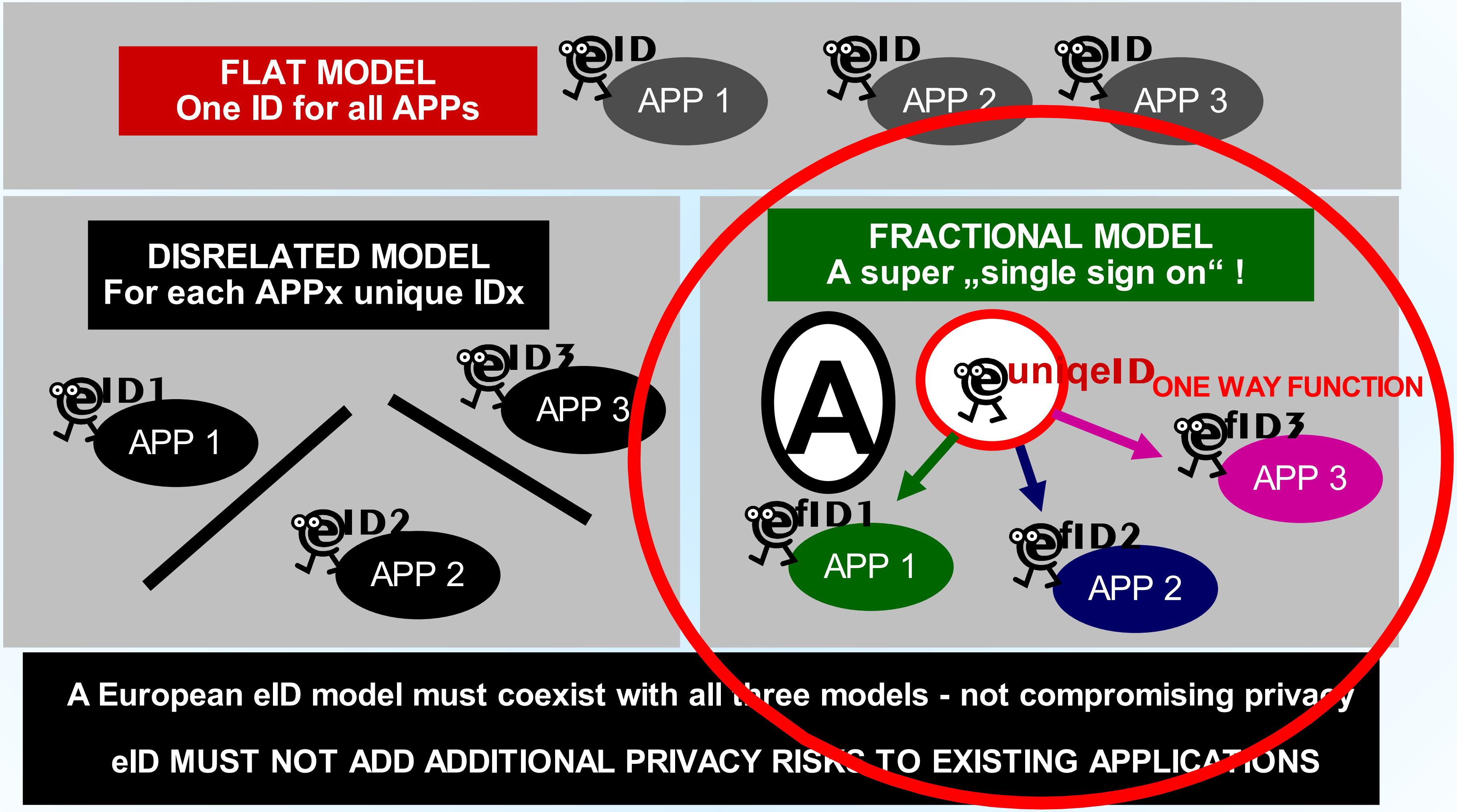
In principle the secure access to many different sectoral Registers is possible using the

CONCEPT of the eID + e-Authent.
Sorce PIN -> fPIN (=ssPIN or pssPIN)
+ electronic signature

ALL OF THEM ARE TECHNOLOGICALLY NEUTRAL
i.e. THEY DEPEND ON MATHEMATICAL FORMULAS ONLY,
not on solutions of supliers, nor on pure technical standards

Austrian Bundeskanzleramt does not use paper documents any more – they have the e-gov implemented and proved in real praxis

U - eID and Data Protection – models in place



FLAT MODEL
One ID for all APPs

DISRELATED MODEL
For each APPx unique IDx

FRACTIONAL MODEL
A super „single sign on“ !

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

eID MUST NOT ADD ADDITIONAL PRIVACY RISKS TO EXISTING APPLICATIONS

Summary

- E- government, E- Health , E-“anything“ secure solutions exist – it is Austrian – really implemented Fractional model of eID combined with an independent eAuthentication (e-sign.) that is TECHNOLOGICALY NEUTRAL CONCEPT :
  - It is applicable to any E- system, E- government subsystem, or E- Health, Registries, private appl., e.g. secure acces to bank acounts, e- business ...
  - It is applicable for integrating already existing E- gov & E- health solutions of other EU Member states
    - Belgian, Estonian, Finish, Italian ID cards – already INTEGRATED with Austrian IDM!
  - In our opinion it works , it is secure and it is reliable. We think that this concept will be implemented by many EU countries, because it is one of the possibly most secure ones.
  - Goverment and state administration bodies need accurate and up-to-date information to gain a reliable knowledge from all E-gov systems * The key to the all information access (creation of all fPINS for all E-gov subsystems) is in hands of the government (in Auistria the Office of the Austrian Chancellor- Bundeskanzleramt)
- The EU needs to have the MS that have knowledgeable and strong governments

*(data => information =>knowledge. KNOWLEDGE MEANS THE POWER . If a democratic government is really knowledgeable and powerful, the country is led effectively , safely and reliably).

I thank you for your attention