Technology for eID

Prof. Dr. Reinhard Posch

Scientific Director

A-SIT WIEN

2006/10/05

WITH THE CONCEPT FOR THE AUSTRIAN CITIZEN CARD
A-SIT CONTRIBUTED TO THE EUROPEAN eID DISCUSSION

eID and ID-cards –Technology view

features of ID cards?

- biometric data (e.g. photo)
- Methods to verify
  e.g. by police

NON features?

- RECOGNISED IDENTITY
- NO methods to authenticate in with eDevices
- user has limited control

THERE IS NO NEED TO IMPLMENT BOTH ON A SINGLE CARD

SECURTIY IS NOT ONLY A TECHNOLOGY QUESTION

- Size of signature data matters (data basis, printouts, mobile applications,…)
  - e.g. RSA

Signaturwert	AeMD9fCgsL6RpSkEmXQqAopnzrs7JOsfO99AzYi0l5FGnMxDL8R6G0VsIPP4LOSgxFghMLQiXcrjpE iw4JdFNKE26ILLPJsQmWRbo9Xs35GWqTTHDgreKiFK+EO78bkJOUiXgqA1j2MqTWvQh1WIBe4fsz 0hp+UqEgRiQXsiDr5+wl5sfbEEed2x+zX7k/u99ttwW86RPUft8eW2zk6MdbuujX305LRqMbpUGJ2rsk2 ixeh8Zu/NFBBhtAFW9Rcc7Uc/irSlljns7f5z5vuZLUM1h0P1r4WV6ZoaV8kWmORLeyJRw+wX8LfKUB JESbjtzVH7LJbkebRMAHMb7ejp1g==

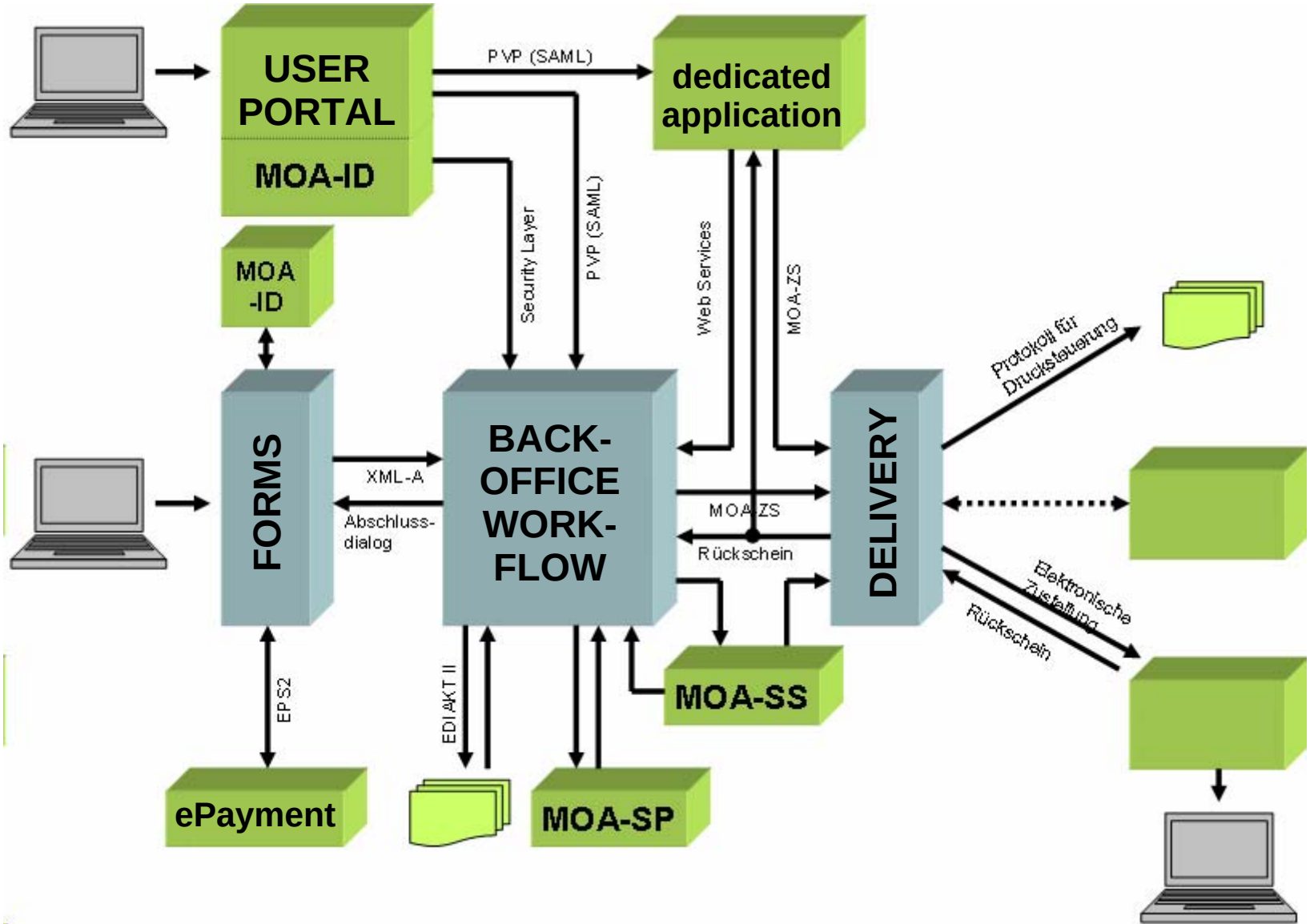
  - e.g. ECC (of same or higher security)

Signaturwert	VNmiFITMKABSqR8ewIpO7qTEIsWBfzdkqFWyNyNYnrUPP8L8CCqRSN6oHl/zmmUs

- Are contactless technologies the future of eID?
  - safe „interconnect“ eID device application
  - entry of authentication data (PIN)

- disseminating awareness and necessary knowledge

eID needs a holistic view



IDENTIFICATION

AUTHENTIFICATION

eID

SOURCE PIN

ONE WAY FUCNTION

bPK

bPK DB & APPLICATION

bPK DB & APPLICATON

DATA

NATURAL AND NON NATURAL PESONS

NATURAL PERSONS ONLY

eAuthentication

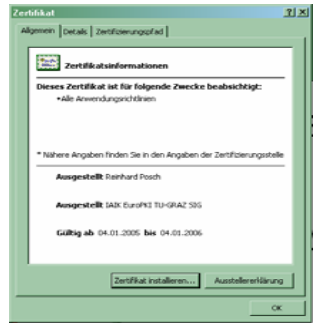
SOURCE PIN ←→ SIGNATURE

PRESONA BINDING
SIGNED BY SZRB

bPK

ACCESS
TOKEN
e.g. date& time

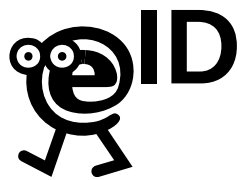
user authenticated
by use of signature



ACCESS

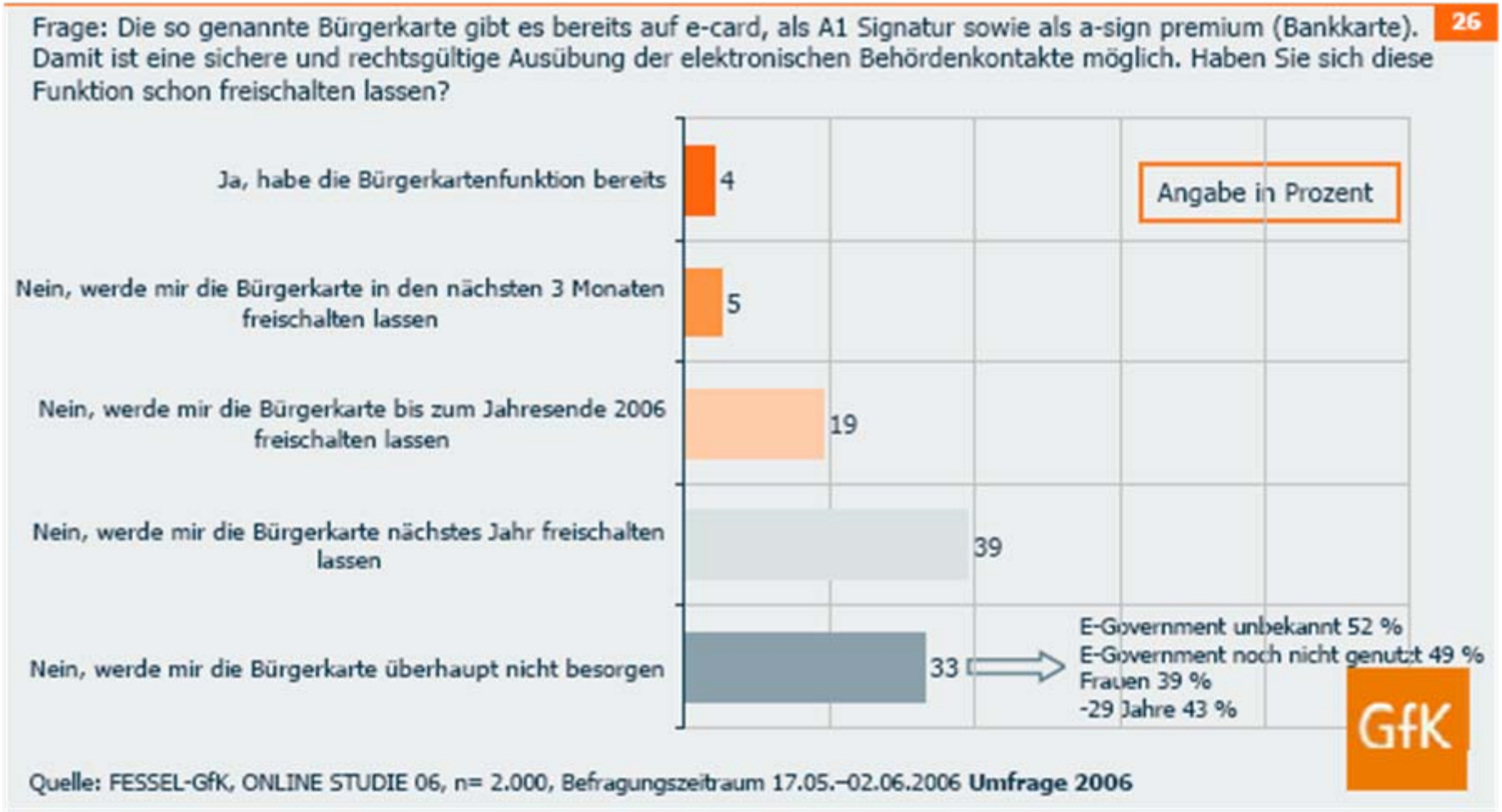
eID and businesses

- Need for a European model
- data protection needs to be included
- availability
- legal implications
- simplicity of use



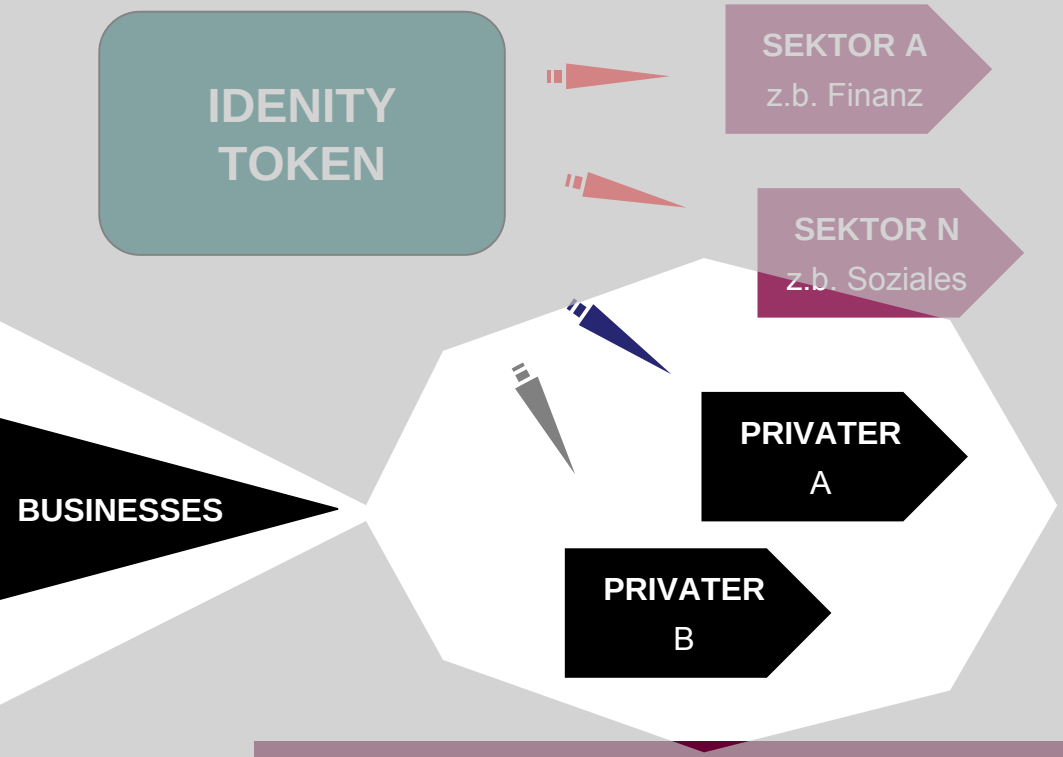
BUSINESSES CAN PROFIT FROM “SINGLE REGISTRATION”

eID is well accepted by the user



FRACTIONAL PIN AND BUSINESSES

CITIZEN CARD >> FRACTIONAL PIN



- ONE WAY FUNCTION
- eID within a sector
- businesses can be treated as sectors

Cyrpto: ensures strong binding and sector splitting

GENERAL PRINCIPLE: NO ADDITIONAL RISK

eID Cards and encryption

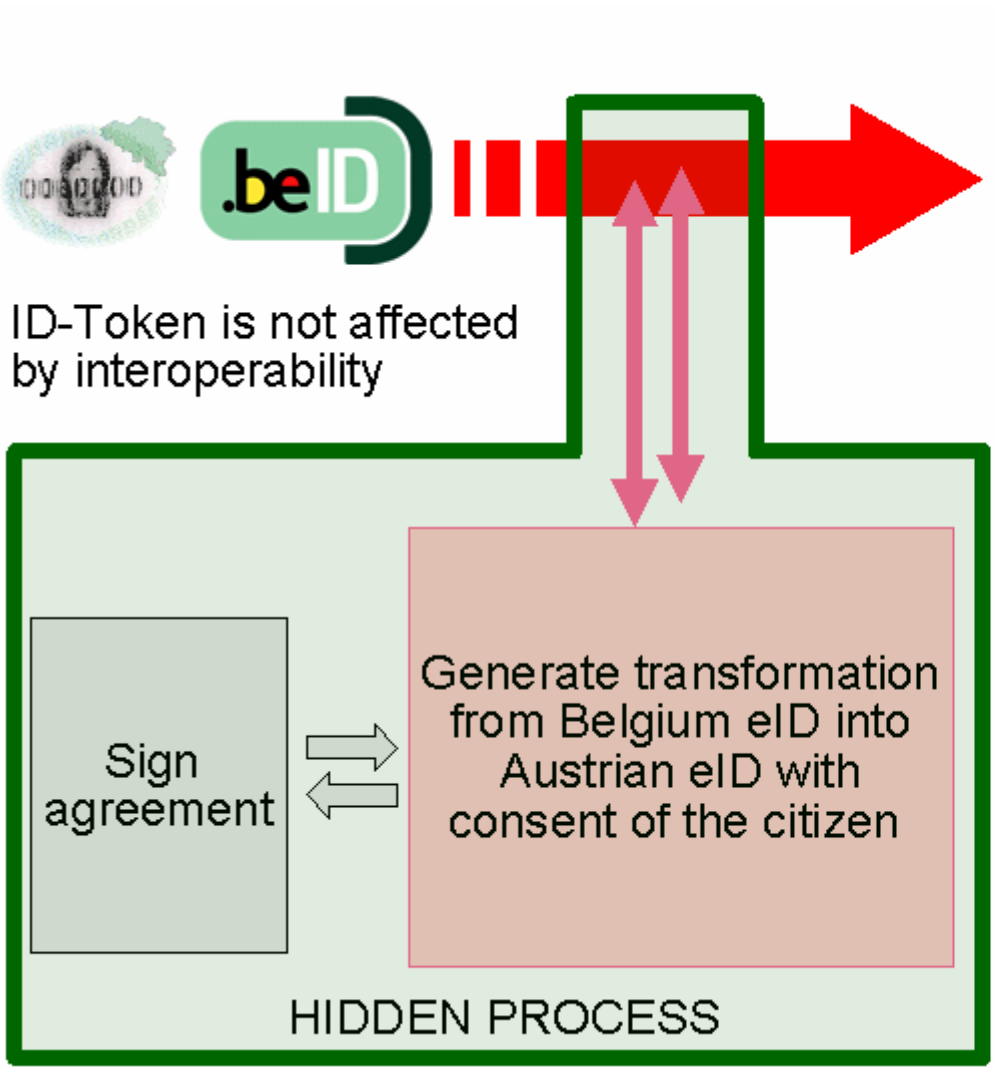
- eID = ID + Security (Signature)
  - with eID a single identity may be linked to several tokens
- with encryption the SECRET (key) must exist prior to encryption.
  - replacement, transition etc will NOT work (the same way)

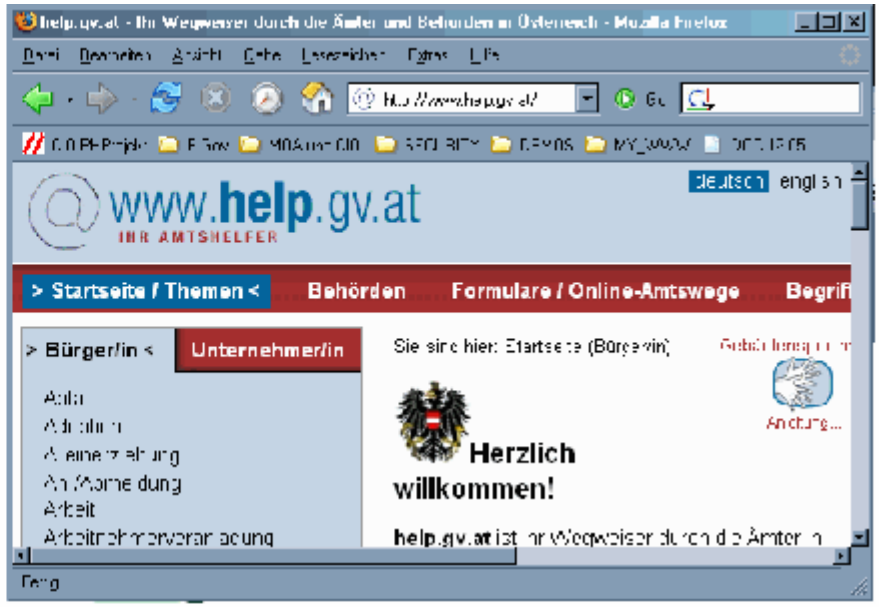
- KEY – MANAGEMENT
  - Third Party?
  - private?
  - risk of loosing the key

eID and international cooperation

- compatible technologies – the challenge
- European cooperation within i2010
  - eID
  - eDOC
  - eProcurement
  - eInclusion
- LARGE SCALE DEMONSTRATORS
  - to gain experience with eID and interoperability

EXAMPLE: BELGIUM eID in AUSTRIA





Application is not affected
by interoperability

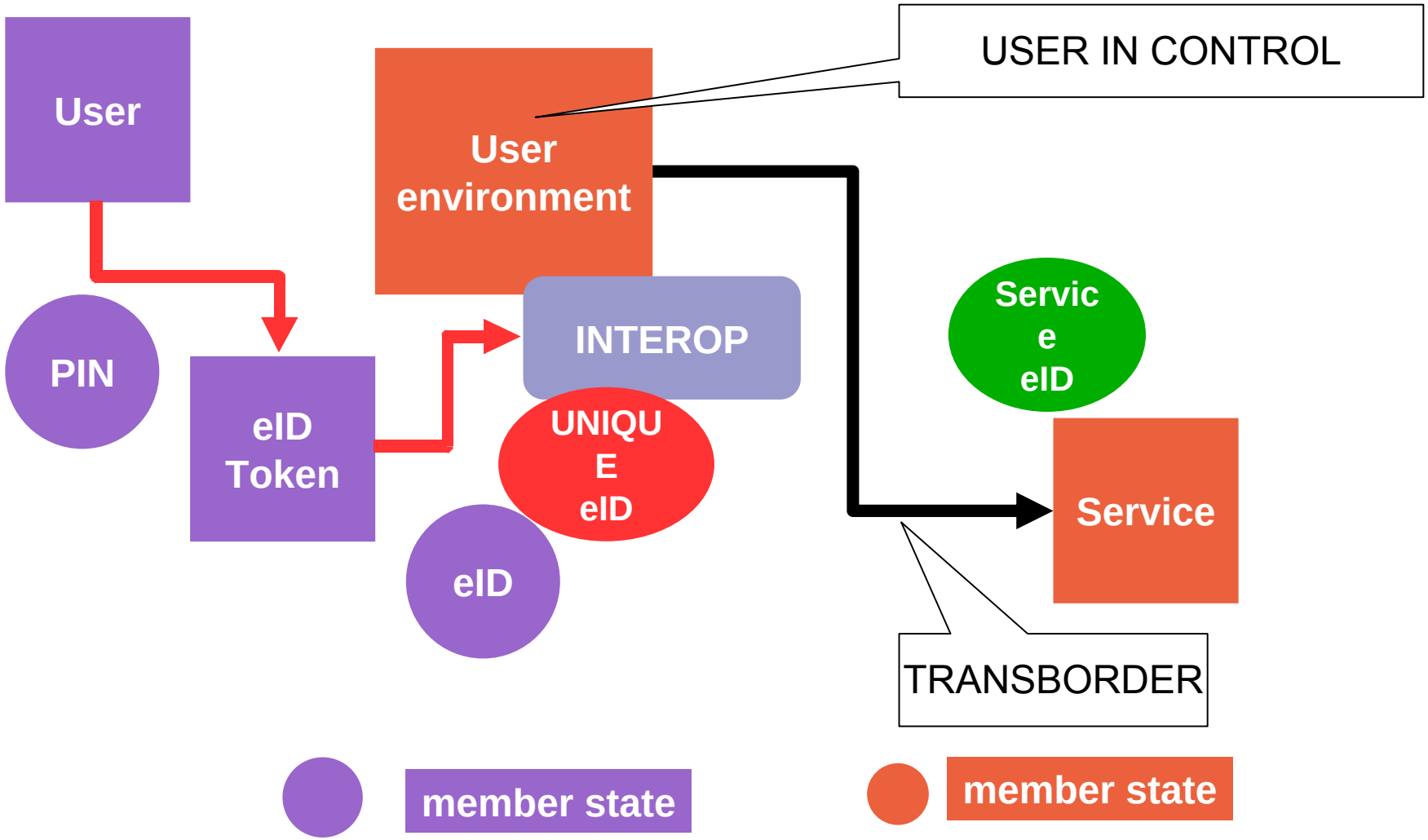
LEGAL AGREEMENTS?
TECHNICAL INTEROPERABILTY?
……

the i2010 goals

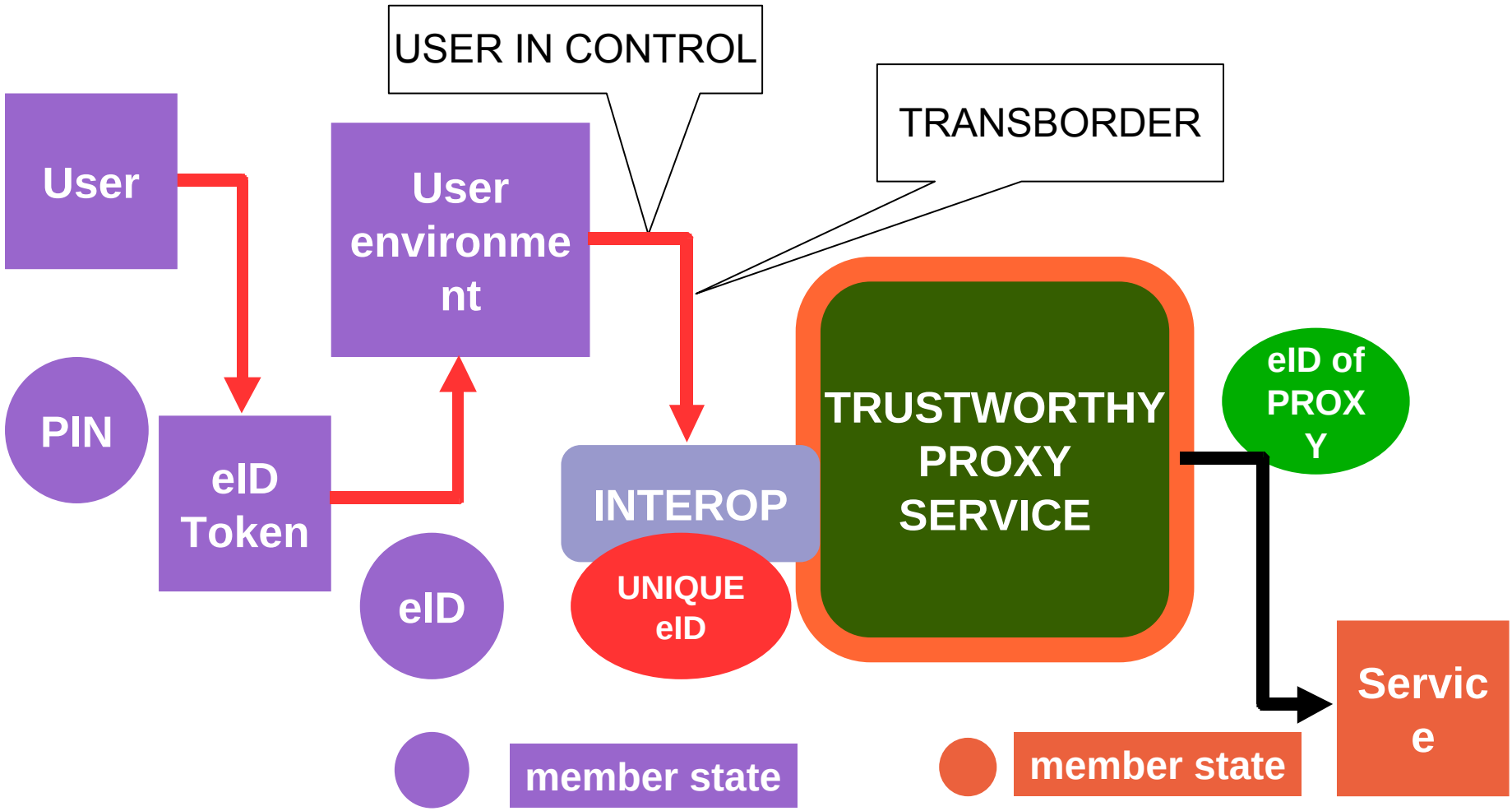
- identify obstacles
- experience showcases
- communicate interoperability
- evaluate security needs
- Identify further steps…

i2010
Information Space
Innovation & Investment in R&D
Inclusion

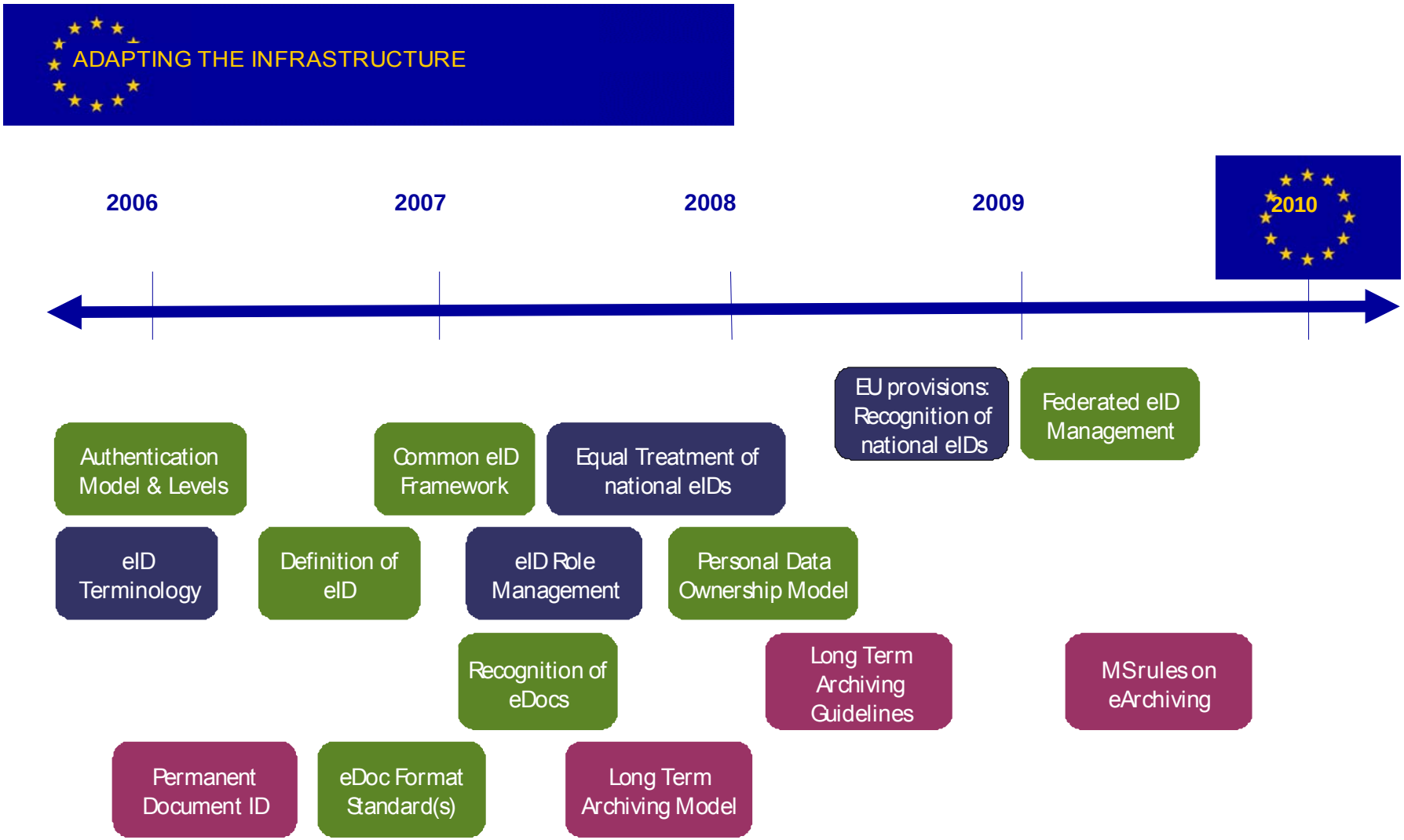
interoperability at the user side



interoperability through proxies



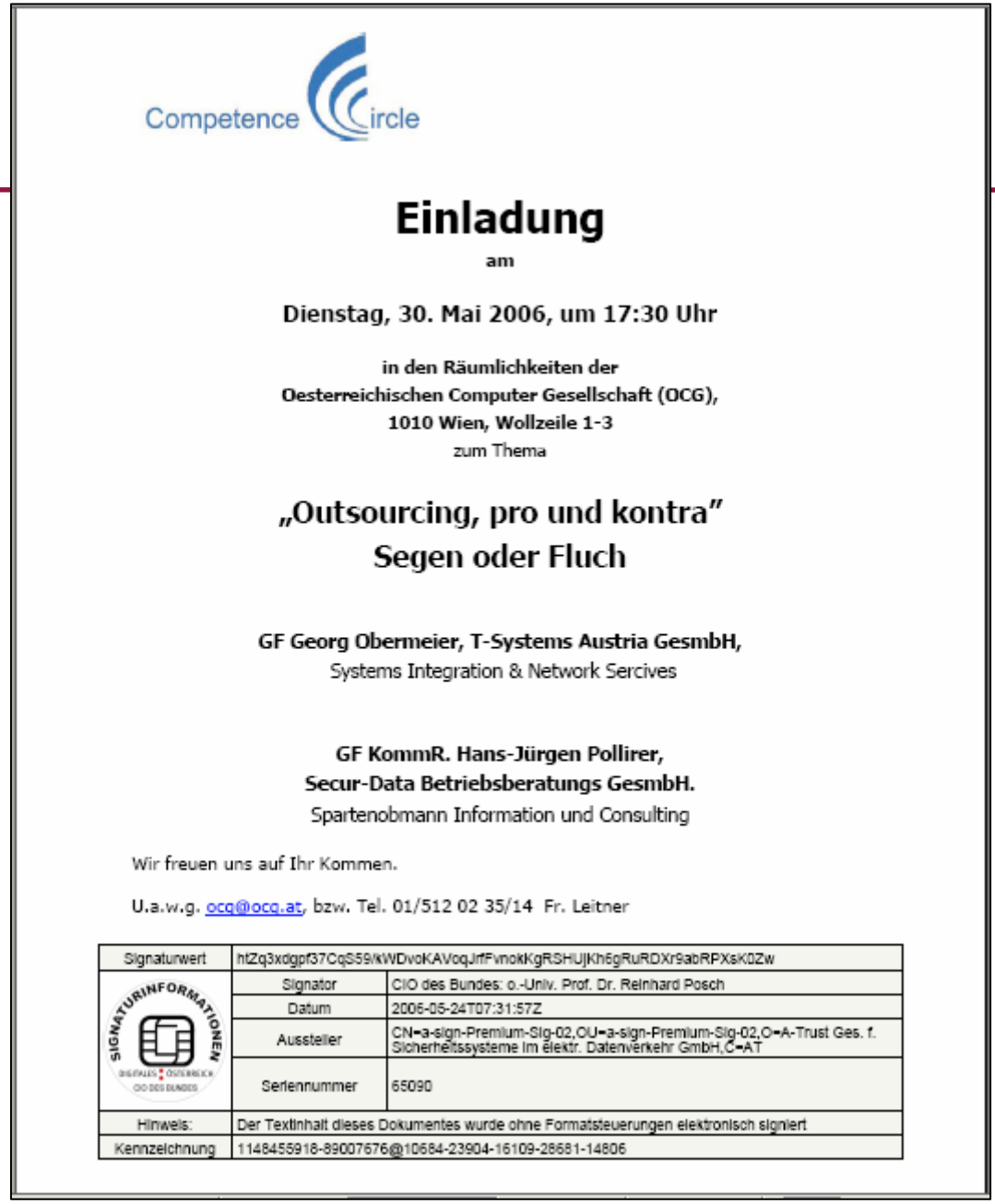
i2010 signposts



eID and electronic documents

- there is no eGoverment without eDocuments
- signature must ensure quality cross media
- XML-structures – bridging the language gap, fostering inclusiveness (e.g. blind people)

we need a notion “what is an original”



Competence Circle

Einladung

am

Dienstag, 30. Mai 2006, um 17:30 Uhr

in den Räumlichkeiten der
Oesterreichischen Computer Gesellschaft (OCG),
1010 Wien, Wollzeile 1-3
zum Thema

„Outsourcing, pro und kontra"
Segen oder Fluch

GF Georg Obermeier, T-Systems Austria GesmbH,
Systems Integration & Network Sercives

GF KommR. Hans-Jürgen Pollirer,
Secur-Data Betriebsberatungs GesmbH.
Spartenobmann Information und Consulting

Wir freuen uns auf Ihr Kommen.

U.a.w.g. ocg@ocg.at, bzw. Tel. 01/512 02 35/14 Fr. Leitner

Signaturwert	htZq3xdgpf37CqS59/kWDvoKAVoqJrfFvnokKgRSHUjKh6gRuRDXr9abRPXsK0Zw	
SIGNATURINFORMATIONEN	Signator	CIO des Bundes: o.-Univ. Prof. Dr. Reinhard Posch
	Datum	2006-05-24T07:31:57Z
	Aussteller	CN=a-sign-Premium-Sig-02,OU=a-sign-Premium-Sig-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Seriennummer	65090
Hinweis:	Der Textinhalt dieses Dokumentes wurde ohne Formatsteuerungen elektronisch signiert	
Kennzeichnung	1148455918-89007676@10684-23904-16109-28681-14806	

RFID the future eID technology?

- through its independent structure RFID offers even enhanced security

- still we have issues to sort out

  - how is the intended use under control in an open system
  - how is the strong linking to the selected device managed
  - how is the authentication data (PIN) entered in a safe way

RESEARCH HAS TO GIVE ANSWERS SO THAT DATA PROTECTION DOES NOT BECOME AN ISSUE

EU AT

Österreich 2006 . Präsidentschaft der Europäischen Union
Austria 2006 . Presidency of the European Union
Autriche 2006 . Présidence de l'Union européenne

Administration on the Net

An ABC Guide to E-Government in Austria

CIO – AUSTRIA
reinhard.posch@cio.gv.at