



# Demonstrations

First steps towards eID Interoperability

Herbert Leitold

[Herbert.Leitold@a-sit.at](mailto:Herbert.Leitold@a-sit.at)

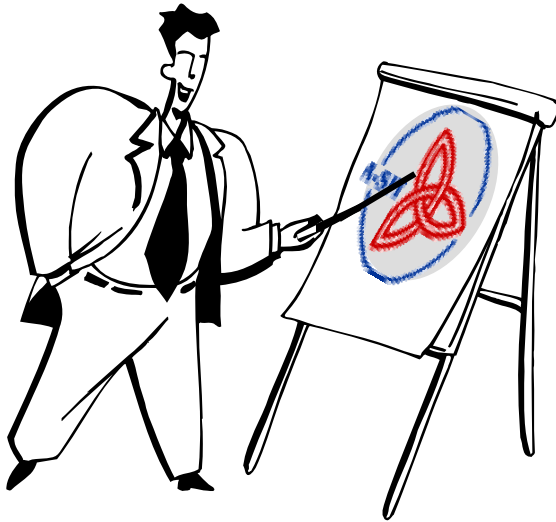


---

Secure Information Technology Center - Austria

Brussels, 4th May 2006

# Table of Contents



- AT foreign eID-integration
  - Basics of AT eID / IDM model
  - Foreign eID integration concept
- BE signatures with AT application

*Demo* Word 2007 signatures

*Demo* PDF signature

- BE eID in AT Webshop

*Demo* Activate BE eID card as Austrian citizen card

*Demo* Using a BE card in Austrian service

# Recurring ID concept

- eGovernment Act [art. 2(3) and art. 6(5)]

“**Recurring identity**”: designation of a specific person (data subject, No 7) 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;

For the purpose solely of validating recurring identity, a person may, at his request, be provided with a **substitute sourcePIN** by the sourcePIN Register Authority, where ...

- SourcePIN register authority order [art. 11(2)]

If the application is made using an eID that holds a **foreign personal identifier** included in a signature creation device, the Source PIN Register Authority may use this identifier as a substitute sourcePIN , if the identifier – in its country of origin – is an identifier in official proceedings and is linked to reliable means of authentication ....

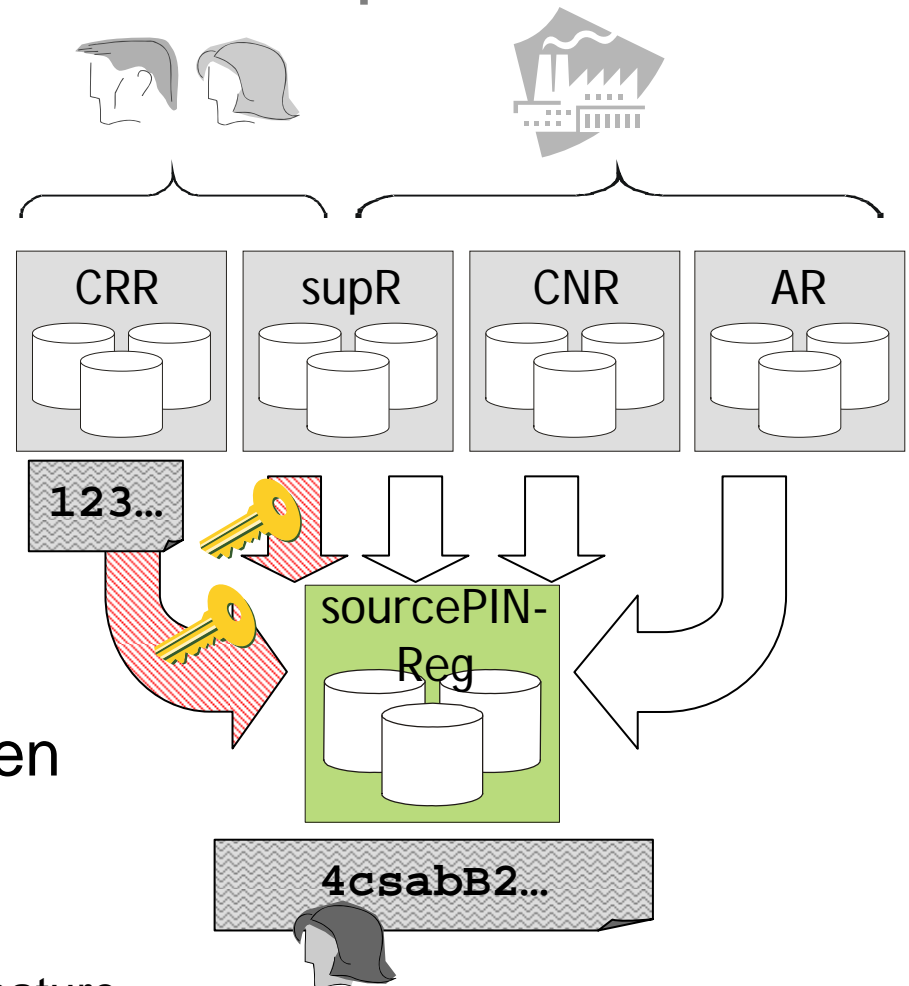
# sourcePIN Register – unique IDs

- Source PINs

- derived from unique IDs in registers
- strong encryption for physical persons
- sourcePIN Register maintained by Data Protection Commission

- SourcePIN stored in Citizen Card Environment

- Data structure *Identity Link*
- Links identity to electronic signature

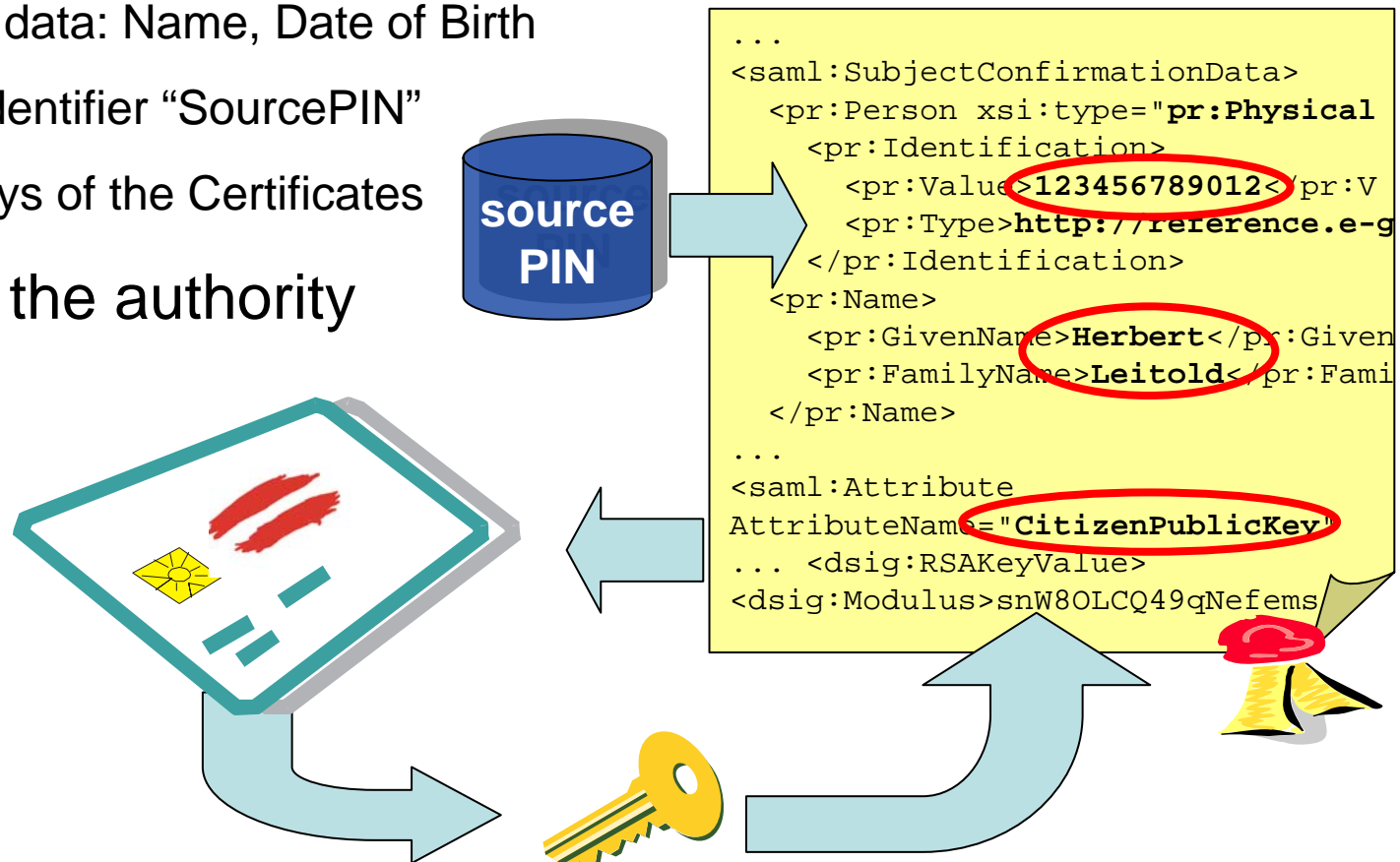


# Identity Link

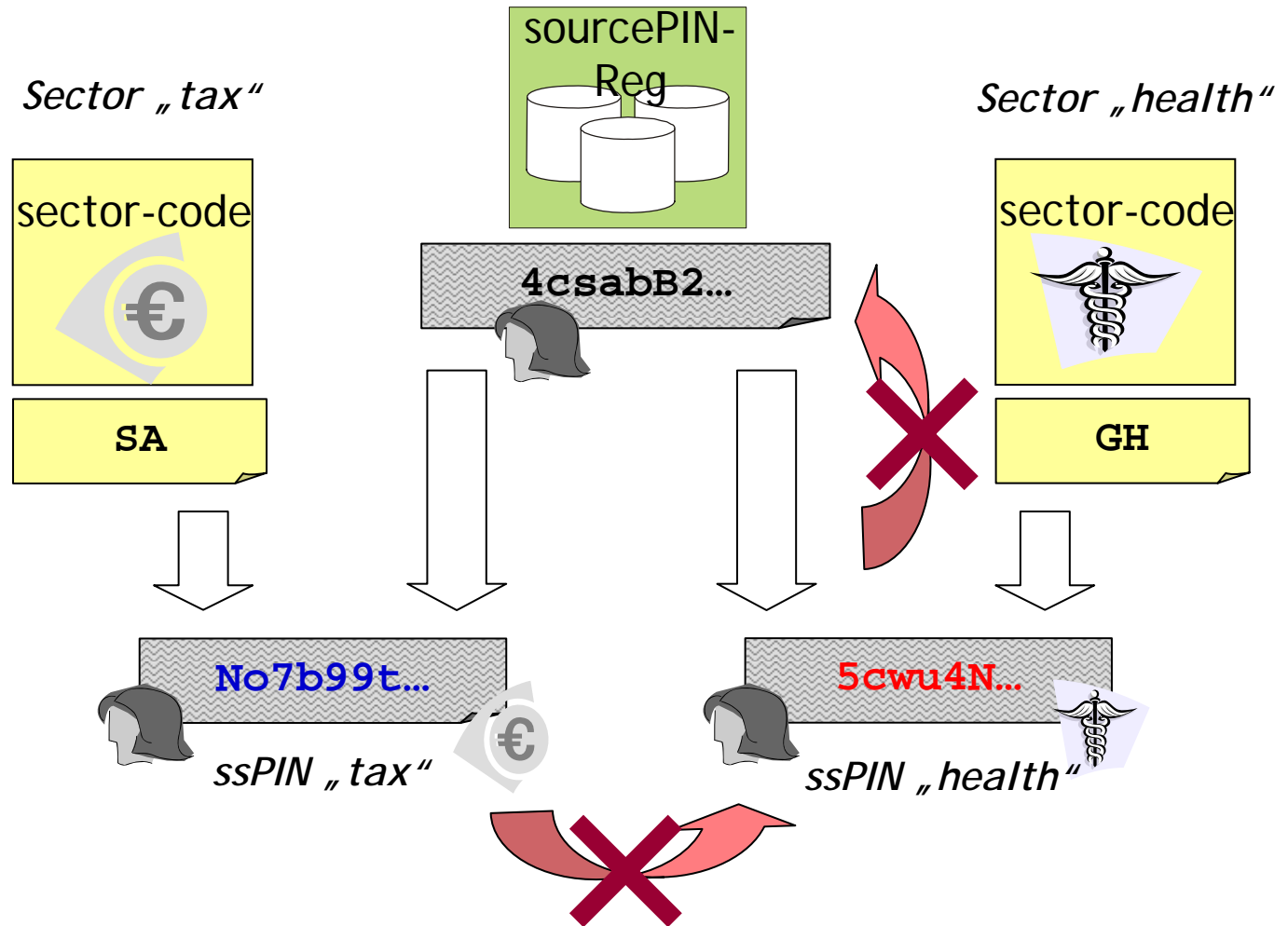
- XML data structure stored in the Citizen Card that holds

- Personal data: Name, Date of Birth
- Unique Identifier "SourcePIN"
- Public keys of the Certificates

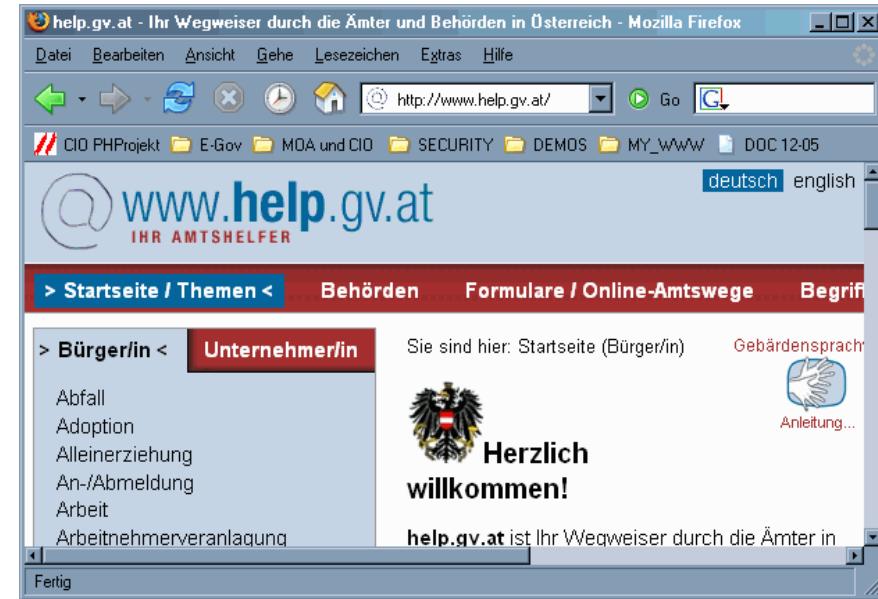
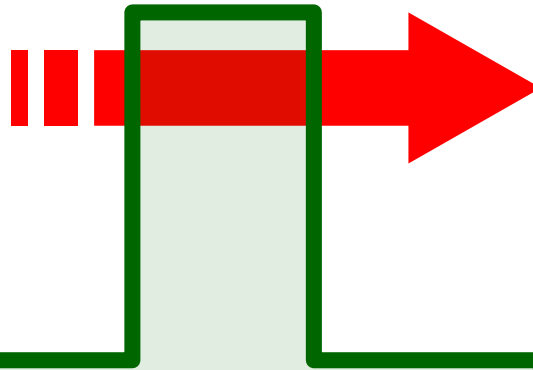
signed by the authority



# Sector-specific IDM concept



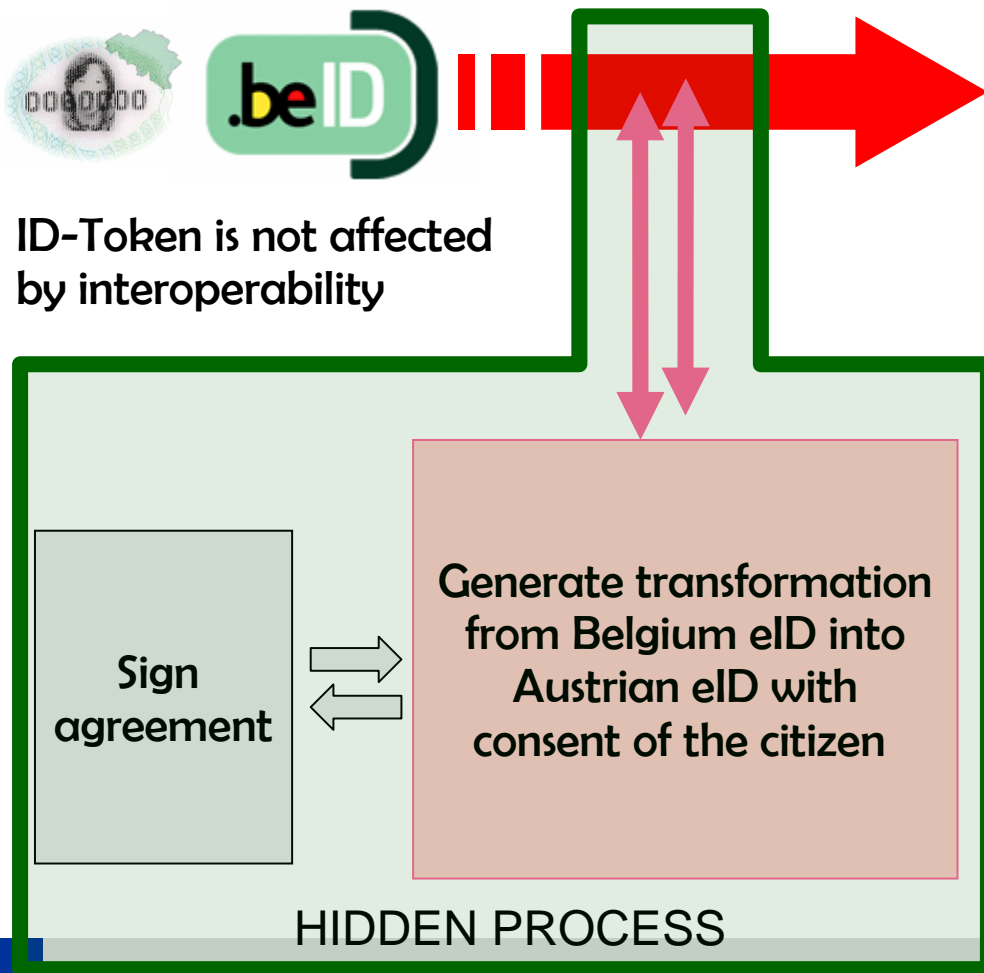
# AT eID in AT eGovernment service



Free software, several vendors on the market

Transformation sourcePIN → ssPIN  
done in the *Citizen Card Environment*  
(Software running on the citizen's PC)

# example BE → AT eID



ID-Token is not affected by interoperability



Application is not affected by interoperability

LEGAL AGREEMENTS?  
TECHNICAL INTEROPERABILITY?

.....



# Foreign-eID integration

- Integration of foreign eID
  - Austria has so far integrated the Belgian, the Estonian, the Finish, and the Italian eID into its domestic IDM concept
  
- Uses “Recurring Identity” concept
  - Unique identifier of foreign certificate used as “substitute sourcePIN”
  - Service started in 02/2006



# Demos

- Create AT Official Signature
  - Concept of AT Official Signature



*Demo* Create using Office 2007

*Demo* Using PDF Documents


- Belgian eID in AT process

*Demo* Activate BE signature

*Demo* Use it in AT process

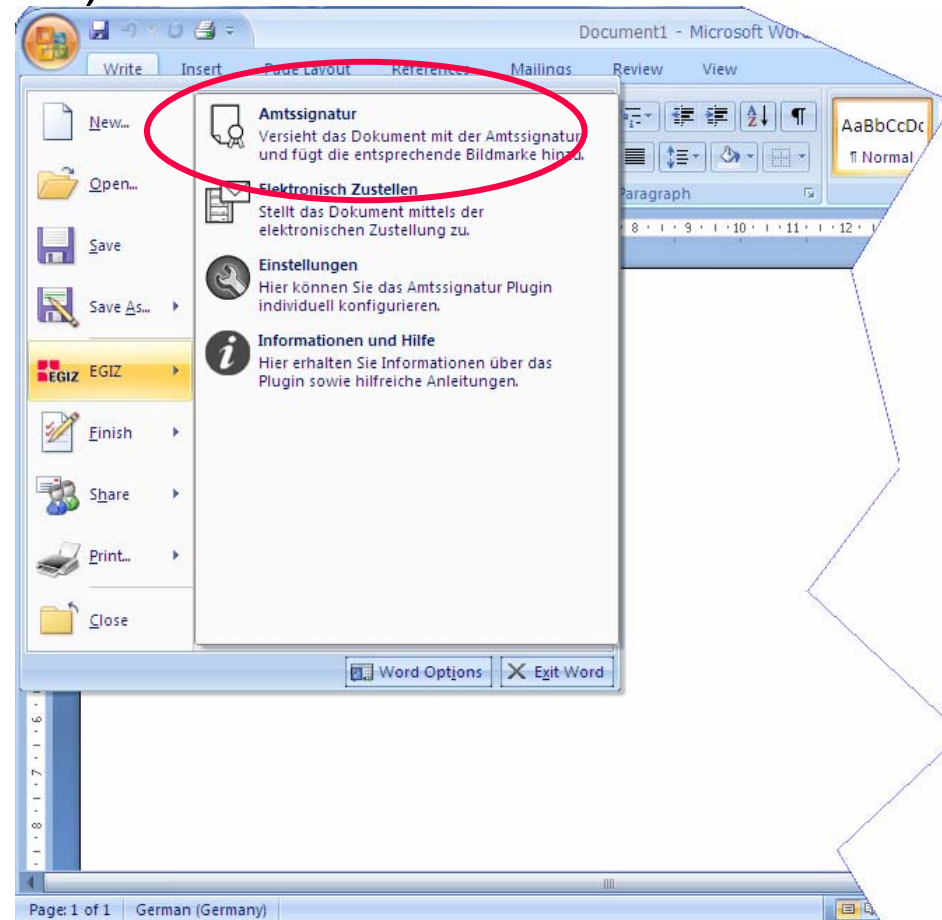
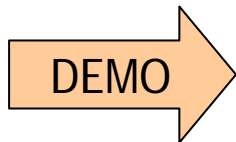
# Official signature

- Enclose electronic signature as visible data with the document
  - Maintain probative value on print outs

	Signiert von	BMI SU-ZMR	signing person
	Datum	2005-09-04T11:30:38	date and time
	Zertifikat	A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH, a-sign-corporate-light-02, AT (80524)	CA and serial-number
	Verfahren	urn:publicid:bmi.gv.at:ZP+bescheid+mb-1.2	unique form identifier
Signaturwert	QMTAo0s5c/fZK/txebJvcUnGaxBGChAeFpxuzGSseliP3822awt8+HSI9re fdk0 dQG9KYRpHfWnFpbjqSvHCHRm6C/QnwZex2MF+Euzr36O36IG1MuOu1EOQJ31L HLcEbBD0jppW0970gw/ A8e00XVPO/hsHgtE7FRC09do=		
			signature value

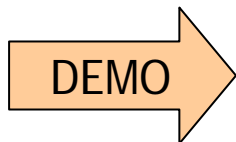
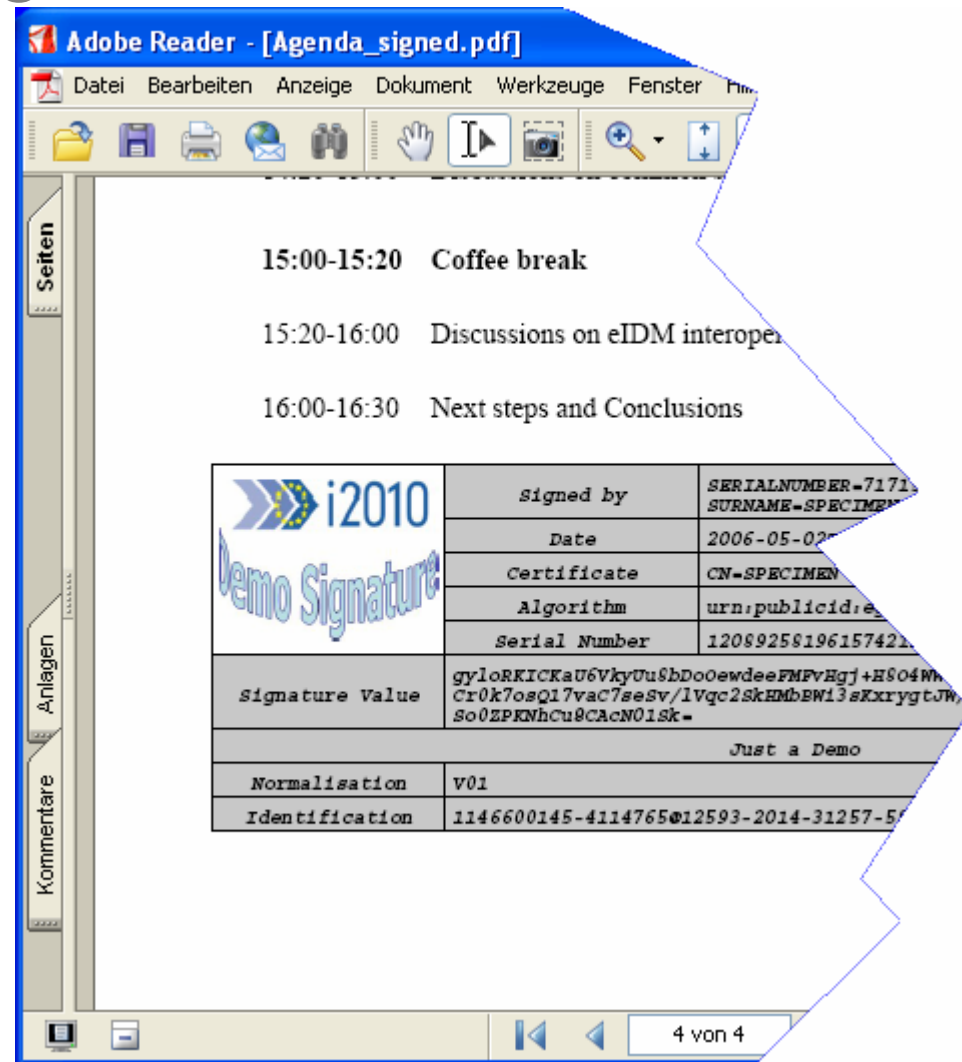
# Example: Using Word 2007

- Word 2007 (formerly Office 12) has signature capabilities
- EGIZ developed a plugin to
  - create official signature
  - deliver signed document electronically



# Example: Sign PDF 2007

- PDF documents widely used
- To sign and attach official signature
  - extract raw text
  - normalize
  - sign
  - feed back signature

Adobe Reader - [Agenda\_signed.pdf]



Datei Bearbeiten Anzeige Dokument Werkzeuge Fenster

Seiten

15:00-15:20 Coffee break

15:20-16:00 Discussions on eIDM interoper

16:00-16:30 Next steps and Conclusions

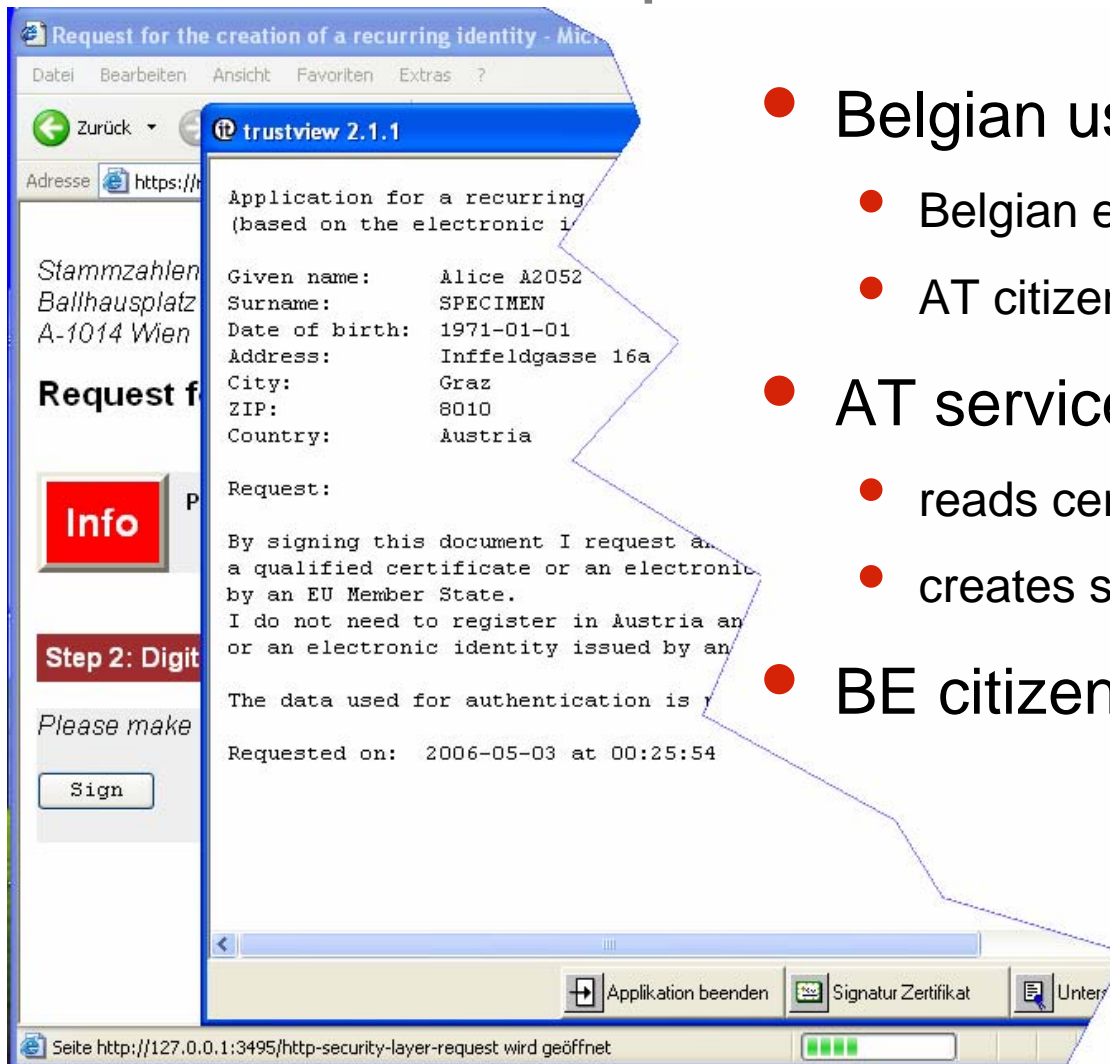
 	Signed by	SERIALNUMBER=7171 SURNAME=SPECIMEN
	Date	2006-05-02
	Certificate	CN=SPECIMEN
	Algorithm	urn:publicid,e
	Serial Number	12089258196157421
Signature Value	gylorKICKaU6VkyUuSbDoOewdeeFMPvHgj+H804Wh Cr0k7osQ17vac7eeSV/1Vqc2SkEMBw13sKxrygtJW So0ZPRNhCu9CAcN01sk-	
Just a Demo		
Normalisation	V01	
Identification	1146600145-4114765@12593-2014-31257-5	

Anlagen

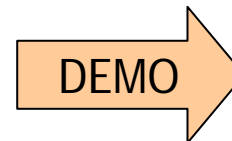
Kommentare

4 von 4

# Example: Activate BE eID

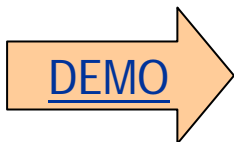
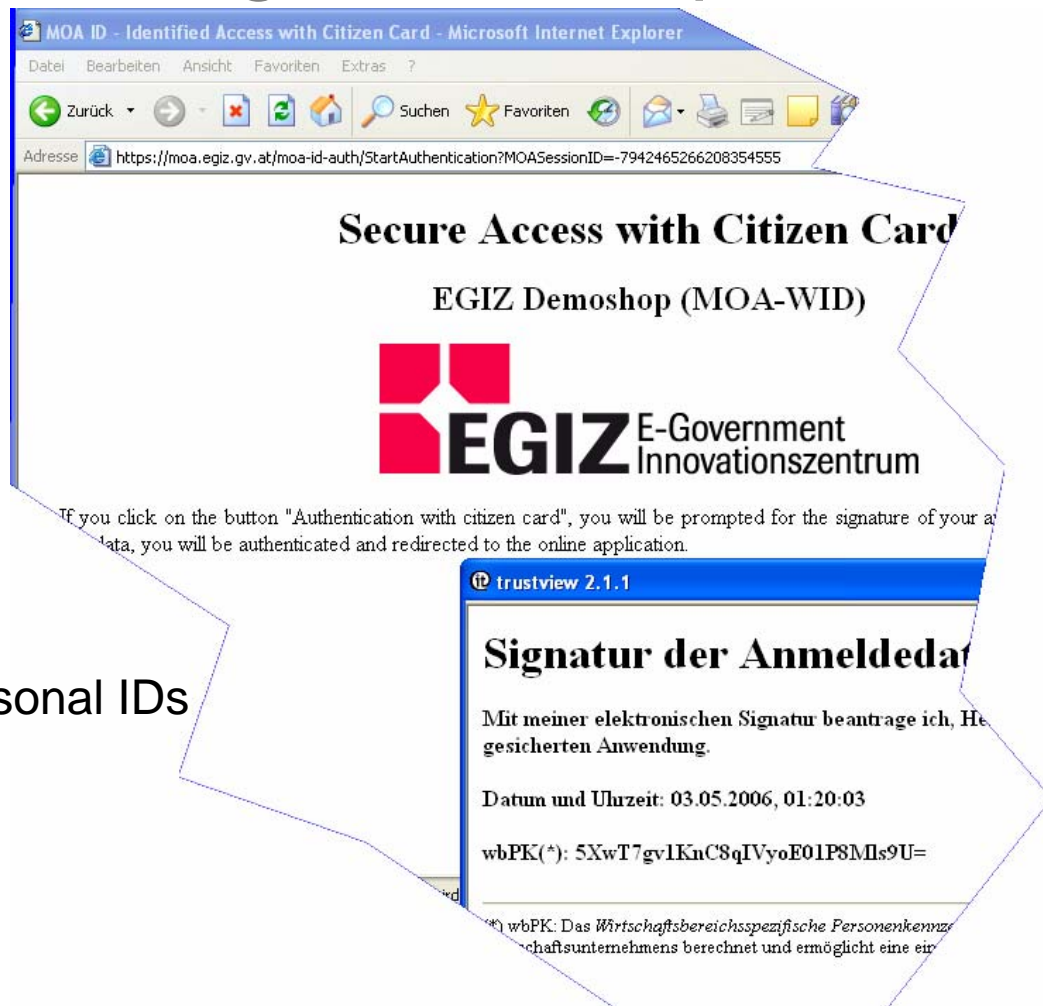


- Belgian user has
  - Belgian eID
  - AT citizen card software installed
- AT service
  - reads certificate
  - creates substitute PIN
- BE citizen signs application



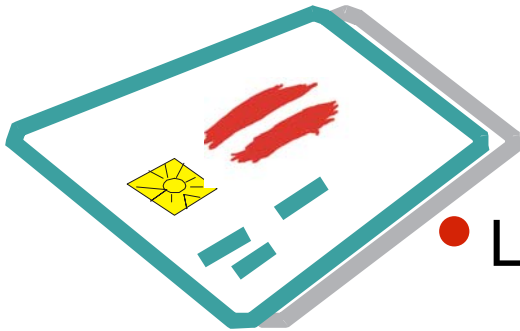
# Example: Accessing a Webshop

- Identity Link created for BE eID is used in AT application
- Webshop is a private sector application
  - Additional data protection measures
  - Private-sector specific personal IDs



# Conclusions

- AT has implemented an
  - decentralized model using foreign tokens
  - interoperability is handled at the user environment level
- Legal basis settled by eGovernment Act
- Identity Management model allows data protection compliant “export” of AT eID using the sector-specific PIN concept





Thank you for your attention



Herbert Leitold  
[Herbert.Leitold@a-sit.at](mailto:Herbert.Leitold@a-sit.at)

---

Secure Information Technology Center - Austria

Brussels, 4th May 2006