

# eSignatures in Austria

Herbert Leitold  
Reykjavik; May 23<sup>rd</sup>, 2013

# Presentation Overview

- Some Highlights
- Is it used?
- eID - eSig Relation
- Citizen Signature
- Official Signature

# Signature highlights in Austria

- Promulgation: Federal laws published by an electronic version on the Internet (2004)
- Qualified signatures for free for citizens
  - Mass deployment of smartcard SSCDs from 2005
  - Mobile phone qualified signature (STORK, 2009)
- Administrative acts and rulings electronically signed; mandatory since 2011, even if printed
- Professions' archives (lawyers, notaries, civil engineers) hold ~6 mio. el. signed documents

# Major initiatives – Citizen Cards



## Bank cards (ATM cards)

Each bank card issued from March 2005 has been an SSCD (as of 1999/93/EC) – about 6.5 mio. cards  
Activation to be paid by citizen



## Health insurance cards:

Rollout Mai-Nov. 2005, is an SSCD  
100 % coverage reached end of Nov. 2005 (~9 mio.)  
activation free of charge for citizens



## Mobile signatures:

- 2005-2008
- relaunched 2009 (STORK)
- free of charge for citizens



## Further initiatives:

- official's service card
- CSP signature cards
- student service cards, etc.

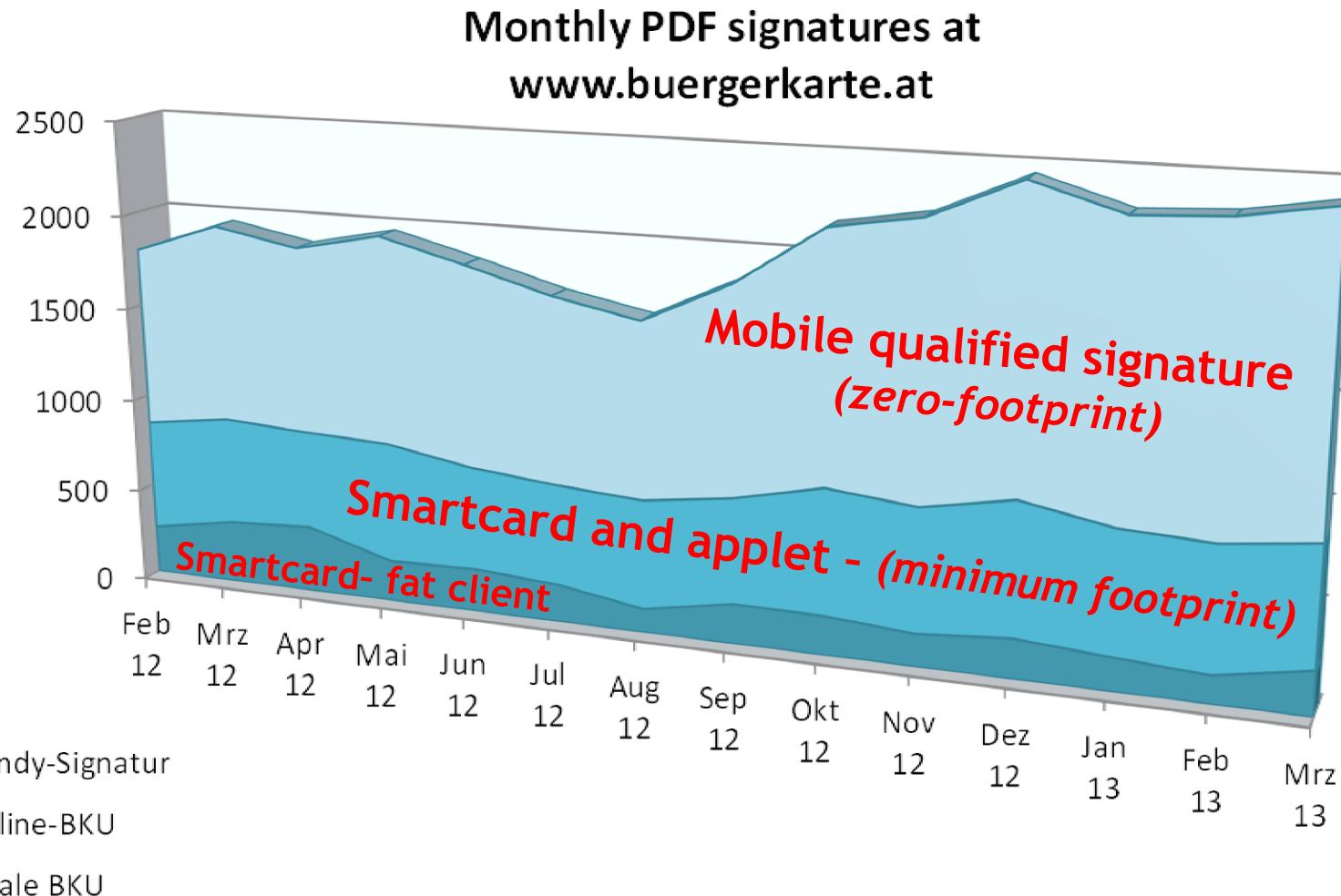


**so far, no  
ID card with chip**

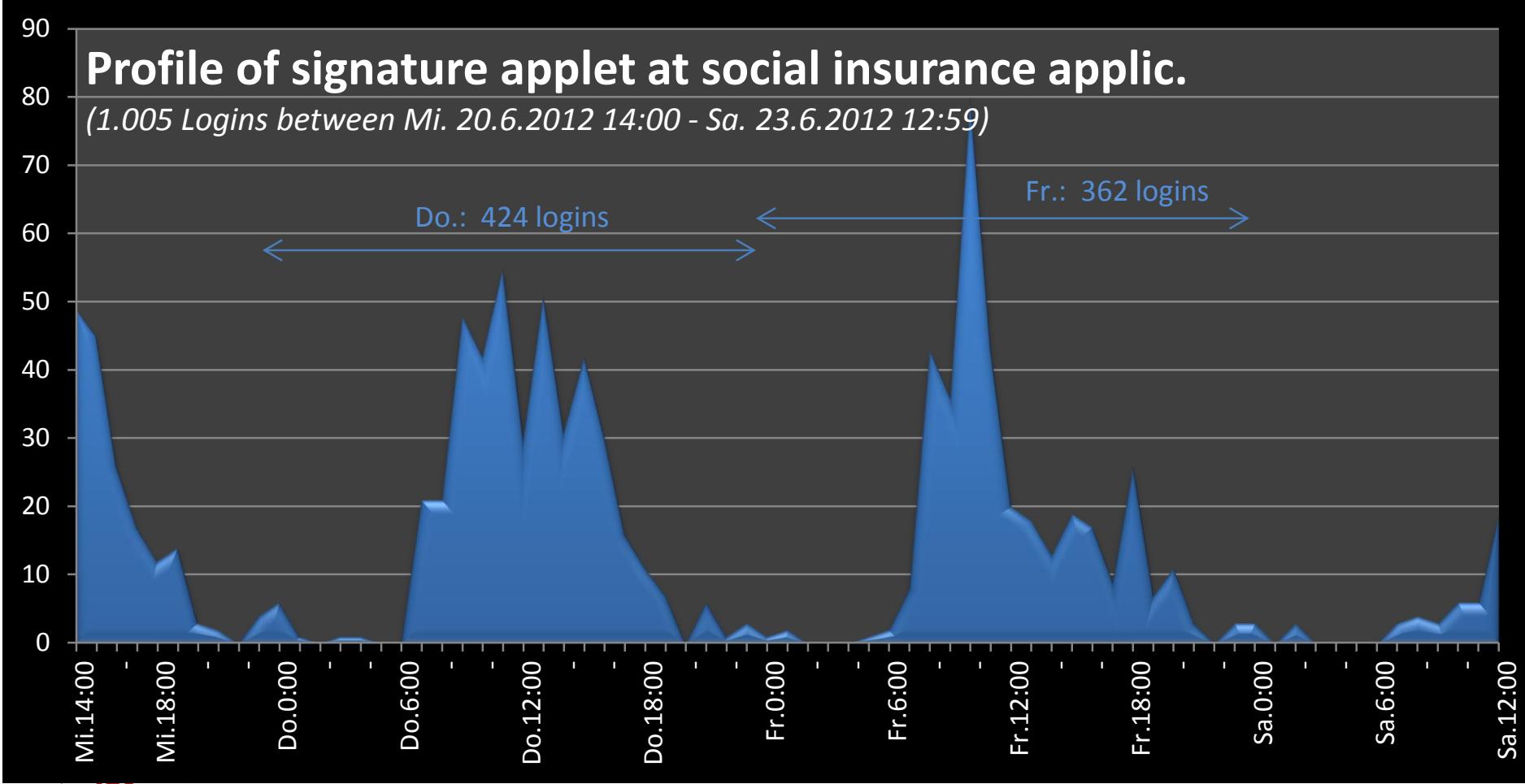
# Presentation Overview

- Some Highlights
- Is it used?
- eID - eSig Relation
- Citizen Signature
- Official Signature

# 1<sup>st</sup> use example: PDF - upload&sign - service



# 2<sup>nd</sup> use example: a daily profile



# Presentation Overview

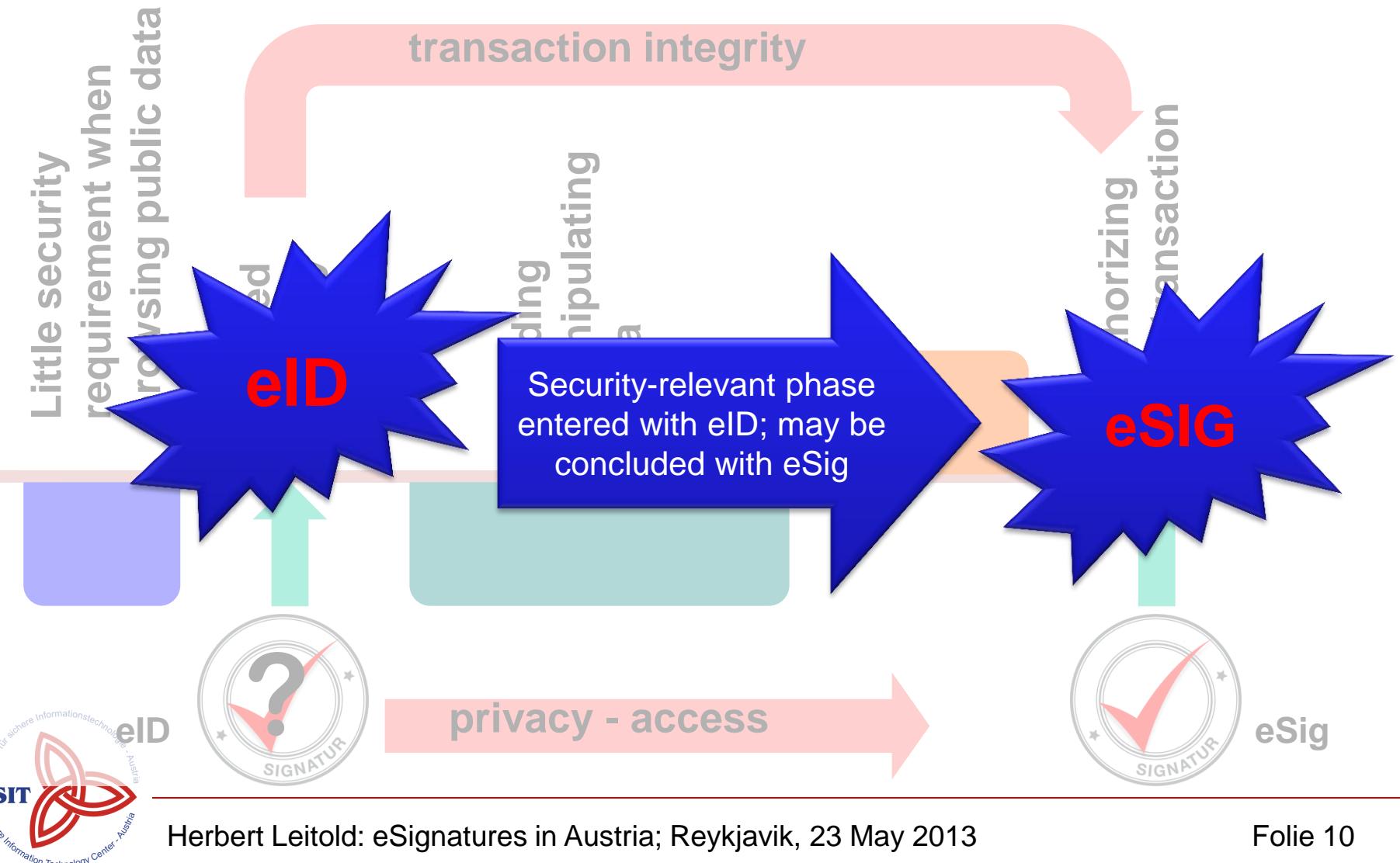
- Some Highlights
- Is it used?
- eID - eSig Relation
- Citizen Signature
- Official Signature

# Citizen transaction and security

Little security  
requirement when browsing  
public data

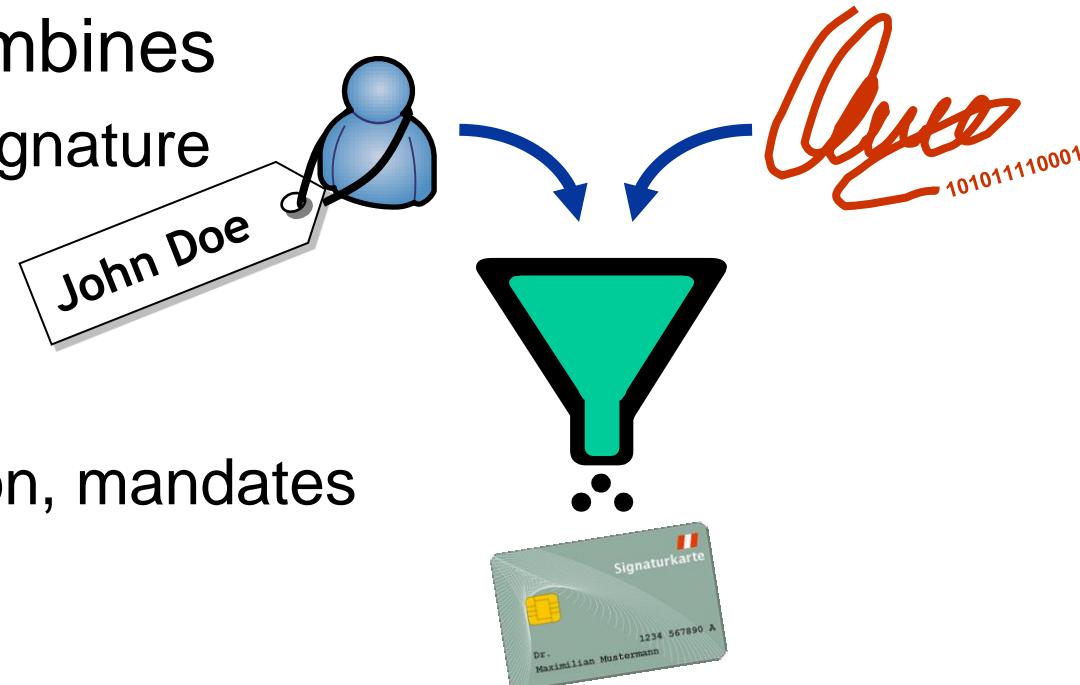


# Citizen transaction and security



# Citizen Card - Basic functions

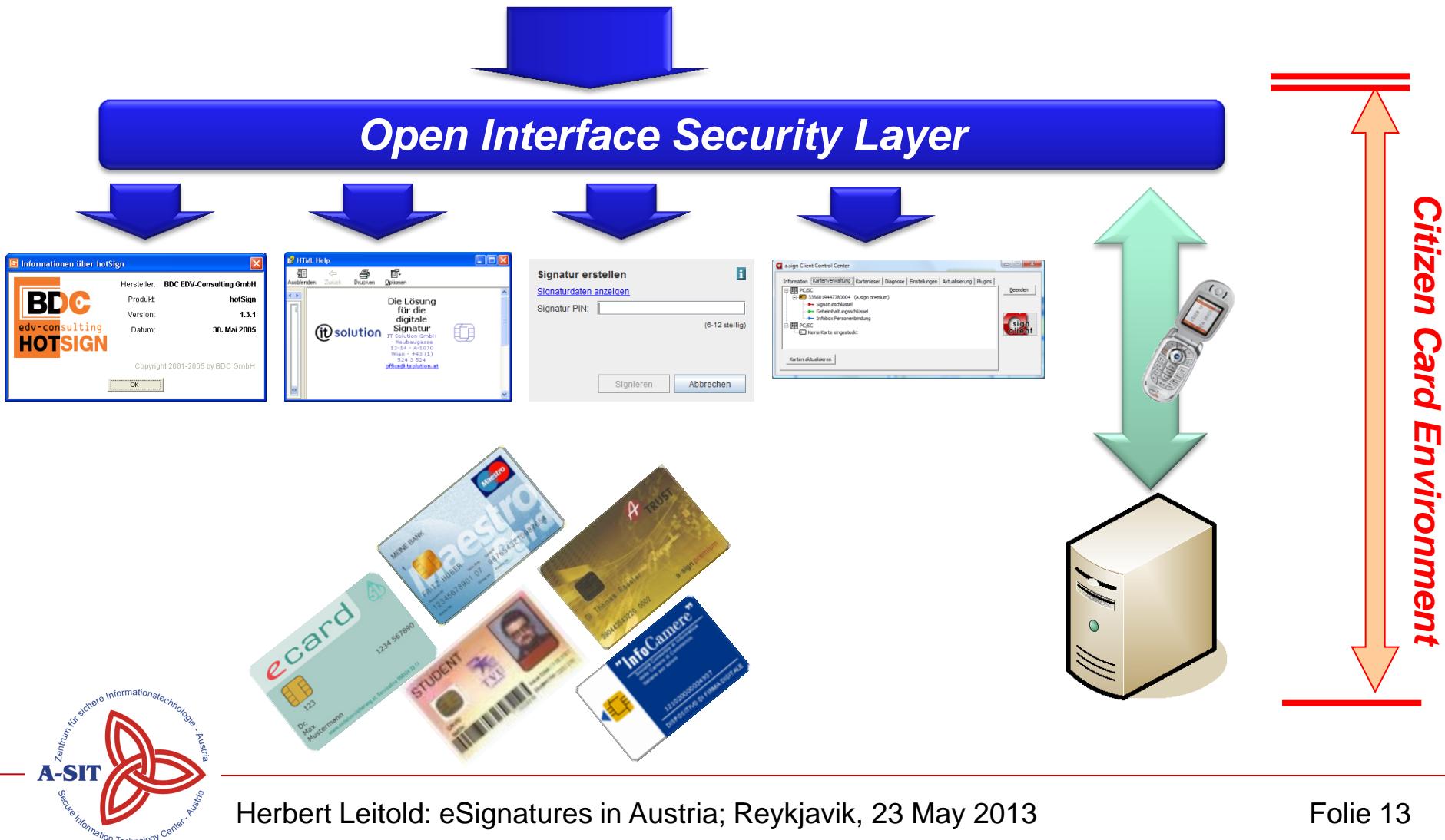
- The Austrian Citizen Card is a concept, not a specific technology
- The Citizen Card combines
  - qualified electronic signature  
*Authentication*
  - electronic identity  
*Identification*
  - data on representation, mandates  
*Representation*



# Presentation Overview

- Some Highlights
- Is it used?
- eID - eSig Relation
- Citizen Signature
- Official Signature

# Integration of technologies



# High-level interface



**Open Interface Security Layer**

- Simple XML requests via Web browser

```
<?xml version="1.0" encoding="UTF-8"?>
<CreateXMLSignatureRequest xmlns="http://www.cio
    <KeyboxIdentifier>SecureSignatureKeypair</K
    <DataObjectInfo Structure="enveloping">
        <sl:DataObject>
            <sl:XMLContent>Data to be signed
            </sl:XMLContent>
        </sl:DataObject>
        <sl:TransformsInfo>
            <sl:FinalDataMetaInfo>
                <sl:MimeType>text/plain</sl10:Mim
            </sl:FinalDataMetaInfo>
        </sl:TransformsInfo>
    </DataObjectInfo>
</CreateXMLSignatureRequest>
```

# Citizen Card Environment Variants

Local installation



Login mit Bürgerkarte

KARTE      HANDY

Informationen zur Bürgerkarte

Lokale DRU

Minimum-footprint

finanzonline.bmf.gv.at

Login mit Bürgerkarte

Infobox-PIN eingeben

Infobox-PIN:  (4 stellig)

OK

Login mit Zugangskennungen

Teilnehmer-Identifikation:

Benutzer-Identifikation:

PIN:

Online-Erstanmeldung      Erstanmeldung



Mobile Phone

Mobiltelefonnummer:

Bitte auswählen

Signatur Passwort:

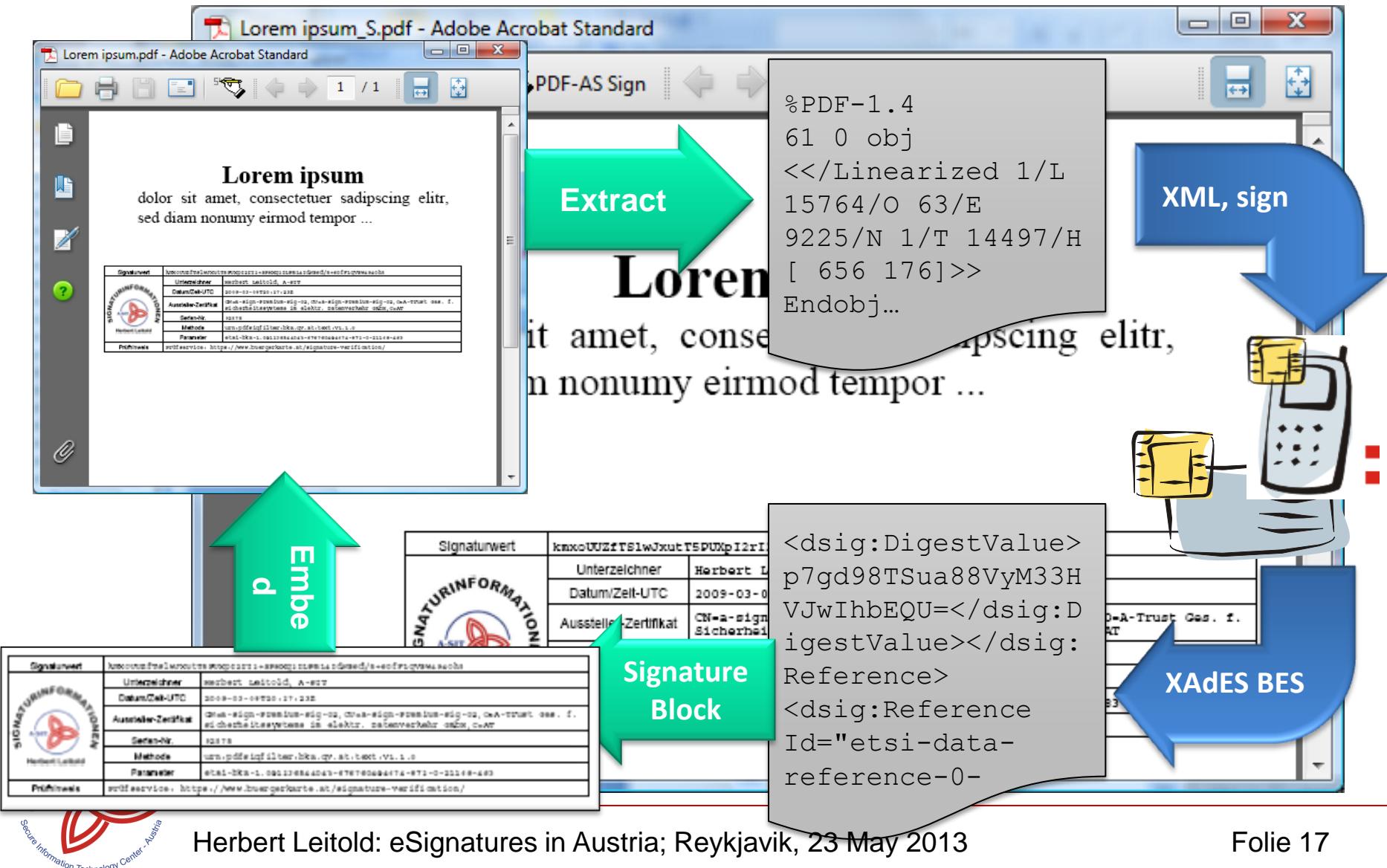
Identifizieren      Abbruch



# Signature formats

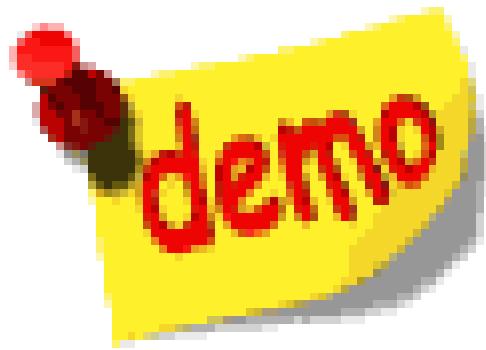
- Security Layer Specification provides for
  - XMLDSIG (XAdES)
  - CMS (CAdES)using the browser as the software controlling the process.
- With the broader use of PDF, solutions have been needed
  - Some issues with early PDF signature formats
  - Defined an on format based on XAdES
    - Will be migrated to PAdES soon

# PDF-AS signature process



# A short demo

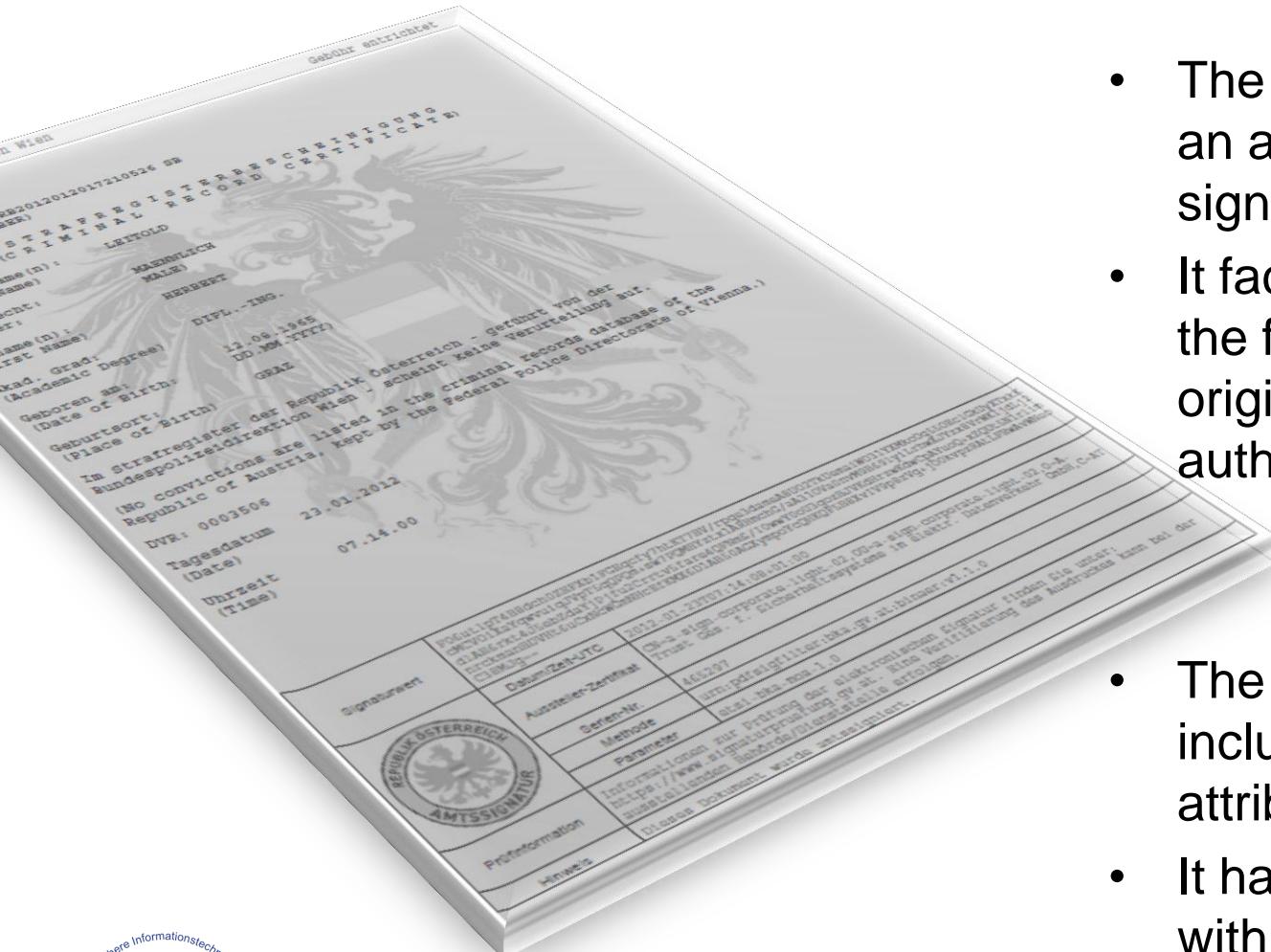
---



# Presentation Overview

- Some Highlights
- Is it used?
- eID - eSig Relation
- Citizen Signature
- Official Signature

# „Official signature“ of documents



- The „Official signature“ is an advanced electronic signature of an authority.
- It facilitates recognition of the fact that a document originates from an authority

- The signature certificate includes a specific attribute - eGov OID
- It has to be visualized with certain elements

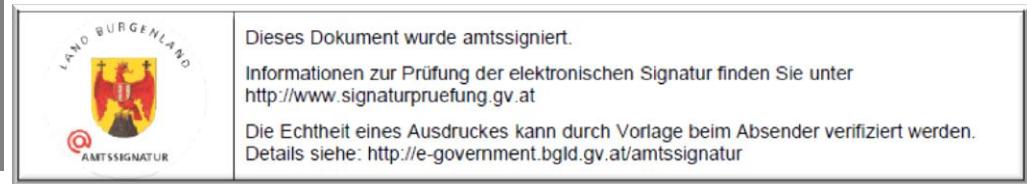
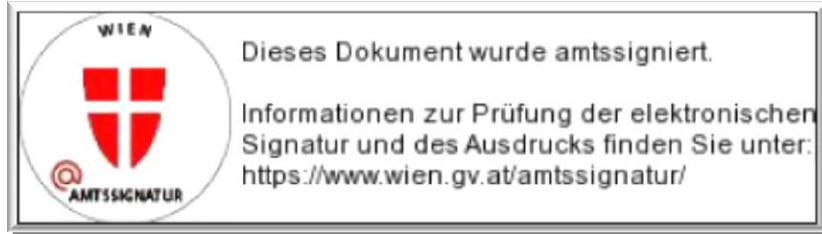
Printouts have **probative value!**

# Different implementations rgd visualization

Signaturwert	LF0bBxaQvybBYuzAFMr0C3LuSBBDnz2knSA22A+6K6M8Ur37KCoG80WSROcQ2hU4uPw97qpUs1nmmWJC8TpMqb9sX8BVsS9m9T1bjQ0jfnPFkhLiWe9gBzjU5CiWjpP//Bq4ZgcaFfdj1ZqskWuSQ1V56G+mZziPyKai7iFfZjx0GeX49V8hVklZk+QJaks0oIJMqEypKjZyAHQ4PuLMch3+YIfytB/u5bfbjYbxrPo6iZaTMVXOHjYPCu9qD6Ifgl6/fZpaDdTZLQaniiYqa6LXX827WzLQ9Q27ZoTaTgld5jbVKt6D1UmpPpOH/LU5QAiC5jiHW72f6G0IWHRHlw==
	Unterzeichner BMI SU-ZMR
	Datum/Zeit-UTC 2010-09-07T14:08:30+02:00
	Aussteller-Zertifikat CN=a-sign-corporate-light-02,OU=a-sign-corporate-light-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr. 450207
	Methode urn:pdfsigfilter:bka.gv.at:text:v1.2.0
	Parameter etsi-bka-moa-1.0
Prüfinformation	Informationen zur Prüfung der elektronischen Signatur finden Sie unter: <a href="http://www.signaturpruefung.gv.at">http://www.signaturpruefung.gv.at</a> . Zur Prüfung des Ausdrucks senden Sie bitte einen Scan an zmr-clearingstelle@bmi.gv.at
Hinweis	Dieses Dokument wurde amtssigniert. Auch ein Ausdruck dieses Dokuments hat gemäß § 20 E-Government-Gesetz die Beweiskraft einer öffentlichen Urkunde.

## Minimum content:

- logo of the authority
- Explicit information that it was “officially signed”
- Information needed for the verification of the electronic signature and the printout



	Datum/Zeit-UTC	2012-05-21T15:19:03+02:00
	Hinweis	Dieses Dokument wurde elektronisch signiert. Auch ein Ausdruck dieses Dokuments hat die Beweiskraft einer öffentlichen Urkunde.
	Prüfinformation	Informationen zur Prüfung der elektronischen Signatur und des Ausdrucks finden Sie unter: <a href="http://kundmachungen.justiz.gv.at/justizsignatur">http://kundmachungen.justiz.gv.at/justizsignatur</a> .

# Example: Criminal record certificate

Bundespolizeidirektion Wien Strafregisteramt		Gebühr entrichtet
Wassergasse 22 1090 Wien		
REDESS: SER2012012017210526 SR (REFERENCE NUMBER)		
S T R A F R E G I S T E R R E C H N I G U N G (C R I M I N A L   R E C O R D   C E R T I F I C A T E)		
Familienname (n):	LITTOOLD	
(Family Name)		
Geschlecht:	MAENNLICH	
(Gender:	MALE)	
Vorname (n):	HERBERT	
(First Name)		
Akad. Grad:	DIPLO.-ING.	
(Academic Degree)		
Geboren am:	12.08.1965 (Date of Birth: DD.MM.YYYY)	
Geburtsort:	GRAZ (Place of Birth)	
Im Strafregister der Republik Österreich - geführt von der Bundespolizeidirektion Wien - scheint keine Verurteilung auf.		
(No convictions are listed in the criminal records database of the Republic of Austria, kept by the Federal Police Directorate of Vienna.)		
DVR:	0003506	
Tagessdatum	23.01.2012	
(Date)		
Uhrzeit	07.14.00	
(Time)		
Signaturent	  	
Datum/Ziel-UTC	2012-01-23T07:14:00+01:00	
Aussteller-Zertifikat	ca-n-wsg-corporate-light-e2.com-a-wsg-corporate-light-e2.ca-a-trust.ee. f. sicherheitssignatur im flakt. unterschreibt mitz...caar...	
Seiten-Nr.	1/2/2012	
Methode	urn:nitfingertip:dko.gv.at:binary.v1.1.e	
Parameter	etzel-dko.msa.v1.0	
Prüfinformation	Informationen zur Prüfung der elektronischen Signatur finden Sie unter: <a href="https://www.signturpruefung.gv.at/">https://www.signturpruefung.gv.at/</a> . Eine Verifizierung des Ausdrucks kann bei der ausstellenden Behörde/Behörde erfolgen.	
Hinweis	Dieses Dokument wurde elektronisch unterschrieben.	

Since 2011 all administrative acts hold an official signature

# Conclusions

---

- Austrian citizen signature infrastructure started with mass-deployments in 2005
- Citizen can activate tokens for free
- Mobile phone signature outperforms smartcards
- Official signature allows for authentic eDocuments of authorities

*Thank you for your attention!*