



Security in e-Government in Austria

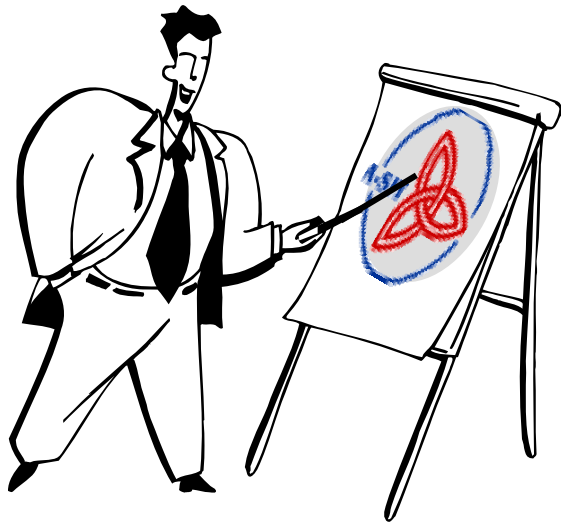


Herbert Leitold

Secure Information Technology
Center - Austria A-SIT



Contents



- Introduction
- Citizen Infrastructure
 - the Client-side
- Server-side
 - Open source security modules for e-Government
- In Action
- Supplementary Tools
- Conclusions



Some eGovernment players

BUNDESKANZLERAMT  ÖSTERREICH

CIO DES BUNDES

Federal Chancellery

Coordination, Chief Information Officer, operational services, tools, etc.



e-Government Innovation Center - EGIZ

Research & competence center



A-SIT

Security advise, electronic signatures, etc.





e-Government Challenges

- Trust & Security
 - Identification and authentication
 - Confidentiality
 - Data protection
- Representation, acting as proxy
- Technology neutrality
 - Long-term investments vs. technology life cycle
- Cross-border challenge
 - To be considered from the beginning
- Openness towards the market





e-Signature in e-Government



*crypto based security
for e-government*

Nachfolgend finden Sie das Ergebnis der Prüfung der eingereichten elektronischen Signatur.

Unterzeichner

Name	Christian Wregar
Organisationseinheit	Verfassungsdienst
Organisation	Bundeskanzleramt der Republik Österreich
Staat	AT

Aussteller des Zertifikats

Name	a-sign-corporate-light-01
Organisationseinheit	a-sign-corporate-light-01
Organisation	A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH
Staat	AT

Informationen zum Zertifikat

Seriennummer	21221
Qualität	gewöhnliches Zertifikat

Prüfungen

Signatur	Die Überprüfung der Hash-Werte und des Werts der Signatur konnte erfolgreich durchgeführt werden.
Zertifikat	Eine formal korrekte Zertifikatskette vom Signatorzertifikat zu einem vertrauenswürdigen Wurzelzertifikat konnte konstruiert werden. Jedes Zertifikat dieser Kette ist nun in der

- legal acts need electronic signature to get in force
- XML-document structure for securing adequate format
- online verification offered
- same methods as for e-government application





Citizen Infrastructure



- Smart card initiatives
- IDM concept - data protection
- Cross-border IDM





Major rollouts



Bank cards (ATM cards)

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



Health insurance cards:

Rollout Mai-Nov. 2005, ~70.000 cards/day
so far ~ 6 Mio. cards, 100 % coverage (8 Mio.) end of Nov.



Mobile phones:

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



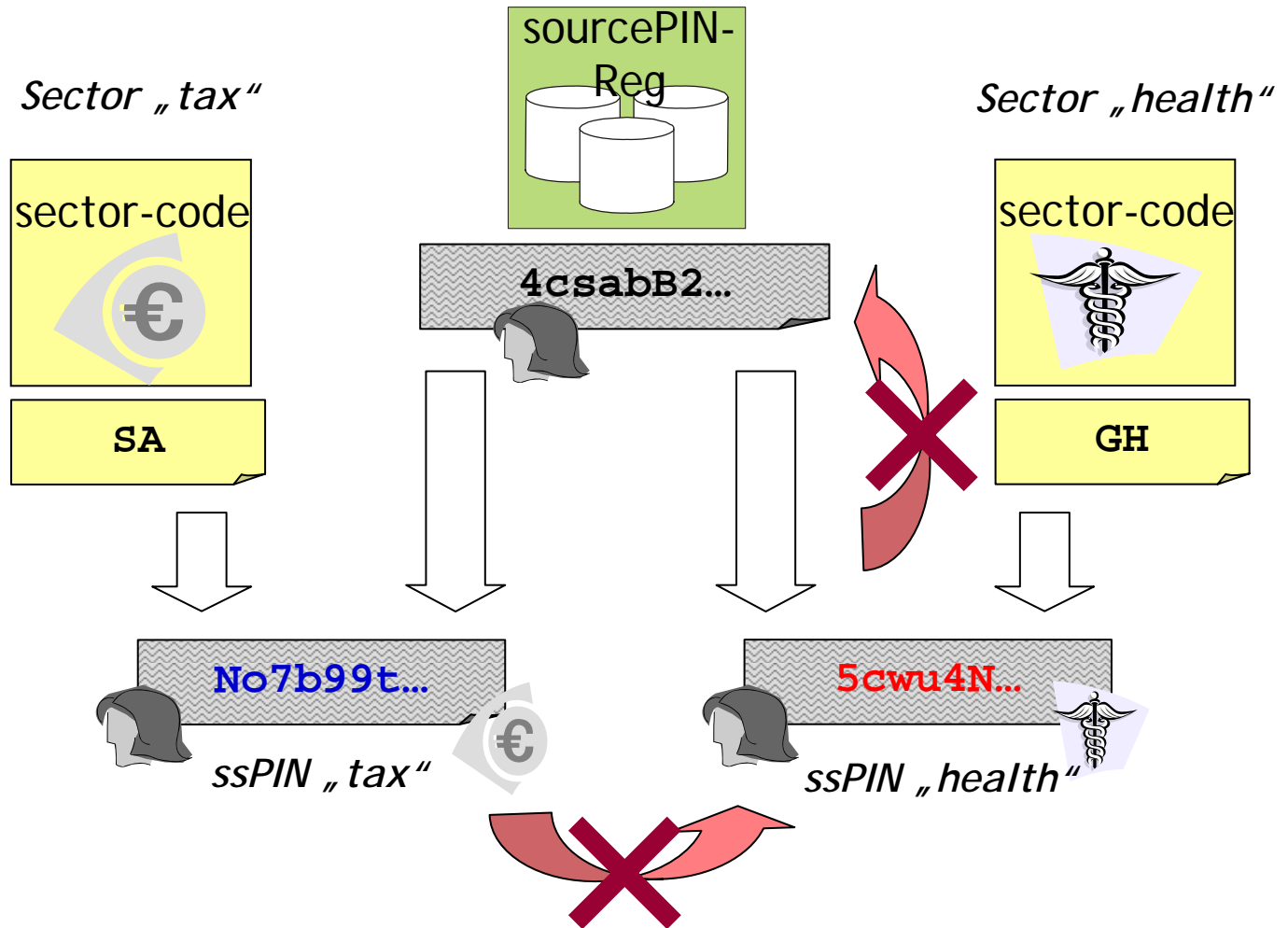
Further initiatives:

- CSP signature cards
- Student service cards, etc.





Sector-specific IDM concept





Cross-border integration

- Integration of foreign eID
 - Belgian, Estonian, Italian eID currently being integrated
- Uses "Supplementary Register"
 - Recurring identity concept





Server Side



- MOA - Module for On-line Applications
 - Basic modules
 - Open source
- Example "Official Signature"





The MOA species

- MOA-ID/ID+, MOA-wID: Identification
- MOA-SS: Server Signature
 - Official Signature
- MOA-SP: Signature Verification
- MOA-ZS: Electronic Delivery
 - substitute registered letter
- MOA-VV: Representation
- further to come ...





Official signature

Meldebestätigung - Microsoft Internet Explorer

Adresse: C:\users\hleitold\privat\Meldebest\meldebestaetigung.html

BMI SU-ZMR
Hahngasse 8
1090 Wien

MELDEBESTÄTIGUNG
aus dem Zentralen Melderegister

PERSONENDATEN

Titel:	Dipl.-Ing.
Familienname:	Leitold
Vorname:	Herbert
Geschlecht:	Männlich
Geburtsdatum:	12.08.1965
Geburtsort:	Unbekannt
Staatsangehörigkeit:	Österreich

Im Zentralen Melderegister scheinen folgende Meldedaten auf:

Wohnsitzqualität:	Haar
Strasse:	St. Ulrichsplatz
PLZ/Ort:	1040 Wien, Bez.:Innere Stadt
Ortsgemeinde:	1040 Wien
gemeldet seit:	12.08.1965

	Signiert von	BMI SU-ZMR
	Datum	2005-09-04T11:30:38
	Zertifikat	A-Trust Ges. f. Sicherheitstechnik im elektr. Datenverkehr GmbH, a-sign-corporate-light-02, AT (80524)
	Verfahren	urn:publicid:bmi.gv.at:meldebest+m-1.2
Signaturwert	QMTAo0s5c/£ZK/txebJvcUnGaxBG...GSSee1iP3822awt8+HSI9ra5fdK0 gQG9KYRpHfWnFpbjQSVhCHrM6C/...F+Euzr36036IG1Mu0u1E0QJ3LLOPY HLcEbBD0jppW0970gw/A8eQOY...CE7FRC09do=	

Weitere Hinweise zu dieser elektronischen Meldebestätigung finden Sie unter https://meldung.cio.gv.at/info/mb_info.html,
Hinweise zur Signatur unter http://meldung.cio.gv.at/info/mb_sig.html

Tagesdatum: 04.09.2005
Uhrzeit: 13:29:56

Fertig Arbeitsplatz

Electronic certificate of enrollment





Media independence

- Probative value maintained on print outs
 - reconstruction of XML document possible from the paper copy

	Signiert von	BMI SU-ZMR
	Datum	2005-09-04T11:30:38
	Zertifikat	A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH, a-sign-corporate-light-02, AT (80524)
	Verfahren	urn:publicid:bmi.gv.at:ZP+bescheid+mb-1.2
Signaturwert	QMTAo0s5c/fZK/txebJvcUnGAXBGChAeFpxuzGSseliP3822awt8+HSI9ra...dKO dQG9KYRpHfWnFpbjqSvHCHRm6C/QnwZex2MF+Euzr36036IG1MuOu1E0QJ31L... HLcEbBD0jppW0970gw/A8e00XVPO/hsHgtE7FRC09do=	





In Action



- My “register of convictions certificate” (clearance cert.) step by step
 - as e.g. frequently needed in public procurement





Step 1: Fill in a form, ...

Ausstellung einer Strafregisterbescheinigung - Microsoft Internet Explorer

Adresse https://labs.cio.gv.at/egov/cgi-bin/formular.pl?generate=1&Eingabe_An_ID=polizei%2Fstrafregister&FormData_VN=strafregister&FormData_CitizenCardURL=http%3A%2F% Wechseln zu Links

SICHERHEIT&HILFE
Ihre Wiener
POLIZEI

Info beachten Sie: * Feld muss ausgefüllt sein
! Hinweis auf Fehler

Information und Hilfe zum Ausfüllen
Zutreffendes ankreuzen oder auswählen

Ausstellung einer Strafregisterbescheinigung - Schritt 1: Formular ausfüllen

Absender/in

E-Mail-Adresse: [für Empfangsbestätigung] *

Zur Anfrage im Register benötigte Personenmerkmale

Geschlecht * weiblich männlich

Frühere Familiennamen

Geburtsort *

Vorname des Vaters *

Vorname der Mutter *

Auswahl der Zustelladresse (Hauptwohnsitz gemäß ZMR ODER andere Adresse)

Zustelladresse * Hauptwohnsitz Andere Adresse

Falls Zustellung an andere Adresse gewünscht

Strasse *

Hausnummer * Stiege Tür

Postleitzahl * A-

Fertig

Internet





Step 2: control it, ...

Ausstellung einer Strafregisterbescheinigung - Microsoft Internet Explorer

Adresse: http://127.0.0.1:3495/http-security-layer-request

SICHERHEIT&HILFE
Ihre Wiener
POLIZEI

Info beachten Sie: * Feld muss ausgefüllt sein
! Hinweis auf Fehler

Information und Hilfe zum Ausfüllen
Zutreffendes ankreuzen oder auswählen

Ausstellung einer Strafregisterbescheinigung - Schritt 2: Antrag signieren

Absender/in

Vorname	Herbert
Familienname	Leitold
Geburtsdatum	1965-08-12
E-Mail-Adresse: [für Empfangsbestätigung]	Herbert.Leitold@iaik.tugraz.at

Zur Anfrage im Register benötigte Personenmerkmale

Geschlecht	männlich
Frühere Familiennamen	
Geburtsort	Graz
Vorname des Vaters	Wilhelm
Vorname der Mutter	Theresia

Zustellung erfolgt an folgende Adresse

Zustelladresse	Hauptwohnsitz gemäß ZMR
----------------	-------------------------

Art der Zustellung

	mittels	Normalbrief
--	---------	-------------

Antrag signieren

Fertig

Internet

„Intelligent form“: Data Taken from identity-link in the Citizen Card

Needed by the process (entered by citizen in step 1)

Data (home address) know to administration. Consent to use given in step 1

Proceed with signature





Step 3: sign it, ...

The screenshot shows a Microsoft Internet Explorer window titled 'Ausstellung einer Strafregisterbescheinigung'. The address bar shows 'http://127.0.0.1:3495/http-security-...'. The main content area displays a form with the following sections:

- Info beachten Sie:** A red box with the word 'Info' and the text 'beachten Sie:'.
- Ausstellung einer Strafregisterbescheinigung**
- Absender/in**

Vorname	Herbert
Familienname	Leitold
Geburtsdatum	1965-08-12
E-Mail für Empfangsbestätigung	Herbert.Leitold@iaik.tugraz.at
- Zur Anfrage im Register benötigte Personenmerkmale**

Geschlecht	männlich
Frühere Familiennamen	
Geburtsort	Graz
Vorname des Vaters	Wilhelm
Vorname der Mutter	Theresia
- Ergeht an**

Adressat	BPD Wien - Strafregisteramt
----------	-----------------------------
- Zustellung erfolgt an folgende Adresse**

Zustelladresse	Hauptwohnsitz gemäß ZMR
----------------	-------------------------
- Art der Zustellung**

	mittels	Normalbrief
--	---------	-------------

The 'trustview 2.1.1' overlay window is positioned over the right side of the browser window, displaying the same form content. At the bottom of the browser window, there are buttons for 'Applikation beenden', 'Signatur Zertifikat', and 'Unterschreiben'. The status bar at the bottom shows 'Fertig' and 'Internet'.





Step 4: pay it, ...

Ausstellung einer Strafregisterbescheinigung - Microsoft Internet Explorer

Adresse: <http://127.0.0.1:3495>

QGOV - Auswahl des Zahlungsmittels - QENTA paymentsolutions - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

Info beachten Sie:

Ausstellung einer Strafre

Für die Ausstellung einer Strafregisterbescheinigung gemäß § 10 Gebührengesetz für Anträge,

Zu Ihrem Antrag liegen uns folgende Daten vor:

Empfänger:	BPDWV Strafregisteramt
Betrag:	15.10 EUR
Datum:	2005-09-23
Ref.Nr.:	8888
Rem.ID:	SRB20050923130024
Order Nr.:	10872258

Wählen Sie Ihr gewünschtes Zahlungsmittel:

- Kreditkarte
- eps Online-Überweisung

Bitte wählen Sie Ihre Bank.

Abbrechen

powered by **QENTA**

Done www.qenta.com 13,48

Fertig Internet

Payment backed with e-Signatures





Step 5: receive confirmation, ...

Empfangsbestätigung: GZ: SRB200509231 211 39 - Nachricht (HTML)

Sie haben diese Nachricht am 23.09.2005 12:20 weitergeleitet.

Von: srb@labs.cio.gv.at
An: Herbert.Leitold@iaik.tugraz.at
Cc:
Betreff: Empfangsbestätigung: GZ: SRB20050923121139
Anlagen: [Antrag.xml \(11 KB\)](#)

Gesendet: Fr 23.09.2005 12:16

SICHERHEIT&HILFE
Ihre Wiener
POLIZEI

Ausstellung einer Strafregisterbescheinigung - Endansicht

Absender/in

Titel [aus Zertifikat entnommen]	DI
Vorname	Herbert
Familiennamen	Leitold
Geburtsdatum	1965-08-12
E-Mail-Adresse: [für Empfangsbestätigung]	Herbert.Leitold@iaik.tugraz.at

Zur Anfrage im Register benötigte Personenmerkmale

Geschlecht	männlich
Frühere Familiennamen	
Geburtsort	Graz
Vorname des Vaters	Wilhelm
Vorname der Mutter	Theresia

Zustellung erfolgt an folgende Adresse

Zustelladresse	Hauptwohnsitz gemäß ZMR
----------------	-------------------------

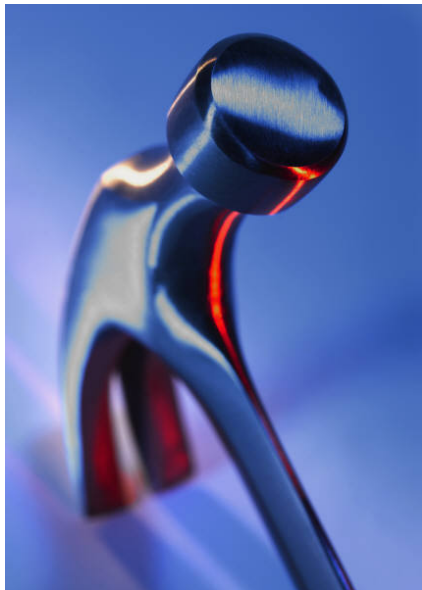
Art der Zustellung

mittels	Normalbrief
---------	-------------





Supplementary Tools



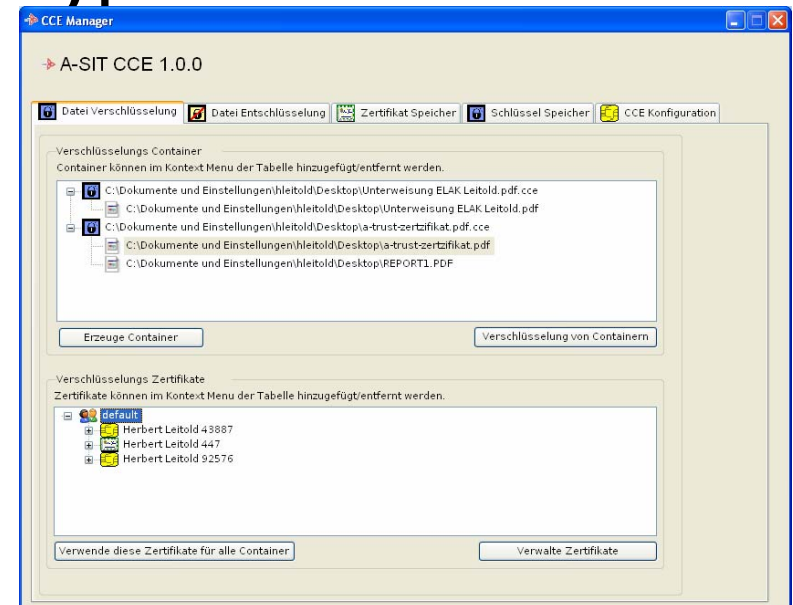
- e-Security for the citizen's PC
 - using the citizen card
 - freely available





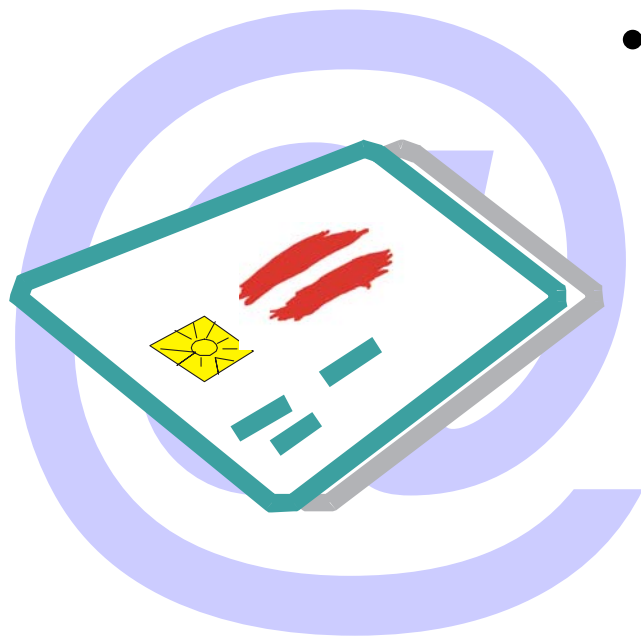
Tools

- Secure EFS
 - Use the citizen card to secure the Encrypting File System Key
- CCE - Citizen Card Encrypted
 - File encryption
 - e.g. used for classified data





Conclusions



- Core concepts are
 - Citizen Card
 - Open-Source MOAs
 - Technology neutrality
 - Openness for private sector





Thank you for your attention



Secure Information Technology
Center - Austria

Herbert.Leitold@a-sit. at

<http://www.a-sit.at>