Austrian experience of using electronic identity and signature

Prof. Dr. Reinhard Posch
CIO Federal Government Austria
the journey to uncertainty

from voice to increasingly text

from one to one to one to many

from contracted services to open communications
computation is under a change

where are my data

who wrote my programs

standards – silos – containers

full integration cyber and physical

who is responsible for security integrity and confidentiality
data storage is under a change

where are my data

whom do I need to trust

where is the data location physical / jurisdiction

who manages / owns / applies keys

does the concept allow privacy - control?
The basis of all interoperability is cooperation.
legal background and recommendations

- Datenschutzgesetz
- Signaturgesetz
- E-GovG
- AVG
- ZustG
- secondary legislation
- specifications & recommendations
we are living in a dynamic world

EU-level cooperation

Federal Government

CIO

spokesperson

synergy and cooperation
towns, länder,
communities, private sector

Change of benchmark

DIGITAL: AUSTRIA
communicating interoperability – the big picture

Common eGovernment building blocks as a basis

• essential component of Austria’s national eGovernment strategy
• common solutions for data exchange, identity management, authorization, etc.
• field-tested and open source modules (via joinup.eu)
eGovernment building blocks in Austria

- E-Government law
- Online processes
- Methods and processes in administration
- Standards
- Policies: E-Mail, security, inclusiveness
- Electronic payment
- Identity management („bPK-concept“)
- Privacy by design
- Portals-concept (PVP)
- Electronic delivery
- Electronic signature
- Modules for online processes

„Handy-Signatur“ / citizen card
the goal: seamless processes

e.g. HELP.gv.at, USP.gv.at, Wien.gv.at etc.

e.g. ELAK, register (ZMR, GWR, mandate register, address register), Finanz Online, other dedicated applications etc.

www.bka.gv.at/zustelldienste
the core: E-GovG

eGovernment law

- "citizen card"
- persona-binding
- acting on behalf
- source PIN
- derived PIN
- source PIN-register
- extension-register
- standard-dokuments-register
- register-query
- official-signature
grasping the role of CLOUD

- the future
- the challenge

STORAGE
DOCUMENT COLLABORATION
WEB SERVICES

HOW TO ACCESS
HOW TO SIGN
HOW TO ENCRYPT

SECURITY PROVIDER

Tablet
Mobile
Laptop
PC ...

USER
the great challenge: documents and collaboration

THERE HAS BEEN A SUBSTANTIAL CHANGE OVER THE LAST YEARS

CONTINUITY?

LOCK IN?

STANDARDS?

IMPACT ON OTHER SYSTEMS?

ALTERNATIVES?
understanding CLOUD : understanding RISK
Open Government Data: politics / administration / open public

SOURCE data.wien.gv.at
CRYPTO and the CLOUD

KEEPING USABILITY AND CONVENIENCE

OBSERVING NATIONAL INTERSTS

MANAGING THE COMPLEXITY

RESEARCH TO CLOSE THE OPEN ISSUES

KEEPING CONTROL OF COST AND EFFICIENCY

CRYPTO UNDER NATIONAL CONTROL

DATA PROTECTION AND SECURITY MIGHT ALLOW EUROPE TO APPROACH COMPETITIVENESS IN CLOUD COMPUTING.
data.gv.at wins the United Nations Public Service Award 2014

- category: „Improving the delivery of public services”
- Jury: „data.gv.at has been the consequent improvement of public-sector services, the excelling performance in the area Open Government Data, inspiration and model for many other countries.”
Interconnected base registers

- based on common Austrian eGovernment building blocks
- operated by different public bodies
- holding (person-related) data from different administrative sectors
- data exchange based on common interfaces and specifications
  - security and data protection 'by design' (data exchange powered by sector-specific identifiers (ssPIN))
- authentication & authorization at the back-office interaction powered by federation of portals-concept (PVP)
the Austrian eID
the who is who of Austrian eID

BMF, BMG, BMLFUW, BMJ, HV, BKA

A-Trust

financed by:
BMF, BMG, BMLFUW, BMJ, HV, BKA

base registers
BMI, Statistik, BKA

eID &
electronic signature
TOKENS

service provider

A-Trust

registration outlets
BMF – finance offices
HV – social security communities
BKA, BMI, banks
…..

applications
administration
private sector

services

MOA und Innovation
EGIZ

private sector
electronic - identity = CSP* + public register

eID, electronic identity

* CSP = Certificate Service Provider
identity management – the aim

- unique identifiers based on core registers
- conformance with data protection - privacy friendly: Sector specific derivations (bPK) in electronic services/ applications
- reliable, high quality information
bPK: Generation

Conversion impossible!

if person-related data (lawfully) is transmitted across sectors, encrypted bPKs have to be used thus avoiding the easy creation of comprehensive citizen profiles
identity management – "provisioning"
identity management – “access”
eID function

- administrative applications
- private sector applications

MOA-(W)ID application

- unique identification of citizen (persona binding)
- Authenticated by verifying the qualified signature

bPK (derived PIN)

Security Layer

Antrag

Persona binding certificate

Source PIN

"citizen card"
persona binding

- XML structure in Chip or HSM:
  - name and date of birth
  - unique identifier “source PIN”
  - public key
- Signed by StZRegBeh

```xml
...<saml:SubjectConfirmationData>
  <pr:Person xsi:type="pr:Physical"
    <pr:Identification>
    <pr:Value>123456789012</pr:Value>
    <pr:Type>http://reference.e-g</pr:Type>
  </pr:Identification>
  <pr:Name>
    <pr:GivenName>Peter</pr:GivenName>
    <pr:FamilyName>Kustor</pr:FamilyName>
  </pr:Name>
...
...<saml:Attribute
  AttributeName="CitizenPublicKey"
  <dsig:RSAKeyValue>
    <dsig:Modulus>snW80LCQ49qNefems</dsig:Modulus>
...
the flavors of the Austrian „citizen card“

- social insurance card (eCard)
- service cards
- student cards
- mobile
Handy-Signatur

- since 4Q09 qualified signatures via mobile phone

- technology:
  - server side calculation (HSM)
  - sole control via two factor mobile phone and code

- usage:
  - alternative to card based eID
  - no cost for smartcard and reader
  - enhanced usability no installation

- 2016:
  - over 1 mio eIDs
  - over 700K Handy-Signature
  - number of eIDs exceeds number of identity cards
**using eID : Handy-Signatur**

1. **Schritt:**
   - Die Signaturanfrage wird gestartet.
   - Geben Sie ihre Handy-Nummer und ihr Signatur-password.

2. **Schritt mit QR-Code wählen:**
   - »speed-sign«: Erfassen Sie den QR-Code am Bildschirm mit Ihrer Kamera am Mobiltelefon – und fertig.

3. **Schritt**
   - Geben Sie die TAN ein
   - Klicken Sie »Signieren« an und fertig.

**Hinweis:** Durch Klick auf »Signaturdaten« im Browserfenster bzw. »Dokumente anzeigen« in der App können Sie die Daten, die Sie unterschreiben, nochmals kontrollieren.
Handy-Signatur > 200 applications...

HELP – Online-Formulare - www.help.gv.at
FinanzOnline - www.finanzonline.at

Meldebestätigung/Meldeauskunft - https://www.help.gv.at/meldebestaetigung
Strafregisterbescheinigung - https://www.help.gv.at/strafregisterbescheinigung
Online-Services Sozialversicherung - www.sozialversicherung.at
Pensionskonto - www.neuespensionskonto.at
Transparenzportal - www.transparenzportal.gv.at
Unternehmensserviceportal - www.usp.gv.at
Studienbeihilfe - https://www.help.gv.at/studienbeihilfe

Petitionen - www.petitionen.wien.gv.at
e. Wahl- und Stimmkartenbestellung
Demokratiepaket (Volksbegehren, Bürgerinitiativen)

Elektronische Zustellung - www.zustellung.gv.at
BriefButler - www.briefbutler.at
Post Manager - www.postmanager.at
Handy-Signatur in administration
some examples
HELP.gv.at – the figures

HELP.gv.at - 2015: (www.help.gv.at)

- 17,034,708 sessions
- 47,893,816 page views
- app. 491 24/7 counters

<table>
<thead>
<tr>
<th>Rang</th>
<th>Lebenslagen</th>
<th>Page Impressions 2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Geburt eines Kindes</td>
<td>2,616,602</td>
</tr>
<tr>
<td>2</td>
<td>Kfz</td>
<td>1,325,630</td>
</tr>
<tr>
<td>3</td>
<td>Erben</td>
<td>1,322,535</td>
</tr>
<tr>
<td>4</td>
<td>Führerschein</td>
<td>1,111,766</td>
</tr>
<tr>
<td>5</td>
<td>Pension</td>
<td>887,253</td>
</tr>
</tbody>
</table>
USP.gv.at - the figures

USP.gv.at - 2015:
(www.usp.gv.at)

- 2.480.629 sessions
- 7.969.099 pageviews

<table>
<thead>
<tr>
<th>USP.gv.at</th>
<th>Page Impressions 2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Umsatzsteuer</td>
<td>192.625</td>
</tr>
<tr>
<td>Firmenbuch</td>
<td>105.281</td>
</tr>
<tr>
<td>Gewerbe</td>
<td>102.738</td>
</tr>
<tr>
<td>Online Verfahren</td>
<td>95.452</td>
</tr>
<tr>
<td>Betriebeinnahmen und -ausgaben</td>
<td>80.398</td>
</tr>
</tbody>
</table>
FinanzOnline:
(https://finanzonline.bmf.gv.at/fon/)

- ~ 2,500,000 users
- ~10,000,000 online-applications (e.g. tax declarations) per year
social insurance Austria:
(www.sozialversicherung.at)

- servicing patients, contractors, employers and pharmaceutical companies
- wide selection of processes (pension application, etc.)
- online information about consumed services for insured people
- pension account (insured time, contributed amount, status, etc.)
- Account for fees for recipes
- personal insurance data
proof of residency
residence deregistration
extract of the criminal record
Handy-Signatur „enabling“ the private sector – some examples
online contract cancellation service

- legally effective cancellation of contracts and subscriptions (journals, pone contracts, etc.)
- status 04/2016: choice of 2589 recipients

online contract cancellation:
(www.online-kuendigen.at)
CLOUD services

- winner "best cloud" 2012
- Handy-Signatur for secure login

[http://www.foliocloud.com]
...key to secure and trustworthy services (e.g. Postmanager.at)

- client base: 2.3 mio households
- 27% of identity processes via Handy-Signatur
...basis for seamless electronic processes at low cost

**electronic delivery:**
- highest security & comfort, access to delivered documents from anywhere (no paper formalities for proof of delivered)
- all delivery to a single box
- valid for any quality of delivery
- unavailability (e.g. vacation) can be specified
- speeding up processes
...the key to secure, trustworthy
Austrian eID goes Europe
SMS > QR advancing security & usability
THANK YOU FOR LISTENING

REINHARD.POSCH@CIO.GV.AT