Austrian Experience with Mobile ID vs. Smartcard ID

Herbert.Leitold@a-sit.at

ISSE 2016
Session “Mobile Security”
Paris, November 15th, 2016
Contents

• Austrian eID Programme
• Austrian Mobile Signature
• Usage and Business Model
• Lessons Learned
Austrian Citizen Card - an Overview

• Launched 2003, mass-rollouts from 2005
• Defines functions, not the technology
  – Identification, sector-specific to enhance privacy
  – Qualified signatures, for written form
  – Electronic mandates, representation
• Technology-neutral approach allowed for different implementations
  – Smartcards and mobile from 2005
  – Foreign eID recognised from 2008
The technologies

**Smartcard**
- Bank cards
  - from 2005; ceased
- Health insurance card
  - since 2005
- Profession cards, service cards, ...
  - e.g. notaries, lawyers, ministries, ...

**Mobile**
- A1 signature
  - service by a MNO
    - from 2005; ceased in 2008
    - limited success
- Mobile phone signature
  - Launched end 2009 through the LSP STORK
  - Contracted by gvmnt. to a private sector CSP
  - Success? Well, let’s see ...
Austria: Card vs mobile ID active users


Health card, ~1 k eID activations/month

MobileID ~1k new users per workday
Austrian eID – key characteristics

• Gvnmt. identity base (Population Register), but
  – open to public and private sector credential providers
  – open to public and private sector relying parties
  – LoA “high” (eIDAS definition, not yet notified)

• Voluntary system
  – Citizen may activate credentials is has (health insurance card, (bank cards), mobile phone, CA’s smart cards)

• Free of charge for
  – relying parties (both private sector and public sector)
  – citizens (health insurance card or mobile phone)
Some 300+ applications

https://www.buergerkarte.at/en/applications-mobile.html
Contents

• Austrian eID Programme
• Austrian Mobile Signature
• Usage and Business Model
• Lessons Learned
The Basics

- Follows a server-based approach
  - Crypto-keys kept at a central server (HSM)
    - No changes in mobile phone or SIM
  - 2-factor authent. (knowledge and possession)
- Qualified Signature-Creation Device (QSCD)
  - Confirmed by notified body (Signature-Directive / eIDAS)
- Service operated by a trust service provider for qualified certificates
The Architecture

Mobile Phone Signature Domain

Mobile Phone

User Domain

Database

HSM

SMS Gateway

User

Mobile Phone

Web-based user interface

SMS-based or APP-based 2nd factor

Storage of private signature keys. Signature keys are stored encrypted under:
- Phone number
- Password
- HSM key

Key generation during activation
- Decryption of signature keys
- Signature Creation

Slide 10
The Operation: a) SMS  b) QR code

Mobile Phone Signature Domain
- Database
- Encrypted signature key

User Domain
- User
- Mobile Phone

Web Frontend
- SMS Gateway
- HSM
- SMS Gateway
- Database

a) TAN (SMS)
- Phone number
- Password
- TAN

b) QR-Code
- b) QR-Code
- a) TAN (SMS)
Demo: Business Service Portal

Über das Unternehmensserviceportal – USP
Das Unternehmensserviceportal (USP) ist das zentrale Internetportal der österreichischen Bundesregierung für Unternehmen und bietet direkten Zugang zu zahlreichen E-Government-Anwendungen sowie unternehmensrelevante Informationen.

News / Newsletter
BMF: Stärkung des österreichischen Wohnbaus
Produzierender Bereich mit leichem Umsatzrückgang
Personal Austria 2016

Aktuelles Thema: Mitarbeit von Familienangehörigen
Das Unternehmensserviceportal informiert über die "Mitarbeit von Familienangehörigen".
Demo: Select Card or Mobile ID
Demo: Mobile ID dialogue

From here 2 variants:
- a) SMS one-time-code
- b) QR code app for smartphones
Demo: Variant „a“ - SMS-OTC
Demo: Variant „b“ - QR Code App
Demo: Representation information

Unternehmen auswählen
Bitte wählen Sie das Unternehmen aus, für das Sie jetzt tätig werden wollen.

- Stiftung Secure Information and Communication Technologies - SIC
  8010 Graz
  Teilnehmer: 14217269-007
  Benutzer: hiertold1

- Letold Herbert DI
  8010 Graz
  Teilnehmer: 211904b45256
  Benutzer: bk0501idy

OK Abbrechen

USP Service Center
- Antworten auf häufige Fragen
- Kontakt
Demo: Done

Herbert Leitold, Stiftung Secure Information and Communication Technologies - SIC

Contents

- Austrian eID Programme
- Austrian Mobile Signature
- Usage and Business Model
- Lessons Learned
Mobile ID initial design considerations

• Easy to use, no additional effort for citizens
  – E.g., no change of SIMs
• Independent from mobile device and MNO
  – Server-based credentials, Web-based approach
• Gvmnt. has interest in broad take-up
  – Free of charge for citizens
    • as it is the case for health card eID
  – No costs for public or private relying parties
    • qualified certificates and SMS costs paid by gvnmt.
Deployment (through STORK LSP)

- Signed contract with A-Trust
- Launch of pilot
- Certification by notified Austrian body A-SIT
- AT initial planning
- Start of productive operation
Actual usage …

- About 15-25 k/day uses on a typical working day
- ~4-6 k/day uses on weekends
... actual usage (cntd.)
Zooming into SMS vs. Smartphone App

Monthly Use of Austrian Mobile ID

SMS-OTP vs. AppQR/OTP

Core promotional milestones

Integration into Tax Online and press release

Promotion campaigns, e.g. letters by social insurance to all citizens
Contents

- Austrian eID Programme
- Austrian Mobile Signature
- Usage and Business Model
- Lessons Learned
Lessons learned on smartcard eID

- It needs a card reader
- It needs integration with (all!) OS
- It lacks integration with (all!) browsers
- It needs software on the PC / tablet

- Java-applets helped out, but are gone
Lessons learned

• Smartcard eID
  – Satisfactory business users take-up
  – But quite limited take-up by citizens

• Mobile signat. clear preference by citizens
  – 2014/15/16: 15/10/24 times higher mobile ID activation to health card activation
  • Under comparable conditions like free of charge

• **Ease of use and easy activation** essential
Joice of convenient registration is essential

Activation Channels 2016 YTD

- "Classical" direct F2F
- Alternative methods (prior F2F, bankident, el. delivery, etc.)
Thank You for Listening!

Herbert Leitold
ISSE 2016
Session “Mobile Security”
Paris, November 15th, 2016