Austrian mobile ID

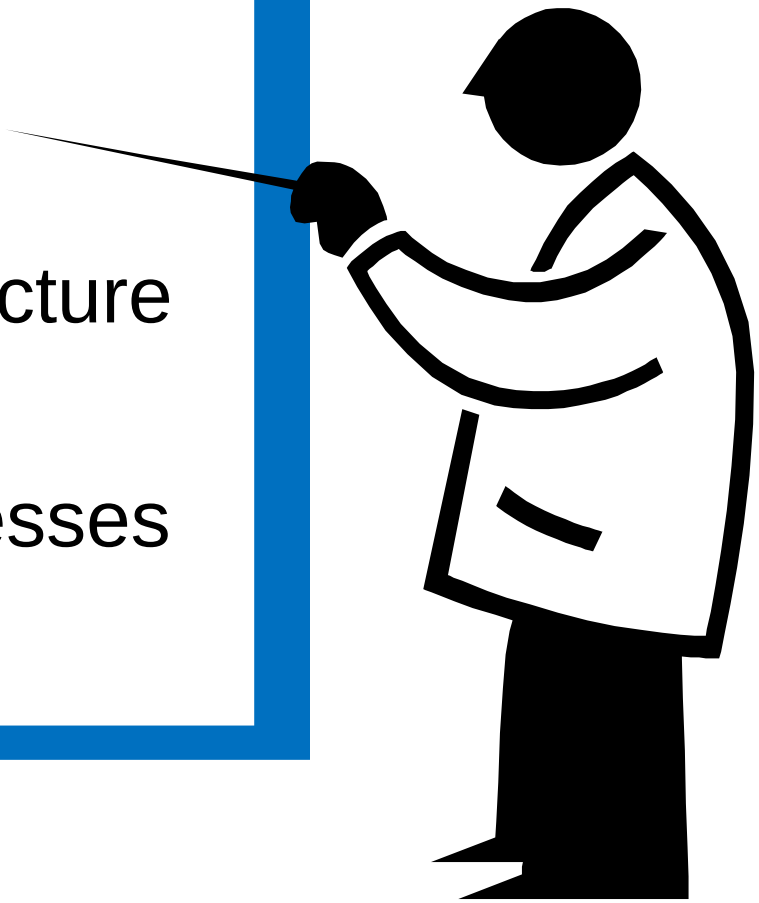
Herbert Leitold

ITU Expert Group Meeting on mID

18-19 October 2016, Warsaw

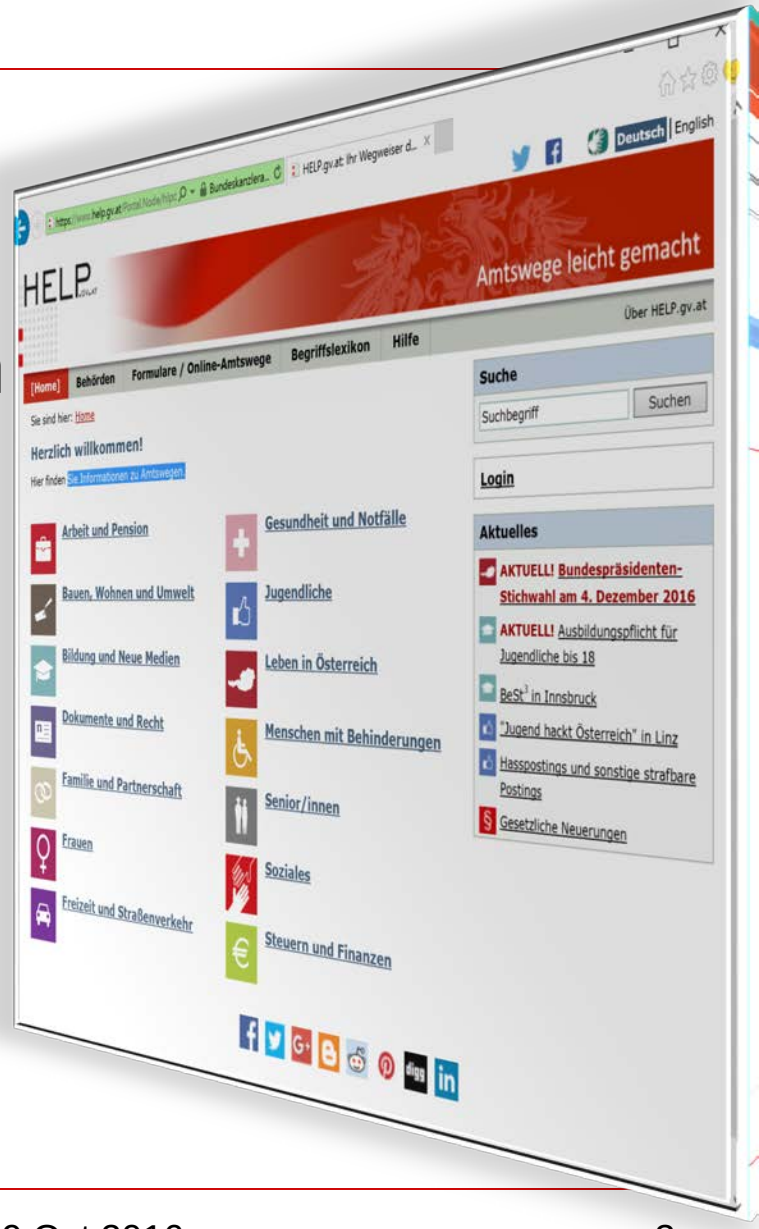
Contents

1. Introduction
2. Business Model
3. IT & Technical Architecture
4. Security an Privacy
5. Use Cases and Processes
6. Awareness Raising



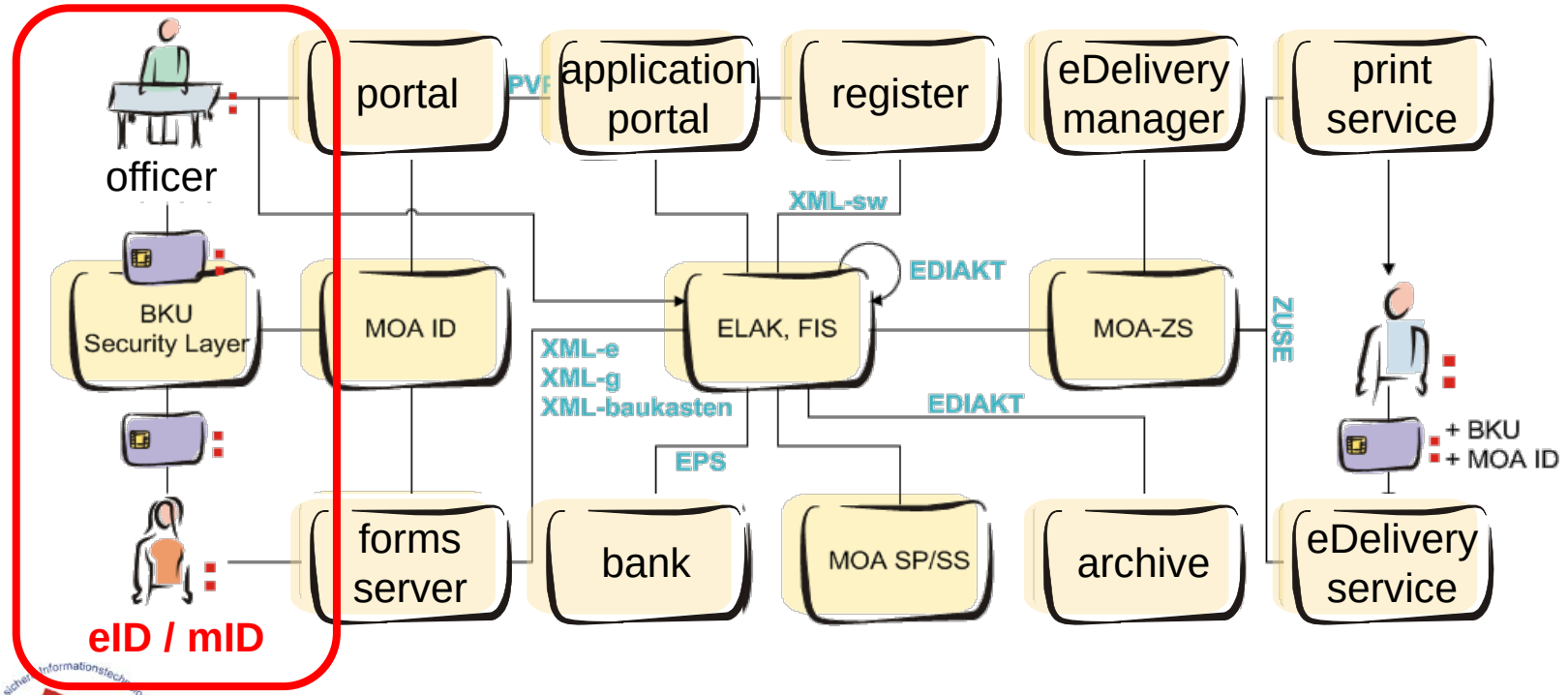
eGovernment Portals

- General federal portals
  - help.gv – citizen information
  - Business Service Portal
- Sectorial portals
  - FinanzOnline – tax portal
  - Social Security Portal
  - Health Portal
- Regional and local portals



Portal Big Picture – Building Blocks

- Common architecture supported through Open Source Building Blocks



eID Timeline

- November 2000: Austrian Cabinet Council decision
  - … to employ chip-card technology to improve citizen's access to public services; to supplement the planned health insurance card with electronic signatures
- February 2003: 1st Citizen Card
  - Austrian Computer Society membership card
- March 2004: E-Government Act
  - Legal basis of the Identity Management System
- 2005 - now
  - Several private-sector and public-sector borne Citizen Card initiatives
  - 2005 both **card ID** and **mobile ID** started

Legal Framework Overview

- E-Government Act an bylaws
  (issued 2004, major amendments 2008, 2010, 2016)
  - Electronic Identity
    - Public Sector use and Private Sector Use
  - Base Registers
  - Official Signatures
    - All official notifications electronically signed (even if delivered on paper)
  - Electronic Delivery *(in Delivery Act)*

Austrian eID technologies & history

Smartcard

Bank cards
from 2005; ceased

Health insurance card
since 2005

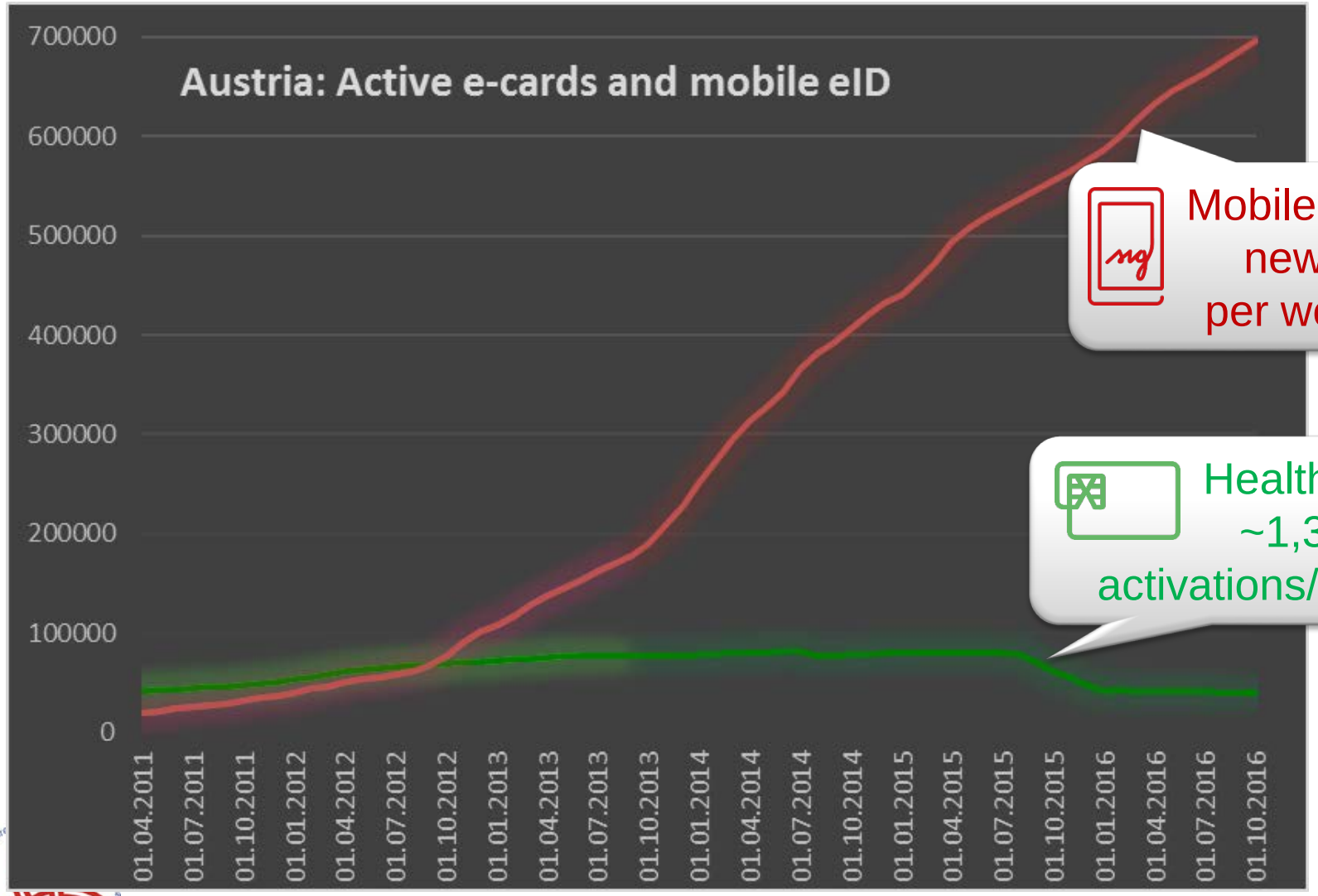
Profession cards, service cards, …
e.g. notaries, lawyers, ministries, …

Mobile

A1 signature
service by a MNO
from 2005; ceased in 2008
limited success

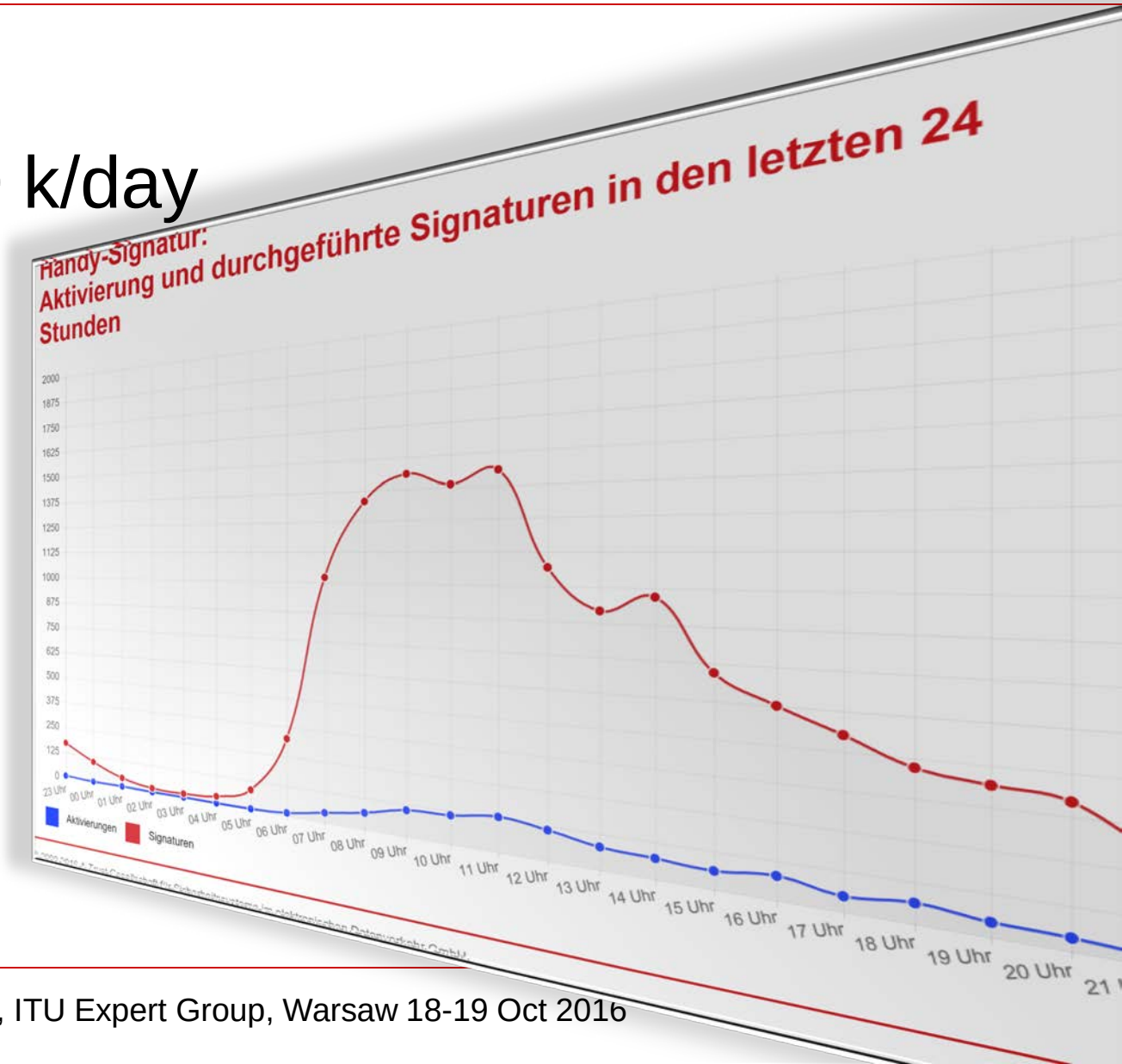
Mobile phone signature
Launched end 2009 through the LSP STORK
Contracted by gvmnt. to a private sector CSP
Success? Well, let's see ...

Austria: Card vs mobile ID active users



Austria: Actual usage … (mobile only)

- About 15-20 k/day uses on a typical working day
- ~4-6 k/day uses on weekends

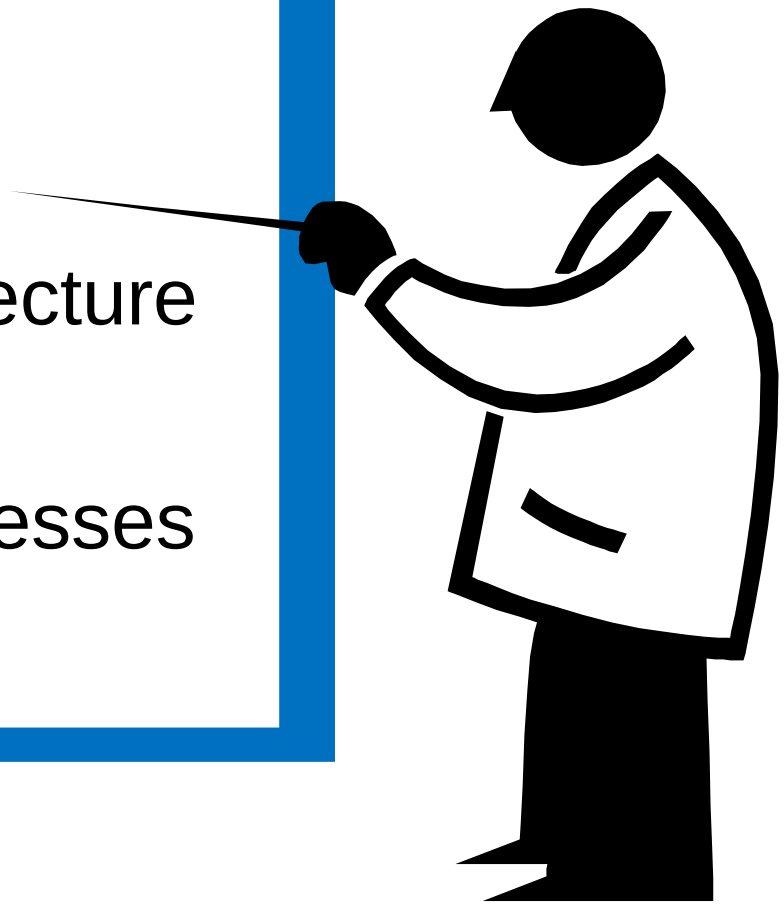


Austrian mobile ID Key Success Factors

- Zero footprint
  - No additional hardware
  - Just a browser needed, works with each OS
- Independent from mobile phone and MNO
  - No SIM change through server-based solution
- Ease of activation for citizen
- Low development costs, no cost for citizen

Contents

1. Introduction
2. **Business Model**
3. IT & Technical Architecture
4. Security an Privacy
5. Use Cases and Processes
6. Awareness Raising

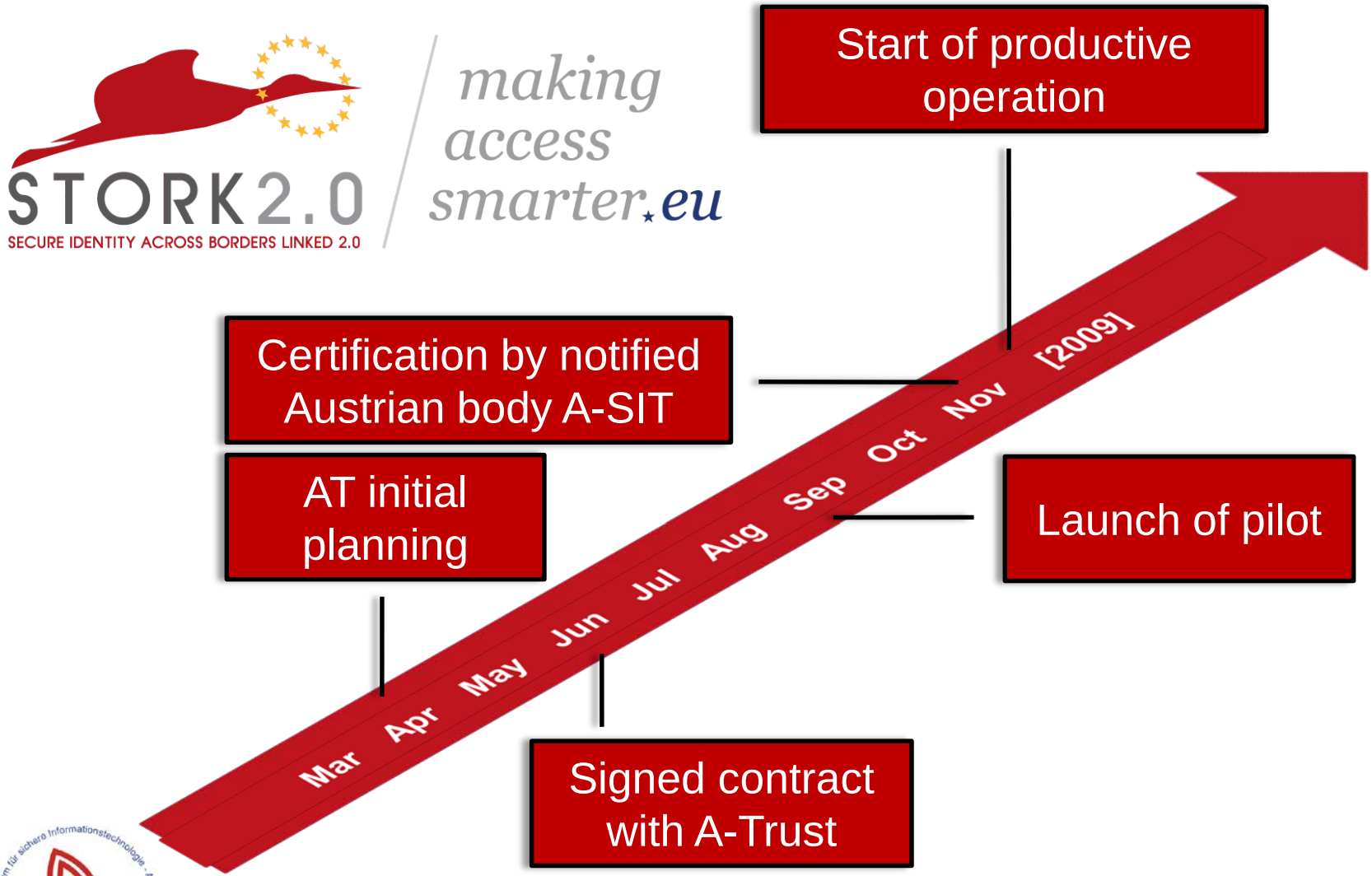


Cost Model

- Development costs funded through STORK
  - 50 % carried by Austrian government
  - 50% by European Commission (CIP ICT-PCP)
- Operations costs by Austrian government
  - Operated by private sector provider “A-Trust”
- Mobile ID free of charge for …
  - Citizens (no costs for activation and use)
  - Service Providers (public and private sector)

… same for card eID (health insurance card)

AT mID Deyployment (through STORK)



Contents

1. Introduction
2. Business Model
3. **IT & Technical Architecture**
4. Security an Privacy
5. Use Cases and Processes
6. Awareness Raising

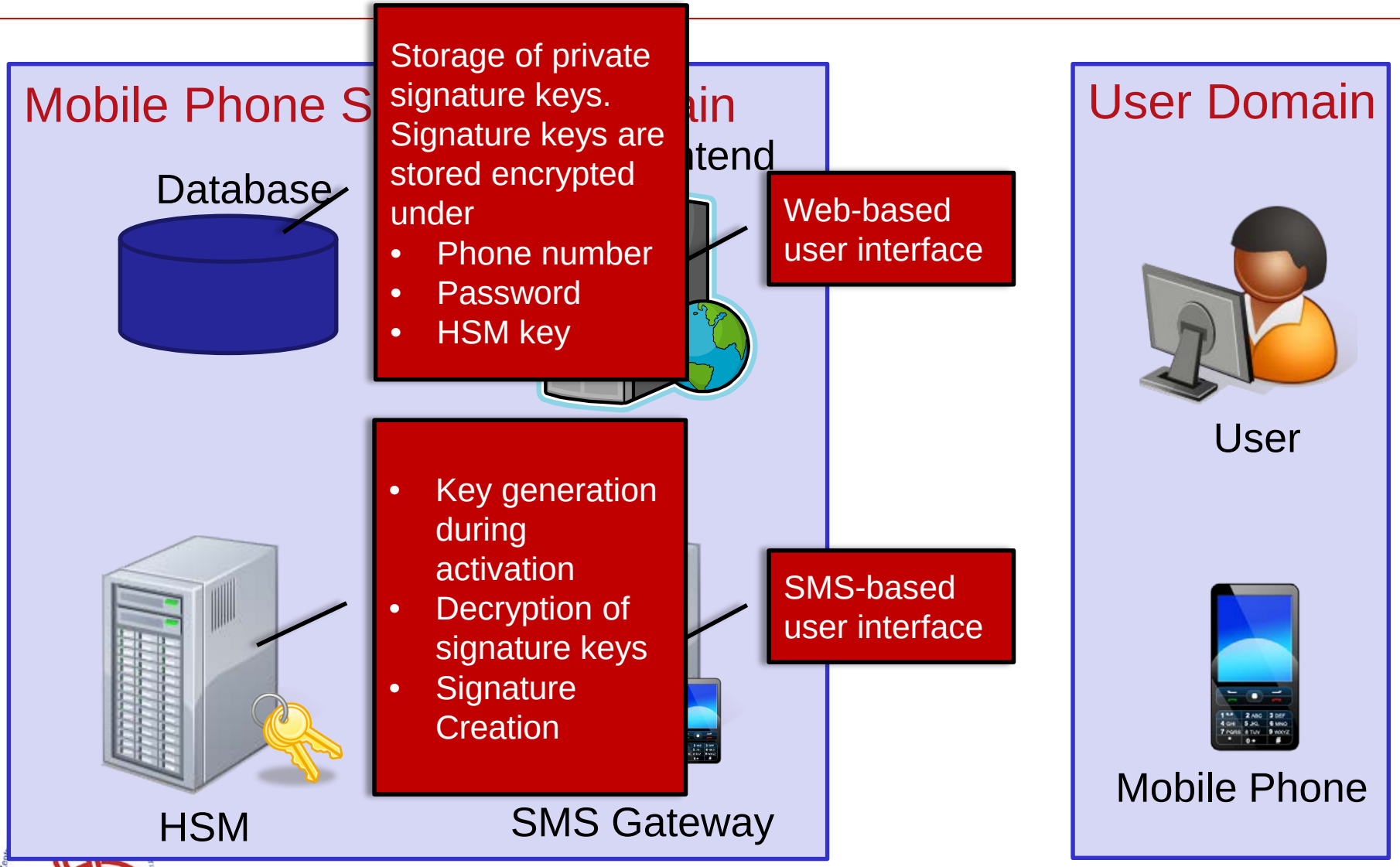
General planning considerations

- Various options considered
  - SIM as SSCD via crypto co-processor
    - Estonia, Norway, Turkey, …
    - SIM to be replaced
    - Negotiate with (several) operators
  - Server-Signature as SSCD
    - **Finally chosen in Austria, as**
      - no change to mobile infrastructure
      - Citizen can keep SIM and mobile device
      - Open for foreign mobile operators

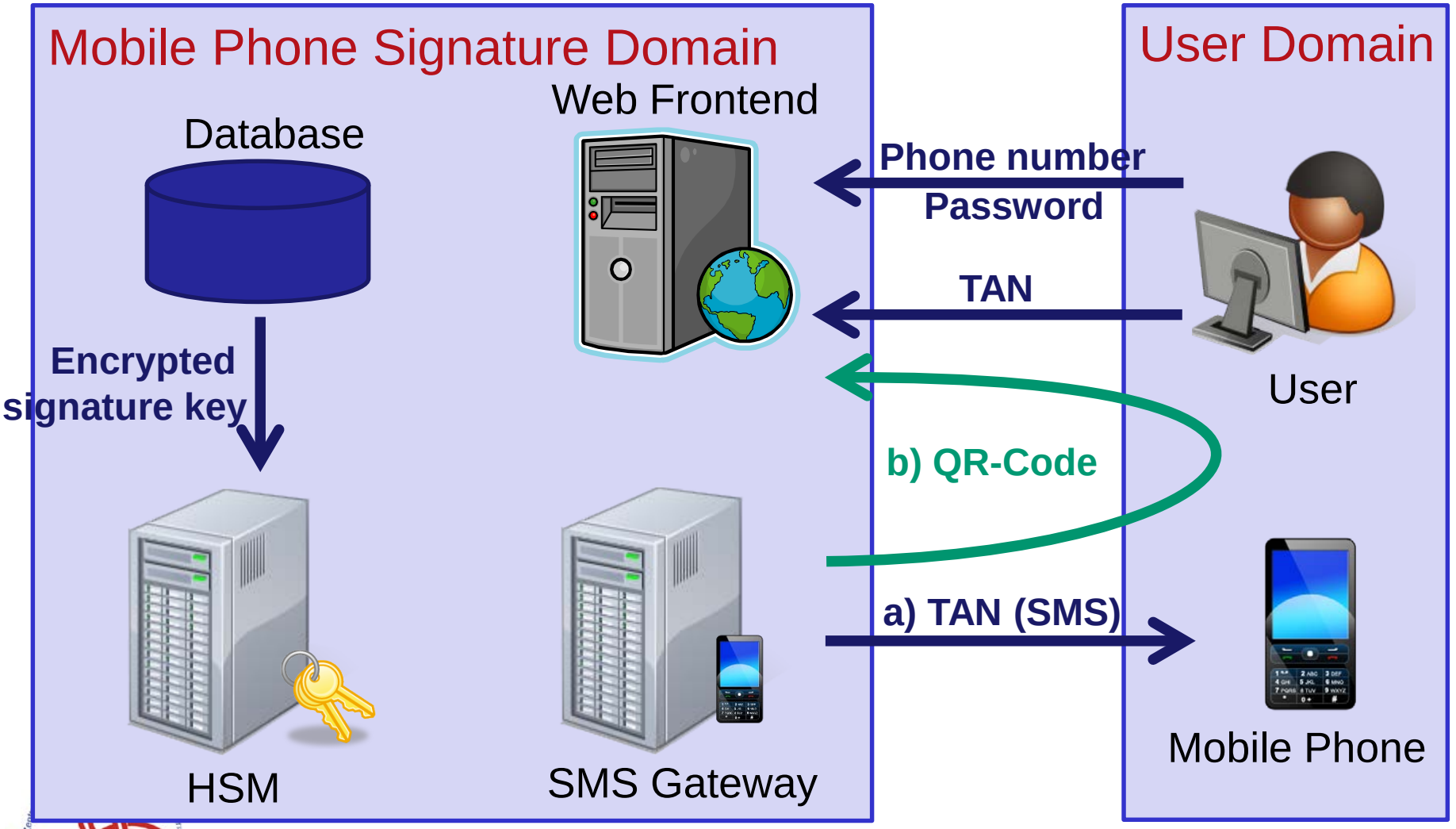
Austrian mobile eID: Core Aspects

- Operated by a Ceritifcation Service Provider (CSP) for qualified certificates
- Signature-creation data (cryptographic keys) kept at CSP but controlled by the signatory
- 2-factor authentication (knowledge & possession)
- Secure Signature-Creation Device
  - 1999/93/EC Ann. III, confirmed by notified body
  - now eIDAS qualified signature-creation device

The Architecture



The Operation: a) SMS b) QR code



Other guideline questions on section 3

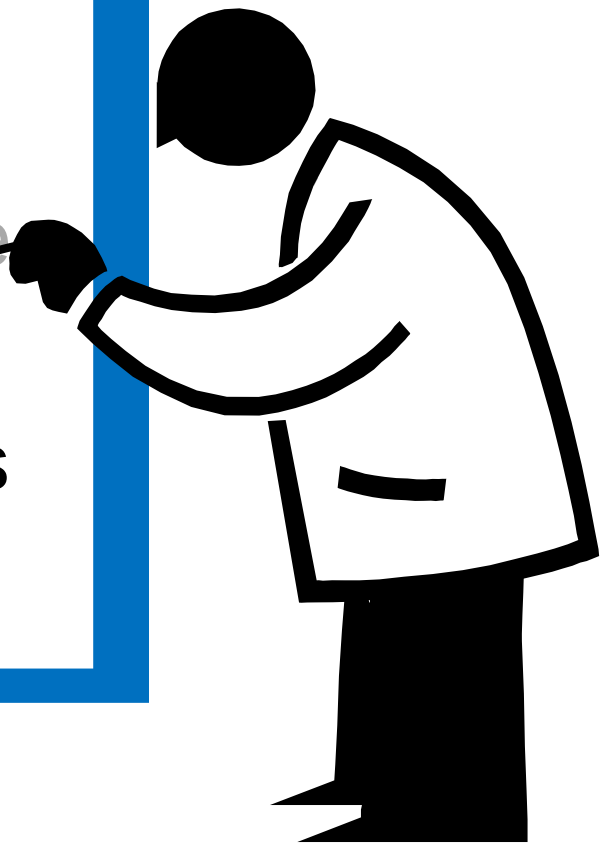
- Does mID solution use biometrics?
  => Answer Austria: No
- Does mID allow to use it in physical work or only digital?
  => AT: Electronic only
- Is there any central system which logs every transactions?
  => AT: Server-based system, limited logs (data protection)
- Is every transaction handled by central system? This means that country / system knows about every transactions (citizen could have problem with privacy)
  => AT: Server-based system, limited logs (data protection)

Other guideline questions on section 3

- Does citizen has access to his transactions and logs (like where his mID was used?)
  => AT: No, data not available
- How is mID verified? Are there any physical chips or scanners which are used by eg. Policeman in order to verify mID ?
  => AT: In electronic online processes only (no verification in physical world like by police)

Contents

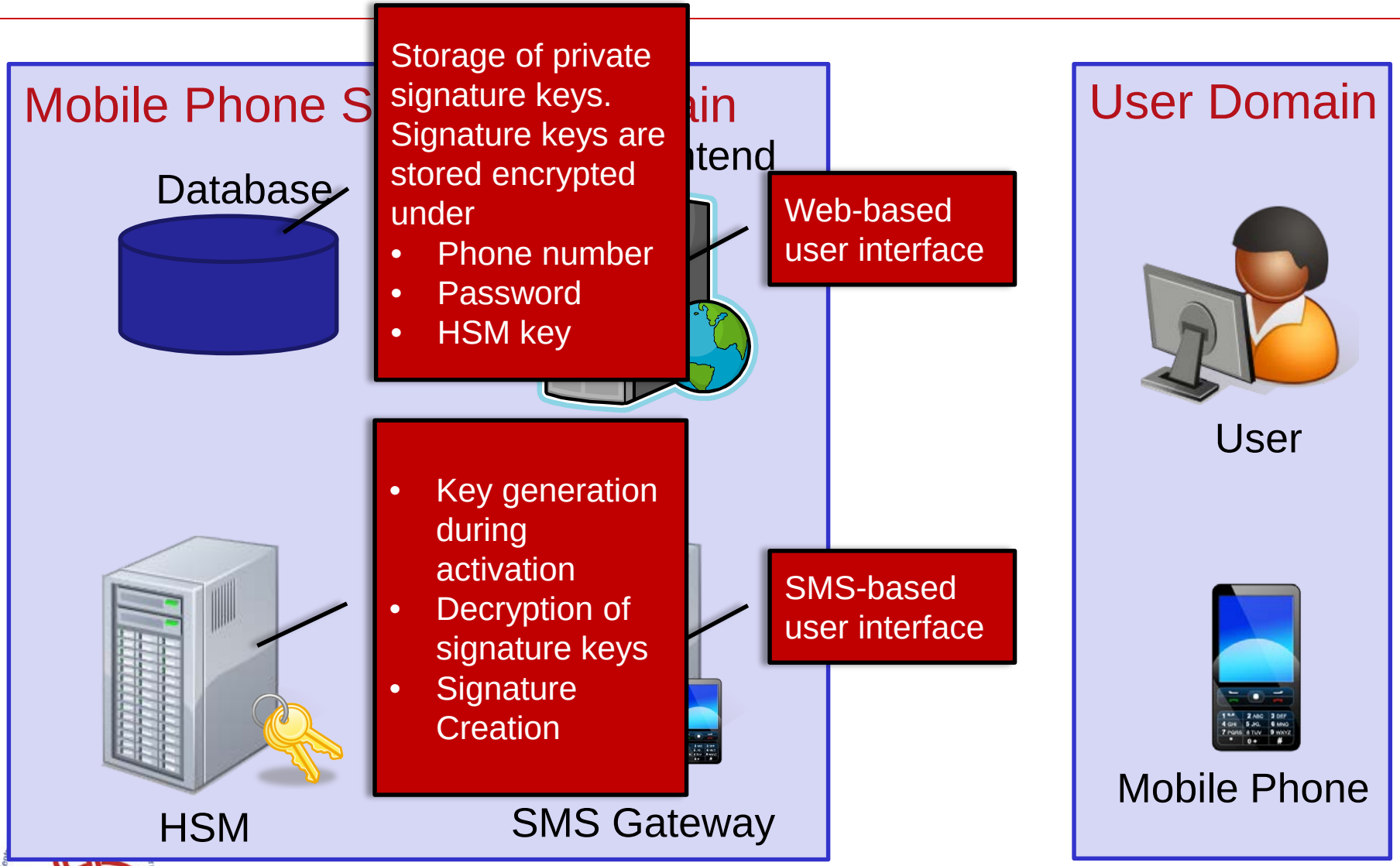
1. Introduction
2. Business Model
3. IT & Technical Architecture
4. **Security an Privacy**
5. Use Cases and Processes
6. Awareness Raising



Main security / privacy features

- Data-protection is a main feature of the Austrian eID (both smartcard and mobile ID)
  - Sector specific identifiers (cryptographically derived)
    - *Public sector*: per sector identifiers (tax, health, …)
    - *Private s.*: per organisation (+ additional measures)
- Security based on hardware modules
  - Hardware Security Module
  - Certification as "*secure signature-creation device*" under EU signature Directive; confirmed by a notified body
  - State supervision, regular re-certification and audits

The Architecture



Other guideline questions on section 4

- Have the mID solution been ever hacked or did somebody tried to hack mID? What were the typical attacks?
  => Answer AT: No incident known
- Is there a central certification body? Its is public or private?
  => AT: State supervision (under EU Signature Directive and EU eIDAS); Certification by body notified by the state
- Was there any generated false mID on the market?
  => AT: None known
- What are the key security requirements for secured ID?
  => AT: “SSCD” under EU Signature Directive and “QSCD” under EU eIDAS;
  Expected to meet Level of Assurance “high” of EU eIDAS

Other guideline questions on section 4

- How is the mID verified during registration?
  => AT: Various options:
  - Physical presence at Registration Officer showing a photo ID
  - Processes at equivalent security that link to previous phy. presence and can start online (plus e.g. registered letter, bank transfer, …)
- If mID is an app then how is it certified and distributed?
  => AT: not applicable *(QR-protocol part of SSCD-certification)*
- Is mID device paired with mID?
  => AT: Cryptographic pairing between HSM and QR-app
- How privacy is secured for citizens?
  => AT: Through sector-specific identifiers
  cryptographically derived per sector or organisation (private sector)

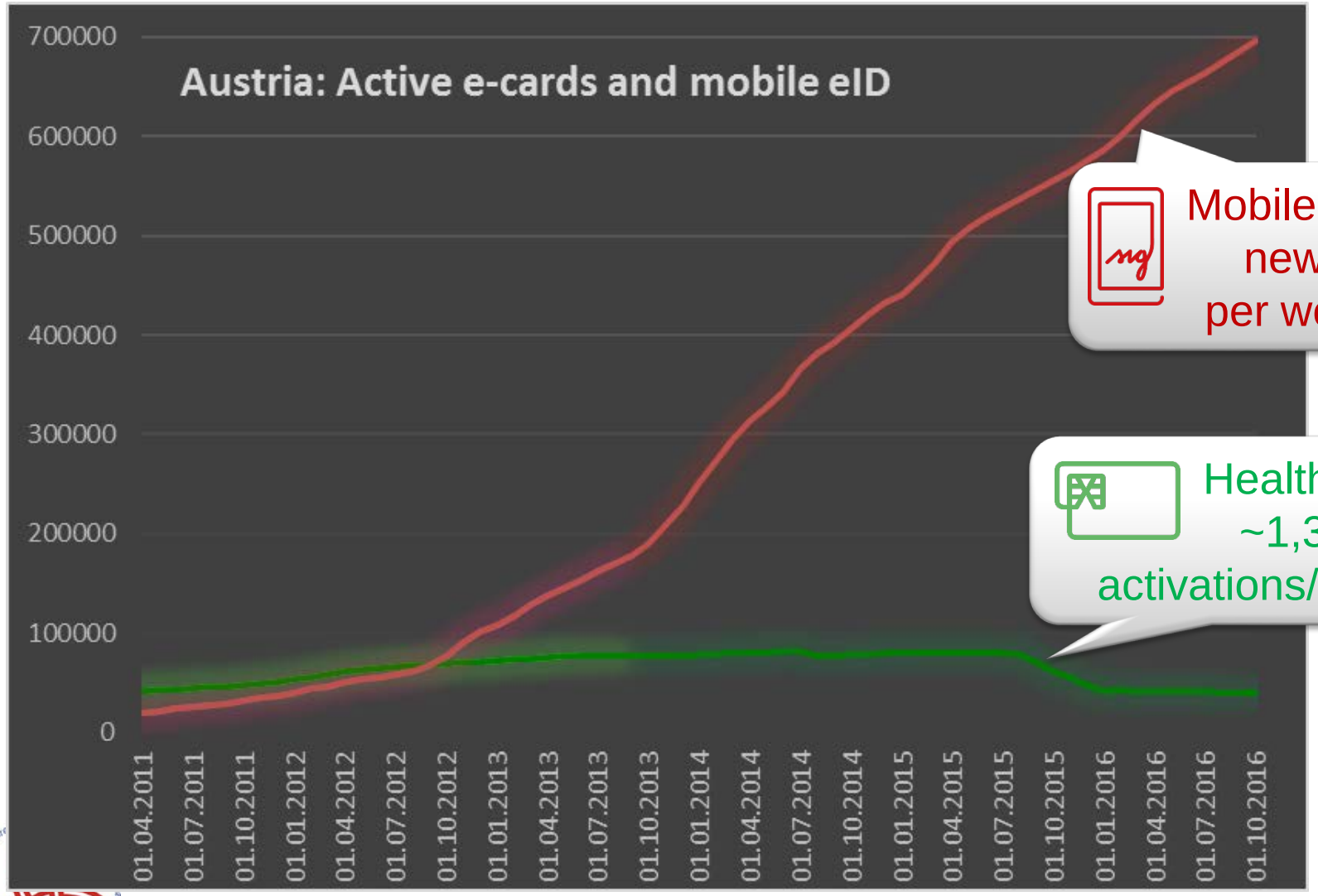
Contents

1. Introduction
2. Business Model
3. IT & Technical Architecture
4. Security an Privacy
5. **Use Cases and Processes**
6. Awareness Raising

Services overview

- Mobile ID used in about 300 online services
  - Both Public Sector and Private Sector
- Offered to all citizens (voluntary)
  - Currently about 700 thousand active mobile IDs
  - *Comparison: about 120 thousand active smartcards*
    - *40 k health insurance cards as eID*
    - *80 k profession cards (lawyer, notaries, public officials, …)*
- About 15 – 20 k mobile ID uses per day
  (no figures known for smartcard, as it is decentralized)

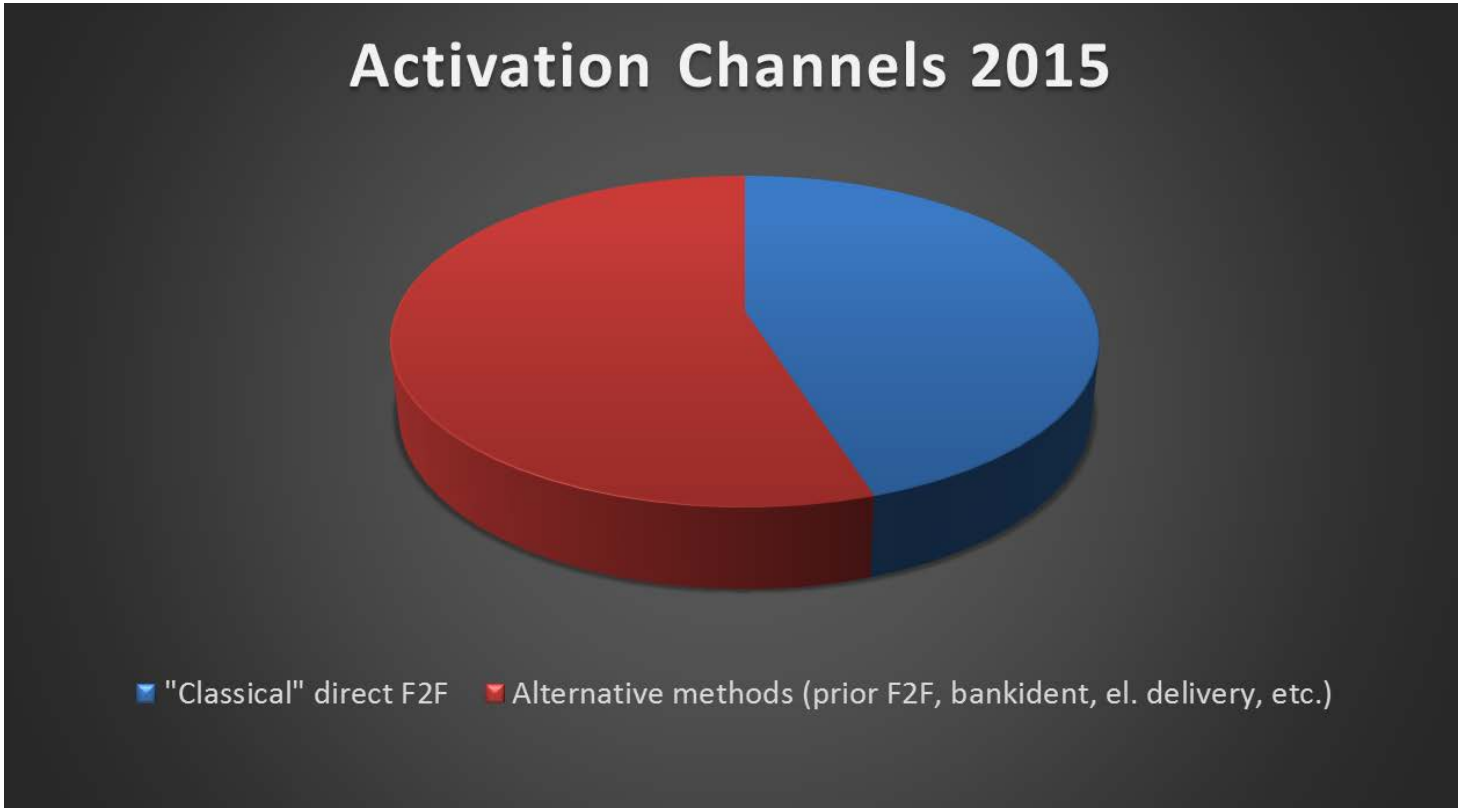
Austria: Card vs mobile ID active users



Registration Options

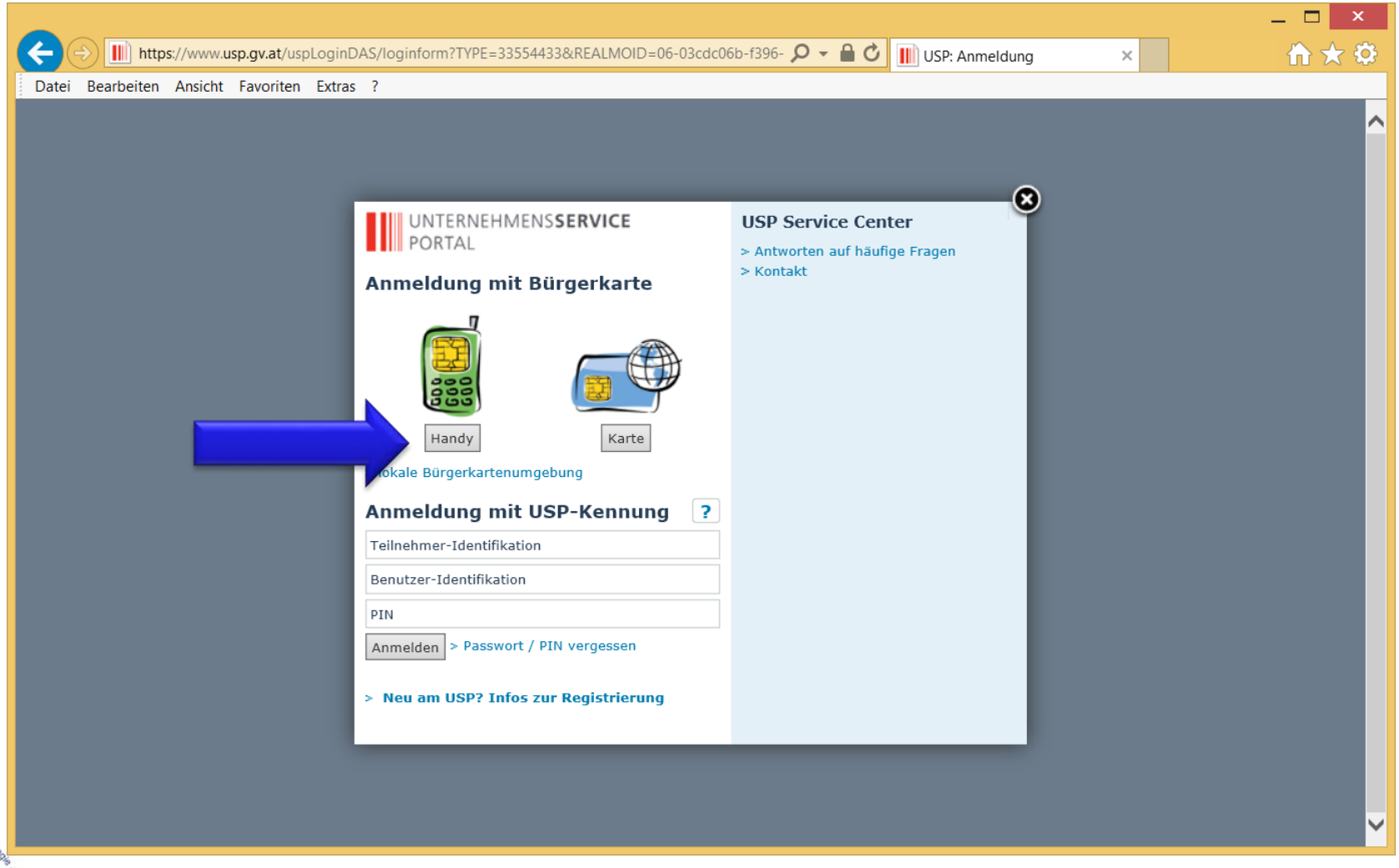
- Citizen can choose several options
  - Physical presence at Registration Office
    - Post office, tax office, notary, town hall, etc.
  - Online using another eID (e.g. a smartcard)
  - Online through secure alternative authentication and linked to previous physical presence
    - Online banking, tax portal, etc.
      - Depending on process further info (e.g. activation letter)
- Convenience important to get take-up!

Joice of convenient registration is essential

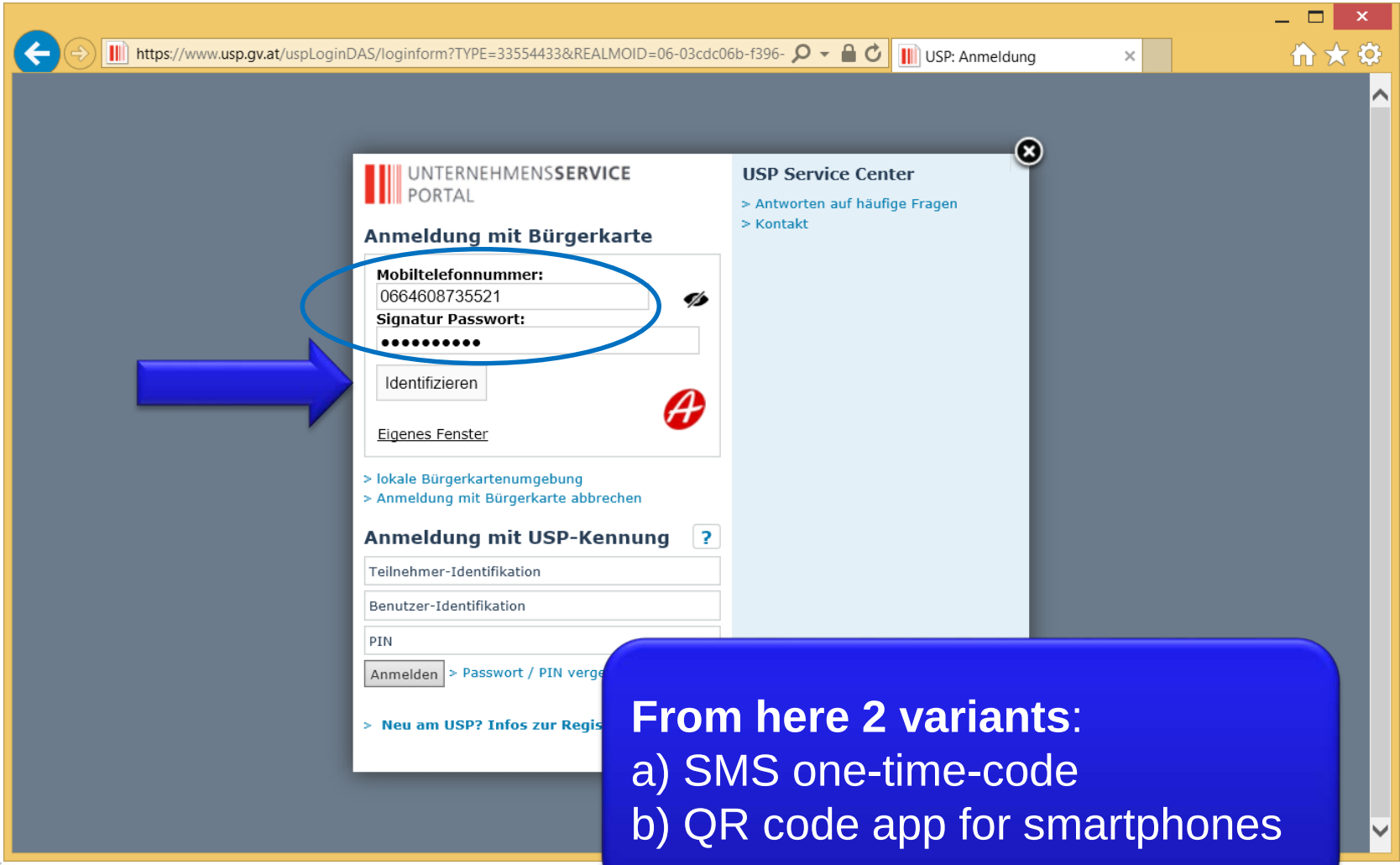


Demo: Business Service Portal

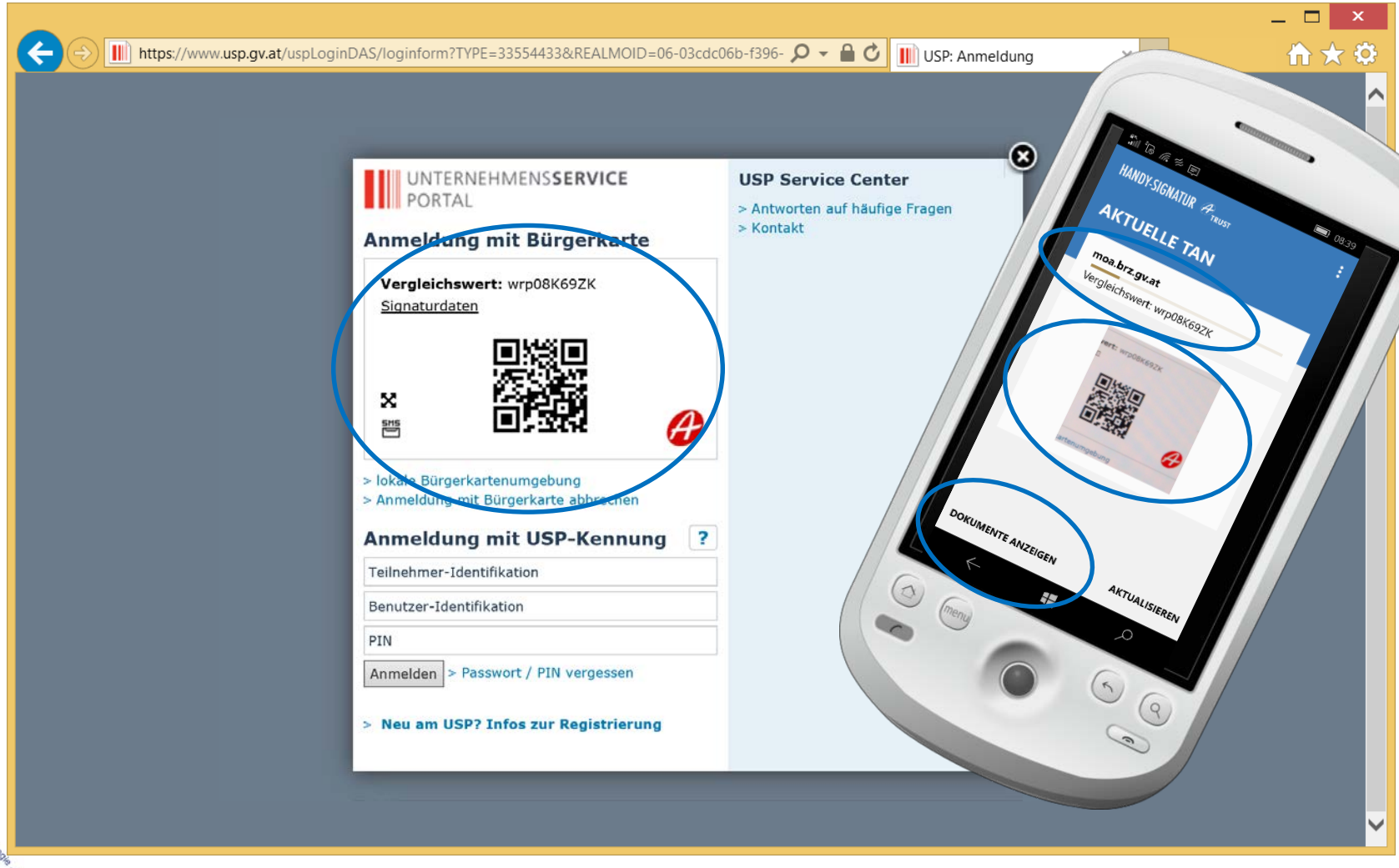
Demo: Select Card or Mobile ID



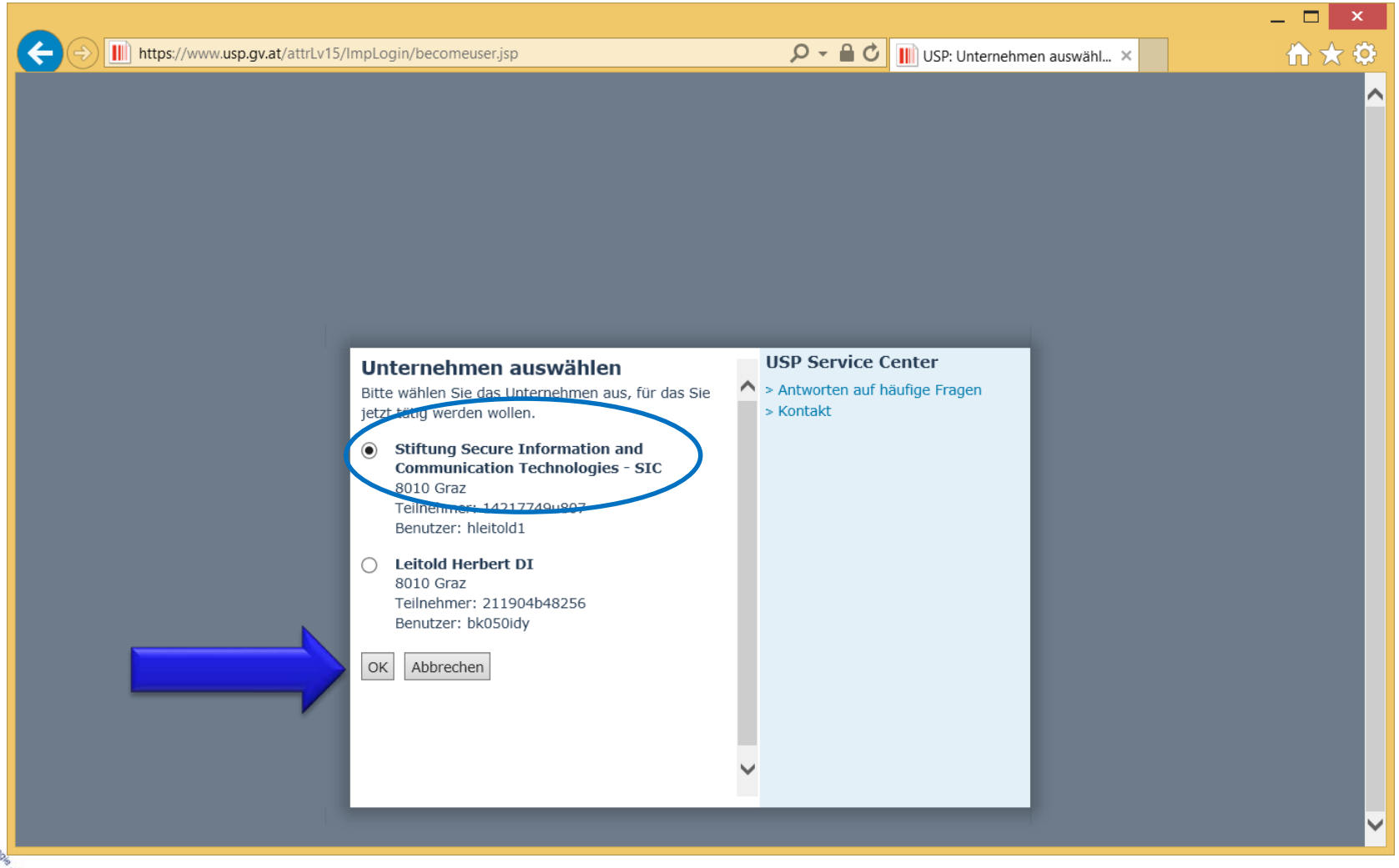
Demo: Mobile ID dialogue



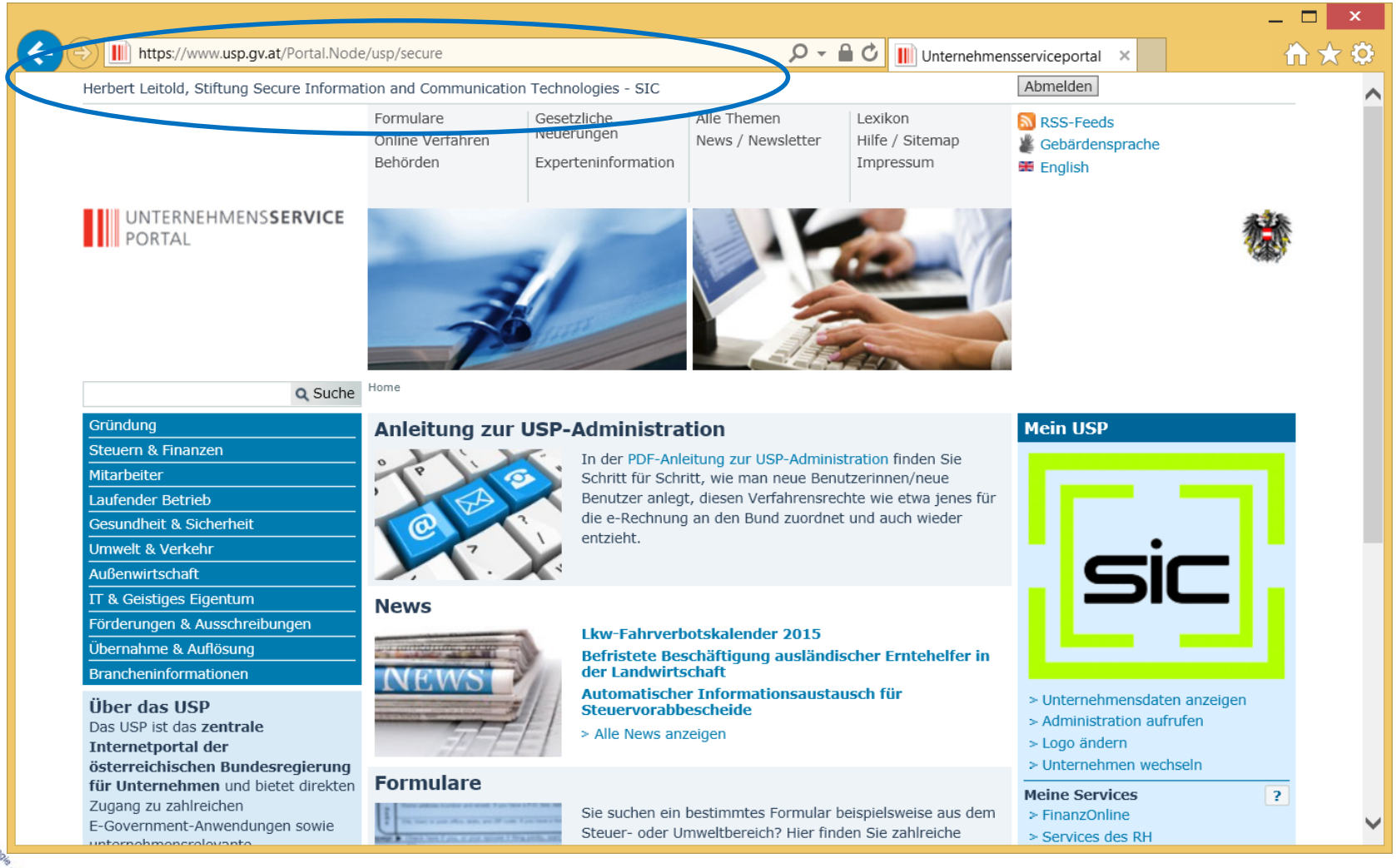
Demo: Variant „b“ - QR Code App



Demo: Representation information

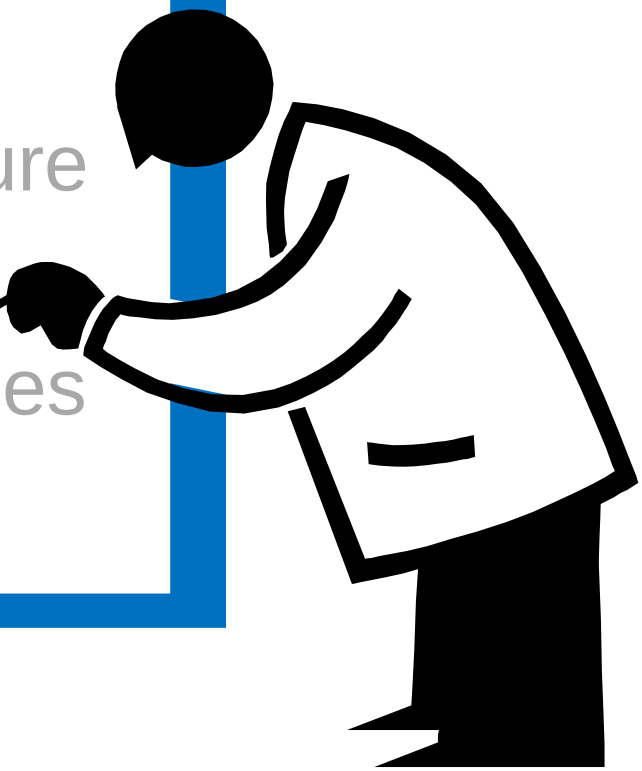


Demo: Done


https://www.usp.gv.at/Portal.Node/usp/secure
Unternehmensserviceportal
Herbert Leitold, Stiftung Secure Information and Communication Technologies - SIC
Abmelden
Formulare
Online Verfahren
Behörden
Gesetzliche Neuerungen
Experteninformation
Alle Themen
News / Newsletter
Lexikon
Hilfe / Sitemap
Impressum
RSS-Feeds
Gebärdensprache
English
UNTERNEHMENSSERVICE PORTAL
Suche
Home
Gründung
Steuern & Finanzen
Mitarbeiter
Laufender Betrieb
Gesundheit & Sicherheit
Umwelt & Verkehr
Außenwirtschaft
IT & Geistiges Eigentum
Förderungen & Ausschreibungen
Übernahme & Auflösung
Brancheninformationen
Über das USP
Das USP ist das zentrale Internetportal der österreichischen Bundesregierung für Unternehmen und bietet direkten Zugang zu zahlreichen E-Government-Anwendungen sowie
Anleitung zur USP-Administration
In der PDF-Anleitung zur USP-Administration finden Sie Schritt für Schritt, wie man neue Benutzerinnen/neue Benutzer anlegt, diesen Verfahrensrechte wie etwa jenes für die e-Rechnung an den Bund zuordnet und auch wieder entzieht.
News
Lkw-Fahrverbotskalender 2015
Befristete Beschäftigung ausländischer Erntehelfer in der Landwirtschaft
Automatischer Informationsaustausch für Steuervorabbescheide
> Alle News anzeigen
Formulare
Sie suchen ein bestimmtes Formular beispielsweise aus dem Steuer- oder Umweltbereich? Hier finden Sie zahlreiche
Mein USP
sic
> Unternehmensdaten anzeigen
> Administration aufrufen
> Logo ändern
> Unternehmen wechseln
Meine Services
> FinanzOnline
> Services des RH

Contents

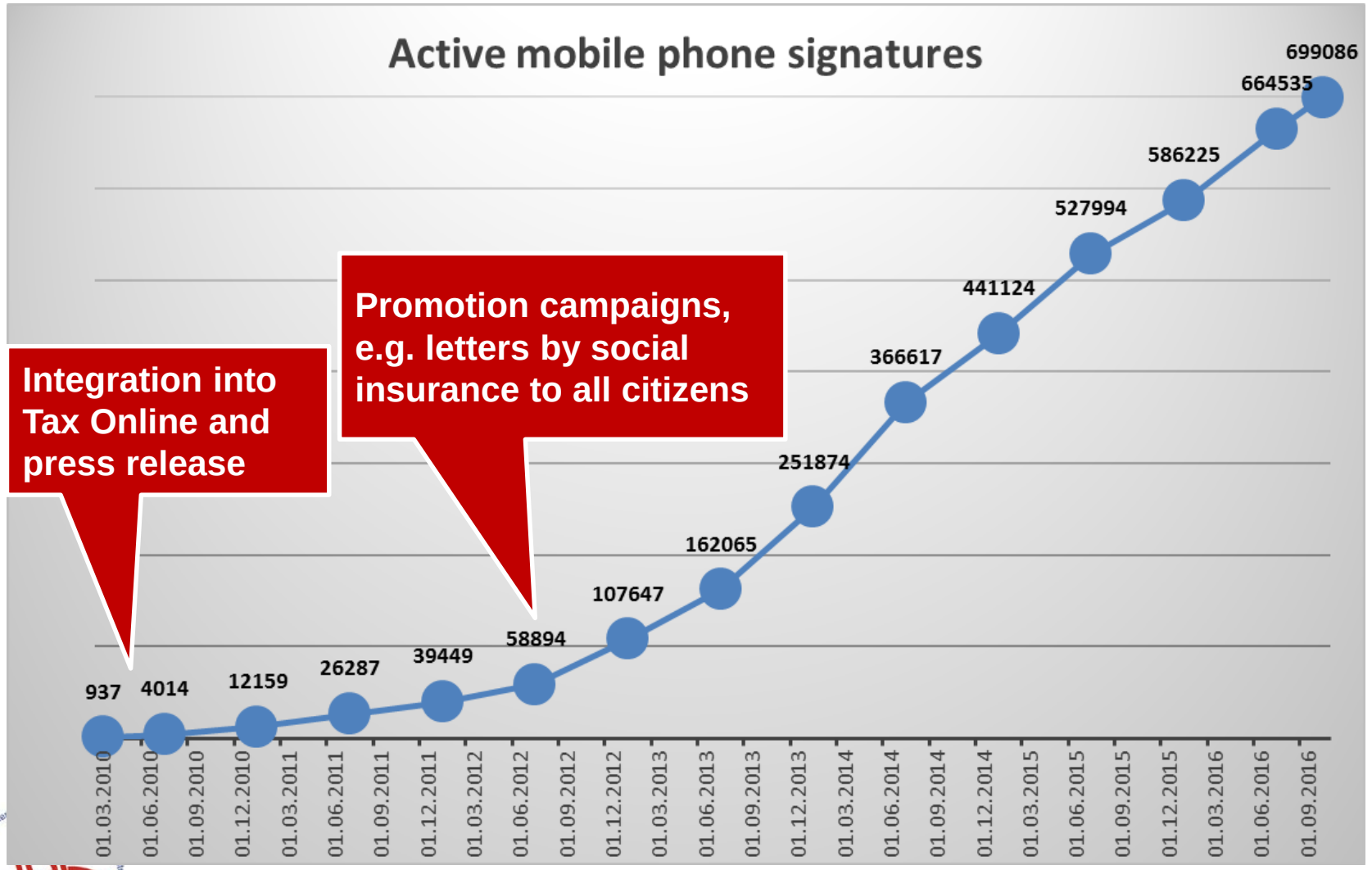
1. Introduction
2. Business Model
3. IT & Technical Architecture
4. Security an Privacy
5. Use Cases and Processes
6. **Awareness Raising**



Awareness rising

- To Service Providers
  - through events (conferences, workshops)
  - through E-Gov. coordination “Digital Austria”
- To Citizens
  - Web: www.buergerkarte.at
  - Advertisements: press, radio, Websites
  - Mailings: e.g. inclusion in pension account letters by to all citizens by social insurance
  - Integration/mentioning in public sector Web sites (e.g. tax portal)

Core promotional milestones



The end

Thank you for your attention!