

Austrian mobile eID/signature

Herbert.Leitold@a-sit.at

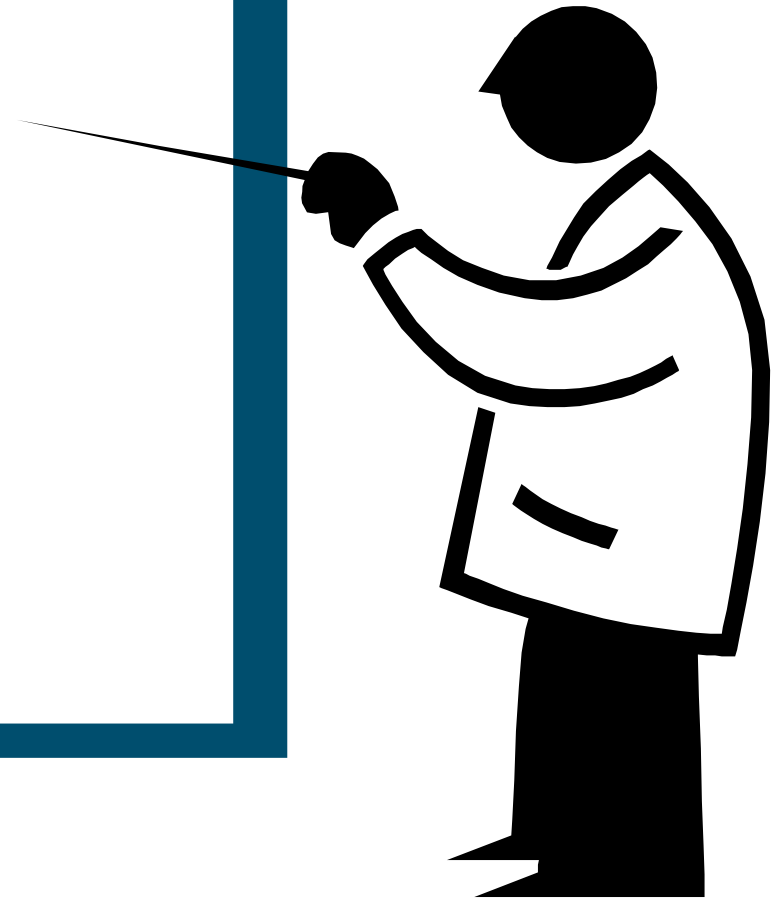
Workshop with Slovenia,
Ljubljana, 29th October 2019

*Several figures and slides
kindly provided by BMDW*

 Federal Ministry
Republic of Austria
Digital and
Economic Affairs

Contents

- Some History
- Technology
- Mobile-First, New E-ID
- Conclusions



Austrian eID Overview

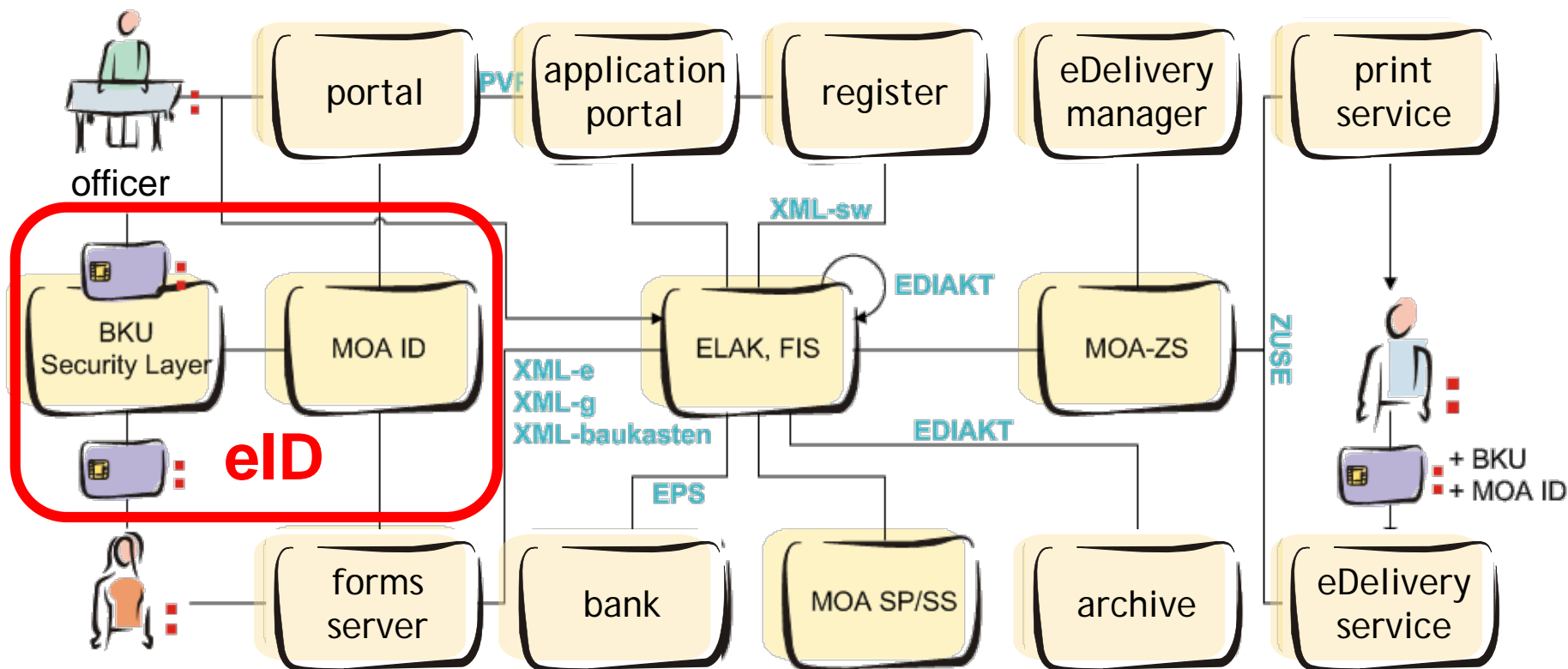
- Voluntary eID introduced in 2005
 - Defines functions, not technologies
 - Sector-specific, persistent identifiers
 - Qualified signature
 - Representation and mandates
 - Technology neutral, started with
 - Smartcards (bank cards, health insurance, service c.)
 - Mobile eID
- Redesign and relaunch early 2020
 - Focus on mobile use



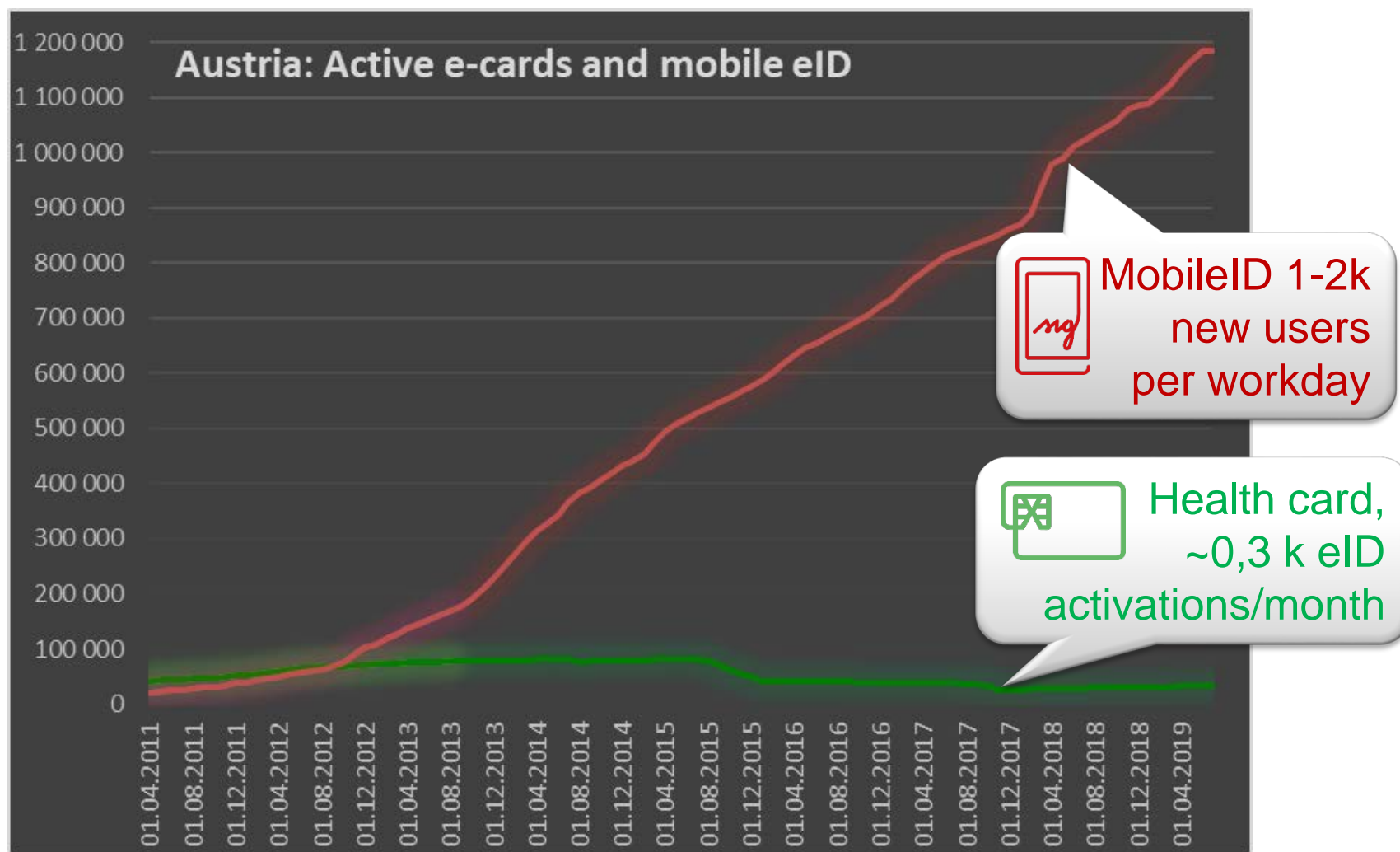
Core principles

- Public and private relying parties
 - 350+ services
see <https://www.buergerkarte.at/en/applications-mobile.html>
- eID is free of charge for
 - Citizens
 - Relying parties (public and private)
- eGovernment big picture
 - Open specifications for interfaces
 - Open source building blocks (eID and beyond)

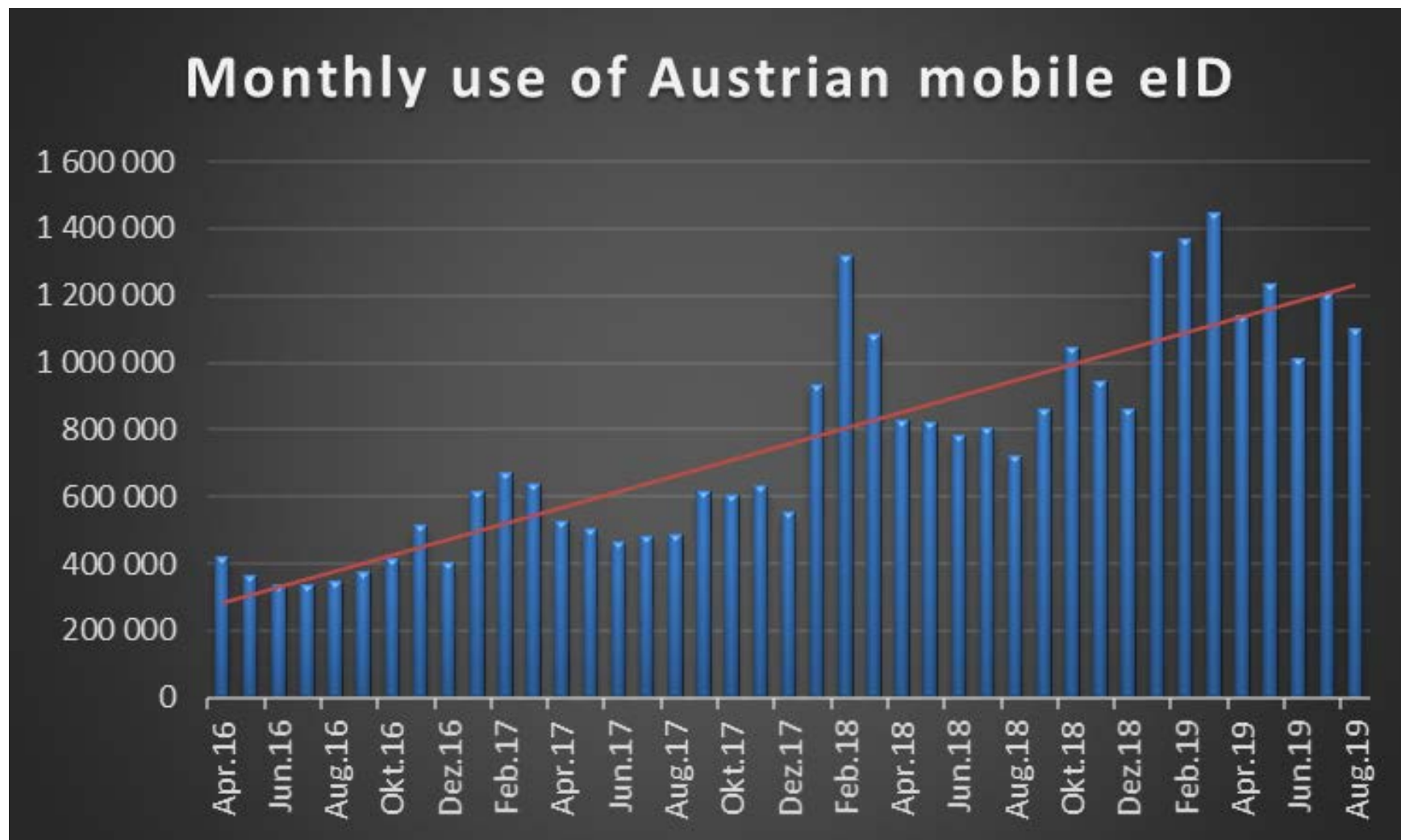
eGovernment Big Picture



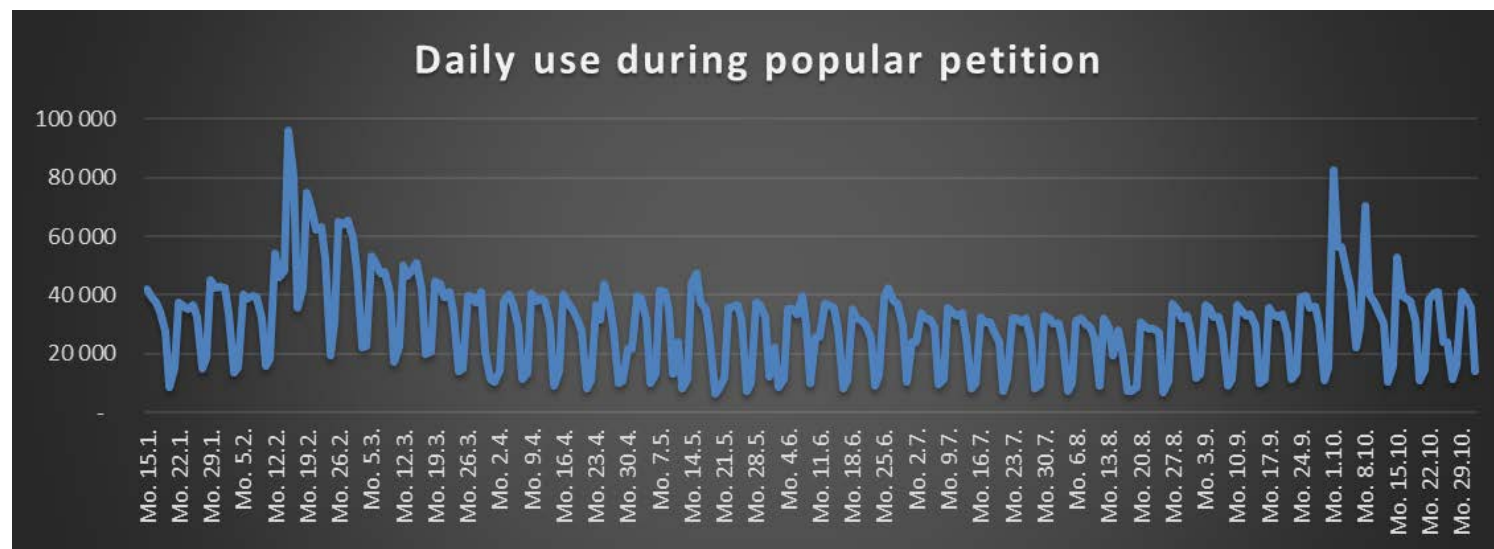
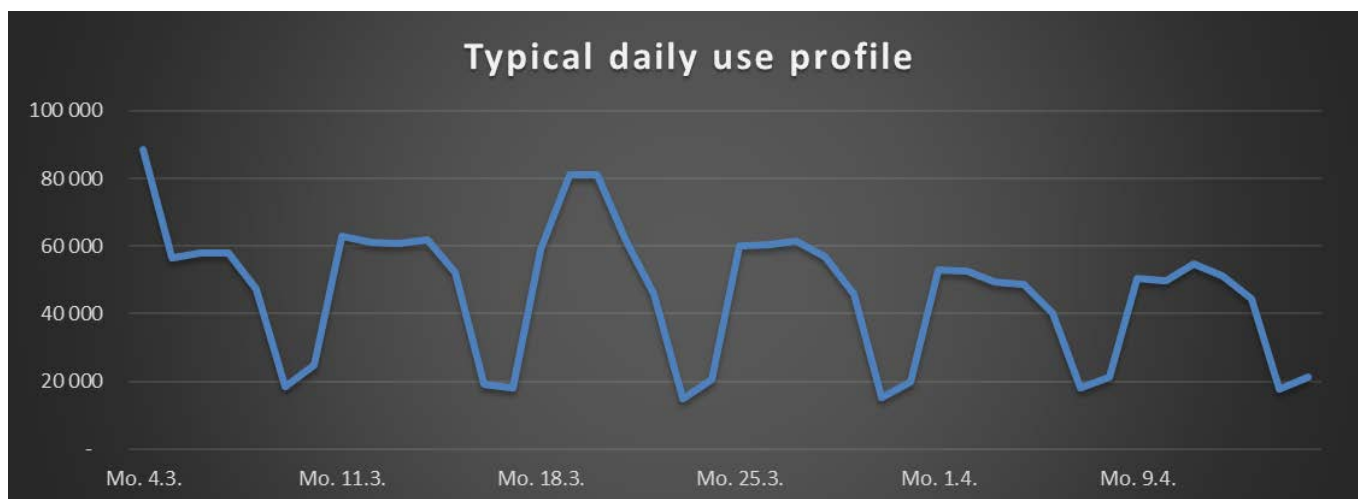
Austria: Card vs mobile ID active users



Mobile eID monthly use

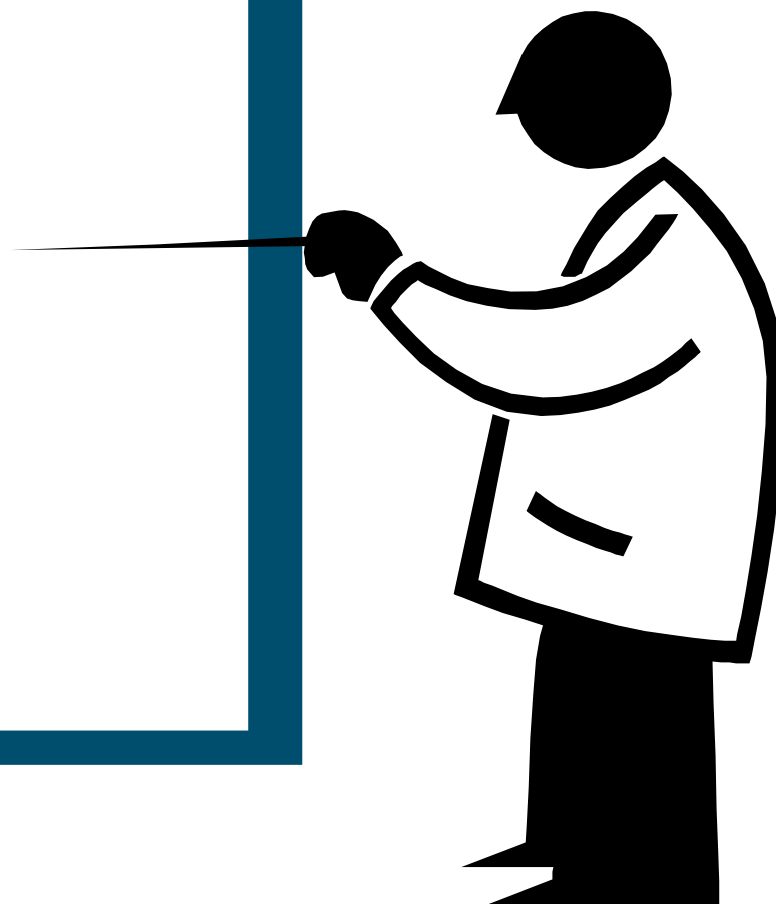


Daily use profiles

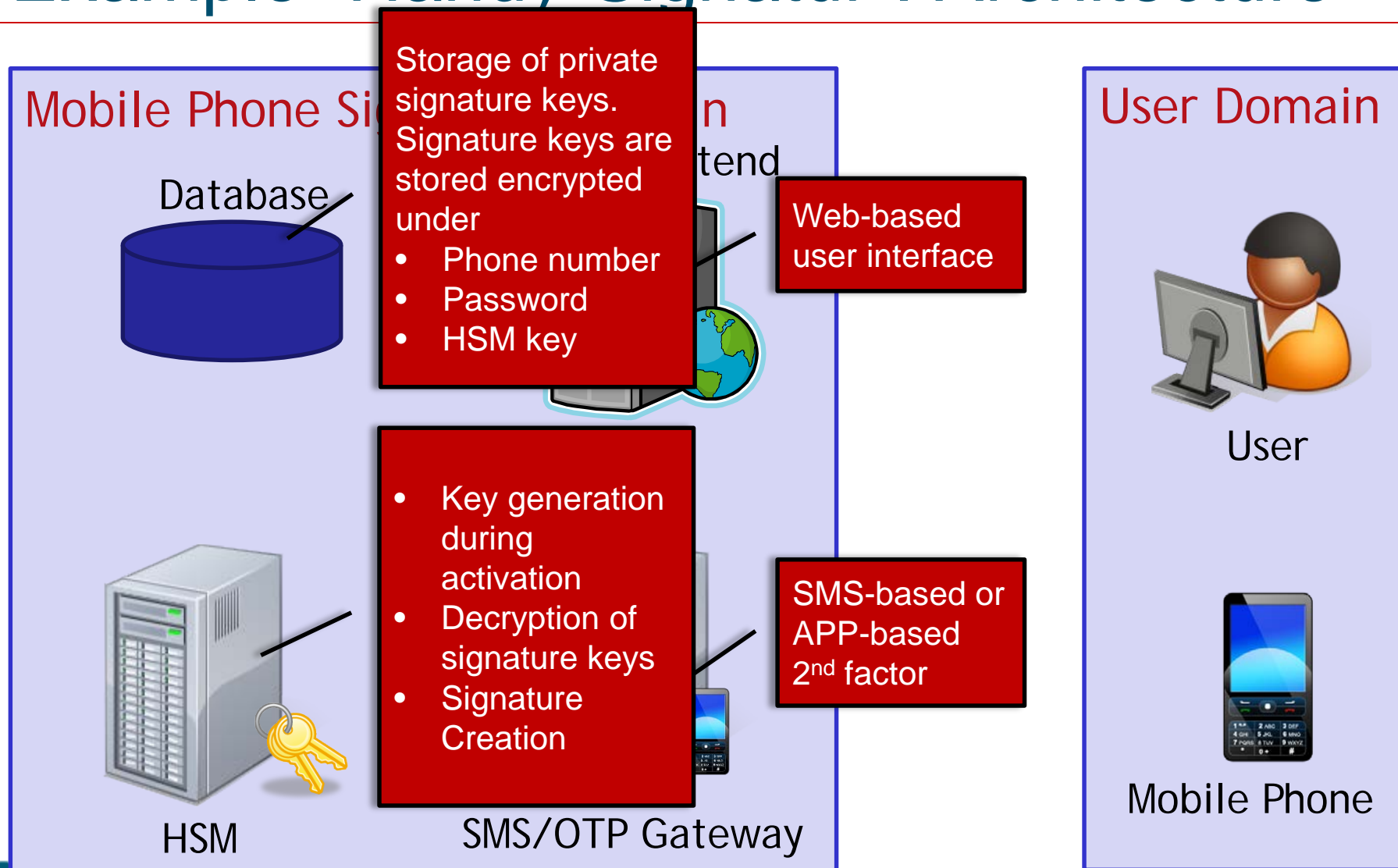


Contents

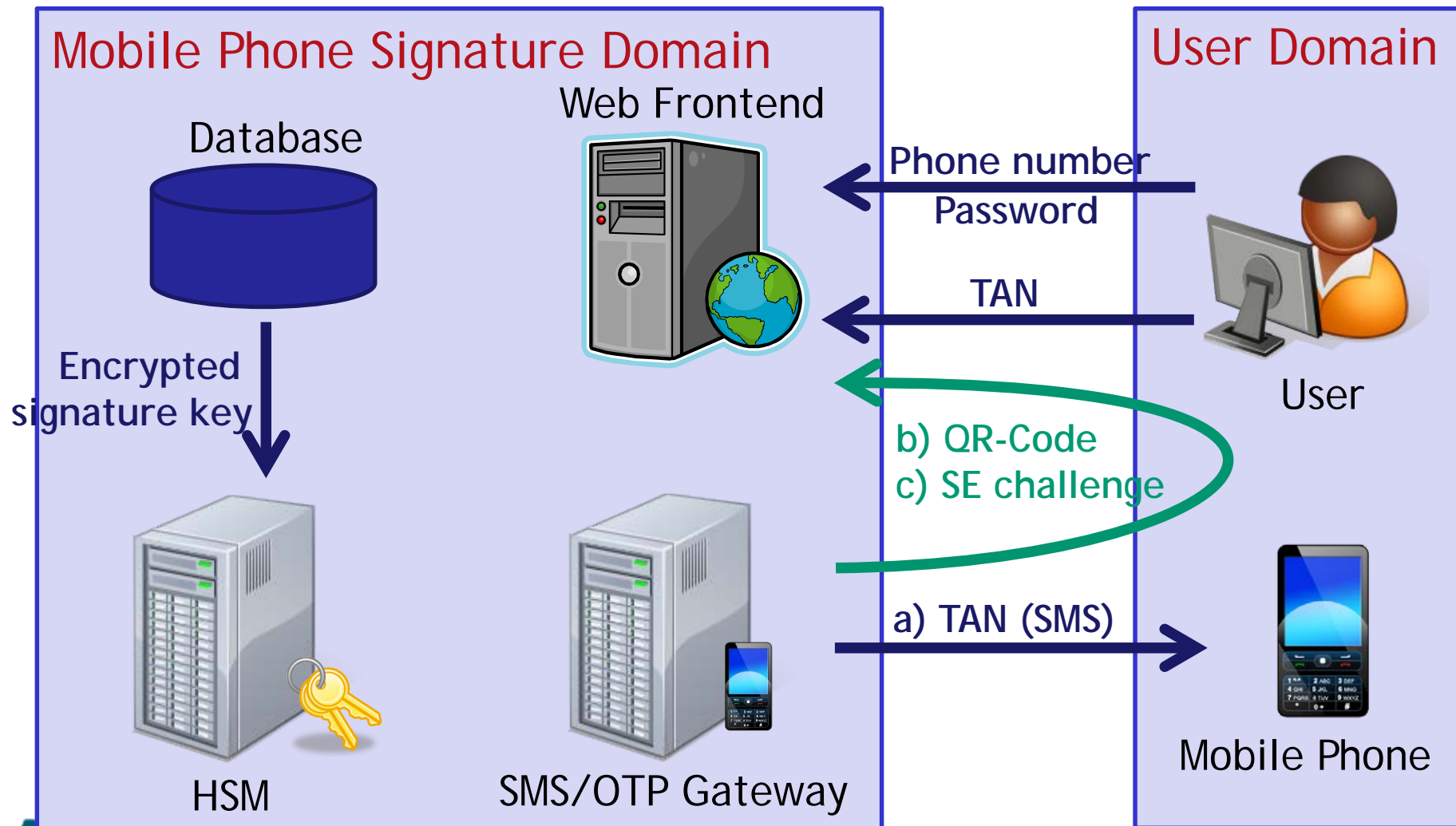
- Some History
- Technology
- Mobile-First, New E-ID
- Conclusions



Example “Handy-Signatur”: Architecture



Operation: a) SMS b) QR c) TEE/SE

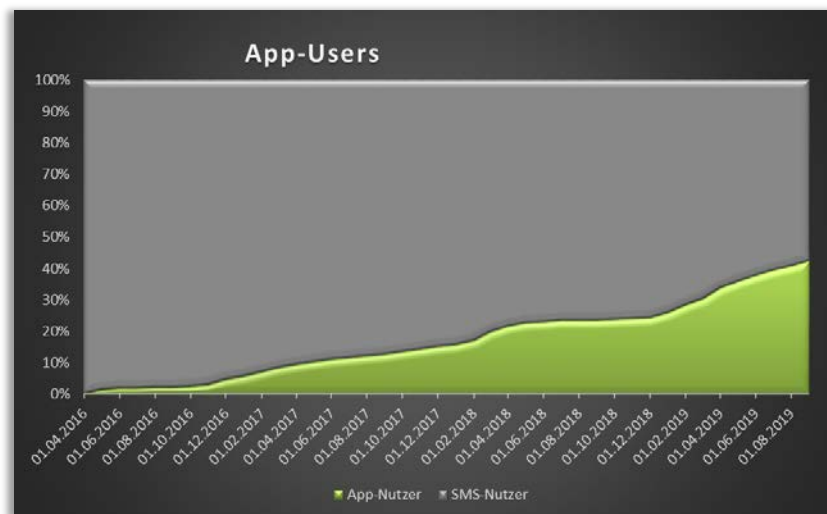


Core components

- QSCD based on
 - HSM nShield 500e F3
 - Signature keys (ECC 256 bit) encrypted under
 - HSM key
 - Mobile number
 - Password (user-chosen)
 - Server and HSM in a safe at the QTSP

Authorisation Options

- Three OTP options
 - SMS-OTP (*original version since 2005*)
 - OCR-app (*two devices enforced with advent of smartphones*)
 - SE/TEE app (*binding to HW sec. element; fingerprint, faceID*)
- App with SE/TEE meanwhile default
 - But convergence takes time



Authentication Process

1. Creating a sector-specific identifier

- Cryptographically derived from identifier in Central Population register (encrypt + hash)
- Unique per *public* sector (health, tax, education, ...)
- Unique per private-sector organization
- Unique per receiving MS

2. Qualified signature over human-readable auth-block

Anmeldedaten:

Daten zur Person

Name: Herbert Leitold
Geburtsdatum: 12.08.1965

Daten zur Anwendung

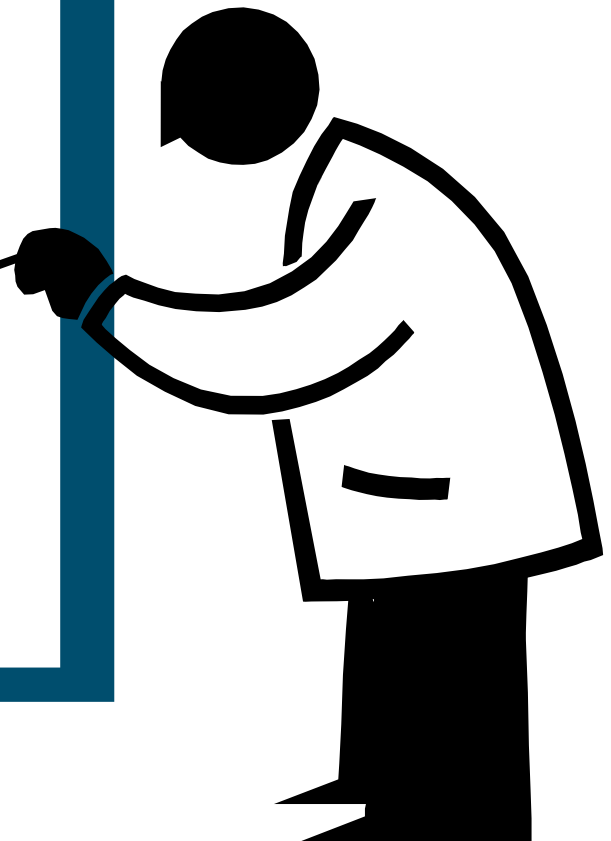
Name: ECAS (Production instance)
Staat: Österreich

Technische Parameter

URL: <https://ecas.ec.europa.eu/cas/eidas/metadata/ecas-ec-europa-eu.xml>
eIDAS: urn:publicid:gv.at:eidasid+AT+EU
Identifikator: AT/EU/e[REDACTED]UE=
SessionToken: x3230313932323130aa93a45f1cbef41d5818ba
Datum: 22.10.2019
Uhrzeit: 17:59:27

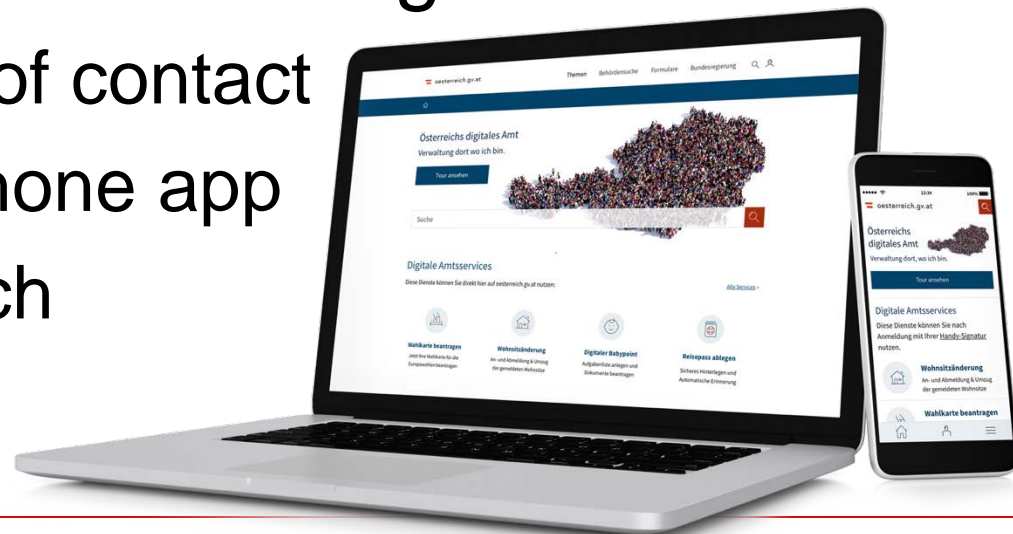
Contents

- Some History
- Technology
- **Mobile-First, New E-ID**
- Conclusions



New developments

- New E-ID to be launched early 2020
 - Taking experience since 2005 into account
 - Server-based mobile eID (drop smartcard-eID)
 - Enable **single device use** (SE or TEE)
- eGov/mGov App Oesterreich.gv.at
 - Digital single point of contact
 - Desktop or smartphone app
 - Mobile first approach
 - eID integration



Oesterreich.gv.at project facts

50

project team staff

9

interfaces

>5 k

information-pages

14

connected systems

4

legal changes

20

productive systems

11

new programmes

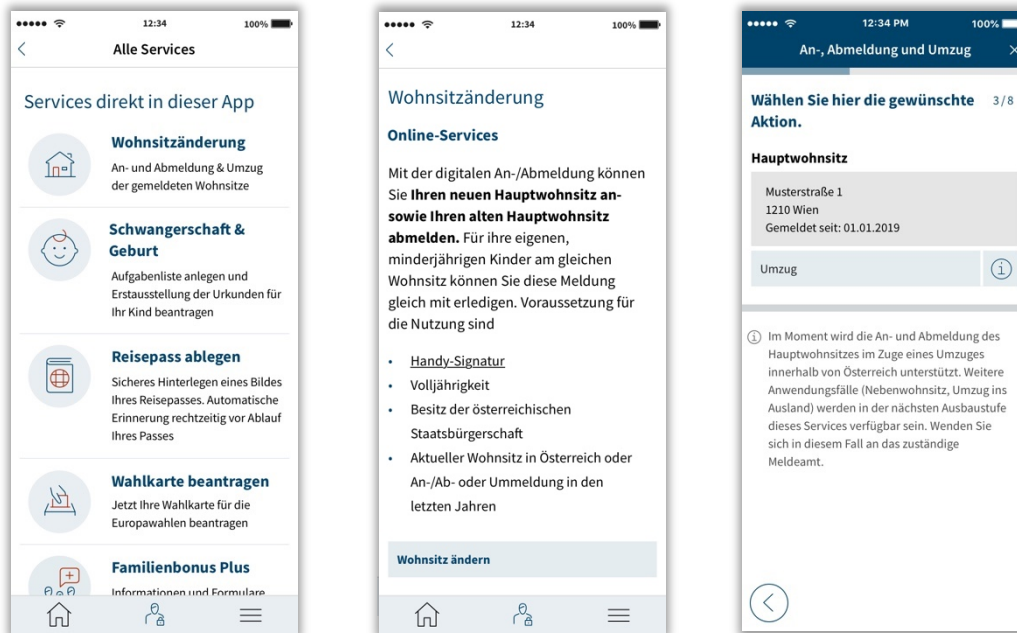
1

central platform

Some processes with online demand

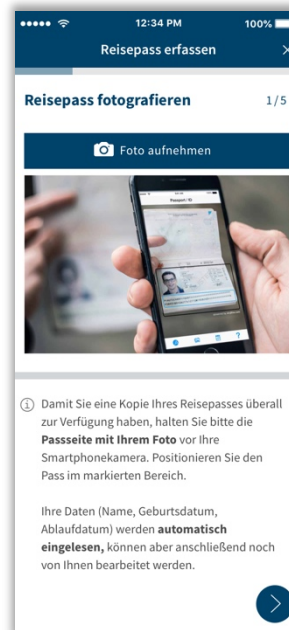
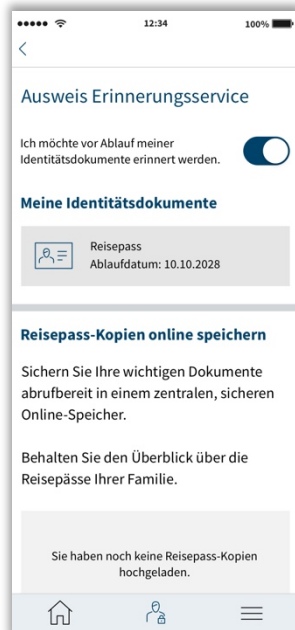
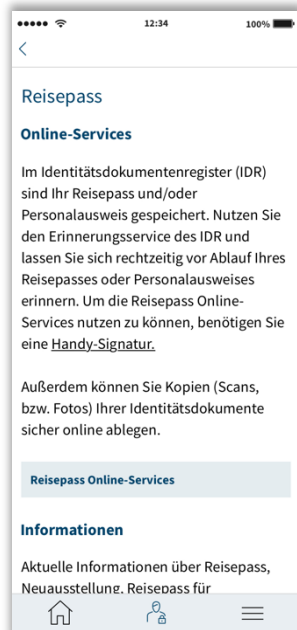
- 800.000 changes of address p.a.
(78% asked for online service)
- 1 000.000 election-cards at last general election
(65% asked for online service)
- 850.000 passports expire p.a.
- 80.000 births p.a.
- 55 000.000 client-contacts at connected platforms

Change of address



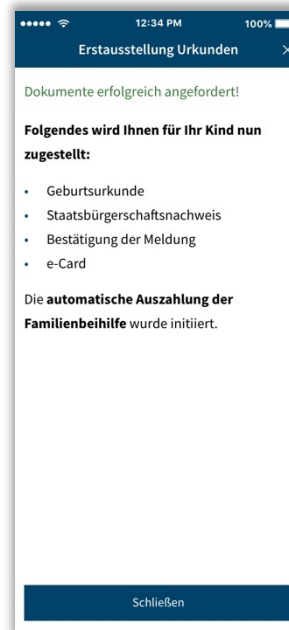
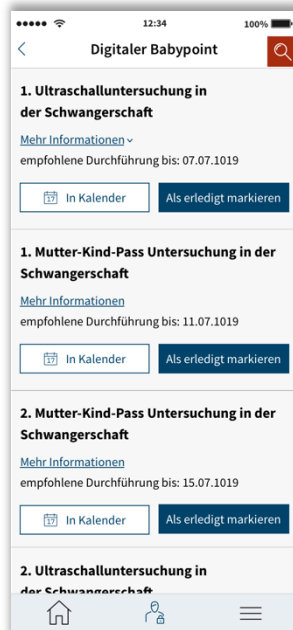
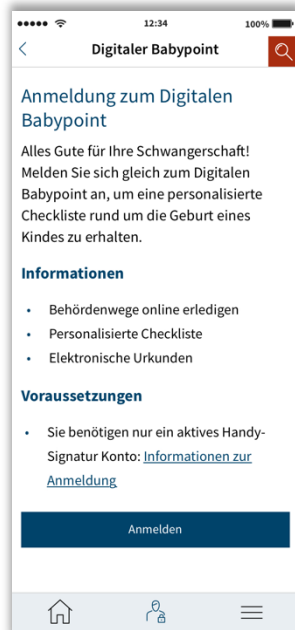
- Connected to Central Population Register
- De-register previous residence, register new residence

Passport-Expiry Reminder




- Connected to ID Document Register
- Reminder before expiry
- Upload of passport scan to eID-secured document safe

Digital Baby-Point



- Apply for
 - Birth certificate
 - Certificate of citizenship
 - Residence certif. at parent home address
 - Delivery of health insurance card
- Information services
- Suggestions and reminders for medical checks

Further services ...

- SSO to major portals
 - Business Service Portal
 - Social Security Portal
 - Tax Online
 - Transparency Portal
 - etc.
 - Life-event structured information platform
- 
- relevant for businesses

Example SSO to Transparency Portal

00:46 4G+

Transparenzportalabfrage
gem. § 32 TDBG 2012

erstellt am 30.09.2019

Leistungsempfänger Grunddaten

Familien-/Nachname Vorname:
Leitold Herbert

Geburtsdatum:
12.08.1965

Abgefragtes Jahr:
2018

1. Einkommen gesamt gem. § 5 TDBG 2012

Bruttoeinkommen gesamt (Bescheid 2018)

Nettoeinkommen gesamt (Bescheid 2018)

2. Einkommen Details gem. § 5 TDBG 2012

3. Sozialversicherungsleistungen, Ruhe- und Versorgungsbezüge gem. § 6 TDBG 2012

Hinweis
Es sind keine gemeldeten Leistungen im abgefragten Jahr vorhanden.

4. Ertragsteuerliche Ersparnisse gem. § 7 TDBG 2012

Steuerbefreiungen für Reisevergütungen bzw. Reiseaufwandsentschädigungen für Arbeitnehmer	2.373,34	
Sonderausgaben gemäß § 18 Abs. 1 EStG 1988 oder der Pauschbetrag gemäß § 18 Abs. 2 EStG 1988	660,00	
Zwischensumme x Grenzsteuersatz (50%)	3.033,34	1.516,67

5. Förderungen / Transferzahlungen gem. § 8 TDBG 2012

Bausparprämie gemäß § 108 EStG 1988	18,00
Zwischensumme	18,00

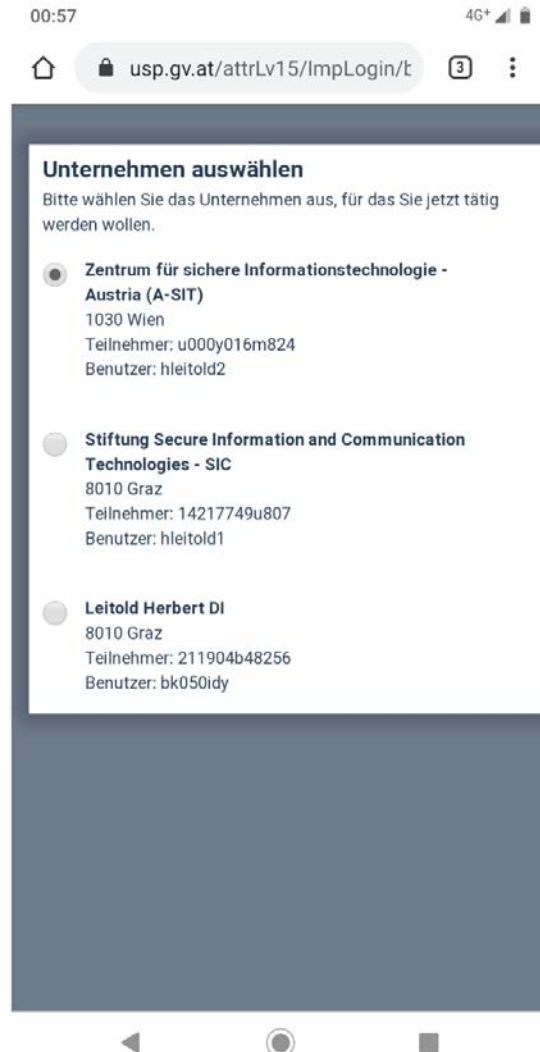
6. Erhaltene Beiträge als Leistungsverpflichteter gem. § 9 TDBG 2012

Leitold Herbert, letztes Login am 30.09.2019 00:45:38 Uhr

Österreichische Datenschutzbehörde

- Overview of income and all transfer payments

Example Business Service Portal

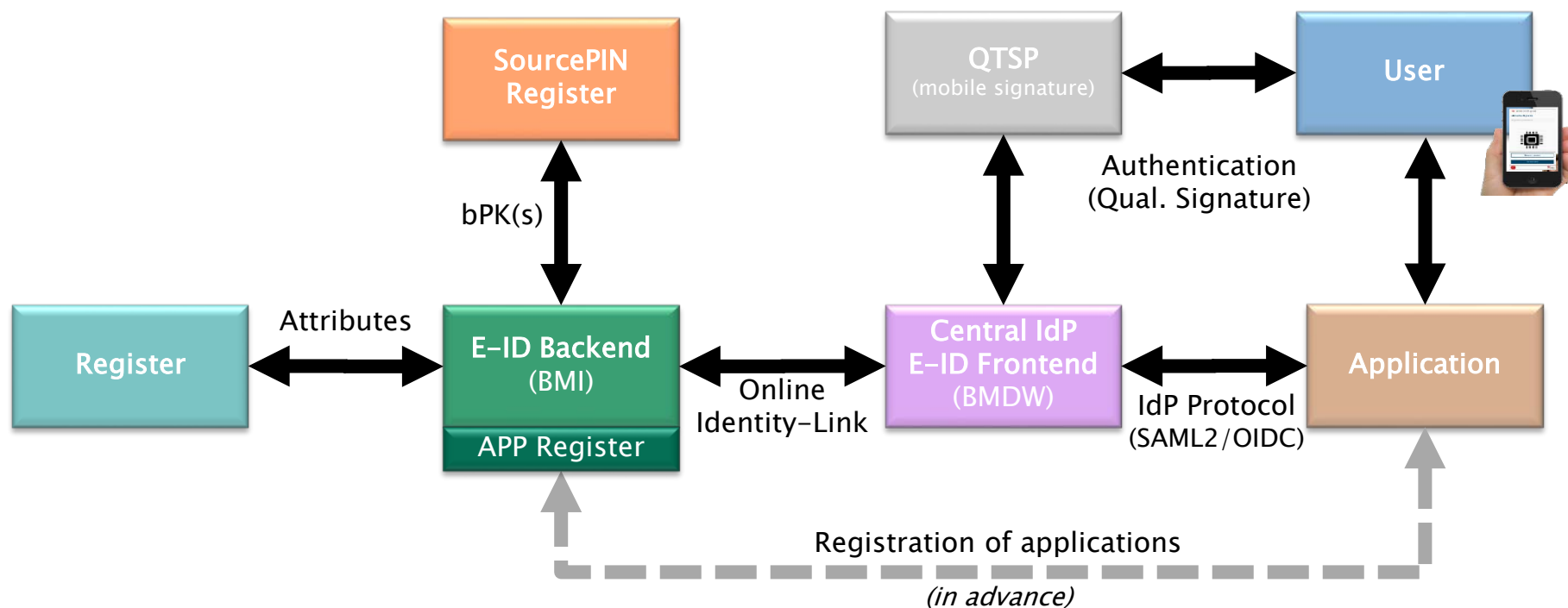


- Example of representation

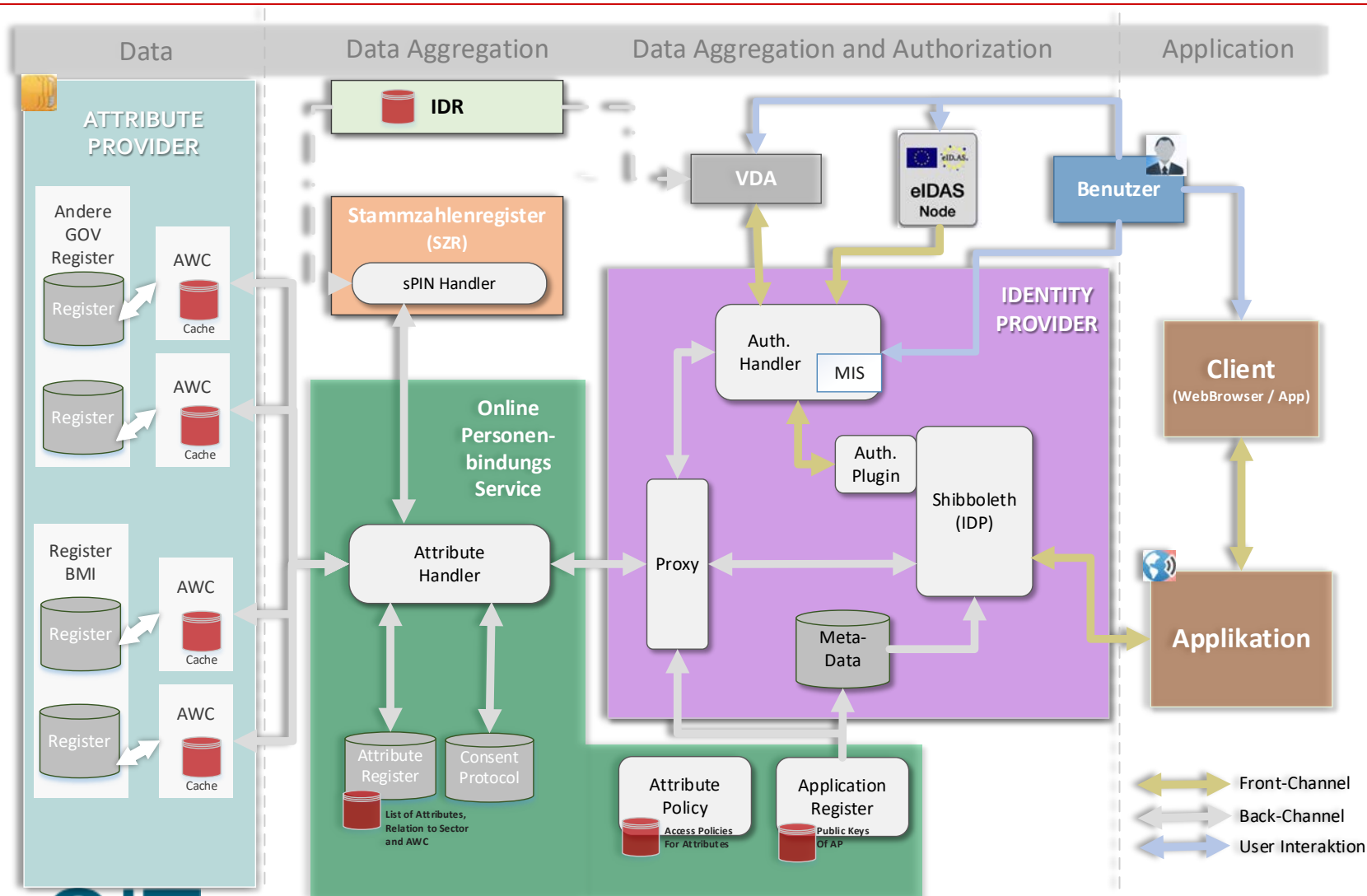
New E-ID: Core Concept (from 2020)

- De-coupling of IdP and QTSP
 - Ministry operates central interface
 - Interface with QTSP
- (Future) Integration of attribute providers
- SPs no longer needs special middleware
 - SAML2 or OIDC interfaces
- F2F registration only (with online renewal)
- Registration of applications

New E-ID: high-level architecture

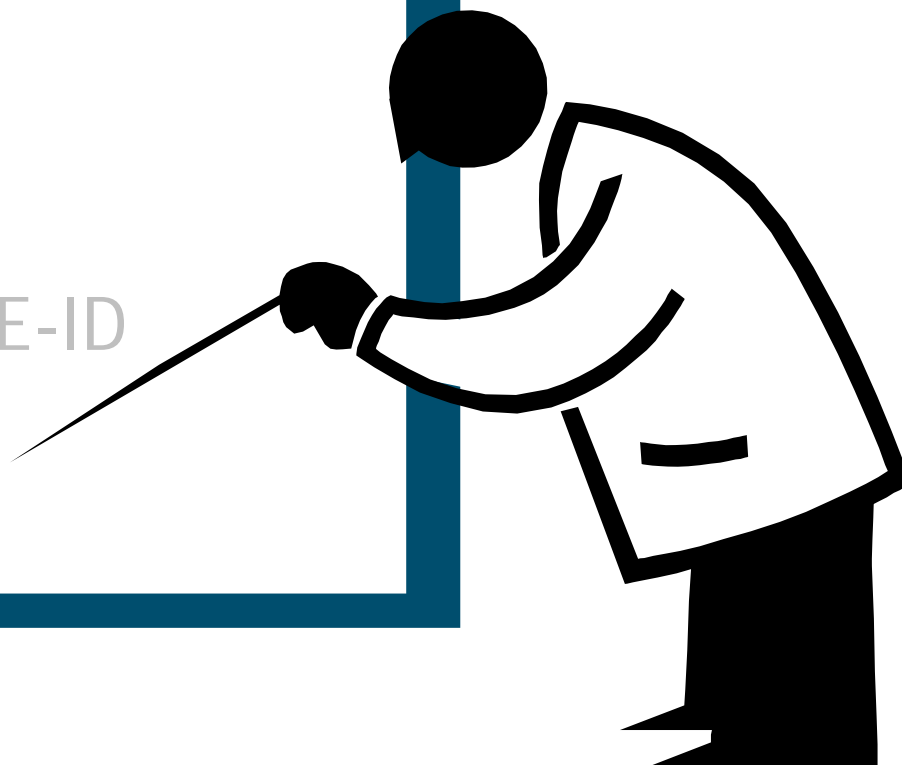


New E-ID: Detailed Architecture



Contents

- Some History
- Technology
- Mobile-First, New E-ID
- **Conclusions**

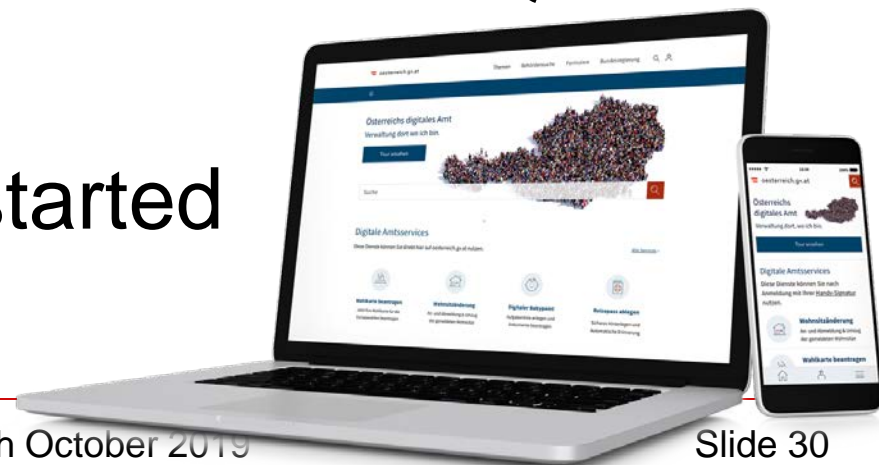


Some challenges

- Mobile asks for re-thinking the service
 - Avoid using forms, use registers and once-only
- Mobile gives paradigm shifts
 - Transaction-based, not session-oriented
 - Strategy to keep authentication / re-authenticate
 - 3rd party app integration, app-app communic.
- But mobile brings major security advantages
 - Sandboxing, SE/TEE, app permissions, ...

Summary

- Austrian eID programme started in 2005
 - Sector-specific identifiers, qSig, representation
- Satisfactory take-up only with mobile ID
 - Launched 2010 through STORK
 - Based on remote QSCD
- New E-ID only mobile-ID & remote QSCD
 - Starting Q2 2020
- Mobile first approach started



Thank You for
Your Attention!



Workshop with Slovenia,
Ljubljana, 29th October 2019

Herbert.Leitold@a-sit.at