Remote-QSCD: Solutions, Certification, and Use

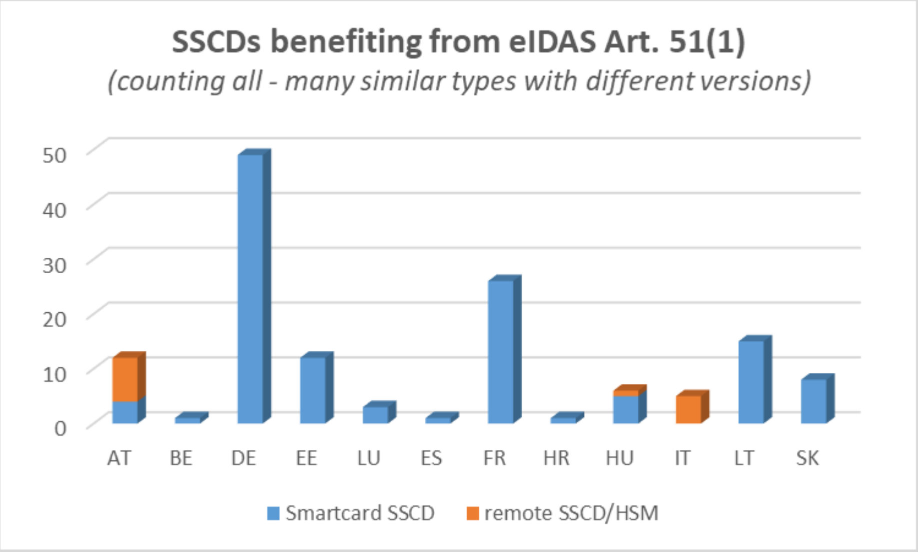
Herbert.Leitold@a-sit.at

SmartCard Workshop,
Darmstadt – February 21st, 2019

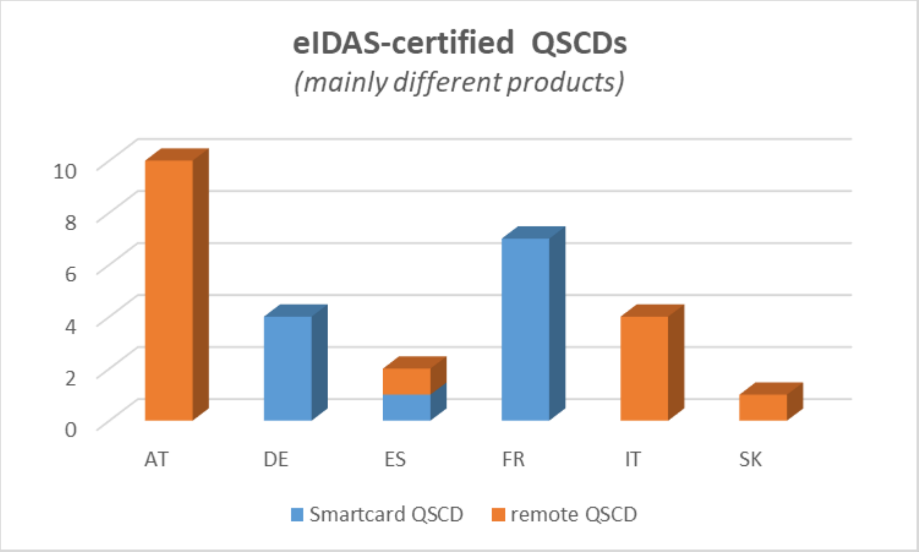
A-SIT
Zentrum für sichere Informationstechnologie - Austria
Secure Information Technology Center - Austria

Motivation (I/II)

- Remote QSCDs increased significantly with eIDAS
  - SSCDs/QSCDs counted by certification body‘s country



SSCDs benefiting from eIDAS Art. 51(1)
(counting all - many similar types with different versions)



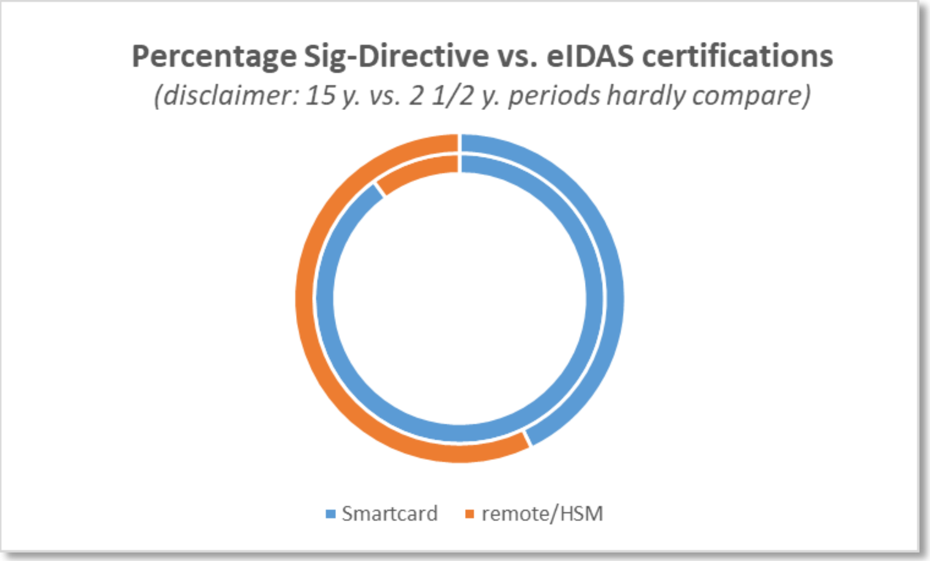
eIDAS-certified QSCDs
(mainly different products)

Counted from : https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds , version 5 Feb. 2019
(*note: counting each SSCD/QSCD listed, even if many are similar components in different mask/OS versions)*

Motivation (II/II)

- … in total numbers for EU/EEA

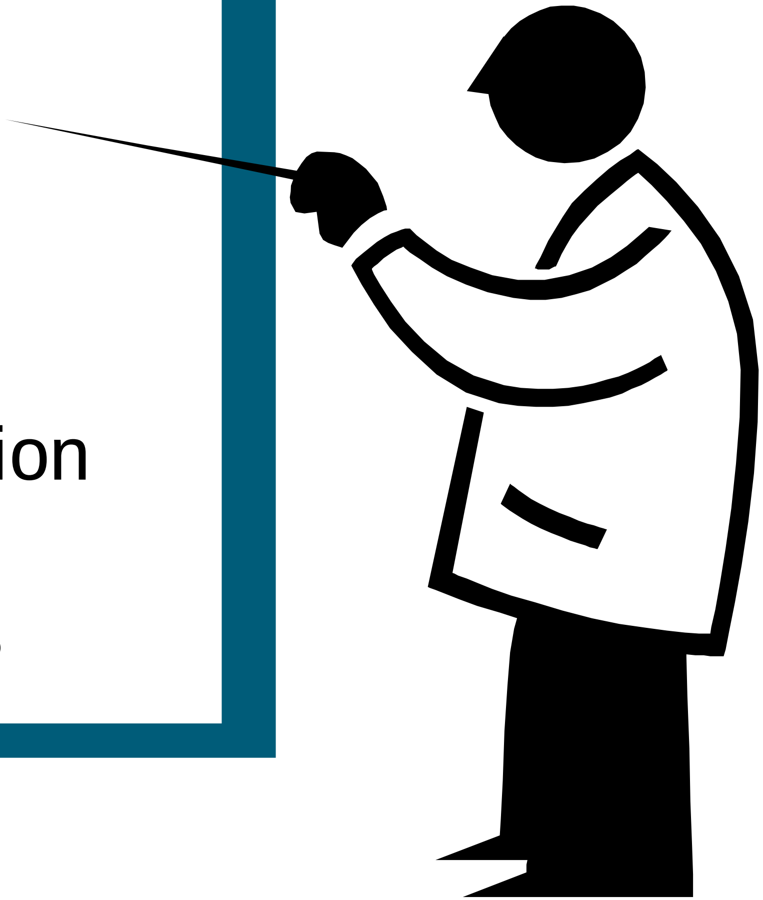
	SmartCard	Remote/HSM
Sig.-Dir SSCD *(eIDAS §51(1) transition)*	125 (56)	14 (9)
eIDAS QSCD	12 (12)	16 (15)



Counted from : https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds , version 5 Feb. 2019
(note: counting each SSCD/QSCD listed, even if many are similar components in different versions. Some clustering given in brackets)

Contents

- Environment in Austria
- Sig-Directive vs. eIDAS
- Remote-QSCD certification
- Experience, Conclusions



My/Our role on eSignature Certification

- Accredited Conformity Assessment Body
  - Assess eIDAS qualified trust service providers
- Notified body
  - Signature Directive art. 3(4) (SSCD certification)
  - eIDAS art. 30(1) (QSCD certification)
- eIDAS expert group & technical subgroups
- Standardisation: SSCD-PP

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

The technologies

Smartcard

Bank cards
SSCD from 2005; ceased

Health insurance card
SSCD/QSCD since 2005

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

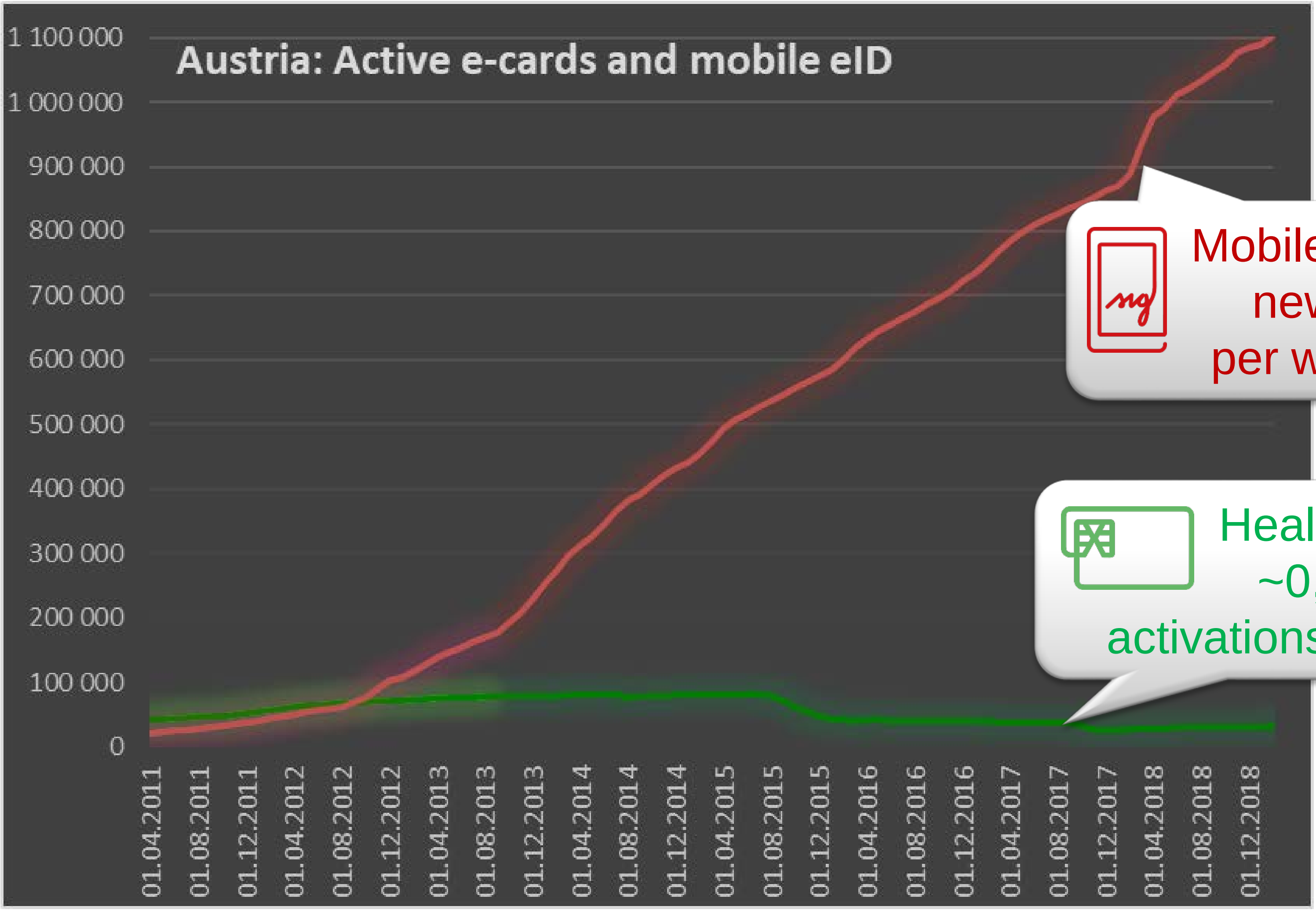
Mobile

A1 signature
service by a MNO from 2005 (no SSCD); ceased 2008, limited success

Mobile phone signature
Launched as QSCD end of 2009 through LSP STORK
Contracted by gvmnt. to a private sector QTSP

Success? Well, let's see ...

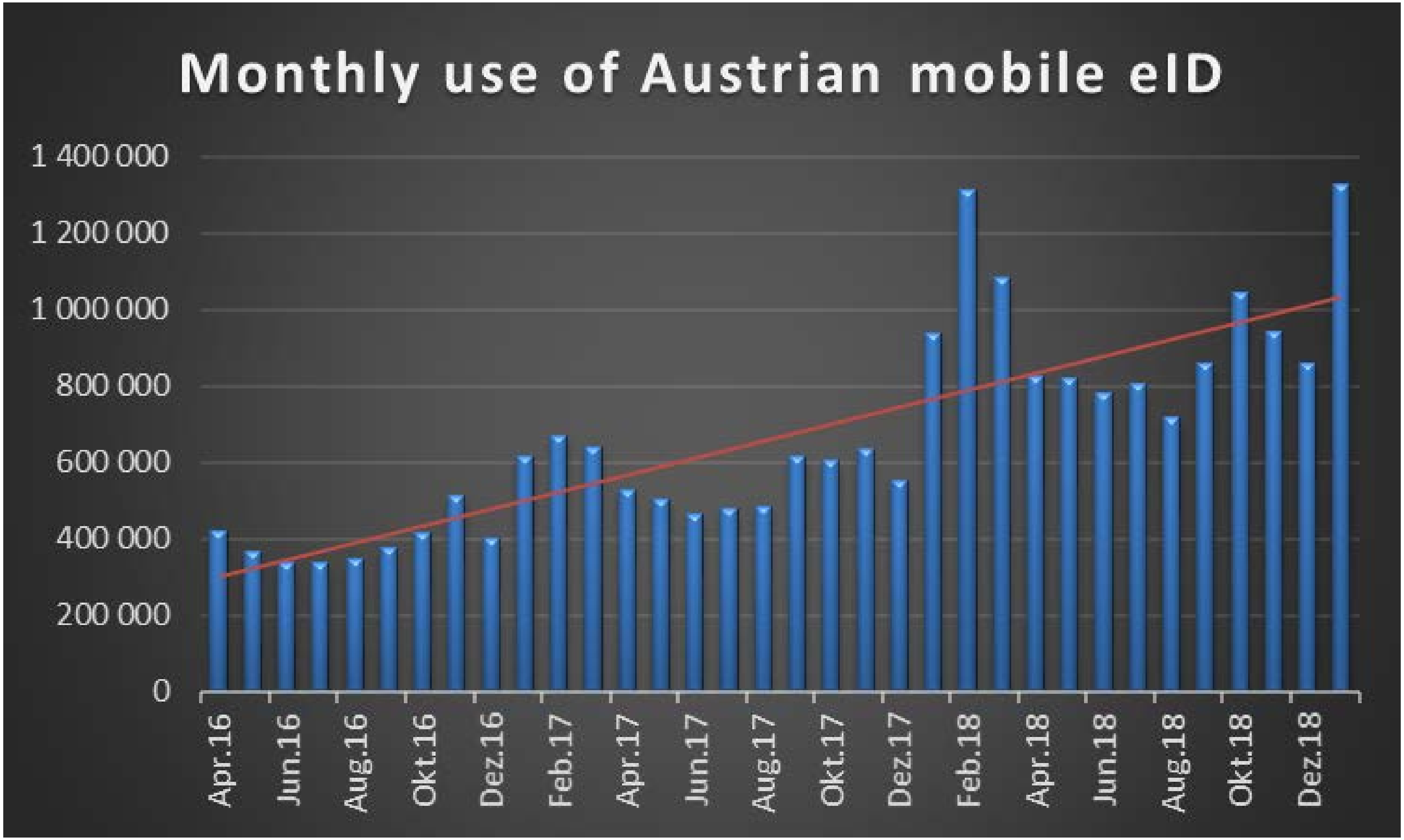
Austria: Card vs mobile ID active users



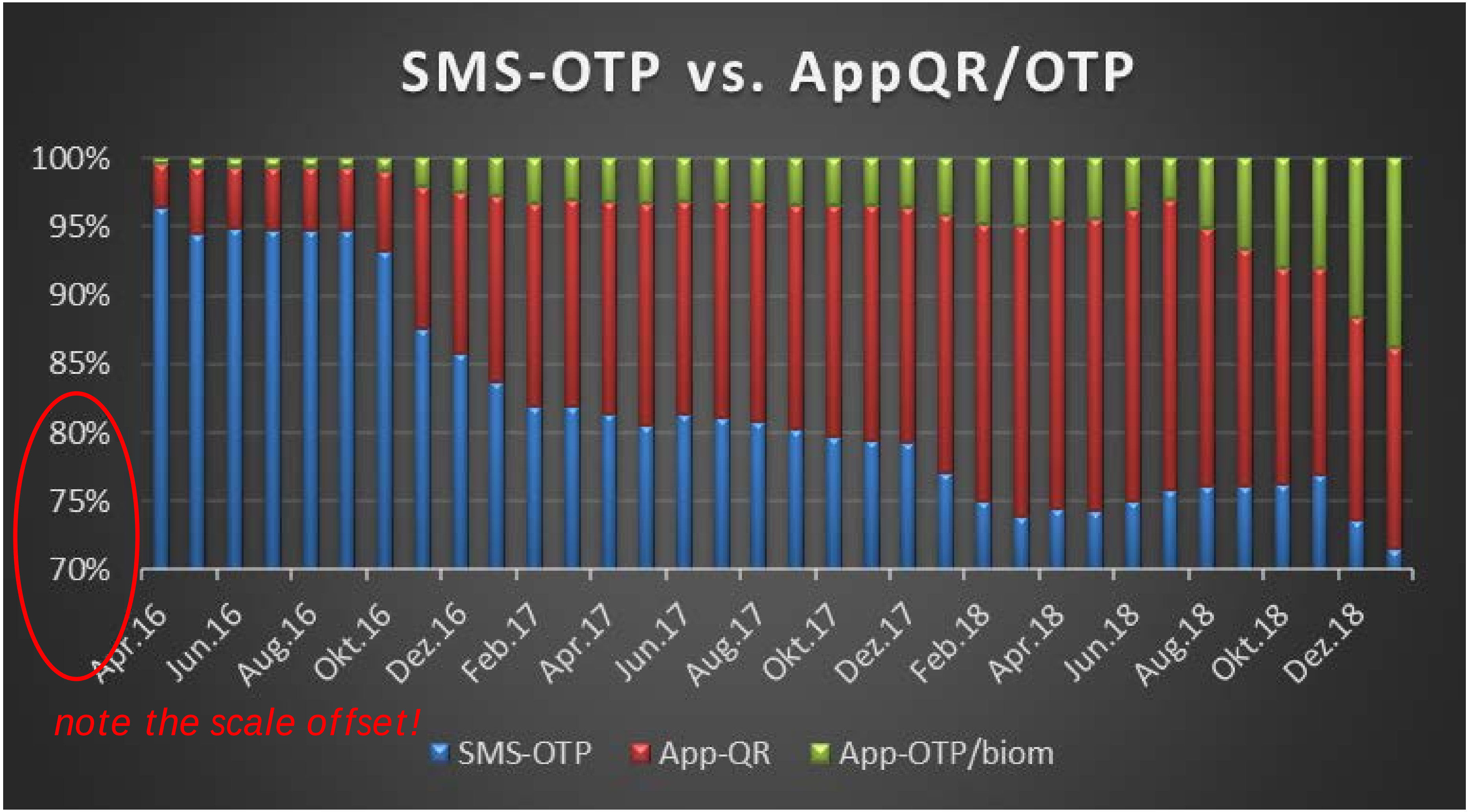
MobileID >1k new users per workday

Health card, ~0,4 k eID activations/month

Austria: Remote signature monthly use



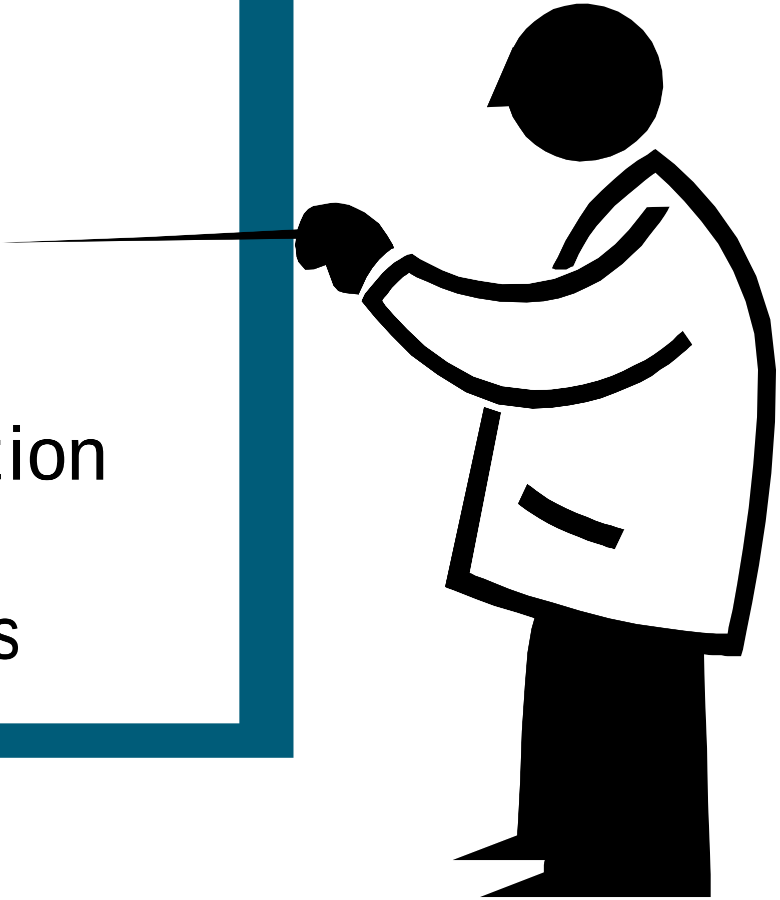
Austria: rem.Sig. authorisation options



note the scale offset!

Contents

- Environment in Austria
- **Sig-Directive vs. eIDAS**
- Remote-QSCD certification
- Experience, Conclusions



Qualified electronic signature

- A QES needs
  - an advanced electronic signature
    - functions digital signatures usually provide plus
    - requirement of "*sole control by signatory*"
  - a secure / qualified device (SSCD / QSCD)
    - certification by designated bodies
  - a qualified public key certificate
    - provided by a qualified trust service provider

Sole control requirement

- Source of dispute (confusion) with the Signature Directive
  - Does *sole control* mean *physical possession*?
    - “no” acc. to
      - EESSI SSCD-PP Guidelines 2004
      - FESA 2005 (dissenting note by German supervisory body)
      - Austrian legislator (Signature Act amendment 2007)
    - “yes” acc. to
      - some other laws, some expert opinions
  - Conclusively settled by eIDAS (“no”)
    - But requires QSCD operation by qualified TSP!

SSCD / QSCD Certification

Signature Directive

- MS-designated body
- Reference numbers as „maximum standard"
  - SSCD-PP: Gave certainty on meeting requirements, MS could not set higher, mandatory requirements
  - A designated body could still certify against national standards or Annex III

eIDAS Regulation

- MS-designated body
- "Minimum standards", if listed in EC decision
  - Becomes mandatory
  - National certification only, if no standard listed (or ongoing certification)
- Decision 2016/650
  - Common Criteria PPs for smartcard-like devices
  - No standards for remote QSCDs, alternative certif.

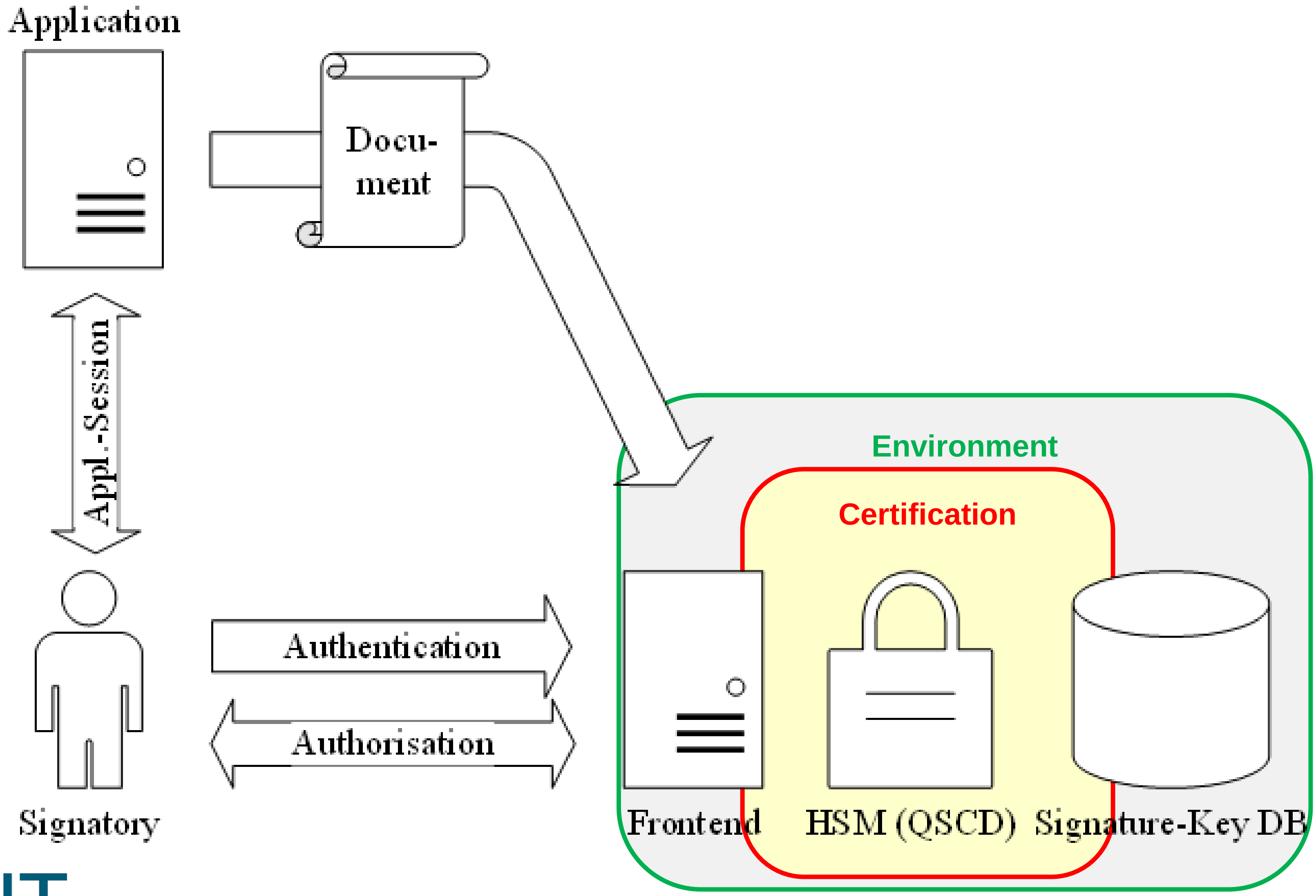
Contents

- Environment in Austria
- Sig-Directive vs. eIDAS
- **Remote-QSCD certification**
- Experience, Conclusions

A-SIT remote QSCD certifications, so far

- A-Trust „Handy-Signatur“ (AT)
- PrimeSign Remote Signing-Device (AT)
- SwissCom All-In Signing Service (AT)
- LuxTrust Qualified Remote Signing Server (LU)
- DocuSign Protect&Sign (FR)
- AliasLab CryptoAccelerator (IT)
- Intesi PkBox (IT)
- Cryptomathic Signer (DK)
- SafeLayer TrustedX eIDAS (ES)

Common architecture



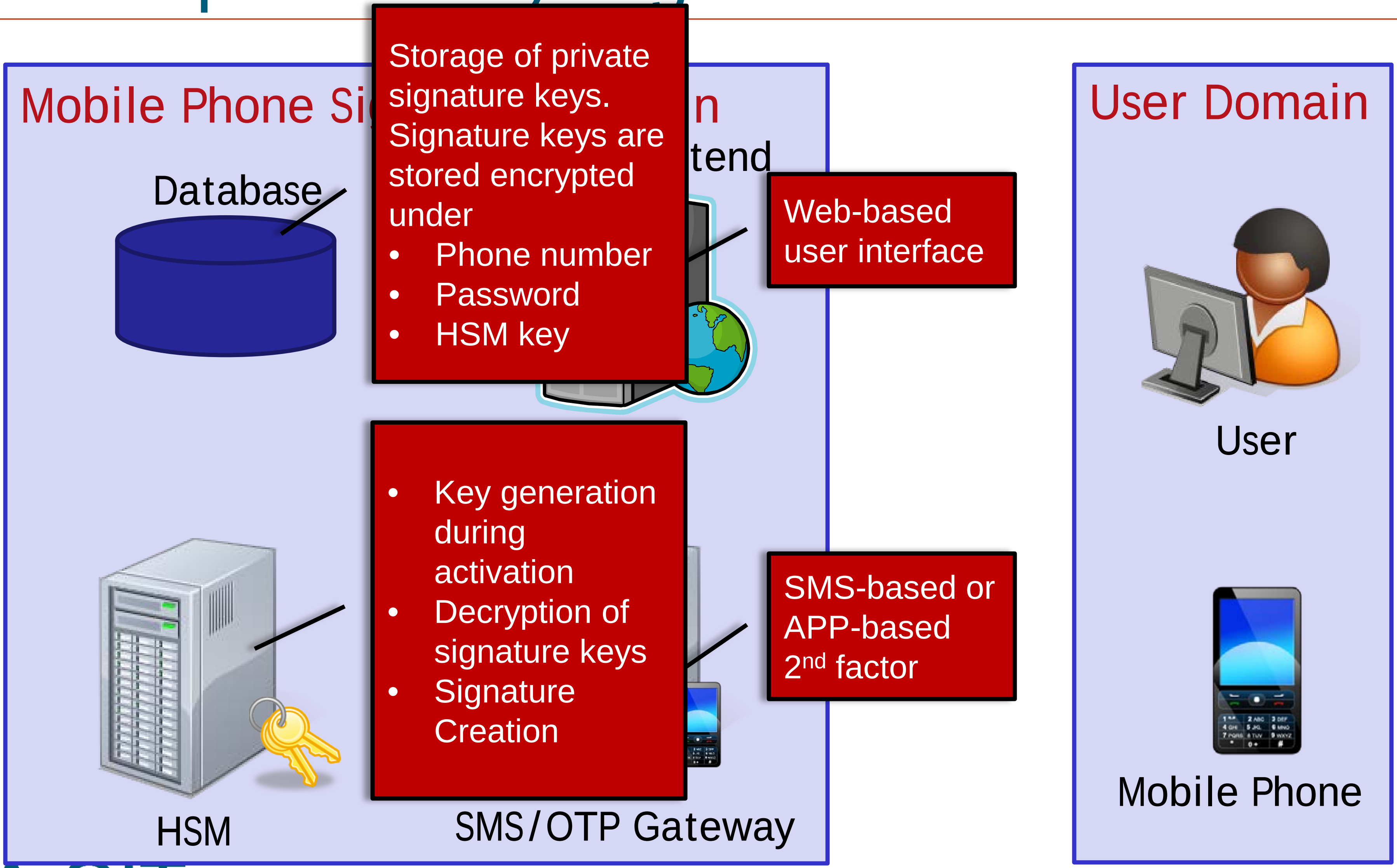
Approaches followed by many QSCDs

- All use a HSM for core functions
  - In fact, we so far saw just two HSM types
  - Plus servers (signature format processing, etc.)
- User- and device-binding through crypto
  - Username/mobile-number and User-password part of signing-key encryption or HSM verified
  - Plus HSM key
- Authorisation challenge / OTP
  - Created and verified by HSM

Variants by some remote QSCDs

- Different OTP solutions
  - – SMS-OTP, OTP tokens
  - – Smartphone Apps
    - e.g., QR code to enforce two-device approach
    - TEE/SE for single device, biometrics as convenience
- Delegated authentication
  - – EN 419241 *SCAL2* / LoA high to authorize sig.
- Short-time keys
  - – New key/cert. for each sig. (no encrypted export)

Example “Handy-Signatur”: Architecture



Storage of private signature keys. Signature keys are stored encrypted under

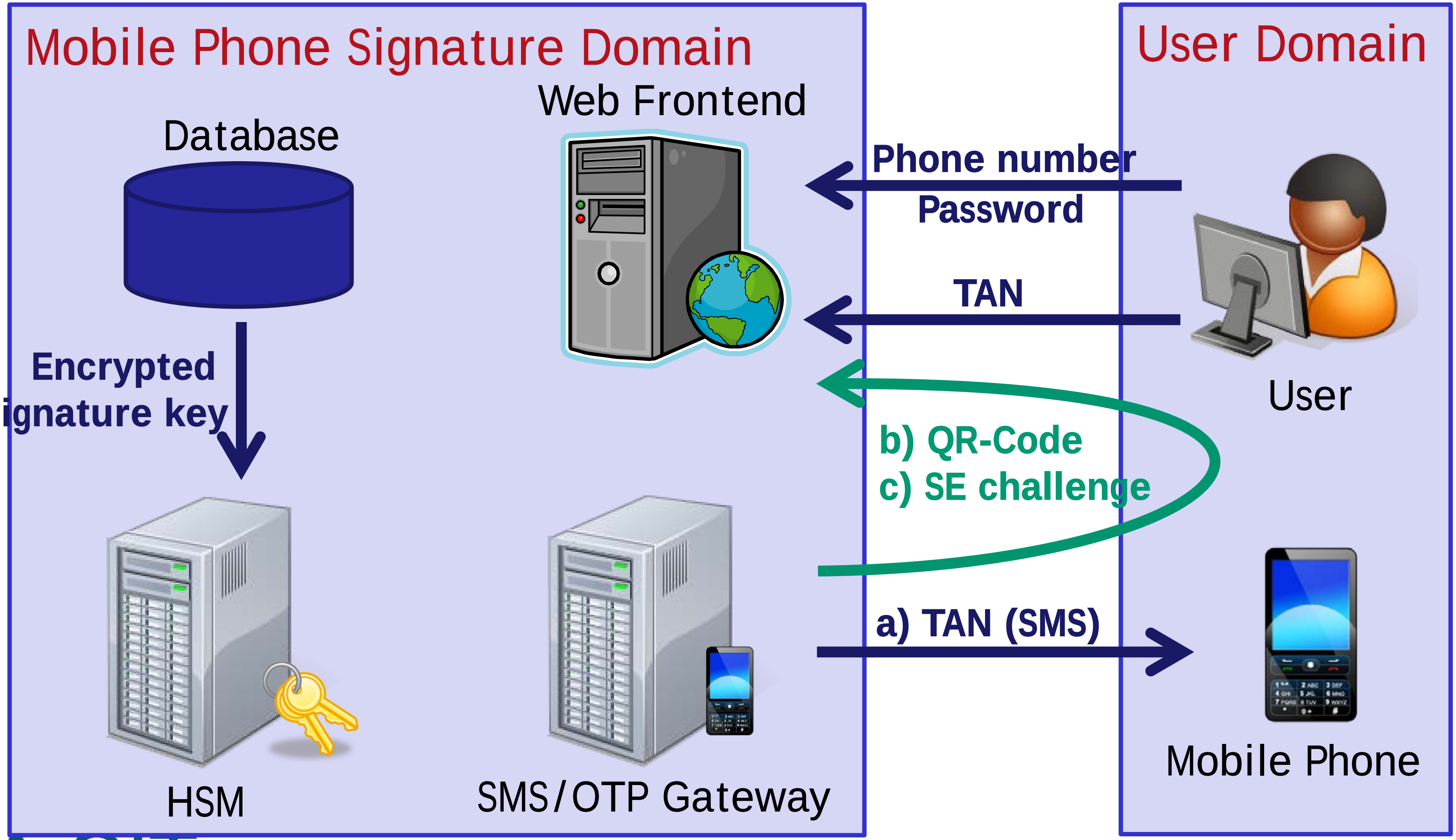
- Phone number
- Password
- HSM key

Web-based user interface

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

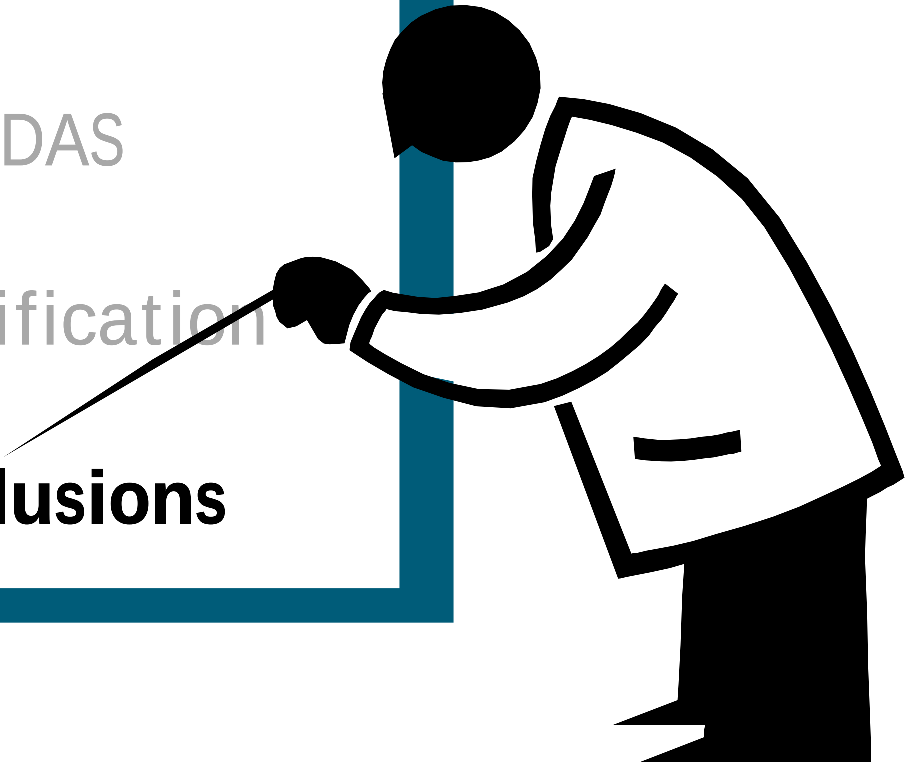
SMS-based or APP-based 2nd factor

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



Contents

- Environment in Austria
- Sig-Directive vs. eIDAS
- Remote-QSCD certification
- **Experience, Conclusions**



Experience, conclusions

- Emerging technology
  - – Providers change/amend (e.g. OTP methods)
  - – Needs some flexibility when certifying
- eIDAS “minimum standard” is a challenge
  - – Standards need to be mature and proven in practice, before mandating them
  - – Field does not yet have decades experience, like with smartcard certification or SSCD-PP
- Split in (EU) 2016/650 still sensible

Thank You for Listening!

Herbert.Leitold@a-sit.at

SmartCard Workshop,
Darmstadt – February 21st, 2019

A-SIT

Zentrum für sichere Informationstechnologie - Austria
Secure Information Technology Center - Austria