VZDÁLENÝ ELEKTRONICKÝ PODPIS

Jan Tejchman | senior konzultant | FTSB |
jan.tejchman@ftsb.cz


architektura
ECM
CMS
digitální
TSA
HSM
ZFO
PEPS
PKCS
dokumenty
token
důvěra
doručování
biometrie
procesy
CAdES
XAdES
B2C
certifikát
PKI
NIA
eID
ISDS
PAdES
ETSI
eIDAS
EU
standardy
klíč
ověření
razítko
podpis
CRL
dostupnost
normy
CA
archivace
identifikace
pečeť
B2B DMS
služby
AIP
PDF
OCSP
paperless
integrita
eOP

PROČ VŮBEC ELEKTRONICKÝ PODPIS?

Protože chceme a **můžeme** fungovat elektronicky!

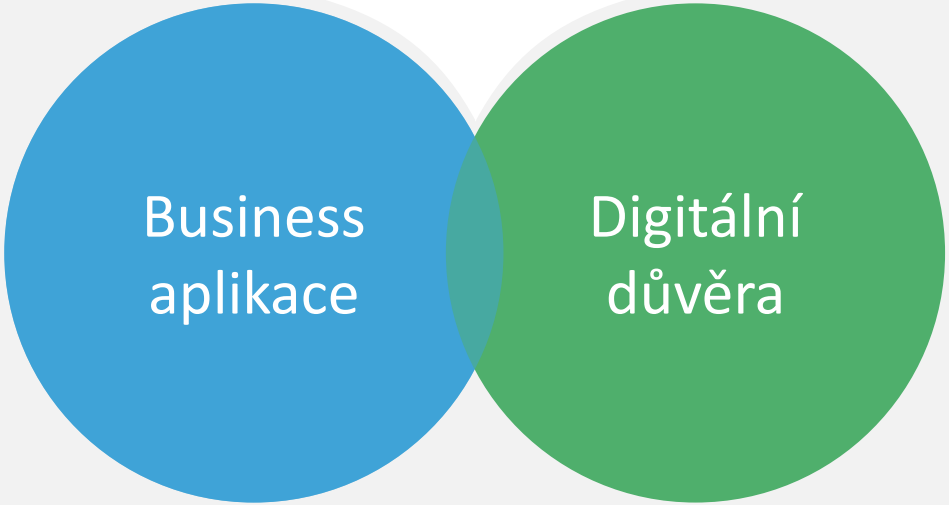
Digitální Evropa

Digitální transformace

Elektronické dokumenty

Právní validita

Služby vytvářející důvěru



CÍL = DŮVĚRYHODNÝ ELEKTRONICKÝ DOKUMENT

Dle nařízení eIDAS

Papírový dokument

=

Elektronický dokument

El. podpis

El. pečeť

Čas. razítko

- El. dokumentu nesmějí být upírány právní účinky jen proto, že je elektronický
- Kvalifikovaný el. podpis má stejnou váhu jako podpis vlastnoruční

DŮVĚRYHODNÝ ELEKTRONICKÝ DOKUMENT

Základní požadavky

Jedná se o originální (primární) dokument

Lze určit původ dokumentu

Lze ověřit, že nedošlo ke změně obsahu

Lze doložit shodu s originálem

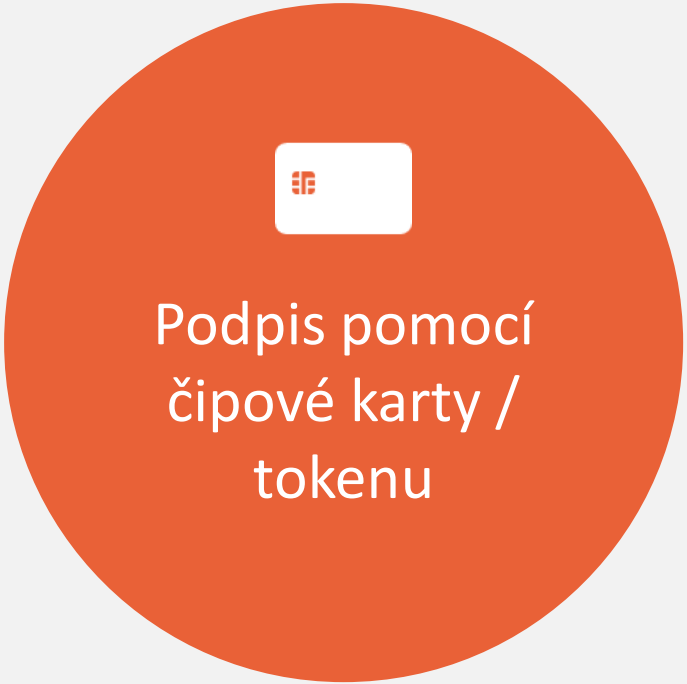
Lze prokázat existenci dokumentu v čase

Lze nezávisle ověřit důvěryhodnost dokumentu

ELEKTRONICKÝ PODPIS JAKO SLUŽBA

ELEKTRONICKÝ PODPIS

Způsoby elektronického podepisování



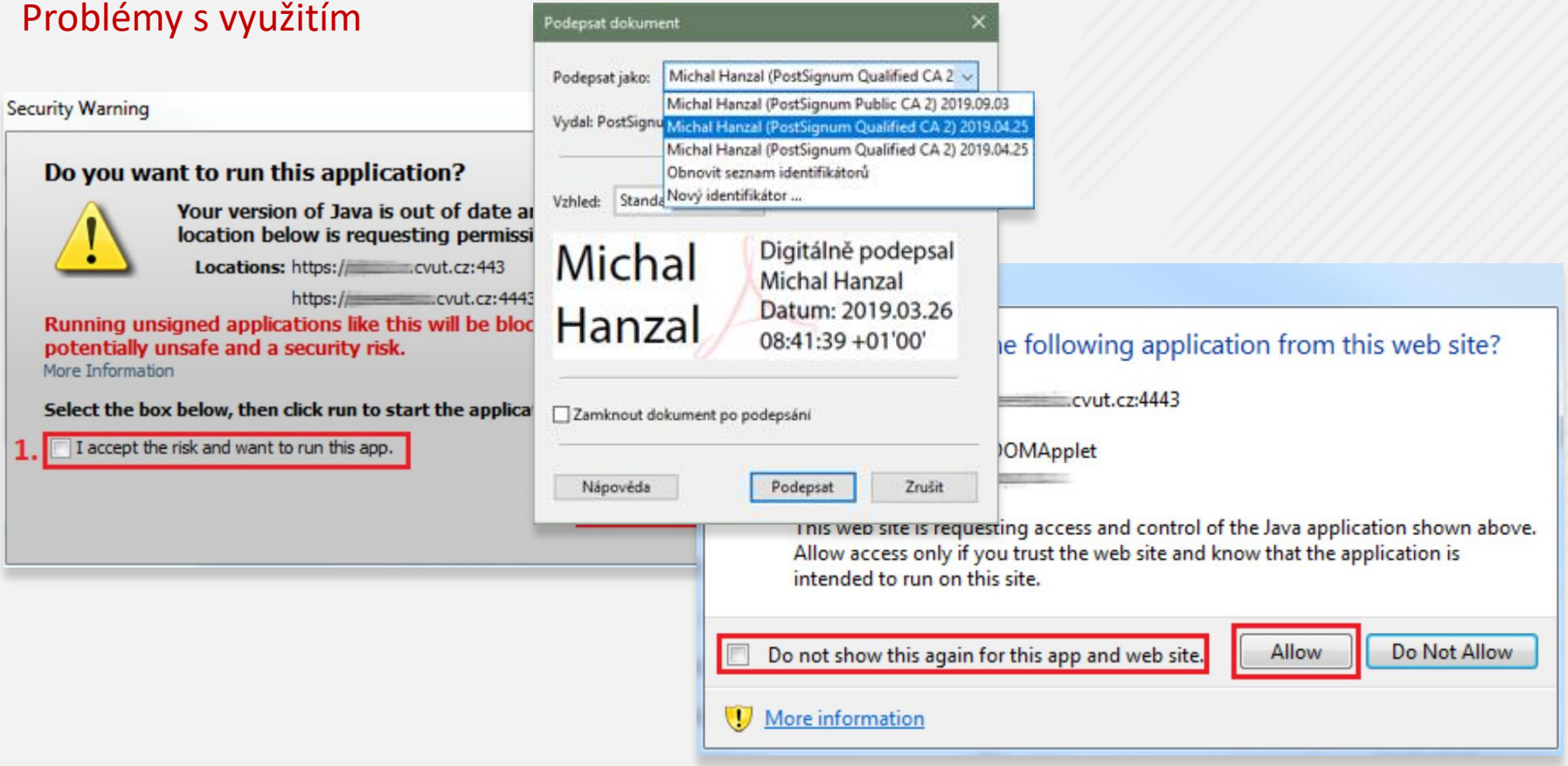
TYPICKÉ POŽADAVKY NA PODEPISOVACÍ KOMPONENTU

Klientské podepisování

- ✔ SW řešení musí být plně integrované do webového prohlížeče MSIE, CHROME, FIREFOX
- ✔ SW řešení vytváří podpis do pole v HTML formuláři na základě dat v poli v HTML formuláři
- ✔ SW řešení umí podpis souboru na disku
- ✔ SW řešení pracuje s certifikáty v úložišti Windows a v úložišti čipové karty
- ✔ SW řešení vytváří podpis dle požadavků legislativy (eIDAS) – formáty XAdES, PAdES, CAdES
- ✔ SW řešení může být provozováno v OS Windows a UNIX

ELEKTRONICKÝ PODPIS POMOCÍ ČIPOVÉ KARTY / TOKENU

Problémy s využitím



ELEKTRONICKÝ PODPIS POMOCÍ ČIPOVÉ KARTY / TOKENU

Problémy s využitím podpisu na koncovém zařízení uživatele

vyžaduje čtečku karet
USB pro token

vyžaduje SW
a příslušné ovladače

kompatibilita
prohlížečů

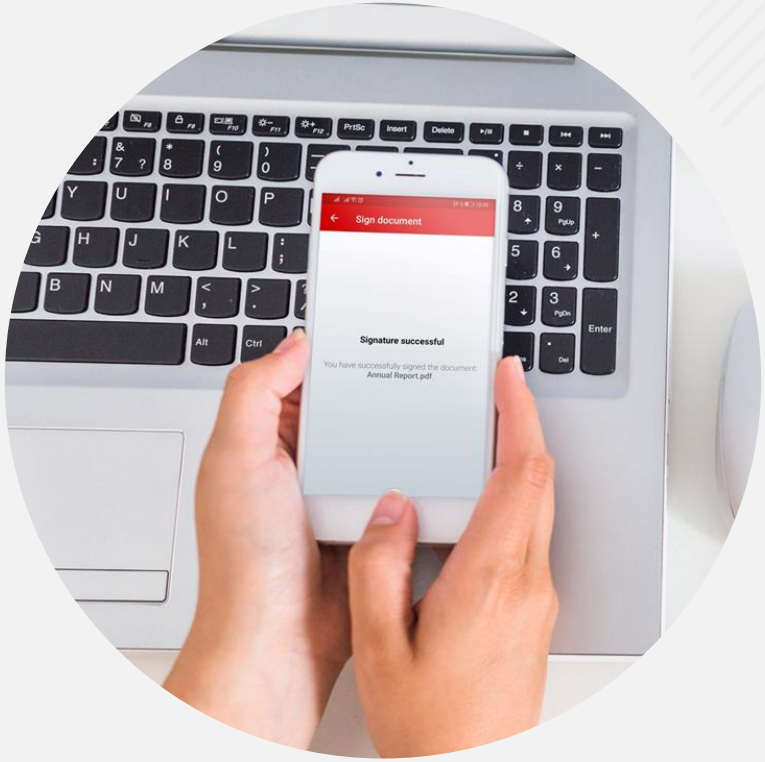
podpis na mobilních
zařízeních

ztráta čipové
karty

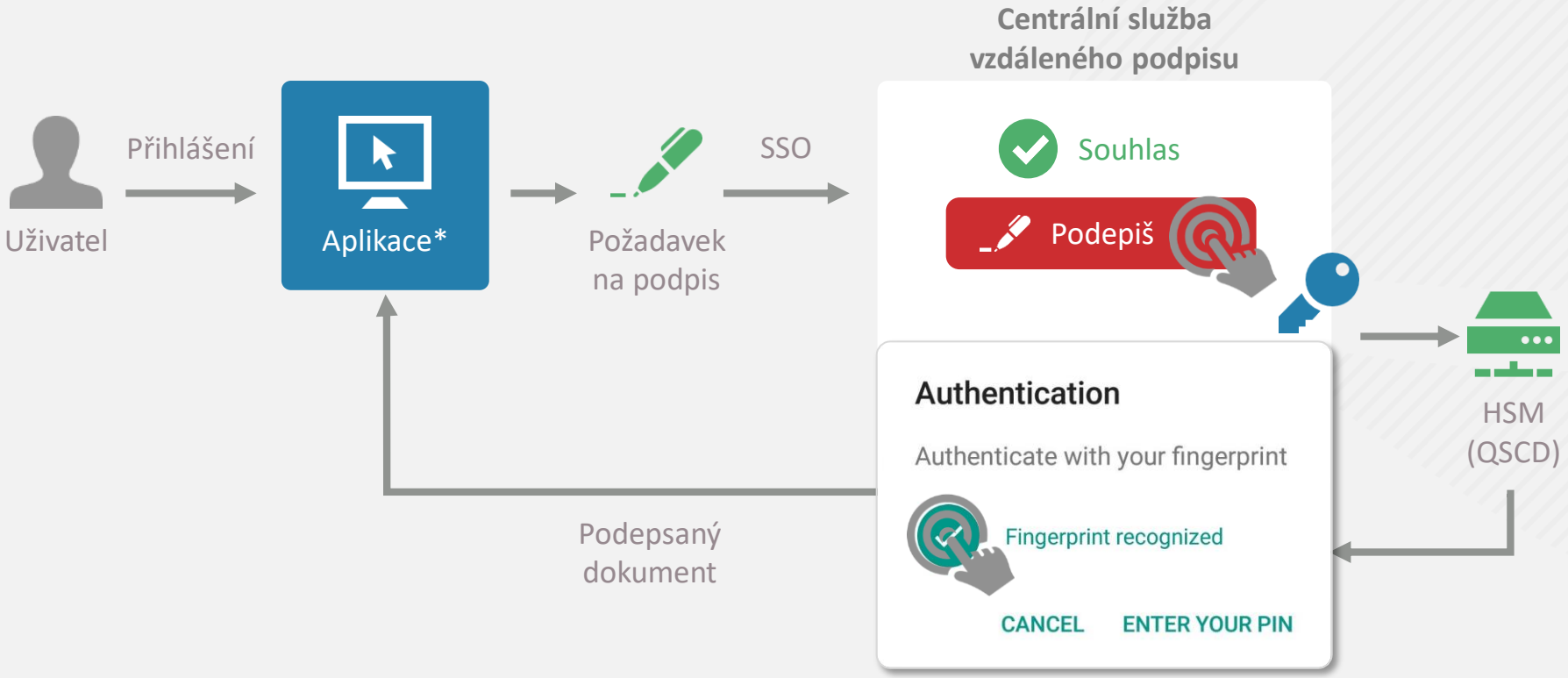
možnost jednoduchého
„zapůjčení“

ELEKTRONICKÝ PODPIS JAKO SLUŽBA

Až takto jednoduché to může být

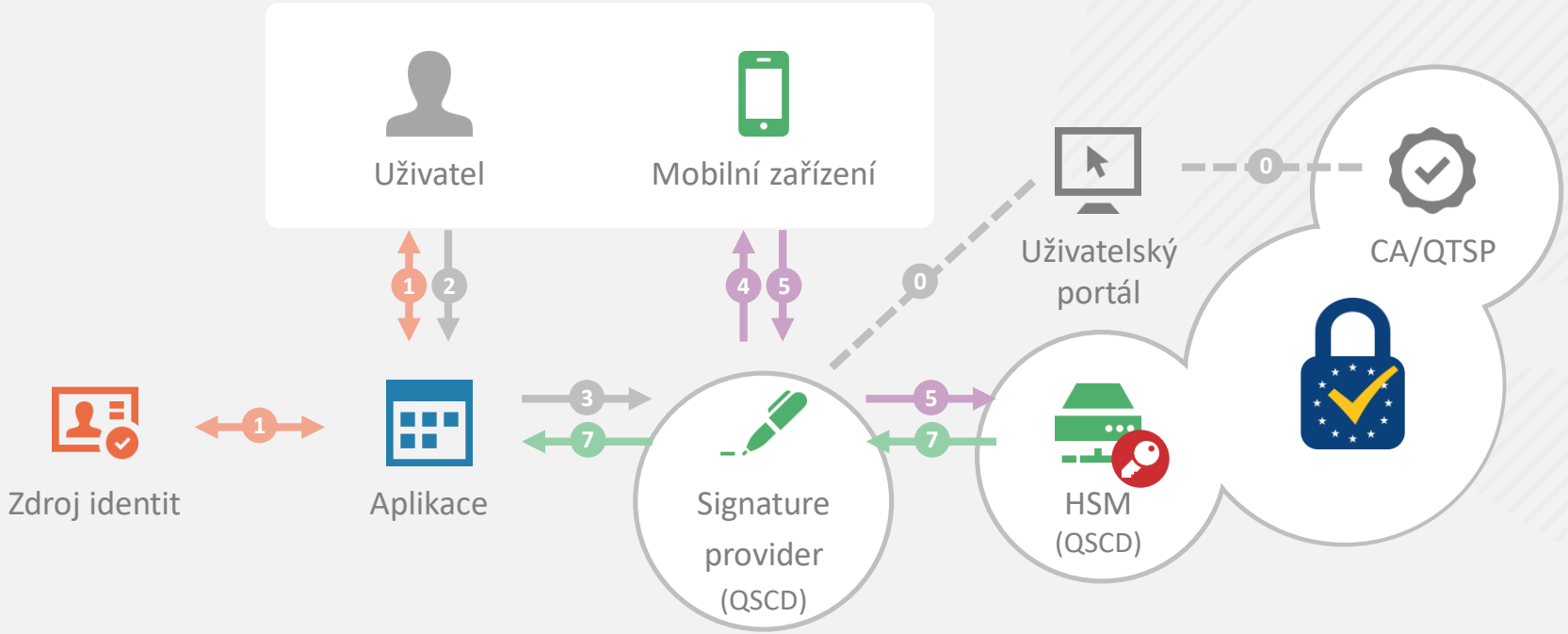


ELEKTRONICKÝ PODPIS JAKO SLUŽBA



** Univerzální aplikace pro všechny PC/mobilní platformy nezávislá na OS, web prohlížeči či aplikačním toolkitu*

ELEKTRONICKÝ PODPIS JAKO SLUŽBA



0 Zajištění certifikátu
1 Přihlášení do aplikace
2 Vyžádání podepsání
3 Zahájení procesu podepisování
4 Požadavek na autorizaci podepsání
5 Aktivace a použití soukromého klíče v HSM
6 Vygenerování el. podpisu v HSM
7 Vytvoření el. podepsaného dokumentu a jeho předání aplikaci

ELEKTRONICKÝ PODPIS

Srovnání

Podpis pomocí čipové karty/tokenu

Podpis na koncovém zařízení uživatele

- vyžaduje čtečku karet, USB pro token, …
- vyžaduje příslušné ovladače a SW
- problém s kompatibilitou prohlížečů
- problém s podpisem na mobilních zařízeních
- problém s životností karet a jejich ztrátou
- možnost jednoduchého „zapůjčení“

Podpis jako služba pomocí HSM modulu

Podpis v rámci bezpečné infrastruktury

- podpis vytvořen v HSM modulu ***(QSCD)***
- pro libovolné koncové zařízení ***(PC, mobil, tablet)***
- uživatelská přívětivost jako internet banking
- využití moderních funkcí smartphonu
- integrace se správou identit (IAM)
- podpora silné autentizace
- až do úrovně kvalifikovaného el. podpisu

STANDARDY PRO ELEKTRONICKÝ PODPIS/PEČEŤ

ETSI EN 319 401: General Policy Requirements for Trust Service Providers

Certificates

ETSI EN 319 411: Policy and Security Requirements for Trust Service Providers issuing Certificates

CEN TS 419 261: Security Requirements for Trustworthy Systems Managing Certificates and Time-Stamps

ETSI EN 319 412: Profiles for Trust Service Providers issuing Certificates

- **ETSI EN 319 412-1**: Overview and common data structures
- **ETSI EN 319 412-2**: Certificates issued to natural persons
- **ETSI EN 319 412-3**: Certificates issued to legal persons
- **ETSI EN 319 412-4**: Web site certificates issued to org.
- **ETSI EN 319 412-5**: QC Statements

CEN EN 419 221: Protection Profiles for TSP cryptographic modules

Time-Stamps

ETSI EN 319 421: Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

CEN TS 419 261: Security Requirements for Trustworthy Systems Managing Certificates and Time-Stamps

ETSI EN 319 422: Time-stamping protocol and time-stamp profiles

CEN EN 419 231: Protection Profiles for Trustworthy Systems supporting time stamping

CEN EN 419 221: Protection Profiles for TSP cryptographic modules

Signatures/Seals

CEN EN 419 241-1: General System Security Requirements

QSCD

- **CEN EN 419 241-2: Protection Profile for QSCD for Server Signing**
- **CEN EN 419 221-5**: Cryptohgraphic Modules for Trust Services

ETSI TS 119 612: Trusted Lists

ETSI EN 319 102: Procedures for Creation and Validation of AdES Digital Signatures

- **ETSI EN 319 122/TS103 173**: CAdES digital signatures
- **ETSI EN 319 132/TS103 171**: XAdES digital signatures
- **ETSI EN 319 142/TS103 172**: PAdES digital signatures

CEN EN 419 221: Protection Profiles for TSP cryptographic modules

ELEKTRONICKÝ PODPIS JAKO SLUŽBA

Hlavní přínosy

User experience

Kdekoli, kdykoli, na čemkoli

Kvalifikovaný podpis

Nasazení On Premise

Další využití HSM

Vyšší bezpečnost

PŘÍKLADY Z PRAXE

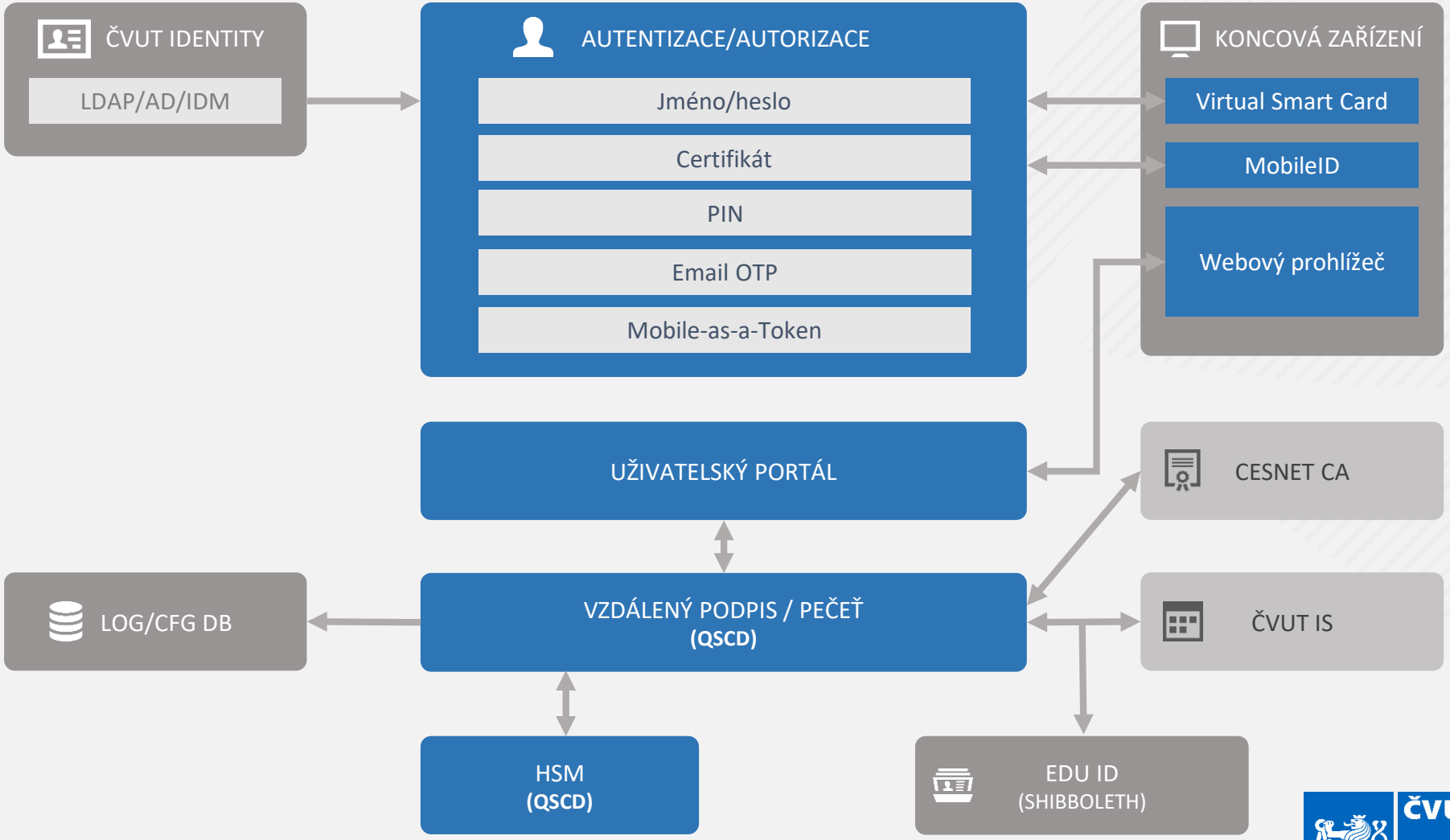
PROJEKT VZDÁLENÉHO PODEPISOVÁNÍ PRO ČVUT

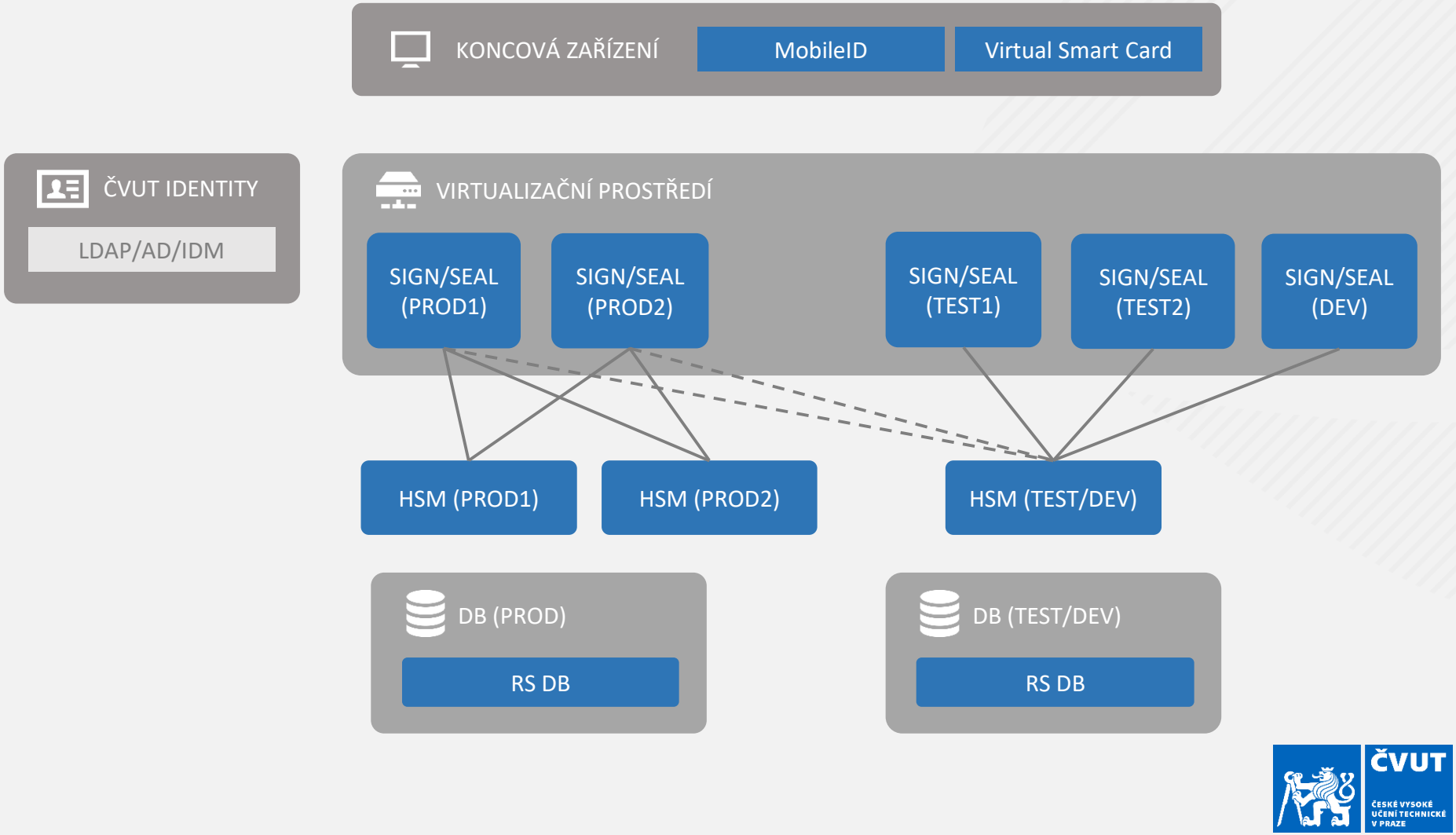
Případová studie

POŽADAVKY NA ŘEŠENÍ

Jak na to?

- ✔ Využití standardních dostupných řešení
  - ideálně s certifikací jako kvalifikovaný prostředek
- ✔ Uživatel nepotřebuje čipovou kartu nebo token
- ✔ Vzdálený podpis jako služba pro interní systémy
  - eliminace nebezpečných/nepraktických appletů
- ✔ Vzdálený podpis i pro lokální aplikace
  - bez nutnosti jejich změn – virtuální čipová karta

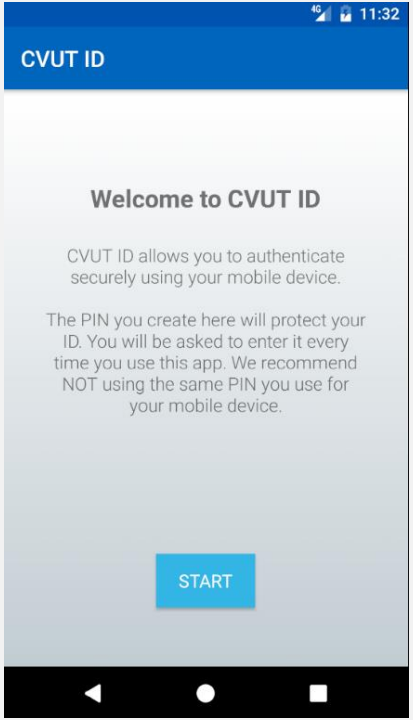

ČVUT IDENTITY
LDAP/AD/IDM
AUTENTIZACE/AUTORIZACE
Jméno/heslo
Certifikát
PIN
Email OTP
Mobile-as-a-Token
KONCOVÁ ZAŘÍZENÍ
Virtual Smart Card
MobileID
Webový prohlížeč
UŽIVATELSKÝ PORTÁL
CESNET CA
LOG/CFG DB
VZDÁLENÝ PODPIS / PEČEŤ
(QSCD)
ČVUT IS
HSM
(QSCD)
EDU ID
(SHIBBOLETH)


KONCOVÁ ZAŘÍZENÍ
MobileID
Virtual Smart Card
ČVUT IDENTITY
LDAP/AD/IDM
VIRTUALIZAČNÍ PROSTŘEDÍ
SIGN/SEAL (PROD1)
SIGN/SEAL (PROD2)
SIGN/SEAL (TEST1)
SIGN/SEAL (TEST2)
SIGN/SEAL (DEV)
HSM (PROD1)
HSM (PROD2)
HSM (TEST/DEV)
DB (PROD)
RS DB
DB (TEST/DEV)
RS DB

NASAZENÍ ELEKTRONICKÉHO PODPISU JAKO SLUŽBY

Bezpečná appliance pro identifikaci, autorizaci a služby vzdáleného el. podpisu

- ✔ Identifikace a autentizace
  - adaptivní autentizace, federace identit, OTP
  - podpora certifikátů, mobilní telefon jako token
  - SAML, OpenID Connect, OAuth 2.0
- ✔ Služby el. podpisu pro koncového uživatele (primárně pro interní uživatele)
  - služby vzdáleného podepisování, integrace s HSM moduly (kval. prostředky)
  - virtuální čipová karta *(pouze pro MS Windows)*
  - robustní autentizace pro povolení přístupu ke klíčům
  - AdES formáty a standardy dle nařízení eIDAS



ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Kooperativa

VIENNA INSURANCE GROUP

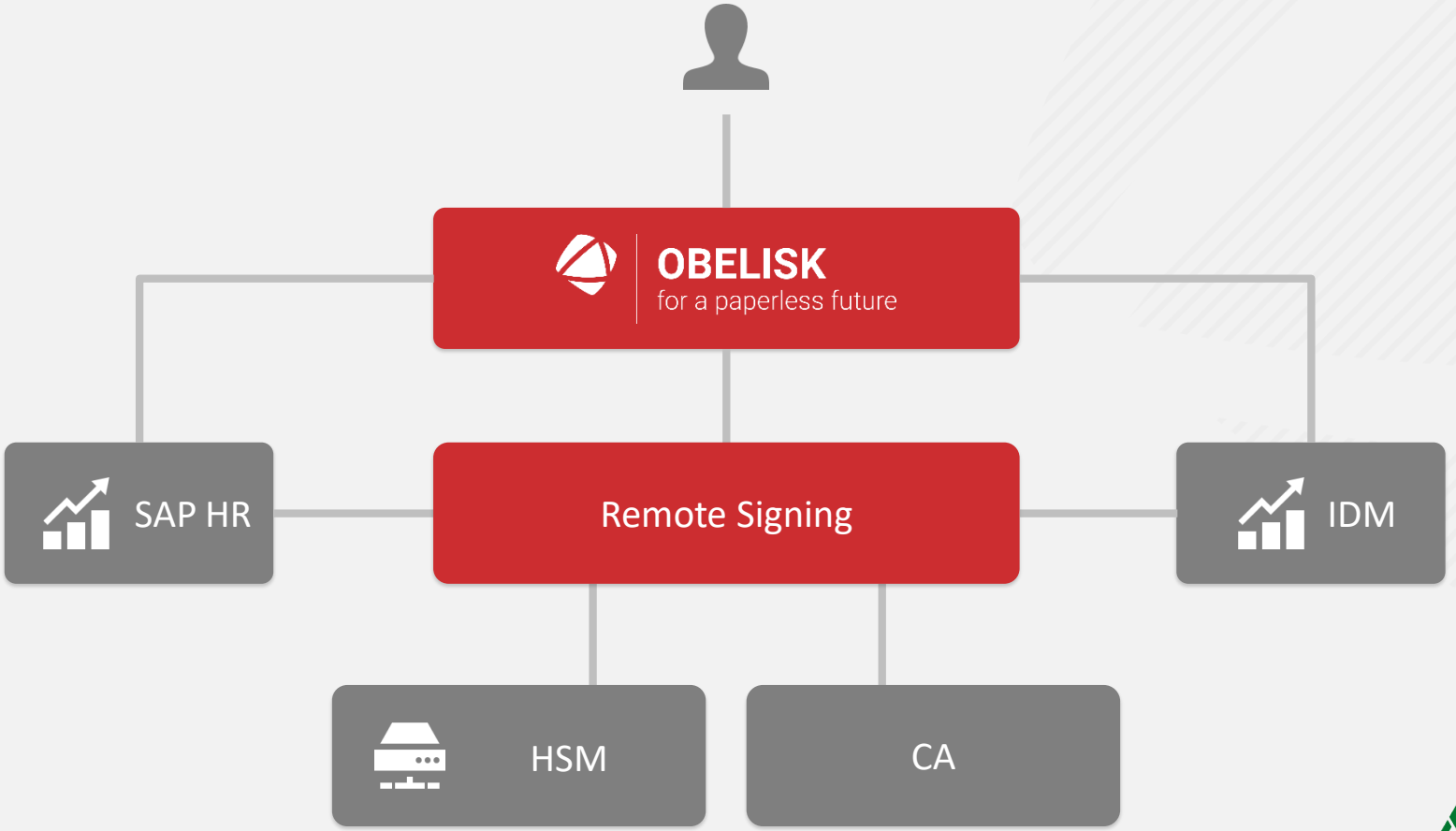
PROJEKT DIGITÁLNÍ TRANSFORMACE V HR

Případová studie

BEZPAPÍROVÁ PERSONALISTIKA

- Unikátní projekt v ČR
- Synergie existujících infrastrukturních a procesních prvků
- Podepisování zaměstnaneckých smluv pomocí biometrie / kval. certifikátů
- Podepisování interní dokumentace interními certifikáty

Kooperativa
VIENNA INSURANCE GROUP



Kooperativa
VIENNA INSURANCE GROUP

VÝHLED OD BUDOUCNA

- ✔ Rozšíření vzdáleného podepisování na další procesy
  - Smlouvy o obchodním zastoupení
  - Správa majetku

Kooperativa
VIENNA INSURANCE GROUP

Státní veterinární správa

VZDÁLENÝ PODPIS

Probíhající projekt

VZDÁLENÝ ELEKTRONICKÝ PODPIS

Probíhající projekt

- ✔ Organizace po celé republice
- ✔ Použitelnost pro libovolné aplikace
- ✔ **Kvalifikovaná úroveň podpisu**
- ✔ Provoz v externím datovém centru pod správou QTSP

Státní veterinární správa

Dotazy ?

Děkuji za pozornost!

jan.tejchman@ftsb.cz