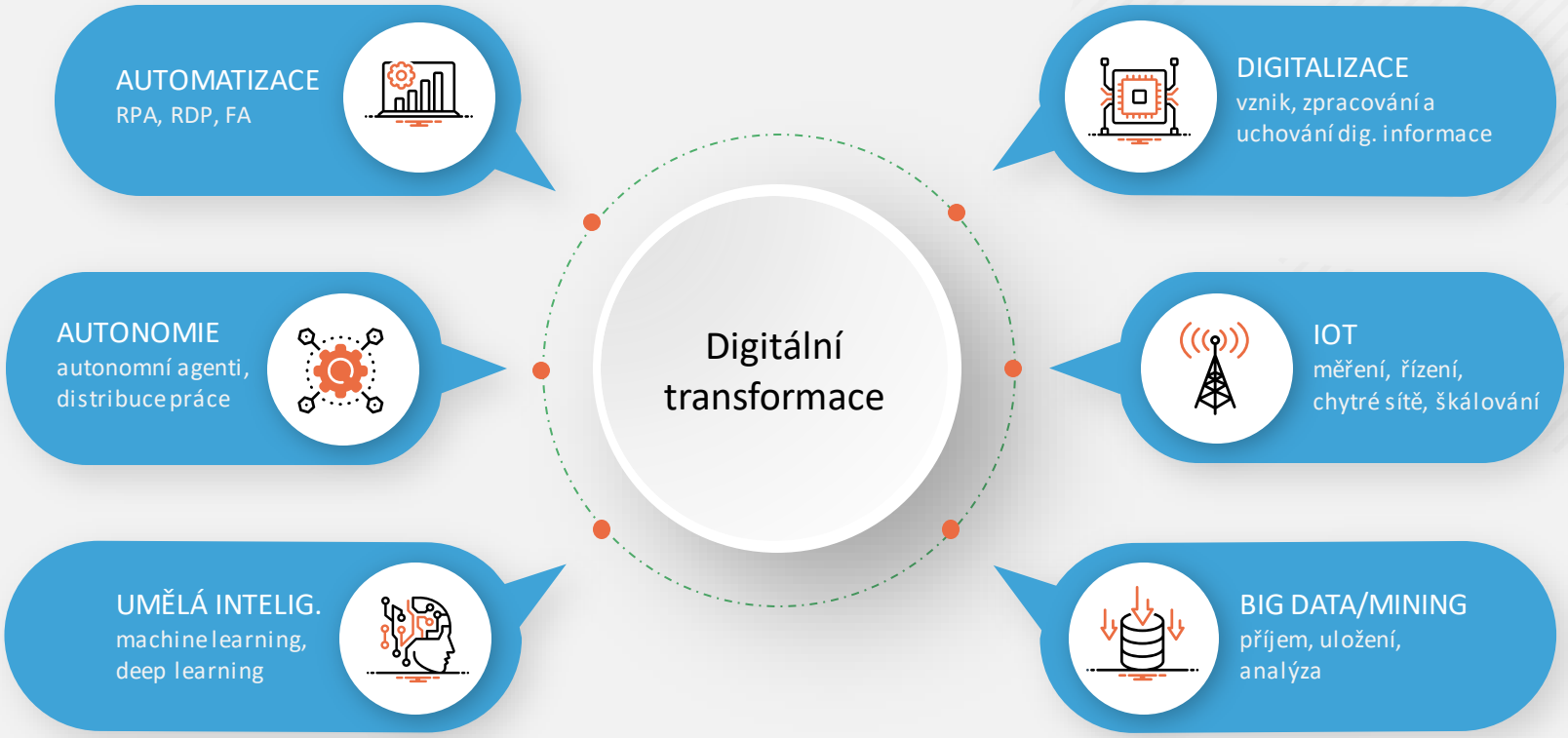
# DIGITÁLNÍ DŮVĚRA, PILÍŘ DIGITALIZACE A DIGITÁLNÍ TRANSFORMACE

| Michal Hanzal | Solution Consultant |

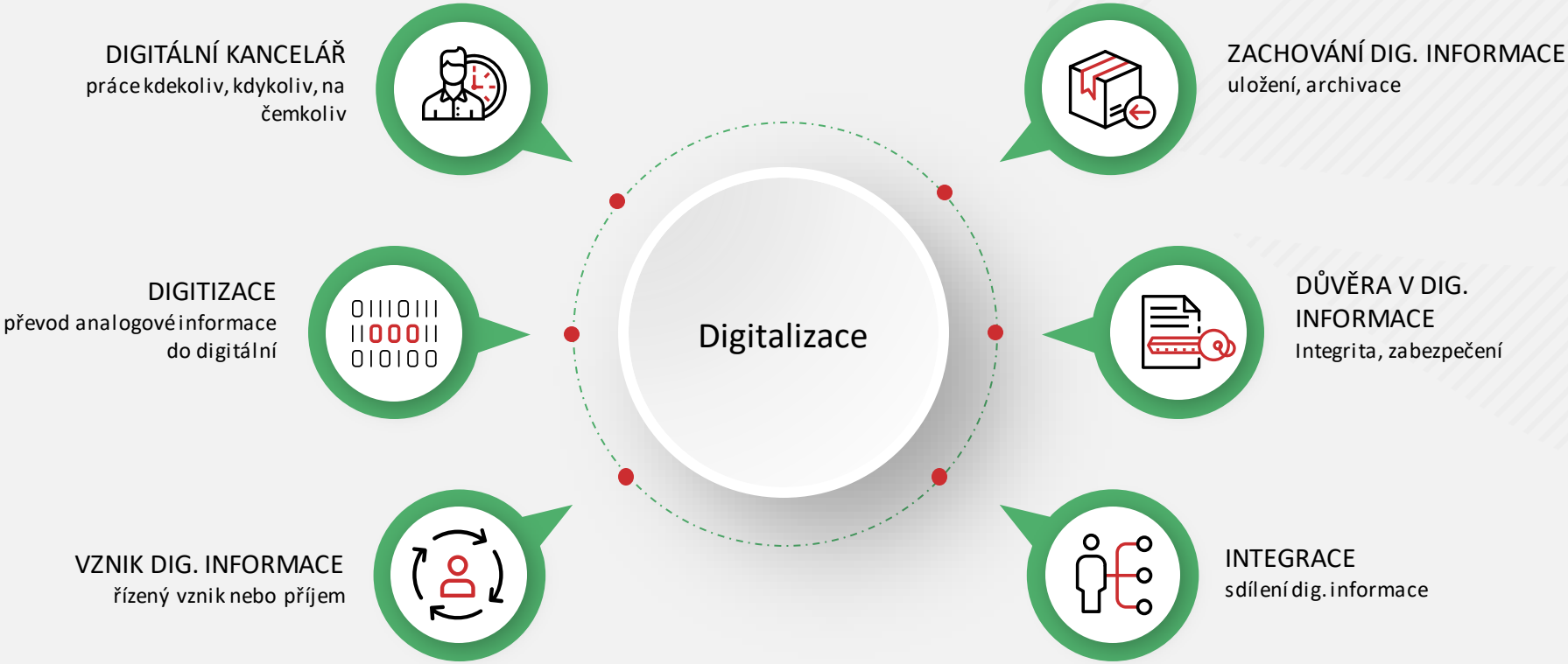
# DIGITÁLNÍ DŮVĚRA & PAPERLESS

## v kontextu digitální transformace



# DIGITÁLNÍ DŮVĚRA & PAPERLESS

## v kontextu digitalizace



# PŘÍBĚHY DIGITALIZACE

## Pro každého je to něco jiného

Modernizace
interních procesů

Výměna obchodních
informací/dat


Jednorázové
služby

Základní
finanční služby

Dlouhodobé
závazky a smlouvy

Služby
sdílené ekonomiky

# RŮZNÉ PŘÍBĚHY DIGITALIZACE

## Banky a pojišťovny

### Klient

**„Ať je to klidně elektronicky, mnoho věcí dokážu vyřídit bez návštěv pobočky.“**

- *nástroje musí poskytnout banka / pojišťovna*
- *důraz na UX / jednoduchost, musí se počítat s širokým spektrem uživatelů*
- *onboarding / získání nových klientů*

### Bankéř

**Má nástroje jak to dělat**

- *ale když to umí provést elektronicky na dálku, musí to umět elektronicky i na přepážce*
- *a musí zajistit správu plně elektronické klientské dokumentace*

# RŮZNÉ PŘÍBĚHY DIGITALIZACE

## Zdravotnictví

### Pacient

**Elektronická zdravotní dokumentace existuje**

- *už o tom slyšel, ale neví jak se k ní dostat*
- *prakticky by ji neměl potřebovat, protože mají obíhat data a ne pacient s dokumenty*
- *podobně jako lékaři, dnešní el. způsob je častokrát komplikovanější než konvenční*

### Lékař

**Lékař má léčit a až potom papírovat**

- *a elektronicky mu to obvykle trvá ještě déle*
- *často roztříštěné SW řešení pro jednotlivé agendy/kliniky*
- *neochota/nepřipravenost sdílet informace mezi zdr. zařízeními*

# RŮZNÉ PŘÍBĚHY DIGITALIZACE

## Veřejná správa a samospráva

### Občan / Podnikatel

**Všude o tom slyší, ale nikdy to neviděl,**

- *„podpora digitalizace napříč politickým spektrem“*
- *služby dostupné pouze pro „nadšence“ nebo nástroje s nechtěnými podmínkami (např. ISDS, eOP)*

**nebo to chce aktivně dělat, ale neví jak.**

- *minimální rozšíření mezi uživateli (certifikáty, eID, …)*
- *neschopnost dlouhodobé péče o dokumenty*
- *minimální podpora pro nové technologie (mobil, tablet)*
- *z toho plynoucí nejistota a strach z neznámého*

### Úředník

**Má nástroje,**

- *kvalifikovaný el. podpis / pečeť*
- *aplikace (spisové služby, agendy, …)*

**má zákonnou povinnost, ale ne vždy tak činí,**

- *důvěřuje se především papíru, i když má el. forma stejnou váhu*

**a někdy se jde proti již zavedené praxi.**

- *vyžaduje se papír*
- *vyrobí se el. dokument a ten si pak převede do papíru*

# RŮZNÉ PŘÍBĚHY DIGITALIZACE

## Interní procesy / Personalistika

### Zaměstnanec

**Chtěl by vidět všechny své dokumenty na jednom místě**

- *musí je umět dohledat a vytisknout*
- *pokud je vyžadován jejich podpis, musí je umět elektronicky podepsat*
- *rád by se obsloužil sám*

### Personalista

**Rád by se zbavil rutinních úkonů,**

- *a měl prostor věnovat se zaměstnancům a neřešit papírování*

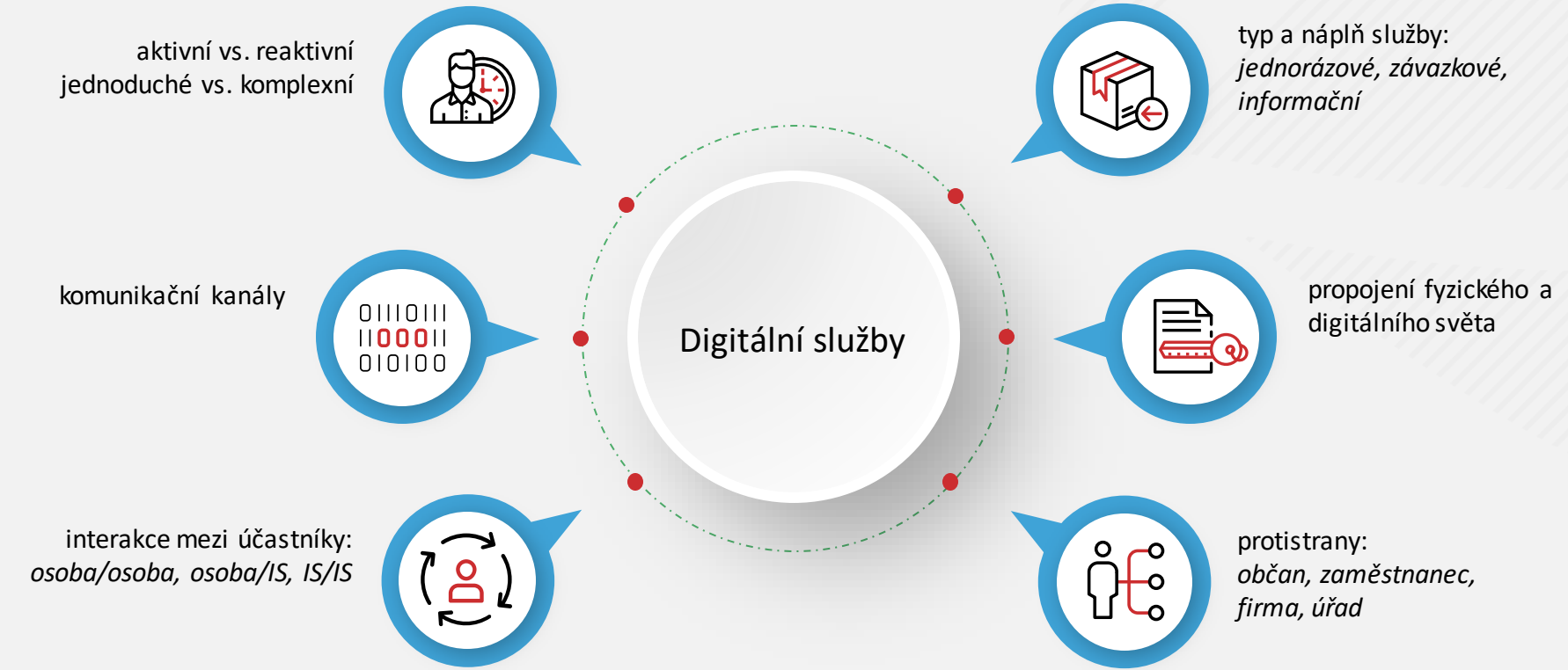
**digitalizací procesů by se vše zjednodušilo a zefektivnilo**

- *zrychlily by se interní procesy*
- *zvýšil by se přehled o vyřízených dokumentech*

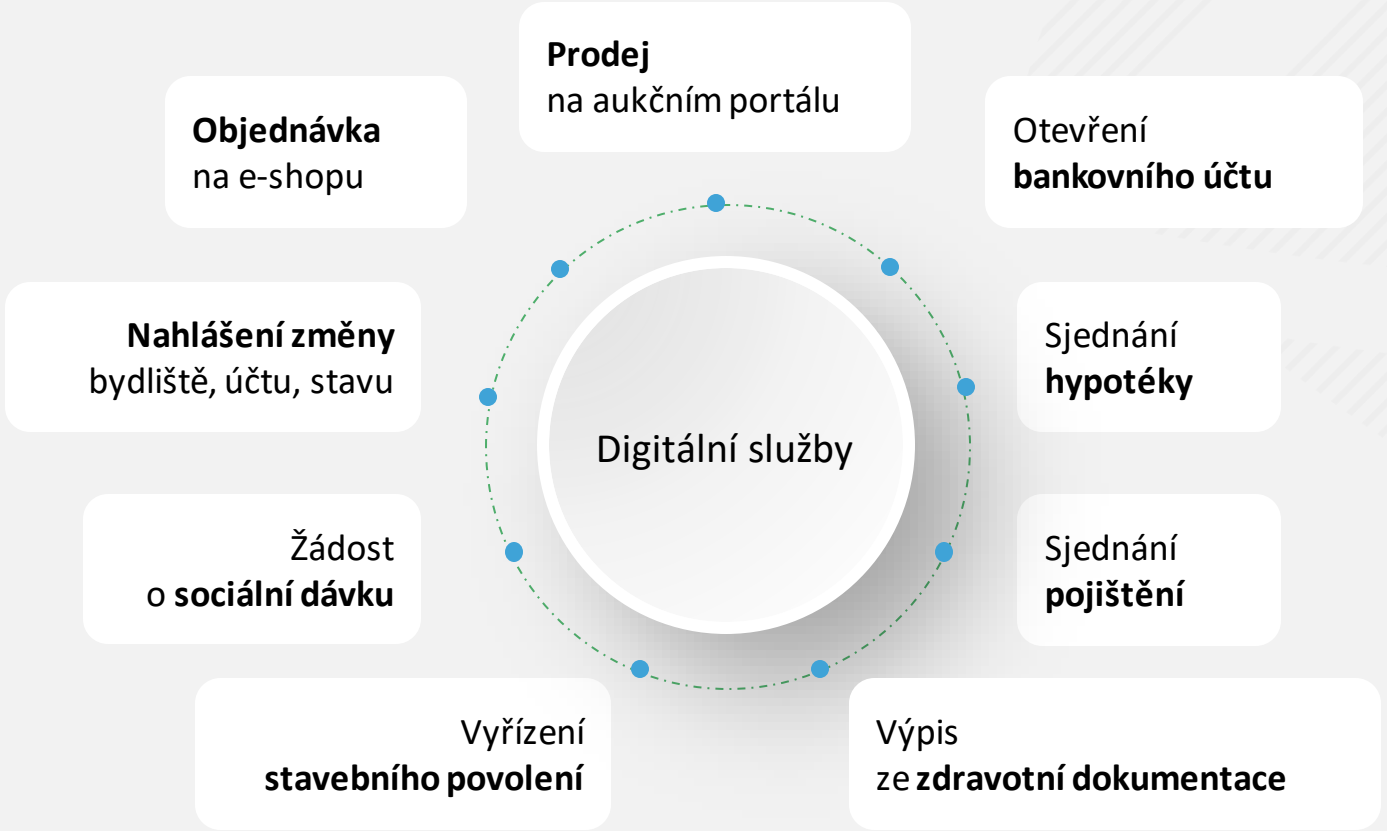
# DIGITÁLNÍ SLUŽBY

# DIGITÁLNÍ SLUŽBY

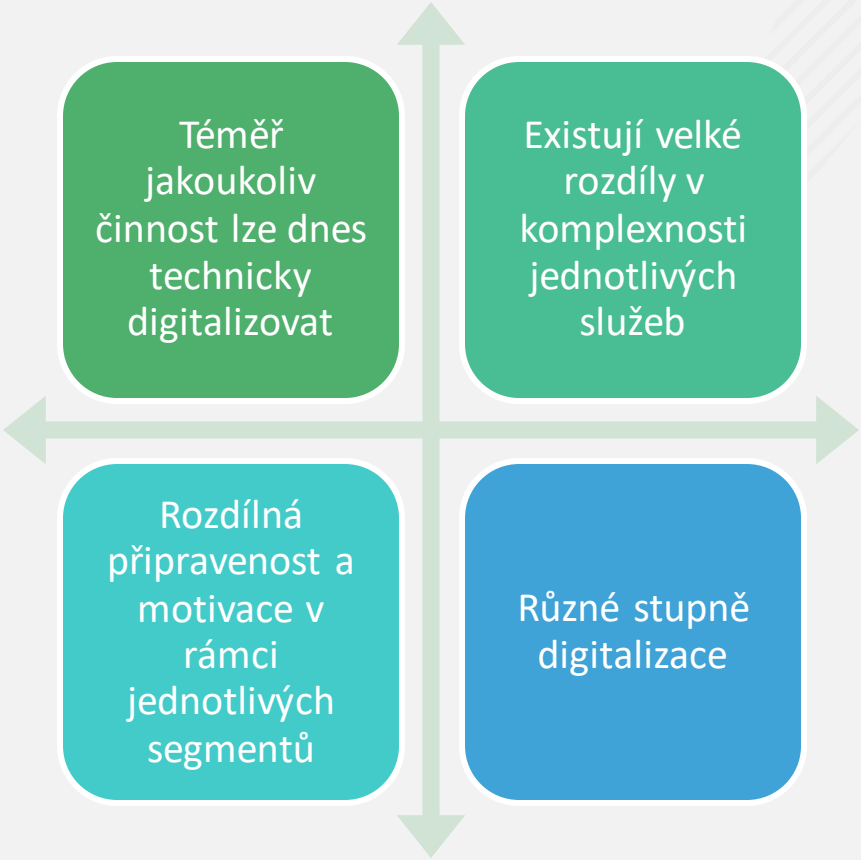
## jako nástroj digitální důvěry



# PŘÍKLADY DIGITÁLNÍCH SLUŽEB



# ZÁKLADNÍ CHARAKTERISTIKY DIGITÁLNÍ SLUŽBY



# ÚSPĚŠNÁ DIGITÁLNÍ SLUŽBA

Příjemná
uživatelská zkušenost

Jednoduchost

Srozumitelnost

„PASSWORD LESS“

„PAPERLESS“

Digitální onboarding

# DIGITÁLNÍ DŮVĚRA

# DŮVĚRA V DIGITÁLNÍ INFORMACE/DOKUMENTY

## Základní atributy

Jedná se
o originál

Lze doložit shodu
s originálem

Důvěryhodnost
lze nezávisle ověřit

Lze určit
zdroj/původce

Lze prokázat existenci
v čase

Lze ověřit, že nedošlo
ke změně obsahu

# PROSTŘEDÍ

## Legislativa

| Nařízení / Zákon | |
|---|---|
| eIDAS | Nařízení Evropského Parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce |
| GDPR | Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů |
| ZoSVD | Zákon č. 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce |
| ZoEID | Zákon č. 250/2017 Sb. o elektronické identifikaci |
| ZoPDS | Zákon č. 12/2020 Sb. o právu na digitální služby |
| ZoASS | Zákon č. 499/2004 Sb. o archivnictví a spisové službě |
| ZoKB | Zákon č. 181/2014 Sb. o kybernetické bezpečnosti |

# PROSTŘEDÍ

## Technické standardy



# VÝBĚR ETSI TECHNICKÝCH STANDARDŮ

| Standard | Zaměření |
|---|---|
| ETSI EN 319 102 | Creation and validation of AdES digital signatures |
| ETSI EN 319 122 | CAdES digital signatures |
| ETSI EN 319 132 | XAdES digital signatures |
| ETSI EN 319 142 | PAdES digital signatures |
| ETSI EN 319 172 | Signature Policies |
| ETSI EN 319 312 | Cryptographic Suites |
| ETSI TS 119 511 | Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques |

# ZROVNOPRÁVNĚNÍ DŮVĚRY V DOKUMENTY


Papírový dokument

=

PDF

Elektronický dokument

El. podpis

El. pečeť

Čas. razítko

# DŮVĚRA V DIGITÁLNÍ INFORMACE/DOKUMENTY

## Stručná historie v prostředí ČR

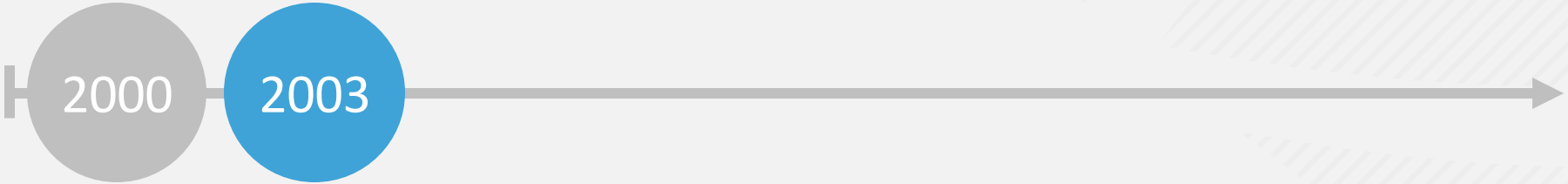
2000

**Schválen Zákon č. 227/2000 Sb. o elektronickém podpisu**

Používání technologického elektronického podpisu
pro zabezpečení výměny dat

# DŮVĚRA V DIGITÁLNÍ INFORMACE/DOKUMENTY

## Stručná historie v prostředí ČR



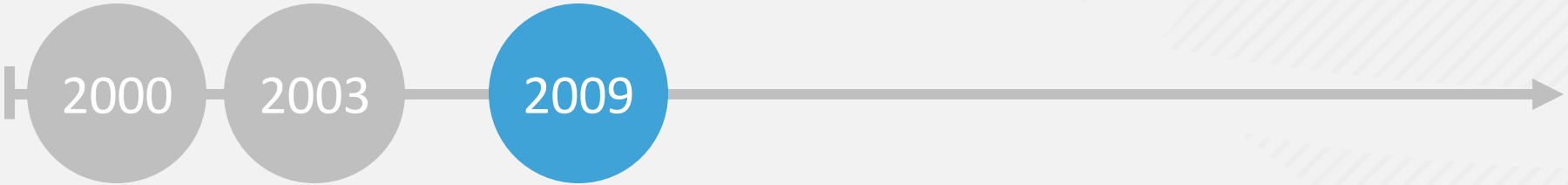

**Vznik první kvalifikované certifikační autority v ČR**

Kvalifikovaná časová razítka – 2004

Uznávaná elektronická značka – 2006

# DŮVĚRA V DIGITÁLNÍ INFORMACE/DOKUMENTY

## Stručná historie v prostředí ČR

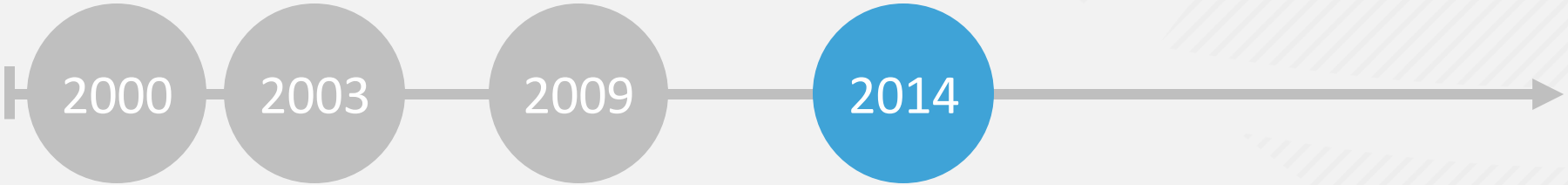



**Spuštění Datových schránek**

Praktický start vytváření a výměny
důvěryhodných elektronických dokumentů

# DŮVĚRA V DIGITÁLNÍ INFORMACE/DOKUMENTY

## Stručná historie v prostředí ČR

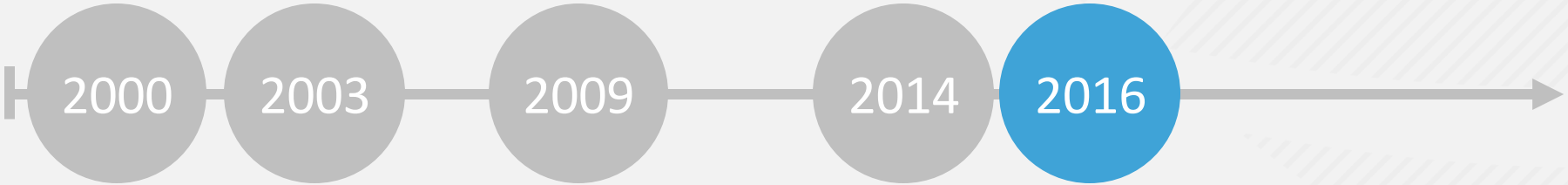



**Schválení evropského nařízení eIDAS**

Nařízení Evropského Parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce

# DŮVĚRA V DIGITÁLNÍ INFORMACE/DOKUMENTY

## Stručná historie v prostředí ČR

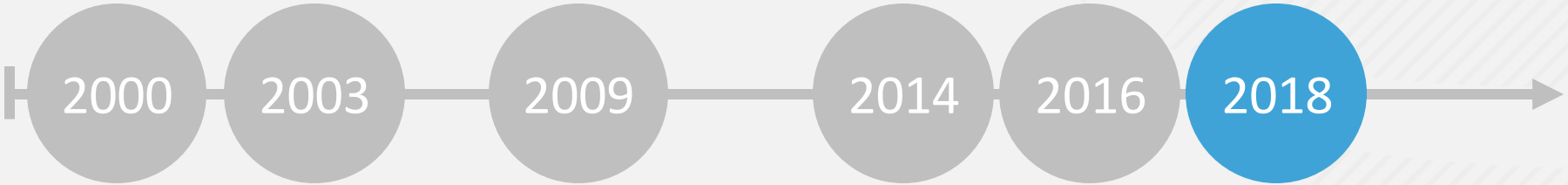



Vstoupení **eIDAS** v platnost **pro dokumenty**

Implementační zákon č. 297/2016 Sb.
o službách vytvářejících důvěru

# DŮVĚRA V DIGITÁLNÍ INFORMACE/DOKUMENTY

## Stručná historie v prostředí ČR

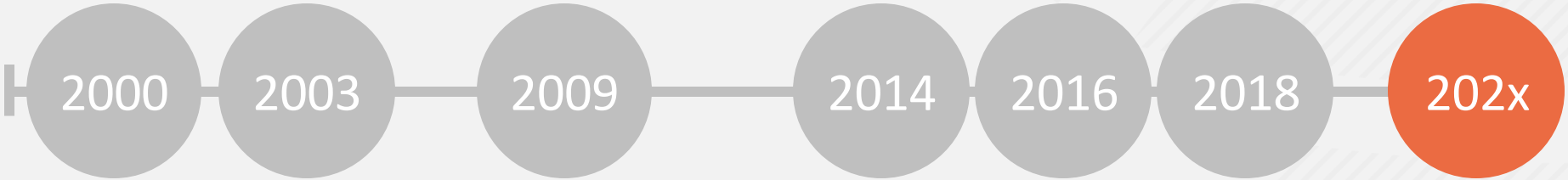



**Plná účinnost nařízení eIDAS a lokálních úprav**

dokumenty, el. identifikace, NIA, nové eOP, Portál občana

# DŮVĚRA V DIGITÁLNÍ INFORMACE/DOKUMENTY

## Stručná historie v prostředí ČR




**Spouštění podpůrných projektů a nová legislativa**

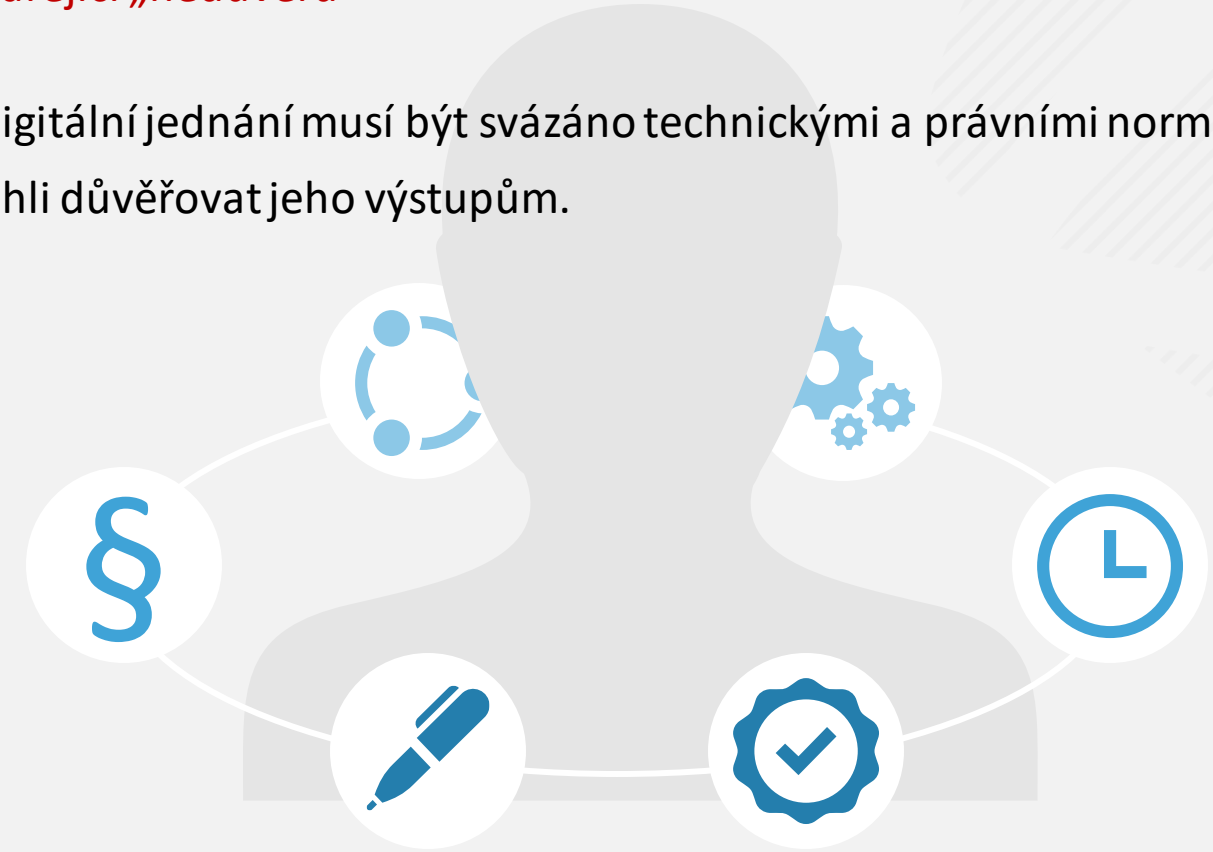
SONIA, Zákon č. 12/2020 o právu na digitální služby…

# KLÍČOVÉ PRVKY DIGITÁLNÍ DŮVĚRY

# UŽIVATEL / ČLOVĚK

## Element vytvářející „nedůvěru“

Uživatelské digitální jednání musí být svázáno technickými a právními normami, abychom mohli důvěřovat jeho výstupům.



# ELEKTRONICKÁ IDENTITA

## Řekni, kdo jsi

- **Identita** – souhrn atributů popisující/definující danou entitu ve virtuálním prostředí odpovídající entitě reálné osoby
  - jedna reálná osoba má obecně více el. identit
- Úrovně elektronické identity dle eIDAS
  - **Nízká** – Google / Facebook ID
  - **Značná** – MojeID
  - **Vysoká** – elektronická identita na nových OP, bankovní identita (v přípravě)
- Vznik elektronické identity = onboarding
- Občanský průkaz je forma „uživatelské“ identity

# AUTENTIZACE

Prokaž, že jsi ten, kdo tvrdíš, že jsi

- **Autentizace** – soubor technik, které s určitou mírou záruky pomáhají ověřit identitu uživatele
- Techniky:
  - Něco jsem (bio), něco mám (mobil/token), něco vím (heslo/pin)
- V praxi:
  - Hesla, PINy
  - OTP – SMS, email, autentikátory, poštovní schránka
  - Biometrická ověření – otisk prstu, sken obličeje
  - Prostředky státu – datová schránka, prostředky eObčanky
- Dvou / více faktorová autentizace (2FA, MFA)

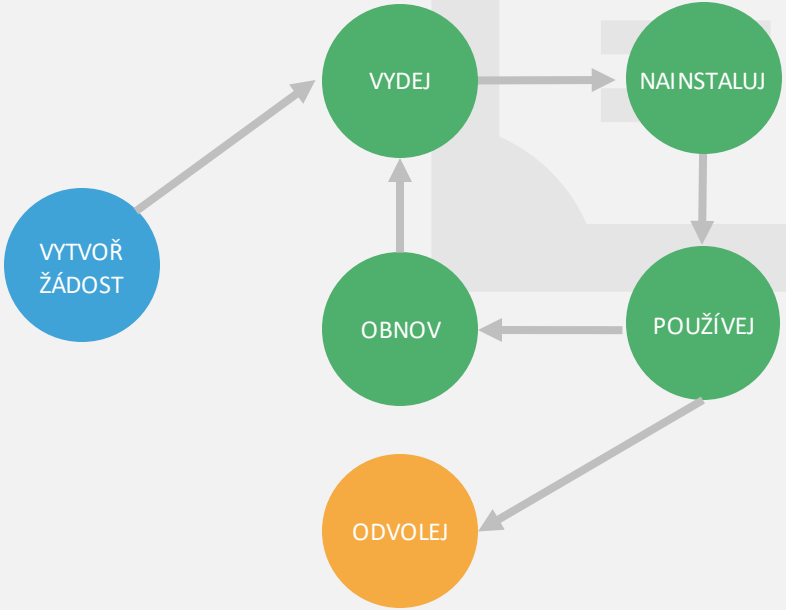
# PUBLIC KEY INFRASTRUCTURE (PKI)

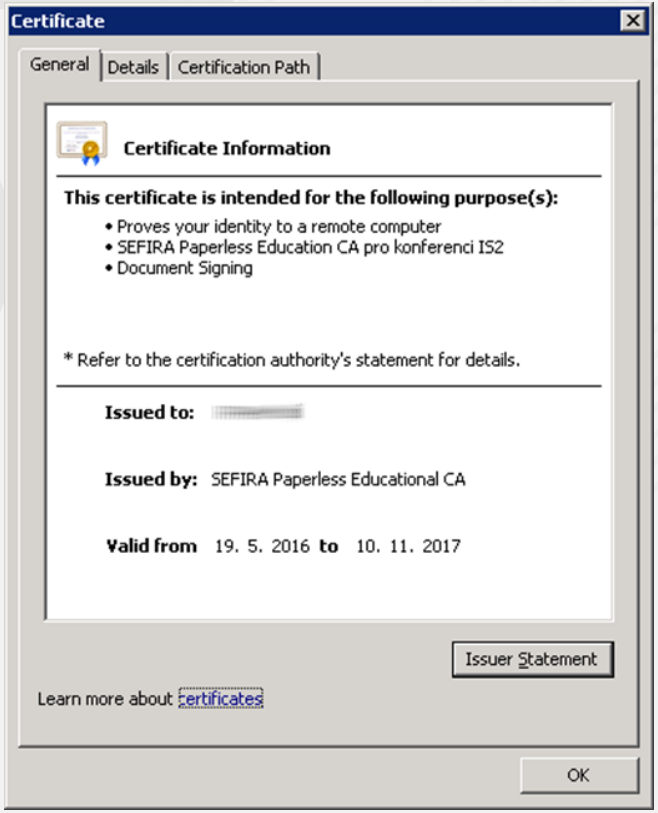
## Klíče, autority a certifikáty

- **PKI** – široký souhrn znalostí, dohod, standardů, postupů, hardware & software, legislativy, osob, …
- Asymetrická kryptografie – soukromý a veřejný klíč + certifikáty
- Soustava certifikačních autorit vydávajících certifikáty
- Certifikát = časově omezené písemné „potvrzení“ CA o existenci a vlastnictví určitého páru klíčů a o zamýšleném způsobu použití těchto klíčů

# CERTIFIKAČNÍ AUTORITA

- Vydává certifikáty
- Řídí životní cyklus certifikátu
- Garantuje správnost informací v certifikátu



# CERTIFIKAČNÍ AUTORITA

## Organizaci vytvářející důvěru

- Typy certifikačních autorit
  - **Interní**
    podpisové, autentizační i šifrovací certifikáty (pouze pro interní potřebu organizace)
  - **Komerční**
    autentizační certifikáty (přihlašování certifikátem), šifrovací certifikáty (šifrování dat)
  - **Kvalifikované**
    podpisové / pečetící certifikáty (kvalifikované podpisy)
- Ručí za vazbu osoba – certifikát – soukromý klíč

# KVALIFIKOVANÍ POSKYTOVATELÉ

- Zpravidla organizace poskytující jednu nebo více kvalifikovaných služeb vytvářející důvěru
- Orgánem dohledu (Ministerstvo vnitra) jim byl udělen status kvalifikovaného poskytovatele (na základě provedeného auditu)
- Poskytované kvalifikované služby:
  - Vydávání **kvalifikovaných certifikátů** pro podpis / pečeť / autentizaci webových stránek
  - Vydávání **kvalifikovaných časových razítek**
  - **Ověřování** elektronických podpisů / pečetí
  - **Dlouhodobé uchování** podpisů / pečetí

# KVALIFIKOVANÝ PROSTŘEDEK

## pro vytváření elektronických podpisů a pečetí (QSCD)

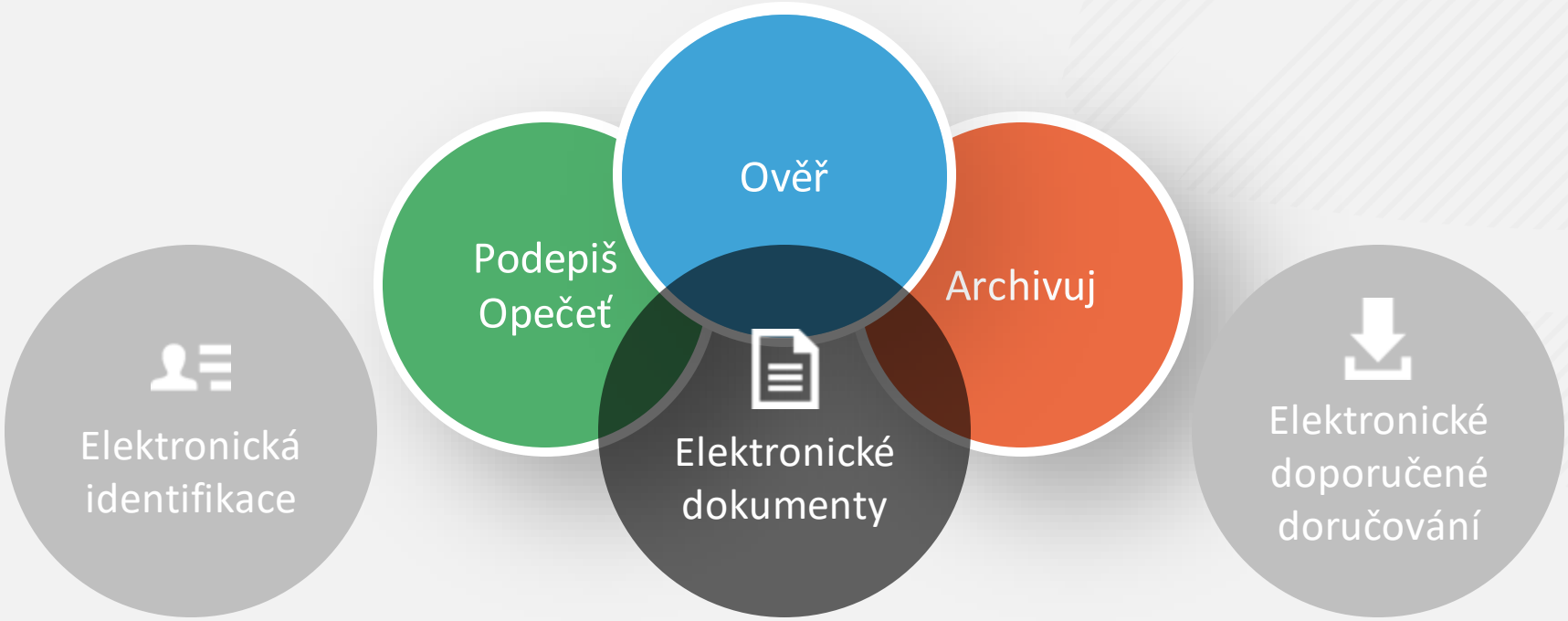
- ✔ eIDAS čl. 29 + příloha II
- ✔ QSCD = QSignCD nebo QSealCD
- ✔ Informativní EU seznam schválených QSCD*
  - QSignCD vs. QSealCD
  - tokeny, čipové karty i **HSM**
- ✔ Zařízení pro správu a uložení klíčů musí být certifikováno dle standardu EN 419 221-5: eIDAS Protection Profile vydaného akreditovaným orgánem dle nařízení eIDAS

* https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds

# SLUŽBY VYTVÁŘEJÍCÍ DŮVĚRU

# SLUŽBY VYTVÁŘEJÍCÍ DŮVĚRU

## Dle eIDAS



# ELEKTRONICKÝ PODPIS

**Vyjádření souhlasu**
fyzické osoby s obsahem podepsaného dokumentu.

**Zajištění integrity**
Umožňuje detekci neautorizovaných změn v dokumentu opatřeného elektronickým podpisem.

# ELEKTRONICKÁ PEČEŤ

**Prokázání původu**

Vnáší do dokumentu nezměnitelné informace o původci dokumentu opatřeného elektronickou pečetí.

**Zajištění integrity**

Umožňuje detekci neautorizovaných změn v dokumentu opatřeného elektronickou pečetí.

# VALIDACE EL. PODPISŮ A PEČETÍ

**Ověření validity**

Validace zajišťuje prozkoumání úrovně a kvality podpisu/pečeti včetně prověření platnosti použitých certifikátů.

**Ověření integrity**

Validace zajišťuje detekci neautorizovaných změn v dokumentu opatřeného elektronickým podpisem nebo pečetí.

# DŮVĚRYHODNÁ ARCHIVACE

**Zafixování**
archivovaného obsahu pomocí prostředků kryptografie a elektronického pečetění

**Zachování**
digitální kontinuity a ověřitelnosti elektronických podpisů a pečetí i po konci platnosti certifikátů

# PRAKTICKÁ PŘÍRUČKA DIGITÁLNÍ DŮVĚRY

# NÁVOD JAK NA TO – ZÁKLADNÍ DOPORUČENÍ

## Praktická příručka digitální důvěry

- ✔ ŘEŠTE zadání na všech úrovních *(management, business vlastník, právníci, ICT, uživatelé)*
- ✔ BUDUJTE sdílené služby digitální důvěry *(jedna implementace pro všechny aplikace)*
- ✔ PŘIPRAVTE SE na externí systémy el. identifikace *(NIA, SONIA, …)*
- ✔ ZAMĚŘTE SE na dobrou User eXperience *(UX)*
- ✔ NEBOJTE SE nechat si poradit

# PRAKTICKÁ PŘÍRUČKA DIGITÁLNÍ DŮVĚRY

## Vím co chci! Vím co chci?

- ✔ CHCI realizovat/zlepšit digitalizaci v oblasti ……
  - které jsou v souladu se strategií organizace nebo posvěcené od managementu
- ✔ VÍM/TUŠÍM jak mají vypadat výsledné digitální služby pro ……
- ✔ MÁM/BUDUJI potřebné agendové/business aplikace ……
  - ALE nevím co bude potřeba ještě doplnit
- ✔ MÁM „nějaké“ informace o UŽIVATELÍCH nových digitálních služeb
  - ALE pravděpodobně nejsou konsolidovány za celou organizaci
  - NEBO se bude jednat o nové uživatele z ulice

# 4 ÚLOHY PRO BUSINESS

- ✔ Změna myšlení / přístupu
  - digitalizace není pouze náhrada papíru za el. dokument
  - příležitost změnit/zjednodušit stávající procesy
- ✔ Formulace zadání pro nové řešení (odpovědnost business)
  - podpora ze strany managementu nebo naplňování strategie
  - ověření proveditelnosti ve spolupráci s ICT a bezpečností
- ✔ Právní posouzení dopadů na společnost/klienty
  - legislativa může být současně nápomocná i blokující/omezující
  - hledání cest k ošetření právních rizik
- ✔ Analýza stavu a návrh řešení

# ANALÝZA STAVU A NÁVRH ŘEŠENÍ

## Kooperace business / ICT / právníků / uživatelů

- ✔ Revize existujících procesů & technologií
- ✔ Radši menší, ale jasně definované změny (evoluce, ne revoluce)
  - práce s prototypy pro lepší představu
  - pilot na menší agendě nebo pro menší skupinu uživatelů
- ✔ Orientace na znovupoužitelnost, synergii a efektivitu
- ✔ Dostatek prostoru pro ověření a akceptaci nových funkcí
  - jednoduchost, srozumitelnost, UX
  - především aplikace pro koncové uživatele
- ✔ Řešení celého životního cyklu digitálních informací/dokumentů
  - nestačí je pouze vytvořit nebo zpracovat

# 4 ZÁSADNÍ ÚKOLY PRO ICT

Cíle v digitalizaci procesů

Možnosti jednotlivých systémů

Integrace sdílených služeb
digitální důvěry a paperless

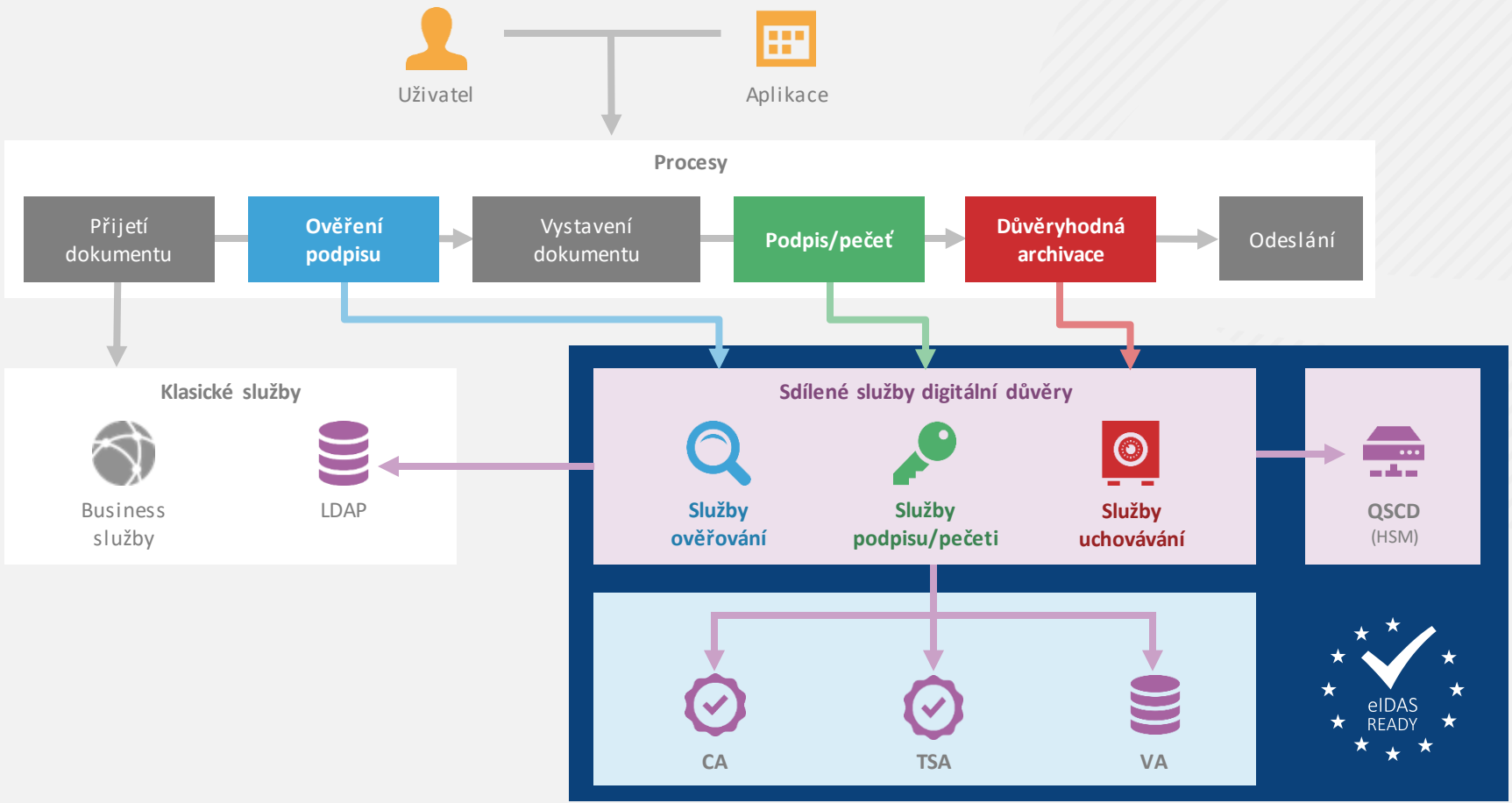
Integrace služeb PKI

# SDÍLENÉ SLUŽBY – ZÁKLADNÍ PRINCIPY

## Praktická příručka digitální důvěry

- ✔ Centrální služby pro všechny informační systémy => efektivita
  - Nechejme business systémy podporovat procesy, digitální důvěru čerpejme jako infrastrukturní službu
- ✔ Orientace na znovupoužitelnost, synergii a efektivitu
  - Není potřeba znova vymýšlet něco již vymyšleného, implementovat něco již implementovaného, …
- ✔ Důraz na certifikaci řešení

# SDÍLENÉ SLUŽBY DIGITÁLNÍ DŮVĚRY



# PŘÍPRAVA NA EL. IDENTIFIKACI

- Je třeba si vyjasnit:
  - Je pro nás zajímavé čerpat služby elektronické identifikace?
  - A pro které procesy?
  - Jakou míru důvěry potřebujeme?
- Již dnes existuje mnoho eID služeb.
  - Státní eID / NIA – omezené možnosti použití
  - MojeID – několik úrovní důvěry
  - Vzniká české BankID

# USER EXPERIENCE (UX)

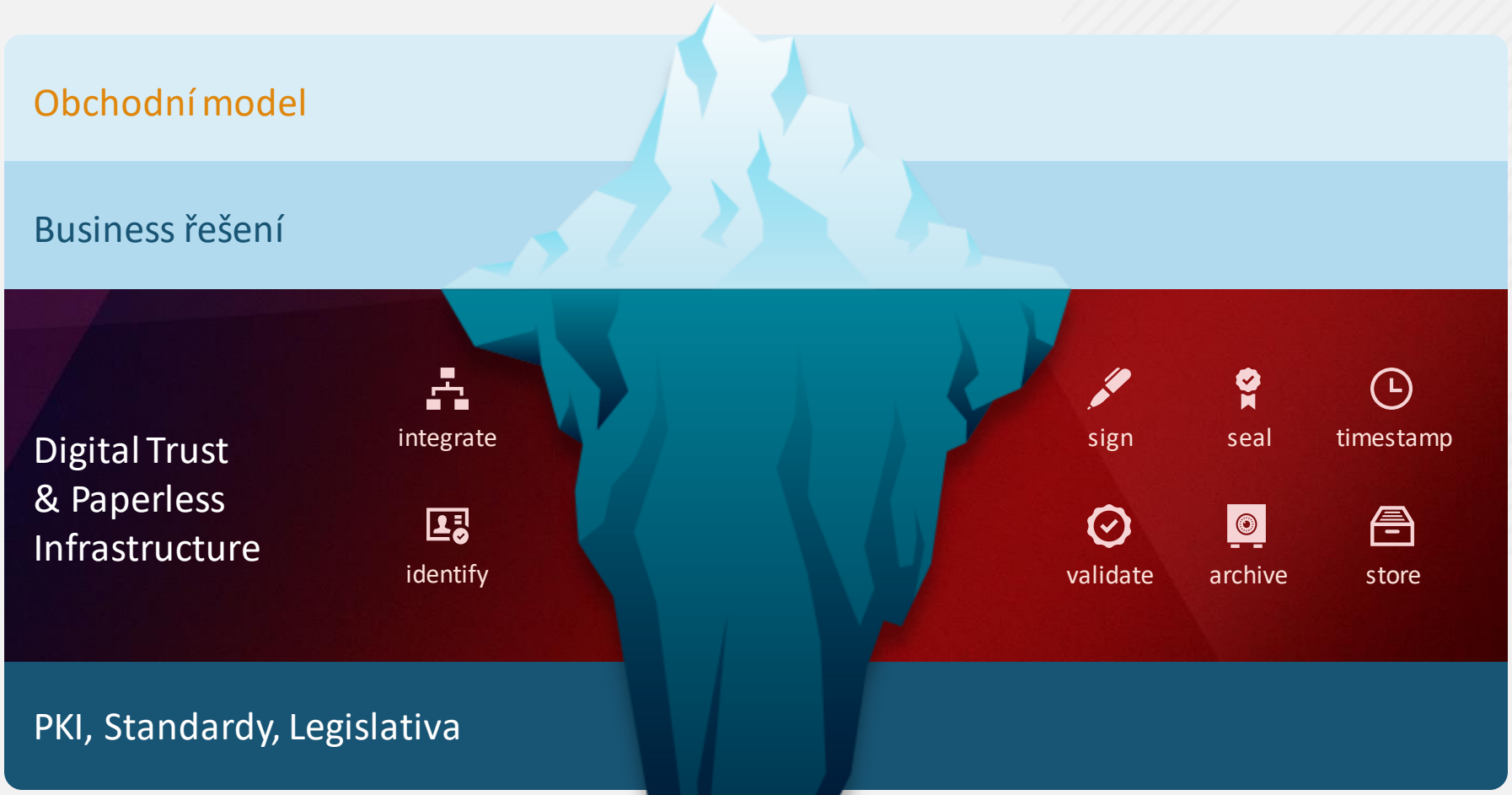
## Praktická příručka digitální důvěry

# KONZULTUJTE, NECHEJTE SI PORADIT

## Praktická příručka digitální důvěry

- ✔ Proč si lámat se vším hlavu, když už to jinde někdo řešil/umí
  - edukace odpovědných osob v nové problematice
  - konzultace k návrhu řešení a architektury
  - sdílení zkušeností z úspěšných realizovaných projektů
  - identifikace a uplatňování ověřených standardů
- ✔ Co mi brání v realizaci či nasazení (technicky, legislativně)
- ✔ Na co si dát pozor při pořizování nových technologií (když 2 dělají totéž není to totéž)
- ✔ Nezávislé posouzení návrhu/implementace
- ✔ …

# VRSTVA INFRASTRUKTURY DIGITÁLNÍ DŮVĚRY




www.sefira.cz