KVALIFIKOVANÁ PEČEŤ

| Jan Tejchman | Senior Solution Consultant |

PROČ VŮBEC ELEKTRONICKÝ PODPIS A PEČEŤ?

Protože chceme fungovat elektronicky!

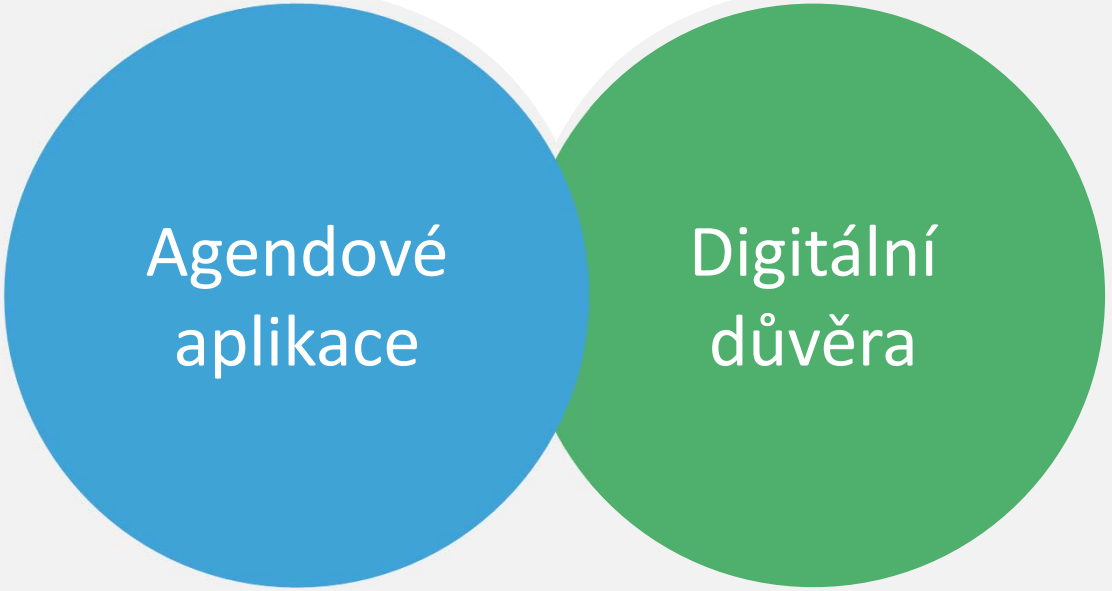
Digitální Evropa

Digitální transformace

Elektronické dokumenty

Právní validita

Služby vytvářející důvěru



DIGITÁLNÍ DŮVĚRA

DŮVĚRA A JEJÍ NÁSTROJE VE FYZICKÉM SVĚTĚ

DIGITÁLNÍ DŮVĚRA – ANALOGIE ZALOŽENÁ NA PKI

EVROPSKÉ NAŘÍZENÍ eIDAS

Ukotvení digitální důvěry

- Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 ***„o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES“***
- Stanovuje rámec **závazný** pro celou EU v oblastech
  - Elektronické identifikace
  - Elektronických dokumentů, podpisů, pečetí, časových razítek a certifikátů
  - Elektronického ověřování platnosti
  - Elektronického dlouhodobého uchovávání
  - Elektronické doporučené doručování
  - Autentizace internetových stránek

EUROPEAN COMMISSION

DIGITÁLNÍ DŮVĚRA STOJÍ NA PKI

Dohledový orgán

Public Key Infrastructure

Certifikační autorita

Validační autorita

Soukromý /veřejný klíč

Certifikát

Podpis/pečeť

Časové razítko

CRL/OCSP

UPLATNĚNÍ EIDAS

G2C	G2B	G2G	G2E
▪ Čerpání informací ▪ Žádosti ▪ Oznamovací povinnost	▪ Čerpání informací ▪ Žádosti ▪ Oznamovací povinnost	▪ Agendy ▪ Výměna informací	▪ Interní procesy ▪ HR ▪ Asset Management
individuální/adhoc požadavky	dávkové/opakované požadavky	dávkové/opakované požadavky	individuální/dávkové požadavky

B2C	B2B	B2G	B2E
▪ Smlouvy ▪ Objednávky ▪ Změny ▪ Přístup k informacím	▪ Smlouvy ▪ Faktury ▪ Objednávky ▪ Přístup k informacím	▪ Reporting, daně ▪ Úřední korespondence	▪ Interní procesy ▪ HR ▪ Asset Management
individuální/adhoc požadavky	dávkové/opakované požadavky	dávkové/opakované požadavky	individuální/dávkové požadavky

NAŘÍZENÍ EIDAS
A JEHO NÁSTROJE

NAŘÍZENÍ EIDAS

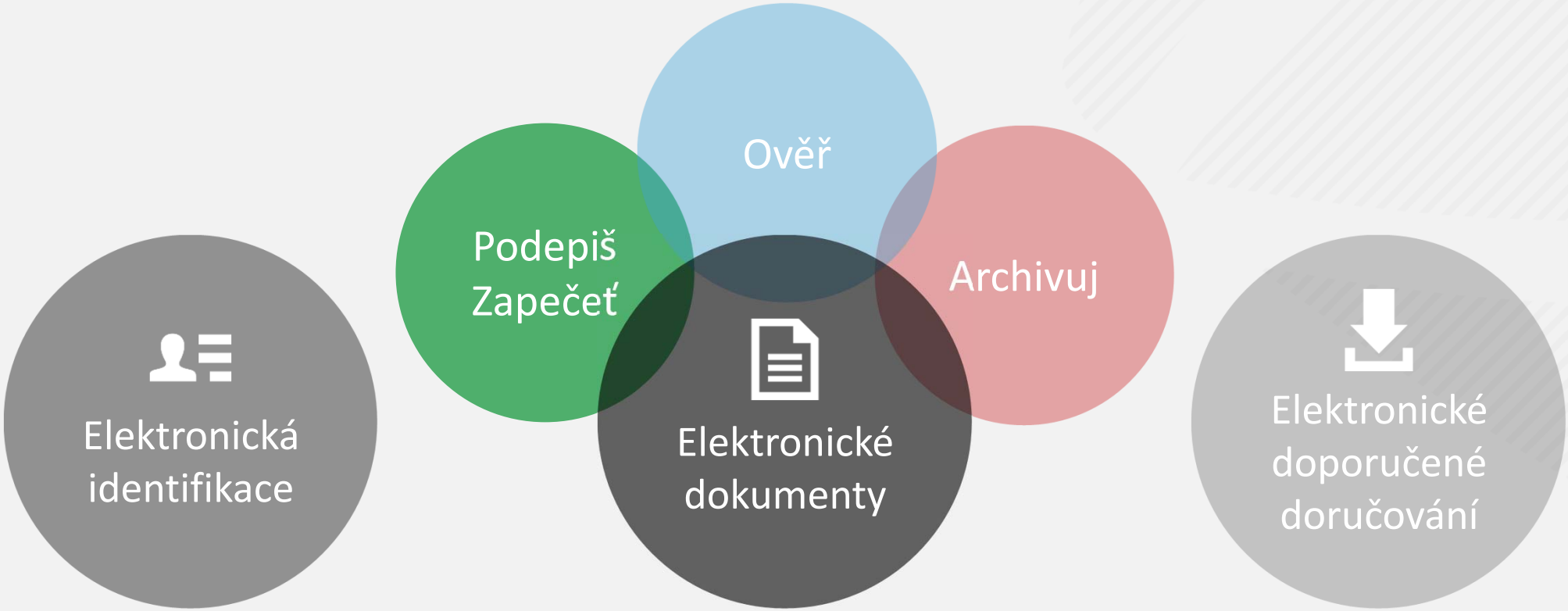
Zrovnoprávnění elektronických a listinných dokumentů

Kvalifikovaný elektronický podpis má stejnou váhu jako podpis vlastnoruční

Elektronickému dokumentu nesmějí být upírány právní účinky jen proto, že je elektronický

NAŘÍZENÍ EIDAS

Služby vytvářející důvěru



ELEKTRONICKÝ PODPIS A PEČEŤ

ELEKTRONICKÝ PODPIS VS. PEČEŤ

Rozlišení účelu použití (pouze právní rozdíl)

Podpis

prostředek vyjádření vůle člověka (fyzické osoby) k obsahu dokumentu

Pečeť

prokázání původu dokumentu (OVM, právnické osoby)

ÚROVNĚ ELEKTRONICKÝCH PODPISŮ/PEČETÍ

dle nařízení eIDAS a zákona o službách vytvářejících důvěru

Kvalifikovaný

- AdES
- certifikát vydaný kvalifikovaným poskytovatelem služeb
- soukromý klíč uložen v QSCD

Uznávaný (CZ)

- AdES
- certifikát vydaný kvalifikovaným poskytovatelem služeb

Ostatní typy

- Zaručený (AdES)

nebo

- Biometrický

nebo

- Prostý

ZÁKON O SLUŽBÁCH VYTVÁŘEJÍCÍCH DŮVĚRU (ZoSVD)

Elektronický dokument a elektronický podpis

- Elektronický dokument podepisuje **výhradně kvalifikovaným** el. podpisem pokud právně jedná při výkonu své působnosti „**veřejnoprávní podepisující**“ (viz **§5**)
- Elektronický dokument **může** být podepsán **uznávaným** el. podpisem pokud se právně jedná vůči **veřejnoprávním podepisujícím** (viz **§6**)
- Elektronický dokument **může** být podepsán **jakýmkoli** el. podpisem pokud se právně jedná v jiných případech než uvedených v **§5** a **§6** (viz **§7**)

ZÁKON O SLUŽBÁCH VYTVÁŘEJÍCÍCH DŮVĚRU (ZoSVD)

Elektronický dokument a elektronická pečeť, čas. razítko

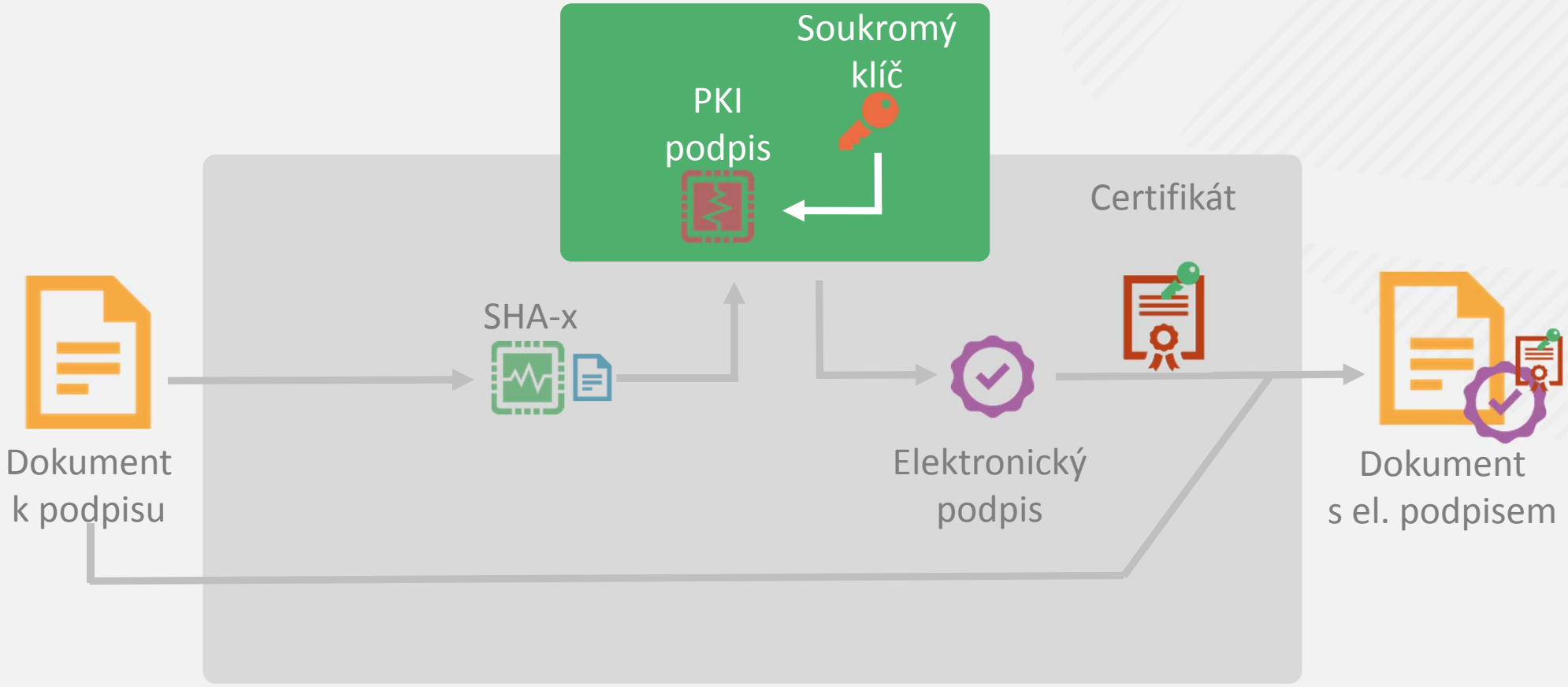
- Elektronický dokument **musí** být opatřen, v rámci výkonu působení veřejnoprávního podepisujícího, **kvalifikovanou** el. pečetí pokud **nemusí** být opatřen **kvalifikovaným** el. podpisem (viz **§8**)
- Elektronický dokument **musí** být opatřen **kvalifikovaným** el. časovým razítkem, pokud jde o dokument, kterým právně jedná v rámci své působnosti veřejnoprávní podepisující (viz **§11**)
- Elektronický dokument **nemusí** být opatřen **kvalifikovaným el.** časovým razítkem, pokud jde o dokument, kterým se právně jedná vůči veřejnoprávnímu podepisujícímu (viz **§11**)

ZÁKONEM VYŽADOVANÉ ÚROVNĚ PODPISU

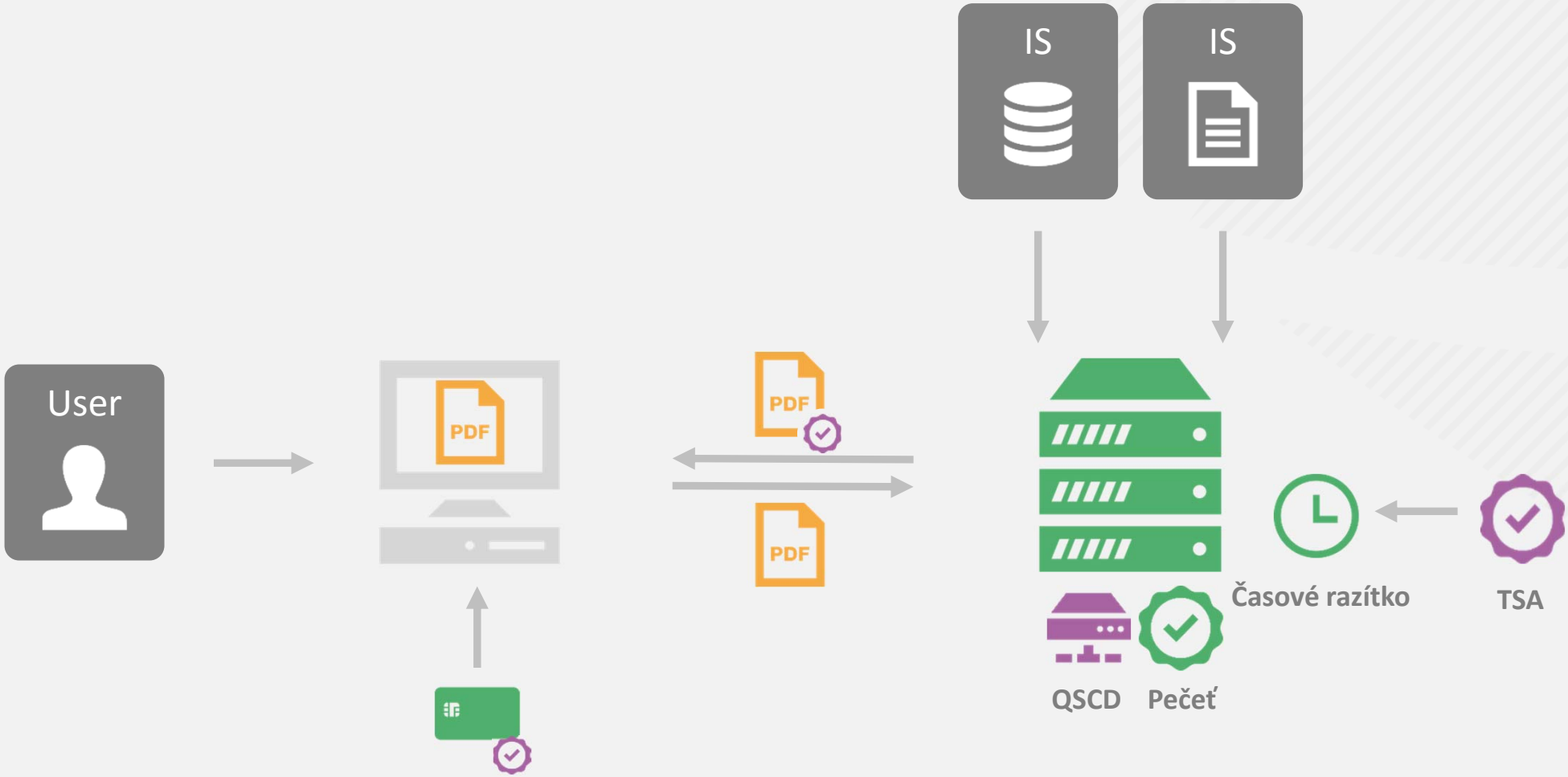
Matice použití typů elektronických podpisů v praxi (od 09/2018)

od \ pro	Veřejná správa	Občan	Komerce
Veřejná správa	Kvalifikovaný	Kvalifikovaný	Kvalifikovaný
Občan	Uznávaný	*Libovolný typ*	*Libovolný typ*
Komerce	Uznávaný	*Libovolný typ*	*Libovolný typ*

ELEKTRONICKÝ PODPIS/PEČEŤ



VYTVÁŘENÍ KVALIFIKOVANÝCH PODPISŮ A PEČETÍ



KVALIFIKOVANÁ PEČEŤ

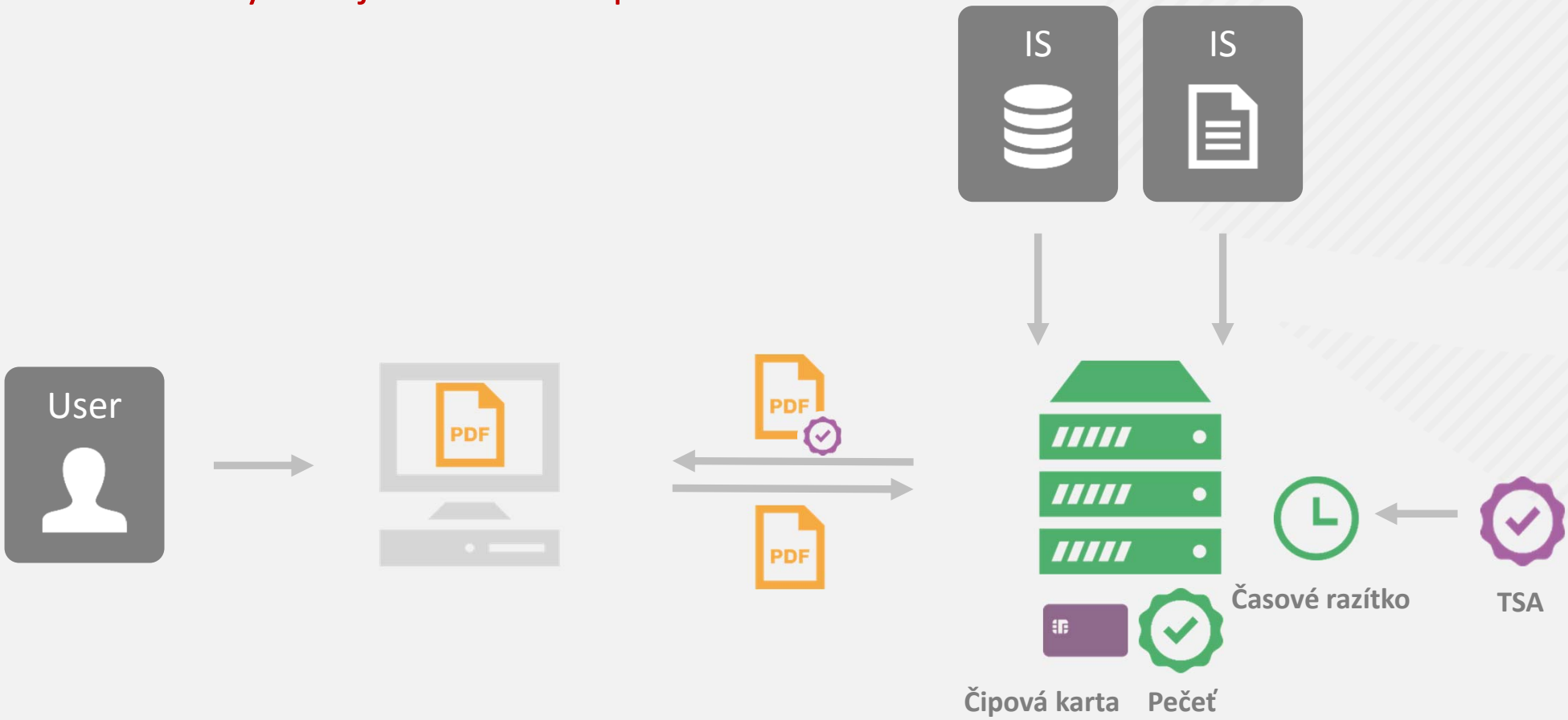
Jak se rozhodnout?

- ✔ Ekonomické parametry
- ✔ Technické parametry

- ✔ TCO na 3-5
- ✔ Výkon/propustnost
- ✔ Dostupnost
- ✔ Složitost integrace

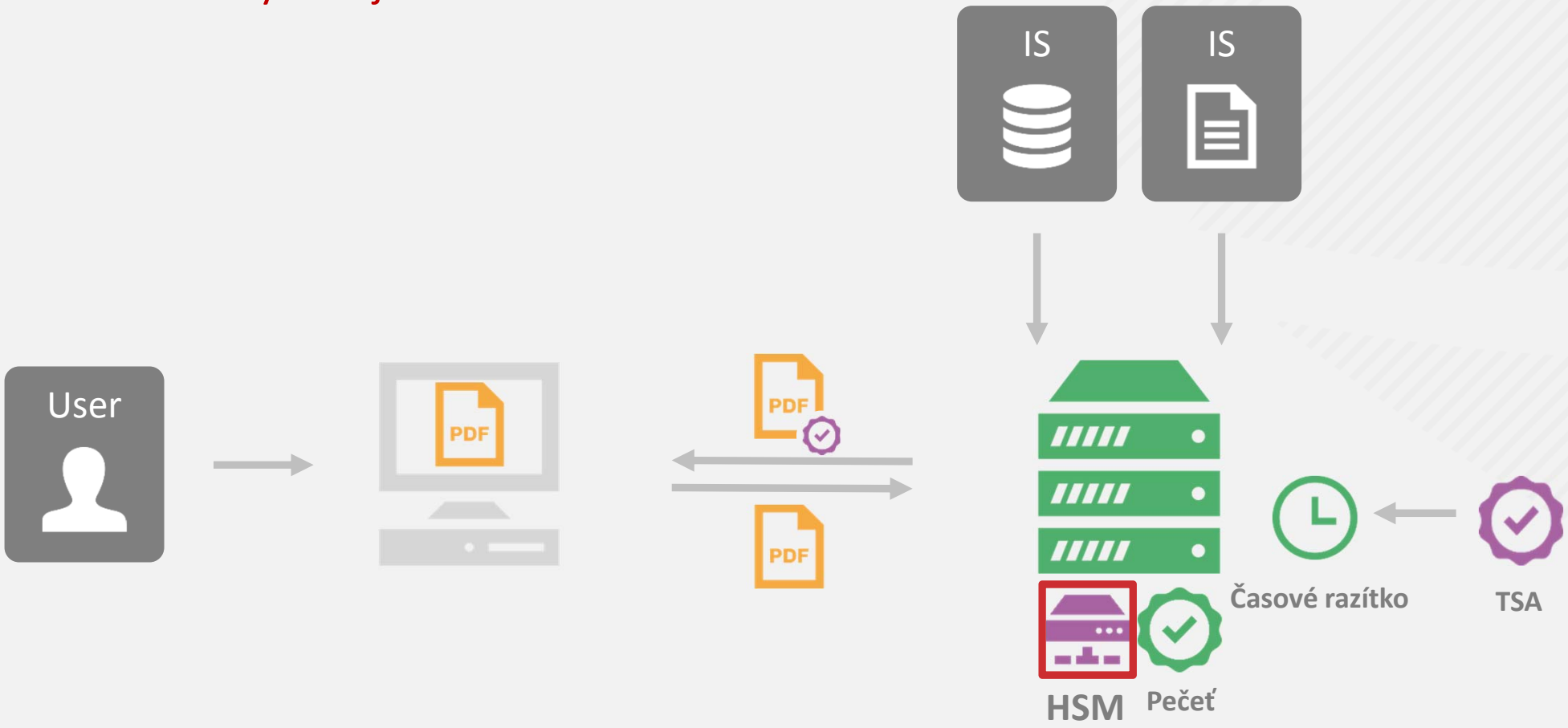
KVALIFIKOVANÁ PEČEŤ

Interní služba vytvářející důvěru - čipová karta



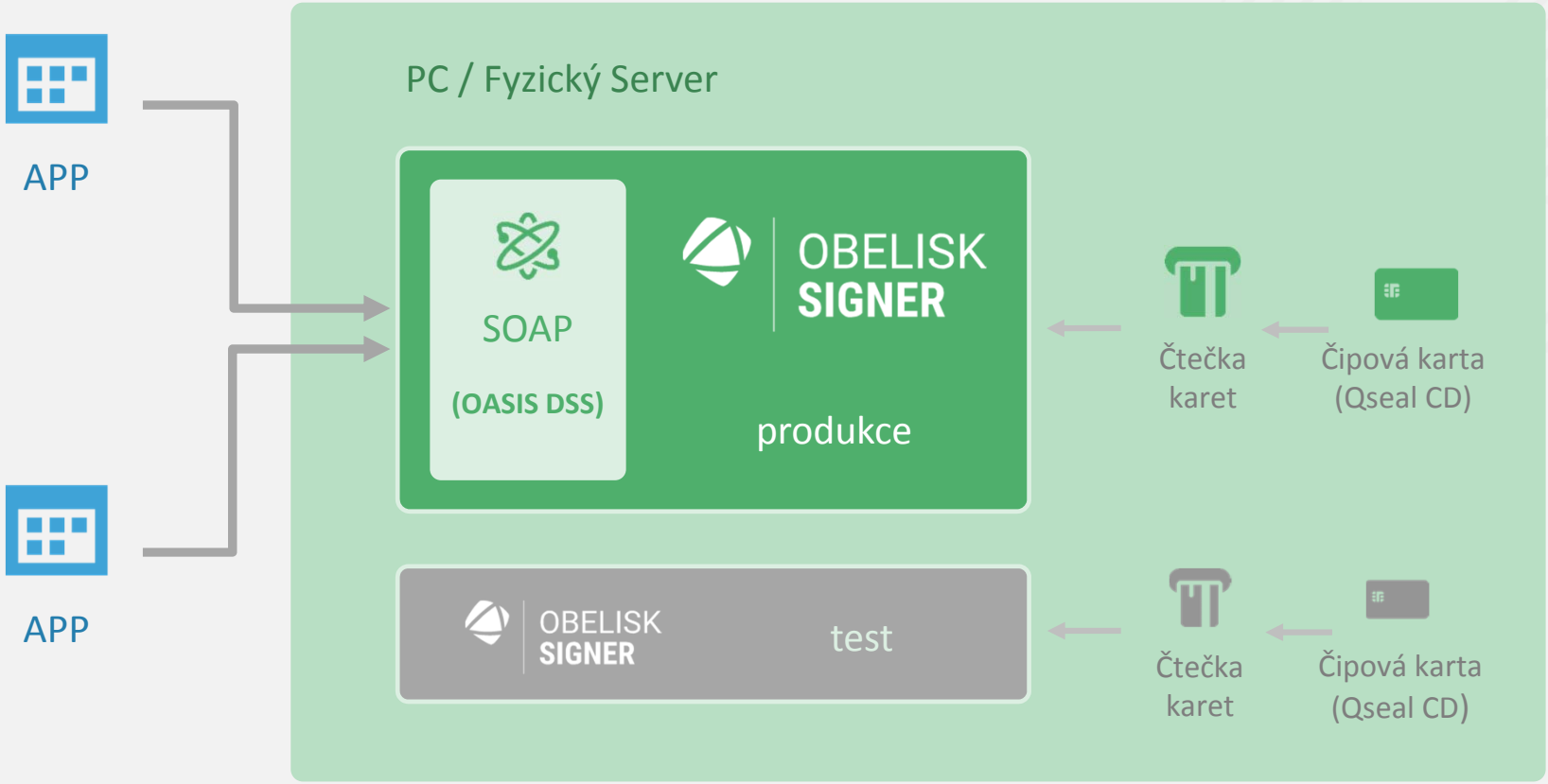
KVALIFIKOVANÁ PEČEŤ

Interní služba vytvářející důvěru – HSM



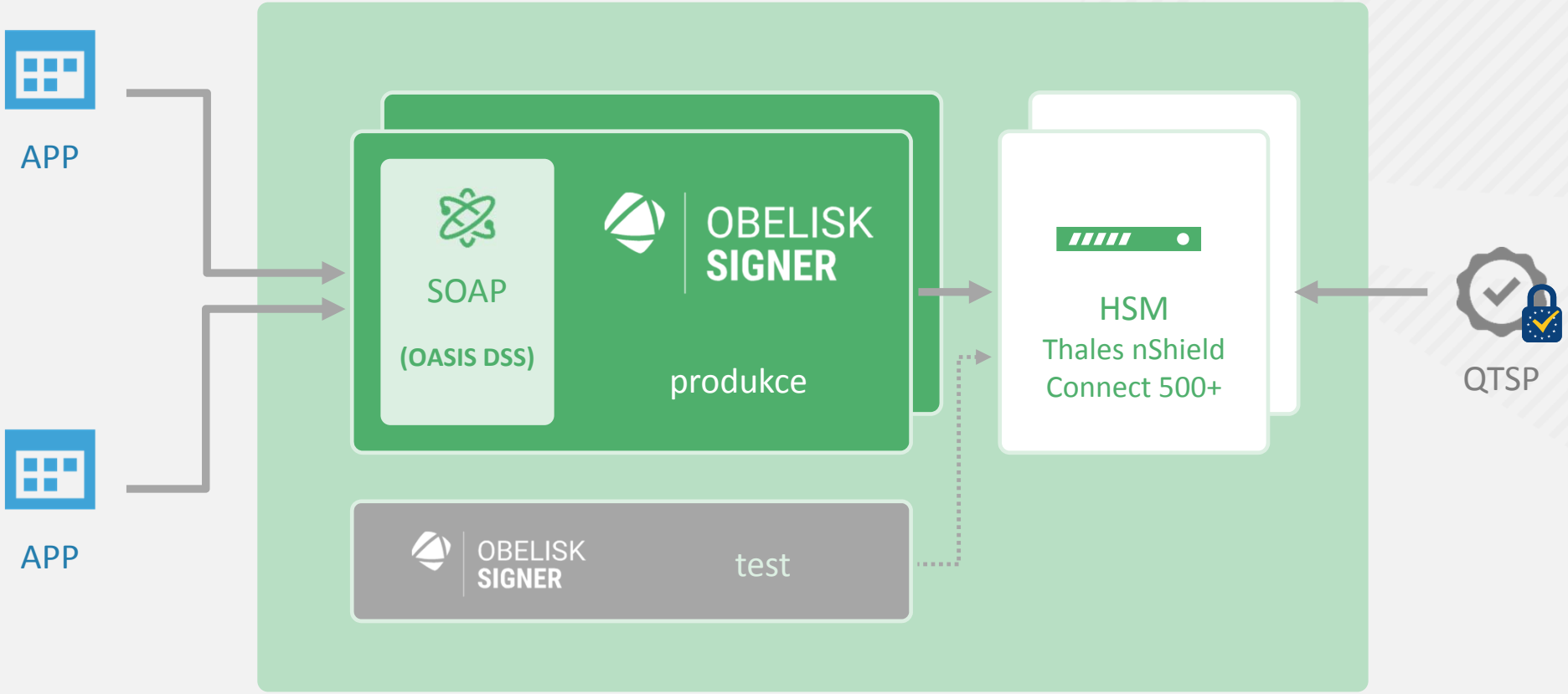
KVALIFIKOVANÁ PEČEŤ

Použití v aplikacích

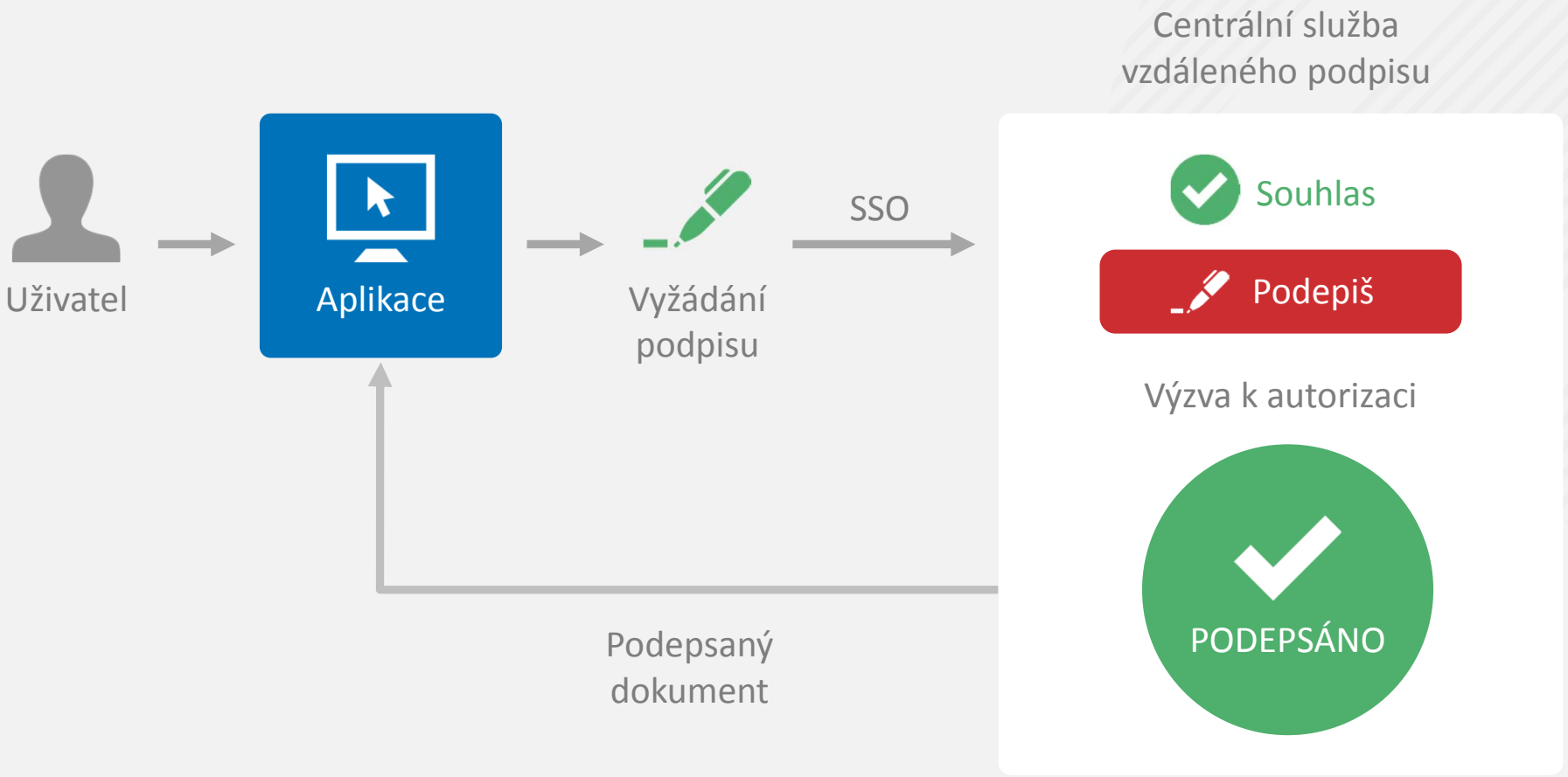


KVALIFIKOVANÁ PEČEŤ

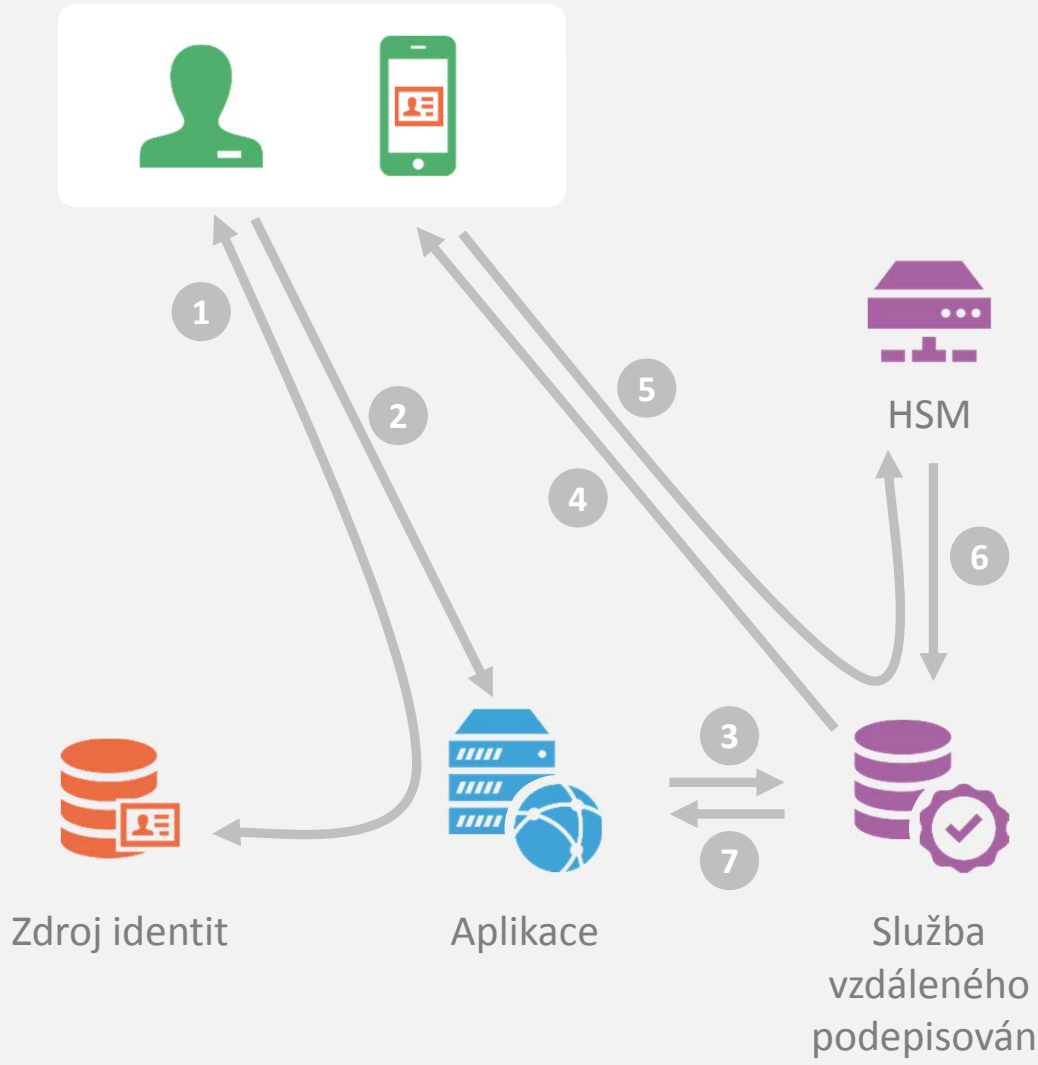
Použití v aplikacích



ELEKTRONICKÝ PODPIS JAKO INTERNÍ SLUŽBA



PROCES VZDÁLENÉHO PODPISU



1. Autentizace v Aplikaci
2. Vyžádání podepsání
3. Zahájení procesu podepisování
4. Požadavek na autorizaci požadavku
5. Autorizace použití soukromého klíče
6. Vygenerování elektronického podpisu v HSM
7. Vytvoření elektronicky podepsaného dokumentu a jeho předání aplikaci

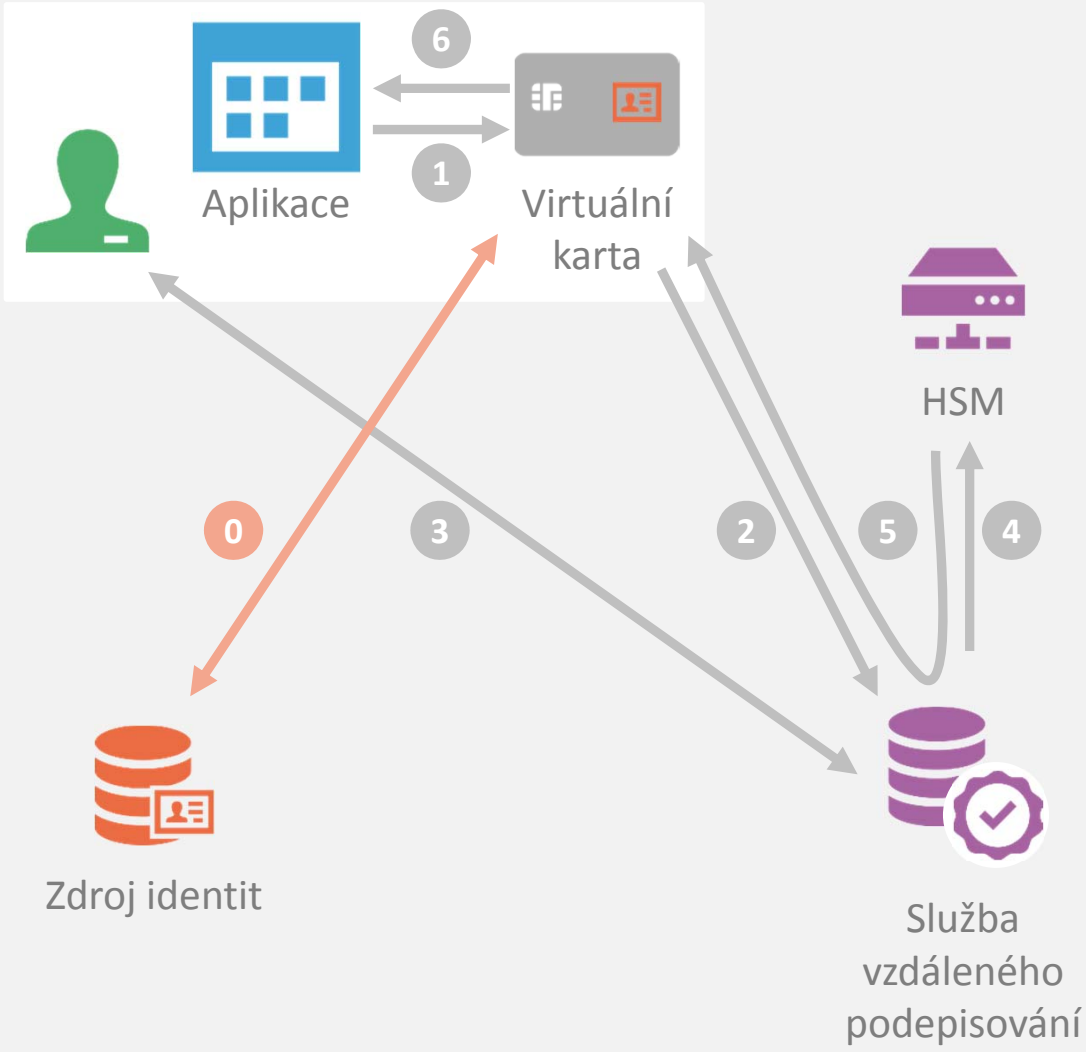
VIRTUÁLNÍ ČIPOVÁ KARTA

PostSignum

Užitečná aplikace pro vzdálený elektronický podpis

- ✔ Náhrada fyzické karty pro lokální aplikace
  - chování obdobné jako při vložení fyzické čipové karty do čtečky
- ✔ Aplikace není nutné jakkoliv upravovat
  - pokud již dnes podporují podepisování pomocí standardních rozhraní OS
- ✔ Vzdálený podpis jako přímá náhrada fyzické karty
  - vhodné například i do prostředí s virtualizovanými desktopy
- ✔ Překlenovací řešení do přechodu na aplikace s podporou mobilních platforem

VIRTUÁLNÍ ČIPOVÁ KARTA



0. Přihlášení k virtuální čipové kartě
1. Vyžádání podpisu v aplikaci pomocí standardního rozhraní
2. Požadavek na vyřízení podpisu centrální službou
3. Provedení autorizace požadavku uživatelem
4. Aktivace klíčů v HSM po autorizaci
5. Vygenerování elektronického podpisu v HSM a jeho předání přes virtuální čipovou kartu
6. Vytvoření elektronicky podepsaného dokumentu v aplikaci

ELEKTRONICKÝ PODPIS JAKO INTERNÍ SLUŽBA

PostSignum

Základní vlastnosti

- ✔ Zjednodušení elektronického podepisování na klientské straně
- ✔ Možnost použit jakékoliv zařízení i operační systém
- ✔ Bezpečně uložené privátní klíče v HSM modulu jako kvalifikovaném prostředku
- ✔ Použití silné identifikace a autorizace pro řízení přístupu ke klíčům

- ✔ Možnost dosažení úrovně **kvalifikovaného elektronického podpisu** při použití kvalifikovaného prostředku (HSM) a kvalifikovaných certifikátů od vhodného QTSP

KVALIFIKOVANÉ PROSTŘEDKY (QSCD) DLE NAŘÍZENÍ EIDAS

KVALIFIKOVANÝ PROSTŘEDEK

pro vytváření elektronických podpisů a pečetí (QSCD)

- ✔ eIDAS čl. 29 + příloha II
- ✔ QSCD = QSignCD nebo QSealCD
  - přičemž QSignCD seznamu dominuje
- ✔ Informativní EU seznam schválených QSCD*
  - tokeny, čipové karty i **HSM**

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

HSM – HARDWARE SECURITY MODULE

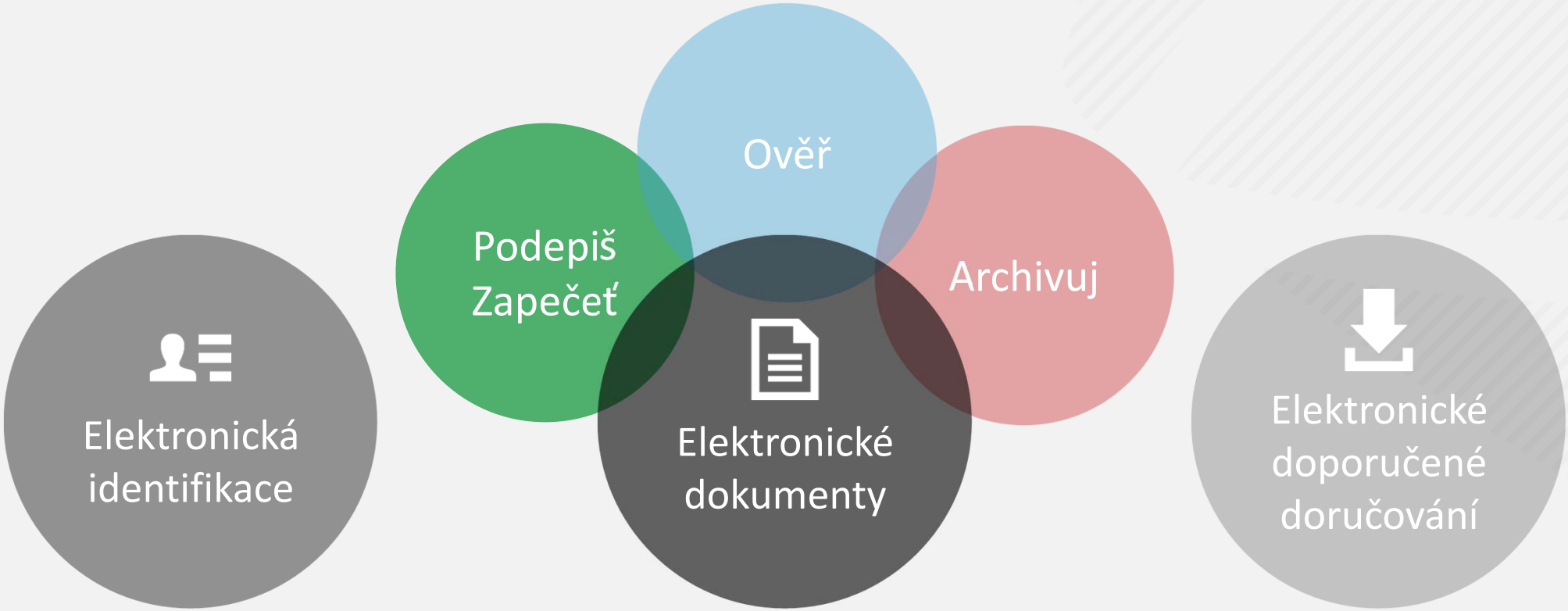
Pro vytváření kvalifikovaných podpisů a pečetí

- Specializované vysoce bezpečné zařízení pro:
  - **generování** silných kryptografických klíčů
  - **ochranu** privátních klíčů
  - poskytování **podepisovacích** a šifrovacích služeb
  - **správu** a **archivaci** kryptografických klíčů
- Typické způsoby nasazení HSM:
  - sdílené pro více serverů
  - nasazení v HA architektuře
  - podpora virtualizace (síťové varianty)

SLUŽBY VYTVÁŘEJÍCÍ DŮVĚRU

NAŘÍZENÍ EIDAS

Služby vytvářející důvěru

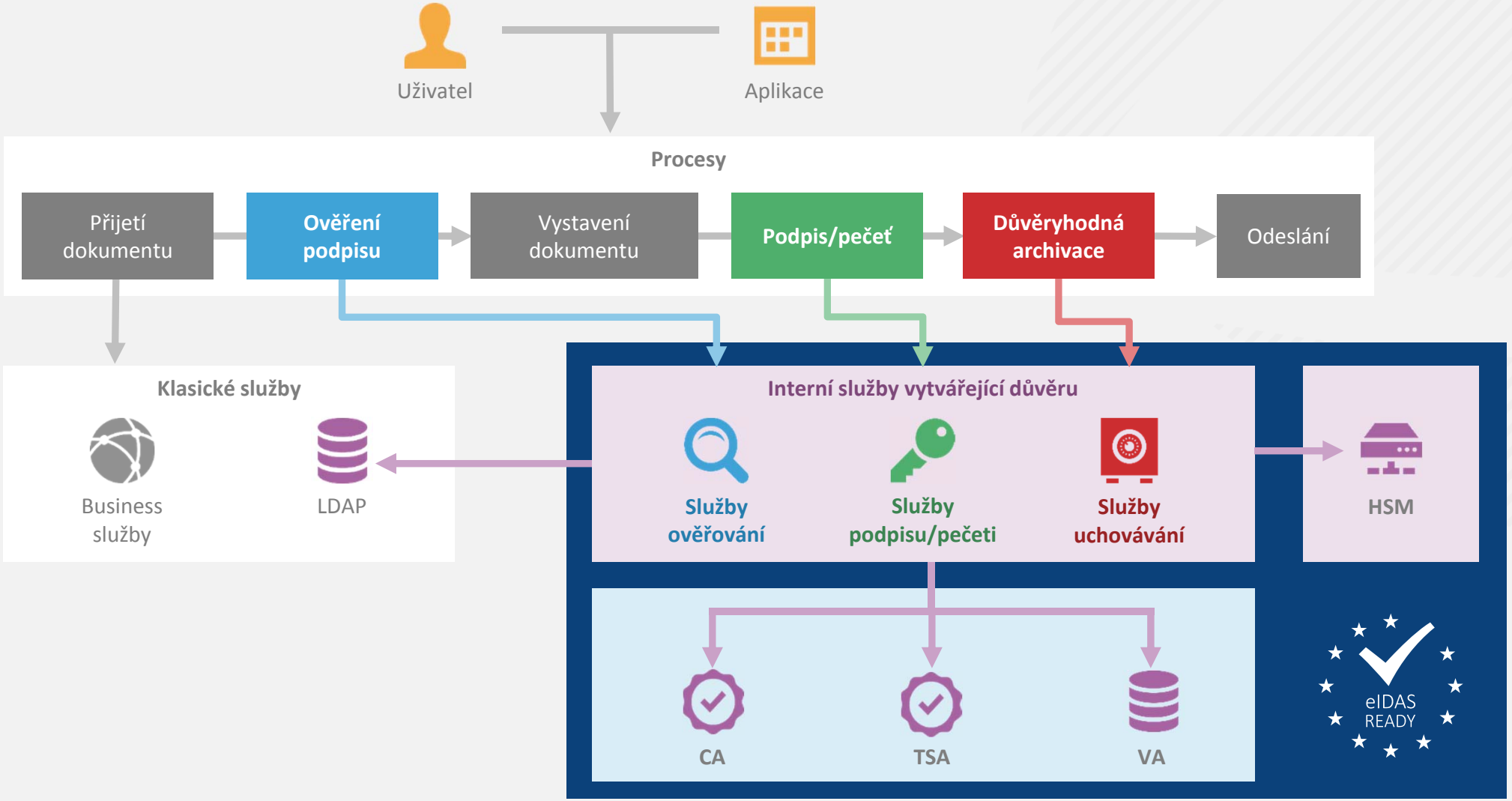


POVINNOSTI PŘICHÁZEJÍCÍ S NAŘÍZENÍM EIDAS A ZoSVD

Elektronický dokument a elektronický podpis

- ✔ Vytvářet kvalifikovaný elektronický podpis, pečeť, časové razítko
  - vyžaduje kvalifikovaný prostředek (čipová karta, token, HSM)
  - Vyžaduje kvalifikovaný certifikát
  - AdES formáty (PAdES, CAdES, XAdES)
- ✔ Ověřovat platnost elektronických podpisů, pečetí, časových razítek
  - dle nových standardů – rozšířený rozsah kontrol
  - pro všechny kvalifikované certifikáty z celé EU
- ✔ Zajistit dlouhodobé uchování el. podpisů, pečetí, časových razítek

UPLATNĚNÍ SLUŽEB VYTVÁŘEJÍCÍCH DŮVĚRU



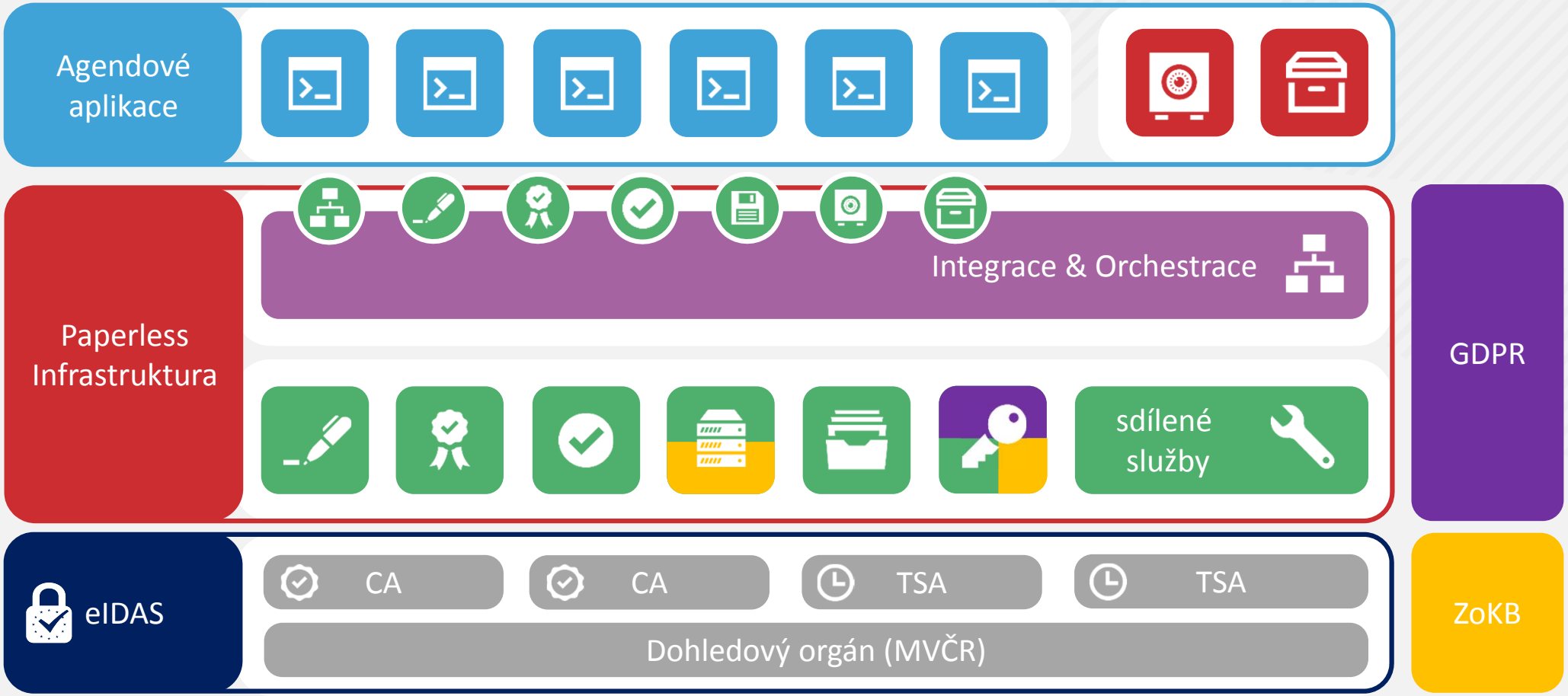
BEZPAPÍROVÁ ORGANIZACE

BEZPAPÍROVÁ ORGANIZACE

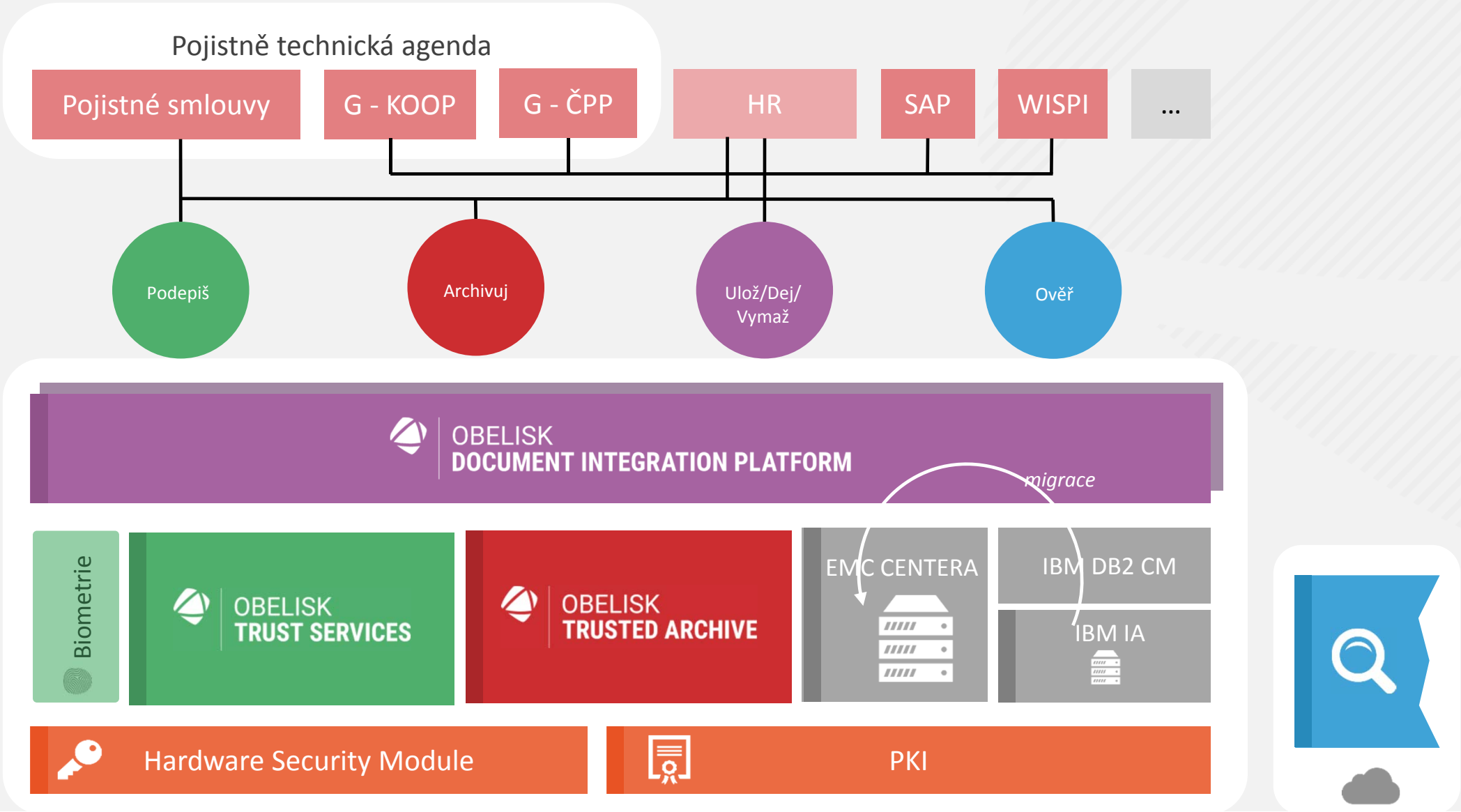
Od základů postupnými kroky k cíli

PAPERLESS INFRASTRUKTURA

Vrstva služeb mezi aplikacemi a zákonem definovanými elementy digitální důvěry

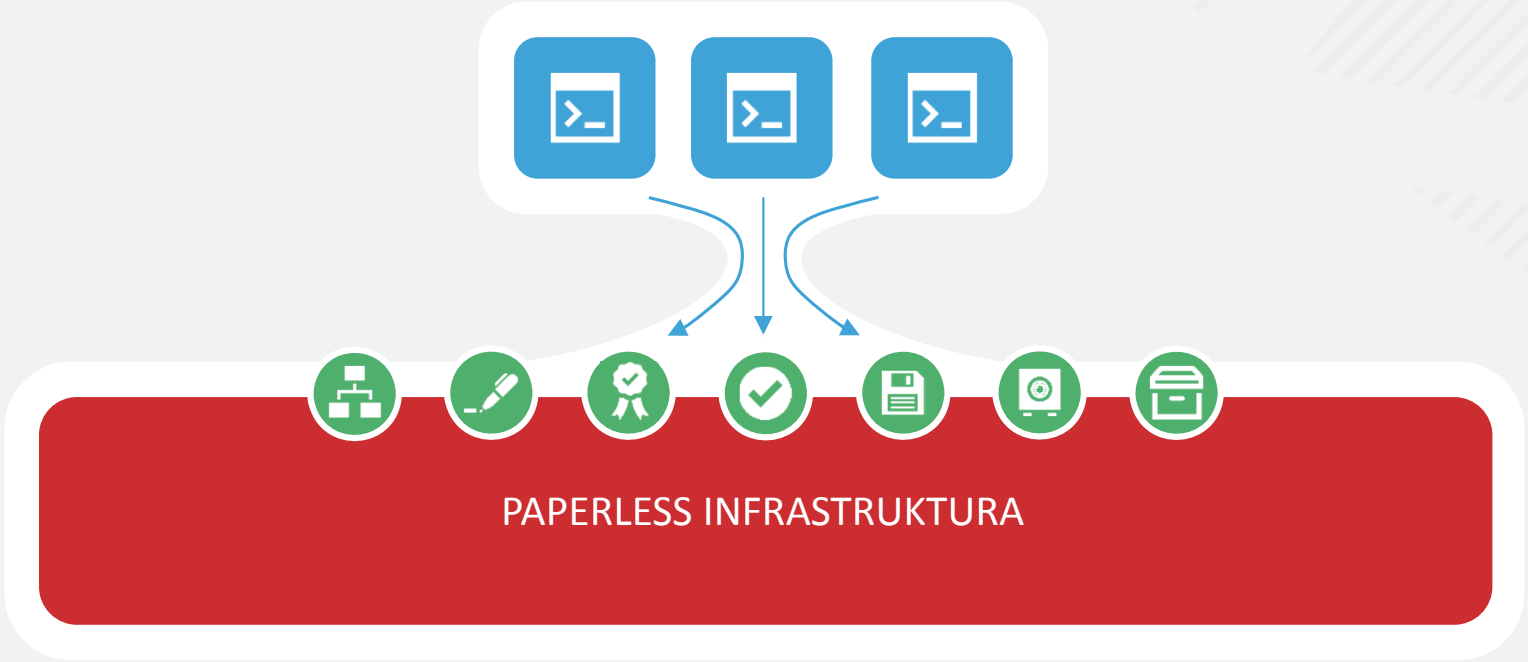


PAPERLESS INFRASTRUKTURA SKUPINY VIG

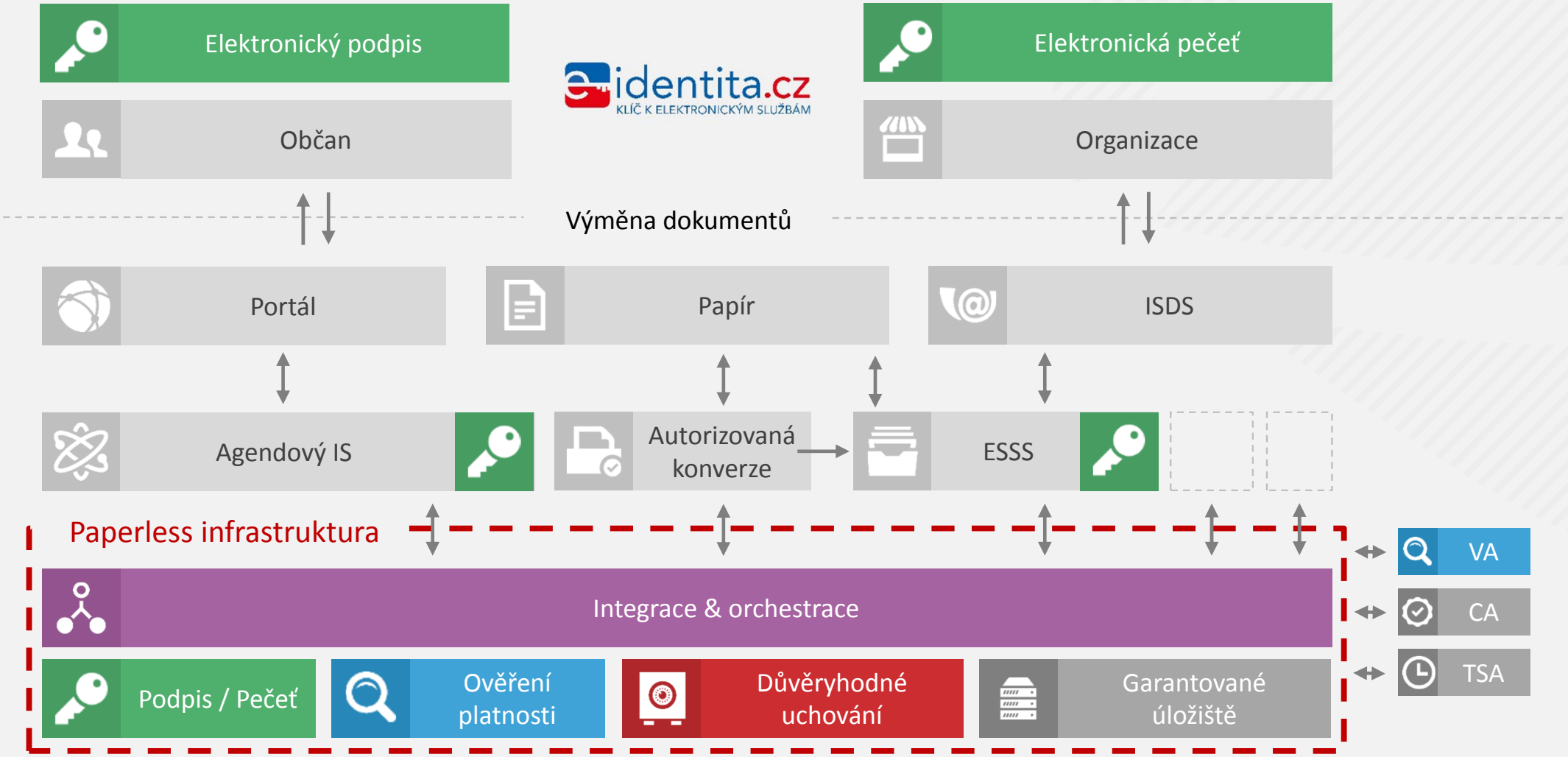


PAPERLESS INFRASTRUKTURA

Univerzální vrstva pro komplexní péči o veškeré elektronické dokumenty



BEZPAPÍROVÝ ÚŘAD



www.sefira.cz