



# VEŘEJNÁ SPRÁVA BEZ PAPÍRU

| Jan Tejchman | Senior Solution Consultant |



# MODERNÍ PAPERLESS



Digitální  
Evropa



Digitální  
transformace



Elektronické  
dokumenty



Právní  
validita



Služby vytvářející  
důvěru

Agendové  
aplikace

Digitální  
důvěra

Integruji agendové aplikace se světem digitální důvěry

# MODERNÍ PAPERLESS

---

## Infrastrukturní a integrační úloha



Agendové  
aplikace

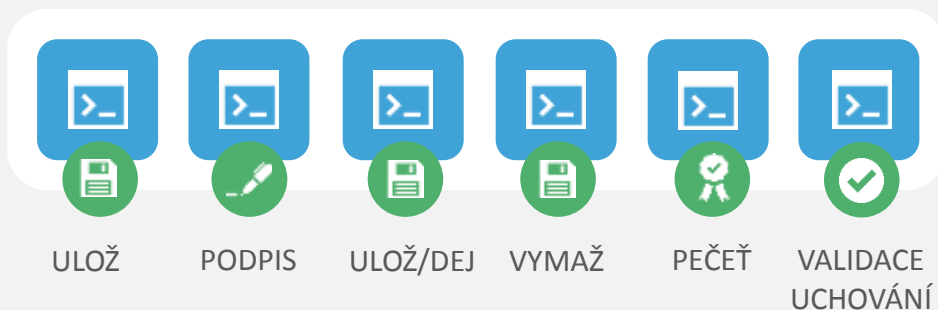


Infrastrukturní  
služby

# PAPERLESS

## Typické operace s elektronickými dokumenty

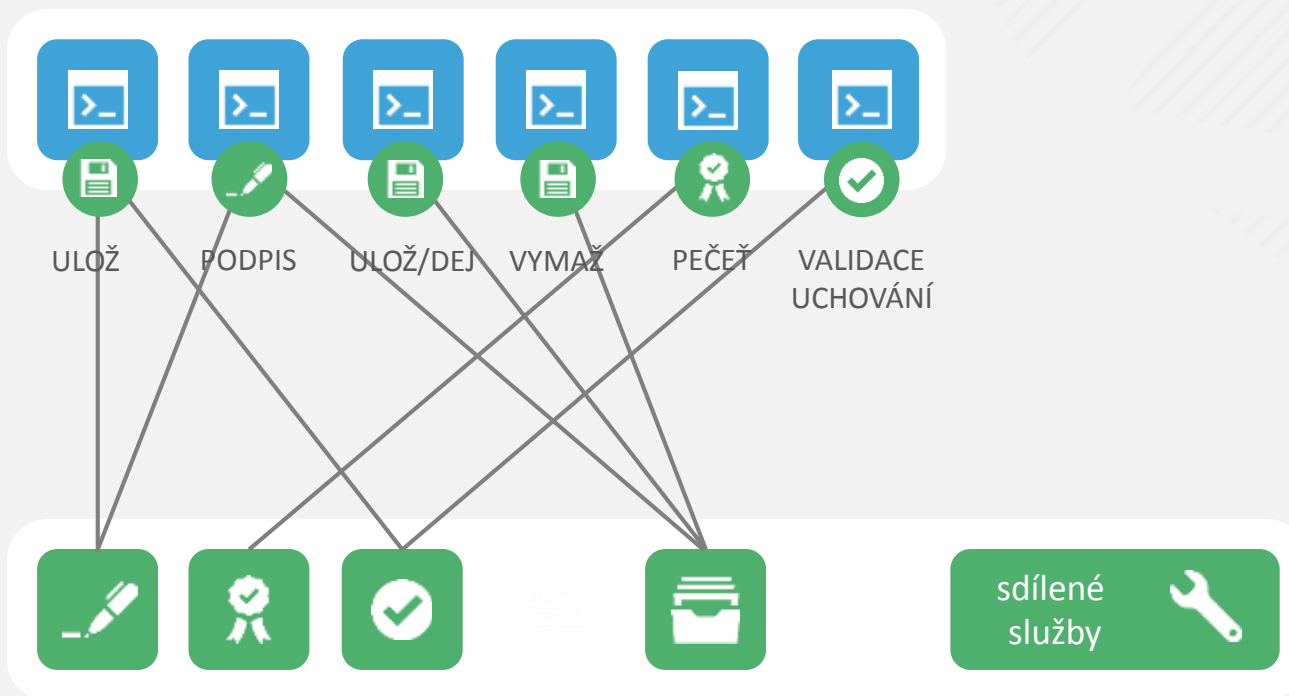
Agendové aplikace



# MODERNÍ PAPERLESS

## Infrastrukturní služby

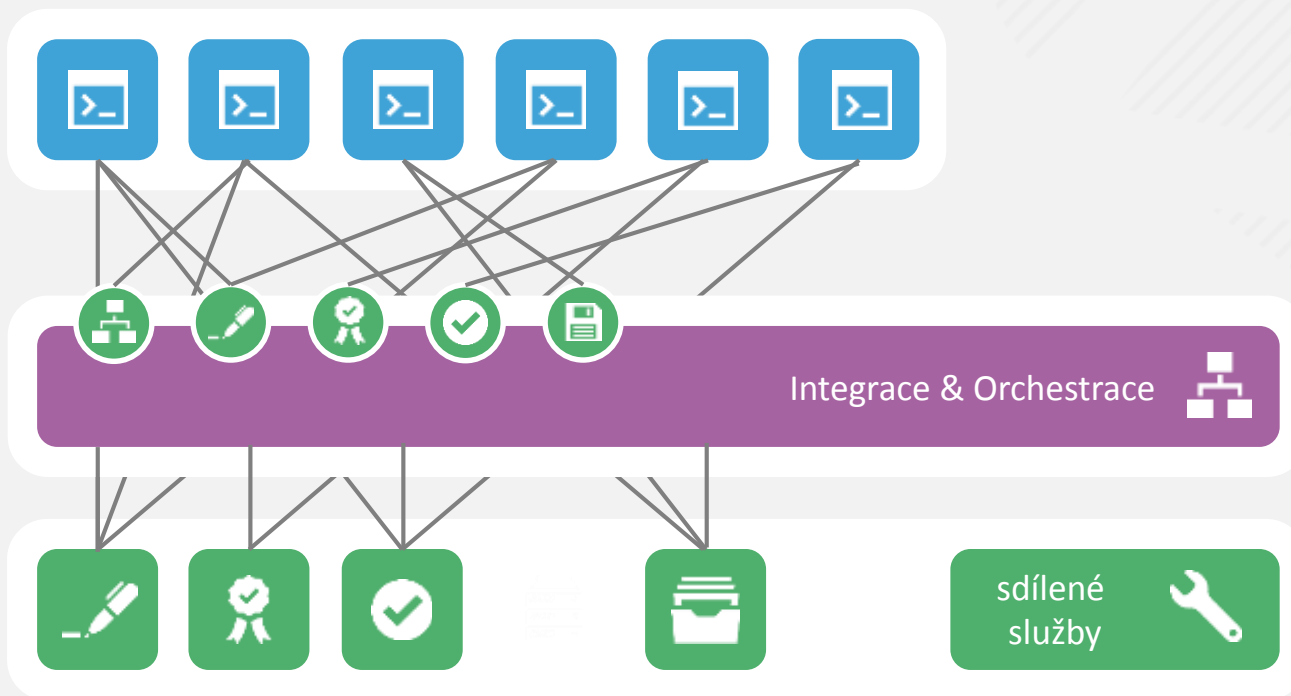
Agendové aplikace



# MODERNÍ PAPERLESS

## Integrace

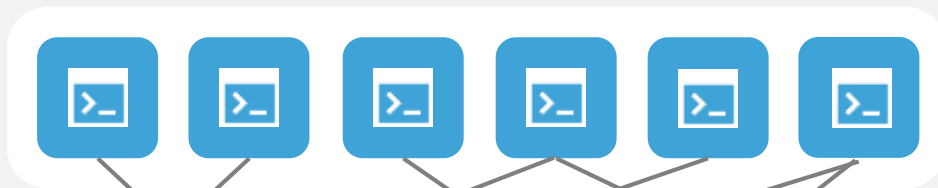
Agendové aplikace



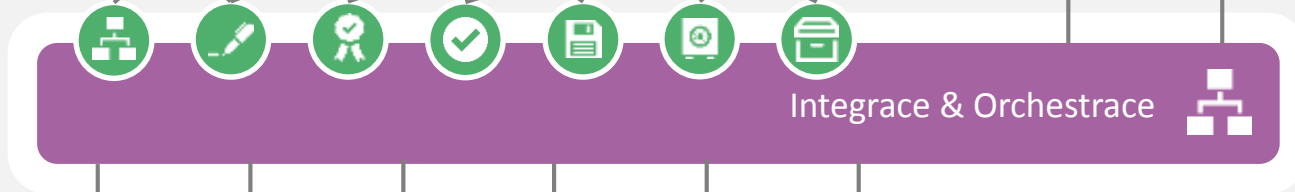
# MODERNÍ PAPERLESS

## Integrovaná paperless infrastruktura

Agendové aplikace



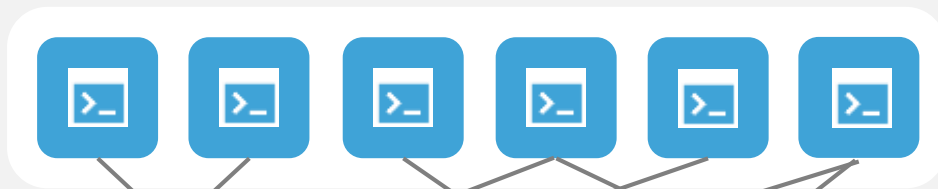
Kompozitní aplikace



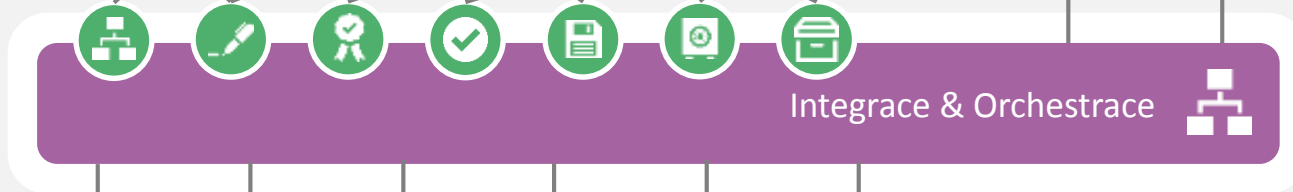
# MODERNÍ PAPERLESS

## Integrovaná paperless infrastruktura

Agendové aplikace



Kompozitní aplikace



Důvěryhodný dokument

Bezpečný a dostupný dokument



# MODERNÍ PAPERLESS

---

Jak na to



Všechny dokumenty



Implementovat služby  
Podepiš – Ověř – Archivuj

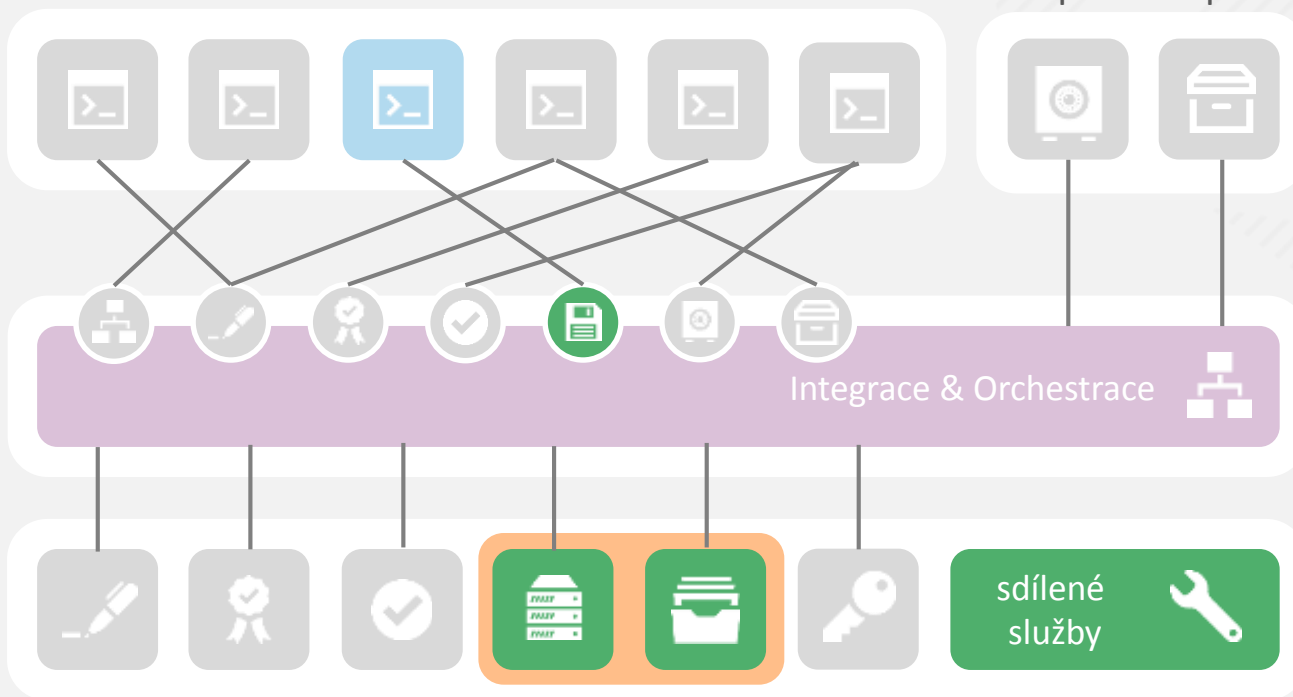


Ve shodě  
s legislativou

# KONSOLIDACE UKLÁDÁNÍ

Agendové aplikace

Kompozitní aplikace

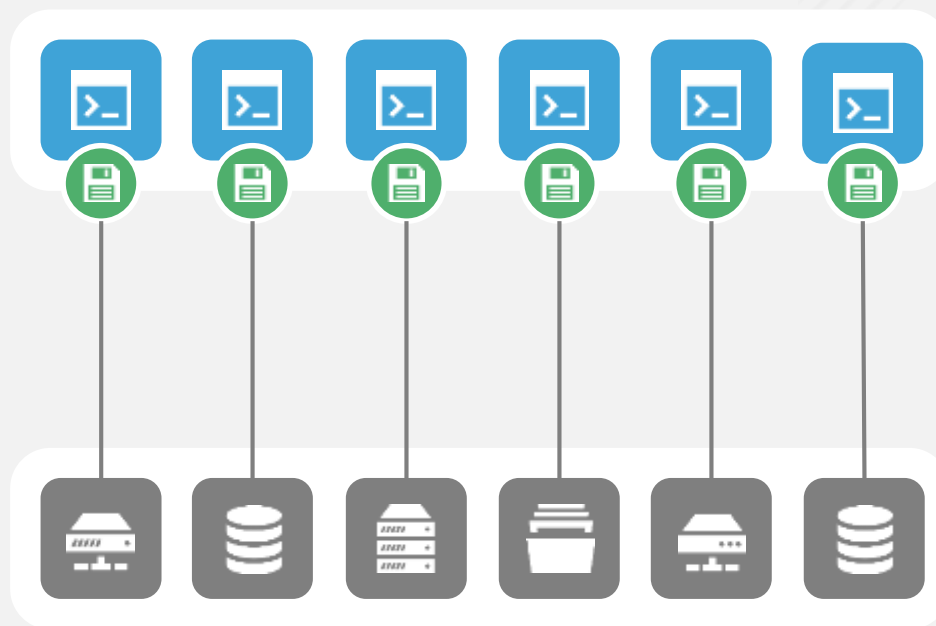


Bezpečný a dostupný dokument

# KONSOLIDACE UKLÁDÁNÍ

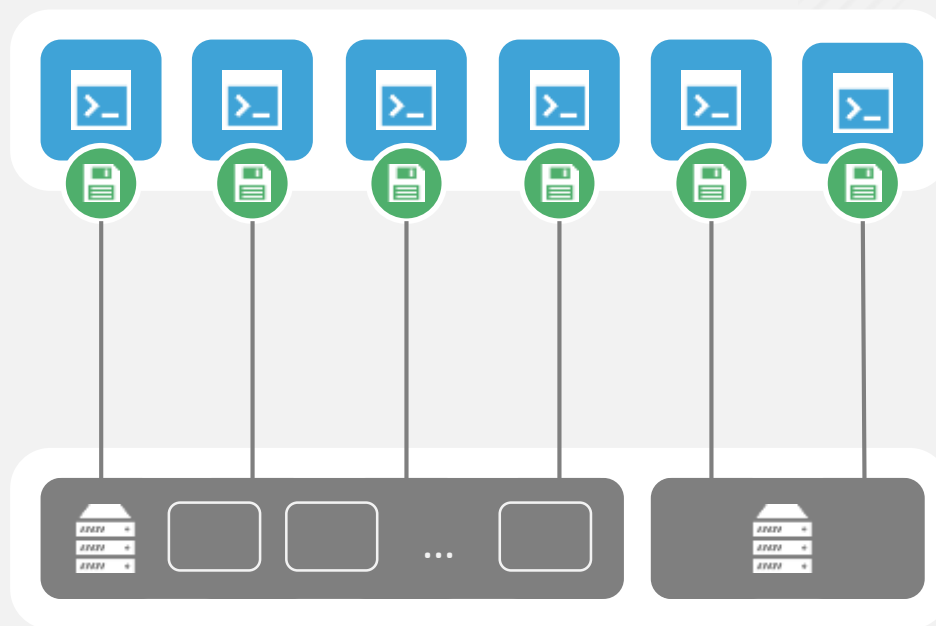
---

Roztříštěnost



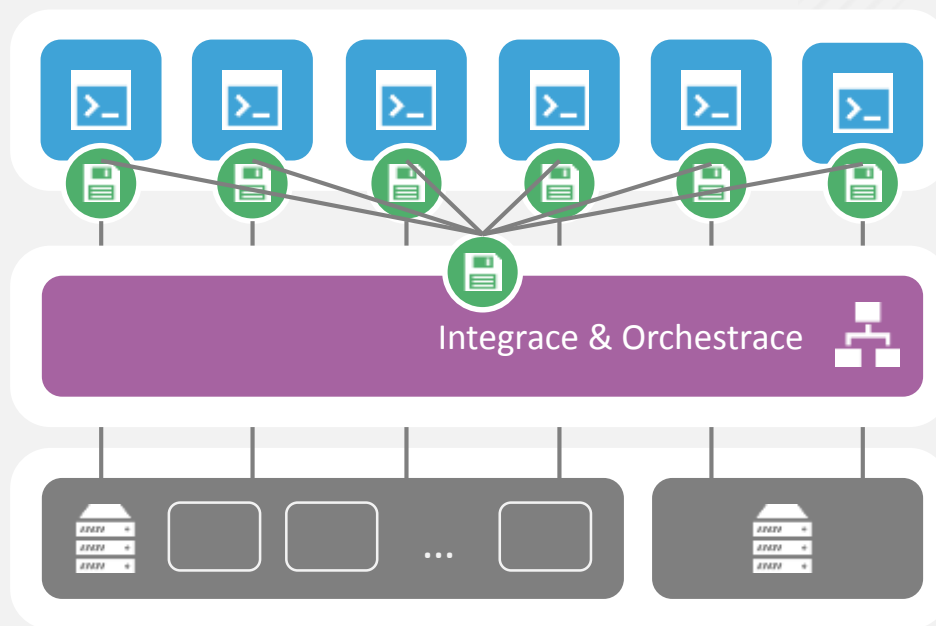
# KONSOLIDACE UKLÁDÁNÍ

## Konsolidace



# KONSOLIDACE UKLÁDÁNÍ

## Abstrakce

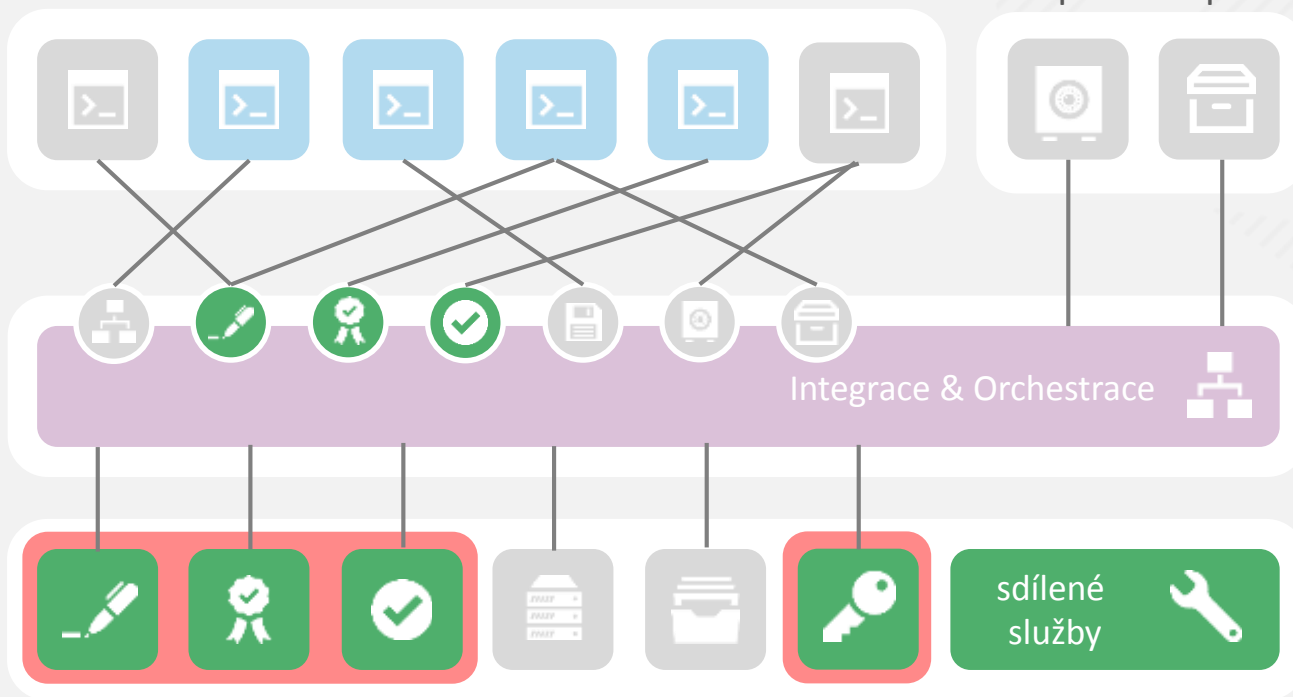


# DIGITÁLNÍ DŮVĚRA

## Služby vytvářející důvěru

Agendové aplikace

Kompozitní aplikace

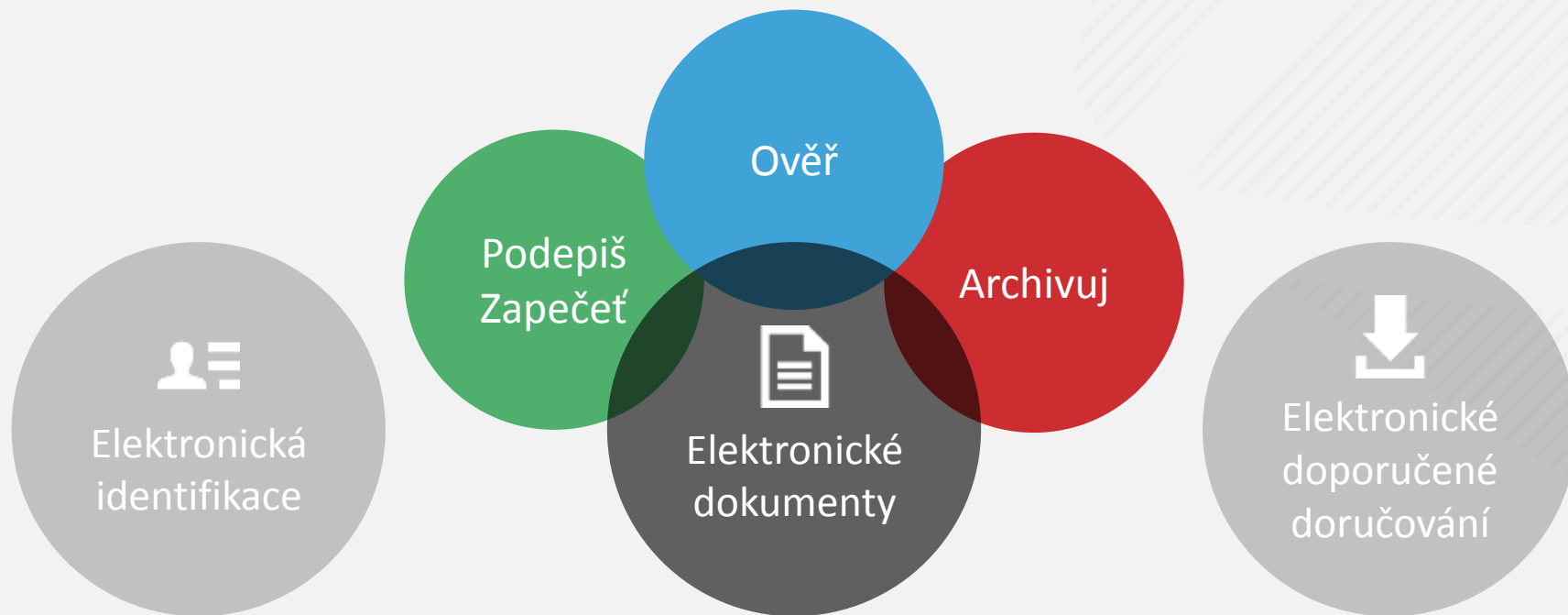


Důvěryhodný dokument

# EIDAS - SLUŽBY VYTVÁŘEJÍCÍ DŮVĚRU

---

## Elektronické dokumenty



# ELEKTRONICKÝ PODPIS VS. PEČEŤ

PODEPIŠ

## Rozlišení účelu použití



### Podpis

prostředek vyjádření  
vůle/souhlasu člověka



### Pečeť

prokázání původu dokumentu  
(OVM, právnické osoby)



# ÚROVNĚ ELEKTRONICKÝCH PODPISŮ

PODEPIŠ

dle Zákona o službách vytvářejících důvěru



## Kvalifikovaný

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



## Uznávaný

- AdES
- Certifikát vydaný kvalifikovaným poskytovatelem služeb



## Ostatní typy

- Zaručený (AdES)  
nebo
- Biometrický  
nebo
- Prostý

# ZÁKONEM VYŽADOVANÉ ÚROVNĚ PODPISU

PODEPIŠ

Matice použití typů elektronických podpisů v praxi

od \ pro	Státní správa	Občan	Komerce
Státní správa	Kvalifikovaný	Kvalifikovaný	Kvalifikovaný
Občan	Uznávaný	Libovolný typ	Libovolný typ
Komerce	Uznávaný	Libovolný typ	Libovolný typ

# KVALIFIKOVANÝ PROSTŘEDEK

PODEPIŠ

pro vytváření elektronických podpisů (QSCD)

- ✓ eIDAS čl. 29 + příloha II
- ✓ EU seznam schválených QSCD\*
  - tokeny, čipové karty i HSM



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

# HSM – KVALIFIKOVANÝ PROSTŘEDEK

PODEPIŠ

pro vytváření kvalifikovaných podpisů a pečeti (QSCD)

- ✓ 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)



# ELEKTRONICKÝ PODPIS JAKO SLUŽBA

PODEPIŠ



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

# OVĚŘENÍ PLATNOSTI

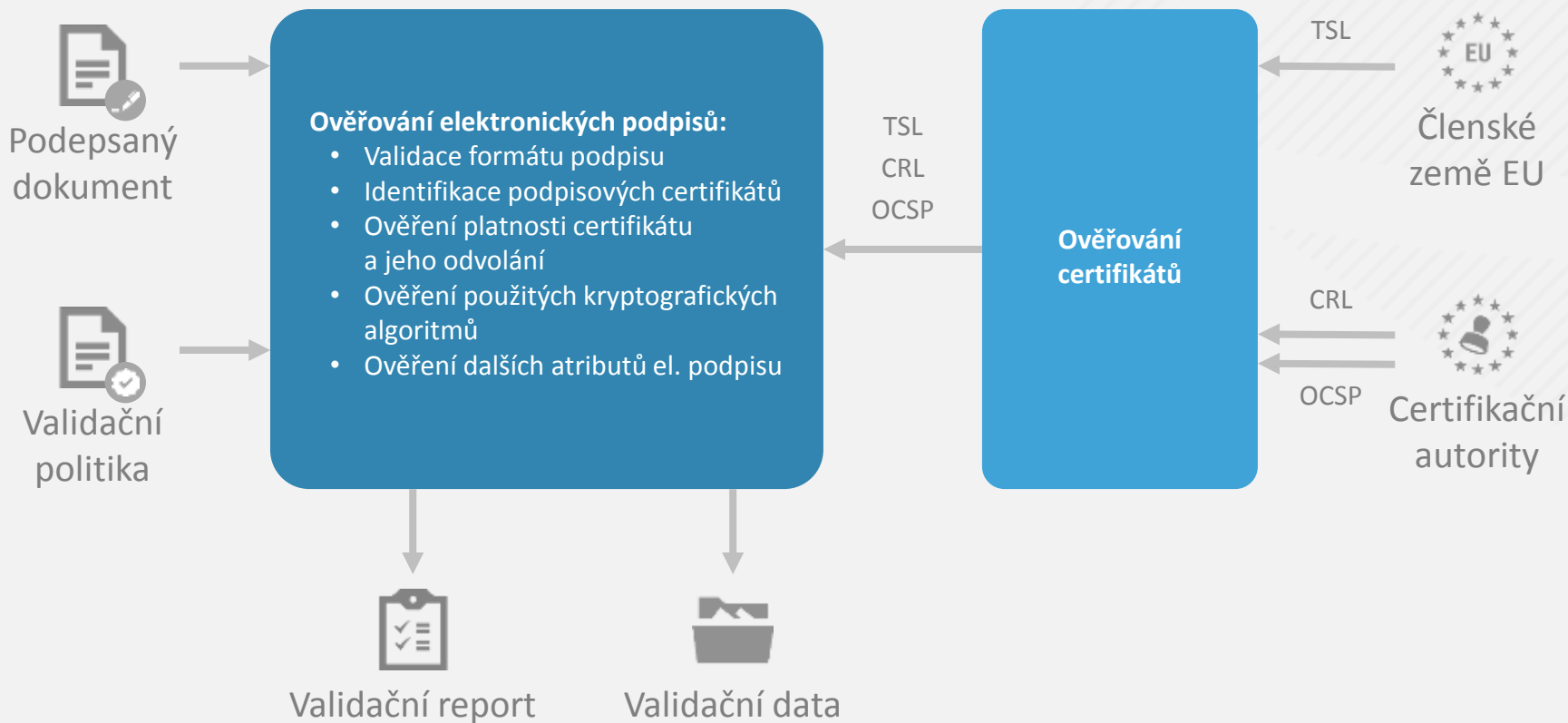
---

## Požadavky na ověření platnosti elektronických podpisů, pečetí, časových razítek

- ✓ Schopnost ověřovat platnost napříč EU
- ✓ Formáty, algoritmy, integrita, certifikáty, ...
- ✓ Validací report, validační data
- ✓ Archivační politiky – vlastnosti podpisu
  - Formáty (AdES, PDF/A, ZFO, ...)
  - Úrovně (kvalifikovaný, uznávaný)

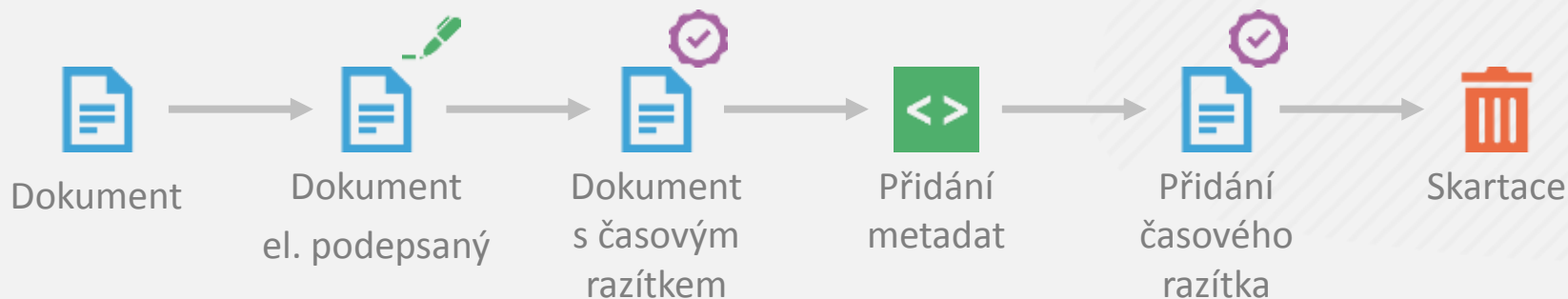
# OVĚŘOVÁNÍ PLATNOSTI PODPISŮ A PEČETÍ

OVĚŘ



# ŘEŠENÍ DLOUHODOBÉ PLATNOSTI

ARCHIVUJ



## ✓ Podpis + razítko + přerazítkování

- Integrita
- Identifikace podepsaného
- Nepopiratelnost
- Fixace v čase
- Udržení dlouhodobé kontinuity

## ✓ Co ještě musíme řešit?

- Je podpis opravdu platný?
- Jak poznáme za 5, 10, 15 a více let, že je platný?



# UCHOVÁVÁNÍ PODPISŮ A PEČETÍ

## Služba vytvářející důvěru

- ✓ eIDAS definuje uchovávání podpisů a pečetí (ne uchovávání dokumentů)
  - správně uchovaný el. podpis prokazuje důvěryhodnost dokumentu
  - je nutné zajistit bezpečné uložení dat a dokumentů
- ✓ Zajistí důvěryhodnost i po vypršení platnosti certifikátu
- ✓ Mohu realizovat uchovávání vlastními prostředky a službami
- ✓ Referenční normy a standardy ETSI

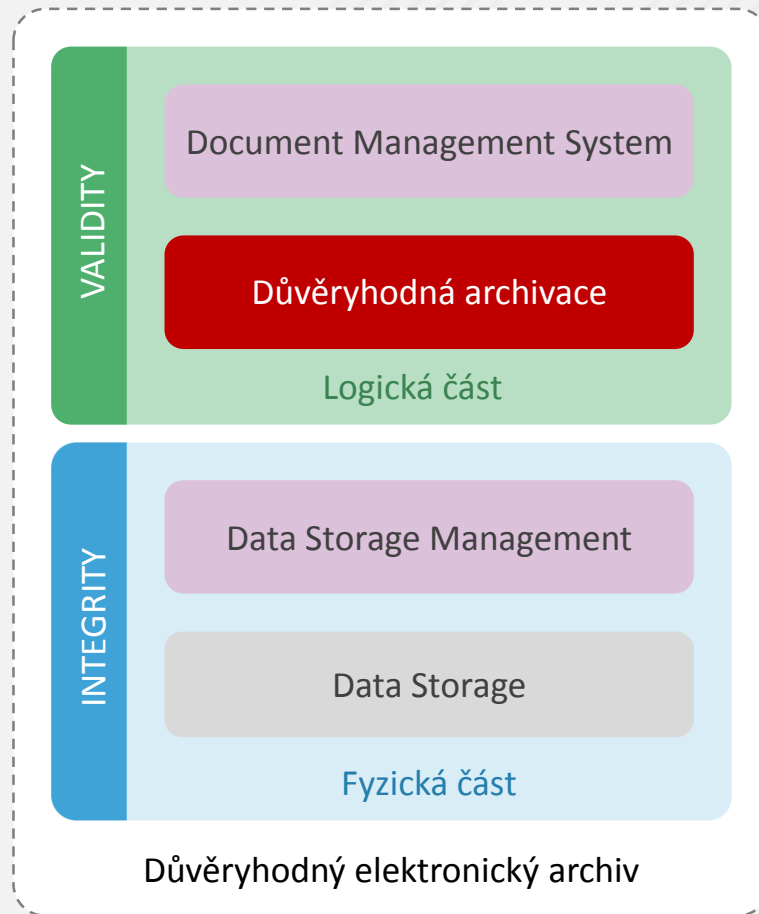
# DŮVĚRYHODNÝ ELEKTRONICKÝ ARCHIV

## ✓ Logická část

- důvěryhodnost
- legislativní platnost
- průkaznost i mimo fyzické úložiště
- sdílení důvěryhodnosti s okolím

## ✓ Fyzická část

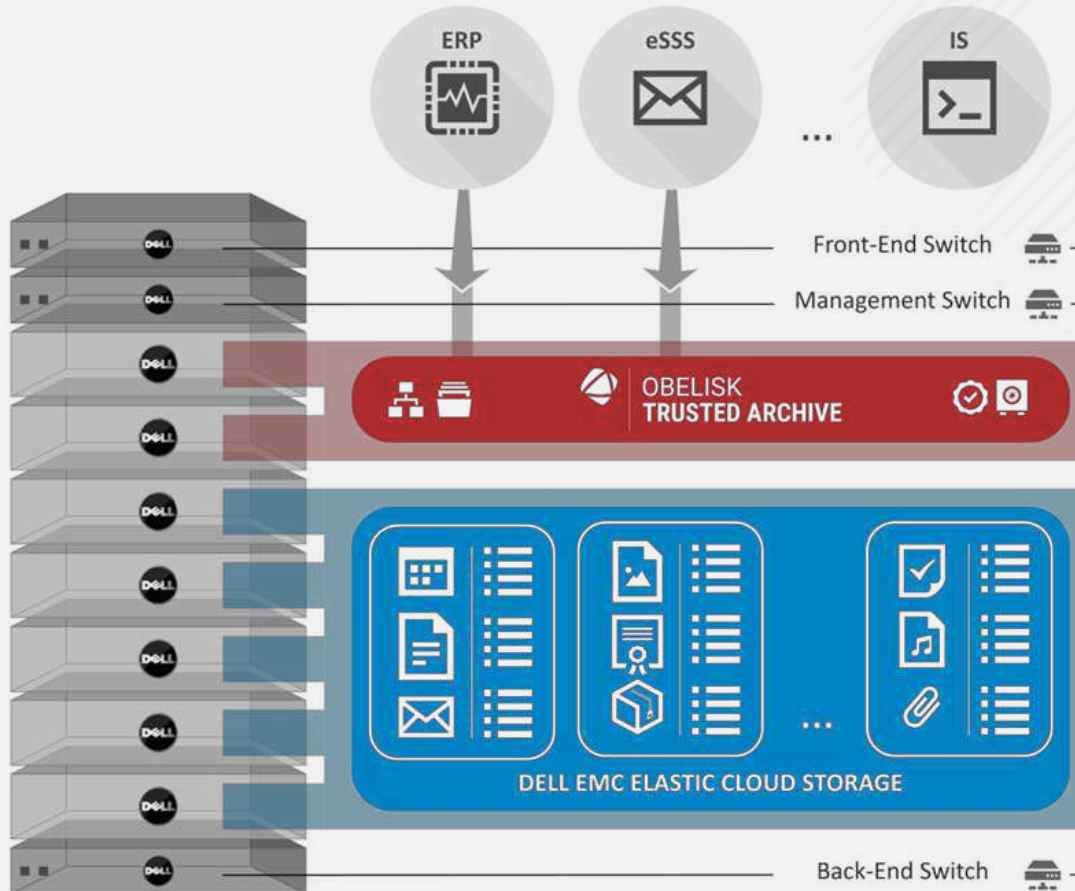
- neměnnost
- nesmazatelnost
- replikace
- automatická detekce a oprava
- bezpečná skartace



# DIGITÁLNÍ ARCHIV

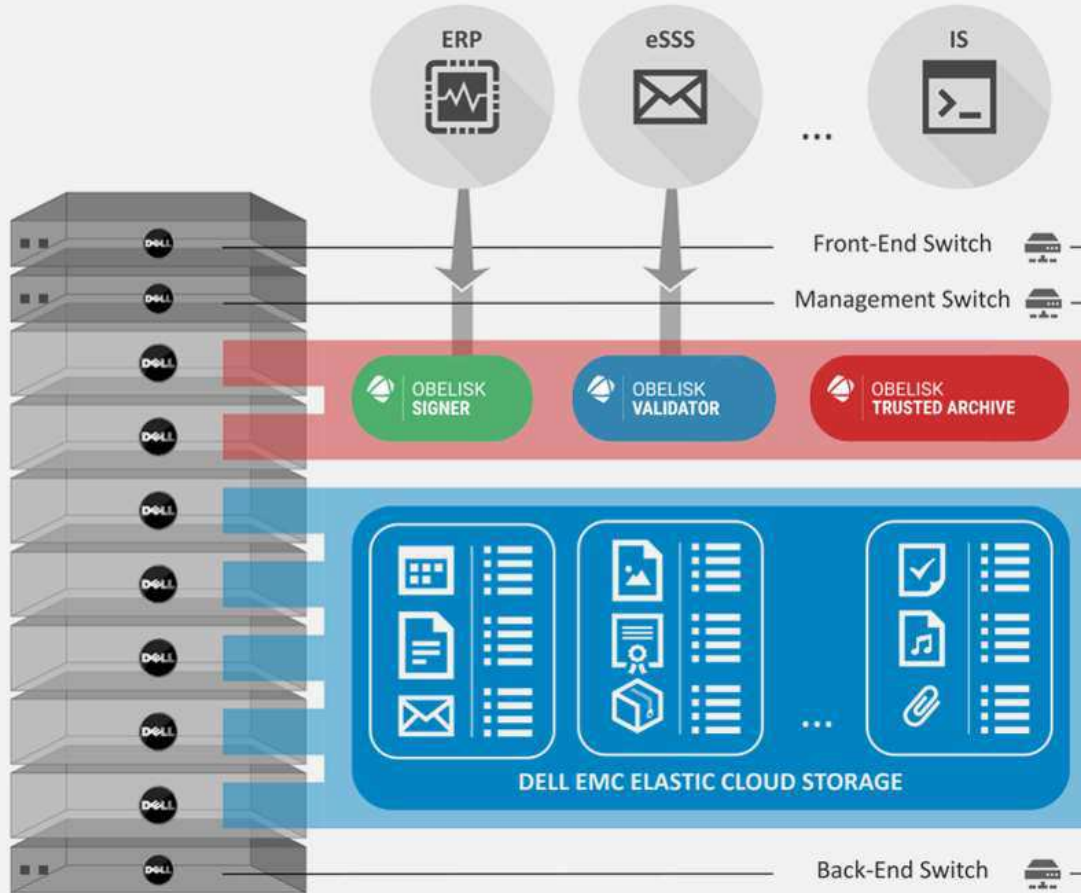
ARCHIVUJ

## OBELISK TA & Dell EMC ECS



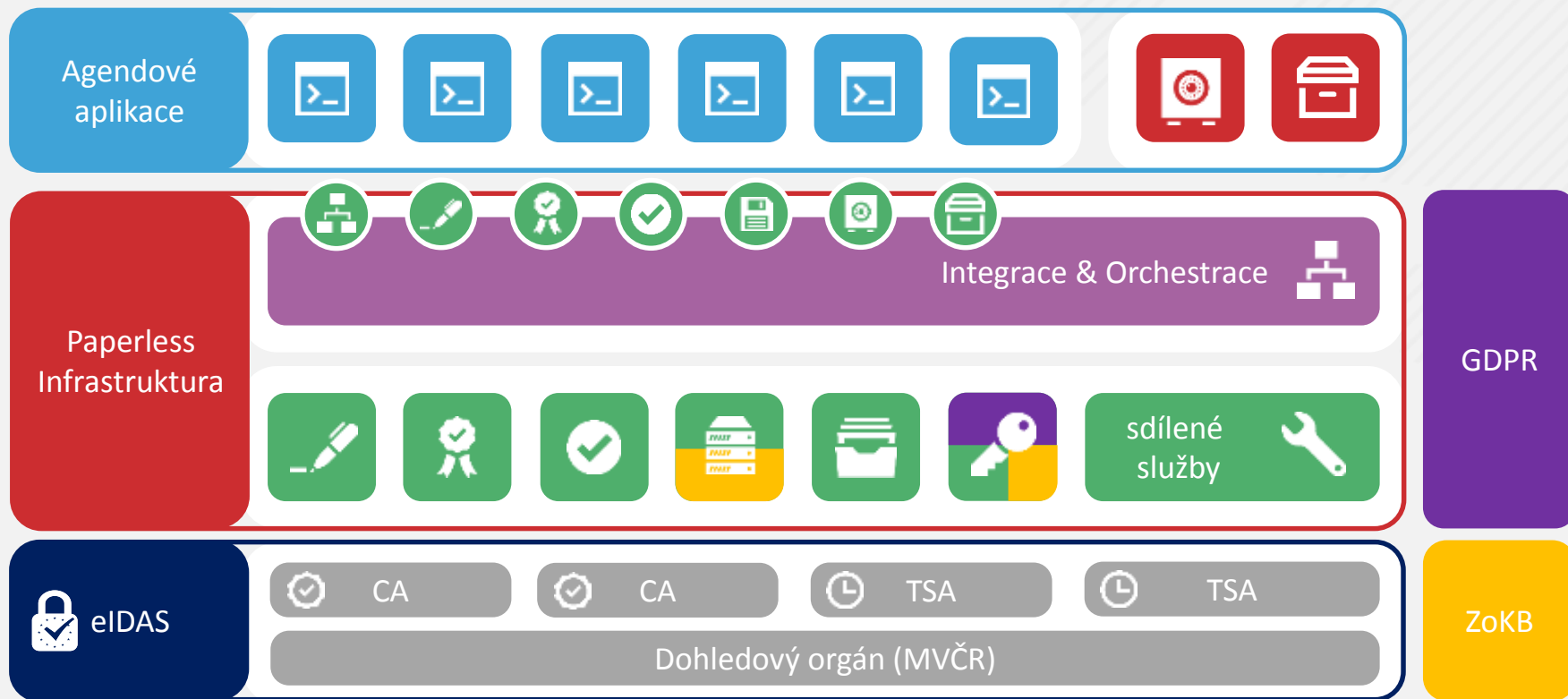
# PAPERLESS APPLIANCE

## OBELISK & DellEMC ECS



# PAPERLESS INFRASTRUKTURA

Vrstva služeb mezi aplikacemi a zákonem definovanými elementy digitální důvěry

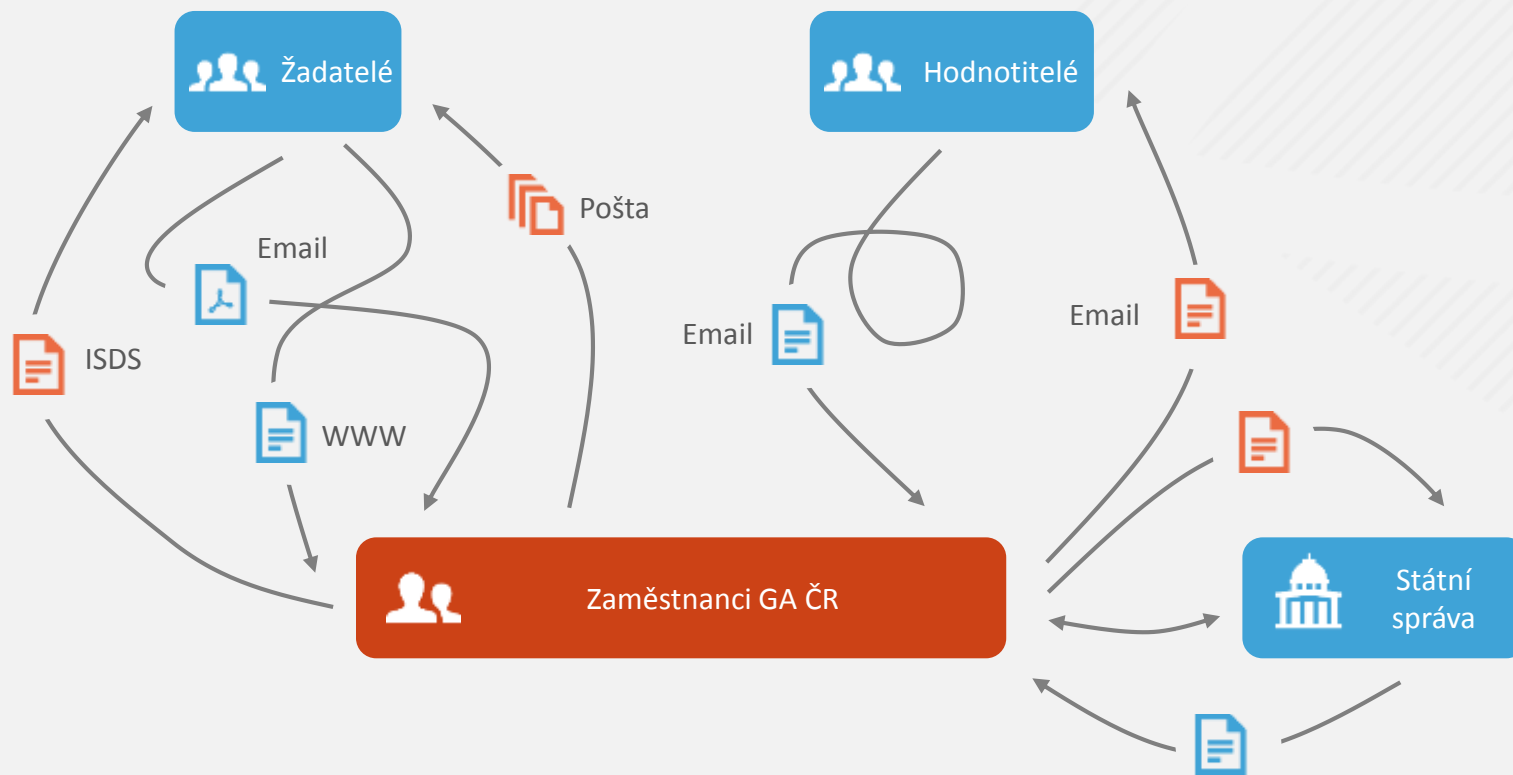


## Cíle

- ✓ Financovat vědecké projekty
- ✓ Podporovat mezinárodní vědeckou spolupráci
- ✓ Vytvářet v rámci platných zákonů co nejlepší podmínky pro administrativní zpracování žádostí a projektů

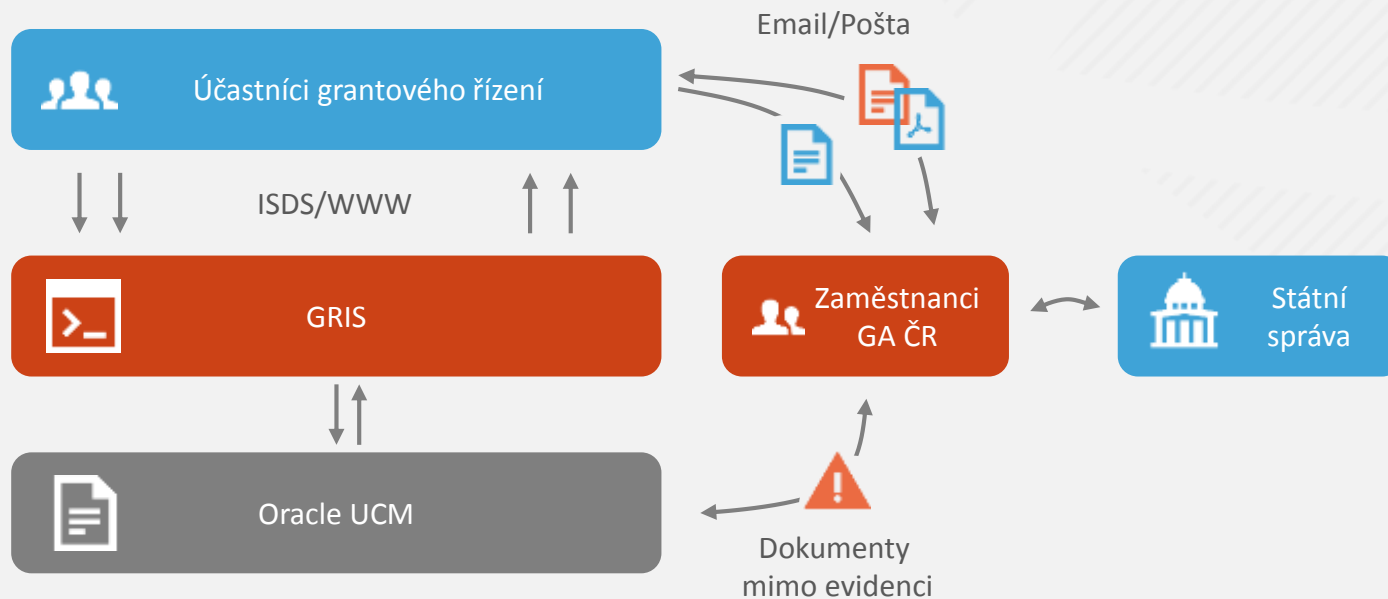
# GRANTOVÁ AGENTURA ČESKÉ REPUBLIKY

## Grantové řízení



# GRANTOVÁ AGENTURA ČESKÉ REPUBLIKY

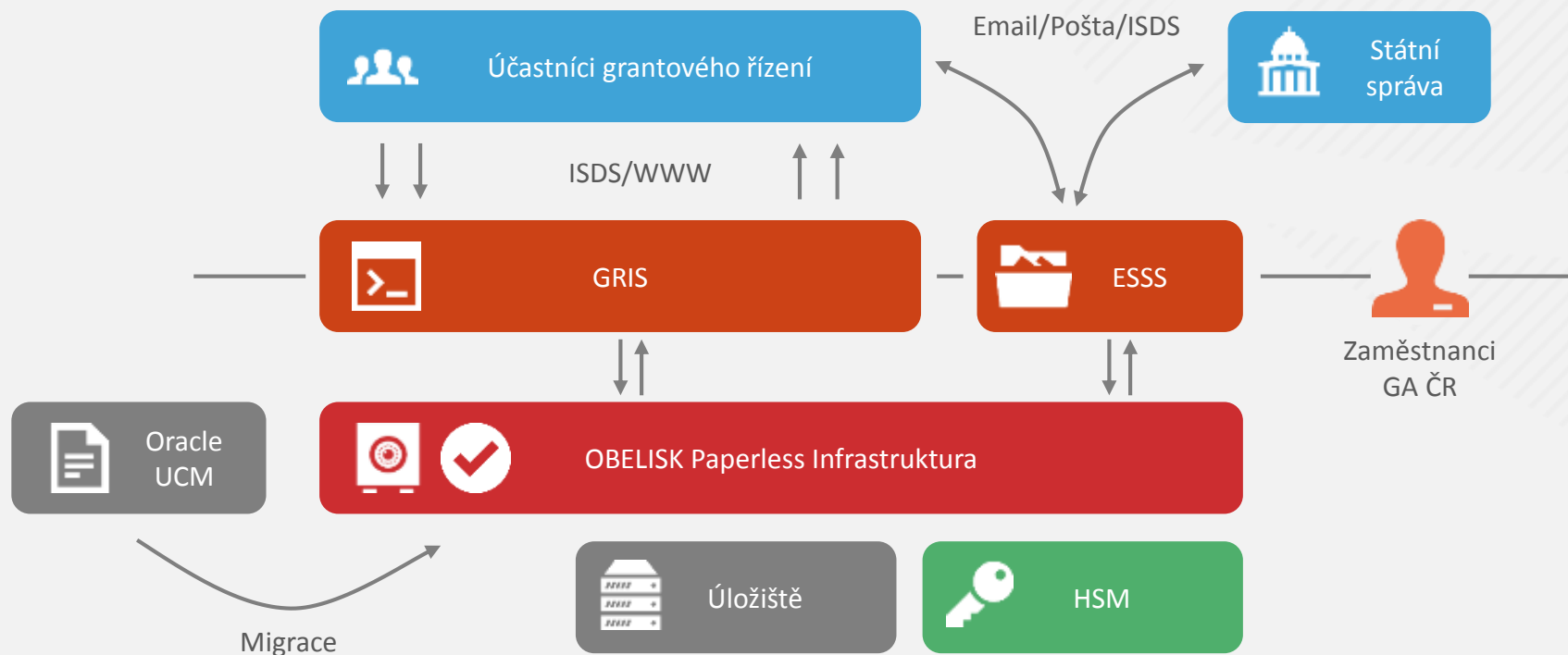
## Agendový systém GRIS



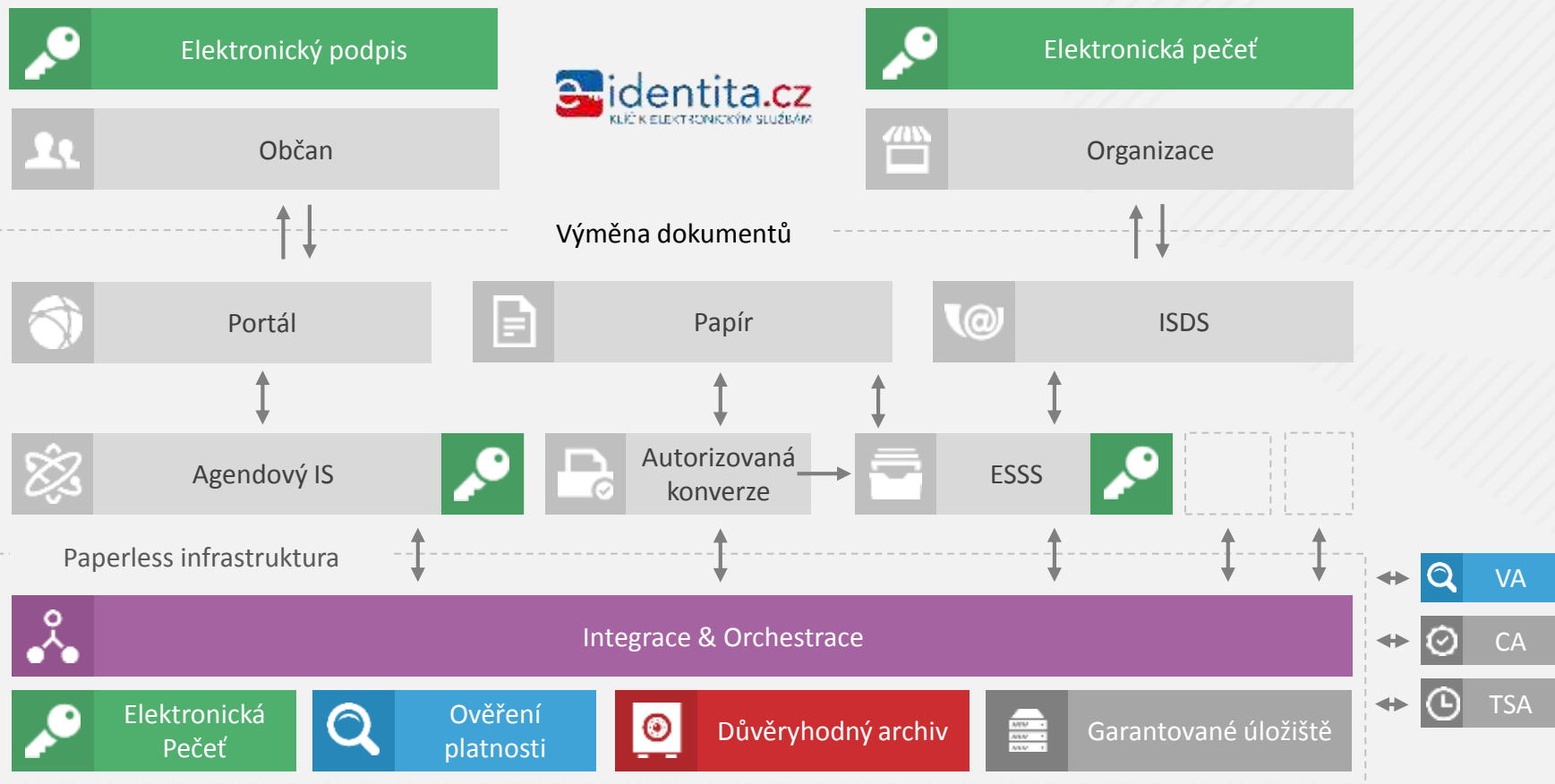


# GRANTOVÁ AGENTURA ČESKÉ REPUBLIKY

## Archiv pro agendové systémy



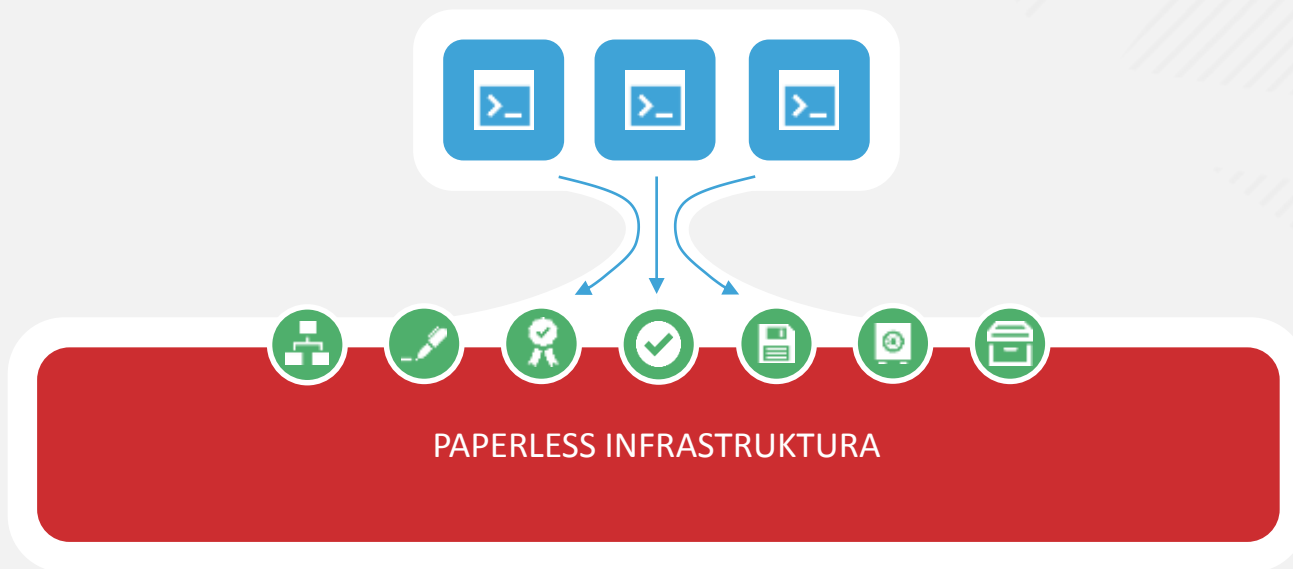
# BEZPAPÍROVÝ ÚŘAD



# PAPERLESS INFRASTRUKTURA

---

**Univerzální vrstva** pro komplexní péči o veškeré elektronické dokumenty





24. dubna 2018 | Vila Grébovka | Praha

# DIGITAL TRUST & PAPERLESS CONFERENCE

6. ročník



ZÁŠTITA



PARTNEŘI



THALES

