Digitální důvěra a paperless

Jan Tejchman

Primárně
jde o důvěru

eIDAS
konec
pochybností

Důvěra je
infrastrukturní
záležitost

Paperless
není revoluce

Primárně jde o důvěru

Kdo

Co

Kdy

Dokumenty v digitálním světě

Právní relevance

Digitální kontinuita

Datová integrita

Dlouhodobá dostupnost

Pro elektronické dokumenty je třeba zajistit stejné existenční podmínky, jako pro listinné. Musíme pouze použít jiné nástroje, které jsou však často lepší než jejich listinné ekvivalenty.

Digitální důvěra stojí na PKI

Digitální důvěra

Dohledový orgán

Public Key Infrastructure

Certifikační autorita

Validační autorita

Soukromý /veřejný klíč

Certifikát

Podpis/pečeť

Časové razítko

CRL/OCSP

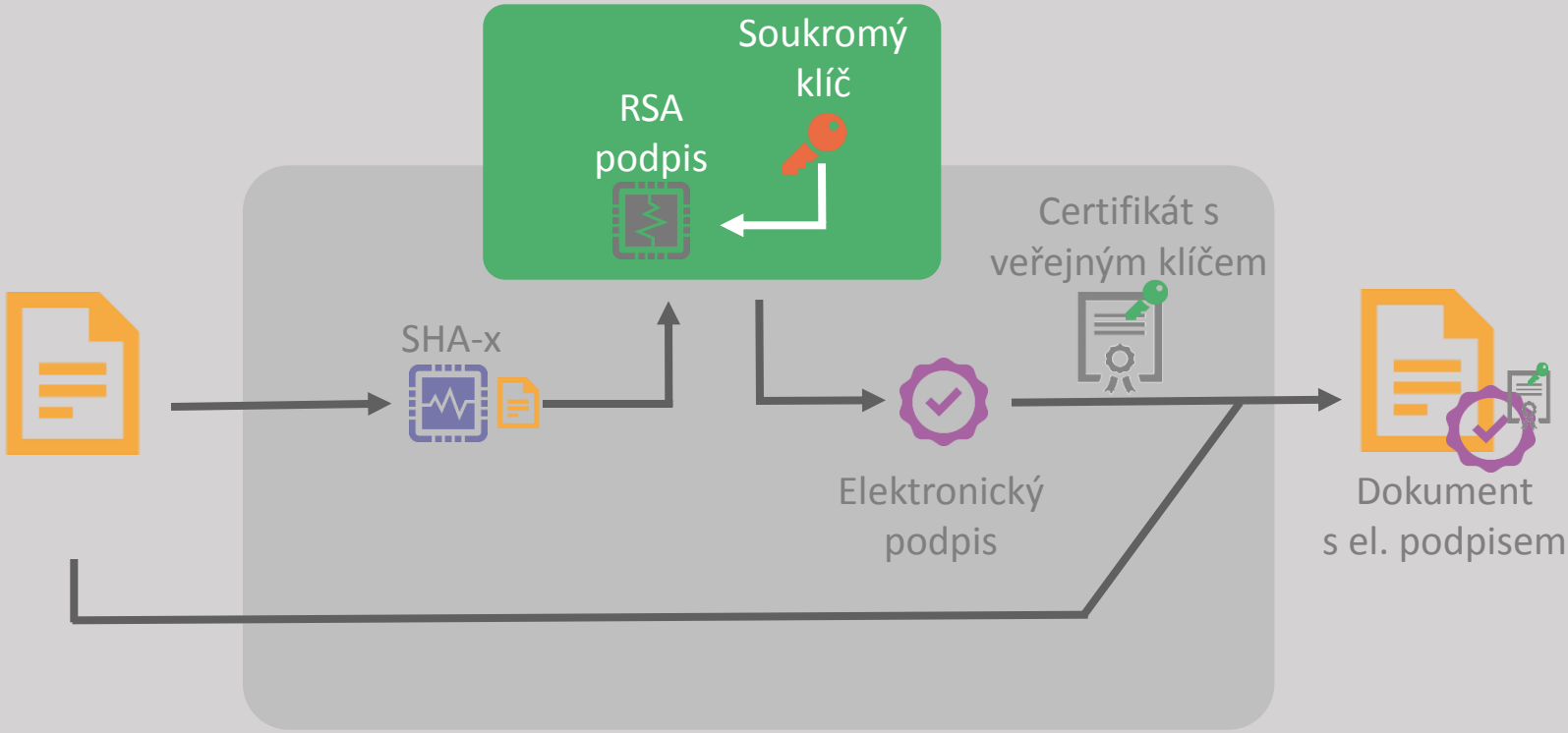
Prostředky pro vytváření digitální důvěry

Elektronický podpis

Elektronická pečeť

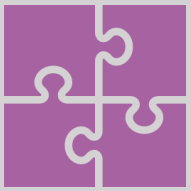
Elektronické časové razítko

Elektronický podpis



eIDAS konec pochybností

eIDAS - cesta k jednotnému digitálnímu trhu



- Interoperabilita
  - vzájemné uznávání prostředků elektronické identifikace napříč EU
  - vzájemné uznávání kvalifikovaných elektronických podpisů/pečetí
  - založeno na jednotných standardech a normách
- Harmonizace
  - uvedení národních legislativ do souladu s eIDAS
  - určení oblastí využívání jednotlivých typů nástrojů

Hlavní principy nařízení eIDAS

- Elektronickému dokumentu nesmějí být upírány právní účinky jen proto, že je elektronický.
- Kvalifikovaný elektronický podpis má stejnou váhu jako podpis vlastnoruční.
- Poskytování kvalifikovaných služeb poskytujících důvěru na území jednoho státu nesmí být omezeno na území jiného státu v rámci EU.

Praktické dopady eIDAS

- Elektronická identita
  - výběr vhodných národních systémů eID (**eOP**, ISDS, MojeID)
  - od 09/2018 povinná akceptace zahraničních eID systémů pro veřejné systémy
- Elektronický podpis/pečeť
  - eIDAS definuje 3 úrovně elektronického podpisu/pečeti
  - pro různé účely mohou být požadovány různé typy podpisů/pečetí
  - podoba podpisu a technické požadavky na vytváření jednotlivých podpisů byly upřesněny prováděcími akty z 8. 9. 2015 – **formáty AdES a ASiC**
- Elektronické časové razítko
  - zachovává stejné principy jako v současnosti

Rodina formátů AdES

- AdES = Advanced Electronic Signature = Zaručený elektronický podpis
- Založeny na principech PKI
- Legislativní základ v eIDAS
  - Oddíl 4 (čl. 25 – 34) – Elektronický popis
  - Oddíl 5 (čl. 35 – 40) – Elektronické pečetě
  - Oddíl 6 (čl. 41 – 44) – Elektronická časová razítka
- Prováděcí rozhodnutí Komise (EU) 2015/1506, kterým se stanoví specifikace pro formáty zaručených elektronických podpisů a zaručených pečetí…
  - ETSI TS 103172 v.2.2.2 – PAdES
  - ETSI TS 103173 v.2.2.1 – CAdES
  - ETSI TS 103171 v.2.1.1 – XAdES
  - ETSI TS 103174 v.2.2.1 – ASiC

ETSI Plugtest – AdES formáty

- Pořadatel ETSI (skupina Electronic Signatures and Infrastructures)
  - skupina zastřešující vznik technických standardů týkajících se elektronického podpisu v Evropě
- Účastníci AdES Plugtestů
  - certifikační autority (I.CA, InfoCert, Unizeto, …)
  - společnosti zabývající se IT bezpečností (Thales, Safelayer, Gemalto)
  - další (Adobe, Národný bezpečnostný úrad SR, Universidad Politecnica de Catalunya, Digital Agenda Agency for Romania, SEFIRA, …)
- Pozitivní vs. negativní testovací scénáře

Ověřování platnosti podpisů a pečetí

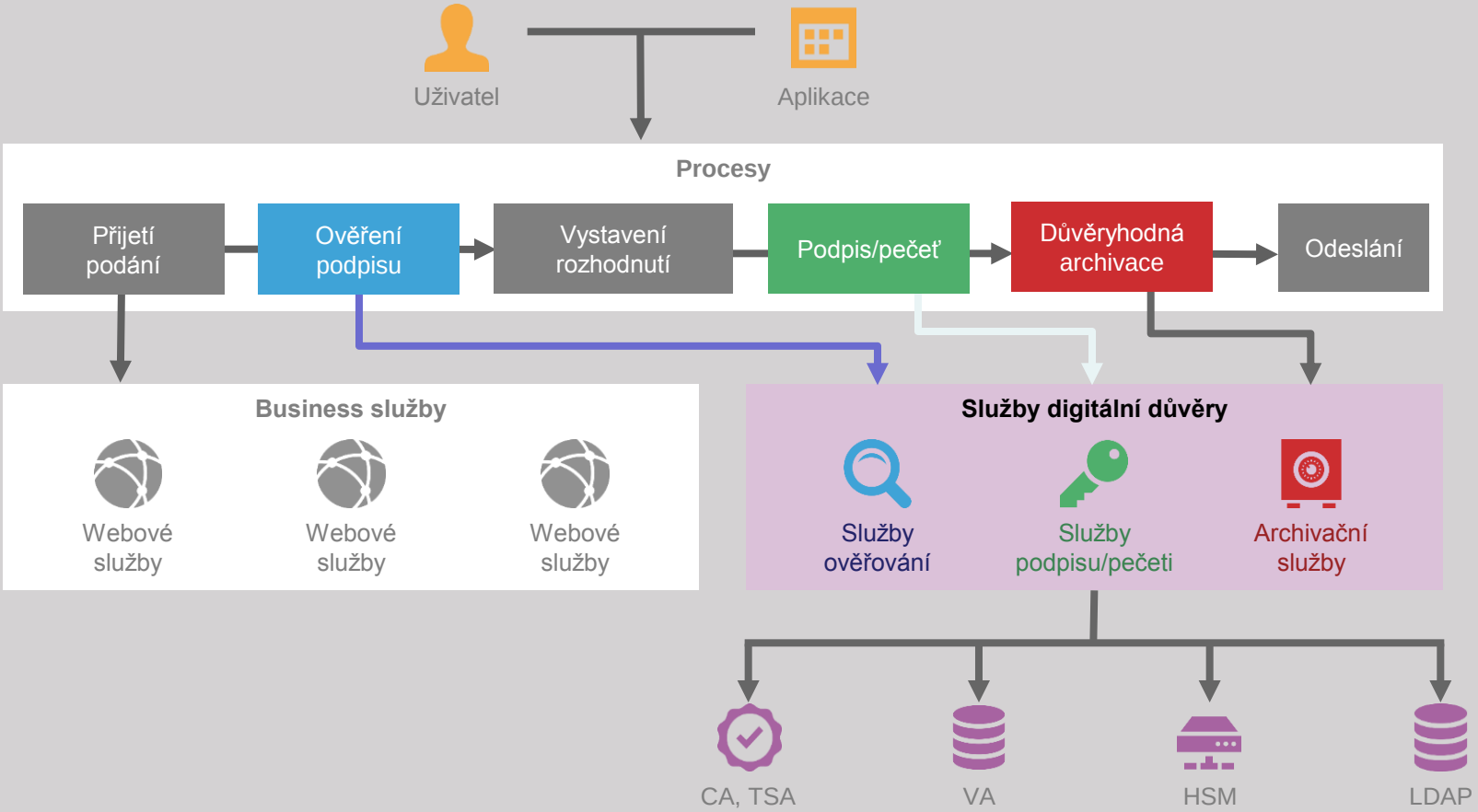
- Správné ověření platnosti podpisů a pečetí = právní jistota
- Musíme umět ověřovat kvalifikované podpisy a pečetě v rámci celé EU
- Ověření může spoléhající strana provést sama nebo může využít službu ověřování podpisů/pečetí
- Výsledky ověření je potřeba ukládat jako důkaz

Uchovávání kvalifikovaných podpisů a pečetí

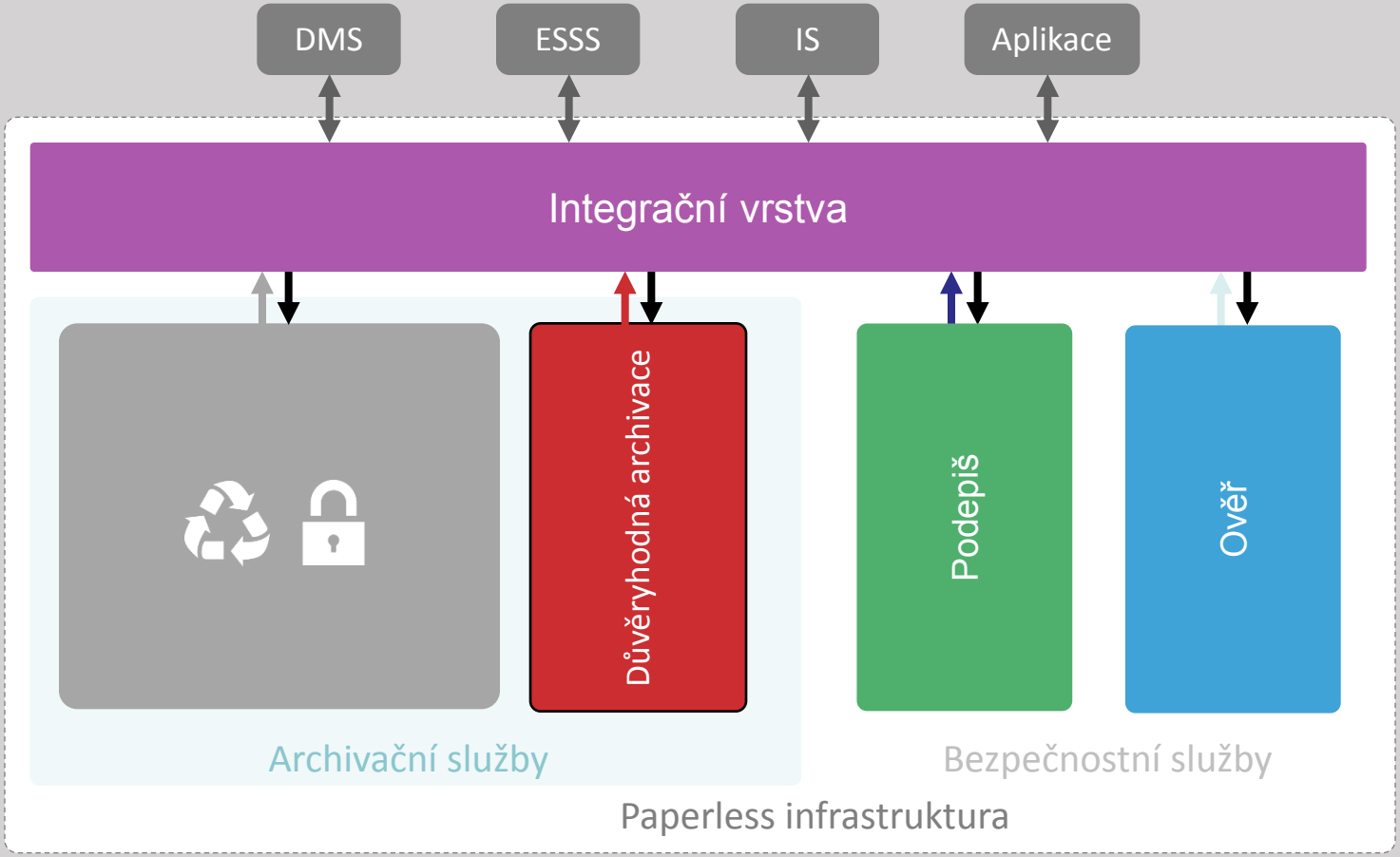
- eIDAS definuje uchovávání podpisů a pečetí (ne uchovávání dokumentů)
  - správně uchovaný EP prokazuje důvěryhodnost dokumentu nezávisle na místě jeho uložení
  - je nutné zajistit bezpečné uložení dat a dokumentů
- Služba uchování EP zajistí důvěryhodnost i po plynutí doby platnosti podpisu/pečetě
- Při dodržení postupů a norem v souladu eIDAS mohu uchovávat EP sám

Důvěra je infrastrukturní záležitost

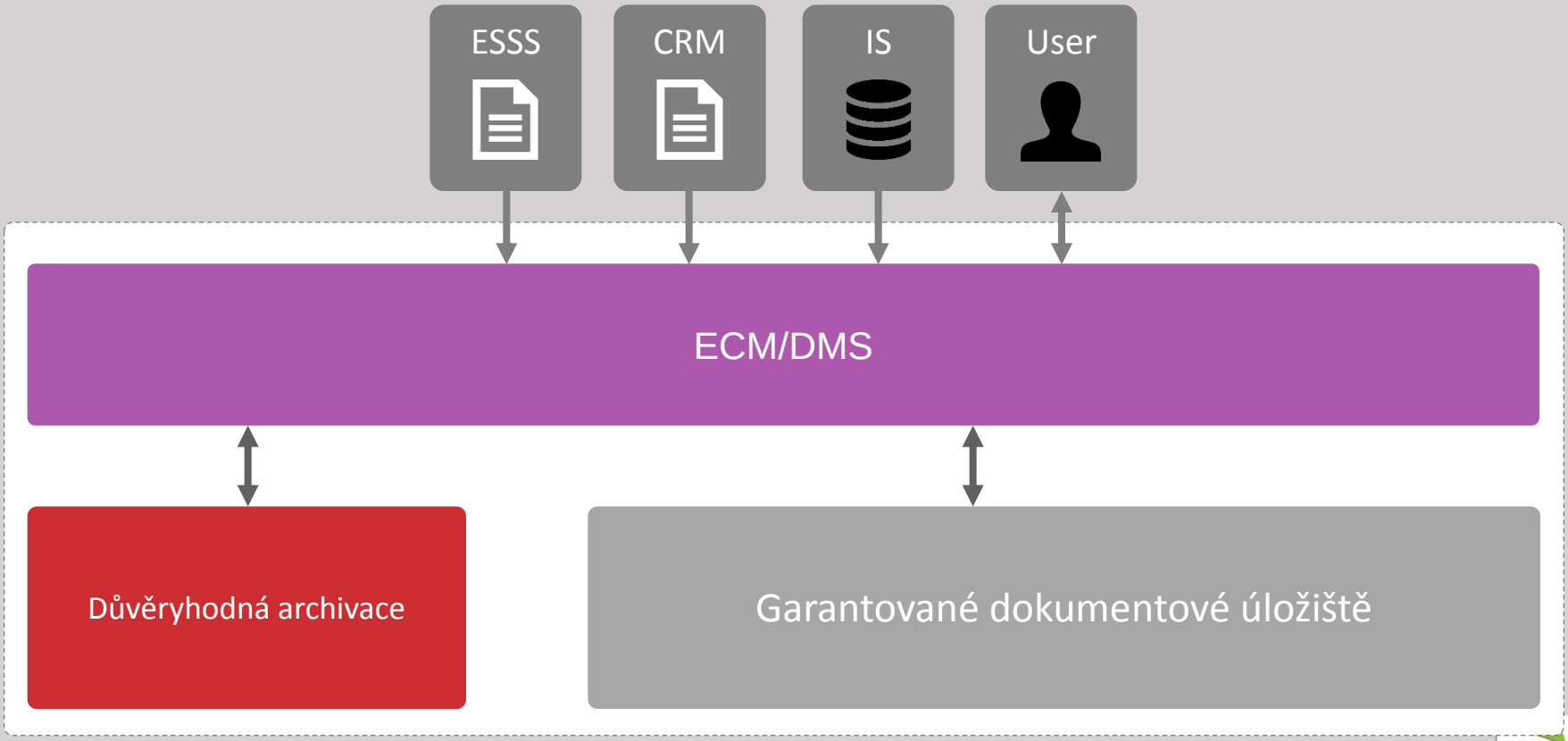
Digitální důvěra jako služba



Digitální důvěra jako služba

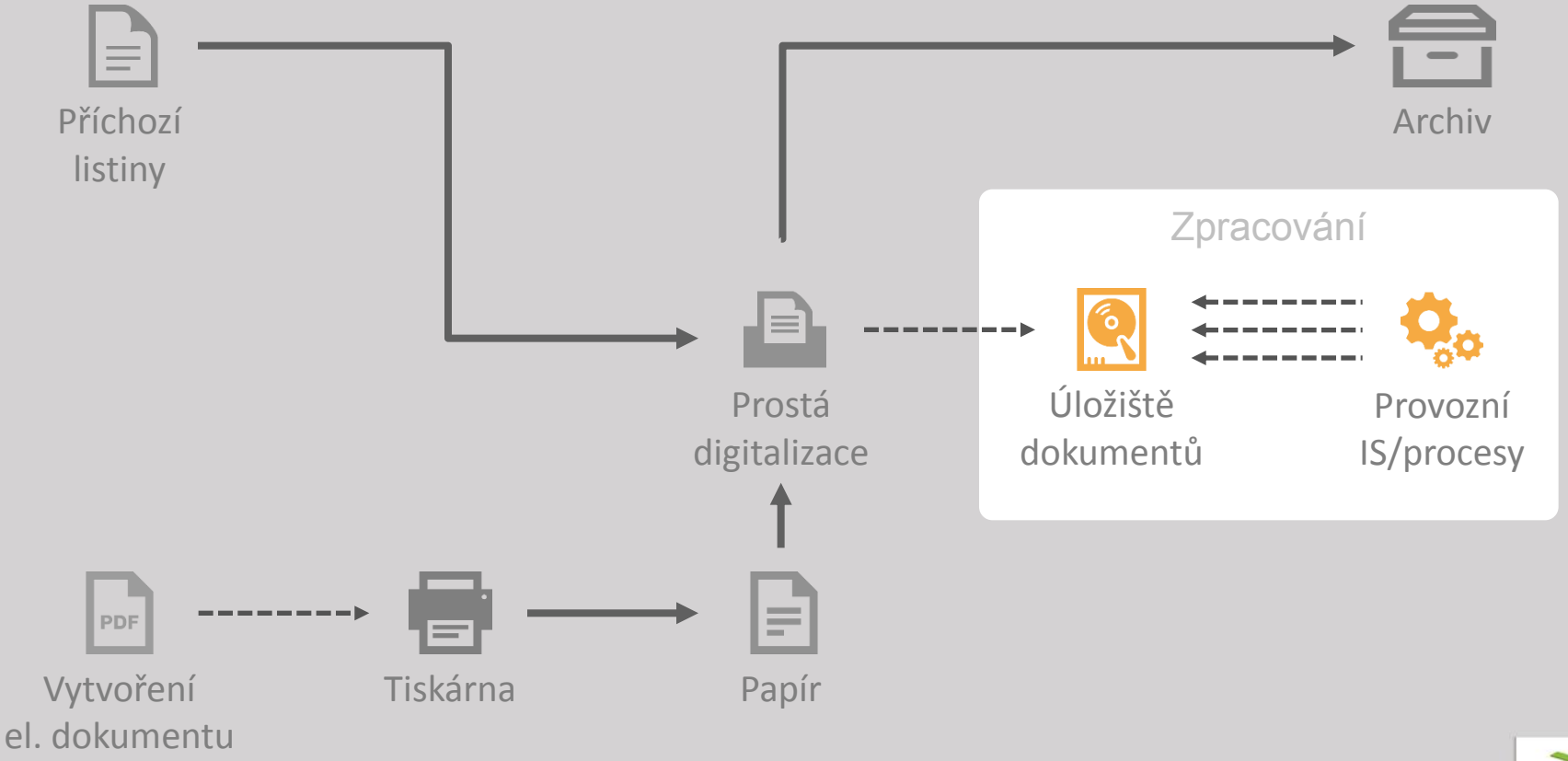


Důvěryhodná archivace jako služba

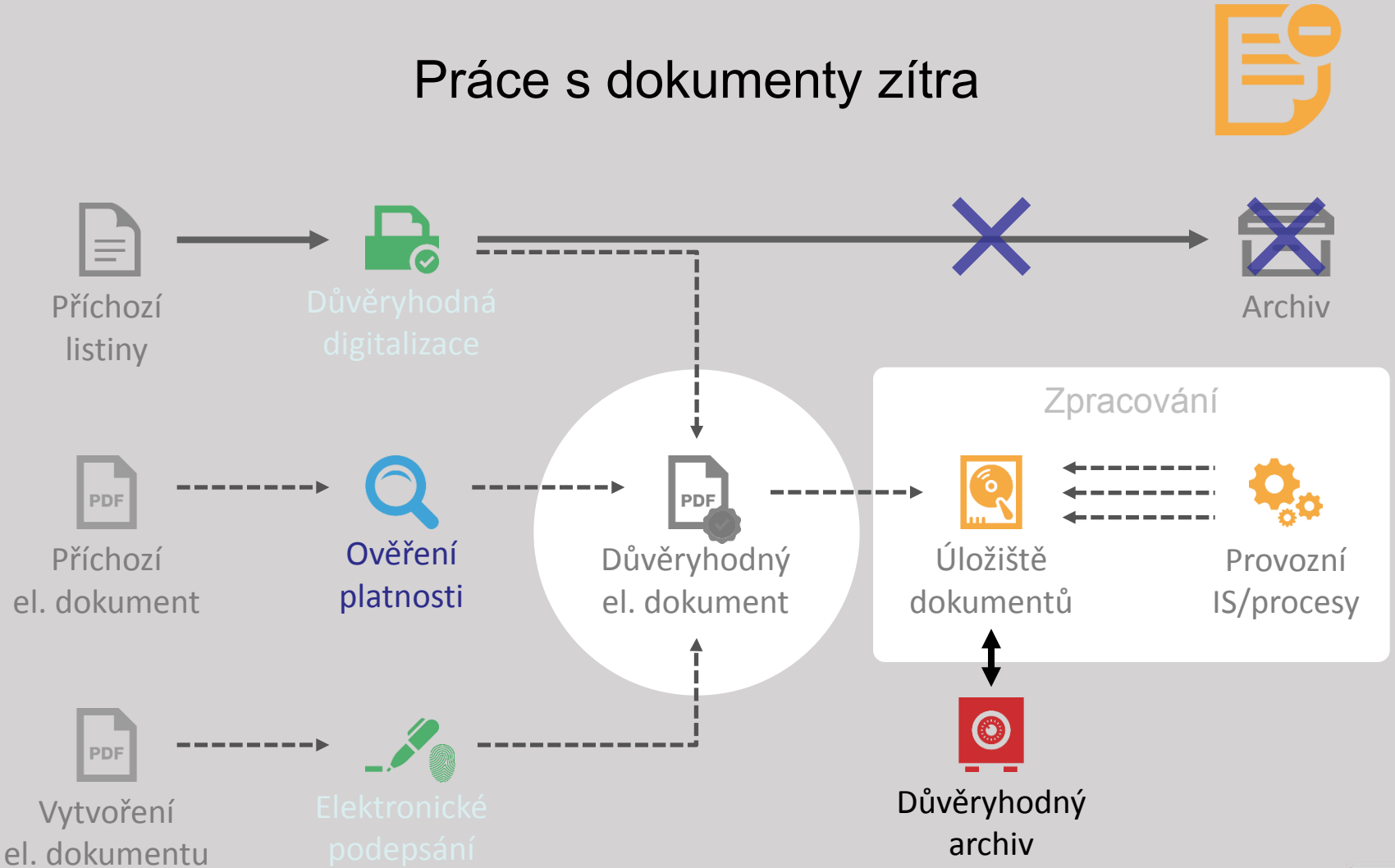


Paperless není revoluce

Práce s dokumenty dnes

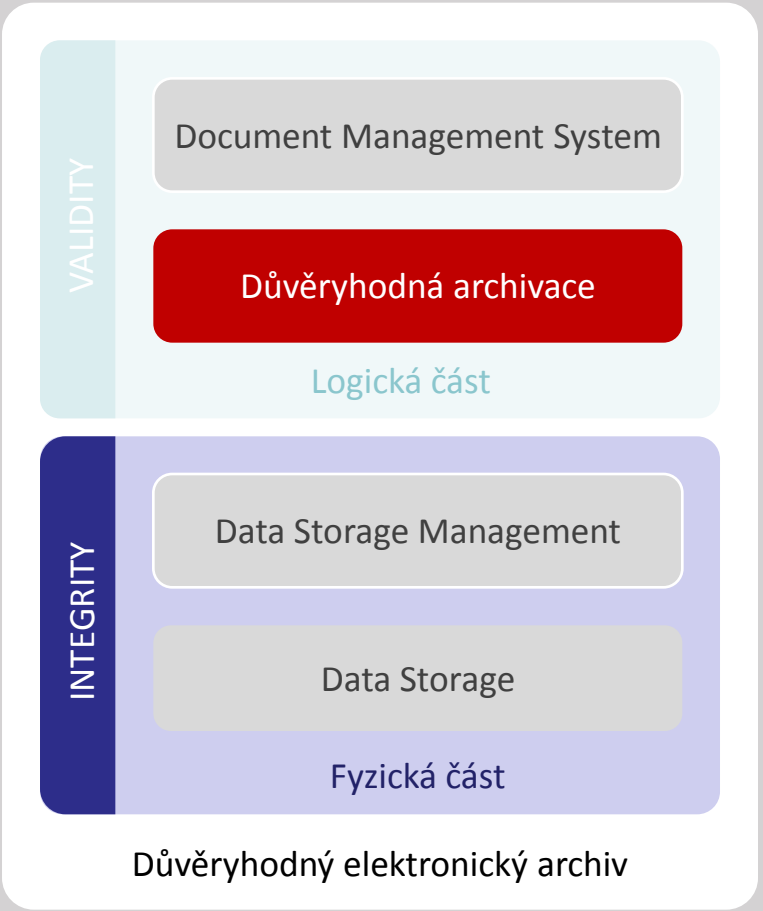


Práce s dokumenty zítra



Důvěryhodný elektronický archiv

- Fyzická část
  - neměnnost
  - nesmazatelnost
  - replikace
  - automatická detekce a oprava
  - bezpečná skartace
- Logická část
  - důvěryhodnost
  - legislativní platnost
  - průkaznost i mimo fyzické úložiště
  - sdílení důvěryhodnosti s okolím



Důvěryhodný elektronický archiv