



Ověřování platnosti elektronických dokumentů v čase

Lenka Vrzalová, ČÚZK
Jiří Bříza, aplis.cz, a.s.

- Úvod
- Elektronické dokumenty v praxi ČÚZK
- Ověřování platnosti dokumentů
- Jak udržovat dlouhodobou schopnost ověřování platnosti ?
 - Připojováním časových razítek
 - Funkcionalitou eSSL
- Problematika předávání evidovaných dokumentů další straně
- Závěr

- **Proč společná prezentace ČÚZK a aplis.cz, a.s.?**
 - implementace sw řešení eSSL
 - zahájení spolupráce květen 2009
 - implementace výchozího řešení květen 2010
 - další vývoj - stále
 - společné řešení metodických i praktických problémů

Elektronické dokumenty v praxi ČÚZK

- **současný stav:**

- zpracování datových zpráv z ISDS
 - za dobu funkčnosti eSSL již přijato přes milion zpráv
 - za rok 2011 do konce srpna téměř 600 tis. přijatých zpráv
 - za měsíc v průměru 73 tis., za den 3.856 datových zpráv

- **další rozvoj:**

- zpracování e-mailových zpráv prostředky EPVDS
- napojení na agendový systém ISKN
- doplnění dalších funkcí zejm. v souvislosti s dlouhodobým uchováváním dokumentů

Dlouhodobá platnost digitálních dokumentů – základní praktický problém.

Ověřování platnosti dokumentů v čase

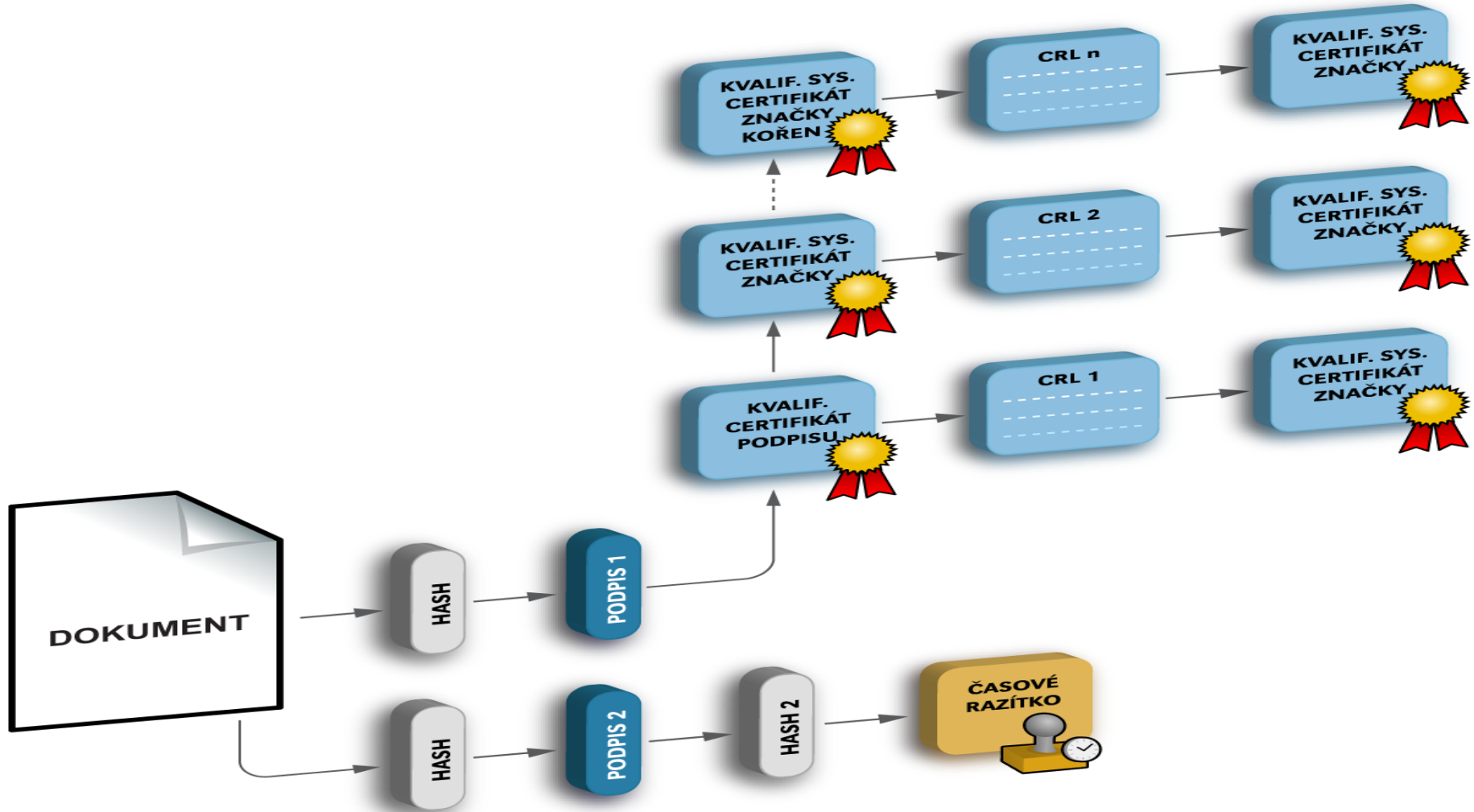
Co je nutné zajistit?

1. při převzetí do evidence - ověření platnosti el. podpisů
2. dlouhodobé udržení schopnosti ověřit platnost podpisů na evidovaném dokumentu
3. předání evidovaného dokumentu s možností ověřit/garantovat platnost podpisů:
 - druhé straně
 - archivu
4. převzetí dříve evidovaných dokumentů od druhé strany

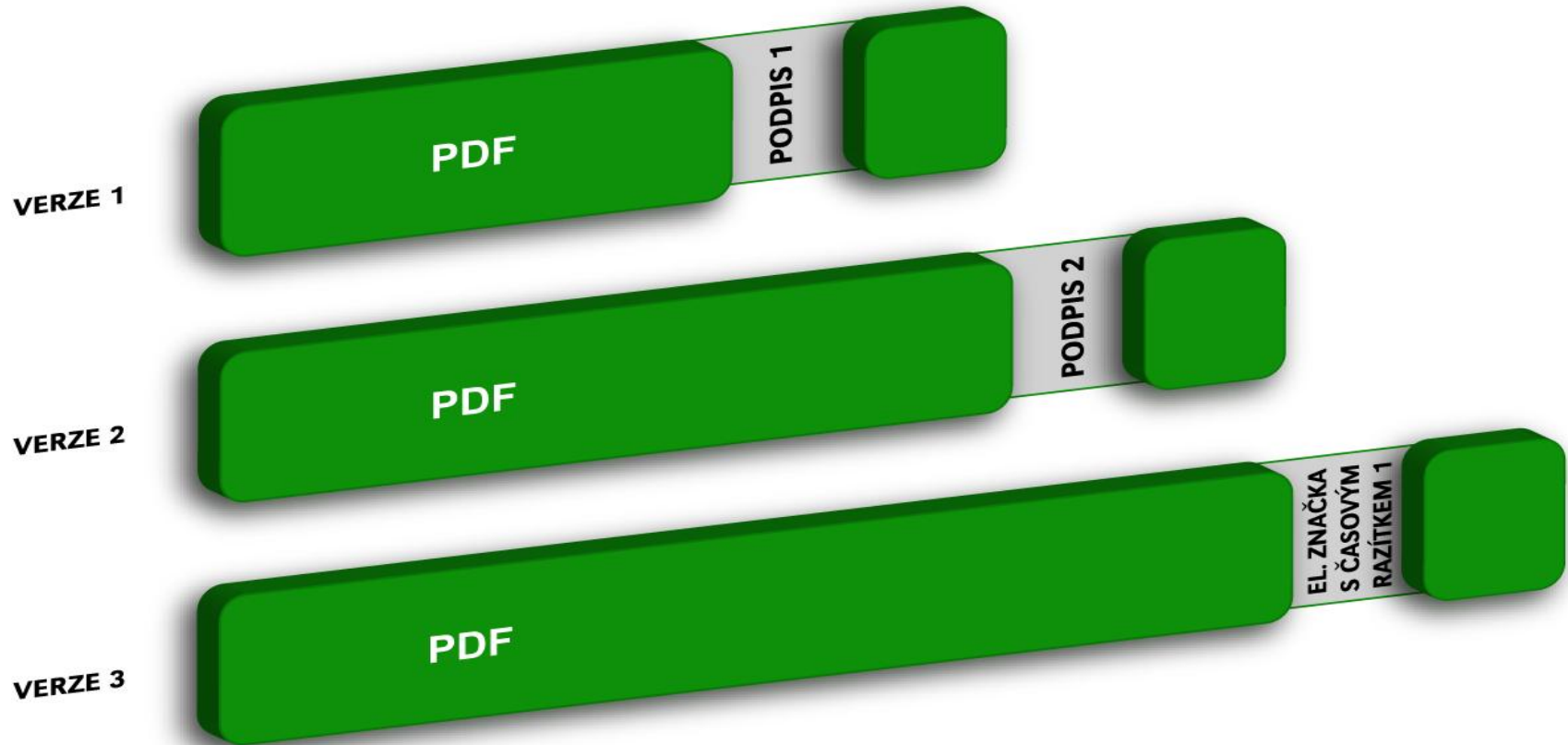
Ověření podpisů

- Zákonné úkony a uchování výsledků ověření
 - *ověření integrity dokumentu*
 - *explicitní určení okamžiku, ke kterému ověřujeme podpisy*
 - *zjištění certifikační cesty, případně posouzení certifikační politiky daného certifikátu*
 - *zjištění, zda nevyexpiroval některý z certifikátů na certifikační cestě*
 - *zjištění, zda k rozhodnému okamžiku není uveden některý z certifikátů na seznamu zneplatněných certifikátů (CRL)*
- Protokol XML (struktura)

Elektronický podpis - ověření



Elektronický podpis - ověření



Příklad protokolu o ověření

- **<ID evidence>** ... počáteční evidence zachycující DZ nebo email (evidenční číslo CKDP, čj. podacího deníku). Toto číslo musí být známe při ověřování podpisů.
- **<Způsob doručení>** ... email/DZ/medium
- **<ID datové zprávy>**
- **<Obálkové údaje DZ1>** ... vzít z evidence, je to sice duplicita, ale snadnější pro dokazování
-
- **<Obálkové údaje DZn>**
- **<Datum, čas dodání do DS>**
- **<Datum, čas doručení>**
- **<Počet dokumentů - příloh>**
- **<Dokumenty>**
 - **<Dokument>**
 - **<IDobjektu>** ... jednoznačné id dokumentu
 - **<Název dokumentu>**
 - **<Velikost dokumentu>**
 - **<Elektronické podpisy>**
 - **<Elektronicky podpis>**
 - **<Umístění podpisu>** externí/interní
 - **<Název souboru externího podpisu>**
 - **<IDobjektu externího podpisu>**
 - **<Typ certifikátu>** kvalifikovaný / kvalifikovaný systémový, jiný</Typ certifikátu>
 - **<časové razítko podpisu>** null/dd.mm.rrrr hh:mm:ss+údaj o typu času
 - **<seriové číslo certifikátu>** (HEX)
 - **<vystavitel certifikátu>**
 - **<země původu CA>** „C“=CZ
 - **<akreditovaná CA>** ano/ne </akreditovaná CA>

Příklad protokolu o ověření

- <údaje podepisující osoby> CN, OID, OU,
 - <platnost certifikátu od>
 - <platnost certifikátu do>
 - <použité CRL> číslo a další údaje o CRL např. pořadové číslo
 - <datum čas zneplatnění> ... z CRL
 - <datum čas ověření platnosti certifikátu>
 - <datum čas rozhodný pro ověření certifikátu>
 - <výsledek ověření podpisu> 0 ... ověřeno
 - 1 ... není vydán autorizovanou CA (nelze aut. rozhodnout)
 - 2 ... chybný hash ... narušený dokument
 - 3 ... vyexpirovaný certifikát (nelze aut. rozhodnout)
 - 4 ... zneplatněn, uveden v CRL (pokud není časové razítko, nelze aut. rozhodnout)
 - 5 ... platný podpis, za interním podpisem pdf je revize (nelze
 - automaticky rozhodnout)
- </Elektronicky podpis>
- </Elektronické podpisy>
- <Výsledek ověření podpisů dokumentu>
 - 0 ... všechny podpisy jsou OK (uznávané a platné)
 - 1 ... výskyt systémového certifikátu, všechny jsou OK (uznávané a platné)
 - 2 ... výskyt neplatného podpisu
 - 3 ... výskyt podpisu k rozhodnutí
 - 9 ... žádný podpis
- </Dokument>
- </Dokumenty>

Příklad protokolu o ověření

- **<Výsledek ověření podpisů záznamu>**
 - **0 ... všechny podpisy jsou OK (uznávané a platné)**
 - **1 ... výskyt systémového certifikátu, všechny jsou podpisy OK (uznávané a platné)**
 - **2 ... výskyt neplatného podpisu**
 - **3 ... výskyt podpisu k rozhodnutí**
 - **9 ... žádný podpis**

Dlouhodobé udržení platnosti

Dvě základní strategie:

- Doplnění časového razítka (přerazítkovávání) na objekty potřebné k ověřování dříve, než vyexspiruje jejich certifikát
- Udržení prostředky eSSL – na základě norem a standardů zejména zákona o archivnictví a spisové službě, Národního standardu eSSL – Moreq2.

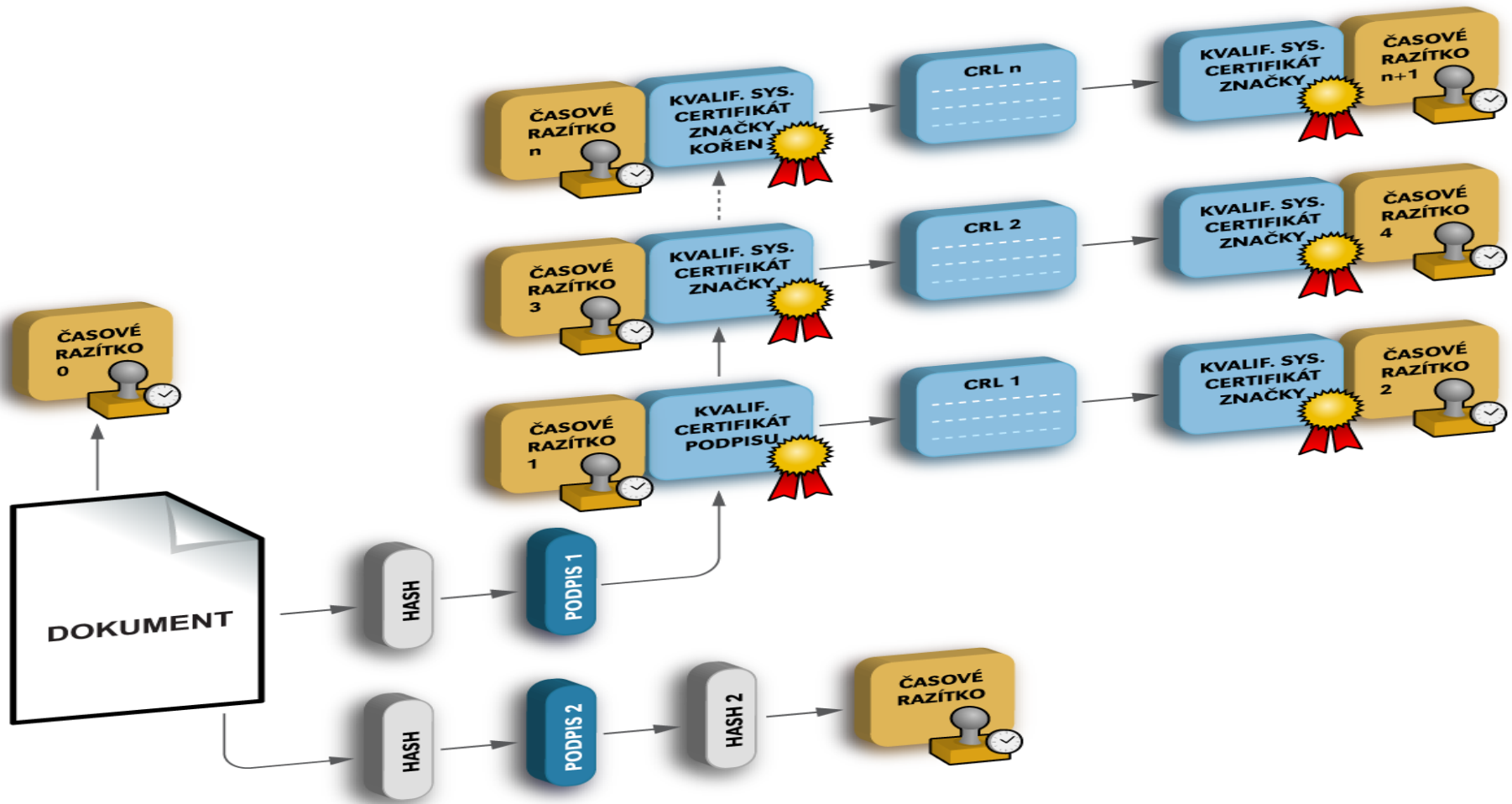
Doplňování časových razítek

Cíl: stále udržovat schopnost ověřovat platnost potřebných podpisů na dokumentu

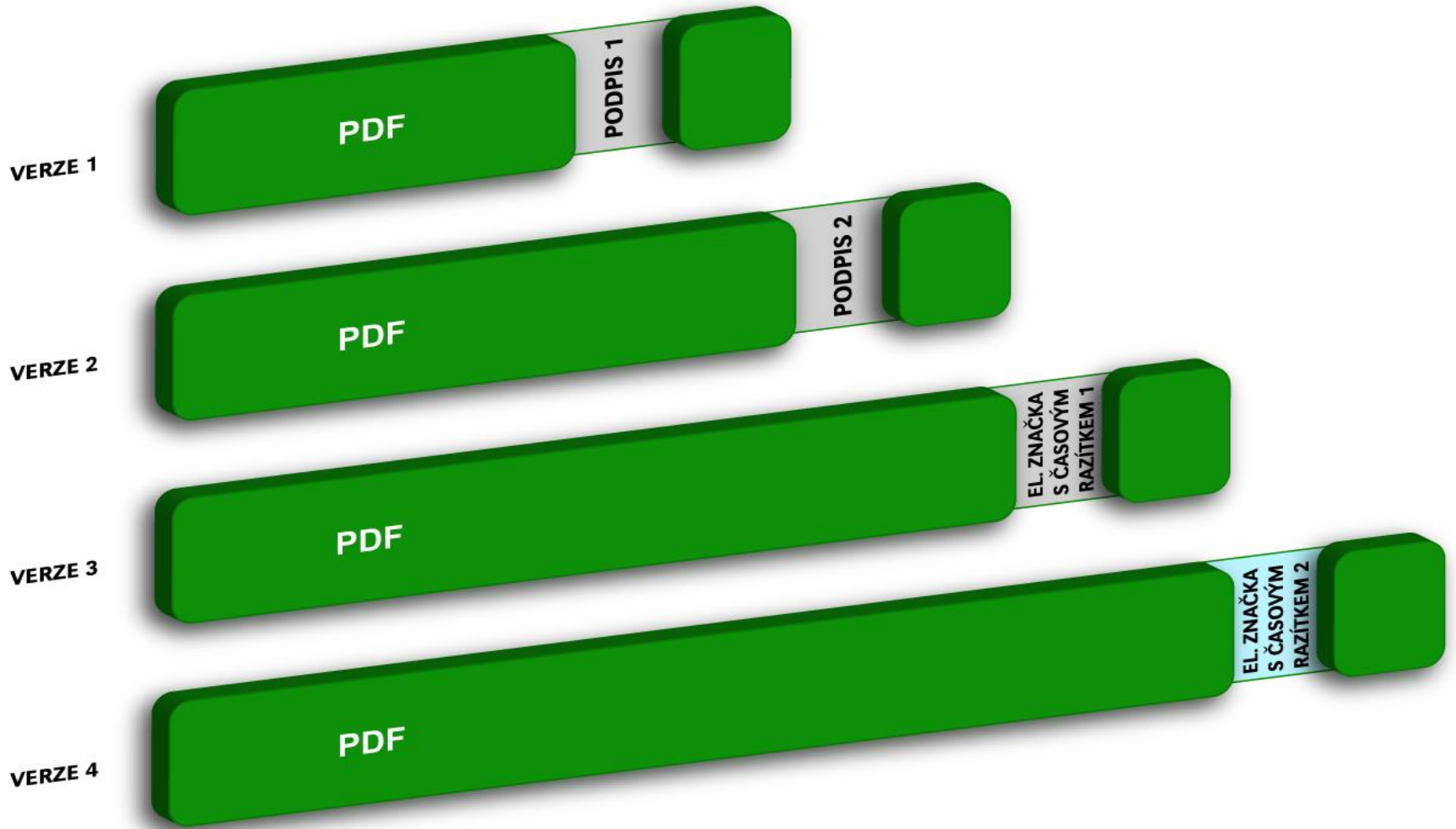
Řešení přerazítkováním:

- Prodlužování platnosti **všech komponent** nutných k ověřování podpisu (časové razítko) – výlučně podle zákona 227/2000 Sb.
 - Přidání nového podpisu dříve, než vyexspiruje původní certifikát. Účelem není vyjádřit se k obsahu, proto je nutné časové razítko.
 - Lze tak reagovat i na rozvoj kryptografie (delší hash u nového časového razítka, ...)

Doplnění časového razítka, ale jedno nestačí



Doplnění časového razítka



Doplnění časového razítka

Problémy:

- zjišťování, kdy končí platnost certifikátů v čase, je technicky řešitelné, ale nikoliv jednoduché (objekty certifikační cesty)
- finanční náklad na časová razítka na potřebné objekty
- nelze připojit samostatné interní časové razítko k PDF souboru
- vložením interní značky se mění/verzují i dokumenty po ukončení jejich životního cyklu
- při opatřování PDF souborů externími časovými razítky vznikne mix interních a externích podpisů a značek
- není obvyklé v EU doplňovat dokumenty časovými razítky

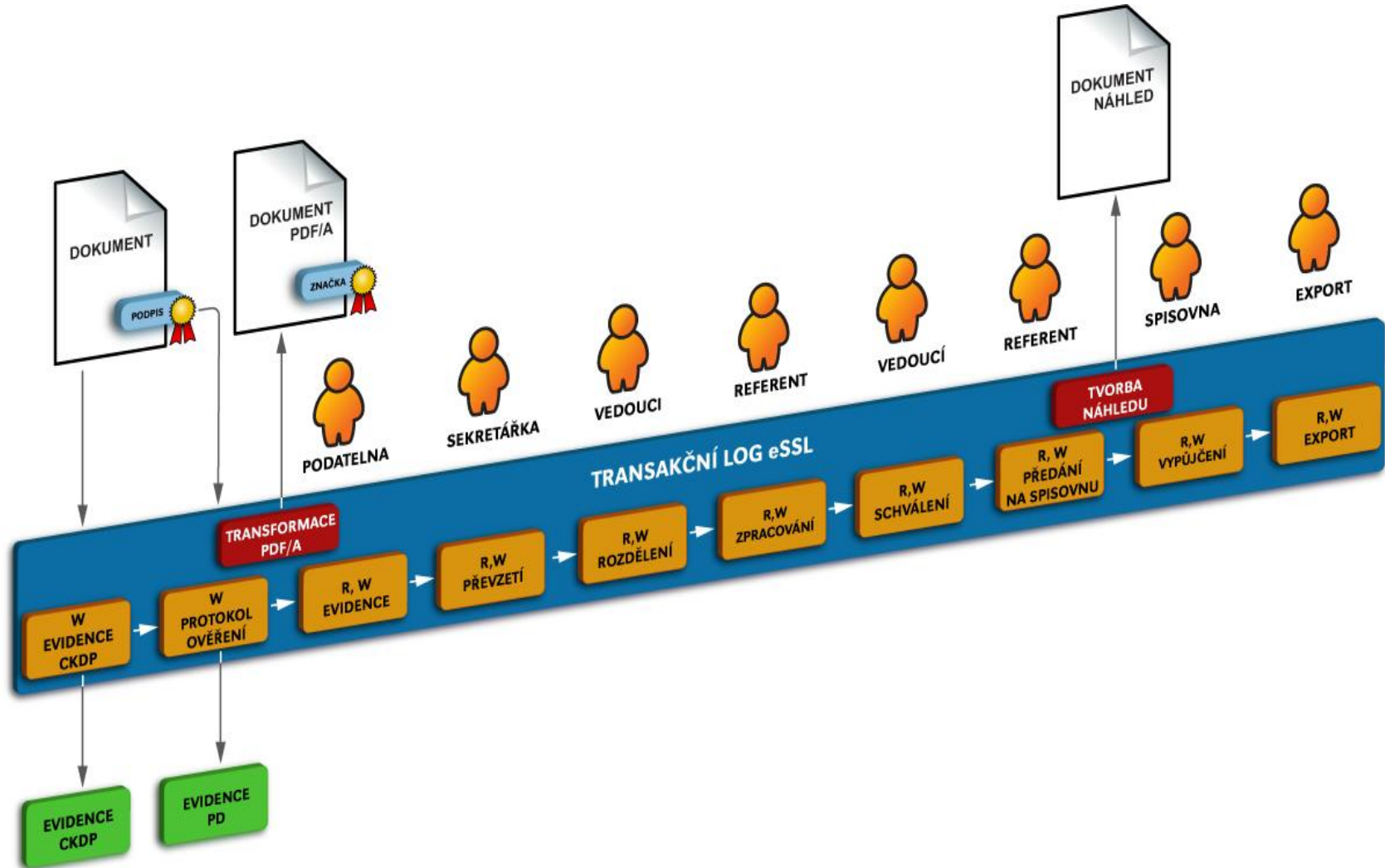
Udržení prostředky eSSL

Schopnost prokázat platnost podpisů jiným způsobem:

Východiska:

- Provést ověření platnosti v okamžiku, kdy to jsme schopni provést jednoduše, včetně záznamu o veškerých vstupech, podmínkách a výsledcích
- Zajištění dokumentu: nemožnost vyměnit původní dokument kolizním dokumentem, u kterého „sedí“ původní podpis, tzv. fixace původního dokumentu.
- Právním rámcem je zákon 499/2004 Sb.
- Praktické řešení – eSSL podle Národního standardu, tj. Moreq2

Udržení prostředky eSSL



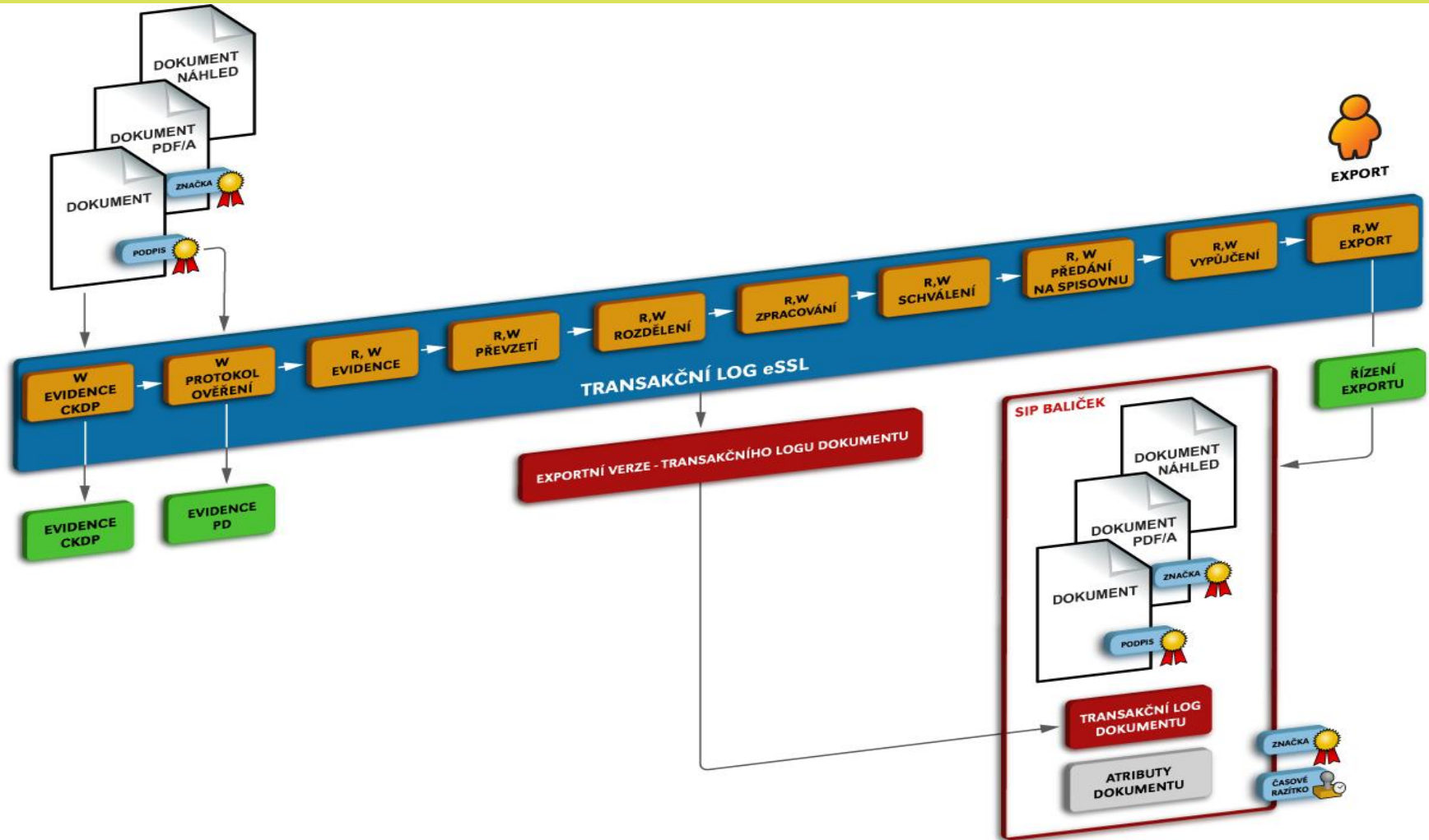
Předání s možností ověření platnosti

Jde o dlouhodobě řešený problém i na eu úrovni.

cesta dokumentu původce → archiv → badatel je standardizována na úrovni objektů a procesů:

- **Model OAIS**
 - SIP balíček (AIP, DIP)
- **Předání druhé straně**
 - Plná verze, která podporuje ověření platnosti a uznatelnosti podpisů, vhodná pro zpracování pomocí IS eSSL, tj. SIP balíček doplněný transakčním protokolem podle Národního standardu
 - Zjednodušená verze – pro běžné uživatele
 - Připojení ověřovací doložky k předávanému dokumentu
- **Předání archivu ... dále nerozvedeno**

Tvorba SIP balíčku



Přijetí SIP balíčku

- Převzetí balíčku SIP, jako jeden objekt, do evidence
- Ověření platnosti balíčku ... vyšší transakční tlak na zpracování než při předání do archivu
 - Antivirová ochrana
 - Dočasné úložiště
 - Vybraná metadata do atributů
 - Ostatní metadata z XML SIP - výběrově indexovat pro vyhledávání
- Parsování obsahů (dokumentů)
- Ověření platnosti uznávaných podpisů, standardní protokol
- Výběr obsahu pro evidenci (např. původní dokument, konvertovaný dokument, náhled,...)

Závěr

- Výběr strategie pro dlouhodobé udržování možnosti ověřovat podpisy by neměl být omezován legislativními posuny směrem k neustálému doplňování časových razítek
- Zpochybňování dostatečné věrohodnosti eSSL (ERMS), které jsou vedeny podle Národního standardu, při fixování obsahů dokumentů a jejich atributů, narušuje celý koncept ukládání a archivování dokumentů bez ohledu na jejich fyzickou podstatu.
- Nutnost opírat se i nadále o evropské standardy a nevytvářet vlastní „českou“ cestu kvůli partikulárním zájmům

Děkujeme za pozornost.

Lenka Vrzalová, ČÚZK
Jiří Bříza, aplis.cz, a.s.