



DLHODOBÁ OVERITEĽNOSŤ PODPISOV A PEČATÍ LACNO A JEDNODUCHO

Knižnice EÚ, Digital Signature Services v praxi

AGENDA

Čo si ukážeme:

- Ako dlhodobé overovanie súvisí s SDM (JDT)
- CEF-TELECOM výzva a projekt DMS-LTV
- Východiska projektu, partneri projektu a cieľ projektu.
- Produkt – LTV Service for ECM
- Aktuálna legislatíva
- Aktuálne výzvy
- Záver, plány

JEDNOTNÝ DIGITÁLNY TRH - PRAKTICKY



CEF Digital

- vyvinul a udržiava tzv. stavebné bloky (softvérové knižnice, nástroje, metodiky) pre ľahšiu implementáciu súčastí Jednotného Digitálneho Trhu.
- ponúka množinu služieb a nástrojov, ktorá pomôže naštartovať prácu s pripravenými stavebnými blokmi. Všetky služby a nástroje CEF Digital sú k dispozícii zdarma v otvorených licenciách.

JEDNOTNÝ DIGITÁLNY TRH - PRAKTICKY

Nové stavebné bloky vo výstavbe pre oblasti:

- European Blockchain Services Infrastructure
- Big Data Test Infrastructure
- Context Broker

Aktuálne stavebné bloky sú už vyzreté a niekoľko rokov je ich možné používať pre tieto oblasti:

- eDelivery
- eInvoicing



DIGITAL SIGNATURE SERVICES (DSS)

JAVA KNIŽNICE PRE
VYTVÁRANIE A OVEROVANIE
EIDAS ELEKTRONICKÝCH
PODPISOV A PEČATÍ

DEMO IMPLEMENTÁCIA WEB
APLIKÁCIE NA PODPISOVANIE A
OVEROVANIE PODPISOV.

KONKRÉTNÁ IMPLEMENTÁCIA
STAVEBNÉHO BLOKU PRE
ESIGNATURE



DIGITAL SIGNATURE SERVICES V SLUŽBE PODPISUJ.SK

Už rok máme v prevádzke službu Podpisuj.sk

V plnej miere využíva DSS knižnice CEF-Digital EU

Získala si už stabilných zákazníkov, hlavne z radov advokátskych kancelárií a obcí

DSS knižnice sa využívajú na niekoľko funkcií a prípadov použitia:

Overovanie eIDAS podpisov a pečatí

Vytváranie ASiCE/XAdES a PAdES podpisov, vrátane hromadného, násobného a vizuálneho podpisovania

Zaručená konverzia

Autorizačné doložky pre Rozhodnutia

The screenshot displays the 'Overenie podpisu dokumentu' (Document Signature Verification) interface of Podpisuj.sk. The main window shows a list of documents, with 'ROZHODNUTIE.xzep' selected. The right-hand panel provides detailed information about the document and the verification results.

Dokument na overenie

Názov	ROZHODNUTIE.xzep
Umiestnenie	C:\Praca_Archimetes_Podpisovanie_dokumentov_PodpisoveTesty\0061-Hudec-DSS55-nejdu-asicy
Veľkosť	128,6 kB
Druh obsahu	application/vnd.etsi.asic-e+zip

Výsledky overenia

Počet podpisov	1
Počet platných podpisov	1
Čas overenia	22.10.2019 10:45:35

Zaručená elektronická pečať mesta Žarnovica (5.2.2019 9:01:04)

Formát podpisu

XAdES-BASELINE-T
(podpis s časovou pečiatkou)

Platnosť podpisu

Podpis je **PLATNÝ**
(Kvalifikovaná elektronická pečať)

Rozsah podpisu

Object20190205080104160.pdf
(Celý dokument)

Použité certifikáty

- KCA NBU SR 3
- CA Disig QCA3
- Zaručená elektronická pečať mesta Žarnovica

LTV SLUŽBA NAD ECM/DMS ÚLOŽISKOM

CEF-TELECOM výzvy na využitie
stavebných blokov pre eID a eSignature:
2018 CEF Telecom Call - eldentification &
eSignature (CEF-TC-2018-1)

Myšlienka: Vytvorenie LTV služby,
spolupracujúcej s bežnými úložiskami
dokumentov (ECM/DMS). Vyriešiť tým
problém uskladnenia podpísaných
dokumentov v jednotlivých OVM, kvôli
neskoršiemu bezproblémovému overeniu.

Navrhli sme projekt: „Document
management system with long term
signature validation“

Projekt bol schválený v Bruseli a počas
roku 2019 implementovaný

S výskumom pomáhajú 3 diplomanti z 2



This Photo by Unknown Author is licensed under [CC BY](#)

PREČO VÝSKUM A PROTOTYP ?

Podpisové profily podľa eIDAS	Základný profil	S časovou pečiatkou	Dlhodobý	Dlhodobý archívny
CAdES-BASELINE	Baseline-B	Baseline-T	Baseline-LT	Baseline-LTA
PAdES-BASELINE	Baseline-B	Baseline-T	Baseline-LT	Baseline-LTA
XAdES-BASELINE	Baseline-B	Baseline-T	Baseline-LT	Baseline-LTA
ASiCE (XAdES, CAdES)	Baseline-B	Baseline-T	Baseline-LT	Baseline-LTA
ASiCS (XAdES, CAdES)	Baseline-B	Baseline-T	Baseline-LT	Baseline-LTA

Sporadicky používané eIDAS formáty v Slovenskej verejnej správe

Bežne používané eIDAS formáty v Slovenskej verejnej správe

PREČO VÝSKUM A ?

Zatiaľ sa v SVK nevyužívajú

Podpisové profily podľa eIDAS	Základný profil	S časovou pečiatkou	Dlhodobý	Dlhodobý archívny
CAdES-BASELINE	Baseline-B	Baseline-T	Baseline-LT	Baseline-LTA
PAdES-BASELINE	Baseline-B	Baseline-T	Baseline-LT	Baseline-LTA
XAdES-BASELINE	Baseline-B	Baseline-T	Baseline-LT	Baseline-LTA
ASiCE (XAdES, CAdES)	Baseline-B	Baseline-T	Baseline-LT	Baseline-LTA
ASiCS (XAdES, CAdES)	Baseline-B	Baseline-T	Baseline-LT	Baseline-LTA

Obsahujú v podpise všetky informácie na jeho overenie

Pridáva archívne časové pečiatky. Udržiava konzistenciu a nemennosť dokumentu, ako aj jeho priamu a okamžitú

PREČO VÝSKUM A F

?

Budu tieto podpisové profily overiteľné na CEP, alebo rezortných podateľniach

Podpisové profily podľa eIDAS	Základný profil	S časovou pečiatkou	Dlhodob	Dlhodob
CAdES-BASELINE	Baseline-B	Baseline-T	Baseline-LT	Baseline-LTA
PAdES-BASELINE	Baseline-B	Baseline-T	Baseline-LT	Baseline-LTA
XAdES-BASELINE	Baseline-B	Baseline-T	Baseline-LT	Baseline-LTA
ASiCE (XAdES, CAdES)	Baseline-B	Baseline-T	Baseline-LT	Baseline-LTA

NBU Metodický pokyn: Subjekty verejného sektora si musia aktualizovať svoje aplikácie pre QES, aby boli v súlade s nariadením (EÚ) č. 910/2014, ak ich aplikácie boli posúdené podľa legislatívy platnej pred 1.7.2016.

POROVNANIE LTV: INTEGRITNÝ VS. EIDAS

	LTV Archív s Integritným podpisom (napr. MDURZ)	LTV Úložisko s eIDAS B- LTA podpismi Podpisuj.ltv service
Priame overenie v ľubovoľnej eIDAS overovacej službe	Nie	Áno
Potreba „Diplomu“ o overení	Áno	Nie
Čas overenia	Čím starší dokument, tým dlhšie overenie (minúty)	Okamžité
Akceptácia na OVM	???	Áno
Akceptácia v zahraničí	Nie	Áno
Kompatibilita s eIDAS	???	Áno

VÝCHODI SKÁ A PARTNERI PROJEKTU

DMS-LTV

Cieľ projektu: Vytvorenie

- Služba 1 – Archívnej nadstavby nad ECM/DMS, s funkciami:
 - Overenia podpisu/pečate na vstupe
 - Ošetreniu vstupného dokumentu do profilu BASELINE-LTA
 - Uloženie prijatého dokumentu do dokumentového úložiska a naplnenie meta údajov o dokumente
 - Pravidelné znova ošetrenie dokumentu 2 týždne pred expiráciou platnosti LTA podpisu
 - Vyradenie z úložiska po dobe, počas ktorej bol dokument udržiavaný.
 - Zápisy ošetrovacích transakcií do histórie transakcií
- Služba 2 – jednorazového ošetrenia dokumentu na vstupe a vrátenie ošetreného dokumentu na výstupe.
 - Overenia podpisu/pečate na vstupe
 - Ošetreniu vstupného dokumentu do profilu BASELINE-LTA
 - Vytvorenie a poskytnutie overovacieho reportu, ošetreného súboru
 - Zápisy ošetrovacích transakcií do histórie transakcií

VÝCHODI SKÁ A PARTNERI PROJEKTU

DMS-LTV

Partneri projektu:

- Obec Môlča
 - Pán starosta aktívne rieši digitalizáciu Verejnej správy
 - Vyjadril potrebu mať vlastné LTV úložisko
- Obec Kynceľová
 - Pani starostka je členkou komisie pre digitalizáciu ZMOS
 - Potešila sa možnosti spolupracovať na vývoji DMS-LTV platformy
- Erika Kusyová – Infocom.sk
 - Nezávislý poradca a školiteľ pre informatizáciu verejnej správy
 - Členka pracovnej skupiny pri ÚPVII

Autorizácia projektu:

- ÚPVII

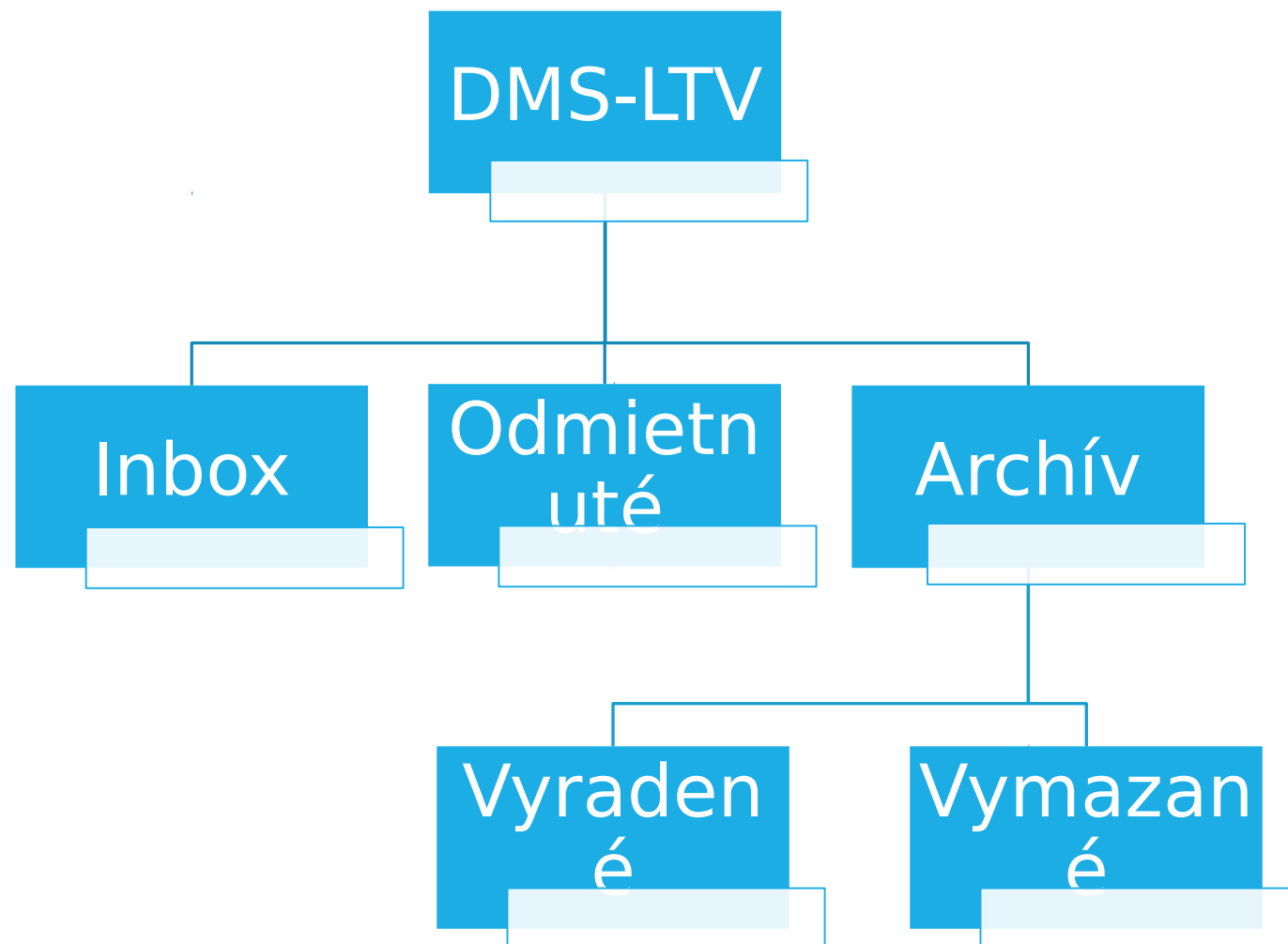
1. DMS-LTV / LIFFRAY

DOKUMENT DO VSTUPNÉHO
ADRESÁRA (INBOX)

VSTUPNÝ MODUL OVERÍ A
ROZHODNE. AK JE PRIJATÝ DO
ARCHÍVU - OŠETRENIE NA LTA
ÚROVEŇ A NAPLNÍ META DÁTA

PRAVIDELNÁ KONTROLA - 2
TÝŽDNE PRED EXSPIRÁCIOU -
NOVÉ OŠETRENIE
(REGISTRATÚRNY PLÁN)

PO UPLYNUTÍ ÚLOŽNEJ DOBY JE
DOKUMENT VYRADENÝ (V SÚLADE
S REGISTRATÚRNYM PLÁNOM)



2. LTV OŠETRENIE

DOKUMENT NA VSTUP
SLUŽBY

VSTUPNÝ MODUL OVEŘI
DOKUMENT A
ROZHODNE, AK JE
PLATNÝ OŠETRENIE NA
LTA ÚROVEŇ

TRANSAKČNÝ ZÁPIS,
VALIDAČNÝ REPORT A
DOKUMENT SA PONÚKNE
NA STIAHNUTIE

LTV ošetrenie

Baseline(-
T) Vstup

Baseline-
LTA

Výstup

AKTUÁLNY STAV PROJEKTU

DMS-LTV

Pilotná prevádzka pre obce:

- Obec Môlča, Obec Kynceľová
- Od 1. kvartálu 2020 chceme službu ponúkať v rámci nášho portfólia služieb SaaS Podpisuj(.sk)
- Pilotná prevádzka potrvá pár mesiacov
- Vývoj konektorov pre ďalšie ECM/DMS systémy, alebo registratúry
- Oslovenie potencionálnych partnerov, potencionálnych zákazníkov.
- Príprava infraštruktúry Archimetes na poskytovanie oboch služieb:
 - 1 DMS-LTV
 - 2 LTV ošetrovanie formou SaaS komerčne.

AKTUÁLNY STAV PROJEKTU DMS-LTV

Transakcie Správa používateľov TSA server Výber organizácie LTV

LTV Manual validation

Vložte súbor na validáciu

Vybrať súbor Nie je vybratý žiadny súbor

Odoslať

- **Archimetes-FUZKUV.xdc.xml.asice**

Subor je validny a bol prepodpísaný, stiahnite si novú verziu.

[Stiahnuť súbor](#) [Stiahnuť XML report](#) [Stiahnuť HTML report](#) [Zobraziť report](#)

Podpisuj.sk

Overenie podpisu dokumentu

Archimetes-FUZKUV.xdc.xml (2).asice

Výsledky overenia

Počet podpisov 2
Počet platných podpisov 2
Čas overenia 27.10.2019 22:22:39

- ▶ Ján Procháška (16.7.2019 20:31:22)
- ▼ Robert Kuchár (17.7.2019 10:33:56)

Formát podpisu
XAdES_BASELINE_LTA

Platnosť podpisu
Podpis je PLATNÝ
🔒 (Kvalifikovaný elektronický podpis)
▶ Podrobnosti

Rozsah podpisu
Archimetes-FUZKUV.xdc.xml
(Celý dokument)

Použité certifikáty

- KCA NBU SR 3
- SVK eID ACA
- Robert Kuchár

Časové pečiatky

Pridať Odobrať

Prípraviť na podpis

PRÍPADY POUŽITIA

Kde v praxi je potrebné dlhodobé overenie autorizácie elektronických dokumentov ?

- akýkoľvek dokument, ktorý úrad vyrobí, autorizuje, následne správoplatní (zas autorizuje ..) .. napríklad Rozhodnutie o dani musí mať úrad takto, aby mohol rozhodnutie dať na exekučný sud ..
- kolaudačne, stavebné, iné .. akékoľvek Rozhodnutie, ktoré by si účastník konania vyžiadal od úradu niekoľko rokov neskôr potom, ako bolo vydane ..
- účtovne dokumenty

OTVOR ENÉ VÝZVY ?

Čo sú najväčšie výzvy v oblasti LTA/LTV ?

- Legislatíva EÚ (eIDAS)
- Legislatíva SVK (LTA/LTV nie je ukotvené v žiadnom predpise)
- Nejasný praktický rozdiel medzi uložením dokumentu a jeho archivovaním

ĎAKUJEM
E ZA
POZORN
OSTĚ

www.podpisuj.sk

www.archimetes.com



[!\[\]\(e78f798d4ea5c530c9db49e7d26e6b95_img.jpg\)facebook.com/archim
etes](https://facebook.com/archimetes)

[!\[\]\(23d9fc146e83b5c3013cfa32c784f8d5_img.jpg\)Youtube.com/archimot](https://Youtube.com/archimot)