Dokumentácia technickej funkčnosti Modulu dlhodobého uchovávania a známych obmedzení

Zoznam zmien:

Dátum vydania	Verzia	Popis zmien
26. 03. 2021	1.0	

Úvod **2**
Obmedzenia využívania služieb modulu dlhodobého uchovávania **2**
Formáty podpisov a pečatí 2
Podpisy bez časových pečiatok alebo s neplatnými časovými pečiatkami 4
Uchovávanie elektronických správ z elektronickej schránky 4
Archívna forma systémových záznamov 5
Zobrazovaná informácia o platnosti podpisov 5
Prístup do MDU 6
Konverzia pôvodného dokumentu do PDF 6
Spôsob ochrany dokumentov a platnosti podpisov **6**
Stavy záznamov 10

Úvod

Modul dlhodobého uchovávania (ďalej aj „MDU“) je podľa zákona č. 305/2013 Z. z. o e-Governmente (ďalej len „zákon o e-Governmente) jedným zo spoločných modulov, ktoré slúžia pri elektronickej komunikácii na účely výkonu verejnej moci elektronicky.

Modul zabezpečuje na Ústrednom portáli verejne správy (ďalej aj „ÚPVS“) dlhodobé uchovávanie elektronických dokumentov, elektronických správ alebo registratúrnych záznamov, jednoznačnosť ich obsahu a platnosť elektronických podpisov. Do modulu je možné ukladať dokument (záznam) v ľubovoľnom formáte avšak veľkosť jedného záznamu je obmedzená na najviac 35 MB.

Dokumenty uložené do modulu dlhodobého uchovávania sú chránené v samotnom úložisku.
Po skončení uchovávania budú dokumenty vrátené do elektronickej schránky organizácie, ktorá o ich uchovávanie žiadala, a to v stave, v akom boli do MDU vložené, pričom v prípade kvalifikovaných elektronických podpisov a pečatí budú doplnené o kvalifikovanú časovú pečiatku, ak MDU pri vložení záznamu podporoval pridanie časovej pečiatky pre daný formát podpisu. V rovnakom stave sú poskytované uchovávané dokumenty aj v prípade vyžiadania dokumentov. Požadovanú minimálnu dobu uchovávania určuje používateľ, pričom môže uchovávanie kedykoľvek sám ukončiť alebo predĺžiť. Do roka 2021 sa dokumenty uchovávajú aj po zvolenej minimálnej dobe.
Pred plánovaným ukončením uchovávania budú používatelia informovaní oznamom.

Viac informácií o využití MDU nájdete v špecifickom návode pre využitie fyzickými/právnickými osobami alebo v návode pre využitie orgánmi verejnej moci.

Obmedzenia využívania služieb modulu dlhodobého uchovávania

Základné obmedzenia funkčnosti služby MDU boli pôvodne uvádzané v návode MDU a v Dokumentácii funkčnosti CEP, ktorú MDU využíva.

Formáty podpisov a pečatí

MDU v súčasnosti chráni:

- kvalifikované elektronické podpisy a pečate vo formátoch podporovaných v centrálnej elektronickej podateľni,

- zdokonalené elektronické podpisy založené na kvalifikovanom certifikáte vo formátoch XAdES, XAdES_ZEP a CAdES, s výnimkou PAdES (dané obmedzeniami CEP).

Chránené sú v MDU aj podpisy, ktoré boli vyhodnotené ako neplatné. Obvykle nie sú chránené v MDU podpisy, ktoré boli vyhodnotené ako neoveriteľné.

MDU v súčasnosti nechráni podpisy a pečate v záznamoch, ak obsahujú:

a) podpisy a pečate vyhotovené s nekvalifikovanými certifikátmi, nakoľko centrálna elektronická podateľňa získava údaje pre overenie platnosti certifikátu len pre kvalifikované certifikáty,
b) kvalifikované podpisy/pečate, ktoré centrálna elektronická podateľňa neumožňuje plne overiť a získať údaje pre overenie platnosti certifikátu (najmä v prípade stavu overenia „Neoveriteľná“),
c) podpisy/pečate vo formátoch nepodporovaných v centrálnej elektronickej podateľni ÚPVS,
d) ak v PAdES je vnorený podpis bez pripojenej časovej pečiatky pričom posledný podpis časovú pečiatku má (ide o chybu, ktorej opravu pripravujeme),
e) ak ide o vnorené podpisy alebo vnorené podpisové kontajnery (napríklad ASiC nachádzajúci sa v ASiC, PDF s PAdES nachádzajúci sa v ASiC alebo v XAdES_ZEP) vzhľadom na chýbajúcu podporu v službách CEP.

V prípadoch vnorených podpisov alebo podpisových kontajnerov je potrebné vkladať do MDU tieto vnorené podpisy samostatne. Je to možné napríklad nasledovným postupom:

- pripojiť do príloh žiadosti o uloženie v MDU dokument,
- v prílohách konštruktora správy sa po pripojení dokumentu zobrazí jeho obsah,
- kliknutím na „tri bodky“ je potrebné pre vnorený podpis / kontajner (.asice, .asics, .sce, .scs, .zep, .xzep, .zepx) zvoliť „Stiahnuť“, uložiť si ho do počítača a následne nahrať do prílohy ako samostatný súbor.

Neuchovávajú sa k nim v MDU teda ani údaje potrebné pre dlhodobé overenie platnosti. MDU chráni v prípadoch podľa písmena b) a e) len samotný podpísaný dokument proti narušeniu integrity. V prípadoch podľa písmena a), c), d) nie sú v súčasnosti vytvárané fixačné manifesty ani systémové záznamy (na úprave služby sa pracuje).

Podpisy bez časových pečiatok alebo s neplatnými časovými pečiatkami

V prípade záznamov obsahujúcich kvalifikované elektronické podpisy alebo pečate budú doplnené o kvalifikovanú časovú pečiatku, ak MDU pri vložení záznamu podporoval pridanie časovej pečiatky pre daný formát podpisu. V prípade nemožnosti pripojiť kvalifikovanú časovú pečiatku k podpisu alebo pečati neobsahujúcemu časovú pečiatku nie je záznam v MDU plne chránený.

Kvalifikovaná elektronická časová pečiatka sa **nepripája** k podpisom alebo pečatiam v záznamoch vložených do MDU:

a) ak podpis/pečať má pripojenú elektronickú časovú pečiatku – kvalifikovanú, nekvalifikovanú alebo neplatnú (t.j. v prípade foriem T, LT a LTA),
b) k podpisom/pečatiam PAdES, v ktorých nie je dostatok miesta na pridanie časovej pečiatky,
c) k podpisom/pečatiam vo formátoch nepodporovaných v centrálnej elektronickej podateľni v čase vloženia záznamu,
d) k podpisom/pečatiam vyhotoveným s nekvalifikovanými certifikátmi.

V prípadne nemožnosti pripojiť kvalifikovanú časovú pečiatku v bodoch b), c) a d) nie je záznam v súčasnosti v MDU plne chránený. Uvedené obmedzenia funkčnosti súvisia s obmedzeniami služby centrálnej elektronickej podateľne.

Čas začiatku ochrany záznamu

Vytvorenie systémového záznamu chrániaceho podpisy môže trvať niekoľko dní po odoslaní žiadosti, a to v závislosti od:

- dostupnosti údajov o platnosti certifikátu od vydavateľa kvalifikovaného certifikátu použitého v podpise alebo pečati,
- formátu podpisu (napr. pri PAdES podľa doby "caution period" v podpisovej politike Národného bezpečnostného úradu SR),
- vyťaženosti modulu.

Uchovávanie elektronických správ z elektronickej schránky

Elektronické správy uložené funkciou „Vložiť do MDU“ sa uchovávajú s nasledujúcimi obmedzeniami:

- neukladajú sa údaje o dátume a čase uloženia pôvodnej správy v elektronickej schránke,
- uchováva sa štruktúra MessageContainer a objekty v nej uložené, pričom nie je zachovaný digitálny odtlačok pôvodnej štruktúry správy (je zachovaný digitálny odtlačok jednotlivých objektov zo správy uložených v base64, nie je však zachovaný odtlačok štruktúry správy, a teda napríklad v prípade uloženia doručovanej správy nebude odtlačok uvedený v „Doručenke“ zhodný),
- neuchováva sa celá štruktúra Sk-Talk, nakoľko jednotným formátom elektronických správ je štruktúra MessageContainer. Uchovávajú sa jednotlivé objekty a atie sa pri vyžiadaní poskytnú používateľovi. (Poznámka: V prípade potreby opätovného uloženia celej elektronickej správy uchovávanej v MDU do elektronickej schránky a jej ďalšieho spracovania ako elektronickej správy je potrebné vyskladať Sk-Talk cez systémy tretích strán.)

Archívna forma systémových záznamov

MDU prevádza systémové záznamy na archívnu formu pred exspiráciou certifikátu pečate chrániacej systémový záznam. Z kapacitných a výkonnostných dôvodov môžu byť systémové záznamy prevádzané na archívnu formu až po exspirácii certifikátu pečate chrániace systémový záznam resp. po konci platnosti archívnej časovej pečiatky. Takéto systémové záznamy budú postupne dospracované počas roka 2021. Systémové záznamy vytvorené do konca roka 2018 vo formáte XAdES_ZEP budú na archívnu formu prevedené v roku 2021.

Upozornenie:
Vzhľadom na kapacitné obmedzenia MDU v súčasnosti neodporúčame ukladať do MDU väčšie množstvá nepodpísaných záznamov len pre účely archivácie. Modul dlhodobého uchovávania odporúčame používať primárne pre dlhodobé uchovávanie elektronických dokumentov podpísaných kvalifikovaným elektronickým podpisom alebo pečaťou.

Zobrazovaná informácia o platnosti podpisov

MDU pre overenie podpisov využíva informatívne overenie podpisov centrálnej elektronickej podateľne, ktoré nie je kvalifikovanou službou validácie kvalifikovaných elektronických podpisov alebo pečatí v zmysle Nariadenia EP a Rady EÚ č. 910/2014.

MDU v grafickom rozhraní v „Bádateľni“ zobrazuje informáciu o platnosti iba jedného podpisu, avšak pri viacerých podpisoch v rámci jedného súboru sa informácia

nezaznamenáva a nezobrazuje v MDU. Zobrazovaná je teda informácia o platnosti podpisu iba jedného z podpisov v danom podpisovom kontajneri.

MDU nerozlišuje, či je podpis/pečať zdokonalený založený na kvalifikovanom certifikáte alebo kvalifikovaný. Pri oboch zobrazuje informáciu „ZEP“ a informáciu o zistenej platnosti.

Platnosť podpisu je označená ako „Platná“ v prípade, ak všetky podpisy v danom dokumente sú vyhodnotené ako platné. V prípade, ak je jeden z podpisov neplatný, platnosť podpisu je označená ako „Neplatná“.

Modul v používateľskom rozhraní informatívne zobrazí aj výsledok informatívneho overenia podpisov, tento však nie je chránený integritným podpisom. Ak bol podpis vyhodnotený ako neplatný alebo neoverený, modul o tom zobrazí pri danom dokumente informáciu. Modul dlhodobého uchovávania rovnako overí, či ukladaný záznam neobsahuje poškodené súbory.

Prístup do MDU

Prihlásenie sa do používateľského prostredia modulu s názvom Centrálne úložisko záznamov je podmienené úspešným **prihlásením sa na portál**. Všetky funkcionality modulu sú sprístupnené iba **majiteľovi elektronickej schránky** alebo **osobe, ktorej bolo udelené plné zastupovanie** na prístup a disponovanie s elektronickou schránkou.

Konverzia pôvodného dokumentu do PDF

V prípade vyžiadania jednotlivých dokumentov zo záznamu uchovávaného v MDU so zvolením formátu dokumentu „PDF“ v žiadosti sú do schránky žiadateľa zaslané dokumenty skonvertované do formátu PDF/A-1a zapečatené pečaťou MIRRI – ÚPVS vo formáte PAdES. Aktuálne ide pri formátoch .txt, .rtf, .docx, .doc o demonštráciu funkčnosti.

Poznámky:
- nejde o zaručenú konverziu v zmysle zákona o e-Governmente,
- spoločne autorizované súbory sú pri konverzii v súčasnosti podporované iba čiastočne.

Spôsob ochrany dokumentov a platnosti podpisov

Ochrana dokumentov a platnosť podpisov je v MDU ÚPVS zabezpečená naraz pre päť záznamov (bez ohľadu na počet dokumentov v daných záznamoch) vytvorením tzv. systémového záznamu (Obr. 1), v ktorom sú integritným podpisom (kvalifikovanou elektronickou pečaťou) chránené digitálne odtlačky jednotlivých dokumentov (záznamov) a údajov potrebných pre overenie platnosti podpisového certifikátu v čase ukladania záznamu (CRL súbory s údajmi o zneplatnených certifikátoch platné v čase uloženia a overenia dokumentu v MDU, súbory podpisových certifikátov a certifikát vydavateľa certifikátu) a samotné súbory. Systémový záznam je uchovávaný aj po ukončení doby uchovávania dokumentu, ku ktorému sa viaže. Integritný podpis chrániaci digitálne odtlačky dokumentov je pred vypršaním jeho platnosti prevádzaný na archívnu formu.

Pre integritný podpis sa používa:

- od 1. júla 2020 kvalifikovaná elektronická pečať Ministerstva investícií, regionálneho rozvoja a informatizácie SR – ÚPVS,
- od 1. januára 2019 do 30. júna 2020 kvalifikovaná elektronická pečať Úradu podpredsedu vlády SR pre investície a informatizáciu,
- od roku 2014 do 31. decembra 2018 sa používala pečať Úradu vlády SR – ÚPVS.

Informácie o dostupnosti záznamu 486d58b7-2416-4583-ba9d-03be45f5e636

Záznam je verejne dostupný.

Informácie o zázname

Číslo záznamu	486d58b7-2416-4583-ba9d-03be45f5e636
Vlastník záznamu	ico://sk/50349287_10005
Názov	Validation Record Thu Feb 13 14:00:56 CET 2020
Značka	-
Popis	Records: bc1df00e-4e5d-45f4-80b3-31d734afbbc7 1f571d8d-179e-44b4-b947-aacd2843b3c4 235e44c0-6f64-4ee4-b04e-2058bb293dd5 11f7b36b-b663-4159-accb-75e873723afe 516cd635-3120-42b0-b96e-ec572335e8c3
Prístupnosť záznamu	Verejný
Dátum vytvorenia	13. 02. 2020
Exspirácia záznamu	
Veľkosť záznamu	17 MB
Overovacie údaje	-
Stav podpisu	Obsah chránený integritným podpisom
Stav záznamu	Aktívny

Zoznam dokumentov záznamu

	Názov súboru	Typ súboru	Podpis	Platnosť podpisu	Veľkosť
☐	Manifest_Fix_486d58b7-2416-4583-ba9d-03be45f5e636.xml	application/vnd.etsi.asic-e+zip	ZEP	Neoverený	7 kB
☐	CN=SNCA2, OU=SIBEP, O=Narodny bezpecnostny urad, L=Bratislava, C=SK_30830.cer	application/x-x509-ca-cert			1 kB
☐	OID.2.5.4.97=NTRCZ-26439395, O=První certifikační autorita, a.s., CN=I.CA TSACA/RSA 05/2017, C=CZ_11555516.cer	application/x-x509-ca-cert			1 kB
☐	SERIALNUMBER=NTRCZ-26439395, O=První certifikační autorita, a.s., CN=I.CA Qualified CA/RSA 07/2015, C=CZ_11638145.cer	application/x-x509-ca-cert			2 kB
☐	OID.2.5.4.97=NTRCZ-26439395, O=První certifikační autorita, a.s., CN=I.CA TSACA/RSA 05/2017, C=CZ_11555526.cer	application/x-x509-ca-cert			1 kB
☐	CN=SVK eID ACA, OU=ACA-307-2007-2, O=Disig a.s., L=Bratislava, C=SK_ba222819-88e7-4eb1-bfa9-fd3117227878.crl	application/pkix-crl			8 MB
☐	CN=KCA NBU SR 3, OU=SIBEP, O=Narodny bezpecnostny urad, L=Bratislava, C=SK_b46163b9-3d25-4b91-a686-229d685ff101.crl	application/pkix-crl			785 B
☐	CN=SNCA2, OU=SIBEP, O=Narodny bezpecnostny urad, L=Bratislava, C=SK_18fbe02c-dea2-472f-96ab-fe27f29a158a.crl	application/pkix-crl			8 kB
☐	Manifest_486d58b7-2416-4583-ba9d-03be45f5e636.xml	application/vnd.etsi.asic-e+zip	ZEP	Neoverený	9 kB

VYŽIADAŤ OZNAČENÝ DOKUMENT

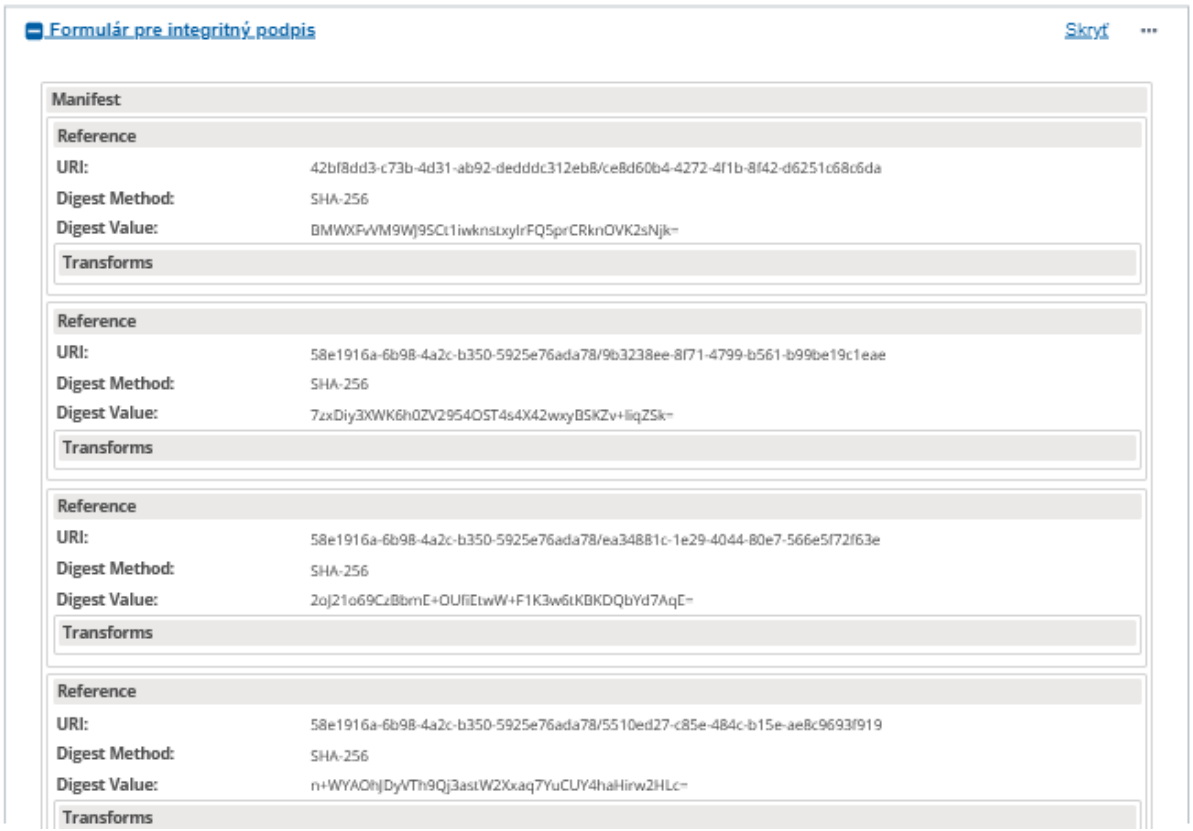
Obr.1 – Ukážka systémového záznamu

Systémový záznam obsahuje:

- Zapečatený fixačný manifest obsahujúci digitálne odtlačky samotných dokumentov vytváraný po uložení dokumentov do MDU, pričom pri podpísaných dokumentoch je vytváraný až po kontrole prítomnosti časovej pečiatky v podpisoch a úspešnom doplnení časovej pečiatky v prípade jej absencie. Fixačný manifest sa v prípade podpísaných dokumentov vytvára pred úplným overením podpisov a zozbieraním údajov pre dlhodobé overenie platnosti certifikátu.
- Finálny manifest (Obr. 2) vytváraný po úplnom overení podpisov, ak záznamy obsahujú podpisy. Ak podpisy neobsahujú, vytvára sa finálny manifest krátko po fixačnom manifeste.
- Podpisové certifikáty, certifikáty z certifikačnej cesty vydavateľa certifikátu osoby, ktorá dokument podpísala/zapečatila, certifikáty časových pečiatok.

Poznámka:
Systémový záznam neobsahuje informáciu o výsledku overenia platnosti podpisu alebo pečate, ktorú poskytla služba centrálnej elektronickej podateľne.

Manifest_58e1916a-6b98-4a2c-b350-5925e76ada78.xml



Obr. 2 - Manifest zo systémového záznamu obsahujúci digitálne odtlačky chránených dokumentov

Údaje o chránených dokumentoch sa uvádzajú v XML dátovej štruktúre elektronického formulára s identifikátorom MDURZ.Manifest. V manifeste sú uvedené údaje:

- URI - obsahuje číslo záznamu a za znakom „lomka“ oddelené interné číslo dokumentu v rámci záznamu,
- DigestMethod - hašovacia funkcia pre výpočet digitálneho odtlačku, v súčasnosti SHA-256,
- DigestValue - hodnota digitálneho odtlačku dokumentu vypočítaná hašovacou funkciou uvedenou v poli DigestMethod.

Ako dôkaz o predĺžení dôveryhodnosti a overiteľnosti platnosti podpisu alebo pečate v prípade, že je dokument podpísaný kvalifikovaným elektronickým podpisom alebo s mandátnym certifikátom alebo kvalifikovanou elektronickou pečaťou je možné použiť takzvaný systémový záznam označený v MDU ako „Overovacie údaje“. Tento záznam je možné z MDU vyžiadať na základe jeho čísla rovnako ako iné záznamy vložené používateľom.

Stavy záznamov

- Používateľský záznam:

Stav	Text	Popis
INGESTED	Vložený	Nastaví sa po vložení záznamu do MDURZ. Záznam je uložený, zatiaľ nie je chránený manifestom.
VALIDATED	Validovaný	Záznam bol analyzovaný, k podpísaným objektom bez časovej pečiatky bola pripojená kvalifikovaná časová pečiatka (t.j. boli rozšírené na T formu). Systémový záznam už môže byť vytvorený, avšak nie sú pozbierané všetky revokačné údaje a nie je vytvorený finálny systémový záznam.
PROTECTED	Chránený	Záznam je chránený – podpisy úplne overené, získané revokačné údaje a všetky objekty chránené integritným podpisom (prostredníctvom zapečateného manifestu). Systémový záznam je v stave CONTENT_PROTECTED.

- Systémový záznam:

Stav	Text	Popis
CONTENT_AGGREGATED	Vložený	Systémový záznam vytvorený – vytvorený fixačný manifest a systémový záznam označený za verejný. Všetky záznamy, ktoré ním budú chránené, označené (prelinkované).
CONTENT_FIXED	Zafixovaný	Fixačný manifest je podpísaný (zapečatený).
CONTENT_VALIDATED	Validovaný	Podpísané objekty zo záznamov overené, validačné údaje (CRL, certifikáty) pozbierané a uložené.
CONTENT_PROTECTED	Chránený	Vytvorený finálny manifest Manifest podpísaný (zapečatený) a uložený.

- Stav záznamu – stavy životného cyklu záznamu

Stav	Text	Popis
INCOMPLETE	Pripravuje sa	Záznam je vytváraný (postupne skladaný). Týka sa len Systémových záznamov. (Stav sa uvádza v prípade, ak záznam aktuálne čaká na dokončenie kroku spracovania, napríklad na vytvorenie manifestu, overenie v CEP a pod..)
ACTIVE	Aktívny	Platný aktívny záznam.
NEAR_EXPIRATION	Pred exspiráciou	Záznam blízko doby jeho exspirácie. Vlastník bol na blížiacu sa exspiráciu upozornený.