

Dokumentácia technickej funkčnosti Modulu dlhodobého uchovávania a známych obmedzení

Zoznam zmien:

Dátum vydania	Verzia	Popis zmien
26. 03. 2021	1.0	
23. 05. 2024	1.1	Aktualizácia informácií v kapitole 1, 2.1, 2.2, 2.3, 2.5, 2.6
05. 05. 2025	1.2	Aktualizácia informácií v kapitolách 1, 2.1, 2.2, 2.3, 2.5, 2.6, 2.8, 3, 3.1 v nadväznosti na aktuálnu funkcionality a poskytovanie kvalifikovanej dôveryhodnej služby. Doplnenie nového bodu 2.9 pre prípad nedostupnosti detailu záznamu.
25. 06. 2025	1.3	Doplnenie nového bodu 2.10 pre prípad dočasnej nedostupnosti platnej pečate systémového záznamu. Doplnenie nového bodu 2.11 pre prípad systémových záznamov, ktoré nechránia používateľské záznamy. Doplnenie bodu 2.12 pre prípad doplňujúcej kvalifikovanej pečate pre systémové záznamy.

1. Úvod.....	3
2. Obmedzenia využívania služieb modulu dlhodobého uchovávania.....	4
2.1. Formáty podpisov a pečatí.....	4
2.2. Podpisy bez časových pečiatok alebo s neplatnými časovými pečiatkami.....	5
2.3. Čas začiatku ochrany záznamu.....	6
2.4. Uchovávanie elektronických správ z elektronickej schránky.....	7
2.5. Archívna forma systémových záznamov.....	7
2.6. Zobrazovaná informácia o platnosti podpisov.....	8
2.7. Prístup do MDU.....	8
2.8. Konverzia pôvodného dokumentu do PDF	9
2.9. Nedostupnosť detailov záznamov.....	9
2.10. Dočasná nedostupnosť platnej pečate systémového záznamu.....	10
2.11. Nedostupnosť kvalifikovanej pečate systémového záznamu	10
2.12. Doplnujúce kvalifikované pečate pre systémové záznamy	11
3. Spôsob ochrany dokumentov a platnosti podpisov.....	11
3.1. Stavy záznamov.....	14

1. 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 elektronicke. Zároveň poskytuje kvalifikovanú službu uchovávania kvalifikovaných elektronických podpisov a pečatí v zmysle Nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách. Služby sú poskytované ako kvalifikované dôveryhodné služby v časových obdobiach od 14. januára 2018 do 31. decembra 2018 a od 12. decembra 2024.

Modul zabezpečuje na Ústrednom portáli verejnej správy (ďalej aj „ÚPVS“) dlhodobé uchovávanie elektronických dokumentov, elektronických správ alebo registratúrnych záznamov, jednoznačnosť ich obsahu a predlžovanie dôveryhodnosti elektronických podpisov aj po ich technologickej platnosti. 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 a zdokonalených elektronických podpisov a pečatí vložených bez pripojenej kvalifikovanej časovej pečiatky budú obsahovať doplnenú 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 bez ukončenia ich uchovávania. Požadovanú minimálnu dobu uchovávania určuje používateľ, pričom môže uchovávanie kedykoľvek sám ukončiť alebo predĺžiť. Do roku 2025 sa dokumenty uchovávajú aj po zvolenej dobe uchovávania, pokiaľ sa používateľ nerozhodne ukončiť uchovávanie zaslaním príslušnej požiadavky na ukončenie uchovávania. Pred plánovaným ukončením uchovávania budú používatelia v dostatočnom predstihu informovaní oznamom zaslaným do schránky vlastníka záznamu.

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

2. 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.

2.1. Formáty podpisov a pečatí

MDU v súčasnosti chráni:

- kvalifikované elektronické podpisy a pečate,
- zdokonalené elektronické podpisy založené na kvalifikovanom certifikáte (resp. vyhotovené s certifikátom vydaným kvalifikovaným poskytovateľom dôveryhodných služieb)

vo formátoch podporovaných v [centrálnej elektronickej podateľni](#).

Poznámka: Pôvodne do roku 2022 neboli v MDU chránené zdokonalené elektronické podpisy založené na kvalifikovanom certifikáte vo formáte PAdES, pričom tento problém bol v roku 2022 vyriešený.

Chránené sú v MDU aj podpisy, ktoré boli vyhodnotené v centrálnej elektronickej podateľni ako neplatné (t.j. sú k nim uchovávané údaje potrebné pre ich overenie – CRL/certifikáty). Nie je však predĺžená dôveryhodnosť podpisov, ktoré boli vyhodnotené ako neoveriteľné, nakoľko k nim nie sú získané dôkazové materiály (CRL, certifikáty).

MDU v súčasnosti nepredlžuje dôveryhodnosť podpisov a pečatí 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 a certifikáty vydané kvalifikovanými poskytovateľmi dôveryhodných služieb),
- 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 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 pre overovanie vnorených podpisov a vnorených kontajnerov v službách CEP.

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. (Pozn.: V prípadoch podľa písmena a) a c) dočasne nebolivytvárané fixačné manifesty ani systémové záznamy, problém bol vyriešený v roku 2021).

Dokument sa považuje za nepodpísaný v prípade, ak služba centrálnej elektronickej podateľne pre zistenie typu a formy podpisu vráti niektorý z výsledkov:

- Vstupné dáta neobsahujú podpis alebo obsahujú nepodporovaný typ podpisu (2123249)
- Nepodarilo sa dekomponovať zložený podpis (2123040).
- CMS neobsahuje žiadny podpis (2123238)
- Nepodarilo sa vyžiadať CMS (2123311)
- Nepodarilo sa inicializovať overovací komponent (2123212)
- Nepodporované dáta (2123042).

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, .pdf) zvoliť „Stiahnuť“, uložiť si ho do počítača a následne nahráť do prílohy ako samostatný súbor.

2.2. Podpisy bez časových pečiatok alebo s neplatnými časovými pečiatkami

V prípade záznamov obsahujúcich kvalifikované alebo zdokonalené elektronické podpisy alebo pečate bez pripojenej časovej pečiatky budú doplnené o kvalifikovanú časovú pečiatku, ak MDU a centrálna elektronickej podateľňa 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 chránený (nakoľko nie je možné v centrálnej

elektronickej podateľni vykonať úplné overenie podpisov a zozbierať CRL a certifikáty).

Kvalifikovanú elektronickú časovú pečiatku **nie je možné pripojiť** 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 (toto obmedzenie bolo odstránené v roku 2022 nahradením časových pečiatok pripájaných k podpisom dokumentovými časovými pečiatkami zahŕňajúcimi všetky predchádzajúce podpisy),
- c) k podpisom/pečatiam vo formátoch nepodporovaným v [centrálnej elektronickej podateľni v čase vloženia záznamu](#),
- d) k podpisom/pečatiam vyhotoveným s nekvalifikovanými certifikátmi.

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

MDU chráni digitálny odtlačok podpísaných dokumentov neobsahujúcich časové pečiatky až po tom, ako bola do nich pripojená kvalifikovaná časová pečiatka. Neuchováva resp. nechráni digitálny odtlačok podpísaných dokumentov v podobe bez pripojenej časovej pečiatky (resp. pred pripojením časovej pečiatky ak ju neobsahoval).

2.3. 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 podpisoch vytvorených do roku 2022 sa pri PAdES uplatňovala doba "caution period", ktorá bola uvedená do roku 2022 v podpisovej politike Národného bezpečnostného úradu SR do času, kým NBÚ aktualizovalo podpisovú politiku),
- vyťažnosti modulu.

2.4. 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 tie 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.)

2.5. Archívna forma systémových záznamov

MDU prevádza systémové záznamy na archívnu formu pred expiráciou certifikátu časovej pečiatky pripojenej k pečati chrániace systémový záznam. Z kapacitných a výkonnostných dôvodov môžu byť systémové záznamy prevádzané na archívnu formu až po expirácii certifikátu časovej pečiatky pečate chrániace systémový záznam resp. po konci platnosti certifikátu archívnej časovej pečiatky. Takéto systémové záznamy budú postupne dospracované ešte počas dôveryhodnosti služby časovej pečiatky podľa príslušného dôveryhodného zoznamu v zmysle Nariadenia eIDAS (stav služby „granted“). Systémové záznamy vytvorené do konca roka 2018 vo formáte XAdES_ZEP boli 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 pečatou, zdokonaleným elektronickým podpisom alebo pečatou založenými na kvalifikovanom certifikáte.

2.6. 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 Európskeho parlamentu a Rady EÚ č. 910/2014. Overenie v kvalifikovanej službe validácie preto potenciálne môže skončiť s iným výsledkom resp. informáciou o platnosti. MDU v rámci svojej funkcionality predlžuje dôveryhodnosť ochranou digitálnych odtlačkov uchovávaných dokumentov a údajov potrebných pre overenie kvalifikovaných podpisov a pečatí alebo zdokonalených elektronických podpisov a pečatí založených na kvalifikovanom certifikáte.

MDU v grafickom rozhraní v „Bádateľni“ zobrazuje orientačnú informáciu o platnosti iba jedného podpisu, avšak v prípade viacerých podpisov nachádzajúcich sa v rámci jedného súboru (resp. podpisového kontajnera) sa informácia nezaznamenáva a nezobrazuje v MDU. Zobrazovaná je teda sumárna informácia, aký bol najhorší zistený výsledok overenia platnosti podpisu v danom podpisovom kontajneri. MDU nerozlišuje, či je podpis/pečať zdokonalený založený na kvalifikovanom certifikáte alebo kvalifikovaný. Pri oboch zobrazuje informáciu o zistenej informatívnej platnosti. Napríklad: 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“ prípadne „nie je možné rozhodnúť“, platnosť podpisu je označená ako „Neplatná“ alebo „Nie je možné rozhodnúť“.

Modul v používateľskom rozhraní teda informatívne zobrazí aj sumárny výsledok informatívneho overenia podpisov, tento však nie je chránený integritným podpisom.

Platnosť podpisov, pečatí a časových pečiatok je potrebné na právne účely zisťovať s využitím údajov pre overenie podpisov uchovávaných v MDU.

Modul dlhodobého uchovávania rovnako v prípade podpísaných dokumentov overí, či ukladaný záznam neobsahuje poškodené súbory (v prípade poškodenia súboru po podpísaní súboru by sa podpis v rámci informatívneho overenia vyhodnotil ako neplatný).

2.7. 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.

2.8. 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 služby vo formáte PAdES. Aktuálne ide pri formátoch .txt, .rtf, .docx, .doc o demonštráciu funkčnosti, ktorá sa do budúcnosti plánuje odstrániť.

Poznámky:

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

2.9. Nedostupnosť detailov záznamov

V prípade automatizovaného spracovania väčšieho počtu záznamov v MDU môže byť nedostupná funkcionálna zobrazenia detailu jednotlivých záznamov v grafickom rozhraní a rovnako aj získanie detailných vlastností záznamu cez integračné rozhranie.

Dočasne nedostupné informácie a funkcionality tak môžu byť nasledovné informácie a funkcionality, pričom uvádzame pre také prípady aj náhradné postupy:

- identifikátor systémového záznamu slúžiaceho ako dôkaz o predĺžení dôveryhodnosti uchovávaných podpisov a pečatí,
 - NASES v takom prípade poskytne identifikátor systémového záznamu na vyžiadanie na základe žiadosti používateľa s použitím služby "Všeobecná agenda" do elektronickej schránky NASES,
- informácie o stave spracovania záznamu,
 - prevádzka NASES rieši prípadné problémy so spracovaním záznamu priebežne, nie je preto potrebné ich priebežne sledovať zo strany používateľa služby,
- informácia o zozname dokumentov záznamu, ich veľkosti a informatívnej platnosti podpisov
 - informácie o dokumentoch je možné získať zo žiadosti odoslanej do MDU, informatívnu platnosť dokumentov je možné získať v elektronickej schránke funkciou „Overiť podpisy“ pre jednotlivé dokumenty. Zároveň

*Vypracovala Sekcia stratégie, IT architektúry a riadenia projektov,
Národná agentúra pre sieťové a elektronické služby*

NASES poskytne informácie aj na základe žiadosti zo strany používateľa s použitím služby "Všeobecná agenda" do elektronickej schránky NASES.

- funkcionality vyžiadania konkrétneho dokumentu záznamu,
 - dostupná je funkcionality vyžiadania celého záznamu s použitím elektronickej schránky,
- funkcionality predĺženia uchovávania záznamu v grafickom rozhraní
 - dostupná je však možnosť predĺženia uchovávania cez integračné rozhranie a používateľ môže v prípade nedostupnosti v grafickom rozhraní bádateľne požiadať NASES o predĺženie uchovávania zaslaním žiadosti s použitím služby "Všeobecná agenda" do elektronickej schránky NASES.

Vyžiadanie záznamu a ukončenie uchovávania záznamu môžu používatelia v grafickom rozhraní elektronickej schránky vykonať s využitím tlačidla "Vyžiadať záznam", resp. "Ukončiť uloženie", ktoré sú dostupné v správe "Potvrdenie o vložení záznamu". Cez integračné rozhranie je možné záznam vyžiadať zaslaním príslušnej žiadosti cez integračné rozhranie podľa integračného manuálu.

2.10. Dočasná nedostupnosť platnej pečate systémového záznamu

V prípade spracovania väčšieho počtu záznamov v MDU počas júna a júla 2025 môže byť z dôvodu technického obmedzenia služby v prípade vyžiadania kvalifikovanej elektronickej pečate systémového záznamu vytvoreného do roku 2021 dočasne poskytovaná neplatná kvalifikovaná elektronická pečať. NASES počas tohto prechodného obdobia poskytne platnú kvalifikovanú pečať na základe žiadosti zo strany majiteľa záznamu chráneného danou kvalifikovanou pečaťou s použitím služby "Všeobecná agenda" zaslanej do elektronickej schránky NASES.

Od augusta 2025 bude služba poskytovať platné kvalifikované pečate aj pre takéto systémové záznamy.

2.11. Nedostupnosť kvalifikovanej pečate systémového záznamu

V prípade systémových záznamov vytvorených počas roka 2015, pre ktoré už v MDU nie sú uchovávané žiadne používateľské záznamy, nie je vykonávaný prevod pečatí na archívnu formu. Preto takéto pečate chrániace systémový záznam môžu byť po vyžiadaní neplatné.

2.12. Dopĺňujúce kvalifikované pečate pre systémové záznamy

V prípade systémových záznamov vytvorených počas 14. až 21. júna 2021 bola pre ich zapečatenie použitá podpisová prezentačná schéma určená pre zobrazovanie v elektronickej schránke namiesto podpisovej prezentačnej schémy. Z tohto dôvodu bola v systémových záznamoch dodatočne vytvorená druhá kvalifikovaná pečať manifestu, ktorá je následne poskytovaná v prípade vyžiadania obsahu systémového záznamu zo strany používateľa. Dátum pečate na systémovom zázname preto nemusí byť v súlade s dátumom vloženia používateľského záznamu do MDU.

3. Spôsob ochrany dokumentov a platnosti podpisov

Ochrana dokumentov a platnosť podpisov je v MDU ÚPVS zabezpečená naraz najviac 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 a chránený 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 12. decembra 2024 kvalifikovaná elektronická pečať NASES – Ústredný portál verejnej správy (certifikát zapísaný v dôveryhodnom zozname SR),
- 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 Slovenskej republiky – ÚPVS (certifikát zapísaný v dôveryhodnom zozname SR).

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
Expirácia 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_18f8e02c-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 informatívneho overenia platnosti podpisu alebo pečate, ktorú poskytl služba centrálnej elektronickej podateľne.

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

Formulár pre integritný podpis Skryť ...

Manifest	
Reference	
URI:	42b18dd3-c73b-4d31-ab92-dedddc312eb8/ce8d60b4-4272-4f1b-8f42-d6251c68c6da
Digest Method:	SHA-256
Digest Value:	BMWxFWM9Wj95Ct1iwnstxylrFQ5prCRknOVK2sNjK=
Transforms	
Reference	
URI:	58e1916a-6b98-4a2c-b350-5925e76ada78/9b3238ee-8f71-4799-b561-b99be19c1eae
Digest Method:	SHA-256
Digest Value:	7zxDiy3XWK6h0ZV2954OST4s4X42wxyB5KZv+liqZ5k=
Transforms	
Reference	
URI:	58e1916a-6b98-4a2c-b350-5925e76ada78/ea34881c-1e29-4044-80e7-566e5f72f63e
Digest Method:	SHA-256
Digest Value:	2oj21o69CzBbmE+OUfiEtWw+F1K3w6tKBKDQbYd7AqE=
Transforms	
Reference	
URI:	58e1916a-6b98-4a2c-b350-5925e76ada78/5510ed27-c85e-484c-b15e-ae8c9693f919
Digest Method:	SHA-256
Digest Value:	n+WYAOHjDyVTh9Qj3astW2Xxaq7YuCUY4haHirw2HLc=
Transforms	

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 je možné použiť takzvaný systémový záznam označený v údajoch systémového záznamu v MDU ako „Overovacie údaje“. Tento záznam je možné z MDU vyžiadať na základe jeho čísla rovnako ako iné záznamy vložené používateľom.

3.1. 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:

*Vypracovala Sekcia stratégie, IT architektúry a riadenia projektov,
Národná agentúra pre sieťové a elektronické služby*

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 expiráciou	Záznam blízko doby jeho expirácie. Vlastník bol na blížiacu sa expiráciu upozornený.
DELETED	Vymazaný (odstránený)	Záznam expiroval alebo bolo jeho uloženie ukončené na žiadosť vlastníka. Obsah záznamu sa už v úložisku nenachádza. (Nepoužíva sa pre systémový záznam, keďže ten sa uchováva trvalo.)