Informace pro vývojáře aplikací – září 2025

Datum: 17.09.2025
Verze: 1.1
Klasifikace: veřejný dokument

1 Anotace změn

1. Úprava v CAdES pečeti –> z VT na PROD
2. Služba pro přerazítkování (archivaci) –> z VT na PROD
3. Možnost uložit k registraci HSS v KP více certifikátů
4. Déletrvající AV skeny
5. Nový typ příloh – DDD tachografy –> pouze na VT
6. 4096 bitový certifikát domény

2 Harmonogram změn

Pro bod 1 a 2:

Na Veřejném testu od 27.3.2025, na Produkci od 18.9.2025.
Dokumentace verze 3.6 a odpovídající WSDL verze 3.09.

Pro body 3 a 4:

Na Veřejném testu i Produkci od 18.9.2025.

Pro bod 5:

Na Veřejném testu od 18.9.2025, na Produkci později

Pro bod 6:

Na Veřejném testu od prosince 2024, na Produkci v polovině října 2025

3 Popis změn

3.1 Úprava pečeti na stažených zprávách

Od 18.9.2025 dochází (v prostředí Veřejného testu již o půl roku dříve) k drobnějším změnám v CAdES podpisu (pečeti) stažené datové zprávy (tzv. ZFO formát).

Struktura (formát) pečeti (původně značky) DIA (původně MV) byla původně navržena dle standardu **ETSI TS 101 733 v1.8.3** (CAdES) v dubnu 2011. V době návrhu se nerozhodlo, jaká podpisová politika bude v pečetích ISDS použita. Jako náhrada bylo použito OID certifikační politiky pečetícího certifikátu

ISDS a žádná hash. Neuvedení hashe této politiky bylo možné, ale ve specifikaci nebylo technicky zcela přesně popsáno. Zvolené řešení bylo schváleno bezpečnostním auditem.

Od této nové verze (prozatím nasazené na VT) je opuštěno vkládání podpisové politiky, tedy mezivrstva odpovídající úrovni CAdES-EPES. Tato varianta, tj. pečeť bez atributu s podpisovou politikou, splňuje specifikaci **ETSI TS 103 173 v2.2.1**, nařízenou platným PROVÁDĚCÍM ROZHODNUTÍM KOMISE (EU) 2015/1506, které mají aplikace veřejné správy dodržovat. Varianta není v rozporu s novější specifikací **ETSI EN 319 122-1 v1.3.1** (která však dosud není pro ISDS, ani pro český eGov, závazná).

Vynechání mezivrstvy CAdES-EPES znamená také to, že pokud v okamžiku stahování datové zprávy by nebylo k dispozici časové razítko (výjimečná, spíše teoretická situace), byla by pečeť ve formátu CAdES-BES.

Tato nová varianta je konformní s referenční DSS aplikaci.

Pro běžné uživatele změna nepřináší žádné změny. Pokud však spisové aplikace provádějí rozebírání CAdES pečeti, resp. aplikují vlastní archivní razítka pro zprávy, měly by zkontrolovat, že zprávy stažené z VT prostředí nezpůsobí problémy, v opačném případě bude nutno aplikaci upravit. Změna byla proto nasazena půl roku v prostředí Veřejného testu.

3.2 Služba pro archivaci stažených zpráv (ZFO)

Přerazítkování zprávy v exportním formátu ZFO (CAdES), tj. přidání (prvního nebo dalšího) archivního časového razítka do stávajícího podpisu v pečeti, bylo dosud implementováno pouze v klientském portálu ISDS. Bylo rozhodnuto o vystavení této funkčnosti i do rozhraní webových služeb.

Webová služba ArchiveISDSDocument

Vstup:

- kompletní zapečetěný dokument ISDS (zpráva či doručenka) ve formátu ZFO (CAdES pečeť nad XML podobou zprávy či doručenky). Použije se (volitelně) MTOM/XOP.

Výstup:

- v případě úspěchu aktualizovaná verze vstupního dokumentu ISDS opět ve formátu ZFO, doplněná o nové informace zaručující platnost pečetě správce do konce platnosti nově přidaného časového razítka, jinak hodnota nil v elementu `dmResultDoc`. Volitelně MTOM/XOP.
- Datum, do kdy je nutno provést další razítkování v elementu `nextStampTo` jako datum exspirace posledního razítka minus jeden den.
- status operace v `dmStatus`, reflektující stavy dle tabulky níže (totožné s hlášením v KP).

Popis:

Služba přijme ISDS dokument (zprávu nebo doručenku) ve formátu ZFO a vrátí stejný dokument s přidaným razítkem. Podle formátu na vstupu platí:

- CAdES-EPES (-BES) -> CAdES-T – doplní se chybějící razítko do pečetě
- CAdES-T -> CAdES-A – přidá se první archivní razítko
- CAdES-A -> CAdES-A – přidá se další archivní razítko

Služba však umožní přerazítkování jen v posledních X časových jednotkách před exspirací. Hodnotu `nextStampTo` by si tedy spisovka měla nějakým způsobem (třeba i do názvu souboru, jako to dělá ISDS) uložit ke každému ZFO, aby nemusela naslepo zkoušet, kdy už bude přerazítkování povoleno (tj. zbytečně do systému ZFO nahrávat a očekávat chybu 2206). Není potřeba nutit vývojáře, aby rozebírali CMS strukturu pečetě za účelem zjištění data exspirace.

Spisovky by rovněž měly mít nějaký asynchronní proces na průběžné pře-razítkování zpráv, nejlépe v noci za malého provozu.

Stáří razítka – kdy přerazítkovat?

V Klientském portálu se v současnosti posuzuje, zda bude pečeť platná ještě po „dostatečně dlouhou" dobu a přerazítkování by tedy bylo zbytečné. Zjistí se zbývající doba platnosti posledního archivního razítka (z CAdES-A na vstupu) a je-li větší než rok a půl, vrátí se chyba 2206 a nové razítko se nepřidá. Pro WS rozhraní bude přísnější test než v KP: zjistí se zbývající doba platnosti **posledního razítka (podpisového či archivního)**, a je-li větší než půl roku, vrátí se chyba 2206 (platí pro prostředí PRODUKCE). Tímto omezením se zabrání přerazítkování zpráv stažených/přerazítkovaných jindy než v okně [- 6 let, -5,5 roku] a proto se hromadné jednorázové archivování starých zpráv po nasazení rozmělní v čase. Pro KP zůstane časové okno stejné jako dnes.

Chování **v prostředí Veřejného testu**: aby mohla být testována chyba 2206, je (pouze pro VT) změněno časové okno pro archivaci – archivaci je možno provést **již druhý den** po stažení zprávy.

Omezení služby:

Kromě omezení zbývající doby platnosti posledního časového razítka (půl roku) bude existovat limit N1 na **počet souběžně prováděných požadavků** a také limit N2 na počet souběžných požadavků jednoho klienta.

Limit **N1** bude nastaven na **20** a limit **N2** na **2**; půjde je konfiguračně měnit pro potřeby testování. Při překročení se vrátí chyba 2210.

Nový endpoint:

Nová WS (SOAP 1.2 kvůli MTOM/XOP) bude publikována na **endpointu ws2** pro VoDZ. Celá cesta bude:

```
https://ws2.mojedatovaschranka.cz/DS/arch
```

resp.

```
https://ws2c.mojedatovaschranka.cz/cert/DS/arch
```

atd. Případné omezování VoDZ komunikace dopadne tedy i na archivaci pomocí WS.

Nová služba je popsána ve WSDL verze 3.09.

Specifické aplikační chyby:

Služba může (kromě úspěchu) vrátit jednu z následujících chyb:

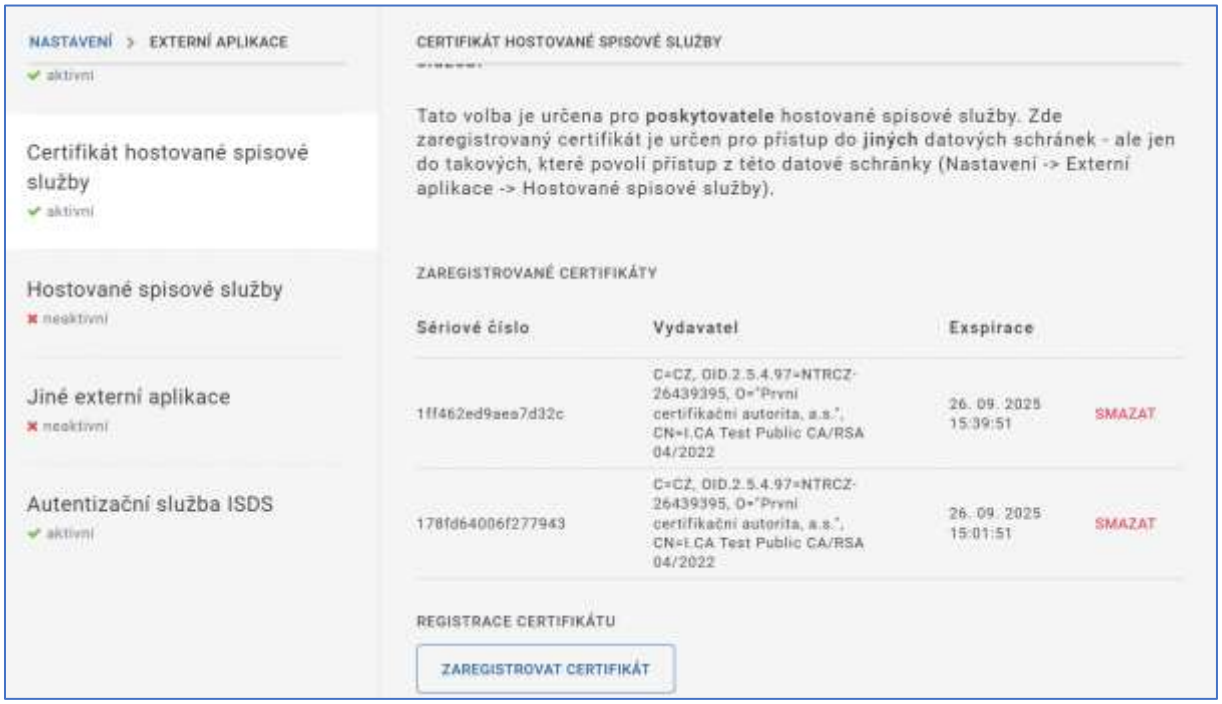
2200	"Předložená data nejsou ve formátu podepsané datové zprávy, dodejky ani doručenky."
2201	"Předložená data neodpovídají žádné datové zprávě, dodejce ani doručence."
2202	"Služba <služba> není zapnutá."
2204	"Nejsou splněny podmínky pro provedení re-autorizace, volejte službu ArchiveISDSDocument pro archivaci."
2205	"Platnost elektronické značky / pečeti MV vypršela. Archivace již není možná. "

2206	"Dokument v tomto okamžiku splňuje podmínky dlouhodobé průkaznosti a není třeba jej zatím doplňovat časovým razítkem"
2207	"Nepodařilo se získat časové razítko. Opakujte akci později. "
2208	"Neočekávaná chyba v procesu autorizace. Zkuste akci opakovat později, a pokud potíže přetrvávají, obraťte se na Infolinku. "
2209	"Od okamžiku získání posledního časového razítka neuplynula minimální lhůta <N> hodin. Opakujte akci po uplynutí minimální lhůty."
2210	"Překročen povolený limit souběžných požadavků. Opakujte, prosím, požadavek později. "
2212	"Nepodařilo se rozšířit podpis."
2214	"Nejsou splněny podmínky pro provedení archivace, zavolejte službu Re-signISDSDocument pro získání novější verze pečeti."

3.3 Registrace více certifikátů pro službu HSS

V dosavadní verzi ISDS bylo možno při registraci přístupového systémového certifikátu služby Hostovaná spisová služba (HSS) v klientském portálu vložit pouze jeden certifikát, a proto bylo nutno pravidelnou výměnu certifikátu složitěji plánovat, zejména pokud služba měla více klientů. Vložení druhého nahradilo první

Nově lze vložit certifikátů více – v portálu je vidět seznam vložených a všechny jsou použitelné (až do expirace). Vložené certifikáty jde také jednotlivě mazat.



Obrázek 1 - dva zaregistrované certifikáty pro HSS pod schránkou poskytovatele služby

3.4 Déletrvající AV skeny

V ojedinělých případech v současné verzi ISDS dochází k selhání AV kontroly přílohy, protože samotná kontrola není dokončena v nastaveném čase (vyprší timeout AV kontroly). Nejčastěji problém nastává

na mnohamegovém ZIPu obsahujícím velmi mnoho souborů ve formátu, který není triviální na posouzení antivirem, třeba PDF. Při překročení timeoutu dojde k odmítnutí přílohy a podle situace až odmítnutí odeslání celé zprávy. Odezva systému na překročení timeoutu AV je příliš obecnou hláška, ze které není poznat, proč se to stalo.

Základní timeout kontroly bude zvětšen na 25 sekund, a pokud do té doby kontrola neskončí, předá se do jiného procesu, který nebude zatěžovat normální provoz a kde bude kontrolován až 240 sekund.

Pro případ timeoutu (dlouhého) v KP nebo u WS **UploadAttachment** se odliší tato chyba od ostatních: vznikla nová chyba 2046 s textem „*U souboru <nazev> není možno v rozumném čase dokončit antivirovou kontrolu, proto byl odmítnut a nelze jej použít jako přílohu datové zprávy.*“.

V případě asynchronní kontroly běžné zprávy poslané přes webovou službu s BASE64 přílohou odesílatel i nadále nebude schopen odlišit výskyt viru od extrémně pomalé AV kontroly. Ale pro malé zprávy bude timeout velmi řídký (byl navýšen).

Reálný dopad na aplikace, které vkládají velké přílohy pro VoDZ, je nutnost čekat až 240 sekund na reakci WS **UploadAttachment**.

3.5 Soubory DDD jako přílohy datové zprávy

Na žádost významných uživatelů ISDS byl mezi povolené přílohy datové zprávy přidán formát digitálních tachografů, binárních souborů s příponou DDD.

Technické specifikace souborového formátu .ddd vychází z nařízení Komise (EU) 2016/799 ze dne 18. března 2016, kterým se provádí nařízení Evropského parlamentu a Rady (EU) č. 165/2014, kterým se stanoví požadavky na konstrukci, zkoušení, montáž, provoz a opravy tachografů a jejich součástí, které definuje způsob uchovávání a přenosu těchto dat. Toto nařízení pak v příloze odkazuje na normy ISO/IEC 7816-n, která stanoví technické parametry a standardy pro elektronickou výměnu dat. Nařízení bylo novelizováno nařízením Komise (EU) 2018/502 (pro druhou generaci tachografů).

Ze zjištění plyne, že existují dva druhy DDD souborů – z tachografů a karet řidiče. Tyto dva druhy se binárně odlišují a musejí se kontrolovat odlišně. ISDS bude propouštět oba typy.

DDD formát nemá specifický MIME-type – bude se proto používat obecný `application/octet-stream`.

Existují i soubory tachografů s jinými příponami (např. „c1b“, „v1b“ a „tgd“), těch se ale dle požadavku Správce změna netýká, používají se u nás minimálně. Přidání je ale možné, případně pište Správci ISDS.

Dočasně bude nasazeno pouze na Veřejném testu ISDS. Vzorky na zkoušení budou uloženy na vývojářském webu poradnaisds.cz v sekci Testovací prostředí > Dokumentace a formuláře.

3.6 4096 bitový certifikát domény

V reakci na Doporučení v oblasti kryptografické bezpečnosti, platné od 1.7.2023, vydané NUKIBem, se postupně na všech prostředích mění klíč pro šifrování doménového certifikátu – z délky 2048 bitů se přechází na klíč s délkou 4096 bitů. V prostředí Veřejného testu ISDS je nový certifikát (GeoTrust) již nasazen od prosince 2024, na Produkci bude nasazen nyní, v polovině října 2025 (předpoklad je 23.10.2025).

Změna ve velikosti veřejného klíče v doménovém certifikátu může mít teoreticky negativní vliv na napojené aplikace třetích stran, proto byl nový doménový certifikát v dostatečném předstihu nasazen na prostředí VT, aby dodavatelé měli dostatek času otestovat kompatibilitu svých aplikací.