Informace pro vývojáře aplikací – březen 2025

Datum: 04.04.2025
Verze: 1.1
Klasifikace: veřejný dokument

1 Anotace změn

1. Omezení počtu stránek u výsledku fulltextového vyhledávání
2. Možnost nahlášení „spamu“ a označení podezřelých zpráv
3. Úprava v CAdES pečeti – pouze VT
4. Služba pro přerazítkování (archivaci) – pouze VT
5. Výměna autority u podpisového certifikátu e-mailových notifikací

2 Harmonogram změn

Pro bod 1 a 2:

Na Veřejném testu od 30.1.2025, na Produkci od 27.3.2025.

Dokumentace verze 3.5 a odpovídající WSDL verze 3.08.

Pro body 3 a 4:

Na Veřejném testu ISDS od 27.3.2025.

WSDL verze 3.09 – pouze na VT

Pro bod 5:

Na Veřejném testu od 13.3., na Produkci později

3 Popis změn

3.1 Omezení počtu stránek u výsledku fulltextového vyhledávání

Služba **ISDSSearch3** (i starší **ISDSSearch2**) může vracet neomezený počet stránek výsledků fulltextového hledání schránek.

Služba **ISDSSerach3** umožňuje stránkování výsledků pomocí dvou parametrů: `pageSize` = velikost stránky a `page` = pořadové číslo stránky. Zatímco velikost stránky je omezena na 100 záznamů (konstanta MAXSIZE), počet stránek omezen není - služba má v případě, že se žádá o stránku, která neobsahuje žádné výsledky, vracet prázdnou odpověď. Spisovky obvykle rozumně stránkují výsledky doporučeným způsobem (od první až do poslední neprázdné).

Kvůli jedné nerozumné aplikaci ISDS zavádí nový test vstupních parametrů. Bude zavedena konstanta MAXPAGE, implicitně = 99 (stránky jsou počítány od 0, tedy max. počet stránek je 100). Systém bude kontrolovat, že zadaná hodnota požadované stránky s výsledky (page) není větší než MAXPAGE. Pokud ano, vrátí se nová aplikační chyba č. 1189 s textem „Příliš velká hodnota parametru page.“

Až 100x100 výsledků fulltextu je daleko více, než spisové aplikace potřebují k vyhledání schránky. Tato služba nemá fungovat jako zdroj dat o schránkách.

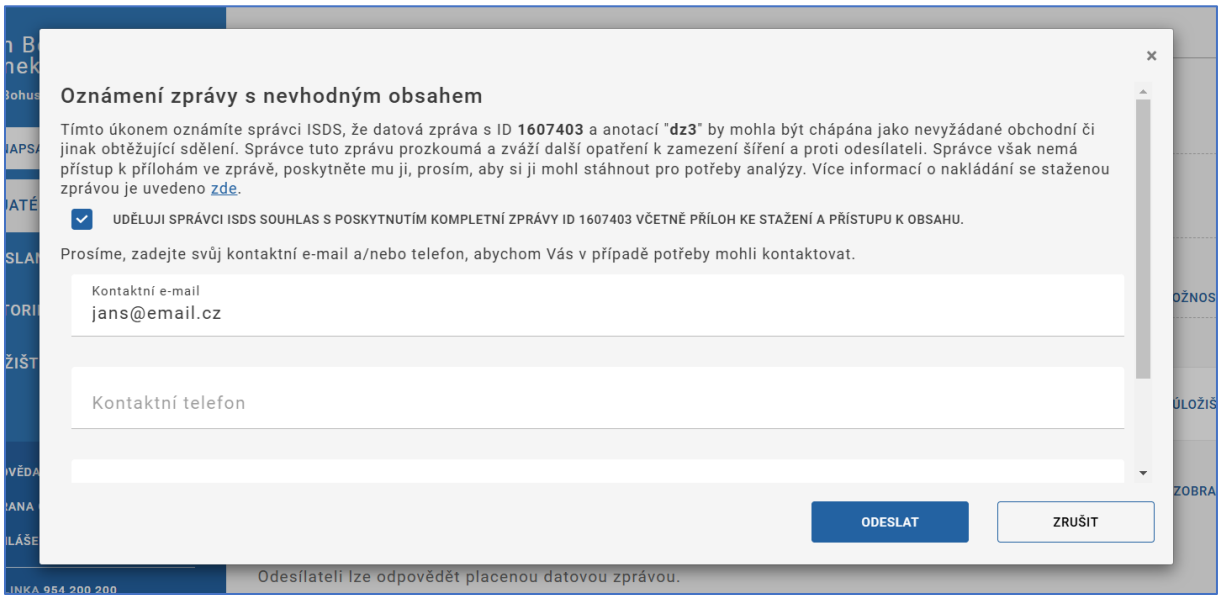
Prozatím nasazeno na VT pro úpravu aplikací.

3.2 Nahlášení „spamu“ a nový příznak u zpráv

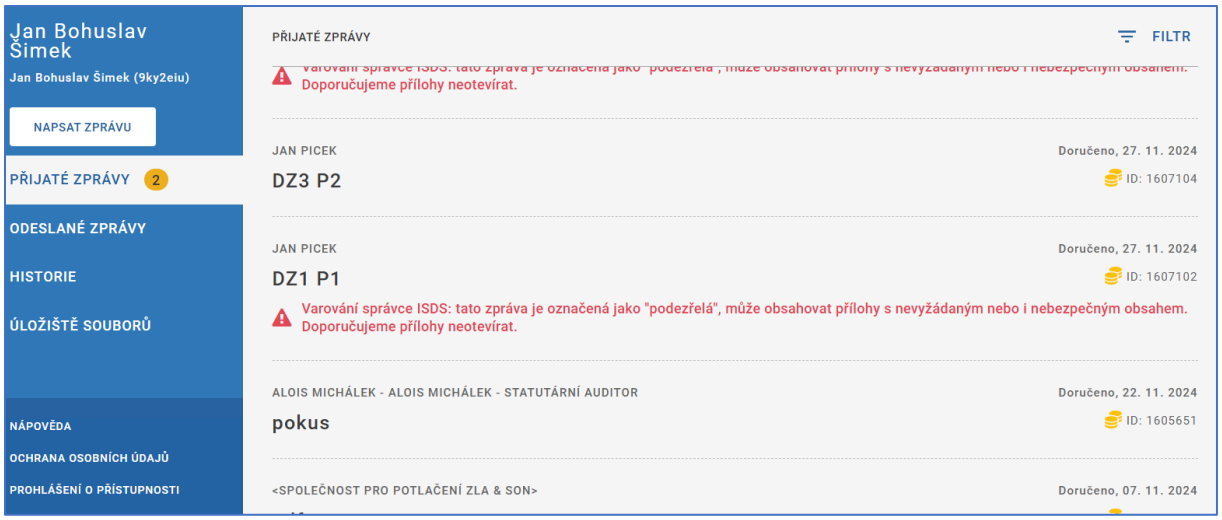
V ISDS byl implementována možnost nahlášení podezřelých nebo obtěžujících zpráv (zaslaných po datu nasazení, nelze aplikovat na starší zprávy), jejich analýza a případné zpětné označení takových zpráv novým příznakem (+ různá opatření proti odesílateli). Aplikace se na to měly připravit. Správce vydá metodická doporučení, jak na případy podezřelých zpráv mají aplikace reagovat.

Změny jsou zavedeny ve WSDL/XSD definicích **verze 3.08**.

Obdobné nahlášení bude možné provést i z klientského portálu (z detailu došlé zprávy):



Zpráva s případným příznakem bude výrazně označena:



Aplikace by se měly chovat podobně.

3.2.1 Nová služba pro nahlášení „podezřelé zprávy“

Existuje veřejná WS **SuspMessageReport**, na vstupu povinně ID zprávy a nepovinně jméno, kontaktní email a telefon a příznak Předat komplet a Poznámka. Zpráva musí být došlá do schránky volajícího a musí v ní ještě existovat (nebýt u daného příjemce – oznamovatele smazaná), jinak se oznámení odmítne. Nesmí být ze schránky OVM ani zpráva systémová.

Vstup:

- `dmID` – ID oznamované zprávy, povinné
- `repName` – jméno oznamovatele, nepovinné
- `repMail` – kontaktní mail oznamovatele, nepovinné
- `repTel` – kontaktní telefon oznamovatele, nepovinné
- `allowComplete` – BOOL příznak svolení se stažením kompletní zpráv včetně příloh, povinné
- `note` – obecná poznámka, nepovinná

Výstup:

- status

Specifické aplikační chyby:

- 1600 Zpráva se zadaným ID neexistuje mezi živými zprávami
- 1609 Systémovou zprávu nelze nahlásit jako spam
- 1610 Zprávu ze schránky typu OVM nelze nahlásit jako spam
- 1611 Lze nahlásit pouze zprávu z vlastní schránky
- 1612 Zprávu z datového trezoru nelze nahlásit jako spam
- 1613 Zprávu s tímto nebo starším datem doručení nelze nahlásit jako spam
- 1614 Nepovolený formát telefonního čísla
- 1615 Nepovolený formát e-mailové adresy
- 1616 Oznamovatel musí být příjemcem nahlášené zprávy

Popis:

Pokud uživatel spisové aplikace nabude podezření, že došlá zpráva (kromě zpráv zaslaných ze schránek OVM!) vykazuje znaky „spamu“ (tj. nevyžádané obchodní sdělení, opakované bezdůvodné urážení, možnost mallware apod.), může takovou zprávu nahlásit touto službou správci. Správce provede analýzu zprávy a rozhodne o oprávněnosti oznámení.

Je třeba zadat ID existující zprávy došlé do schránky, z níž je služba volána a povolit správci stažení kompletní zprávy (tj. ekvivalent stažení a poslání, správce sám stahovat zprávy nemůže). Pokud stažení nebude povoleno, pak v případě, že nikdo jiný zprávu nenahlásí, bude pravděpodobně oznámení odloženo, protože bez příloh se analýza provést nedá.

Samotným nahlášením zprávy tato zpráva nezíská žádný nový příznak. Teprve po analýze, která může trvat hodiny až dny, se tato zpráva (a její „kopie“ v jiných schránkách) může zpětně označit jako „podezřelá“ a získá speciální příznak, abys ní mohla aplikace zacházet „jinak“.

3.2.2 Nový příznak v seznamech a detailech

Zprávy, které analýza spamu označí jako podezřelé, získají speciální příznak. Příznak se objeví u níže uvedených služeb u elementu `dmRecord` (nebo obdobného, detaily v XSD) jako nepovinný atribut `specMessFlag="1"`:

- **GetListOfReceivedMessages**
- **MessageEnvelopeDownload**
- **MessageDownload**
- **BigMessageDownload**

3.2.3 Zablokování stahování

Zcela výjimečně, pro případy nebezpečného agresivního malware, který prošel AV kontrolou jako příloha zprávy, bude mít správce možnost u některých zpráv zablokovat stahování. Aplikace pak při volání služeb na stažení zprávy dostane specifickou chybu 3022 „Správce zakázal stažení této zprávy (antiSpam opatření).“. Při získání této chyby by aplikace měla přestat tuto zprávu stahovat (je zbytečné to zkoušet dokola) a kontaktovat podporu ISDS.

3.3 Úprava pečeti na stažených zprávách

Od 27.3.2025 dochází (v prostředí Veřejného testu) 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, měli by zkontrolovat, že zprávy stažené z VT prostředí nezpůsobí problémy, v opačném případě bude nutno aplikaci upravit. Změna byla proto nasazena v prostředí Veřejného testu, a teprve po otestování vývojáři bude (spolu s novou službou pro archivaci – viz následující kapitola) nasazena do Produkce. Pokud budete mít technické dotazy, neváhejte nás kontaktovat přes Poradnu.

3.4 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, je implementováno pouze v klientském portálu ISDS. Bylo rozhodnuto o vystavení této funkčnosti i do rozhraní webových služeb. Prozatím bude k dispozici jen na Veřejném testu.

WS 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 se 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."

3.5 Nová autorita pro podpis notifikačních mailů

Pro podepisování notifikačních e-mailů se historicky používá certifikát vystavený autoritou PostSignum. Protože zahraniční mailové systémy začaly tento podpis označovat jako nedůvěryhodný a odrazují příjemce od čtení takto podepsaných e-mailů, bylo rozhodnuto o jeho nahrazení autoritou Digicert.

Pokud aplikace zpracovává notifikační maily automatizovaně, zkontrolujte si prosím, že nový podpis nic ve zpracování nezmění.

V prostředí VT se nový podpis používá od 13.3.2025, o nasazení na PROD nebylo zatím rozhodnuto.