Informace pro vývojáře aplikací – červen 2022

Datum: 03.06.2022
Verze: 1.2
Klasifikace: veřejný dokument

1 Anotace změn

1. Je zavedeno přidání volitelné přidání osobních dat odesílatele do datové zprávy. Jedná se kompatibilní změnu, úprava je doporučená, ne však nutná. Aplikace, které budou chtít tyto údaje číst, musí použít novou službu **GetMessageAuthor2**.
2. Je zaveden speciální typ datové zprávy Výhradně do vlastních rukou (VVR). Změna se týká pouze aplikací, které obsluhují schránky typu FO a přihlašují se do ISDS pomocí serverového certifikátu (typ Spisová služba nebo Hostovaná spisová služba).
3. Je nově omezena délka názvu přílohy na 255 znaků včetně přípony.
4. V souladu s všeobecně doporučovanými postupy budou v ISDS vypnuty nedoporučené šifrovací sady pro TLS. Toto opatření může mít dopad na některé zastaralé, neaktualizované aplikace, které se připojují k ISDS.

2 Harmonogram změny

Bod 1: V prostředí veřejného testu i produkčního ISDS se změny objeví po odstávce 5.6.2022.

Bod 2: Na Veřejném testu od 5.6.2022, na Produkci od 1.1.2023.

Bod 3: Na Veřejném testu od 5.6.2022, na Produkci od 1.1.2023.

Bod 4: Na Veřejném testu je již nastaveno od jara 2021, v produkčním ISDS od 5.6.2022. Držitelé schránek, jejichž aplikace na jaře 2022 používaly tyto šifry, byli upozorněni.

3 Popis změn

3.1 Osobní údaje v datové zprávě

Popsáno v dokumentaci verze **2.75**.

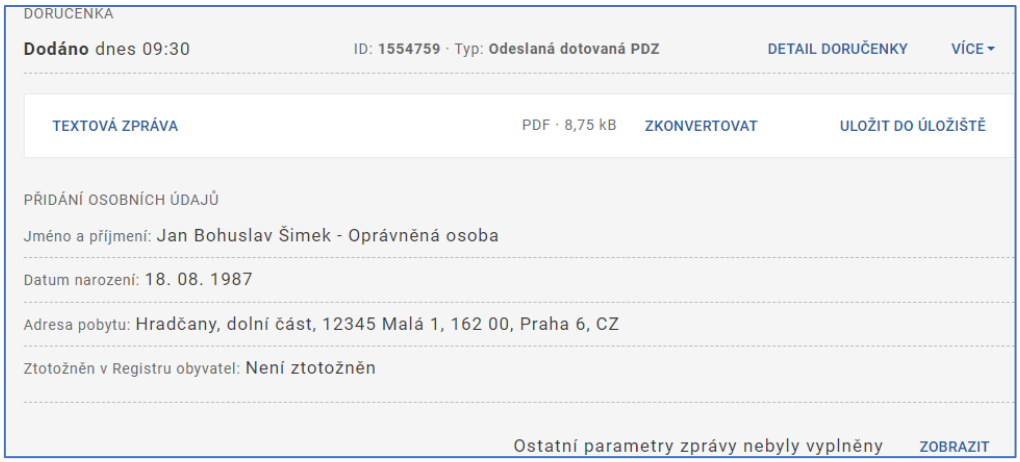
Do každé datové zprávy mohou být dobrovolně přidány osobní údaje odesílající osoby, aby příjemce mohl snadněji identifikovat odesílatele. Ve staré verzi ISDS se mohlo přidat jen jméno a příjmení (role ve schránce se přidává automaticky a nejde ji zakázat), v nové verzi zle přidat jméno, příjmení, datum narození, místo narození, adresní kód, složenou adresu a příznak, je-li tato osoba ztotožněné v ROB (tedy jsou-li údaje aktualizované). Pro osobní údaje ve zprávě platí:

1. Volitelný výčet údajů včetně hodnot v době odeslání zprávy se přidá k metadatům obálky v systému, nepřidává se do ZFO exportu zprávy
2. Výčet údajů (bez hodnot) se přidá i do uloženého konceptu nedokončené zprávy.
3. Příjemce si může stáhnout osobní údaje podle výčtu u každé DZ pomocí WS nebo přečíst v KP u detailu zprávy (ale pouze 3 měsíce od dodání).
4. Po načtení ZFO exportované zprávy v portálu ISDS, zaslané s výčtem atributů, se stejně jako dnes nezobrazí výčet a hodnota povolených atributů.

Portáloví uživatelé při odeslání zprávy si sami vyberou, jaké své osobní údaje přiloží ke zprávě:

Obrázek 1 - podoba klientského portálu ISDS

Podobně portál ISDS zobrazuje v detailu došlé či odeslané zprávy tyto údaje:



Obrázek 2 - detail zprávy s osobními údaji

Aplikace podobné chování při odeslání zprávy musí implementovat (chce-li to využívat).

3.1.1 Výčet osobních dat

Tabulka 1 - přehled údajů, které lze zapsat ke zprávě

	hodnota	hodnota „key“	popis
vždy (od roku cca 2010)	0	userType	typ uživatele (role ve schránce); nabývá hodnot "PRIMARY_USER" (vlastník, primární oprávněná osoba, statutární zástupce) dále „LIQUIDATOR“ pro likvidátora, „RECEIVER“ pro nuceného správce nebo „GUARDIAN“ pro opatrovníka PO, "ENTRUSTED_USER" (pověřená osoba), "ADMINISTRATOR" (administrátor schránky), "OFFICIAL" (pro systémovou zprávu), "VIRTUAL" (spisovka) nebo nil pro hodně staré zprávy
u starých zpráv	1	pnGivenNames	křestní jména, např. Jan Bohuslav
		pnLastName	příjmení, např. Šimek, u typu VIRTUAL je zde identifikátor aplikace
u nových zpráv (navíc ke jménu a příjmení)	2	biDate	datum narození ve tvaru YYYY-MM-DD
	4	biCity	místo narození, např. Opočno (jen u pověřených osob schránek FO či PFO, ne profesních)
	8	biCounty	okres narození, např. Dobruška, u cizinců stát narození (jen u pověřených osob schránek FO či PFO, ne profesních)
	16	adCode	adresní kód RUIAN, např. 2536358
	32	fullAddress	složená adresa
	64	robIdent	příznak, že osoba je ztotožněná s ROB a údaje jsou tudíž aktualizované

Některé požadované údaje se v ISDS nevedou u všech uživatelů. Zatímco jméno je u všech uživatelů (někdy nestrukturované), datum narození a adresa u většiny, adresní kód jen u ztotožněných osob, místo a okres narození jen u ztotožněných držitelů schránek FO a PFO.

Pokud zprávu odesílá aplikace se serverovým certifikátovým přístupem, nelze určit fyzického uživatele, proto již dnes pracuje ve WS s konstantou „VIRTUAL“ a ve jménu identifikátor spisovky odvozený z ID schránky (v KP označeno jako „Spisová služba“).

Pokud se jedná o systémovou zprávu, vrací se role „OFFICIAL“ a prázdné údaje (v KP nic).

3.1.2 Odeslání zprávy

Ve staré verzi WS pro odeslání zprávy používá nepovinný příznak `dmPublishOwnID` pro přidání jména a příjmení odesílající osoby

```
…
    <p:dmPersonalDelivery>false</p:dmPersonalDelivery>
    <p:dmAllowSubstDelivery xsi:nil="true"/>
    <p:dmPublishOwnID>true</p:dmPublishOwnID>
  </p:dmEnvelope>
…
```

V nové verzi je možno určit výčet údajů. K elementu `dmPublishOwnID` bude možno přidat nepovinný atribut `IdLevel` , integer složený jako součet hodnot jednotlivých údajů v tabulce výše.

Podoba XML bude A) pro povolení **všech** údajů:

```
…
    <p:dmLegalTitlePoint xsi:nil="true"/>
    <p:dmPersonalDelivery>false</p:dmPersonalDelivery>
    <p:dmAllowSubstDelivery xsi:nil="true"/>
    <p:dmPublishOwnID IdLevel="127">true</p:dmPublishOwnID>
  </p:dmEnvelope>
  <p:dmFiles>
…
```

B) Pro povolení **pouze jména a příjmení** lze použít po novu

```
…
    <p:dmLegalTitlePoint xsi:nil="true"/>
    <p:dmPersonalDelivery>false</p:dmPersonalDelivery>
    <p:dmAllowSubstDelivery xsi:nil="true"/>
    <p:dmPublishOwnID IdLevel="1">true</p:dmPublishOwnID>
  </p:dmEnvelope>
  <p:dmFiles>
…
```

nebo postaru

```
…
    <p:dmLegalTitlePoint xsi:nil="true"/>
    <p:dmPersonalDelivery>false</p:dmPersonalDelivery>
    <p:dmAllowSubstDelivery xsi:nil="true"/>
    <p:dmPublishOwnID>true</p:dmPublishOwnID>
  </p:dmEnvelope>
  <p:dmFiles>
…
```

C) Pro nepovolení **ničeho** (tj. pouze role ve schránce) lze použít

```
…
    <p:dmLegalTitlePoint xsi:nil="true"/>
    <p:dmPersonalDelivery>false</p:dmPersonalDelivery>
    <p:dmAllowSubstDelivery xsi:nil="true"/>
    <p:dmPublishOwnID>false</p:dmPublishOwnID>
  </p:dmEnvelope>
  <p:dmFiles>
…
```

nebo element vůbec nezadat:

```
…
    <p:dmLegalTitlePoint xsi:nil="true"/>
    <p:dmPersonalDelivery>false</p:dmPersonalDelivery>
    <p:dmAllowSubstDelivery xsi:nil="true"/>
  </p:dmEnvelope>
  <p:dmFiles>
…
```

3.1.3 Čtení údajů ve zprávě

Existuje služba **GetMessageAuthor**, které vrací roli (vždy), jméno a příjmení (podle volitelného příznaku) osoby, která odeslala zprávu. Tato služba zůstane i nadále použitelná v původní podobě.

Stará služba **GetMessageAuthor** se bude chovat i pro (nové) zprávy s povoleným výčtem větším než 1 stejně jako dnes, vrátí roli, jméno a příjmení, nic víc. Pokud se služba použije na starou zprávu (tj. odeslanou před 5.6.2022), bude přidáno omezení na dobu, po níž lze data o odesílateli (jméno a

příjmení) číst: *3 měsíce ode dne dodání*. Po této lhůtě služba vrátí jen roli z doby odeslání, nic víc.

Pokud bude stará služba **GetMessageAuthor** použita na novou zprávu, obsahující osobní údaje, pak pokud je v údajích jméno a příjmení, vrací jméno a příjmení z doby odeslání, jen po dobu života zprávy.

3.1.3.1 Nová služba

Vznikne nová služba **GetMessageAuthor2**, která bude vracet rozšířenou množinu údajů ve tvaru klíč – hodnota. Služba bude připravená na případné přidávání dalších údajů.

Operace: **GetMessageAuthor2**

Vstup:

- `dmID` – ID zprávy

Výstup:

Opakovací sekce `dmMessageAuthor`, obsahující jednotlivé údaje o odesílateli. Jednotlivé hodnoty budou vraceny jako atributy elementu `maItem`:

```
<dmMessageAuthor>
  <maItem key="string" value="string" />
</dmMessageAuthor>
```

Popis:

Příjemce nebo odesílatel zprávy může zavolat tuto WS, aby zjistil informaci o konkrétním odesílateli zprávy. Ptát se je možné na zprávy jakéhokoliv typu, ne však na smazané zprávy.

Atribut `key` nabývá hodnot podle tabulky výše.

Typ odesílatele (`UserType`) je u zpráv po 27.11.2010 k dispozici vždy, ostatní údaje o odesílateli jen pokud to odesílatel povolil při odeslání DZ. Povolené prázdné hodnoty a nepovolené hodnoty se nevracejí.

Hodnota „VIRTUAL“ v `UserType` znamená přístup externí aplikace, která se přihlašuje skrze systémový certifikát (SS nebo HSS - tedy ne účtem konkrétní osoby). Přihlášení přes HSSU (např. Portál občana) je prováděno pod účtem osoby.

Testuje se jen oprávnění a příslušnost zprávy ke schránce.

Oprávnění:

Nutné schránkové oprávnění *PRIVIL_VIEW_INFO* (čtení seznamů a doručenek).

Příklad 1 (kompletní data pro ztotožněného držitele schránky FO, povoleno vše):

```
<dmMessageAuthor>
  <maItem key="userType" value="PRIMARY_USER" />
  <maItem key="pnGivenNames" value="Jan Ladislav" />
  <maItem key="pnLastName" value="Novák" />
  <maItem key="biDate" value="1989-12-29" />
  <maItem key="biCity" value="Opočno" />
  <maItem key="biCounty" value="Dobruška" />
  <maItem key="adCode" value="2536358" />
  <maItem key="fullAddress" value="Mšenská 45, 19425 Karusice, CZ" />
  <maItem key="robIdent" value="true" />
</dmMessageAuthor>
```

Příklad 2 (nekompletní data pro neztotožněného statutára schránky PO, povoleno vše, nestrukturované údaje):

```
<dmMessageAuthor>
  <maItem key="userType" value="PRIMARY_USER" />
```

```
  <maItem key="pnLastName" value="Horst Mueller />
  <maItem key="fullAddress" value="Braunenschweig, Am Hasselteich 31, DE" />
</dmMessageAuthor>
```

1.1.1.1 Shrnutí chování GetMessageAuthor a GetMessageAuthor2:

Novou zprávou se myslí zpráva odeslaná po 4.6.2022.

	stará zpráva	**nová zpráva**
GetMessageAuthor	chová se jako dnes – vrací aktuální jméno a příjmení, ale jen po 3 měsíce od dodání, pak již nevrátí jméno a příjmení, pouze roli	pokud je v metadatech jméno a příjmení, vrací jméno a příjmení z doby odeslání, ale jen po dobu života zprávy
GetMessageAuthor2	chová se jako GetMessageAuthor (tj. omezení na 3 měsíce)	chová se dle popisu - vrací to, co odesílatel zatrhnul, ale jen po dobu života zprávy

Důsledek změny chování ke starým zprávám je, že aktualizované údaje o odesílateli (z formátu staré zprávy) se definitivně přestanou zobrazovat 3 měsíce po nasazení. Pravděpodobnost, že toto někdo potřebuje využívat, je minimální.

3.1.4 Nové definice služeb

Upravené či nové služby jsou popsány ve `dm_info.wsdl` a `dmBaseTypes.xsd` verze 2.35. Pro aplikace, implementující změny k roku 2023 proti Veřejnému testu ISDS, je totéž obsaženo ve verzi 3.01.

3.2 Zpráva výhradně do vlastních rukou (VVR)

Systémové zprávy, obsahující přístupové údaje, zasílané ze systémové schránky správce „aaaaaaa“ do schránky FO příjemce těchto přístupových údajů, jsou v současné verzi označeny jako „Zpráva do vlastních rukou“. Takovou zprávu může číst i pověřená osoba ve schránce, resp. aplikace přistupující systémovým certifikátem (jako Spisová služba nebo Hostovaná spisová služba). Novelou zákona bylo rozesílání přístupových údajů zpřísněno, takové zprávy (obsahující čitelné přístupové údaje) může nově číst jen oprávněná osoba (držitel, majitel) schránky FO, které jsou určeny, nikdo jiný.

Byl proto zaveden speciální typ datové zprávy „Zpráva výhradně do vlastních rukou“ (VVR). Neplánuje se obecné použití v komunikaci mezi schránkami, využití je pouze pro zasílání přístupových údajů. Zpráva typu VVR bude doručena přihlášením pouze v případě, že se přihlásí uživatel, který ji může číst (tj. adresát). Doručení fikcí zůstává beze změny.

Příznak je interní, v popisu DZ pro webové služby není vidět. Klientský portál s ním pracuje tak, že VVR nabídne v seznamu došlých, nedovolí ale otevření (ani nedojde k doručení přihlášením) jiné osobě, než je oprávněná osoba ve schránce FO, místo toho upozorní na tuto situaci.

Externí aplikace (pouze ty, které obsluhují schránky FO) s tím musejí počítat a správně reagovat na chybová hlášení. Netýká se aplikací, které přistupují ke zprávám pod účtem oprávněné osoby (tedy i aplikace Portál občana) – pro ně se nic nemění.

Kdy **nebude umožněno** zprávu typu VVR doručit (a zůstane ve stavu Dodána (4)):

1. Pokud se přihlásí jakýmkoliv způsobem pověřená osoba či administrátor, bez ohledu na nastavená práva.
2. Pokud se přihlásí externí aplikace, používají serverový certifikát ve variantě Spisová služba (SS) nebo Hostovaná spisová služba (HSS).

Pak zpráva ve stavu Dodána (4) nebo Doručena fikcí (5) nelze stáhnout pomocí WS a nelze otevřít v KP.

Kdy **nebude umožněno** zprávu typu VVR ve stavu > 5 přečíst/stáhnout:

1. Pokud se přihlásí jakýmkoliv způsobem pověřená osoba či administrátor, bez ohledu na nastavená práva.

3.2.1 Důsledky pro aplikace

Externích aplikací se serverovým certifikátem není pro schránky FO mnoho, ale mohou se objevit. Taková aplikace bude stahovat seznamy zpráv současným způsobem, ale VVR zůstane ve stavu (4) Dodána, nebude doručena přihlášením. Pokud je aplikace rozumně napsaná, nestahuje zprávy ve stavu 4, protože ví, že to skončí chybou č. 1222 *„Zpráva dosud nebyla označena jako doručená, proto ji nelze číst“* (již dnes se v seznamu přijatých mohou objevit zprávy dodané až po zahájení subprocesu Doručení přihlášením, které budou pro tento okamžik ve stavu 4, až do příštího stažení seznamu přijatých).

Aby mohla aplikace reagovat specificky na tuto novou (řídkou) situaci (odlišně od reakce na chybu 1222, kdy má význam to zkusit ještě minimálně jednou), bude se v případě pokusu o stažení nedoručené zprávy typu VVR vracet jiná, nová chyba číslo 1178 – *„Pokus o stažení nedoručené zprávy určené výlučně do vlastních rukou adresáta“*.

Doporučujeme, aby při výskytu chyby 1178 aplikace neopakovala stahování a nějakým způsobem informovala adresáta o této situaci s doporučením, aby si zprávu stáhnul na klientském portálu (nebo Portálu občana).

Aplikacím bude umožněno (na rozdíl od portálu), aby již doručenou VVR mohly stahovat, v opačném případě by se muselo složitě rozlišovat, jde-li o chybu při stavu VVR 4 či 5 (kdy se musí reagovat) od téže chyby při stavu VVR větším než 5 (kdy by se muselo ignorovat).

Časté jsou i externí aplikace, které se přihlašují jménem a heslem uživatelů svých klientů, ale zde se používají pro toto přihlášení obvykle pověřené osoby, a ne osoby oprávněné. I v tomto případě se nepodaří stáhnout VVR a aplikace musí nějak reagovat. Pokud je tato externí služba natolik komplexní, že přebírá i příjem notifikací, tak se oprávněná osoba o VVR zprávě nemusí vůbec dozvědět a ta se doručí fikcí.

3.3 Omezení délky názvu přílohy

Název přílohy, vkládaný do datové zprávy pomocí webové služby **CreateMessage** nebo **UploadAttachment** (pro VoDZ) atributem `dmFileDescr`, bude omezen na 255 znaků včetně přípony. Týká se normálních zpráv i velkoobjemových.

V případě, že v atributu webové služby bude nalezen delší název, vrátí služba chybu číslo 1280 *„Příliš dlouhé jméno přílohy“* a zpráva se neodešle (příloha VoDZ se neuloží).

3.4 Vypnutí starých šifrovacích sad

V souladu s doporučovanými bezpečnostními postupy bylo rozhodnuto o úpravě konfigurace webového serveru, která odstraní zastaralé šifrovací sady používající šifrovací metodu AES v CBC módu. Jde o pokračování řetězce úprav bezpečnostní konfigurace, které mohou mít dopad na některé staré nebo chybně nakonfigurované aplikace a spisové služby.

V rámci těchto úprav dojde k odstranění dosluhujících šifrovacích sad používajících AES v módu CBC, který NÚKIB ve svém doporučení (https://www.nukib.cz/download/uredni_deska/Kryptograficke_prostredky_doporuceni_v1.0.pdf) již na konci roku 2018 označil jako potenciálně problematický. Tyto šifrovací sady se již příliš nepoužívají, neboť jsou v novějších aplikacích nahrazeny aktuálními šifrovacími sadami protokolu TLSv1.2.

Na produkčním prostředí bude vypnuta podpora těchto šifrovací sad:

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67)

Pro ověření funkčnosti se stačí přihlásit do nějaké schránky v testovacím prostředí ISDS. Pro naprostou většinu aplikací se nic nezmění, stejně tak jako pro uživatele webové aplikace Klientský portál ISDS.