Informace pro vývojáře aplikací – leden 2022 – Veřejný test ISDS

Datum: 18.01.2022
Verze: 1.4
Klasifikace: veřejný dokument

1 Anotace změn

1. Lze odeslat datové zprávy o velikosti příloh nad 20 MB, cílově až 1024 MB, tzv. **VoDZ**, čili Velkoobjemové DZ.
2. Končí zasílání až 50 MB datových zpráv do vybraných několika schránek OVM_REQ.
3. Jsou povoleny kontejnerové formáty ZIP a ASiC (u běžných DZ i VoDZ), s určitými omezeními.
4. Je omezen počet příloh v jedné zprávě, normální i velkoobjemové.

Tyto změny jsou v roce 2022 nasazeny pouze v prostředí Veřejného testu ISDS.

2 Harmonogram změny

V prostředí veřejného testu ISDS (VT) se změny objeví po odstávce 7.1.2022. Na produkčním ISDS (PROD) budou změny nasazeny **až k 1.1.2023**. Týká se klientského portálu i webových služeb.

Vývoj ISDS je v tomto okamžiku rozdělen – na VT a na PROD jsou výrazně odlišné verze WS (odpovídající WSDL verzím 2.34 a 3.0). Vývojáři mají cca rok na to připravit se na změny na PROD od roku 2023, ale současně musí udržovat stávající verzi, protože pokud by bylo nutno řešit nějakou situaci, bude oprava v roce 2022 provedena do stávající verze 2.34 (i do 3.0).

Věříme, že nová verze rozhraní ISDS bude intenzivně od začátku roku testována vývojáři na vývojovém prostředí a není vyloučeno, že finální verze dozná případných změn na základě zpětné vazby. Předpokládáme, že finální verze bude uzavřena v polovině roku.

2.1 Dokumentace změn

Změny ve veřejné dokumentaci budou prozatím udržovány v této podobě, aktuální dokumentace v Provozním řádu bude odpovídat verzi nasazené na PROD. V druhé polovině roku 2022 vznikne dokumentace odpovídající WSDL verze 3.0 ve finální podobě.

Pro čtení tohoto dokumentu je nezbytné velmi dobře znát aktuální příručku z Provozního řádu ISDS *WS_manipulace_s_datovymi_zpravami.pdf, verze 2.74* (nebo novější, pokud ještě vznikne), tento text ji rozšiřuje a doplňuje. V textu bude odkazováno na tuto příručku pomocí symbolu **[1]**.

2.2 Kompatibilita změn

Změny jsou pojaty jako rozšíření stávajícího rozhraní o nové služby, určené pro přenosy objemnějších dat v souvislosti s VoDZ. Kde se zpravování DZ a VoDZ setkává (zejména seznamy zpráv), je VoDZ rozpoznatelná novým atributem, který sice není uveden ve stávajícím WSDL (v. 2.33), ale z principu nepřináší nekompatibilitu při zpracování SOAP odpovědi.

Aplikace, neupravené dle tohoto dokumentu, mohou po roce 2023 nadále fungovat postaru (pokud budou ignorovat nové atributy), ale neodešlou VoDZ (což pro stávající způsob používání ISDS nevadí) a nestáhnou došlou VoDZ (což vadit může). Aplikace dostane speciální chybu a jediná cesta, jak se k takové došlé VoDZ může adresát dostat, je použít klientský portál.

3 Velkoobjemové zprávy

3.1 VoDZ stručně

1. Jsou zavedeny **Velkoobjemové zprávy** (**VoDZ**) s max. velikostí příloh určenou technickým limitem, který bude nastaven na produkčním prostředí na 1 GB, uložené odlišně od běžných zpráv (do 20 MB). Horní limit je konfigurovatelný, a) pro budoucí rozvoj a b) pro nasazení na VT, kde může být z provozních důvodů velikost omezena, zprvu na 250 MB a bude se podle provozní situace upravovat.
2. Použití VoDZ není nijak omezeno, např. typem schránky příjemce či odesílatele, není povolováno či jednotlivě zakazováno.
3. Pro VoDZ se použije stejný exportní formát datové zprávy jako dnes, tedy soubor s příponou ZFO, tvořený XML daty obalenými CAdES podpisem. Soubory ZFO (obsahujícího přílohy v BASE64 kódování) pro VoDZ mohou mít velikost přes 1 GB a aplikace s tím musí počítat.
4. Zavedení VoDZ nahrazuje velké zprávy pro OVM_REQ (do 50 MB), zavedené novelou zákona v roce 2019.
5. VoDZ bude možno použít jak veřejnou DZ, tak i jako Poštovní DZ.
6. Nebude umožněno použití velkých příloh v multizprávách, ani se nebudou používat v systémových zprávách.
7. Nebude umožněno odesílání VoDZ z Odesílací brány.
8. Prozatím není omezeno ukládání VoDZ v trezorech, budoucí stav na PROD bude záviset na podmínkách ČP.
9. Je velmi pravděpodobné, že VoDZ nad 50 MB jako celek, ani samotné PDF přílohy větší než 50 MB nepůjde konvertovat do listinné podoby

3.2 Nový endpoint pro služby pracující s VoDZ

Vznikla nová verze WSDL (**verze 3.0**) pro některé stávající a nové služby. Pro použití MTOM/XOP ve službách musí být **použit SOAP verze 1.2**. Je vystaven nový, **samostatný endpoint**, i proto, aby se oddělily oba toky, aby bylo možno nezávisle sledovat objemy dat, případně vytvořit vlastní instanci AV kontroly aj. **Tok dat na novém kontextu bude sledován a v případě velkého objemu zpomalován či omezován**. Díky oddělení endpointů nebude mít možné zahlcení velkými zprávami zásadní dopad na provoz běžných zpráv.

Stávají endpoint zůstane v provozu prakticky beze změny pro manipulaci s malými zprávami. Aplikace budou muset implementovat obě rozhraní.

K dnešnímu endpointu pro WS manipulující se zprávami (na Veřejném testu – přesný popis a alternativy v **[1]**)

`https://ws1.czebox.cz/DS/[dz|dx]` pro basic autentizaci jménem a heslem

resp.

`https://ws1c.czebox.cz/.../DS/[dz|dx]` pro certifikátové přístupy apod.

je vytvořen nový endpoint pouze pro nové služby:

`https://ws2.czebox.cz/DS/vodz`

resp.

`https://ws2c.czebox.cz/DS/vodz`

Na Produkčním prostředí bude záměna `czebox` -> `mojedatovaschranka`.

3.3 Seznam služeb

V prostředí Veřejného testu ISDS budou současně existovat dvě verze webových služeb:

- **Verze 2.34** (SOAP 1.1) – pro ty, kteří dosud neimplementovali VoDZ. Od stávající verze 2.33 na produkčním prostředí se liší pouze novým XSD souborem (`dmBaseTypes.xsd`), společným pro staré i nové služby (s označením verze 3.0).
- **Verze 3.0** (SOAP 1.2 s MTOM/XOP i SOAP 1.1) – pro implementaci VoDZ. Od verze 2.34 se liší (kromě komentářů) jedním novým souborem `dm_VoDZ.wsdl`; soubor `dmBaseTypes.xsd` verze 3.0 je shodný s verzí v 2.34.

Na produkčním prostředí od 1.1.2023 bude k dispozici už jen verze 3.x.

3.3.1 Nové služby pro VoDZ

Balíček WSDL 3.0 definuje v souboru `dm_VoDZ.wsdl` (includující definice z `dmBaseTypes.xsd` verze 3.0) následující služby pro velké zprávy (SOAP 1.2).

CreateBigMessage	vytvoření VoDZ s použitím předem nahraných příloh (VoDZ varianta služby **CreateMessage**)
AuthenticateBigMessage	ověření validity VoDZ (VoDZ varianta služby **AuthenticateMessage**)
UploadAttachment	nahrání jedné (velké) přílohy pro budoucí použití ve VoDZ
DownloadAttachment	stažení jedné velké přílohy z VoDZ, alternativa ke stažení celé zprávy do ZFO souboru
SignedBigMessageDownload	stažení celé došlé VoDZ do ZFO souboru (VoDZ varianta služby **SignedMessageDownload**)
SignedSentBigMessageDownload	stažení celé odeslané VoDZ do ZFO souboru (VoDZ varianta služby **SignedSentMessageDownload**)
BigMessageDownload	stažení XML podoby datové zprávy, včetně příloh (VoDZ varianta služby **MessageDownload**)

3.3.2 Pozměněné služby, pro DZ i VoDZ

Tyto služby jsou definované v souboru `dm_info.wsdl`, verze 3.0 i verze 2.34, (SOAP1.1), změny jsou uvedeny v `dmBaseTypes.xsd` (verze 3.0) Pro běžné zprávy se nic nemění, VoDZ jsou odlišeny jedním nebo dvěma novými atributy.

GetListOfReceivedMessages	seznam došlých zpráv, běžných i VoDZ najednou

GetListOfSentMessages	seznam odeslaných zpráv, běžných i VoDZ najednou
MessageEnvelopeDownload	stažení obálky zprávy, běžné i VoDZ

Další, zde neuvedené služby pro manipulaci se zprávami (obsažené v `dm_info.wsdl` nebo v `dm_operation.wsdl` verze 3.0 nebo verze 2.34), lze použít jak na normální zprávy, tak na VoDZ. Jedná se o stažení doručenky **GetDeliveryInfo**, označení zprávy jako Přečtená **MarkMessageAsDownloaded**, seznam zpráv, u nichž došlo ke změně stavu **GetMessageStateChanges**, získání informace o odesílateli **GetMessageAuthor**, vymazání trezorové zprávy **EraseMessage**, seznam obálek smazaných zpráv **GetListOfErasedMessages**, stažení informací pro externí notifikace **GetListForNotifiations**. Popis je uveden v **[1]**.

Ostatních služeb (vyhledávání, související s přístupem, správa schránek a uživatelů) se změny netýkají.

3.4 MTOM/XOP

U webových služeb na novém endpointu, které přenášejí jedním nebo druhým směrem velký objem dat, lze data předat v binární podobě, definované standardem MTOM/XOP, a ušetřit tím zdroje oproti BASE64 kódování.

Služby, které zasílají do ISDS velký objem dat (**UploadAttachment, AuthenticateBigMessage**) mohou vstupní data předat v binární podobě, pokud využijí SOAP 1.2 a `Content-Type: application/xop+xml` nebo `multipart/related`. Pokud nebude požadavek rozpoznám jako validní, vrátí systém HTTP chybu 599 a v SOAP Fault přibližný popis:

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://www.w3.org/2003/05/soap-envelope"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
   <SOAP-ENV:Body>
      <SOAP-ENV:Fault>
         <SOAP-ENV:Code>
            <SOAP-ENV:Value>SOAP-ENV:Sender</SOAP-ENV:Value>
         </SOAP-ENV:Code>
         <SOAP-ENV:Reason>
            <SOAP-ENV:Text xml:lang="en-US">Outer Content-Type has type
parameter=application/soap+xml, should be application/xop+xml. Use SOAP 1.2.</SOAP-
ENV:Text>
         </SOAP-ENV:Reason>
      </SOAP-ENV:Fault>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Služby, které vracejí velký objem dat (**DownloadAttachment**, **SignedBigMessageDownload**, **SignedSentBigMessageDownload**) mohou vracet data buď v BASE64 kódování uvnitř XML odpovědi nebo jako samostatnou binární část v multipart odpovědi (při použití SOAP 1.2, tj. `Content-Type: application/soap+xml;charset=UTF-8`). Tvar výstupních dat si volající aplikace volí sama použitím headeru `Accept`:

- pokud v SOAP 1.2 požadavku bude existovat hlavička `Accept:` obsahující možnost `multi-part/related`, vrátí se data podle standardu MTOM/XOP (místo binárních dat v BASE64 je odkaz na jinou část odpovědi, která obsahuje tato data přímo, bez zakódování do BASE64.)

- pokud v požadavku není hlavička `Accept:` (nebo neobsahuje možnost `multipart/related`), vrátí se v odpovídajícím elementu požadovaná data v BASE64 kódování.

3.5 Doporučený způsob práce

Stažení zpráv:

1. na starém endpointu volá seznam zpráv (**GetListOfReceivedMessages**) a prochází jednotlivé zprávy, pokud není zpráva VoDZ (nový atribut `dmVODZ`), pracuje postaru (na starém endpointu);
2. pokud je zpráva VoDZ, stáhne ZFO v novém endpointu (**SignedBigMessageDownload**) nebo
3. stáhne si obálku (**MessageEnvelopeDownload**), přečte počet příloh (nový atribut `attsNum`) a stahuje jednotlivé přílohy (**DownloadAttachment**).

Odeslání zprávy:

1. aplikace spočte sumární velikost příloh budoucí zprávy, pokud je menší než 20 MB, pracuje jako dnes (**CreateMessage** na starém endpointu),
2. pokud je větší než 20 MB, provede upload jednotlivých příloh (**UploadAttachment**) a výsledky uploadu použije v popisu nové zprávy na novém endpointu (**CreateBigMessage**).
3. případně stáhne podepsanou odeslanou VoDZ pomocí **SignedSentBigMessageDownload.**

Stažení doručenky:

1. jako dnes na starém endpointu.

Stažení obálky:

1. jako dnes na starém endpointu.

Verifikace zprávy:

1. aplikace buď zná typ zprávy a pak volí pro normální zprávy a doručenky starou službu (**AuthenticateMessage**) a pro VoDZ novou službu (**AutenticateBigMessage**),
2. nebo zná jen velikost ZFO, a pak volí podle velikosti starou či novou službu (zprávy s velikostí příloh okolo 20MB je možno verifikovat na obou endpointech).

3.6 Manipulace s přílohami

3.6.1 UploadAttachment

Služba na uložení přílohy do úložiště velkých příloh (UVP). Předpokládá se použití pro velké přílohy, ale není zakázáno vkládat i menší přílohy (aby se zachovalo stejné chování jako pro Portál). Celkový součet velikostí příloh pro jednu zprávu bude muset překročit limit pro VoDZ (zatím 18 MB).

Vstup:

- **Příloha** – zadaná jako BASE64 text nebo binární část multipart požadavku při použití MTOM/XOP
- **Mime typ** a **název souboru** v atributech.

Výstup:

- **Identifikátor přílohy** – použije se při sestavení nové velkoobjemové zprávy
- **Hashe přílohy** – aplikace by si měla, po úspěšném uložení, zkontrolovat vrácené hashe se svými výpočty a v případě rozdílu upload opakovat. Oba hashe (definovaného algoritmu) také použije při sestavení **CreateBigMessage**.
- **Algoritmus hashů**

Popis:

Služba vloží jeden soubor do úložiště velkých příloh ISDS. Aplikace ji pak může později použít jako přílohu datové zprávy. Neporušenost souboru lze zkontrolovat pomocí vrácených hashů. Algoritmy hashů se mohou v čase měnit.

Se souborem budou provedeny synchronní kontrola antivirem, kontrola přípustnosti použitého formátu a kontrola souladu obsahu s deklarací – v případě chyby se příloha neuloží, důvod se zapíše do kódu a textu chyby.

Nahranou přílohu lze použít opakovaně v různých VoDZ, po dobu její existence v úložišti.

Je stanovena konstanta provozní konstanta o velikosti 10*max_velikost_příloh (tj. standardně 10 GB, na testu zpočátku 2,5 GB). Při vložení nové přílohy pomocí **UploadAttachment** se zkontroluje, jaký objem již zabírají přílohy z této schránky ve stavu „dosud nepoužitá“, a pokud se překročí limit, upload se nezdaří s novou chybou č. 1286 „*Nelze vložit přílohu, nejprve použijte dříve vložené k odeslání zpráv*“. Jedná se o ochranu před zlým úmyslem nebo před chybou aplikace, která by mohla jinak bez omezení vkládat přílohy a zabírat místo na poli a datový tok, do doby, než by periodický proces začal přílohy v tomto stavu mazat.

Nahraná příloha, která nebyla využita v odeslané zprávě, je v ISDS uložena pouze po omezenou dobu, stanovenou konfiguračně měnitelným parametrem (implicitně 24 hodin). Po uplynutí této lhůty je smazána periodickým procesem.

Nahrané přílohy, použité ve zprávě, budou v ISDS existovat po stejnou dobu, po jakou existuje alespoň jedna přijatá nebo odeslaná datová zpráva, do níž patří. Bude se separátně evidovat každý výskyt velké přílohy v živé nebo trezorové DZ. Když počet výskytů klesne na 0, příloha bude smazána novým periodickým procesem.

Oprávnění:

Volající musí mít oprávnění PRIVIL_SEND_MESSAGE

Ukázka vložení přílohy v BASE64:

```
<urn:UploadAttachment>
   <urn:dmFile dmMimeType="text/plain" dmFileDescr="priloha1.txt">
         <urn:dmEncodedContent>VG8gamUg… …dGV4dC4=</urn:dmEncodedContent>
    </urn:dmFile>
 </urn:UploadAttachment>
```

Ukázka vložení přílohy pomocí odkazu na jinou část multipart požadavku (MTOM/XOP):

```
POST https://ws2.czebox.cz/DS/vodz HTTP/1.1
Connection: close
Accept-Encoding: gzip,deflate
Content-Type: multipart/related; type="application/xop+xml";
start="<rootpart@soapui.org>"; start-info="application/soap+xml"; action="";
boundary="----=_Part_3_11130068.1639402668471"
```

```
MIME-Version: 1.0
Content-Length: 308997
Host: ws2.czebox.cz
User-Agent: Apache-HttpClient/4.1.1 (java 1.5)
Authorization: --hidden--


------=_Part_3_11130068.1639402668471
Content-Type: application/xop+xml; charset=UTF-8; type="application/soap+xml";
action="UploadAttachment"
Content-Transfer-Encoding: 8bit
Content-ID: <rootpart@soapui.org>

<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope"
xmlns:v20="http://isds.czechpoint.cz/v20">
   <soap:Header/>
   <soap:Body>
      <v20:UploadAttachment>
         <v20:dmFile dmMimeType="application/pdf" dmFileDescr="3210342.pdf">
            <v20:dmEncodedContent><inc:Include href="cid:att_1"
xmlns:inc="http://www.w3.org/2004/08/xop/include"/></v20:dmEncodedContent>
         </v20:dmFile>
      </v20:UploadAttachment>
   </soap:Body>
</soap:Envelope>
------=_Part_3_11130068.1639402668471
Content-Type: application/pdf; name=3210342.pdf
Content-Transfer-Encoding: binary
Content-ID: <att_1>
Content-Disposition: attachment; name="3210342.pdf"; filename="3210342.pdf"

%PDF-1.5
… (pokračují binární data z PDF)
…
…

------=_Part_3_11130068.1639402668471
```

Ukázka vrácené odpovědi (aplikace Id přílohy a její hashe použije v konstrukci **CreateBigMessage**):

```
  <q:UploadAttachmentResponse xmlns:q="http://isds.czechpoint.cz/v20"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <q:dmAttID>54520</q:dmAttID>
    <q:dmAttHash1
AttHashAlg="SHA-256">e226488b85c22f80bc0bb91580e09292c83ba70222201ce6a1473c5a2dfc2ae3
</q:dmAttHash1>
    <dmAttHash2
AttHashAlg="SHA3-256">e226488b85c22f80bc0bb91580e09292c83ba70222201ce6a1473c5a2dfc2ae3
</q:dmAttHash1>
    <q:dmStatus>
      <q:dmStatusCode>0000</q:dmStatusCode>
      <q:dmStatusMessage>Provedeno úspěšně.</q:dmStatusMessage>
    </q:dmStatus>
  </q:UploadAttachmentResponse>
```

3.6.2 DownloadAttachment

Služba pro stažení jedné přílohy z úložiště velkých příloh do počítače.

Vstup:

- **ID zprávy** – ID přijaté či odeslané zprávy, ve které je požadovaná příloha
- **Index přílohy** – pořadové číslo přílohy, počítáno od 0.

Výstup:

- **Příloha** – požadovaná příloha jako BASE64 nebo binární forma

Popis:

Pomocí této služby si aplikace stáhne jednu přílohu VoDZ, pokud ještě existuje v úložišti. Volající schránka musí mít ke zprávě vztah (je odesílatelem či adresátem). Zpráva nesmí být smazaná.

Každá zpráva má minimálně jednu přílohu. Volající by předem měl znát počet příloh (z obálky zprávy) a volat stažení; pokud nezná, bude službu volat opakovaně s inkrementovaným indexem do doby, než dostane speciální chybu 1299 „Příloha N neexistuje“.

Služba je určena pro ty aplikace, které nepotřebují stahovat kompletní ZFO (CAdES podepsané XML). Volající si sám určuje, má-li být příloha stažena standardem MTOM/XOP

Oprávnění:

Je-li na vstupu zadáno ID zprávy, volající musí být adresát nebo odesílatel zprávy. Volající musí mít oprávnění PRIVIL_SEND_MESSAGE pro odeslanou zprávu a PRIVIL_READ nebo PRIVIL_READ_ALL pro přijatou zprávu, podle příznaku „do vlastních rukou“.

Ukázka XML požadavku (první příloha ze zprávy s ID: 1544602)**:**

```
<v20:DownloadAttachment>
   <v20:dmID>1544602</v20:dmID>
   <v20:attNum>0</v20:attNum>
</v20:DownloadAttachment>
```

Ukázka stažené PDF přílohy při použití MTOM/XOP:

```
HTTP/1.1 200
Date: Mon, 13 Dec 2021 19:05:32 GMT
Server: ISDS
Content-Type: multipart/related; start="<rootpart>"; type="application/xop+xml";
boundary="==1927659895719436937==; start-info="application/soap+xml"
Connection: close
Transfer-Encoding: chunked

--==1927659895719436937==
Content-Id: <rootpart>
Content-Type: application/xop+xml;charset=utf-8;type="application/soap+xml"
Content-Transfer-Encoding: binary

<?xml version='1.0' encoding='utf-8'?><SOAP-ENV:Envelope xmlns:SOAP-
ENV="http://www.w3.org/2003/05/soap-envelope"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><SOAP-
ENV:Body><q:DownloadAttachmentResponse xmlns:q="http://isds.czechpoint.cz/v20"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><q:dmFile
xmlns:p="http://isds.czechpoint.cz/v20" dmFileMetaType="main"
dmFileDescr="neco_smazat.pdf"
dmMimeType="application/pdf"><p:dmEncodedContent><xop:Include
xmlns:xop="http://www.w3.org/2004/08/xop/include"
href="cid:1"></xop:Include></p:dmEncodedContent></q:dmFile><q:dmStatus><q:dmStatusC
ode>0000</q:dmStatusCode><q:dmStatusMessage>Provedeno
ĂşspÄ›ĹˇnÄ›.</q:dmStatusMessage></q:dmStatus></q:DownloadAttachmentResponse></SOAP-
ENV:Body></SOAP-ENV:Envelope>

--==1927659895719436937==
Content-Id: <1>
```

```
Content-Type: application/pdf
Content-Transfer-Encoding: binary

%PDF-1.5
…(pokračují binární data z PDF)
…
…
--==1927659895719436937==
```

3.7 Příprava odeslání VoDZ - CreateBigMessage

Aplikace se musí rozhodnout, jestli vytvoří standardní zprávu (do 20 MB) nebo VoDZ (nad 20 MB). Podle toho zvolí jeden ze dvou způsobů odeslání zprávy.

Odeslání normální zprávy (do 20 MB příloh) je shodné s dnešním stavem (volá se **CreateMessage** na starém endpointu) – vložení příloh v BASE64 přímo do XML požadavku. Pokud budou v tomto případě přílohy celkově větší než 20 MB, nastane chyba a zpráva se nevytvoří.

Odeslání VoDZ pomocí nové služby **CreateBigMessage** (pouze na novém endpointu) musí předcházet upload některých (nebo všech) příloh opakovaným voláním služby **UploadAttachment**. Získaná ID příloh a jejich hashe se použijí v popisu příloh VoDZ – viz níže. Pokud bude velikost příloh menší než 20 MB (v toleranci dané konfigurovatelnou konstantou, prozatím 2 MB), dojde k chybě 1297 a zpráva se nevytvoří.

Do VoDZ lze přidat i přímo vloženou přílohu (postaru jako BASE64 text) – pro případy, kdy je vložen třeba krátký text k velkému ZIPu apod.

Není zavedena služba pro odeslání velkoobjemové multizprávy. Lze ale provést jednou upload velké přílohy a poté opakovaně ji vkládat do mnoha zpráv.

3.7.1 Popis externích příloh ve zprávě

Externí příloha musí v popisu v **CreateBigMessage** v elementu `dmExtFile` obsahovat novou sadu atributů (v ukázce níže červeně). Každá externí příloha má v popisu uvedeno ID přílohy a její dva hashe různých typů a naopak nesmí mít zadaný obsah (doplní se dříve uploadovanou přílohou (**UploadAttachment**) podle jejího ID).

Ukázka popisu velké přílohy (uložené samostatně s ID 4131) a malé přílohy (vložené přímo):

```
…
<v20:dmFiles>

    <v20:dmExtFile dmFileMetaType="main" dmAttID="4131"
   dmAttHash1="7ff16254c3d04893f6153f094f2ecd19b93fd5c41fe8d70ab0642a749d101465"
   dmAttHash1Alg="SHA-256"
   dmAttHash2="e95731dbcfbd39456e775755cea9b4128f8efc6a30f326ce26a5ac26a9f8993c"
   dmAttHash2Alg="SHA3-256"/>      <-- prázdné, naplní se odkazem na AttID

    <v20:dmFile dmFileMimeType="enclosure" dmMetaType="application/pdf"
dmFileDescr="průvodní dopis ke spisu.pdf"> <-- normální příloha

<v20:dmEncodedContent>/9j/4AAQgABAAEAYABgAAD//gAcQ3JlYXRlZCBieSBBY2N1U29mdCB...
...
A94DASEAAhEBAxEB/9sAhAABAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQIBAgIBAQEBAgIDAgIC
dS4NCg0KUyBwb3pkcmF2ZW0NCk5vdj1FMWtvdj1FMQ==</v20:dmEncodedContent> <-- BASE64
    </v20:dmFile>
</v20:dmFiles>
```

…

Jádro ISDS zadané údaje zkontroluje (ověří existenci příloh, zkontroluje hashe, AV kontrola a kontroly obsahu proběhy již při uploadu) a pokud zjistí nesoulad, zprávu neodešle. Jako přílohu lze použít i takovou, která již byla použita v jiné zprávě z této schránky (až do doby, než bude vymazána z úložiště). Možné nové chyby:

- Příloha daného ID není v úložišti (č. 1294)
- Příloha daného ID existuje, ale patří k jiné schránce (č. 1293)
- U přílohy nesouhlasí hashe (č. 1288 nebo č. 1289)

Elementy zprávy, kromě výše uvedených, jsou shodné se službou **CreateMessage** v **[1]**.

3.8 Stažení zprávy

Běžné zprávy lze stahovat na starém kontextu, VoDZ pouze na novém kontextu novými službami. Při pokusu o stažení VoDZ starou službou nebo naopak dojde k chybě č. 1281 *„Zvolená služba není určena pro tento typ zprávy“*.

Nový kontext půjde použít pouze pro VoDZ, při pokusu o stažení normální zprávy dojde k chybě. Při stažení došlé VoDZ do souboru novou webovou službou **BigMessageDownload** vznikne standardní XML struktura popisující datovou zprávu včetně XML příloh v BASE64. Jedinou změnou bude kompatibilní přidání atributů `dmVODZ` a `attsNum` (počet příloh) v případě VoDZ. Do XML dat nebudou přenášeny hashe příloh. Důvod nové a staré služby, lišící se jen atributy, je optimalizační.

Ukázka začátku XML stažené VoDZ:

```
<q:BigMessageDownloadResponse xmlns:q="http://isds.czechpoint.cz/v20"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
   <q:dmReturnedMessage dmType="E" dmVODZ="true" attsNum="1">
      <p:dmDm xmlns:p="http://isds.czechpoint.cz/v20">
         <p:dmID>1546004</p:dmID>
         <p:dbIDSender>9ky2eiu</p:dbIDSender>
         <p:dmSender>Jan Bohuslav Šimek</p:dmSender>
         <p:dmSenderAddress>Hradčany, dolní část, 12345 Malá 1, 162 00, Praha 6,
CZ</p:dmSenderAddress>
         <p:dmSenderType>40</p:dmSenderType>
         <p:dmRecipient>&lt;Společnost pro potlačení zla &amp; Son></p:dmRecipient>
…
```

Služby pro stažení podepsaných zpráv (**SignedBigMessageDownload** a **SignedSentBigMessageDownload**) vracejí XML strukturu stažené zprávy, podepsané pečetí MV ve formátu CAdES, tj. formát známý jako ZFO. Volající aplikace může pomocí headeru Accept zvolit, jestli chce binární data získat jako BASE64 součást odpovědi nebo jako binární část multipart odpovědi (MTOM/XOP) – viz kap. 3.4.

Formát souboru ZFO, staženého službou **SignedBigMessageDownload** nebo **SignedSentBigMessageDownload** je shodný s formátem ZFO pro normální zprávy, staženého starými službami **SignedMessageDownload** a **SignedSentMessageDownload** nebo z portálu ISDS**.** Je tím zachována kompatibilita pro externí čtečky ZFO dokumentů.

3.8.1 Stažení obálky

Pro stažení obálky DZ i VoDZ se použije stejná služba na starém endpointu **MessageEnvelopeDownload**, která pro VoDZ k elementu `dmReturnedMessageEnvelope` přidá atributy `dmVODZ` a `attsNum`.

Ukázka XML obálky VoDZ s jednou přílohou:

```
      <q:MessageEnvelopeDownloadResponse xmlns:q="http://isds.czechpoint.cz/v20"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
         <q:dmReturnedMessageEnvelope dmType="E" dmVODZ="true" attsNum="1">
            <p:dmDm xmlns:p="http://isds.czechpoint.cz/v20">
               <p:dmID>1544557</p:dmID>
               <p:dbIDSender>2wc9wqq</p:dbIDSender>
               <p:dmSender>Pavel Pohled</p:dmSender>
               <p:dmSenderAddress>Na strži 1201/47, 14000 Praha 4,
CZ</p:dmSenderAddress>
               <p:dmSenderType>40</p:dmSenderType>
               <p:dmRecipient>Jan Bohuslav Šimek</p:dmRecipient>
…
```

3.9 Seznamy zpráv

Služby pro získání seznamu přijatých a odeslaných zpráv (**GetLisOfReceivedMessaged** a **GetListOfSentMessages**) budou na výstupu rozšířeny o nepovinný atribut `dmVODZ` s hodnotou „true“ pro VoDZ (kompatibilní změna). Souhrnná velikost příloh (v elementu `dmAttachmentSize`) je v kB, spočítaná pro BASE64 formát. Pokud potřebujte skutečnou binární velikost příloh, vynásobte hodnotu konstantou ¾.

Tyto služby zůstanou vystaveny pouze na starém endpointu.

Ukázka seznamu s první zprávou VoDZ, druhou normální:

```
   <q:GetListOfReceivedMessagesResponse xmlns:q="http://isds.czechpoint.cz/v20"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
     <q:dmRecords>
      <q:dmRecord dmType="E" dmVODZ="true"> <-- Velkoobjemová zpráva
        <q:dmOrdinal>1</q:dmOrdinal>
        <q:dmID>1546004</q:dmID>
        <q:dbIDSender>9ky2eiu</q:dbIDSender>
        <q:dmSender>Jan Bohuslav Šimek</q:dmSender>
        <q:dmSenderAddress>Hradčany, dolní část, 12345 Malá 1, 162 00, Praha 6,
CZ</q:dmSenderAddress>
        <q:dmSenderType>40</q:dmSenderType>
        <q:dmRecipient>&lt;Společnost pro potlačení zla &amp; Son></q:dmRecipient>
        <q:dmRecipientAddress>Dlouhá 1/1, 10100 Praha 1, CZ</q:dmRecipientAddress>
        <q:dmSenderOrgUnit xsi:nil="true"/>
        <q:dmSenderOrgUnitNum xsi:nil="true"/>
        <q:dbIDRecipient>kv62bqf</q:dbIDRecipient>
        <q:dmRecipientOrgUnit xsi:nil="true"/>
        <q:dmRecipientOrgUnitNum xsi:nil="true"/>
        <q:dmToHands xsi:nil="true"/>
        <q:dmAnnotation>nová WS</q:dmAnnotation>
        <q:dmRecipientRefNumber xsi:nil="true"/>
        <q:dmSenderRefNumber xsi:nil="true"/>
        <q:dmRecipientIdent xsi:nil="true"/>
        <q:dmSenderIdent xsi:nil="true"/>
        <q:dmLegalTitleLaw xsi:nil="true"/>
        <q:dmLegalTitleYear xsi:nil="true"/>
```

```
        <q:dmLegalTitleSect xsi:nil="true"/>
        <q:dmLegalTitlePar xsi:nil="true"/>
        <q:dmLegalTitlePoint xsi:nil="true"/>
        <q:dmPersonalDelivery>false</q:dmPersonalDelivery>
        <q:dmAllowSubstDelivery>true</q:dmAllowSubstDelivery>
        <q:dmMessageStatus>6</q:dmMessageStatus>
        <q:dmAttachmentSize>71254</q:dmAttachmentSize>
        <q:dmDeliveryTime>2021-12-13T15:42:53.578+01:00</q:dmDeliveryTime>
        <q:dmAcceptanceTime>2021-12-13T15:44:17.424+01:00</q:dmAcceptanceTime>
      </q:dmRecord>
      <q:dmRecord dmType="E">   <-- běžná zpráva
        <q:dmOrdinal>2</q:dmOrdinal>
        <q:dmID>1545750</q:dmID>
        <q:dbIDSender>9ky2eiu</q:dbIDSender>
        <q:dmSender>Jan Bohuslav Šimek</q:dmSender>
        <q:dmSenderAddress>Hradčany, dolní část, 12345 Malá 1, 162 00, Praha 6,
CZ</q:dmSenderAddress>
        <q:dmSenderType>40</q:dmSenderType>
        <q:dmRecipient>&lt;Společnost pro potlačení zla &amp; Son></q:dmRecipient>
        <q:dmRecipientAddress>Dlouhá 1/1, 10100 Praha 1, CZ</q:dmRecipientAddress>
        <q:dmSenderOrgUnit xsi:nil="true"/>
…
```

Přidaný atribut do XML struktury výstupu WS by neměl způsobit nesprávné zpracování odpovědi v případě, kdy aplikace používá starší WSDL, měl by být ignorován.

3.10 Ověření zprávy

Současná služba **AuthenticateMessage** dostane na vstupu ZFO a vrátí výsledek ANO/NE, jde-li o zprávu, která v této podobě prošla ISDS. Pro VoDZ se musí použít nová varianta **AuthenticateBigMessage**.

Aplikace by měla znát kontrolovanou zprávu – pokud jde o běžnou zprávu, musí se volat stará služba. Pokud jde o VODZ, musí se volat nová služba. Pokud aplikace nezná obsah ZFO (a nechce jej rozebírat) musí rozhodnout dle velikosti ZFO, kterou službu volat. Typicky velikost nad 26.7MB indikuje, že přílohy mohou být větší než 20MB. Je-li velikost ZFO „na hranici“ lze použít starou i novou službu.

Při volání služby **AuthenticateBigMessage** (předání VoDZ k analýze) lze použít MTOM/XOP standard, aby se zmenšila velikost požadavku.

4 ZIP jako příloha zpráv

Kontejnerový formát ZIP byl povolen jako jedna z typů příloh datové zprávy. Z důvodu zabezpečení a plynulosti provozu je však na formát kladena řada omezení popsaných níže.

Platí pro běžné zprávy i VoDZ, pro veřejné i Poštovní datové zprávy. Je implementováno v klientském portálu i u webových služeb **CreateMessage**, **CreateMultipleMessage** a **CreateBigMessage**.

4.1 Vlastnosti a parametry souborů ZIP, které lze použít jako přílohu zprávy

Přípona souboru	zip

Mime typy	`application/zip`
	`application/x-compressed`
	`application/x-zip-compressed`

4.2 Omezení struktury ZIP souborů

Šifrované ZIP soubory	nejsou povolené
Splitované ZIP soubory	nejsou povolené
Vícenásobně vnořené ZIP soubory	nejsou povolené, platí i pro ASiC
Počet souborů v ZIPu	omezený konfigurovatelnou konstantou, default 1000
Počet souborů a adresářů ZIPu	omezený konfigurovatelnou konstantou, default 1000
Adresářová struktura	jsou povoleny 4 úrovně adresářů, tedy tři úrovně souborů.
Velikost rozbaleného obsahu	omezená konstantou, která je dána jako 3x velikost VoDZ (tedy 3 GB, na VT zpočátku 750 MB)

Typy souborů, vložených do ZIP kontejneru, jsou dané vyhláškou o ISDS, tedy standardní typy jako v současné verzi. Vložené soubory jsou jednotlivě kontrolovány na shodu s vyhláškou. Antivirová kontrola se provádí pro celý ZIP soubor.

4.3 SIP balíčky

Jedním z cílů správce, proč povolit formát ZIP, je existence tzv. SIP balíčků, používaných v eSSL zejména pro předávání dokumentů do archivů, ale i pro další účely.

Jedná se o ZIP (soubor s příponou ZIP) definované struktury. Popis – viz https://www.mvcr.cz/clanek/narodni-standard-pro-elektronicke-systemy-spisove-sluzby.aspx.

ISDS nebude provádět validaci SIP balíčku na úrovni XSD – k tomu autorům slouží externí nástroj Validátor SIP. ISDS nepřenese každý SIP balíček, byť validní dle validátoru – i zde platí omezení na ZIP soubory a zejména omezení na typy souborů uvnitř kontejneru (SIP balíček může obsahovat cokoliv, např. EXE nebo další ZIPy, i šifrované, zatímco ZIP v ISDS jen povolené typy příloh).

4.4 Chyby hlášené systémem při kontrole ZIP a ASiC příloh

Pokud dojde při analýze ZIP/ASiC přílohy k nesouladu s výše uvedenými vlastnostmi, vrátí se chyba 1214 a některý z následujících chybových textů:

Text u chyby 1214	**Popis**
Soubor je šifrovaný, nemůžete jej vložit jako přílohu datové zprávy.	Šifrovaný ZIP je zakázaný, nelze provést AV kontrolu. Neplatí pro DOCX, kde šifrování je povoleno.
Přílohy v ZIP formátu nesmí být rozděleny do více částí (split).	Splitovaný ZIP je zakázaný.
Použita nepodporovaná vlastnost kompresního formátu.	Systém nedokáže zpracovat ZIP soubor.
Použita nepodporovaná vlastnost kompresního formátu - chybějící délka nekomprimované položky.	Odpovídá chybě hlášené java knihovnou „only DEFLATED entries can have EXT descriptor“, která brání rozbalení ZIPu při způsobu zpracování v ISDS.

Text u chyby 1214	Popis
Uvnitř komprimované přílohy nesmí být komprimovaný soubor: (<file_name>).	Uvnitř ZIPu nesmí být jiný ZIP nebo ASiC. Neplatí prot DOCX, ZFO a jiné, založené na ZIP, ale povolené vyhláškou.
Uvnitř komprimované přílohy je soubor <file_name> nepovoleného formátu.	Uvnitř ZIPu nesmí být soubor nepovolený vyhláškou, např. EXE.
Překročen maximální počet <N1> souborů v komprimované příloze.	Překročen bezpečnostní limit.
Překročen maximální počet <N2> souborů nebo složek v komprimované příloze.	Překročen bezpečnostní limit.
Překročena maximální povolená velikost příloh po rozbalení.	Překročen bezpečnostní limit, daný jako trojnásobek povolené velikosti příloh VoDZ (na VT je zpočátku limit nastaven na cca 750 MB)
Hloubka zanoření adresářové struktury nesmí překročit <N4> úrovně.	Překročen bezpečnostní limit.
Chyba ve struktuře ASiC přílohy.	Pravděpodobně se nejedná o ASiC-S nebo ASiC-E formát.
Nespecifický problém s formátem komprimovaného souboru.	Ostatní neošetřené chyby – pokud na takovou narazíte, prosíme o zaslání souboru.

Chyba 1214 hlásí také postaru chyby komponenty na hlídání obsahu příloh (shoda přípony, mime type a obsahu).

5 ASiC jako příloha zpráv

Kontejnerové formáty ASiC-S (Simple Form) a ASiC-E (Extended Form) jsou povoleny jako typy příloh datové zprávy. Nadále v textu používáme pojem ASiC pro oba tyto formáty. Více informací o formátu - viz https://en.wikipedia.org/wiki/Associated_Signature_Containers a příslušné ETSI standardy.

ISDS ASiC formáty nově povoluje, v normálních zprávách i VoDZ, veřejných i Poštovních.

5.1 Vlastnosti a parametry souborů ASiC, které lze použít jako přílohu zprávy

Přípona souboru	`asics, scs, asice, sce`
Mime typy	`application/vnd.etsi.asic-s+zip, application/vnd.etsi.asic-e+zip`

5.2 Omezení struktury ASiC souborů

ASiC je kontejnerový formát, asociující vložené soubory s jejich digitálními podpisy; jako výchozí kontejnerový formát používá ZIP kompresi. Proto se pro ASiC soubor uplatní všechna omezení kladená na ZIP soubory, viz kap. 4.2. Navíc je prováděna formální kontrola struktury ASiC kontejneru. Nejsou však kontrolovány vazby, hashe, podpisy, definované výše uvedenými ETSI normami, tato úloha nepřísluší do ISDS, ale až aplikaci příjemce.

V současné době nám není známa podoba ASiC souborů, které budou zavedeny v české veřejné správě.

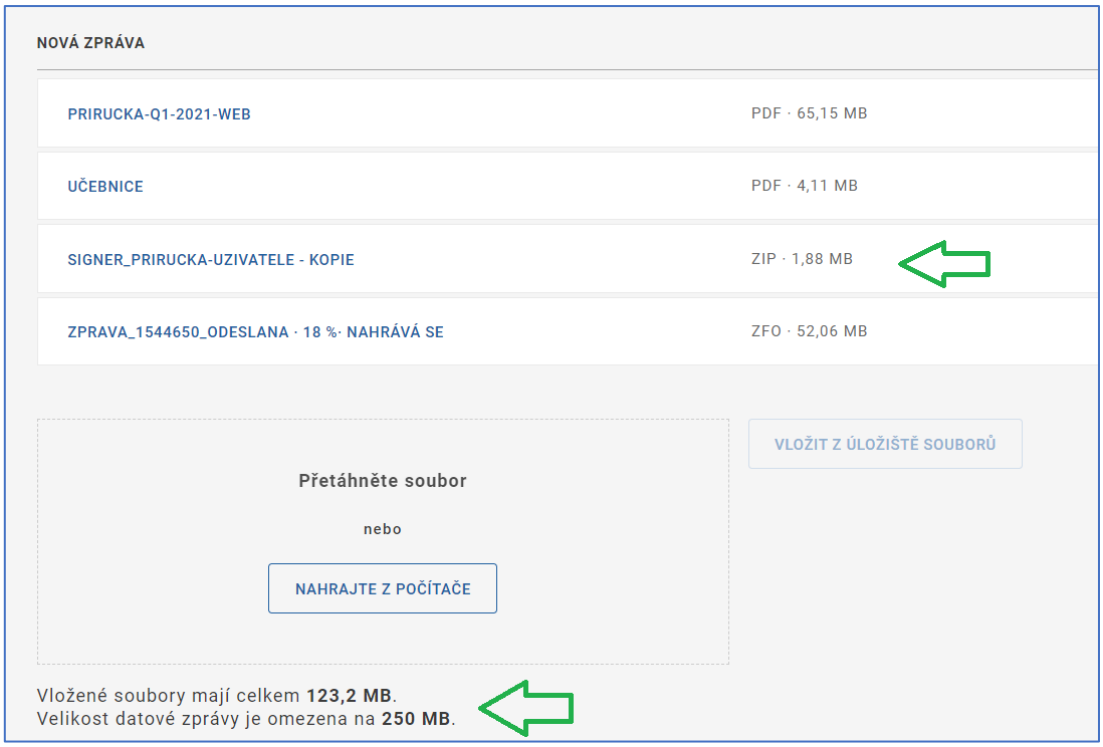
6 Omezení počtu příloh

Se zavedení VoDZ a ZIP formátu dojde k omezení počtu příloh, které lze přiložit do jedné datové zprávy, normální i VoDZ. Z dnešních 900 pro webovou službu a 300 pro portál bude počet snížen na **100**. Zprávy obsahující stovky příloh dělají příjemcům potíže.

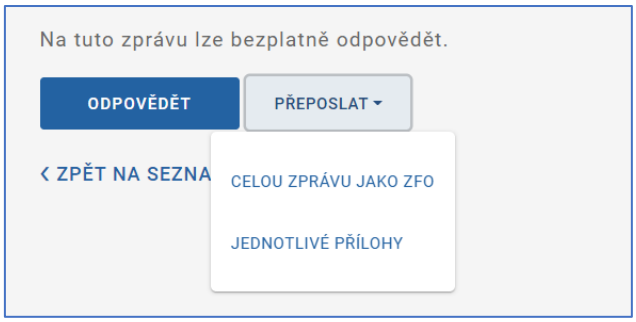
7 Změny v klientském portálu

Změny v portálu nejsou velké.

- Je povoleno vkládat přílohy až do daného limitu (v prostředí veřejného testu zpočátku 250 MB).
- Je povoleno vkládat ZIP a ASIC soubory.



- Při přeposlání zprávy se nově vybírá, jestli přeposlat kompletní podepsanou zprávu (ZFO) nebo jen soubory ze zprávy. Druhá varianta slouží k zaslání velkou přílohu více adresátům při jednom uploadu.



- Všechny ostatní funkce portálu (seznamy, detail zprávy, stahování do ZFO, ověřování ZFO atd.) fungují pro VoDZ stejně jako pro běžnou zprávu.