

Informace pro vývojáře aplikací – březen 2024

Datum: 19.03.2024

Verze: 1.1

Klasifikace: veřejný dokument

1 Anotace změn

Reálné používání Velkoobjemových zpráv (VoDZ) v produkčním prostředí ISDS od ledna 2024 ukázalo některé menší problémy, zejména při vkládání příloh pro VoDZ. Zde popsané změny na ně reagují.

1. Zvětšení limitu celkové velikosti uploadovaných a nepoužitých příloh VoDZ (služba **UploadAttachment**).
2. Rychlejší mazání nepoužitých příloh (sirotků) VoDZ.
3. Přidání povinnosti obsahu atributu `dmMimeType` u služby **UploadAttachment**.
4. Zpřesnění popisu vlastností atributu `dmUpFileGuid` v `dmBaseType.xsd`.
5. Ukončení podpory šifrovací sady **TLS DHE_RSA_WITH_AES_128_GCM_SHA256**.

Změna v bodu 4 je uplatněna ve verzi **3.05** WSDL/XSD.

2 Harmonogram změn

Pro bod 1:

Ve všech prostředích od 21.3.2024

Pro body 2 až 4:

Na Veřejném testu ISDS od 21.3.2024, na Produkci cca od května.

Pro bod 5:

Na Produkčním prostředí od 21.3.2024 (na Veřejném testu již vypnuto od listopadu 2023)

3 Popis změn

3.1 Limit velikosti nepoužitých uploadovaných příloh (sirotků)

Vkládání příloh pro VoDZ pomocí služby **UploadAttachments** bez odesílání zpráv s těmito přílohami je limitováno celkovou velikostí příloh. Jde o bezpečnostní opatření, aby omylem či zlým úmyslem nevznikl problém s volným místem v tomto úložišti. V současné verzi jde o 1 GB. Limit je nově zvětšen na 5 GB.

Změna nemá žádný dopad na aplikace.

3.2 Rychlejší mazání nepoužitých uploadovaných příloh (siroteků)

Pokud se vloží příloha VoDZ pomocí služby **UploadAttachments** a neodešle v nějaké zprávě, vzniká „sirotek“, zabírající místo. Tyto sirotky maže periodický proces po 24 hodinách (a tím uvolňuje místo pro další přílohy – viz bod 3.1).

Na přání vývojářů byla tato akce zrychlena na 2 hodiny (tedy je nutno odeslat VoDZ s uploadovanou přílohou do 2 hodin, jinak se příloha smaže a zpráva neodejde).

Drtivá většina spisovek, která tuto funkcionalitu používá, se dle našich zkušeností chová tak, že nahrané přílohy připojí ke zprávám s velmi krátkým časovým odstupem poté, co získá jejich identifikátory – pro ně jsou dvě hodiny dostatečná doba. Současně máme za to, že zkrácení na 2 hodiny (spolu se zvětšením limitu) bude dostatečnou prevencí toho, aby si daná spisovka příliš brzy nevyčerpala prostor pro předem nahrané přílohy budoucích zpráv a pokud ho i tak spotřebuje, nepředstavují 2 hodiny zase tolik, aby si nemohla počkat na jejich výmaz a tím uvolnění prostoru pro další práci.

Protože změna může mít teoreticky dopad na aplikace, bude změna nasazena nejprve v testovacím prostředí ISDS a teprve později na produkčním.

3.3 Atribut `dmMimeType`

U webové služby **UploadAttachment** pro vložení jedné přílohy Velkoobjemové zprávy je definován povinný atribut `dmMimeType` u elementu `dmFile`. Pro některé typy příloh procházela prázdná hodnota, která však při použití této přílohy vyvolala chybu při odeslání v **CreateBigMessage**.

Od této verze je povinný nejen atribut, ale i neprázdný obsah (samozřejmě odpovídající typu přílohy). Změna nevyžaduje úpravu XSD a odpovídajících vygenerovaných tříd. Volání služby bez uvedeného mime-typu skončí chybou 2035.

Dopad na aplikace je minimální, naprostá většina aplikací prázdný atribut nepoužívá (u ZIP např. je to vynucováno již nyní). Jedná se však o nekompatibilní změnu rozhraní, proto je nasazena nejprve na testovací prostředí a teprve později na produkční.

3.4 Atribut `dmUpFileGuid`

U nepovinného atributu `dmUpFileGuid` elementů `dmFile` (od roku 2009) a `dmExtFile` (od roku 2024) u služeb **CreateMessage** a **CreateBigMessage**, používaný výjimečně pro aplikační vazby příloh jedné zprávy, chyběla definice vlastnosti `use="optional"`. Z hlediska definice XSD bezvýznamné opomenutí mělo důsledek v sestavování ZFO u určitým způsobem definovaných Velkoobjemových zpráv – ZFO zpráva nešla validovat.

Chyba samotná byla opravena již na začátku ledna 2024, oprava definice (byť nyní již nepodstatná) byla doplněna do `dmBaseType.xsd` verze 3.05. Protože změna XSD bude znamenat přegenerování nových tříd v aplikacích, bude nové XSD umístěno nejprve na testovací prostředí a teprve později na produkční. Změna by neměla mít žádný vliv na aplikace.

3.5 Ukončení TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

Je ukončena podpora dosloužilé (v souladu s doporučením NUKIB) šifrovací sady TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 v produkčním prostředí ISDS. Klienti, jejichž aplikace používají tuto zastaralou šifrovací sadu, byli notifikováni datovou zprávou Správce systému ISDS. Prostředí Veřejného testu ISDS (czebox.cz) tuto sadu již nepodporuje od listopadu minulého roku a vývojáři byli již tehdy upozorněni.

Více: <https://info.mojedatovaschranka.cz/info/cs/79.html>