Informace pro vývojáře aplikací – prosinec 2024

Datum: 03.12.2024
Verze: 1.1
Klasifikace: veřejný dokument

1 Anotace změn

1. Nová služba **SentMessageEnvelopeDownload** pro získání obálky odeslané zprávy.
2. Služba **GetDataBoxList** s parametrem ALL2 povolena i pro HSS.
3. Povolení mp3 příloh s MPEG 2.5.
4. Omezení počtu příloh na 100, z toho 10 kontejnerových (ZIP/ASiC).
5. Nový algoritmus podpisu v pečeti stažených zpráv **RSA-PSS**.
6. Ukončení používání šifrovací sady **DHE-RSA-AES256-GCM-SHA384** z TLS.
7. Výměna doménového certifikátu za variantu s 4096 bity klíče.
8. Výměna klíče v pečeti za variantu s 4096 bity klíče.
9. Informace k používání endpointů **ws1** a **ws2**.

2 Harmonogram změn

Pro bod 1 až 3:

Na všech prostředích od 5.12.2024.

Pro bod 4 a 5:

Na Veřejném testu ISDS již bylo nasazeno dříve, na Produkci 5.12.2024.

Pro bod 6:

Na Veřejném testu ISDS od června 2024, na Produkci znovu **odloženo do konce ledna 2025**.

Pro bod 7 a 8:

Na Veřejném testu ISDS od 5.12.2024, předpoklad pro Produkci: během roku 2025, až vyprší stávající certifikáty.

3 Popis změn

3.1 Služba SentMessageEnvelopeDownload

Služba vrací obálku odeslané zprávy odeslané ze své schránky, obdoba existující služby **MessageEnvelopeDownload**. Služba nebyla dosud zavedena, protože se předpokládalo, že odesílatel zná své zprávy. Pro některé případy užití složitějších aplikací je však vyžadována.

Oprávnění: Nutné schránkové oprávnění PRIVIL_VIEW_INFO nebo PRIVIL_CREATE_DM.

Podrobnosti v příručce *WS_manipulace_s_datovymi_zptavami.pdf*. Odpovídající verze dokumentace je **3.4** a odpovídající verze WSDL je **3.07**.

3.2 Služba GetDataBoxList s parametrem ALL2

Služba **GetDataBoxList** s parametrem ALL2 (tj. získat seznam všech schránek) mohla volat jen OVM aplikace, která se přihlašuje spisovkovým certifikátem (do vlastní schránky). Nově tak může činit i aplikace typu HSS (Hostovaná spisová služba), přihlašující se do různých schránek svých klientů.

3.3 MP3 přílohy

Správce povolil volnější výklad vyhlášky č. 194/2009 Sb., která definuje formáty příloh, povolené v datových zprávách. Pro mp3 audio přílohy je nově povolen formát i MPEG 2.5.

Neoficiální standard MPEG 2.5 je z roku 2000 (aktualizace 2008), nebyl standardizován (organizací MPEG ani ISO/IEC). Standard 2.5 definuje nižší vzorkovací frekvence než původní standard, a proto se například používá k záznamu telefonních hovorů (které proto mohou být nově posílány datovou schránkou).

3.4 Navýšení počtu příloh ve zprávě

Byl navýšen povolený počet příloh v datové zprávě z 50 na 100. Z toho může být maximálně 10 příloh kontejnerových (ZIP nebo ASiC). Platí pro WS i klientský portál. Protože omezení kontejnerových příloh může mít dopad na spisové aplikace, bylo nasazení rozfázováno.

3.5 Nový algoritmus pečeti

Stažené zprávy a doručenky ve formátu ZFO (podepsané XML - CAdES) jsou pečetěny pečetí správce s novým algoritmem – místo dosavadního RSA se začne používat **RSA-PSS** (RSA Probabilistic Signature Scheme). Je to v reakci na Doporučení v oblasti kryptografické bezpečnosti, platné od 1.7.2023, vydané NUKIBem.

Varování: některé starší a neaktualizované tooly a nástroje s tímto algoritmem neumějí pracovat. Zkontrolujte si, že Vaše aplikace toto umí. Pokud používáte k zobrazení stažené zprávy či doručenky aplikace Software602 FormFiller, stáhněte se poslední verzi. OpenSSL či referenční DSS to zvládnou bez problémů.

V prostředí veřejného testu ISDS bylo nasazeno od června 2024.

3.6 Odstranění šifrovací sady DHE-RSA-AES256-GCM-SHA384

V souladu s doporučovanými bezpečnostními postupy bylo rozhodnuto o úpravě konfigurace webového serveru, která odstraní zastaralou TLS šifrovací sadu používající šifrovací metodu Diffie-Hellman (DH) AES256 v GCM módu. Jde o pokračování řetězce úprav bezpečnostní konfigurace, které mohou mít dopad na některé staré nebo chybně nakonfigurované aplikace a spisové služby. Proto se každá změna nasazuje nejprve na Veřejný test a teprve při některé z dalších aktualizací, pokud nevzniknou zásadní komplikace, na produkční prostředí ISDS.

V rámci těchto úprav dojde k odstranění dosluhující šifrovací sady používající výměnu klíčů DH, kterou NÚKIB ve svém Doporučení v oblasti kryptografické bezpečnosti, označuje jako dosluhující s doporučením přestat s jejím používáním **do konce roku 2023**.

Šifrovací sada již byla odstraněna nejprve na prostředí Veřejného testu a časem bude odstraněna i z Produkce. Předběžně stanovený termín je konec ledna 2025.

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.

Upozornění: **stále existují aplikace, které přistupují do ISDS s využitím této šifrovací sady. Po konci ledna 2025 přestanou tyto aplikace fungovat (nepřipojí se do ISDS přes WS)!** Do schránek, z nichž probíhá tato komunikace, byla správcem v říjnu zaslána datová zpráva s varováním. Může jít též o nové aplikace provozované na starém OS nebo se starou Javou apod.

3.7 Delší doménový klíč

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 (GeoTrust) – z délky 2048 bitů se přechází na klíč s délkou 4096 bitů. V prostředí Veřejného testu ISDS je nový certifikát (GeoTrust) již nasazen, na Produkci bude nasazen před expirací stávajícího, v roce 2025.

3.8 Delší klíč pro pečetění

V reakci na Doporučení v oblasti kryptografické bezpečnosti, platné od 1.7.2023, vydané NUKIBem, se postupně na všech prostředích mění klíč pečetícího certifikátu – z délky 2048 bitů se přechází na klíč s délkou 4096 bitů. V prostředí Veřejného testu ISDS je nový certifikát již nasazen, na Produkci bude nasazen před expirací stávajícího, na jaře 2025. Pokud aplikace rozebírá zapečetěnou zprávu (formát ZFO – CAdES), měla by si zkontrolovat, že používané nástroje nepoznají žádnou změnu.

3.9 Upozornění k používání endpointu ws2 pro VoDZ

Se zavedením Velkoobjemových zpráv (VoDZ) a webových služeb pro jejich správu se začal využívat speciální endpoint ws2 (např. `ws2.mojedatovaschranka.cz/DS/vodz`). Tento endpoint není zablokován pro volání služeb pro běžné (malé) zprávy (opačně to možné není). Nyní jsme si všimli, že některé aplikace to takto používají, např. stahují malé i velké zprávy společně na endpointu ws2 (resp. ws2c). Chceme varovat, že toto zjednodušení programování se může vymstít – provoz na endpointu

ws2 je regulován podle zatížení – při velkém počtu nebo objemu manipulací s VoDZ může být omezován tak, aby provoz na standardním endpointu ws1 nebyl zásadně dotčen.

Zatím je stále objem VoDZ malý a k omezování nedochází, ale to se může v budoucnu změnit.