Informace pro vývojáře aplikací – červen 2024

Datum: 07.06.2024
Verze: 1.1
Klasifikace: veřejný dokument

1 Anotace změn

1. Doplněný popis některých chyb.
2. Nová služba pro odregistraci klienta HSSU (Přístupového rozhraní).
3. Zavedení kreditní události č. 7. – obnovení zpráv z trezorového koše, dopad do WS **DataBoxCreditInfo**.
4. Oprava WSDL pro (zastaralou) službu **DummyOperation**.
5. Odstranění šifrovací sady **DHE-RSA-AES256-GCM-SHA384** z TLS.
6. Nový algoritmus podpisu v pečeti stažených zpráv **RSA-PSS**.

2 Harmonogram změn

Pro bod 1 a 2:

Na všech prostředích od 13.6.2024

Pro body 3 až 6:

Na Veřejném testu ISDS od 13.6.2024, na Produkci nejdříve od září.

3 Popis změn

3.1 Popis chyb

V číselníku chyb (i v dokumentaci) chyběl popis a vysvětlení chyby č. 1295 – „Velikost přílohy v těle datové zprávy přesahuje povolenou délku.“. Ta nastane, pokud příloha vložená v BASE64 do elementu `dmEncodedContent` v **CreateBigMessage** je větší než 20 MB.

Pokud se posílá více příloh v jedné zprávě a některá příloha neprojde kontrolou na shodu formátu s příponou a mime-typem, vrací se chyba 1214. K textovému popisu této chyby (kterých může být mnoho různých) byl přidán za dvojtečku název přílohy (tzn. první přílohy, která není validní).

Příklad:

```
<p:CreateMessageResponse xmlns:p="http://isds.czechpoint.cz/v20"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <p:dmStatus>
     <p:dmStatusCode>1214</p:dmStatusCode>
```

```
     <p:dmStatusMessage>Obsah souboru nebyl identifikován.:
testovací.docx</p:dmStatusMessage>
  </p:dmStatus>
</p:CreateMessageResponse>
```

3.2 Služba RevokeConfirmation

Klient (tj. uživatel datové schránky) Přístupového rozhraní, alias HSSU (v současné době jej používá pouze jediná aplikace – Portál občana) musí souhlasit s tím, aby externí aplikace přistupovala do jeho schránky. Tím vznikne speciální záznam v ISDS. Klient může sám přístup ukončit v klientském portálu, ale pokud externí aplikace ukončí provoz (nebo ze své strany ukončí službu pro klienta), tak registrace k této službě zůstávají. Byla proto přidána služba **RevokeConfirmation** z `GetCredential.wsdl`, kterou externí aplikace ukončí vazbu na klienta a ztratí přístup pod jeho účtem do ISDS. Tuto službu by měla volat externí aplikace, pokud již nadále nebude provozovat službu pro daného klienta.

3.3 Nová kreditní událost

V ISDS se zavádí nová kreditní událost, označená typem 7. Jedná se o obnovení datových zpráv omylem smazaných z Datového trezoru, dosud uložených v trezorovém koši, provedené v Klientském portálu. Obnovení z koše je placená službu, hrazená výhradně z kreditu u schránky.

Událost č. 7 se nově objeví ve výpisech událostí v KP, i ve výstupu z WS **DataBoxCreditInfo**, spolu s údajem, kdo akci inicioval. Je proto upraven soubor *dbTypes.xsd*.

3.4 DummyOperation

V souboru `dm_operations.wsdl` je definována historická služba **DummyOperation**, která byla důležitá pro ISDS v letech 2009 – 2010. Po změně způsobu přihlašování aplikací v roce 2010 již nemá valný význam, kromě zkoušení komunikace.

U této služby ve WSDL (už několik let) omylem chyběl popis odpovědi, takže některé nástroje hlásily při zpracování chybu. Proto byl popis pro `DummyOperationResponse` dodatečně nyní přidán.

3.5 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 (https://www.nukib.cz/download/uredni_deska/Minimalni%20pozadavky%20na%20kryptograficke%20algoritmy.pdf) označuje jako dosluhující s doporučením přestat s jejím používáním do konce roku 2023.

Šifrovací sada bude odstraněna nejprve na prostředí Veřejného testu a později i z Produkce, pokud se nevyskytnou zásadní problémy při testování aplikací.

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.

3.6 Nový algoritmus pečeti

Stažené zprávy a doručenky ve formátu ZFO (podepsané XML - CAdES) budou na VT 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.

Na PROD bude nasazeno nejdříve v září.

3.7 Dokumentace a WSDL

Změny nasazované v červnu 2024 na PROD jsou uplatněny ve verzi **3.05** WSDL/XSD a popsány ve vývojářské dokumentaci verze **3.2**.

Změny nasazované v červnu 2024 na VT jsou uplatněny ve verzi **3.06** WSDL/XSD a popsány ve vývojářské dokumentaci verze **3.3**.

HSSU služby mají samostatnou dokumentaci.