# Informace pro vývojáře aplikací – říjen 2024

Datum: 03.10.2024
Verze: 1.2
Klasifikace: veřejný dokument

## 1 Anotace změn

1. Nová webová služba **GetDataBoxAdress** pro získání kompletní adresy schránky.
2. Změna v počtu povolených příloh datové zprávy.
3. Umožnění posílat VoDZ z Odesílací brány.
4. Zavedení kreditní události č. 7. – obnovení zpráv z trezorového koše, dopad do WS **DataBoxCreditInfo**.
5. Nový algoritmus podpisu v pečeti stažených zpráv **RSA-PSS**.
6. Delší klíč pro pečetění výstupů.
7. Odstranění šifrovací sady **DHE-RSA-AES256-GCM-SHA384** z TLS.

## 2 Harmonogram změn

Pro bod 1, 3 a 4:

Na všech prostředích od 3.10.2024. Některé ze změn byly již dříve nasazeny na Veřejný test.

Pro bod 2:

Na Veřejném testu ISDS od 3.10.2024, na Produkci v příští aktualizaci (předpoklad do konce roku 2024).

Pro bod 5:

Na Veřejném testu ISDS od června 2024, 3.10.2024 nová opravená verze, na Produkci v příští aktualizaci (předpoklad do konce roku 2024).

Pro bod 6:

Na Veřejném testu ISDS od června 2024, na Produkci nejdříve začátkem roku 2025.

Pro bod 7:

Na Veřejném testu ISDS byla šifra odstraněna v červnu 2024, na Produkci bude odstraněna pravděpodobně 5.12.2024.

# 3 Popis změn

## 3.1 Služba GetDataBoxAddress

Služba vrací pro zadanou nesmazanou schránku adresní elementy včetně čísla evidenčního a adresu složenou v jednořádkové podobě (elementy na vhodných místech odděleny čárkou – dle vyhlášky vyhlášce RUIAN (č. 359/2011 Sb.)) a v podobě rozlámané do více řádků pro použití jako adresa na dopis. Konce řádků jsou označeny znakem tilda „~“ (ASCII 126 (U+007E)).

Příklad odpovědi:

```
<p:GetDataBoxAddressResponse xmlns:p="http://isds.czechpoint.cz/v20"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <p:adCode>22251057</p:adCode>
    <p:adCity>Praha 6</p:adCity>
    <p:adDistrict>Řepy</p:adDistrict>
    <p:adStreet>Bazovského</p:adStreet>
    <p:adNumberInStreet>7</p:adNumberInStreet>
    <p:adNumberInMunicipality>1117</p:adNumberInMunicipality>
    <p:adZipCode>16300</p:adZipCode>
    <p:adState>CZ</p:adState>
    <p:adRegistrationNumber xsi:nil="true"/>
    <p:adFullAddress1>Bazovského 1117/7, Řepy, 16300 Praha 6</p:adFullAddress1>
    <p:adFullAddress2>Bazovského 1117/7~Řepy~16300 Praha 6</p:adFullAddress2>
    <p:dbStatus>
       <p:dbStatusCode>0000</p:dbStatusCode>
       <p:dbStatusMessage>Provedeno úspěšně.</p:dbStatusMessage>
    </p:dbStatus>
</p:GetDataBoxAddressResponse>
```

Podrobnosti v příručce *WS_vyhledavani_datovych_schranek.pdf*. Odpovídající verze dokumentace je **3.3** a odpovídající verze WSDL je **3.06**.

## 3.2 Počet 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, je nasazení rozfázováno: nyní na Veřejný test a v příští aktualizaci na Produkci.

## 3.3 VoDZ v Odesílací bráně

Odesílací brána (komponenta ISDS umožňující odesílání zpráv z externí aplikace pod svým účtem po přihlášení) může nově posílat též Velkoobjemové zprávy (VoDZ), s velikostí příloh až 100 MB. Současné aplikace musí posílání VoDZ doprogramovat.

Odesílací brána má samostatnou příručku *OdesilaciBrana_ISDS.pdf*, jako součást provozního řádu ISDS, a tako vlastní WSDL definice.

## 3.4 Nová kreditní událost

V ISDS byla zavedena 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 služba, 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.

Podrobnosti v příručce *WS_vyhledavani_datovych_schranek.pdf*. Odpovídající verze dokumentace je **3.3** a odpovídající verze WSDL je **3.06**. V prostředí veřejného testu ISDS bylo nasazeno od června 2024.

## 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 Delší klíč pro pečetění

V reakci na Doporučení v oblasti kryptografické bezpečnosti, platné od délky 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.

## 3.7 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 5.12 2024.

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 5.12.2024 přestanou tyto aplikace fungovat (nepřipojí se do ISDS přes WS)!** Do schránek, z nichž probíhá tato komunikace, bude správcem ještě zaslána datová zpráva s varováním.