1 Změny v prostředí Veřejného testu ISDS

V odstávce Veřejného testu ISDS ve dnech 22.2. až 23.2.2018 dojde ke dvěma významným změnám, které mohou mít dopad na spisové aplikace komunikující s ISDS pomocí rozhraní webových služeb.

1.1 Vypnutí TLS 1.0 a TLS 1.1

Správce Informačního systému datových schránek vypne v roce 2018, v souladu se závěry bezpečnostního auditu systému, starší a již bezpečnostně nevyhovující komunikační protokoly TLS 1.0 a TLS 1.1. Ke stejnému kroku postupně přikročí i ostatní IS veřejné správy, pokud tak již dokonce neučinily.

Po tomto vypnutí bude možné používat pouze protokol TLS 1.2. Protokol je již implementován ve všech aktuálních OS a prohlížečích. Proto nepředpokládáme problémy uživatelů přistupujících z podporovaných prohlížečů na portály ISDS (pokud uživatelé z nějakého důvodu nezměnili předdefinované nastavení výrobců prohlížečů a/nebo OS). Domníváme se však, že některé aplikace spisových služeb se na tuto změnu budou muset připravit.

Kromě vypnutí protokolů budou zakázány i bezpečnostně již nevyhovující šifrovací sady:

- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA

Nadále půjde používat šifrovací sady:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA

1.1.1 Dopad na uživatele klientského Portálu ISDS

Uživatelé ISDS, kteří přistupují do své schránky pomocí podporovaných internetových prohlížečů, změnu nezaznamenají.

1.1.2 Dopad na externí aplikace

Pokud aplikace používají k připojování k systému ISDS aktuální a výrobci podporované programovací balíky, nezaznamenají pravděpodobně žádný problém. Do ISDS však stále přichází značné množství požadavků, které budou po uvedených změnách odmítány. Proto je rozumné svoji aplikaci

zkontrolovat a vyzkoušet v prostředí Veřejného testu ISDS do doby, než budou změny zapnuty i na produkčním prostředí.

Podpora aplikační architektury pro TLS 1.2:

- Java: doporučujeme používat Java verze 8. Lze používat verzi Java 7, ale aplikace musí protokol TLS 1.2 explicitně povolit
- Prostředí .NET: používejte .NET verze 4.6 nebo novější. Lze používat verzi .NET 4.5, ale aplikace musí protokol TLS 1.2 explicitně povolit. Podpora prostředí .NET závisí na podpoře protokolu TLS 1.2 systémem Windows (od Windows Server 2008 R2 nebo Windows 8)
- Aplikace používající OpenSSL: používejte OpenSSL 1.0.1 nebo novější

1.1.3 Harmonogram nasazování změny

Prostředí Veřejného testu ISDS: **23.2.2018**

Produkční prostředí ISDS: termín bude sdělen později, **předpoklad léto 2018**.

1.2 Změna IP adres

IP adresy přístupových bodů ISDS se v odstávce změní podle následující tabulky:

hostname	IPv4	IPv6
ws1.czebox.cz	90.182.206.214	2a00:1028:d:122:1:0:3:16
ws1c.czebox.cz	90.182.206.215	2a00:1028:d:122:1:0:4:16
cert.czebox.cz	90.182.206.213	2a00:1028:d:122:1:0:2:16
www.czebox.cz	90.182.206.212	2a00:1028:d:122:1:0:1:16

Pokud aplikace používá k přístupu přímo IP adresy, musí je ve své konfiguraci změnit. Na původních adresách se bude dočasně vracet HTTP chyba 503.