Informace pro vývojáře aplikací – únor/březen 2021

Datum: 11.2.2021
Verze: 1.2
Klasifikace: veřejný dokument

1 Anotace změn

1. V souladu s všeobecně doporučovanými postupy zavádí ISDS další bezpečnostní úpravy konfigurace webového serveru. Toto opatření může mít dopad na některé zastaralé, neaktualizované aplikace, které se připojují k ISDS.
2. Ukončuje se používání služby **GetDataBoxUsers**.
3. Zavádějí se dva nové typy profesních schránek PFO: **PFO_ZNALEC** (35) a **PFO_TLUMOCNIK** (36).

2 Harmonogram změny

V prostředí veřejného testu ISDS bude změna nasazena **11.2.2021**. Na produkčním ISDS se změny objeví:

- bod 1.: při odstávce ISDS, zřejmě v druhé polovině roku 2021
- bod 2.: při odstávce ISDS, pravděpodobně v červnu 2021
- bod 3.: podpora pro nové typy schránek bude od odstávky v březnu 2021, nicméně první takové schránky budou zřízeny nejdříve v květnu 2021 (ale ještě před odstávkou v červnu 2021).

3 Popis změn

3.1 Vypnutí starých šifrovacích sad

V souladu s doporučovanými bezpečnostními postupy bylo rozhodnuto o úpravě konfigurace webového serveru, která odstraní zastaralé šifrovací sady používající šifrovací metodu AES v CBC 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 odstávek, pokud nevzniknou zásadní komplikace, na produkční prostředí ISDS.

V rámci těchto úprav dojde k odstranění dosluhujících, již prakticky nepoužívaných, šifrovacích sad používajících AES v módu CBC, který NÚKIB ve svém doporučení (https://www.nukib.cz/download/uredni_deska/Kryptograficke_prostredky_doporuceni_v1.0.pdf) na konci roku 2018 označil jako potenciálně problematický. Tyto šifrovací sady se již prakticky

nepoužívají, neboť jsou v novějších aplikacích nahrazeny aktuálními šifrovacími sadami protokolu TLSv1.2.

Na všech rozhraních bude (postupně) vypnuta podpora těchto šifrovací sad:

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA256 (0xc028)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67)

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.

3.2 Ukončení GetDataBoxUsers

V květnu roku 2018 bylo oznámeno budoucí ukončení webové služby **GetDataBoxUsers**. Nahrazena byla službou **GetDataBoxUsers2** a čekalo se, až významní klienti služeb ISDS si upraví své aplikace. Původně se předpokládalo vypnutí do konce roku 2018, z různých důvodů však rozhodnutí o ukončení této služby bylo odkládáno.

Byť byli vývojáři již na tuto změnu v roce 2018 upozorněni, stále dochází k volání této služby. Proto bude dán ještě poslední termín na úpravy aplikací – do červnové odstávky ISDS. V prostředí Veřejného testu ISDS však bude služba vypnuta již nyní. Místo odpovědi se vrátí chyba *1301 - Služba byla ukončena, přejděte prosím na novější verzi WSDL*.

Vývojářská dokumentace ani WSDL definice (součást Provozní řádu ISDS) již starou službu **GetDataBoxUsers** neuvádějí více než dva roky.

3.3 Nové typy schránek

Novela zákona o ISDS zavádí dva nové typy profesních schránek podnikající fyzické osoby:

- schránky pro soudní znalce: **PFO_ZNALEC**, kód 35.
- schránky pro soudní tlumočníky nebo překladatele **PFO_TLUMOCNIK**, kód 36.

První schránky tohoto typu se v ISDS objeví po hromadném zřízení zřejmě v květnu 2021. Do té doby je třeba upravit aplikace, aby s těmito typy schránek pracovaly.

Tyto schránky nemají žádná specifika – všechny obsahují IČO, jsou synchronizovány s daty z Registru osob.

Pro testovací účely byly v prostředí Veřejného testu ISDS zřízeny tyto schránky nových typů:

Typ DS: **PFO_ZNALEC**
DS ID: **ss6hzz9**
Název DS: **Cyril Znalec – soudní znalec**

a

Typ DS: **PFO_TLUMOCNIK**
DS ID: **3kfhzz4**
Název DS: **Metoděj Tlumočník – soudní překladatel**