Informace pro vývojáře aplikací – prosinec 2021

Datum: 10.12.2021
Verze: 1.4
Klasifikace: veřejný dokument

1 Anotace změn

1. Je zavedeno doručování Poštovních datových zpráv (PDZ) fikcí. Tedy pokud není PDZ doručena přihlášením (uživatele s právem číst) je po 10 dnech doručena náhradně (fikcí). Je tím sjednoceno technické doručování veřejných a Poštovních zpráv.
2. Všechny schránky typu PO nebo PFO budou mít povinně povolený příjem PDZ (bez možnosti jej zakázat). Spolu s bodem 1 to znamená, že se nemohou vyhnout přijímání PDZ.
3. Jako důsledek bodu 2 je redukován vstup ze služby **GetDataBoxList** s parametrem „POA“ = seznam schránek s povoleným příjmem PDS. Nemá význam vracet všechny schránky typu PO a PFO.

Změny se týkají jen těch aplikací, které obsluhují schránky neOVM subjektů – pro OVM schránky se nic nemění (nepoužívají PDZ). Změny jsou reakcí na novelu zákona č. 300/2008 Sb.

Důsledkem budou změny spíše organizační a procesní u subjektů, které začnou být povinně příjemcem PDZ a dosud to odmítaly. Pro odesílatele PDZ se prakticky nic nemění.

4. **Opakované upozornění:** V souladu s všeobecně doporučovanými postupy zavede ISDS další bezpečnostní úpravy konfigurace webového serveru – vypnutí nedoporučených šifrovacích sad pro TLS. Toto opatření může mít dopad na některé zastaralé, neaktualizované aplikace, které se připojují k ISDS.

2 Harmonogram změny

V prostředí veřejného testu ISDS se změny objeví po odstávce 12.12.2021. Na produkčním ISDS se změny projeví až po 1.1.2022. U stávajících schránek bude příjem PDZ hromadně zapnut v zatím neupřesněné odstávce v lednu nebo únoru 2022.

Vypnutí zastaralých šifer dle bodu 4: na veřejném testu ISDS je již nastaveno od jara 2021, na produkčním prostředí zatím není rozhodnuto, nejpozději však 1.1.2023.

3 Popis změn

3.1 Doručování PDZ fikcí

Od 1.1.2022 platí zákonná úprava doručování: PDZ budou doručovány shodně s veřejnými zprávami fikcí, tedy po 10 dnech od dodání. Neplatí pro PDZ dodané (10 dní) před 31.12.2021 23:59.999, byť by datum doručení spadalo již do roku 2022.

Odesílatel PDZ nemůže zprávu označit příznakem Nedoručovat fikcí, tato funkčnost je povolena jen pro schránky OVM.

Současně se mění texty událostí související s doručování v doručence, texty se liší pro PDZ a veřejné DZ.

3.2 Povinný příjem DZ

U schránek PO a PFO, včetně podtypů, bude příjem PDZ povinný. U schránek typu FO bude jednorázově zapnut, nicméně držitelé či administrátoři si příjem mohou vypnout přímo v klientském portálu nebo na kontaktním místě Czech POINT.

Pro nově vznikající schránky platí již od 1.1.2022. Pro stávající schránky bude změna provedena v termínu dle novely, max. do 1.3.2022 (prakticky v únorové odstávce – bude správcem oznámeno). V tomto krátkém přechodném období je třeba počítat s tím, že PO či PFO schránka má příjem ještě zakázaný – pak odeslání PDZ pomocí webové služby skončí chybou 1232.

Pro odesílání do schránek FO se nic nemění – mohou mít příjem PDZ povolený i zakázaný. Proto zůstávají v platnosti veškeré služby na zjišťování příjmu PDZ před odesláním zprávy. Pouze služba **GetDataBoxList** s parametrem „POA“ již nebude vracet jiné schránky než FO (a proto sloupec pro IČO subjektu bude nadále prázdný).

3.3 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 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) již na konci roku 2018 označil jako potenciálně problematický. Tyto šifrovací sady se již příliš nepoužívají, neboť jsou v novějších aplikacích nahrazeny aktuálními šifrovacími sadami protokolu TLSv1.2. Nicméně ISDS na konci roku 2021 stále eviduje určitý počet takových přístupů, včetně některých velkých a důležitých subjektů, proto bylo konečné vypnutí na produkčním prostředí opět odloženo.

Na produkčním prostředí bude vypnuta podpora těchto šifrovací sad:

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (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.