Informace pro vývojáře aplikací – listopad 2023

Datum: 21.11.2023
Verze: 1.2
Klasifikace: veřejný dokument

1 Anotace změn

1. Zavedení nových formátů příloh datových zpráv
2. Změny v aplikaci SDS
3. Odstranění zastaralé TLS šifry

2 Harmonogram změn

Pro bod 1:

Na Veřejném testu ISDS od 24.11.2023, na Produkci od 1.1.2024.

Pro bod 2:

Na Veřejném testu ISDS od 24.11.2023, na Produkci od 1.2.2024.

Pro bod 3:

Na Veřejném testu ISDS od 24.11.2023, na Produkci v první polovině roku 2024.

3 Popis změn

3.1 Nové multimediální formáty příloh

Podle nové verze vyhlášky č. 194/2009 Sb. se povolují další formáty příloh datových zpráv.

Formáty rodiny **MP4** (MPEG-4) - v tabulce jsou uvedeny i příslušné mime typy, potřebné pro webové služby. Tučně zvýrazněný typ se použije v případě, kdy je třeba z přípony souboru poznat a doplnit MIME typ.

Přípona	**MIME typ**	**Poznámka**
mp4	**audio/mp4** video/mp4	MPEG-4 part 14
m4a	audio/mp4	
m4p	**audio/mp4** video/mp4	

m4v	video/mp4	

Formát **HEIF** je nástupce obrázkového formátu JPEG. Jeho výhodou je výrazně nižší velikost při stejné kvalitě (resp. při stejné velikosti výrazně vyšší kvalita) a podpora užitečných funkcí jako jsou např. animace nebo ukládání sekvencí do jediného souboru. Formát je definován normou ISO/IEC 23008-12.

Přípona	**MIME typ**	**Poznámka**
heic	**image/heic** image/heic-sequence	High Efficiency Video Coding
heif	**image/heif** image/heif-sequence	High Efficiency Image File Format

Formáty příloh jsou na vstupu standardně kontrolovány na soulad přípony, mime-typu a obsahu dle zveřejněných specifikací. Ukazuje se však, že některé programy ukládají chybně soubory tak, že kontrolou neprojdou (přípona neodpovídá obsahu). V současné verzi bude takový soubor odmítnut – pokud by se objevil větší problém s určitou používanou aplikací, lze v budoucnu pravidla kontroly zmírnit. Objevíte-li při testování nějaké standardně vytvořené soubory, které nelze poslat, nahlaste to prosím přes web PoradnaIsds.cz.

3.2 Změny v aplikaci Seznamu datových schránek (SDS)

Novela zákona o ISDS (zákon č. 327/2023 Sb.) přináší s účinností od 1.2.2024 tyto změny a požadavky v datech ISDS a SDS:

1. Budou vymazána všechna data o FO a PFO schránkách ze SDS a všechny schránky FO a PFO (včetně podtypů) budou nastaveny do režimu Publikovat do SDS = False ke dni účinnosti.
2. Schránkám PFO (včetně podtypů) se umožní povolovat či zakazovat předávat svá data do SDS (pro schránky FO se nic nemění – budou to moct provádět stále).
3. Všechny nové schránky FO a PFO (včetně podtypů) budou mít implicitně nastaven příznak Publikovat do SDS na False.

Důsledek změn bude zejména to, že aplikace SDS (https://www.mojedatovaschranka.cz/sds/) nebude na jaře obsahovat prakticky žádné údaje o schránkách FO a PFO a plnění na vlastní žádost bude postupné. Tedy tato aplikace bude jen velmi omezeně použitelná při vyhledávání schránek FO a PFO. Stejně tak stahovaný seznam PFO schránek (jako OpenData) nebude příliš k užitku. Aplikace, které používaly neautentizované hledání v SDS nebo stahovaly OpenData u schránek FO a PFO, by měly přejít na autentizované hledání v ISDS.

3.3 Odstranění šifry DHE-RSA-AES128-GCM-SHA256

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) AES128 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, již prakticky nepoužívané šifrovací sady používající AES128 v módu GCM, 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. Tato šifrovací sada se již používá velmi málo, neboť je v novějších aplikacích nahrazena aktuálními šifrovacími sadami protokolu TLSv1.2.

Na všech rozhraních bude (postupně) vypnuta podpora této šifrovací sady:

TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)

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.