Informace pro vývojáře aplikací – říjen 2026

Datum: 23.10.2026
Verze: 1.0
Klasifikace: veřejný dokument

1 Anotace změn

1. Zpřísněná kontrola EDI a dalších minoritních formátů
2. Zapnutí TLS 1.3
3. Podpisový certifikát pod QCA5

Novinky v PROD jsou bez dopadu do dokumentace či WSDL.

2 Harmonogram změn

Pro bod 1:

Na Veřejném testu od 30.9.2026, na Produkci od 22.10.2026.

Pro bod 2:

Na Veřejném testu již od 8.6.2026, na Produkci od 22.10.2026

Pro bod 3:

Na Veřejném testu již od 8.6.2026, na Produkci od 22.10.2026

3 Popis změn

3.1 Zpřísněné kontroly příloh

3.1.1 Formát Edifact

Kontroly provozu objevily případy, kdy odesílatelé vkládali do datových zpráv s deklarovaným formátem EDI jiné přílohy, včetně takových, které by nebyly při správné deklaraci povoleny (např. složité ZIPy). Bylo využito příliš benevolentní kontroly EDI formátu, který předpokládal různé mnohé formáty Edifact, včetně binárních.

Od této verze jsou povoleny (v souladu s vyhláškou o ISDS) jen textové EDI formáty standardu UN/EDIFACT, ODETTE nebo EANCOM. Všechny tyto tři vyjmenované standardy **jsou čistě textové**. Ukázka:

```
UNH+1+INVOIC:D:96A:UN'
BGM+380+INV-9876'
DTM+137:20240930:102'
NAD+SU+5412345000013::9'
NAD+BY+4012345000094::9'
```

```
LIN+1'
PIA+5+BP12345:SA'
QTY+47:1000'
MOA+203:25000'
UNT+10+1'
```

Existují i jiné EDI modernější formáty (ty vyjmenované vycházejí z normy ANSI ASC X12 z roku 1979), např. v XML, ale ty vyhláška o provozu ISDS nezmiňuje a proto nebudou povoleny.

V současné verzi k příponě EDI povolujeme více odlišných mime-typů:

```
application/edifact
application/edi-x12
application/edi-consent
text/plain
```

3.1.2 Formáty QIX, SBN, SBX

Další zpřísnění kontrol souladu obsahu a deklarovaného mime-typu jsou formáty QIX, SBN, SBX. Jedná se o pracovní soubory z GIS systémů. Nemají zavedený odpovídající IANA mime-typ, proto i nadále budeme akceptovat a vracet obecný `application/octet-stream`.

Je však nově zaveden kontrola obsahu podle magic znaků na začátku souboru, protože se formáty již dostatečně standardizovaly.

3.1.3 Dopad na vývojáře

Pro aplikace, které výše uvedené přílohy posílají v souladu s provozním řádem ISDS, se nic nemění. Aplikacím, které se snaží Provozní řád obcházet, se bude při odesílání zprávy vracet chyba 1214.

3.2 Zapnutí TLS verze 1.3

Na přístupových branách ISDS bylo povoleno TLS verze 1.3.

TLS 1.3 přináší vyšší bezpečnost, kratší čas navázání spojení a je dnes standardem v moderních prohlížečích i bezpečnostních doporučeních. Z pohledu bezpečnosti TLS 1.3 odstraňuje některé zastaralé mechanismy z TLS 1.2.

3.2.1 Dopad na vývojáře

Po změně se velká část klientů automaticky přepne na TLS 1.3. Klienti, kteří ho nepodporují, se budou nadále připojovat přes TLSv1.2 bez nutnosti zásahu. Z běhu aplikací v prostředí veřejného testu je vidět, že naprostá většina aplikací přešla na TLS 1.3 bez problémů.

3.3 Nový podpisový certifikát

V září 2026 bylo zavedeno do rozhraní webových služeb tzv. přerazítkování, tj. vložení nového časového razítka do CAdES pečetě stažené DZ (ZFO soubor).

Příslušná ETSI norma pro archivní razítka vyžaduje, aby v razítkách bylo potvrzení platnosti podepisovacího certifikátu v okamžiku podpisu. ISDS historicky (od zahájení archivování) používá vložení tzv. CRL (seznam odvolaných certifikátů) do struktury razítka. Alternativní cesta využívající OCSP není v prostředí CA PostSignum technicky možná.

Historicky se pro pečeť využívá certifikát od PostSignum, vydaný pod aktuálně aktivní autoritou pro kvalifikovaný podpis/pečeť (nyní PostSignum Qualified CA 4). Seznam odvolaných certifikátů pod QCA4 je však poměrně veliký – každým přerazítkováním (vložením jednoho razítka) naroste proto velikost ZFO souboru o cca 0,5 MB.

ISDS proto získalo nový podepisovací (pečetící) certifikát vydaný pod jinou autoritou s výrazně menším CRL – Qualified CA 5. Pod touto autoritou je vydáno výrazně méně certifikátů, proto i CRL do budoucna nebude narůstat.

3.3.1 Dopad na vývojáře

Externí aplikace by při příjmu ZFO přílohy zprávy měly ověřovat platnost pečetě na elektronickém dokumentu. Nyní se u pečetě po mnoha letech změní vystavitel – to by mohlo teoreticky nějaké aplikace zmást. Za dobu 4 měsíců nasazení na Veřejném testu jsme však nezaznamenali jediný dotaz na tuto změnu.