Informace pro vývojáře aplikací, které pracují s datovými zprávami – podzim 2019

Datum: 27.8.2019
Verze: 1
Klasifikace: veřejný dokument

Anotace změny

Poskytovatel časových razítek pro ISDS (PostSignum) mění formát a strukturu časového razítka. Zdroj: http://www.postsignum.cz/novinky_postsignum.html#N307

Harmonogram změny

V prostředí veřejného testu ISDS bude změna nasazena v odstávce 30.8.2019 (veřejný test ISDS bude napojen na již běžící zdroj TSU-7). Na produkčním ISDS bude změna nasazena později, nejspíš v prosincové odstávce 8.12.2019. Toto datum se může ovšem změnit, pokud PostSignum změnu nasadí dříve, než bude odstávka ISDS.

Dokumentace

Struktura časových razítek (stará ani nová) není popsána ve veřejné dokumentaci ISDS.

Vysvětlení

Některé aplikace pracující s datovými zprávami samy rozebírají časová razítka v datové zprávě (tj. podací razítko a razítko obsažené v pečeti u stažené zprávy či doručenky). Víme již o aplikacích, kterým změna struktury působí potíže. Proto, byť nejde o změnu v ISDS, dáváme vývojářům s předstihem možnost otestovat si své aplikace na testovacím prostředí, a případně ještě reagovat do doby, než se nová razítka objeví v produkčním ISDS.

Změny ve struktuře razítek

PostSignum již nyní provozuje TSU7 vydávající razítka v nové struktuře. Detailním porovnáním staré a nové struktury časových razítek jsme došli k těmto hlavním rozdílům:

Výčet hlavních změn

Tyto změny jsou popsány v informačním materiálu od PostSignum (viz Anotace změny).

Stávající formát časového razítka v ISDS:

- Razítko obsahuje pečetící certifikát (a žádný z vystavujících certifikátů).

- Mezi hashovacím algoritmem uvedeným v žádosti o razítko a hashovacím algoritmem užitým ve výsledné elektronické pečeti (razítku) existuje vztah.
- Časové razítko obsahuje atributový certifikát.

Nový formát časového razítka v ISDS:

- Razítko bude obsahovat nejen **pečetící certifikát, ale i certifikát jeho vystavitele** – toto je klíčová změna, která může přinést problémy při analýze razítka.
- Mezi hashovacím algoritmem uvedeným v žádosti o razítko a hashovacím algoritmem užitým ve výsledné elektronické pečeti (razítku) již nebude existovat žádný vztah. Posledně zmíněný algoritmus bude vždy nastaven na SHA-256.
- Časové razítko nebude obsahovat atributový certifikát.

Výčet vedlejších změn

Stávající formát časového razítka uvádí následující položky a hodnoty:

- `SignedData.SignerInfo.digestAlgorithm` => specifikace parametrů uvádí ASN.1 NULL.
- `SignedData.SignerInfo.signatureAlgorithm` => sha256WithRSAEncryption
- `SignedData.SignerInfo.signedAttrs.signingCertificate`

Budoucí formát časového razítka bude uvádět:

- `SignedData.SignerInfo.digestAlgorithm` => specifikace parametrů je prázdná
- `SignedData.SignerInfo.signatureAlgorithm` => rsaEncryption (Poznámka: obecnější určení algoritmu)
- `SignedData.SignerInfo.signedAttrs.signingTime` (Poznámka: do pečetě razítka bude přidán atribut `signingTime`.)
- `SignedData.SignerInfo.signedAttrs.signingCertificateV2` (Poznámka: přechod podepsaného atributu `signingCertificate` z verze 1 (signingCertificateV1; RFC 2634) do verze 2 (signingCertificateV2; RFC 5035).)

V novém časovém razítku se změní také DN (distinguished name) PostSignum, které je inkludováno v několika částech razítka, resp. pečetě. Změna pramení ze změny v TSU certifikátech a QCA5. Do DN přibude "organizationIdentifier" (typu PRINTABLESTRING) a z položky "organizationName" zmizí IČ.

Úprava aplikací

Úprava (kontrola funkčnosti) se týká jen malého množství aplikací, které analyzují časová razítka nestandardním způsobem.

V ISDS budou nadále existovat dva typy časových razítek – starý a nový. Aplikace, rozebírající razítka, musí umět pracovat s oběma typy. CAdES struktura pečeti datové zprávy je natolik obecná, že akceptuje oba formáty razítek.

Velikost razítka se přidáním druhého certifikátu zvýší z cca 3.5 kB na cca 5 kB – je třeba pamatovat na prostor pro případné ukládání.