Modul dlhodobého uchovávania

ÚPVS

Prezervačný profil pre kvalifikovanú službu uchovávania kvalifikovaných elektronických podpisov a pečatí ÚPVS podľa ETSI TS 119 511

Obsah

Úvod

Prezervačný profil kvalifikovanej služby uchovávania ÚPVS je vytvorený podľa požiadaviek špecifikácie ETSI TS 119 511.

1. Identifikátor prezervačného profilu

Identifikátor prezervačného profilu: ÚPVS 1.0

(OVR-6.4-04 a)

2. Platnosť prezervačného profilu (validity period of the profile)

Začiatok platnosti: 12. decembra 2024

Koniec platnosti: 11. mája 2027

Časový interval pokrýva obdobie od začiatku využívania certifikátu zapísaného v TSL pre službu uchovávania po koniec platnosti tohto certifikátu.

Certifikát je dostupný v dôveryhodnom zozname.

(OVR-6.4-04 d)

3. Popis prezervačného profilu (description of the preservation profile in a human understandable language)

(OVR-6.4-04 i)

Prezervačný profil sa používa počas celej doby uchovávania konkrétneho dokumentu. Počas doby uchovávania však môže byť na rovnaký dokument použitý súčasne aj ďalší prezervačný profil (napríklad ochrana odtlačku jedného dokumentu dvoma odlišnými pečaťami).

Pre validáciu podpisov, pečatí a časových pečiatok a získanie dôkazových materiálov sa používajú služby centrálnej elektronickej podateľne, ktorej funkcionalita je popísaná v osobitnej špecifikácii.

Samotný princíp dlhodobej overiteľnosti KEP/KEPe je založený na vytváraní integritných elektronických podpisov (pečatí) vo formáte ASiC-XAdES pre zoznam digitálnych odtlačkov vytvorený z dokumentov podpísaných KEP/KEPe a z údajov potrebných pre ich overenie a na vytváraní archívnej formy integritných podpisov pred koncom ich platnosti. Pre tento účel sa využívajú služby modulu CEP – pečatenie, overenie podpisov, prevod el. podpisu na archívnu formu a časové pečiatky vydávané kvalifikovaným poskytovateľom dôveryhodných služieb.

Pred koncom platnosti integritného elektronického podpisu sa vykoná prevod tohto integritného podpisu na archívnu formu (LTA). V takýchto prípadoch bude možné podpis overiť a považovať za platný vďaka tomu, že archívny podpis zabezpečí dlhodobejšie dôveryhodné uzavretie obsahu všetkých potrebných informácií na overenie podpisu.

Funkcionalita pravidelne kontroluje platnosť certifikátov vyhotovených integritných elektronických podpisov. Na tento účel MDUERZ eviduje všetky certifikáty časových pečiatok, ktoré boli použité počas jeho činnosti a sleduje dátumy konca platnosti časových pečiatok.

Integritný elektronický podpis zároveň zabezpečí aj kontrolu integrity obsahu. Aplikuje sa na podpísaný aj nepodpísaný obsah. V prípade podpísaných dokumentov integritný podpis sa aplikuje aj na údaje potrebné pre overenie kvalifikovaného elektronického podpisu alebo pečate.

Dokumenty uložené do modulu dlhodobého uchovávania sú chránené v samotnom úložisku. Po skončení uchovávania budú dokumenty vrátené do elektronickej schránky organizácie, ktorá o ich uchovávanie žiadala, a to v stave, v akom boli do MDU vložené, pričom v prípade kvalifikovaných elektronických podpisov a pečatí vložených bez pripojenej kvalifikovanej časovej pečiatky budú obsahovať doplnenú kvalifikovanú časovú pečiatku, ak MDU pri vložení záznamu podporoval pridanie časovej pečiatky pre daný formát podpisu.

4. Podporované vstupné a výstupné formáty (supported operations of the preservation protocol)

(OVR-6.4-04 b)

Komponent implementuje predlžovanie dôveryhodnosti kvalifikovaných elektronických podpisov a pečatí a zdokonalených elektronických podpisov a pečatí založených na kvalifikovanom certifikáte vo formátoch podporovaných modulom Centrálnej elektronickej podateľne (ďalej „CEP“), prevádzkovanej v rámci internej infraštruktúry ÚPVS. Podporované formáty KEP a KEPe sú uvedené v kapitole 5.1 dokumentu „Dokumentácia funkčnosti Centrálnej elektronickej podateľne“ dostupného na adrese: https://www.slovensko.sk/_img/CMS4/Dokumentacia_funkcnosti_CEP.pdf

Do modulu je taktiež možné ukladať dokument (záznam) v ľubovoľnom inom formáte avšak v takom prípade nie je uplatňovaná funkcionalita predlžovania dôveryhodnosti podpisov a pečatí.

Služba implementuje štandardy podpisových štruktúr:

- CAdES ETSI TS 103173 v.2.2.1,
- PAdES ETSI TS 103172 v.2.2.2,

- XAdES ETSI TS 103171 v.2.1.1,
- kontajnera ASiC ETSI TS 103174 v.2.2.1.

Zároveň podporuje aj historické slovenské formáty podpisov XAdES_ZEP a CAdES.

Maximálna veľkosť akceptovaného súboru pre zaradenie do archivačnej služby je 35 MB.

Archivačná služba nepodporuje uchovávanie vnorených kontajnerov, t. j. kontajnerov, ktoré obsahujú ďalšie kontajnery. Na vnorené kontajnery je nahliadané ako na binárne súbory a ich vnútorné podpisy/pečate nebudú uchovávané v zmysle predlžovania ich platnosti.

Výstupné formáty:

Ochrana dokumentov a platnosť podpisov je v MDU ÚPVS zabezpečená naraz pre päť záznamov (bez ohľadu na počet dokumentov v daných záznamoch) vytvorením tzv. systémového záznamu, v ktorom sú integritným podpisom (kvalifikovanou elektronickou pečaťou) chránené digitálne odtlačky jednotlivých dokumentov (záznamov) a údajov potrebných pre overenie platnosti podpisového certifikátu v čase ukladania záznamu (CRL súbory s údajmi o zneplatnených certifikátoch platné v čase uloženia a overenia dokumentu v MDU, súbory podpisových certifikátov a certifikát vydavateľa certifikátu) a samotné súbory. Systémový záznam je uchovávaný a chránený aj po ukončení doby uchovávania dokumentu, ku ktorému sa viaže. Integritný podpis chrániaci digitálne odtlačky dokumentov je pred vypršaním jeho platnosti prevádzaný na archívnu formu.

Údaje o chránených dokumentoch sa uvádzajú v XML dátovej štruktúre elektronického formulára s identifikátorom MDURZ.Manifest, ktorá je zapečatená vo formáte podpisového kontajnera ASiC-XAdES. XML súbor manifestu je zapečatený v rámci dátovej štruktúry XMLDataContainer. V manifeste sú uvedené údaje:

- URI - obsahuje číslo záznamu a za znakom „lomka“ oddelené interné číslo dokumentu v rámci záznamu,
- DigestMethod - hašovacia funkcia pre výpočet digitálneho odtlačku chránených súborov, v súčasnosti SHA-256,
- DigestValue - hodnota digitálneho odtlačku dokumentu vypočítaná hašovacou funkciou uvedenou v poli DigestMethod.

Systémový záznam obsahuje:

- Zapečatený fixačný manifest obsahujúci digitálne odtlačky samotných dokumentov vytváraný po uložení dokumentov do MDU, pričom pri podpísaných dokumentoch je vytváraný až po kontrole prítomnosti časovej pečiatky v podpisoch a úspešnom doplnení časovej pečiatky v prípade jej absencie. Fixačný

manifest sa v prípade podpísaných dokumentov vytvára pred úplným overením podpisov a zozbieraním údajov pre dlhodobé overenie platnosti certifikátu.
- Finálny manifest vytváraný po úplnom overení podpisov, ak záznamy obsahujú podpisy. Ak podpisy neobsahujú, vytvára sa finálny manifest krátko po fixačnom manifeste.
- Podpisové certifikáty, certifikáty z certifikačnej cesty vydavateľa certifikátu osoby, ktorá dokument podpísala/zapečatila, certifikáty časových pečiatok.

5. Technické pravidlá pre dôkazy o uchovávaní (Technical policy / Preservation service policy)

(OVR-6.4-04 c)

Používané algoritmy v pečatiach systémových záznamov a v časových pečiatkach: RSA - SHA 256

Veľkosť RSA kľúča v pečatiach a v časových pečiatkach: 3072 bit.

V rámci prevodu podpisov z B formy na T formu, taktiež v rámci pečatenia systémových záznamov a taktiež v rámci prevodu na archívnu formu sú používané kvalifikované dôveryhodné služby vyhotovovania kvalifikovaných časových pečiatok:

- NASES Time Stamp Authority 1 (TLISK 137)
- NASES Time Stamp Authority 2 (TLISK 138)
- NASES Time Stamp Authority 3 (TLISK 139)

Prevody integritných podpisov na archívnu formu sú vykonávané počas platnosti kvalifikovaných časových pečiatok v nich použitých.

6. Model uchovávania (preservation storage model)

(OVR-6.4-04 e)

Model uchovávania: úložisko (Preservation service with storage - WST)

Samotné dokumenty sú uchovávané v úložisku služby. Ich digitálne odtlačky sú však chránené aj v prípade ukončenia ich uchovávania v úložisku služby.

7. Ciele uchovávania (preservation goals)

(OVR-6.4-04 f)

Ciele uchovávania: uchovávanie elektronických podpisov a dôkazových materiálov potrebných pre ich overenie, ochrana ich integrity pečaťou.

V prípade nemožnosti získať dôkazové materiály (CRL a certifikáty) služba uchovávania indikuje chybu pre prevádzku. V prípade nemožnosti získať dôkazové materiály

- z dôvodu nedostupnosti služby CEP, sa čaká na jej dostupnosť (v rámci retry-policy alebo manuálnym zásahom prevádzky),
- z dôvodu neoveriteľnosti podpisov (nekvalifikované certifikáty alebo nepodporované formáty) nie je chránená platnosť podpisov a pečatí (podrobnosti sú uvedené v dokumente Dokumentácia funkčnosti MDU a známych obmedzení.

[PDS+PGD] combined preservation of digital signatures and general data

1) the provision of proofs of existence over long periods of time of general data whether this data is signed or not;

2) the preservation over long periods of time of the ability to validate a digital signature, to maintain its validity status and to get a proof of existence of the associated signed data

8. Podporované evidenčné formáty (supported evidence formats)

(OVR-6.4-04 g)

Podporované evidenčné formáty potvrdzujúce predĺženie dôveryhodnosti podpisov aj po uplynutí ich technologickej platnosti: manifest obsahujúci digitálne odtlačky chránených súborov, zapečatený kvalifikovanou pečaťou s pripojenou kvalifikovanou časovou pečiatkou (evidence record – protected with QSeal and time-stamp)

9. Technické špecifikácie (publicly available specification in which the preservation profile is described)

Služba pre účely prevodov integritných podpisov na archívnu formu implementuje postup popísaný vyššie.