Návod k používaniu správy Výsledok informatívneho overenia podpisov a pečatí pre orgány verejnej moci

Obsah

Vypracovalo: oddelenie redakcie ÚPVS, Národná agentúra pre sieťové a elektronické služby
Pozn.: Použité obrázky sú iba ilustračné.

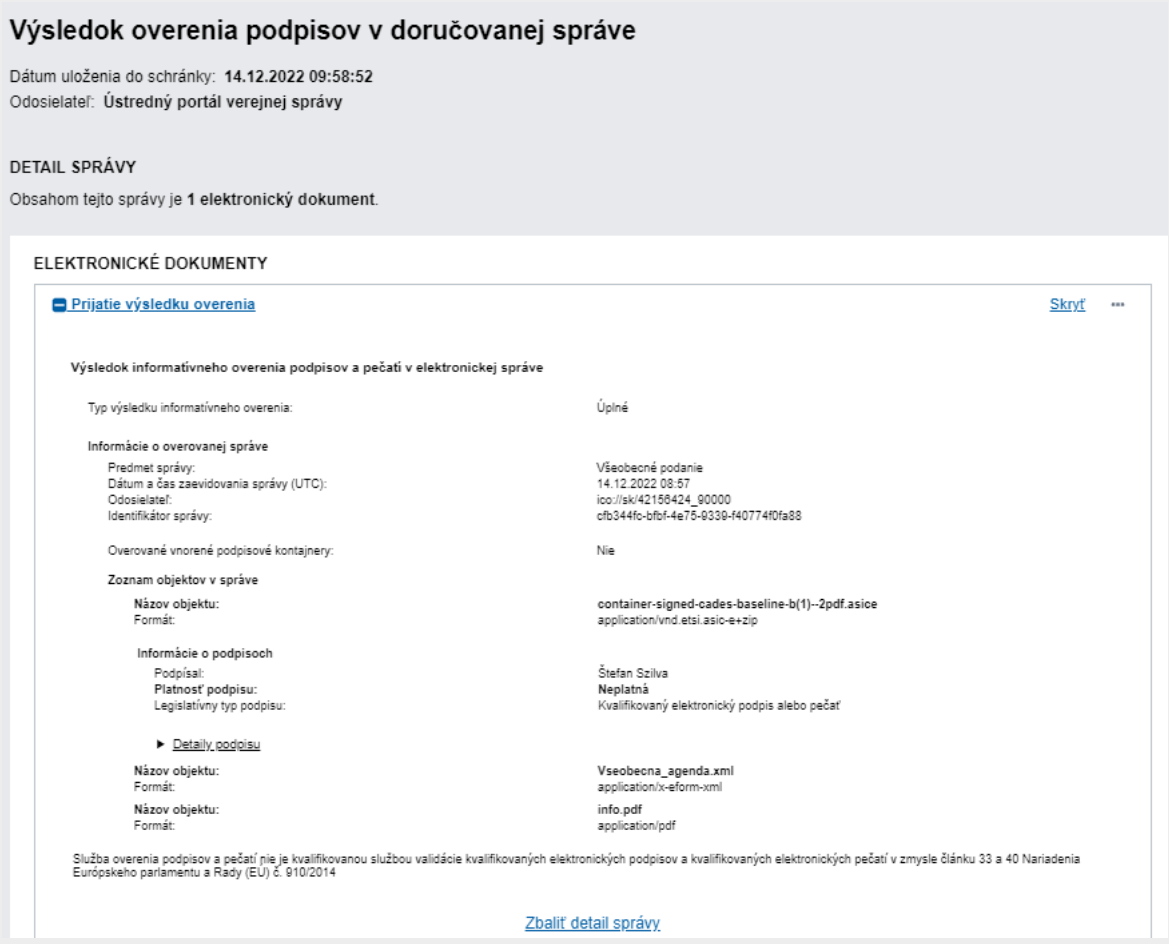
Úvod

Orgánom verejnej moci, ktoré používajú centrálnu elektronickú podateľňu ako svoju podateľňu, je ku každému elektronickému podaniu a elektronickému úradnému dokumentu doručenému do elektronickej schránky automaticky zasielaný výsledok overenia podpisov.

Cieľom tohto dokumentu je vysvetliť obsah tohto výsledku overenia podpisov.

Výsledok informatívneho overenia podpisov od 19. decembra 2022

Od 19. decembra 2022 je orgánom verejnej moci, ktoré používajú centrálnu elektronickú podateľňu ako svoju podateľňu, zasielaná nová štruktúra výsledku overenia podpisov (Obr. 1).



Výsledok overenia podpisov v doručovanej správe

Dátum uloženia do schránky: **14.12.2022 09:58:52**
Odosielateľ: **Ústredný portál verejnej správy**

DETAIL SPRÁVY

Obsahom tejto správy je **1 elektronický dokument**.

ELEKTRONICKÉ DOKUMENTY

Prijatie výsledku overenia — Skryť

Výsledok informatívneho overenia podpisov a pečatí v elektronickej správe

Typ výsledku informatívneho overenia: Úplné

Informácie o overovanej správe

Predmet správy: Všeobecné podanie
Dátum a čas zaevidovania správy (UTC): 14.12.2022 08:57
Odosielateľ: ico://sk/42156424_90000
Identifikátor správy: cfb344fc-bfbf-4e75-9339-f40774f0fa88

Overované vnorené podpisové kontajnery: Nie

Zoznam objektov v správe

Názov objektu: container-signed-cades-baseline-b(1)--2pdf.asice
Formát: application/vnd.etsi.asic-e+zip

Informácie o podpisoch

Podpísal: Štefan Szilva
Platnosť podpisu: **Neplatná**
Legislatívny typ podpisu: Kvalifikovaný elektronický podpis alebo pečať

▶ Detaily podpisu

Názov objektu: Vseobecna_agenda.xml
Formát: application/x-eform-xml

Názov objektu: info.pdf
Formát: application/pdf

Služba overenia podpisov a pečatí nie je kvalifikovanou službou validácie kvalifikovaných elektronických podpisov a kvalifikovaných elektronických pečatí v zmysle článku 33 a 40 Nariadenia Európskeho parlamentu a Rady (EU) č. 910/2014

Zbaliť detail správy

Obr. 1: Príklad výsledku overenia podpisov zasielaného od 19. decembra 2022.

Vypracovalo: oddelenie redakcie ÚPVS, Národná agentúra pre sieťové a elektronické služby
Pozn.: Použité obrázky sú iba ilustračné.

Výsledok overenia obsahuje nasledujúce pomocné a hlavné údaje:

Pomocné údaje:

Typ výsledku informatívneho overenia – uvádza, či ide o predbežné overenie, ktoré ešte môže obsahovať podpisy so stavom „predbežne platná“ alebo ide o úplné overenie, v ktorom sa už stav „predbežne platná“ nemôže vyskytovať. Dôvodom zasielania dvoch typov výsledku overenia je, že pre úplné overenie môže byť najmä v prípadoch, kedy vydavateľ certifikátov neposkytuje online údaje potrebné pre overenie certifikátu (cez službu OCSP).

Predmet správy – obsahuje predmet elektronického podania alebo rozhodnutia, ku ktorému je vytvorený výsledok overenia podpisov

Dátum a čas zaevidovania správy – obsahuje dátum a čas, kedy prišlo k prijatiu správy v centrálnej elektronickej podateľni

Odosielateľ – obsahuje URI identifikátor elektronickej schránky osoby, ktorá zaslala podanie alebo rozhodnutie, ku ktorému je vytvorený výsledok overenia podpisov. Ide o technický identifikátor schránky vytváraný Ústredným portálom verejnej správy v zmysle Vyhlášky č. 385/2022 Z. z. o jednotnom formáte elektronických správ.

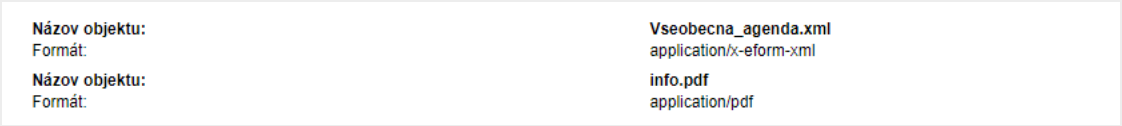
Identifikátor správy – obsahuje jedinečný identifikátor elektronickej správy (MessageId), ku ktorej je vytvorený výsledok overenia podpisov v zmysle Vyhlášky č. 385/2022 Z. z. o jednotnom formáte elektronických správ.

Overované vnorené podpisové kontajnery – uvádza informáciu, či služba overuje vnorené podpisové kontajnery. V súčasnosti centrálna elektronická podateľňa nepodporuje overovanie vnorených kontajnerov a preto sa vždy uvádza informácia „Nie“.

Hlavné údaje potrebné pre vyhodnotenie podpisu

Zoznam objektov v správe – obsahuje zoznam súborov (dokumentov) nachádzajúcich sa v elektronickej správe, ku ktorej sa vytvára overenie podpisov (Obr. 2).

Názov objektu – obsahuje názov súboru v doručenej správe (napríklad názov ASiC súboru, PDF súboru a podobne). Tento údaj umožňuje porozumieť, ktorý z doručených súborov bol podpísaný. V prípade nepodpísaných súborov sa pod názvom a formátom objektu nezobrazuje sekcia „Informácie o podpisoch“. Príklad nepodpísaného objektu vo výsledku overenia podpisov:



Obr. 2: Hlavné údaje potrebné pre vyhodnotenie podpisu

Formát – obsahuje technické označenie formátu súboru (tzv. mimetype) v zmysle § 18 písm. f) Vyhlášky č. 78/2020 Z. z. o štandardoch. Napríklad v prípade ASiC súboru ide o „application/vnd.etsi.asic-e+zip“, v prípade PDF súboru ide o „application/pdf“. Dôvodom pre uvádzanie tohto údaja je, že prípona súboru v „Názov objektu“ nie je vždy uvedená, resp. nie vždy zodpovedá formátu uvedenému v podpise.

Informácie o podpisoch – sekcia obsahuje podrobné informácie o jednotlivých podpisoch

Podpísal – uvádza meno a priezvisko alebo názov podpisujúcej osoby a detailné informácie uvedené v podpisovom certifikáte.

V prípade mandátneho certifikátu obsahuje aj údaje o mandáte podľa zoznamu oprávnení zverejňovaného Národným bezpečnostným úradom, údaje o fyzickej osobe a môže obsahovať aj údaje o právnickej osobe, pre ktorú vykonáva činnosť.

V prípade fyzickej osoby obsahuje meno a priezvisko alebo pseudonym a nemusí obsahovať iné osobné údaje. Kvalifikované certifikáty pre kvalifikovaný elektronický podpis vydávané v Slovenskej republike obsahujú aj rodné číslo, prípadne ďalšie údaje.

V prípade pečate obsahuje najmenej názov právnickej osoby a prípadné registračné číslo, ako sa uvádza v úradných záznamoch.

Platnosť podpisu – obsahuje jednu z možností: platná, predbežne platná, neplatná, neoveriteľná, nie je možné rozhodnúť. V prípade úplného overenia podpisov sa hodnota „predbežne platná“ nevyskytuje.

K jednotlivým stavom overenia podpisov uvádzame vysvetlenie:

- "**predbežne platná**" - výsledok je poskytovaný len v predbežnom overení, odporúčame počkať na konečný výsledok overenia, nakoľko vo výnimočných prípadoch by mohlo prísť k zneplatneniu daného certifikátu v čase medzi poslednou dostupnou informáciou o zrušených certifikátoch a novou, ktorú podateľňa získa pri najbližšej aktualizácii údajov. Stav, kedy:

  a) podpis nemá platnú kvalifikovanú časovú pečiatku podpisu a overuje sa k aktuálnemu času, pričom pre overenie sú použité aktuálne dostupné údaje o zrušení certifikátov (revokácii),

  b) podpis má platnú kvalifikovanú časovú pečiatku podpisu, ale pre overenie sú dostupné a použité údaje o revokácii (CRL alebo OCSP), ktorých údaj o aktuálnosti informácií (údaj „thisUpdate“ je menší ako čas z časovej pečiatky, napr. z dôvodu, že CRL po časovej pečiatke ešte nebolo vypublikované).

- "**nie je možné rozhodnúť**" - tento výsledok je v prípade konečného výsledku úplného overenia obvykle možné interpretovať ako neplatný podpis. Služba ho poskytuje:

  a) len pre formáty podpisov ASiC (obsahujúcim XAdES podpis) a priamo podpísaným PDF (obsahujúcim PAdES podpis),

  b) v prípade, ak ide o exspirovaný certifikát a absentuje dôkaz o existencii podpisu v čase pred alebo po exspirácii certifikátu potrebný pre určenie platnosti.

Stav, kedy na základe dostupných validačných údajov nie je možné vyhodnotiť platnosť podpisu. Tento výsledok však v niektorých prípadoch znamená, že overovacia aplikácia nepodporuje plné overenie daného podpisu napríklad v dôsledku nepodporovaného povinného algoritmu predpísaného Národným bezpečnostným

úradom SR, pričom v takých prípadoch je vhodné vykonať overenie s využitím inej aplikácie, nakoľko centrálna elektronická podateľňa v súčasnosti v prípade formátov XAdES a CAdES nepodporuje všetky povinné algoritmy.

- "**neoveriteľná**" - tento výsledok je obvykle možné interpretovať ako neplatný podpis, napríklad v prípade formátu ASiC (s podpisom CAdES), ak ide o exspirovaný certifikát; tento výsledok však v niektorých prípadoch znamená, že overovacia aplikácia nepodporuje plné overenie daného podpisu napríklad v dôsledku nepodporovaného povinného algoritmu predpísaného Národným bezpečnostným úradom SR, pričom v takých prípadoch je vhodné vykonať overenie s využitím inej aplikácie, nakoľko centrálna elektronická podateľňa v súčasnosti v prípade formátov XAdES a CAdES nepodporuje všetky povinné algoritmy. Stav autorizácie, ak je splnená niektorá z nižšie uvedených podmienok:

1) autorizácia je chybná (chybný formát resp. štruktúra podpisu)

2) nie je možné vyzbierať validačné údaje (v CEP nie je nakonfigurovaný vydavateľ podpisového certifikátu alebo certifikátu časovej pečiatky alebo sú validačné údaje podpísané nepodporovaným algoritmom).

3) overovací komponent pre XAdES_ZEP alebo CAdES vráti niektorú z chýb:

a) 514 - Nemožno vyhodnotiť platnosť podpisového certifikátu. Príliš stará revokačná informácia v parametroch volania.

b) 518 - Chyba pri overovaní certifikačnej cesty certifikátu časovej pečiatky. V parametroch volania bol nájdený nedôveryhodný koreňový certifikát. V službách informatívneho overenia sa takýto stav autorizácie/podpisu nevracia. Pri splnení vyššie uvedených podmienok sa vráti chyba volania (Kód odlišný od 0).

Legislatívny typ podpisu – uvádza typ podpisu definovaný v Nariadení Európskeho parlamentu a Rady EÚ č. 910/2014 alebo v slovenskej legislatíve (napr. Vyhláška o uznaných spôsoboch autorizácie). Podrobné vysvetlenie zverejňujeme na stránke slovensko.sk.

„1“ - Kvalifikovaný elektronický podpis / Kvalifikovaná elektronická pečať,

„2“ - Zdokonalený elektronický podpis založený na kvalifikovanom certifikáte / Zdokonalená elektronická pečať založená na kvalifikovanom certifikáte,

„3“ - Zdokonalený elektronický podpis / Zdokonalená elektronická pečať,

„4“ - Iný elektronický podpis/pečať,

„5“ - Uznaný spôsob autorizácie (informácie o uznanom spôsobe autorizácie),

„6“ – Zdokonalený elektronický podpis / Zdokonalená elektronická pečať poskytovateľa kvalifikovanej služby validácie,

„7“ – Zdokonalený elektronický podpis / Zdokonalená elektronická pečať kvalifikovanej služby uchovávania

Pomocné technické informácie

Detaily podpisu – sekcia obsahuje detailné informácie o podpisoch

Popis výsledku overenia – obsahuje technické informácie o príčine výsledku overenia podpisov, napríklad príčinu neplatnosti alebo neoveriteľnosti. Príklad: „Chyba pri overovaní certifikačnej cesty podpisového certifikátu. Certifikát v certifikačnej ceste vystavanej z parametrov volania je neplatný pre špecifikovaný čas overenia."

Kód výsledku overenia – obsahuje kód priradený k popisu výsledku overenia, slúži len pre identifikáciu konkrétnej príčiny pri strojovom spracovaní

Deklarovaný dátum a čas podpisu (UTC) – obsahuje nedôveryhodný dátum a čas podpisu, ktorý manuálne uviedla podpisujúca osoba alebo automatizovane podpisová aplikácia. Čas je uvádzaný v časovom pásme „UTC" (koordinovaný svetový čas), ktorý má časový posun oproti časovému pásmu stredoeurópskeho času alebo stredoeurópskeho letného času o mínus 1 alebo mínus 2 hodiny.

Dátum a čas kvalifikovanej časovej pečiatky pripojenej k podpisu (UTC) – obsahuje dôveryhodný dátum a čas, pred ktorým vznikol podpis. Čas je uvádzaný v časovom pásme „UTC", ktorý má časový posun oproti časovému pásmu stredoeurópskeho času alebo stredoeurópskeho letného času.

Pokiaľ je tento údaj vyplnený a obsahuje čas dostatočne skorší ako je „Dátum a čas overenia" (napríklad aspoň o minútu), k podpisu bola zo strany odosielateľa pred doručením podania pripojená platná kvalifikovaná časová pečiatka. Prítomnosť kvalifikovanej časovej pečiatky v danom podpise je možné overiť aj overením daného podpisu napríklad službou v elektronickej schránke alebo na ÚPVS.

Dátum a čas overenia (UTC) – obsahuje čas, kedy bolo vykonané overenie podpisov v centrálnej elektronickej podateľni. Čas je uvádzaný v časovom pásme „UTC", ktorý má časový posun oproti časovému pásmu stredoeurópskeho času alebo stredoeurópskeho letného času.

Informácie o certifikáte – sekcia obsahuje podrobnejšie informácie o podpisovom certifikáte

Subjekt – obsahuje informácie o osobe, ktorej bol certifikát vydaný

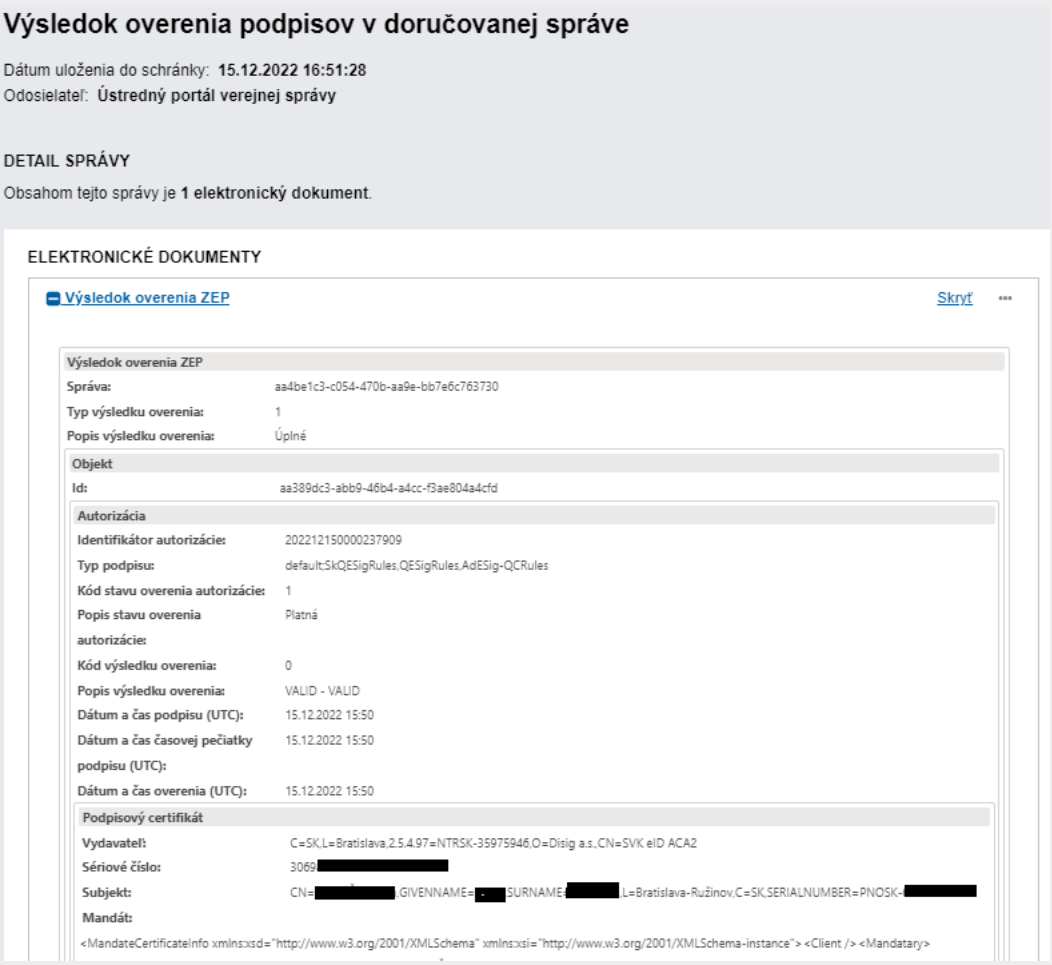
Vydavateľ certifikátu - obsahuje informácie o vydavateľovi certifikátu

Sériové číslo certifikátu - obsahuje identifikačný kód certifikátu, ktorý musí byť jedinečný pre kvalifikovaného poskytovateľa dôveryhodných služieb

Výsledok informatívneho overenia podpisov do 18. decembra 2022

Do 18. decembra 2022 sa orgánom verejnej moci, ktoré nepožiadali o zasielanie novej štruktúry, zasielala jednoduchšia dátová štruktúra overenia podpisov, ktorá neuvádzala v čitateľnej podobe názov podpísaného súboru a neumožňovala tak spárovať podpísané dokumenty s podpismi (Obr. 3)

Orgány verejnej moci, ktoré požiadali o posun termínu, dostávajú túto štruktúru aj po 18. decembri 2022.



Výsledok overenia podpisov v doručovanej správe

Dátum uloženia do schránky: **15.12.2022 16:51:28**
Odosielateľ: **Ústredný portál verejnej správy**

DETAIL SPRÁVY

Obsahom tejto správy je **1 elektronický dokument**.

ELEKTRONICKÉ DOKUMENTY

Výsledok overenia ZEP — Skryť

Výsledok overenia ZEP	
Správa:	aa4be1c3-c054-470b-aa9e-bb7e6c763730
Typ výsledku overenia:	1
Popis výsledku overenia:	Úplné
Objekt	
Id:	aa389dc3-abb9-46b4-a4cc-f3ae804a4cfd
Autorizácia	
Identifikátor autorizácie:	202212150000237909
Typ podpisu:	default:SkQESigRules,QESigRules,AdESig-QCRules
Kód stavu overenia autorizácie:	1
Popis stavu overenia autorizácie:	Platná
Kód výsledku overenia:	0
Popis výsledku overenia:	VALID - VALID
Dátum a čas podpisu (UTC):	15.12.2022 15:50
Dátum a čas časovej pečiatky podpisu (UTC):	15.12.2022 15:50
Dátum a čas overenia (UTC):	15.12.2022 15:50
Podpisový certifikát	
Vydavateľ:	C=SK,L=Bratislava,2.5.4.97=NTRSK-35975946,O=Disig a.s.,CN=SVK eID ACA2
Sériové číslo:	3069[redacted]
Subjekt:	CN=[redacted],GIVENNAME=[redacted],SURNAME=[redacted],L=Bratislava-Ružinov,C=SK,SERIALNUMBER=PNOSK-[redacted]
Mandát:	

<MandateCertificateInfo xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"> <Client /> <Mandatary>

Obr. 3: Príklad výsledku overenia podpisov zasielaného do 18. decembra 2022.

Správa – obsahuje jedinečný identifikátor elektronickej správy (MessageId), ku ktorej je vytvorený výsledok overenia podpisov v zmysle Vyhlášky č. 385/2022 Z. z. o jednotnom formáte elektronických správ.

Typ výsledku overenia a **Popis výsledku overenia** – uvádza, či ide o predbežné overenie (1), ktoré ešte môže obsahovať podpisy so stavom „predbežne platná“ alebo ide o úplné overenie, v ktorom sa už stav „predbežne platná“ nemôže vyskytovať. Dôvodom zasielania dvoch typov výsledku overenia je, že pre úplné overenie môže byť najmä v prípadoch, kedy vydavateľ certifikátov neposkytuje online údaje potrebné pre overenie certifikátu (cez službu OCSP).

Objekt – **Id** – uvádza jednoznačný identifikátor objektu elektronickej správy v zmysle Vyhlášky č. 385/2022 Z. z. o jednotnom formáte elektronických správ

Identifikátor autorizácie – jedinečný interný technický kód centrálnej elektronickej podateľne použitý pre danú autorizáciu.

Typ podpisu – obsahuje pravidlá splnené podpisovým certifikátom. Ak certifikát spĺňa viaceré pravidlá, sú uvádzané všetky. Tento údaj je primárne určený pre automatizované spracovanie. Je ho však možné vyhodnotiť aj manuálne podľa tabuľky uvedenej nižšie (nie je vhodné pre bežného používateľa).

Popis stavu overenia autorizácie – obsahuje jednu z možností: platná, predbežne platná, neplatná, neoveriteľná, nie je možné rozhodnúť. V prípade úplného overenia podpisov sa hodnota „predbežne platná“ nevyskytuje. Podrobné informácie sú uvedené pre údaj „Platnosť podpisu“ v predošlej kapitole.

Popis výsledku overenia – obsahuje technické informácie o príčine výsledku overenia podpisov, napríklad príčinu neplatnosti alebo neoveriteľnosti. Príklad: *„Chyba pri overovaní certifikačnej cesty podpisového certifikátu. Certifikát v certifikačnej ceste vystavanej z parametrov volania je neplatný pre špecifikovaný čas overenia.“*

Kód výsledku overenia – obsahuje kód priradený k popisu výsledku overenia, slúži len pre identifikáciu konkrétnej príčiny pri strojovom spracovaní

Podpisový certifikát – obsahuje

Vydavateľ certifikátu - obsahuje informácie o vydavateľovi certifikátu – kvalifikovanom poskytovateľovi dôveryhodných služieb

Sériové číslo certifikátu - obsahuje identifikačný kód certifikátu, ktorý musí byť jedinečný pre kvalifikovaného poskytovateľa dôveryhodných služieb

Subjekt – obsahuje informácie o osobe, ktorej bol certifikát vydaný. V prípade mandátneho certifikátu obsahuje aj údaj o mandáte.

Mandát – obsahuje v technickej podobe informácie o mandáte (Mandatary , Mandate) v prípade mandátneho certifikátu. V prípade ostatných osôb obsahuje iba údaje o danej osobe, bez uvedenia detailov o mandáte.

Technický postup pre určenie typu certifikátu a odvodenie legislatívneho typu podpisu

Pre určenie typu certifikátu a následné odvodenie legislatívneho typu podpisu je potrebné:

1. z poľa TypPodpisu získať druhú časť (oddelovač je bodkočiarka). Príklad: “default;SkQESigRules,QESigRules,AdESig-QCRules”
2. Z hodnôt získaných v prvom kroku (oddeľovač hodnôt je čiarka) vybrať hodnotu s najvyššou váhou podľa nasledujúcej tabuľky v stĺpci “Názov”. Tabuľka je zoradená v poradí od najvyššej váhy, v prípade položiek s rovnakou váhou je potrebné vybrať

položku, ktorá je v tabuľke umiestnená vyššie. Tým sa určí typ certifikátu a aj legislatívny typ podpisu.

Kód	**Názov**	Váha	**Typ certifikátu - popis**	**Legislatívny typ podpisu**
11	QESValidationRules	12	Certifikát kvalifikovanej služby validácie elektronických podpisov/pečatí	Zdokonalený elektronický podpis / Zdokonalená elektronická pečať poskytovateľa kvalifikovanej služby validácie
12	PSESRules	10	Certifikát kvalifikovanej služby uchovávania elektronických podpisov/pečatí	Zdokonalený elektronický podpis / Zdokonalená elektronická pečať kvalifikovanej služby uchovávania
3	SkQESig-MQCRules	8	SK kvalifikovaný mandátny certifikát pre elektronický podpis uložený na QSCD zariadení	Kvalifikovaný elektronický podpis / Kvalifikovaná elektronická pečať
1	SkQESigRules	6	SK kvalifikovaný certifikát pre elektronický podpis uložený na QSCD zariadení	Kvalifikovaný elektronický podpis / Kvalifikovaná elektronická pečať
2	SkQESealRules	6	SK kvalifikovaný certifikát pre elektronickú pečať uložený na QSCD zariadení	Kvalifikovaný elektronický podpis / Kvalifikovaná elektronická pečať
4	QESigRules	4	Kvalifikovaný certifikát pre elektronický podpis uložený na QSCD zariadení	Kvalifikovaný elektronický podpis / Kvalifikovaná elektronická pečať
5	QESealRules	4	Kvalifikovaný certifikát pre elektronickú pečať uložený na QSCD zariadení	Kvalifikovaný elektronický podpis / Kvalifikovaná elektronická pečať
6	AdESig-QCRules	2	Kvalifikovaný certifikát pre elektronický podpis	5 - počas platnosti vyhlášky o uznaných spôsoboch autoriácie Zdokonalený elektronický podpis založený na kvalifikovanom certifikáte / Zdokonalená elektronická pečať založená na kvalifikovanom certifikáte
7	AdESeal-QCRules	2	Kvalifikovaný certifikát pre elektronickú pečať	2
8	AdESigRules	1	Nekvalifikovaný certifikát pre elektronický podpis	3
9	AdESealRules	1	Nekvalifikovaný certifikát pre elektronickú pečať	3
10	OtherSigSealRules	0	Iný certifikát pre elektronický podpis/pečať	4