Návod k používaniu správy Upozornenie na neplatnosť zaslaného podpisu

Obsah

1. Úvod

Odosielateľ, ktorý odosiela podanie, v ktorom je niektorý z podpisov vyhodnotený ako „neplatný“, „neoveriteľný“ alebo „nie je možné rozhodnúť“, dostane od konca roka 2022 do elektronickej schránky správu „Upozornenie na neplatnosť zaslaného podpisu“ s informáciou o tomto probléme.

Cieľom správy je čo najskôr po odoslaní podania upozorniť používateľa na neplatnosť podpisov, ktorá potenciálne môže mať za následok zamietnutie alebo odloženie podania. K zamietnutiu alebo odloženiu (bez informovania odosielateľa ak to osobitný predpis umožňuje) môže orgán verejnej moci pristúpiť, ak vyhodnotí danú autorizáciu ako nepostačujúcu z hľadiska právnych predpisov. V správe je uvedené upozornenie, že ide iba o informatívne overenie podpisov a overenie podpisov nevyhodnocuje splnenie požiadaviek na autorizáciu pre danú elektronickú službu, nakoľko v súčasnosti nie je k dispozícii centrálna evidencia požiadaviek na autorizáciu podania a / alebo jeho príloh, ktorá by umožňovala vykonávať v CEP takúto automatizovanú kontrolu.

Treba však upozorniť, že táto správa nehovorí, či boli alebo neboli požiadavky na autorizáciu podania alebo príloh splnené. Informuje iba o autorizáciách, ktoré sú neplatné, neoveriteľné alebo o ich platnosti nie je možné rozhodnúť. O tom, ako bude autorizácia podania (podpisov) vyhodnotená, rozhodujú jednotlivé orgány verejnej moci, ktorým sú podania a ich prílohy adresované a iba oni môžu rozhodnúť o akceptácii alebo odmietnutí prijatia podania. Táto správa / informácia je teda len pomôcka pre odosielateľa / podávajúceho, aby mohol prípadne chybné podanie opraviť a podať platne autorizované.

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

Správa neupozorňuje ani na nedostatočnú autorizáciu podľa príslušnej legislatívy týkajúcej sa konkrétneho druhu podania a toto posudzuje až adresát podania. Napríklad:

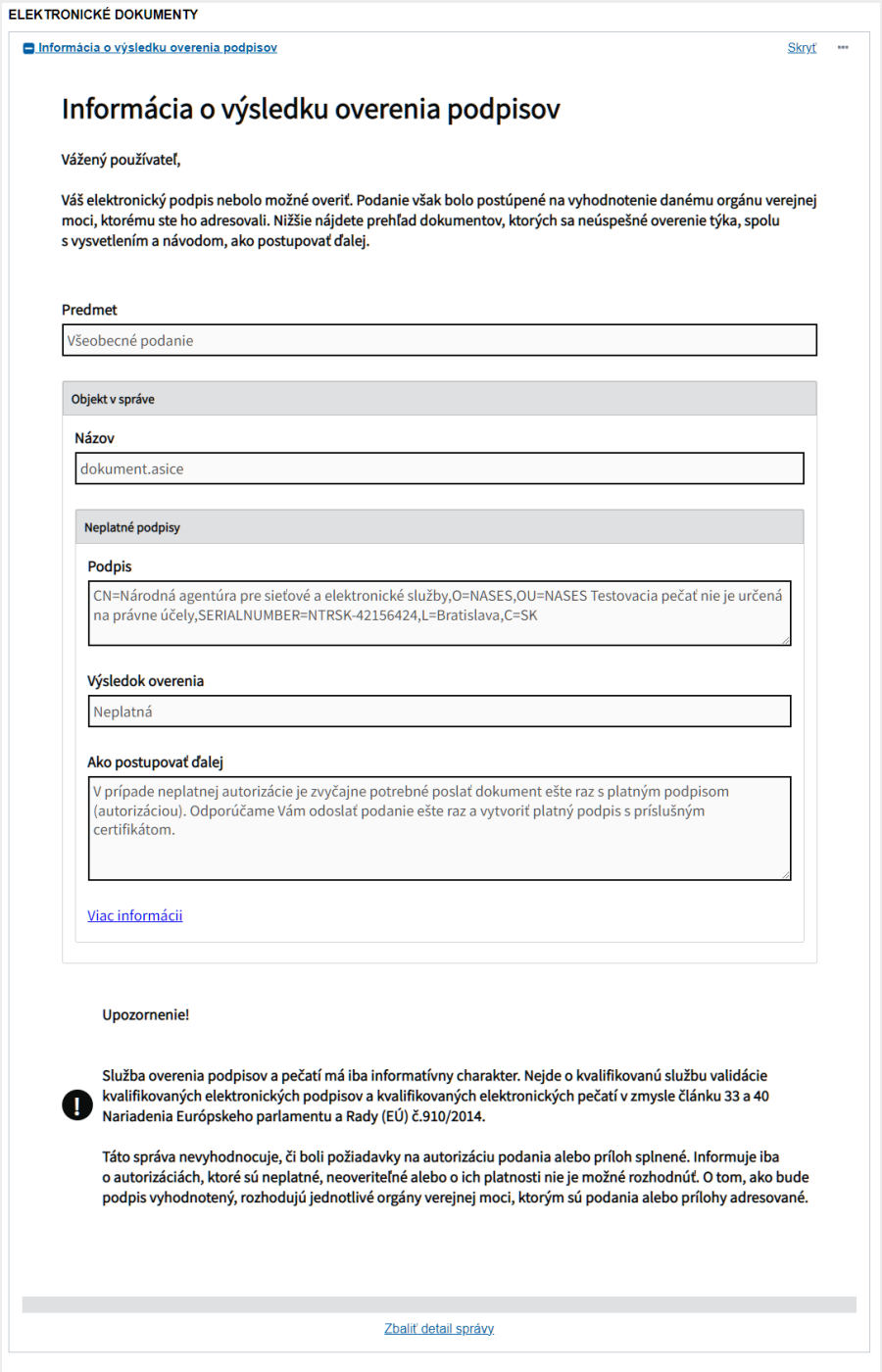
- chýbajúcu autorizáciu (podpis alebo pečať),
- ak dané podanie vyžaduje autorizáciu kvalifikovaným elektronickým podpisom a používateľ použije iba „uznaný spôsob autorizácie“ resp. zdokonalený podpis založený na kvalifikovanom certifikáte,
- chýbajúci podpis druhej osoby (konateľ/štatutár), ak podanie majú podpísať dve a viac osôb,
- a podobne.

Správa nie je zasielaná ani v prípade, ak podanie je adresované orgánu verejnej moci, ktorý nevyužíva centrálnu elektronickú podateľňu ako svoju podateľňu.
V takom prípade by mal "Upozornenie na neplatnosť zaslaného podpisu" zasielať daný orgán verejnej moci zo svojho informačného systému.

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

2. Obsah správy „Upozornenie na neplatnosť zaslaného podpisu“

Ako je uvedené v úvode, odosielateľovi, ktorý odošle podanie, kde niektorý z podpisov je vyhodnotený ako neplatný alebo neoveriteľný, dostane do svojej schránky správu „Upozornenie na neplatnosť zaslaného podpisu“[i]. Zobrazenie takejto správy môže vyzerať napríklad takto:



Obrázok 1: Príklad zobrazenia správy „Upozornenie na neplatnosť zaslaného podpisu“.

Upozornenie na neplatnosť zaslaného podpisu obsahuje nasledujúce údaje:

- **Predmet** – obsahuje predmet elektronického podania, ku ktorému je Upozornenie na neplatnosť zaslaného podpisu zaslané
- Skupina „**Objekt v správe**“ – obsahuje informácie o jednotlivých objektoch (hlavný formulár alebo prílohy) z elektronického podania, v ktorých boli zistené problémy s podpismi. Objekty, v ktorých neboli zistené problémy (ako aj objekty, ktoré nie sú podpísané) v tejto správe nie sú. Skupina obsahuje informácie o problematických podpisoch, ktoré môžu pomôcť identifikovať samotný objekt, podpis, alebo problém, ktorý s podpisom bol identifikovaný:
    - **Názov** – obsahuje názov súboru v doručenej správe (názov súboru vo formáte ASiC, PDF , XAdES_ZEP, ZEPf, typicky s príponami .asice, asics, .sce, .scs, .pdf, .xzep, .zepx, .zep). Tento údaj umožňuje porozumieť, ktorý z doručených súborov bol problematicky podpísaný.
    - Skupina „**Neplatné podpisy**“ – opakovateľná sekcia, ktorá obsahuje informácie o problematických podpisoch. Opäť obsahuje len informácie o problematických podpisoch. (Teda podpisy, ktoré boli vyhodnotené ako platné sa v tejto správe nezobrazujú.)
      Obsahuje súčasti:
        - **Podpis** – obsahuje informácie o osobe, ktorej bol certifikát, ktorým bol vytvorený problematický podpis, vydaný. Informácie sú uvedené tak, ako sú zapísané v certifikáte podpisovateľa. Jednotlivé údaje sú uvádzané v nasledovnej štruktúre, pričom poradie sa môže líšiť:

          „CN“ – plné meno osoby alebo názov organizácie resp. obvyklé označenie; v prípade mandátneho certifikátu obsahuje údaj podľa schémy dohľadu NBÚ (text „OPRÁVNENIE“ alebo „MANDÁT“ a príslušné číslo oprávnenia podľa zoznamu oprávnení zverejňovaného Národným bezpečnostným úradom)

          „G“ (GIVENNAME) – krstné meno v prípade fyzickej osoby,

          „S“ (SURNAME) – priezvisko v prípade fyzickej osoby,

          „O“ (Organization) – názov organizácie v prípade pečate alebo mandátneho certifikátu; v prípade mandátneho certifikátu môže obsahovať text „MANDANT“ pri údaji o mandantovi,

          „SERIALNUMBER“ – rodné číslo alebo iný identifikátor fyzickej osoby alebo právnickej osoby (v štruktúre podľa schémy dohľadu NBÚ); v prípade mandátneho certifikátu obsahuje text „MANDANT“ pri údaji o mandantovi

          „2.5.4.97“ alebo „OrganizationIdentifier“ – identifikátor právnickej osoby, ak nie je uvedený v SERIALNUMBER,

          „T“ – názov funkcie resp. oprávnenia (nepovinné),

          „STREET“ – ulica bydliska alebo sídla (nepovinné),

          „L“ – mesto bydliska alebo sídla (nepovinné),

          „C“ – štát bydliska alebo sídla (nepovinné)

          Napríklad:

          STREET=Pekná ulica 1234/11, GIVENNAME=Jozef, CN=Jozef Mrkvička, SERIALNUMBER=PNOSK-1234567890, SURNAME=Mrkvička,L=Bratislava,C=SK

- **Výsledok overenia** – obsahuje výsledok overenia podpisu (podľa zoznamu uvedeného nižšie)
- **Ako postupovať ďalej** – obsahuje textový návod pre používateľa, ako postupovať pre nápravu problému.
- Odkaz - na stránku s podrobnejšími informáciami o probléme a jeho prípadných riešeniach (nepovinné, pre niektoré typy problémov nemusí byť uvedený).

3. Možné výsledky overenia podpisov a postup pre nápravu

V poli **Výsledok overenia** sa môže objaviť niektorá z možností: neplatná, neoveriteľná, nie je možné rozhodnúť. Postup pre nápravu je závislý na zdrojovom probléme a je bližšie popísaný v poli „**Ako postupovať ďalej**“.

K jednotlivým výsledkom overenia podpisov uvádzame vysvetlenie:

- „**neplatná**“ – tento výsledok je vrátený v prípade, ak sa jedná o neplatný podpis. Zvyčajne je to spôsobené exspirovaným alebo revokovaným (zrušeným) certifikátom, ale môže to byť aj z dôvodu porušenia integrity podpisu. Postup pre nápravu je závislý na zdrojovom probléme a je bližšie popísaný v poli „**Ako postupovať ďalej**“. V tomto prípade je opravou zvyčajne vytvorenie nového podpisu s platným kvalifikovaným certifikátom.

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

  a) v prípade, ak ide o exspirovaný alebo zrušený certifikát v čase overovania platnosti ním vytvoreného podpisu a absentuje dôkaz o existencii podpisu v čase pred alebo po exspirácii certifikátu potrebný pre určenie platnosti (podpis teda obvykle nemá pripojenú kvalifikovanú časovú pečiatku).

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

  Opravou je zvyčajne vytvorenie nového podpisu s platným certifikátom a pripojenie kvalifikovanej časovej pečiatky, ktorá preukazuje čas vytvorenia podpisu, resp. preukazuje čas, v ktorom podpis vytvorený príslušným certifikátom už existoval. Overovanie podpisu potom bude prevedené k času z časovej pečiatky a teda prípadná expirácia alebo zrušenie (revokácia) podpisového certifikátu po tomto čase nespôsobí neplatnosť alebo nemožnosť overenia podpisu.

- „**neoveriteľná**“ - tento výsledok je obvykle možné interpretovať ako neplatný podpis. Vzniká napríklad v prípade:
  - chybného formátu podpisu alebo poškodeného podpisu,
  - nepodporovaného algoritmu podpisu (napr. ECDSA, RSA-PSS, SHA3),

pričom v takých prípadoch je vhodné vykonať overenie s využitím inej aplikácie pre validáciu podpisov,

- v prípade formátu ASiC (s podpisom CAdES), ak ide o exspirovaný certifikát a od jeho vydavateľa už nie je možné získať dôkaz (CRL) o platnosti tohto certifikátu v čase rozhodnom pre overovanie podpisu.

Oprava na strane používateľa je v tomto prípade obvykle možná novým vytvorením podpisu v inej podpisovej aplikácii alebo rovnaká ako v predchádzajúcom prípade.

[i] Ide o správu technického typu SIGN_VERIFY_RESULT_INFORMATION