

# Návod k používaniu správy Upozornenie na neplatnosť zaslaného podpisu

## Obsah

Návod k používaniu správy Upozornenie na neplatnosť zaslaného podpisu .....	1
1. Úvod .....	1
2. Obsah správy „Upozornenie na neplatnosť zaslaného podpisu“ .....	3
3. Možné výsledky overenia podpisov a postup pre nápravu .....	5

## 1. Úvod

Odosielateľ elektronického podania, v ktorom je niektorý z podpisov vyhodnotený ako „neplatný“, „neoveriteľný“ alebo „nie je možné rozhodnúť“, dostáva po odoslaní podania 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 alebo neoveriteľnosť 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 elektronicкую 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.

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.

## 2. Obsah správy „Upozornenie na neplatnosť zaslaného podpisu“

Odosielateľovi, ktorý odošle podanie, v ktorom je niektorý z podpisov vyhodnotený ako neplatný alebo neoveriteľný, dostane do svojej schránky správu „Upozornenie na neplatnosť zaslaného podpisu“<sup>41</sup>. Zobrazenie takejto správy môže vyzeráť napríklad takto:

The screenshot shows an email interface with the following content:

**ELEKTRONICKÉ DOKUMENTY**

[Informácia o výsledku overenia podpisov](#) Skrýť

### Informácia o výsledku overenia podpisov

Vážený používateľ,

Váš elektronický podpis nebolo možné overiť. Podanie však bolo postúpené na vyhodnotenie danému orgánu verejnej moci, ktorému ste ho adresovali. Nižšie nájdete prehľad dokumentov, ktorých sa neúspešné overenie týka, spolu s vysvetlením a návodom, ako postupovať ďalej.

**Predmet**  
Všeobecné podanie

**Objekt v správe**

**Názov**  
dokument.asice

**Neplatné podpisy**

**Podpis**  
CN=Národná agentúra pre sieťové a elektronické služby,O=NASES,OU=NASES Testovacia pečať nie je určená na právne účely,SERIALNUMBER=NTRSK-42156424,L=Bratislava,C=SK

**Výsledok overenia**  
Neplatná

**Ako postupovať ďalej**  
V prípade neplatnej autorizácie je zvyčajne potrebné poslať dokument ešte raz s platným podpisom (autorizáciou). Odporúčame Vám odoslať podanie ešte raz a vytvoriť platný podpis s príslušným certifikátom.

[Viac informácií](#)

**Upozornenie!**

Služba overenia podpisov a pečatí má iba informatívny charakter. Nejde o kvalifikovanú službu validácie kvalifikovaných elektronických podpisov a kvalifikovaných elektronických pečatí v zmysle článku 33 a 40 Nariadenia Európskeho parlamentu a Rady (EÚ) č.910/2014.

Táto správa nevyhodnocuje, či boli 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 podpis vyhodnotený, rozhodujú jednotlivé orgány verejnej moci, ktorým sú podania alebo prílohy adresované.

[Zbaliť detail správy](#)

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
- Sekcia „**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 uvádzané nie sú. Sekcia obsahuje informácie o problematických podpisoch, ktoré môžu pomôcť identifikovať samotný objekt, podpis, alebo problém, ktorý 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 odoslaných 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 vydaný certifikát, ktorým bol vytvorený problematický podpis. 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 údajoch 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 údajoch 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. V tomto prípade je opravou zvyčajne vytvorenie nového podpisu s platným kvalifikovaným certifikátom.
- „**nie je možné rozhodnúť**“ - tento výsledok je obvykle možné interpretovať ako neplatný podpis. Služba centrálnej elektronickej podateľne 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 expirácii certifikátu potrebný pre určenie platnosti (podpis teda obvykle nemá pripojenú platnú kvalifikovanú časovú pečiatku vyhotovenú službou zapísanou v dôveryhodnom zozname členských štátov EÚ).
  - 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. zatiaľ nepodporované ECDSA, RSA-PSS, SHA3), pričom v takých prípadoch je na strane

---

prijímateľa podania vhodné vykonať overenie podpisov s využitím inej služby pre validáciu podpisov, nakoľko akceptovanie podpisov vytvorených s uvedenými algoritmami je v zmysle zákona o dôveryhodných službách povinné,

- 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.

---

<sup>i</sup> Ide o správu technického typu SIGN\_VERIFY\_RESULT\_INFORMATION