VÚ 8116 Trenčín
ODBOR INFORMAČNEJ BEZPEČNOSTI

Použitie zaručeného elektronického podpisu v praxi

(Pomôcka pre používateľov)

2013 VÚ 8116 Trenčín

Vypracoval: Skupina bezpečnosti technických prostriedkov
Centrum informačnej bezpečnosti Trenčín
Spracované na základe dokumentácie Certifikačnej autority MOSR a používateľskej príručky QSign 3.4.1

Táto brožúra je určená výhradne pre potreby Ozbrojených síl Slovenskej republiky.

Dokument neprešiel jazykovou úpravou.

Pripomienky k tomuto dokumentu môžete posielať na adresu: pki@mil.sk

OBSAH

1. Základný opis aplikácie

Základnou podmienkou platnosti dokumentu podpísaného zaručeným elektronickým podpisom (ZEP) je použitie bezpečnej aplikácie určenej na tvorbu a overenie zaručeného elektronického podpisu, certifikovanej Národným bezpečnostným úradom SR. Takouto aplikáciou je **QSign**.

Obrázok 1 Štart aplikácie Qsign

Aplikácia QSIGN je primárne určená na podpisovanie a overovanie dokumentov pomocou zaručeného elektronického podpisu v zmysle legislatívy Slovenskej republiky. Je určená pre operačný systém Microsoft Windows ako univerzálny prostriedok na podpisovanie dokumentov. Umožňuje zabezpečiť a overiť autenticitu a integritu elektronických dokumentov.

Základom integrity a autenticity elektronických dokumentov je zabezpečiť, aby údaje, ktoré sú zobrazené na obrazovke, boli zhodné s tými, ktoré používateľ svojim podpisom potvrdzuje („What you see is what you sign“ „Podpisuješ to čo vidíš“) a navyše dokument v sebe neskrýval ďalšie údaje, o ktorých podpisovateľ nevie, alebo ich môže ľahko prehliadnuť („What you see is what you trust“- „Čo vidíš tomu môžeš veriť“).

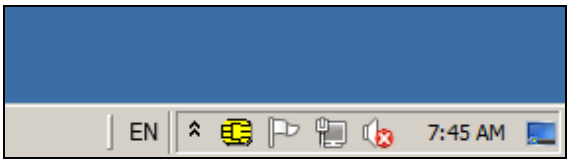
Tento dokument slúži iba ako pomôcka pre použitie aplikácie QSign na okamžité podpísanie dokumentu resp. pre overenie podpisu. Podrobné informácie o používaní aplikácie sú uvedené v používateľskej príručke, ktorá je umiestnená v ponuke **“ŠTART- PROGRAMY-ARDACO-QSIGN-QSIGN DOKUMENTÁCIA“**

Návod k používaniu aplikácie QSign je implementovaný aj v aplikácii pod názvom **Pomocník** a je dostupný z menu ovládania. Okrem podrobného popisu postupu inštalácie a ovládania vysvetľuje aj základné pojmy z oblasti zaručeného elektronického podpisu.

2. Prihlásenie užívateľa do aplikácie Q-Sign

Pre podpisovanie dokumentov si aplikácia vyžaduje prihlásenie používateľa.

1. Pred procesom prihlásenia je potrebné sa presvedčiť, či je čipová karta s kvalifikovaným certifikátom pre ZEP korektne vložená do čítacieho zariadenia (čítačka čipových kariet)

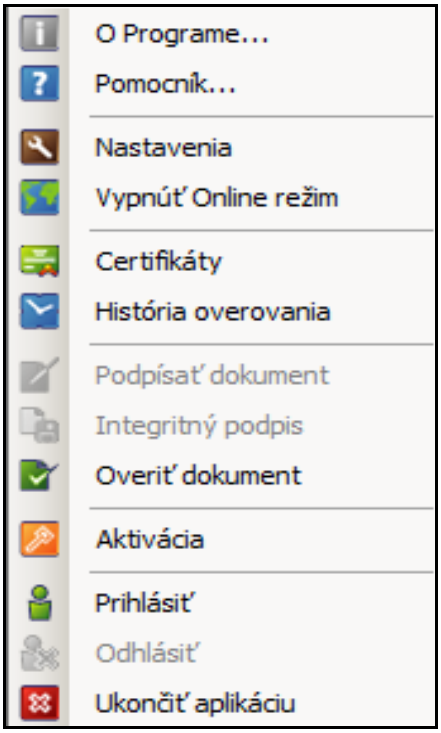


Obrázok 2 Korektné pripojenie čítačky a čipovej karty

2. Prihlasovacie okno je dostupné cez ovládacie menu aplikácie. Pravým tlačidlom myši kliknite na ikonu **Q** na paneli úloh

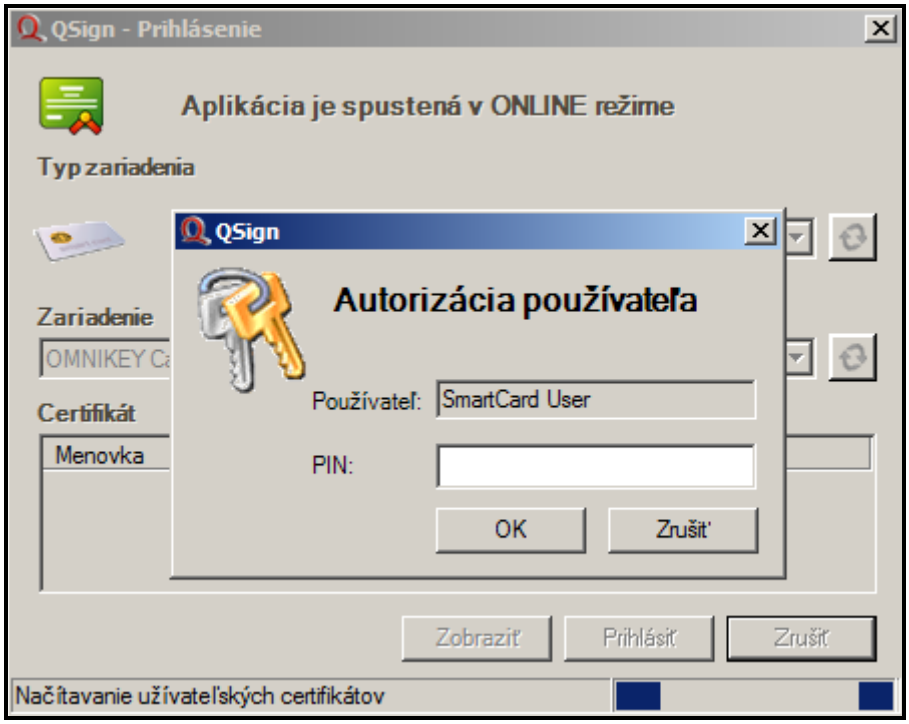
Obrázok 3 Aplikácia Qsign v oznamovacej oblasti

3. Zo zobrazenej ponuky menu **QSign** kliknite na voľbu **Prihlásiť**



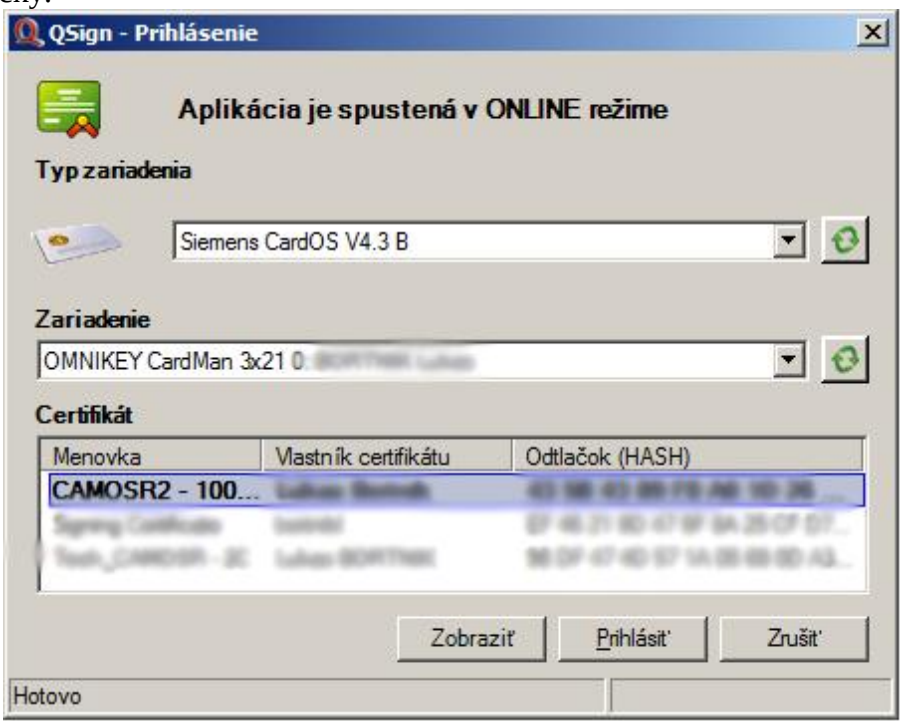
Obrázok 4 Menu aplikácie

4. Po zobrazení prihlasovacieho okna a načítaní pripojených zariadení je potrebné zadať PIN k čipovej karte.



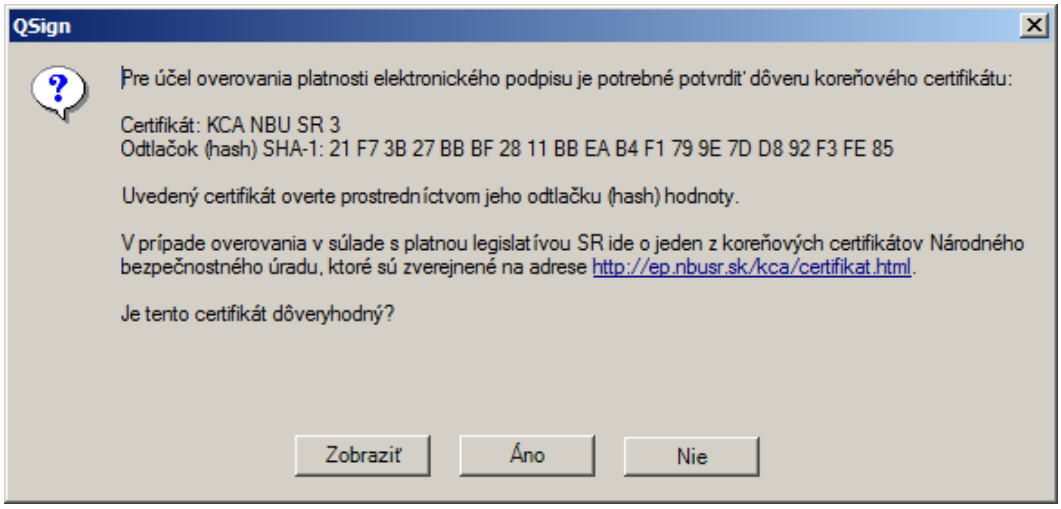
Obrázok 5 Autorizácia používateľa

5. Následne sa vo výberovom okne dialógu „**Certifikáty**“ zobrazia všetky certifikáty nainštalované na vybranom zariadení, ktorými je možné sa prihlásiť. V prípade, že je pripojené práve jedno zariadenie, po Vašej autorizácii sa dostupné certifikáty načítajú automaticky.



Obrázok 6 Prihlasovanie používateľ

6. Po označení požadovaného certifikátu sa môžete prihlásiť stlačením tlačidla **Prihlásiť** a potvrdiť dôveryhodnosť Certifikátu KCA NBU SR 3:



Obrázok 4 Kontrola dôveryhodnosti certifikátu KCA NBU

3. Základné funkcie

Medzi najdôležitejšie funkcie, ktoré aplikácia poskytuje používateľovi patrí:

1. Podpisovanie dokumentov

Zahŕňa jednoduché podpisovanie dokumentov, viacnásobné podpisovanie, uzatváranie podpisu alebo archívne podpisovanie s nastaveniami, ktoré používateľovi umožňujú vytvoriť podpis presne podľa jeho požiadaviek.

2. Overovanie podpisov

Overovanie ľubovoľného externého elektronického podpisu v medzinárodnom formáte ETSI (CMS - PKCS7), alebo uloženého v ZEP (ZIP) type súboru.

3. História overovania

Zjednodušuje používateľovi spravovanie overovaných dokumentov. Jednotlivé podpisy je možné dopĺňať o časové pečiatky alebo na archívne podpisy. Umožňuje overovať podpisy bez časovej pečiatky.

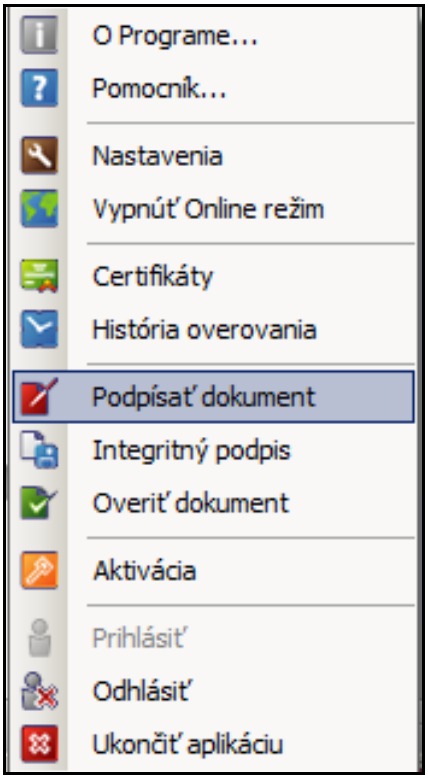
3.1. Podpisovanie dokumentov

Aplikácia umožňuje podpísanie ľubovoľného dokumentu na Vašom počítači. Pre inicializovanie podpisovania máte na výber nasledujúce možnosti:

- Podpisovanie pomocou ovládacieho menu aplikácie
- Podpisovanie pomocou kontextového menu
- Podpisovanie pomocou virtuálnej tlačiarne

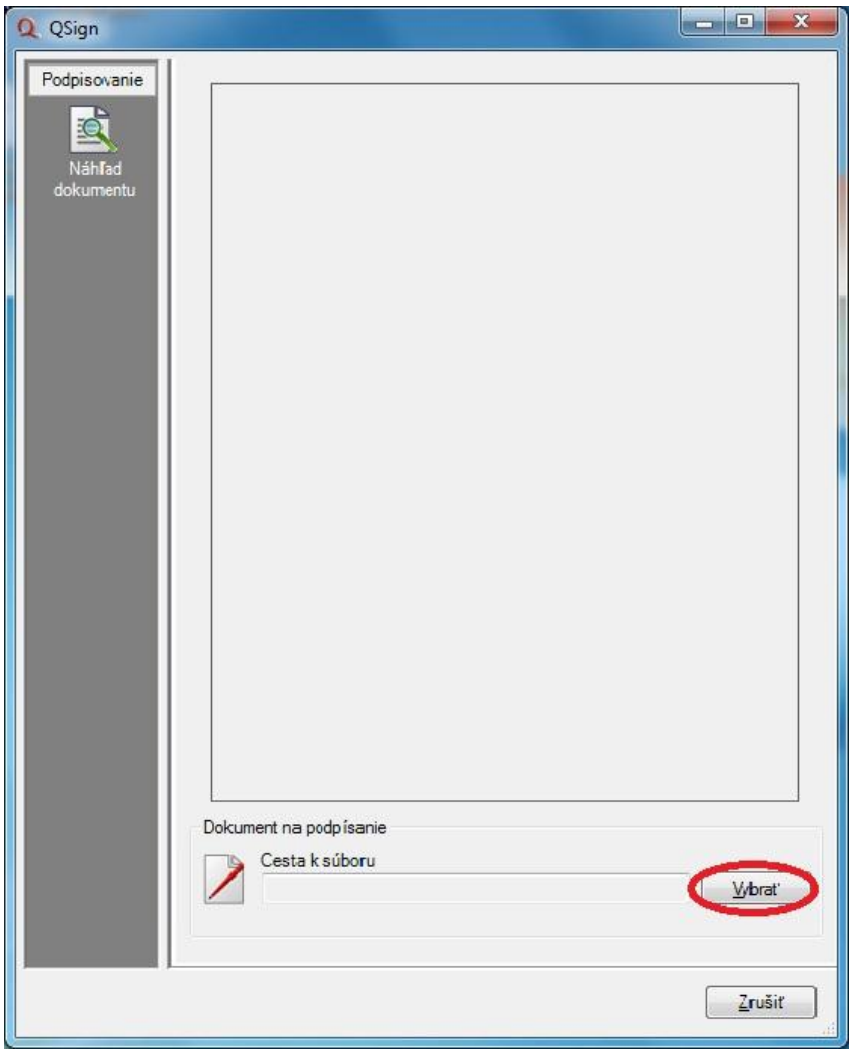
3.1.1. Podpisovanie pomocou ovládacieho menu aplikácie

1. Otvorte ovládacie menu aplikácie
2. Vyberte položku **Podpísať dokument**



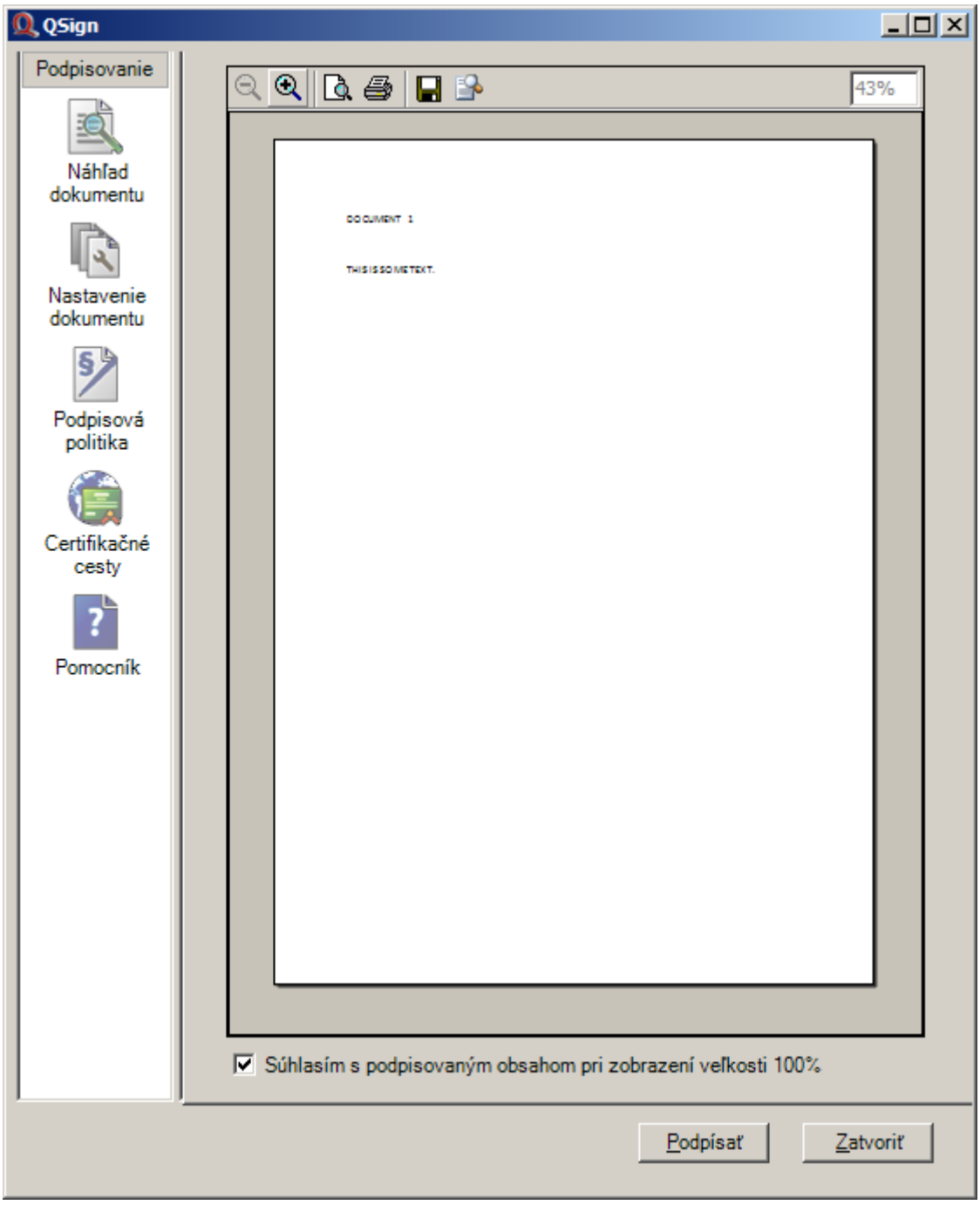
Obrázok 8 Podpis dokumentu z menu aplikácie

3. V otvorenom okne aplikácie stlačte tlačidlo **Vybrať** a zadajte cestu k podpisovanému dokumentu.



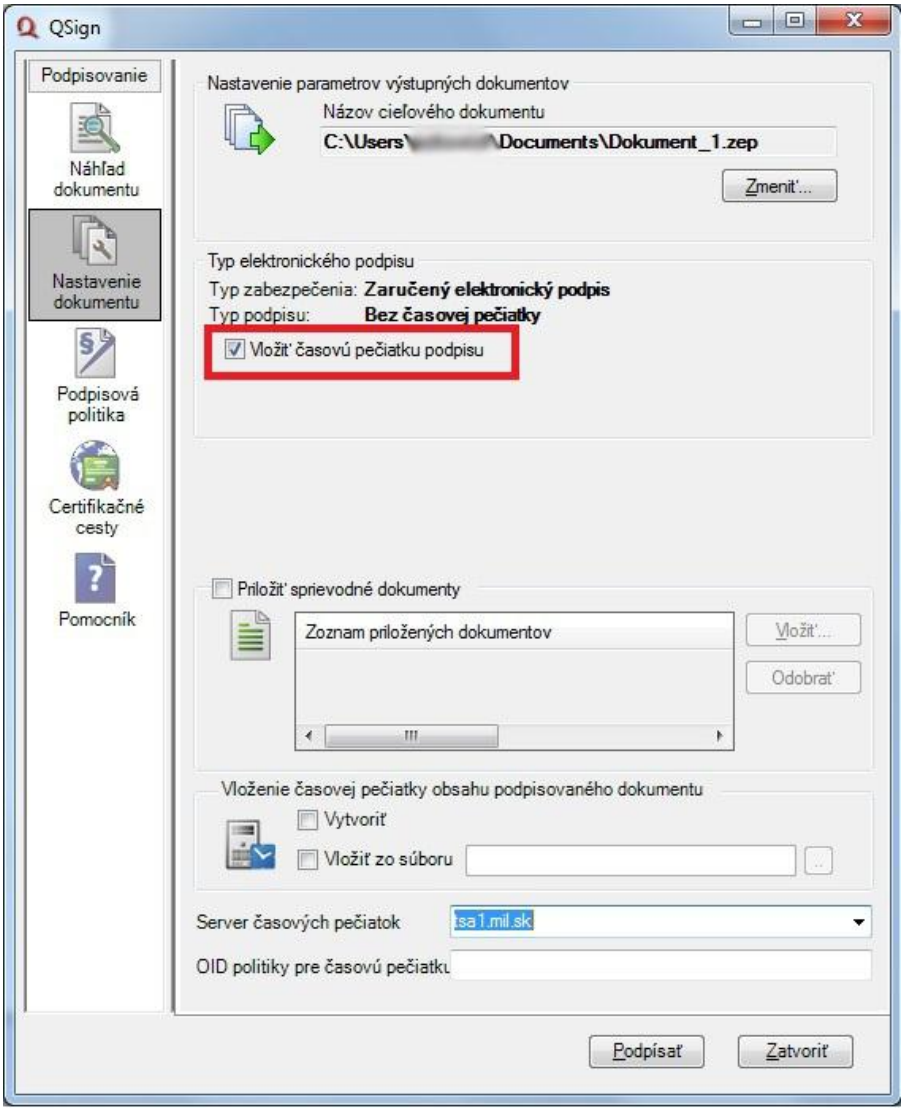
Obrázok 9 Súbor na podpis

4. Zobrazí sa podpisové okno – Náhľad dokumentu. Tlačidlo **Podpísať** nie je prístupné, pred podpisom je potrebné zväčšiť a skontrolovať obsah dokumentu. Po skontrolovaní dokumentu pripraveného na Váš podpis kliknite na lupu pre zmenšenie náhľadu



Obrázok 10 Náhľad dokumentu

5. Kliknite na **Nastavenie dokumentu** a zašktnite **Vložiť časovú pečiatku**



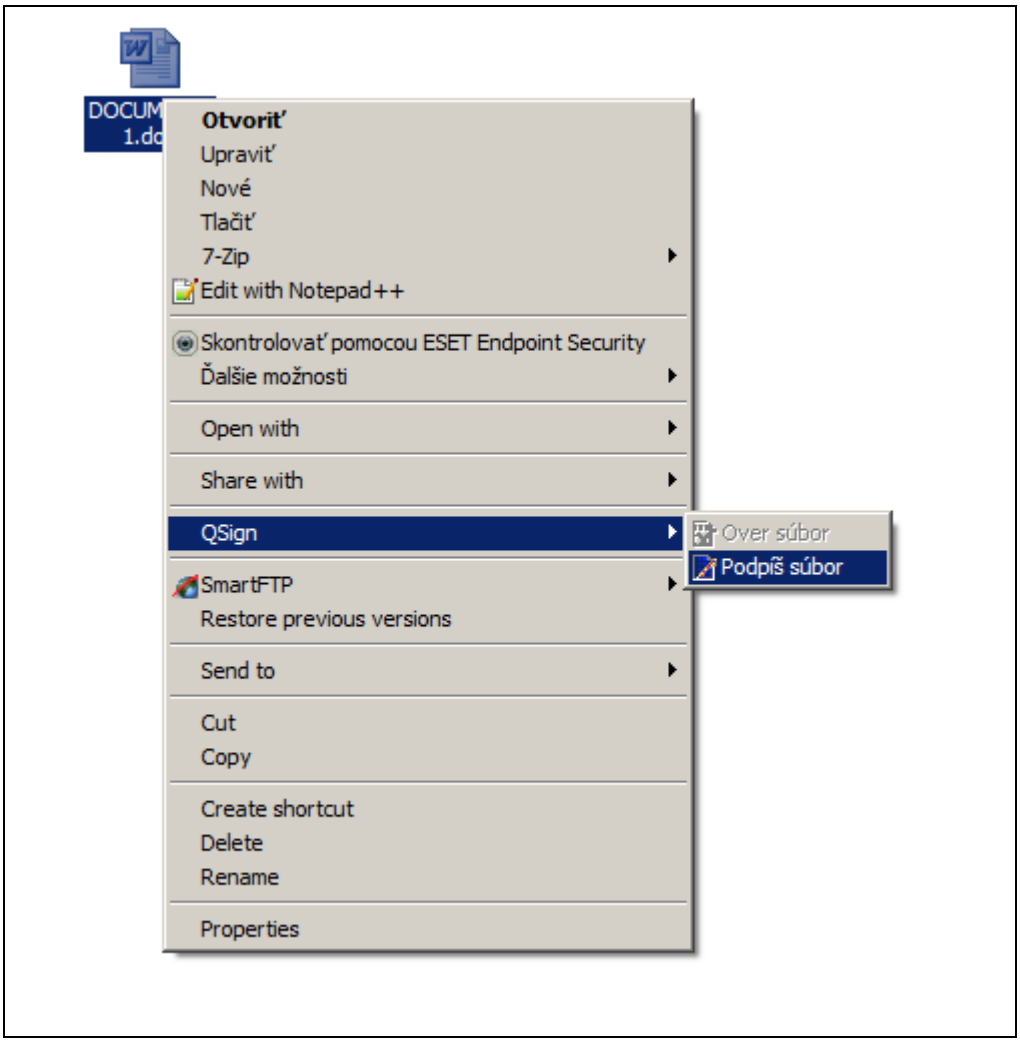
Obrázok 11 Nastavenie časovej pečiatky

6. Stlačením tlačidla **Podpísať** dokument podpíšete

3.1.2. Podpisovanie pomocou kontextového menu

Operácia podpisovanie dokumentov vyžaduje prihlásenie používateľa

1. Kliknúť pravým tlačidlom myši nad dokumentom zobrazíte menu
2. V menu vyberte položku **QSign - Podpíš súbor**



Obrázok 12 Podpis dokumentu z kontextoveho menu

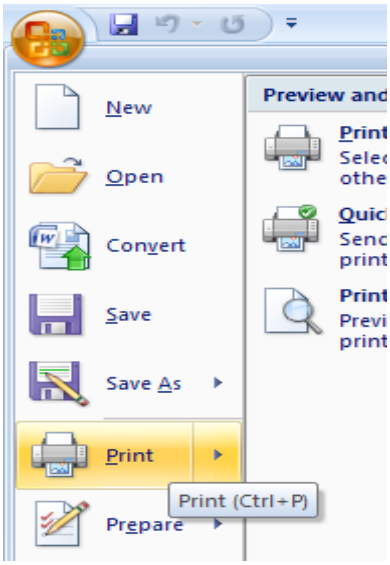
3. V prípade, že ste sa pred podpísaním dokumentu neprihlásili do QSign, aplikácia Vám oznámi, že nie ste prihlásený.
4. Po Vašej autorizácii sa načítajú dostupné certifikáty. Po označení požadovaného certifikátu sa môžete prihlásiť stlačením tlačidla **Prihlásiť.**
5. Ďalší postup je rovnaký ako v prípade podpisu prostredníctvom menu aplikácie.

3.1.3. Podpisovanie pomocou virtuálnej tlačiarne

Táto voľba je dostupná z ľubovoľného programu nainštalovaného na vašom počítači, ktorý umožňuje tlač dokumentov. Pred tlačou je potrebné vybrať virtuálnu *Tlačiareň pre ZEP* a nechať dokument vytlačiť do prostredia Aplikácie pre ZEP.

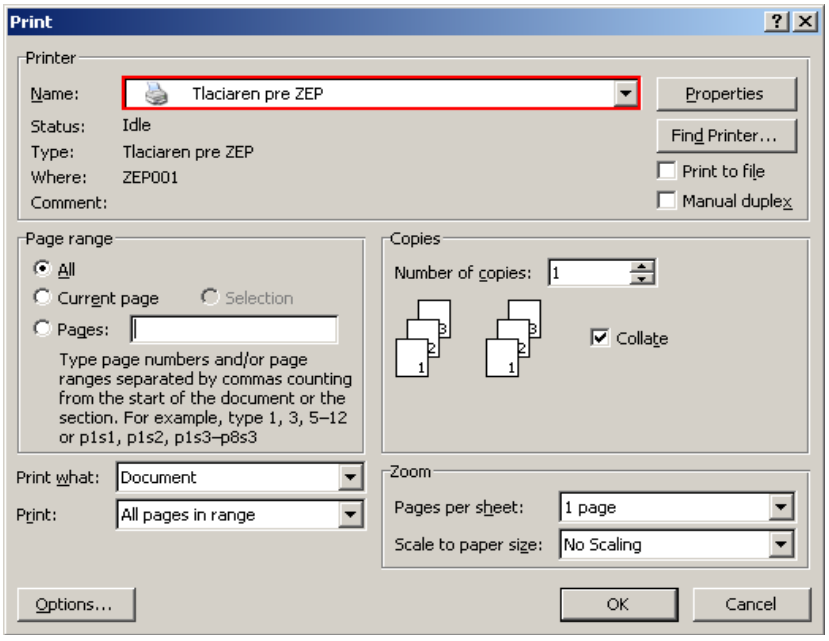
1. Otvorte dokument na podpísanie v aplikácií MS Word alebo iný.

2. Vyberte položku menu *Súbor* > *Tlač*.



Obrázok 13 Tlač dokumentu

3. Zo zoznamu tlačiarní vyberte *Tlačiareň pre ZEP*.



Obrázok 14 Podpis dokumentu cez tlačiareň ZEP

3.2. Viacnásobný podpis

3.2.1. Použitie viacnásobného podpisu

V praxi sa vyskytujú prípady, v ktorých je potrebné dokument podpísať viacerými osobami, napr. dokument podliehajúci schvaľovaciemu procesu v štruktúre organizácie alebo zmluva medzi viacerými zmluvnými stranami. V týchto prípadoch je vhodné využiť pri podpisovaní elektronického dokumentu možnosť vytvorenia viacnásobného podpisu.

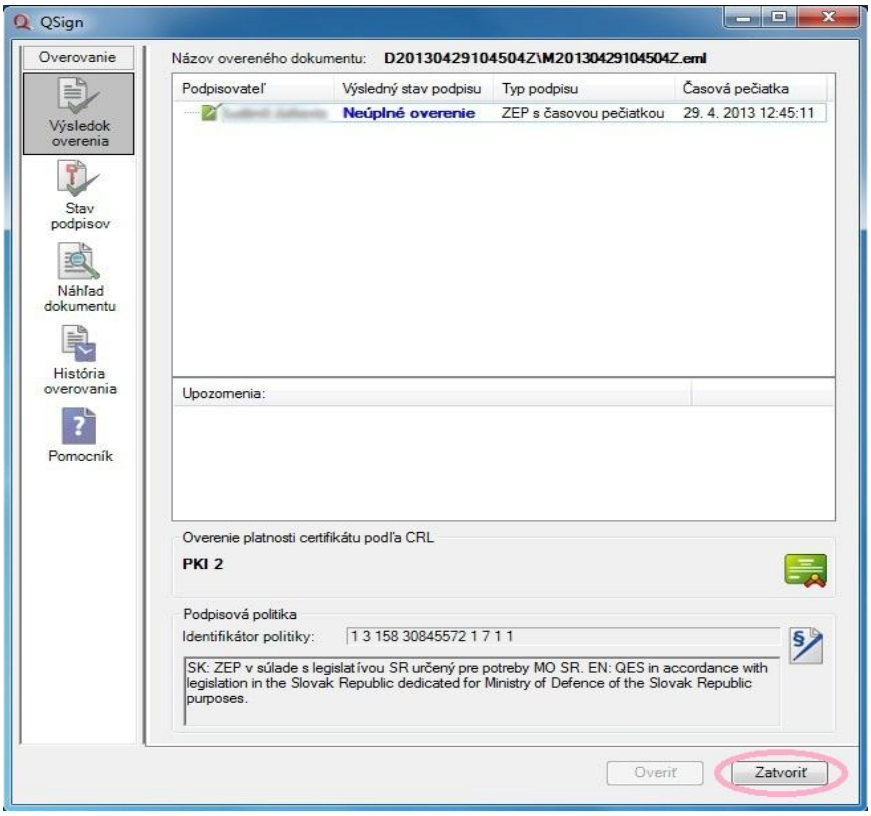
3.2.2. Ako vytvoriť viacnásobný podpis

Viacnásobný podpis sa vytvorí podpísaním súboru ZEP s jednoduchým podpisom. Podpíše sa tak dokument, ktorého podpis je uložený v súbore ZEP a vznikne ďalší jednoduchý podpis. Ten sa uloží spolu s predchádzajúcim podpisom do súboru ZEP. Viacnásobný podpis je teda tvorený viacerými jednoduchými podpismi v súbore ZEP.

Na vytvorenie viacnásobného podpisu nemôžete použiť podpísanie pomocou virtuálnej tlačiarne.

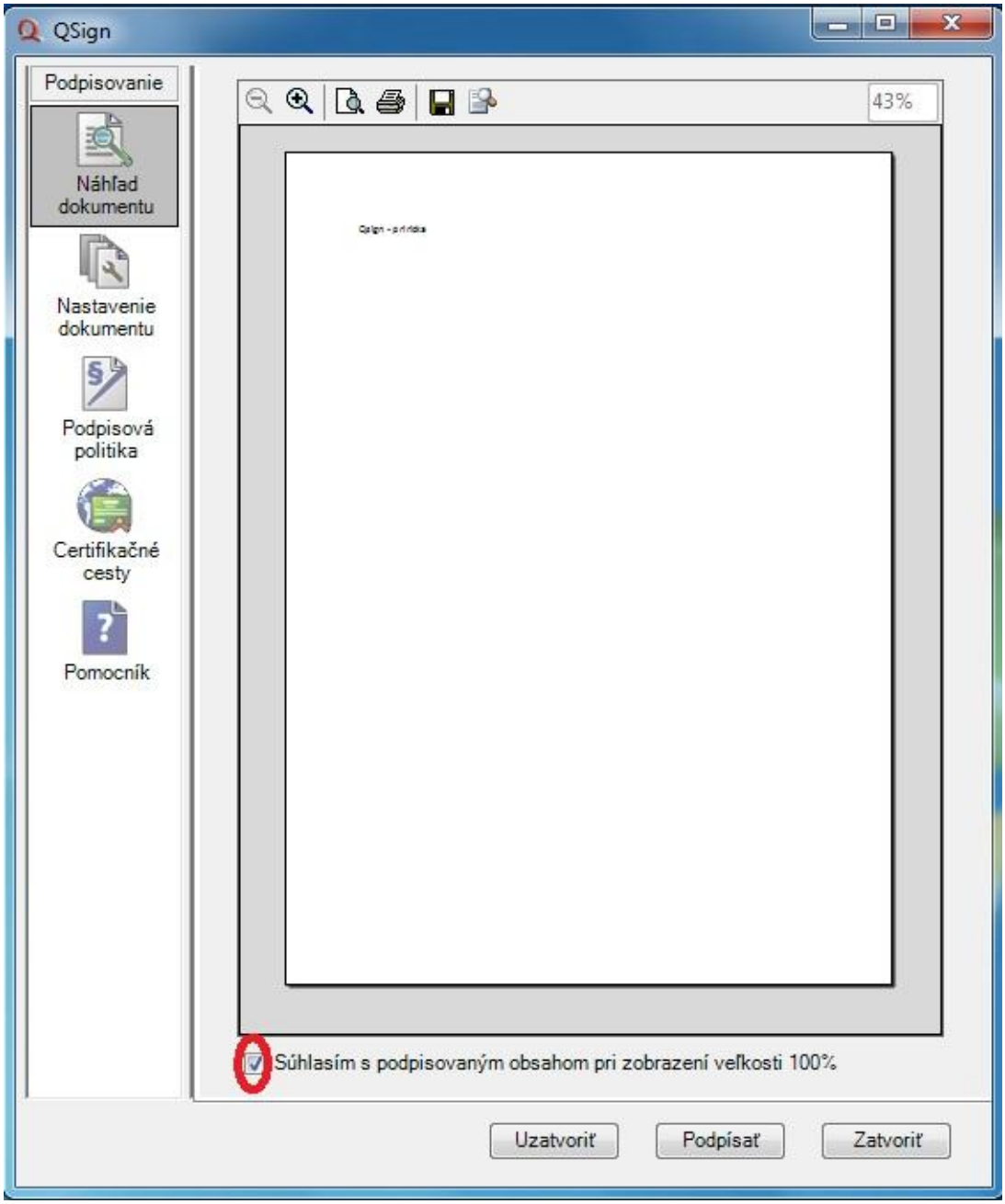
Môžete použiť kontextové menu po stlačení pravého tlačidla myši nad už existujúcim súborom ZEP s jednoduchým podpisom. Prípadne cez ovládacie menu aplikácie, voľbou **Podpísať dokument**.

1. Pred podpísaním už podpísaného dokumentu aplikácia QSign ponúkne možnosť overenia už existujúceho podpisu. V prípade voľby **Áno** sa výsledok overenia zobrazí v overovacom okne. V prípade voľby **Nie** pokračujte krokom **3.**



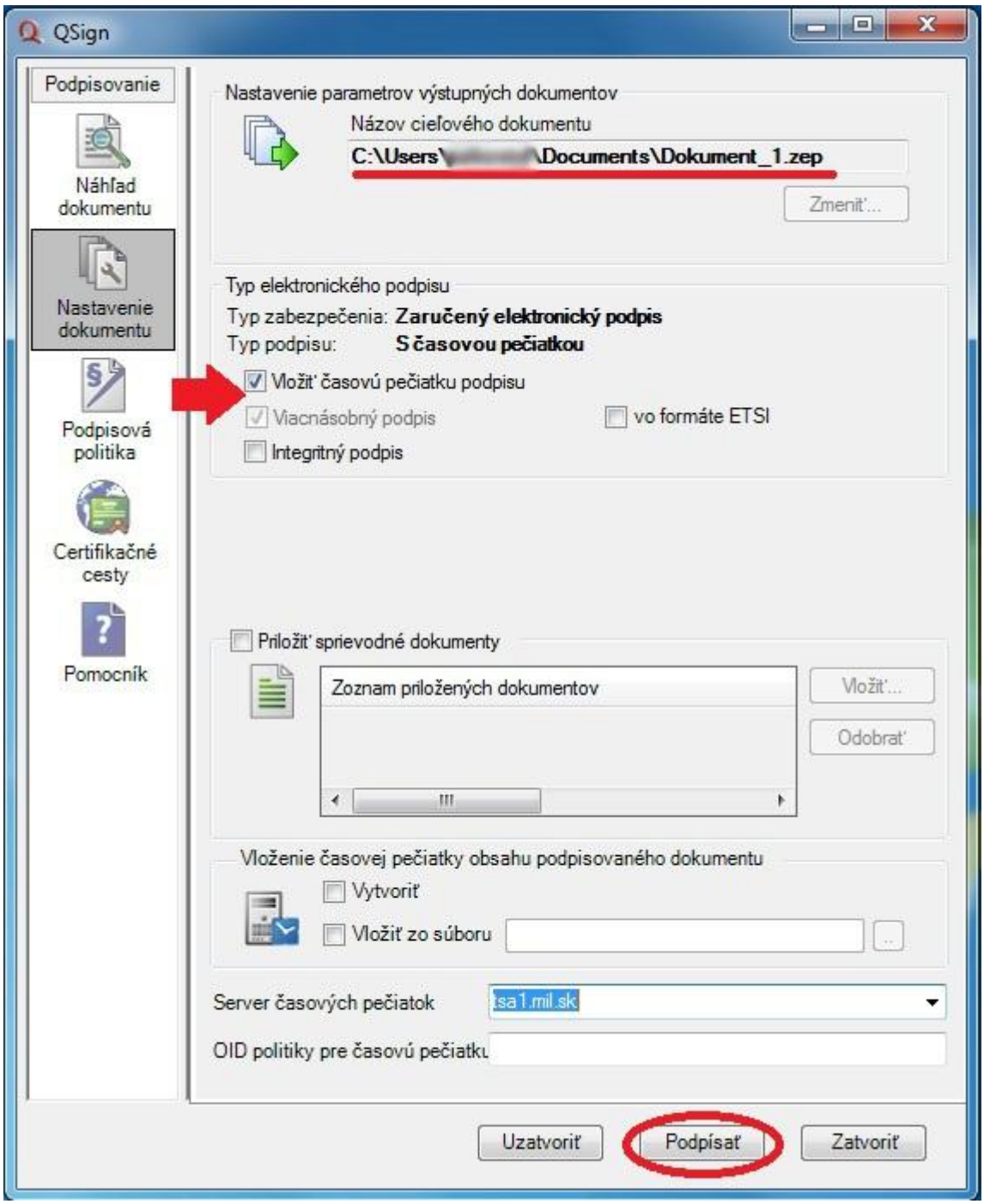
Obrázok 15 Výsledok overenia elektronického podpisu

2. Pre zatvorenie overovacieho okna stlačte tlačidlo **Zatvoriť**
3. Zobrazí sa podpisové okno – Náhľad dokumentu. Tlačidlo **Podpísať** nie je prístupné, pred podpisom je potrebné zväčšiť a skontrolovať obsah dokumentu. Po skontrolovaní dokumentu pripraveného na Váš podpis kliknite na lupu pre zmenšenie náhľadu



Obrázok 16 Kontrola a potvrdenie obsahu dokumentu

4. V časti **Nastavenie dokumentu** sa môžete presvedčiť(viď šípka), či ide o viacnásobný podpis, a ku ktorému dokumentu pripájate časovú pečiatku (názov cieľového dokumentu).



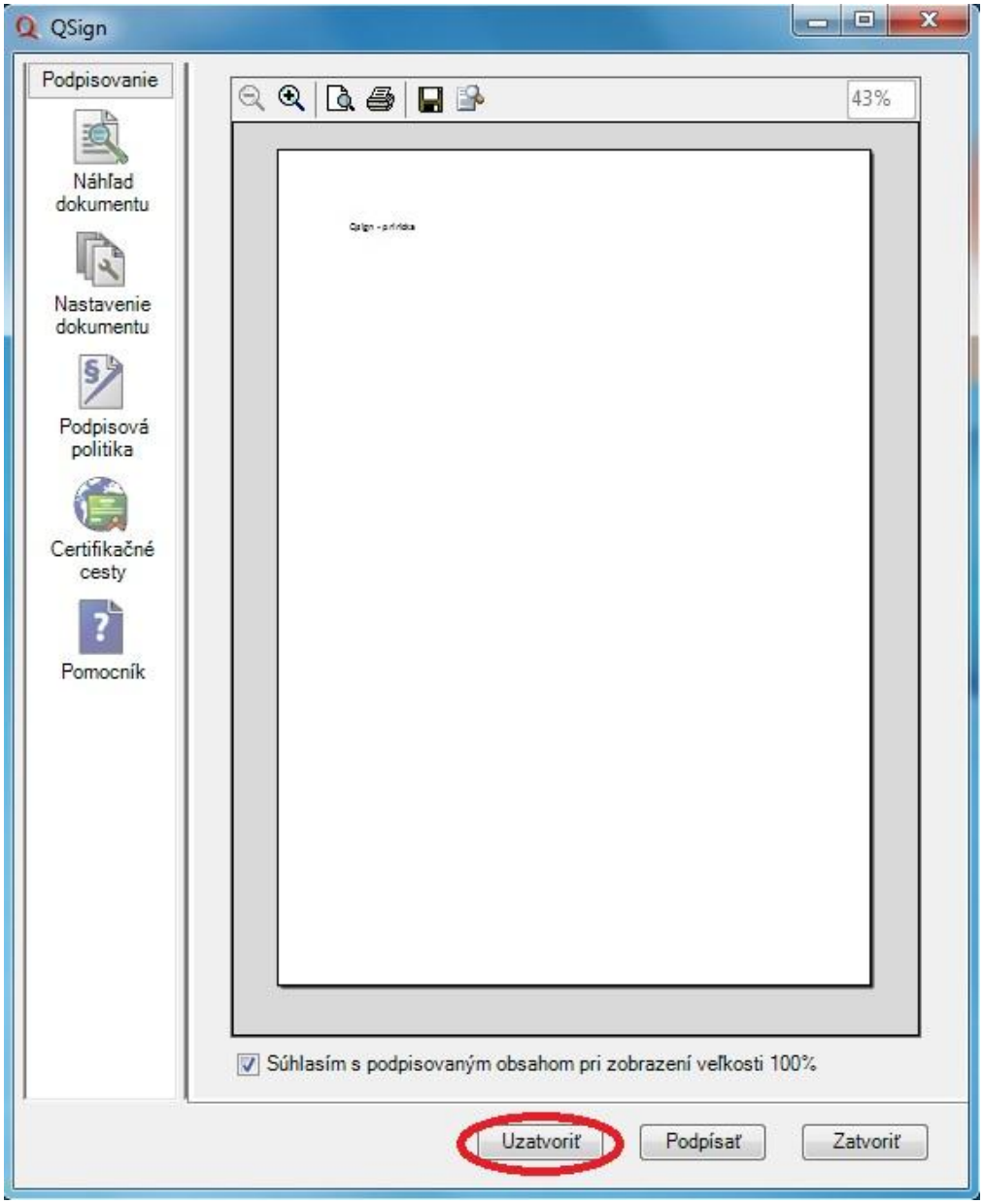
Obrázok 17 Podpísanie dokumentu

Stlačením tlačidla **Podpísať** dokument podpíšete

3.3. Ako uzatvoriť podpis

Viacnásobný, ale aj jednoduchý podpis je možné uzatvoriť. To znamená, že sa nepodpisuje dokument, ale všetky jednoduché a uzatváracie podpisy v archíve.

Postup pri vytváraní uzatváracieho podpisu je zhodný s postupom pri vytváraní jednoduchého či viacnásobného podpisu. Namiesto tlačidla **Podpísať** je však potrebné použiť tlačidlo **Uzatvoriť**.



Obrázok 18 Uzatvorenie dokumentu

Súbor ZEP s uzatváracím podpisom je možné znovu podpísať alebo aj ďalej uzatvoriť, ak je to potrebné. **Pred uzatvorením podpisu musia byť všetky podpisy doplnené na úplnú informáciu.**

POZOR: Pred podpísaním dokumentu si vždy dôkladne preštudujte, čo podpisujte.

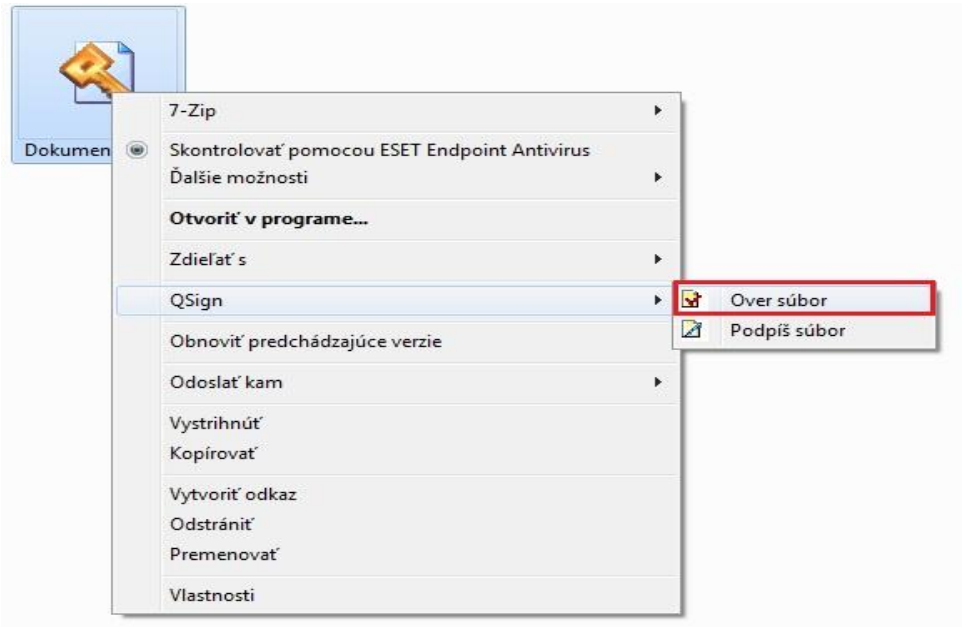
3.4. Overovanie prijatých podpísaných dokumentov

Overiť podpísaný dokument môže každý, kto:

1. má spustenú aplikáciu QSign v režime „Online“.
2. je pripojený na Internet.

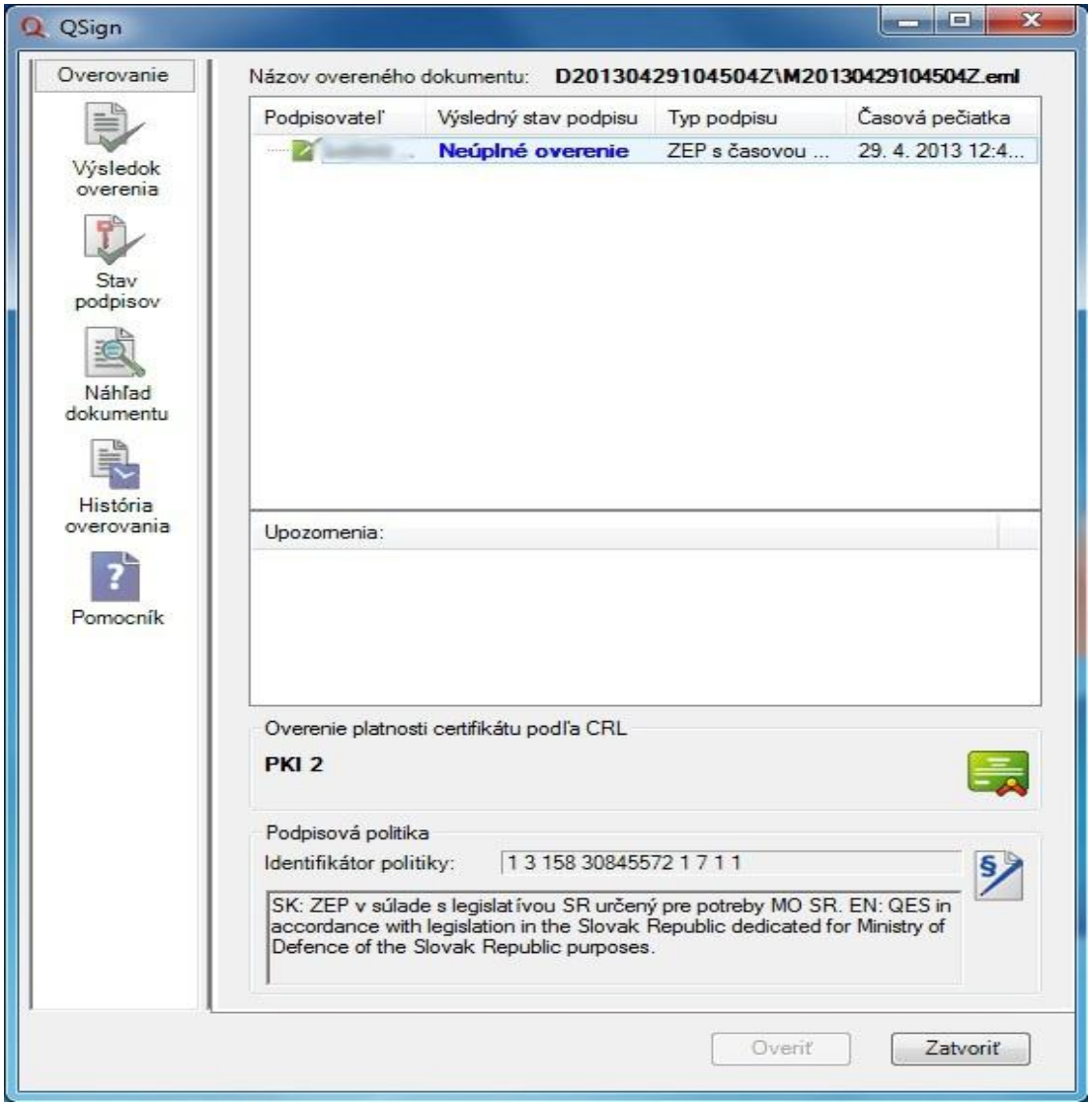
Postup overovania podpisu pomocou kontextového menu je nasledovný:

1. v prostredí Prieskumníka otvoríte kontextové menu nad súborom, ktorý chcete overiť, v menu vyberte položku **QSign** > **Over súbor**



Obrázok 19 Overenie dokumentu cez kontextové menu

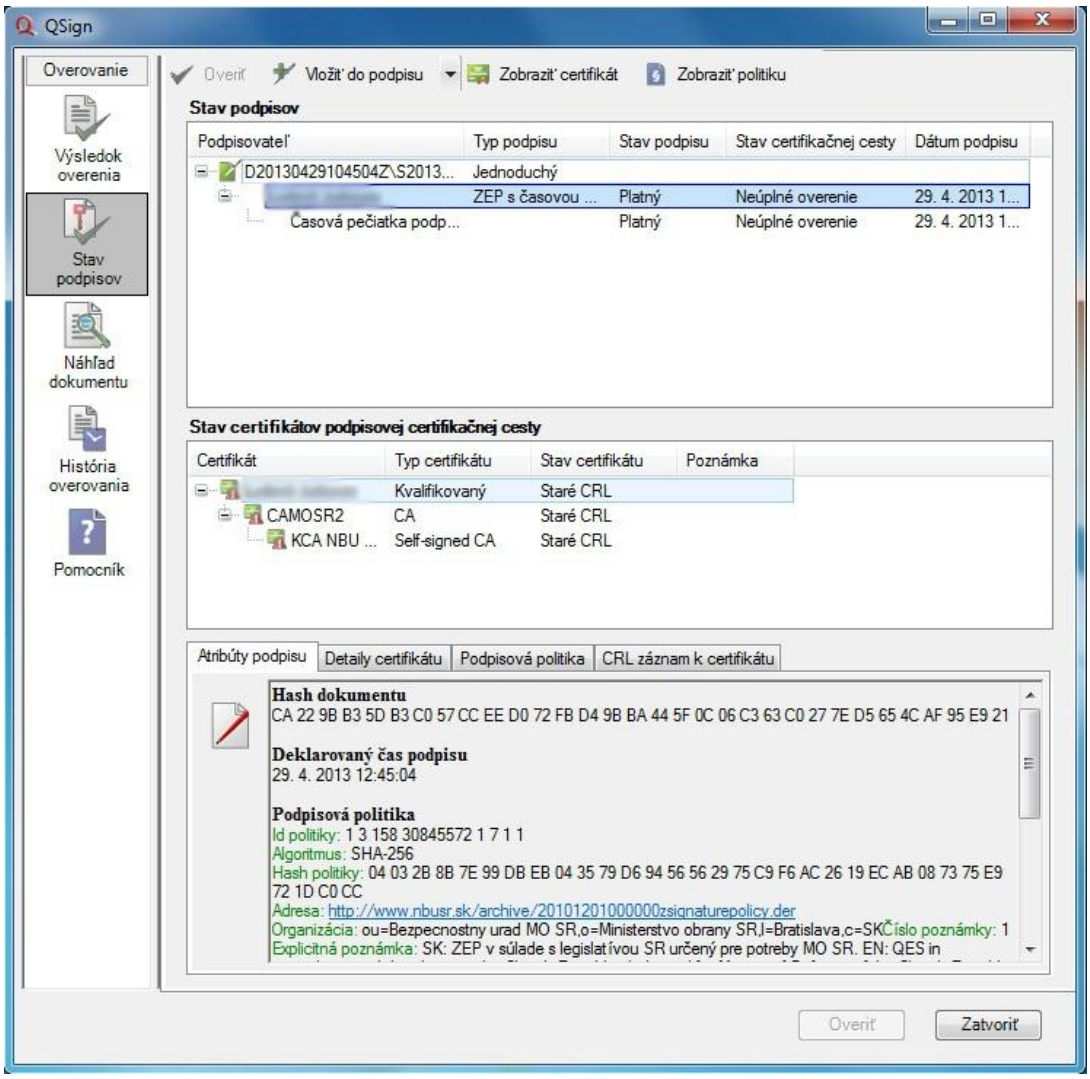
2. Po stlačení tlačidla **Over súbor** aplikácia overí platnosť podpisu pomocou informácií získaných z dôveryhodných internetových zdrojov. Vykonanie operácie vyžaduje určitý čas (približne 30 sekúnd)
3. Po dokončení operácie overovania sa zobrazí výsledok overenia



Obrázok 20 Výsledok overenia

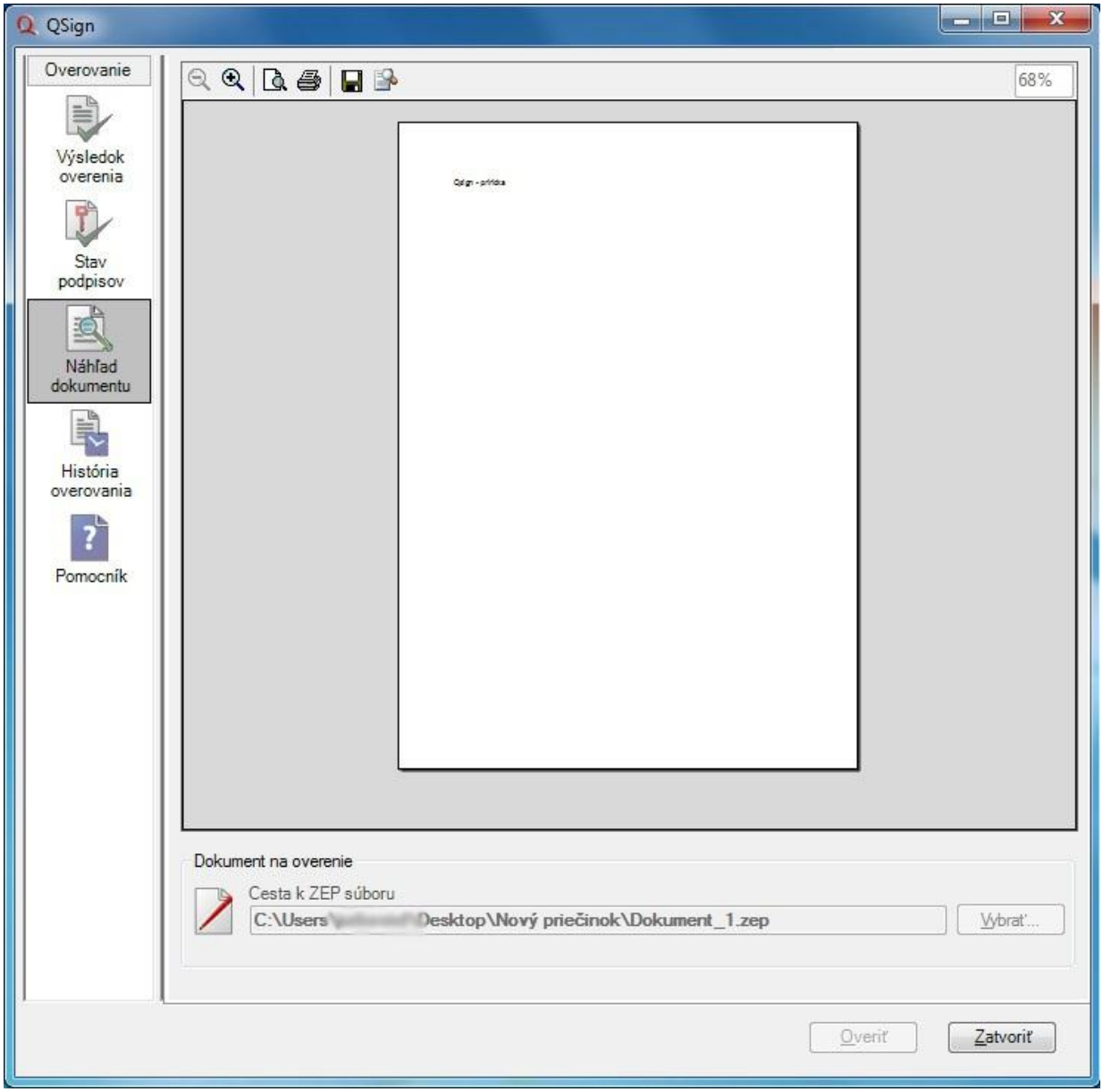
V prípade zobrazenia stavu „**Neúplné overenie**“ je potrebné pre úplnosť overenia zopakovať overenie podpisu podľa uvedeného postupu, znovu po uplynutí 12-24 hodín. Možné stavy podpisov, certifikátov a typy podpisov sú uvedené v bode **4** tejto pomôcky.

4. V záložke Stav podpisov na ľavej strane sú zobrazené detaily certifikátu a certifikačnej cesty



Obrázok 21 Podrobné informácie o certifikátoch

5. Kliknutím na záložku Náhľad dokumentu na ľavej strane si môžete dokument pozrieť, uložiť alebo vytlačiť



Obrázok 22 Náhľad dokumentu pri overovaní

Podrobný popis overovacieho okna a možností jeho použitia obsahuje **Pomocník** aplikácie QSign (dostupný z menu ovládania na paneli úloh).

4. Definícia stavu podpisu certifikátu

Po overení dokumentu sa vám v overovacom okne zobrazí časť „**Výsledok overenia**“. Dôležitou položkou je „**Výsledný stav podpisu**“ (viď obrázok vyššie).

Možné stavy	Presnejší opis
Platný	Podpis ostane platný pokiaľ obsahuje platnú časovú pečiatku. Tento stav je pri overovaní zvýraznený Zelenou farbou - Platný. **Upozornenie**: Pokiaľ podpis neobsahuje časovú pečiatku a je zobrazený tento stav, tak časom môže dôjsť k zmene tohto stavu, pretože podpis bol overovaný k systémovému času z histórie overovania
Neplatný	Pokiaľ bol nejaký podpis vyhlásený za neplatný jeho stav sa už nemôže zmeniť. Tento stav je pri overovaní zvýraznený Červenou farbou - Neplatný.
Neúplne overenie	Nie je k dispozícii CRL záznam s ktorým je možno rozhodnúť platnosť podpisu. CRL záznam nemusí byť ešte vydaný alebo nebol importovaný do aplikácie. Tento stav je pri overovaní zvýraznený Modrou farbou. Neúplné overenie neznamená, že podpis nie je platný. V čase overovania podpisu aplikácia nie je schopná jednoznačne rozhodnúť o platnosti podpisu nakoľko nemá dostupné CRL k danému momentu. Avšak po získaní nového CRL (t.j. v rozsahu maximálne 12-24 hodín) doplní uvedenú informáciu na úplné overenie a teda rozhodne o platnosti, resp. neplatnosti podpisu.
Nemožno rozhodnúť	Vzhľadom na Slovenskú legislatívu sa nedá rozhodnúť o platnosti podpisu. Podpis bol vytvorený v dobe, kedy sa nedá automaticky, aplikačne rozhodnúť či bol certifikát podpisovateľa zneplatnený. Tento stav nemôže nastať pri overovaní podľa PKI alebo PKI 2. Tento stav je pri overovaní zvýraznený Modrou farbou - Nemožno rozhodnúť. Upozornenie: V takomto prípade musíte požiadať certifikačnú autoritu, ktorá vydala príslušný certifikát o určenie, či v čase vytvorenia podpisu bol certifikát platný.