



 **QSign™ 5**

Používateľská príručka

© 2014-2020 Ardaco, a.s. Všetky práva vyhradené.

Kopírovanie, prenášanie, rozširovanie alebo uchovávanie časti alebo celého obsahu tohto dokumentu v akejkoľvek forme bez predchádzajúceho písomného súhlasu spoločnosti Ardaco, a.s. je zakázané.

Názvy produktov a spoločností uvedené v tomto dokumente môžu byť ochrannými známkami alebo obchodnými označeniami príslušných vlastníkov.

Aplikácia používa knižnicu jWMI zo stránky www.henryranch.net. Zoznam licencií ďalších použitých komponentov sa nachádza v cieľovom inštaláčnom adresári aplikácie.

Spoločnosť Ardaco, a.s. uplatňuje politiku kontinuálneho rozvoja. Spoločnosť Ardaco, a.s. si vyhradzuje právo meniť a zdokonaľovať akýkoľvek z produktov opísaných v tomto dokumente bez predchádzajúceho upozornenia.

Spoločnosť Ardaco, a.s. nie je za nijakých okolností zodpovedná za stratu údajov alebo príjmov za akokoľvek spôsobené osobitné, náhodné, následné alebo nepriame škody. Obsah tohto dokumentu sa vykladá „tak, ako je“. Neponúkajú sa nijaké záruky akéhokoľvek druhu, či už výslovné alebo implikované, súvisiace so správnosťou, spoľahlivosťou alebo s obsahom tohto dokumentu, vrátane, ale aj nie výhradne, implikovaných záruk obchodovateľnosti a vhodnosti na určitý účel, okrem záruk, ktoré stanovuje príslušný právny predpis.

Spoločnosť Ardaco, a.s. si vyhradzuje právo tento dokument kedykoľvek upraviť alebo stiahnuť z obehu bez predchádzajúceho upozornenia.

V 5.3.15

Vydanie SK

OBSAH

1. Úvod	4
1.1. O aplikácii	4
1.2. Použité skratky.....	4
2. Inštalácia	5
2.1. Systémové požiadavky.....	5
2.2. Postup inštalácie	6
2.3. Odinštalovanie aplikácie	11
3. Prvé spustenie	12
3.1. Pripojenie k internetu	13
3.2. Aktivácia aplikácie	14
3.2.1. Aktivácia licenčným kľúčom	14
3.2.2. Aktivácia elektronickou poštou.....	15
3.3. Inštalácia podporných komponentov	17
3.4. Výber certifikátu	19
4. Práca s aplikáciou	21
4.1. Okno aplikácie.....	22
4.2. Otvorenie dokumentu	23
4.3. Podpísanie dokumentu	26
4.3.1. Nastavenie certifikátu.....	26
4.3.2. Voliteľné parametre podpisu	29
4.3.2.1. Časová pečiatka	29
4.3.2.2. Dôvod podpisu	30
4.3.2.3. Miesto podpisu.....	30
4.3.2.4. Sprievodné dokumenty	30
4.3.3. Podpisovanie.....	31
4.4. Overenie podpisu.....	34
4.4.1. Výsledok overenia	34
4.4.1.1. Výsledný stav overenia	34
4.4.1.2. Upozornenia	35
4.4.1.3. Stav podpisov	35
4.4.1.4. Sprievodné dokumenty	35
4.4.2. Podrobnosti overenia	36
4.4.2.1. Certifikát podpisovateľa	36
4.4.2.2. Časové pečiatky vložené do podpisu	37
4.4.2.3. Podpisová politika podpisu	37

4.4.2.4. Pridanie časovej pečiatky	37
4.5. Viacnásobný podpis	38
4.6. Hromadný podpis	40
4.7. Podpis viacerých dokumentov	43
5. Nastavenia	44
5.1. Základné nastavenia	44
5.1.1. Automatické aktualizácie	44
5.1.2. Predvolený formát podpisu	45
5.1.2.1. Predvolený typ kontajnera pre podpisy CAdES	45
5.1.2.2. Predvolený typ kontajnera pre podpisy XAdES	45
5.1.2.3. Predvolený formát vloženia podpisu pre dokumenty PDF	45
5.1.3. Časové pečiatky	46
5.2. Rozšírené nastavenia	47
5.2.1. Nastavenie overovania	47
5.2.2. XML formuláre	49
5.2.3. Priečinkov na ukladanie súborov	50
5.2.4. Podpisové politiky	50
5.2.5. Pripojenie na internet	51
5.3. O aplikácii	52
6. Slovník pojmov	53
6.1. Časová pečiatka	53
6.2. CRL	53
6.3. OCSP	53
6.4. Certifikačná cesta	53
6.5. Neúplné overenie	54
6.6. Neúplné automatické overenie	54
6.7. Podpisová politika	54

1. Úvod

V tomto dokumente sú popísané funkcie a postupy používania klientskej aplikácie QSign. Používateľská príručka nemá za cieľ vysvetľovať termíny, atribúty alebo technické detaily elektronického podpisu a súvisiacich náležitostí jeho používania. Ak nie je uvedené inak, popisy a obrázky sa vzťahujú k aplikácii používanej v operačnom systéme Microsoft Windows 10. Používanie aplikácie v inom operačnom systéme je veľmi podobné ak nie rovnaké. Iný postup alebo funkčnosť je v takom prípade samostatne popísaná a označená na začiatku odseku skratkou operačného systému, viď kapitola 1.2 *Použité skratky*.

1.1. O aplikácii

QSign - Aplikácia pre KEP je klientska softvérová aplikácia určená na vytváranie a overovanie kvalifikovaných elektronických podpisov (KEP) alebo zdokonalených elektronických podpisov (EP), resp. podpisovanie dokumentov alebo akýchkoľvek súborov a overovanie ich podpisov v súlade s Nariadením Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (Nariadenie eIDAS) a v zmysle legislatívy Slovenskej republiky.

Na podpisovanie je možné použiť elektronický občiansky preukaz (eID) alebo iné zariadenie na podpis a pečať (QSCD), ktoré je certifikované podľa Nariadenia eIDAS.

Dokumenty podpísané aplikáciou QSign je možné použiť v administratívnom aj obchodnom styku.

1.2. Použité skratky

Skratka	Význam
CRL	Zoznam zneplatnených certifikátov (Certificate Revocation List)
ČP	Časová pečiatka
EP	Elektronický podpis
KEP	Kvalifikovaný elektronický podpis
WIN	Operačný systém Microsoft® Windows®
MAC	Operačný systém Apple® macOS®

2. Inštalácia

2.1. Systémové požiadavky

Operačný systém:	<ul style="list-style-type: none">› Windows 7 32bit/64bit a novší› macOS 10.12 Sierra a novší
Procesor:	<i>Minimálne:</i> 800 MHz <i>Optimálne:</i> 2.4 GHz
Operačná pamäť (RAM):	<i>Minimálne:</i> 1 GB a viac
Voľné miesto na pevnom disku:	200 MB
Zariadenie na podpisovanie¹:	<ul style="list-style-type: none">› Elektronický občiansky preukaz (eID karta)› Zariadenie kompatibilné so štandardom PKCS#11
Podporný softvér:	<ul style="list-style-type: none">› Java 8,› GhostScript 9.27 (aplikácia QSign umožňuje jeho automatizovanú inštaláciu)

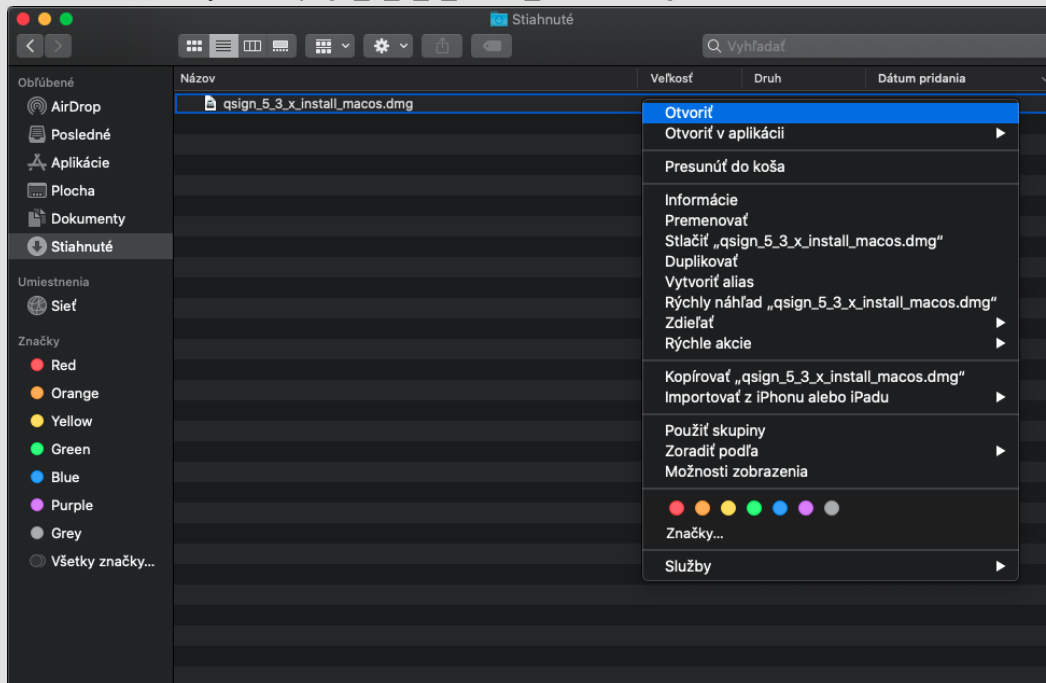
¹ Na umožnenie pripojenia a využívania zariadenia na podpisovanie je nutné nainštalovať ovládače dodávané spolu s ním. Na tvorbu KEP je vyžadované certifikované [QSCD zariadenie](#) podľa nariadenia Európskeho parlamentu a Rady č. 910/2014.

2.2. Postup inštalácie

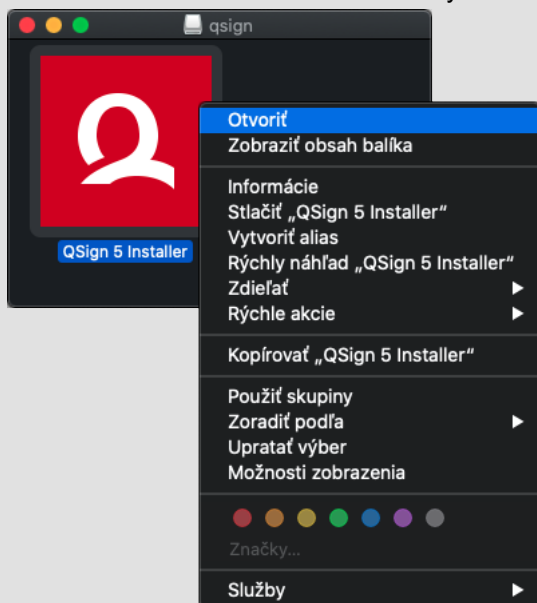
Spustíte inštalačný súbor *qsign_5_3_x_install_win32.exe*, resp. *qsign_5_3_x_install_win64.exe*.

MAC:

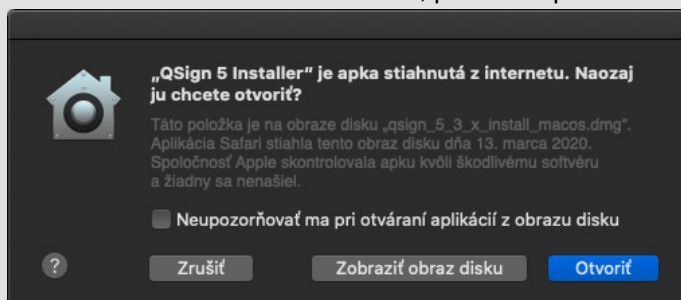
Otvorte inštalačný balík *qsign_5_3_x_install_macos.dmg*.



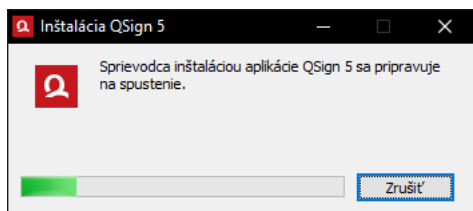
V zobrazenom okne otvorte inštalačný súbor *QSign 5 Installer*.



Ak sa zobrazí nasledovné hlásenie, potvrdte spustenie inštalátora stlačením „**Otvoriť**“.

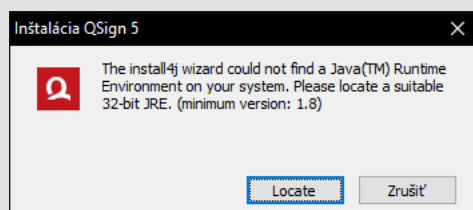


1. Spustí sa sprievodca inštaláciou.

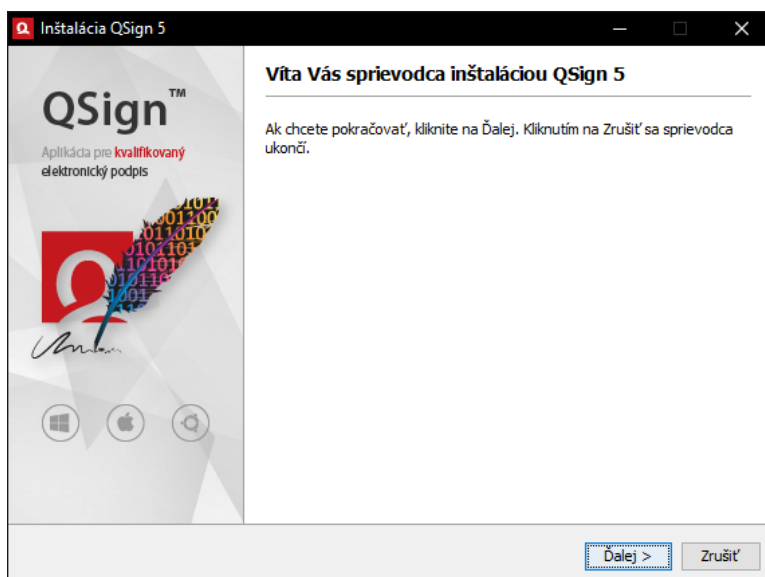


UPOZORNENIE:

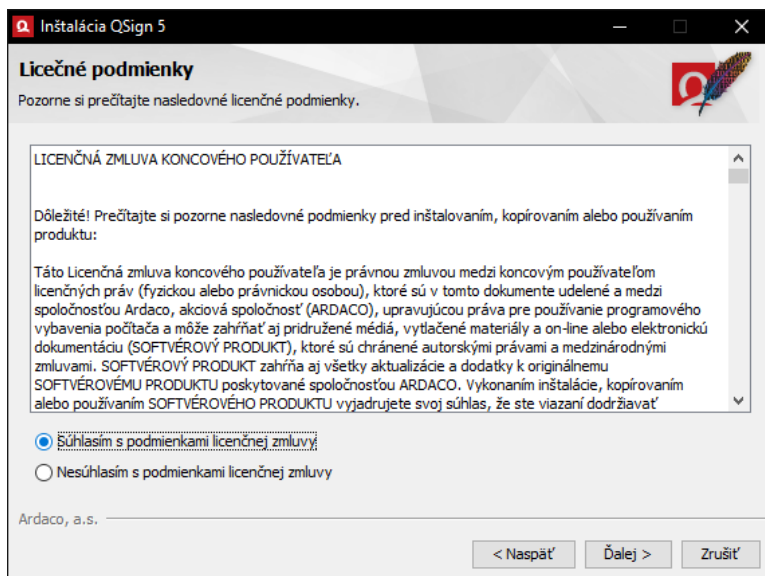
Pokiaľ nie je v počítači nainštalovaná Java alebo nie je kompatibilná, zobrazí sa nasledovné hlásenie. Určite umiestnenie, kde je Java nainštalovaná, alebo preinštalujte Javu. Ak inštalujete 32-bitovú verziu QSign, mala by byť v počítači nainštalovaná Java v 32-bitovej verzii. Ak inštalujete 64-bitovú verziu QSign, musí byť v počítači nainštalovaná Java v 64-bitovej verzii.



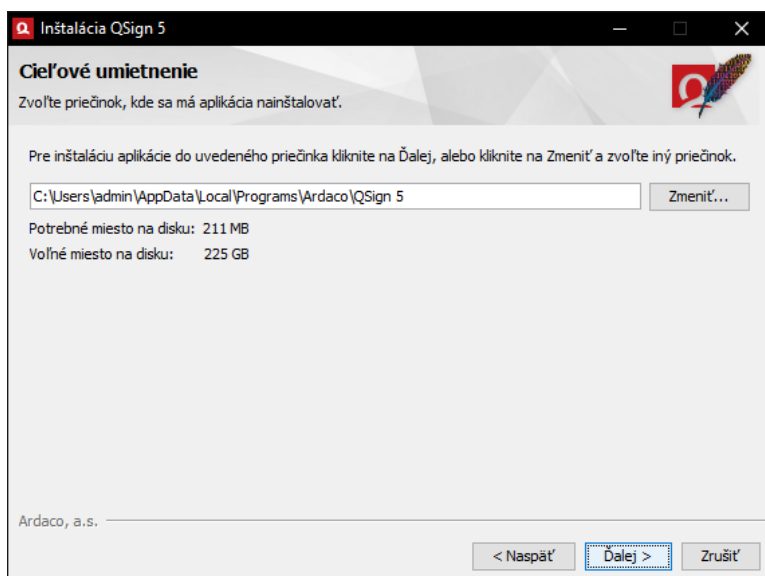
2. Zobrazí sa úvodné okno sprievodcu inštaláciou. Pokračujte stlačením „Ďalej“.



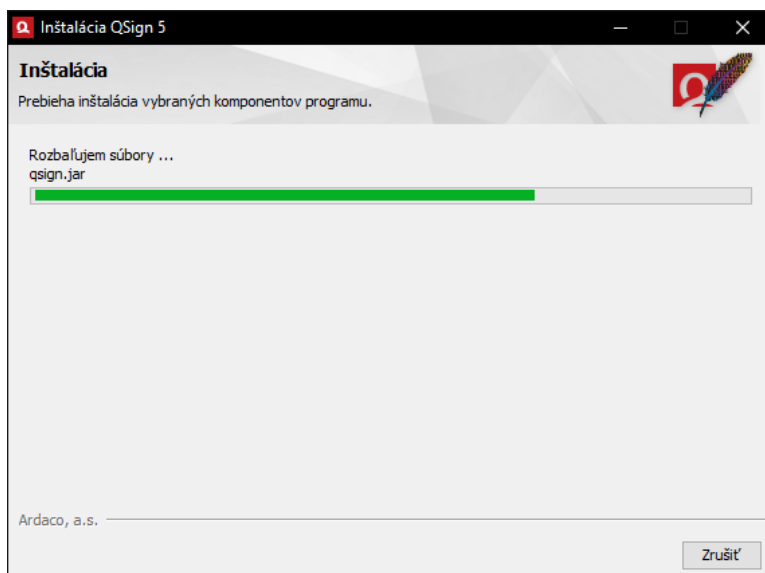
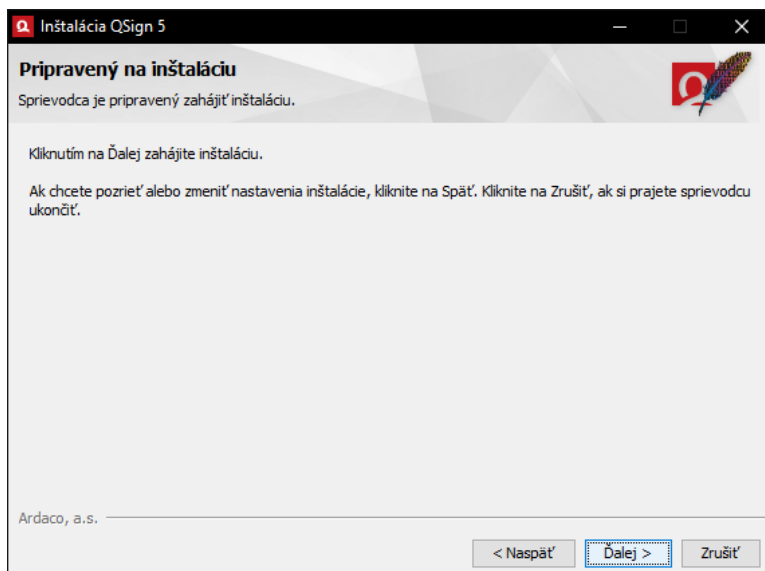
3. Aby bolo možné pokračovať v inštalácii aplikácie, musíte súhlasiť s licenčnými podmienkami použitia aplikácie, inak bude inštalácia ukončená. Prečítajte si pozorne licenčné podmienky pred inštalovaním, kopírovaním alebo používaním produktu. Vyjadrite súhlas s podmienkami licenčnej zmluvy a pokračujte stlačením „**Ďalej**“.



4. Zvoľte cieľový priečinok, kde sa má aplikácia nainštalovať, alebo ponechajte predvolené umiestnenie. Na pokračovanie stlačte „**Ďalej**“.

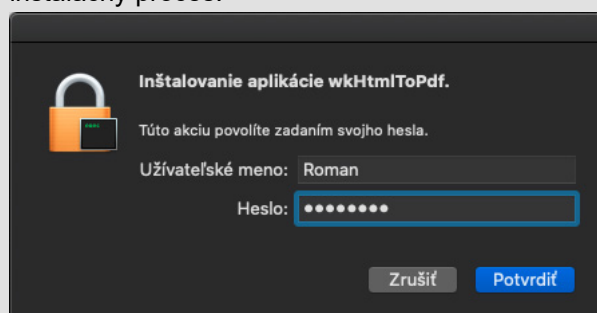


5. Inštalácia je pripravená. Stlačením „**Ďalej**“ sa začne proces inštalácie aplikácie.



MAC:

Počas inštalácie môžete byť operačným systémom vyzvaný na potvrdenie prístupových práv pre inštaláciu programu.



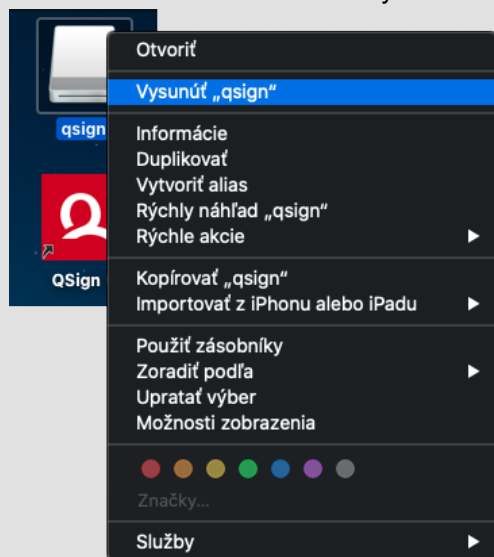
6. Po vykonaní inštalácie sa zobrazí záverečné okno s výsledkom procesu inštalácie. Na ukončenie inštalácie stlačte „Ukončiť“.



7. Po úspešnom ukončení inštalácie sa vytvorí zástupca aplikácie v ponuke programov/aplikácií operačného systému a na pracovnej ploche.

MAC:

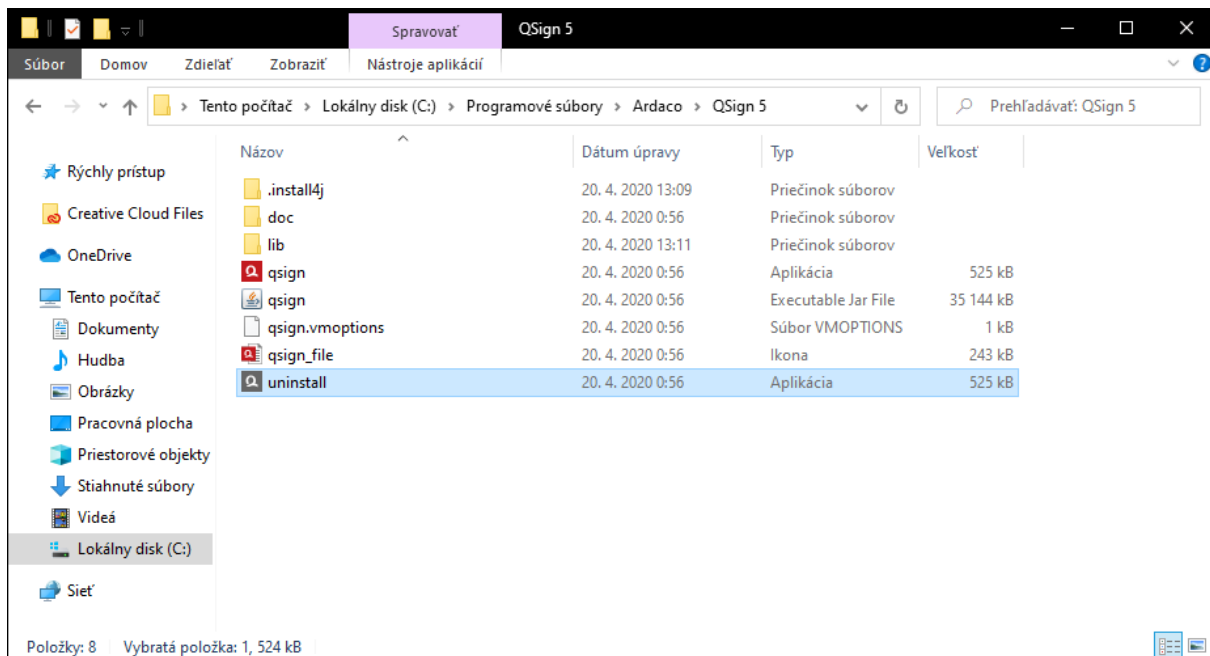
Teraz môžete zatvoriť inštaláčny balík voľbou „Vysunúť...“.



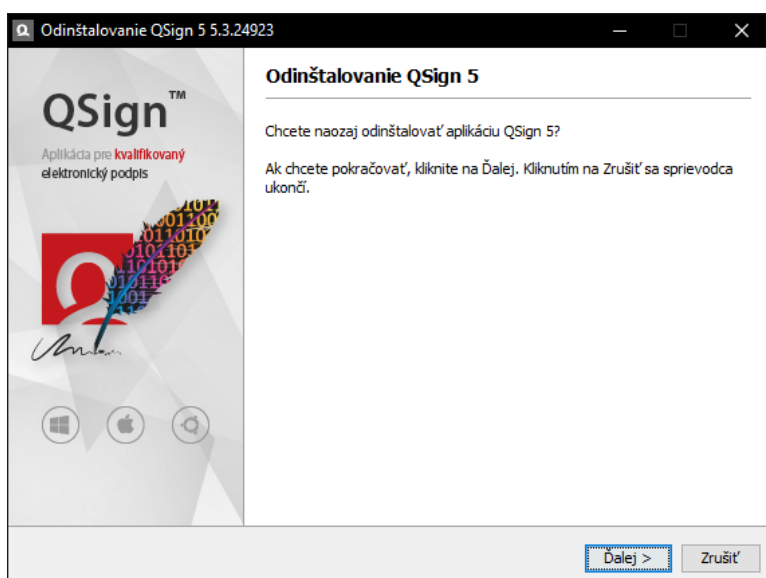
2.3. Odinštalovanie aplikácie

Odinštalovanie aplikácie je možné spustiť dvoma spôsobmi:

- › Otvorte Prieskumníka súborov (Tento počítač), na systémovom disku v Programových súboroch prejdite do priečinka Ardaco\QSign 5 ako zobrazuje nasledovný obrázok a spustíte súbor „**uninstall**“.



- › Otvorte ponuku ŠTART, prejdite do priečinka Ardaco, otvorte kontextovú ponuku stlačením pravého tlačidla myši na položku QSign 5 a zvolte „**Odinštalovať**“. Otvorí sa okno *Programy a súčasti*, kde vyhľadajte a označte riadok QSign 5. Stlačte „**Odinštalovať alebo zmeniť**“.

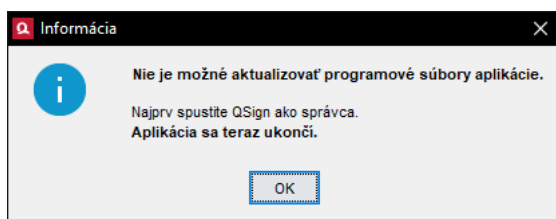


MAC:

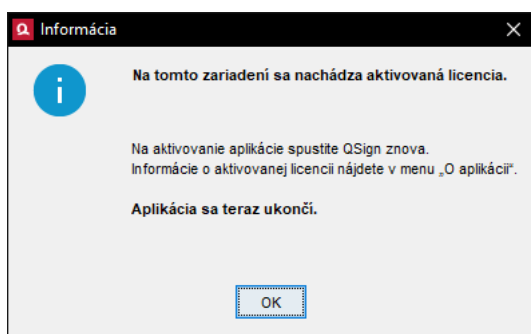
Aplikáciu odinštalujete štandardne jej presunutím do koša.

3. Prvé spustenie

Aplikáciu po nainštalovaní možno bude potrebné prvý krát spustiť ako správca. Kliknite pravým tlačidlom na ikonu aplikácie QSign a v kontextovom menu zvolíte „Spustiť ako správca“.



Ak aplikácia pri prvom spustení rozpozná, že na danom počítači bola aktivovaná licencia, ktorá je platná, zobrazí nasledovné hlásenie. Stlačením „OK“ sa preruší jej spustenie (okno sa zatvorí) a aktivujú sa potrebné licencované komponenty. Aplikáciu spustíte znova.



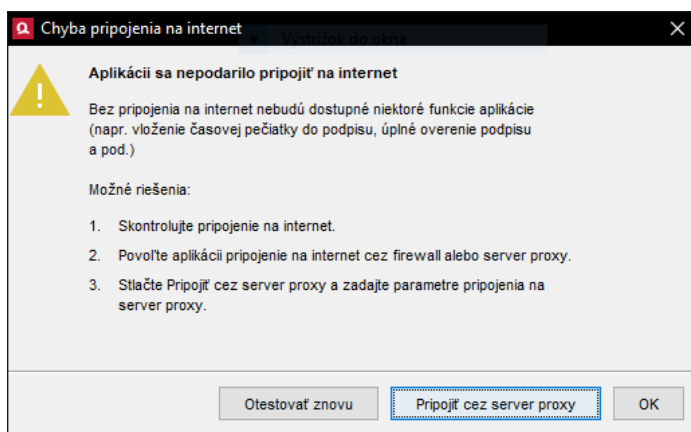
Po prvom spustení aplikácie môžete byť vyzvaný na nastavenie niektorých parametrov aplikácie, napr. zadanie licenčného kľúča (aktivácia), podpisovacieho certifikátu alebo nastavenie pripojenia na internet cez proxy. Ak sa v operačnom systéme nenájdu vyžadované komponenty potrebné na správne fungovanie aplikácie (napr. GhostScript), tak počas prvého spustenia aplikácie alebo prvého použitia komponentu budete vyzvaný na ich inštaláciu.

3.1. Pripojenie k internetu

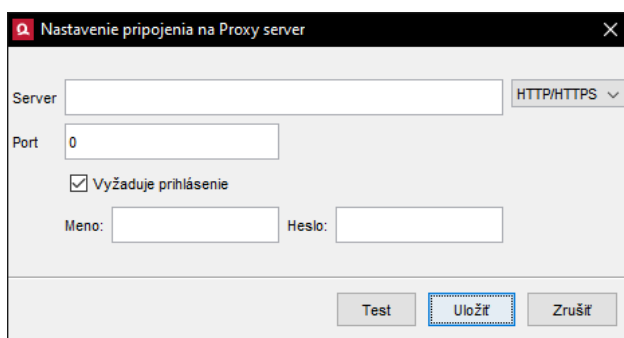
Aby sa mohli naplno využívať všetky funkcie aplikácie, potrebuje mať aplikácia v určitých činnostiach prístup na internet, a to napríklad pri zisťovaní platnosti certifikátov (služba OCSP alebo sťahovanie CRL záznamov) alebo pri podpise s časovou pečiatkou (prístup na server časových pečiatok) a pod.

Pri prvom spustení aplikácie sa kontroluje pripojenie na internet. Ak sa nenájde žiadne pripojenie, budete vyzvaný na nastavenie pripojenia cez server proxy. V prípade, že neexistuje pripojenie na internet ani cez server proxy, môžete toto nastavenie preskočiť. V takom prípade bude aplikácia fungovať aj bez pripojenia na internet, ale niektoré funkcie nebudú pracovať správne alebo nebudú dostupné.

1. Ak sa aplikácii nepodarí pripojiť na internet, zobrazí sa nasledujúca výzva. Stlačte **„Pripojiť cez server proxy“** pre nastavenie parametrov pripojenia cez server proxy, alebo **„OK“** pre pokračovanie bez pripojenia na internet.



2. Ak poznáte potrebné parametre pripojenia cez Proxy server, vyplňte ich a uložte stlačením **„Uložiť“**. Ak parametre nepoznáte, vyžiadajte si ich od sieťového administrátora.



Stlačením **„Test“** môžete otestovať vyplnené parametre. Stlačením **„Zrušiť“** budete pokračovať bez nastavenia Proxy.

3.2. Aktivácia aplikácie

Pri prvom spustení aplikácie alebo použití funkcie podpisovania sa kontroluje, či je na počítači aktivovaná príslušná softvérová licencia pre aplikáciu QSign. Ak sa licencia nenájde, budete vyzvaný na aktiváciu licenčným kľúčom získaným kúpou softvérovej licencie k produktu.

UPOZORNENIE:

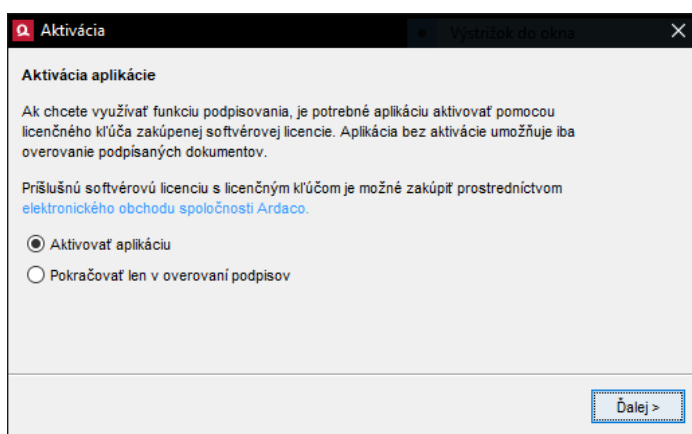
Po úspešnej aktivácii aplikácia vytvorí súbor s licenciou. Táto licencia je medzi počítačmi neprenositeľná, čo znamená, že jedno licenčné číslo sa dá použiť na aktiváciu produktu iba na jednom počítači. Viac informácií nájdete v licenčných podmienkach produktu.

Bez vykonania aktivácie aplikácia umožní len overovanie podpísaných dokumentov.

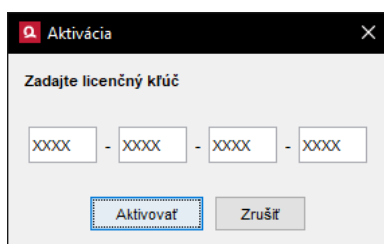
Na aktiváciu nebudete vyzvaný v prípade, ak sa na počítači nájde licenčný súbor. V takom prípade sa licenčný kľúč získa automaticky a rovnaký typ licencie sa použije aj pre novú verziu aplikácie.

3.2.1. Aktivácia licenčným kľúčom

1. Vyberte možnosť „Aktivovať aplikáciu“ a stlačte „Ďalej“.



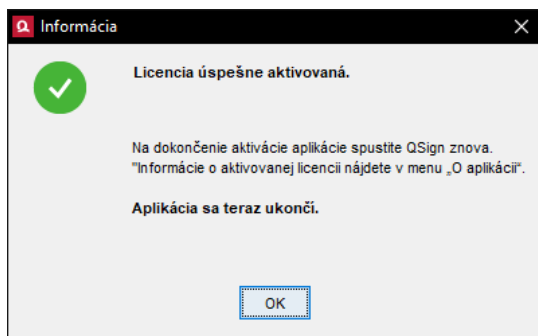
2. Zadať licenčný kľúč a stlačte „Aktivovať“.



Do políček zadajte licenčný kľúč, ktorý ste obdržali pri kúpe softvérovej licencie produktu. Aby ste nemuseli opisovať ručne celý licenčný kľúč, pre pohodlnejšie zadanie ho môžete celý skopírovať do schránky stlačením **Ctrl+C** a vložiť naraz stlačením **Ctrl+V** (pri vkladaní môžete nastaviť kurzor na ľubovoľné zo štyroch editovateľných políček).

Stlačením „Aktivovať“ sa začne proces aktivácie, ktorý prebieha na pozadí a využíva sa pri ňom pripojenie na internet. Tento proces by nemal trvať viac ako niekoľko sekúnd. Ak aktivácia zlyhá z dôvodu nedostupnosti pripojenia na internet, budete na to upozornení a vyzvaný na aktiváciu cez e-mail (viď nasledujúca kapitola).

- Po úspešnej aktivácii sa zobrazí informačné okno.



3.2.2. Aktivácia elektronickou poštou

Ak aktivácia licenčným kľúčom zlyhá z dôvodu nedostupnosti pripojenia na internet, bude používateľ vyzvaný na aktiváciu prostredníctvom elektronickej pošty. Tento spôsob aktivácie sa môže využiť napr. pri dočasnom výpadku internetového pripojenia, keďže pri samotnom procese aktivácie nie je internet potrebný. Internetové pripojenie je potrebné iba na prijatie a odoslanie elektronickej pošty a táto komunikácia sa môže uskutočniť aj z iného počítača.

- Skopírujte registračný kód do schránky stlačením „**Kopírovať**“.
- Vložte registračný kód do tela novej správy e-mailu.

UPOZORNENIE:

Správa nesmie obsahovať nič iné, iba kód začínajúci textom

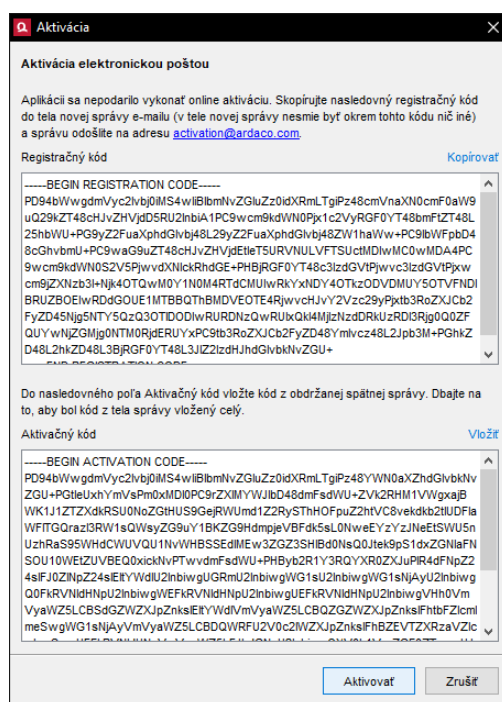
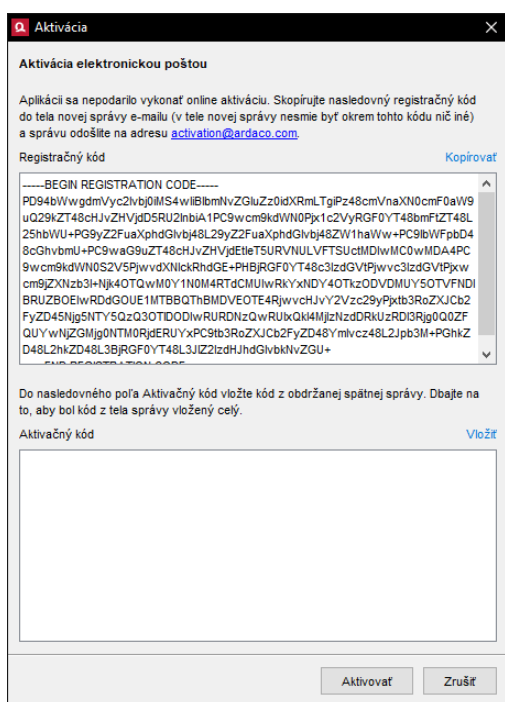
-----BEGIN REGISTRATION CODE-----

a končiaci textom

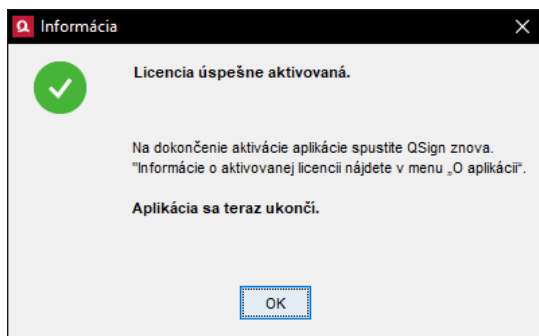
-----END REGISTRATION CODE-----

- E-mail odošlite na adresu activation@ardaco.com.

- Aktivačný kód, ktorý dostanete späť e-mailom, vložte následne do editovateľného poľa v spodnej časti okna a stlačte „**Aktivovať**“ (Na tento krok nie je potrebné pripojenie na internet).



5. Po úspešnom dokončení aktivácie sa zobrazí informačné okno.



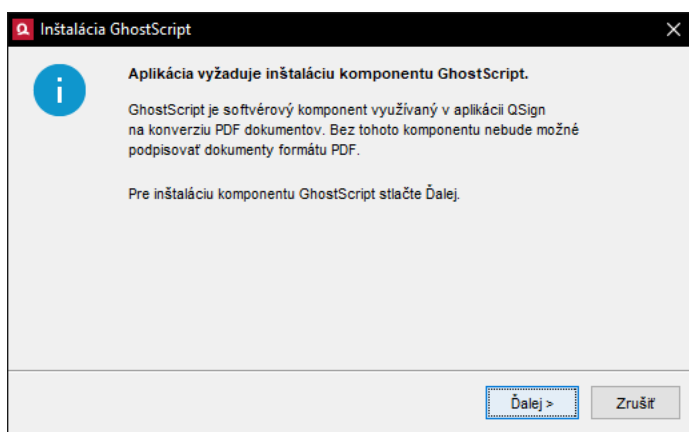
3.3. Inštalácia podporných komponentov

Pri prvom spustení aplikácie QSign alebo pri podpisovaní PDF dokumentu sa kontroluje prítomnosť programového komponentu GhostScript. Ak sa tento programový komponent v operačnom systéme nenájde, budete vyzvaný na jeho inštaláciu.

UPOZORNENIE:

Inštaláciu programového komponentu GhostScript je možné preskočiť, ale v takom prípade nebude možné podpisovať dokumenty vo formáte PDF.

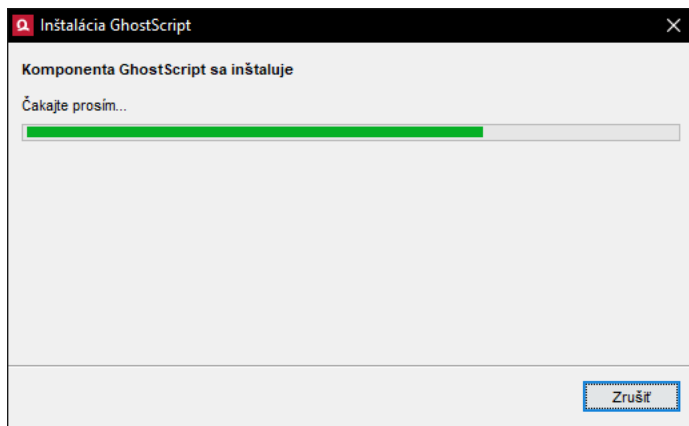
1. Zobrazí sa výzva na nainštalovanie komponentu GhostScript. Na pokračovanie stlačte „**Ďalej**“.



2. Ak chcete tento komponent nainštalovať, musíte súhlasiť s licenčnými podmienkami jeho poskytovateľa. Na spustenie inštalácie stlačte „**Inštalovať**“.

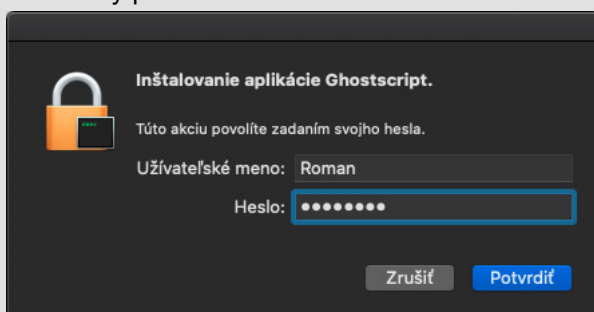


3. Inštalačné súbory GhostScript sa automaticky prevezmú prostredníctvom internetu a následne sa GhostScript nainštaluje.

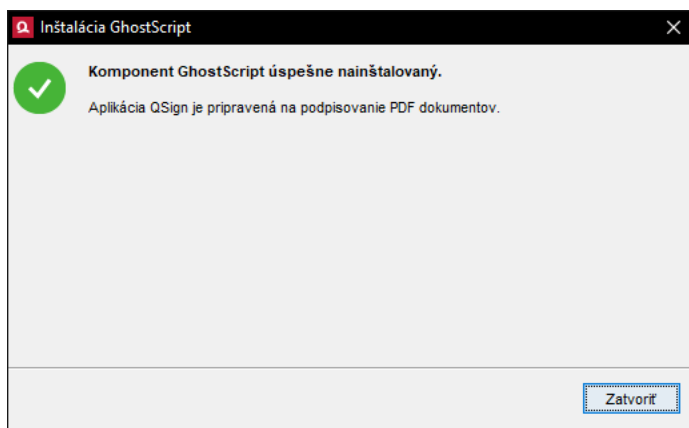


MAC:

Počas inštalácie môžete byť operačným systémom vyzvaný na potvrdenie prístupových práv pre inštalačný proces.



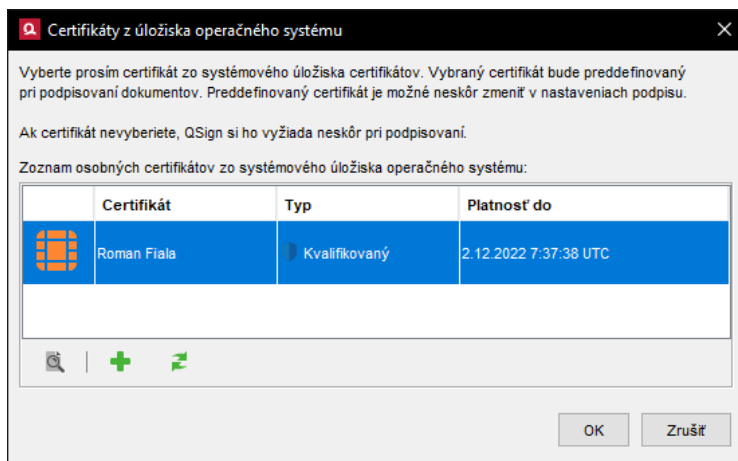
4. Po ukončení inštalácie sa zobrazí informačné okno.



3.4. Výber certifikátu

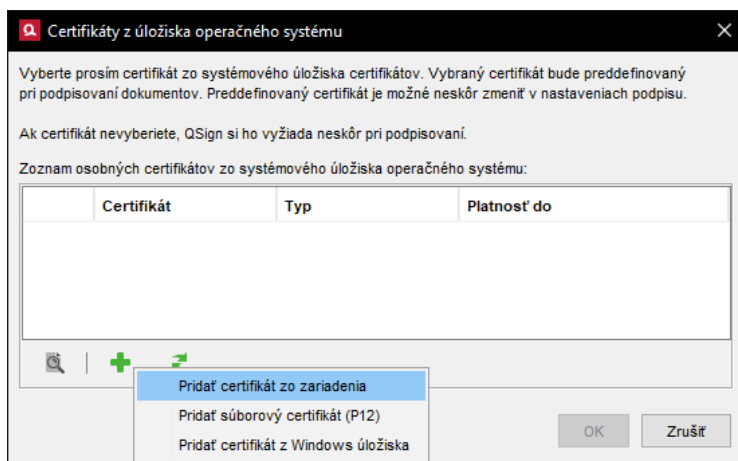
Aby bolo možné použiť aplikáciu po prvom spustení hneď aj na podpisovanie, je potrebné zvoliť certifikát podpisovateľa, t. j. certifikát osoby, ktorým sa budú dokumenty podpisovať. Zvolený certifikát môžete neskôr zmeniť (pozrite kapitolu 4.3.1 *Nastavenie certifikátu*).

1. Zo systémového úložiska sa v nasledovnom okne načítajú všetky certifikáty inštalované v operačnom systéme. Certifikát označte a stlačte „OK“.

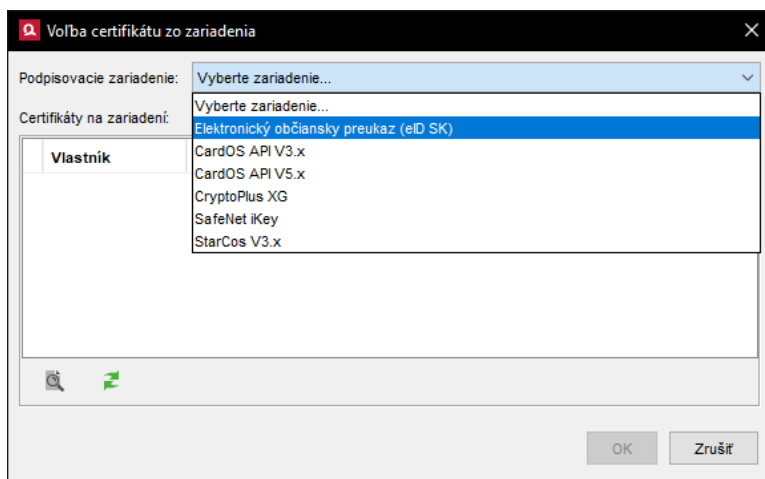


Detaily označeného certifikátu zobrazíte stlačením 🔍.

2. Ak sa v zozname požadovaný certifikát nenachádza, stlačte tlačidlo + pre prídanie certifikátu. V prípade použitia hardvérového zariadenia zvolte „Pridať certifikát zo zariadenia“. Zobrazí sa okno pre načítanie zariadenia a certifikátu.



3. Vyberte podpisovacie zariadenie z rolovacieho zoznamu. Tento zoznam obsahuje všetky zariadenia, ktoré aplikácia QSign podporuje.

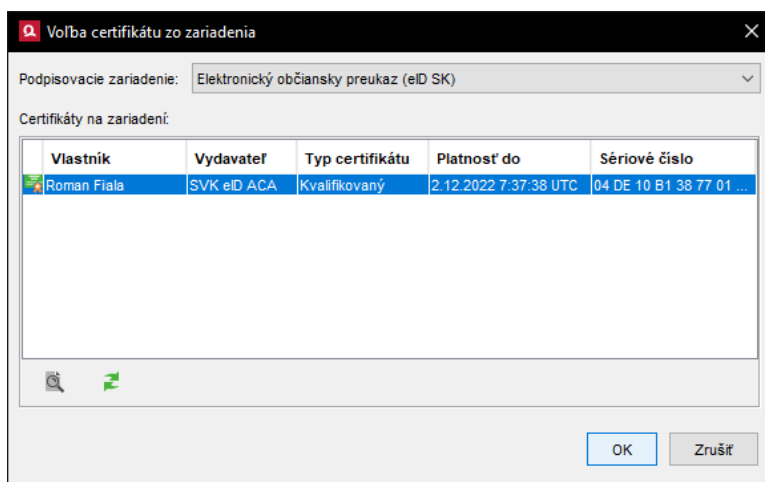


UPOZORNENIE:

Predtým ako vyberiete zariadenie, uistite sa, či máte nainštalované ovládače tohto zariadenia a zariadenie zasunuté do počítača.

Ak je v počítači nainštalovaná Java 64-bit, odporúčame inštalovať 64-bit ovládače pre podpisovacie zariadenie. Ak je Java 32-bit, aj ovládače musia byť 32-bitové.

4. Po zvolení podpisovacieho zariadenia sa v zozname nižšie zobrazia certifikáty, ktoré sa nachádzajú na zvolenom zariadení. Označte požadovaný certifikát a stlačte „OK“.



5. Zvolený certifikát sa zobrazí v zozname predvolených certifikátov (viď obrázok z kroku 1.). Ak sa tak nestane, stlačte ↺ pre obnovu zoznamu. Označte certifikát a stlačte „OK“. Certifikát bude použitý na podpisovanie dokumentov.

4. Práca s aplikáciou

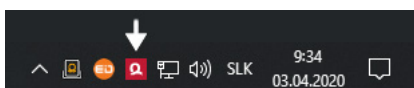
Aplikáciu QSign spustíte zástupcom na pracovnej ploche operačného systému, alebo cez ponuku Štart.

MAC:

Aplikáciu QSign môžete spustiť zástupcom na pracovnej ploche, v ponuke Launcher alebo v záložke Aplikácie okna Finder.

Spustenie aplikácie je indikované stavovou ikonou na systémovej lište operačného systému medzi ikonami aplikácií spustených na pozadí.

WIN:



Stlačte pravé tlačidlo myši na zobrazenie menu.

Dvojitým kliknutím ľavým tlačidlom otvoríte hlavné okno aplikácie.

MAC:



Stlačte ľavé tlačidlo myši na zobrazenie menu.

Dvojitým kliknutím pravým tlačidlom otvoríte hlavné okno aplikácie.

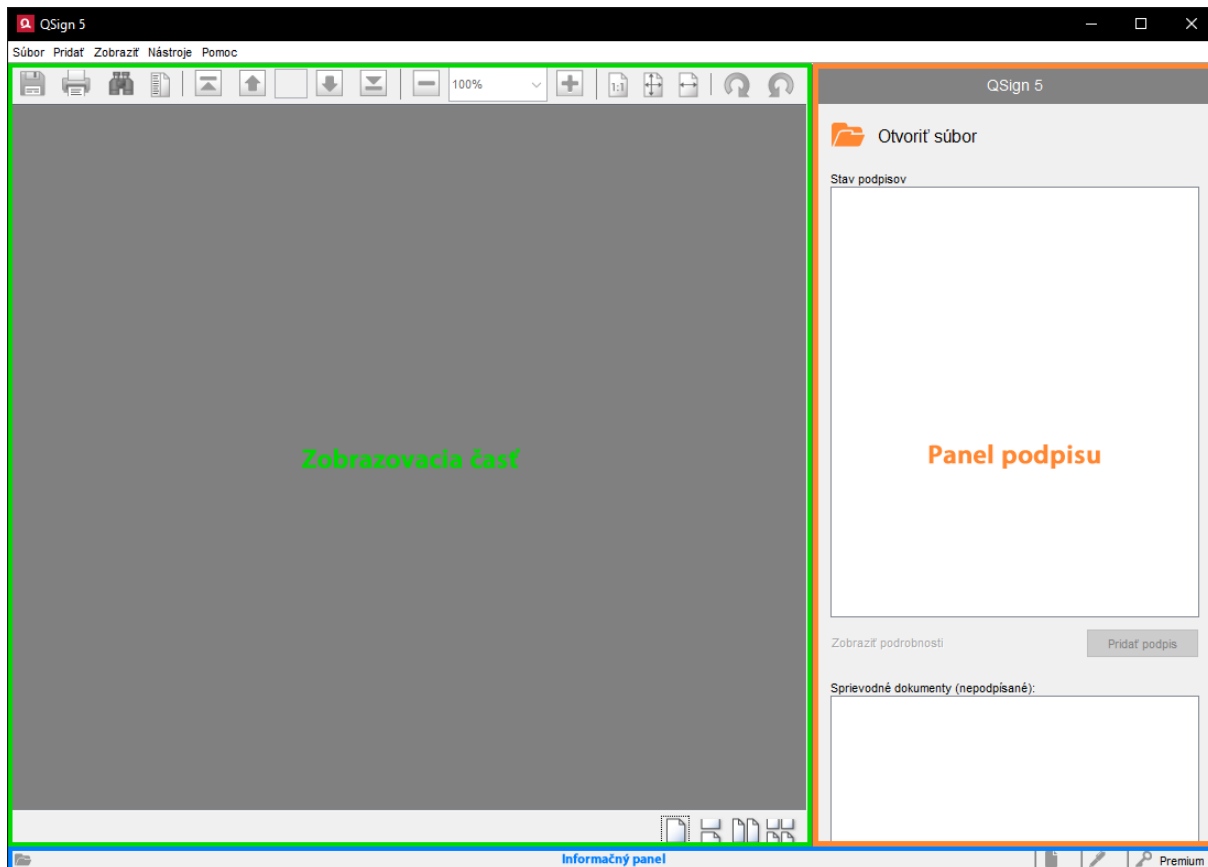
UPOZORNENIE:

Aplikáciu ukončíte voľbou „Ukončiť“ cez menu stavovej ikony na systémovej lište.

4.1. Okno aplikácie

Po spustení aplikácie QSign sa otvorí hlavné okno aplikácie, v ktorom sa vykonávajú všetky hlavné činnosti: podpisovanie dokumentu a overovanie podpisu dokumentu. Z tohto okna sú ďalej prístupné ostatné funkcie aplikácie.

Tvorí ho **Zobrazovacia časť** na ľavej strane pre náhľad podpisovaného alebo overovaného dokumentu. Na pravej strane okna je **Panel podpisu**, ktorý slúži na nastavenie podpisu alebo zobrazenie informácií o výsledku overenia podpisov. V spodnej časti sa nachádza **Informačný panel** zobrazujúci názov (cestu k súboru) a typ otvoreného dokumentu, typ podpisu (ak je otvorený podpísaný dokument) a typ licencie produktu.




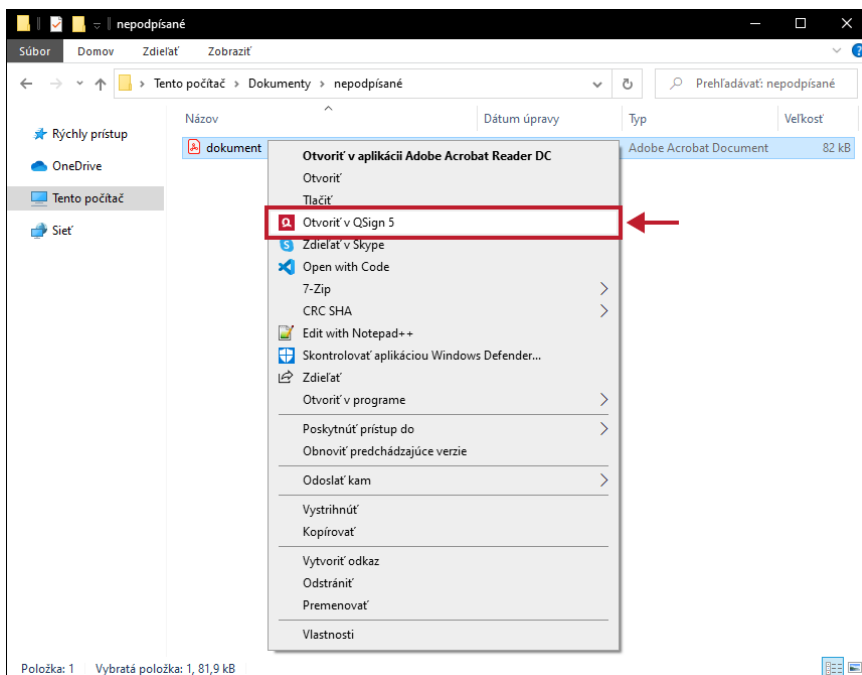
UPOZORNENIE:

Zatvorením hlavného okna sa aplikácia neukončí. Aplikáciu ukončíte cez menu jej stavovej ikony na systémovej lište.

4.2. Otvorenie dokumentu

Dokument môžete v aplikácii QSign otvoriť viacerými spôsobmi:

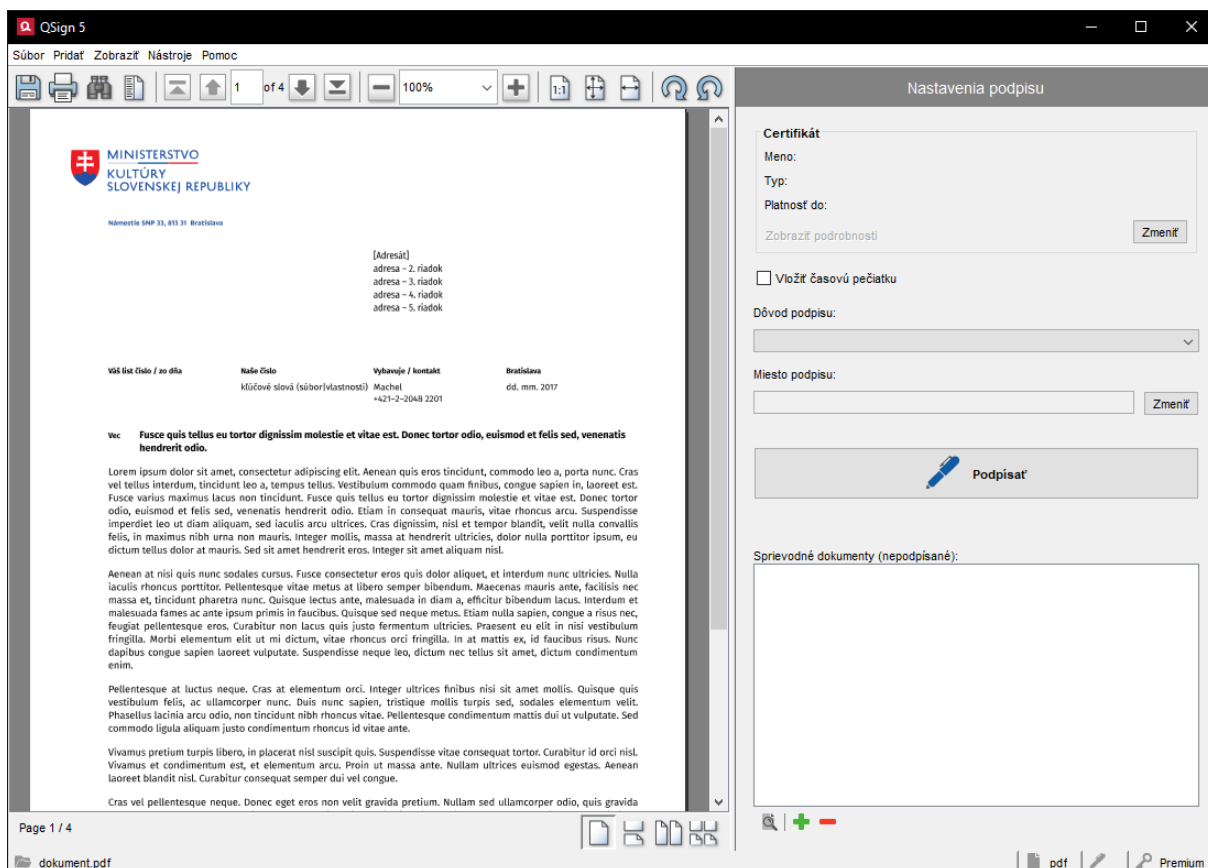
- › Kliknite na  „Otvoriť súbor“ na Paneli podpisu.
- › Použite funkciu *Drag&Drop*: uchyťte dokument myšou, potiahnite ho nad Zobrazovaciu časť a pustite.
- › Zvoľte položku „Súbor->Otvoriť“ z horného menu hlavného okna aplikácie.
- › Použite kontextové menu operačného systému Windows a zvoľte „Otvoriť v QSign 5“:



POZNÁMKA:

Otvoriť súbor je možné aj ďalšími spôsobmi využívanými hlavne pri prepojení s inými aplikáciami/systémami (napr. zadaním parametrov cez príkazový riadok operačného systému). Tieto možnosti sú popísané v dokumente „QSign 5.3 - Programátorská príručka“.

Po otvorení dokumentu sa jeho náhľad zobrazí v Zobrazovacej časti hlavného okna. Hlavné okno aplikácie s otvoreným dokumentom zobrazuje nasledovný obrázok.



Aplikácia pri otvorení dokumentu automaticky zistí, či je dokument podpísaný alebo nie. V závislosti na tom sa hlavné okno aplikácie prepne do jedného z dvoch nasledovných základných režimov, čo sa prejaví zmenou Panela podpisu:

› **Režim podpisu**

Ak otvoríte ešte nepodpísaný dokument, na Paneli podpisu sa zobrazia ovládacie prvky slúžiace na vytvorenie podpisu (Nastavenie podpisu).

› **Režim overenia**

Ak otvoríte už podpísaný dokument, na Paneli podpisu sa zobrazia informácie o podpise/podpisoch a výsledku jeho/ich overenia (Výsledok overenia).

Po otvorení dokumentu aplikácia umožňuje vykonať aj nasledovné činnosti prístupné cez horné menu hlavného okna aplikácie:

- › zmeniť veľkosť zobrazenia v náhľade („Zobrazit' -> Zväčšenie.../Zväčšiť/Zmenšiť“)
- › otvoriť dokument v externej aplikácii - otvoríte kópiu dokumentu v aplikácii, ktorú máte v operačnom systéme nastavenú ako preddefinovanú pre otvorenie daného typu súboru („Zobrazit' -> Zobrazit' v externej aplikácii“)
- › exportovať kópiu podpísaného dokumentu („Súbor -> Exportovať dokument...“)
- › vytlačiť dokument („Súbor -> Tlačiť...“) - vytlačíte iba nepodpísanú kópiu dokumentu
- › zatvoriť dokument - dokument sa zatvorí a hlavné okno aplikácie sa prepne do počiatočného stavu, ako pri spustení aplikácie („Súbor -> Zatvoriť“).

POZNÁMKA:

Väčšina položiek v menu aplikácie má priradenú aj klávesovú skratku. Jej tvar je zobrazený vždy vedľa názvu danej položky.

TIP:

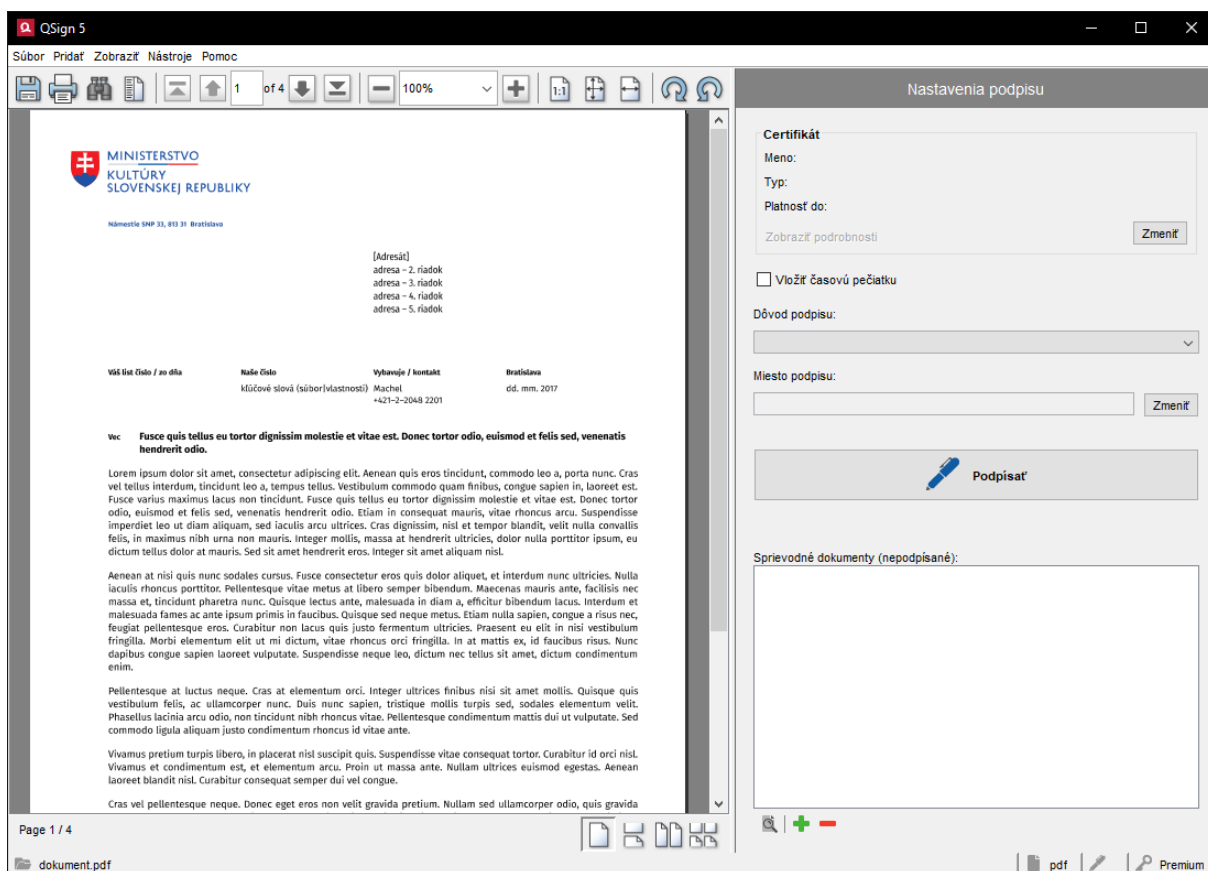
Ak máte v aplikácii otvorený dokument, ale chcete otvoriť iný, nie je potrebné otvorený dokument predtým zatvoriť. Stačí hneď otvoriť iný, jedným z možných spôsobov popísaných na začiatku tejto kapitoly.

TIP:

Funkciu **Zobraziť v externej aplikácii** použite v prípade, že nie je možné korektne zobraziť dokument v Zobrazovacej časti hlavného okna aplikácie.

4.3. Podpísanie dokumentu

Otvorením nepodpísaného dokumentu sa hlavné okno aplikácie QSign prepne do režimu podpisu, ako ukazuje nasledovný obrázok.



Podpisový režim okna je určený na vytvorenie elektronického podpisu (EP) alebo kvalifikovaného elektronického podpisu (KEP). V Zobrazovacej časti okna je zobrazený náhľad dokumentu a na paneli podpisu ovládacie prvky na nastavenie parametrov a vytvorenie podpisu.

Na vytvorenie podpisu je potrebné nastaviť podpisový certifikát. Voliteľnými parametrami sú vloženie časovej pečiatky, dôvod podpisu, miesto podpisu a sprievodné dokumenty. Predvolené nastavenie časovej pečiatky a podpisovej politiky, ktorou bude podpis vytvorený, sa vykonáva v Nastaveniach aplikácie (viď kapitola 5. *Nastavenia*).

Samotný podpis vytvoríte stlačením tlačidla „**Podpísať**“.



4.3.1. Nastavenie certifikátu

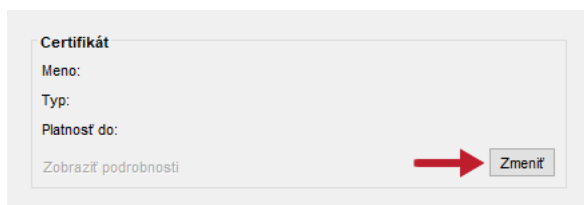
V hornej časti Panela podpisu v časti „Certifikát“ sú zobrazené základné údaje zvoleného certifikátu, ktorý sa použije na podpis. Zobrazené je tu:

- › **Meno** – meno držiteľa alebo názov certifikátu (podpisovateľa)
- › **Typ** – typ certifikátu (kvalifikovaný/mandátny/systémový)
- › **Platnosť do** – dátum, do kedy je certifikát platný

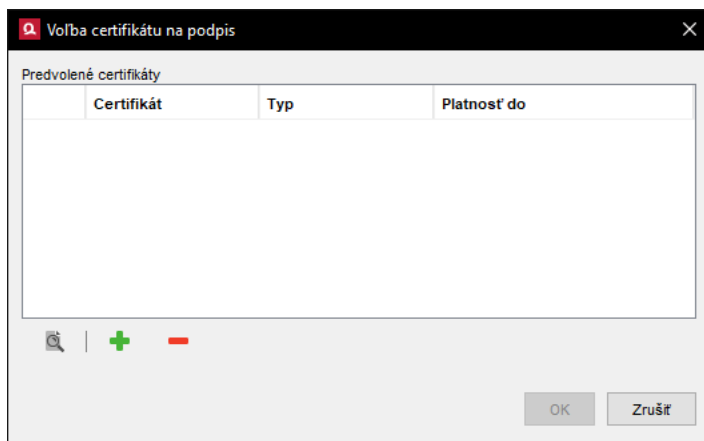
Kliknutím na „**Zobrazíť podrobnosti**“ sa zobrazí okno s parametrami certifikátu. Stlačením tlačidla „**Zmeniť**“ môžete zvoliť iný certifikát, ktorým sa bude podpisovať.

Ak nie je zobrazený žiadny certifikát alebo chcete použiť iný, podpisový certifikát nastavíte nasledovným postupom:

1. Stlačte tlačidlo „Zmeniť“.



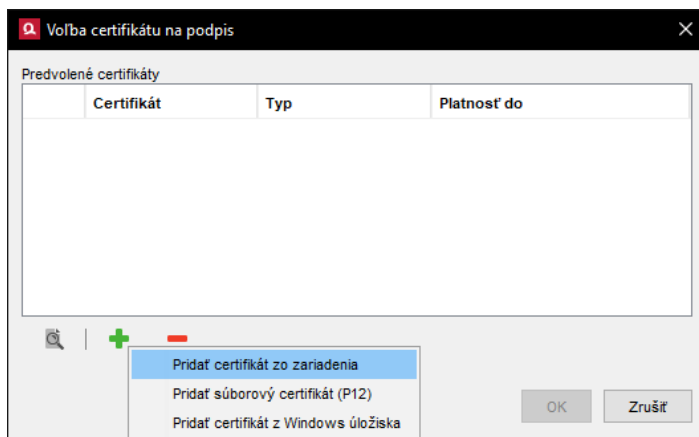
2. Zobrazí sa nasledovné okno so zoznamom predvolených certifikátov.



Ak sa v ňom nachádza požadovaný certifikát, označte ho a stlačte tlačidlo „OK“. Zvolený certifikát sa zobrazí na paneli podpisu a bude použitý ako predvolený na podpisovanie dokumentov (zakaždým, pokiaľ túto voľbu nezmeníte).

Ak je zoznam predvolených certifikátov prázdny, alebo sa v ňom požadovaný certifikát nenachádza, pokračujte nasledujúcimi krokmi.

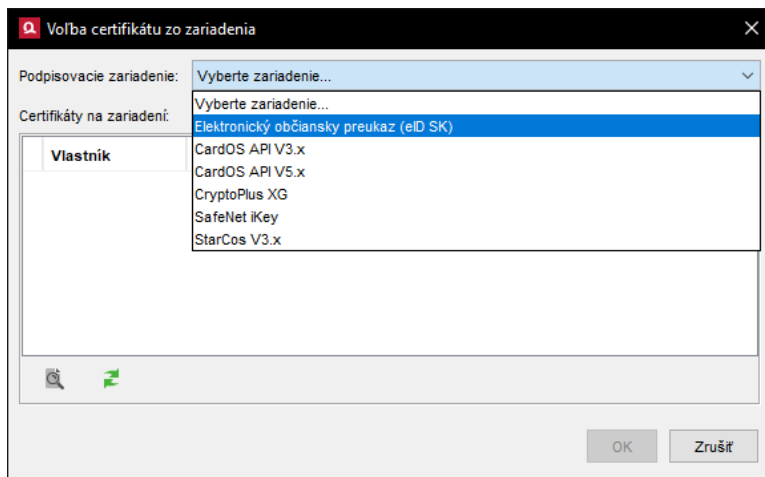
3. Stlačte tlačidlo + pre pridanie certifikátu. V prípade použitia hardvérového zariadenia zvolte „Pridať certifikát zo zariadenia“. Zobrazí sa okno pre načítanie zariadenia a certifikátu.



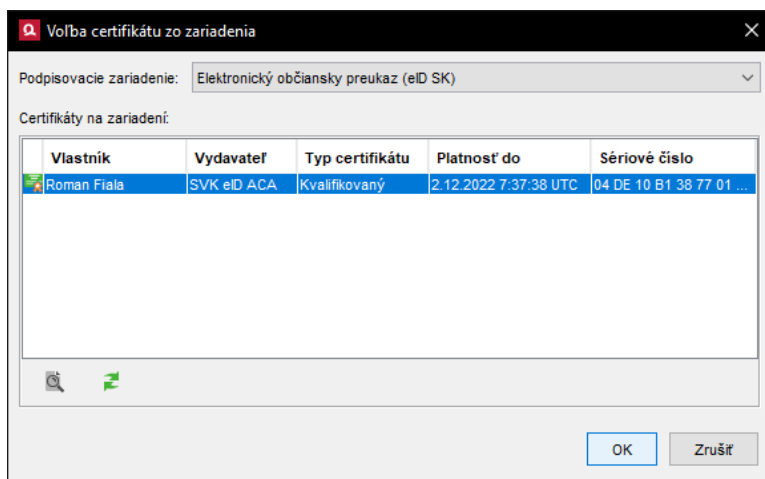
POZNÁMKA:

Predtým ako vyberiete zariadenie, uistite sa, či máte nainštalované ovládače tohto zariadenia, čítačku a čipovú kartu zasunutú do počítača. V prípade karty eID, po jej zasunutí do čítačky, počkajte na zobrazenie okna na zadanie BOK.

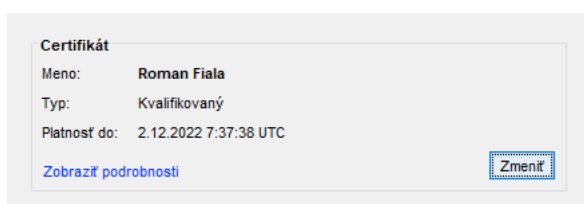
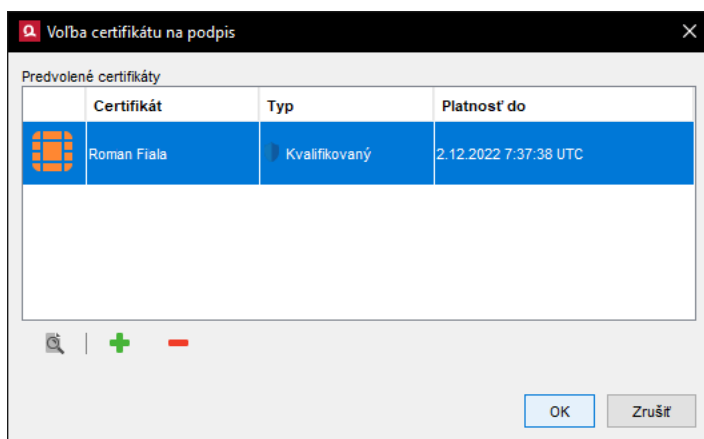
4. Vyberte podpisovacie zariadenie z rolovacieho zoznamu. Tento zoznam obsahuje všetky zariadenia, ktoré aplikácia QSign podporuje.



5. Po zvolení podpisovacieho zariadenia sa v zozname nižšie zobrazia certifikáty, ktoré sa nachádzajú na zvolenom zariadení.



6. Označte požadovaný certifikát a stlačte „OK“.
7. Zvolený certifikát sa zobrazí v zozname predvolených certifikátov. Označte ho a stlačte „OK“.



Certifikát bude použitý na podpisovanie dokumentov.

POZNÁMKA:

Naposledy použitý certifikát si aplikácia pamätá a bude nastavený aj keď aplikáciu ukončíte a znova spustíte.

4.3.2. Voliteľné parametre podpisu

Pri podpisovaní dokumentu môžete definovať aj nasledovné voliteľné parametre podpisu:

- › vloženie časovej pečiatky
- › dôvod podpisu
- › miesto podpisu
- › sprievodné dokumenty.

The screenshot shows a dialog box for configuring signature parameters. At the top, there is a checkbox labeled "Vložiť časovú pečaťku" (Add time stamp) which is currently unchecked. Below it is a dropdown menu labeled "Dôvod podpisu:" (Reason for signature). Underneath is a text input field labeled "Miesto podpisu:" (Signature location) with a "Zmeniť" (Change) button to its right. A large grey button with a blue pen icon and the text "Podpísať" (Sign) is centered below these fields. At the bottom, there is a section titled "Sprievodné dokumenty (nepodpísané):" (Attached documents (unsigned)) with a large empty rectangular area for document thumbnails. At the very bottom left, there are small icons for zooming in (+) and zooming out (-).

4.3.2.1. Časová pečaťka

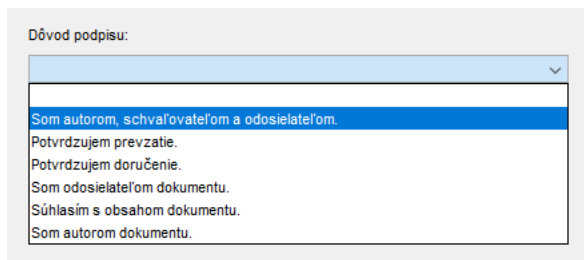
Použitím zaškrtnutého políčka „**Vložiť časovú pečaťku**“ sa vykoná vloženie časovej pečiatky do podpisu.

Vložiť časovú pečaťku

Aby bolo možné vložiť časovú pečaťku do podpisu, je potrebné nastaviť parametre časovej pečiatky v Nastaveniach aplikácie QSign (pozrite kapitolu 5.1.3 *Časové pečiatky*).

4.3.2.2. Dôvod podpisu

Táto voliteľná položka umožňuje vybrať dôvod podpisu. Zvoľte hodnotu z rolovacieho zoznamu.



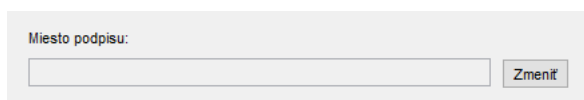
Dôvod podpisu:

- Som autorom, schvaľovateľom a odosielateľom.
- Potvrďujem prevzatie.
- Potvrďujem doručenie.
- Som odosielateľom dokumentu.
- Súhlasím s obsahom dokumentu.
- Som autorom dokumentu.

Zoznam dôvodov podpisov je pevne daný a nie je možné pridávať iné dôvody podpisu ako tie, ktoré sú definované.

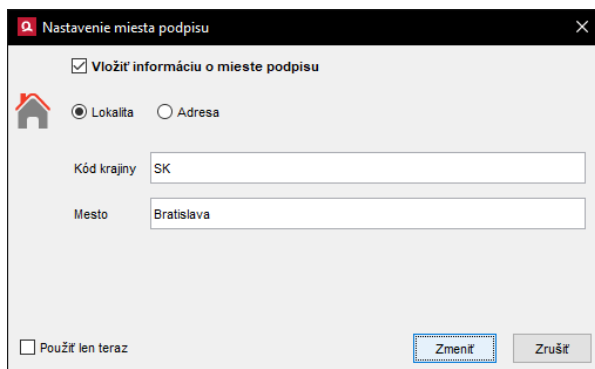
4.3.2.3. Miesto podpisu

Do podpisu je možné vložiť informácie o mieste podpisu. Stlačte „Zmeniť“ a zobrazí sa dialógové okno pre nastavenie miesta podpisu.




Miesto podpisu:

Miesto podpisu môžete zadať v dvoch rôznych formátoch: *Lokalita* alebo *Adresa*. Jednotlivé formáty sa líšia položkami zadávaných informácií. Označte, ktorý sa má použiť.



Nastavenie miesta podpisu

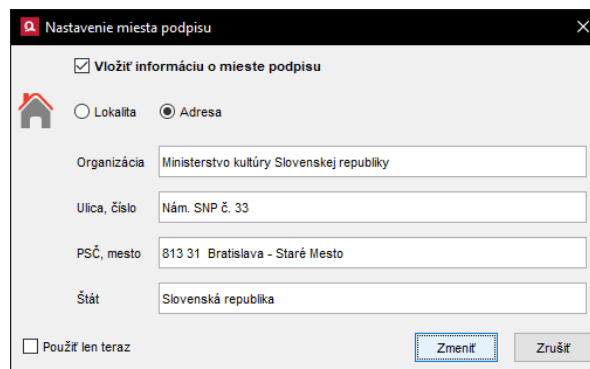
Vložiť informáciu o mieste podpisu

 Lokalita Adresa

Kód krajiny: SK


Mesto: Bratislava

Použiť len teraz



Nastavenie miesta podpisu

Vložiť informáciu o mieste podpisu

 Lokalita Adresa

Organizácia: Ministerstvo kultúry Slovenskej republiky

Ulica, číslo: Nám. SNP č. 33

PSČ, mesto: 813 31 Bratislava - Staré Mesto

Štát: Slovenská republika

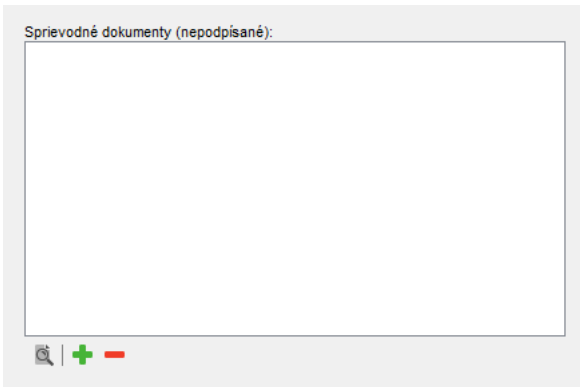
Použiť len teraz

Údaje o mieste podpisu si aplikácia zapamätá, takže aj pri ukončení a následnom spustení aplikácie ostávajú nezmenené. Výnimkou je iba zaškrtnutie políčka „Použiť len teraz“, čo znamená, že vyplnená adresa sa nezapamätá, ale použije sa iba pri najbližšom podpisovaní. Túto možnosť je vhodné použiť vtedy, ak potrebujete iba jednorazovo zmeniť miesto podpisu a nechcete, aby ostalo zapamätané.

Zaškrťavacie políčko „Vložiť informáciu o mieste podpisu“ určuje, či sa táto informácia do podpisu vloží, alebo nie. Pri nezaškrtnutom políčku tak údaje o mieste podpisu zostanú vyplnené a zapamätané, ale do podpisu sa nevložia.

4.3.2.4. Sprievodné dokumenty

Do podpisu máte možnosť pridať sprievodné súbory (prílohy), ktoré sa k podpísanému dokumentu iba priložia. **Tieto súbory sa nepodpisujú.** Vkladajú sa do zoznamu pod tlačidlom „Podpísať“.



Sprievodný dokument môžete do zoznamu pridať viacerými spôsobmi:

- › stlačte **+** a následne vyberte súbor
- › použite funkciu *Drag&Drop*: uchyťte súbor myšou, potiahnite ho nad bielu plochu so zoznamom sprievodných súborov a pustite.
- › zvolte položku „Pridať -> Sprievodný súbor“ v hornom menu hlavného okna aplikácie.

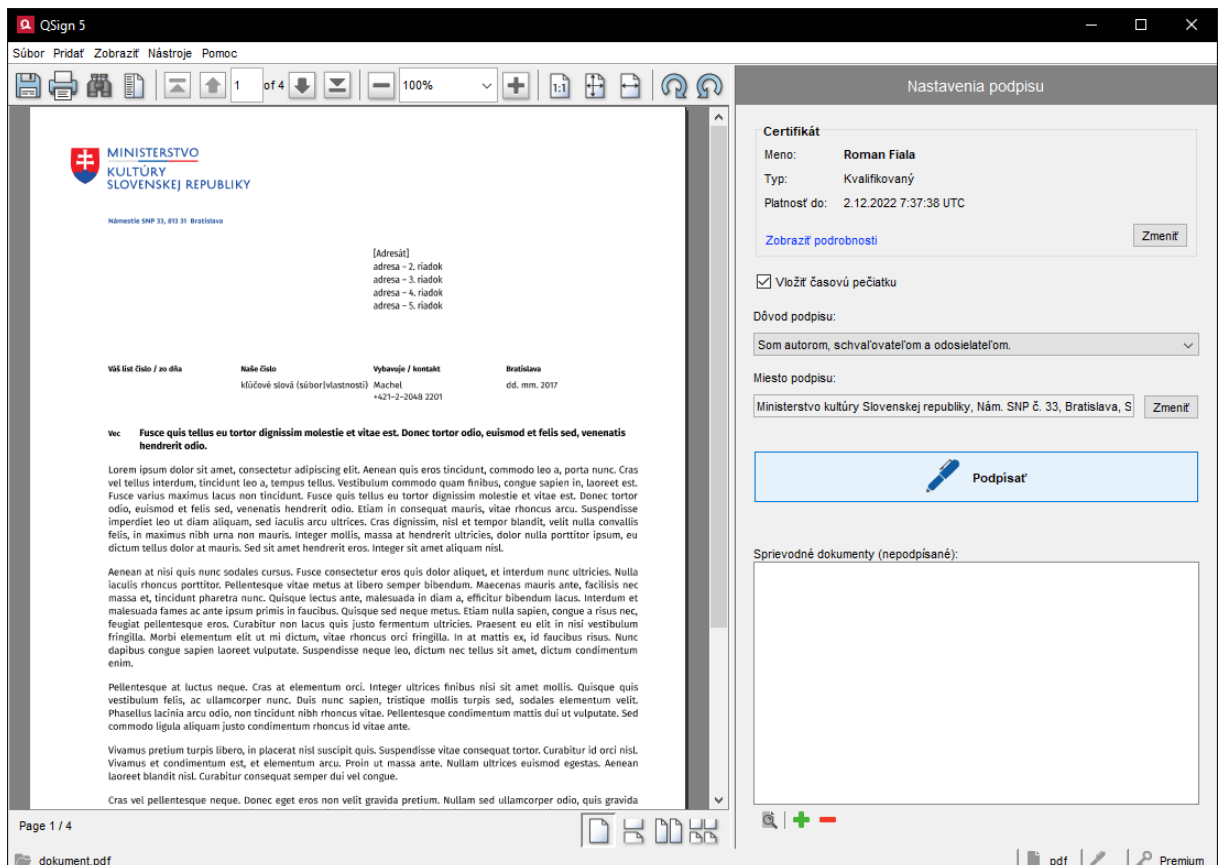
Ak chcete dokument zo zoznamu odstrániť, stlačte **-**.

POZNÁMKA:

Sprievodné dokumenty je možné pridať iba do podpisu formátu CADES.

4.3.3. Podpisovanie

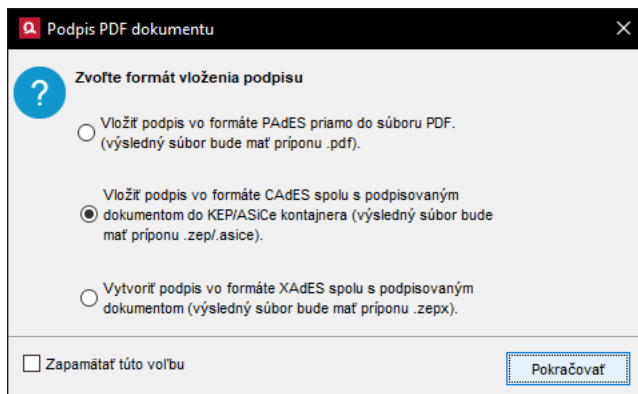
Jediným nutným nastavením na vytvorenie podpisu je mať zvolený podpisový certifikát (viď kapitola 4.3.1. *Nastavenie certifikátu*). Ak máte vykonané nastavenia podpisu, môžete pristúpiť k podpísaniu dokumentu.



1. Stlačte „**Podpísať**“.



2. Ak podpisujete dokument typu PDF, môžete byť vyzvaný na zadanie formátu vloženia podpisu.



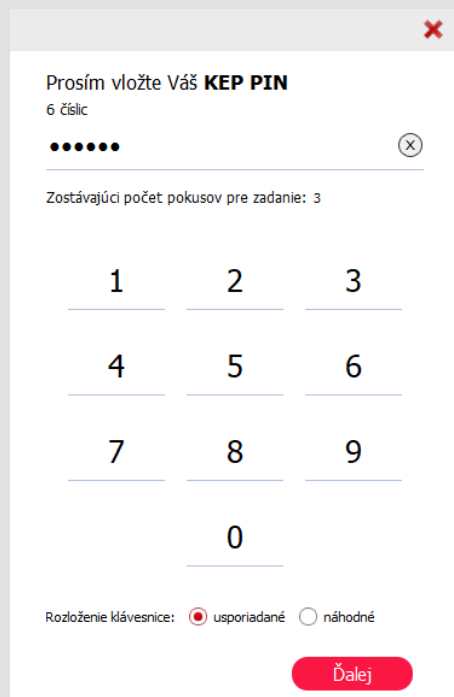
Zvoľte požadovaný formát a stlačte „**Pokračovať**“. Ak označíte „**Zapamätať túto voľbu**“, aplikácia nastaví tento formát ako predvolený. Nabudúce sa už na túto voľbu nebude pýtať. Predvolený formát vloženia podpisu sa dá potom kedykoľvek zmeniť v Nastaveniach aplikácie (pozrite kapitolu 5.1.2 *Predvolený formát podpisu*).

POZNÁMKA:

Ak zvolíte možnosť vloženia podpisu vo formáte PAdES, výsledný podpísaný dokument bude uložený znova vo formáte PDF (pozrite krok 4.).

3. Zadajte heslo alebo PIN kód (KEP PIN) pre podpisovacie zariadenie.

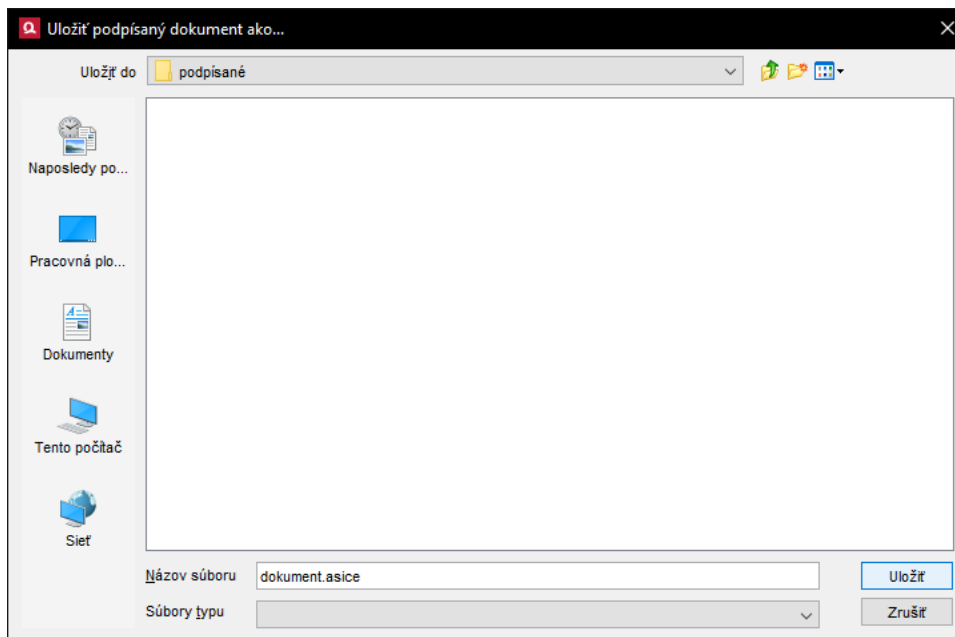
Dialóg na zadanie PIN kódu je zobrazený maximálne po dobu 20 sekúnd. Ak do tohto časového limitu nestihnete zadať PIN, z bezpečnostných dôvodov sa dialóg sám zatvorí a proces podpisovania sa tak preruší.



POZNÁMKA:

Dialóg na zadávanie PIN kódu sa môže líšiť podľa toho, akým zariadením podpisujete.

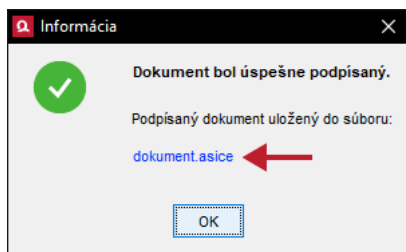
4. Začne sa proces podpisovania, ktorý môže trvať niekoľko sekúnd. Po jeho skončení sa zobrazí dialógové okno, kde zadajte umiestnenie a názov podpísaného dokumentu a stlačte „Uložiť“.



POZNÁMKA:

Pokiaľ zvolíte možnosť vloženia podpisu vo formáte PAdES, názov ukladaného dokumentu, ak ho nezmeníte, bude obsahovať predvolené slovo „podpisane“.

5. Po úspešnom podpísaní a uložení dokumentu sa zobrazí nasledovné okno. V prípade chyby sa zobrazí okno s upozornením na danú chybu.



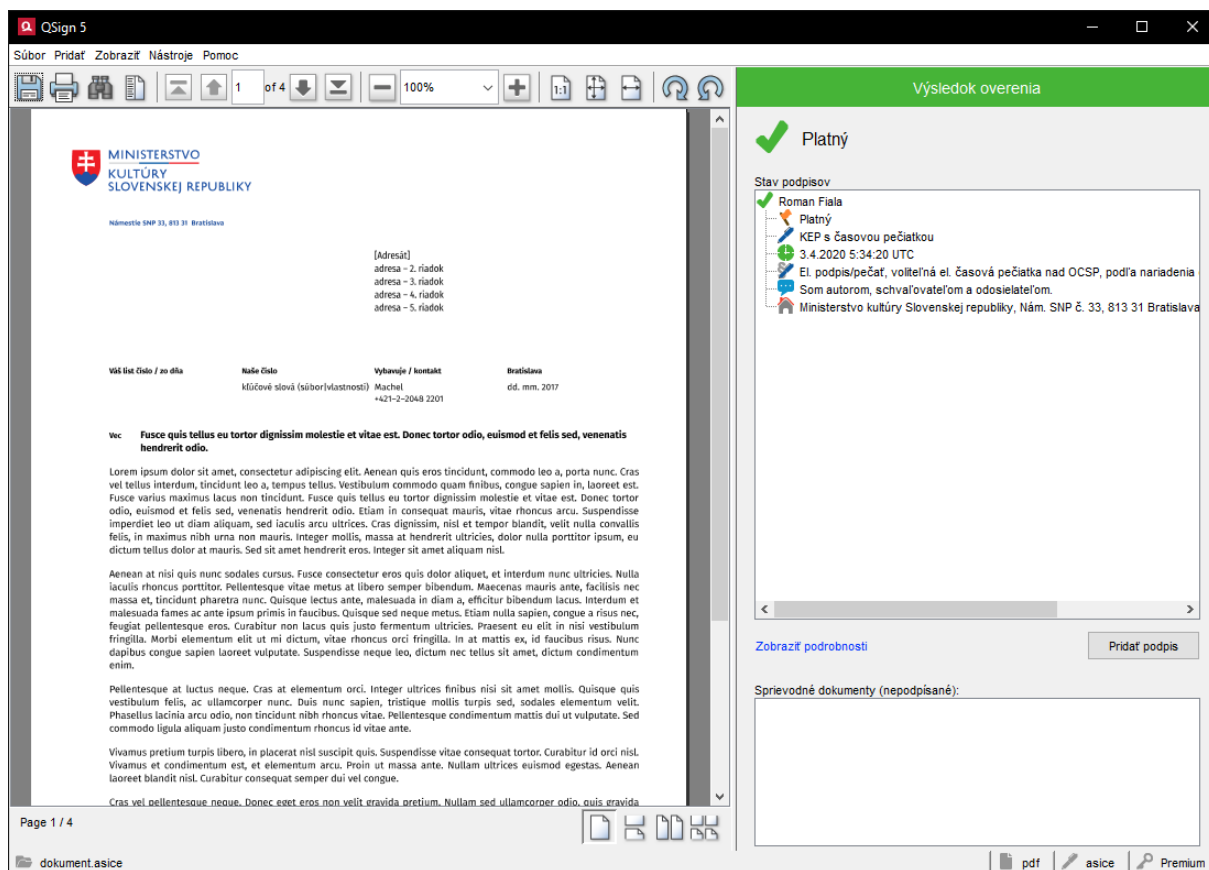
Kliknutím na odkaz názvu podpísaného dokumentu (ako ukazuje šípka) je možné tento podpísaný dokument hneď aj otvoriť a automaticky overiť. Inak okno zatvorte stlačením „OK“.

UPOZORNENIE:

Dokumenty typu PDF budú po podpise konvertované do formátu PDF/A-2b verzie 1.7 (podľa ISO 19005-2:2011) s výnimkou PDF dokumentov, ktoré už boli pred podpisom vo formáte PDF/A-1 alebo PDF/A-2b verzie 1.3 a 1.4, alebo boli už podpísané (len pridávate ďalší podpis).

4.4. Overenie podpisu

Otvorením podpísaného dokumentu sa hlavné okno aplikácie QSign prepne do režimu overenia.



4.4.1. Výsledok overenia

Po overení podpísaného dokumentu sa v Paneli podpisu hlavného okna aplikácie (v režime overenia) zobrazí výsledok overenia.

Panel zobrazuje nasledovné časti:

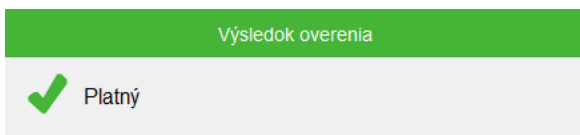
- › výsledný stav overenia
- › upozornenia
- › stav podpisov
- › sprievodné dokumenty

4.4.1.1. Výsledný stav overenia

Výsledný stav overenia môže nadobudnúť tieto stavy:

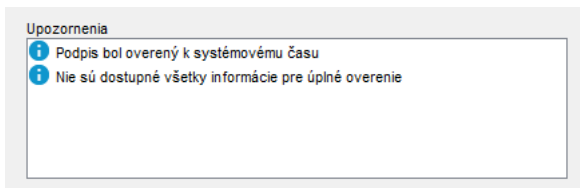
- ✓ **Platný** - aspoň jeden z podpisov dokumentu je platný
- ? **Neúplné overenie** - ak žiaden z podpisov nemá stav Platný, pričom aspoň jeden nadobúda stav neúplného overenia (viac v kapitole 6.5. *Neúplné overenie*)
- ? **Neúplné automatické overenie** - ak neplatia predchádzajúce podmienky a aspoň jeden z podpisov nadobúda stav neúplného automatického overenia (viac v kapitole 6.6. *Neúplné automatické overenie*)
- ✗ **Neplatný** - všetky podpisy dokumentu sú neplatné

Zároveň je daný stav reprezentovaný aj ikonou a farbou pozadia hornej lišty Panelu podpisu.



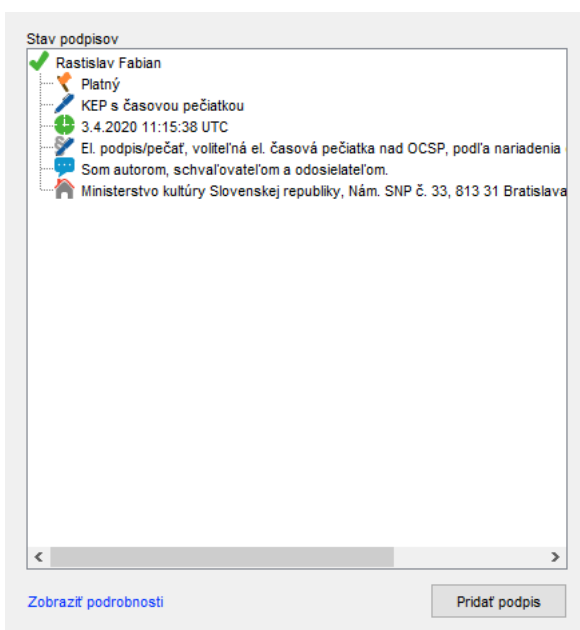
4.4.1.2. Upozornenia

V časti „Upozornenia“, ktorá sa zobrazí len ak nastane dôvod na zobrazenie upozornenia, sa môžu zobraziť hlásenia týkajúce sa výsledku overenia, ako napr. „*Neplatná časová pečiatka*“, „*Podpis bol overený k systémovému času*“, „*Dokument obsahuje Java skripty*“ a pod.



4.4.1.3. Stav podpisov







Táto časť zobrazuje zoznam všetkých podpisov daného dokumentu, kde každý podpis je reprezentovaný podpisovateľom nasledovne:



✓ **Názov certifikátu podpisovateľa**

Ikona pred názvom zobrazuje stav overenia podpisu daného podpisovateľa (použité sú rovnaké symboly ako pre výsledný stav overenia). Názov certifikátu je meno alebo názov držiteľa certifikátu.

Ku každému podpisu sú potom priradené nasledujúce parametre:

-  stav podpisu
-  typ podpisu
-  dátum a čas, ku ktorému sa podpis overil
-  vložená podpisová politika
-  dôvod podpisu
-  miesto podpisu.

POZNÁMKA:

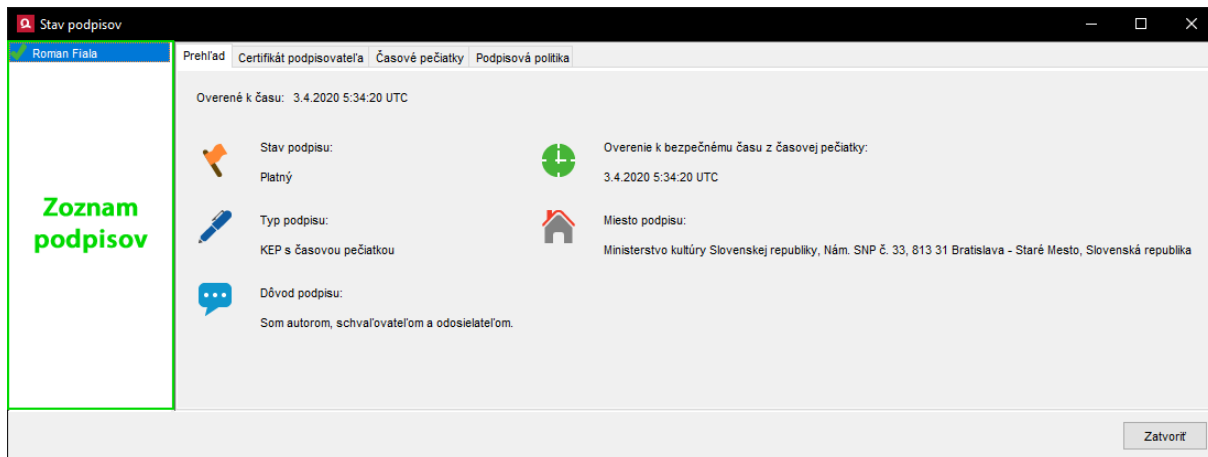
Ak podpis neobsahuje niektorý z parametrov, znamená to, že ide o niektorý z voliteľných parametrov podpisu (viď kapitola 4.3.2. *Voliteľné parametre podpisu*) a daný podpis bol vytvorený bez vloženia tohto parametra.

4.4.1.4. Sprievodné dokumenty

Sprievodné dokumenty zobrazujú zoznam príloh, ktoré však nie sú podpísané. Každý súbor prílohy je možné zvlášť otvoriť v prednastavenom programe alebo uložiť do zvoleného priečinka. Prílohy je možné exportovať naraz cez horné menu „**Súbor -> Exportovať sprievodné súbory...**“.

4.4.2. Podrobnosti overenia

Kliknutím na odkaz „**Zobrazit' podrobnosti**“ pod časťou Stav podpisov (viď kapitola 4.4.1.3 Stav podpisov) sa otvorí okno *Stav podpisov*, ktoré umožňuje zobrazit' všetky podrobnosti overenia dokumentu pre každý podpis zvlášť.



V ľavej časti okna sa nachádza **Zoznam podpisov** dokumentu. Kliknutím na meno/názov podpisovateľa sa v pravej časti okna zobrazia podrobnosti daného podpisu a jeho overenia, ktoré sú rozdelené na tieto záložky:

- › **Prehľad** - zobrazuje základné informácie o podpise (tie isté ako v časti „Stav podpisov“ na Paneli podpisu hlavného okna aplikácie)
- › **Certifikát podpisovateľa** - zobrazuje podrobné informácie o certifikáte podpisovateľa
- › **Časové pečiatky** - zoznam a parametre vložených časových pečiatok
- › **Podpisová politika** - údaje o podpisovej politike použitej na podpis.

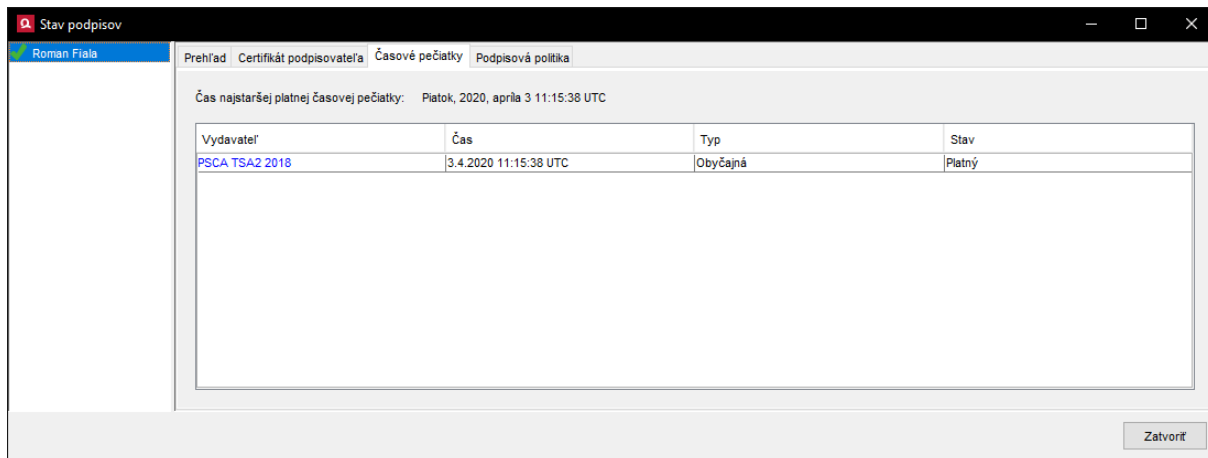
4.4.2.1. Certifikát podpisovateľa

Na tejto záložke sú zobrazené základné informácie o certifikáte podpisovateľa. V hornej časti je uvedená certifikačná cesta daného certifikátu. Na zobrazenie všetkých informácií kliknite na odkaz „**Zobrazit' podrobnosti**“.



4.4.2.2. Časové pečiatky vložené do podpisu

Záložka Časové pečiatky obsahuje tabuľku so zoznamom časových pečiatok vložených do podpisu. Nad tabuľkou je uvedený čas najstaršej platnej pečiatky. Dvojitým kliknutím na príslušný riadok časovej pečiatky v tabuľke zobrazíte podrobnosti o certifikáte danej časovej pečiatky.



4.4.2.3. Podpisová politika podpisu

Na záložke Podpisová politika sú uvedené informácie o podpisovej politike, ktorá bola pri podpísaní dokumentu určená podpisovateľom a podľa nej sa aj podpis overil. Na zobrazenie všetkých informácií o podpisovej politike kliknite na odkaz „Zobrazit' podrobnosti“.



POZNÁMKA:

Ak chcete podpis overiť voči inej podpisovej politike, alebo v podpise nebola podpisová politika určená, zvolte v hornom menu hlavného okna aplikácie voľbu „**Nástroje -> Overiť k politike...**“. V zozname súborov podpisových politík, ktoré sú v aplikácii importované (pozrite kapitolu 5.2.4. Podpisové politiky) označte príslušný riadok a stlačte „OK“. Podpis sa overí znova voči zvolenej podpisovej politike.

4.4.2.4. Pridanie časovej pečiatky

Ak v podpise nie je vložená časová pečiatka alebo chcete pridať ďalšiu, môžete tak urobiť cez voľbu v hornom menu aplikácie „**Pridať -> Časovú pečiatku**“.

4.5. Viacnásobný podpis

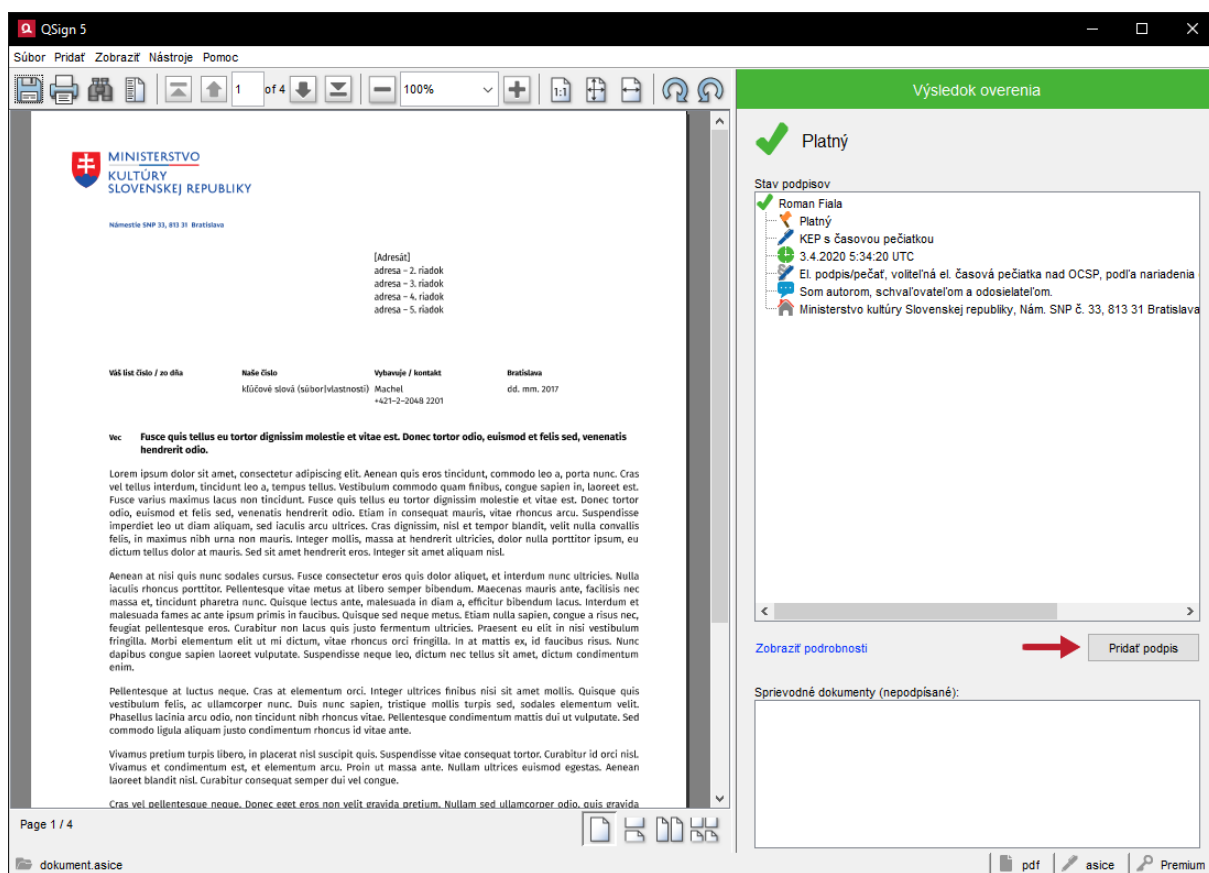
Aplikácia QSign umožňuje aj podpisovanie elektronických dokumentov dvoma a viac podpismi. V takom prípade hovoríme o viacnásobnom elektronickom podpise.

V súčasnej verzii aplikácie sú podporované viacnásobné nezávislé podpisy, čo znamená, že poradie, v akom ich jednotliví podpisovatelia vytvárajú (podpisujú dokument), nie je podstatné. Je tak možné podpisovať napríklad kúpno-predajné zmluvy alebo iné dokumenty, pri ktorých nezáleží na tom, v akom poradí majú byť podpísané.

Pri vytváraní viacnásobného podpisu sa dokument podpisuje postupne vždy vytvorením jedného podpisu s nastavením vlastných parametrov podpisu daného podpisovateľa zvlášť. Následne po overení tohto podpisu sa môže pridať ďalší podpis inej osoby.

Viacnásobný podpis vytvoríte podľa nasledovného postupu:

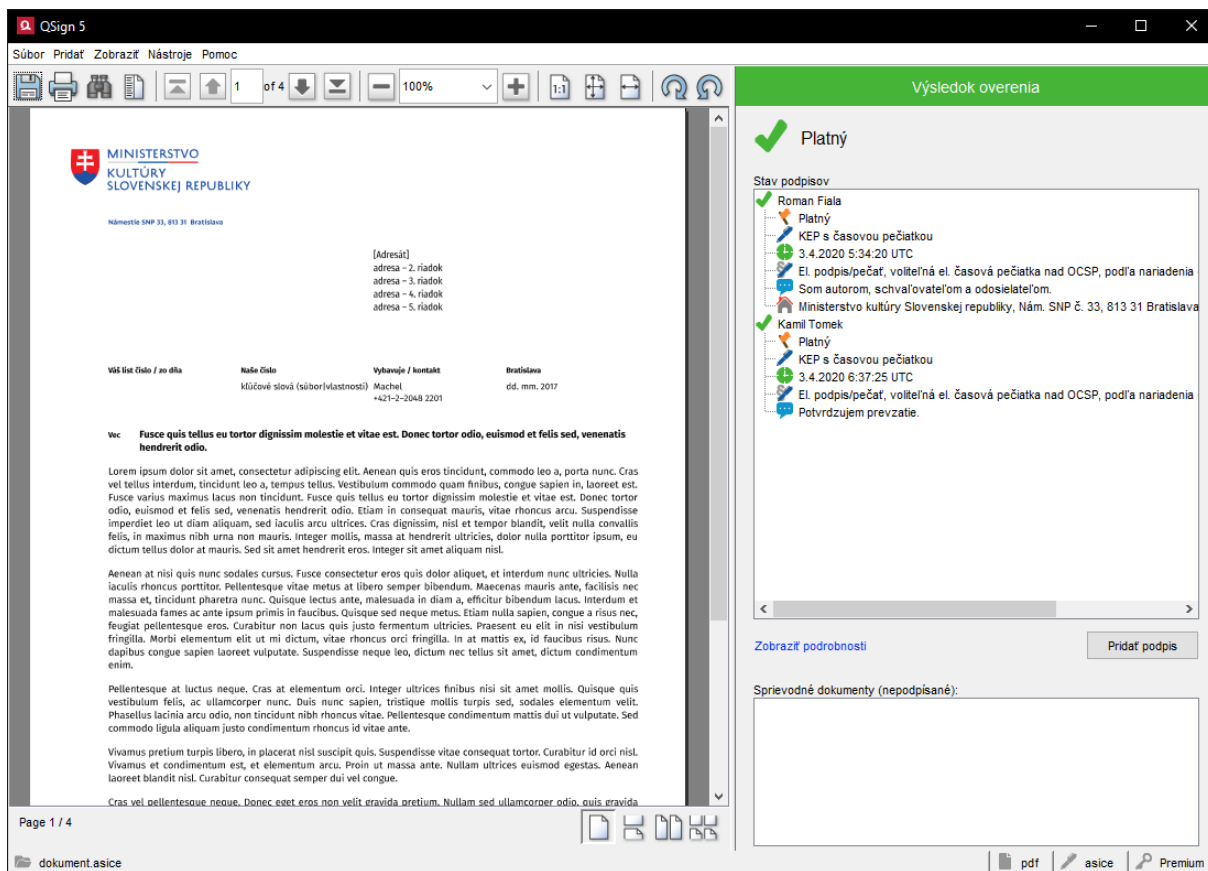
1. Otvorte už podpísaný dokument.



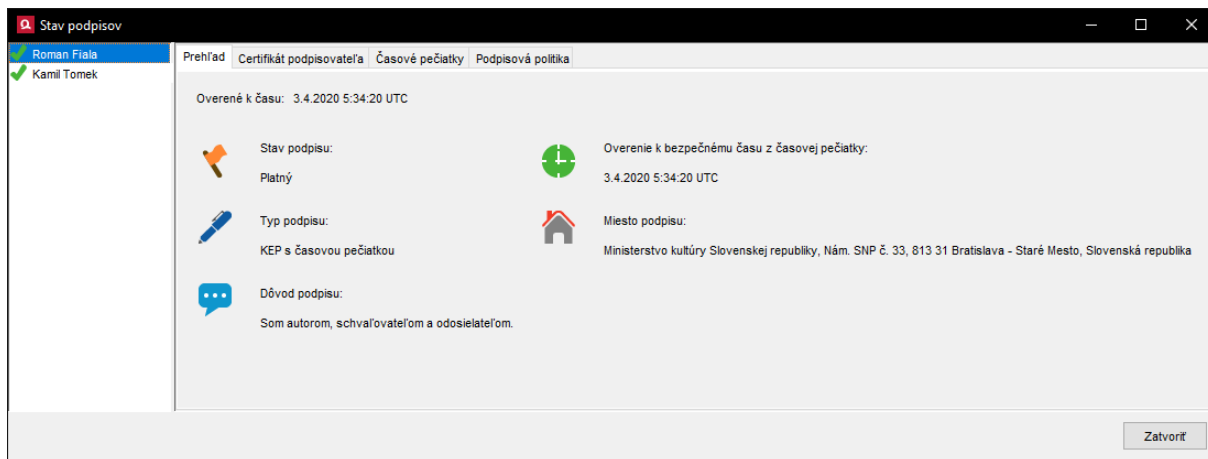
Dokument na obrázku obsahuje jeden podpis, ktorý vytvorila osoba s menom Roman Fiala.

2. Kliknite na tlačidlo „**Pridať podpis**“ na Paneli podpisu alebo zvolte položku „**Pridať** -> **Pridať podpis**“ v hornom menu aplikácie.
3. Hlavné okno sa prepne do režimu podpisu. Na Paneli podpisu sa tak namiesto informácií o overení zobrazia ovládacie prvky na nastavenie parametrov a vytvorenie podpisu. Od tohto kroku je vytvorenie viacnásobného podpisu už identické s bežným podpisovaním.
4. Nastavte parametre podpisu a stlačte tlačidlo „**Podpísať**“.
5. Ak chcete pridať ďalší podpis, takto podpísaný dokument znova otvorte a vykonajte tento postup od začiatku.

Po otvorení a overení dokumentu s viacnásobným podpisom sa na Paneli podpisu v časti „Stav podpisov“ zobrazia jednotlivé podpisy s ich parametrami označené menom/názvom certifikátu podpisovateľa, pred ktorým je ikona stavu overenia daného podpisu (pozrite kapitolu 4.4.1. *Výsledok overenia*).



Keďže ide o nezávislé podpisy, poradie, v akom sa podpisy zobrazia, je určené stavom, v akom sa každý podpis nachádza. Najprv sa zobrazia všetky platné podpisy, potom podpisy s neúplným overením a na záver neplatné podpisy. V rovnakom poradí sa podpisy zobrazia aj v okne *Stav podpisov* (otvorte kliknutím na odkaz „Zobraziť podrobnosti“).



4.6. Hromadný podpis

Funkcia hromadného podpisu (alebo tiež „dávkové podpisovanie“) umožňuje podpísať väčšie množstvo dokumentov naraz (v jednej dávke). Na rozdiel od viacnásobného podpisu, pri ktorom sa jeden dokument podpíše viacerými podpismi, pri hromadnom podpise sa podpíše jedným podpisom každý zvolený dokument samostatne.

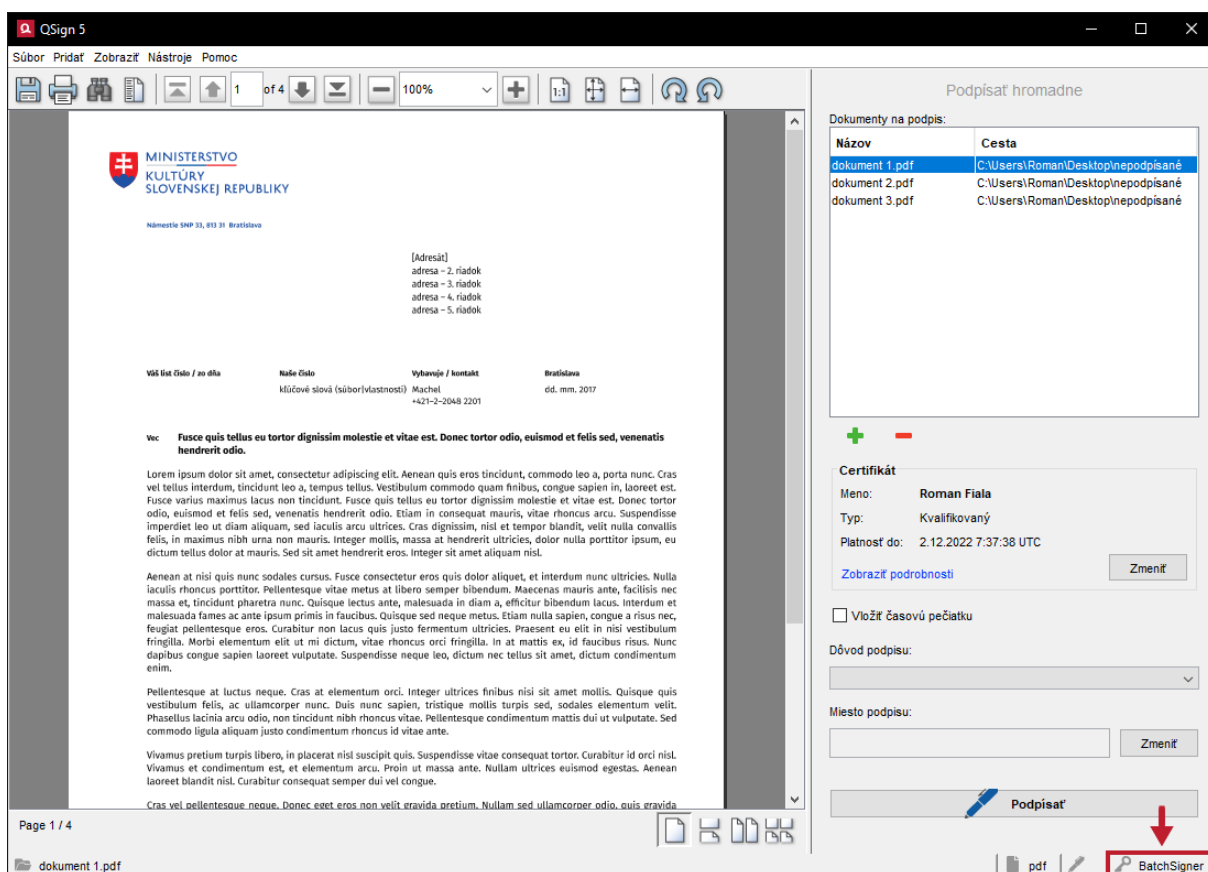
UPOZORNENIE:

Funkciu hromadného podpisovania nie je možné plnohodnotne použiť s eID kartou (elektronickým občianskym preukazom), ale iba so zariadením, ktoré nevyžaduje zadávanie sekundárneho PIN kódu. V opačnom prípade budete musieť KEP PIN zadať pri podpise každého dokumentu z podpisovanej dávky.

POZNÁMKA:

Na použitie funkcie hromadného podpisovania je potrebné mať aplikáciu QSign aktivovanú príslušnou licenciou (viď nasledujúci obrázok).

Jedným úkonom môže podpisovateľ pridať podpis do viacerých dokumentov bez toho, aby do procesu podpisovania musel nejako zasahovať. Stačí len navoliť zoznam dokumentov na podpis a nastaviť vstupné parametre podpisu (certifikát, časovú pečiatku a pod.).



Hromadné podpisovanie vykonáte podľa nasledovného postupu:

1. V hornom menu hlavného okna aplikácie zvolíte „Súbor -> Hromadný podpis“.

POZNÁMKA:

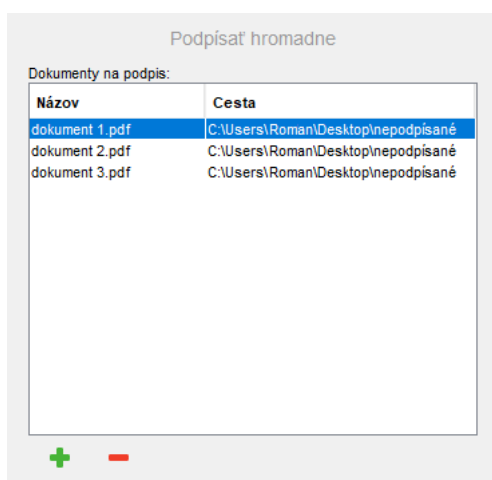
Ak už máte otvorený dokument pre obyčajné podpisovanie, zvolením tejto položky menu sa dokument automaticky pridá do zoznamu pre hromadný podpis. Stačí potom len pridať ostatné dokumenty.

2. Aplikácia sa prepne do režimu hromadného podpisu. Na Paneli podpisu sa oproti obyčajnému režimu podpisu zobrazí navyše zoznam dokumentov na podpis (môže byť zatiaľ prázdny).

POZNÁMKA:

Pre hromadné podpisovanie nie je možné pridávať sprievodné dokumenty. Táto položka nastavenia tu teda chýba.

3. Do tabuľky „*Dokumenty na podpis*“ pridajte požadované dokumenty.



Dokument môžete do zoznamu pridať viacerými spôsobmi:

- › stlačte **+** a následne vyberte súbor
- › použite funkciu *Drag&Drop*: uchytte súbor myšou, potiahnite ho nad bielu plochu so zoznamom sprievodných súborov a pustite.

Ak chcete dokument zo zoznamu odstrániť, stlačte **-**.

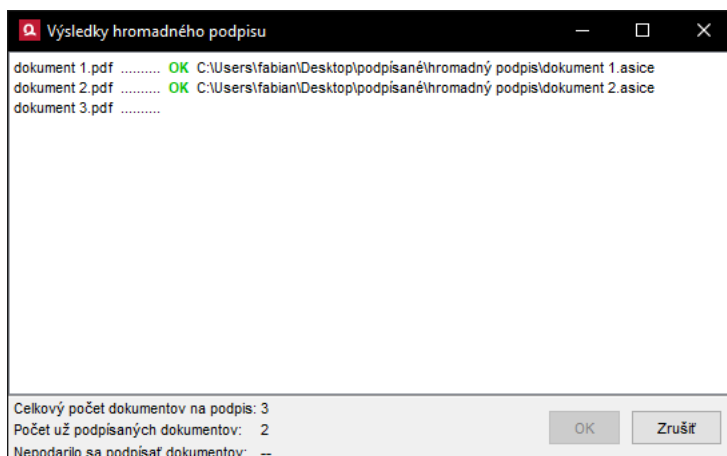
Označte riadok s názvom dokumentu v zozname a v Zobrazovacej časti sa zobrazí náhľad označeného dokumentu.

4. Nastavte podpisový certifikát (viď kapitola 4.3.1. *Nastavenie certifikátu*) a voliteľné parametre podpisu (viď kapitola 4.3.2. *Voliteľné parametre podpisu*) a stlačte „**Podpísať**“.

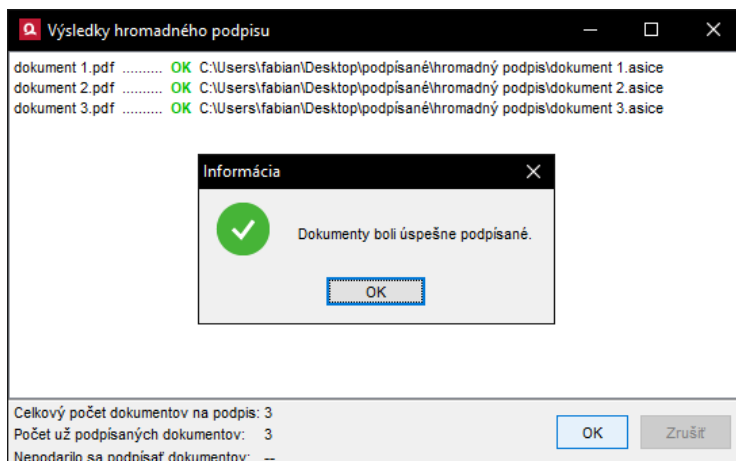
UPOZORNENIE:

Ak podpisujete aj dokumenty formátu PDF, pred spustením podpisovania sa uistíte aký formát vloženia podpisu PDF dokumentov máte predvolený v nastaveniach aplikácie (viď kapitola 5.1.2. *Predvolený formát podpisu*). Ak je nastavená voľba „Spýtať sa“, pri každom PDF dokumente budete vyzvaný na výber formátu, čo pri väčšom počte dokumentov môže byť pre vás nekomfortné a stráca sa tým výhoda hromadného podpisovania. Preto odporúčame túto voľbu preddefinovať.

5. Zadajte PIN pre podpisovacie zariadenie a stačte „OK“.
6. Zvoľte cieľový priečinok, kam sa majú podpísané dokumenty uložiť.
7. Začne sa podpisovanie. V okne „Výsledky podpisu“ sa postupne zobrazuje priebeh a výsledok podpisovania jednotlivých dokumentov.



8. Po dokončení procesu podpisovania sa zobrazí informačné dialógové okno. Okná zatvoríte stlačením „OK“.



9. Režim hromadného podpisovania ukončíte voľbou „Súbor -> Zatvoriť“ v hornom menu hlavného okna aplikácie alebo len hlavné okno zatvorte.

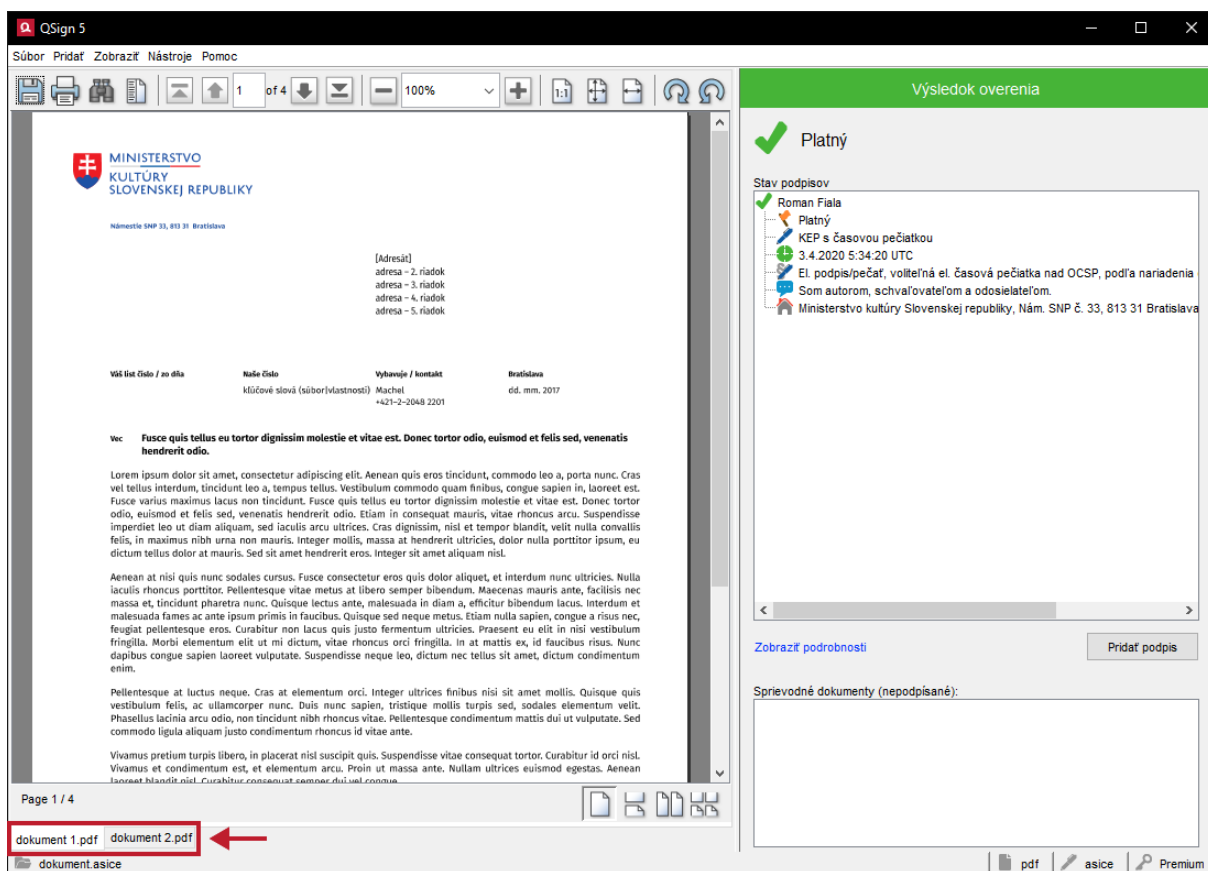
4.7. Podpis viacerých dokumentov

V prípade, že potrebujete podpísať viac dokumentov, ktoré budú navzájom tvoriť neoddeliteľnú súčasť v jednom podpisovom kontajneri (t.j. spojiť dokumenty spoločným jedným podpisom), zvolte menu „Súbor -> Spojenie podpisom“.

Na rozdiel od hromadného podpisovania, kde každý dokument sa podpisuje samostatne v jednej dávke (pozrite kapitolu 4.6. *Hromadný podpis*), v tomto prípade je jedným podpisom podpísaných viac dokumentov spoločne a uložených do jedného kontajnera formátu ASiC-E. To znamená, že výsledkom je jeden súbor s príponou *.asice*.

Postup podpisovania je obdobný ako pri hromadnom podpise, viď kapitola 4.6. *Hromadný podpis*.

Po otvorení takéhoto súboru náhľady jednotlivých dokumentov je možné zobraziť kliknutím na záložku v Zobrazovacej časti hlavného okna aplikácie.



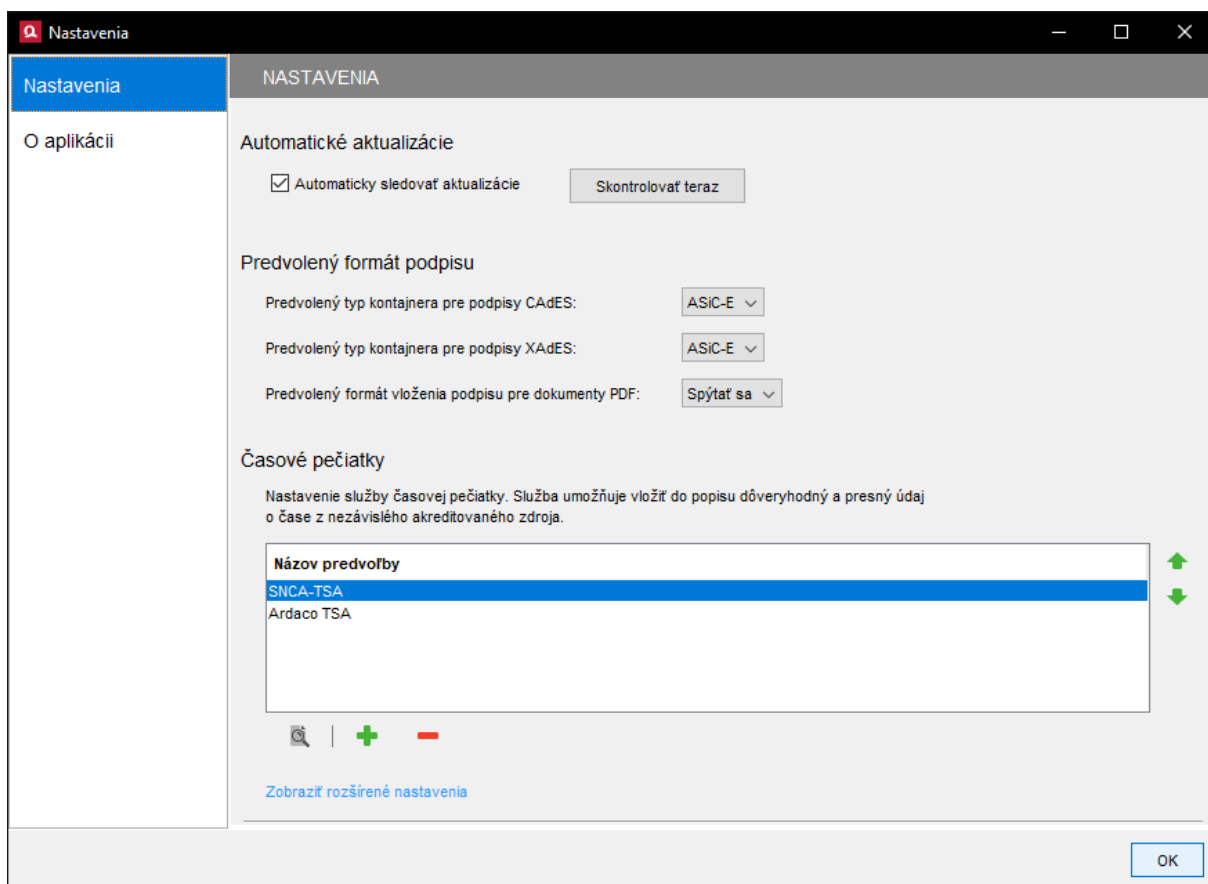
5. Nastavenia

Nastavenia aplikácie je možné vykonať v okne „Nastavenia“, ktoré zobrazíte voľbou „**Nástroje** -> **Nastavenia**“ v hornom menu hlavného okna aplikácie.

V okne sú zobrazené primárne len základné nastavenia. Ďalšie nastavenia je možné zobrazit' kliknutím na odkaz „**Zobrazit' rozšírené nastavenia**“.

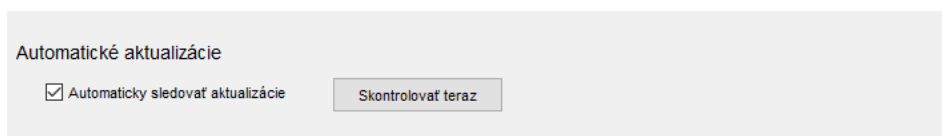
5.1. Základné nastavenia

Základné nastavenia ponúkajú možnosti, ktoré sú pre funkcionality aplikácie najčastejšie používané alebo používateľom častejšie menené.



5.1.1. Automatické aktualizácie

Stlačte tlačidlo „**Skontrolovať teraz**“ aby aplikácia vykonala kontrolu, či je k dispozícii novšia verzia aplikácie. Túto kontrolu môže aplikácia vykonávať automaticky pri spustení, ak zaškrtnete voľbu „**Automaticky sledovať aktualizácie**“.



Ak je aktualizácia dostupná, budete na to upozornený hlásením. V takom prípade na vykonanie aktualizácie zvolte „**Pomoc** -> **Skontrolovať aktualizácie**“ v hlavnom menu aplikácie.

5.1.2. Predvolený formát podpisu

Predvolený formát podpisu

Predvolený typ kontajnera pre podpisy CADES:

Predvolený typ kontajnera pre podpisy XAdES:

Predvolený formát vloženia podpisu pre dokumenty PDF:

Časové pečiatky

Nastavenie služby časovej pečiatky. Služba umožňuje vložiť vhodný a presný údaj o čase z nezávislého akreditovaného zdroja.

Spýtať sa
PADES
CADES
XAdES

5.1.2.1. Predvolený typ kontajnera pre podpisy CADES

Typ kontajnera pre podpisy CADES určuje, do akého formátu sa zabalí podpísaný dokument spolu s informáciami o samotnom podpise. Na výber sú formáty:

- › **ZEP** - formát KEP vytvorený pre potreby slovenskej legislatívy
- › **ASiC-E** - medzinárodným štandard, aplikácia QSign podporuje špecifikáciu ASiC-E (Extended Associated Signature Container).

5.1.2.2. Predvolený typ kontajnera pre podpisy XAdES

Typ kontajnera pre podpisy XAdES určuje, do akého formátu sa zabalí podpísaný dokument spolu s informáciami o samotnom podpise. Na výber sú formáty:

- › **ZEPx** - formát KEP vytvorený pre potreby slovenskej legislatívy
- › **ASiC-E** - medzinárodným štandard, aplikácia QSign podporuje špecifikáciu ASiC-E (Extended Associated Signature Container).

5.1.2.3. Predvolený formát vloženia podpisu pre dokumenty PDF

Pri podpise dokumentov formátu PDF máte možnosť zvoliť, do akého formátu sa podpis vytvorí. Na výber sú možnosti:

- › **PADES** - podpis je vytvorený a vložený priamo do súboru PDF, kedy formát podpísaného dokumentu zostáva nezmenený („.pdf“)
- › **CADES** - podpis je vytvorený a vložený spolu s podpisovaným dokumentom do ZEP/ASiC kontajnera, kedy formát podpísaného dokumentu sa zmení na „.zep/.asice“.
- › **XAdES** - podpis je vytvorený a vložený spolu s podpisovaným dokumentom do ZEPx/ASiC kontajnera, kedy formát podpísaného dokumentu sa zmení na „.zepx/.asice“.

Ak ponecháte nastavenú voľbu „**Spýtať sa**“, aplikácia si pri každom podpisovanom PDF dokumente vyžiada, aby ste zvolili jeden zo spomínaných formátov vloženia podpisu.

Pri iných formátoch dokumentov táto voľba formátu podpisu nie je možná.

POZNÁMKA:

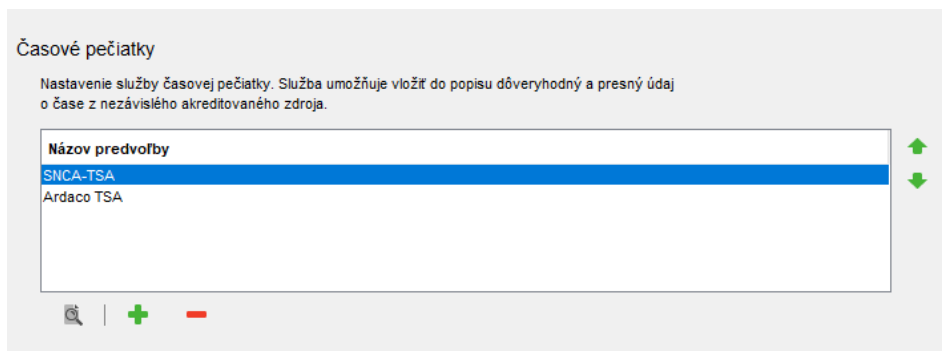
Pri používaní funkcie hromadného podpisu odporúčame nastaviť (predvoliť) jeden z týchto formátov.



UPOZORNENIE:




Dokumenty typu PDF budú po podpise konvertované do formátu PDF/A-2b verzie 1.7 (podľa ISO 19005-2:2011) s výnimkou PDF dokumentov, ktoré už boli pred podpisom vo formáte PDF/A-1 alebo PDF/A-2b verzie 1.3 a 1.4, alebo boli už podpísané (len pridávate ďalší podpis).

5.1.3. Časové pečiatky

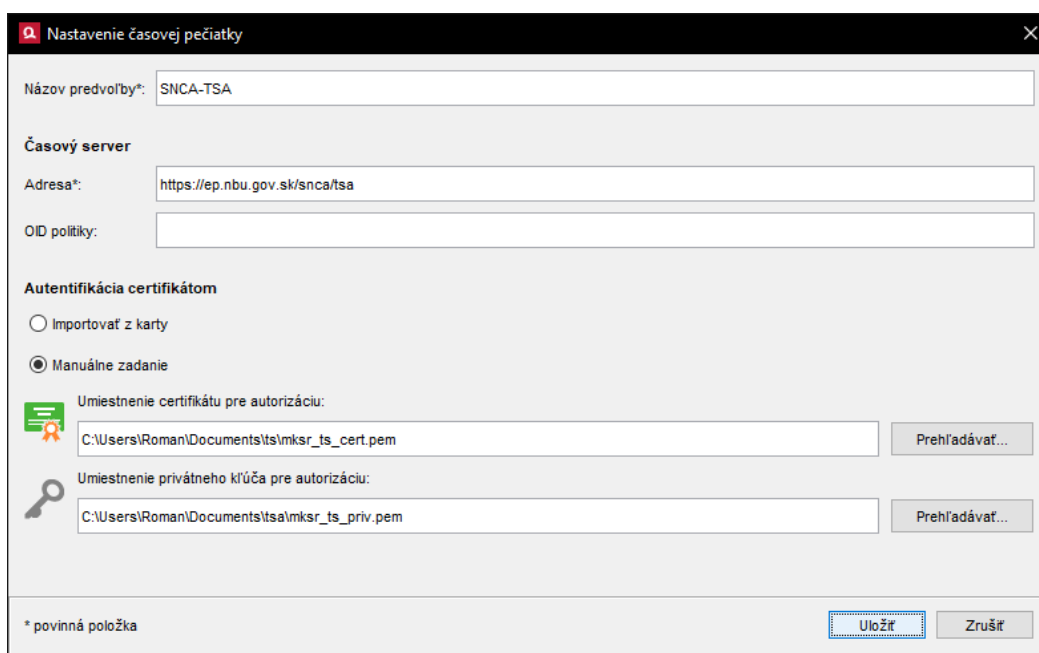
V tejto časti nastavení sa nachádza zoznam predvolieb parametrov pre nastavenie služby časovej pečiatky, ktorá poskytuje presný dátum a čas, ktorý aplikácia potom vloží do podpisu.



Službu časovej pečiatky môžete využívať od rôznych poskytovateľov, preto máte možnosť definovať viac predvolieb, ktoré sa budú nachádzať v tomto zozname, pričom pri podpise sa použije prvá predvoľba v tomto zozname. Poradie predvolieb v zozname zmeníte pomocou tlačidiel  a  napravo od zoznamu.

Na vytvorenie predvoľby nastavenia časovej pečiatky stlačte . Predvoľbu zo zoznamu odstránite kliknutím na . Ak chcete už vytvorenú predvoľbu zmeniť, kliknite na .

Do prvej položky („**Názov predvoľby**“) zadajte ľubovoľný vami určený názov nastavenia predvoľby. Zvyšné položky slúžia na zadanie parametrov, ktoré ste obdržali poskytovateľa služby časovej pečiatky.



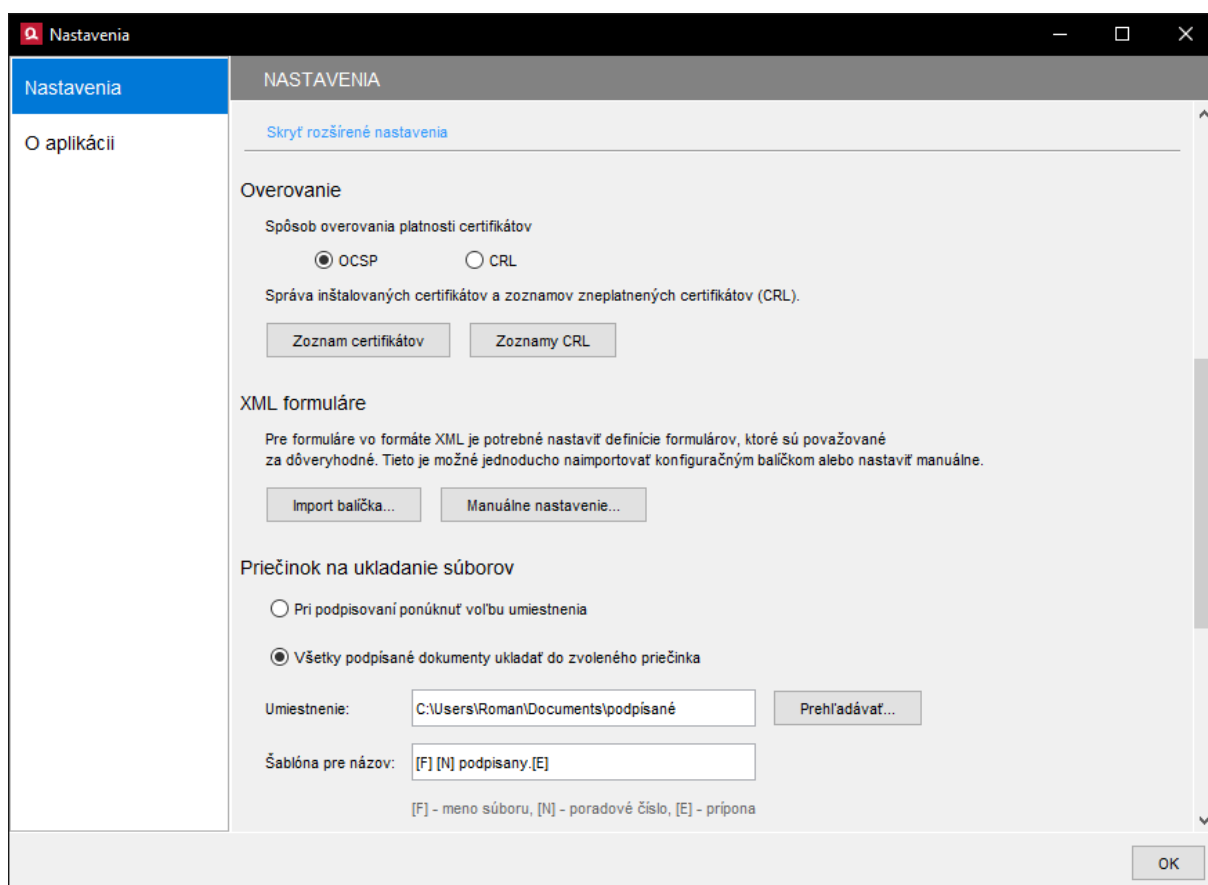
V časti „Časový server“ zadajte adresu servera časových pečiatok, Ak je to vyžadované, zadajte aj OID politiky tohto servera.

Na pripojenie k serveru časových pečiatok je potrebná autentifikácia. V časti „Autentifikácia certifikátom“ zvolte nastavenie, či sa certifikát a privátny kľúč pre túto autentifikáciu použije z čipovej karty, ktorú používate na podpisovanie (máte na nej uložený aj podpisový certifikát), alebo manuálne nastavte umiestnenie v počítači, kde máte súbory certifikátu a privátneho kľúča (s príponou „.pem“) uložené.

Nastavenie predvoľby uložte stlačením „Uložiť“.

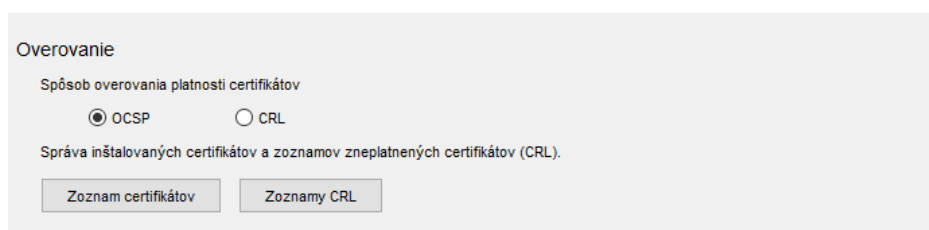
5.2. Rozšírené nastavenia

Rozšírené nastavenia ponúkajú ostatné možnosti aplikácie, ktoré sú určené pre pokročilejšieho používateľa alebo nie sú z hľadiska použitia často využívané.



5.2.1. Nastavenie overovania





V časti „Overovanie“ môžete nastaviť spôsob overovania platnosti certifikátov buď cez **OCSP** (internetový protokol overovania stavu certifikátu) alebo pomocou **CRL** (zoznam zrušených certifikátov). Viac informácií nájdete v kapitole 6. *Slovník pojmov*.



POZNÁMKA:

Ak je označený spôsob overovania certifikátov cez OCSP, ale pre daný certifikát OCSP nie je dostupné, certifikát sa automaticky overuje pomocou CRL.

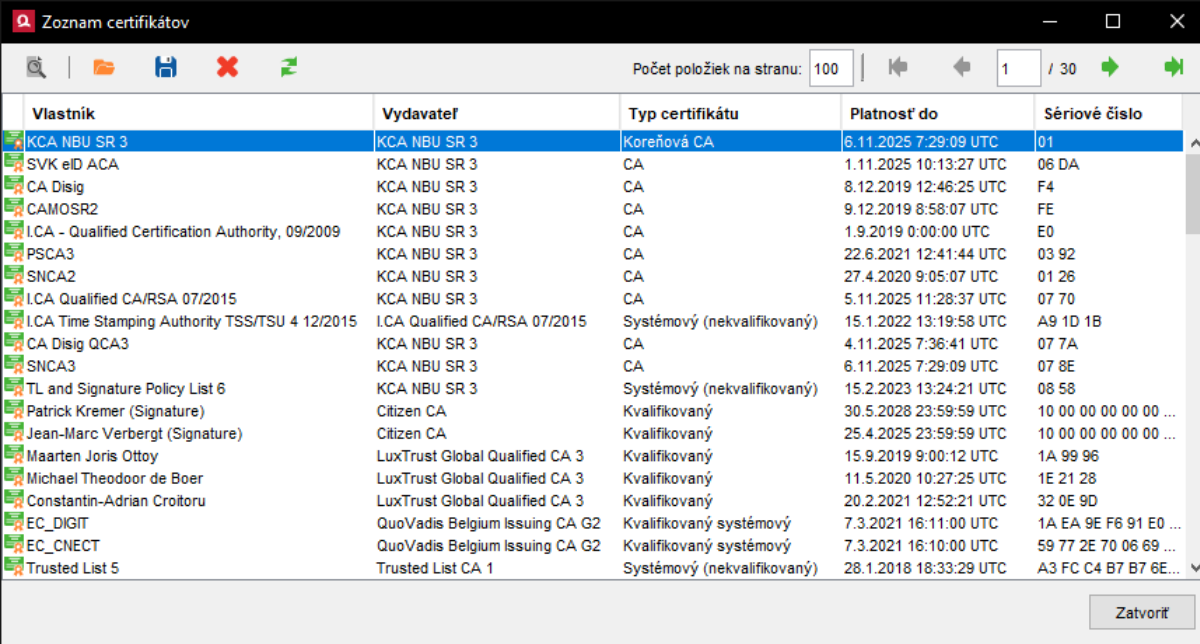
Na správu certifikátov inštalovaných v aplikácii stlačte tlačidlo „**Zoznam certifikátov**“. V zobrazenom okne, kliknutím na príslušnú ikonu, môžete vykonať nasledovné úkony:

-  zobrazíť podrobnosti označeného certifikátu (môžete použiť aj dvojklik na určitý riadok certifikátu)
-  pridať (nainštalovať) ďalší certifikát
-  exportovať (uložiť) certifikát do zvoleného priečinka
-  odstrániť (odinštalovať) označený certifikát.

POZNÁMKA:

Ak aplikácia pri overovaní zobrazí chybové hlásenie, že nie sú dostupné všetky certifikáty z certifikačnej cesty, v tomto okne je potrebné chýbajúce certifikáty najprv pridať.

Pravá horná časť okna slúži na stránkovanie položiek zoznamu. Okno zatvoríte tlačidlom „**Zatvoriť**“.



Vlastník	Vydavateľ	Typ certifikátu	Platnosť do	Sériové číslo
KCA NBU SR 3	KCA NBU SR 3	Koreňová CA	6.11.2025 7:29:09 UTC	01
SVK eID ACA	KCA NBU SR 3	CA	1.11.2025 10:13:27 UTC	06 DA
CA Disig	KCA NBU SR 3	CA	8.12.2019 12:46:25 UTC	F4
CAMOSR2	KCA NBU SR 3	CA	9.12.2019 8:58:07 UTC	FE
LCA - Qualified Certification Authority, 09/2009	KCA NBU SR 3	CA	1.9.2019 0:00:00 UTC	E0
PSCA3	KCA NBU SR 3	CA	22.6.2021 12:41:44 UTC	03 92
SNCA2	KCA NBU SR 3	CA	27.4.2020 9:05:07 UTC	01 26
LCA Qualified CA/RSA 07/2015	KCA NBU SR 3	CA	5.11.2025 11:28:37 UTC	07 70
LCA Time Stamping Authority TSS/TSU 4 12/2015	LCA Qualified CA/RSA 07/2015	Systémový (ne kvalifikovaný)	15.1.2022 13:19:58 UTC	A9 1D 1B
CA Disig QCA3	KCA NBU SR 3	CA	4.11.2025 7:36:41 UTC	07 7A
SNCA3	KCA NBU SR 3	CA	6.11.2025 7:29:09 UTC	07 8E
TL and Signature Policy List 6	KCA NBU SR 3	Systémový (ne kvalifikovaný)	15.2.2023 13:24:21 UTC	08 58
Patrick Kremer (Signature)	Citizen CA	Kvalifikovaný	30.5.2028 23:59:59 UTC	10 00 00 00 00 00 ...
Jean-Marc Verbergt (Signature)	Citizen CA	Kvalifikovaný	25.4.2025 23:59:59 UTC	10 00 00 00 00 00 ...
Maarten Joris Ottoy	LuxTrust Global Qualified CA 3	Kvalifikovaný	15.9.2019 9:00:12 UTC	1A 99 96
Michael Theodoor de Boer	LuxTrust Global Qualified CA 3	Kvalifikovaný	11.5.2020 10:27:25 UTC	1E 21 28
Constantin-Adrian Croitoru	LuxTrust Global Qualified CA 3	Kvalifikovaný	20.2.2021 12:52:21 UTC	32 0E 9D
EC_DIGIT	QuoVadis Belgium Issuing CA G2	Kvalifikovaný systémový	7.3.2021 16:11:00 UTC	1A EA 9E F6 91 E0 ...
EC_CNECT	QuoVadis Belgium Issuing CA G2	Kvalifikovaný systémový	7.3.2021 16:10:00 UTC	59 77 2E 70 06 69 ...
Trusted List 5	Trusted List CA 1	Systémový (ne kvalifikovaný)	28.1.2018 18:33:29 UTC	A3 FC C4 B7 B7 6E...

Spravovať môžete aj zoznamy CRL. Stlačte tlačidlo „**Zoznamy CRL**“ a zobrazí sa okno s inštalovanými CRL v aplikácii. Viac informácií nájdete v kapitole 6.2. CRL.

Funkcie správy CRL zoznamov sú obdobné ako pri zozname certifikátov.

ID	Veľkosť	Vydavateľ	Platnosť od
18706	0.001 MB	Microsec e-Szigno Root CA 2009	2.4.2020 5:30:00 UTC
18712	0.975 MB	Qualified e-Szigno CA 2009	2.4.2020 8:45:02 UTC
18718	0.051 MB	Qualified e-Szigno QCP CA 2012	2.4.2020 4:10:40 UTC
19620	8.701 MB	SVK eID ACA	2.4.2020 5:30:00 UTC
19626	0.001 MB	KCA NBU SR 3	2.4.2020 10:05:35 UTC
19663	0.009 MB	LCA Qualified CA/RSA 07/2015	2.4.2020 11:50:02 UTC
19694	0.027 MB	CA Disig QCA3	2.4.2020 6:05:00 UTC
19725	0.009 MB	SNCA2	2.4.2020 10:00:58 UTC
19781	0.034 MB	CA Disig	6.12.2019 10:33:58 UTC
19787	0.001 MB	LCA Root CA/RSA	5.11.2019 11:30:37 UTC
19793	0.975 MB	Qualified e-Szigno CA 2009	2.4.2020 12:30:03 UTC
19811	0.975 MB	Qualified e-Szigno CA 2009	2.4.2020 12:45:02 UTC
19817	0.975 MB	Qualified e-Szigno CA 2009	2.4.2020 14:00:03 UTC
19823	0.009 MB	SNCA2	2.4.2020 14:01:08 UTC
19829	0.001 MB	KCA NBU SR 3	2.4.2020 14:05:35 UTC
19848	0.975 MB	Qualified e-Szigno CA 2009	2.4.2020 16:15:07 UTC
19904	0.052 MB	Qualified e-Szigno QCP CA 2012	2.4.2020 16:15:01 UTC
19922	0.052 MB	Qualified e-Szigno QCP CA 2012	2.4.2020 16:30:06 UTC
19928	0.975 MB	Qualified e-Szigno CA 2009	2.4.2020 16:45:05 UTC
19934	0.001 MB	Microsec e-Szigno Root CA 2009	2.4.2020 17:30:00 UTC

Zoznam CRL sa počas doby, kedy aplikácia QSign beží, dopĺňa priebežne podľa intervalu v akom sú jednotlivé CRL certifikačnými autoritami vydávané. To znamená, že ak je potrebné certifikát overiť k CRL v konkrétnom čase a toto CRL aplikácia neobsahuje, pretože v období, kedy bolo toto CRL aktuálne, aplikácia nebola spustená, je potrebné chýbajúce CRL doplniť manuálne.

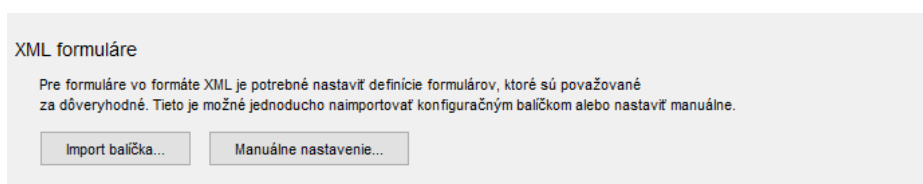
POZNÁMKA:

Ak je stav overenia podpisu „Neúplné automatické overenie“ (pozrite kapitolu 6.6. *Neúplné automatické overenie*), chýbajúce CRL doplníte práve v tomto okne.

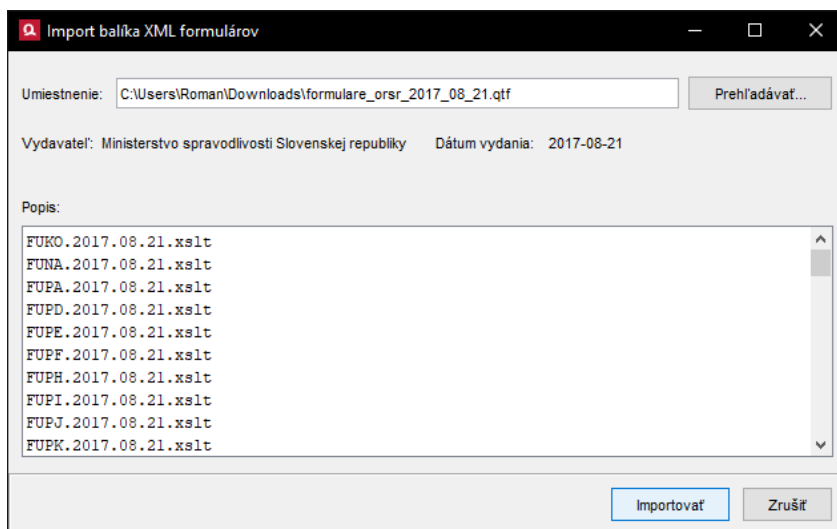
5.2.2. XML formuláre

Ak chcete podpísať XML formulár (napr. eFormulár pre Obchodný register SR), aplikácia potrebuje poznať dôveryhodnú definíciu tohto formulára, ktorá pozostáva so zobrazovacej transformácie (XSLT) a schémy (XSD). To je nevyhnutné pre zobrazenie a podpis XML formulára.

Pre elektronické formuláre orgánov verejnej moci Slovenskej republiky, resp. formuláre zverejnené na Ústrednom portáli verejnej správy (slovensko.sk), aplikácia dokáže tieto definície automaticky stiahnuť online. Pokiaľ definíciu pre daný formulár nenájde alebo z nejakého dôvodu nedokáže stiahnuť, je potrebné definíciu tohto formulára nahráť do aplikácie manuálne.



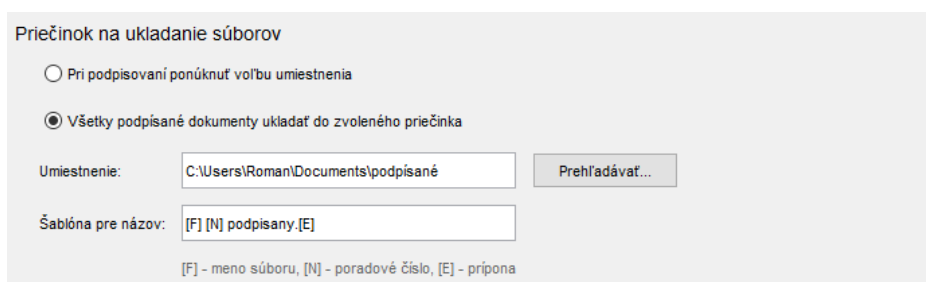
Dôveryhodné definície pre určitú skupinu formulárov (napr. pre Obchodný register SR) môžu byť zverejnené balíčky XML formulárov, a tak ich je možné nahráť do aplikácie všetky naraz. Stlačte „**Import balíčka...**“ a v zobrazenom okne zvolíte umiestnenie balíčka. V okne sa zobrazia informácie o vydavateľovi, dátume vydania a popis daného balíčka. Import definícií XML formulárov spustíte stlačením „**Importovať**“.



Zobrazovacie transformácie a schémy XML formulárov je možné spravovať aj ručne po stlačení „**Manuálne nastavenie...**“.

5.2.3. Priečinko na ukladanie súborov

Po vytvorení podpisu sa dokument s podpisom uloží do súboru, ktorého umiestnenie môžete buď zvoliť hneď po podpise alebo predefinovať v tomto nastavení.



Prvá voľba nastavenia ponúka možnosť výberu uloženia súboru hneď po podpise. Ak označíte druhú možnosť, zvolte predefinovaný priečinko (jeho umiestnenie) kam sa budú ukladať všetky podpísané dokumenty. Taktiež máte možnosť definovať aj šablónu pre názov súboru:

[F] – použije pôvodný názov podpisovaného dokumentu (súboru)



[N] – vloží do názvu poradové číslo

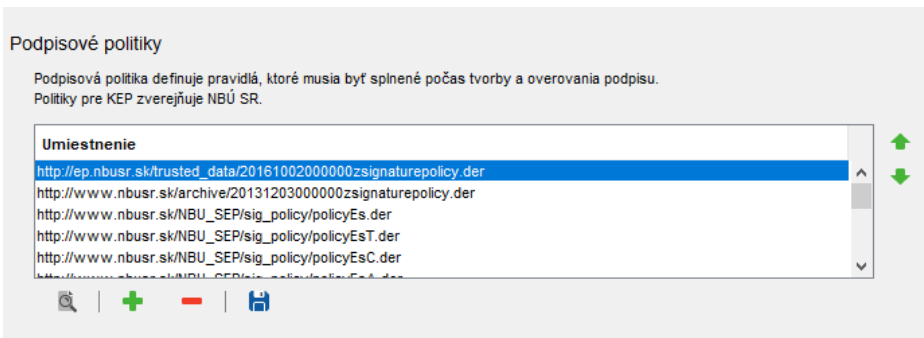
[E] – túto značku zadajte na koniec pre vloženie prípony súboru.

PRÍKLAD:

Ak použijete tvar šablóny [F] [N] podpísany.[E] pre dokument, ktorého názov súboru je „dokument.pdf“, podpísaný dokument bude mať názov súboru „dokument 1 podpísany.asice“.

5.2.4. Podpisové politiky

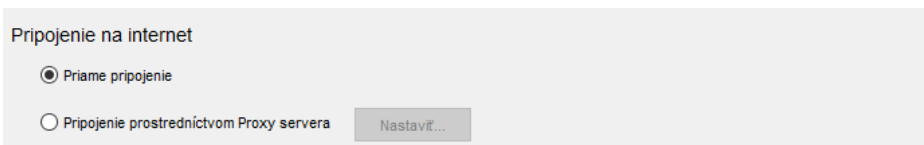
V tomto zozname sa nachádzajú podpisové politiky (pozrite kapitolu 6.7. *Podpisová politika*) importované do aplikácie, ktoré môžu byť použité na vytvorenie podpisu. Pri podpise sa použije vždy prvá v poradí. Ak chcete určiť na podpis inú podpisovú politiku, premiestnite ju na prvé miesto pomocou tlačidiel  a  napravo od zoznamu.



Ak chcete zobrazit' detaily podpisovej politiky, označte ju a kliknite na 🔍. Ak chcete overit' podpis voči inej politike (viď kapitola 4.4.2.3. *Podpisová politika podpisu*), ktorá sa v tomto zozname nenachádza, pridajte súbor pre politiku do tohto zoznamu po stlačení +. Politiku môžete odstrániť stlačením - alebo exportovať v podobe súboru (uložit') do zvoleného priečinka stlačením 💾.

5.2.5. Pripojenie na internet

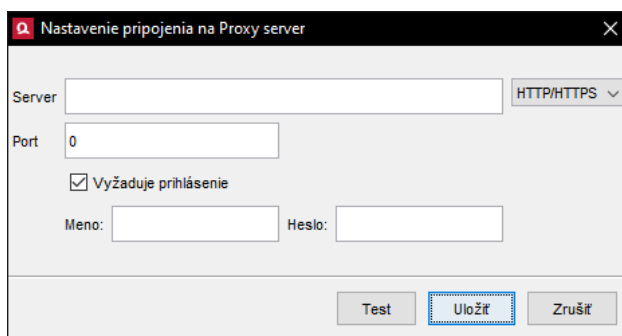
Nastavenie pripojenia na internet určuje aplikácii akým spôsobom je počítač, na ktorom beží aplikácia, pripojený na internet.



Na výber sú dve možnosti:

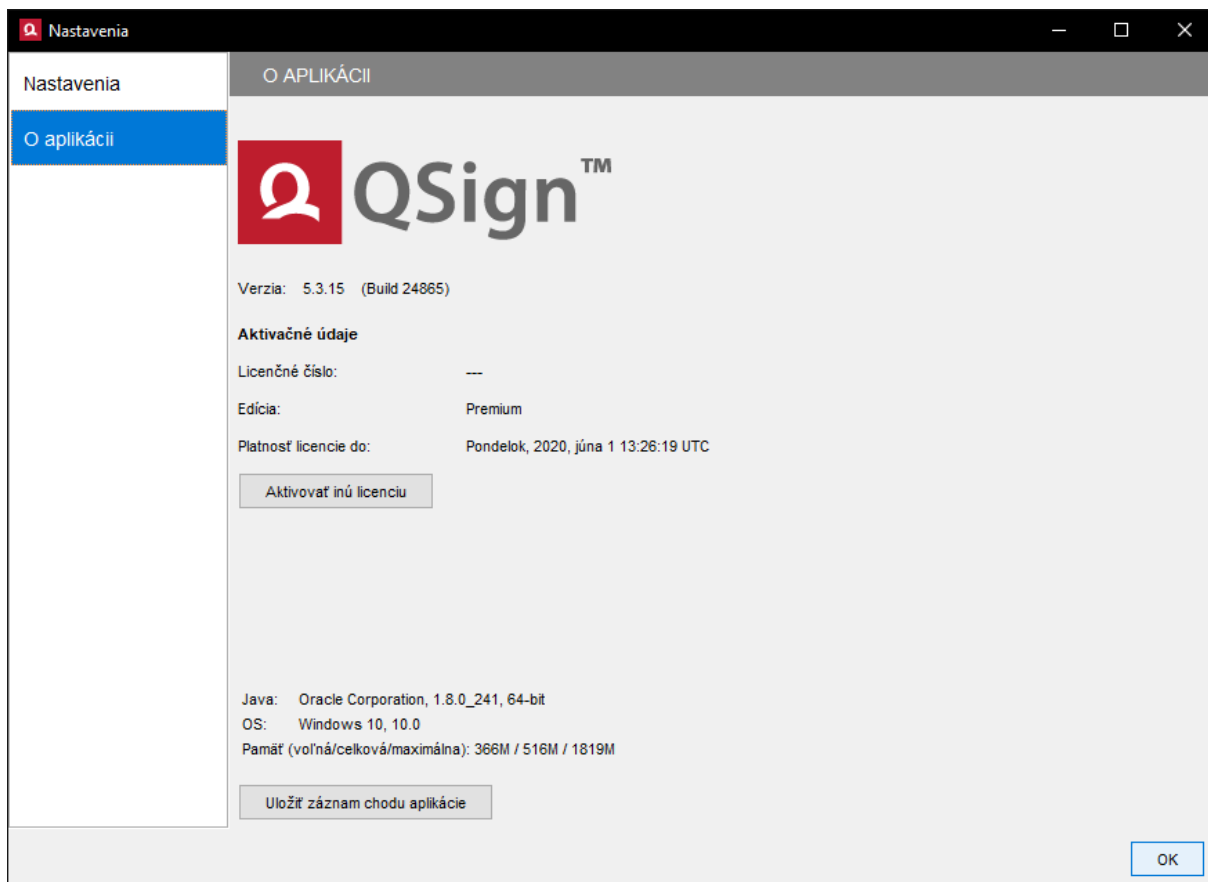
- › Priame pripojenie
- › Pripojenie prostredníctvom Proxy servera

Ak zvolíte pripojenie cez Proxy server, stlačte tlačidlo „**Nastaviť...**“ a zadajte potrebné parametre pripojenia cez Proxy server. Ak tieto parametre nepoznáte, vyžiadajte si ich od sieťového administrátora. Stlačením „**Test**“ môžete vyplnené parametre otestovať. Nastavenie uložte stlačením „**Uložit'**“.



5.3. O aplikácii

Na záložke „O aplikácii“ sú zobrazené informácie o verzii aplikácie, aktivačných údajoch a v spodnej časti okna systémové informácie.



Tlačidlom „**Aktivovať inú licenciu**“ môžete aktivovať QSign inou licenciou. Napríklad tak môžete pridať funkciu hromadného podpisovania (pozrite kapitolu 4.6. *Hromadný podpis*).

Ak aplikácia pri používaní vyhlási chybu a potrebujete na jej vyriešenie technickú pomoc, stlačte „**Uložiť záznam chodu aplikácie**“. Súbor „qsign_logging.log“ uložte a následne ho pošlite v prílohe správy s popisom situácie výskytu tejto chyby na adresu support@ardaco.com.

TIP:

Okno „O aplikácii“ je možné zobrazit' aj cez menu stavovej ikony aplikácie na systémovej lište operačného systému (pozrite kapitolu 4. *Práca s aplikáciou*). Zároveň je tak možné pristúpiť aj k nastaveniam aplikácie (kliknutím na záložku „Nastavenia“) bez potreby otvorenia hlavného okna QSign.

6. Slovník pojmov

Vymedzenie všetkých pojmov používaných v súvislosti s kvalifikovaným elektronickým podpisom je uvedené v [Čl. 3 nariadenia \(EÚ\) č. 910/2014](#) (Nariadenie eIDAS). Na základe tohto nariadenia bol v Slovenskej republike vydaný [zákon č. 272/2016 Z. z.](#) Zákon o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách).

6.1. Časová pečiatka

Na overenie elektronického podpisu je dôležitý časový údaj, kedy bol podpis vytvorený. Tento údaj sa nazýva časová pečiatka.

Časová pečiatka musí byť vyhotovená dôveryhodným zdrojom času, tzv. serverom časových pečiatok. Ten garantuje, že časová pečiatka bola vytvorená použitím presného času. Nestačí, aby na vyhotovenie časovej pečiatky bol použitý systémový čas vášho počítača. Ten si totiž viete kedykoľvek zmeniť.

Časová pečiatka teda garantuje presný dátum a čas vytvorenia podpisu. Ak podpis neobsahuje časovú pečiatku, overuje sa k systémovému času počítača.

6.2. CRL

Zoznam zrušených („zneplatnených“) certifikátov (CRL = Certificate Revocation List) je zoznam certifikátov, ktoré boli počas doby ich platnosti zrušené z dôvodu neaktuálnosti údajov na certifikáte, straty zariadenia s certifikátom, úmrtia vlastníka certifikátu a pod. Zoznamy CRL vydávajú a spravujú kvalifikovaní poskytovatelia dôveryhodných služieb (certifikačné authority) a koreňová certifikačná autorita, ktoré dané certifikáty vydali a poskytujú všetky vydané CRL na stiahnutie z archívu prostredníctvom svojho webového sídla.

6.3. OCSP

OCSP (Online Certificate Status Protocol) je internetový protokol slúžiaci k overeniu stavu certifikátu, hlavne či certifikát nebol zrušený (zneplatnený). OCSP protokol bol vytvorený ako náhrada za starší spôsob overovania pomocou CRL, ktorý už veľmi nevyhovuje dnešným nárokom. Server poskytujúci službu OCSP spravidla prevádzkuje poskytovateľ dôveryhodných služieb (certifikačná autorita), ktorá vystavila tento certifikát. OCSP komunikácia prebieha na báze žiadosť-odpoveď cez HTTP a nestahuje sa súbor s celým zoznamom. Hlavnou výhodou OCSP oproti CRL sú teda rýchlosť a výrazne nižšie nároky na prenos dát, pretože odpoveď spravidla obsahuje menej informácií.

6.4. Certifikačná cesta

Kvalifikovaný certifikát vydáva fyzickým osobám kvalifikovaný poskytovateľ dôveryhodných služieb, ktorý získal kvalifikovaný štatút od koreňovej certifikačnej authority. Na Slovensku je koreňovou certifikačnou autoritou Národný bezpečnostný úrad SR (NBÚ SR), ktorý poskytovateľom dôveryhodných služieb vydáva tzv. certifikát dôveryhodných služieb. Táto postupnosť vydania certifikátov sa nazýva certifikačná cesta.

6.5. Neúplné overenie

Neúplné overenie je stav overenia podpisu, kedy nie je možné úplne overiť jeho platnosť. Väčšinou ide o prípad, kedy nie je pre úplné overenie platnosti všetkých certifikátov z certifikačnej cesty možné zistiť, či k času overenia alebo času časovej pečiatky sú jednotlivé certifikáty z certifikačnej cesty platné a neboli zrušené. Toto sa zisťuje prostredníctvom služby OCSP alebo podľa aktuálneho CRL (pozrite kapitolu 5.2.1 *Nastavenie overovania*).

Pri overovaní podľa CRL je potrebné brať do úvahy, že CRL sa aktualizujú iba v určitých časových intervaloch, a preto nie je možné s určitosťou rozhodnúť, či v danom okamihu je certifikát podpisovateľa platný. Podpisovateľ mohol svoj certifikát medzičasom zrušiť a táto informácia, ktorá je v takomto prípade uvedená až v nasledujúcom vydaní CRL zoznamu, ešte počas overenia nie je dostupná. Zároveň musí byť CRL vydané koreňovou certifikačnou autoritou novšie ako CRL vydané kvalifikovaným poskytovateľom dôveryhodných služieb.

Ak je teda výsledný stav overenia „Neúplné overenie“, je potrebné počkať do najbližšej aktualizácie všetkých CRL z certifikačnej cesty. Potom, ak je v podpise vložená časová pečiatka, podpísaný dokument otvorte/overte znova.

Ak však v podpise nie je vložená časová pečiatka, podpis overte použitím menu „**Nástroje -> Overiť k času...**“ a nastavte dátum a čas starší ako posledná aktualizácia všetkých CRL z certifikačnej cesty.

6.6. Neúplné automatické overenie

V prípade overenia podpisu s časovou pečiatkou platnou v čase overovania, kde certifikát, ktorým sa podpis vytvoril už nie je platný, je takýto podpis považovaný ešte za platný (do doby platnosti časovej pečiatky) za predpokladu, že má aplikácia pre overenie k dispozícii CRL všetkých certifikátov z certifikačnej cesty z dátumu vytvorenia tohto podpisu.

Ak aplikácii nejaký tento CRL záznam chýba, nie je možné podpis automaticky úplne overiť. Hovoríme teda, že ide o „Neúplné automatické overenie“, čo sa zobrazí ako výsledný stav podpisu v aplikácii.

V takomto prípade je potrebné importovať chýbajúce CRL do aplikácie ručne (pozrite kapitolu 5.2.1. *Nastavenie overovania*). Tento CRL záznam získate od kvalifikovaného poskytovateľa dôveryhodných služieb alebo koreňovej certifikačnej autority (môžete ho stiahnuť z ich web stránky), uvedených v certifikačnej ceste daného certifikátu, ktorým bol podpis vytvorený.

6.7. Podpisová politika

Podpisová politika je súbor pravidiel upravujúcich vyhotovovanie a overovanie kvalifikovaných elektronických podpisov a určuje parametre podpisu. Podľa vybranej podpisovej politiky sa ďalej určuje, či podpis je kvalifikovaným elektronickým podpisom v zmysle platnej legislatívy.

- › Kvalifikovaný elektronický podpis vyhotovuje podpisovateľ v súlade s určenou podpisovou politikou.
- › Podpisové politiky pre kvalifikovaný elektronický podpis schvaľuje NBÚ SR.
- › Platnosť kvalifikovaného elektronického podpisu overuje overovateľ vzhľadom na podpisovú politiku, ktorá bola použitá pri jeho vyhotovení.
- › Subjekt, ktorý prijíma dokumenty podpísané kvalifikovaným elektronickým podpisom, určí podpisovú politiku, ktorú akceptuje.
- › Podpisovateľ a overovateľ kvalifikovaného elektronického podpisu použijú tú istú podpisovú politiku.



www.ardaco.com | www.qsign.sk