Návod

Aplikáciu QES, dostupnú na Aplikácie TL a QES -NBU (gov.sk), je možné spustiť bez potreby inštalácie a priamo v QES podpisovať a validovať, alebo po prepnutí QES do Web Signer módu žiadať podpísať/validovať napr. z web stránky.

Podpis konateľa alebo splnomocnenej osoby

Mandátny certifikát môže v položkách mena subjektu obsahovať údaje o dvoch rôznych osobách:

- Položky podpisovateľa, osoby držiteľa certifikátu, nezačínajú s „MANDANT“.
- Ak položky začínajú s „MANDANT“, potom obsahujú údaje o osobe za ktorú držiteľ certifikátu koná, alebo ktorú zastupuje.

Správnosť všetkých položiek certifikátu overil vydavateľ certifikátu v čase vydania certifikátu. Ak údaje v certifikáte prestanú byť aktuálne, **je povinnosťou osôb uvedených v mene subjektu certifikátu, požiadať o zrušenie certifikátu**.

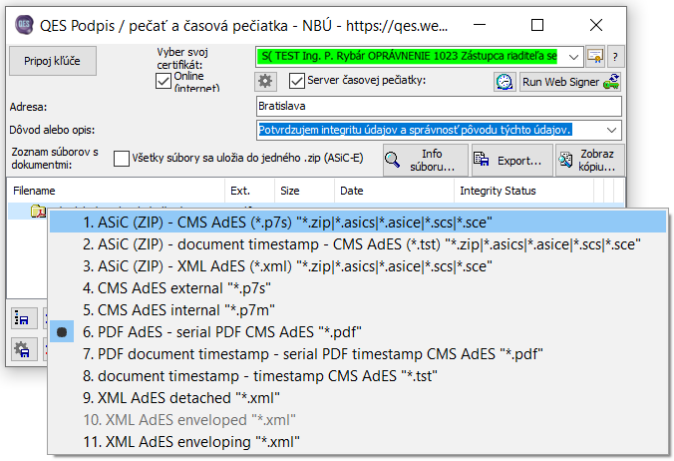
Podpisovateľ môže uviesť/vybrať do položky "Dôvod alebo opis" text, ktorý upraví alebo napíše podľa toho, v akej funkcii podpisuje písomnosť a uvedie http adresu na register, ktorý umožní overenie napr. jeho funkcie, alebo uvedie názov priloženého elektronického dokumentu, ktorý obsahuje napr. plnú moc a ktorý elektronicky podpísal alebo zapečatil splnomocniteľ.

Elektronický dokument

Elektronický dokument podľa definície v čl. 3 ods. 35 nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 (Corrigendum) o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (ďalej aj „nariadenie eIDAS“), je akýkoľvek obsah uložený v elektronickej forme, najmä text alebo zvukový, obrazový či audiovizuálny záznam.

Právne účinky elektronických dokumentov sú uvedené v článku 46 nariadenia (EÚ) č. 910/2014: právny účinok elektronického dokumentu a jeho prípustnosť ako dôkazu v súdnom konaní sa nesmie odmietnuť výlučne z dôvodu, že má elektronickú formu.

Podľa typu dokumentu, zadaného do zoznamu aplikácie QES, sa vyberie prednastavený formát podpisu, pozri prílohu vykonávacieho rozhodnutia Komisie (EÚ) 2015/1506 EUR-Lex - 32015D1506 - EN - EUR-Lex (europa.eu). Napr. pre PDF sa vyberie PDF podpis. Podpisovateľ si môže formát podpisu zmeniť pravým tlačidlom myši po kliknutí na riadok s názvom dokumentu.



Slovenský formát elektronického dokumentu definuje § 46 ods. 2 písm. c) vyhlášky Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy, ako štandard prijímania a čítania podpísaných

elektronických dokumentov vo formáte jazyka pre prenos dátových prvkov podľa § 12 v štruktúre podľa prílohy č. 7 (ďalej len „kontajner XML údajov“). Keďže štát vyžaduje použitie elektronického dokumentu formátu „Kontajner XML údajov“ (XMLDataContainer), musí bezplatne zabezpečiť aj jeho vyhotovenie, modifikovanie, spracovanie a čítanie. Aplikácia QES neslúži na editovanie elektronických dokumentov, ale na vyhotovenie ich zabezpečenia a informatívnu validáciu ich zabezpečenia kvalifikovaným elektronickým podpisom, pečaťou a časovou pečiatkou. Editovanie dokumentu „Kontajner XML údajov“ formátu (XMLDataContainer), musí občanom zabezpečiť orgán verejnej moci, ktorý vyžaduje použitie dokumentu „Kontajner XML údajov“.

Aplikácia QES umožňuje podpísanie a validáciu ľubovoľného formátu elektronického dokumentu, ktorý je identifikovaný vo validačnej správe rozšírením mena súboru a aj prostredníctvom MIME *Content-Type*, ktorý je registrovaný v systéme, kde je QES aplikácia použitá.
Odporúčania, ako zabrániť aby ste sa stali obeťou útokov na elektronické dokumenty, nájdete na stránke Aplikácie TL a QES -NBU (gov.sk).

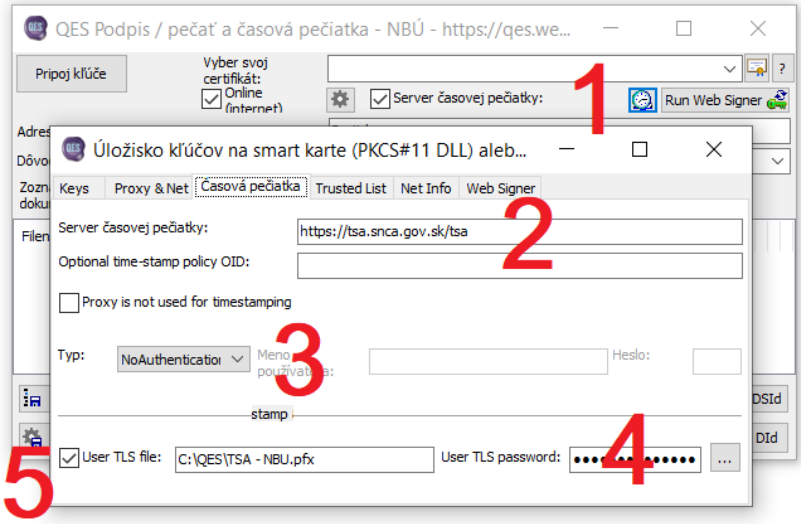
Kvalifikovaná elektronická časová pečiatka

Kvalifikovaná elektronická časová pečiatka je poskytovaná kvalifikovanou dôveryhodnou službou. Dôveryhodnú službu definuje v čl. 3 ods. 16 nariadenie (EÚ) č. 910/2014: „dôveryhodná služba“ je elektronická služba, ktorá **sa spravidla poskytuje za odplatu** a spočíva... . Občan si môže vybrať, od ktorého kvalifikovaného poskytovateľa služieb kvalifikovaných časových pečiatok sa rozhodne službu odoberať, po zvážení podmienok za akých je služba poskytovaná vybraným poskytovateľom. Kvalifikovaného poskytovateľa si môže vybrať z poskytovateľov z celej EÚ, ak je uvedený v dôveryhodnom zozname ktorejkoľvek krajiny EÚ. Prezerať ich je možné napr. prostredníctvom nástroja Komisie EÚ: EU Trust Services Dashboard (europa.eu) označenú ako „QTimestamp“.

Nastavenie v aplikácii QES. Zaškrtne sa (1) „Server časovej pečiatky“ a kliknutím na tlačidlo hodín je vyzvaný na zadanie (2) adresy získanej od poskytovateľa časovej pečiatky.
Ak poskytovateľ požaduje ďalšie nastavenia, je možné zadanie

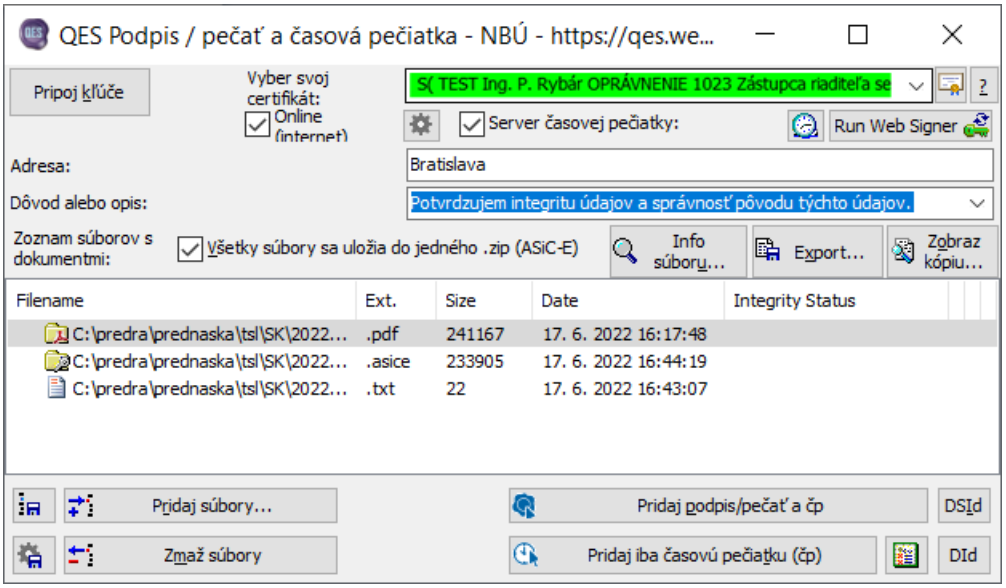
- OID politiky poskytovateľa časových pečiatok,
- zapnúť autentifikáciu heslom výberom (3) „Basic“ a zadaním mena a hesla, alebo
- zapnúť (4) autentifikáciu klientskym TLS certifikátom, kedy sa zaškrtne „User TLS file:“, zadá zaslané heslo od poskytovateľa a kliknutím na „...“ zadá cestu na súbor s kľúčom na autentifikáciu, ktorý mu zašle poskytovateľ a uložený je na disk, napr. "*.pfx" alebo "*.p12".

Nastavenia sa uložia po zatvorení dialógového okna v okne hlavnej aplikácie tlačidlom uloženia (5).



Nevyhnutné podmienky pre podpisovanie v aplikácii QES

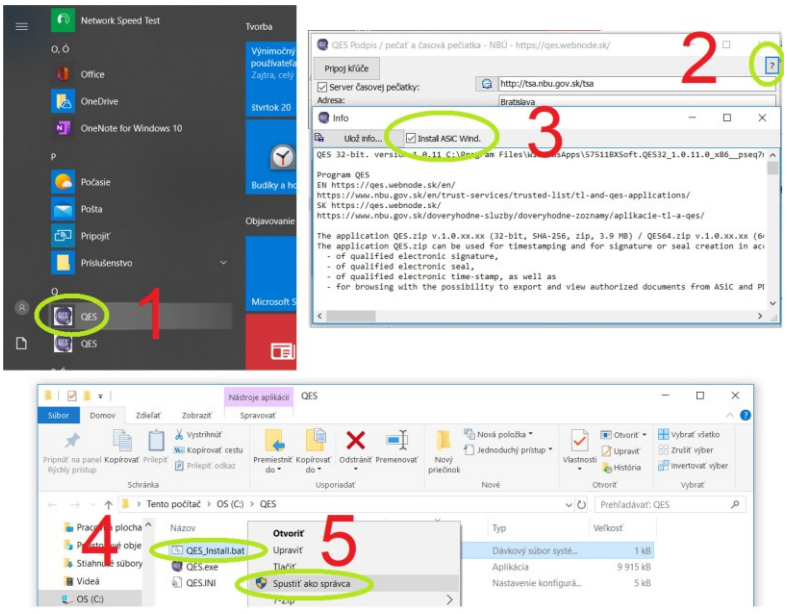
Podpisovateľ musí mať pred spustením aplikácie QES v systéme Windows nainštalovanú čítačku čipovej karty, ovládače pre čipovú kartu (Windows alebo PKCS#11) a musí mať do čítačky vloženú čipovú kartu, napr. občiansky preukaz s čipom. V karte musí mať vydaný kvalifikovaný certifikát. Do občianskeho preukazu s čipom (eID) môže osoba požiadať aj o vydanie kvalifikovaného certifikátu, alebo požiadať o vydanie kvalifikovaného certifikátu cez eID aplikáciu MV SR.



Ak chceme kliknutím otvárať súbory s koncovkou **ASiCS**, **ASiCE**, **SCS**, **SCE**, **ZEP** a **P7M**, potom je potrebné aplikáciu QES nainštalovať kliknutím podľa nasledujúcich krokov:

- spustiť aplikáciu QES (1) a zobraziť informáciu o aplikácii kliknutím na „?“ (2),
- zaškrtnúť (3) "Install ASiC Wind." (zopakovať ak je zaškrtnuté), čím sa otvorí prieskumník a vyhotoví odkaz na Pracovnú plochu,
- v prieskumníkovi (4) kliknúť pravým tlačidlom myši na súbor "QES_Install.bat" a v ponuke (5) kliknúť na "Spustiť ako správca".

Aplikácia sa spúšťa odkazom z pracovnej plochy, alebo sa na ikonu na pracovnej ploche QES preťahujú dokumenty určené na podpis alebo na validáciu.



Režim QES - Web Signer

Aplikáciu QES je možné spustiť aj v režime „Web Signer“, kliknutím na tlačidlo „Run Web Signer“, alebo v príkazovom riadku s parametrom „-w“, napr. „QES.EXE -W“ pri štarte počítača.

Systémy žiadajúce podpis alebo validáciu, napr. stránka Web prehliadača, vytvorí spojenie na QES cez adresu http://localhost:8080 a zašle cez http POST súbor „*.QCFG“ (premenovaný ZIP) obsahujúci dokumenty na podpísanie a adresár "META-INF" s konfiguračným súborom "*.cfg" (TXT v UTF-8). Súbor "*.cfg" obsahuje zoznam dvojíc názvov dokumentov na podpis a súborov s typom podpisu, do ktorých sa podpis uloží.

Napr. dva PDF dokumenty (označené žlto) budú podpísané spolu naraz v jednom ASiC súbore „kontajner.asice“:

```
FILE=Test1.pdf
HASH=
NOTICE=Content-Type: application/pdf
FILE=kontajner.asice
HASH=
NOTICE=Content-Type: application/vnd.etsi.asic-e+zip
FILE=Test2.pdf
HASH=
NOTICE=Content-Type: application/pdf
FILE= kontajner.asice
HASH=
NOTICE=Content-Type: application/vnd.etsi.asic-e+zip
```

Podrobné príklady sú v súbore ZIP.

QES aplikácia spustená ako Web Signer, po prijatí http POST žiadosti, zobrazí QES aplikáciu ako žiadosť na podpísanie/validovanie. Po stlačení tlačidla „Pridaj podpis...“ zašle ako odpoveď na POST podpísané súbory v súbore „*.QCFG“ a pri validácii sa zašle prijatý súbor „*.QCFG“ po zavretí aplikácie QES.
Web prehliadač, po podpísaní v QES, príjme v návrate z http POST súbor *.QCFG s výsledkom podpísania.
Pri volaní pre validáciu (iba pre formát PDF a ASiC), napr. po podpísaní po zopakovanom zaslaní súboru *.QCFG, v QCFG súbore by mal ostať len jeden súbor (*.DSId) identifikujúci podpis pre validovanie, ak QCFG obsahuje viacero súborov (*.DSId), použije sa len jeden. Pozri kapitolu 3.3 v ISO 14533-4:2019(en), Processes, data elements and documents in commerce, industry and administration — Long term signature profiles — Part 4: Attributes pointing to (external) proof of existence objects used in long term signature formats (PoEAttributes).

Podrobnosti o obsahu súboru „*.QCFG“ sú uvedené v nápovede po stlačení tlačidla „?“ v aplikácii QES.

Ak by pri podpise, alebo validácii došlo k predčasnému ukončeniu, QES vráti v stave http protokolu info v návrate z POST volania.

Systém žiadajúci podpis získa “*.QCFG” obsahujúci buď podpísané súbory, alebo v prípade chyby má súbor “*.QCFG” nulovú veľkosť a http nasledovný stav:
404: 'Not Found' Ak sa súbor nepodarilo zaslať
408: 'Request Time-out' Ak podpisovateľ nevykonal podpísanie do zadaného času – 10 min
412: 'Precondition Failed' Ak nedošlo k podpísaniu či už chybou podpisovateľa, alebo ukončením aplikácie bez podpísania.

Kroky spojené so stlačením tlačidla "Pridaj podpis"

V štandardnom nastavení podpisovateľ len skontroluje či je v prvom riadku aplikácie QES vybraný jeho podpisový certifikát a či je vyfarbený zeleno (neexpiroval). Ak je táto podmienka splnená, stlačí „Pridaj podpis...".
Ak nie, podpisovateľ nemá správne nastavenia a postupuje podľa nasledovných krokov a po úspešnom nastavení **klikne na tlačidlo „*Ulož nastavenia*" (vľavo dole) aby predošlé kroky už nemusel opakovať pri budúcom podpisovaní**:

- Ak do prvého riadku môže byť vybraný certifikát z viacerých zelených certifikátov, tak v prvom riadku nie je automaticky vybraný certifikát. Podpisovateľ vyberie jeden certifikát z ponuky, po kliknutí na šípku na konci riadku a pokračuje postupom od začiatku tejto kapitoly.
- Po stlačení tlačidla „Pripoj kľúče", podpisovateľ skontroluje či je vybraný Windows, ak nie je, vyberie ho a pokračuje postupom od začiatku tejto kapitoly.
- Ak výber Windows nepomohol, po stlačení tlačidla „Pripoj kľúče" vyberie „Smart karta" a pripojí podpisový kľúč (prepojený na kvalifikovaný certifikát podpisovateľa, aby aplikácia vedela, ktorý certifikát pri podpise použiť) tak, že v otvorenom okne „Úložisko kľúčov" vyberie zeleným obrázkom označenú knižnicu čipovej karty PKCS#11, napr. „eID SK" (ak nie je zelený obrázok pred žiadnou knižnicou (*.dll) vo výbere, nie je nainštalovaný ovládač na čipovú kartu PKCS#11). Podpisovateľ zadá BOK (potom stlačí enter, alebo klikne na Open). Po zatvorení okna na pripojenie kľúčov, ak nie je vybraný certifikát podpisovateľa v zozname, vyberie certifikát podpisovateľa zo zoznamu (napr. ak je na výber z viacerých certifikátov). Ak bude aplikácia QES pre podpísanie potrebovať podpisový PIN, zobrazí výzvu na zadanie podpisového PIN, napr. na vložený občiansky preukaz s čipom v čítačke kariet s čipom. Žiadosť na zadanie PIN môže byť zobrazená aj až úplne na záver podpisovania. Ak čipová karta nemá BOK (dva rôzne PINy), namiesto BOK sa zadá PIN.

Platnosť certifikátu si vie prekontrolovať pred podpisom stlačením tlačidla „?", alebo po podpise kliknutím na „eIDAS Info" podľa postupu v poslednej kapitole.

Ako viacnásobne podpísať napr. dohodu o plnej moci a zmluvu o prevode vlastníctva

Elektronický dokument je možné viacnásobne podpísať podpisom vo formáte PDF AdES, CMS AdES alebo ASiC. Viac informácií nájdete v NBÚ odporúčaní.

- Podpísanie PDF s podpisom v PDF AdES.
    1. V aplikácii QES podpíšete naraz niekoľko PDF s podpisom v PDF AdES, ak do zoznamu aplikácie pridáte niekoľko PDF súborov (veľkosť druhého podpisu a ďalších podpisov, teda aj samotných PDF súborov, bude optimálna na základe skutočnej veľkosti prvého podpisu - odporúča sa ako prvý PDF použiť testovací PDF, ktorý po podpísaní zmažete).
    2. Podpisovateľ pripojí svoj kľúč stlačením "Pripoj kľúče", ak nie je zeleno označený jeho certifikát a podpis pridá stlačením "Pridaj podpis".
    3. Druhý a ďalší podpisovateľ spustí aplikáciu QES, pridá do zoznamu PDF dokumenty a pokračuje bodom 2.
    4. Podpísaný súbor je možné informatívne validovať postupom uvedeným na konci stránky.
    5. Odporúča sa podpísať len verziu získanú validovaním podpisu požadovaného predošlého podpisovateľa.

- Dve osoby podpíšu jeden dokument s CMS AdES podpisom nasledovne:
    1. Do zoznamu dokumentov v aplikácii QES vloží podpisovateľ napr. súbor „splnomocnenie.pdf" (obsahujúci samotnú dohodu o plnej moci, ktorého položky „Splnomocniteľ" a „Splnomocnenec" obsahujú meno, priezvisko a prípadne oprávnenie či funkciu podpisovateľa, pričom toto isté meno a priezvisko je uvedené aj v certifikáte podpisovateľa a certifikát podpisovateľa bude uložený v

CMS AdES podpise v súbore „splnomocnenie.pdf.p7s“ po vyhotovení podpisu),

2. podpisovateľ pripojí kľúč stlačením „Pripoj kľúče“, ak nie je zeleno označený jeho certifikát,
3. pravým tlačidlom myši klikne na „splnomocnenie.pdf“ a vyberie CMS AdES "*.p7s",
4. podpis pridá stlačením „Pridaj podpis“.
5. Druhý a ďalší podpisovateľ spustí aplikáciu QES, pridá do zoznamu „splnomocnenie.pdf“ a pokračuje bodom 2, pričom adresár, kde je súbor „splnomocnenie.pdf“, obsahuje aj súbor s podpisom „splnomocnenie.pdf.p7s“.
6. Podpísaný súbor a aj jeho podpis/y je možné uložiť do ASiC-S kontajneru a následne podpis/y validovať postupom:

   - podpisovateľ spustí aplikáciu QES a zaškrtne "Všetky súbory sa uložia do jedného .zip (ASiC-E)" (ak by zaškrtol až po pridaní dokumentov do zoznamu aplikácie, CMS podpisy a podpísaný dokument by sa neuložili do nového ASiC-S),
   - pridá do zoznamu aplikácie „splnomocnenie.pdf“, pričom adresár, ktorý obsahuje súbor „splnomocnenie.pdf“, obsahuje aj súbor s podpismi "splnomocnenie.pdf.p7s", načo aplikácia QES vyzve na zadanie mena súboru ASiC-S, napr. zadá sa „splnomocnenie.asics“,
   - na záver sa zobrazí druhá žiadosť na zadanie mena ASiC-E, ktorú je ale možné zrušiť alebo zadať meno *.ASiCE, do ktorého je vložený predošlý ASiC-S a súbory zo zoznamu, ale to až po pridaní nového podpisu stlačením „Pridaj podpis“, alebo časovej pečiatky.

- Podpisovateľ, ktorý chce podpísať naraz viaceré dokumenty podpisom v ASiC-E
  1. spustí aplikáciu QES a pridá do zoznamu v aplikácii QES dokumenty, napr. „splnomocnenie.asics“ a iné dokumenty,
  2. zaškrtne "Všetky súbory sa uložia do jedného .zip (ASiC-E)",
  3. pripojí kľúč stlačením "Pripoj kľúče" ak nie je zeleno označený jeho certifikát a podpis pridá stlačením "Pridaj podpis", pričom je vyzvaný na zadanie mena súboru ASiCE, do ktorého sa dokumenty a podpis uložia.

- Podpisovateľ, ktorý chce do ASiC-E pridať ďalšie dokumenty a podpísať ich:
  1. spustí aplikáciu QES, do zoznamu aplikácie QES pridá *.ASiCE kontajner - súbor (ASiC je premenovaný zip), napr. „splnomocnenie.asice“ a dvojitým kliknutím na tento kontajner sa otvorí prehliadač kontajnerov / podpisov, ak nie je vnorený okamžite, prípadne sa vynorí na prvú úroveň tlačidlom „Späť“ a potom,
  2. pridá dokumenty do zoznamu a nastaví ich poradie v zozname (pridanie je povolené len do prvého vnorenia - druhé a ďalšie vnorenia sú už zabezpečené podpisom a ich zmena by znehodnotila/zneplatnila staršie podpisy),
  3. pripojí kľúč stlačením „Pripoj kľúče“ ak nie je zeleno označený jeho certifikát a
  4. podpis pridá stlačením „Pridaj podpis“.

- ASiC (zip) kontajner, napr. "splnomocnenie.asice" obsahujúci dohodu o plnej moci, je možné použiť ako podpísanú prílohu **pri podpisovaní iných elektronických dokumentov,** napr. „Zmluva o prevode vlastníctva.pdf“, a to nasledovne:
  1. súbor „splnomocnenie.asice“ premenuje napr. na súbor „zmluvaPrevodVlastnictva.asice“,
  2. prvý podpisovateľ pridá do zoznamu dokumentov v aplikácii QES ASiC (zip) kontajner, napr. „zmluvaPrevodVlastnictva.asice“,
  3. dvojitým kliknutím na tento kontajner sa otvorí prehliadač kontajnerov / podpisov a
  4. následne vloží do prezeraného kontajnera, na prvej úrovni vnorenia, akékoľvek iné dokumenty ako napr. „Zmluva o prevode vlastníctva.pdf“,
  5. môže zmeniť poradie dokumentov a
  6. potom pripojí kľúč stlačením „Pripoj kľúče“ ak nie je zeleno označený jeho certifikát a
  7. podpis pridá stlačením „Pridaj podpis“.

- Ďalší podpisovatelia zopakujú predošlý krok tak, že do zoznamu dokumentov v aplikácii QES pridajú ASiC (zip) kontajner, napr. „zmluvaPrevodVlastnictva.asice“, dvojitým kliknutím na tento kontajner sa otvorí prehliadač kontajnerov / podpisov, môžu zmeniť poradie dokumentov a potom pripoja kľúč stlačením

„Pripoj kľúče“ ak nie je zeleno označený jeho certifikát a podpis pridajú stlačením „Pridaj podpis“.

- ASiC (zip) kontajner, napr. „zmluvaPrevodVlastnictva.asice“ je potom možné zaslať na kataster ako prílohu cez službu „Všeobecná agenda“, viac na Podávanie návrhu na vklad do katastra nehnuteľností, alebo elektronické podanie na kataster.

Informatívna validácia

Do zoznamu aplikácie sa pridajú súbory vo formátoch ASiC alebo aj PDF. Formát ASiC je potrebné validovať samostatne. Formát PDF môže byť validovaný naraz s viacerými PDF súbormi v zozname.

Ak chceme pre každý podpis vyhotoviť validačnú správu, klikneme na tlačidlo (1) v modrom rámčeku na obrázku nižšie, ktoré sa zobrazí zaškrtnutím servera časových pečiatok, čím sa pre každý podpis vyhotoví samostatný ZIP obsahujúci podpísané súbory a validačnú správu ich podpisu, inak si môžeme každý podpis validovať samostatne:

- Dvojklikom sa vnorí do ASiC kontajneru, alebo PDF.
- Ak po vnorení do PDF je zoznam prázdny, PDF neobsahuje podpis vo formáte podľa nariadenia eIDAS.
- Šípkami sa vyberie riadok podpisu (automaticky sa označia dokumenty podpísané vybraným podpisom) a klikne sa na tlačidlo "eIDAS Info" na zobrazenie informácií o platnosti podpisu.
- Zaškrtnutím CRL/OCSP sa po zatvorení okna Info uložia CRL/OCSP validačné údaje do súboru ASiC alebo PDF, napr. pre opätovnú validáciu neskôr alebo na off-line počítači.
- Podpísané dokumenty (označili sa pri výbere riadku podpisu) je možné zobraziť alebo exportovať napr. na disk kliknutím na tlačidlo "Zobraz" alebo "Export".