DITEC

D.Signer .NET 5.0

Používateľská príručka

Copyright

Všetky práva vyhradené

Tento dokument je vlastníctvom spoločnosti DITEC, a. s. Žiadna jeho časť sa nesmie akýmkoľvek spôsobom (elektronickým, mechanickým) poskytnúť tretej strane, rozmnožovať, kopírovať, vrátane spätného prevodu do elektronickej podoby, bez písomného povolenia spracovávateľa.

Dokument:	D.Signer .NET 5.0 - Používateľská príručka
Dátum vypracovania:	6.8.2025
Ref. číslo dokumentu:	DTCKEP.10
Verzia:	3

Formulár:	Dokumentácia KEP komponentov - DSF cmpnts
Dátum poslednej aktualizácie:	12.02.2025
Ref. číslo:	Fo 154_1
Verzia:	1.01

Záznamy o zmenách

Verzia	Dátum	Popis zmien
1	11.3.2025	aktualizácia dokumentu pre novú verziu balíka aplikácií D.Suite/eIDAS
2	12.6.2025	úprava textov; zmenené obrázky podpisového certifikátu a naskenovania QR kódom pri podpisovaní mobilom
3	6.8.2025	úprava kapitoly Mobilné zariadenie, Trademarks

Obsah

1. Úvod 5
2. Zoznam použitých skratiek 6
3. Popis aplikácie 8
4. Systémové požiadavky 10
5. Inštalácia a odinštalácia 12
5.1. Inštalácia 12
5.2. Odinštalácia 17
6. Používateľské nastavenia 18
6.1. Všeobecné nastavenia aplikácie 18
6.2. Výber poskytovateľa 21
6.2.1. Pridanie používateľského poskytovateľa 22
6.2.2. Úprava poskytovateľa 23
6.2.3. Odobratie poskytovateľa 24
6.3. Sieťové nastavenia 24
6.4. Parametre podpisu 27
6.5. Podpísaný dokument / Podpísané XML 29
6.6. O aplikácii 30
7. Vytvorenie ZEP/KEP používateľom 32
7.1. Načítanie vstupných parametrov 32
7.2. Zobrazenie podpisovaných dát 32
7.2.1. Zobrazenie dokumentov 36
7.3. Nastavenie dátumu a času vytvorenia podpisu 37
7.4. Podpísanie dokumentu 40
7.4.1. Mobilné zariadenie 42
7.4.2. Pracovná stanica 52
7.5. Zobrazenie parametrov podpisu 60
8. Trademarks 63

1. Úvod

Tento dokument je určený pre používateľov aplikácie D.Signer .NET, resp. pre používateľov informačných systémov a aplikácií, v rámci ktorých bude aplikácia D.Signer .NET pre zaručený/kvalifikovaný elektronický podpis (ZEP/KEP) integrovaná.

Jednotlivé časti dokumentácie aplikácie D.Signer .NET je možné použiť pri tvorbe používateľských príručiek týchto klientskych informačných systémov a aplikácií po dohode s vlastníkmi autorských práv aplikácie D.Signer .NET.

2. Zoznam použitých skratiek

CRL	Certificate Revocation List; zoznam zneplatnených certifikátov
HTML	HyperText Markup Language; hypertextový značkový jazyk na vytváranie webových stránok
HTTPS	HyperText Transfer Protocol Secure; zabezpečený hypertextový prenosový protokol
KEP	kvalifikovaný elektronický podpis
NBÚ	Národný bezpečnostný úrad
OCSP	Online Certificate Status Protocol
PDF	formát dokumentov Portable Document Format
PNG	grafický formát Portable Network Graphics
QSCD	Qualified Signature Creating Device; zariadenie na vytváranie kvalifikovaného podpisu
SSCD	Secure Signature Creating Device; bezpečné zariadenie na vytváranie elektronického podpisu
TXT	formát textových súborov
XML	eXtensible Markup Language; rozšíriteľný značkovací jazyk pre štruktúrované dáta
XAdES	XML Advanced Electronic Signatures; formát pokročilého elektronického podpisu na báze XML
XAdES_ZEP	profil formátu elektronického podpisu XAdES pre ZEP
XAdES_ZEPbp	profil formátu kvalifikovaného elektronického podpisu na báze XAdES baseline profile

ZEP	Zaručený elektronický podpis

3. Popis aplikácie

Aplikácia D.Signer .NET predstavuje riešenie pre vytváranie zaručeného/kvalifikovaného elektronického podpisu (ZEP/KEP) nad množinou rôznych formátov dokumentov, resp. typov dát (XML dokumenty, PDF dokumenty atď.), prípadne nad ľubovoľnou kombináciou podporovaných formátov dát, ktoré spolu vytvárajú tzv. *multipart* dokument. Povolené formáty podpisovaných elektronických dokumentov v administratívnom styku špecifikuje Výnos MF SR č. 55/2014 o štandardoch pre IS VS. Požiadavky na formát a obsah podpisovaných dát stanovuje dokument NBÚ SR – Upresnenia obsahu a formálne špecifikácie formátov dokumentov pre ZEP, v1.0.

Zaručený/kvalifikovaný elektronický podpis na druhej strane zabezpečuje integritu podpísaných dát a nepopierateľnosť podpisu. Aplikácia D.Signer .NET môže byť teda nasadená v rámci akéhokoľvek systému, kde je potrebné zabezpečiť jednak integritu prenášaných a spracovávaných dokumentov, ako aj nepopierateľnosť identity ich podpisovateľa.

Aplikácia D.Signer .NET pred samotnou procedúrou vytvorenia ZEP/KEP v zmysle zákona č. 272/2016 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov:

- zabezpečí podpisovateľovi zobrazenie všetkých podpisovaných dát jednoznačným a adekvátnym spôsobom,
- zaručí, že dáta sa pri podpise nezmenia.

Pre vytvorenie ZEP/KEP musí byť aplikácia použitá len v súlade s platnou podpisovou politikou pre ZEP/KEP, ktorá bola schválená NBÚ SR. Používateľ je pred vytvorením podpisu povinný presvedčiť sa, že podpisová politika, ktorú aplikácia používa, je stále platná a nebola zo strany vydavateľa predčasne zrušená. Výrobca, resp. integrátor aplikácie D.Signer .NET je povinný zabezpečiť také nastavenie konfigurácie aplikácie a parametrov volania metód rozhrania aplikácie, aby aplikácia vytvárala podpis v súlade so špecifikovanou podpisovou politikou.

Za obsah a sformátovanie vstupných dát (dokumentov), ako aj za dodržanie správneho postupu vytvorenia ZEP/KEP, definovaného v rámci podpisovej politiky, je zodpovedný podpisovateľ. Za správne vyhodnotenie platnosti vytvoreného ZEP/KEP a za špecifikovanie parametrov procesu verifikácie ZEP/KEP v súlade s podpisovou politikou je zodpovedný prijímateľ alebo prevádzkovateľ systému, ktorý tieto dáta spracováva.

Požiadavky NBÚ SR na vytváraný formát ZEP/KEP upravuje dokument – Formáty zaručených elektronických podpisov, v3.0. Minimálne požiadavky EÚ na cezhraničné spracovanie dokumentov elektronicky podpísaných príslušnými orgánmi v zmysle smernice Európskeho parlamentu a Rady 2006/123/ES o službách na vnútornom trhu stanovuje rozhodnutie komisie 2014/148/EU, ktoré nahrádza rozhodnutie komisie 2011/130/EU. Špecifikácie týkajúce sa formátov zdokonalených elektronických podpisov a zdokonalených elektronických pečatí, ktoré môžu subjekty verejného sektora uznávať ustanovuje Rozhodnutie komisie 2015/1506/EU.

Aplikácia D.Signer .NET vytvára ZEP/KEP v súlade so schválenými formátmi pre zaručený elektronický podpis XAdES_ZEP, v1.0 (http://www.ditec.sk/ep/signature_formats/xades_zep/v1.0), XAdES_ZEP, v1.1 (http://www.ditec.sk/ep/signature_formats/xades_zep/v1.1), XAdES_ZEP, v2.0 (http://www.ditec.sk/ep/signature_formats/xades_zep/v2.0) a KEP v súlade s profilom pre kvalifikovaný elektronický podpis XAdES_ZEPbp, v1.0 (http://www.ditec.sk/ep/signature_formats/xades_zepbp/v1.0). Aplikácia D.Signer .NET vytvára typ podpisu XAdES_ZEP-EPES, resp. XAdES_ZEPbp-EPES, teda elektronický podpis rozšírený o informáciu o čase vzniku ZEP/KEP, o explicitnú podpísanú referenciu podpisovej politiky a podpísané informácie o typoch a formátoch podpísaných dátových objektov, a tiež XAdES_ZEP-T, resp. XAdES_ZEPbp-T, teda elektronický podpis rozšírený o časovú pečiatku podpisu. Aplikácia D.Signer .NET umožňuje vytvárať aj typ podpisu XAdES_ZEPbp-BES, to znamená typ elektronického podpisu bez explicitne uvedenej referencie podpisovej politiky, v súlade s príslušnými nariadeniami komisie 2011/130/EU, 2014/148/EU, 2015/1506/EU a príslušným baseline profilom pre XAdES ETSI TS 103 171.

Aplikácia D.Signer .NET môže byť použitá taktiež pre vytváranie tzv. obyčajného elektronického podpisu zmysle zákona č. 272/2016 Z. z. o elektronickom podpise.

V súlade s §4, odsek (5) zákona č. 305/2013 Z. z. o e-Governmente v znení neskorších predpisov je aplikácia D.Signer .NET implementovaná takým spôsobom, aby poskytovala funkcionalitu vytvorenia ZEP/KEP aj pre osoby so zdravotným postihnutím – pre slabozrakých a nevidiacich pomocou technológie NVDA (http://www.nvaccess.org/).

Aplikácia D.Signer .NET je lokalizovaná v slovenskom, v anglickom a v nemeckom jazyku.

4. Systémové požiadavky

Systémové požiadavky aplikácie D.Signer .NET sú nasledujúce:

- operačný systém MS Windows 7 SP1 / 8 / 8.1 / 10 / 11,
- procesor (architektúra CPU): x86, x86_64,
- platforma – .NET framework, verzia 4.6.2 alebo vyššia,
- občiansky preukaz s čipom alebo iné certifikované SSCD/QSCD zariadenie pre generovanie kľúčových párov a vytváranie elektronického podpisu + čítačka a ovládače podľa odporúčaní akreditovanej certifikačnej autority (ACA); prípadne PKCS#12/PFX súbor ako úložisko podpisového certifikátu,
- príslušná CSP implementácia MS CryptoAPI alebo implementácia KSP providera CNG alebo štandardu PKCS#11; súčasť softvéru dodávaného s SSCD/QSCD zariadením,
- prístup na internet (prípadne správne nastavenia pre proxy),
- správne nastavený systémový dátum a čas.

Ak je aplikácia D.Signer .NET spúšťaná z web portálu pomocou aplikácie D.Launcher v2.x, tak požiadavky na web prehliadač sú nasledujúce:

- Mozilla Firefox verzia 128 (ESR), 138 alebo vyššia, vyžaduje nainštalované a povolené rozšírenie D.Bridge 2
- Google Chrome verzia 136 alebo vyššia, vyžaduje nainštalované a povolené rozšírenie D.Bridge 2
- Chromium verzia 136 alebo vyššia, vyžaduje nainštalované a povolené rozšírenie D.Bridge 2
- Opera verzia 118 alebo vyššia, vyžaduje nainštalované a povolené rozšírenie D.Bridge 2
- Microsoft Edge verzia 131 alebo vyššia, vyžaduje nainštalované a povolené rozšírenie D.Bridge 2.

D.Signer .NET x64 je možné spúšťať výlučne pomocou aplikácie D.Launcher. Systémové požiadavky pre aplikáciu D.Launcher sú špecifikované v rámci používateľskej príručky pre aplikáciu D.Launcher.

Pri vytváraní zaručeného/kvalifikovaného elektronického podpisu pomocou aplikácie D.Signer .NET sa vyžaduje použitie certifikovaného zariadenia pre generovanie a uloženie privátneho kľúča a pre vytvorenie zaručeného/kvalifikovaného elektronického podpisu (SSCD/QSCD – napr. čipová karta, USB token apod.) a použitie kvalifikovaného certifikátu, vydaného akreditovanou certifikačnou autoritou. Ak príslušný právny úkon vyžaduje autorizáciu mandátnym kvalifikovaným certifikátom, používateľ musí zvoliť mandátny kvalifikovaný certifikát s príslušným oprávnením pre daný úkon podľa osobitného predpisu. Zoznam zobrazených certifikátov, ktoré sú k dispozícii pre vytvorenie elektronického podpisu, je možné riadiť nastavením filtra certifikátov v okne pre výber certifikátu v aplikácii D.Signer .NET. Aplikácia D.Signer .NET pristupuje k danému SSCD/QSCD zariadeniu prostredníctvom príslušného CSP providera (implementácia MS Crypto API pre dané SSCD/QSCD zariadenie) alebo implementácie KSP providera CNG alebo prostredníctvom príslušnej implementácie PKCS#11 rozhrania.

Pre aplikáciu D.Signer .NET nie sú potrebné vyššie hardwarové požiadavky, ako vyžaduje samotný operačný systém, prípadne platforma .NET framework 4.6.2 alebo vyššia.

Aplikácia D.Signer .NET môže byť distribuovaná na inštalačnom médiu alebo v rámci klientskej aplikácie, ktorá komponent pre zaručený/kvalifikovaný elektronický podpis používa, či už v rámci jej inštalačných súborov alebo priamo cez Internet na HTTPS stránkach danej web aplikácie.

Podrobný popis požiadaviek na prevádzku aplikácie D.Signer .NET, teda požiadaviek na SSCD/QSCD zariadenie, požiadaviek na prevádzkové prostredie aplikácie, bezpečnostných požiadaviek apod. je špecifikovaný v rámci dokumentu Požiadavky na prevádzkové prostredie a SSCD.

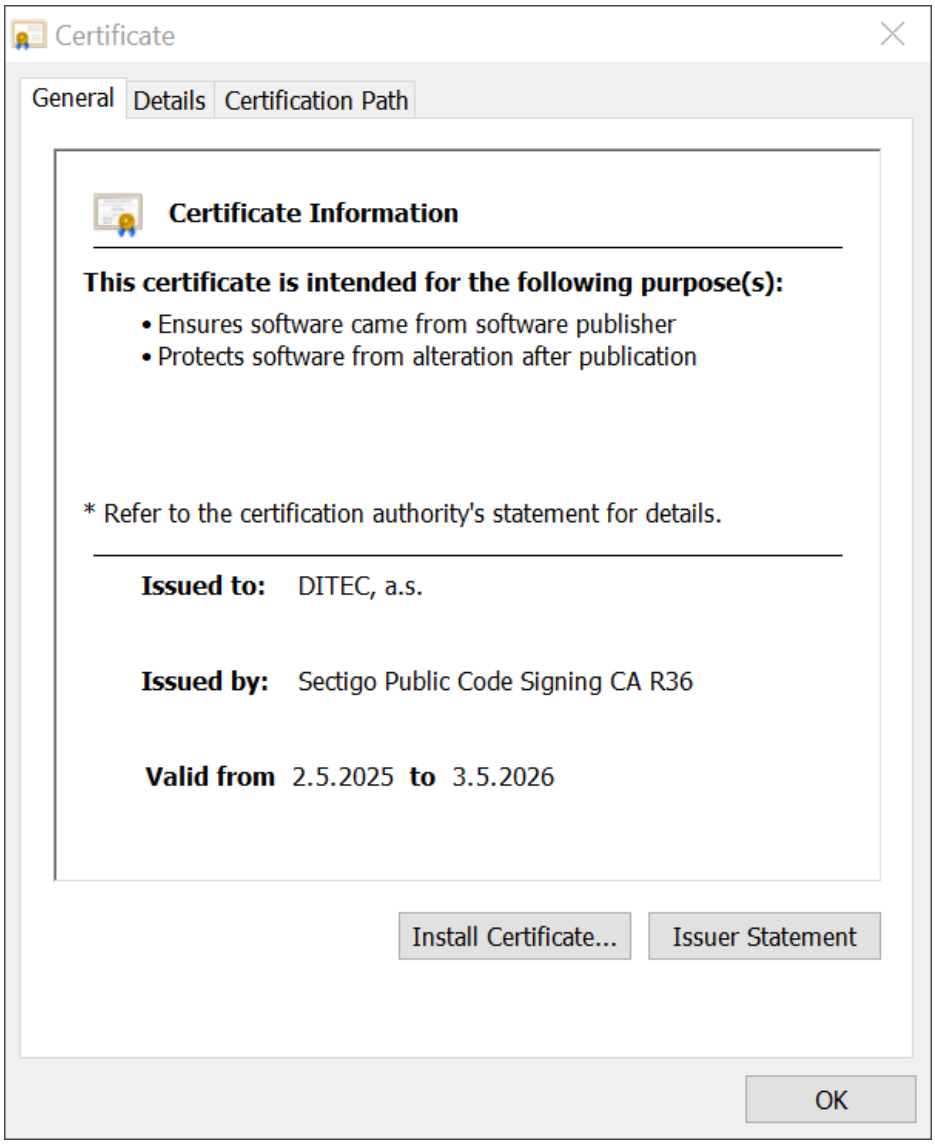
Špecifické systémové požiadavky pre jednotlivé pluginy aplikácie D.Signer .NET sú uvedené v rámci príslušnej integračnej príručky pre daný plugin.

5. Inštalácia a odinštalácia

5.1. Inštalácia

Inštalačný súbor aplikácie D.Signer .NET, resp. inštalačný súbor balíka aplikácií D.Suite/eIDAS odporúčame stiahnuť len z dôveryhodného zdroja a následne odporúčame tiež overiť jeho integritu. Integritu inštalačného súboru balíka aplikácií D.Suite/eIDAS je možné overiť náhľadom na vlastnosti inštalačného programu. Všetky inštalačné súbory musia byť podpísané certifikátom spoločnosti DITEC, a.s., ktorého vydavateľom je certifikačná autorita Sectigo, a je na ne vyžiadaná časová pečiatka. To isté platí aj pre všetky aplikačné súbory s vykonateľným kódom (.exe a .dll súbory), ktoré tvoria aplikáciu.

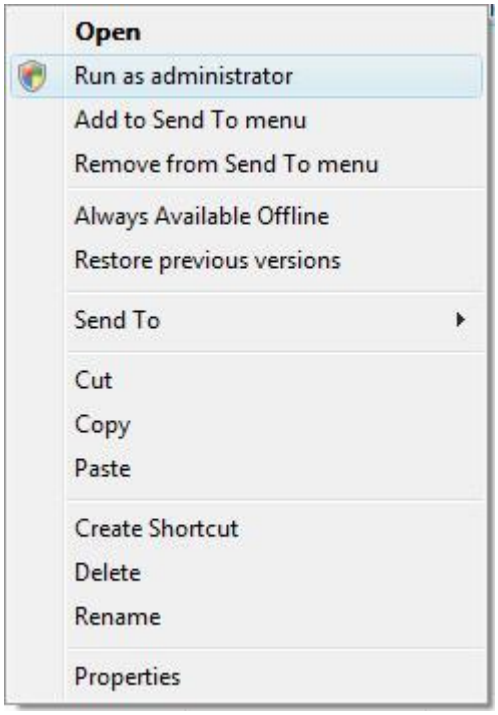
Na nasledujúcom obrázku je zobrazený náhľad na aktuálny podpisový certifikát spoločnosti DITEC, a.s.



Okrem elektronického podpisu certifikátom spoločnosti DITEC, a.s. sú .NET assembly zabezpečené aj pomocou tzv. strong name. Pre príslušný počítač, na ktorom je aplikácia D.Signer .NET nainštalovaná, resp. pre príslušnú klientsku aplikáciu musí byť vypnutý tzv. strong name bypass. Daná kontrola sa

uplatňuje napr. pri spustení aplikácie D.Signer .NET – aplikácia načíta len také plugin moduly, ktoré boli podpísané tým istým kľúčom ako hlavná aplikácia.[1]

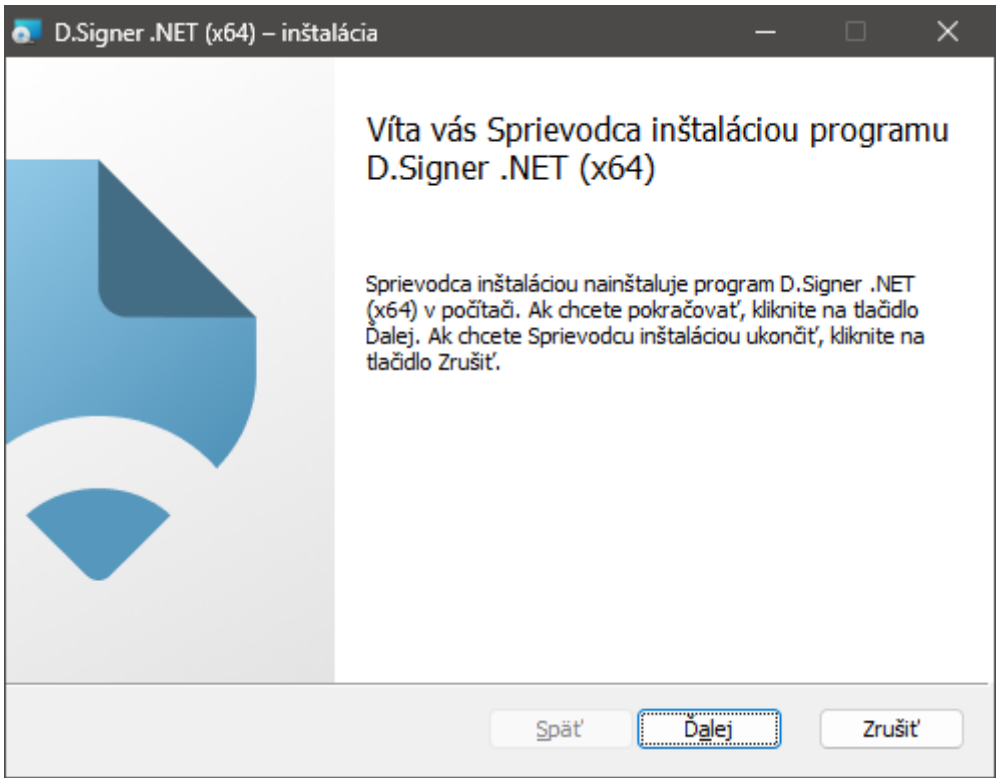
Inštalácia samotnej aplikácie D.Signer .NET sa vykoná spustením inštalačného programu. Pre úspešnú inštaláciu musí mať používateľ v rámci operačného systému administrátorské privilégia. V novších verziách operačného systému MS Windows je možné spustiť inštaláciu aplikácie D.Signer .NET alebo celého balíka aplikácií D.Suite/eIDAS pod administrátorskými privilégiami z kontextového menu.



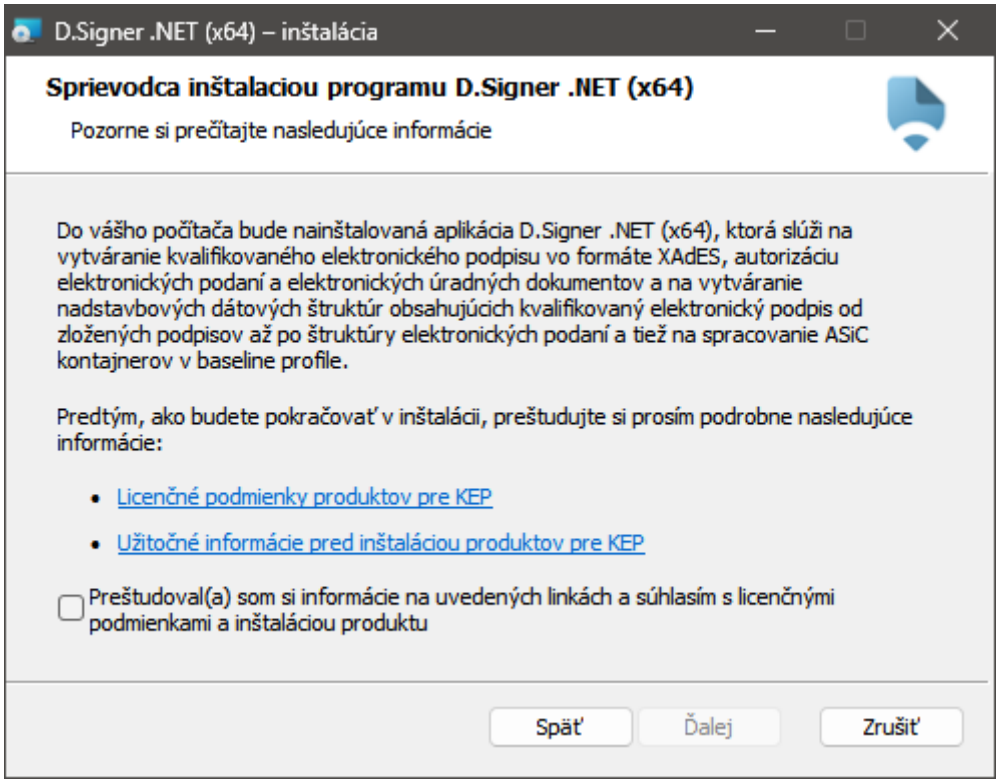
Pozor! Keďže pri inštalácii aplikácie D.Signer .NET je potrebné zaregistrovať v rámci operačného systému Windows aj komponenty pre integráciu aplikácie D.Signer .NET do web stránok internetových aplikácií, odporúčame pred spustením inštalačného programu zavrieť otvorené internetové prehliadače.

Po spustení inštalačného programu sa používateľovi zobrazí úvodná obrazovka sprievodcu inštaláciou aplikácie D.Signer .NET.

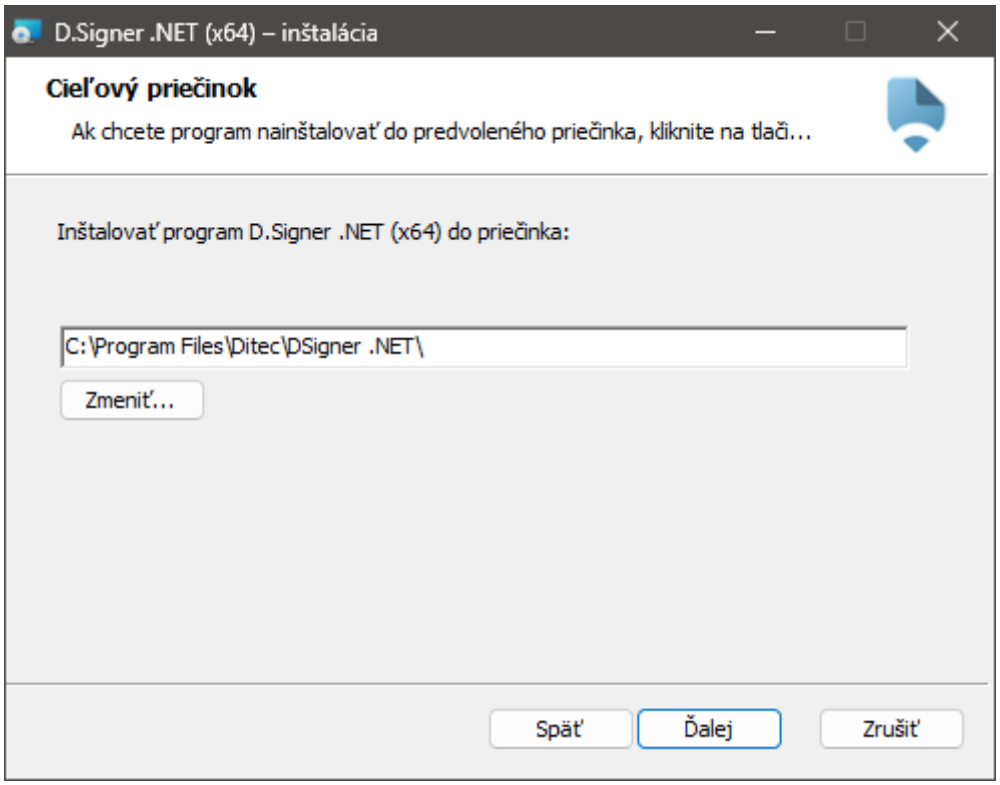
[1] Toto neplatí pre knižnice tretích strán, ktoré môže aplikácia D.Signer .NET využívať. Tieto by mali byť chránené príslušným certifikátom ich výrobcu.



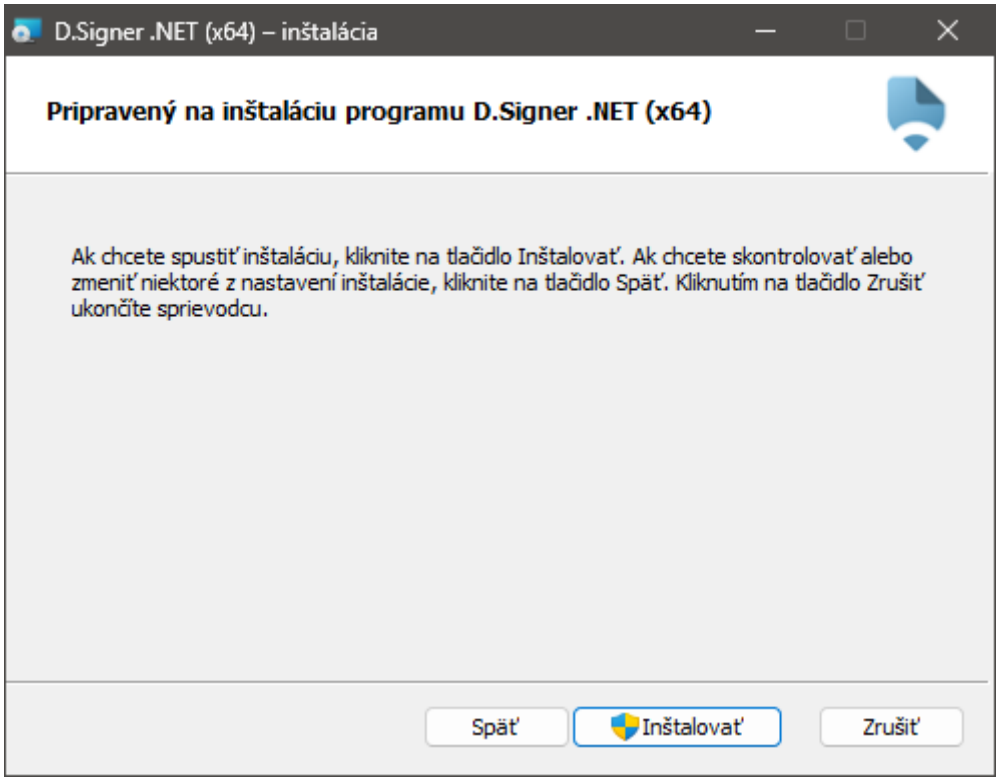
V ďalšom kroku je potrebné si preštudovať licenčné podmienky produktov pre KEP a užitočné informácie pred inštaláciou a potvrdiť súhlas s licenčnými podmienkami a inštaláciou produktu.



V ďalšom kroku používateľ potvrdí tlačidlom "Ďalej" predvolený adresár, prípadne si zvolí iný adresár, do ktorého bude aplikácia D.Signer .NET nainštalovaná.

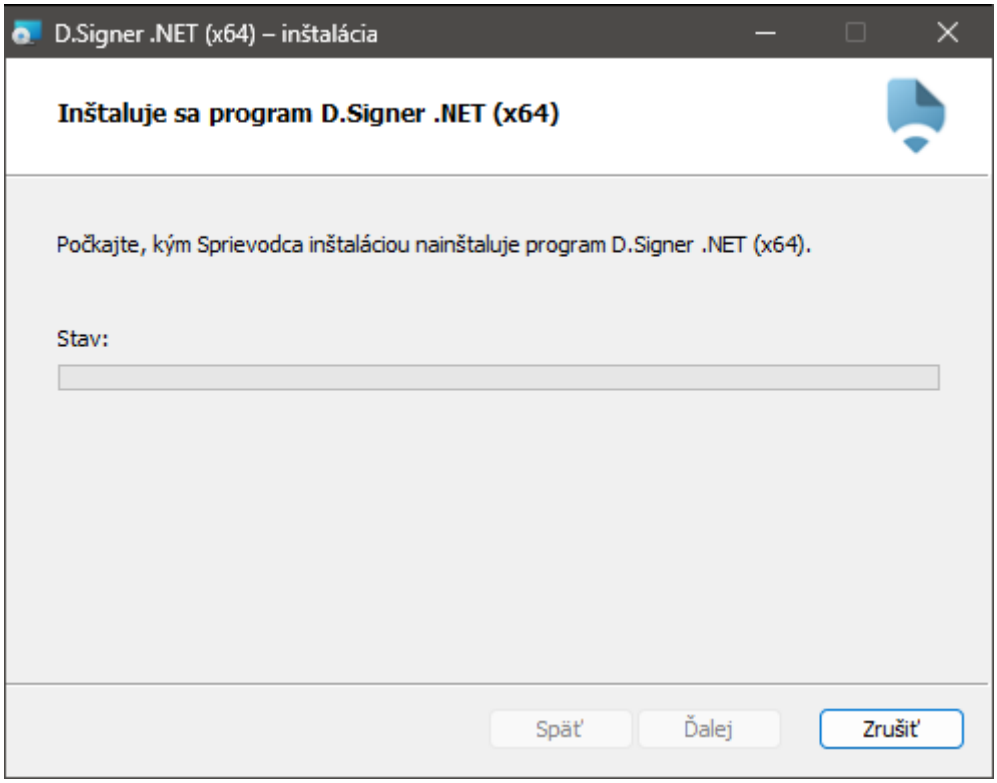


V ďalšom kroku používateľ potvrdí kliknutím na tlačidlo "Inštalovať" inštaláciu aplikácie D.Signer .NET na svoj počítač.

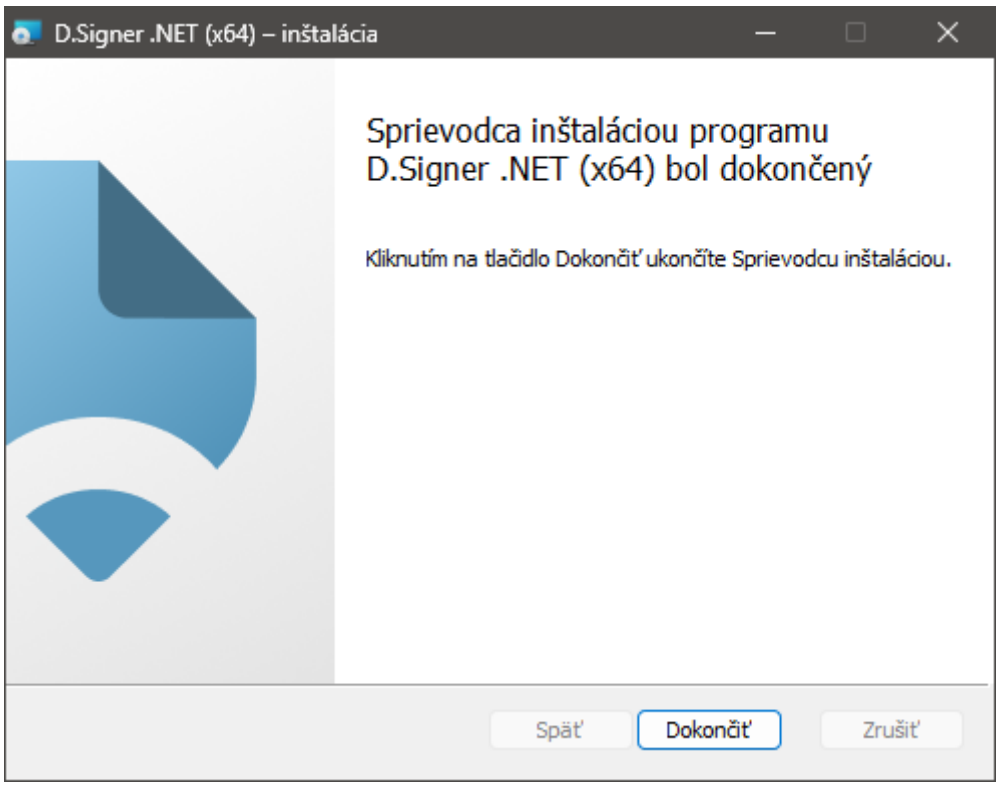


Kliknutím na tlačidlo "Inštalovať" sa spustí samotná inštalácia. Inštalačný program skopíruje požadované aplikačné súbory do špecifikovaného adresára a zabezpečí zaregistrovanie komponentov aplikácie D.Signer .NET v rámci operačného systému Windows.

Používateľ je o priebehu inštalácie informovaný v okne inštalačného programu. V každom okamihu je možné inštaláciu aplikácie D.Signer .NET prerušiť kliknutím na tlačidlo "Zrušiť".

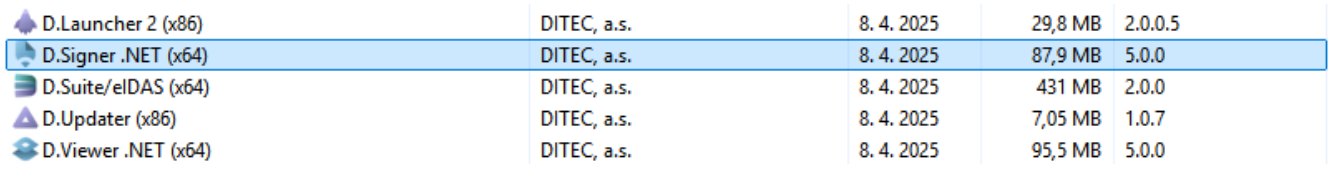


Na záver oznámi sprievodca inštaláciou úspešné dokončenie inštalácie aplikácie D.Signer .NET. Inštalácia sa ukončí po kliknutí na tlačidlo "Dokončiť".

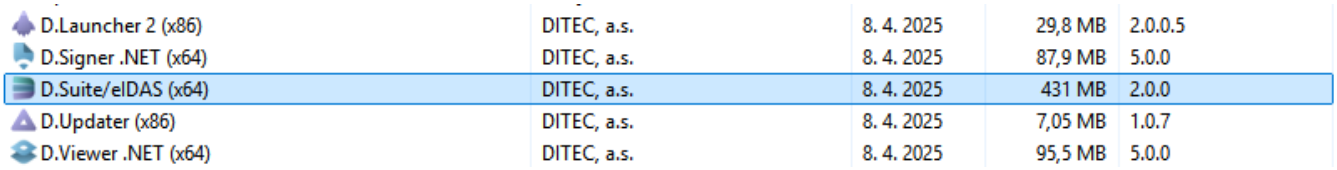


5.2. Odinštalácia

Pre odinštalovanie aplikácie D.Signer .NET otvorte Ovládací panel a kliknite na ikonu Programy a súčasti. V zozname nainštalovaných programov nájdite aplikáciu D.Signer .NET, kliknite pravým tlačidlom na vyvolanie kontextového menu a zvoľte „Odinštalovať".



V prípade, že ste aplikáciu D.Signer .NET nainštalovali v rámci inštalácie celého balíka aplikácií pre kvalifikovaný elektronický podpis D.Suite/eIDAS, tak odinštalovaním balíka D.Suite/eIDAS odinštalujete zároveň aj aplikáciu D.Signer .NET.

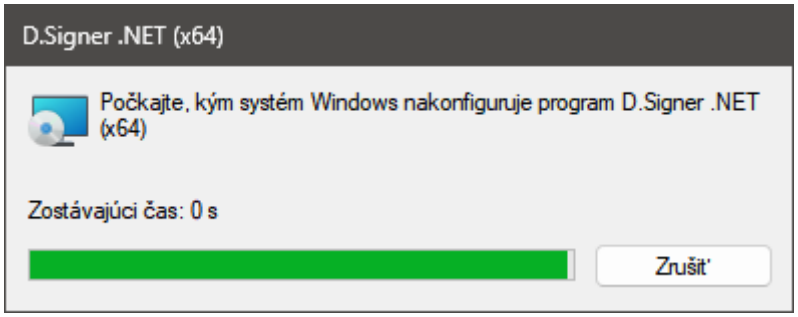


Windows zobrazí okno pre potvrdenie odinštalácie aplikácie D.Signer .NET. Ak chcete naozaj aplikáciu D.Signer .NET odinštalovať kliknite pre potvrdenie na tlačidlo „Áno".



Operačný systém Windows spustí proces odinštalácie, v rámci ktorého odstráni z počítača aplikačné súbory aplikácie D.Signer .NET a zabezpečí tiež odregistrovanie všetkých komponentov aplikácie D. Signer .NET v rámci operačného systému Windows.

Používateľ je o priebehu odinštalácie informovaný v okne odinštalačného programu. V každom okamihu je možné odinštaláciu aplikácie D.Signer .NET prerušiť kliknutím na tlačidlo „Zrušiť".



6. Používateľské nastavenia

Okno aplikácie pozostáva z 2 základných oblastí:

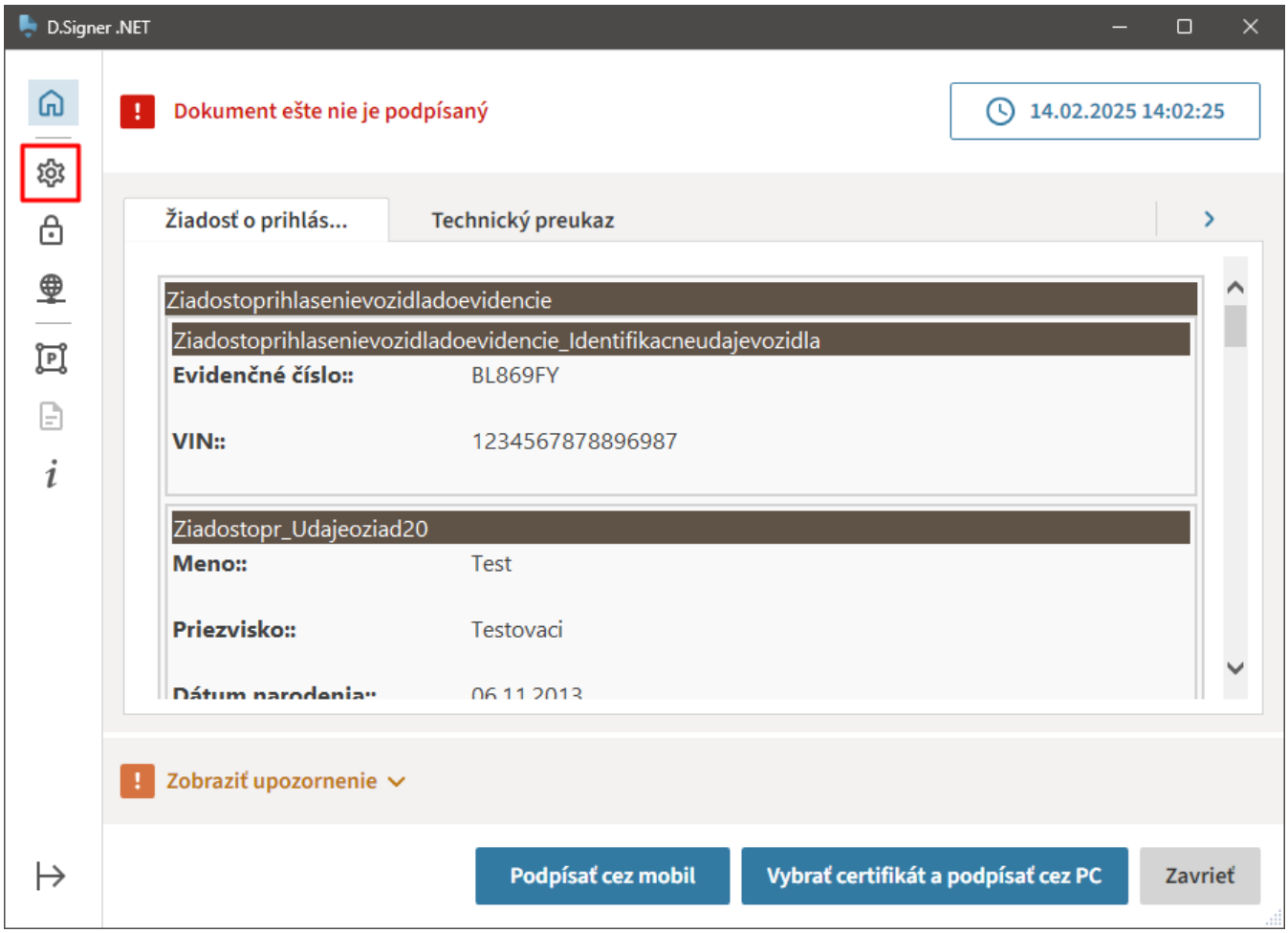
- Ľavá – menu, navigačné ikony s krátkym popisom
- Pravá – väčšia oblasť určená pre dynamický obsah aplikácie

Ľavá oblasť obsahuje ikony:

	**Hlavná obrazovka aplikácie**
	Všeobecné nastavenia
	Výber poskytovateľa
	Sieťové nastavenia
	Parametre podpisu
	Podpísaný dokument / Podpísané XML
	O aplikácii
	Zobraziť/Skryť názvy položiek menu

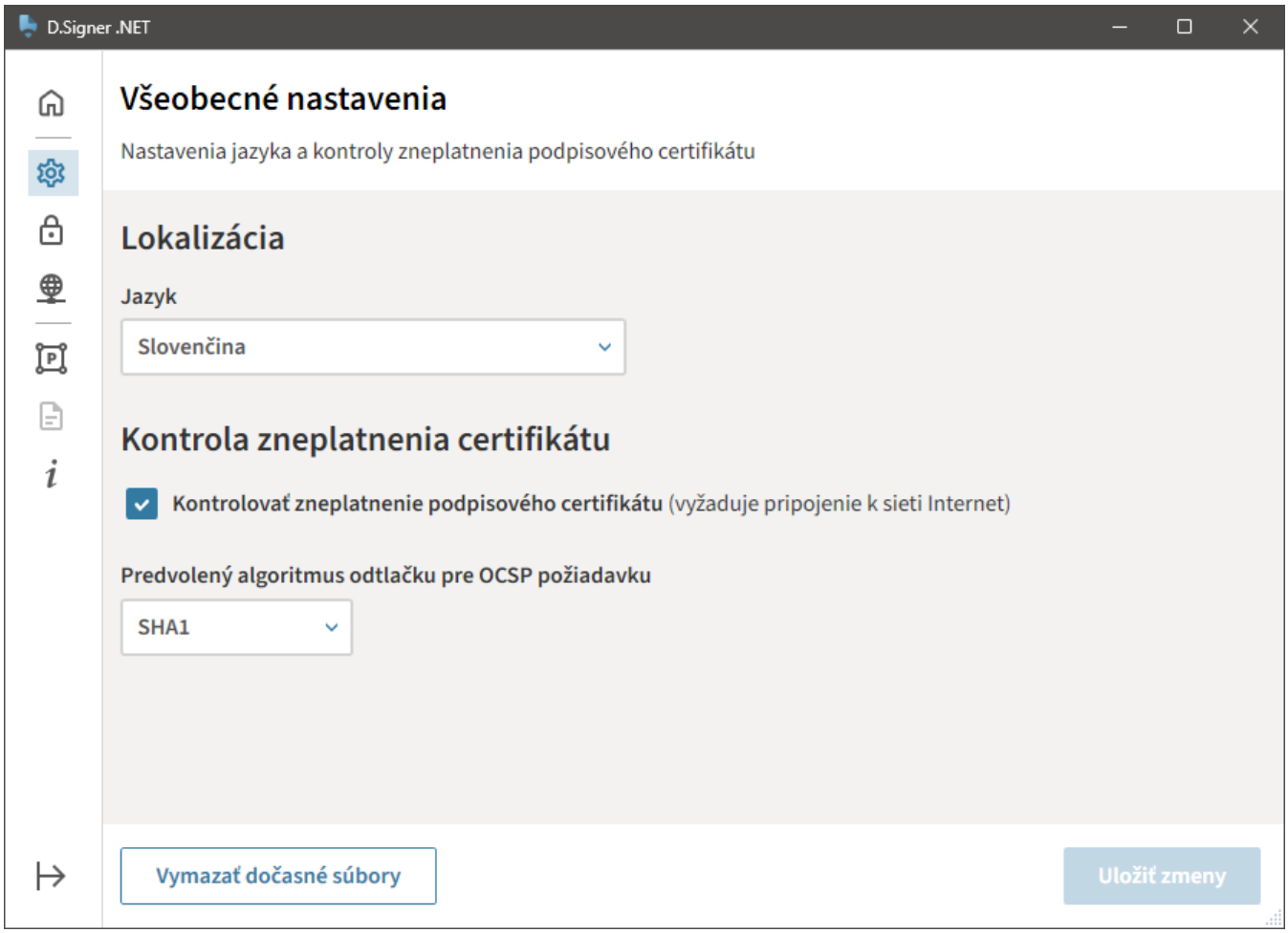
6.1. Všeobecné nastavenia aplikácie

Obrazovka s používateľskými nastaveniami aplikácie D.Signer .NET je prístupná z hlavného okna aplikácie D.Signer .NET prostredníctvom tlačidla "Všeobecné nastavenia".



V rámci všeobecných nastavení aplikácie D.Signer .NET môže používateľ zmeniť:

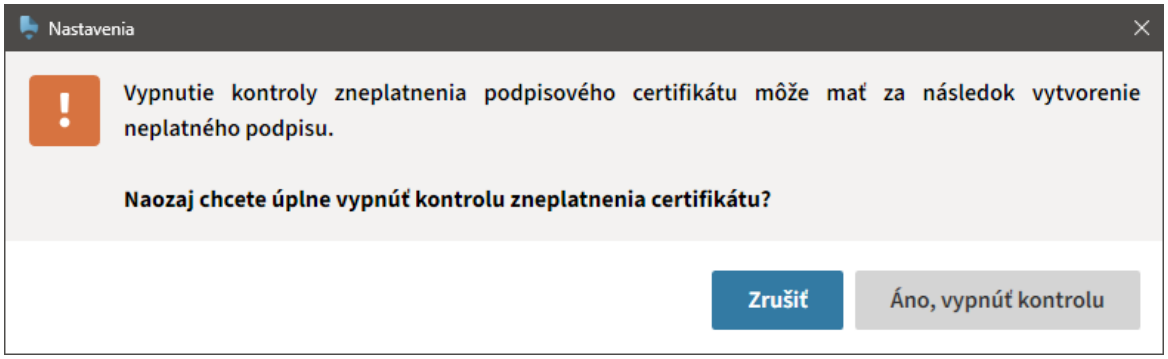
- nastavenie jazyka aplikácie,
- nastavenia kontroly zneplatnenia podpisového certifikátu pred podpisom.



Tlačidlo „Uložiť zmeny“ sa stane aktívnym po akejkoľvek zmene hodnôt na tejto obrazovke.

Jazyk aplikácie D.Signer .NET vyberá používateľ v rámci procesu inštalácie aplikácie. Nastavenie nového jazyka sa aplikuje okamžite po uložení zmien. V prípade vynútenia jazyka aplikácie D.Signer .NET z prostredia klientskej aplikácie nebude konfiguračné nastavenie jazyka aplikácie pre používateľa prístupné na zmenu.

Aplikácia D.Signer .NET pred vytvorením elektronického podpisu kontroluje, či zvolený podpisový certifikát nebol zneplatnený, resp. revokovaný. V prípade, že napríklad aplikácia nemá prístup na internet, je možné túto kontrolu v GUI Všeobecné nastavenia aplikácie D.Signer .NET vypnúť. Aplikácia v tom prípade vyžaduje potvrdenie vypnutia kontroly zneplatnenia certifikátu.



Pozor! Odporúčame nevypínať v konfiguračných nastaveniach kontrolu zneplatnenia podpisového certifikátu. Vypnutie kontroly zneplatnenia podpisového certifikátu môže mať za následok vytvorenie neplatného podpisu.

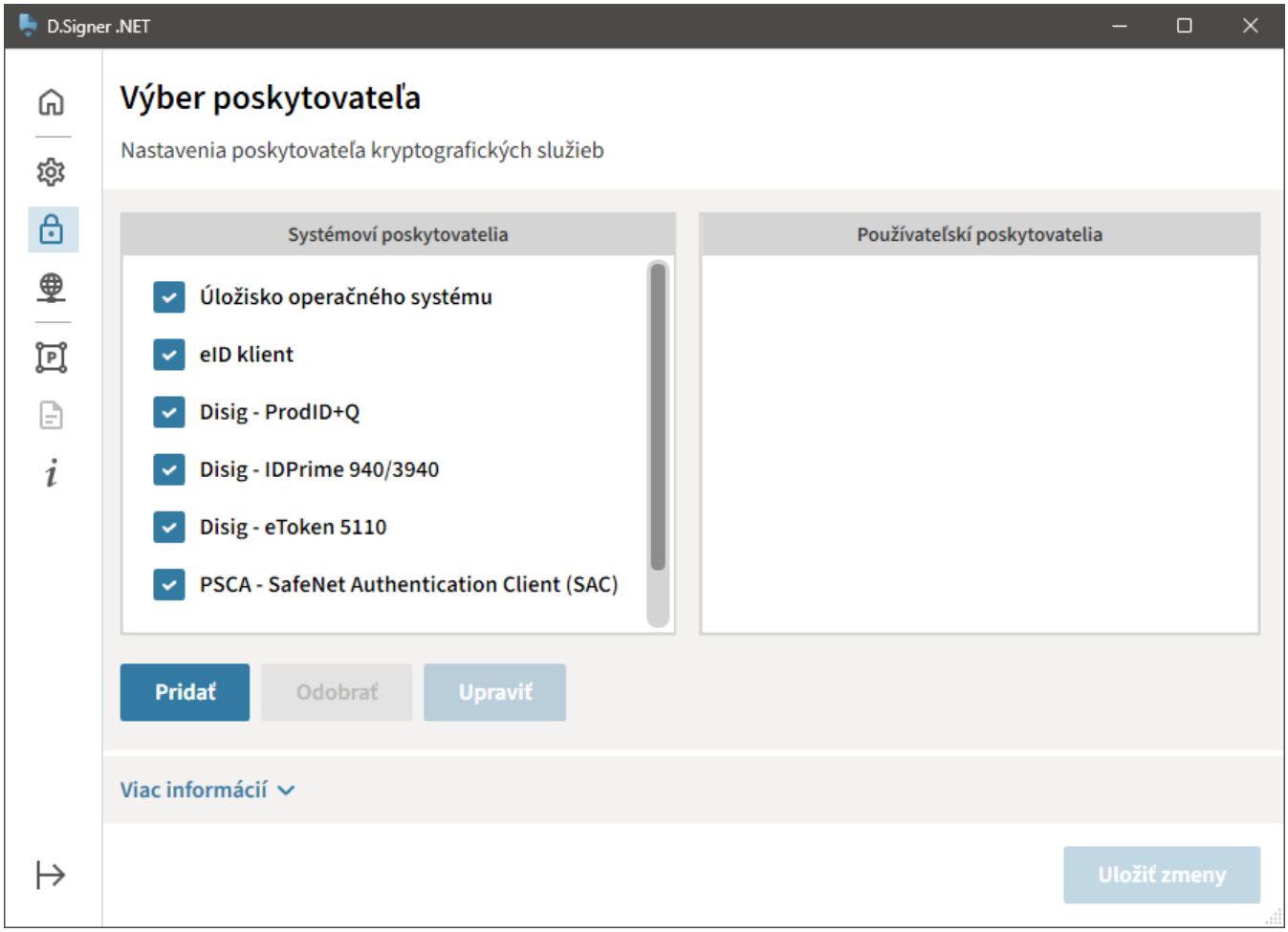
V nastaveniach kontroly zneplatnenia certifikátu je takisto možné zmeniť predvolený algoritmus odtlačku pre OCSP požiadavku v prípade, že certifikačná autorita, ktorá vydala podpisový certifikát podporuje pre OCSP službu iný algoritmus odtlačku pre OCSP požiadavku. V prípade vynútenia kontroly zneplatnenia certifikátu z prostredia klientskej aplikácie nebude konfiguračné nastavenie pre používateľa prístupné na zmenu.

Tlačidlo "Vymazať dočasné súbory" slúži na vymazanie uložených nastavení v internej databáze.

Tlačidlo "Uložiť zmeny" slúži na uloženie týchto nastavení a ich okamžité aplikovanie v aplikácii (napr. pri zmene jazyka).

6.2. Výber poskytovateľa

V rámci nastavení poskytovateľov kryptografických služieb si používateľ zvolí poskytovateľov, ktorých chce v aplikácii používať.



Ponúkame na výber z týchto skupín poskytovateľov:

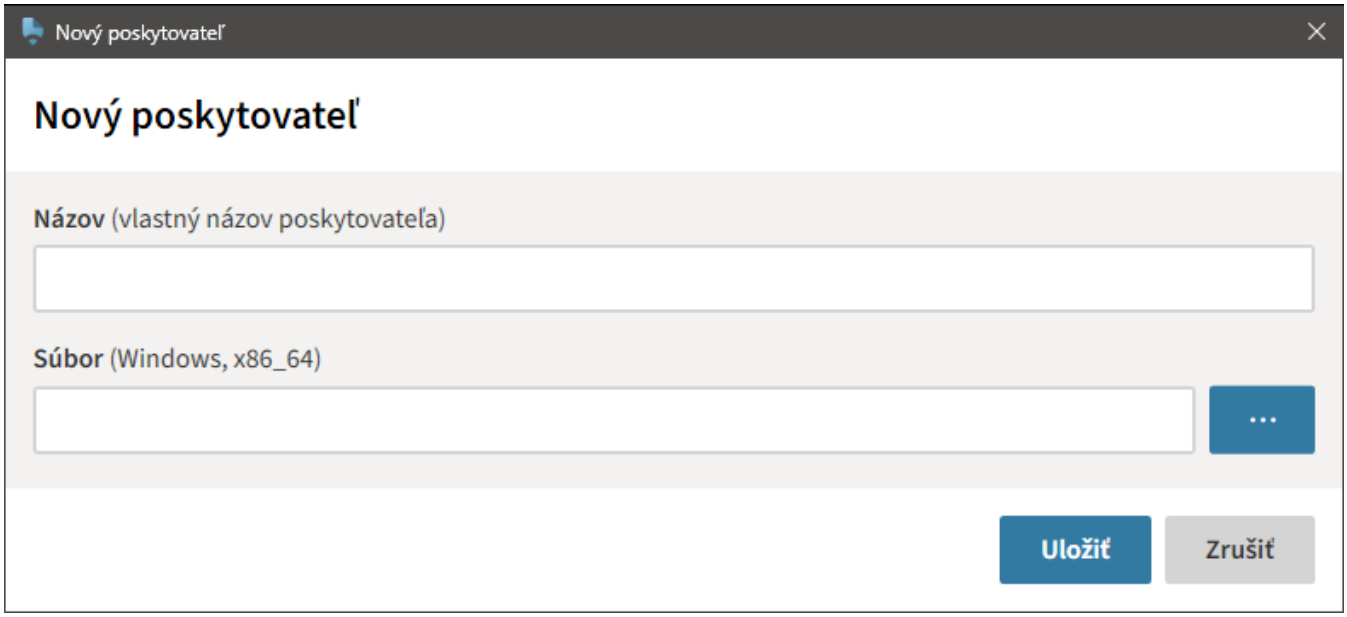
- Systémoví
- Používateľskí

Zoznam systémových poskytovateľov definuje výrobca aplikácie, prípadne dodávateľ. Týchto poskytovateľov používateľ nevie upravovať, ale môže ich zneaktívniť/aktivovať (kliknutím na checkbox).

Zoznam používateľských poskytovateľov si môže používateľ variabilne upravovať. Je možné pridať, editovať a odstrániť poskytovateľa. Všetky zmeny musí potvrdiť kliknutím na tlačidlo „Uložiť zmeny“.

6.2.1. Pridanie používateľského poskytovateľa

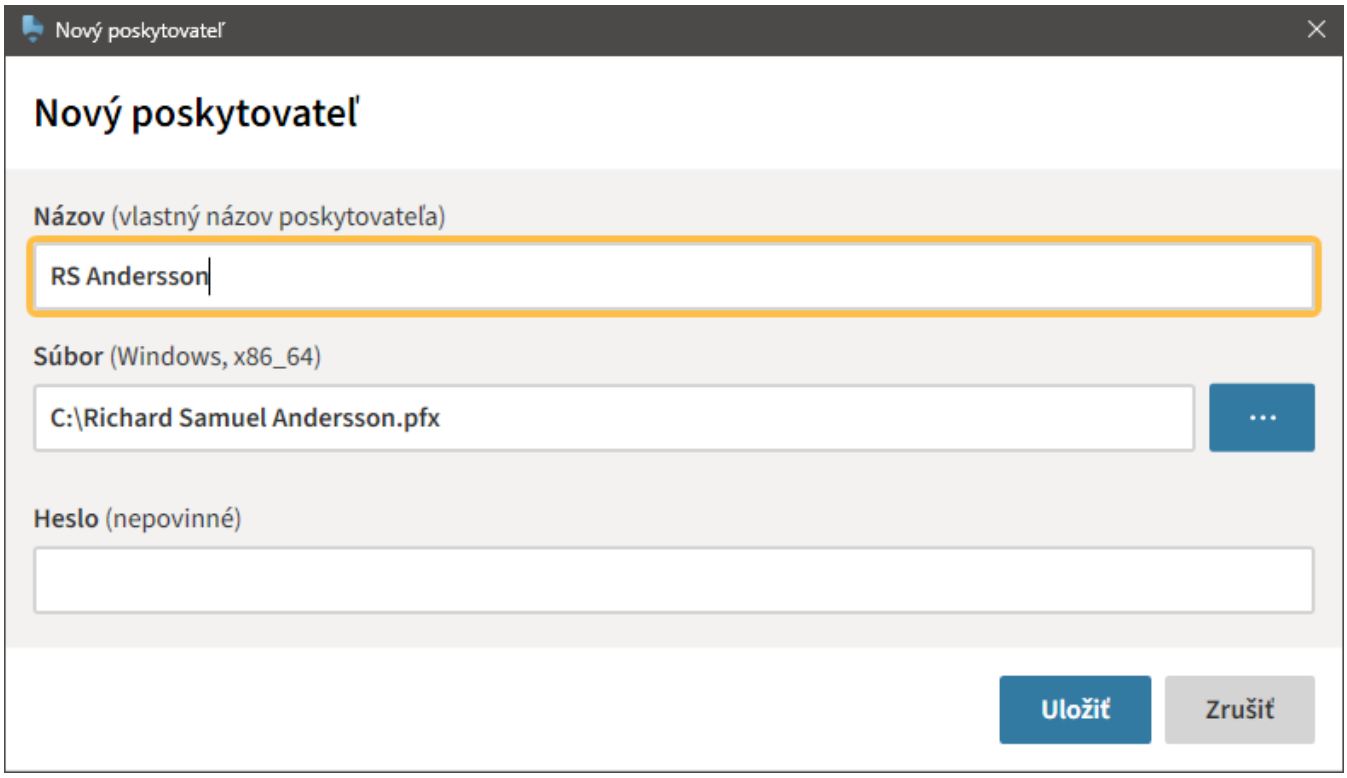
Kliknutím na tlačidlo „Pridať“ si používateľ môže pridať ďalšieho poskytovateľa.



Na pridanie poskytovateľa musí vyplniť všetky položky na obrazovke. Typ poskytovateľa sa určí na základe prípony súboru.

Súbor s príponou „dll“ predstavuje typ „PKCS#11“.

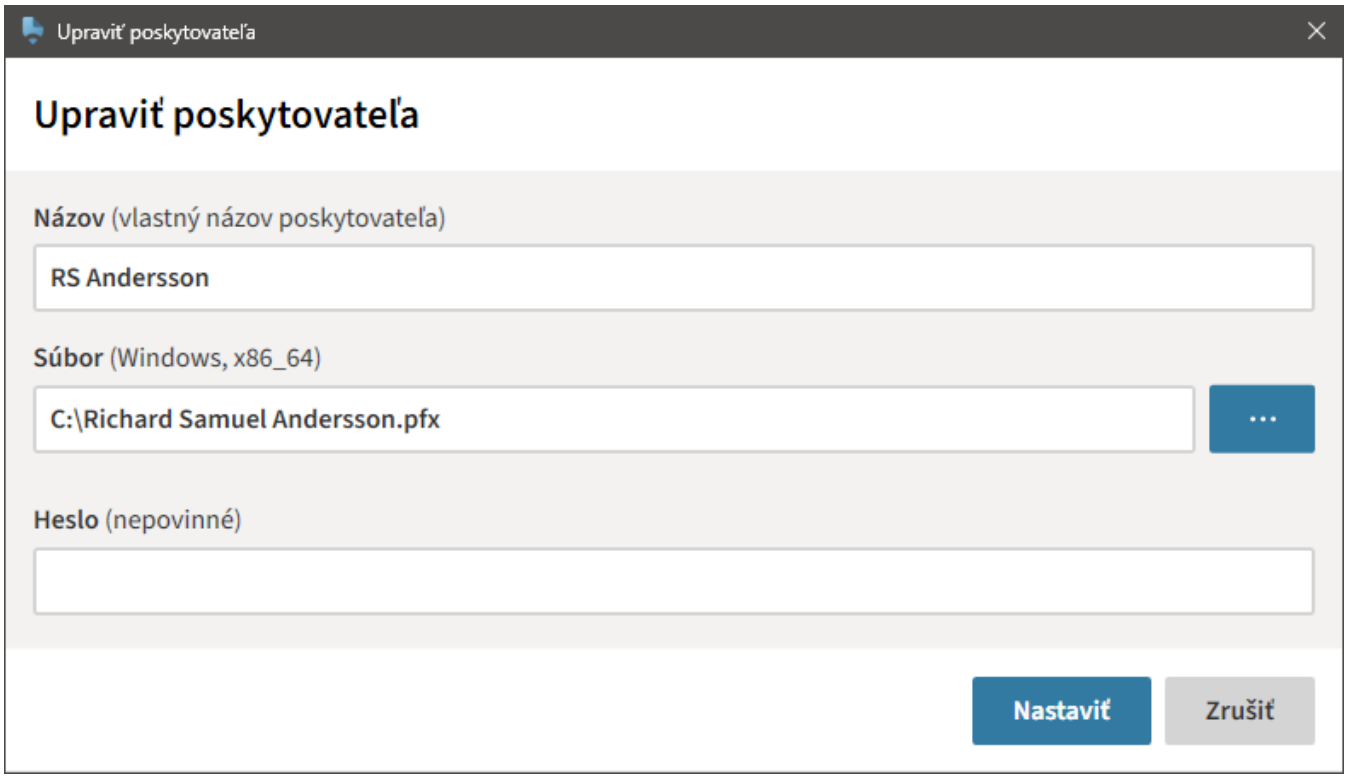
Súbor s príponou „pfx“ alebo „p12“ predstavuje typ „PKCS#12“. Aplikácia si môže k tomuto súboru zapamätať heslo, čo neskôr môže urýchliť proces podpisovania dokumentov. Ak heslo neuvedie, bude oň požiadaný pri každom podpisovaní dokumentov.



6.2.2. Úprava poskytovateľa

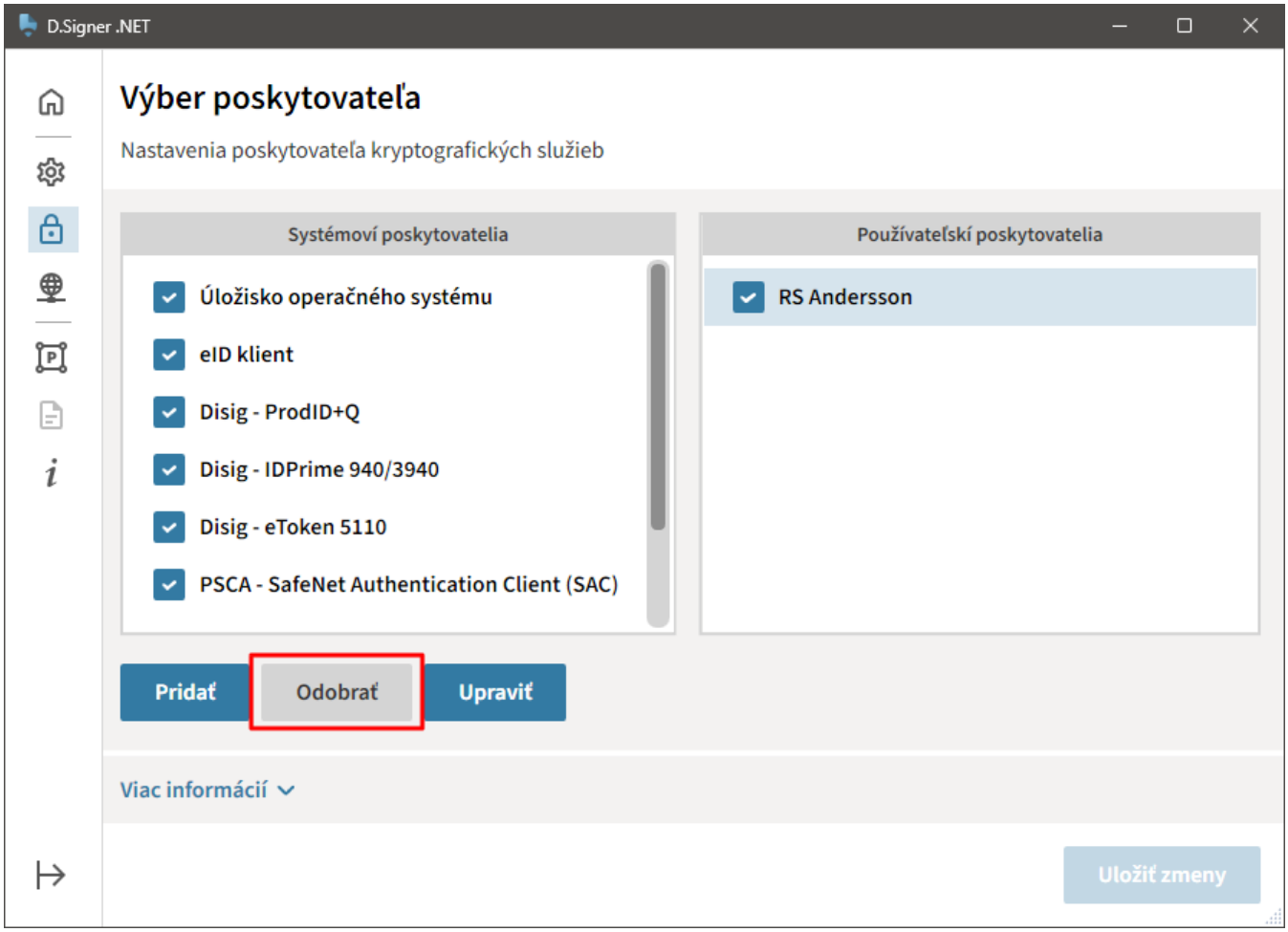
Po zvolení používateľského poskytovateľa a po kliknutí na tlačidlo „Upraviť“ vie používateľ upraviť tohto poskytovateľa. Upraviť môže každú z hodnôt na obrazovke.

Na obrázku je príklad pre typ „PKCS#12“. Pri type „PKCS#11“ sa neuvádza nepovinná položka „Heslo“.



6.2.3. Odobratie poskytovateľa

Po zvolení používateľského poskytovateľa a po kliknutí na tlačidlo „Odobrať“ bude tento poskytovateľ odobraný zo zoznamu.



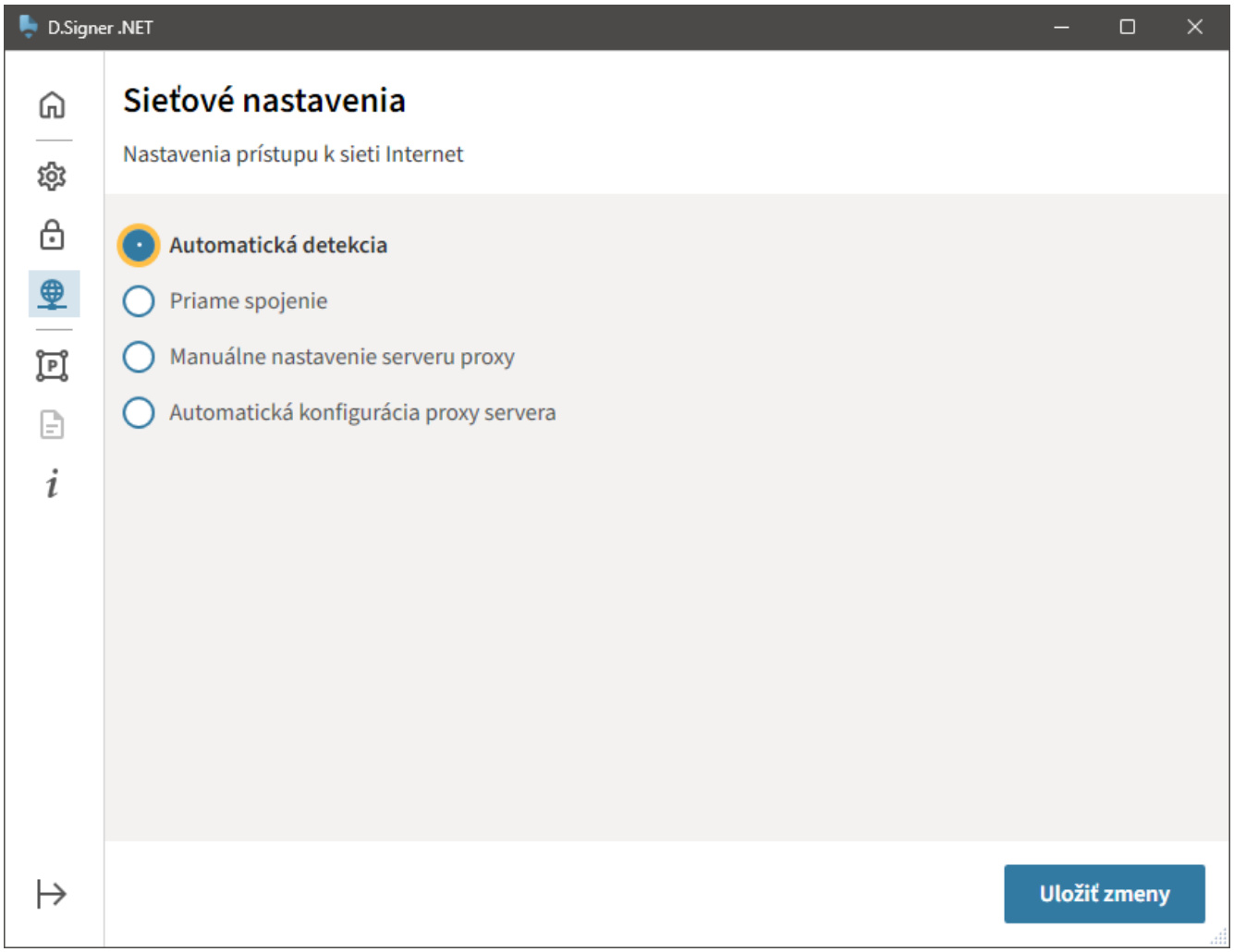
Aby sa táto zmena trvale prejavila je potrebné uložiť zmeny kliknutím na tlačidlo „Uložiť zmeny“.

6.3. Sieťové nastavenia

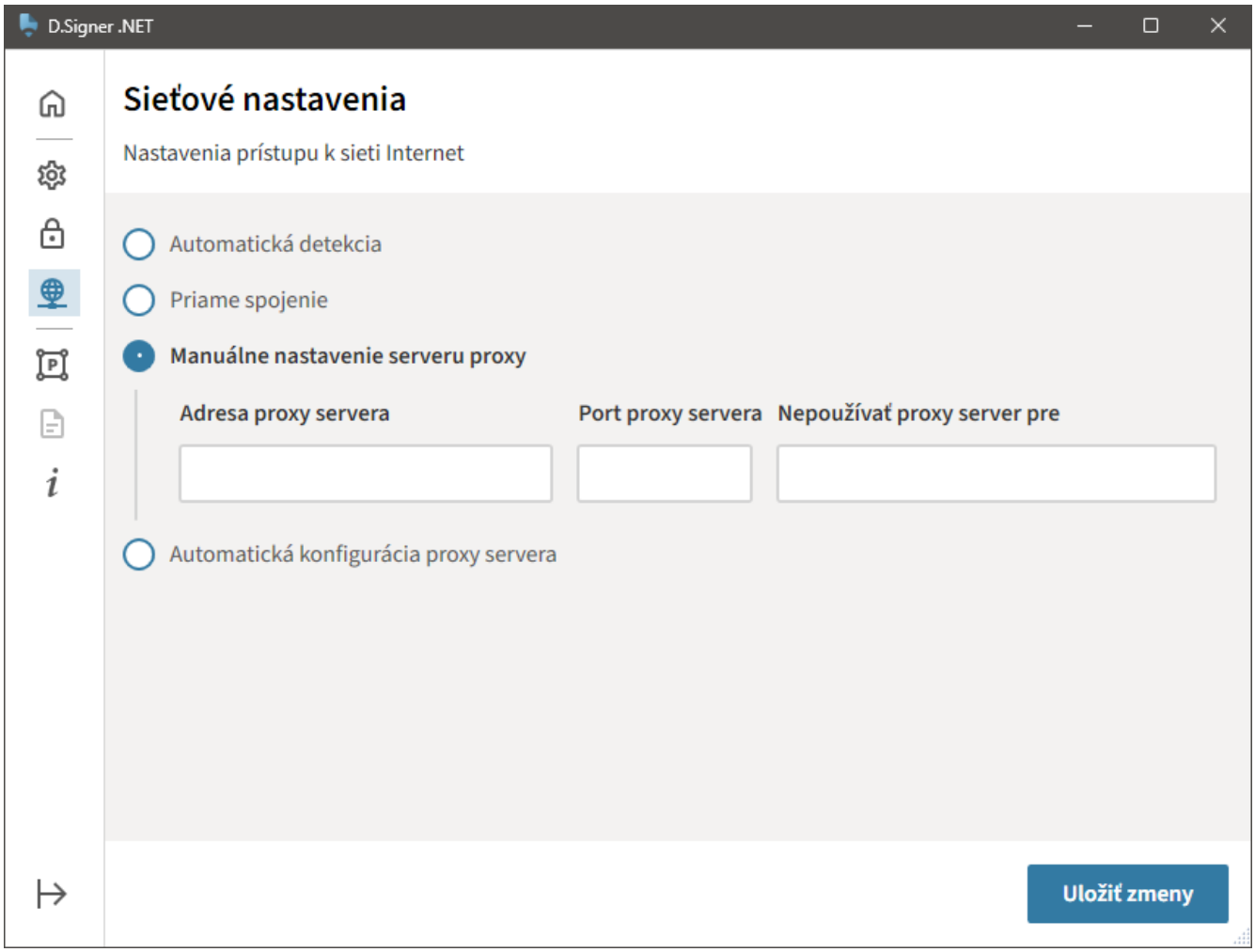
Konfigurácia sieťových nastavení umožňuje správne nastaviť prístup k sieti internet. Možnosti nastavenia prístupu sú nasledujúce:

- Automatická detekcia,
- Priame spojenie,
- Manuálne nastavenie serveru proxy,
- Automatická konfigurácia proxy servera (pomocou súboru PAC).

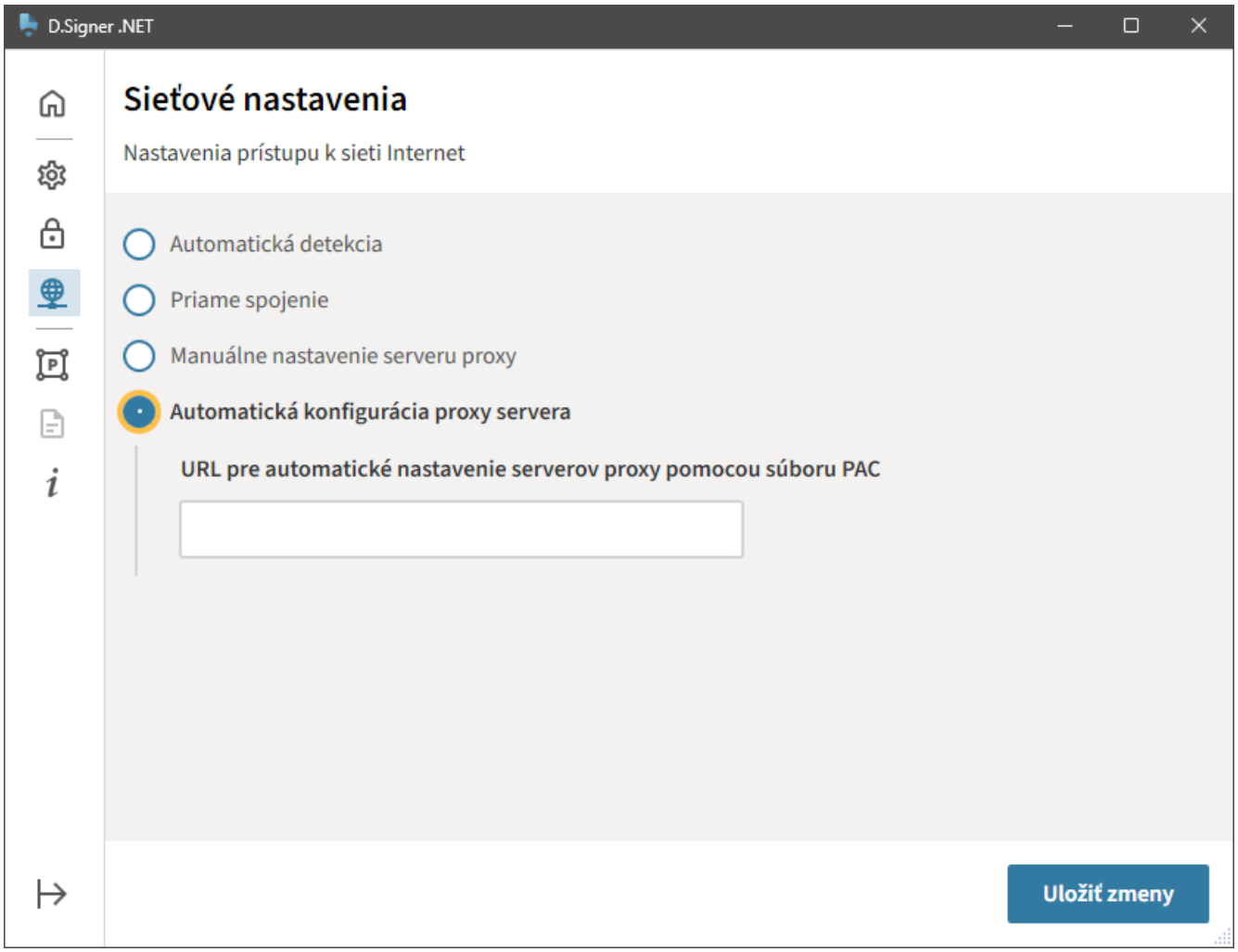
Posledné dve možnosti majú doplňujúce konfiguračné nastavenia.



Manuálne nastavenie proxy servera



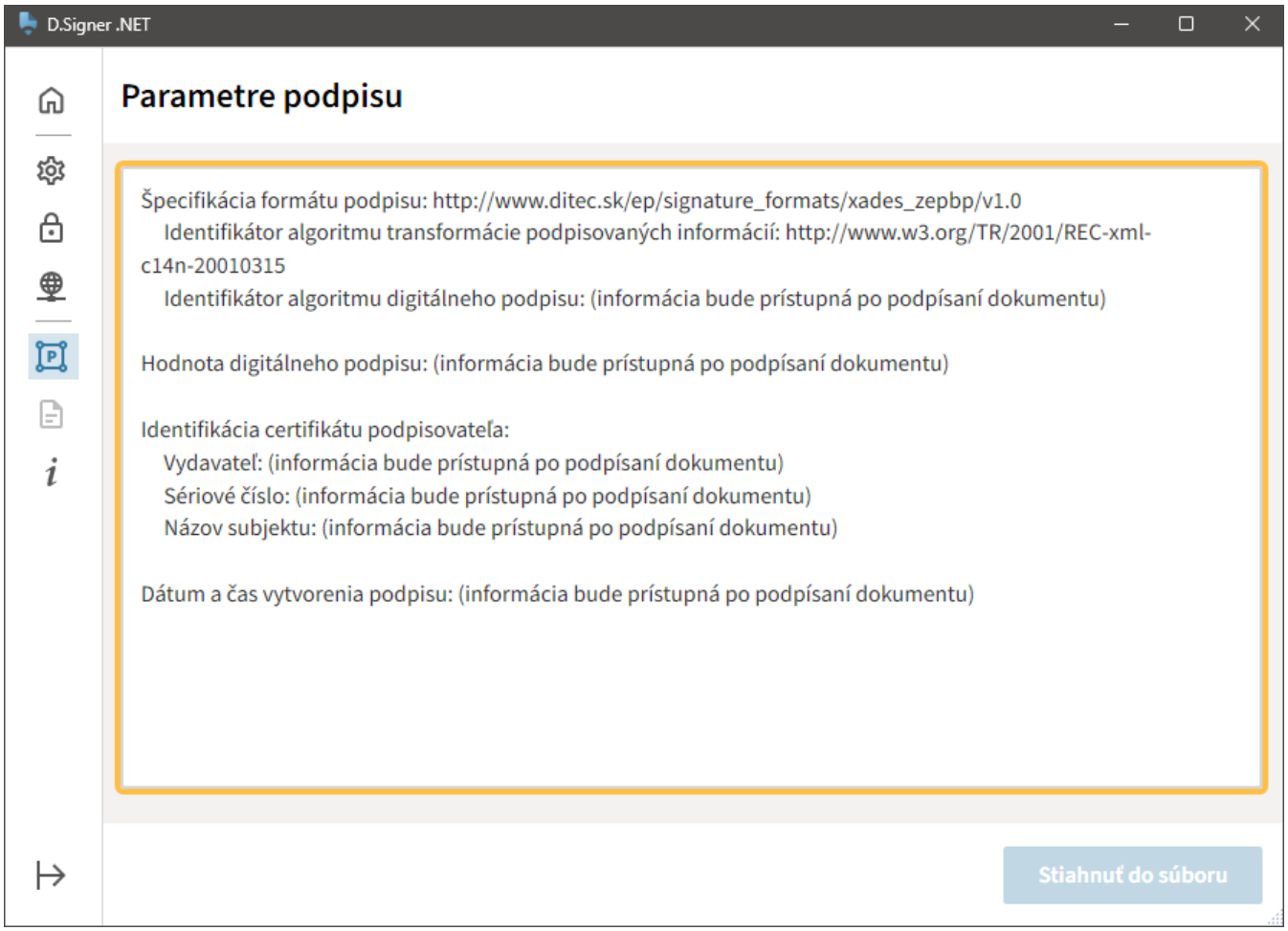
Automatická konfigurácia proxy servera



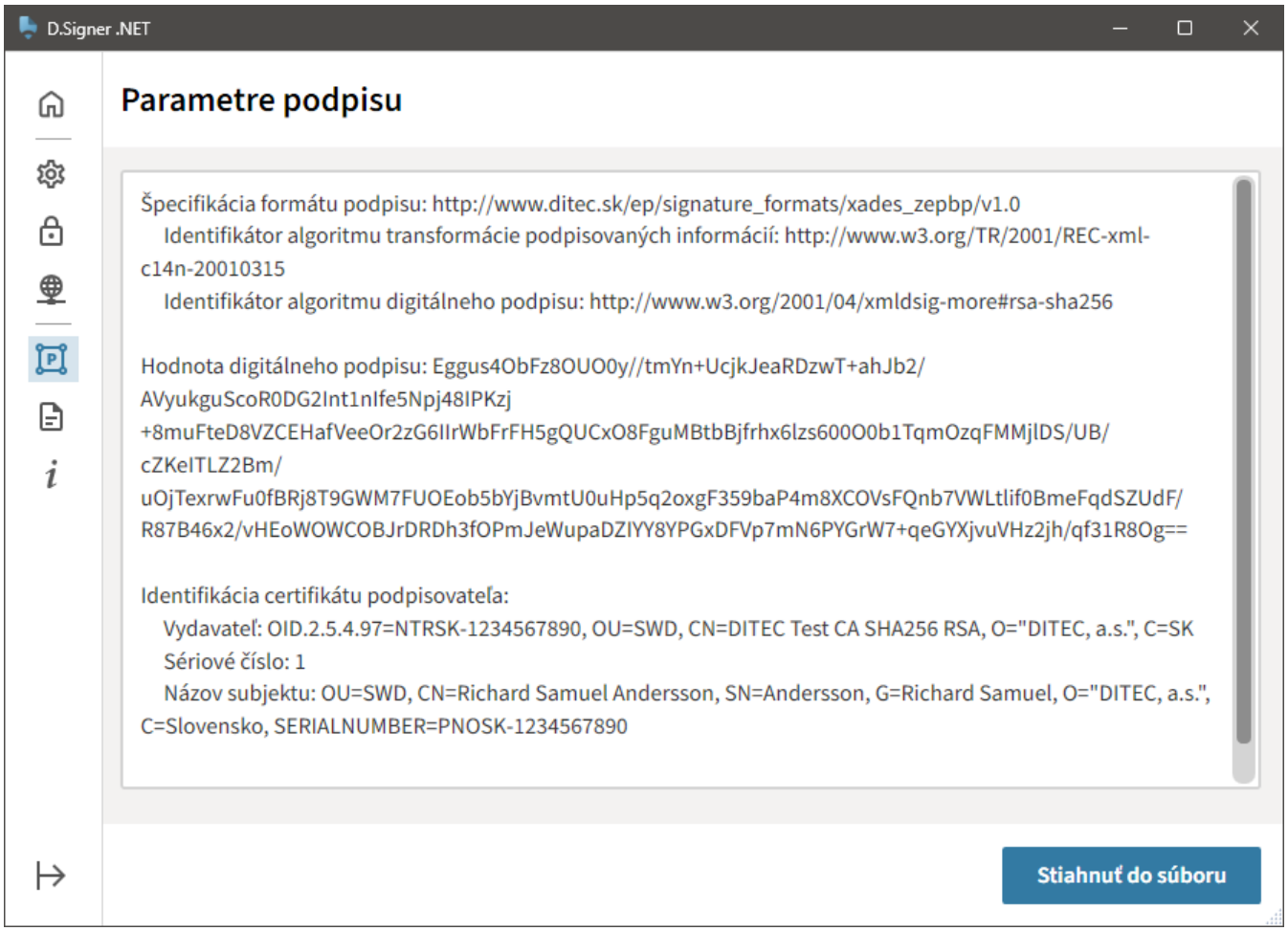
Odporúčame ponechať štandardné nastavenie – Automatická detekcia a len v prípade potreby neštandardnej konfigurácie prístupu k sieti internet sa obrátiť na administrátora vašej lokálnej siete, ktorý vám detaily nastavenia prístupu na internet cez proxy server poskytne.

6.4. Parametre podpisu

Obrazovka „Parametre podpisu“ obsahuje podrobnejšie údaje o podpise.



Väčšina údajov je dostupná až po podpísaní dokumentu.



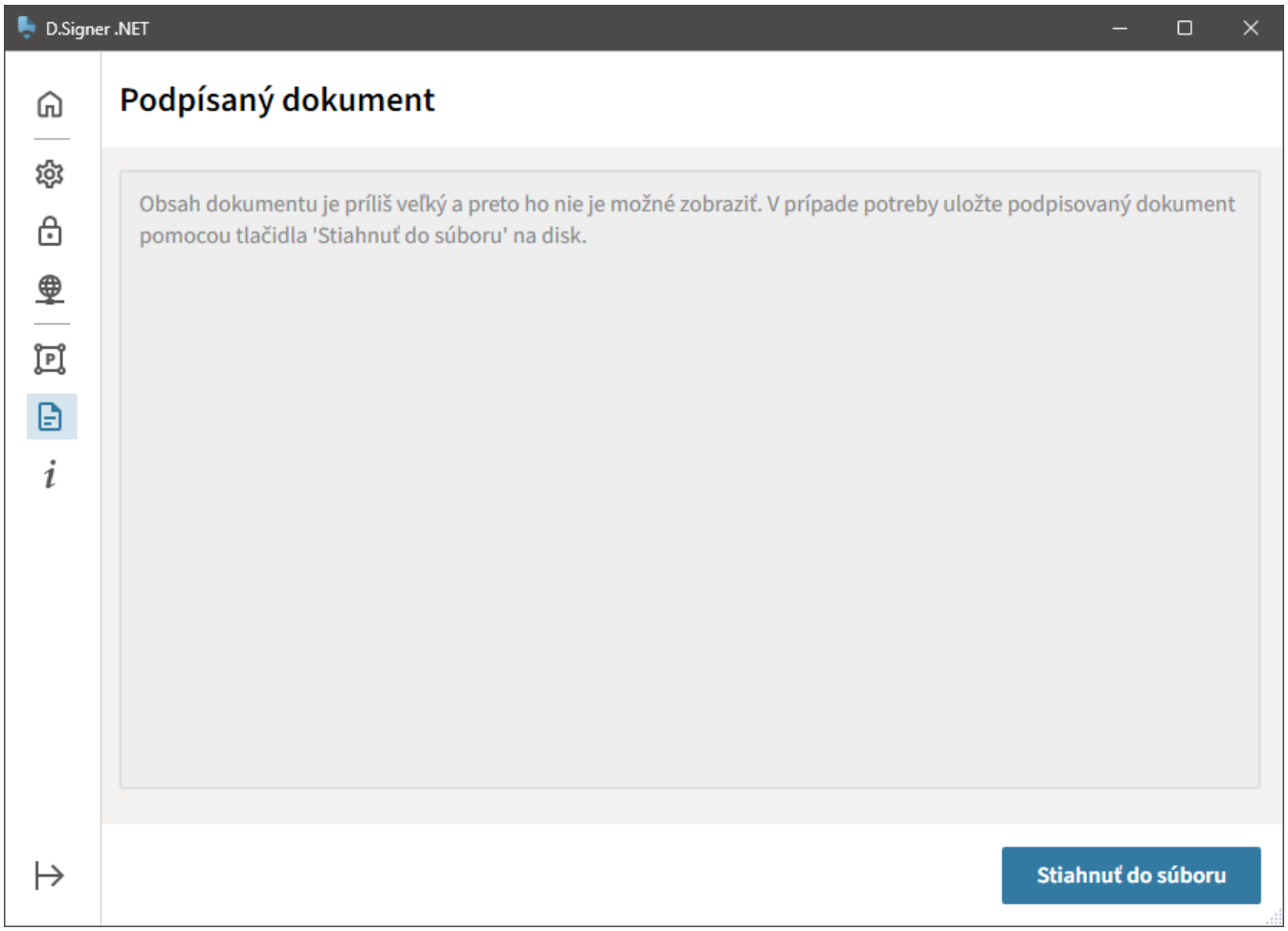
Túto zostavu parametrov si používateľ môže uložiť do textového súboru kliknutím na tlačidlo „Stiahnuť do súboru“.

6.5. Podpísaný dokument / Podpísané XML

Názov obrazovky sa mení na základe formátu podpisu.

Názov obrazovky	Formát podpisu
Podpísaný dokument	XAdES_ZEPbp v1.0
Podpísané XML	XAdES_ZEP v1.0 XAdES_ZEP v1.1 XAdES_ZEP v2.0

Obrazovka je prístupná až po vytvorení podpísaných dokumentov.



Ak je podpísaný dokument malej veľkosti, v okne sa zobrazí kódovaná reprezentácia dokumentu vo formáte base64 alebo XML.

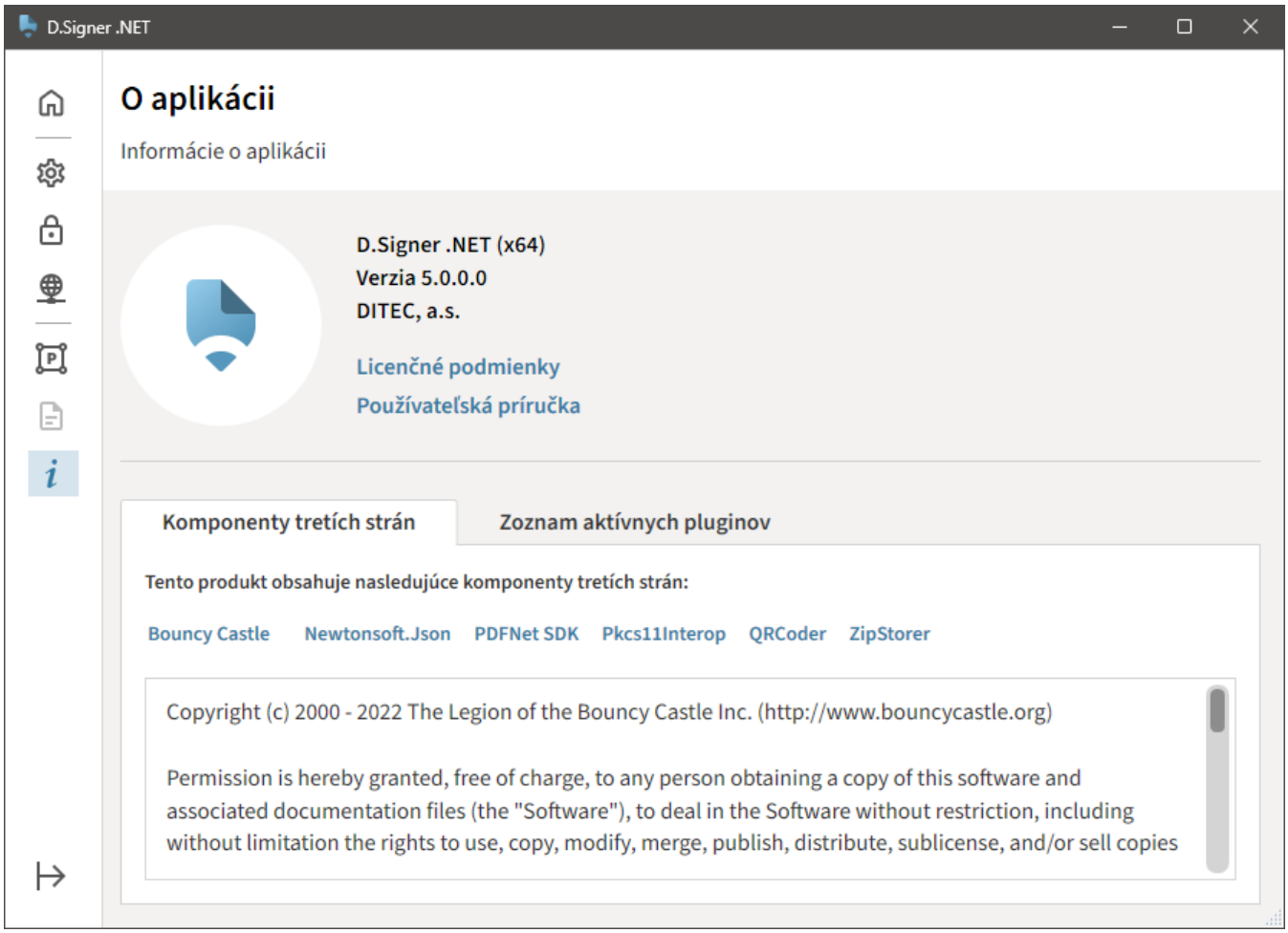
V opačnom prípade je uvedená informácia o možnosti si podpísaný dokument stiahnuť.

Stiahnuť dokument je možné kliknutím na tlačidlo „Stiahnuť do súboru“.

6.6. O aplikácii

Obrazovka zobrazuje informácie:

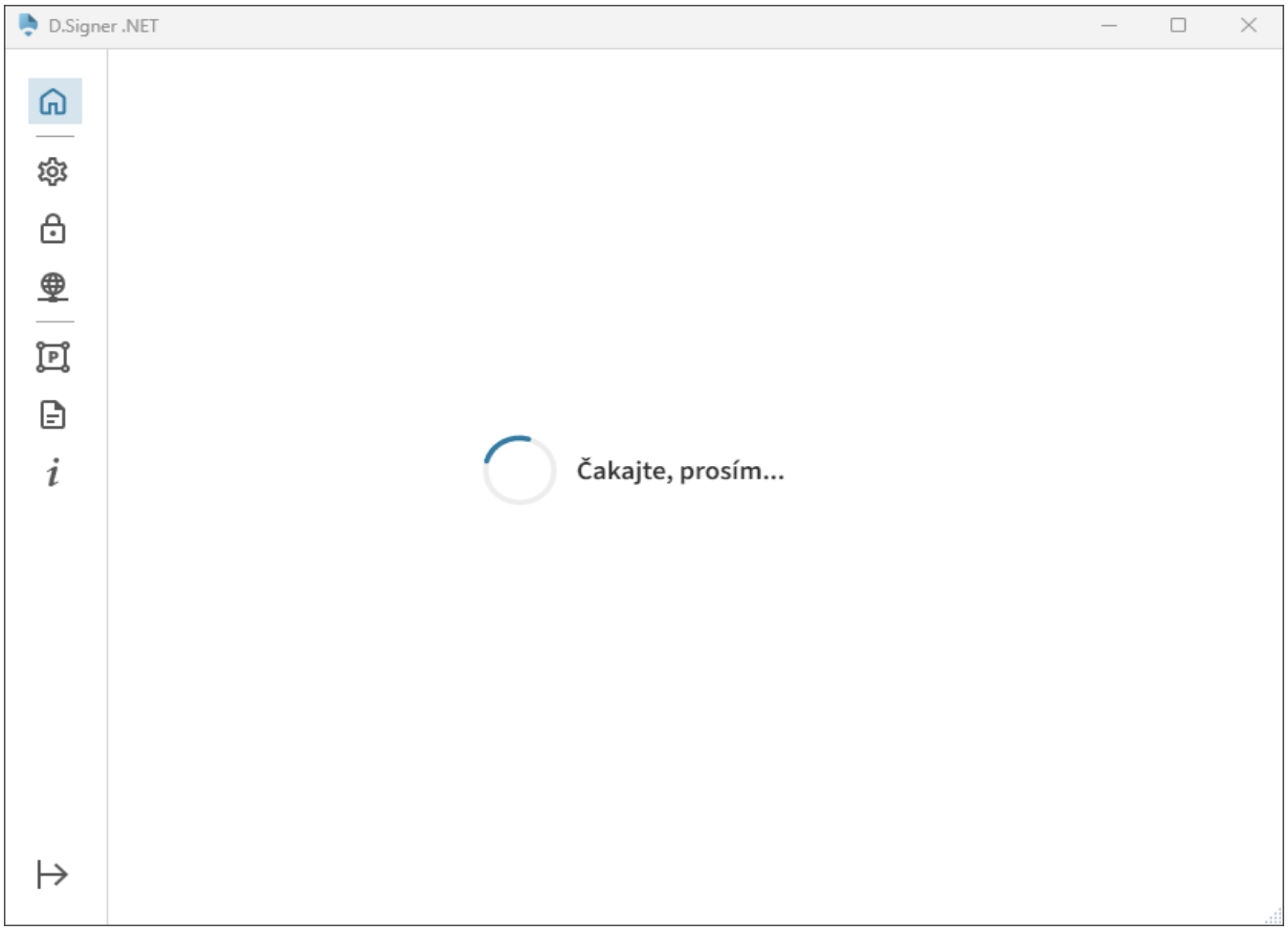
- Aplikačné – názov, verzia, názov autorskej spoločnosti
- Odkaz na znenie licenčných podmienok
- Odkaz na používateľskú príručku
- Licenčné klauzuly komponentov tretích strán
- Zoznam aktívnych pluginov


D.Signer .NET
O aplikácii
Informácie o aplikácii
D.Signer .NET (x64)
Verzia 5.0.0.0
DITEC, a.s.
Licenčné podmienky
Používateľská príručka
Komponenty tretích strán
Zoznam aktívnych pluginov
Tento produkt obsahuje nasledujúce komponenty tretích strán:
Bouncy Castle
Newtonsoft.Json
PDFNet SDK
Pkcs11Interop
QRCoder
ZipStorer
Copyright (c) 2000 - 2022 The Legion of the Bouncy Castle Inc. (http://www.bouncycastle.org)
Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies

7. Vytvorenie ZEP/KEP používateľom

7.1. Načítanie vstupných parametrov

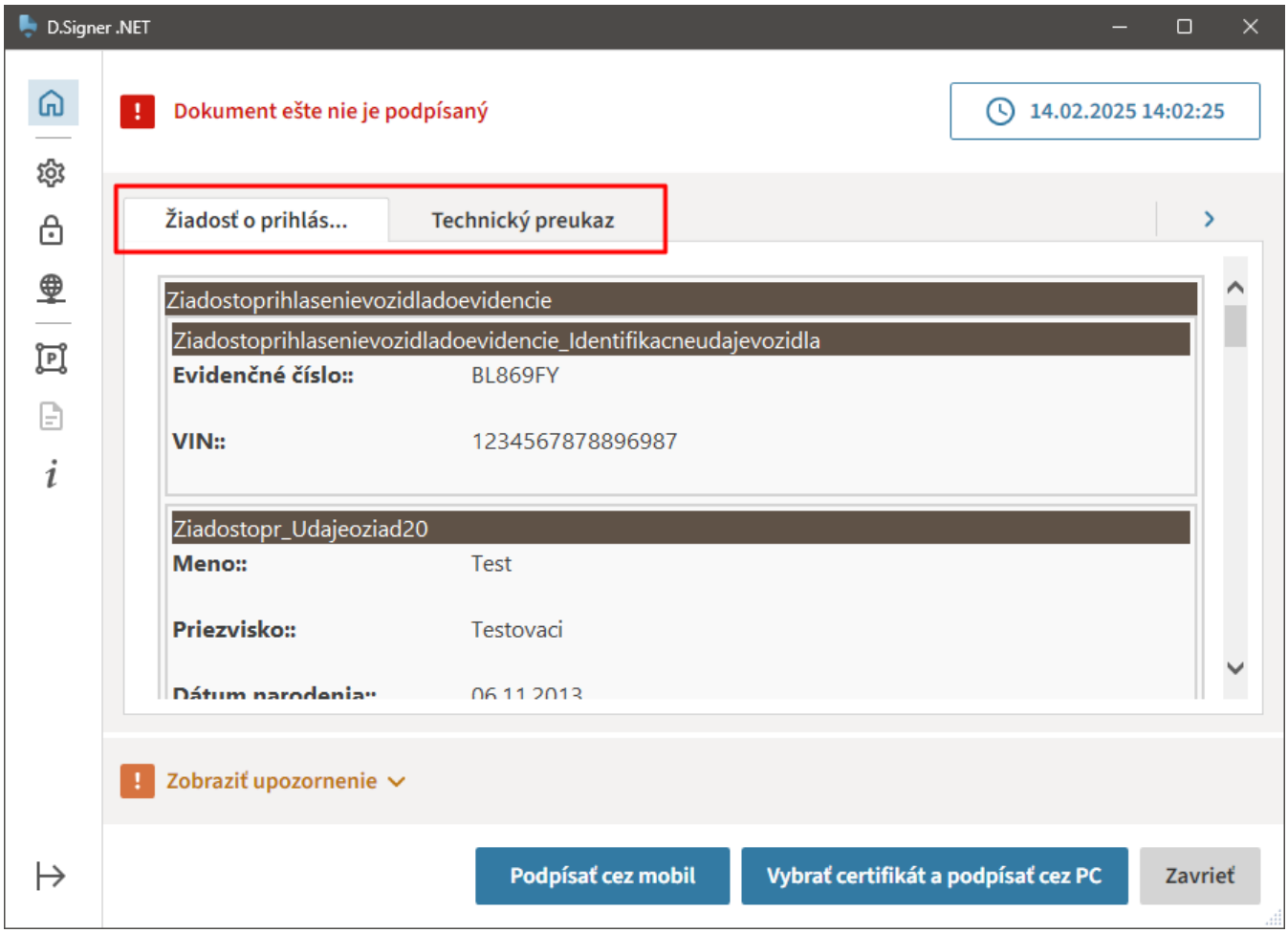
Po zavolaní funkcie pre vytvorenie elektronického podpisu, aplikácia D.Signer .NET vykoná validáciu vstupných parametrov (teda jednotlivých podpisovaných častí *multipart* dokumentu) a zobrazí hlavné dialógové okno aplikácie. Spracovanie vstupných parametrov, najmä rozsiahlych dokumentov, môže vyžadovať istý čas, počas ktorého je zobrazený tzv. *splash screen*.



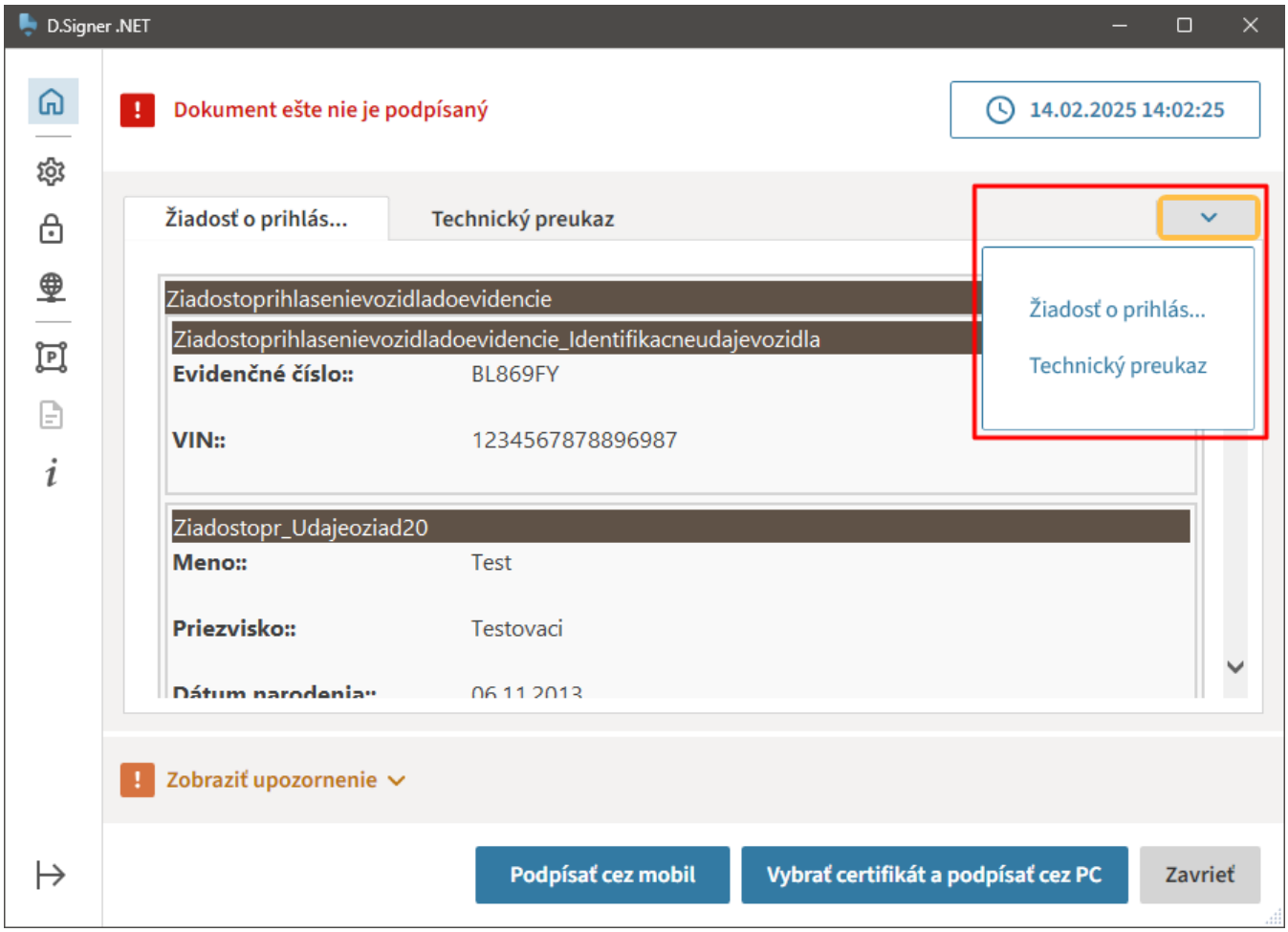
7.2. Zobrazenie podpisovaných dát

Pokiaľ všetky kontroly vstupných parametrov prebehli úspešne, na jednotlivých záložkách hlavného okna sú zobrazené časti podpisovaného *multipart* dokumentu. Používateľ má možnosť prezrieť všetky podpisované dátové objekty a ďalšie parametre podpisu.

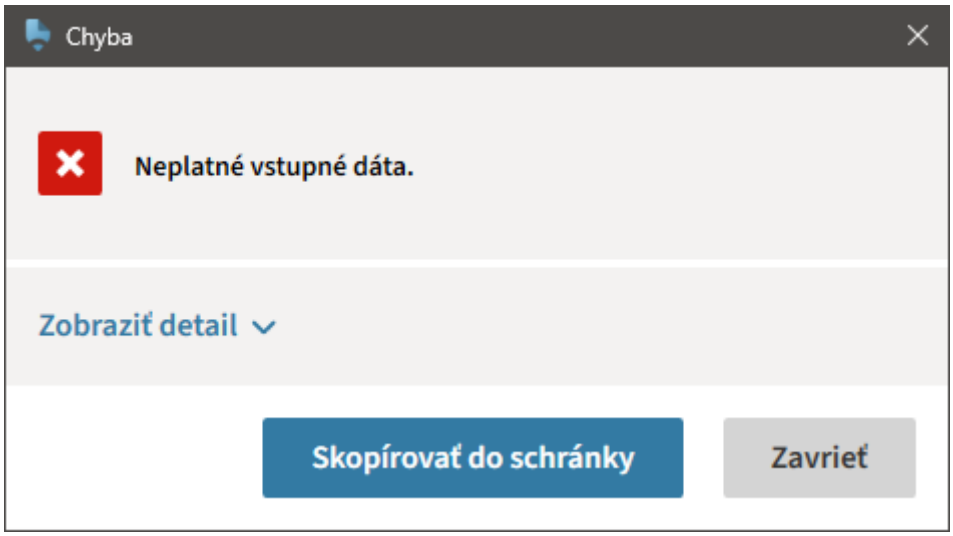
Pozor! Do vášho podpisu, autorizácie, budú zahrnuté všetky zobrazované dátové objekty, dokumenty, a parametre elektronického podpisu. Vzhľadom k tomu, že vytvorením autorizácie vyjadrujete svoj súhlas s obsahom jednotlivých dokumentov, je vo vašom záujme, aby ste sa dôkladne oboznámili s obsahom všetkých zobrazených dátových objektov.



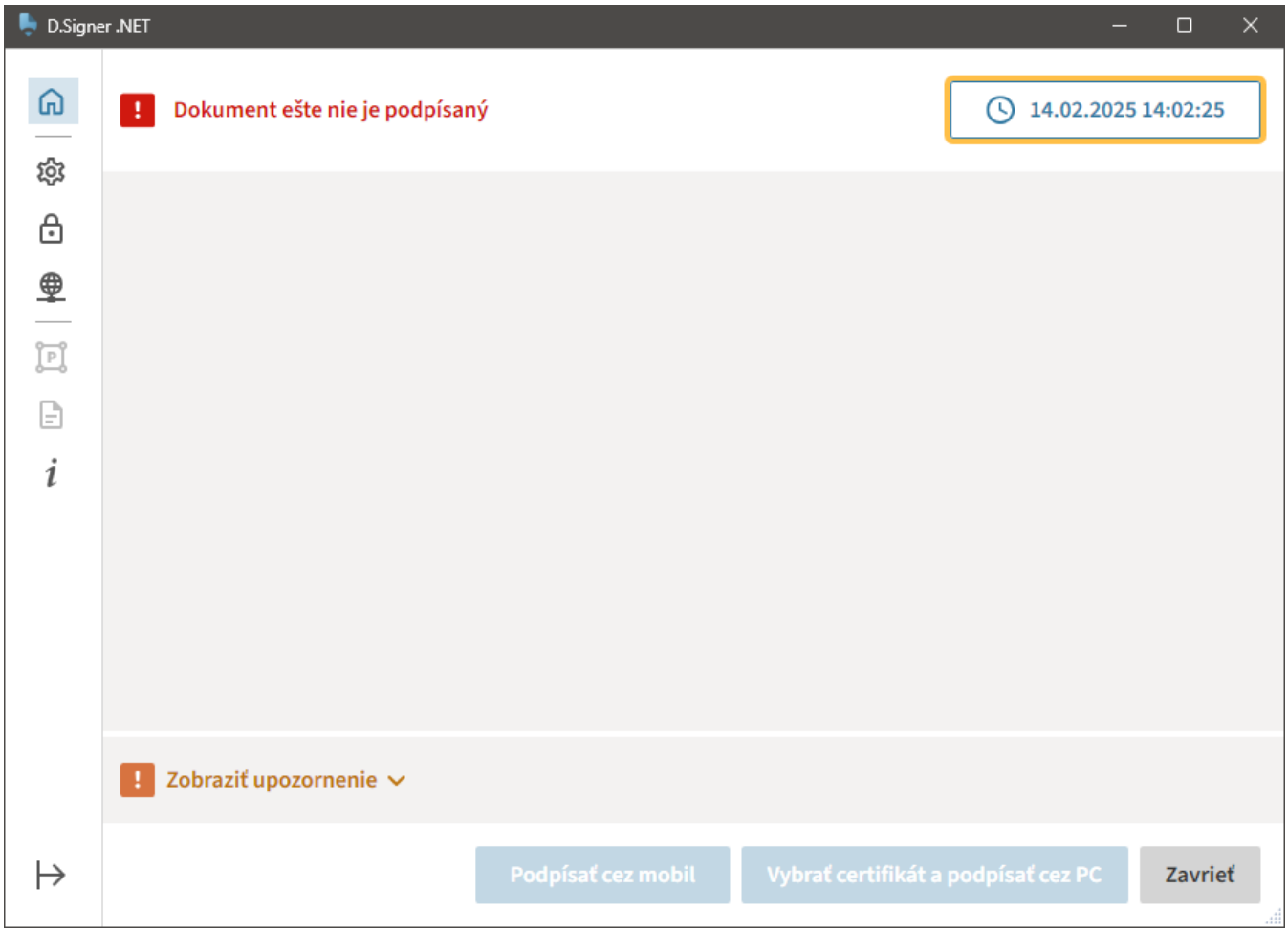
Ak je počet podpisovaných dátových objektov vyšší, zobrazí sa ikonka šípky na pravej strane riadku so záložkami. Kliknutím na túto ikonku sa zobrazí zoznam podpisovaných dátových objektov.



Pokiaľ sa vyskytli pri kontrole vstupných parametrov chyby, aplikácia D.Signer .NET zobrazí chybovú správu.



V takomto prípade sa tiež zobrazí hlavná obrazovka aplikácie D.Signer .NET, ale nebude možné uskutočniť vytvorenie podpisu (tlačidlá pre vytvorenie podpisu nebudú neprístupné).

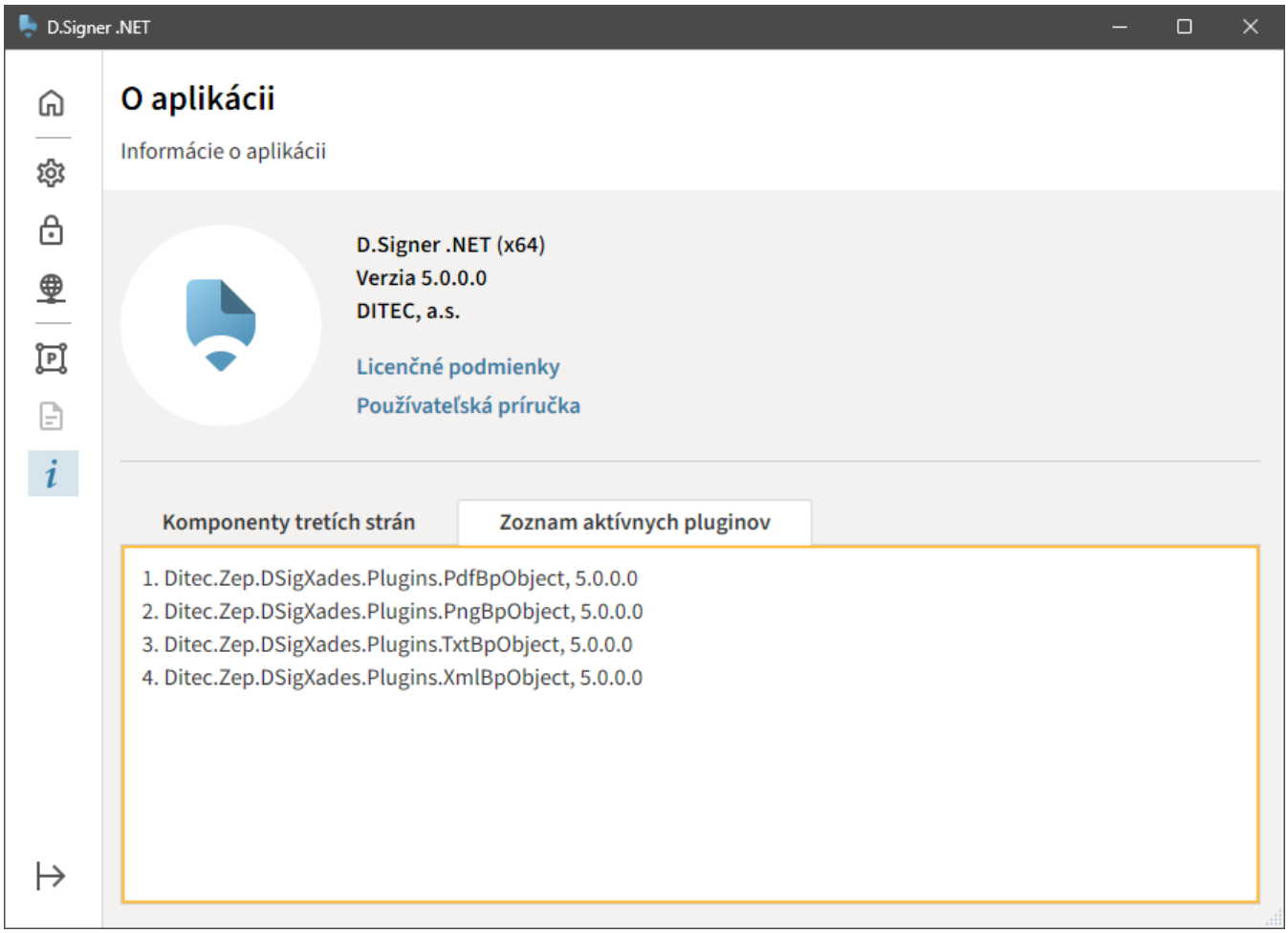


V rámci hlavného okna aplikácie D.Signer .NET je tiež zobrazený stav podpisovaného dokumentu, ktorý môže nadobúdať nasledujúce hodnoty:

- Dokument ešte nie je podpísaný.
- Dokument je pripravený na podpísanie.
- Umiestnite oblasť pre vizualizáciu podpis. Dokument je pripravený na podpísanie.
- Dokument bol úspešne podpísaný.

V závislosti od stavu dokumentu sú jednotlivé tlačidlá hlavného okna aplikácie D.Signer .NET prístupné alebo neprístupné.

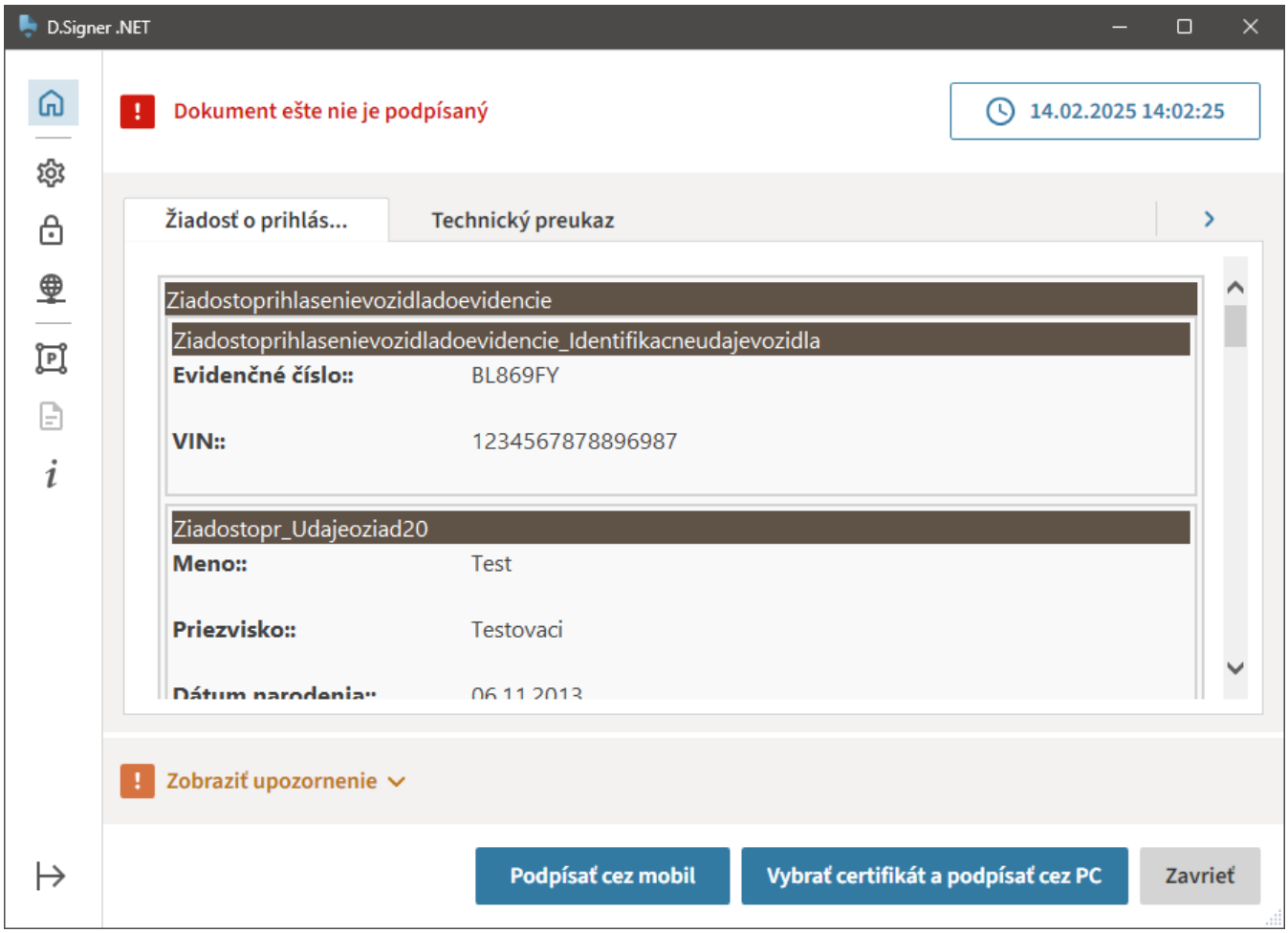
Aplikácia D.Signer .NET slúži na vytváranie elektronického podpisu nad množinou rôznych formátov dokumentov, resp. typov dát (XML dokumenty, PDF dokumenty atď.), prípadne nad ľubovoľnou kombináciou podporovaných formátov dát, ktoré spolu vytvárajú tzv. *multipart* dokument. Pre jednotlivé formáty dokumentov sa inicializujú príslušné plugin moduly aplikácie D.Signer .NET. Informácia o inicializovaných plugin moduloch je prístupná prostredníctvom tlačidla "O aplikácii" (posledná ikona v ľavom stĺpci okna aplikácie D.Signer .NET), pod záložkou „Zoznam aktívnych pluginov“. Počet a typ inicializovaných plugin modulov je závislí od vstupných dátových objektov. Všetky plugin moduly nemusia byť vždy inicializované.



7.2.1. Zobrazenie dokumentov

Zobrazenie dokumentov je realizované v rámci aplikácie D.Signer .NET pomocou príslušného pluginu pre daný typ dát, ktorý poskytuje aplikácii D.Signer .NET funkcie pre vizualizáciu dát daného typu. Jednotlivé podpisované dátové objekty (resp. dokumenty) sú zobrazené na samostatných záložkách, ktorých názov bližšie určuje obsah príslušného dokumentu. Používateľ má takto možnosť pred vytvorením elektronického podpisu prezrieť obsah všetkých podpisovaných dokumentov.

Na nasledujúcom obrázku je príklad zobrazenia XML dokumentu v rámci aplikácie D.Signer .NET.



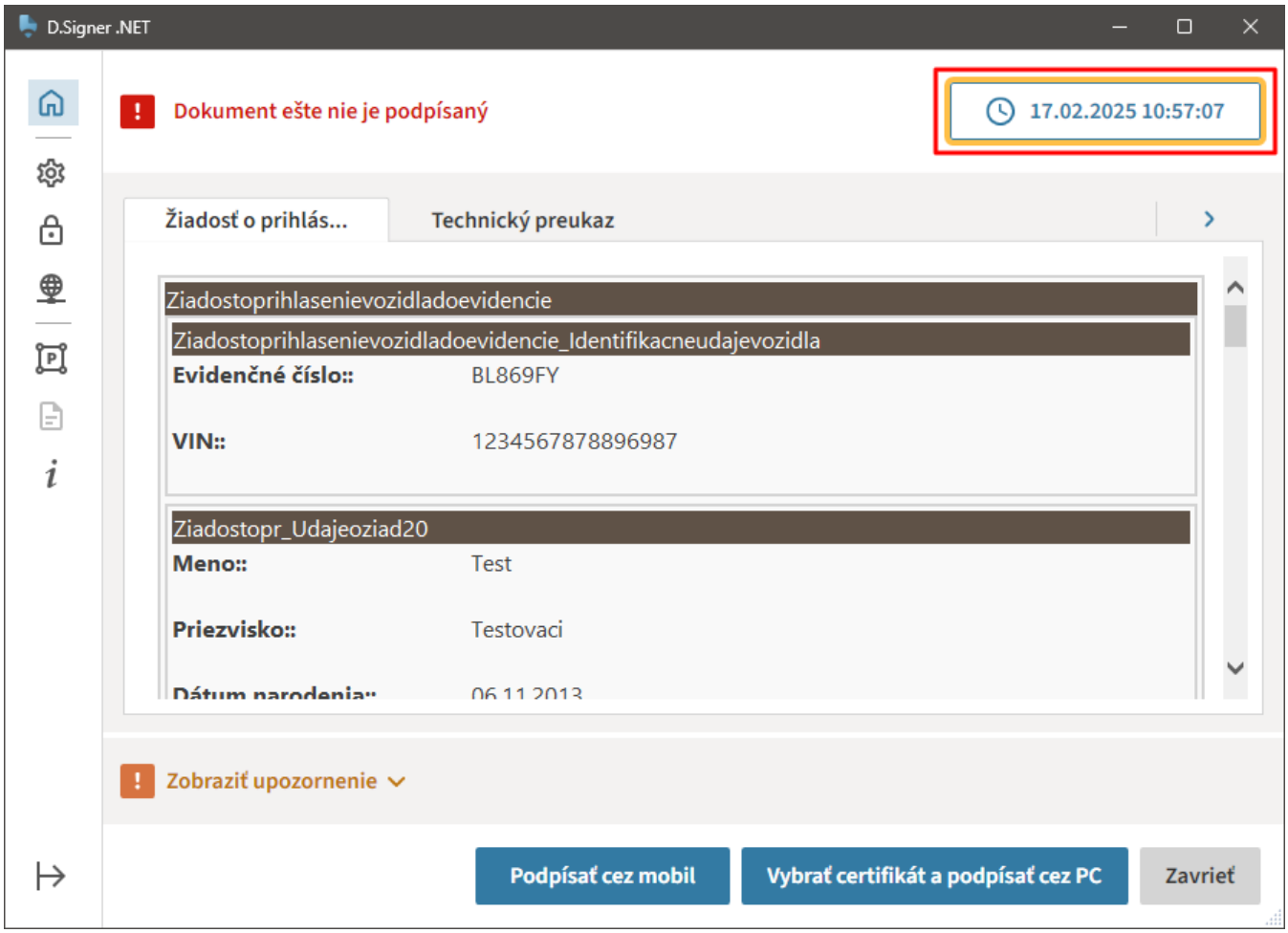
7.3. Nastavenie dátumu a času vytvorenia podpisu

Aplikácia D.Signer .NET umožňuje používateľovi v prípade potreby nastaviť pomocou ovládacích prvkov, ktoré sú prístupné kliknutím na čas v pravom hornom rohu okna aplikácie, dátum a čas vytvorenia podpisu. Používateľ môže takto deklarovať vytvorenie elektronického podpisu v špecifikovanom dátume a čase, pričom tento deklarovaný dátum a čas vytvorenia podpisu je zahrnutý do podpisovaných atribútov vytváraného elektronického podpisu a následne vyhodnocovaný na strane overovateľa. Je teda potrebné, aby používateľ pri vytváraní elektronického podpisu nastavil taký dátum a čas vytvorenia podpisu, ktorý neznemožní spracovanie vytvoreného elektronického podpisu na strane overovateľa.

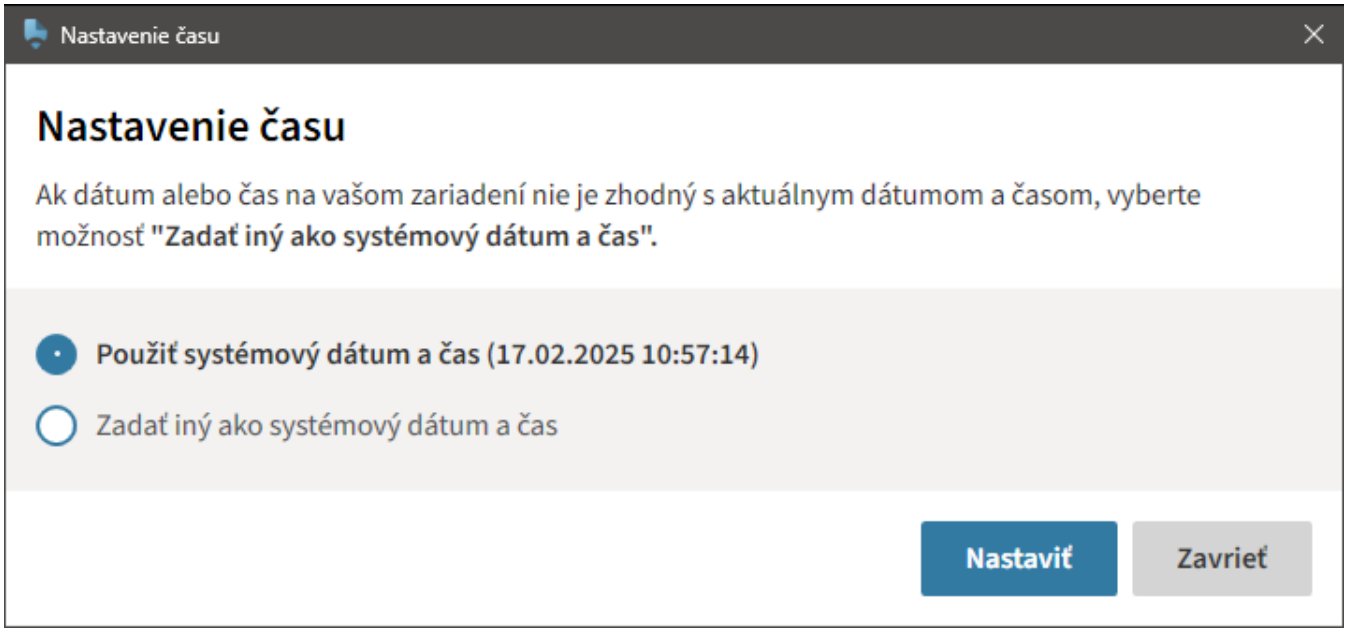
V prípade kvalifikovaných elektronických podpisov sa deklarovaný dátum a čas podpisu obvykle neberie do úvahy, resp. rozhodujúca je kvalifikovaná časová pečiatka pripojená k podpisu.

Aplikácia umožňuje používateľovi deklarovať ako čas vytvorenia podpisu:

- systémový dátum a čas,
- alebo manuálne nastaviť deklarovaný dátum a čas vytvorenia podpisu.



V prvom prípade nie je možné manuálne nastaviť deklarovaný dátum a čas vytvorenia podpisu. Používateľ môže iba prostredníctvom príslušného tlačidla nastaviť systémový dátum a čas (ak má na to príslušné oprávnenia v rámci operačného systému Windows).

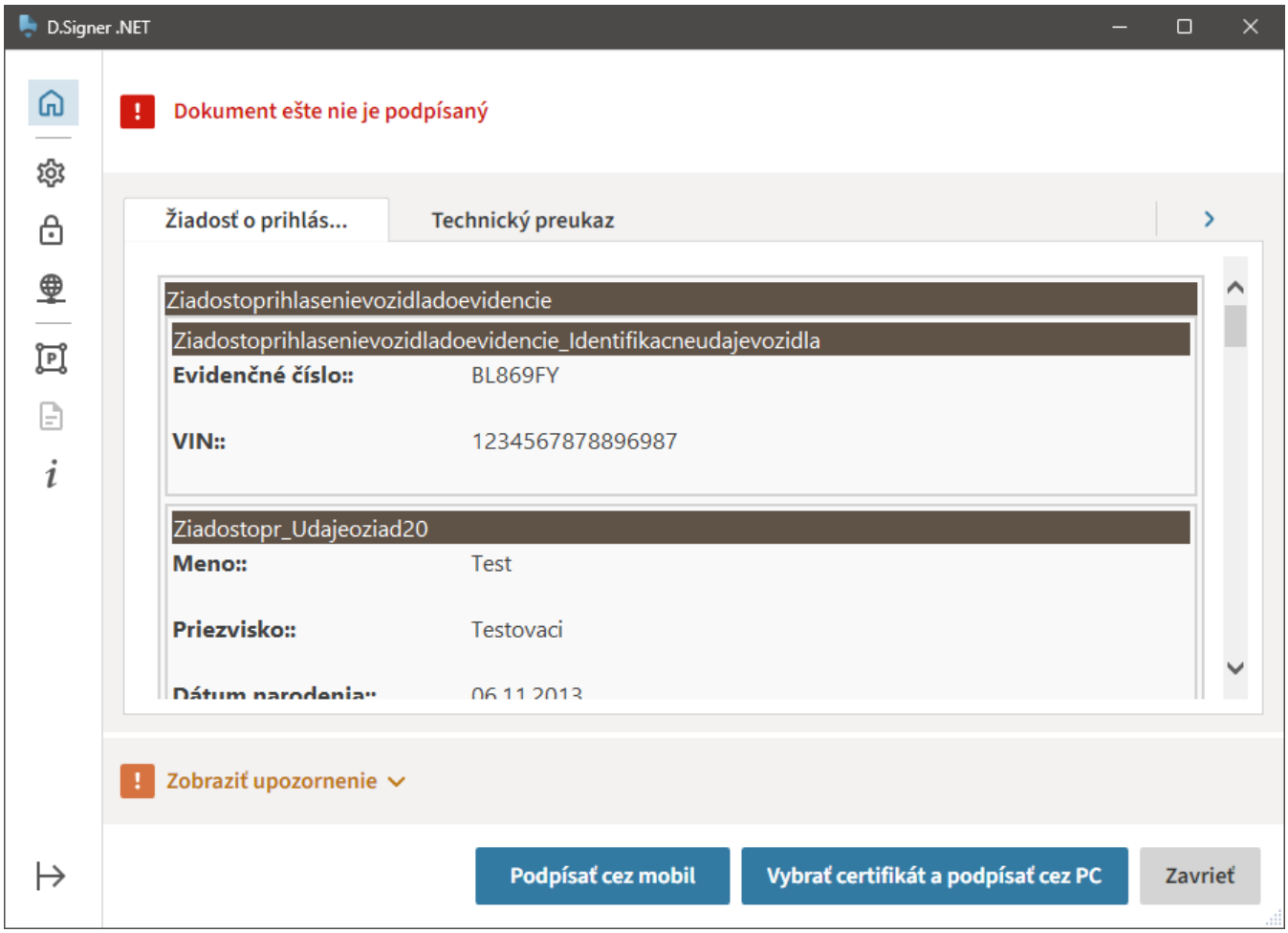


V druhom prípade sa používateľovi sprístupní deklarovaný dátum a čas vytvorenia podpisu na editovanie.



Pozor! Pri vytváraní elektronického podpisu odporúčame použiť správne nastavený systémový dátum a čas.

V prípade, že v rámci danej klientskej aplikácie nie je potrebné do parametrov podpisu zahrnúť aj používateľom deklarovaný dátum a čas vytvorenia podpisu, nemusia byť príslušné ovládacie prvky pre jeho nastavenie k dispozícii. Ich zobrazenie závisí na zavolaní príslušných funkcií aplikačného rozhrania aplikácie D.Signer .NET z klientskej aplikácie.

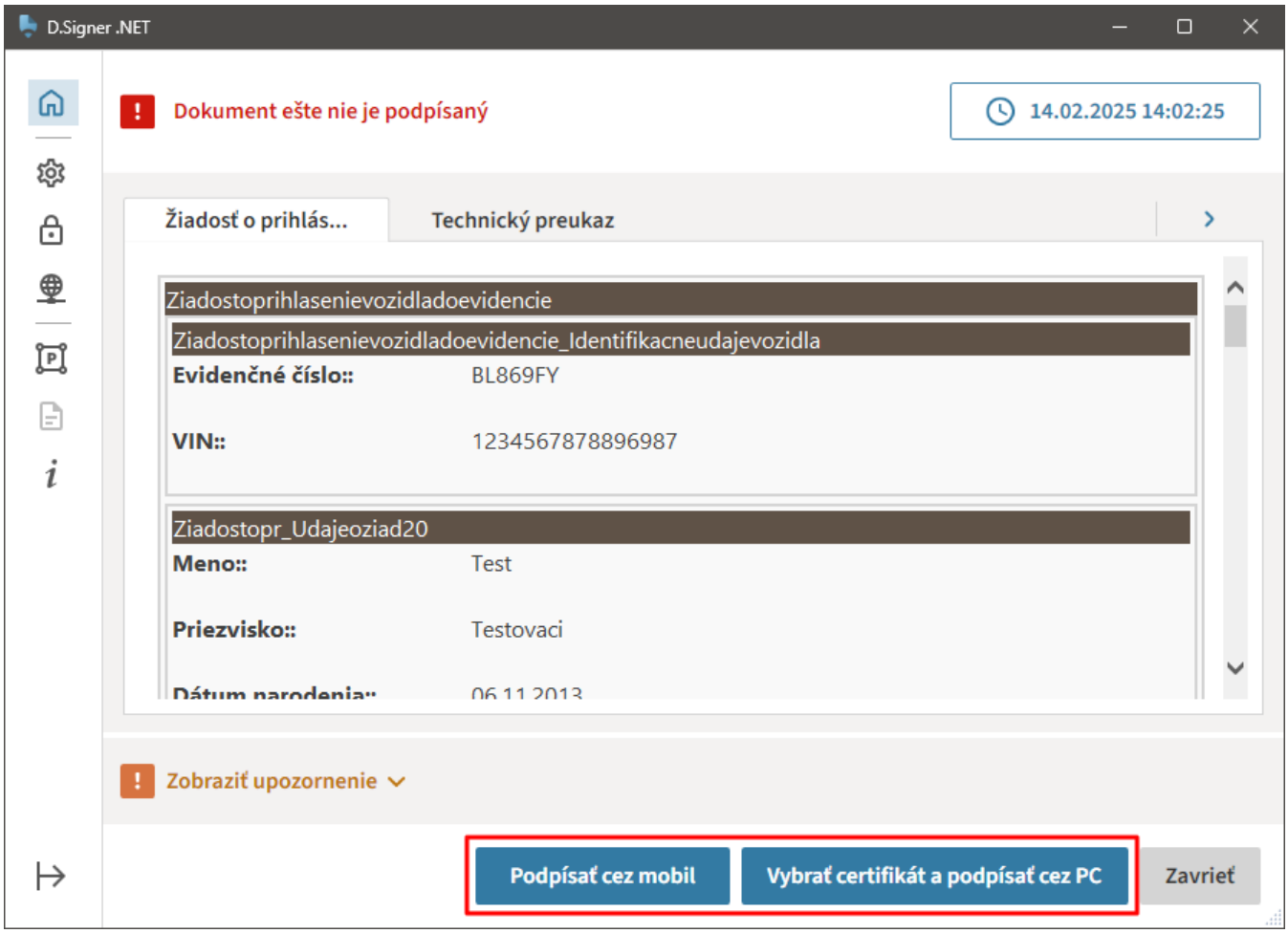


7.4. Podpísanie dokumentu

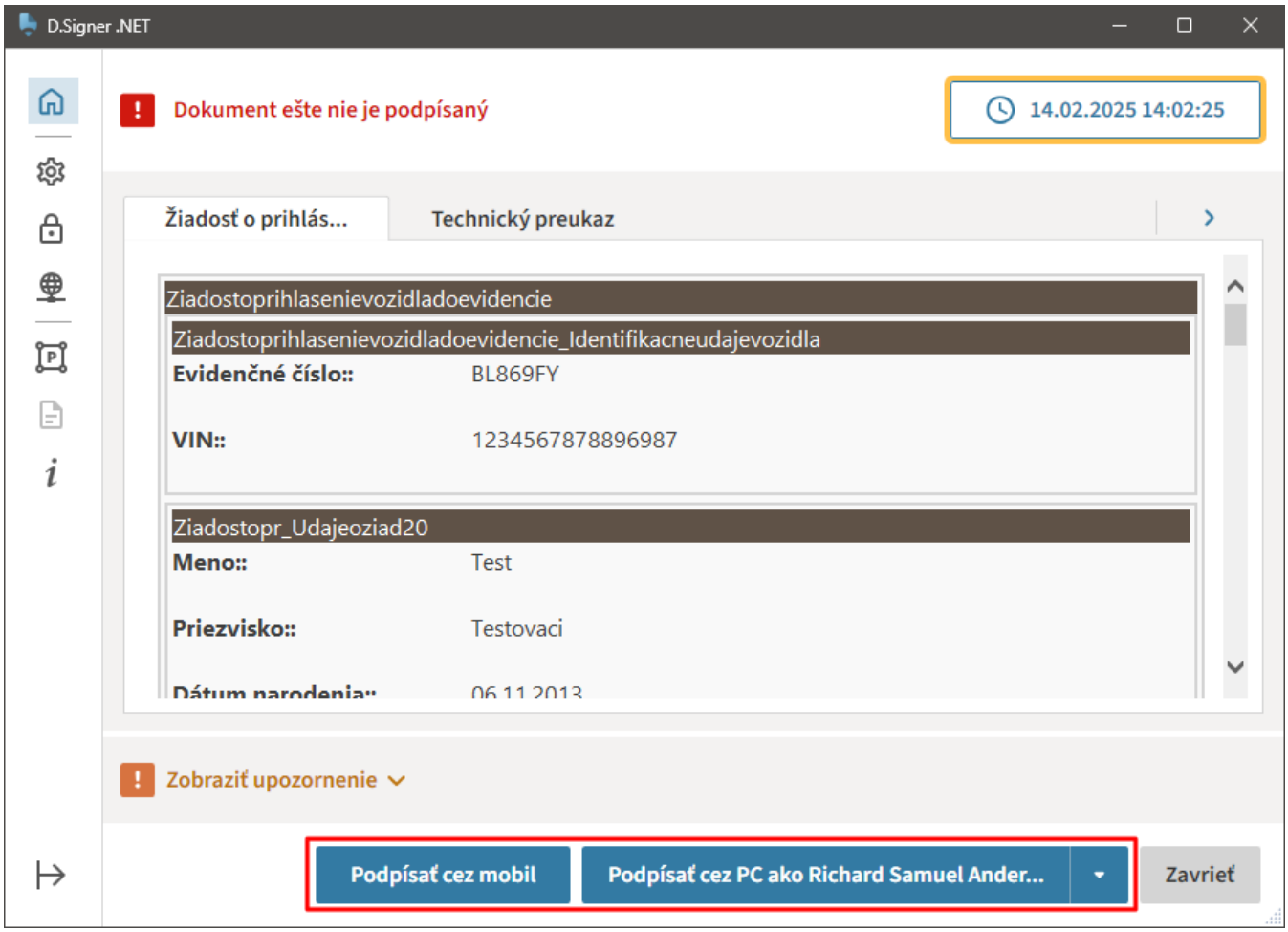
V prípade úspešného načítania podpisovaných dát sa sprístupnia tlačidlá, ktorými používateľ môže aktivovať vytvorenie elektronického podpisu dokumentu, a to rozdielnymi procesmi:

- pomocou mobilného zariadenia – tlačidlo „Podpísať cez mobil“,
- výberom certifikátu v používanom zariadení – tlačidlo „Vybrať certifikát a podpísať cez PC“ (prípadne zvolením zapamätaného certifikátu).

Upozornenie: Integrátor aplikácie môže podpisovanie pomocou mobilného zariadenia deaktivovať, v takom prípade tlačidlo „Podpísať cez mobil“ nebude zobrazené.



Aplikácia v procese vytvárania elektronického podpisu umožňuje zapamätanie podpisového certifikátu. Posledný zapamätaný certifikát je následne ponúknutý ako rýchla voľba pre vytvorenie elektronického podpisu.



7.4.1. Mobilné zariadenie

Pre úspešné vytvorenie elektronického podpisu pomocou mobilného zariadenia ako čítačky eID kariet cez NFC rozhranie je potrebné mať:

- občiansky preukaz s NFC čipom vydaný po 1.12.2022,
- v mobilnom zariadení nainštalovanú aplikáciu „Disig Web Signer Mobile“, s povoleným prístupom ku kamere (potrebné pre skenovanie QR kódu),
- v mobilnom zariadení zapnuté komunikačné NFC rozhranie.

V tomto prípade teda nie je potrebné mať k PC pripojenú fyzickú čítačku čipových kariet a ani na PC nainštalovanú aplikáciu eID klient.

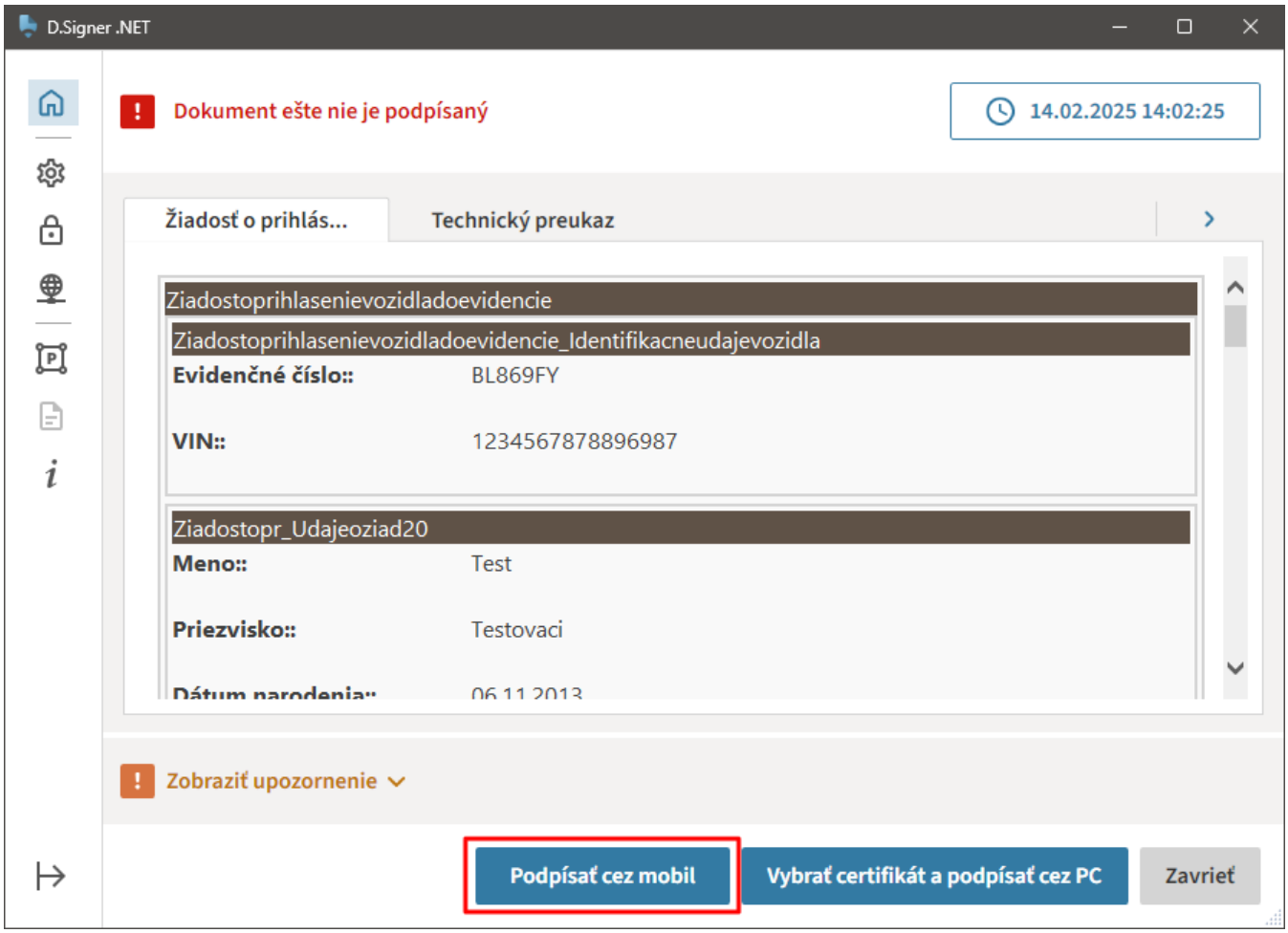
Pre ilustráciu uvádzame vzor občianskeho preukazu s NFC čipom vydaného po 1.12.2022 s vyznačeným symbolom identifikujúcim NFC čip.



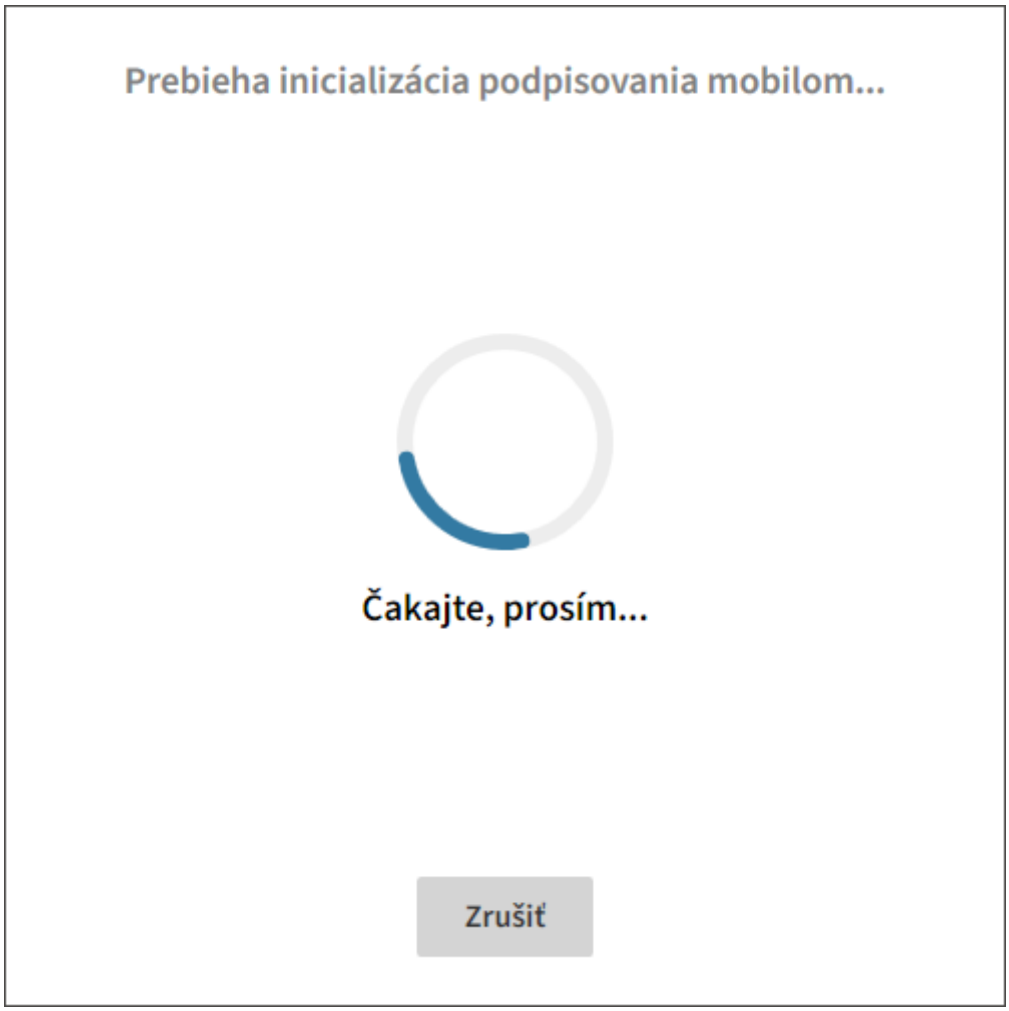
Ak používateľ v mobilnom zariadení nemá nainštalovanú aplikáciu „Disig Web Signer Mobile“, bude po naskenovaní QR kódu (napr. aplikáciou Skener alebo Fotoaparát) vyzvaný na jej inštaláciu. V procese podpisovania môže pokračovať až po jej úspešnej inštalácii.

Pri vytvorení elektronického podpisu pomocou mobilného zariadenia ako čítačky eID kariet cez NFC rozhranie sa vytvára spojenie medzi aplikáciou D.Signer .NET a mobilnou aplikáciou Disig Web Signer Mobile cez QR kód. Podpisované dokumenty, ktoré by mohli obsahovať citlivé údaje, sa však z používateľovho PC neposielajú na server QES Portal, ktorý zabezpečuje spojenie medzi aplikáciou D.Signer .NET a mobilnou aplikáciou Disig Web Signer Mobile, ani do samotnej mobilnej aplikácie – posielajú sa len meta informácie o názvoch podpisovaných dokumentov a ich digitálne odtlačky. S obsahom podpisovaných dokumentov je preto potrebné sa pred vytvorením KEP oboznámiť v rámci desktopovej aplikácie D.Signer .NET.

Vytvorenie elektronického podpisu pomocou mobilného zariadenia (mobil, tablet) prebieha nasledovným postupom. Proces podpisovania sa aktivuje kliknutím na tlačidlo „Podpísať cez mobil“.



Zobrazí sa modálne okno s informáciou o generovaní QR kódu.



Po inicializácii sa zobrazí samotný QR kód.



QR kód musí skenovať a pokračovať v podpisovaní používateľ aplikácie D.Signer .NET. QR kód nesmie zdieľať s inými používateľmi.

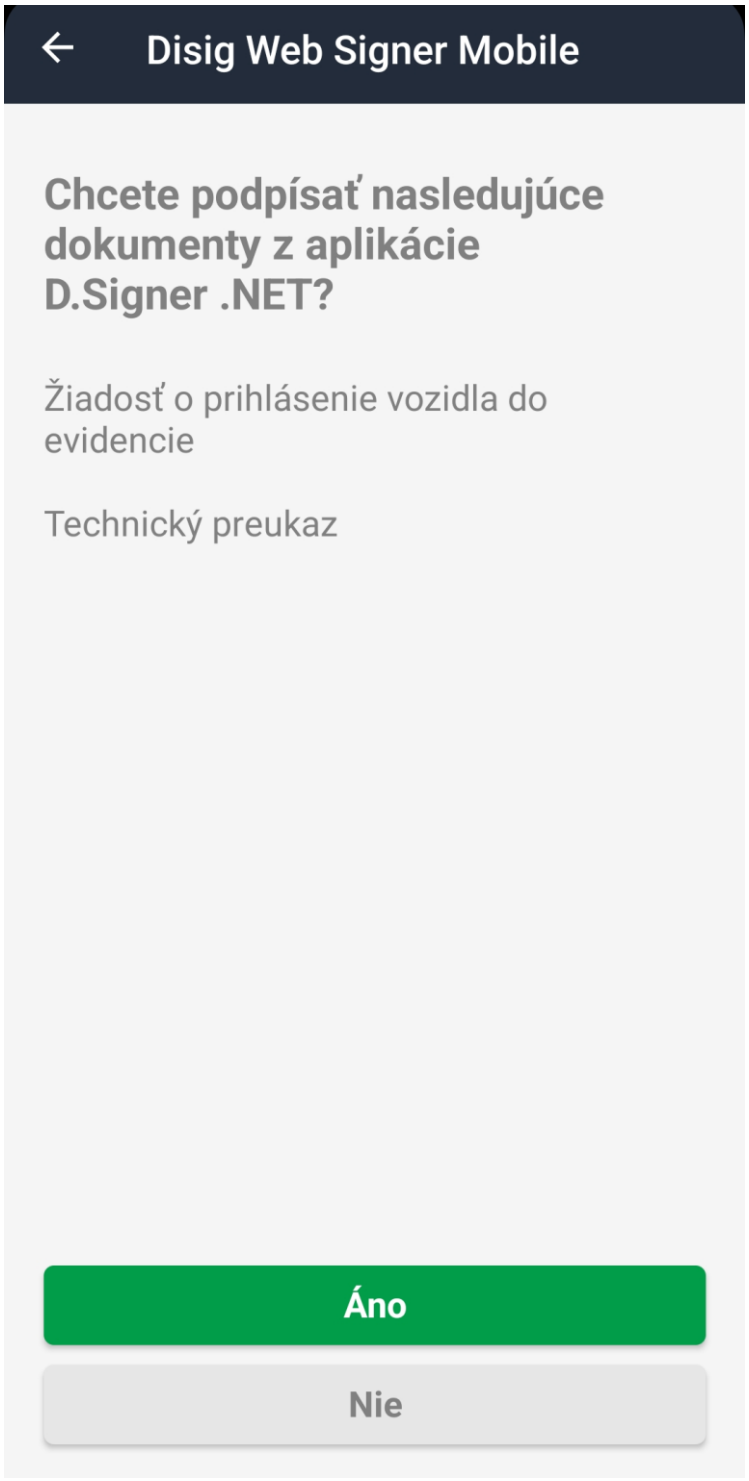
Používateľ má v mobilnom zariadení aktívny komunikačný NFC modul (ak modul nie je aktívny, v neskoršom procese bude na jeho aktiváciu vyzvaný). Spustí mobilnú aplikáciu „Disig Web Signer Mobile“. Ak mobilnú aplikáciu nemá nainštalovanú, načítaním QR kódu v inej aplikácii (napr. aplikáciou Skener alebo Fotoaparát) bude vyzvaný na jej inštaláciu. Pokračovať v procese podpisovania bude môcť až po jej úspešnej inštalácii.



Zvolí „Podpísať cez QR“ a naskenuje vygenerovaný QR kód.



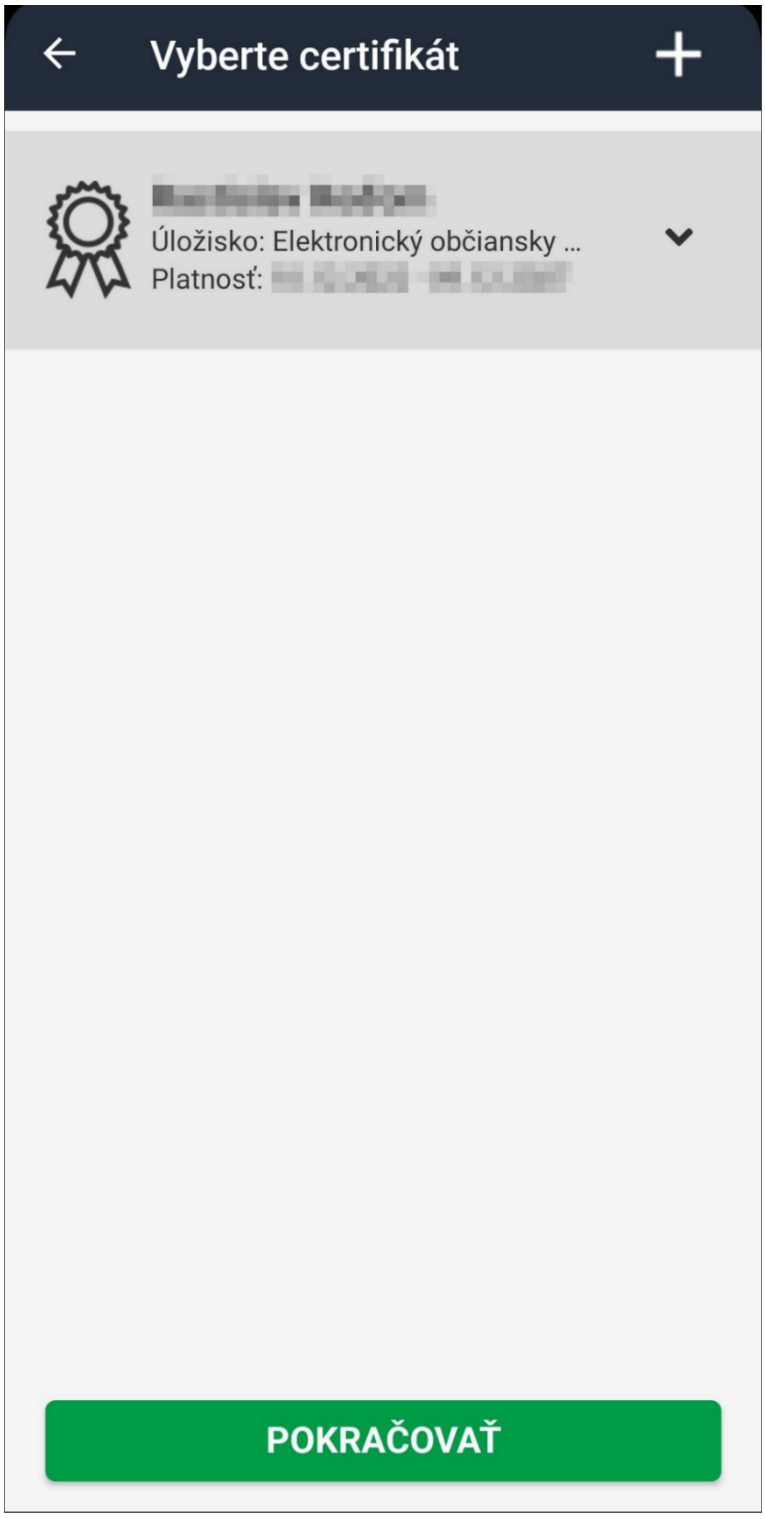
Po naskenovaní QR kódu sa zobrazí zoznam dokumentov na podpísanie s otázkou, či ich chce podpísať. Zvolí „Áno“.



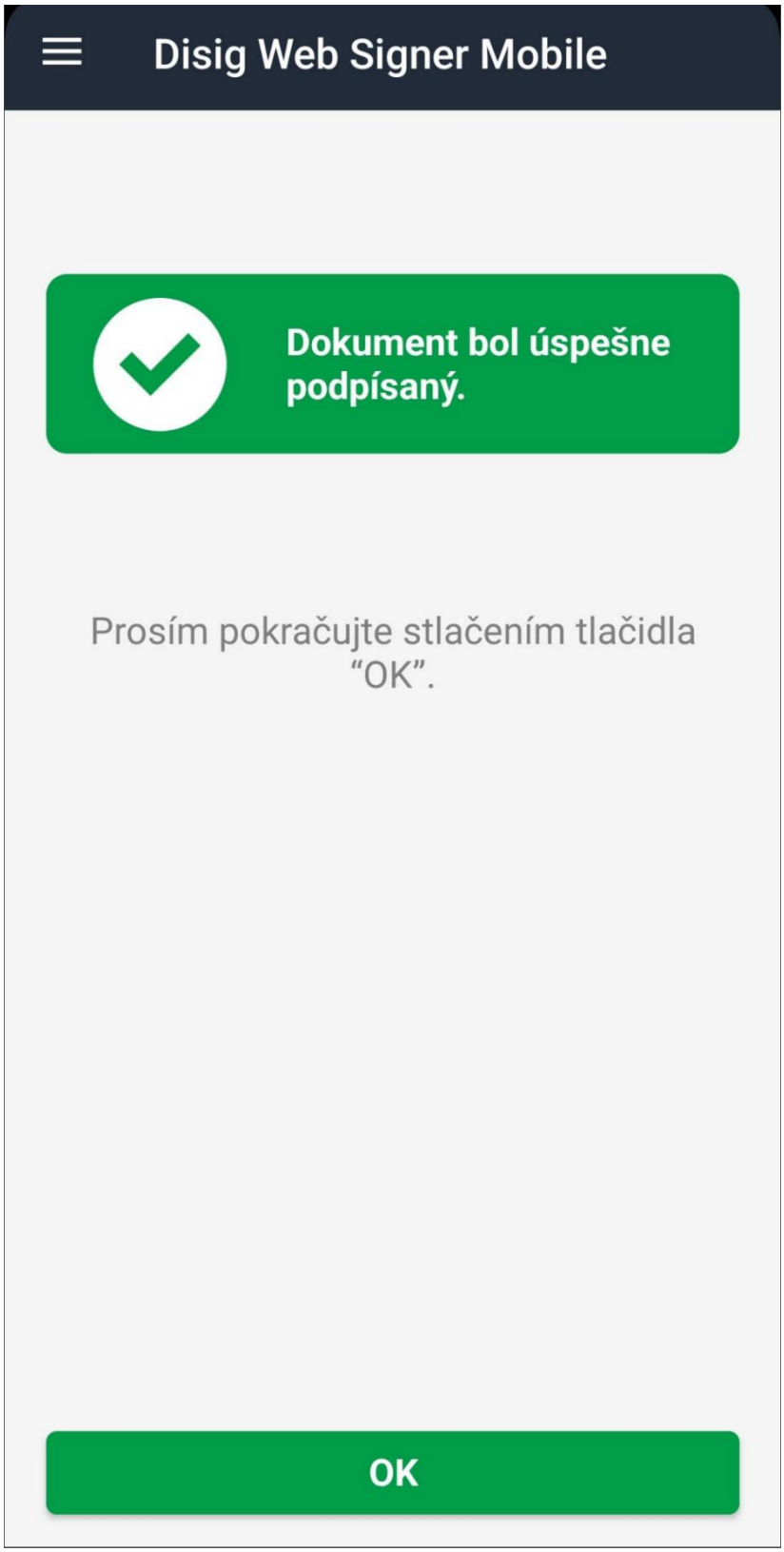
Následne bude vyzvaný na výber podpisového certifikátu.

Ak používateľ aplikáciou ešte nepodpisoval dokument, prejde procesom výberu certifikátu – je nutné mať pri sebe občiansky preukaz, ku ktorému priloží mobilné zariadenie. Predpokladom je mať aktívny NFC modul. Následne bude vyzvaný na zadanie BOK kódu. Po jeho úspešnom zadaní potvrdí súhlas s načítaným certifikátom. Zvolený certifikát si aplikácia uloží do zoznamu použitých certifikátov (neskôr ho zo zoznamu môže odstrániť).

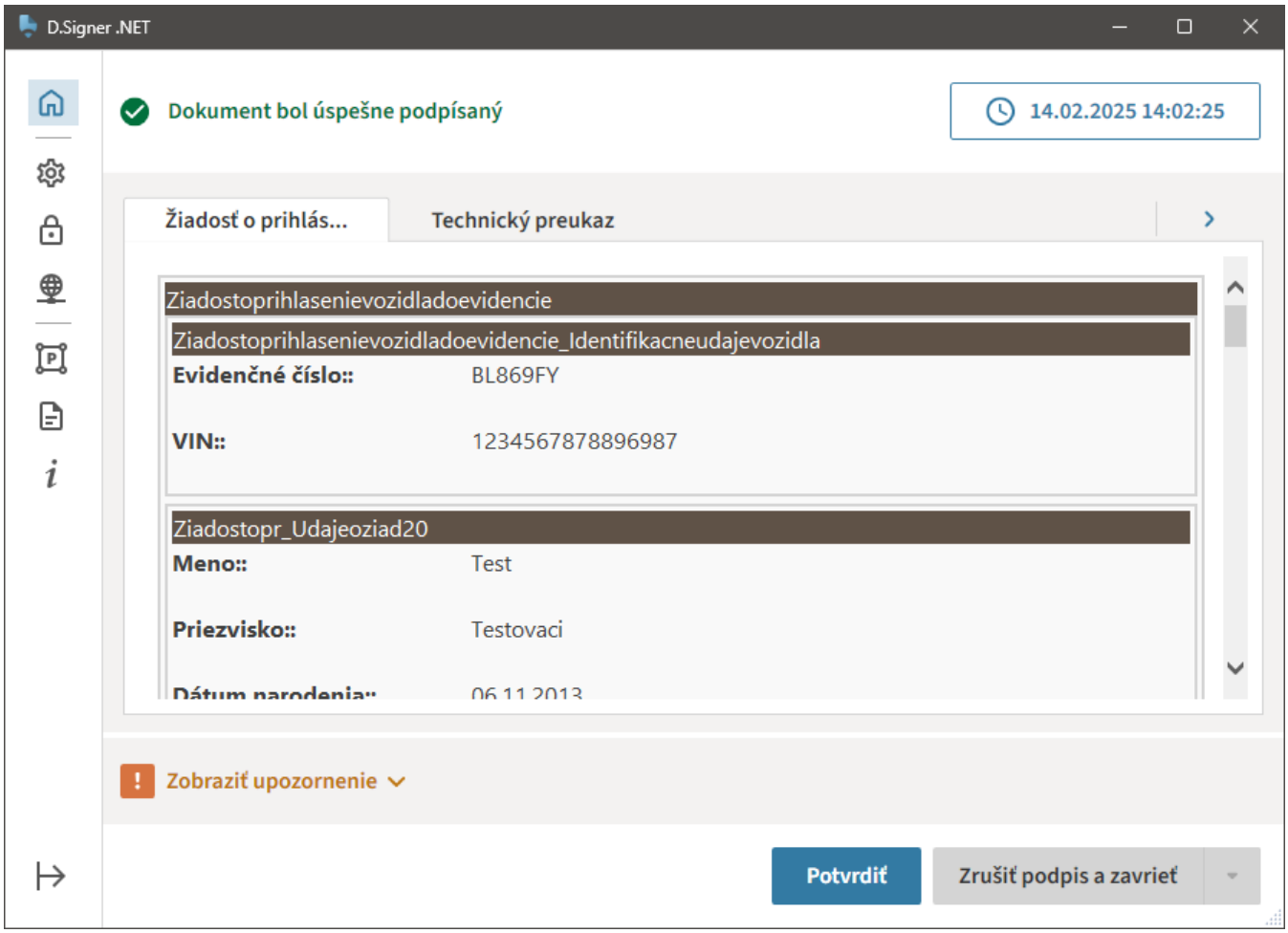
Ak má certifikát uložený v zozname, vyberie ho a zvolí „Pokračovať“.



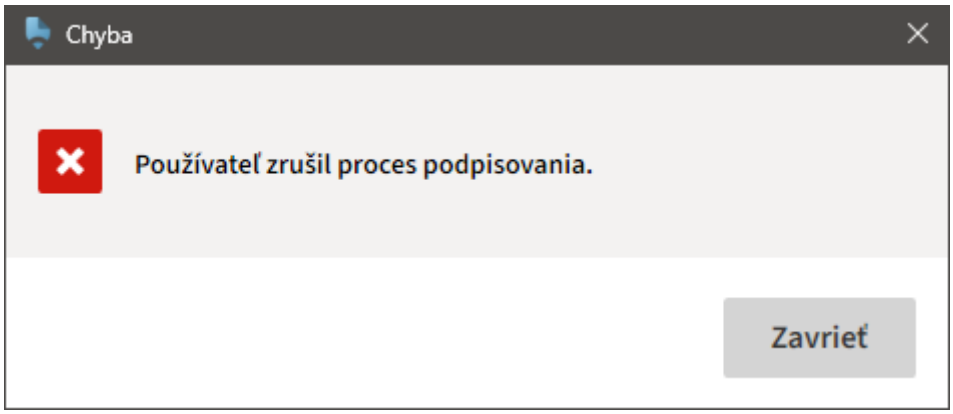
Bude vyzvaný na zadanie BOK kódu. Po úspešnom zadaní bude vyzvaný na zadanie podpisového PIN kódu. Po úspešnom zadaní príde k vytvoreniu podpisu dokumentov.



Úspešné dokončenie sa prejaví správou „Dokument bol úspešne podpísaný.“. Následne používateľ klikne na „OK“. Aplikácia D.Signer .NET zaznamená túto informáciu, vypočíta digitálny odtlačok z podpisovaného súboru a po vytvorení podpisu mobilnou aplikáciou overí, či ide o rovnaký digitálny odtlačok. Ak áno, zobrazí oznam „Dokument bol úspešne podpísaný“.



Ak používateľ preruší proces vytvárania podpisu v mobilnej aplikácii, proces vytvárania podpisu bude ukončený s návratom do aplikácie a zobrazením okna.



7.4.2. Pracovná stanica

Na pracovnej stanici môže mať tlačidlo na vytvorenie elektronického podpisu niekoľko foriem:

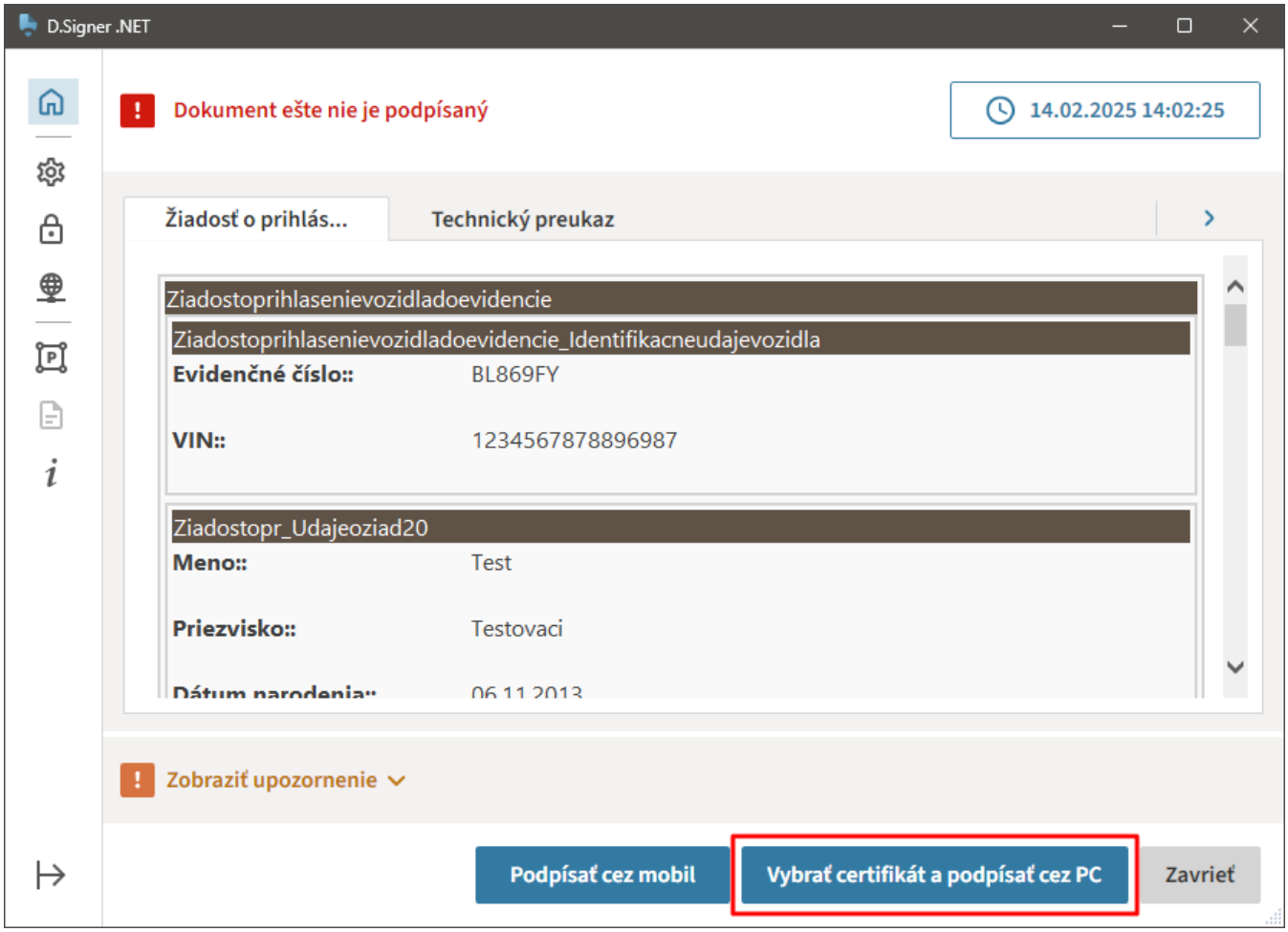
1) Ak aplikácia nemá zapamätaný aspoň jeden podpisový certifikát, ponúkne sa tlačidlo „Vybrať certifikát a podpísať cez PC“ – tento proces podpísania je ďalej uvedený
2) Ak aplikácia má aspoň jeden zapamätaný podpisový certifikát:

⇒ V texte tlačidla sa uvedie Meno a priezvisko z naposledy použitého podpisového certifikátu – kliknutím na tlačidlo dôjde k rýchlej voľbe tohto podpisového certifikátu.

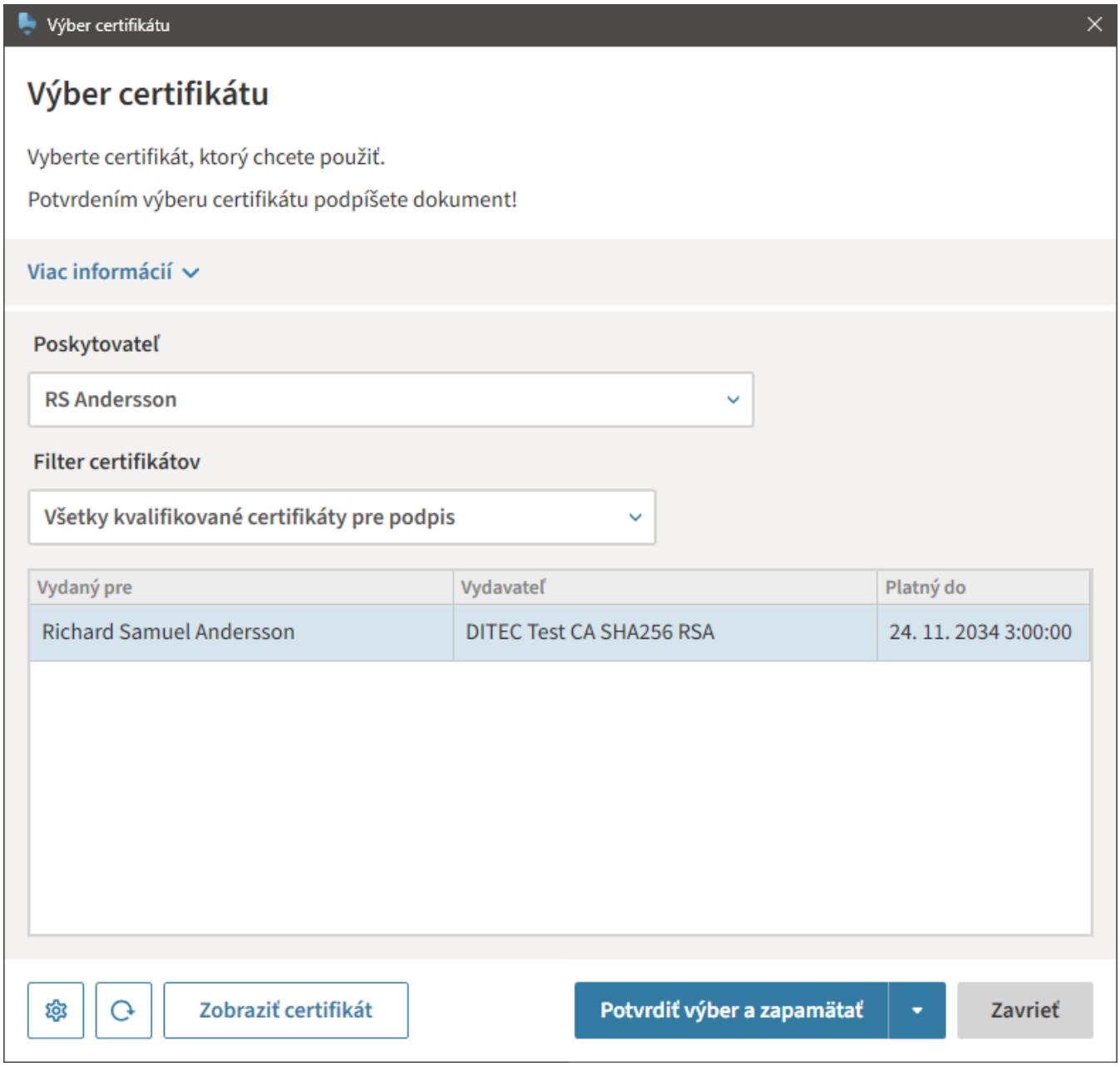
⇒ Vedľa tlačidla je umiestnená ikonka pre zobrazenie ostatných možností, kde na prvom mieste je voľba „Vybrať certifikát a podpísať cez PC“ (proces zhodný s bodom 1) a následne sú položky zo zoznamu zapamätaných certifikátov. Na ľavej strane týchto položiek sa nachádza ikonka na odstránenie podpisového certifikátu zo zoznamu uložených podpisových certifikátov.

Následný text uvádza popis z bodu 1, s uvedením postupu na zapamätanie si zvoleného podpisového certifikátu.

Kliknutím na tlačidlo „Vybrať certifikát a podpísať cez PC“ používateľ spustí proces vytvárania podpisu na dokumente.



Prvým krokom procesu vytvorenia podpisu je výber certifikátu, ktorým bude daný dokument podpísaný. Na nasledujúcom obrázku je znázornený dialóg pre výber certifikátu podpisovateľa.



V rámci zoznamu certifikátov na danom PC sú zobrazené položky:

- meno subjektu, pre ktorý bol certifikát vydaný,
- meno vydavateľa certifikátu,
- dátum konca platnosti certifikátu.

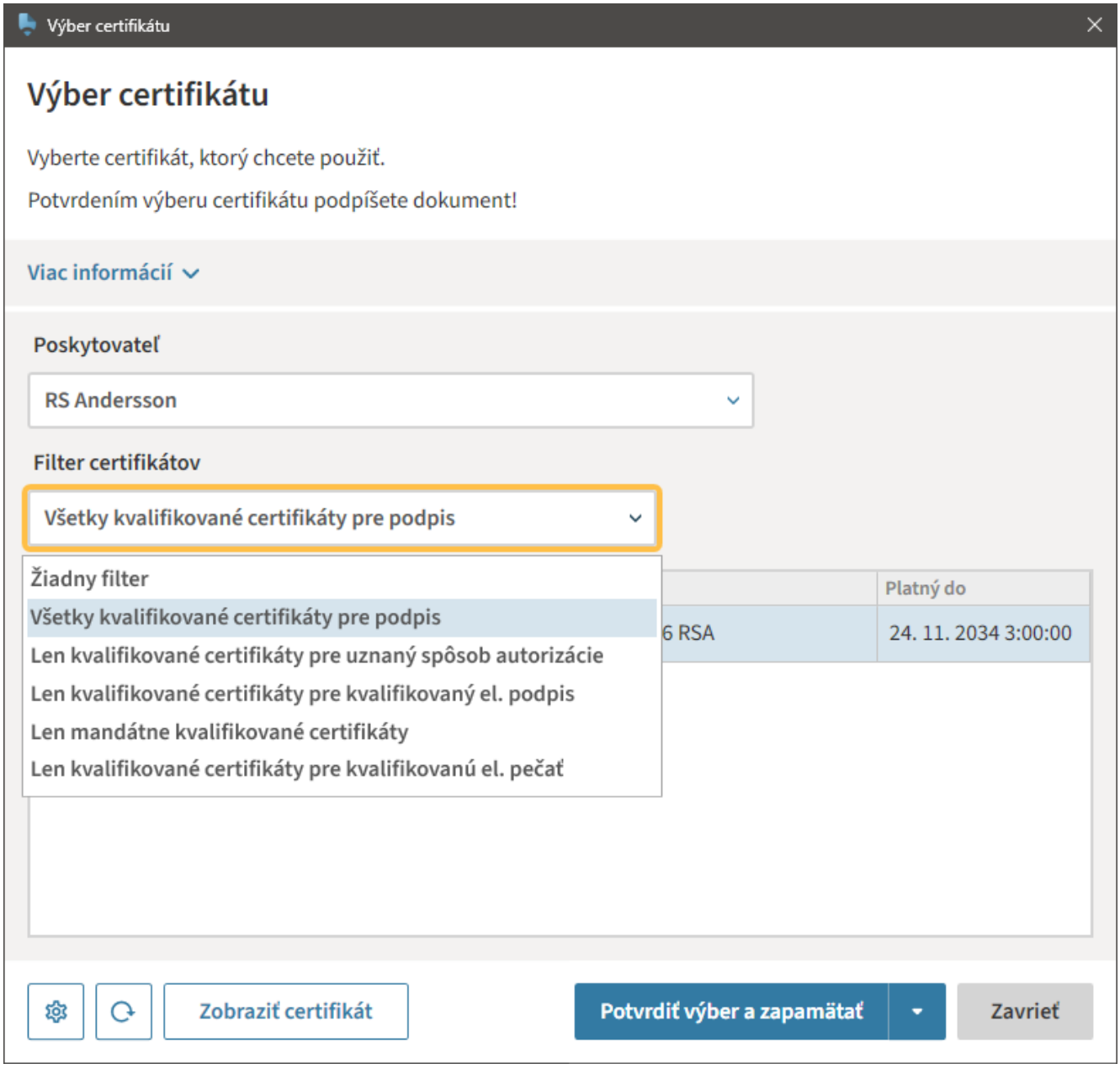
Aplikácia D.Signer .NET ponúkne na výber len certifikáty, ktorým ešte neuplynul dátum exspirácie. Detaily zvoleného certifikátu je možné prezrieť kliknutím na tlačidlo "Zobraziť certifikát".

Integrátor aplikácie D.Signer .NET môže spolu s aplikáciou distribuovať tiež nastavenia filtra pre zobrazenie len určitých certifikátov, ktoré spĺňajú definované pravidlá. V uvedenom dialógu pre výber certifikátu podpisovateľa sú napríklad zobrazené len kvalifikované certifikáty vydané v súlade so slovenskou legislatívou.

Pre vytvorenie zaručeného/kvalifikovaného elektronického podpisu musí podpisovateľ zvoliť zo svojho personálneho úložiska certifikátov kvalifikovaný certifikát, ktorý bol vydaný poskytovateľom

dôveryhodnej služby vydávania kvalifikovaných certifikátov. Ak príslušný právny úkon vyžaduje autorizáciu mandátnym kvalifikovaným certifikátom, používateľ musí zvoliť mandátny kvalifikovaný certifikát s príslušným oprávnením pre daný úkon podľa osobitného predpisu. Ak príslušný právny úkon umožňuje použiť kvalifikovaný certifikát pre uznaný spôsob autorizácie, používateľ si ich môže zobraziť nastavením filtra certifikátov na položku "Len kvalifikované certifikáty pre uznaný spôsob autorizácie". Pre vytvorenie obyčajného elektronického podpisu nie je potrebné použiť kvalifikovaný certifikát.

Zoznam zobrazených certifikátov, ktoré sú k dispozícii pre vytvorenie elektronického podpisu, je možné riadiť nastavením filtra certifikátov v okne pre výber certifikátu v aplikácii D.Signer .NET.



Po zvolení podpisového certifikátu a potvrdení výberu tlačidlom "Potvrdiť výber a zapamätať" aplikácia D.Signer .NET vykoná kontrolu stavu zneplatnenia podpisového certifikátu.[2] Primárne aplikácia vykoná kontrolu zneplatnenia zvoleného podpisového certifikátu pomocou služby OCSP. Ak je kontrola

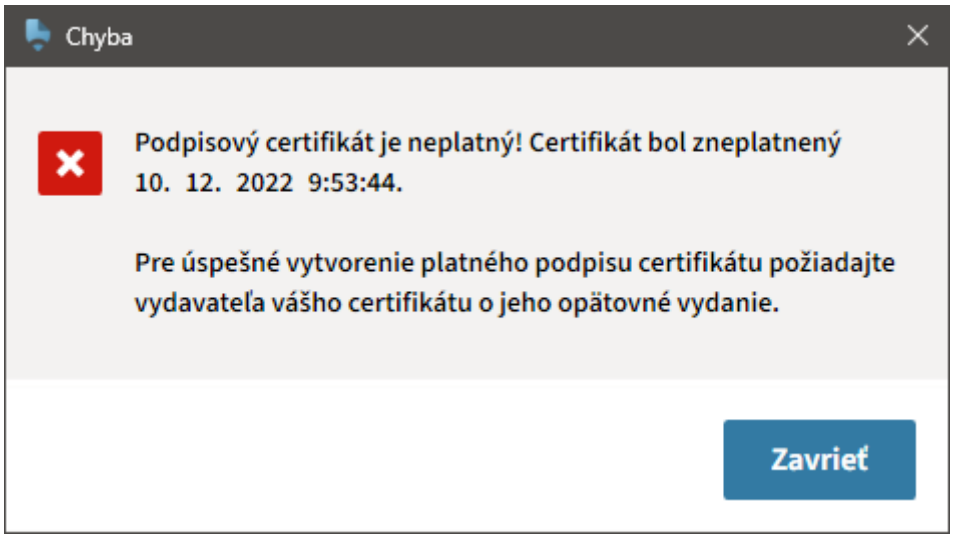
[2] V prípade, že kontrola zneplatnenia podpisového certifikátu je v konfiguračných nastaveniach aplikácie D.Signer .NET zapnutá.

neúspešná, napr. z dôvodu nedostupnej služby OCSP, tak aplikácia vykoná kontrolu zneplatnenia zvoleného podpisového certifikátu aj pomocou CRL.



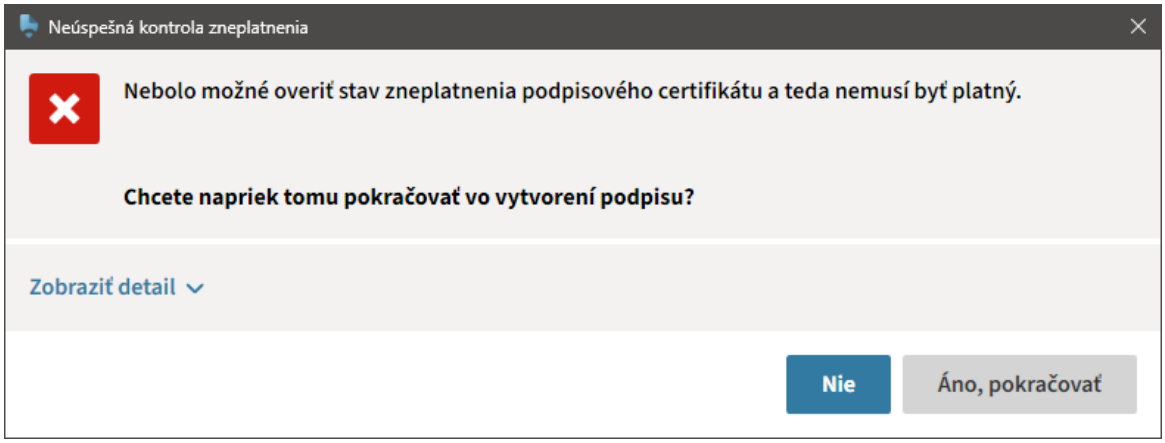


Ak aplikácia zistí, že certifikát bol zneplatnený, tak o tom informuje používateľa s odporúčaním, aby požiadal vydavateľa svojho certifikátu o jeho opätovné vydanie, a nepokračuje vo vytvorení elektronického podpisu.



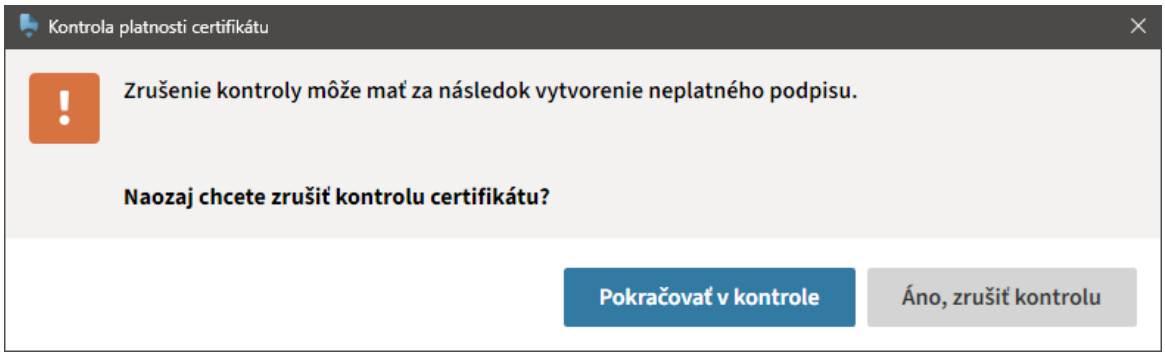
Ak je kontrola zneplatnenia zvoleného podpisového certifikátu neúspešná, tak aplikácia zobrazí upozornenie, že nebolo možné overiť stav zneplatnenia podpisového certifikátu a teda certifikát nemusí byť platný. Zároveň ponúkne používateľovi možnosti:

- Áno, pokračovať – vo vytvorení podpisu,
- Nie – nepokračovať vo vytvorení podpisu.



Ak kontrola zneplatnenia podpisového certifikátu trvá príliš dlho napr. z dôvodu slabého internetového pripojenia, používateľ má možnosť kontrolu zneplatnenia zrušiť kliknutím na tlačidlo "Zrušiť kontrolu". Vtedy aplikácia D.Signer .NET upozorní používateľa, že zrušenie kontroly môže mať za následok vytvorenie neplatného podpisu a vyžaduje potvrdenie zrušenia kontroly zneplatnenia, teda zobrazí okno s možnosťami:

- Pokračovať v kontrole,
- Áno, zrušiť kontrolu.

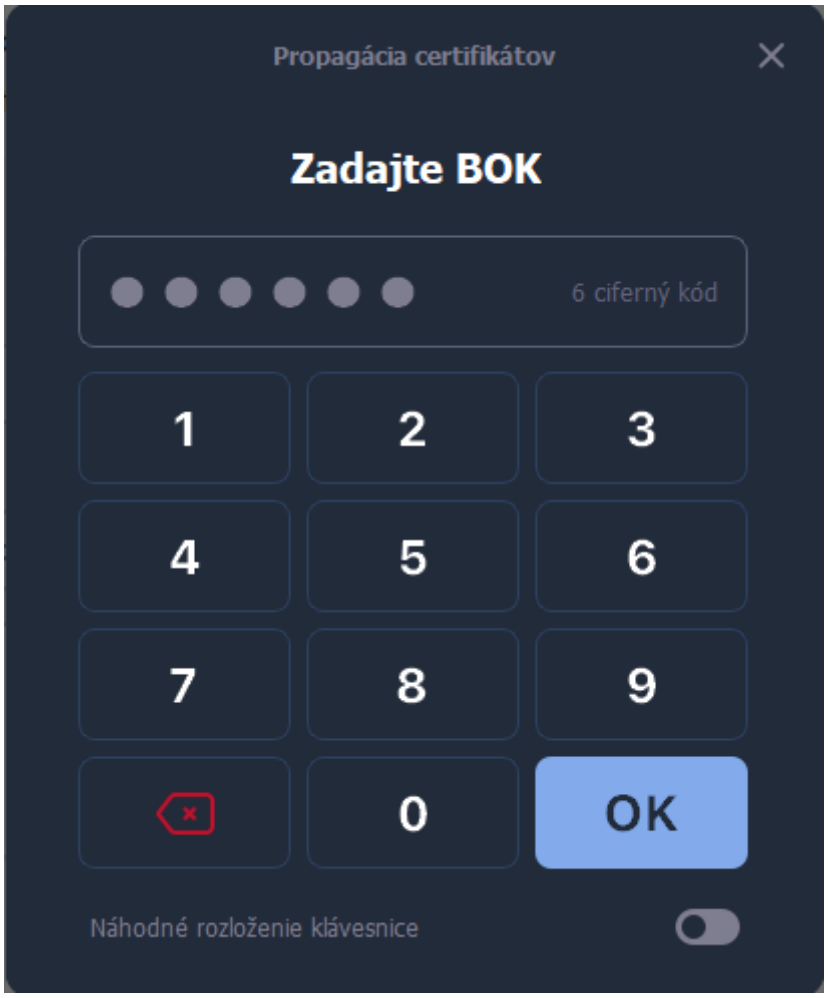


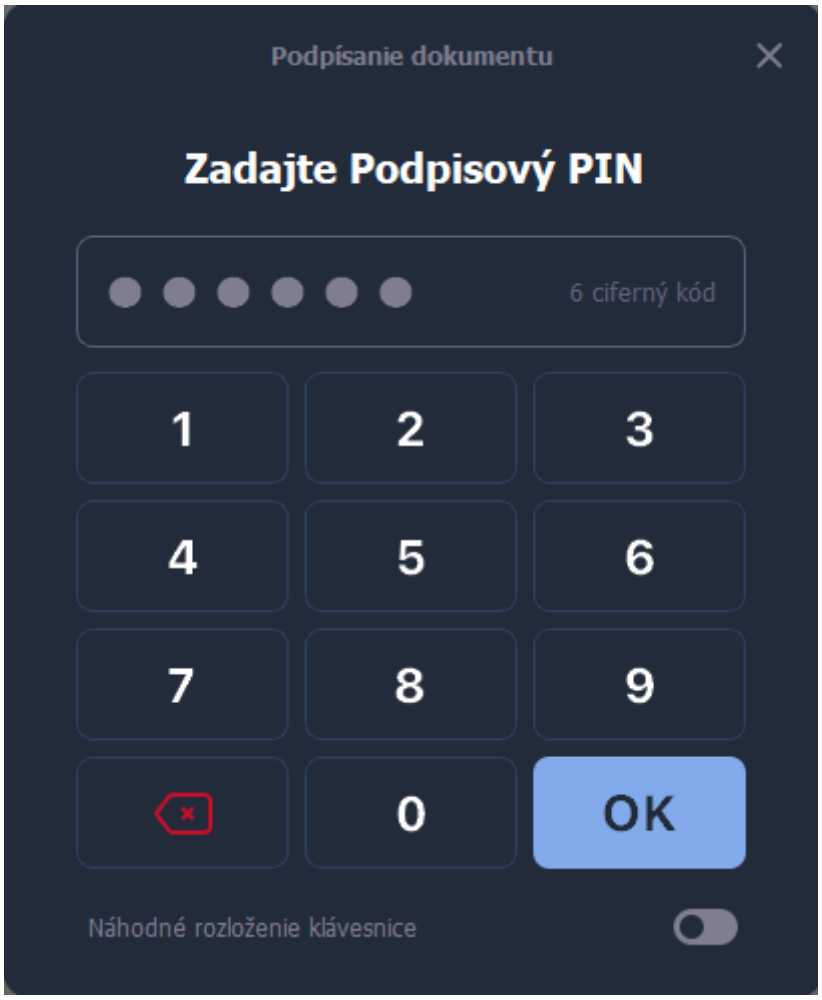
Pozor! Odporúčame nerušiť kontrolu zneplatnenia podpisového certifikátu. Zrušenie kontroly zneplatnenia podpisového certifikátu môže mať za následok vytvorenie neplatného podpisu.

Ak aplikácia pomocou kontroly zneplatnenia zistí, že certifikát je platný, vykoná proces vytvorenia elektronického podpisu. Aplikácia D.Signer .NET vytvorí reprezentáciu podpisovaných dát a parametrov podpisu – digitálny odtlačok. Pomocou rozhrania MS CryptoAPI alebo CNG a príslušného SSCD/QSCD zariadenia, na ktorom je uložený privátny kľúč patriaci k zvolenému podpisovému certifikátu, vytvorí hodnotu elektronického podpisu. Sprístupnenie privátneho kľúča na SSCD/QSCD zariadení môže vyžadovať autentifikáciu používateľa – zadanie BOKu[3] a/alebo PINu.[4]

[3] Bezpečnostný osobný kód.

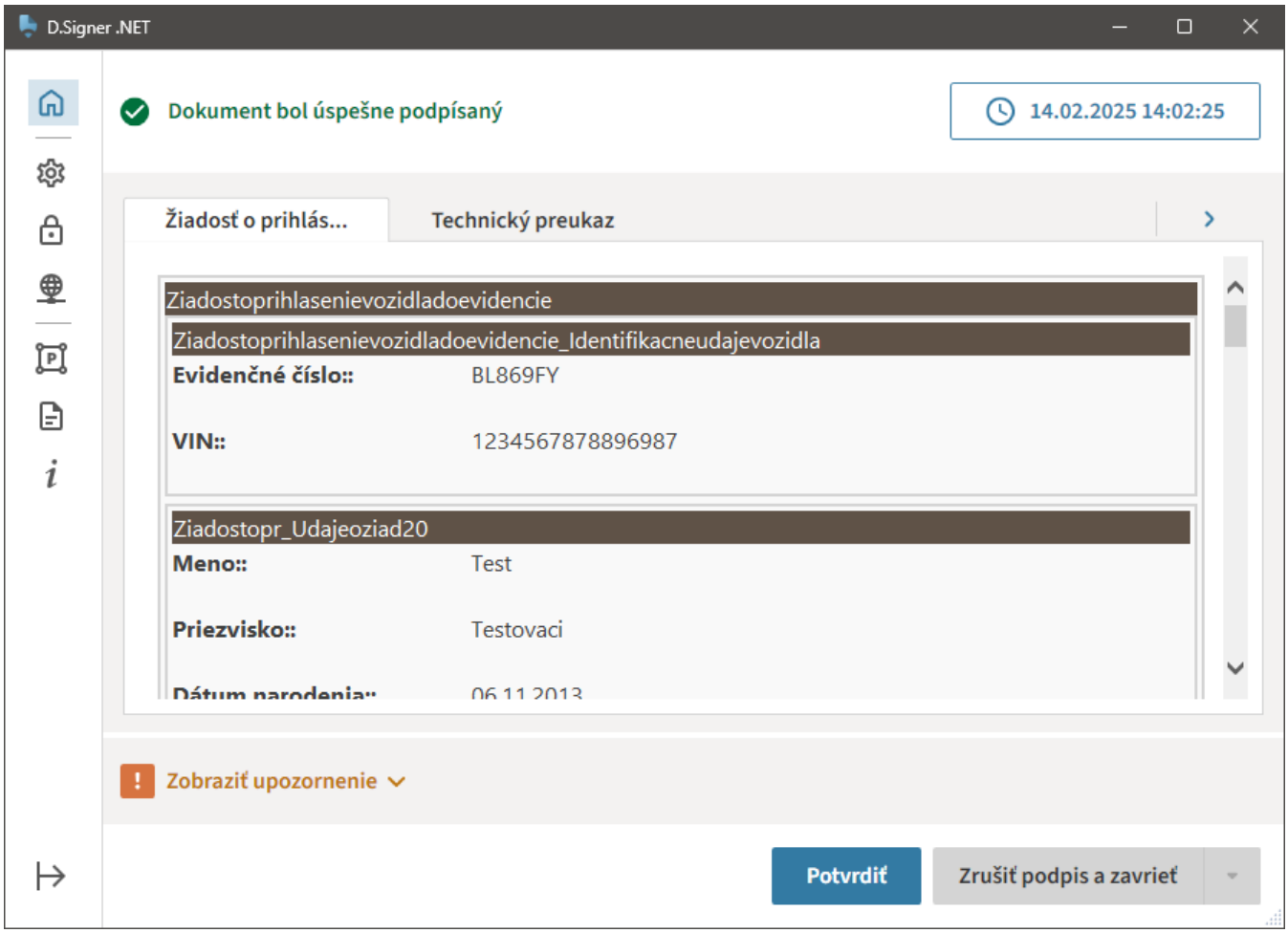
[4] Nastavenia SSCD/QSCD (napr. timeout pre PIN, dĺžka PIN apod.) sú v správe používateľa SSCD/QSCD zariadenia. Aplikácia D.Signer .NET neumožňuje meniť tieto nastavenia.


Propagácia certifikátov
Zadajte BOK
6 ciferný kód
1
2
3
4
5
6
7
8
9
0
OK
Náhodné rozloženie klávesnice



Aplikácia D.Signer .NET následne vytvorí a sformátuje výstupný podpísaný dokument v súlade s profilom XAdES_ZEP, resp. XAdES_ZEPbp. V prípade chyby v rámci procesu vytvorenia podpisu sa zobrazí príslušné chybové hlásenie. Ak sa dokument podarilo podpísať, v hlavnom okne sa zmení stav dokumentu a niektorých tlačidiel (sprístupnia sa tlačidlá tých funkcií, ktoré je možné vykonať len nad podpísaným dokumentom). Tiež sa podpisový certifikát uloží do zoznamu zapamätaných podpisových certifikátov (ak v ňom nie je), a pri budúcom podpisovaní sa tento certifikát ponúkne ako primárny na vytvorenie podpisu.

Používateľ má možnosť si vybrať voľbu „Potvrdiť výber“, ktorým prejde rovnakým procesom podpísania ako je popísaný vyššie, s tým rozdielom, že podpisový certifikát sa neuloží do zoznamu podpisových certifikátov.

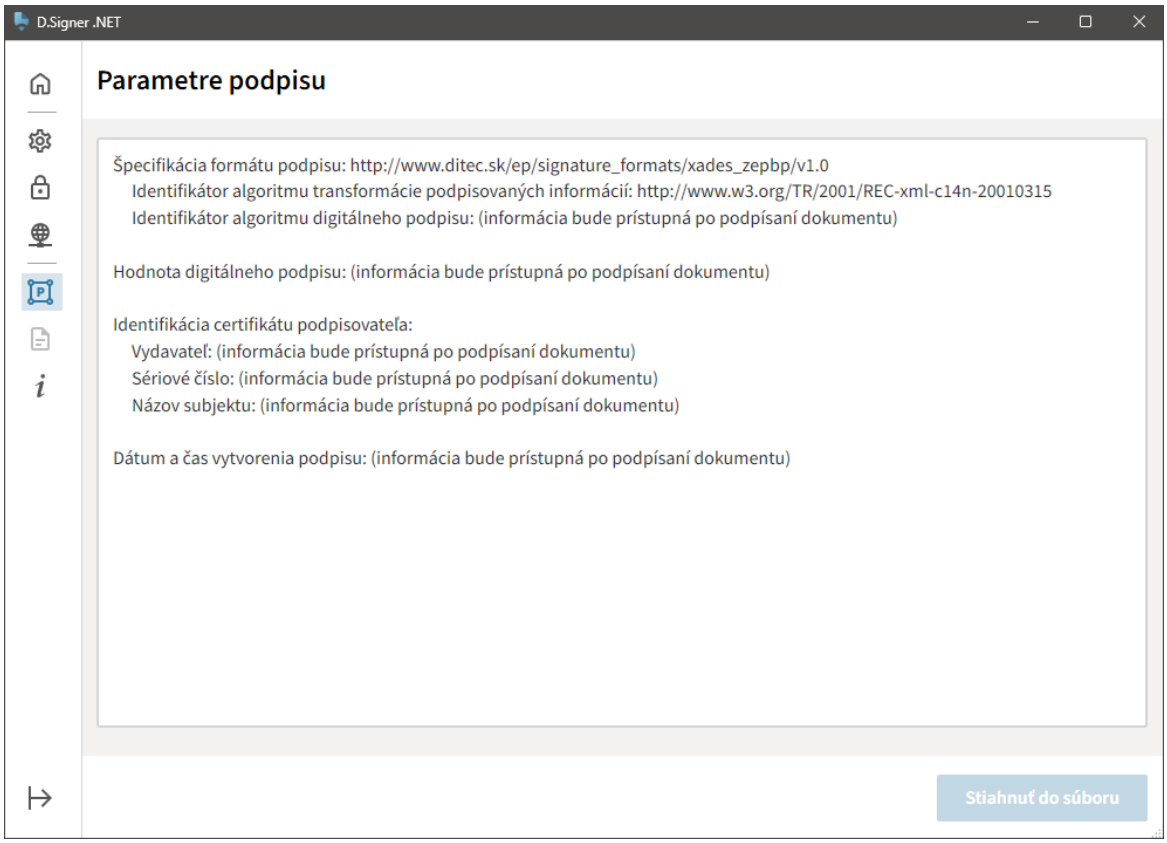


Po úspešnom vytvorení elektronického podpisu je podpísaný dokument odovzdaný klientskej aplikácii až po kliknutí na tlačidlo " Potvrdiť ".

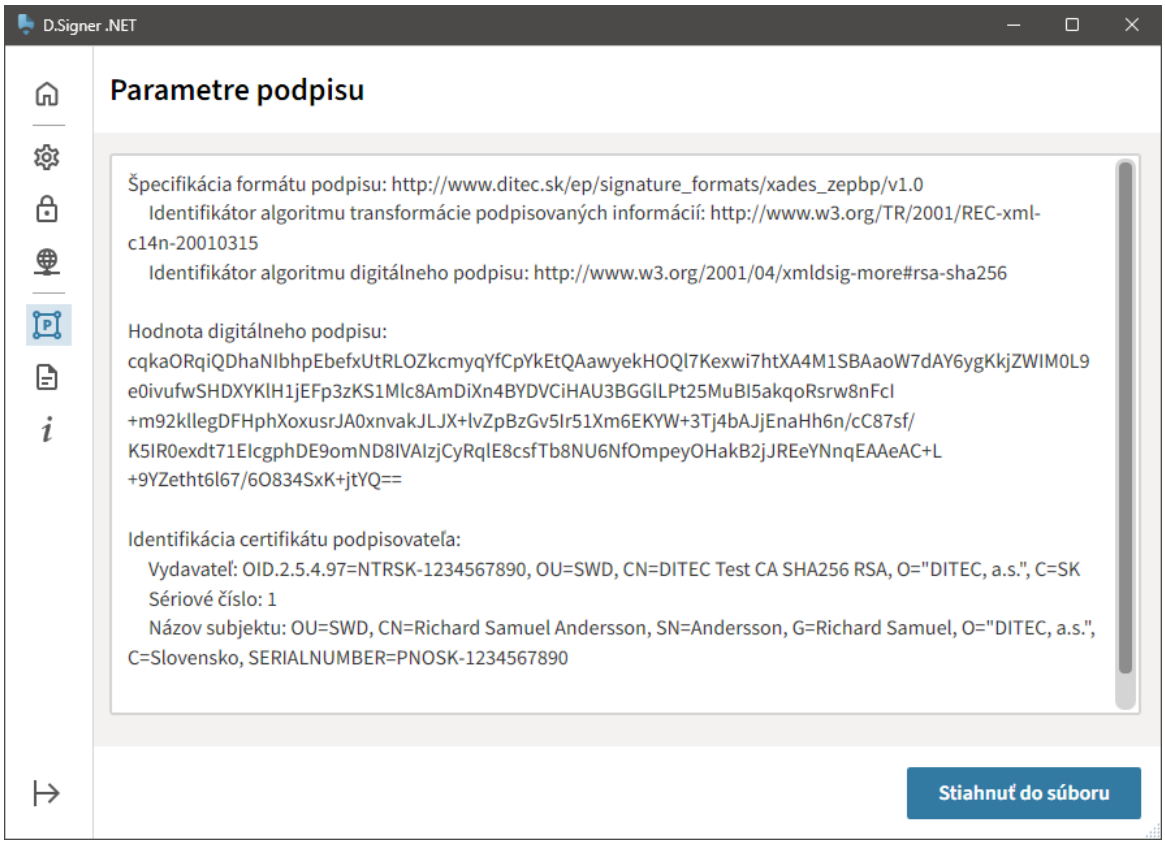
7.5. Zobrazenie parametrov podpisu

Používateľ, resp. podpisovateľ si môže pred alebo po podpísaní dokumentu zobraziť parametre podpisu (ikona s písmenom P v ľavej časti). V prípade ich zobrazenia pred vytvorením podpisu, resp. po vymazaní podpisu (tlačidlo "Zrušiť podpis" alebo „Zrušiť podpis a zavrieť“ v dolnej pravej časti hlavnej obrazovky), zobrazené informácie nebudú úplné, pretože niektoré z nich sú závislé na výbere podpisového certifikátu.

Na nasledujúcom obrázku je zobrazená obrazovka s parametrami podpisu pred podpísaním dokumentu.



Na nasledujúcom obrázku je zobrazená obrazovka s parametrami podpisu po podpísaní dokumentu.



Tieto informácie je možné stiahnuť do súboru, kliknutím na tlačidlo „Stiahnuť do súboru“.

V prípade, že podpis je z nejakého dôvodu potrebné zrušiť, tak je toto umožnené kliknutím na tlačidlo „Zrušiť podpis a zavrieť“, resp. „Zrušiť podpis“ na hlavnej obrazovke.

Zvolením „Zrušiť podpis a zavrieť“ sa vytvorený podpis zruší, a aplikácia sa ukončí.

Zvolením „Zrušiť podpis“ sa vytvorený podpis zruší a aplikácia sa uvedie do východzieho stavu, teda sa neukončí.

8. Trademarks

PDF technology in D.Signer .NET - PDF Plugin is powered by PDFNet SDK copyright © PDFTron™ Systems Inc., 2001-2025, and distributed by DITEC a.s. under license. All rights reserved.



Microsoft® .NET is software for connecting people, information, systems, and devices.