

Registrace do systému SDAT a vytvoření elektronického podpisu Vstupní zprávy

Obsah

Úvod	2
Předpoklady.....	2
Účet v SDAT	2
Nová registrace do prostředí SDAT	2
Elektronický podpis	2
Získání certifikátu	7
PostSignum.....	7
První certifikační autorita	7
eidentity	7
Postup pro vytvoření zálohy privátního klíče	7
Ověření a zavedení certifikátu v SDAT	8
Expirovaný certifikát	8
Možné chyby – důvody odmítnutí podepsané zprávy	11
Expirovaný certifikát	13
Jiný certifikát	14
Chybějící role „Věcný správce“	14

Úvod

Dokument poskytuje pokyny pro registraci do systému SDAT a popisuje předpoklady, požadavky a postup pro uživatelské vytvoření elektronického podpisu Vstupní zprávy pro systém SDAT.

Předpoklady

Aktivní uživatelský účet v SDAT, kvalifikovaný certifikát s veřejným klíčem registrovaným v SDAT, připravené prostředí a doplňky webového prohlížeče.

Účet v SDAT

Pokud jste v loňském roce zasílali výkazy do systému SDAT, jste již registrováni, Vaše uživatelské jméno je Váš e-mail, kterým jste se registrovali. Zapomenuté heslo je možné obnovit na stránce [Zapomenuté heslo](#). Pokud letos vykazujete poprvé, proveďte prosím nejprve registraci do prostředí SDAT. V případě pochybností se obraťte na sdat@cnb.cz. Dovolujeme si upozornit, že dotaz k systému SDAT bude odborným útvarem ČNB zodpovězen pouze v případě, že bude obsahovat alespoň následující informace:

- IČO společnosti, které se dotaz týká.
- Kontakt na osobu, která dotaz podává, včetně telefonu

Také je třeba, aby byl dotaz konkrétní. Bez výše uvedených informací Vám není možné poskytnout podporu.

Nová registrace do prostředí SDAT

Na adresu sdat@cnb.cz zašlete (do předmětu e-mailu uveďte „REGISTRACE FONDY“) požadavek s uvedením právě jednoho uživatele ve tvaru IČO, jméno, příjmení a e-mail (e-mail bude sloužit jako login) - uživatel bude založen s administrátorským oprávněním na produkčním prostředí. Věcný správce aplikace SDAT vytvoří účet a posléze přijde odkaz pro nastavení přístupového hesla. Uživatel následně může prostřednictvím webové aplikace SDAT zakládat další uživatele v kontextu spravované osoby (dle [dokumentace](#)).

Elektronický podpis

Předpoklady

Výkazy zasílané do ČNB je pro zajištění integrity a důvěryhodnosti nutné opatřit elektronickým podpisem. Ten je možné vytvořit přímo v prohlížeči, pokud jsou splněny následující předpoklady:

- Podporovaný operační systém;
- Podporovaný prohlížeč;
- Instalované rozšíření webového prohlížeče (doplňek);
- Instalovanou aplikaci I.CA PKIServiceHost.

Při vstupu na formulář pro odeslání Vstupní zprávy probíhá test splnění výše uvedených předpokladů. Tlačítko Podepsat se stane aktivním po úspěšném provedení testu, v opačném případě je možné kliknutím na odkaz Test zobrazit konkrétní nesplněné předpoklady:

Podpis v prohlížeči

Podepsat

✘ Uživatelské prostředí není připraveno. **Test**

Splnění předpokladů je uvedeno jednotlivě

🏠 > Vykazování > Stav vykazování - přehled > **Test prostředí pro podepisování**

Test prostředí pro podepisování

Test	Výsledek
Operační systém	✓ OK
Prohlížeč	✓ OK
Rozšíření	✓ OK
Aplikace PKI Service Host	✓ OK

a v případě negativního výsledku je u každé položky uvedena informace o problému; např. případě chybějícího rozšíření je uživateli poskytnut odkaz pro jeho instalaci:

🏠 > Vykazování > Stav vykazování - přehled > **Test prostředí pro podepisování**

Test prostředí pro podepisování

Test	Výsledek	
Operační systém	✓ OK	
Prohlížeč	✓ OK	
Rozšíření	✘ KO	Nainstalovat
Aplikace PKI Service Host		

Instalace komponent pro podpis

Aplikaci I.CA PKIServiceHost je možné stáhnout ze stránky

<https://www.ica.cz/aplikace-stazeni>

Aplikace ke stažení

I.CA PKIServiceHost



Aplikace I.CA PKIServiceHost slouží pro podporu generování žádostí o certifikát a k přístupu do portálu klientských služeb v prohlížečích IE/Firefox/Chrome/Opera.

V prohlížečích, vyjma Internetu Exploreru, je nutné současně s aplikací instalovat i její doplněk (dle používaného typu prohlížeče).

Přímý odkaz: <https://www.ica.cz/userfiles/files/app/ICAPKIServiceHost.exe>

Pro instalaci I.CA PKIServiceHost a doplňku kontaktujte správu vašeho IT.

Doplňky je možné dle prohlížeče stáhnout ze stránek:

Chrome

<https://chrome.google.com/webstore/detail/electronic-signature-cnb/hdbmbdpobhimeabanajlbkinlhkoflpk>

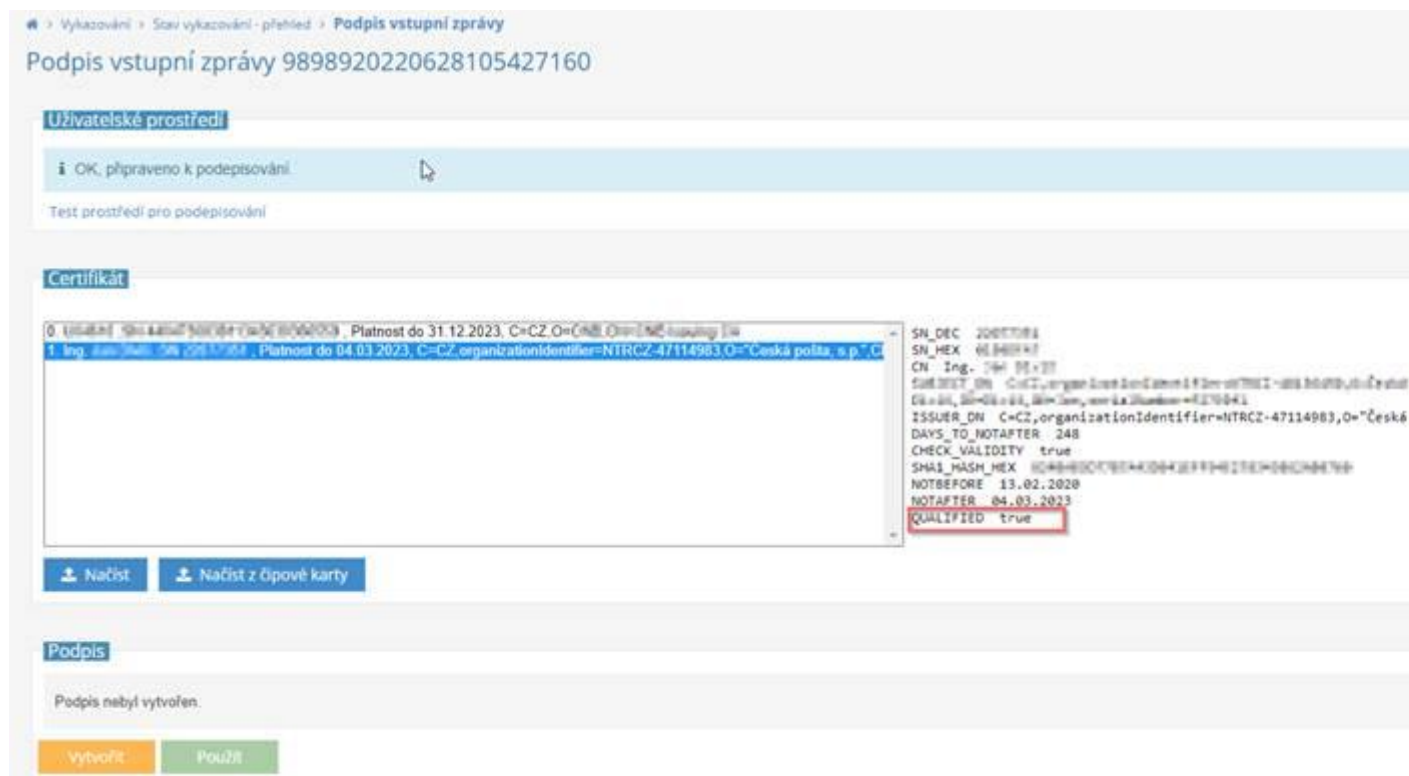
Edge

<https://microsoftedge.microsoft.com/addons/detail/elektronick%C3%BD-podpis-%C4%8Dnb/hlaepfiibpcgbjhnebnlninminifchd>

Dále je vyžadován elektronický kvalifikovaný certifikát dostupný v úložišti operačního systému nebo na čipové kartě / USB tokenu. Veřejný klíč tohoto certifikátu musí být registrován v systému SDAT.

Vytvoření podpisu

Po kliknutí na tlačítko Podepsat dojde k přesměrování na formulář pro vytvoření elektronického podpisu. Zde je nutné zvolit certifikát – lze jej načíst z úložiště operačního systému (Načíst) nebo z připojeného prostředku (Načíst z čipové karty):



Uživatelské prostředí

OK, připraveno k podepisování

Test prostředí pro podepisování

Certifikát

0 [ČNB] [6E36F4F2] [Ing. Petr P. P.] [Platnost do 31.12.2023, C=CZ, O=ČNB, OU=Mořavský ústřední úřad]

1 [ČNB] [6E36F4F2] [Ing. Petr P. P.] [Platnost do 04.03.2023, C=CZ, organizationIdentifier=NTRCZ-47114983, O=Česká pošta, s.p.a.]

Načíst Načíst z čipové karty

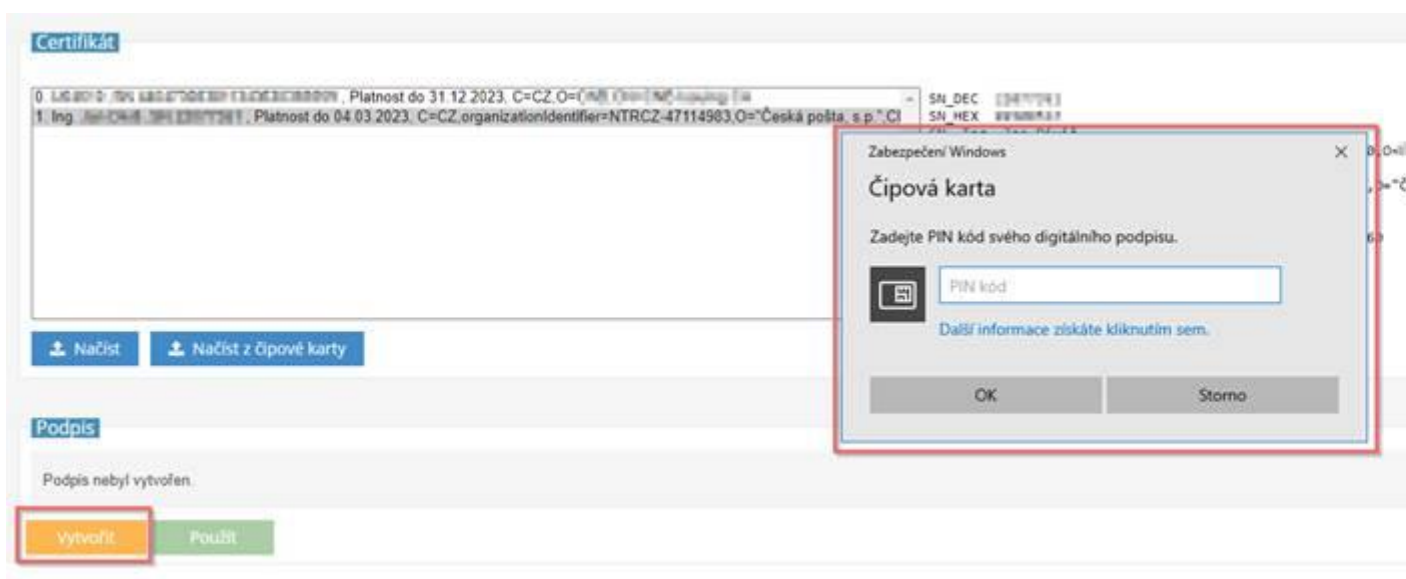
Podpis

Podpis nebyl vytvořen

Vytvořit Použít

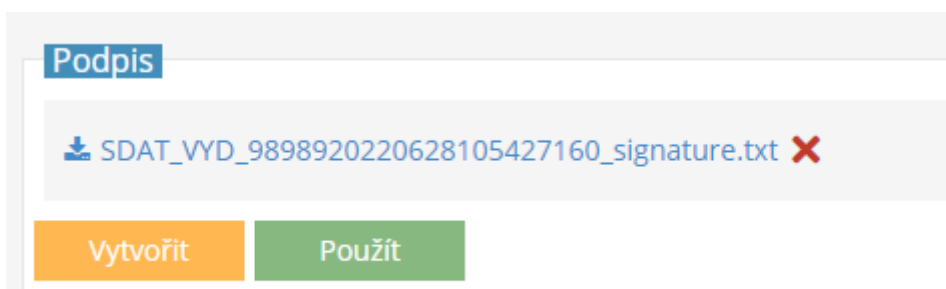
Kvalifikovaný certifikát lze mj. poznat podle atributu QUALIFIED = true v pravé části okna.

Po výběru certifikátu je možné podpis vytvořit (tlačítko vytvořit) a následně použít vytvořený podpis pro příslušnou Vstupní zprávu (tlačítko Použít). Kliknutím na tlačítko Vytvořit je vyvoláno dialogové okno vyžadující přístupový PIN/heslo k prostředku s uloženým certifikátem:

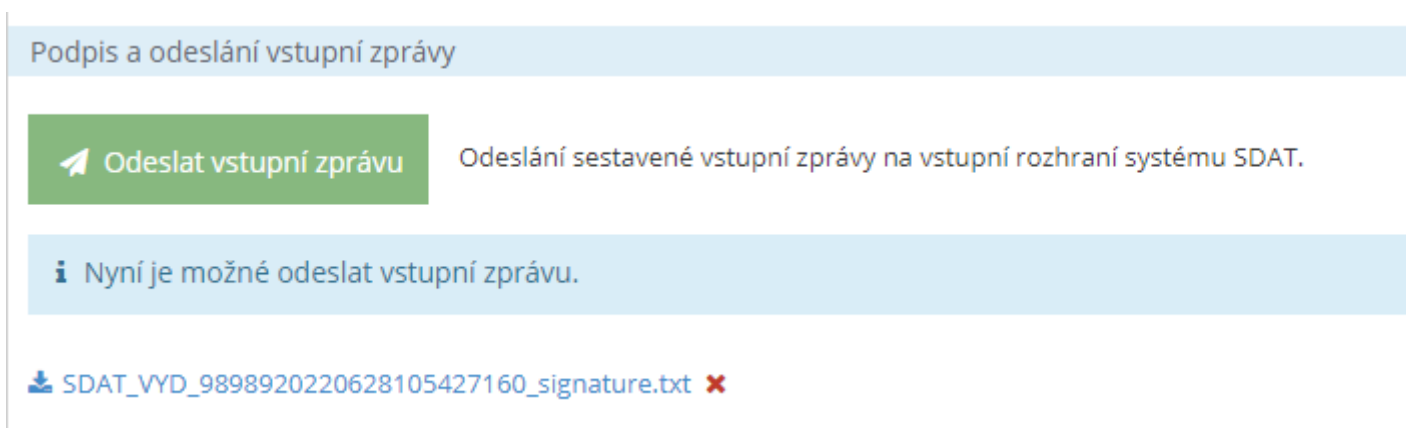


Pozor, nejedná se o heslo do SDAT!

Po úspěšném zadání PIN/hesla je vytvořen podpis:



Kliknutím na tlačítko Použít se vytvořený podpis připojí ke Vstupní zprávě



a nyní je možné ji odeslat pomocí tlačítka Odeslat Vstupní zprávu.

Získání certifikátu

Uživatel vytvářející podpis musí disponovat kvalifikovaným certifikátem, jehož veřejný klíč je registrován v systému SDAT.

Certifikáty vystavují certifikační autority. Pro elektronický podpis je požadován **kvalifikovaný certifikát**, který je možné získat od jedné z následujících autorit:

PostSignum

https://www.postsignum.cz/kvalifikovane_certifikaty.html

(<https://www.postsignum.cz/isignum.html>)

První certifikační autorita

<https://www.ica.cz/kvalifikovany-certifikat-pro-ePodpis>

<https://www.ica.cz/kvalifikovany-certifikat-pro-epecet>

eIdentity

<https://www.eidentity.cz/produkty-a-sluzby/#kvalifikovane>

Každý certifikát má tzv. veřejný (*public key*) a soukromý (též privátní, *private key*) klíč. Veřejný klíč je dohledatelný na stránkách vystavujících autorit a slouží pro **ověření** podpisu – proto je nutné jej registrovat do systému SDAT, který podle něj ověří platnost příslušného podpisu na odpovídající Vstupní zprávě. Soukromý klíč slouží k vytvoření podpisu; náleží pouze svému držiteli (neposílejte je nikomu e-mailem ani nenahrávejte do SDAT). Práce se soukromým klíčem vyžaduje heslo/PIN k certifikátu, nejedná se o heslo do SDAT a stran zapomenutého hesla/PINu k certifikátu nelze od ČNB získat žádnou formu podpory.

Soukromý klíč existuje buď ve formě souboru (zpravidla s příponou .pfx) získaného exportem (zálohou) certifikátu, nebo je uložen na kvalifikovaném prostředku (typicky čipová karta nebo USB token). Pokud máte certifikát na kvalifikovaném prostředku, musí být tento v čase podepisování připojen k počítači.

Soukromý klíč v podobě souboru získáte exportem certifikátu se zahrnutím volby „vč. soukromého klíče“.

Postup pro vytvoření zálohy privátního klíče

PostSignum – pomocí aplikace iSignum (<https://www.postsignum.cz/isignum.html?step=2#m9>) nebo https://www.postsignum.cz/files/navody/zaloha_klice/index.html

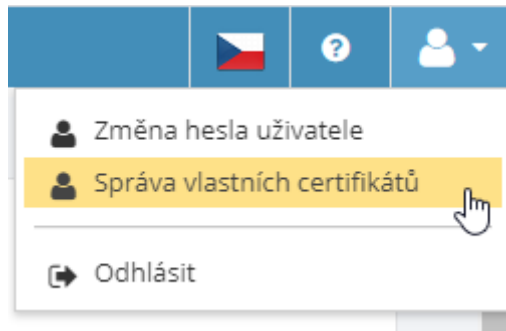
První certifikační autorita - <https://www.ica.cz/zaloha-klice>

eIdentity - <https://www.eidentity.cz/technicka-podpora/>

V případě nejistoty ohledně získání privátního klíče se obraťte na autoritu, která vám certifikát vystavila.

Ověření a zavedení certifikátu v SDAT

Po přihlášení do produkčního prostředí SDAT klikněte na ikonu uživatele



a zvolte Správa vlastních certifikátů.

System zobrazí seznam Vašich certifikátů (v systému lze mít více certifikátů). Ověřte, že datum platnosti aktivního certifikátu, se kterým bude vytvořen podpis, je vyšší, než aktuální datum:

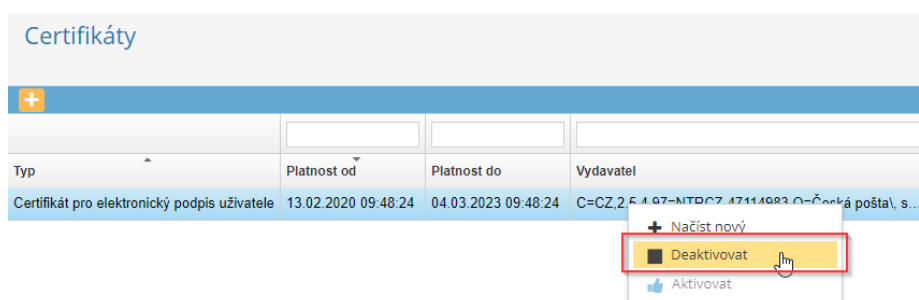
Typ	Platnost od	Platnost do	Vydavatel	Subjekt	Sériové číslo	Aktivní	Zneplatněn	Akce
Certifikát pro elektronický podpis uživatele	22.02.2019 10:26:00	22.02.2020 10:26:00	C=CZ.O=Česká pošta, s.p...	C=CZ.2.5.4.97=NTRCZ-481...	4cf651	<input checked="" type="checkbox"/>		

Pokud je seznam prázdný nebo pokud je **Platnost do** u aktivního certifikátu starší, než aktuální datum (certifikát je expirovaný), je nutné registrovat nový certifikát.

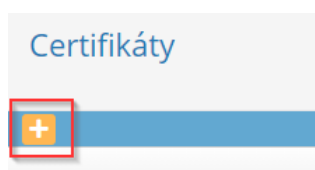
U certifikátu je uvedeno jeho sériové číslo. Pro vytvoření podpisu je nutné použít privátní klíč odpovídajícího sériového čísla.

Expirovaný certifikát

Ohledně vystavení nového nebo následného certifikátu je nutné kontaktovat vystavительskou autoritu. V systému SDAT je vhodné takový certifikát deaktivovat a nahrát nový:



Nový certifikát lze registrovat kliknutím na ikonu 



nebo přes kontextové menu **Načíst nový**:

Certifikáty

Typ	Platnost od	Platnost do	Vydavatel
Certifikát pro elektronický podpis uživatele	13.02.2020 09:48:24	04.03.2023 09:48:24	0-07305103-NT007-17114003,0-

+ Načíst nový
Deaktivovat
Aktivovat

Certifikáty

+

Načtení certifikátu

Typ: Certifikát pro elektronický podpis uživatele Uživatel: [Uživatel]

Soubor: 🔍

Počátek platnosti: Konec platnosti:

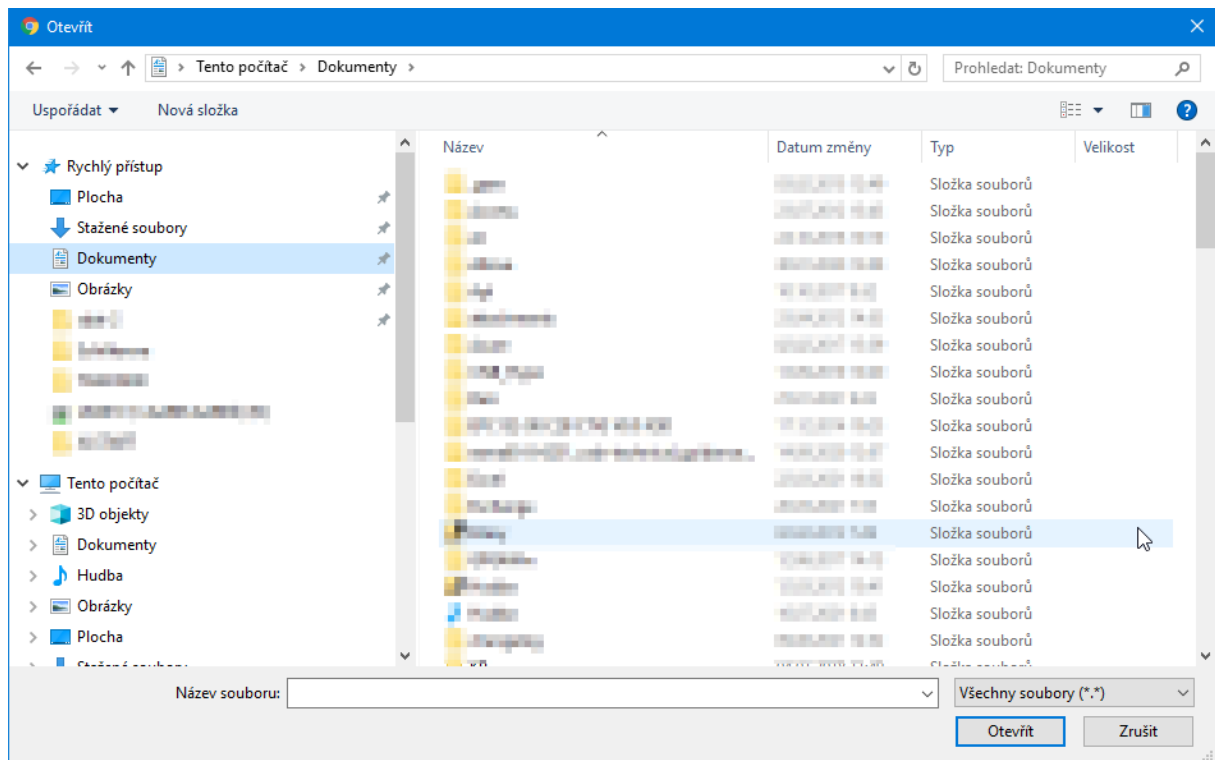
Sériové číslo:

Vydavatel:

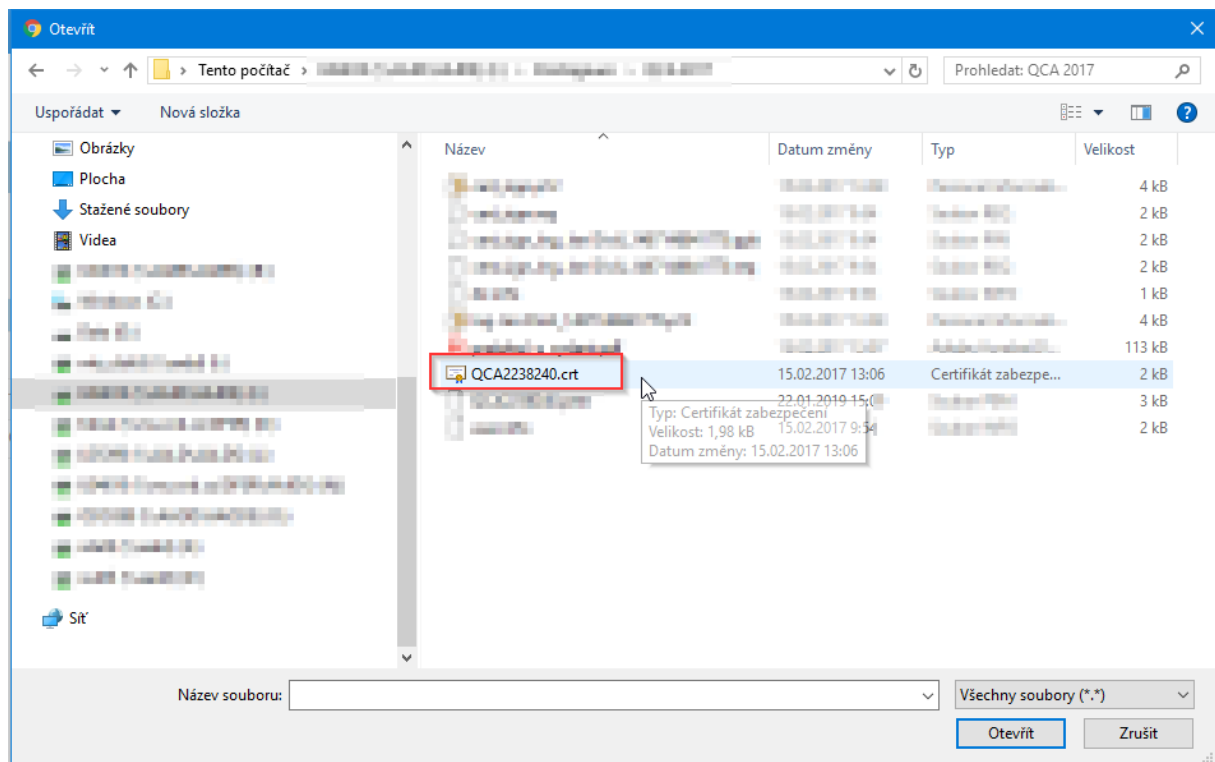
Subjekt:

Uložit

V dialogovém okně **Načtení certifikátu** lze vyhledat (na disku počítače) veřejný klíč kliknutím na ikonu lupy. Zobrazí se systémové okno procházení souborů:



Veřejný klíč najdete na disku zpravidla s příponou **.crt**:



Po výběru vhodného certifikátu se načtou jeho metadata do dialogového okna **Načtení certifikátu**:

Načtení certifikátu

Typ: Certifikát pro elektronický podpis uživatele

Uživatel *

Soubor: QCA22077351.crt

Počátek platnosti: 13.02.2020 09:48:24

Konec platnosti: 04.03.2023 09:48:24

Sériové číslo

Vydavatel: C=CZ,2.5.4.97=NTRCZ-47114983,O=Česká pošta, s.p.,CN=PostSignum Qualified CA 4


Subjekt: C=CZ,2.5.4.97=NTRCZ-48136450,O=Česká národní banka,OU=4610,...

Uložit

a je nutné kliknout na tlačítko **Uložit**.

Poznámka: systém neumožní nahrát expirovaný certifikát:

Varování

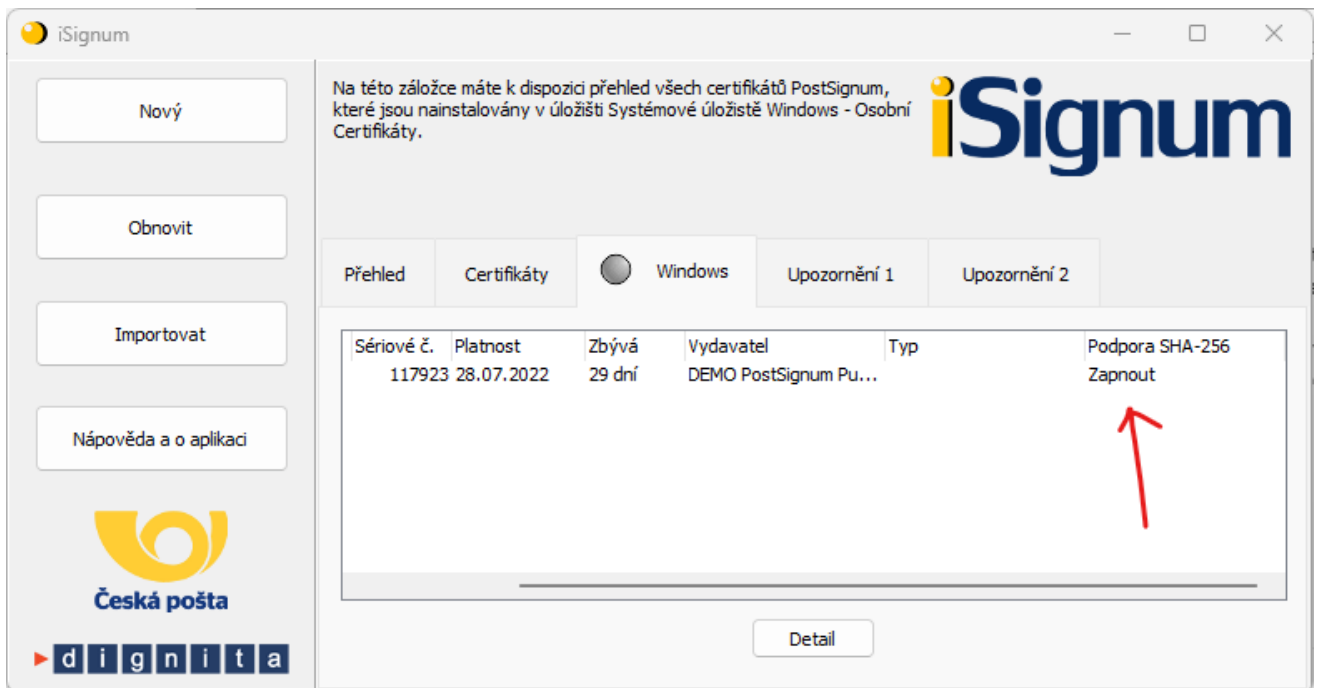
 CRT0001: Systém neumožňuje uložení certifikátu s ukončenou platností.

Zavřít

Možné chyby – důvody odmítnutí podepsané zprávy

Podpis se nepodaří vytvořit

Pokud se zobrazí zpráva „Podpis se nepodařilo vytvořit“, ověřte prosím u příslušného certifikátu zapnutou podporu SHA-256:



Pro ověření je nutné stáhnout program iSignum, pro správu certifikátů PostSignum:

<https://www.postsignum.cz/isignum.html>

Odmítnutí zaslaného podpisu

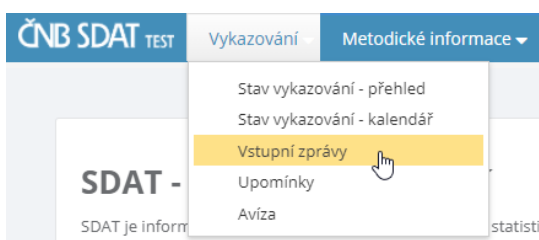
Vstupní zpráva bude při chybném podpisu odmítnuta; v protokolu se objeví chyba SDAT_1006

```

- <Hlavicka>
  <CasVytvoreni>2021-08-03T15:11:12.746</CasVytvoreni>
  <Typ>VZ</Typ>
  <Nazev>Protokol o zpracování vstupní zprávy <img alt="redacted" data-bbox="400 530 450 540"/></Nazev>
  <VerzeProtokolu>1.0.0</VerzeProtokolu>
</Hlavicka>
- <VstupniZprava>
  <VstupniZpravaId><img alt="redacted" data-bbox="180 570 250 580"/></VstupniZpravaId>
  <ReferencniId><img alt="redacted" data-bbox="180 580 250 590"/></ReferencniId>
  <ZasilajiciOsobaKod><img alt="redacted" data-bbox="180 590 250 600"/></ZasilajiciOsobaKod>
  <ZasilajiciOsobaNazev><img alt="redacted" data-bbox="180 600 880 610"/></ZasilajiciOsobaNazev>
  <DatumVytvoreni>2021-08-03T15:07:23.879</DatumVytvoreni>
  <DatumPrijeti>2021-08-03T15:07:24.629</DatumPrijeti>
  <StavVstupniZpravy>ODMITNUTO</StavVstupniZpravy>
  <PocetVydaniCelkem>0</PocetVydaniCelkem>
- <ZjisteneChyby>
  - <Chyba>
    <Kod>SDAT_1006</Kod>
    <Zavaznost>Zavazna</Zavaznost>
    <Text>Vstupní zpráva není podepsána registrovaným certifikátem v SDAT.</Text>
  </Chyba>
</ZjisteneChyby>
</VstupniZprava>

```

XML protokol je dostupný přes Vykazování – Vstupní zprávy:



přes ikonu ve sloupci Protokol:

» > Vykazování > Vstupní zprávy

Vstupní zprávy

Poslední podle času přijetí Datum od 05.05.2021 Datum do 05.08.2021 záznamů: [54]

Kód osoby	Název osoby	Čas vytvoření	Čas přijetí	Vstupní kanál	Stav	Změna stavu	Referenční ID	Uživatel	Přijatá vydání	Odmítnutá vydání	Protokol	Obsah
VZ	Teleskopový stánek	04.08.2021 11:14:28	04.08.2021 11:14:28	Webová aplikace	Dokončené	04.08.2021 11:18:58	SDAT_1006	Uživatel	1	0		
VZ	Teleskopový stánek	03.08.2021 09:50:46	03.08.2021 09:50:46	Webová aplikace	Dokončené	03.08.2021 09:53:17	SDAT_1006	Uživatel	1	0		
VZ	Teleskopový stánek	03.08.2021 09:47:25	03.08.2021 09:47:25	Webová aplikace	Dokončené	03.08.2021 09:48:04	SDAT_1006	Uživatel	1	0		

V aplikaci je chyba a její popis zobrazena na detailu Vstupní zprávy, záložka Chyby zpracování

» > Zpracování > Vstupní zprávy > Detail vstupní zprávy

Detail vstupní zprávy

Běhy akcí Chyby zpracování Přijatá vydání

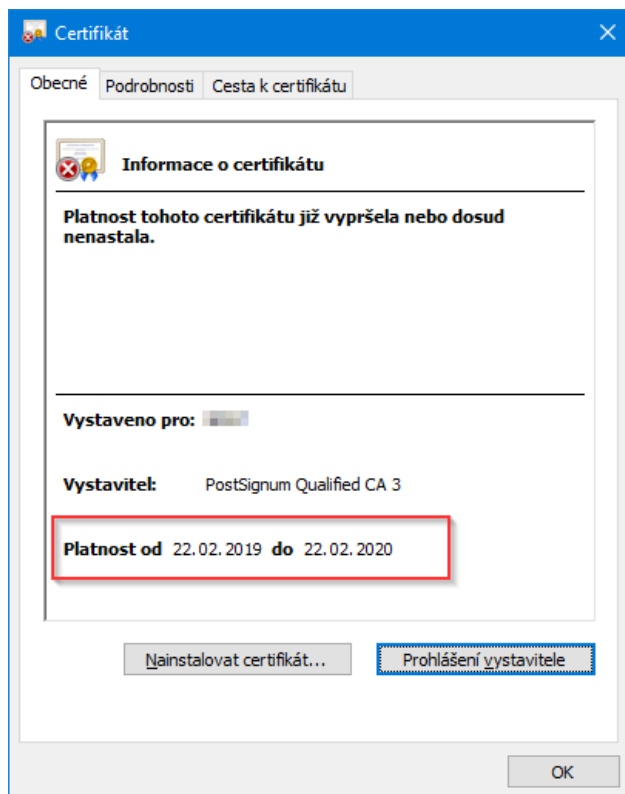
Základní informace

Krok zpracování	Kód	Název	Závažnost	Typ	Popis
VZ	SDAT_1006	Vstupní zpráva není podepsána registrovaným ce...	Závažná	APL	Použitý certifikát není registrovaný pro zasílající osobu nebo pracovníka osoby nebo je neaktivní.

Důvody mohou být následující:

Expirovaný certifikát

Informaci o platnosti certifikátu lze najít v certifikátu samotném, nebo v aplikaci SDAT.



ČNB SDAT TEST

Certifikáty

Změna hesla uživatele
Správa vlastních certifikátů
Odhlásit

Typ	Platnost od	Platnost do	Vydavatel	Subjekt	Sériové číslo
Certifikát pro elektronický podpis uživatele	20.02.2019 09:47:20	11.03.2020 09:47:20	C=CZ,O=Česká pošta, s.p. [...]	C=CZ,O=Česká národní bank...	6655f

Jiný certifikát

Uživatelé mohou disponovat několika certifikáty; pokud je pro podpis zvolen certifikát, který není registrován v SDAT, podpis se sice technicky správně vytvoří, nedojde však k jeho spárování s certifikátem, který v SDAT chybí.

Chybějící role „Věcný správce“

Vykazovat může pouze uživatel s rolí Věcný správce (pro vykazování daného výkazu). Nastavení role je dostupné v Správa osoby – Uživatelé – detail uživatele

Správa osoby > Uživatelé > Uživatel

Jan Dvořák

Základní informace

Titul před Příjmení * Jméno * Titul za

Platnost od 27.06.2017 Platnost do 01.01.4000

Funkce Zaslání eviz Zaslání protokolů

Email Telefon

Role Oprávnění uživatele Certifikáty Historie

Všechny

Role	Platnost od	Platnost do	Kód vykazovacího rámce	Název vykazovacího rámce	Kód výkazu
Věcný správce	27.06.2017	01.01.4000			