Česká pošta

Identifikace		**Číslo jednací**	
Nahrazuje		**Klasifikace**	veřejné
Platnost	16. 2. 2023	**Účinnost**	16. 2. 2023

Uživatelská příručka

ProID+Q
ProID+Q (gen. 2)

Verze 1.7

Obsah dokumentu

Evidence revizí a změn

Verze	Datum revize	Důvod a popis změny	Autor	Schválil
1.0	16. 5. 2018		Česká pošta, s.p.	Manažer CA
1.1	27. 7. 2018	doplněna možnost pro el. pečetě	Česká pošta, s.p.	Manažer CA
1.2	16.4.2019	Odstraněn servisní klíč	Česká pošta, s.p.	Manažer CA
1.3	1. 12. 2019	změna postupu rušení vazby prostředku na osobu	Česká pošta, s.p.	Manažer CA
1.4	28. 1. 2020	přidán postup na výmaz klíčů a certifikátů	Česká pošta, s.p.	Manažer CA
1.5	30. 11. 2020	doplněn nový typ prostředku	Česká pošta, s.p.	Manažer CA
1.6	26. 10. 2022	doplněn typ žádosti KC	Česká pošta, s.p.	Manažer CA
1.7	16. 2. 2023	změna v souvislosti s novou verzí iSignum	Česká pošta, s.p.	Manažer CA

1. Přehled

ProID+Q nebo ProID+Q (gen. 2) (dále jen prostředek) **je čipová karta nebo USB token schválená jako kvalifikovaný prostředek pro vytváření elektronických podpisů a elektronických pečetí v souladu s nařízením eIDAS**. Je to PKI prostředek s kontaktním čipem postavený na kryptografickém mikroprocesoru s certifikací Common Criteria EAL4+ a FIPS 140-2 level 3.

Informace k certifikaci prostředků:
Každý prostředek má certifikaci časově omezenou. Po skončení certifikace přestává být kvalifikovaným prostředkem. K datu skončení certifikace budou zneplatněné všechny platné kvalifikované certifikáty, které jsou na prostředku uloženy.

Po ukončení certifikace již nebude možné na prostředek uložit kvalifikovaný certifikát s příznakem QESCD.

O platnosti certifikace konkrétního prostředku se můžete přesvědčit na webových stránkách PostSignum: https://www.postsignum.cz/certifikace_prostredku.html

Upozornění: Aplikace iSignum bude i v případě ukončené certifikace označovat prostředek jako kvalifikovaný, nicméně funkce prostředku pro kvalifikované certifikáty budou omezeny. Ukončená certifikace se nedotkne komerčních certifikátů.

Prostředek je personalizován již z výroby, tzn., je na ní přednastaven PIN (12345678), PUK (87654321) a QPIN (12345678)**.**

Prostředek obsahuje oblast pro uložení kvalifikovaného certifikátu. Tuto oblast chrání **podpisový PIN** tzv. **QPIN**, který je vyžadován vždy při přístupu do této oblasti, tzn. při generování žádosti o kvalifikovaný certifikát nebo při použití kvalifikovaného certifikátu.

Čipová karta může být kromě kontaktního čipu vybavena také bezdrátovým čipem nebo magnetickým proužkem.

Z bezpečnostních důvodů je při prvním použití nutné změnit PIN, PUK i QPIN.

Upozorňujeme, že při zablokování PIN i PUK i QPIN dojde ke znehodnocení kontaktního čipu.

Při vydání prvního certifikátu dochází k vytvoření vazby **prostředek–žadatel o certifikát**, která je evidována v systému certifikační autority a kontrolována při vydávání dalších (následných) certifikátů do zařízení. Technicky tedy není možné mít na prostředku více certifikátů různých žadatelů s příznakem QESCD (kvalifikované) nebo NCP+ (komerční). Toto platí jak pro osobní kvalifikované a komerční certifikáty, tak pro certifikáty pro el. pečeť.

Pokud dojde k situaci, že je nutné prostředek předat jinému žadateli (např. z důvodu ukončení pracovního poměru) je nutné postupovat dle kapitoly 8.2

2. Co potřebuji?

1. PC s operačním systémem Windows

2. Prostředek nebo USB token

3. Čtečku čipových karet a ovladač ke čtečce čipových karet
   Čtečku je nutné mít připojenou k počítači, např. pomocí USB portu nebo jinou technologií, kterou čtečka podporuje. Čtečka může být také integrovaná přímo v počítači.
   Před započetím instalace softwaru je nutné, aby byla čtečka čipových karet v počítači nainstalována a byla funkční. **Pro USB token není čtečka nutná.**

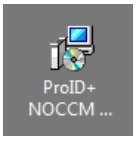
4. Software

   Software je ke stažení na webových stránkách:
   https://www.proid.cz/podpora/

3. Instalace softwaru

Ke správné instalaci softwaru je potřeba vykonat následující kroky:

1. Otevřít aplikaci ProID+ NOCCM CZ x64.msi, případně ProID+ NOCCM CZ x86.msi, dle Vašeho OS.



2. Odsouhlasit instalaci programu ProID+ kliknutím na tlačítko *Další*
3. Akceptovat licenční podmínky zaškrtnutím políčka „Souhlasím s podmínkami uvedenými v licenční smlouvě“ a pokračovat kliknutím na tlačítko *Další*
4. Vybrat cílovou složku a pokračovat kliknutím na tlačítko *Další*
5. Vybrat typ instalace a kliknout na tlačítko *Další*
6. Vybrat z doplňkových funkcí instalace (není nutno) a program nainstalovat kliknutím na tlačítko *Instalovat*
7. Zasunout čipovou kartu do čtečky karet nebo USB token do portu USB. Bude provedena dodatečná instalace ovladačů. Po jejich nainstalování bude možné prostředek používat.

Knihovna PKCS#11

V případě použití prostředku v aplikacích, které nevyužívají systémové úložiště certifikátů ve Windows (např. Mozilla Firefox nebo Thunderbird), lze ke komunikaci s prostředkem využít (pokud to aplikace podporuje) DLL knihovnu PKCS#11 *PROIDQCM11.DLL*, která se nachází v adresáři *C:\WINDOWS\SYSTEM32*.

4. Příprava prostředku pro generování klíčů

Před prvním použití prostředku **je nutné změnit PIN, PUK a QPIN**. Veškeré popsané činnosti se provádějí v programu **Správce karty ProID+**, který je možné otevřít například z nabídky START.

Okno programu Správce karty ProID+ je rozděleno do dvou částí. Levá část zobrazuje připojená zařízení (čipovou kartu nebo token) a objekty na připojených zařízeních (klíče, certifikáty), pravá část zobrazuje informace o vybraném zařízení či objektu, příkazy a funkce.

Před dalšími kroky je potřeba se k prostředku přihlásit tlačítkem *Přihlášení* a zadat přednastavený PIN: **12345678**

4.1. Změna PINu

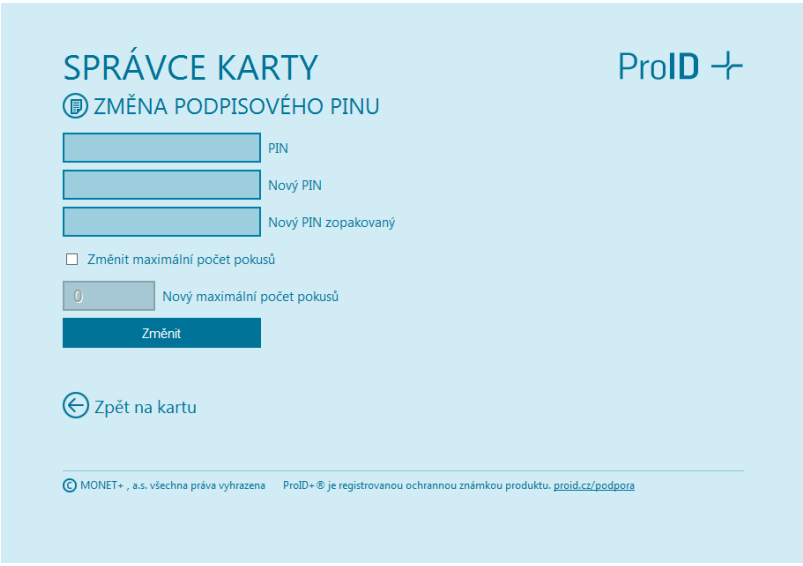
1. Ve správci karty ProID+ v levé části vybrat prostředek a v pravé části kliknout na volbu *Změna PINu*.
2. Do políčka PIN zadat: **12345678**.
3. Do políčka Nový PIN zapsat nový PIN, který musí mít **min. 4 znaky** a **maximálně 15 znaků**.
4. Do políčka Nový PIN zopakovaný, zopakovat nový PIN.
5. Změnu PINu potvrdit tlačítkem *Změnit*.

4.2. Změna PUKu

1. Ve správci karty ProID+ v levé části vybrat prostředek a v pravé části kliknout na volbu *Změna PUKu*.
2. Do políčka PUK zadat: **87654321**.
3. Do políčka Nový PUK zapsat nový PUK, který musí mít **min. 8 znaků a maximálně 15 znaků**.
4. Do políčka Nový PUK zopakovaný, zopakovat nový PUK.
5. Změnu PUKu potvrdit tlačítkem *Změnit*.

4.3. Změna podpisového PINu (QPIN)

1. Ve správci karty ProID+ kliknout na volbu *Více informací*.
2. U položky *Počet pokusů zadání podpisového PINu akt./nast. [max. nast]:* stiskněte tlačítko *(změnit)*.
3. Do políčka PIN zadat: **12345678**.
4. Do políčka Nový PIN zapsat nový PIN, který musí mít **min. 5 znaků** a **maximálně 15 znaků**.
5. Do políčka Nový PIN zopakovaný, zopakovat nový PIN.
6. Změnu PINu potvrdit tlačítkem *Změnit*.



Upozorňujeme, že při současném zablokování PIN i PUK i QPIN dojde ke znehodnocení kontaktního čipu.

4.4. Podpora klíčů o velikosti 4096 bitů

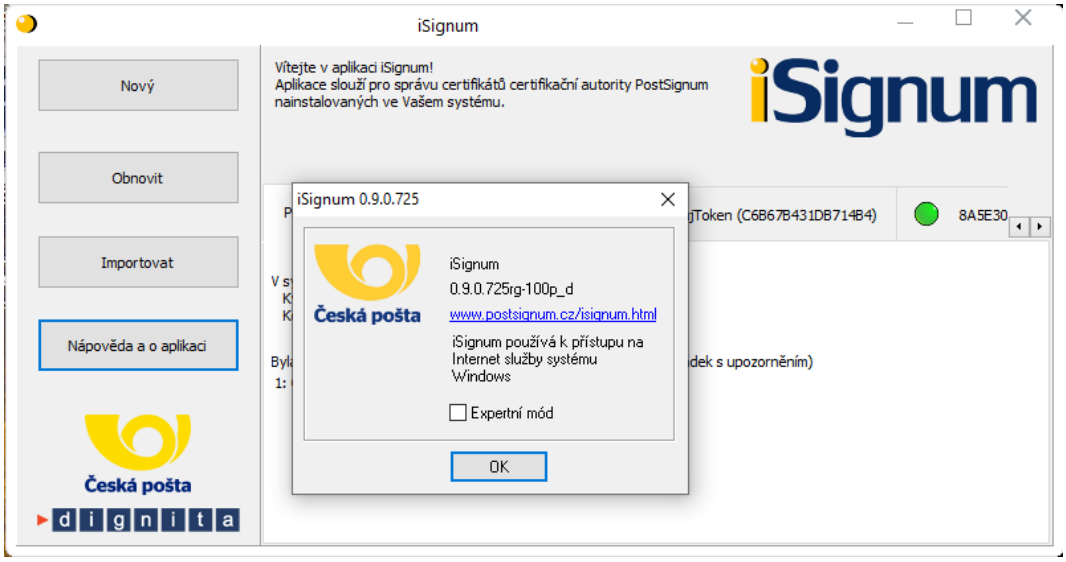
Velikost 4096 bitů není zatím u prostředků ProID+Q v aplikaci iSignum podporována.

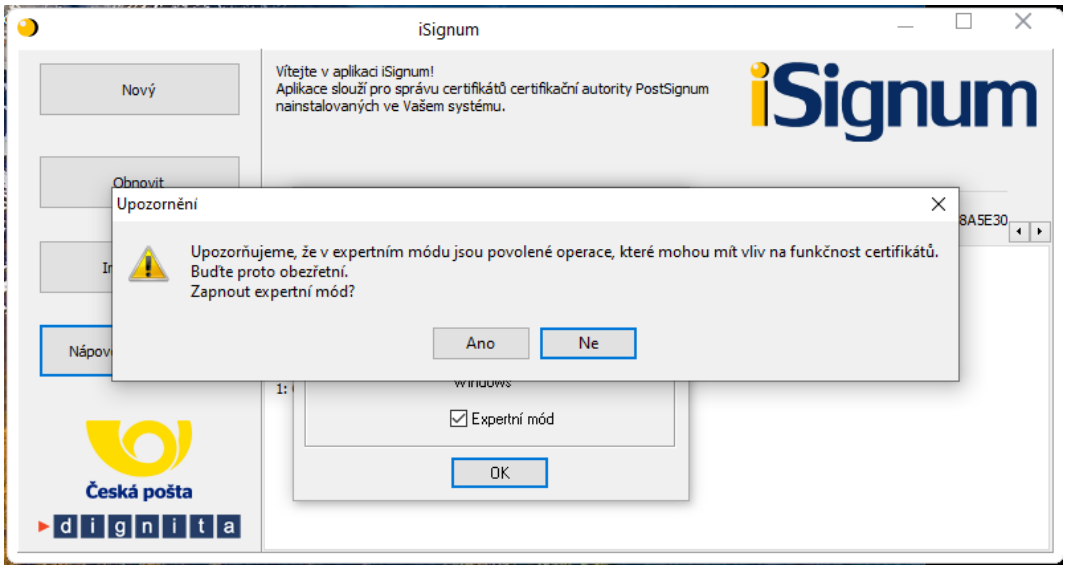
4.5. Expertní mód aplikace iSignum

Expertní mód aplikace iSignum umožňuje:

- Zvolit si velikost klíče při generování nového ID žádosti nebo v případě obnovy certifikátu. V nabídce je vždy velikost klíče 2048 bitů a pokud to vybrané úložiště umožňuje, tak i 4096 bitů.
- Možnost smazat vygenerovaný klíč z kvalifikovaného prostředku, pokud není spárovaný s vydaným certifikátem, viz kap. 7.5.2.
  POZOR! Tato operace může zapříčinit chybnou instalaci certifikátu, provádějte ji vždy s rozmyslem a až po instalaci všech vydaných certifikátů. Výmaz klíčů z prostředku může trvat až 5 minut.

Rozšíření funkcí aplikace iSignum provedete přepnutím aplikace do expertního módu stisknutím tlačítka Nápověda a o aplikaci. Expertní mód bude signalizovat červená barva horní lišty.





5. Generování žádosti o prvotní certifikát

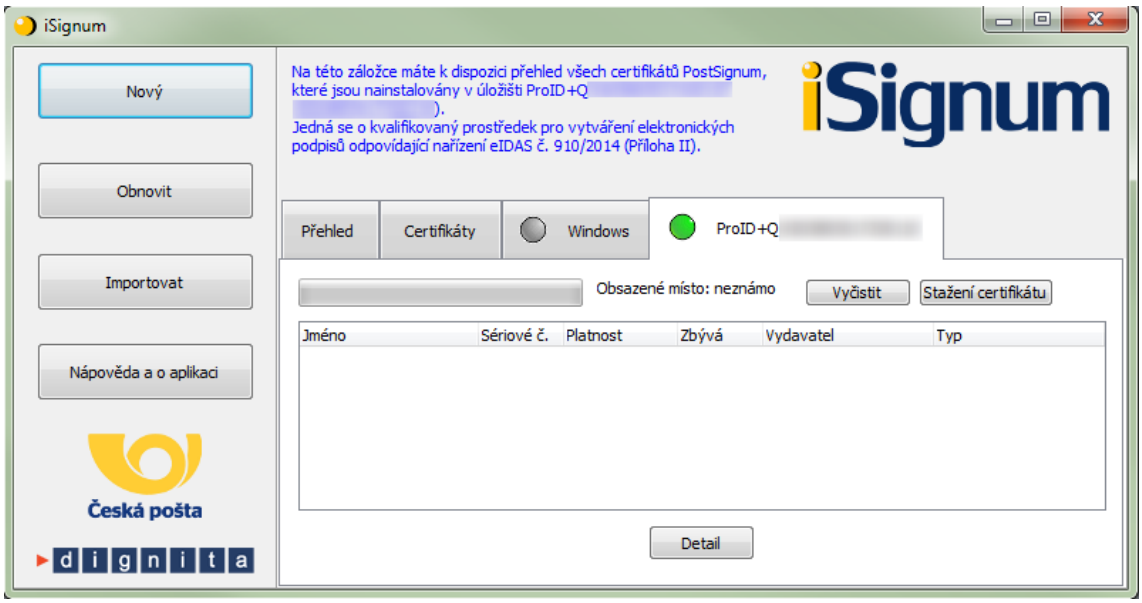
Generování klíčů na prostředek a žádosti o kvalifikovaný certifikát, který bude obsahovat příznak QESCD (kvalifikované cert.) nebo NCP+ (komerční cert.), je možné pouze v programu **iSignum**, který zajistí vytvoření správné žádosti o certifikát. Pokud bude ke generování žádosti využit jiný program, není možné do certifikátu uvedené příznaky vložit.

Program iSignum je ke stažení z webových stránek PostSignum:

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

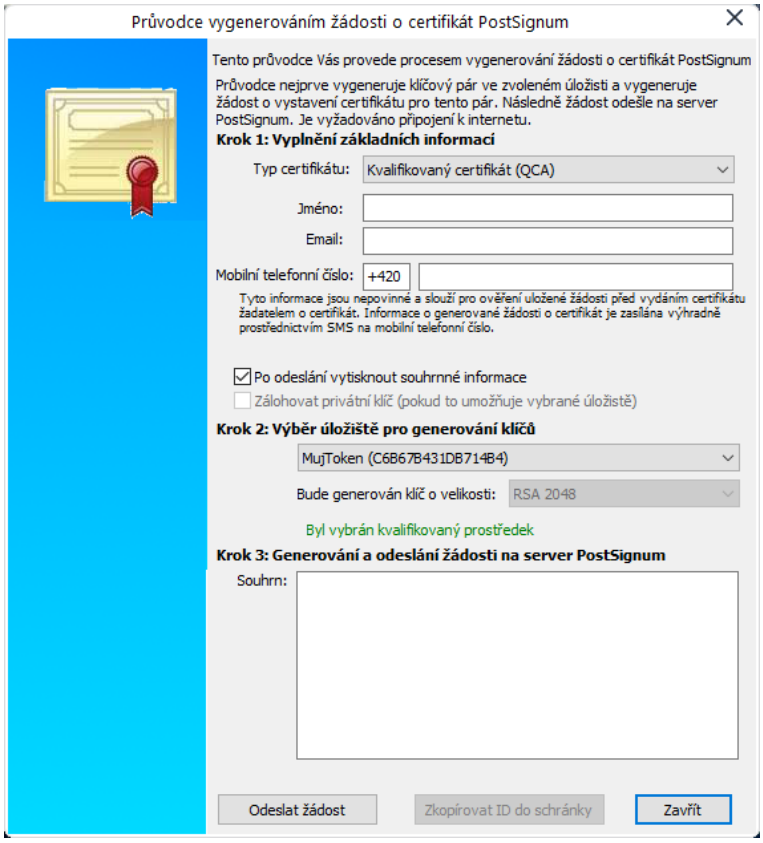
Spustit lze poklikáním na stažený soubor **iSignum.exe.**

Program iSignum rozpozná vložení prostředku, záložka s prostředkem je indikována zelenou ikonou.

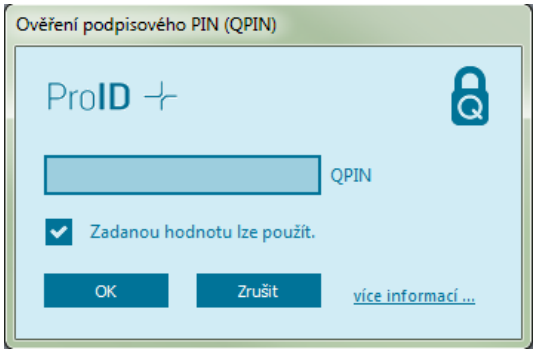


5.1. Vygenerování žádosti o certifikát

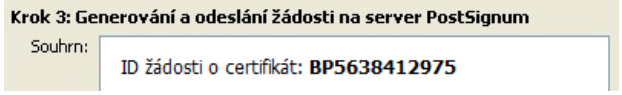
1. Připojit prostředek k PC.
2. V programu iSignum stisknout tlačítko *Nový*. Spustí se průvodce vygenerováním žádosti.
3. Úložiště pro generování klíčů bude přednastaveno na hodnotu **ProID+** a zároveň bude zobrazeno upozornění: Byl vybrán kvalifikovaný prostředek. (Zda je prostředek kvalifikovaný se můžete přesvědčit na webové stránce https://www.postsignum.cz/certifikace_prostredku.html.)
4. **Vybrat typ certifikátu**. Příznak QESCD lze vložit **pouze** do **Kvalifikovaného certifikátu (QCA)**. Pokud bude vybrán komerční certifikát, bude v certifikátu příznak NCP+.
5. Dále je možné vyplnit své jméno, e-mailovou adresu a tel. č. a stisknout tlačítko *Odeslat žádost*.
6. Před generováním klíčů a žádosti bude vyžadován PIN.



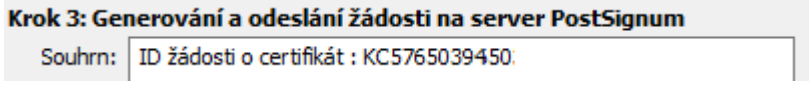
7. Po vygenerování klíčů a žádosti o certifikát bude navázána komunikace se systémem certifikační autority a dojde k bezpečnému předání žádosti o certifikát.
8. Při generování žádosti o Kvalifikovaný certifikát budete vyzváni k zadání Podpisového PINu (QPIN).



9. Pokud vše proběhne v pořádku, bude uživateli vráceno ID žádosti s prefixem **BP** (kvalifikovaný certifikát) nebo **KC** (komerční certifikát) následováno 10timístným číslem. **Na základě tohoto ID bude vystaven kvalifikovaný nebo komerční certifikát s příznakem, že byl klíč vygenerován na prostředku.**



nebo



Toto ID předložíte spolu s dalšími náležitostmi na pobočce České pošty. Postup, jak získat certifikát naleznete na webových stránkách PostSignum:

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

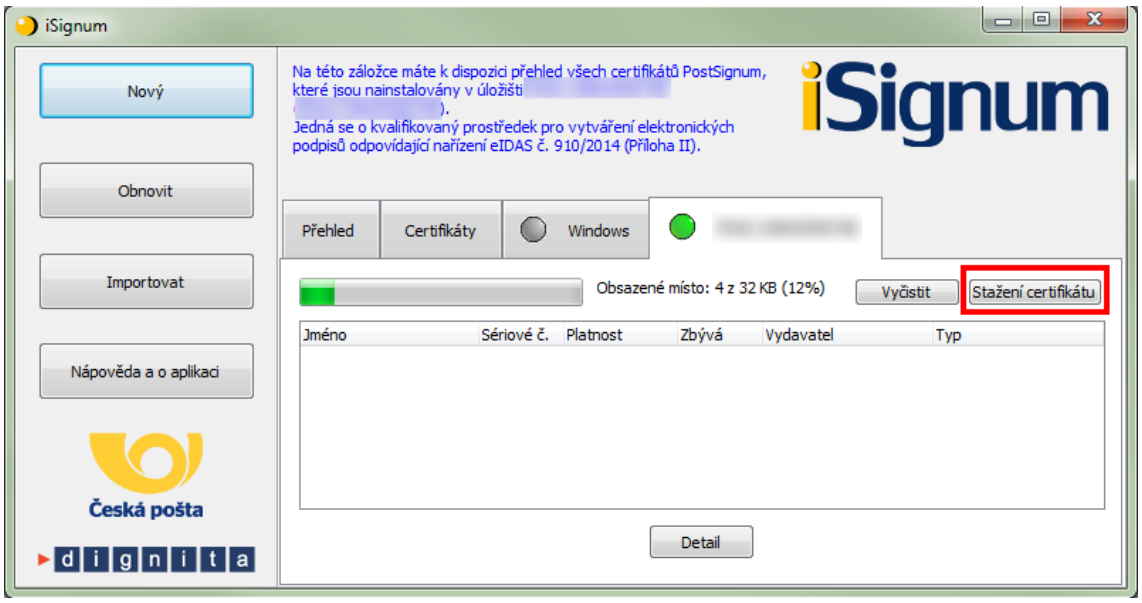
Poznámka (certifikát pro el. pečeť):
Kvalifikovaný certifikát pro elektronickou pečeť není vydáván na pobočkách České pošty. V případě žádosti o tento typ certifikátu postupujte dle pokynů na webových stránkách PostSignum:

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

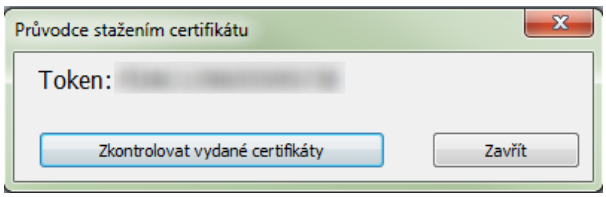
5.2. Instalace certifikátu v iSignum

Instalaci přímo do prostředku lze provést pouze v programu iSignum:

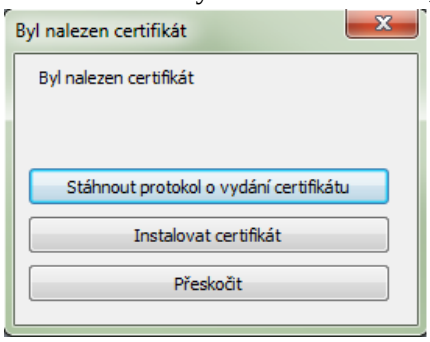
1. Vložit prostředek do USB portu počítače nebo do čtečky.
2. V programu iSignum stisknout tlačítko *Stažení certifikátu*.



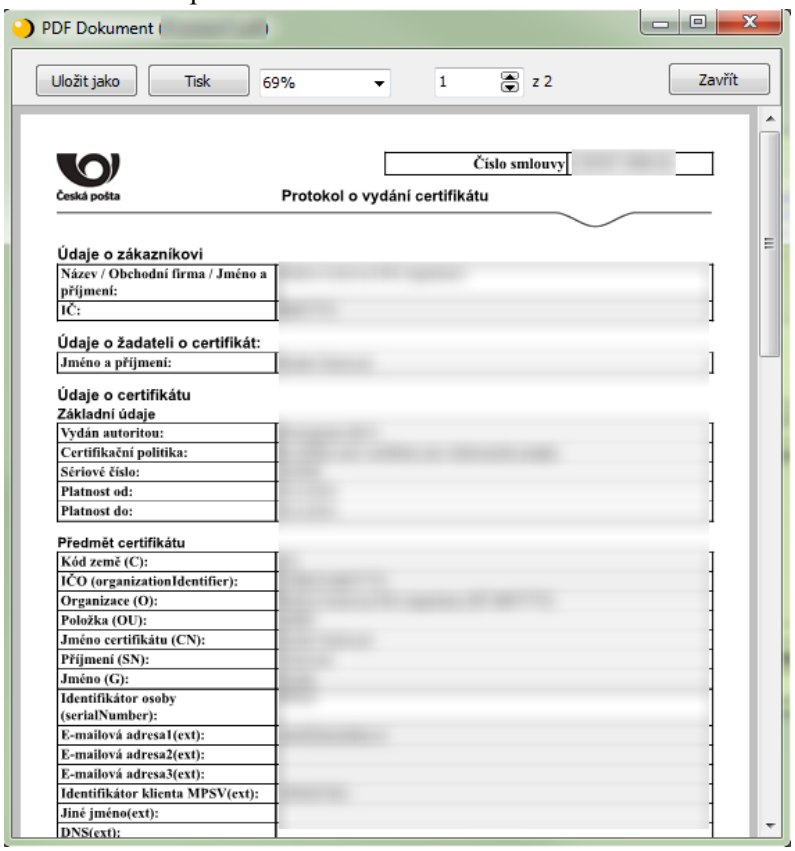
3. Stiskem tlačítka *Zkontrolovat vydané certifikáty* ověřit, zda je již certifikát připraven k instalaci.



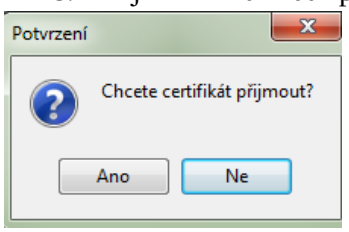
4. Pokud byl certifikát nalezen, bude zobrazeno toto okno:



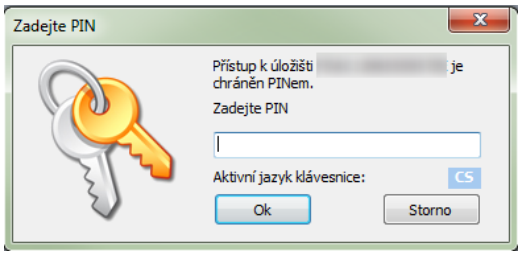
5. Dále je možné zkontrolovat údaje ve vydaném certifikátu v protokolu o vydání certifikátu, který lze stáhnout stiskem tlačítka *Stáhnout protokol o vydání certifikátu*.
6. Protokol lze uložit stiskem tlačítka *Uložit jako* nebo vytisknout tlačítkem *Tisk*.
7. Okno s protokolem lze zavřít stiskem tlačítka *Zavřít*.



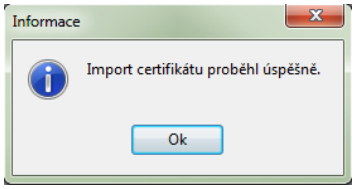
8. Přijmout certifikát - pokud jsou údaje v certifikátu v pořádku.



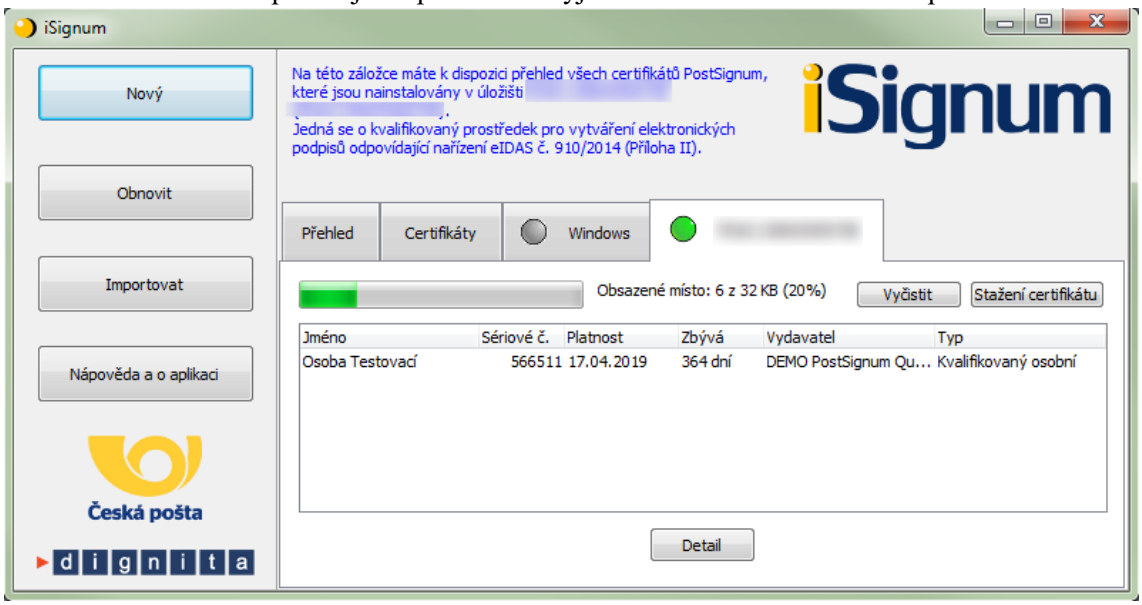
9. Zadat PIN



10. Pokud operace proběhne úspěšně, bude zobrazena hláška:



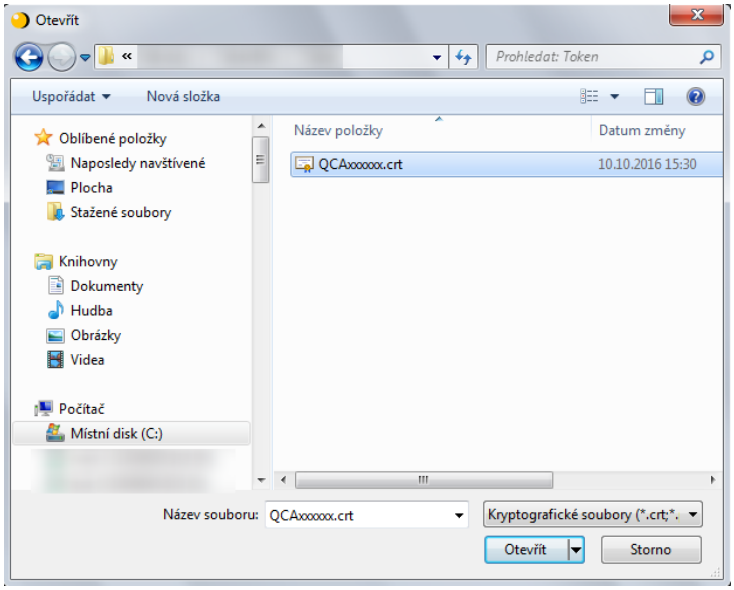
11. Po úspěšném importu bude certifikát vidět v programu iSignum na záložce **ProID+**.
12. Po instalaci doporučujeme prostředek vyjmout a znovu vložit do USB portu nebo do čtečky.



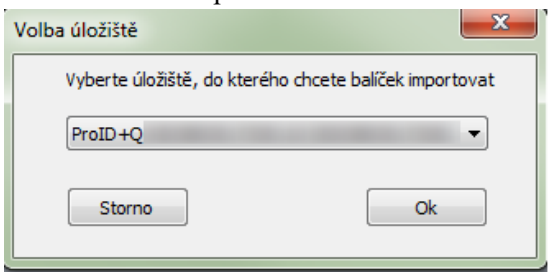
5.3. Instalace certifikátu

Instalaci certifikátu doporučujeme provést taktéž v programu iSignum:

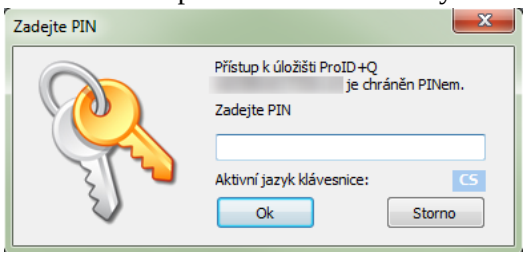
1. Připojit prostředek k PC.
2. V programu iSignum stisknout tlačítko *Importovat*.
3. Vybrat certifikát



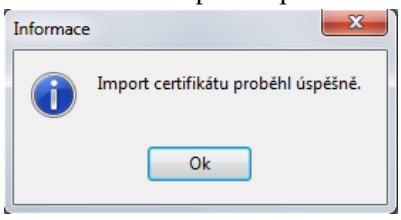
4. Ponechat přednastavené úložiště **ProID+**



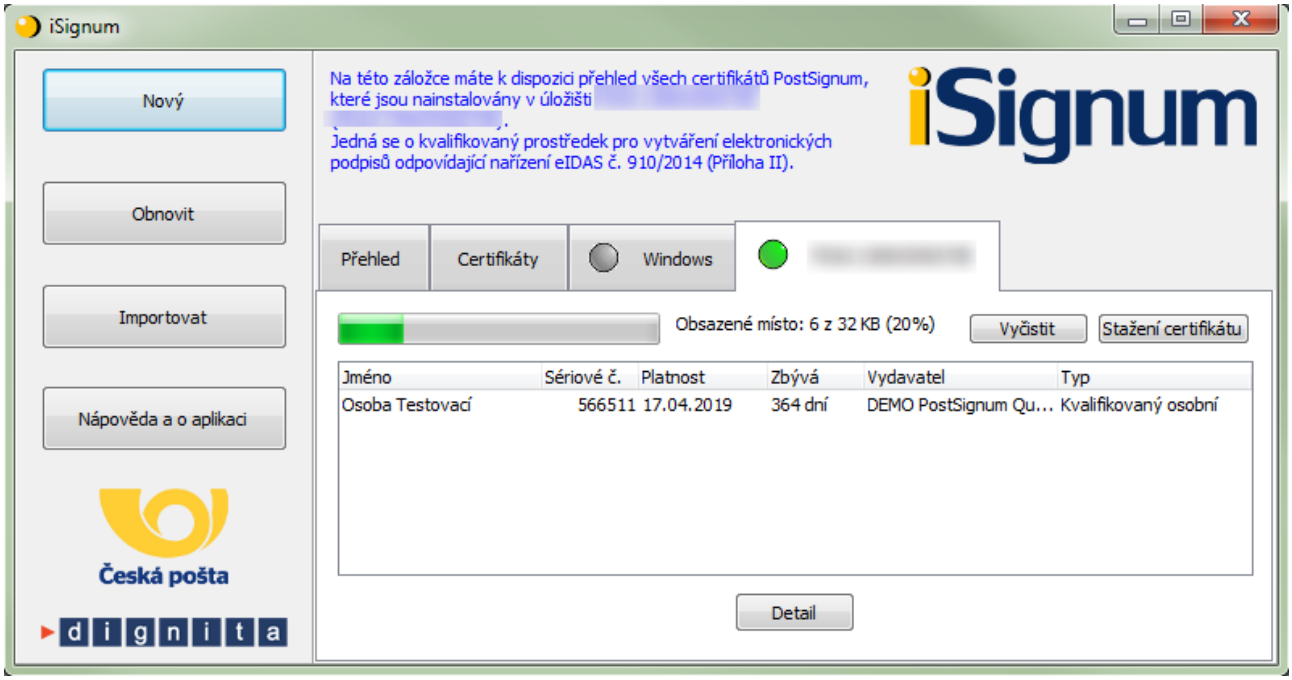
5. Pro import certifikátu bude vyžadován PIN



6. Pokud operace proběhne úspěšně, bude zobrazena hláška:



7. Po úspěšném importu bude certifikát vidět v programu iSignum na záložce **ProID+.**
8. Po instalaci doporučujeme prostředek odpojit a znovu připojit k PC.

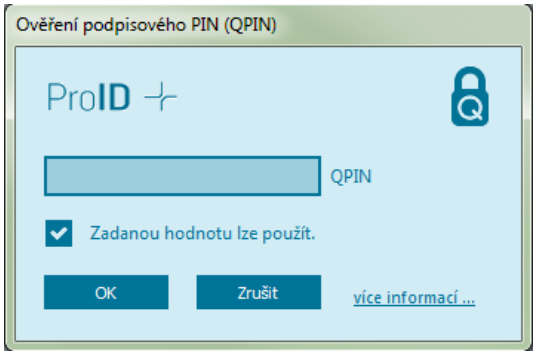

iSignum
Nový
Obnovit
Importovat
Nápověda a o aplikaci
Česká pošta
d i g n i t a
Na této záložce máte k dispozici přehled všech certifikátů PostSignum, které jsou nainstalovány v úložišti
Jedná se o kvalifikovaný prostředek pro vytváření elektronických podpisů odpovídající nařízení eIDAS č. 910/2014 (Příloha II).
iSignum
Přehled
Certifikáty
Windows
Obsazené místo: 6 z 32 KB (20%)
Vyčistit
Stažení certifikátu
Jméno
Sériové č.
Platnost
Zbývá
Vydavatel
Typ
Osoba Testovací
566511
17.04.2019
364 dní
DEMO PostSignum Qu...
Kvalifikovaný osobní
Detail

6. Generování žádosti o následný certifikát

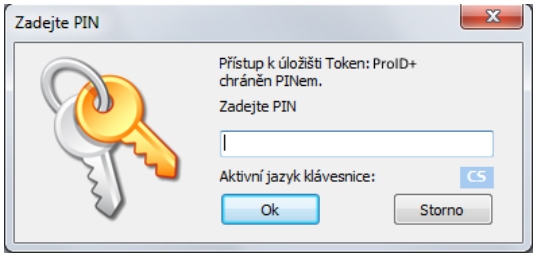
Před provedením obnovy kvalifikovaného certifikátu se přesvědčte, že je na prostředku dostatek místa pro vygenerování nového klíče. Na prostředek do CC části lze uložit maximálně dva kvalifikované certifikáty. Odstranění dat z prostředku je popsáno v kapitole 7.5

1. Připojit prostředek k PC.
2. V programu iSignum stisknout tlačítko *Obnovit*. Spustí se průvodce vygenerováním žádosti o následný certifikát.
3. Vybrat certifikát, který chcete obnovit.
4. A. Pokud je obnovovaný certifikát uložen na prostředku, tak úložiště pro generování klíčů bude přednastaveno na hodnotu **ProID+** a zároveň bude zobrazeno upozornění: Byl vybrán kvalifikovaný prostředek. (Zda je prostředek kvalifikovaný se můžete přesvědčit na webové stránce https://www.postsignum.cz/certifikace_prostredku.html.)
4. B. Pokud obnovovaný certifikát není uložen na prostředku, je nutné vybrat úložiště pro generování klíčů ručně na hodnotu **ProID+**, aby byl obnovený certifikát uložen na prostředku.
5. Stisknout tlačítko *Odeslat žádost* případně *Odeslat žádost o víceletý certifikát.*

6. Při generování žádosti o Kvalifikovaný certifikát budete vyzváni k zadání Podpisového PINu (QPIN).



7. Před generováním klíčů a žádosti bude vyžadován PIN.



8. Po vygenerování klíčů a žádosti o certifikát bude navázána komunikace se systémem certifikační autority a dojde k bezpečnému předání žádosti o certifikát. Při zpracování žádosti o následný certifikát je navíc provedena kontrola vazby *prostředku-žadatel*.
9. Pokud vše proběhne v pořádku, bude žádost o následný certifikát zařazena do systému PostSignum ke zpracování. O vydaném certifikátu budete informováni e-mailem, který bude odeslán na e-mailovou adresu uvedenou v certifikátu.
10. Instalace následného certifikátu probíhá totožným způsobem jako instalace prvotního certifikátu, viz kapitola 5.2.

Poznámka (certifikát pro el. pečeť):
Vygenerování žádosti o obnovu kvalifikovaného certifikátu pro elektronickou pečeť probíhá stejně jako generování žádosti o prvotní certifikát, viz kapitola *Generování žádosti o prvotní certifikát*, následný postup žádosti o obnovu certifikátu je popsán na webových stránkách PostSignum:

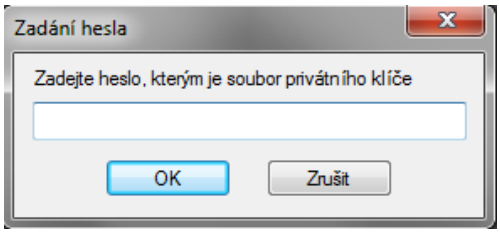
https://www.postsignum.cz/obnova_certifikatu.html

7. Další funkce Správce karty ProID+

7.1. Import certifikátu z PKCS#12

Vložení certifikátů ze zálohy (PFX nebo P12) do prostředku se provede kliknutím na tlačítko Import klíče.

1. Vybrat soubor se zálohou, kde je uložený certifikát ve formátu .pfx či .p12.
2. Zadat heslo k záloze certifikátu.
3. Potvrdit OK.



Po úspěšném vložení certifikátu se zobrazí v horní části programu vybraný certifikát.

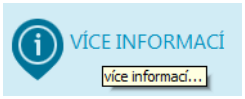
Upozorňujeme, že takto importovaný kvalifikovaný certifikát nebude považován za kvalifikovaný certifikát uložený na bezpečném prostředku QESCD a nebude obsahovat příznak QESCD. Totéž platí i v případě importovaného komerčního certifikátu a příznaku NCP+.

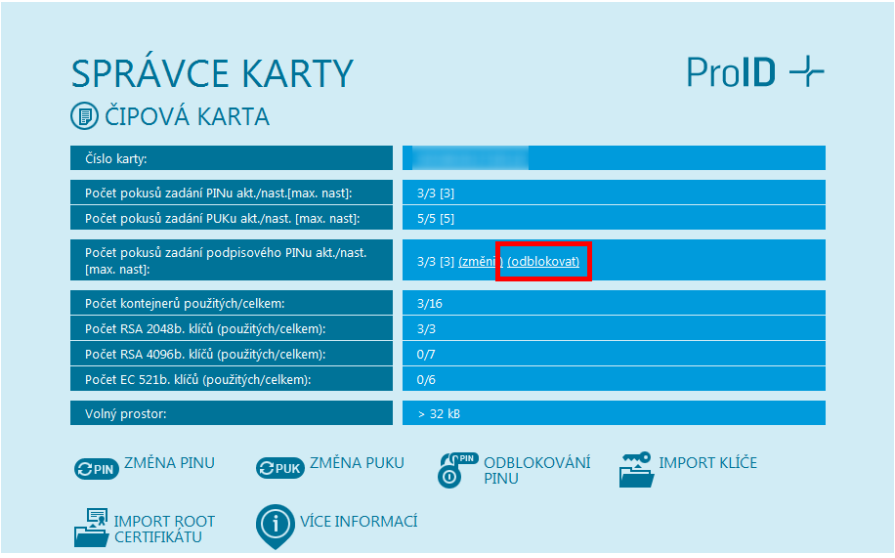
7.2. Export do souboru

Dle typu objektu vyexportuje samotný certifikát nebo veřejný klíč z prostředku do souboru.

7.3. Odblokování PINu a QPINu

Pokud je prostředek zablokován po vícenásobném špatném zadání PINu nebo QPINu, je možné ji touto volbou odblokovat. Pro odblokování je potřeba znát PUK. Po zadání PUKu je rovněž potřeba zadat nový PIN nebo QPIN.

V případě odblokování QPINu je nutné kliknout na tlačítko Více informací  a dále na odblokovat dle obrázku:



Zadat PUK a nový QPIN a stisknout Odblokovat.

Upozorňujeme, že při zablokování PIN i PUK i QPIN dojde ke znehodnocení kontaktního čipu.

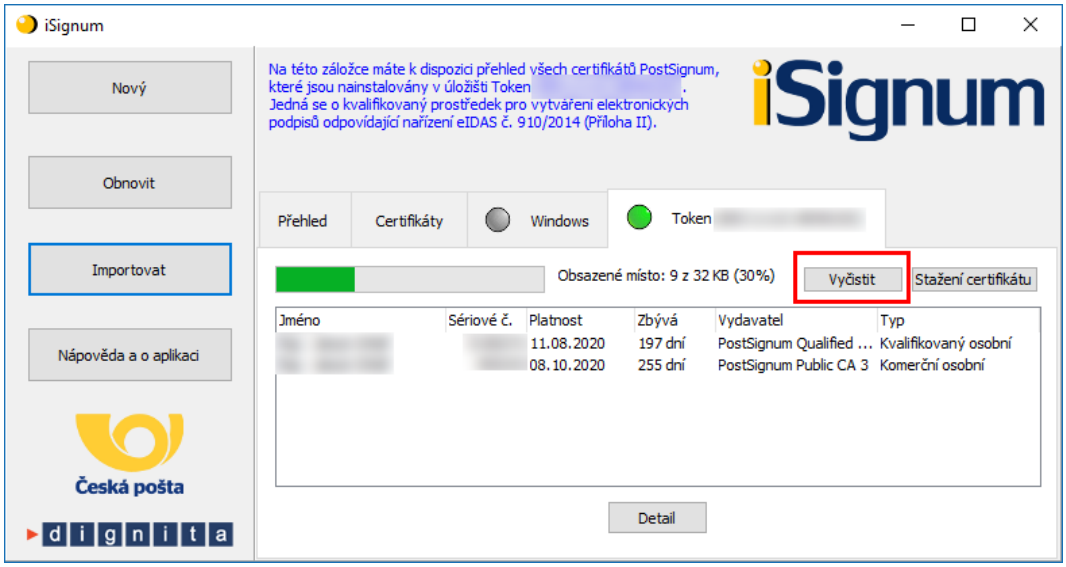
7.4. Registrace certifikátů

Dojde k registraci certifikátu uložených na prostředku do systémového úložiště certifikátů Windows, aby je bylo možné používat v programech, které využívají systémové úložiště. Registrace probíhá automaticky, takže není potřeba tuto volbu používat.

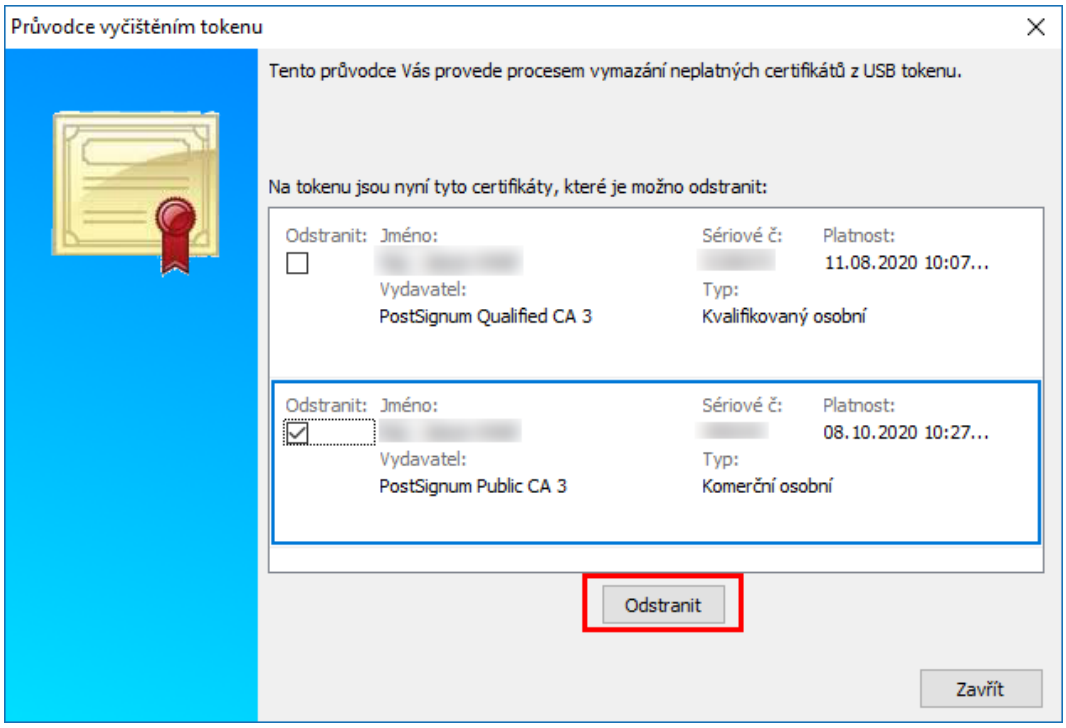
7.5. Odstranění dat

7.5.1. Odstranění certifikátu

Při obnově certifikátu může dojít k chybě 622. Tato chyba může znamenat, že na prostředku, v zabezpečené CC části, již není místo pro další certifikát (do CC části lze uložit maximálně dva certifikáty). Spusťte program iSignum, vyberte záložku s prostředkem a stiskněte tlačítko **Vyčistit**.



Vyberte certifikát, který chcete odstranit a stiskněte tlačítko **Odstranit**.



Pokud se na tokenu již nenachází žádný certifikát k odstranění a chyba 622 přetrvává, můžete zkusit odstranit nepřiřazené klíče, viz následující kapitola.

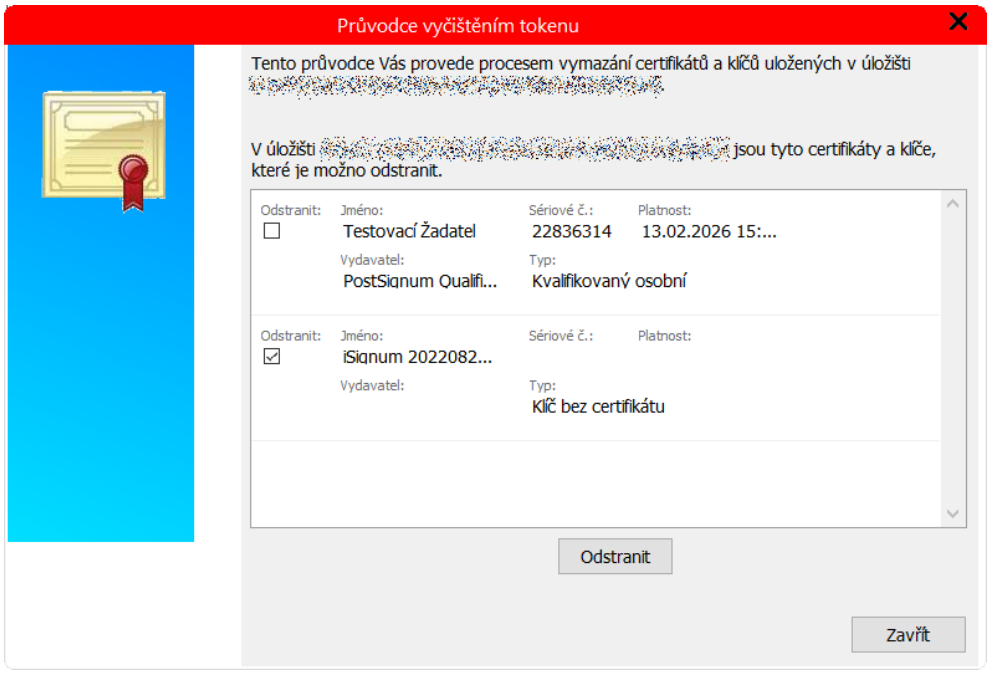
7.5.2. Odstranění klíče

Chyba 622 může být rovněž způsobena tím, že na prostředku jsou uloženy klíče, které nebyly spárovány s certifikátem. Tyto klíče lze odstranit v programu iSignum v expertním módu (přepnutí do tohoto módu viz kapitola 4.5).

POZOR! Tato operace může zapříčinit chybnou instalaci certifikátu, provádějte ji vždy s rozmyslem a až po instalaci všech vydaných certifikátů.

Pro vyčištění stiskněte tlačítko **Vyčistit**.

Nepřiřazené klíče budou označené jako *Klíč bez certifikátu*. Tyto klíče můžete označit k odstranění a stisknout tlačítko **Odstranit**.



Následně budete vyzváni k potvrzení operace a k zadání PINu k tokenu.

Upozorňujeme, že odstranění klíčů může trvat až 5 minut.

8. Předání prostředku jiné osobě

Při vydání prvního certifikátu, jehož soukromý klíč je na prostředku, dochází k vytvoření vazby **osoba-bezpečný prostředek** která je evidována v systému certifikační autority a kontrolována při vydávání dalších (následných) certifikátů do zařízení.

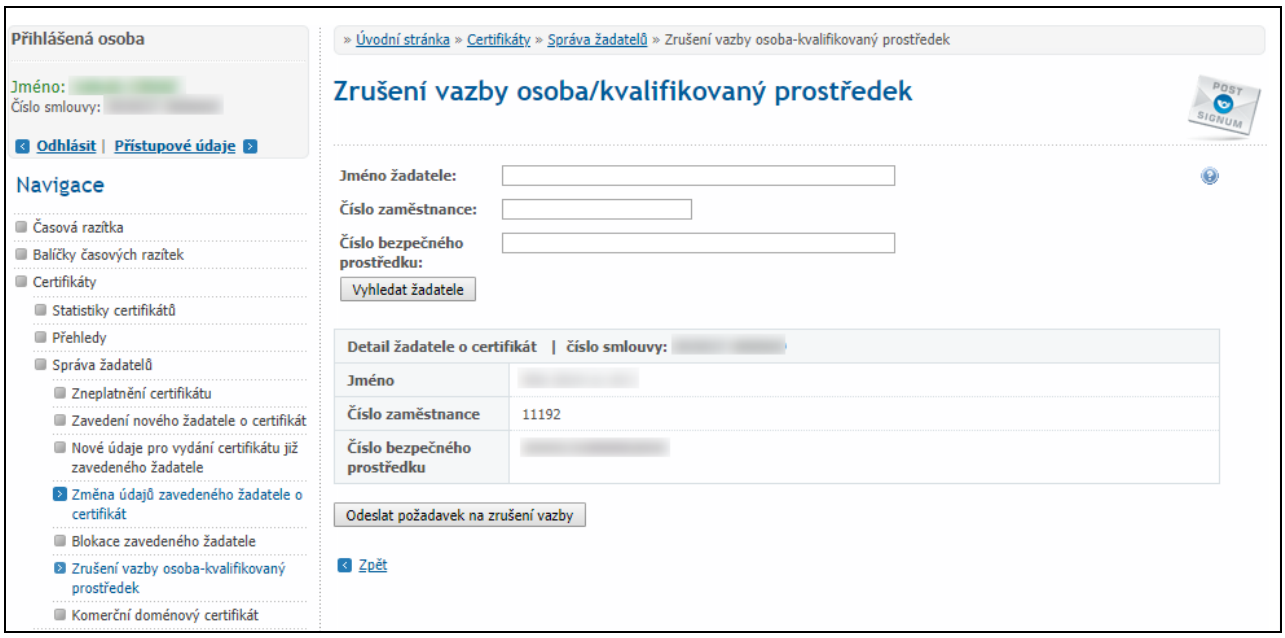
Pokud je nutné tuto vazbu změnit (např. z důvodu předání prostředku jinému žadateli), je nutné postupovat následovně:

1. Zneplatnit certifikáty původního žadatele uložené na prostředku.
2. Provést zrušení vazby **osoba-bezpečný prostředek,** to lze provést dvěma způsoby.

a. Pověřená osoba v Zákaznickém portálu PostSignum v sekci **Certifikáty → Správa žadatelů → Zrušení vazby osoba-bezpečný prostředek** provede zrušení vazby.

Vyplňte jeden z údajů a stiskněte tlačítko **Vyhledat žadatele**. Následně bude zobrazen výsledek vyhledávání.

Pokud byly všechny certifikáty původního žadatele uložené na prostředku zneplatněny, zobrazí se tlačítko **Odeslat požadavek na zrušení vazby**.



Po stisku tlačítka se zobrazí: **Požadavek na zrušení vazby byl úspěšně odeslán.**

b. V případě, že nemá zákazník zřízen přístup do Zákaznického portálu, nebo se jedná o nepodnikající fyzickou osobu, je nutné oznámit zrušení vazby **osoba-bezpečný prostředek** certifikační autoritě elektronicky podepsaným e-mailem (elektronický podpis musí být založený na osobním certifikátu PostSignum)

   Před odesláním e-mailu se ujistěte, že jsou zneplatněny certifikáty žadatele, kterému má být vazba zrušena.

Vzor e-mailu:

Adresát: certifikaty.postsignum@cpost.cz

Předmět: Zrušení vazby osoba-bezpečný prostředek

Tělo: Oznamuji zrušení vazby osoba-bezpečný prostředek.
Jméno osoby: xxx
Sériová čísla certifikátů uložených na prostředku: xxx (nebo výrobní číslo prostředku):

9. Reklamace

V případě reklamace je nutné provést níže uvedené kroky:

1. **Vymazat z prostředku veškeré uživatelské certifikáty, aby nemohlo dojít k jejich zneužití.**
2. **Nastavit na prostředku tovární hodnoty PIN, PUK a QPIN**, **aby bylo možné se k prostředku přihlásit.**

   PIN: 12345678

   PUK: 87654321

   QPIN: 12345678

3. Prostředek spolu s reklamačním listem (ke stažení na webových stránkách PostShopu České pošty – www.postshop.cz) zaslat na adresu:

   Česká pošta, s.p.
   Postshop ČP
   Ortenovo nám. 542/16
   211 11 Praha 7

Pokud nebudou provedeny kroky 1 a 2, nebude možné prostředek ověřit a karta bude vrácena zákazníkovi.