Česká pošta

Identifikace		**Číslo jednací**	
Nahrazuje		**Klasifikace**	veřejné
Platnost	22. 10. 2021	**Účinnost**	22. 10. 2021

Uživatelská příručka

TokenME
TokenME EVO
Crypto Java Card

Verze 3.2

Obsah dokumentu

Evidence revizí a změn

Verze	Datum revize	Důvod a popis změny	Autor	Schválil
0.91	11. 10. 2016		Česká pošta	
1.0	11. 11. 2016	úprava manuálu dle nového middlewaru	Česká pošta	Manažer CA
1.1	23. 6. 2017	doplněn nový vzhled tokenu	Česká pošta	Manažer CA
2.0	9. 4. 2018	manuál změněn na univerzální pro token i čipovou kartu	Česká pošta	Manažer CA
2.1	1. 12. 2019	změna postupu rušení vazby prostředku na osobu	Česká pošta, s.p.	Manažer CA
2.2	28. 1. 2020	přidán postup na výmaz klíčů a certifikátů	Česká pošta, s.p.	Manažer CA
3.0	2. 4. 2020	přidán nový typ tokenu a postup pro získání certifikátu pro el. pečeť	Česká pošta, s.p.	Manažer CA
3.1	23. 7. 2021	přidán nový typ tokenu	Česká pošta, s.p.	Manažer CA
3.2	22. 10. 2021	sjednoceny verze TokenME EVO x pod společný název Token ME EVO	Česká pošta, s.p.	Manažer CA

1. Přehled

Zařízení USB token TokenME, TokenME EVO nebo čipová karta Crypto Java Card (dále jen prostředky) jsou zařízení, které **byly schválené jako kvalifikovaný prostředek pro vytváření elektronických podpisů** (všechny uvedené typy) **a pro vytváření elektronických pečetí** (pouze TokenME EVO) **v souladu s nařízením eIDAS.**

Prostředky jsou personalizovány již z výroby, tzn., je na nich přednastaven PIN (12345678) a PUK (87654321)**.**

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

Upozorňujeme, že při zablokování PIN i PUK dojde ke znehodnocení prostředku.

Před dodáním prostředku zákazníkovi je v prostředí České pošty provedena příprava prostředku pro bezpečné a průkazné předávání žádostí o certifikát. Příprava spočívá ve vygenerování páru klíčů, tzv. „servisní klíč“, v prostředku označen „**SERVICE KEY**“. Tento klíč se používá k zabezpečení komunikace mezi prostředkem a systémem certifikační autority**. Je nutné dbát na to, aby nedošlo ke smazání tohoto klíče z prostředku. Pokud dojde k výmazu servisního klíče, nebude možné vytvořit žádost o certifikát pomocí aplikace iSignum.**

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.

Poznámka (certifikát pro el. pečeť):
V případě kvalifikovaných certifikátů pro elektronickou pečeť se vazba **karta-žadatel** nevytváří.

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

TokenME

TokenME EVO

Crypto Java Card

2. Co potřebuji?

1. PC s operačním systémem Windows

2. USB token TokenME nebo čipovou kartu Crypto Java Card

3. Software

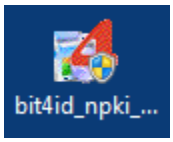
Software je ke stažení na webových stránkách PostSignum:
https://www.postsignum.cz/tokenme

4. V případě čipové karty také 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.

3. Instalace softwaru

Ke správné instalaci softwaru je potřeba vykonat následující kroky:

1. Otevřít aplikaci bit4id_xpki_admin.msi



2. Povolit, aby následující program Bit4id provedl změny ve Vašem PC
3. Odsouhlasit instalaci programu Bit4id Universal Middleware Setup Wizard kliknutím na tlačítko *Next*
4. Akceptovat licenční podmínky zaškrtnutím políčka „I accept the terms of the License Agreement“ a pokračovat kliknutím na tlačítko *Install*
5. Potvrdit dokončení instalace kliknutím na tlačítko *Close*
6. Zasunout prostředek do PC. V tento okamžik je již software plně nainstalován a prostředek se již může zasunout do PC, případně čtečky pro další práci s prostředkem.
7. Po zasunutí prostředku do PC, začne token nebo čtečka blikat a objeví se informativní hláška, že software ovladače byl úspěšně naistalován.

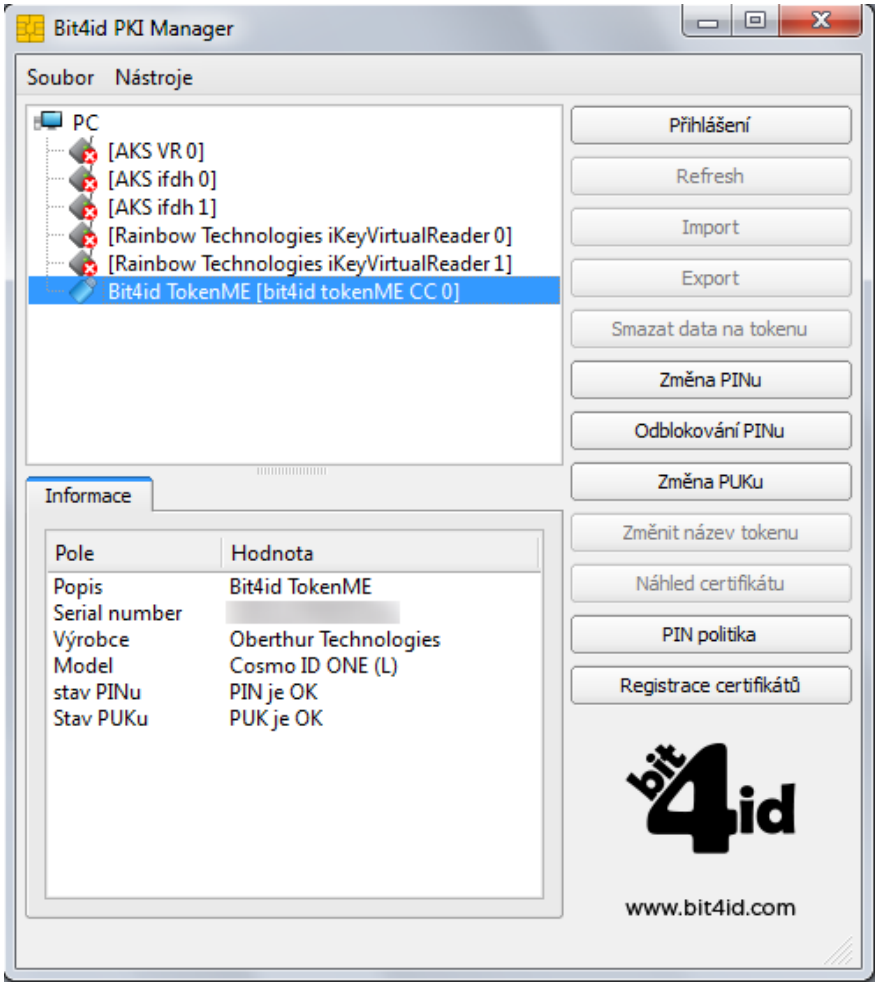
Knihovna PKCS#11

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 *BIT4XPKI.DLL*, která se nachází v adresáři *C:\WINDOWS\SYSTEM32*.

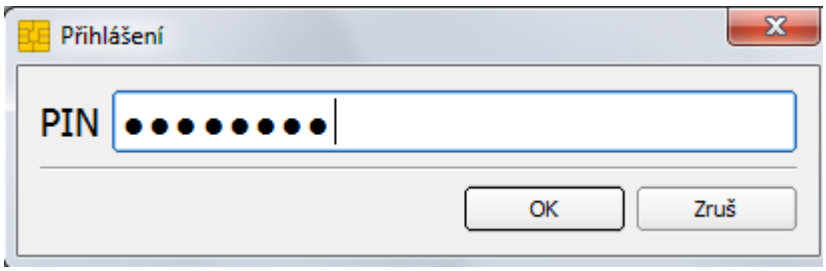
4. Příprava prostředku pro generování klíčů

Před prvním použití prostředku **je nutné změnit PIN a PUK** a přesvědčit se, zda je na prostředku přítomen „servisní klíč“. Veškeré popsané činnosti se provádějí v programu **Bit4id PKI Manager**, který je možné otevřít například z nabídky START.

Okno programu Bit4id PKI Manager je rozděleno do tří částí. Horní část zobrazuje připojené prostředky a objekty na prostředku (klíče, certifikáty), spodní část zobrazuje informace o vybraném prostředku či objektu a pravá část zobrazuje příkazy a funkce.

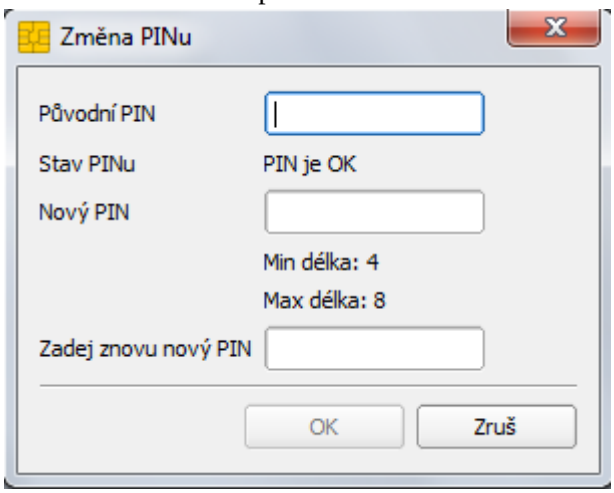


Před dalšími kroky je potřeba se k prostředku přihlásit tlačítkem *Přihlášení* a zadat přednastavený PIN: **12345678**



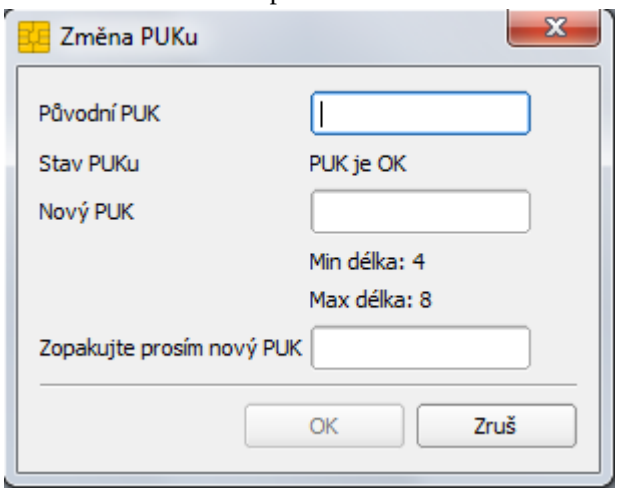
4.1. Změna PINu

1. V PKI Manageru kliknout na volbu *Změna PINu*.
2. Do políčka Původní PIN zadat: **12345678**.
3. Do políčka Nový PIN zapsat nový PIN, který musí mít **min. 4 znaky** a **maximálně 8 znaků**.
4. Do políčka Zadej znovu nový PIN zopakovat nový PIN.
5. Změnu PINu potvrdit tlačítkem OK.



4.2. Změna PUKu

1. V PKI Manageru kliknout na volbu *Změna PUKu*.
2. Do políčka Původní PUK zadat: **87654321**.
3. Do políčka Nový PUK zapsat nový PUK, který musí mít min. 4 znaky a maximálně 8 znaků.
4. Do políčka Zopakujte prosím nový PUK zopakovat nový PUK.
5. Změnu PUKu potvrdit tlačítkem OK.



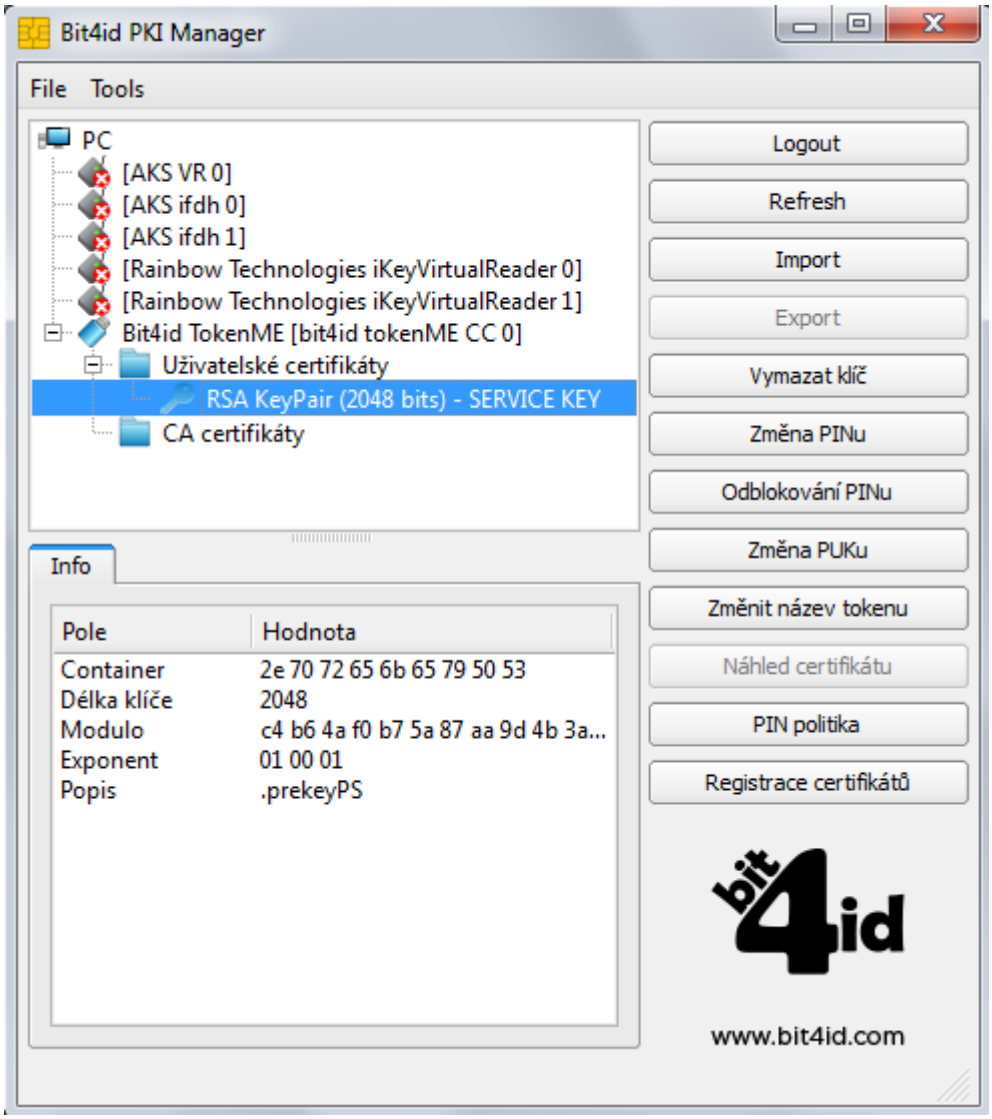
Upozorňujeme, že při zablokování PIN i PUK dojde ke znehodnocení prostředku.

4.3. Kontrola servisního klíče

Servisní klíč je nutný pro zajištění identifikace prostředku v systému certifikační autority a využívá se pro zabezpečení komunikace při předávání žádosti o certifikát. Pokud servisní klíč na prostředku není přítomen, není možné prostředek použít pro vytvoření žádosti o certifikát.

1. V PKI Manageru kliknout v horním okně na znaménko + u položky *Uživatelské certifikáty*.

V seznamu by měl být pouze jeden pár klíčů s označením SERVICE KEY, viz obrázek:



Pokud tento klíč v seznamu chybí, je nutné postupovat dle kapitoly 8.1

5. Generování žádosti o prvotní certifikát

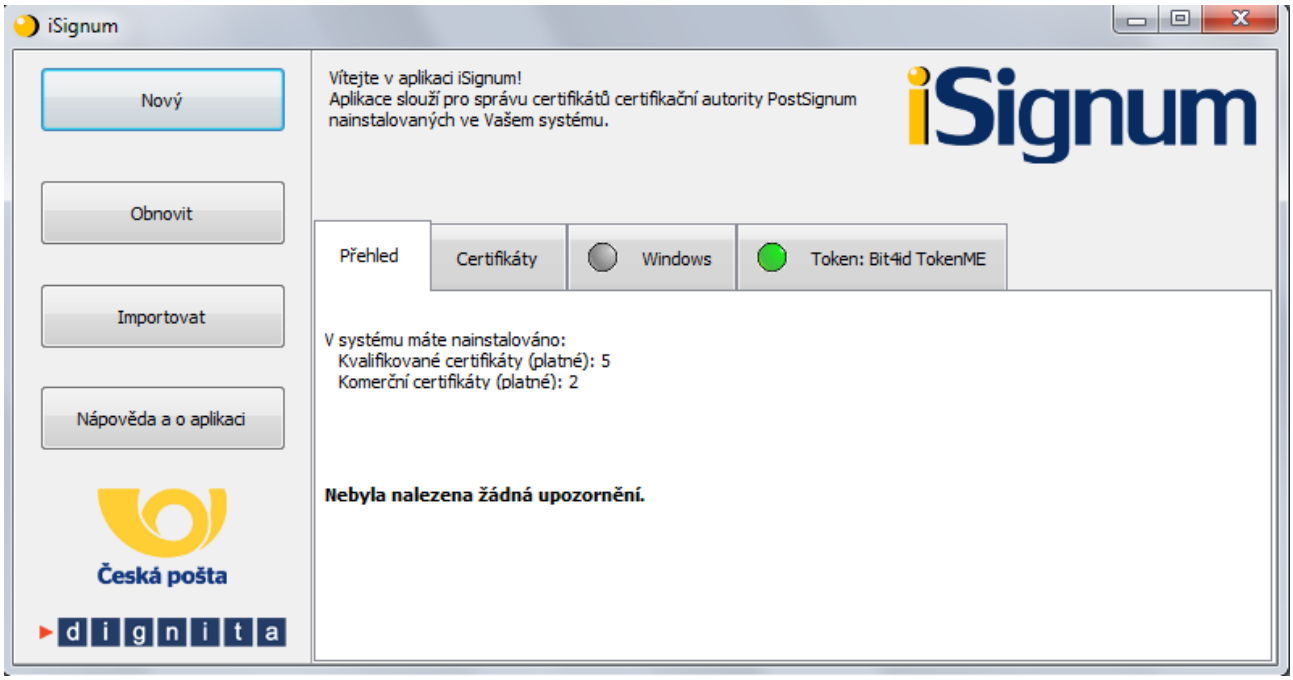
Generování klíčů na prostředek a žádosti o kvalifikovaný certifikát, který bude obsahovat příznak QESCD, je možné pouze v programu **iSignum**, který zajistí vytvoření správné žádosti o certifikát. Pokud bude ke generování žádosti využit jiný program, není možné do certifikátu příznak QESCD vložit.

Program iSignum je ke stažení z webových stránek PostSignum:

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

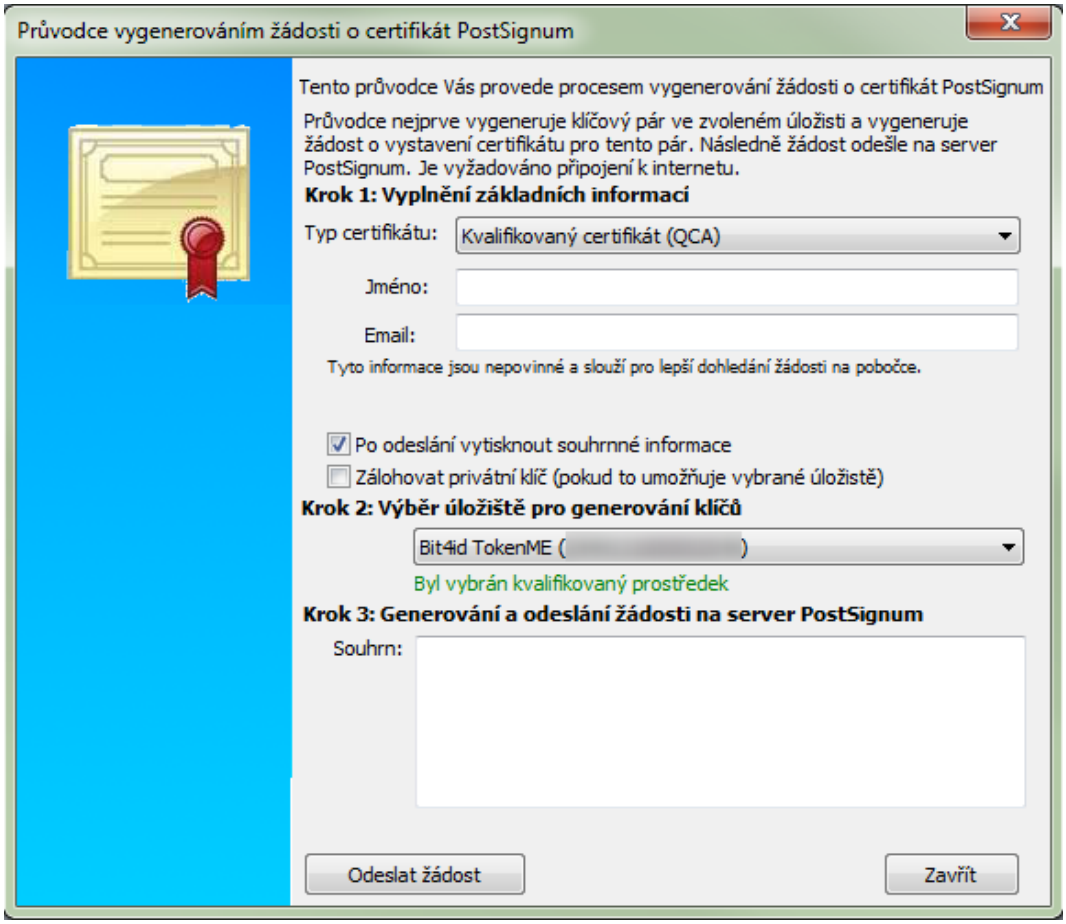
Spustit lze poklikáním na stažený soubor **iSignum.exe.**

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

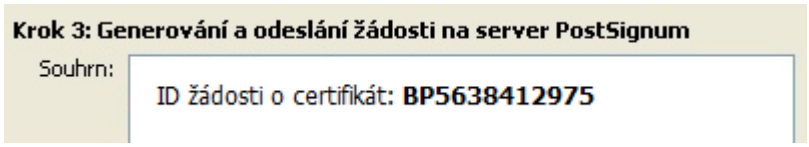


5.1. Vygenerování žádosti o certifikát

1. Vložit prostředek do USB portu počítače nebo do čtečky.
2. V programu iSignum stisknout tlačítko *Nový*. Spustí se průvodce vygenerováním žádosti.
3. Úložiště pro generování klíčů bude přednastaveno na hodnotu **TokenME** a zároveň bude zobrazeno upozornění: Byl vybrán kvalifikovaný prostředek.
4. **Vybrat typ certifikátu**. Příznak QESCD lze vložit **pouze** do **Kvalifikovaného certifikátu (QCA)**.
5. Dále je nutné vyplnit své jméno a e-mailovou adresu 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 za pomoci servisního klíče dojde k autentizaci prostředku do systému a bezpečnému předání žádosti o certifikát.
8. Pokud vše proběhne v pořádku, bude uživateli vráceno ID žádosti s prefixem **BP** následováno 10timístným číslem. **Na základě tohoto ID bude vystaven kvalifikovaný certifikát s příznakem, že byl klíč vygenerován na kvalifikovaném prostředku QESCD.**



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

http://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:

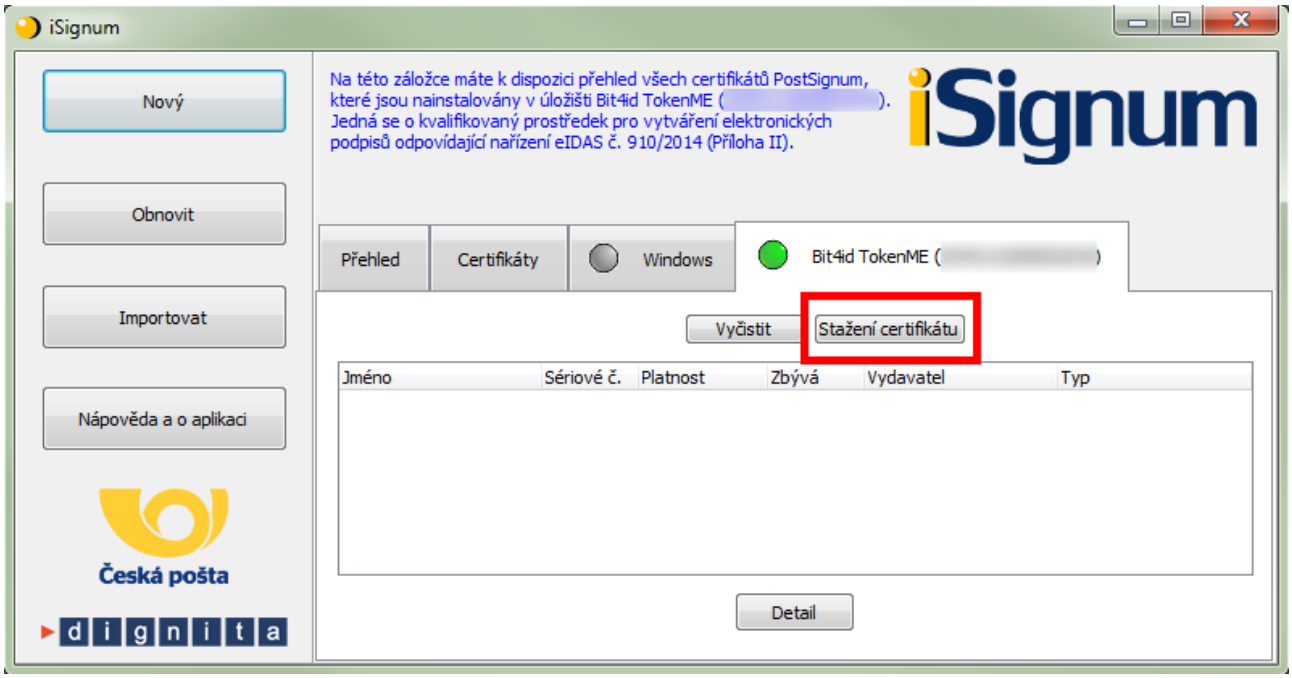
http://www.postsignum.cz/vydani_prvotniho_certifikatu_pro_elektronickou_pecet.html

Platí pouze pro TokenME EVO

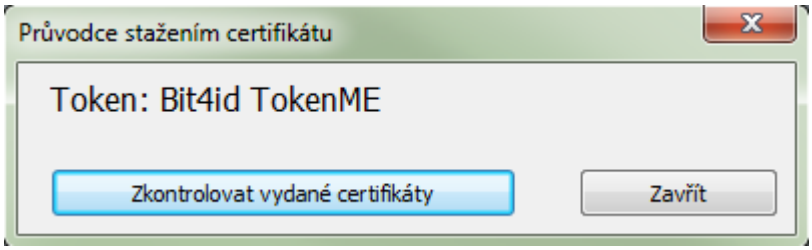
5.2. Instalace certifikátu v iSignum

Instalaci přímo do prostředku lze provést pouze v programu iSignum:

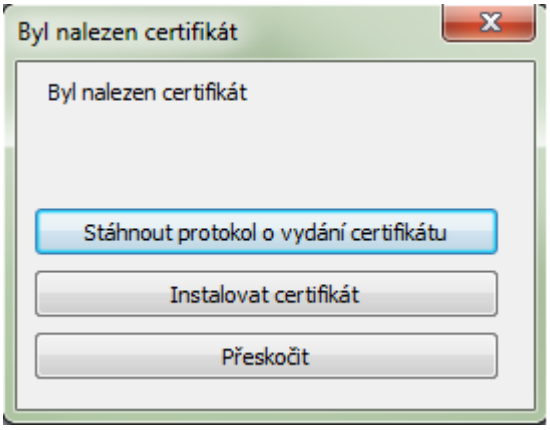
1. Vložit prostředek do USB portu počítače nebo do čtečky.
2. V programu iSignum stisknout tlačítko *Stažení certifikátu*.



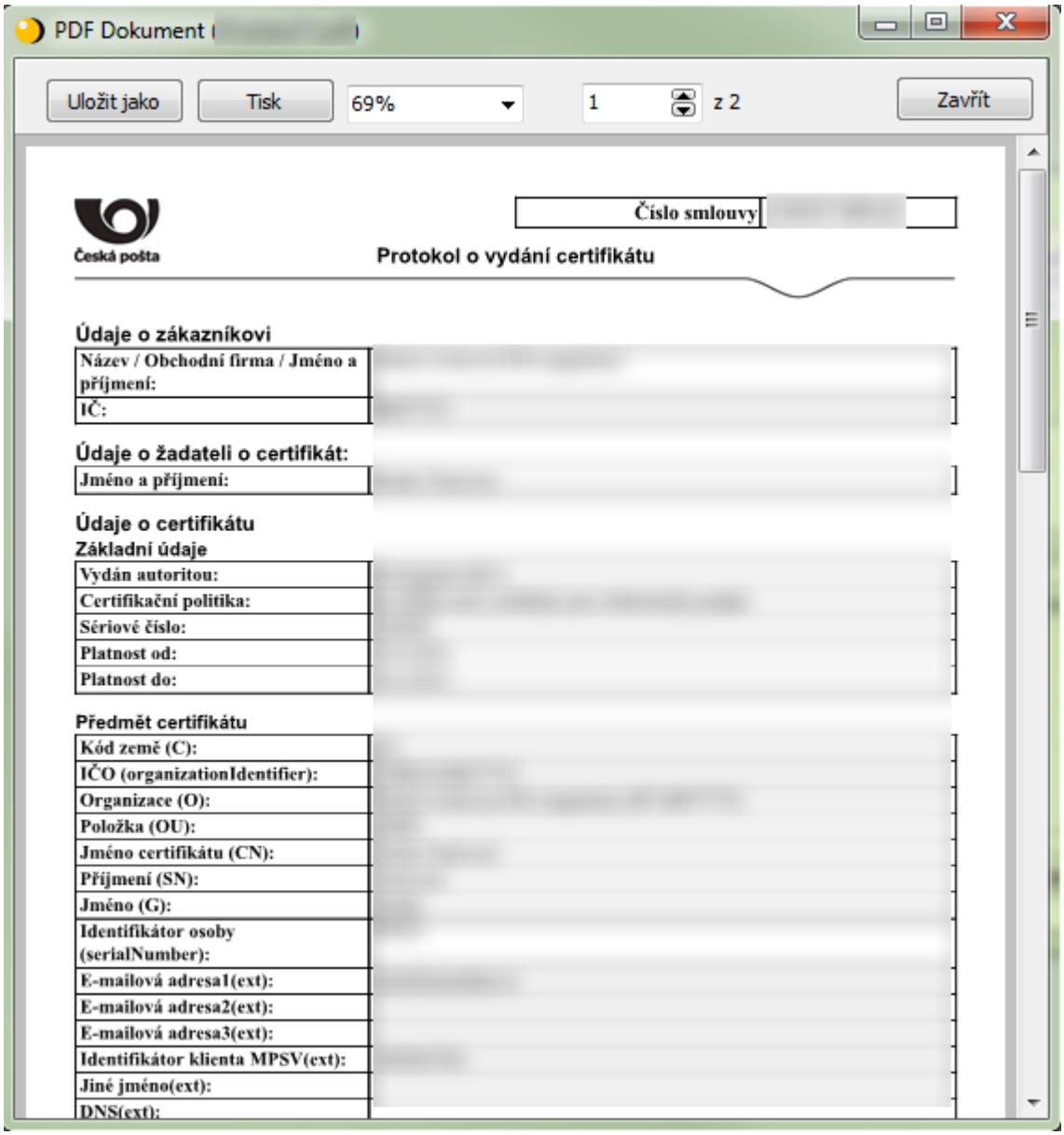
3. Stiskem tlačítka *Zkontrolovat vydané certifikáty* ověřit, zda je již certifikát připraven k instalaci.



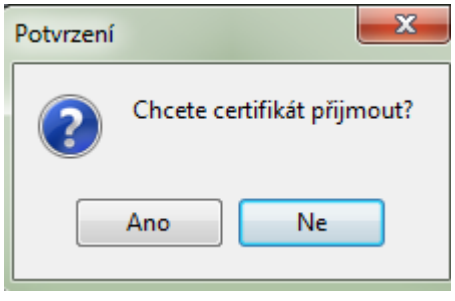
4. Pokud byl certifikát nalezen, bude zobrazeno toto okno:



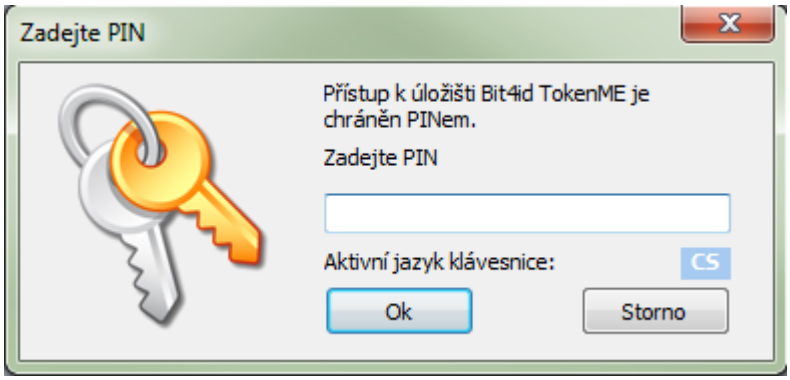
5. Dále je možné zkontrolovat údaje ve vydaném certifikátu v protokolu o vydání certifikátu, který lze stáhnout stiskem tlačítka *Stáhnout protokol o vydání certifikátu*.
6. Protokol lze uložit stiskem tlačítka *Uložit jako* nebo vytisknout tlačítkem *Tisk*.
7. Okno s protokolem lze zavřít stiskem tlačítka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



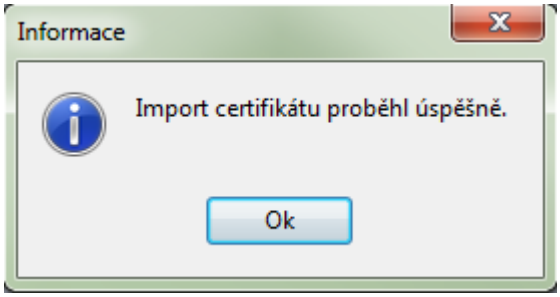
8. Přijmout certifikát - pokud jsou údaje v certifikátu v pořádku.



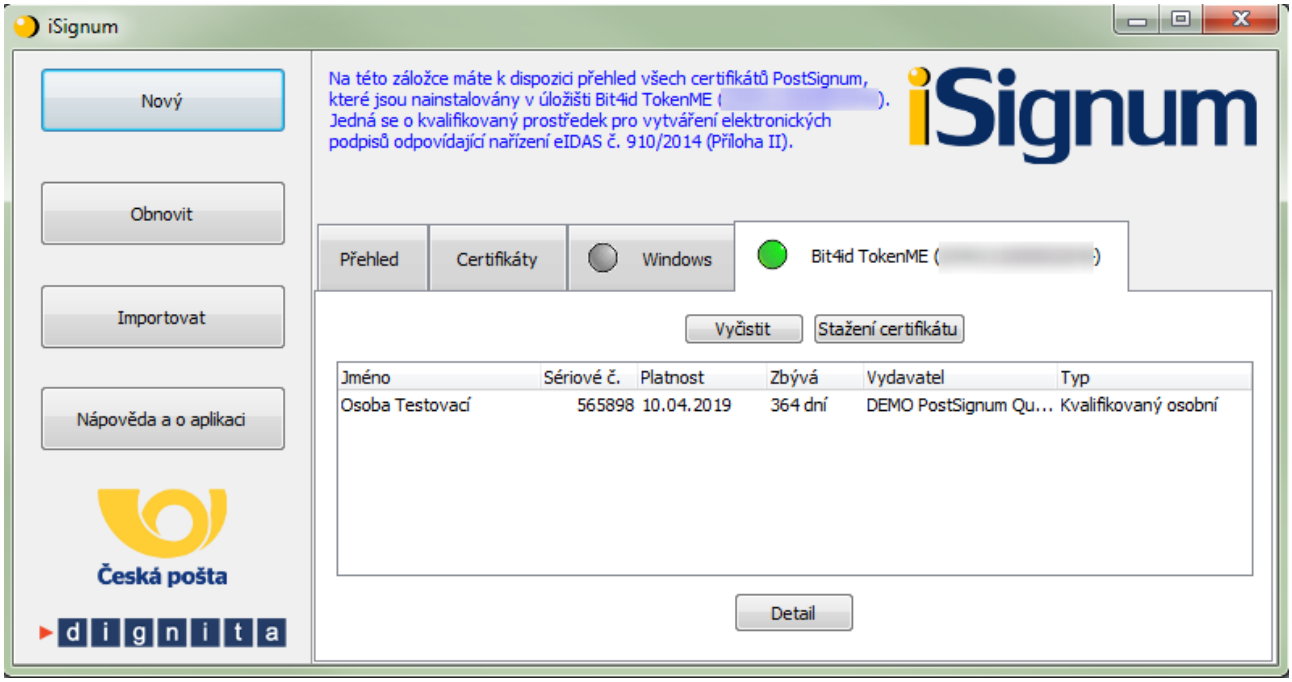
9. Zadat PIN



10. Pokud operace proběhne úspěšně, bude zobrazena hláška:



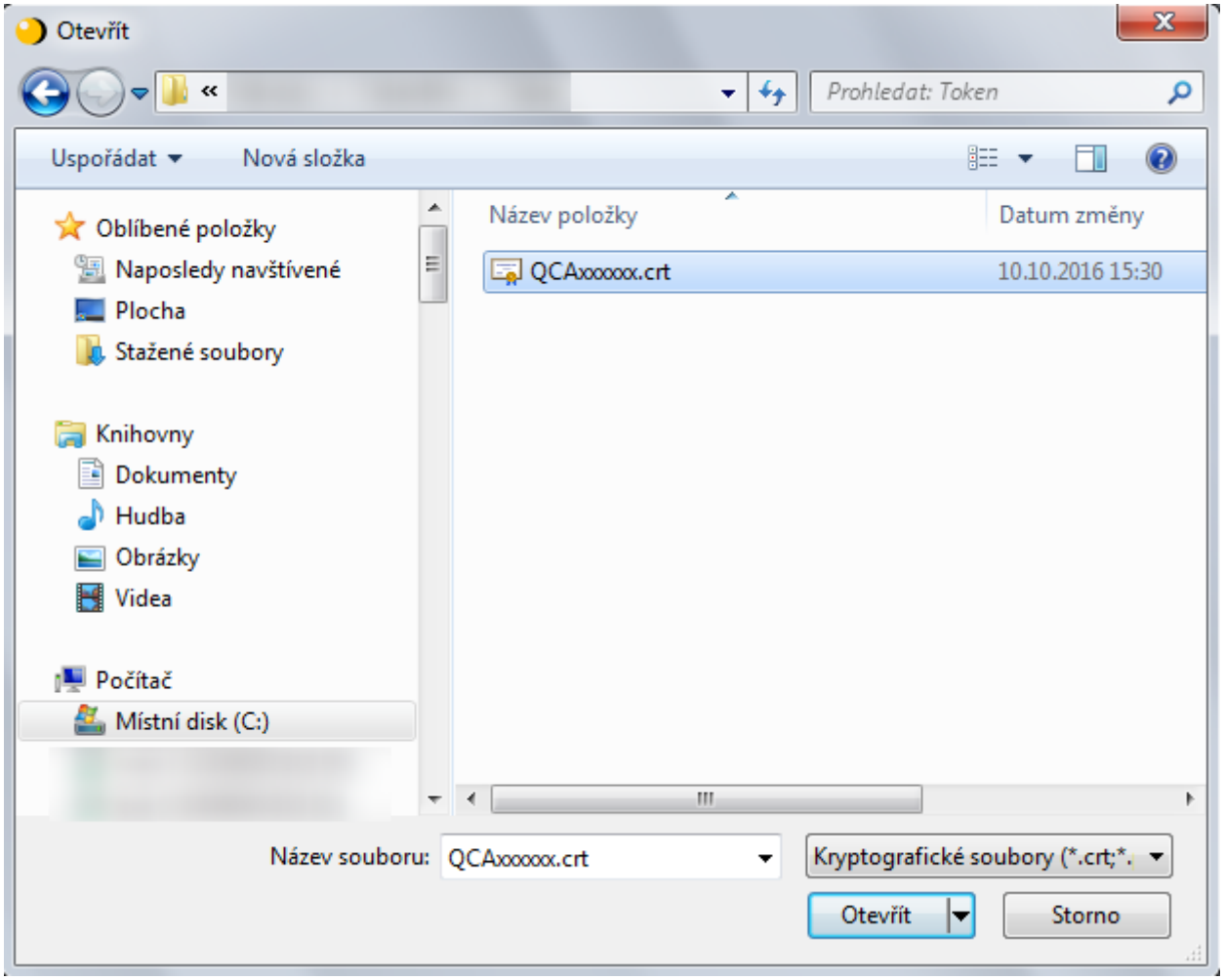
11. Po úspěšném importu bude certifikát vidět v programu iSignum na záložce TokenME.
12. Po instalaci doporučujeme prostředek vyjmout a znovu vložit do USB portu nebo do čtečky.



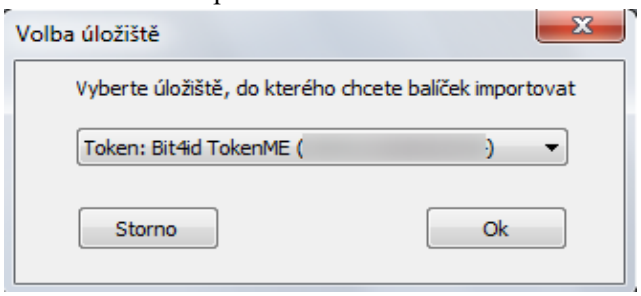
5.3. Instalace certifikátu ze staženého souboru

Instalaci certifikátu doporučujeme provést taktéž v programu iSignum:

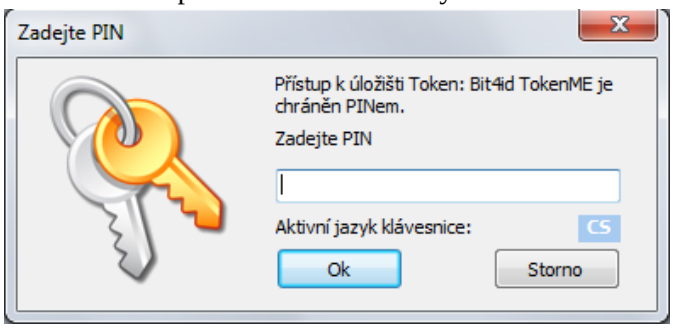
1. Vložit prostředek do USB portu počítače nebo do čtečky.
2. V programu iSignum stisknout tlačítko *Importovat*.
3. Vybrat kvalifikovaný certifikát



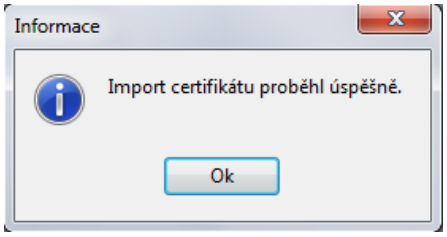
4. Ponechat přednastavené úložiště **TokenME**



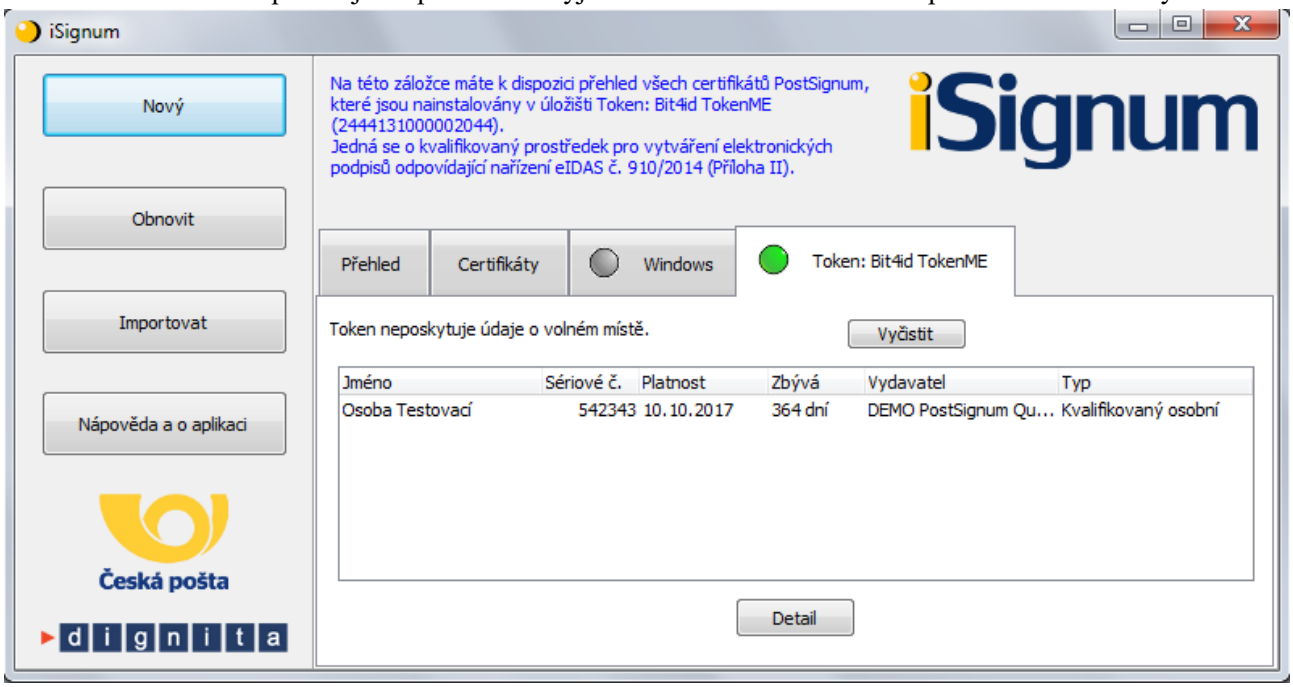
5. Pro import certifikátu bude vyžadován PIN



6. Pokud operace proběhne úspěšně, bude zobrazena hláška:



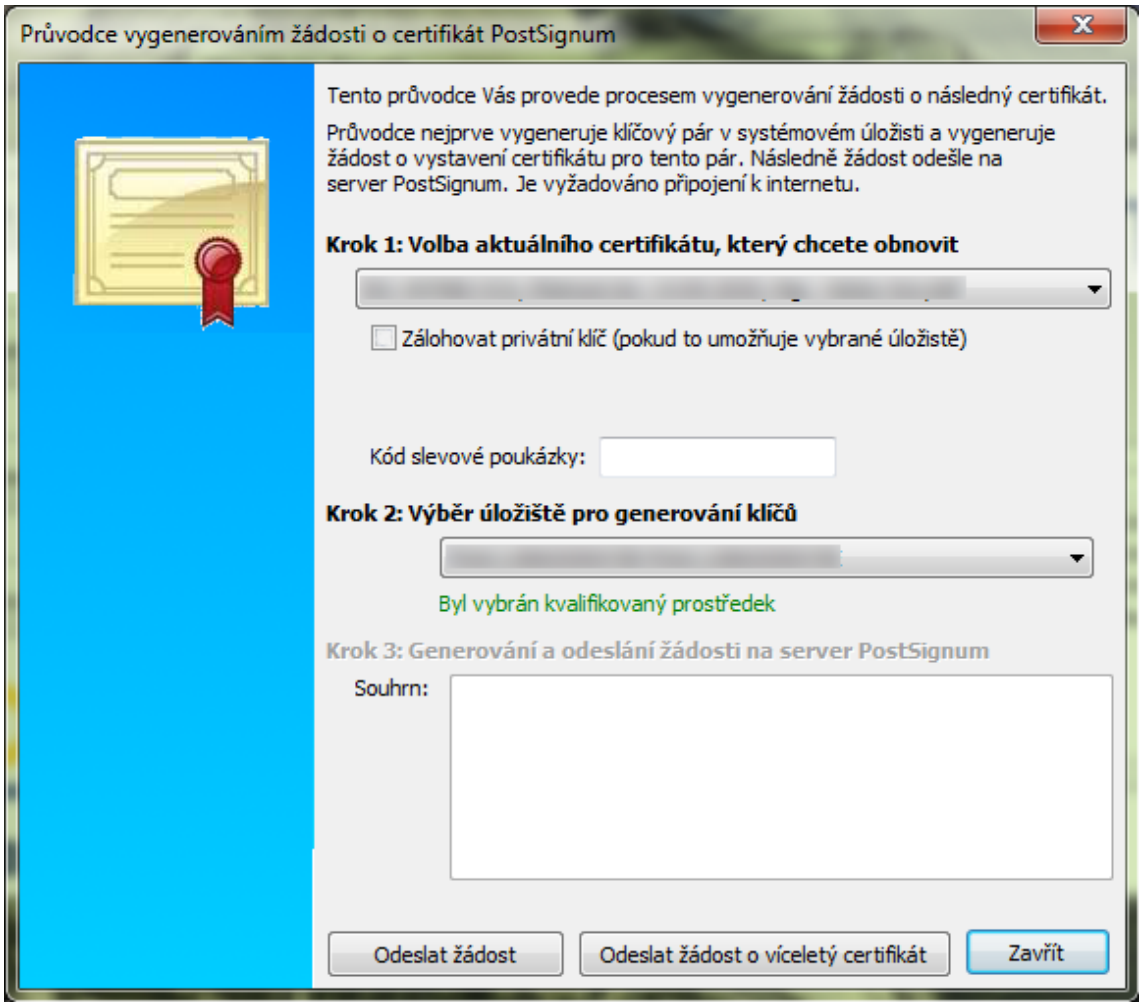
7. Po úspěšném importu bude certifikát vidět v programu iSignum na záložce **TokenME.**
8. Po instalaci doporučujeme prostředek vyjmout a znovu vložit do USB portu nebo do čtečky.



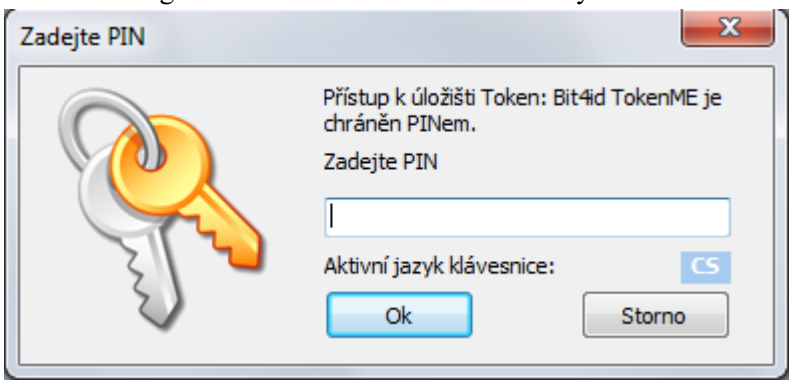
6. Generování žádosti o následný certifikát

Před provedením obnovy certifikátu se přesvědčte, že je na tokenu dostatek místa pro vygenerování nového klíče. Na token lze uložit maximálně pět certifikátů. Odstranění dat z tokenu je popsáno v kapitole 7.5

1. Vložit prostředek do USB portu počítače nebo čtečky.
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 TokenME, tak úložiště pro generování klíčů bude přednastaveno na hodnotu **TokenME** a zároveň bude zobrazeno upozornění: Byl vybrán kvalifikovaný prostředek.
4. B. Pokud obnovovaný certifikát není uložen na TokenME, je nutné vybrat úložiště pro generování klíčů ručně na hodnotu **TokenME**, aby byl obnovený certifikát uložen na prostředku.
5. Stisknout tlačítko *Odeslat žádost* případně *Odeslat žádost o víceletý certifikát.*



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 za pomoci servisního klíče dojde k autentizaci prostředku do systému a bezpečnému předání žádosti o certifikát. Při zpracování žádosti o následný certifikát je navíc provedena kontrola vazby *prostředek-žadatel*.
8. 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.
9. Instalace následného certifikátu probíhá totožným způsobem jako instalace prvotního certifikátu, viz kapitola 5.3. nebo 5.3.

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:

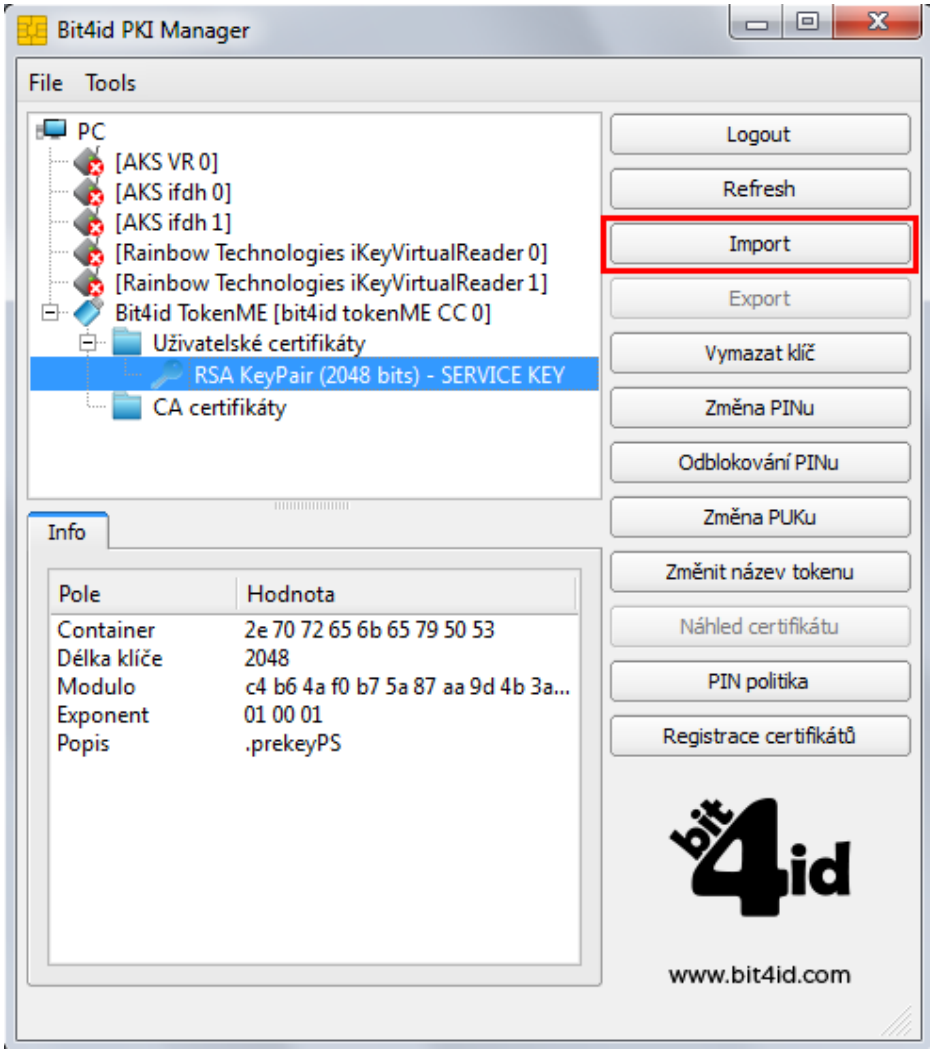
http://www.postsignum.cz/obnova_certifikatu.html

Platí pouze pro TokenME EVO

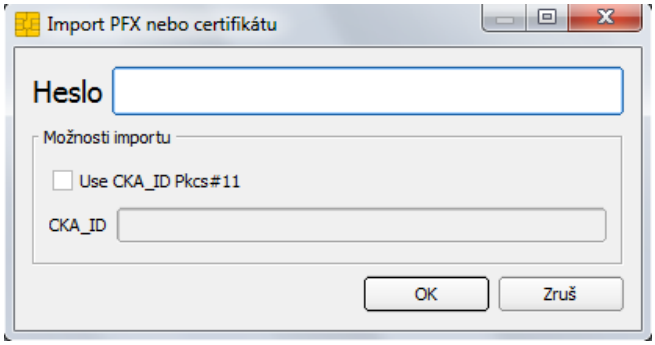
7. Další funkce softwaru Bit4id PKI Manager

7.1. Import certifikátu z PKCS#12

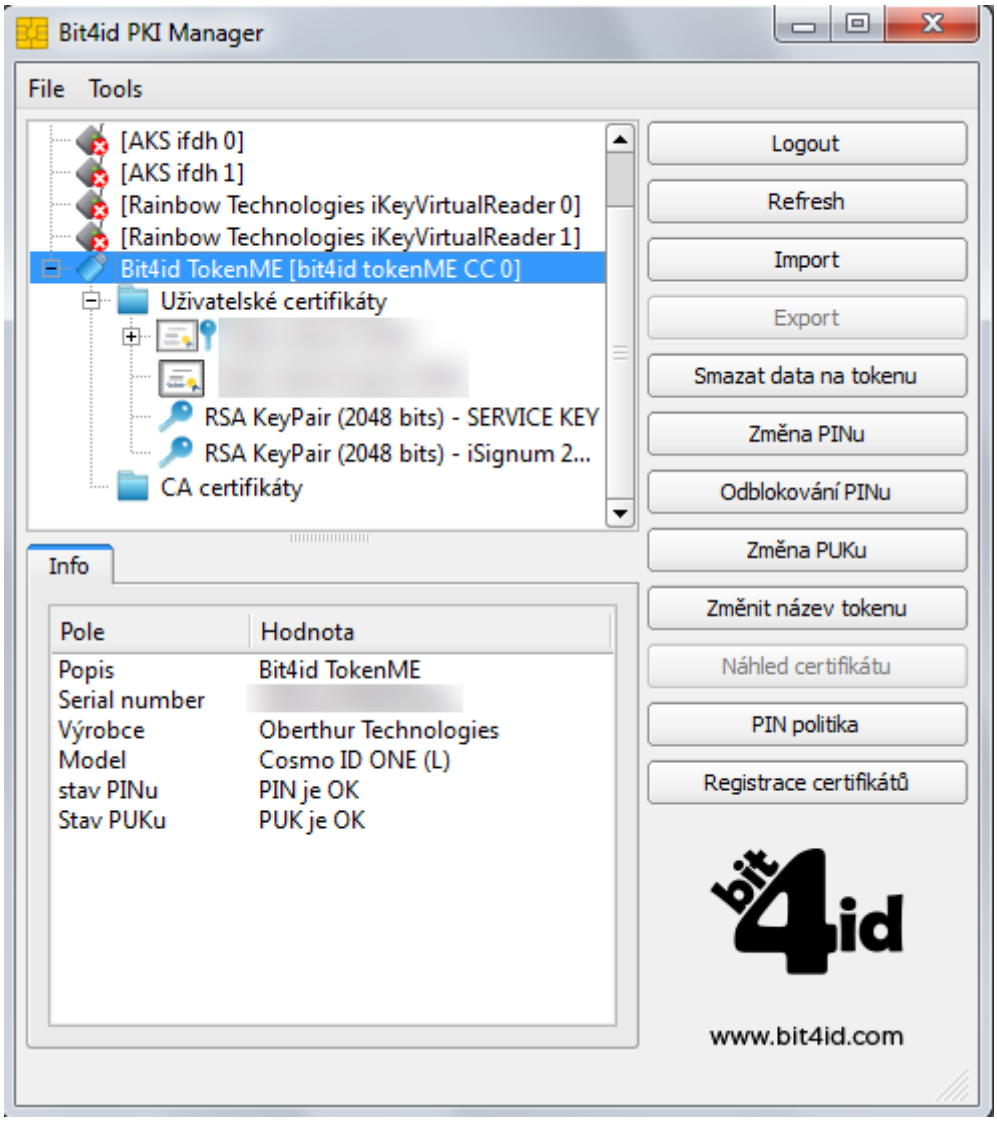
Vložení certifikátů ze zálohy (PFX nebo P12) do prostředku se provede kliknutím na tlačítko Import.



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 zařízení QESCD a nebude obsahovat příznak, že byl vytvořen na QESCD prostředku.

7.2. Logout

Po stisku tlačítka dojde k odhlášení prostředku z aplikace.

7.3. Refresh

Po stisku tlačítka dojde k obnovení zobrazených informací na prostředku.

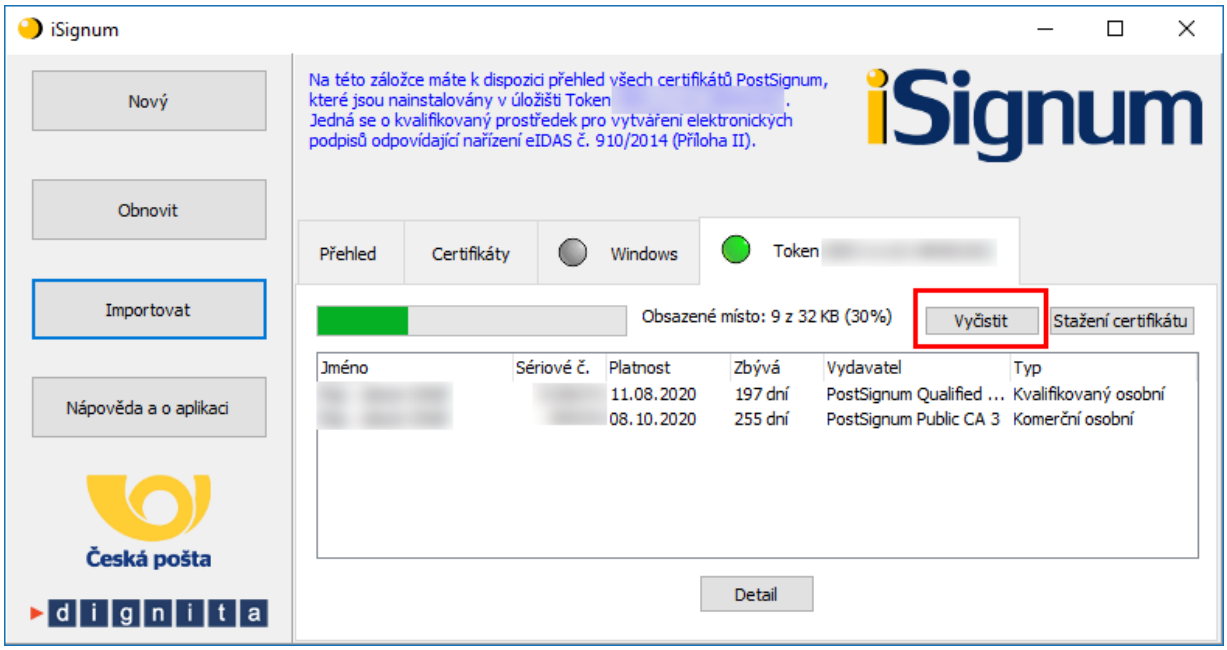
7.4. Export

Vyexportuje samotný certifikát ve formátu DER bez privátního klíče, který je uložen na prostředku.

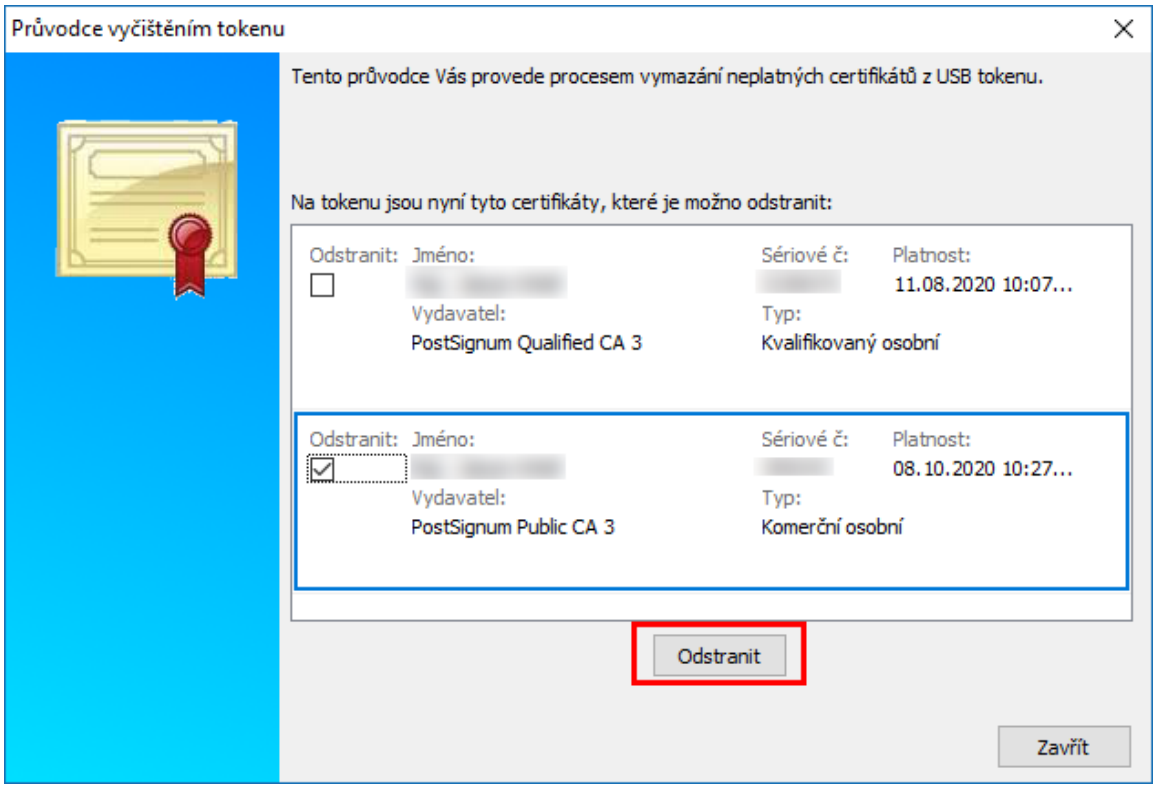
7.5. Odstranění dat

7.5.1. Odstranění certifikátu

Při obnově certifikátu může dojít k chybě 622. Tato chyba může znamenat, že na tokenu již není místo pro další certifikát. Spusťte program iSignum, vyberte záložku s tokenem a stiskněte tlačítko **Vyčistit**. **K výmazu certifikátů na prostředku doporučujeme používat výhradně aplikaci iSignum.**

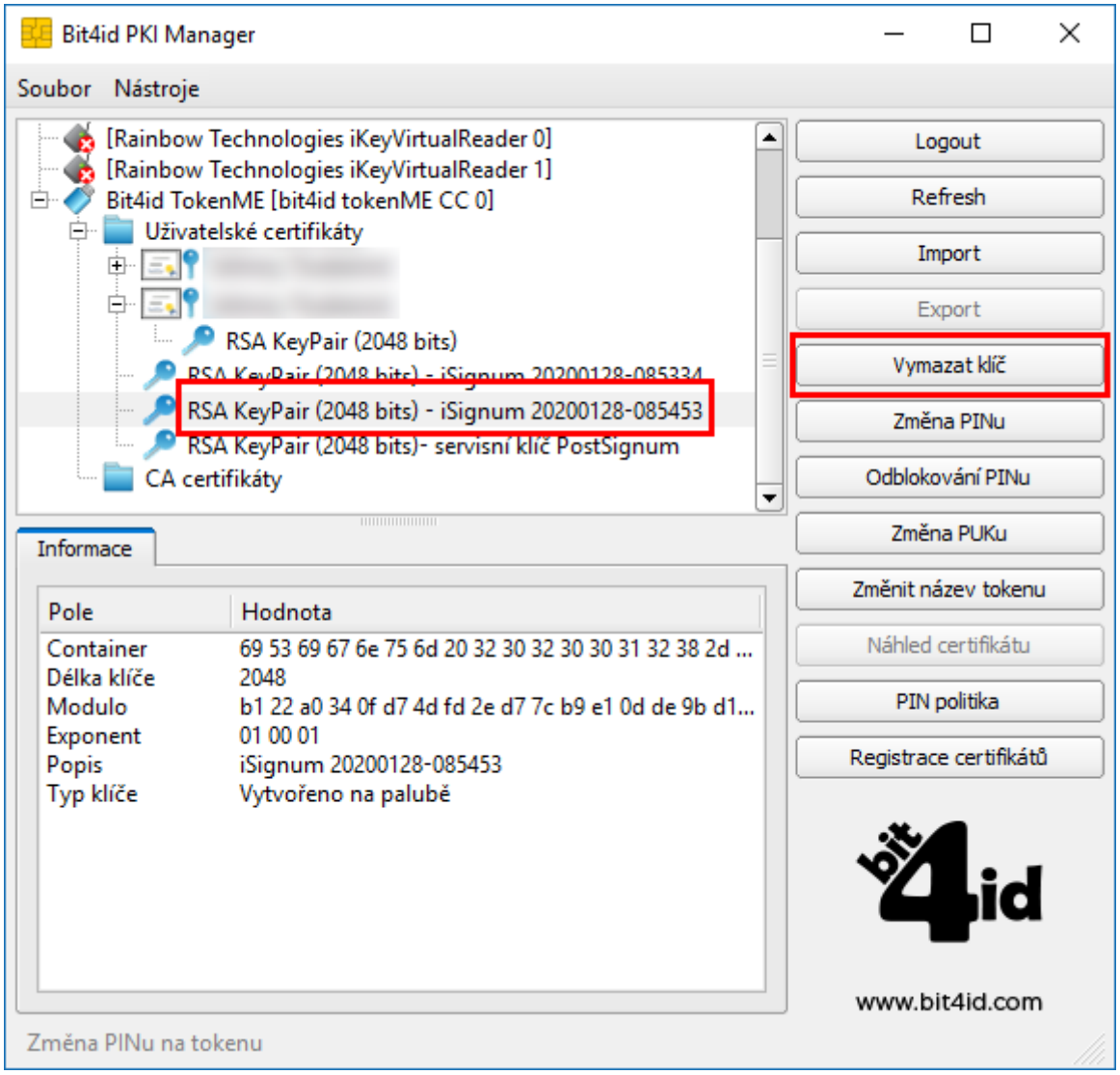


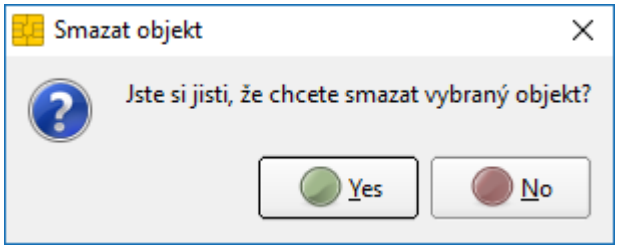
Vyberte certifikát, který chcete odstranit a stiskněte tlačítko **Odstranit**.



7.5.2. Odstranění klíče

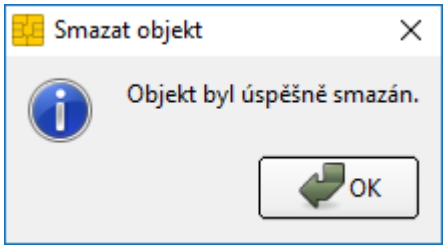
Chyba 622 může být rovněž způsobena tím, že na tokenu jsou uloženy klíče, které nebyly spárovány s certifikátem. Tyto klíče lze odstranit v programu **Bit4id PKI Manager**. Název klíče vždy začíná **RSA KeyPair** a končí příponou složenou z data a času, kdy byl klíč generován. Klíč vyberte a stiskněte tlačítko **Vymazat klíč**. **Dbejte prosím zvýšené opatrnosti, aby nedošlo ke smazání servisního klíče!**





Budete vyzváni k zadání PINu.

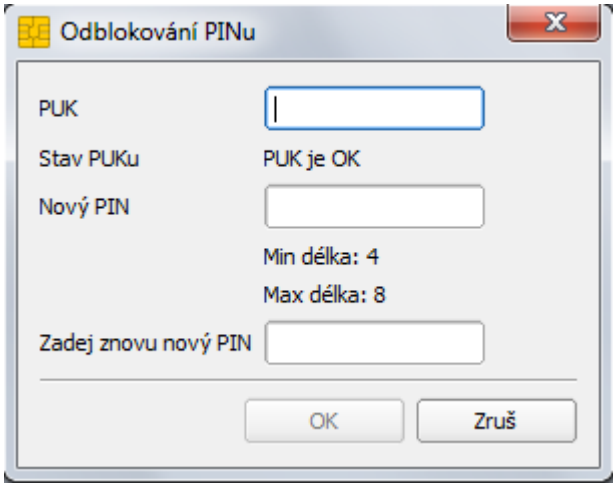
Při úspěšném odstranění bude zobrazena tato hláška.



Pokud dojde ke smazání servisního klíče, postupujte dle kapitoly 8.1

7.6. Odblokování PINu

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

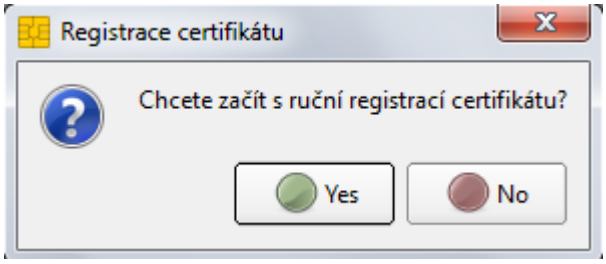


Upozorňujeme, že při zablokování PIN i PUK dojde ke znehodnocení prostředku.

7.7. Náhled certifikátu

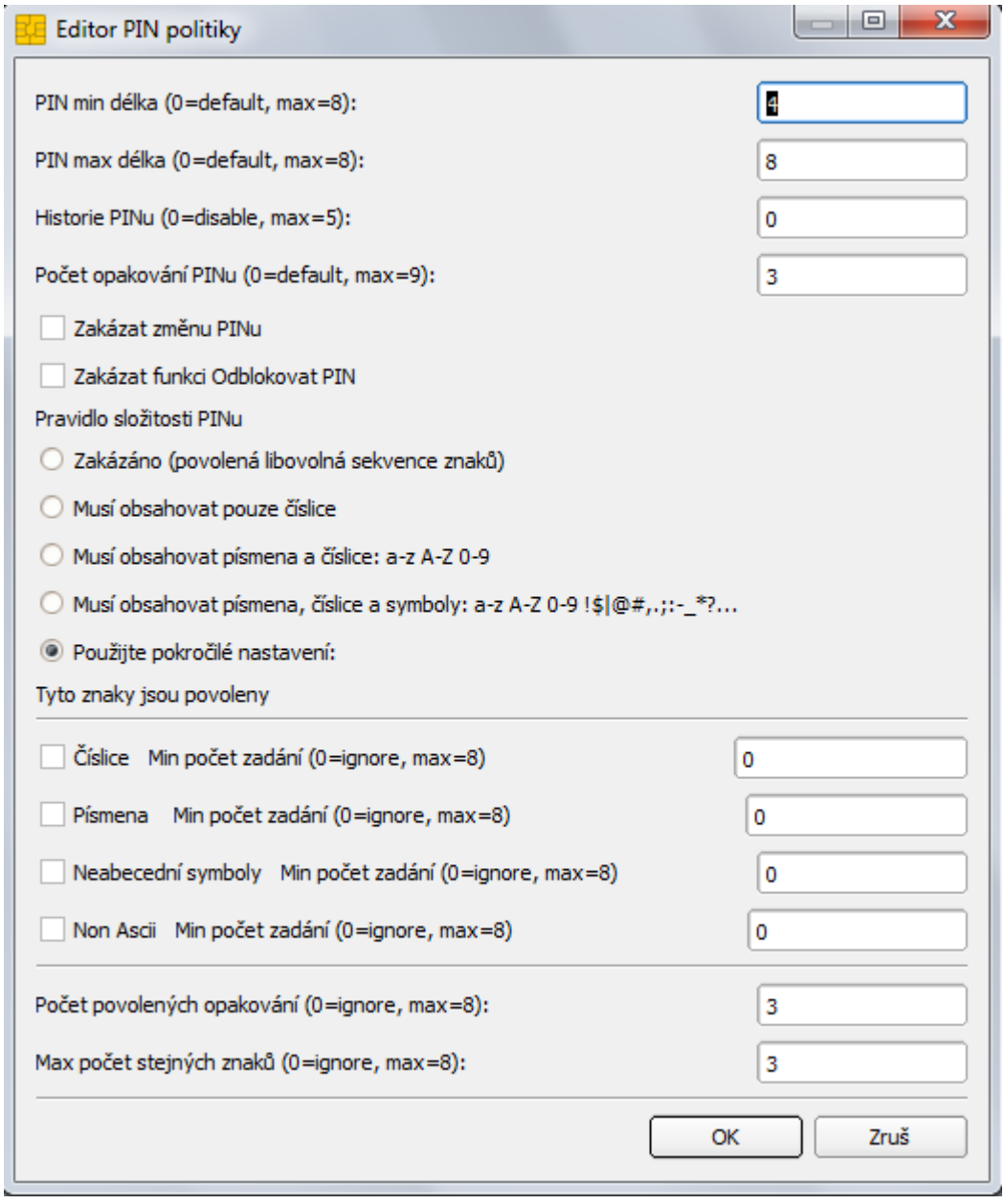
Dojde k zobrazení detailu vybraného certifikátu.

7.8. 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.

7.9. PIN Politika



Zde je možné nastavit pravidla pro vytváření PINu, povinné znaky, atp.

8. Reinicializace prostředku

8.1. Výmaz servisního klíče

V případě, že dojde k výmazu servisního klíče, je nutné na prostředek nahrát nový servisní klíč, což lze provést pouze na specializovaném pracovišti České pošty. V tomto případě, je nutné postupovat jako při reklamaci, viz kapitola 9.

8.2. Předání prostředku jiné osobě

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

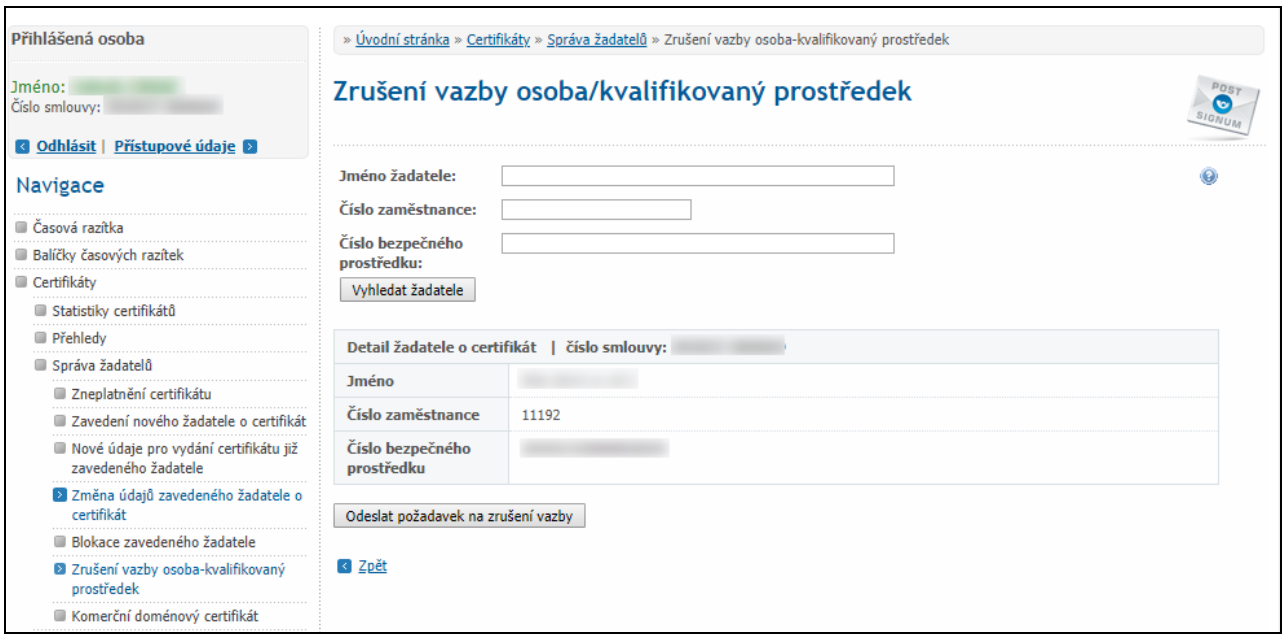
Pokud je nutné tuto vazbu změnit (např. z důvodu předání prostředku jinému žadateli), je nutné postupovat následovně:

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

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

Tělo: Oznamuji zrušení vazby osoba-kvalifikovaný 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 a PUK, aby bylo možné na prostředku vygenerovat nový servisní klíč.**

   PIN: 12345678

   PUK: 87654321
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 na prostředek vygenerovat nový servisní klíč.