Česká pošta

TokenME – Uživatelská příručka

Verze 1.1

Obsah dokumentu

Evidence revizí a změn

Verze	Účinnost od	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

1. Přehled

TokenME (dále také jen token) je prakticky malé zařízení, které **je schválené jako kvalifikovaný prostředek pro vytváření elektronických podpisů v souladu s nařízením eIDAS** a slouží k vytváření kvalifikovaných elektronických podpisů. Je to PKI token postavený na kryptografickém mikroprocesoru s certifikací Common Criteria EAL4+ a FIPS 140-2 level 3.

TokenME je personalizován již z výroby, tzn., je na něm 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 tokenu.

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

Při vydání prvního certifikátu dochází k vytvoření vazby **token–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 tokenu více certifikátů různých žadatelů s příznakem QESCD.

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

Obrázek zařízení TokenME

2. Co potřebuji?

1. PC s operačním systémem Windows

2. TokenME

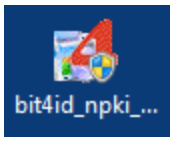
3. Software

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

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 – TokenME provedl změny ve Vašem PC
3. Odsouhlasit instalaci programu Bit4id – TokenME – 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 token do PC. V tento okamžik je již software plně nainstalován a token se již může zasunout do PC pro další práci s tokenem.
7. Po zasunutí tokenu do PC, začne token blikat a objeví se informativní hláška, že software ovladače byl úspěšně naistalován.

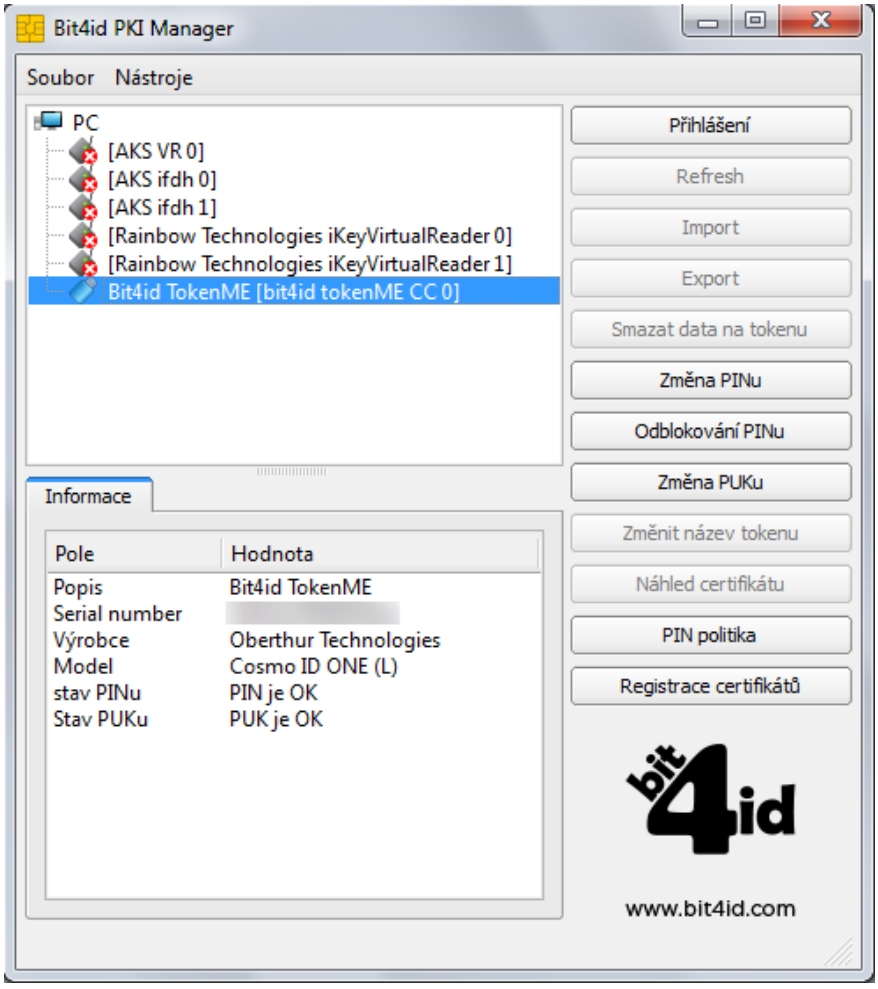
Knihovna PKCS#11

V případě použití tokenu v aplikacích, které nevyužívají systémové úložiště certifikátů ve Windows (např. Mozilla Firefox nebo Thunderbird), lze ke komunikaci s tokenem využít (pokud to aplikace podporuje) DLL knihovnu PKCS#11 *BIT4XPKI.DLL*, která se nachází v adresáři *C:\WINDOWS\SYSTEM32*.

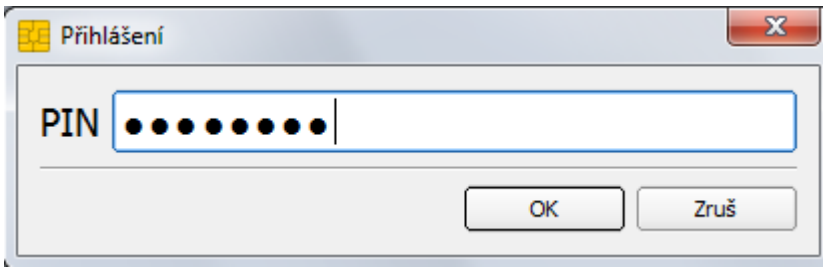
4. Příprava tokenu pro generování klíčů

Před prvním použití tokenu **je nutné změnit PIN a PUK** a přesvědčit se, zda je na tokenu 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 tokeny a objekty na tokenu (klíče, certifikáty), spodní část zobrazuje informace o vybraném tokenu či objektu a pravá část zobrazuje příkazy a funkce.

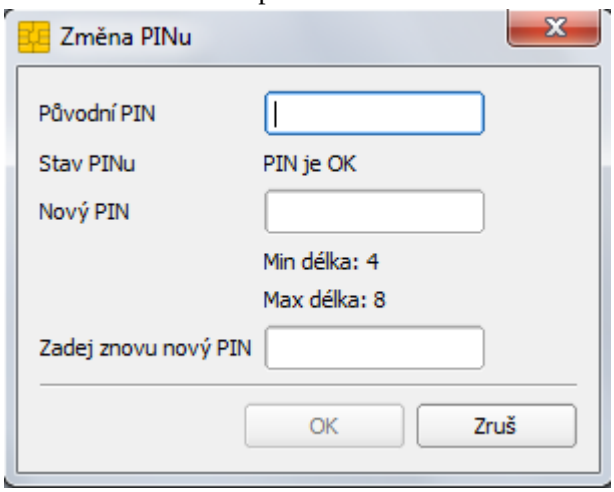


Před dalšími kroky je potřeba se k tokenu přihlásit tlačítkem *Přihlášení* a zadat přednastavený PIN: **12345678**



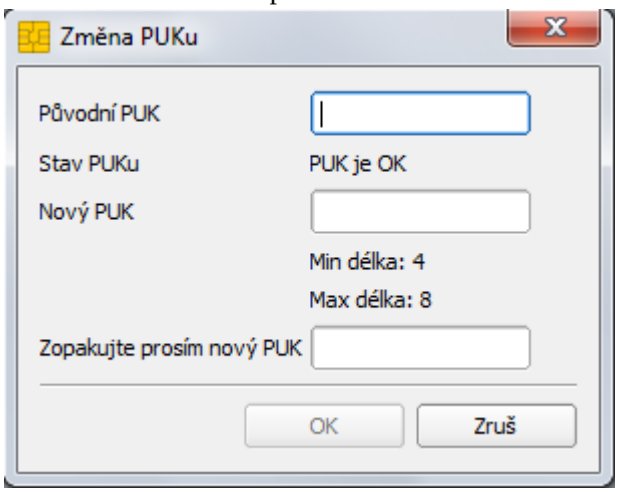
4.1. Změna PINu

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.



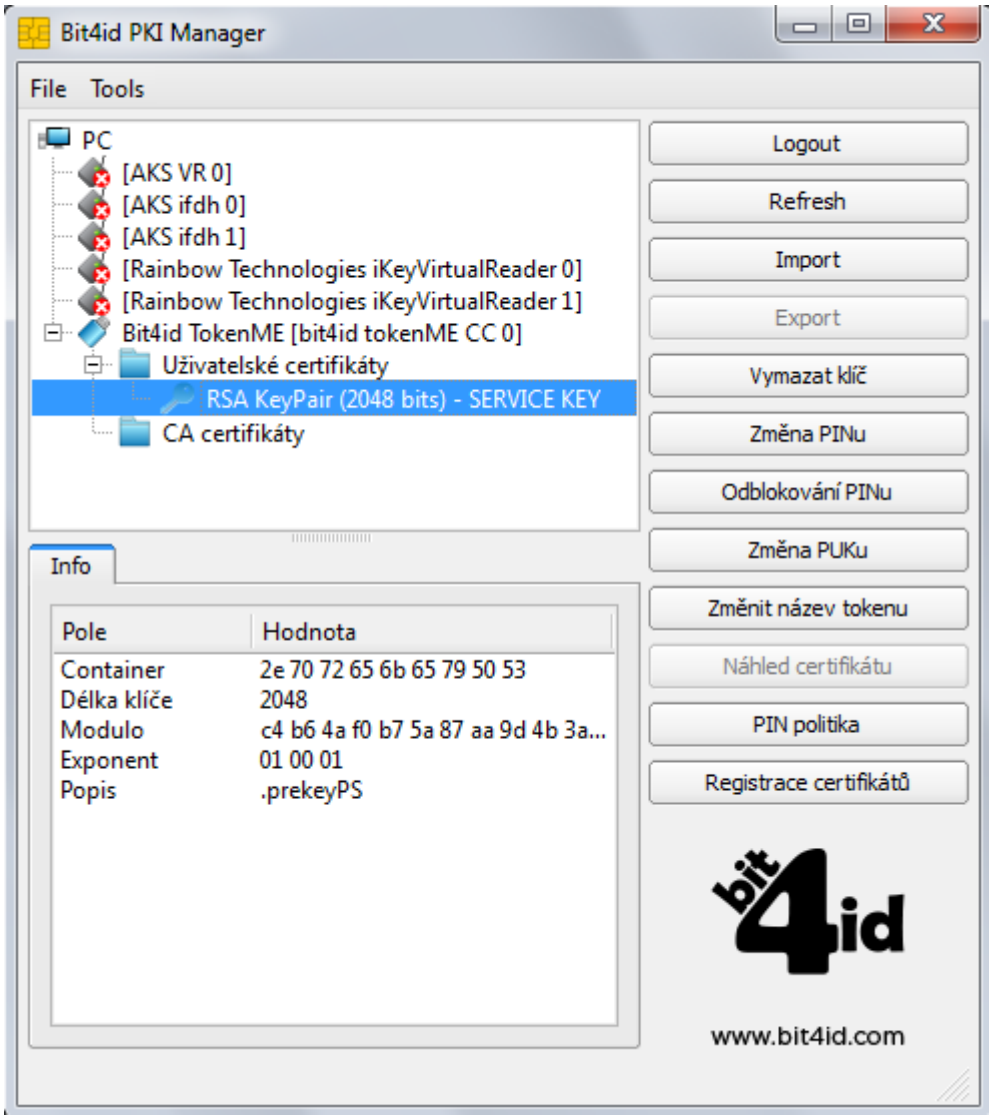
Upozorňujeme, že při zablokování PIN i PUK dojde ke znehodnocení tokenu.

4.3. Kontrola servisního klíče

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

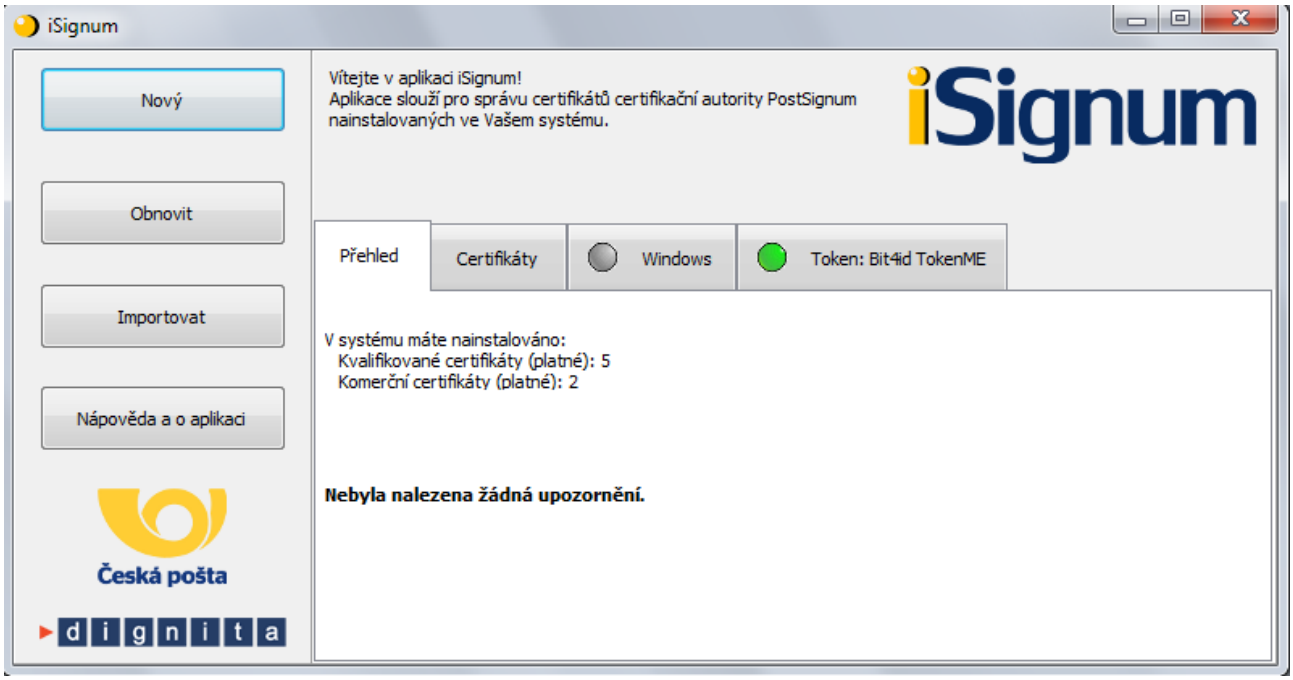
Generování klíčů na token a žádosti o kvalifikovaný certifikát, který bude obsahovat příznak QESCD, je možné pouze v programu **iSignum**, který zajistí vytvoření správné žádosti o certifikát. Pokud bude ke generování žádosti využit jiný program, není možné do certifikátu příznak QESCD vložit.

Program iSignum je ke stažení z webových stránek PostSignum:

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

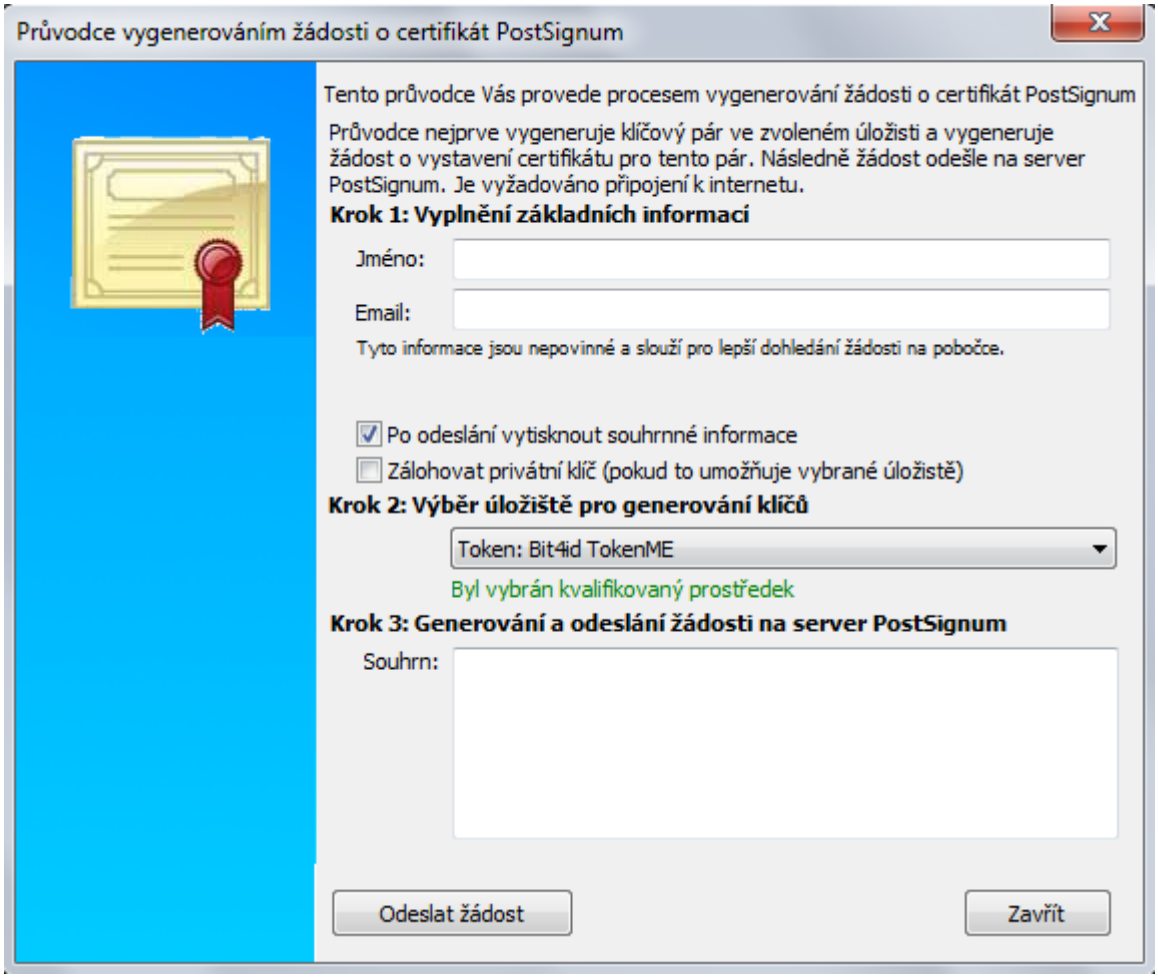
Spustit lze poklikáním na stažený soubor **iSignum.exe.**

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

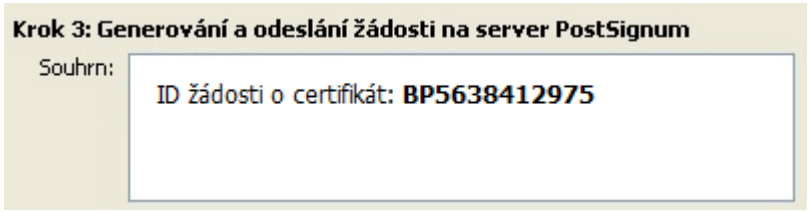


5.1. Vygenerování žádosti o certifikát

1. Vložit token do USB portu počítače.
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. Dále je nutné vyplnit své jméno a e-mailovou adresu a stisknout tlačítko *Odeslat žádost*.
5. Před generováním klíčů a žádosti bude vyžadován PIN.



6. Po vygenerování klíčů a žádosti o certifikát bude navázána komunikace se systémem certifikační autority a za pomoci servisního klíče dojde k autentizaci tokenu do systému a bezpečnému předání žádosti o certifikát.
7. 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.**



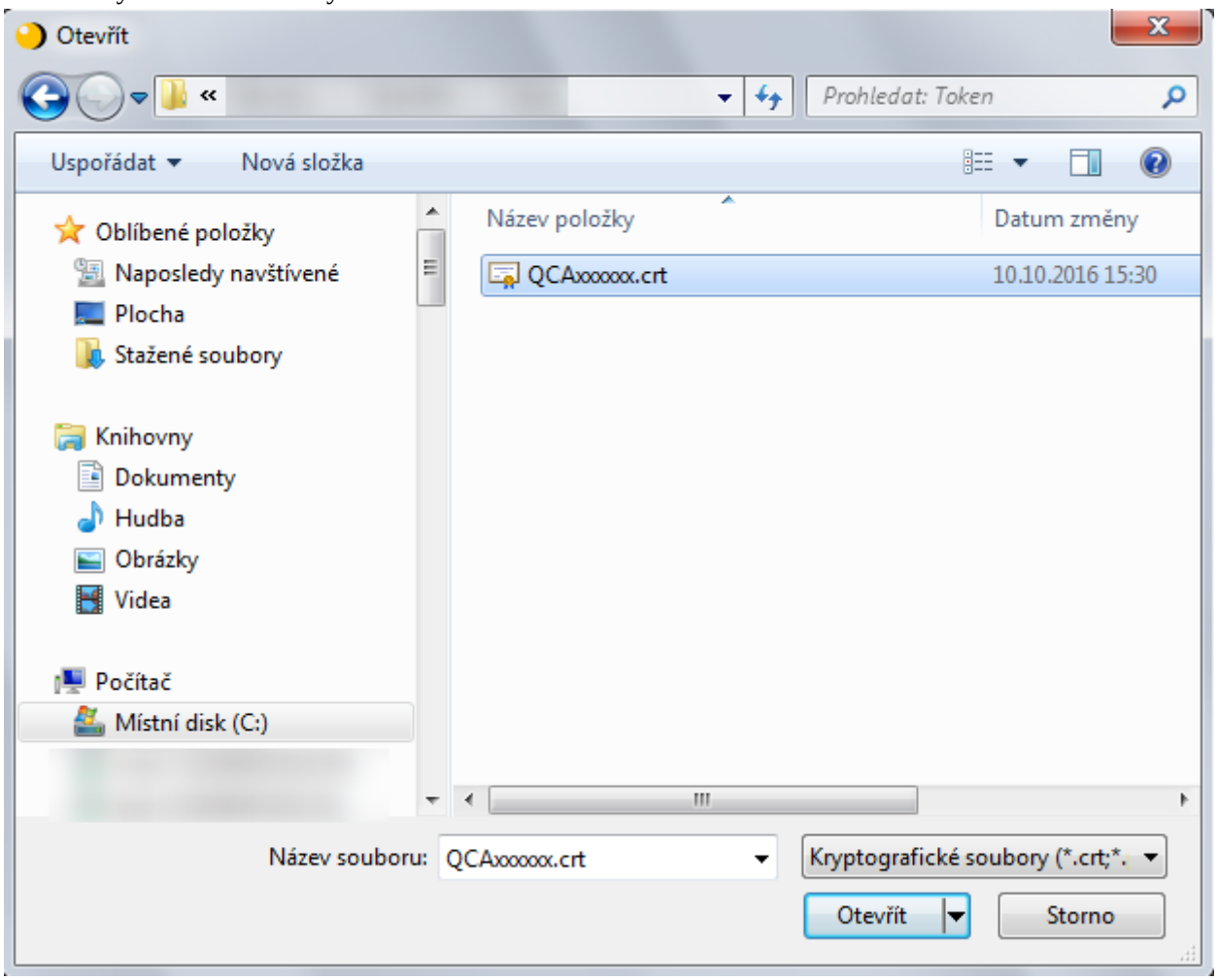
Toto ID předložíte spolu s dalšími náležitostmi na pobočce České pošty. Postup, jak získat certifikát naleznete na webových stránkách PostSignum:

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

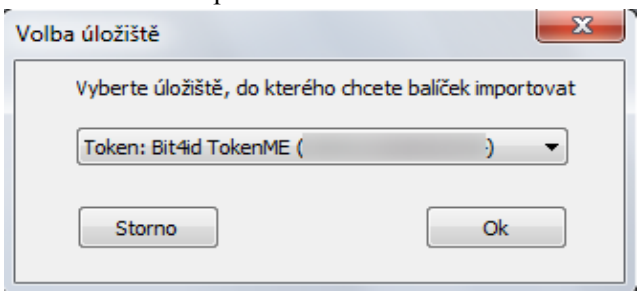
5.2. Instalace certifikátu

Instalaci certifikátu doporučujeme provést taktéž v programu iSignum:

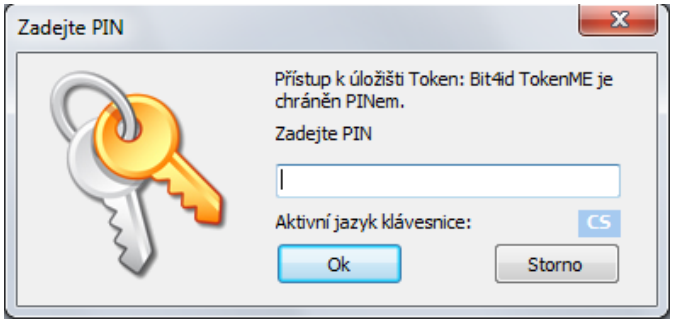
1. Vložit token do USB portu počítače.
2. V programu iSignum stisknout tlačítko *Importovat*.
3. Vybrat kvalifikovaný certifikát



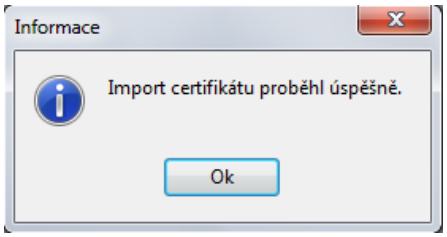
4. Ponechat přednastavené úložiště **TokenME**



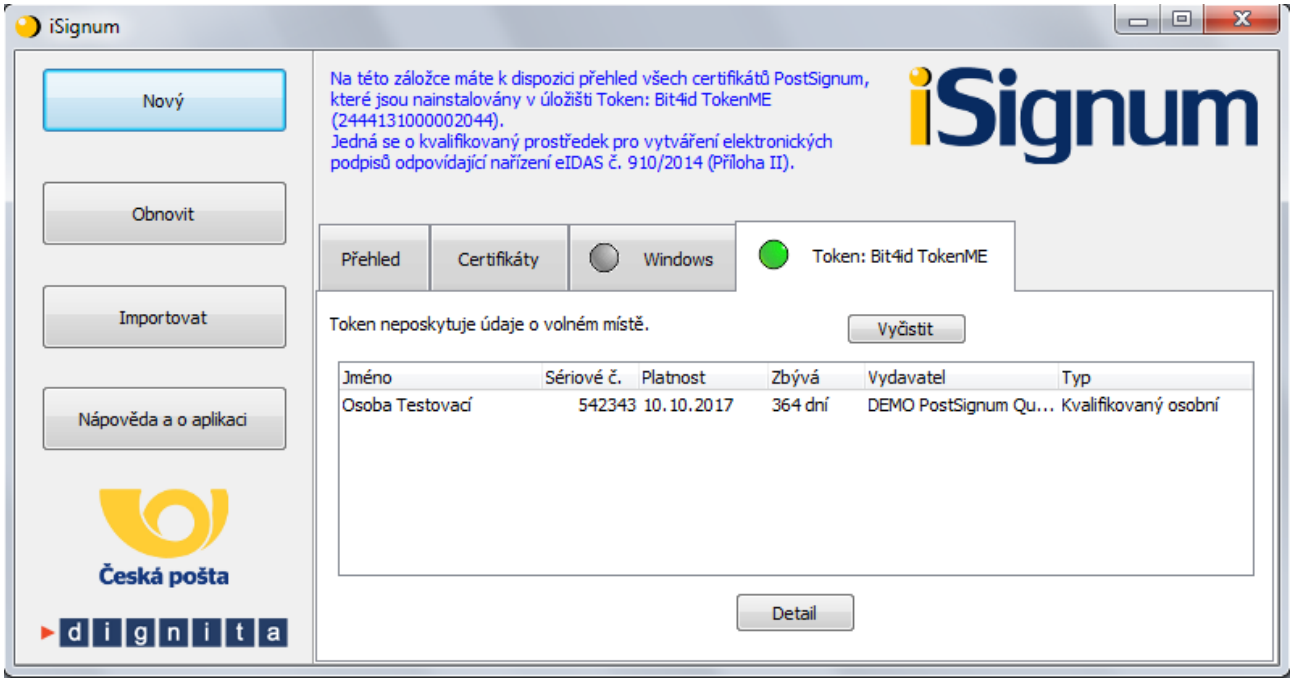
5. Pro import certifikátu bude vyžadován PIN



6. Pokud operace proběhne úspěšně, bude zobrazena hláška:

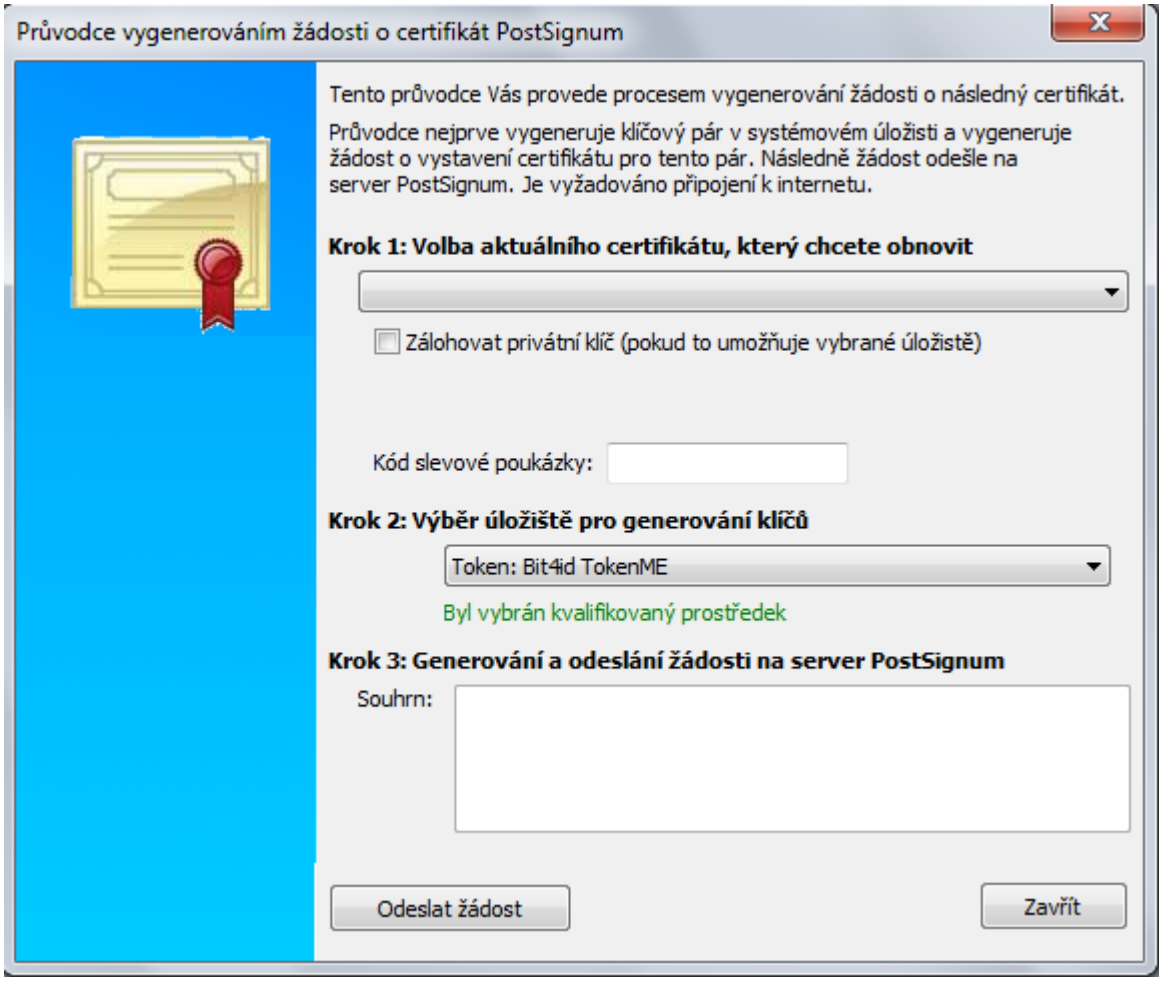


7. Po úspěšném importu bude certifikát vidět v programu iSignum na záložce **TokenME.**
8. Po instalaci doporučujeme token vyjmout a znovu vložit do USB portu.

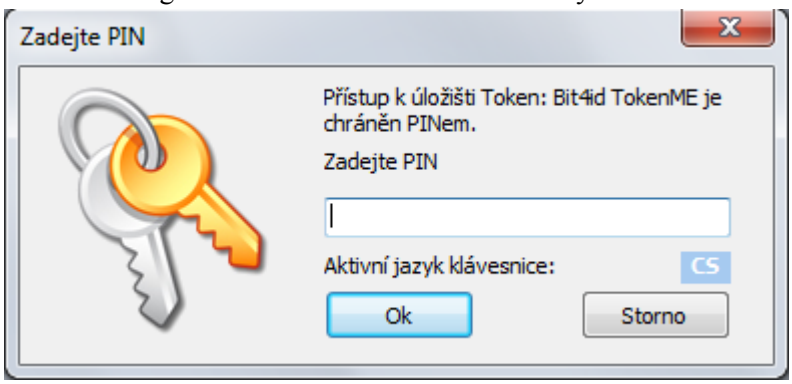


6. Generování žádosti o následný certifikát

1. Vložit token do USB portu počítače.
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 tokenu.
5. Stisknout tlačítko *Odeslat žádost.*



6. Před generováním klíčů a žádosti bude vyžadován PIN.

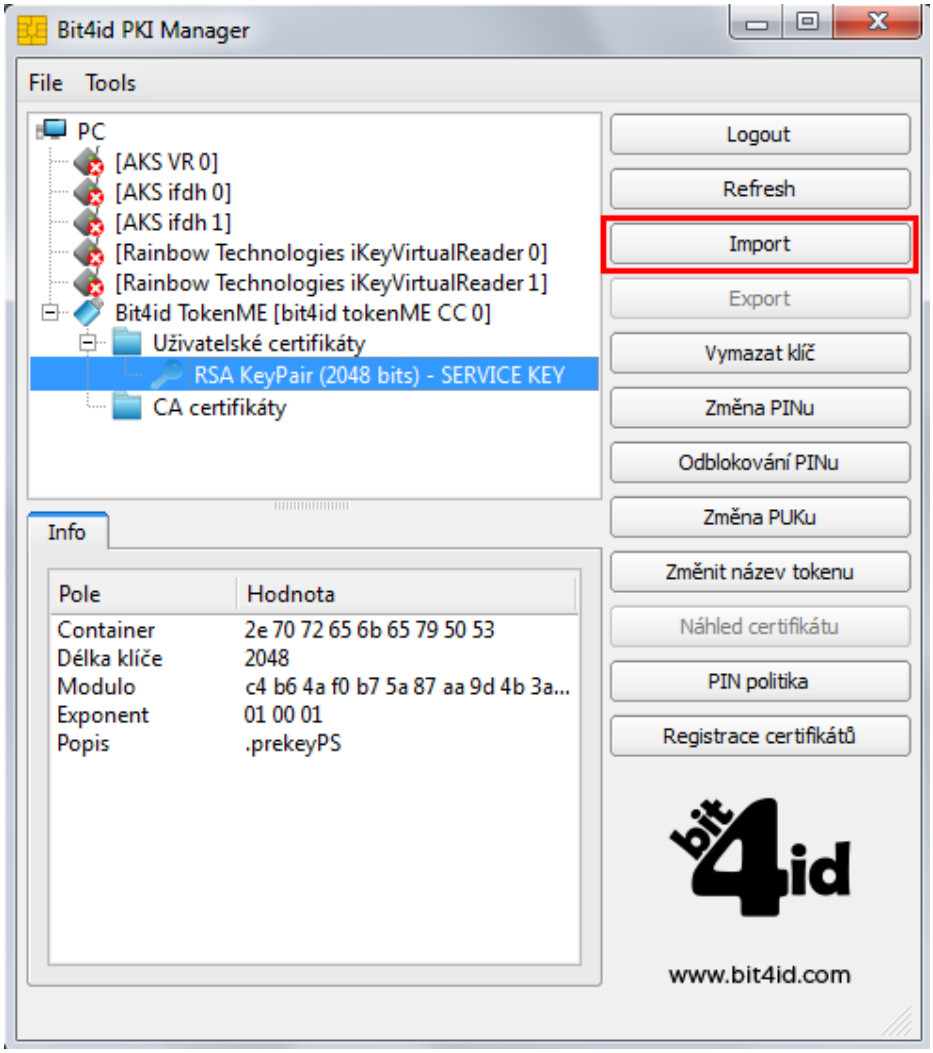


7. Po vygenerování klíčů a žádosti o certifikát bude navázána komunikace se systémem certifikační autority a za pomoci servisního klíče dojde k autentizaci tokenu do systému a bezpečnému předání žádosti o certifikát. Při zpracování žádosti o následný certifikát je navíc provedena kontrola vazby *token-žadatel*.
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 5.2.

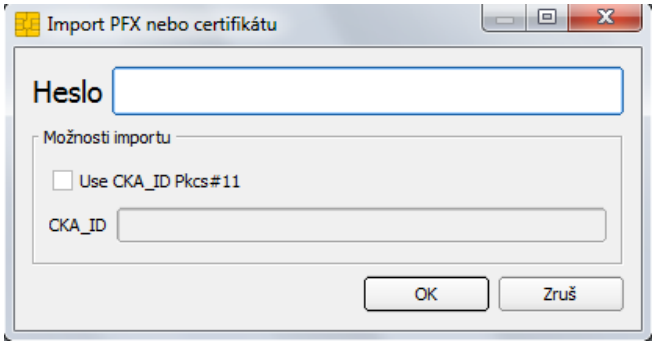
7. Další funkce softwaru Bit4id PKI Manager

7.1. Import certifikátu z PKCS#12

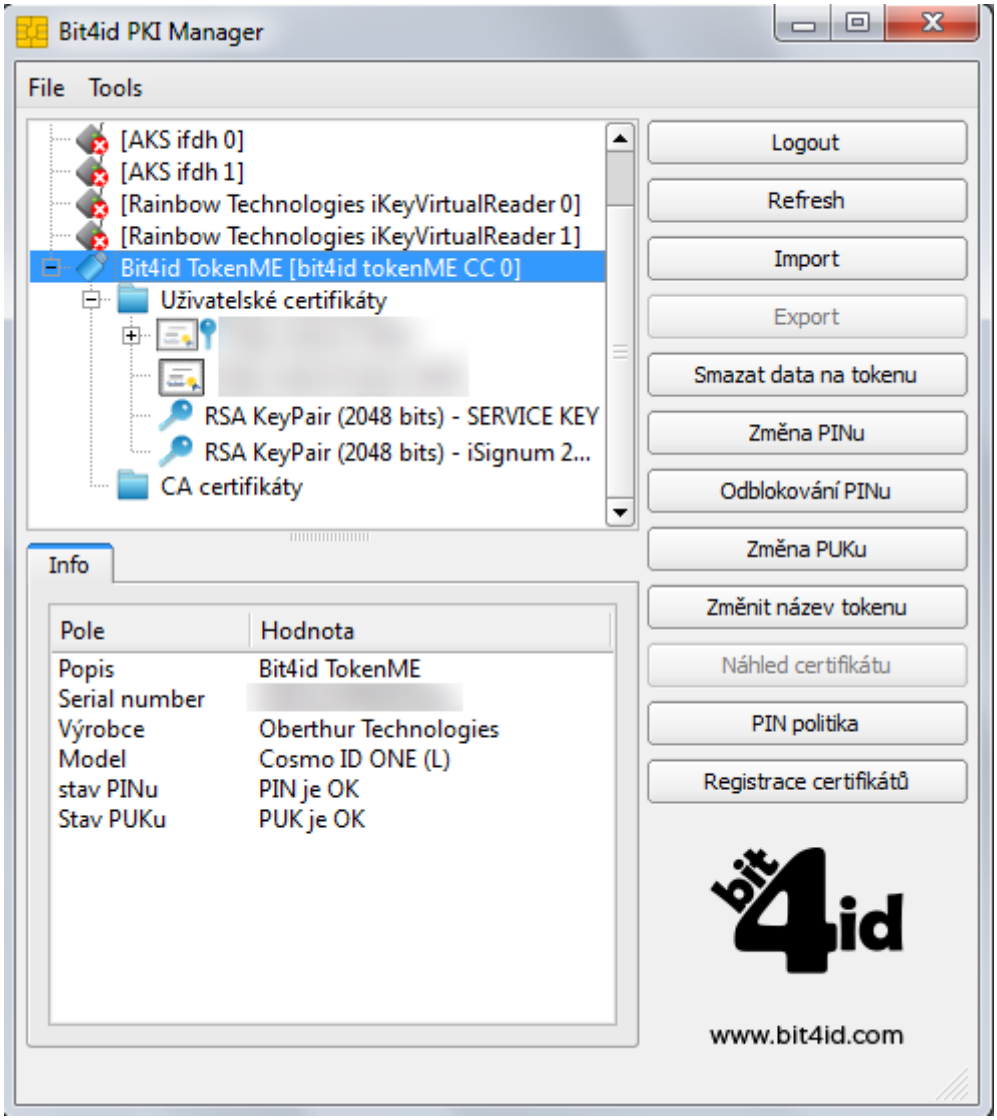
Vložení certifikátů ze zálohy (PFX nebo P12) do tokenu se provede kliknutím na tlačítko Import.



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 tokenu z aplikace.

7.3. Refresh

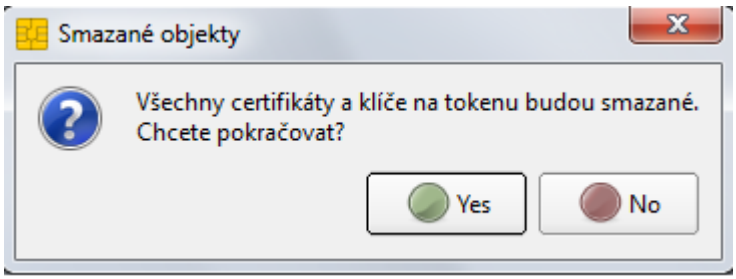
Po stisku tlačítka dojde k obnovení zobrazených informací na tokenu.

7.4. Export

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

7.5. Smazat data na tokenu

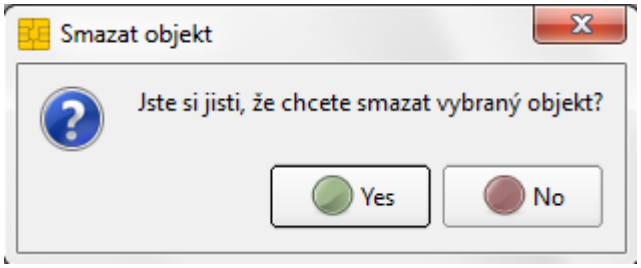
A. Tato volba je dostupná, pokud je kurzor nastaven na objektu TokenME.



Po potvrzení dojde ke smazání veškerých dat z tokenu, včetně servisního klíče. Na tokenu nebude možné vytvořit žádost o certifikát pomocí aplikace iSignum.

TUTO VOLBU NEDOPORUČUJEME SPOUŠTĚT!

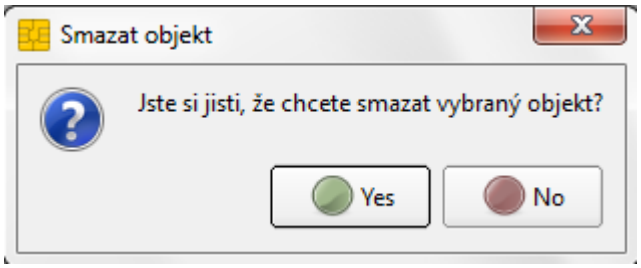
B. Pokud je kurzor nastaven na objektu typu RSA KeyPair, v menu se zobrazí volba **Vymazat klíč**.



Pokud dojde k výmazu klíče, nebude možné nainstalovat vydaný certifikát! Pokud dojde k výmazu servisního klíče, nebude možné vytvořit žádost o certifikát pomocí aplikace iSignum.

TUTO VOLBU NEDOPORUČUJEME SPOUŠTĚT!

C. Pokud je kurzor nastaven na objektu typu certifikát, v menu se zobrazí volba **Vymazat certifikát**.



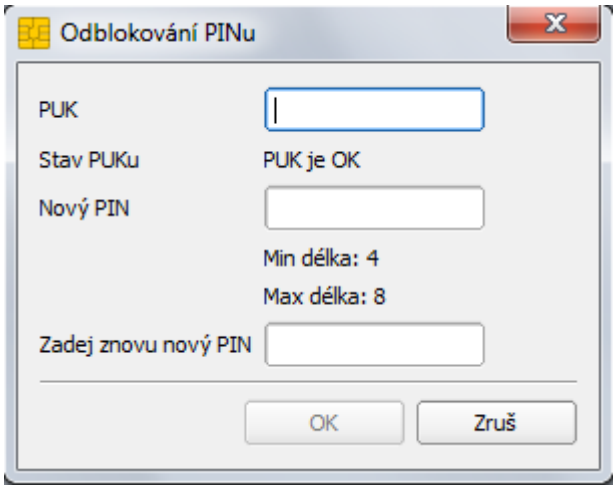
Pokud dojde k výmazu certifikátu, bude smazán i jemu odpovídající klíč a nebude možné nadále certifikát používat.

TUTO VOLBU NEDOPORUČUJEME SPOUŠTĚT!

K výmazu dat na tokenu doporučujeme používat výhradně aplikaci iSignum.

7.6. Odblokování PINu

Pokud je token 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.

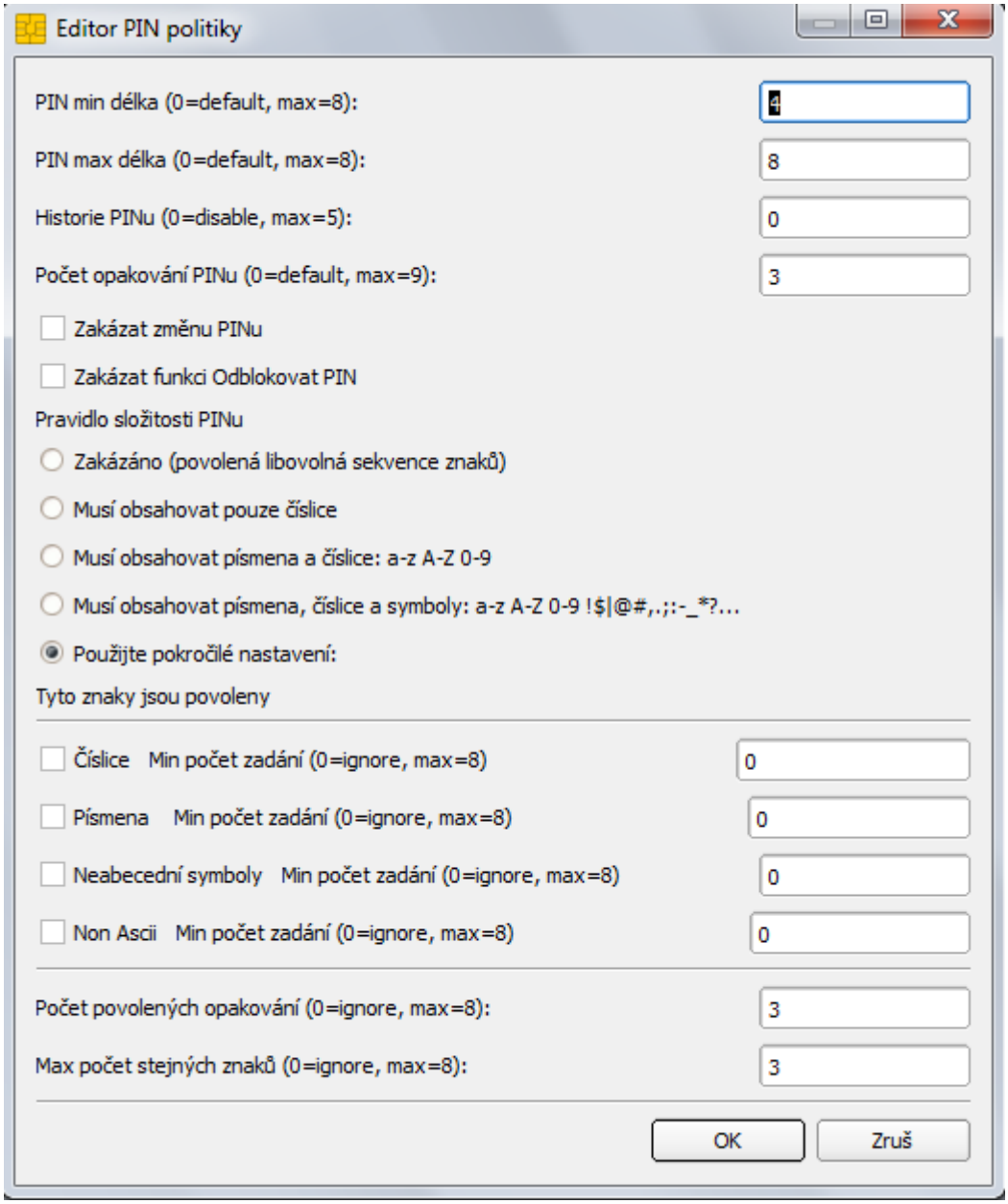


Upozorňujeme, že při zablokování PIN i PUK dojde ke znehodnocení tokenu.

7.7. Náhled certifikátu

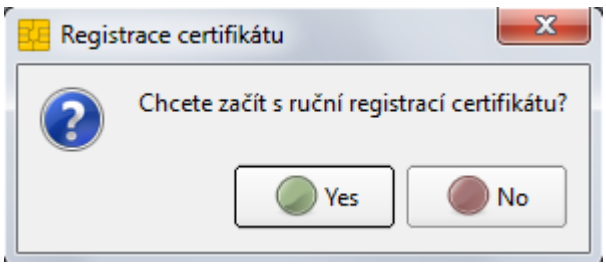
Dojde k zobrazení detailu vybraného certifikátu.

7.8. PIN Politika



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

7.9. Registrace certifikátů



Dojde k registraci certifikátu uložených na tokenu 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.

8. Reinicializace tokenu

8.1. Výmaz servisního klíče

V případě, že dojde k výmazu servisního klíče, je nutné na token nahrát nový servisní klíč, což lze provést pouze na specializovaném pracovišti České pošty. V tomto případě, je nutné postupovat jako při reklamaci zařízení a provést tyto kroky:

1. **Vymazat z tokenu veškeré uživatelské certifikáty, aby nemohlo dojít k jejich zneužití.**
2. **Nastavit na tokenu PIN 12345678, aby bylo možné na tokenu vygenerovat nový servisní klíč.**
3. Token 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 token vygenerovat nový servisní klíč.

8.2. Předání tokenu jiné osobě

Při vydání prvního certifikátu dochází k vytvoření vazby **token–žadatel o certifikát**, 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 tokenu jinému žadateli), je nutné postupovat následovně:

1. Zneplatnit certifikáty původního žadatele uložené na tokenu.
2. Pověřená osoba musí oznámit zrušení vazby token-žadatel certifikační autoritě elektronicky podepsaným (osobním certifikátem PostSignum) e-mailem:

   Adresát: certifikaty.postsignum@cpost.cz

   Předmět: Zrušení vazby token-žadatel o certifikát

   Tělo: Oznamuji zrušení vazby token-žadatel o certifikát.
   Jméno žadatele: xxx
   Sériová čísla certifikátů uložených na tokenu: xxx