

# Uživatelská příručka

## TokenME Crypto Java Card

Verze 2.1

## Obsah dokumentu

|                                                          |           |
|----------------------------------------------------------|-----------|
| <b>1. Přehled .....</b>                                  | <b>4</b>  |
| <b>2. Co potřebuji? .....</b>                            | <b>5</b>  |
| <b>3. Instalace softwaru .....</b>                       | <b>6</b>  |
| <b>4. Příprava prostředku pro generování klíčů .....</b> | <b>7</b>  |
| 4.1. Změna PINu .....                                    | 8         |
| 4.2. Změna PUKu.....                                     | 8         |
| 4.3. Kontrola servisního klíče .....                     | 9         |
| <b>5. Generování žádosti o prvotní certifikát.....</b>   | <b>10</b> |
| 5.1. Vygenerování žádosti o certifikát .....             | 10        |
| 5.2. Instalace certifikátu v iSignum.....                | 12        |
| 5.3. Instalace certifikátu ze staženého souboru .....    | 14        |
| <b>6. Generování žádosti o následný certifikát .....</b> | <b>17</b> |
| <b>7. Další funkce softwaru Bit4id PKI Manager.....</b>  | <b>19</b> |
| 7.1. Import certifikátu z PKCS#12.....                   | 19        |
| 7.2. Logout .....                                        | 20        |
| 7.3. Refresh .....                                       | 20        |
| 7.4. Export.....                                         | 20        |
| 7.5. Smazat data na prostředku.....                      | 21        |
| 7.6. Odblokování PINu .....                              | 22        |
| 7.7. Náhled certifikátu.....                             | 22        |
| 7.8. Registrace certifikátů .....                        | 22        |
| 7.9. PIN Politika.....                                   | 23        |
| <b>8. Reinicializace prostředku .....</b>                | <b>24</b> |
| 8.1. Výmaz servisního klíče .....                        | 24        |
| 8.2. Předání prostředku jiné osobě .....                 | 24        |
| <b>9. Reklamace .....</b>                                | <b>26</b> |

## 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 |
| 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 |

## 1. Přehled

Zařízení USB token TokenME nebo čipová karta Crypto Java Card (dále jen prostředky) jsou zařízení, které **byly schválené jako kvalifikovaný prostředek pro vytváření elektronických podpisů v souladu s nařízením eIDAS** a slouží k vytváření kvalifikovaných elektronických podpisů. Jsou to PKI zařízení postavené na kryptografickém mikroprocesoru s certifikací Common Criteria EAL4+ a FIPS 140-2 level 3.

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.

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



Obrázek USB tokenu TokenME a čipové karty 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>

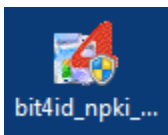
4. V případě čipové karty také čtečku čipových karet a ovladač ke čtečce čipových karet  
Čtečku je nutné mít připojenou k počítači, např. pomocí USB portu nebo jinou technologií, kterou čtečka podporuje. Čtečka může být také integrovaná přímo v počítači.  
Před započítím instalace softwaru je nutné, aby byla čtečka čipových karet v počítači nainstalována a byla funkční.



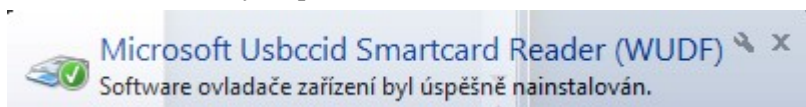
### 3. Instalace softwaru

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 nainstalován.



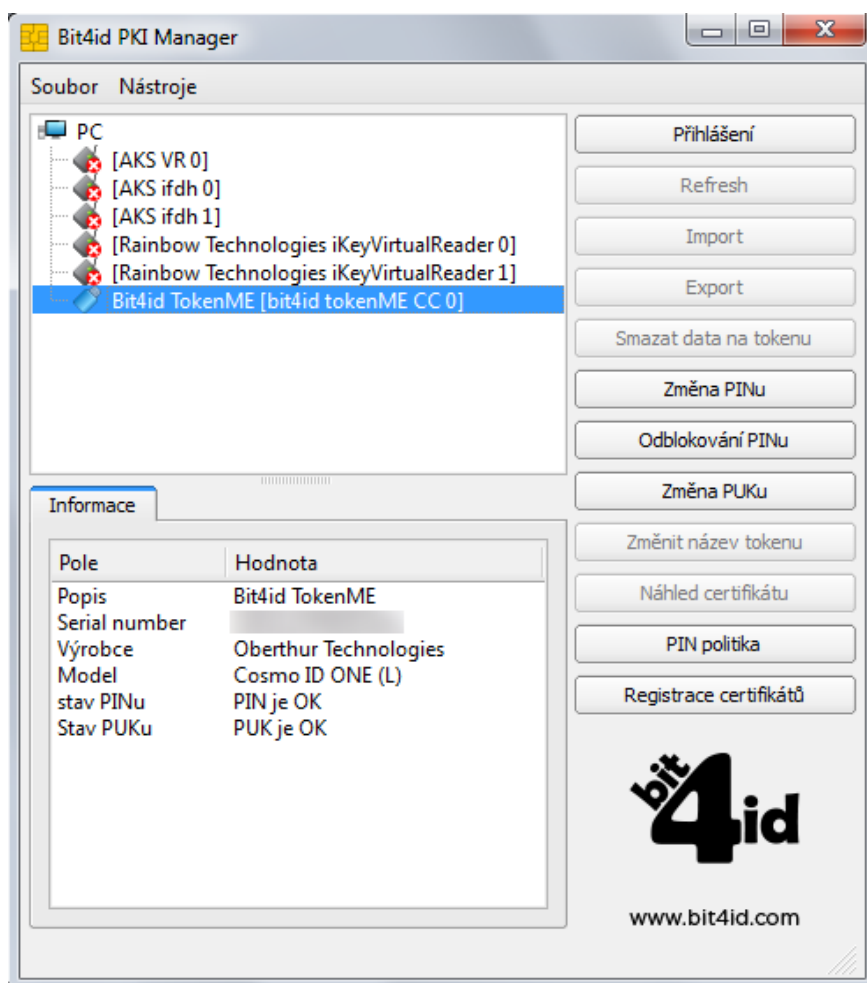
### Knihovna PKCS#11

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*.

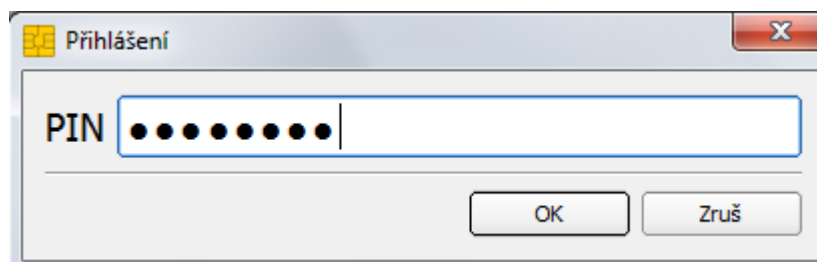
## 4. Příprava prostředku pro generování klíčů

Před prvním použitím 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.

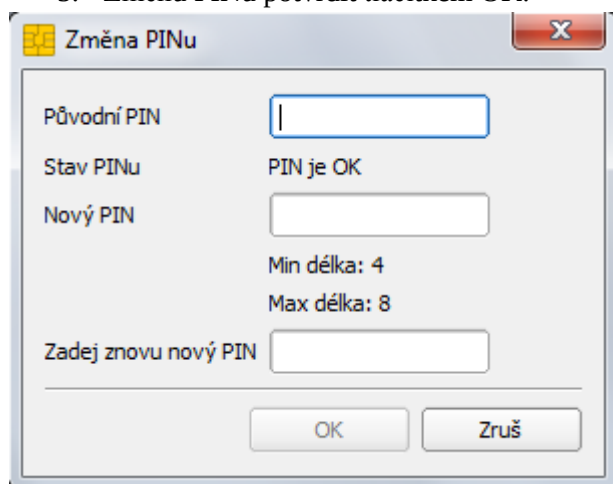


Před dalšími kroky je potřeba se k prostředku přihlásit tlačítkem *Přihlášení* a zadat přednastavený PIN: **12345678**



## 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.



**Změna PINu**

Původní PIN

Stav PINu PIN je OK

Nový PIN

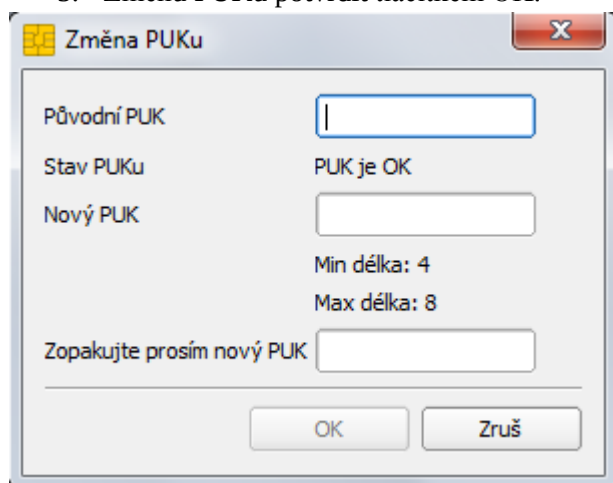
Min délka: 4  
Max délka: 8

Zadej znovu nový PIN

OK Zruš

## 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.



**Změna PUKu**

Původní PUK

Stav PUKu PUK je OK

Nový PUK

Min délka: 4  
Max délka: 8

Zopakujte prosím nový PUK

OK Zruš

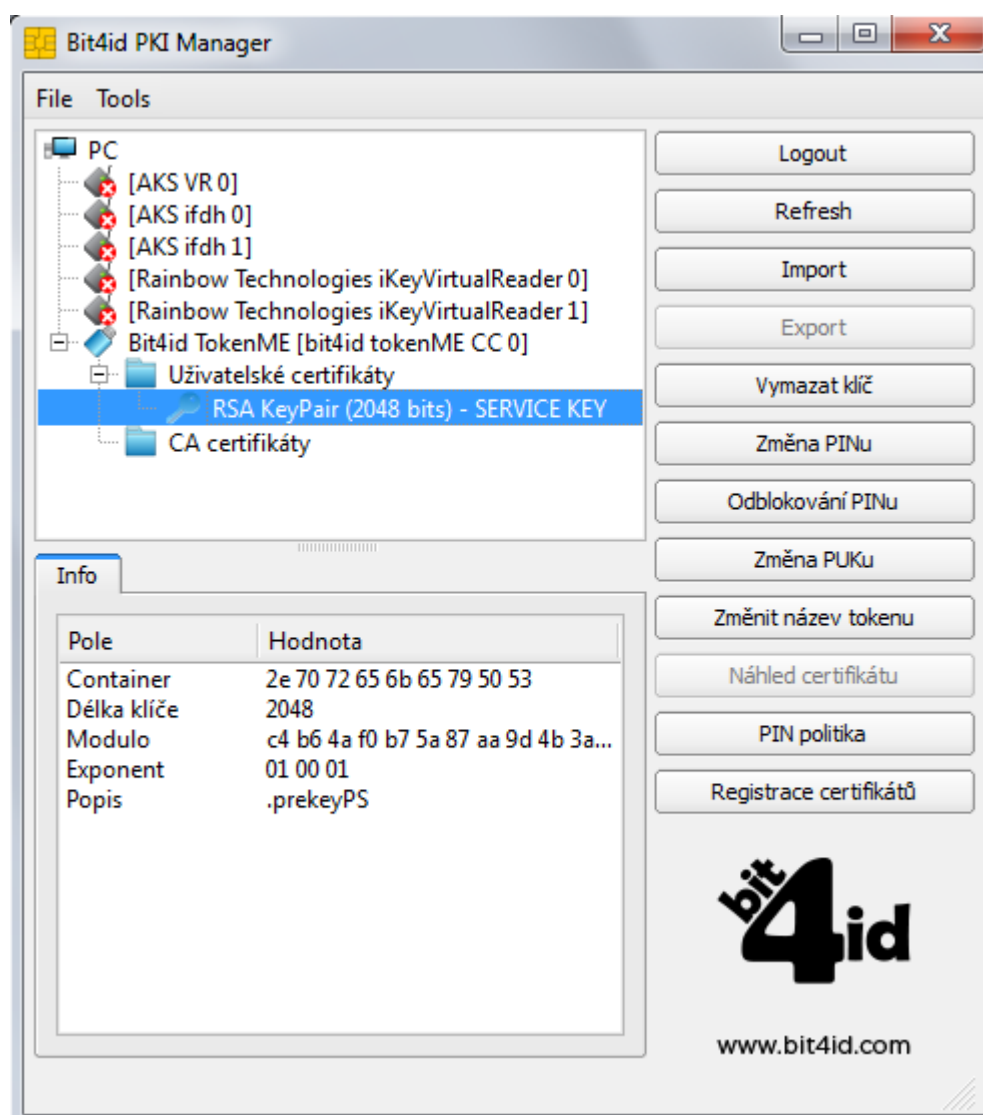
**Upozorňujeme, že při zablokování PIN i PUK  
dojde ke znehodnocení prostředku.**

### 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

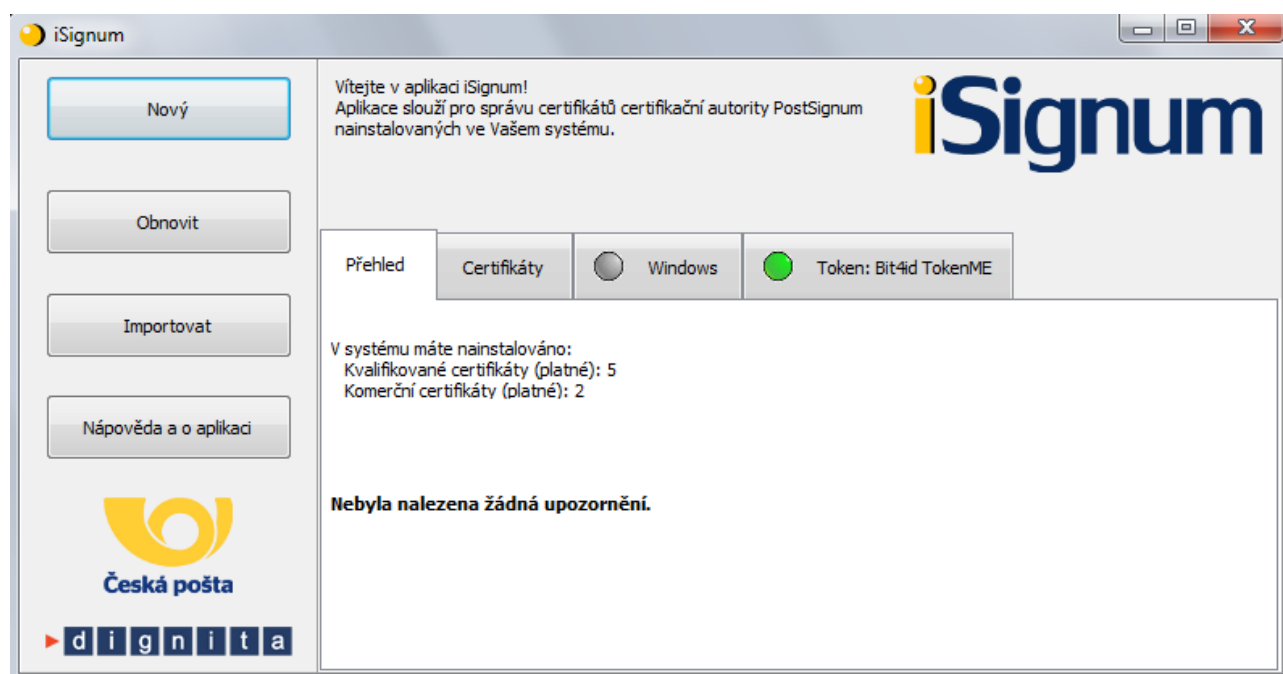
Generování klíčů na prostředek a žádosti o kvalifikovaný certifikát, který bude obsahovat příznak QESCD, je možné pouze v programu **iSignum**, který zajistí vytvoření správné žádosti o certifikát. Pokud bude ke generování žádosti využit jiný program, není možné do certifikátu příznak QESCD vložit.

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.

**Průvodce vygenerováním žádosti o certifikát PostSignum**

Tento průvodce Vás provede procesem vygenerování žádosti o certifikát PostSignum. Průvodce nejprve vygeneruje klíčový pár ve zvoleném úložišti a vygeneruje žádost o vystavení certifikátu pro tento pár. Následně žádost odešle na server PostSignum. Je vyžadováno připojení k internetu.

**Krok 1: Vyplnění základních informací**

Typ certifikátu: Kvalifikovaný certifikát (QCA)

Jméno:

Email:

Tyto informace jsou nepovinné a slouží pro lepší dohledání žádosti na pobočce.

☒ Po odeslání vytisknout souhrnné informace  
☐ Zálohovat privátní klíč (pokud to umožňuje vybrané úložiště)

**Krok 2: Výběr úložiště pro generování klíčů**

Bit4id TokenME ( )

Byl vybrán kvalifikovaný prostředek

**Krok 3: Generování a odeslání žádosti na server PostSignum**

Souhrn:

Odeslat žádost Zavřít

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.

**Krok 3: Generování a odeslání žádosti na server PostSignum**

Souhrn: ID žádosti o certifikát: **BP5638412975**

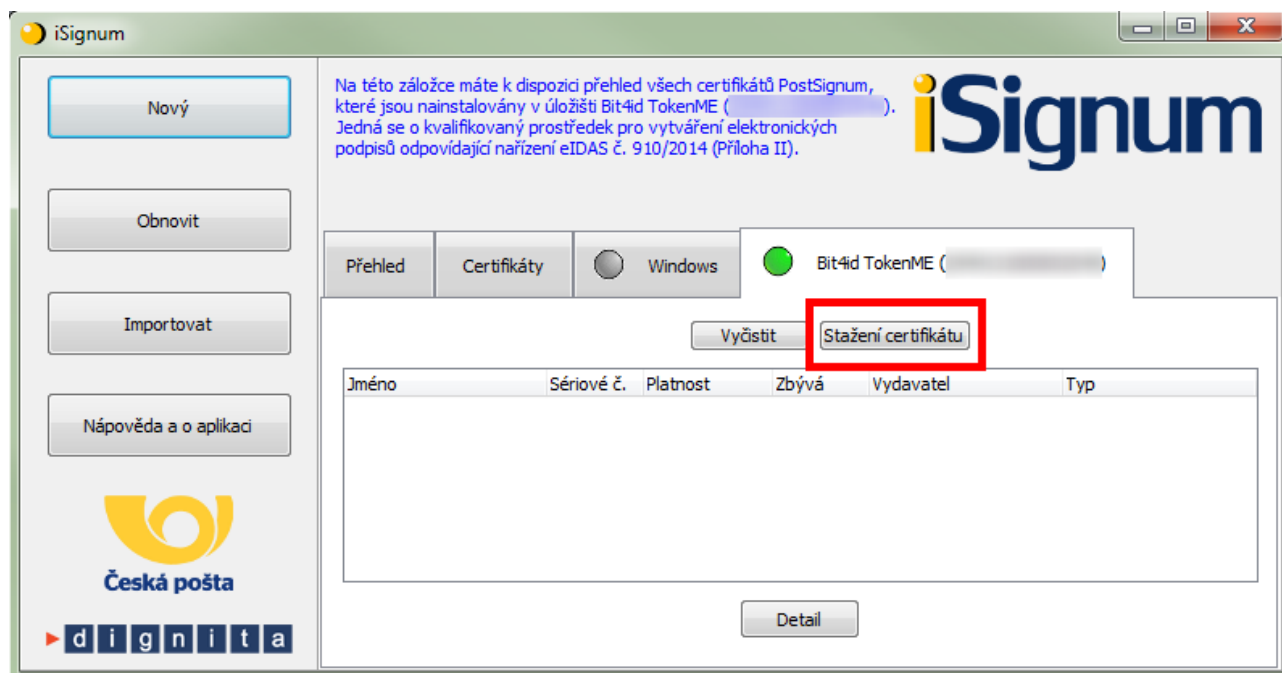
Toto ID je nutné předložit spolu s dalšími náležitostmi na pobočce České pošty. Postup, jak získat certifikát je na webových stránkách PostSignum:

[http://www.postsignum.cz/postup\\_pro\\_ziskani\\_certifikatu.html](http://www.postsignum.cz/postup_pro_ziskani_certifikatu.html)

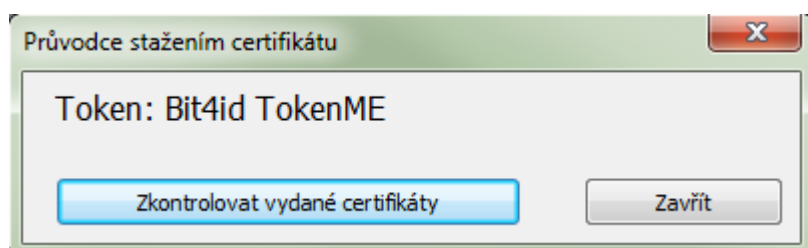
## 5.2. Instalace certifikátu v iSignum

Instalaci přímo do prostředku lze provést pouze v programu iSignum:

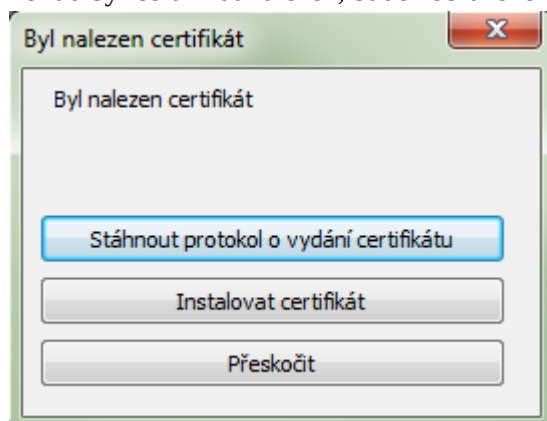
1. Vložit prostředek do USB portu počítače nebo do čtečky.
2. V programu iSignum stisknout tlačítko *Stážení certifikátu*.



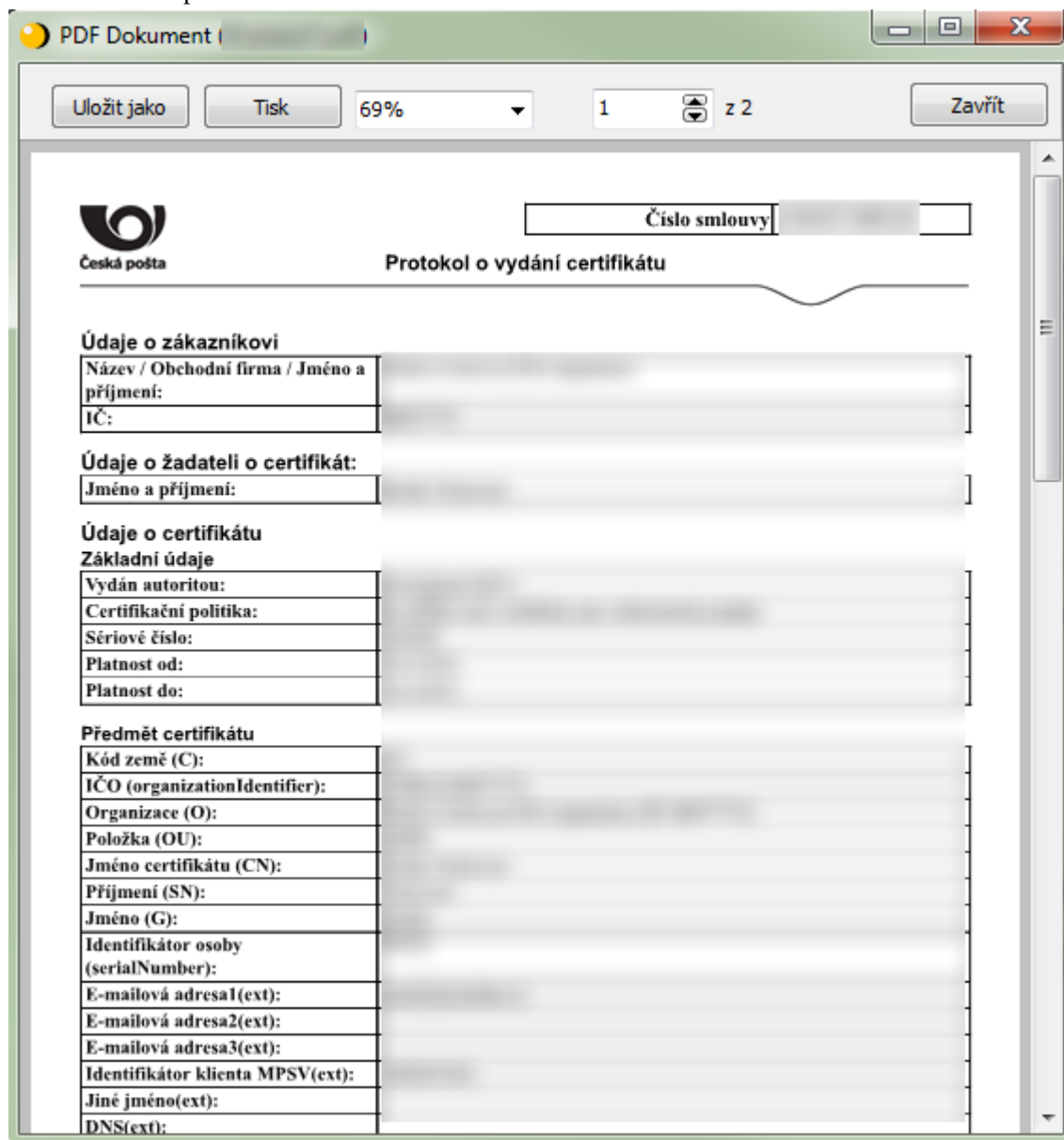
3. Stiskem tlačítka *Zkontrolovat vydané certifikáty* ověřit, zda je již certifikát připraven k instalaci.



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*.



**PDF Dokument** ( )

Uložit jako Tisk 69% 1 z 2 Zavřít

**Česká pošta** **Číslo smlouvy**

**Protokol o vydání certifikátu**

**Údaje o zákazníkovi**

|                                            |  |
|--------------------------------------------|--|
| Název / Obchodní firma / Jméno a příjmení: |  |
| IČ:                                        |  |

**Údaje o žadateli o certifikát:**

|                   |  |
|-------------------|--|
| Jméno a příjmení: |  |
|-------------------|--|

**Údaje o certifikátu**

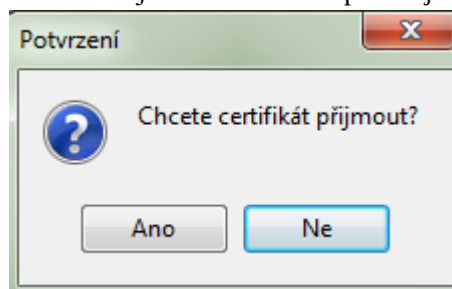
**Základní údaje**

|                        |  |
|------------------------|--|
| Vydán autoritou:       |  |
| Certifikační politika: |  |
| Sériové číslo:         |  |
| Platnost od:           |  |
| Platnost do:           |  |

**Předmět certifikátu**

|                                     |  |
|-------------------------------------|--|
| Kód země (C):                       |  |
| IČO (organizationIdentifier):       |  |
| Organizace (O):                     |  |
| Položka (OU):                       |  |
| Jméno certifikátu (CN):             |  |
| Příjmení (SN):                      |  |
| Jméno (G):                          |  |
| Identifikátor osoby (serialNumber): |  |
| E-mailová adresa1(ext):             |  |
| E-mailová adresa2(ext):             |  |
| E-mailová adresa3(ext):             |  |
| Identifikátor klienta MPSV(ext):    |  |
| Jiné jméno(ext):                    |  |
| DNS(ext):                           |  |

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

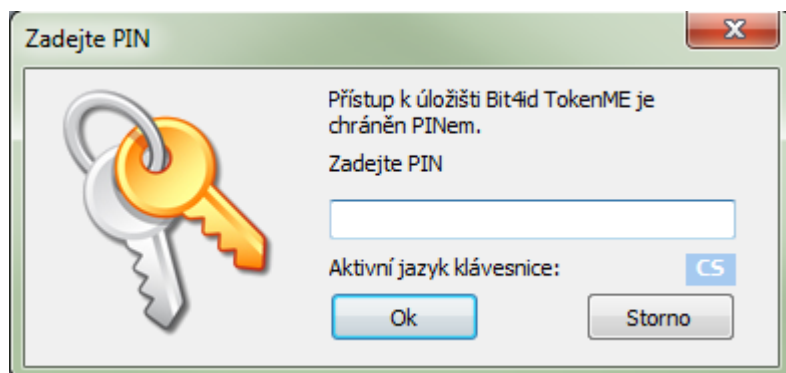


**Potvrzení**

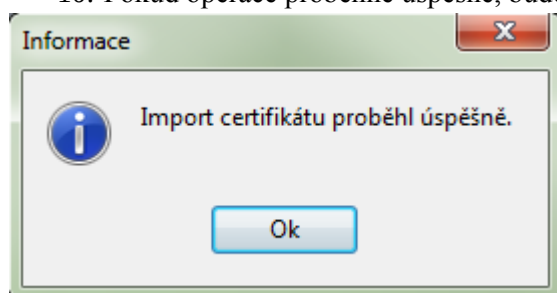
Chcete certifikát přijmout?

Ano Ne

9. Zadat PIN

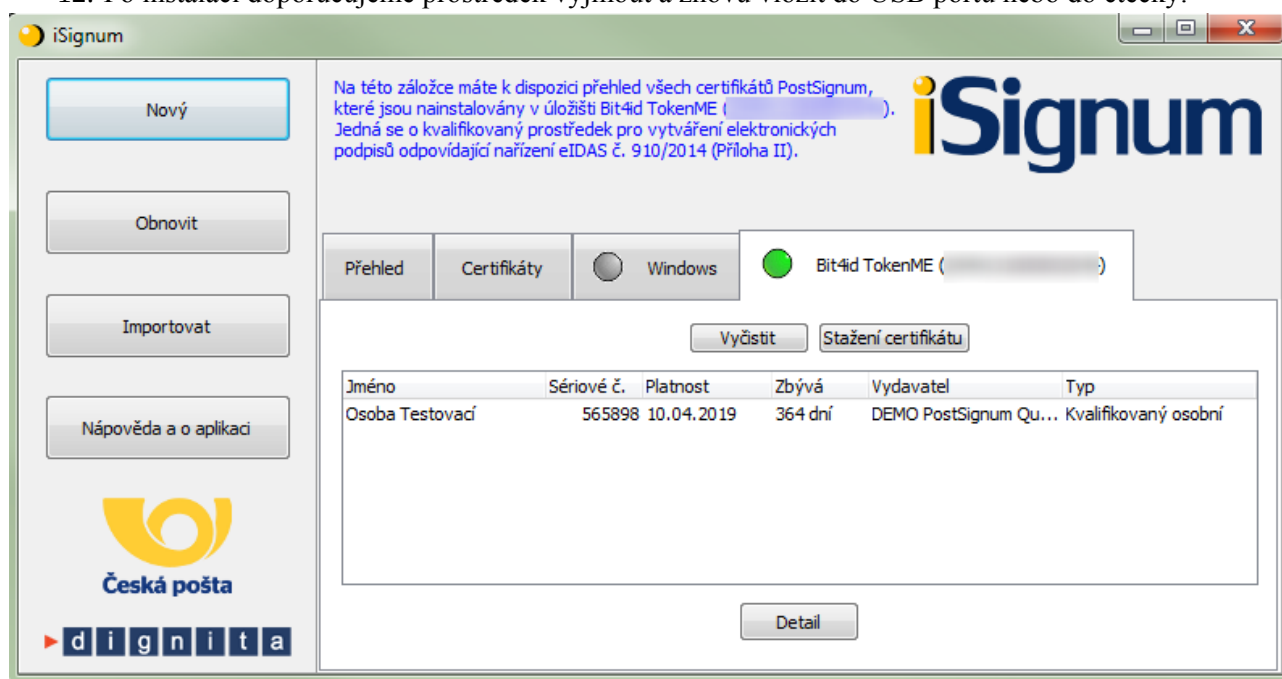


10. Pokud operace proběhne úspěšně, bude zobrazena hláška:



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.

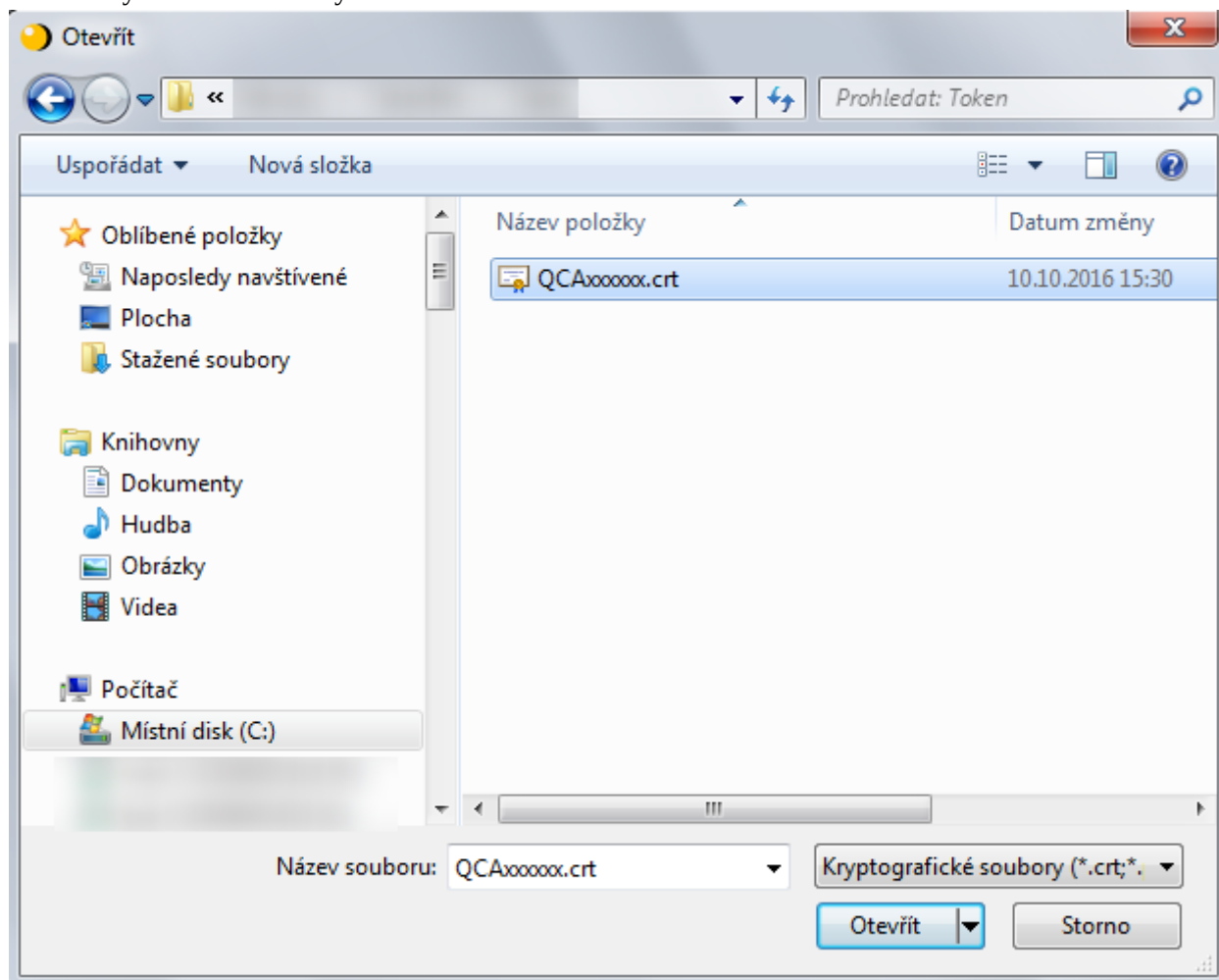


### 5.3. Instalace certifikátu ze staženého souboru

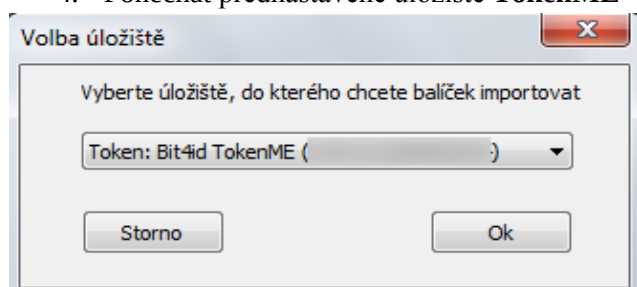
Instalaci certifikátu doporučujeme provést taktéž v programu iSignum:

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

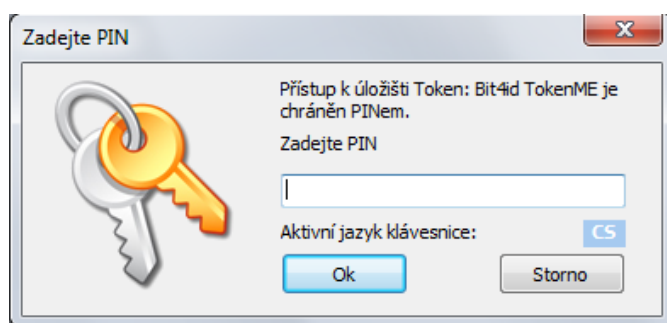
### 3. Vybrat kvalifikovaný certifikát



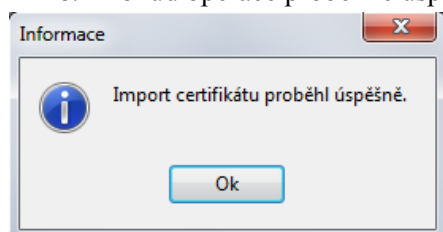
### 4. Ponechat přednastavené úložiště **TokenME**



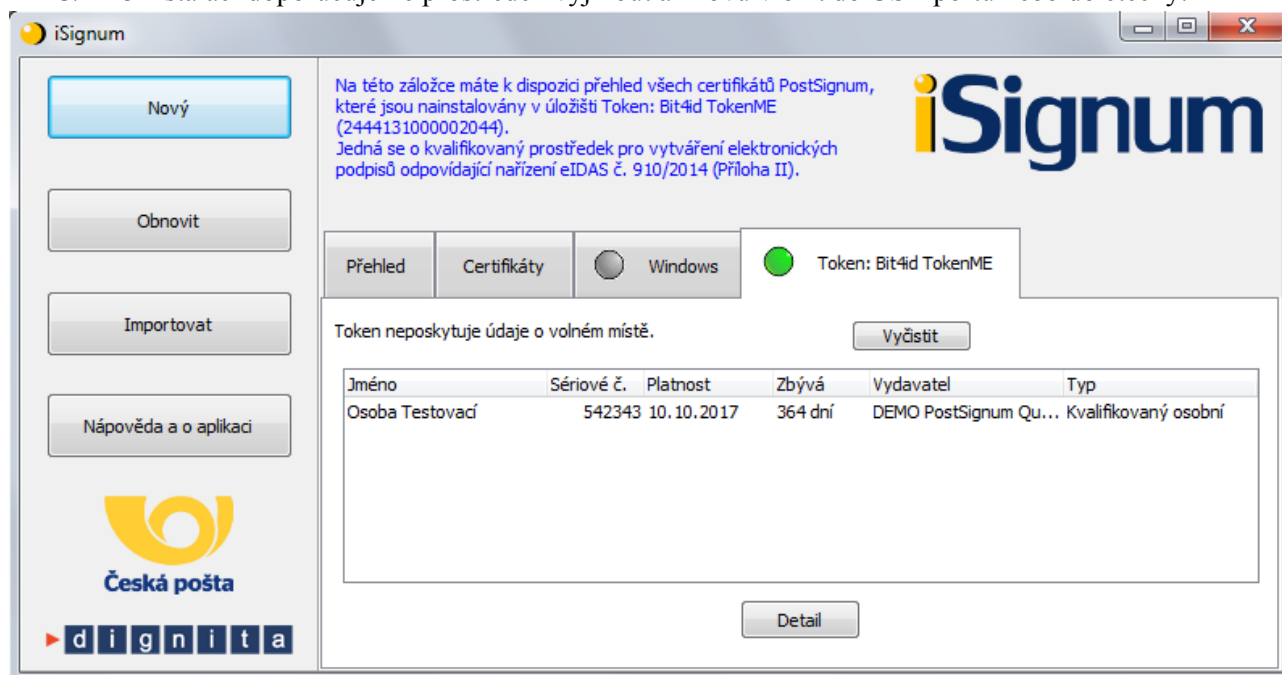
### 5. Pro import certifikátu bude vyžadován PIN



6. Pokud operace proběhne úspěšně, bude zobrazena hláška:

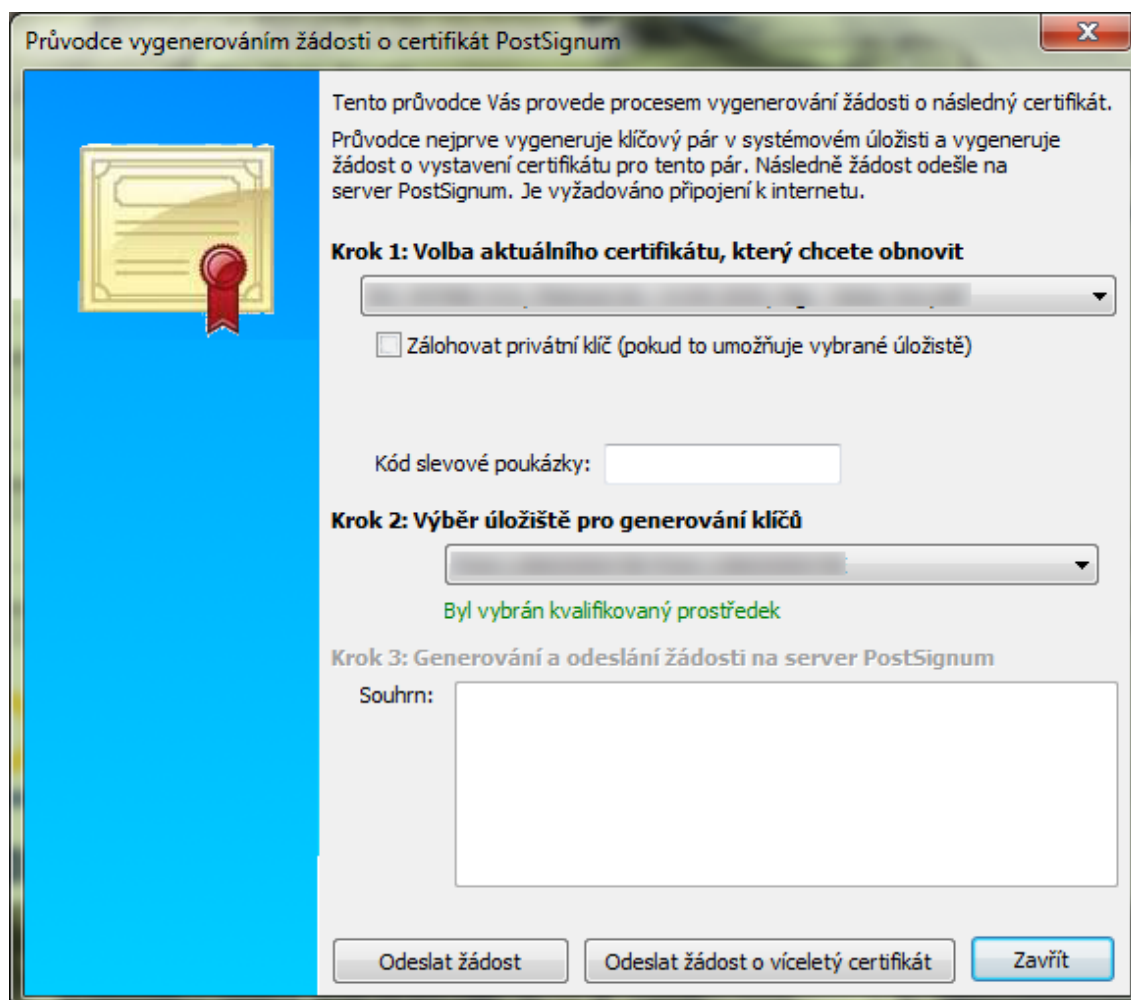


7. Po úspěšném importu bude certifikát vidět v programu iSignum na záložce **TokenME**.
8. Po instalaci doporučujeme prostředek vyjmout a znovu vložit do USB portu nebo do čtečky.



## 6. Generování žádosti o následný certifikát

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*.



Průvodce vygenerováním žádosti o certifikát PostSignum

Tento průvodce Vás provede procesem vygenerování žádosti o následný certifikát. Průvodce nejprve vygeneruje klíčový pár v systémovém úložišti a vygeneruje žádost o vystavení certifikátu pro tento pár. Následně žádost odešle na server PostSignum. Je vyžadováno připojení k internetu.

**Krok 1: Volba aktuálního certifikátu, který chcete obnovit**

[Dropdown menu]

☐ Zálohovat privátní klíč (pokud to umožňuje vybrané úložiště)

Kód slevové poukázky: [Text box]

**Krok 2: Výběr úložiště pro generování klíčů**

[Dropdown menu]

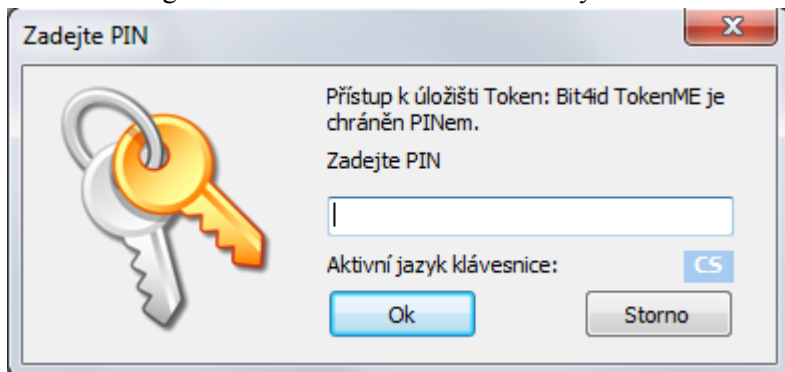
Byl vybrán kvalifikovaný prostředek

**Krok 3: Generování a odeslání žádosti na server PostSignum**

Souhrn: [Text area]

[Odeslat žádost] [Odeslat žádost o víceletý certifikát] [Zavřít]

6. Před generováním klíčů a žádosti bude vyžadován PIN.

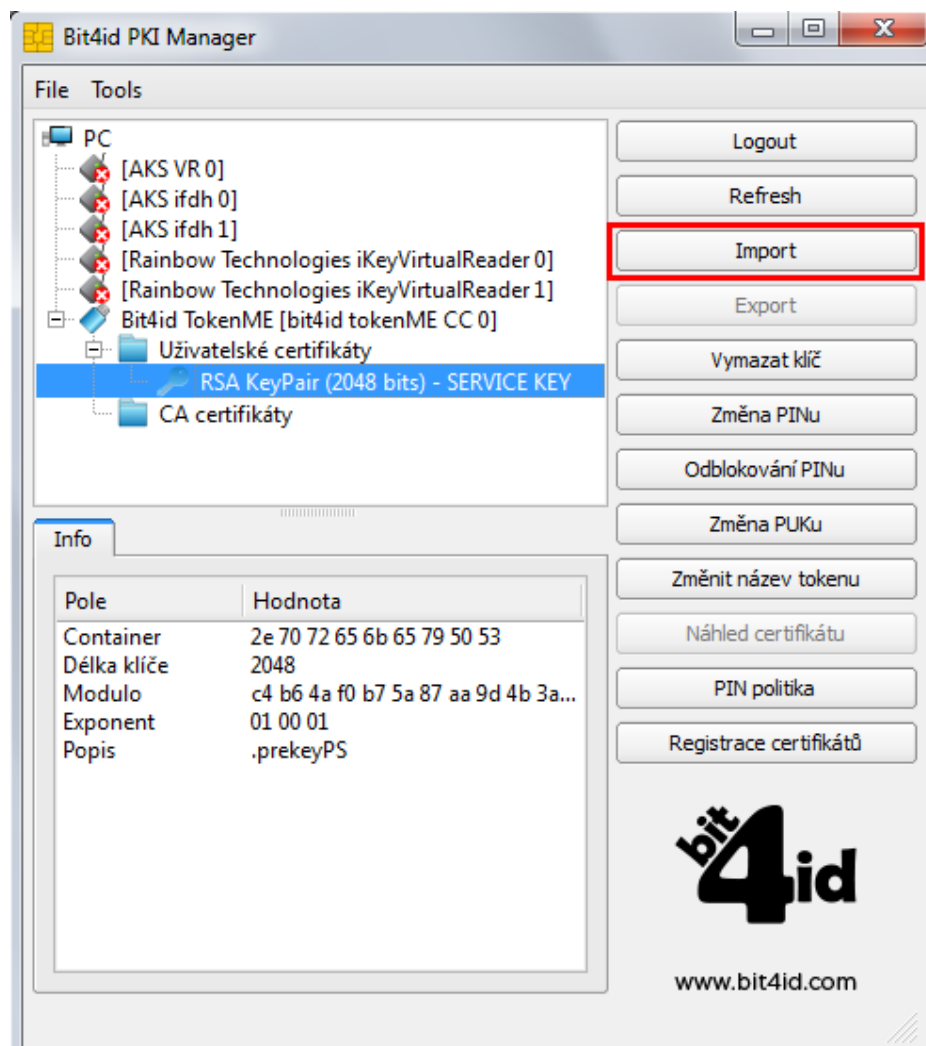


7. Po vygenerování klíčů a žádosti o certifikát bude navázána komunikace se systémem certifikační autority a za pomoci servisního klíče dojde k autentizaci prostředku do systému a bezpečnému předání žádosti o certifikát. Při zpracování žádosti o následný certifikát je navíc provedena kontrola vazby *prostředek-žadatel*.
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 5.2. nebo 5.3.

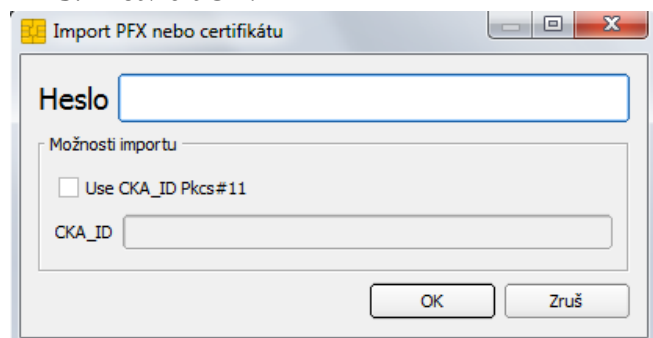
## 7. Další funkce softwaru Bit4id PKI Manager

### 7.1. Import certifikátu z PKCS#12

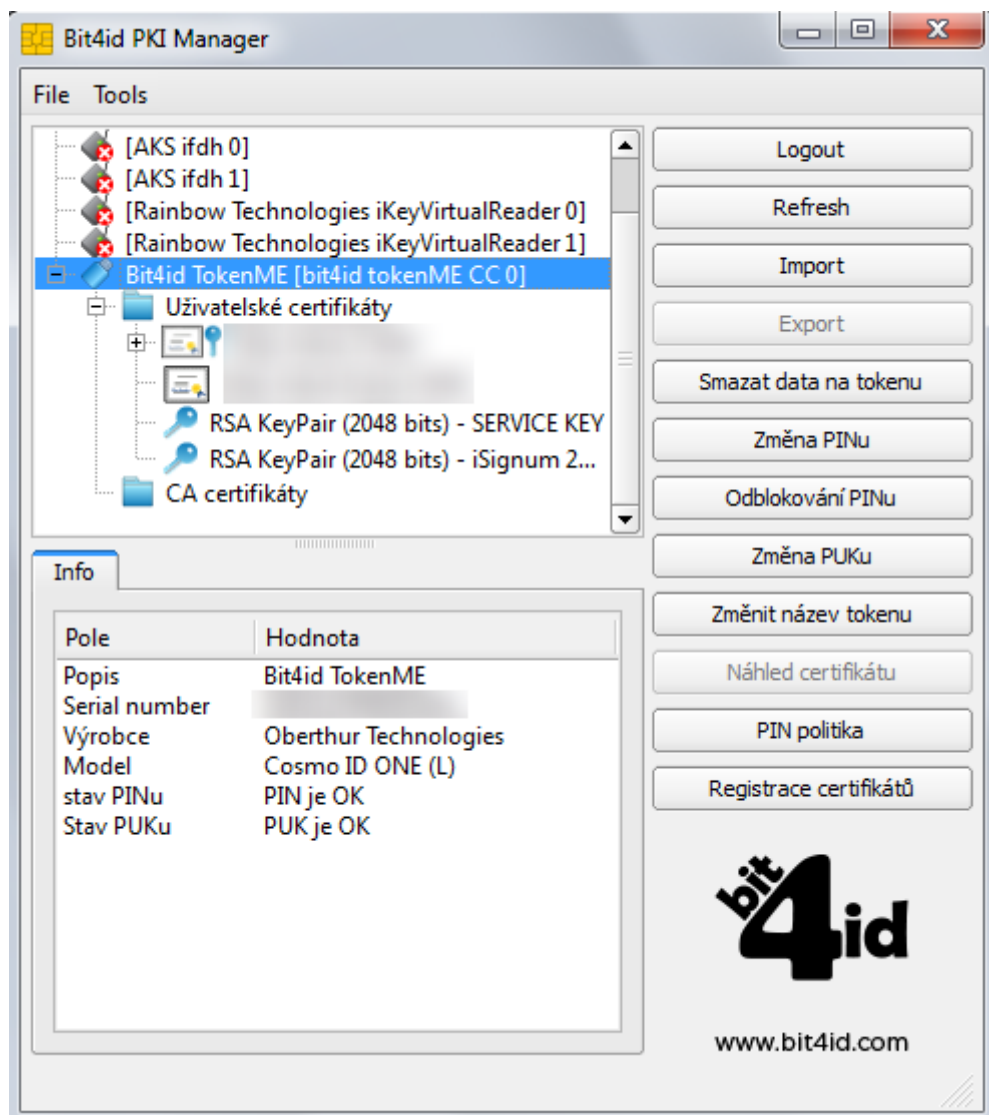
Vložení certifikátů ze zálohy (PFX nebo P12) do prostředí se provede kliknutím na tlačítko Import.



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

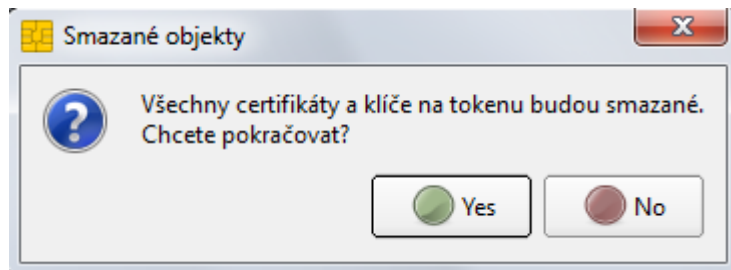
Po stisku tlačítka dojde k obnovení zobrazených informací na prostředku.

## 7.4. Export

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

## 7.5. Smazat data na prostředku

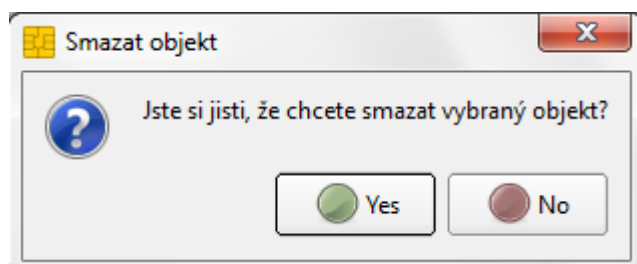
A. Tato volba je dostupná, pokud je kurzor nastaven na objektu prostředku.



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

**TUTO VOLBU NEDOPORUČUJEME SPOUŠTĚT!**

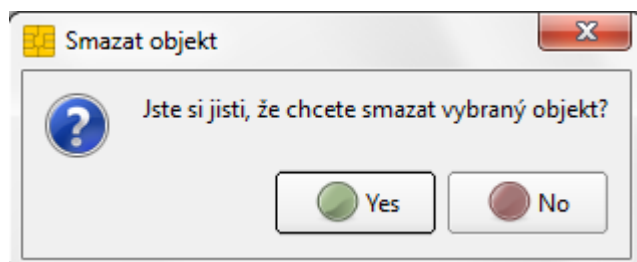
B. Pokud je kurzor nastaven na objektu typu RSA KeyPair, v menu se zobrazí volba **Vymazat klíč**.



**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**.



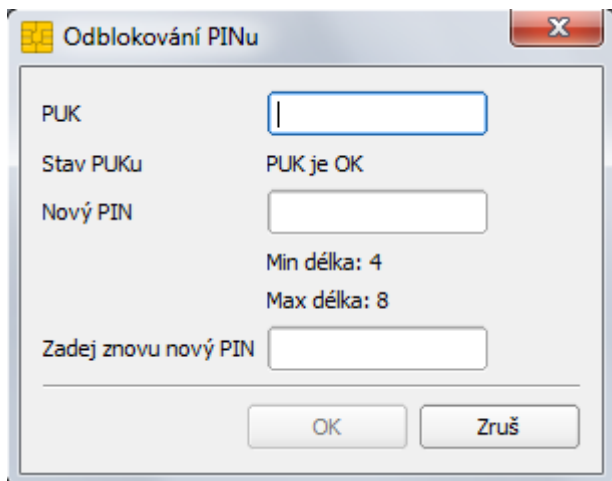
**Pokud dojde k výmazu certifikátu, bude smazán i jemu odpovídající klíč a nebude možné nadále certifikát používat.**

**TUTO VOLBU NEDOPORUČUJEME SPOUŠTĚT!**

**K výmazu dat na prostředku doporučujeme používat výhradně aplikaci iSignum.**

## 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.

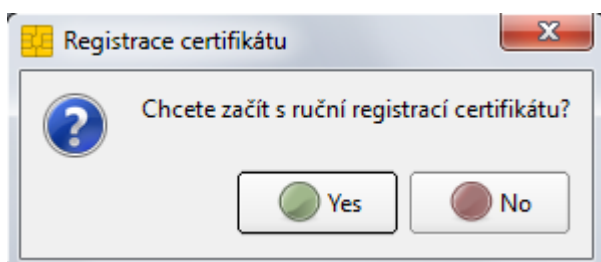


**Upozorňujeme, že při zablokování PIN i PUK  
dojde ke znehodnocení prostředku.**

## 7.7. Náhled certifikátu

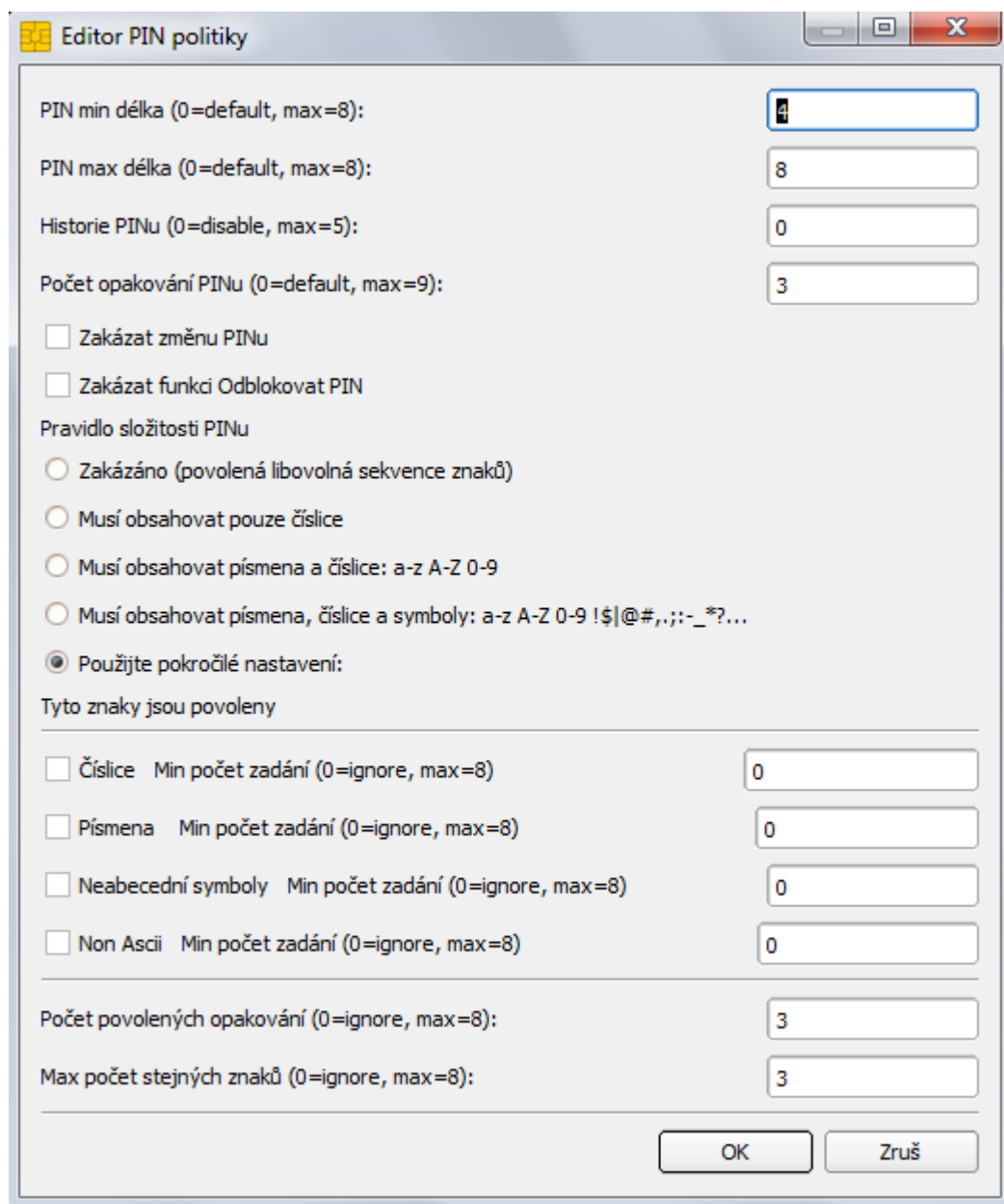
Dojde k zobrazení detailu vybraného certifikátu.

## 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



**Editor PIN politiky**

PIN min délka (0=default, max=8):

PIN max délka (0=default, max=8):

Historie PINu (0=disable, max=5):

Počet opakování PINu (0=default, max=9):

☐ Zakázat změnu PINu

☐ Zakázat funkci Odblokovat PIN

Pravidlo složitosti PINu

☐ Zakázáno (povolená libovolná sekvence znaků)

☐ Musí obsahovat pouze číslice

☐ Musí obsahovat písmena a číslice: a-z A-Z 0-9

☐ Musí obsahovat písmena, číslice a symboly: a-z A-Z 0-9 !\$|@#.,,:-\_\*?...

☒ Použijte pokročilé nastavení:

Tyto znaky jsou povoleny

☐ Číslice Min počet zadání (0=ignore, max=8)

☐ Písmena Min počet zadání (0=ignore, max=8)

☐ Neabecední symboly Min počet zadání (0=ignore, max=8)

☐ Non Ascii Min počet zadání (0=ignore, max=8)

Počet povolených opakování (0=ignore, max=8):

Max počet stejných znaků (0=ignore, max=8):

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.



**Přihlášená osoba**

Jméno: [redacted]  
Číslo smlouvy: [redacted]

[Odhlásit](#) | [Přístupové údaje](#)

**Navigace**

- Časová razítka
- Balíčky časových razítek
- Certifikáty
  - Statistiky certifikátů
  - Přehledy
  - Správa žadatelů
    - Zneplatnění certifikátu
    - Zavedení nového žadatele o certifikát
    - Nové údaje pro vydání certifikátu již zavedeného žadatele
    - Změna údajů zavedeného žadatele o certifikát
    - Blokace zavedeného žadatele
    - Zrušení vazby osoba-kvalifikovaný prostředek**
    - Komerční doménový certifikát
    - Ověření identity osoby

**Zrušení vazby osoba/kvalifikovaný prostředek**

» Úvodní stránka » Certifikáty » Správa žadatelů » Zrušení vazby osoba-kvalifikovaný prostředek

Jméno žadatele:

Číslo zaměstnance:

Číslo bezpečného prostředku:



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

Přihlášená osoba  
Jméno:   
Číslo smlouvy:   
Odhlásit | Přístupové údaje

» Úvodní stránka » Certifikáty » Správa žadatelů » Zrušení vazby osoba-kvalifikovaný prostředek

### Zrušení vazby osoba/kvalifikovaný prostředek

Jméno žadatele:   
Číslo zaměstnance:   
Číslo bezpečného prostředku:   
Vyhledat žadatele

Detail žadatele o certifikát | číslo smlouvy:   

|                             |       |
|-----------------------------|-------|
| Jméno                       |       |
| Číslo zaměstnance           | 11192 |
| Číslo bezpečného prostředku |       |

Odeslat požadavek na zrušení vazby  
Zpět

Časová razítka  
Balíčky časových razítek  
Certifikáty  
Statistiky certifikátů  
Přehledy  
Správa žadatelů  
Zneplatnění certifikátu  
Zavedení nového žadatele o certifikát  
Nové údaje pro vydání certifikátu již zavedeného žadatele  
Změna údajů zavedeného žadatele o certifikát  
Blokace zavedeného žadatele  
Zrušení vazby osoba-kvalifikovaný prostředek  
Komerční doménový certifikát

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](mailto: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](http://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.