



Identifikace	Číslo jednací		
Nahrazuje	Klasifikace	veřejné	
Platnost	1.7. 2026	Účinnost	1.7. 2026

Uživatelská příručka

TokenME EVO

Verze 3.6

Obsah dokumentu

1. Přehled	4
2. Co potřebuji?	5
3. Instalace softwaru	6
4. Příprava prostředku pro generování klíčů	8
4.1. Změna PINu	9
4.2. Změna PUK.....	9
4.3. Kontrola servisního klíče	10
4.4. Podpora klíčů o velikosti 4096 bitů.....	10
4.5. Expertní mód aplikace iSignum	10
5. Generování žádosti o prvotní certifikát.....	13
5.1. Vygenerování žádosti o certifikát	13
5.2. Instalace certifikátu v iSignum.....	15
5.3. Instalace certifikátu ze staženého souboru	18
6. Generování žádosti o následný certifikát	20
7. Další funkce softwaru Bit4id PKI Manager.....	22
7.1. Import certifikátu z PKCS#12.....	22
7.2. Odhlášení.....	23
7.3. Obnovte obsah.....	23
7.4. Přejmenujte zařízení.....	23
7.5. Odstranění dat	24
7.5.1. Odstranění certifikátu.....	24
7.5.2. Odstranění klíče	25
7.6. Odemknout PIN	25
7.7. Náhled certifikátu.....	26
7.8. Otevřít Správce certifikátů systému Windows.....	27
7.9. Nastavení.....	27
8. Reinicializace prostředku	28
8.1. Výmaz servisního klíče	28
8.2. Předání prostředku jiné osobě	28
9. Reklamacce	30

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 TokenME EVO	Česká pošta, s.p.	Manažer CA
3.3	22. 10. 2022	přidány informace o certifikaci prostředků a popis ID žádostí KC	Česká pošta, s.p.	Manažer CA
3.4	16. 2. 2023	změna v souvislosti s novou verzí iSignum	Česká pošta, s.p.	Manažer CA
3.5	24. 4. 2026	Ponechány pouze prostředky s platnou certifikací TokenME EVO	Česká pošta, s.p.	Manažer CA
3.6	1. 7. 2026	úprava manuálu dle nového middlewaru	Česká pošta, s.p.	Manažer CA

1. Přehled

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

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.

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/ SERVISNÍ KLÍČ**“. 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 (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 nezbytné postupovat dle kapitoly 8.2

2. Co potřebuji?

1. PC s operačním systémem Windows



2. USB token TokenME EVO



3. Software



Software je ke stažení na webových stránkách PostSignum:

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

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.

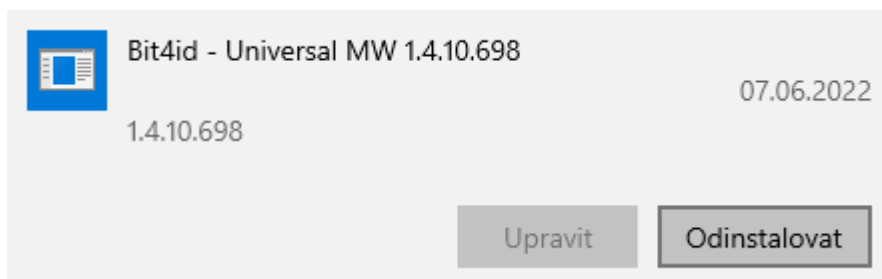
3. Instalace softwaru

Pokud máte již z minulosti instalovanou předcházející verzi ovladače Bit4id, je nezbytné nejprve provést odinstalaci a restart Vašeho PC. Teprve poté je možné zahájit novou instalaci aktuální verze.

Pro odinstalování můžete využít ve složce middlewaru volbu „Uninstall“ pomocí průvodce, případně pomocí odebrání programů správce Windows

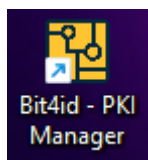


nebo



Ke správné instalaci softwaru je potřeba vykonat následující kroky:

1. Otevřít aplikaci bit4id_xpki_admin_xxx.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. 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.

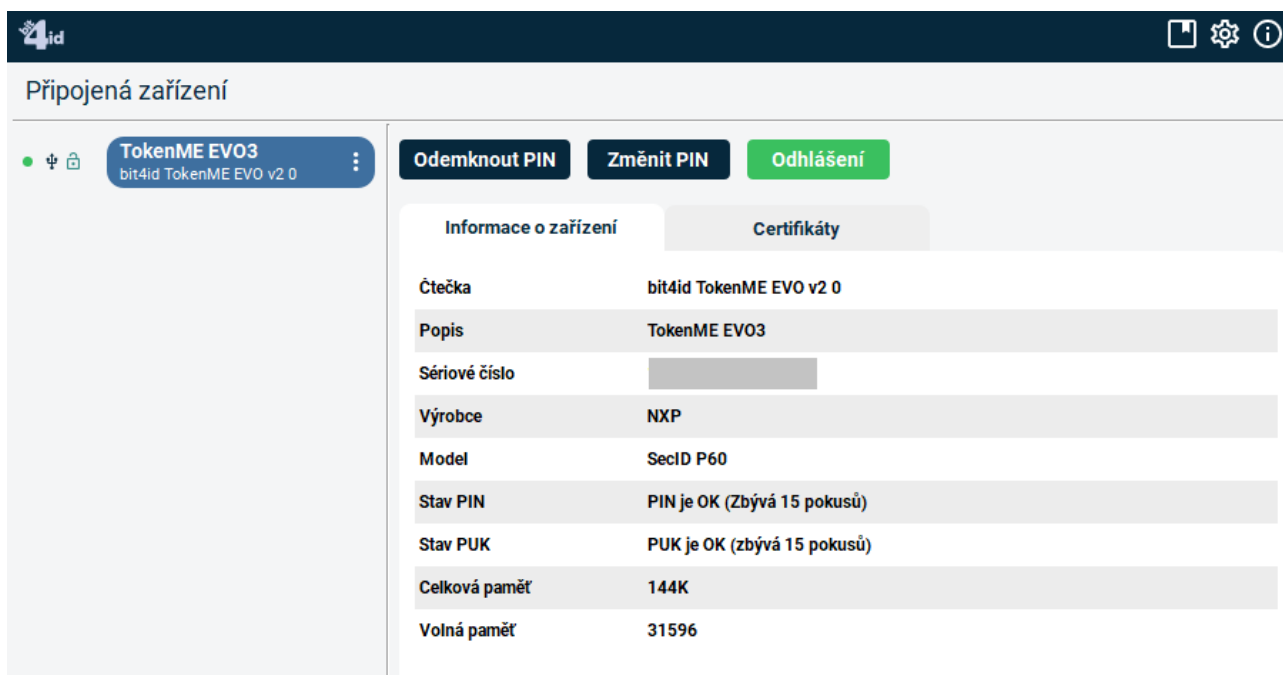
Knihovna PKCS#11

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*.

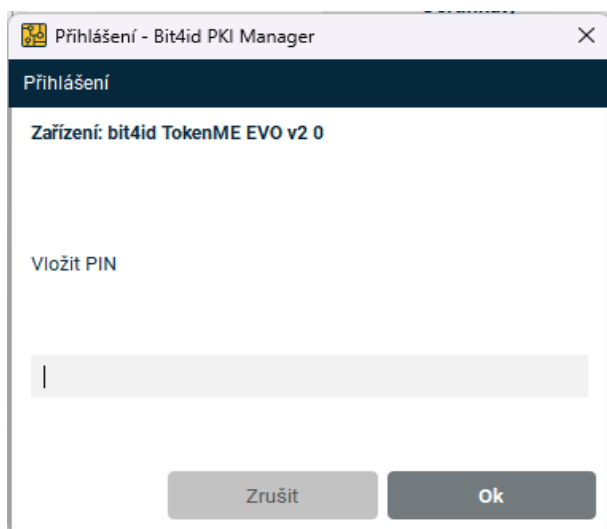
4. Příprava prostředku pro generování klíčů

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.

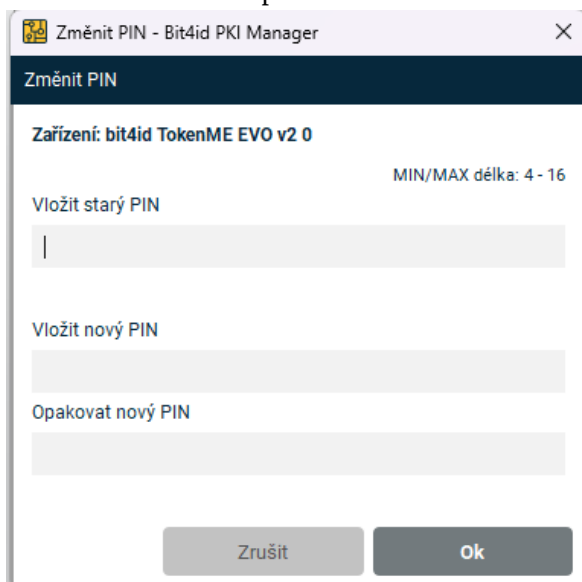


Před dalšími kroky je možné se k prostředku přihlásit tlačítkem *Přihlášení* a zadat přednastavený PIN: **12345678**



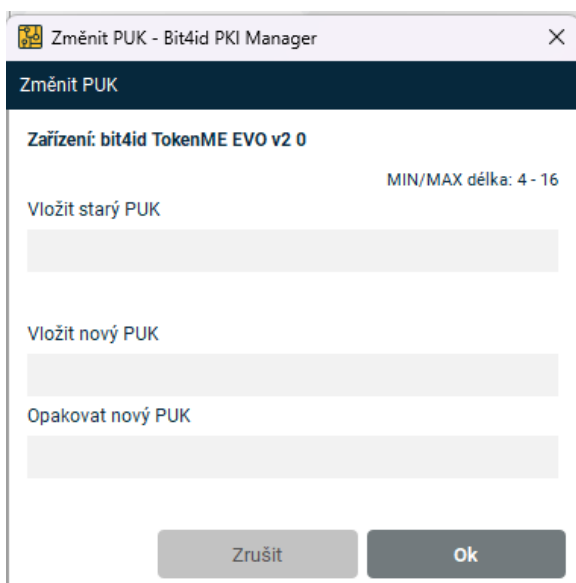
4.1. Změna PINu

1. V PKI Manageru kliknout na tlačítko *Změnit PIN*.
2. Do políčka *Vložit starý PIN* zadat: **12345678**.
3. Do políčka *Vložit nový PIN* zapsat nový PIN, který musí mít **min. 4 znaky** a **maximálně 8 znaků**.
4. Do políčka *Opakovat nový PIN* zopakovat nový PIN.
5. Změnu PINu potvrdit tlačítkem OK.



4.2. Změna PUK

1. Pro zobrazení volby *Změnit PUK* stiskněte CTRL + A.
2. V PKI Manageru je přidáno tlačítko s volbou, kliknout na volbu *Změnit PUK*.
3. Do políčka *Vložit starý PUK* zadat: **87654321**.
4. Do políčka *Vložit nový PUK* zapsat nový PUK, který musí mít min. 4 znaky a maximálně 8 znaků.
5. Do políčka *Opakovat nový PUK* zopakovat nový PUK.
6. Změnu PUKu potvrdit tlačítkem OK.



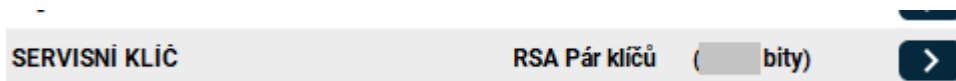
**Upozorňujeme, že při zablokování PIN i PUK
dojde ke znehodnocení prostředku.**

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 po přihlášení v záložce Certifikáty - *Uživatelské certifikáty*.

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



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

4.4. Podpora klíčů o velikosti 4096 bitů

Velikost 4096 bitů podporují tokeny TokenME EVO s platností certifikace do 22.07.2030 a pozdější verze. Maximální možná velikost klíče je zobrazena v aplikaci iSignum při generování žádosti o nový certifikát nebo o obnovu certifikátu.

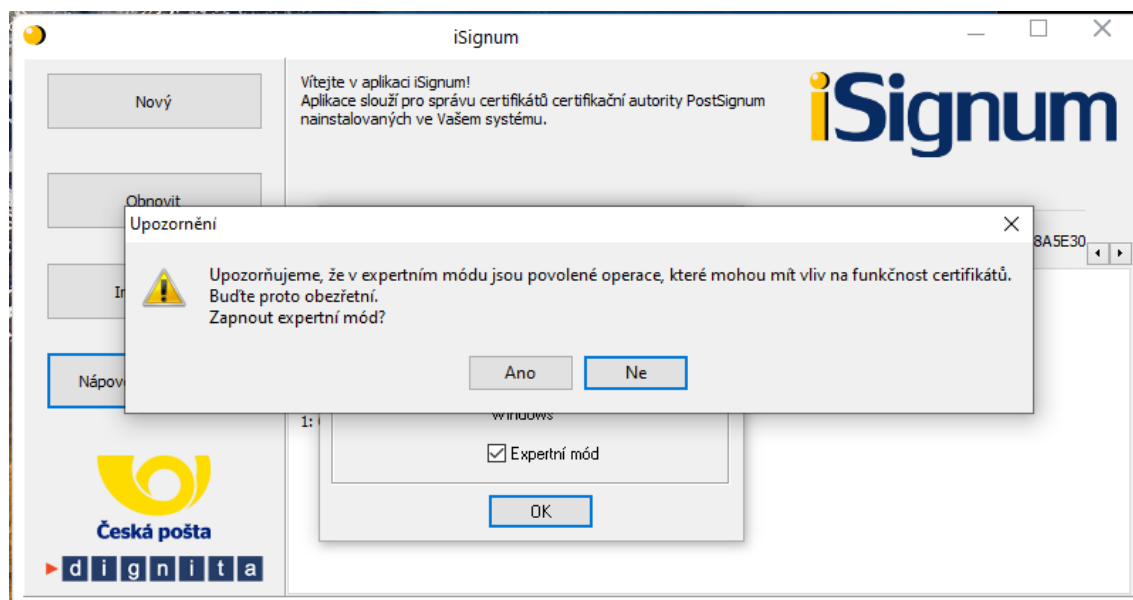
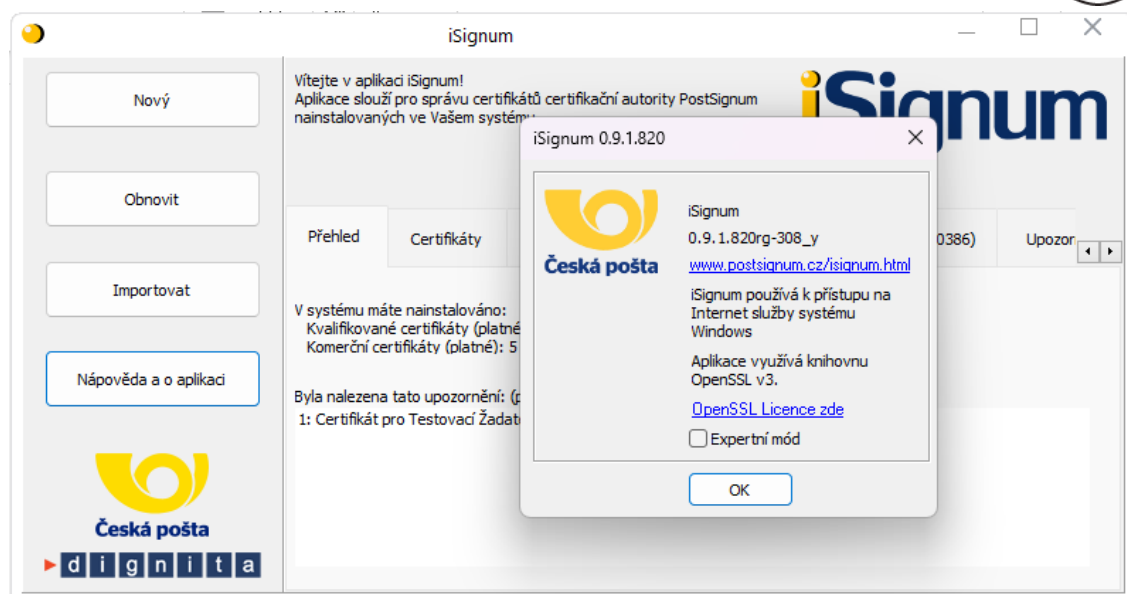
Upozorňujeme, že generování klíče o velikosti 4096 bitů může trvat i několik minut.

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 přednastavena velikost klíče 4096 bitů RSA a v expertním módu jsou v nabídce klíče různé velikosti ECDSA.
- 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.



Změna klíče v expertním módu:



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:

Mobilní telefonní číslo: +420

Tyto informace jsou nepovinné a slouží pro ověření uložené žádosti před vydáním certifikátu žadatelem o certifikát. Informace o generované žádosti o certifikát je zasílána výhradně prostřednictvím SMS na mobilní telefonní číslo.

☒ Po odeslání vytisknout souhrnné informace

☒ Zálohovat privátní klíč (pokud to umožňuje vybrané úložiště)

Krok 2: Výběr úložiště pro generování klíčů

Windows

Bude generován klíč o velikosti: RSA 4096

RSA 4096

EC P-256

EC P-384

EC P-521

Krok 3: Generování a odeslání žádosti

Souhrn:

Odeslat žádostZkopírovat ID do schránkyZavřít

5. Generování žádosti o prvotní certifikát

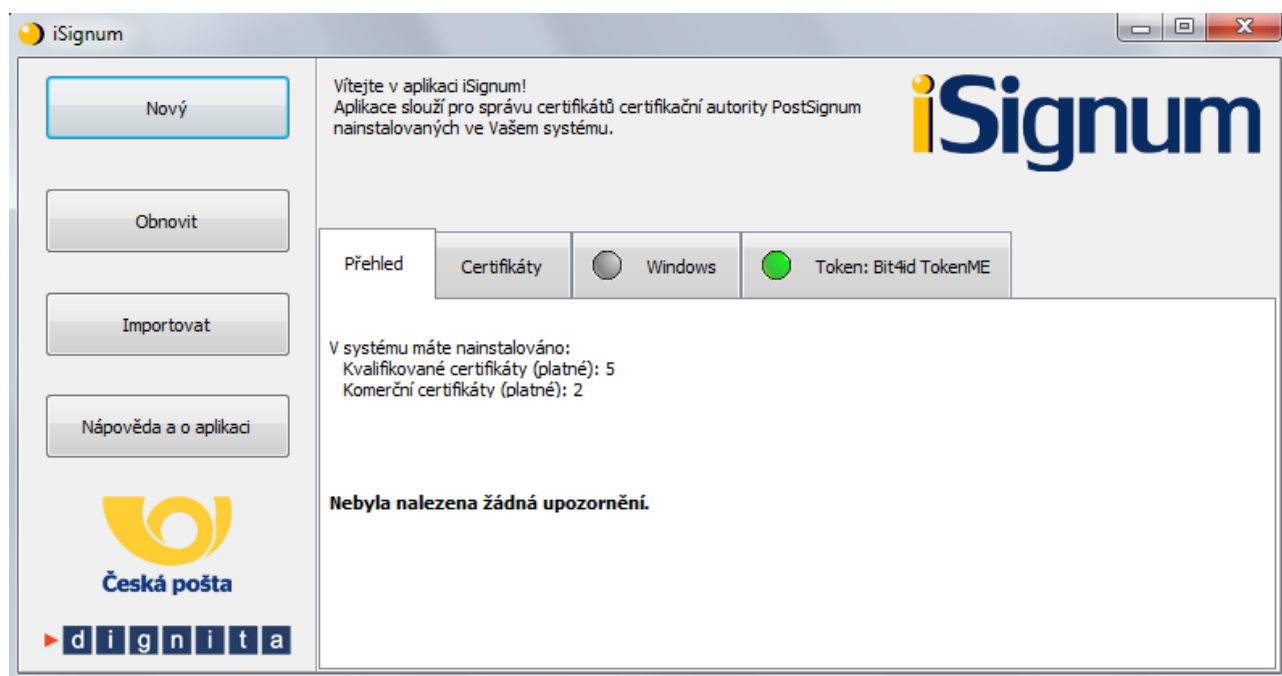
Generování klíčů na prostředek a žádosti o kvalifikovaný certifikát, který bude obsahovat příznak QESCD (kvalifikované cert.) nebo NCP+ (komerční cert.), je možné pouze v programu **iSignum**, který zajistí vytvoření správné žádosti o certifikát. Pokud bude ke generování žádosti využit jiný program,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

Program iSignum je ke stažení z webových stránek PostSignum:

https://www.postsignum.cz/isignum_pro_windows.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. 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 **TokenME EVO** 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, email, telefonní číslo a stisknout tlačítko **Odeslat žádost**.
6. Velikost generovaného klíče (kap. 4.4) lze ovlivnit v expertním módu aplikace iSignum (kap. 4.5).
7. 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:

Mobilní telefonní číslo: +420

Tyto informace jsou nepovinné a slouží pro ověření uložené žádosti před vydáním certifikátu žadatelem o certifikát. Informace o generované žádosti o certifikát je zaslána výhradně prostřednictvím SMS na mobilní telefonní číslo.

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

Krok 2: Výběr úložiště pro generování klíčů

Bude generován klíč o velikosti: RSA-4096

Byl vybrán kvalifikovaný prostředek

Krok 3: Generování a odeslání žádosti na server PostSignum

Souhrn:

Odeslat žádost Zkopírovat ID do schránky Zavřít

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

Krok 3: Generování a odeslání žádosti na server PostSignum

Souhrn:

ID žádosti o certifikát: **BP5638412975**

Nebo

Krok 3: Generování a odeslání žádosti na server PostSignum

Souhrn:

ID žádosti o certifikát : **KC5765039450**

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

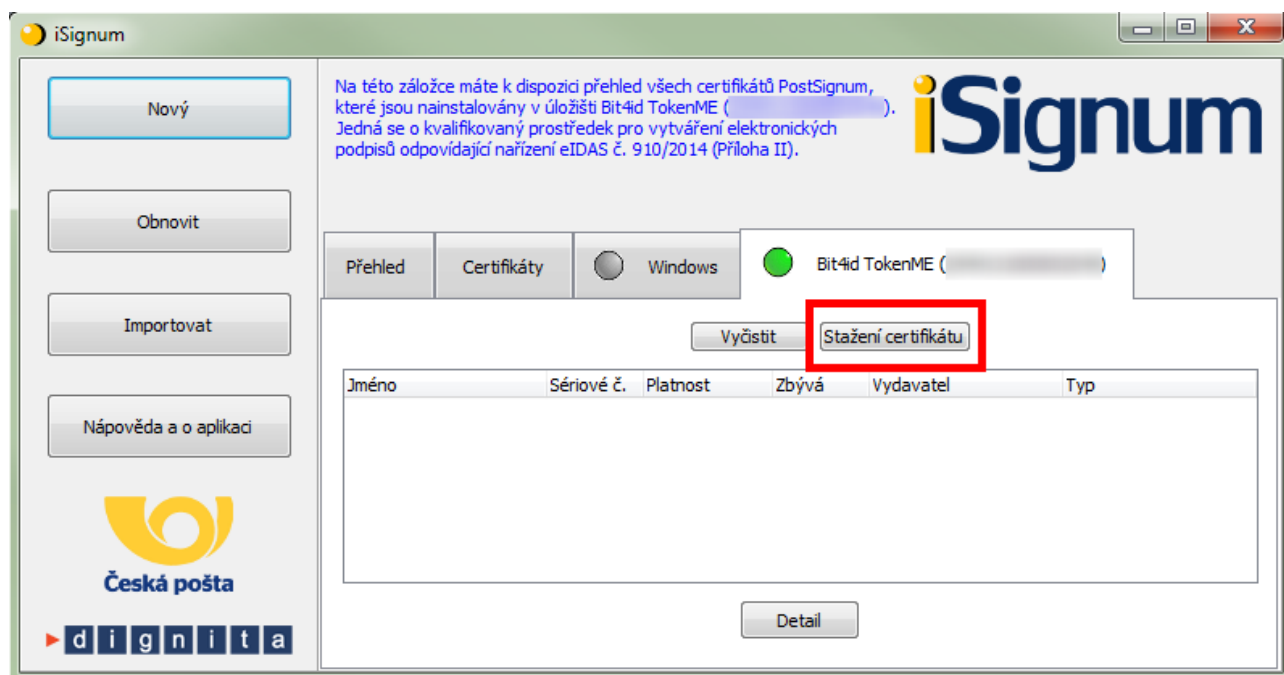
https://www.postsignum.cz/vydani_certifikatu_elektronicky.html

Platí pouze pro TokenME EVO

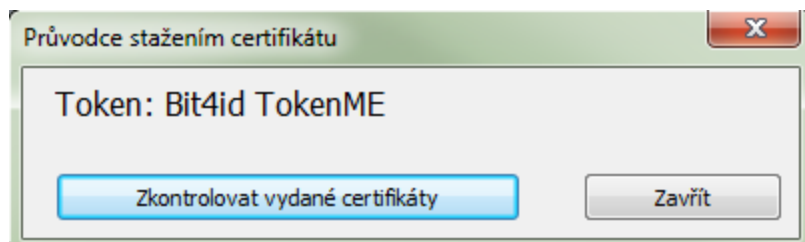
5.2. Instalace certifikátu v iSignum

Instalaci přímo do prostředku lze provést pouze v programu iSignum:

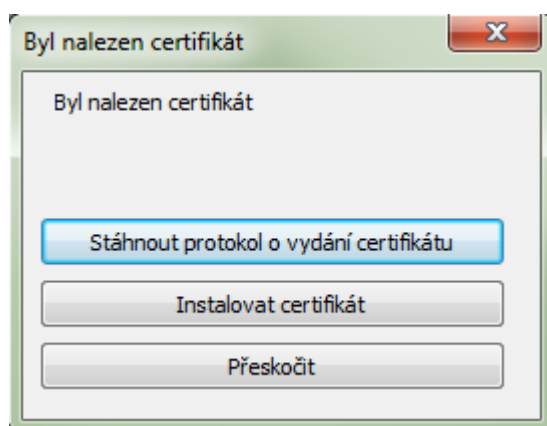
1. Vložit prostředek do USB portu počítače nebo do čtečky.
2. V programu iSignum stisknout tlačítko *Stážení certifikátu*.



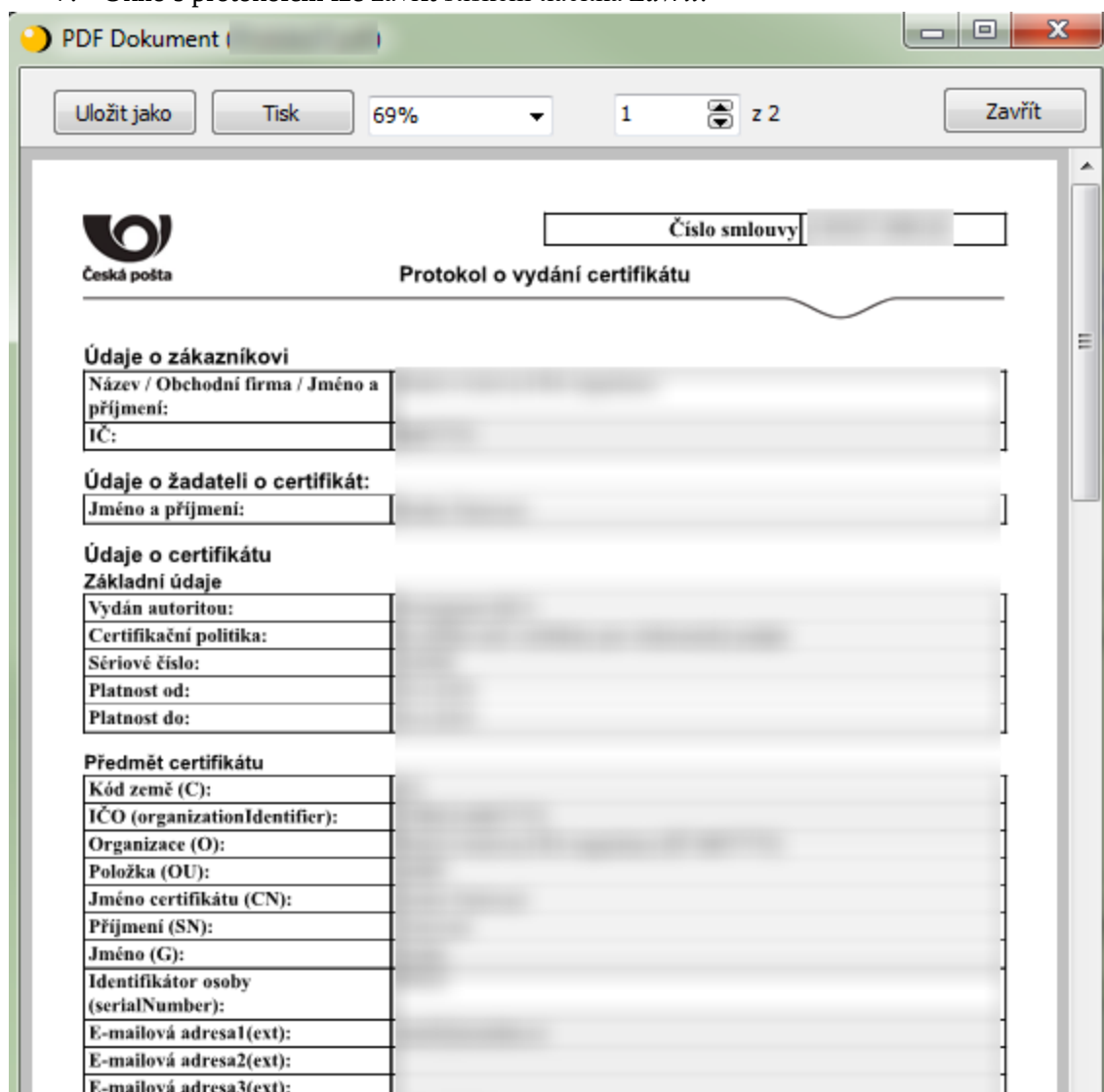
3. Stiskem tlačítka *Zkontrolovat vydané certifikáty* ověřit, zda je již certifikát připraven k instalaci.



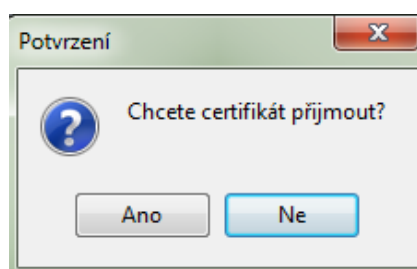
4. Pokud byl certifikát nalezen, bude zobrazeno toto okno:



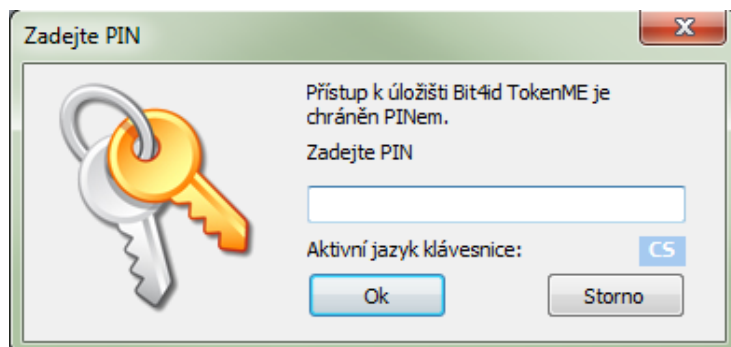
5. Je možné zkontrolovat údaje ve vydaném certifikátu v protokolu o vydání certifikátu, který lze stáhnout stiskem tlačítka *Stáhnout protokol o vydání certifikátu*.
6. Protokol lze uložit stiskem tlačítka *Uložit jako* nebo vytisknout tlačítkem *Tisk*.
7. Okno s protokolem lze zavřít stiskem tlačítka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



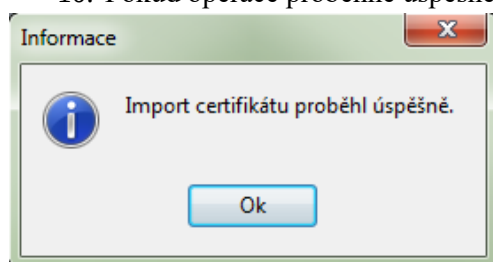
8. Přijmout certifikát - pokud jsou údaje v certifikátu v pořádku.



9. Zadat PIN

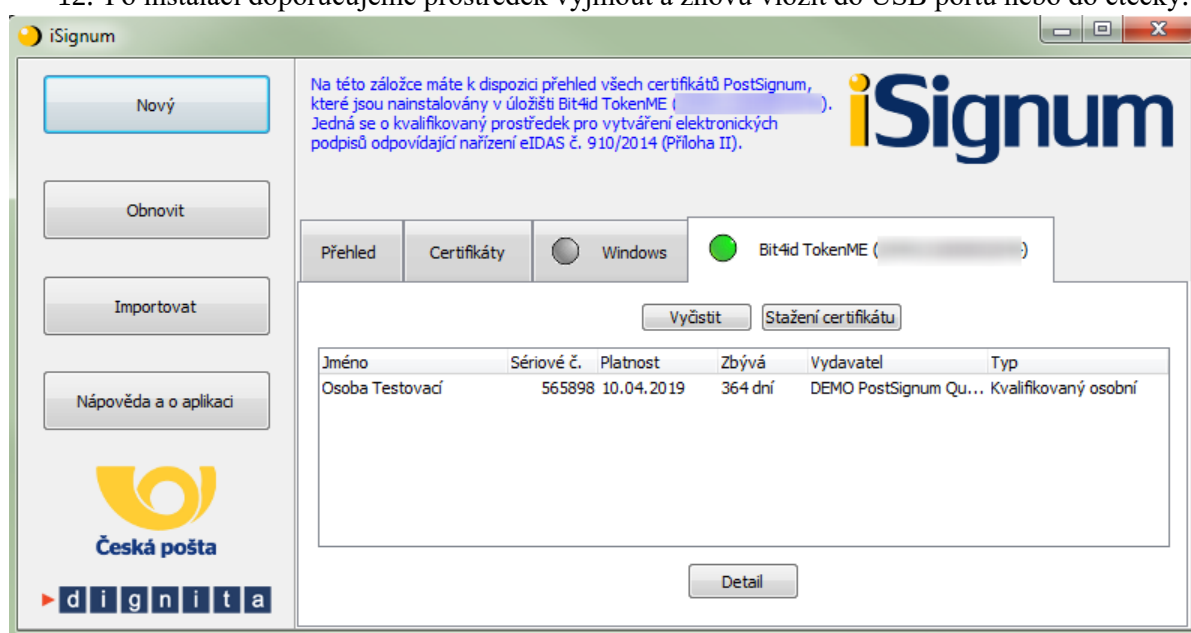


10. Pokud operace proběhne úspěšně, bude zobrazena hláška:



11. Po úspěšném importu bude certifikát vidět v programu iSignum na záložce TokenME EVO.

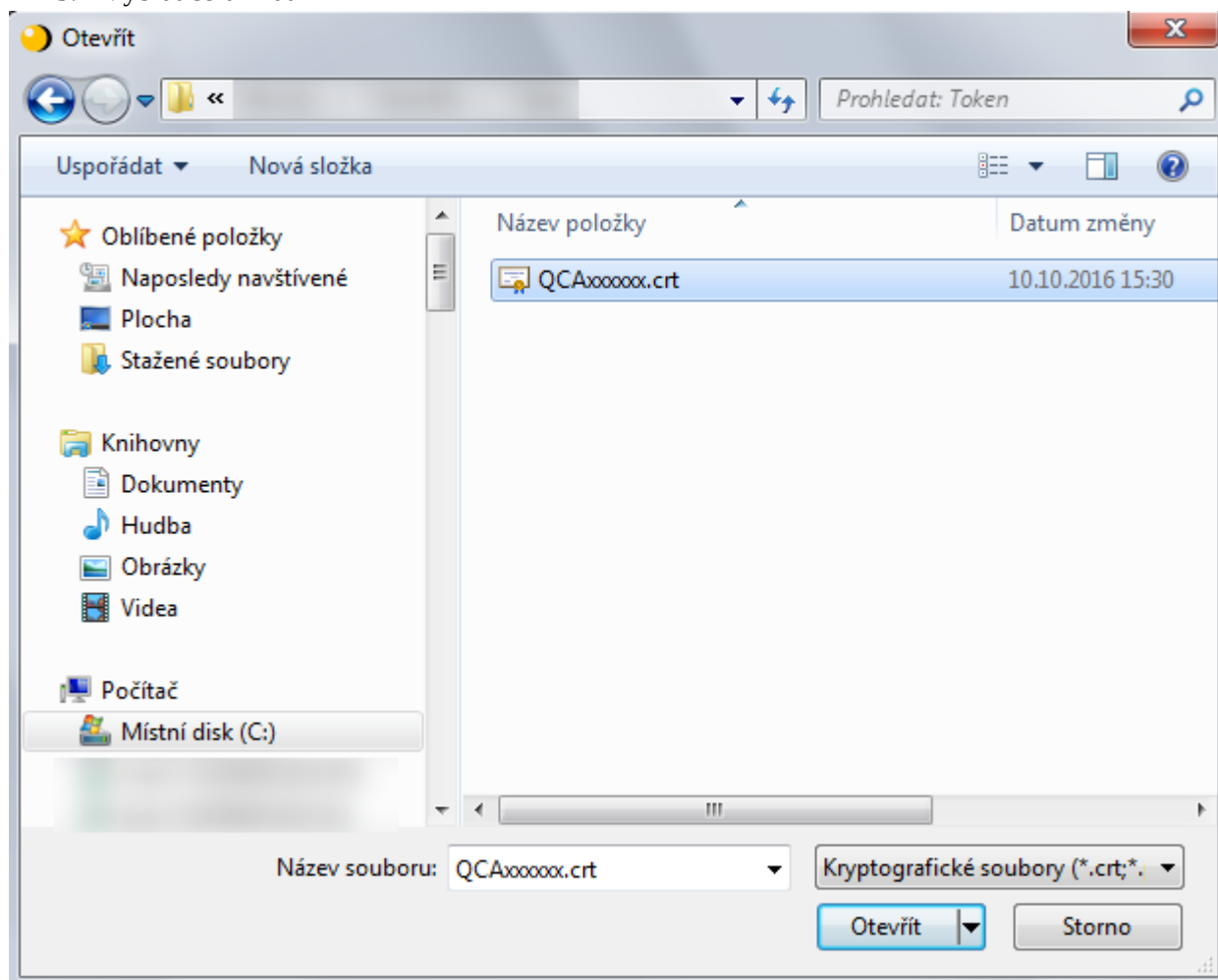
12. Po instalaci doporučujeme prostředek vyjmout a znovu vložit do USB portu nebo do čtečky.



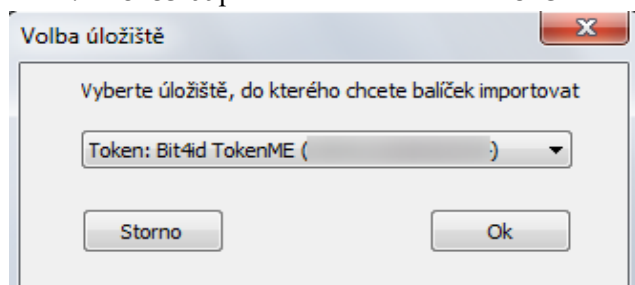
5.3. Instalace certifikátu ze staženého souboru

Instalaci certifikátu doporučujeme provést v programu iSignum:

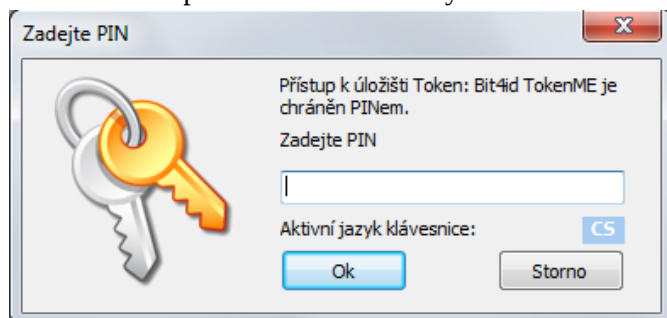
1. Vložit prostředek do USB portu počítače nebo do čtečky.
2. V programu iSignum stisknout tlačítko *Importovat*.
3. Vybrat certifikát



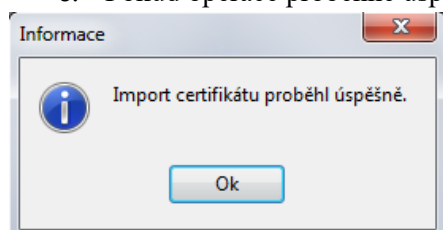
4. Ponechat přednastavené úložiště **TokenME EVO**



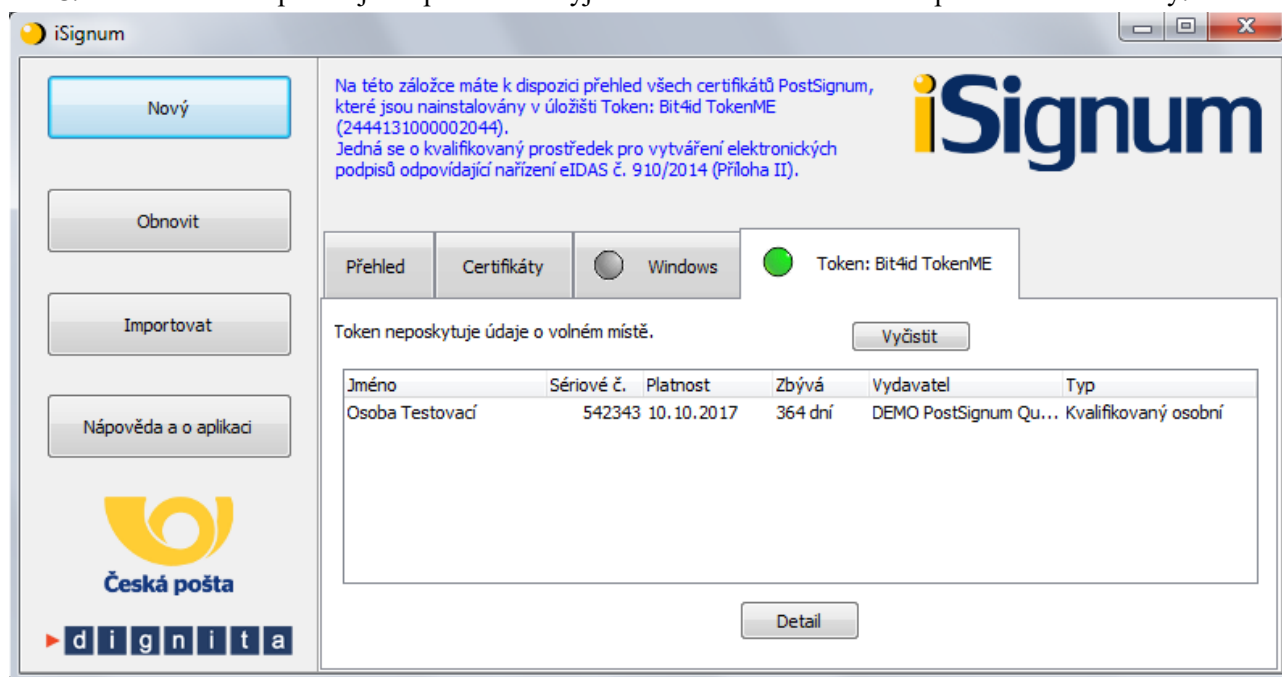
5. Pro import certifikátu bude vyžadován PIN



6. Pokud operace proběhne úspěšně, bude zobrazena hláška:

7. Po úspěšném importu bude certifikát vidět v programu iSignum na záložce **TokenME EVO**.

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 do 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 EVO, tak úložiště pro generování klíčů bude přednastaveno na **TokenME EVO** 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 TokenME EVO, je nutné vybrat úložiště pro generování klíčů ručně na hodnotu **TokenME EVO**, aby byl obnovovaný certifikát uložen na prostředku.
5. Velikost generované klíče (kap. 4.4) lze ovlivnit v expertním módu aplikace iSignum (kap. 4.5).
6. 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

☐ Zálohovat privátní klíč (pokud to umožňuje vybrané úložiště)

Kód slevové poukázky:

Krok 2: Výběr úložiště pro generování klíčů

8A5E30B42AEC53AC 8A5E30B42AEC53AC

Byl vybrán kvalifikovaný prostředek

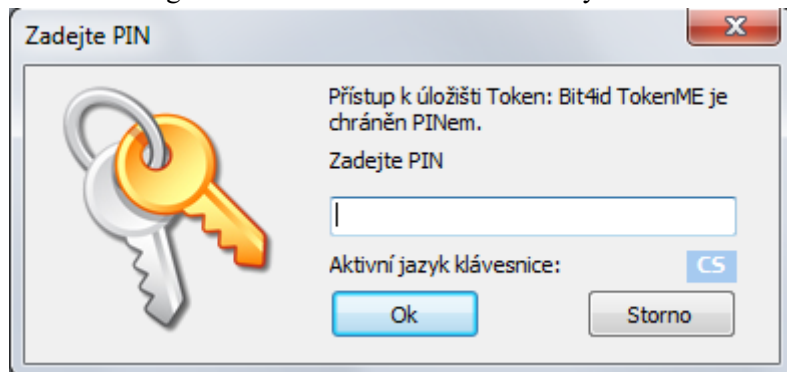
Bude generován klíč o velikosti: RSA 4096

Krok 3: Generování a odeslání žádosti na server PostSignum

Souhrn:

Odeslat žádost Odeslat žádost o víceletý certifikát Zavřít

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 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*.
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 5.3. 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:

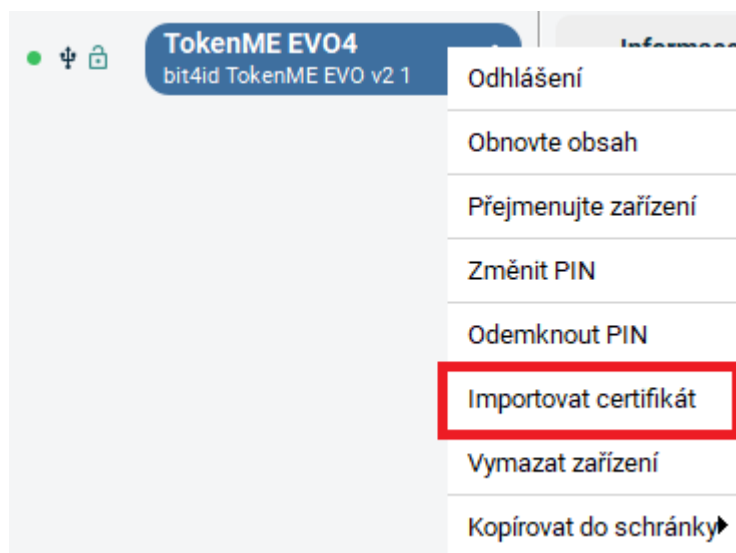
https://www.postsignum.cz/obnova_certifikatu.html

Platí pouze pro TokenME EVO

7. Další funkce softwaru Bit4id PKI Manager

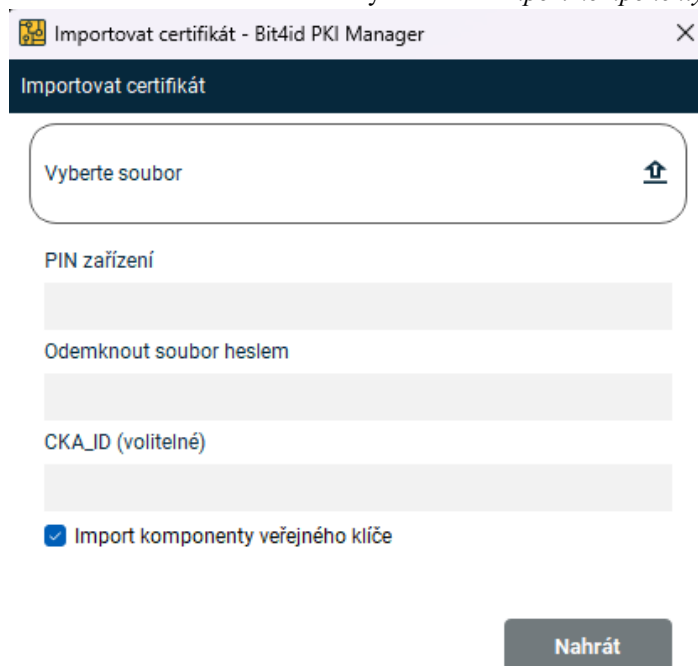
7.1. Import certifikátu z PKCS#12

Vložení certifikátů ze zálohy (PFX nebo P12) do prostředku se provede kliknutím na ikonu tří teček vedle názvu zařízení  a vyberete *Importovat certifikát*.

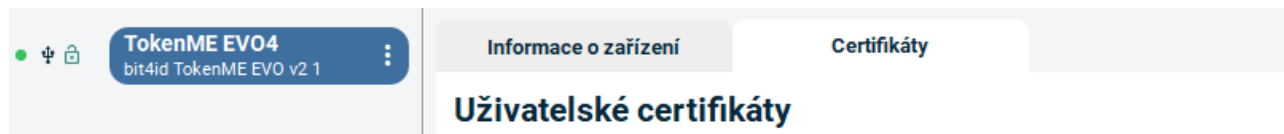


1. Vybrat soubor se zálohou, kde je uložený certifikát ve formátu pfx či p12.
2. Zadat PIN zařízení TokenME EVO.
3. Zadat heslo k importovanému souboru na řádku *Odemknout soubor heslem*.
4. *CKA_ID (volitelné)* je libovolným názvem importovaného souboru.
5. Potvrdit tlačítkem *Nahrát*.

Pozn.: Defaultně zatržený checkbox *Import komponenty veřejného klíče* je doporučeno ponechat.


 The screenshot shows the 'Importovat certifikát' dialog box. It contains a file selection field labeled 'Vyberte soubor' with an upload icon. Below are input fields for 'PIN zařízení', 'Odemknout soubor heslem', and 'CKA_ID (volitelné)'. At the bottom, there is a checked checkbox for 'Import komponenty veřejného klíče' and a 'Nahrát' button.

Po úspěšném vložení certifikátu se zobrazí v záložce *Certifikáty*.



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. Odhlášení

Po stisku zeleného tlačítka dojde k odhlášení prostředku z aplikace.

7.3. Obnovte obsah

Po kliknutí na ikonu tří teček vedle názvu zařízení  vyberete volbu *Obnovte obsah*, po stisku položky na řádku dojde k obnovení zobrazených informací na prostředku.

7.4. Přejmenujte zařízení

Po kliknutí na ikonu tří teček vedle názvu zařízení  vyberete volbu *Přejmenujte zařízení* a do editovatelného řádku vyplňte vlastní název a stiskněte Ok.



Vložit nový název zařízení

TokenME EVO4

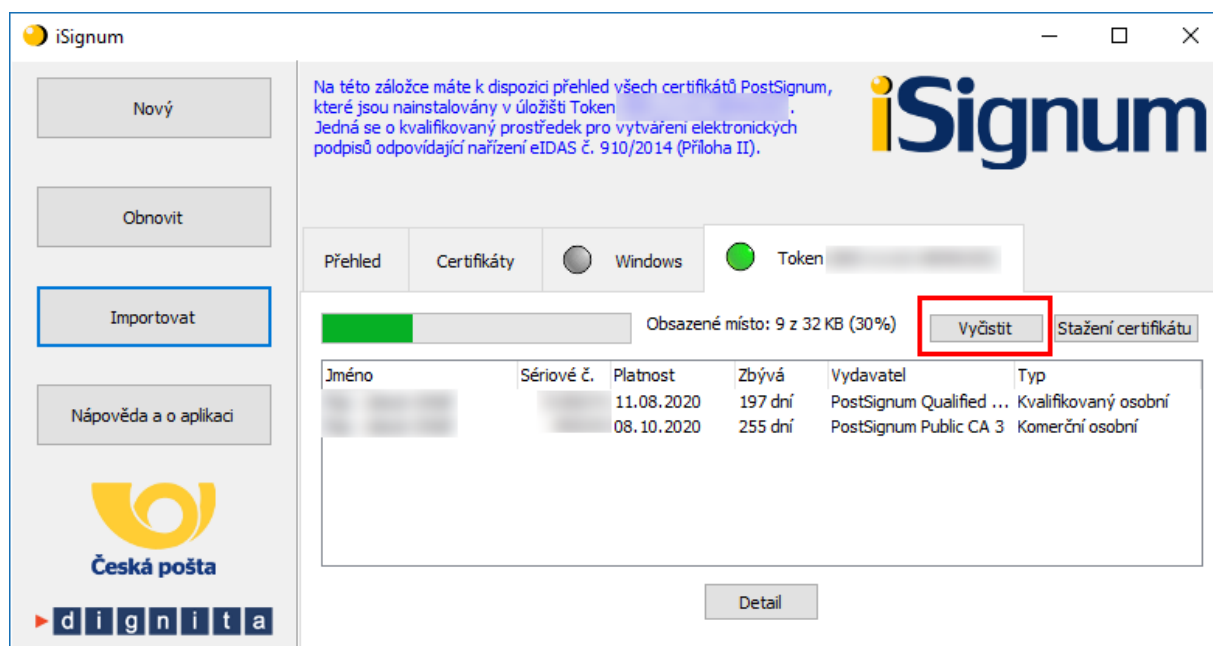
Zrušit

Ok

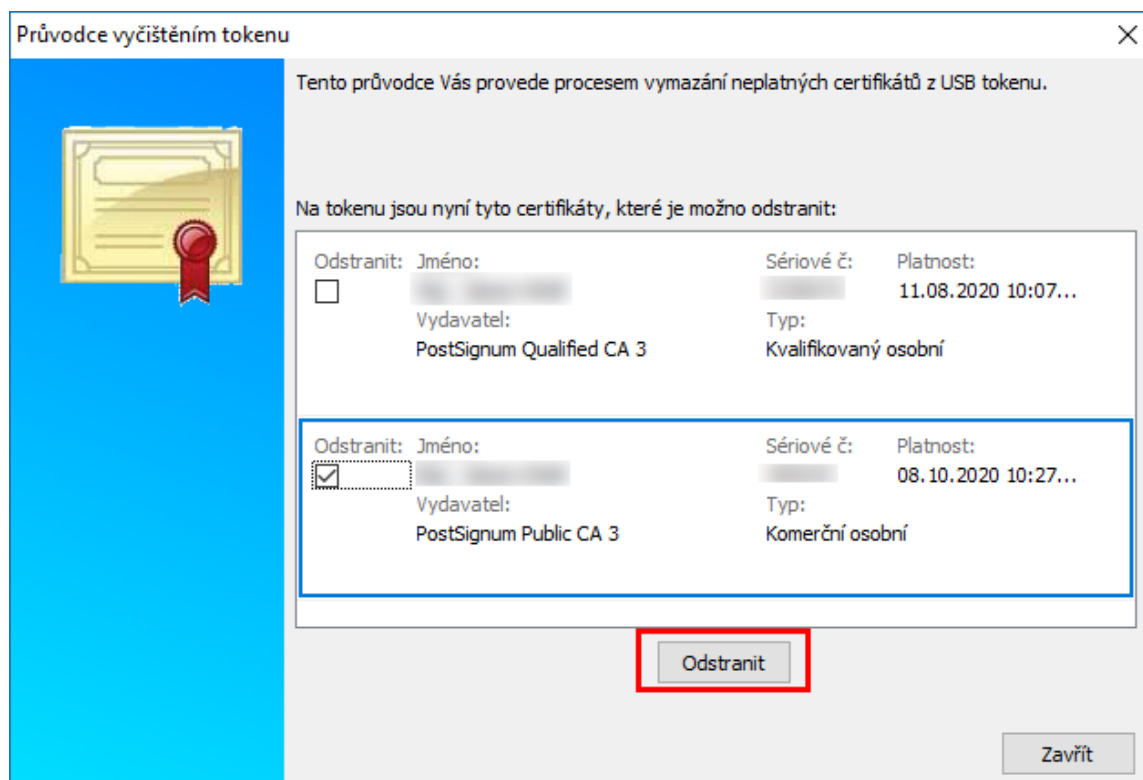
7.5. Odstranění dat

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. Spustíte 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**.



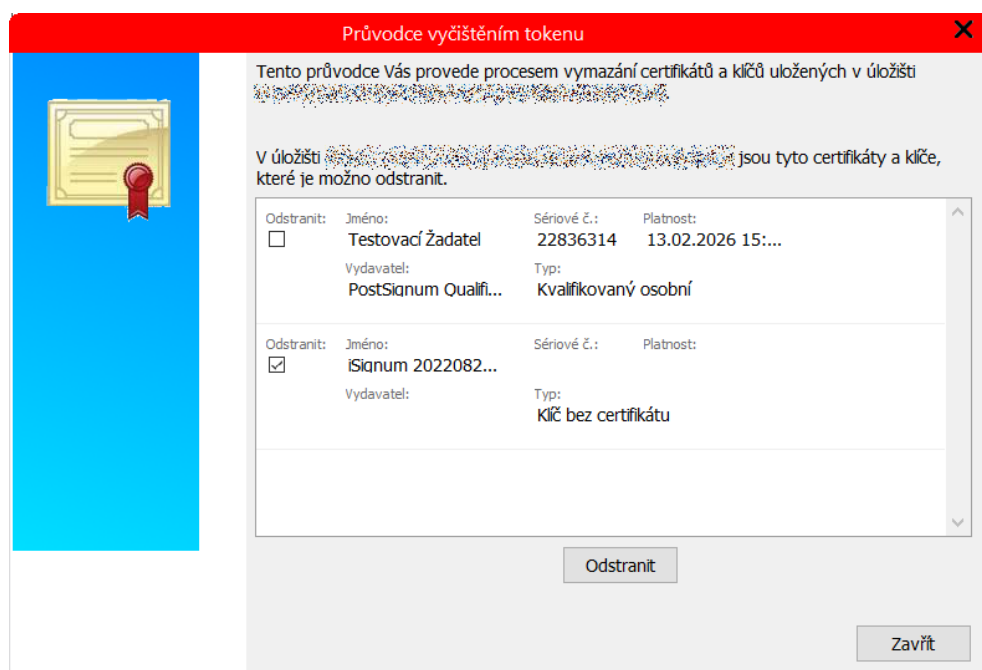
7.5.2. Odstranění klíče

Chyba 622 může být rovněž způsobena tím, že na tokenu jsou uloženy klíče, které nebyly spárovány s certifikátem. Tyto klíče lze odstranit v programu 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**.

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



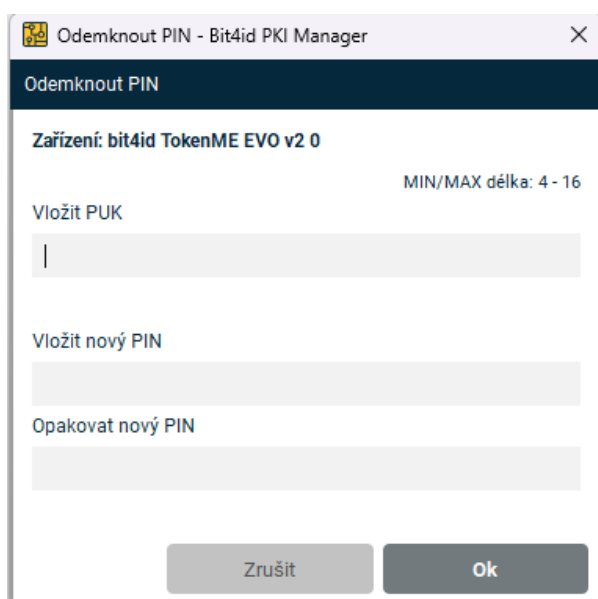
Následně budete vyzváni k potvrzení operace a k zadání PINu k tokenu.

Upozorňujeme, že odstranění klíčů může trvat až 5 minut.

7.6. Odemknout PIN

Pokud je prostředek zablokovaný 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.

1. V PKI Manageru kliknout na volbu *Odemknout PIN*.
2. Do políčka *Vložit PUK* zadat: **PUK k tokenu**.
3. Do políčka *Vložit nový PIN* zapsat nový PIN, který musí mít min. 4 znaky a maximálně 8 znaků.
4. Do políčka *Opakovat nový PIN* zopakovat nový PIN.
5. Změnu PINu potvrdit tlačítkem OK.



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

7.7. Náhled certifikátu

V záložce *Certifikáty* je možné zobrazit detail certifikátu na prostředku po prokliku šipky na černém poli:

Ing. Testovací Žadatel 2026-05-26 2027-06-15 >

Informace o certifikátu jsou rozděleny do záložek:

< Seznam certifikátů

● Ing. Testovací Žadatel

Certifikát

Privátní klíč

Veřejný klíč

Po kliknutí na ikonu tří teček vedle záložek certifikátu  je možné vybrat volby *Exportovat* nebo *Vymazat certifikát*. Možnost exportu certifikátu je k dispozici ve formátu souboru .cer. V případě, že chcete využít volbu *Vymazat certifikát*, jedná se o nevratnou operaci, kterou provádějte pouze pokud jste si jisti, že certifikát je možné z prostředku odstranit.

Exportovat certifikát

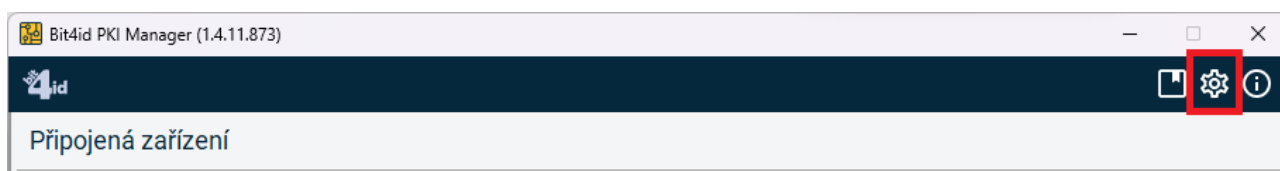
Vymazat certifikát

7.8. Otevřít Správce certifikátů systému Windows



Volba na horním panelu ovladače má možnost pomocí tlačítka otevřít Správce Windows (certmgr). V případě manipulace se zobrazenými certifikáty dbejte zvýšené obezřetnosti, operace provedené ve Správci jsou nevratné.

7.9. Nastavení



Zde je možné povolit import pxf/p12, logování aplikace, vymazat paměť ovladače, povolit připojené zařízení a systémové informace. Přednastavené volby není doporučeno měnit.

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. Servisní klíč není potřeba v případě ukončené certifikace nebo v případě generování žádosti o komerční certifikát.

8.2. 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.

Přihlášená osoba

Jméno:
Číslo smlouvy:

[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

» [Úvodní stránka](#) » [Certifikáty](#) » [Správa žadatelů](#) » Zrušení vazby osoba-kvalifikovaný prostředek

Zrušení vazby osoba/kvalifikovaný prostředek



Jméno žadatele:

Číslo zaměstnance:

Číslo bezpečného prostředku:

Vyhledat žadatele

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

Přihlášená osoba

Jméno:
Číslo smlouvy:

[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

» [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](#)

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. Reklamacce

V případě reklamacce je nutné provést níže uvedené kroky:

1. **Vymazat z prostředku veškeré certifikáty žadatele, aby nemohlo dojít k jejich zneužití.**
2. **Provést zneplatnění certifikátů žadatele, které byly uloženy na prostředku.**
3. **Nastavit na prostředku tovární hodnoty PIN a PUK, aby bylo možné na prostředku vygenerovat nový servisní klíč.**

PIN: 12345678

PUK: 87654321

4. 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, 2 a 3, nebude možné na prostředek vygenerovat nový servisní klíč.