Česká pošta

ProID+Q – Uživatelská příručka

Verze 1.3

Obsah dokumentu

Evidence revizí a změn

Verze	Účinnost od	Důvod a popis změny	Autor	Schválil
1.0	16. 5. 2018		Česká pošta, s.p.	Manažer CA
1.1	27. 7. 2018	doplněna možnost pro el. pečetě	Česká pošta, s.p.	Manažer CA
1.2	16.4.2019	Odstraněn servisní klíč	Česká pošta, s.p.	Manažer CA
1.3	1. 12. 2019	změna postupu rušení vazby prostředku na osobu	Česká pošta, s.p.	Manažer CA

1. Přehled

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

Čipová karta je personalizována již z výroby, tzn., je na ní přednastaven PIN (12345678), PUK (87654321) a QPIN (12345678)**.**

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

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

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

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

Při vydání prvního certifikátu dochází k vytvoření vazby **čipová karta–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 čipové kartě 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 čipovou kartu předat jinému žadateli (např. z důvodu ukončení pracovního poměru) je nutné postupovat dle kapitoly 8.2

Obrázek čipové karty ProID+Q

2. Co potřebuji?

1. PC s operačním systémem Windows

2. Čipovou kartu

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

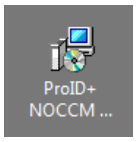
4. Software

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

3. Instalace softwaru

Ke správné instalaci softwaru je potřeba vykonat následující kroky:

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



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

Knihovna PKCS#11

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

4. Příprava čipové karty pro generování klíčů

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

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

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

4.1. Změna PINu

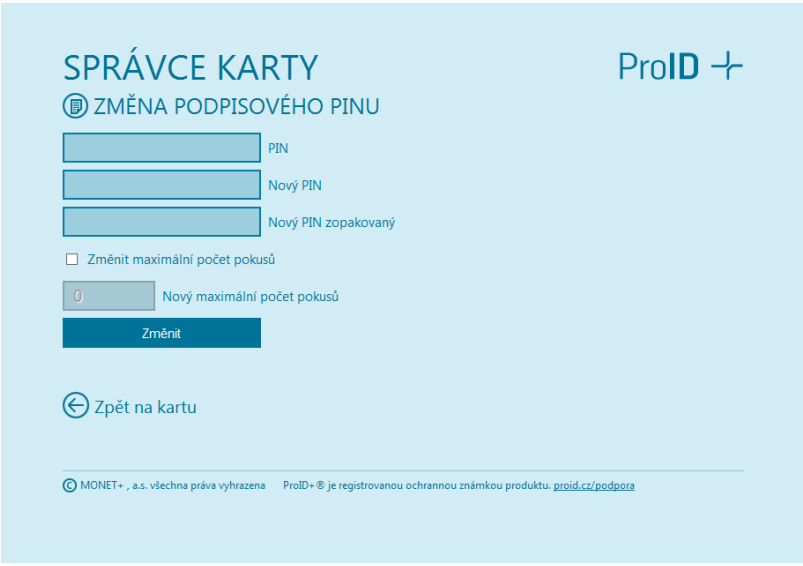
1. Ve správci karty ProID+ v levé části vybrat čipovou kartu a v pravé části kliknout na volbu *Změna PINu*.
2. Do políčka PIN zadat: **12345678**.
3. Do políčka Nový PIN zapsat nový PIN, který musí mít **min. 4 znaky** a **maximálně 15 znaků**.
4. Do políčka Nový PIN zopakovaný, zopakovat nový PIN.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

4.2. Změna PUKu

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

4.3. Změna podpisového PINu (QPIN)

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



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

5. Generování žádosti o prvotní certifikát

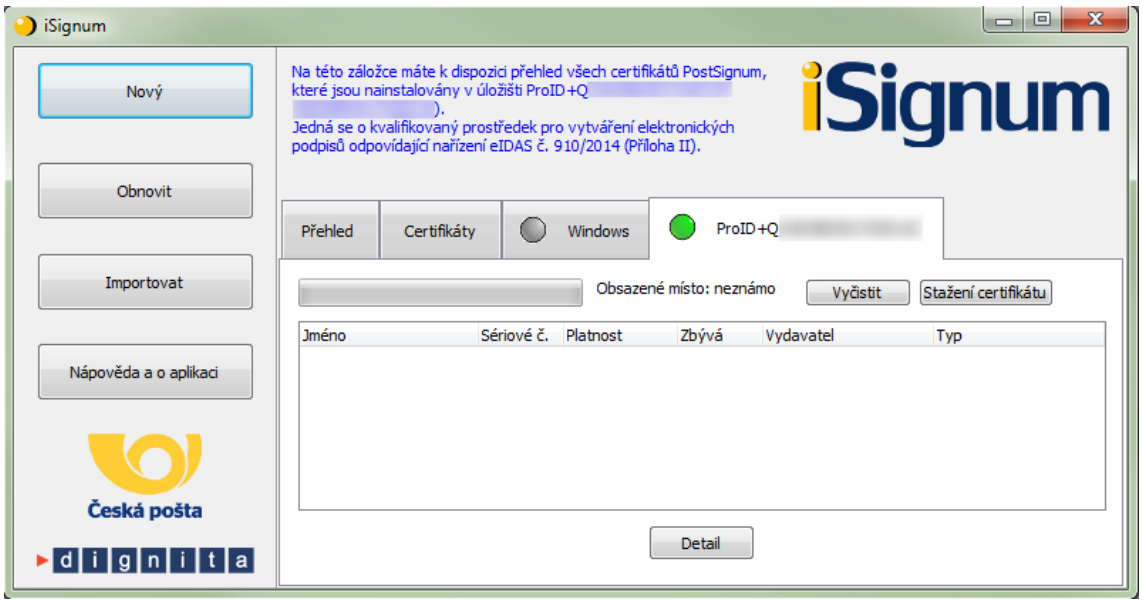
Generování klíčů na čipovou kartu a žádosti o kvalifikovaný certifikát, který bude obsahovat příznak QESCD, je možné pouze v programu **iSignum**, který zajistí vytvoření správné žádosti o certifikát. Pokud bude ke generování žádosti využit jiný program, není možné do certifikátu příznak QESCD vložit.

Program iSignum je ke stažení z webových stránek PostSignum:

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

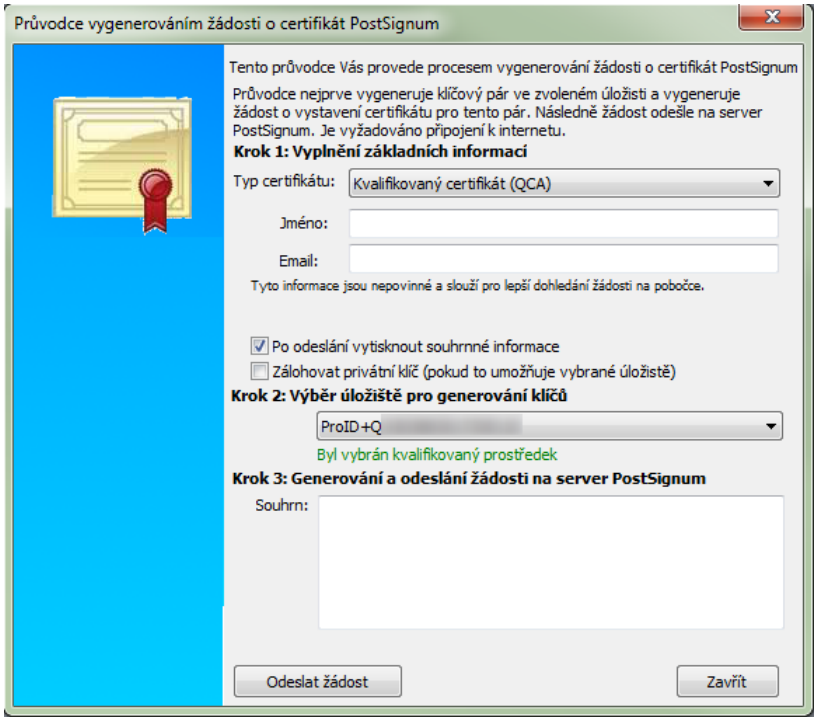
Spustit lze poklikáním na stažený soubor **iSignum.exe.**

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

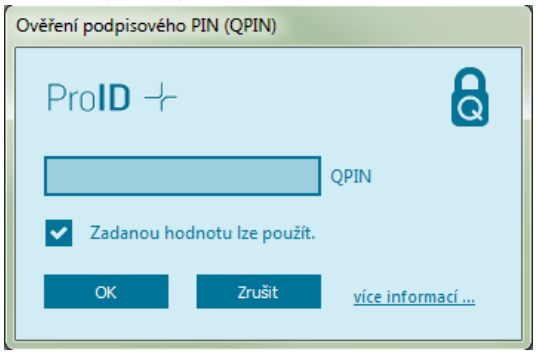


5.1. Vygenerování žádosti o certifikát

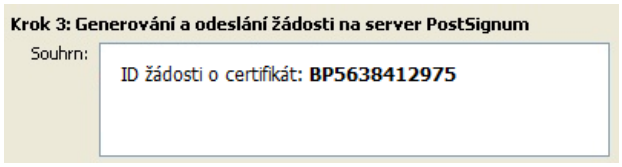
1. Vložit čipovou kartu do čtečky.
2. V programu iSignum stisknout tlačítko *Nový*. Spustí se průvodce vygenerováním žádosti.
3. Úložiště pro generování klíčů bude přednastaveno na hodnotu **ProID+** a zároveň bude zobrazeno upozornění: Byl vybrán kvalifikovaný prostředek.
4. Dále je nutné vyplnit své 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 dojde k bezpečnému předání žádosti o certifikát.
7. Při generování žádosti o Kvalifikovaný certifikát budete vyzváni k zadání Podpisového PINu (QPIN).



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 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

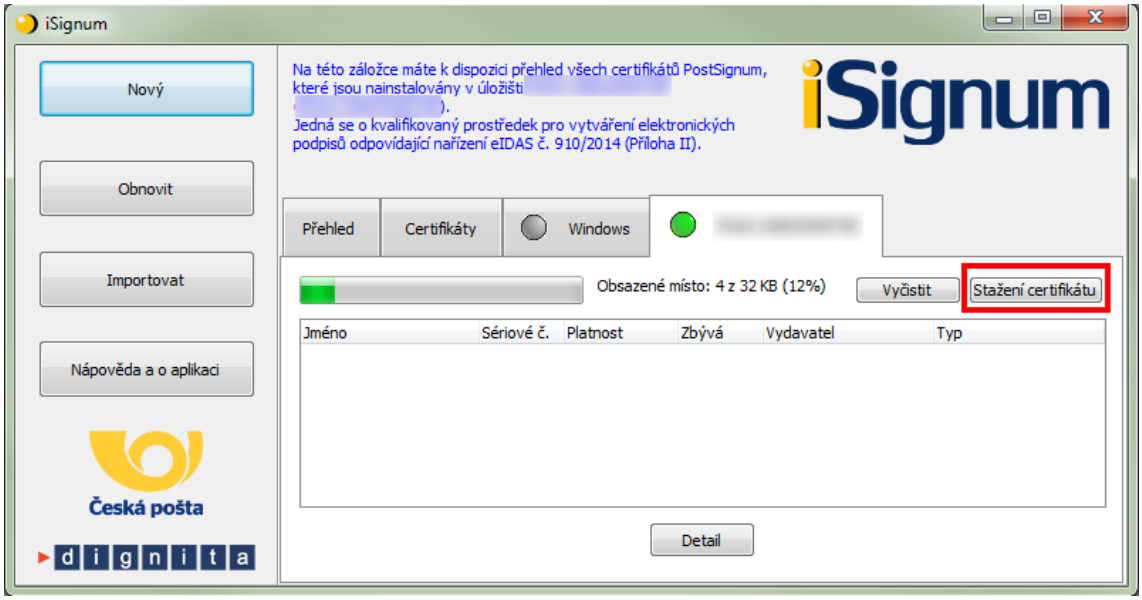
Poznámka (certifikát pro el. pečeť):
Kvalifikovaný certifikát pro elektronickou pečeť není vydáván na pobočkách České pošty. V případě žádosti o tento typ certifikátu postupujte dle pokynů na webových stránkách PostSignum:

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

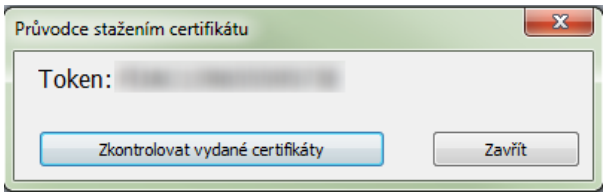
5.2. Instalace certifikátu v iSignum

Instalaci přímo do prostředku lze provést pouze v programu iSignum:

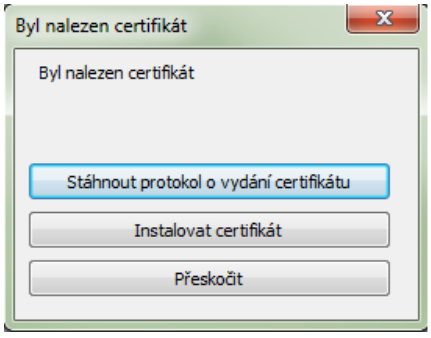
1. Vložit prostředek do USB portu počítače nebo do čtečky.
2. V programu iSignum stisknout tlačítko *Stažení certifikátu*.



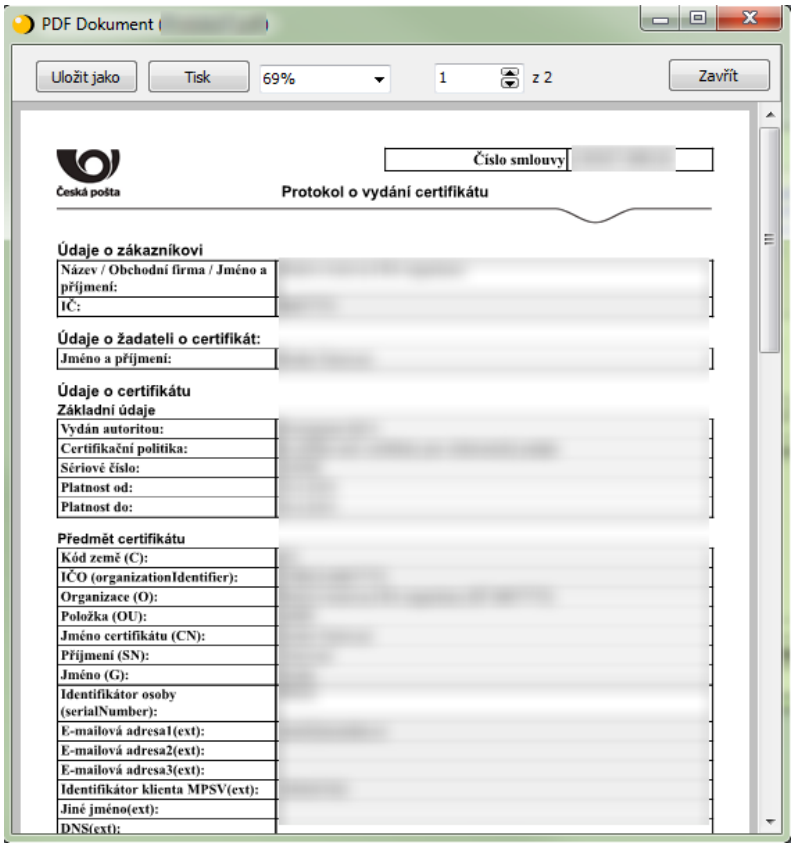
3. Stiskem tlačítka *Zkontrolovat vydané certifikáty* ověřit, zda je již certifikát připraven k instalaci.



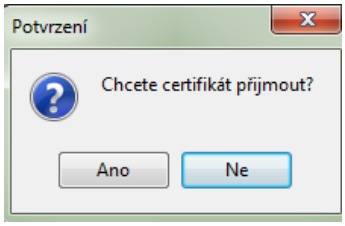
4. Pokud byl certifikát nalezen, bude zobrazeno toto okno:



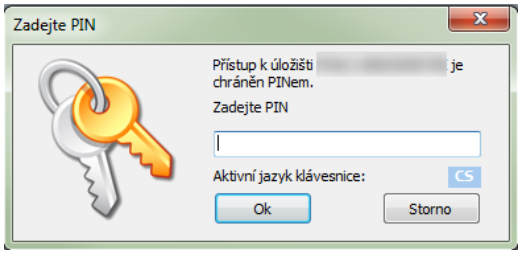
5. Dále je možné zkontrolovat údaje ve vydaném certifikátu v protokolu o vydání certifikátu, který lze stáhnout stiskem tlačítka *Stáhnout protokol o vydání certifikátu*.
6. Protokol lze uložit stiskem tlačítka *Uložit jako* nebo vytisknout tlačítkem *Tisk*.
7. Okno s protokolem lze zavřít stiskem tlačítka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



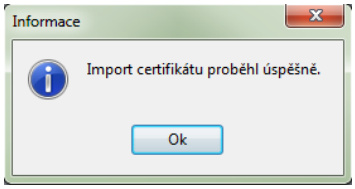
8. Přijmout certifikát - pokud jsou údaje v certifikátu v pořádku.



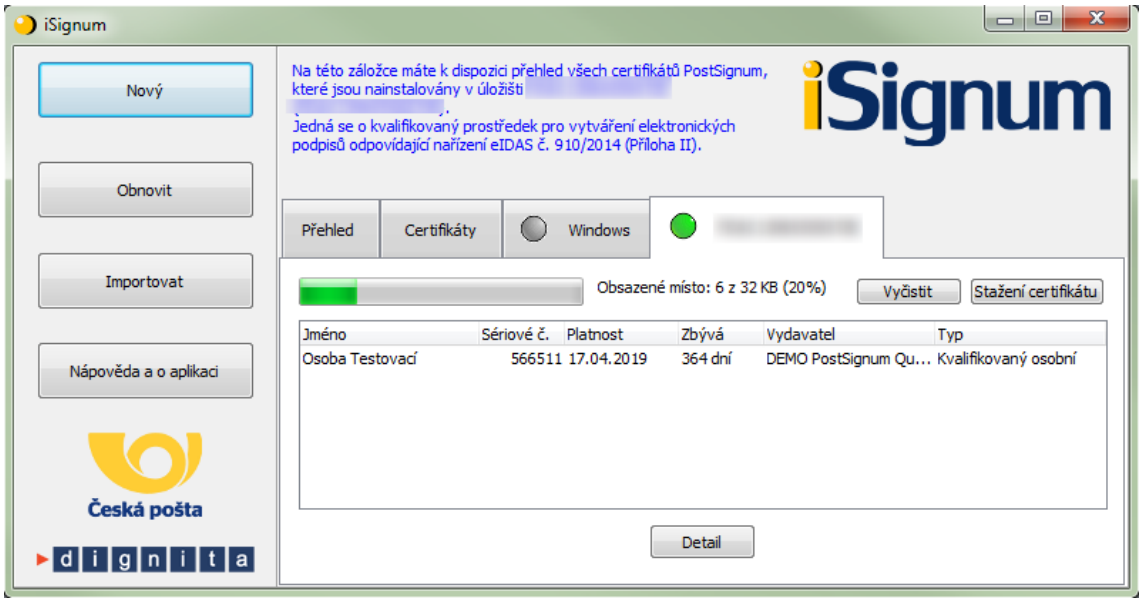
9. Zadat PIN



10. Pokud operace proběhne úspěšně, bude zobrazena hláška:



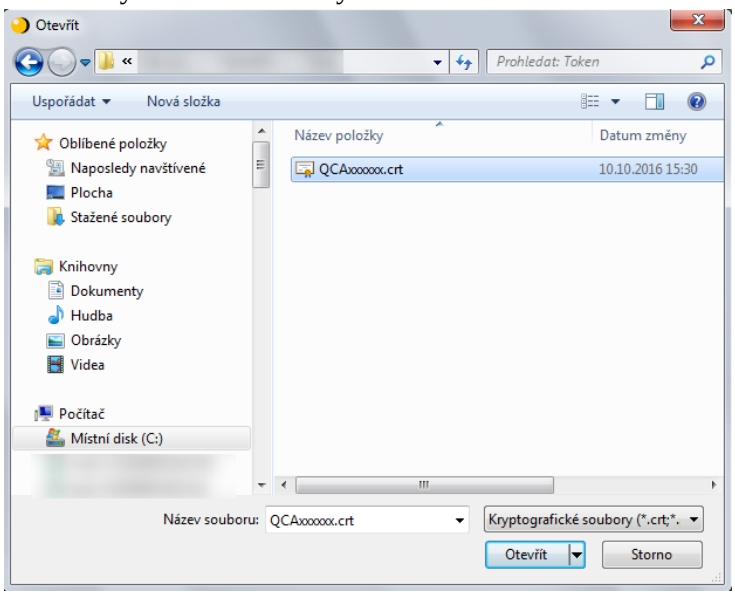
11. Po úspěšném importu bude certifikát vidět v programu iSignum na záložce **ProID+**.
12. Po instalaci doporučujeme prostředek vyjmout a znovu vložit do USB portu nebo do čtečky.



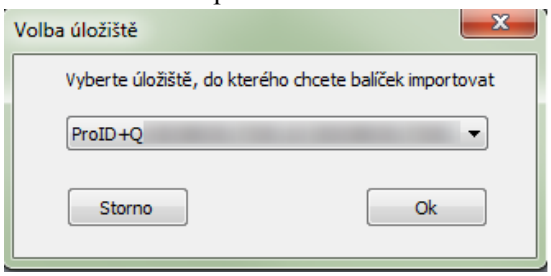
5.3. Instalace certifikátu

Instalaci certifikátu doporučujeme provést taktéž v programu iSignum:

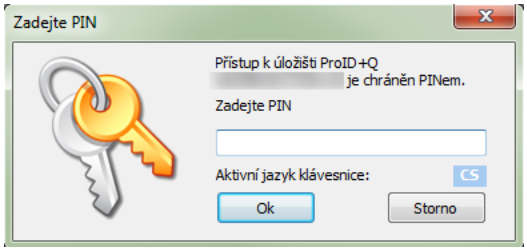
1. Vložit čipovou kartu do čtečky.
2. V programu iSignum stisknout tlačítko *Importovat*.
3. Vybrat kvalifikovaný certifikát



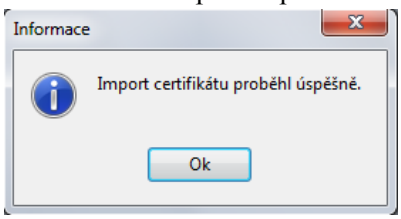
4. Ponechat přednastavené úložiště **ProID+**



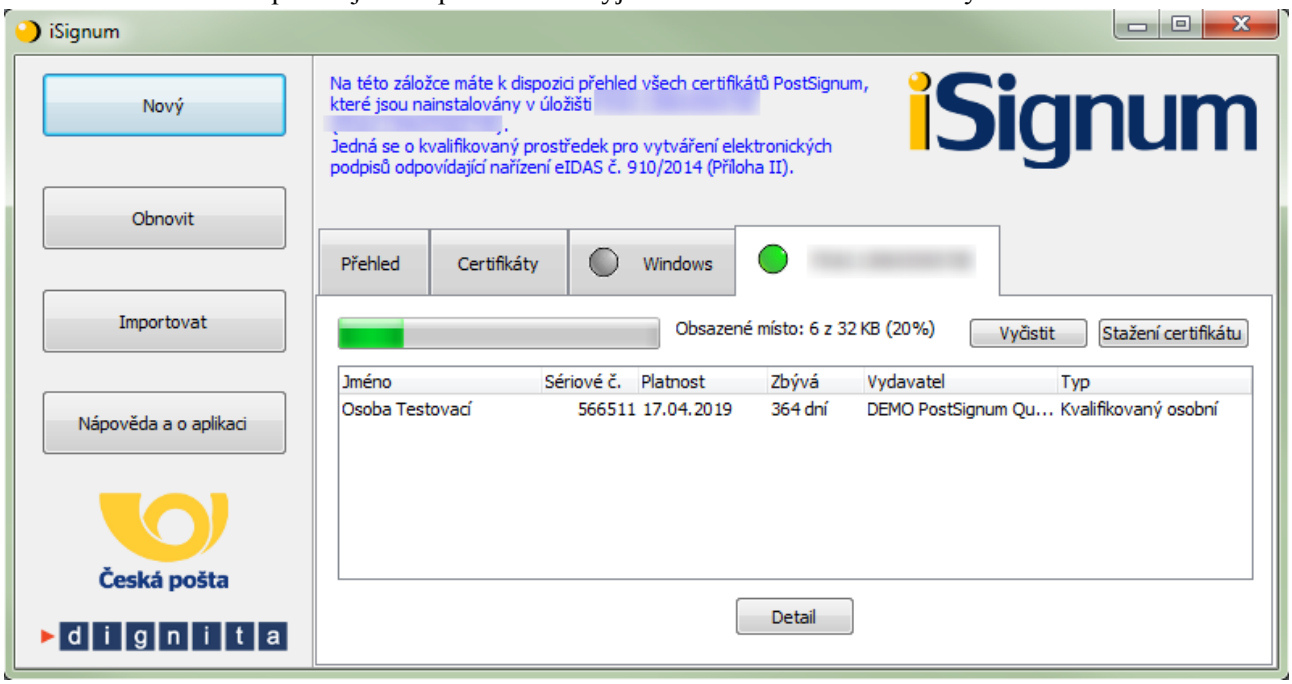
5. Pro import certifikátu bude vyžadován PIN



6. Pokud operace proběhne úspěšně, bude zobrazena hláška:

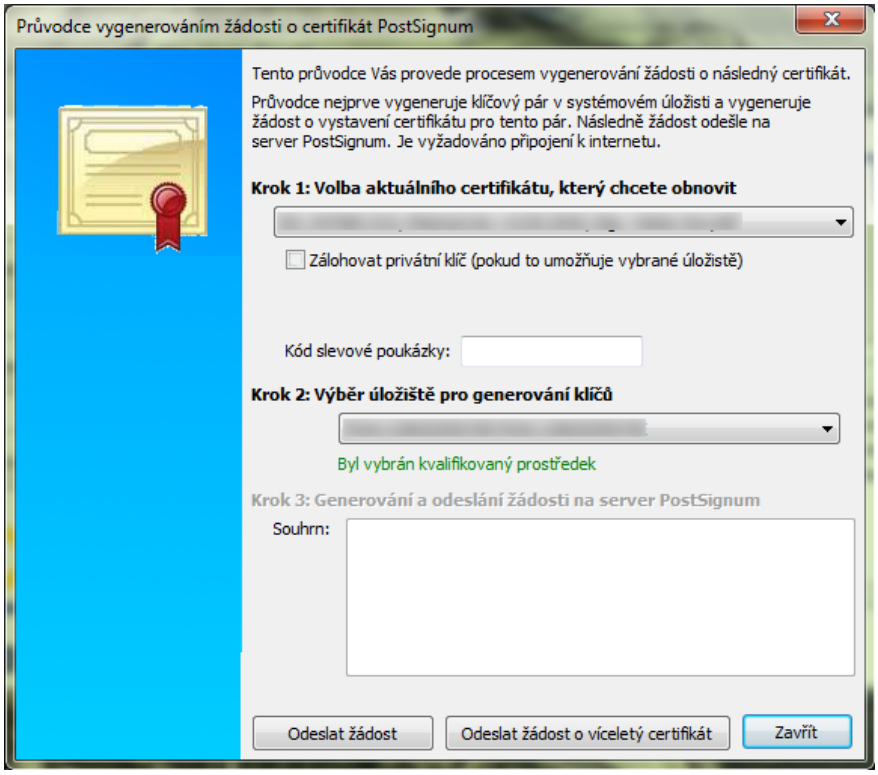


7. Po úspěšném importu bude certifikát vidět v programu iSignum na záložce **ProID+.**
8. Po instalaci doporučujeme čipovou kartu vyjmout a znovu vložit do čtečky.

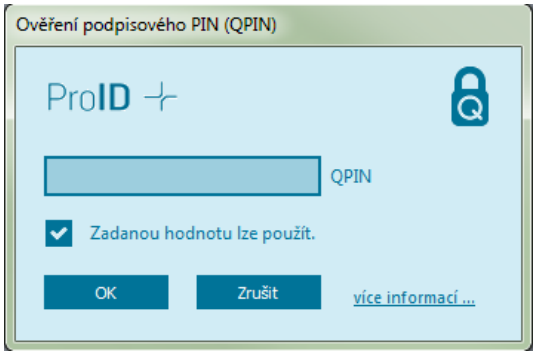


6. Generování žádosti o následný certifikát

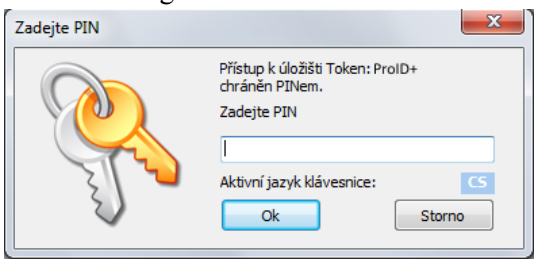
1. Vložit čipovou kartu do čtečky.
2. V programu iSignum stisknout tlačítko *Obnovit*. Spustí se průvodce vygenerováním žádosti o následný certifikát.
3. Vybrat certifikát, který chcete obnovit.
4. A. Pokud je obnovovaný certifikát uložen na čipové kartě, tak úložiště pro generování klíčů bude přednastaveno na hodnotu **ProID+** a zároveň bude zobrazeno upozornění: Byl vybrán kvalifikovaný prostředek.
4. B. Pokud obnovovaný certifikát není uložen na čipové kartě, je nutné vybrat úložiště pro generování klíčů ručně na hodnotu **ProID+**, aby byl obnovený certifikát uložen na čipové kartě.
5. Stisknout tlačítko *Odeslat žádost* případně *Odeslat žádost o víceletý certifikát.*



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



7. Před generováním klíčů a žádosti bude vyžadován PIN.



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

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

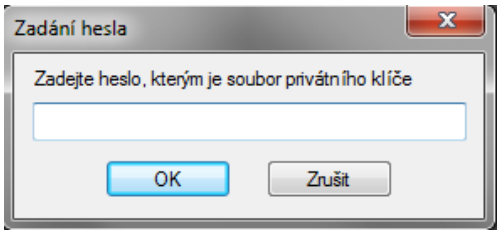
http://www.postsignum.cz/obnova_certifikatu.html

7. Další funkce Správce karty ProID+

7.1. Import certifikátu z PKCS#12

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

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



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

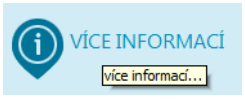
Upozorňujeme, že takto importovaný kvalifikovaný certifikát nebude považován za kvalifikovaný certifikát uložený na bezpečném zařízení QESCD a nebude obsahovat příznak, že byl vytvořen na QESCD prostředku.

7.2. Export do souboru

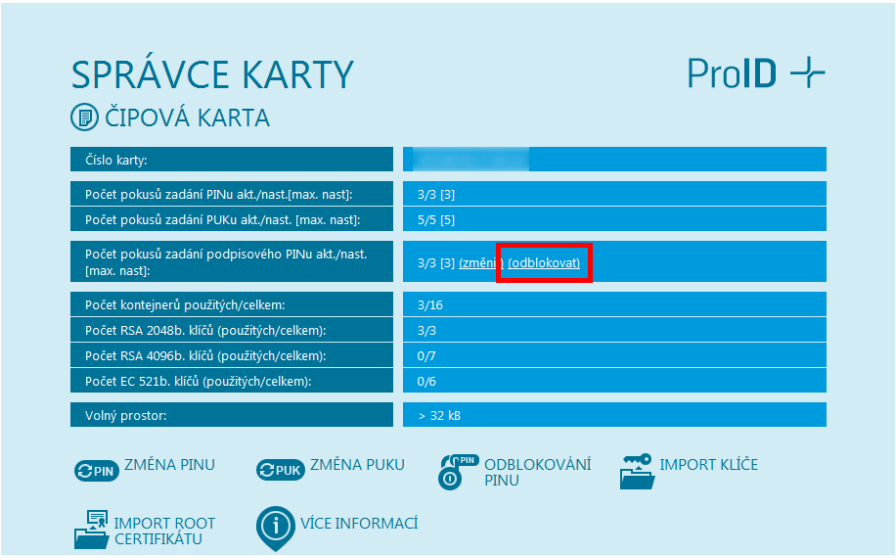
Dle typu objektu vyexportuje samotný certifikát nebo veřejný klíč z čipové karty do souboru.

7.3. Odblokování PINu a QPINu

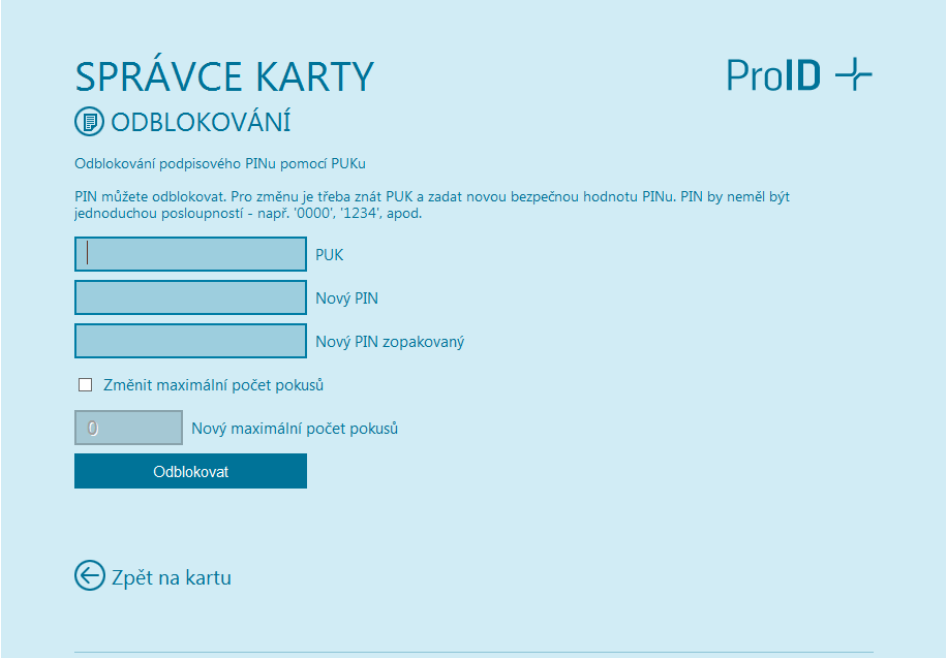
Pokud je čipová karta zablokována po vícenásobném špatném zadání PINu nebo QPINu, je možné ji touto volbou odblokovat. Pro odblokování je potřeba znát PUK. Po zadání PUKu je rovněž potřeba zadat nový PIN nebo QPIN.

V případě odblokování QPINu je nutné kliknout na tlačítko Více informací 

a dále na odblokovat dle obrázku:



Zadat PUK a nový QPIN a stisknout Odblokovat.



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

7.4. Registrace certifikátů

Dojde k registraci certifikátu uložených na čipové kartě 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. Předání čipové karty jiné osobě

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

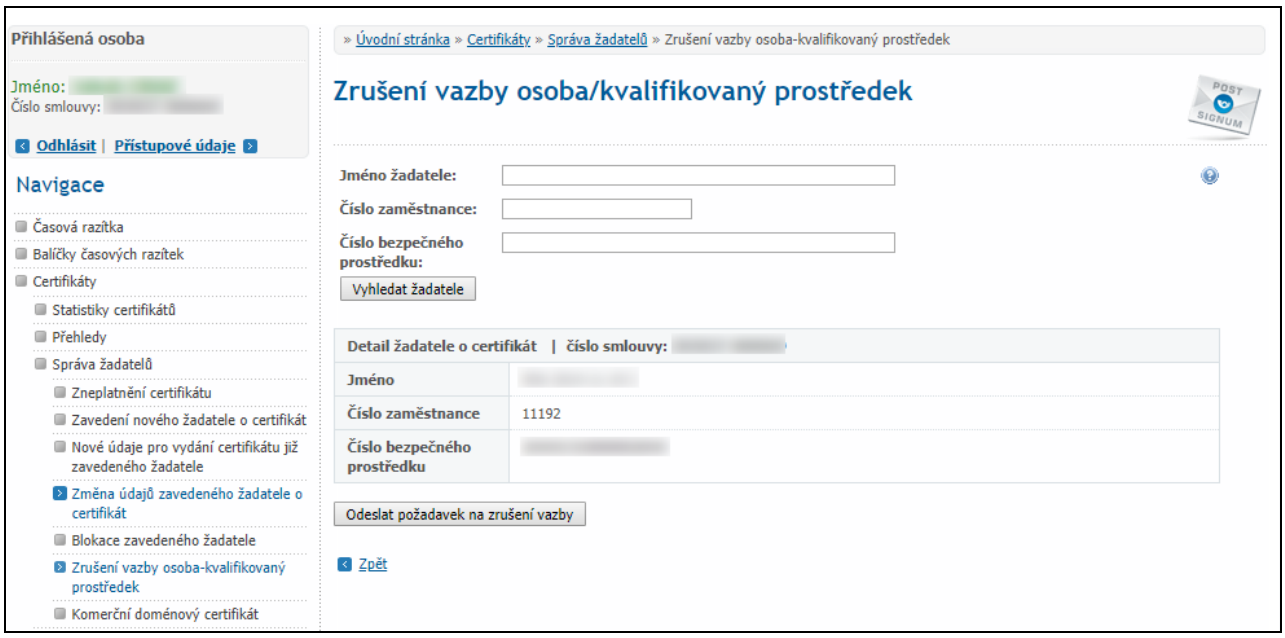
Pokud je nutné tuto vazbu změnit (např. z důvodu předání čipové karty jinému žadateli), je nutné postupovat následovně:

1. Zneplatnit certifikáty původního žadatele uložené na čipové kartě.
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 čipové kartě 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 čipové kartě: xxx (nebo výrobní číslo čipové karty):

9. Reklamace

V případě reklamace je nutné provést níže uvedené kroky:

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

   PIN: 12345678

PUK: 87654321

QPIN: 12345678

3. Čipovou kartu 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 čipovou kartu ověřit a karta bude vrácena zákazníkovi.