ČIPOVÁ KARTA QSCD – NÁVODY A NEJČASTĚJI KLADENÉ DOTAZY

JAK A KDE ZÍSKÁM OVLÁDACÍ SOFTWARE KARTY KB QSCD?

Instalační balíčky pro všechny podporované platformy operačních systémů jsou dostupné na https://www.kb.cz/karta. Pro OS Windows jsou k dispozici jazykové lokalizace (v současné době čeština [CZ] anebo angličtina [EN]).

JE MOŽNÉ UKLÁDAT NA KARTU KB QSCD CERTIFIKÁTY RŮZNÝCH CERTIFIKAČNÍCH AUTORIT?

Na kartu nelze ukládat certifikáty různých certifikačních autorit, je vyhrazena a použitelná pouze pro certifikáty vydávané Komerční bankou, a.s. Kapacita karty KB QSCD je dostatečná, takže držitel může mít na své kartě uloženy všechny své klíče s certifikáty. Klíče jsou chráněny hodnotou PIN, klíče spojené s kvalifikovaným certifikátm v QSCD režimu pak QPINem

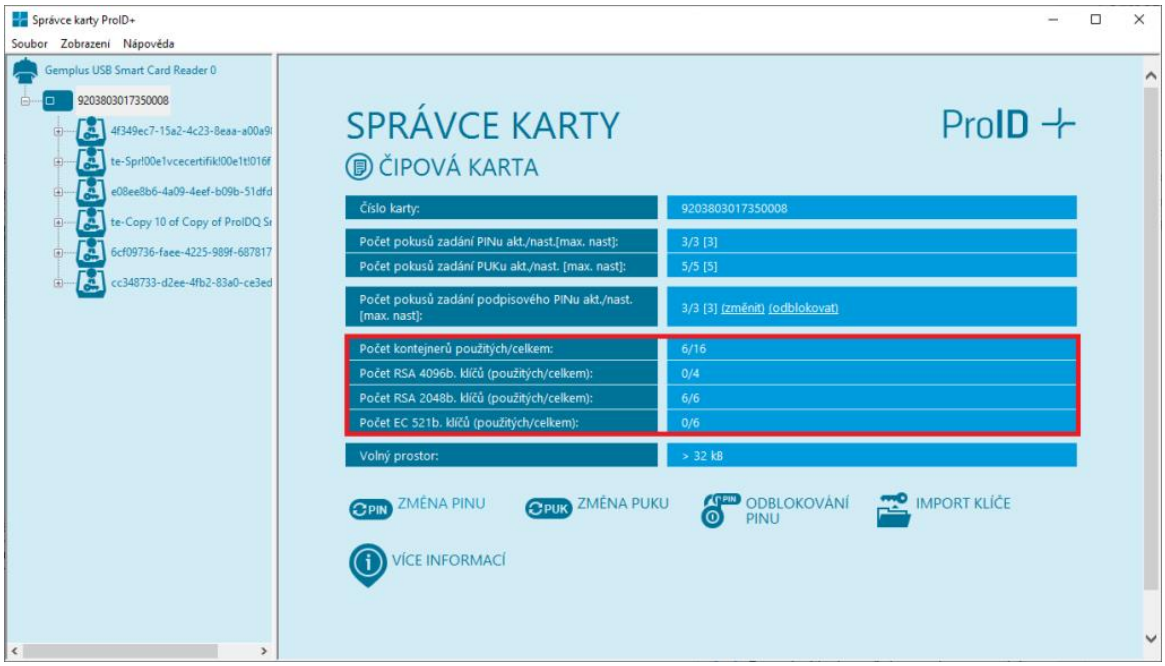
KOLIK CERTIFIKÁTŮ JE MOŽNÉ NA KARTU ULOŽIT?

Karty KB QSCD dodávány s úložnou kapacitou pro

- RSA klíčů 2048 bitů 10x

Karty KB QSCD dodávány s úložnou kapacitou pro

- RSA klíčů/kvalifikovaných max 4096 bitů 2x
- RSA klíčů/komerčních max 4096 bitů 2x
- ECC klíčů/kvalifikovaných max 521 bitů 2x
- ECC klíčů/komerčních max 521 bitů 2x



Detailní informace o zaplnění karty lze zobrazit pomocí aplikace Správce karty, kde se po označení karty ve stromové struktuře levého panelu zobrazí v pravém panelu příslušné informace.

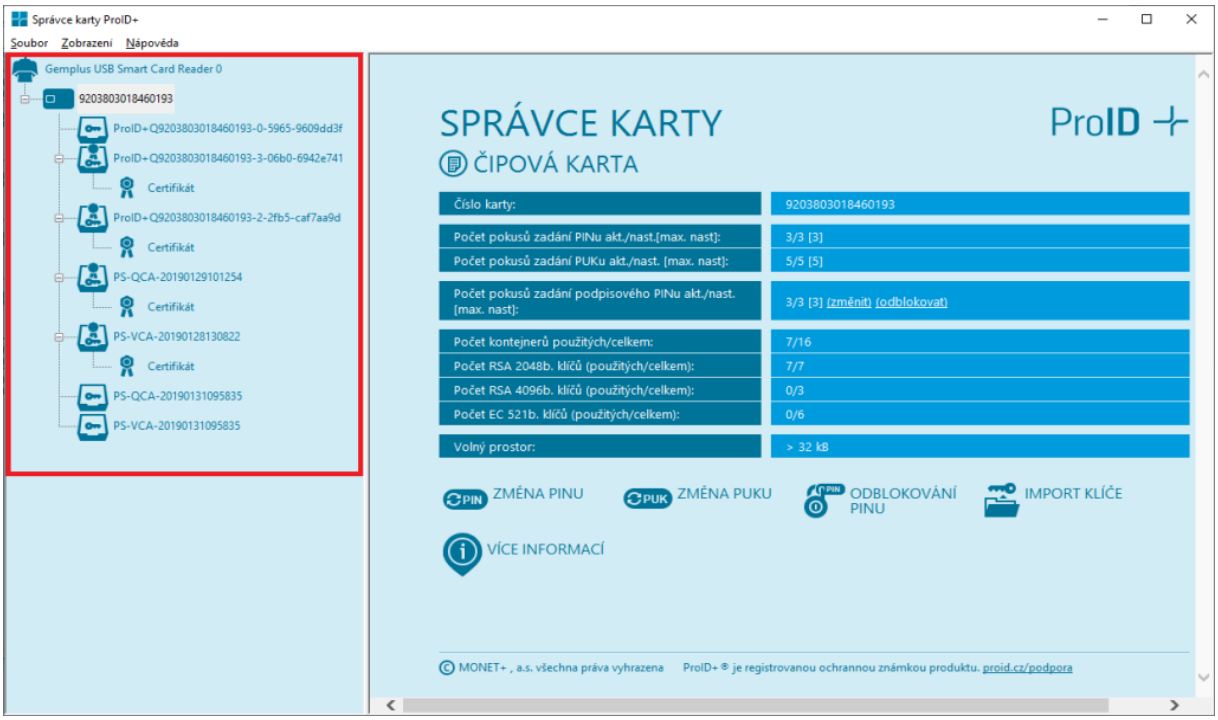
ČIPOVÁ KARTA QSCD – NÁVODY A NEJČASTĚJI KLADENÉ DOTAZY

JAK MOHU ZJISTIT, CO JE NA KARTĚ ULOŽENO?

Obsah karty KB QSCD lze zobrazit pomocí aplikace Správce karty. Po spuštění aplikace je třeba načíst obsah karty tlačítkem Obnovit, popř. funkční klávesou F5. Karta musí být po celou dobu načítání informací zasunuta ve čtečce.

V levém panelu Správce karty se zobrazí v přehledné stromové struktuře důležité objekty:

- Čtečka čipových karet identifikovaná jejím názvem a pořadovým číslem
- Karta KB QSCD identifikovaná číselným označením karty
- Uživatelské objekty na kartě – se vážící certifikát



Jednotlivé objekty lze zvolit pomocí myši a získat tak detailnější informace, které jsou zobrazeny v pravém panelu aplikace.

Aplikaci Správce karty najdete v adresáři c:\Program files\Cryptoplus\KB QSCD. Na operačním systému MacOS najdete správce karty pod názvem “Správce karty”.

JE MOŽNÉ CERTIFIKÁT Z KARTY VYMAZAT?

Aplikace KB spravují certifikáty na kartě samy. Neměli byste mít potřebu manuálně zasahovat do karty a nedoporučujeme jakkoliv zasahovat do obsahu karty bez konzultace nebo přímého pokynu od bankovního poradce nebo Kontaktního centra.

LZE Z KARTY EXPORTOVAT KLÍČ S CERTIFIKÁTEM?

Soukromý klíč nelze z karty exportovat ani kopírovat; to je základní bezpečnostní vlastnost karty KB QSCD.

Certifikát (s veřejným klíčem) lze z karty exportovat pomocí aplikace Správce karty. V levé části okna se zvolí certifikát k exportu a v pravé části se použije volba Export do souboru.

V dalším kroku se zvolí umístění a název souboru a export se provede použitím tlačítka Uložit.

JE MOŽNÉ Z KARTY VYMAZAT KLÍČ S CERTIFIKÁTEM?

Viz dotaz JE MOŽNÉ CERTIFIKÁT Z KARTY VYMAZAT?

JE MOŽNÉ NA KARTU IMPORTOVAT CERTIFIKÁT ULOŽENÝ V SOUBORU?

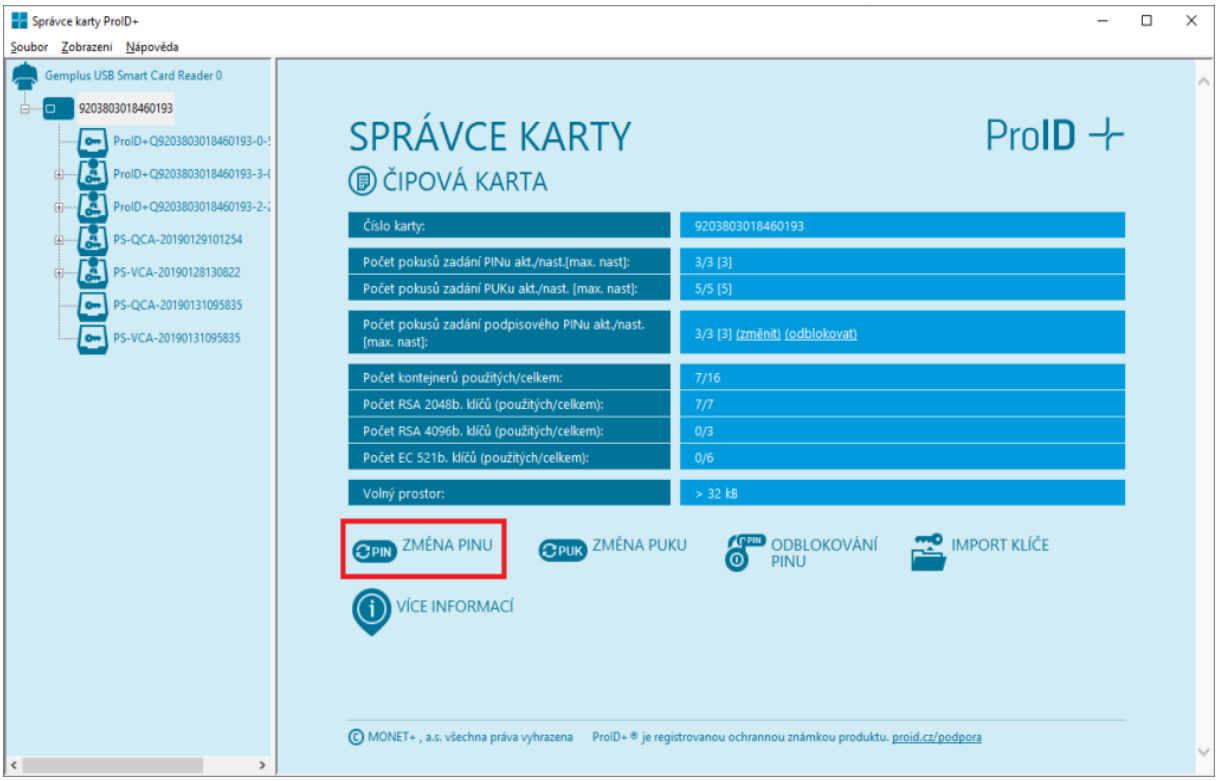
Pomocí aplikace Správce karty je možné na kartu KB QSCD nelze importovat certifikát společně ani soukromým klíč.

JE MOŽNÉ ZMĚNIT KÓD PIN, QPIN A PUK KARTY?

Změna kódu PIN pomocí aplikace Správce Karty

Změnu kódu PIN je možné provést pomocí aplikace Správce karty. Změna PINu je podmíněna znalostí současné (původní) hodnoty.

V levém panelu se zvolí objekt karty a v pravém panelu se použije tlačítko Změna PINu.



Dále se zobrazí dialog Změna uživatelského PINU.

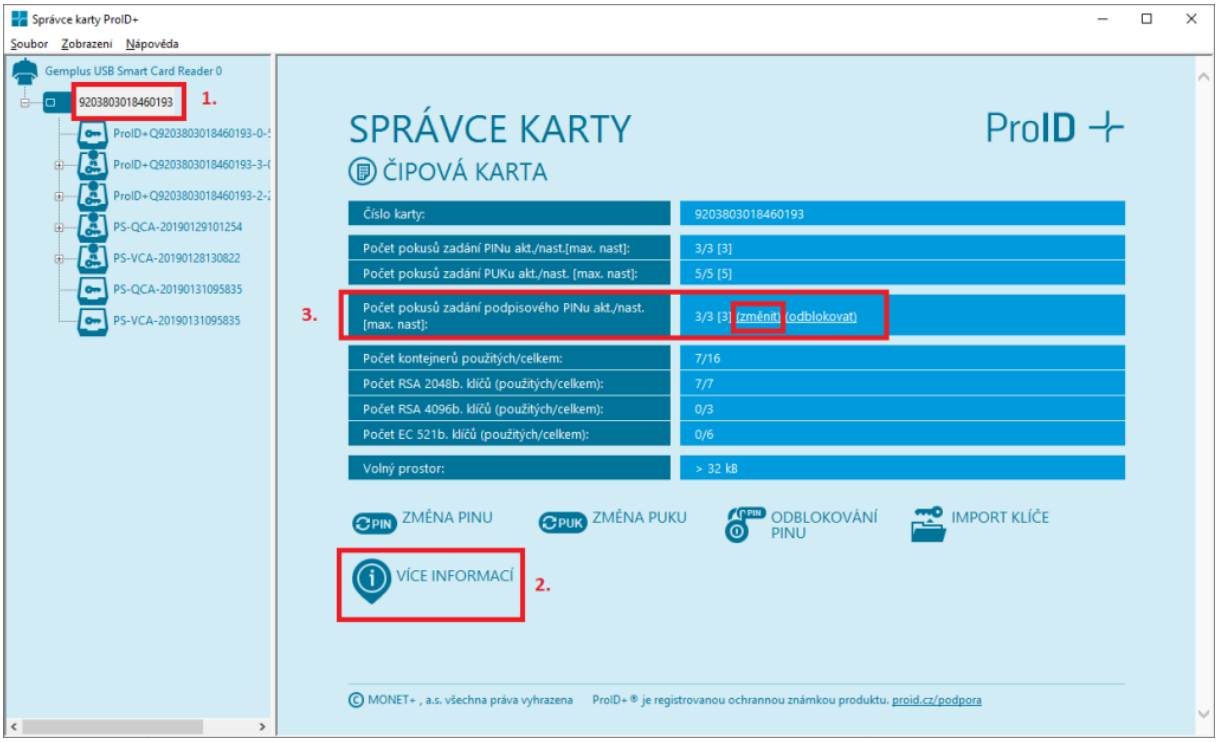
Do pole PIN se zadá původní hodnota PINu, do pole Nový PIN se zadá nová hodnota PINu. Novou hodnotu je nutné – pro kontrolu – zopakovat v poli Nový PIN zopakovaný. Po stisku tlačítka Změnit se provede požadovaná změna hodnoty PIN.

ČIPOVÁ KARTA QSCD – NÁVODY A NEJČASTĚJI KLADENÉ DOTAZY

Změna kódu QPIN (podpisový PIN) pomocí aplikace Správce Karty

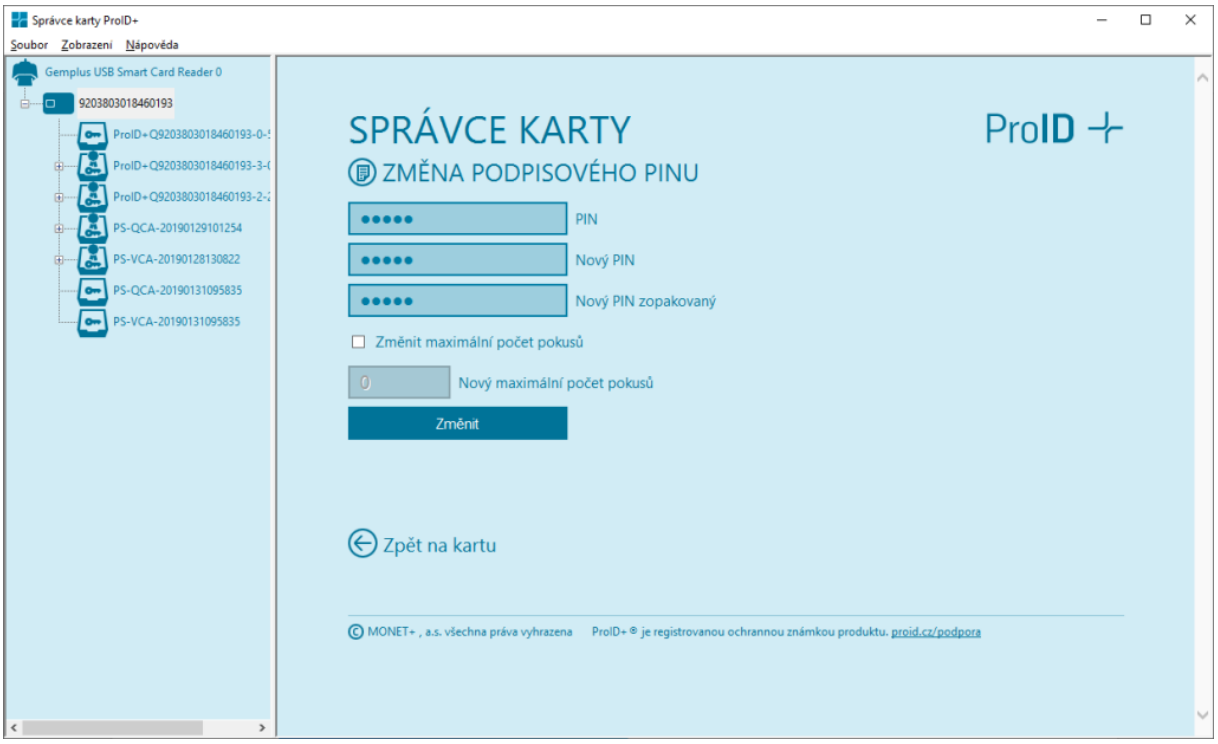
Změnu kódu QPIN je možné provést pomocí aplikace Správce karty. Změna QPINu je podmíněna znalostí současné (původní) hodnoty.

1. V levém panelu se zvolí objekt karty
2. Po kliknutí na tlačítko Více informací se zpřístupní Informace o Počtu pokusů zadání podpisového pinu. Je zde k dispozici tlačítko Změnit
3. Tlačítko Změnit vyvolá dialog Změna podpisového pinu (QPINu).



Dále se zobrazí dialog Změna podpisového PINU

Do pole PIN se zadá původní hodnota PINu, do pole Nový PIN se zadá nová hodnota PINu. Novou hodnotu je nutné – pro kontrolu – zopakovat v poli Nový PIN zopakovaný. Po stisku tlačítka Změnit se provede požadovaná změna hodnoty PIN.

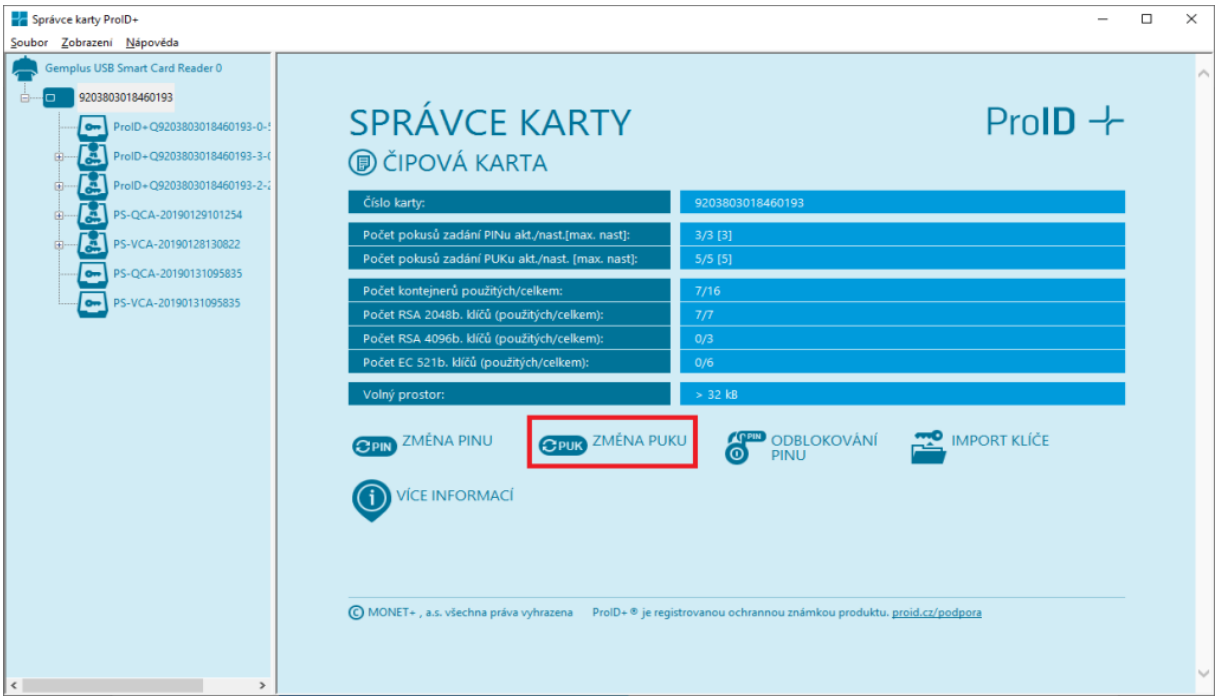


Změna maximálního počtu pokusů zadání hodnoty kódu Podpisového PINu (QPIN) není u karet KB QSCD možná.

Změna kódu PUK pomocí aplikace Správce Karty

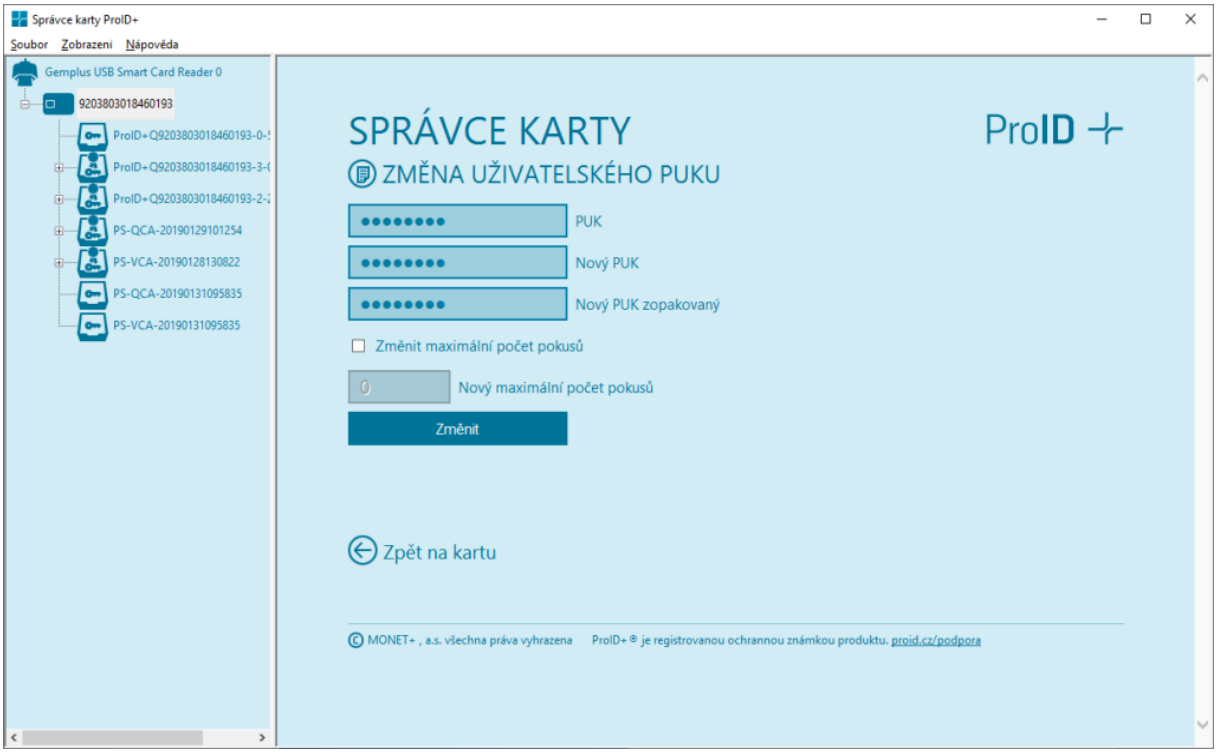
Změnu kódu PUK je možné provést pomocí aplikace Správce karty. Změna PUKu je podmíněna znalostí současné (původní) hodnoty.

V levém panelu se zvolí objekt karty a v pravém panelu se použije tlačítko Změna PUKu.



Dále se zobrazí dialog Změna PUKU.

Do pole PUK se zadá původní hodnota PUKu, do pole Nový PUK se zadá nová hodnota PUKu. Novou hodnotu je nutné – pro kontrolu – zopakovat v poli Nový PUK zopakovaný. Po stisku tlačítka Změnit se provede požadovaná změna hodnoty PUK.



ČIPOVÁ KARTA QSCD – NÁVODY A NEJČASTĚJI KLADENÉ DOTAZY

ZTRATIL/ZAPOMNĚL JSEM PIN K ČIPOVÉ KARTĚ KB QSCD

PIN (Personal Identification Number) je sada alfanumerických znaků, která autorizuje přístup k chráněným objektům na kartě (soukromých klíčů). Bez znalosti PINu nelze kartu použít (ani zneužít).

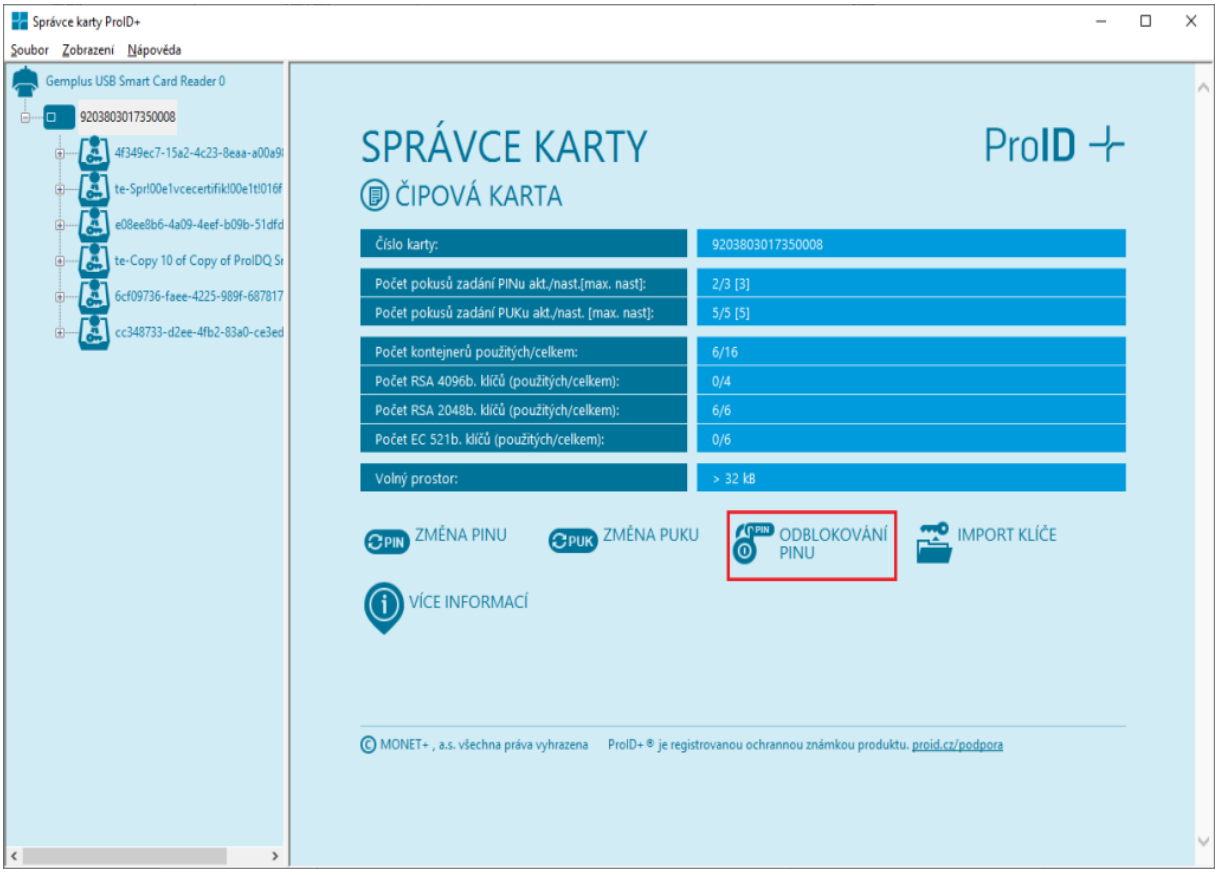
V případě ztráty nebo zablokování PINu lze na kartě nastavit novou hodnotu kódu PIN. Tuto operaci je však nutné autorizovat. Autorizaci lze provést:

1. Kódem PUK (Pin Unblocked Key) – dodaným uživateli spolu s kartou KB QSCD

Nový PIN lze nastavit např. v aplikaci Správce karty.

Odblokování kódu PIN – nastavení nové hodnoty kódu PIN pomocí kódu PUK ve Správci karty

Po načtení karty ve Správci karty (tlačítko Obnovit/F5)se v levém panelu označí karta. V pravém panelu se stiskne tlačítko Odblokování PINu. Do pole **PUK** se zadá hodnota kódu PUK, dodaného k čipové kartě. Do pole **Nový PIN** se zadá nová hodnota kódu PIN. Novou hodnotu je nutné pro kontrolu zopakovat v poli **Nový PIN zopakovaný.**



ČIPOVÁ KARTA QSCD – NÁVODY A NEJČASTĚJI KLADENÉ DOTAZY

ZTRATIL/ZAPOMNĚL JSEM PODPISOVÝ PIN (QPIN) K ČIPOVÉ KARTĚ KB QSCD

PIN (Personal Identification Number) je sada alfanumerických znaků, která autorizuje přístup k chráněným objektům na kartě (soukromých klíčů). Bez znalosti PINu nelze kartu použít (ani zneužít).

Podpisový PIN pro kvalifikované elektronické podpisy (QPIN) – slouží ke schvalování kvalifikovaného elektronického podpisu.

Používá se při každém vytváření kvalifikovaného elektronického podpisu.

V případě ztráty nebo zablokování QPINu lze na kartě nastavit novou hodnotu kódu QPIN. Tuto operaci je však nutné autorizovat. Autorizaci lze provést:

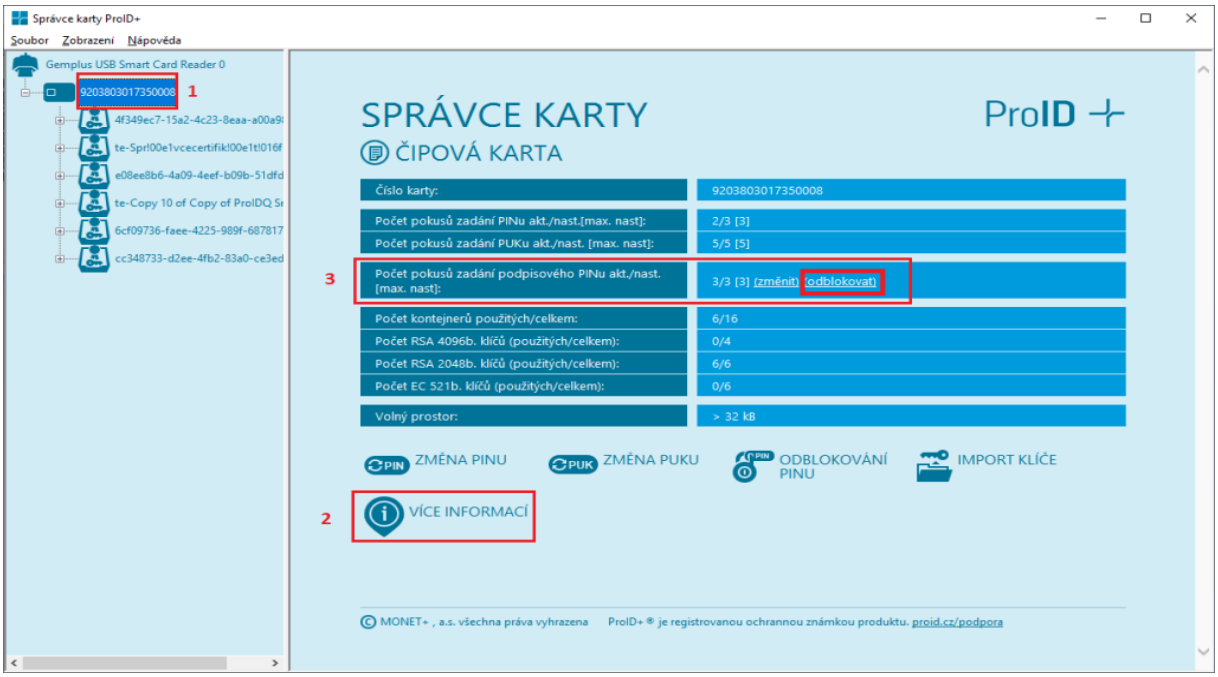
- Kódem PUK (Pin Unblocked Key) – dodaným uživateli spolu s kartou KB QSCD

Nový QPIN lze nastavit např. v aplikaci Správce karty.

Odblokování kódu QPIN – nastavení nové hodnoty kódu QPIN pomocí kódu PUK ve Správci karty

Odblokování kódu QPIN je možné provést pomocí aplikace Správce karty.

1. V levém panelu se zvolí objekt karty
2. Po kliknutí na tlačítko Více informací se zpřístupní Informace o Počtu pokusů zadání podpisového pinu. Je zde k dispozici tlačítko Odblokovat
3. Tlačítko Odblokovat vyvolá dialog Odblokování podpisového PINU.



Dále se zobrazí dialog Odblokování podpisového PINU

Do pole PUK se zadá hodnota PUKu, do pole Nový PIN se zadá nová hodnota QPIN

Novou hodnotu QPIN je nutné – pro kontrolu – zopakovat v poli Nový PIN zopakovaný. Po stisku tlačítka Odblokovat se provede požadovaná změna hodnoty QPIN.

ČIPOVÁ KARTA QSCD – NÁVODY A NEJČASTĚJI KLADENÉ DOTAZY

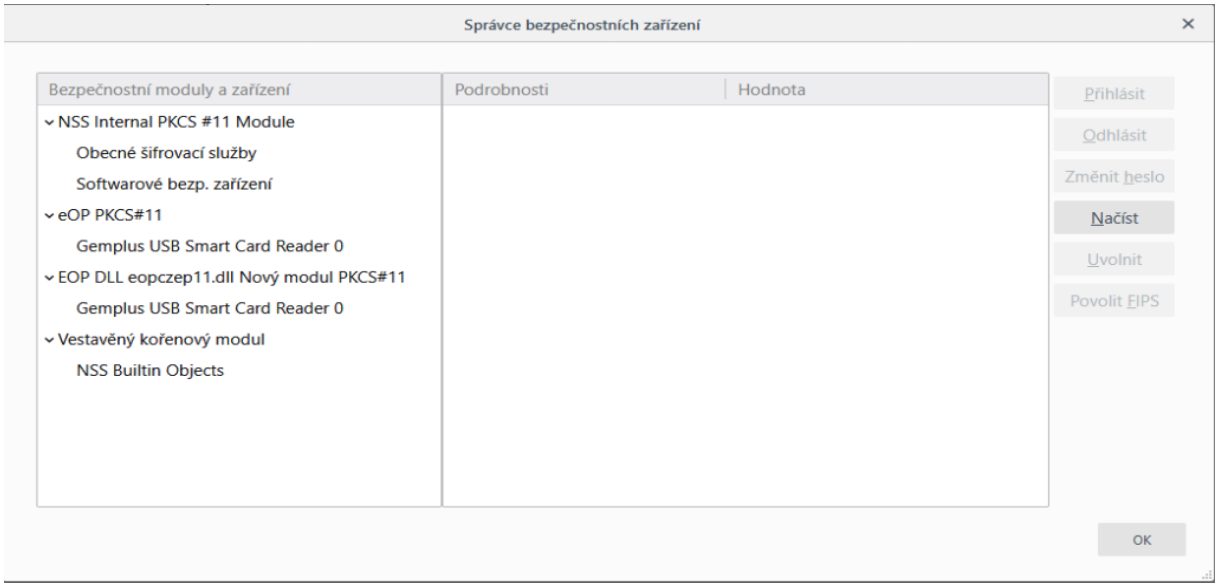
JAK MOHU POUŽÍT KARTU KB QSCD V APLIKACÍCH MOZILLA FIREFOX NEBO THUNDERBIRD?

Webový prohlížeč Mozilla Firefox i poštovní klient Thunderbird mají zabudovanou podporu pro práci s bezpečnostními certifikáty. Jako úložiště klíčů a certifikátů umožňují použít čipovou kartu KB QSCD prostřednictvím standardizovaného modulu PKCS#11 (též nazývaný Cryptoki). Tento modul je součástí standardního instalačního balíčku a má formu dynamicky linkované knihovny (DLL). Jeho jméno je proidcm11.dll a je instalován do systémového adresáře.

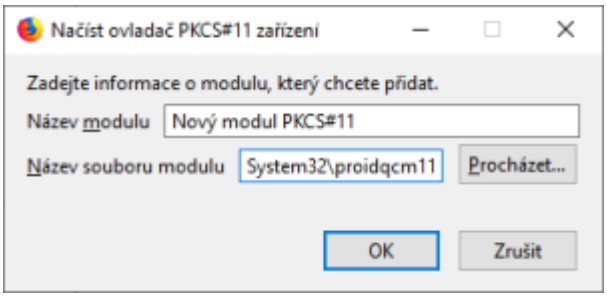
Modul přidaný v aplikaci Mozilla Firefox není automaticky dostupný v Thunderbird a naopak. Pro každou aplikaci je nutné registrovat modul samostatně.

Před použitím je nutné modul zaregistrovat. To lze provést v menu příslušné aplikace.

- Firefox: Nástroje – Možnosti – Soukromí a zabezpečení – Certifikáty – Bezpečnostní zařízení.
- Thunderbird: Nástroje – Možnosti – Rozšířené – Certifikáty – Bezpečnostní zařízení.

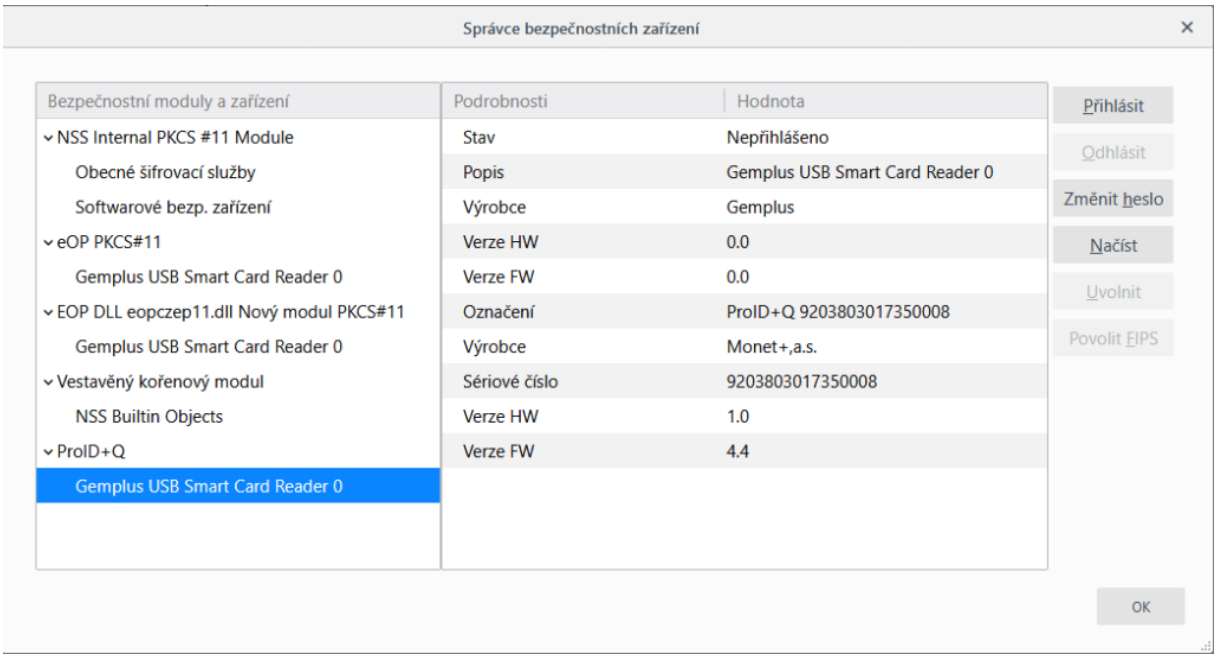


Správce bezpečnostních zařízení zobrazuje seznam všech registrovaných modulů. Další modul lze přidat stiskem tlačítka **Načíst**. Do pole **Jméno modulu** se vyplní libovolný název (např. KBQSCD). Do pole **Název souboru modulu** se zapíše proidcm11.dll. V případě použití karty KB QSCD použijte soubor proidqcm11.dll.

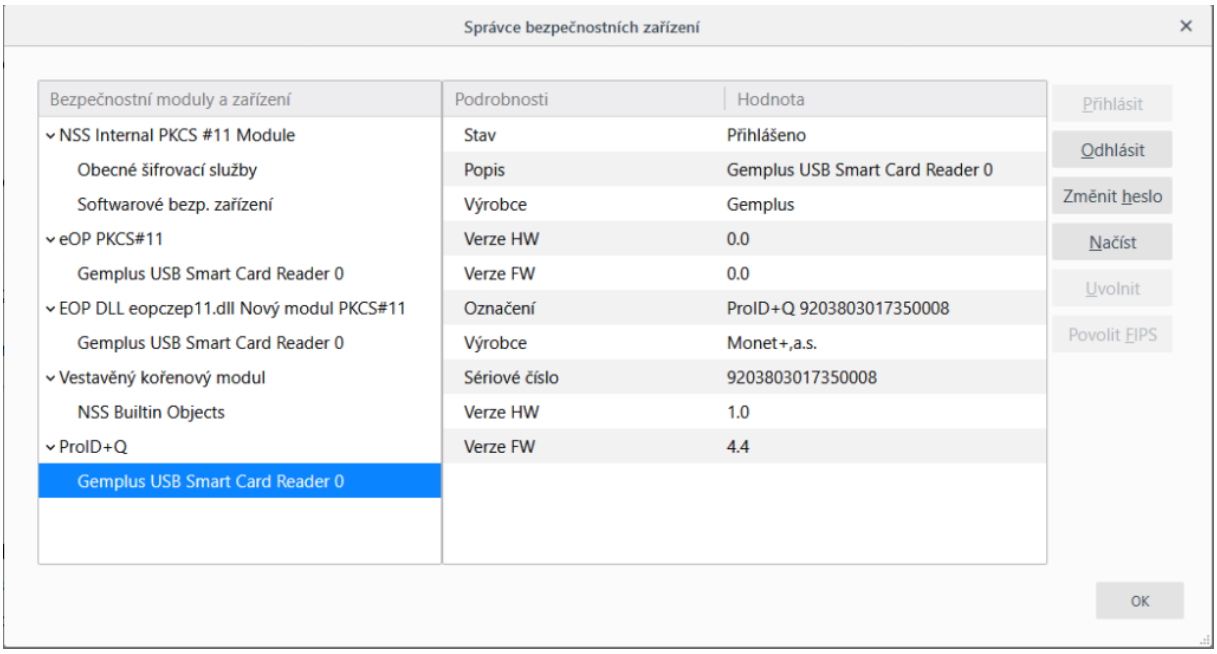


Alternativně lze modul vybrat pomocí tlačítka Procházet v systémovém adresáři (standardně C:\Windows\System32).

Po stisku tlačítka OK aplikace zobrazí modul KB QSCD P11 ve stromu informuje o výsledku přidání modulu.



Použitím volby Přihlásit a vložením kódu PIN se stav modulu změní na Přihlášen.



Správce bezpečnostních zařízení se uzavře stiskem tlačítka OK. Tímto je aplikace připravena k používání karty KB QSCD.

FIREFOX/THUNDERBIRD HLÁSÍ, ŽE CERTIFIKÁT NENÍ DŮVĚRYHODNÝ

Zjednodušeně lze říci, že certifikát je pro danou aplikaci důvěryhodný, pokud je certifikát certifikační autority uveden v seznamu důvěryhodných certifikátů a nastaven příznak důvěryhodnosti pro danou množinu použití. Mozilla Firefox ani Thunderbird nepoužívají úložiště certifikátů Windows, proto je nutné importovat certifikáty certifikačních autorit do

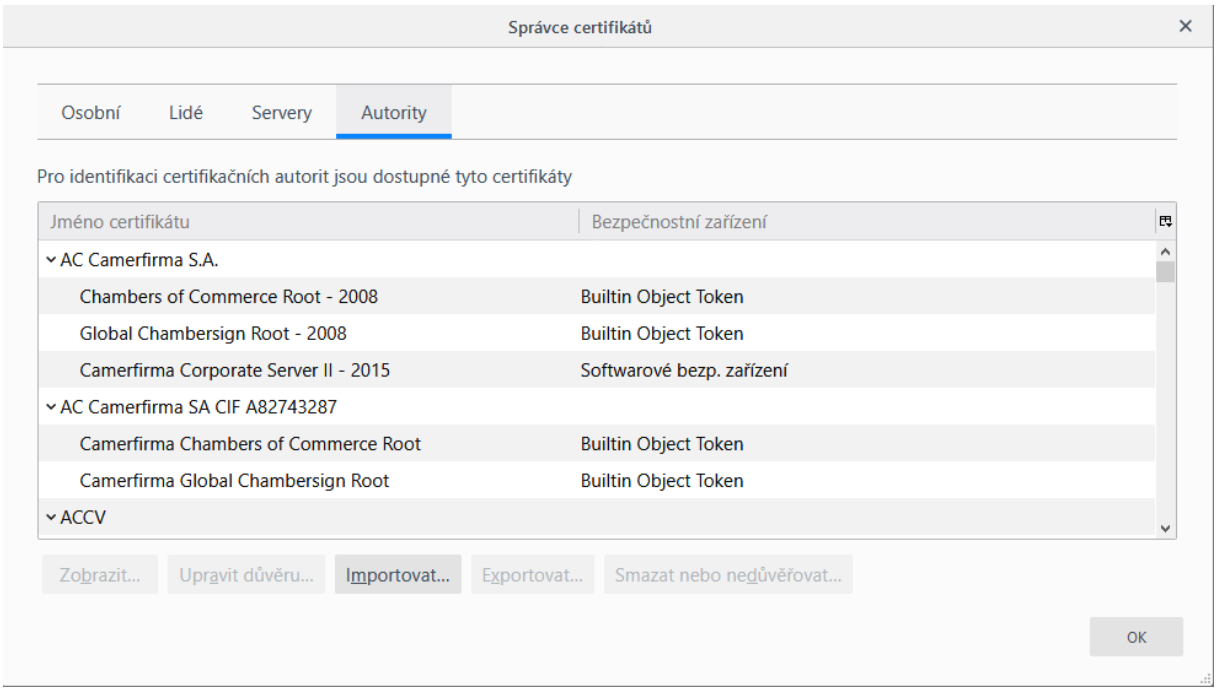
jejich lokálních úložišť. Každá z aplikací si spravuje tato úložiště samostatně. Import certifikátu do úložiště Firefox neovlivní obsah úložiště Thunderbird a naopak.

JAK NAIMPORTUJI CERTIFIKÁT CERTIFIKAČNÍ AUTORITY DO ÚLOŽIŠTĚ APLIKACÍ MOZILLA FIREFOX NEBO THUNDERBIRD?

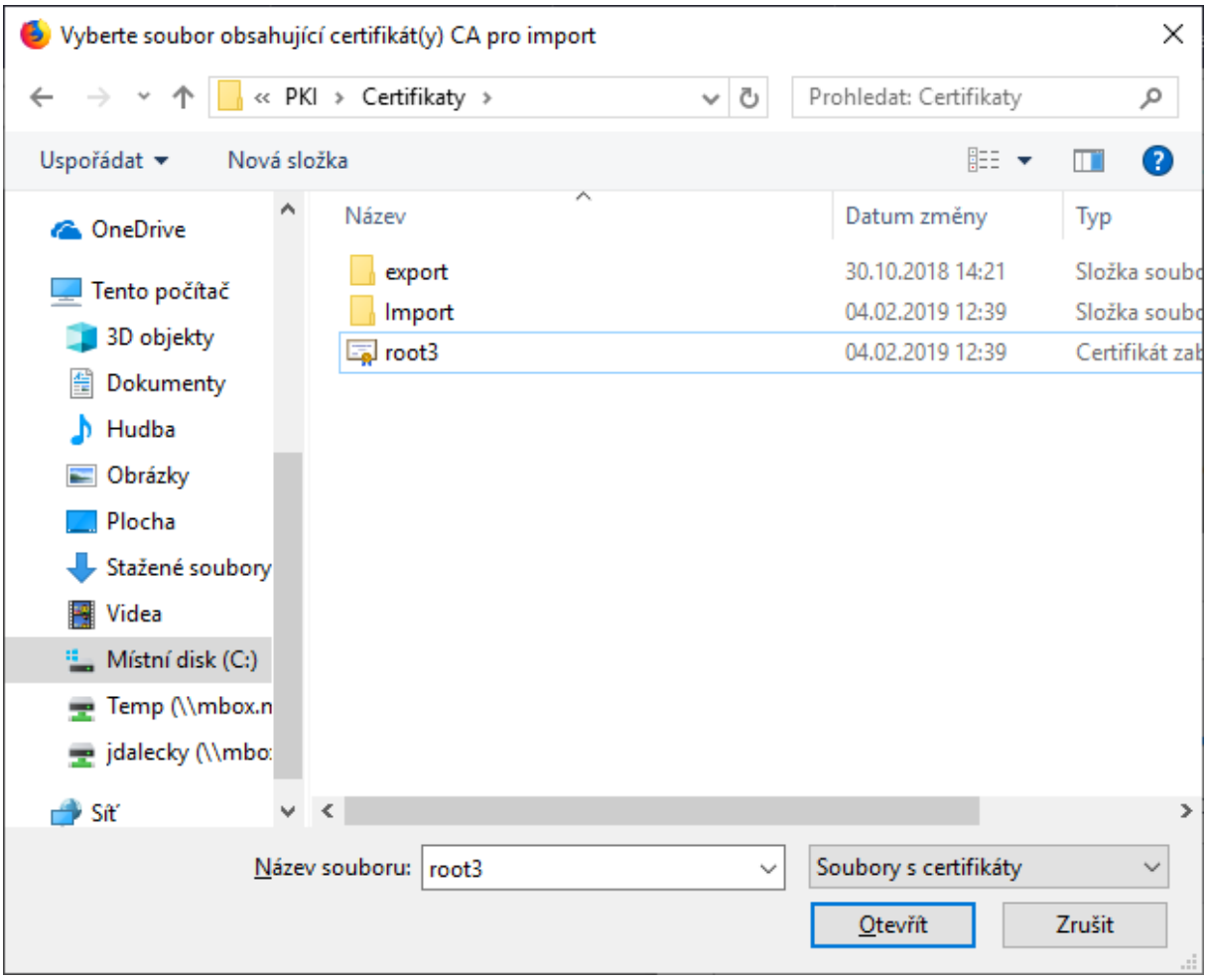
Import certifikátů certifikační autority lze provést v menu příslušné aplikace:

- Firefox: Nabídka Nástroje – Možnosti – Rozšířené – Certifikáty
- Thunderbird: Nabídka Úpravy – Předvolby – Rozšířené – Certifikáty – Certifikáty

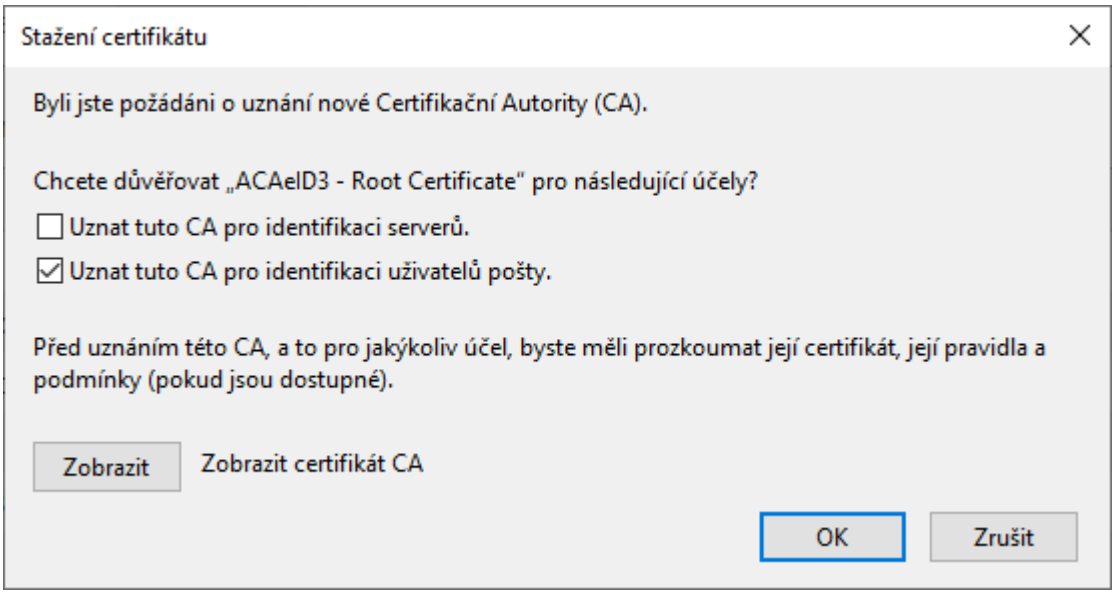
Zobrazí se okno s názvem Správce certifikátů. Vybere se záložka Autority a stiskněte tlačítko Importovat.



V počítači vyhledejte soubor obsahující certifikát vydávající certifikační autority, označte jej a stiskněte tlačítko Otevřít.



Před potvrzením importu certifikátu se současně zvolí účel, pro který je certifikát důvěryhodný.



Import se dokončí stiskem tlačítka OK a opět OK. Pokud se používají certifikáty více certifikačních autorit, je nutné postup opakovat pro každou certifikační autoritu zvlášť.

CHCI POUŽÍT KARTU KB QSCD V APLIKACI ADOBE READER

Koncepce použití karty KB QSCD a bezpečnostních certifikátů v Adobe Reader do značné míry kopíruje koncept použití ve Firefox nebo Thunderbird.

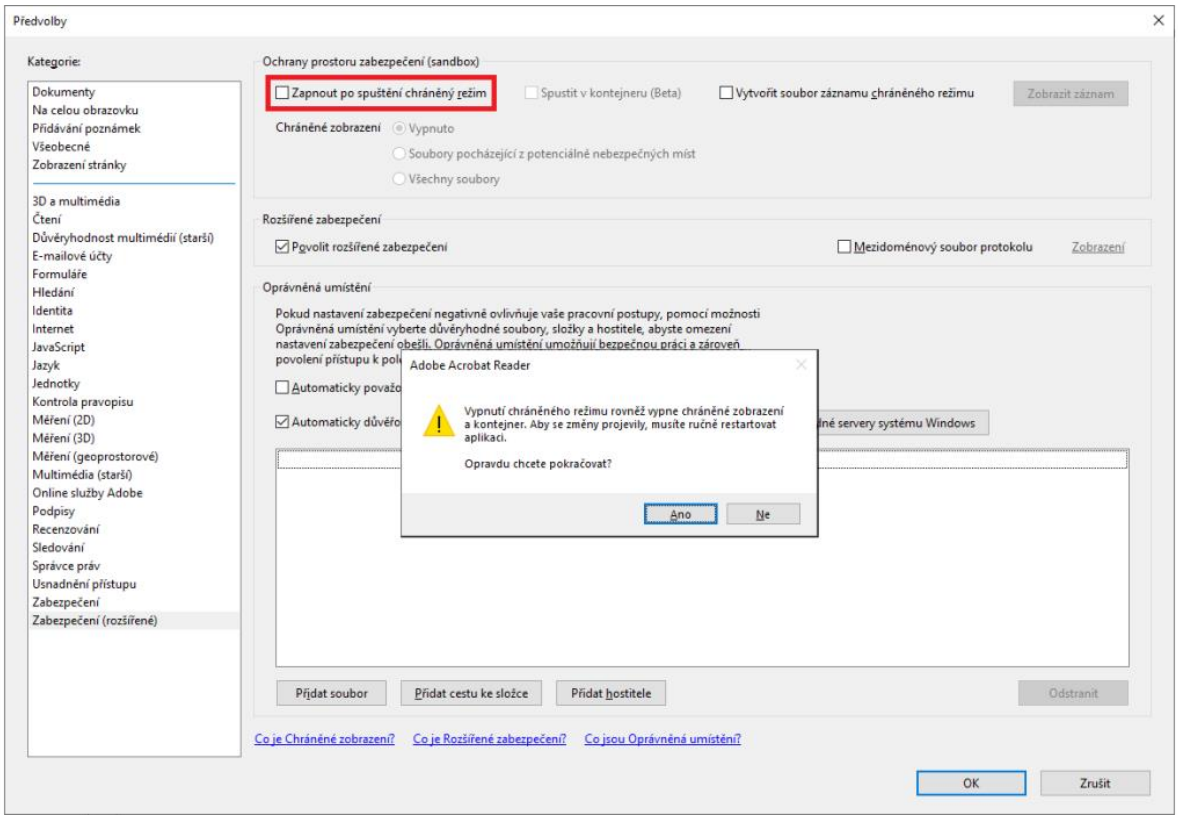
Jednotlivé kroky vedoucí ke zprovoznění podpory KB QSCD v Adobe Readeru jsou však mírně odlišné.

Zpřístupnit certifikát lze buď v operačním systému Windows jeho registrací mezi osobní certifikáty prostřednictvím aplikace Správce karty, volnou registrovat certifikát do Windows.

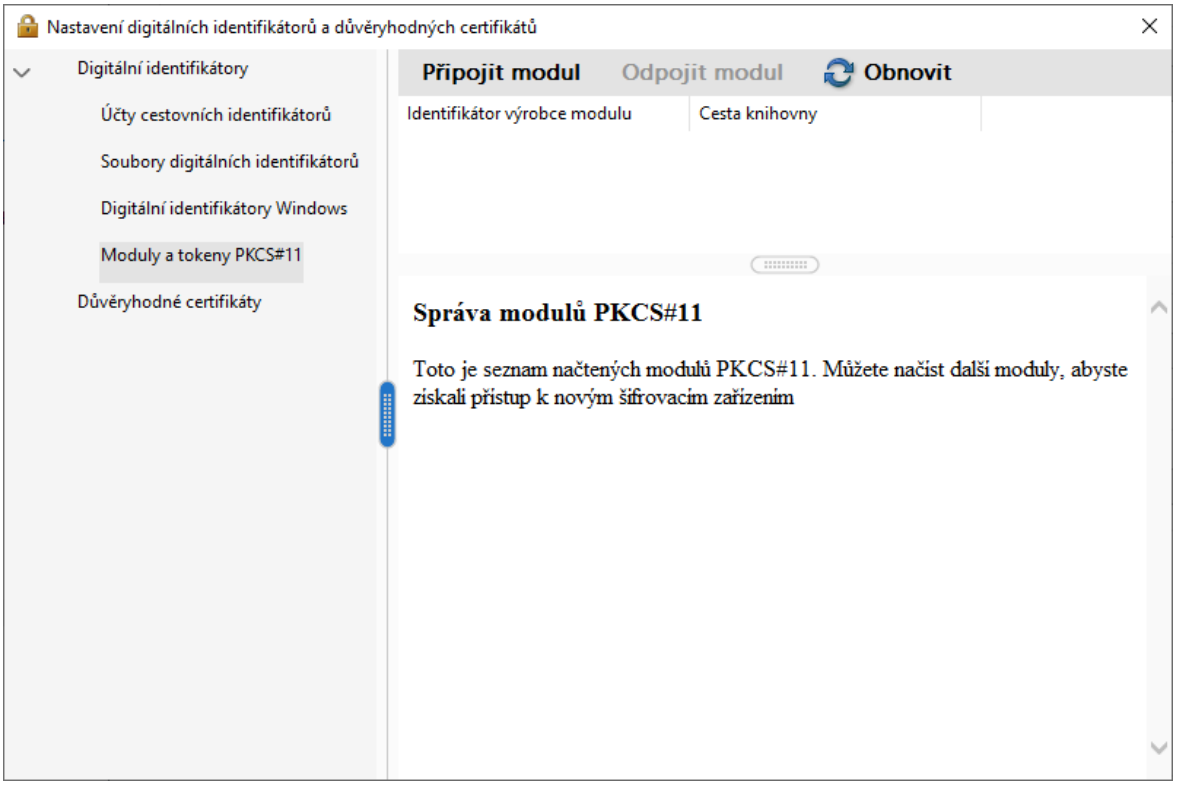
Druhá možnost je registrací PKCS11 modulu.

Ve výchozím nastavení má Adobe Reader zapnut tzv. Chráněný režim. Tento režim omezuje přístup souborů PDF do systému, čímž chrání Windows před škodlivými kódy, které by mohly modifikovat součásti operačního systému. Toto omezení však znemožňuje přístup aplikace k modulu PKCS#11. Pro správnou funkčnost modulu je tedy nutné Chráněný režim deaktivovat. Deaktivace Chráněného režimu může zvýšit riziko infikace systému škodlivým kódem!

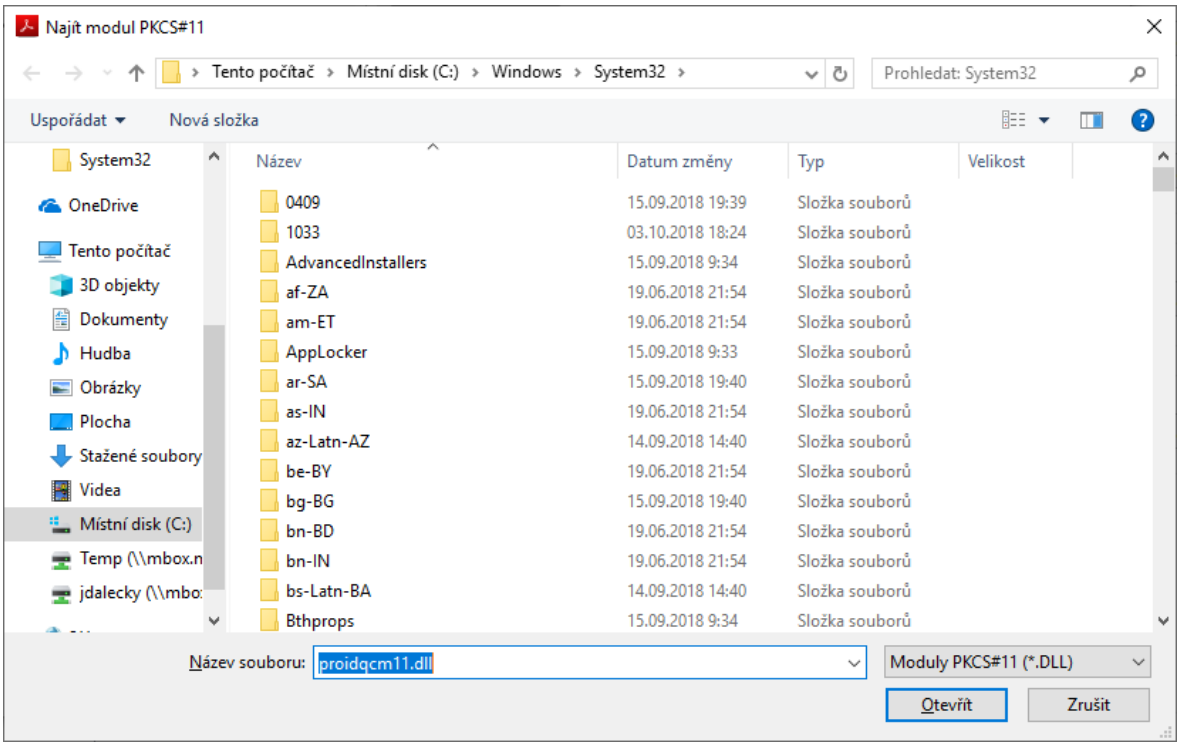
V hlavní nabídce se zvolí menu Úpravy – Předvolby – Zabezpečení (Rozšířené) a zruší se zatržení u pole Zapnout po spuštění chráněný režim. Deaktivace se potvrdí stiskem tlačítka Ano. Proces se dokončí stiskem tlačítka OK a restartem aplikace.



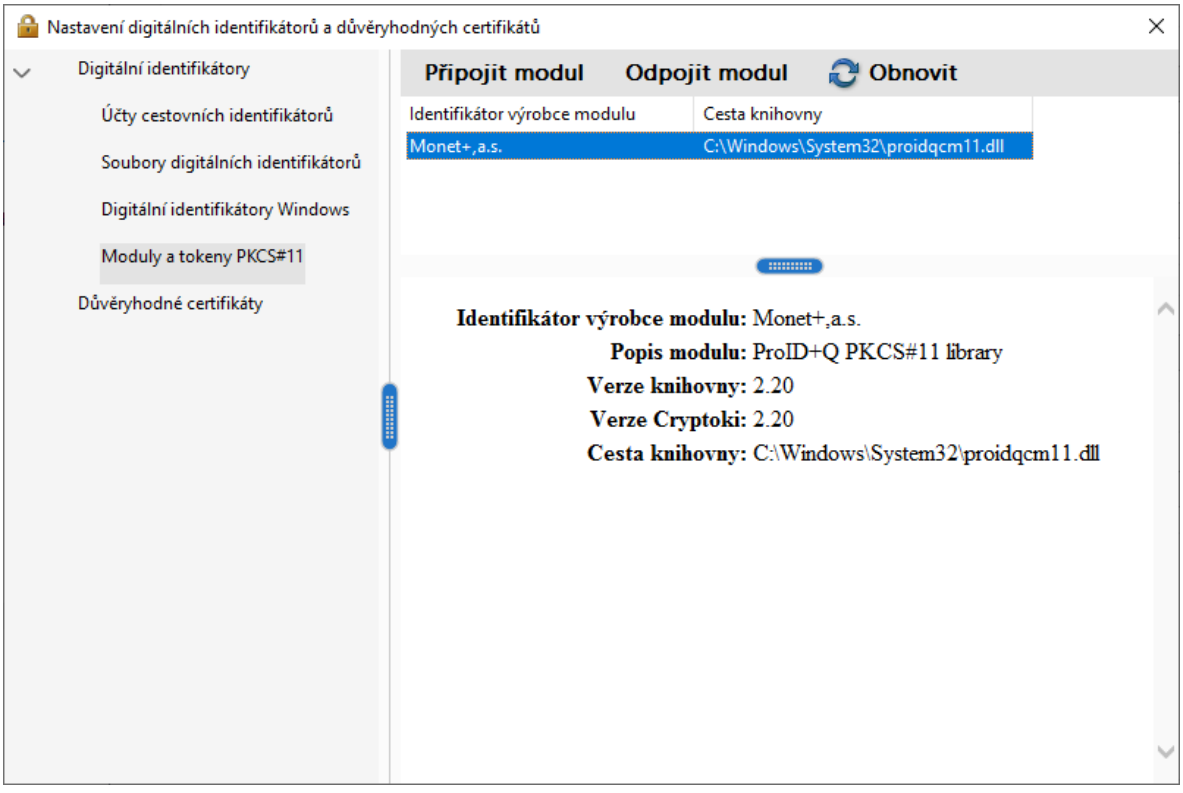
Po opětovném spuštění se zvolí v hlavní nabídce Úpravy – Předvolby – Podpisy – Identity a důvěryhodné certifikáty – tl. Další. Zobrazí se okno Nastavení digitálních identifikátorů a důvěryhodných certifikátů. Označí se položka Moduly a tokeny PKCS#11 a stiskne se tlačítko Připojit modul.



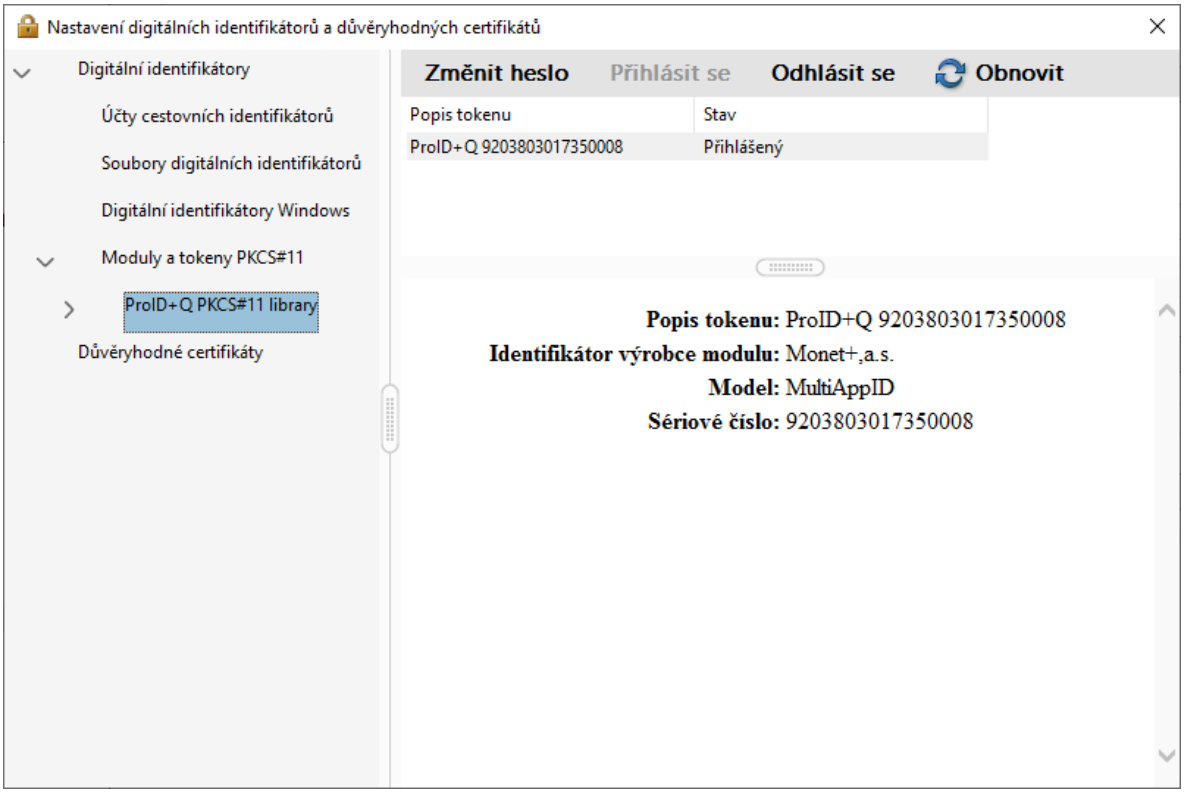
V případě karty KB QSCD se v počítači vyhledá soubor mopkcs11.dll. Pokud používáte kartu KB QSCD tak vyhledejte soubor mopkcs11.dll (instaluje se do systémového adresáře, standardně v C:\Windows\System32\) a stiskne se tlačítko Otevřít.



Po uzavření okna Nastavení digitálních identifikátorů se stiskne tlačítko OK. Restartuje se aplikace Adobe Reader a poté je třeba znovu otevřít okno Nastavení digitálních identifikátorů, zvolit modul Monet+ MiniDriver PKCS#11 a použít tlačítko Přihlásit se.



Na vyžádání je třeba přihlásit se k čipové kartě: zadat PIN. Stav tokenu KB QSCD by se pak měl změnit na Přihlášený.



Stejně jako v aplikacích Firefox a Thunderbird je nutné provést import certifikátu CA; ve stejném okně je třeba zvolit položku Důvěryhodné certifikáty a provést import certifikátu CA tlačítkem Importovat.

PŘI POKUSU O VLOŽENÍ KVALIFIKOVANÉHO PODPISU NA MACOS SE ZOBRAZÍ CHYBA LIBRARY NOT LOADED: /USR/LOCAL/OPT/LIBPNG/LIB/LIBPNG16.16.DYLIB

Operační systém neobsahuje knihovnu libpng a je nutné ji doinstalovat.

Instalaci je možné provést pomocí správce balíků Homebrew https://brew.sh/index_cs

Příkaz pro instalaci repozitáře Homebrew:

/bin/bash -c "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/HEAD/install.sh)"

Příkaz pro instalaci knihovny:

brew install libpng