Manuál pro práci s kontaktním čipem

Obsah

1 Instalace

Pro práci s kontaktním čipem karty je nutné mít:

1) **Připojenou a nainstalovanou kontaktní čtečku karet** – u většiny čteček si nainstaluje ovladače operační systém sám. Ostatní čtečky je nutné nainstalovat ručně. Čtečka musí splňovat následující normy: ISO 7816 třída A, B a C karet (5 V, 3 V, 1,8 V). Čtení a zápis mikroprocesorových karet ISO 7816-1,2,3,4 a podpora protokolů T = 0 a T = 1.

2) **Nainstalovaný minidriver pro práci s čipem** – Automaticky nahrává při vložení karty do čtečky certifikáty z kontaktního čipu do uložiště certifikátů Microsoft. Soukromý klíč zůstává stále na kartě. To znamená, že všechny aplikace, které využívají uložiště Microsoft, uvidí certifikáty na kartě.

   Tento minidriver je možné získat dvěma způsoby:

   a. Uživatelům Windows 7 se minidriver nainstaluje automaticky pomocí Windows update
   b. Dále je možné stáhnout minidriver na adrese:
      i. Windows XP, Vista, 7, 32bit - http://www.oksystem.cz/df/2006
      ii. Windows XP, Vista, 7, 64bit - http://www.oksystem.cz/df/2008
      Umístění na disku po instalaci: Windows/system32/minidriver.dll

3) Aplikace, které nevyužívají uložiště certifikátů Microsoft (např. Thunderbird, Firefox, PES) mohou vyžadovat pro práci s certifikáty **nainstalovanou knihovnu PKCS#11**. Tu je možno stáhnout na adrese:

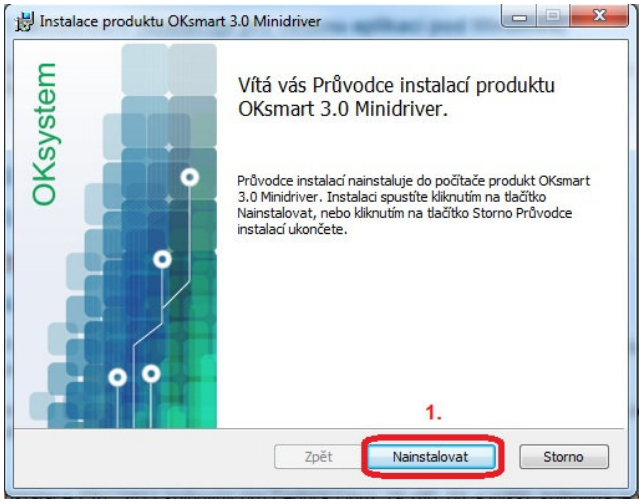
POZOR! Tato knihovna je nutná pro podepisování v Portálu ekonomických služeb (PES)

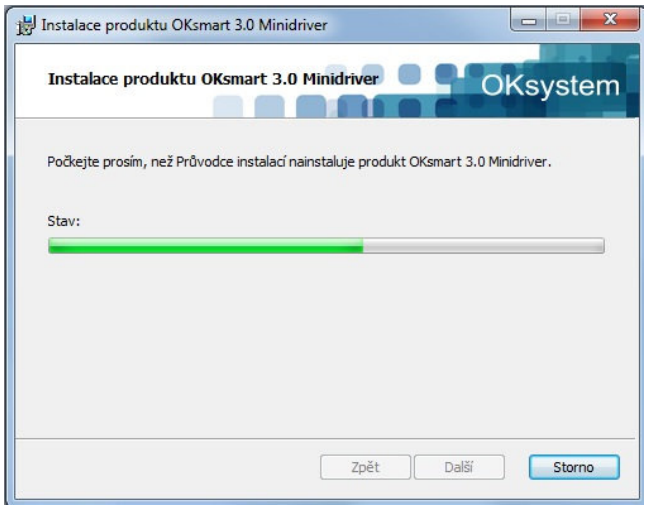
- Windows XP, Vista, 7, 32bit - https://pki.cvut.cz/soubory/oksmart32-pkcs11.msi
- Windows XP, Vista, 7, 64bit - https://pki.cvut.cz/soubory/oksmart64-pkcs11.msi
  - Umístění na disku po instalaci: Windows/system32/oksmartpkcs11.dll
- Fedora Linux 19 x86_64 a vyšší - http://www.oksystem.cz/df/2088
- Debian Linux 7 amd64 a vyšší - http://www.oksystem.cz/df/2090
  - Umístění na disku po instalaci: /usr/lib64/libokpkcs11.so

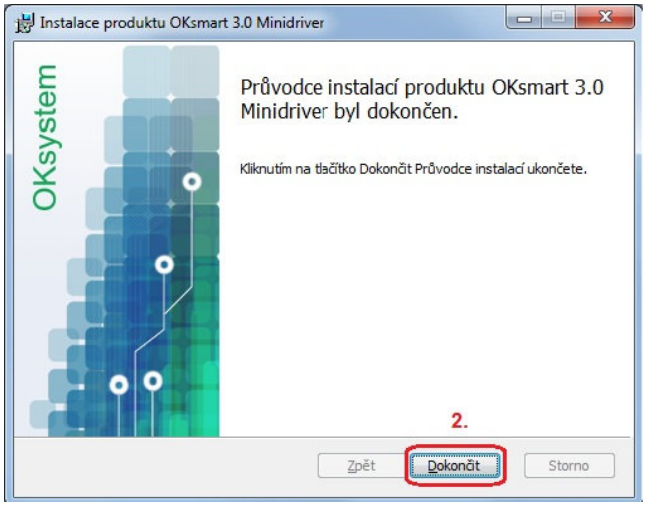
4) **Java minimální verze 5** - http://java.com/en/download/index.jsp
   Pro správnou funkci podpůrných aplikací (OKBase, OKsmart manager, PES …) je nutné při dotazu povolit spouštění JAVA appletů v prohlížečích.

1.1 Postup instalace minidriveru pro Windows (totožný pro PKCS#11 knihovny)

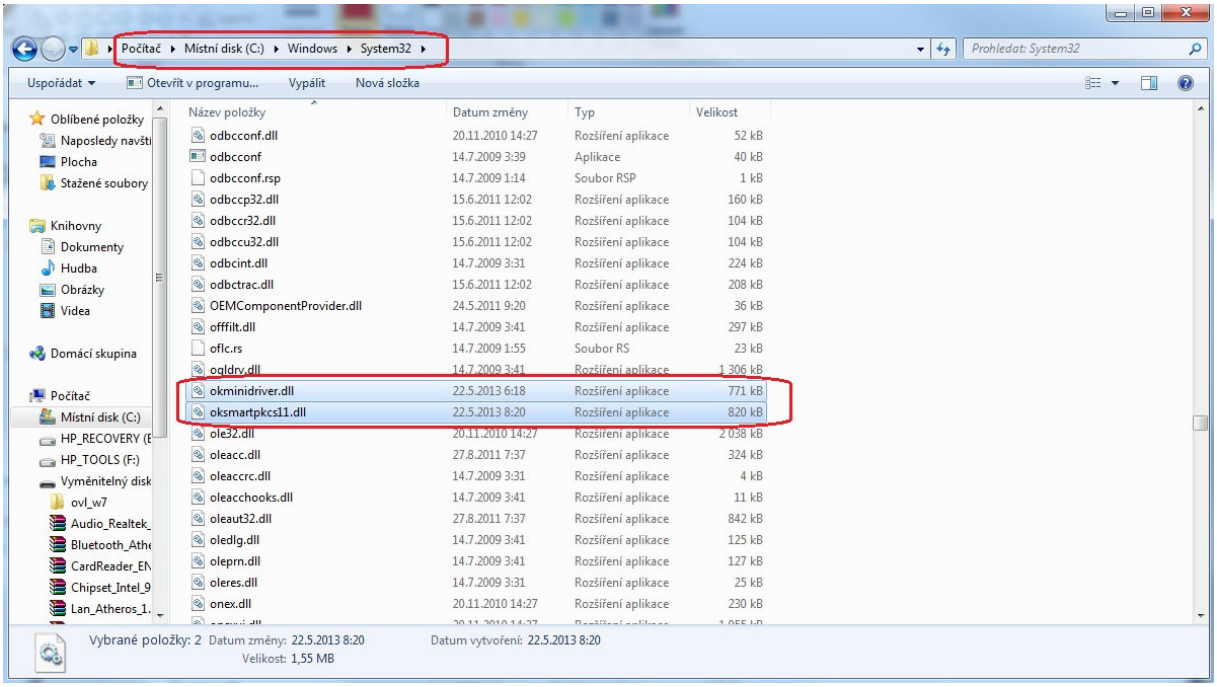
Spustíme stáhnutý instalační balíček







V případě problémů můžete ověřit umístění souborů dle obrázku.



2 Práce s PIN a PUK

Ke kartě s kontaktním čipem uživatel obdrží dva klíče PIN a PUK. PIN slouží pro autentizaci k operacím s kontaktním čipem, jako je podepisování, import certifikátu atd. Uživatel má 3 pokusy pro zadání správného PIN, poté je kontaktní čip zablokován. K odblokování čipu slouží klíč PUK. Odblokování je možné ve *Správě kontaktního čipu* tlačítkem *„Odblokovat PIN pomocí PUK“*. Při ztrátě PUK je nutné kontaktovat administrátora. PIN a PUK je možné si změnit dle vlastních představ ve *Správě kontaktního* čipu tlačítky: *„Změnit PIN“* a *„Změnit PUK“*.

3 Správa kontaktního čipu

Jedná se o webové rozhraní, ve kterém můžete spravovat svůj kontaktní čip.

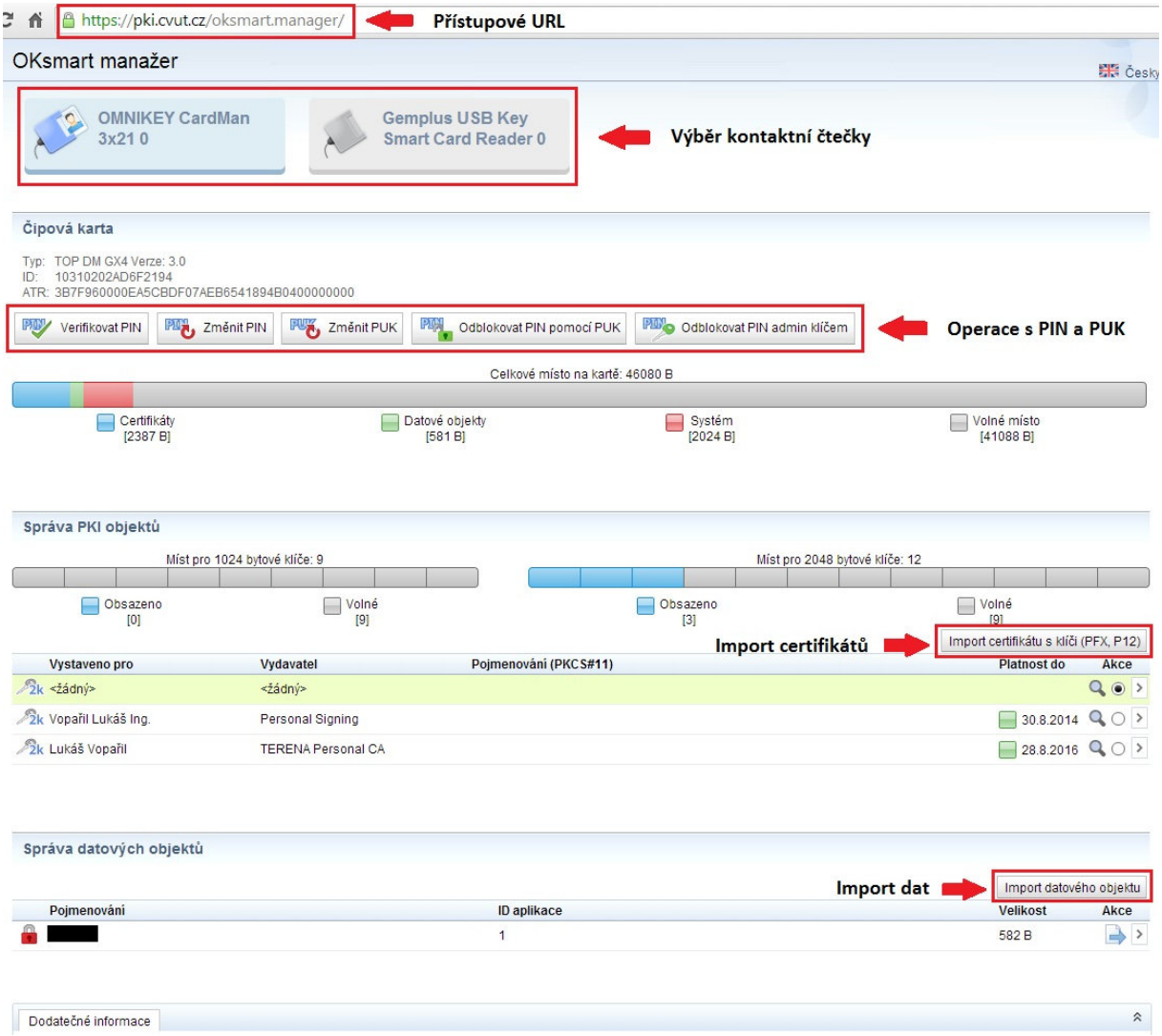
Jeho adresa je: https://pki.cvut.cz/oksmart.manager/

Pro přihlášení musíte mít vloženou kartu ve čtečce. Pokud máte zapojených více čteček, je nutné vybrat tu, ve které máte vloženou kartu.

Funkce správce kontaktního čipu:

- Přehled
- Operace s PIN a PUK
- Import a export certifikátů
- Import a export datových objektů

Pro využití těchto funkcí je nutné se autentizovat PIN kódem.



<u>Upozornění:</u> Při importu certifikátů doporučujeme udělat zálohu certifikátů. Kontaktní čip neumožnuje zpětný export soukromé části certifikátu.

4 Nastavení a správa certifikátů

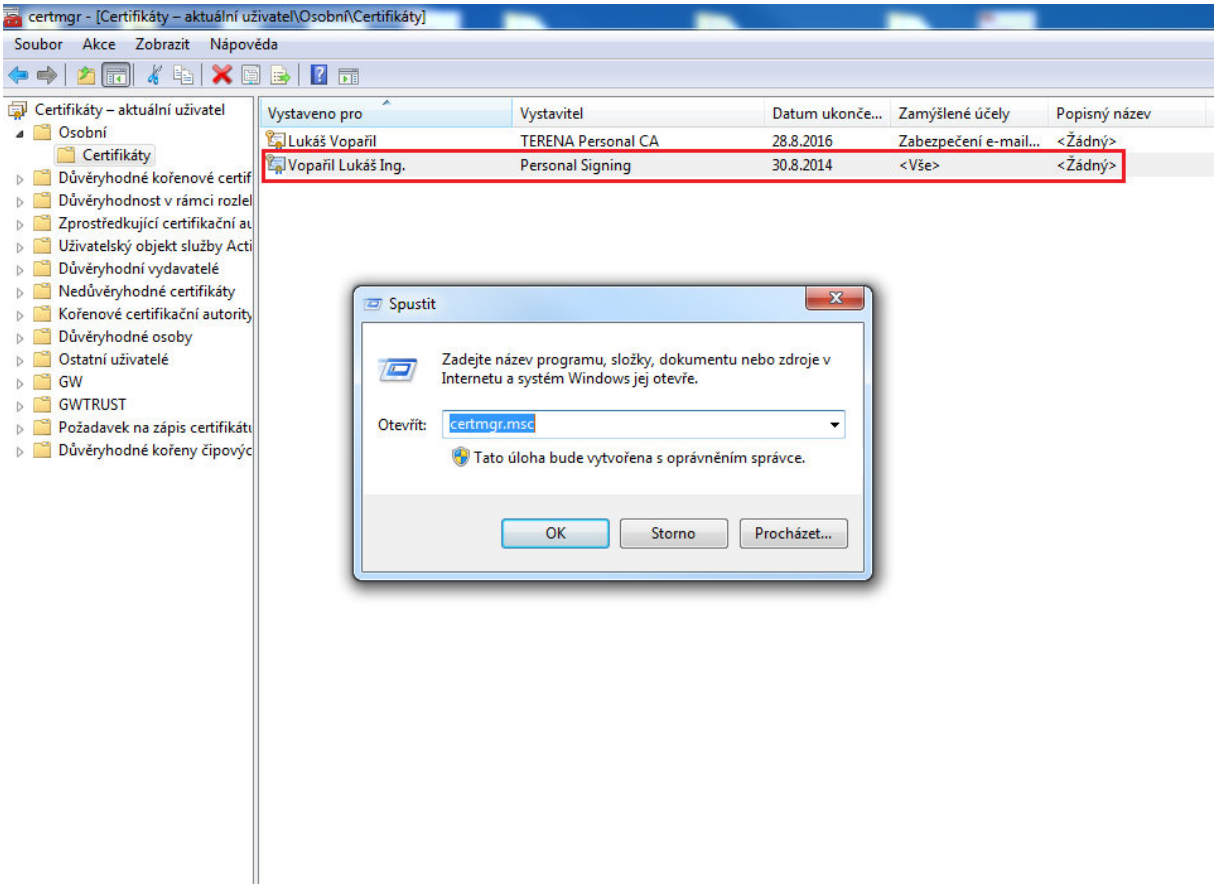
4.1 Úvod

Při vydání karty Vám byl na kontaktní čip nahrán ČVUT osobní certifikát, který vydala certifikační autorita CESNET. Tento certifikát slouží pouze pro účely elektronického podepisování v rámci ČVUT v Praze. Platnost ČVUT certifikátu je 1 rok od data jeho vydání.

Certifikační politiku a certifikační prováděcí směrnice naleznete na adrese:

http://pki.cesnet.cz/CP/Root/1.1/CESNET_Root_CA_CP_CPS-1.1.pdf

Pokud máte správně nainstalován minidriver (odstavec 1), certifikát se automaticky nahraje do úložiště certifikátů Windows při vložení karty do čtečky. To můžeme ověřit spuštěním správce certifikátu Windows **certmgr.msc** a v záložce osobní certifikáty.



Aplikacím, které využívají Microsoft uložiště certifikátů, se bude tento certifikát standardně nabízet.

4.2 Nastavení kořenových a zprostředkujících certifikátů

Kořenové certifikáty jsou vydávány samotnou Certifikační autoritou CESNET. Při instalaci do PC je nutné kořenový certifikát zařadit mezi Důvěryhodné kořenové certifikační úřady a následně umožňuje automatizované ověření klientských certifikátů vydávaných CESNET v systému.

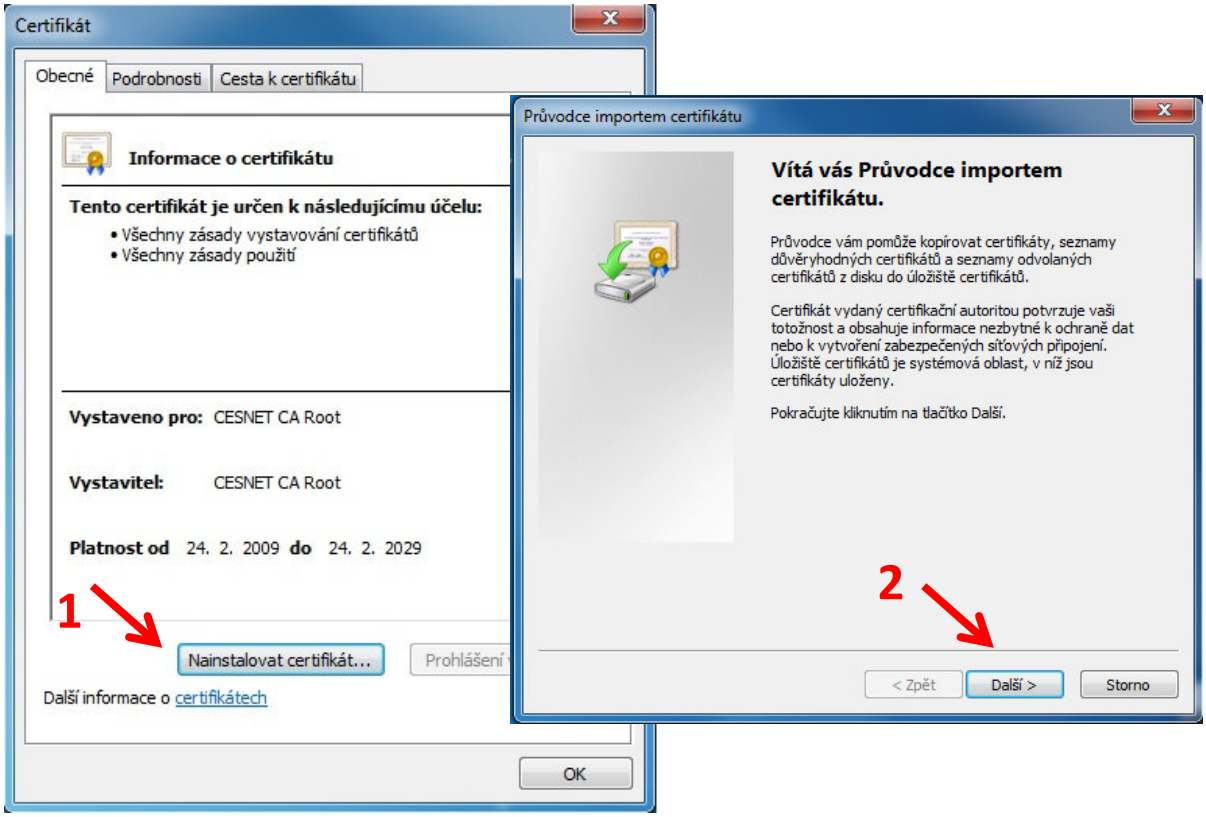
Pro správnou funkci elektronického podpisu ČVUT certifikátem je nutné mít nainstalované:

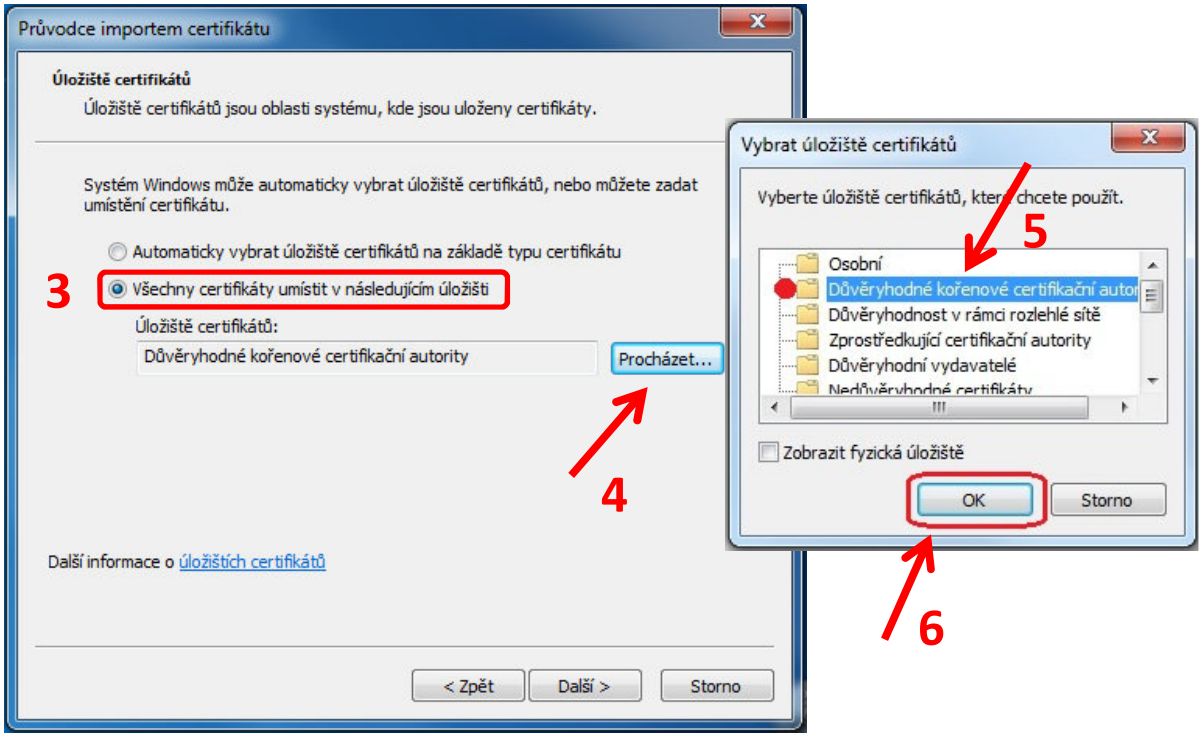
1) CESNET CA Root - http://crt.cesnet-ca.cz/CESNET_CA_Root.crt
2) CESNET Personal Signing CA - http://crt.cesnet-ca.cz/PersonalSigning.crt

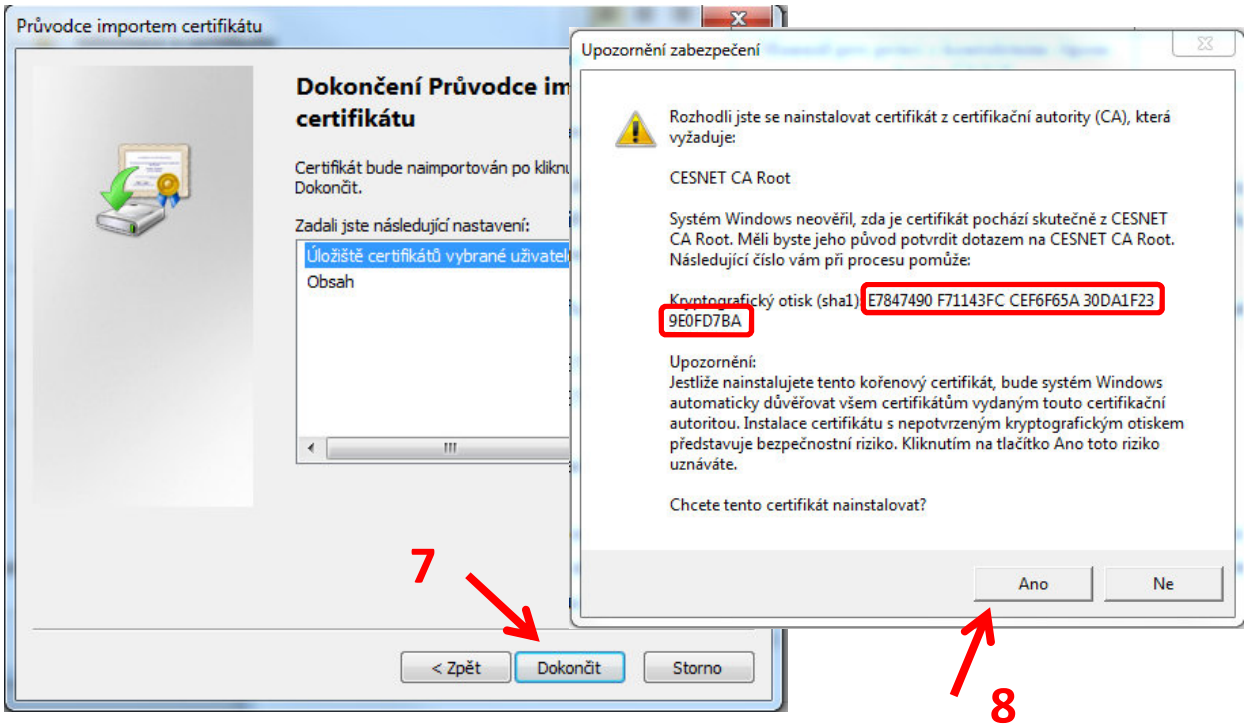
4.2.1 Instalace kořenového certifikátu CA CESNET Root.crt

- Otevřete odkaz pro CESNET CA Root a certifikát se Vám automaticky stáhne do PC. Soubor spusťte a stiskněte tlačítko „Nainstalovat certifikát“. Spustí se vám Průvodce importem certifikátu a dále pokračujte dle obrázků.
- Pokud instalujete certifikát ze souboru CESNET CA Root.crt, zobrazí se okno s dotazem, zda chcete certifikát skutečně nainstalovat. Operační systém požaduje ověření otisku certifikátu, který by měl být totožný s tímto:

  e7 84 74 90 f7 11 43 fc ce f6 f6 5a 30 da 1f 23 9e 0f d7 ba

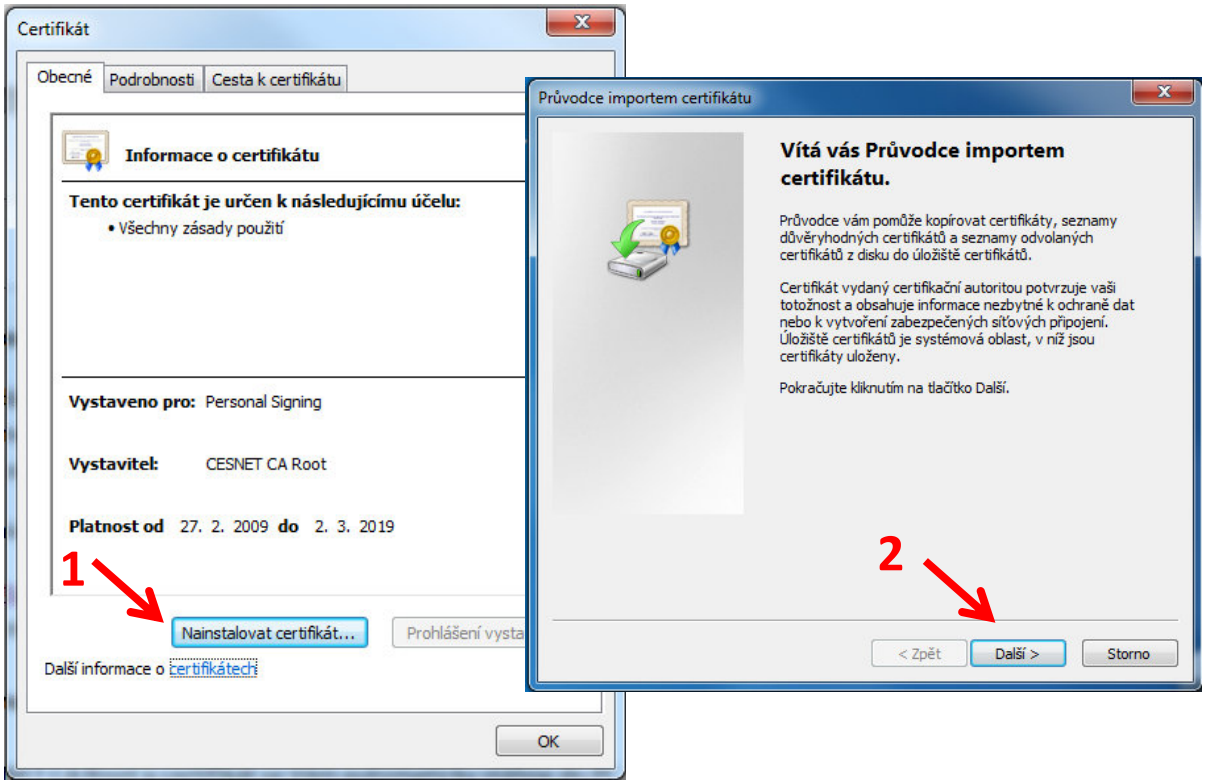


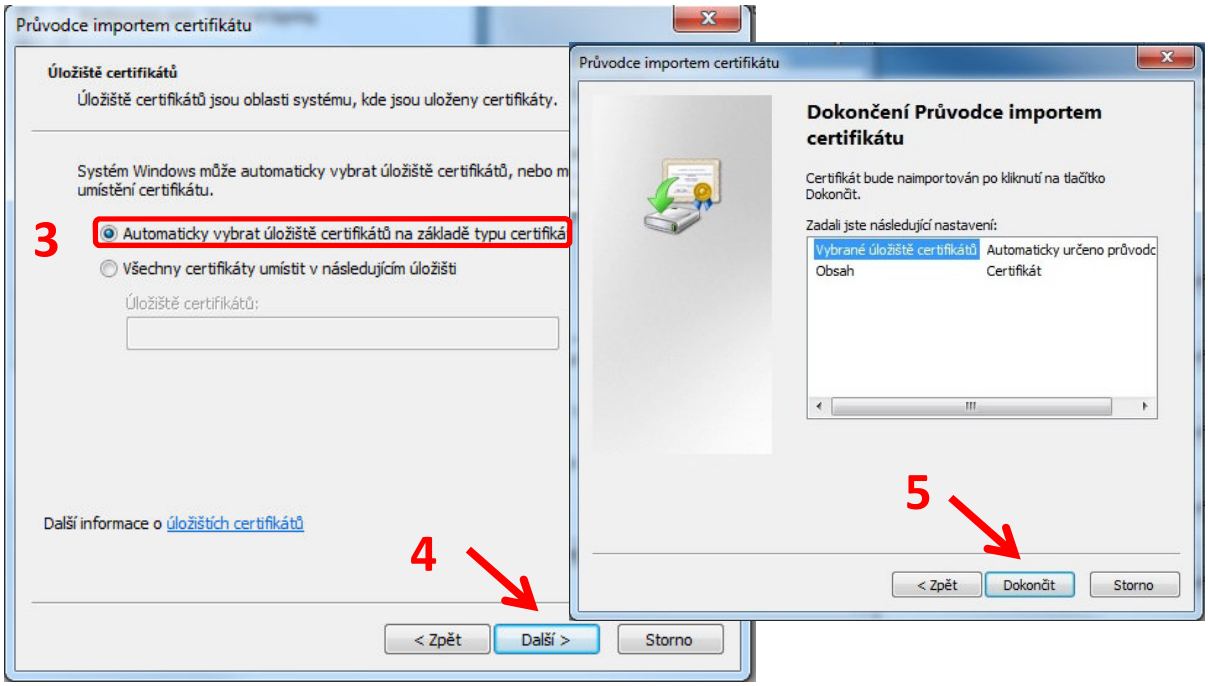

Průvodce importem certifikátu
Úložiště certifikátů
Úložiště certifikátů jsou oblasti systému, kde jsou uloženy certifikáty.
Systém Windows může automaticky vybrat úložiště certifikátů, nebo můžete zadat umístění certifikátu.
Automaticky vybrat úložiště certifikátů na základě typu certifikátu
3
Všechny certifikáty umístit v následujícím úložišti
Úložiště certifikátů:
Důvěryhodné kořenové certifikační autority
Procházet...
4
Další informace o úložištích certifikátů
< Zpět
Další >
Storno
Vybrat úložiště certifikátů
Vyberte úložiště certifikátů, které chcete použít.
5
Osobní
Důvěryhodné kořenové certifikační autor
Důvěryhodnost v rámci rozlehlé sítě
Zprostředkující certifikační autority
Důvěryhodní vydavatelé
Zobrazit fyzická úložiště
OK
Storno
6


Průvodce importem certifikátu
Dokončení Průvodce im
certifikátu
Certifikát bude naimportován po klikn
Dokončit.
Zadali jste následující nastavení:
Úložiště certifikátů vybrané uživatel
Obsah
7
< Zpět
Dokončit
Storno
Upozornění zabezpečení
Rozhodli jste se nainstalovat certifikát z certifikační autority (CA), která vyžaduje:
CESNET CA Root
Systém Windows neověřil, zda je certifikát pochází skutečně z CESNET CA Root. Měli byste jeho původ potvrdit dotazem na CESNET CA Root. Následující číslo vám při procesu pomůže:
Kryptografický otisk (sha1): E7847490 F71143FC CEF6F65A 30DA1F23 9E0FD7BA
Upozornění:
Jestliže nainstalujete tento kořenový certifikát, bude systém Windows automaticky důvěřovat všem certifikátům vydaným touto certifikační autoritou. Instalace certifikátu s nepotvrzeným kryptografickým otiskem představuje bezpečnostní riziko. Kliknutím na tlačítko Ano toto riziko uznáváte.
Chcete tento certifikát nainstalovat?
Ano
Ne
8

4.2.2 Instalace zprostředkujícího certifikátu CESNET Personal Signing CA.crt

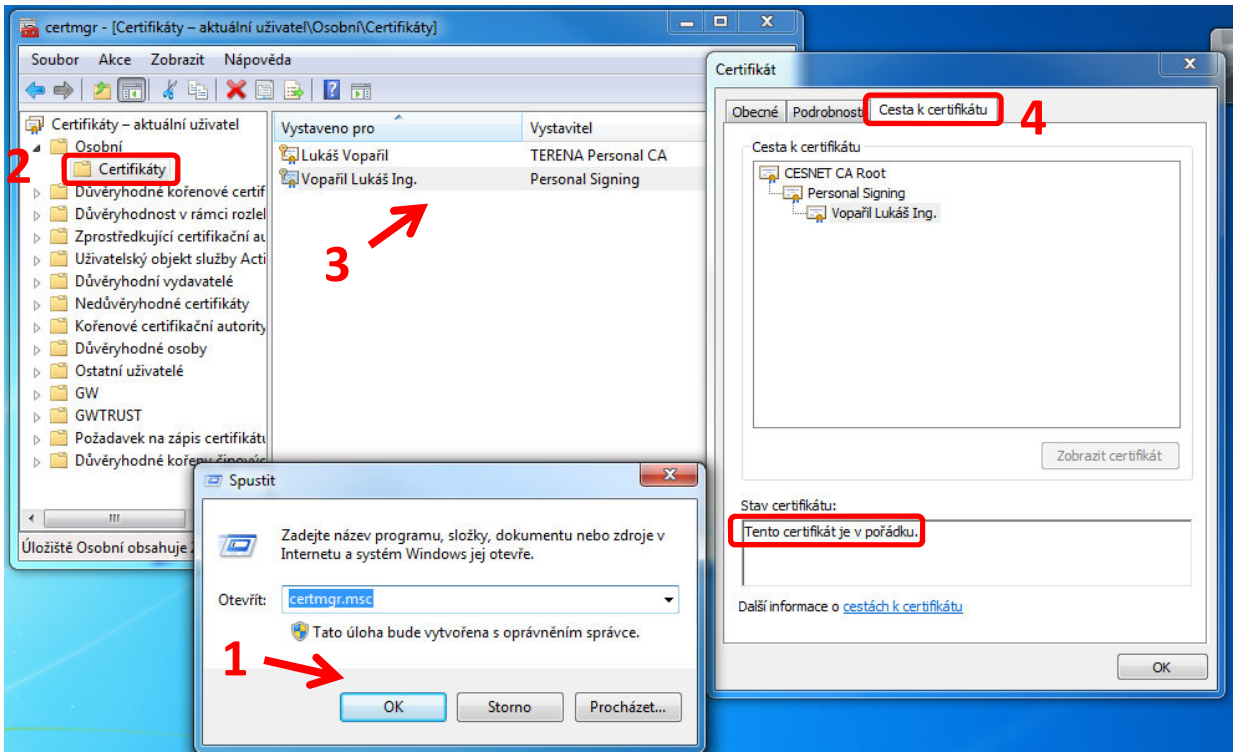
- Otevřete odkaz pro CESNET Personal Signing CA a certifikát se Vám automaticky stáhne do PC. Soubor spusťte a stiskněte tlačítko „Nainstalovat certifikát“. Spustí se vám Průvodce importem certifikátu a dále pokračujte dle obrázků.
- U zprostředkujícího certifikátu není nutné nastavovat manuálně umístění, necháme systém vybrat uložiště automaticky.





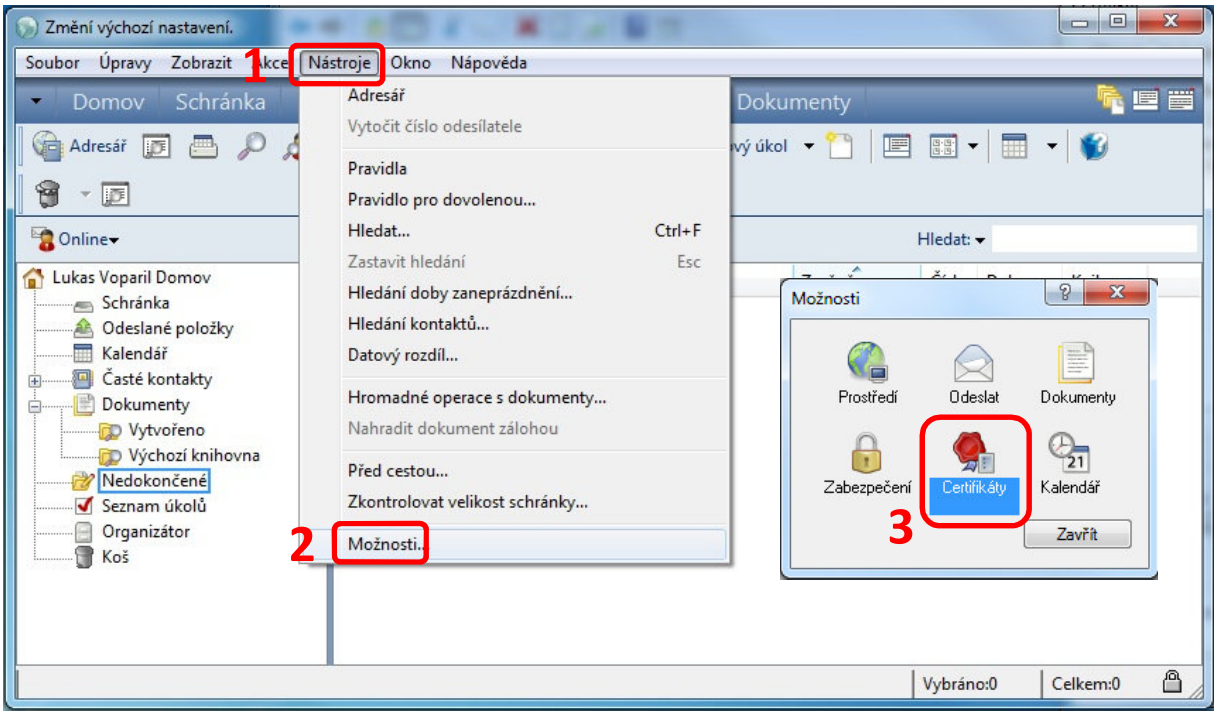
Správné nastavení kořenových certifikátů můžeme ověřit opět ve správci certifikátů:

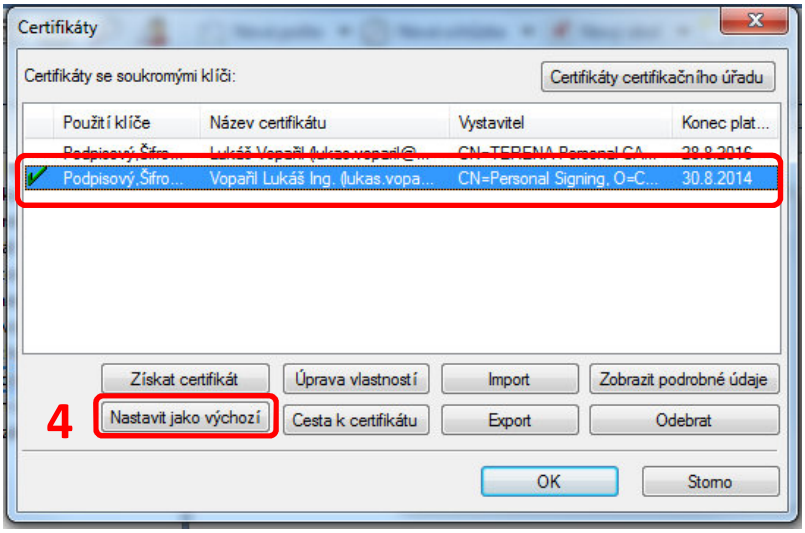
- Poklepáním na náš osobní certifikát otevřeme informace o certifikátu.
- V záložce „Cesta k certifikátu“ ověříme, zda je cesta k certifikátu v pořádku.



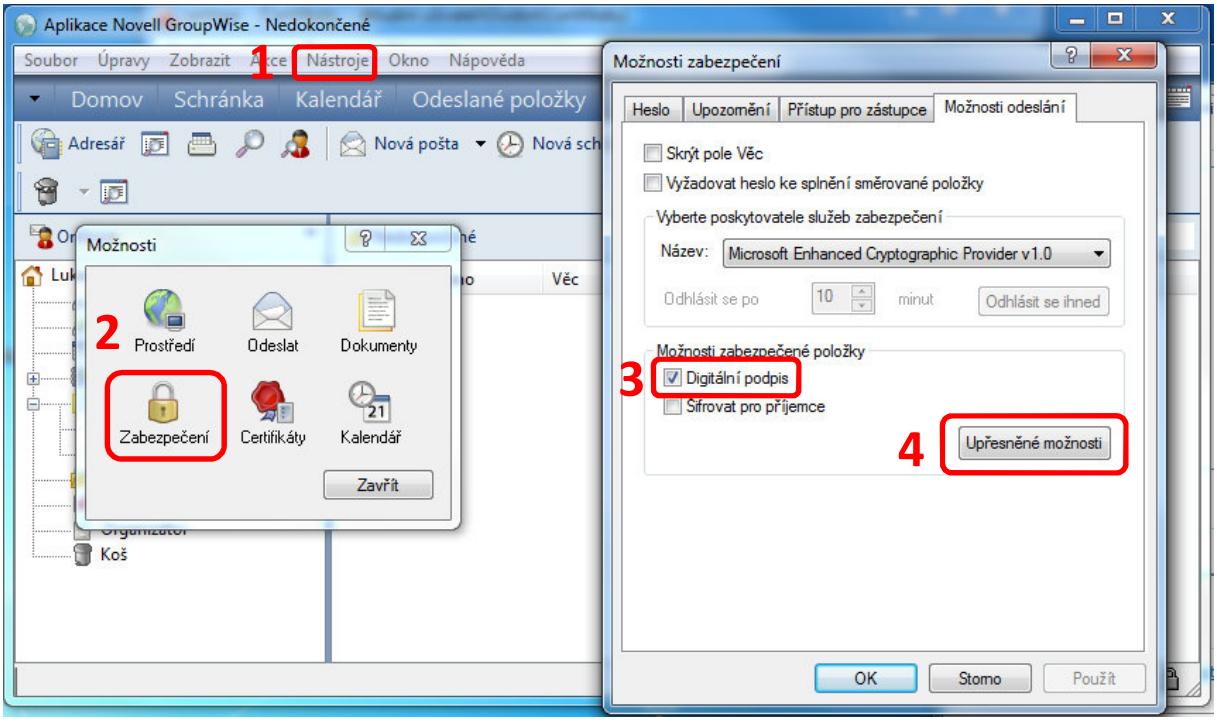
5 Nastavení Groupwise

5.1 Základní nastavení

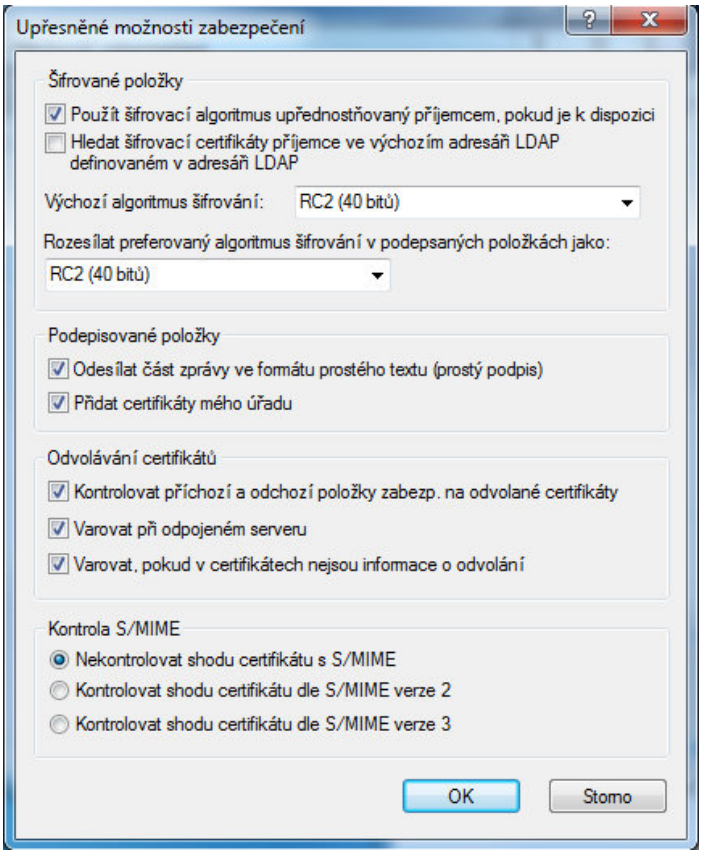




5.2 Rozšířené nastavení

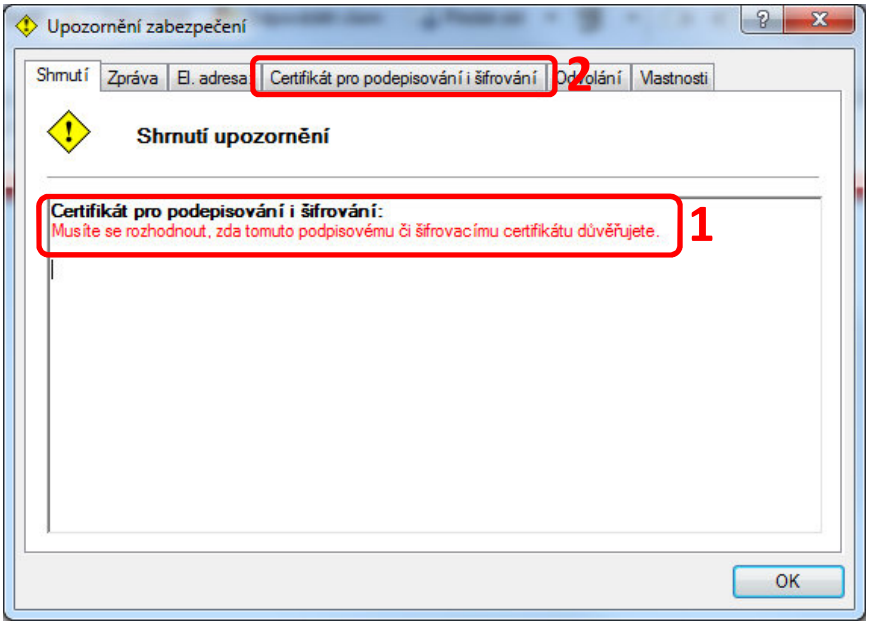


Nastavit dle obrázku.

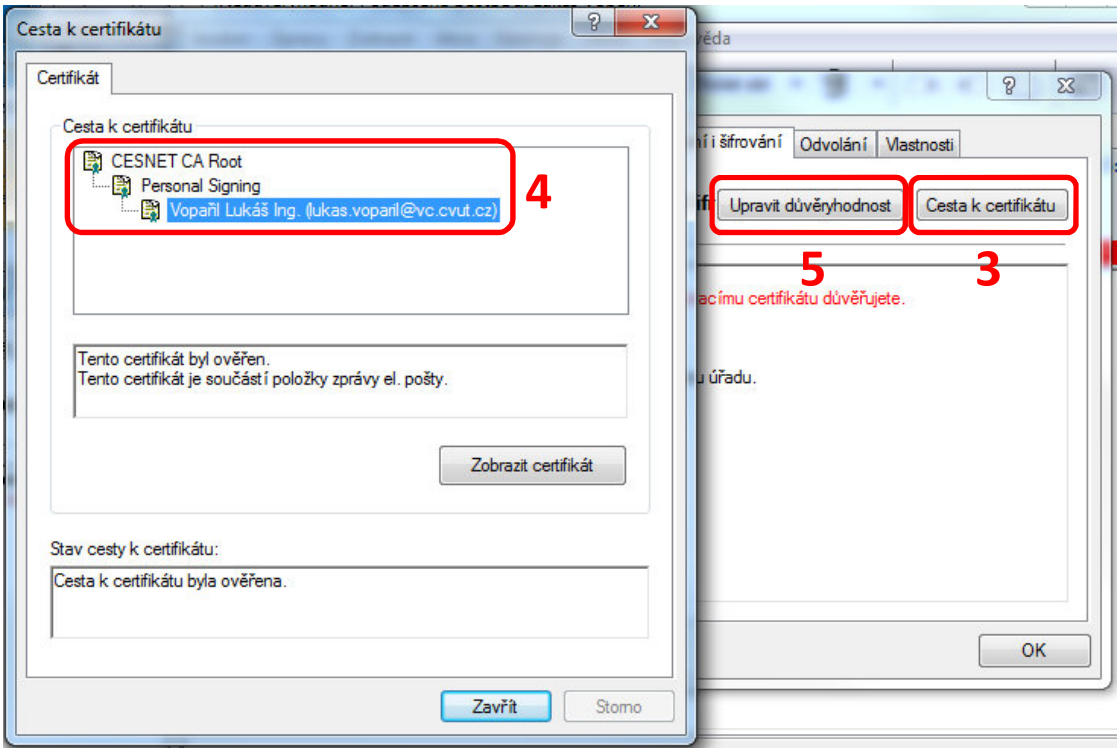


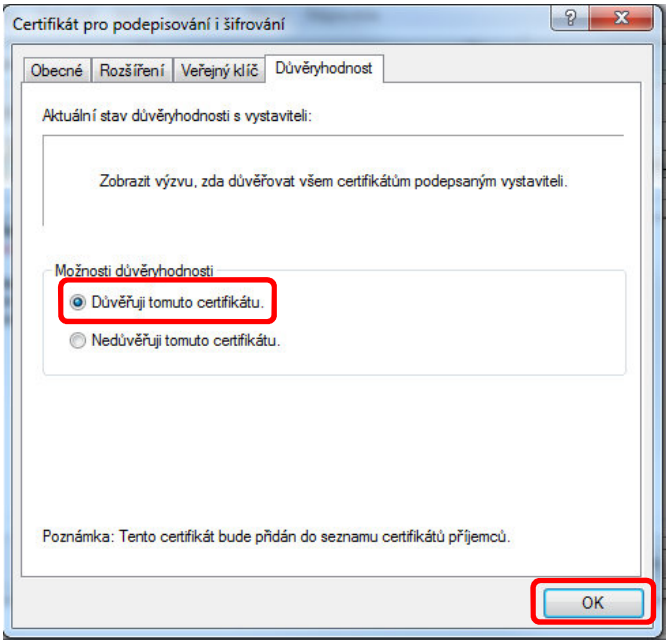
5.3 Nastavení důvěryhodnosti

Pro správné ověřování elektronického podpisu příchozích emailů je nutné nastavit důvěryhodnost pro ČVUT certifikát. V případě, že se Vám objeví toto upozornění, tak se přepněte do záložky „Certifikát pro podepisování i šifrování“



Zvolte „Cesta k certifikátu“ a zkontrolujte, zda cesta vede k CESNET CA Root. Pokud ano, klikněte na tlačítko „Upravit důvěryhodnost“ a zda zaškrtněte „Důvěřuji tomuto certifikátu“

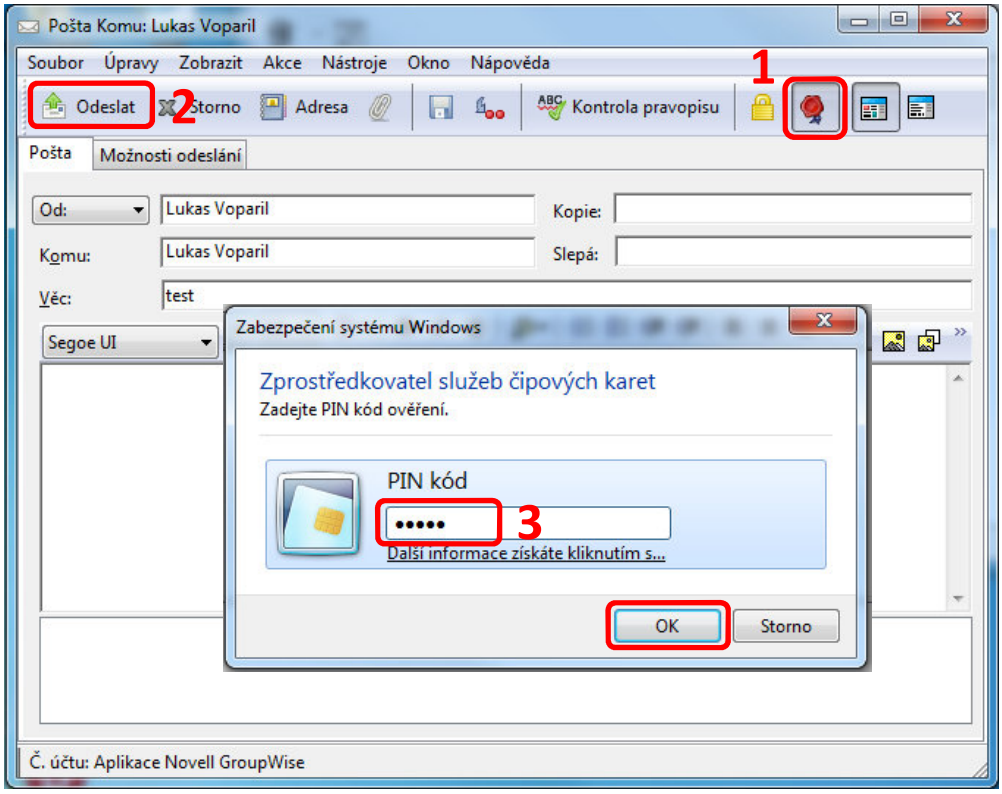




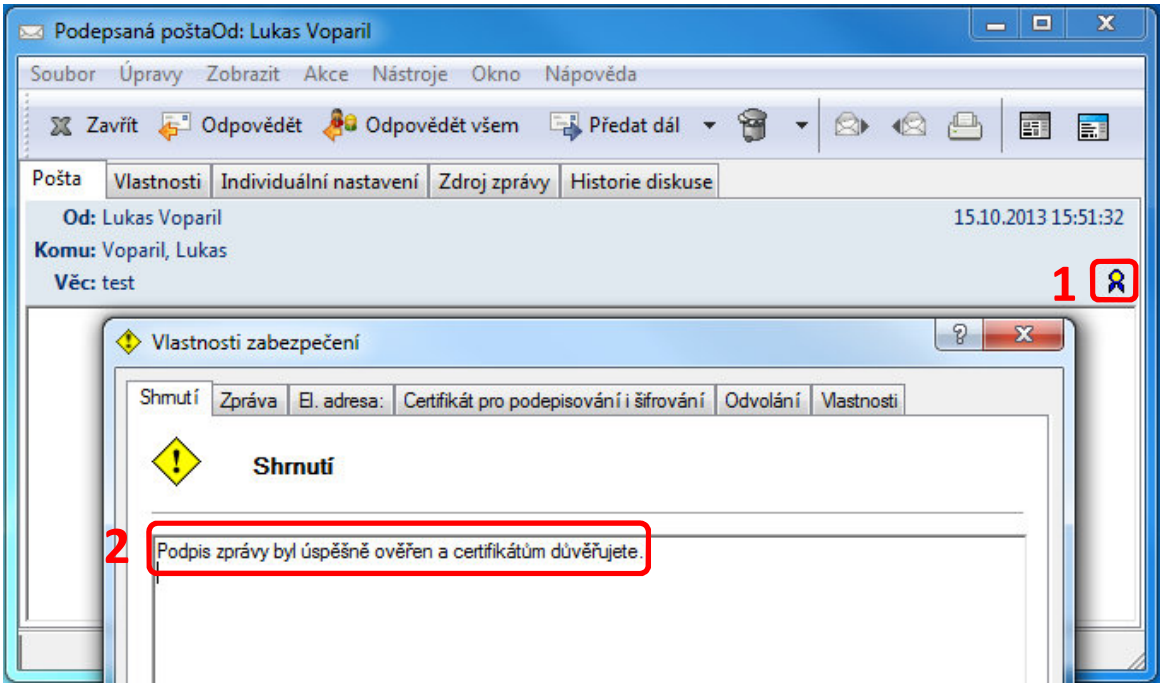
Tento postup se doporučuje, pouze pokud cesta k certifikátu vede k DŮVĚRYHODNÉ certifikační autoritě.

5.4 Podepisování emailů

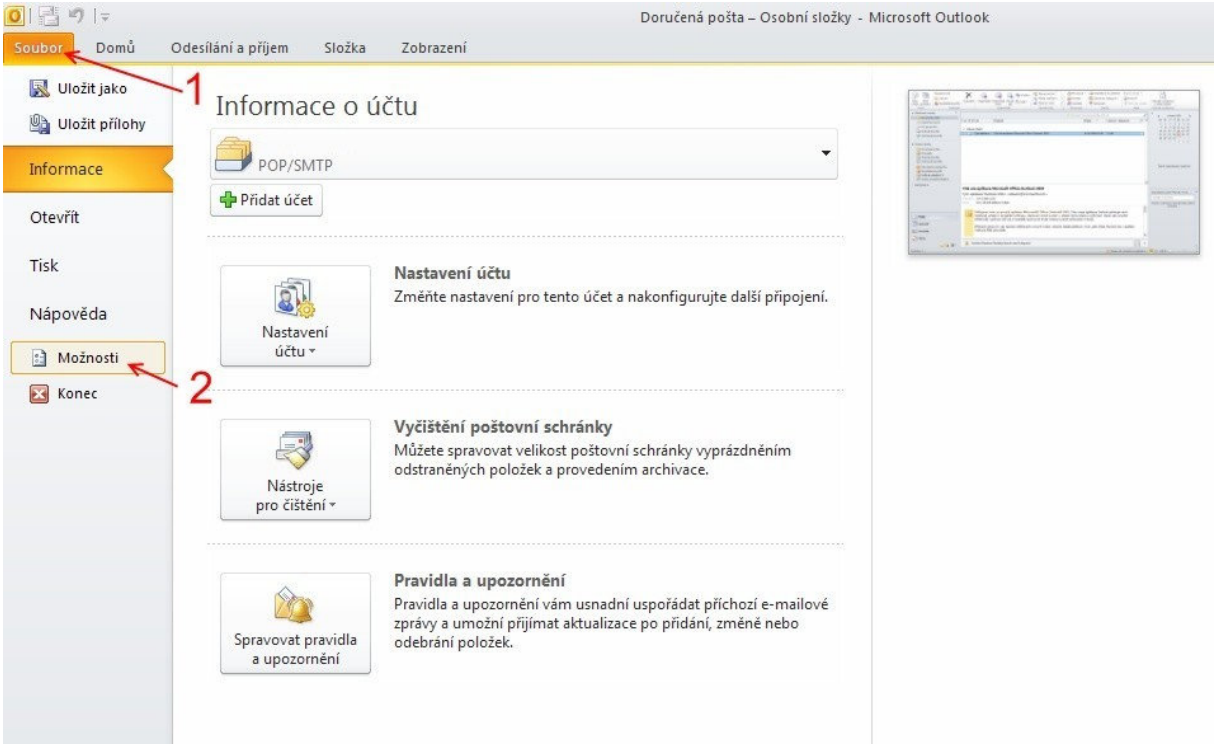
Elektronické podepsání provedení stisknutím tlačítka označeného na obrázku. Po stisknutí tlačítka odeslat je nutné mít vloženou čipovou kartu ve čtečce a zadat svůj PIN.

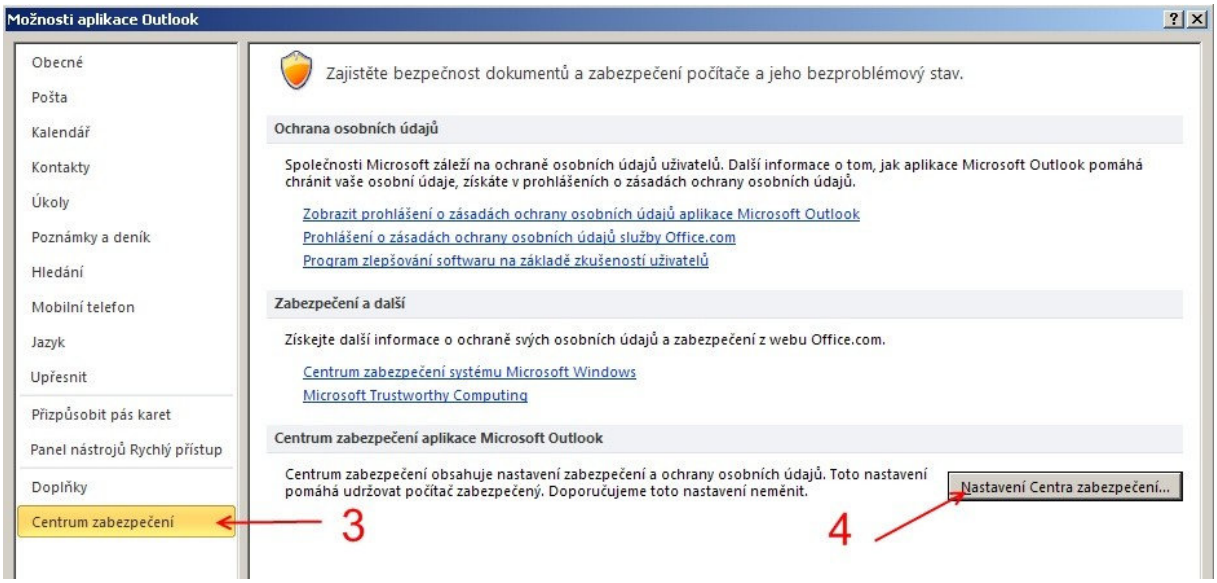


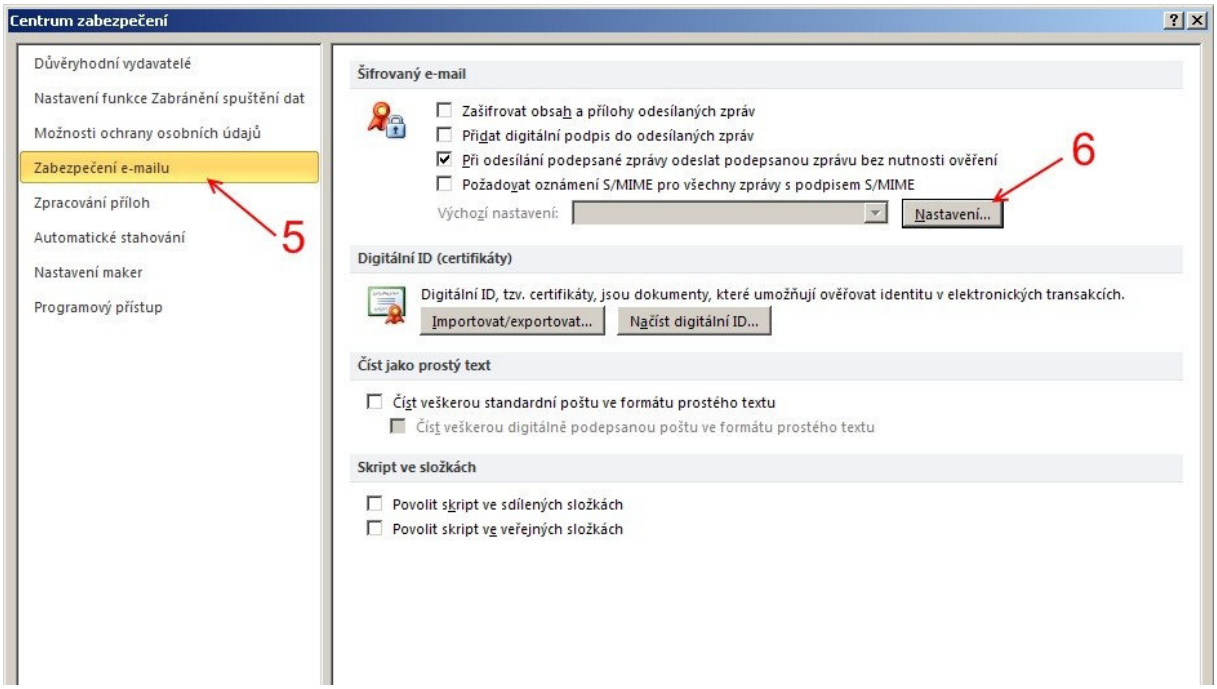
Kontrola příchozích elektronicky podepsaných emailů a úprava důvěryhodnosti

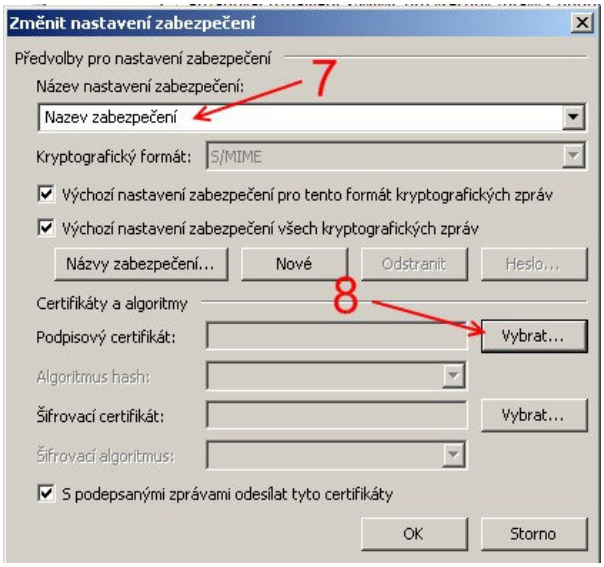

Podepsaná poštaOd: Lukas Voparil
Soubor Úpravy Zobrazit Akce Nástroje Okno Nápověda
Zavřít Odpovědět Odpovědět všem Předat dál
Pošta Vlastnosti Individuální nastavení Zdroj zprávy Historie diskuse
Od: Lukas Voparil
15.10.2013 15:51:32
Komu: Voparil, Lukas
Věc: test
1
Vlastnosti zabezpečení
Shrnutí Zpráva El. adresa: Certifikát pro podepisování i šifrování Odvolání Vlastnosti
Shrnutí
2
Podpis zprávy byl úspěšně ověřen a certifikátům důvěřujete.

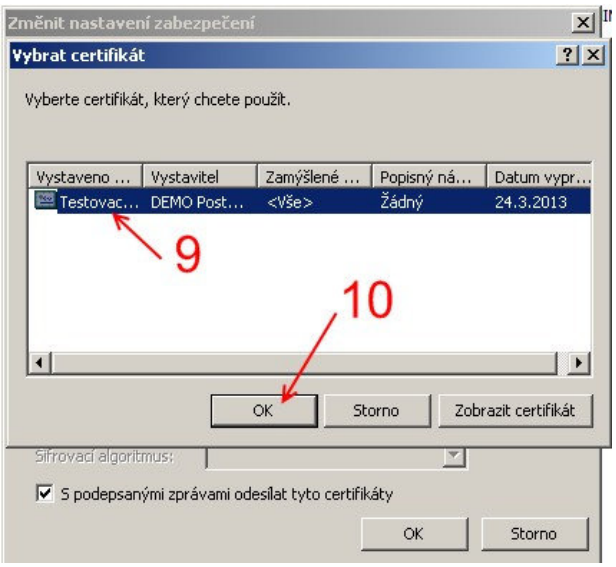
6 Nastavení Outlook 2010



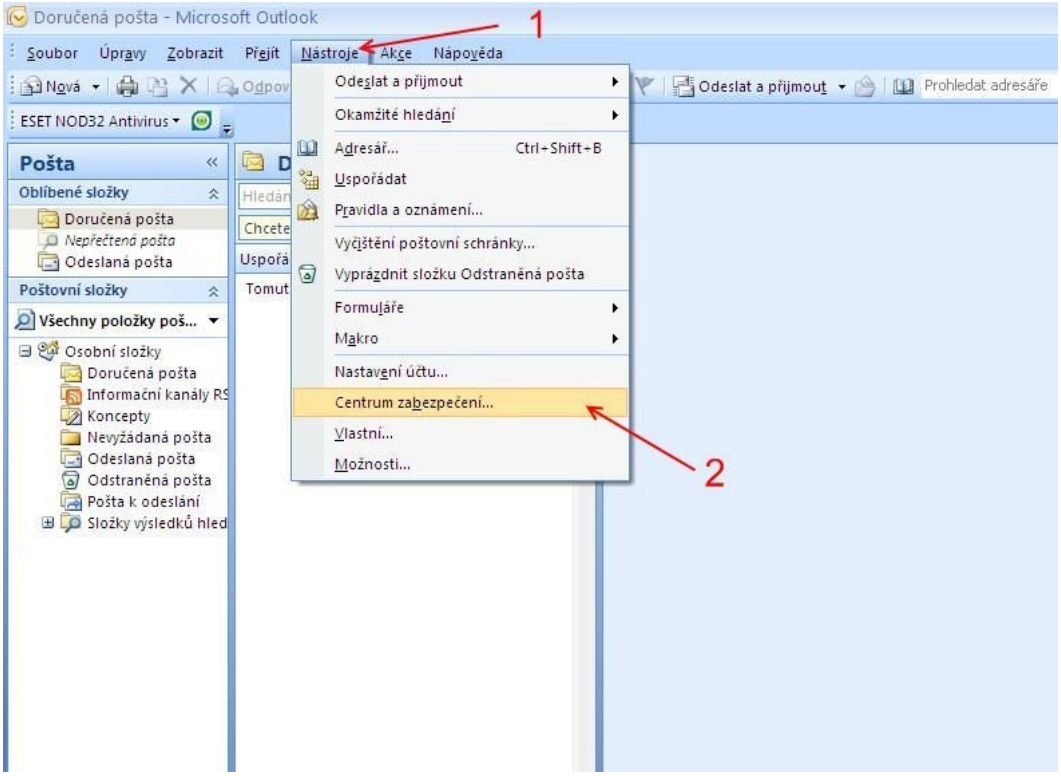


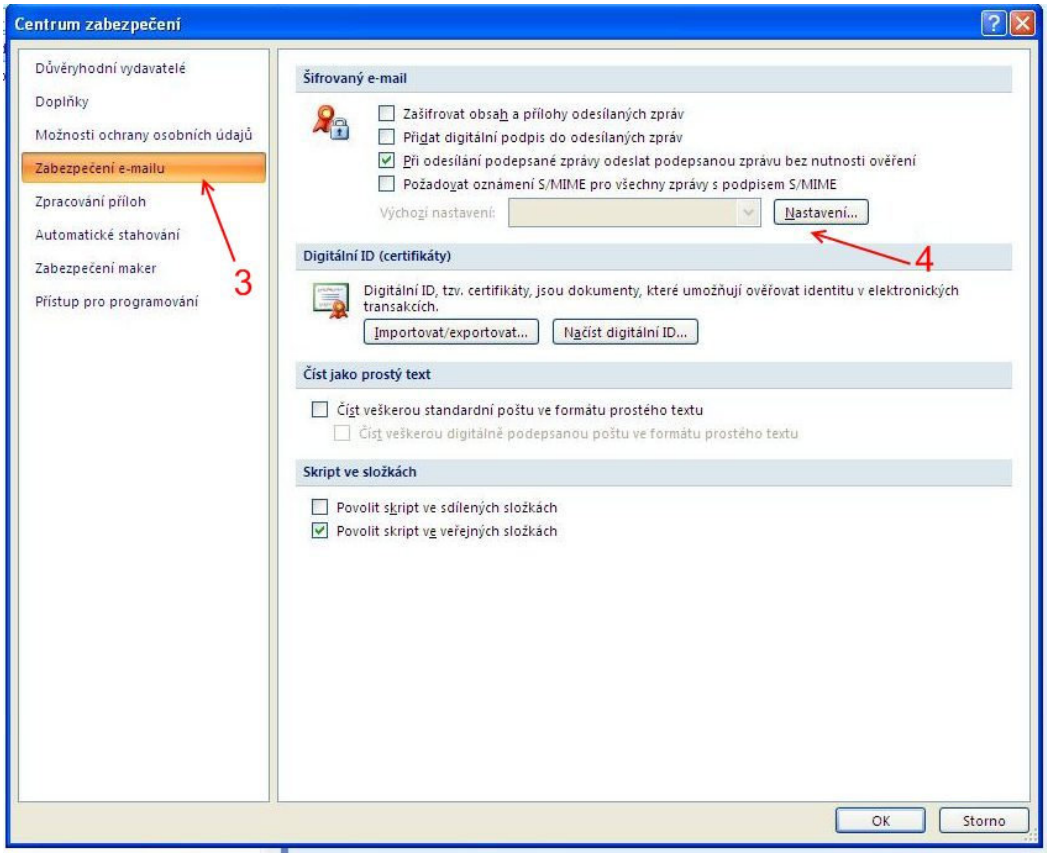

Centrum zabezpečení
Důvěryhodní vydavatelé
Nastavení funkce Zabránění spuštění dat
Možnosti ochrany osobních údajů
Zabezpečení e-mailu
Zpracování příloh
Automatické stahování
Nastavení maker
Programový přístup
5
Šifrovaný e-mail
Zašifrovat obsah a přílohy odesílaných zpráv
Přidat digitální podpis do odesílaných zpráv
Při odesílání podepsané zprávy odeslat podepsanou zprávu bez nutnosti ověření
Požadovat oznámení S/MIME pro všechny zprávy s podpisem S/MIME
Výchozí nastavení:
Nastavení...
6
Digitální ID (certifikáty)
Digitální ID, tzv. certifikáty, jsou dokumenty, které umožňují ověřovat identitu v elektronických transakcích.
Importovat/exportovat...
Načíst digitální ID...
Číst jako prostý text
Číst veškerou standardní poštu ve formátu prostého textu
Číst veškerou digitálně podepsanou poštu ve formátu prostého textu
Skript ve složkách
Povolit skript ve sdílených složkách
Povolit skript ve veřejných složkách

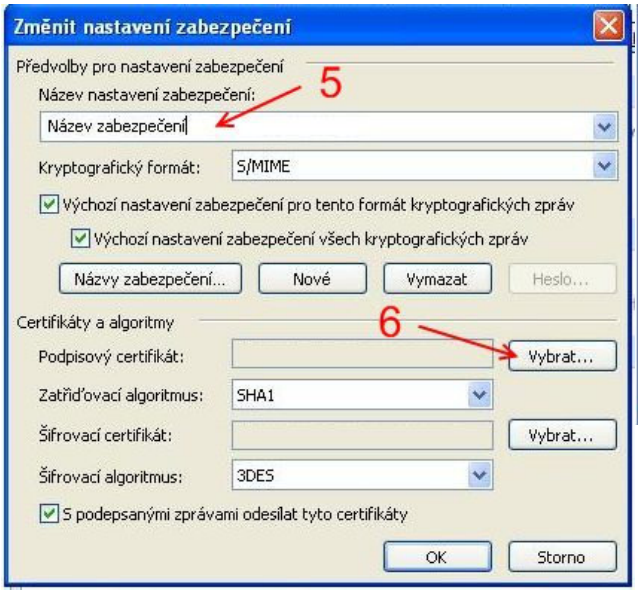

Změnit nastavení zabezpečení
Předvolby pro nastavení zabezpečení
Název nastavení zabezpečení:
7
Nazev zabezpečení
Kryptografický formát:
S/MIME
Výchozí nastavení zabezpečení pro tento formát kryptografických zpráv
Výchozí nastavení zabezpečení všech kryptografických zpráv
Názvy zabezpečení...
Nové
Odstranit
Heslo...
Certifikáty a algoritmy
8
Podpisový certifikát:
Vybrat...
Algoritmus hash:
Šifrovací certifikát:
Vybrat...
Šifrovací algoritmus:
S podepsanými zprávami odesílat tyto certifikáty
OK
Storno

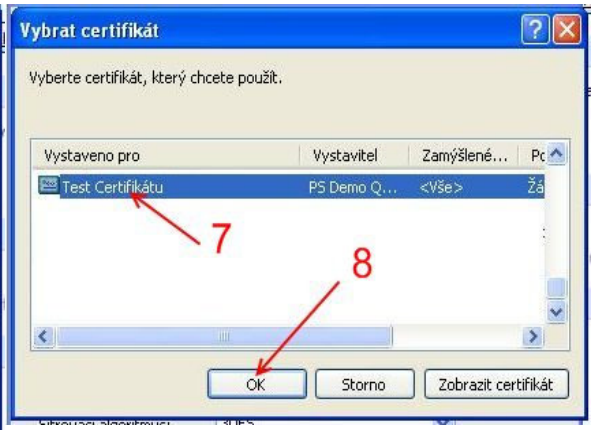

Změnit nastavení zabezpečení
Vybrat certifikát
Vyberte certifikát, který chcete použít.
Vystaveno ...
Vystavitel
Zamýšlené ...
Popisný ná...
Datum vypr...
Testovac...
DEMO Post...
<Vše>
Žádný
24.3.2013
9
10
OK
Storno
Zobrazit certifikát
Šifrovací algoritmus:
S podepsanými zprávami odesílat tyto certifikáty
OK
Storno

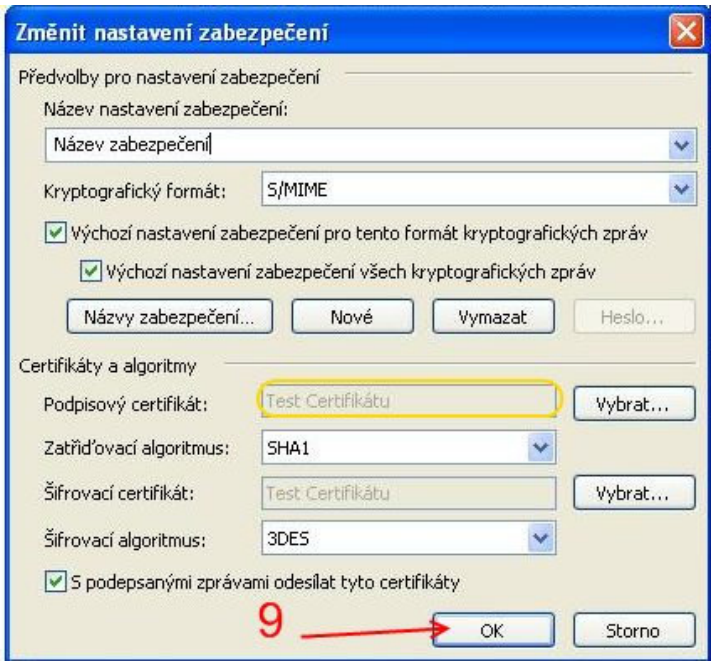
7 Nastavení Outlook 2007





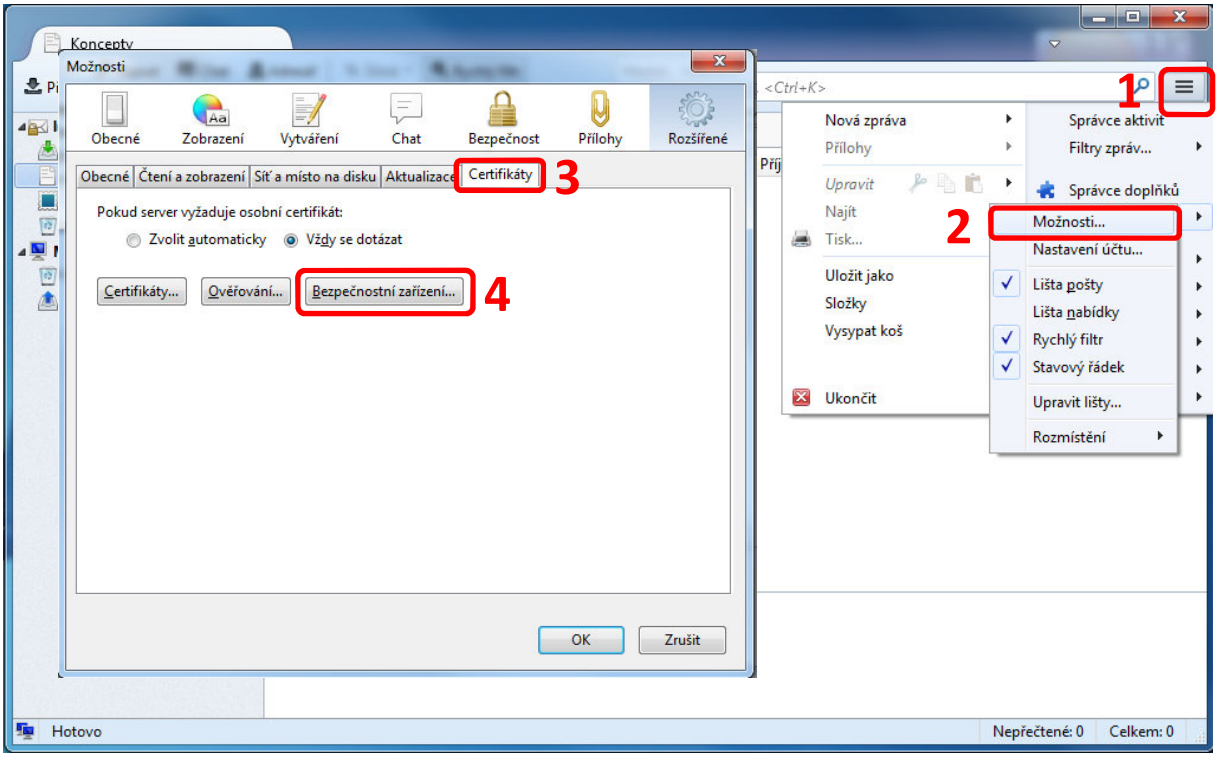

Změnit nastavení zabezpečení
Předvolby pro nastavení zabezpečení
Název nastavení zabezpečení:
5
Název zabezpečení
Kryptografický formát:
S/MIME
Výchozí nastavení zabezpečení pro tento formát kryptografických zpráv
Výchozí nastavení zabezpečení všech kryptografických zpráv
Názvy zabezpečení...
Nové
Vymazat
Heslo...
Certifikáty a algoritmy
6
Podpisový certifikát:
Vybrat...
Zatřiďovací algoritmus:
SHA1
Šifrovací certifikát:
Vybrat...
Šifrovací algoritmus:
3DES
S podepsanými zprávami odesílat tyto certifikáty
OK
Storno

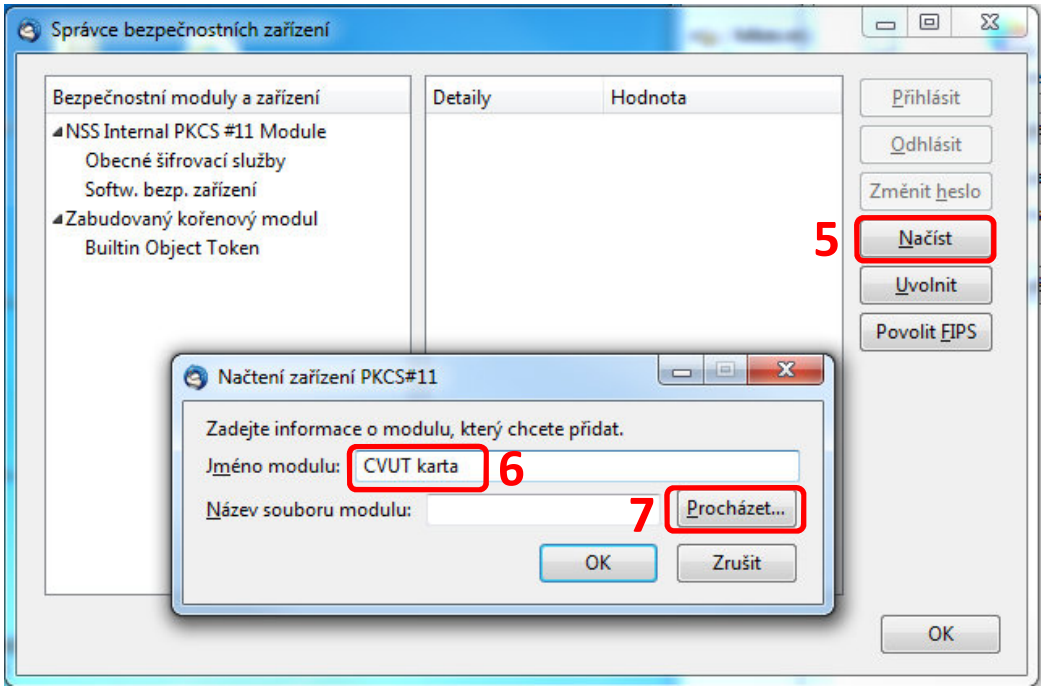

Vybrat certifikát
Vyberte certifikát, který chcete použít.
Vystaveno pro
Vystavitel
Zamýšlené...
Test Certifikátu
PS Demo Q...
<Vše>
7
8
OK
Storno
Zobrazit certifikát


Změnit nastavení zabezpečení
Předvolby pro nastavení zabezpečení
Název nastavení zabezpečení:
Název zabezpečení
Kryptografický formát:
S/MIME
Výchozí nastavení zabezpečení pro tento formát kryptografických zpráv
Výchozí nastavení zabezpečení všech kryptografických zpráv
Názvy zabezpečení...
Nové
Vymazat
Heslo...
Certifikáty a algoritmy
Podpisový certifikát:
Test Certifikátu
Vybrat...
Zatřiďovací algoritmus:
SHA1
Šifrovací certifikát:
Test Certifikátu
Vybrat...
Šifrovací algoritmus:
3DES
S podepsanými zprávami odesílat tyto certifikáty
9
OK
Storno

8 Nastavení Thunderbird

8.1 Instalace bezpečnostního zařízení

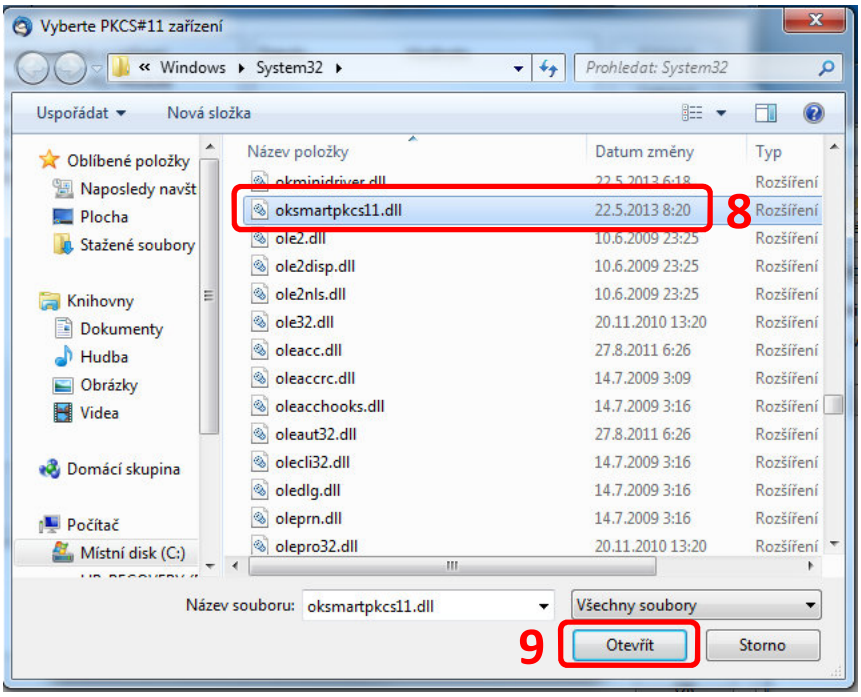


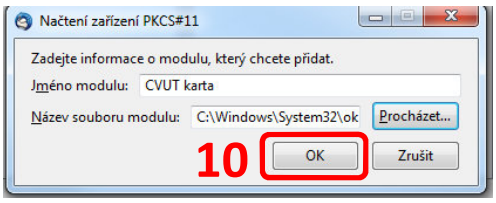


Pro podporu certifikátů z čipové karty je nutné mít nainstalovanou PKCS#11 knihovnu. Tuto knihovnu můžete stáhnout(Odstavec 1) na:

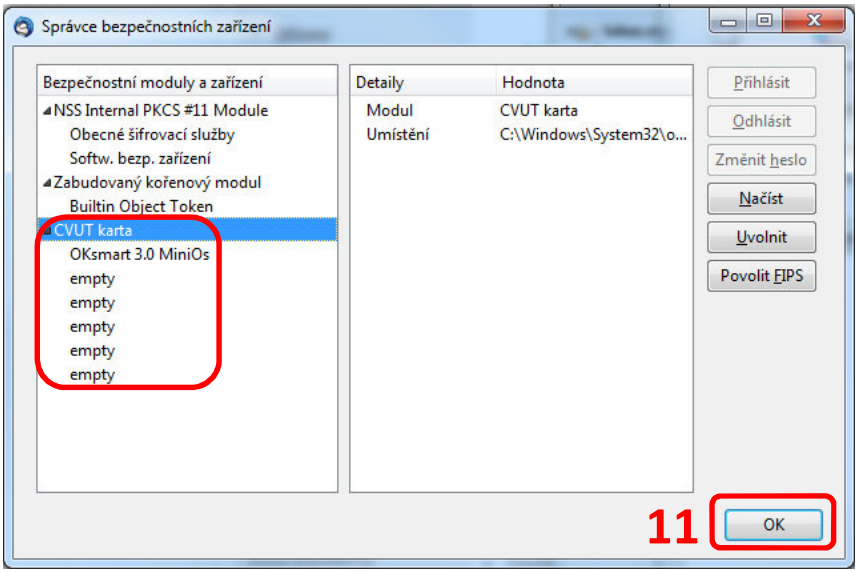
- Windows XP, Vista, 7, 32bit - http://www.oksystem.cz/df/2007
- Windows XP, Vista, 7, 64bit - http://www.oksystem.cz/df/2009

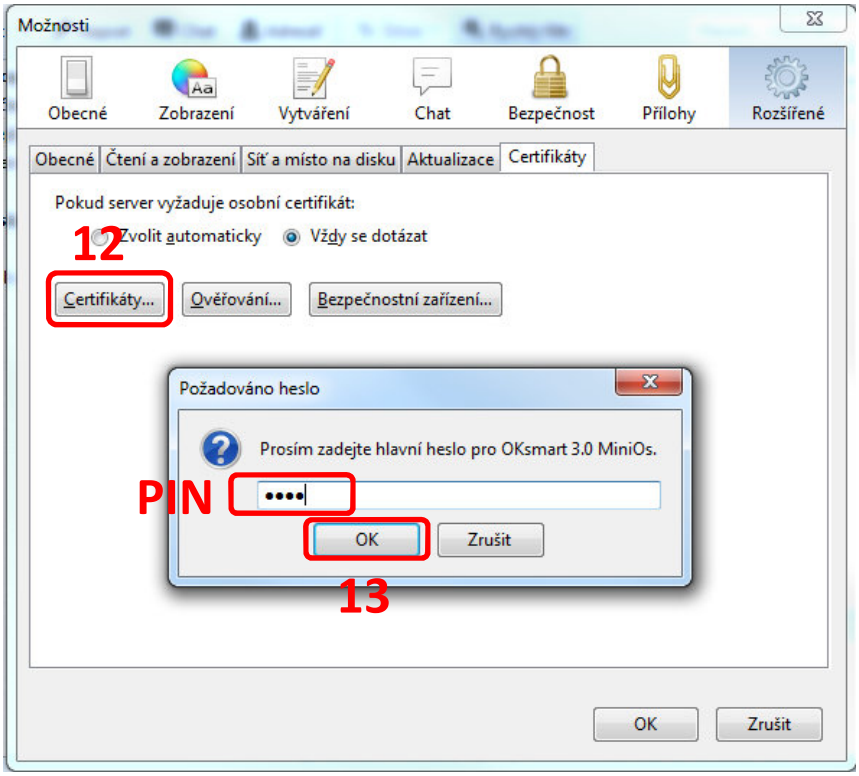
Knihovna se nainstaluje do **X:/Windows/System32/oksmartpkcs11.dll** a zde jí vybereme.



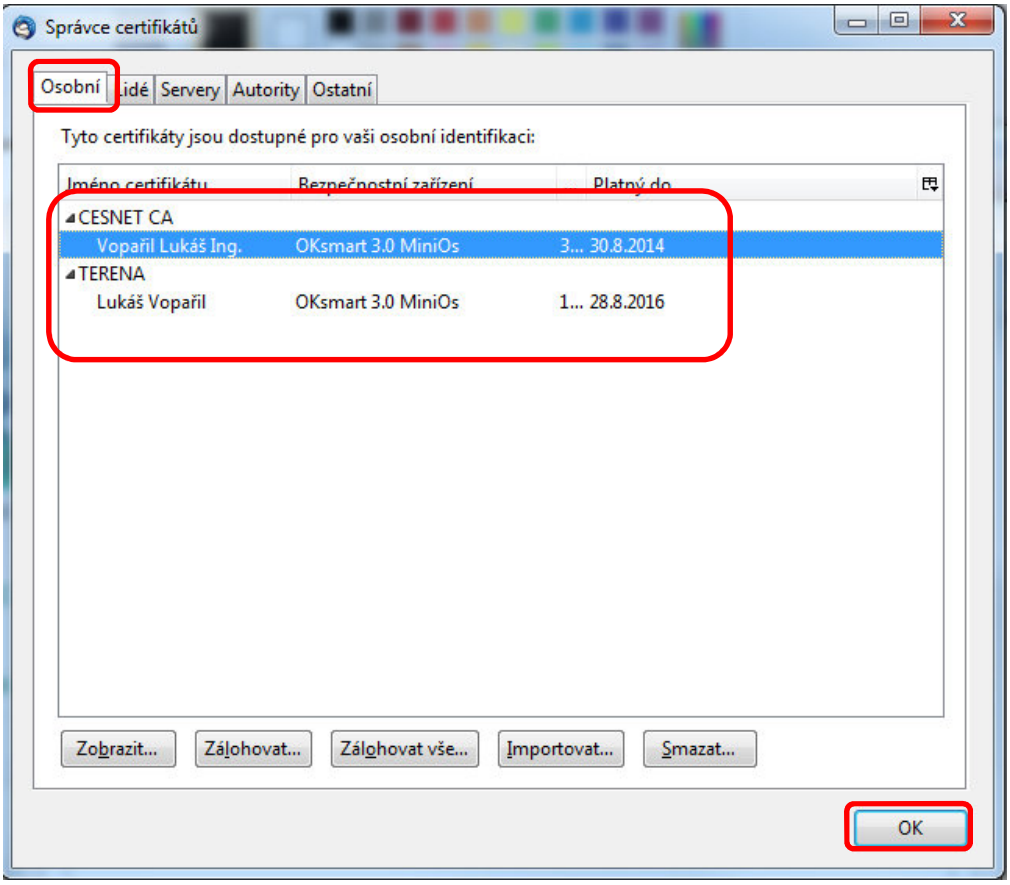


Vložte čipovou kartu do čtečky

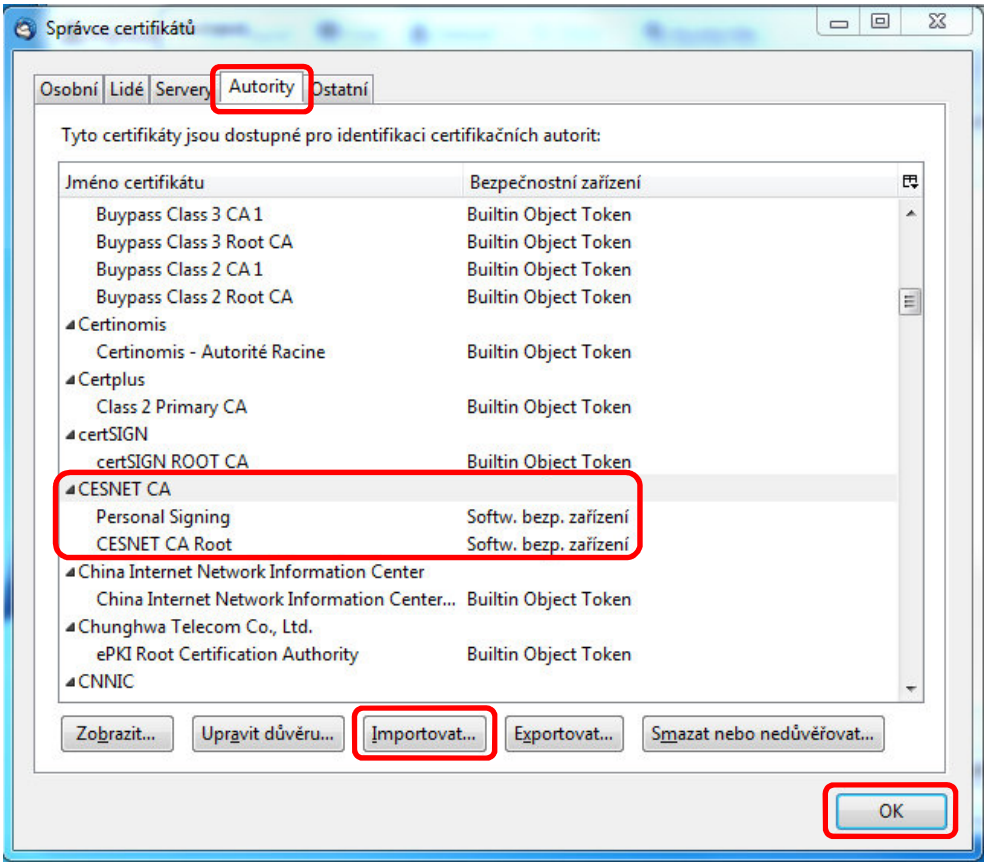




Kontrola osobních certifikátů – pro zobrazení osobních certifikátů musí být vložena karta ve čtečce.

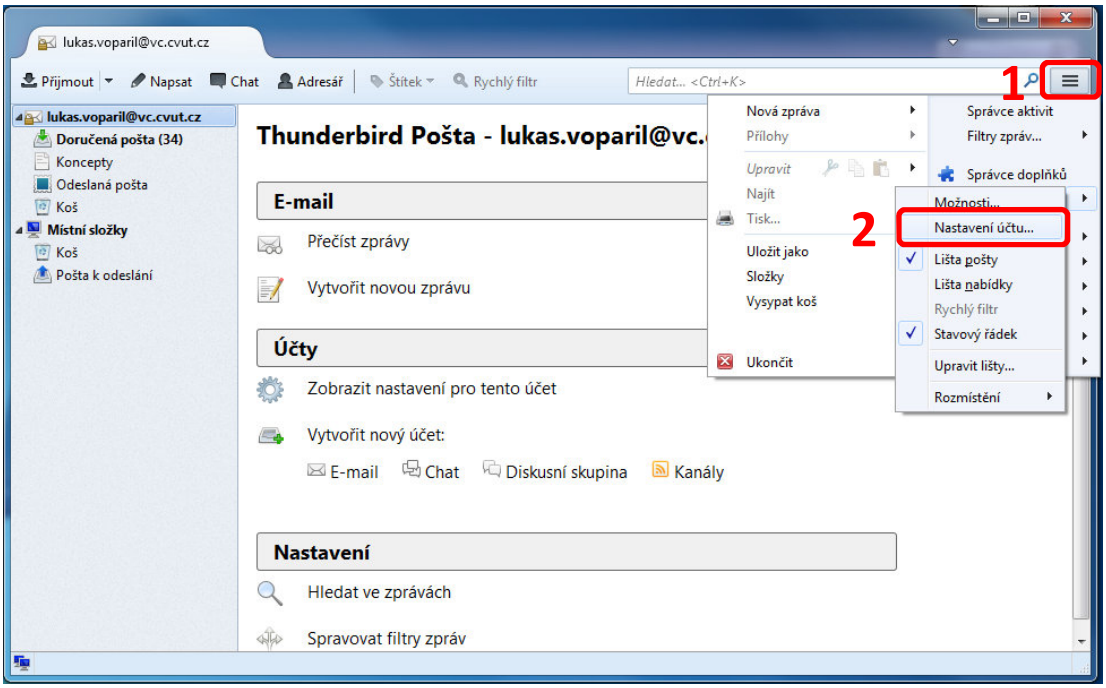


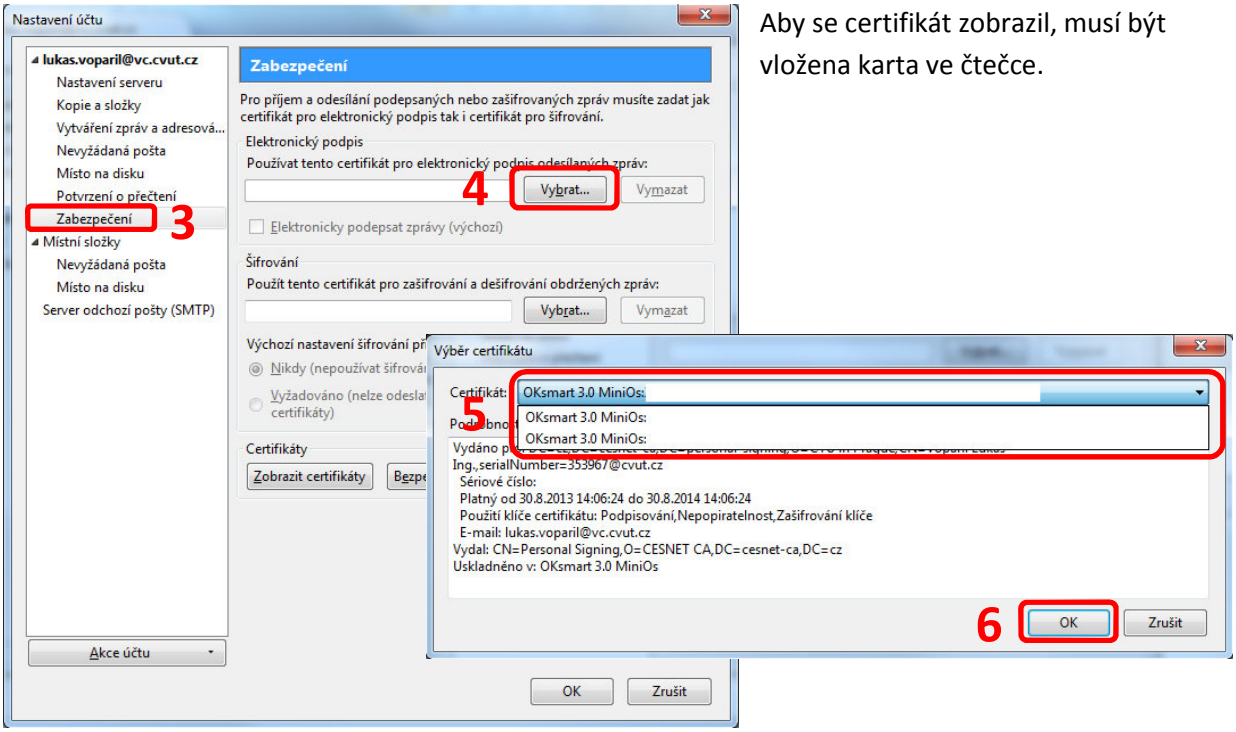
Kontrola certifikátů certifikační autorit, pokud chybí, je vhodné naimportovat.



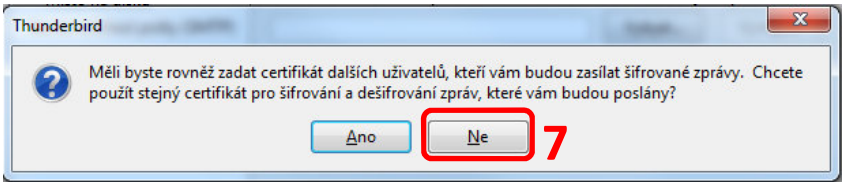
8.2 Nastavení elektronického podpisu

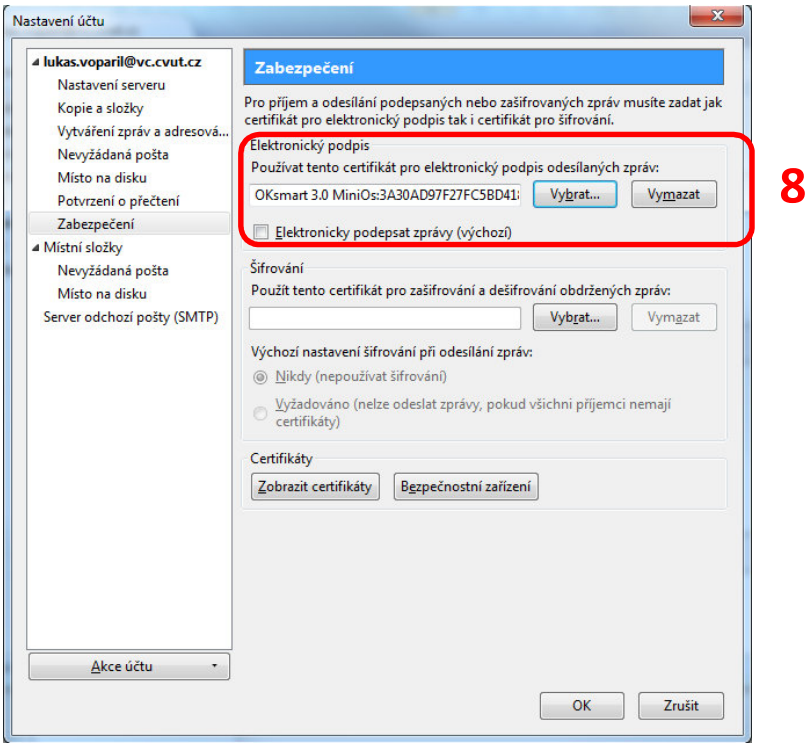
Samotné nastavení elektronického podpisu je nutné provést v nastavení účtu.





Aby se certifikát zobrazil, musí být vložena karta ve čtečce.





9 Vydání následného certifikátu

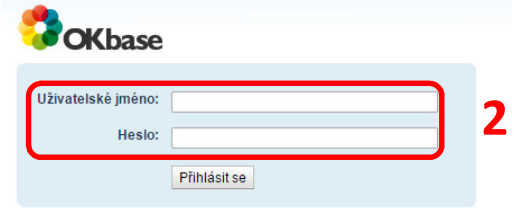
Platnost vydaného certifikátu je 1 rok a nelze ho prodloužit, proto je nutné si zažádat o nový resp. následný certifikát.

Existují dva způsoby vydání následného certifikátu:

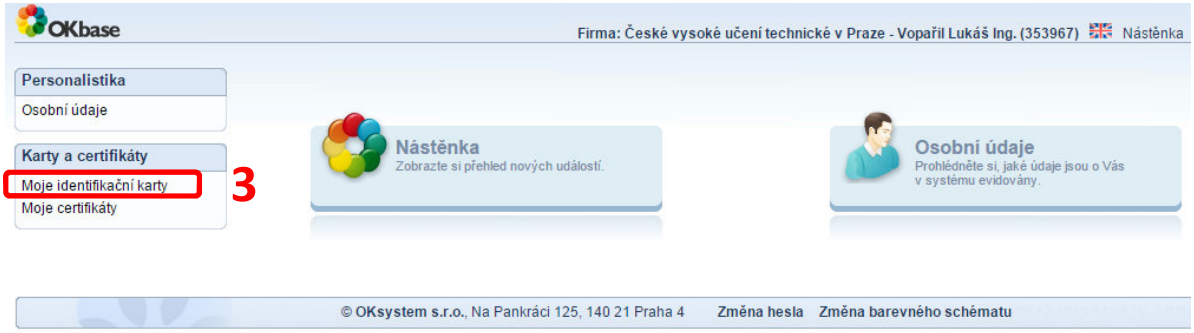
a) **Vydání následného certifikátu přes internet** – pouze pokud je aktuální certifikát stále platný
b) **Vydání následného certifikátu ve Vydavatelství průkazů** – po skočení platnosti certifikátu je z bezpečnostních důvodů možné vydat následný certifikát pouze ve Vydavatelství průkazů

9.1 Vydání následného certifikátu přes internet

1) Jděte na adresu https://pki.cvut.cz/okbase
2) Zadejte uživatelské jméno a heslo (stejné jako v Usermap, KOS ...).

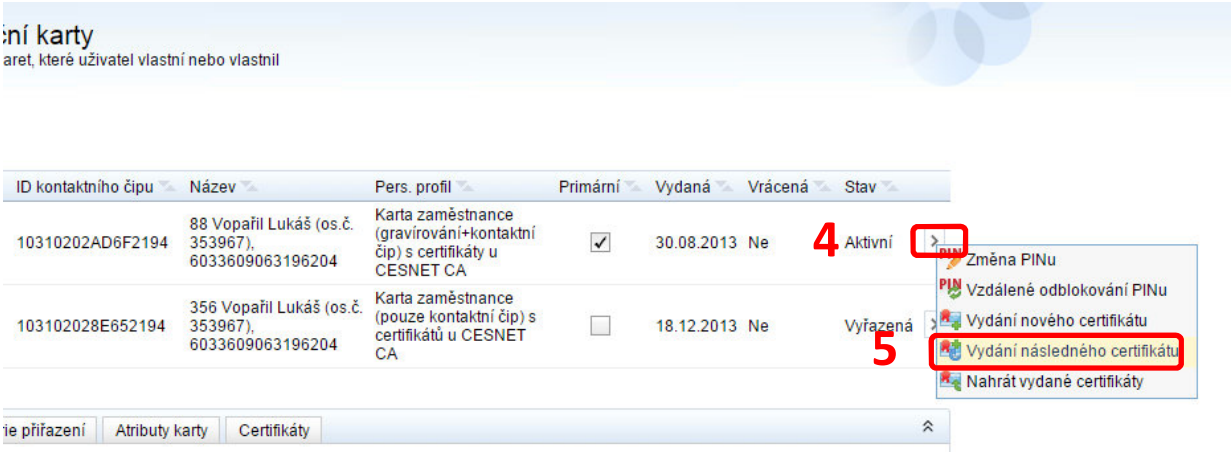


3) Zvolte volbu „Moje identifikační karty“

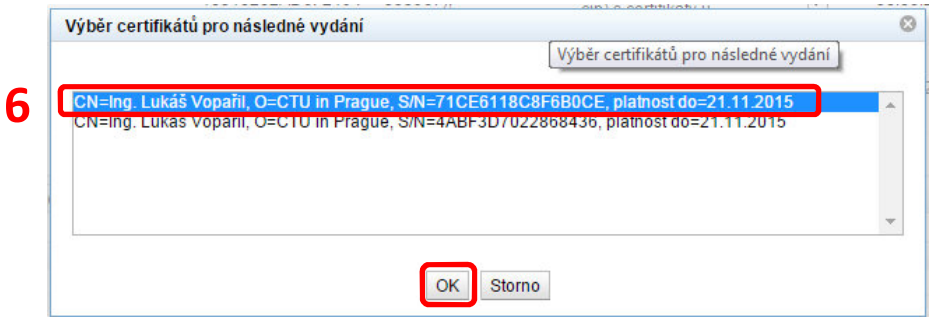


Pro správný průběh musíte mít prohlížeči nainstalováno a povoleno JAVA min. verze 5. V případě dotazů povolte spuštění JAVA appletů.

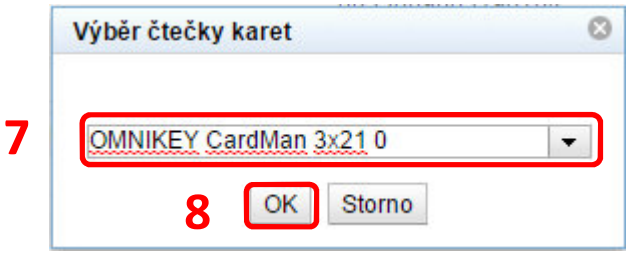
4) V okně „Moje identifikační karty“ vyhledejte kartu, která je ve stavu AKTIVNÍ a rozklikněte šipku nalevo a zvolte možnost – „Vydání následného certifikátu“



5) Vyberte certifikát, který chcete nahradit novým (ten před koncem platnosti)

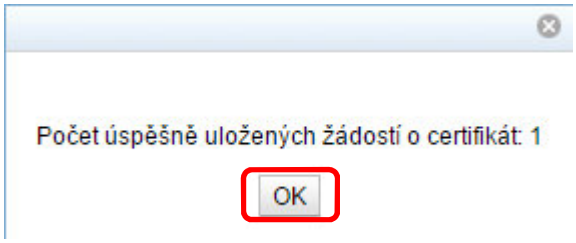


6) Vybere čtečku a vložte do ní průkaz.

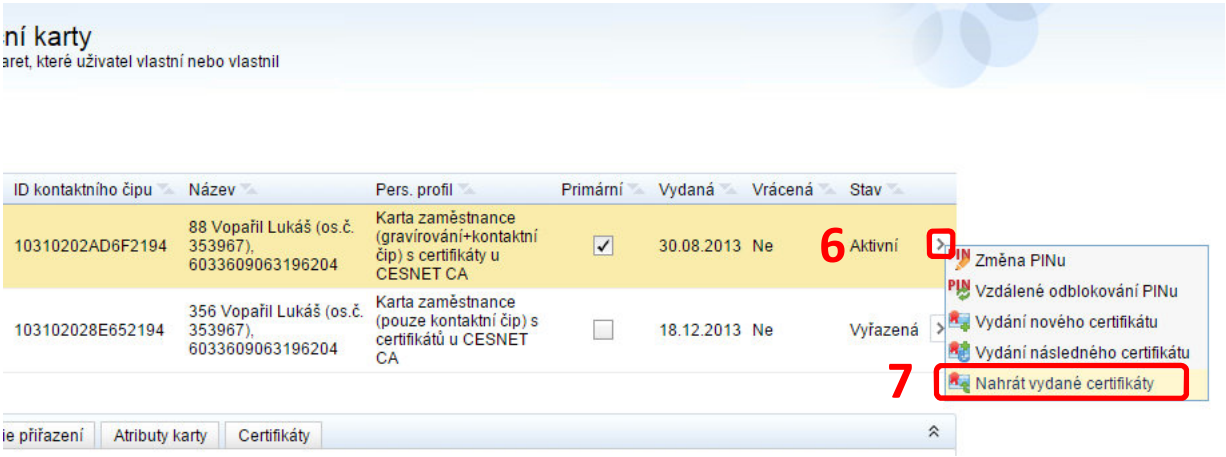


7) Zadejte PIN kód (který jste obdrželi při vydání čipové karty) a potvrďte. Pokud PIN nemáte, obraťte se na Vydavatelství průkazů, kde Vám vydají nový.

8) Poté vyčkejte na potvrzení o uložení žádosti.



9) O vydání certifikátu budete informování emailem. Tento proces obvykle trvá max. 2 pracovní dny.
10) Po obdržení potvrzovacího emailu jděte opět na stránky https://pki.cvut.cz/okbase/ a zvolte „Moje identifikační karty“.
11) V okně „Moje identifikační karty“ vyhledejte kartu, která je ve stavu AKTIVNÍ a rozklikněte šipku nalevo a zvolte možnost – „Nahrát vydané certifikáty“



12) Dále zopakujte krok 5 – 7.

9.2 Vydání následného certifikátu ve Vydavatelství průkazů

Pokud doba platnosti aktuálního certifikátu již vypršela, je možné vydat nový pouze ve Vydavatelství průkazů. Sebou si vezměte svůj průkaz a PIN kód. Pokud PIN neznáte, bude Vám ve Vydavatelství průkazů nastaven nový.