AiS2

AKADEMICKÝ
INFORMAČNÝ SYSTÉM
AiS 2

# Príručka používateľa

# Elektronický podpis

 verzia 1.0

# OBSAH



**V prípade problémov a otázok súvisiacich s elektronickým podpisom sa obráťte na:**
Radovana Engela,
CIIT – TIP, Jesenná 5
radovan.engel@upjs.sk,
VOIP: 2456

**Poznámka:** Zobrazenie okien a znenie textov závisí od konkrétnej inštalácie operačného systému a ďalších aplikácii. V jednotlivých jazykových mutáciách a verziách sa môžu líšiť.

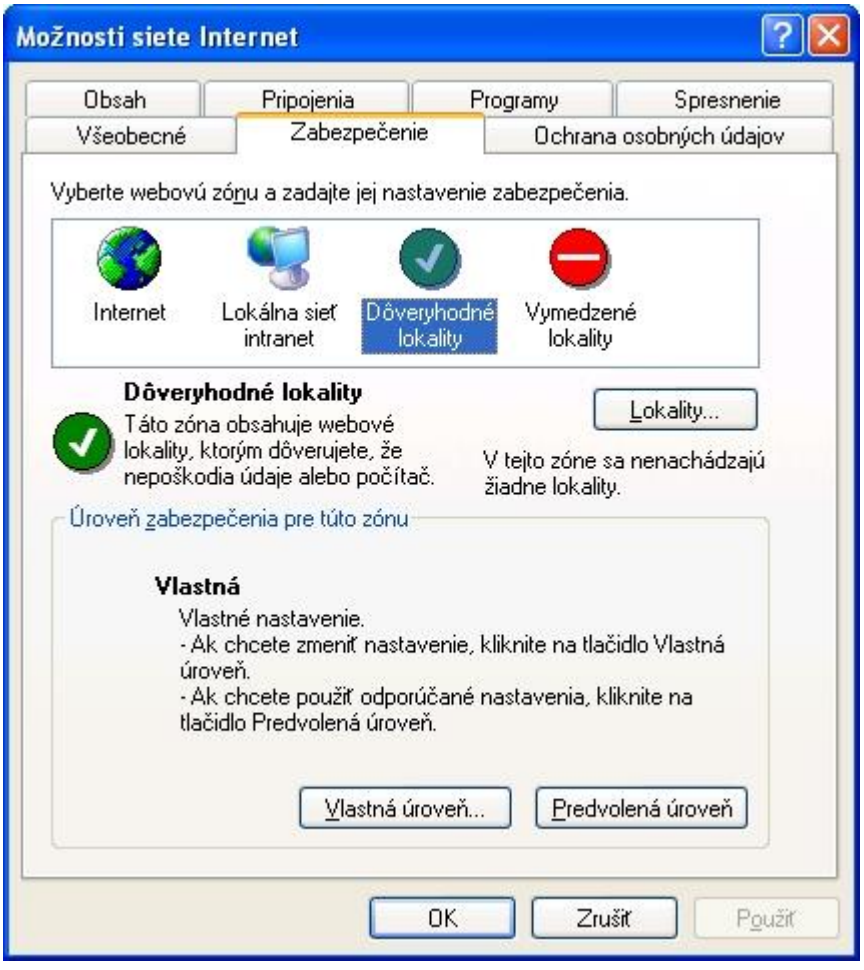
# 1 GENEROVANIE ŽIADOSTI O VYDANIE OSOBNÉHO CERTIFIKÁTU

**Dôležité upozornenie:** Pri generovaní žiadosti majte na zreteli, že Váš osobný certifikát musí byť nainštalovaný **na tom istom počítači (a v tom istom prehliadači)**, na ktorom bola generovaná žiadosť. Po vyexportovaní už nainštalovaného osobného certifikátu ho však budete môcť používať aj na iných počítačoch.

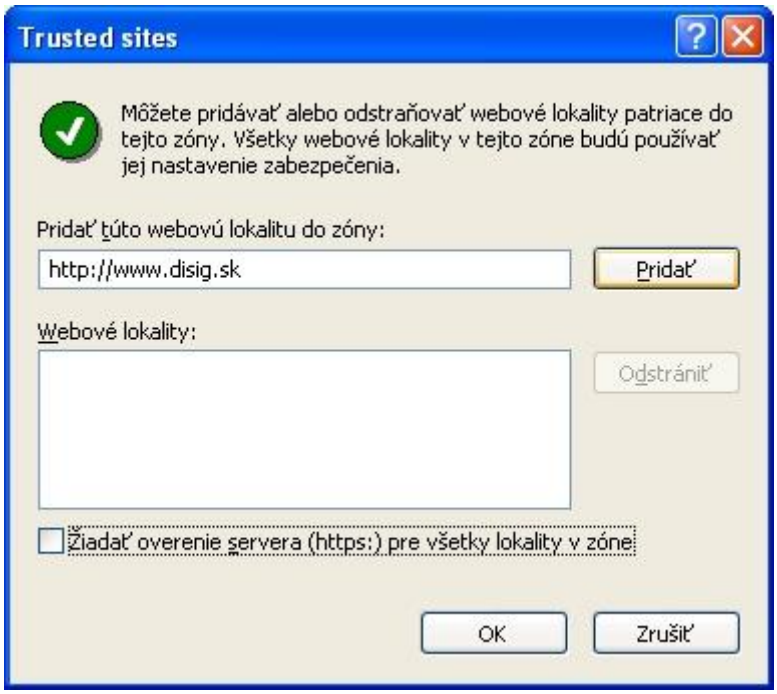
## 1.1 Generovanie žiadosti o vydanie osobného certifikátu v internetovom prehliadači Internet Explorer

**Pre užívateľov operačného systému Windows Vista**: Pred samotným generovaním žiadosti o vydanie osobného certifikátu je potrebné urobiť nasledovné nastavenia Internet Exploreru:

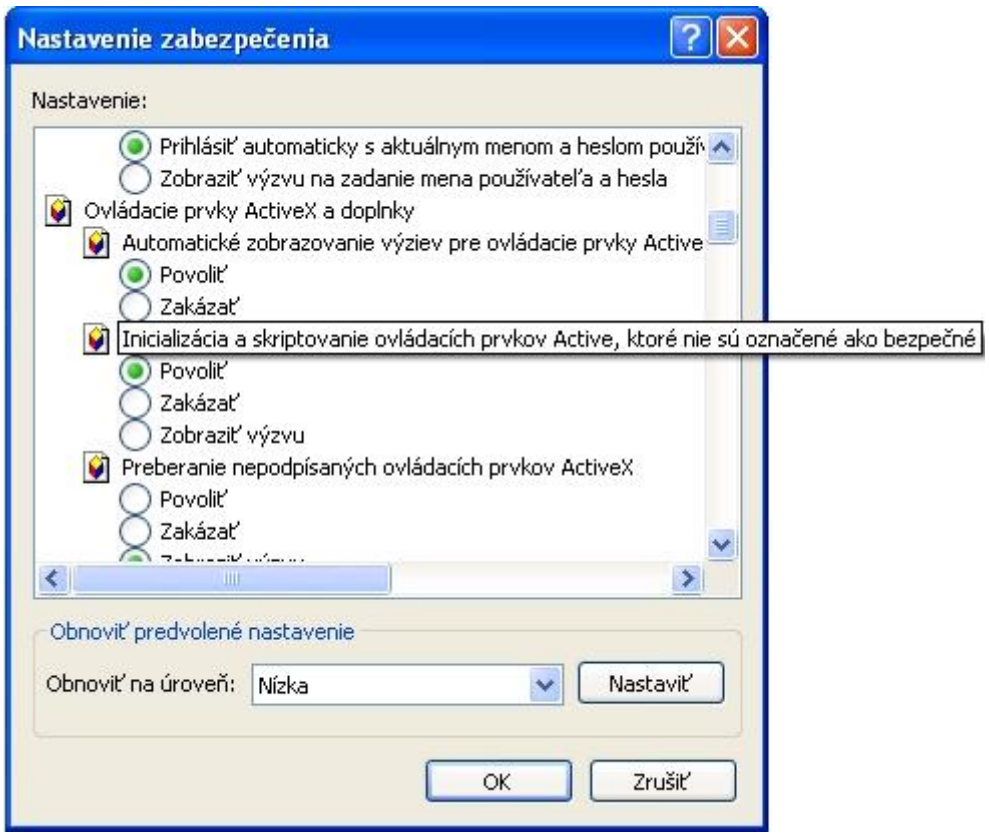
I. Z hlavnej ponuky programu vyberte "**Nástroje**" a potom "**Možnosti siete Internet**". V tomto dialógovom okne zvoľte kartu "**Zabezpečenie**" a kliknite na "**Dôveryhodné lokality**":



II. Kliknite na tlačidlo "**Lokality**" a urobte nastavenia podľa obrázku nižšie (nezabudnite zrušiť možnosť "**Žiadať overenie servera (https:) pre všetky lokality v zóne**"), potom kliknite na "**Pridať**" a napokon na "**OK**". Stránka http://www.disig.sk sa pridá medzi "**Webové lokality**":




III. Na karte "**Zabezpečenie**" dialógového okna "**Možnosti siete Internet**" kliknite na tlačidlo "**Vlastná úroveň**" (ako webová zóna musia byť stále označené "**Dôveryhodné lokality**"). V otvorenom dialógovom okne zabezpečte, aby bolo "**Inicializovanie a skriptovanie ovládacích prvkov Active, ktoré nie sú označené ako bezpečné**" povolené (viď obrázok nižšie). Nastavenia ukončíte kliknutím na "**OK**" a zatvorením dialógového okna "**Možnosti siete Internet**".

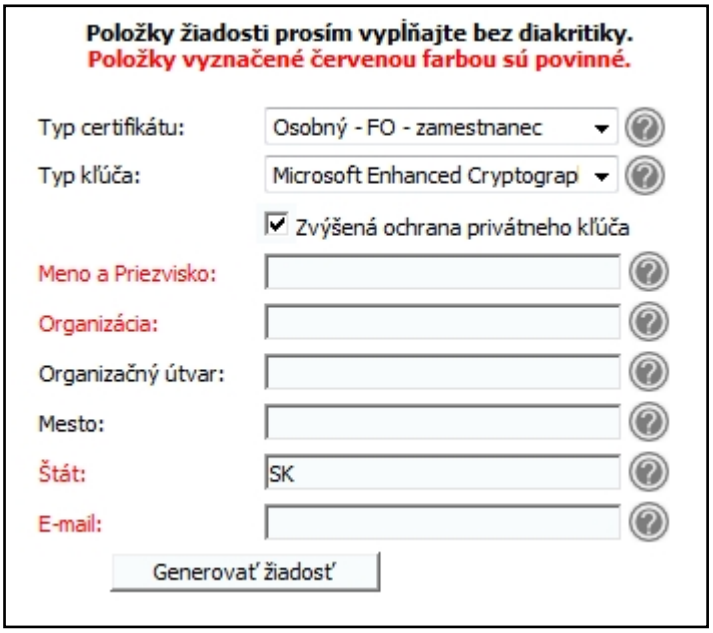



# Postup pri generovaní žiadosti o vydanie o osobného certifikátu

**Poznámka pre užívateľov operačného systému Windows Vista**: Pri generovaní žiadosti o vydanie osobného certifikátu po 2. bode nižšie uvedeného postupu automaticky nasleduje 5.bod.

1. Kliknite na https://eidas.disig.sk/sk/genrequest/:


2. Ako typ certifikátu zvoľte "**Osobný – Fyzická osoba - zamestnanec**". Zobrazí sa Vám nasledujúci formulár, do ktorého je potrebné zadať údaje, ktoré požadujete mať v certifikáte:




**Všetky údaje sa vypisujú bez diakritiky!**

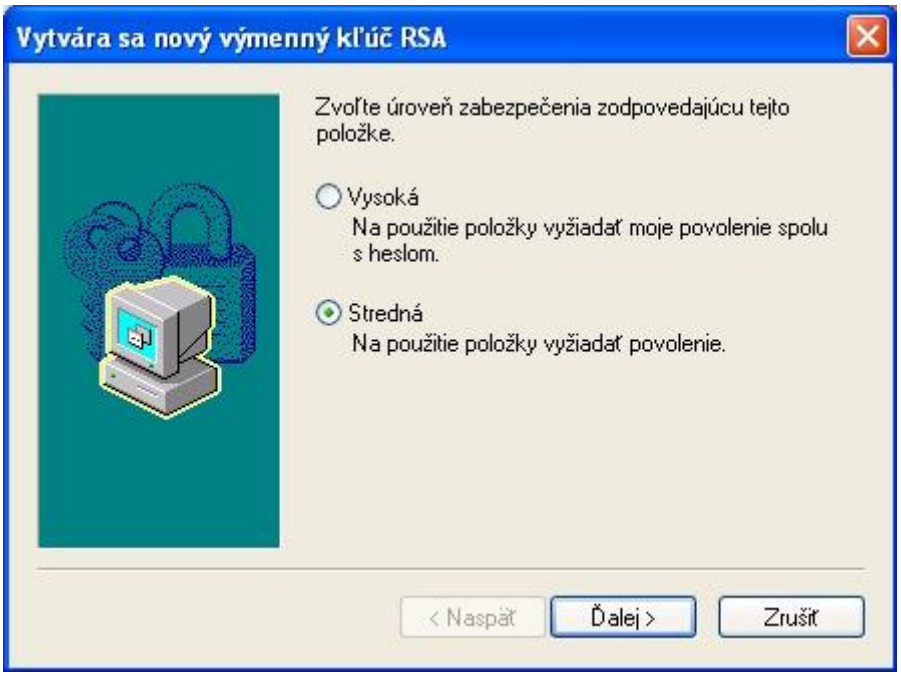
- ***Typ certifikátu*:** zvoľte možnosť "**Osobný – FO – zamestnanec**"
- Políčko **Zvýšená ochrana privátneho kľúča** nechajte zaškrtnuté
- ***Typ kľúča*:** zvoľte možnosť " **Microsoft Enhanced Cryptographic vs 1.0.** "
- ***Meno a priezvisko (POVINNÝ ÚDAJ)*:** zadajte údaje z občianskeho preukazu, pokiaľ máte titul zapísaný v OP a požadujete ho mať uvedený aj v certifikáte, zapíšte ho pred Vaše krstné meno
- ***Organizácia*** – **UPJS v Kosiciach, položka musí byť vyplnená touto hodnotou!!!**
- *Organizačný útvar (NEPOVINNÝ ÚDAJ)*
- *Mesto (NEPOVINNÝ ÚDAJ)*: vypisuje sa podľa trvalého bydliska
- ***Štát (POVINNÝ ÚDAJ)*:** položku nemeňte, jej hodnota je **SK**
- ***E-mail (POVINNÝ ÚDAJ)*:** (školský e-mail, **NIE súkromný**)

3. Zapísané hodnoty si ešte raz skontrolujte, ak s týmito hodnotami súhlasíte, zvoľte možnosť **„Generovať žiadosť“**. Po kliknutí na túto možnosť sa Vám zobrazí nasledovná informácia:


- Webové rozhranie Vás týmto oznamom upozorňuje, že webová stránka žiada o generovanie novej žiadosti o certifikát. Na pokračovanie zvoľte možnosť "**Áno**".

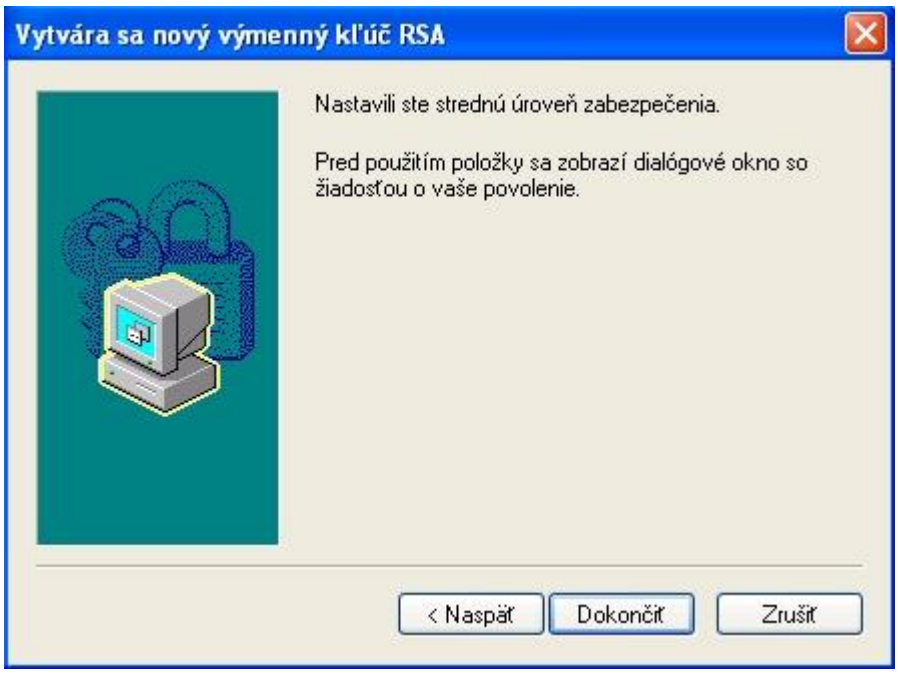
4. Následne budete vyzvaní, aby ste si zvolili úroveň zabezpečenia Vášho súkromného kľúča. V ponúknutom okne kliknite na možnosť "**Nastaviť úroveň zabezpečenia...**":


- Predvolené nastavenie je hodnota "**Stredná**". Znamená to, že Váš **súkromný kľúč nebude chránený** žiadnym **heslom**, takže **práca** s certifikátom prebehne **automaticky**:




***Dôležité upozornenie***: V prípade, že sa rozhodnete úroveň zabezpečenia súkromného kľúča nastaviť na najvyššiu hodnotu (použitie súkromného kľúča bude zabezpečené heslom), zvoľte si možnosť "**Vysoká**". Heslo zapíšete do ponúknutého okna "**Heslo**", a následne zvolené heslo potvrďte zápisom do okna "**Potvrdiť**". Pri každej práci s certifikátom budete musieť zadávať Vami zvolené heslo.

- Pre pokračovanie generovania žiadosti kliknite na "**Ďalej >**" a následne na "**Dokončiť**":

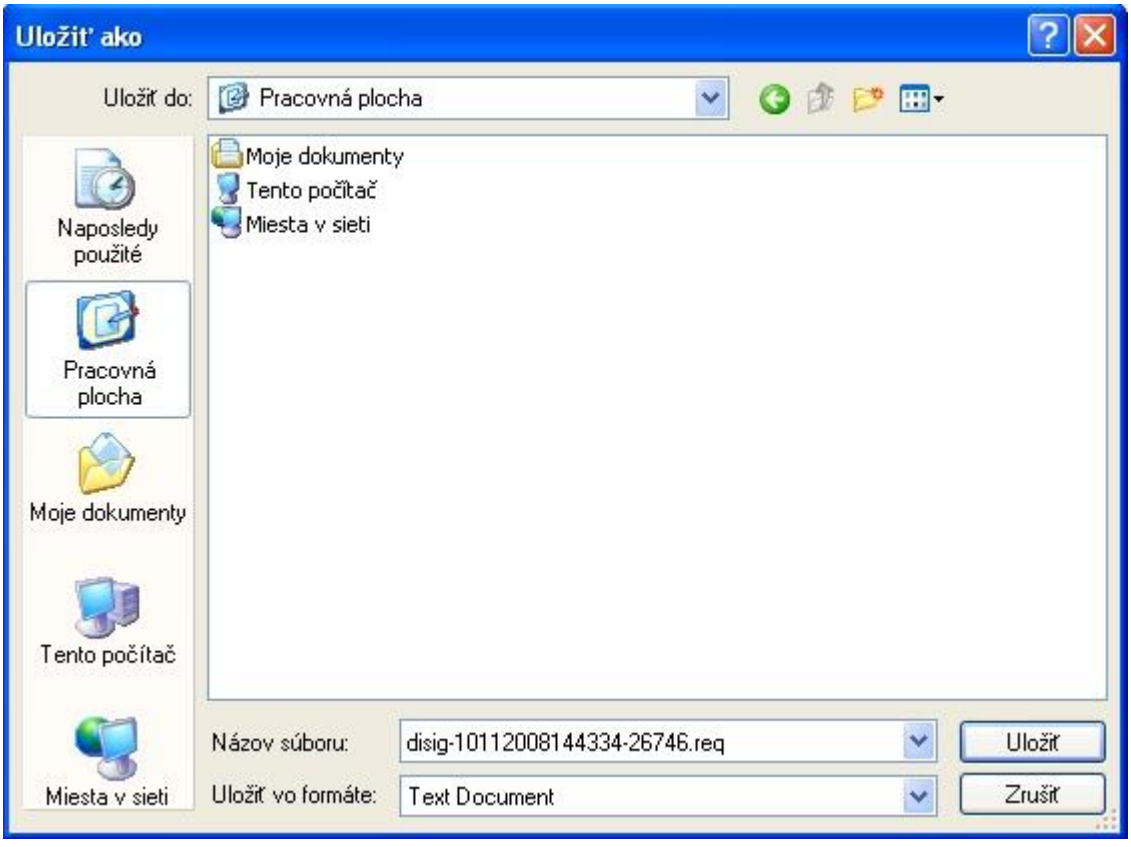



- Proces nastavenia hesla ukončíte kliknutím na "**OK**":

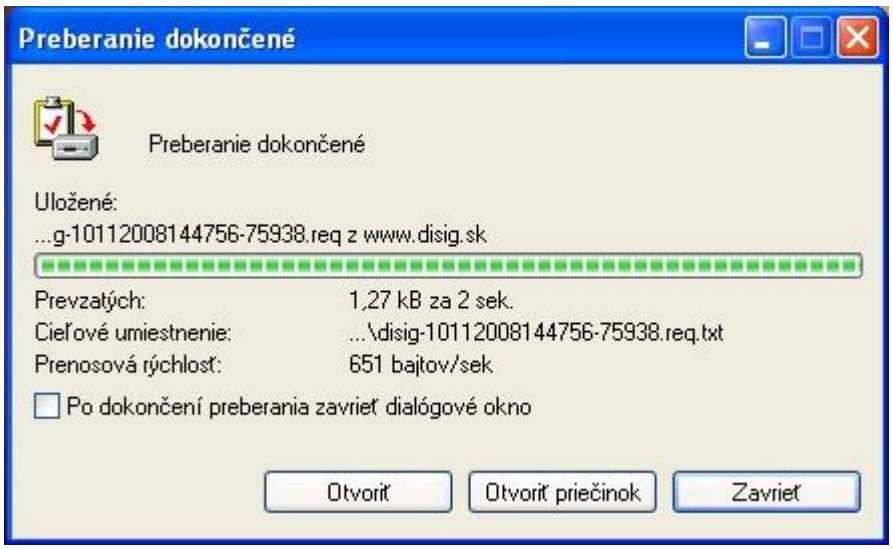

5. Po vygenerovaní žiadosti uvidíte upozornenie, že žiadosť bola vygenerovaná:

6. Kliknite na možnosť "**Uložiť žiadosť o certifikát**", po zobrazení ďalšieho okna kliknite na "**Uložiť**":


7. Zobrazí sa Vám nasledujúce okno, v ktorom je potrebné určiť si cestu uloženia žiadosti. Zvoľte si cestu a kliknite na možnosť "**Uložiť**". Zvolenú cestu si zapamätajte, pretože túto žiadosť je potrebné doručiť na príslušnú registračnú autoritu:



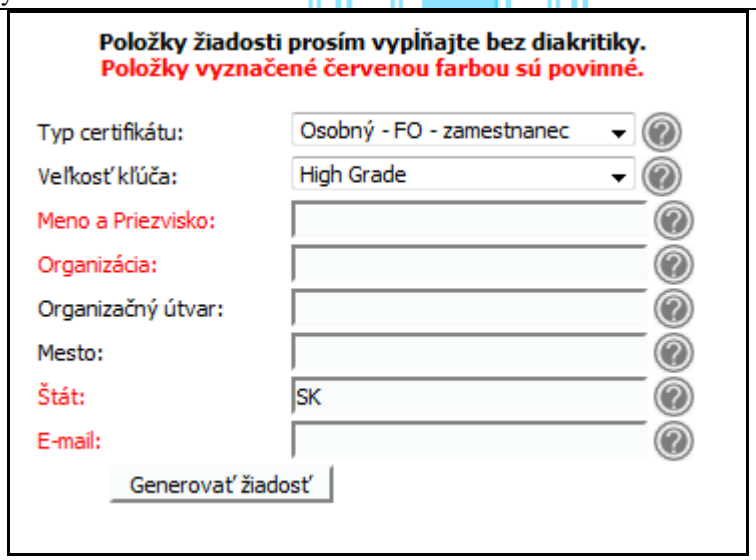

8. Kliknite na "**Zavrieť**", tým sa proces generovania žiadosti končí:




## 1.2 Generovanie žiadosti o vydanie osobného certifikátu v internetovom prehliadači Mozilla Firefox

1. Kliknite na https://eidas.disig.sk/sk/genrequest/:

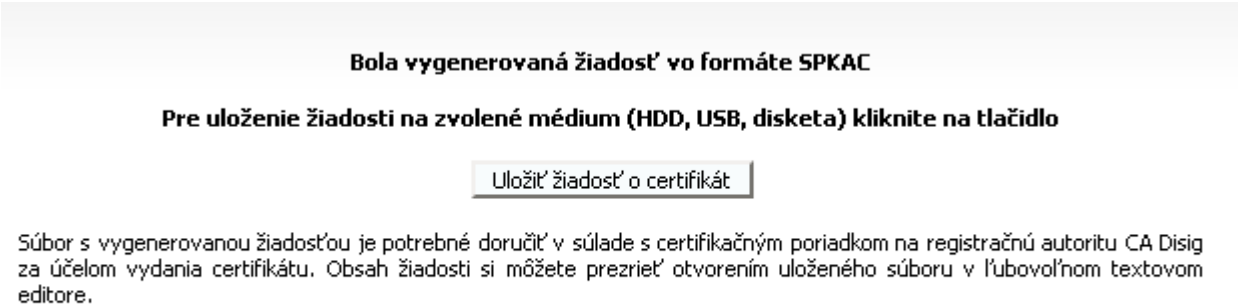

2. Ako typ certifikátu zvoľte "**Osobný – Fyzická osoba - zamestnanec**". Zobrazí sa Vám nasledujúci formulár, do ktorého je potrebné zadať údaje, ktoré požadujete mať v certifikáte:



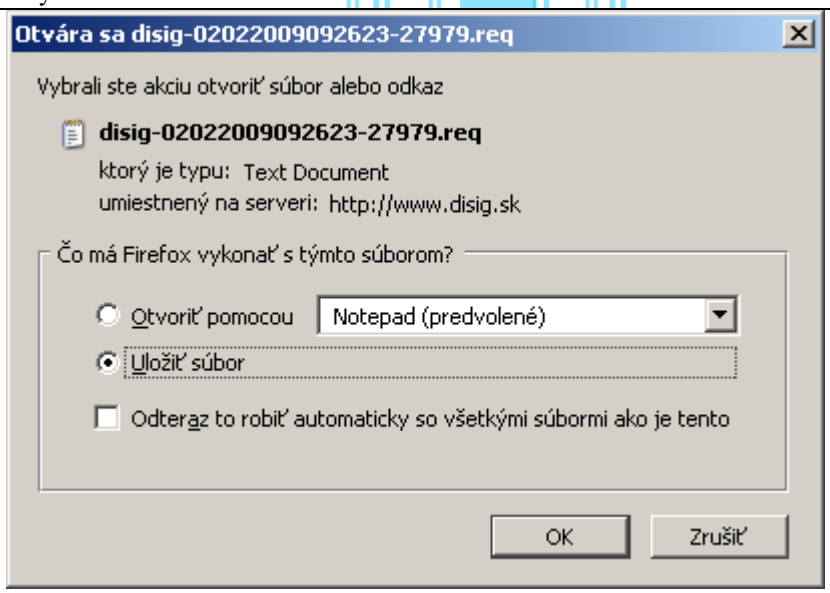

**Všetky údaje sa vypisujú bez diakritiky!**

- ***Typ certifikátu*:** zvoľte možnosť "**Osobný – FO – zamestnanec**"
- ***Typ kľúča*:** zvoľte možnosť "**High Grade**", prípadne dĺžku (veľkosť) kľúča **2048 bitov.**
- ***Meno a priezvisko (POVINNÝ ÚDAJ)*:** zadajte údaje z občianskeho preukazu, pokiaľ máte titul zapísaný v OP a požadujete ho mať uvedený aj v certifikáte, zapíšte ho pred Vaše krstné meno
- ***Organizácia*** – **UPJS v Kosiciach, položka musí byť vyplnená touto hodnotou!!!**
- *Organizačný útvar (NEPOVINNÝ ÚDAJ)*
- *Mesto (NEPOVINNÝ ÚDAJ)*: vypisuje sa podľa trvalého bydliska
- ***Štát (POVINNÝ ÚDAJ)*:** položku nemeňte, jej hodnota je **SK**
- ***E-mail (POVINNÝ ÚDAJ)*:** (školský e-mail, **NIE súkromný**)

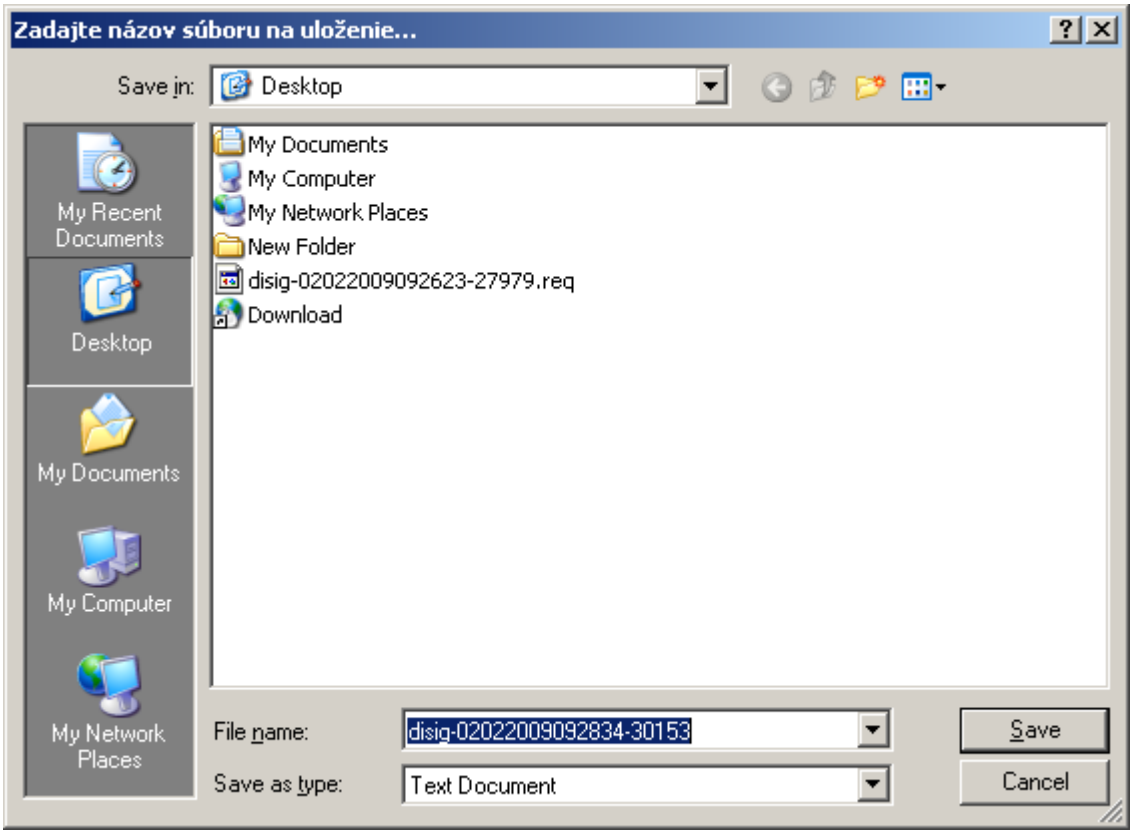
3. Zapísané hodnoty si ešte raz skontrolujte, ak s týmito hodnotami súhlasíte, zvoľte možnosť **„Generovať žiadosť“**. Po kliknutí na túto možnosť sa Vám zobrazí upozornenie, že žiadosť bola vygenerovaná:



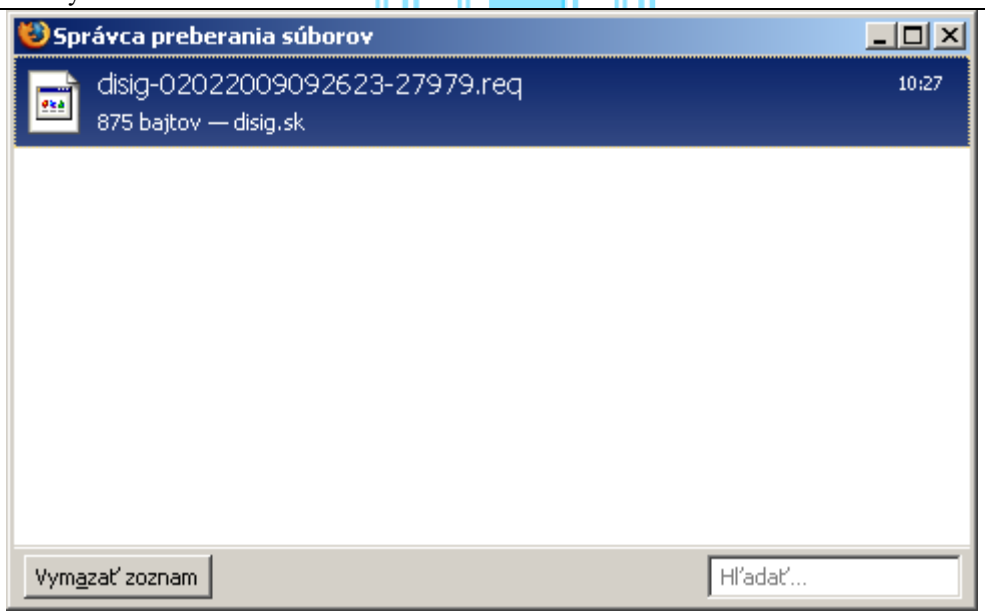

4. Kliknite na možnosť "**Uložiť žiadosť o certifikát**", po zobrazení ďalšieho okna kliknite na "**Uložiť súbor**":




5. V závislosti od nastavenia programu Mozilla Firefox sa Vám môže zobraziť nasledujúce okno, v ktorom je potrebné určiť si cestu uloženia žiadosti. Prípadne sa súbor uloží na vopred nastavené miesto a pokračujete hneď bodom 6 tohto návodu. Zvoľte si cestu a kliknite na možnosť "**Uložiť**". Zvolenú cestu si zapamätajte, pretože túto žiadosť je potrebné doručiť na príslušnú registračnú autoritu:




6. Zatvorte okno "**Správcu preberania súborov**", tým sa proces generovania žiadosti končí:




7. Ak vám už aspoň raz bol vydaný certifikát od Disigu, tak stačí odoslať vygenerovanú žiadosť mailom z emailovej adresy uvedenej v žiadosti na adresu aio@upjs.sk (tel. kontakty s ďalšími informáciami 055/2341512 alebo 055/2341514)

   V prípade, že sa **zmenili** vaše osobné údaje, je **nutná** vaša **osobná návšteva registračnej autority** (Správa AIO na Šrobárovej 2, Ing. Ondrejová, p. Sedláková) a predloženie dokladov (OP + ďalší doklad (zamestnanecký preukaz, cestovný pas, vodičský preukaz, preukaz zdravotného poistenia, ...)) s aktuálnymi osobnými údajmi spolu s vygenerovanou žiadosťou na USB kľúči (prípadne inom nosiči). Rovnako je nutná osobná návšteva ak je Vám certifikát vydávaný prvý krát, alebo ak sa ukáže, že Vaše údaje **nie sú v aplikačnej databáze prístupné** (včas budete v takom prípade vyrozumený).

# 2 INŠTALÁCIA OSOBNÉHO CERTIFIKÁTU

## 2.1 Inštalácia osobného certifikátu do systémového úložiska certifikátov MS Windows

Inštalácia osobného certifikátu vydaného certifikačnou autoritou CA Disig do systémového úložiska certifikátov MS Windows sa vykonáva v dvoch krokoch.

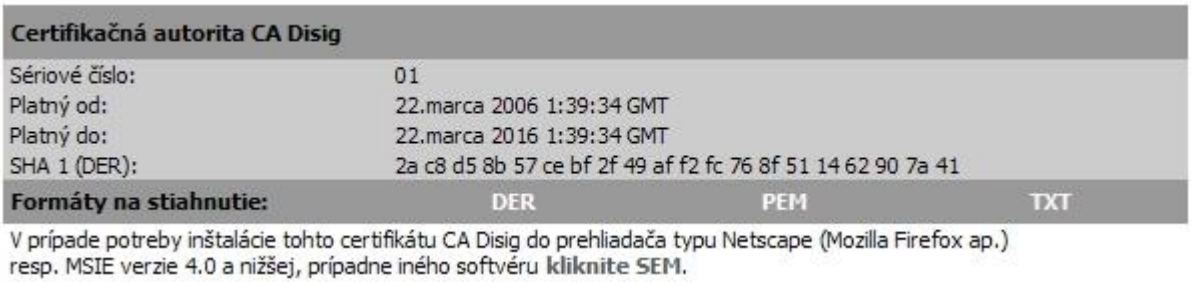
V prvom kroku sa vykoná inštalácia certifikátu samotnej certifikačnej autority CA Disig, čím táto bude pridaná medzi "**Dôveryhodné úrady pre vydávanie základných certifikátov**". V druhom kroku sa vykoná vlastná inštalácia osobného certifikátu.

**Pre užívateľov operačného systému Windows Vista**: Pretože certifikát certifikačnej autority CA Disig je súčasťou operačného systému Windows Vista, môžete v uvedenom postupe automaticky prejsť na druhý krok. Podľa návodu na stranách 2-3 tejto príručky si medzi dôveryhodné lokality musíte pridať aj stránku https://www.disig.sk (teda **zabezpečenú** stránku, nezabezpečenú stránku http://www.disig.sk ste medzi dôveryhodné lokality museli pridať už pri generovaní žiadosti).

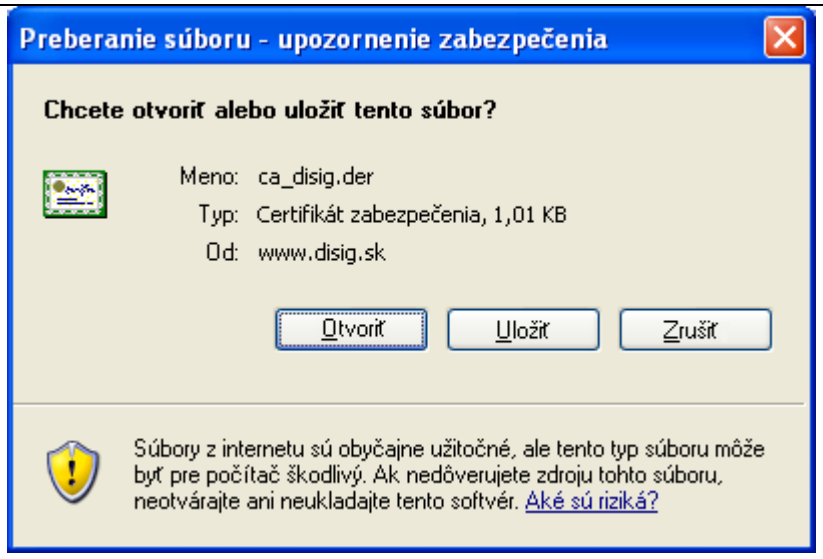
### Prvý krok - Inštalácia certifikátu certifikačnej autority CA Disig

1. Kliknite na https://eidas.disig.sk/sk/cacert/.

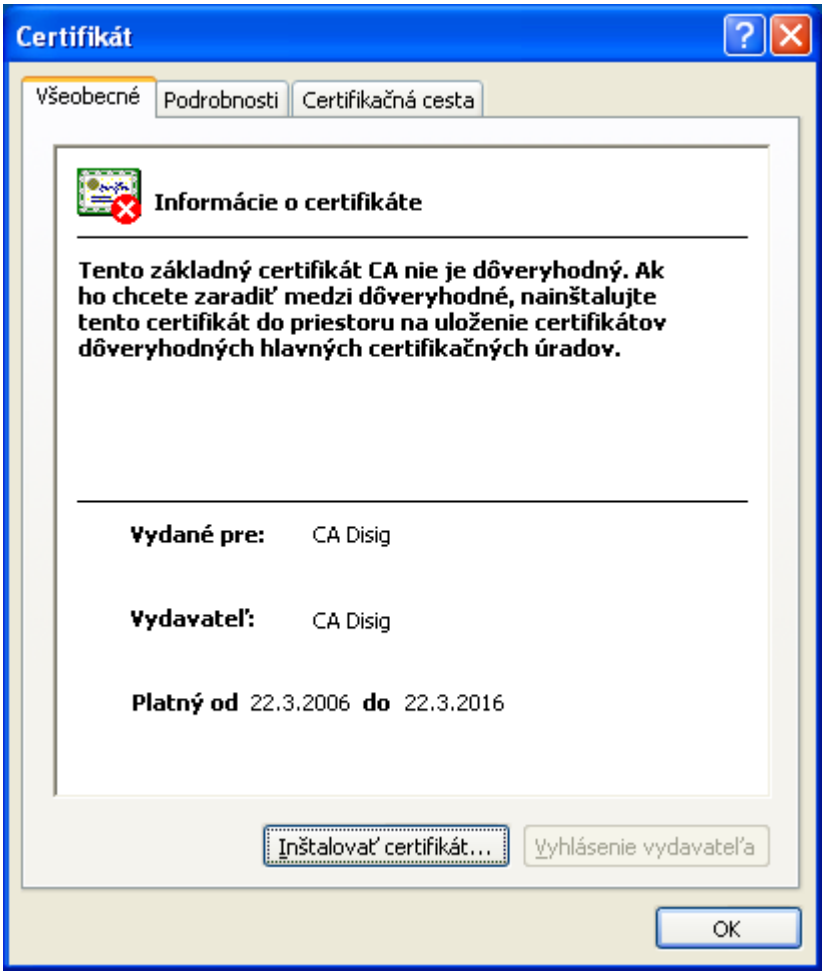
2. Po zobrazení stránky s aktuálnym certifikátom CA Disig kliknite na text "**DER**" v spodnej časti tabuľky "**Certifikačná autorita CA Disig**" v časti "**Formáty na stiahnutie**":



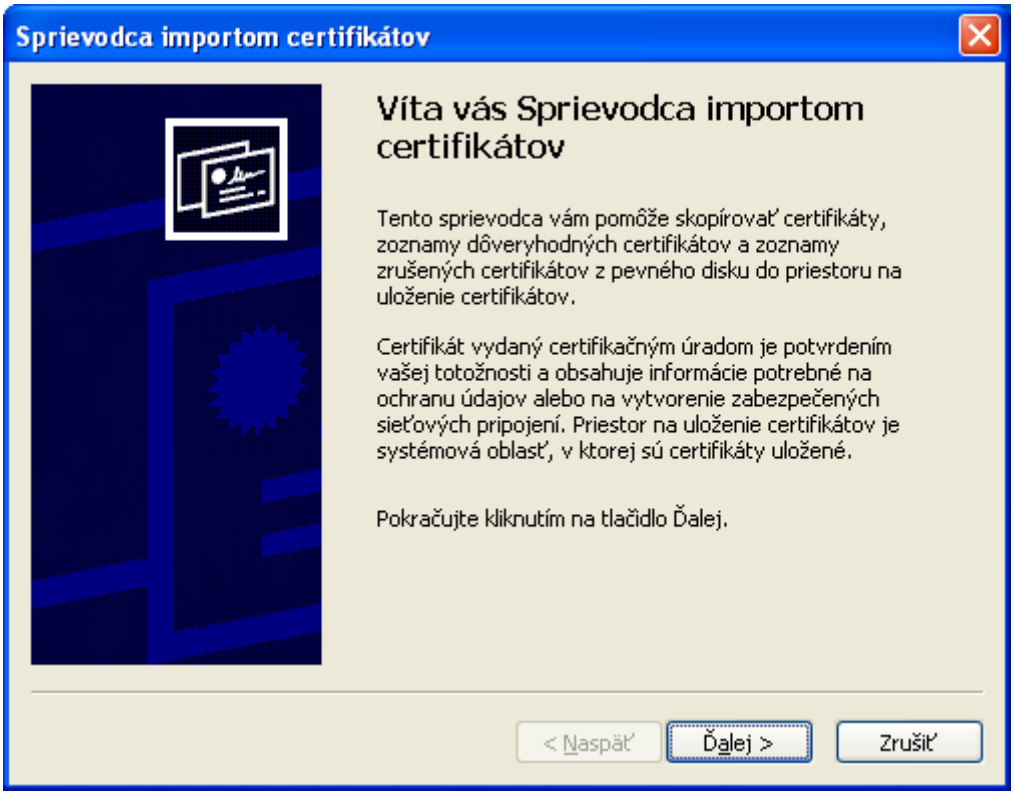

3. Po zobrazení okna s ponukou na výber akcie zvoľte "**Otvoriť**":



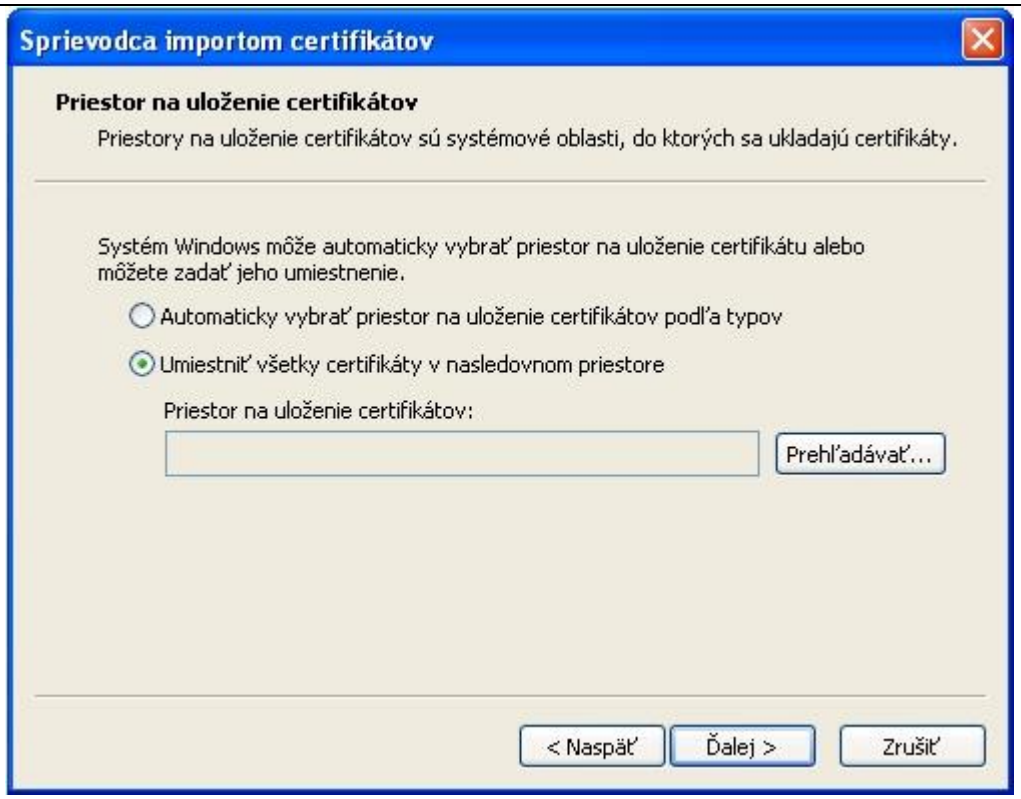

4. Otvorí sa okno s informáciami o certifikáte. Zvoľte "**Inštalovať certifikát**":




5. Pokračujte voľbou "**Ďalej >**":



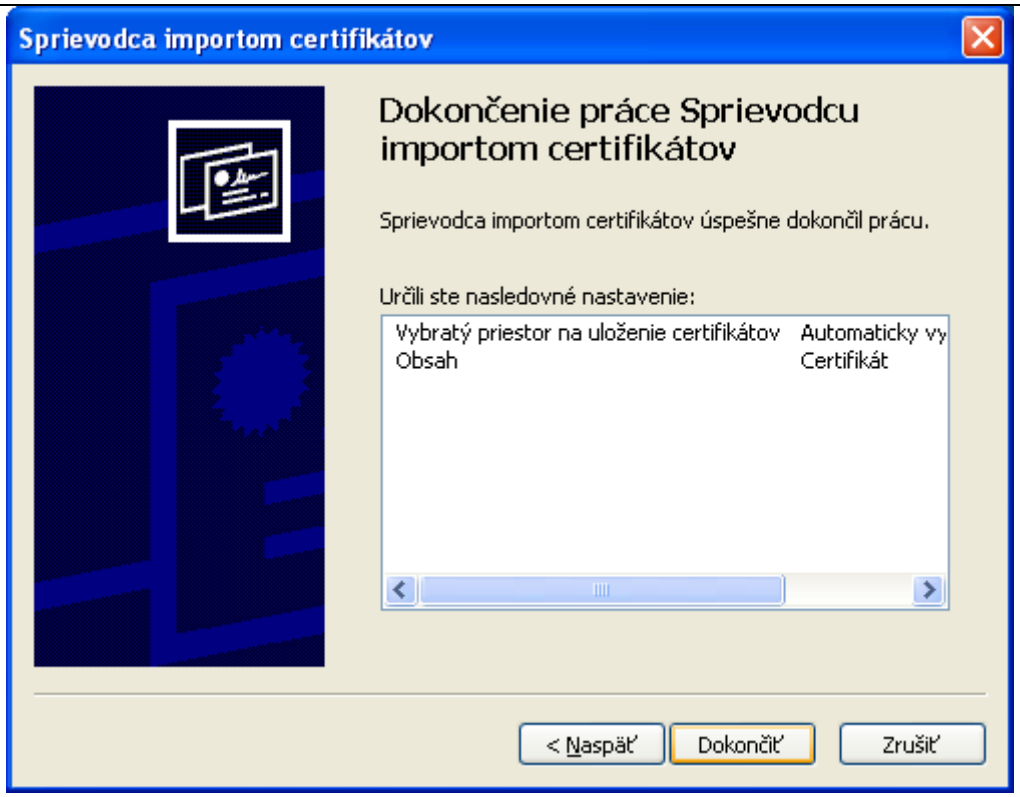

6. Skontrolujte, či je zvolená možnosť "**Umiestniť všetky certifikáty v nasledovnom priestore**" a stlačte tlačidlo "**Prehľadávať**":



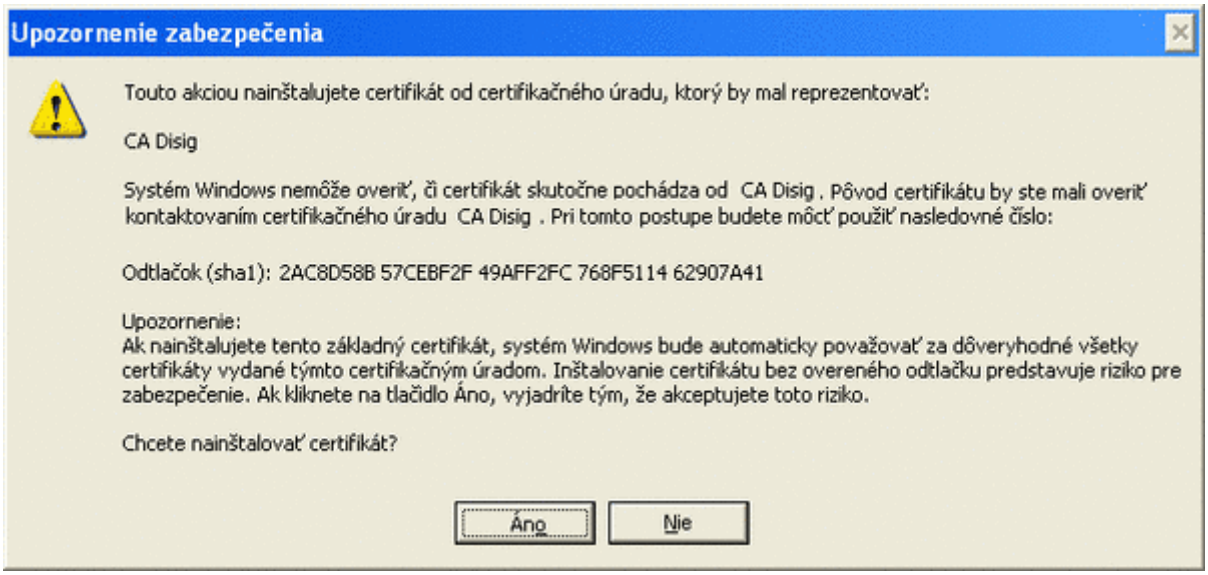

7. Ako priestor na uloženie certifikátov použite "**Dôveryhodné úrady pre vydávanie základných certifikátov**". Svoju voľbu potvrďte stlačením tlačidla "**OK**":


8. Pokračujte voľbou "**Ďalej >**".

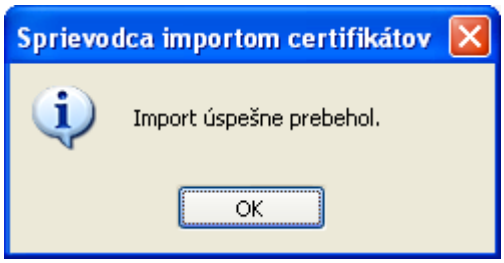
9. Kliknite na tlačidlo "**Dokončiť**":




10. Zobrazí sa upozornenie, že sa chystáte nainštalovať certifikát certifikačnej autority CA Disig. Na potvrdenie zvoľte "**Áno**":



11. Zobrazí sa informácia o úspešnom nainštalovaní certifikátu. Inštaláciu certifikátu CA Disig ukončíte stlačením "**OK**":




Týmto je ukončená inštalácia certifikátu certifikačnej autority CA Disig. Ďalej nasleduje inštalácia Vášho osobného certifikátu.

## Druhý krok - Inštalácia osobného certifikátu

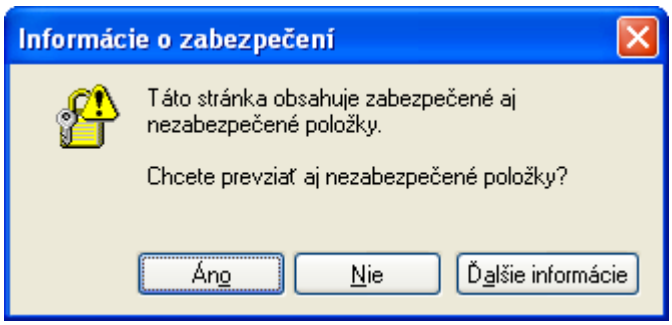
Po vydaní osobného certifikátu Vám certifikačná autorita CA Disig odošle automaticky e-mail s upozornením, že Vám bol vydaný certifikát a zároveň v ňom dostanete linku, prostredníctvom ktorej si certifikát môžete nainštalovať.

1. Kliknite na linku v e-maile, ktorá má tvar (linka sa musí otvoriť v tom webovom prehliadači, ktorý ste použili pri generovaní žiadosti o vydanie certifikátu):

   **https://www.disig.sk/cgi-bin/get_cert?serial=$eSerial**

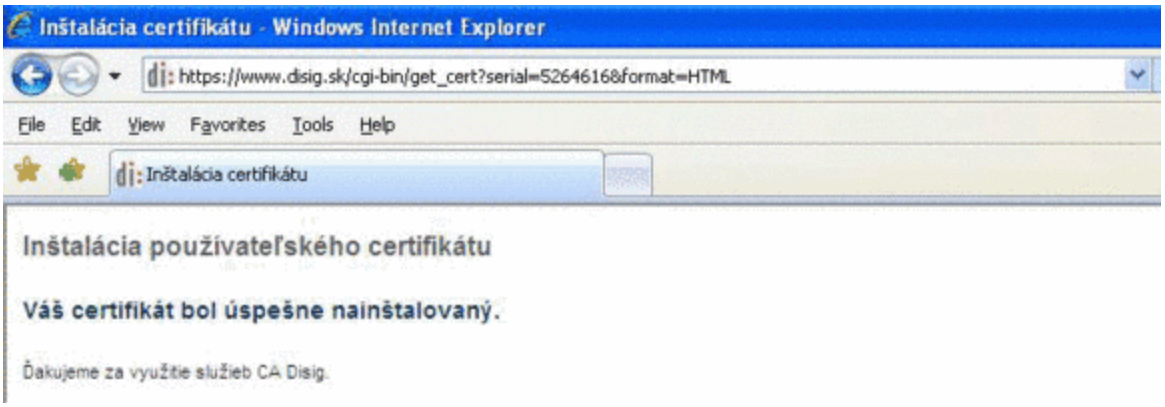
   (**$eSerial** je 7 miestne sériové číslo Vášho osobného certifikátu)

2. Po kliknutí na linku sa v závislosti od nastavenie Vášho internetového prehliadača môže otvoriť okno s informáciou, že stránka, ktorá sa ide otvárať, obsahuje zabezpečené aj nezabezpečené položky. Na pokračovanie zvoľte "**Áno**":



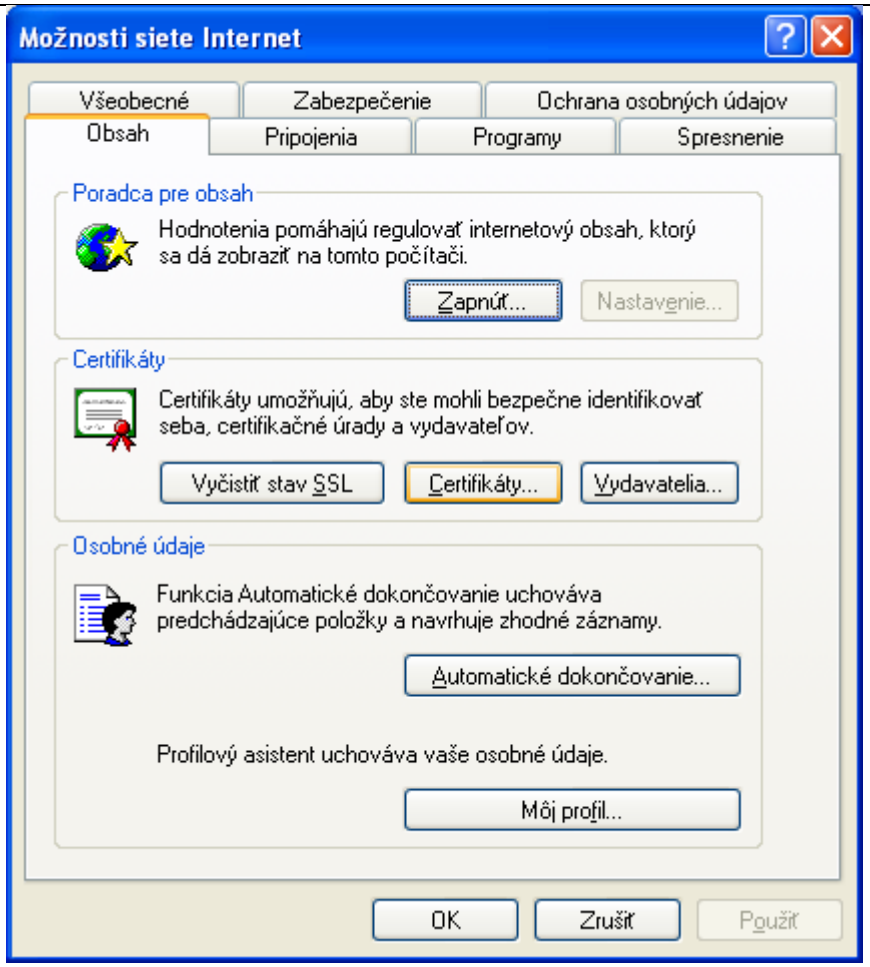

3. Po stlačení "**Áno**" sa otvorí okno s bezpečnostným upozornením o tom, že webová stránka ide pridať nový certifikát do Vášho počítača. Na otázku, či chcete pridať tento nový certifikát do Vášho úložiska certifikátov musíte odpovedať "**Áno**":


4. V prípade, že sú splnené všetky predpoklady na úspešnú inštaláciu certifikátu, je certifikát nainštalovaný a Vám sa zobrazí nasledovné okno s oznamom o úspešnej inštalácii certifikátu:

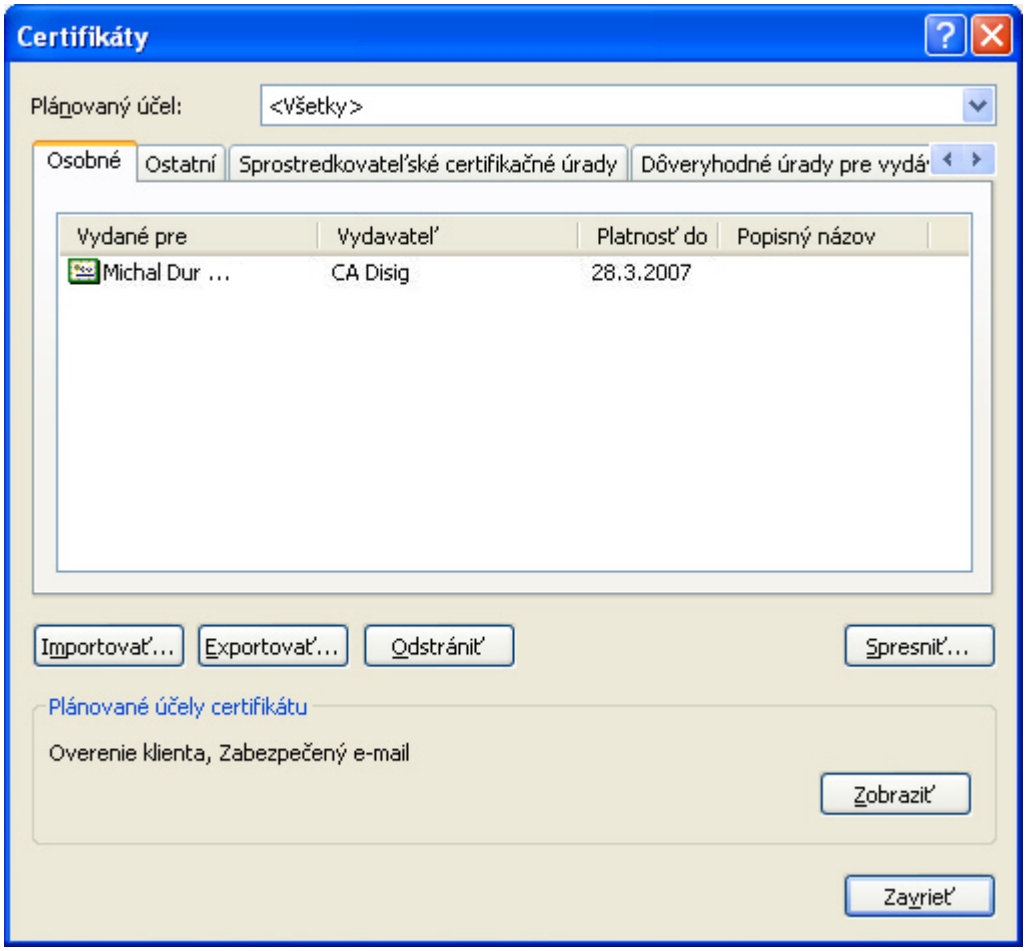



5. V prípade, že sa Vám nepodarilo nainštalovať Váš osobný certifikát prostredníctvom zaslanej linky, je ho možné nainštalovať po jeho vyhľadaní na stránkach Disig-u. Kliknite na tento odkaz a v otvorenom okne vpíšte do položky "**CN**" bez diakritiky celé Vaše meno, (je uvedené v bode 4. protokolu o prevzatí certifikátu). Identifikujte certifikát, ktorý hodláte nainštalovať (spravidla prvý v poradí) a následne v stĺpčeku "**Inštalácia**" kliknite na hrubo vytlačený nápis "**Explorer**". Ďalej postupujte ako je popísané v bodoch 2 až 4.

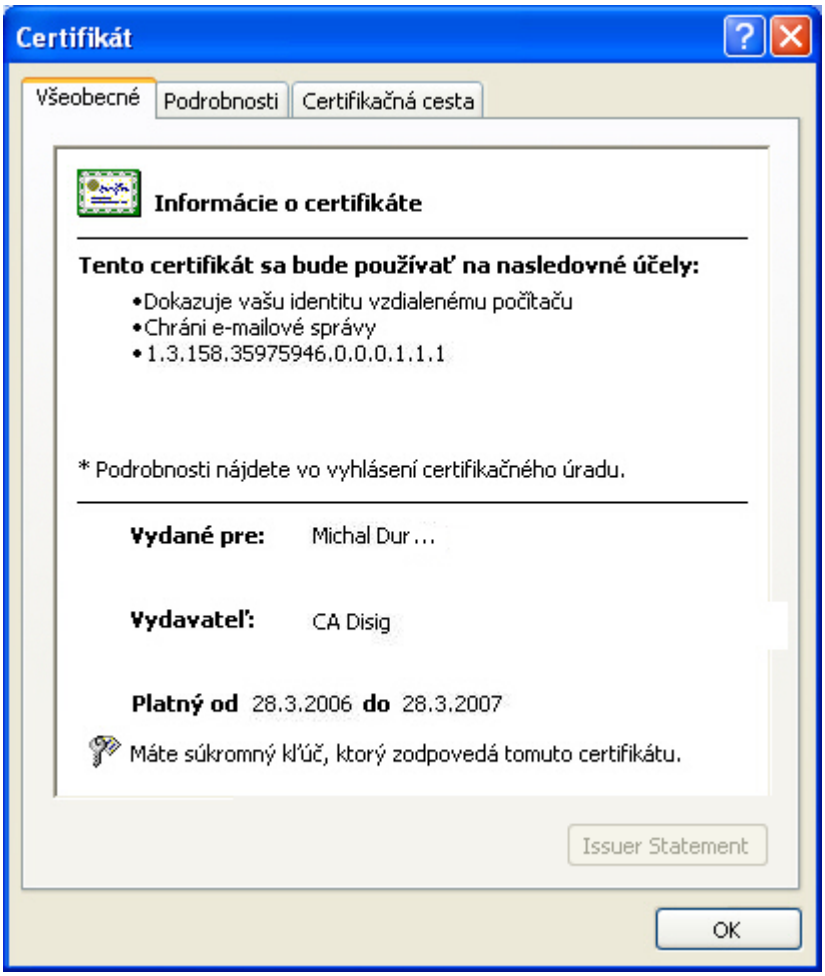
6. Po inštalácii je potrebné overiť nainštalovanie certifikátu. V prehliadači Internet Explorer zvoľte "**Nástroje** -> **Možnosti siete Internet...**-> **Obsah** -> **Certifikáty**":

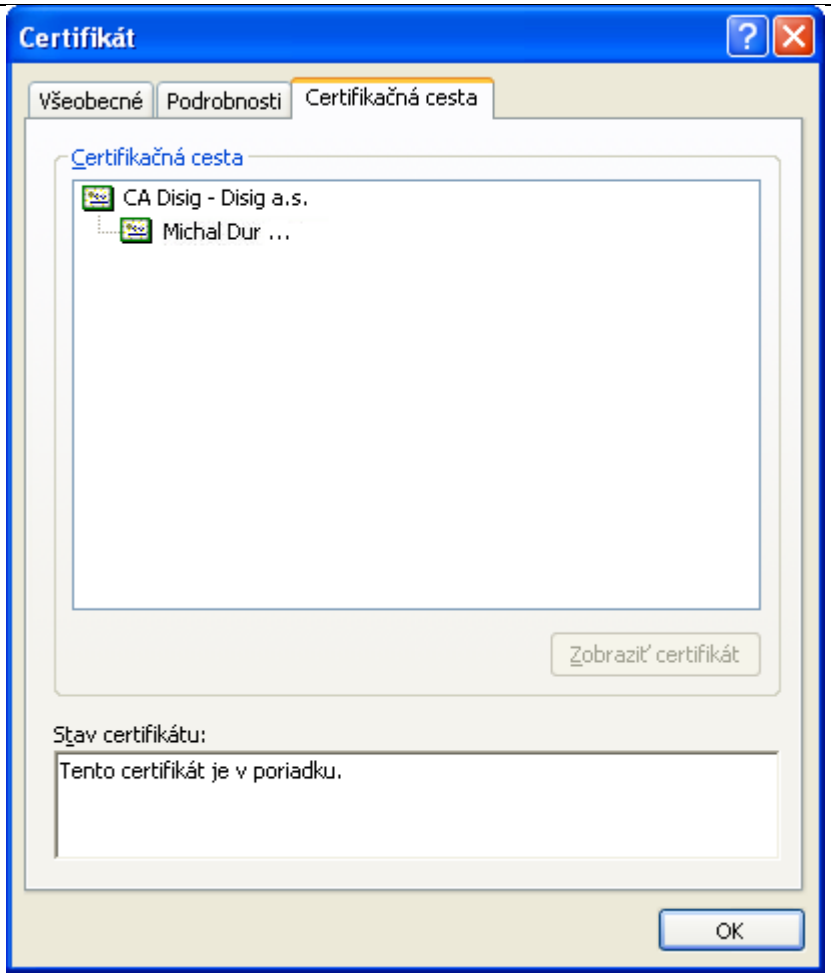



7. Správne nainštalovaný certifikát (užívateľ vlastní zodpovedajúci privátny kľúč) sa po inštalácii nachádza v záložke "**Osobné**":




8. Po označení certifikátu kliknutím na Vaše meno a zvolením možnosti "**Zobraziť**" sa certifikát otvorí. Ak je všetko v poriadku, tak sa v záložke "**Všeobecné**" nachádza pod vyznačením platnosti text "**Máte súkromný kľúč, ktorý zodpovedá tomuto certifikátu**", v záložke "**Certifikačná cesta** " sú zobrazené oba inštalované certifikáty a v spodnej časti je vypísané "**Tento certifikát je v poriadku**":


Certifikát
Všeobecné
Podrobnosti
Certifikačná cesta
Informácie o certifikáte
Tento certifikát sa bude používať na nasledovné účely:
•Dokazuje vašu identitu vzdialenému počítaču
•Chráni e-mailové správy
•1.3.158.35975946.0.0.0.1.1.1
* Podrobnosti nájdete vo vyhlásení certifikačného úradu.
Vydané pre: Michal Dur...
Vydavateľ: CA Disig
Platný od 28.3.2006 do 28.3.2007
Máte súkromný kľúč, ktorý zodpovedá tomuto certifikátu.
Issuer Statement
OK




9. Týmto je ukončená inštalácia Vášho osobného certifikátu.

V prípade úspešného overenia funkčnosti ako ďalší krok jednoznačne odporúčame vykonať zálohu nainštalovaného certifikátu podľa postupu, ktorý je popísaný v kapitole "**Zálohovanie a obnova osobného certifikátu**".

**Poznámka:** V prípade, že sa Váš certifikát po inštalácii nenachádza v záložke "**Osobné**", ale je uložený napríklad v záložke "**Ostatní**", je pravdepodobné, že Váš systém nie je schopný zistiť umiestnenie Vášho privátneho kľúča a tým úspešne nainštalovať certifikát. Skôr ako sa pokúsite o opakovanú inštaláciu, kontaktujte podporu CA Disig.

## 2.2 Inštalácia osobného certifikátu do systémového úložiska certifikátov Mozilla Firefox

**Dôležité upozornenie:** Webový prehliadač Mozilla Firefox **zvyčajne nezdieľa systémové úložisko certifikátov** s ďalším softvérom (ani typu Mozilla, ako je napr. poštový klient Thunderbird, ...). Z toho dôvodu je potrebné ešte importovať certifikáty aj do ďalších programov (popisujú to nasledujúce kapitoly 3.1 až 3.4).

Inštalácia osobného certifikátu vydaného certifikačnou autoritou CA Disig do systémového úložiska Mozilla sa vykonáva v dvoch krokoch.

V prvom kroku sa vykoná inštalácia osobného certifikátu. V druhom kroku sa vykoná inštalácia certifikátu vydávajúcej certifikačnej CA Disig do úložiska dôveryhodných certifikačných autorít.

### 2.2.1 Prvý krok - Inštalácia osobného certifikátu

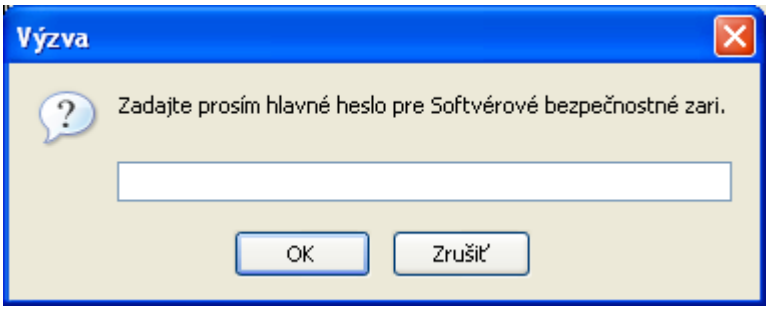
Po vydaní osobného certifikátu Vám certifikačná autorita CA Disig odošle automaticky e-mail s upozornením, že Vám bol vydaný certifikát a zároveň v ňom dostanete linku, prostredníctvom ktorej si certifikát môžete nainštalovať.

1. Kliknite na linku v e-maile, ktorá má tvar (linka sa musí otvoriť v tom webovom prehliadači, ktorý ste použili pri generovaní žiadosti o vydanie certifikátu):

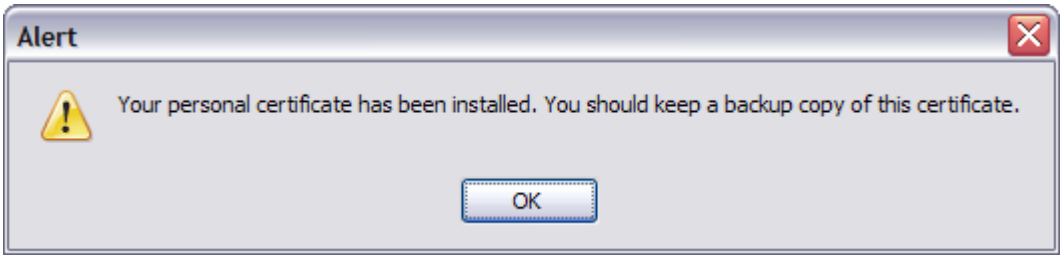
   **https://www.disig.sk/cgi-bin/get_cert?serial=$eSerial**

   (**$eSerial** je 7 miestne sériové číslo Vášho certifikátu)

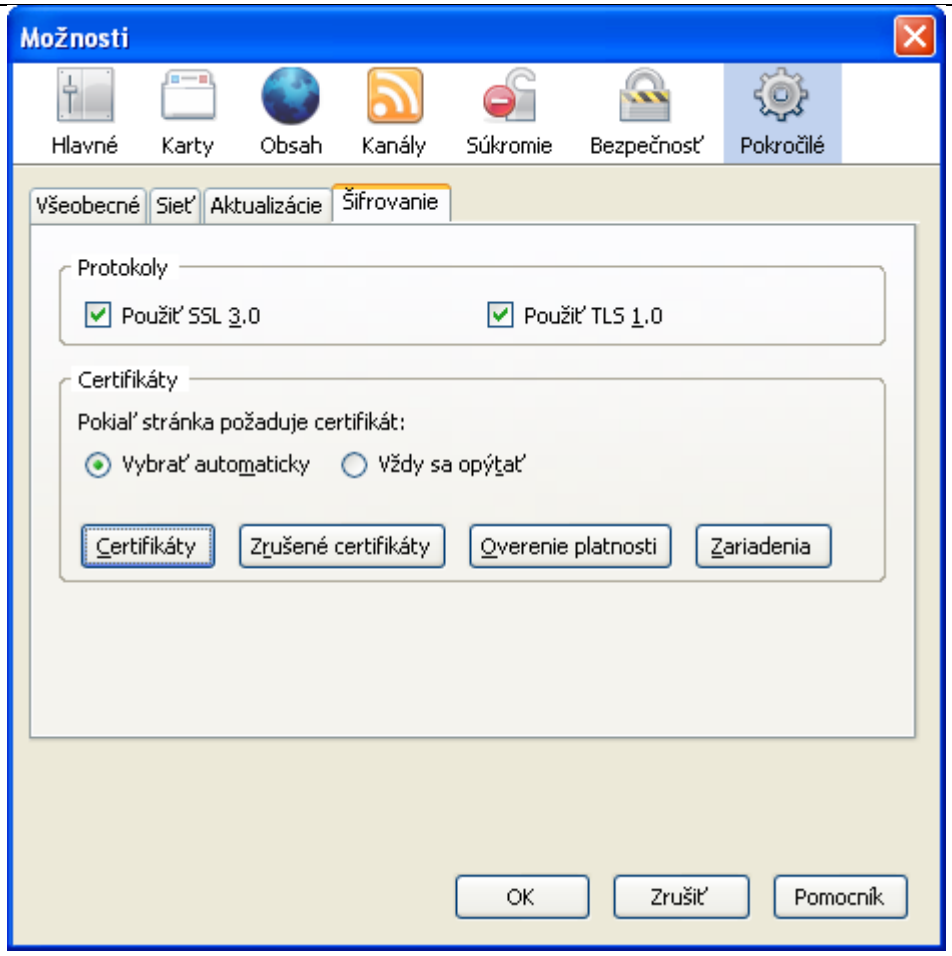
2. V prípade, že sa objaví výzva na zadanie hlavného hesla, zadajte heslo a pokračujte kliknutím na "OK".
   **Poznámka:** Hlavné heslo je heslo, ktorým je chránený prístup k súkromným kľúčom daného užívateľa. Toto heslo, pokiaľ je aktivované, si zvolil samotný užívateľ už predtým v nastaveniach príslušného programu Mozilla:



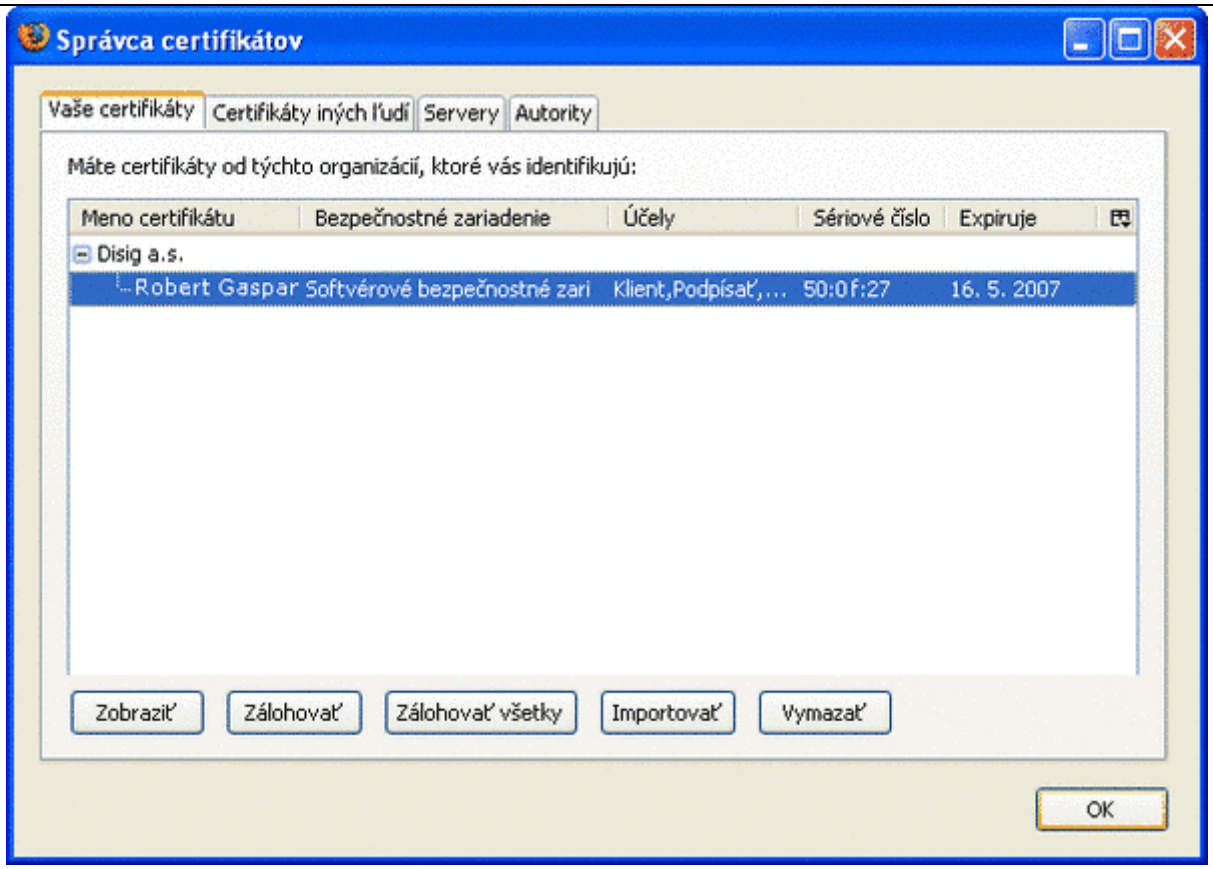

3. Podľa použitej verzie prehliadača sa Vám zobrazí okno s oznamom o úspešnej inštalácii osobného certifikátu. U starších verzii sa toto okno nemusí zobraziť. Zároveň ste upozornený aj na potrebu vytvorenia zálohy práve nainštalovaného certifikátu (pozrite kapitolu "**Zálohovanie a obnova osobného certifikátu**"):




4. Na overenie, či inštalácia skutočne prebehla kliknite na "**Nástroje**" v hlavnom menu príslušného programu Mozilla a zvoľte "**Možnosti**". Potom zvoľte "**Pokročilé**" (prípadne "**Rozšírené**") (pre staršie verzie programov "**Ostatné**"), ďalej zvoľte záložku "**Šifrovanie**" (prípadne "**Zabezpečenie**") a nakoniec tlačidlo "**Certifikáty**" (alebo tlačidlo "**Správa certifikátov**"):




5. Otvorí sa okno "**Správca certifikátov**". Po úspešnej inštalácii musí byť certifikát uložený v okne "**Správca certifikátov**" v záložke "**Vaše certifikáty** (prípadne **Osobné certifikáty**)":




**Poznámka**: V prípade, že sa Váš certifikát po inštalácii nenachádza v záložke "**Osobné**", ale je uložený napríklad v záložke "**Certifikáty iných ľudí**", je pravdepodobné, že Váš systém nie je schopný zistiť umiestnenie Vášho privátneho kľúča a tým úspešne nainštalovať certifikát. Skôr ako sa pokúsite o opakovanú inštaláciu, kontaktujte podporu CA Disig.

6. V prípade, že sa Vám nepodarilo nainštalovať Váš osobný certifikát prostredníctvom zaslanej linky, je ho možné nainštalovať po jeho vyhľadaní na stránkach Disig-u. Kliknite na tento odkaz a v otvorenom okne vpíšte do položky "**CN**" bez diakritiky celé Vaše meno, (je uvedené v bode 4. protokolu o prevzatí certifikátu). Identifikujte certifikát, ktorý hodláte nainštalovať (spravidla prvý v poradí) a následne v stĺpčeku "**Inštalácia**" kliknite na hrubo vytlačený nápis "**Mozilla**". Ďalej postupujte ako je popísané v bodoch 2 až 5.

## Druhý krok - Inštalácia certifikátu certifikačnej autority CA Disig

1. Kliknite na https://eidas.disig.sk/sk/cacert/.

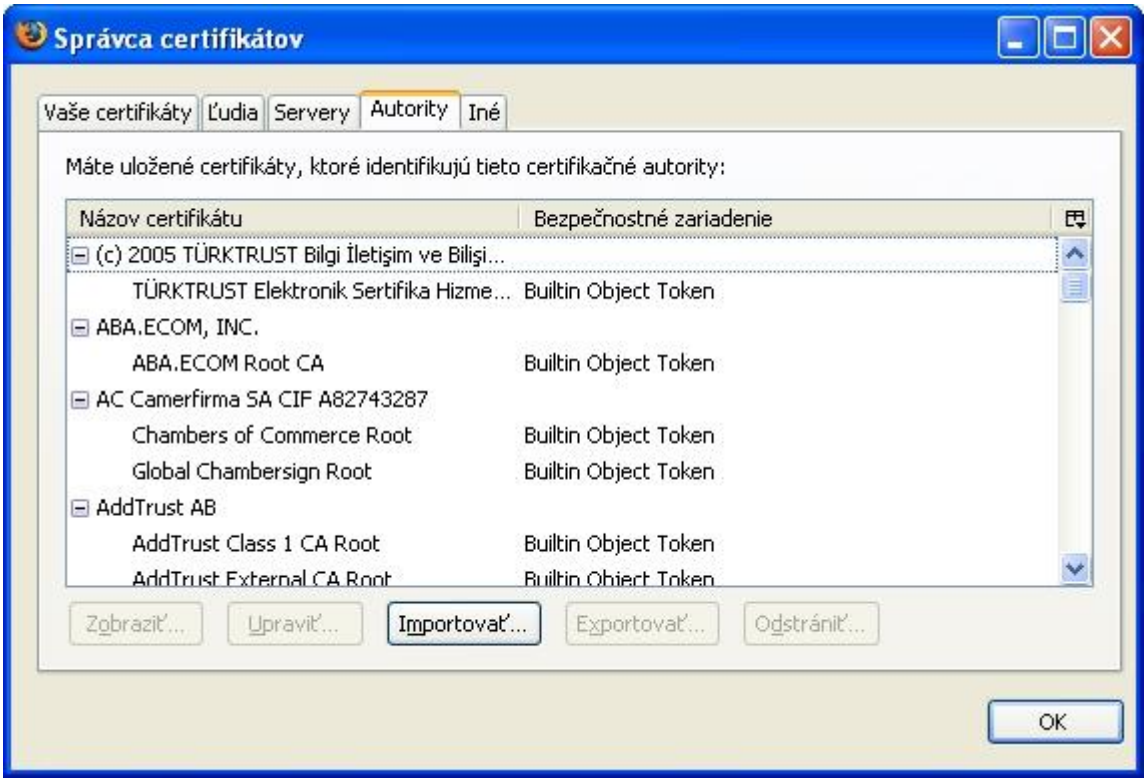
2. Po zobrazení stránky s aktuálnym certifikátom CA Disig kliknite na text "**DER**" v časti Formáty na stiahnutie:

| Certifikačná autorita CA Disig | | | |
|---|---|---|---|
| Sériové číslo: | 01 | | |
| Platný od: | 22.marca 2006 1:39:34 GMT | | |
| Platný do: | 22.marca 2016 1:39:34 GMT | | |
| SHA 1 (DER): | 2a c8 d5 8b 57 ce bf 2f 49 af f2 fc 76 8f 51 14 62 90 7a 41 | | |
| **Formáty na stiahnutie:** | DER | PEM | TXT |

V prípade potreby inštalácie tohto certifikátu CA Disig do prehliadača typu Netscape (Mozilla Firefox ap.) resp. MSIE verzie 4.0 a nižšej, prípadne iného softvéru **kliknite SEM.**

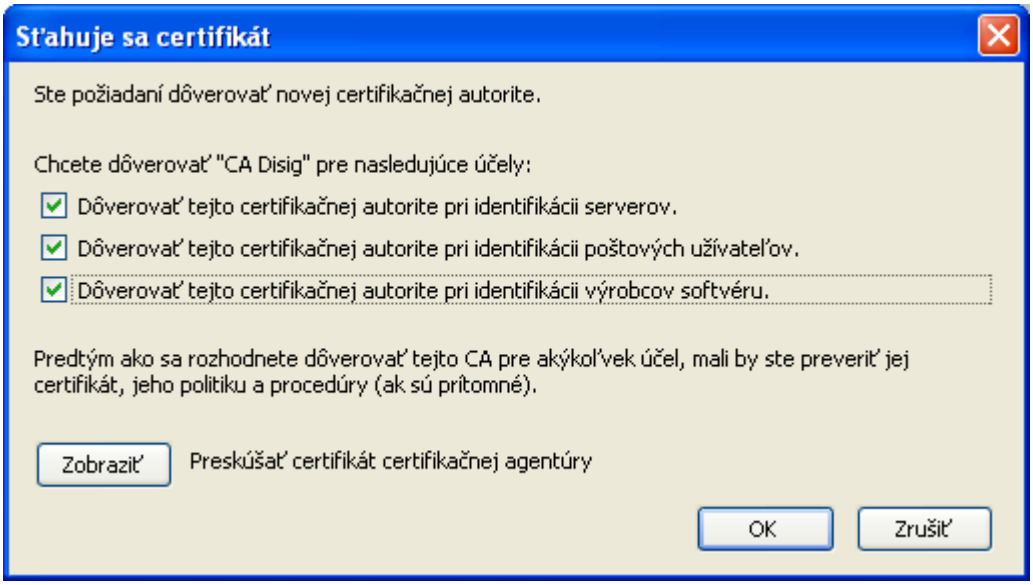
3. Po kliknutí na text "**DER**" sa Vám otvorí nasledovné okno. Zvoľte možnosť "**Uložiť súbor**" a potvrďte ju stlačením tlačidla "**OK**". Ďalej uložte súbor do Vami určeného (prípadne preddefinovaného) priečinku.


4. Kliknite na "**Nástroje**" v hlavnom menu príslušného programu Mozilla a zvoľte "**Možnosti**". Potom zvoľte "**Pokročilé**" (prípadne "**Rozšírené**") (pre staršie verzie programov "**Ostatné**"), ďalej zvoľte záložku "**Šifrovanie**" (prípadne "**Zabezpečenie**") a nakoniec tlačidlo "**Certifikáty**" (alebo tlačidlo "**Správa certifikátov**"). V otvorenom okne "**Správcu certifikátov**" vyberte záložku "**Autority**":

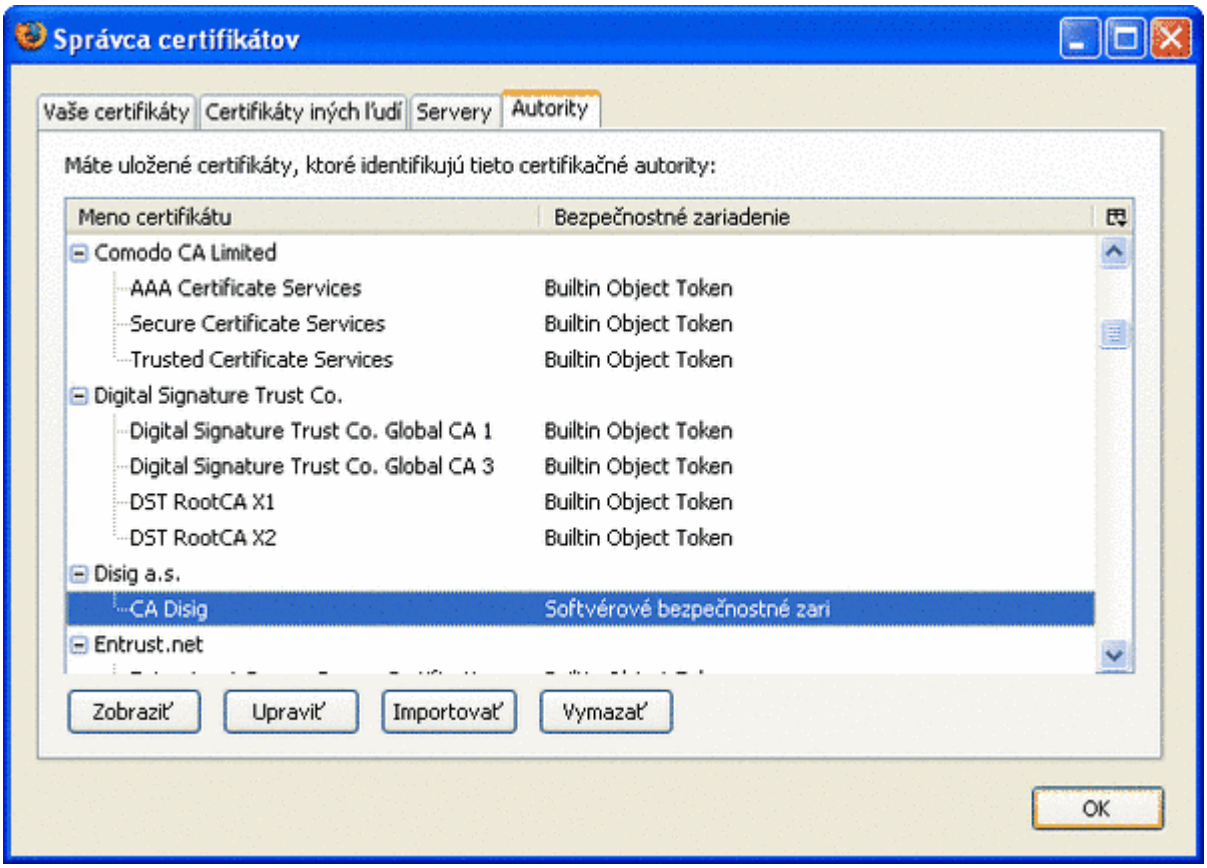



5. Kliknite na "**Importovať...**", vyhľadajte a otvorte súbor, ktorý ste uložili bode 3.

6. Otvorí sa Vám okno "**Sťahuje sa certifikát**", kde je potrebné zaškrtnúť všetky možnosti a pokračovať kliknutím na "**OK**":




7. Po úspešnej inštalácii musí byť certifikát certifikačnej autority CA Disig umiestnený v záložke "**Autority**" v okne "**Správca certifikátov**":




8. Týmto je ukončená inštalácia certifikátu certifikačnej autority CA Disig.

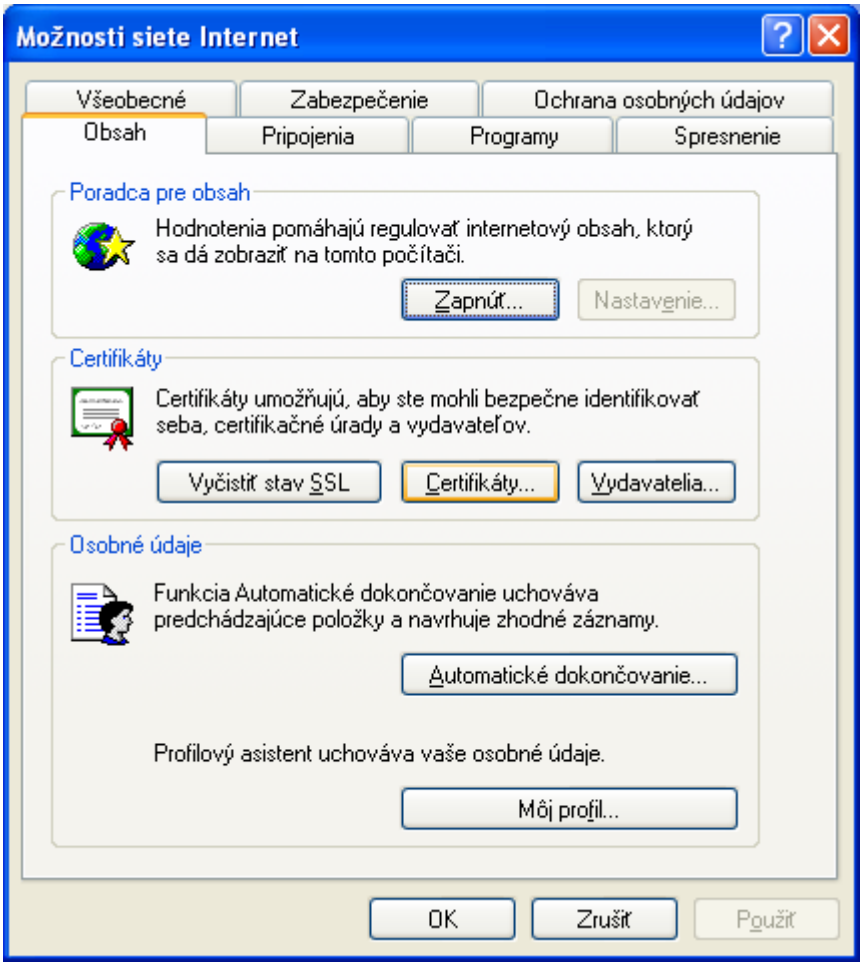
# 3 ZÁLOHOVANIE A OBNOVA OSOBNÉHO CERTIFIKÁTU

## 3.1 Zálohovanie (export) osobného certifikátu zo systémového úložiska certifikátov MS Windows

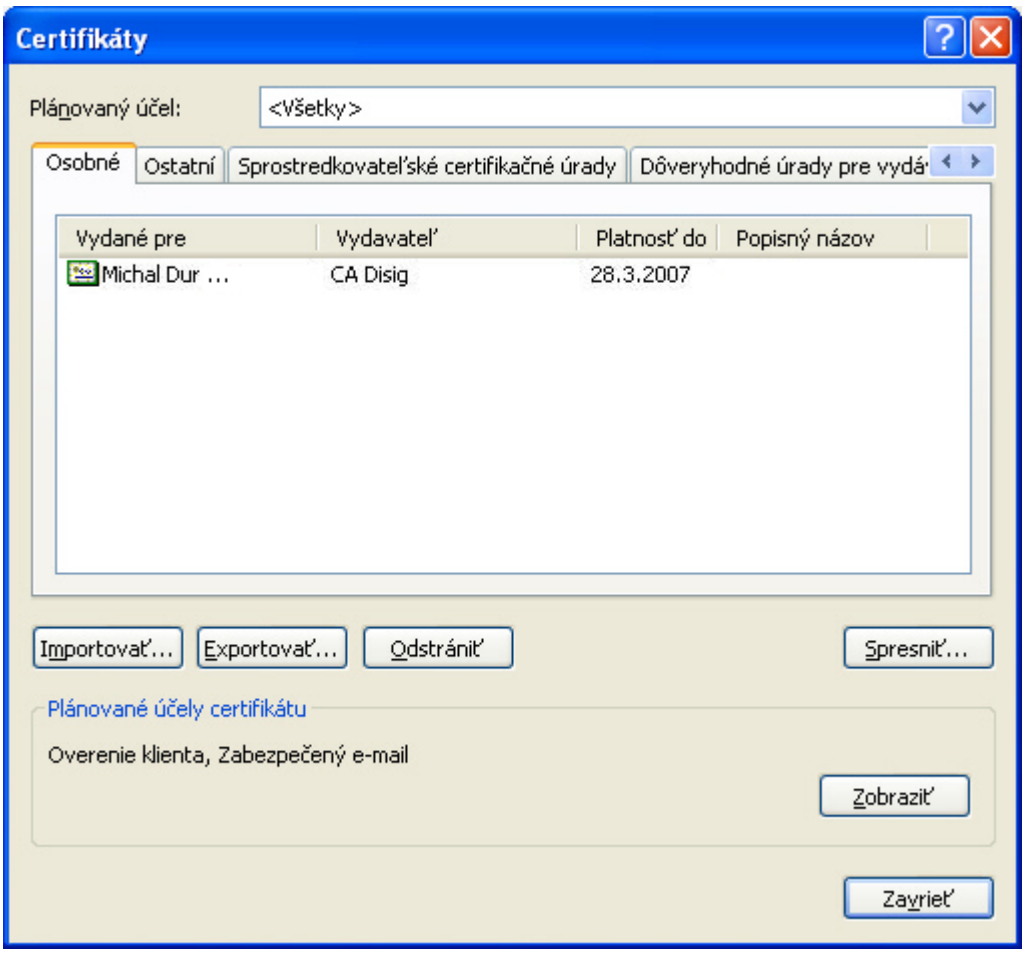
Zálohu užívateľského certifikátu zo systémového úložiska certifikátov MS Windows vykonáte podľa nasledovného postupu:

1. Otvorte program Internet Explorer. V hlavnom menu programu kliknite na "**Nástroje**". Zobrazí sa roletové menu. V ňom kliknite na "**Možnosti siete Internet...**".

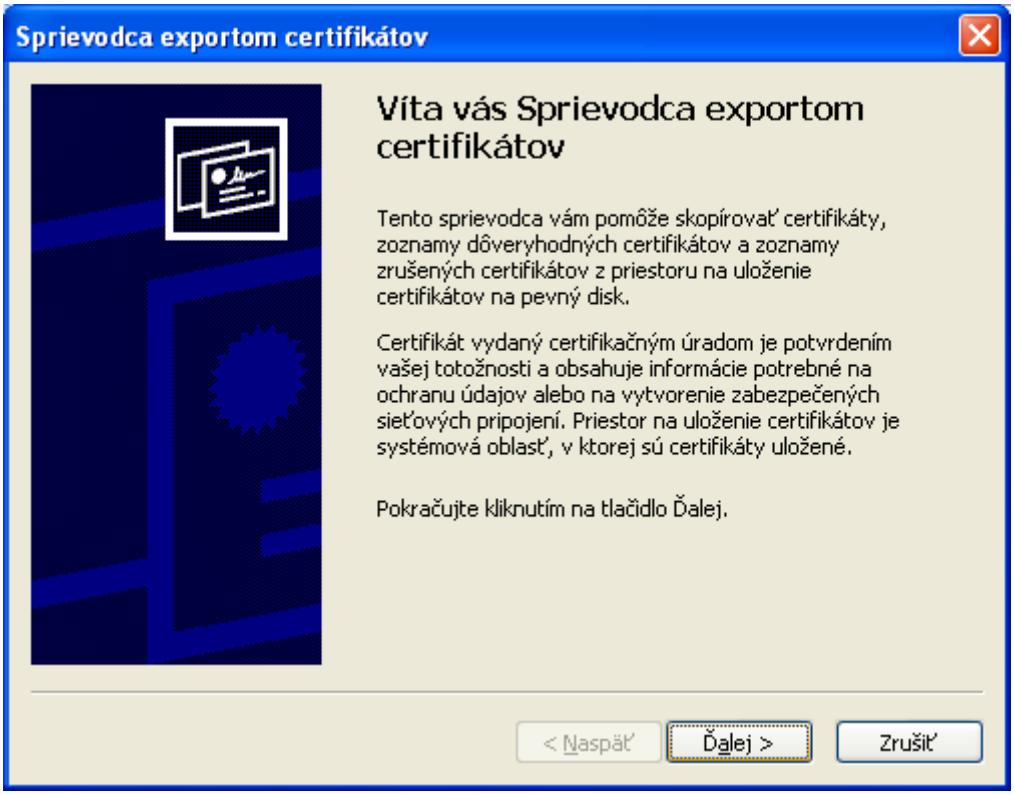
2. V zobrazenom okne vyberte záložku "**Obsah**" a potom kliknite na tlačidlo "**Certifikáty...**":



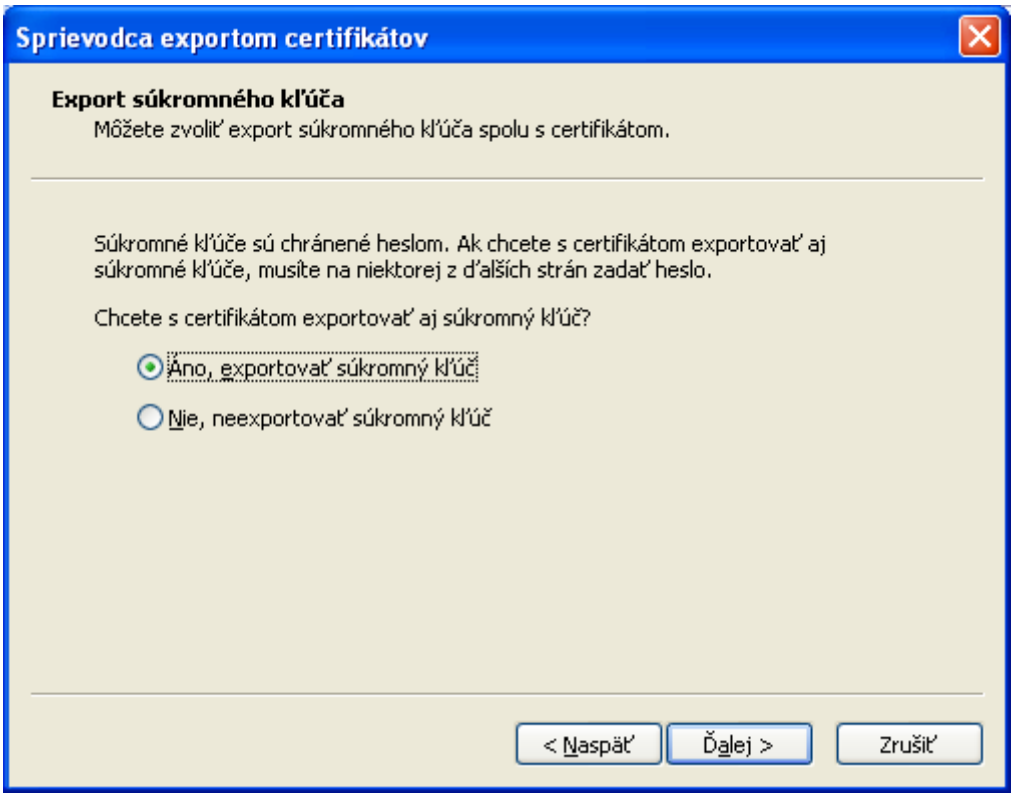

3. Zobrazí sa okno s certifikátmi. Overte, či je zobrazená záložka "**Osobné**". Zvoľte certifikát, ktorý chcete zálohovať. Stlačte tlačidlo "**Exportovať...**":



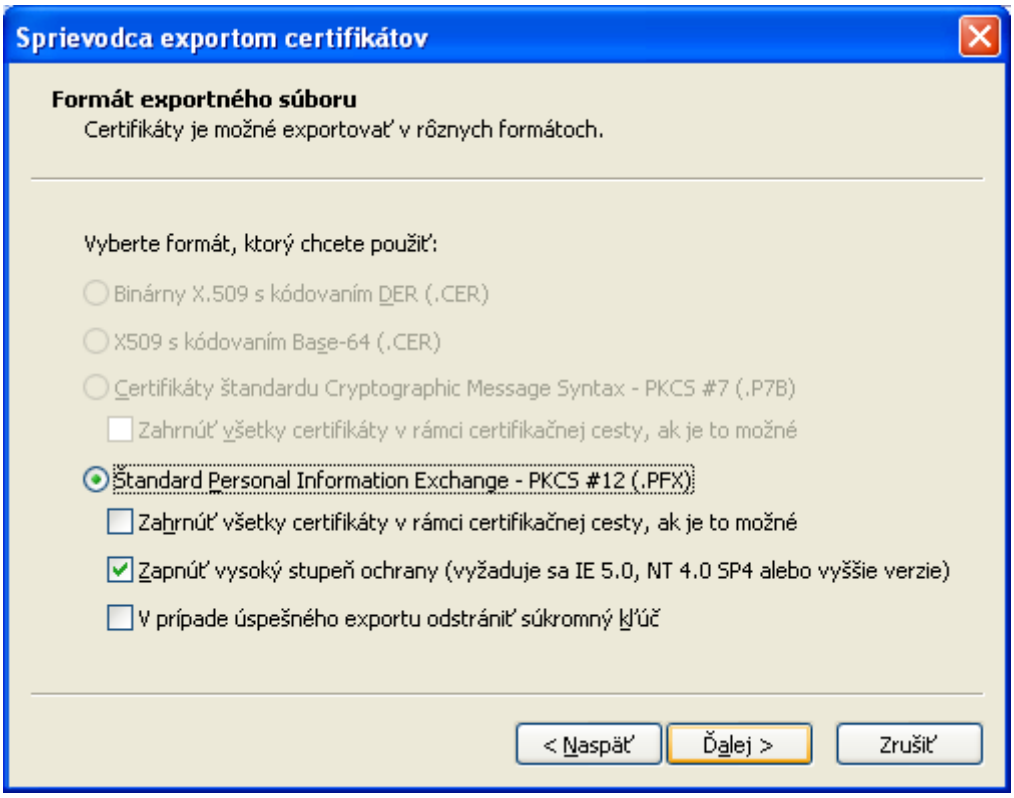

4. Pokračujte voľbou "**Ďalej** >":



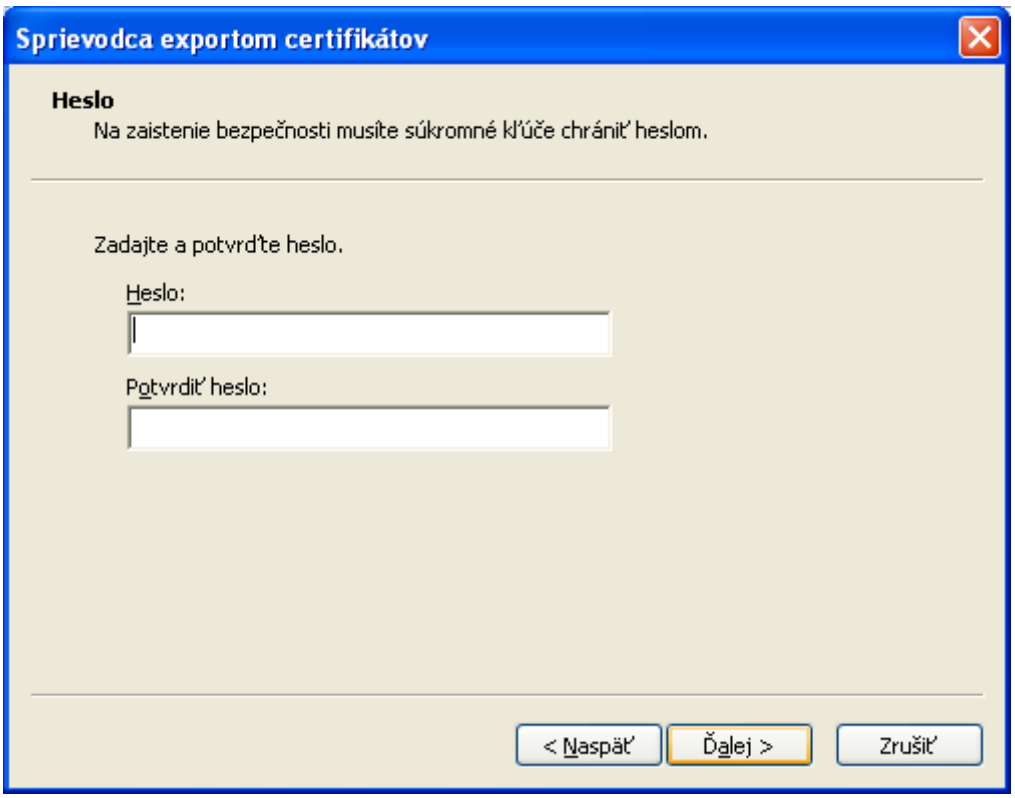
5. Zvoľte položku "**Áno, exportovať privátny kľúč**". Pokračujte voľbou "**Ďalej >**":



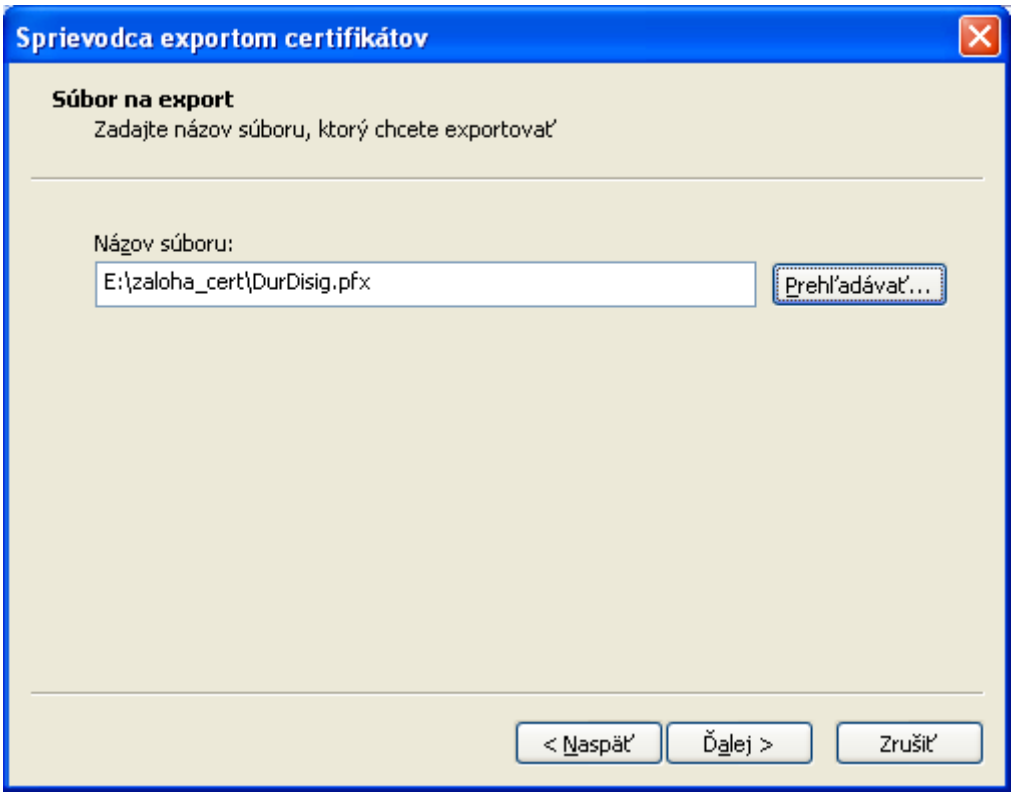

6. Zvoľte nastavenia podľa obrázku a pokračujte voľbou "**Ďalej >**":



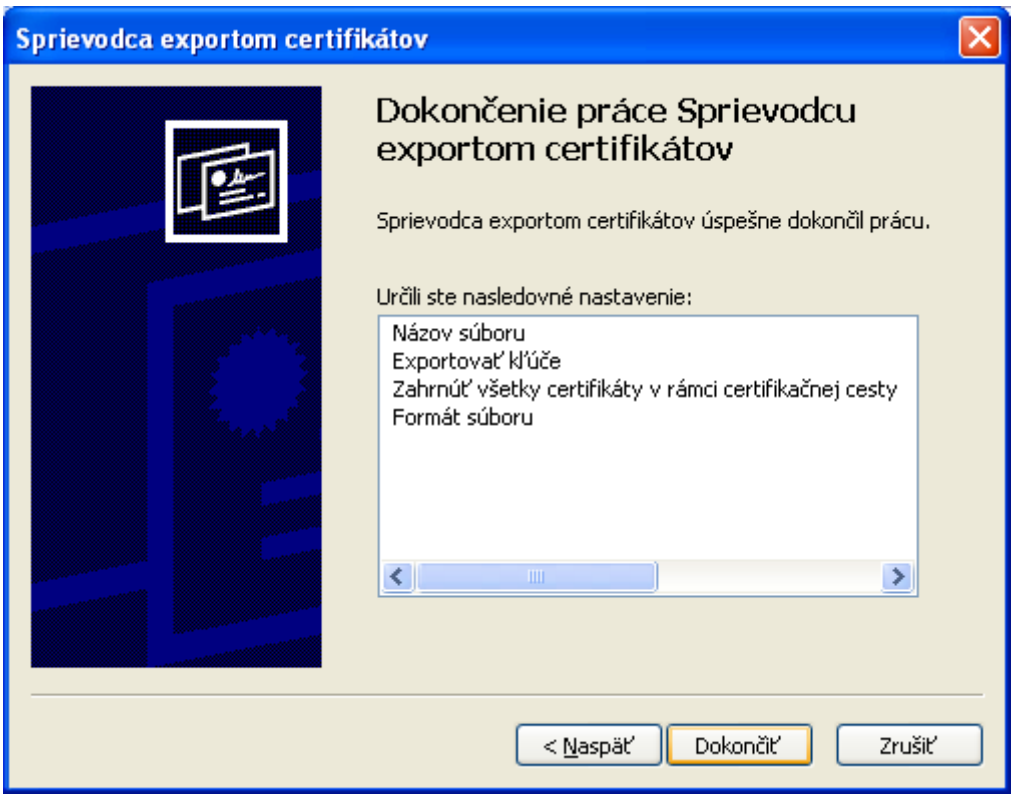

7. Napíšte heslo, ktorým bude chránený Váš privátny kľúč do poľa "**Heslo**" a zopakujte ho v poli "**Potvrdiť heslo**". Pokračujte voľbou "**Ďalej >**":



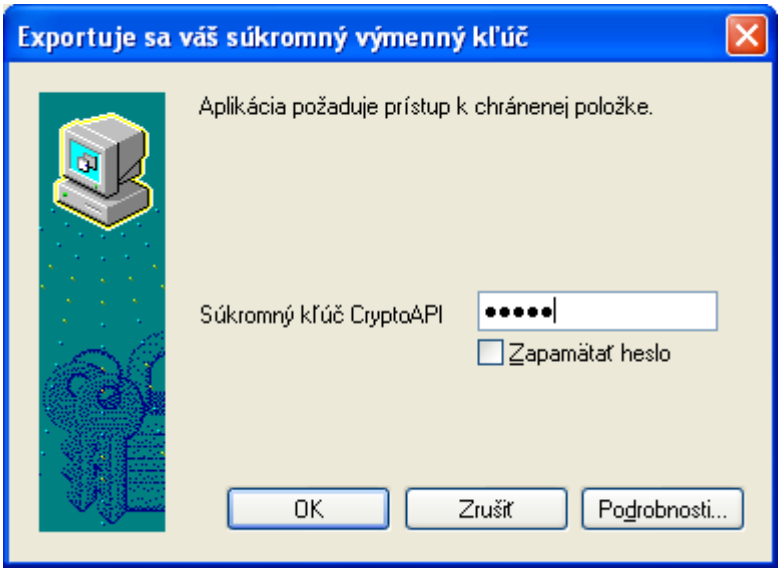

8. Napíšte meno, pod akým sa má súbor uložiť a cestu k nemu alebo kliknite na tlačidlo "**Prehľadávať...**", vyberte adresár, do ktorého sa má súbor uložiť a napíšte meno súboru. Pokračujte voľbou "**Ďalej** >":




9. Kliknite na tlačidlo "**Dokončiť**":




10. Ak je privátny kľúč chránený heslom, otvorí sa okno, kde ho môžete zadať. Pokračujte voľbou "**OK**":

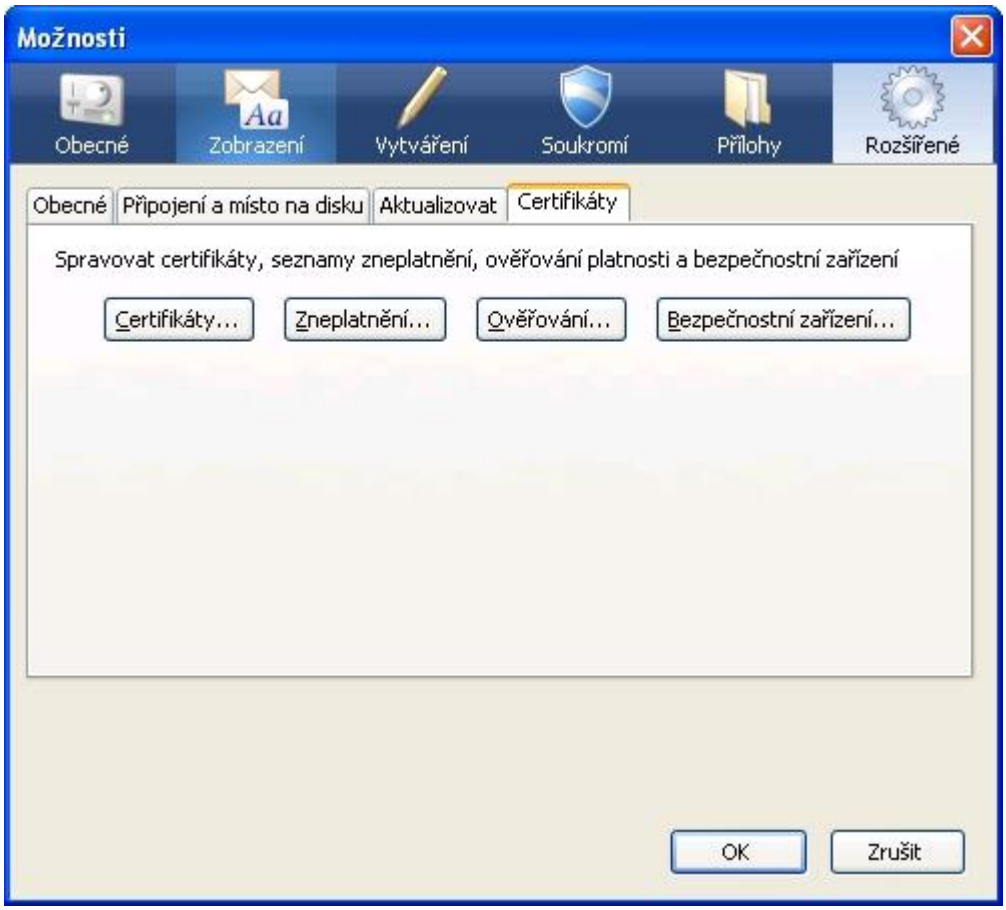



11. Zobrazí sa okno oznamujúce, že export certifikátu bol úspešný. Export ukončite voľbou "**OK**":

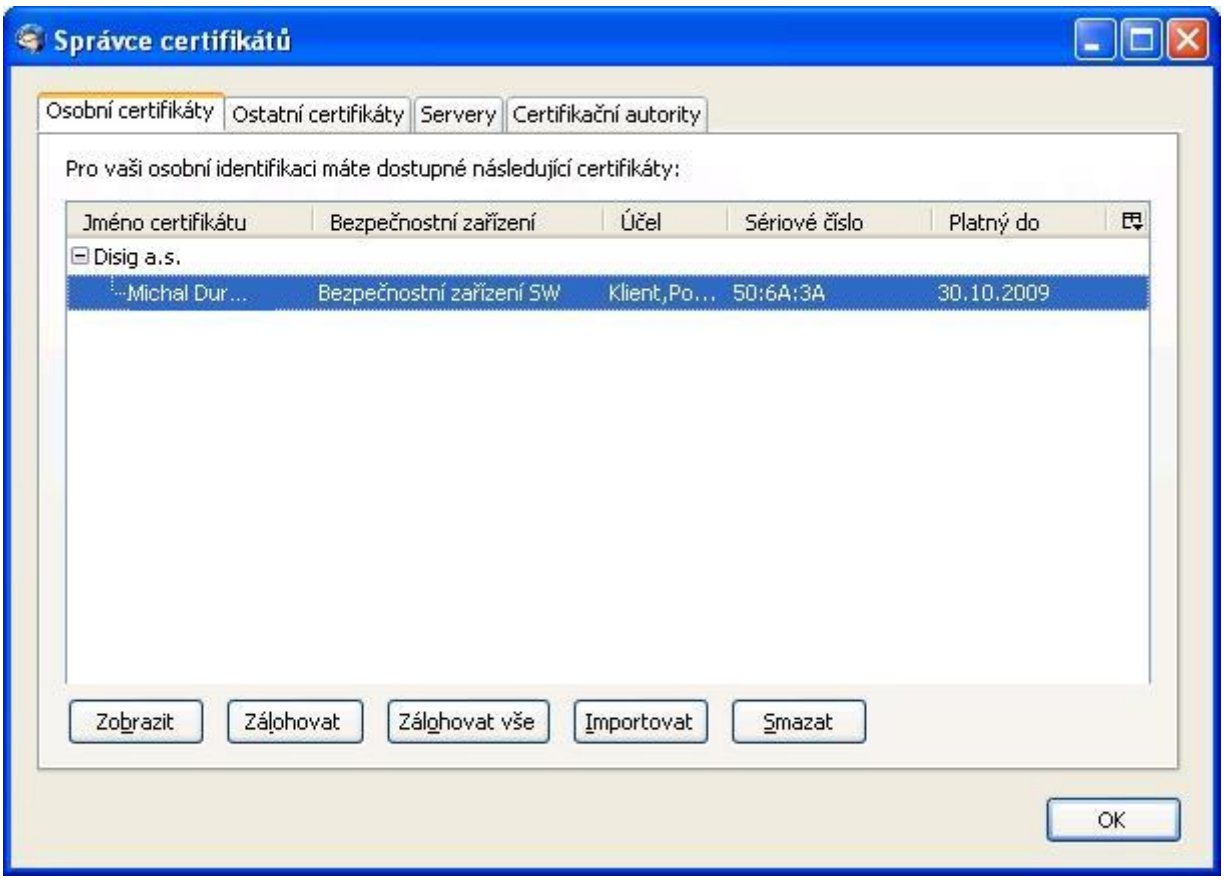
## 3.2 Zálohovanie (export) osobného certifikátu zo systémového úložiska certifikátov Mozilla

Zálohu užívateľského certifikátu zo systémového úložiska certifikátov Mozilla vykonáte podľa nasledovného postupu:

1. Otvorte program Mozilla Thunderbird alebo Mozilla Firefox. V hlavnom menu programu kliknite na "**Nástroje**". Zobrazí sa roletové menu. V ňom kliknite na "**Možnosti...** ". Potom zvoľte "**Rozšírené**" (prípadne "**Pokročilé**") (pre staršie verzie programov "**Ostatné**") a ďalej zvoľte záložku "**Certifikáty**" (prípadne "**Šifrovanie** "):

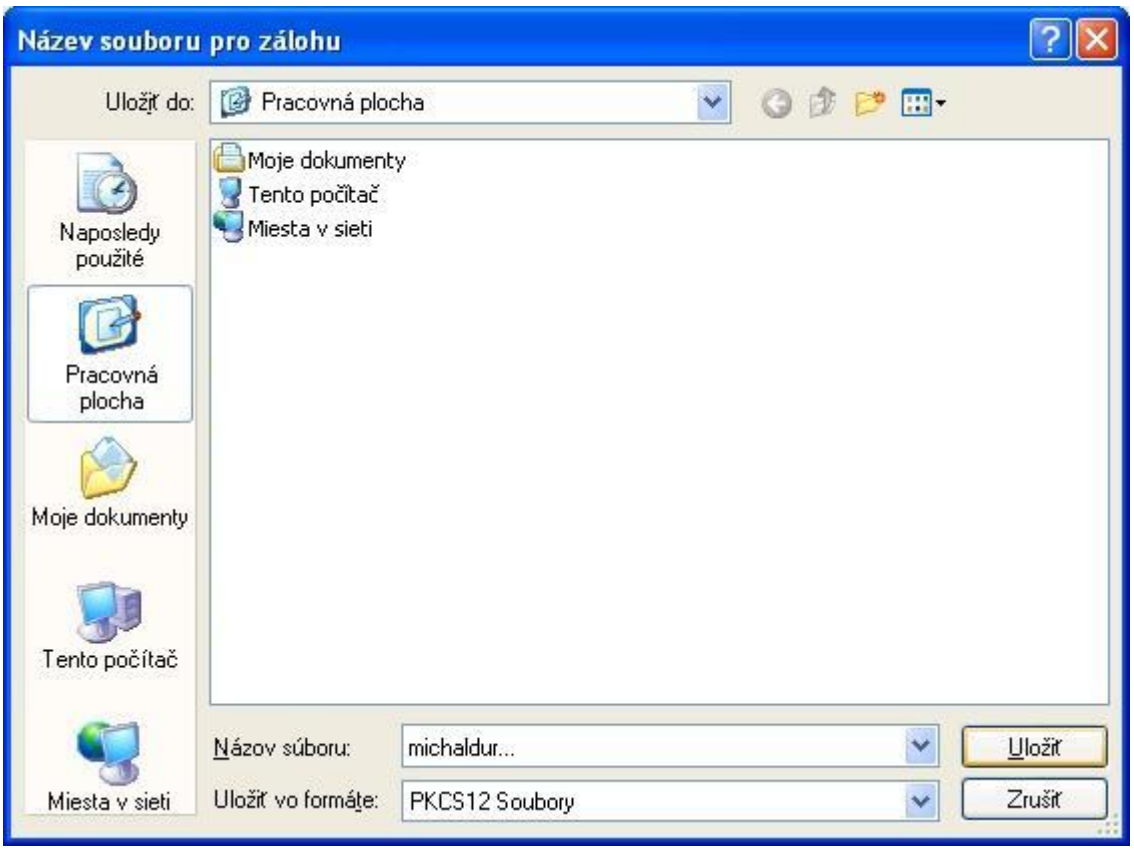



2. Stlačte tlačidlo "**Certifikáty**" (prípadne "**Správa certifikátov**"). Týmto sa otvorí okno "**Správca certifikátov**". Vyberte záložku "**Osobné certifikáty**":




3. Kliknite na vaše meno a potom na tlačidlo "**Zálohovať**".

4. Prostredníctvom dialógového okna určte názov súbor s vašim osobným certifikátom a jeho umiestnenie vo Vašom počítači. Vaše nastavenie potvrďte stlačením tlačidla "**Uložiť**":




5. Otvorí sa okno, kde musíte hlavné heslo, ktorým sú v programe Mozilla chránené Vaše osobné údaje. Pokračujte voľbou "**OK**":

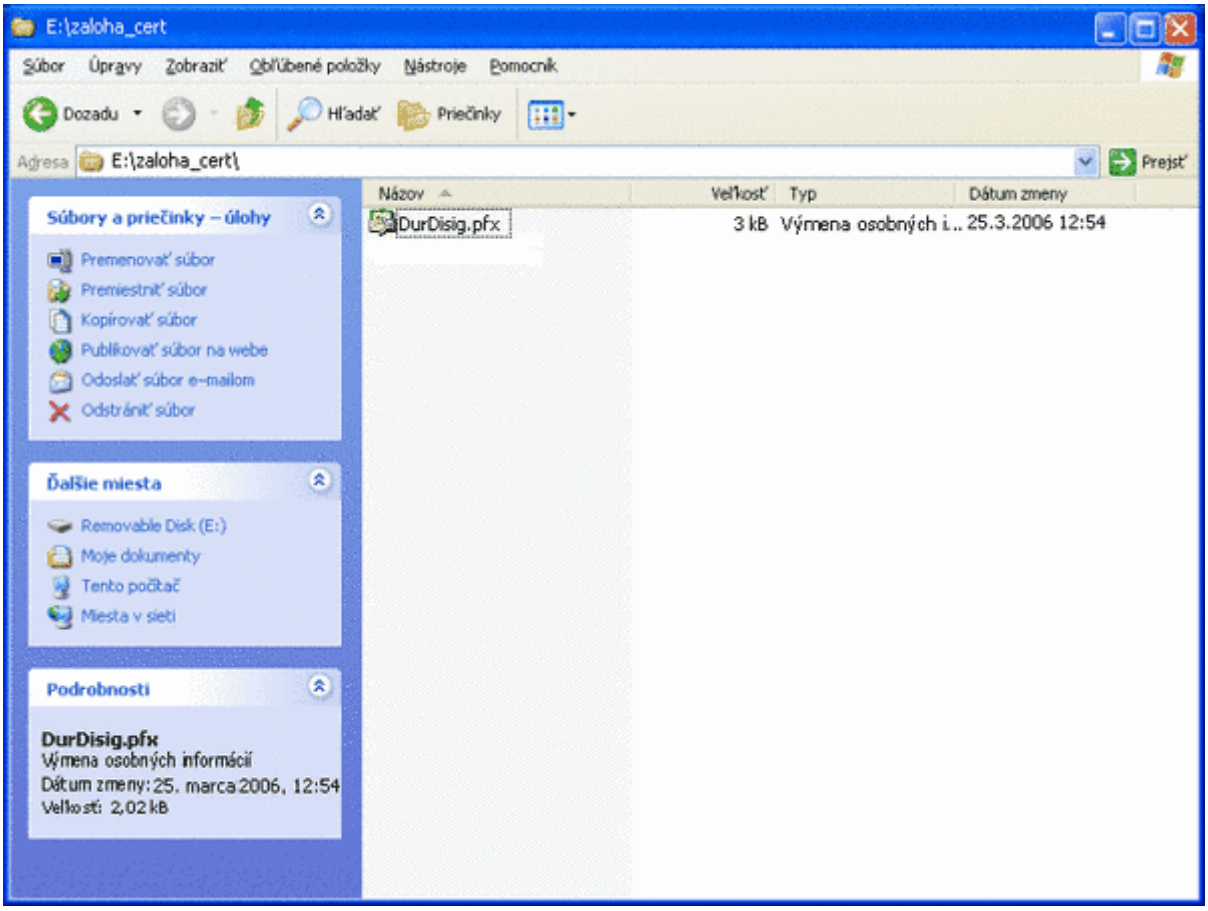

6. Napíšte heslo, ktorým bude chránená záloha Vášho osobného certifikátu do poľa "**Heslo zálohy certifikátu**" a zopakujte ho v poli "**Heslo zálohy certifikátu (znovu)**". Pokračujte voľbou "**OK**":


7. Zobrazí sa okno oznamujúce, že export certifikátu bol úspešný. Export ukončíte voľbou "**OK**":

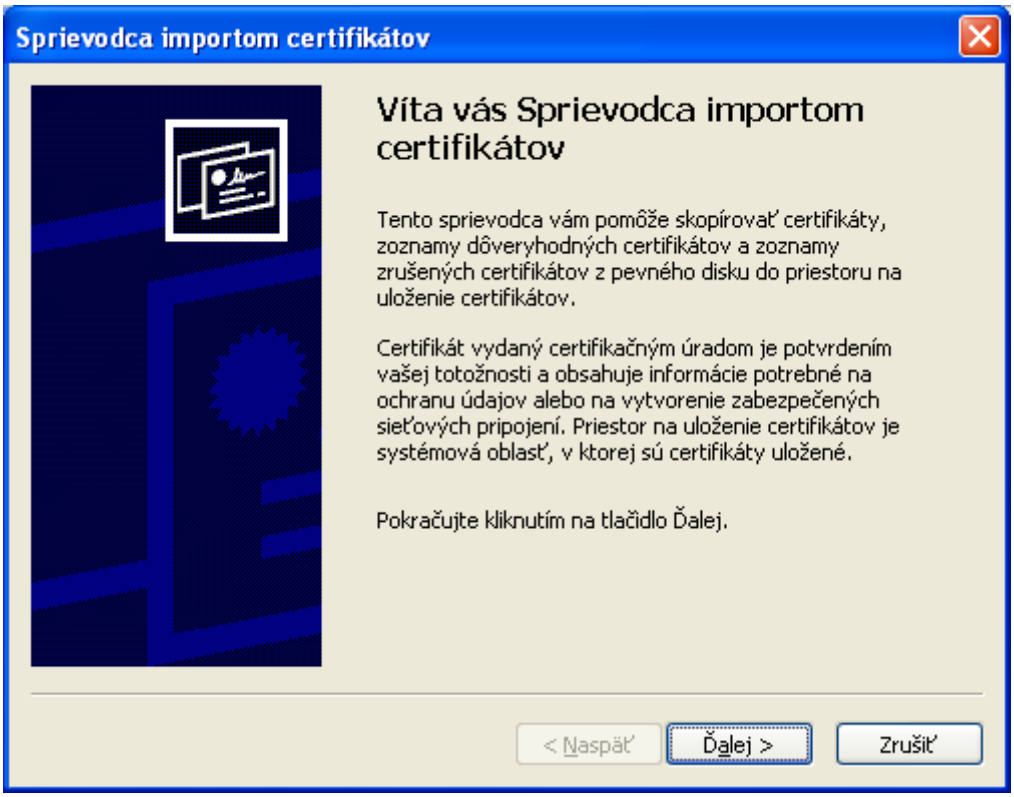

## 3.3 Obnova (import) osobného certifikátu do systémového úložiska certifikátov MS Windows

Obnovu užívateľského certifikátu do systémového úložiska certifikátov MS Windows vykonáte podľa nasledovného postupu:

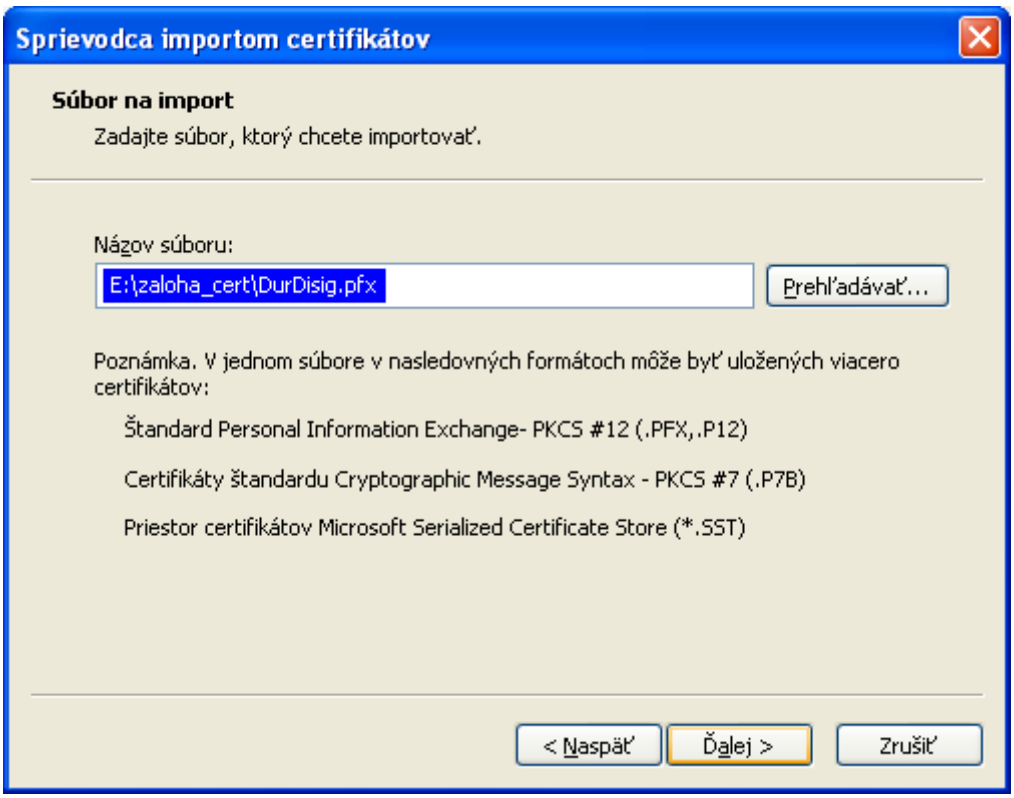
1. Najskôr je potrebné použiť médium s uloženou zálohou (HDD, disketa, USB kľúč) a prejsť do adresára, kde je uložená záloha Vášho certifikátu (napr. E:\zaloha_cert). Potom dvakrát rýchlo kliknite na súbor so zálohou certifikátu, alebo kliknite na súbor so zálohou certifikátu a stlačte **Enter**:



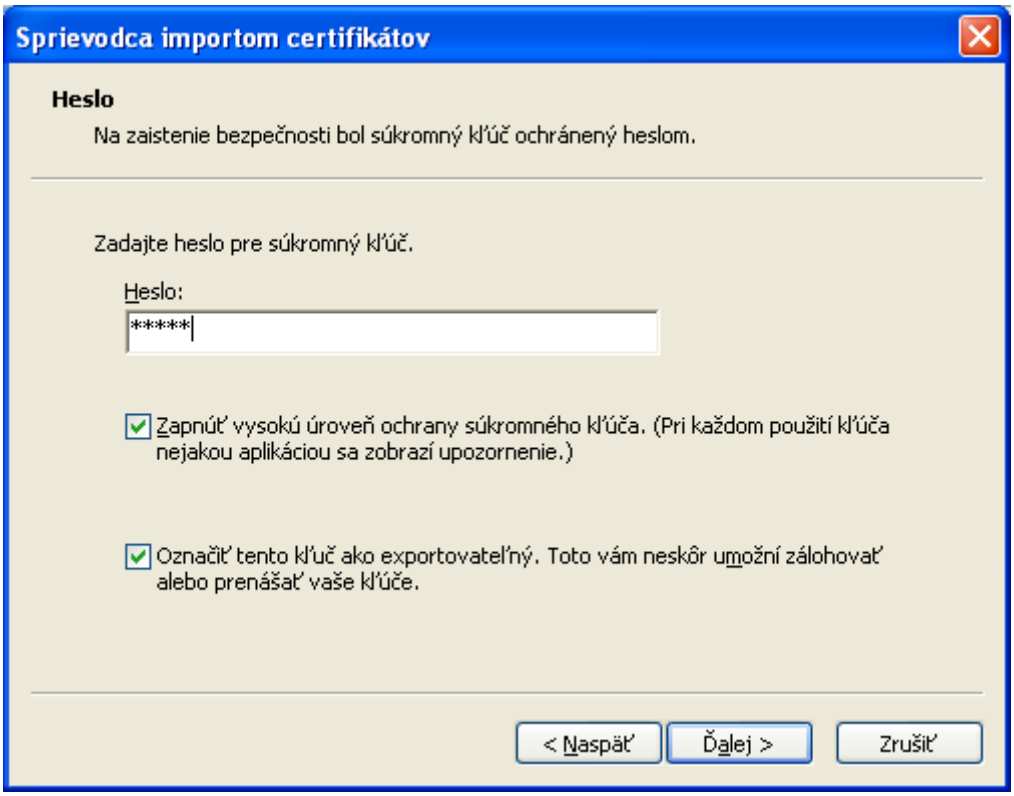

2. Otvorí sa úvodné okno sprievodcu importom certifikátu. Kliknite na tlačidlo "**Ďalej >**":



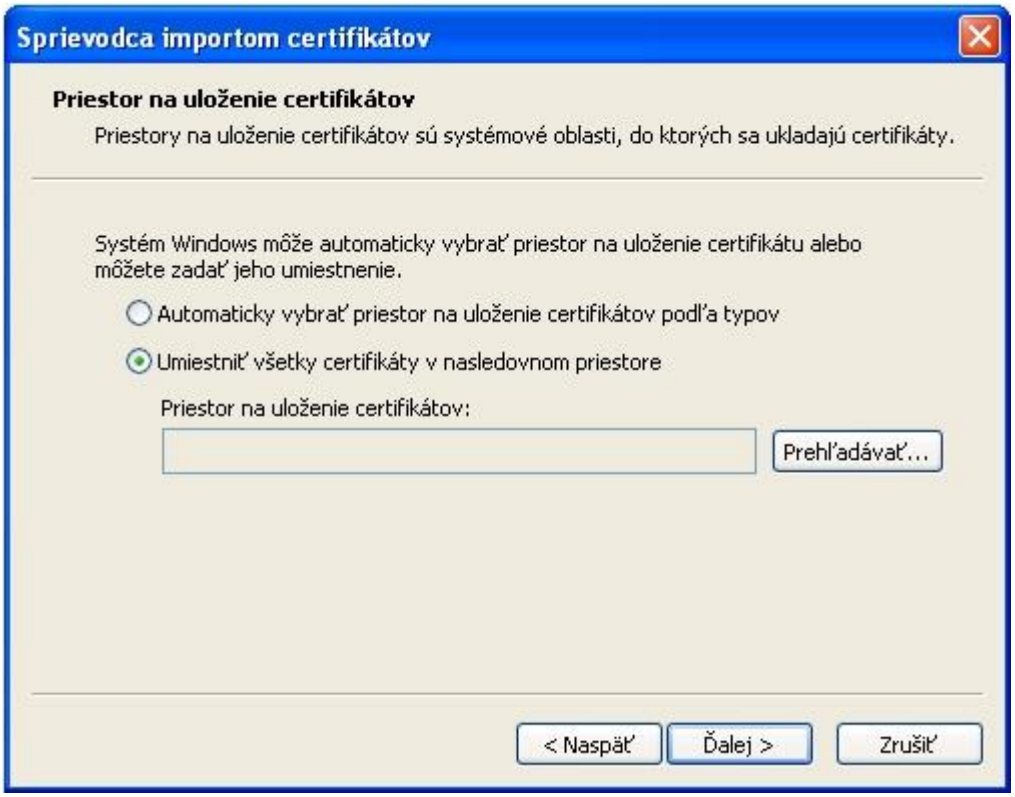

3. Pokračujte voľbou "**Ďalej >**":




4. Napíšte heslo, ktorým je chránený Váš privátny kľúč. Zaškrtnite prvú možnosť ak chcete zvýšenú ochranu privátneho kľúča. Zaškrtnite druhú možnosť ak chcete, aby sa certifikát dal znovu zálohovať (Odporúčame zaškrtnúť obe možnosti). Pokračovať voľbou "**Ďalej >**":



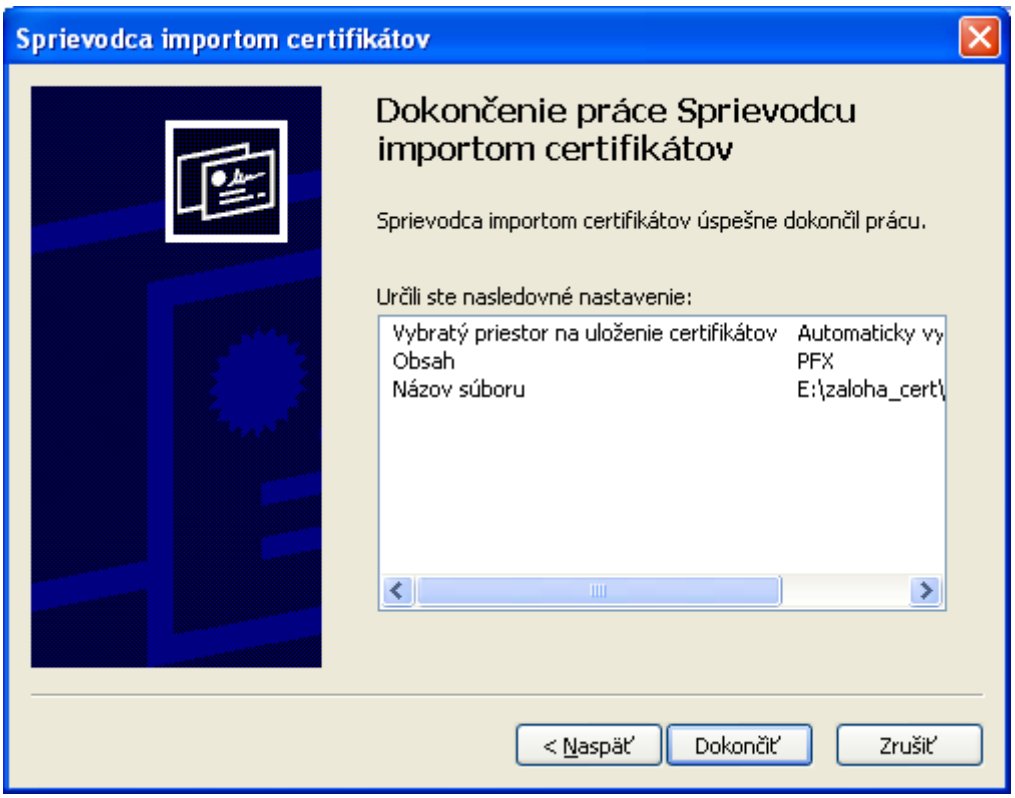

5. Skontrolujte, či je zvolená možnosť "Umiestniť všetky certifikáty v nasledovnom priestore" a stlačte tlačidlo "**Prehľadávať**":




6. Ako priestor na uloženie certifikátov použite "**Osobné**". Svoju voľbu potvrďte stlačením tlačidla "**OK**":

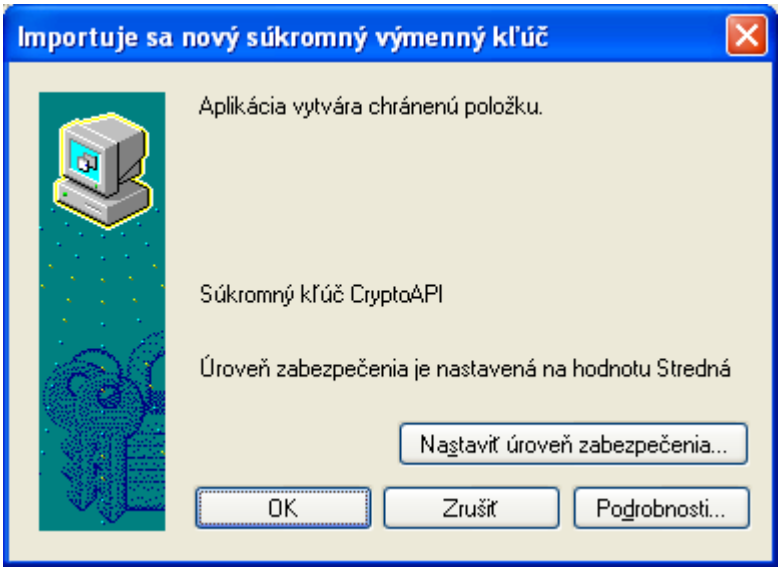

7. Pokračujte voľbou "**Ďalej >**":

8. Importovanie ukončite voľbou "**Dokončiť**":

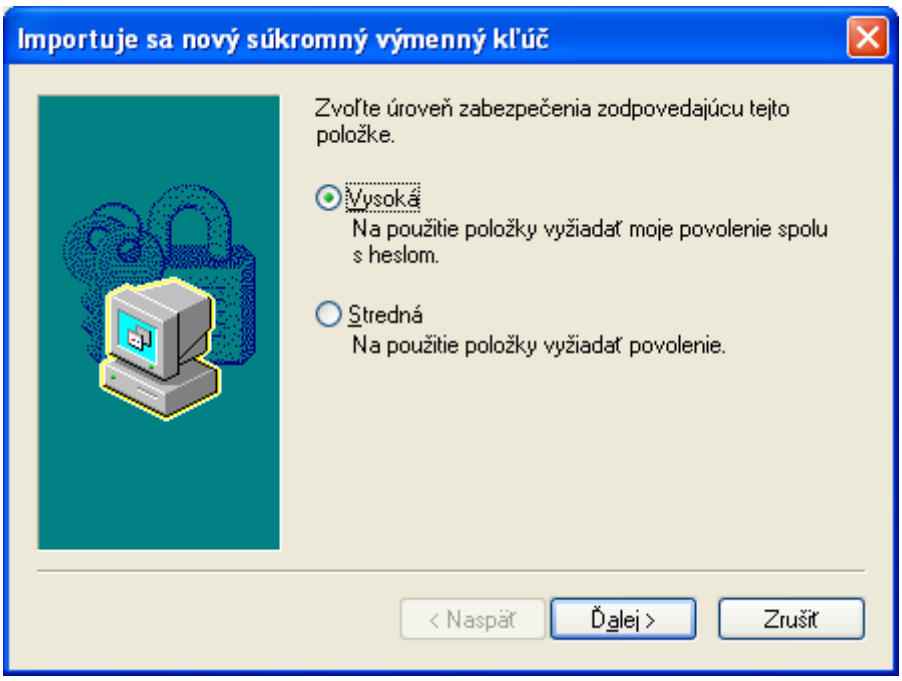



9. Ak ste zvolili zvýšenú ochranu privátneho kľúča, pokračujte bodom 10, inak pokračujte bodom 14.

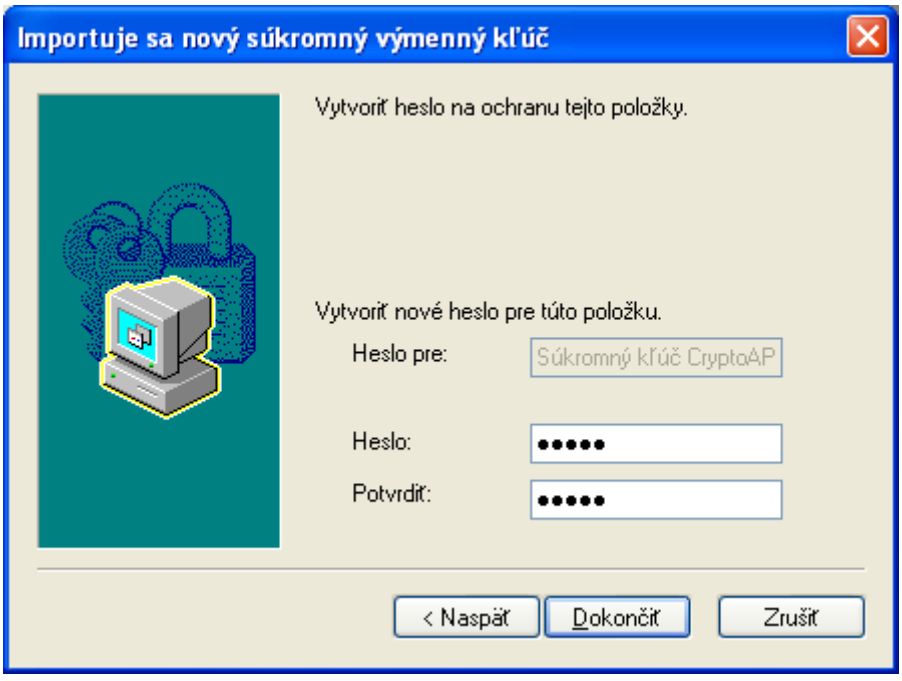
10. Kliknite na tlačidlo "**Nastaviť úroveň zabezpečenia...**":



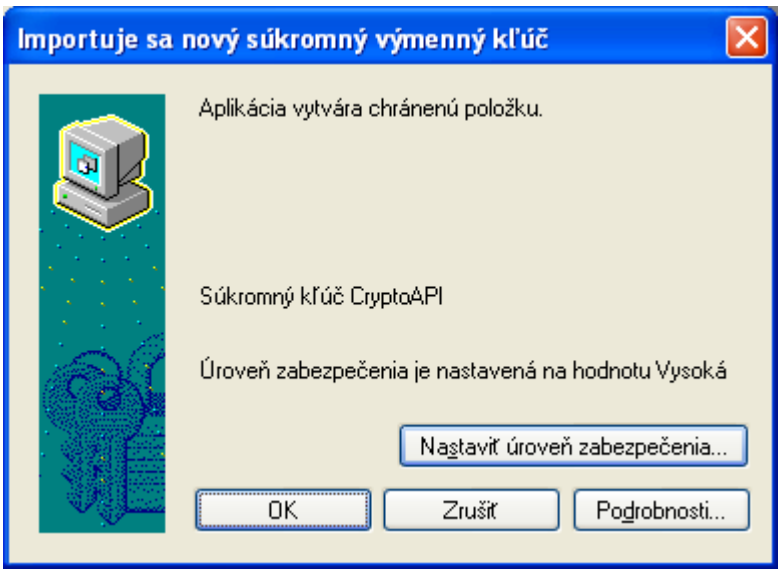

11. Zvoľte "**Vysoká**" a pokračujte voľbou "**Ďalej >**":



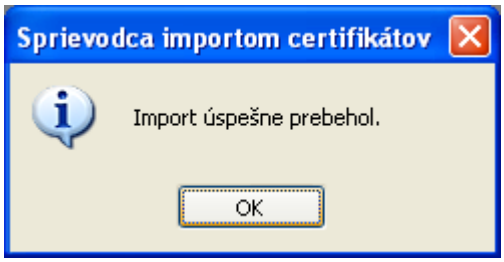

12. Napíšte heslo ktorým chcete chrániť Váš privátny kľúč do poľa "**Heslo**" a zopakujte ho v poli "**Potvrdiť**". Pokračujte voľbou "**Dokončiť**":




13. Pokračujte voľbou "**OK**":



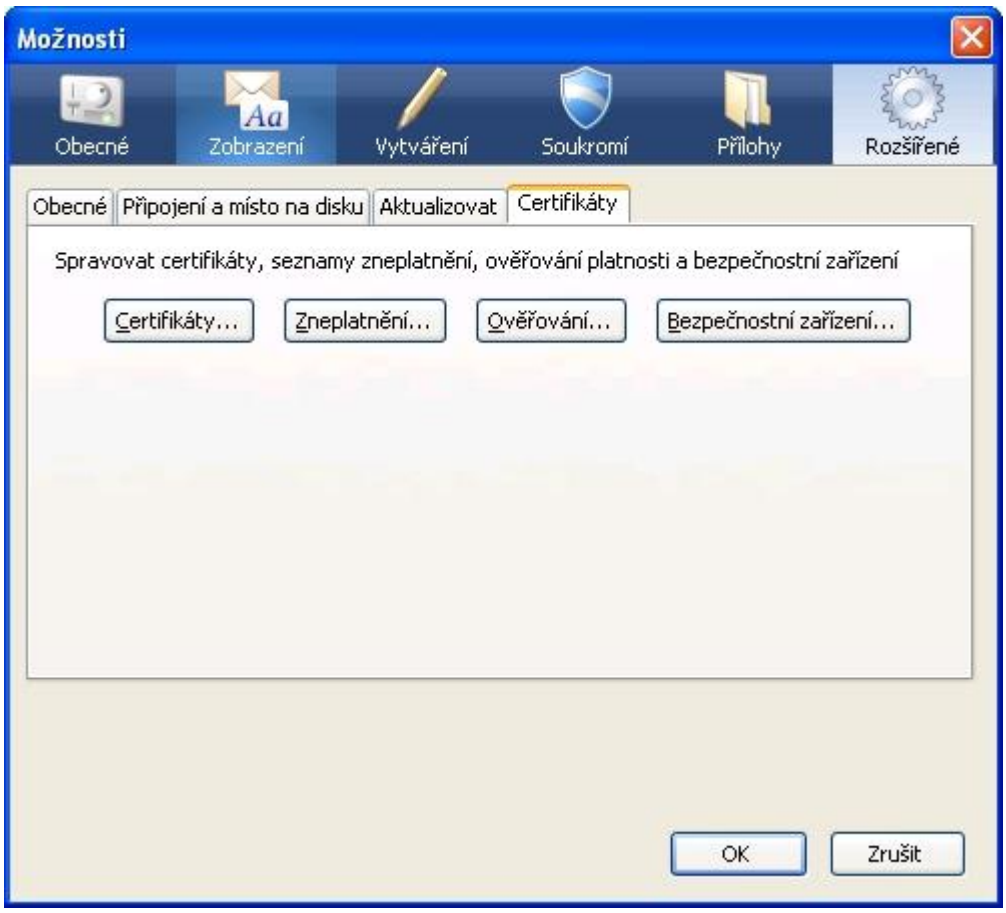

14. Po úspešnom importovaní certifikátu za zobrazí okno oznamujúce, že import certifikátu bol úspešný. Importovanie ukončíte voľbou "**OK**":



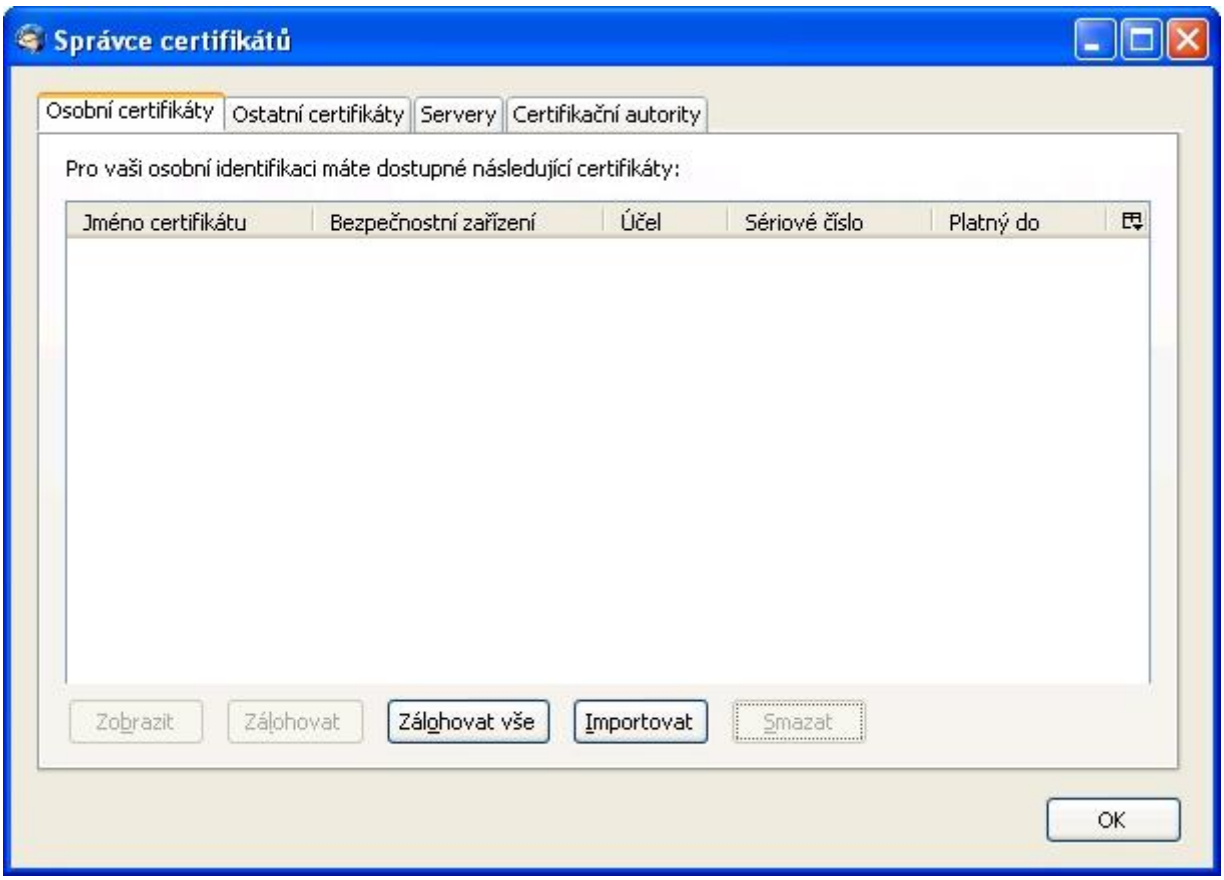

## 3.4 Obnova (import) osobného certifikátu do systémového úložiska certifikátov Mozilla

Obnovu užívateľského certifikátu do systémového úložiska certifikátov Mozilla vykonáte podľa nasledovného postupu:

1. Otvorte program Mozilla Thunderbird alebo Mozilla Firefox. V hlavnom menu kliknite na "**Nástroje**". Zobrazí sa roletové menu. V ňom kliknite na "**Možnosti ...**". Potom zvoľte "**Rozšírené**" (prípadne "**Pokročilé**") (pre staršie verzie programov "**Ostatné**") a ďalej zvoľte záložku "**Certifikáty**" (prípadne "**Šifrovanie**"):

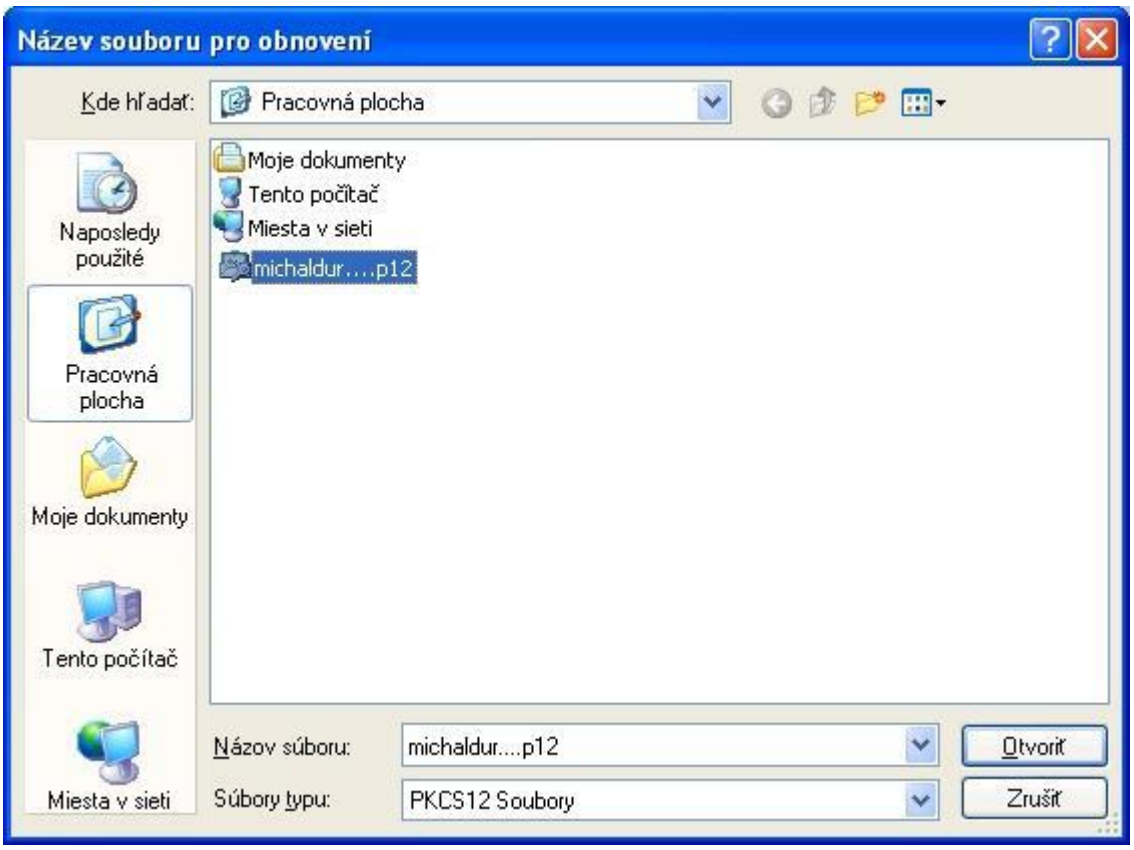



2. Stlačte tlačidlo "**Certifikáty**" (alebo "**Správa certifikátov**"). Týmto sa otvorí okno "**Správca certifikátov**". Vyberte tu záložku "**Osobné certifikáty**":



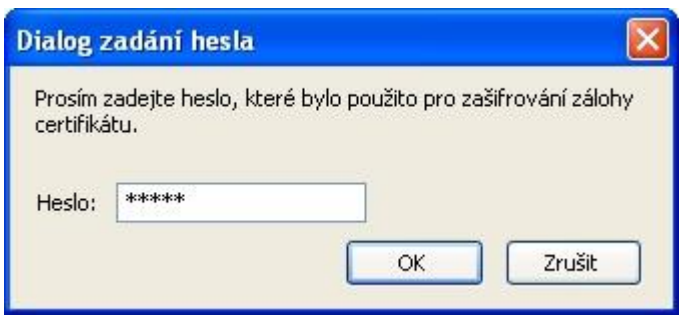

3. Zvoľte tlačidlo "**Importovať**".

4. Otvorí sa dialógové okno, prostredníctvom ktorého nájdite súbor so zálohou Vášho osobného certifikátu. Výber potvrďte tlačidlo "**Otvoriť**":




8. Zadajte hlavné heslo, ktorým sú v programe Mozilla chránené Vaše osobné údaje. Pokračujte voľbou "**OK**":


5. Zadajte heslo, ktorým je chránená záloha Vášho osobného certifikátu. Pokračujte voľbou "**OK**":




6. Po úspešnom importovaní certifikátu za zobrazí okno oznamujúce, že import certifikátu bol úspešný. Importovanie ukončíte voľbou "**OK**":


Výstraha
Váš(e) bezpečnostní certifikát(y) a soukromý klíč(e) byl(y) úspěšně obnoven(y).
OK

# 4 VYUŽÍVANIE OSOBNÉHO CERTIFIKÁTU

Osobný certifikát je možné využiť na podpisovanie e-mailových správ a dokumentov a taktiež na šifrovanú komunikáciu prostredníctvom e-mailov. Na odoslanie šifrovanej správy je však potrebné mať nainštalovaný aj certifikát adresáta.

## 4.1 Import certifikátov iných osôb do systémového úložiska certifikátov MS Windows

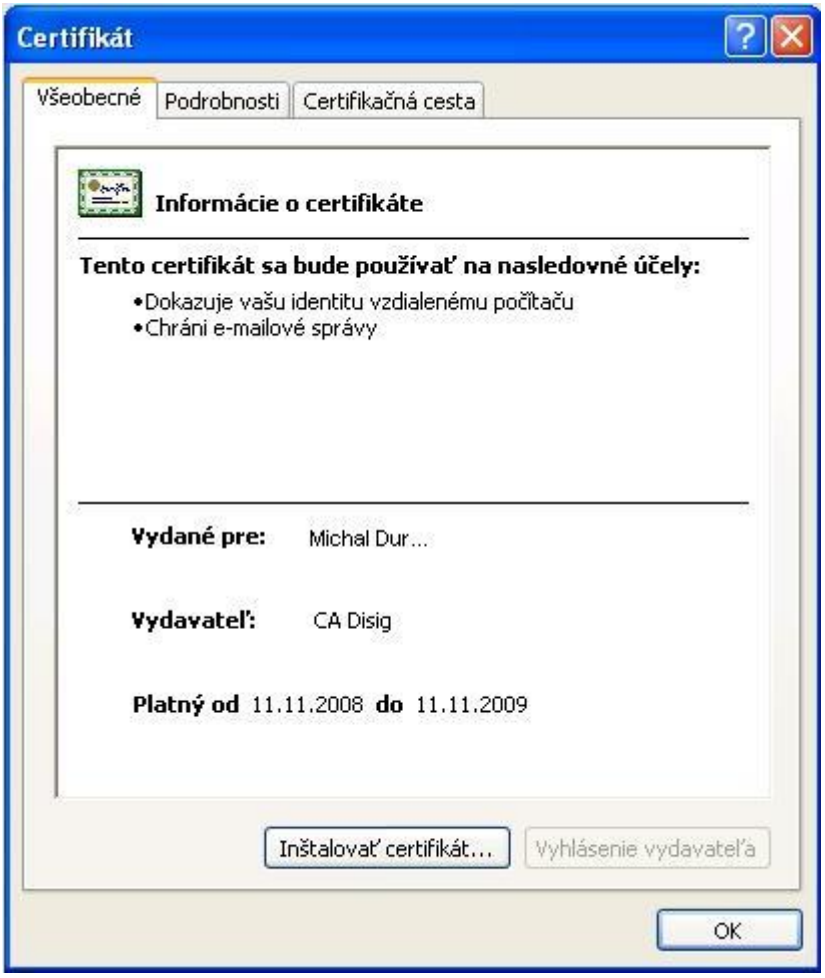
Import certifikátu inej osoby (a tým zároveň jej verejného kľúča) do systémového úložiska certifikátov MS Windows vykonáte podľa nasledovného postupu:

1. Kliknite na https://eidas.disig.sk/sk/crtsearch/.

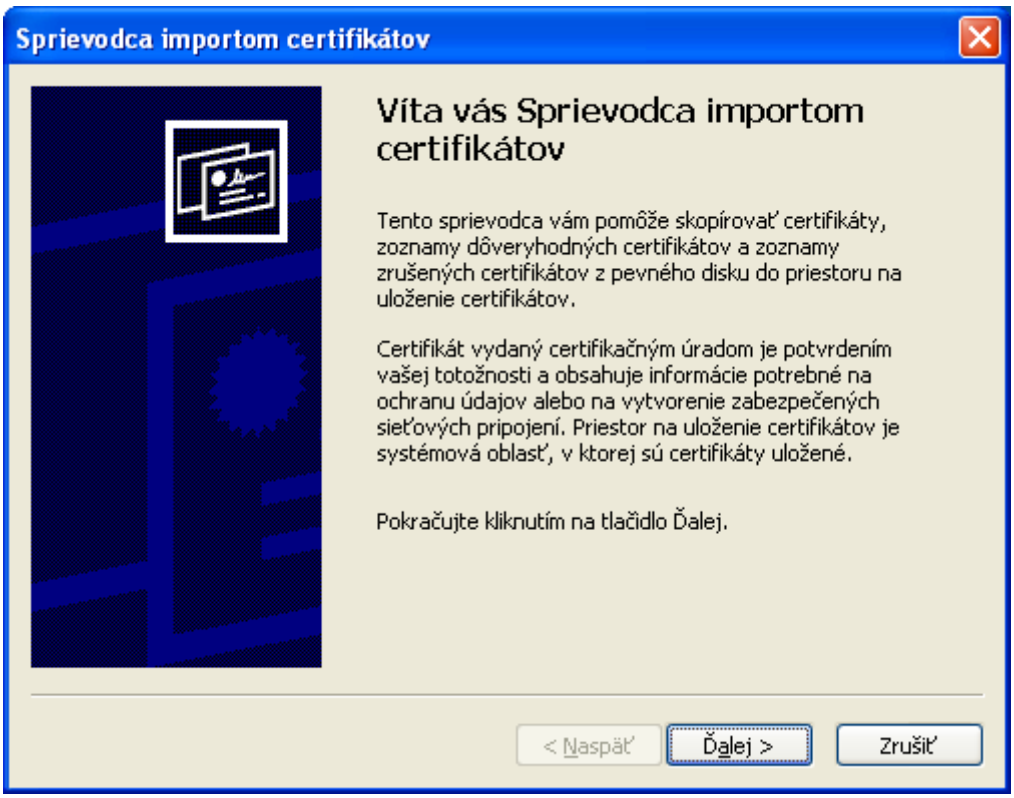
2. V otvorenom okne vpíšte do položky "**CN**" bez diakritiky celé meno osoby, ktorej bol certifikát vydaný. Identifikujte certifikát, ktorý hodláte nainštalovať a následne kliknite na text "**DER**" v časti "**Stiahnutie**":


3. Po zobrazení okna s ponukou na výber akcie zvoľte "**Otvoriť**":

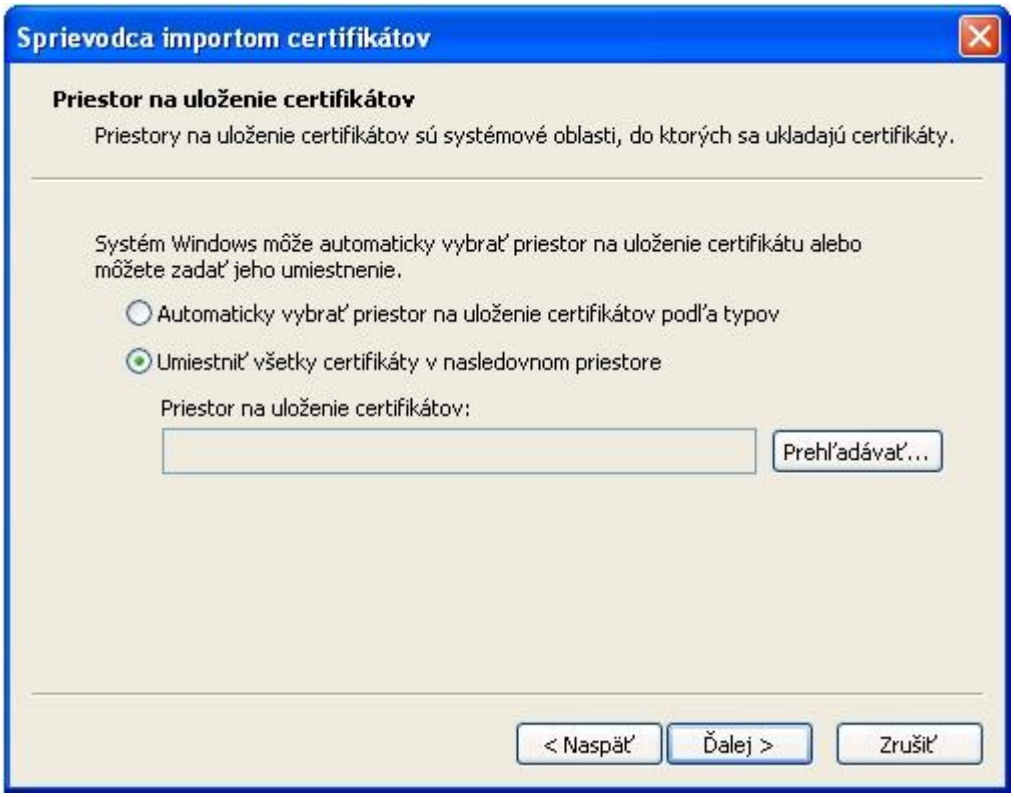
4. Otvorí sa okno s informáciami o certifikáte. Zvoľte "**Inštalovať certifikát**":



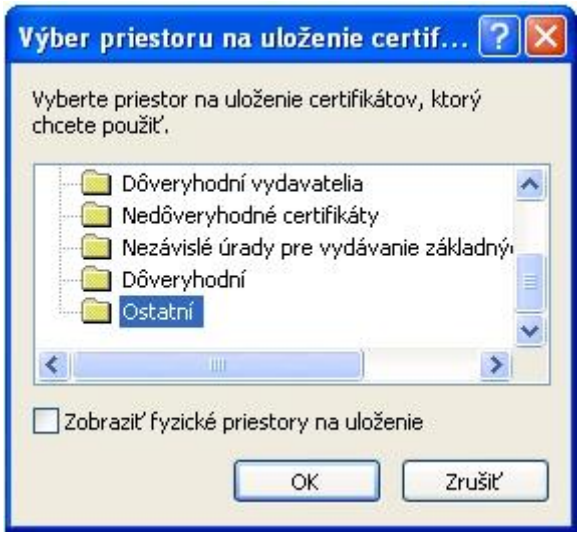

5. Pokračujte voľbou "**Ďalej >**":




6. Skontrolujte, či je zvolená možnosť "**Umiestniť všetky certifikáty v nasledovnom priestore**" a stlačte tlačidlo "**Prehľadávať**":

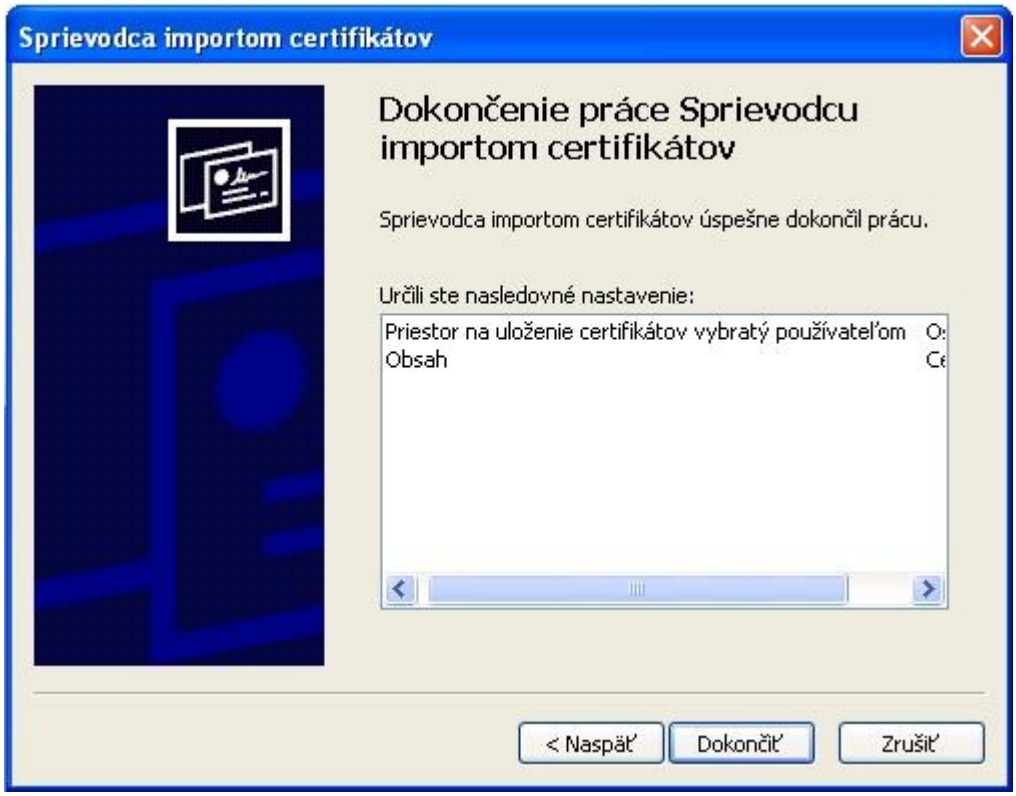



7. Ako priestor na uloženie certifikátov použite "**Ostatní**". Svoju voľbu potvrďte stlačením tlačidla "**OK**":

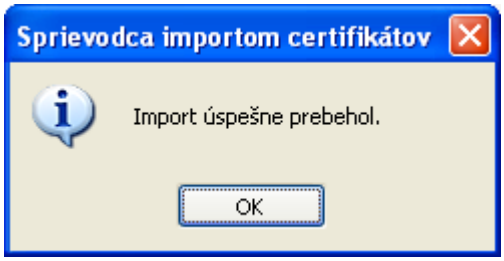



8. Pokračujte voľbou "**Ďalej** >".

9. Kliknite na tlačidlo "**Dokončiť**":




10. Zobrazí sa informácia o úspešnom nainštalovaní certifikátu. Inštaláciu certifikátu CA Disig ukončíte stlačením "**OK**":



**Poznámka**: Prijatím a akceptovaním digitálne podpísanej správy sa automaticky importuje certifikát odosielateľa.

## 4.2 Import certifikátov iných osôb do systémového úložiska certifikátov Mozilla

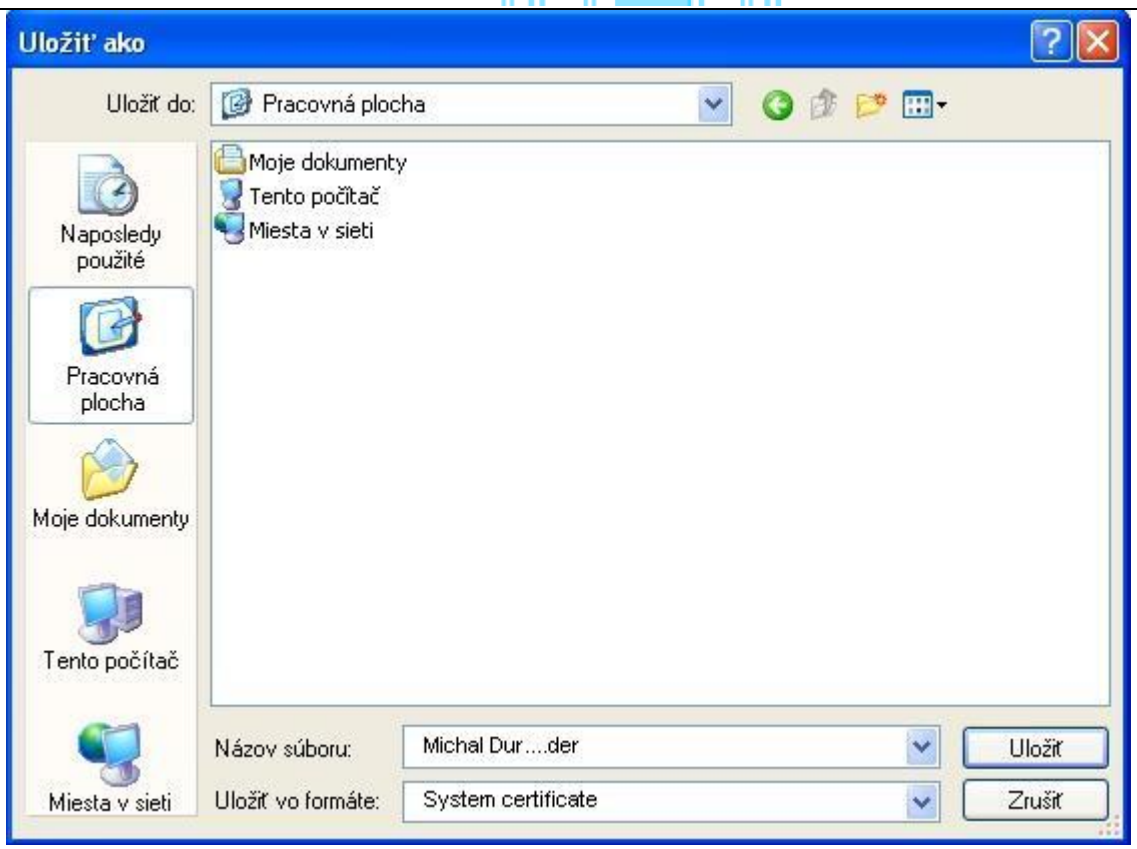
Import certifikátu inej osoby (a tým zároveň jej verejného kľúča) do systémového úložiska certifikátov Mozilla vykonáte podľa nasledovného postupu:

1. Kliknite na https://eidas.disig.sk/sk/crtsearch/.

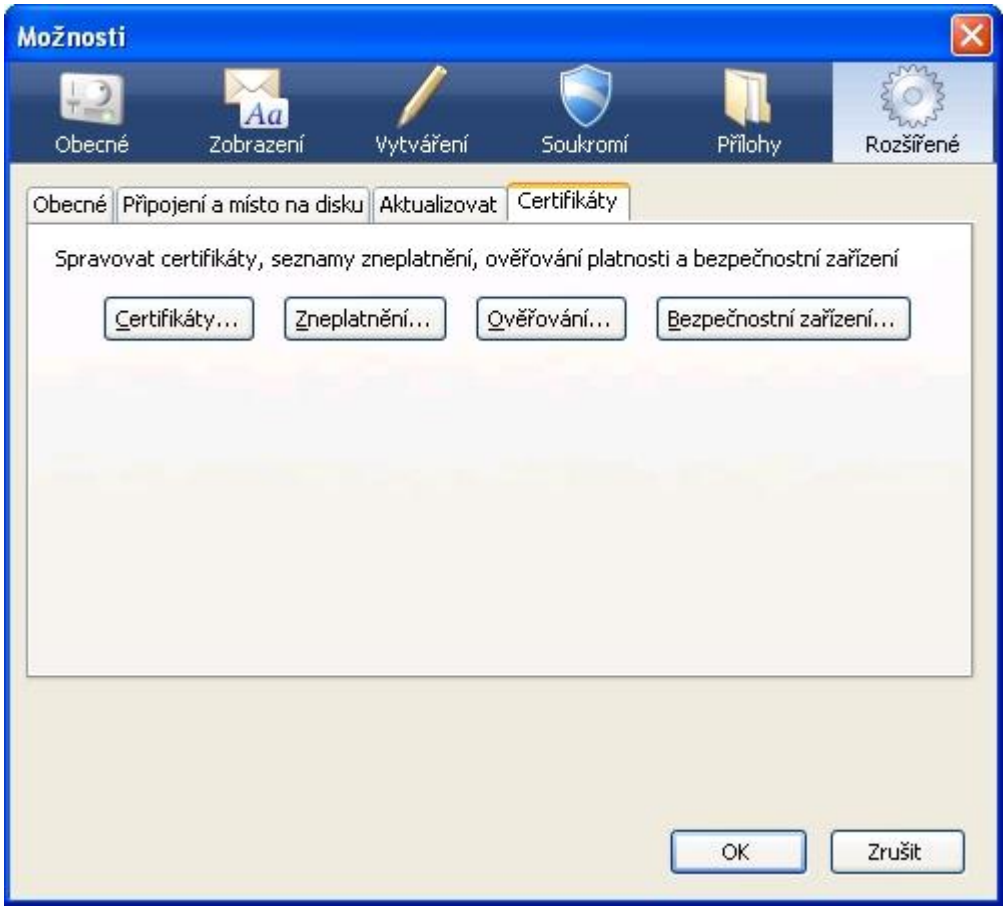
2. V otvorenom okne vpíšte do položky "**CN**" bez diakritiky celé meno osoby, ktorej bol certifikát vydaný. Identifikujte certifikát, ktorý hodláte nainštalovať a následne kliknite na text "**DER**" v časti "**Stiahnutie**":


3. Po zobrazení okna s ponukou na výber akcie zvoľte "**Uložiť**":

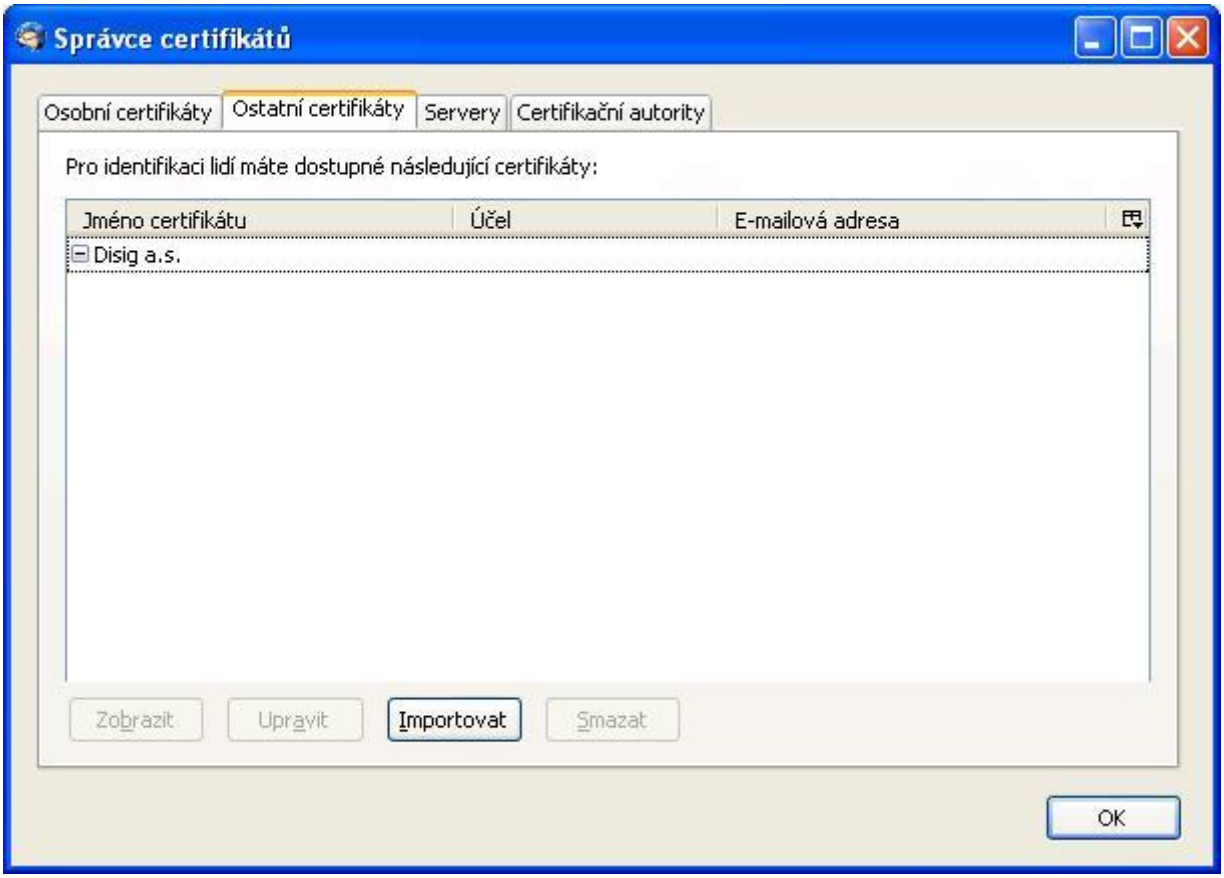

4. Zobrazí sa Vám nasledujúce okno, v ktorom je potrebné určiť si cestu uloženia žiadosti. Zvoľte si cestu a kliknite na možnosť **„Uložiť“**. Zvolenú cestu si zapamätajte:



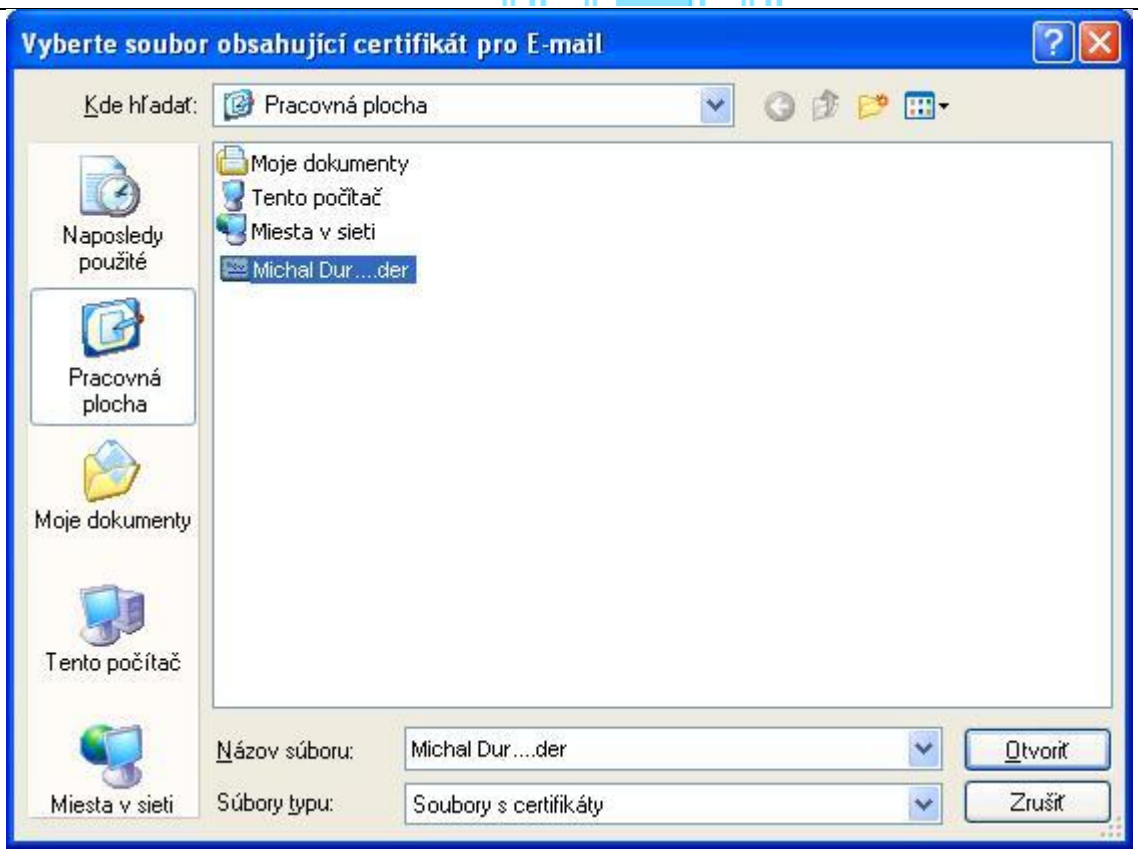

5. V hlavnom menu programu Mozilla zvoľte "**Nástroje -> Možnosti ...**". Vyberte " **Rozšírené**" (prípadne "**Pokročilé**") a ďalej zvoľte záložku "**Certifikáty**" (prípadne "**Šifrovanie**"):



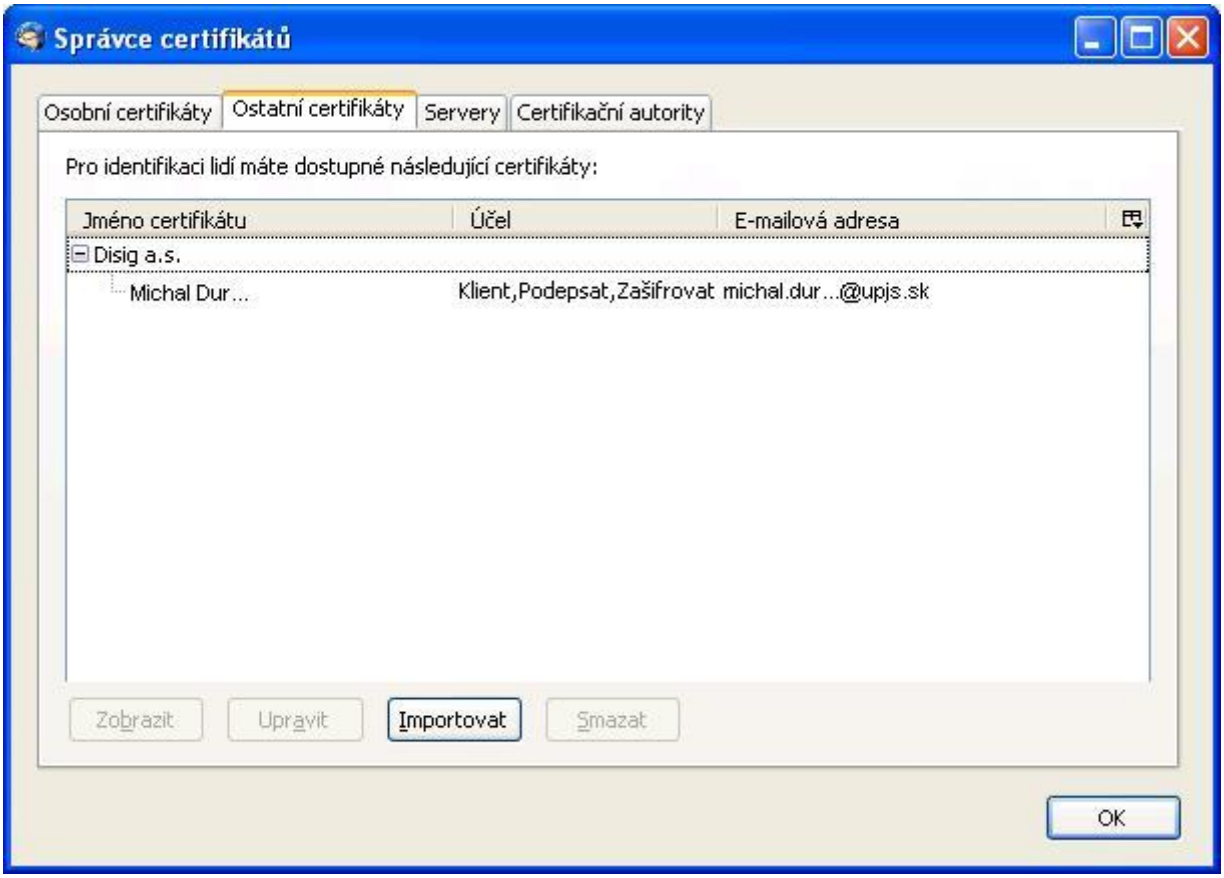
6. Kliknite na tlačidlo "**Certifikáty...** " a potom zvoľte kartu "**Ostatné certifikáty**":




7. Zvoľte možnosť "**Importovať**". Otvorí sa dialógové okno, prostredníctvom ktorého nájdite súbor uložený v bode 4. Výber potvrďte tlačidlo "**Otvoriť**":




8. Import ukončíte voľbou tlačidla "**OK**":



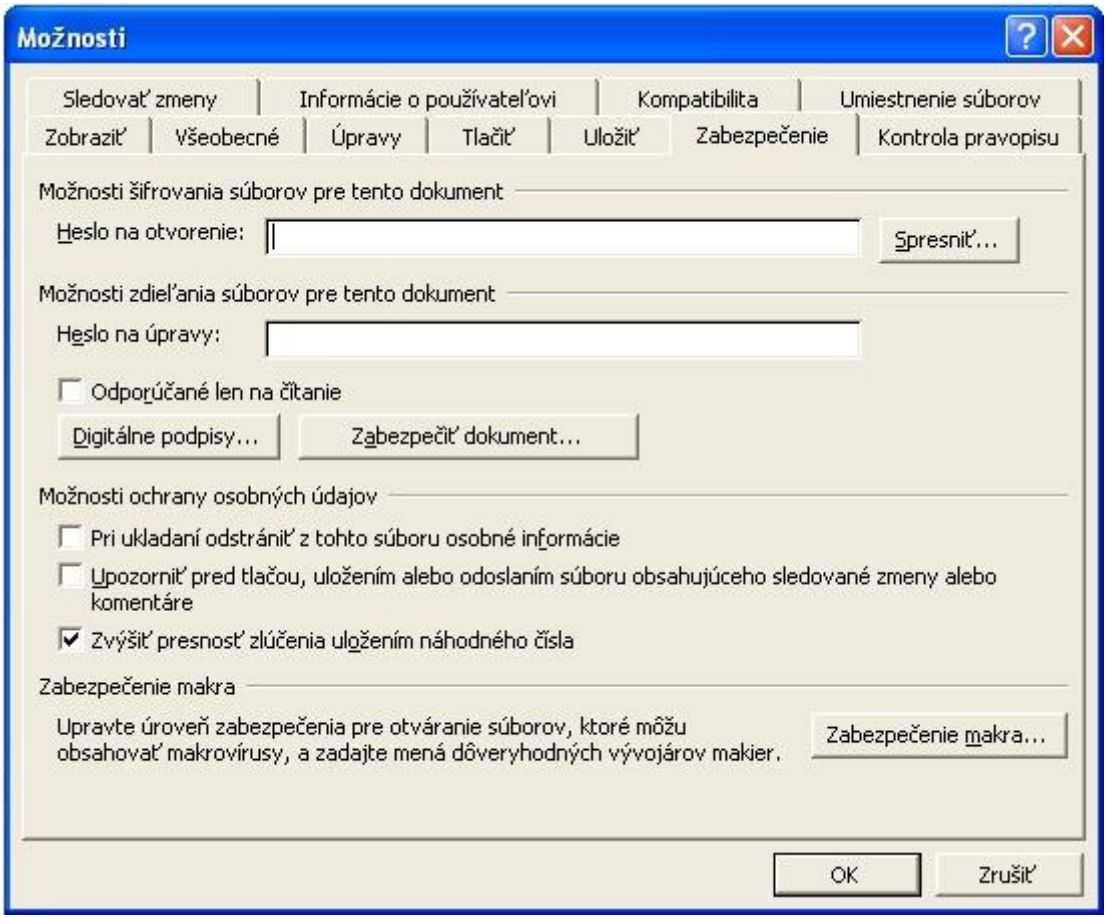
## 4.3 Elektronické podpísanie textového dokumentu MS Wordu

Predpokladá sa, že máte svoj osobný certifikát nainštalovaný v systémovom úložisku certifikátov MS Windows.

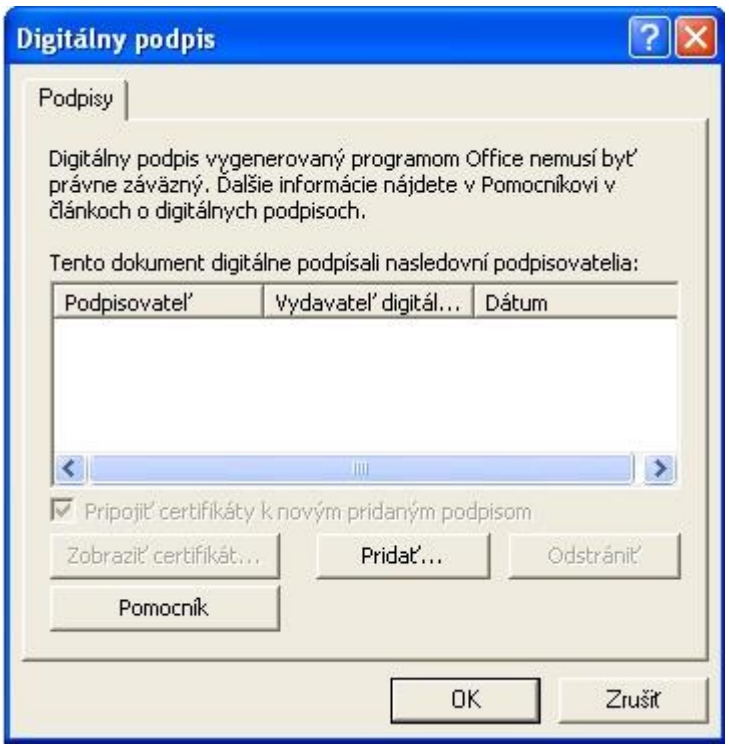
Textový dokument MS Wordu elektronicky podpíšete podľa nasledovného postupu:

1. Textový dokument musí byť vo svojej finálnej podobe a musí byť uložený. Elektronické podpisovanie vykonávame ako posledný krok.

2. Z hlavnej ponuky programu vyberte "**Nástroje**" a potom "**Možnosti...**". V dialógovom okne "**Možnosti**" zvoľte kartu "**Zabezpečenie**":

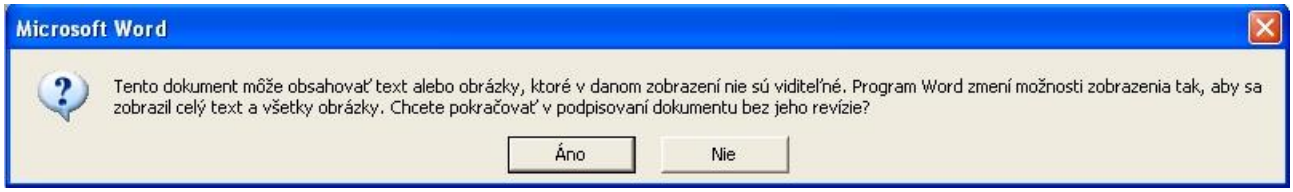



3. Pokračujte voľbou tlačidla "**Digitálne podpisy...**":



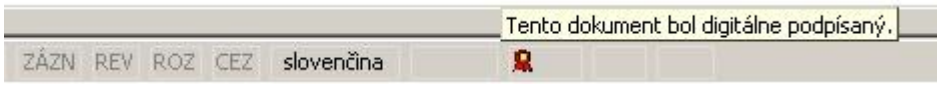

4. Kliknite na tlačidlo "**Pridať...**".

5. Na pokračovanie zvoľte "**Áno**:




6. Vyberte certifikát, ktorý chcete použiť. Svoj výber potvrďte voľbou "**OK**":

7. Postupne zatvorte dialógové okná "**Digitálny podpis**" a "**Možnosti**" kliknutím na tlačidlo "**OK**". Podpísanie dokumentu indikuje ikona v stavovom riadku programu:




**Poznámka**: Analogickým spôsobom možno digitálne podpísať aj iné typy dokumentov z kancelárske balíka MS Office.

## 4.4 Elektronické podpísanie textového dokumentu z kancelárskeho balíku Open Office

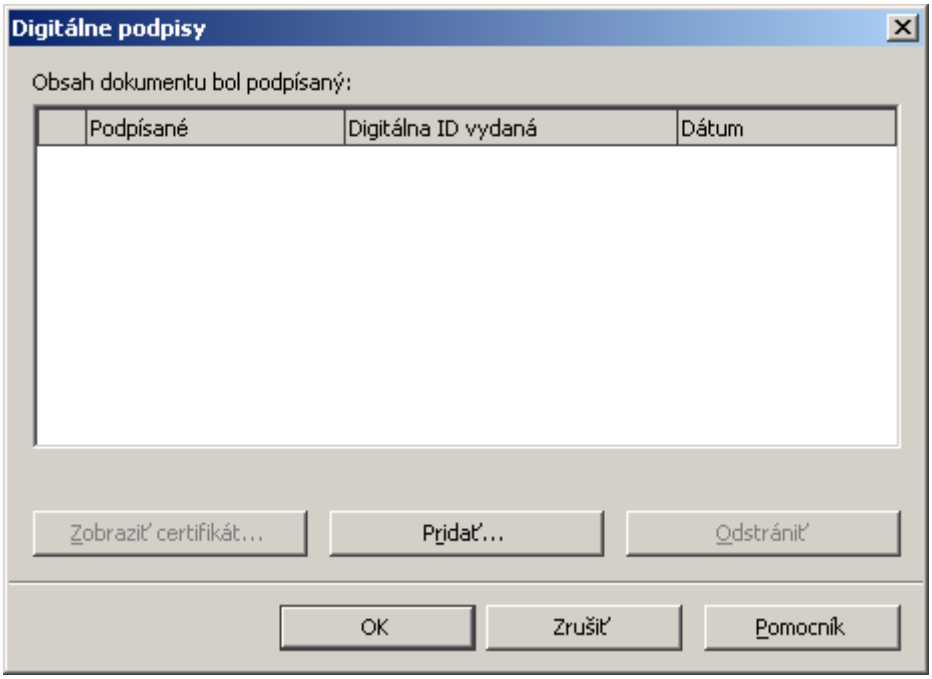
Predpokladá sa, že máte svoj osobný certifikát nainštalovaný v systémovom úložisku certifikátov MS Windows. V operačnom systéme Windows totiž kancelársky balík OpenOffice zdieľa systémové úložisko certifikátov s Windows.

**Poznámka**: V OpenOffice možno elektronicky podpisovať len dokumenty formátu OpenDokument. Súbory typu doc nemožno v OpenOffice elektronicky podpísať.

Textový dokument OpenOffice elektronicky podpíšete podľa nasledovného postupu:

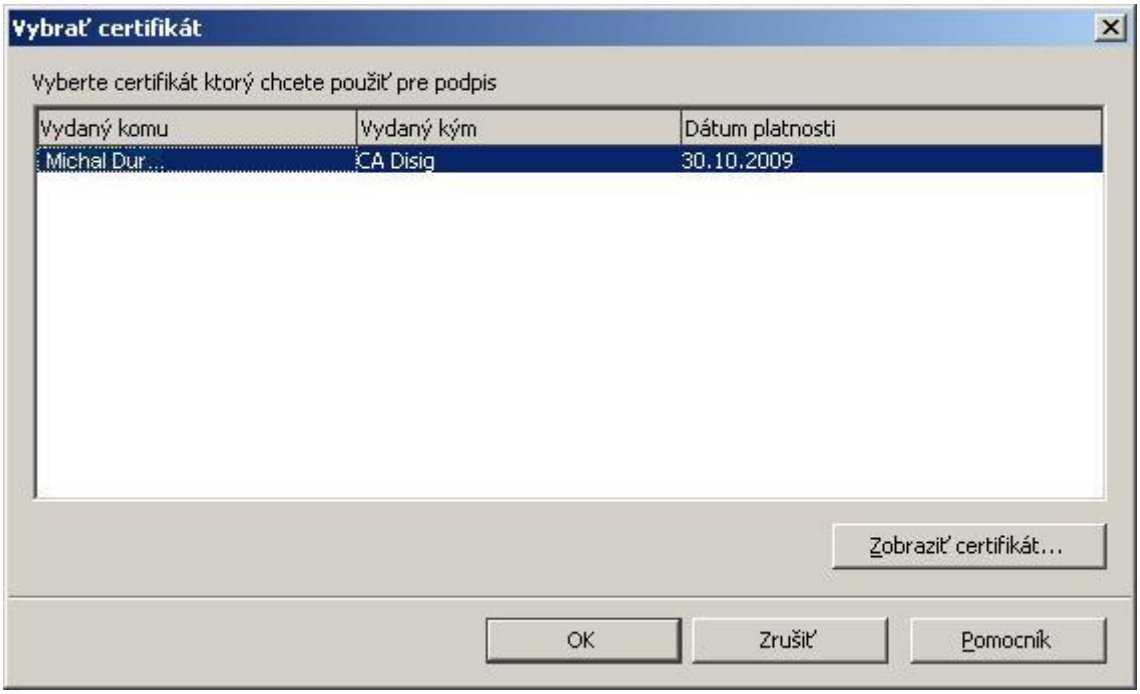
8. Textový dokument musí byť vo svojej finálnej podobe a musí byť uložený. Elektronické podpisovanie vykonávame ako posledný krok.

9. Z hlavnej ponuky programu vyberte "**Súbor**" a potom "**Digitálne podpisy...**":




10. Kliknite na tlačidlo "**Pridať...**".

11. Vyberte certifikát, ktorý chcete použiť. Svoj výber potvrďte voľbou "**OK**":




12. Zatvorte dialógové okno "**Digitálne podpisy**" kliknutím na tlačidlo "**OK**". Podpísanie dokumentu indikuje ikona v stavovom riadku programu:


**Poznámka**: Analogickým spôsobom možno digitálne podpísať aj iné typy dokumentov z kancelárske balíka OpenOffice.

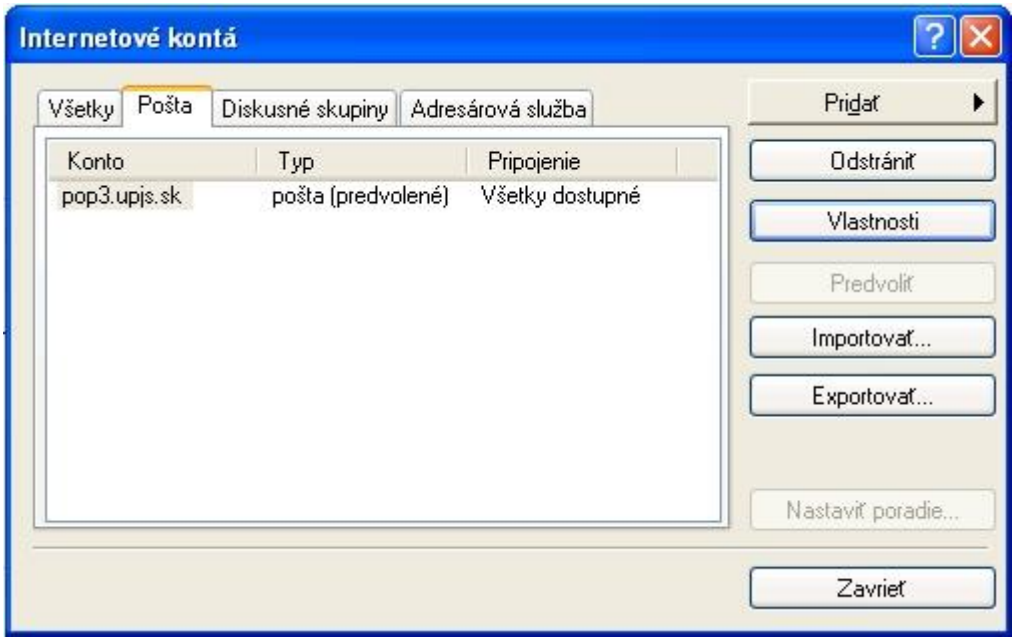
## 4.5 Využívanie osobného certifikátu s poštovým klientom Outlook Express

**Dôležité upozornenie:** Pre správne fungovanie poštového klienta Outlook Express s Vašim osobným certifikátom je nutné, aby emailová adresa vo Vašom osobnom certifikáte odpovedala emailovej adrese v nastaveniach Vášho poštového konta.

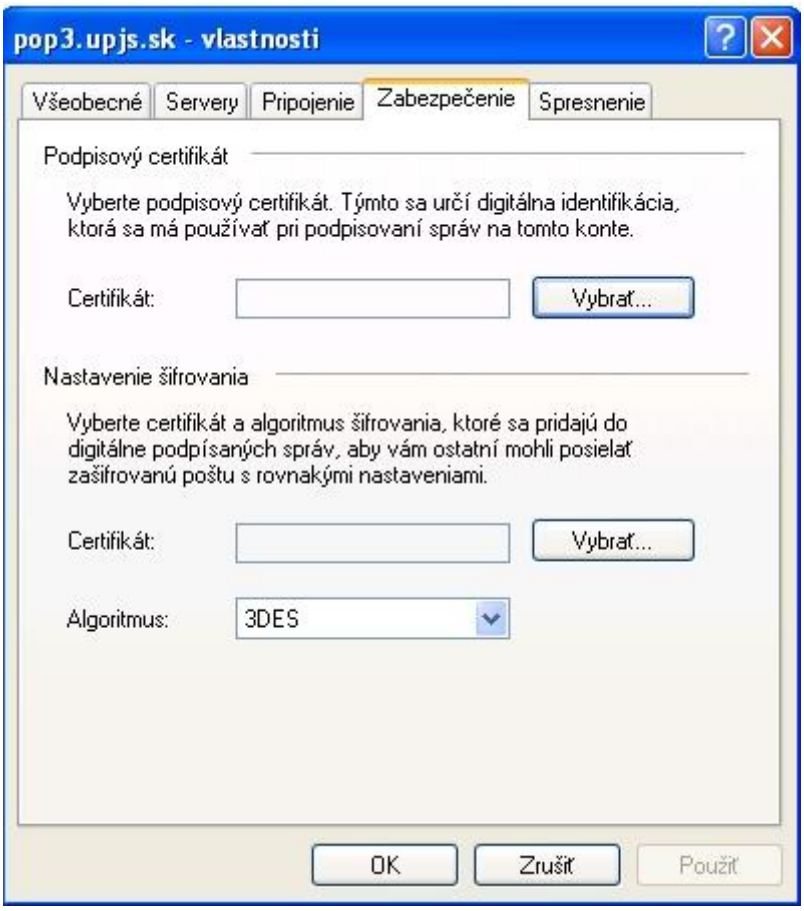
Predpokladá sa, že máte svoj osobný certifikát a certifikáty osôb, s ktorými si chcete vymieňať zašifrované správy nainštalované v systémovom úložisku certifikátov MS Windows.

Nastavenie účtu elektronickej pošty v programe Outlook Express vykonáte podľa nasledovného postupu:

1. V hlavnom okne programu vyberte "**Nástroje**", potom "**Kontá...**" a napokon kartu "**Pošta**":




2. Označte účet univerzitnej elektronickej pošty a stlačte tlačidlo Vlastnosti. V otvorenom dialógovom okno aktivujte kartu "**Zabezpečenie**". Pomocou tlačidiel "**Vybrať...**" môžete nastaviť certifikát používaný na podpisovanie elektronickej pošty a taktiež na jej šifrovanie. Na obe účely môže byť použitý ten istý certifikát:

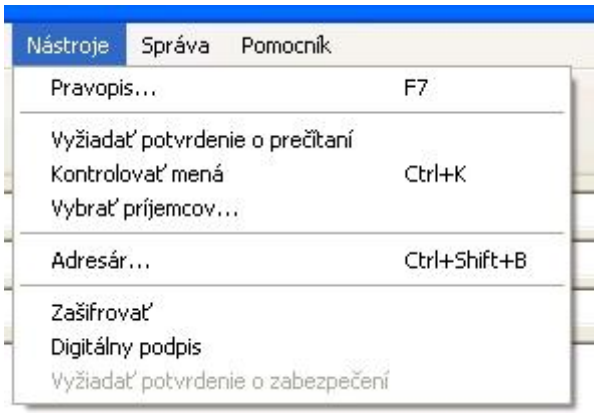



3. Vyberte certifikát, ktorý chcete použiť. Svoj výber potvrďte voľbou "**OK**":


4. Postupne zatvorte dialógové okná "**Vlastnosti**" a "**Internetové kontá**" kliknutím na tlačidlo "**OK**" a "**Zavrieť**".

5. Pri tvorbe novej správy sa tlačidlá na podpísanie, prípadne šifrovanie správy (na to je potrebné mať nainštalovaný certifikát adresáta, pozrite 4.1) nachádzajú priamo v paneli nástrojov:


prípadne v ponuke "**Nástroje**":




6. Podpísanie emailu indikuje ikona pečate a zašifrovanie ikona zámky:

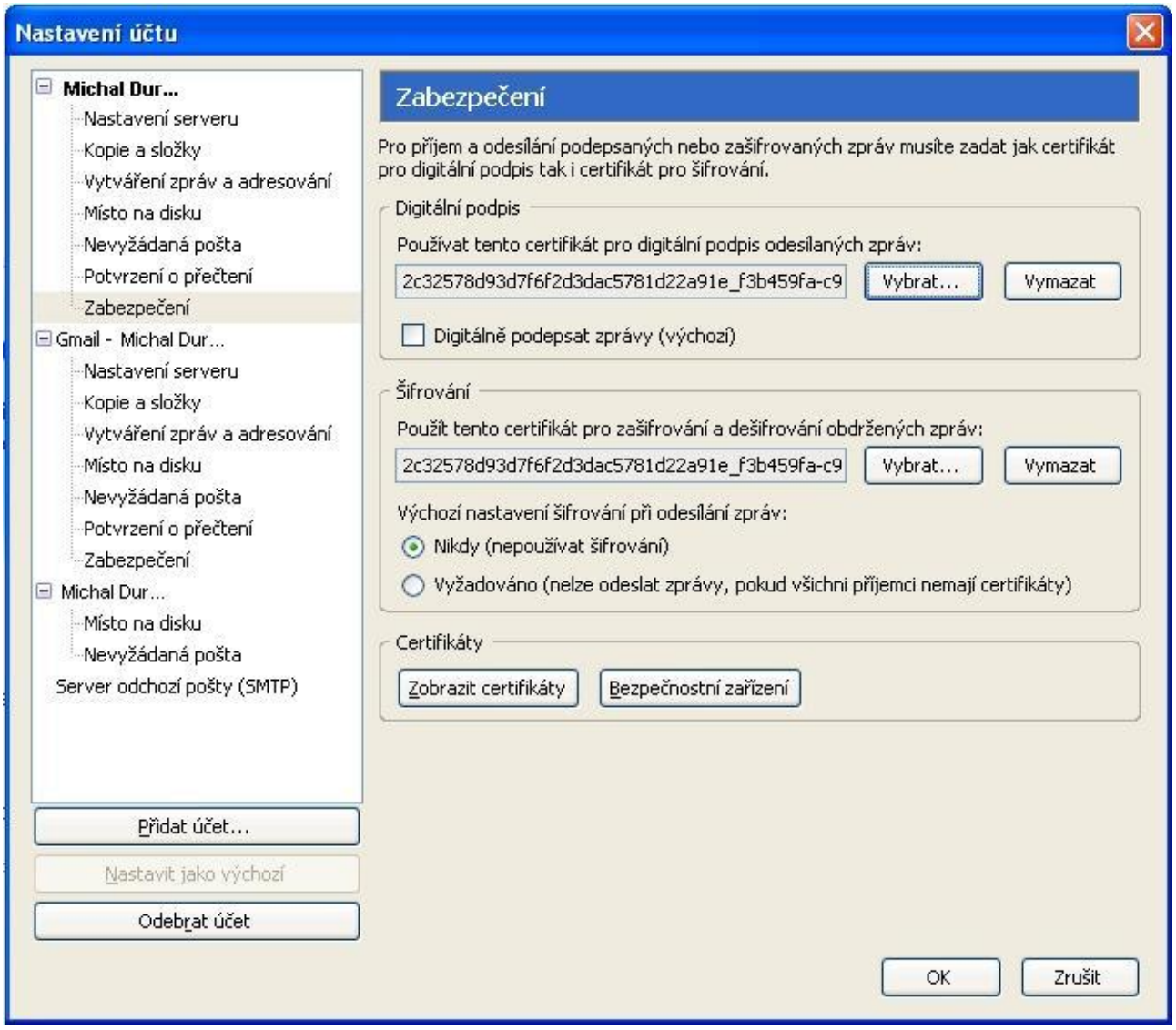
## 4.6 Využívanie osobného certifikátu s poštovým klientom Mozilla Thunderbird

**Dôležité upozornenia:**

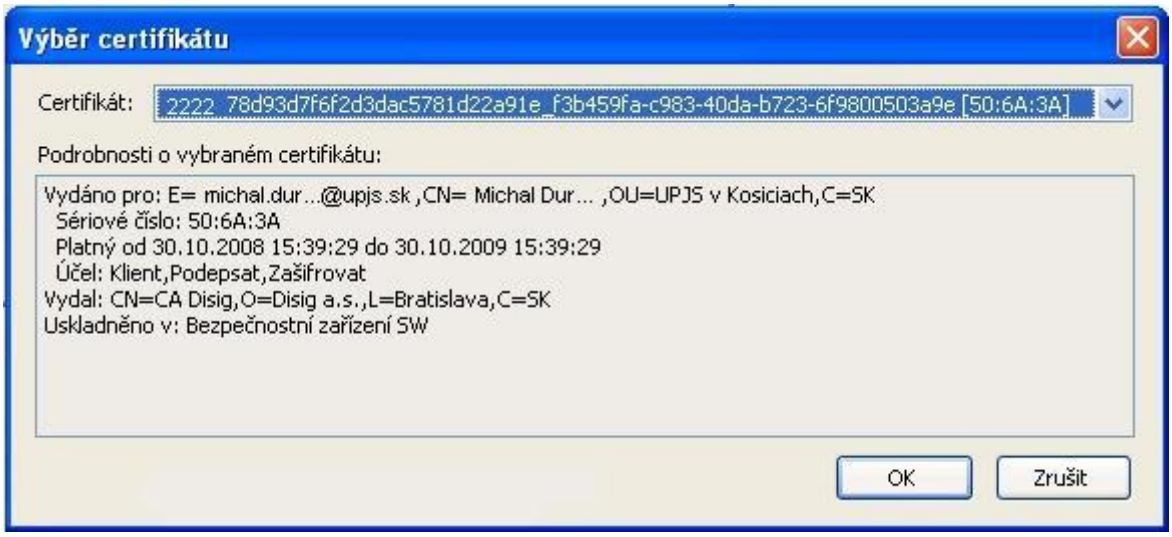
- Pre správne fungovanie poštového klienta Mozilla Thunderbird s Vašim osobným certifikátom je nutné, aby emailová adresa vo Vašom osobnom certifikáte odpovedala emailovej adrese v nastaveniach Vášho poštového konta.
- Predpokladá sa, že máte svoj osobný certifikát a certifikáty osôb, s ktorými si chcete vymieňať zašifrované správy nainštalované v systémovom úložisku certifikátov programu Mozilla Thunderbird (**Firefox a Thunderbird zvyčajne svoje úložiská certifikátov nezdieľajú!**).

Nastavenie účtu elektronickej pošty v programe Mozilla Thunderbird vykonáte podľa nasledovného postupu:

1. V hlavnom okne programu vyberte "**Nástroje**" a potom "**Nastavenia účtu...**". Kliknite na text "**Zabezpečenie**" v ľavej časti dialógového okna účtu univerzitnej elektronickej pošty. Pomocou tlačidiel "**Vybrať...**" môžete nastaviť certifikát používaný na podpisovanie elektronickej pošty a taktiež na jej šifrovanie. Na obe účely môže byť použitý ten istý certifikát:

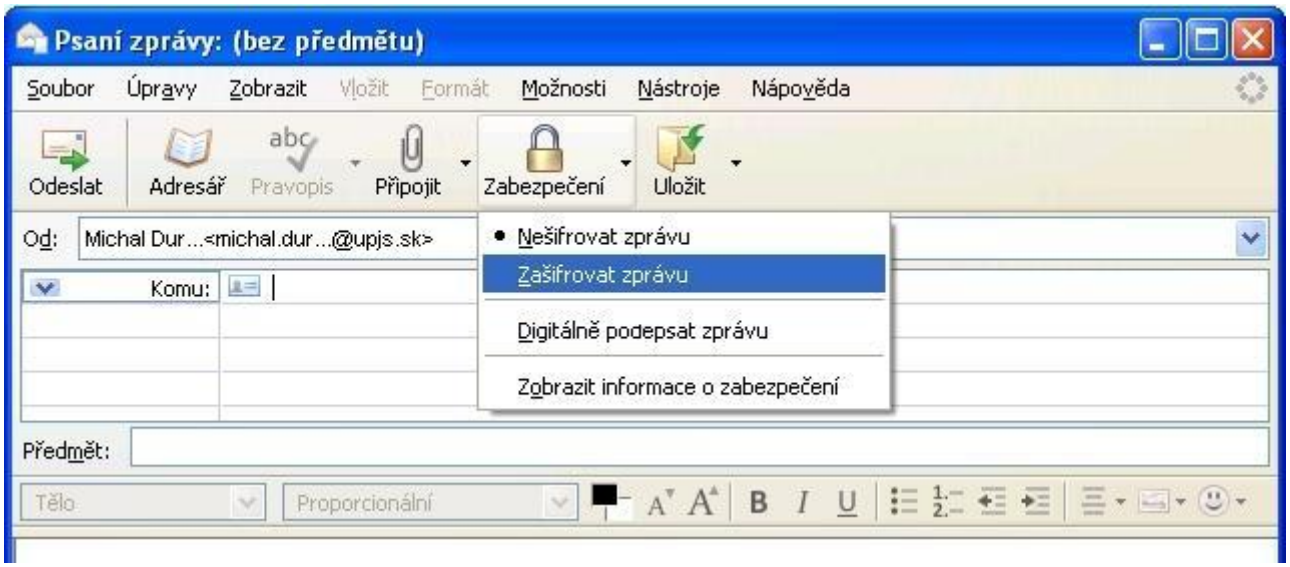


2. Vyberte certifikát, ktorý chcete použiť. Svoj výber potvrďte voľbou "**OK**":

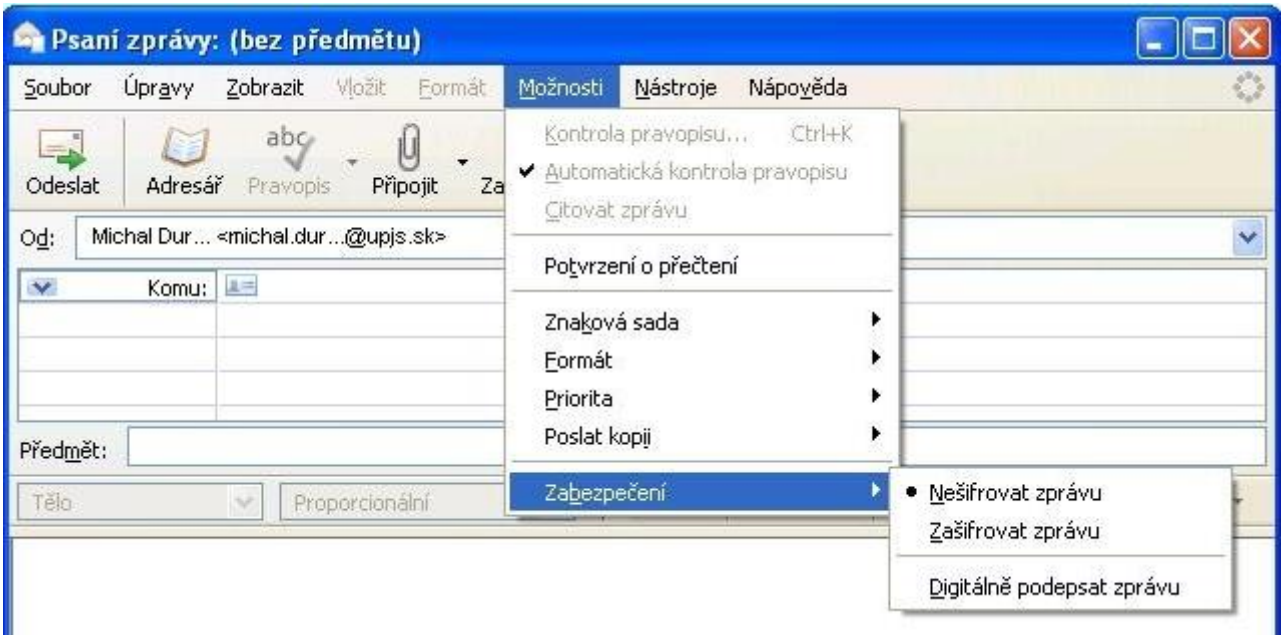



3. Zatvorte dialógové okno "**Nastavenia účtu**" kliknutím na tlačidlo "**OK**".

4. Pri tvorbe novej správy sa tlačidlá na podpísanie, prípadne šifrovanie správy (na to je potrebné mať nainštalovaný certifikát adresáta, pozrite 4.2) nachádzajú priamo v paneli nástrojov:




prípadne v ponuke "**Možnosti**":




5. Podpísanie emailu indikuje ikona obálky a zašifrovanie ikona zámky v okne správy vpravo dole:

# 5 VYSVETLENIE POJMOV

**Certifikačná autorita**
Certifikačná autorita je „dôveryhodná tretia strana“, ktorá sprostredkúva dôveru medzi komunikujúcimi stranami. Vydáva certifikáty verejného kľúča, ktoré umožňujú komunikujúcim stranám dôveryhodne doložiť svoju identitu.

**Elektronický podpis**
Elektronický podpis predstavuje elektronickú obdobu klasického podpisu. Obidva typy podpisov (klasický aj elektronický) slúžia na potvrdenie autenticity podpisovaného dokumentu a na identifikáciu autora podpisu. Elektronický podpis (EP) je informácia pripojená k podpisovanému dokumentu, pomocou ktorej je možné overiť autenticitu a integritu podpísaného dokumentu (Zákon č. 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v platnom znení). Na jeho vytvorenie je potrebné, aby autor vlastnil súkromný kľúč a k nemu prislúchajúci certifikát, pričom identitu autora podpisu potvrdzuje dôveryhodná tretia strana - certifikačná autorita. Pomocou kryptografických algoritmov a súkromného kľúča je vytvorená štruktúra, ktorá je následne spolu s certifikátom prislúchajúcim k použitému súkromnému kľúču pripojená k elektronickému dokumentu. Prostredníctvom tejto štruktúry s použitím pripojeného certifikátu je možné kedykoľvek neskôr zistiť, či elektronický dokument je autentický alebo v ňom boli vykonané zmeny.

**Súkromný kľúč**
Súkromným kľúčom je tajná informácia, ktorá slúži na vyhotovenie elektronického podpisu elektronického dokumentu.

**Verejný kľúč**
Verejným kľúčom je informácia dostupná adresátovi (overovateľovi) podpísaného elektronického dokumentu, ktorá slúži na overenie pravosti elektronického podpisu vyhotoveného pomocou odpovedajúceho súkromného kľúča.

**Certifikát**
Certifikát (inak aj certifikát verejného kľúča) je elektronický dokument, ktorým vydavateľ certifikátu (certifikačná autorita) potvrdzuje, že v certifikáte uvedený verejný kľúč patrí osobe, ktorej je certifikát vydaný. Certifikát je určený na overovanie správnosti elektronického podpisu vyhotoveného pomocou súkromného kľúča patriaceho k danému verejnému kľúču.