SOFTIDEA

Šifrovanie elektronickej pošty

Príručka používateľa

(AN101011)

December 2011

Obsah

Táto príručka popisuje nastavenie poštového klienta ***Thunderbird*** pre zabezpečenie dôvernosti a zaručenie integrity elektronickej poštovej komunikácie s využitím hardvérového kryptografického zariadenia ***GNT USB Token*** od spoločnosti ***SoftIdea***. Nastavenie poštového klienta podľa tejto príručky umožní šifrovať a digitálne podpisovať správy elektronickej pošty.

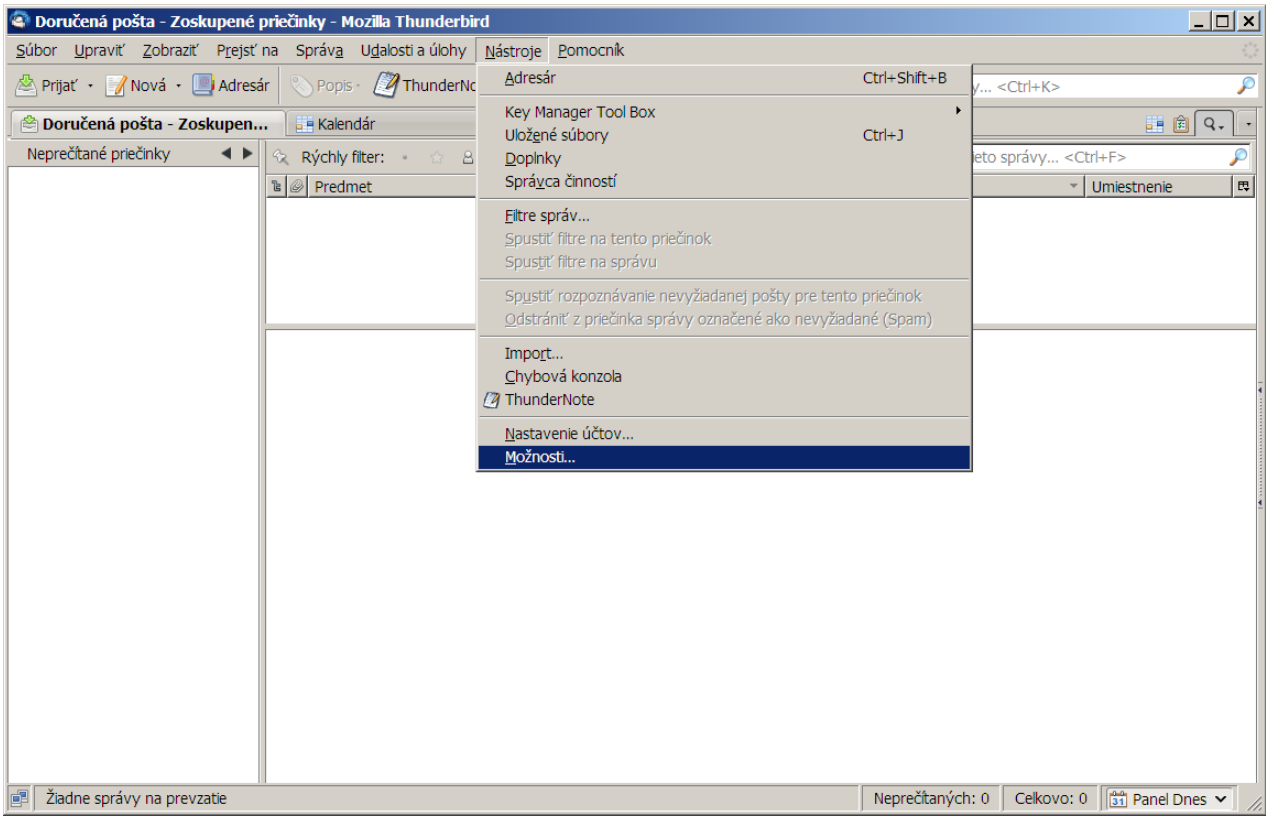
1 Systémové požiadavky

1. Operačný systém: Microsoft Windows XP, Vista, 7, 8.
2. ***GNT USB Token*** inicializovaný administrátorom pre funkciu zabezpečenia poštového klienta Thunderbird. Takýto Token obsahuje kľúče užívateľa, certifikáty užívateľa a certifikačnej autority.
3. Poštový klient Mozilla Thunderbird
4. Bezpečnostný modul SIPKCS vo forme dynamickej knižnice "*sipkcs.dll*". Modul SIPKCS je typicky umiestnený v systémovom adresáry.

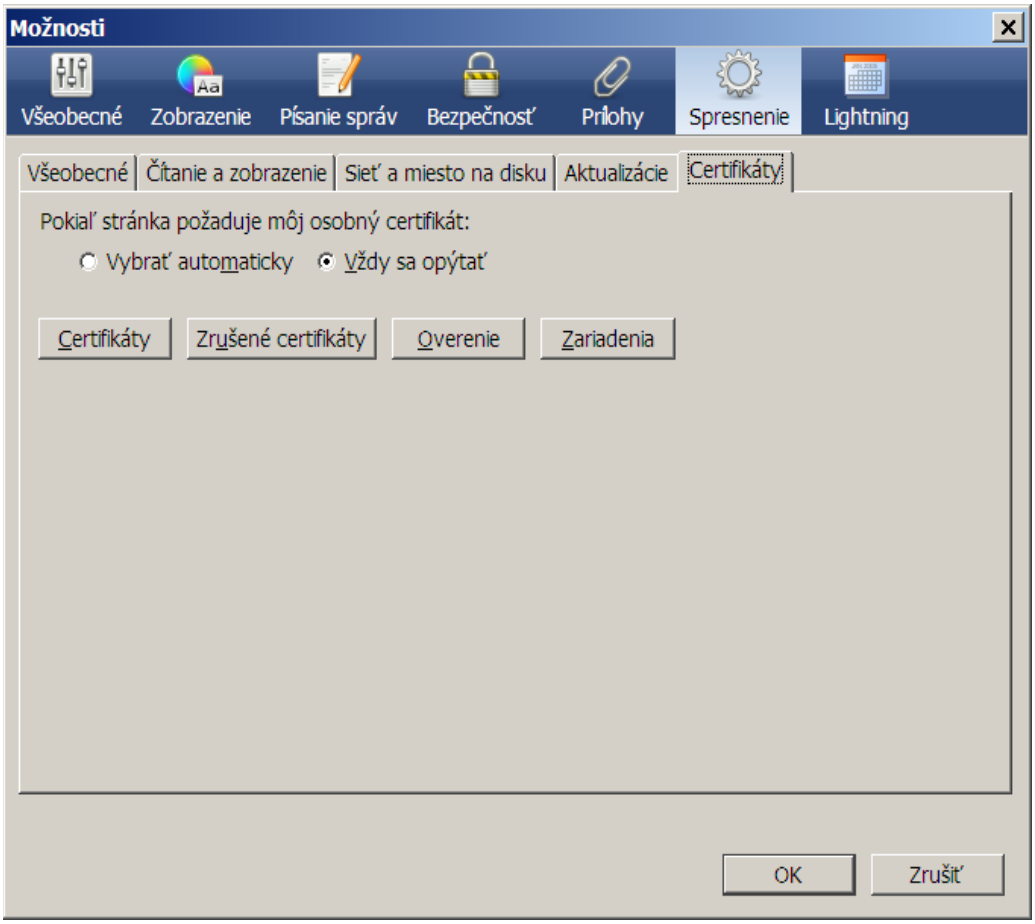
2 Zavedenie bezpečnostného modulu SIPKCS

Bezpečnostný modul SIPKCS umožňuje poštovému klientovi Thunderbird komunikovať s hardvérovým kryptografickým zariadením.

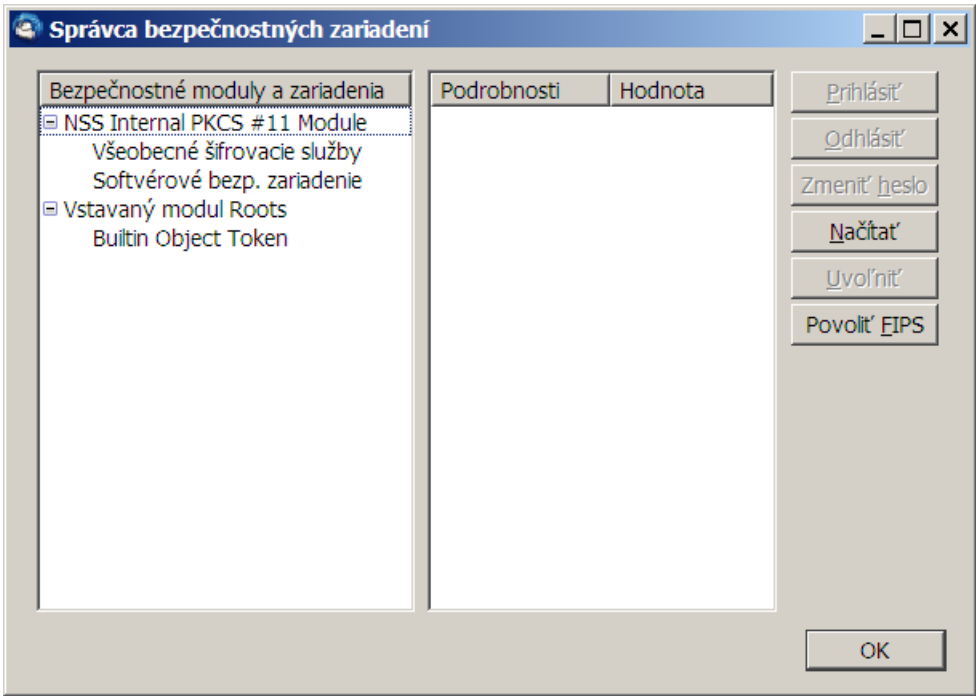
1. Otvorte Thunderbird a zvolte "Nástroje->Možnosti"



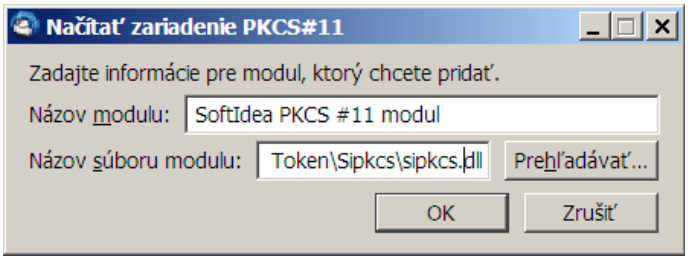
2. Zvoľte kartu "Spresnenie, Certifikáty" a zvoľte tlačidlo "Zariadenia"



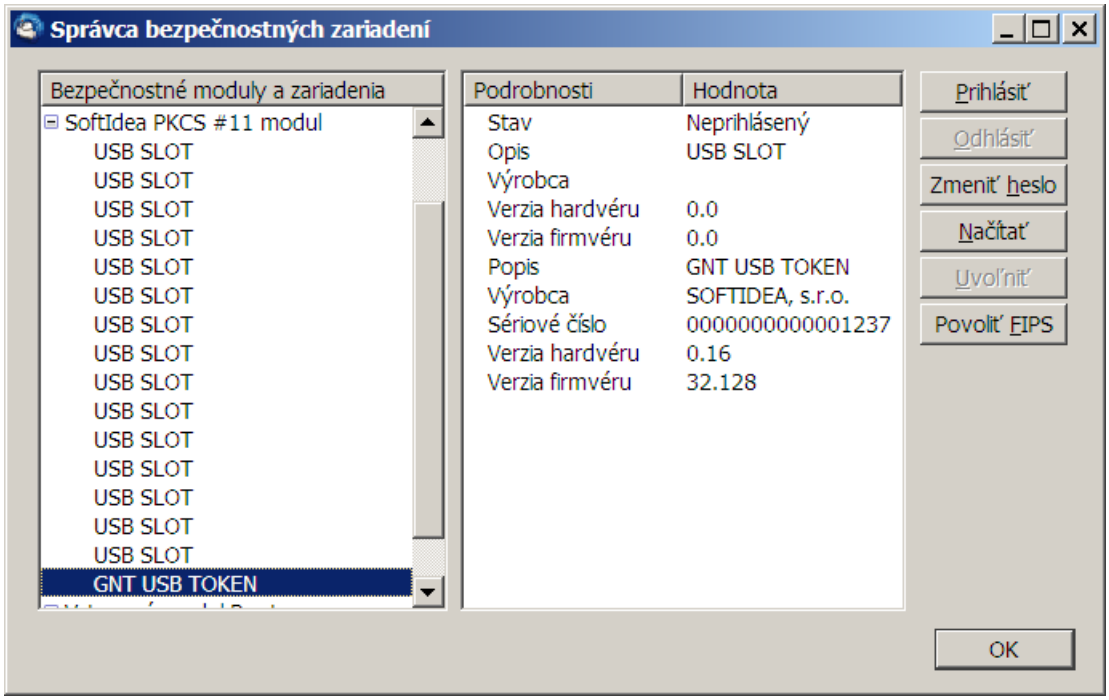
3. V nasledujúcom okne zvoľte tlačidlo "Načítať"



4. Zadajte názov modulu "*SoftIdea PKCS #11 modul*" a s pomocou tlačidla "Prehľadávať" zvoľte názov súboru modulu. Typický názov súboru je "*C:\Windows\System32\sipkcs.dll*". Stlačte tlačidlo OK. Vložte Token.

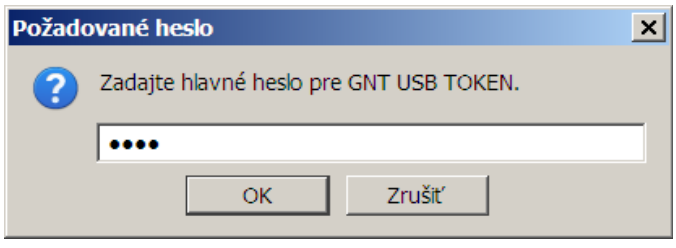


5. Správca bezpečnostných zariadení teraz zobrazuje načítaný modul SIPKCS a podrobnosti o vloženom Tokene. V tomto okamihu je vhodné zmeniť užívateľské heslo postupom podľa kapitoly 7. Stlačte OK.



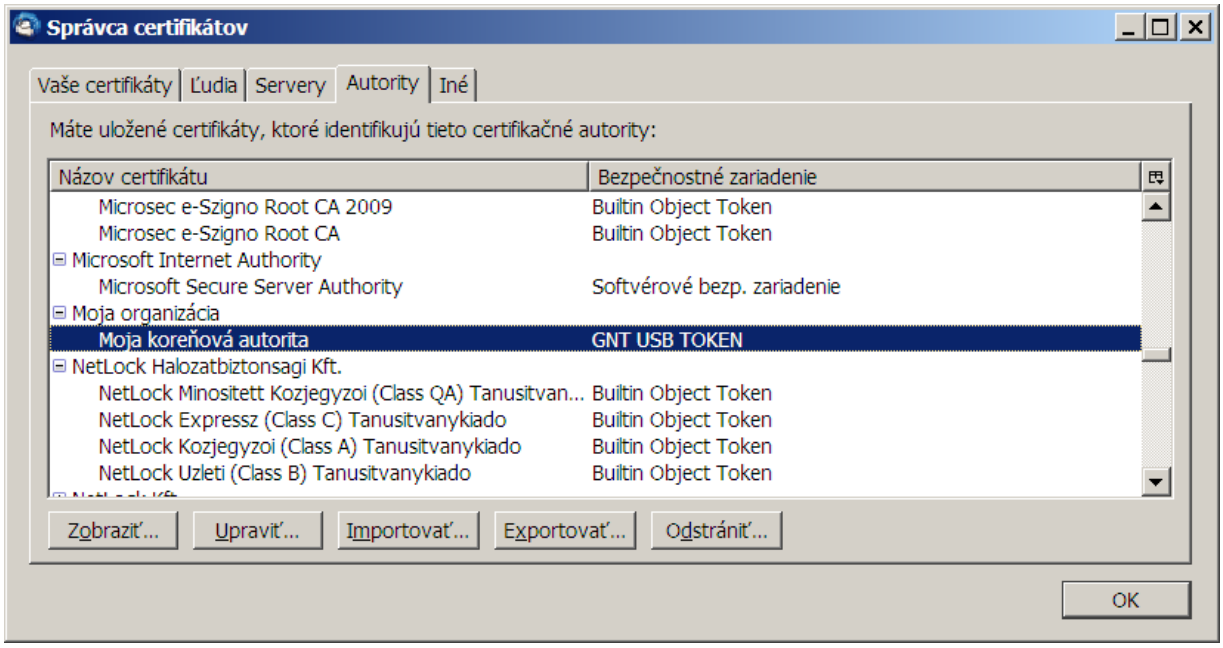
3 Nastavenie dôvery v certifikát koreňovej autority

1. Otvorte okno "Nástroje->Možnosti", zvoľte kartu "Spresnenie, Certifikáty" a zvoľte tlačidlo "Certifikáty". V nasledujúcom okne zadajte užívateľské heslo pre prihlásenie k Tokenu.

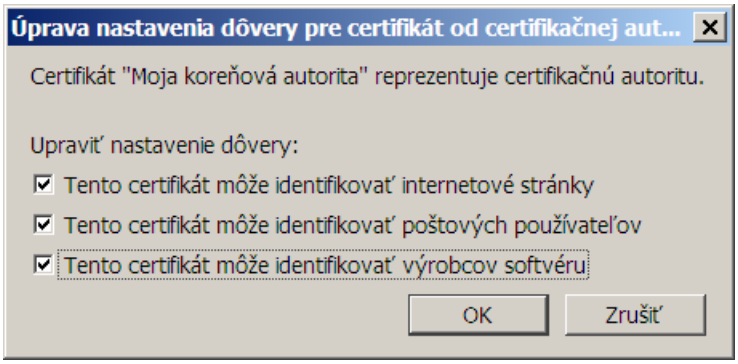


2. V okne "Správca certifikátov"zvoľte kartu "Autority" a zvoľte certifikát koreňovej autority uložený na zariadení "GNT USB TOKEN". Názov certifikátu koreňovej autority Vám oznámi administrátor. V príklade na nasledujúcom obrázku sa jedná o certifikát s názvom "Moja koreňová autorita" vydaný organizáciou "Moja organizácia".

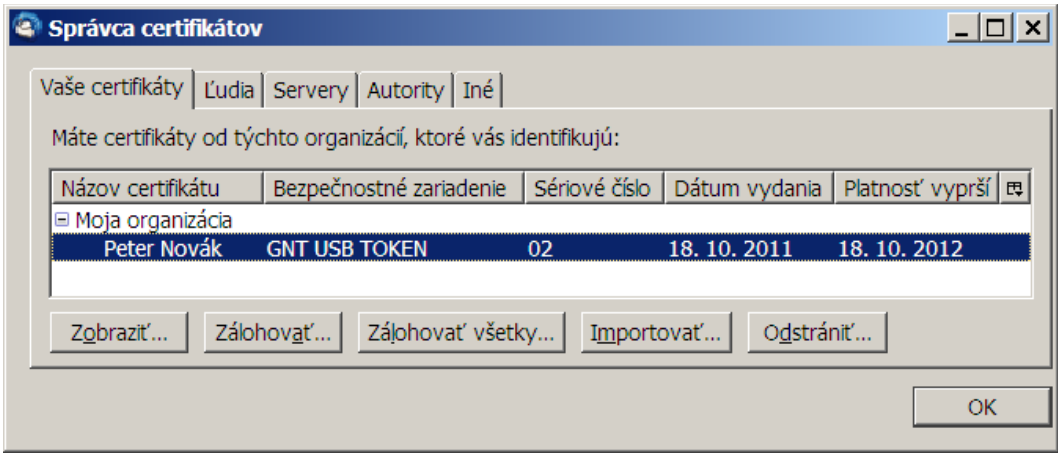
Poznámka: v okne "Správca certifikátov" sa dá vyhľadávať vkladaním začiatočných písmen názvu koreňovej autority.



3. Zvoľte tlačidlo "Upraviť"a nastavte dôveru certifikačnej autorite pre všetky identifikácie podľa nasledujúceho obrázka. Stlačte tlačidlo OK.



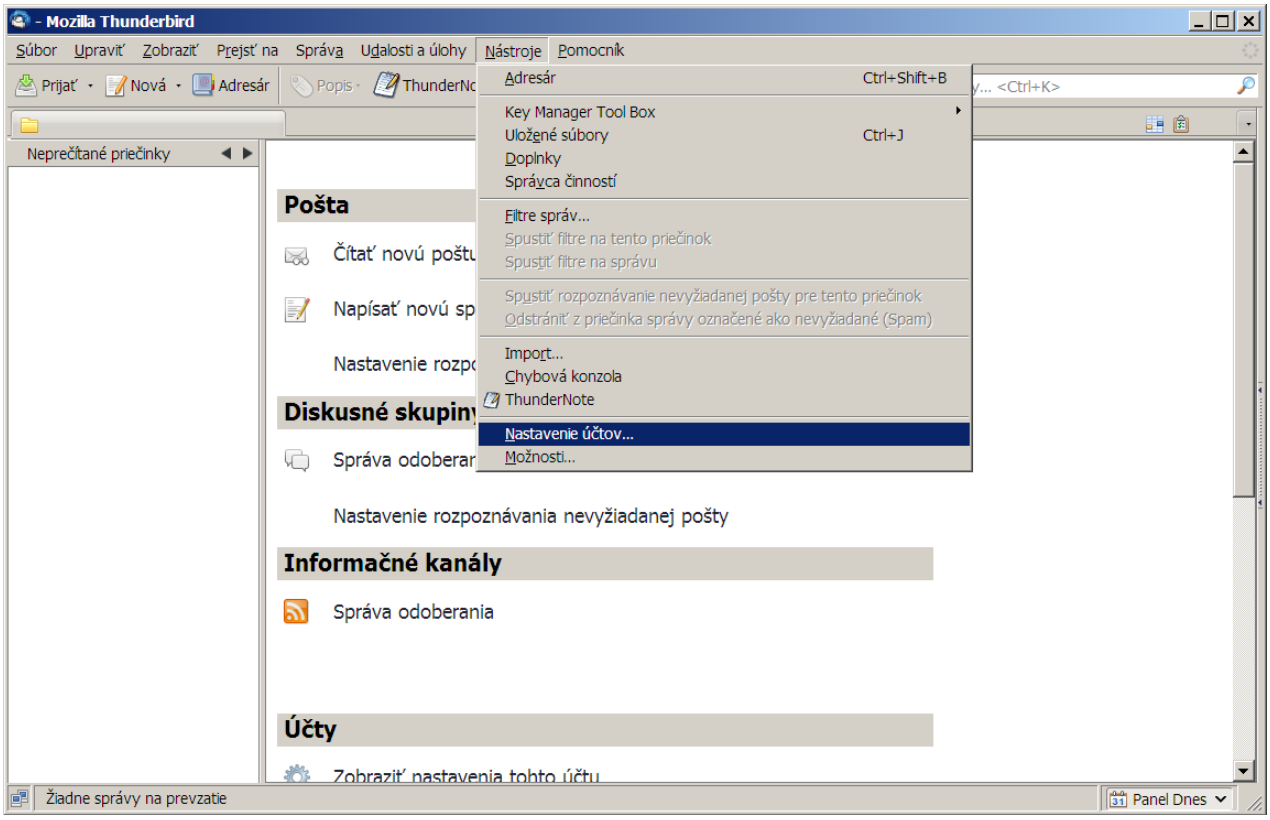
4. V okne "Správca certifikátov"zvoľte kartu "Vaše certifikáty" a overte že vaše certifikáty uložené na zariadení "GNT USB TOKEN" sú zobrazené.



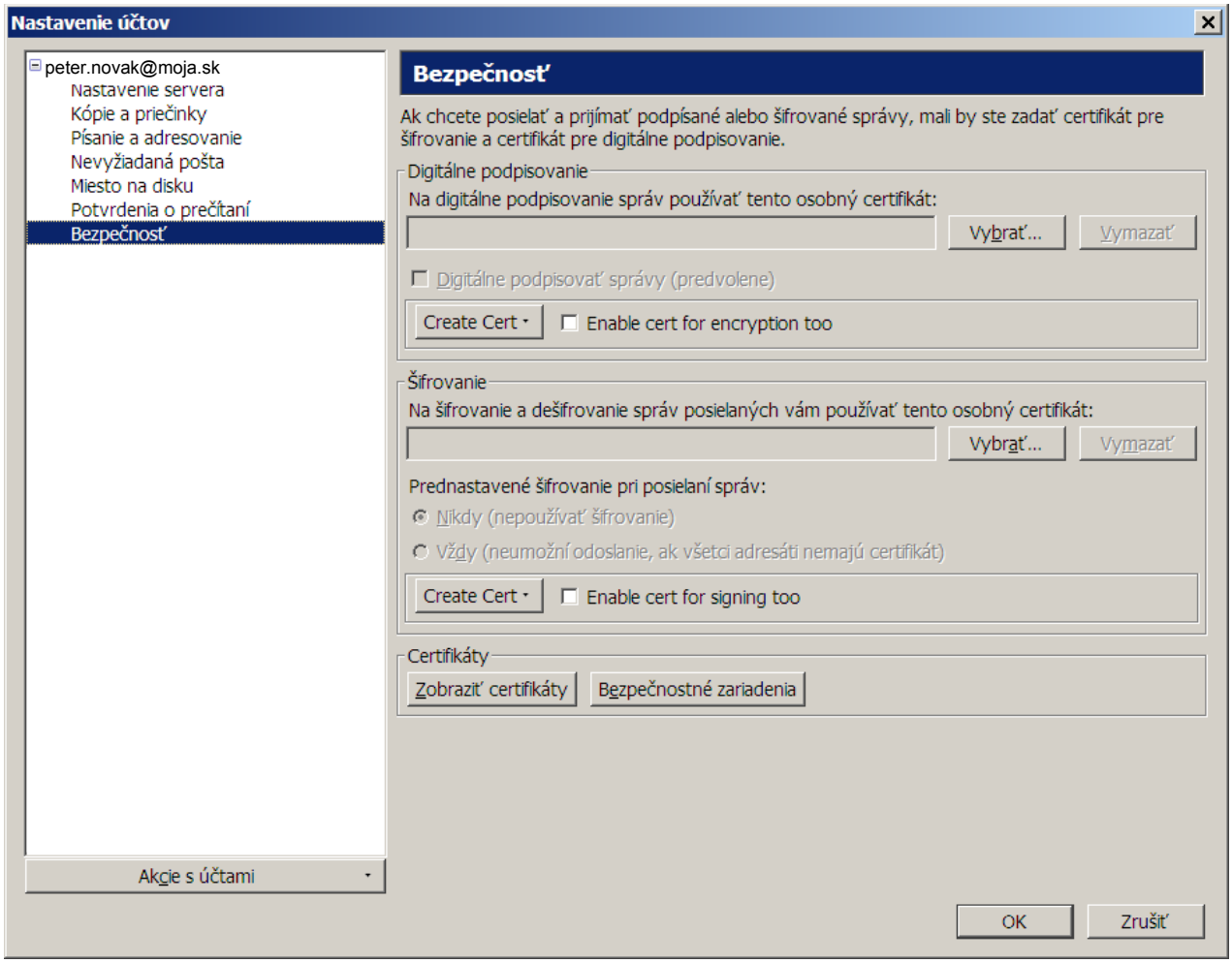
V závislosti od spôsobu, akým administrátor implementoval systém zabezpečenia, môže Váš Token obsahovať jeden, alebo dva vaše certifikáty. V prvom prípade sa ten istý certifikát použije na podpisovanie i šifrovanie správ. V druhom prípade je jeden z certifikátov určený na podpisovanie a druhý na šifrovanie správ.

4 Voľba certifikátov pre šifrovanie a podpisovanie správ

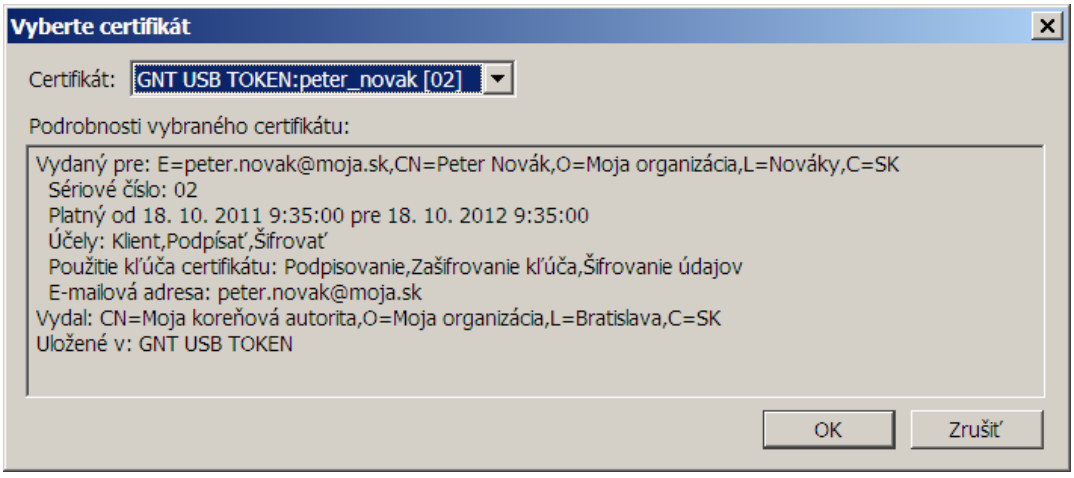
1. Zvoľte "Nástroje->Nastavenie účtov..."



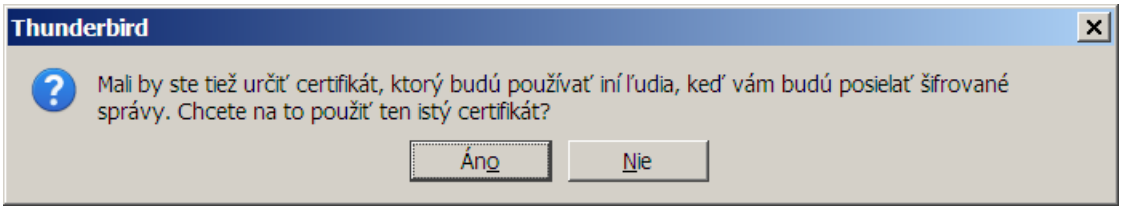
2. Zvoľte účet elektronickej pošty ktorý chcete zabezpečiť. E-mailová adresa účtu by sa mala zhodovať s adresou na vašom certifikáte uloženom na Tokene. Zvoľte kartu "Bezpečnosť".



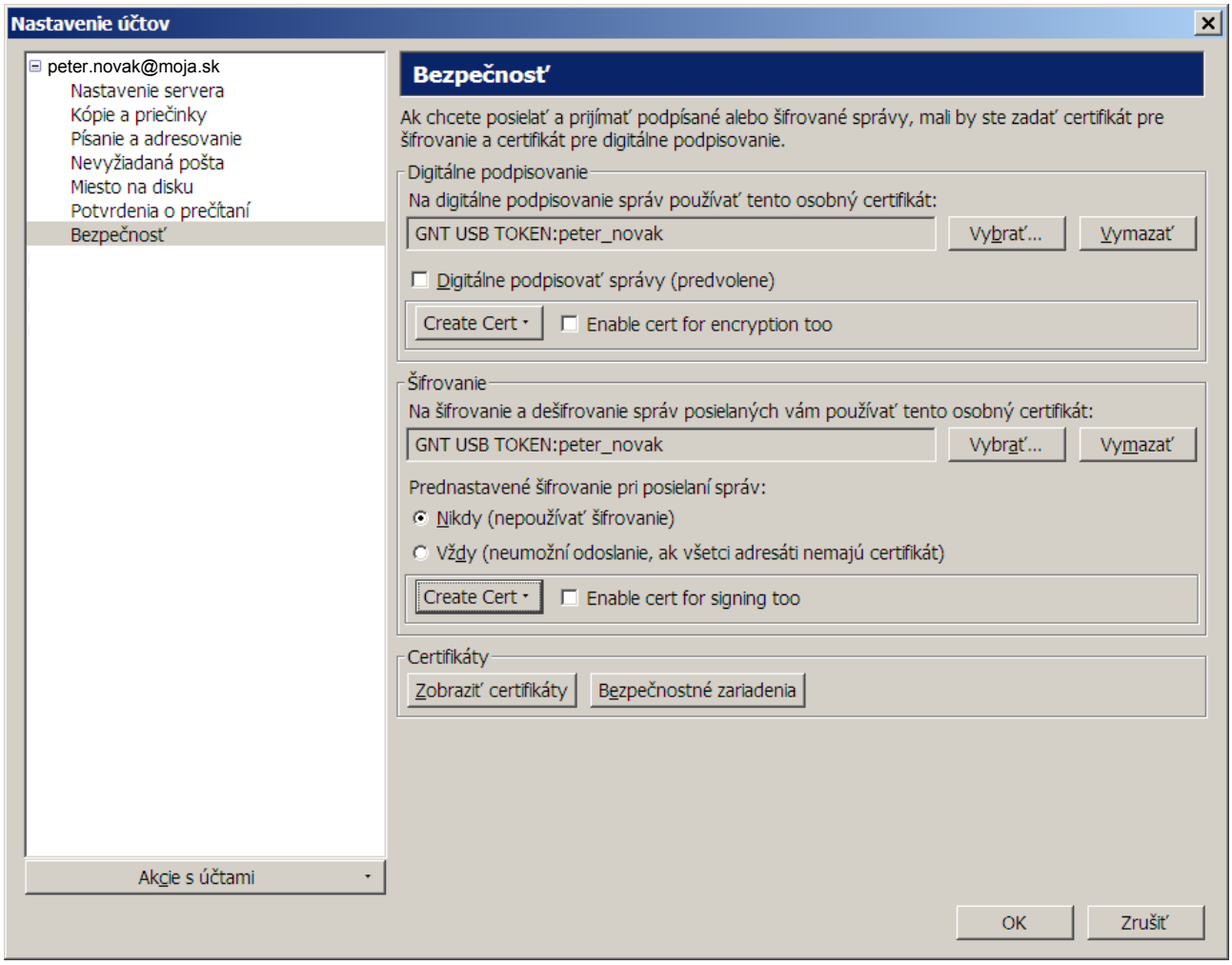
3. V poli "Digitálne podpisovanie" zvoľte tlačidlo "Vybrať". Systém Vám ponúkne vhodný certifikát uložený na bezpečnostnom zariadení GNT USB TOKEN. Potvrďte výber tlačidlom OK.



4. Poštový klient Vám ponúkne možnosť nastaviť ten istý certifikát i pre šifrovanie správ. Ak máte jeden certifikát pre podpisovanie i šifrovanie, zvoľte v nasledujúcom okne "Áno". Ak máte samostatné certifikáty pre podpisovanie a pre šifrovanie, zvoľte "Nie" a nastavte certifikát pre šifrovanie podľa bodu 5.



5. V poli "Šifrovanie" v okne "Nastavenie účtov" zvoľte tlačidlo "Vybrať". Systém Vám ponúkne vhodný certifikát uložený na bezpečnostnom zariadení GNT USB TOKEN. Potvrďte výber tlačidlom OK.
6. Úspešne ste zvolili certifikáty pre šifrovanie a podpisovanie správ. Tlačidlom "OK" zatvorte okno "Nastavenie účtov".



5 Distribúcia certifikátov

Pre zabezpečenie poštovej komunikácie s inými účastníkmi poštovej siete je potrebné, aby každý účastník vlastnil certifikáty svojich partnerov. Jednoduchý spôsob vzájomnej výmeny bezpečnostných certifikátov medzi dvoma účastníkmi je popísaný v nasledujúcom texte.

1. Vytvorte novú správu pre účastníka, s ktorým si chcete vymeniť certifikáty. Pred odoslaním správy kliknite na tlačidlo "Bezpečnosť" a označte voľbu "Digitálne podpísať túto správu" pre podpísanie správy (kapitola 6.1). Zašlite správu.

Poznámka: Túto úvodnú správu považujte za nezabezpečenú ! Keďže v tomto okamihu ešte nevlastníte certifikát Vášho partnera, nemôžete správu zašifrovať.

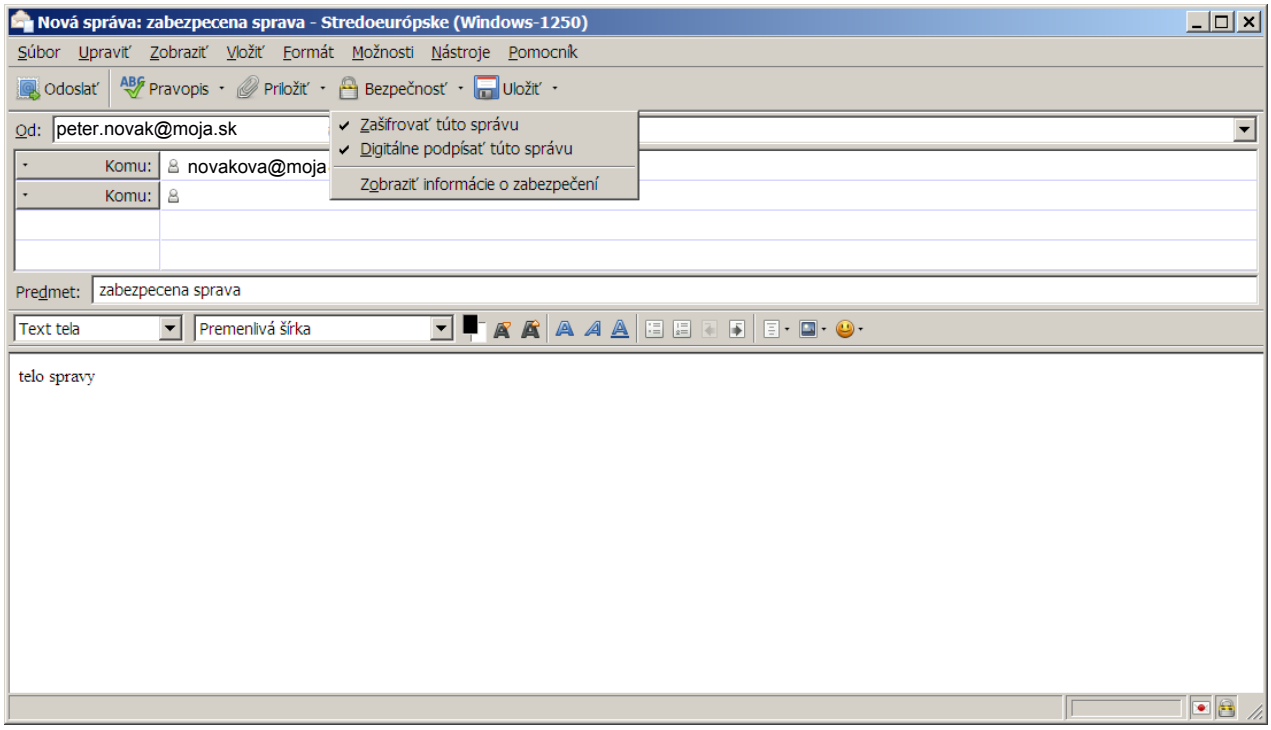
---

2. Partner príjme vami podpísanú správu. Keďže správa je podpísaná certifikátom vydaným dôverihodnou certifikačnou autoritou, poštový klient potvrdí, že správa je podpísaná a jej integrita nebola narušená. Zároveň poštový klient partnera automaticky uloží Váš certifikát do svojej databázy. Od tohoto okamihu Vám môže partner posielať zabezpečené správy.
3. Partner vytvorí pre Vás správu, zašifruje ju a podpíše. Váš poštový klient správu dešifruje a potvrdí, že je podpísaná a jej integrita nebola narušená. Zároveň Váš poštový klient automaticky uloží certifikát partnera do svojej databázy. Od tohoto okamihu je prevádzka zabezpečenej poštovej komunikácie s vaším partnerom automatická.

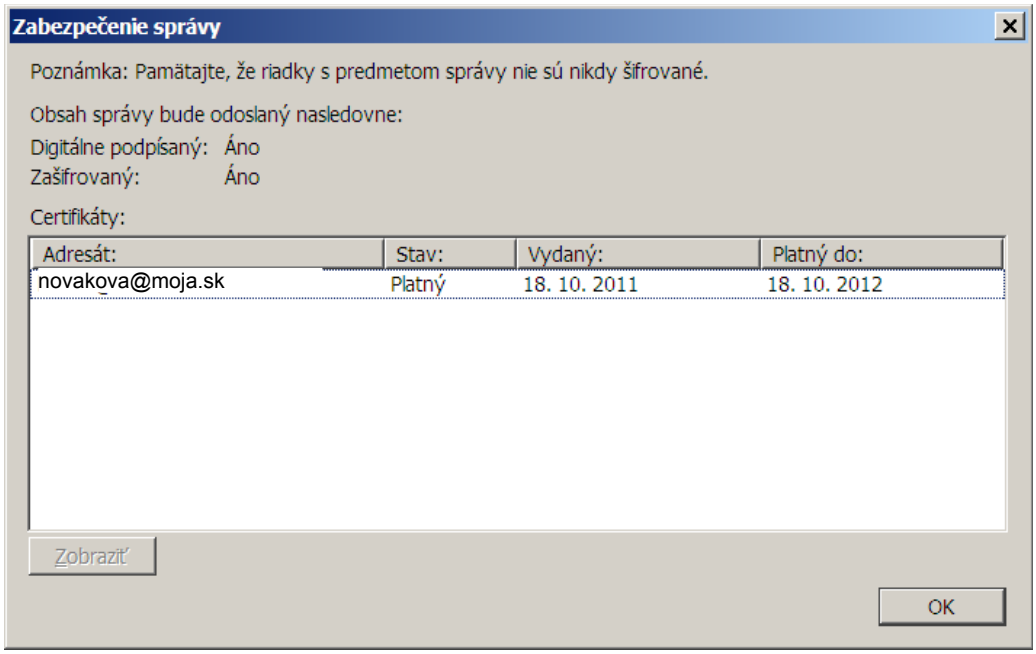
6 Zabezpečenie elektronickej pošty

6.1 Odoslanie zabezpečenej správy

1. Pred odoslaním správy kliknite na tlačidlo "Bezpečnosť" a označte voliče "Zašifrovať túto správu" pre zašifrovanie obsahu správy a "Digitálne podpísať túto správu" pre podpísanie správy.

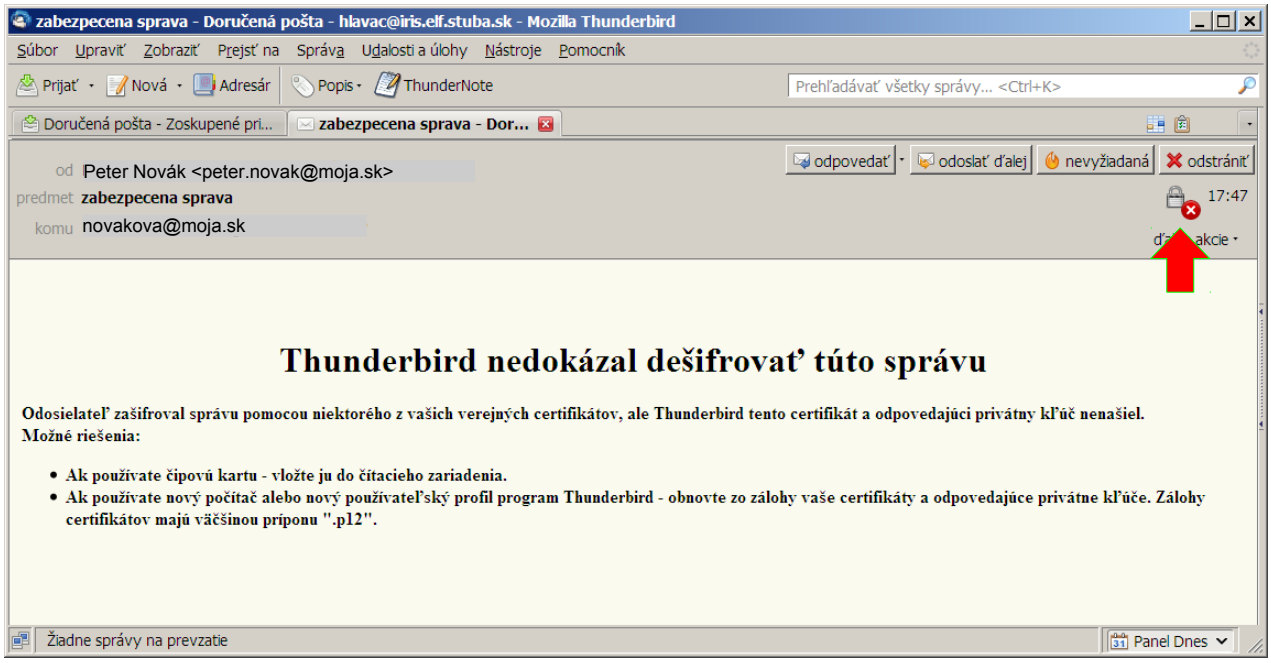


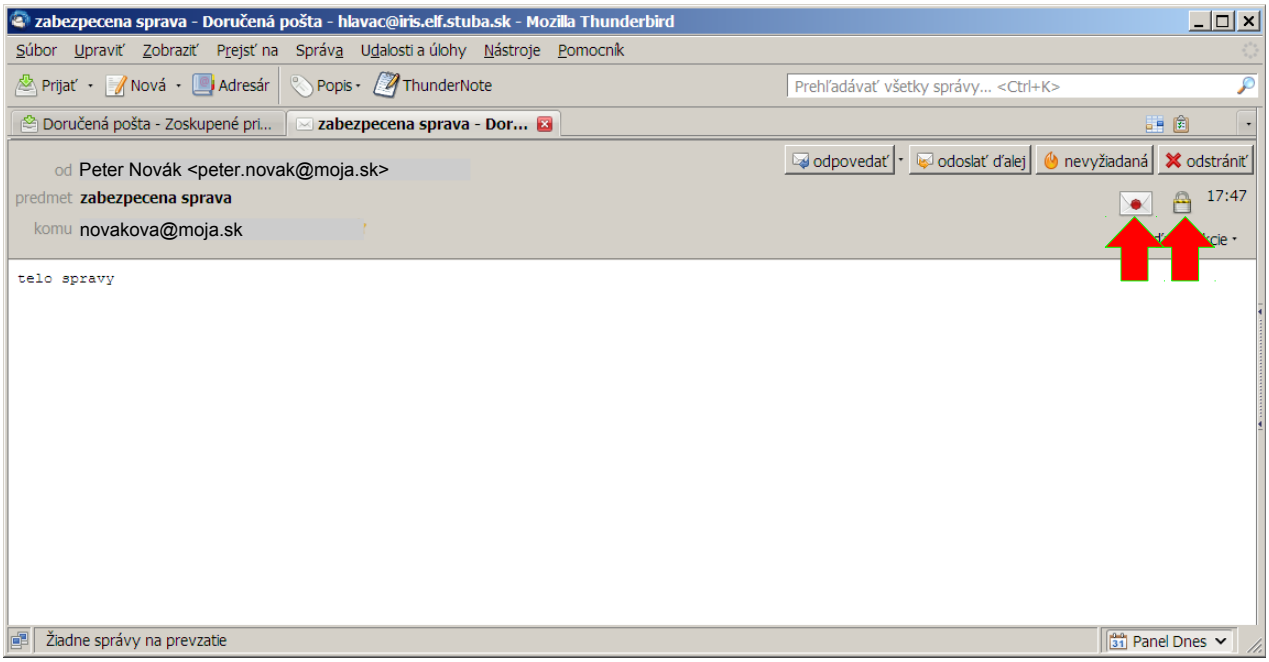
2. Po kliknutí na "Zobraziť informácie o zabezpečení" sa zobrazia informácie o zabezpečení odchádzajúcej správy. Overte, že správa bude podpísaná a zašifrovaná.



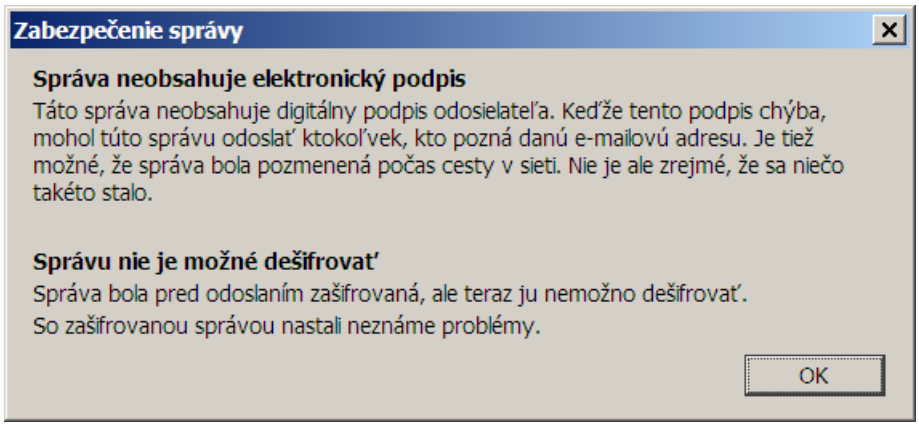
6.2 Príjem zabezpečenej správy

Dešifrovanie prijatej zabezpečenej správy a overenie jej integrity je automatické. O stave zabezpečenia informujú ikony v pravej hornej časti okna zobrazujúceho správu (na nasledujúcich dvoch obrázkoch označené šipkou).

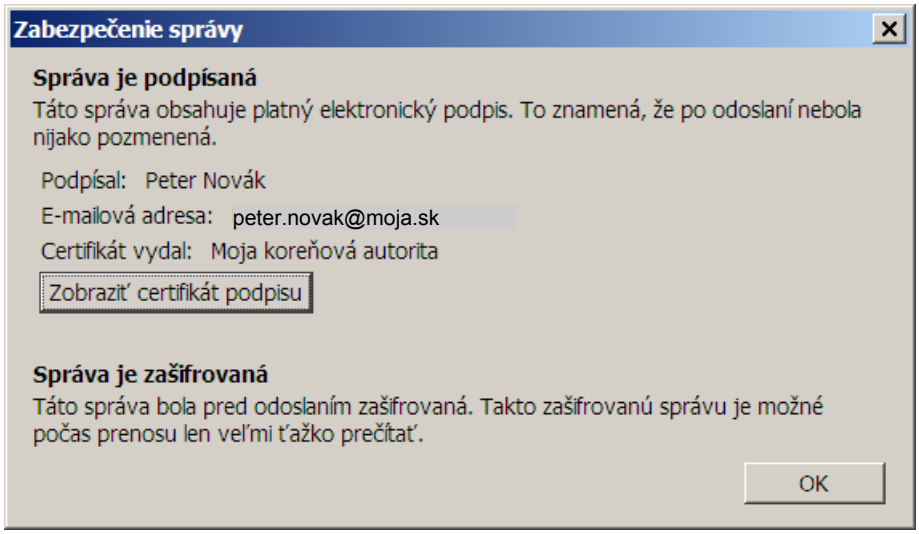




Po kliknutí na niektorú z týchto ikon sa zobrazí podrobný výpis o stave zabezpečenia správy. Ak správu nemožno dešifrovať a/alebo nieje možné overiť jej integritu, výpis má obsah ako na nasledujúcom obrázku.



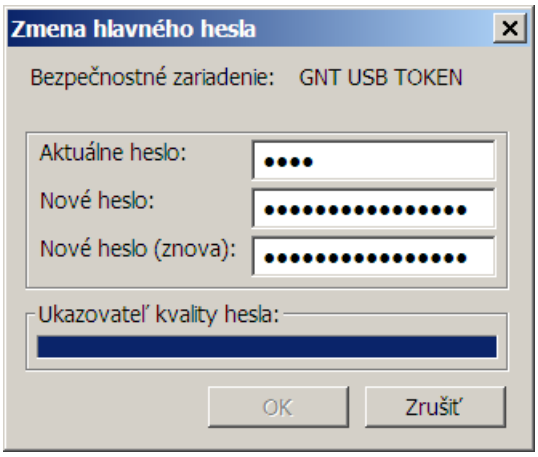
Ak bola správa úspešne dešifrovaná a jej integritu bola overená, výpis má obsah ako na nasledujúcom obrázku.



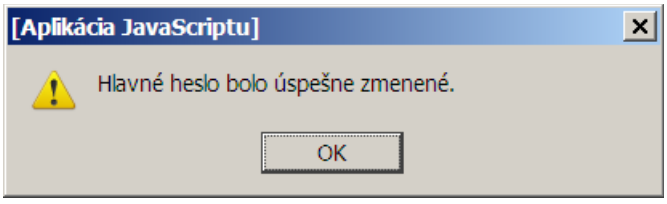
Poznámka: Pre správne dešifrovanie a overenie integrity prijatej zabezpečenej správy je potrebné, aby bol Váš Token pripojený k počítaču.

7 Zmena prístupového hesla k Tokenu

1. Otvorte okno "Správca bezpečnostných zariadení", zvoľte Váš GNT USB Token a stlačte tlačidlo "Zmeniť heslo". Vyplňte aktuálne a nové heslo. Stlačte OK.



2. O úspešnej zmene hesla budete informovaný nasledujúcim oknom.



8 Dokumentácia

1 GNT USB Token - dátový list, SoftIdea, s.r.o. , Máj 2011, http://www.softidea.sk/gnt_datasheet_sk.pdf

SoftIdea s.r.o.
Sliačska 10, 831 02 Bratislava
tel.: +421 2 444 60 444
fax.: +421 2 446 40 441
http://www.softidea.sk
info@softidea.sk