

## Odesílání citlivých dat prostřednictvím šifrovaného emailu s elektronickým podpisem standardem S/MIME

Je dostupnou možností, jak lze zaslat lékařskou dokumentaci elektronicky.

### Co je třeba k odeslání šifrovaného emailu?

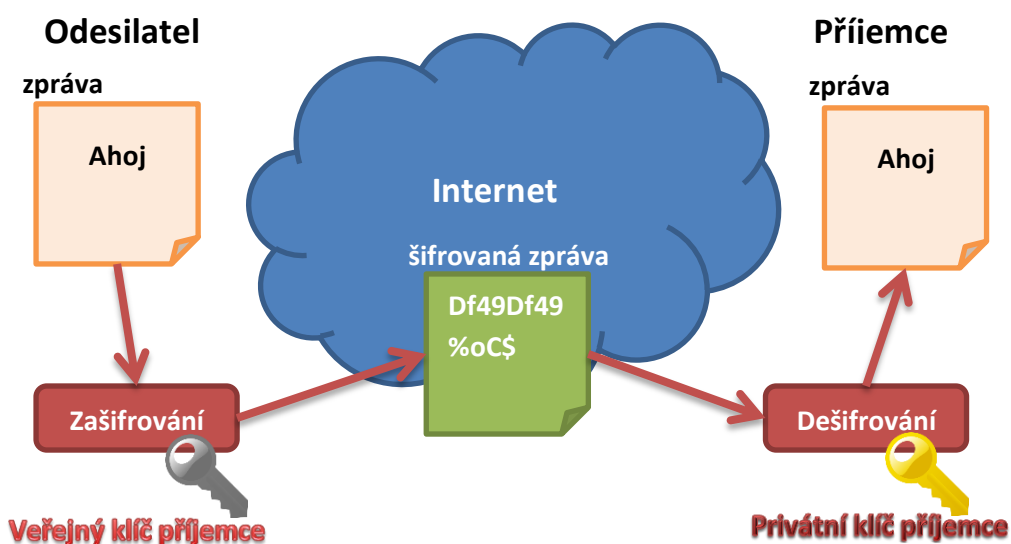
- Emailový klient s podporou šifrování
- Certifikát příjemce s veřejným klíčem určený k šifrování (mnohdy označován jako komerční či standardní) – běžně dostupný automaticky z komunikace elektronicky podepsané příjemcem, někdy dostupný ke stažení z webových stránek příjemce ve formě souboru k importu.

### Co je třeba k elektronickému podepsání emailu?

- Emailový klient s podporou elektronického podpisu
- Osobní certifikát s privátním klíčem, vzhledem k současné legislativě ideálně kvalifikovaný, a emailový účet s tímto certifikátem provázaný

### Jaký je princip šifrování S/MIME v elektronické poště?

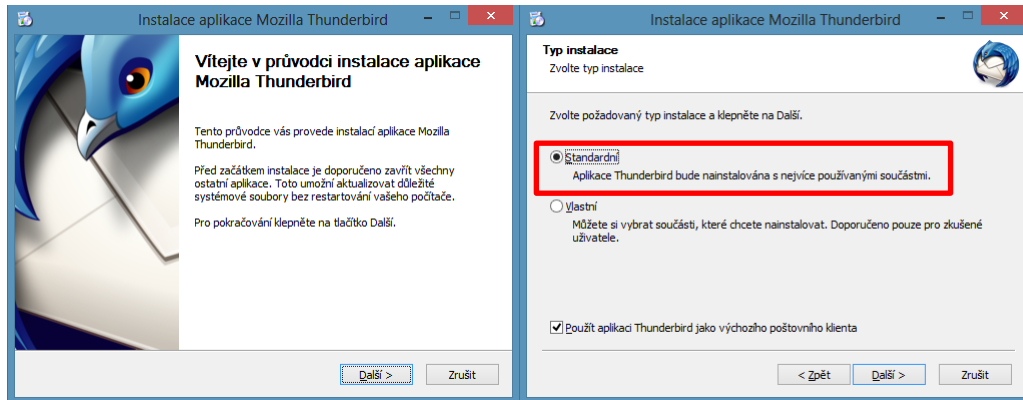
Odesílatel potřebuje k odeslání veřejný klíč příjemce, kterým zprávu zašifruje. Vše se děje zcela automaticky v poštovním klientu po příslušném nastavení. Šifrovaná zpráva následně putuje internetem jako každý jiný email. K jejímu přečtení je však potřeba privátní klíč příjemce. Příjemce, který tento klíč, má zobrazí zprávu dešifrovanou jako kterýkoli jiný email, pokud má správně nastavený poštovní klient.



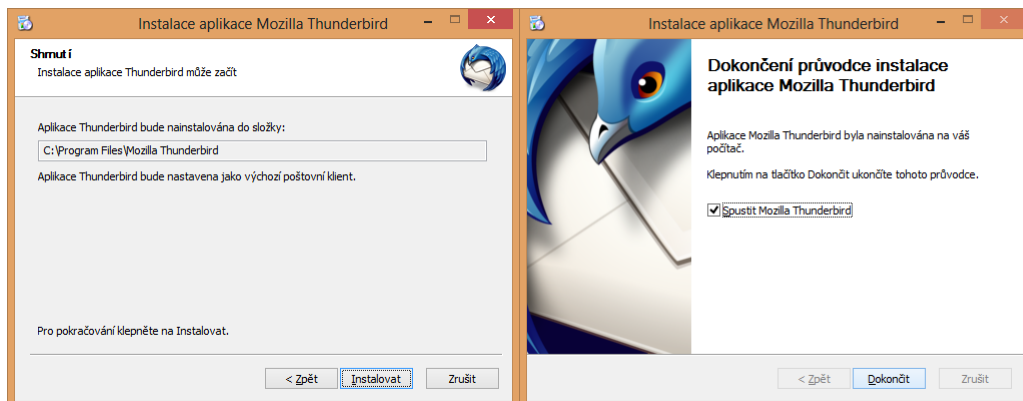
## Instalace a nastavení poštovního klienta Thunderbird

Thunderbird je zdarma dostupný poštovní klient, který má veškerou potřebnou funkcionalitu pro elektronický podpis a šifrování standardem S/MIME.

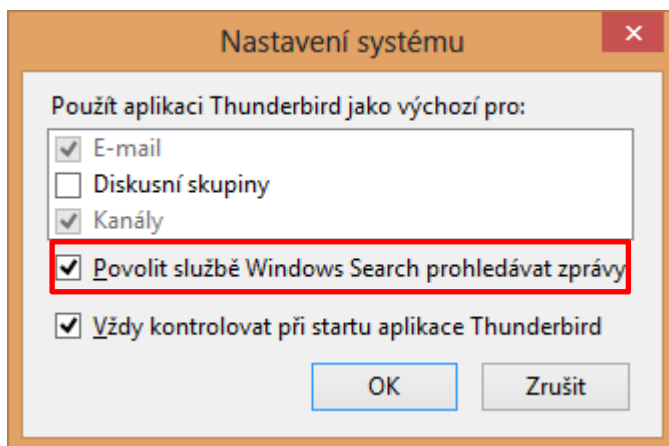
- Poslední verze je ke stažení na adrese: <http://thunderbird.mozilla.cz/>



Při instalaci je zcela dostačující zvolit *Standardní* typ a postupně po projití průvodce instalaci dokončit.



Po instalaci se systém zeptá, zda má být Thunderbird výchozím poštovním klientem. Pokud chcete, aby vyhledávání ve Windows prohledávalo zprávy, zvolte *Povolit službě Windows Search prohledávat zprávy*





Následně se objeví průvodce nastavením účtu, vyberte *Přeskočit průvodce a použít existující e-mail*.

Vítejte v aplikaci Thunderbird

### Chtěli byste novou e-mailovou adresu?

Vaše jméno nebo přezdívka

Ve spolupráci s řadou poskytovatelů vám Thunderbird umožní založit si vlastní poštovní účet. Do pole výše vložte prosím vaše křesné jméno a příjmení nebo jakéholiv jiné slovo, které se vám líbí.

 gandi.net   Hover.com

Zadané výrazy jsou odesílány na servery Mozilly ([Zásady ochrany soukromí](#)) a poskytovatelům pošty gandi.net ([Zásady ochrany soukromí](#), [Podmínky služby](#)) a Hover.com ([Zásady ochrany soukromí](#), [Podmínky služby](#)) za účelem nelezení dostupných adres.

V okně, které se zobrazí, zadejte Vaše jméno, které bude zobrazeno v emailové zprávě v kolonce odesílatel a následně zadejte Váš email a heslo. V případě většiny obecně dostupných emailových služeb proběhne nastavení Vašeho účtu zcela automaticky.

Pokud se tak nestane, obraťte se na provozovatele Vašeho emailového účtu s prosbou o nastavení poštovního klienta ideálně na protokol **IMAP**. Většinou mají poskytovatelé emailových služeb podrobné návody pro nastavení jednotlivých klientů na svých webových stránkách.

Založení poštovního účtu

Vaše jméno:  Vaše jméno tak, jak se bude zobrazovat ostatním.

E-mail:

Heslo:

Památovat si heslo

**Založení poštovního účtu** ✕

Vaše jméno:  Vaše jméno tak, jak se bude zobrazovat ostatním.

E-mail:

Heslo:

Pamatovat si heslo

Mezi poskytovateli v databázi Mozilly bylo nalezeno následující nastavení

IMAP (vzdálené složky)  POP3 (místní uložení pošty)

Příchozí IMAP, imap.googlemail.com, SSL


Odchozí SMTP, smtp.googlemail.com, SSL

Uživatelské jméno mudr.tomas.nosek@gmail.com

Získat nový účet

Pokud se Vám po potvrzení nastavení objeví výzva ke schválení bezpečnostní výjimky, tuto klidně schvalte a zvolte *Uložit tuto výjimku trvale*. Znamená to pouze, že certifikát či certifikační autorita Vašeho poskytovatele emailových služeb není v emailovém klientovi označena jako důvěryhodná (více viz níže).

**Přidání bezpečnostní výjimky** ✕

 Chystáte se změnit způsob, jakým aplikace Thunderbird identifikuje tento server.  
**Legitimní banky, obchody a ostatní veřejné servery vás o toto žádat nebudou.**

Server

Adresa:

Stav certifikátu

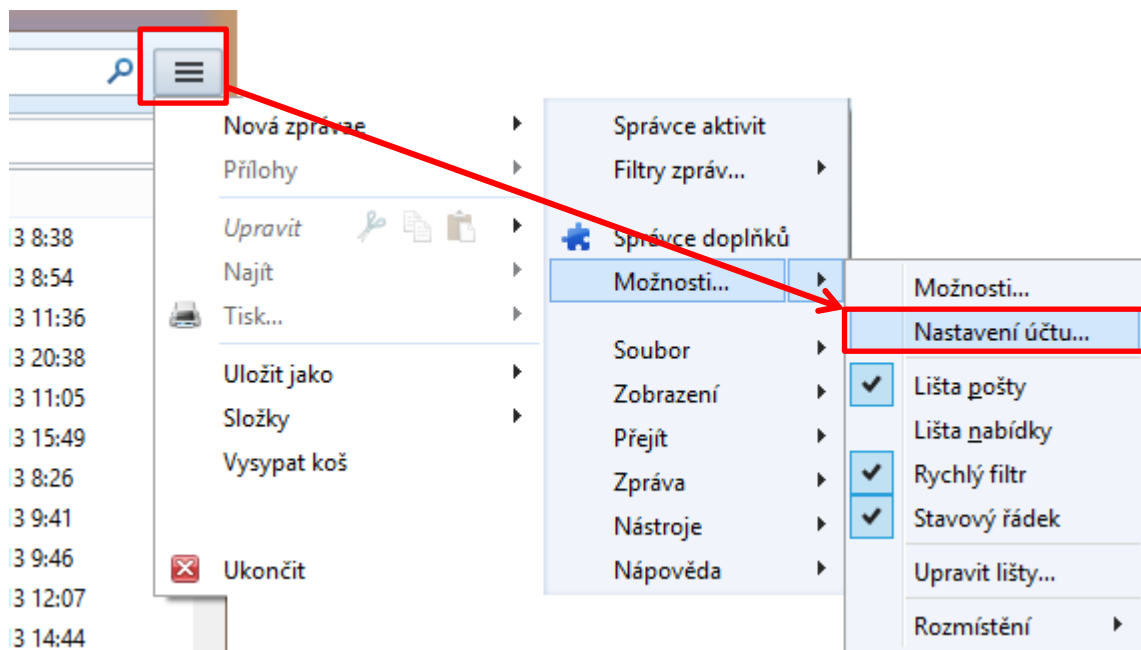
Tento server se prokazuje neplatnými informacemi.

**Neznámá identita**

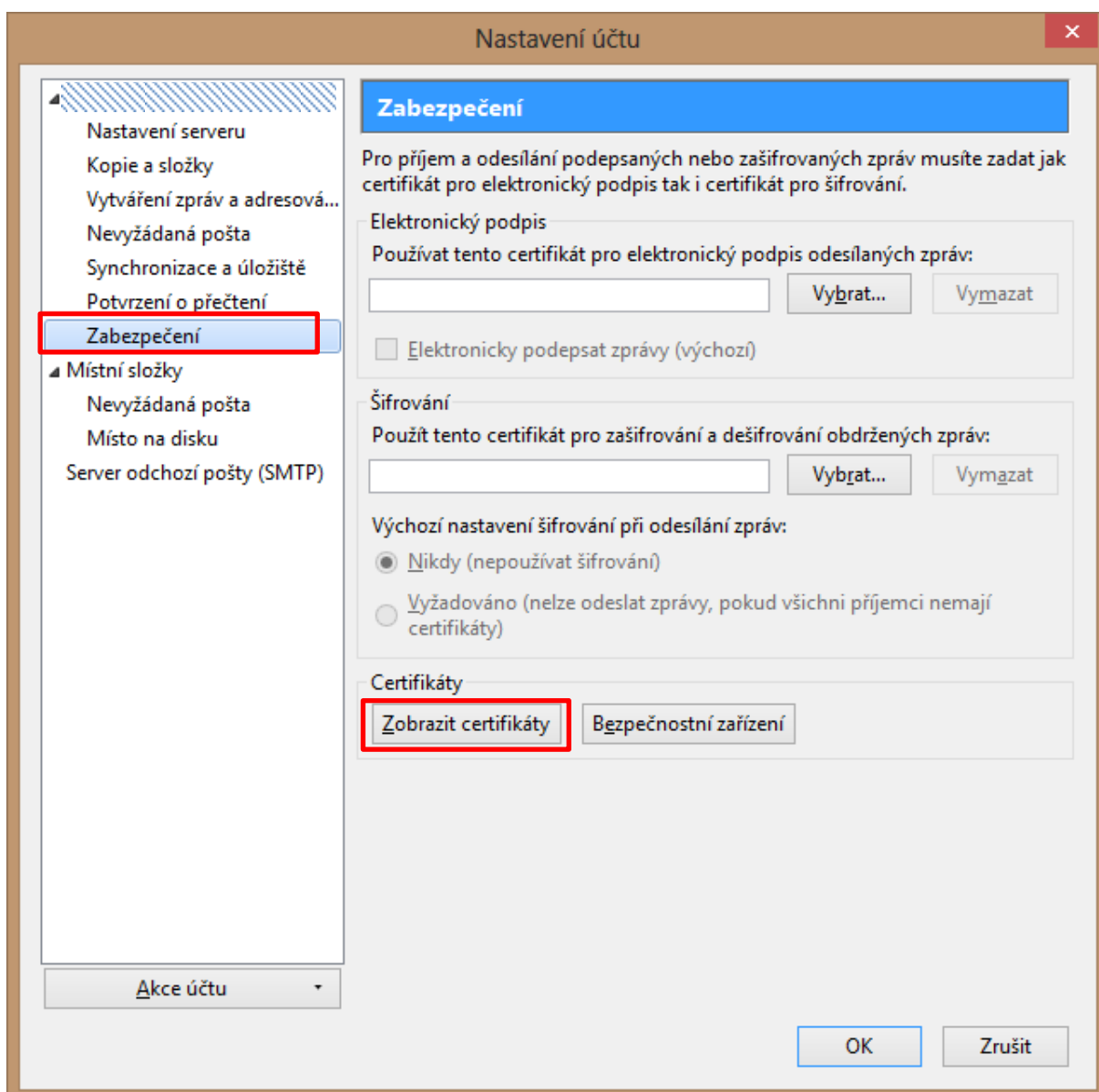
Certifikát je nedůvěryhodný, protože nebyl ověřen důvěryhodnou autoritou pomocí bezpečného podpisu.

Uložit tuto výjimku trvale

Nyní, když máte účet nastaven, je třeba přidat nastavit elektronický podpis a šifrování. Menu klienta (tlačítko se třemi čárkami vedle vyhledávacího okna) vyberte volbu *Možnosti* → *Nastavení účtu*.



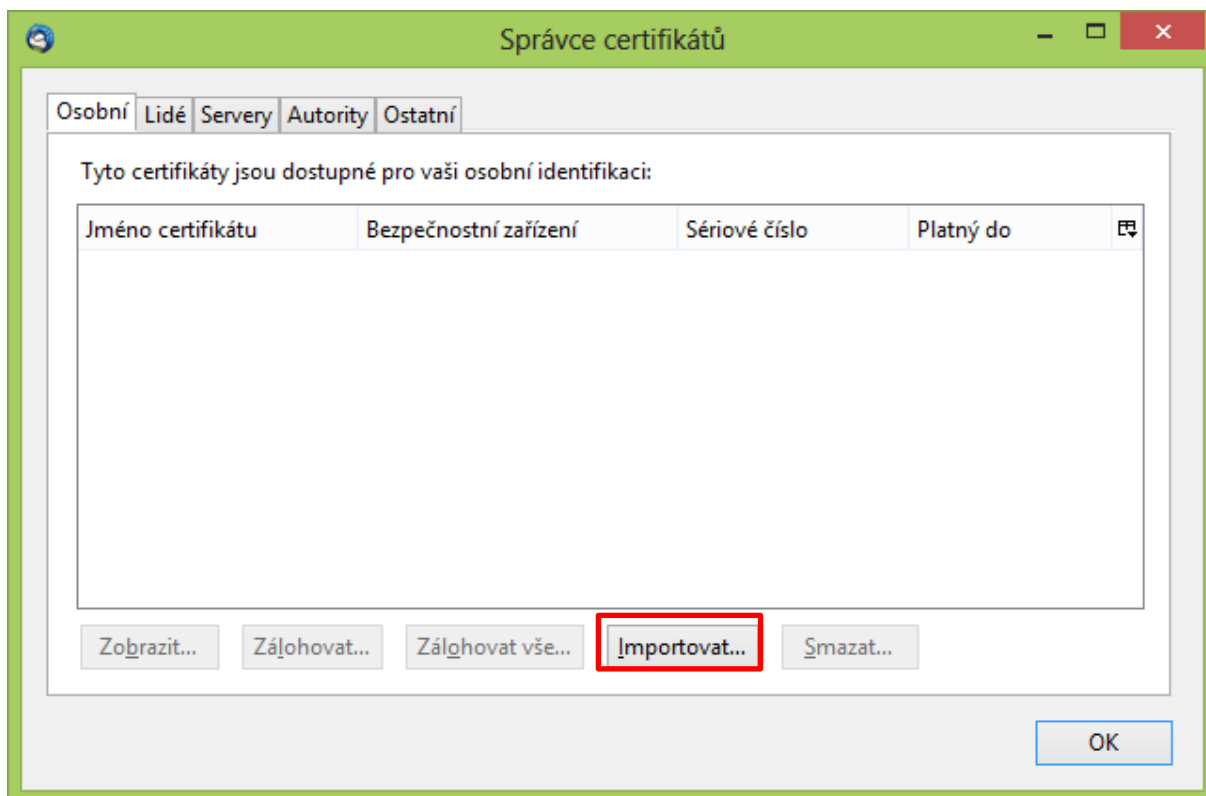
V menu *Nastavení účtu* vyberte účet, který jste vytvořili a zvolte *Zabezpečení*. Jelikož Thunderbird není propojen s centrálním úložištěm certifikátů ve Windows, bude třeba nejdříve importovat osobní certifikáty s privátním klíčem pro podpis a šifrování. V našem ukázkovém případě nastavíme pro podpis certifikát kvalifikovaný a pro šifrování certifikát komerční. Zvolte tedy v menu *Zabezpečení* tlačítko *Zobrazit certifikáty*, čímž se dostanete do *Správce certifikátů*.



Ve *Správci certifikátů* jsou jednotlivé certifikáty rozděleny podle typu. V našem případě jsou důležité záložky *Osobní*, kde jsou uloženy certifikáty s privátním klíčem určené k podpisu. Záložka *Lidé* obsahuje certifikáty s veřejným klíčem od ostatních korespondenčních partnerů. V případě, že je přichází email podepsán, a příslušný certifikát od korespondenčního partnera je platný, tak je automaticky uložen, alternativně je možnost certifikáty korespondenčních partnerů naimportovat. Poslední záložkou, která je v souvislosti s elektronickým podepisováním a šifrováním emailů zajímavá, je záložka *Autority*. Zde se nacházejí **kořenové certifikáty** certifikačních autorit. V případě, že přijde email podepsaný elektronickým podpisem vydaným danou autoritou, musí být certifikát této autority dostupný v záložce *Autority* a musí být označen jako důvěryhodný, jinak emailový klient hlásí problém s elektronickým podpisem.

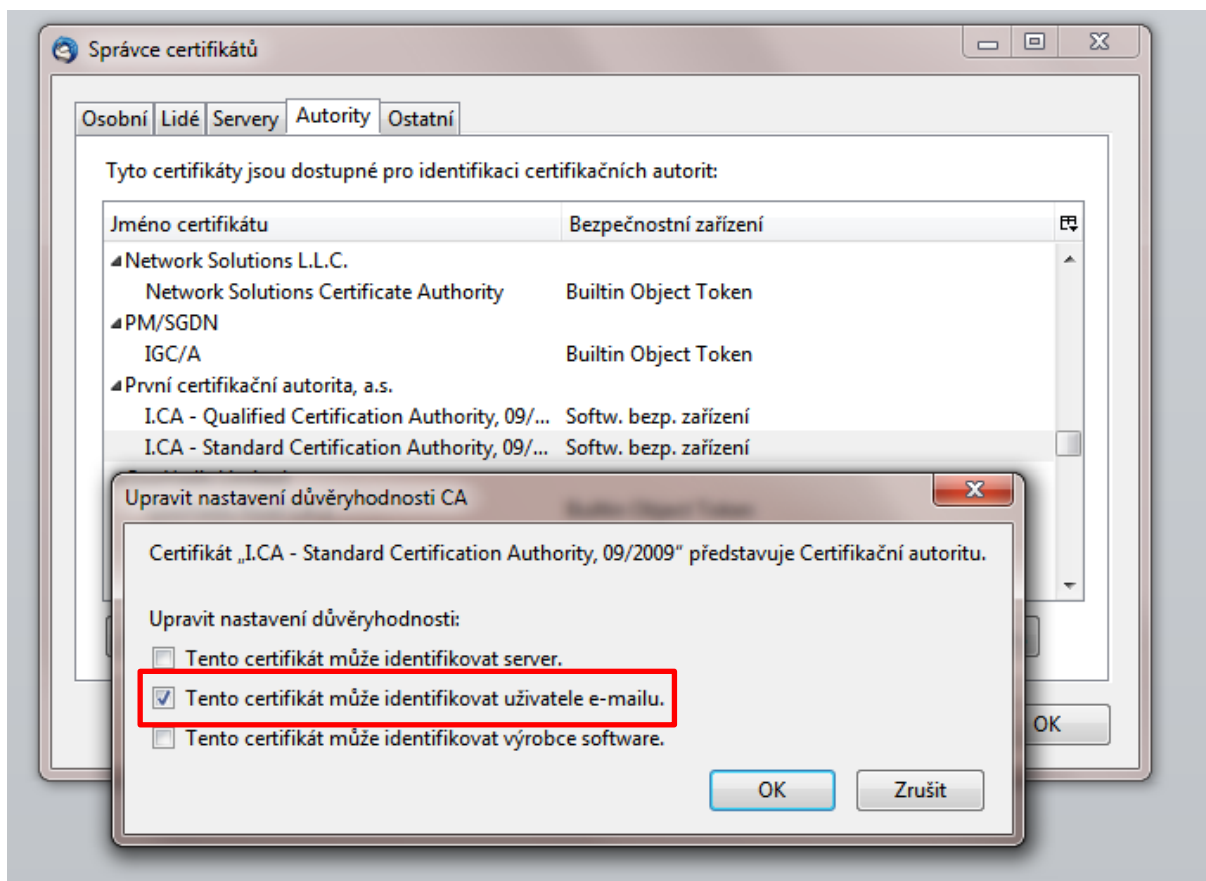
Aby bylo možné emaily elektronicky podepisovat a šifrovat, je třeba importovat **kvalifikovaný certifikát s privátním klíčem pro podpis** a **komerční certifikát s osobním klíčem pro šifrování** (kvalifikovaný certifikát nelze k zašifrování zprávy použít).

Import certifikátu se provede po stisknutí tlačítka *Importovat* v dolní části příslušné záložky v okně *Správce certifikátů*.



Poslední věcí k úspěšnému nastavení certifikátů pro podpis a šifrování je kontrola, zda jsou dostupné **kořenové certifikáty certifikační authority**, která vydala importované osobní certifikáty. Zároveň musí být tento certifikát nastaven jako **důvěryhodný**. **Všechny certifikační authority mají kořenové certifikáty běžně dostupné ke stažení na svých webových stránkách.**

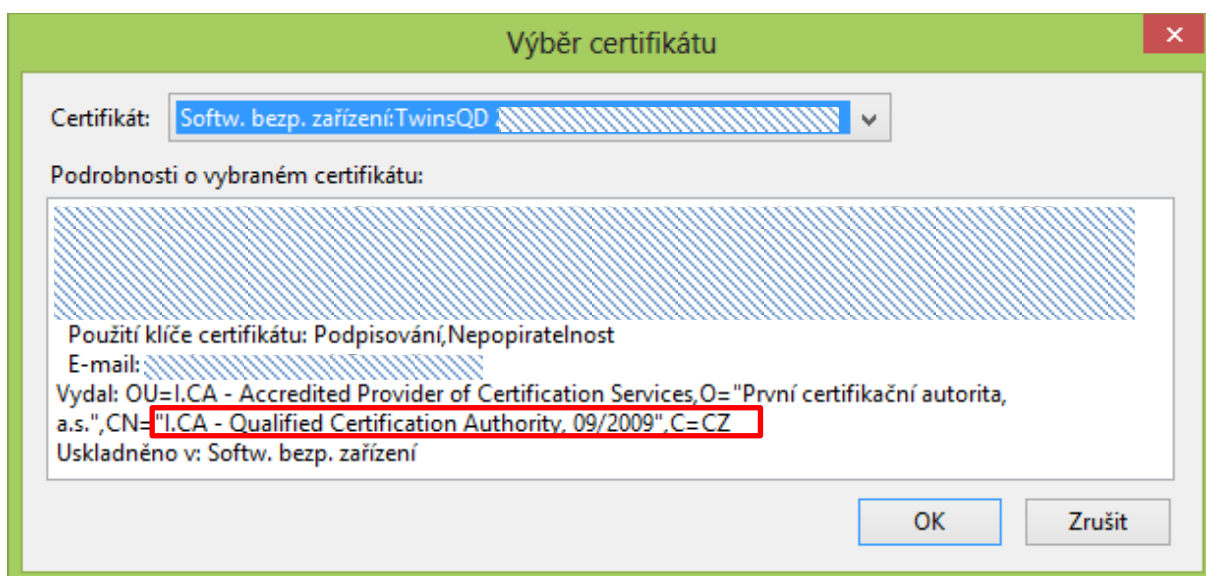
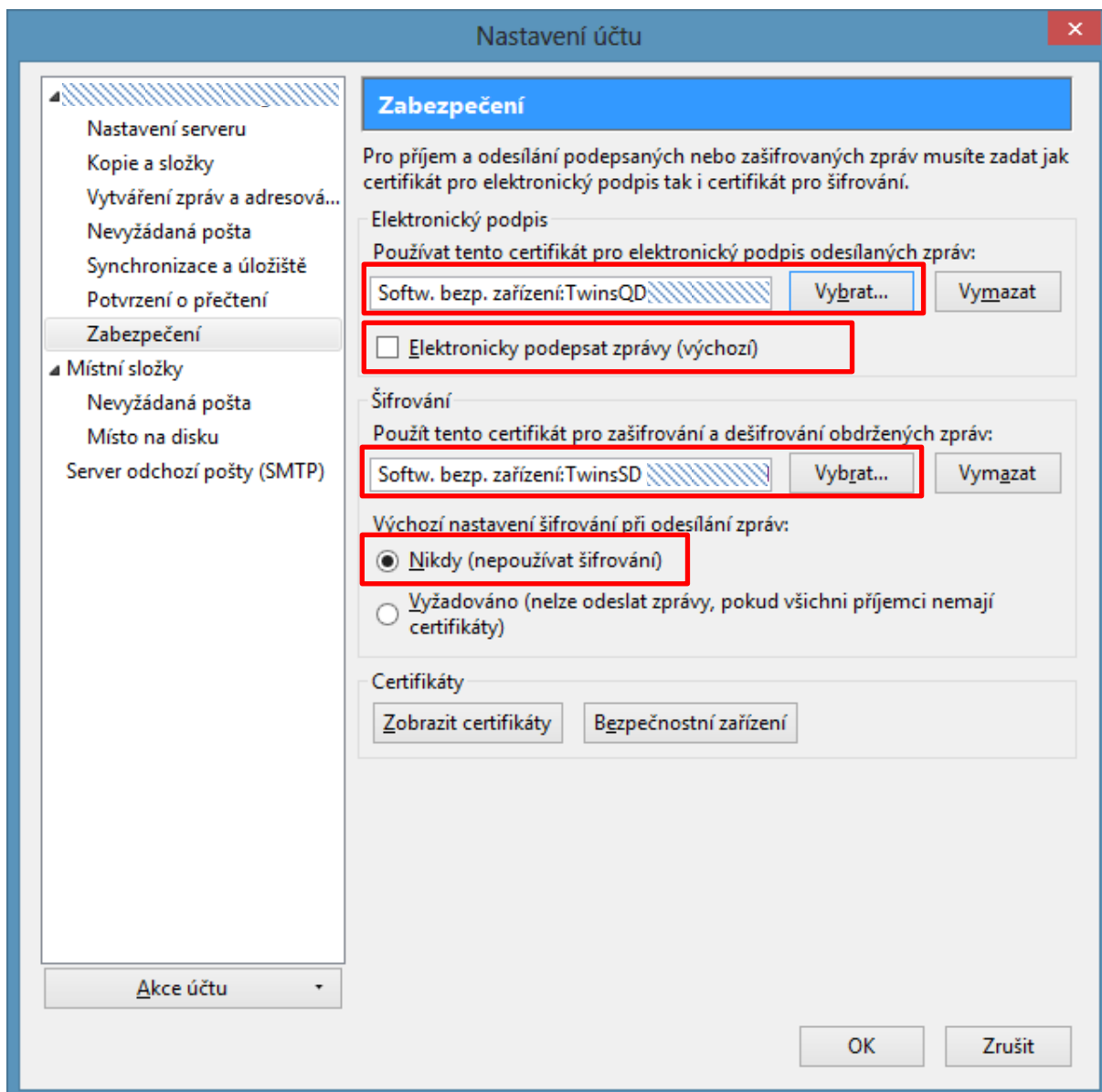
V záložce *Authority* zkontrolujte, zda jsou dostupné kořenové certifikáty authority, která vydala importované osobní certifikáty. V případě, že dostupné nejsou, což v případě lokálních českých certifikačních autorit není výjimkou, je třeba je nainportovat. V dolní části záložky *Authority* je opět umístěno tlačítko *Importovat*. Po importu pro jistotu zkontrolujte nastavení důvěryhodnosti tlačítkem *Upravit důvěru*. V okně, které se objeví, zkontrolujte, zda je zaškrtnuto *Tento certifikát může identifikovat uživatele emailu* a případně zaškrtněte i ostatní volby dle potřeby a potvrďte stisknutím tlačítka *OK*. Nyní můžete *Správce certifikátů* ukončit s potvrzením změn stisknutím tlačítka *OK*.



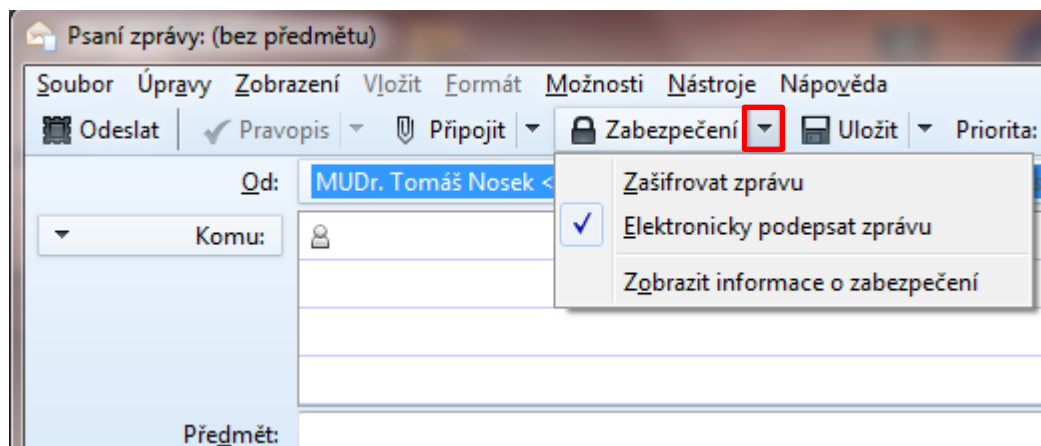
V nastavení poštovního účtu ve volbě *Zabezpečení* vyberte **kvalifikovaný certifikát pro elektronický podpis a komerční pro šifrování**. Email lze podepsat i komerčním certifikátem, ale aby elektronický podpis splňoval požadavky současné legislativy pro zaručený elektronický podpis, je třeba použít certifikát kvalifikovaný. Při výběru certifikátu se Vám zobrazí okno s výběrem dostupných informací v jehož dolní části jsou veškeré podrobnosti o certifikátu včetně toho zda jde o certifikát komerční či kvalifikovaný.

Dále můžete nastavit, zda chcete implicitně elektronicky podepisovat všechny zprávy, což vřele doporučuji, protože na to nebude třeba myslet při odesílání každého emailu, a zda je chcete šifrovat. V případě nastavení šifrování emailu však implicitní nastavení nedoporučuji, protože minimálně z počátku zcela jistě nebudete mít certifikáty s veřejným klíčem od korespondenčních partnerů.

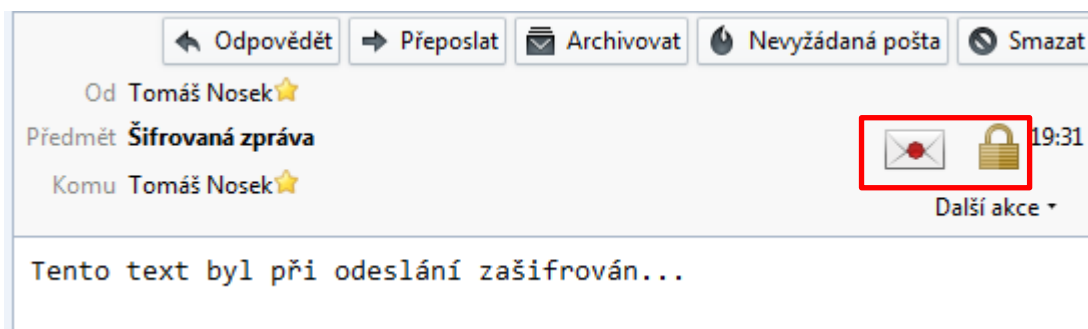




Při odesílání emailu můžete nastavení podpisu a šifrování nastavit a měnit v okně odesílané zprávy po stisknutí šipky dolů u tlačítka zabezpečení.



V případě, že Vám přijde email opatřený elektronickým podpisem, Thunderbird informaci zobrazí ikonou zapečetěné obálky v pravé části záhlaví zprávy. Pokud byl navíc email šifrován, zobrazí se vedle ikony dopisu navíc ještě ikona zámku.



V emailovém klientu, který neobsahuje certifikát pro dešifrování je obsah zprávy viditelný pouze jako soubor přílohy *smime.p7m*, stejně tak je zobrazen i ve webovém rozhraní většiny emailových služeb.

