Podepisování elektronické pošty (Mozzila Thunderbird)

Podepisování e-mailu je proces, při kterém dojde k vytvoření hashe z e-mailové zprávy a tento hash (délka závisí na použitém algoritmu, např. SHA-1...160bitů) je zašifrován privátní částí asymetrického klíče (ve většině případů algoritmus RSA). Podpis (zašifrovaný hash) je připojen ke zprávě. Verifikace podpisu probíhá u příjemce porovnáním hashe došlé zprávy a hashe, který se dešifruje z elektronického podpisu pomocí veřejné části asymetrického klíče použitého při podpisu.

Asymetrický klíč pro elektronický podpis je spojen s identitou uživatele nebo počítače pomocí certifikátu. Z něj lze vyčíst informace o uživateli, typu certifikátu, certifikační autoritě (CA), která jej vydala a podobně.

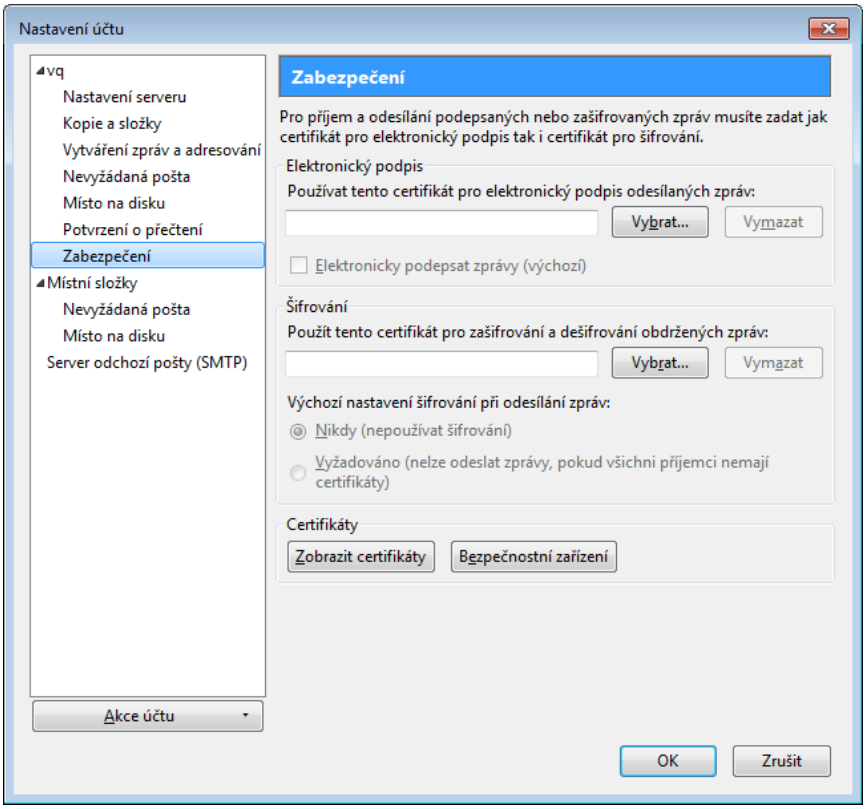
Co je potřeba:

- Autentizační token (eToken PRO 72k, iKey 4000)
- SafeNet Authentication Client 8.0 a vyšší (middleware pro podporu tokenů)
- Certifikát umožňující digitální podpis e-mailu
- Emailový klient Mozzila Thunderbird

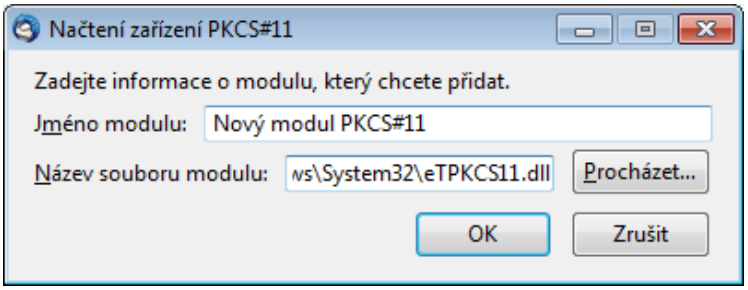
Postup:

1) Vygenerování páru RSA klíčů na tokenu, vytvoření žádosti o certifikát a vydání certifikátu na token.
   Tento proces může být proveden u místní (např. firemní) certifikační autority nebo u externí, akreditované CA. V obou případech je třeba zajistit, aby byl nastaven minimálně parametr Key Usage Extension v šabloně certifikátu na „Digital Signature“ (šablona může obsahovat i více použití). Zároveň je nutné při generování žádosti vyplnit e-mailovou adresu, ke které bude certifikát vydán.

2) Otevřete e-mailového klienta Mozzila Thunderbird. V menu vyberte Nástroje a Nastavení účtu. V otevřené kartě zvolte Zabezpečení.

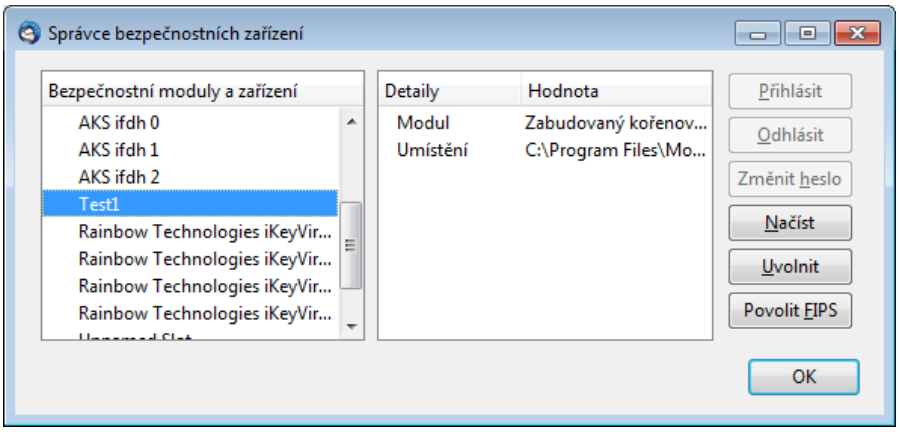


3) Nejprve je potřeba zvolit PKCS#11 knihovnu Safenet, která zprostředkuje komunikaci tokenu/karty a poštovního klienta. Klikněte na tlačítko Bezpečnostní zařízení.
Zde zvolte Načíst, objeví se podobné okno:



Vyberte knihovnu eTPKCS11.dll, kterou najdete zpravidla pod C:\Windows\System32\

4) Měly by se načíst USB čtečky, případně názvy vložených tokenů (zde „Test1“)



5) Na kartě Zabezpečení (viz bod 2) Vyberte příslušný certifikát pro Elektronický podpis případně pro Šifrování. Dále je někdy nutné certifikační autoritu (CA), která vydala Váš certifikát pro podpis, nastavit v Thunderbirdu (Mozzile) jako důvěryhodnou (např. importem certifikátu CA mezi Autority).