Podepisování elektronické pošty (MS Outlook)

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.

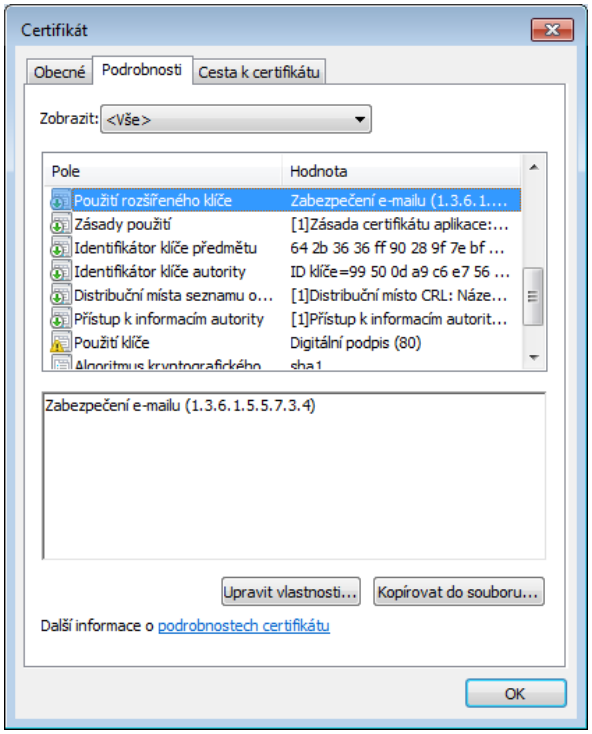
Asymetrický klíč pro elektronický podpis je spojen s identitou uživatele nebo počítače pomocí certifikátu. Z něj lze vyčíst informace o uživateli, typu certifikátu, certifikační autoritě (CA), která jej vydala a podobně.

Co je potřeba:

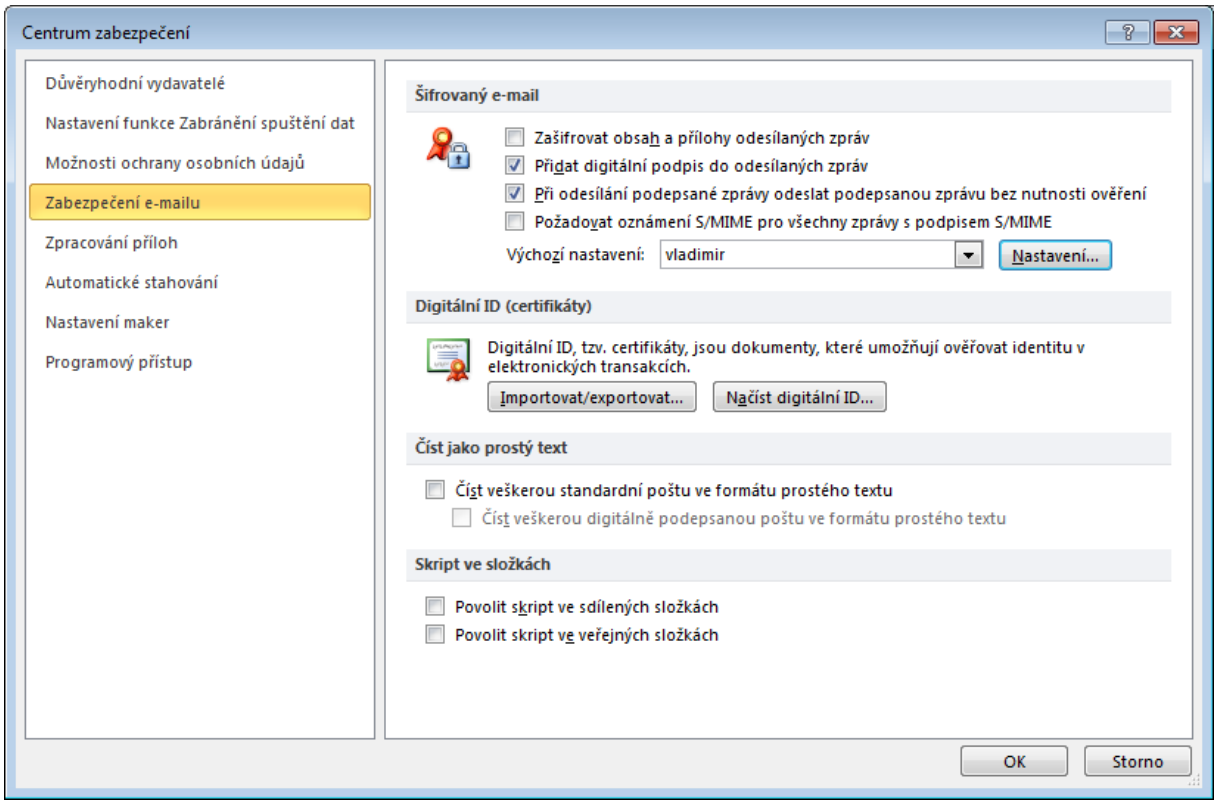
- Autentizační token (eToken PRO 72k, iKey 4000)
- SafeNet Authentication Client 8.0 a vyšší (middleware pro podporu tokenů)
- Certifikát umožňující digitální podpis e-mailu
- Emailový klient MS Outlook 2003 a vyšší

Postup:

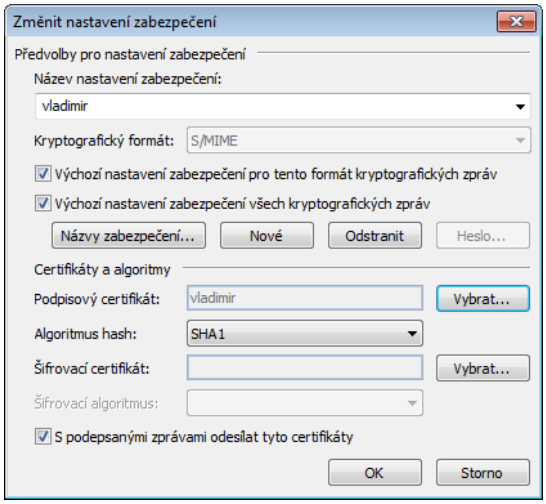
1) Vygenerování páru RSA klíčů na tokenu, vytvoření žádosti o certifikát a vydání certifikátu na token.
   Tento proces může být proveden u místní (např. firemní) certifikační autority nebo u externí, akreditované CA. V obou případech je třeba zajistit, aby byl nastaven minimálně parametr Key Usage Extension 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.



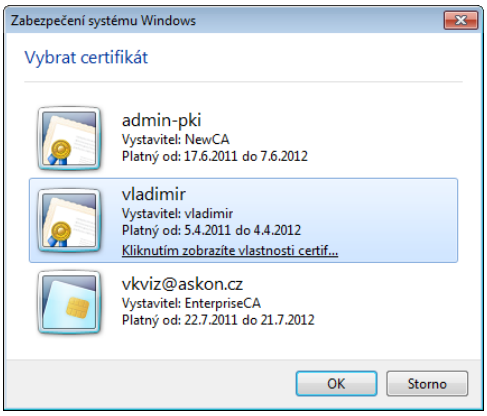
2) Spusťte MS Outlook 2003 a vyšší (ukázka z verze 2010). V nabídce Soubor klikněte na Možnosti a vyberte Centrum zabezpečení. Zde klikněte na Nastavení Centra zabezpečení… a v dalším okně na Zabezpečení e-mailu. Mělo by se otevřít okno podobné tomu na obrázku:



3) V poli Šifrovaný e-mail zvolte Nastavení…



4) Vyberte podpisový certifikát. Po kliknutí na Vybrat… se zobrazí pouze relevantní certifikáty použitelné pro podpis e-mailu z místního úložiště Windows nebo čipové karty/USB tokenu (musí být připojena). Aby šlo certifikát použít s Vaším e-mailovým účtem, je potřeba při jeho generování zadat příslušnou e-mailovou adresu. Při automatickém vydávání certifikátu je nutné vyplnit e-mailovou adresu do Active Directory/LDAP.



5) Případně podobně nastavte certifikát pro šifrování e-mailů.