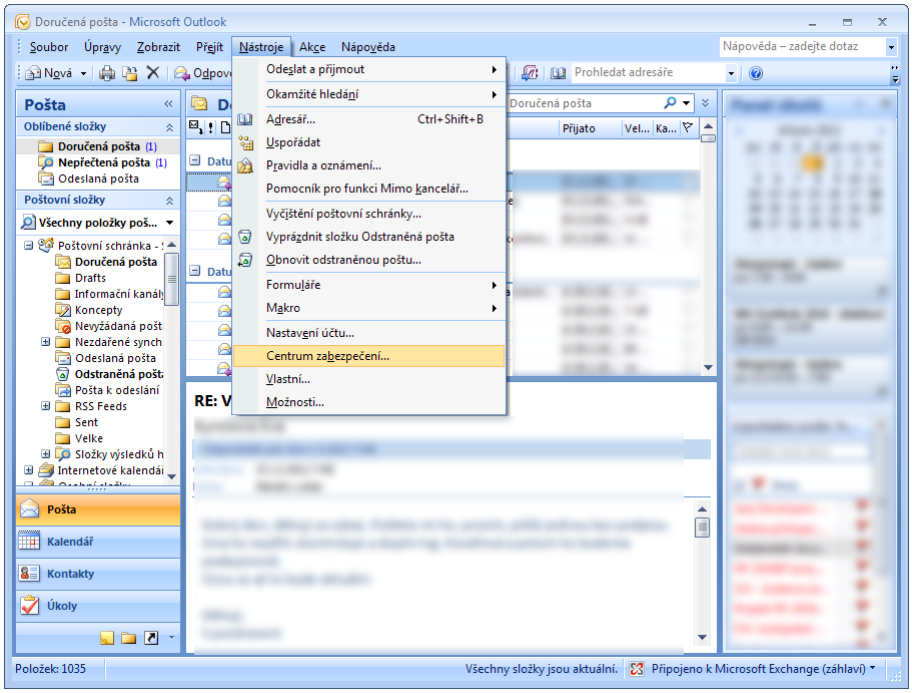
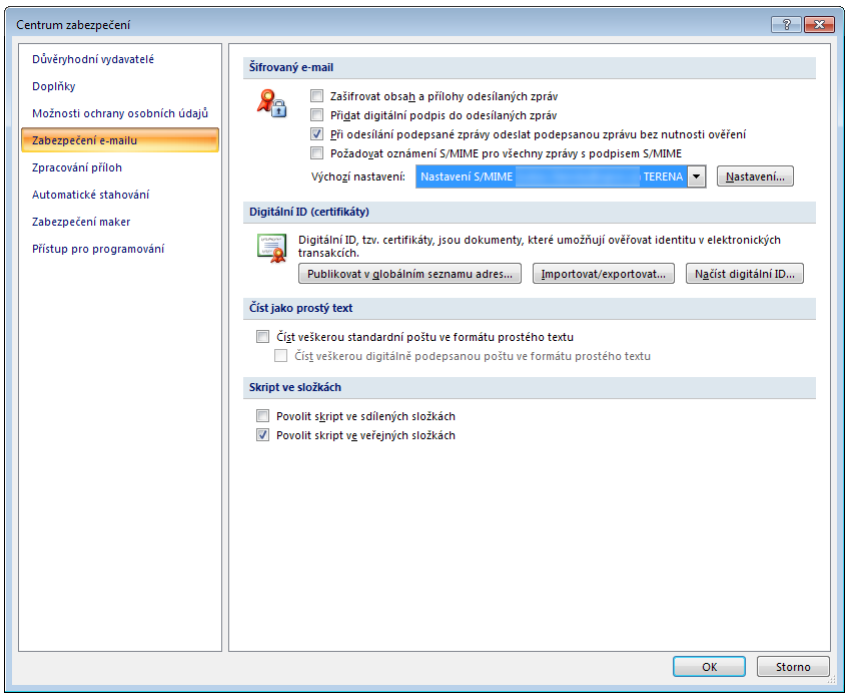
Vytváření elektronického podpisu v Microsoft Outlook

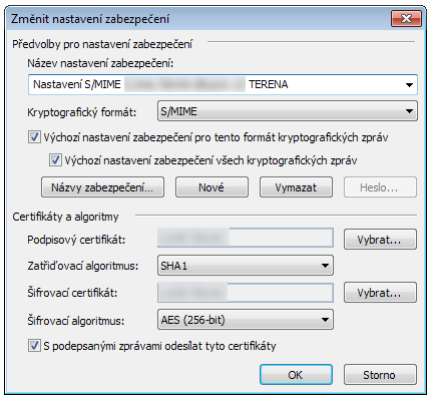
1. Pro využití elektronického certifikátu musíte mít certifikát vygenerovaný a uložený v úložišti certifikátů systému Windows. Viz návod na vystavení certifikátu.
2. V nabídce „*Nástroje/Centrum zabezpečení*“ můžete nastavit vlastnosti elektronického podpisu, který budete pro e-mailové zprávy využívat.



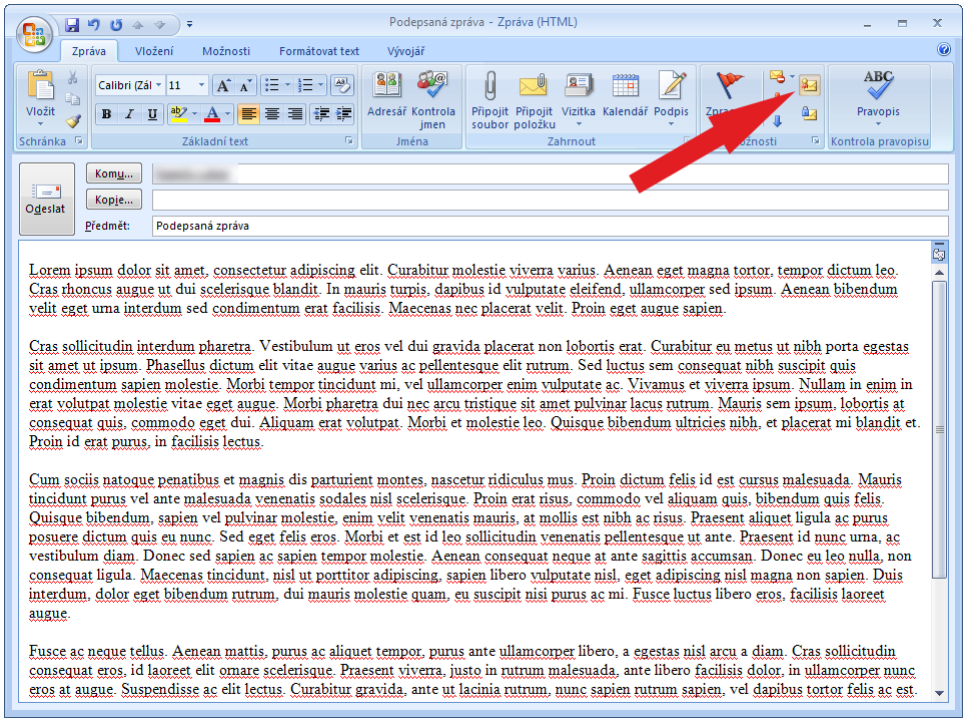
3. Na kartě „Zabezpečení e-mailu“ je volba pro nainstalované osobní certifikáty. Kliknutím na „*Nastavení*“ můžete zjistit, jakým způsobem je podepisování certifikátu nastaveno,



4. Pro algoritmus zatřiďování (hashování) zvolte algoritmus „*SHA1*“, který je dostatečně bezpečný a zároveň kompatibilní s většinou používaných systémů. Algoritmus MD5 není bezpečný k používání, algoritmy „*SHA256*“, „*SHA384*“ a „*SHA512*“ nemusí být podporovány ve starších verzích systémů.
   Pro šifrovací algoritmus je optimální zvolit „*AES (256-bit)*“, který představuje maximální ochranu, přičemž zachovává vysokou kompatibilitu.



5. Při psaní zprávy můžete stisknutím obálky s červenou stužkou přidat ke své e-mailové zprávě elektronický podpis.
   Obálka s modrou stužkou e-mailovou zprávu zašifruje i podepíše, takže si ji bude moci přečíst pouze příjemce zprávy. Pro tuto možnost musí váš počítač znát certifikát příjemce, ten je přenesen při každé podepisované komunikaci a automaticky ukládán do úložiště operačního systému[1].



[1] Takto přikládaný elektronický certifikát neobsahuje tzv. soukromý klíč, který je nutný pro podepisování a dešifrování. Obsahuje pouze veřejný klíč sloužící k ověření identity a šifrování.