

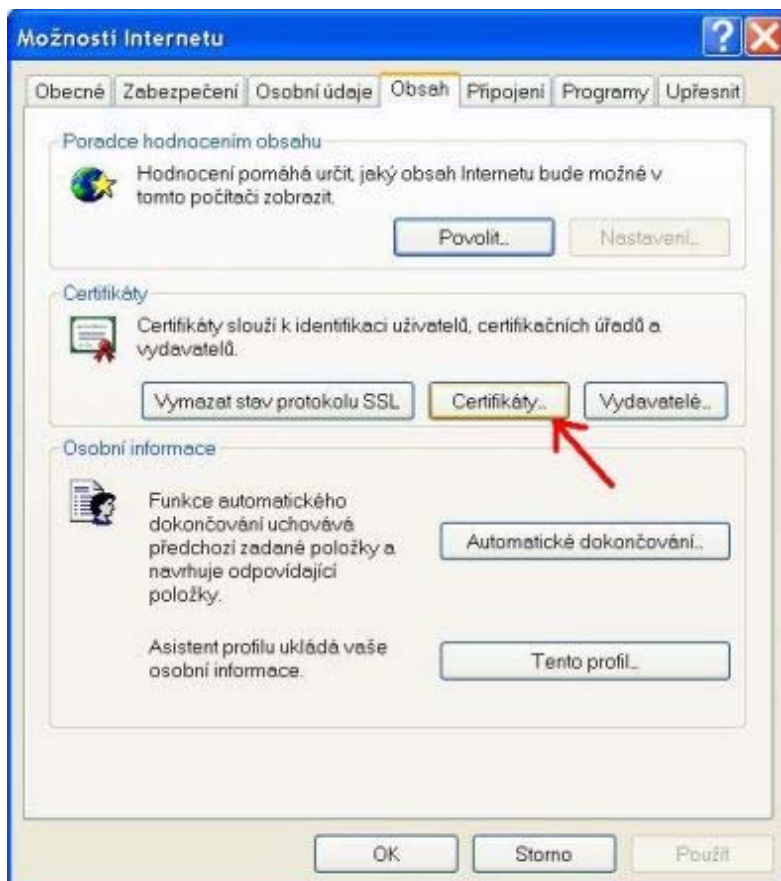
Instalace certifikátů

Pro správná elektronická podání je zapotřebí správně nainstalovat certifikáty a nakonfigurovat program Alis-PVS.

Pozn.: Zde uvedené postupy jsou pro operační systém Windows XP. U jiných systémů se mohou jednotlivé nabídky mírně lišit.

1. Kořenový certifikát certifikační autority (certifikát důvěryhodného úřadu pro šifrování a podepisování)

Kořenový certifikát instalujte do systému na počítači, kde budou elektronická podání i na počítači, kde se bude aktivovat podpisový certifikát. Je důležitý pro to, aby vydané certifikáty touto autoritou (Post Signum, ICA, ČSSZ, ...) byly považovány jako důvěryhodné. Instalace se provádí z menu Internet Exploreru – Nástroje – Možnosti internetu – záložka Obsah – tlačítko Certifikáty:



Přepněte se na záložku „Důvěryhodné kořenové certifikační úřady“ a stiskněte tlačítko „Importovat“:



Spustí se průvodce importem certifikátu. Stiskněte tlačítko „Další“ a na další obrazovce průvodce tlačítko „Procházet“. V adresářové struktuře nalistujte kořenový certifikát certifikační autority. Potvrďte soubor a stiskněte „Další“ – „Další“ – „Dokončit“. V seznamu certifikátů se objeví kořenový certifikát.

Pozn.: při poklepnání na certifikátu v jeho původním umístění (např. na disketě nebo na webových stránkách autority) lze přes tlačítko "instalovat" dojít ke stejnému výsledku.

2. Podpisový klíč (podpisový certifikát, kvalifikovaný certifikát, elektronický podpis)

Postup, jak získat podpisový klíč od vámi zvolené certifikační autority (ICA, Post Signum, E-identity ...) je uveden na stránkách certifikační autority.

(www.ica.cz, www.postsignum.cz, www.eidentity.cz)

Nejprve se **vygeneruje žádost o certifikát** na počítači, kde potom bude probíhat aktivace klíče (certifikátu). Tato žádost je jeden malý soubor, obvykle má příponu **.req** a buď se nahraje na disketu, kterou dodáte certifikační autoritě nebo to probíhá plně elektronicky.

Pozn.: Při vytváření žádosti o kvalifikovaný certifikát udejte e-mailovou adresu, pro kterou bude certifikát využíván v prostředí Outlook.

Instalaci (aktivaci) podpisového klíče je nutné provést na počítači, kde se generovala žádost o klíč, jinak nebude možné tímto klíčem elektronicky podepisovat. Elektronický podpis je prováděn prostřednictvím soukromé části klíče, která byla vygenerována společně s žádostí a neopustila zdrojový počítač. Až instalací na stejném počítači se spojí klíč se soukromou částí klíče a stává se použitelný.

Po úspěšné aktivaci je možné kompletní klíč vyexportovat a zadat si k němu heslo.

Provedte si jeho zálohu a uložte např. na disketě na bezpečné místo (nezapomeňte si k němu poznamenat heslo). Vyexportovaný kompletní klíč lze případně přenést na jiný počítač.

Instalace podpisového klíče na počítači, kde se generovala žádost o klíč

Předpokládejme, že jste od certifikační autority obdrželi na základě vaší vygenerované žádosti podpisový klíč na disketě nebo třeba e-mailem (např. soubor "prijmeni.cer") - ten je potřeba aktivovat.

Instalace se provádí z menu **Internet Exploreru – Nástroje – Možnosti internetu – záložka Obsah – tlačítko Certifikáty**.

Přepněte se na záložku „**Ostatní uživatelé**“ a stiskněte tlačítko „**Importovat**“. Spustí se průvodce importem certifikátu. Stiskněte tlačítko „**Další**“ a na další obrazovce průvodce tlačítko „**Procházet**“. V adresářové struktuře nalistujte podpisový klíč, který jste dostali od autority (např. „prijmeni.cer“). Potvrďte soubor a stiskněte „**Další**“ – „**Další**“ – „**Dokončit**“. V seznamu certifikátů se objeví podpisový klíč.

Pokud vše proběhlo v pořádku, měl by se v tuto chvíli spojit certifikát se soukromou částí klíče, která od vygenerování žádosti neopustila počítač.

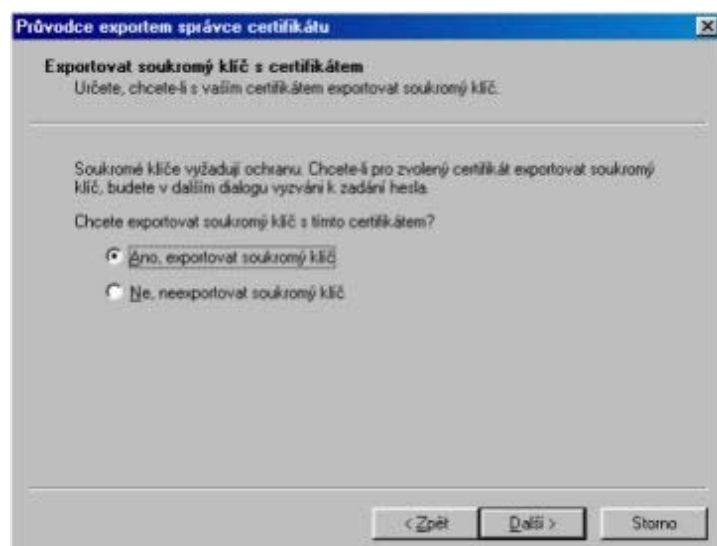
Pozn.: při poklepání na certifikátu v jeho původním umístění (např. na disketě) lze přes tlačítko "instalovat" dojít ke stejnému výsledku.

Export podpisového klíče

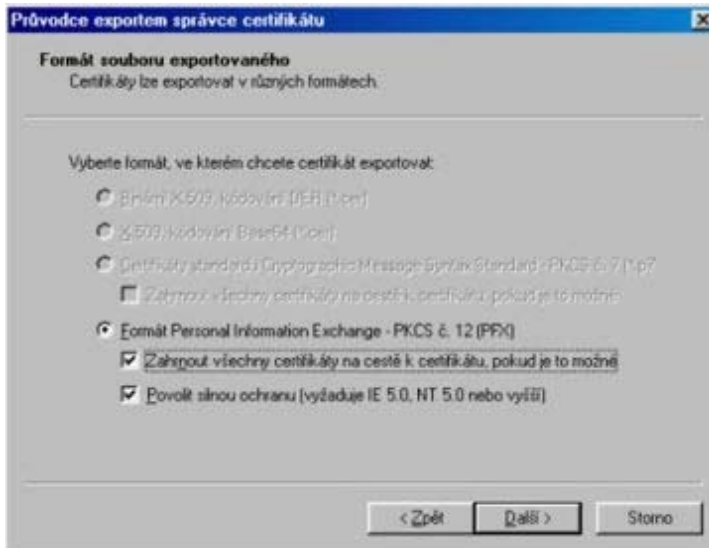
Export kompletního klíče (přípona **.pfx**) provedte vždy pro zálohu certifikátu, pro přenos na jiný počítač, resp. pro potřeby programu Alis-PVS.

Přesuňte se do seznamu certifikátů v menu **Internet Exploreru – Nástroje – Možnosti internetu – záložka Obsah – tlačítko Certifikáty** a přepněte se na záložku „**Ostatní uživatelé**“ (popř. "Osobní").

Vyberte (označte) v seznamu certifikátů váš podpisový klíč (např. „prijmeni.cer“) a stiskněte „**Exportovat**“. Spustí se průvodce exportem certifikátu. Stiskněte „**Další**“ a na další obrazovce zvolte možnost „**Ano, exportovat soukromý klíč**“:



Na další obrazovce zvolte „**Formát Personal Information Exchange ... (PFX)**“ a zaškrtněte volby „**Zahrnout všechny certifikáty ...**“ a „**Povolit silnou ochranu ...**“:



Dále je nutné zvolit heslo pro certifikát. Na další obrazovce si vymyslete jednoduché heslo, zadejte jej do formuláře (dvakrát) a zapamatujte si jej.

Na další obrazovce zadejte cestu pro uložení certifikátu. Pro přenos na disketu doporučujeme zadat např.: A:\prijmeni.pfx.

Export proveďte vždy. Pokud budou elektronická podání probíhat z jiného počítače, přenesete výsledný klíč **.pfx** na počítač, ze kterého budou podání probíhat (např. na disketu). Pokud budou podání probíhat ze stejného počítače, potřebujeme výsledný soubor **.pfx** pro program Alis-PVS.

Pozn.: Pokud se vám neobjevuje obrazovka "Exportovat soukromý klíč..." a volba formátu PFX není přístupná, tak se nepovedlo správně importovat certifikát. Zkontrolujte, zda se generovala žádost na stejném počítači, dále by mezi vygenerováním žádosti a importem certifikátu nemělo být s počítačem manipulováno (instalace Windows, konfigurace profilů ...) a neměla by mezi generováním žádosti a instalací klíče být delší časová prodleva (více než týden). Problematické také bývá použití PC s Win98.

Pokud máte přesně tento problém, nezoufejte a zkuste ještě provést aktivaci klíče přes speciální program vaší certifikační autority.

Pokud žádný recept nepomůže, pravděpodobně budete muset provést znovu vygenerování žádosti a získat nový certifikát od certifikační autority.

Použití podpisového klíče v programu Alis-PVS

Vytvořený kompletní podpisový klíč **.pfx** potřebuje program Alis-PVS nakopírovat do vlastní složky, aby mohl podepisovat elektronická podání.

Kopii pro Alis-PVS proveďte buď přímo v instalaci programu (viz popis "Instalace programu – [Certifikát pro podpis \(.pfx\)](#)") nebo v nastavení programu (viz popis "Pracovní postupy - [podpisový certifikát](#)").

Pokud je ve složce více podpisových certifikátů (.pfx), musí být vámi vytvořený certifikát vybraný jako „Aktivní“.

3. Šifrovací certifikát

Tato kapitola je pouze pro odborníky a běžný uživatel s tímto nepřijde do styku (zajišťuje si program automaticky).

Někteří poskytovatelé služeb (např. ČSSZ, Daňová správa) požadují, aby el. podání bylo i zašifrováno. K tomu dodávají své šifrovací certifikáty.

Tyto certifikáty jsou součástí programu Alis-PVS a pro jiné účely jsou volně ke stažení přímo od poskytovatele služeb:

- ČSSZ: http://www.cssz.cz/tiskopisy/ELDP_2004/sifrovaci-certifikat.cer,
- Daňová správa: <https://bezpecne.dev.gov.cz/diskuze/files/281/download.aspx>

V běžných případech není nutné stahovat (je součástí programu).

Použití šifrovacího certifikátu v programu Alis-PVS

Tento certifikát nemusíte instalovat do systémového úložiště certifikátů jako předchozí dva certifikáty. Musí však být ve vlastní složce programu Alis-PVS, aby se jím mohla šifrovat elektronická podání.

Instalace je plně automatická, pokud byste šifrovací certifikáty nastavovali ručně, provede se buď přímo v instalaci programu (viz popis "Instalace programu – [Certifikát pro šifrování \(.cer\)](#)") nebo v nastavení programu (viz popis "Pracovní postupy - [šifrovací certifikát](#)"). Pokud je ve složce více šifrovacích certifikátů (.cer), musí být vámi vytvořený certifikát vybraný jako „Aktivní“.