Technické podmínky pro používání ABO-K

Pro používání ABO-K je potřebný **operační systém Windows XP + SP3 nebo vyšší**, přístup na **Internet** a internetový prohlížeč **MS Internet Explorer verze 7, 8, 9 a 10.**

Pro bezproblémový chod aplikace ABO-K doporučujeme udržovat operační systém Windows v aktualizovaném stavu, tj. aplikovat poslední aktualizace operačního systému a dodržovat bezpečnostní pravidla podle posledních doporučení výrobce uvedeného operačního systému.

Elektronický podpis / značka

Od 1.7.2013 nebude možné podepsat datové soubory s příkazy prostřednictvím ABO-K. Klient si musí zajistit aplikační řešení pro podepisování dávky. Elektronický podpis nebo značka je extra soubor, jež daná aplikace vytvoří s použitím kvalifikovaného certifikátu a to takového, který je zaregistrován v ABO-K pomocí podpisových vzorů. Klienti, kteří používají dva podpisy, musí při vkládání dávky vložit dva externí podpisy / značky.

Požadavky na vytvoření elektronického podpisu:

Elektronický podpis či značka musí být vytvořen ve struktuře signedData dle PKCS#7 v DER kódování, přičemž soubor s podpisem neobsahuje vlastní podepisovaná data (jedná se o externí podpis) a obsahuje podpisující certifikát a vždy jeden podpis. Elektronický podpis je v binárním tvaru (tj. není zakódován pomocí base64). Používá se hashovací funkce SHA-256, jejíž OID je 2.16.840.1.101.3.4.2.1.

Modul pro podporu pro práci s certifikáty

ABO-K pro elektronické podepisování používá komponentu Signer. Bez této komponenty nelze v ABO-K podepsat dávku a tedy nelze předat příkazy ke zpracování. Pro přístup do ABO-K a další jeho funkce nutná není.

Po přihlášení do ABO-K je popis instalace podpory pro práci s certifikáty uveden v menu *Různé → Nápověda, dokumenty* v bodu *1. Popis instalace podpory pro práci s certifikáty*. Aplikace ABO-K je přístupná na internetové adrese **http://abok.cnb.cz** .

Poznámka: 64 bitový Windows 7 nebo 8 má přednostně nainstalovaný 32 bitový Internet Explorer, proto je nutné, instalovat do Internet Exploreru 32 bitový modul Signer, a to samozřejmě jen v případě, že jste extra neinstalovali 64 bitový Internet Explorer.

Nastavení Microsoft Internet Exploreru

Kontrola kořenových certifikátů v záložce *Důvěryhodné kořenové certifikační autority / úřady* – v menu IE *Nástroje / Možnosti Internetu* záložka *Obsah* a stiskněte tlačítko *Certifikáty*. Zde by měl být nainstalován **kořenový certifikát PostSignum** pro HTTPS komunikaci. U OS Windows 7 by měl být automaticky nainstalován při instalaci OS nebo při jeho aktualizaci. U OS Windows XP je nutné kořenový certifikát instalovat.

Jak bylo výše uvedeno aplikace ABO-K musí být provozována na verzi Windows XP + 3SP a vyšší a na prohlížeči Internet Explorer (dále jen "IE") verze 7,8. Verze 9 a 10 vyžaduje další nastavení, která jsou uvedena v bodu 5, 6 a 7.
Menu *Nástroje* je spouštěno z *Panelu nástrojů*, který se nazývá *Řádek nabídek*, jestliže není tento zobrazen, klikněte pravým tlačítkem myši na záhlaví okna IE a v rozbaleném menu vyberte *Řádek nabídek*.

Co je nutné, ale ne vždy postačující, udělat v IE, aby se disponent připojil do ABO-K:

1. Kontrola certifikátu – Při přihlášení do ABO-K musí být vybrán takový certifikát, který je zaregistrován v ABO-K. Kontrola certifikátu může být provedena proti podpisovým vzorům. Certifikát musí být zobrazen v záložce *Osobní*. Zde se zobrazí vždy a nezáleží jestli je uložen na kartě, tokenu nebo byl importován do úložiště počítače.
   Kontrola certifikátu v záložce *Osobní* – v menu IE *Nástroje / Možnosti Internetu* záložka *Obsah* a stiskněte tlačítko *Certifikáty*.
   Otevře se okno *Certifikáty* se seznamem přístupných certifikátů z daného počítače. Zde v záložce *Osobní* označte kliknutím certifikát a tlačítkem *Zobrazit* otevřete okno *Certifikát* se záložkami *Obecné*, *Podrobnosti* a *Cesta k certifikátu*. Certifikát by měl být vydán na konkrétní právnickou nebo fyzickou osobu, vydán certifikační autoritou PostSignum, 1.CA nebo eIdentity a měl by být platný. Zkontrolujte též na záložce *Cesta k certifikátu* kořenové certifikáty příslušné certifikační autority.
2. V menu IE *Nástroje / Možnosti Internetu* záložka *Zabezpečení*, klikněte na zónu *Internet* a stiskněte tlačítko *Vlastní úroveň ...*. Vyhledejte volbu *Při odesílání souborů na server zahrnout cestu místního adresáře* a nastavte *Povolit*. Po stisku *OK* stiskněte tlačítko *Výchozí úroveň*.
3. V menu IE *Nástroje / Možnosti Internetu* záložka *Zabezpečení*, klikněte na zónu *Důvěryhodné servery* a stiskněte tlačítko *Vlastní úroveň ...*. Vyhledejte volbu *Při odesílání souborů na server zahrnout cestu místního adresáře* a nastavte *Povolit*. Po stisku *OK* stiskněte tlačítko *Výchozí úroveň*.
4. V menu IE *Nástroje / Možnosti Internetu* záložka *Zabezpečení*, klikněte na zónu *Důvěryhodné servery* a stiskněte tlačítko *Servery (*nebo též *Weby)* a zkontrolujte, zda v seznamu důvěryhodných serverů jsou servery:
   https://abok.cnb.cz
   https://www.postsignum.cz
   Když nejsou, tak doplňte pomocí tlačítka *Přidat*.
5. V IE 9 a 10 zkontrolovat používání protokolů – v menu IE *Nástroje / Možnosti Internetu* záložka *Upřesnit* v části *Zabezpečení* musí být zvoleny / zaškrtnuty pouze protokoly SSL 3.0 a TLS 1.0., jiné ne!
6. Nastavení IE v 9 a 10 – v menu IE *Nástroje / Možnosti Internetu* záložka *Zabezpečení* odškrtnout *Povolit chráněný režim* (tzn. nepovolovat chráněný režim) pro zónu *Místní Intranet* a *Důvěryhodné servery*. U zóny *Internet* je chráněný režim povolen. U zón *Internet*, *Místní Intranet* a *Důvěryhodné servery* musí být nastavena výchozí úroveň (tlačítko *Výchozí úroveň* je nedostupné) na *Středně vysoké*, *Středně nízké* a *Střední*.
7. Nastavení IE v 9 a 10 – v menu IE *Nástroje / Nastavení kompatibilního zobrazení* přidejte do seznamu web *cnb.cz*. Tři volby dole pod seznamem webů přidaných do kompatibilního zobrazení, nemusí být zaškrtnuté. Po této akci, když se provádí ze stránky *abok.cnb.cz*, se automaticky v menu IE *Nástroje / Kompatibilní zobrazení* objeví "fajfka" jako příznak aktivní volby.
8. Restartovat IE.

Doporučení -> Pro udržování IE v kondici je též dobré občas vymazat vnitřní paměť IE (cache):

IE *Nástroje / Možnosti Internetu* blok *Historie procházení* tlačítko *Odstranit ...* a zaškrtnout minimálně *Dočasné soubory internetu* a potvrdit

a nastavit následující:

IE *Nástroje / Možnosti Internetu* blok *Historie procházení* tlačítko *Nastavení* blok *Dočasné soubory Internetu* a v *Zjišťovat existenci novějších verzí uložených stránek* zaškrtnout volbu *Při každé návštěvě webové stránky*.

Další možné akce pro zprovoznění ABO-K na IE

a) Obnovení nastavení IE – menu IE *Nástroje / Možnosti Internetu* záložka *Upřesnit* tlačítko *Obnovit*. Pak zkontrolujte a popřípadě znovu nastavte IE podle výše uvedených bodů.

b) Reinstalace certifikátu v úložišti počítače – týká se jen počítačů, kde jsou certifikáty v úložišti počítače (ne na kartě, flash disku nebo tokenu). K reinstalaci však **musíte mít bezpodmínečně zálohu certifikátu (soubor PFX nebo P12) a znát heslo k certifikátu**. Jinak se import nezdaří a budete muset žádat o nový certifikát, což znamená pro vás finanční náklady.
Jestliže soubor máte a heslo znáte, proveďte -> *Nástroje / Možnosti Internetu* záložka *Obsah* a stiskněte tlačítko *Certifikáty*. Zde kliknutím na certifikát vyberte certifikát. Tlačítkem *Odebrat* certifikát odeberete z úložiště. Tlačítkem *Importovat* spusťte průvodce importu. Doporučujeme v průvodci nastavit silnou ochranu certifikátu a nastavit certifikát jako neexportovatelný.

c) Přechod na vyšší verzi Windows – v případě, že jste generovali žádost o certifikát např.: na Windows XP, tak při povýšení na Windows 7, přestane certifikát plnit svojí funkci a nelze ho použít pro podpis. Návody na znovu zprovoznění certifikátu najdete na stránkách příslušných certifikačních autorit.
Uvádím zde příklad pro certifikát PostSignum – stáhněte z www.postsignum.cz aplikaci *iSignum* a tou importujte ze souboru PFX do osobního úložiště vše potřebné pro podpis. Certifikát v osobním úložišti je v exportovatelném tvaru a není zabezpečen heslem. Proto důrazně doporučujeme certifikát exportovat z úložiště i s osobním klíčem do nového souboru PFX. Pak certifikát z úložiště odebrat. Nový soubor PFX pak použít pro import certifikátu do externího úložiště (token, karta) nebo úložiště počítače se silnou ochranou klíče a jako neexportovatelný.