Technické podmínky pro používání ABO-K

Obsah

1. Provozní prostředí ABO-K

Pro používání ABO-K jsou potřebné:

a) Český operační systém Windows verze 7 + SP1 s pravidelnými aktualizacemi pomocí utility Windows Update, nebo vyšší verze Windows (8, 8.1 a 10),
b) přístup na **Internet,**
c) internetový prohlížeč **MS Internet Explorer** (dále jen "IE") **verze 11,**
d) přenosový protokol minimálně **TLS 1.1**

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 operačního systému.

2. Ověření pravosti datových souborů s příkazy

Pravost datových souborů s příkazy vkládaných disponenty do ABO-K je ověřována v centrálním účetním systému ČNB na základě externího souboru s elektronickým podpisem, nebo elektronickou pečetí. Tyto musí být vytvořeny daným programovým vybavením prostřednictvím platného certifikátu, jenž je registrovaný v ABO-K pro podpis. V podpisových vzorech ABO-K je uvedeno jaký certifikát disponent pro elektronický podpis použije. V případě osobního kvalifikovaného certifikátu do ABO-K vkládá disponent uznávaný elektronický podpis, v případě kvalifikovaného certifikátu pro elektronickou pečeť vkládá uznávanou elektronickou pečeť.

3. Elektronický podpis dávek vytvořených uvnitř ABO-K

Příkazy a instrukce vytvořené po přihlášení do ABO-K jsou realizovány prostřednictvím dávek, z nichž některé je nezbytné elektronicky podepsat použitím kvalifikovaných osobních certifikátů zaregistrovaných v ABO-K pro podpis. Podpis vytváří programová komponenta s názvem Signer (založená na technologii ActiveX), která se spouští kliknutím na ikonu ve sloupci *Podpis* na stránce *Přehled dávek – předání dávky*. Signer jako podpora pro práci s certifikáty v ABO-K je funkční pouze v prohlížeči IE, který musí být nastaven tak, jak je uvedeno níže v odstavci *Nastavení Microsoft Internet Exploreru*. Jinými internetovými prohlížeči je možné se do ABO-K

přihlásit a kromě podepisování využívat všechny další funkce. Pro úspěšný podpis dávky musí být na daném počítači dostupný osobní kvalifikovaný certifikát, jenž je zaregistrovaný v ABO-K pro podpis a **musí být uložen na externím médiu (USB token, čipová karta) – viz příloha č.1 Bezpečnostní zásady.**

Popis instalace Signeru pro podporu pro práci s certifikáty je uveden v menu *Různé Návody, dokumenty* v bodu *1. Popis instalace podpory pro práci s certifikáty*.

Poznámka: 64 bitový Windows 7, 8 a 10 má přednostně nainstalovaný 32 bitový IE, proto je nutné instalovat 32 bitový modul Signer, a to samozřejmě jen v případě, že jste extra neinstalovali 64 bitový IE. Windows 10 nabízí prohlížeč Microsoft Edge a Internet Explorer je třeba najít v programové nabídce a nejlépe jeho zástupce připnout na hlavní panel.

4. Kontrola hodnot atributů webových certifikátů

Aby uživatel ověřil, že se nachází skutečně na webu ČNB, musí zkontrolovat atributy certifikátu tohoto webu.

Zobrazení atributů tzv. SSL certifikátu se provádí kliknutím do adresního řádku internetového prohlížeče na název *Česká národní banka* a dále podle typu použitého prohlížeče. U IE kliknete dále na odkaz *Zobrazit certifikáty* a v okně *Certifikát* vyberte záložku *Podrobnosti*.

V záložce Podrobnosti je tabulka se sloupci Pole, kde je uvedené jméno atributu, a Hodnota atributu. Kliknutím myši na řádek tabulky se celý řádek zvýrazní a ve spodní části okna se zobrazí celá hodnota označeného atributu. Uživatel by měl ověřit níže uvedené hodnoty atributů.

5. Atributy certifikátu provozního webu **abok.cnb.cz**

Sériové číslo: hex.: 0d 03 f2 3d 91 76 a2 e5 06 2e 6a e0 29 e5 fc 3e

Vystavitel:
CN = DigiCert Global CA G2
O = DigiCert Inc
C = US

Platnost od: 1. března 2018 2:00:0
Platnost do: 18. ledna 2019 14:00:00

Subjekt:
CN = abok.cnb.cz
OU = Sekce peněžní a platebního styku
O = Česká národní banka
L = Praha - Nové Město
C = CZ
SERIALNUMBER = 48136450
1.3.6.1.4.1.311.60.2.1.3 = CZ
2.5.4.15 = Private Organization

Kryptografický otisk:
b1 61 49 98 db 5b c1 12 37 06 55 4a be d4 92 9f 80 52 92 f1

6. Atributy certifikátu testovacího webu **aboktest.cnb.cz**

Sériové číslo: hex.: 0d c4 7a 98 4c af 1c a9 bd d1 f2 57 eb 02 3f 2c

Vystavitel:
CN = DigiCert Global CA G2
O = DigiCert Inc
C = US

Platnost od: 1. března 2018 2:00:0
Platnost do: 3. prosince 2018 14:00:0

Subjekt:
CN = aboktest.cnb.cz
OU = Sekce peněžní a platebního styku
O = Česká národní banka
L = Praha - Nové Město
C = CZ
SERIALNUMBER = 48136450
1.3.6.1.4.1.311.60.2.1.3 = CZ
2.5.4.15 = Private Organization

Kryptografický otisk:
d2 80 c8 09 61 12 7d 64 b9 aa 13 a9 3a 14 24 a0 1e dd 12 d8

7. Důvěryhodnost webů

Důvěryhodnost provozního webu *abok.cnb.cz* a testovacího webu *aboktest.cnb.cz* je ověřována na základě kořenového certifikátu certifikační autority *DigiCert*. Pro plynulou komunikaci s webem je vhodné mít tento certifikát na Vašem počítači uvedený v seznamu důvěryhodných certifikačních autorit. Pokud kořenový certifikát *DigiCert* nebudete mít na svém počítači, budete při každém přihlášení do ABO-K upozorněni, že certifikát webu *abok.cnb.cz* nebo *aboktest.cnb.cz* pochází z nedůvěryhodného zdroje.

Kontrola přítomnosti kořenových certifikátů se provádí v záložce *Důvěryhodné kořenové certifikační autority* – v menu IE *Nástroje / Možnosti Internetu* záložka *Obsah* a stiskněte tlačítko *Certifikáty*. Zde by měl být zobrazen **kořenový certifikát DigiCert** pro HTTPS komunikaci.

U OS Windows 7 a u vyšších verzí by měl být automaticky nainstalován při instalaci OS nebo při jeho aktualizaci. Certifikát kořenové certifikační autority „DigiCert Global Root G2“ je možné stáhnout z následující webové stránky certifikační autority DigiCert jako soubor „DigiCertGlobalRootG2.cet“:

https://www.digicert.com/digicert-root-certificates.htm

Jeho vystavitelem je:
CN = DigiCert Global Root G2
OU = www.digicert.com
O = DigiCert Inc
C = US

Instalace do důvěryhodných certifikačních autorit se provede jednoduše tak, že poklepem se soubor spustí. V záložce *Obecné* tlačítkem *Nainstalovat certifikát ...* se instaluje pomocí průvodce instalace.

8. Nastavení Microsoft Internet Exploreru

ABO-K vyžaduje určitá nastavení u IE pomocí menu *Nástroje*. Menu *Nástroje* lze spustit klávesovou zkratkou *Alt-X* a nebo 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, ne postačující, udělat v IE, aby se disponent přihlásil do ABO-K tlačítkem *Přihlásit*:

a) Při přihlášení do ABO-K musí být vybrán takový certifikát, který je zaregistrován v ABO-K. Jestliže po vybrání certifikátu a jeho potvrzení prohlížeč napíše, že web ČNB není bezpečně dostupný je velmi pravděpodobné, že přístup na web je blokován antivirem (Kaspersky, Esset) a nebo že není certifikát fyzicky dostupný, i když je v úložišti vidět.

   Zobrazení podrobností certifikátu v IE - menu *Nástroje / Možnosti Internetu* záložka *Obsah* a stiskněte tlačítko *Certifikáty*. Otevře se okno *Certifikáty* se seznamem certifikátů, které jsou uživateli dostupné. V záložce *Osobní* označte kliknutím certifikát a tlačítkem *Zobrazit* otevřete okno *Certifikát* se záložkami *Obecné*, *Podrobnosti* a *Cesta k certifikátu*. Certifikát by měl být pro konkrétní fyzickou osobu (tzv. osobní certifikáty), vydán certifikační autoritou PostSignum, 1.CA nebo eIdentity a měl by být platný. Zkontrolujte na záložce *Cesta k certifikátu* kořenové certifikáty příslušné certifikační autority.

   Kontrolu polí certifikátu, zejména pole *Subjekt*, můžete provést proti podpisovým vzorům ABO-K. **Certifikát musí být zobrazen v záložce *Osobní*. (Zde se zobrazí vždy a nezáleží na tom, jestli je uložen na kartě, tokenu nebo byl importován do úložiště počítače).**

   Poznámka: Od Windows 8 a výše a při použití IE verze 11 certifikáty uložené na kartě nebo tokenu jsou v záložce *Osobní* vidět, i když jsou karta nebo token vytažené z počítače a tudíž fyzicky nedostupné. Nepřišel jsem na to, jak pravý stav věci zobrazit a nepomohl ani trojhmat *Ctrt/Alt/Del*. Zkrátka může se stát, že i při vytaženém tokenu nebo čipové kartě jsou certifikáty vidět, ale fyzicky nejsou dostupné.

b) Zkontrolujte použité protokoly přenosu – v menu IE *Nástroje / Možnosti Internetu* záložka *Upřesnit* v části *Zabezpečení* zaškrtnutý minimálně TLS 1.1. Web *abok.cnb.cz* pracuje jen s přenosovými protokoly TLS 1.1 a TLS 1.2. **Nesmí být zaškrtnut SSL 2.0.**

c) Dále nastavte *Nástroje / Možnosti Internetu* záložka *Zabezpečení* odškrtnout *Povolit chráněný režim* (tzn. nepovolovat chráněný režim) pro zónu *Místní Intranet* a *Důvěryhodné weby*. U zóny *Internet* je chráněný režim povolen. U zón *Internet, Místní Intranet* a *Důvěryhodné weby* musí být nastavena výchozí úroveň (tlačítko *Výchozí úroveň* je nedostupné) na *Středně vysoké, Středně nízké* a *Střední.*

9. Co je nutné udělat v IE, aby se spustil Signer

Signer je komponenta ActiveX, kterou používá ABO-K pro podepisování dávek vytvořených uvnitř ABO-K a v jiném prohlížeči než v Internet Exploreru nefunguje.:

a) Zrušit filtrování ActiveX – kliknutím na ikonu *zubaté kolečko* v pravém horním rohu okna IE vybrat *Zabezpečení*. Otevře se menu, kde u volby *Filtrování ActiveX* nesmí být "fajfka", nebo z řádku nabídek rozbalit menu *Nástroje* a zkontrolovat nepřítomnost "fajfky" u *Filtrování ActiveX* zde. "Fajfka" se odstraňuje nebo zobrazuje kliknutím na text *Filtrování ActiveX*.

b) V menu IE *Nástroje / Možnosti Internetu* záložka *Zabezpečení*, klikněte na zónu

Důvěryhodné weby a stiskněte tlačítko *Weby* a zkontrolujte, zda v seznamu důvěryhodných webů je web:
https://abok.cnb.cz
Když není, tak doplňte pomocí tlačítka *Přidat*.

10.Co je možné dále udělat, aby ABO-K v IE fungovalo

a) Obnovení nastavení IE (proveďte až po té, co výše uvedená nastavení nepomohou) – menu IE *Nástroje / Možnosti Internetu* záložka *Upřesnit* tlačítko *Obnovit*. I když IE hlásí, že je nutné restartovat počítač, postačí restartovat IE. Pak zkontrolujte a popřípadě znovu nastavte IE podle výše uvedených bodů.

b) Kompatibilita nastavení pomáhá jen u Windows 7) – *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.

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*.

Můžete též v menu *Nástroje / Možnosti Internetu* záložka *Upřesnit* v části *Zabezpečení* zaškrtnout poslední volbu *Vyprázdnit složku Dočasné soubory Internetu při ukončení prohlížeče*.

Poznámka**: Disponent se do webových služeb** může přihlásit jen nekvalifikovaným certifikátem vydaným právnické osobě a podepisování souborů s příkazy posílaných webovými službami může být provedeno s použitím certifikátů pro právnické nebo fyzické osoby (viz Podmínky ABO-K Článek 8 a Článek 9).