Bezpečnostní zásady

Česká národní banka (ČNB) věnuje trvalou pozornost nadstandardnímu zabezpečení aplikace ABO-K internetové bankovnictví (dále jen „ABO-K“) a z těchto důvodů využívá moderní technologie pro ochranu důvěrnosti a integrity dat, dostupnosti a spolehlivosti celé aplikace.

Vedle opatření realizovaných ČNB je nutno, aby Klient věnoval náležitou pozornost i rizikům na své straně, a to zejména rizikům vyplývajícím ze způsobu přípravy, předávání a autorizace Dávek, zajištění ochrany soukromého klíče[1] příslušejícího ke Kvalifikovanému i Komerčnímu certifikátu, zajištění ochrany uživatelského jména a hesla, mobilního telefonu Disponenta, klientského počítače a systémového prostředí.

Klient je povinen dodržovat následující povinnosti a musí zajistit, aby tyto povinnosti dodržovali i všichni Disponenti pověření Klientem pracovat s ABO-K, včetně osob pověřených zabezpečením systému Klienta. Porušení těchto povinností může mít za následek, že třetí osoba provede neautorizovanou Transakci z Účtu Klienta a způsobí tak Klientovi ztrátu, za kterou nebude ČNB odpovídat.

1. Ochrana soukromých klíčů příslušejících k osobním certifikátům používaným pro přihlášení do ABO-K nebo pro Podpis dávky

a) Disponent nesmí sdílet soukromý klíč s jinou osobou.

b) Disponent je povinen mít uložen soukromý klíč výhradně na USB tokenu nebo čipové kartě, na kterých byl soukromý klíč vygenerován při vytváření žádosti o certifikát.

c) Disponent smí čipové karty nebo USB token, na nichž je uložen soukromý klíč k certifikátu používanému v ABO-K, ponechávat ve čtečce čipových karet, resp. v USB portu pouze po dobu potřebnou pro práci s čipovou kartou nebo USB tokenem.

d) Disponent je povinen při používání čipové karty nebo USB tokenu, na nichž je uložen soukromý klíč k certifikátu používanému v ABO-K, tato zařízení zabezpečit PINem nebo heslem, které splňuje následující podmínky:
   - PIN[2] musí být tvořen nejméně čtyřmi číslicemi v kombinaci s omezeným počtem pokusů o jeho zadání,
   - heslo musí být tvořeno nejméně 8 znaky a kombinací nejméně jednoho velkého a jednoho malého písmene, jedné číslice a jednoho speciálního znaku (např. plus, mínus, otazník, hvězdička, tečka),
   - PIN a heslo nesmí být tvořeno ze slov či kombinací čísel, která mohou být snadno uhodnutelná (např. jména, přezdívky, data narození, telefonní čísla apod.),
   - PIN a heslo musí být odlišné od PIN a hesel používaných v jiných aplikacích Klienta,

[1] Soukromým klíčem se rozumí data pro vytváření uznávaného elektronického podpisu nebo uznávané elektronické pečeti (Kvalifikovaný certifikát) a data pro ověření identity Disponenta (Komerční certifikát) .
[2] PIN je číselné identifikační číslo (personal identification number).

e) Disponent nesmí PIN a heslo k čipové kartě nebo USB tokenu, na nichž je uložen soukromý klíč k certifikátu používaného v ABO-K,
   - zaznamenat takovým způsobem, aby k nim umožnil přístup třetí osobě (tj. např. do diářů, na poznámkové papírky uložené v blízkosti počítače, nebo na obal čipové karty či USB tokenu apod.),
   - zaznamenat takovým způsobem, ze kterého je zřejmé, že se jedná o PIN nebo heslo k příslušné čipové kartě nebo USB tokenu,
   - nikomu sdělit ani jej zadávat za přítomnosti třetí osoby tak, aby se s ním tato osoba mohla seznámit,
   - ukládat pomocí funkce zapamatování PIN a hesel v nastavení počítače, internetového prohlížeče nebo mobilního telefonu.

f) Disponent je povinen při podezření, že by mohl být nebo že byl zneužit soukromý klíč k jeho certifikátu, tento certifikát neprodleně zneplatnit u Certifikační autority.

2. Ochrana uživatelského jména a hesla používaného pro přihlášení do ABO-K

a) Disponent je povinen uživatelské jméno a heslo důsledně chránit a nesmí je sdílet s jinou osobou.

b) Disponent je povinen před odchodem od počítače ukončit práci s ABO-K odhlášením a zavřením okna internetového prohlížeče.

c) Heslo Disponenta pro přihlášení musí být odlišné od hesel používaných v jiných aplikacích Klienta nebo Disponenta, resp. k zabezpečení čipových karet nebo USB tokenu, na nichž má Disponent uloženy soukromé klíče k osobním certifikátům.

d) Disponent nesmí uživatelské jméno a heslo používané pro přihlášení do ABO-K
   - zaznamenat takovým způsobem, aby k nim umožnil přístup třetí osobě (např. do diářů, na poznámkové papírky uložené v blízkosti počítače apod.),
   - zaznamenat takovým způsobem, ze kterého je zřejmé, že se jedná o uživatelské jméno nebo heslo,
   - nikomu sdělit ani je zadávat za přítomnosti třetí osoby tak, aby se s nimi tato osoba mohla seznámit,
   - ukládat pomocí funkce zapamatování hesel v nastavení počítače, internetového prohlížeče nebo mobilního telefonu.

e) Disponent je povinen při podezření, že by uživatelské jméno a heslo mohlo být nebo že bylo zneužito, neprodleně kontaktovat ČNB na adrese abok@cnb.cz nebo telefonicky na kontaktních telefonních číslech +420 224 414 659, +420 224 412 119 nebo +420 224 412 531.

3. Ochrana soukromých klíčů příslušejících k systémovým certifikátům používaným pro přihlášení do ABO-K nebo pro Podpis dávky

a) Klient je povinen zajistit, aby soukromý klíč k certifikátu používanému v ABO-K spravoval s odbornou péčí expert znalý bezpečnosti informačních technologií.

4. Bezpečnost klientského počítače používaného pro přístup do ABO-K

a) Disponent je povinen na počítači, který používá pro přístup do ABO-K, používat pouze legálně nabytý software, u nějž výrobce garantuje podporu ve formě pravidelných bezpečnostních aktualizací, a tyto aktualizace pravidelně provádět. To platí zejména pro operační systém, prohlížeč internetových stránek Internet

Explorer a prohlížeče PDF.

b) Disponent je povinen mít na počítači, který používá pro přístup do ABO-K, nainstalovaný firewall a software zajišťující ochranu před viry, spamem a malwarem, a to v souladu s podmínkami uvedenými v bodu 4 písm. a) v průběžně aktualizované podobě; aktualizovat je třeba i virové a malwarové definice.

c) Disponent nesmí na počítači, který používá pro přístup do ABO-K, pracovat s vyššími než uživatelskými oprávněními (tj. nesmí používat oprávnění administrator, root), není-li použití vyššího než uživatelského oprávnění aktuálně nezbytné pro údržbu softwarového vybavení počítače[3].

d) Disponent je povinen být při práci s ABO-K přihlášen k operačnímu systému, a to pod dostatečně složitým PIN nebo heslem, které splňuje požadavky uvedené v bodě 1 písm. d), popřípadě na základě jiného mechanismu se stejnou nebo vyšší úrovní bezpečnosti.

e) Disponent je povinen vhodnými prostředky bránit neoprávněným osobám v užívání počítače, který používá pro přístup do ABO-K. Počítač je zejména třeba po dobu, kdy s ním Klient právě nepracuje, takto zabezpečit: po dobu krátké nepřítomnosti uzamknout, v případě delší nepřítomnosti vypnout.

5. Zabezpečení při vytváření souborů s Příkazy a při zpracování výpisů z ABO-K

a) Disponent je povinen opatřit Externí dávku uznávaným elektronickým podpisem nebo uznávanou elektronickou pečetí v zabezpečeném informačním systému[4] Klienta.

b) Disponent je povinen ověřovat pravost souborů s výpisy z Účtu kontrolou zaručené elektronické pečeti ČNB[5]. Pokud má Disponent jakékoli pochybnosti o pravosti souborů s výpisy z Účtu, neprodleně kontaktuje ČNB na adrese abok@cnb.cz nebo telefonicky na kontaktních telefonních číslech +420 224 414 659, +420 224 412 119 nebo +420 224 412 531.

6. Bezpečnostní pravidla při práci s Internetem

a) Disponent nesmí reagovat na žádné výzvy k poskytnutí přihlašovacích údajů do ABO-K obdržené prostřednictvím e-mailů, sociálních sítí, telefonicky nebo písemně v SMS či v jiné formě. ČNB za žádných okolností tímto způsobem přihlašovací údaje nepožaduje, jde vždy o snahu přihlašovací údaje podvodně vylákat (spam, phishing).

b) Disponent je povinen po přihlášení do ABO-K zkontrolovat na stránkách https://abok.cnb.cz existenci ikony „zámku“ v prohlížeči, který používá pro přístup do ABO-K. Po kliknutí na ikonu „zámku“ se zobrazí certifikát ČNB, který potvrzuje platnost a ověřuje identitu stránky aplikace. ČNB pro zabezpečení stránek ABO-K používá serverové certifikáty. Podrobné informace o vystaviteli a vlastnostech těchto certifikátů jsou dostupné na internetové stránce www.cnb.cz, v části Platební styk/Služby pro klienty, ceník/v části ABO-K internetové

[3] Vyšší oprávnění umožňující instalaci programového vybavení je bezpečnostním rizikem, které by mohlo umožnit třetí osobě instalaci škodlivého programu a ovládnutí počítače.
[4] Informační systém Klienta, který vytváří Externí dávku.
[5] Bližší informace k postupu ověřování lze nalézt uvnitř ABO-K, na adrese: https://abok.cnb.cz v části Různé/Návody, dokumenty.

bankovnictví/Dokumenty k ABO-K/Technické podmínky pro používání ABO-K. Pokud má Disponent jakékoli pochybnosti ohledně platnosti nebo pravosti certifikátu ČNB, neprodleně kontaktuje ČNB na adrese abok@cnb.cz nebo telefonicky na kontaktních telefonních číslech +420 224 414 659, +420 224 412 119 nebo +420 224 412 531.

7. Ochrana mobilního telefonu určeného pro přijímání SMS kódu pro přihlášení nebo autorizaci Dávek v ABO-K

a) Disponent je povinen chránit mobilní telefon, který je určen pro příjem SMS kódu tak, aby nemohl být tento kód zneužit třetí osobou. Je povinen tento mobilní telefon zabezpečit heslem a mít nastaveno automatické uzamčení tohoto mobilního telefonu.

b) Používá-li Disponent pro příjem SMS kódu chytrý mobilní telefon (mobilní telefon s operačním systémem Android, Windows, iOs apod.),
- nesmí provádět programové úpravy operačního systému (OS) tohoto mobilního telefonu, které umožňují plný administrátorský přístup (jedná se o úpravy typu: jailbreak u iOS/iPHONE, root u OS Android, a unlock/odemčení u OS Windows Phone),
- je povinen do tohoto mobilního telefonu instalovat aplikace a jejich aktualizace pouze z důvěryhodných zdrojů, tj. prostřednictvím aplikací nabízených dodavatelem operačního systému (Google Play, Windows Phone Store, Apple iTunes). Aplikace nesmí být instalovány z odkazů či příloh v e-mailech, na sociálních sítích či SMS,
- je povinen pravidelně aktualizovat operační systém tohoto mobilního telefonu.

8. Podezření na možný bezpečnostní problém

a) Klient i Disponent jsou povinni bezodkladně kontaktovat ČNB e-mailem na adrese abok@cnb.cz nebo telefonicky na kontaktních číslech +420 224 414 659, +420 224 412 119 nebo +420 224 412 531 v případě:
- neobvyklého chování aplikace ABO-K,
- podezření, že by mohlo dojít nebo že došlo k neautorizovaným Příkazům,
- při podezření, že by mohl být nebo že byl zneužit soukromý klíč příslušející k certifikátu, mobilní telefon, uživatelské jméno nebo heslo,
- pochybnosti o platnosti výpisu či certifikátu,

b) Klient je povinen při podezření na možný bezpečnostní problém poskytnout ČNB plnou součinnost při řešení vzniklé situace, tj. je zejména povinen
- řídit se pokyny ČNB,
- poskytnout všechny údaje požadované ČNB za účelem analýzy bezpečnostního problému.

Zásady bezpečného používání internetového bankovnictví:

Pro zvýšení bezpečnosti ABO-K ČNB dále, kromě výše uvedených minimálních požadavků, které jsou Klienti ČNB, jejich Disponenti a osoby, které pověřili zabezpečením systému, povinni dodržovat, doporučuje i dodržování následujícího:

a) Je-li to možné, měla by administrátorskými oprávněními disponovat jen osoba odlišná od Disponenta.

b) Klient by měl zvyšovat zabezpečení počítačů používaných pro Přístup do ABO-K, zejména
   - systematickým vyhledáváním známých zranitelností a omezením přístupu z těchto počítačů k nebezpečnému obsahu a adresám v Internetu, a
   - pravidelným prováděním bezpečnostního auditu informačního systému s kontrolou zaměřenou na dodržování bezpečnostních zásad při práci s ABO-K.

c) Klient by měl pravidelně instalovat aktualizační soubory i pro programy, které nejsou nezbytné pro běh ABO-K. Aktualizace odstraňují chyby a zranitelnosti programového vybavení a snižují bezpečnostní rizika.

d) Disponent by neměl na počítači, který používá pro práci s ABO-K, používat externí paměťová média bez toho, že u nich nejprve provede kontrolu na přítomnost virů a malware.

e) Pokud má Disponent v počítači, který používá pro práci s ABO-K, programy, které nepoužívá, měl by tyto nepotřebné programy odinstalovat.

f) Disponent by neměl z počítače, který používá pro práci s ABO-K, vstupovat na internetové stránky s pochybným obsahem, otevírat na něm přílohy z nevyžádaných či podezřelých e-mailů ani odkazy v takových e-mailech obsažené.

g) Disponent by měl při nestandardním chování prohlížeče internetových stránek upozornit svého správce počítače (známým typickým neobvyklým chováním prohlížeče internetových stránek při napadení malware je například jeho zpomalování či nemožnost spustit některé jeho standardní funkce, samovolné vyskakování nežádoucích oken, nemožnost otevřít některé stránky, které jsou obvykle dostupné atd.).

h) Disponent by z tzv. „chytrého“ mobilního telefonu sloužícího pro příjem Přihlašovacího SMS kódu nebo Autorizačního SMS kódu neměl vstupovat na stránky s pochybným obsahem, otevírat přílohy nevyžádaných či podezřelých e-mailů, SMS či zpráv na sociálních sítích ani odkazy v takových e-mailech, SMS či zprávách obsažené.

Aplikace ABO-K není podporována a určena pro používání v mobilních zařízeních (mobilní telefon, tablet), proto by Klient a jeho Disponenti měli aplikaci používat výhradně v osobních počítačích (PC, notebook).

Je třeba zdůraznit, že sebekvalitnější ochrana a výše popsaná bezpečnostní opatření se neobejdou bez uvážlivého přístupu ze strany Klienta a jeho Disponentů a jejich obezřetného chování při používání služby ABO-K.