Bezpečnostní zásady

Česká národní banka (ČNB) věnuje trvalou pozornost nadstandardnímu zabezpečení aplikace ABO-K internetové bankovnictví (dále jen „ABO-K“), proto 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 a předávání souborů s Příkazy, zajištění ochrany soukromého klíče[1] příslušejícího k podpisovému i přístupovému certifikátu, klientského počítače a systémového prostředí.

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

1. Ochrana soukromých klíčů příslušejících k osobním certifikátům používaným pro Přístup do ABO-K nebo pro podepisování dávek s příkazy

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 je povinen při používání čipové karty nebo USB tokenu, na nichž je uložen soukromý klíč k certifikátu používanému pro Přístup do ABO-K nebo pro Podepisování dávek s Příkazy, ponechávat tato zařízení ve čtečce čipových karet, resp. v USB portu pouze po dobu potřebnou pro práci s čipovou kartou nebo USB tokenem. Disponent je povinen před odchodem od počítače ukončit práci s ABO-K odhlášením a zavřením okna internetového prohlížeče, a vyjmout čipovou kartu / USB token, na kterých je uložen soukromý klíč Klienta příslušející k jeho osobnímu certifikátu.

d) Disponent je povinen při používání čipové karty nebo USB tokenu, na nichž je uložen soukromý klíč k certifikátu používaného pro Přístup do ABO-K nebo pro Podepisování dávek s Příkazy, tato zařízení zabezpečit heslem, které splňuje následující podmínky:

- musí být tvořeno kombinací nejméně jednoho velkého a jednoho malého písmene, jedné číslice a jednoho speciálního znaku (např. plus, mínus, otazník, hvězdička nebo tečka),
- musí mít nejméně 8 znaků,

[1] Soukromým klíčem příslušejícím ke kvalifikovanému certifikátu se rozumí data pro vytváření elektronického podpisu nebo elektronické značky ve smyslu Zákona č. č. 227/2000, o elektronickém podpisu (dále jen „soukromý klíč“)

- nesmí být tvořeno ze slov či kombinací čísel, která představují jména, přezdívky, data narození ani telefonní čísla Klienta či jeho rodinných příslušníků,
- musí být odlišné od PINů a hesel používaných v jiných aplikacích Klienta,
- musí být pravidelně měněno, nejméně jednou za kalendářní čtvrtletí.

e) Disponent nesmí heslo k čipové kartě nebo USB tokenu, na nichž je uložen soukromý klíč k certifikátu používaného pro Přístup do ABO-K nebo pro Podepisování dávek s Příkazy,

- zaznamenat takovým způsobem, aby k nim umožnil přístup třetí osobě (tj. zejména zaznamenat do diářů a na poznámkové papírky nalepené na nebo položené v blízkosti počítače), nebo na obal čipové karty či USB tokenu,
- zaznamenat takovým způsobem, ze kterého je zřejmé, že se jedná o 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 hesel v nastavení počítače nebo mobilního telefonu.

2. Ochrana soukromých klíčů příslušejících k systémovým certifikátům používaným pro Přístup do ABO-K nebo pro Podepisování dávek s Příkazy

a) Pokud Klient používá systémový certifikát, je povinen zajistit, aby soukromý klíč k němu příslušející spravoval s odbornou péčí expert znalý bezpečnosti informačních technologií.

3. 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 a prohlížeče PDF, jsou-li na počítači nainstalovány.

b) Disponent je povinen mít na počítači, který používá pro Přístup do ABO-K, nainstalovaný software zajišťující ochranu před viry, spamem, malwarem, a firewall, a to v souladu s podmínkami uvedenými v bodu 3 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.[2]

d) Disponent je povinen být při práci s ABO-K přihlášen k operačnímu systému pomocí uživatelského (neprivilegovaného) účtu bez administrátorského oprávnění, a to pod dostatečně složitým heslem, které splňuje požadavky uvedené v bodě 1

[2] Vyšší oprávnění umožňují instalaci programového vybavení a jsou bezpečnostním rizikem, které by mohlo umožnit třetí osobě instalaci škodlivého programu a ovládnutí počítače.

písm. e), 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.

4. Zabezpečení systémů určených pro přípravu souborů s Příkazy a pro zpracování výpisů z ABO-K

a) Disponent je povinen opatřit Externí dávku uznávaným elektronickým podpisem nebo uznávanou elektronickou značkou v zabezpečeném informačním systému[3] Klienta.

b) Disponent je povinen ověřovat pravost souborů s výpisy z Účtu kontrolou elektronické značky ČNB v zabezpečeném informačním systému Klienta.[4,5] Pokud má Disponent jakékoli pochybnosti o pravosti souborů s výpisy z Účtu, neprodleně kontaktuje ČNB na adrese abok@cnb.cz nebo telefonicky na číslech +420 224 412 531 nebo +420 224 414 659.

5. Bezpečnostní pravidla při práci s Internetem

a) Disponent nesmí reagovat na výzvy obdržené prostřednictvím e-mailů, sociálních sítí či telefonicky (včetně SMS) k poskytnutí přihlašovacích údajů do ABO-K. 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“ lze zobrazit certifikát ČNB, který potvrzuje platnost a ověřuje identitu stránky ABO-K. ČNB pro zabezpečení stránek ABO-K používá serverové certifikáty vydané společností Symantec, jejíž certifikát vydala společnost VeriSign. Pokud má Disponent jakékoli pochybnosti o platnosti certifikátu ČNB, neprodleně kontaktuje ČNB na adrese abok@cnb.cz nebo telefonicky na číslech +420 224 412 531 nebo +420 224 414 659.

6. Ochrana mobilního telefonu určeného pro přijímání potvrzovacích SMS kódů podle článku 14 Podmínek pro ABO-K

a) Disponent je povinen chránit mobilní telefon, který je určen pro přijímání potvrzovacích SMS kódů tak, aby nemohly být SMS kódy zneužity třetí osobou. Je povinen tento mobilní telefon zabezpečit heslem a mít nastaveno automatické

[3] informační systém Klienta, který vytváří datový soubor s Příkazy (Externí dávku)

[4] Vyhláška 212/2012 Sb. o struktuře údajů, na základě kterých je možné jednoznačně identifikovat podepisující osobu, a postupech pro ověřování platnosti zaručeného elektronického podpisu, elektronické značky, kvalifikovaného certifikátu, kvalifikovaného systémového certifikátu a kvalifikovaného časového razítka (vyhláška o ověřování platnosti zaručeného elektronického podpisu)

[5] bližší informace k postupu ověřování lze nalézt na stránkách https://abok.cnb.cz v části Různé/Návody, dokumenty

uzamčení tohoto mobilního telefonu, pokud jej Disponent nepoužívá.

b) Používá-li Disponent pro přijímání potvrzovacích SMS kódů 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 jeho operační systém.

7. Podezření na možný bezpečnostní problém

a) Klient i Disponent jsou povinni bezodkladně kontaktovat ČNB e-mailem na adrese abok@cnb.cz nebo telefonicky na číslech +420 224 412 531 nebo +420 224 414 659 v případě:

- neobvyklého chování aplikace ABO-K,
- podezření, že by mohlo dojít nebo že došlo k neautorizovaným Příkazům v ABO-K,
- při podezření, že by mohl být nebo že byl zneužit soukromý klíč příslušející k certifikátu,
- pochybnosti o platnosti výpisu (bod 4 písm. b)) či certifikátu (bod 5 písm. b))

a dohodnout se s ČNB na dalším postupu.

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 zjištění a odstranění bezpečnostního problému, popřípadě umožnit osobě pověřené ČNB přístup (včetně kopírování souborů) ke Klientovu počítači za účelem nalezení a analýzy bezpečnostního problému.

Doporučení nad rámec výše uvedených povinností:

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:

- Je-li to možné, měla by administrátorskými oprávněními disponovat jen osoba odlišná od Disponenta.
- 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.
- 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.
- 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.
- Pokud má Disponent v počítači, který používá pro práci s ABO-K, programy, které nepoužívá, měl by tyto nepotřebné programy odinstalovat.
- 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.
- 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.).
- Disponent by z tzv. „chytrého“ mobilního telefonu sloužícího pro příjem potvrzovacích SMS kódů 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.
- Disponent by měl při podezření, že by mohl být nebo že byl zneužit soukromý klíč jeho certifikátu, neprodleně tento certifikát zneplatnit u certifikační autority, která jej vydala, v souladu se Zákonem o elektronickém podpisu.