

Bezpečnostní zásady uživatele služby ABO-K

1. Úvod

Česká národní banka (ČNB) věnuje trvalou pozornost nadstandardnímu zabezpečení aplikace ABO-K internetové bankovníctví (dále jen ABO-K), proto implementovala moderní technologie pro ochranu důvěrnosti a integrity jeho aktiv, dostupnosti a spolehlivosti celé aplikace.

Pro zajištění bezpečnosti autorizace platební transakce je využívána funkce elektronického podpisu/elektronické značky pomocí kvalifikovaného certifikátu vydaného akreditovanou certifikační autoritou.

Přes veškerá opatření, realizovaná zejména v systémovém prostředí ČNB, je nutné věnovat náležitou pozornost také rizikům na straně klienta, resp. jeho disponentů, vyplývajících ze způsobu přípravy a předání dávek s příkazy, zajištění ochrany podpisového certifikátu, klientské stanice a systémového prostředí.

Dodržováním těchto bezpečnostních zásad lze tato rizika eliminovat.

2. Rizika a jak se jim bránit

- ☛ **Nezajištěná ochrana informačních systémů, v nichž se připravují dávky s příkazy, představuje největší nebezpečí, které spočívá v podvržení příkazů ještě před podpisem dávky a předáním dávky ke zpracování. Následně je dávka podepsána a odeslána disponentem, který si podezřelého příkazu nevšimne.**

Jak k tomu může dojít: Informační systém na straně klienta vytvoří soubor s dávkou a uloží jej na disk klientské stanice přístupující do ABO-K. K tomuto souboru má přístup jiný uživatel v síti, např. administrátor, kolega, servisní organizace, případně i útočník prostřednictvím škodlivého softwaru, který může soubor pozměnit běžným editorem.

Jak tomu předcházet: Nesdílet PC, zabránit neřízenému přístupu administrátorů, servisu, zajistit ochranu před škodlivým softwarem a minimalizovat dobu, po kterou je soubor na disku nechráněn. Soubor musí být neprodleně zpracován po svém vytvoření, disponent nesmí opustit PC v době mezi vytvořením souboru a jeho podepsáním. K povinnostem klienta patří zajištění kontroly všech údajů podepisované dávky a následná kontrola a stažení výpisu z účtu opatřeného elektronickou značkou ČNB.

- ☛ **Privátní klíč kvalifikovaného certifikátu je určen výhradně svému uživateli - disponentovi. Nedostatečná ochrana privátního klíče umožní potenciálnímu útočníkovi tento klíč nebo celý certifikát získat a následně vložit a elektronicky podepsat dávku stejným způsobem jako disponent.**

Jak k tomu může dojít: Například, když disponent svěří instalaci certifikátu třetí osobě, nebo jej uloží do PC v exportovatelném tvaru, případně nezvolí silný způsob jeho zabezpečení (zabezpečení heslem) či nastaví příliš slabé heslo.

Jak tomu předcházet: ČNB doporučuje pořídit certifikát instalovaný na tokenu nebo čipové kartě přímo u certifikační autority, v ostatních případech je nezbytné instalovat certifikát do PC v režimu silného zabezpečení, bez možnosti jeho exportu a se silným heslem (alespoň 10 znaků, s volbou malých i velkých písmen, číslic a nealfanumerických znaků). Certifikát, zejména privátní klíč, disponent v žádném případě nepředává třetí osobě.

- ☛ **Nedostatečné zabezpečení klientské stanice přistupující k Internetu může způsobit nežádoucí zavlečení softwaru, kterého útočník využije ke skrytému spojení do aplikace nebo krádeži privátního klíče kvalifikovaného certifikátu, případně jeho hesla.**

Jak k tomu může dojít: Neopatrným prohlížením webových stránek nebo otevíráním příloh elektronické pošty si může disponent stáhnout škodlivý software (vir, trojský kůň, spyware) na své PC přistupující k ABO-K nebo nechat odvést komunikaci skrze útočnickův systém. Následně je pak celá komunikace „řízena“ útočnickovým softwarem nebo systémem.

Jak tomu předcházet: Disponent je povinen uplatňovat základní zásady obezřetnosti při prohlížení webových stránek Internetu a při otevírání zejména nevyžádané pošty, používat firewally, antivirové, antispamové, či antimalwarové programy pro zvýšení ochrany svého PC a systémového prostředí. Dále je nutné věnovat pozornost pravidelnému a systematickému vyhledávání zranitelností v systému (chybějící opravy softwaru, chybné konfigurace, slabá hesla) a zajistit jejich odstranění.

- ☛ **Sdílená prostředí v rámci organizační struktury klienta představují riziko přístupu dalších osob ke klientské stanici, např. IT specialistů, administrátorů či servisní organizace.**

Jak k tomu může dojít: V organizaci mohou k PC disponenta přistupovat IT specialisté, helpdesk, servisní organizace, kolegové sdílející jeho PC a další, v domácím prostředí např. rodinní příslušníci.

Jak tomu předcházet: Důsledným řízením přístupových práv, volbou bezpečného úložiště pro podpisový klíč na tokenu nebo čipové kartě.

- ☛ **Útočníci využívají celé škály metod sociálního inženýrství a prostředků, aby vylákali přihlašovací údaje disponentů pro přístup do ABO-K.**

Jak k tomu může dojít: Prostřednictvím podvržené webové stránky disponent nevědomky poskytne své osobní údaje cizí osobě.

Jak tomu předcházet: Nereagovat na nevyžádanou elektronickou poštu a jiné formy vylákání přihlašovacích údajů (tzv. phishing). ČNB nikdy takové údaje od svých klientů nevyžaduje, a proto lze každý takový pokus prostřednictvím jména ČNB považovat za falešný.

3. Povinnosti klienta

Klient je povinen:

- a) zajistit vysokou úroveň zabezpečení systému pro přípravu dávek určených pro zpracování v ABO-K, aby s nimi nebylo možné neautorizovaným způsobem manipulovat před předáním do ABO-K,
- b) zajistit adekvátní úroveň zabezpečení klientských počítačů disponentů, zejména prostředky firewallů, antivirového, antispamového softwaru a dalšími prostředky pro ochranu před škodlivým softwarem, zejména viry, trojskými koni, spamem, spyware apod., dále systematickým vyhledáváním známých zranitelností, aktualizací operačního systému a instalovaných aplikací a dále omezením přístupu klientských stanic k nebezpečnému obsahu a adresám v Internetu,
- c) zajistit systémovou a fyzickou ochranu privátního klíče certifikátu pro vytváření elektronického podpisu/elektronické značky nejlépe technickými prostředky (token, čipová karta) na principu „potřeby mít a znát“ nebo alespoň nastavením vysoké úrovně zabezpečení, tj. s přístupem pouze přes silné hesla, při uložení klíčů do zabezpečeného softwarového úložiště na klientské stanici a v neexportovatelném tvaru,
- d) zajistit pravidelné aktualizace a opravy softwaru, především operačního systému, prohlížeče webových stránek a dalších instalovaných aplikací,
- e) přihlášení disponenta k operačnímu systému realizovat pomocí standardního uživatelského účtu bez administrátorského oprávnění, a dostatečně složitého hesla, resp. na základě jiného mechanismu s odpovídající nebo vyšší úrovní bezpečnosti,
- f) vhodnými prostředky bránit neoprávněným osobám v užívání počítače a zejména ABO-K, např. odhlášením nebo alespoň uzamčením počítače v době nepřítomnosti disponenta,
- g) nereagovat na výzvy k poskytnutí přihlašovacích údajů třetími osobami (spam, phishing), přihlašovací údaje jsou určeny pouze danému disponentovi a ČNB je nikdy za žádných okolností tímto způsobem nepožaduje,
- h) zajistit co nejbezpečnější způsob předání dávek s příkazy, optimálně tak, aby byla dávka elektronicky podepsána již v systému, ve kterém jsou dávky v prostředí klienta připravovány,
- i) zajistit kontrolu správnosti všech zadaných příkazů, jejich počtu a součtu převáděné částky v průběhu realizace elektronického podpisu/elektronické značky a před předáním dávky ke zpracování,
- j) zajistit bezodkladné předání dávek ke zpracování,
- k) ověřovat věrohodnost elektronického výpisu z účtu kontrolou elektronické značky ČNB a ukládat je pro potřeby případných reklamací,

- l) ověřovat správnost zaúčtování transakcí pomocí položkové kontroly ověřeného výpisu z účtu ČNB oproti souborům s dávkami vloženými do ABO-K za předpokladu, že je vyloučena nežádoucí modifikace těchto souborů mezi okamžikem jejich vytvoření a okamžikem jejich podepsání v ABO-K; pokud tato jistota není, pak je nutná kontrola oproti původním dokladům, na jejichž základě transakce proběhly,
- m) v případě podezření na bezpečnostní incident bezodkladně zajistit zablokování přístupu do ABO-K a odvolání platnosti kvalifikovaného certifikátu pro elektronický podpis/elektronickou značku, případně certifikátu pro přihlášení, u příslušné certifikační autority. Dále neprodleně kontaktovat ČNB, sekci peněžní a platebního styku a dohodnout další postup (zablokování účtu, určení alternativního disponenta apod.). Kontakt: abo@cnb.cz, tel.:+420-2-2441-2531 nebo 4659. Případně rovněž zablokovat oprávnění všech disponentů, uvedených v Podpisových vzorech pro ABO-K, komunikovat s ČNB prostřednictvím ABO-K, a to předáním vyplněného tiskopisu „Zrušení přístupu do ABO-K“.

4. Potvrzovací SMS kód

ČNB doporučuje všem klientům, aby jako ochranu před použitím soukromého klíče pro předání dávky s příkazy neoprávněnou osobou volili prostřednictvím tiskopisu Podpisové vzory pro ABO-K službu **potvrzovací SMS kódy**, a to optimálně pro všechny disponenty, kteří jsou oprávněni předávat dávky s příkazy.

Je-li nastavena tato služba, dávka s příkazy se nepředá okamžitě, ale ABO-K zašle potvrzovací SMS kód na mobilní telefon disponenta, který dávku předává. SMS obsahuje kromě potvrzovacího kódu rovněž údaj o **celkovém počtu příkazů v dávce** a o **součtu částek příkazů v dávce**, která je připravena k předání. ČNB doporučuje, aby disponent vždy před odesláním dávky provedl kontrolu souhlasnosti s dávkou s příkazy, kterou se chystá prostřednictvím ABO-K předat. Po provedení kontroly disponent zadá zasláný potvrzovací SMS kód a předá dávku s příkazy ke zpracování.