Internetové bankovnictví: Kde je bezpečné?

Banky chrání účty svých klientů různými způsoby. Jaké metody využívají české banky a jaké má jejich zabezpečení slabiny? Na co si musí klient využívající internetové bankovnictví dát největší pozor?

PETR ZÁMEČNÍK

V poslední době se rozšířily pokusy získat od klientů bank jejich citlivé údaje. Prostřednictvím podvodných e-mailů byli klienti České spořitelny vyzýváni, aby v rámci ověření (neexistující) transakce, potvrzení fiktivní výhry či varování před podvodnými e-maily předali své údaje. Zatímco celosvětově se nejčastějším terčem phishingových akcí stává Citibank, jejíž klienti nejsou v bezpečí ani v České republice (první český phishingový e-mail, psaný dokonce téměř bez gramatických chyb, byl odeslán právě s hlavičkou Citibank), na našem území je nejčastějším terčem největší česká retailová banka Česká spořitelna.

Zabezpečení internetového bankovnictví

Internetové bankovnictví lze zabezpečit více způsoby a každá banka využívá kombinaci několika metod – od certifikace stránek přes zabezpečení komunikačního kanálu mezi bankou a klientem až po monitoring provozu. Nezbytnou součástí a zároveň nejslabším článkem celého zabezpečení je ověření identity klienta – tedy zda za počítačem připojeným k bankovnímu systému sedí klient, který je oprávněn nakládat s účtem.

Pro ověření klienta využívají banky celou řadu prostředků, jejichž základem je uživatelské jméno a heslo. Dalšími, podpůrnými ověřovacími prostředky mohou být například podpisové certifikáty, mobilní telefony, nebo PIN kalkulátory.

Novinkou je generátor jednorázových hesel pomocí aplikace uložené na čipové platební kartě od BAWAG Bank.

Přístup jednotlivých bank k otázce zabezpečení je velmi rozdílný. Některé banky již „standardně" nabízejí vyšší úroveň zabezpečení, jiné mají k dispozici pouze nižší úroveň zabezpečení a další nabízejí vyšší formu zabezpečení pouze za příplatek (nejčastěji ve formě dokoupení PIN kalkulátoru). Jak se tedy k ověřování klienta staví jednotlivé české banky?

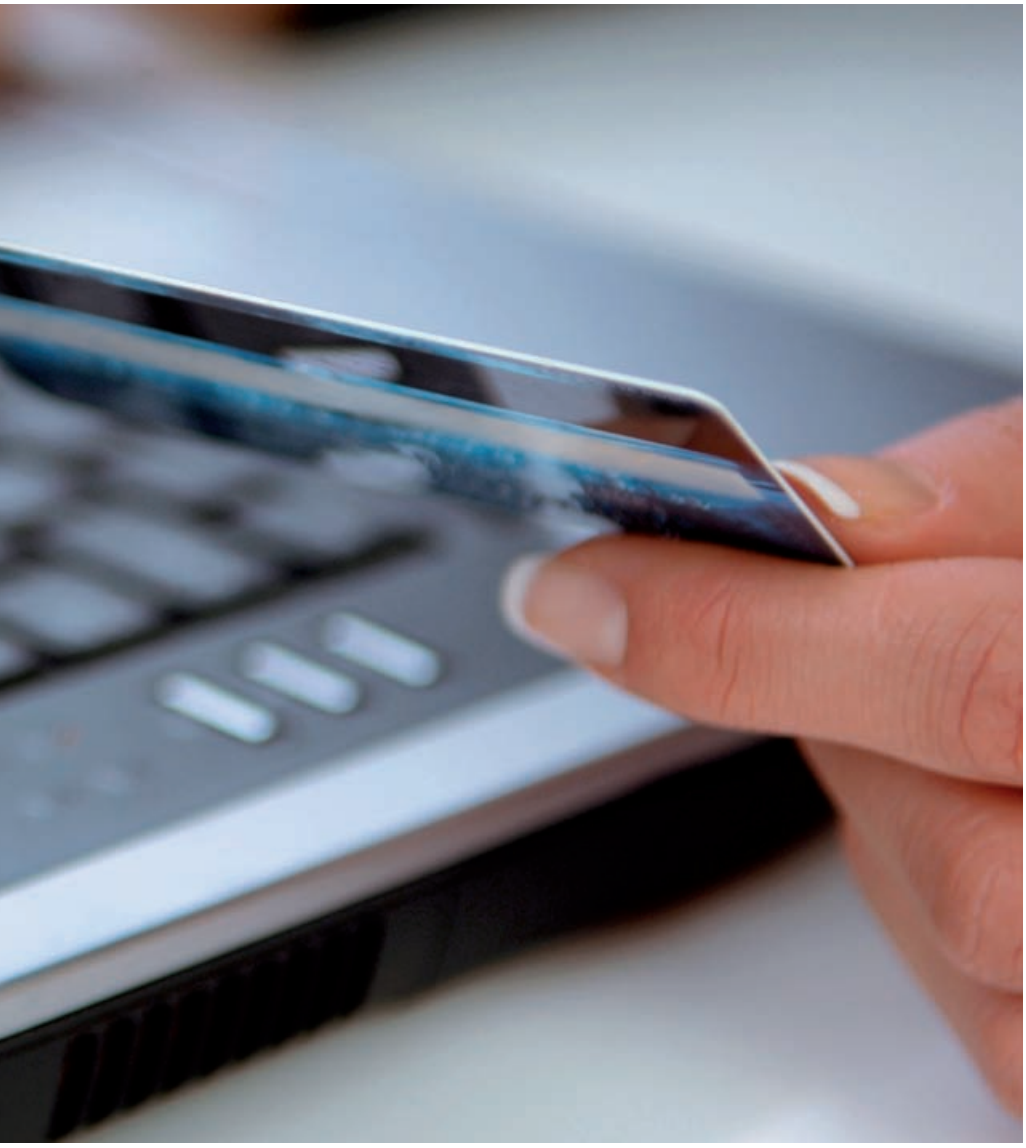
BAWAG Bank

BAWAG Bank využívá jako základní ověřovací mechanismus klienta (vedle uživatelského jména a hesla) podpisový certifikát, který by měl mít klient uložený na přenosném médiu. Novinkou je možnost autentifikace (ověření identity) klienta a následná autorizace aktivních pokynů (např. platebních příkazů) pomocí autentifikátoru (PIN kalkulátoru) a čipové karty s nahranou příslušnou aplikací.

PŘÍSTUP K ZABEZPEČENÍ SE LIŠÍ

Banky nabízejí různé úrovně zabezpečení a liší se též jejich postoj k bezpečnějším, ale nákladnějším řešením. Některé nabízejí vyšší úroveň zabezpečení jako standard, jiné si ji nechají dobře zaplatit. Při výběru banky, u níž chce klient využívat i internetové bankovnictví, by měl způsob zabezpečení hrát důležitou roli.

Důležitá je též otázka odpovědnosti banky za případnou škodu. Odpovědnost při zneužití je sice právně postavena na klienta, banky se však vzhledem k obavám z negativní reklamy často přiklánějí k dohodě a škodu uhradí. Tím, kdo může bezpečnost svým přístupem nejvíce ovlivnit, ale stále zůstává především klient.



Autentifikátor v kombinaci s čipovou kartou, která může být platební nebo vydaná přímo k tomuto účelu, generuje jednorázová hesla. Případný útočník by k narušení účtu musel získat jak čipovou kartu s PIN, tak autentifikátor, a navíc i uživatelské jméno klienta. Jedná se o jeden z nejbezpečnějších způsobů zabezpečení. Čtečka čipové karty je klientům poskytována zdarma, pouze v případě ztráty či zničení klient za novou zaplatí 273,70 Kč.

Citibank

Citibank je nejčastějším bankovním terčem útočníků na data klientů. Citibank je podle některých kritérií největší světovou bankou, a tak je zde dostatek potenciálních obětí. Kromě toho pro přístup k účtu využívala tato banka identifikační údaje platební karty. To je samo o sobě ojedinělé a nezvyklé – a navíc krajně nebezpečné.

Kromě dříve užívaného přístupu k účtu prostřednictvím uživatelského jména a hesla, kterým byly identifikační údaje platební nebo kreditní karty, nyní Citibank využívá k ověření identity klienta též kód vygenerovaný PIN kalkulátorem. Ten si ovšem klient musí pořídit za 450 Kč.

Zvláštností (a potenciálním bezpečnostním rizikem) je nabídka registrace k užívání internetového bankovnictví přímo u přihlašovacího formuláře. Po kliknutí na odkaz „Registrace“, který je na vstupní stránce internetového bankovnictví, se klient přenese na stránku vyžadující číslo karty a PIN… Stránka je sice ověřená společností VeriSign a patří Citibank, nicméně banka opět na internetových stránkách vyžaduje číslo karty a PIN.

Česká spořitelna

Česká spořitelna rozlišuje identifikaci klienta, kde postačuje uživatelské jméno (přidělené bankou) a heslo (volené klientem), což ovšem lze rozšířit i o další bezpečnostní prvky (certifikát na či-

INFO

Způsoby zabezpečení e-bankovnictví

UŽIVATELSKÉ JMÉNO A HESLO

Uživatelské jméno a heslo je nejjednodušším, ale zároveň nejméně bezpečným způsobem zabezpečení internetového bankovnictví. Banky od tohoto způsobu upouštějí, některé umožňují v tomto případě pouze pasivní operace (tj. zjistit stav a pohyby na účtu, nikoli však zadávat platební příkazy). Zabezpečení je náchylné nejen na vyzrazení hesla a uživatelského jména, ale také na „odposlech“ klávesnice.

SMS KÓD

Kód zasílaný prostřednictvím SMS zpráv je nejoblíbenějším způsobem zabezpečení. Využívají se dvě možnosti – klasická SMS zpráva, která je méně bezpečná, a šifrovaná SMS s využitím tzv. SIM Toolkitu. V tomto případě je třeba dbát na bezpečnost mobilního telefonu. Kritickým bodem je též změna čísla telefonu, na které se SMS zprávy zasílají. Aby byl systém bezpečný, je třeba mít možnost změnit číslo telefonu pouze na pobočce po ověření totožnosti klienta.

CERTIFIKÁT

Podpisový certifikát uložený v souboru slouží k ověření identity klienta. Jeho nevýhodou je možnost zkopírování certifikátu a jeho následného zneužití. Certifikát by měl být uložen na přenosném médiu, které uživatel připojuje k počítači při využívání internetového bankovnictví. Zásadní chybou je uložení certifikátu na pevném disku v počítači, nebo dokonce na internetu. Bezpečnější jsou certifikáty na čipové kartě či iKey tokenu.

CERTIFIKÁT NA ČIPOVÉ KARTĚ

Certifikát na čipové kartě či iKey tokenu má tu výhodu, že ho nelze zkopírovat. Případný útočník by musel získat kartu i hesla, která ji chrání.

PIN KALKULÁTOR

PIN kalkulátor je generátor hesel pro vstup a pro ověření transakcí. Klient pro ověření pokynu musí zadat atributy transakce i do kalkulátoru a na jejich základě je mu vygenerován PIN. Jedná se o jeden z nejbezpečnějších způsobů ověření. Novinkou je kombinace generátoru jednorázových hesel s čipovou kartou, kterou přinesla BAWAG Bank.

TAN

TAN kódy jsou jednorázové kódy zasílané zpravidla poštou, které slouží k ověření klienta i potvrzení transakce. Klientovi je vydána vždy sada hesel (zpravidla 50 až 100), po jejichž spotřebování obdrží nová. Tento systém je poměrně bezpečný, nebezpečím je ale případná ztráta kódů.

pové kartě či PIN kalkulátor), a autorizaci aktivních transakcí, kdy je vyšší zabezpečení vyžadováno.

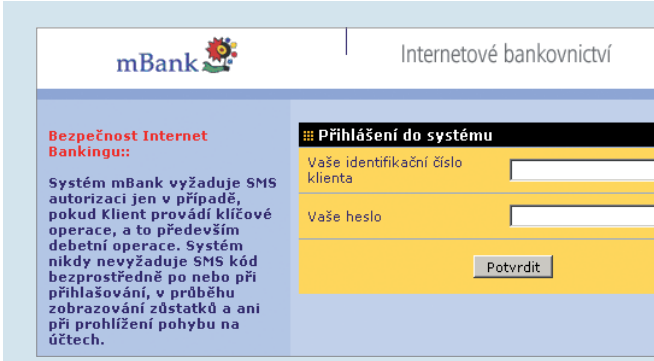
K autorizaci plateb lze využít buď certifikát na čipové kartě, nebo PIN kalkulátor (využívá-li klient tyto možnosti, je vhodné je užívat i ke vstupu na účet), případně zaslání nešifrované SMS zprávy na mobilní telefon. Klienti tak mají poměrně široký výběr.

Cenově nejdostupnější je kombinace přístupu k účtu prostřednictvím uživatelského jména a hesla a ověřování transakcí SMS kódem. V takovém případě klient nedoplácí nic nad cenu samotné služby. Za čtečku čipových karet zaplatí 350 Kč, za čipovou kartu 320 Kč a dále je třeba počítat s nákladem na vygenerování a roční obnovu certifikátu ve výši 320 Kč. PIN kalkulátor Česká spořitelna již nenabízí a mohou ho využívat pouze klienti, kteří ho již mají.

ČSOB

ČSOB nabízí tři způsoby přihlášení k účtu a dva způsoby autorizace platebních transakcí. Přihlásit k účtu se lze prostřednictvím uživatelského jména a hesla, které je možné podpořit ještě SMS kódem, nebo pomocí certifikátu na čipové kartě. SMS kód nebo čipovou kartu je nutné využívat pro aktivní operace.

Čtečky čipových karet nabízí ČSOB v ceně od 500 Kč do 1 950 Kč. Výhodou tohoto zařízení je, že je univerzální a že si ho klient může opatřit i jinde, případně využít čtečku, kterou získal v jiné bance. Vydání čipové karty s certifikátem vyjde mnohem levněji než v České spořitelně – na 100 Kč. Za obnovu čipové karty pak klient platí 100 Kč a stejnou částku si musí připravit i na pravidelnou roční obnovu certifikátu. ČSOB umí vydat též zaručený podpis, který lze využívat v komunikaci se státní správou. Za aktivaci SMS zasílání kódů klient nic neplatí.



mBank: K přihlášení uživatelské jméno a heslo, pro ověření aktivních operací zaslaný SMS kód.

eBanka

eBanka byla průkopníkem internetového bankovnictví. Již od počátku svého působení na trhu (tehdy jako Expandia banka) nabízí tři způsoby ověření klienta i autorizace plateb: certifikát, PIN kalkulátor a šifrované SMS zprávy.

Banka si účtuje za nahrání aplikace do SIM Toolkit jednorázově 50 Kč, další náklady již klient nemá až do výměny telefonu, resp. SIM karty. Lze využívat i nešifrované SMS zprávy, ovšem pouze v odůvodněných případech. Při používání jednorázových hesel, což je další z možností, která není bankou preferována, si klient připlatí 20 Kč měsíčně. Oproti ceně za PIN kalkulátor, kdy platí měsíčně 89 Kč, se však jedná o nevýznamnou položku. Certifikát je levnější, klienta vyjde pouze na 100 Kč ročně.

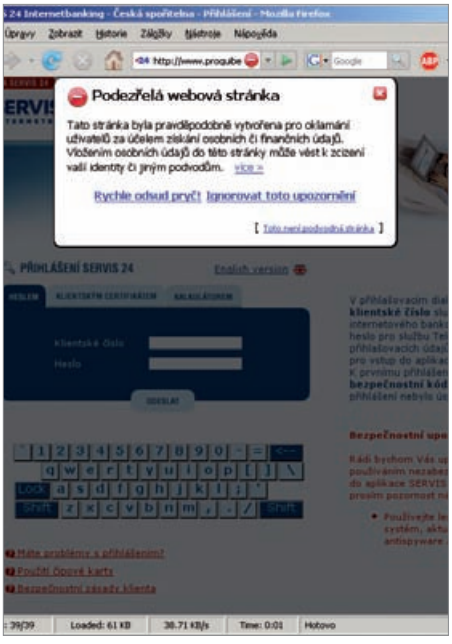
Fio, družstevní záložna

Zatímco eBanka byla první bankou, která v České republice uvedla internetové bankovnictví, Fio, družstevní záložna, ji o několik měsíců předběhla a byla první finanční institucí nabízející tuto službu. Vzhledem k pochmurné minulosti družstevního záložnictví se na ni však při udílení vavřínů za prvenství často zapomíná.

Pro identifikaci klienta využívá Fio uživatelské jméno a heslo. Pokud chce klient provést aktivní transakci, musí si nainstalovat podpisovou aplikaci. Klient je však vyzýván, aby certifikát instaloval pouze na bezpečné a dostatečně zabezpečené počítače. Vyšší úroveň zabezpečení není k dispozici. Certifikát je poskytován zdarma.

GE Money Bank

GE Money Bank nabízí dvě možnosti přihlášení k internetovému bankovnictví. Při použití jednodušší varianty přístupu, která má ale limitovaný objem denních transakcí, stačí zadat uživatelské jméno a heslo, na základě nichž je klientovi zaslán osmimístný kód na mobilní telefon, pomocí něhož se přihlásí do aplikace. Pro přihlášení do aplikace lze zasílání SMS kódu vypnout a používat ho



Obrana: Některé phishingové útoky dokáže odhalit i Firefox.

INFO

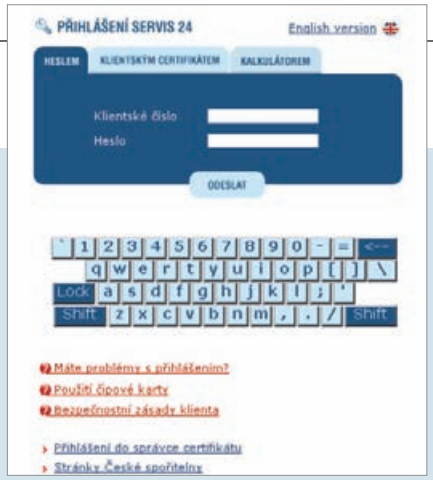
Jednoduchá obrana

Nejlepší obranou proti phishingu je dodržování základních bezpečnostních pravidel.

V prvé řadě to znamená nereagovat na nevyžádané e-maily „od banky". Pokud se již klient dostane na stránky internetového bankovnictví, neměl by kamkoliv zadávat citlivé údaje, které po něm banka dříve nevyžadovala. Jestliže „banka" nové údaje vyžaduje (zpravidla se zdůvodněním „zvýšení bezpečnosti"), je lepší si tuto informaci ověřit – nejlépe na infolince banky. Stránky pro přístup k internetovému bankovnictví mají vždy certifikát vydaný renomovanou společností (nejčastěji VeriSign), který zaručuje, že se skutečně jedná o stránky, za které se vydávají. To je dobrou pomůckou v případě, že si klient není jistý, zda je na správném místě.

Banky vždy klienty varují:
„NIKDY VÁM NEZASÍLÁME NEVYŽÁDANÉ E-MAILY."
Zasílají pouze potvrzení transakcí, o které klient v aplikaci zažádá. Možná i proto jsou úspěšné phishingové e-maily typu „Vaše transakce byla zamítnuta"...
„Jaká, když jsem žádnou neprováděl, to musím zkontrolovat," říká si obeslaný klient.

„NIKDY PO VÁS NECHCEME ČÍSLO KARTY ANI PIN."
To je možná důvod, proč je tak oblíbeným terčem Citibank – uživatelským jménem pro vstup do internetového bankovnictví bylo ještě nedávno číslo platební karty...



Česká spořitelna: K základní identifikaci klienta postačuje uživatelské jméno a heslo, které se zadává pomocí grafické klávesnice.

pouze k ověření aktivních operací. Druhou možností je přihlašování prostřednictvím certifikátu. Aktuální ani připravovaný sazebník poplatků neobsahuje žádnou platbu za vystavení certifikátu.

ING Bank

ING nabízí své internetové bankovnictví ke spořicímu účtu. Vstup je chráněn číslem klienta, jeho PIN a heslem. Transakce jsou povolovány pouze na jiné účty v rámci ING (např. majetkový, penzijní fond, pojištění apod.) a na předem písemně definované transakční účty u jiných bank. To činí aplikaci dostatečně bezpečnou i bez vyšších forem zabezpečení účtu.

Komerční banka

Mojebanka – internetové bankovnictví Komerční banky je primárně chráněno podpisovým certifikátem. Ten může být uložen na čipové kartě nebo v souboru. Ve druhém případě je k aktivním operacím vyžadováno potvrzení též zaslaným SMS kódem.

Zatímco certifikát je vydáván zdarma, využití čipové karty jako nosiče vyjde na 390 Kč. V sazebníku se nachází též jinak nezmiňovaná položka „vydání karty optického klíče“ s částkou 1 000 Kč – nejde však o nic jiného než o jinou formu PIN kalkulátoru, který lze využít místo podpisových certifikátů.

mBank

mBank přišla do České republiky z Polska koncem minulého roku. Sází na internetové bankovnictví a přímou obsluhu klientů bez poboček. K přihlášení stačí klientovi uživatelské jméno a heslo, pro ověření aktivních operací ještě zaslaný SMS kód. Vše je zdarma.

Oberbank

Oberbank přistoupila ke starému, ale osvědčenému způsobu. Klient se přihlašuje uživatelským jménem a heslem, kdežto transakce potvrzuje TAN kódy – jednorázovými transakčními autorizačními čísly, která obdrží z banky v sadách po 100 kusech. Jakmile se blíží vyčerpání TAN kódů, jsou klientovi zaslány nové. Tato metoda je citlivá na vyzrazení PIN (jako víceméně každá jiná) a ztrátu obálky s TAN kódy. Klient navíc nesmí zapomenout, že k objednávce nové zásilky zmiňovaných TAN kódů, za kterou si banka naúčtuje 20 Kč, potřebuje jeden TAN.

Poštovní spořitelna

Poštovní spořitelna je druhým brandem ČSOB – „obě banky“ fungují na jedné bankovní licenci. Přesto se jejich služby v oblasti zabezpečení internetového bankovnictví liší, stejně jako se liší nabídka jejich produktů.

U Poštovní spořitelny není na rozdíl od ČSOB možné využít pro přihlášení a autorizaci transakcí čipovou kartu. Klient má na výběr ze dvou možností: buď se přihlašuje jen uživatelským jménem a heslem, nebo si k nim přidá i SMS kód. SMS kód je ostatně nezbytný i k ověření platební transakce. Za tento způsob zabezpečení klient nad rámec platby za internetové bankovnictví a vedení účtu podle svého „tarifu“ nic nepřiplácí.

Raiffeisenbank

Raiffeisenbank začala v rámci koupě eBanky aktivně nabízet eKonto, které vychází z produktů eBanky. U tohoto účtu je zabezpečení stejné jako v případě eBanky. Klienti Raiffeisenbank ovšem mohou využívat i internetové bankovnictví Raiffeisenbank. Na této platformě se klienti ověřují buď podpisovým certifikátem, nebo jednorázovým heslem zaslaným na mobilní telefon. Oba způsoby zabezpečení jsou poskytovány zdarma (resp. v ceně vedení účtu a internetového bankovnictví).

UniCredit Bank

UniCredit Bank využívala dlouho jediný způsob zabezpečení přístupu klienta – a to jeden z nejlepších: PIN kalkulátor. Za něj si však účtuje 490 Kč. Od 1. dubna 2008 přidala též možnost využívání jednorázových kódů zasílaných SMS zprávou. V tomto případě si účtuje 90 Kč za 100 zaslaných SMS.

Volksbank

Po sjednání přístupu k účtu prostřednictvím internetu zašle Volksbank obálku s přístupovými kódy. Pomocí nich si klient vygeneruje podpisový certifikát, prostřednictvím něhož se následně přihlašuje k účtu.

WSPK

Waldviertler Sparkasse von 1842 je regionální banka, která se v Česku soustřeďuje především na jižní Čechy a jižní Moravu. K ověření totožnosti klienta využívá podpisový certifikát, který je poskytován zdarma, klient si však může připlatit 2 000 Kč za iKey token, který slouží obdobně jako čipová karta.

ZAMECNIK@INVESTUJEME.CZ

INFO_OVĚŘENÍ KLIENTA / AUTORIZACE PLATBY

	Uživatelské jméno a heslo	Sms klíč	Certifikát	Certifikát na čipové kartě	Pin kalkulátor	Tan
Citibank	–		–	–	450 Kč	–
Česká spořitelna	Pouze vstup na účet	•	–	990 Kč, následně 320 kč/rok	Jen stávající	–
Čsob	Pouze vstup na účet	•	–	600 Kč, následně 100 kč/rok	–	–
eBanka	–	50 Kč	100 Kč/rok	–	89 Kč/měsíc	20 Kč/měsíc
Fio	Pouze vstup na účet	–	•	–	–	–
Ge Money Bank	Pouze vstup na účet	•	•	–	–	–
Ing Bank	•	–	–	–	–	–
Komerční banka	–	•	•	390 Kč	1 000 Kč	–
mBank	Pouze vstup na účet	•	–	–	–	–
Oberbank	–	–	–	–	–	20 Kč/100 ks
Poštovní spořitelna	Pouze vstup na účet	•	–	–	–	–
Raiffeisenbank	–	•	•	–	–	–
Unicredit Bank	–	90 Kč/100 sms	–	–	490 Kč	–
Volksbank	–	–	–	–	–	•
Wspk	–	–	•	2 000 Kč*	–	–

* Ikey token – alternativa k čipové kartě