PŘIHLÁŠKA VYNÁLEZU

Zveřejněná podle §31 zákona č. 527/1990 Sb.

(21) Číslo dokumentu:

2014-126

(13) Druh dokumentu: **A3**

(51) Int. Cl.:

G06Q 20/32	(2012.01)
G06Q 20/40	(2012.01)
G06F 21/35	(2013.01)

(19) ČESKÁ REPUBLIKA

ÚŘAD PRŮMYSLOVÉHO VLASTNICTVÍ

(22) Přihlášeno: **03.03.2014**

(40) Datum zveřejnění přihlášky vynálezu: **16.09.2015**

(Věstník č. 37/2015)

(71) Přihlašovatel:
AVAST Software s.r.o., Praha 4, Michle, CZ

(72) Původce:
Ing. Tomáš Rosa, Ph.D., Praha 10- Petrovice, CZ
Mgr. Petr Dvořák, Pardubice- Srnojedy, CZ

(74) Zástupce:
KANIA*SEDLÁK*SMOLA Patentová a známková kancelář, Ing. Veronika Zemanová, Mendlovo náměstí 1a, 603 00 Brno

(54) Název přihlášky vynálezu:

Způsob a sestava pro zabezpečení ovládání bankovního účtu

(57) Anotace:
Způsob zabezpečení bankovního účtu z přenosného elektronického zařízení, které zahrnuje zařízení pro připojení k internetu a Bluetooth, pomocí pomocného zabezpečovacího zařízení zahrnujícího Bluetooth zahrnuje tyto kroky: i) přenosné elektronické zařízení se uzpůsobí pro internetové ovládání bankovního účtu, ii) pomocnému zabezpečovacímu zařízení se přiřadí jeho adresa a klíč zahrnující privátní a veřejnou část a tyto se uloží na pomocném zabezpečovacím zařízení a v systému bankovní instituce se uloží jeho adresa a veřejná část klíče, iii) pomocné zabezpečovací zařízení se přiřadí k uvedenému přenosnému elektronickému zařízení pro připravení jejich součinnosti při výpočtu klíče pro přihlášení do bankovního účtu, iv) přenosné elektronické zařízení vyhledává pomocí Bluetooth přiřazené pomocné zabezpečovací zařízení a v) při nalezení signálu Bluetooth z přiřazeného pomocného zabezpečovacího zařízení se klíč pro ovládání bankovního účtu vypočítává na základě kombinace klíče uloženého v přenosném elektronickém zařízení a klíče uloženého v přiřazeném pomocném zabezpečovacím zařízení.

CZ 2014 - 126 A3

03.03.14
2014 - 126

Způsob a sestava pro zabezpečení ovládání bankovního účtu

Oblast techniky

Vynález se týká způsobu zabezpečení proti neoprávněnému ovládání bankovního účtu z přenosného elektronického zařízení, které zahrnuje zařízení pro připojení k internetové síti a zařízení pro bezdrátovou elektronickou komunikaci protokolem Bluetooth, pomocí pomocného zabezpečovacího zařízení zahrnujícího zařízení pro bezdrátovou elektronickou komunikaci protokolem Bluetooth, přičemž tento způsob zahrnuje krok uzpůsobení přenosného elektronického zařízení pro internetové ovládání bankovního účtu. Vynález se rovněž týká přenosného elektronického zařízení a pomocného zabezpečovacího zařízení obsahujících software pro provádění tohoto způsobu a rovněž sestavy přenosného elektronického zařízení a pomocného zabezpečovacího zařízení, přičemž přenosné elektronické zařízení zahrnuje paměť, procesor, s ním propojené zařízení pro připojení k internetové síti a zařízení pro bezdrátovou elektronickou komunikaci protokolem Bluetooth.

Dosavadní stav techniky

Z dosavadního stavu techniky jsou známy různé způsoby zabezpečení proti neoprávněnému přístupu ke službám poskytovaným jednotlivým klientům po síti. Například v případě elektronického bankovnictví klienti bank běžně využívají pro ovládání jejich účtu z počítače jištění pomocí kódů zasílaných na jejich mobilní telefon. Takovéto jištění ovšem nemá smysl v případě internetového bankovnictví realizovaného přes mobilní telefon, tzv. mobile banking, smart banking apod. Dále existuje celá řada samostatných zařízení, která je možné použít pro zabezpečení služeb poskytovaných klientům, ta však pro své fungování vyžadují uživatelskou interakci (stisknutí tlačítka či zadání hesla / PINu a přepsání generovaného kódu, popř. přiložení bezdotykového zařízení, např. NFC karty, k chráněnému systému). Úkolem vynálezu tedy je navrhnout takové řešení, které by jednoduchým způsobem umožnilo ověřování oprávněnosti požadavku vyslaného přes internet z mobilního telefonu, zejména u bankovních a podobných, z bezpečnostního hlediska choulostivých operací, a to bez nutnosti součinnosti klienta, čili s výrazným zvýšením pohodlí.

Podstata vynálezu

Tento úkol je vyřešen způsobem zabezpečení proti neoprávněnému ovládání bankovního účtu z přenosného elektronického zařízení, které zahrnuje zařízení pro připojení k internetové síti a zařízení pro bezdrátovou elektronickou komunikaci protokolem Bluetooth, pomocí pomocného zabezpečovacího zařízení zahrnujícího zařízení pro bezdrátovou elektronickou komunikaci protokolem Bluetooth, přičemž tento způsob zahrnuje následující krok:

i) přenosné elektronické zařízení se uzpůsobí pro internetové ovládání bankovního účtu.

Podle vynálezu tento způsob dále zahrnuje následující kroky:

ii) pomocnému zabezpečovacímu zařízení se přiřadí jeho sériové číslo, adresa a klíč zahrnující privátní a veřejnou část a tyto se uloží na pomocném zabezpečovacím zařízení a v systému bankovní instituce se uloží sériové číslo, adresa a veřejná část klíče daného pomocného zabezpečovacího zařízení,

iii) pomocné zabezpečovací zařízení se přiřadí k uvedenému přenosnému elektronickému zařízení pro připravení jejich součinnosti při výpočtu klíče pro přihlášení do bankovního účtu a / nebo podepisování jednotlivých vybraných typů bankovních operací,

iv) přenosné elektronické zařízení vyhledává technologií Bluetooth ve svém okolí uvedené přiřazené pomocné zabezpečovací zařízení,

v) při nalezení signálu Bluetooth z uvedeného přiřazeného pomocného zabezpečovacího zařízení o předem stanovené nebo vyšší intenzitě se klíč pro přihlášení do bankovního účtu a / nebo podepisování jednotlivých vybraných typů bankovních operací vypočítává na základě kombinace klíče uloženého v přenosném elektronickém zařízení a klíče uloženého v přiřazeném pomocném zabezpečovacím zařízení.

S výhodou se při nenalezení signálu Bluetooth z uvedeného přiřazeného pomocného zabezpečovacího zařízení zablokuje a / nebo odpojí přihlášení do bankovního účtu z uvedeného přenosného elektronického zařízení.

Rovněž s výhodou se vyhledávání přiřazeného pomocného zabezpečovacího zařízení technologií Bluetooth zahájí při pokusu o přihlášení do bankovního účtu z uvedeného přenosného elektronického zařízení.

Také je výhodné, když se vyhledávání přiřazeného pomocného zabezpečovacího zařízení technologií Bluetooth opakuje v pravidelných časových intervalech o délce nejvýše 30 vteřin, a to alespoň po dobu přihlášení do bankovního účtu.

Klíč uložený v přiřazeném pomocném zabezpečovacím zařízení se s výhodou automaticky obměňuje po každém jeho použití.

Dle zvlášť výhodného provedení se v kroku ii) vytvoří symetrický klíč odvozením z veřejného klíče banky a privátního klíče pomocného zabezpečovacího zařízení a tento symetrický klíč se uloží v paměti pomocného zabezpečovacího zařízení a / nebo v kroku iii) se přiřazení pomocného zabezpečovací zařízení k uvedenému přenosnému elektronickému zařízení uskuteční tím, že přenosné zabezpečovací zařízení vygeneruje transportní klíč a vyšle ho technologií Bluetooth spolu s identifikačním údajem veřejného klíče banky do přenosného zabezpečovacího zařízení, které na základě již uložených dat a přijatých dat vypočte klíč pomocného zabezpečovacího zařízení pro krok v).

Dle vynálezu je stanovený úkol rovněž vyřešen pomocným zabezpečovacím zařízením, které zahrnuje paměť, procesor a zařízení pro bezdrátovou elektronickou komunikaci protokolem Bluetooth, přičemž paměť pomocného zabezpečovací zařízení obsahuje software umožňující provádění výše uvedeného způsobu.

Dle vynálezu je stanovený úkol rovněž vyřešen přenosným elektronickým zařízením, které zahrnuje paměť, procesor, s ním propojené zařízení pro připojení k internetové síti a zařízení pro bezdrátovou elektronickou komunikaci protokolem Bluetooth, přičemž paměť přenosného elektronické zařízení obsahuje software umožňující provádění výše uvedeného způsobu.

Zejména je stanovený úkol dle vynálezu vyřešen sestavou přenosného elektronického zařízení a pomocného zabezpečovacího zařízení, přičemž přenosné elektronické zařízení zahrnuje paměť, procesor, s ním propojené zařízení pro připojení k internetové síti a zařízení pro bezdrátovou elektronickou komunikaci protokolem Bluetooth, přičemž pomocné zabezpečovací zařízení zahrnuje paměť, procesor a zařízení pro bezdrátovou elektronickou komunikaci protokolem Bluetooth, přičemž paměť přenosného elektronického zařízení a paměť pomocného zabezpečovací zařízení obsahují software umožňující provádění výše uvedeného způsobu.

S výhodou v této sestavě zahrnuje uvedené přiřazené pomocné zabezpečovací zařízení zařízení pro vydávání zvukového signálu a uvedené přenosné elektronické zařízení zahrnuje spínač pro spouštění zvukového signálu z uvedeného přiřazeného pomocného zabezpečovacího zařízení a / nebo uvedené přenosné elektronické zařízení zahrnuje zařízení pro vydávání zvukového signálu a uvedené přiřazené pomocné zabezpečovací zařízení zahrnuje spínač pro spouštění zvukového signálu z uvedeného přenosného elektronického zařízení.

Popis příkladných provedení

Příkladným provedením vynálezu je sestava mobilního telefonu, nejlépe smartphonu, který představuje přenosný elektronický přístroj, a malého elektronického předmětu, například přívěšku na klíče, tzv. klíčenky, která představuje pomocné zabezpečovací zařízení. Mobilní telefon zahrnuje procesor, zařízení pro připojení k internetové síti, zařízení pro bezdrátovou elektronickou komunikaci protokolem Bluetooth a rovněž je vybaven softwarem, který umožňuje využívání internetového bankovnictví. Klíčenka zahrnuje procesor, zařízení pro bezdrátovou elektronickou komunikaci protokolem Bluetooth, například Bluetooth 4.0 Low Energy, a je vybavena softwarem pro realizaci komunikace s příslušným mobilním telefonem. Oba přístroje umožňují jednoznačnou vzájemnou identifikaci. Jednu klíčenku je možné použít pro jednu a více aplikací na více zařízeních, jedna aplikace na daném zařízení může být svázána s jednou nebo více klíčenkami.

Příkladné provedení pracuje například následovně. Mobilní telefon i klíčenka jsou opatřeny programovým vybavením, umožňujícím jednoznačnou vzájemnou identifikaci. Majitel mobilního telefonu se na svém mobilním telefonu po síti přihlásí do svého elektronického bankovnictví. Pro tento účel může například zadávat autorizační kód či heslo, jak je to známo z dosavadního stavu techniky. Mobilní telefon současně vyhledává ve svém okolí, například v okruhu 20m signál z jemu příslušející klíčenky. Velikost okruhu může být dána maximálním dosahem daného zařízení pro komunikaci protokolem Bluetooth nebo pevným nastavením na okruh menší než je maximální dosah omezením minimální požadované síly signálu. Pokud mobilní telefon zjistí přítomnost klíčenky v daném okruhu, umožní pokus o přihlášení do elektronického bankovnictví, přičemž klíčenka slouží jako jedna z komponent kryptografického algoritmu operace přihlášení (podílí se na podepisování požadavku o přihlášení). Přihlášení do elektronického bankovnictví pomocí mobilního telefonu je

tedy doplňkově jištěno pomocným bezpečnostním zařízením, ale majitel mobilního telefonu nemusí toto zařízení vyhledat, zapnout a opsat z něj kód, ani nemusí mít ve svém telefonu doplňkové zabezpečovací přístroje, například pro rozpoznávání duhovky nebo otisků prstů uživatele. Postačí, když má majitel mobilního telefonu klíčenku v kapse nebo v tašce, kterou má při sobě. Pokud mobilní telefon klíčenku nenalezne v daném okruhu, přístup do bankovnictví zablokuje.

Pokud se přihlášení do elektronického bankovnictví zdaří, mobilní telefon pak i dále sleduje dostupnost klíčenky a při ztrátě konektivity ke klíčence po dobu delší než např. 5 sekund, elektronické bankovnictví zablokuje, resp. odpojí přístup k elektronickému bankovnictví. K tomu může dojít například v případě, že se majitel mobilního telefonu přihlásil do elektronického bankovnictví ve veřejném prostoru a po přihlášení mu neoprávněný uživatel vytrhl přístroj z rukou a utíká s ním pryč. Klíčenka se rovněž podílí na zabezpečení další aktivity uživatele v elektronickém bankovnictví. Bez dostupnosti klíčenky tak není možné podepisovat a v důsledku ani provádět vybrané transakce (např. novou platbu), protože část podepisování dat požadavku probíhá přímo na klíčence. Podepisování je přitom jednoznačně ověřitelné na straně bankovních systémů – klíčenka je globálně rozpoznatelná, před-personalizovaná a unikátní od továrního nastavení.

Každá jednotlivá klíčenka je od výroby personalizována. Úvodní personalizace klíčenky bude technicky probíhat skrze personalizační stanici.

Do celkového schématu bezpečnosti vstupují mimo jiné jako parametry privátní a veřejná část klíč banky, a dále pak privátní a veřejná část klíč každé jednotlivé klíčenky (který je pro každou instanci zařízení unikátní). Do procesu personalizace jednotlivé klíčenky pak přitom nevstupuje privátní část klíče banky – v celém procesu výroby klíčenky se tak za stranu banky pracuje zásadně jen s její veřejnou částí klíče.

Pár veřejná / soukromá část klíče banky je možné předpočítat jednorázově ještě před továrním nastavením samotné klíčenky (popř. mohou být z kapacitních důvodů předpočítány pro danou geografickou polohu, např. pro střední Evropu, na které se předpokládá s přenositelností klíčenky). Práce s privátní částí klíče banky podléhá speciálnímu zacházení z důvodu citlivosti tohoto klíče – privátní část klíče je bance předána bezpečným způsobem.

Banka zároveň obdrží tabulku S veřejných částí klíčů všech klíčenek (resp. všech pro danou geografickou polohu, na které má být zajištěna přenositelnost mezi bankami).

Na každé jednotlivé klíčence se během personalizace uloží unikátní symetrický klíč vzniklý odvozením z veřejné části klíče banky a privátní části klíče dané klíčenky. Aby bylo možné zajistit to, že banka dokáže ověřit klíčenku vydanou jinou bankou (tj. aby byla zajištěna přenositelnost klíčenek mezi bankami), na klíčenku se negeneruje pouze jeden odvozený symetrický klíč pro jednu banku, ale tabulka T například 64 odvozených symetrických klíčů uložených na příslušné indexy tabulky T pro 64 bank, přičemž indexy a jim příslušející privátní části klíčů bank jsou dané konkrétní bance přiřazeny až následně (klíčenka může být vyrobena a personalizována před tím, než daná banka obdrží svou privátní část klíče). Následně je bance předán příslušný index do tabulky T, který banka použije pro adresaci svého symetrického klíče, –který – jak již bylo uvedeno – byl dopočtený z privátní části klíče klíčenky a veřejné části klíče banky a který odpovídá privátní části klíče dané banky a veřejné části klíče klíčenky.

Banka tak tedy má svou privátní část klíče banky, databázi S všech veřejných klíčů klíčenek a index do tabulky T uložené na klíčence, který používá k adresaci symetrického klíče, vzniklého na bázi privátní části klíče přívěšku a veřejné části klíče banky.

Koncovou personalizaci klíčenky (tedy spojení klíčenky s účtem klienta banky) provádí koncový uživatel na svém přenosném elektronickém zařízení pomocí softwarové aplikace, například na svém mobilním telefonu pomocí mobilní aplikace. Instrukce pro postup koncové personalizace jsou s výhodou zobrazeny v rámci uživatelského rozhraní na mobilním telefonu. Koncová personalizace spočívá v tom, že se na přívěšku v tabulce A propojených aplikací pro danou aplikaci vyhradí "slot" (pozice v tabulce A), který obsahuje další vygenerované symetrické klíče používané pro podepisování požadavků. Během alokace slotu aplikací musí uživatel operaci aktivně potvrdit, například stiskem tlačítka na pomocném zabezpečovacím zařízení. V případě, že jsou navíc obsazeny všechny dostupné sloty v tabulce A, je uživateli na mobilním telefonu zobrazen seznam pro výběr slotu k přepsaní. Tato operace přepsání pak může vyžadovat například dvojitý stisk tlačítka na pomocném zabezpečovacím zařízení.

Postup koncové personalizace klíčenky může být přitom následující:

1. Mobilní aplikace, která si chce alokovat slot v tabulce A, vygeneruje transportní klíč a zvolí index, který označuje veřejný klíč konkrétní banky v alokační tabulce T.
2. Klíčenka vygeneruje symetrický klíč pro budoucí podepisování certifikační výzvy a dopočte kryptogram uvedeného klíče a doplňkovou bezpečnostní konstantu (jejím úkolem je dodání entropie do algoritmů). Pro uložení těchto klíčů na klíčence slouží tabulka A.
3. Mobilní aplikace, která si chce alokovat slot, si uloží svůj slot a jeho signaturu, aby byla schopná rozpoznat stav, že jiná aplikace slot přepsala.
4. Pomocí klíčů uložených v tabulce T dojde pomocí síťového připojení k bezpečnému přenosu klíče pro budoucí podepisování certifikační výzvy uloženého v tabulce A na klíčence s koncovými systémy banky (serverovými systémy).

Od této doby je možné data z tabulky A používat pro podepsání transakcí na přívěšku, protože banka sdílí bezpečně předaný tajný klíč pro podepisování certifikační výzvy s klíčenou.

Po koncové personalizaci je klíčenka nachystaná pro běžné používání.

V případě, že aplikace na přenosném elektronickém zařízení, například na mobilním telefonu, vyžaduje pro nějakou operaci součinnost s klíčenkou, je postup následující:

1. Mobilní aplikace spočítá certifikační výzvu
2. Klíčenka spočítá certifikační odpověď pomocí klíče pro podepisování certifikační výzvy (tabulka A). Mohou přitom existovat dva typy klíče pro podepisování certifikační výzvy:
    a. Běžný typ, pro jehož vydání není potřeba manuálně potvrdit operaci na klíčence například stiskem tlačítka, což je vhodné zejména pro operace s nižší senzitivitou.
    b. Typ se zvýšenou bezpečností, pro jehož vydání je nutné manuálně potvrdit operaci na klíčence například stiskem tlačítka, což je vhodné zejména u některých velmi citlivých aktivních operací.
3. Klíčenka provede obnovení transportního klíče.

Pro veškerou komunikaci mezi klíčenkou a přenosným elektronickým zařízením je s výhodou používáno výchozí Bluetooth 4.x šifrování. Komunikace mezi mobilní aplikací a klíčenkou je (kromě standardního šifrování Bluetooth) chráněna ještě transportním klíčem nastaveným během alokace použitého slotu. Tento klíč je

sdílen mezi mobilní bankovní aplikací a klíčenkou (čili do banky se nepředává). Použité schéma má vlastnost dopředné bezpečnosti (Forward Secrecy), díky které případná pozdější kompromitace transportního klíče z ukradeného telefonu nevede k možnosti odšifrovat dříve zachycenou a uloženou rádiovou komunikaci s klíčenkou.

Použité algoritmy asymetrické kryptografie mohou být založeny například na Diffie-Hellman protokolu s využitím eliptických křivek (použitá křivka např. P256). Tento protokol využívá jako privátní klíč celé číslo d a jako veřejný klíč bod [x,y]. Pro potřeby zjištění veřejného klíče je nutné znát pouze souřadnici x (souřadnici y lze dovodit, "komprese bodů"). Veškerá asymetrická kryptografie přitom probíhá buď na straně banky (při ověřování), nebo na personalizační stanici (během úvodní personalizace pomocného zabezpečovacího zařízení). Na samotné klíčence probíhá pouze symetrická kryptografie (algoritmus AES).

V dalším příkladném provedení sestava podle vynálezu umožňuje vyhledávání / prozvánění přenosného elektronického zařízení pomocí pomocného zabezpečovacího zařízení, pokud jsou zařízení navzájem v dosahu. Zmáčknutím knoflíku na pomocném zabezpečovacím zařízení se spustí signalizace na přenosném elektronickém zařízení, která usnadní jeho vyhledání. A pokud to přenosné elektronické zařízení umožňuje, může být také použito pro nalezení pomocného zabezpečovacího zařízení. Typickým příkladem je hledání smartphonu nebo tabletu pomocí klíčenky a hledání klíčenky pomocí smartphonu nebo tabletu.

Ve výše uvedeném popise byla jako výhodný příklad pomocného zabezpečovacího zařízení uvedena klíčenka. Je ale zřejmé, že se může jednat o jakýkoli přenosný předmět, s výhodnou malých rozměrů, který zahrnuje příslušné elektronické součásti, tedy procesor, paměť, akumulátor a zařízení pro bezdrátovou elektronickou komunikaci technologií Bluetooth. Například se může jednat o hodinky, náramek apod.

Ačkoli bylo popsáno příkladné výhodné provedení vynálezu, odobrníkovi z dané oblasti budou zřejmé různé modifikace a možnost alternativního provedení některých částí řešení. Proto je rozsah ochrany bez ohledu na představená výhodná provedení dán zněním patentových nároků.

03.03.14

2014-126

PATENTOVÉ NÁROKY

1. Způsob zabezpečení proti neoprávněnému ovládání bankovního účtu z přenosného elektronického zařízení, které zahrnuje zařízení pro připojení k internetové síti a zařízení pro bezdrátovou elektronickou komunikaci protokolem Bluetooth, pomocí pomocného zabezpečovacího zařízení zahrnujícího zařízení pro bezdrátovou elektronickou komunikaci protokolem Bluetooth, přičemž tento způsob zahrnuje následující krok:

   i) přenosné elektronické zařízení se uzpůsobí pro internetové ovládání bankovního účtu,

   vyznačující se tím, že dále zahrnuje následující kroky:

   ii) pomocnému zabezpečovacímu zařízení se přiřadí jeho sériové číslo, adresa a klíč zahrnující privátní a veřejnou část a tyto se uloží na pomocném zabezpečovacím zařízení a v systému bankovní instituce se uloží sériové číslo, adresa a veřejná část klíče daného pomocného zabezpečovacího zařízení,

   iii) pomocné zabezpečovací zařízení se přiřadí k uvedenému přenosnému elektronickému zařízení pro připravení jejich součinnosti při výpočtu klíče pro ovládání bankovního účtu z přenosného elektronického zařízení,

   iv) přenosné elektronické zařízení vyhledává technologií Bluetooth ve svém okolí uvedené přiřazené pomocné zabezpečovací zařízení,

   v) při nalezení signálu Bluetooth z uvedeného přiřazeného pomocného zabezpečovacího zařízení o předem stanovené nebo vyšší intenzitě se klíč pro přihlášení do bankovního účtu a / nebo podepisování jednotlivých vybraných typů bankovních operací vypočítává na základě kombinace klíče uloženého v přenosném elektronickém zařízení a klíče uloženého v přiřazeném pomocném zabezpečovacím zařízení.

2. Způsob podle nároku 1, **vyznačující se tím, že** při nenalezení signálu Bluetooth z uvedeného přiřazeného pomocného zabezpečovacího zařízení se zablokuje a / nebo odpojí přihlášení do bankovního účtu z uvedeného přenosného elektronického zařízení.

3. Způsob podle nároku 1 nebo 2, **vyznačující se tím, že** vyhledávání přiřazeného pomocného zabezpečovacího zařízení technologií Bluetooth se zahájí při pokusu o přihlášení do bankovního účtu z uvedeného přenosného elektronického zařízení.

4. Způsob podle kteréhokoli z nároků 1 až 3, **vyznačující se tím, že** vyhledávání přiřazeného pomocného zabezpečovacího zařízení technologií Bluetooth se opakuje v pravidelných časových intervalech o délce nejvýše 30 vteřin, a to alespoň po dobu přihlášení do bankovního účtu.

5. Způsob podle kteréhokoli z nároků 1 až 4, **vyznačující se tím, že** klíč uložený v přiřazeném pomocném zabezpečovacím zařízení se automaticky obměňuje po každém jeho použití.

6. Způsob podle kteréhokoli z nároků 1 až 5, **vyznačující se tím, že** v kroku ii) se vytvoří symetrický klíč odvozením z veřejné části klíče banky a privátní části klíče pomocného zabezpečovacího zařízení a tento symetrický klíč se uloží v paměti pomocného zabezpečovacího zařízení a / nebo v kroku iii) se přiřazení pomocného zabezpečovací zařízení k uvedenému přenosnému elektronickému zařízení uskuteční tím, že přenosné zabezpečovací zařízení vygeneruje transportní klíč a vyšle ho technologií Bluetooth spolu s identifikačním údajem veřejné části klíče banky do přenosného zabezpečovacího zařízení, které na základě již uložených dat a přijatých dat vypočte klíč pomocného zabezpečovacího zařízení pro krok v).

7. Pomocné zabezpečovací zařízení, které zahrnuje paměť, procesor a zařízení pro bezdrátovou elektronickou komunikaci protokolem Bluetooth, **vyznačující se tím, že** paměť pomocného zabezpečovací zařízení obsahuje software umožňující provádění způsobu podle kteréhokoli z nároků 1 až 5.

8. Přenosné elektronické zařízení, které zahrnuje paměť, procesor, s ním propojené zařízení pro připojení k internetové síti a zařízení pro bezdrátovou elektronickou komunikaci protokolem Bluetooth, **vyznačující se tím, že** paměť přenosného

elektronické zařízení obsahuje software umožňující provádění způsobu podle kteréhokoli z nároků 1 až 5.

9. Sestava přenosného elektronického zařízení a pomocného zabezpečovacího zařízení, přičemž přenosné elektronické zařízení zahrnuje paměť, procesor, s ním propojené zařízení pro připojení k internetové síti a zařízení pro bezdrátovou elektronickou komunikaci protokolem Bluetooth, **vyznačující se tím, že** pomocné zabezpečovací zařízení zahrnuje paměť, procesor a zařízení pro bezdrátovou elektronickou komunikaci protokolem Bluetooth, přičemž paměť přenosného elektronického zařízení a paměť pomocného zabezpečovací zařízení obsahují software umožňující provádění způsobu podle kteréhokoli z nároků 1 až 5.

10. Sestava podle nároku 9, **vyznačující se tím, že** uvedené přiřazené pomocné zabezpečovací zařízení zahrnuje zařízení pro vydávání zvukového signálu a uvedené přenosné elektronické zařízení zahrnuje spínač pro spouštění zvukového signálu z uvedeného přiřazeného pomocného zabezpečovacího zařízení a / nebo uvedené přenosné elektronické zařízení zahrnuje zařízení pro vydávání zvukového signálu a uvedené přiřazené pomocné zabezpečovací zařízení zahrnuje spínač pro spouštění zvukového signálu z uvedeného přenosného elektronického zařízení.