HU 000224788 B1

(19) HU

MAGYAR KÖZTÁRSASÁG
Magyar Szabadalmi Hivatal

(11) Lajstromszám: 224 788 (13) B1

SZABADALMI LEÍRÁS

(21) A bejelentés ügyszáma: P 02 00463
(22) A bejelentés napja: 2002. 02. 07.

(51) Int. Cl.: *G06F 15/80* *(2006.01)*

(40) A közzététel napja: 2003. 11. 28.
(45) A megadás meghirdetésének dátuma a Szabadalmi Közlöny és Védjegyértesítőben: 2006. 02. 28.

(72) Feltalálók:
Inotay Balázs 50%, Budaörs (HU);
Fűkő László 6%, Taktaharkány (HU);
Hadik Barkóczy Bánk 8%, Érd (HU);
Kapitány András 6%, Budapest (HU);
Kárpáti Péter 6%, Budapest (HU);
Kokovai Ferenc 8%, Budapest (HU);
Lipcsei Gábor 6%, Szolnok (HU);
Parragh Gábor 10%, Budajenő (HU)

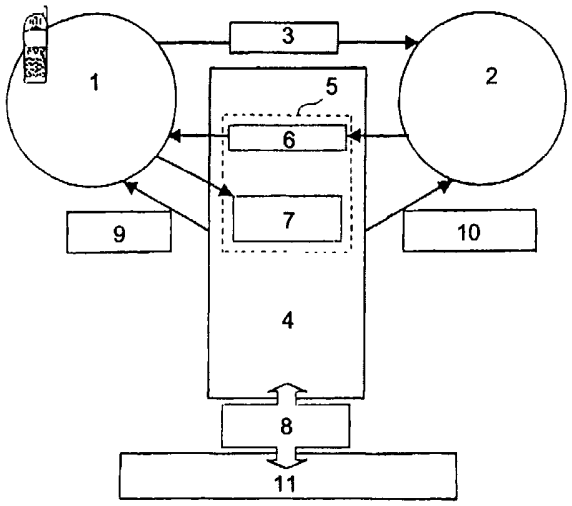
(73) Jogosult:
Enigma Software Rt., Budaörs (HU)

(74) Képviselő:
dr. Köteles Zoltán, S. B. G. & K. Budapesti Nemzetközi Szabadalmi Iroda, Budapest

(54) **Architektúra kiterjedt ügyfélkörben végrehajtható bankkártyás fizetési tranzakciók egyszerűsített hardverigényű lebonyolításához, tranzakciós terminálegység, bővített funkciós SIM kártya, valamint eljárások megszemélyesítésre és tranzakciók lebonyolítására**

(57) Kivonat

Az architektúrában bankkártya kibocsátására jogosult egy vagy több kibocsátó banknál bankszámlát vezető, szokványos bankkártya-azonosító információt hordozó mobil bankkártyával, valamint GSM-mobiltelefonnal és a GSM-szolgáltatás elérését biztosító érvényes SIM kártyával rendelkező ügyfelek (1), valamint egy vagy több elfogadó banknál bankszámlát vezető, tranzakciós terminál funkciójú egységgel és rendszerüzenetek fogadására alkalmas eszközzel rendelkező szolgáltatók (2) vannak. Az ügyfél (1) bővített funkciós SIM kártyával



1. ábra

HU 224 788 B1

van ellátva, amely a fizetési alkalmazást, valamint a szokványos bankkártya-azonosító információt is tartalmazza. Az architektúrában van egy mobil fizetési központ (4), amely GSM-szolgáltató által biztosított első típusú kommunikációs csatornán és kétirányú kriptográfiai illesztőfelületen keresztül csatlakozik az adott tranzakcióban részt vevő adott ügyfélhez (1) és szolgáltatóhoz (2), és második típusú kommunikációs csatornán és kétirányú kriptográfiai illesztőfelületen keresztül csatlakozik a tranzakcióban érintett elfogadó banki bankkártya-autorizációs központ(ok)hoz (11). A mobil fizetési központ (4) szolgáltatóhoz (2) rendelt tranzakciós terminálegységként minden egyes szolgáltatóhoz (2) legalább egy virtuális POS-terminált (5) tartalmaz, amely legalább a tranzakciós terminálegységként alkalmazott bankkártyaolvasó hagyományos hardver POS-terminálok (5) által kezelt adatok ellenőrzésére és/vagy a második típusú kommunikációs csatornán keresztüli autorizációsüzenet-válaszkezelésre alkalmas kialakítású. A tranzakciós terminálegység bankkártyaadatok ellenőrzésére és/vagy kommunikációs csatornán keresztüli autorizációsüzenet-kezelésre szolgál.

A bővített funkciós SIM kártya a GSM-szolgáltatás igénybevételéhez szükséges SIM-kártya-funkciók ellátásán kívül egy attól elkülönített második tárterületet tartalmaz további adatok tárolásához, és legalább logikai műveletek végzésére alkalmas műveleti egységet (CPU) tartalmaz. A második tárterület legalább a szokványosan szükséges összes bankkártya-információ tárolására alkalmas kialakítású, és a bővített funkciós SIM kártya továbbá a GSM-alapfunkciótól elkülönített kétirányú kriptográfiai illesztőfelületet tartalmaz. Megszemélyesítési eljárásában a második tárterületet előre megformázott fájlszerkezetű, a GSM-szolgáltató által korábban aktivált bővített funkciós SIM kártyát a GSM-szolgáltatótól független mobil fizetési központban kriptográfiai illesztőfelületen keresztül titkosított bankkártya-információval látják el a második tárterületen.

A fizetési tranzakciót az ügyfél (1) az aktivált és megszemélyesített bővített funkciós SIM kártyát tartalmazó előfizetői GSM-mobiltelefon-készülékről kezdeményezi, a kezdeményezéssel aszimmetrikus kriptográfiás módon kódolt SMS-alapú üzenetet juttat el egy mobil fizetési központba (4), ahol virtuális POS-terminálon (5) ismert tartalmú módon autorizációs üzenetet állítanak elő, és ezt a bankkártya-autorizációs központba (11) juttatják el, s az autorizáció eredményéről hasonlóan kódolt SMS-alapú üzenetet juttatnak vissza az ügyfél (1) előfizetői GSM-mobiltelefon-készülékre és a szolgáltatóhoz (2).

A találmány tárgya egy architektúra kiterjedt ügyfélkörben végrehajtható bankkártyás fizetési tranzakciók egyszerűsített hardverigényű lebonyolításához, amelyben bankkártya kibocsátására jogosult egy vagy több kibocsátó banknál bankszámlát vezető, szokványosbankkártya-azonosító információt hordozó mobil bankkártyával, valamint GSM-mobiltelefonnal és a GSM-szolgáltatás elérését biztosító érvényes SIM kártyával rendelkező ügyfelek, valamint egy vagy több elfogadó banknál bankszámlát vezető, tranzakciós terminál funkciójú egységgel és rendszerüzenetek fogadására alkalmas eszközzel rendelkező szolgáltatók vannak.

A találmány tárgya továbbá egy tranzakciós terminálegység bankkártyaadatok ellenőrzésére és/vagy kommunikációs csatornán keresztüli autorizációsüzenet-kezelésre, amely tranzakciós terminálegység olyan, kiterjedt ügyfélkörben végrehajtható pénzügyi tranzakciók egyszerűsített hardverigényű lebonyolítására szolgáló architektúrába van illesztve, amelyben bankkártya kibocsátására jogosult egy vagy több kibocsátó banknál bankszámlát vezető, szokványos bankkártya-azonosító információt hordozó mobil bankkártyával, vagy más – tágabb értelemben vett, és a következőkben részletezendő – mobil fizetőeszközzel, valamint GSM-rendszerű mobiltelefonnal és a GSM-szolgáltatás elérését biztosító érvényes SIM kártyával rendelkező ügyfelek, valamint egy vagy több elfogadó banknál bankszámlát vezető, tranzakciós terminál funkciójú egységgel és rendszerüzenetek fogadására alkalmas eszközzel rendelkező szolgáltatók vannak.

A találmány tárgya továbbá bővített funkciós SIM kártya előfizetői GSM-mobiltelefon-készülékhez, amely a GSM-szolgáltatás igénybevételéhez szükséges SIM-kártya-funkciók ellátásán kívül egy attól elkülönített második tárterületet tartalmaz további adatok tárolásához, és legalább logikai műveletek végzésére alkalmas műveleti egységet (CPU) tartalmaz.

A találmány tárgya továbbá egy megszemélyesítési eljárás előfizetői GSM-mobiltelefon-készülékhez való bővített funkciós SIM kártyához, amely a GSM-szolgáltatás igénybevételéhez szükséges SIM-kártya-funkciók ellátásán kívül egy attól elkülönített második tárterületet tartalmaz további adatok tárolásához, és legalább logikai műveletek végzésére alkalmas műveleti egységet (CPU) tartalmaz. A második tárterület előre megformázott fájlszerkezetű.

A találmány tárgya továbbá eljárás az említett architektúra segítségével tranzakciók lebonyolítására.

A technika állásából ismertek olyan kezdeményezett műszaki megoldások, amelyek mobiltelefon-rendszereken keresztül végbevihető fizetési tranzakciókat valósítanak meg. Azonban ezek vagy csekély biztonsági szintet képviselnek, a tranzakciók valóságos jogosult akaratából történt megindítása ellenőrzésére vonatkozóan, vagy a rendszeralkotók jelentős műszaki változtatását teszik szükségessé, mint például a mobilkészülékek, vagy a banki könyvelési/ellenőrzési rendszer gyökeres megváltoztatása.

A találmány célkitűzése egy olyan architektúra és rendszer kialakítása volt, amely kényelmes és biztonságos fizetést tesz lehetővé. Lényege az elektronikus

számlaprezentáción alapuló bankkártyás fizetés a meglévő mobiltelefon-hálózaton keresztül. Biztos megoldást nyújtson olyan helyzetekben, amelyekben a bankkártya használata ma kényelmetlen vagy kockázatos, vagy éppenséggel nem lehetséges, mint például közüzemi számlák és mobiltelefondíjak fizetése; vásárlás benzinkútnál, étteremben, egyéb üzletekben vagy az interneten keresztül.

A találmány szerinti architektúra lényege a következő pontokban foglalható össze:

- a találmány szerinti architektúra a bankkártyás fizetés ma létező kiszolgáló környezetéhez kapcsolódva biztosít tranzakciógyűjtő csatornát;
- a találmány szerinti PKI-alapú biztonságos fizetési megoldást ad, amelyben az ügyféloldali biztonsági elem a SIM kártya;
- a találmány szerinti architektúra része egy virtuális POS-eszköz, amely POS-szerű bankkártyás fizetést valósít meg GSM-, illetve webkörnyezetben;
- a találmány szerinti rendszerben a hagyományos SIM kártyát egy többalkalmazásos intelligens és egyben SIM-funkciót ellátó kártya váltja fel.

A találmány szerinti architektúra az elektronikus számlaprezentációt és az ezt követő fizetést támogatja – kivétel ez alól a GSM prepaid egyenlegfeltöltés, amelynél az ügyfél (a kártyabirtokos) maga indítja a tranzakciót a mobiltelefon-készülék menüjéből. E megoldások közös előnye, hogy a fizetési tranzakció indítása nem igényli a tranzakciós adatoknak a kártyabirtokos részéről történő előzetes begépelését, ami mind a hibák keletkezésének meggátolása, mind az ügyfél kényelmének szempontjából lényeges.

A szereplők közötti kommunikáció SMS-ek formájában zajlik. Az alkalmazott kriptográfiai megoldások folytán minden egyes üzenet 1 SMS-blokk-méretű. Egy-egy teljes fizetési tranzakció során igénybe vett SMS-blokkmennyiség a tranzakciótípus konkrét üzleti követelményeitől függ; a blokkok száma 2 (bankkártya-beültetés) és 5 (bolti/éttermi fizetés) között alakul.

A szolgáltatás lényege, hogy a jelenlegi hagyományos bankkártyás fizetési rendszert átülteti olyan környezetbe, ahol az átvitelt a GSM-hálózat, a biztonságot az aszimmetrikus kriptográfia, az ügyféloldali azonosítást a SIM kártya, a fizetőterminált egy mobil fizetési központban elhelyezkedő virtuális POS-terminál biztosítja.

A különféle üzleti környezetekben és élethelyzetekben különböző szolgáltatások értelmezhetők. Ezek közül néhány példa:

- Prepaid (előre fizetett, feltöltőkártyás) GSM-egyenlegfeltöltés. A GSM-ügyfél a saját prepaid egyenlegét a készülékéről, menüből vezérelt módon tudja feltölteni úgy, hogy a bankszámláját közvetlenül e tranzakció során terhelik meg az ellenértékkel.
- Postpaid (előfizetői, számlás) GSM-számlák fizetése. A GSM-ügyfél a saját havi számláit, a GSM-szolgáltatótól kiinduló számlaprezentációt követően a mobil bankkártyájával fizeti.
- Közüzemi számlák fizetése. Készpénzkímélő megoldás a meghatározott rendszerességgel jelentkező, kis és közepes értékű tételek fizetésére, elektronikus számlával szemben.
- Webáruház. Biztonságos webes vásárlás lehetővé tétele, ahol a logisztikai funkciók vezérlése a webes felületről, a fizetés pedig a rendszerben azonosított GSM-készülékről történik, a szintén a rendszerben azonosított célpontra, vagyis egy egy vagy több elfogadó banknál bankszámlát vezető, tranzakciós terminál funkciójú egységre.
- Katalógusból történő vásárlás. Ez az eset a webes vásárláshoz hasonló módon történhet. Készpénzkímélő és biztonságos módszer lehet katalógusban, óriásplakáton stb. azonosított tételek megrendelésére és az ellenérték kifizetésére.
- Mobil fizetés bolti/éttermi környezetben. Hasonlóan ez is készpénzkímélő, biztonságos módszer bolti vásárlásnál vagy éttermi fogyasztásnál keletkező fizetési kötelezettségek teljesítésére.

A találmány szerinti rendszerben a SIM kártya a következő működési elemekkel van ellátva:

- GSM-alkalmazás;
- GSM-szolgáltatás-azonosító adatok;
- a találmány szerinti alkalmazás;
- SIM kártya egyedi azonosító (SIM ID vagy másképpen CSN);
- kriptográfiai publikus kulcs és magánkulcs.

A mobil bankkártya-szolgáltatás szereplői a banki ügyfél (kártyabirtokos) és a kibocsátó bank. A regisztrációnál az ügyfél kinyilvánítja, hogy mobil bankkártyát szeretne igényelni. Ezt megteheti személyesen a bankfiókban, illetve – amennyiben a Bank támogatja a távszámlanyitást és bankkártyaigénylést – az ügyfél a SIM-kártya-cserével egyidejűleg a GSM-szolgáltató ügyfélkapcsolati pontján átveheti a számlanyitáshoz és a bankkártya-igényléshez szükséges dokumentumokat. Az ügyfél kitölti a mobil bankkártya regisztrációs lapot, ami egy biztonságos – önmagában ismert és alkalmazott – ügyviteli eljárás keretében eljut a Bankhoz, amely előállítja az ügyfél meglévő bankszámlájához csatlakozó, teljes egészében virtuális mobil társkártyát, a Bank a mobil társkártyához kapcsolódó bankkártya- és SIM-kártya-azonosító adatokat átadja a Bankban elhelyezett, a rendszer által üzemeltetett banki kártyaadatgyűjtő eszköznek. A banki kártyaadatgyűjtő eszköz előállítja a mobil társkártya kriptogramját és a megfelelő kriptográfiai lépéseket követően a SIM-azonosító adatokkal együtt a fizetési központ felé küldi tovább, előnyösen egy kétirányú kriptográfiai illesztőfelületen keresztül. A mobil fizetési központ a mobil társkártyakriptogramot felírja az ügyfél SIM kártyájára. A regisztráció befejeztével az ügyfél készüléke alkalmas a fizetésre.

A találmány szerinti rendszer több – ügyviteli folyamat és működés szempontjából – elkülönülő alrendszerből épül fel, amelyek az alábbiak:

- SIM-kártya-előkészítés.
- Fizetőeszköz-kibocsátás és menedzsment.
- Tranzakció- és üzenetfeldolgozás.
- Kriptográfia.

– Telefonoldali szoftver.
– Archiválás.
– CRM alrendszer.

A fizetőeszköz-kibocsátás előfeltétele, hogy a felhasználó a találmány szerinti alkalmazást tartalmazó SIM kártyával rendelkezzen. Ennek érdekében például az ügyfél bemegy a GSM-szolgáltató legközelebbi értékesítési pontjára és igényli a szolgáltatást. Az igénylő személy megkapja az előre megformázott fájlszerkezetű, a GSM-alkalmazással ellátott (még nem aktivált, de a rendszerben nyilvántartott) SIM kártyát. A tranzakciók többféle típusú fizetőeszközzel történhetnek (például: bankkártya, folyószámla stb.). Ahhoz, hogy egy adott fizetőeszközzel tranzakciót kezdeményezhessünk, előtte regisztrálni kell a fizetőeszközt a kibocsátó intézménynél, jelen esetben a kibocsátó banknál, melynek során a fizetőeszköz felkerül a mobiltelefon-SIM-kártyára.

Bankkártya- vagy számlaalapú fizetőeszköz igénylése esetén az ügyfél a kibocsátó bankot fogja felkeresni. Ha még nem rendelkezik számlával, akkor számlát nyit, ha már van számlája, akkor értelemszerűen nem, majd – bankkártya típusú fizetőeszköz esetén – megrendel egy mobil társkártyát. A fizetőeszköz igénylése során a megszokott adatokon kívül az ügyfélnek meg kell adnia a SIM kártyája azonosítóját (CSN) és a mobiltelefonjának hívószámát.

Bankkártyaalapú fizetőeszköz esetén a banki informatikai rendszer a megszokott eljárás keretében létrehozza az ügyfél mobiltárskártya-adatait, azzal a különbséggel, hogy a Bank számára választható opció, hogy készüljön-e tényleges bankkártya.

Következő lépésként a Bank kezdeményezi a fizetőeszköz adatainak átküldését a mobil fizetési központ felé, a találmány szerinti rendszer egy adott elemén keresztül, amely elem ebben az összefüggésben a rendszernek egy ugyanolyan perifériája, mint a kártyagyártó gép.

A továbbiakban egy rajz segítségül hívásával mutatjuk be, példán keresztül, a találmány szerinti rendszer funkcionális vázlatát.

Az 1. ábra az architektúra működési folyamatait és funkcionális kiépítését mutatja.

A rendszerbe az 1. ábra szerinti 2 szolgáltató (vásárlási hely) egy 5 virtuális POS-terminál birtokosaként lép be, amely 5 virtuális POS-terminál fizikailag egy 4 mobil fizetési központ kijelölt elektronikus része, tárolótartománya. Minden használatos 5 virtuális POS-terminálnak egyedi azonosítóval kell rendelkeznie, ami az 1 ügyféllel történő üzenetváltásokban a 2 szolgáltató és szolgáltatás neveként jelenik meg. Mivel az azonosító nemcsak numerikus értékeket tartalmazhat, kiválasztását a doménnév-regisztrációhoz hasonlóan célszerű elvégezni. A hagyományos POS-terminálokhoz hasonlóan, 5 virtuális POS-terminál-üzemeltetés esetén is szükséges egy bank által vezetett számla megléte, amely fogadja az átutalásokat. Ezért a számlamegnyitás alkalmával, ami hagyományosan a bankban történik, meg kell tenni az 5 virtuális POS-terminál-azonosító nevesítését is.

A mobil fizetőeszköz-kibocsátási és -regisztrálási folyamat első lépéseként a leendő virtuális POS-terminál-tulajdonos meghatározza az általa kívánt nevet. A névválasztás nem alapkövetelmény. A 2 szolgáltató, például a kereskedő kérheti, hogy a rendszer automatikusan generáljon számára egy virtuális POS-terminál-azonosítót. Minden esetben névfoglalási kísérletről szabad beszélnünk, mivel előfordulhat, hogy a használni kívánt név már foglalt. Ha a 2 szolgáltató igényét kiszolgáló banki ügyintéző közvetlen kapcsolatban van a 4 mobil fizetési központtal (például internet-hozzáférés), azonnal megtehető a név foglaltságának ellenőrzése, a mobil fizetési központ erre a célra fenntartott interfészén keresztül. Amennyiben ez nem lehetséges, a kereskedő később kap információt az általa választott virtuális POS-terminálnév állapotáról a bankon keresztül. Sikeres foglalás esetén a rendszer a kívánt nevet a bank és a kereskedő által közösen meghatározott ideig foglaltnak tekinti, és más forrásból ugyanezen névre érkező kérelmeket elutasítja. A foglalás megszűnik a megállapított idő leteltekor, illetve véglegessé válik abban az esetben, amikor a bank jóváhagyta az ügyfél virtuális POS-terminál-üzemeltetési kérelmét.

Az 1 szolgáltató működéshez az alábbi adatokra van szükség:

– Virtuális POS-terminál-azonosító.
– Terheléstől függően egy vagy több TID-azonosító (virtuális POS-terminál-azonosító).
– A 2 szolgáltató számlaszáma átutalás típusú tranzakciókhoz.
– Tranzakció-visszaigazolásokat (E-Slip) közvetítő kommunikációs csatornák adatai.
– Felhasználók által kiválasztható fizetőeszközökre vonatkozó korlátozások.

TID-azonosítókra a bankkártyaalapú – például az ismert BASE24 protokollon keresztül történő – tranzakcióautorizációhoz van szükség, amit egy banki 11 bankkártya-autorizációs központ állít ki [ez lehet például a jelenleg ma hazánkban a GIRO Bankkártya Rt. (GBC) néven ismert szervezet]. Az 5 virtuális POS-terminált igénylő 2 szolgáltatónak lehetősége van várhatóan nagy forgalom esetén több TID-et igényelni egyazon 5 virtuális POS-terminálhoz. Az egy virtuális POS-terminálra eső terhelés csökkenthető párhuzamos, külön TID-et használó átutaláskezdeményezéssel, maximum a 11 bankkártya-autorizációs központ által biztosított csatornák számáig.

Fizetőeszköz-korlátozásokon keresztül a 2 szolgáltató konkrétan megszabhatja, hogy mely kibocsátó intézményektől (bank) milyen fizetőeszköz-típusokat hajlandó elfogadni. Több ilyen fizetőeszköz-korlátozási kategória is megadható, ami számlakiküldés során akár ügyfelenként is más korlátozás (kategória) kiválasztását teszi lehetővé.

A 2 szolgáltató regisztrációkezdeményezése nagy szolgáltatók esetében papír alapon történhet. A telefontulajdonosokat mint potenciális 2 szolgáltatókat a találmány szerinti rendszerbe bevonó szolgáltatások esetén igény jelentkezik az automatizált virtuális POS-ter-

minál-regisztrációra, amit egy internetalapú interfész bevezetése oldhat meg.

A mobil bankkártya és virtuális POS-terminál-regisztrációk mobil fizetési központba továbbításához elengedhetetlen egy, a találmány szerinti rendszer részét képező munkaállomás, ami csatlakozik a banki igénylések (fizetőeszköz- és virtuális POS-terminál) feldolgozásáért felelős rendszerhez. A nevezett számítógép fizikai kapcsolatban van a banki számítógépes hálózattal, de a munkaállomásnak semmilyen hálózati hozzáférési jogosultsággal nem kell rendelkeznie. A munkaállomás részét képezi előnyösen egy csipkártyaolvasó berendezés, egy kulcskártya és egy a találmány szerinti központtal adatkapcsolatot biztosító kommunikációs egység.

A banki informatikai rendszer a feldolgozott találmány szerinti fizetőeszköz- és virtuális POS-terminál-igényléseket a munkaállomás megosztott könyvtárában teszi elérhetővé. Az adatcsere meghatározott formátumú szövegfájlokon keresztül történik (saját ellenőrző kódokat tartalmazó fájlszerkezet). A mobil kártya és virtuális POS-terminál-igénylések ugyanazon input könyvtárba kerülnek. A fájlok könyvtárban történő létrehozásának idejét és a benne szereplő rekordok számát a felgyülemlett igénylések száma és a legrégebbi igénylés dátuma szabja meg. A fájlokon keresztüli adattovábbítás ütemezése a Bank feladatköre.

A 4 mobil fizetési központban futó – az egyes regisztrációs típusokat (fizetőeszköz és virtuális POS-terminál) képviselő – komponensek időközönként ellenőrzik a banki input könyvtárat és összevetik a rendszerben nyilvántartott fájlkatalógussal, ha új bejegyzéseket találnak, kezdeményezik azon fájlok feldolgozását. A feldolgozás első lépésében a komponens kikódolja a fájlt a mobil fizetési központ privát kulcsával, majd a mobil fizetési központ banki publikus kulcsával, utána a regisztráció típusától függően továbbítja a megfelelő feldolgozókomponensnek.

A később sikertelen eredménnyel záruló regisztrációs műveletek visszaigazolásáért felelős komponens gondoskodik a Bank számára továbbítandó válaszfájlok generálásáról.

Ha a SIM kártyára nem érkezett még regisztráció, akkor aktiválja a rendszerben a megadott SIM kártyát és elmenti a 1. ábra szerinti 3 GSM-telefonszám-megadással kapott hívószámot. A már egyszer sikeresen regisztrált SIM kártya esetén összeveti a küldött telefonszámot a jelenleg a rendszerben nyilvántartottal, eltérés esetén hibaüzenetet küld a banki visszaigazolás-puffernek. Sikeres SIM-kártya-aktiválás után a banki fizetőeszköz-regisztrációt végző komponens regisztrációs üzenetet generál, amit a SIM kártyához tartozó telefonszámra címezve átad az üzenetkérést kiszolgáló komponensnek. A bankkártyaigénylést feldolgozó komponens minden egyes műveletről regisztrációs naplót vezet, a napló segítségével azonosíthatóak, hogy az egyes fizetőeszköz-regisztrációk melyik banki fájlba érkeztek. A regisztrációs naplónak elsősorban archiválásnál, illetve archívumból történő adat-visszakeresésnél van jelentősége. A felhasználó telefonjáról a fizetőeszköz-regisztrációs üzenetekre érkező válaszokat az Üzenetfeldolgozó megfelelő komponense értékeli ki.

A regisztrációs folyamat a virtuális POS-terminál-azonosító találmány szerinti rendszerbeli aktiválását és a banki POS-kezeléshez szükséges ellenőrzések, illetve esetenként TID-ekhez tartozó kulcsaktiválások egymásutánját takarja. Egy virtuális POS-terminál-aktiválás sikeressége, illetve sikertelensége kapcsán keletkező információk egy válaszfájlba kerülnek. Miután a forrásfájl minden virtuális POS-terminál-rekordja feldolgozásra került és ezzel párhuzamosan a rögzítések eredményei is előálltak, a válaszfájl bekerül a 4 mobil fizetési központ banki visszaigazolásokat tartalmazó könyvtárába.

A 4 mobil fizetési központon belül futó visszaigazolásokat továbbító komponens feladata a sikertelen fizetőeszköz-regisztrációkról visszaigazolásfájlok készítése, és a banki output könyvtárba másolása. Az időben elhúzódó eseti jelleggel bekövetkező hibás fizetőeszköz-igénylések ideiglenesen a banki visszaigazolás-pufferben foglalnak helyet. Adott időközönként lefutó folyamat gondoskodik a pufferbe bekerült sikertelen regisztrációs kísérletek visszaigazoló fájlba generálásáról. Ezután az említett fizetőeszköz-regisztrációs és virtuális POS-terminál-regisztrációs visszaigazoló fájlokat a komponens bekódolja a 4 mobil fizetési központ privát kulcsával, a Bank publikus kulcsával, és továbbítja a Bank felé.

Az elküldött fájlok a 4 mobil fizetési központ válaszfájlok számára megosztott könyvtárába kerülnek. A 4 mobil fizetési központban futó visszaigazolás-közvetítő komponens kikódolja az újonnan érkezett fájlokat és bemozgatja a banki információs rendszer számára megosztott könyvtárba.

A tranzakciófeldolgozási folyamat – logikailag és külső erőforrástól való függés szempontjából – több elkülönülő műveletsorra bontható. Az egyes műveletsorokat megvalósító modulok (komponensek) önállóan futtatható alkalmazások. Az egyes modulok aszinkrón várakozási sorokon keresztül kommunikálnak egymással, ezáltal más modulok rendelkezésre állásától függetlenül működhetnek. Az alkalmazásszervereken a komponensek (modulok) komponensfuttató környezetben működnek, amin keresztül indíthatóak új komponenspéldányok, illetve konnektorokon keresztül lehetőséget biztosítanak egy már futó modulpéldányra történő csatlakozásra. A keretrendszer fogja össze a tranzakciófeldolgozási folyamatban részt vevő modulokat, nyilvántartja az alkalmazásszervereket és a rajtuk futó modulpéldányokat.

A keretrendszeren keresztül nyílik lehetőség a modulpéldányokon futó folyamatok nyomon követésére, az egyes modulokra jellemző egyediállapot-táblázatokon keresztül. A modulpéldányokban végbemenő fontosabb eseményekről az üzenetnaplón keresztül szerezhetünk tudomást. A modulpéldányok egységes üzenetfeladó komponensen keresztül adják fel az üzeneteket a keretrendszernek. Minden esemény az egész rendszeren belüli egyedi üzenetkóddal és kategória-

megjelöléssel rendelkezik. Az egyes üzenetkódokra, kategóriákra szűrők állíthatóak be. A várakozási sorok állapottáblázat segítségével nyomon követhetőek az egyes modulok kapacitása, illetve a teljesítményváltozások.

A felvázolt műveletek lehetővé teszik a rendszerben zajló minden lényegesebb folyamat pontos figyelemmel kísérését. Az erre épülő automatizmusok, illetve riasztások lehetővé teszik a nem várt eseményekre történő gyors reagálást; előre látható esetben még az alkalmazás szintjén, nem várt esetben az adminisztrátorok részéről.

Az SMS-kommunikációs réteg az adatcsatornákon közlekedő üzenetcsomagok irányának megfelelően a csomagok fogadását vagy a küldését vezérli. A ki- és bemenő adatforgalomra külön adatcsatornák vannak fenntartva. A rendszer különböző komponenseket alkalmaz az adatforgalom irányának megfelelően.

A bejövőadatok egy feketelistás szűrőn esnek át, a véglegesen tiltólistára került forráscímekről érkező üzenetek azonnal eldobásra kerülnek. Az ideiglenesen feketelistára jelölt forrásból érkező csomagok külön hibanaplóba kerülnek a forrás megjelölésével; a napló tartalma később elemezhető. Az azonos forrásból érkezett hibás csomagok számát egy rutin figyeli, és a határérték-túllépés esetén véglegesen feketelistára helyezi a küldő forrást.

Az feketelistás ellenőrzésen átesett (még bekódolt) nyersüzenet-csomag a megfelelő adatokkal, többek között az egyedi üzenetazonosítóval bekerül a bemenőüzenet-pufferbe. A kommunikációs réteg mögött kialakított csomagpuffer elsődleges szerepe, hogy függetlenítse a kommunikációs alrendszert a rendszer egyéb komponenseinek rendelkezésre állásától; másrészt leegyszerűsíti a párhuzamos feldolgozást.

A felhasználóknak szánt üzenetek a titkosítás után a kommunikációt, illetve nyilvántartást segítő adatok társaságában a kimenőadat-pufferbe kerülnek. Az üzenettovábbításért felelős komponensek az általuk kezelt adatcsatornatípusra küldött csomagokat egymás után veszik ki a kimenő adatpufferből, majd a már előkészített üzenetet a 4 mobil fizetési központ továbbítja a címzettnek.

Egy SMS-kommunikációs modul feladata lehet, hogy kapcsolatot teremtsen a 4 mobil fizetési központ és a 2 szolgáltató SMS-központjával, továbbítsa, illetve fogadja a központból érkező, illetve a központnak szóló tranzakciókat. A 4 mobil fizetési központot lényegében 5 virtuális POS-terminálok sokasága képezi, amelyek ezáltal az 1 ügyféltől, a 2 szolgáltatótól, a GSM-szolgáltatótól és a kibocsátó/elfogadó bankoktól fizikailag, térben elkülönülten vannak telepítve.

A SIM-azonosító szerint meghatározott kulcsok alapján kikódolásra kerül a 4 mobil fizetési központba beérkezett üzenet. Az eredeti formájába visszaállított üzenetet a feldolgozó a tartalmazott típusnak megfelelően konvertálja és adja át a mezőket továbbfeldolgozó komponenseknek. Az üzenetfeldolgozó akár több példányban futva kérheti ki az input pufferből az üzeneteket. Minden egyes üzenet egy műveletet ír le. A mobil fizetési központba beérkező üzenetek fajtái és az üzenetet képviselő feldolgozókomponensek:

- fizetőeszközregisztráció-visszaigazolás;
- alkalmazásaktiválás, illetve -deaktiválás visszaigazolása;
- fizetési megbízás, elutasítás, reklamáció, elfogadás (számlaprezentáció esetén);
- számlaprezentáció-küldés kezdeményezése egy másik, a rendszerben levő telefonra.

Fizetésimegbízás-előkészítő komponens az üzenet mezőinek formai és lehetőség szerint tartalmi leellenőrzése után az adatokat beszúrja a tranzakciókat tartalmazó 7 tranzakciós pufferbe. Ez együtt kezeli a szerkezetileg némiképp eltérő tranzakciótípusokat. A tranzakció-előkészítés eredményétől függően válaszüzenet készül, ami a küldő forrásnak megcímezve a kimenő-üzenet-pufferbe kerül. A válaszüzenet lehet: hibajelzés (ha az üzenet tartalmi ellenőrzésen bukott meg) vagy egy időközi visszaigazolás (késleltetett tranzakciótípusoknál).

Számlaprezentációküldés-kezdeményezés esetén a céltelefon rendszerbeli státusának függvényében egy hibaüzenet érkezik a kezdeményezőhöz, vagy egy számlaprezentáció a fogadóhoz. Ez a számlaprezentáció formailag megegyezik az egyébként szerveroldalról kezdeményezett számlaprezentációkkal, és rendelkezik azok tulajdonságaival is.

Az egyes üzenettípusok funkciójukat és szerkezetüket tekintve eltérnek egymástól. Az üzenettípusok szerkezetét struktúraleíró táblázat határozza meg. Az üzenetek típusazonosítóval vannak ellátva, ami alapján a fogadóoldali feldolgozófolyamat be tudja azonosítani a struktúraleíró táblázatból az üzenet szerkezetét (mezők sorrendjét, hosszát és típusát).

Az alkalmazott titkosítási eljárás által létrehozott kriptogram mérete 1024 bites kulcsú RSA aszimmetrikus titkosítási algoritmus esetén 128 byte. Az SMS-alapú kommunikációs csatornán a maximális csomagméret 140 byte.

Tranzakció feldolgozásakor a 7 tranzakciós puffer tárolja a rendszerbe beérkezett és az Üzenetfeldolgozó által előkészített tranzakciókérelmeket. A 7 tranzakciós pufferből kéri ki a pufferkezelő a megfelelő státusú tranzakciókat. A pufferkezelő menedzseli a kialakuló várakozási sorokat, sorszámozza a tranzakciókérelmeket, figyeli a késleltetett tranzakciók lejártát, sikertelen kísérlet esetén újraütemezi a tranzakciót és regisztrálja a próbálkozások számát. Minden egyes tranzakciókérelem tartalmazza esedékességének dátumát, amit bizonyos tranzakciótípusoknál a szolgáltató adhat meg, egyébként a tranzakció regisztrálásának dátumával egyezik meg. Sikertelen tranzakciólebonyolítás esetén a feldolgozófolyamat kérheti a pufferkezelőtől a tranzakciómegbízás várakozási sorba való visszatételét sorszámeltolással, melynek során a megbízáspuffer sorszáma a még ki nem osztott legnagyobb sorszám és az eltolás összegét kapja értékül. A tranzakciókérelem újbóli visszahelyezésekor a pufferkezelő automatikusan megnöveli a bejegyzéshez tartozó feldolgozási kísérletek számát. A 7 tranzakciós pufferből történő kiké-

rése során a pufferkezelő az eddigi sikertelen kísérletek számát is közli a feldolgozófolyamattal, ami adott esetben véglegesen hibásnak minősítheti a tranzakciókérelmet.

A tranzakciókezdeményezést ütemező csatornakezelő mindig egy felszabadult csatornatípus számára kér tranzakciót. A pufferkezelőnek figyelembe kell vennie, hogy a szabad csatornatípus milyen fizetőeszköztípus átutalására alkalmas, és ezen fizetőeszköznek megfelelő tranzakciókérelmet választhat ki a 7 tranzakciós pufferből.

Bankkártyaalapú fizetőeszköz esetén még figyelembe kell venni, hogy az átutalandó tranzakcióban szereplő 5 virtuális POS-terminálhoz rendelt TID-ek közül van-e még szabad (párhuzamos átutalásokban pillanatnyilag nem szereplő). Sikeres tranzakcióválasztás esetén a pufferkezelőnek kell lefoglalnia a megbízást, illetve bankkártya esetén a szóban forgó TID-et.

Az átutalás végeztével a feldolgozófolyamat kéri a tranzakció kivételét a 7 tranzakciós pufferből, melynek során a lefoglalt TID felszabadul.

A teljes tranzakciófeldolgozási folyamat szűk keresztmetszetét a tranzakciómegbízás banki autorizációs központ(ok)on keresztüli végrehajtása jelenti. Az autorizációs központtal történő tranzakció lebonyolítása egyszerre több kommunikációs csatornán keresztül is folyhat. A kommunikációs csatornák az alkalmazott kommunikációs protokoll és az elfogadott fizetőeszköz (bankkártya, számlaszám stb.) szerint több típusba sorolhatóak. A szűk keresztmetszetet jelentő autorizációs központokon keresztüli kommunikáció figyelembevételével, az optimális tranzakciófeldolgozás érdekében, az adatcsatornák rendelkezésre állása szabja meg a tranzakciófeldolgozási folyamatok ütemezését. A folyamatok ütemezését a csatornakezelő végzi. Egy bizonyos típusú csatorna felszabadulásának eseménye eredményezi egy a csatorna típusának megfelelő újabb tranzakció kikérését a pufferkezelőtől. Ha nem kap feldolgozásra alkalmas tranzakciót a pufferkezelőtől, akkor a szabad csatornák listájában sorban következő csatorna számára kér tranzakciót. Ha a lista végére ér, elölről kezdi a csatornák kiválasztását, ezáltal biztosítva van, hogy minden csatornatípus közel egyforma gyakorisággal kaphasson tranzakciót.

Sikeres tranzakciókérés után a pufferkezelőtől kapott adatokkal átadja az adott csatornát képviselő tranzakciófeldolgozónak. A csatornakezelő az adatok átadása után azonnal visszakapja a vezérlést, így folytathatja a szabad csatornák vizsgálatát.

A tranzakciófeldolgozó komponens az általa megszemélyesített kommunikációs csatornán hajtja végre a tranzakciómegbízás lebonyolítását. A tranzakciófeldolgozó feladata az átutalás eredményének kiértékelése, melynek során köteles az átutalási folyamat eredményétől függően utasítani a pufferkezelőt a további lépések megtételére: ha a művelet sikeres volt, akkor a tranzakció megbízás kivétele a várakozási sorból; kommunikációs hiba esetén a megbízás későbbre ütemezése (sorszám állítása); kezelhetetlen hiba előfordulásakor a tranzakciókérelem rosszá minősítése. Sikeres tranzakciólebonyolítás eredményeként egy úgynevezett 8,9 E-Slip-et generál a feldolgozókomponens, amit a felhasználónak és a virtuális POS-terminál üzemeltetőjének címezve a kimenőüzenet-pufferbe tesz. A 8,9 E-Slip generálási munkafázis végeztével a tranzakciófeldolgozó jelzi a képviselt csatorna felszabadulását a Csatornakezelőnek. A rendszerben a kommunikációs csatornák számával megegyezően párhuzamosan (külön szálakon) fut a tranzakciókérelmek feldolgozása.

Az átutalást végző komponens paraméterként kapja a tranzakció adatait, a TID-et és a kommunikációs csatorna számát.

A találmány szerinti rendszerben minden elfogadóhoz (kereskedő) tartozik egy virtuális POS-terminál-azonosító. Ehhez a virtuális POS-terminál-azonosítóhoz legalább egy terminálazonosító (TID) tartozik, amely utóbbi a 11 bankkártya-autorizációs központ rendszerében kerül regisztrálásra. A terhelés függvényében egy 5 virtuális POS-terminálhoz, több TID rendelhető. A 2 szolgáltatókhoz befutó tranzakciók ezen a TID-en keresztül autorizálódnak. Egy adott virtuális POS-regisztráláskor a „normál"-POS-hoz hasonlóan a banki kapcsolaton (bérelt vonal, illetve kapcsolt vonali modem) keresztül letöltődnek a TID-tranzakció hitelesítőkulcsai.

A találmány szerinti rendszerből az 5 virtuális POS-terminál megkapja a kártyaadatokat, a vásárlás összegét, és a 2 szolgáltató TID-jét. Az 5 virtuális POS-terminál ellenőrzi a kártyaadatokat, illetve a lejárat idejét. Amennyiben ezek közül valamelyik kizárja a vásárlást, a tranzakciót elutasítja, egyébként a fenti adatokból egy tranzakciót képez, és azt a 11 autorizációs központ felé továbbítja. Ha az a küldött tranzakciót elfogadja, a találmány szerinti rendszer felé elfogadást jelez, egyébként elutasítja a kért tranzakciót.

Az elektronikus számlafizetési rendszerben, a ma postai forgalomban lévő szokásos (sárga) csekket, pénzátutalási megbízás nyomtatványt, a telefonra kiküldött fizetési felszólítás váltja fel. Ezen felszólításnak eleget téve az 1 ügyfél a számlájáról levonásra kerülő összeg, a felszólítást kiküldő 2 szolgáltató, például víz-, gáz-, áramszolgáltató számláján kerül jóváírásra.

A 2 szolgáltató kezdeményezi a fizetési felszólítást a találmány szerinti előfizetéssel rendelkező 1 ügyfél telefonszáma felé. A fizetési felszólításban röviden megjelöli a fizetési felszólítás alapját, a fizetés határidejét, valamint a fizetendő összeget, majd elküldi azt a 4 mobil fizetési központ számára. A 2 szolgáltató a 4 mobil fizetési központtal történt előzetes egyeztetés alapján megválaszthatja, hogy az elektronikus számlát milyen típusú fizetőeszközzel egyenlítheti ki az ügyfél.

A rendszerben alkalmazott kriptográfiai elem feladata, hogy biztosítsa a rendszerben áramló adatok megfelelő kriptográfiai védelmét.

Az előnyösen választott algoritmus az önmagában ismert RSA algoritmus, a kulcshosszúság 1,024 bit. Az RSA algoritmus egy publikus és egy privát kulcsot használ a titkosításra. A privát kulccsal kódolt üzenetet csak a publikus kulccsal, a publikus kulccsal kódolt

üzenetet csak a privát kulccsal lehet elolvasni. Ebben az esetben bárki, aki ismeri a publikus kulcsot, küldhet üzenetet a privát kulcs tulajdonosának. Az üzenet küldőjének hitelességét ebben az esetben nem lehet garantálni. A kettős kulcsolás bevezetésére azért van szükség, hogy a fent említett hitelességi kérdés megoldódjon. A küldő fél a saját privát kulcsával kódolja az üzenetet, majd az így kódolt üzenetet a fogadó fél publikus kulcsával kódolja. Ebben az esetben csak a fogadó fél tudja kibontani az üzenetet, először a saját privát kulcsával, majd a küldő publikus kulcsával. Ezzel a hitelességi probléma megoldódott.

Az eddigiekben ismertetett megoldások, megoldási részletek, programozási és konkretizált számítástechnikai módozatok csupán példaként szolgálnak. A találmány lényegét összefoglaló következő igénypontjaink körén belül más, alternatív és kiegészítő megoldások is elképzelhetők.

SZABADALMI IGÉNYPONTOK

1. Architektúra kiterjedt ügyfélkörben végrehajtható bankkártyás fizetési tranzakciók egyszerűsített hardverigényű lebonyolításához, amelyben bankkártya kibocsátására jogosult egy vagy több kibocsátó banknál bankszámlát vezető, szokványos bankkártya-azonosító információt hordozó mobil bankkártyával, valamint GSM-mobiltelefonnal és a GSM-szolgáltatás elérését biztosító érvényes SIM kártyával rendelkező ügyfelek, valamint egy vagy több elfogadó banknál bankszámlát vezető, tranzakciós terminál funkciójú egységgel és rendszerüzenetek fogadására alkalmas eszközzel rendelkező szolgáltatók vannak, *azzal jellemezve,* hogy az ügyfél bővített funkciós, de a szokványos telefonokban alkalmazottakkal azonos hardvert tartalmazó SIM kártyával van ellátva, amely a fizetési alkalmazást, valamint a szokványos bankkártya-azonosító információt is tartalmazza, az architektúrában van továbbá egy mobil fizetési központ, amely a banktól, a szolgáltatótól és az ügyféltől egyaránt független módon telepíthető, és amely egy GSM-szolgáltató által biztosított első típusú kommunikációs csatornán és kétirányú kriptográfiai illesztőfelületen keresztül csatlakozik az adott tranzakcióban részt vevő adott ügyfélhez és szolgáltatóhoz, és második típusú kommunikációs csatornán és kétirányú kriptográfiai illesztőfelületen keresztül csatlakozik a tranzakcióban érintett elfogadó banki bankkártya-autorizációs központ(ok)hoz, és a mobil fizetési központ szolgáltatóhoz rendelt tranzakciós terminálegységként minden egyes szolgáltatóhoz legalább egy virtuális POS-terminált tartalmaz, amely virtuális POS-terminál legalább a tranzakciós terminálegységként alkalmazott bankkártyaolvasó hagyományos hardver POS-terminálok által kezelt adatok ellenőrzésére és/vagy a második típusú kommunikációs csatornán keresztüli autorizációsüzenet-válaszkezelésre alkalmas kialakítású.

2. Az 1. igénypont szerinti architektúra, *azzal jellemezve,* hogy a kriptográfiai illesztőfelület nyilvános és privát kulccsal dolgozó, aszimmetrikus titkosítást alkalmazó felület.

3. Az 1. vagy 2. igénypont szerinti architektúra, *azzal jellemezve,* hogy az első típusú kommunikációs csatorna SMS-alapú üzenetváltásra van kialakítva.

4. A 3. igénypont szerinti architektúra, *azzal jellemezve,* hogy a kétirányú kriptográfiai illesztőfelület a SIM kártyába integrált kialakítású.

5. A 4. igénypont szerinti architektúra, *azzal jellemezve,* hogy a kétirányú kriptográfiai illesztőfelületet megelőző titkosítás előtti SMS üzenet felhasználói szinten hozzáférhetetlen.

6. Az 1–5. igénypontok bármelyike szerinti architektúra, *azzal jellemezve,* hogy a második típusú kommunikációs csatorna vezetékes távközlési csatorna.

7. Az 1–6. igénypontok bármelyike szerinti architektúra, *azzal jellemezve,* hogy a szolgáltató a GSM-szolgáltató, és a tranzakció prepaid számlaegyenleg-feltöltés.

8. Tranzakciós terminálegység bankkártyaadatok ellenőrzésére és/vagy kommunikációs csatornán keresztüli autorizációsüzenet-kezelésre, amely tranzakciós terminálegység olyan, kiterjedt ügyfélkörben végrehajtható pénzügyi tranzakciók egyszerűsített hardverigényű lebonyolítására szolgáló architektúrába van illesztve, amelyben bankkártya kibocsátására jogosult egy vagy több kibocsátó banknál bankszámlát vezető, szokványos bankkártya-azonosító információt hordozó mobil bankkártyával, valamint GSM-mobiltelefonnal és a GSM-szolgáltatás elérését biztosító érvényes SIM kártyával rendelkező ügyfelek, valamint egy vagy több elfogadó banknál bankszámlát vezető, tranzakciós terminál funkciójú egységgel és rendszerüzenetek fogadására alkalmas eszközzel rendelkező szolgáltatók vannak, *azzal jellemezve,* hogy a tranzakciós terminálegység egy, az adott tranzakcióban szereplő elfogadó banktól, kibocsátó banktól, ügyféltől és szolgáltatótól független mobil fizetési központban elhelyezkedő számítógépben létrehozott virtuális POS-terminál, amely GSM-szolgáltató által biztosított első típusú kommunikációs csatornán és kétirányú kriptográfiai illesztőfelületen keresztül csatlakozik egy adott tranzakcióban részt vevő adott ügyfélhez, és második típusú kommunikációs csatornán keresztül csatlakozik a tranzakcióban érintett kibocsátó és elfogadó bankokhoz.

9. A 8. igénypont szerinti tranzakciós terminálegység, *azzal jellemezve,* hogy a mobil fizetési központban elhelyezkedő számítógépben, egymástól elkülönített tárterületeken, tetszőleges számú virtuális POS-terminál van kialakítva.

10. A 9. igénypont szerinti tranzakciós terminálegység, *azzal jellemezve,* hogy a mobil fizetési központban elhelyezkedő számítógépben minden egyes szolgáltatóhoz (bankkártya-elfogadóhoz) legalább egy virtuális POS-terminál van hozzárendelve.

11. A 8–10. igénypontok bármelyike szerinti tranzakciós terminálegység, *azzal jellemezve,* hogy a virtuális POS-terminál az első típusú kommunikációs csatornán és a kétirányú kriptográfiai illesztőfelületen keresztül az adott tranzakcióban részt vevő adott ügyfél

GSM-mobiltelefon-készülékének bővített funkciós SIM kártyájához van csatlakoztatva, amely bővített funkciós SIM kártya szokványos bankkártya-információt is tartalmaz egy elkülönített tárterületen.

12. Bővített funkciós SIM kártya előfizetői GSM-mobiltelefon-készülékhez, amely a szokványos telefonokban alkalmazottakkal azonos hardvert tartalmaz, amelyen belül a GSM-szolgáltatás igénybevételéhez szükséges SIM-kártya-funkciók ellátásán kívül egy attól elkülönített második tárterületet tartalmaz további adatok tárolásához, és legalább logikai műveletek végzésére alkalmas műveleti egységet (CPU) tartalmaz, *azzal jellemezve,* hogy a második tárterület legalább a szokványosan szükséges összes bankkártya-információ tárolására alkalmas kialakítású, és a bővített funkciós SIM kártya továbbá a GSM-alapfunkciótól elkülönített kétirányú kriptogáfiai illesztőfelületet tartalmaz.

13. Megszemélyesítési eljárás előfizetői GSM-mobiltelefon-készülékhez való bővített funkciós SIM kártyához, amely a szokványos telefonokban alkalmazottakkal azonos hardvert tartalmaz, amelyen belül a GSM-szolgáltatás igénybevételéhez szükséges SIM-kártya-funkciók ellátásán kívül egy attól elkülönített második tárterületet tartalmaz további adatok tárolásához, és legalább logikai műveletek végzésére alkalmas műveleti egységet (CPU) tartalmaz, a második tárterület előre megformázott fájlszerkezetű, *azzal jellemezve,* hogy egy GSM-szolgáltató által korábban aktivált bővített funkciós SIM kártyát a GSM-szolgáltatótól független mobil fizetési központban kriptogáfiai illesztőfelületen keresztül titkosított bankkártya-információval látunk el a második tárterületen.

14. Eljárás az 1. igénypont szerinti architektúra segítségével tranzakciók lebonyolítására, amelyben egy ügyfél kezdeményez fizetési tranzakciót, *azzal jellemezve,* hogy az ügyfél a fizetési tranzakciót aktivált és megszemélyesített bővített funkciós SIM kártyát tartalmazó előfizetői GSM-mobiltelefon-készülékről kezdeményezi, a kezdeményezéssel aszimmetrikus kriptogáfiás módon kódolt SMS-alapú üzenetet juttatunk el egy mobil fizetési központba, ahol virtuális POS-terminálon ismert tartalmú módon autorizációs üzenetet állítunk elő, és ezt a bankkártya-autorizációs rendszerbe juttatjuk el, s az autorizáció eredményéről hasonlóan kódolt SMS-alapú üzenetet juttatunk vissza az ügyfél előfizetői GSM-mobiltelefon-készülékre és a szolgáltatóhoz.

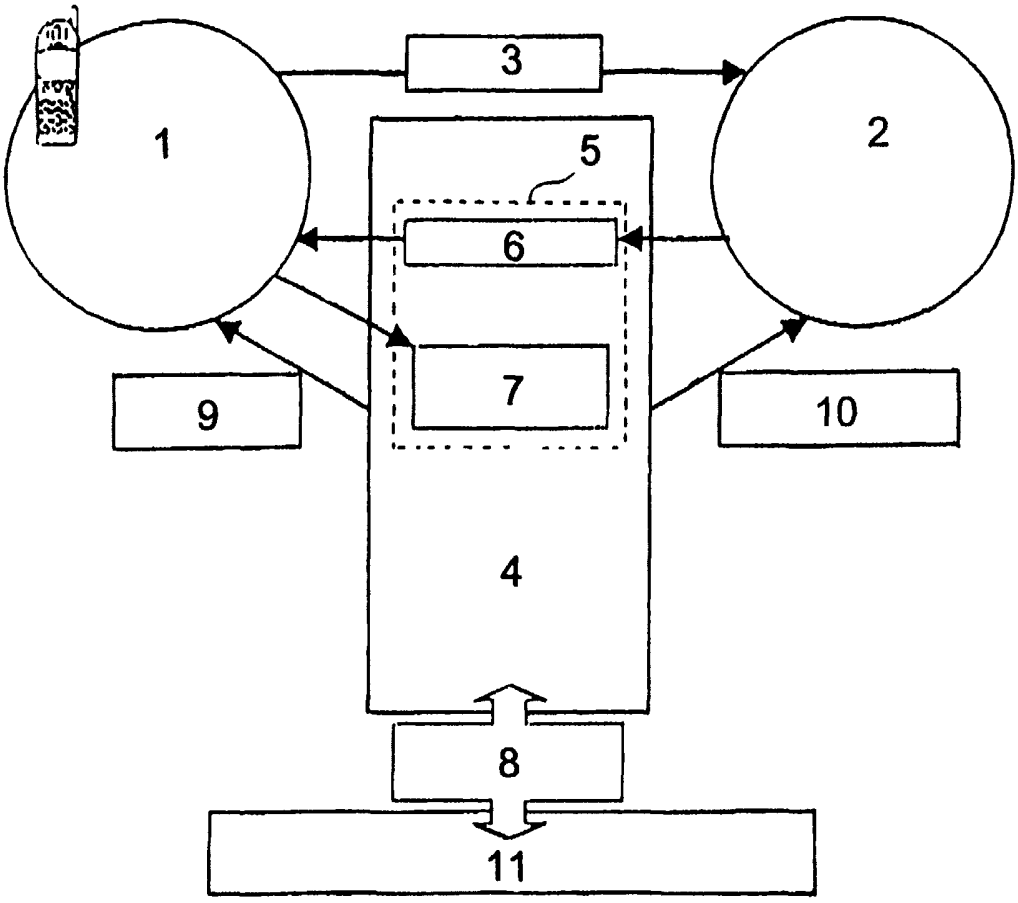
15. Eljárás az 1. igénypont szerinti architektúra segítségével tranzakciók lebonyolítására, amelyben egy szolgáltató a közötte és egy ügyfél között létrejött egyezség alapján egy szolgáltató kezdeményez fizetési tranzakciót, *azzal jellemezve,* hogy a tranzakciót kezdeményező, aszimmetrikus kriptogáfiás módon kódolt SMS-alapú üzenetet a mobil fizetési központon keresztül juttatjuk el az ügyfél előfizetői GSM-mobiltelefon-készülékre, majd a megjelenített üzenet és a tranzakció ügyfél általi jóváhagyása esetén egy másik, aszimmetrikus kriptogáfiás módon kódolt SMS-alapú üzenetet juttatunk el az ügyfél előfizetői GSM-mobiltelefon-készülékéről a mobil fizetési központba, és itt egy második típusú kommunikációs csatornán keresztül a tranzakcióban érintett kibocsátó bankokkal és elfogadó bankokkal a hardver POS-terminálóknál ismert módozatú és szokásos tartalmú üzenetváltással terhelési és jóváírási műveleteket kezdeményezünk, és a lebonyolított tranzakcióról a szolgáltatónak előfizetői GSM-mobiltelefon-készülékre aszimmetrikus kriptogáfiás módon kódolt SMS-alapú elektronikus nyugtát (E-slip) küldünk.

16. Eljárás az 1. igénypont szerinti architektúra segítségével tranzakciók lebonyolítására, amelyben egy ügyfél kezdeményez fizetési tranzakciót, *azzal jellemezve,* hogy az ügyfél a vásárlást kezdeményező üzenetet aktivált és megszemélyesített bővített funkciós SIM kártyát tartalmazó előfizetői GSM-mobiltelefon-készülékről kezdeményezi, a kezdeményezéssel aszimmetrikus kriptogáfiás módon kódolt SMS-alapú üzenetet juttatunk el egy mobil fizetési központba, majd ezt az üzenetet második típusú kommunikációs csatornán keresztül az üzenetben egyértelműen azonosított szolgáltató kapja meg, és a szolgáltató a vásárlást kezdeményező üzenetben egyértelműen azonosított ügyféllel harmadik típusú kommunikációs csatornán keresztül egyezséget hoz létre, amelynek alapján a szolgáltató kezdeményez fizetési tranzakciót, amennyiben a tranzakciót kezdeményező, aszimmetrikus kriptogáfiás módon kódolt SMS-alapú üzenetet a mobil fizetési központon keresztül juttatjuk el az ügyfél előfizetői GSM-mobiltelefon-készülékre, majd a megjelenített üzenet és a tranzakció ügyfél általi jóváhagyása esetén egy másik, aszimmetrikus kriptogáfiás módon kódolt SMS-alapú üzenetet juttatunk el az ügyfél előfizetői GSM-mobiltelefon-készülékéről a mobil fizetési központba, és itt egy második típusú kommunikációs csatornán keresztül a tranzakcióban érintett kibocsátó bankokkal és elfogadó bankokkal a hardver POS-terminálóknál ismert módozatú és szokásos tartalmú üzenetváltással terhelési és jóváírási műveleteket kezdeményezünk, és a lebonyolított tranzakcióról a szolgáltatónak előfizetői GSM-mobiltelefon-készülékre aszimmetrikus kriptogáfiás módon kódolt SMS-alapú elektronikus nyugtát (E-slip) küldünk.

17. A 14., a 15. vagy a 16. igénypont szerinti eljárás, *azzal jellemezve,* hogy az SMS-alapú üzenetváltást és a második típusú kommunikációs csatornán keresztüli üzenetváltást időben egymástól szétválasztjuk.

18. A 14., a 15. vagy a 16. igénypont szerinti eljárás, *azzal jellemezve,* hogy bankkártyaként tetszőleges elektronikus banki fizetőeszközt használunk.

19. A 8. igénypont szerinti tranzakciós terminálegység, *azzal jellemezve,* hogy virtuális POS-eszközként bármely banki fizetőeszköz elfogadására alkalmas elemet alkalmazunk.



1. ábra

Kiadja a Magyar Szabadalmi Hivatal, Budapest
A kiadásért felel: Törőcsik Zsuzsanna főosztályvezető-helyettes
Windor Bt., Budapest