PATENTOVÝ SPIS

(11) Číslo dokumentu:

287 424

(19) ČESKÁ REPUBLIKA

(13) Druh dokumentu: **B6**

(51) Int. Cl.[7]:
G 07 F 7/10

(21) Číslo přihlášky: **1998 - 1758**

(22) Přihlášeno: **14.11.1996**

(30) Právo přednosti:
08.12.1995 NL 1995/1001863

(40) Zveřejněno: **13.01.1999**
(Věstník č. 1/1999)

(47) Uděleno: **21.09.2000**

(24) Oznámeno udělení ve Věstníku: **15.11.2000**
(Věstník č. 11/2000)

(86) PCT číslo: **PCT/EP96/05027**

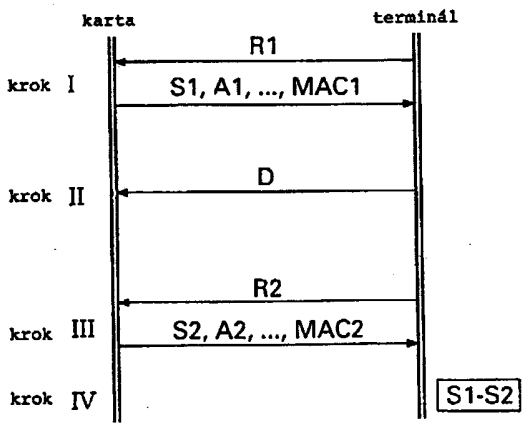
(87) PCT číslo zveřejnění: **WO 97/22091**

ÚŘAD PRŮMYSLOVÉHO VLASTNICTVÍ

(73) Majitel patentu:
KONINKLIJKE PTT NEDERLAND N. V., Hague, NL;

(72) Původce vynálezu:
Wissenburgh Jelle, Delfgauw, NL;
Brehler Johannes, Leidschendam, NL;
Muller Frank, Delft, NL;
De Lange Martin Klaas, Voorburg, NL;
Feiken Albertus, Amstelveen, NL;
Van de Pavert Hendricus Johannes Wilhelmus Maria, Veenendaal, NL;

(74) Zástupce:
Čermák Karel Dr., Národní 32, Praha 1, 11000;



(54) Název vynálezu:

Způsob chráněného provádění transakce s použitím elektronického platebního prostředku

(57) Anotace:

Způsob se týká chráněného provádění transakce s použitím elektronického platebního prostředku (11), zejména takzvané inteligentní "smart" karty, a platebního místa (12), zejména pokladny. Pro zabránění současného provádění transakce platebního prostředku (11) s několika platebními místy (12) se vytvoří opravňovací hodnota (A), která se použije pro výměnu dat mezi platebním prostředkem (11) a platebním místem (12) pro jednoznačné označení následných kroků (například I, III) transakce.

CZ 287424 B6

Způsob chráněného provádění transakce s použitím elektronického platebního prostředku

Oblast techniky

Vynález se týká způsobu chráněného provádění transakce s použitím elektronického platebního prostředku. Vynález se obecně týká způsobu zatížení elektronického platebního prostředku, zejména elektronické platební karty opatření integrovaným obvodem, takzvané „čipové karty", určitou částkou. Vynález se zejména, avšak nikoliv výlučně, týká způsobu chráněného zatížení předplacených elektronických platebních karet, to jest takzvaných „předplatních karet", které se používají například v telefonních budkách. Výraz „platební prostředek" bude v následujícím textu použit bez ohledu na formu nebo typ specifického platebního prostředku. Platebním prostředkem proto může být například nabíjitelná platební karta nebo elektronický platební prostředek.

Dosavadní stav techniky

V poslední době se elektronické platební prostředky používají stále častěji nejen pro placení ve veřejných telefonních automatech, nýbrž rovněž pro mnoho jiných druhů placení. Protože takový platební prostředek musí všeobecně obsahovat (kreditní) zůstatek, který představuje peněžní hodnotu, je zapotřebí, aby mezi tímto platebním prostředkem a platebním místem (jakým je telefonní automat navržený pro elektronické placení nebo elektronická pokladna) probíhala výměna dat podle chráněného způsobu (platebního protokolu). Zde je nutno zdůraznit, že částka (peněžní hodnota nebo počet početních jednotek) připsané na vrub platebního prostředku odpovídá částce (peněžní hodnotě nebo početních jednotek) úvěrované kdekoli: částka placená zákazníkem by měla odpovídat částce přijmuté dodavatelem. Úvěrovaná částka může být uložena, například v chráněném modulu, nacházejícím se v platebním místě.

Známé způsoby placení, které jsou uvedeny například v evropské přihlášce vynálezu EP 0 637 004, zahrnují první krok, v němž se platebním místem vyvolá zůstatek platebního prostředku, druhý krok, v němž se zůstatek platebního prostředku sníží (zatížení platebního prostředku určitou částkou), a třetí krok, v němž se zůstatek platebního prostředku opět vyvolá. Z rozdílu mezi zůstatky v prvním kroku a třetím kroku se určí částka, která má být zaplacena, a spolu s ní částka, která má být v platebním místě úvěrována. Druhý krok je možno opakovat několikrát, popřípadě v kombinaci s třetím krokem.

Pro zabránění podvodu v případě takového způsobu se při prvním kroku používá náhodné číslo, které je generováno platebním místem a přeneseno do platebního prostředku, například jako část kódu, kterým se vyvolá zůstatek. Na základě tohoto náhodného čísla generuje platební prostředek jako první odezvu opravňovací kód, který může mimo jiné obsahovat (například šifrovaně) zpracovanou formu náhodného čísla a zůstatku. Použitím odlišného náhodného čísla pro každou transakci se zabrání padělání opakováním. Navíc se v třetím kroku používá druhé náhodné číslo, které je rovněž generováno platebním místem a přeneseno do platebního prostředku. Na základě tohoto druhého náhodného čísla generuje platební prostředek jako druhou odezvu druhý, nový opravňovací kód, který může mimo jiné obsahovat zpracovanou formu druhého náhodného čísla a nový zůstatek. Na základě rozdílu dvou přenesených zůstatků stanoví platební místo (nebo chráněný modul platebního místa), jakou částkou má být zůstatek platebního místa úvěrován.

Tento známý způsob je v zásadě velmi odolný proti podvodům, pokud platební prostředek komunikuje s platební stanicí (nebo s chráněným modulem). Nevýhodou známého způsobu však je, že první opravňovací kód a druhý opravňovací kód jsou nezávislé. Jestliže s platebním prostředkem komunikuje druhé nebo třetí platební místo (nebo chráněný modul), je možné, v důsledku zmíněné nezávislosti, oddělit první krok od druhého a třetího kroku. Výsledkem toho je, že celá transakce může proběhnout, aniž by zmíněný platební prostředek byl zatížen stejnou

částkou, jako je částka, kterou jsou platební místa (nebo chráněné moduly) celkově úvěrována. Je zřejmé, že tato skutečnost není žádoucí.

V patentu US 5 495 098 a v odpovídající evropské přihlášce vynálezu EP 0 621 570 je uveden způsob, při němž se používá identita bezpečnostního modulu platebního místa pro zajištění toho, že výměna dat proběhne pouze mezi kartou a jedním terminálem. Ochrana výměny dat mezi bezpečnostním modulem, platebním místem a kartou je relativně komplikovaná a vyžaduje náročné šifrovací výpočty.

Další známé způsoby jsou uvedeny například v evropských přihláškách vynálezu EP 0 223 213 a EP 0 570 924, avšak tyto dokumenty neobsahují řešení výše zmíněných problémů.

Úkolem vynálezu je odstranit výše uvedené i jiné nedostatky dosavadního stavu a vytvořit způsob, kterým bude dosaženo vyššího stupně ochrany platebních transakcí. Úkolem vynálezu zejména je vytvořit způsob, který zajistí, že v průběhu transakce dojde pouze ke komunikaci mezi platebním prostředkem a jedním platebním místem nebo chráněným modulem. Úkolem vynálezu zejména je vytvořit způsob, který zajistí, že částka, o kterou se v průběhu transakce sníží zůstatek platebního prostředku, bude odpovídat částce, o kterou se zvýší zůstatek pouze jednoho platebního místa nebo chráněného modulu.

Podstata vynálezu

Uvedený úkol splňuje způsob chráněného provádění transakce s použitím elektronického platebního prostředku a platebního místa, který obsahuje

- počáteční krok, při němž
  - platební místo přenese první náhodné číslo do platebního prostředku,
  - platební prostředek, v odezvě na první náhodné číslo, přenese první opravňovací kód do platebního místa, přičemž tento první opravňovací kód se stanoví na bázi alespoň prvního náhodného čísla a první opravňovací hodnoty,
  - platební místo přezkoumá první opravňovací kód a

- další krok, při němž
  - platební místo přenese druhé náhodné číslo do platebního prostředku,
  - platební prostředek přenese druhý opravňovací kód do platebního místa, přičemž druhý opravňovací kód se stanoví na základě alespoň druhého náhodného čísla a druhé opravňovací hodnoty, přičemž druhá opravňovací hodnota se odvodí z první opravňovací hodnoty, a
  - platební místo odvodí druhou opravňovací hodnotu z první opravňovací hodnoty a přezkoumá druhý opravňovací kód.

Způsob provádění transakce s použitím platebního prostředku a platebního místa tedy obsahuje opakované provádění dotazovacího kroku, v němž se platební místo dotazuje platebního prostředku a v odezvě obdrží data platebního prostředku, přičemž data platebního prostředku zahrnují opravňovací kód vytvořený předem stanoveným způsobem, přičemž následný opravňovací kód je vztažen k předcházejícímu opravňovacímu kódu stejné transakce prostřednictvím opravňovací hodnoty vytvořené jednak v platebním prostředku a jednak v platebním místě. Vazba opravňovacích kódů prostřednictvím opravňovacích hodnot umožňuje rozlišení opravňovacích kódů počáteční transakce od opravňovacích kódů zprostředkovací transakce. S výhodou se opravňovací hodnota mění v každém dotazovacím kroku, čímž se dosáhne zvýšené bezpečnosti.

Vytvořením opravňovacích kódů mimo jiné na bázi vzájemně vztažených opravňovacích hodnot se vytvoří možnost zkontrolovat, zda druhý opravňovací kód (ve třetím kroku) je vztažen k prvnímu opravňovacímu kódu (v prvním kroku). Nyní, vytvořením nové opravňovací hodnoty

pokaždé, když musí být stanoven opravňovací kód, se vytvoří možnost rozlišení postupných opravňovacích kódů a spolu s tím rozlišení opravňovacích kódů spojených s různými transakcemi. Jestliže se pokaždé, když se provede první nebo třetí krok, vytvoří jediná opravňovací hodnota, může se jednoznačně stanovit, který druhý opravňovací kód je vztažen k prvnímu opravňovacímu kódu. Spolu s tím je rovněž možno stanovit, zda v transakci byl již vydán druhý opravňovací kód.

Opravňovací hodnoty jsou v zásadě generovány neboli vytvářeny samotným platebním prostředkem. S výhodou není možno tuto tvorbu jakýmkoli způsobem ovlivňovat zvenčí, aby se zabránilo podvodu. Opravňovací hodnoty mohou být vytvářeny různými způsoby, například generátorem náhodných čísel nebo čítačem.

První a druhá opravňovací hodnota transakce mohou být vztaženy k sobě navzájem například tak, že mají stejnou hodnotu nebo že mají navzájem závislé hodnoty, jako jsou postupné hodnoty čítače. První opravňovací hodnota může být rovněž náhodným číslem a druhá opravňovací hodnota může být vytvořena z první opravňovací hodnoty připočtením určitého čísla. V zásadě by každý pár opravňovacích hodnot měl mít takový vzájemný vztah, aby mohl být přezkoumán jednoznačně.

Přehled obrázků na výkresech

Vynález bude dále blíže objasněn na příkladném provedení podle přiložených výkresů, na nichž

obr. 1 schematicky znázorňuje platební systém, v němž může být aplikováno řešení podle vynálezu,

obr. 2 způsob, na nějž je řešení podle vynálezu aplikováno,

obr. 3 vytváření opravňovacího kódu použitého u způsobu podle obr. 2a

obr. 4 integrovaný obvod platebního prostředku, s nímž může být řešení podle vynálezu aplikováno.

Příklady provedení vynálezu

Systém 10 pro elektronické placení, znázorněný schematicky na obr. 1, obsahuje elektronický platební prostředek 11 ve formě takzvané čipové karty neboli takzvané inteligentní „smart" karty, dále platební místo 12, první platební instituci 13 a druhou platební instituci 14. Platební místo 12 (terminál) je znázorněno na obr. 1 jako pokladna, avšak může být rovněž provedeno například jako (veřejný) telefonní automat. Platební instituce 13 a 14, znázorněné na obr. 1, mohou být bankami, avšak rovněž i jinými institucemi, které mají své dostupné prostředky (počítače) pro zúčtovací platby. Ve skutečnosti mohou obě platební instituce 13 a 14 tvořit jednu platební instituci. Ve znázorněném příkladu provedení obsahuje platební prostředek 11 substrát a integrovaný obvod opatřený kontakty 15, přičemž tento integrovaný obvod je určen pro provádění transakcí (placení). Platební prostředek 11 může být rovněž tvořen elektronickou peněženkou.

Mezi platebním prostředkem 11 a platebním místem 12 dochází při transakci k výměně platebních dat PD1. Platební prostředek 11 je spojen s první platební institucí 13, zatímco platební místo 12 je spojeno s druhou platební institucí 14. Mezi oběma platebními institucemi 13 a 14 se po transakci provede zúčtování výměnou platebních dat PD2, která jsou odvozena z platebních dat PD1. V průběhu transakce zásadě nedochází ke komunikaci mezi platebním místem 12 a druhou platební institucí 14 (takzvaný systém off-line). Transakce musí být proto

prováděny pod kontrolou pro zajištění toho, že nemůže dojít ke zneužití systému 10. Takové zneužití může být provedeno například zvýšením zůstatku platebního prostředku 11, který není upraven změnou zůstatku spolupracujícího účtu v první platební instituci 13.

Graf na obr. 2 znázorňuje výměnu dat mezi platebním prostředkem 11 (jeho integrovaným obvodem), označeným na obr. 1 jako „karta", a platebním místem 12 (jeho chráněným modulem), označeným na obr. 1 jako „terminál", přičemž postupné kroky I–VI jsou znázorněny pod sebou.

V prvním kroku I vytvoří terminál, neboli platební místo 12, první náhodné číslo R1 a přenese je do karty, neboli platebního prostředku 11 (vedlejší krok Ia). Ve skutečnosti může být první náhodné číslo R1 částí kódu pro vyhledání opravňovacího kódu. Podle vynálezu vytvoří karta a terminál první opravňovací hodnotu A1, například zvětšením hodnoty v čítači, aktivováním generátoru náhodných čísel nebo těmito oběma úkoly. Na základě prvního náhodného čísla R1, první opravňovací hodnoty A1 a dalších údajů, včetně prvního zůstatku S1 platebního prostředku 11, vytvoří karta opravňovací kód MAC1 = F(R1, A1, S1, ...), F je šifrovací funkce známá jako taková (vedlejší krok Ib). První zůstatek S1 a první opravňovací hodnota A1, stejně jako první opravňovací kód MAC1, se přenesou do terminálu (vedlejší krok Ic). Terminál přezkoumá první opravňovací kód MAC1, mimo jiné na základě R1, S1 a A1, a v případě kladného výsledku zaznamená první zůstatek S1.

Je nutno poznamenat, že předání první opravňovací hodnoty A1 do terminálu není podstatné po předložený vynález, avšak slouží k zajištění přídavné ochrany proti podvodu.

Ve druhém kroku II vytvoří terminál debetní povel D, který obsahuje částku (množství), která má být odepsána z platebního prostředku 11. Debetní povel D se přenese do karty, načež první zůstatek S1 platebního prostředku 11, neboli karty, se sníží o hodnotu odepsaného množství neboli částky na druhý zůstatek S2. Druhý krok II se může opakovat několikrát.

Ve třetím kroku III vytvoří terminál druhé náhodné číslo R2 a přenese je do karty (vedlejší krok IIIa). Karta vytvoří druhou opravňovací hodnotu A2 a dalších údajů, obsahujících nový zůstatek S2 karty, vytvoří karta opravňovací kód MAC2 = F(R2, S2, ...), kde F je šifrovací funkce známá jako taková (vedlejší krok IIIb). Zůstatek S2 karty a druhá opravňovací hodnota A2, stejně jako druhý opravňovací kód MAC2, se přenesou do terminálu (vedlejší krok IIIc). Třetí kok III tak může probíhat zcela analogicky vůči prvnímu kroku I.

Terminál přezkoumá obdržený druhý opravňovací kód MAC2, například reprodukováním opravňovacího kódu a porovnáním druhého náhodného čísla R2. Terminál rovněž přezkoumá, zda se obdržená druhá opravňovací hodnota A2 rovná odpovídající hodnotě vytvořené v terminálu. Jestliže nejsou druhé opravňovací hodnoty A2 shodné, transakce se ukončí a zůstatek v terminálu proto zůstane nezměněný.

Jestliže kontrola druhého opravňovacího kódu MAC2 má kladný výsledek, zaznamená terminál druhý zůstatek S2. Místo reprodukce opravňovacích kódů MAC1 a MAC2 se může provést rovněž dešifrování neboli dekódování, například provedením inverze funkce F.

Ve čtvrtém kroku IV se stanoví rozdíl mezi zůstatky S1 a S2 a zaznamená v terminálu. V tomto případě může být tento rozdíl buď odděleně uložen, nebo přidán k existující hodnotě (zůstatku terminálu), což bude zúčtováno později. Zmíněný čtvrtý krok IV, který je možným následujícím krokem není podstatný pro řešení podle vynálezu. Před kroky I–IV, znázorněnými na obr. 2, může být proveden opravňovací nebo ověřovací krok, což však není podstatné pro řešení podle vynálezu.

V grafu, který byl podrobněji popsán výše, jsou náhodná čísla R1 a R2 odlišná. Náhodná čísla R1 a R2 však mohou být identická (R1 = R2 = R), takže ve třetím kroku III může být rovněž

provedena kontrola, zda použití v druhém opravňovacím kódu MAC2 je stále provedeno ze stejného náhodného čísla R (= R1).

Je nutno poznamenat, že první náhodné číslo R1, stejně jako druhé náhodné číslo R2, nemusí být náhodným číslem, neboť slouží pro jednoznačnou identifikaci prvního opravňovacího kódu MAC1 v odezvu na první náhodné číslo R1 („výzva"). Podstatné pouze je, že první náhodné číslo R1 nemusí být kartou rozeznatelné.

Podle známých způsobů jsou opravňovací kódy MAC1 a MAC2 v zásadě nezávislé. Je nutno říct že, jestliže se náhodná čísla R1 a R2 liší, neexistuje žádný přímý nebo nepřímý vztah mezi opravňovacími kódy MAC1 a MAC2. V důsledku této nezávislosti neexistuje v základě žádná záruka, že kroky I a III jsou prováděny mezi stejnou kartou a stejným terminálem.

Podle vynálezu však, když se stanoví druhý opravňovací kód MAC2, existuje předpokládaná opravňovací hodnota, která je přímo vztažena k opravňovací hodnotě použité při stanovování prvního opravňovacího kódu MAC1. Výsledkem toho je, že mezi dvěma opravňovacími kódy příslušné transakce se vytvoří vztah. Tento vztah je s výhodou přímým vztahem (například A2 = A1 + 1), umožňujícím jednoduchou kontrolu.

Jestliže například karta obdrží (první) náhodné číslo R1' z druhého terminálu poté, co karta vyslala první opravňovací kód MAC1 do prvního terminálu, vyšle karta druhý opravňovací kód MAC2. Jestliže potom první terminál poté, co vyslal debetní povel D, ještě jednou vyhledá opravňovací kód, vyšle karta další opravňovací kód MAC3, který je mimo jiné založen na další opravňovací hodnotě A3. Terminál zjistí, že opravňovací kódy MAC1 a MAC3 nemají vůči sobě žádný vztah a nebude schopen použití hodnoty zůstatku S3, který byl obsažen v dalším opravňovacím kódu MAC3. Podobně nevytvoří další opravňovací kód MAC4, který se vyhledá druhým terminálem, žádné platné oprávnění, a proto žádnou platnou hodnotu zůstatku. Tímto způsobem se účinně brání přenosu hodnot modifikovaného zůstatku do několika terminálů.

Opravňovací hodnoty jsou s výhodou tvořeny postupnými čísly, například polohami čítače. Je však rovněž možné použít čítač, který se zvyšuje objednou (podruhé po vytvoření opravňovací hodnoty), takže pokaždé budou dvě následné opravňovací hodnoty shodné. Je nutno poznamenat, že platební prostředek 11 může, avšak nemusí, rozlišovat mezi prvním krokem I a třetím krokem III.

Zmíněná závislost opravňovacích hodnot podle vynálezu zajišťuje, že všechny kroky transakce, v nichž je způsob podle vynálezu aplikován, nastávají mezi stejným platebním prostředkem 11 a stejným terminálem.

Na obr. 3 je schematicky znázorněno, jak může být vytvářen opravňovací kód MAC („Message Authentication Code"), například opravňovací kódy MAC1 a MAC2 z obr. 2. Do zpracovávacího prostředku 20, provádějícího funkci F, se přivádí několik parametrů. Funkce F může být šifrovací funkcí (jako je například velmi dobře známu funkce DES) nebo takzvanou „pseudo" funkcí, přičemž obě tyto funkce jsou velmi dobře známé. Alternativně může být funkce F relativně jednoduchou kombinační funkcí, přičemž v tom případě může být zpracovávací prostředek 20 obsahovat posouvací registr se selektivní zpětnou vazbou. Parametry přiváděné do zpracovávacího prostředku 20, a tudíž do funkce F, jsou v příkladu na obr. 3 tyto: náhodné číslo R, zůstatek S karty, opravňovací hodnota A, klíč K a inicializační vektor Q (počáteční hodnota). Náhodné číslo R odpovídá například prvnímu náhodnému číslu R1 a druhému náhodnému číslu R2 přenášenému do karty v kroku I a v kroku III. Zůstatek S karty odpovídá například zůstatkům S1 a S2 uloženým v kartě. Klíč K může být (tajným) klíčem, který je s výhodou jediný pro specifickou kartu nebo pro sérii karet. Klíčový identifikátor může být změněn terminálem v opravňovacím nebo ověřovacím kroku před krokem I na obr. 2.

Inicializační vektor Q, který spustí funkci F, může mít vždy pevnou hodnotu, například nulu. Alternativně závisí inicializační vektor Q na zbytku (konečném stavu) funkce F po předcházejícím kroku transakce. S výhodou se inicializační vektor Q nastaví na původní hodnotu, když začne nová transakce.

Opravňovací hodnota A je v příkladu, znázorněném na obr. 3, generována čítačem 21. Čítač 21 má s výhodou větší hodnotu po každém dotazovacím kroku (například kroku I a kroku III), to znamená po každém kroku, v němž se v odezvu na náhodné číslo R vytvoří opravňovací kód MAC. Tím vznikne odlišná opravňovací hodnota A použitá pro každý opravňovací kód. Protože přírůstek (v tomto případě +1, avšak přírůstek +2 nebo +10 jsou rovněž možné) se stanoví předem, může terminál ověřit opravňovací kód. S výhodou se opravňovací hodnota rovněž přenese do terminálu a je terminálem ověřena. Čítač 21 se nastaví na původní hodnotu vždy, když začne nová transakce.

V příkladu, znázorněném na obr. 3, je opravňovací hodnota A vytvářena čítačem 21. Alternativně je čítač 21 nahrazen generátorem náhodných čísel, který generuje novou opravňovací hodnotu A pro každý dotazovací krok (například kroky I a III) transakce. V tom případě by opravňovací hodnota předcházejícího kroku měla být použita jako inicializační vektor („zárodečný“) generátoru náhodných čísel, aby se předešlo vzájemné závislosti a reprodukovatelnosti opravňovacích hodnot.

Je zřejmé, že schéma na obr. 3 platí jak pro kartu, tak pro terminál. Terminál tedy rovněž produkuje opravňovací hodnoty A1, A2, ... a opravňovací kódy MAC1, MAC2, ... a porovnává je s odpovídajícími opravňovacími kódy a hodnotami obdrženými z karty. Terminálem bude akceptován zůstatek, například druhý zůstatek, S2 pouze tehdy, když vytvořené a obdržené opravňovací kódy a hodnoty se sobě rovnají.

Na základě obr. 4 nyní bude objasněno použití způsobu podle vynálezu u platebních karet.

Schéma na obr. 4 znázorňuje obvod 100, který obsahuje řídicí jednotku 101, paměť 102 a vstupní/výstupní jednotku 103, které jsou vzájemně spojeny. Řídicí jednotka 101 může být tvořena například mikroprocesorem nebo mikrořadičem. Paměť 102 může obsahovat paměť RAM neboli paměť s přímým výběrem a/nebo paměť ROM neboli permanentní paměť. Paměť 102 s výhodou obsahuje přepsatelnou paměť ROM (EEPROM).

Podle vynálezu obsahuje obvod 100 rovněž přídavnou paměť 105 pro ukládání opravňovacích hodnot. Jak je znázorněno na obr. 4, může přídavná paměť 105 tvořit oddělenou jednotku, avšak může být rovněž součástí paměti 102 a může být například tvořena několika paměťovými místy paměti 102. Přídavná paměť 105 je s výhodou tvořena obvodem čítače. Alternativně může být použit oddělený obvod čítače, jak je znázorněno na obr. 3.

Podle výhodného provedení se postupnými polohami čítače tvoří postupné opravňovací hodnoty. První opravňovací hodnota A1, která se použije pro vytvoření prvního opravňovacího kódu MAC1, odpovídá poloze čítače uložené v paměti 105. Po druhém kroku II (viz rovněž obr. 2) se poloha čítače zvýší o jednu. Počáteční poloha čítače může být v zásadě náhodná, avšak může být rovněž opětovně nastavená na předem stanovenou hodnotu, například na nulu.

Vytváření opravňovacích hodnot nastává autonomně, to znamená bez (možného) ovlivňování zvenčí. Výsledkem toho je, že odolnost proti podvodům se dále zvýší.

Je zřejmé, že místo každého zvýšení polohy čítače o jednu může být poloha čítače rovněž snížena o jednu. Podobně může být poloha čítače pokaždé zvýšena nebo snížena o více než jednu, například o dvě nebo čtyři. Je rovněž možné zkonstruovat obvod 100 tak, že ověřovací hodnota nebo hodnoty nejsou modifikovány při transakci, avšak pouze mezi transakcemi. V takovém případě je ovšem podobným způsobem uspořádáno i platební místo.

Platební místo pro aplikaci řešení podle vynálezu obsahuje prostředek (jako je čtecí přístroj karet) pro komunikaci s platebním prostředkem, prostředek pro provádění opravňování (jako je procesor) a prostředek pro zaznamenávání hodnot zůstatků (jako je polovodičová paměť). Platební místo je zkonstruováno tak, že neúspěšné oprávnění znemožňuje zaznamenání nové hodnoty zůstatku. Oprávnění podle vynálezu rovněž zahrnuje opravňovací hodnoty. Kroky způsobu podle vynálezu mohou být uloženy jak ve vybavení (specifickém obvodu, jakým je ASIC) a v software (vhodném programu pro procesor).

Odborníkům je zřejmé, že vynález není omezen na znázorněná a popsaná provedení, a že v rámci rozsahu vynálezu je možno provádět četné modifikace a doplňky. Princip vynálezu je výše popsán na zatěžování platebního prostředku určitou částkou, avšak uvedený princip může být rovněž použit u kreditních platebních prostředků.

PATENTOVÉ NÁROKY

1. Způsob chráněného provádění transakce s použitím elektronického platebního prostředku (11) a platebního místa (12), který obsahuje
- počáteční krok (I), při němž
  - platební místo (12) přenese první náhodné číslo (R1) do platebního prostředku (11),
  - platební prostředek (11), v odezvě na první náhodné číslo (R1), přenese první opravňovací kód (MAC1) do platebního místa (12), přičemž tento první opravňovací kód (MAC1) se stanoví na bázi alespoň prvního náhodného čísla (R1) a první opravňovací hodnoty (A1),
  - platební místo (12) přezkoumá první opravňovací kód (MAC1) a
- další krok (III), při němž
  - platební místo (12) přenese druhé náhodné číslo (R2) do platebního prostředku (11),
  - platební prostředek (11) přenese druhý opravňovací kód (MAC2) do platebního místa (12), přičemž druhý opravňovací kód (MAC2) se stanoví na základě alespoň druhého náhodného čísla (R2) a druhé opravňovací hodnoty (A2), přičemž druhá opravňovací hodnota (A2) se odvodí z první opravňovací hodnoty (A1), a
  - platební místo (12) odvodí druhou opravňovací hodnotu (A2) z první opravňovací hodnoty (A1) a přezkoumá druhý opravňovací kód (MAC2).

2. Způsob podle nároku 1, **vyznačující se tím**, že první a druhá opravňovací hodnota (A1, A2) jsou identické.

3. Způsob podle nároku 2, **vyznačující se tím**, že první a druhá opravňovací hodnota (A1, A2) obsahující postupné hodnoty čítače.

4. Způsob podle nároku 1, **vyznačující se tím**, že opravňovací hodnota, například druhá opravňovací hodnota (A2), se pokaždé vytvoří na základě náhodného čísla, například druhého náhodného čísla (R2), a předchozí první opravňovací hodnoty (A1).

5. Způsob podle jednoho z nároků 1 až 4, obsahující vložený krok (II), při němž
- platební místo (12) přenese povel (D) do platebního prostředku (11) a zůstatek platebního prostředku (11) se změní na základě povelu (D).

6. Způsob podle jednoho z nároků 1 až 5, **vyznačující se tím**, že první náhodné číslo (R1) se rovná druhému náhodnému číslu (R2).

7. Způsob podle jednoho z nároků 1 až 6, **vyznačující se tím**, že opravňovací kód, například druhý opravňovací kód (MAC2), se rovněž stanoví na základě klíče a identifikačního kódu.

8. Způsob podle jednoho z nároků 1 až 7, **vyznačující se tím**, že opravňovací kód, například první opravňovací kód (MAC1) se stanoví s pomocí šifrovací funkce (F).

9. Způsob podle jednoho z nároků 1 až 8, **vyznačující se tím**, že v prvním a třetím kroku (I, III) přenese platební prostředek (11) zůstatek, například první zůstatek (S1), do platebního místa (12).

10. Způsob podle jednoho z nároků 1 až 9, **vyznačující se tím**, že v prvním a třetím kroku (I, III) přenese platební prostředek (11) aktuální opravňovací hodnotu, například první opravňovací hodnotu (A1), do platebního místa (12).

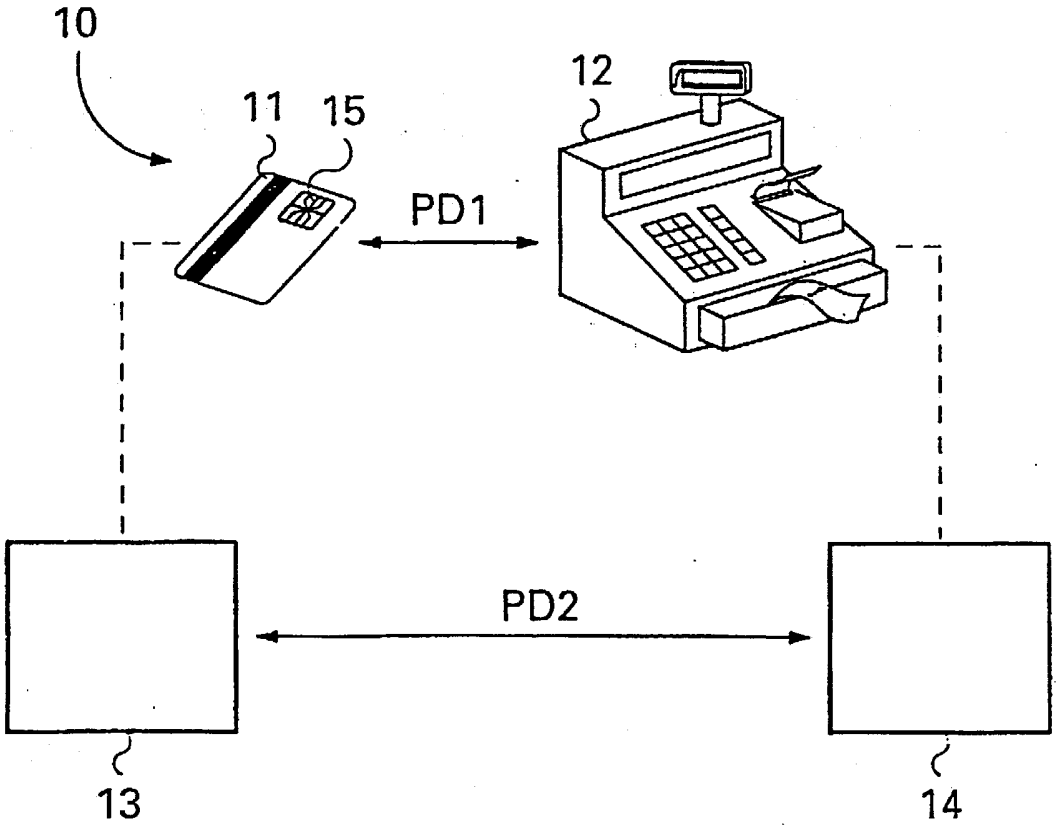
11. Způsob podle jednoho z nároků 1 až 10, **vyznačující se tím**, že třetí krok (III) se provádí opakovaně.

12. Způsob podle jednoho z nároků 1 až 11, **vyznačující se tím**, že dále obsahuje čtvrtý krok (IV), v němž se rozdíl (S1 - S2) mezi zůstatky v prvním a třetím kroku zaznamená v platebním místě (12).

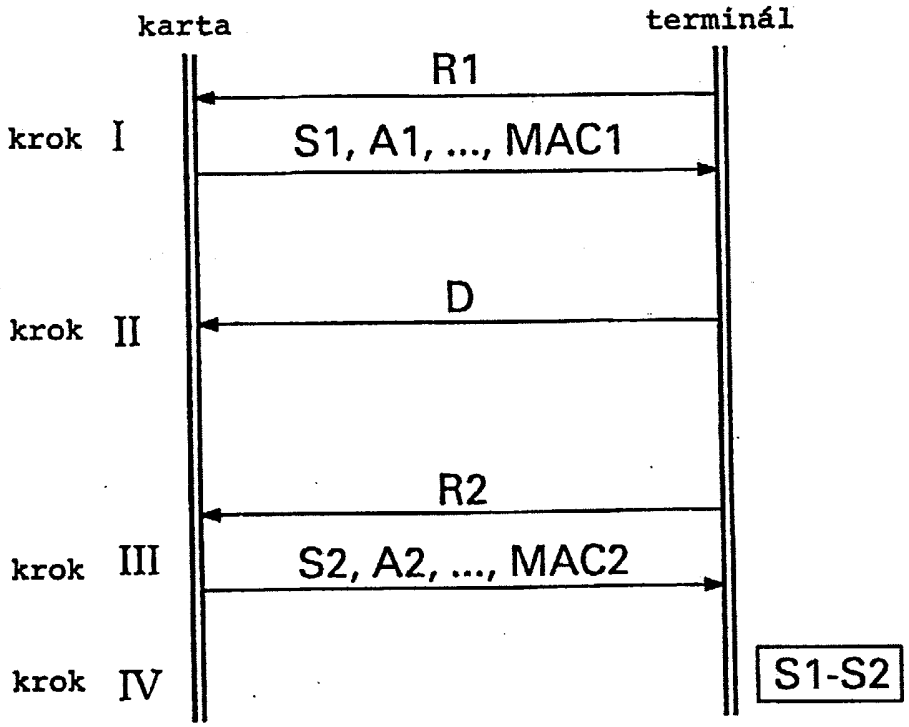
13. Způsob podle jednoho z nároků 1 až 12, **vyznačující se tím**, že platební místo obsahuje modul pro chráněné zaznamenávání dat.

14. Způsob podle jednoho z nároků 1 až 13, **vyznačující se tím**, že povel (D) je debetním povelem prováděným v druhém kroku (II) a snižujícím první zůstatek (S1) platebního prostředku (11).

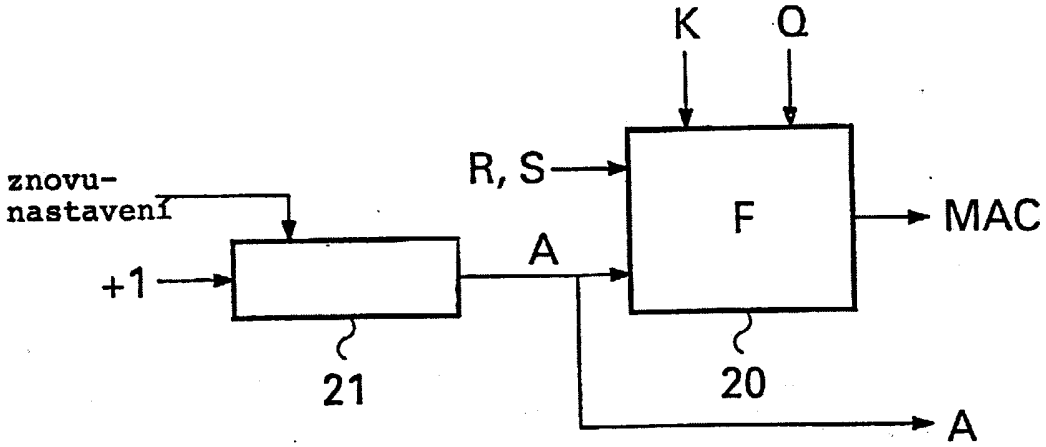
3 výkresy



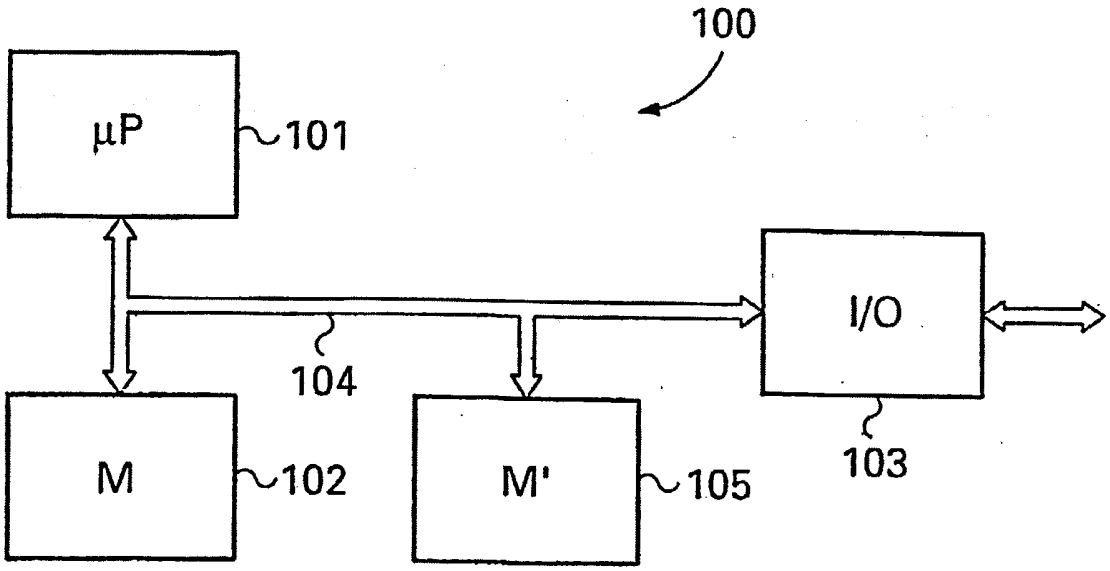
obr. 1


karta
terminál
R1
krok I
S1, A1, ..., MAC1
D
krok II
R2
krok III
S2, A2, ..., MAC2
krok IV
S1-S2

obr. 2


K
Q
R, S
znovu-
nastavení
F
MAC
A
+1
21
20
A

obr. 3



obr. 4

Konec dokumentu