PŘIHLÁŠKA VYNÁLEZU

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

(21) Číslo dokumentu:

1785-99

(19)

ČESKÁ REPUBLIKA

(22) Přihlášeno: **20. 11. 97**

(32) Datum podání prioritní přihlášky: **20.11.96**

(31) Číslo prioritní přihlášky: **96/031283**

(33) Země priority: **US**

(40) Datum zveřejnění přihlášky vynálezu: **17. 11. 99**
(Věstník č. 11/99)

(86) PCT číslo: **PCT/US97/21809**

(87) PCT číslo zveřejnění: **WO 98/22914**

(13) Druh dokumentu: **A3**

(51) Int. Cl.[6]:
G 06 K 19/067
G 06 K 19/073
G 07 F 7/08

ÚŘAD PRŮMYSLOVÉHO VLASTNICTVÍ

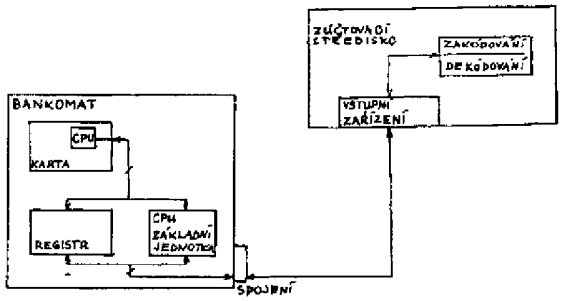
(71) Přihlášovatel:
TECSEC, INCORPORATED, Vienna, VA, US;

(72) Původce:
Wack Carl J., Clarksburg, MD, US;
Scheidt Edward M., McLean, VA, US;
Hershlow John H., Berkeley, NJ, US;

(74) Zástupce:
PATENTSERVIS PRAHA a.s., Jivenská 1, Praha 4, 14000;

(54) Název přihlášky vynálezu:
Kryptografický prostředek k provádění zabezpečených transakcí

(57) Anotace:
Kryptografický prostředek /karta/ obsahuje zapuštěné kovové částice. Tyto částice poskytují unikátní podpis, když je karta vystavena vysokofrekvenčnímu signálu. Prostředek má programovací a paměťovou schopnost, takže na něm jsou ukládány protokoly pro různé typy transakcí, spolu s osobními informacemi týkajícími se uživatele karty. Prostředek má např. podobu plastické karty, která obsahuje elektronický modul sestavený použitím vzoru vícečipového modulu a má programovací a paměťovou schopnost. Toto provedení umožňuje na kartě větší výpočetní a paměťovou kapacitu. Alespoň elektronický modul je zapouzdřen v plasconovém materiálu.



CZ 1785-99 A3

Kryptografický prostředek k provádění zabezpečených transakcí

Oblast techniky

Vynález se obecně týká nosiče informací, který se používá k vyřizování záležitostí (transakcí), a to obzvláště kryptografického (kódového) prostředku užívaného k provádění zabezpečených úkonů jako jsou bankovní a jiné komerční transakce.

Dosavadní stav techniky

V současné době je aktivita v oblasti inteligentních karet na prvém místě řízena potřebou chránit telefonní odvětví. Zejména celulární telefony jsou předmětem problémů, v nejhorším případě s podvodným účtováním a v nejlepším s odmítáním platit; každopádně jsou tyto ztráty v New York City samotném vyčíslovány v milionech dolarů denně. V Evropě podnikl celulární systém GSM akci a zavedl systém telefonních karet, který vyžaduje použití karty k předplacení telefonního hovoru či debetování předplaceného účtu. Tento přístup do jisté míry napravil problémy se systémem telefonního účtování. Avšak kriminální živly přesunuly svoji pozornost na

různé jiné způsoby, od klonování (padělání) telefonů k napadání (podvodným používáním) předplacených karet. Tyto karty navržené pro telefonní použití jsou většinou pouze odečítací (úbytkové) karty či předplacené karty, které jsou používány a potom odhozeny. Tento typ karet představuje přibližně 80% z celkového množství ve světě vyráběných „inteligentních" karet.

Karty s průmyslovým standardem, které byly vyvinuty s ohledem na použití telefonních karet, těžily ze snadné přístupnosti polovodičových paměťových čipů a výrobci karet, kteří viděli trh karet na jedno použití jako ideální, se rozhodli vyrábět „inteligentní kartu" jako ne drahý, po použití odhazovaný prostředek. Provedením tak mála změn v existujících výrobcích jak jen to bylo možné, způsob účtování telefonních hovorů vyžadoval pouze vsunutí malého polovodičového čipu, jenž byl pak vodičem (drátkem) připojen k minimálnímu množství kontaktních bodů, do karty (papírové anebo plastické). Tyto pouhé požadavky, které byly nezbytné pro jednu aplikaci, poháněly zbytek tohoto odvětví. Špatné fyzikální zabezpečení čipu zapuštěného do čtvercového zahloubení se stranou 25 mm, vyfrézovaného do plastické karty, rovněž znamenalo, že životnost této karty by mohla být měřena pouze v horizontu dní. Pro telefonní odvětví to však stále ještě zůstává jako výhodné.

Na všech úrovních informační infrastruktury je jako celek přezkoumávána bezpečnost (zabezpečení). Tato pozornost je rovněž věnována počítačům, které se používají k ovládání přístupu k informacím a do zvláštních oblastí. Všechna řešení software pokud jde o zabezpečení jsou příliš snadno diskreditována. Bylo vyžadováno, aby jednotlivý uživatel měl nějaké žetonové zařízení (resp. kartu).

V současné době je široké přijetí těchto konceptů evidentní, potřebou průměrného jedince nosit sebou půl tuctu,

či více karet. To co bylo dříve jednoduchou potřebou a požadavkem, se během času vyvinulo do přijímané praxe. Omezením širokého přijímání karet je pouhé množství těchto karet požadovaných jednotlivcem.

Rovněž je zahrnut vzájemný vztah každého jedince vůči vnějšímu prostředí pomocí počítače. Microsoft a ostatní firmy v podnikání počítačového software pokročily daleko v dodávání sebevědomí každé osobě spoléhat se ve stále větším měřítku na počítač doma a v jejím zaměstnání. Průmysl rovněž investuje veliké částky peněz, aby těžil z účinnosti a zdokonalení pracovního procesu poskytovaných počítačem.

Počítačový software k dispozici obsahuje stovky aplikací (použití), které se na první pohled jeví jako neškodné, ale mohou uživatele učinit zranitelným a dokonce ani celá odvětví nemají nyní jasný pohled se zřetelem na počítače. Například, kde a co je „virtuální bod přítomnosti"? Bankovnictví obzvláště, jež je odvětvím tradičně vydělávajícím své ziskové marže na službách a na potřebě zákazníků navštívit, či alespoň směňovat papírové dokumenty (peníze, akcie, záruky atd.) má závažný problém s poskytováním těchto tradičních bankovních služeb použitím software prostřednictvím spřažených společností jako jsou Microsoft a Intuit.

V posledních letech bylo považováno zabezpečení (bezpečnost) informací v rámci bankovní komunity jako pouze nezbytné během přenášení informací po zvláštních, pronajatých linkách „soukromé sítě". Banky umisťovaly(ťují) mezi jeden a druhý bod komunikace kryptografická (kódová) spojovací zařízení, například banka vůči bance. V původním schématu věcí to fungovalo, protože banky byly na prvém místě institucemi, které pracovaly s papíry a pouze přenos informací byl prováděn v podobě zpráv specifických typů informací, majících určitý formát a strukturu, ale stále

ještě mezi bankami a nakonec pak vůči Federálnímu reservnímu úřadu a Ministerstvu financí (podmínky USA).

Když se počítače dostaly velikostí a výkonností na úroveň stolního zařízení, banky ve snaze stát se efektivními začaly spojovat více a více zaměstnanců a skupin služeb dohromady. Spojení mezi kancelářemi bylo považováno většinou za „bezpečně", protože ve všech případech šlo o spojování uvnitř banky a ještě relativně izolované.

Když se banky rozvětvovaly aby dosáhly k zákazníkům, totéž se dělo se zařízením bankovních sítí při informování a rozšiřování schopnosti bankovních zaměstnanců a pro vedení vzájemné komunikace. Řešení zabezpečení bylo stále ještě definováno jako pouze nezbytné pro ty transakce, ke kterým dochází mezi zařízeními (resp. pobočkami atd.), a tomuto požadavku bylo možno vyhovět vybavením přenosové linky. Avšak, růst přenosových drah (spojení) mezi bankami dosáhl stupně složitosti a úplnosti, který nebyl zcela očekáván. Odborníci na hardware uspěli a každý se mohl elektronicky bavit s kýmkoli jiným o čemkoli. Avšak, všechny informace nejsou stejné a něco musí být provedeno, aby se ovládal tok informací úměrně k potřebě různých zaměstnanců banky znát určitý přístup. Údaje o zákazníkovi potřebovaly být chráněny před těmi zaměstnanci, kteří nepotřebovali vědět o zůstatcích na účtech. Pracovníkovi u přepážky nebylo možno dát k dispozici v okénku jeho počítačové jednotky informace týkající se fůzí a informace o pořizování majetku obchodníka.

Navíc, jak se vzájemná propojenost banky jako instituce zvyšovala, použitelnost informací se stávala více a více přístupnou pro více a více lidí. Zakódování linek mezi zařízeními, ačkoli stále ještě nutné k chránění informací zasílaných z jednoho místa do druhého, neposkytovalo oddělení (rozdělení či vyjmutí, pozn. překl.) požadovaných informací. Jiné příklady potřeby pro příslušné rozdělení informací

vznikly přijetím „Zákona o právu na soukromí", z roku 1974 (Privacy Act). Tento zákon učinil povinným udržovat důvěrné informace získávané buď zaměstnanci nebo bankami anebo lékaři a podobně, v tajnosti a chráněné před nepovoleným anebo nepřislušným přístupem.

Dále komplikujícím problémem rozdělování informací je rostoucí poptávka po poskytování bankovních služeb a produktů zákazníkům prostřednictvím systémů EDI nebo Internet. Současné užívání hardwarových spojovacích zařízení nedovoluje ochranu informací pohybujících se z adresy na adresu či osoby na osobu uvnitř sítě určité banky anebo organizace. Ani postup chránění přenosové linky nezajišťuje žádnou důvěrnost pro informace pohybující se uvnitř této linky.

Stejná situace je pravdivá pro informace pohybující se z bankomatu (ATM) do banky anebo zúčtovacího střediska (zpravidla též banky). Toto odvětví se jako celek pokusilo řešit tuto situaci a předložilo technické parametry: „Technické podmínky zabezpečené elektronické transakce", či SET. Tyto technické normy poskytují ochranu informací při přenosu z jednoho umístění systému EDI do druhého, to jest od obchodníka do banky anebo z bankomatu do zúčtovacího střediska. Těmito technickými podmínkami se však nesleduje ochrana informací samotných, pouze jejich příslušná dráha. Je na funkčním vlastníkovi daných informací aby těmto informacím poskytl zabezpečení. Pro tento problém se nabízí toto řešení.

Jsou to souběžné potřeby těchto okolností, které vyžadují celkové řešení. Nedostatků přítomných v tradičních kartách, jež je činí nevhodnými jako řešení, je mnoho. Například, každá karta má malou velikost čipu, definovanou zahloubením či otvorem v kartě s rozměrem 25 mm. Dále, praxe připevňování čipu v kapce epoxydové pryskyřici ho vystavuje vnějšímu prostředí, logickému a fyzikálnímu zneužití. Tento typ výrobku nabízí omezenou fyzikální a logickou bezpečnost.

Výsledkem je použitelná minimální funkčnost a kapacita paměti, jestliže je polovodičový průmysl vázán definicí čtverce se stranou 25 milimetrů, zavedenou odvětvím karet. Dodatečným omezením je závislost tohoto odvětví na existujících řešeních v oblasti kryptografické (kódovací) bezpečnosti a celkového nesprávného použití těchto generických řešení na tento velmi specifický úkol.

Ohledně logického problému, tradiční karty se obecně pokoušely(jí) používat pro řízení přístupu k informacím na kartě přístupu veřejného/soukromého klíče. Toto má svá omezení z několika důvodů. Za prvé, postup s přístupem veřejného/soukromého klíče vyžaduje oddělený koprocesor k provádění vlastních výpočtů a tento koprocesor může zabírat až 40% celkové velikosti čipu a rovněž omezeného prostoru v jímce karty. Dále, výpočty veřejného/soukromého klíče zabírají čas a každý případ poskytuje nežádoucí zpomalení ve výkonu (provádění nějakého úkonu, transakce). Problém ochrany soukromého klíče jednotlivce se často přehlíží, to jest, celkové schéma zabezpečení je závislé na soukromé polovině klíče zůstávajícího tajným.

Plastické karty se používají již mnoho roků. Plastická hmota není drahá, umožňuje tvarování, potiskování, vyrážení a přidání proužku magnetické pásky. Avšak, všechny tyto společné charakteristiky rovněž umožňují zneužití, když je nějaká plastická karta užívána pro finanční či úvěrovou aplikaci. Podvody s kreditními kartami jsou hlavním problémem kvůli snadnému duplikování plastické karty.

To co se požaduje, je způsob anebo postup poskytující dané plastické kartě/materiálu unikátní charakteristiky, jež nejsou rovněž drahé aby měly dopad na všeobecné používání tohoto produktu a ve stejném momentě bránily zneužití tohoto zařízení v jeho finančních použitích (aplikacích).

Podstata vynálezu

Přístup používání v kartě malého čtvercového otvoru se stranou 25 mm byl fyzikálně vymezen polovodičovým čipem. Celkové rozměry jednoduchého paměťového čipu se měří na šířku, délku a výšku. Délka a šířka jsou pevné a nezměnitelné. Avšak průměrný čip je silný mezi 20 a 25 tisícinami palce (0,5 a 0,64 mm). A z této tloušťky je přibližně 12 až 17 tisícin palce (0,3 až 0,4 mm) zabíráno aluminiovou podkladovou vrstvou, vynucenou si fotoleptacím postupem výroby polovodiče. Sestavením dohromady vzoru vícečipového modulu (MCM), který poskytuje vysoký stupeň hustoty a kapacity, a potom zapouzdřením tohoto MCM do plasconového materiálu, který je podobný materiálu současně používanému ve výrobním postupu standardního polovodiče, může být k zajištění stability proveden postup zužování, který udělí celému modulu tloušťku mezi 6 a 10 tisícinami palce (0,15 mm a 0,25 mm). Tento velmi tenký produkt rovněž získává velmi vysoký stupeň flexibility (ohebnosti), podobný hliníkové folii a hliníkovému polepu. Toto zúžení odstraňuje potřebu pro omezení 25 mm, která existuje ve všech jiných produktech odvětví. Ve skutečnosti může být užito k umístění elektronických komponent 80% plochy plastické karty.

Kvůli plasconu je flexibilní MCM zcela uzavřen od znečišťujících látek vnějšího prostředí. Výsledný modul může být laminován uvnitř dvou vnějších vrstev a může být skutečně opět použit, jestliže by mělo být vnější pouzdro poškozeno nehodou anebo zneužitím.

Toto poskytuje zlepšení v zabezpečení, které je v existujících kartách ve fyzikálním smyslu minimální. Nechráněný čip paměťových nebo procesorových funkcí je běžně vodičem připojen ke kovovému kontaktnímu materiálu se

standardem ISO (viz. ISO Std. 7816-2 /Fyzikální technické normy a -3 / Elektrické technické normy). Jako takový je tento čip otevřen k pronikání (zkoumání), připojením či jakémukoli jinému druhu fyzikální analýzy. Dále, když ohnete současnou standardní kartu, zapuštěný čip vyskočí nahoru a ven z karty jako blecha.

Přehled obrázků na výkresech

Obr. 1 - blokové schéma znázorňující příkladné použití tohoto vynálezu.

Příklady provedení vynálezu

Kovový materiál může být tvarován do velmi malých částic. Tenké plátky kovu s proměnlivými délkami mají zvláštní charakteristiky, když jsou použity jako anténa pro vysokou frekvenci (RF). Když jsou délka kovu a vlnová délka vysoké frekvence stejné, kovový materiál rezonuje, či přesněji odráží signál velmi účinným způsobem. Smíchání velmi malých, submikronových dvojpólových antén, to jest kovových částic v plastické kaši v průběhu výroby, bude generovat přirozeně nahodilé rozdělení kovových částic ve výsledné plastické kartě. Toto nahodilé rozmístění částic pak může být vystaveno signálu RF s velmi nízkou úrovní, který odráží unikátní vzor založený na fyzikální poloze částic zavěšených v daném materiálu. Tento odražený vzor je unikátní pro každou kartu, unikátní pro frekvenci použitou na vystavenou kartu, a odlišný v závislosti na tom, jaká část karty je použita k porovnání vzorů.

Tento unikátní fyzikální podpis může být použit k ujištění fyzikální integrity určité karty, stejně jako unikátní identity karty, protože porušení částic, nejenom jako jednotlivých částic, ale rovněž ve vztahu ke každé jiné částici jako celé entity (toto je 3 rozměrová událost), je detekovatelné.

V případě použití kreditních karet či bankomatů (ATM), může být karta a její unikátní podpis RF čten (snímán)v době vsunutí velmi rychle, a fyzikální integrita a unikátní identifikace karty je potvrzena. Frekvence, při níž je karta čtena může být rovněž změněna anebo kolísat v jakékoli žádoucí periodicitě. Například, první den výroby je karta čtena proužkovým způsobem, v podstatě stejným způsobem jako se dnes běžně čte magnetický proužek. Avšak toto snímání signálem vysoké frekvence (RF) je provedeno v počáteční frekvenci 10 Ghz. Odražený signál je charakterizován a uložen v databázi spolu s číslem účtu a jménem příjemce dané karty. Při každém následném čtení této karty nejenže bude potvrzeno počáteční čtení, tato karta může být čtena při ještě další frekvenci za účelem přidání k původní charakteristické databázi a může být použita ke kontrole stejné integrity a unikátnosti. V záležitosti dnů stálé používání karty umožní kontrolu a opětnou kontrolu proti nezměnitelné fyzikální charakteristice, ujišťujíce vydavatele karty, že s ní před tím nebylo žádným způsobem nedovoleně manipulováno.

Karta přítomného vynálezu má dvě fyzikální složky, nosič či těleso karty z plastické hmoty a elektronický modul (přibližně 1 čtvereční palec (6,45 cm²) polovodičových čipů, vzájemně propojeného a zapuštěného v plasconu). Podpis by může být čten (snímán) na modulu jako samostatná entita a/nebo spojen s podpisem karty samotné, k ujištění toho, že vztah těchto dvou zařízení je jak bylo původně zamýšleno. Navíc, jestliže by těleso karty či nosič měly být poškozeny

za úroveň tolerance vydavatele nebo držitele, původní karta může být zničena a část s elektronickým modulem může být zapuštěna do tělesa další karty, v kterémžto případě bude čten (snímán) nový podpis a použit pro budoucí postupy validace vystavením signálu vysoké frekvence (RF). Toto umožní nepřetržité použití obsahu elektroniky a sníží výdaje pro vydavatele spojené s náklady na plastického těleso či kartu.

Žetonové zařízení (identifikačního či jiného dokladového a transakčního charakteru, pozn. překl.) je v souladu s Věstníkem Systému zveřejňování federálních informací (USA, Federal Information Publication Systém Bulletin č. 140-1.) Je to v tomto dokumentu, kde je vyjádřen koncept, že identifikace individua vůči systému by měla být založena na nějakém žetonu (kartě). Touto myšlenkou je, že informace o jednotlivci by měly být umístěny mimo počítačový systém, který se používá pro sdílení informací, a v nějaké bázi, jež je oddělená a izolovaná od přístupu ostatními osobami v tomto systému. To znamená, že tento žeton může být představován pružným diskem, kartou PCMCIA anebo nějakou inteligentní kartou. Omezení funkce a kapacity jiných karet omezují použití tohoto druhu systému.

Žetony se používají mnoho roků. Ve skutečnosti, jedním z problémů trhu řízení bezpečnosti/přístupu je množství různých žetonů nezbytných v každodenním použití. Žeton (spouštěcí karta) se používá k vjezdu do prostoru garáže, další dovoluje vstup do budovy a třetí umožňuje přístup do zvláštního zabezpečeného prostoru, a ještě další karta je potřeba pro přístup k terminálu počítače. V některých prostředích může počet karet přesáhnout tucet. Situace je na prvém místě zapříčiněna vývojem každého z rozmanitých systémů různými výrobci, z nichž každý se pokouší získat většinu prodeje trvající na svých kartách. Spouštěcí karta pro

všechny funkce nebyla možná kvůli nedostatku výpočetního výkonu a kapacity paměti.

Přítomný vynález se svou 16-ti bitovou základní jednotkou (CPU) a velkou kapacitou paměti (na počátku 1 megabyte) nabízí několik důležitých částí pro soubor celkového řešení problémů spojených s bezpečností a elektronickými transakcemi.

Tato 16-ti bitová základní jednotka (CPU) nabízí výpočetní schopnost nezbytnou nejen ke zpracování velkých identifikačních (resp. adresovacích) schémat, ale rovněž ke zpracování rozmanitosti protokolů a přenosových struktur různých výrobců. Karta přítomného vynálezu může podporovat velké paměťové přesuny a co je důležitější, na jediné kartě může podporovat vícenásobné aplikace. Zavedení kódování „tvořivého řízení zápisu (klíče)" (Constructive Key Management) umožňuje kartě podporovat toto aplikační rozdělení. Každý funkční vlastník paměťové části (segmentu) nebo aplikace může provozovat zcela odlišné postupy přístupu a ukládání dat s vědomím, že není možné aby měl kdokoli jiný přístup k nepříslušnému předmětu informací.

Taková karta byla vyrobena firmami Lockheed Martin, Sillcocks Plastics a Secure Transaction Solutions, použitím základní jednotky Intel 80188EB CPU; 64 kB (kilobyte) jednorázových programovatelných procesorových instrukcí; 512 kB DRAM pro vyrovnávací paměť a zápisníkovou paměť pro činnost CPU (provedení programu); 512 kB elektricky měnitelné programové paměti; a sdružených zdrží a spínačů nutných k provozu karty. Mohou být použita dodatečná uspořádání. Systém adresování CPU umožňuje pro adresování přímého přístupu do paměti 32 megabajtů paměti v různých uspořádáních RAM a ROM v souladu s požadavky různých aplikací.

Materiál plastického polotovaru, ze kterého je daná karta řezána, je impregnován (napuštěn) submikronovým kovovým

páskovým materiálem, nezbytným k provádění postupu identifikace (ID) dopadem vysokofrekvenčního signálu (RF). Podpis RF a postup ID je tímto spojen s určitou kartou (například, podpis RF na různých frekvencích a různých místech na kartě).

Tato karta je rovněž schopna podporování magnetického proužku, tištěné informace jako je 4 barevná fotografie, otisk prstu, rubriky s podpisem, speciálních symbolů anebo log, hologramů a jiných položek tištěných či připojených informací.

Základní operační systém pro CPU může být instalován v paměti EEPROM v době výroby nebo před výrobou v továrně na EEPROM.

Karta je přiřazena konkrétnímu uživateli, s unikátním číslem účtu a identifikace vysokofrekvenčním signálem (dále jen „RF ID") je snímána a uložena v energeticky nezávislé paměti, spolu s jakýmikoli jinými nutnými informacemi vydavatele/uživatele, které mohou být žádoucí, jako je 4 barevná fotografie uživatele (komprimovaná a upravená), a je vytvořena Tabulka přidělování paměti (FAT) k umožnění CPU syntakticky analyzovat paměťové sektory k pozdější aktivaci pro dodatečné aplikace. Uživatel bude, při přijetí, aktivovat kartu na dálku jako se to dělá u tradičních karet a v souladu s bezpečnostní praxí, jestliže je udělen přístup pod samostatný kanál distribuce, například, telefon, pošta US či kurýr. Uživatel může přijmout nabízené Osobní identifikační číslo (PIN) anebo si zvolit jeho/její vlastní.

Příkladné použití karty tohoto vynálezu je znázorněno poukazem na Obr. 1. Karta je předložena nějakému bankomatu (ATM). Identifikace vysokofrekvenčním signálem, RF ID, je čtena (snímána) z karty a její hodnota je načítána k registru. CPU karty a bankomat si vyměňují řadu signálu ke stanovení (navázání) společného protokolu. Karta je schopna

vícenásobných protokolů a tudíž umožňuje daleko větší stupeň svobody účasti pro daného uživatele.

Po dosažení společné komunikační báze požaduje bankomat od uživatele karty PIN, jež je uloženo v zakódované podobě v paměťovém sektoru příslušném pro tento druh zařízení, například, transakci MOST či *Cirrus*. PIN je přenášen on-line (spřaženě) do příslušného zúčtovacího střediska přes vyhrazený přenosový spoj, spolu s dříve uloženým číslem RF ID. Tyto informace jsou posílány do vstupního zařízení zúčtovacího střediska, kde jsou kontrolovány na konformitu (shodu). Jestliže budou přijatelné, datovému paketu bude dovoleno aby dále pokračoval směrem do oblasti dekódování, kde je tento informační paket dekódován použitím indexovacích informačních bitů v hlavičce posílaných informací spolu s daty RF ID k vytvoření klíče uživatele, který, když je spojen s v databázi uloženým komponentem tabulky přístupu uživatele, generuje klíč k dekódování vlastního paketu. Uvnitř tohoto paketu jsou doklady individuálního účtu, potvrzení držitele a karty a audit předem stanoveného množství minulých transakcí, jež jsou relevantní pro tohoto konkrétního vydavatele (pokynu, transakce). Je prováděna kontrola platnosti dat (validace) minulých transakcí a bankomatu je posláno povolení aby pokračoval v postupu. Validace posledních transakcí obsahuje provedení několika funkcí, zřejmou aktualizaci či opravu je-li to nutné, a rovněž ujištění nabídnuté vydavateli, že daná zpráva či obsah zakódovaných dat jsou dost velké, takže zajišťují aby nedošlo k žádnému nedovolenému zasahování či částečným změnám. Bankomat potom představuje seznam činností, jež mohou být zvoleny uživatelem a tyto volby jsou použity jako kódovaná rozdělení ke generování v bankomatu zakódované žádosti/ pokynu, které jsou zasílány do daného zúčtovacího střediska. Postup podrobné prohlídky (screeningu) je opakován a jestliže

bude příslušný, daná transakce je povolena. Aktualizovaný (prověřovací záznam obsahující) paket uživatele je zakódován v zúčtovacím středisku a poslán zpátky do bankomatu k zapsání na kartu uživatele. V této konkrétní transakci nedošlo na kartě k žádnému kódování. V dalším protokolu, či v odlišné aplikaci, může být zakódování žádoucí a žádoucí aby k němu došlo na kartě. Výkonný 16-ti bitový procesor a konfigurace paměti karty podporují danou volbu.

Nyní je popsáno použití karty přítomného vynálezu při provádění transakce kreditní karty. Karta je předložena terminálu (koncovému zařízení) obchodníka. Terminál snímá hodnotu RF ID a ukládá ji do registru. Karta dohoduje výměnu (respektive převod dat, pozn. překl.) ke stanovení správného protokolu se zařízením obchodníka. Karta, mající výkonnou 16-ti bitovou CPU (základní zpracovatelskou jednotku), je schopna zpracování mnoha různých aplikací a protokolů a po dosažení přijatelného přenosového spoje rovněž dohoduje nejvyšší přijatelnou míru rychlosti přenosu dat, až do 115 200 Bd (současně). Terminál obchodníka vyžaduje spřažený (on-line) status s příslušným zúčtovacím střediskem a spojená hodnota RF ID a členského čísla obchodníka, spolu s číslem terminálu, jsou použity ke generaci unikátního klíče, který je použit ke komunikaci a vytvoření klíče relace se zúčtovacím střediskem. Unikátní klíč relace ujišťuje účastnícího se obchodníka a uživatele dané karty, že do zúčtovacího střediska bude přenesena úplná transakce a výsledná odpověď bude zakódována použitím identických stran pro sestavení klíče, ujišťujíce, že odpověď či potvrzení mohou být zakódovány pouze příslušnými stranami, t.j. uživatelem a obchodníkem na tomto konkrétním zařízení. Tyto informace jsou v zúčtovacím středisku dekódovány a zpracovány a ověřená transakce je zpracována.

Karta přítomného vynálezu může být rovněž použita k vytvoření bezpečného, internetového komerčního vzájemného vztahu. Uživatel Internetu si zvolí nějakou webovou stránku konkrétního prodejce. Stránka nabízí možnost zavést software transakce. Kliknutí myší a daný přenos je ukončen. Software je zasílán jako sérializovaný (měněný na sériové bity) sebevyjímající proveditelný soubor, jenž když je zvolen bude se sám vyjímat a instalovat a představí obrazovku, která se dotazuje, jestli nyní bude vhodná doba k vyplnění registračního formuláře pro toho konkrétního prodejce. Toto se rovněž navrhuje k provedení off-line. Registrační formulář je vyplněn a jsou zapsány všechny významné údaje včetně typu platby, čísla kreditní karty atd. Software se dotazuje, zda si uživatel přeje použít výhody funkce uložení (paměti) povolení, která umožňuje uživateli ukládat na kartu rozdělení oprávnění ke vstupu/identifikačních rozdělení, která byla generována softwarem prodejce. Uživatel souhlasí a karta je prezentována a informace uloženy. Je zvolen odesílací knoflík a automaticky zakódovaný svazek je poslán zpátky vybranému prodejci. Prodejce přijímá zakódovaný svazek a otevírá ho. Rozpoznávajíce určitou formu/strukturu svazku, zakódování je automaticky zapsáno s pořadovým číslem kopie nataženého softwaru a vstupní zařízení prodejce dovoluje svazku postoupit do oblasti zpracování. Uživatel, který se vrátil zpátky na danou webovou stránku, se nyní dívá na katalog prodejce a vybírá si položky k zakoupení, z nichž každá má nějaké číslo. Je to kombinace (spojení) těchto čísel a číslice sérializovaného software, jež generuje vybrané složky zakódování dělenému zápisu. Všechny zprávy jsou chráněny a všechny přenosy mezi prodejcem a uživatelem jsou unikátní.

P A T E N T O V É N Á R O K Y

1. Kryptografický prostředek (karta) zahrnující:
   - plastický podklad;
   - tenké kovové plátky zapuštěné v nahodilých umístěních v plastickém podkladu za účelem poskytnutí unikátního podpisu při vystavení karty signálu vysoké frekvence; a
   - elektronický modul připojený k plastickému podkladu a obsahující:
     - zpracovatelský prostředek a
     - paměťový prostředek.

2. Kryptografický prostředek podle nároku 1, v y z n a č u j í c í s e t í m, že plastický podklad obsahuje plasconový materiál, jenž zapouzdřuje alespoň elektronický modul.

3. Kryptografický prostředek podle nároku 1, v y z n a č u j í c í s e t í m, že tenké kovové plátky v něm jsou formovány v nahodilých velikostech.

4. Kryptografický prostředek podle nároku 1, v y z n a č u j í c í s e t í m, že tenké kovové plátky v něm jsou formovány v nahodilých, submikronových velikostech.

5. Kryptografický prostředek podle nároku 1, v y z n a č u j í c í s e t í m, že elektronický modul v něm obsahuje základní zpracovatelskou jednotku (CPU).

6. Kryptografický prostředek podle nároku 5, v y z n a č u j í c í s e t í m, že touto základní zpracovatelskou jednotkou je 16-ti bitová základní jednotka.

7. Kryptografický prostředek podle nároku 1, v y z n a č u j í c í s e t í m, že elektronický modul obsahuje ukládací paměť.

8. Kryptografický prostředek podle nároku 7, v y z n a č u j í c í s e t í m, že ukládací paměť obsahuje identifikační údaje uživatele.

9. Kryptografický prostředek podle nároku 8, v y z n a č u j í c í s e t í m, že identifikační číslo uživatele je vyhovující pro poskytnutí přístupu k finančnímu účtu prostřednictvím použití bankomatu (ATM).

10. Způsob zformování kryptografického prostředku zahrnující:

a) formování plastického podkladu majícího v sobě dutinu, a tenkých kovových plátků v něm zapuštěných;
b) sestavení elektronického modulu použitím vzoru vícečipového modulu;
c) umístění tohoto elektronického modulu uvnitř dutiny; a
d) zapouzdření alespoň elektronického modulu v plasconovém materiálu.

11. Způsob dle nároku 10, v y z n a č u j í c í s e t í m, že sestavení elektronického modulu obsahuje sestavení základní zpracovatelské jednotky (CPU).

12. Způsob dle nároku 11, v y z n a č u j í c í s e t í m, že sestavení této základní zpracovatelské jednotky obsahuje sestavení 16-ti bitové základní jednotky.

13. Způsob dle nároku 10, v y z n a č u j í c í s e t í m, že sestavení elektronického modulu obsahuje sestavení ukládací paměti.

14. Způsob užívání kryptografického prostředku při provádění transakce, zahrnující:

a) předložení karty (žetonu) v bodě transakce (jednání);
b) snímání fyzikálních charakteristik karty k získání podpisu této karty;
c) vyhodnocení tohoto podpisu k výběru informací; a
d) stanovení, zda na základě vyjmutých informací bude určitá transakce pokračovat.

15. Způsob dle nároku 14, v y z n a č u j í c í s e t í m, že fyzikální charakteristiky karty obsahují přítomnost tenkých kovových plátků obsažených v kartě.

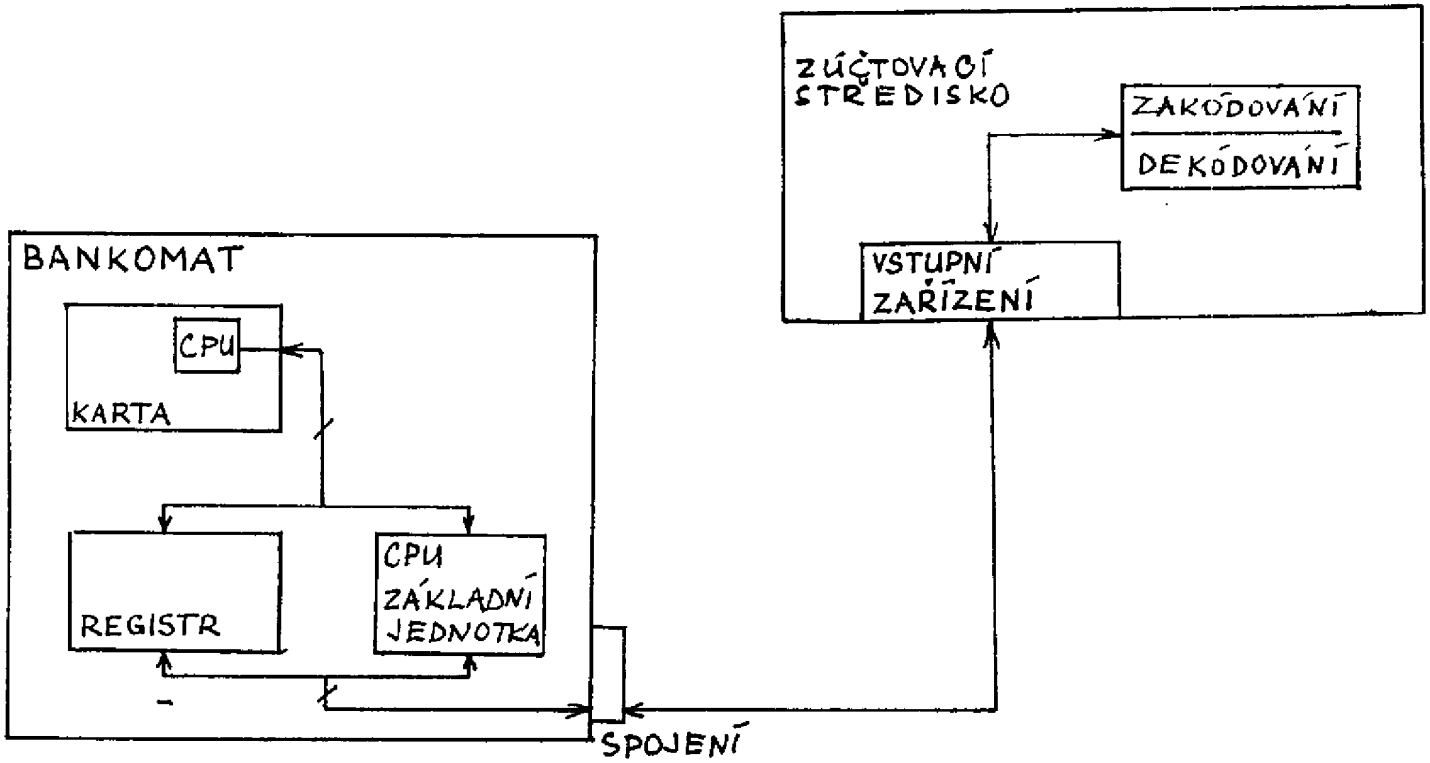
16. Způsob dle nároku 15, v y z n a č u j í c í s e t í m, že podpisem dané karty je podpis čtený při vystavení karty vysokofrekvenčnímu signálu.

17. Způsob dle nároku 14, v y z n a č u j í c í s e t í m, že vybírané informace jsou bezpečnostními informacemi.

18. Způsob dle nároku 14, v y z n a č u j í c í s e t í m, že vybírané informace jsou identifikačními informacemi uživatele karty.

19. Způsob dle nároku 14, dále zahrnující čtení (snímání) údajů z karty.

20. Způsob dle nároku 19, v y z n a č u j í c í s e t í m, že čtení údajů z karty obsahuje komunikaci se základní jednotkou, uspořádanou na kartě za účelem čtení údajů uložených v paměti uspořádané na této kartě.


ZÚČTOVACÍ STŘEDISKO
ZAKÓDOVÁNÍ
DEKÓDOVÁNÍ
VSTUPNÍ ZAŘÍZENÍ
BANKOMAT
CPU
KARTA
REGISTR
CPU ZÁKLADNÍ JEDNOTKA
SPOJENÍ