

PŘIHLÁŠKA VYNÁLEZU

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

(19)
ČESKÁ
REPUBLIKA



ÚŘAD
PRŮMYSLOVÉHO
VLASTNICTVÍ

- (22) Přihlášeno: **30.07.1998**
(32) Datum podání prioritní přihlášky: **11.08.1997 16.01.1998**
(31) Číslo prioritní přihlášky: **1997/055418 1998/008122**
(33) Země priority: **US US**
(40) Datum zveřejnění přihlášky vynálezu:
(Věstník č: 3/2004)
(86) PCT číslo: **PCT/GB1998/002283**
(87) PCT číslo zveřejnění: **WO 1999/008238**

(21) Číslo dokumentu:

2000-470

(13) Druh dokumentu: **A3**

(51) Int. Cl. :
G07F 7/10
G07F 19/00

(71) Přihlašovatel:

INTERNATIONAL BUSINESS MACHINES
CORPORATION, Armonk, NY, US

(72) Původce:

Maes Stephane, Danbury, CT, US
Sedivy Jan, Praha, CZ

(74) Zástupce:

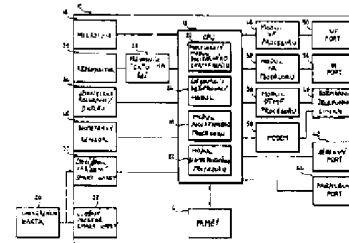
Kalenský Petr JUDr., Hálkova 2, Praha 2, 12000

(54) Název přihlášky vynálezu:

**Přenosný systém zpracovávající informace a
transakce a způsob využívající biometrickou
autorizaci a zabezpečení digitálního certifikátu**

(57) Anotace:

Osobní digitální asistent (PDA) s dotykovou obrazovkou nebo jiným ekvivalentním uživatelským rozhraním má mikrofon a lokální centrální procesorovou jednotku (CPU) pro zpracovávání hlasových příkazů a pro zpracování biometrických dat kvůli zajištění ověření uživatele. PDA také obsahuje paměť (14) pro uložení finančních a osobních informací uživatele a I/O funkce pro čtení a zápis informací na různé karty jako například karty smartcard, magnetické karty, optické karty nebo EAROM karty. PDA obsahuje univerzální kartu (14), což je běžná generická karta smartcard s jedinečným otiskem dodaným poskytovatelem služby, na kterou lze stáhnout zvolené finanční nebo osobní informace uložené v PDA kvůli provedení jistých spotřebitelských transakcí. PDA obsahuje modem, sériový port a/nebo paralelní port kvůli zajištění funkce přímé komunikace s periferními zařízeními – jako například POS a ATM terminály – a je schopné vysílat nebo přijímat informace prostřednictvím bezdrátové komunikace, jako je vysokofrekvenční (VF) a infračervená (IR) komunikace. Tento vynález je přednostně provozován ve dvou režimech, tj. režimu klient/server a v lokálním režimu.



**PŘENOSNÝ SYSTÉM ZPRACOVÁVJÍCÍ INFORMACE A TRANSAKCE A
ZPŮSOB VYUŽÍVAJÍCÍ BIOMETRICKOU AUTORIZACI A ZABEZPEČENÍ
DIGITÁLNÍHO CERTIFIKÁTU**

Oblast techniky

Vynález se týká přenosného systému a způsobu zpracovávajícího informace a transakce a podrobněji přenosného systému zpracovávajícího informace a transakce a způsobu, který využívá zabezpečení digitálního certifikátu a biometrickou autorizaci k zajištění ověřování osob před zpracováním uživatelem požadovaných finančních transakcí a poskytnutím osobních informací.

Dosavadní stav techniky

Nyní je na domácím spotřebitelském trhu všeobecně uznáváno, že nákup nebo prodej zboží nebo služeb pomocí kreditních karet v terminálech na místě prodeje (POS) a také provádění elektronických převodů financí na automatických terminálech (ATM) pomocí ATM karet je účinnější, než používání hotovosti k placení za zboží nebo služby nebo splácení dluhů. Použití hotovosti jako prostředků k nákupu zboží nebo splácení dluhů se z několika důvodů obecně považuje za těžkopádné. Za prvé ve smyslu účtování musí spotřebitel ručně vytvářet záznamy a potvrzovat své účty, aby měl přehled o těchto transakcích v hotovosti. Při použití kreditní karty vydané finanční institucí však transakce spotřebitele zaznamenává tato finanční instituce a

účty jsou spotřebiteli dodávány měsíčně, což zajišťuje vylepšené účtování a odsouhlasení účtů.

Navíc použití hotovosti je finančně nejistý způsob ochrany spotřebitelů vůči zneužití a krádeži. Pokud je například spotřebitel přesvědčen, že mu byl prodán druhořadý nebo předražený produkt, což se obvykle stává během rychlých spotřebitelských transakcí, kdy spotřebitel nemusí mít po nějakou dobu od koupě adekvátní čas přemýšlet o koupi, je pro spotřebitele mnohem jednodušší kontaktovat finanční instituci aby zastavila platbu za zboží zakoupené s použitím kreditní karty, než aby uživatel dostal zpět hotovost od prodejce, od kterého bylo toto zboží zakoupeno. Dále je fakticky nemožné pro spotřebitele dostat zpět hotovost, která byla ukradena nebo ztracena. Na druhé straně pokud budou kreditní karty spotřebitele ukradeny nebo ztraceny, může spotřebitel kontaktovat odpovídající finanční instituci kvůli zrušení těchto karet a získání nových účtů s kreditními kartami.

Tudíž dnes existuje silný trend v přesunu směrem k "bezhotovostní společnosti", který způsobil podstatný nárůst v použití kreditních karet, ATM karet a přímých debetních karet (souhrnně "finančních karet") pro umožnění spotřebitelských transakcí. Nehledě na viditelné výhody použití finančních karet místo hotovosti existuje několik nevýhod v použití těchto karet. Pokud například spotřebitel často používá značné množství finančních karet, musí spotřebitel fyzicky vlastnit všechny takovéto karty, aby mohl přistupovat k požadovanému účtu. Nutnost nosit takové velké množství finančních karet může být pro spotřebitele příliš těžkopádné, protože podstatné množství prostoru je zabráno těmito kartami v peněžence nebo kabelce

spotřebitele. Pokud je dále peněženka nebo kabelka ztracena nebo ukradena, musí spotřebitel kontaktovat finanční instituci pro každou finanční kartu kvůli zrušení účtu, aby se zabránilo neoprávněnému uživateli v nakupování s těmito kartami, což je také zdlouhavý úkol.

Jiná nevýhoda v použití finančních karet je, že spotřebitelé nejsou úplně chráněni před neoprávněným použitím ztracených nebo ukradených karet. Například obchodník může potvrdit vlastnictví kreditní karty během transakce spotřebitele porovnáním schváleného podpisu, který je (nebo by měl být) zapsán na zadní straně kreditní karty, s podpisem osoby podepisující potvrzení ke kreditní kartě. Ve skutečnosti obchodníci obecně neporovnávají tyto podpisy během takové transakce a i když ano, nemusí porovnávat takové podpisy tak pečlivě a profesionálně aby rozlišili vedlejší rozdíly mezi podpisem spotřebitele a zfalšovaným podpisem neoprávněného spotřebitele. Tudíž během časového období mezi ztrátou nebo krádeží kreditní karty spotřebitele a dobou, kdy si spotřebitel uvědomí tuto ztrátu nebo odcizení a zruší účet, může neoprávněný uživatel, který našel nebo odcizil kartu, platit podstatným množstvím peněz na účet karty spotřebitele, přičemž ponechá na spotřebiteli břemeno nutnosti sporu o tyto neoprávněné poplatky s finanční institucí.

WO-A-9417498 popisuje transakční systém, kde data z několika karet jsou přenášena do udržovací modulové paměti a karta je pak vymazána. Data z karty, která se mají použít, jsou znovu přenesena na libovolnou kartu před transakcí zadáním PIN nebo biometrických dat.

WO-A9522810 popisuje certifikáty pro ověřování určité

transakce, ale tímto odkazem není navržen jedinečný certifikát, který ověřuje všechny aplikace.

Podstata vynálezu

Je tudíž předmětem tohoto vynálezu zajistit přenosné zařízení zpracovávající informace a transakce ("osobní digitální asistent" neboli "PDA") do kterého může uživatel uložit informace o své kreditní kartě (tj. finanční), ATM kartě a/nebo debetní kartě a také osobní informace a pak přistupovat ke zvoleným informacím a zapisovat zvolené informace na kartu smartcard („Univerzální kartu“), která se pak použije k zahájení POS, ATM, nebo spotřebitelské transakce.

Je dalším předmětem tohoto vynálezu zajistit PDA zařízení, které využívá biometrické zabezpečení k zajištění ověření uživatele před přístupem ke zvoleným finančním a osobním informacím a zápisem zvolených finančních a osobních informací na Univerzální kartu.

Je dalším předmětem tohoto vynálezu zajistit PDA zařízení se zabezpečením digitálního certifikátu, pomocí něhož se po uživateli požaduje periodicky stahovat dočasný digitální certifikát z centrálního serveru poskytovatele služeb takové univerzální karty do PDA zařízení před přístupem ke zvoleným finančním a osobním informacím a zápisem zvolených finančních a osobních informací do Univerzální karty.

Je dalším předmětem tohoto vynálezu zajistit zařízení PDA se zabezpečením digitálního certifikátu, který je



slučitelný s aktuální infrastrukturou (tj. okamžitě použit bez nutnosti měnit existující infrastrukturu) a který přináší biometrické zabezpečení do systémů pro přenos elektronických dat, které momentálně nejsou schopné provádět biometrické ověřování.

Je dalším předmětem tohoto vynálezu zajistit PDA zařízení se zabezpečením digitálního certifikátu, který může být rozšířen na všechny aplikace nebo systémy, kde se používají magnetické karty a/nebo karty smartcard, jako například přístupové řídicí karty pro přístup ke službě zařízení nebo do budovy, hotovostní karty k provádění ATM transakcí, telefonní karty nebo celulární karty (např. pro GSM digitální celulární mobilní radio systém) k provádění telefonních hovorů a zaměstnanecké karty pro přístup k důvěrným informacím.

Z jednoho hlediska tohoto vynálezu obsahuje přenosné zařízení pro zpracování informací a transakcí: centrální procesorovou jednotku pro řízení funkce a pro zpracovávání množství operací zařízení; paměťové prostředky, operativně připojené k centrální procesorové jednotce k ukládání finančních a osobních informací a k ukládání dočasného digitálního certifikátu; komunikační prostředky operativně připojené k centrální procesorové jednotce k ustavení komunikačního spojení s centrálním serverem ze vzdáleného místa kvůli získání dočasného digitálního certifikátu; prostředky uživatelského rozhraní operativně připojené k centrální procesorové jednotce pro zahájení alespoň jedné z více operací zařízení a zvolení části buď z finančních nebo osobních informací z paměťových prostředků; univerzální kartu, oddělitelně připojenou k centrální procesorové jednotce pro přijetí zvolené části buď z finančních, nebo



osobních informací; a programové prostředky, operativně připojené k centrální procesorové jednotce a reagující na dočasný digitální certifikát pro zápis zvolené části buď z uložených finančních nebo osobních informací na univerzální úložnou kartu, kde programovým prostředkům je zabráněno v zápise zvolené části buď z finančních nebo osobních informací na univerzální kartu pokud je dočasný digitální certifikát neplatný.

Toto provedení je přenosný klientský PDA s dotykovou obrazovkou nebo jiným ekvivalentním uživatelským rozhraním, které obsahuje mikrofon a lokální centrální procesorovou jednotku (CPU) ke zpracování hlasem aktivovaných příkazů a ke zpracování biometrických dat kvůli zajištění biometrického ověřování uživatele. Tento vynález obsahuje paměť k ukládání finančních a osobních informací uživatele a I/O funkce pro zápis informací na a čtení informací z různých karet jako jsou karty smartcard, magnetické karty, optické karty nebo karty EAROM (elektricky měnitelná paměť pouze ke čtení). Tento vynález obsahuje univerzální kartu, což je běžná obecná karta smartcard s jednoznačným otiskem (tj. číslem účtu) opatřeným poskytovatelem služby, na kterou lze stahovat zvolené finanční nebo osobní informace uložené v PDA kvůli provádění různých transakcí. PDA přednostně obsahuje modem a sériový port a/nebo paralelní port kvůli zajištění schopnosti přímé komunikace s periferními zařízeními. PDA je také schopno přenášet nebo přijímat informace prostřednictvím bezdrátové komunikace jako je vysokofrekvenční (VF) a infračervená (IR) komunikace.

Tento vynález je přednostně provozován ve dvou režimech, tj. režimu klient/server a v lokálním režimu. Režim klient/server se periodicky provádí kvůli stažení



dočasného digitálního certifikátu z centrálního serveru poskytovatele služby PDA a univerzální karty. Režim klient/server se provádí založením komunikace mezi PDA a centrálním serverem poskytovatele služby prostřednictvím modemu nebo bezdrátové komunikace. Po založení komunikace ověří centrální server uživatele buďto biometricky nebo prostřednictvím PIN nebo hesla nebo jejich kombinací a pak generuje dočasný digitální certifikát, který se stáhne do PDA. Dočasný platný digitální certifikát je nutný pro přístup ke zvoleným informacím uloženým v PDA a k zápisu těchto informací do univerzální karty.

Dále se provádí lokální režim provozu PDA kvůli zahájení spotřebitelské transakce. Přednostně v lokálním režimu uživatel zvolí jednu z předem přihlášených kreditních karet, které jsou uloženy v PDA sdělením verbálního příkazu do mikrofonu PDA, pomocí kterého CPU zpracuje verbální příkaz a provede ověření uživatele. Eventuálně lze ověření uživatele (tj. lokální ověření) provést s použitím buďto biometrických dat, PIN nebo hesla nebo jejich kombinací. Po lokálním ověření se získají zvolené informace z paměti a zapíší se do univerzální karty, která je pak schopná zahájit transakci. Při nepřítomnosti platného digitálního certifikátu se však zvolené informace nezapíší do univerzální karty bez ohledu na to, zda uživatel poslal lokální ověření.

Tento vynález s výhodou omezuje obtíže s nutností přenášet více finančních karet a/nebo kreditních karet, které uživatel může často používat. Finanční informace pro každou kartu mohou být uloženy v PDA a zapsány v případě potřeby do univerzální karty. Pokud je univerzální karta ztracena nebo ukradena, uživatel bude muset kontaktovat

pouze poskytovatele služby kvůli zrušení a opětovnému vydání nového účtu. Navíc kvůli biometrickému zabezpečení a zabezpečení pomocí digitálního certifikátu, které chrání vůči neoprávněnému přístupu k finančním a osobním informacím uživatele, je ztracená nebo ukradená univerzální karta nepoužitelná pro neoprávněného uživatele.

Dále lze tento vynález okamžitě využít bez potřeby změn v existující infrastruktuře protože PDA a univerzální karta se mohou použít s libovolným systémem, který využívá magnetické karty nebo karty smartcard k elektronickému přenosu dat, jako například POS terminály (v místě prodeje) nebo automatické pokladní stroje (ATM), které poskytují funkci přímého debetu.

Přehled obrázků na výkresech

Vynález bude blíže vysvětlen prostřednictvím konkrétních příkladů provedení znázorněných na výkresech, na kterých představuje

obr. 1 blokové schéma znázorňující prvky přenosného zařízení zpracovávajícího informace a transakce podle provedení tohoto vynálezu;

obr. 2a a 2b schémata univerzální karty podle provedení tohoto vynálezu;

obr. 3 blokové schéma ukazující interakci přenosného zařízení zpracovávajícího informace a transakce ve spojení se zpracováním transakce podle tohoto vynálezu;

- obr. 4 blokové schéma znázorňující režim provozu klient/server podle tohoto vynálezu;

- obr. 5 blokové schéma znázorňující lokální režim provozu podle tohoto vynálezu; a

- obr. 6 blokové schéma znázorňující jiný lokální režim provozu podle tohoto vynálezu.

Příklady provedení vynálezu

Rozumí se, že stejné nebo podobné součásti znázorněné na obrázcích jsou označeny stejnou vztahovou značkou. Dále se rozumí, že prvky funkčních modulů zde popsaných podle tohoto vynálezu mohou být implementovány v různých formách hardwaru, softwaru nebo jejich kombinací. Přednostně jsou hlavní biometrické ověřovací prvky a prvky pro rozpoznávání řeči implementovány softwarem a mohou obsahovat libovolnou vhodnou a upřednostňovanou architekturu procesoru k provedení vynálezu naprogramováním jednoho nebo více procesorů k obecnému použití. Dále se rozumí, že, protože některé z komponent vynálezu zde popisovaného jsou přednostně implementovány jako softwarové moduly, mohou se aktuální spojení ukázaná na obrázcích lišit podle způsobu, jakým je vynález naprogramován. Samozřejmě lze k implementaci vynálezu použít speciální procesory.

S odkazem na obr. 1 je ukázáno blokové schéma znázorňující prvky přenosného zařízení 10 PDA zpracovávajícího informace a transakce podle provedení tohoto vynálezu. Srdcem zařízení je centrální procesorová

jednotka (CPU) 12, která řídí operace zařízení 10 PDA prostřednictvím programů uložených v paměti 14 a spouštěných CPU 12. Podrobně obsahuje CPU 12 modul 16 akustického procesoru pro zpracování hlasových příkazů vkládaných do zařízení PDA 10 mikrofonom 18. Modul 16 s akustickým procesorem se také používá k provádění ověření lokální hovořící osoby. CPU 12 také obsahuje modul 20 procesoru digitálního certifikátu pro zpracovávání digitálního certifikátu získaného v režimu provozu klient/server (podrobněji bude popsán níže) a modul 22 biometrického procesoru pro zpracovávání biometrických dat navíc k nebo alternativně k hlasovým datům, kvůli zajištění ověření uživatele. CPU 12 dále obsahuje šifrovací /dešifrovací modul 24 pro šifrování osobních a finančních informací předtím, než se uloží do paměti 14 a pro dešifrování takových informací jakmile k nim přistupuje uživatel. Přestože ilustrativní provedení zde ukazuje CPU 12 obsahující modul 20 digitálního certifikátu, šifrovací/dešifrovací modul 24, modul 16 akustického procesoru a modul 22 biometrického procesoru, rozumí se, že takové moduly mohou také být implementovány jako moduly pro speciální účely, přičemž každý má procesor, připojenou paměť a uložené programy k provádění těchto funkcí.

Zařízení 10 PDA obsahuje čtecí/zapisovací zařízení 26 karet smartcard (jak je v oboru známo) pro čtení informací z různých karet a zápis informací na různé karty, např. magnetické karty, IC karty a/nebo EAROM karty (s použitím známých standardů a technik). Během lokálního režimu provozu zařízení 10 PDA, se univerzální karta 26 podle tohoto vynálezu vloží do čtecího/zapisovacího zařízení 30 karet smartcard a po ověření uživatele se zvolené finanční nebo osobní informace zapíše na univerzální kartu 26. Pokud se



univerzální karta 26 nepoužívá, může se uložit do úložného oddělení 32 karet smartcard zařízení 10 PDA.

Zařízení 10 PDA obsahuje uživatelské rozhraní/displej 34, což je přednostně dotykový displej s tekutými krystaly (LCD) (nebo ekvivalentní uživatelské rozhraní) pro zobrazování a/nebo vkládání dat spojených s operacemi nebo funkcemi zařízení 10 PDA. Eventuálně může být rozhraní/displej 24 tvořen klávesnicí a běžným LCD displejem. Navíc zařízení 10 PDA může akusticky komunikovat s uživatelem, nebo od něj požadovat informace reproduktorem 26, který je účinně připojen k CPU 12 prostřednictvím převodníku 38 textu na řeč. Převodník 38 textu na řeč převádí signály z CPU 12 na syntetickou řeč, která se pak pouští na reproduktoru 36. Zařízení 10 PDA může být nastaveno tak, aby současně zobrazovalo tyto informace spolu s generováním syntetické řeči. Dále může PDA zařízení 10 pracovat bez displeje (nebo s omezeným displejem) a spoléhat na funkce převodu textu na řeč ke sdělení informací uživateli takového zařízení.

Biometrický senzor 40 libovolného konvenčního typu může být také opatřen pro sběr biometrických dat (jiných nežli zvukových dat, která jsou přijímána mikrofonem 18) jako například otisku prstu, palce nebo dlaně, vzorku rukopisu, vzorku cév sítnice, nebo jejich kombinace, kvůli zajištění biometrického ověření jako alternativy k nebo navíc kromě biometrického ověřování hlasu. Tato data pak zpracuje modul 22 biometrického procesoru kvůli zajištění ověření uživatele (tj. biometrické zabezpečení) před přístupem k finančním a osobním informacím uloženým v paměti 14. Odborníci ocení, že funkce biometrického ověření zařízení PDA lze nahradit nebo doplnit PIN (osobní identifikační číslo) nebo heslem kvůli

zajištění ověření uživatele.

Zařízení 10 PDA může být přednostně vybaveno různými komunikačními porty jako je sériový port 42 a paralelní port 44 (s využitím známých standardů počítačového rozhraní), operativně připojenými k CPU 12 a také rozhraním 46 telefonní linky (s použitím známých spojení prostřednictvím rozhraní) kvůli zajištění prostředků pro ustavení komunikačního spojení mezi zařízením 10 PDA a jinými periferními zařízeními jako jsou počítače, modemy a tiskárny. Kvůli založení bezdrátové komunikace může být zařízení přednostně vybaveno modulem 48 VF procesoru operativně připojeného mezi CPU 12 a VF portem 50, kvůli zpracování příchozích VF informací přijatých VF portem 50 a kvůli generování přenosových signálů, které se posílají na výstup z VF portu 50 s použitím běžných konstrukcí a technik. Zařízení může být také vybaveno modulem 52 IR procesoru, operativně připojeného mezi CPU 12 a IR port 54 kvůli zpracování příchozích optických informací a kvůli generování výstupních optických signálů s použitím běžných konstrukcí a známých technik. Přednostně obsahuje PDA zařízení 10 modul 56 DTMF (kmitočtová volba duálními tóny) procesoru a modem 58, operativně připojený mezi CPU 12 a rozhraním 46 telefonní linky. Komunikace finančních informací se může provést prostřednictvím komunikace modemem a/nebo komunikací DTMF tóny na telefonní lince s použitím známých metod. DTMF komunikaci lze použít ke zpracování PINů pro ověření a autorizaci uživatele.

Nyní s odkazem na obr. 2a a 2b jsou ukázána schémata univerzální karty 26 podle provedení tohoto vynálezu. Univerzální karta 26 je v zásadě generická karta smartcard, která obsahuje buďto magnetický pásek 28 (obr. 2a) nebo

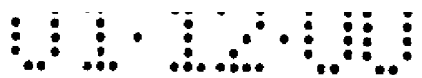
integrovaný čip (IC) 29 (obr. 2b) nebo obojí, k uložení zvolených informací, které se získají z paměti 14 a zapíší se do univerzální karty 26 prostřednictvím čtecího/zapisovacího zařízení karet smartcard 30 během lokálního režimu provozu zařízení 10 PDA. Univerzální karta 26 (vydaná poskytovatelem služby) obsahuje jedinečné číslo 27 univerzální karty, které je na ní vtisknuté a které odpovídá číslu určeného konta uživatele dodaného poskytovatelem služby (který je analogický s číslem účtu poskytnutým na kreditní kartě nebo ATM kartě).

Jak bude podrobněji popsáno níže, může být číslo 27 univerzální karty využito k zajištění ověření uživatele v POS transakcích spotřebitele využitím tradičního mechanického snímače místo magnetického snímače, který je schopen magneticky přečíst magnetický pásek 28 univerzální karty 26. Jedinečné číslo 27 univerzální karty lze také použít k zajištění ověření uživatele v případech, kdy se provádí spotřebitelské transakce vzdáleně prostřednictvím telefonu. V takovém případě, jak bylo vysvětleno níže, se zobrazí autorizační číslo, které je jedinečné pro aktuální digitální certifikát na zařízení 10 PDA po ověření uživatele. Autorizační číslo spolu s jedinečným číslem 27 univerzální karty, lze použít k ověření uživatele.

S odkazem na obr. 3, je ukázáno blokové schéma znázorňující interakci zařízení 10 PDA ve spojení se zpracováním transakce podle tohoto vynálezu. Uživatel zařízení 10 PDA a univerzální karty 26 (obr. 1 a 2) musí nejdříve provést proceduru přihlášení k poskytovateli služby. Přihlášení zahrnuje získání univerzální karty 26 s určeným číslem účtu (tj. jedinečným otiskem 27 na univerzální kartě 26) a poskytnutí poskytovateli služby

informací o kreditní kartě uživatele nebo o ATM kartě tak, aby se tyto informace mohly ověřit na finančních institucích 70, které tyto karty vydali. Tyto informace se pak uloží na centrální server 60 poskytovatele služby. Uživatel pak může následně stáhnout tyto informace do zařízení 10 PDA ustavením komunikačního spojení (L1) s centrálním serverem 60. Eventuálně se mohou kreditní karty nebo ATM karty stáhnout do PDA zařízení 10 přímým přečtením informací obsažených na těchto kartách prostřednictvím čtecího/zapisovacího zařízení 30 karet smartcard zařízení 10 PDA. V takovéto situaci porovná zařízení 10 PDA ID uživatele kreditních karet s ID uživatele zařízení PDA kvůli ověření uživatele a kvůli zabránění uživateli ve stažení informací z karet vlastněných jinou osobou do zařízení 10 PDA uživatele. V případě že zařízení PDA není schopné ověřit vlastníka karty, která je přímo stahována prostřednictvím čtecího/zapisovacího zařízení 30 karet smartcard (tj. karta neobsahuje název svého vlastníka), bude po uživateli vyžadováno přihlášení karty dodáním poskytovateli služby informací o kartě (kvůli získání ověření od příslušné finanční instituce) a pak připojení k centrálnímu serveru 60 kvůli stažení informací o kartě.

Přihlášení také obsahuje dodání poskytovateli služby osobních informací jako je číslo pojištěnce uživatele, adresa, jméno za svobodna a datum narození, které jsou uloženy na centrálním serveru 60. Tyto informace se pak použijí k ověření uživatele během režimu klient/server před vydáním digitálního certifikátu. Osobní identifikační číslo PIN a univerzální karta 26 s jedinečným číslem 27 účtu je dodáno poskytovatelem služby. Tyto informace stejně jako biometrická data jako například hlasové záznamy (modely) uživatele, jsou také uloženy na centrálním serveru 60



poskytovatele služby pro ověření uživatele během režimu klient/server kvůli získání digitálního certifikátu (bude podrobněji popsán níže). Centrální server 60 je počítač, který je naprogramován k provádění funkcí zde popsaných jako biometrické ověření, rozpoznávání řeči a generování a stahování dočasného digitálního certifikátu.

S odkazem na obr. 1, 3 a 4 je nyní popsán režim činnosti klient/server tohoto vynálezu. Jak je uvedeno výše, musí uživatel periodicky připojovat PDA zařízení 10 s centrálním serverem 60 poskytovatele služby (spojení L1, obr. 3) kvůli získání platného digitálního certifikátu z centrálního serveru 60 před zahájením spotřebitelské transakce. Podrobně je digitální certifikát binárně zašifrovaný soubor, který se musí stáhnout do zařízení 10 PDA předtím, než bude možné zapsat osobní nebo finanční informace uživatele do univerzální karty 26. Digitální certifikát obsahuje informace týkající se (ale nikoli pouze) čísla účtu zařízení 10 PDA, datum, ve kterém byl digitální certifikát ověřen a jeho datum vypršení a také všechna omezení, která existují pro každou přihlášenou kartu. Digitální certifikát je uložen v paměti 14 zařízení 10 PDA. Před spuštěním transakce (tj. stažením informací o zvolené kartě z paměti 14 do univerzální karty 26) se digitální certifikát zašifruje šifrovacím/dešifrovacím modulem 24 a zavede do modulu 20 procesoru digitálního certifikátu, kde se zpracuje, aby se zjistilo, zda je platný.

Aby se získal digitální certifikát, musí uživatel ustavit komunikační spojení (spojení L1, obr. 3) s centrálním serverem 60 poskytovatele služby (krok 100, obr. 4). Komunikace se může založit vytočením čísla na centrální server 60 prostřednictvím telefonní linky



prostřednictvím modemu 58 a rozhraní 46 telefonní linky. Tento vynález také očekává možnost ustavení komunikace s centrálním serverem 60 prostřednictvím digitálního komunikačního kanálu jako je internet, intranet nebo místní počítačová síť. Eventuálně se může komunikace mezi zařízením 10 PDA a centrálním serverem 60 založit prostřednictvím bezdrátové komunikace, např. prostřednictvím VF portu 50 a modulu 48 VF procesoru. Dále může být zařízení 10 PDA připojeno k centrálnímu serveru prostřednictvím speciálního ATM (nebo jiných takových kiosků), který používá intranet a TCP/IP ke spojení s centrálním serverem 60. Rozumí se, že zařízení 10 PDA může být operativně připojeno ke kiosku buďto přímo (např. prostřednictvím sériového nebo paralelního portu 42 a 44) nebo prostřednictvím bezdrátové komunikace prostřednictvím VF portu 50 nebo IR portu 53. Jak bylo ukázáno výše, odborníci ocení, že centrální server 60 podle tohoto vynálezu je přístupný prostřednictvím libovolného běžného komunikačního kanálu.

Po ustavení komunikace bude uživatel vyzván (buďto textově na uživatelském rozhraní/displeji 34 nebo slovně prostřednictvím převodníku 38 textu na řeč a reproduktoru 36) k zadání jistých ověřovacích dat (krok 102). Tato data se pak přenesou na centrální server 60 prostřednictvím komunikačního spojení L1. Podrobně se může centrální server 60 dotázat uživatele na několik otázek (které se náhodně vyberou z celkového počtu otázek, na které se zeptalo a odpovědělo během procesu přihlašování). Tyto otázky získá CPU 12 zařízení 10 PDA buďto se zobrazí na uživatelském rozhraní/displeji 34, nebo se odešlou do převodníku 38 textu na řeč, kde se převedou na syntetickou řeč a akusticky vyšlou uživateli prostřednictvím reproduktoru 36. Centrální server 60 může také vyzvat

uživatele k zadání PIN, který byl vydán uživateli během procesu přihlášení.

Pokud nejsou tato požadovaná ověřovací data dodána během předem určené doby (krok 104), centrální server 60 automaticky rozpojí komunikační spojení L1, a digitální certifikát se nestáhne (krok 106). Na druhé straně pokud uživatel včas vloží požadovaná ověřovací data (krok 104), zpracuje centrální server 60 tato data (krok 108). Uživatel může dodat požadovaná ověřovací data zadáním odpovědi na otázky mluvením do mikrofonu 18. Zvukové signály pak přijme CPU 12 a pak se nasměrují do modulu 16 akustického procesoru, kde se odpovědi uživatele zpracují a přenesou na centrální server 60 prostřednictvím komunikačního spojení L1. Navíc může uživatel zadat svůj přidělený PIN prostřednictvím uživatelského rozhraní/displeje 34. Tento PIN se pak zpracuje modulem 56 procesoru DTMF kvůli vygenerování odpovídajících tónových signálů, které se přijmou a zpracují na centrálním serveru 60. Přednostně se může PIN zadat sdělením např. „Moje číslo pin je 3456“ do mikrofonu 18, kde se zvukové signály zpracují akustickým procesorovým modulem 16 a pak se vyšlou na centrální server 60 prostřednictvím ustaveného komunikačního spojení L1.

Zatímco uživatel zadává požadovaná ověřovací data, začíná centrální server 60 zpracovávat ověřovací data (krok 108). Konkrétně centrální server 60 provede ověření hovořící osoby a porovná modely hlasu uživatele, které byly zpracovány a sestaveny CPU 12 zařízení 10 PDA s hlasovými záznamy uživatele, které byly uloženy na centrálním serveru 60 během procesu přihlášení. Dále centrální server 60 porovná odpovědi zadané uživatelem s odpověďmi zadanými



během procesu přihlášení kvůli zjištění, zda se shodují. Centrální server 60 může také ověřit, zda PIN zadaný uživatelem odpovídá PIN, které bylo vydané během procesu přihlášení. Pokud po zpracování ověřovacích dat centrální server 60 zjistí, že uživatel není autorizovaný uživatel (krok 110), rozpojí se komunikační spojení L1 a nestáhne se žádný digitální certifikát (krok 106).

Lze ocenit, že v tomto vynálezu lze použít libovolný běžný rozpoznávací systém řeči/hovořící osoby. Tento vynález není žádným způsobem omezen na použití s žádnými detaily ani metodikami, ani závislý na žádných detailech ani metodikách žádného konkrétního systému pro rozpoznávání řeči/hovořící osoby, který lze použít. Přednostně je systém pro rozpoznávání hovořící osoby použitý centrálním serverem 60 a zařízením 10 PDA podle tohoto vynálezu systém, který provádí ověřování hovořící osoby nezávislé na textu a ptá se na náhodné otázky, tj. kombinace rozpoznávání řeči, na textu nezávislé rozpoznávání hovořící osoby a porozumění přirozenému jazyku s použitím akustických a neakustických modelů k zajištění zabezpečení vůči neoprávněnému přístupu ke službě/zařízení (tj. centrální server 60) jak je zveřejněno v U.S. sériové číslo 08/871 784, podaným 11. června 1997 a nazvaným: „Apparatus And Methods For Speaker Verification / Identification / Classification Employing Non-Acoustic And/Or Acoustic Models and Databases“, který je běžně udělen přihlašovatelovi tohoto vynálezu. Podrobněji je na textu nezávislý systém ověřování hovořící osoby přednostně založen na klasifikaci schopnosti rámec-po-rámci jak je podrobně zveřejněno v U.S. sériové číslo 08/788 471 podaném 28. ledna 1997 a nazvaném: „Text Independent Speaker Recognition for Transparent Command Ambiguity Resolution And Continuous Access Control“, který



je běžně udělen tomuto přihlašovateli.

Jak bylo popsáno ve výše uvedeném odkaze U.S. sériové číslo 08/871 784, upřednostňuje se rozpoznávání hovořící osoby nezávisle ne textu před rozpoznáváním hovořící osoby v závislosti na textu nebo s textovou výzvou, protože nezávislost na textu umožňuje provedení funkce rozpoznávání hovořící osoby paralelně s jinými funkcemi založenými na rozpoznávání řeči způsobem srozumitelným pro volajícího. Rozumí se však, že tento vynález může využít ověřování hovořící osoby závislé na textu nebo s textovou výzvou.

Dále lze ocenit, že automatický systém pro rozpoznávání řeči/hovořící osoby zveřejněný v U.S. sériové číslo 08/873 079, podaný 11. června 1997, nazvaný „Portable Acoustic Interface For Remote Access to Automatic Speech/Speaker Recognition Server“, který je běžně udělen tomuto přihlašovateli, lze přednostně použít v tomto vynálezu k zajištění přesné komunikace rozpoznávání řeči při vzdálených transakcích mezi zařízením 10 PDA a centrálním serverem 60.

Zejména jak bylo popsáno ve výše uvedeném U.S. sériové číslo 08/873 079, existují jisté problémy spojené se vzdálenou komunikací mezi systémy server/klient s využitím automatického rozpoznávání řeči/hovořící osoby. Tyto problémy obsahují ztrátu přesnosti dat kvůli znehodnocení hlasových dat, která se přenáší komunikačním kanálem a různé šumy na pozadí na konci uživatele, které snižují přesnost rozpoznávání řeči. Tyto problémy se odstraňují předběžným zpracováním signálů řeči, které se přenášejí komunikačním kanálem na server. Takové předběžné zpracování obsahuje charakterizování akustických znaků vysílajícího zařízení,



prostředí, hovořící osoby a komunikačního kanálu, pomocí něhož jsou tyto informace pak zpracovány centrálním serverem kvůli nastavení referenčních hodnot, zvolení příslušných dekódovacích modelů a algoritmů k rozpoznání hovořící osoby nebo dekódování řeči modelováním přenosové funkce kanálu a šumu na pozadí kvůli snížení chybovosti slov řeči nebo přesnému provádění rozpoznávání hovořící osoby.

Opět s odkazem na obr. 4, pokud bude na druhé straně uživatel ověřen (krok 110), centrální server 60 pak vyzve uživatele k zadání jistých omezení transakcí jako jsou specifické informace o použité finanční kartě, omezení povoleného čerpání během životnosti dočasného digitálního certifikátu a/nebo časové rozmezí, ve kterém zůstane dočasný digitální certifikát platný (krok 112). Tyto informace se přijmou a zpracují centrálním serverem 60 a digitální certifikát se pak vytvoří a zakóduje s požadovanými uživatelskými omezeními (krok 114). Tento digitální certifikát se pak zašifruje centrálním serverem 60 a stáhne do modulu 20 zpracování digitálního certifikátu CPU 12 prostřednictvím ustaveného komunikačního spojení L1 (krok 116). Rozumí se, že tento vynález může používat libovolnou známou techniku šifrování nebo algoritmus k procesu šifrování/dešifrování, jako jsou techniky známé v „Applied Cryptography“ od Bruce Scheniera, druhé vydání, Wiley, 1996. Digitální certifikát se pak uloží do paměti 14 zařízení 10 PDA. S platným digitálním certifikátem může pak uživatel provozovat lokální režim provozu zařízení 10 PDA.

Lze ocenit, že, jak bylo ukázáno výše, může vynález využívat ochranu PIN nebo heslem navíc k nebo místo biometrického ověřování kvůli získání nezbytného digitálního certifikátu od centrálního serveru 60. Dále metody

zveřejněné ve výše uvedeném odkazu U.S. sériové číslo 08/873 079 lze využít v tomto vynálezu ke vzdálenému ověření, obnově nebo novému vyvolání klíče hesla uživatele, přihlašovacího klíče, PIN a/nebo šifrovacího/dešifrovacího klíče, pomocí nějž může uživatel ustavit komunikaci s centrálním serverem 60 (prostřednictvím zařízení 10 PDA) např. kvůli požadavku změny PIN.

Nyní s odkazem na obr. 1, 3 a 5 bude popsán lokální režim provozu podle tohoto vynálezu. Lokální režim provozu je zahájen uživatelem zvolením předem přihlášené kreditní karty, která je uložena v paměti 14 (krok 200). Proces výběru se přednostně provádí hlasem aktivovanými příkazy (např. sdělením do mikrofonu 18 "Chci použít svou kartu American Express"). Tyto hlasové příkazy pak přijme CPU 12 a zpracují se v akustickém procesorovém modulu 16. Lze ocenit, že lze v tomto vynálezu k rozpoznávání řeči použít libovolný známý příkazový a řídicí stroj, jako je komerčně dostupný systém s velkým slovníkem IBM VIAVOICE GOLD k provádění funkcí rozpoznávání řeči podle tohoto vynálezu.

Eventuálně lze požadovanou kartu zvolit prostřednictvím uživatelského rozhraní/displeje 34. CPU 12 pak hledá v paměti 14 požadované informace (krok 202). Pokud nebyla karta předtím uložena v zařízení 10 PDA během procesu přihlášení, bude uživatel vyzván ke zvolení jiné karty (krok 204).

Pokud se informace o požadované kartě naleznou v paměti, musí se provést biometrické ověření předtím, nežli se smí informace o kartě zapsat do univerzální karty 26. Eventuálně, jak bylo uvedeno výše, může se provést ověření pomocí PIN nebo hesla místo nebo navíc k biometrickému



ověřování. V upřednostňovaném provedení tohoto vynálezu se používají hlasem aktivované příkazy ke zvolení požadované karty, funkce mikrofonu 18 jako biometrického senzoru pro příjem biometrických hlasových dat. Tato biometrická hlasová data se pak posílají do akustického procesorového modulu 16, kde se tato data zpracují (krok 206) porovnáním aktuálních biometrických hlasových dat s hlasovými modely uživatele uloženými v paměti 14.

Přestože takové ověření lze provést libovolným běžným způsobem, způsoby ověřování hovořící osoby zveřejněné ve výše uvedených odkazech na aplikace, U.S. sériová čísla 08/871 784 a 08/788 471 jsou přednostně využity v tomto vynálezu.

V dalším provedení tohoto vynálezu lze použít biometrický senzor 40 libovolného známého typu místo nebo spolu s mikrofonom ke sběru biometrických dat, která se mají zpracovat modulem 22 biometrického procesoru s použitím známých technik, např. dat otisku prstu, palce nebo dlaně, dat rukopisu, dat vzoru cév sítnice nebo jejich kombinací. V dalším provedení tohoto vynálezu lze opět využít ověření pomocí PIN nebo hesla místo nebo navíc k těmto biometrickým ověřovacím technikám.

Poté co jsou biometrická data zpracována akustickým procesorovým modulem 16 (při využití ověření hlasu) nebo biometrickým procesorovým modulem 22 (při použití jiných metod biometrického ověřování), nebo oběma, provede se zjištění toho, zda je uživatel oprávněný uživatel (krok 208). Pokud není uživatel ověřený, zvolené informace o kartě se nezapiší do univerzální karty 26 (krok 210). Pokud uživatel je ověřen, získá se digitální certifikát (předtím

získaný v režimu klient/server) z paměti 14 a zavede se do modulu 20 procesoru digitálního certifikátu. Modul 20 procesoru digitálního certifikátu zpracuje digitální certifikát, aby zjistil, zda je digitální certifikát stále ještě platný (tj. nevypršel) a zda bylo použití zvolené karty zakázáno nebo omezeno uživatelem požadovanými omezeními této karty během režimu klient/server (krok 212). Pokud není digitální certifikát platný, (tj. vypršel), nezapiší se zvolené informace o kartě na univerzální kartu 26 (krok 210).

Pokud je digitální certifikát platný (tj. nevypršel), informace o požadované kartě se pak získají z paměti 14 a uloží se do šifrovacího/dešifrovacího modulu 24. Informace o zvolené kartě se pak dešifrují šifrovacím/dešifrovacím modulem 24 s použitím šifrovacího klíče jedinečného pro zařízení 10 PDA (krok 214). Dešifrované informace o kartě se pak pošlou do zapisovacího/čtecího zařízení 30 karet smartcard, kde se pak zapiší do univerzální karty 26 (krok 216). Univerzální karta 26 se pak odstraní ze zapisovacího/čtecího zařízení 30 karet smartcard a protáhne se magnetickým čtecím zařízením transakčního terminálu 80 (obr. 3) (krok 218). Informace o transakci spotřebitele se pak odešlou příslušné finanční instituci 70 prostřednictvím komunikačního spojení L4 (krok 220).

Ve zdokonaleném transakčním terminálu 80 může být univerzální karta 26 přepsána potvrzením transakce transakčním terminálem POS nebo ATM transakčním terminálem 80 (krok 222). Pomocí této funkce může uživatel udržovat účetnictví svých transakcí vložení univerzální karty 26 do čtecího/zapisovacího zařízení 30 karet smartcard a pak stáhnout informace o potvrzení do paměti 14

zařízení 10 PDA (krok 224). Uživatel může následně přenášet tyto informace do osobního počítače obsahujícího účtovací software jako je software prodáváný pod obchodní značkou QUICKEN.

S výhodou lze tento vynález okamžitě využít se současnou infrastrukturou, protože univerzální karta 26 je slučitelná se všemi systémy pro přenos elektronických financí kreditními kartami a/nebo kartami smartcard (např. systémy, které zpracovávají ATM karty, debetní karty, kreditní karty, karty pro řízení přístupu, telefonní karty a/nebo služební průkazy).

Lze ocenit, že tento vynález lze použít k ukládání osobních informací a k přístupu k osobním informacím jako například zdravotním, finančním informacím a jiným důvěrným informacím, ke kterým lze přistupovat a které lze zapisovat na univerzální kartu 26 nebo lze zobrazovat na uživatelském rozhraní/displeji 34 (za předpokladu platného digitálního certifikátu a lokálního ověření uživatele). Například lékaři se speciálními kartami smartcard mohou přistupovat k jistým lékařským informacím ze zařízení PDA pacienta (po ověření pacienta) zapsáním těchto informací do karty smartcard prostřednictvím čtecího/zapisovacího zařízení karet smartcard zařízení 10 PDA. Eventuálně lze tyto informace přenášet bezdrátovou komunikací mezi zařízením PDA pacienta a zařízením PDA doktora.

Dále lze ocenit, že vynález může komunikovat s elektronickými přenosovými systémy financí nebo transakčními terminály, které mají schopnost bezdrátové nebo přímé komunikace, aniž by dokonce musely používat univerzální kartu 26. Podrobně, jak bylo ukázáno tečkovanými

čarami na obr. 5, lze transakci spotřebitele provést vysláním informací o zvolené kartě přímo ze zařízení PDA do transakčního terminálu ATM nebo POS prostřednictvím ustaveného komunikačního spojení L2 (krok 228, obr. 3) (tj. prostřednictvím sériového portu 42, modemu 42 paralelního portu 44, IR portu 54 nebo VF portu 50), spíše nežli získání a zápisu informací o kartě do univerzální karty 26. Dále potvrzení o transakci se může přímo přenést do zařízení 10 PDA prostřednictvím komunikačního spojení L2 (krok 230). Rozumí se, že v tomto provedení zamezí CPU 12 zařízení 10 PDA v získání a odeslání na transakční terminál 80 informací o zvolené kartě, pokud uživatel není biometricky ověřen a/nebo pokud není digitální certifikát platný (krok 226). V tomto konkrétním provedení tohoto vynálezu samo zařízení 10 PDA vlastně přebírá místo univerzální karty 26 a proto tedy odstraňuje potřebu nutnosti nejdříve zapsat informace o zvolené kartě do univerzální karty 26 a pak protáhnout univerzální kartu 26 magnetickým čtecím zařízením transakčního terminálu POS nebo ATM.

Tento vynález s výhodou zajišťuje biometrické zabezpečení pro transakce, které neobsahují přenos elektronických dat, jako jsou transakce, které se zpracovávají tradičními mechanickými čtecími zařízeními pro kreditní karty, nebo transakce, které se provádí vzdáleně telefonicky. V takových situacích může prodejce potvrdit, že uživatel předal lokální ověření použitím jedinečného čísla 27 univerzální karty (obr. 2) spolu s autorizačním číslem, které je založeno na aktuálním platném digitálním certifikátu a generováno po ověření uživatele.

Vysvětlením na příkladu s odkazem na obr. 6 je ukázáno

blokové schéma znázorňující lokální režim zařízení 10 PDA během vzdálené (nebo mechanického čtecího zařízení) uživatelské transakce. Při práci zařízení 10 PDA v lokálním režimu, pokud je uživatel biometricky ověřen (krok 308) a zařízení 10 PDA obsahuje platný digitální certifikát (krok 310), se získají informace o zvolené kartě z paměti 14 a zašifrují se (krok 314). Informace o požadované kreditní kartě stejně jako autorizační číslo se pak zobrazí na uživatelském rozhraní/displeji 34 (krok 316). Tyto informace lze pak verbálně sdělit prodejci kvůli zpracování transakce. Pokud uživatel není biometricky ověřen nebo pokud zařízení 10 PDA obsahuje neplatný digitální certifikát, nezobrazí se informace o zvolené kartě, ani autorizační číslo. (krok 312).

Prodejce může ověřit, že lokální ověření uživatele bylo správně získáno ustavením komunikačního spojení L3 (obr. 3) s centrálním serverem 60. Pokud informace o zvolené kartě odpovídají kreditní kartě, která byla předtím přihlášená, (tj. registrována) u poskytovatele služby zařízení 10 PDA a univerzální karty 26, po vyslání informací o zvolené kartě finanční instituci (nebo zavolání této instituce kvůli potvrzení platnosti kreditní karty), bude se po obchodníkovi požadovat zadání autorizačního čísla (které se generuje po ověření uživatele) kromě data vypršení kreditní karty. Obchodník pak vyšle číslo 27 univerzální karty a zobrazené autorizační číslo na centrální server 60. Protože autorizační číslo je funkcí platného digitálního certifikátu, který byl získán z centrálního serveru 60 v režimu klient/server, informuje centrální server 60 obchodníka o tom, že byl uživatel správně ověřen (krok 318).

Lze ocenit, že lokální ověření se také může provést

ověřením podpisu, kde se digitalizovaný obraz platného podpisu uživatele zobrazí na rozhraní/displeji 34 uživatele s použitím známých technik, takže obchodník může porovnat digitalizovaný podpis na obrazovce se zapsaným podpisem uživatele kvůli zajištění dalšího ověření. Dále tento vynález může využívat libovolný běžný displej citlivý na dotyk, kdy uživatel zařízení 10 PDA může napsat svůj podpis na displej, který se pak zpracuje a porovná s autentickým digitalizovaným podpisem uloženým v paměti 14 zařízení 10 PDA. Příklad takové techniky je zveřejněn například v publikaci „Automatic On-Line Signature Verification“ od Vic Nalwa, Proc. IEEE, str. 215-239, únor 1997.

Dále lze ocenit, že zařízení 10 PDA a systém podle tohoto vynálezu, lze nakonfigurovat tak, aby se umožnila další úroveň zabezpečení pro ověření uživatele, kdy finanční instituce (např. společnost vydávající kreditní karty) může ověřit totožnost spotřebitele během nákupní transakce. Podrobně během spotřebitelské transakce po lokálním ověření (biometrickém, pomocí PIN a/nebo heslem) a samozřejmě za předpokladu, že byl předtím platný digitální certifikát stažen z centrálního serveru 60, může být PDA zařízení 10 naprogramováno ke stažení informací o zvolené kartě v zašifrované podobě do univerzální karty 26 a také zašifrovaného souboru obsahujícího informace o jedinečné identifikaci týkající se spotřebitele obsahující, ale bez omezení na, například jméno spotřebitele a číslo účtu (vydané poskytovatelem služby zařízení 10 PDA a univerzální karty 26). Informace o zvolené kartě a také zašifrovaný soubor s informacemi by se přenesly na POS terminál (prostřednictvím univerzální karty, VF nebo IR) a pak by se přenesly v zašifrované podobě přímo do zpracovávající finanční instituce spolu s podrobnostmi o koupi.

Podobně u nákupních transakcích se vzdálenými službami (např. prostřednictvím internetu s webovským místem prodejce), by se informace o zvolené kartě zašifrované podobě stejně jako zašifrované informace o uživateli, přenesly prostřednictvím modemu (TCP/IP) na vzdálenou službu (tj. místo na webu) a pak přenesly v zašifrovaném tvaru do finanční instituce. Lze ocenit, že zašifrované informace se mohou přenášet na webovské místo obchodníka buďto přímo z modemu 58 zařízení 10 PDA, nebo stažením těchto informací do univerzální karty 26, které se pak přečtou a přenesou z PC vybaveného čtecím zařízením karet smartcard a modemem.

Dále, za předpokladu, že kreditní karta byla předtím přihlášená u poskytovatele služby, by zpracovávající finanční instituce vlastnila nutný klíč (dodaný poskytovatelem služby po přihlášení) k dekodování (tj. dešifrování) vyslaných informací kvůli ověření totožnosti uživatele. Dále zpracovávající finanční instituce by dodala autorizační číslo pro transakci obchodníkovi pokud byl spotřebitel ověřen nebo na druhé straně odepřela transakci a informovala obchodníka pokud není spotřebitel oprávněn použít zvolenou kartu. Eventuálně lze zařízení 10 PDA naprogramovat ke stažení kopie platného dočasného digitálního certifikátu v zašifrované podobě (stejně jako informací o zvolené kartě v zašifrované podobě) do univerzální karty 26, pomocí které by se digitální certifikát obsahující nutné informace k identifikaci uživatele vyslal (s informacemi o zvolené kartě) odpovídající finanční instituci.

Tento vynález byl tudíž znázorněn jako oddělené přenosné zařízení. Odborníkům je jasné, že konfiguraci

tohoto vynálezu lze začlenit do systémů založených na jiných CPU, jako je celulární telefon, přenosný laptop, síťový počítač (NC) nebo PC s vestavěnými komponenty výše popsaného zařízení 10 PDA. Například přenosný laptop, který má čtecí/zapísovací zařízení 30 karet smartcard zařízení 10 PDA může být přímo připojen k centrálnímu serveru 60 prostřednictvím modemu nebo prostřednictvím internetového serveru protokoly jako například TCP/IP ke stažení platného digitálního certifikátu.

Dále funkce a komponenty zařízení 10 PDA mohou být vestavěny do celulárního telefonu, kdy komunikace s centrálním serverem 60 lze dosáhnout prostřednictvím celulárního komunikačního kanálu, který může být analogový nebo digitální (např. CDMA, GSM, atd.).

Odborníci také ocení, že lze využít speciální ATM, kiosky nebo POS terminál k provedení metod a funkcí tohoto vynálezu místo aktuálního zařízení PDA a tím odstranit potřebu fyzicky vlastnit zařízení 10 PDA. Například karta smartcard, která má platný digitální certifikát a ověřovací data uživatele (např. biometrická data (hlasový záznam), PIN a/nebo heslo) a informace o kartě v sobě uložené, se může vložit do ATM, kiosku nebo POS terminálu, který může být vybaven biometrickými senzory jako je mikrofon. ATM může pak ověřit uživatele biometricky nebo prostřednictvím PIN nebo hesla. Za předpokladu, že je digitální certifikát platný, může ATM inicializovat kartu smartcard, která se pak může použít k provedení například kupní transakce. Kartu smartcard lze pak použít po dobu platnosti digitálního certifikátu (tj. dokud digitální certifikát nevyprší) nebo dokud se nezavede jiná karta. V tomto provedení lze použít kartu smartcard pouze pro omezené množství transakcí.



Digitální certifikát lze stáhnout do karty smartcard libovolným způsobem analogickým s technikami údržby PIN zveřejněným ve výše uvedeném U.S. sériové číslo 08/873 079 „Portable Acoustic Interface For Remote Access to Automatic Speech/Speaker Recognition Server“. Uživatel může například ustavit komunikační spojení s poskytovatelem služby centrálního serveru 60 prostřednictvím osobního počítače, který má čtecí zařízení karet smartcard, pomocí něhož lze stáhnout platný digitální certifikát na kartu smartcard poté co uživatel zadá informace o ověření jako jsou ID uživatele, PIN, sériové číslo karty smartcard a/nebo biometrická data.

Dále lze ocenit, že zařízení 10 PDA podle tohoto vynálezu lze použít jako osobní centrum kreditních karet, kde lze přesouvat finance přímo mezi jednotlivci, kteří mají taková zařízení PDA prostřednictvím kreditních karet nebo debetních karet. Například předpokládejme, že uživatel A dluží uživateli B jistou částku peněz. Uživatel A provede lokální ověření (za předpokladu, že uživatel A má platný digitální certifikát) aby stáhnul informace o zvolené kreditní kartě nebo debetní kartě do univerzální karty uživatele A. Uživatel A pak dodá uživateli B univerzální kartu, která se pak vloží do čtecího/zápisového zařízení 30 karet smartcard zařízení 10 PDA uživatele B. Uživatel B pak zvolí částku peněz, která se má přenést (tj. debitovat) z univerzální karty (tj. zvolené kreditní karty) na libovolný z přihlášených finančních účtů uživatele B (např. účty kreditních karet). Uživatel B pak získá autorizační číslo vytvořené zařízením PDA uživatele A po lokálním ověření a zadá toto číslo do zařízení PDA uživatele B. Výše uvedená procedura se samozřejmě může provést přímo (např. prostřednictvím IR komunikace) místo fyzické výměny

univerzální karty.

Aby se zabránilo podvodným transakcím, autorizační číslo vytvořené zařízením PDA uživatele A se musí zadat do zařízení PDA uživatele B po zadání částky transakce do zařízení PDA uživatele B a ověření uživatelem A. Jinými slovy, zařízení PDA uživatele B musí být nakonfigurováno tak, aby autorizační číslo od uživatele A nebylo přijato zařízením PDA uživatele B, dokud se nejdříve nezadá částka transakce do zařízení PDA uživatele B. Dále PDA zařízení uživatele B se musí nakonfigurovat tak, aby autorizační číslo uživatele A zadané do zařízení PDA uživatele B bylo platné pouze pro jednu transakci (tj. jednu částku peněz zadanou do zařízení PDA uživatele B), proto celý proces musí následně opakovat pro každou další transakci mezi uživatelem A a uživatelem B. Eventuálně, aby se zabránilo podvodu, lze nakonfigurovat zařízení PDA uživatele A tak, aby autorizační číslo vytvořené zařízením PDA uživatele A obsahovalo částku peněz, která se má přenést na účet uživatele B v zašifrované nebo jinak skryté podobě tak, aby uživatel B nemohl přistupovat k této částce a manipulovat s touto částkou.

Po zadání autorizačního čísla uživatele A ustaví uživatel B komunikační spojení s poskytovatelem služby kvůli ověření toho, zda autorizační číslo odpovídá jedinečnému číslu univerzální karty uživatele A a pak přesune finance na zvolený účet uživatele B (za předpokladu, že je účet registrován u poskytovatele služby).

Odborník může předvídat různé způsoby implementace tohoto vynálezu pro komunikaci informací o zvolené kartě. Již brzy se například budou moci sdělovat informace mezi

jednotlivci a systémy prostřednictvím osobních oblastních sítí (PAN), které spojují speciální elektronická zařízení, které mají vysílač/přijímač a CPU nesený jednotlivci s využitím vodivosti člověka. Takovou představu lze využít v tomto vynálezu, pomocí ní se informace o zvolené kartě budou přenášet po kontaktu lidí (např. podáním ruky) a nikoli přenášet magneticky ani kartami smartcard ani bezdrátovou komunikací. Podrobně lze tento vynález začlenit do CPU zařízení PAN, pomocí něž lze přenášet informace o zvolené kartě do přijímacích zařízení jako jsou ATM a POS terminály, které jsou vybavené nutným softwarem a hardwarem, který podporuje výměnu PAN dat.

Zastupuje:

Dr. Petr Kalenský v.r.



SPOLČNÁ ADVOKÁTNÍ KANCELÁŘ
VŠETECKA ZELENÝ ŠVORČIK KALENSKÝ
A PARTNEŘI
120 00 Praha 2, Hájkova 2
Česká republika

PATENTOVÉ NÁROKY

1. Přenosné zařízení (10) zpracovávající informace a transakce, **vyznačující se tím**, že obsahuje:

centrální procesorovou jednotku (12) pro řízení funkce a pro zpracování více operací zařízení (10) zpracovávajícího informace a transakce;

paměť (14), operativně připojenou k centrální procesorové jednotce (12) k ukládání finančních a osobních informací a k ukládání dočasného digitálního certifikátu;

komunikační prostředky, operativně připojené k centrální procesorové jednotce (12) k ustavení komunikačního spojení (L1) s centrálním serverem (60), umístěným ve vzdáleném místě, kvůli získání dočasného digitálního certifikátu;

uživatelské rozhraní (34), operativně připojené k centrální procesorové jednotce (12) pro zahájení alespoň jedné z více operací zařízení (10) zpracovávajícího informace a transakce a zvolení části buď z finančních nebo osobních informací z paměti (14);

univerzální kartu (26), oddělitelně připojenou k centrální procesorové jednotce (12) pro získání zvolené části buď z finančních nebo osobních informací; a

programové prostředky, operativně připojené k centrální procesorové jednotce (12) a reagující na dočasný digitální



certifikát pro zápis zvolené části z uložených, ⁽²⁶⁾ buď finančních nebo osobních informací do univerzální karty, kdy je prostředkům programu zabráněno v zápise zvolené části buď z finančních nebo osobních informací do univerzální karty (26) pokud je dočasný digitální certifikát neplatný.

2. Zařízení (10) zpracovávající informace a transakce podle nároku 1, **vyznačující se tím**, že dále obsahuje ověřovací prostředky, operativně připojené k centrální procesorové jednotce (12) pro ověřování oprávněného uživatele a pro zabránění programovým prostředkům v zápise zvolené části buď z finančních nebo osobních informací do univerzální karty, ⁽²⁶⁾ dokud nejsou dodána ověřovací data oprávněným uživatelem zařízení.

3. Zařízení (10) zpracovávající informace a transakce podle nároku 2, **vyznačující se tím**, že ověřovací prostředky obsahují biometrické ověřovací prostředky a ověřovací data jsou biometrická data.

4. Zařízení (10) zpracovávající informace a transakce podle nároku 3, **vyznačující se tím**, že biometrické ověřovací prostředky obsahují: biometrické senzorové prostředky (40) pro shromažďování biometrických dat; a biometrické procesorové prostředky (22) ke zpracovávání biometrických dat kvůli zjištění toho, zda biometrická data jsou dodána oprávněným uživatelem.

5. Zařízení (10) zpracovávající informace a transakce podle nároku 3, **vyznačující se tím**, že biometrická data jsou odvozena z jednoho z otisku prstu, palce nebo dlaně, vzorku hlasu, vzoru rukopisu a struktury cévního zásobení sítnice a jejich kombinace.



6. Zařízení (10) zpracovávající informace a transakce podle nároku 4, **vyznačující se tím**, že biometrické ověřovací prostředky provádí ověřování hovořící osoby a biometrická data jsou hlasová data.

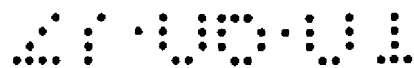
7. Zařízení (10) zpracovávající informace a transakce podle nároku 6, **vyznačující se tím**, že ověření hovořící osoby je ověření hovořící osoby nezávislé na textu.

8. Zařízení (10) zpracovávající informace a transakce podle nároku 1, **vyznačující se tím**, že dále obsahuje šifrovací/dešifrovací prostředky (24), operativně připojené k centrální procesorové jednotce (12) pro zašifrování osobních a finančních informací před uložením informací do paměti (14) a pro zašifrování zvolené části buď z uložených finančních nebo osobních informací.

9. Zařízení (10) zpracovávající informace a transakce podle nároku 1, **vyznačující se tím**, že dále obsahuje prostředky rozpoznávání řeči, operativně připojené k centrální procesorové jednotce (12) pro zpracování hlasových příkazů od oprávněného uživatele zařízení.

10. Zařízení (10) zpracovávající informace a transakce podle nároku 9, **vyznačující se tím**, že prostředky pro rozpoznávání řeči obsahují mikrofon (18) pro příjem zvukových hlasových signálů a převod zvukových hlasových signálů na elektrické signály, a akustické procesorové prostředky (16), operativně připojené k mikrofonu pro zpracování hlasových příkazů.

11. Systém zpracovávající informace a transakce,



vyznačující se tím, že obsahuje:

přenosné zařízení (10) zpracovávající informace a transakce, které má:

centrální procesorovou jednotku (12) pro řízení funkce a pro zpracování více operací zařízení;

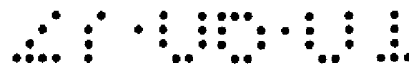
paměť (14), operativně připojenou k centrální procesorové jednotce (12) pro uložení finančních a osobních informací a pro uložení dočasného digitálního certifikátu;

ověřovací prostředky, operativně připojené k centrální procesorové jednotce (12) pro příjem a zpracování ověřovacích dat od oprávněného uživatele kvůli ověření oprávněného uživatele;

komunikační prostředky, operativně připojené k centrální procesorové jednotce (12) pro vysílání a příjem dat komunikačním kanálem;

uživatelské rozhraní (34), operativně připojené k centrálním procesorovým prostředkům (12) pro zahájení alespoň jedné z více operací zařízení (10) zpracovávající informace a transakce a zvolení části buď z finančních nebo osobních informací z paměti;

prostředky reagující na dočasný digitální certifikát, tvořené zejména modulem (20) procesoru digitálního certifikátu a modulem (22) biometrického procesoru, pro přenos zvolené části buď z finančních nebo osobních informací do periferního systému pro zahájení transakce; a



centrální server (60), vzdáleně připojený ke komunikačnímu kanálu pro generování digitálního certifikátu, přičemž digitální certifikát se přenáší do přenosného zařízení (10) zpracovávající informace a transakce zpracovávajícího informace a transakce komunikačním kanálem a ukládá se do paměti (14) zařízení.

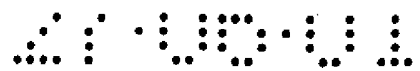
12. Systém podle nároku 11, **vyznačující se tím**, že centrální server (60) obsahuje prostředky pro zpracovávání ověřovacích dat přenášených z přenosného zařízení kvůli ověření oprávněného uživatele, kde se digitální certifikát přenesse do přenosného zařízení (10) zpracovávající informace a transakce pokud je oprávněný uživatel ověřen.

13. Způsob provádění elektronické datové přenosové transakce v přenosném systému zpracovávajícím informace a transakce, který má režim provozu klient/server a lokální režim provozu, **vyznačující se tím**, že způsob obsahuje kroky:

práce v režimu provozu klient/server kvůli získání dočasného digitálního certifikátu, přičemž režim klient/server obsahuje kroky:

připojení k centrálnímu serveru (60) komunikačním kanálem z přenosného zařízení (10) zpracovávajícího informace a transakce, umístěného vzdáleně od centrálního serveru (60), přičemž centrální server (60) má ověřovací data oprávněného uživatele uložená v paměti (14);

vložení ověřovacích dat do přenosného zařízení (10) zpracovávající informace a transakce;



přenos vložených ověřovacích dat komunikačním kanálem na centrální server (60);

zpracování ověřovacích dat poskytnutých na centrální server (60) s použitím uložených ověřovacích dat oprávněného uživatele kvůli ověření uživatele; a

přenos dočasného digitálního certifikátu komunikačním spojením (L1) pokud je oprávněný uživatel ověřen po zpracování přenesených ověřovacích dat; a

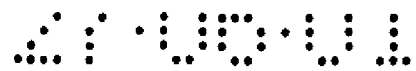
práce v lokálním režimu provozu, kde lokální režim provozu obsahuje kroky:

dodání ověřovacích dat oprávněného uživatele systému;

zpracování ověřovacích dat kvůli ověření oprávněného uživatele;

zjištění toho, zda je dočasný digitální certifikát platný;

zvolení alespoň části buď z osobních nebo finančních informací; a

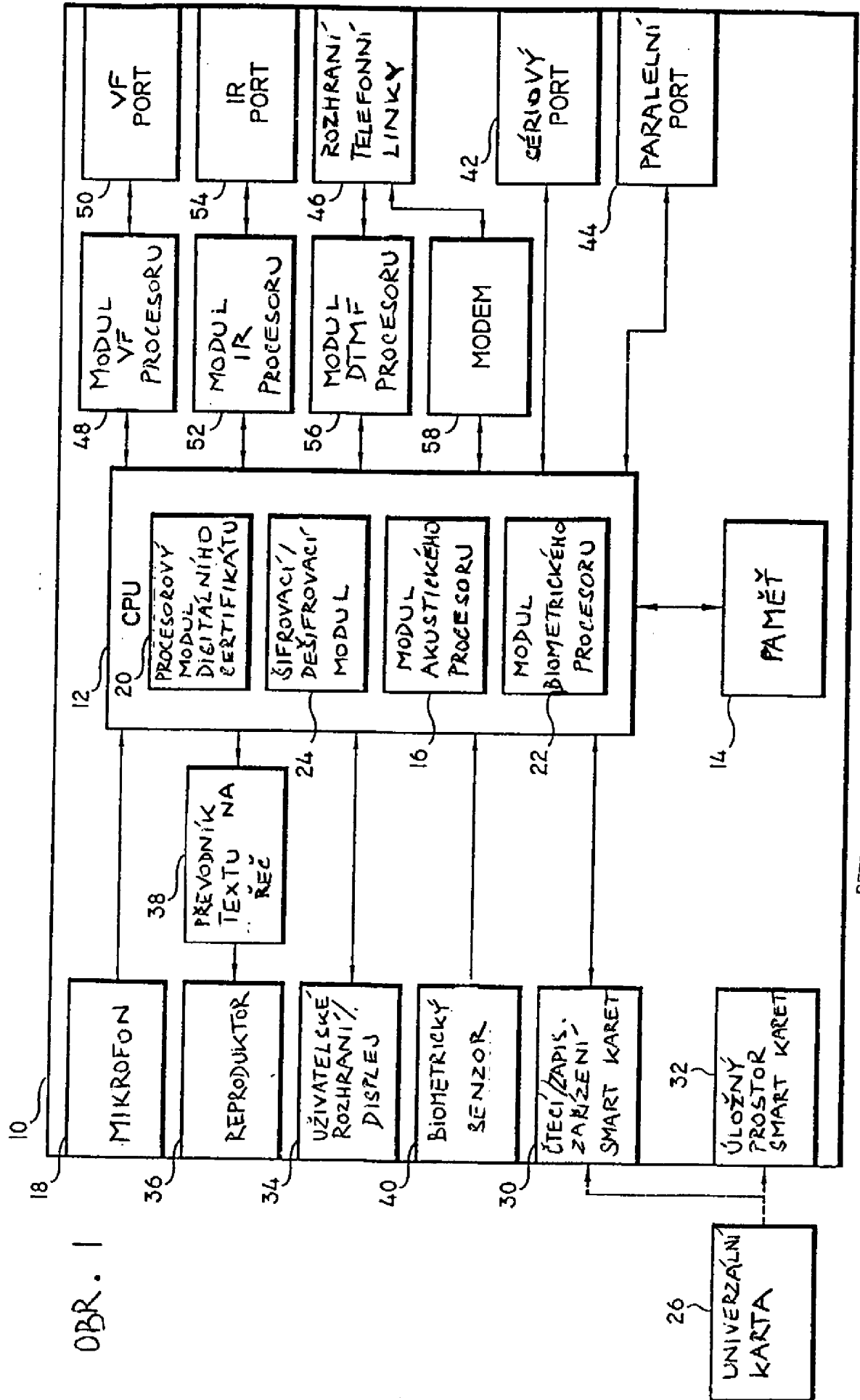


přenos zvolené části buď z osobních nebo finančních informací na externí systém pokud je oprávněný uživatel ověřený a zjistí se, že dočasný digitální certifikát je platný.

Zastupuje:

Dr. Petr Kalenský v.r.

A handwritten signature in black ink, appearing to be 'Petr Kalenský', written over a faint, illegible printed name.



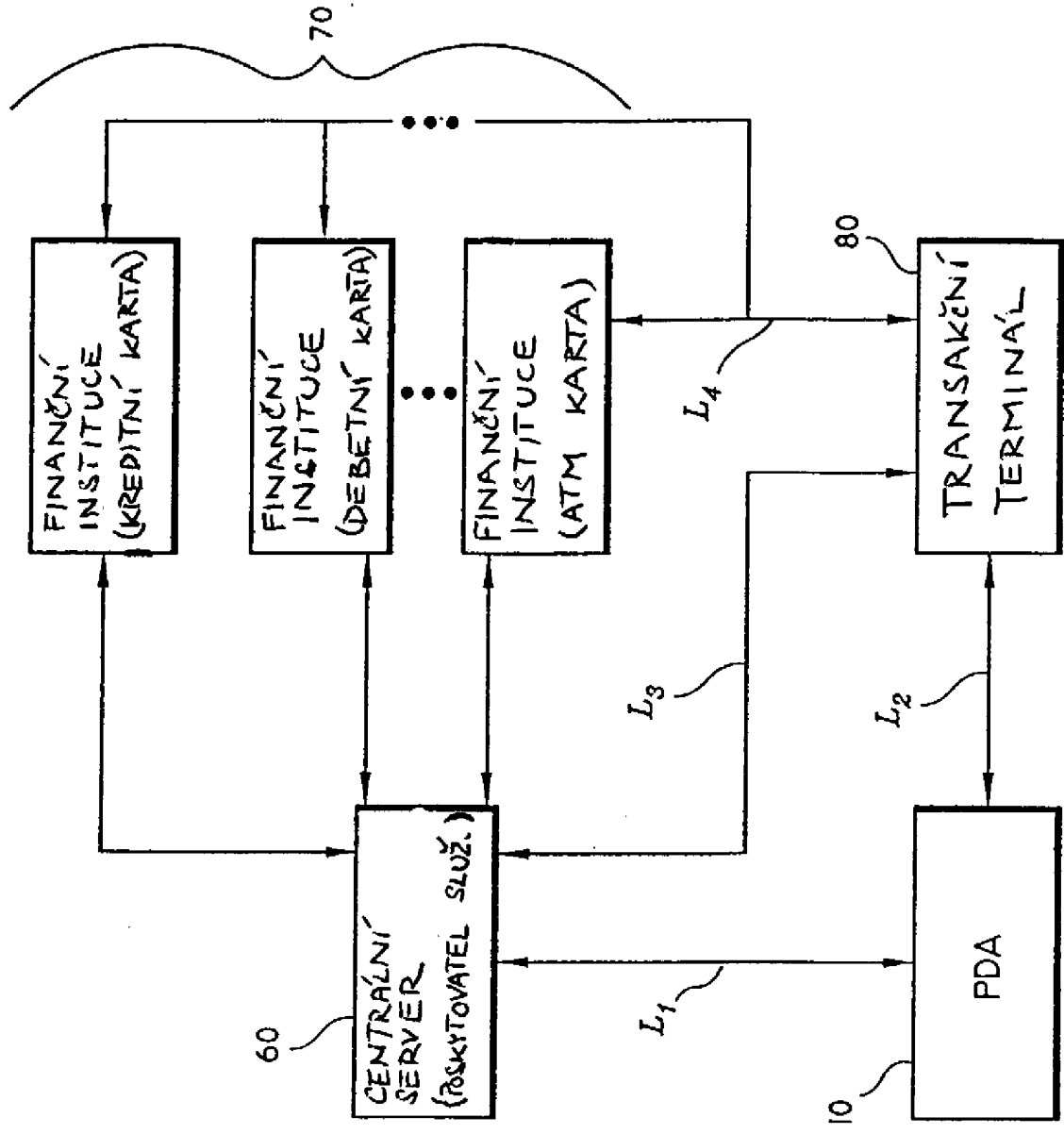
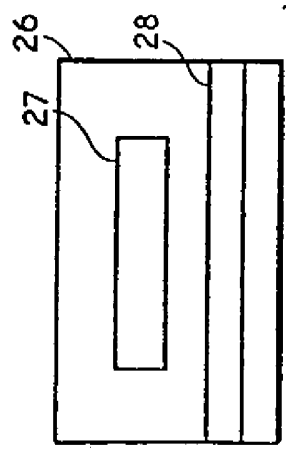
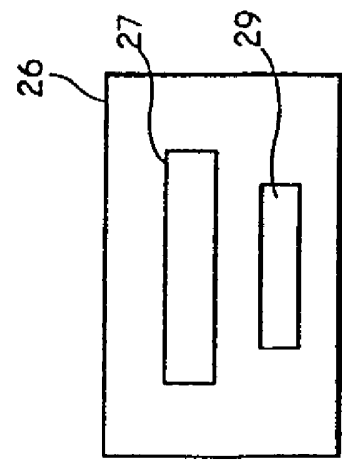


FIG. 3

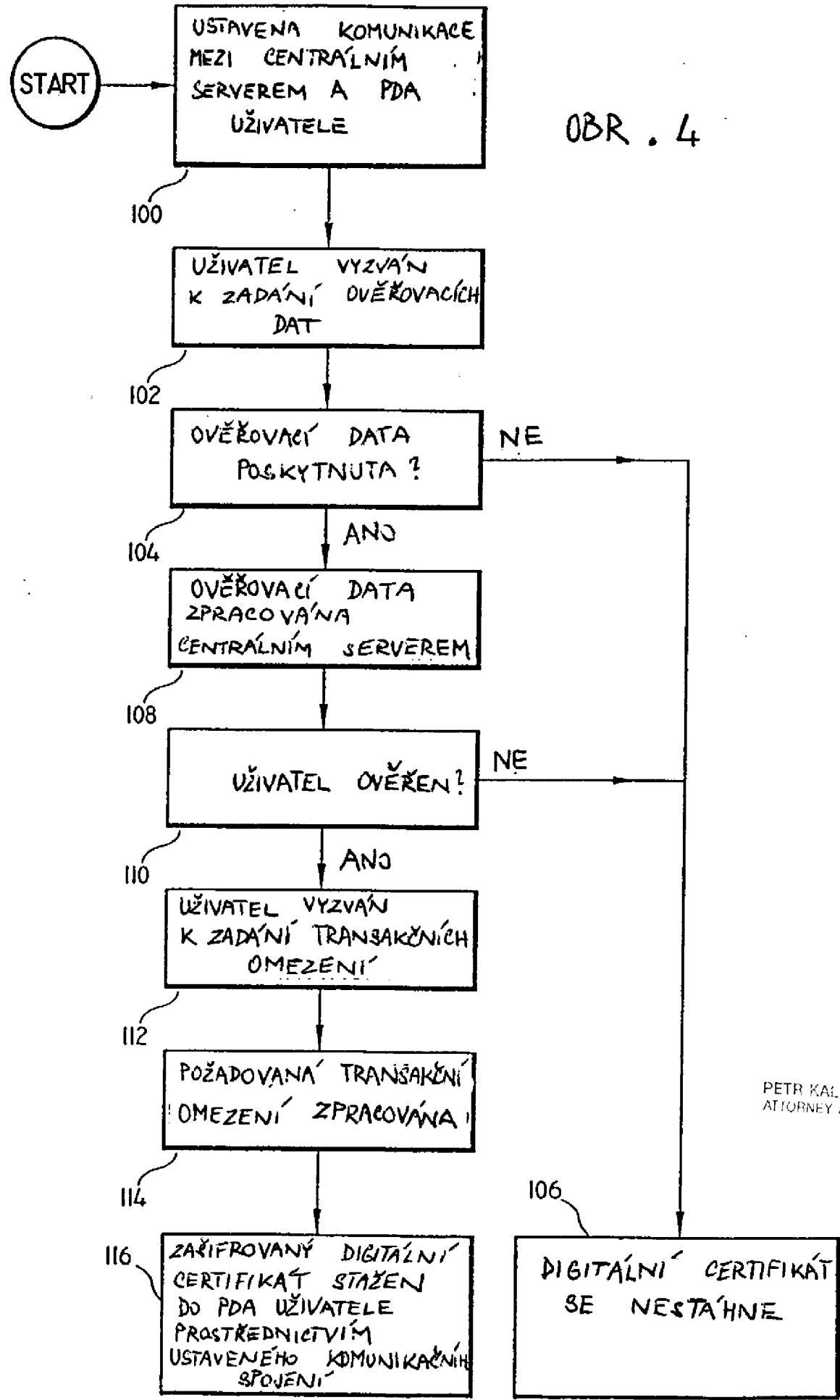


(a)



(b)

OBŘ. 2

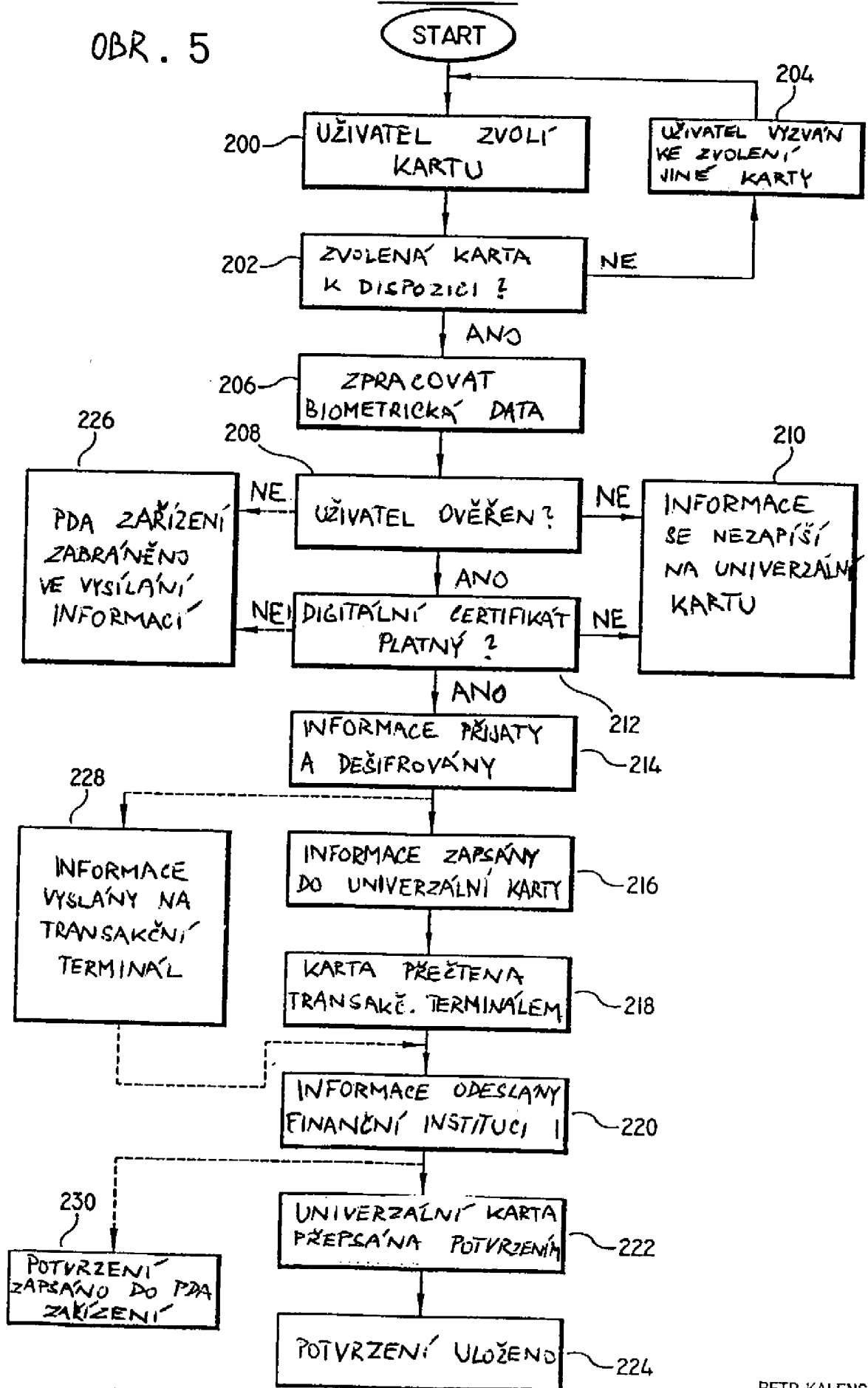


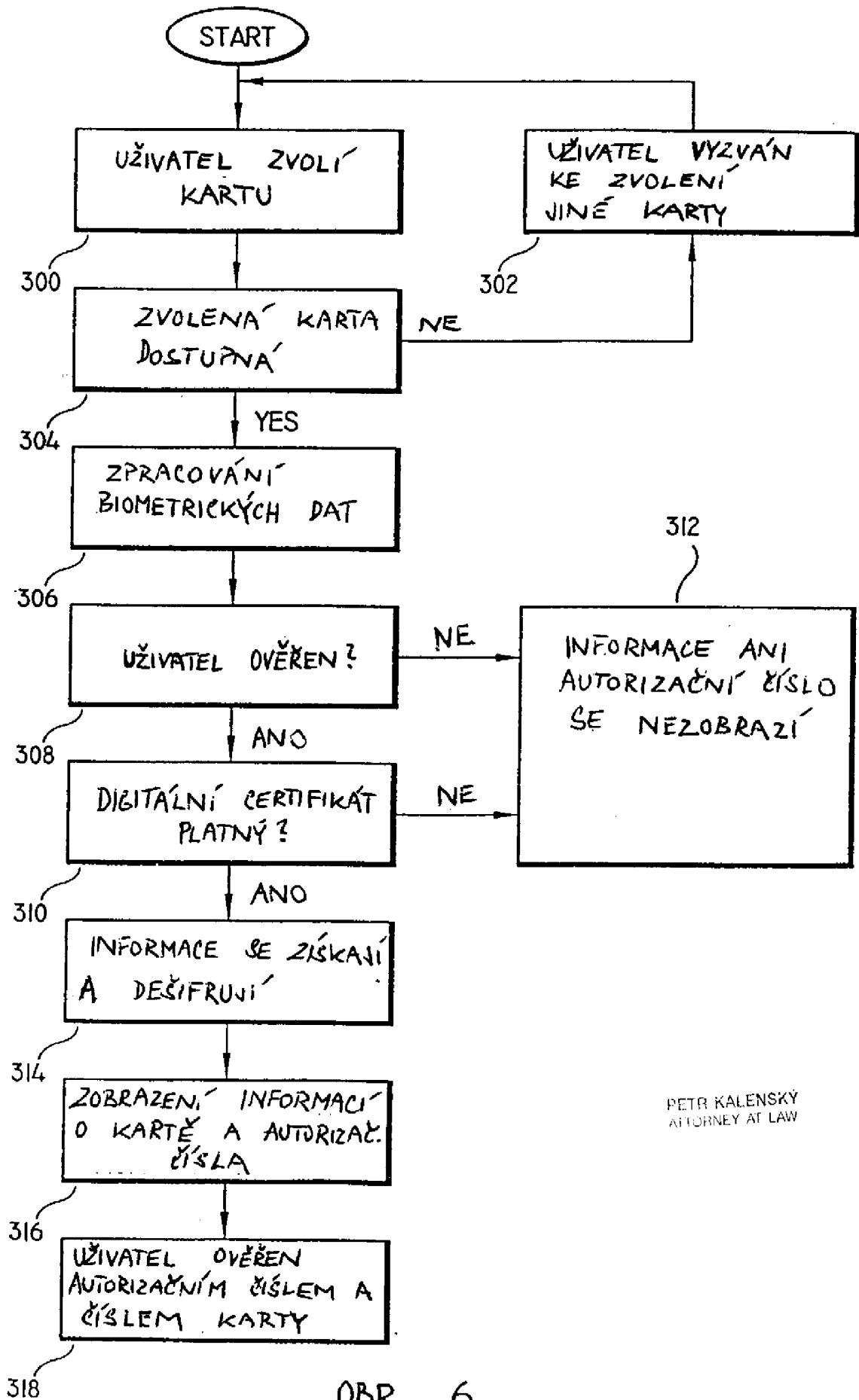
OBR. 4

PETR KALENSKY
ATTORNEY AT LAW

LOKÁLNÍ REŽIM

OBR. 5





PETR KALENSKÝ
ATTORNEY AT LAW

OBR. 6