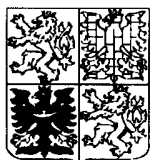


PŘIHLÁŠKA VYNÁLEZU

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

(19)

ČESKÁ
REPUBLIKA



ÚŘAD
PRŮMYSLOVÉHO
VLASTNICTVÍ

(22) Přihlášeno: **19. 04. 96**

(32) Datum podání prioritní přihlášky: **21.04.95**

(31) Číslo prioritní přihlášky: **95/427287**

(33) Země priority: **US**

(40) Datum zveřejnění přihlášky vynálezu: **16. 09. 98**
(Věstník č. 9/98)

(86) PCT číslo: **PCT/US96/05521**

(87) PCT číslo zveřejnění: **WO 96/33476**

(21) Číslo dokumentu:

3323-97

(13) Druh dokumentu: **A3**

(51) Int. Cl.⁶:

G 07 F 7/08
G 06 F 17/60

(71) Přihlášovatel:

CITIBANK, N. A., New York, NY, US;

(72) Původce:

Rosen Sholom S., New York, NY, US;

(74) Zástupce:

PATENTSERVIS PRAHA a.s., Jivenská 1273,
Praha 4, 14021;

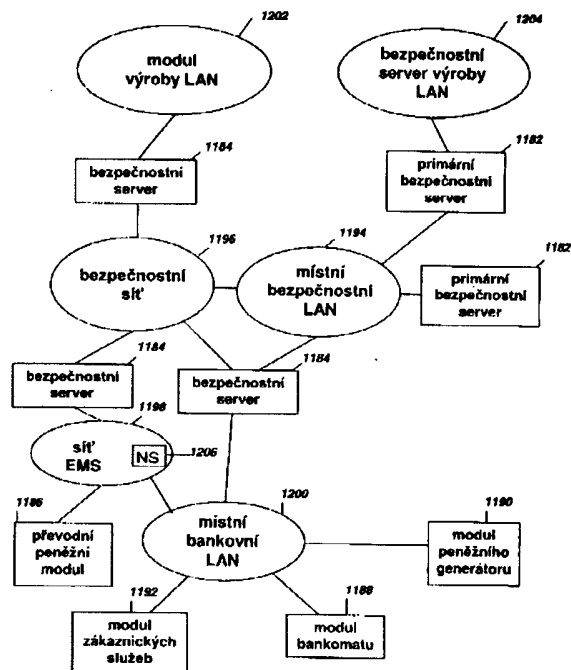
(54) Název přihlášky vynálezu:

Elektronický peněžní systém

(57) Anotace:

Elektronický monetární systém zahrnuje banku /1/ nebo finanční instituce, které jsou spojeny se zařízením na generaci peněz pro tvorbu a vydávání elektronických peněz včetně elektronické hotovosti, která je podle požadavku zálohována vklady a elektronickými úvěrovými oprávněními. Systém dále zahrnuje odpovídající banky /2/, které přijímají a distribuují elektronické peníze /3/ řadou převodních zařízení, která jsou používána klienty pro ukládání elektronických peněz, provádění peněžních transakcí pomocí on-line systémů zúčastněných bank, tj. těch, které jsou zapojeny na centrální počítač nebo pro výměnu elektronických peněz s jinými podobnými převodními zařízeními pracujícími off-line, tj. bez zapojení na centrální počítač, bankomatů /4/ přidružených s vydávajícími a odpovídajícími bankami pro zpracování a připojení těchto zařízení k vydávajícím odpovídajícím bankám a pro propojení samotných těchto vydávajících a odpovídajících bank. Systém též zahrnuje cleringovou banku /5/ pro udržení rovnováhy mezi účty elektronických peněz různých vydávajících bank; datovou komunikační síť /6/ pro poskytování komunikačních služeb všem složkám systému; a bezpečnostních

opatření /7/ pro udržení soudržnosti systému a pro detekci padělatelských a jiných kriminálních zneužití systému. Jedno provedení řešení obsahuje modul zákaznických služeb, který zpracovává reklamace ztracených peněz a propojuje účty s peněžními moduly, aby umožnil bankovní přístup.





Elektronický ^{peněžní} monetární systém

Tato patentová přihláška je částečné pokračování současně podané patentové přihlášky US, pořadového čísla 08/234,461 ze dne 28. dubna 1994.

Oblast techniky

Vynález se týká elektronického monetárního systému pro zavedení elektronických peněžních převodů jako alternativního prostředí výhodné směny k získání peněžní hotovosti, kontrolám, úvěrovým a vkladovým kartám, a elektronickému převodu fondů.

Dosavadní stav techniky

V současné době proběhne mezi institucemi a samostatnými osobami přibližně 350 milionů převodů v bankovkách a mincích. Extensivní použití mincí a bankovek omezilo automatizaci individuálních převodů, jako jsou nákupy, jízdné, a vklady a výběry bankovních účtů. Individuální hotovostní převody jsou zatěžovány potřebou mít přesnou částku nebo být navíc vybaven drobnými. Manipulace - společně s ostrahou - s papírovými penězi a mincemi je nevýhodná, nákladná a časově náročná jak pro jednotlivce, tak pro finanční instituce. Bylo odhadnuto, že v samotných Spojených státech se utratí okolo 60 miliard US dolarů jen za pohyb peněz. Kromě toho, bezpečnost papírových peněz je vážně ohrožena relativně jednoduchým padělatelským použitím například snadno dostupných vysoce kvalitních barevných kopírek.

Ačkoli šeky mohou být napsány pro jakoukoli specifickou částku až do částky dostupné na účtu, šeky mají velmi omezenou převoditelnost a musí být dodávány z fyzické zásoby. Kontrolní systémy založené na papírových dokumentech sdílejí podobná omezení a obtíže jako převod hotovosti a přidávají k nim zpoždění způsobené zpracováním šeků. K tomu došla ekonomická



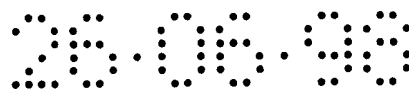
směna náročnou cestou hledání většího pohodlí a nižších nákladů, zatímco se také pokoušela o zlepšení bezpečnosti.

Automatizace dosáhla některých z těchto kvalit pro velké převody pomocí elektronických převodů fondů (electronic funds transfer, dále EFT). Převod elektronických fondů je v podstatě postup směny hodnot dosažený pomocí převodů pomocí centrálního počítačového bankovního systému. Služby EFT představují převod plateb, který využívá elektronické "šeky", používané především ve velkých obchodních organizacích.

Systémy automatizované clearingové banky (Automated Clearing House, dále ACH) a místa prodeje (point of sale, dále POS) jsou příklady převodních systémů elektronických fondů, které v posledních letech začaly být používány v maloobchodních a komerčních organizacích ve významném měřítku. Platby uskutečněné těmito typy EFT systémů jsou však limitovány tím, že nemohou být prováděny bez bankovního systému. Dále, převody ACH obvykle nemohou být prováděny mimo pracovní dobu.

Domácí služby šekových plateb známé jako "Home Banking" jsou příklady převodního systému elektronických fondů používaných jednotlivci k uskutečnění plateb. V současné době domácí bankovní iniciativy mají málo zákazníků. V bankách, které nabídly možnosti plateb, účtových převodů a informací pomocí telefonní linky použitím osobního počítače, používá tyto služby méně než jedno procento bankovních zákazníků. Jedním z důvodů, proč se "Home Banking" nestal úspěšným produktem je to, že zákazník nemůže v tomto systému uložit a vybrat peníze, jak potřebuje.

Současné EFT systémy, úvěrové karty či vkladové karty, které jsou používány s on-line systémem k převodu peněz mezi účty, jako např. mezi účty obchodníka a zákazníka, nemohou uspokojit potřebu po automatizovaném převodním systému, který poskytuje převod univerzálně akceptované ekonomické hodnoty mimo bankovní systém. Dále, úvěrové a debetní kartové systémy jsou obecně nedostatečně zajištěny proti zneužití a neposkytují odpovídající soukromí.



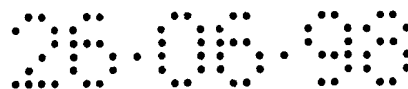
Při zavádění automatického a ještě vhodnějšího převodního systému, který nevyžaduje zprostředkování pomocí bankovního systému, a který může rozdělovat určitou formu finančních prostředků, byl zřetelný trend směřující k elektronickým peněžním převodům typu "off-line". Na příklad pro určitou formu "elektronických peněz" byly navrženy četné řešení, které mohou být použity při bezhotovostních platebních převodech jako náhrada za tradiční hotovostní a šekový způsob platby. Viz patentová přihláška US č. 4,977,595, s názvem "Způsob a zařízení pro realizaci elektronické hotovosti", a patentová přihláška US č. 4,305,059, s názvem "Modulární systém převodu fondů".

Známější techniky používají karty s magnetickým záznamem zakoupené za daný obnos, ze kterých může být předplacená hodnota odebírána pro specifické účely. Po vyčerpání jejich hodnoty se karty zahodí. Jiné příklady zahrnují paměťové karty nebo tzv. chytré karty, které jsou schopny opakovaně uschovat informaci představující hodnotu, která je podobně odčerpávána pro specifické účely.

Tyto navržené systémy však selhávají při stanovování významu bankovních deposit jako peněz, a jejich nezbytnosti zálohovat jakoukoli formu obecně akceptovaných monetárních reprezentací, které mohou být vydávány. V těchto systémech je reprezentace ekonomické hodnoty, ať již elektronická či papírová, vydávána bez podpory přiměřeně hodnotných ručení jako protějšku k jejich aktivům.

Žádný z těchto navržených platebních systémů bez papírů není tak mocný, aby bylo možno zavést víceúčelový elektronický monetární systém, který obsahuje jak automatická zařízení, která umožňují klientům převádět elektronické fondy nebo peníze mezi nimi bez jakéhokoli zprostředkovávajícího systému, tak také úplný bankovní systém pro generování hodnoty reprezentované elektronickými penězi a pro clearing a potvrzení stavu účtů elektronických peněz bank a finančních institucí zajišťujících monetární rovnováhu systému.

Tedy, je potřeba zavést systém, který dovoluje běžné ekonomické směny plátce příjemce provádět bez zprostředkování



bankovním systémem, a který předává kontrolu platebního postupu jednotlivci. Dále, je potřeba systém ekonomické směny, který může být použit velkými organizacemi pro komerční platby libovolné velikosti, který není omezen jako současný systém EFT.

V běžně uváděné patentové přihlášce USA č. 07/794,112, z 15. listopadu 1991, na kterou se odkazujeme, je popisován elektronický monetární systém (EMS), který překonává výše popsaná a jiná dřívější omezení, a poskytuje kompletní elektronický monetární systém, který využívá elektronické peníze, směnitelné s tradiční hotovostí a univerzálně akceptované. Vynalezený EMS poskytuje způsob a systém pro bezpečné a spolehlivé převody ekonomické hodnoty včetně hotovosti a úvěrů mezi odběrateli, mezi finančními institucemi a nebo mezi odběrateli a finančními institucemi. EMS umožňuje také použití elektronických peněz ve formě několika měn. Nicméně velká důležitost bezpečnosti a spolehlivosti vyvolává potřebu dalšího zlepšování EMS.

Tedy, předmětem současného vynálezu je zlepšený EMS systém a příbuzné způsoby ekonomické směny, které jsou odolné zneužití, duplikování a padělatelství.

Dalším předmětem vynálezu je systém, který umožňuje reklamovat ztracené peníze.

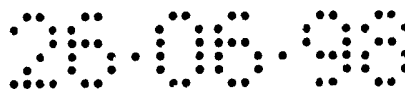
A dále je předmětem vynálezu monetární systém, který je pro klienta optimální a který lze spolehlivě a bezpečně použít pro převody peněz od kupujícího k prodávajícímu v reálném čase.

Výše zmíněné vlastnosti a výhody vynálezu jsou příklady toho, co může být dosaženo pomocí tohoto vynálezu a nejsou vyčerpávajícím ani omezujícím výčtem výhod, které mohou být dosaženy. Tedy tyto a jiné cíle a výhody současného vynálezu budou zřejmé z popisu nebo mohou být získány používáním vynálezu, obojí, jak je zde popsáno nebo jak je modifikováno ve všech variacích, které mohou být zřejmé odborníkům. Podle toho spočívá tento vynález v nových metodách, uspořádáních, kombinacích a vylepšeních zde ukázaných a popsaných.

Podstata vynálezu

K dosažení výše zmíněných vlastností a dalších výhod používají se ve způsobu a zařízení podle tohoto vynálezu s výhodou provedení ve formě elektronického monetárního systému, který obsahuje: (1) banky nebo finanční instituce, které jsou spojeny se zařízením generujícím peníze, které vytváří a vydává zavedeným klientům elektronické peníze, včetně elektronické hotovosti zálohovanou, které jsou podle požadavků kryty vklady a chráněny autorizacemi elektronických úvěrů; (2) odpovídající banky, které akceptují a distribuují elektronické peníze; (3) řadu převodních zařízení, které jsou používány klienti pro uchovávání elektronických peněz, pro provádění peněžních převodů pomocí systémů zúčastněných bank zapojených na centrální počítač (on-line) nebo pro směnu elektronických peněz s jinými podobnými převodními zařízeními při převodech, které nejsou prováděny v systémech zapojených na centrální počítač, tedy v systémech off-line; (4) bankomaty, spojené s vydávajícími a klientskými bankami, pro postup zpracování a umožnění činnosti převodních zařízení v jejich styku s vydávajícími a klientskými bankami, a pro zprostředkování styku mezi vydávajícími a klientskými bankami navzájem; (5) clearingovou banku pro vyrovnávání účtů elektronických peněz různých vydávajících bank; (6) datovou komunikační síť umožňující komunikační služby všem složkám systému; a (7) bezpečnostní uspořádání pro zabezpečení integrity systému a pro detekci zneužití a padělatelství uvnitř systému.

V preferovaném provedení budou následující funkce, zařízení pro generování peněz, zařízení pro převody, a zařízení bankomatů zajišťovány pomocí kombinace počítačových hardwarových modulů odolných proti zneužití a aplikačních softwarových modulů, které mohou být vzájemně propojeny v síti. Informace je převáděna v šifrované formě, aby se tak zamezilo neoprávněnému úniku informace. Elektronické peníze jsou převedeny spolu s digitálními podpisy za účelem autenticity a odolnosti vůči změnám a padělání.



Elektronické peníze převáděné těmito zařízeními mohou být elektronickou reprezentací hotovosti nebo úvěru. Důležitý aspekt elektronické měny spočívá v tom, že tato měna je ekvivalentní bankovkám a je směnitelná s konvenčními papírovými penězi proti vkladu u vydávající banky, ale může být vybrána nebo uložena jak ve vydávající bance, tak v klientské (obslužné) bance. Avšak pouze vydávající banky mohou vytvářet elektronickou hotovost, a budou odpovědné za jejich krytí.

Vydávající banky později využijí vnitřní bankovní clearingové a schvalovací postupy k zajištění monetární rovnováhy bankovního systému, jak praktikuje současné bankovníctví.

Representace elektronických peněz jsou směnitelné, univerzálně akceptované, a bezpodmínečně umořitelné u vydávajících bank, tj. mají vlastnosti peněžních převodů. K ochraně integrity elektronického monetárního systému každá směna elektronických peněz představuje současně s jiným také výměnu informace o datech identifikujících peněžní jednotku úvěru nebo hotovosti, (tj. dolary, jeny, atd.) částku úvěru nebo hotovosti, banku vydávající elektronický úvěr nebo hotovost, a několik digitálních podpisů.

Podle širokého chápání tohoto vynálezu, je místo převodu v hotovosti navržen elektronický monetární systém, převod elektronických peněz, včetně elektronické hotovosti, kde na vyžádání může být požadován vklad v bance a elektronické úvěrové autorizace. V jednom provedení tohoto vynálezu se elektronický monetární systém skládá: z peněžního modulu, který generuje elektronické peníze; peněžního modulu pro vydávání, distribuci a příjem elektronických peněz; a peněžního modulu pro příjem, ukládání a převod elektronických peněz mezi jiným přijímacím peněžním modulem a mezi přijímacím peněžním modulem a vydávajícím peněžním modulem.

Podle dalšího aspektu vynálezu elektronický monetární systém nabízí zavedení a správu elektronických peněz, což zahrnuje elektronickou hotovost, která je směnitelná za běžné peníze pomocí požadavků vůči vkladům v bance a pomocí autorizací elektronických úvěrů.



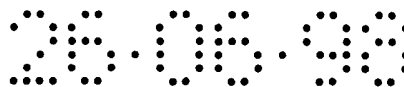
V provedení podle tohoto vynálezu zahrnuje systém řadu vydávajících bank; modul generátoru pro tvorbu elektronických peněz; peněžní automaty spojené s moduly generátorů pro provádění bankomatových převodů a pro komunikaci s jinými bankomaty, jako jsou převody včetně příjmu a distribuce elektronických peněz; bezpečnostní systém poskytující celkovou integritu elektronického monetárního systému; clearingový a schvalovací postup pro vyrovnaní účtů elektronických peněz odděleně vydávajících bank a pro clearing elektronických peněz vydaných vydávajícími bankami; a řadu převodních modulů vlastněných autorizovanými klienti pro přenos elektronických peněz mezi převodními moduly a mezi převodními moduly a bankomaty; a moduly zákaznických služeb, které se starají o reklamaci ztracených peněz a pro spojení účtů s peněžními moduly, aby se umožnil přístup k bance.

V souladu s jiným aspektem tohoto vynálezu, jsou funkce *modulů generátorů, převodních modulů, bankomatů a modulů zákaznických služeb*, realizovány pomocí kombinace hardwaru a softwaru, která je odolná proti zneužití a může být použita v síti.

Elektronické peníze směňované těmito moduly mohou být elektronické reprezentace hotovosti zálohované na požádání vkladovými účty u vydávající banky nebo úvěrovými autorizacemi a, aby se zajistila bezpečnost vůči neoprávněné modifikaci nebo padělání, mohou být převáděny s digitálními podpisy.

V preferovaném provedení je dosaženo odolnosti vůči padělatelství a zneužití tím, že se požaduje, aby pravidelná obnova modulů a jednotlivých jednotek elektronických peněz. S výhodou obsahuje přenos poukázky mezi moduly řadu identifikačních čísel umožňujících ověření všech předchozích převodů elektronické poukázky. Moduly nechovající se podle požadavků a padělané elektronické poukázky mohou být odstraněny ze systému ihned po jejich odhalení.

V souladu s dalším aspektem tohoto vynálezu, je pro reklamaci ztracených peněz ještě navržen postup, umožňující majiteli/držiteli převodního modulu předložit nároky vůči



bankovnímu systému prostřednictvím modulu zákaznických služeb a následně uznat ověření všech předchozích operací bankovního systému s elektronickou poukázkou; majitel/držitel tak může získat zpět jakoukoliv ztracenou a reklamovanou poukázku.

Další aspekt tohoto vynálezu poskytuje postup obnovu úvěru převodním modulem, ve kterém je použita pouze jediná úvěrová poukázka pro každý úvěrový účet v peněžním modulu.

V souvislosti s preferovaným provedením tohoto vynálezu je majiteli/držiteli převodního modulu také nabídnut postup umožňující bezpečně a spolehlivě nakupovat zboží od obchodníka.

Přehled obrázků na výkresech

Další aspekty, rysy a výhody vynálezu budou pochopeny a stanou se zřejmější, pokud bude vynález posuzován v souvislosti s následujícím popisem a doprovodnými obrázky, kde:

Obr. 1A představuje schema ukazující bezpečnostní hierarchii elektronického monetárního systému

Obr. 1B představuje schema ukazující bezpečnostní síť předávající zprávy mezi primárním bezpečnostním serverem a obyčejným bezpečnostním serverem.

Obr. 2 představuje schema bezpečnostní síťové struktury elektronického monetárního systému.

Obr. 3A ilustruje funkční součásti bezpečnostního serveru.

Obr. 3B ilustruje funkční součásti síťového serveru.

Obr. 4A ilustruje funkční součásti modulu zákaznických služeb.

Obr. 4B ilustruje funkční součásti primárního bezpečnostního serveru.

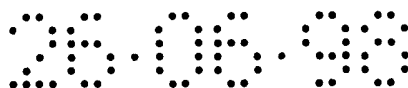
Obr. 5 ukazuje přehled síťové přihlašovací procedury.

Obr. 6A ÷ 6K ilustrují síťový přihlašovací protokol.

Obr. 7A ÷ 7E ilustrují protokol vytvoř spojení v elektronickém monetárním systému.

Obr. 8A ÷ 8B ilustrují protokol převed' poukázky.

Obr. 9A ÷ 9D ilustrují protokol zahraniční směna.



Obr. 10 ilustruje protokol závazek provést převod pro moduly elektronického monetárního systému.

Obr. 11A ÷ 11B ilustrují protokol přerušení převodu pro moduly elektronického monetárního systému.

Obr. 12A ÷ 12C ilustrují protokol o platbě na místě prodeje.

Obr. 13A ÷ 13B ilustrují protokol obnov úvěr u výdejní banky.

Obr. 14 ilustruje sestavení úvěrového protokolu.

Obr. 15A ÷ 15B ilustrují protokol požaduj úvěr.

Obr. 16 ukazuje příklad historie převodu poukázky.

Obr. 17 ukazuje schema (typu strom) převodu poukázky.

Obr. 18A ÷ 18C ilustrují protokol spoj peněžní modul s bankovním účtem (účty) pro přístup k bance.

Obr. 19A ÷ 19C ilustrují protokol opětovné legalizace spojení peněžního modulu s bankovním účtem (bankovními účty).

Obr. 20 ukazuje protokol platné číslo účtu.

Obr. 21A ÷ 21B ilustrují protokol vytvoř reklamaci ztracených poukázek.

Obr. 22A ÷ 22E ilustrují protokol reklamace ztracených poukázek.

Detailní popis vynálezu

Tento vynález představuje zlepšený monetární systému používající elektronická média k bezpečné a spolehlivé směně ekonomických hodnot. Systém může být zaveden integrací nových systémů zpracovávajících data s jinými procedurami, což může být realizováno v současných celosvětových bankovních systémech. V souladu s tímto vynálezem, několik vylepšení je obsaženo v elektronickém monetárním systému (Electronic Monetary System), zveřejněným v patentové přihlášce USA č. 07/794, 112, podané 15. listopadu 1991, na kterou se odkazujeme. Tato vylepšení obsahují: sadu vylepšení týkajících se bezpečnosti obsahující zdokonalenou zahraniční směnu (F/X) a dále postupu při převodu poukázek, postupu při reklamace ztracených peněz, postup při spojování peněžních modulů pro bankovní přístup, postupu při platbě na místě prodeje, a postupu pro aktualizaci úvěrů.

Bezpečnost

Účinné zabezpečení monetárního systému má tři požadavky: bránit se padělatelům, zjistit je a zadržet je. Popisovaný elektronický monetární systém je navržený tak, aby všechny splňoval.

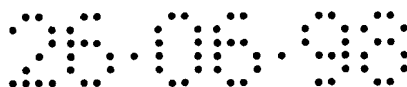
Aby peněžní moduly při komunikaci odolaly padělatelům používají šifrování se symetrickým a asymetrickým klíčem. Všechny zprávy jsou šifrované. Modulové protokoly jsou navíc fyzicky chráněny hardwarem, který odolává všem neoprávněným zásahům.

Padělatelství je detekováno pomocí postupu, ve kterém se ověřují poukázky¹. Časové protokoly používané v celém systému (např., viz expirace) vyžadují, aby elektronické poukázky byly pravidelně opětovně schvalovány. Také elektronické poukázky jsou při bankovních převodech aktualizovány (tj. nahrazovány novou poukázkou s novým expiračním datem).

Peněžní moduly jsou blokovány (např. zápisem do seznamu neplatných ID), jsou-li duplikovány nebo je k nim připojena zfalšovaná poznámka. Převod nebude povolen také těm poukázkám, které prošly takto blokovánými moduly. Převod duplikovaných či padělaných poukázek bude odložen do doby expirace nebo případně deponován v bance. Dále, v případě vážných systémových bezpečnostních problémů elektronického monetárního systému může systém požádat o celkové opětovné ověření, přičemž si, pro případ jejich nového přihlášení do sítě elektronického monetárního systému, vyžádá ověření všemi moduly, včetně převodních peněžních modulů.

Následující seznam vylepšení by měl sloužit k ochraně veškeré informace před odposlechem modulových interakcí. Všechny informace jsou šifrovány, dokonce i veřejné klíče a modulové identifikátory. Seznam vylepšených bezpečnostních opatření:

- 1) Ochrana přihlášení do sítě spočívající v tom, že nikdo nemůže zneužít² peněžní modul nebo získat z něj jakoukoli informaci v použitelné formě, což je dále popsáno v odkazu na Obr. 5.



- 2) Vytvoření metody pro přiřazení bezpečnostního serveru generátoru peněz a identifikátorů bankomatů (viz Schema číslování modulů). Tyto identifikátory jsou kontrolovány při :
 - (a) vytváření spojení (viz Obr. 7);
 - (b) převodu poukázek - kontrolou převodních záznamů (viz Obr. 8).
- 3) Zavedením struktury serveru vázaného na dvě strany (viz Bezpečnostní hierarchie a Bezpečnostní síť), zahrnující primární bezpečnostní sever, kde všechny moduly nesou veřejné klíče primárního bezpečnostního serveru, a bezpečnostní server, který ověřuje všechny další moduly.
- 4) Zlepšení převodních poukázek tak, aby umožnily kontrolu podle seznamu neplatných ID u všech převodů před přijetím poukázek k vyplacení nebo zahraniční směně (F/X) a dále kontrolu duplikovaných poukázek (viz Obr. 8).
- 5) Šifrování všech certifikátů použitím soukromých klíčů bezpečnostního serveru (viz Ověřovací struktura a uvedení v platnost).
- 6) Dynamické obměňování velikosti veřejných klíčů (viz Bezpečnostní síť a Obr. 6).
- 7) Změna protokolu o závazku zajišťující, že selhání neduplikuje vydaný obnos peněz³ (viz Obr. 10).
- 8) Změnu zahraniční směny (F/X) takovou, aby žádná strana nemohla podvodně přerušit převod a tak bezpečně přijmout peníze a současně žádné neodeslat.
- 9) Změnu protokolu přeruš záznam informace při nedodržení závazku převodu pokud platící převádí, ale přijímající přerušuje (viz Obr. 11).
- 10) Umožnění celkového opětovného ověření, pokud je to třeba (viz Bezpečnostní síť a Obr. 6).

Uvedený seznam bezpečnostních zlepšení dále objasňuje některé bezpečnostní rysy poskytované vylepšeným bezpečnostním systémem tohoto vynálezu. Tato a další vylepšení mohou být dále

pochopena z následujícího detailního popisu alternativního preferovaného provedení bezpečnostního systému pro elektronický monetární systém.

Bezpečnostní hierarchie

V souvislosti s tímto vynálezem je nabízeno jiné možné provedení bezpečnostního zajištění elektronického monetárního systému. Podle odkazů na Obr. 1A, bude mít elektronický monetární systém dva typy bezpečnostních serverů a to primární 1182 a běžné 1184. Primární bezpečnostní servery 1182 ověřují (běžné) bezpečnostní servery 1184. Bezpečnostní servery 1184 ověřují všechny další moduly (moduly peněžního převodu 1186, moduly bankomatu 1188, moduly peněžních generátorů - moduly 1190, a moduly zákaznických služeb 1192) tohoto systému.

Primární servery 1182 pouze komunikují s jinými primárními servery 1182 nebo bezpečnostními servery 1184. Podle Obr. 2, primární bezpečnostní servery 1182 jsou umístěny v bezpečném zařízení spojeném se všemi ostatními pomocí místní bezpečnostní sítě LAN 1194. Tato místní síť LAN 1194 je připojena s bezpečnostní sítí 1196 bezpečnou bránou. Po této síti komunikují pouze bezpečnostní servery. Všechny bezpečnostní servery jsou fyzicky zabezpečeny.

Bezpečnostní servery 1184 jsou také připojeny k síti elektronického monetárního systému 1198 a bankovním místním sítím 1200. Předpokládá se, že bezpečnostní servery mohou být zneužity a proto jsou legalizovány po všech interakcích s ostatními moduly.

Pouze bezpečnostní servery (Security Server, dále také SS) 1184 a moduly mají certifikáty. Veřejné klíče primárního bezpečnostního serveru jsou přenášeny pomocí těchto zařízení. Existují dva druhy certifikátů: bezpečnostního serveru a modulu.



Struktura certifikátu a legalizace

Struktura certifikátu je tato:

$$\text{Cert}(\text{SS}) = E_{\text{PSS}}[\text{SS}(\text{id}) * \text{SS}(\text{PK}) * \text{datum expirace} * \sigma_{\text{PSS}}(\text{X})] * [\text{PSS}(\text{id}) \text{ XOR } \text{C}]$$

_____ X _____

$$\text{Cert}(\text{M}) = E_{\text{SS}}[\text{M}(\text{id}) * \text{M}(\text{PK}) * \text{datum expirace} * \sigma_{\text{SS}}(\text{Y})] * \text{Cert}(\text{SS})$$

_____ Y _____

1) Protokoly legalizace certifikátu jsou tyto:

- a) $\text{PSS}(\text{id}) = [\text{PSS}(\text{id}) \text{ XOR } \text{C}] \text{ XOR } \text{C}$
- b) $D_{\text{PSS}}(E_{\text{PSS}}(\text{X} * \sigma_{\text{PSS}}(\text{X}))) = \text{X} * \sigma_{\text{PSS}}(\text{X})$
- c) Zkontroluj, zda $\text{SS}(\text{id})$ je autentické (viz schema číslování modulů)
- d) Zkontroluj, zda je platné datum
- e) Zkontroluj, zda platí $D_{\text{PSS}}(\sigma_{\text{PSS}}(\text{X})) = h(\text{X})$

2) Legalizuj $\text{Cert}(\text{M})$

- a) Legalizuj $\text{Cert}(\text{M})$
- b) $D_{\text{SS}}(E_{\text{SS}}(\text{Y} * \sigma_{\text{SS}}(\text{Y}))) = \text{Y} * \sigma_{\text{SS}}(\text{Y})$
- c) Zkontroluj, zda $\text{M}(\text{id})$ je autentické (viz schema modulového číslování modulů)
- d) Zkontroluj, zda je platné datum
- e) Zkontroluj, zda platí $D_{\text{SS}}(\sigma_{\text{SS}}(\text{Y})) = h(\text{Y})$

Kde PSS ... Prim. bezp. server PK ... veřejný klíč (včetně délky)

SS ... Bezp. server σ ... digitální podpis=EBh

* ... zřetězení Cert ... certifikát

id ... ident. číslo E ... Algoritmus se soukromým klíčem

h ... Hashova funkce používaný pro šifrování a pro

C... konstantní náhodné vytvoření digitálního podpisu

číslo sdílené všemi D ... algoritmus pro dešifrování a

dalšími moduly kontrolu digitálního podpisu

využívající veřejný klíč.

Všimněte si, že E může být použito pro dešifrování a D pro šifrování, pokud budou použity v jiné aplikaci.



Schema číslování modulů

Primární bezpečnostní servery 1182, bezpečnostní servery 1184, moduly peněžních automatů 1188, moduly peněžních generátorů 1190, moduly zákaznických služeb 1192, a převodní peněžní moduly 1186 mají přiřazena identifikační čísla (id) tak, že je možné zkontrolovat jejich autentičnost. 48-bitové prvočíslo "p" je generováno a primitivní kořen "a" modulo p (kde $a^n \neq 1(p)$ pro všechna $1 \leq n < p-1$) se nalezne pomocí bezpečného postupu. Jak a tak p se zavedou do všech modulů systému bezpečně pomocí primárních bezpečnostních serverů při instalaci.

Pracovní schema je toto:

Pokud $a^n \equiv m(p)$ a

- 1) $1 \leq m \leq 99\ 999$ pak n je přiřazeno jako id primárního bezpečnostního serveru
- 2) $100\ 000 \leq m \leq 999\ 999$ potom n je přiřazeno jako id bezpečnostního serveru
- 3) $1\ 000\ 000 \leq m \leq 6\ 999\ 999$ potom n je přiřazeno jako id modulu peněžního automatu
- 4) $7\ 000\ 000 \leq m \leq 9\ 999\ 999$ potom n je přiřazeno jako id modulu generátoru peněz
- 5) $10\ 000\ 000 \leq m \leq 11\ 999\ 999$ potom n je přiřazeno jako id modulu zákaznických služeb
- 6) $m > 12\ 000\ 000$ potom n je přiřazeno jako id modulu převodu peněz.

Pokud modul nebo server legalizuje certifikát, kontroluje autenticitu identifikačního čísla (např. $M(id)$, $SS(id)$ $PSS(id)$) n tak, že spočte $a^n \equiv m(p)$ a potom kontroluje zda m je ve správném rozsahu.

Bezpečnostní síť

Jak je ukázáno na Obr. 2, bezpečnostní síť 1196 a bezpečnostní místní síť LAN 1194 spojují bezpečnostní servery 1184 s primárními bezpečnostními servery 1182. Při instalaci nejprve bezpečnostní servery 1184 ověří peněžní moduly a moduly

zákaznických služeb 1192. Takové bezpečnostní servery mohou být propojeny instalačním modulem místní sítě LAN 1202. Pak předávají bezpečnostní informaci, jako je seznam neplatných id a seznam primárních bezpečnostních serverů a jejich veřejných klíčů modulům. Seznam neplatných id obsahuje totožnosti peněžních modulů, serverů zákaznických služeb a bezpečnostních serverů, u kterých jsou převody blokovány. Opětné ověření těchto modulů je popsáno následně ve vývojovém diagramu síťového přihlášení.

Při instalaci jsou primárními bezpečnostními servery 1182 nejprve ověřeny bezpečnostní sever 1184. Tyto primární bezpečnostní servery mohou být spojeny pomocí bezpečnostního serveru instalace LAN 1204. Podle Obr. 1B, bezpečnostní servery 1184 přijímají různou bezpečnostní informaci, kterou postupují ostatním modulům. Bezpečnostní sever nabízejí bezpečnostní služby síti elektronického monetárního systému 1198 a místním bankovním sítím LAN 1200, jako při přihlášení do sítě, kde předávají aktualizované bezpečnostní informace. Bezpečnostní servery 1184 přijímají tuto informaci od primárních bezpečnostních serverů 1182 pomocí bezpečnostní sítě 1196. Převodní peněžní moduly 1186 komunikují se sítí EMS 1198 prostřednictvím síťových serverů 1206 (NS). Zúčastněné banky mají modul(y) bankomatu(ů) 1188 a možná i modul peněžního generátoru 1190 připojeny k jejich místní bankovním sítím LAN 1200.

Bezpečnostní síť 1196 je propojeně zašifrována. Navíc, primární bezpečnostní servery a bezpečnostní servery sdílejí společný symetrický klíč (bezpečnostní síťový šifrovací klíč). Tento klíč je periodicky obměňován určeným primárním bezpečnostním serverem 1182, veřejným klíčem, výměnou klíče.

Seznam neplatných ID je spravován určeným primárním bezpečnostním severem 1182. Tento seznam je vytvořen z interakcí se zúčastněnými bankami, s právně zplnomocněnými autoritami, a klienti systému.

Periodicky bude obměňována délka klíče pro bezpečnostní sever a moduly. Aby se zabezpečila vysoká bezpečnostní úroveň,



běžně se prodlužuje délka klíče. Nové stanovené délky klíčů budou sděleny primárním bezpečnostním serverům prostřednictvím určeného primárního serveru. Nové délky klíče budou sděleny bezpečnostním serverům primárními servery, po zaslání nových seznamů neplatných ID nebo po novém ověření. V případě nebezpečného narušení bezpečnosti může primární bezpečnostní server vyžádat celkové opětovné ověření.

Délka veřejného klíče pro každý primární server se nebude měnit. Bude vytvořen časový plán, který časově rozvrhne zavádění primárních bezpečnostních serverů do provozu i jejich stahování z provozu. Nové servery budou mít velmi pravděpodobně delší klíče, ledaže by byly zavedeny kvůli zvýšenému objemu převodů. Seznam aktivních veřejných klíčů primárních bezpečnostních serverů je vytvořen primárním bezpečnostním severem a podepsán soukromým klíčem serveru. Potom je tento seznam rozeslán ostatním bezpečnostním serverům.

Obr. 3A ukazuje funkční složky bezpečnostního serveru 1184. Funkce *vnější interface* 1208 - poskytuje komunikační vrstvu pro spojení se sítí. Funkce *manager spojení* 1210 - řídí bezpečnostní aspekty převodového spojení. Funkce *přihlášení k síti* 1212 - ovládá bezpečnostní funkce pro přihlášení do sítě. Funkce *tvorba certifikátu* 1214 ověřuje certifikát všech peněžních modulů (v primárním bezpečnostním serveru tuto funkci zajišťují bezpečnostní servery). Funkce *distribuce ověřovacích klíčů* 1218 distribuuje seznam platných veřejných klíčů primárních bezpečnostních serverů od ověřovací agentury peněžním modulům (primární bezpečnostní servery také distribuuji celkovou zprávu opětovného ověření). Funkce *kontrola seznamu neplatných ID* 1220 kontroluje a distribuuje seznam neplatných identifikátorů. Funkce *synchronizace data/času* 1222 zajišťuje synchronizaci služeb hodiny/časovač peněžního modulu se systémovým časem. Funkce *hodiny/časovač* 1224 a *šifrování* 1226 jsou identické s těmito funkcemi v peněžních modulech.

Obr. 3B ukazuje funkční součásti síťového serveru 1206. Funkce *vnější interface* 1228 poskytuje komunikační prostředí

pro spojení se sítí. Funkce *manažer komunikace při spojení* 1230 zprostředkovává komunikační spojení mezi peněžními moduly, a mezi peněžním modulem a bezpečnostním serverem. Funkce *přihlášení do sítě* 1232 řídí postup přihlášení peněžního modulu do sítě. Funkce *zpráva o cestě* 1234 poskytuje adresářové služby pro cestující zprávy tím, že řídí směrování zpráv při přihlášení a při spojení peněžního modulu. Funkce *přímý přístup ke službám banky* 1236 poskytuje informaci o službách zúčastněných bank. Funkce *šifrování* 1238 zajišťuje funkci *symetrický klíč* 1240 a funkci *generátor náhodných čísel* 1242. Funkce *symetrický klíč* 1240 šifruje zprávy mezi síťovým serverem 1206 a modulem připojujícím se na síť a mezi síťovým serverem 1206 a bezpečnostními servery 1184. Funkce *generátor náhodných čísel* 1242 generuje náhodná čísla pro šifrovací klíče a ověřovací zprávy.

V souhlasu s tímto vynálezem je s výhodou doporučena jiná zabezpečovací součást, modul zákaznických služeb (CSM) 1192. Modul zákaznických služeb je zařízení odolné proti zneužití a používané pro vytváření a aktualizování účtových profilů. Modul zákaznických služeb obsahuje jedinečný certifikát podobný certifikátu v peněžních modulech a bezpečnostních serverech. Moduly zákaznických služeb mohou vytvářet bezpečná spojení s jinými moduly (např. bezpečnostními servery). Modul zákaznických služeb, CSM, vyžaduje připojení hostitele k reprezentantovi zákaznických služeb a on-line bankovní systémy.

Modul zákaznických služeb má dvě základní funkce. Zaprvé vytváří účetní profily tak, že peněžní modul se může spojit s bankovními účty, obnovit platnost spojení peněžního modulu s bankovním účtem a uvést v platnost čísla účtů. Tyto převody jsou detailněji popsány níže s odkazy na Obr. 18-20. Za druhé, modul zákaznických služeb zpracovává nároky na ztracené poukázky v reakci na požadavek reprezentanta hostitelských zákaznických služeb, což je vysvětleno přesněji na Obr. 21 a 22. Modul zákaznických služeb má stejné bezpečnostní funkce jako peněžní modul a speciální rozsah čísel pro své identifikátory (viz Schema číslování modulů). Výkonnost těchto



funkcí modulu zákaznických služeb (CSM) zjednodušuje postup legalizace čísel účtů modulu bankomatu.

V souvislosti s provedením elektronického monetárního systému, která používá modul zákaznických služeb se struktura profilu účtu pro každou banku mění na:

datum expirace $*M(id)*B(id)*LA*\sigma_{CSM}(X)]*Cert(CSM)$, kde
 $M(id)$ identifikátor modulu
 $B(id)$ identifikátor banky
 LA seznam čísel účtů a druhu účtu (vkladový nebo úvěrový)
 σ_{CSM} označení modulu zákaznických služeb, CSM
 $Cert(CSM)$ certifikát modulu zákaznických služeb, CSM
 $*$ zřetězení

Legalizační procedura pro takový profil je popsána níže s odkazem na Obr. 20.

Obr. 4A ukazuje funkční součásti modulu zákaznických služeb, CSM 1192. Vnější interface 3000 je prostředníkem mezi modulem zákaznických služeb hostitele, CSMH, a dalšími zpracovávajícími a komunikačními prostředky uvnitř procesoru hostitele modulu zákaznických služeb, CSM; Manager komunikace při spojení 3001 působí při řízení a převodu (tj. ukončení) nebo přerušuje převodní spojení mezi modulem zákaznických služeb, CSM, a převodním peněžním modulem nebo reprezentantem zákaznických služeb. Funkce *vytvoř profil účtu* 3002 vytváří z informací o účtu zákazníka profil účtu, který dovoluje peněžnímu modulu přístup k různým bankovním účtům klienta. Funkce *veřejný klíč* ověřuje a podepisuje bankovní účetní profil. Jelikož modul zákaznických služeb, CSM, vyžaduje od hostitele zprostředkování mezi reprezentantem zákaznických služeb a on-line bankovními systémy funkce *k hostiteli* 3006 zprostředkovává oddělení povinností mezi aplikacemi modulu zákaznických služeb, CSM, a hostitelskými aplikacemi. Funkce *reklamace ztracených poukázek* 3008 odpovídá na klientovy nároky ztracených poukázek, které modul zákaznických služeb, CSM, legalizuje a distribuuje

vydávacím bankám. Funkce *zajištění bezpečnosti* 3004 spravuje seznam ohrožených peněžních modulů, žádá o certifikáty, synchronizuje hodiny, a spravuje tvorbu nových digitálních klíčů. Funkce *hodiny/časovač* 3012 a funkce *šifrování* 3010 jsou identické s těmito funkcemi v peněžních modulech.

Obr. 4B ukazuje funkční komponenty primárního bezpečnostního serveru 1182. Funkce *vnější interface* 3020 poskytuje komunikační vrstvy pro spojení se sítí. Funkce *manager spojení* 3002 řídí bezpečnostní aspekty spojení s bezpečnostními servery, se kterými se zachází tak, jako by byly ohrožené, a dále s dalšími primárními bezpečnostními servery. Funkce *tvorba certifikátu* 3024 vytváří certifikát pro jakýkoli bezpečnostní server. Funkce *distribuce ověřovacích klíčů* 3026 distribuuje seznam ověřovací agentury s platnými veřejnými klíči primárních bezpečnostních serverů mezi bezpečnostní servery. Funkce *distribuce bezpečnostních síťových klíčů* 3032 řídí a rozděluje bezpečnostní síťové klíče primárním bezpečnostním serverům a bezpečnostním serverům. Funkce *přikaz celkové opětovné ověření* 3030 stanoví, zda je potřeba provést celkové opětovné ověření (tj. v důsledku nebezpečného porušení bezpečnosti) a když je považuje za nezbytné, zařídí jej. Funkce *distribuce seznamu neplatných ID* 3028 řídí a rozděluje seznam neplatných identifikátorů. Funkce *hodiny/časovač* 3034 a *šifrování* 3036 jsou stejné s obdobnými funkcemi v peněžních modulech.

Síťové přihlášení

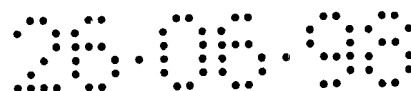
Přehled procedury síťového přihlášení je zřejmý ze schématu na Obr. 5. Přihlašovací protokol popisuje situaci, ve které modul 1243 vyžaduje přístup k síti elektronického monetárního systému, EMS 1198 pro opětovné ověření, uložení, výběr či z jiného důvodu. Modul 1243 může být modul peněžního převodu 1186 modul bankomatu 1138 modul peněžního generátoru 1188 nebo modul zákaznických služeb 1192. K Obr. 5 patří ještě tato vysvětlení. (a) ... Vytvoř komunikaci mezi modulem 1243 a síťovým serverem 1206. (b) ... Předej certifikát modulu síťovému serveru



1206. (c) ... Síťový server 1206 generuje náhodné ověřovací číslo V a náhodný klíč K; síťový server poté postoupí certifikát modulu V a K bezpečnostnímu serveru 1184 (šifrované pomocí NS/SS klíče). (d) ... modul 1243 a bezpečnostní server 1184 vytvoří bezpečné komunikační spojení (viz klíč spojení (MM/SS)). (e) ... Bezpečnostní server 1184 postoupí čas/datum, aktualizuje Seznam neplatných ID, aktualizuje seznam veřejných klíčů primárních bezpečnostních serverů, délku veřejného klíče, celkové opětovné ověření (v případě nutnosti), a znovu ověří modulový certifikát (v případě nutnosti). (f) ... Ukončí spojení s modulem 1243 a pošle V a K modulu 1243. (g) ... Zašifruj V a K a pošle je síťovému serveru 1206. (h) ... Síťový server 1206 uzná síťové přihlášení k modulu 1243. (i) ... modul 1243 poté informuje síťový server 1206 o cílovém připojení (pokud existuje) ke kterému je třeba se připojit. (j) ... Síťový server 1206 vytvoří spojení s cílem.

Síťové připojení je navrženo tak, že nikdo nemůže podvést modul 1243 nebo získat neoprávněně jakoukoli informaci ve srozumitelné formě. Obr. 6 popisuje detailně průběh procedury síťového přihlášení.

Komunikace A vytváří spojení se sítí elektronického monetárního systému 1198 (krok 1244). Zajištění bezpečnosti A pošle svůj certifikát síťovému serveru (network server dále NS) 1206 (krok 1246). Přihlášení do sítě NS přijme certifikát NS (krok 1248). Generátor náhodných čísel NS generuje náhodný klíč K a náhodné ověřovací číslo V (krok 1250). Symetrický klíč NS zašifruje certifikát modulu, K a V pomocí NS/SS klíče (krok 1252). NS/SS klíče jsou lokální symetrické klíče instalované v síťových serverech 1206 a bezpečnostních serverech 1184, které komunikují při přihlašování do sítě. Síťové přihlášení NS pošle certifikát, K a V bezpečnostnímu serveru (SS) 1184, kde jeho síťové přihlášení obdrží zprávu a Symetrický klíč SS dešifruje zprávu (kroky 1254 - 1258). Síťové přihlášení SS ukládá K i V a poté posílá modulový certifikát veřejnému klíči SS k legalizaci (kroky 1260 - 1264). Aby se umožnila možnost opětovného



ověření, veřejný klíč SS neuvažuje datum expirace při posuzování platnosti modulového certifikátu.

Jestliže modulový certifikát není platný, pak funkce *síťové přihlášení SS* připraví zprávu, na základě které se odepře přístup, k přenosu k síťovému serveru 1206 a modulu 1243 (krok 1266). Veřejný klíč SS zašifruje zprávu pro modul 1243 veřejným klíčem modulu a Manager spojení SS pošle zprávu síťovému serveru (kroky 1268 - 1270). Síťové přihlášení NS přijme zprávu a zaznamená zamítnutí přístupu. Šifrovaná zpráva je poté poslána modulu, a síťový server se odpojí (krok 1272). Manager spojení A tuto přijme zprávu, veřejný klíč A dešifruje tuto zprávu, a manager spojení A zaznamená, že přihlášení bylo zamítnuto (kroky 1274 - 1278). Jestliže zařízením žadajícím přihlášení byl peněžní modul převodu, pak funkce *ke klientovi A* informuje klienta (kroky 1280 - 1282). Jinak funkce *k bance A* informuje banku (krok 1284).

Na druhé straně, je-li certifikát modulu platný, pak SS funkce *kontrola seznamu neplatných id na SS* zjistí zda id modulu je na seznamu neplatných ID (kroky 1286 - 1288). Jestliže id je na tomto seznamu, je přístup k síti zamítnut. Jinak generátor náhodného čísla SS vytvoří náhodné číslo R a ověřovací zprávu (krok 1290). Funkce bezpečnostního serveru SS *síťové přihlášení SS* sloučí R a ověřovací zprávu do zprávy, která je šifrována veřejným klíčem SS pomocí veřejného klíče A. Veřejný klíč A dále rozšíří tuto šifrovanou zprávu přidáním certifikátu bezpečnostního serveru (kroky 1292 - 1294). Zpráva je poslána k A, kde veřejný klíč A dešifruje zprávu a legalizuje certifikát bezpečnostního serveru (krok 1298).

V případě, že je certifikát neplatný, A zaznamená ukončení spojení a informuje klienta nebo banku (kroky 1304 - 1306). Je-li certifikát platný, pak zajištění bezpečnosti A zkontroluje, zda id bezpečnostního serveru není na seznamu neplatných id (kroky 1308 - 1310). Je-li na seznamu, je spojení ukončeno (kroky 1300 - 1306). Když tam není, vytvoří generátor náhodných čísel (RNG) patřící k A náhodné číslo R(A) (krok



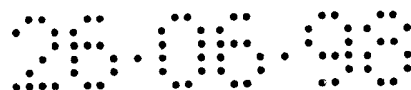
1312). Zajištění bezpečnosti A utvoří klíč spojení (MM/SS) pomocí funkce $R(A) \text{ XOR } R$ a poté uloží klíč spojení (krok 1314).

Zpráva obsahující ověřovací zprávu a $R(A)$ je sestavena a zašifrována pomocí veřejného klíče bezpečnostního serveru (krok 1316). Manager spojení A pošle zprávu k Síťovému přihlášení SS a Veřejný klíč SS dešifruje zprávu (kroky 1318 - 1322).

Síťové přihlášení SS ověřuje, zda kontrolní zpráva je ta, kterou samo vytvořilo (kroky 1324 - 1326). Pokud to tak není, zamítne bezpečnostní server přístup k síti. Je-li kontrolní zpráva v pořádku, pak symetrický klíč SS vytvoří klíč spojení (MM/SS) podle $R(A) \text{ XOR } R$ (krok 1328). Manager spojení SS zaznamená počátek spojení a pošle vyrozumění k A pomocí podprogramu *pošli zprávu* (kroky 1330 - 1332). Manager spojení A přijme toto vyrozumění a zaznamená počátek spojení (krok 1334).

Hodiny/časovač A pošlou čas a datum manažerovi spojení, který je dále pošle bezpečnostnímu serveru (kroky 1336 - 1340). Synchronizace data/času SS obdrží čas a datum a zkontroluje, zda jsou v dovoleném parametrovém rozmezí (kroky 1342 - 1344). Nejsou-li v tomto rozmezí, pak synchronizace data/času SS pošle nový čas a datum manažerovi spojení A (kroky 1346 - 1350). Hodiny/časovač A potom nastaví čas i datum (krok 1352). Dále A znovu pošle svůj čas a datum bezpečnostnímu serveru pro opětovnou kontrolu. Je-li synchronizace hodin provedena víckrát než je stanoveno, pak je klientovi nebo bance ohlášena chybná funkce hodin. Je-li to třeba, mohou se potom pokusit znovu o další synchronizaci (kroky 1354 - 1362).

Jsou-li však jsou hodnoty času a data v určených mezích parametrů, pak síťové přihlášení SS sestaví zprávu obsahující seznam neplatných id, nový seznam veřejných klíčů primárních bezpečnostních serverů (které pocházejí z funkce *distribuce ověřovacích klíčů*), a délku veřejného klíče (velikost veřejných klíčů je pravidelně obměňována) (krok 1364). Tvorba certifikátů SS kontroluje zda bylo požádáno o globální opětovné ověření a zajistí, aby časová perioda pro celkové opětovné ověření nevypršela (kroky 1366 - 1368). Tato časová perioda má být dost dlouhá na to, aby v jejím průběhu jakýkoliv certifikát vypršel,



nebo byl nově ověřen. Tato funkce má také kontrolovat, kdy byl modul naposled opětovně ověřován, protože modul není třeba ověřovat znovu, byl-li ověřen během celkového opětovného ověřování.

Je-li vyžadováno opětovné ověření, pak funkce vytvoř certifikát SS přidá k předchozí zprávě informaci "modul má znovu ověřit" (krok 1370). Pak, ať již je nebo není požadováno opětovné ověření, veřejný klíč SS podepíše zprávu (krok 1372). Zpráva je zaslána k A, kde veřejný klíč A zkontroluje digitální podpis zprávy (kroky 1374 - 1378). Je-li podpis neplatný, je spojení ukončeno. Zajištění bezpečnosti A potom aktualizuje své seznamy neplatných id, veřejných klíčů, a délek klíče (krok 1382).

Modul A poté zkontroluje, zda jeho certifikát potřebuje být opětovně ověřen (buď v důsledku celkového opětovného ověření nebo kvůli prošlému certifikátu) (kroky 1384 - 1386). Je-li vyžadován nový certifikát, pak zajištění bezpečnosti A dá podnět ke generaci nového certifikátu (krok 1388). Veřejný klíč A vytvoří nové klíče a stvrdí podpisem nové veřejné klíče pomocí svého starého soukromého klíče (krok 1390). Manažer spojení A pošle potvrzený nový veřejný klíč k jednotce vytvoř certifikát SS bezpečnostního serveru (kroky 1392 - 1396). Veřejný klíč SS potom legalizuje podpis na novém veřejném klíči (kroky 1398 - 1400). Pokud není podpis platný, pak bezpečnostní server odepře přístup k síti. Je-li podpis platný, pak veřejný klíč SS stvrdí podpisem nový certifikát modulu a pošle jej modulu (krok 1402). Manažer spojení A obdrží certifikát, zajištění bezpečnosti A provede legalizaci certifikátu a veřejný klíč A legalizuje podpis (kroky 1404 - 1410).

Jestliže certifikát není platný, pak manažer spojení A pošle bezpečnostnímu serveru pomocí funkce *pošli zprávu* jak zprávu "neplatný certifikát", tak tento certifikát (kroky 1412 - 1413). Funkce *síťové přihlášení SS* přijme zprávu a funkce *veřejný klíč SS* legalizuje podpis (kroky 1414 - 1418). Jestliže bezpečnostní server uzná, že certifikát je skutečně platný⁴, pak odepře přístup tomuto modulu k síti. Je-li však certifikát



neplatný, pak manažer spojení SS informuje síťový server, že se odpojuje od sítě (krok 1420). Síťové přihlášení NS informuje modul o selhání (krok 1422). Modul potom požádá klienta nebo banku o nový pokus (kroky 1424 - 1432).

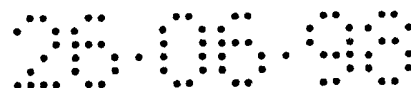
Když na druhé straně, modul určí, že je jeho nový certifikát platný, manažer spojení A pošle potvrzení bezpečnostnímu serveru (krok 1434). Podobně, pokud nebyl požadován nový certifikát, pak zajištění bezpečnosti A pošle vyrozumění bezpečnostnímu serveru kroky 1436 - 1438). V obou případech, manažer spojení SS přijme toto vyrozumění a zaznamená konec svého spojení s modulem (krok 1440). Síťové přihlášení SS pak pošle K i V do A (kroky 1442 - 1444). Manažer spojení A přijme zprávu a symetrický klíč A zašifruje V a stanovení cíle pomocí K a pošle zprávu síťovému serveru (kroky 1446 - 1448). Síťové přihlášení NS přijme zprávu a symetrický klíč NS dešifruje zprávu a zkontroluje, zda V je identické s tím V, které bylo předtím generováno (kroky 1450 - 1454).

Není-li toto V identické s předchozím, pak síťové přihlášení NS pošle zprávu přístup odepřen k A a odpojí se (kroky 1456 - 1458). Je-li V správné, pak síťové přihlášení NS vytvoří spojení s místem určení a pošle vyrozumění k A (krok 1460). Nakonec, manažer spojení A přijme vyrozumění a zaznamená, že A bylo přihlášeno k síti elektronického monetárního systému 1198 (krok 1462).

Vytvoření spojení

Obr. 7 ukazuje protokol vytvoř spojení. Zajištění bezpečnosti A pošle certifikát modulu manažera spojení a manažer spojení A přijme certifikát a zkontroluje, je-li peněžní modul A připojen k síti (kroky 1464 - 1466). Jestliže peněžní modul A není připojen k síti, manažer spojení A pošle certifikát přijatý od zajištění bezpečnosti A do místa určení B (krok 1476).

Alternativně, je-li peněžní modul A připojen k síti, symetrický klíč A zašifruje certifikát pomocí K a manažer spojení pošle zašifrovaný certifikát síťovému serveru (kroky



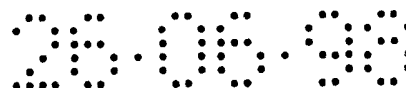
1468 - 1472). Síťový server dešifruje certifikát pomocí K a pošle jej do místa určení B.

Bez ohledu na to, zda byl certifikát poslán síťovým serverem nebo manažerem spojení A, manažer spojení B přijme certifikát a zajištění bezpečnosti B (jestliže B je bezpečnostní server, je tato funkce prováděna manažerem spojení) legalizuje certifikát (kroky 1480 - 1482). Je-li certifikát neplatný, pak manažer spojení B zaznamená, že je spojení ukončeno a informuje o tom buď žadatele, nebo banku (kroky 1486 - 1492) (jestliže B je bezpečnostní server, pak B pouze zaznamená, že se převod ukončil).

Je-li certifikát platný, zajištění bezpečnosti B zkontroluje, zda je A na seznamu neplatných ID (kroky 1494 - 1496). Jestliže A je na seznamu, spojení je ukončeno. Jestliže A není na seznamu, pak generátor náhodných čísel B vytvoří náhodné číslo $R(B)$ a ověřovací zprávu B (krok 1498). Hodiny/časovač B obnoví čas a datum (krok 1500). Zajištění bezpečnosti B sestaví $R(B)$, ověřovací zprávu B, čas a datum ve jednu zprávu (krok 1502). Veřejný klíč B zašifruje tuto zprávu pomocí veřejného klíče A a manažer spojení B připojí certifikát B k zašifrované zprávě a pošle zprávu k A (kroky 1504 - 1506).

Manažer spojení A přijme zprávu, veřejný klíč A dešifruje zašifrovanou část zprávy, a zajištění bezpečnosti A legalizuje certifikát B (kroky 1508 - 1514). Je-li certifikát neplatný, manažer spojení A zaznamená ukončení spojení a informuje buď klienta nebo banku (kroky 1516 - 1522). Je-li certifikát platný, zajištění bezpečnosti A zkontroluje, zda B je na seznamu neplatných id (kroky 1524 - 1526). Je-li B na tomto seznamu, je spojení ukončeno. Není-li B na tomto seznamu, zajištění bezpečnosti A obnoví čas a datum a porovná je s datem a časem příslušejícím B (kroky 1528 - 1530). Jsou-li datum a čas mimo rozmezí, je spojení ukončeno.

Jsou-li čas i datum v rozmezí, pak generátor náhodných čísel A vytvoří náhodné číslo $R(A)$ a ověřovací zprávu A (krok 1532). Zajištění bezpečnosti A pak vytvoří spojovací klíč pomocí funkce $R(A) \text{ XOR } R(B)$ (krok 1534). Ověřovací zpráva čísla A,

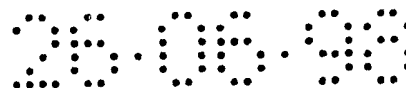


ověřovací zpráva čísla B, čas, datum a $R(A)$ jsou složeny do jedné zprávy a zašifrovány veřejným klíčem B (krok 1536). Zpráva je poslána do B manažerem spojení A (krok 1538). Manažer spojení B přijme zprávu, Veřejný klíč B dešifruje zprávu a zajištění bezpečnosti B zkontroluje ověřovací zprávu B (kroky 1540 - 1546). Je-li ověřovací zpráva B je nesprávná, pak je spojení ukončeno. Je-li ověřovací zpráva B správná, pak zajištění bezpečnosti B vytvoří klíč spojení pomocí $R(A) \text{ XOR } R(B)$ (krok 1548). Datum a čas jsou obnoveny a pro kontrolu porovnány s časem A, aby se zkontrolovalo, zda jsou v předem určeném povoleném pásmu odchylek (krok 1550). Nejsou-li, je spojení ukončeno. Jsou-li v tomto povoleném pásmu, pak manažer spojení B zaznamená počátek spojení (krok 1552).

Manažer spojení B pak pošle vyrozumění a ověřovací zprávu A do A (kroky 1554 - 1556). Manažer spojení A tuto zprávu přijme a zabezpečení bezpečnosti A zkontroluje ověřovací zprávu A (kroky 1558 - 1562). Není-li ověřovací zpráva v pořádku, spojení je ukončeno. Je-li v pořádku, manažer spojení zaznamená počátek spojení (krok 1564).

Převod poukázek

Obr. 8 ukazuje protokol převodu poukázek. Adresář poukázek X vybere poukázku(y), a hodnotu(y) pro převod, obnoví hodnoty poukázky(zek) a sekvenční číslo(a) a potom posílá zprávu do jednotky poukázky (krok 1566). Možné úlohy pro volbu poukázek pro převod mohou například být: (1) minimalizace počtu digitálních podpisů (ty potřebují pro zpracování jistý čas); (2) minimalizace velikosti tzv. paketů; (3) maximalizace užitečnosti elektronických poukázek ponechaných převádějícímu klientovi (tj. postoupení poukázek s nejkratší zbývající platností tj. do konce expirační doby). Tyto úlohy mohou být vyřešeny pomocí následujícího algoritmu převodu poukázek: (1) určete všechny možné alternativy, s nejmenším počtem poukázek; (2) určete, které z těchto alternativ mají nejmenší počet převodů; (3) jestliže zůstane více než jedna možnost z kroku 2, vyberte tu, která představuje nejmenší počet peněžních



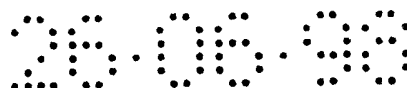
jednotkových dní. Peněžní jednotkové dni = zbytková hodnota poukázky k převodu násobená počtem dní zbývajících do vypršení expirační doby, sečteno pro všechny poukázky v paketu.

Poukázky X, při přijímání zprávy od adresáře poukázek X vytvoří převod, který má být připojen ke každé poukázce, která se přenáší (krok 1568). Veřejný klíč X vytvoří podpis(y)⁵ pro poukázku(y) (krok 1570). Manažer paketů X poté sjednotí poukázky s jejich novými převod(y), a podpisem (podpisy)⁶ do jednoho paketu a pošle jej do Y (kroky 1572 - 1574). Manažer paketů Y přijme paket a rozebere jej (krok 1576).

Ověřovatel Y legalizuje všechny certifikáty v poukázce(kách) (např. certifikát peněžního generátoru, a všechny převodové certifikáty). Potom ověření Y zkontroluje, zda identifikační čísla v převodové skupině odpovídají modulovým identifikačním číslům certifikátu v podpisu a skupině certifikátů v celé historii elektronické poukázky. Také je legalizována konzistentnost částky převodu pro každou poukázku a to tím, že v průběhu historie elektronické poukázky je zajištěno, aby částka přenášená v každém následném kroku byla nižší než u bezprostředně předcházejícího převodu. Navíc, aby bylo jisté, že celková převáděná částka je rovna částce očekávané, je kontrolována její výše (kroky 1578 - 1580). Jestliže výše částek nesouhlasí, je převod zrušen (krok 1582).

Jestliže to platí a Y je převodní peněžní modul, pak ověřovatel Y ověřuje expirační data poukázky (poukázek) (kroky 1584 - 1588)⁷. Je-li některá z poukázek prošlá, je převod přerušen. Jestliže není žádná prošlá, pak ověřovatel Y porovná každé id se seznamem neplatných id (kroky 1590 - 1592). Je-li některé převodové id na seznamu neplatných id, je převod přerušen.

Jestliže převodová id nejsou na seznamu neplatných id (nebo Y není převodní peněžní modul), veřejný klíč Y ověří platnost podpisů poukázek (kroky 1594 - 1596). Je-li některý podpis neplatný, je převod přerušen. Jsou-li podpis platný, ověřovatel Y zkontroluje, zda obsah poukázky odpovídá obsahu poukázky uschované v Aplikaci Poukázek nebo umístěné v Zápis o převodu



Tran Log (kroky 1598 - 1600). Pro každý obsah poukázky, který odpovídá, je pro převod poukázky vytvořeno schema typu strom, aby bylo možno určit, zda poukázka nebyla nějak duplikována (kroky 1602 - 1604). Byla-li některá poukázka duplikována, je převod přerušen. Tato kontrola duplikace (tj. kroky 1598 - 1604) je zejména zaměřena na a dobře eliminuje kriminální živly, pokoušející se získat pro sebe peníze převodem poukázek pomocí úmyslného zneužití ohroženého převodového peněžního modulu.

Nebyly-li nalezeny duplikáty, ani nebyly identifikovány žádné souhlasy obsahu poukázek, poukázky Y umístí poukázku(y) do peněžní schránky (krok 1606). Nakonec, adresář poukázek Y aktualizuje umístění a hodnotu(y) poukázky (poukázek), a také inicializuje sekvenční číslo(čísla) (krok 1608).

Mohlo by se říci, že postup při převodu poukázek obsahuje kroky pro aktualizaci a inicializaci sekvenčních čísel k usnadnění odsouhlasení poukázek (viz "Odsouhlasení poukázaných peněz"), které kontrolují, zda příjemce jakékoli poznámky je na seznamu neplatných Id, a zda jsou poukázky duplikovány. Tyto přídatné rysy a kroky prakticky znemožňují pachatelům uvádět do oběhu a cirkulovat duplikované poukázky, a zvyšují schopnost zjišťovat duplikované poukázky v oběhu.

Zahraniční směna

Obr. 9 ukazuje protokol pro zahraničního směnného převodu peněz při použití dolarů a liber jako příkladů peněžních jednotek. Nejprve, A souhlasí směniti dolary s B za libry (£) ve směnném kurzu \$/£ (krok 1602). A i B potom přihlásí své peněžní moduly a ty vyžádají od svých klientů typ převodu (kroky 1604 - 1610). A si vybere nákup cizí měny a B si vybere prodej cizí měny (kroky 1612 - 1614). A a B vytvoří bezpečné převodové spojení (kroky 1616 - 1620).

Ke klientovi A pobídne majitele/držitele A o částku podle typu dolarových bankovek, které si přeje vyměnit (krok 1622). Platba/směna A přijme částku a adresář poukázek A zkontroluje, zda A má dostatek prostředků (kroky 1624 - 1628). Nejsou-li



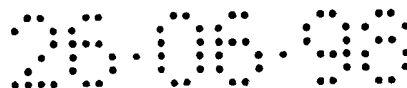
prostředky dostatečné, pak funkce *ke klientovi A* požádá o zadání nové částky, u které je znovu zjišťováno, zda je kryta existujícími fondy (kroky 1630 - 1632). Není-li zadána nová částka, je převod přerušen (krok 1634).

Jsou-li prostředky dostatečné, platba/směna A pošle dolarovou částku k B (kroky 1636 - 1638). Ke klientovi B poté požádá majitele/držitele o zadání buď částky v librách, kterou si přeje vyměnit za dolary, nebo alternativně pouze směnného kursu dolarů (krok 1640). Adresář poukázek B zkontroluje, zda jsou fondy dostatečné (kroky 1642 - 1644). Nejsou-li dostatečné, pak funkce *ke klientovi B* požádá o nový kurz a znovu se zkontroluje, zda jsou dostatečné existující fondy. Není-li však vybrán nový kurz, pak platba/směna B informuje A o jeho nedostatečných fondech (kroky 1650 - 1652). A potom může vybrat novou částku pro směnu, nebo převod zrušit (kroky 1630 - 1634).

Má-li B dostatečné fondy pro převod, platba/směna B pošle A vyrozumění i částku liber k směně (je také poslán ekvivalentní kurz) (kroky 1654 - 1656). Ke klientovi A vyzve ke kontrole obnosu v librách i kurzu (kroky 1658 - 1660). Jsou-li tento obnos a kurz nesprávné, pak platba/směna informuje B, že obnos a kurz jsou nesprávné (kroky 1662 - 1664). Funkce *ke klientovi B* potom požádá o nový kurz (kroky 1666 - 1668). Není-li zvolen nový kurz, pak je převod přerušen (krok 1670).

Jestliže však A ověří správnost obnosu i kursu převodu, platba/směna A postoupí dolarovou částku peněžní schránce (krok 1672). Dolarové poukázky jsou pak převedeny z A do B (krok 1674). Platba/směna B postoupí částku liber své peněžní schránce (krok 1676). Librové poukázky jsou pak převedeny z B do A (krok 1678).

V tomto bodě převodu, oba A i B dočasně drží cizí směnné poukázky ve správných částkách. A i B se oba zúčastnili dvou převodů: převody A: (1) A převedl dolary k B; (2) A přijal libry od B. Převody B: (1) B převedl libry A; (2) B přijal dolary od A. K dokončení převodu cizí směny musí nyní A předat (tj., dokončit a trvale zapsat do svého záznamu o převodu) oba své převody. Podobně, B musí odevzdat oba své převody. Všimněte



si, že A může dokončit převod cizí měny $A \rightarrow B$ (dolary z A do B) a $B \rightarrow A$ (libry z B do A) odděleně. Podobně B může dokončit převod cizí měny $A \rightarrow B$ a $B \rightarrow A$ odděleně.

Další díl protokolu cizí směny je navržen tak, že žádná skupina nezná pořadí, ve kterém bude proveden převod mezi převodními peněžní moduly. Tato nejistota odradí kohokoliv od účelových pokusů falšovat převody. Podstatou toho je, že funkce $S(X)$ je definována tak, aby $S(0) = A$ a $S(1) = B$, kde A a B představují peněžní moduly A a B. Tedy, jestliže X je náhodně vybráno jako 0 nebo 1, pak je náhodně vybírán i peněžní modul A nebo B.

Následující postup je použit proto, aby umožnil A a B společné určení náhodného X. $R(A)$ a $R(B)$ jsou náhodná čísla generovaná postupně A a B během podprogramu vytvoření spojení. Parita $R(A) \text{ XOR } R(B)$ je stanovena (pomocí exkluzivního OR pro každý bit $R(A) \text{ XOR } R(B)$). Tato parita je náhodné číslo X. $\underline{X}$ je doplněk k X ($\underline{X} = X \text{ XOR } 1$)⁸.

Opět podle Obr. 9, Záznam o převodu A podmíněně aktualizuje svůj záznam o převodu aby zaznamenal převod $S(X)$ do $S(\underline{X})$ (krok 1680). Je-li X generováno tak, že se rovná 0, pak je podmíněně zapsán převod z A do B (tj. dolarový převod). Je-li X generováno tak, že se rovná 1, pak je podmíněně zapsán převod z B do A (tj. převod liber). Protože záznam je zapsán podmíněně, můžeme se k němu vrátit, když peněžní modul A přeruší převod. Aktualizace záznamu se stává trvalou v okamžiku, kdy tato byla nastavena nepodmíněně (buď jako je explicitně ukázáno ve vývojovém diagramu nebo implicitně při dokončení převodu). Manažer spojení A potom pošle zprávu "záznam aktualizován" k B (kroky 1682 - 1684). V odpovědi na to, záznam o převodu B také podmíněně aktualizuje záznam, aby zaznamenal převod $S(X)$ do $S(\underline{X})$ (krok 1686).

Jestliže $X = 1$, pak záznam o převodu B nastaví aktualizaci log jako nepodmíněnou (kroky 1688 - 1690). Tedy, v tomto bodě B odevzdalo své převody liber A. Dále postupuje B podle předávacího protokolu závazek (krok 1692), který je popsán dále s odkazy na Obr. 10. V této situaci, A se zavazuje k provedení

obou svých převodů (tj. převádí dolary a přijímá libry) a B se zavazuje k provedení svého zbývajícího převodu, tj. přijímá dolary.

Jestliže však $X = 0$ (krok 1688), manažer Spojení B pošle k A zprávu pošli zprávu zahájení závazku (kroky 1694 - 1696). Záznam o převodu A potom nastaví jeho aktualizaci na nepodmíněnou (krok 1698), a tak realizuje svůj převod dolarů. Protokol o závazné realizaci převodu z obr. 10 je pak aktivován⁹ (krok 1700). Během provádění tohoto protokolu (popsaného dále) zrealizuje B oba své převody (tj., převod liber a příjem dolarů) a A se odhodlá k jednomu svému zbývajcímu převodu, příjmu liber.

Jak je možno vidět, zahraniční směnný převod, F/X , se zavazuje ke každému z převodů poukázek, což znemožňuje jejich duplikování, které by se mohlo vyskytnout, pokud by zde byl pouze jeden závazek. Protokol zahraniční směny zajišťuje, že žádná strana neví, který převod bude realizován jako první (převod dolarů týkající se A nebo převod liber týkající se B). Toto redukuje podněty některé ze stran zneužívat tento převod. Každý převod je realizován odděleně, ale jejich pořadí je vybráno náhodně pomocí dvou modulů. Strana, která se pokouší zasahovat do převodu, má 50% pravděpodobnost, že přijde o své peníze. Také neexistuje žádný jiný popud k zásahu do provedení, jelikož ztracené peníze mohou být vyžádány zpět (viz reklamace ztracených peněz)

Závazek

Obr. 10 ukazuje protokol o závazném prohlášení pro moduly. Manažer spojení X pošle k Y zprávu "připraven ke splnění závazku převodu" (kroky 1702 - 1704). Ten postoupí zprávu "připraven ke splnění závazku převodu" modulu přijímajícímu zprávu. Podle konvenčního scénáře peněžních převodů je tato technika (využívající zatížení břemenem závazného prohlášení předem), použita tak, aby strana převádějící peníze je nejprve odevzdala, což eliminuje možnost duplikace peněz.

Manažer spojení Y potom pošle oznámení k X (kroky 1706 - 1708) a realizuje všechny zbývající převody pomocí aktualizace svého záznamu o převodech (krok 1710). Také, pokud Y je převodní peněžní modul, pak funkce ke klientovi Y informuje klienta o úspěšném převodu (kroky 1712 - 1714). Manažer spojení Y zaznamená konec spojení (krok 1716).

Záznam o převodu X přijme oznámení od Y a aktualizuje svůj záznam o převodu, čímž realizuje všechny zbývající převody. X ukončí své převody stejně jako Y (kroky 1718 - 1724).

Přerušení převodu

Obr. 11 ukazuje protokol přerušení převodu pro moduly elektronického monetárního systému. Manažer spojení X zruší zpětně změny a zaznamená, že převod byl přerušen (krok 1726). Manažer spojení X potom zkontroluje, zda zpráva "připraven ke splnění závazku převodu" byla odeslána (kroky 1728 - 1730). Je-li tomu tak, X aktualizuje svůj záznam o převodu (krok 1732) zápisem o tom, že X přerušil po odeslání zprávy "připraven ke splnění závazku převodu" a zapsáním identifikátorů poukázek a obnosů každé poukázky přijaté během protokolu převod poukázek. Tedy, protokol o přerušení shromažďuje informace když je během selhání podprogramu závazek volán podprogram přerušení.

Jestliže X je převodní peněžní modul 1186, a zpráva "připraven ke splnění závazku převodu" byla odeslána, pak funkce ke klientovi X informuje své klienty o tom, že převod byl přerušen a že mohly nastat chyby v převodu peněz (kroky 1734 - 1738).

Jestliže X je bankomat 1188, pak funkce k bance X informuje banku, aby obrátila své účetní převody (vhodným má dátí a dal) (kroky 1740 - 1742). Jestliže X je převodní peněžní modul 1186 a žádná zpráva "připraven ke splnění závazku převodu" nebyla odeslána, pak ke klientovi X informuje klienta o tom, že převod byl přerušen (krok 1744).

Ve všech případech manažer spojení X posílá k Y zprávu o tom, že převod nemůže být dokončen (kroky 1746 - 1748). Manažer spojení Y zpětně zruší provedené změny a zaznamená, že převod



byl přerušen (krok 1750). Y pak informuje své klienty, že převod byl přerušen (kroky 1752 - 1754) nebo informuje banku, aby obrátila své účetní převody (kroky 1756 - 1758).

Jak je popsáno, je-li převod přerušen během protokolu závazek k převodu, je možné, že poukázky budou ztraceny. Jestliže se toto stane, příjemce poukázky bude mít přerušen převod a odesílatel poukázky bude mít ukončen převod poukázky. V tomto případě peněžní modul příjemce zaznamená informaci o poukázkách, které měly být přijaty a upozorní klienty, že zde může být vzniknout potencionální problém (tj., neobdržel poukázky poslané od A). Za těchto okolností by se dalo říci, že modul plátce správně převedl poukázky.

Klient peněžního modulu příjemce může potom nárokovat peníze u certifikační agentury. Informace týkající se nároku bude obsahovat záznam o převodu, který selhal. Certifikační agentura může potom zkontrolovat s vydávajícími bankami, zda byly poukázky uvedeny do pořádku. Po určité době, pokud nebyly poukázky uvedeny do pořádku, může klient může své peníze nárokovat.

Platba na místě prodeje (Point of Sale, dále POS)

Obr. 12 ukazuje platební protokol pro místo prodeje POS. Platební protokol POS¹⁰ je určený k zjednodušení plateb uskutečněných mezi převodním peněžním modulem kupujícího 1186 a převodním peněžním modulem prodávajícího 1186. Převodní peněžní modul prodávajícího 1186 může, např. být umístěn v hotovostní pokladně supermarketu.

Nejdříve souhlasí A s nákupem produktů nebo služeb od B (krok 1760). Majitel/držitel převodního peněžního modulu A se přihlašuje na svůj peněžní modul (krok 1762). Ke klientovi A požádá majitele/držitele o převod a A si zvolí platbu na místě prodeje, POS, (kroky 1764 - 1766). Současně, prodejce stanoví celkovou nákupní cenu (krok 1768). Ke klientovi B požádá o převod a B si zvolí možnost přijmout platbu POS (kroky 1770 -



1772). A a B potom vytvoří bezpečné spojení (kroky 1774 - 1776).

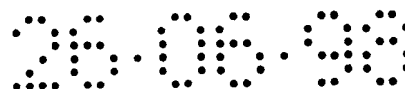
Ke klientovi B požádá o částku platby a platba/směna B přijme obnos a pošle jej A (kroky 1778 - 1782). Ke klientovi A pak požádá svého klienta, aby ověřil požadovanou částku (kroky 1784 - 1786). Navíc je klient požádán, aby zvolil poukázku, ve které bude platit (např. měna nebo úvěr), a částku tak, aby se součet rovnal požadované částce. Jestliže požadovaná částka není správná, pak platba/směna A pošle k B zprávu o tom, že požadovaná částka je nesprávná (kroky 1788 - 1790). Ke klientovi B potom požádá svého hostitele o novou částku (kroky 1792 - 1794). Není-li částka není zvolena, je převod přerušen (krok 1796).

Je-li požadovaná částka správná, platba/směna A přijme obnos podle typu poukázky (krok 1798). Adresář poukázek A pak zkontroluje zda jsou fondy dostatečné (kroky 1800 - 1802). Nejsou-li fondy nedostatečné, pak ke klientovi A požádá o nové částky podle typu poukázky (kroky 1804 - 1806). Není-li zadána nová částka, pak platba/směna A pošle B zprávu, že nemá dostatečné fondy (kroky 1808, 1790). Ke klientovi B požádá hostitele o novou částku (kroky 1792 - 1794). Není-li nová částka zvolena, je převod přerušen (krok 1796). Je-li zvolena nová, pak převod platby začne znovu.

Jsou-li jsou fondy dostatečné, pak platba/směna A postoupí částku peněžní schránce (krok 1810). Poukázky jsou poté převedeny z A do B (krok 1812). Nakonec, převodní peněžní moduly závazek převodu dokončí (krok 1814).

Jak je možné vidět, POS platba je pro kupujícího zjednodušena, neboť je to platba inicializovaná věřitelem. Obecně, POS platba by byla použita pro platbu obchodníkům za zboží, zatímco platba klienta klientovi (subscriber-to-subscriber, dále STS) by byla použita k placení jednotlivcům nebo k placení účtů.

Aktualizace úvěru vydávající banky



Obr. 13 ukazuje protokol Aktualizace úvěru po převodu vydávající banky, a zejména popisuje, jak klienti získají úvěrovou poukázku, která je autorizovaným nositelem úvěrové platby. Klient může mít až jednu úvěrovou poukázku pro každý úvěrový účet, který vlastní. Všimněte si, že každá banka, která dovolí klientovi přijmout aktualizovanou úvěrovou poukázku je vydávající bankou pro tyto úvěrové poukázky.

Postup při zavádění aktualizovaného úvěrového převodu začíná zavedením úvěru mezi peněžním modulem A a bankovním bankomatem modulu B (krok 1854), který je zde popsán dále s odkazy na Obr. 14.

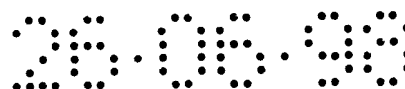
Zavedení úvěru

Postup zavedení úvěru pro výběr peněz začíná tím, že se vlastník/držitel převodního peněžního modulu A rozhodne aktualizovat úvěr a přihlásí se ke svému peněžnímu modulu (krok 1876). Na příklad, klient A může vlastnit úvěrovou poukázku, ale přeje si změnit (tj. zvýšit nebo snížit) úvěrovou částku, včetně snížení částky až na nulu, nebo nemusí v daném okamžiku vlastnit úvěrovou poukázku, ale přeje si ji získat. Ke klientovi A požádá držitele/vlastníka o převod a A si vybere možnost aktualizovat úvěr určité částky určité banky a určitého účtu (kroky 1878 - 1880). V tomto provedení je aktualizovaná úvěrová částka specifikovaná klientem A celkovou úvěrovou částkou, kterou si přeje mít klient A. Potom převodní peněžní modul A započne proceduru komunikace s bankou, která byla vybrána sítí pomocí procedury přihlášení do sítě popsané výše (krok 1882).

Po dokončení kroků přihlášení peněžního modulu, výběru převodu a přihlášení do sítě, vytvoří A a B bezpečné spojení (krok 1884).

Pak převodní peněžní modul A vytvoří žádost o úvěr od modulu bankomatu B (krok 1886), podle procedury žádost o úvěr podrobněji popsané s odkazem na obr. 15.

Žádost o úvěr



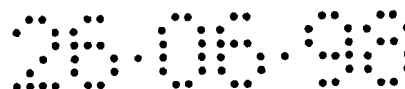
S odkazy na Obr. 15 bude popsán postup pro vyžádání úvěru. Mělo by se říci, že ačkoli tento obrázek používá k označení stran X a Y v krocích postupu níže popsanych, je možné je aplikovat na jakýkoliv peněžní modul obchodující s modulem bankomatu.

Je-li na začátku úvěrová poukázka pro vybraný účet, adresář poukázek X pošle částku této úvěrové poukázky na k bankomatu X (krok 1897). K bankomatu X určí čistý rozdíl mezi celkovou úvěrovou částkou požadovanou klientem A a částkou úvěrové poukázky a pošle úvěrovou aktualizovanou žádost modulu bankomatu, a přitom požaduje určitou čistou částku z úvěru, který má být autorizován ze specifického účtu. V tomto převodu aktualizované úvěrové žádosti bude číslo účtu a profil účtu převeden z žádajícího peněžního modulu na modul bankomatu společně s čistou úvěrovou částkou (krok 1898). Tato zpráva je poslána podle protokolu pošli zprávu (krok 1900), ve kterém je zpráva zašifrována pomocí popsanych šifrovacích technik.

Jakmile jsou žádost o úvěrový výběr a číslo a profil účtu převedeny modulu bankomatu, je iniciována procedura legalizace čísla účtu (krok 1902). Vývojový diagram popisující, jak je číslo účtu legalizováno je na Obr. 20, který je dále odděleně popsán pro objasnění.

S legalizací účetních informací, funkce *k bance Y* ověřuje, zda úvěr pro zajištění požadované aktualizace úvěru je dostatečný (krok 1904). Dostatečný úvěr vyvolá u funkce *k převodu Y* závazek k převodu pro X, které přijme vyrozumění prostřednictvím své aplikační funkce *k bankomatu* (kroky 1906 - 1912).

Nedostatečná úvěrová výše však způsobí, že klient bude požádán o zadání nové částky pro aktualizaci úvěru (kroky 1914 - 1918, Obr. 15B). Vstup nové částky pro aktualizaci úvěru od klienta povede k zaslání nové úvěrové částky pomocí funkce *k bankomatu* funkcí *k bankovní aplikaci peněžního modulu bankomat*, aby se ověřilo, zda fondy stačí ke krytí naposled žádané částky (kroky 1922 - 1924), a dále se vracíme ke kroku 1904 podle Obr.

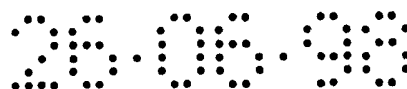


15A. Není-li klientem žádána žádná nová částka, je převod přerušen (krok 1926).

Vraťme se k Obr. 14, po návratu z programu realizujícího žádost o úvěrový výběr. K bankomatu A zahájí převod všech bankovek, převáděných úvěrových poukázek (tj. úvěrových poukázek přijatých v předchozích převodech) a úvěrových poukázek pro tento účet k peněžnímu modulu bankomatu (krok 1888). Nejsou-li v době, kdy je žádost úvěrového výběru vytvářena, v převodním peněžním modulu žádné bankovky, pošle funkce *k bankomatu A* zprávu peněžnímu modulu bankomatu, že zde nejsou žádné bankovky (kroky 1892 - 1894). Jestliže jsou bankovky v převodním peněžním modulu, pak jsou elektronické poukázky převedeny z A do bankomatu B funkcí *převod poukázek* popsané výše s odkazem na Obr. 8 (krok 1896).

Podle Obr. 13, funkce *k převodu B* kontroluje, zda všechny bankovky a převáděné úvěrové poukázky byly skutečně převedeny (kroky 1856 - 1858), a jestliže některé z těchto poukázek (bankovek) byla skutečně převedena z převodního peněžního modulu A, účetní převody odrazí zaznamenají tuto situaci pomocí funkce *B k bance* (krok 1860). V obou případech, jak v případě, kdy nebyly převedeny žádné poukázky z peněžního modulu, tak po účetních převodech provedených v kroku 1860, se vytvoří spojení mezi peněžním modulem bankomatu a modulem peněžního generátoru (krok 1862). Funkce *k bance B* aktualizuje úvěrové spojení přidáním částky úvěrové poukázky (pokud existuje) do dostupné úvěrové výše, aby zjistila celkový dostupný úvěr a odečetla požadovanou úvěrovou částku od celkového dostupného úvěru. Jestliže není třeba vytvořit poukázky (včetně bankovek a úvěrových poukázek), protože požadovaná částka byla nulová a žádné bankovky nebyly převedeny, pak peněžní moduly dokončí převod podle procedury závazek popsané výše s odkazem na Obr. 10 (kroky 1865 - 1875).

Je-li třeba vytvořit nějaké poukázky (úvěrové nebo bankovky) v důsledku nenulové úvěrové žádosti a / nebo převedených bankovek, pak jsou vyžádány bankovky bankomatem B od modulu generátor peněz podle procedury *žádost o bankovky* (kroky 1865 -



1866). Bankovky vyžádané v generátoru peněz jsou převedeny do modulu bankomat B pomocí funkce převod poukázek popsané výše (viz Obr. 8) pro převod elektronických poukázek (krok 1868). Poukázky jsou poté převedeny z modulu bankomatu B na převodní peněžní modul použitím stejné funkce převod poukázek (krok 1870). Nakonec, aby se úspěšně dokončila procedura aktualizace úvěru, peněžní modul dokončí převod podle procedury závazek popsané výše s odkazem na Obr. 10. Funkce závazek je iniciována nejprve převodním peněžním modulem uzavírajícím svůj převod s modulem bankomatu B (krok 1872). Pak funkce závazek realizuje převod mezi moduly Bankomat B a generátor peněz (krok 1874). To dokončí jednu úplnou aktualizaci úvěru od vydávající banky.

Odsouhlasení vydaných peněz

Postup při odsouhlasení poukázky/bankovky kontroluje padělání a duplikaci poukázky/bankovky a je popsán pomocí odkazů na Obr. 16 a 17. Systém odsouhlasení vydaných peněz, založený na informaci uložené v řídicím souboru vydané peníze, vytváří strom převodu poukázky, který modeluje historii převodu poukázky.

Obr. 16 schematicky ilustruje hypotetickou řadu převodů mezi generátorem peněz s identifikačním číslem "1" (dále generátor peněz 1), a modulem bankomatu s identifikátor "2" (dále modul bankomatu 2), a čtyř převodních peněžních modulů s celočíselnými identifikátory 3 až 6 (dále převodní moduly 3 - 6), přidruženými k jedné poukázce generované generátorem peněz 1 v čase/datu označeném jako 1:00:00.

V souladu s příkladem historie převodu ukázaným na Obr. 16, ilustruje Obr. 17, jak převod elektronické reprezentace hotovosti vytváří stromu podobnou strukturu elektronické reprezentace hotovosti odvozené od počáteční poukázky vytvořené modulem generátoru peněz. Tak, jak jsou ukládány nebo vráceny jednotlivé převody (část větve stromu) poukázky bankovnímu systému podle aktualizace poukázky, tak je budován strom převodů poukázek na Obr. 17 pomocí zabudovaného systému odsouhlasení vydaných peněz. V tomto případě, generátor peněz 1



(modulové identifikátory jsou obsaženy v digitálně ověřených certifikátech) vytváří elektronickou reprezentaci hotovosti 2300 mající podstatnou skupinu datových polí a převodovou skupinu datových polí, které jsou ukázány schematicky v detailu pro jasnost výkladu. Mimoto pro zjednodušení není ukázána skupina datových polí podpisů a certifikátů.

Hlavní skupina podstatných datových polí obsahuje identifikátor poukázky (např., "N12"), identifikátor modulu peněžního generátoru (např. "MG1"), identifikátor vydávající banky (např. "Jméno Banky"), datum vydání (např. 1:00:00), datum expirace (např., 12:00:00), částku poukázky a identifikátor peněžní jednotky (např., \$50). Jiná datová pole hlavní skupiny jako typ poukázky nejsou pro zjednodušení ukázány. Různá datová pole v elektronických poukázkách jsou ukázána z ilustrativních důvodů ve formě den: hodina: minuta. Jiné formy monitorování (např. včetně sekund) jsou také možné.

Převodová skupina datových polí obsahuje převodní záznam obsahující identifikační číslo příjemce, datum převodu, a převáděnou částku. Převodová skupina také s výhodou obsahuje sekvenční číslo, které je obohaceno o poukázkový adresář plátce po každém převodu. Normálně by měly být čas/datum a převodové id dostatečné k jednoznačné identifikaci převodu. Je však možné, že převod, převodové id, čas/datum a částka mohly být duplikovány, pokud byl upraven čas mezi převody a stejně velká částka je převáděna na stejný modul. Aby se předešlo tomuto problému, je k převodnímu záznamu a poukázkovému adresáři s výhodou přidáno sekvenční číslo k jednoznačné identifikaci převodu. Sekvenční číslo je přidáno k adresáři poukázky po každém převodu. Je-li sekvenční číslo nově nastaveno, pak to bude detekováno jako duplikát.

Tedy, když je elektronická reprezentace hotovosti 2300 převedena k bankomatu 2, převodní záznam 2302 je připojen k převodní skupině a obsahuje identifikační číslo příjemce (např. "2"), datum převodu (např. 1:00:00), převáděnou částku (např. \$50), a sekvenční číslo (např. "1"). Pro přehlednost ukazují poukázkové převody na Obr.17 jen nově připojené



převodní záznamy převáděné poukázky. Pro přehlednost není také ukázána převodní skupina datového pole ukazující celkový počet převodů.

Elektronická representace hotovosti 2300 z peněžního generátoru 1 je uchována v modulu bankomatu 2. Jako část výběru \$50 převodním modulem 3, modul bankomatu 2 vytvoří elektronickou representaci hotovosti pomocí připojení převodního záznamu 2304 ke kopii datových polí v elektronické representaci hotovosti 2302 zvětšené o převodní záznam 2302. Tato poukázka je poté uložena v převodním modulu 3 do dokončení výběru. To lze chápat tak, že každý uzel stromu převodu poukázky ukazuje nově připojenou část převodového záznamu převáděné poukázky.

Representován stromem převodu poukázky, v 1:00:05, převodní modul TR3 platí \$10 převodním záznamem 2306 převodnímu modulu 4. V 1:01:00, převodní modul 3 platí \$10 převodním záznamem 2308 převodnímu modulu 5. V 3:08:01 převodní modul 3 platí \$25 převodním záznamem 2310 převodnímu modulu 5. V 4:11:08 převodní modul 3 převádí \$5 pomocí převodního záznamu 2312 převodnímu modulu 6.

V 2:00:01 převodní modul 4 převede \$5 převodním záznamem 2314 převodnímu modulu 6. V 2:01:07 převodní modul 4 převede dalších \$5 převodním záznamem 2315 převodnímu modulu 6, který obratem v 3:07:05 převede \$5 převodnímu modulu 3 převodním záznamem 2321.

V 2:00:06 převodní modul 5 převede celou \$10 poukázku převodnímu modulu 3 převodním záznamem 2316. Z \$25 poukázky přijaté ve 3:08:01 převodním modulem 5 z převodového modulu 3 ve 3:09:12 převodní modul 5 zaplatí \$20 převodnímu modulu 6 převodním záznamem 2318, a uloží ve 4:12:05 zbývajících \$5 v modulu bankomatu 2 převodním záznamem 2320.

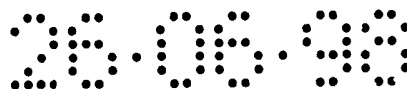
Ve 4:10:00 převodní modul 6 převede \$10 převodnímu modulu 5 podle převodního záznamu 2322, a v 5:00:06 převede zbývajících \$10 převodnímu modulu 3 převodním záznamem 2324. V souladu s provedením tohoto vynálezu se rozumí, že po uložení peněz z převodního modulu do banky všechny poukázky (včetně úvěrových



poukázek) převodního modulu jsou poslány bankovnímu systému a aktualizovány. V důsledku toho proběhne automaticky dodatečný a souběžný převod reprezentovaný převodním záznamem 2326. Je ve své podstatě simultánní s výše popsaným převodem¹¹ zálohou z převodního modulu 5 k modulu bankomatu 2, který je reprezentován převodním záznamem 2320. Potom bude generována peněžním modulem 1 nová poukázka o hodnotě \$5 (za předpokladu, že převodní modul nemá žádné úvěrové poukázky) a převedena do převodního modulu 3 prostřednictvím modulu bankomatu 2, spolu s připojenými příslušnými převodními záznamy (není vyznačeno). Souhlasně, může být přínosem, že aktualizace všech poukázek v převodním peněžním modulu po převodu (např. uložení nebo výběru) mezi převodním modulem a modulem bankomatu pomáhá postupu odsouhlasení poukázky poskytnutím dodatečných prostředků pro navrácení poukázek do bankovního systému.

V 5:00:10 převodní modul 3 uloží \$10 v modulu bankomatu 2 pomocí převodního záznamu 2328. Jak je popsáno výše pro uložení převodním modulem 5, souběžně s uložení převodním modulem 3, reprezentovaným převodním záznamem 2328, probíhá přídatný a souběžný převod (není uveden) všech poukázek vlastněných převodním modulem 3 k bankovnímu systému, včetně těch reprezentovaných převodním záznamem 2316 a převodním záznamem 2321. Poté, bankovní systém vrátí převodnímu modulu 3 poukázku s hodnotou rovnou součtu všech poukázek poslaných bankovnímu systému k aktualizaci (tj. \$15).

V této chvíli tedy pouze převodní modul 6 vlastní převoditelné doklady o původní poukázce 2300, jak je reprezentováno převodními poukázkami 2314 a 2312. Jestliže převodní modul 6 provede převod (např. uložení nebo výběr) s modulem bankomatu před tím, než převede tyto poukázky jiným převodním peněžním modulům, pak nebudou v oběhu žádné převoditelné poukázky, které by odkazovaly na původní poukázku 2300; všechny poukázky pocházející z převodů originální poukázky 2300 budou navráceny bankovnímu systému. To dovolí kompletní konstrukci stromu převodů poukázky ukázaného na Obr. 17. Datum expirace efektivně pomáhá při odsouhlasení



poukázky pomocí omezení období, kdy může být poukázka převedena.

Ze stromu převodů poukázky je zřejmé, že jestliže byla poukázka zfalšována, pak nebude hlavní část poukázky odpovídat prvnímu depositu. Jestliže byl převod duplikován, pak převody dole uvedené budou dávat větší součet, než nadřazená převodní částka. Například, jestliže převodní modul 6 převedl \$20 převodnímu modulu 3 v 5:00:06 místo \$10 (tj. převodní záznam 2324), pak převody pod převodním záznamem 2318 (tj. SEQ1, 3:09:12, TR6, \$20) by dávaly součet \$30 což znamená, že převodní modul 6 duplikoval převod.

Připojení peněžního modulu k bankovnímu účtu(tům) pro bankovní přístup

Obr. 18 ukazuje protokol pro připojení peněžního modulu k bankovním účtům pro bankovní přístup. Postup začne, když se klient(ka) identifikuje vůči reprezentantu zákaznické služby (Customer Service Representative dále CSR) a požádá CSR o připojení klientského účtu k peněžnímu modulu (krok 1928). CSR postoupí žádost CSM hostiteli A (CSMHA) ke spojení účtů pro identifikovaného klienta, a CSMHA získá přístup k informaci o účtu identifikovaného klienta z bankovního systému (kroky 1930 - 1934). Pak klient a CSR ověří informaci o účtu a klient vybere, které účty má spojit s peněžním modulem (krok 1936).

Po žádosti klienta, aby jeho/její peněžní modul B propojil bankovní účty a žádosti CSR, pomocí CSMHA a těchto bankovních účtů propojených pomocí CSMA, je vytvořeno bezpečné spojení mezi peněžním modulem klienta B a tímto CSMA (kroky 1938 - 1946). Poté, jako odpověď na žádost od funkce k hostiteli A patřící CSMA, CSMHA¹² pošle účetní informaci k CSMA, které přijme účetní informaci a vytvoří z nich profil účtu (kroky 1948 - 1952). Veřejný klíč A pak podepíše účtový profil a Vytvoření profilu účtu zkonstruuje zprávu z profilu účtu a podpisů a pošle ji peněžnímu modulu B (kroky 1954 - 1958). Zajištění bezpečnosti B přijme zprávu, a Veřejný klíč B



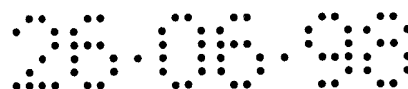
zkontroluje digitální podpisy na zprávě (kroky 1958 - 1952).
Nejsou-li podpisy platné, pak je spojení přerušeno (krok 1966).

Je-li podpis platný, pak ke klientovi B pošle profil k hostiteli, aby zákazník ověřil profil účtu. Jestliže zákazník neodsouhlasí profil účtu, je převod přerušen. Potvrdí-li zákazník profil, pak Zajištění bezpečnosti B přidá CSM certifikát k profilu účtu (krok 1968).

Funkce *k bankomatu B* pak zjišťuje, zda profil účtu je již uložen pro banku přidruženou s nově vytvořeným ("novým") profilem účtu. Jestliže profil účtu pro tuto banku již v aplikaci *K bankomatu B* existuje, pak jej *K Bankomatu B* nahradí novým profilem účtu; jinak, *K Bankomatu B* přidá nový profil účtu (kroky 1970 - 1974).

Opětovná legalizace připojení peněžního modulu k bankovním účtům

Obr. 19 ukazuje protokol opětovné legalizace připojení peněžního modulu k bankovním účtům prováděnou klientem. Postup začíná se přihlášením klienta na jeho/její peněžní moduly, a v odpověď na žádost o převod generovanou funkcí ke klientovi A, klient zvolí nové schválení spojení bankovního účtu s bankou spojenou s modulem zákaznických služeb (CSM) B (kroky 1978 - 1982). Peněžní modul vyvolá a postupuje podle protokolu síťového zápisu popsaného s odkazem na Obr. 6, výše, a tak se vytvoří bezpečné spojení mezi peněžním modulem A a CSMB (krok 1986). *K Bankomatu A* pak pošle profil účtu pro bankovní účty k CSMB (kroky 1988 - 1990). Vytvoř profil účtu B přijme zprávu, a Zajištění bezpečnosti B legalizuje CSM certifikát a podpis profilu účtu (kroky 1992 - 1995). Je-li certifikát nebo podpis neplatný, pak CSM přeruší převod (krok 2000). Je-li certifikát platný, funkce *k hostiteli B* pošle seznam účtů z profilu účtu k CSM hostiteli (CSMH), který porovnáním s použitím on-line bankovního systému zjistí, zda každý účet je právě nyní aktivní (kroky 1996 - 2001). Jestliže některý z účtů je prošlý, pak CSMH zašle zprávu o přerušení k CSM (krok 2010), který potom přeruší převod podle postupu přerušení (krok 2000).



Jsou-li jsou všechny účty aktivní, pak CSMH signalizuje instrukci o opětovné legalizaci k CSM, a funkce *vytvoř profil účtu* B přijme zprávu a vytvoří profil účtu z účetních informací (kroky 2002 - 2004). Veřejný klíč B potom podepíše profil účtu, a vytvoř profil účtu B zkonstruuje z profilu účtu zprávu a podpis a pošle ji peněžnímu modulu A (kroky 2006 - 2010). Veřejný klíč A přijme zprávu a ověří digitální podpis (krok 2012). Jestliže není podpis platný, pak peněžní modul A zruší převod (krok 2018); je-li platný, podpis profilu a CSM certifikát jsou přidány k profilu účtu (krok 2014) a peněžní modul A realizuje převod (krok 2016).

Legalizace čísla účtu

V souhlasu s provedením tohoto vynálezu užívajícího modul zákaznických služeb (CSM), který je popsán výše, je na Obr. 20 uveden vývojový diagram popisující, legalizaci čísla účtu. V tomto postupu zajištění bezpečnosti Y přijme číslo účtu a profil účtu, včetně certifikátu CSM a ověří certifikát CSM (krok 2020). Neplatný certifikát způsobí přerušení převodu mezi dvěma peněžními moduly (krok 2028).

Je-li certifikát platný, funkce *zajištění bezpečnosti Y* přenese profil účtu k veřejnému klíči Y k ověření CSM podpisu (krok 2022). Neplatný podpis způsobí, že Zajištění bezpečnosti Y informuje manažera spojení o tom, že profil účtu je neplatný (krok 2026), a převod mezi dvěma moduly je přerušen (krok 2028).

Jestliže test podpisu potvrdí jeho platnost, funkce pokračuje tím, že funkce *k bance Y* pošle číslo účtu, které přijal prostřednictvím bankovního on-line počítačového systému (krok 2024). Neaktivní účet způsobí, že funkce *zajištění bezpečnosti Y* informuje manažera spojení o neaktivním účtu (krok 2030) a přeruší převod (krok 2028); aktivní účet způsobí, že postup legalizace čísla účtu se vrátí k dalšímu kroku v operačního vývojového diagramu, který vyvolal postup při legalizaci čísla účtu.

Je zřejmé, že ve srovnání s tímto provedením vynálezu, které neobsahuje CSM, je postup při legalizaci čísla účtu pro modul bankomatu zjednodušen.

Reklamáce ztracených peněz

Jak bylo diskutováno, elektronické peníze mohou být ztraceny z několika důvodů, včetně: (1) peněžní modul je zničený a nefunkční; (2) peněžní modul je ztracený nebo ukradený; nebo (3) závazek nebyl splněn. Pro monetární systém je důležité, aby klient věřil, že jeho peníze jsou bezpečně uloženy. Je tedy důležité, aby příjemce byl schopen vyreklamovat peníze ztracené v důsledku systémového selhání. Schopnost směny peněz v případě poškození peněžního modulu by zlepšila pocit bezpečí, neboť elektronické selhání je pravděpodobnější, než ztráta papíru fyzickým zničením. Náhrada peněz z důvodu omylů plynoucích ze ztraceného nebo ukradeného peněžního modulu je problematičtější. Povolení takových reklamací by mohlo přilákat rozsáhlé reklamace v systému, pokud by klienti neučinili předběžné kroky proti takovým škodám.

Ve všech případech popsanych v tomto vynálezu existují metody, které dovolují náhradu peněz ztracených v některém z těchto případů. V prvních dvou případech (tj. případ (1) a případ (2) výše) by klient musel periodicky vytvářet požadavek na ztracenou poukázku(ky) (viz Obr. 21), který by byl uložen mimo peněžní modul. V případě selhání by požadavek mohl být předložen s klientovou identifikací u vydávající banky (viz Obr. 22). Požadavek by obsahoval poslední známý stav klientova peněžního modulu. Popis nárokovaných poukázek by byl legalizován a rozdělen vydávajícím bankám. Vydávající banky by mohly vyměnit peníze po jisté době, pokud by nárokované poukázky nebyly uloženy.

V případě, kdy není splněn závazek (tj. případ (3)) a je-li peněžní modul stále funkční (viz Obr. 22), je takový nárok reklamace vytvořen interaktivně mezi peněžním modulem a modulem zákaznických služeb. Tento požadavek, jako v případech (1) a (2), je postoupen vyšetřovacímu systému pro vydané peníze, který sleduje nároky proti úločkám peněz. Vydávající banky se



mohou cítit bezpečně při hrazení ztracených peněz, protože mohou monitorovat vstupující peníze proti přihláškám defraudantů a protože mají identifikaci toho, kdo se přihlašuje.

Tyto metody jsou podrobněji popsány u odkazů na Obr. 21 a 22.

Vytvoř nárok na ztracenou poukázku(y)

S odkazem na Obr. 21A, je ukázán postup při vytvoření nároku, reklamace, na ztracenou poukázku(y), který může být použit v souhlasu s provedením tohoto vynálezu. Postup začne, když se klient přihlásí k peněžnímu modulu; funkce *ke klientovi A* požádá klienta o převod a klient vybere možnost vytvoř nárok na ztracenou poukázku (kroky 2032 - 2036).

Poté následuje několik kroků, které konsolidují¹³ ty poukázky a nenárokované závazky, které selhaly (kroky 2038 - 2042). Specificky, adresář poukázek A vytvoří jedinečné pořadové číslo nároku (které je použito pro identifikaci požadavku) a převede kopii adresáře poukázek s pořadovým číslem k manažeru paketů. Funkce *poukázky A* převede kopie všech poukázek s podpisy a certifikáty do manažera paketů. Poté funkce *zápis o převodu A* odešle všechny nenárokované převody, co selhaly při realizaci, a ty, které byly přihlášeny při přerušení do manažera paketů.

Dále funkce *veřejný klíč A* používá soukromý klíč peněžního modulu k podpisu pořadového čísla požadavku, adresáře poukázek, poukázek, a selhání při realizaci, které byly poslány do manažera paketů, a manažer paketů připojí podpis k sloučeným datům, výsledkem čehož je paket sloučených dat (kroky 2044 - 2046), který je potom zašifrován pomocí veřejného klíče A (krok 2048). K zašifrovanému požadavku přidá veřejný klíč A poté popis požadavku skládající se z pořadového čísla požadavku, celkového monetárního obnosu požadavku, a certifikátu peněžního modulu A (krok 2050). Funkce *ke klientovi A* pošle tento požadavek k hostiteli peněžního modulu, který přijme a uloží požadavek -- na médiu fyzicky nezávislém na penězích -- pro budoucí použití (kroky 2052 - 2054).



Je tedy zřejmé, že postup reklamace ztracených poukázek poskytuje způsob pro generování a ochranu potenciálních finančních nároků, které nejsou zničeny poškozením či selháním peněžního modulu.

Reklamace Ztracené Poukázky

Obr. 22 ukazuje protokol pro reklamaci ztracených poukázek, který začíná klientovou žádostí o reklamaci ztracené poukázky vůči reprezentantovi zákaznických služeb (customer service representative) dále CSR, žadatelova identita je oznámena CSR (krok 2056). CSR pak předá klientovu identitu k hostiteli modulu zákaznických služeb (CSMH) A, a zkontroluje, zda reklamace je důsledkem nesplnění závazku nebo důsledkem ztráty či destrukce peněžního modulu (kroky 2058 - 2060). Jestliže důvodem k reklamaci je nesplnění závazku (a klientovy peníze nebyly ztraceny nebo zničeny), pak na základě klientovy volby reklamovat ztracené poukázky od peněžního modulu a volby CSR přijmout reklamace ztracených poukázek od peněžního modulu, manažer Spojení B klientova peněžního modulu a manažer Spojení A modulu zákaznických služeb (CSM) přidružený k reprezentantovi zákaznických služeb (prostřednictvím hostitele modulu zákaznických služeb (HCSM)) jsou každý zvlášť vyzváni k vytvoření bezpečného spojení mezi CSM A a peněžním modulem B (kroky 2062 - 2070).

Jakmile je spojení vytvořeno, funkce k hostiteli A patřící k CSM vyžádá identitu klienta a HCSM A odpoví na tuto žádost odesláním zprávy obsahující klientovu identitu k CSM (2072 - 2074). Reklamace ztracené poukázky A přijme tuto zprávu a pošle peněžnímu modulu B zprávu o tom, že reklamace má být poslána (kroky 2076 - 2078).

Zápis o převodu B přijme tuto zprávu a obnoví ty záznamy nesplnění závazku, které nebyly reklamovány (krok 2080). Nejsou-li nalezeny žádné záznamy nesplnění závazku, pak je převod přerušen (krok 2083). Jinak ke klientovi B pošle informaci (např. datum, čas, a výši obnosu) z obnovených záznamů o nesplnění závazku ke klientovi k přezkoumání (krok



2082). Z této informace klient vybere převody, které budou reklamovány (krok 2084). Na příklad, klient nevybere převody, u kterých nebyl splněn závazek, které byly řešeny jednotlivě. Pak, pro každý klientem vybraný převod, u kterého nebyl splněn závazek, vytvoří zápis o převodu B zprávu obsahující záznam informace o těchto převodech, a pošle tuto zprávu k CSM (kroky 2086 - 2088).

Reklamace ztracených poukázek A přijme tuto zprávu a pošle k B vyrozumění včetně identifikátoru reklamace (např. ověřovací číslo) pro budoucí odkaz k reklamaci (krok 2092). Zápis o převodu B přijme vyrozumění a označí každý vybraný převod s nesplněným závazkem časem/datem reklamace a identifikátorem reklamace poskytnutým od CSM (krok 2094). Potom B realizuje převod (krok 2096).

Potom, co je funkce závazného prohlášení skončena, reklamace ztracených poukázek A vytvoří z přijaté zprávy obsahující informaci o převodech, u kterých nebyl splněn závazek, nárok, který má být odeslán do vyšetřovacího systému vydávaných peněz (Money Issued Investigation System - dále MIIS). Ten s výhodou vytvoří část vyšetřovacího systému převodů. Funkce *k hostiteli* A pošle tento požadavek k HCSMA ¹⁴, který jej přijme a odešle dále k MIIS (kroky 2098 - 2102).

A nyní zpět ke kroku 2060 z obr. 22. Jestliže reklamace není založena na nesplnění závazku (např. pro ztracený¹⁵ či poškozený peněžní modul), pak klient může vybrat reklamaci ztracených poukázek od hostitele B, který má přístup ke všem reklamacím klienta, které byly generovány a odhlášeny z počítačového prostředí peněžního modulu (např. do FLASH paměti) v souladu s postupem reklamace ztracené(ých) poukázky(zek) popsáním výše s odkazem na obr. 21. CSR odděleně vybere vyvolání postupu vedoucího k přijetí reklamace ztracených poukázek od peněžního modulu hostitele - a hostitelé vytvoří komunikační spojení podle jakékoliv známé metody (kroky 2104 - 2108).

Potom pošle klient hostitele B požadavek, obsahující certifikát peněžního modulu, k CSMHA, který pošle reklamaci k CSMA (kroky 2108 - 2112). Reklamace ztracených poukázek A



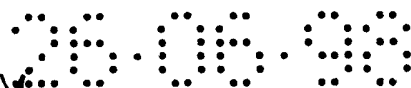
přijme tuto reklamaci a pošle ji veřejnému klíči A, který legalizuje certifikát peněžního modulu (2114 - 2116). Je-li certifikát peněžního modulu neplatný, pak funkce k hostiteli A pošle k CSMHA zprávu o tom, že požadavek byl odmítnut a CSMHA ji přesměruje k hostiteli klienta B a reklamace ztracených poukázek je ukončena (kroky 2120 - 2121).

Je-li certifikát peněžního modulu platný, Veřejný klíč A dešifruje nárok a ověří všechny poukázkové certifikáty a podpisy (krok 2118). Jestliže některý certifikát nebo podpis nejsou platné, je převod ukončen (kroky 2119 - 2121). Jestliže jsou certifikáty a podpisy poukázky platné, pak reklamace ztracených poukázek A ověří, zda souhlasí převáděné částky, aby se zajistilo, že hodnota peněz převáděných příjemci není vyšší než hodnota přijatá od odesílatele pro převodní historii každé poukázky (kroky 2122 - 2123). Je-li zde nějaká nesrovnalost, je převod ukončen (kroky 2120 - 2121).

Jestliže však jsou převodní částky v pořádku pro všechny poukázky, pak reklamace ztracených poukázek A vytvoří nárok, který bude zaslán do MIIS, a také vytvoří identifikátor nároku, který se připojí k nároku. Funkce k hostiteli A potom vyšle vytvořený nárok a jeho identifikátor k CSMHA, který je přijme a příslušně nasměruje ke klientovi hostitele B a nárok pošle k MIIS (kroky 2124 - 2128), tím dokončí reklamaci ztracených poukázek.

Ačkoli výše uvedený popis ukazuje mnoho zvláštností, nemají tyto detaily být výčtem omezujícím rozsah tohoto vynálezu, a odborníkovi je zřejmé, že tento vynález umožňuje mnoho modifikací, adaptací a ekvivalentních realizací, aniž se tím překročí rozsah tohoto vynálezu a omezí nějak jeho výhody. Je tedy účelné, aby tento vynález nebyl limitován podle uvedených realizací, ale byl definován v souladu s následujícími patentovými nároky.

P A T E N T O V É N Á R O K Y



1. Systém pro převod elektronických poukázek mezi elektronickým module založeným na procesoru, který obsahuje:

elektronické moduly založené na procesoru, kde každý modul je schopný vytvořit šifrovaný bezpečný kanál a převádět a přijímat elektronické poukázky cestou zmíněného šifrovaného bezpečného kanálu, a kde každý zmíněný elektronický modul má paměť pro uchovávání zmíněných elektronických poukázek; kde každá elektronická poukázka obsahuje:

hlavní skupinu datových polí obsahující data vyjadřující monetární hodnotu spojenou se zmíněnou elektronickou poukázkou;

převodovou skupinu datových polí obsahující seznam převodních záznamů, kde každý převodní záznam je vytvářen převodním elektronickým modulem a obsahuje pořadové číslo, které odlišuje převáděnou elektronickou poukázku od jiných převáděných elektronických poukázek převáděných zmíněným převodním elektronickým modulem.

2. Systém podle nároku 1, v y z n a č u j í c í s e t í m , že zmíněná monetární hodnota je původní monetární hodnota spojená se zmíněnou elektronickou poukázkou, a zmíněný převodní záznam dále obsahuje převáděnou monetární hodnotu.

3. Metoda platby používající první peněžní modul k převodu elektronické reprezentace peněz na druhý peněžní modul, skládající se z kroků:

- (a) vytvoření šifrovaného bezpečného spojení mezi zmíněným prvním peněžním modulem a zmíněným druhým peněžním modulem, kde ani jeden z obou peněžních modulů nelze zneužít;
- (b) zmíněného druhého peněžního modulu, který vyžádá na druhém klientovi podmínky převod, a zmíněný druhý klient dodá převodní podmínky zmíněnému peněžnímu modulu;
- (c) zmíněného druhého peněžního modulu, který posílá zmíněné převodní podmínky zmíněnému prvnímu peněžnímu modulu, cestou zmíněného šifrovaného bezpečného spojení;



- (d) zmíněného prvního peněžního modulu, který vyžádá u prvního klienta ověření převodních podmínek; zmíněný první klient dodává zmíněné převodní podmínky;
- (e) zmíněného prvního peněžního modulu, který převádí elektronickou reprezentaci peněz do zmíněného druhého peněžního modulu, cestou zmíněného šifrovaného bezpečného spojení.
- (f) zmíněného prvního peněžního modulu, který odevzdává zmíněný převod elektronických peněz pomocí zaznamenání zmíněného převodu elektronických peněz tak, že zmíněný první peněžní modul nemůže již zrušit zmíněný převod elektronických peněz návratem do původního stavu; a
- (g) zmíněného druhého peněžního modulu, který odevzdává zmíněný převod elektronických peněz pomocí zaznamenání zmíněného převodu elektronických peněz tak, že zmíněný druhý peněžní modul nemůže již zrušit zmíněný převod elektronických peněz návratem do původního stavu.

4. Platební metoda podle nároku 3, v y z n a č u j í c í s e t í m , že zmíněné podmínky převodu obsahují monetární částku zmíněné elektronické reprezentace peněz, a kde zmíněné kroky zmíněného prvního klienta dodávajícího ověření určující rozdělení zmíněných monetárních částek mezi úvěr a oběživo.

5. Metoda převodu elektronických poukázek mezi elektronickými, na procesoru založenými moduly, skládající se z kroků:
vytvoření šifrovaného bezpečného spojení mezi elektronickým modulem plátce a elektronickým modulem příjemce;
vytvoření převodní elektronické poukázky pomocí přidání převodového záznamu k elektronické poukázce uchovávané v zmíněném převodním elektronickém modulu, kde zmíněný převodní záznam ukazuje, zda všechny nebo některé části monetární částky zmíněné elektronické poukázky jsou právě převáděny;

převod zmíněné převodové elektronické poukázky od zmíněného elektronického modulu plátce ke zmíněnému elektronickému modulu příjemce; a

kde zmíněný záznam o převodu obsahuje pořadové číslo, které odlišuje zmíněnou převodní elektronickou poukázku od jiných převodních elektronických poukázek z daného převodního elektronického modulu.

6. Způsob pro přihlášení elektronického modulu do elektronické monetární systémové sítě se síťovým serverem, který připojí zmíněný elektronický modul k bezpečnostnímu serveru, skládající se z kroků, ve kterých:

zmíněný elektronický modul posílá svoje certifikát danému síťovému serveru;

zmíněný síťový server generuje náhodný klíč a náhodné ověřovací číslo, a posílá zašifrovanou zprávu včetně zmíněného certifikátu, zmíněného náhodného klíče, a zmíněného náhodného ověřovacího čísla ke zmíněnému bezpečnostnímu serveru;

zmíněný bezpečnostní server dešifruje zmíněnou zašifrovanou zprávu, ukládá zmíněný náhodný klíč a náhodné ověřovací číslo, a ověří platnost zmíněného certifikátu;

zmíněný bezpečnostní server vytváří bezpečné komunikační spojení se zmíněným elektronickým modulem;

zmíněný bezpečnostní server posílá zmíněnému elektronickému modulu aktualizovanou bezpečnostní informaci, která je digitálně označena šifrovacím klíčem zmíněného bezpečnostního serveru;

zmíněný elektronický modul ověřuje platnost zmíněné digitálně označené aktualizované bezpečnostní informace, a aktualizuje uloženou bezpečnostní informaci se zmíněnou aktualizovanou bezpečnostní informací;

zmíněný bezpečnostní server posílá zmíněný náhodný klíč a zmíněné náhodné ověřovací číslo zmíněnému elektronickému modulu, a ukončí zmíněné bezpečné komunikační spojení;

zmíněný elektronický modul vytváří zprávu pro místo určení zašifrováním zmíněného náhodného ověřovacího čísla a místa

určení se zmíněným náhodným klíčem, a posílá zmíněnou zprávu pro místo určení do zmíněného síťového serveru; zmíněný síťový server dešifruje zmíněnou zprávu a ověřuje zmíněné náhodné ověřovací číslo; a zmíněný síťový server navazuje spojení se zmíněným místem určení.

7. Způsob podle nároku 6, v y z n a č u j í c í s e t í m , že zmíněný elektronický modul je převodní modul, modul zákaznických služeb, modul generující peníze, nebo modul bankomatu.

8. Způsob podle nároku 6, dále se skládající z kroků, ve kterých:

zmíněný elektronický modul posílá zmíněnému bezpečnostnímu serveru svou informaci o času a datu zmíněnému bezpečnostnímu serveru;

zmíněný bezpečnostní server kontroluje zmíněnou informaci o času a datu, aby zjistil zda je mimo přijatelný předem určený parametr; a

zmíněný bezpečnostní server, v případech, kdy zmíněná informace o času a datu je mimo zmíněný přijatelný předem definovaný parametr, pošle zmíněnému elektronickému modulu nové datum a čas za účelem synchronizace zmíněného elektronického modulu.

9. Způsob podle nároku 6, v y z n a č u j í c í s e t í m , že zmíněná zašifrovaná zpráva mezi zmíněným síťovým serverem a zmíněným bezpečnostním serverem je opatřena symetrickým klíčem uloženým v zmíněném síťovém serveru a v zmíněném bezpečnostním serveru.

10. Způsob podle nároku 6, v y z n a č u j í c í s e t í m , že zmíněná aktualizovaná bezpečnostní informace obsahuje aktualizovaný seznam neplatných elektronických modulů a identifikačních čísel bezpečnostních severů, aktualizovaný seznam veřejných klíčů a aktualizovanou délku klíče.

11. Způsob podle nároku 6, v y z n a č u j í c í s e t í m , že zmíněný krokem zmíněného bezpečnostního serveru, ve kterém se navazuje ustavující bezpečné komunikační spojení se

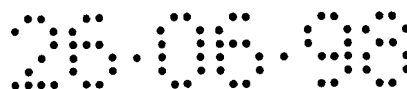
zmíněným elektronickým modulem obsahuje výměnný protokol veřejného klíče k zabezpečení klíče spojení společného zmíněnému bezpečnostnímu serveru a zmíněnému elektronickému modulu.

12. Postup podle nároku 6, v y z n a č u j í c í s e t í m ,
že dále obsahuje krok zmíněného bezpečnostního serveru znovu ověřujícího zmíněný certifikát.
13. Postup podle nároku 12, v y z n a č u j í c í s e t í m ,
že zmíněný krok opětovného ověření se vyskytuje v reakci na zaslání nové zprávy zmíněného bezpečnostního serveru se žádostí opětovného ověření ke zmíněnému elektronickému modulu.
14. Postup podle nároku 12, v y z n a č u j í c í s e t í m ,
že zmíněný certifikát obsahuje expirační čas, a ještě tím, že zmíněný krok opětovného ověření se vzniká jako odpověď zmíněnému elektronickému modulu, který určuje, že zmíněný certifikát má prošlou expirační dobu.
15. Monetární převodní systém, který je založen na elektronickém modulu a obsahuje:
 - primární bezpečnostní server;
 - řadu sekundárních bezpečnostních serverů, z nichž každý má jedinečný certifikát bezpečnostního serveru digitálně označený zmíněným primárním bezpečnostním serverem;
 - řadu elektronických modulů odolných proti zneužití, z nichž každý má jedinečný modulový certifikát, který je digitálně označen jedním ze zmíněných sekundárních bezpečnostních serverů, paměť uchovávající elektronické representace peněz a procesor přizpůsobený poskytovat šifrovaný bezpečný kanál pro převádění a přijímání zmíněných elektronických reprezentací peněz, av y z n a č u j í c í s e t í m , že zmíněné certifikáty bezpečnostních serverů jsou legalizovány potom, co se zmíněný elektronický server komunikuje se zmíněným elektronickým modulem nebo zmíněným primárním bezpečnostním serverem, a dále tím, že zmíněný certifikát modulu je legalizován potom, co zmíněný elektronický modul komunikuje s jiným ze zmíněných



elektronických modulů nebo se zmíněnými bezpečnostními servery.

16. Systém podle nároku 15, v y z n a č u j í c í s e t í m ,
že zmíněné modulové certifikáty a zmíněné certifikáty
bezpečnostních serverů jsou opatřeny respiračním časem, a kde
zmíněné elektronické moduly jsou uzpůsobeny tak, aby
neprováděly převody s jinými elektronickými moduly nebo
sekundárními bezpečnostními servery s prošlou expirační dobou
certifikátů.
17. Systém podle nároku 15, v y z n a č u j í c í s e t í m ,
že každý ze zmíněné řady elektronických modulů, zmíněných
primárních bezpečnostních serverů a každý ze zmíněné řady
sekundárních bezpečnostních serverů má jedinečný
identifikátor popisující typ serveru nebo typ elektronického
modulu.
18. Systém podle nároku 17, v y z n a č u j í c í s e t í m ,
že zmíněný typ elektronického modulu obsahuje převodní modul,
modul zákaznických služeb, modul generující peníze, a modul
bankomatu, a kde zmíněný typ serveru obsahuje zmíněný
primární bezpečnostní server a zmíněné bezpečnostní
sekundární servery.
19. Systém podle nároku 17, v y z n a č u j í c í s e t í m ,
že každý zmíněný typ serveru a každý zmíněný typ
elektronického modulu je přidružen k jedinečnému rozsahu
typové proměnné, kde každý zmíněný jedinečný identifikátor
zobrazí v hodnotě zmíněné typové proměnné uvnitř zmíněného
jedinečného rozsahu přiřazeného ke zmíněnému typu serveru
nebo typu elektronického modulu podle mechanismu zobrazení
bezpečně uloženém v každém zmíněném elektronickém modulu,
každém zmíněném sekundárním serveru a zmíněném primárním
serveru.
20. Systém podle nároku 19, v y z n a č u j í c í s e t í m ,
že každý zmíněný jedinečný identifikátor je jedinečná
celočíselná hodnota zmenšená o předem určené prvočíslo, a kde
zmíněná hodnota zmíněné typové proměnné je generována podle
umocněním primitivní odmocniny zmíněného prvočísla na zmíněný



jedinečný identifikátor, který je zlomkem zmíněného předem určeného prvočísla a aritmetického modulu, a kde každý ze zmíněné řady elektronických modulů, zmíněných primárních bezpečnostních serverů a každý ze zmíněné řady sekundárních bezpečnostních serverů má bezpečně uloženu zmíněnou odmocninu a zmíněné prvočíslo.

21. Systém podle nároku 15, v y z n a č u j í c í s e t í m , že zmíněný primární bezpečnostní server udržuje seznam zmíněných jedinečných identifikátorů pro neplatné elektronické moduly a neplatné sekundární bezpečnostní servery, kde zmíněné seznamy jsou poskytovány zmíněným sekundárním bezpečnostním serverům a zmíněným elektronickým modulům.
22. Systém podle nároku 15, v y z n a č u j í c í s e t í m , že zmíněný certifikát bezpečnostního serveru je zašifrován zmíněným primárním bezpečnostním serverem a zmíněný certifikát modulu je zašifrován zmíněným sekundárním bezpečnostním serverem.
23. Systém podle nároku 22, v y z n a č u j í c í s e t í m , že zmíněný certifikát bezpečnostního serveru obsahuje:
první a druhé datové pole zašifrované pomocí soukromého klíče zmíněného primárního bezpečnostního serveru, kde zmíněné první datové pole obsahuje jedinečný identifikátor zmíněného sekundárního bezpečnostního serveru, veřejný klíč zmíněného bezpečnostního serveru, a expirační dobu pro zmíněného certifikátu serveru, a kde zmíněné druhé datové pole obsahuje zmíněné první datové pole označená zmíněným primárním bezpečnostním serverem; a
třetí datové pole, které obsahuje jedinečný identifikátor zmíněného primárního bezpečnostního serveru.
24. Systém podle nároku 23, v y z n a č u j í c í s e t í m , že zmíněný jedinečný identifikátor zmíněného primárního bezpečnostního serveru je zašifrován.
25. Systém podle nároku 22, v y z n a č u j í c í s e t í m , že zmíněný modulový certifikát obsahuje:

první a druhé datové pole zašifrované pomocí soukromého klíče sekundárního bezpečnostního serveru, a kde zmíněné první datové pole obsahuje jedinečný identifikátor zmíněného elektronického modulu, veřejný klíč zmíněného elektronického modulu, a datum expirace zmíněného modulového ověření, a dále se vyznačující tím, že zmíněné druhé datové pole obsahuje zmíněné první datové pole digitálně označené zmíněným sekundárním bezpečnostním serverem; a
třetí datové pole obsahující zmíněný certifikátu bezpečnostního serveru.

26. Systém podle nároku 15, v y z n a č u j í c í s e t í m ,
že primární bezpečnostní server a zmíněné sekundární bezpečnostní servery sdílejí společný symetrický klíč, který je periodicky měněn pomocí změny veřejného klíče.
27. Systém podle nároku 15, v y z n a č u j í c í s e t í m ,
že zmíněný primární bezpečnostní server selektivně ovládá globální opětovné ověření zmíněných bezpečnostních certifikátů bezpečnostních serverů a zmíněných modulových certifikátů.
28. Způsob platby používající první peněžní modul k převodu elektronických reprezentací peněz na druhý peněžní modul, skládající se z kroků:
vytvoření šifrovaného bezpečného spojení mezi zmíněným prvním peněžním modulem se zmíněným druhým peněžním modulem, kde zmíněný první a druhý peněžní modul jsou elektronické moduly, které se nedají zneužít.
zmíněný první peněžní modul převádějící elektronické reprezentace peněz do zmíněného druhého peněžního modulu cestou zmíněného šifrovaného bezpečného spojení;
zmíněný druhý peněžní modul posílá zprávu "připraven ke splnění závazku převodu" zmíněnému prvnímu peněžnímu modulu;
zmíněný první peněžní modul posílající vyrozumění zmíněnému druhému peněžnímu modulu jako odpověď na zprávu "připraven ke splnění závazku převodu", a pak provede zmíněný převod

elektronických peněz tak, že zmíněný první peněžní modul již nemůže zrušit zmíněný převod elektronických peněz navrácením do původního stavu; a
zmíněný druhý peněžní modul, po příjmu zmíněného vyrozumění, odevzdá (ukončí) tak, že zmíněný druhý peněžní modul již nemůže zrušit zmíněný převod elektronických peněz navrácením modulu do jeho původního stavu.

29. Způsob platby podle nároku 28, v y z n a č u j í c í s e t í m , že každý zmíněný peněžní modul může přerušit před realizací zmíněného převodu jej přerušit pomocí podprogramu přerušení v zmíněných peněžních modulech.

30. Způsob platby podle nároku 28, v y z n a č u j í c í s e t í m , že zmíněné podprogramy přerušení obsahují tyto provedené kroky peněžního modulu:

kontrolu, zda zmíněná zpráva "připraven ke splnění závazku převodu" byla odeslána;
tam, kde zmíněná zpráva "připraven ke splnění závazku převodu" byla odeslána, zaznamenání informace spojené se zmíněnou elektronickou reprezentací peněz přijatých od zmíněného prvního peněžního modulu, vyznačující se tím, že zmíněná informace spojená se zmíněnou elektronickou reprezentací peněz může být použita k reklamaci ztracených elektronických peněz.

31. Způsob platby odpovídající nároku 30, vyznačující se tím, že zmíněný podprogram přerušení obsahuje kroky vykonané peněžním modulem:

poslání zprávy k jiným zmíněným peněžním modulům, o tom, že zmíněný převod elektronických peněz nemůže být dokončen; a
kde zmíněné jiné peněžní moduly v odpovědi na zmíněnou zprávu vrátí zpátky své změny týkající se zmíněného převodu elektronických peněz a zaznamenají, že zmíněný převod elektronický převod peněz je přerušen.

32. Způsob platby podle nároku 31, který dále obsahuje v případech, kdy zmíněný jiný peněžní modul je převodní modul užívaný druhým klientem, krok, kterým je zaslána zpráva

zmíněnému druhému klientovi, že zmíněný elektronický převod je přerušen.

33. Způsob platby podle nároku 31, který dále obsahuje v případech, kdy zmíněný jiný ze zmíněných peněžních modulů je modul bankomatu spojený s bankou, krok, kterým je informována zmíněná banka o tom, aby změnila směr účetních převodů vykonávaných pro zmíněný elektronický převod.
34. Způsob platby podle nároku 30, dále obsahující krok zmíněného prvního peněžního modulu navracející zpět změny a zaznamenávající, že tento zmíněný převod byl přerušen.
35. Způsob platby podle nároku 30, dále obsahující v případech, kdy zmíněný peněžní modul je převodní peněžní modul používaný klientem a zmíněná zpráva "připraven ke splnění závazku převodu" nebyla odeslána, krok, který posílá zmíněnému klientovi zprávu, že zmíněný elektronický převod je přerušen.
36. Způsob platby podle nároku 30 dále obsahující v případech, kdy zmíněný peněžní modul je převodní peněžní modul používaný klientem a zmíněná zpráva "připraven ke splnění závazku převodu" byla poslána, krok, ve kterém je poslána zmíněnému klientovi zpráva, že zmíněný elektronický převod je přerušen a že se objevila chyba převodu peněz.
37. Způsob platby podle nároku 30, dále obsahující v případech, kdy zmíněný peněžní modul je modul bankomatu spojený s bankou a zmíněná zpráva "připraven ke splnění závazku převodu" byla odeslána, krok informující zmíněnou banku o tom, aby změnila směr účetních převodů vykonávaných pro zmíněný elektronický převod.
38. Způsob navázání spojení prvního a druhého zařízení, kde první a druhé zařízení jsou elektronické moduly nebo server elektronického monetárního systému, který se skládá z kroků, ve kterých:
 - a) zmíněné druhé zařízení přijímá certifikát od zmíněného prvního zařízení;
 - b) zmíněné druhé zařízení ověřuje platnost zmíněného certifikátu zmíněného prvního zařízení;

- c) zmíněné druhé zařízení posílá zprávu zmíněnému prvnímu zařízení, zmíněná zpráva obsahuje část zašifrovanou pomocí veřejného klíče zmíněného prvního zařízení, a certifikát zmíněného druhého zařízení, zmíněná část obsahuje první náhodné číslo, časovou informaci druhého zařízení, a první ověřovací zprávu;
- d) zmíněné první zařízení ověřuje platnost zmíněného certifikátu zmíněného druhého zařízení, a určuje, zda zmíněná časová informace druhého zařízení je uvnitř předem určeného rozpětí časové informace prvního zařízení;
- e) zmíněné první zařízení posílá zmíněnému druhému zařízení druhou zprávu zašifrovanou pomocí veřejného klíče zmíněného druhého zařízení; zmíněná zpráva obsahuje druhé náhodné číslo generované zmíněným prvním zařízením, druhou ověřovací zprávu vytvořenou zmíněným prvním zařízením, zmíněnou ověřovací zprávu vytvořenou zmíněným druhým zařízením, a zmíněnou časovou informaci prvního zařízení;
- f) zmíněné první zařízení vytváří spojovací klíč z kombinace zmíněného prvního náhodného čísla a zmíněného druhého náhodného čísla;
- g) zmíněné druhé zařízení ověřuje zmíněnou první ověřovací zprávu, vytváří zmíněný spojovací klíč ze zmíněné kombinace zmíněného prvního a zmíněného druhého náhodného čísla, a určuje, zda zmíněná časová informace je uvnitř předem určeného rozpětí od časové informace druhého zařízení.
- h) zmíněné druhé zařízení posílá zmíněnému prvnímu zařízení vyrozumění zašifrované zmíněným spojovacím klíčem, zmíněné vyrozumění obsahuje zmíněnou druhou ověřovací zprávu; a
- i) zmíněné první zařízení dešifruje zmíněné vyrozumění a ověřuje zmíněnou druhou ověřovací zprávu.



39. Metoda podle nároku 38, v y z n a č u j í c í s e t í m ,
že, pro případy kdy zmíněné první zařízení je připojeno k
elektronickému monetárnímu systému se síťovým serverem, krok
a) obsahuje kroky zmíněného prvního zařízení posílajícího
zmíněnému síťovému serveru zprávu obsahující zmíněné
certifikát zmíněného prvního zařízení zašifrovanou pomocí
symetrického klíče, a zmíněný síťový server dešifrující
zmíněnou zprávu a posílající zmíněné certifikát zmíněného
prvního zařízení ke zmíněnému druhému zařízení.
40. Způsob podle nároku 38, v y z n a č u j í c í s e t í m ,
že každý certifikát obsahuje jedinečný identifikátor, který
je jedinečný pro každé zařízení, dále obsahující kroky
zmíněného druhého zařízení, které určují, zda je jedinečný
identifikátor zmíněného prvního zařízení obsažen v prvním
seznamu uchovávaném v zmíněném druhém zařízení, a zmíněné
první zařízení určující, zda jedinečný identifikátor
zmíněného druhého zařízení je obsažen v druhém seznamu
uchovávaném ve zmíněném prvním zařízení, přičemž první a
druhý seznam jsou seznamy zmíněných jedinečných
identifikátorů pro neplatná zařízení.
41. Způsob podle nároku 40, v y z n a č u j í c í s e t í m ,
že každé zařízení je jedním z řady typů, a přitom každý ze
zmíněných typů je spojen s jedinečným rozsahem typové
proměnné, a kde zmíněný jedinečný identifikátor daného
zařízení se zobrazuje v hodnotě zmíněné typové proměnné
uvnitř zmíněného jedinečného rozsahu přiřazeného zmíněnému
typu zmíněného daného zařízení podle zobrazovacího mechanismu
bezpečně uloženého v každém zmíněném zařízení, a kde krok (b)
zahrnuje kroky zobrazení zmíněného jedinečného identifikátoru
zmíněného prvního zařízení v proměnné prvního typu zařízení,
a který určuje zda zmíněná proměnná prvního typu zařízení
odpovídá očekávanému typu zmíněného prvního zařízení, a kde
krok (d) zahrnuje kroky zobrazení zmíněného jedinečného
identifikátoru, a který určuje, zda zmíněná proměnná druhého
typu zařízení odpovídá očekávanému typu zmíněného druhého
zařízení.



42. Způsob převodu elektronických poukázek předem určené celkové monetární hodnoty od peněžního modulu plátce na peněžní modul příjemce, v y z n a č u j í c í s e t í m , že zmíněný způsob skládá z kroků, ve kterých:

- a) zmíněný peněžní modul plátce vybere jednu nebo více elektronických poukázek, ze kterých poskytne zmíněnou předem určenou celkovou monetární hodnotu;
- b) zmíněný peněžní modul plátce vytvoří jednu nebo více elektronických převodních poukázek pomocí přidání odpovídajícího převodního záznamu a digitálního podpisu zmíněného peněžního modulu plátce ke každé jedné nebo více zmíněné(ých) poukázek, a kde pro každou zmíněnou jednu či více převodních poukázek zmíněný individuální záznam ukazuje, zda je převáděna celá nebo nějaká část monetární hodnoty zmíněné jedné či více elektronických poukázek;
- c) zmíněný peněžní modul plátce posílá zmíněnou jednu nebo více převodních elektronických poukázek do zmíněného peněžního modulu příjemce;
- d) zmíněný modul příjemce ověřuje platnost zmíněné jedné či více elektronických poukázek;
- e) zmíněný peněžní modul příjemce uchová po ověření zmíněnou jednu či více převodních elektronických poukázek v adresáři poukázek; zmíněný adresář poukázek obsahuje všechny elektronické poukázky vlastněné zmíněným peněžním modulem příjemce a kde peněžní moduly plátce i příjemce ukládají do záznamu o poukázkách informaci obsahující základní informaci o poukázce záznamy o přenosu pro každou ze zmíněných jedné nebo více elektronických poukázek a kde krok d) obsahuje pro každou převodní poukázku ze zmíněných jedné nebo více převodních poukázek kroky kontrolující základní informaci o poukázce ve zmíněném adresáři poukázek a zmíněný záznam o převodu, zda odpovídají zmíněné převodní poukázce a vytváří strom převodu poukázek pro identifikované souhlasy a kontroly duplikátů.



43. Způsob podle nároku 42, v y z n a č u j í c í s e t í m ,
že zmíněný převodní záznam obsahuje sekvenční identifikační
číslo, u kterého pro každou ze zmíněných jedné nebo více
elektronických poukázek zmíněné sekvenční identifikační číslo
odlišuje každou od toho vytvořenou převodní elektronickou
poukázku.
44. Způsob podle nároku 42, v y z n a č u j í c í s e t í m ,
že krok d), pro každou převodní elektronickou poukázku ze
zmíněné jedné nebo více převodních elektronických poukázek,
obsahuje kroky kontrolující převodní záznam a všechny další
převodní záznamy připojené jiným peněžním modulem plátce, aby
se potvrdilo, že v každém převodu byla převedena monetární
částka, která nepřevyšuje monetární hodnotu převedenou v
bezprostředně předchozím převodu.
45. Způsob podle nároku 42, v y z n a č u j í c í s e t í m ,
že každá převodní elektronická poukázka ze zmíněné jedné nebo
více převodních elektronických poukázek obsahuje digitální
podpis a certifikát každého peněžního modulu plátce za celou
dobu převodu zmíněné elektronické poukázky; přičemž krok d)
dále obsahuje kroky ověřující platnost digitálního podpisu a
certifikátu.
46. Způsob podle nároku 42, v y z n a č u j í c í s e t í m ,
že každá převodní elektronická poukázka ze zmíněné jedné nebo
více převodních elektronických poukázek obsahuje datum
expirace; a jestliže zmíněný peněžní modul příjemce je
převodní peněžní modul, pak obsahuje krok d) zahrnující krok
zmíněného peněžního modulu příjemce, ve kterém se ověřuje
každé datum expirace elektronické poukázky.
47. Způsob podle nároku 42, v y z n a č u j í c í s e t í m ,
že zmíněná elektronická poukázka je elektronická reprezentace
hotovosti s datem expirace a monetární hodnotou; a kde
krok a) obsahuje krok :
 - (a) zmíněného peněžního modulu postupujícího, který
určuje všechny možné alternativy pro poskytování
předem určené celkové monetární hodnoty a používá
minimální počet elektronických poukázek;



- (b) určující, který soubor všech zmíněných možných alternativ obsahuje nejmenší počet převodů; a
 - (c) tam kde zmíněný soubor obsahuje více než jeden prvek, vybírá prvek zmíněného souboru, který obsahuje minimální počet monetárních-jednotkových-dnů sečtených pro všechny poukázky prvku, a kde monetární-jednotkové-dny představují součin počtu dní zbývajících do vypršení expirace elektronické poukázky a zbytkové monetární hodnoty elektronické poukázky.
48. Způsob podle nároku 42, v y z n a č u j í c í s e t í m , že v kroku d) zmíněný peněžní modul příjemce ověří, zda zmíněná převáděná předem určená monetární hodnota odpovídá očekávané hodnotě.
49. Způsob převodu elektronických poukázek předem určené celkové monetární hodnoty z peněžního modulu plátce na peněžní modul příjemce, který se skládá z kroků:
- (a) ve kterém zmíněný peněžní modul plátce vybere jednu nebo více elektronických poukázek, ze kterých poskytne zmíněnou předem určenou celkovou monetární hodnotu;
 - (b) ve kterém zmíněný peněžní modul plátce vytvoří jednu nebo více převodních elektronických poukázek připojením odpovídajícího převodního záznamu a digitálního podpisu zmíněného peněžního modulu plátce ke každé zmíněné jedné či více elektronickým poukázkám, kde pro každou zmíněnou jednu nebo více elektronických převodních poukázek zmíněný odpovídající převodní záznam vyjadřuje, zda celý či nějaká část monetárního obnosu zmíněné jedné nebo více elektronických poukázek, jsou převáděny¹⁶;
 - (c) ve kterém zmíněný peněžní modul plátce posílá jednu nebo více převodních elektronických poukázek zmíněnému peněžnímu modulu příjemce;



- (d) ve kterém zmíněný peněžní modul příjemce ověřuje platnost zmíněné jedné nebo více převodních elektronický poukázek;
- (e) ve kterém zmíněný peněžní modul příjemce ukládá jednu nebo více převodních elektronických poukázek v adresáři poukázek;

a kde každá převodní elektronická poukázka ze zmíněné jedné či více převodních elektronických poukázek obsahuje digitální podpisy a certifikáty každého peněžního modulu plátce za celou dobu převodu zmíněné elektronické poukázky; a každý ze zmíněných certifikátů obsahuje jedinečný identifikátor určující přidružený peněžní modul plátce, a kde zmíněný převodní záznam obsahuje zmíněný jedinečný identifikátor elektronického modulu příjemce; a kde krok d) dále představuje krok ve kterém se kontroluje, zda zmíněný jedinečný identifikátor zmíněného převodního záznamu odpovídá zmíněnému jedinečnému identifikátoru ve zmíněném certifikátu pro každý následující převod v celé době převodu zmíněné elektronické poukázky.

50. Způsob převodu elektronických poukázek předem určené celkové monetární hodnoty z peněžního modulu plátce na peněžní modul příjemce, který se skládá z kroků ve kterých:

- (a) zmíněný peněžní modul plátce vybírá jednu nebo více elektronických poukázek, ze kterých získá zmíněnou předem určenou celkovou monetární hodnotu;
- (b) zmíněný peněžní modul plátce vytváří jednu nebo více převodních elektronických poukázek pomocí připojení příslušného převodního záznamu a digitálního podpisu zmíněného peněžního modulu plátce ke každé ze zmíněných jedné či více převodních elektronických poukázek, kde pro každou zmíněnou jednu nebo více převodních elektronických poukázek zmíněný příslušná převodní záznam ukazuje, zda je převáděna celá či pouze část monetární částky zmíněné jedné nebo více elektronických poukázek;



- (c) zmíněný peněžní modul plátce posílá jednu nebo více převodních elektronických poukázek zmíněnému peněžnímu modulu příjemce;
- (d) zmíněný peněžní modul příjemce ověřuje platnost zmíněné jedné nebo více převodních elektronických poukázek;
- (e) zmíněný peněžní modul příjemce ukládá po ověření platnosti jednu nebo více převodních elektronických poukázek v adresáři poukázek;

kde každá převodní elektronická poukázka ze zmíněné jedné nebo více převodních elektronických poukázek obsahuje jedinečné identifikátory všech peněžních modulů příjemce po celou dobu převodu zmíněné elektronické poukázky; a kde pro případy, že zmíněný převodní peněžní modul příjemce je převodní peněžní modul, dále obsahuje krok d) představující kontrolní krok, který zjišťuje, zda každý zmíněný jedinečný identifikátor je na seznamu jedinečných identifikátorů pro neplatné peněžní moduly, který je uložen ve zmíněném peněžním modulu příjemce.

51. Způsob, směny elektronické reprezentace první cizí měny, uchovávané v prvním převodním modulu, za elektronickou reprezentací druhé cizí měny, uchovávané v druhém převodním modulu pro prvního klienta, který se skládá z kroků ve kterých:

- (a) se vytvoří šifrované bezpečné spojení mezi zmíněným prvním převodním modulem a zmíněným druhým převodním modulem;
- (b) zmíněný klient vybírá, pomocí zmíněného prvního převodního modulu, první částku zmíněné první cizí měny, která má být prodána;
- (c) kontroluje, zda první převodní modul má dostatečné fondy;
- (d) zmíněný první převodní modul posílá zmíněnou první částku zmíněnému druhému převodnímu modulu, pomocí zmíněného šifrovaného bezpečného spojení;



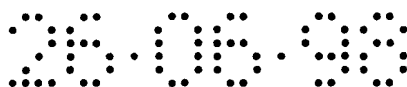
- (e) zmíněný druhý převodní modul žádá svého vlastníka, aby vybral směnný kurz nebo druhou částku ve zmíněné druhé měně;
- (f) se kontroluje, zda zmíněný druhý převodní modul má dostatečné fondy;
- (g) zmíněný druhý převodní modul posílá zprávu obsahující zmíněnou druhou částku nebo zmíněný směnný kurz zmíněnému prvnímu převodnímu modulu zmíněným šifrovaným bezpečným spojením;
- (h) zmíněný první klient potvrdí zmíněnou druhou částku nebo zmíněný směnný kurz;
- (i) zmíněný první převodní modul posílá zmíněnou elektronickou reprezentaci první cizí měny zmíněnému druhému převodnímu modulu, ve výši zmíněné první částky zmíněným šifrovaným bezpečným spojením;
- (j) zmíněný druhý převodní modul posílá zmíněnou elektronickou reprezentaci zmíněné druhé cizí měny zmíněnému prvnímu převodnímu modulu ve výši zmíněné druhé částky, zmíněným šifrovaným bezpečným spojením;
- a
- (k) zmíněný první převodní modul realizuje převod zmíněné první cizí měny ke zmíněnému druhému převodnímu modulu a zmíněný druhý převodní modul přijímá zmíněnou první cizí měnu od zmíněného prvního převodního modulu, a zmíněný druhý převodní modul realizuje převod zmíněné druhé cizí měny ke zmíněnému prvnímu převodnímu modulu, a zmíněný první převodní modul přijímá zmíněnou druhou cizí měnu od zmíněného druhého převodního modulu, v pořadí, které není předvídatelné.

52. Způsob odpovídající nároku 51, v y z n a č u j í c í s e t í m , že krok k) se skládá z kroků, ve kterých:

- (a) zmíněný první převodní modul a zmíněný druhý převodní modul sdílejí společnou náhodnou binární hodnotu, mající buď první hodnotu nebo druhou hodnotu;



- (b) zmíněný první převodní modul se podmíněně přihlašuje k převodu buď zmíněného převodu zmíněné první cizí měny zmíněnému druhému převodnímu modulu nebo zmíněné přijetí zmíněné druhé cizí měny od zmíněného druhého převodního modulu, přičemž zmíněná společná náhodná binární hodnota má v prvním případě zmíněnou první hodnotu a ve druhém případě zmíněnou druhou hodnotu, takže zpětný převod může nastat;
- (c) zmíněný první převodní peněžní modul posílá zprávu zmíněnému druhému převodnímu modulu, která sděluje, že zmíněný první převodní modul ukončil podmíněné přihlášení převodu
- (d) zmíněný druhý převodní modul v reakci na zmíněnou zprávu se podmíněně přihlašuje k převodu buď zmíněného příjmu zmíněné první cizí měny od zmíněného prvního převodního modulu nebo zmíněného převodu zmíněné druhé cizí měny ke zmíněnému prvnímu převodnímu modulu, přičemž zmíněná společná náhodná binární hodnota se rovná v prvním případě zmíněné první hodnotě nebo ve druhém případě druhé hodnotě, takže zpětný převod může nastat.
- (e) zmíněný druhý převodní peněžní modul, v těch případech, kdy zmíněná hodnota společného náhodného čísla se rovná první hodnotě, posílá zprávu začni realizaci zmíněnému prvnímu převodnímu modulu
- (f) zmíněný první převodní modul v reakci na zmíněnou zprávu začni realizaci přiřadí podmíněnému přihlášení převodu statut bezpodmínečného přihlášení a zahájí protokol o realizaci, kde zmíněný první převodní modul se zavazuje k nevyřízenému převodu takže zmíněný první převodní modul již nemůže přerušit zmíněný převod návratem do původního stavu a kde zmíněný druhý peněžní modul se realizuje zmíněný převod druhé cizí měny zmíněný příjem první cizí měny přihlášením zmíněného převodu a příjmu, takže zmíněný



druhý peněžní modul již nemůže přerušit směnu cizí měny návratem do původního stavu; a

- (g) zmíněný druhý převodní modul, kde zmíněná společná hodnota náhodného čísla se rovná druhé hodnotě tím, že přiřadí podmíněnému přihlášení atribut nepodmíněného přihlášení a zahájí realizační protokol, kde zmíněný druhý převodní modul realizuje nevyřízený převod, aby zmíněný druhý převodní modul nemohl již přerušit zmíněný převod návratem do původního stavu a kde zmíněný první převodní modul se zavazuje provést zmíněný převod první cizí měny a příjem druhé cizí měny aby zmíněný první peněžní modul již nemohl přerušit zmíněnou směnu cizí měny návratem do původního stavu.

53. Způsob podle nároku 52, v y z n a č u j í c í s e t í m , že zmíněné společné náhodné číslo je generováno jako spojovací klíč v průběhu zmíněného kroku vytváření šifrovaného bezpečného spojení.

54. Způsob podle nároku 51, v y z n a č u j í c í s e t í m , že zmíněný realizační protokol zahájená daným peněžním modulem pro jakýkoli nevyřízený peněžní převod vůči jinému peněžnímu modulu se skládá z kroků, ve kterých :

zmíněný daný modul posílá zprávu "připraven ke splnění závazku převodu" zmíněnému jinému peněžnímu modulu;

zmíněný jiný peněžní modul posílá vyrozumění zmíněnému danému peněžnímu modulu jako odpověď na zmíněnou zprávu "připraven ke splnění závazku převodu";

zmíněný daný peněžní modul realizující přihlášením jakýkoliv zmíněný nevyřízený peněžní převod tak, aby zmíněný daný peněžní modul již nemohl zrušit jakýkoliv zmíněný nevyřízený peněžní převod návratem do původního stavu; a

zmíněný jiný peněžní modul realizující přihlášením jakýkoli zmíněný nevyřízený peněžní převod tak, aby zmíněný jiný peněžní modul nemůže již nemohl zrušit jakýkoliv zmíněný nevyřízený peněžní převod návratem do původního stavu.



55. Způsob podle nároku 51, v y z n a č u j í c í s e t í m ,
že v kroku b) zmíněný klient vybere zmíněnou první částku
zmíněné první cizí měny, aby byla prodána podle typu
poukázky??
56. Systém pro převod elektronických poukázek mezi
elektronickými moduly řízenými procesorem, kde každý
procesorový elektronický modul je jedním z řady modulových
typů, a který obsahuje:
procesorové elektronické moduly, kde každý procesorový
elektronický modul ukládá jedinečný modulový identifikátor,
a každý je schopný vytvořit šifrovaný bezpečný kanál a
převádět a přijímat elektronické poukázky zmíněným
šifrovaným bezpečným kanálem, a kde každý zmíněný
elektronický modul má paměť pro uchovávání zmíněných
elektronických poukázek;
kde každý ze zmíněné řady modulových typů je spojený s
jedinečným rozsahem modulových typových proměnných, a dále
kde každý jedinečný modulový identifikátor zobrazuje
v hodnotě zmíněné typové proměnné uvnitř zmíněného
jedinečného rozsahu přiřazeného ke zmíněnému modulovému
typu mechanismu zobrazení bezpečně uloženého v každém
zmíněném elektronickém modulu.
57. Systém podle nároku 56, v y z n a č u j í c í s e t í m ,
že každý zmíněný jedinečný identifikátor je jedinečná
celočíselná hodnota menší než předem určené prvočíslo, a kde
zmíněná hodnota zmíněné typové proměnné je generována podle
umocněním primitivní odmocniny zmíněného prvočísla na zmíněný
jedinečný identifikátor modulární aritmetiky pro předem
určené prvočíslo, a kde každý ze zmíněné řady elektronických
modulů, zmíněný primární bezpečnostní server a každý ze
zmíněné řady sekundárních bezpečnostních serverů má bezpečně
uloženu zmíněnou odmocninu a zmíněné prvočíslo.
58. Způsob, při kterém klient používá převodní modul
k aktualizaci úvěrové poukázky pro zmíněný klientův bankovní
účet ve vydávající bance, která má modul bankomatu, modul



generátoru peněz, a účetní systém zapojený na počítač (on-line), a zmíněný způsob se skládá z kroků, ve kterých :

- (a) zmíněný klient vybírá pomocí zmíněného převodního modulu bankovní účet, ze kterého bude aktualizována zmíněná úvěrová poukázka a požadovaná částka určující požadovanou celkovou úvěrovou částku pro zmíněnou úvěrovou poukázku;
- (b) zmíněný převodní modul vytvoří první šifrované bezpečné spojení se zmíněným modulem bankomatu;
- (c) zmíněný převodní modul pošle zprávu se žádostí o úvěr ke zmíněnému modulu bankomatu cestou zmíněného prvního šifrovaného bezpečného spojení, kde zmíněná zpráva s úvěrovou žádostí obsahuje úvěrovou aktualizovanou částku odpovídající čisté úvěrové částce pro zmíněnou úvěrovou poukázku a informaci o bankovním účtu odpovídající zmíněnému bankovnímu účtu.
- (d) kontroluje zmíněnou informaci o bankovním účtu, aby se ověřila její platnost;
- (e) kontroluje úvěrové spojení přidružené ke zmíněnému bankovnímu účtu klienta, aby se zjistilo, zda k poskytnutí zmíněné požadované úvěrové částky jsou fondy dostatečné;
- (f) v těch případech, kdy existují současné úvěrové poukázky pro zmíněný klientův bankovní účet, zmíněný převodní modul posílá zmíněnou současnou úvěrovou poukázku zmíněnému modulu bankomatu;
- (g) zmíněný modul bankomatu vytváří druhé šifrované bezpečné spojení se zmíněným modulem generátoru peněz;
- (h) je aktualizováno zmíněné úvěrové spojení přidružené ke zmíněnému bankovnímu účtu podle zmíněné požadované celkové úvěrové částky pro zmíněnou úvěrovou poukázku;
- (i) zmíněný modul bankomatu posílá žádost o vytvoření poukázky zmíněnému modulu generátoru peněz, cestou



zmíněného druhého šifrovaného bezpečného spojení, kde
zmíněná žádost o vytvoření poukázky obsahuje
požadovanou poukázkovou hodnotu;

- (j) zmíněný modul generátoru peněz vytváří úvěrovou
poukázku zmíněné požadované hodnoty;
- (k) převedení zmíněné úvěrové poukázky zmíněnému modulu
bankomatu cestou zmíněného druhého šifrovaného
bezpečného spojení;
- (l) převedení zmíněné úvěrové poukázky zmíněnému
převodnímu modulu cestou prvního šifrovaného
bezpečného spojení;
- (m) se závazně potvrdí spojení zmíněného převodního
modulu a zmíněného modulu bankomatu; a
- (n) zmíněný modul bankomatu se závazně propojí s modulem
generátoru peněz.

59. Způsob aktualizace úvěru podle nároku 58

v y z n a č u j í c í s e t í m , že v těch případech, kdy
existuje zmíněná úvěrová poukázka, potom v kroku (c) zmíněná
čistá úvěrová částka představuje rozdíl mezi zmíněnou
požadovanou celkovou částkou a současnou úvěrovou částkou
zmíněné současné úvěrové poukázky.

60. Způsob aktualizace úvěru podle nároku 58,

v y z n a č u j í c í s e t í m , že zmíněná bankovní účtová
informace obsahuje profil účtu, který má číslo bankovního
účtu, které je digitálně označeno modulem zákaznických
služeb; kde zmíněný kroky kontrolování platnosti zmíněné
bankovní účetní informace obsahuje krok kontrolující zmíněný
digitální podpis na zmíněném profilu účtu s veřejným klíčem
zmíněného modulu zákaznických služeb.

61. Způsob aktualizace úvěru podle nároku 58,

v y z n a č u j í c í s e t í m , že:

krok f) dále obsahuje krok zmíněného převodního modulu
posílající zmíněnému modulu bankomatu kteroukoliv
pokladniční poukázku a kteroukoliv převedenou úvěrovou
poukázku uloženou ve zmíněném převodním modulu;



krok f) je následován krokem zmíněného modulu bankomatu, který aktualizuje zmíněný on-line účetní systém připojený na centrální počítač (on-line) podle zmíněných pokladničních poukázek a převedených úvěrových poukázek; v kroku i) zmíněná žádost o vytvoření poukázky obsahuje požadovanou hodnotu pokladniční poukázky odpovídající celkové hodnotě zmíněné pokladniční poukázky a zmíněné převedené úvěrové poukázky uchovávané ve zmíněném převodním modulu;

vydaný peněžní účet je úvěrován ve zmíněném účetním systému napojeném na centrální počítač (on-line) hodnotou zmíněné vyžádané pokladniční poukázky;

krok j) obsahuje krok zmíněného modulu generátoru vytvářejícího pokladniční poukázku bankovku zmíněné požadované hodnoty pokladniční poukázky;

krok k) obsahuje krok, převádějící zmíněnou pokladniční poukázku zmíněnému modulu bankomatu cestou zmíněného druhého šifrovaného bezpečného spojení; a

krok l) obsahuje krok převádějící zmíněnou pokladniční poukázku zmíněnému převodnímu modulu cestou zmíněného prvního šifrovaného bezpečného spojení.

62. Způsob, který umožňuje klientovi, pomocí modulu zákaznických služeb přidruženého k hostiteli, který má přístup k jedné i více bankám, spojit převodní peněžní modul se zmíněným klientovým bankovním účtem klienta v bance, která má modul bankomatu, modul generátoru peněz, a účetní systém připojený na centrální počítač (on-line) přitom tento způsob se skládá z kroků, ve kterých:

(a) zmíněný hostitel zmíněného modulu zákaznických služeb získá přístup k bankovní informaci o účtu zmíněného klienta ve zmíněné jedné či více bankách v reakci na přijetí identifikační informace zmíněného kliente;

(b) je ověřena zmíněná informace o bankovním účtu, a zmíněný klient identifikuje svůj bankovní účet zmíněný pro spojení se zmíněným převodním peněžním modulem;



- (c) je vytvořeno spojení mezi zmíněným převodním peněžním modulem a zmíněným modulem zákaznických služeb;
 - (d) zmíněný modul zákaznických služeb generuje účetní profil pro zmíněný klientův bankovní účet;
 - (e) zmíněný modul zákaznických služeb posílá zprávu zmíněnému převodnímu peněžnímu modulu, a tato zmíněná zpráva obsahuje zmíněný účetní profil a digitální podpis zmíněného účetního profilu označený soukromým klíčem zmíněného modulu zákaznických služeb;
 - (f) zmíněný převodní peněžní modul ověří zmíněný digitální podpis;
 - (g) zmíněný převodní peněžní modul připojí certifikát zmíněného modulu zákaznických služeb ke zmíněnému účetnímu profilu;
 - (h) zmíněný převodní peněžní modul uloží zmíněný účetní profil; a
 - (i) učiní závazným spojení zmíněného převodního peněžního modulu a zmíněného modulu zákaznických služeb.
63. Způsob podle nároku 62, v y z n a č u j í c í s e t í m ,
že krok f) dále obsahuje krok zmíněného klienta, ve kterém se kontroluje profil účtu.
64. Způsob podle nároku 62, v y z n a č u j í c í s e t í m ,
že krok h) obsahuje kroky zmíněného převodního peněžního modulu, kterým zaměňuje existující druhý profil účtu za zmíněný bankovní účet se zmíněným profilem účtu.
65. Způsob při kterém klient pomocí modulu zákaznických služeb přistupuje k jedné nebo více bankám, aby obnovil platnost spojení převodního peněžního modulu se zmíněnými klientovými bankovními účty u bance mající modul bankomatu, modul generátoru peněz a účetní systém připojený k centrálnímu počítači (on-line) přičemž tento způsob obsahuje kroky, ve kterých:
- (a) zmíněný klient vybere pomocí zmíněného převodního peněžního modulu zmíněnou banku, u které obnoví platnost spojení;

- (b) zmíněný převodní peněžní modul vytvoří šifrované bezpečné spojení se zmíněným modulem zákaznických služeb;
 - (c) zmíněný převodní peněžní modul pošle zmíněnému modulu zákaznických služeb účetní profil pro zmíněné bankovní účty, který je uložen v zmíněném převodním peněžním modulu;
 - (d) zmíněný modul zákaznických služeb ověřuje platnost zmíněného účetního profilu;
 - (e) zmíněný modul zákaznických služeb kontroluje u zmíněné banky, zda jsou aktivní zmíněné klientovy bankovní účty obsažené v zmíněném účetním profilu;
 - (f) zmíněný modul zákaznických služeb vytváří účetní profil pro zmíněný klientův bankovní účet;
 - (g) zmíněný modul zákaznických služeb posílá zprávu zmíněnému převodnímu peněžnímu modulu, která obsahuje zmíněný účetní profil a digitální podpis zmíněného účetního profilu označené soukromým klíčem zmíněného modulu zákaznických služeb;
 - (h) zmíněný převodní peněžní modul ověřuje zmíněný digitální podpis;
 - (i) zmíněný převodní peněžní modul připojuje ověření zmíněného modulu zákaznických služeb ke zmíněnému účetnímu profilu; a
 - (j) učiní závazným spojení zmíněného převodního peněžního modulu a zmíněného modulu zákaznických služeb.
66. Způsob podle nároku 65, v y z n a č u j í c í s e t í m , že zmíněný účtový profil obsahuje specifické digitální podpisy modulu zákaznických služeb a certifikát zmíněného specifického modulu zákaznických služeb, kde zmíněný krok d) ověřující platnost zmíněných účetních profilů obsahuje krok, ve kterém se kontrolují zmíněné specifické digitální podpisy zákaznického modulu a uvádí v platnost zmíněný certifikát zmíněného modulu zákaznických služeb.
67. Elektronický monetární systém, v y z n a č u j í c í s e t í m , že obsahuje:

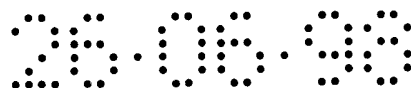


vydávající banku mající účetní systém zapojený na centrální počítač (on-line);
systém vyrovnání vydaných peněz;
elektronické representace peněz, které jsou účtovány ve zmíněném on-line účetním systému;
modul generátoru peněz spojený se zmíněnou vydávající bankou, který vytváří zmíněné elektronické representace peněz;
modul bankomatu spojený se zmíněnou vydávající bankou, schopný uchovávat zmíněné elektronické representace peněz;
převodní peněžní modul schopný převádět zmíněné elektronické representace peněz;
a dále v případech, ve kterých převodní záznam je připojen ke zmíněné elektronické reprezentaci peněz po každém převodu mezi dvěma jakýmkoliv zmíněnými moduly, a kde zmíněné elektronické poukázky jsou periodicky postupovány zmíněnému systému vyrovnání vydaných peněz;
zmíněný systém vyrovnání vydaných peněz má procesor pro analyzování zmíněných převodních záznamů pro každou poukázku za účelem identifikace elektronických representací peněz, které jsou ztraceny či duplikovány; a
tam, kde klient daného převodního peněžního modulu předloží nárok ztracených peněz identifikující ztracené elektronické representace peněz zmíněné vydávající bance, a zmíněná vydávající banka odškodní zmíněného klienta na základě zmíněného nároku ztracených peněz a na základě systému vyrovnání vydaných peněz, které potvrdí platnost zmíněných nároků ztracených peněz pro každou ztracenou elektronickou reprezentaci peněz.

68. Elektronický monetární systém podle nároku 67, v y z n a č u j í c í s e t í m , že zmíněné převodní peněžní moduly jsou všechny uzpůsobeny k ukládání informace spojené s elektronickými representacemi peněz, které jsou zahrnuty v přerušených převodech a kde zmíněný nárok na ztracené peníze obsahuje zmíněnou informaci.



69. Elektronický monetární systém podle nároku 67,
v y z n a č u j í c í s e t í m , že všechny zmíněné převodní
peněžní moduly jsou uzpůsobeny k ukládání zmíněných nároků
ztracených peněz na nezávislém paměťovém zařízení, kde
zmíněné nároky na ztracené peníze jsou digitálně označeny
soukromým klíčem zmíněných převodních peněžních modulů.
70. Elektronický monetární systém podle nároku 69,
v y z n a č u j í c í s e t í m , že zmíněné nároky na
ztracené peníze obsahují informaci spojenou se všemi
elektronickými reprezentacemi peněz, které jsou uloženy ve
zmíněném převodním peněžním modulu.
71. Způsob, podle kterého vytvoří klient nárok na ztracené
poukázky, který identifikuje ztracené elektronické poukázky
spojené s klientovým převodním peněžním modulem přičemž se
zmíněná metoda skládá z kroků, ve kterých:
- (a) zmíněný klient volí pomocí zmíněného převodního
peněžního modulu možnost vytvoření nároku na ztracené
poukázky;
 - (b) zmíněný převodní peněžní modul generuje jedinečné
pořadové číslo nároku a formuluje zmíněný nárok na
ztracené poukázky jako paket obsahující zmíněné
jedinečné pořadové číslo nároku, informaci pro
všechny převoditelné elektronické poukázky uložené v
převodním peněžním modulu, informaci o selhání při
realizaci pro všechny elektronické poukázky spojené
se selháním při realizaci pomocí zmíněného převodního
peněžního modulu, a digitální podpis a certifikát
zmíněného převodního peněžního modulu; a
 - (c) uloží zmíněný nárok na ztracené poukázky na paměťovém
médiu, které je nezávislé na zmíněném převodním
peněžním modulu.
72. Systém podle nároku 71, v y z n a č u j í c í s e t í m ,
že nárok na ztracené poukázky obsahuje:
- první a druhé datové pole zašifrované zmíněným soukromým
klíčem převodního peněžního modulu, kde zmíněné první
datové pole obsahuje zmíněné jedinečné pořadové číslo



nároku, zmíněnou informaci pro všechny převoditelné elektronické poukázky uchované v zmíněném převodním peněžním modulu obsahující současnou hodnotu a kopii každé zmíněné převoditelné elektronické poukázky, a zmíněnou informaci o nesplnění závazku pro nereklamované nesplněné závazky, a dále kde druhé datové pole obsahuje zmíněné první datové pole digitálně označené zmíněným soukromým klíčem převodního peněžního modulu; a třetí datové pole obsahující zmíněné pořadové číslo nároku, celkovou monetární hodnotu částky pro zmíněný nárok na ztracené poukázky, a zmíněný certifikát zmíněného převodního peněžního modulu.

73. Způsob, v y z n a č u j í c í s e t í m , že pomocí modulu zákaznických služeb majícího přístup k jedné či více vydávajícím bankám umožňuje klientovi nárokovat ztracené poukázky sdružené s převodním peněžním modulem pomocí použití zmíněného převodního peněžního modulu, přičemž tento způsob obsahuje kroky, ve kterých:

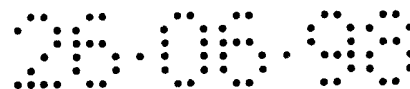
- (a) zmíněný klient poskytne identifikaci hostiteli zmíněného modulu zákaznických služeb;
- (b) se vytvoří šifrované bezpečné spojení mezi zmíněným převodním peněžním modulem a zmíněným modulem zákaznických služeb;
- (c) zmíněný modul zákaznických služeb přijme od zmíněného hostitele zmíněnou identifikační informaci zmíněného kliente;
- (d) zmíněný převodní peněžní modul pošle zmíněnému modulu zákaznických služeb zprávu obsahující informaci o nereklamovaných nesplněných závazků sdruženou se záznamem nenárokovaných nesplněných závazků uloženým ve zmíněném převodním peněžním modulu; a
- (e) zmíněný modul zákaznických služeb vytváří nárok ze zmíněné informace nenárokovaných selhání odevzdání, a posílá zmíněný nárok cestou zmíněného hostitele do



vyšetřovacího systému vydaných peněz sdruženého se
zmíněnou jednou nebo více vydávajícími bankami.

74. Způsob reklamace ztracených poukázek podle nároku 73,
v y z n a č u j í c í s e t í m , že dále obsahuje krok
zmíněného klienta modulu zákaznických služeb, který v reakci
na zmíněnou zprávu posílá identifikátor nároku zmíněnému
převodnímu peněžnímu modulu, a zmíněný převodní peněžní modul
označuje každý ze zmíněných záznamů nenárokovaných realizací
zmíněným identifikátorem nároku.
75. Způsob reklamace ztracených poukázek podle nároku 73,
v y z n a č u j í c í s e t í m , že zmíněná informace o
nenárokovaných nesplněných závazků¹⁷ poslaná zmíněnému modulu
zákaznických služeb v kroku d) je sdružena pouze se záznamy
nenárokovaných nesplněných závazků, které nebyly dříve
nárokovány.
76. Způsob reklamace ztracených poukázek podle nároku 73,
v y z n a č u j í c í s e t í m , že před krokem d) zmíněný
klient vybere pomocí zmíněného převodního peněžního modulu
zmíněné záznamy neplněných závazků ze seznamu záznamů
nesplněných závazků.
77. Způsob umožňující klientovi pomocí modulu zákaznických
služeb majícího přístup k jedné či více vydávajícím bankám
nárokovat ztracené poukázky sdružené s převodním peněžním
modulem pomocí použití paměťového zařízení, které obsahuje
nároky ztracených poukázek uložené od zmíněného převodního
modulu a zmíněné paměťové zařízení je nezávislé na zmíněném
převodním modulu; přičemž tento způsob obsahuje kroky, ve
kterých:
- (a) zmíněný klient poskytne identifikaci hostiteli
zmíněného modulu zákaznických služeb;
 - (b) zmíněný modul zákaznických služeb umožňuje přístup ke
zmíněným nárokům na ztracené poukázky ve zmíněném
úložném zařízení;
 - (c) zmíněný modul zákaznických služeb přijímá zmíněný
nárok na ztracených poukázek od zmíněného paměťového
zařízení;

- (d) zmíněný modul zákaznických služeb ověřuje platnost zmíněného nároku ztracených poukázek; a
 - (e) zmíněný modul zákaznických služeb vytváří nárok ze zmíněné informace nenárokovaného nesplněného závazku, a posílá zmíněný nárok cestou zmíněného hostitele do vyšetřovacího systému vydaných peněz sdruženého se zmíněnou jednou či více bankami.
78. Způsob reklamace ztracených poukázek podle nároku 77, v y z n a č u j í c í s e t í m , že zmíněný nárok na ztracené poukázky obsahuje certifikát zmíněného převodního peněžního modulu, a tím, že zmíněný krok d) zmíněného modulu zákaznických služeb, který ověřuje platnost zmíněného nároku na ztracené poukázky zahrnuje ověření platnosti zmíněného certifikátu.
79. Způsob reklamace ztracených poukázek podle nároku 77, v y z n a č u j í c í s e t í m , že zmíněný nárok na ztracené poukázky obsahuje kopie ztracených poukázek, každá kopie ze zmíněných kopií ztracených poukázek má skupinu datových polí certifikátů, která obsahuje seznam každého peněžního modulu plátce, který převáděl originál zmíněné ztracené poukázky a obsahuje všechny digitální podpisy zmíněného peněžního modulu plátce a certifikát, a kde krok d) dále obsahuje krok ověřující platnost každého certifikátu a digitálního podpisu peněžního modulu plátce.
80. Způsob reklamace ztracených poukázek podle nároku 77, v y z n a č u j í c í s e t í m , že zmíněný nárok ztracených poukázek obsahuje kopie ztracených poukázek, kde každá kopie ze zmíněných kopií ztracených poukázek má datové pole záznamu převodu, které obsahuje seznam každé monetární hodnoty převedené v každém převodu originálu zmíněné ztracené poukázky, a kde krok d) dále obsahuje krok kontrolující zmíněné datové pole záznamu převodu, aby se zjistilo, zda v každém převodu byla převedena monetární částka, která není vyšší než monetární částka převedená v bezprostředně předcházejícím převodu.



81. Způsob reklamace ztracených poukázek podle nároku 77,
v y z n a č u j í c í s e t í m , že v kroku b) je vytvořeno
komunikační spojení mezi zmíněným modulem zákaznických služeb
a hostitelským zařízením sdruženým se zmíněný paměťovým
zařízením, a zmíněný modul zákaznických služeb má přístup ke
zmíněnému nároku na ztracené poukázky cestou zmíněného
komunikačního spojení.
82. Monetární převodní systém založený na elektronickém
modulu, v y z n a č u j í c í s e t í m , že zmíněný převodní
systém se skládá z:
- řady bezpečnostních serverů;
 - řady elektronických modulů odolných proti zneužití, z nichž
každý má jedinečný modulový certifikát, který je digitálně
označen jedním ze zmíněných bezpečnostních serverů, paměť
na ukládání elektronických reprezentací peněz, a procesor
uzpůsobený tak, aby zabezpečil šifrovaný bezpečný kanál pro
převod a příjem zmíněných elektronických reprezentací
peněz; a
 - kde zmíněný modulový certifikát je uveden v platnost po
spojení zmíněného elektronického modulu s jiným ze
zmíněných elektronických modulů nebo ze zmíněných
bezpečnostních serverů; a
 - kde zmíněná řada bezpečnostních serverů selektivně ovládá
globální opětovné ověření zmíněných modulových certifikátů,
vyžadující aby každý elektronický modul, který se spojí
s jedním ze zmíněných bezpečnostních serverů opětovně
ověřil zmíněný modulový certifikát.

P A T E N T O V É N Á R O K Y

1. System pro převod elektronických poukázek mezi elektronickými moduly, který obsahuje:

elektronické moduly, kde každý elektronický modul má procesor, paměť a je schopný tvořit šifrovaný bezpečný kanál a převádět a přijímat elektronické poukázky cestou zmíněného šifrovaného bezpečného kanálu a kde každý elektronický modul uchovává zmíněné elektronické poukázky v jeho příslušné paměti, přičemž každá uchována elektronická poukázka zahrnuje hlavní skupinu datových polí obsahující data vyjadřující monetární hodnotu spojenou se zmíněnou elektronickou poukázkou, převodovou skupinu datových polí obsahující seznam převodních záznamů, kde každý převodní záznam je vytvářen převodním elektronickým modulem a obsahuje pořadové číslo, které odlišuje převáděnou elektronickou poukázku od jedné nebo více převáděných elektronických poukázek, převáděných zmíněným běžným převodním elektronickým modulem a generované běžnou elektronickou poukázkou.

42. Způsob převodu elektronických poukázek předem určené celkové monetární hodnoty od peněžního modulu plátce na peněžní modul příjemce v y z n a č u j í c í s e t í m, ž e zmíněný způsob sestává z kroků, ve kterých:

a) zmíněný modul plátce vybere jednu, nebo více elektronických poukázek, ze kterých poskytne zmíněnou předem určenou celkovou monetární hodnotu,

b) zmíněný peněžní modul plátce vytvoří jednu, nebo více elektronických převodních poukázek pomocí přidání odpovídajícího převodního záznamu a digitálního podpisu zmíněného peněžního modulu plátce ke každé jedné, nebo více zmíněných poukázek, a kde pro každou zmíněnou jednu či více převodních poukázek zmíněný individuální záznam ukazuje, zda je převáděna celá nebo nějaká část monetární hodnoty zmíněné jedné, nebo více elektronických poukázek,

c) zmíněný peněžní modul plátce posílá zmíněnou jednu, nebo více převodních elektronických poukázek do zmíněného peněžního modulu příjemce,

d) zmíněný modul příjemce ověřuje platnost zmíněné jedné, či více elektronických poukázek,

e) zmíněný modul příjemce uchová informaci pro každou ze zmíněných jedné, nebo více elektronických poukázek a kde

krok (d) obsahuje pro každou převodní poukázku ze zmíněné jedné, nebo více převodních poukázek kroky, kontrolující informační záznam uchovaný v peněžním modulu příjemce, kde uvedený informační záznam představuje ostatní předchozí záznamy převedené na nebo mimo peněžní modul příjemce, zda má srovnatelný protějšek ke zmíněné převodní poukázce a kontrolují duplikátní záznam analýzou znaku stromu převodní poukázky založené na identifikovaných protějšcích převodní poukázky.

25.06.99

„ZMĚNĚNÝ LIST“

50. Způsob převodu elektronických poukázek předem určené celkové monetární hodnoty z peněžního modulu plátce na peněžní modul příjemce, který sestává z kroků ve kterých

a) zmíněný modul plátce vytváří jednu, nebo více převodních elektronických poukázek pomocí připojení příslušného převodního záznamu zmíněného peněžního modulu plátce ke každé ze zmíněných jedné, či více elektronických poukázek,

b) zmíněný peněžní modul plátce posílá jednu, nebo více převodních elektronických poukázek zmíněnému peněžnímu modulu příjemce,

c) zmíněný peněžní modul příjemce ověřuje platnost zmíněné jedné, nebo více převodních elektronických poukázek,

kde každá převodní elektronická poukázka ze zmíněné jedné, nebo více převodních elektronických poukázek obsahuje jedinečné identifikátory všech peněžních modulů příjemce po celou dobu převodu zmíněné elektronické poukázky a kde pro případy, kdy peněžním modulem příjemce je převodní peněžní modul, krok (c) dále zahrnuje kontrolní krok, zda každý zmíněný jedinečný identifikátor je na seznamu jedinečných identifikátorů pro neplatné peněžní moduly, který je uložen ve zmíněném peněžním modulu příjemce.

83. System podle nároku 1 v y z n a č u j í c í s e t í m, ž e zmíněný seznam převodních záznamů je způsobilý obsáhnout množství převodních záznamů.

84. System podle nároku 1 v y z n a č u j í c í s e t í m, ž e seznam převodních záznamů zahrnuje množství převodních záznamů, přičemž každý převodní záznam je generován odpovídajícím elektronickým modulem plátce.

85. System podle nároku 5 v y z n a č u j í c í s e t í m, ž e zmíněná elektronická poukázka před přidáním převodního záznamu obsahuje jiný převodní záznam, který má jiné pořadové číslo, kde zmíněný jiný převodní záznam odpovídá zmíněné elektronické poukázce dříve převedené do zmíněného elektronického modulu plátce.

86. Způsob podle nároku 50 v y z n a č u j í c í s e t í m, ž e peněžní modul příjemce je převodní peněžní modul.

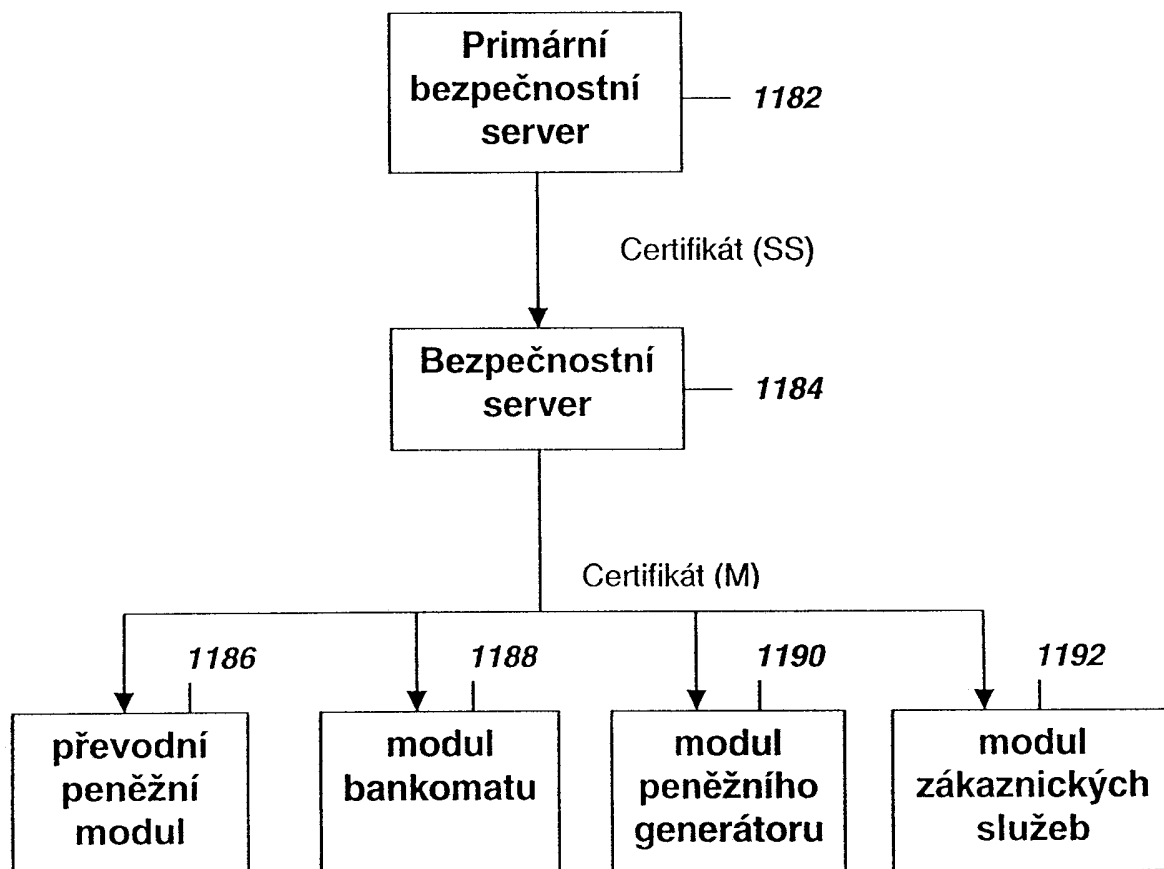
87. Způsob podle nároku 50 v y z n a č u j í c í s e t í m, ž e zmíněný krok peněžního modulu plátce vytváří jednu nebo více převodních elektronických poukázek, včetně připojení příslušného digitálního podpisu zmíněného peněžního modulu plátce na každou zmíněnou jednu, nebo více elektronických poukázek.

88. Způsob podle nároku 50 v y z n a č u j í c í s e t í m, ž e pro každou zmíněnou jednu, nebo více elektronických poukázek příslušného převodního záznamu se indikuje zda všechny, nebo některá část peněžní částky zmíněné jedn, nebo více elektronických poukázek je převedena.

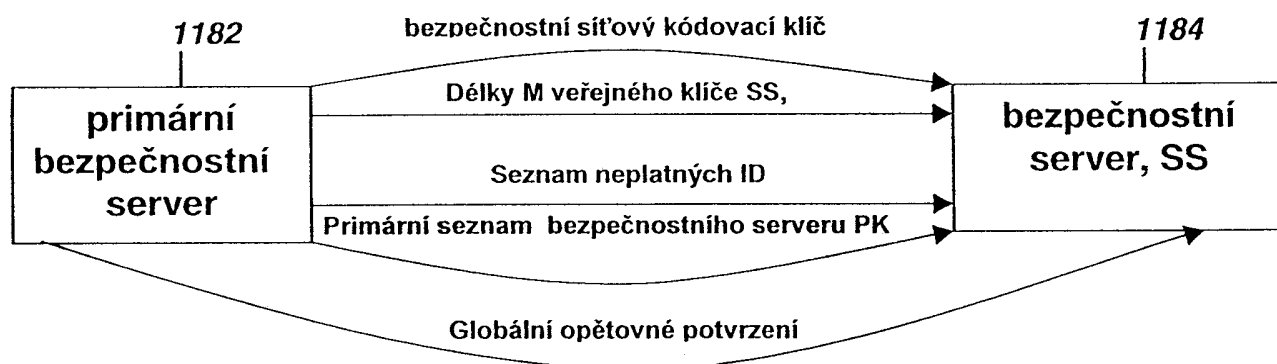
Poznámky překladatele:

- ¹ se vzory
- ² ve významu napálit, překonat, podvést
- ³ ve významu všechny převáděné nebo vydávané obnosy peněz
- ⁴ tato věta musí mít obrácený smysl, tedy místo platný musí být neplatný chyba v originálu
- ⁵ originál upraven tak, aby byl v souladu s Obr. 8A
- ⁶ upraveno podle Obr. 8A
- ⁷ MM znamená peněžní modul
- ⁸ zde bude asi chyba, protože doplněk je obvykle definován jako rozdíl množin
- ⁹ rozumí se jako funkce
- ¹⁰ tento text se odkazuje na obrázek 12, který není v souboru. V souboru jsou Obr. 12A a 12B, které však neobsahují prvek, který je označen číslem 1186
- ¹¹ slovo "převod" doplnil překladatel
- ¹² pravděpodobně má být CSMHA
- ¹³ ve významu "slučují"
- ¹⁴ pravděpodobně má být CSMHA
- ¹⁵ rozumí se i ukradený
- ¹⁶ změněn singulár na plurál
- ¹⁷ v originálu vypadlo slovo správně má asi být ...unclaimed failed commit information...

1/54

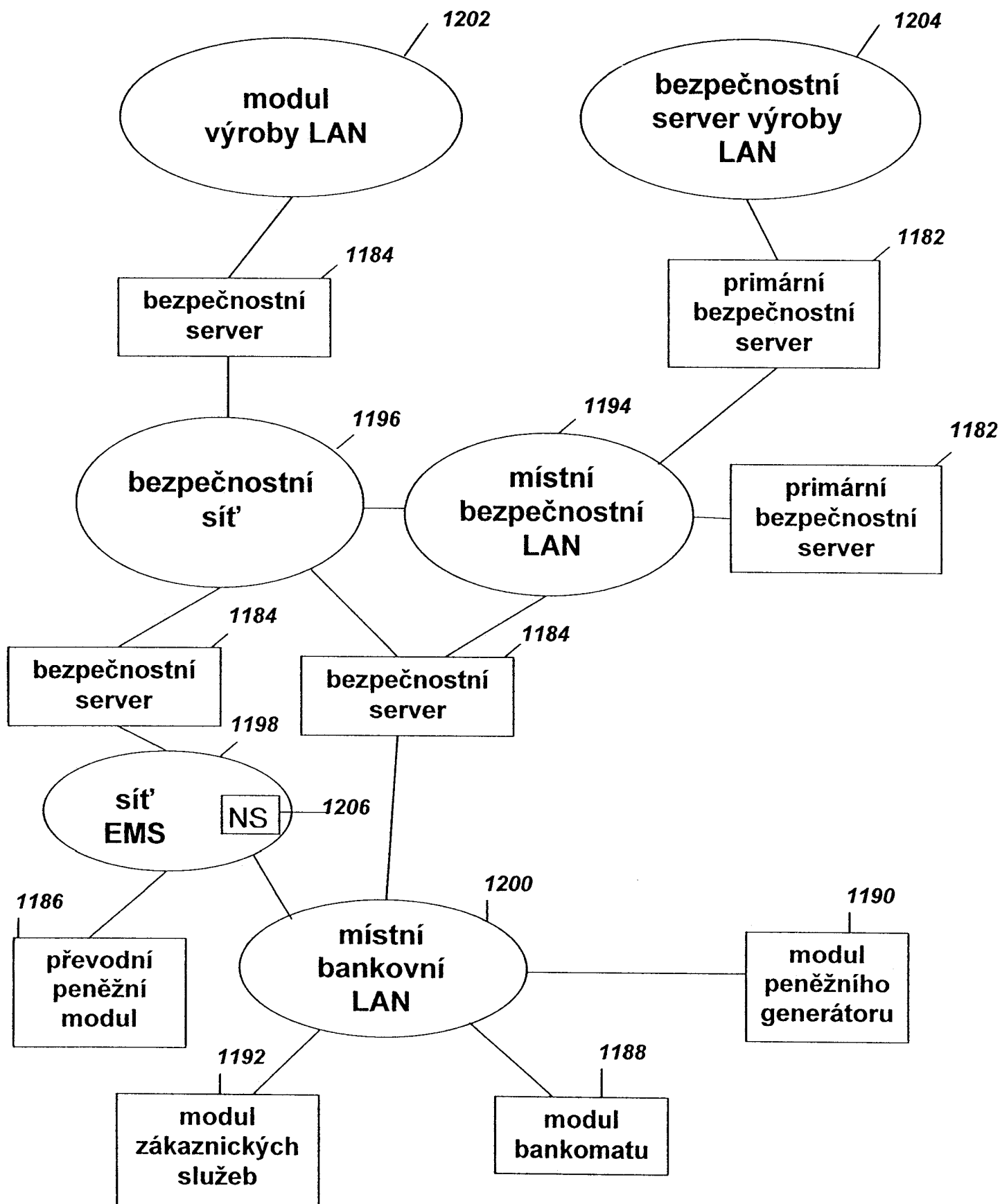


Obr. 1A



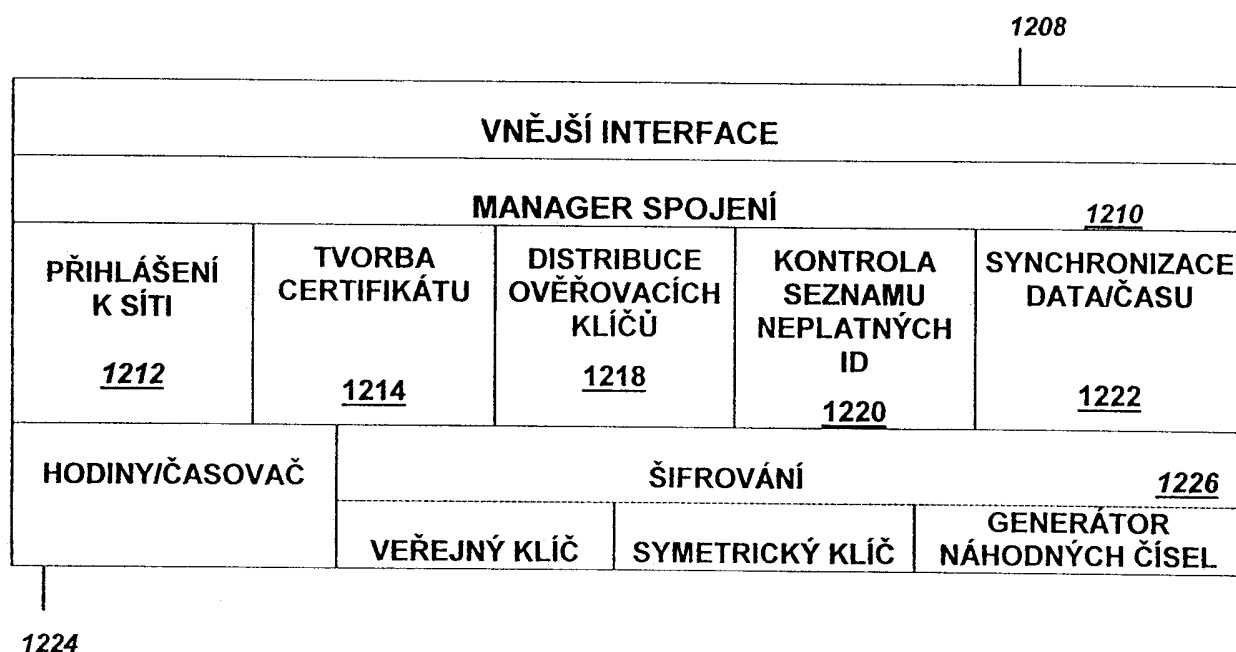
Obr. 1B

2/54

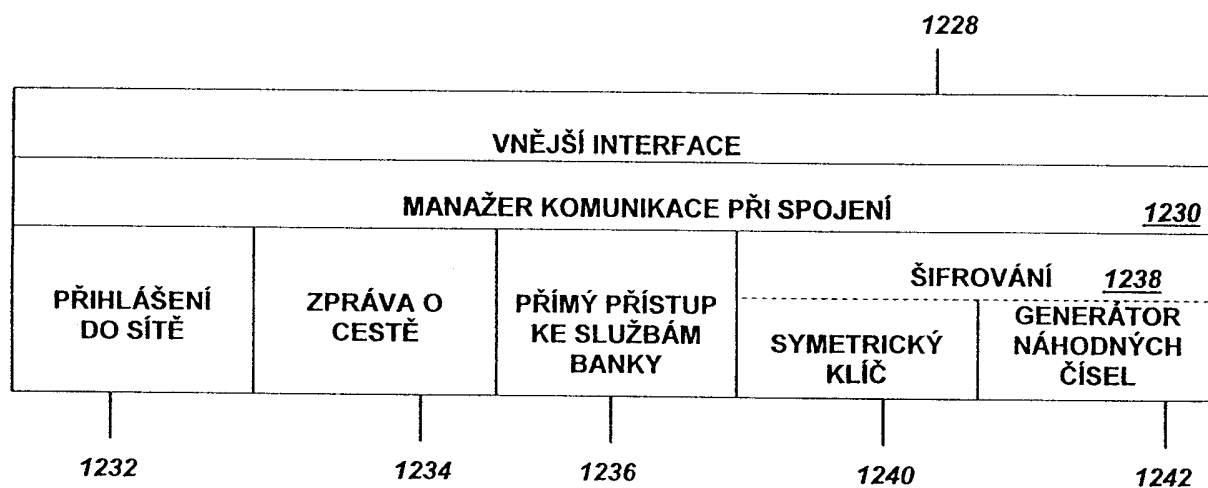


Obr. 2

3/54

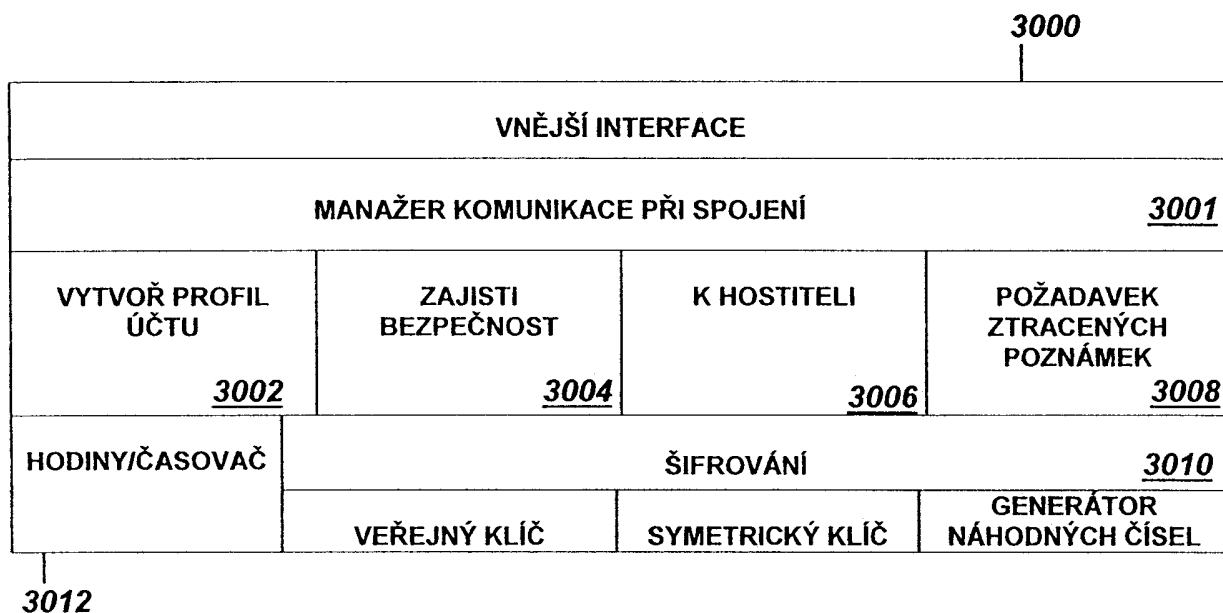


Obr. 3A

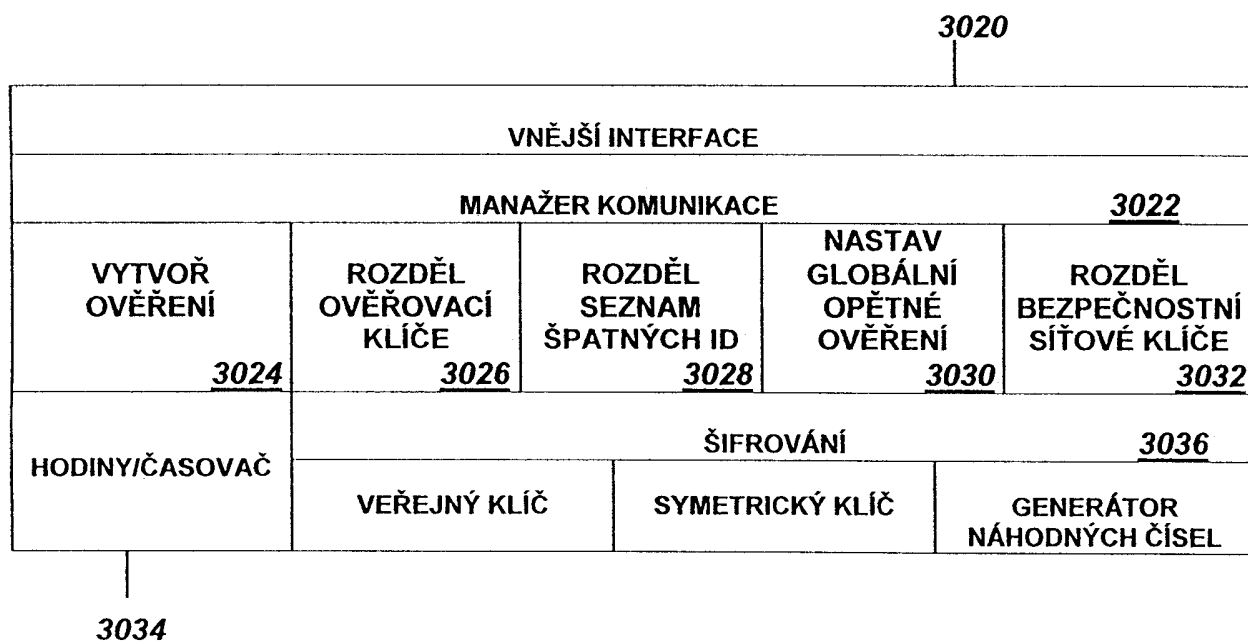


Obr. 3B

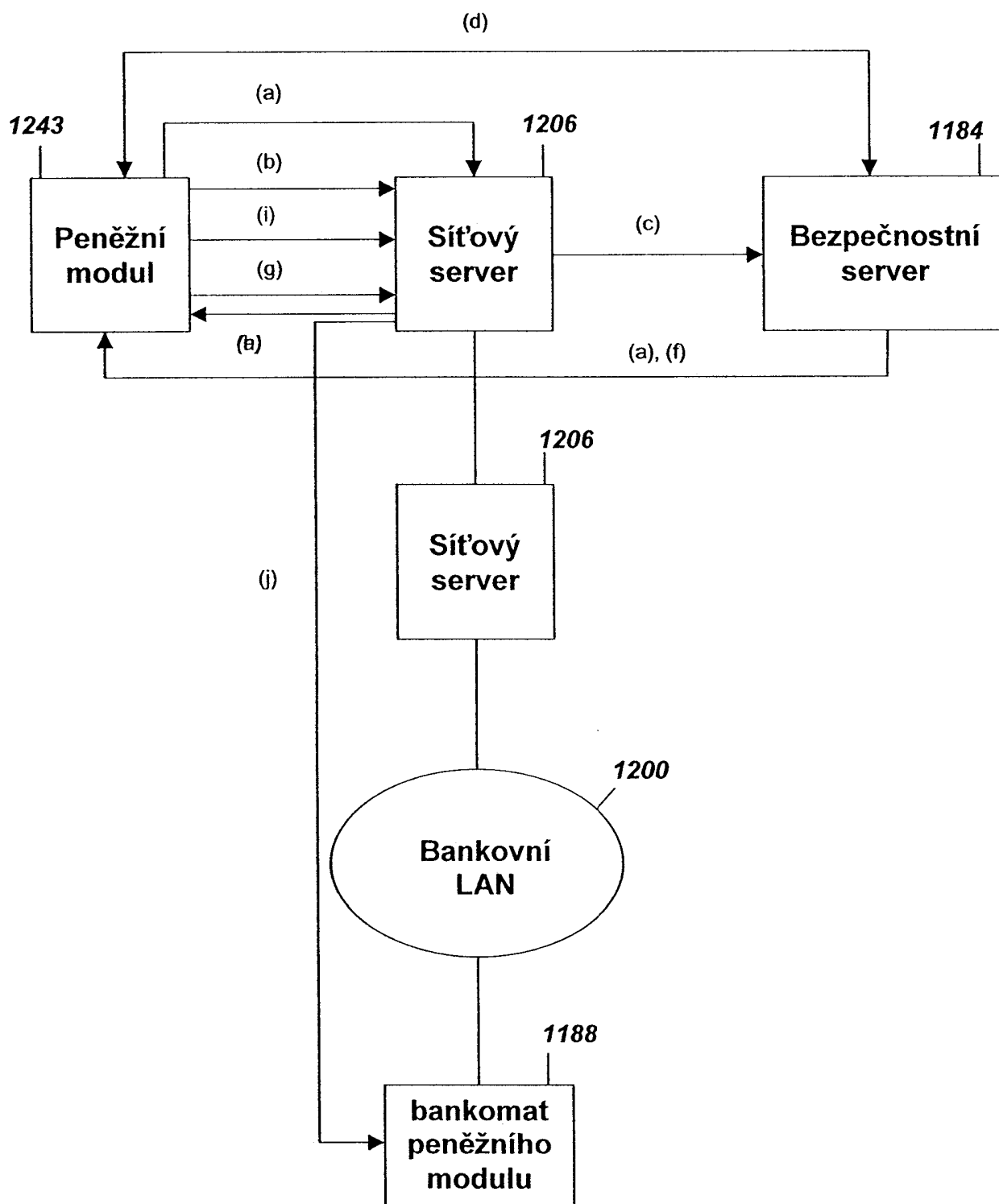
4/54



Obr. 4A

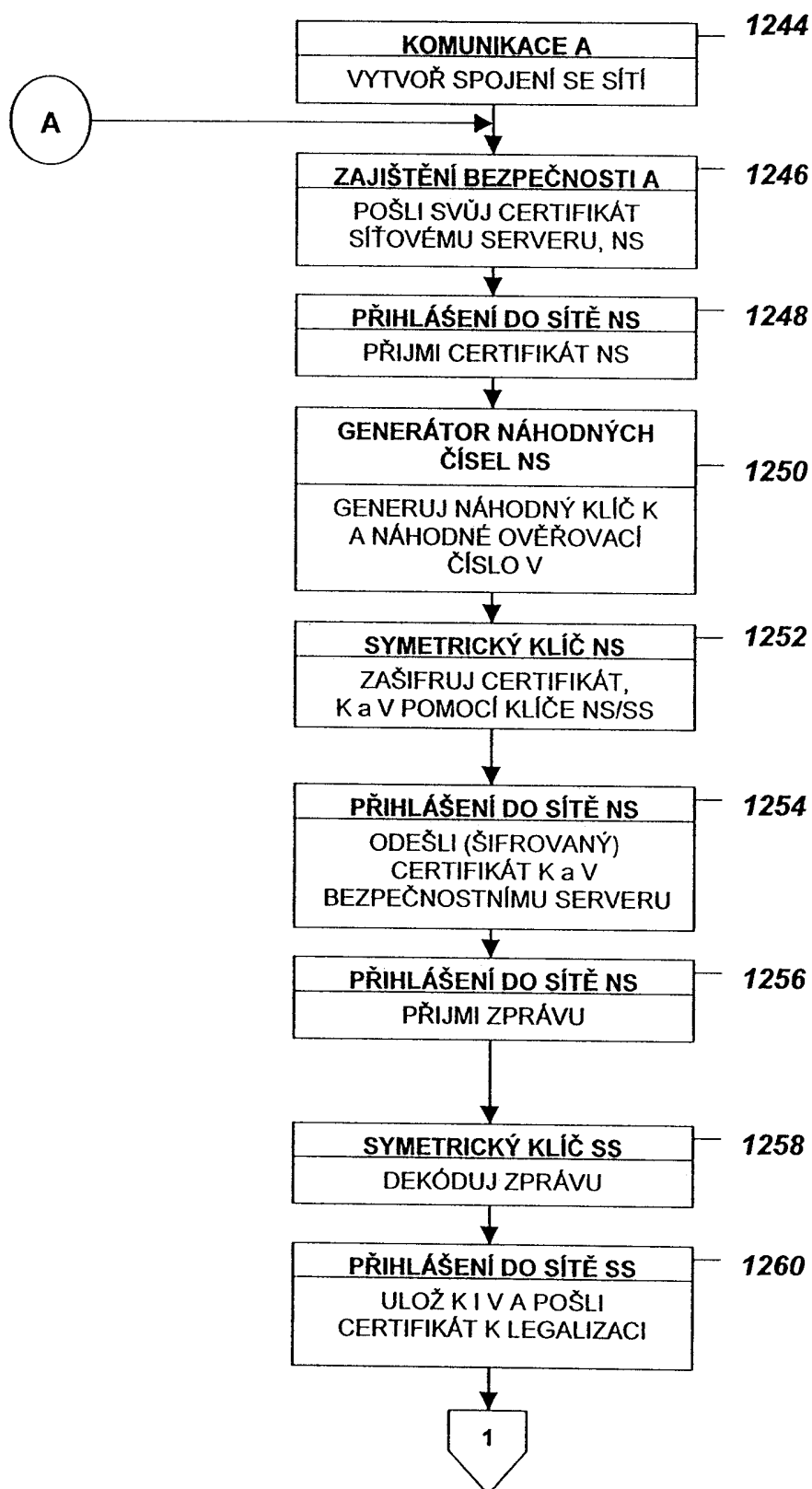


Obr. 4B

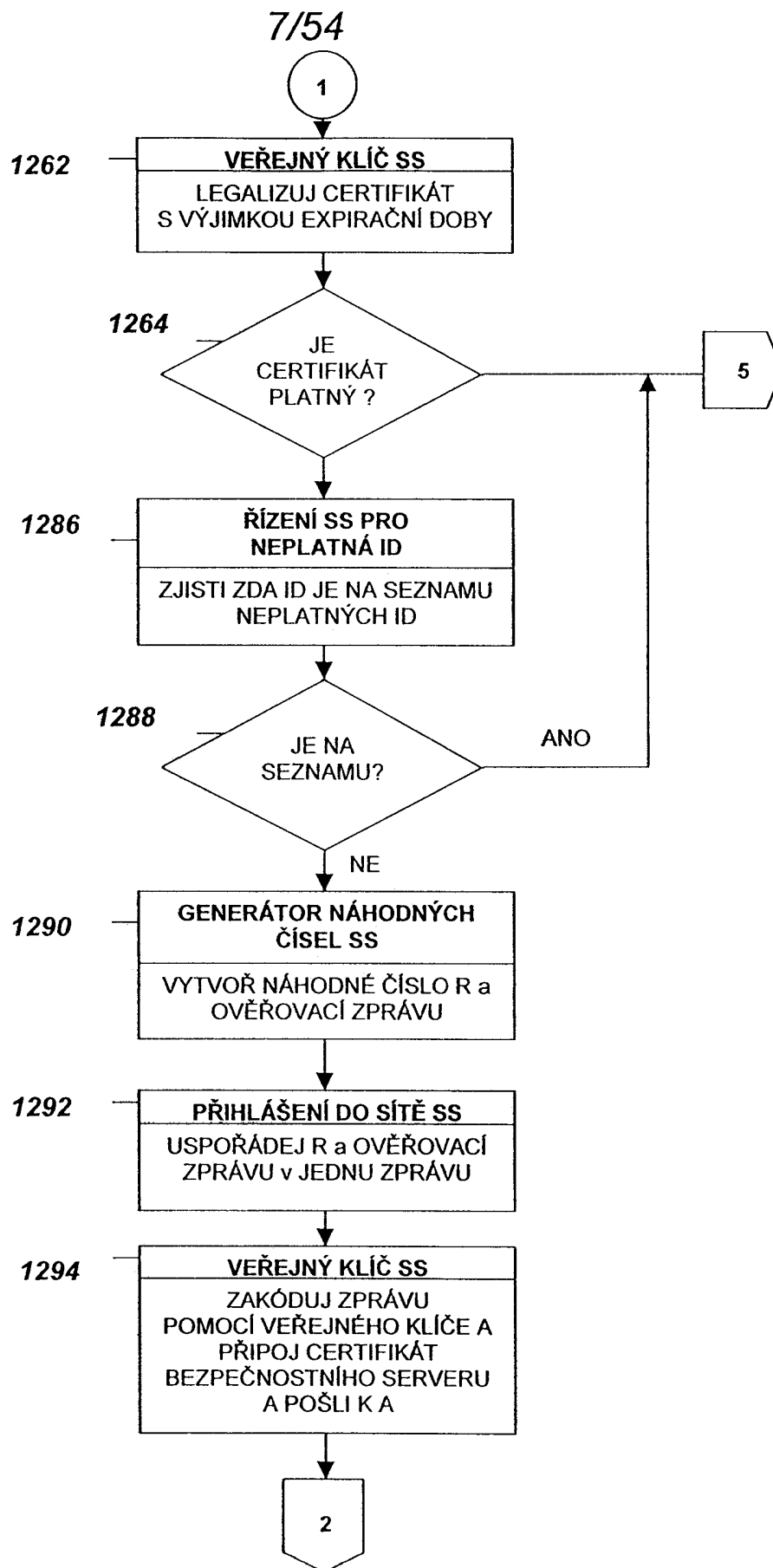


Obr. 5

6/54

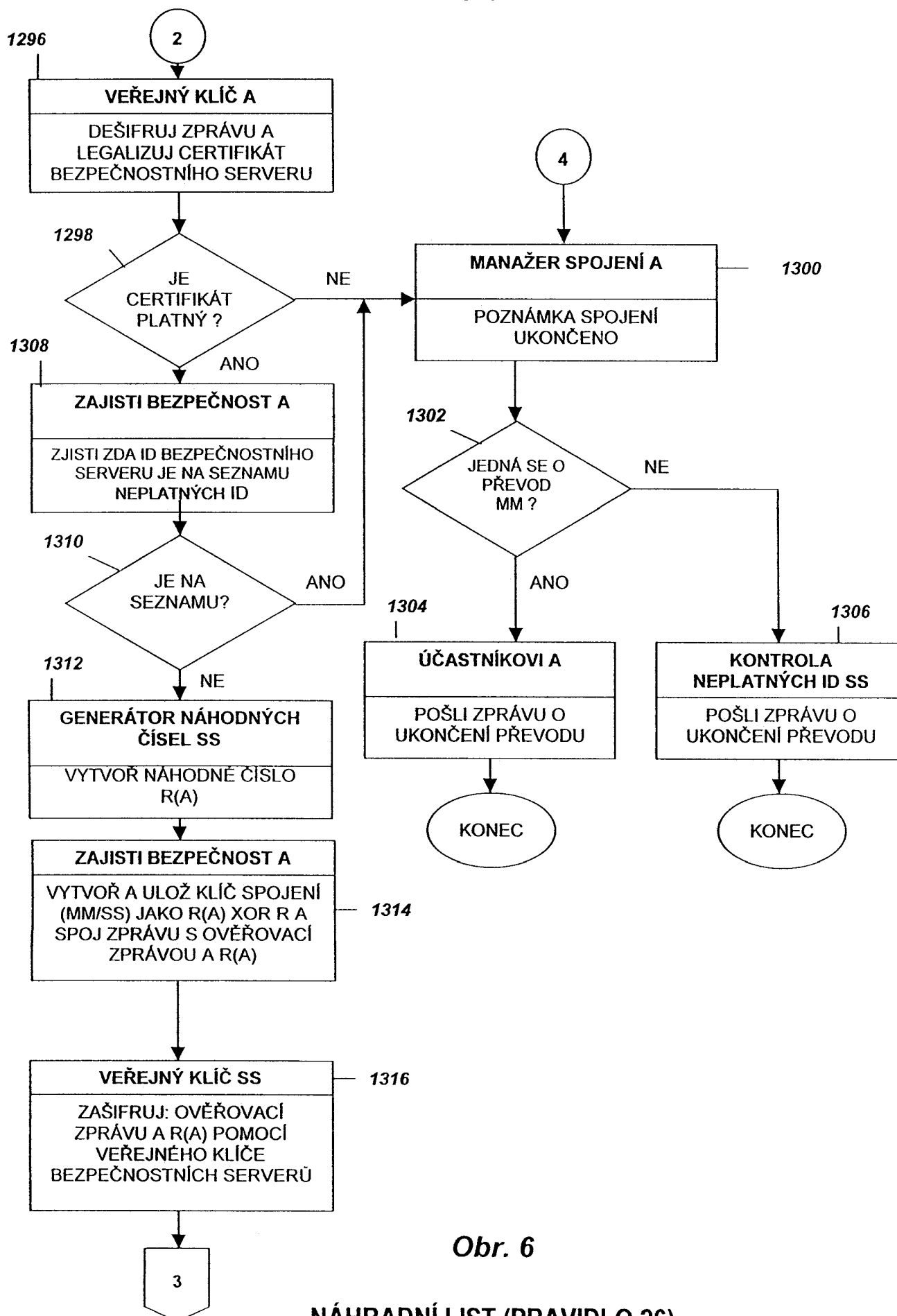


Obr. 6A

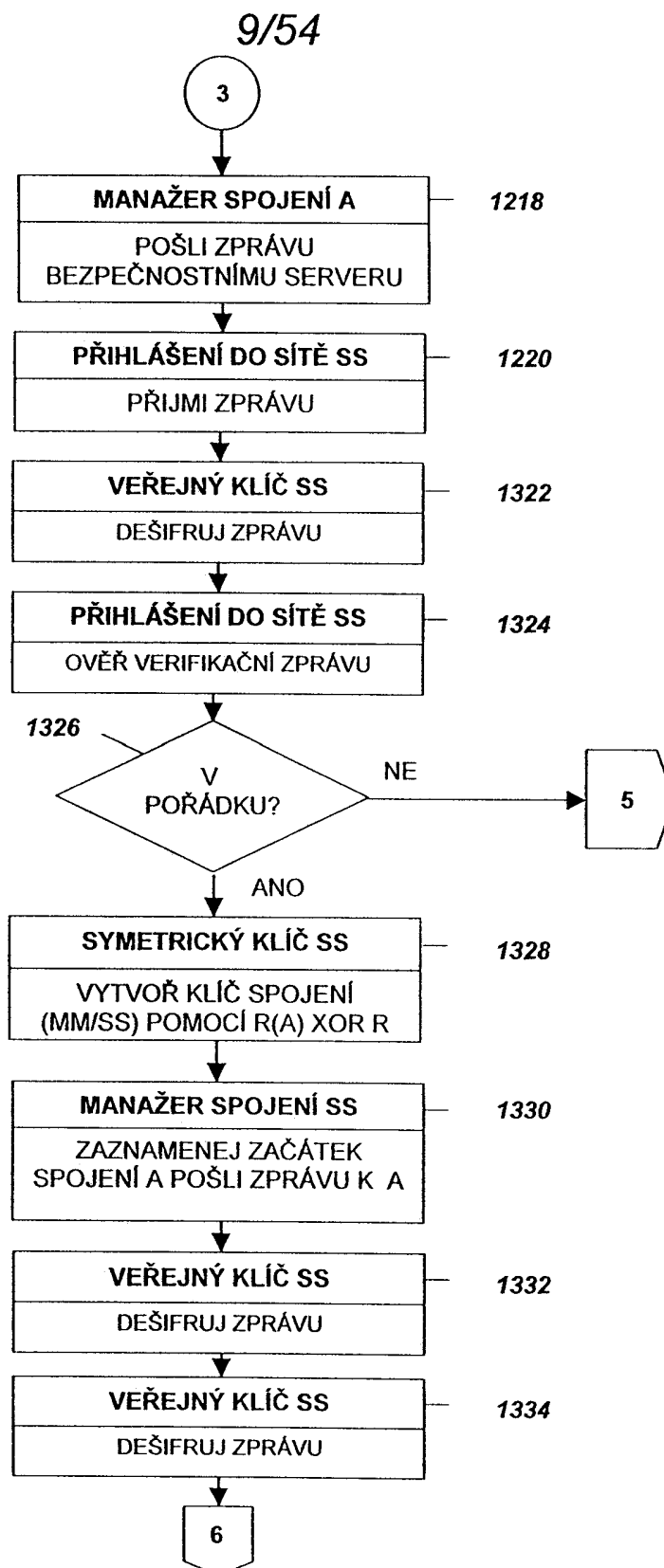


Obr. 6B

8/54

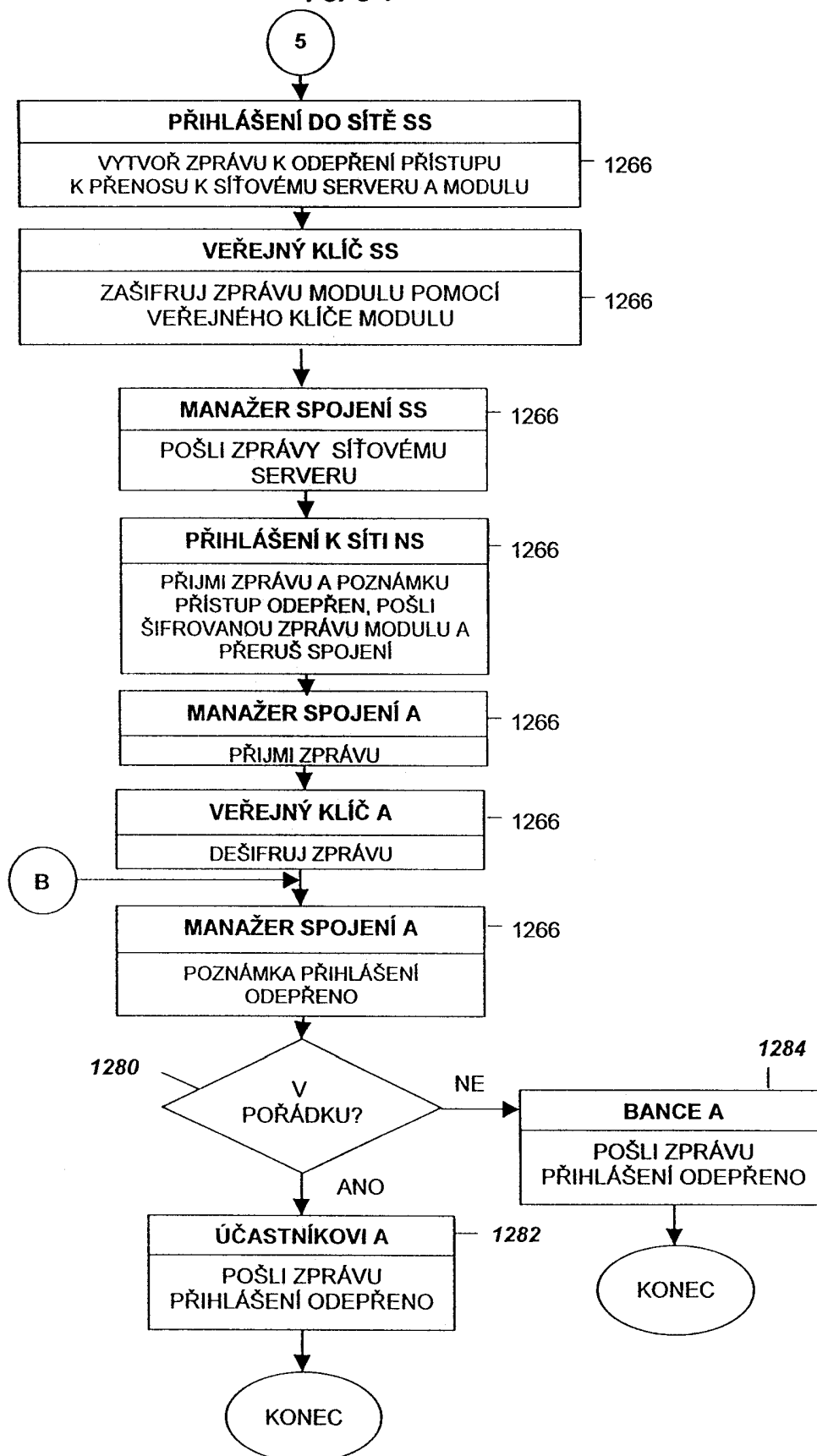


Obr. 6

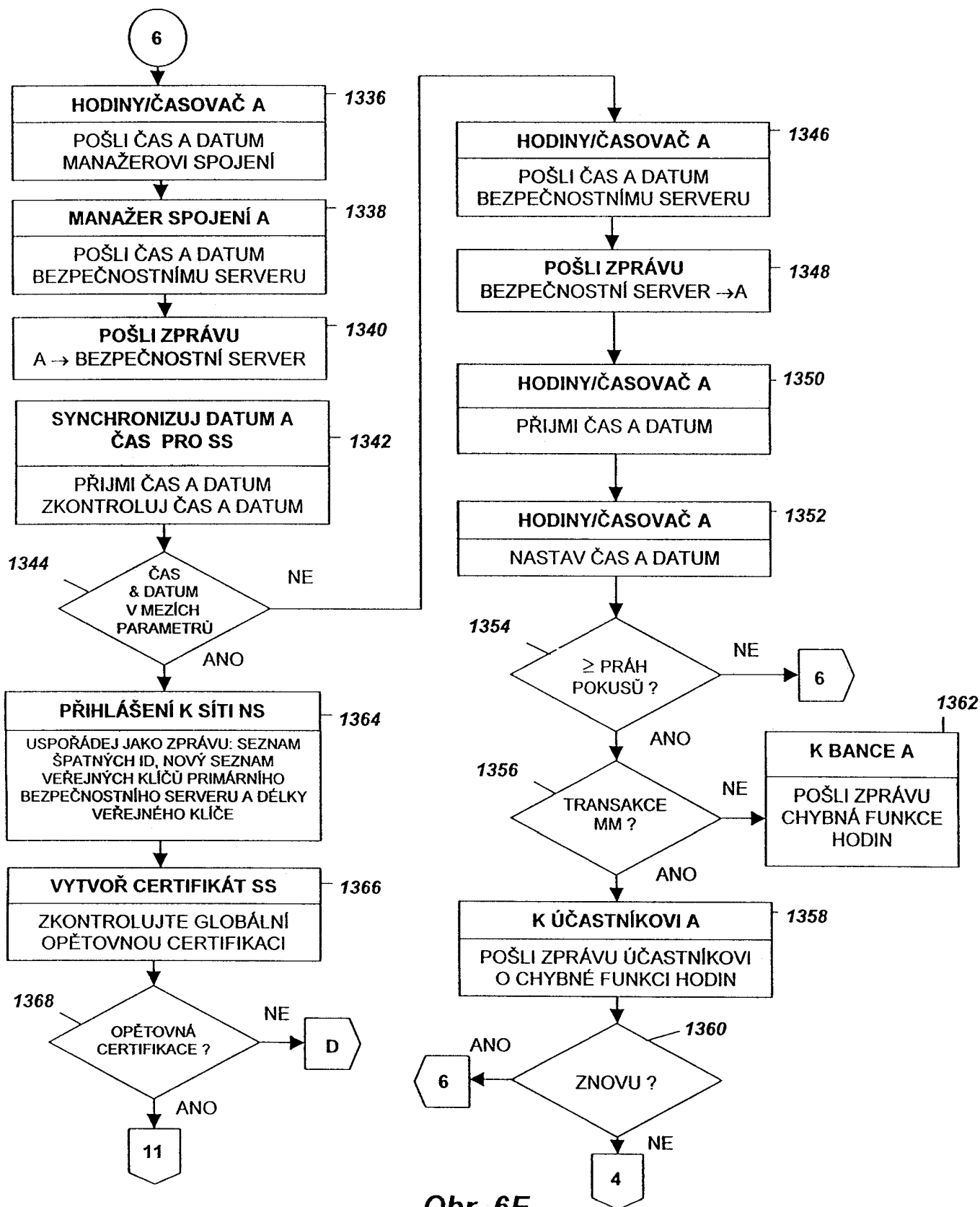


Obr. 6D

10/54

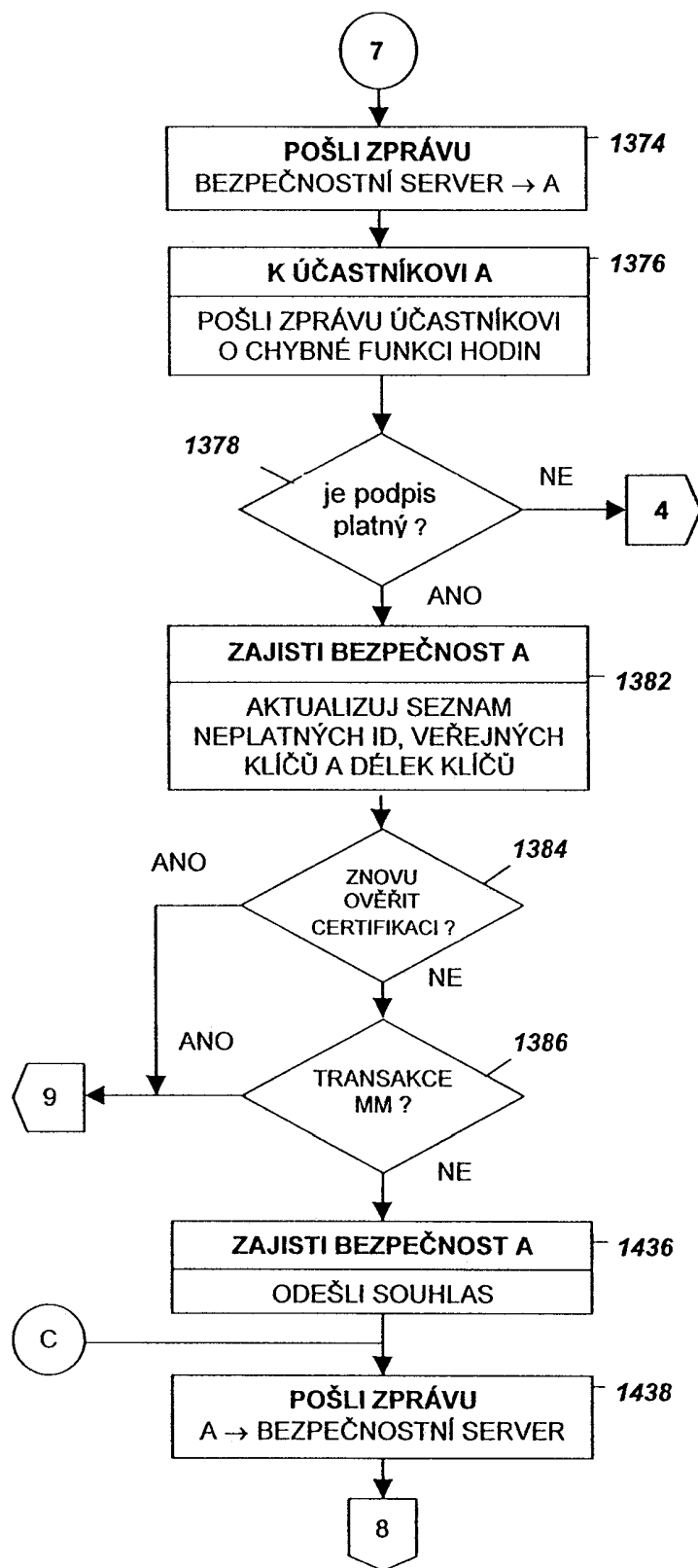


Obr. 6E



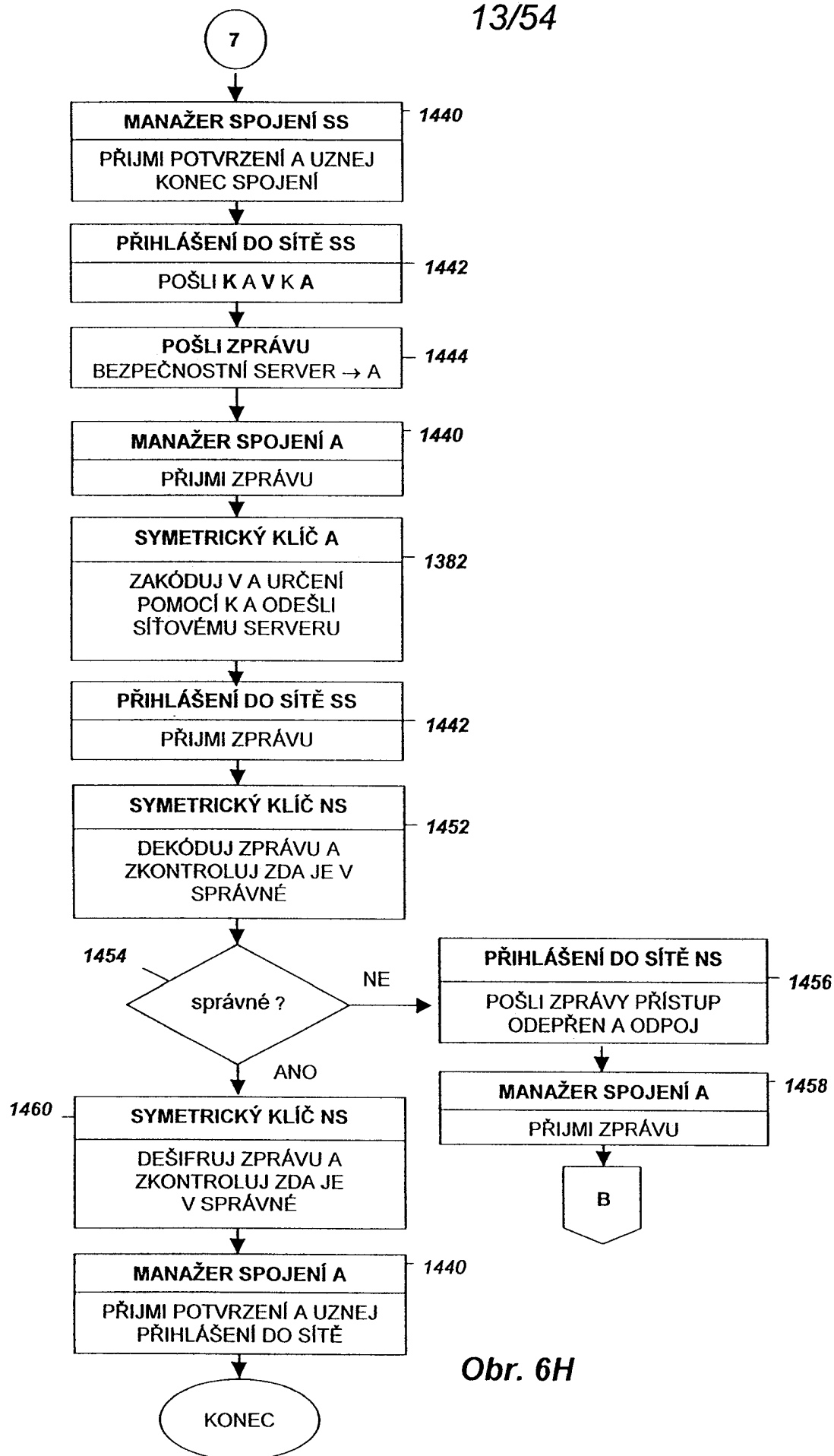
Obr. 6F

12/54



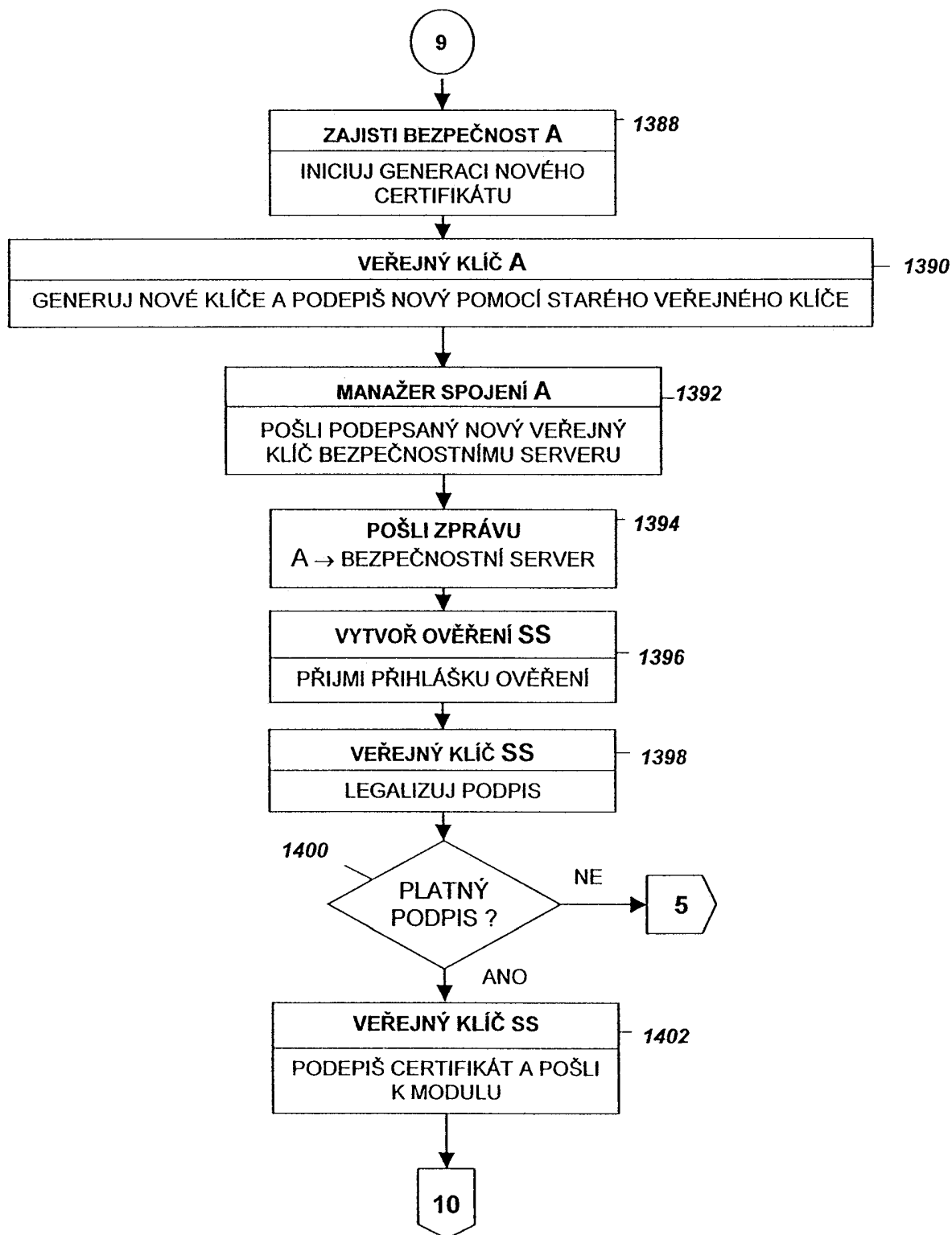
Obr. 6G

13/54



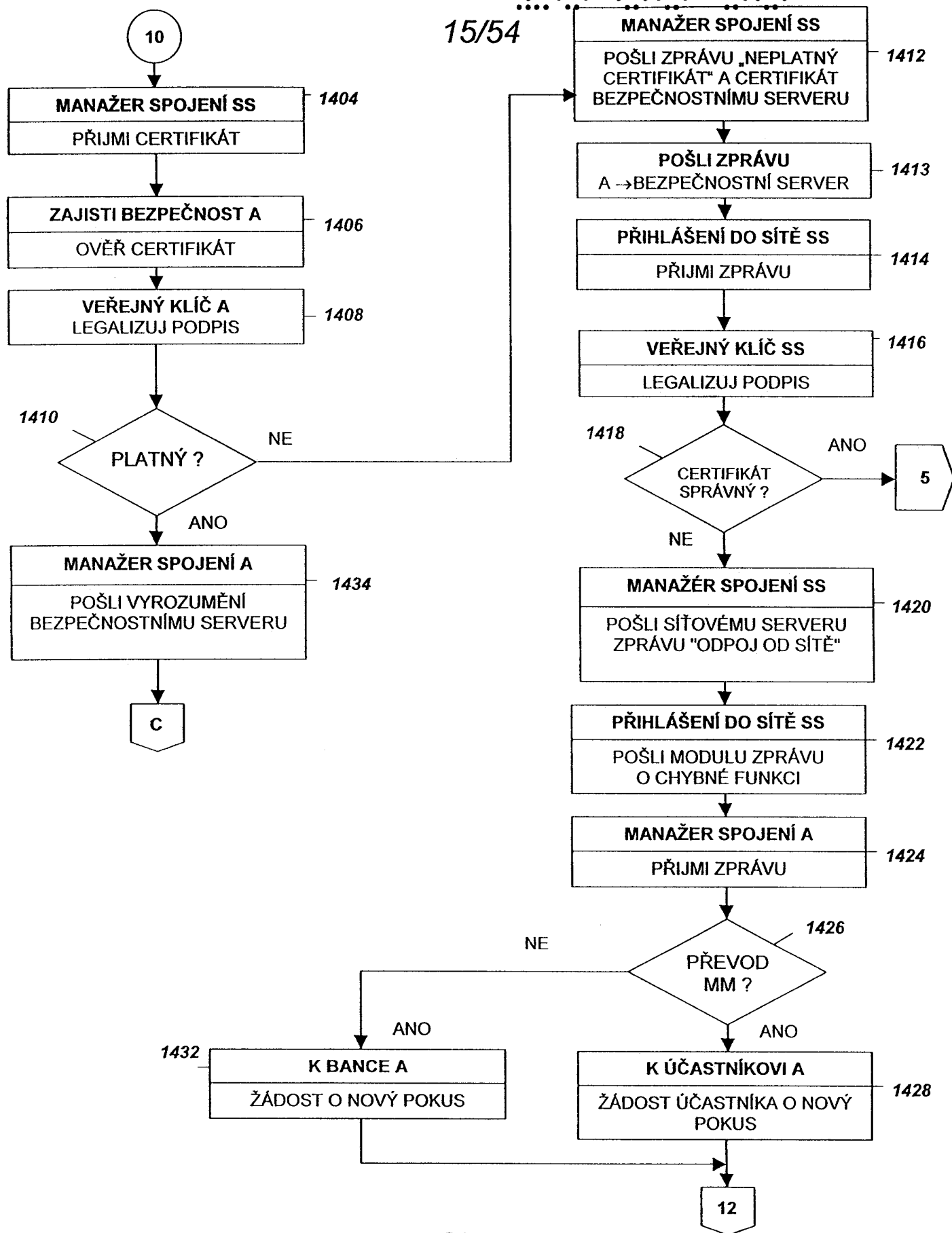
Obr. 6H

14/54

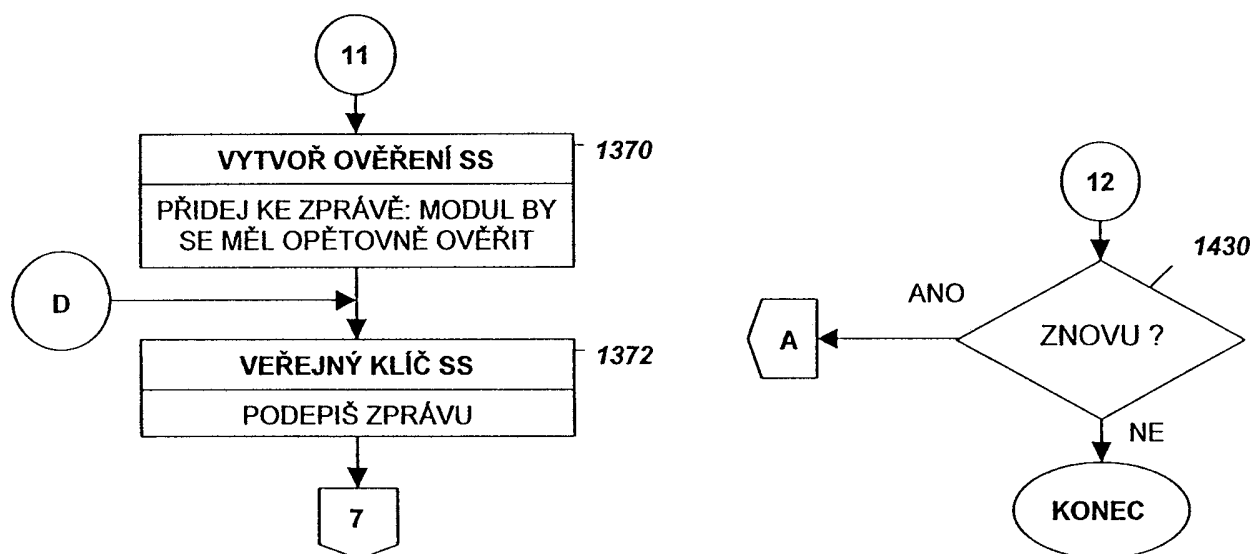


Obr. 6I

15/54

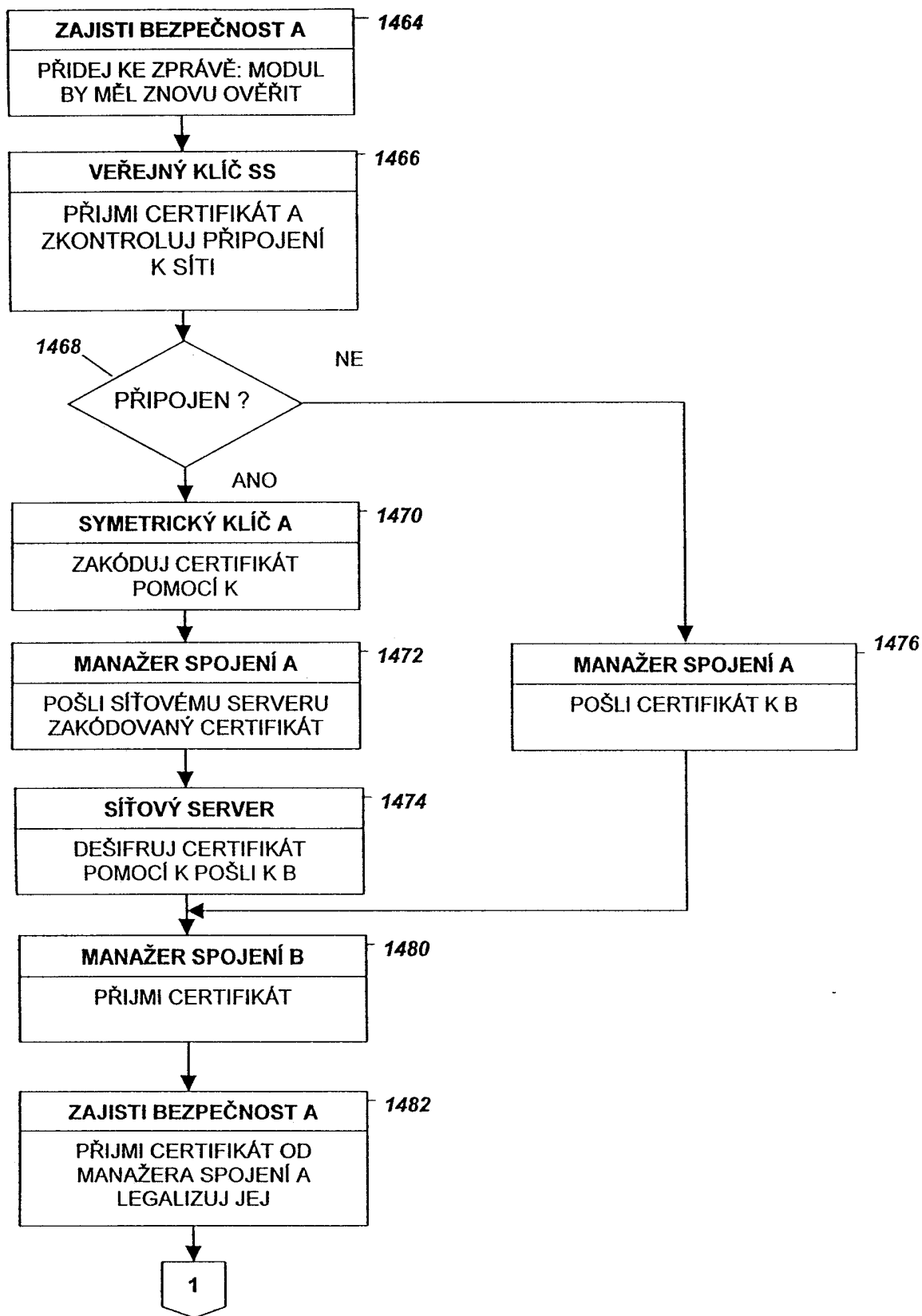


Obr. 6J

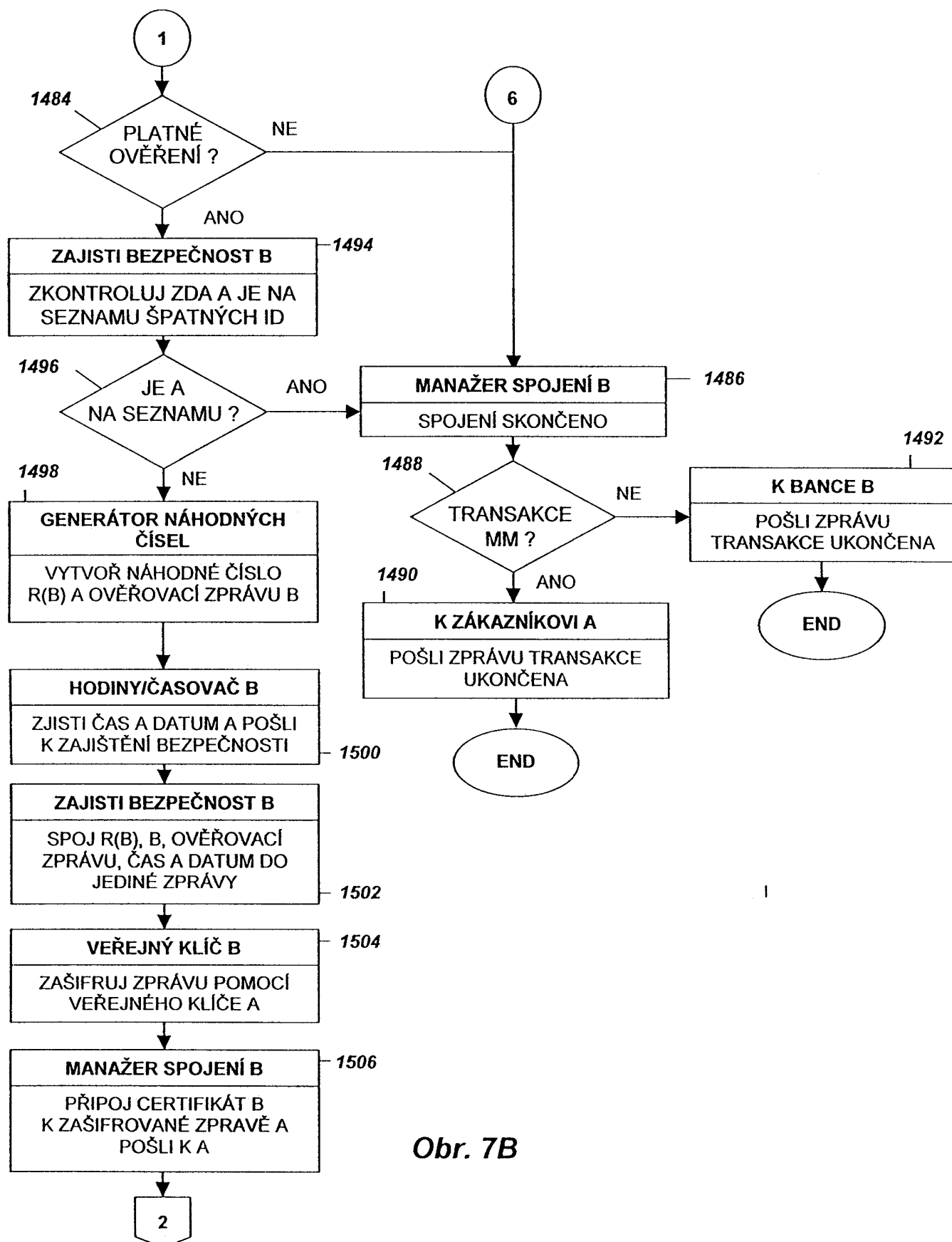


Obr. 6K

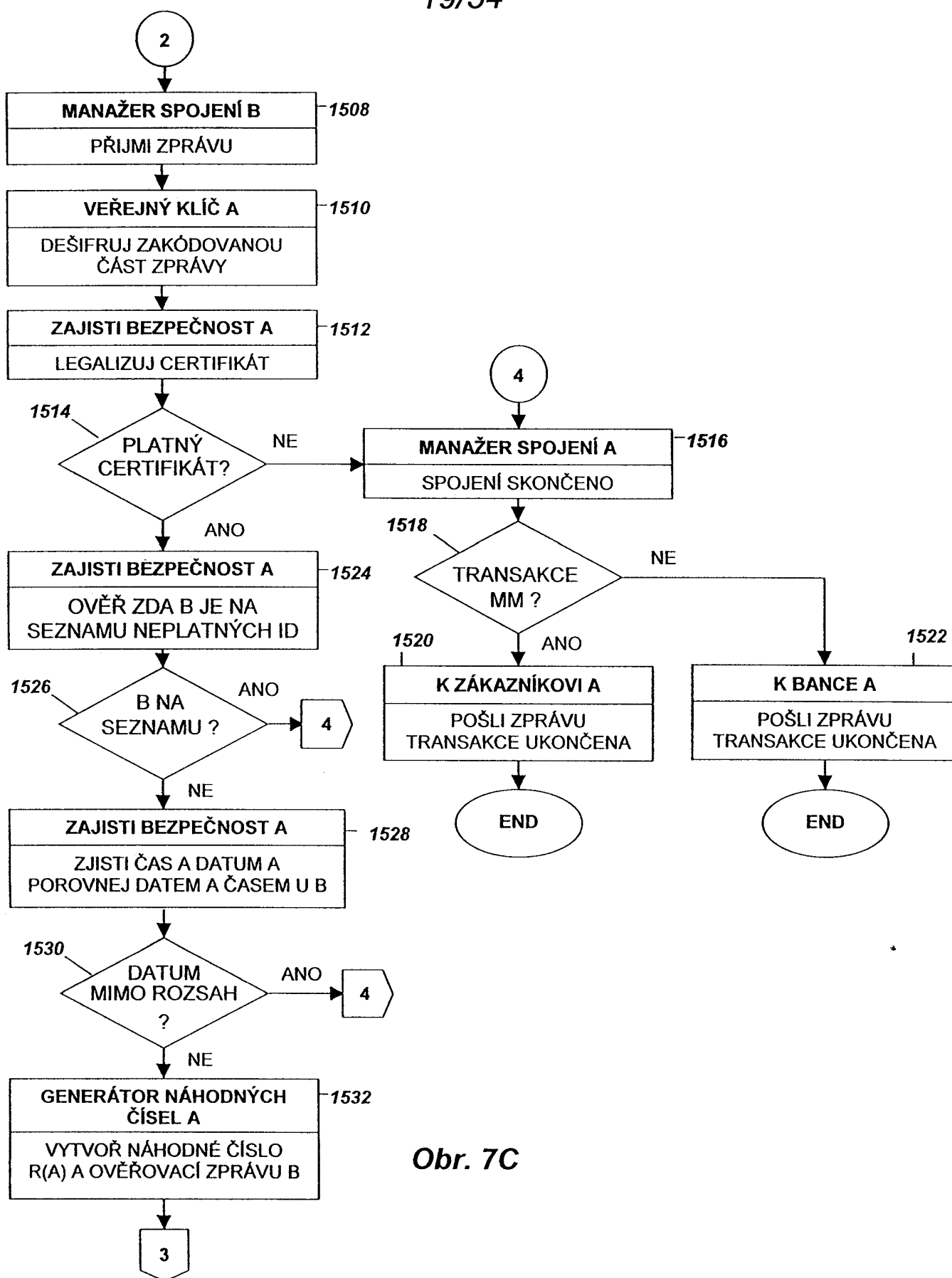
17/54



Obr. 7A

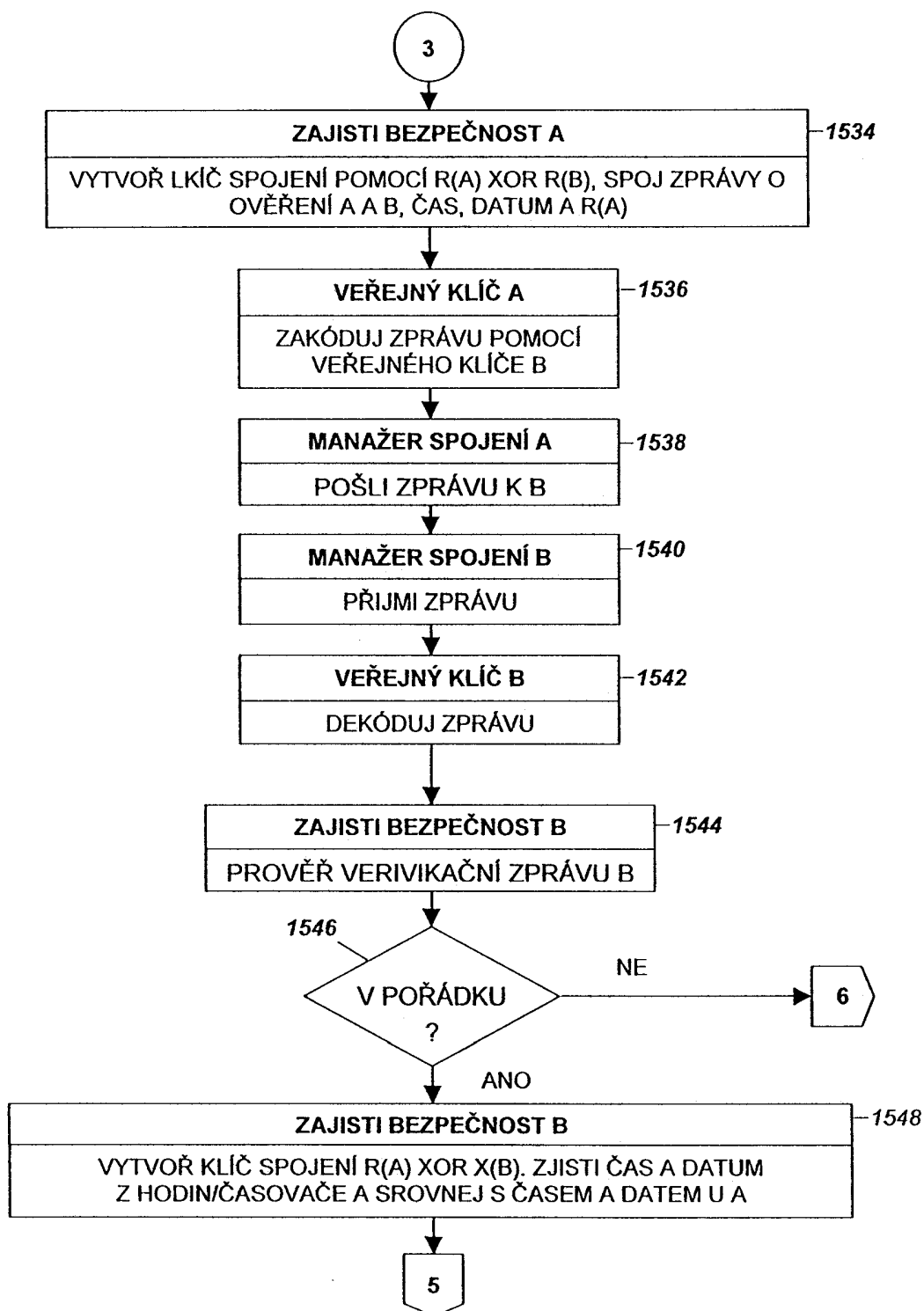


Obr. 7B

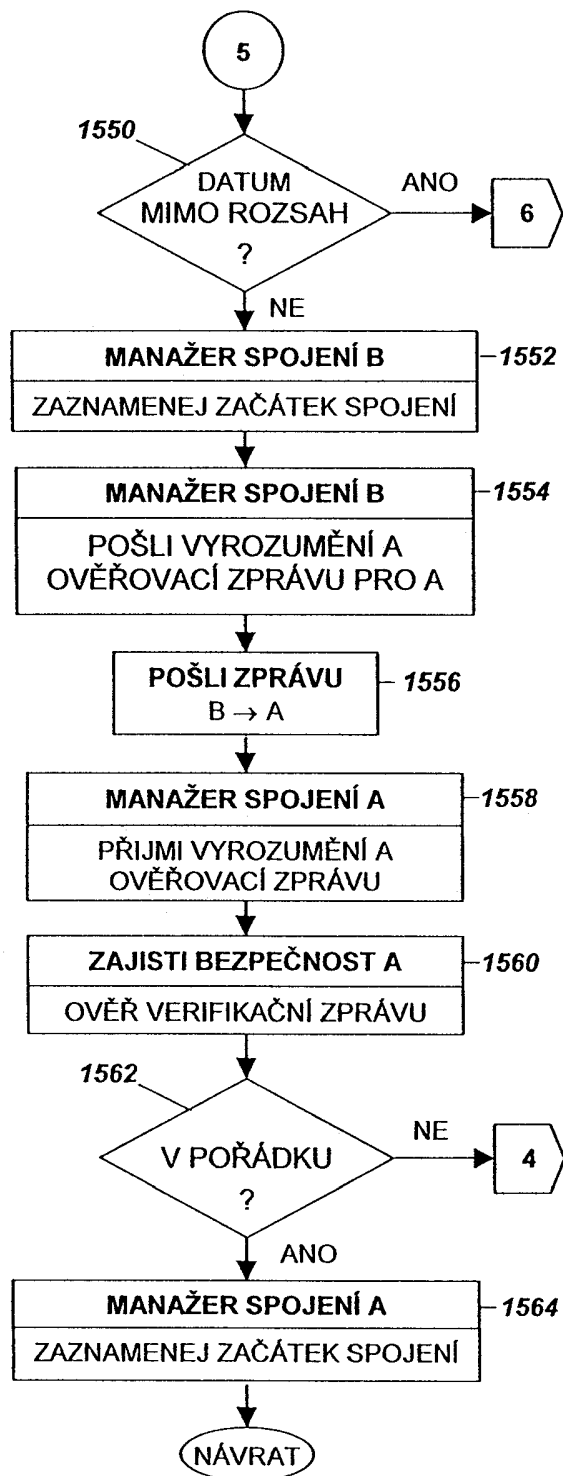


Obr. 7C

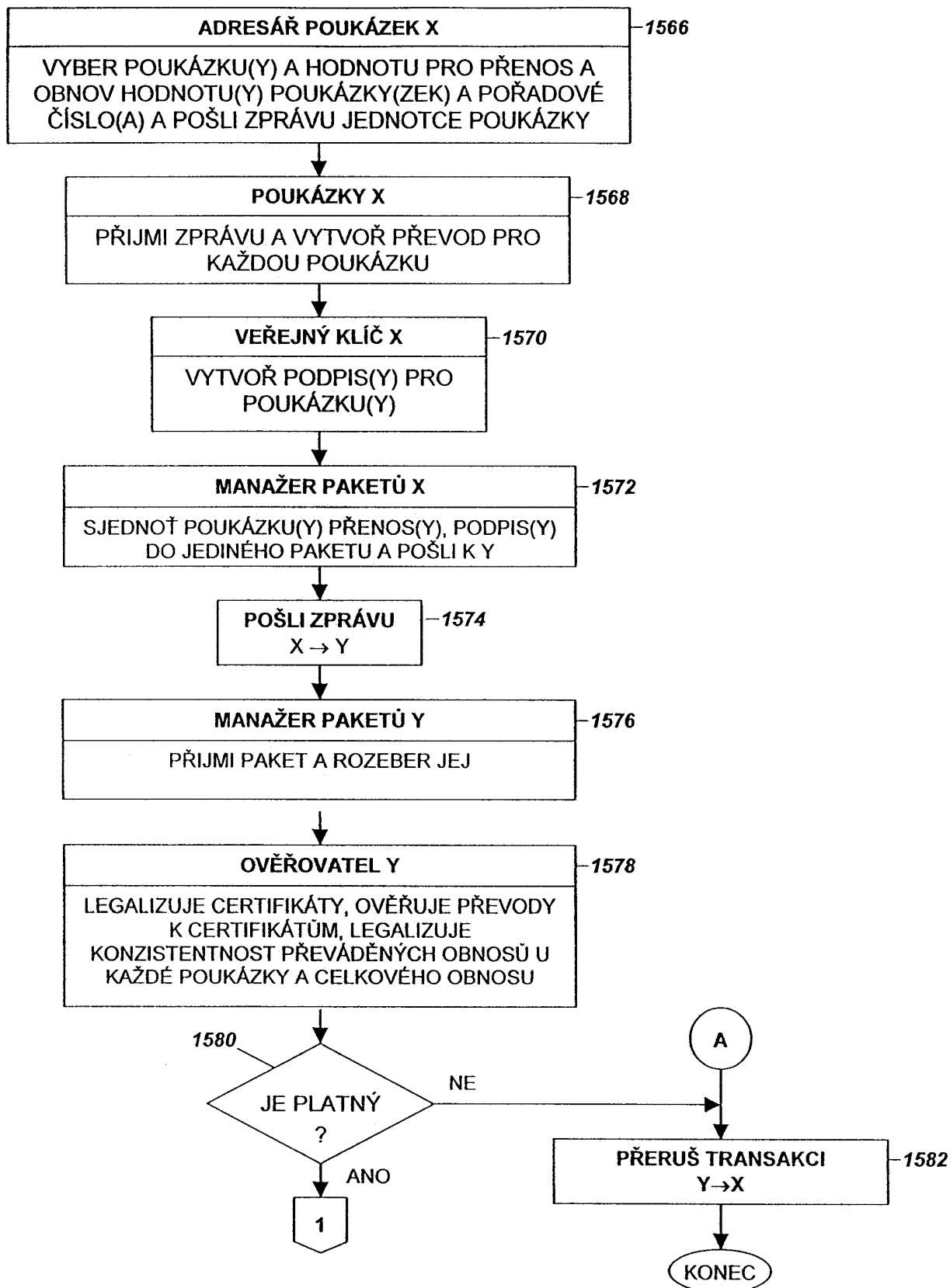
20/54



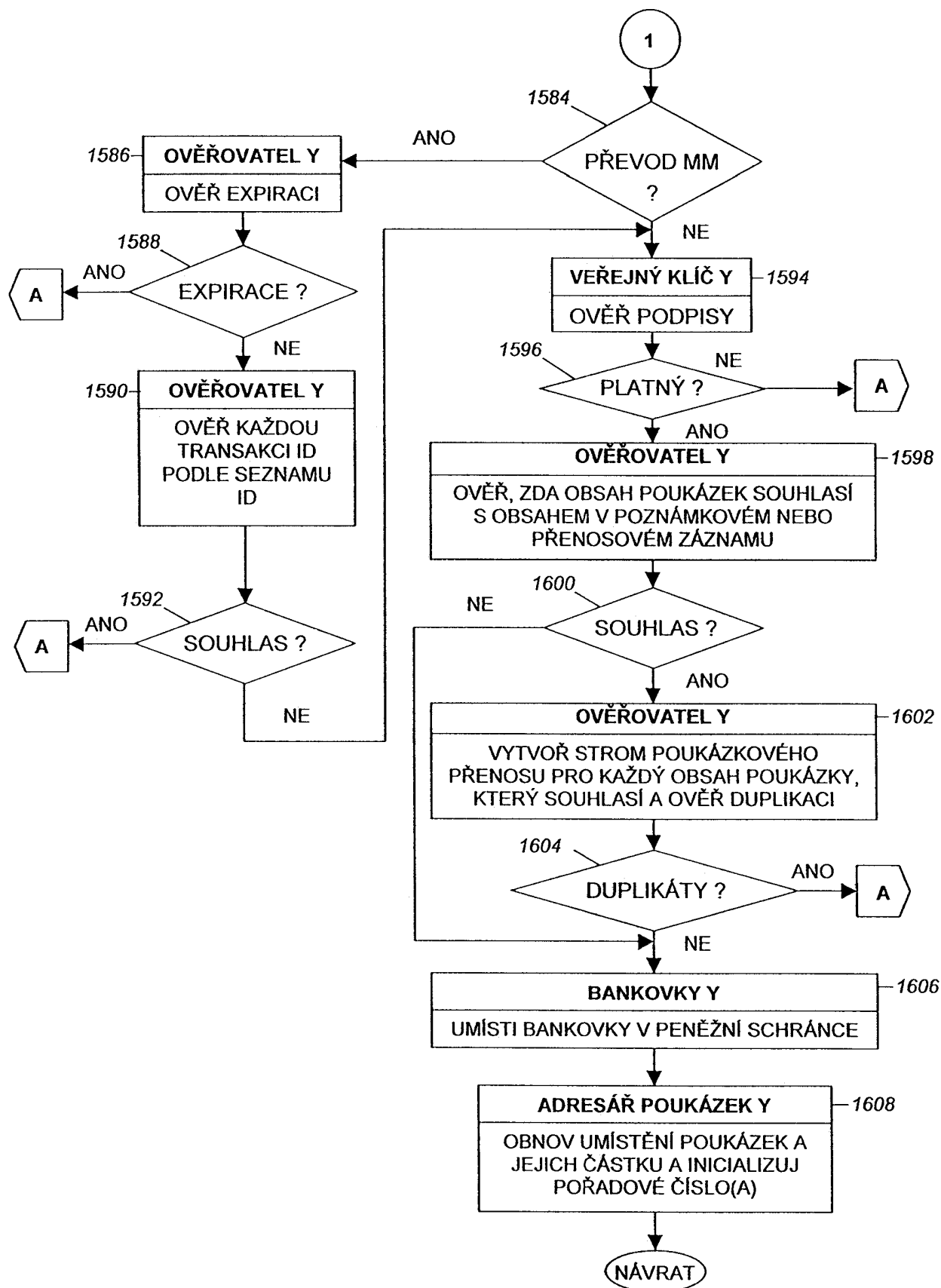
Obr. 7D



Obr. 7E

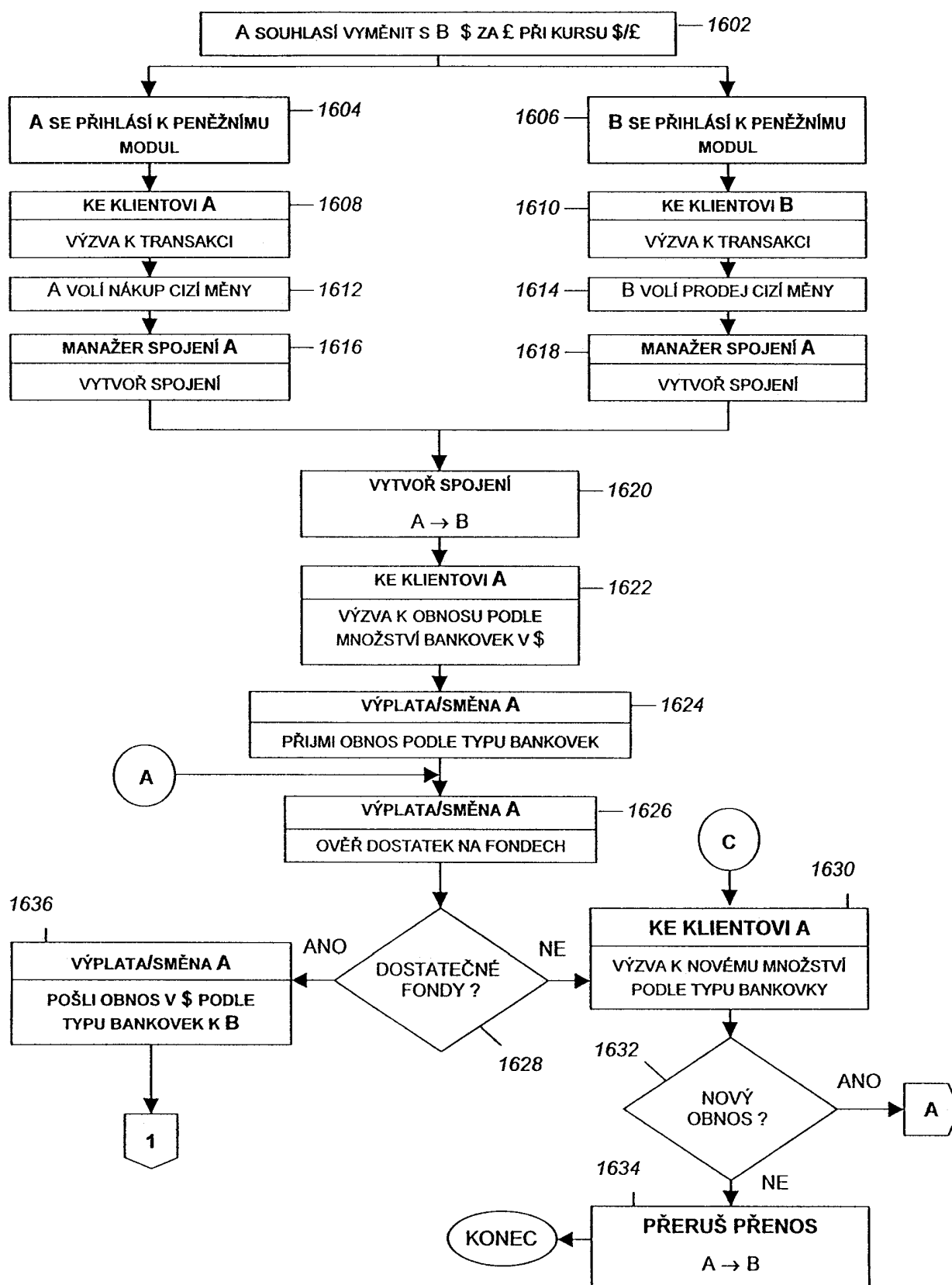


Obr. 8A

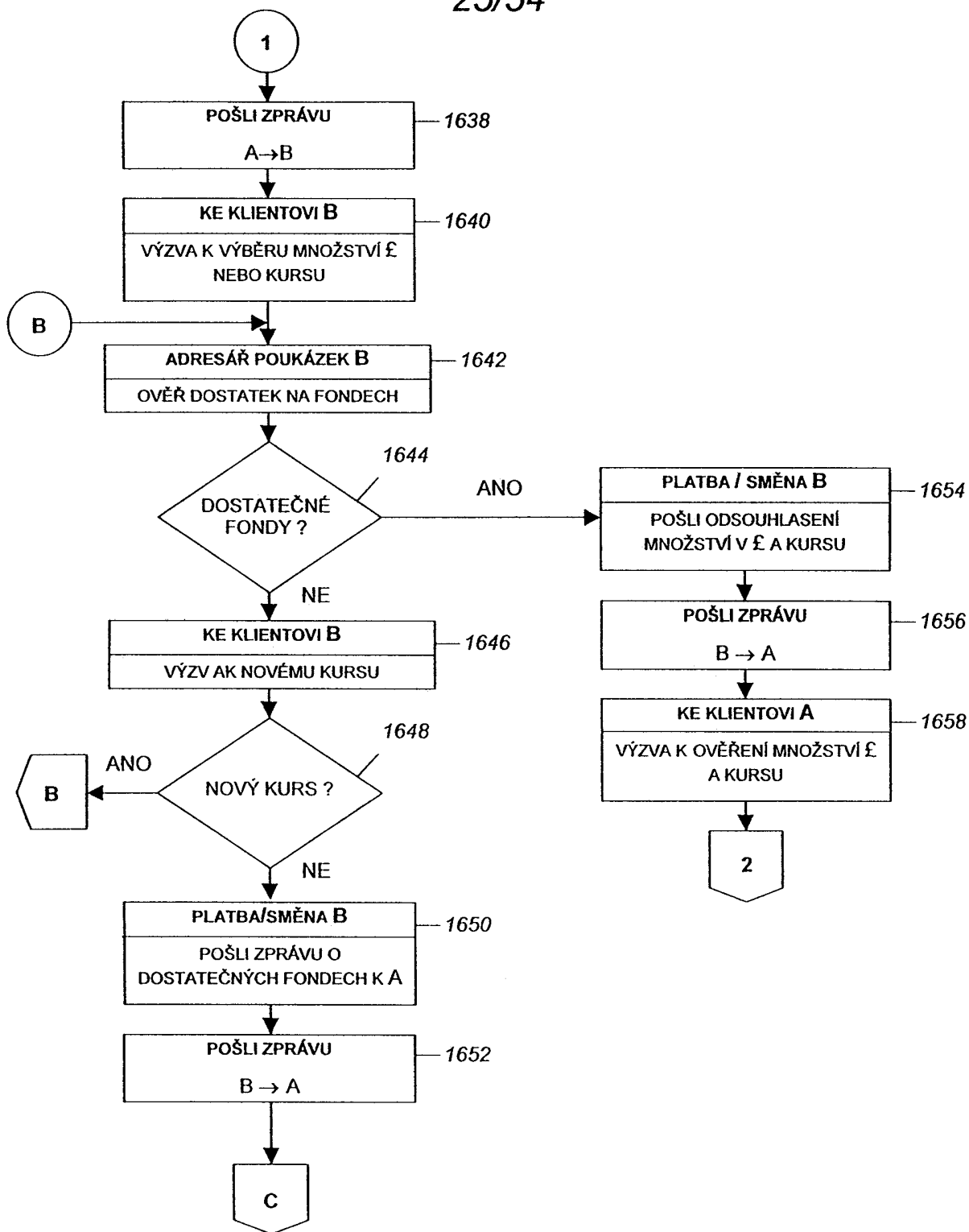


Obr. 8B

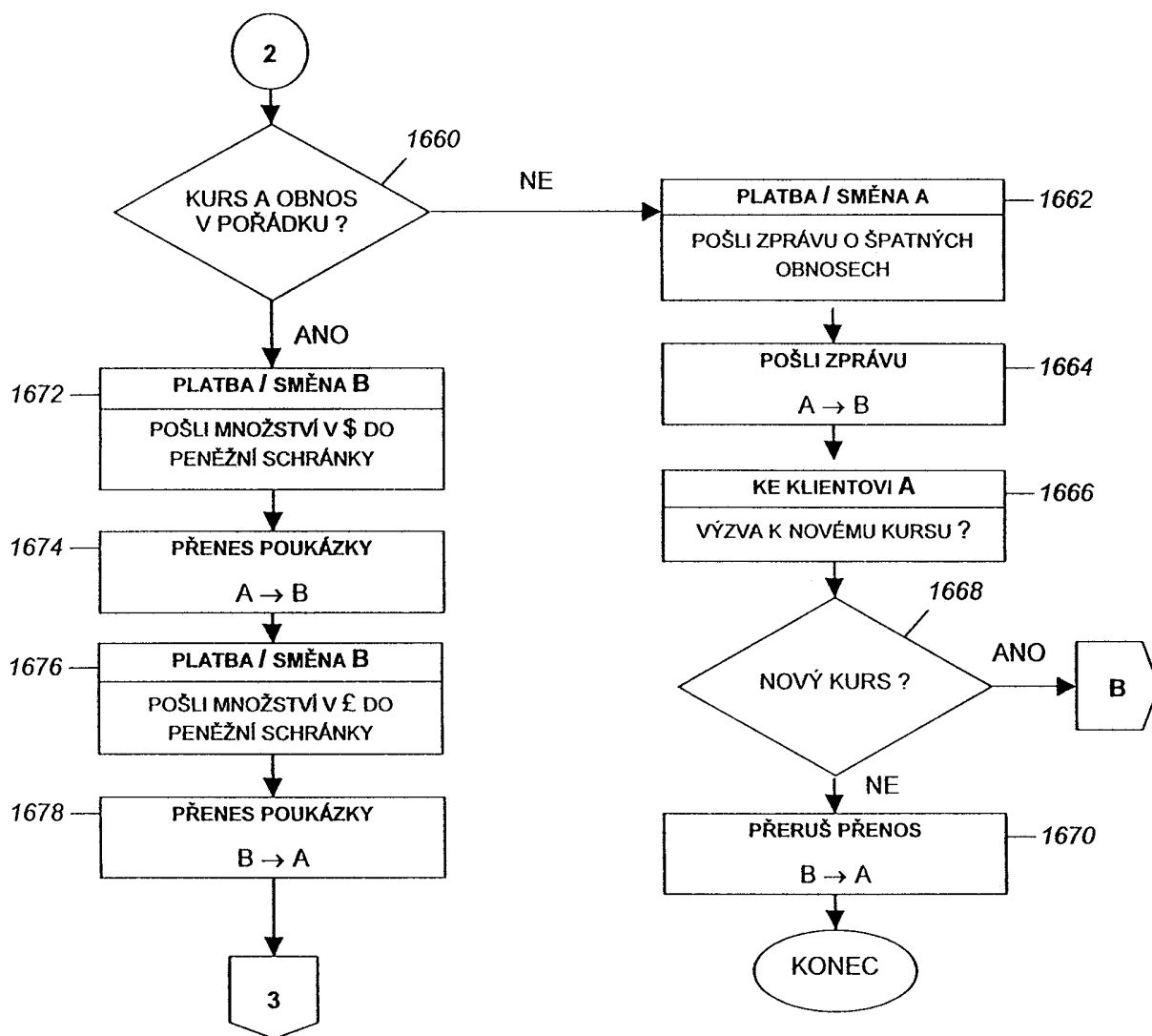
24/54



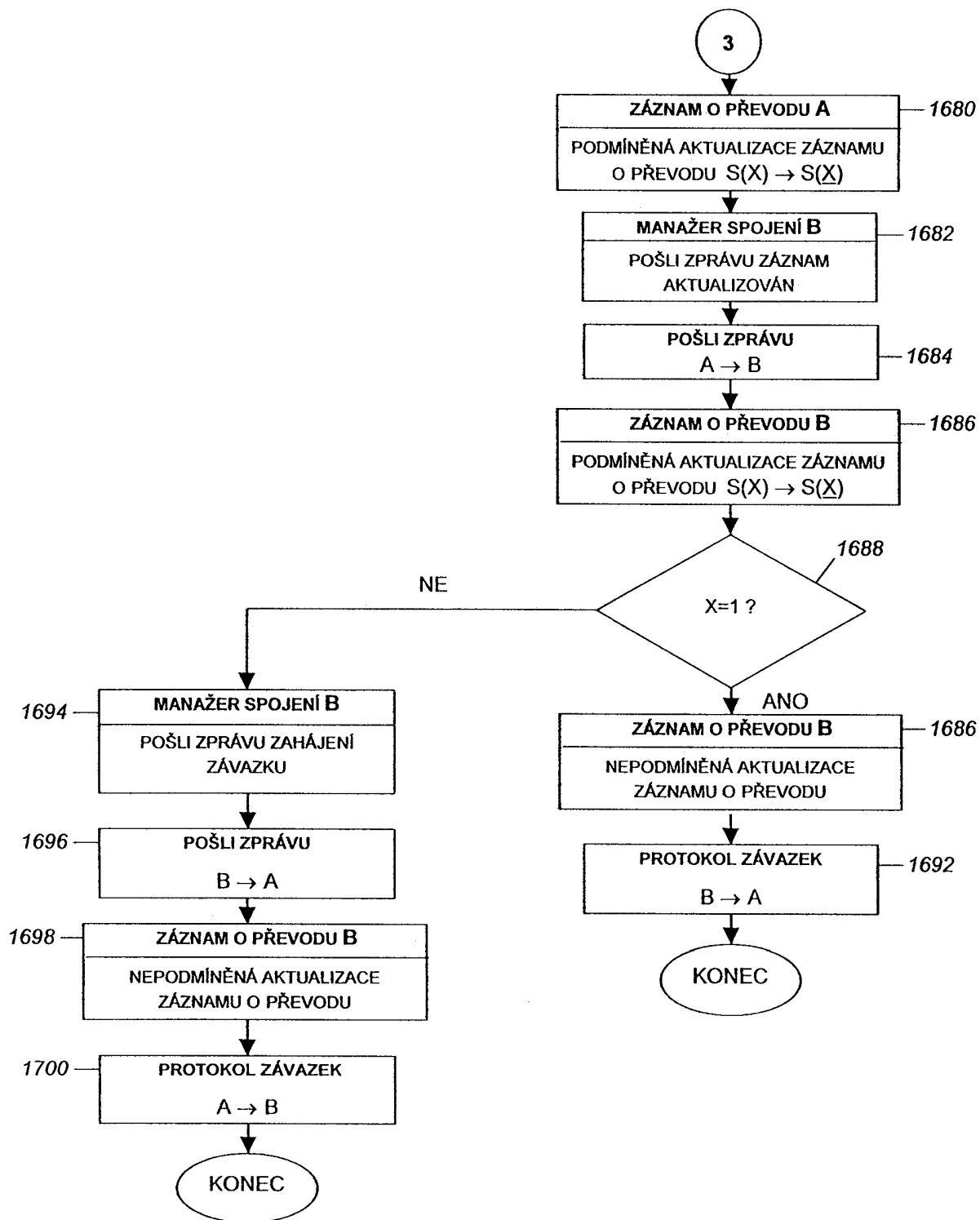
Obr. 9A



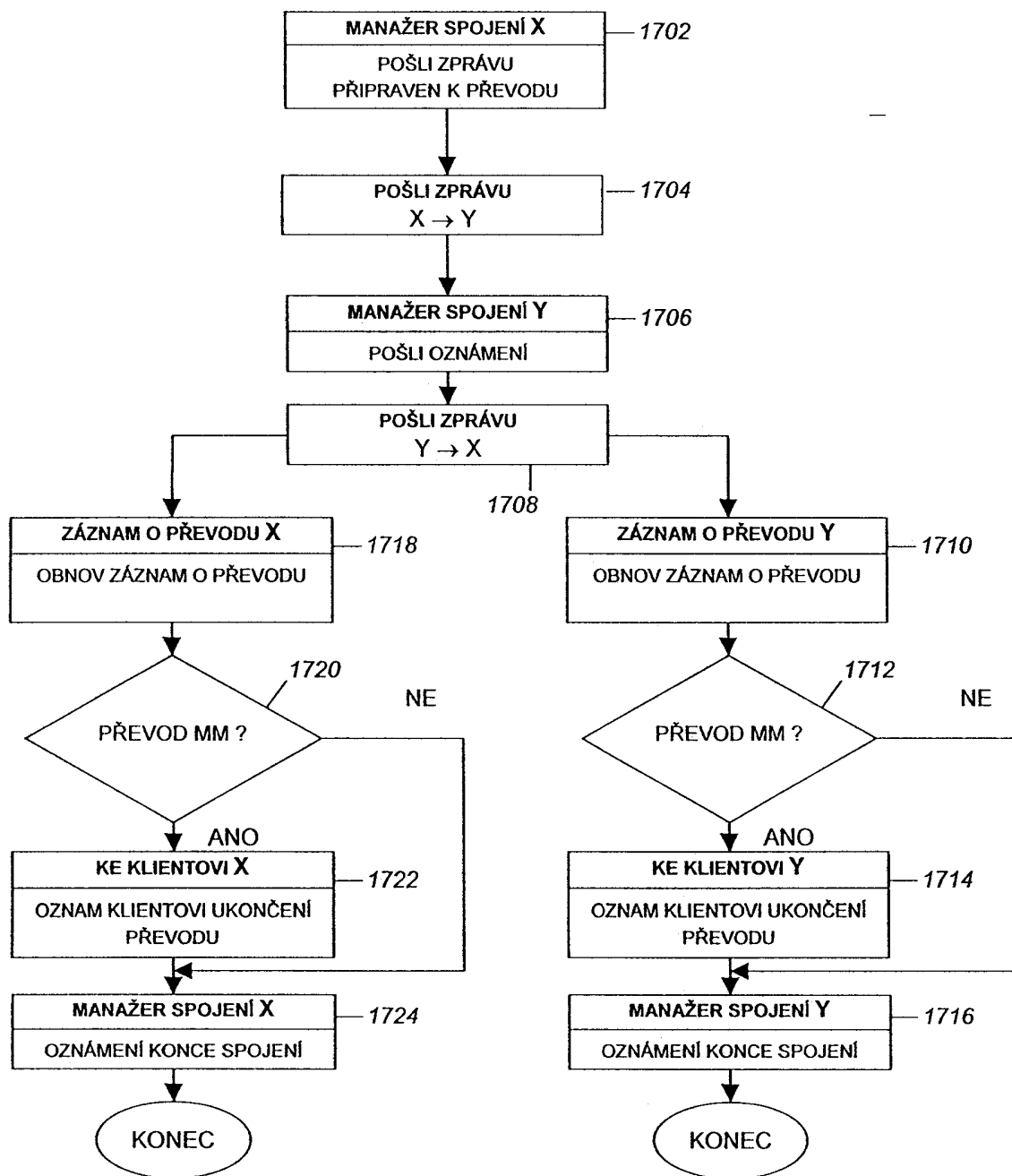
Obr. 9B



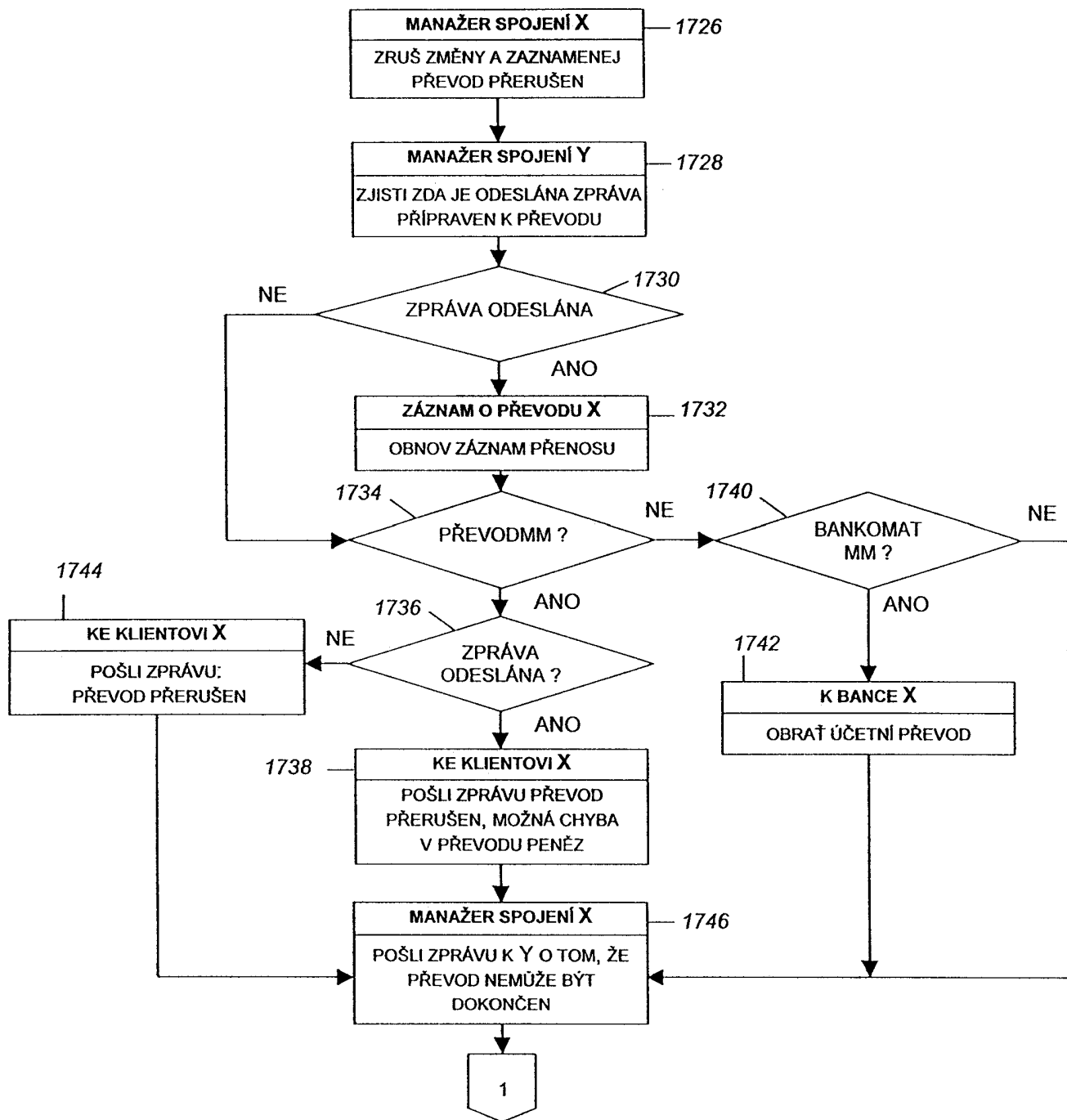
Obr. 9C



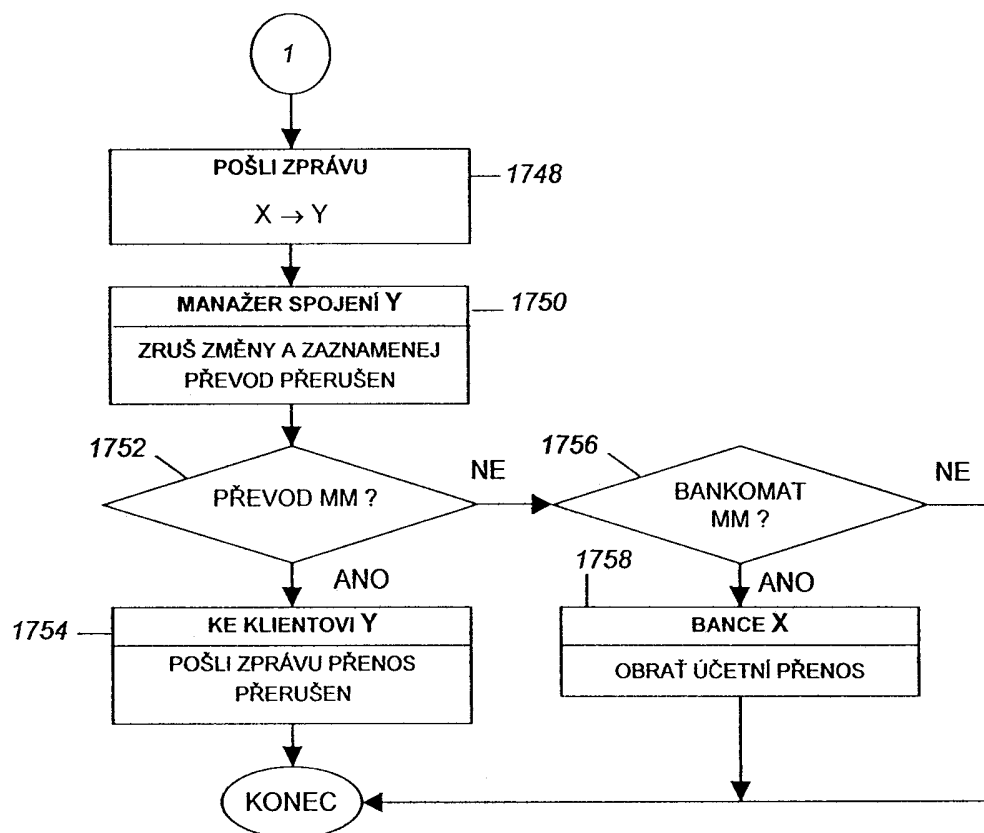
Obr. 9D



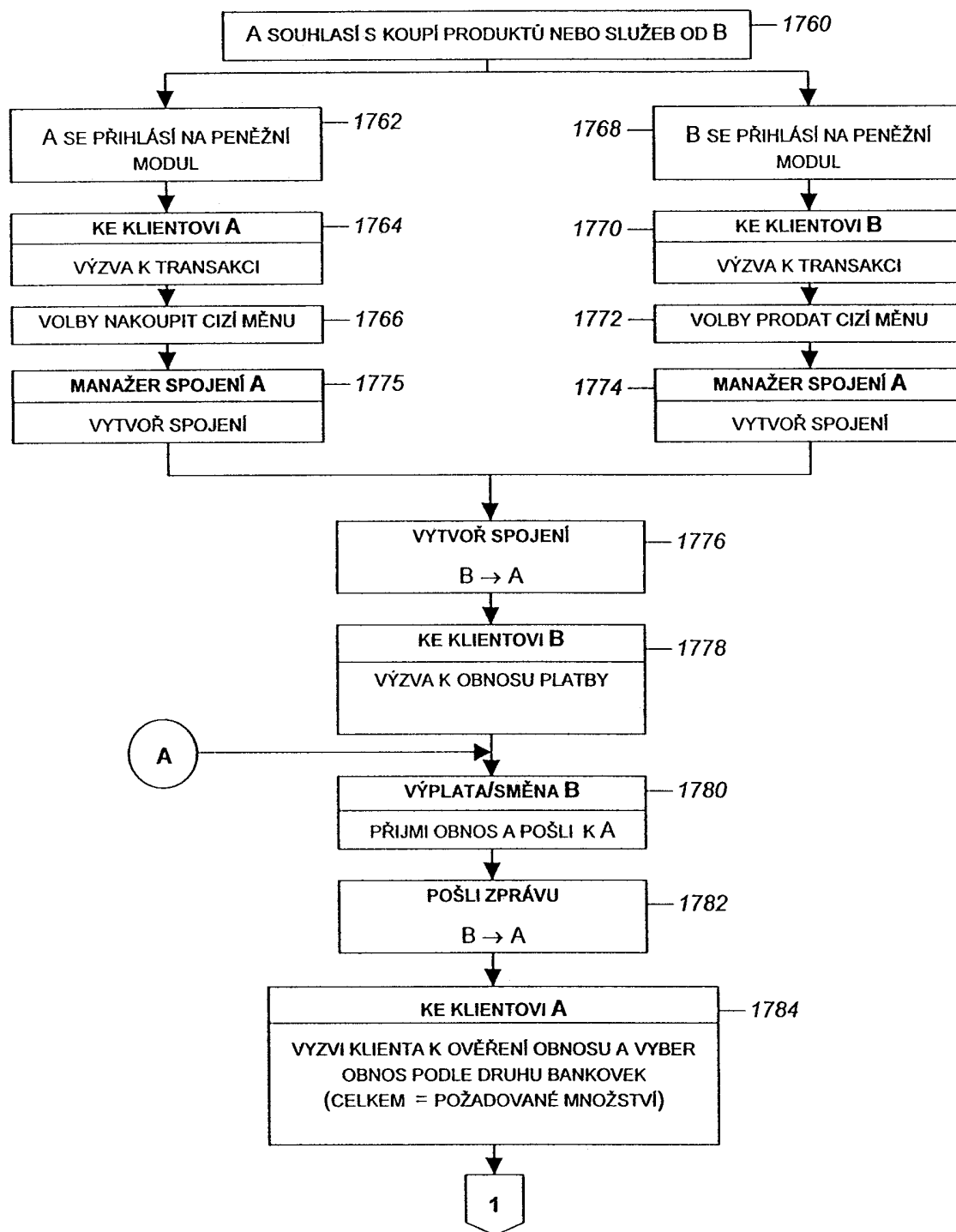
Obr. 10



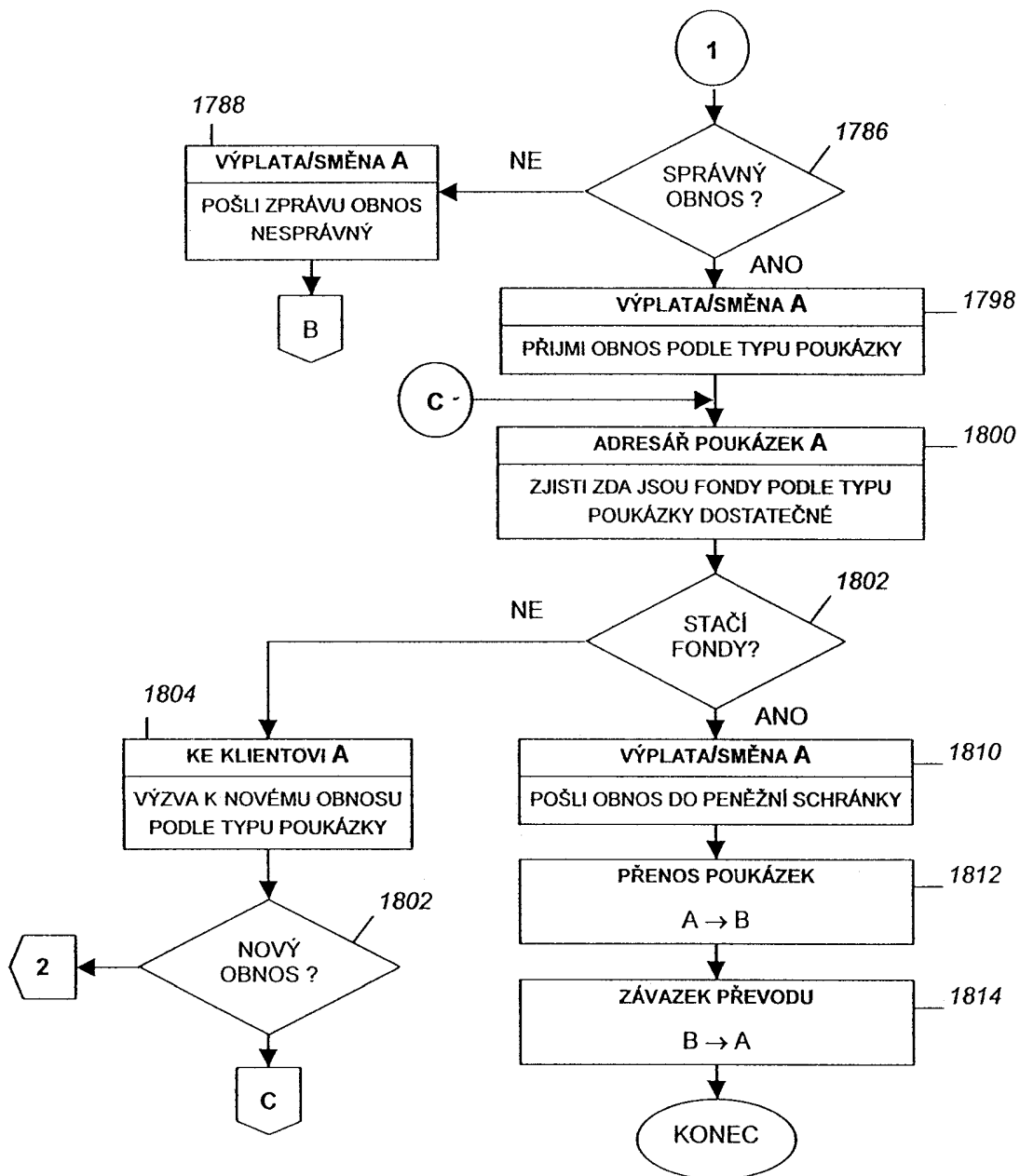
Obr. 11A



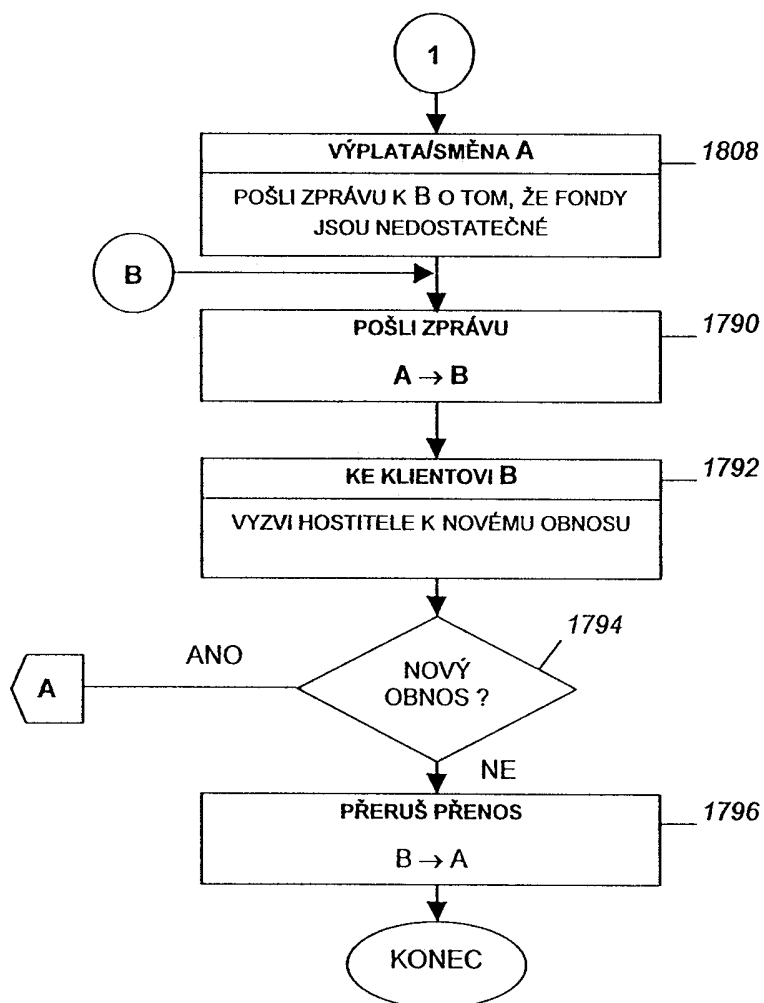
Obr. 11B



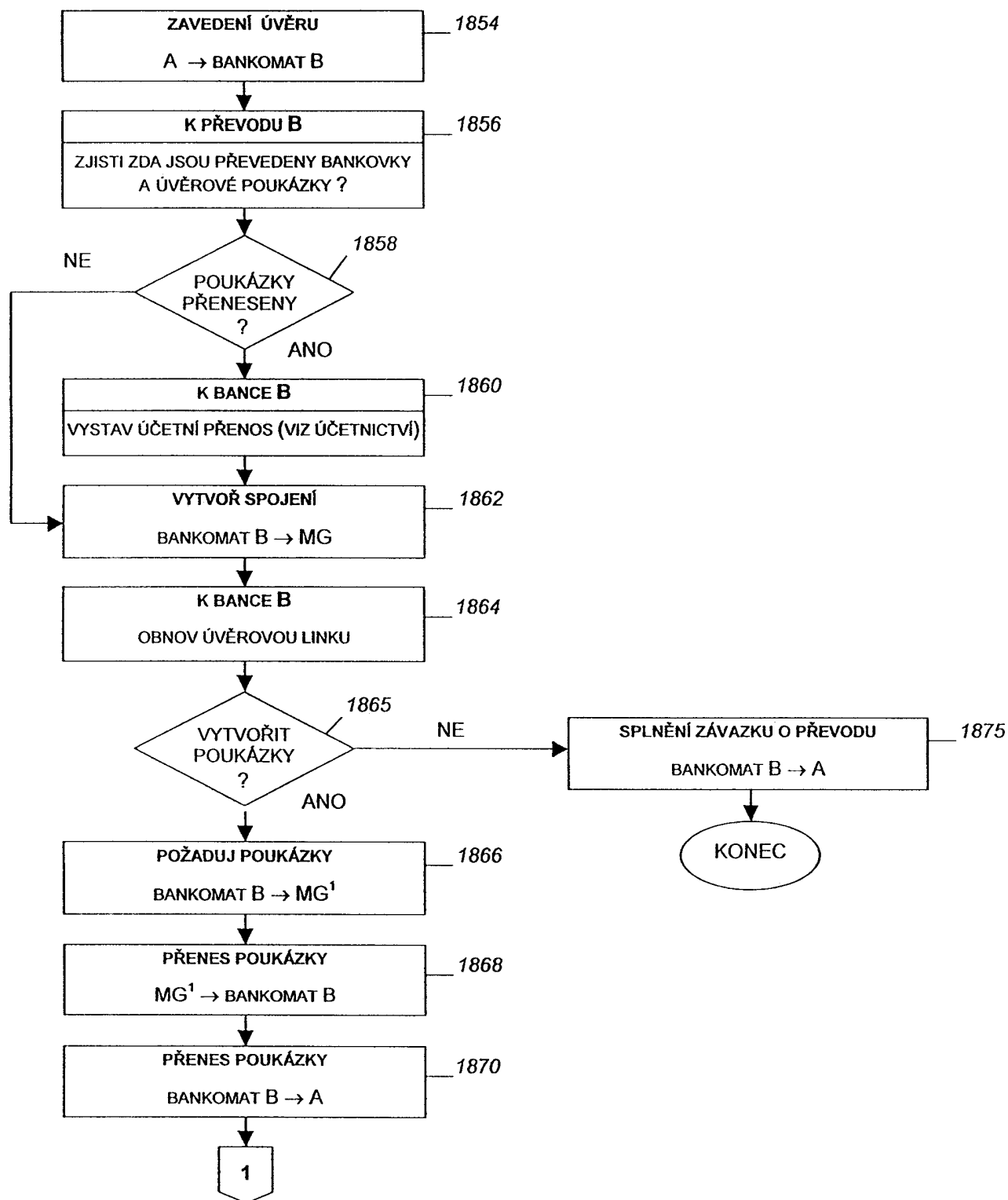
Obr. 12A



Obr. 12B

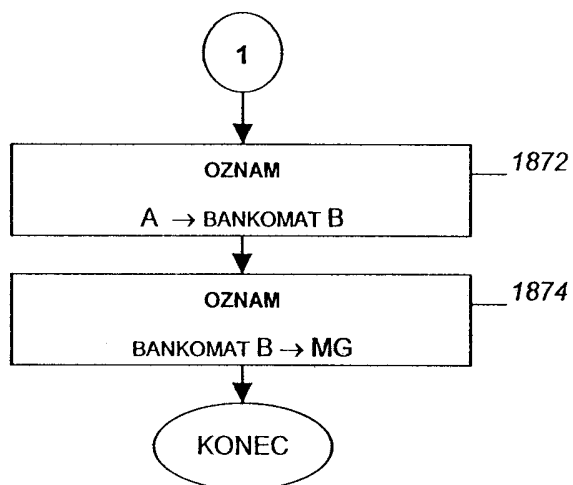


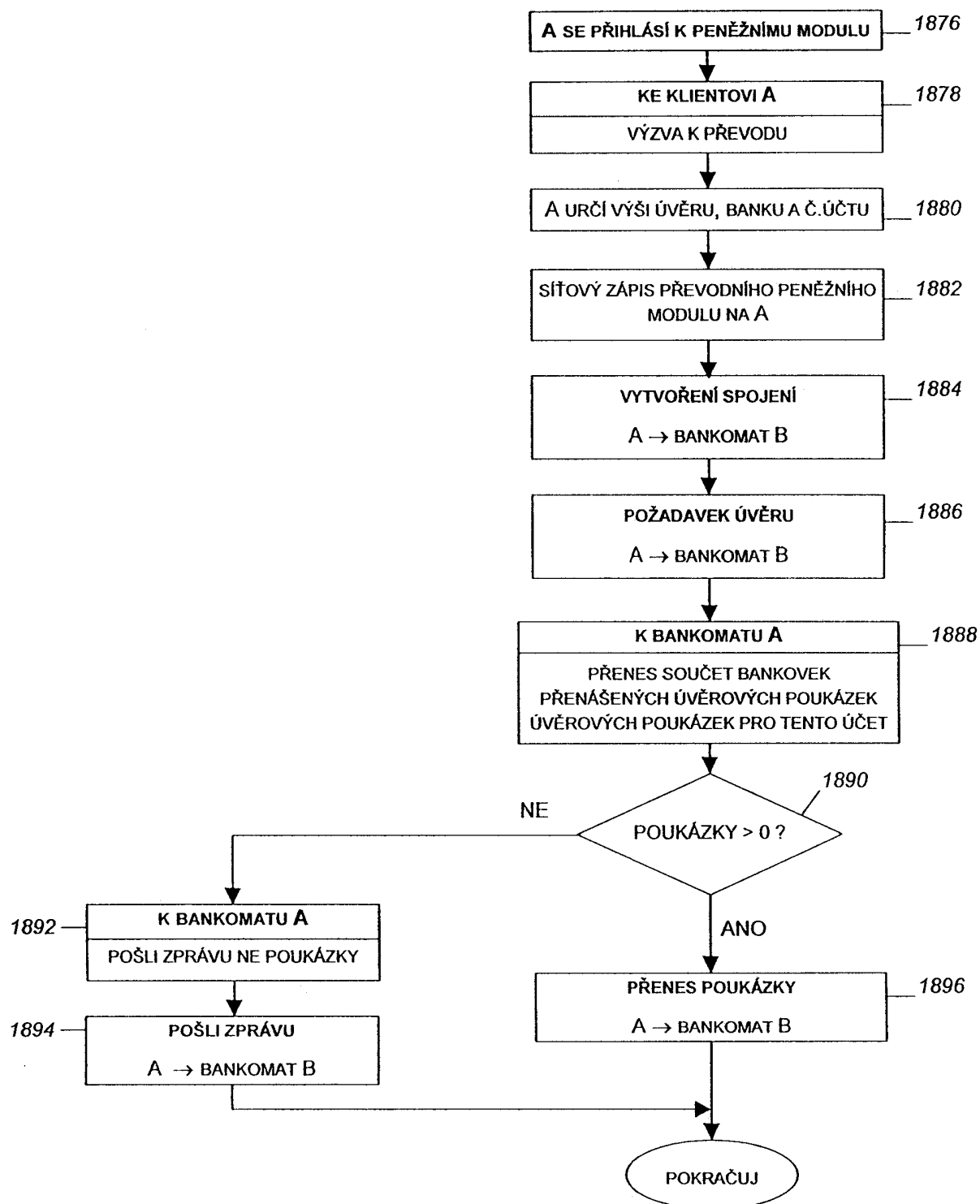
Obr. 12B



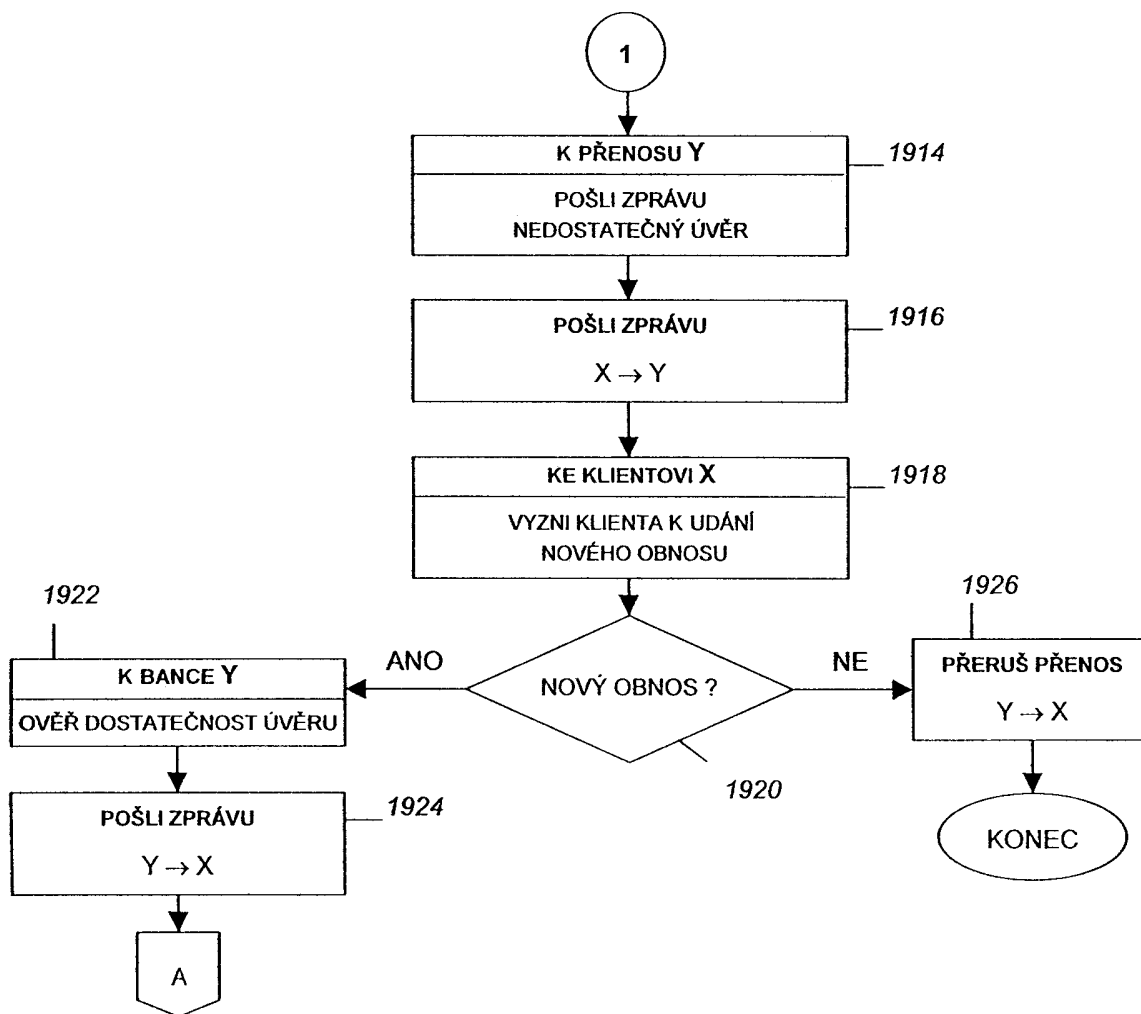
Obr. 13A

1 tato zkratka není vysvětlena (pozn.překl.)

*Obr. 13A*



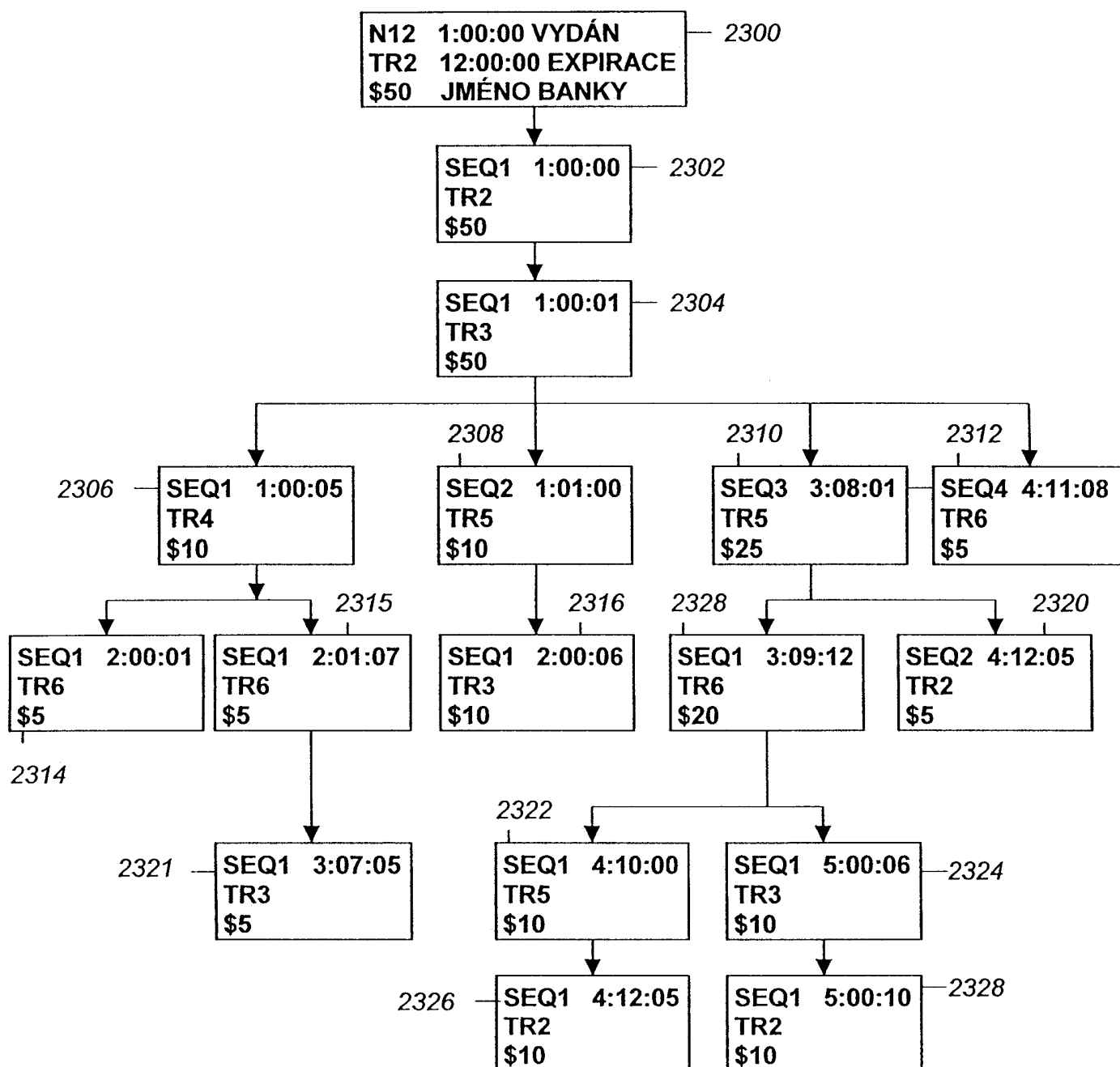
Obr. 14



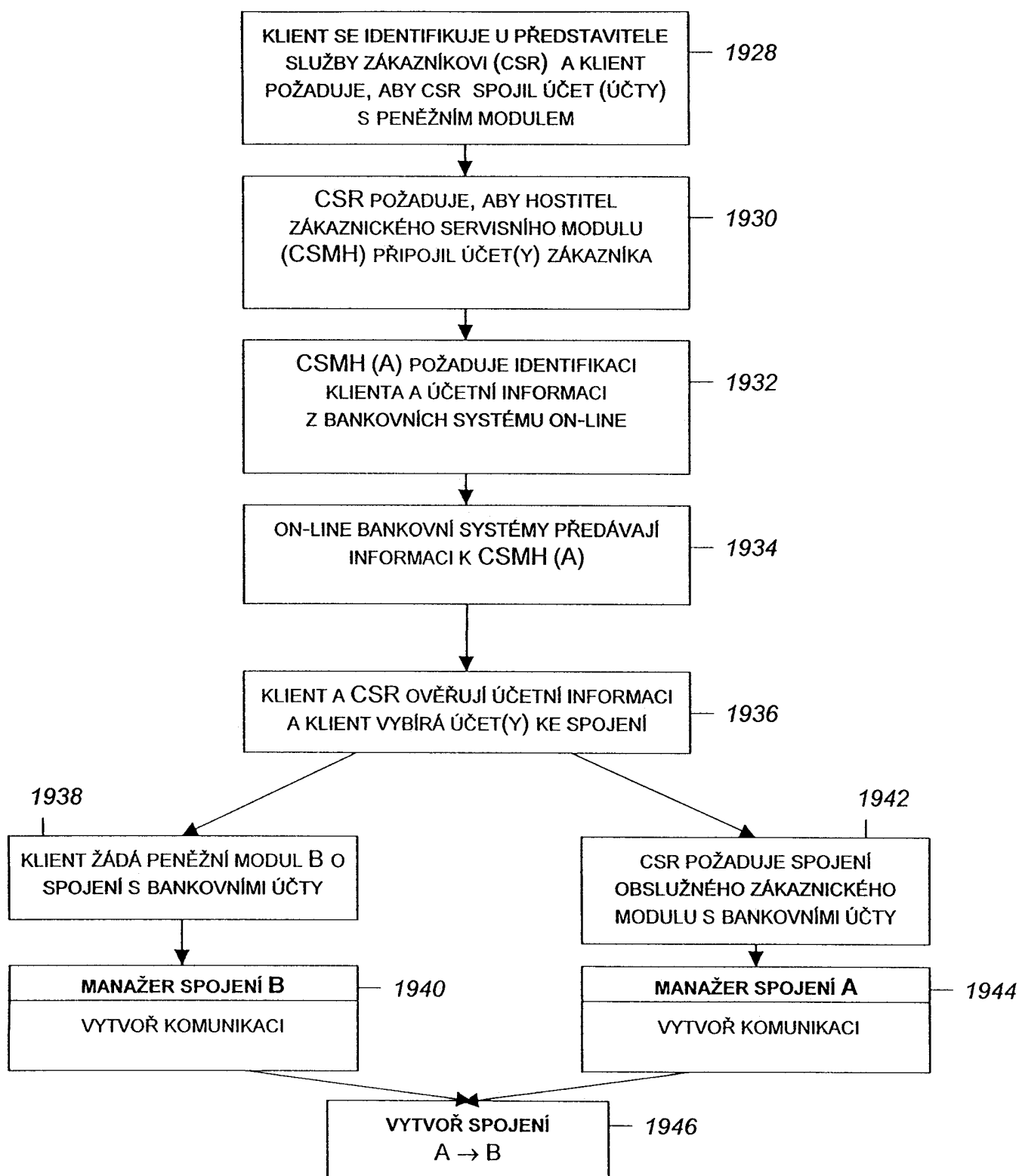
Obr. 15B

DATUM/ČAS	MG BANKOMAT						PŘENOS	
	1	2	3	4	5	6		
1:00:00	VYTVOŘ \$50							
1:00:01		VYBER \$50						
1:00:05			VYPLAŤ \$10					
1:01:00				VYPLAŤ \$10				
2:00:01					VYPLAŤ \$5			
2:00:06				VYPLAŤ \$10				
2:01:07					VYPLAŤ \$5			
3:07:05				VYPLAŤ \$5				
3:08:01				VYPLAŤ \$25				
3:09:12					VYPLAŤ \$20			
4:10:00					VYPLAŤ \$10			
4:11:08					VYPLAŤ \$5			
4:12:05				ZÁLOHA \$5				
5:00:06				VYPLAŤ \$10				
5:00:10			ZÁLOHA \$10					

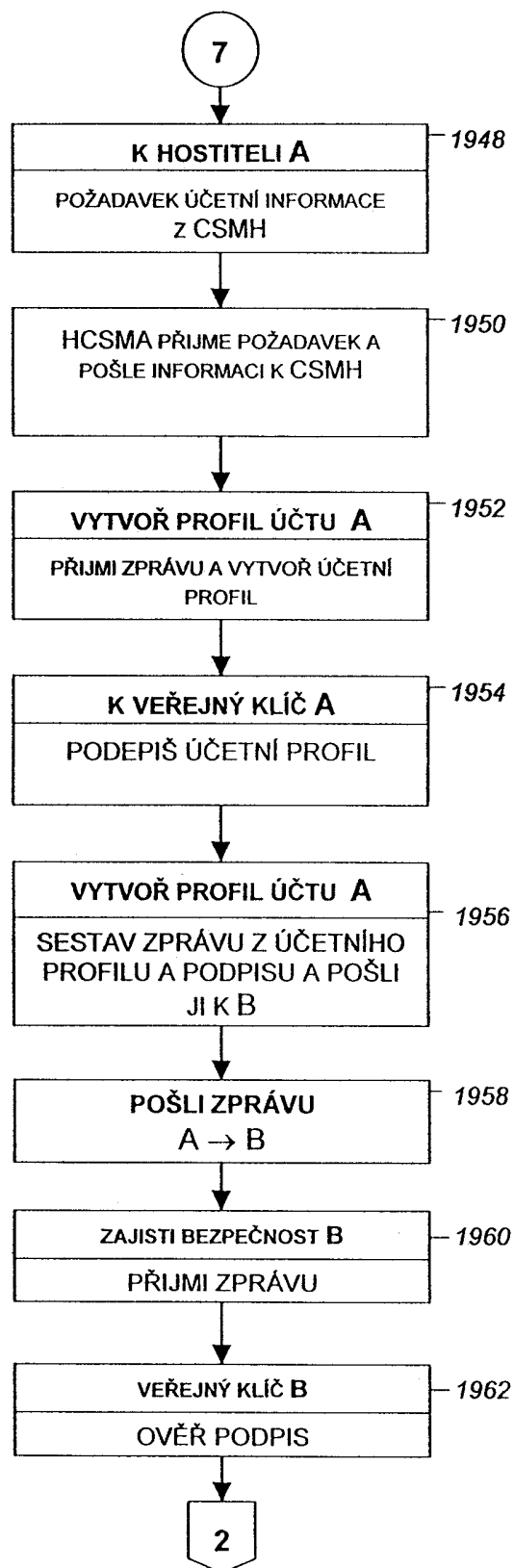
Obr. 16



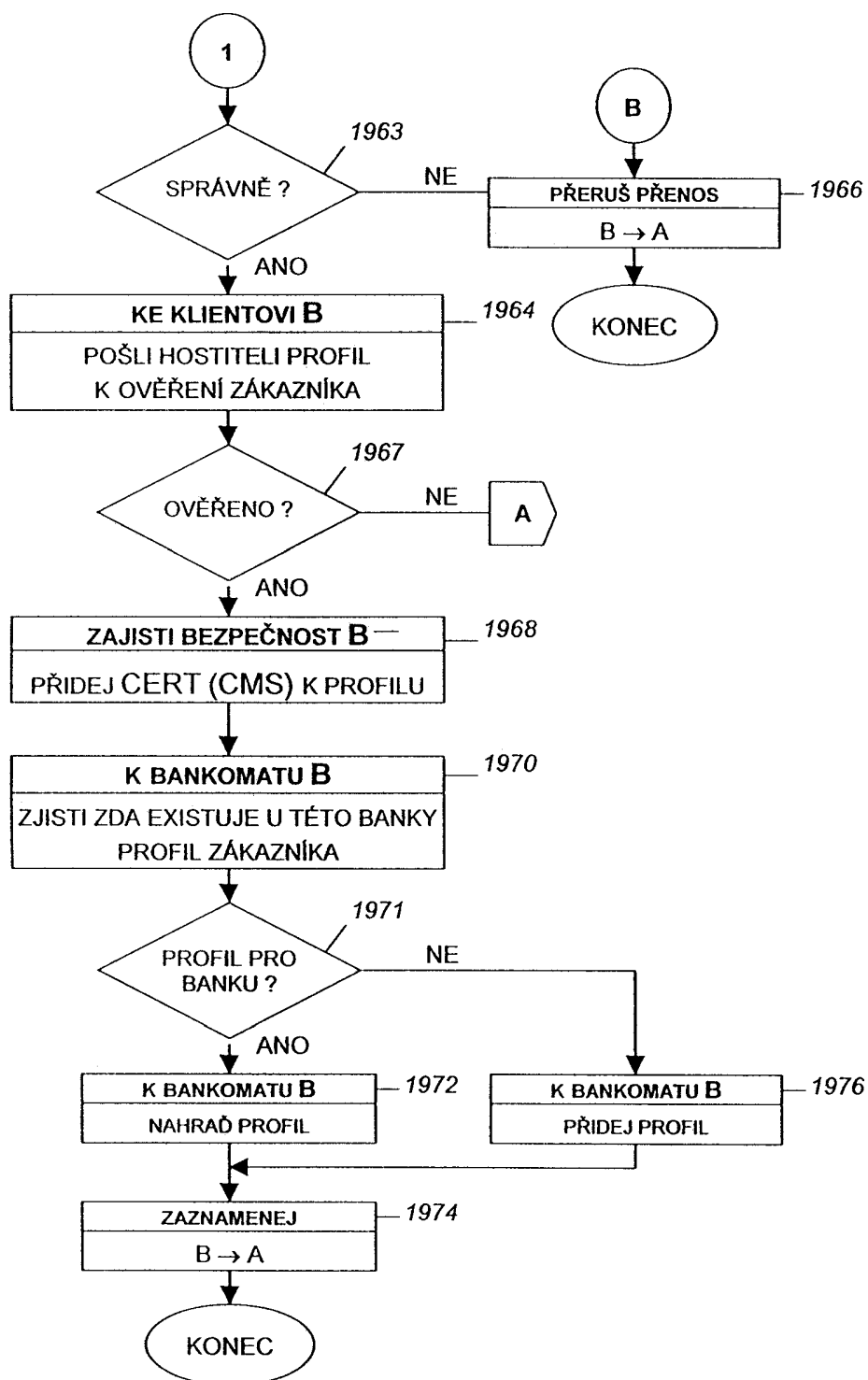
Obr. 17



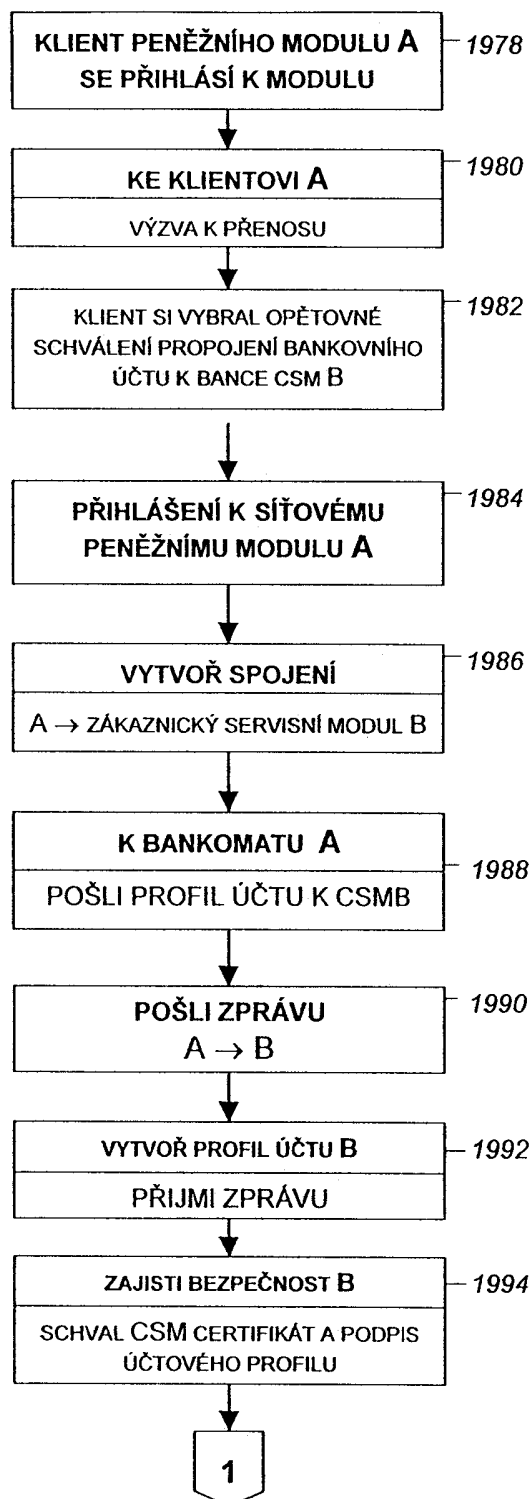
Obr. 18A



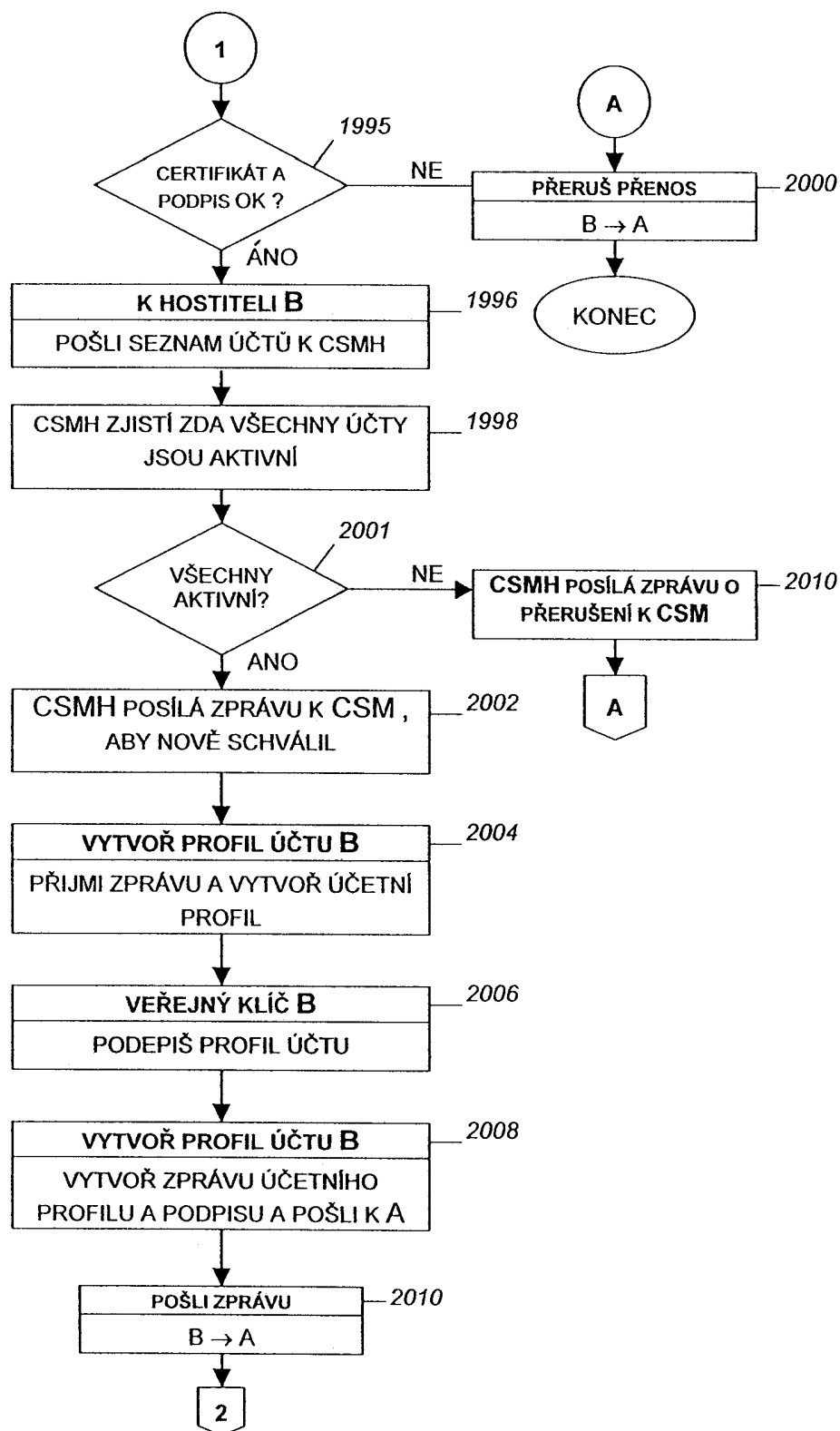
Obr.18B



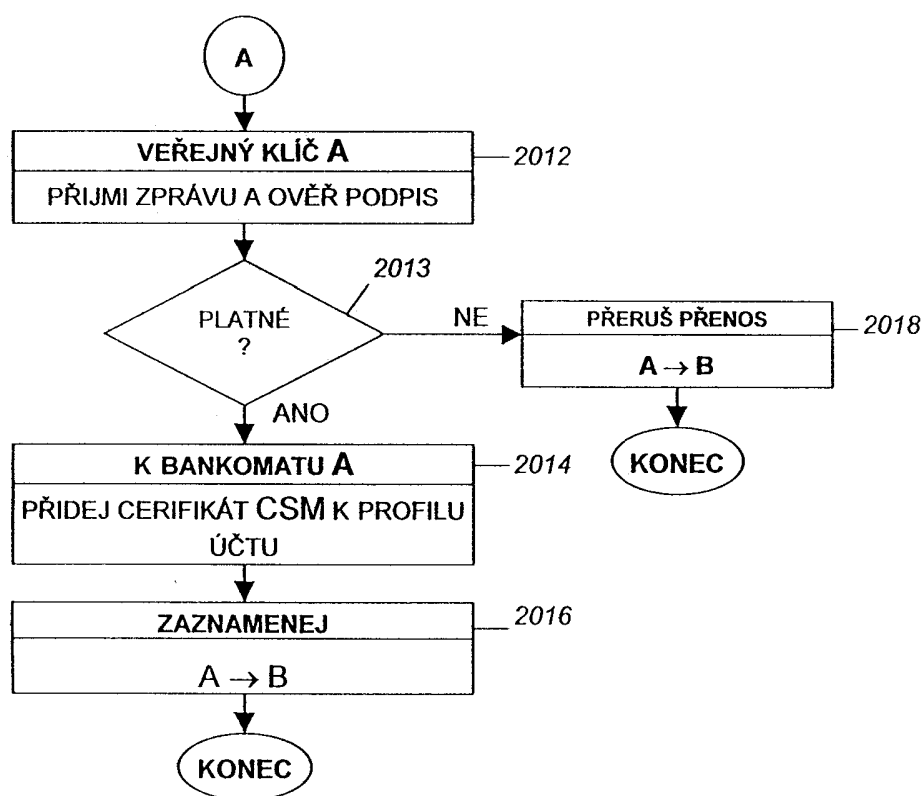
Obr. 18C



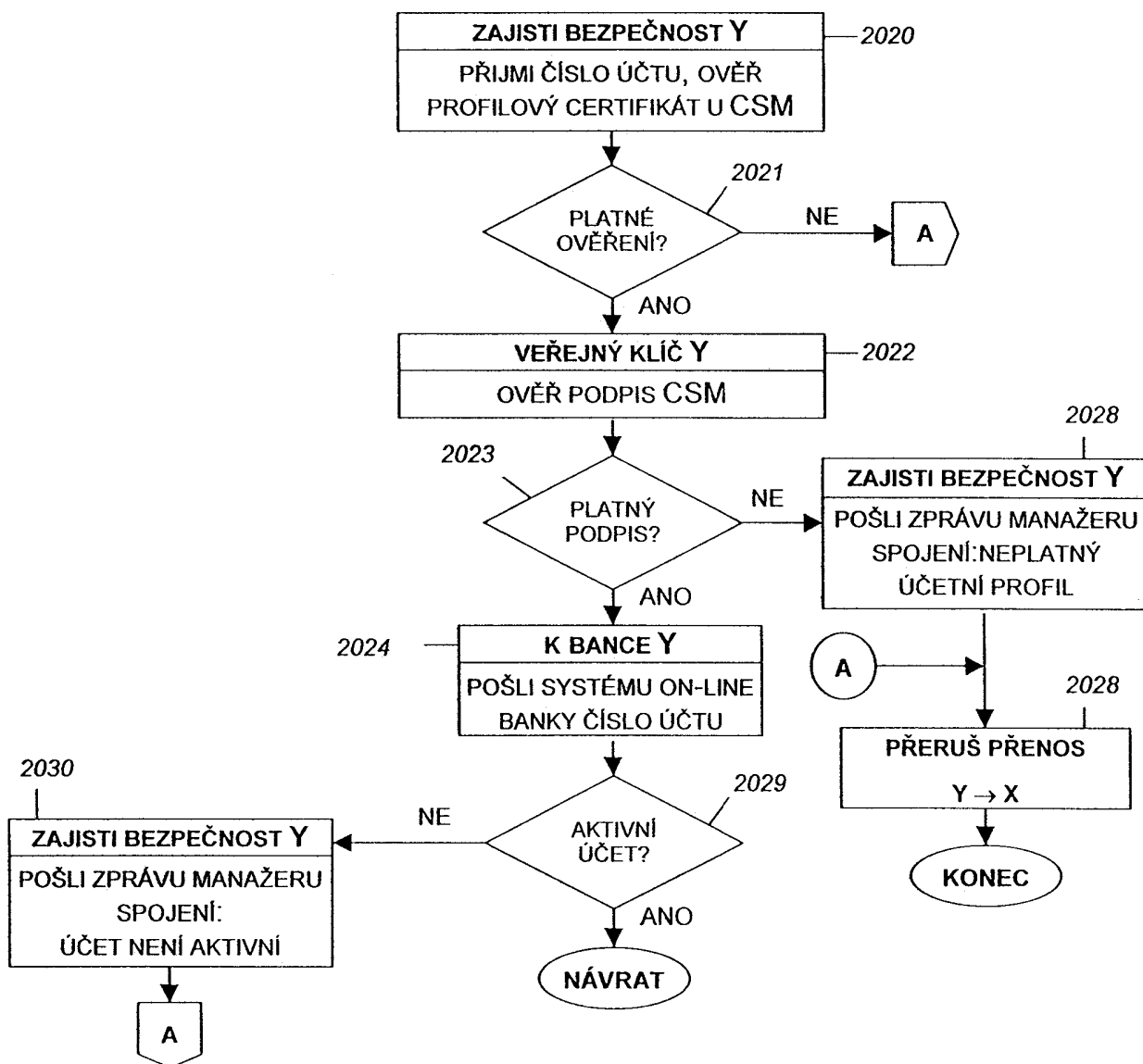
Obr. 19A



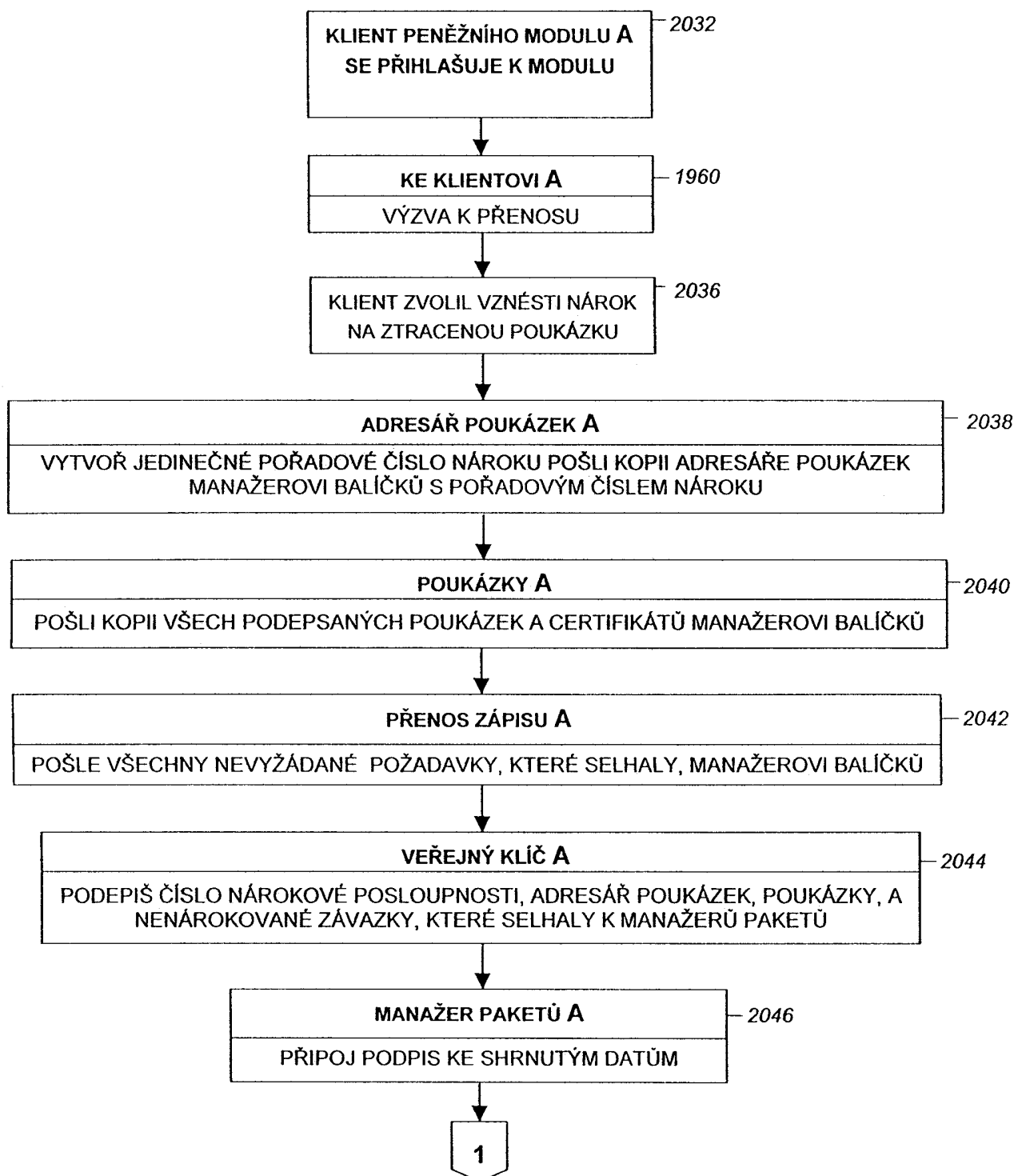
Obr. 19B



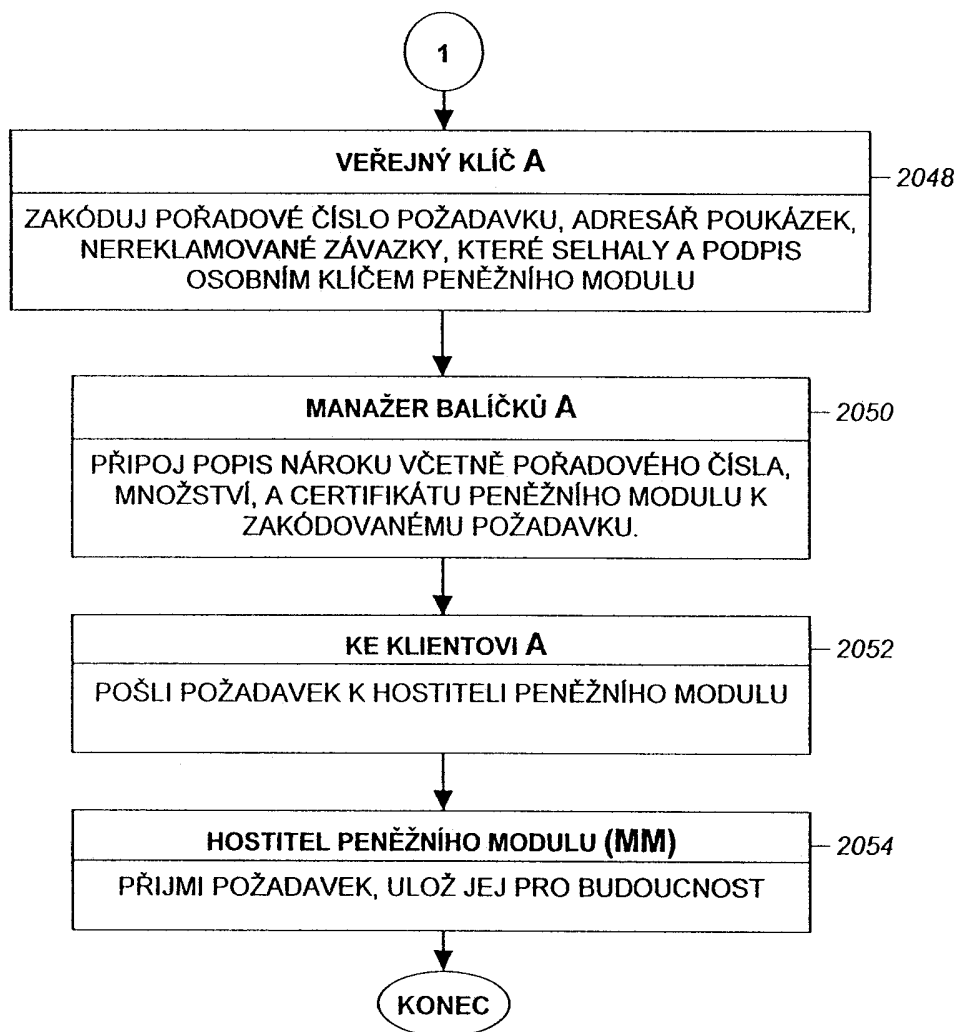
Obr. 19C



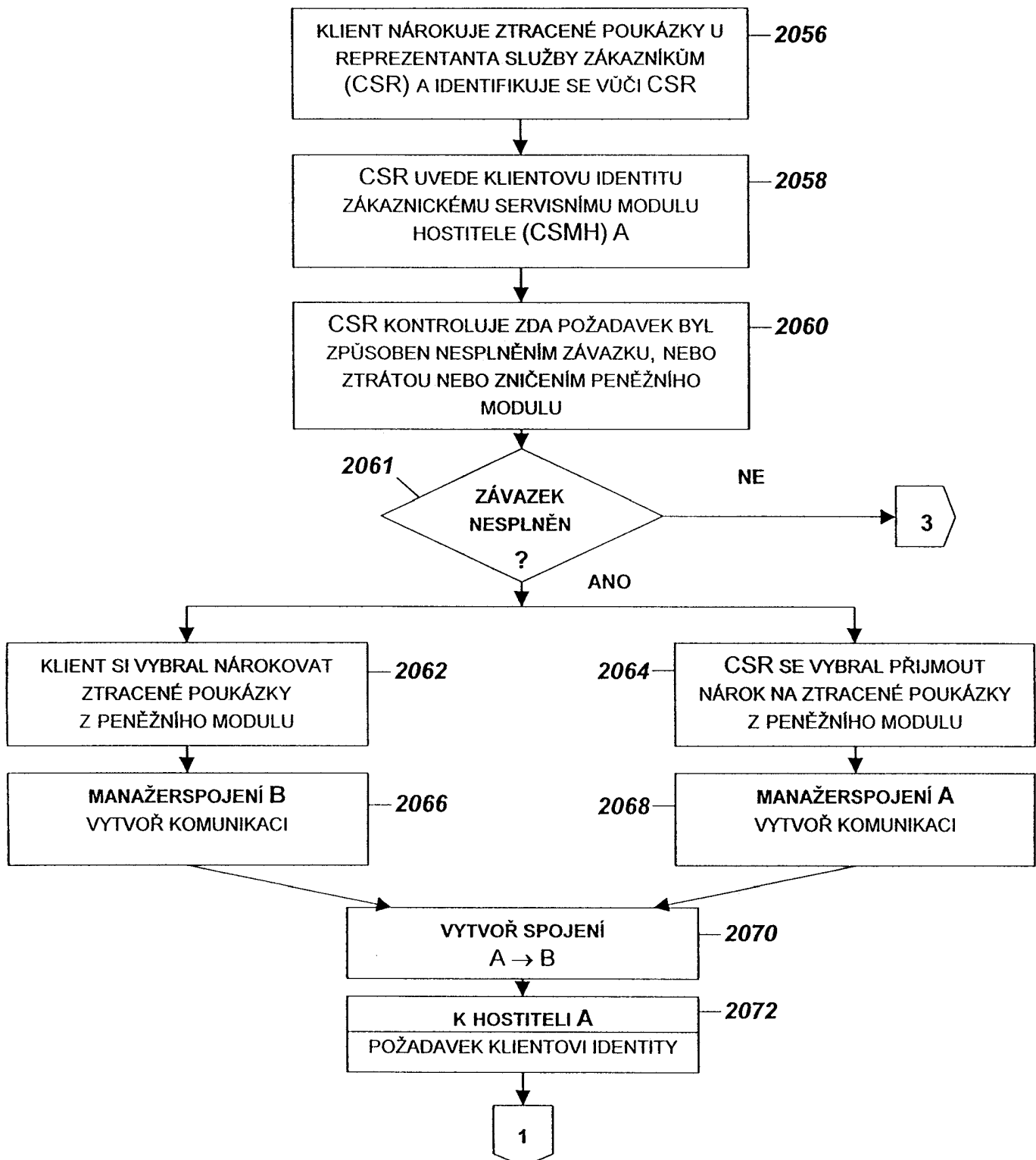
Obr. 20



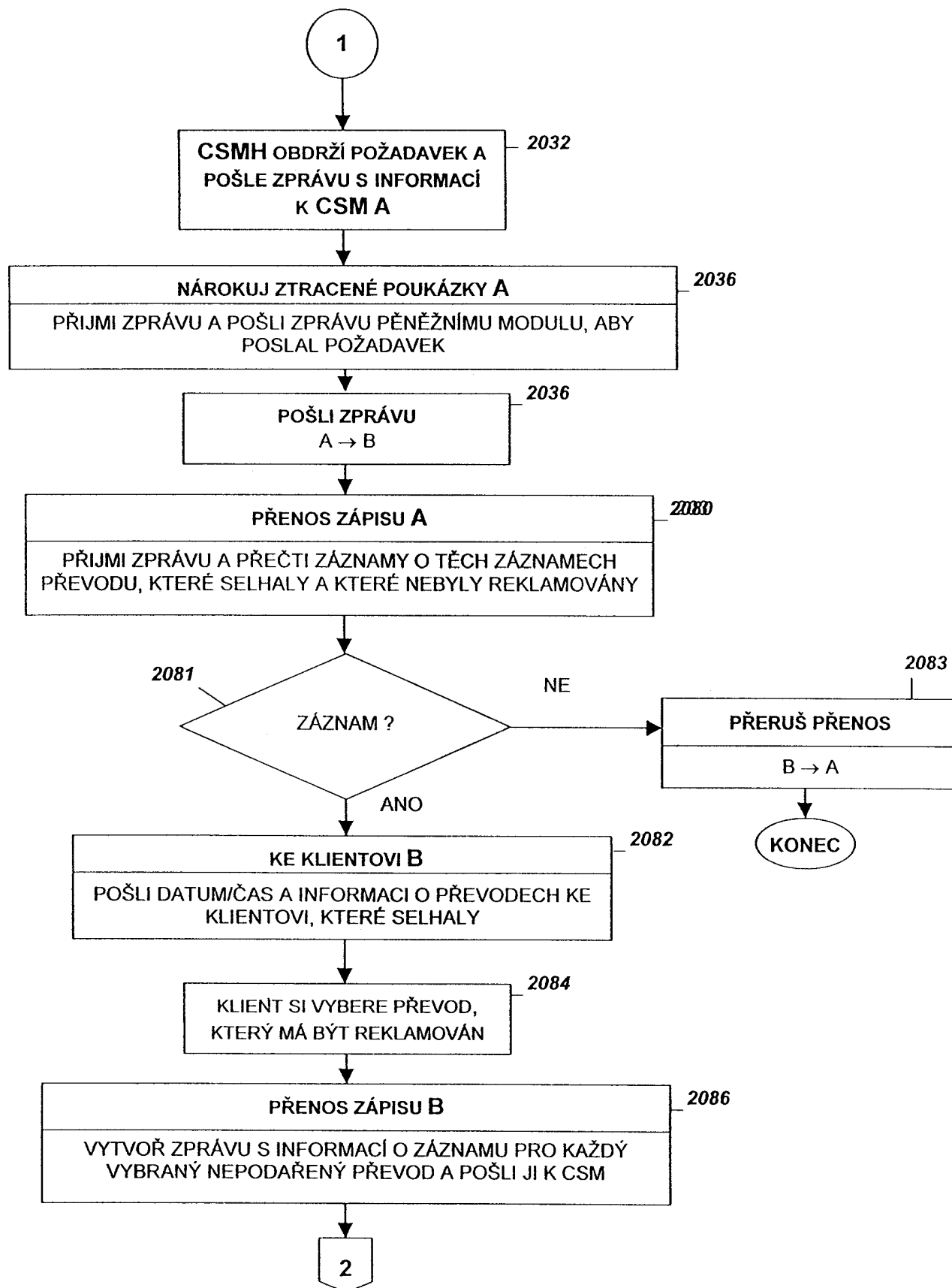
Obr.21A



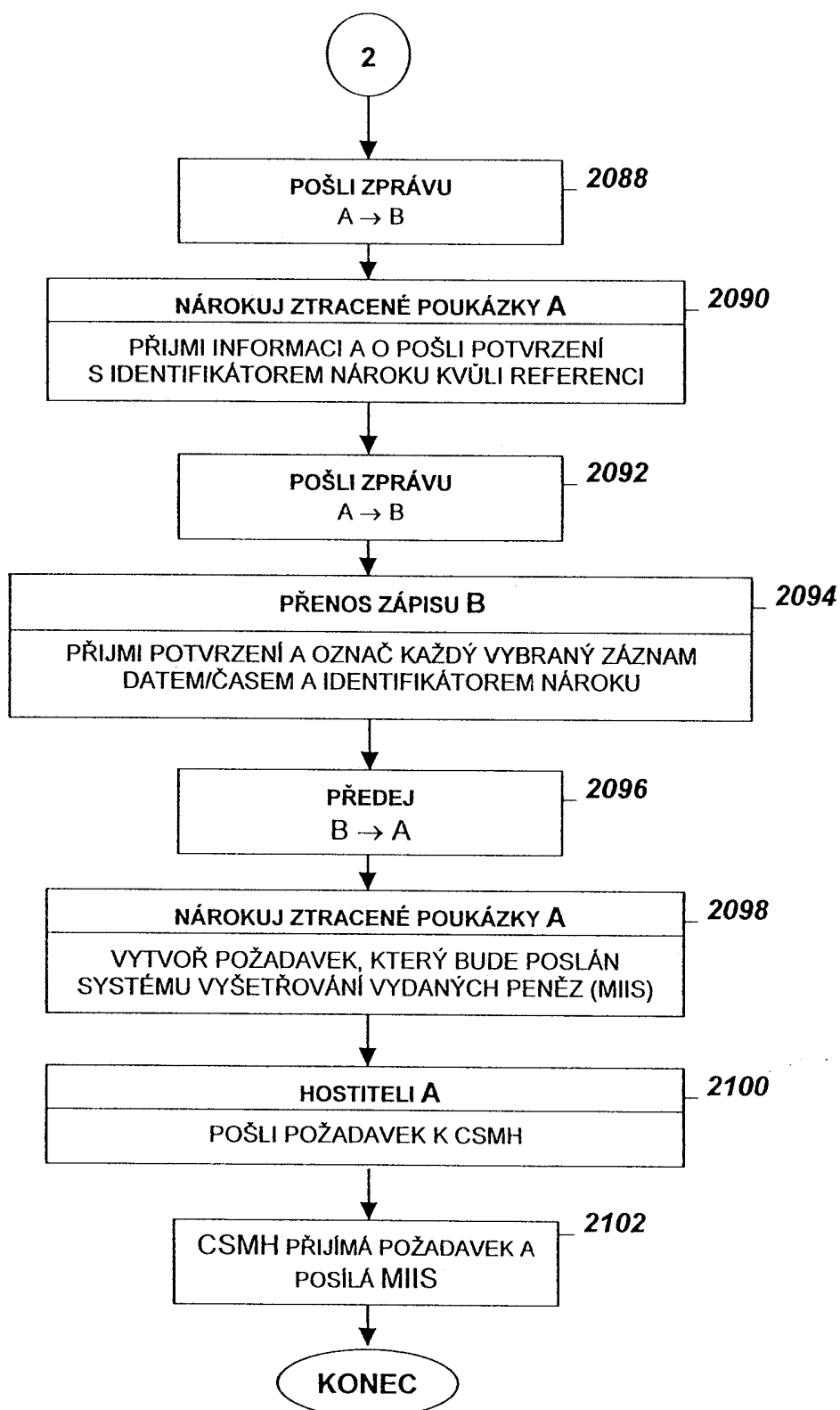
Obr.21B



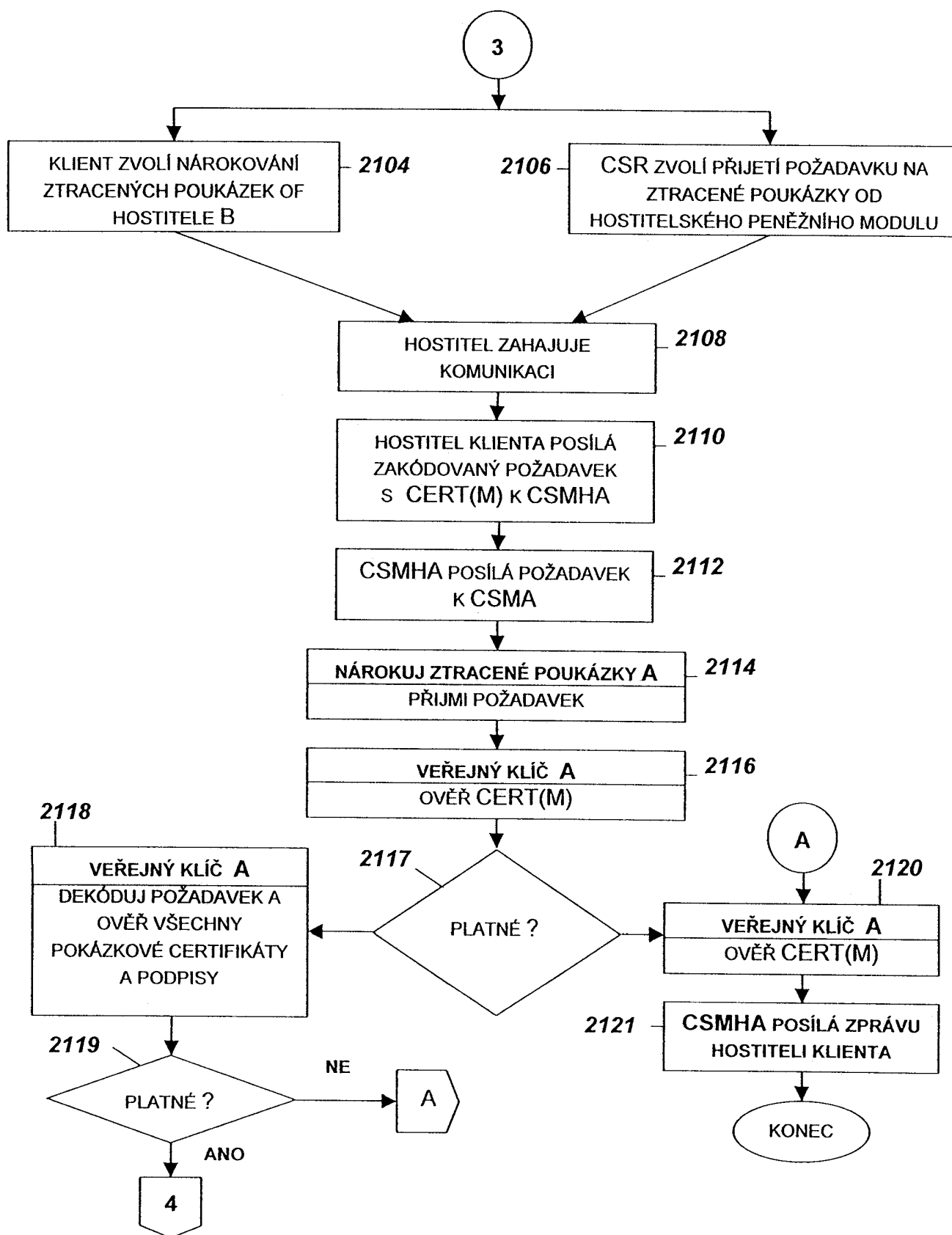
Obr. 22A



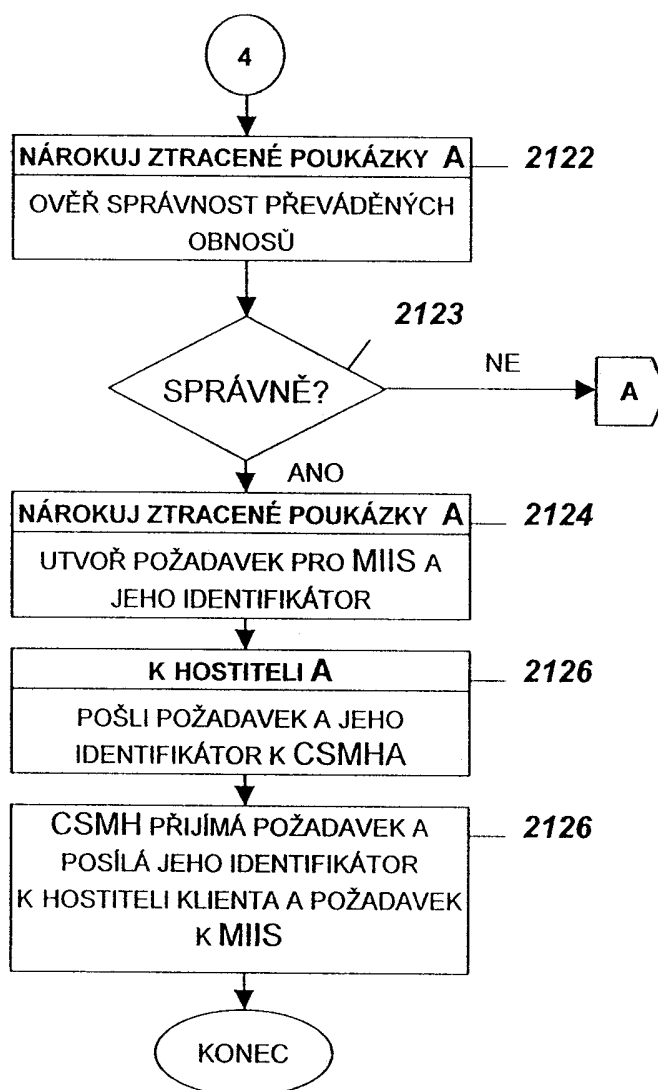
Obr.22B



Obr.22C



Obr.22D



Obr. 22E