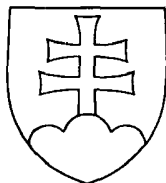


SLOVENSKÁ REPUBLIKA

(19)

SK



ÚRAD
PRIEMYSELNÉHO
VLASTNÍCTVA
SLOVENSKEJ REPUBLIKY

ZVEREJNENÁ PRIHLÁŠKA VYNÁLEZU

- (22) Dátum podania: 19.04.96
(31) Číslo prioritnej prihlášky: 08/427 287
(32) Dátum priority: 21.04.95
(33) Krajina priority: US
(40) Dátum zverejnenia: 04.11.98
(86) Číslo PCT: PCT/US96/05521, 19.04.96

(21) Číslo dokumentu:

1426-97

(13) Druh dokumentu: A3

(51) Int. Cl.⁶:

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

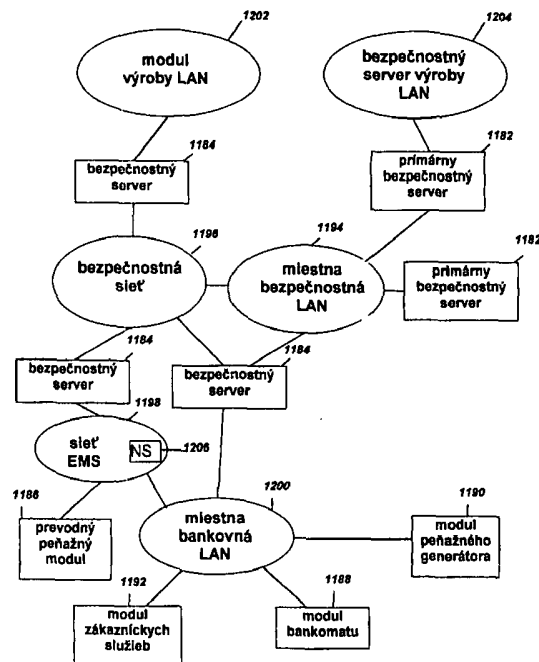
(71) Prihlasovateľ: CITIBANK, N.A., New York, NY, US;

(72) Pôvodca vynálezu: Rosen Sholom S., New York, NY, US;

(54) Názov prihlášky vynálezu: **Elektronický monetárny systém**

(57) Anotácia:

Elektronický monetárny systém (1) zahŕňajúci banku alebo finančné inštitúcie, ktoré sú spojené so zariadením na generáciu peňazí na tvorbu a vydávanie elektronických peňazí vrátane elektronickej hotovosti, ktorá je podľa požiadavky zálohovaná vkladmi a elektronickými úverovými oprávneniami, zodpovedajúce banky (2), ktoré prijímajú a distribuujú elektronické peniaze (3) radom prevodových zariadení, ktoré sú používané klientmi na ukladanie elektronických peňazí, uskutočňovanie peňažných transakcií pomocou on-line systémov zúčastnených bánk, t. j. tých, ktoré sú zapojené na centrálny počítač alebo na výmenu elektronických peňazí s inými prevodnými zariadeniami pracujúcimi off line, t. j. bez zapojenia na centrálny počítač, bankomatov (4) pridružených s vydávajúcimi a zodpovedajúcimi bankami na spracovanie a pripojenie týchto zariadení k vydávajúcim zodpovedajúcim bankám a na prepojenie samotných týchto vydávajúcich a zodpovedajúcich bánk; klíringovú banku (5) na udržanie rovnováhy medziúčtov elektronických peňazí rôznych vydávajúcich bánk; dátovú komunikačnú sieť (6) na poskytovanie komunikačných služieb všetkým zložkám systému; a bezpečnostných opatrení (7) na udržiavanie súdržnosti systému a na detekciu falšovaných a iných kriminálnych zneužití systému. Jedno uskutočnenie vynálezu obsahuje modul zákazníckych služieb, ktorý spracováva reklamácie stratených peňazí a prepojuje účty s peňažnými modulmi, aby umožnil bankový prístup.



Elektronický monetárny systém

Táto patentová prihláška je čiastočne pokračovanie súčasne podanej patentovej prihlášky US, poradového čísla 08/234,461 z 28. apríla 1994.

Oblasť techniky

Vynález sa týka elektronického monetárneho systému pre zavedenie elektronických peňažných prevodov ako alternatívneho prostredia výhodnej zmeny k získaniu peňažnej hotovosti, kontrolám, úverovým a vkladovým kartám, a elektronickému prevodu fondov.

Doterajší stav techniky

V súčasnej dobe prebehne medzi inštitúciami a samotnými osobami približne 350 miliónov prevodov v bankovkách a minciach. Extenzívne použitie mincí a bankoviek obmedzilo automatizáciu individuálnych prevodov, ako sú nákupy, cestovné, a vklady a výbery bankových účtov. Individuálne hotovostné prevody sú zťažované potrebou mať presnú čiastku alebo byť navyše vybavený drobnými. Manipulácia - spoločne s ochranou - s papierovými peniazmi a mincami je nevýhodná, nákladná a časovo náročná ako pre jednotlivca, tak pre finančné inštitúcie. Bolo odhadnuté, že v samotných Spojených štátoch sa utratí okolo 60 miliárd US dolárov len za pohyb peňazí. Okrem toho, bezpečnosť papierových peňazí je vážne ohrozená relatívne jednoduchým falšovateľským použitím napríklad ľahko dostupných vysoko kvalitných farebných kopírovacích strojov.

Aj keď šeky môžu byť napísané pre akúkoľvek špecifickú čiastku až do čiastky dostupnej na účte, šeky majú veľmi obmedzenú prevoditeľnosť a musia byť dodávané z fyzickej

zásoby. Kontrolne systémy založené na papierových dokumentoch majú podobné obmedzenia a ťažkosti ako prevod hotovosti a pridávajú k nim oneskorenie spôsobené spracovaním šekov. K tomu došla ekonomická zmena náročnou cestou hľadania väčšieho pohodlia a nižších nákladov, zatiaľ čo sa tiaľ pokúšala o zlepšenie bezpečnosti.

Automatizácia dosiahla niektoré z týchto kvalít pre veľké prevody pomocou elektronických prevodov fondov (electronic funds transfer, ďalej EFT). Prevod elektronických fondov je v podstate postup zmeny hodnôt dosiahnutý pomocou prevodov centrálného počítačového bankového systému. Služby EFT predstavujú prevod platieb, ktorý využíva elektronické "šeky", používané predovšetkým vo veľkých obchodných organizáciách.

Systémy automatizovanej clearingovej banky (Automated Clearing House, ďalej ACH) a miesta predaja (point of sale, ďalej POS) sú príkladmi prevodných systémov elektronických fondov, ktoré v posledných rokoch začali byť používané v maloobchodných a komerčných organizáciách vo významnej mierke. Platby uskutočnené týmito typmi EFT systémov sú limitované tým, že nemôžu byť uskutočňované bez bankového systému. Ďalej, prevody ACH obvykle nemôžu byť uskutočňované mimo pracovnú dobu.

Domáce služby šekových platieb známe ako "Home Banking" sú príkladmi prevodného systému elektronických fondov používaných jednotlivcami k uskutočneniu platieb. V súčasnej dobe domáce bankové iniciatívy majú málo zákazníkov. V bankách, ktoré ponúkli možnosti platieb, účtových prevodov a informácií pomocou telefónnej linky použitím osobného počítača, používa tieto služby menej ako jedno percento bankových zákazníkov. Jedným z dôvodov, prečo sa "Home Bankig" nestal úspešným produktom je to, že zákazník nemôže v tomto systéme uložiť a vybrať peniaze, ako potrebuje.

Súčasný EFT systémy, úverové karty či vkladové karty,

ktoré sú používané s on-line systémom k prevodu peňazí medzi účtami, ako napr. medzi účtami obchodníka a zákazníka, nemôžu uspokojiť potrebu po automatizovanom prevodnom systéme, ktorý poskytuje prevod univerzálne akceptovanej ekonomickej hodnoty mimo bankový systém. Ďalej, úverové a debetné kartové systémy sú obecné nedostatočne zaistené proti zneužitiu a neposkytujú zodpovedajúce súkromie.

Pri zavádzaní automatického a ešte vhodnejšieho prevodného systému, ktorý nevyžaduje sprostredkovanie pomocou bankového systému, a ktorý môže rozdeľovať určitú formu finančných prostriedkov, bol jasný trend smerujúci k elektronickým peňažným prevodom typu "off-line". Napríklad pre určitú formu "elektronických peňazí" boli navrhnuté mnohé riešenia, ktoré môžu byť použité pri bezhotovostných platobných prevodoch ako náhrada za tradičný hotovostný a šekový spôsob platby. Vid' patentová prihláška US č.4977,595, s názvom "Spôsob a zariadenie pre realizáciu elektronickej hotovosti", a patentová prihláška US č. 4,305,059, s názvom "Modulárny systém prevodu fondov".

Známejšie techniky používajú karty s magnetickým záznamom zakúpené za daný suma, z ktorých môže byť predplatená hodnota odberaná pre špecifické účely. Po vyčerpaní ich hodnoty sa karty zahodia. Iné príklady zahrňujú pamäťové karty alebo tzv. múdre karty, ktoré sú schopné opakovane uschovať informáciu predstavujúcu hodnotu, ktorá je podobne odčerpávaná pre špecifické účely.

Tieto navrhnuté systémy však zlyhávajú pri stanovovaní významu bankových depozít ako peňazí, a ich nutnosti zálohovať akúkoľvek formu obecné akceptovaných monetárnych reprezentácií, ktoré môžu byť vydávané. V týchto systémoch je reprezentácia ekonomickej hodnoty, či už je elektronická alebo papierová, vydávaná bez podpory primerane hodnotných ručení ako náprotivku k ich aktívam.

Žiadny z týchto navrhnutých platobných systémov bez

papierov nie je tak mocný, aby bolo možné zaviesť viacúčelový elektronický monetárny systém, ktorý obsahuje ako automatické zariadenia, ktoré umožňujú klientom predvádzať elektronické fondy alebo peniaze medzi nimi bez akéhokoľvek sprostredkovávajúceho systému, tak tiež úplný bankový systém pre generovanie hodnoty reprezentovanej elektronickými peniazmi a pre clearing a potvrdenie stavu účtov elektronických peňazí bank a finančných inštitúcií zaistujúcich monetárnu rovnováhu systému.

Teda, je potrebné zaviesť systém, ktorý dovoľuje bežnej ekonomickej zmeny platcu príjemcu uskutočňovať bez sprostredkovania bankovým systémom, a ktorý odovzdáva kontrolu platobného postupu jednotlivcovi. Ďalej je potrebný systém elektronickej zmeny, ktorý môže byť použitý veľkými organizáciami pre komerčné platby ľubovoľnej veľkosti, ktorý nie je obmedzený ako súčasný systém EFT.

V bežne uvádzanej patentovej prihláške USA č. 07/794,112, z 15. novembra 1991, na ktorú sa odkazujeme, je popísaný elektronický monetárny systém (EMS), ktorý prekonáva vyššie popísané a iné prvé obmedzenie, a poskytuje kompletný elektronický monetárny systém, ktorý využíva elektronické peniaze, zmeniteľné s tradičnou hotovosťou a univerzálne akceptované. Vynájdený EMS poskytuje spôsob a systém pre bezpečné a spoľahlivé prevody ekonomickej hodnoty vrátane hotovosti a úverov medzi odberateľmi medzi finančnými inštitúciami a alebo medzi odberateľmi a finančnými inštitúciami. EMS umožňuje tiež použitie elektronických peňazí vo forme niekoľko mien. Nič menej veľká dôležitosť bezpečnosti a spoľahlivosti vyvoláva potrebu ďalšieho zlepšovania EMS.

Teda, predmetom súčasného vynálezu je zlepšený EMS systém a príbuzné spôsoby ekonomickej zmeny, ktoré sú odolné proti zneužitiu, duplikovaniu a falšovaniu.

Ďalším predmetom vynálezu je systém, ktorý umožňuje

reklamovať stratené peniaze.

A ďalej je predmetom vynálezu monetárny systém, ktorý je pre klienta optimálny a ktorý je možné spoľahlivo a bezpečne použiť pre prevody peňazí od kupujúceho k predávajúcemu v reálnom čase.

Vyššie zmienené vlastnosti a výhody vynálezu sú príkladmi toho, čo môže byť dosiahnuté pomocou tohto vynálezu a nie sú vyčerpávajúcim ani obmedzujúcim výčtom výhod, ktoré môžu byť dosiahnuté. Teda tieto majú iné ciele a výhody súčasného vynálezu budú zrejmé z popisu alebo môžu byť získané používaním vynálezu, obidvoje, ako je tu popísané alebo ako je modifikované vo všetkých variáciách, ktoré môžu byť zrejmé odborníkom. Podľa toho spočíva tento vynález v nových metódach, usporiadaných, kombináciách a vylepšeniach tu ukázaných a popísaných.

Podstata vynálezu

K dosiahnutiu vyššie zmienených vlastností a ďalších výhod používajú sa v spôsobe a zariadení podľa tohto vynálezu s výhodou uskutočnenia vo forme elektronického monetárneho systému, ktorý obsahuje: (1) banky alebo finančné inštitúcie, ktoré sú spojené so zariadením generujúcim peniaze, ktoré vytvára a vydáva zavedeným klientom elektronické peniaze, vrátane elektronickej hotovosti zálohovanou, ktoré sú podľa požiadaviek kryté vkladmi a chránené autorizáciami elektronických úverov; (2) zodpovedajúce banky, ktoré akceptujú a distribuujú elektronické peniaze; (3) rad prevodných zariadení, ktoré sú používané klientmi pre uchovávanie elektronických peňazí, pre uskutočňovanie peňažných prevodov pomocou systémov zúčastnených bánk zapojených na centrálny počítač (on-line) alebo pre zmenu elektronických peňazí s inými podobnými prevodnými zariadeniami pri prevodoch, ktoré nie sú

uskutočňované v systémoch zapojených na centrálny počítač, teda v systémoch off-line; (4) bankomaty, spojené s vydávajúcimi a klientskými bankami, pre postup spracovania a umožnenia činnosti prevodných zariadení v ich styku s vydávajúcimi a klientskými bankami, a pre sprostredkovanie styku medzi vydávajúcimi a klientskými bankami navzájom; (5) clearingovú banku pre vyrovňovanie účtov elektronických peňazí rôznych vydávajúcich bank; (6) dátovú komunikačnú sieť umožňujúcu komunikačné služby všetkým zložkám systému; a (7) bezpečnostné usporiadanie pre zabezpečenie integrity systému a pre detekciu zneužitia a falšovania vo vnútri systému.

V preferovanom uskutočnení budú nasledujúce funkcie, zariadenie pre generovanie peňazí, zariadenie pre prevody, a zariadenie bankomatov zaistované pomocou kombinácie počítačových hardwarových modulov odolných proti zneužitiu a aplikačných softwarových modulov, ktoré môžu byť vzájomne prepojené v sieti. Informácia je prevádzaná v šifrovanej forme, aby sa tak zamedzilo neoprávnenému úniku informácií. Elektronické peniaze sú prevedené spolu s digitálnymi podpismi za účelom autenticity a odolnosti voči zmenám a falšovaniu.

Elektronické peniaze prevádzané týmito zariadeniami môžu byť elektronickou reprezentáciou hotovosti alebo úveru. Dôležitý aspekt elektronickej meny spočíva v tom, že táto mena je ekvivalentná bankovkám a je zmeniteľná s konvenčnými papierovými peniazmi proti vkladu u vydávajúcej banky, ale môže byť vybraná alebo uložená ako vo vydávajúcej banke, tak v klientskej (obslužnej) banke. Avšak len vydávajúce banky môžu vytvárať elektronickú hotovosť, a budú zodpovedné za ich krytie.

Vydávajúce banky neskôršie využijú vnútorné bankové clearingové a schvaľovacie postupy k zaisteniu monetárnej rovnováhy bankového systému, ako praktikuje súčasné

bankovníctvo.

Reprezentácie elektronických peňazí sú zmeniteľné, univerzálne akceptované, a bezpodmienečne umoriteľné u vydávajúcich bank, tj. majú vlastnosti peňažných prevodov. K ochrane integrity elektronického monetárneho systému každá zmena elektronických peňazí predstavuje súčasne s iným tiež výmenu informácie o dátach identifikujúcich peňažnú jednotku úveru alebo hotovosti, (tj. doláre, jeny, atď.) čiastku úveru alebo hotovosti, bankou vydávajúci elektronický úver alebo hotovosť, a niekoľko digitálnych podpisov.

Podľa širokého chápania tohto vynálezu, je namiesto prevodu v hotovosti navrhnutý elektronický monetárny systém, prevod elektronických peňazí, vrátane elektronickej hotovosti, kde na vyžiadanie môže byť požadovaný vklad v banke a elektronické úverové autorizácie. V jednom uskutočnení tohto vynálezu sa elektronický monetárny systém skladá: z peňažného modulu, ktorý generuje elektronické peniaze; peňažného modulu pre vydávanie distribúciu a príjem elektronických peňazí; a peňažného modulu pre príjem, ukladanie a prevod elektronických peňazí medzi iným prijímacím peňažným modulom a medzi prijímacím peňažným modulom a vydávajúcim peňažným modulom.

Podľa ďalšieho aspektu vynálezu elektronický monetárny systém ponúka zavedenie a správu elektronických peňazí, čo zahrňuje elektronickú hotovosť, ktorá je zmeniteľná za bežné peniaze pomocou požiadaviek voči vkladom v banke a pomocou autorizácií elektronických úverov.

V uskutočnení podľa tohto vynálezu zahrňuje systém rad vydávajúcich bank; modul generátora pre tvorbu elektronických peňazí; peňažné automaty spojené s modulmi generátorov pre uskutočňovanie bankomatových prevodov a pre komunikáciu s inými bankomatmi, ako sú prevody vrátane príjmu a distribúcie elektronických peňazí; bezpečnostný systém poskytujúci celkovú integritu elektronického

monetárneho systému; clearingový a schvaľovací postup pre vyrovnanie účtov elektronických peňazí oddelene vydávajúcich bánk a pre clearing elektronických peňazí vydaných vydávajúcimi bankami; a rad prevodných modulov vlastnených autorizovanými klientmi pre prenos elektronických peňazí medzi prevodnými modulmi a medzi prevodnými modulmi a bankomatmi; a moduly zákazníckych služieb, ktoré sa starajú o reklamáciu stratených peňazí a pre spojenie účtov s peňažnými modulmi, aby sa umožnil prístup k banke.

V súlade s iným aspektom tohto vynálezu, sú funkcie *modulov generátorov, prevodných modulov, bankomatov a modulov zákazníckych služieb*, realizované pomocou kombinácie hardwaru a softwaru, ktorá je odolná proti zneužitiu a môže byť použitá v sieti.

Elektronické peniaze zmieňané týmito modulmi môžu byť elektronickej reprezentácie hotovosti zálohované na požiadanie vkladovými účtami u vydávajúcej banky alebo úverovými autorizáciami a, aby sa zaistila bezpečnosť voči neoprávnenej modifikácii alebo falšovaniu, môžu byť prevádzané s digitálnymi podpismi. V preferovanom uskutočnení je dosiahnutá odolnosť voči falšovaniu a zneužitiu tým, že sa požaduje, aby pravidelná obnova modulov a jednotlivých jednotiek elektronických peňazí. S výhodou obsahuje prenos poukážky medzi modulmi rad identifikačných čísiel umožňujúcich overenie všetkých predchádzajúcich prevodov elektronickej poukážky. Moduly nechovajúce sa podľa požiadaviek a falšované elektronické poukážky môžu byť odstránené zo systému ihneď po ich odhalení.

V súlade s ďalším aspektom tohto vynálezu, je pre reklamáciu stratených peňazí ešte navrhnutý postup, umožňujúci majiteľovi/držiteľovi prevodného modulu predložiť nároky voči bankovému systému prostredníctvom modulu zákazníckych služieb a následne uznať overenie všetkých

predchádzajúcich operácií bankového systému s elektronickou poukážkou; majiteľ/držiteľ tak môže získať späť akúkoľvek stratenú a reklamovanú poukážku.

Ďalší aspekt tohto vynálezu poskytuje postup obnovy úveru prevodným modulom, v ktorom je použitá len jediná úverová poukážka pre každý úverový účet v peňažnom module.

V súvislosti s preferovaným uskutočnením tohto vynálezu je majiteľovi/držiteľovi prevodného modulu tiež ponúknutý postup umožňujúci bezpečne a spoľahlive nakupovať tovar od obchodníka.

Prehľad obrázkov na výkresoch

Ďalšie aspekty, rysy a výhody vynálezu budú pochopené a stanú sa jasnejšie, pokiaľ bude vynález posudzovaný v súvislosti s nasledujúcim popisom a sprievodnými obrázkami, kde:

Obr. 1A predstavuje schému ukazujúcu bezpečnostnú hierarchiu elektronického monetárneho systému

Obr.1B predstavuje schému ukazujúcu bezpečnostnú sieť odovzdávajúcu správu medzi primárnym bezpečnostným serverom a obyčajným bezpečnostným serverom.

Obr. 2 predstavuje schému bezpečnostnej sieťovej štruktúry elektronického monetárneho systému.

Obr. 3A ilustruje funkčné súčasti bezpečnostného serveru.

Obr. 3B ilustruje funkčné súčasti sieťového serveru.

Obr. 4A ilustruje funkčné súčasti modulu zákazníckych služieb.

Obr. 4B ilustruje funkčné súčasti primárneho bezpečnostného serveru.

Obr. 5 ukazuje prehľad sieťovej prihlasovacej procedúry.

Obr. 6A + 6K ilustrujú sieťový prihlasovací protokol.

Obr. 7A + 7E ilustrujú protokol vytvor spojenie v elektronickom monetárnom systéme.

Obr. 8A + 8B ilustrujú protokol preveď poukážky.

Obr. 9A + 9D ilustrujú protokol zahraničná zmena.

Obr. 10 ilustruje protokol záväzok uskutočniť prevod pre moduly elektronického monetárneho systému.

Obr. 11A + 11B ilustrujú protokol prerušenia prevodu pre moduly elektronického monetárneho systému.

Obr. 12A + 12C ilustrujú protokol o platbe na mieste predaja.

Obr. 13A + 13B ilustrujú protokol obnov úverov u výdajnej banky.

Obr. 14 ilustruje zostavenie úverového protokolu.

Obr. 15A + 15B ilustrujú protokol požaduj úver.

Obr. 16 ukazuje príklad histórie prevodu poukážky.

Obr. 17 ukazuje schému (typu strom) prevodu poukážky.

Obr. 18A + 18C ilustrujú protokol spoj peňažný modul s bankovým účtom (účty) pre prístup k banke.

Obr. 19A + 19B ilustrujú protokol opätovnej legalizácie spojenia peňažného modulu s bankovým účtom (bankovými účtami).

Obr. 20 ukazuje protokol platné číslo účtu.

Obr. 21A + 21B ilustrujú protokol vytvor reklamáciu stratených poukážok.

Obr. 22A + 22E ilustrujú protokol reklamácie stratených poukážok.

Detailný popis vynálezu

Tento vynález predstavuje zlepšenie monetárneho systému používajúci elektronické média k bezpečnej a spoľahlivej zmene ekonomických hodnôt. Systém môže byť zavedený integráciou nových systémov spracovávajúcich dáta s inými procedúrami, čo môže byť realizované v súčasných

celosvetových bankových systémoch. V súlade s týmto vynálezom, niekoľko vylepšení je obsiahnuté v elektronickom monetárnom systéme (Electronic Monetary System), zverejneným v patentovej prihláške USA č. 07/794, 112 podanej 15. novembra 1991, na ktorú sa odkazujeme. Toto vylepšenie obsahuje: sadu vylepšení týkajúcich sa bezpečnosti obsahujúcej zdokonalenú zahraničnú zmenu (F/X) a ďalej postupu pri prevode poukážok, postupu reklamácie stratených peňazí, postup pri spojovaní peňažných modulov pre bankový prístup, postupu pri platbe na mieste predaja, a postupu pre aktualizáciu úverov.

Bezpečnosť

Účinné zabezpečenie monetárneho systému má tri požiadavky: brániť sa falšovateľom, zistiť ich a zadržať ich. Popisovaný elektronický monetárny systém je navrhnutý tak, aby všetky spĺňal.

Aby peňažné moduly pri komunikácii odolali falšovateľom používajú šifrovanie so symetrickým a asymetrickým kľúčom. Všetky správy sú šifrované. Modulové protokoly sú navyše fyzicky chránené hardwarom, ktorý odoláva všetkým neoprávneným zásahom.

Falšovateľstvo je detekované pomocou postupu, v ktorom sa overujú poukážky¹. Časové protokoly používané v celom systéme (napr., vid'. expirácia) vyžadujú, aby elektronické poukážky boli pravidelne opätovne schvaľované. Tiež elektronické poukážky sú pri bankových prevodoch aktualizované (tj. nahradzované novou poukážkou s novým expiračným dátumom).

Peňažné moduly sú blokovanie (napr. zápisom do zoznamu neplatných ID), ak sú duplikované alebo je k nim pripojená sfalšovaná poznámka. Prevod nebude povolený tiež tým poukážkam, ktoré prešli takto blokovacími modulmi. Prevod

duplikovaných či falšovaných poukážok bude odložený do doby expirácie alebo prípadne deponovaný v banke. Ďalej v prípade vážnych systémových bezpečnostných problémov elektronického monetárneho systému môže systém požiadať o celkové opätovné overenie, pričom si, pre prípad ich nového prihlásenia do siete elektronického monetárneho systému, vyžiada overenie všetkými modulmi, vrátane prevodných peňažných modulov.

Nasledujúci zoznam vylepšenia by mal slúžiť k ochrane všetkej informácie pred odposluchom modulových interakcií. Všetky informácie sú šifrované, dokonca i verejné kľúče a modulové identifikátory. Zoznam vylepšených bezpečnostných opatrení:

- 1) Ochrana prihlásenia do siete spočíva v tom, že nikto nemôže zneužiť² peňažný modul alebo získať z neho akúkoľvek informáciu v použiteľnej forme, čo je ďalej popísané v odkaze na Obr. 5.
- 2) Vytvorenie metódy pre priradenie bezpečnostného serveru generátora peňazí a identifikátorov bankomatov (viď Schéma číslovania modulov). Tieto identifikátory sú kontrolované pri :
 - (a) vytváraní spojenia (viď Obr. 7);
 - (b) prevodu poukážok - kontrolou prevodných záznamov (viď Obr. 8).
- 3) Zavedením štruktúry serveru viazaného na dve strany (viď Bezpečnostná hierarchia a Bezpečnostná sieť), zahrňujúca primárny bezpečnostný server, kde všetky moduly nie sú verejné kľúče primárneho bezpečnostného serveru, a bezpečnostný server, ktorý overuje všetky ďalšie moduly.
- 4) Zlepšenie prevodných poukážok tak, aby umožnili kontrolu podľa zoznamu neplatných ID u všetkých prevodov pred prijatím poukážok k vyplateniu alebo zahraničnej zmene (F/X) a ďalej kontrolu duplikovaných poukážok (viď Obr. 8).
- 5) Šifrovanie všetkých certifikátov použitím súkromných kľúčov bezpečnostného serveru (viď Overovacia štruktúra

a uvedenie v platnosť).

6) Dynamické obmeňovanie veľkosti verejných kľúčov (viď Bezpečnostná sieť a Obr.6).

7) Zmena protokolu o záväzku zaistujúca, že zlyhanie neduplikuje vydaný suma peňazí³ (viď Obr. 10).

8) Zmenu zahraničnej zmeny (F/X) takú, aby žiadna strana nemohla podvodne prerušiť prevod a tak bezpečne prijať peniaze a súčasne žiadne neodoslať.

9) Zmenu protokolu prerušiť záznam informácie pri nedodržaní záväzku prevodu pokiaľ platiaci prevádza, ale prijímajúci prerušuje (viď Obr. 11).

10) Umožnenie celkového opätovného overenia, pokiaľ je to treba (viď Bezpečnostná sieť a Obr. 6).

Uvedený zoznam bezpečnostných zlepšení ďalej objasňuje niektoré bezpečnostné rysy poskytované vylepšeným bezpečnostným systémom tohto vynálezu. Toto a ďalšie vylepšenia môžu byť ďalej pochopené z nasledujúceho detailného popisu alternatívneho preferovaného uskutočnenia bezpečnostného systému pre elektronický monetárny systém.

Bezpečnostná hierarchia

V súvislosti s týmto vynálezom je ponúknuté iné možné uskutočnenie bezpečnostného zaistenia elektronického monetárneho systému. Podľa odkazov na Obr. 1A, bude mať elektronický monetárny systém dva typy bezpečnostných serverov a to primárny 1182 a bežné 1184. Primárne bezpečnostné servery 1182 overujú (bežné) bezpečnostné servery 1184. Bezpečnostné servery 1184 overujú všetky ďalšie moduly (moduly peňažného prevodu 1186, moduly bankomatu 1188, moduly peňažných generátorov - moduly 1190, a moduly zákazníckych služieb 1192) tohto systému.

Primárne servery 1182 len komunikujú s inými primárnymi servermi 1182 alebo bezpečnostnými servermi 1184. Podľa Obr.

2, primárnej bezpečnostnej servery 1182 sú umiestnené v bezpečnom zariadení spojenom so všetkými ostatnými pomocou miestnej bezpečnostnej siete LAN 1194. Táto miestna sieť LAN 1194 je pripojená s bezpečnostnou sieťou 1196 bezpečnou bránou. Po tejto sieti komunikujú len bezpečnostné servery. Všetky bezpečnostné servery sú fyzicky zabezpečené.

Bezpečnostné servery 1184 sú tiež pripojené k sieti elektronického monetárneho systému 1198 a bankovým miestnym sietiam 1200. Predpokladá sa, že bezpečnostné servery môžu byť zneužitú a preto sú legalizované po všetkých interakciách s ostatnými modulmi.

Len bezpečnostné servery (Security Server, ďalej tiež SS) 1184 a moduly majú certifikáty. Verejné kľúče primárneho bezpečnostného serveru sú prenášané pomocou týchto zariadení. Existujú dva druhy certifikátov: bezpečnostného serveru a modulu.

Štruktúra certifikátu a legalizácie

Štruktúra certifikátu je táto:

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

$$\text{Cert (M)} = E_{SS} [M(id) * M(PK) * \text{dátum expirácia} * \sigma_{PSS}(Y)] * \text{Cert (SS)}$$

1. Protokoly legalizácie certifikátu sú tieto:

- a) $PSS(id) = [PSS(id) \text{ XOR } C] \text{ XOR } C$
 - b) $D_{PSS}(E_{PSS}(X * \sigma_{PSS}(X))) = X * \sigma_{PSS}(X)$
 - c) Skontroluj či SS(id) je autentické (viď schéma číslovania modulov)
 - d) Skontroluj, či je platný dátum
 - e) Skontroluj, či platí $D_{PSS}(\sigma_{PSS}) = h(X)$
- 2) Legalizuj Cert (M)

- a) Legalizuj Cert (M)
- b) $D_{ss}(E_{ss}(Y * \sigma_{ss}(Y))) = Y * \sigma_{ss}(Y)$
- c) Skontroluj, či M(id) je autentické (viď schéma modulového číslovania modulov)
- d) Skontroluj, či je platný dátum
- e) Skontroluj, či platí $D_{ss}(\sigma_{ss}(Y)) = h(Y)$

Kde PSS ... Prim. bezp. server

PK ... verejný kľúč (vrátane) dĺžky

SS ... Bezp. server

σ ... digitálny podpis=EBh

* ... zretazenie

Cert ... certifikát

id ... ident. číslo

E ... Algoritmus so súkromným kľúčom kľúčom používaný pre šifrovanie a pre vytvorenie digitálneho podpisu

h ... Hashova funkcia

C ... konštantné náhodné číslo zdieľané všetkými ďalšími modulmi

D ... algoritmus pre dešifrovanie a kontrolu digitálneho podpisu využívajúci verejný kľúč.

Všimnite si, že E môže byť použité pre dešifrovanie a D pre šifrovanie, pokiaľ budú použité v inej aplikácii.

Schéma číslovania modulov

Primárne bezpečnostné servery 1182, bezpečnostné servery 1184, moduly peňažných automatov 1188, moduly peňažných generátorov 1190, moduly zákazníckych služieb 1192, a prevodné peňažné moduly 1186 majú priradené identifikačné čísla (id) tak, že je možné skontrolovať ich autentičnosť. 48-bitové prvé číslo "p" je generované a primitívny koreň "a" modulu p (kde $a^n \neq 1(p)$ pre všetky

$1 \leq n < p-1$) sa nájde pomocou bezpečnostného postupu. Ako a tak p sa zavedú do všetkých modulov systému bezpečne pomocou primárnych bezpečnostných serverov pri inštalácii.

Pracovná schéma je táto:

Pokiaľ $a^n \equiv m(p)$ a

- 1) $1 \leq m \leq 99\,999$ potom n je priradené ako id bezpečnostného serveru
- 2) $100\,000 \leq m \leq 999\,999$ potom n je priradené ako id bezpečnostného serveru
- 3) $1\,000\,000 \leq m \leq 6\,999\,999$ potom n je priradené ako id modulu peňažného automatu
- 4) $7\,000\,000 \leq m \leq 9\,999\,999$ potom n je priradené ako id modulu generátora peňazí
- 5) $10\,000\,000 \leq m \leq 11\,999\,999$ potom n je priradené ako id modulu zákazníckych služieb
- 6) $m \geq 12\,000\,000$ potom n je priradené ako id modulu prevodu peňazí.

Pokiaľ modul alebo server legalizuje certifikát, kontroluje autenticitu identifikačného čísla (napr. $M(id)$, $SS(id)$, $PSS(id)$) a tak, že spočíta $a^n \equiv m(p)$ a potom kontroluje či m je v správnom rozsahu.

Bezpečnostná sieť

Ako je ukázané na Obr. 2, bezpečnostná sieť 1196 a bezpečnostná miestna sieť LAN 1194 spojujú bezpečnostné servery 1184 s primárnymi bezpečnostnými servermi 1182. Pri inštalácii najprv bezpečnostné servery 1184 overia peňažné moduly a moduly zákazníckych služieb 1192. Také bezpečnostné servery môžu byť prepojené inštalačným modulom miestnej siete LAN 1202. Potom odovzdávajú bezpečnostné informácie, ako je zoznam neplatných id a zoznam primárnych bezpečnostných serverov a ich verejných kľúčov modulom. Zoznam neplatných id obsahuje totožnosti peňažných modulov,

serverov zákazníckych služieb a bezpečnostných serverov, u ktorých sú prevody blokované. Opätovné overenie týchto modulov je popísané následne vo vývojovom diagrame sieťového prihlásenia. Pri inštalácii sú primárnymi bezpečnostnými servermi 1182 najprv overené bezpečnostné servery 1184. Tieto primárne bezpečnostné servery môžu byť spojené pomocou bezpečnostného serveru inštalácie LAN 1204. Podľa Obr. 1B, bezpečnostné servery 1184 prijímajú rôznu bezpečnostnú informáciu, ktorú postupujú ostatným modulom. Bezpečnostné servery ponúkajú bezpečnostné služby sieti elektronického monetárneho systému 1198 a miestnym bankovým sieťam LAN 1200, ako pri prihlásení do siete, kde predávajú aktualizované bezpečnostné informácie. Bezpečnostné servery 1184 prijímajú túto informáciu od primárnych bezpečnostných serverov 1182 pomocou bezpečnostnej siete 1196. Prevodné peňažné moduly 1186 komunikujú so sieťou EMS 1198 prostredníctvom sieťových serverov 1206 (NS). Zúčastnené banky majú modul(y) bankomat(ov) 1188 a možno i modul peňažného generátora 1190 pripojené k ich miestnym bankovým sieťam LAN 1200.

Bezpečnostná sieť 1196 je prepojene zašifrovaná. Navyiac, primárne bezpečnostné servery a bezpečnostné servery zdieľajú spoločný symetrický kľúč (bezpečnostný sieťový šifrovací kľúč). Tento kľúč je periodicky obmeňovaný určeným primárnym bezpečnostným serverom 1182, verejným kľúčom, výmenou kľúča.

Zoznam neplatných ID je spravovaný určeným primárnym bezpečnostným severom 1182. Tento zoznam je vytvorený s interakcií so zúčastnenými bankami, s právne splnomocnenými autoritami, a klientmi systému.

Periodicky bude obmeňovaná dĺžka kľúča pre bezpečnostné servery a moduly. Aby sa zabezpečila vysoká bezpečnostná úroveň, bežne sa predlžuje dĺžka kľúča. Nové stanovené dĺžky kľúčov budú oznámené primárnym bezpečnostným serverom

prostredníctvom určeného primárneho serveru. Nové dĺžky kľúča budú oznámené bezpečnostným serverom primárnymi servermi, po zaslaní nových zoznamov neplatných ID alebo po novom overení. V prípade nebezpečného narušenia bezpečnosti môže primárny bezpečnostný server vyžiadať celkové opätovné overenie.

Dĺžka verejného kľúča pre každý primárny server sa nebude meniť. Bude vytvorený časový plán, ktorý časove rozvrhne zavádzanie primárnych bezpečnostných serverov do prevádzky i ich sťahovanie z prevádzky. Nové servery budú mať veľmi pravdepodobne ďalšie kľúče, ibaže by boli zavedené kvôli zvýšenému objemu prevodov. Zoznam aktívnych verejných kľúčov primárnych bezpečnostných serverov je vytvorený primárnym bezpečnostným serverom a podpísaný súkromným kľúčom serveru. Potom je tento zoznam rozposlaný ostatným bezpečnostným serverom.

Obr. 3A ukazuje funkčné zložky bezpečnostného serveru 1184. Funkcia *vonkajší interface* 1208 - poskytuje komunikačnú vrstvu pre spojenie sietí. Funkcia *manager spojenia* 1210 - riadi bezpečnostné aspekty prevodového spojenia. Funkcia *prihlásenia k sieti* 1212 - ovláda bezpečnostnú funkciu pre prihlásenie do siete. Funkcia *tvorba certifikátu* 1214 overuje certifikát všetkých peňažných modulov (v primárnom bezpečnostnom serveru túto funkciu zaistujú bezpečnostné servery). Funkcia *distribúcie overovacích kľúčov* 1218 distribuuje zoznam platných verejných kľúčov primárnych bezpečnostných serverov od overovacej agentúry peňažným modulom (primárne bezpečnostné servery tiež distribujú celkovú správu opätovného overenia). Funkcia kontrola zoznamu neplatných ID 1220 kontroluje a distribuuje zoznam neplatných identifikátorov. Funkcia *synchronizácie dátumu/času* 1222 zaistuje synchronizáciu služieb hodiny/časovač peňažného modulu so systémovým časom. Funkcia *hodiny/časovač* 1224 a šifrovanie

1226 sú identické s týmito funkciami v peňažných moduloch.

Obr. 3B ukazuje funkčnú súčasť sieťového serveru 1206. Funkcia *vonkajšia interface* 1228 poskytuje komunikačné prostredie pre spojenie so sieťou. Funkcia *manager komunikácie pri spojení* 1230 sprostredkováva komunikačné spojenie medzi peňažnými modulmi, a medzi peňažným modulom a bezpečnostným serverom. Funkcia *prihlásenia do siete* 1232 riadi postup prihlásenia peňažného modulu do siete. Funkcia *správa o ceste* 1234 poskytuje adresárove služby pre cestujúce správy tým, že riadi smerovanie správ pri prihlásení a pri spojení peňažného modulu. Funkcia *priamy prístup ku službám banky* 1236 poskytuje informáciu o službách zúčastnených bánk. Funkcia *šifrovanie* 1238 zaistuje funkciu *symetrický kľúč* 1240 a funkciu *generátor náhodných čísiel* 1242. Funkcia *symetrický kľúč* 1240 šifruje správy medzi sieťovým serverom 1206 a modulom pripojujúcim sa na sieť a medzi sieťovým serverom 1206 a bezpečnostnými servermi 1184. Funkcia *generátor náhodných čísiel* 1242 generuje náhodné čísla pre šifrovacie kľúče a overovacie správy.

V súhlase s týmto vynálezom je s výhodou doporučená iná zabezpečovacia súčasť, modul zákazníckych služieb (CSM) 1192. Modul zákazníckych služieb je zariadenie odolné proti zneužitiu a používané pre vytváranie a aktualizovanie účtových profilov. Modul zákazníckych služieb obsahuje jedinečný certifikát podobný certifikátu v peňažných moduloch a bezpečnostných serveroch. Moduly zákazníckych služieb môžu vytvárať bezpečné spojenia s inými modulmi (napr. bezpečnostnými servermi). Modul zákazníckych služieb, CSM, vyžaduje pripojenie hostiteľa k reprezentantovi zákazníckych služieb a on-line bankové systémy.

Modul zákazníckych služieb má dve základné funkcie. Za prvé vytvára účtovné profily tak, že peňažný modul sa môže spojiť s bankovými účtami, obnoviť platnosť spojenia

peňažného modulu s bankovým účtom a uviesť v platnosť čísla účtov. Tieto prevody sú detailnejšie popísané nižšie s odkazmi na Obr. 18-20. Za druhé, modul zákazníckych služieb spracováva nároky na stratené poukážky v reakcii na požiadavku reprezentanta hostiteľských zákazníckych služieb, čo je vysvetlené presnejšie na Obr. 21 a 22. Modul zákazníckych služieb má rovnaké bezpečnostné funkcie ako peňažný modul a špeciálny rozsah čísiel pre svoje identifikátory (viď Schéma číslovanie modulov). Výkonnosť týchto funkcií modulu zákazníckych služieb (CSM) zjednodušuje postup legalizácie čísiel účtov modulu bankomatu.

V súvislosti s uskutočnením elektronického monetárneho systému, ktorý používa modul zákazníckych služieb sa štruktúra profilu účtu pre každú banku mení na:

dátum expirácie * M(id) * B(id) * LA * $\sigma_{\text{CSM}}(X)$ * Cert(CSM), kde

M(id) ... identifikátor modulu

B(id) ... identifikátor banky

LA zoznam čísiel účtov druh účtu (vkladový alebo úverový)

σ_{CSM} ... označenie modulu zákazníckych služieb, CSM

Cert(CSM) .certifikát modulu zákazníckych služieb, CSM

* zreťazenie

Legalizačná procedúra pre taký profil je popísaná nižšie s odkazom na Obr. 20.

Obr. 4A ukazuje funkčné súčasti modulu zákazníckych služieb, CSM 1192. Vonkajší inteface 3000 je prostredníkom medzi modulom zákazníckych služieb hostiteľa, CSMH, a ďalšími spracovávajúcimi a komunikačnými prostriedkami vo vnútri procesoru hostiteľa modulu zákazníckych služieb, CSM; Manager komunikácie pri spojení 3001 pôsobí pri riadení a prevode (tj. ukončenie) alebo prerušuje prevodné spojenie medzi modulom zákazníckych služieb, CSM, a prevodným

peňažným modulom alebo reprezentantom zákazníckych služieb. Funkcia *vytvor profil účtu 3002* vytvára z informácií o účte zákazníka profil účtu, ktorý dovoľuje peňažnému modulu prístup k rôznym bankovým účtom klienta. Funkcia *verejný kľúč* overuje a podpisuje bankový účtový profil. Pretože modul zákazníckych služieb, CSM, vyžaduje od hostiteľa sprostredkovanie medzi reprezentantom zákazníckych služieb a on-line bankovými systémami funkcia *k hostiteľovi 3006* sprostredkováva oddelenie povinnosti medzi aplikáciami modulu zákazníckych služieb, CSM, a hostiteľskými aplikáciami. Funkcia *reklamácia stratených poukážok 3008* odpovedá na klientove nároky stratených poukážok, ktoré modul zákazníckych služieb, CSM, legalizuje a distribuuje vydávacím bankám. Funkcia *zaistenia bezpečnosti 3004* spravuje zoznam ohrozených peňažných modulov, žiada o certifikáty, synchronizuje hodiny, a spravuje tvorbu nových digitálnych kľúčov. Funkcia *hodiny/časovač 3012* a funkcia *šifrovania 3010* sú identické s týmito funkciami v peňažných moduloch.

Obr. 4B ukazuje funkčné komponenty primárneho bezpečnostného serveru 1182. Funkcia *vonkajšia interface 3020* poskytuje komunikačné vrstvy pre spojenie so sieťou. Funkcia *manager spojenie 3002* riadi bezpečnostné aspekty spojenia s bezpečnostnými servermi, s ktorými sa zachádza tak, ako by boli ohrozené, a ďalej s ďalšími primárnymi bezpečnostnými servermi. Funkcia *tvorba certifikátu 3024* vytvára certifikát pre akýkoľvek bezpečnostný server. Funkcia *distribúcia overovacích kľúčov 3026* distribuuje zoznam overovacej agentúry s platnými verejnými kľúčmi primárnych bezpečnostných serverov medzi bezpečnostné servery. Funkcia *distribúcia bezpečnostných sieťových kľúčov 3032* riadi a rozdeľuje bezpečnostné sieťové kľúče primárnym bezpečnostným serverom a bezpečnostným serverom. Funkcia *prikáž celkové opätovné overenie 3030* stanoví, či je

potrebné uskutočniť celkové opätovné overenie (tj. v dôsledku nebezpečného porušenia bezpečnosti) a keď ho považuje za nevyhnutné, zariadi ho. Funkcia *distribúcia zoznamu neplatných ID* 3028 riadi a rozdeľuje zoznam neplatných identifikátorov. Funkcia *hodiny/časovač* 3034 šifrovanie 3036 sú rovnaké s obdobnými funkciami v peňažných moduloch.

Sieťové prihlásenie

Prehľad procedúry sieťového prihlásenia je jasný zo schémy na Obr. 5. Prihlasovací protokol popisuje situáciu, v ktorej modul 1243 vyžaduje prístup k sieti elektronického monetárneho systému, EMS 1198 pre opätovné overenie, uloženie, výber či z iného dôvodu. Modul 1243 môže byť modul peňažného generátora 1188 alebo modul zákazníckych služieb 1192. K Obr. 5 patria ešte tieto vysvetlenia. (a) ... Vytvor komunikáciu medzi modulom 1243 a sieťovým serverom 1206. (b) 1206. (c) ... Sieťový server 1206 generuje náhodne overovacie číslo V a náhodný kľúč K; sieťový server potom postúpi certifikát modulu V a K bezpečnostnému serveru 1184 (šifrované pomocou NS/SS kľúča). (d) ... modul 1243 a bezpečnostný server 1184 vytvoria bezpečné komunikačné spojenie (viď kľúč spojenia (MM/SS)). (e) ... Bezpečnostný server 1184 postúpi čas/dátum, aktualizuje Zoznam neplatných ID, aktualizuje zoznam verejných kľúčov primárnych bezpečnostných serverov, dĺžku verejného kľúča, celkové opätovné overenie (v prípade nutnosti), a znovu overí modulový certifikát (v prípade nutnosti). (f) ... Ukonči spojenie s modulom 1243 a pošlite V a K modulu 1243. (g) (h) ... Sieťový server 1206 uzná sieťové prihlásenie k modulu 1243. (i) ... modul 1243 potom informuje sieťový server 1206 o cieľovom pripojení (pokiaľ existuje) ku ktorému je potrebné sa pripojiť. (j) ... Sieťový server

1206 vytvorí spojenie s cieľom.

Sieťové pripojenie je navrhnuté tak, že nikto nemôže podviesť modul 1243 alebo získať neoprávnene akúkoľvek informáciu vo zrozumiteľnej forme. Obr. 6 popisuje detailne priebeh procedúry sieťového prihlásenia.

Komunikácia A vytvára spojenie so sieťou elektronického monetárneho systému 1198 (krok 1244). Zaistenie bezpečnosti A pošle svoj certifikát sieťovému serveru (network server ďalej NS) 1206 (krok 1246). Prihlásenie do siete NS prijme certifikát NS (krok 1246). Generátor náhodných čísiel NS generuje náhodný kľúč K a náhodné overovacie číslo V (krok 1250). Symetrický kľúč NS zašifruje certifikát modulu, K a V pomocou NS/SS kľúča (krok 1252). NS/SS kľúče sú lokálne symetrické kľúče inštalované v sieťových serveroch 1206 a bezpečnostných serveroch 1184, ktoré komunikujú pri prihlasovaní do siete. Sieťové prihlásenie NS pošle certifikát, K a V bezpečnostnému serveru (SS) 1184, kde jeho sieťové prihlásenie obdrží správu a Symetrický kľúč SS dešifruje správu (kroky 1254 - 1258). Sieťové prihlásenie SS ukladá K i V a potom posiela modulový certifikát verejnému kľúču SS k legalizácii (kroky 1260 - 1264). Aby sa umožnila možnosť opätovného overenia, verejný kľúč SS neuvažuje dátum expirácie pri posudzovaní platnosti modulového certifikátu.

Ak modulový certifikát nie je platný, potom funkcia *sieťové prihlásenia SS* pripraví správu, na základe ktorej sa odoprie prístup, km prenosu k sieťovému serveru 1206 a modulu 1243 (krok 1266). Verejný kľúč SS zašifruje správu pre modul 1243 verejným kľúčom modulu a Manager spojenia SS pošle správu sieťovému serveru (kroky 1268 - 1270). Sieťové prihlásenie NS prijme správy a zaznamená zamietnutie prístupu. Šifrovaná správa je potom poslaná modulu, a sieťový server sa odpojí (krok 1272). Manager spojenia A túto správu prijme, verejný kľúč A dešifruje túto správu, a manager spojenie A zaznamená, že prihlásenie bolo

zamietnuté (kroky 1274 - 1278). Ak zariadením žiadajúcim prihlásenie bol peňažný modul prevodu, potom funkcia ku klientovi A informuje klienta (kroky 1280 - 1282). Ináč funkcia k banke A informuje banku (krok 1284).

Na druhej strane, ak je certifikát modulu platný, potom SS funkcia kontrola zoznamu neplatných id na SS zistí či id modulu je na zozname neplatných ID (kroky 1286 - 1288). Ak id je na tomto zozname, je prístup k sieti zamietnutý. Inak generátor náhodného čísla SS vytvorí náhodné číslo R a overovaciu správu (krok 1290). Funkcia bezpečnostného serveru SS sieťové prihlásenie SS zlúči R a overovaciu správu do správy, ktorá je šifrovaná verejným kľúčom SS pomocou verejného kľúča A. Verejný kľúč A ďalej rozšíri túto šifrovanú správu pridaním certifikátu bezpečnostného serveru (kroky 1292 - 1294). Správa je poslaná l AS, kde verejný kľúč A dešifruje správu a legalizuje certifikát bezpečnostného serveru (krok 1298).

V prípade, že je certifikát neplatný, A zaznamená ukončenie spojenia a informuje klienta alebo banku (kroky 1304 - 1306). Ak je certifikát platný, potom zaistenie bezpečnosti A skontroluje, či id bezpečnostného serveru nie je na zozname neplatných id (kroky 1308 - 1310). Ak je na zozname, je spojenie ukončené (kroky 1300 - 1306). Keď tam nie je, vytvorí generátor náhodných čísiel (RNG) patriaci k A náhodné číslo R(A) (krok 1312). Zaistenie bezpečnosti A utvorí kľúč spojenie (MM/SS pomocou funkcie R(A) XOR a potom uloží kľúč spojenie (krok 1314).

Správa obsahujúca overovaciu správu a R (A) je zostavená a zašifrovaná pomocou verejného kľúča bezpečnostného serveru (krok 1316). Manager spojenia A pošle správu k Sieťovému prihláseniu SS a Verejný kľúč SS dešifruje správu (kroky 1318 - 1322).

Sieťové prihlásenie SS overuje, či kontrolná správa je tá, ktorú samo vytvorilo (kroky 1324 - 1326). Pokiaľ to tak

nie je, zamietne bezpečnostný server prístup k sieti. Ak je kontrolná správa v poriadku, potom symetrický kľúč SS vytvorí kľúč spojenie (MM/SS) podľa $R(A) \text{ XOR } R$ (krok 1328). Manager spojenia zaznamená začiatok spojenia a pošle vyrozumienie k A pomocou podprogramu *pošli správu* (kroky 1330 - 1332). Manager spojenia A prijme toto vyrozumienie a zaznamená začiatok spojenia (krok 1334).

Hodiny/časovač A pošlú čas a dátum manažérovi spojenia, ktorý ich ďalej pošle bezpečnostnému serveru (kroky 1336 - 1340). Synchronizácia dátumu/času SS obdrží čas a dátum a skontroluje, či sú v dovolenom parametrovom rozmedzí (kroky 1342 - 1344). Ak nie sú v tomto rozmedzí, potom synchronizácia dátumu/času pošle nový čas a dátum manažérovi spojenia A (kroky 1346 - 1350). Hodiny/časovač A potom nastaví čas i dátum (krok 1352). Ďalej A znovu pošle svoj čas a dátum bezpečnostnému serveru pre opätovnú kontrolu. Ak je synchronizácia hodín uskutočnená viackrát ako je stanovené, potom je klientovi alebo banke ohlásená chybná funkcia hodín. Ak je to treba, môžu sa potom pokúsiť znovu o ďalšiu synchronizáciu (kroky 1354 - 1362).

Ak sú však hodnoty času a dátumu v určených medziach parametrov, potom sieťové prihlásenie SS zostaví správu obsahujúcu zoznam neplatných id, nový zoznam verejných kľúčov, primárnych bezpečnostných serverov (ktoré pochádzajú z funkcie *distribúcie overovacích kľúčov*), a dĺžku verejného kľúča (veľkosť verejných kľúčov je pravidelne obmedzovaná) (krok 1364). Tvorba certifikátov SS kontroluje či bolo požiadané o globálne opätovné overenie a zaistí, aby časová perióda pre celkové opätovné overenie nevypršala (kroky 1366 - 1368). Táto časová perióda má byť dosť dlhá na to, aby v jej priebehu akýkoľvek certifikát vypršal, alebo bol nanovo overený. Táto funkcia má tiež kontrolovať, kedy bol modul naposledy opätovne overovaný, pretože modul nie je treba overovať znovu, ak bol overený v priebehu celkového

opätovného overovania.

Ak je požadované opätovné overenie, potom funkcia vytvor certifikát SS pridá k predchádzajúcej správe informáciu "modul má znovu overiť" (krok 1370). Potom, ak už je alebo nie je požadované opätovné overenie, verejný kľúč SS podpíše správu (krok 1372). Správa je zaslaná k A, kde verejný kľúč A skontroluje digitálny podpis správy (kroky 1374 - 1378). Ak je podpis neplatný, je spojenie ukončené. Zaistenie bezpečnosti A potom aktualizuje svoje zoznamy neplatných id, verejných kľúčov, a dĺžky kľúča (krok 1382).

Modul A potom skontroluje, či jeho certifikát potrebuje byť opätovne overený (buď v dôsledku celkového opätovného overenia alebo kvôli uplynulému certifikátu) (kroky 1384 - 1386). Ak je požadovaný nový certifikát, potom zaistenie bezpečnosti A dá podnet ku generácii nového certifikátu (krok 1388). Verejný kľúč A vytvorí nové kľúče a potvrdí podpisom nové verejné kľúče pomocou svojho starého súkromného kľúča (krok 1390). Manažér spojenia A pošle potvrdený nový verejný kľúč k jednotke vytvor certifikát SS bezpečnostného serveru (kroky 1392 - 1396). Verejný kľúč SS potom legalizuje podpis na novom verejnom kľúči (kroky 1398 - 1400). Pokiaľ nie je podpis platný, potom bezpečnostný server odoprie prístup k sieti. Ak je podpis platný, potom verejný kľúč SS potvrdí podpisom nový certifikát modulu a pošle ho modulu (krok 1402). Manažér spojenia A obdrží certifikát, zaistenie bezpečnosti A uskutoční legalizáciu certifikátu a verejný kľúč A legalizuje podpis (kroky 1404 - 1410).

Ak certifikát nie je platný, potom manažér spojenia A pošle bezpečnostnému serveru pomocou funkcie pošli správu ako správu "neplatný certifikát", tak tento certifikát (kroky 1412 - 1413). Funkcia sieťové prihlásenie SS prijme správu a funkcia verejný kľúč SS legalizuje podpis (kroky 1414 - 1418). Ak bezpečnostný server uzná, že certifikát je

skutočne platný⁴, potom odoprie prístup tomuto modulu k sieti. Ak je však certifikát neplatný, potom manažér spojenia SS informuje sieťový server, že sa odpojuje od siete (krok 1420). Sieťové prihlásenie NS informuje modul o zlyhaní (krok 1422). Modul potom požiada klienta alebo banku o nový pokus (kroky 1424 - 1432).

Keď na druhej strane, modul určí, že je jeho nový certifikát platný manažér spojenia A pošle potvrdenie bezpečnostnému serveru (krok 1434). Podobne, pokiaľ nebol požadovaný nový certifikát, potom zaistenie bezpečnosti A pošle vyrozumienie bezpečnostnému serveru kroky (1436 - 1438). V oboch prípadoch, manažér spojenia SS prijme toto vyrozumienie a zaznamená koniec svojho spojenia s modulom (krok 1440). Sieťové prihlásenie SS potom pošle K i V do A (kroky (1442 - 1444)). Manažér spojenia A prijme správu a symetrický kľúč A zašifruje V a stanovenie cieľa pomocou K a pošle správu sieťovému serveru (kroky 1446 - 1448). Sieťové prihlásenie NS prijme správu a symetrický kľúč NS dešifruje správu a skontroluje, či V je identické s tým V, ktoré bolo predtým generované (kroky 1450 - 1454).

Ak nie je toto V identické s predchádzajúcim, potom sieťové prihlásenie NS pošle správu prístup odopretý k A a odpojí sa (kroky 1456 - 1458). Ak je V správne, potom sieťové prihlásenie NS vytvorí spojenie s miestom určenia a pošle vyrozumienie k A (krok 1460). Nakoniec, manažér spojenia A prijme vyrozumienie a zaznamená, že A bolo prihlásené k sieti elektronického monetárneho systému 1198 (krok 1462).

Vytvorenie spojenia

Obr. 7 ukazuje protokol vytvor spojenie. Zaistenie bezpečnosti A pošle certifikát modulu manažéra spojenia a manažér spojenia A prijme certifikát a skontroluje, či je

peňažný modul A pripojený k sieti (kroky 1464 - 1466). Ak peňažný modul A nie je pripojený k sieti, manažér spojenia A pošle certifikát prijatý od zaistenia bezpečnosti A do miesta určenia B (krok 1476).

Alternatívne, ak je peňažný modul A pripojený k sieti, symetrický kľúč A zašifruje certifikát pomocou K a manažér spojenia pošle zašifrovaný certifikát sieťovému serveru (kroky 1468 - 1472). Sieťový server dešifruje certifikát pomocou K a pošle ho do miesta určenia B.

Bez ohľadu na to, či bol certifikát poslaný sieťovým serverom alebo manažérom spojenia A, manažér spojenia B prijme certifikát a zaistenie bezpečnosti B (ak B je bezpečnostný server, je táto funkcia uskutočňovaná manažérom spojenia) legalizuje certifikát (kroky 1480 - 1482). Ak je certifikát neplatný, potom manažér spojenia B zaznamená, že je spojenie ukončené a informuje o tom buď žiadateľa, alebo banku (kroky 1486 - 1492) (ak B je bezpečnostný server, potom B len zaznamená, že sa prevod ukončil).

Ak je certifikát platný, zaistenie bezpečnosti B skontroluje, či je A na zozname neplatných ID (kroky 1494 - 1496). Ak A je na zozname, spojenie je ukončené. Ak A nie je na zozname, potom generátor náhodných čísiel B vytvorí náhodné číslo R(B) a overovaciu správu B (krok 1498). Hodiny/časovač B obnoví čas a dátum (krok 1500). Zaistenie bezpečnosti B zostaví R (B), overovaciu správu B, čas a dátum v jednu správu (krok 1502). Verejný kľúč B zašifruje túto správu pomocou verejného kľúča A a manažér spojenia B pripojí certifikát B k zašifrovanej správe a pošle správu k A (kroky 1504 - 1506).

Manažér spojenia A prijme správu, verejný kľúč A dešifruje zašifrovanú časť správy, a zaistenie bezpečnosti A legalizuje certifikát B (kroky 1508 - 1514). Ak je certifikát neplatný, manažér spojenia A zaznamená ukončenie spojenia a informuje buď klienta alebo banku (kroky 1516

- 1522). Ak je certifikát platný, zaistenie bezpečnosti A skontroluje, či B je na zozname neplatných id (kroky 1524 - 1526). Ak je B na tomto zozname, je spojenie ukončené. Nie je B na tomto zozname, zaistenie bezpečnosti A obnoví čas a dátum a porovná ich s dátumom a časom zodpovedajúcim B (kroky 1528 - 1530). Ak je dátum a čas mimo rozmedzia, je spojenie ukončené.

Ak sú čas i dátum v rozmedzí, potom generátor náhodných čísiel A vytvorí náhodné číslo $R(A)$ a overovaciu správu A (krok 1532). Zaistenie bezpečnosti A potom vytvorí spojovací kľúč pomocou funkcie $R(A) \text{ XOR } R(B)$ (krok 1534). Overovacia správa čísla A, overovacia správa čísla B, čas, dátum a $R(A)$ sú zložené do jednej správy a zašifrované verejným kľúčom B (krok 1536). Správa je poslaná do B manažérom spojenia A (krok 1538). Manažér spojenia B prijme správu, Verejný kľúč B dešifruje správu a zaistenie bezpečnosti B skontroluje overovaciu správu B (kroky 1540 - 1546). Ak overovacia správa B je nesprávna, potom je spojenie ukončené. Ak je overovacia správa B správna, potom zaistenie bezpečnosti B vytvorí kľúč spojenia pomocou $R(A) \text{ XOR } R(B)$ (krok 1548). Dátum a čas sú obnovené a pre kontrolu porovnané s časom A, aby sa skontrolovalo, či sú vo vopred určenom povolenom pásme odchýlok (krok 1550). Ak nie sú, je spojenie ukončené. Ak sú v tomto povolenom pásme, potom manažér spojenia B zaznamená začiatok spojenia (krok 1552).

Manažér spojenia B potom pošle vyrozumenie a overovaciu správu A do A (kroky 1554 - 1556). Manažér spojenia A túto správu prijme a zabezpečenie bezpečnosti A skontroluje overovaciu správu A (kroky 1558 - 1562). Ak nie je overovacia správa v poriadku, spojenie je ukončené. Ak je v poriadku, manager spojenia zaznamená začiatok spojenia (krok 1564).

Prevod poukázok

Obr. 8 ukazuje protokol prevodu poukázok. Adresár poukázok X vyberie poukážku(y), a hodnotu(y) pre prevod, obnoví hodnoty poukážky(žok), a sekvenčné číslo(a) a potom posielá správu do jednotky poukážky (krok 1566). Možné úlohy pre voľbu poukázok pre prevod môžu napríklad byť: (1) minimalizácia počtu digitálnych podpisov (tie potrebujú pre spracovanie istý čas); (2) minimalizácia veľkosti tzv. paketov; (3) maximalizácia užitočnosti elektronických poukázok ponechaných predvádzajúcemu klientovi (tj. postúpenie poukázok s najkratšou zostávajúcou platnosťou tj. do konca expiračnej doby). Tieto úlohy môžu byť vyriešené pomocou nasledujúceho algoritmu prevodu poukázok: (1) určite všetky možné alternatívy, s najmenším počtom poukázok; (2) určite, ktoré z týchto alternatív majú najmenší počet prevodov; (3) ak zostane viac ako jedna možnosť z kroku 2, vyberte tú, ktorá predstavuje najmenší počet peňažných jednotkových dní. Peňažné jednotkové dni = zostatková hodnota poukážky k prevodu násobená počtom dní zostávajúcich do vypršania expiračnej doby, sčítané pre všetky poukážky v pakete.

Poukážky X, pri prijímaní správy od adresára poukázok X vytvoria prevod, ktorý má byť pripojený ku každej poukážke, ktorá sa prenáša (krok 1568). Verejný kľúč X vytvorí podpis(y)⁵ pre poukážku(y) (krok 1570). Manažér paketov X potom zjednotí poukážky s ich novými prevod(mi), a podpisom (podpismi)⁶ do jedného paketu a pošle ich do Y (kroky 1572 - 1574). Manažér paketov Y prijme paket a rozoberie ho (krok 1576).

Overovateľ Y legalizuje všetky certifikáty v poukážke(kach) (napr. certifikát peňažného generátora, a všetky prevodové certifikáty). Potom overenie Y skontroluje, či identifikačné čísla v prevodovej skupine

zodpovedajú modulovým identifikačným číslam certifikátu v podpise a skupine certifikátov v celej histórii elektronickej poukážky. Tiež je legalizovaná konzistentnosť čiastky prevodu pre každú poukážku a to tým, že v priebehu histórie elektronickej poukážky je zaistené, aby čiastka prenášaná v každom následnom kroku bola nižšia ako u bezprostredne predchádzajúceho prevodu. Navyiac, aby bolo isté, že celková prevádzaná čiastka je rovná čiastke očakávanej, je kontrolovaná jej výška (kroky 1578 - 1580). Ak výška čiastok nesúhlasí, je prevod zrušený (krok 1582).

Ak to platí a Y je prevodný peňažný modul, potom overovateľ Y overuje expiračné dáta poukážky (poukážok) (kroky 1584 - 1588)⁷. Ak je niektorá z poukážok uplynulá, je prevod prerušený. Ak nie je uplynulá žiadna, potom overovateľ Y porovná každé id so zoznamom neplatných id (kroky 1590 - 1592). Ak je niektoré prevodové id na zozname neplatných id, je prevod prerušený. Ak prevodové id nie sú na zozname neplatných id (alebo Y nie je prevodný peňažný modul), verejný kľúč Y overí platnosť podpisov poukážok (kroky 1594 - 1596). Ak je niektorý podpis neplatný, je prevod prerušený. Ak je podpis platný, overovateľ Y skontroluje, či obsah poukážky zodpovedá obsahu poukážky uschovanej v Aplikácii Poukážok alebo umiestnená v Zápise o prevodu Tran Log (kroky 1598 - 1600). Pre každý obsah poukážky, ktorý zodpovedá, je pre prevod poukážky vytvorená schéma typu strom, aby bolo možné určiť, či poukážka nebola duplikovaná (kroky 1602 - 1604). Ak niektorá poukážka bola duplikovaná, je prevod prerušený. Táto kontrola duplikácie (t.j. kroky 1598 - 1604) je najmä zameraná na a dobre eliminuje kriminálne živly, pokúšajúce sa získať pre seba peniaze prevodom poukážok pomocou úmyselného zneužitia ohrozeného prevodového peňažného modulu.

Ak neboli nájdené duplikáty, ani neboli identifikované žiadne súhlasy obsahu poukážok, poukážky Y umiestnia

poukážku(y) do peňažnej schránky (krok 1606). Nakoniec adresár poukážok Y aktualizuje umiestnenie a hodnotu(y) poukážky (poukážok), a tiež inicializuje sekvenčné číslo (čísla) (krok 1608).

Mohlo by sa povedať, že postup pri prevode poukážok obsahuje kroky pre aktualizáciu a inicializáciu sekvenčných čísel k uľahčeniu odsúhlasenia poukážok (viď "Odsúhlasenie poukázaných peňazí"), ktoré kontrolujú, či príjemca akejkoľvek poznámky je na zozname neplatných Id, a či sú poukážky duplikované. Tieto prídavné rysy a kroky prakticky znemožňujú páchatelom uvádzať do obehu a cirkulovať duplikované poukážky, a zvyšujú schopnosť zisťovať duplikované poukážky v obehu.

Zahraničná zmena

Obr. 9 ukazuje protokol zahraničného výmenného prevodu peňazí pri použití dolárov a libier ako príkladov peňažných jednotiek. Najprv, A súhlasí zmeniť doláre s B za libry (£) vy výmennom kurze \$/£ (krok 1602). A i B potom prihlásia svoje peňažné moduly a tie vyžadujú od svojich klientov typ prevodu (kroky 1604 - 1610). A si vyberie nákup cudzej meny a B si vyberie predaj cudzej meny (kroky 1612 - 1614). A a B vytvorí bezpečné prevodové spojenie (kroky 1616 - 1620).

Ku klientovi A bude nabádať majiteľa/držiteľa A o čiastku podľa typu dolárových bankoviek, ktoré si praje vymeniť (krok 1622). Platba/zmena A príjme čiastku a adresár poukážok A skontroluje, či A má dostatok prostriedkov (kroky 1624 - 1628). Ak nie sú prostriedky dostatočné, potom funkcia ku klientovi A požiada o zadanie novej čiastky, u ktorej je znova zisťované, či je krytá existujúcimi fondmi (kroky 1630 - 1632). Ak nie je zadaná nová čiastka, je prevod prerušený (krok 1634).

Ak sú prostriedky dostatočné, platba/zmena A pošle dolárovú čiastku k B (kroky 1636 - 1638). Ku klientovi B potom požiada majiteľa/držiteľa o zadanie buď čiastky v librách, ktorú si praje vymeniť za doláre, alebo alternatívne iba výmenného kurzu dolárov (krok 1640). Adresár poukážok B skontroluje či sú fondy dostatočné (kroky 1642 - 1644). Ak nie sú, potom funkcia ku klientovi B požiada o nový kurz a znovu skontroluje, či sú dostatočné existujúce fondy. Ak však nie je vybratý nový kurz, potom platba/zmena B informuje A o jeho nedostatočných fondoch (kroky 1650 - 1652). A potom môže vybrať novú čiastku pre zmenu, alebo prevod zrušiť (kroky 1630 - 1634).

Ak B má dostatočné fondy pre prevod, platba/zmena B pošle A vyrozumienie i čiastku libier k zmene (je tiež poslaný ekvivalentný kurz) (kroky 1654 - 1656). Ku klientovi A vyzve ku kontrole sumy v librách i kurzu (kroky 1658 - 1660). Ak sú tento suma a kurz nesprávne, potom platba/zmena informuje B, že suma a kurz sú nesprávne (kroky 1662 - 1664). Funkcia ku klientovi B potom požiada o nový kurz (kroky 1666 - 1668). Ak nie je zvolený nový kurz, potom je prevod prerušený (krok 1670).

Ak však A overí správnosť sumy a kurzu prevodu, platba/zmena A postúpi dolárovú čiastku peňažnej schránke (krok 1672). Dolárové poukážky sú potom prevedené z A do B (krok 1674). Platba/zmena B postúpi čiastku libier svojej peňažnej schránke (krok 1676). Librové poukážky sú potom prevedené z B do A (krok 1678).

V tomto bode prevodu, obidva A i B dočasne držia cudzie výmenné poukážky v správnych čiastkach. A i B sa obidva zúčastnili dvoch prevodov" prevody A: (1) previedol doláre k B; (2) A prijal libry od B. Prevody B: (1) B previedol libry A; (2) B prijal doláre od A. K dokončeniu prevodu cudzej zmeny musí teraz A predať (t.j. dokončiť a trvale zapísať do svojho záznamu o prevode) obidva svoje prevody.

Podobne, B musí odovzdať obidva svoje prevody. Všimnite si, že A môže dokončiť prevod cudzej meny $A \rightarrow B$ (doláre z A do B) a $B \rightarrow A$ (libry z B do A) oddelene. Podobne B môže dokončiť prevod cudzej meny $A \rightarrow B$ a $B \rightarrow A$ oddelene.

Ďalší diel protokolu cudzej zmeny je navrhnutý tak, že žiadna skupina nepozná poradie, v ktorom bude prevod uskutočnený medzi prevodnými peňažnými modulmi. Táto neistota odradí kohokoľvek od účelových pokusov falšovať prevody. Podstatou toho je, že funkcia $S(X)$ je definovaná tak, aby $S(0) = A$ a $S(1) = B$, kde A a B predstavujú peňažné moduly A a B. Teda, ak X je náhodne vybraté ako 0 alebo 1, potom je náhodne vybratý i peňažný modul A alebo B.

Nasledujúci postup je použitý preto, aby umožnil A a B spoločné určenie náhodného X. $R(A)$ a $R(B)$ sú náhodné čísla generované postupne A a B počas podprogramu vytvorenia spojenia. Parita $R(A) \text{ XOR } R(B)$ je stanovená (pomocou exkluzívneho OR) pre každý bit $R(A) \text{ XOR } R(B)$. Táto parita je náhodné číslo X. $\underline{X}$ je doplnok k X ($\underline{X} = X \text{ XOR } 1$)^a.

Opäť podľa Obr. 9, Záznam o prevode A podmienene aktualizuje svoj záznam o prevode aby zaznamenal prevod $S(X)$ do $S(\underline{X})$ (krok 1680). Ak je X generované tak, že sa rovná 0, potom je podmienene zapísaný prevod z A do B (t.j. dolárový prevod) Ak je X generované tak, že sa rovná 1, potom je podmienene zapísaný prevod z B do A (t.j. prevod libier). Pretože záznam je zapísaný podmienene, môžeme sa k nemu vrátiť, keď peňažný modul A preruší prevod. Aktualizácia záznamu sa stáva trvalou v okamihu, keď táto bola nastavená nepodmienene (buď ako je explicitne ukázané vo vývojovom diagrame alebo implicitne pri dokončení prevodu). Manažér spojenia A potom pošle správu "zoznam aktualizovaný" k B (kroky 1682 - 1684). V odpovedi na to, záznam o prevode B tiež podmienene aktualizuje záznam, aby zaznamenal prevod $S(X)$ do $S(\underline{X})$ (krok 1686).

Ak $X = 1$, potom záznam o prevode B nastaví aktualizáciu

log ako nepodmienenú (kroky 1688 - 1690). Teda v tomto bode B odovzdalo svoje prevody libier A. Ďalej postupuje B podľa predávacieho protokolu záväzok (krok 1692), ktorý je popísaný ďalej s odkazmi na Obr. 10. V tejto situácii, A sa zaväzuje k uskutočneniu obidvoch svojich prevodov (t.j. prevádza doláre a prijíma libry) a B sa zaväzuje k uskutočneniu svojho zvyšného prevodu, t.j. prijíma doláre.

Ak však $X = 0$ (krok 1688), manažér Spojenia B pošle k A správu pošli správu zahájenia záväzku (kroky 1694 - 1696). Záznam o prevode A potom nastaví jeho aktualizáciu na nepodmienenú (krok 1698), a tak realizuje svoj prevod dolárov. Protokol o záväznej realizácii prevodu z obr. 10 je potom aktivovaný⁹ (krok 1700). Počas uskutočňovania tohoto protokolu (popísané ďalej) zrealizuje B obidva svoje prevody (t.j. prevod libier a príjem dolárov) a A s odhodlá k jednému svojmu zvyšnému prevodu, príjmu libier.

Ako je možné vidieť, zahraničný výmenný prevod, F/X , sa zaväzuje ku každému z prevodov poukážok, čo znemožňuje ich duplikovanie, ktoré by sa mohlo vyskytnúť, pokiaľ by tu bol iba jeden záväzok. Protokol zahraničnej zmeny zaisťuje, že žiadna strana nevie, ktorý prevod bude realizovaný ako prvý (prevod dolárov týkajúci sa A alebo prevod libier týkajúci sa B. Toto redukuje podnety niektorej zo strán zneužívať tento prevod. Každý prevod je realizovaný oddelene, ale ich poradie je vybraté náhodne pomocou dvoch modulov. Strana, ktorá sa pokúša zasahovať do prevodu, má 50% pravdepodobnosť, že príde o svoje peniaze. Tiež neexistuje žiadny iný popud k zásahu do uskutočnenia, pretože stratené peniaze môžu byť vyžiadané späť (viď reklamácia stratených peňazí).

Záväzok

Obr. 10 ukazuje protokol o záväznom prehlásení pre

moduly. Manažér spojenia X pošle k Y správu "pripravený k splneniu záväzku prevodu" (kroky 1702 - 1704). Ten postúpi správu "pripravený k splneniu záväzku prevodu" modulu prijímajúceho správu. Podľa konvenčného scenára peňažných prevodov je táto technika (využívajúca zaťaženie bremenom záväzného prehlásenia vopred), použitá tak, aby strana prevádzajúca peniaze najprv odovzdala, čo eliminuje možnosť duplikácie peňazí.

Manažér spojenia Y potom pošle oznámenie k X (kroky 1706 - 1708) a realizuje všetky zvyšné prevody pomocou aktualizácie svojho záznamu o prevodoch (krok 1710). Tiež, pokiaľ Y je prevodný peňažný modul, potom funkcia ku klientovi Y informuje klienta u úspešnom prevode (kroky 1712 - 1714). Manažér spojenia Y zaznamená koniec spojenia (krok 1716).

Záznam o prevode X príjme oznámenie od Y a aktualizuje svoj záznam o prevode, čím realizuje všetky ostatné prevody. X ukončí svoje prevody rovnako ako Y (kroky 1718 - 1724).

Prerušenie prevodu

Obr. 11 ukazuje protokol prerušenia prevodu pre moduly elektronického monetárneho systému. Manažér spojenia X zruší spätne zmeny a zaznamená, že prevod bol prerušený (krok 1726). Manažér spojenia X potom skontroluje, či správa "pripravený k splneniu záväzku prevodu" bola odoslaná (kroky 1728 - 1730). Ak tomu tak je, X aktualizuje svoj záznam o prevode (krok 1732) zápisom o tom, že X prerušil po odoslaní správy "pripravený k splneniu záväzku prevodu" a zapísaním identifikátorov poukážok a súm každej poukážky prijatej počas protokolu prevod poukážok. Teda, protokol o prerušení zhromažďuje informácie keď je počas zlyhania podprogramu záväzok volaný podprogram prerušenia.

Ak X je prevodný peňažný modul 1186, a správa

"pripravený k splneniu záväzku prevodu" bola odoslaná, potom funkcia ku klientovi X informuje svojich klientov o tom, že prevod bol prerušený a že mohli nastať chyby v prevode peňazí (kroky 1734 - 1738).

Ak X je bankomat 1188, potom funkcia k banke X informuje banku, aby obrátila svoje účtovné prevody (vhodným má dať a dal) (kroky 1740 - 1742). Ak X je prevodný peňažný modul 1186 a žiadna správa "pripravená ku splneniu záväzku prevodu" nebola odoslaná, potom ku klientovi X informuje klienta o tom, že prevod bol prerušený (krok 1744).

Vo všetkých prípadoch manažér spojenia X posiala k Y správu o tom, že prevod nemôže byť dokončený (kroky 1746 - 1748). Manažér spojenia Y spätne zruší uskutočnené zmeny a zaznamená, že prevod bol prerušený (krok 1750). Y potom informuje svojich klientov, že prevod bol prerušený (kroky 1752 - 1754) alebo informuje banku, aby obrátila svoje účtovné prevody (kroky 1756 - 1758).

Ako je popísané, ak je prevod prerušený v priebehu protokolu záväzok k prevodu, je možné, že poukážky budú stratené. Ak sa toto stane, príjemca poukážky bude mať prerušený prevod a odosielateľ poukážky bude mať ukončený prevod poukážky. V tomto prípade peňažný modul príjemca zaznamená informáciu o poukážkach, ktoré mali byť prijaté a upozorní klientov, že tu môže vzniknúť potencionálny problém (tj., neobdržal poukážky poslané od A). Za týchto okolností by sa dalo povedať, že modul platcu správne previedol poukážky.

Klient peňažného modulu príjemca môže potom nárokovať peniaze u certifikačnej agentúry. Informácia týkajúca sa nároku bude obsahovať záznam o prevode, ktorý zlyhal. Certifikačná agentúra môže potom skontrolovať s vydávajúcimi bankami, či boli poukážky uvedené do poriadku. Po určitej dobe, pokiaľ neboli poukážky uvedené do poriadku, môže

klient svoje peniaze nárokovat späť.

Platba na mieste predaja (Point of Sale, ďalej POS)

Obr. 12 ukazuje platobný protokol pre miesto predaja POS. Platobný protokol POS¹⁰ je určený ku zjednodušeniu platieb uskutočnených medzi prevodným peňažným modulom kupujúceho 1186 a prevodným peňažným modulom predávajúceho 1186. Prevodný peňažný modul predávajúceho 1186 môže, napr. byť umiestnený v hotovostnej pokladne supermarketu.

Najskôr súhlasí A s nákupom produktov alebo služieb od B (krok 1760). Majiteľ/držiteľ prevodného peňažného modulu A sa prihlasuje na svoj peňažný modul (krok 1762). Ku klientovi A požiada majiteľa/držiteľa o prevod a A si zvolí platbu na mieste predaja, POS. (kroky 1764 - 1766) Súčasne, predajca stanoví celkovú nákupnú cenu (krok 1768). Ku klientovi B požiada o prevod a B so zvolí možnosť prijať platbu POS (kroky 1770 - 1772). A a B potom vytvoria bezpečné spojenie (kroky 1774 - 1776).

Ku klientovi B požiada o čiastku platby a platba/zmena B príjme suma a pošle o A (kroky 1778 - 1782). Ku klientovi A potom požiada svojho klienta, aby overil požadovanú čiastku (kroky 1784 - 1786). Naviac je klient požiadaný, aby zvolil poukážku, v ktorej bude platiť (napr. mena alebo úver), a čiastku tak, aby sa súčet rovnal požadovanej čiastke. Ak požadovaná čiastka nie je správna, potom platba/zmena A pošle k B správu o tom, že požadovaná čiastka je nesprávna (kroku 1788 - 1790). Ku klientovi B potom požiada svojho hostiteľa o novú čiastku (kroky 1792 - 1794). Ak nie je čiastka zvolená, je prevod prerušený (krok 1796).

Ak je požadovaná čiastka správna, platba/zmena A príjme suma podľa typu poukážky (krok 1798). Adresár poukážok A potom skontroluje suma či sú fondy dostatočné (kroky 1800

- 1802). Ak fondy nie sú dostatočné, potom ku klientovi A požiada o nové čiastky podľa typu poukážky (kroky 1804 - 1806). Ak nie je zadaná nová čiastka, potom platba/zmena A pošle správu B, že nemá dostatočné fondy (kroky 1808, 1790). Ku klientovi B požiada hostiteľa o novú čiastku (kroky 1792 - 1794). Ak nie je nová čiastka zvolená, je prevod prerušený (krok 1796). Ak je zvolená nová, potom prevod platby začne znovu.

Ak sú fondy dostatočné, potom platba/zmena A postúpi čiastku peňažnej schránke (krok 1810). Poukážky sú potom prevedené z A do B (krok 1812). Nakoniec, prevodné peňažné moduly záväzkov prevodu dokončia (krok 1814).

Ako je možné vidieť, POS platba je pre kupujúceho zjednodušená, pretože to je platba inicializovaná veriteľom. Obecne, POS platba by bola použitá pre platbu obchodníkom za tovar, zatiaľ čo platba klienta klientovi (subscriber-to-subscriber, ďalej STS) by bola použitá k plateniu jednotlivcom alebo k plateniu účtov.

Aktualizácia úveru vydávajúcej banky

Obr. 13 ukazuje protokol Aktualizácia úveru po prevode vydávajúcej banky, a najmä popisuje, ako klienti získajú úverovú poukážku, ktorá je autorizovaným nositeľom úverovej platby. Klient môže mať až jednu úverovú poukážku pre každý úverový účet, ktorý vlastní. Všimnite si, že každá banka, ktorá dovoľí klientovi prijať aktualizovanú úverovú poukážku je vydávajúcou bankou pre tieto úverové poukážky.

Postup pri zavádzaní aktualizovaného úverového prevodu začína zavedením úveru medzi peňažným modulom A a bankovým bankomatom modulu B (krok 1854), ktorý je tu popísaný ďalej s odkazmi na Obr. 14.

Zavedenie úveru

Postup zavedenia úveru pre výber peňazí začína tým, že sa vlastník/držiteľ prevodného peňažného modulu A rozhodne aktualizovať úver a prihlási sa ku svojmu peňažnému modulu (krok 1876). Napríklad, klient A môže vlastniť úverovú poukážku, ale praje si zmeniť (tj. zvýšiť alebo znížiť) úverovú čiastku, vrátane zníženia čiastky až na nulu, alebo nemusí v danom okamžiku vlastniť úverovú poukážku, ale praje si ju získať. Ku klientovi A požiada držiteľa/vlastníka o prevod a A si vyberie možnosť aktualizovať úver určitej čiastky určitej banky a určitého účtu (kroky 1878 - 1880). V tomto uskutočnení je aktualizovaná určitá čiastka špecifikovaná klientom A celkovou úverovou čiastkou, ktorú si praje mať klient A. Potom prevodný peňažný modul A započne procedúru komunikácie s bankou, ktorá bola vybraná sieťou pomocou procedúry prihlásenia do siete popísanej vyššie (krok 1882).

Po dokončení krokov prihlásenia peňažného modulu, výberu prevodu a prihlásenia do siete, vytvorí A a B bezpečné spojenie (krok 1884).

Potom prevodný peňažný modul A vytvorí žiadosť o úver od modulu bankomatu B (krok 1886), podľa procedúry žiadosť o úver podrobnejšie popísanej s odkazom na obr. 15.

Žiadosť o úver

S odkazmi na Obr. 15 bude popísaný postup pre vyžiadanie úveru. Malo by sa povedať, že aj keď tento obrázok používa k označeniu strán X a Y v krokoch postupu nižšie popísaných, je možné ich aplikovať na akýkoľvek peňažný modul obchodujúci s modulom bankomatu.

Ak je na začiatku úverová poukážka pre vybratý účet, adresár poukážok X pošle čiastku tejto úverovej poukážky na

k bankomatu X (krok 1897). K bankomatu X určí čistý rozdiel medzi celkovou úverovou čiastkou požadovanou klientom A a čiastkou úverovej poukážky a pošle úverovú aktualizovanú žiadosť modulu bankomatu, a pritom požaduje určitú čistú čiastku z úveru, ktorý má byť autorizovaný zo špecifického účtu. V tomto prevode aktualizovanej úverovej žiadosti bude číslo účtu a profil účtu prevedený zo žiadajúceho peňažného modulu na modul bankomatu spoločne s čistou úverovou čiastkou (krok 1898). Táto správa je poslaná podľa protokolu pošli správu (krok 1900), v ktorom je správa zašifrovaná pomocou popísaných šifrovacích techník.

Akonáhle sú žiadosť o úverový výber a číslo a profil účtu prevedené modulu bankomatu, je iniciovaná procedúra legalizácie čísla účtu (krok 1902). Vývojový diagram popisujúci, ako je číslo účtu legalizované je na Obr. 20, ktorý je ďalej oddelene popísaný pre objasnenie.

S legalizáciou účtovných informácií, funkcia *k banke Y* overuje, či úver pre zaistenie požadovanej aktualizácie úveru je dostatočný (krok 1904). Dostatočný úver vyvolá u funkcii *k prevodu Y záväzok k prevodu pre X*, ktorý príjme vyrozumienie prostredníctvom svojej aplikačnej funkcie *k bankomatu* (kroky 1906 - 1912).

Nedostatočná úverová výška však spôsobí, že klient bude požiadaný o zadanie novej čiastky pre aktualizáciu úveru (kroky 1914 - 1918, Obr. 15B). Vstup novej čiastky pre aktualizáciu úveru od klienta povedie k zaslaní novej úverovej čiastky pomocou funkcie *k bankomatu* funkciou *k bankovej aplikácii peňažného modulu bankomat*, aby sa overilo, či fondy stačia ku krytiu naposledy žiadanej čiastky (kroky 1922 - 1924), a ďalej sa vraciame ku kroku 1904 podľa Obr. 15A. Ak nie je klientom žiadaná žiadna nová čiastka, je prevod prerušený (krok 1926).

Vráťme sa k Obr. 14, po návrate z programu realizujúceho žiadosť o úverový výber. K bankomatu A zahájí

prevod všetkých bankoviek, prevádzaných úverových poukážok (tj. úverových poukážok prijatých v predchádzajúcich prevodoch) a úverových poukážok pre tento účet k peňažnému modulu bankomatu (krok 1888). Ak nie sú v dobe, keď je žiadosť úverového výberu vytváraná, v prevodnom peňažnom modulu žiadne bankovky, pošle funkcia k bankomatu A správu peňažnému modulu bankomatu, že tu nie sú žiadne bankovky (kroky 1892 - 1894). Ak sú bankovky v prevodnom peňažnom module, potom sú elektronické poukážky prevedené z A do bankomatu B funkciou prevod poukážok popísané vyššie s odkazom na Obr. 8 (krok 1986).

Podľa Obr. 13, funkcia k prevodu B kontroluje, či všetky bankovky a prevádzané úverové poukážky boli skutočne prevedené (kroky 1856 - 1858), a ak niektoré z týchto poukážok (bankoviek) bola skutočne prevedené z prevodného peňažného modulu A, účtovné prevody odrazia zaznamenajú túto situáciu pomocou funkcie B k banke (krok 1860). V oboch prípadoch, ako v prípade, kde neboli prevedené žiadne poukážky z peňažného modulu, tak po účtovných prevodoch uskutočnených v kroku 1860, sa vytvorí spojenie medzi peňažným modulom bankomatu a modulom peňažného generátora (krok 1862). Funkcia k banke B aktualizuje úverové spojenie pridaním čiastky úverovej poukážky (pokiaľ existuje) do dostupnej úverovej výšky, aby zistila celkový dostupný úver, a odčítala požadovanú úverovú čiastku od celkového dostupného úveru. Ak nie je treba vytvoriť poukážky (vrátane bankoviek a úverových poukážok), pretože požadovaná čiastka bola nulová a žiadne bankovky neboli prevedené, potom peňažné moduly dokončia prevod podľa procedúry záväzok popísanej vyššie s odkazom na Obr. 10 (kroky 1865 - 1875).

Ak je potrebné vytvoriť nejaké poukážky (úverové alebo bankovky) v dôsledku nenulovej úverovej žiadosti a/alebo prevedených bankoviek, potom sú vyžiadané bankovky bankomatom B od modulu generátor peňazí podľa procedúry

žiadost o bankovky (kroky 1865 - 1866). Bankovky vyžiadané v generátore peňazí sú prevedené do modulu bankomat B pomocou funkcie prevod poukážok popísané vyššie (viď Obr. 8) pre prevod elektronických poukážok (krok 1868). Poukážky sú potom prevedené z modulu bankomatu B na prevodný peňažný modul použitím rovnakej funkcie prevod poukážok (krok 1870). Nakoniec, aby sa úspešne dokončila procedúra aktualizácie úveru, peňažný modul dokončí prevod podľa procedúry záväzok popísanej vyššie s odkazom na Obr. 10. Funkcia záväzok je iniciovaná najprv prevodným peňažným modulom uzatvárajúcim svoj prevod s modulom bankomatu B (krok 1872). Potom funkcia záväzok realizuje prevod medzi modulmi Bankomat B a generátor peňazí (krok 1874). To dokončí jednu úplnú aktualizáciu úveru od vydávajúcej banky.

Odsúhlasenie vydaných peňazí

Postup pri odsúhlasení poukážky/bankovky kontroluje falšovanie a duplikáciu poukážky/bankovky a je popísaný pomocou odkazov na Obr. 16 a 17. Systém odsúhlasenia vydaných peňazí, založený na informácii uloženej v riadiacom súbore vydané peniaze, vytvára strom prevodu poukážky, ktorý modeluje históriu prevodu poukážky.

Obr. 16 schematicky ilustruje hypotetický rad prevodov medzi generátorom peňazí s identifikačným číslom "1" (ďalej generátor peňazí 1), a modulom bankomatu s identifikátorom "2" (ďalej modul bankomatu 2), a štyroch prevodných peňažných modulov s celočíselnými identifikátormi 3 a 6 (ďalej prevodné moduly 3 - 6), pridruženými k jednej poukážke generovanej generátorom peňazí 1 v čase/dátume označenom ako 1:00:00.

V súlade s príkladom histórie prevodu ukázaným na Obr. 16, ilustruje Obr. 17, ako prevod elektronickej reprezentácie hotovosti vytvára stromu podobnú štruktúru

elektronickej reprezentácie hotovosti odvodenej od počiatočnej poukážky vytvorenej modulom generátora peňazí. Tak, ako sú ukladané alebo vračané jednotlivé prevody (časť vetve stromu) poukážky bankovému systému podľa aktualizácie poukážky, tak je budovaný strom prevodov poukážok na Obr. 17 pomocou zabudovaného systému odsúhlasenia vydaných peňazí. V tomto prípade, generátor peňazí 1 (modulové identifikátory sú obsiahnuté v digitálne overených certifikátoch) vytvárajú elektronickú reprezentáciu hotovosti 2300 majúcu podstatnú skupinu dátových polí a prevodovú skupinu dátových polí, ktoré sú ukázané schematicky v detaile pre jasnosť výkladu.

Mimo toho pre zjednodušenie nie je ukázaná skupina dátových polí podpisov a certifikátov.

Hlavná skupina podstatných dátových polí obsahuje identifikátor poukážky (napr. "N12"), identifikátor modulu peňažného generátora (napr. "MG1"), identifikátor vydávajúcej banky (napr. "Meno Banky"), dátum vydania (napr. 1:00:00), dátum expirácie (napr., 12:00:00), čiastku poukážky a identifikátor peňažnej jednotky (napr., \$50). Iné dátové polia hlavnej skupiny ako typ poukážky nie sú pre zjednodušenie ukázané. Rôzne dátové polia v elektronických poukážkach sú ukázané z ilustratívnych dôvodov vo forme deň: hodina: minúta. Iné formy monitorovania (napr. vrátane sekúnd) sú tiež možné.

Prevodová skupina dátových polí obsahuje prevodný záznam obsahujúci identifikačné číslo príjemcu, dátum prevodu, a prevádzanú čiastku. Prevodová skupina tiež s výhodou obsahuje sekvenčné číslo, ktoré je obohatené o poukážkový adresár platcu po každom prevode. Normálne by mali byť čas/dátum a prevodové id dostatočné k jednoznačnej identifikácii prevodu. Je však možné, že prevod, prevodové id, čas/dátum a čiastka by mohli byť duplikované, pokiaľ bol upravený čas medzi prevodmi a rovnako veľká čiastka je

prevádzaná na rovnaký modul. Aby sa predišlo tomuto problému, je k prevodnému záznamu a poukážkovému adresáru s výhodou pridané sekvenčné číslo k jednoznačnej identifikácii prevodu. Sekvenčné číslo je pridané k adresáru poukážky po každom prevode. Ak je sekvenčné číslo novo nastavené, potom to bude detekované ako duplikát.

Teda, keď je elektronická reprezentácia hotovosti 2300 prevedená k bankomatu 2, prevodný záznam 2302 je pripojený k prevodnej skupine a obsahuje identifikačné číslo príjemcu (napr. "2"), dátum prevodu (napr. 1:00:00), prevádzanú čiastku (napr. \$50), a sekvenčné číslo (napr. "1"). Pre prehľadnosť ukazujú poukážkové prevody na Obr.17 len novo pripojené prevodné záznamy prevádzanej poukážky. Pre prehľadnosť nie je tiež ukázaná prevodná skupina dátového poľa ukazujúca celkový počet prevodov.

Elektronická reprezentácia hotovosti 2300 z peňažného generátora 1 je uchovaná v module bankomatu 2. Ako časť výberu \$50 prevodným modulom 3, modul bankomatu 2 vytvorí elektronickú reprezentáciu hotovosti pomocou pripojenia prevodného záznamu 2304 ku kópii dátových polí v elektronickej reprezentácii hotovosti 2302 zväčšenej o prevodný záznam 2302. Táto poukážka je potom uložená v prevodnom modulu 3 do dokončenia výberu. To je možné chápať tak, že každý uzol stromu prevodu poukážky ukazuje novo pripojenú časť prevodového záznamu prevádzanej poukážky.

Reprezentovaný stromom prevodu poukážky, v 1:00:05, prevodný modul TR3 platí \$10 prevodným záznamom 2306 prevodnému modulu 4. V 1:01:00, prevodný modul 3, platí \$10 prevodným záznamom 2308 prevodnému modulu 5. V 3:08:01 prevodný modul 3 platí \$25 prevodným záznamom 2310 prevodnému modulu 5. V 4:11:08 prevodný modul 3 prevádza \$5 pomocou prevodného záznamu 2312 prevodnému modulu 6.

V 2:00:01 prevodný modul 4 prevedie \$5 prevodným

záznamom 2314 prevodnému modulu 6. V 2:01:07 prevodný modul 4 prevedie ďalších \$5 prevodným záznamom 2315 prevodnému modulu 6, ktorý obratom V 3:07:05 prevedie \$5 prevodnému modulu 3 prevodným záznamom 2321.

V 2:00:06 prevodný modul 5 prevedie celú \$10 poukážku prevodnému modulu 3 prevodným záznamom 2316. Z \$25 poukážky prijatej v 3:08:01 prevodným modulom 5 z prevodového modulu 3 v 3:09:12 prevodný modul 5 zaplatí \$20 zostávajúcich \$5 v module bankomatu 2 prevodným záznamom 2320.

V 4:10:00 prevodný modul 6 prevedie \$10 prevodnému modulu 5 podľa prevodného záznamu 2322, a V 5:00:06 prevedie zostávajúcich \$10 prevodnému modulu 3 prevodným záznamom 2324. V súlade s uskutočnením tohto vynálezu sa rozumie, že po uložení peňazí z prevodného modulu do banky všetky poukážky (vrátane úverových poukážok) prevodného modulu sú poslané bankovému systému a aktualizované. V dôsledku toho prebehne automaticky dodatočný a súbežný prevod reprezentovaný prevodným záznamom 2326. Je vo svojej podstate simultánny s vyššie popísaným prevodom¹¹ zálohou z prevodného modulu 5 k modulu bankomatu 2, ktorý je reprezentovaný prevodným záznamom 2320. Potom bude generovaná peňažným modulom 1 nová poukážka o hodnote \$5 (za predpokladu, že prevodný modul nemá žiadne úverové poukážky) a prevedená do prevodného modulu 3 prostredníctvom modulu bankomatu 2, spolu s pripojenými príslušnými prevodnými záznamami (nie je vyznačené). Súhlasne, môže byť prínosom, že aktualizácia všetkých poukážok v prevodnom peňažnom module po prevode (napr. uložení alebo výberu) a modulom bankomatu pomáha postupu odsúhlasenia poukážky poskytnutím dodatočných prostriedkov pre navrátenie poukážok do bankového systému.

V 5:00:10 prevodný modul 3 uloží \$10 v module bankomatu 2 pomocou prevodného záznamu 2328. Ako je popísané vyššie pre uloženie prevodným modulom 5, súbežne s uložением

prevodným modulom 3, reprezentovaným prevodným záznamom 2328, prebieha prídavný a súbežný prevod (nie je uvedený) všetkých poukážok vlastnených prevodným modulom 3 k bankovému systému, vrátane tých reprezentovaných prevodným záznamom 2316 a prevodným záznamom 2321. Potom, bankový systém vráti prevodnému modulu 3 poukážku s hodnotou rovnou súčtu všetkých poukážok poslaných bankovému systému k aktualizácii (tj. \$15).

V tejto chvíli teda len prevodný modul 6 vlastní prevoditeľné doklady o pôvodnej poukážke 2300, ako je reprezentované prevodnými poukážkami 2314 a 2312. Ak prevodný modul 6 uskutoční prevod (napr. uloženie alebo výber) s modulom bankomatu pred tým, ako prevedie tieto poukážky iným prevodným peňažným modulom, potom nebudú v obehu žiadne prevoditeľné poukážky, ktoré by odkazovali na pôvodnú poukážku 2300; všetky poukážky pochádzajúce z prevodov originálnej poukážky 2300 budú navrátené bankovému systému. To dovoľí kompletnú konštrukciu stromu prevodov poukážky ukázaného na Obr. 17. Dátum expirácie efektívne pomáha pri odsúhlasení poukážky pomocou obmedzenia obdobia, keď môže byť poukážka prevedená.

Zo stromu prevodov poukážky je jasné, že ak bola poukážka sfalšovaná, potom nebude hlavná časť poukážky zodpovedať prvému depozitu. Ak bol prevod duplikovaný, potom prevody dolu uvedené budú dávať väčší súčet, ako nadradená prevodná čiastka. Napríklad, ak prevodný modul 6 previedol \$20 prevodnému modulu 3 v 5:00:06 miesto \$10 (tj. prevodný záznam 2324), potom prevody pod prevodným záznamom 2318 (tj. SEQ1, 3:09:12, TR6, \$20) by dávali súčet \$30 čo znamená, že prevodný modul 6 duplikoval prevod.

Pripojenie peňažného modulu k bankovému účtu (tým) pre bankový prístup

Obr. 18 ukazuje protokol pre pripojenie peňažného modulu k bankovým účtom pre bankový prístup. Postup začne, keď sa klient(ka) identifikuje voči reprezentantovi zákazníckej služby (Customer Service Representative ďalej CSR) a požiada CSR o pripojenie klientského účtu k peňažnému modulu (krok 1928). CSR postúpi žiadosť CSM hostiteľovi A (CSMHA) ku spojeniu účtov pre identifikovanie klienta, a CSMHA získa prístup k informácii o účte identifikovaného klienta z bankového systému (kroky 1930 - 1934). Potom klient a CSR overia informáciu o účte a klient vyberie, ktoré účty má spojiť s peňažným modulom (krok 1936).

Po žiadosti klienta, aby jeho/jej peňažný modul B pripojil bankové účty a žiadosti CSR, pomocou CSMHA a týchto bankových účtov prepojených pomocou CSMA, je vytvorené bezpečné spojenie medzi peňažným modulom klienta B a týmto CSMA (kroky 1938 - 1946). Potom, ako odpoveď na žiadosť od funkcie k hostiteľovi A patriacej CSMA, CSMHA¹² pošle účtovnú informáciu k CSMA, ktorá príjme účtovnú informáciu a vytvorí z nich profil účtu (kroky 1948 - 1952). Verejný kľúč A potom podpíše účtovný profil a Vytvorenie profilu účtu skonštruuje správu z profilu účtu a podpisov a pošle ju peňažnému modulu B (kroky 1954 - 1958). Zaistenie bezpečnosti B príjme správu, a Verejný kľúč B skontroluje digitálne podpisy na správe (kroky 1958 - 1952). Ak nie sú podpisy platné, potom je spojenie prerušené (krok 1966).

Ak je podpis platný, potom ku klientovi B pošle profil k hostiteľovi, aby zákazník overil profil účtu. Ak zákazník neodsúhlasí profil účtu, je prevod prerušený. Ak potvrdí zákazník profil, potom Zaistenie bezpečnosti B pridá CSM certifikát k profilu účtu (krok 1968)).

Funkcia *k bankomatu B* zisťuje, či profil účtu je už uložený pre banku pridruženú s novo vytvoreným ("novým") profilom účtu. Ak profil účtu pre túto banku už v aplikácii *K bankomatu B* existuje, potom ho *K Bankomatu B* nahradí novým profilom účtu; inak, *K Bankomatu B* pridá nový profil účtu (kroky 1970 - 1974).

Opätovná legalizácia pripojenia peňažného modulu k bankovým účtom

Obr. 19 ukazuje protokol opätovnej legalizácie pripojenia peňažného modulu k bankovým účtom uskutočňovanou klientom. Postup sa začína prihlásením klienta na jeho/jej peňažné moduly, a v odpovedi na žiadosť o prevod generovanou funkciou ku klientovi A, klient zvolí nové schválenie spojenia bankového účtu s bankou spojenou s modulom zákazníckych služieb (CSM) B (kroky 1978 - 1982). Peňažný modul vyvolá a postupuje podľa protokolu sieťového zápisu popísaného s odkazom na Obr. 6, vyššie, a tak sa vytvorí bezpečné spojenie medzi peňažným modulom A a CSMB (krok 1986). *K Bankomatu A* potom vyšle profil účtu pre bankové účty k CSMB (kroky 1988 - 1990). Vytvor profil účtu B prijme správu, a *Zaistenie bezpečnosti B* legalizuje CSM certifikát a podpis profilu účtu (kroky 1992 - 1995). Ak je certifikát alebo podpis neplatný, potom CSM preruší prevod (krok 2000). Ak je certifikát platný, funkcia *k hostiteľovi B* pošle zoznam účtov z profilu účtu k CSM hostiteľovi (CSMH), ktorý porovnaním s použitím on-line bankového systému zistí, či každý účet je práve teraz aktívny (kroky 1996 - 2001). Ak niektorý z účtov je uplynulý, potom CSMH pošle správu o prerušení k CSM (krok 2010), ktorý potom preruší prevod podľa postupu prerušenia (krok 2000).

Ak sú všetky účty aktívne, potom CSMH signalizuje inštrukciu o opätovnej legalizácii *K CSM*, a funkcia *vytvor profil účtu B* prijme správu a vytvorí profil účtu z účtovných informácií (kroky 2002 - 2004. Verejný kľúč

B potom podpíše profil účtu, a vytvor profil účtu B skonštruuje z profilu účtu správu a podpis a pošle ju peňažnému modulu A (kroky 2006 - 2010). Verejný kľúč A pošle správu a overí digitálny podpis (krok 2012). Ak nie je podpis platný, potom peňažný modul A zruší prevod (krok 2018); ak je platný, podpis profilu a CSM certifikát sú pridané k profilu účtu (krok 2014) a peňažný modul A realizuje prevod (krok 2016).

Legalizácia čísla účtu

V súhlase s uskutočnením tohto vynálezu používajúceho modul zákazníckych služieb (CSM), ktorý je popísaný vyššie, je na Obr. 20 uvedený vývojový diagram popisujúci, legalizáciu čísla účtu. V tomto postupe zaistenie bezpečnosti Y prijme číslo účtu a profil účtu, vrátane certifikátu CSM a overí certifikát CSM (krok 2020). Neplatný certifikát spôsobí prerušenie prevodu medzi dvomi peňažnými modulmi (krok 2028).

Ak je certifikát platný, funkcia *zaistenie bezpečnosti* Y prinesie profil účtu k verejnému kľúču Y k overeniu CSM podpisu (krok 2022). Neplatný podpis spôsobí, že *Zaistenie bezpečnosti Y* informuje manažéra spojenia o tom, že profil účtu je neplatný (krok 2026), a prevod medzi dvomi modulmi je prerušený (krok 2028).

Ak test podpisu potvrdí jeho platnosť, funkcia pokračuje tým, že funkcia k banke Y pošle číslo účtu, ktoré prijal prostredníctvom on-line počítačového systému (krok 2024). Neaktívny účet spôsobí, že funkcia *zaistenie bezpečnosti Y* informuje manažéra spojenia o neaktívnom účte (krok 2030) a preruší prevod (krok 2028); aktívny účet spôsobí, že postup legalizácie čísla účtu sa vráti k ďalšiemu kroku z operačného vývojového diagramu, ktorý vyvolal postup pri legalizácii čísla účtu.

Je zrejmé, že v porovnaní s týmto uskutočnením vynálezu, ktorý neobsahuje CSM, je postup pri legalizácii čísla účtu pre modul bankomatu zjednodušený.

Reklamácia stratených peňazí

Ako bolo diskutované, elektronické peniaze môžu byť stratené z niekoľko dôvodov, vrátane: (1) peňažný modul je zničený a nefunkčný; (2) peňažný modul je stratený alebo ukradnutý; alebo (3) záväzok nebol splnený. Pre monetárny systém je dôležité, aby klient veril, že jeho peniaze sú bezpečne uložené. Je teda dôležité, aby príjemca bol schopný vyreklamovať peniaze stratené v dôsledku systémového zlyhania. Schopnosť zmeny peňazí v prípade poškodenia peňažného modulu by zlepšila pocit bezpečia, pretože elektronické zlyhanie je pravdepodobnejšie ako strata papierov fyzickým zničením. Náhrada peňazí z dôvodu omylov vyplývajúcich zo strateného alebo ukradnutého peňažného modulu je problematickejšia. Povolenie takých reklamácií by mohlo prilákať rozsiahle reklamácie v systéme, pokiaľ by klienti neučinili predbežné kroky proti takým škodám.

Vo všetkých prípadoch popísaných v tomto vynáleze existujú metódy, ktoré dovoľujú náhradu peňazí stratených v niektorom z týchto prípadov. V prvých dvoch prípadoch (tj. prípad (1) a prípad (2) vyššie) by klient musel periodicky vytvárať požiadavku na stratenú poukážku(ky) (viď Obr. 21), ktorá by bola uložená mimo peňažný modul. V prípade zlyhania by požiadavka mohla byť predložená s klientovou identifikáciou u vydávajúcej banky (viď Obr. 22). Požiadavka by obsahovala posledný známy stav klientovho peňažného modulu. Popis nárokováných poukážok by bol legalizovaný a rozdelený vydávajúcim bankám. Vydávajúce banky by mohli vymeniť peniaze po istej dobe, pokiaľ by nárokované poukážky neboli uložené.

V prípade, keď nie splnený záväzok (tj. prípad (3) a ak je peňažný modul stále funkčný (vid' Obr. 22), je taký nárok reklamácie vytvorený interaktívne medzi peňažným modulom a modulom zákazníckych služieb. Táto požiadavka, ako v prípadoch (1) a (2), je postúpená vyšetrovaciemu systému pre vydané peniaze, ktorá sleduje nároky proti úložkám peňazí. Vydávajúce banky sa môžu cítiť bezpečne pri hradení stratených peňazí, pretože môžu monitorovať vstupujúce peniaze proti prihláškam defraudantov a pretože majú identifikáciu toho, kto sa prihlasuje.

Tieto metódy sú podrobnejšie popísané u odkazov na Obr. 21 a 22.

Vytvor nárok na stratenú poukážku(y)

S odkazom na Obr. 21A, je ukázaný postup pri vytvorení nároku, reklamácie, na stratenú poukážku(y), ktorý môže byť použitý v súhlase s uskutočnením tohto vynálezu. Postup začne, keď sa klient prihlási k peňažnému modulu: funkcia ku klientovi A požiada klienta o prevod a klient vyberie možnosť vytvor nárok na stratenú poukážku (kroky 2032 - 2036).

Potom nasleduje niekoľko krokov, ktoré konsolidujú¹³ tie poukážky a nenárokované záväzky, ktoré zlyhali (kroky 2038 - 2042). Špecificky, adresár poukážok A vytvorí jedinečné poradové číslo nároku (ktoré je použité pre identifikáciu požiadavky) a prevedie kópiu adresára požiadaviek s poradovým číslom k manažérovi paketov. Funkcia poukážky A prevedie kópie všetkých poukážok s podpismi a certifikátmi do manažéra paketov. Potom funkcia zápis o prevode A odošle všetky nenárokované prevody, čo zlyhali pri realizácii, a tie, ktoré boli prihlásené pri prerušení do manažéra paketov.

Ďalej funkcia verejný kľúč A používa súkromný kľúč

peňažného modulu k podpisu poradového čísla požiadavky, adresára poukážok, poukážok, a zlyhanie pri realizácii, ktoré boli poslané do manažéra paketov, a manažér paketov pripojí podpis k zlúčeným dátam, výsledkom čoho je paket zlúčených dát (kroky 2044 - 2046ä, ktorý je potom zašifrovaný pomocou verejného kľúča A (krok 2048). K zašifrovanej požiadavke pridá verejný kľúč A potom popis požiadavky skladajúcej sa z poradového čísla požiadavky, celkového monetárneho sumy požiadavky, a certifikátu peňažného modulu A (krok 2050). Funkcia ku klientovi A pošle túto požiadavku k hostiteľovi peňažného modulu, ktorý príjme a uloží požiadavku -- na médiu fyzicky nezávislom na peniazoch -- pre budúce použitie (kroky 2052 - 2054).

Je teda jasné, že postup reklamácie stratených poukážok poskytuje spôsob pre generovanie a ochranu potenciálnych finančných nárokov, ktoré nie sú zničené poškodením či zlyhaním peňažného modulu.

Reklamácia Stratenej Poukážky

Obr. 22 ukazuje protokol pre reklamáciu stratených poukážok, ktorý začína klientovou žiadosťou o reklamáciu stratenej poukážky voči reprezentantovi zákazníckych služieb (customer service representative) ďalej CSR, žiadateľova identita je oznámená CSR (krok 2056). CSR potom odovzdá klientovu identitu k hostiteľovi modulu zákazníckych služieb (CSMH) A, a skontroluje, či reklamácia je dôsledkom nesplnenia záväzku alebo dôsledkom straty čo deštrukcie peňažného modulu (kroky 2058 - 2060). Ak dôvodom k reklamácii je nesplnenie záväzku (a klientove peniaze neboli stratené alebo zničené), potom na základe klientovej voľby reklamovať stratené poukážky od peňažného modulu a voľby CSR prijať reklamáciu stratených poukážok od peňažného modulu, manažér Spojenia B klientovho peňažného

modulu a manažér Spojenia A modulu zákazníckych služieb (CDSM) pridružený k reprezentantovi zákazníckych služieb (prostredníctvom hostiteľa modulu zákazníckych služieb (HCSM) sú každý zvlášť vyzvaný k vytvoreniu bezpečného spojenia medzi CSM A a peňažným modulom B (kroky 2062 - 2070).

Akonáhle je spojenie vytvorené, funkcia k hostiteľovi A patriaca k CSM vyžiada identitu klienta a HCSM A odpovie na túto žiadosť odoslaním správy obsahujúcej klientovu identitu k CSM (2072 - 2074). Reklamácia stratenej poukážky A príjme túto správu a pošle peňažnému modulom B správu o tom, že reklamácia má byť poslaná (kroky 2076 - 2078).

Zápis o prevode B príjme túto správu a obnoví tie záznamy nesplnenia záväzku, ktoré neboli reklamované (krok 2080). Ak nie sú nájdené žiadne záznamy nesplnenia záväzku, potom je prevod prerušený (krok 2083). Inak ku klientovi B pošle informáciu (napr. dátum, čas, a výšku sumy) z obnovených záznamov o nesplnení záväzku ku klientovi k preskúmaniu (krok 2082). Z tejto informácie klient vyberie prevody, ktoré budú reklamované (krok 2084). Napríklad, klient nevyberie prevody, u ktorých nebol splnený záväzok, ktoré boli riešené jednotlivo. Potom, pre každý klientom vybraný prevod, u ktorého nebol splnený záväzok vytvorí zápis o prevode B správu obsahujúcu záznam informácie o týchto prevodoch, a pošle túto správu k CSM (kroky 2086 - 2088).

Reklamácia stratených poukážok A príjme túto správu a pošle k B vyrozumienie vrátane identifikátora reklamácie (napr. overovacie číslo pre budúci odkaz k reklamácii (krok 2092). Zápis o prevode B príjme vyrozumienie a označí každý vybraný prevod s nesplneným záväzkom časom/dátumom reklamácie a identifikátorom reklamácie poskytnutým od CSM (krok 2094). Potom B realizuje prevod (krok 2096). Potom, čo je funkcia záväzného prehlásenia skončená, reklamácia

poukážok A vytvorí z prijatej správy obsahujúcej informáciu o prevodoch, u ktorých nebol splnený záväzok, nárok, ktorý má byť odoslaný do vyšetrovacieho systému vydávaných peňazí (Money Issued Investigation Systém - ďalej MIIS). Ten s výhodou vytvorí časť vyšetrovacieho systému prevodov. Funkcia k hostiteľovi A pošle túto požiadavku k HCMSA¹⁴, ktorý ju prijme a odošle ďalej k MIIS (kroky 2098 - 2102).

A teraz späť ku kroku 2060 z obr. 22. Ak reklamácia nie je založená na nesplnení záväzku (napr. pre stratenie¹⁵ či poškodenie peňažného modulu), potom klient môže vybrať reklamáciu stratených poukážok od hostiteľa B, ktorý má prístup ku všetkým reklamáciám klienta, ktoré boli generované a odhlásené z počítačového prostredia peňažného modulu (napr. do FLASH pamäti) v súlade s postupom reklamácie stratenej(ých) poukážky(žok) popísaným vyššie s odkazom na obr. 21. CSR oddelene vyberie vyvolanie postupu vedúceho k prijatiu reklamácie stratených poukážok od peňažného modulu hostiteľa - a hostitelia vytvoria komunikačné spojenia podľa akejkoľvek známej metódy (kroky 2104 - 2108).

Potom pošle klient hostiteľa B požiadavku, obsahujúcu certifikát peňažného modulu, k CSMHA, ktorý pošle reklamáciu k CSMHA (kroky 2108 - 2112). Reklamácia stratených poukážok A prijme túto reklamáciu a pošle ju verejnému kľúču A, ktorý legalizuje certifikát peňažného modulu (2114 - 2116). Ak je certifikát peňažného modulu neplatný, potom funkcia k hostiteľovi A pošle k CSMHA správu o tom, že požiadavka bola odmietnutá a CSMHA ju presmeruje k hostiteľovi klienta B a reklamácia stratených poukážok je ukončená (kroky 2120 - 2121).

Ak je certifikát peňažného modulu platný, Verejný kľúč A dešifruje nárok a overí všetky poukážkové certifikáty a podpisy (krok 2118). Ak niektorý certifikát alebo podpis nie sú platné, je prevod ukončený (kroky 2119 - 2121). Ak sú

certifikáty a podpisy poukážky platné, potom reklamácia stratených poukážok A overí, či súhlasia prevádzané čiastky, aby sa zaistilo, že hodnota peňazí prevádzaných príjemcovi nie je vyššia ako hodnota prijatá od odosielateľa pre prevodnú históriu každej poukážky (kroky 2122 - 2123). Ak je tu nejaká nezrovnalosť, je prevod ukončený (kroky 2120 - 2121).

Ak sú však prevodné čiastky v poriadku pre všetky poukážky, potom reklamácia stratených poukážok A vytvorí nárok, ktorý bude poslaný do MIIS, a tiež vytvorí identifikátor nároku, ktorý sa pripojí k nároku. Funkcia k hostiteľovi A potom vyšle vytvorený nárok a jeho identifikátor k CSMHA, ktorý ho príjme a príslušne nasmeruje ku klientovi hostiteľa B a nárok pošle k MIIS (kroky 2124 - 2128), tým dokončí reklamáciu stratených poukážok.

Aj keď vyššie uvedený popis ukazuje veľa zvláštností, nemajú tieto detaily byť výčtom obmedzujúcim rozsah tohoto vynálezu, a odborníkovi je jasné že tento vynález umožňuje veľa modifikácií, adaptácií a ekvivalentných realizácií, bez toho aby sa tým prekročil rozsah tohoto vynálezu a obmedzil nejak jeho výhody. Je teda účelné, aby tento vynález nebol limitovaný podľa uvedených realizácií, ale bol definovaný v súlade s nasledujúcimi patentovými nárokmi.

P A T E N T O V É N Á R O K Y

1. Systém pre prevod elektronických poukážok medzi elektronickým modulom založeným na procesore, ktorý obsahuje:
elektronické moduly založené na procesore, kde každý modul je schopný vytvoriť šifrovaný bezpečnostný kanál a prevádzať a prijímať elektronické poukážky cestou zmieneného šifrovaného bezpečného kanálu, a kde každý zmienený elektronický modul má pamäť pre uchovávanie zmienených elektronických poukážok; kde každá elektronická poukážka obsahuje:
hlavnú skupinu dátových polí obsahujúcu dáta vyjadrujúce monetárnu hodnotu spojenú so zmienenou elektronickou poukážkou;
prevodovú skupinu dátových polí obsahujúcu zoznam prevodných záznamov, kde každý prevodný záznam je vytváraný prevodným elektronickým modulom a obsahuje poradové číslo, ktoré odlišuje prevádzanú elektronickú poukážku od iných prevádzaných elektronických poukážok prevádzaných zmieneným prevodným elektronickým modulom.
2. Systém podľa nároku 1, v y z n a č u j ú c i s a t ý m, že zmienená monetárna hodnota je pôvodná monetárna hodnota spojená so zmienenou elektronickou poukážkou, a zmienený prevodný záznam ďalej obsahuje prevádzanú monetárnu hodnotu.
3. Metóda platby používajúca prvý peňažný modul k prevodu elektronickej reprezentácie peňazí na druhý peňažný modul, skladajúci sa z krokov:
(a) vytvorenie šifrovaného bezpečného spojenia medzi zmieneným prvým peňažným modulom a zmieneným druhým peňažným modulom, kde ani jeden z obidvoch peňažných

modulov nie je možné zneužiť;

(b) zmieneného druhého peňažného modulu, ktorý vyžiada na druhom klientovi podmienky prevodu, a zmienený druhý klient dodá prevodné podmienky zmienenému peňažnému modulu;

(c) zmieneného druhého peňažného modulu, ktorý posielá zmienené prevodné podmienky zmienenému prvému peňažnému modulu, cestou zmieneného šifrovaného bezpečného spojenia;

(d) zmieneného prvého peňažného modulu, ktorý vyžiada u prvého klienta overenie prevodných podmienok; zmienený prvý klient dodáva zmienené prevodné podmienky;

(e) zmieneného prvého peňažného modulu, ktorý prevádza elektronickú reprezentáciu peňazí do zmieneného druhého peňažného modulu, cestou zmieneného šifrovaného bezpečného spojenia.

(f) zmieneného prvého peňažného modulu, ktorý odovzdáva zmienený prevod elektronických peňazí pomocou zaznamenania zmieneného prevodu elektronických peňazí tak, že zmienený prvý peňažný modul nemôže už zrušiť zmienený prevod elektronických peňazí návratom do pôvodného stavu; a

(g) zmieneného druhého peňažného modulu, ktorý odovzdáva zmienený prevod elektronických peňazí pomocou zaznamenania zmieneného prevodu elektronických peňazí tak, že zmienený druhý peňažný modul nemôže už zrušiť zmienený prevod elektronických peňazí návratom do pôvodného stavu.

4. Platobná metóda podľa nároku 3, v y z n a č u j ú c a s a t ý m, že zmienené podmienky prevodu obsahujú monetárnu čiastku zmienenej elektronickej reprezentácie peňazí, a kde zmienené kroky zmieneného prvého klienta

odrávajúceho overenie určujúce rozdelenie zmienených monetárnych čiastok medzi úver a obeživo.

5. Metóda prevodu elektronických poukážok medzi elektronickými na procesore založenými modulmi, skladajúca sa z krokov:

vytvorenie šifrovaného bezpečného spojenia medzi elektronickým modulom platcu a elektronickým modulom príjemca;

vytvorenie prevodnej elektronickej poukážky pomocou pridania prevodového záznamu k elektronickej poukážke uchováwanej v zmienenom prevodnom elektronickej module, kde zmienený prevodný záznam ukazuje, či všetky alebo niektoré časti monetárnej čiastky zmienenej elektronickej poukážky sú práve prevádzané;

prevod zmienenej prevodovej elektronickej poukážky od zmieneného elektronickej modulu platcu ku zmienenému elektronickej modulu príjemcu: a

kde zmienený záznam o prevode obsahuje poradové číslo, ktoré odlišuje zmienenú prevodnú elektronickej poukážku od iných prevodných elektronickej poukážok z daného prevodného elektronickej modulu.

6. Spôsob pre prihlásenie elektronickej modulu do elektronickej monetárnej systémovej siete so sieťovým serverom, ktorý pripojí zmienený elektronickej modul k bezpečnostnému serveru, skladajúci sa z krokov, v ktorých:

zmienený elektronickej modul posiela certifikát danému sieťovému serveru;

zmienený sieťový server generuje náhodný kľúč a náhodné overovacie číslo, a posiela zašifrovanú správu vrátane zmieneného certifikátu, zmieneného náhodného kľúča, a zmieneného náhodného overovacieho čísla ku zmienenému

bezpečnostnému serveru;

zmienený bezpečnostný server dešifruje zmienenú zašifrovanú správu, ukladá zmienený náhodný kľúč a náhodné overovacie číslo, a overí platnosť zmieneného certifikátu;

zmienený bezpečnostný server vytvára bezpečné komunikačné spojenie so zmieneným elektronickým modulom;

zmienený bezpečnostný server posíla zmienenému elektronickému modulu aktualizovanú bezpečnostnú informáciu, ktorá je digitálne označená šifrovacím kľúčom zmieneného bezpečnostného serveru;

zmienený elektronický modul overuje platnosť zmienenej digitálne označenej aktualizovanej bezpečnostnej informácie, a aktualizuje uloženú bezpečnostnú informáciu so zmienenou aktualizovanou bezpečnostnou informáciou;

zmienený bezpečnostný server posíla zmienený náhodný kľúč a zmienené náhodné overovacie číslo zmienenému elektronickému modulu, a ukončí zmienené bezpečné komunikačné spojenie;

zmienený elektronický modul vytvára správu pre miesto určenia zašifrovaním zmieneného náhodného overovacieho čísla a miesta určenia so zmieneným náhodným kľúčom, a posíla zmienenú správu pre miesto určenia do zmieneného sieťového serveru;

zmienený sieťový server dešifruje zmienenú správu a overuje zmienené náhodné overovacie číslo; a

zmienený sieťový server nadväzuje spojenie so zmieneným miestom určenia.

7. Spôsob podľa nároku 6, v y z n a č u j ú c i s a t ý m, že zmienený elektronický modul je prevodný modul, modul zákazníckych služieb, modul generujúci

peniaze, alebo modul bankomatu.

8. Spôsob podľa nároku 6, ďalej sa skladajúci z krokov, v ktorých:
zmienený elektronický modul posiela zmienenému bezpečnostnému serveru svoju informáciu o čase a dátume zmienenému bezpečnostnému serveru;
zmienený bezpečnostný server kontroluje zmienenú informáciu o čase a dátume, aby zistil či je mimo prijateľný vopred určený parameter; a
zmienený bezpečnostný server, v prípadoch, keď zmienená informácia o čase a dátume je mimo zmienený prijateľný vopred definovaný parameter, pošle zmienenému elektronickému modulu nový dátum a čas za účelom synchronizácie zmieneného elektronického modulu.
9. Spôsob podľa nároku 6, v y z n a č u j ú c i s a t ý m, že zmienená zašifrovaná správa medzi zmieneným sieťovým serverom a zmieneným bezpečnostným serverom je opatrená symetrickým kľúčom uloženým v zmienenom sieťovom servere a v zmienenom bezpečnostnom servere.
10. Spôsob podľa nároku 6, v y z n a č u j ú c i s a t ý m, že zmienená aktualizovaná bezpečnostná informácia obsahuje aktualizovaný zoznam neplatných elektronických modulov a identifikačných čísiel bezpečnostných serverov, aktualizovaný zoznam verejných kľúčov a aktualizovanú dĺžku kľúča.
11. Spôsob podľa nároku 6, v y z n a č u j ú c i s a t ý m, že zmienený krokom zmieneného bezpečnostného serveru, v ktorom sa nadväzuje ustavujúce bezpečné komunikačné spojenie so zmieneným elektronickým modulom obsahuje výmenný protokol verejného kľúča

k zabezpečeniu kľúča spojenia spoločného zmienenému bezpečnostnému serveru a zmienenému elektronickému modulu.

12. Postup podľa nároku 6, v y z n a č u j ú c i s a t ý m, že ďalej obsahuje krok zmieneného bezpečnostného serveru znovu overujúceho zmienený certifikát.
13. Postup podľa nároku 12, vyznačujúci sa tým, že zmienený krok opätovného overenia sa vyskytuje v reakcii na zaslanie novej správy zmieneného bezpečnostného serveru so žiadosťou opätovného overenia ku zmienenému elektronickému modulu.
14. Postup podľa nároku 12, v y z n a č u j ú c i s a t ý m, že zmienený certifikát obsahuje expiračný čas, a ešte tým, že zmienený krok opätovného overenia sa vzniká ako odpoveď zmienenému elektronickému modulu, ktorý určuje, že zmienený certifikát má uplynulú expiračnú dobu.
15. Monetárny prevodný systém, ktorý je založený na elektronickom module a obsahuje:
 - primárny bezpečnostný server;
 - rad sekundárnych bezpečnostných serverov, z ktorých každý má jedinečný certifikát bezpečnostného serveru digitálne označený zmieneným primárnym bezpečnostným serverom;
 - rad elektronických modulov odolných proti zneužitiu, z ktorých každý má jedinečný modulový certifikát, ktorý je digitálne označený jedným zo zmienených sekundárnych bezpečnostných serverov, pamäť uchovávajúcú elektronické reprezentácie peňazí a procesor prispôsobený poskytovať šifrovaný bezpečný kanál pre

prevádzanie a prijímanie zmienených elektronických reprezentácií peňazí, a
v y z n a č u j ú c i s a t ý m, že zmienené certifikáty bezpečnostných serverov sú legalizované potom, čo sa zmienený elektronický server komunikuje so zmieneným elektronickým modulom alebo zmieneným primárnym bezpečnostným serverom, a ďalej tým, že zmienený certifikát modulu je legalizovaný potom, čo zmienený elektronický modul komunikuje s iným zo zmienených elektronických modulov alebo so zmienenými bezpečnostnými servermi.

16. Systém podľa nároku 15, v y z n a č u j ú c i s a t ý m, že zmienené modulové certifikáty a zmienené certifikáty bezpečnostných serverov sú opatrené respiračným časom a kde zmienené elektronické moduly sú usporiadané tak, aby neuskutočňovali prevody s inými elektronickými modulmi alebo sekundárnymi bezpečnostnými servermi s uplynulou expiračnou dobou certifikátov.
17. Systém podľa nároku 15, v y z n a č u j ú c i s a t ý m, že každý zo zmieneného radu elektronických modulov, zmienených primárných bezpečnostných serverov a každý zo zmieneného radu sekundárných bezpečnostných serverov má jedinečný identifikátor popisujúci typ serveru alebo typ elektronického modulu.
18. Systém podľa nároku 17, v y z n a č u j ú c i s a t ý m, že zmienený typ elektronického modulu obsahuje prevodný modul, modul zákazníckych služieb, modul generujúci peniaze, a modul bankomatu, a kde zmienený typ serveru obsahuje zmienený primárny bezpečnostný server a zmienené bezpečnostné sekundárne servery.

19. Systém podľa nároku 17, v y z n a č u j ú c i s a t ý m, že každý zmienený typ serveru a každý zmienený typ elektronického modulu je pridružený k jedinečnému rozsahu typovej premennej, kde každý zmienený jedinečný identifikátor zobrazí v hodnote zmienenej typovej premennej vo vnútri zmieneného jedinečného rozsahu priradeného ku zmienenému typu serveru alebo typu elektronického modulu podľa mechanizmu zobrazenia bezpečne uloženom v každom zmienenom elektronickom module, každom zmienenom sekundárnom servere a zmienenom primárnom servere.
20. Systém podľa nároku 19, v y z n a č u j ú c i s a t ý m, že každý zmienený jedinečný identifikátor je jedinečná celočíselová hodnota zmenšená o vopred určené prvočíslo, a kde zmienená hodnota zmienenej typovej premennej je generovaná podľa umocnenia primitívnej odmocniny zmieneného prvočísla na zmienený jedinečný identifikátor, ktorý je zlomkom zmieneného vopred určeného prvočísla a aritmetického modulu, a kde každý zo zmieneného radu elektronických modulov, zmienených primárnych bezpečnostných serverov a každý zo zmieneného radu sekundárnych bezpečnostných serverov má bezpečne uloženú zmienenú odmocninu a zmienené prvočíslo.
21. Systém podľa nároku 15, v y z n a č u j ú c i s a t ý m, že zmienený primárny bezpečnostný server udržiava zoznam zmienených jedinečných identifikátorov pre neplatné elektronické moduly a neplatné sekundárne bezpečnostné servery, kde zmienené zoznamy sú poskytované zmieneným sekundárnym bezpečnostným serverom a zmieneným elektronickým modulom.

22. Systém podľa nároku 15, v y z n a č u j ú c i s a t ý m, že zmienený certifikát bezpečnostného serveru je zašifrovaný zmieneným primárnym bezpečnostným serverom a zmienený certifikát modulu, je zašifrovaný zmieneným sekundárnym bezpečnostným serverom.
23. Systém podľa nároku 22, v y z n a č u j ú c i s a t ý m, že zmienený certifikát bezpečnostného serveru obsahuje:
prvé a druhé dátové pole zašifrované pomocou súkromného kľúča zmieneného primárneho bezpečnostného serveru, kde zmienené prvé dátové pole obsahuje jedinečný identifikátor zmieneného sekundárneho bezpečnostného serveru, verejný kľúč zmieneného bezpečnostného serveru, a expiračnú dobu pre zmieneného certifikátu serveru, a kde zmienené druhé dátové pole obsahuje zmienené prvé dátové polia označené zmieneným primárnym bezpečnostným serverom; a
tretie dátové pole, ktoré obsahuje jedinečný identifikátor zmieneného primárneho bezpečnostného serveru.
24. Systém podľa nároku 23, v y z n a č u j ú c i s a t ý m, že zmienený jedinečný identifikátor zmieneného primárneho bezpečnostného serveru je zašifrovaný.
25. Systém podľa nároku 22, v y z n a č u j ú c i s a t ý m, že zmienený modulový certifikát obsahuje:
prvé a druhé dátové pole zašifrované pomocou súkromného kľúča sekundárneho bezpečnostného serveru, a kde prvé dátové pole obsahuje jedinečný identifikátor zmieneného elektrického modulu, verejný kľúč zmieneného elektrického modulu, a dátum expirácie zmieneného modulového overenia, a ďalej sa vyznačujúci tým, že

zmienené druhé dátové pole obsahuje zmienené prvé dátové pole digitálne označené zmieneným sekundárnym bezpečnostným serverom; a
tretie dátové pole obsahujúce zmienený certifikát bezpečnostného serveru.

26. Systém podľa nároku 15, v y z n a č u j ú c i s a t ý m, že primárny bezpečnostný server a zmienené sekundárne bezpečnostné servery majú spoločný symetrický kľúč, ktorý je periodicky menený pomocou zmeny verejného kľúča.
27. Systém podľa nároku 15, v y z n a u č u j ú c i s a t ý m, že zmienený primárny bezpečnostný server selektívne ovláda globálne opätovné overenie zmienených bezpečnostných certifikátov bezpečnostných serverov a zmienených modulových certifikátov.
28. Spôsob platby používajúci prvý peňažný modul k prevodu elektronických reprezentácií peňazí na druhý peňažný modul, skladajúci sa z krokov:
vytvorenie šifrovaného bezpečného spojenia medzi zmieneným prvým peňažným modulom so zmieneným druhým peňažným modulom, kde zmienený prvý a druhý peňažný modul sú elektronické moduly, ktoré sa nedajú zneužiť.
zmienený prvý peňažný modul prevádzajúci elektronické reprezentácie peňazí do zmieneného druhého peňažného modulu cestou zmieneného šifrovaného bezpečného spojenia;
zmienený druhý peňažný modul posiela správu "pripravený ku splneniu záväzku prevodu" zmienenému prvému peňažnému modulu;
zmienený prvý peňažný modul posielajúci vyrozumienie zmienenému druhému peňažnému modulu ako odpoveď na

správu "pripravený ku splneniu záväzku prevodu", a potom uskutoční zmienený prevod elektronických peňazí tak, že zmienený prvý peňažný modul už nemôže zrušiť zmienený prevod elektronických peňazí navrátením do pôvodného stavu; a

zmienený druhý peňažný modul, po príjme zmieneného vyrozumenia, odovzdá (ukončí) tak, že zmienený druhý peňažný modul už nemôže zrušiť zmienený prevod elektronických peňazí navrátením modulu do jeho pôvodného stavu.

29. Spôsob platby podľa nároku 28, v y z n a č u j ú c i s a t ý m, že každý zmienený peňažný modul môže prerušiť pred realizáciou zmieneného prevodu ho prerušiť pomocou podprogramu prerušenie v zmienených peňažných moduloch.

30. Spôsob platby podľa nároku 28, v y z n a č u j ú c i s a t ý m, že zmienené podprogramy prerušenia obsahujú tieto uskutočnené kroky peňažného modulu:

kontrolu, či zmienená správa "pripravený ku splneniu záväzku prevodu" bola odoslaná;

tam, kde zmienená správa "pripravený ku splneniu záväzku prevodu" bola odoslaná, zaznamenanie informácie spojené so zmienenou elektronickou reprezentáciou peňazí prijatých od zmieneného prvého peňažného modulu, vyznačujúceho sa tým, že zmienená informácia spojená so zmienenou elektronickou reprezentáciou peňazí môže byť použitá k reklamácii stratených elektronických peňazí.

31. Spôsob platby zodpovedajúci nároku 30, vyznačujúci sa tým, že zmienený podprogram prerušenia obsahuje kroky vykonané peňažným modulom:

poslanie správy k iným zmieneným peňažným modulom,

o tom, že zmienený prevod elektronických peňazí nemôže byť dokončený; a kde zmienené iné peňažné moduly v odpovedi na zmienenú správu vráti späť svojej zmeny týkajúcej sa zmieneného prevodu elektronických peňazí a zaznamenajú, že zmienený prevod elektronický prevod peňazí je prerušený.

32. Spôsob platby podľa nároku 31, ktorý ďalej obsahuje v prípadoch, keď zmienený iný peňažný modul je prevodný modul používaný druhým klientom, krok, ktorým je zaslaná správa zmienenému druhému klientovi, že zmienený elektronický prevod je prerušený.
33. Spôsob platby podľa nároku 31, ktorý ďalej obsahuje v prípadoch, keď zmienený iný zo zmienených peňažných modulov je modul bankomatu spojený s bankou, krok, ktorým je informovaná zmienená banka o tom, aby zmenila smer účtovných prevodov vykonávaných pre zmienený elektronický prevod.
34. Spôsob platby podľa nároku 30, ďalej obsahujúci krok zmieneného prvého peňažného modulu navracujúci späť zmeny a zaznamenávajúci, že tento zmienený prevod bol prerušený.
35. Spôsob platby podľa nároku 30, ďalej obsahujúci v prípadoch, keď zmienený peňažný modul je prevodný peňažný modul používaný klientom a zmienená správa "pripravený ku splneniu záväzku prevodu" nebola odoslaná, krok, ktorý posiela zmienenému klientovi správu, že zmienený elektronický prevod je prerušený.
36. Spôsob platby podľa nároku 30 ďalej obsahujúci v prípadoch, keď zmienený peňažný modul je prevodný

peňažný modul používaný klientom a zmienená správa "pripravený ku splneniu záväzku prevodu" bola poslaná, krok, v ktorom je poslaná zmienenému klientovi správa, že zmienený elektronický prevod je prerušený a e sa objavila chyba prevodu peňazí.

37. Spôsob platby podľa nároku 30, ďalej obsahujúci v prípadoch, keď zmienený peňažný modul je modul bankomatu spojený s bankou a zmienená správa "pripravený ku splneniu záväzku prevodu" bola odoslaná, krok informujúci zmienenú banku o tom, aby zmenila smer účtovných prevodov vykonávaných pre zmienený elektronický prevod.
38. Spôsob nadviazania spojenia prvého a druhého zariadenia, kde prvé a druhé zariadenie sú elektronické moduly alebo server elektronického monetárneho systému, ktorý sa skladá z krokov, v ktorých:
 - a) zmienené druhé zariadenie prijíma certifikát od zmieneného prvého zariadenia;
 - b) zmienené druhé zariadenie overuje platnosť zmieneného certifikátu zmieneného zariadenia;
 - c) zmienené druhé zariadenie posiela správu zmienenému prvému zariadeniu, zmienená správa obsahuje časť zašifrovanú pomocou verejného kľúča zmieneného prvého zariadenia, a certifikát zmieneného druhého zariadenia, zmienená časť obsahuje prvé náhodné číslo, časovú informáciu druhého zariadenia, a prvú overovaciu správu;
 - d) zmienené prvé zariadenie overuje platnosť zmieneného certifikátu zmieneného druhého zariadenia, a určuje, či zmienená časová informácia druhého zariadenia je vo vnútri vopred určeného rozpätia časovej informácie prvého zariadenia;

- e) zmienené prvé zariadenie posiela zmienenému druhému zariadeniu druhú správu zašifrovanú pomocou verejného kľúča zmieneného druhého zariadenia; zmienená správa obsahuje druhé náhodné číslo generované zmieneným prvým zariadením, druhú overovaciu správu vytvorenú zmieneným prvým zariadením, zmienenú overovaciu správu vytvorenú zmieneným druhým zariadením, a zmienenú časovú informáciu prvého zariadenia;
- f) zmienené prvé zariadenie vytvára spojovací kľúč z kombinácie zmieneného prvého náhodného čísla a zmieneného druhého náhodného čísla;
- g) zmienené druhé zariadenie overuje zmienenú prvú overovaciu správu, vytvára zmienený spojovací kľúč zo zmienenej kombinácie zmieneného prvého a zmieneného druhého náhodného čísla, a určuje, či zmienená časová informácia je vo vnútri vopred určeného rozpätia od časovej informácie druhého zariadenia.
- h) zmienené druhé zariadenie posiela zmienenému zariadeniu vyrozumenie zašifrované zmieneným spojovacím kľúčom, zmienené vyrozumenie obsahuje zmienenú druhú overovaciu správu; a
- i) zmienené prvé zariadenie dešifruje zmienené vyrozumenie a overuje zmienenú druhú overovaciu správu.

39. Metóda podľa nároku 38, v y z n a č u j ú c a s a t ý m, že pre prípady keď zmienené prvé zariadenie je pripojené k elektronickému monetárnemu systému so sieťovým serverom, krok a) obsahuje kroky zmieneného prvého zariadenia posielajúceho zmienenému sieťovému serveru správu obsahujúceho zmienený certifikát zmieneného prvého zariadenia zašifrovanú pomocou symetrického kľúča, a zmienený sieťový server dešifrujúci zmienenú správu a posielajúci zmienený certifikát zmieneného prvého zariadenia ku zmienenému

druhému zariadeniu.

40. Spôsob podľa nároku 38, v y z n a č u j ú c i s a t ý m, že každý certifikát obsahuje jedinečný identifikátor, ktorý je jedinečný pre každé zariadenie, ďalej obsahuje kroky zmieneného druhého zariadenia, ktoré určujú, či je jedinečný identifikátor zmieneného prvého zariadenia obsiahnutý v prvom zozname uchovávanom v zmienenom druhom zariadení, a zmienené prvé zariadenie určujúce, či jedinečný identifikátor zmieneného druhého zariadenia je obsiahnutý v druhom zozname uchovávanom vo zmienenom prvom zariadení, pričom prvý a druhý zoznam sú zoznamy zmienených jedinečných identifikátorov pre neplatné zariadenie.
41. Spôsob podľa nároku 40, v y z n a č u j ú c i s a t ý m, že každé zariadenie je jedným z radu typov, a pritom každý zo zmienených typov je spojený s jedinečným rozsahom typovej premennej, a kde zmienený jedinečný identifikátor daného zariadenia sa zobrazuje v hodnote zmienenej typovej premennej vo vnútri zmieneného jedinečného rozsahu priradeného zmienenému typu zmieneného daného zariadenia podľa zobrazovacieho mechanizmu bezpečne uloženého v každom zmienenom zariadení, a kde krok (b) zahrňuje kroky zobrazenia zmieneného jedinečného identifikátora zmieneného prvého zariadenia v premennej prvého typu zariadenia, a ktorý určuje či zmienená premena prvého typu zariadenia zodpovedá očakávanému typu zmieneného prvého zariadenia, a kde krok (d) zahrňuje kroky zobrazenia zmieneného jedinečného identifikátora, a ktorý určuje, či zmienená premenná druhého typu zariadenia zodpovedá očakávanému typu zmieneného druhého zariadenia.

42. Spôsob prevodu elektronických poukážok vopred určenej celkovej monetárnej hodnoty od peňažného modulu platcu na peňažný modul príjemcu, v y z n a č u j ú c i s a t ý m, že zmienený spôsob sa skladá z krokov, v ktorých:
- a) zmienený peňažný modul platcu vyberie jednu alebo viac elektronických poukážok, z ktorých poskytne zmienenú vopred určenú celkovú monetárnu hodnotu;
 - b) zmienený peňažný modul platcu vytvorí jednu alebo viac elektronických prevodných poukážok pomocou pridania zodpovedajúceho prevodného záznamu a digitálneho podpisu zmieneného peňažného modulu platcu ku každej jednej alebo viac zmienenej(ých) poukážok, a kde pre každú zmienenú jednu či viac prevodných poukážok zmienený individuálny záznam ukazuje, či je prevádzaná celá alebo nejaká časť monetárnej hodnoty zmienenej jednej či viacerých elektronických poukážok;
 - c) zmienený peňažný modul platcu posielá zmienenú jednu alebo viac prevodných elektronických poukážok do zmieneného peňažného modulu príjemcu;
 - d) zmienený modul príjemcu overuje platnosť zmienenej jednej či viac elektronických poukážok;
 - e) zmienený peňažný modul príjemcu zachová po overení zmienenú jednu či viac prevodných elektronických poukážok; zmienený adresár poukážok obsahuje všetky elektronické poukážky vlastnené zmieneným peňažným modulom príjemcu a kde peňažné moduly platcu i príjemcu ukladajú do záznamu o poukážkach informáciu obsahujúcu základnú informáciu o poukážke záznamy o prenose pre každú zo zmienených jednej alebo viacerých elektronických poukážok a kde krok d) obsahuje pre každú prevodnú poukážku zo zmienených jednej alebo viacerých prevodných poukážok kroky kontrolujúce

základnú informáciu o poukážke v zmienenom adresári poukážok a zmienený záznam o prevode, či zodpovedajú zmienenej prevodnej poukážke a vytvára strom prevodu poukážok pre identifikované súhlasy a kontroly duplikátov.

43. Spôsob nároku 42, v y z n a č u j ú c i s a t ý m, že že zmienený prevodný záznam obsahuje sekvenčné identifikačné číslo, u ktorého pre každú zo zmienených jednej alebo viacerých elektronických poukážok zmienené sekvenčné identifikačné číslo odlišuje každú od toho vytvorenú prevodnú elektronickú poukážku.
44. Spôsob podľa nároku 42, v y z n a č u j ú c i s a t ý m, že krok d), pre každú prevodnú elektronickú poukážku zo zmienenej jednej alebo viacerých prevodných elektronických poukážok, obsahuje kroky kontrolujúce prevodný záznam a všetky ďalšie prevodné záznamy pripojené iným peňažným modulom platcu, aby sa, potvrdilo že v každom prevode bola prevedená monetárna čiastka, ktorá neprevyšuje monetárnu hodnotu prevedenú v bezprostredne predchádzajúcom prevode.
45. Spôsob podľa nároku 42, v y z n a č u j ú c i s a t ý m, že každá prevodná elektronická poukážka zo zmienenej jednej alebo viacerých prevodných elektronických poukážok obsahuje digitálny podpis a certifikát každého peňažného modulu platcu za celú dobu prevodu zmienenej elektronickej poukážky; pričom krok d) ďalej obsahuje kroky overujúce platnosť digitálneho podpisu a certifikátu.
46. Spôsob podľa nároku 42, v y z n a č u j ú c i s a t ý m, že každá prevodná elektronická poukážka zo

zmienenej jednej alebo viacerých prevodných elektronických poukážok obsahuje dátum expirácie; a ak zmienený peňažný modul príjemcu je prevodný peňažný modul, potom obsahuje krok d) zahrňujúci krok zmieneného peňažného modulu príjemcu, v ktorom sa overuje každý dátum expirácie elektronickej poukážky.

47. Spôsob podľa nároku 42, v y z n a č u j ú c i s a t ý m, že zmienená elektronická poukážka je elektronická reprezentácia hotovosti s dátumom expirácie a monetárnou hodnotou; a kde krok a) obsahuje krok:
 - a) zmieneného peňažného modulu postupujúceho, ktorý určuje všetky možné alternatívy pre poskytovanie vopred určenej monetárnej hodnoty a používa minimálny počet elektronických poukážok;
 - b) určujúci, ktorý súbor všetkých zmienených možných alternatív obsahuje najmenší počet prevodov; a
 - c) tam kde zmienený súbor obsahuje viac ako jeden prvok, vyberá prvok zmieneného súboru, ktorý obsahuje minimálny počet monetárnych-jednotkových-dní sčítaných pre všetky poukážky prvku, a kde monetárne-jednotkové-dni predstavujú súčin počtu dní zostávajúcich do vypršania expirácie elektronickej poukážky a zostatkové monetárne hodnoty elektronickej poukážky.
48. Spôsob podľa nároku 42, v y z n a č u j ú c i s a t ý m, že v kroku d) zmienený peňažný modul príjemcu overí, či zmienená prevádzaná vopred určená monetárna hodnota zodpovedá očakávanej hodnote.
49. Spôsob prevodu elektronických poukážok vopred určenej celkovej monetárnej hodnoty z peňažného modulu platcu

na peňažný modul príjemcu, ktorý sa skladá z krokov:

(a) v ktorom zmienený peňažný modul platcu vyberie jednu alebo viac elektronických poukážok, z ktorých poskytne zmienenú vopred určenú celkovú monetárnu hodnotu;

(b) v ktorom zmienený peňažný modul platcu vytvorí jednu alebo viac prevodných elektronických poukážok pripojením zodpovedajúceho prevodného záznamu a digitálneho podpisu zmieneného peňažného modulu platcu ku každej zmienenej jednej či viacerým elektronickým poukážkam, kde pre každú zmienenú jednu alebo viac elektronických prevodných poukážok zmienený zodpovedajúci prevodný záznam vyjadruje, či celý alebo nejaká časť monetárneho sumy zmienenej jednej alebo viacerých elektronických poukážok, sú prevádzané¹⁶;

(c) v ktorom zmienený peňažný modul platcu posielajú jednu alebo viac prevodných elektronických poukážok zmienenému peňažnému modulu príjemcu;

(d) v ktorom zmienený peňažný modul príjemcu overuje platnosť zmienenej jednej alebo viacerých prevodných elektronických poukážok;

(e) v ktorom zmienený peňažný modul príjemcu ukladá jednu alebo viac prevodných elektronických poukážok v adresári poukážok;

a kde každá prevodná elektronická poukážka zo zmienenej jednej či viacerých prevodných elektronických poukážok obsahuje digitálne podpisy a certifikáty každého peňažného modulu platcu za celú dobu prevodu zmienenej elektronickej poukážky; a každý zo zmienených certifikátov obsahuje jedinečný identifikátor určujúci pridružený peňažný modul platcu, a kde zmienený prevodný záznam obsahuje zmienený jedinečný identifikátor elektronického modulu príjemcu; a kde krok d) ďalej predstavuje krok v ktorom sa kontroluje,

či zmienený jedinečný identifikátor zmieneného prevodného záznamu zodpovedá zmienenému jedinečnému identifikátoru v zmienenom certifikáte pre každý nasledujúci prevod v celej dobe prevodu zmienenej elektronickej poukážky.

50. Spôsob prevodu elektronických poukážok vopred určenej monetárnej hodnoty z peňažného modulu platcu na peňažný modul príjemcu, ktorý sa skladá z krokov v ktorých:
- a) zmienený peňažný modul platcu vyberá jednu alebo viac elektronických poukážok, z ktorých získa zmienenú vopred určenú celkovú monetárnu hodnotu;
 - (b) zmenený peňažný modul platcu vytvára jednu alebo viac prevodných elektronických poukážok pomocou pripojenia príslušného prevodného záznamu a digitálneho podpisu zmieneného peňažného modulu platcu ku každej zo zmienených jednej či viacerých prevodných elektronických poukážok, kde pre každú zmienenú jednu alebo viac prevodných elektronických poukážok zmienený príslušný prevodný záznam ukazuje, či je predvádzaná celá či len časť monetárnej čiastky zmienenej jednej alebo viacerých elektronických poukážok;
 - (c) zmienený peňažný modul platcu posielá jednu alebo viacej prevodných elektronických poukážok zmienenému peňažnému modulu príjemcu;
 - (d) zmienený peňažný modul príjemcu overuje platnosť zmienenej jednej alebo viacerých prevodných elektronických poukážok;
 - (e) zmienený peňažný modul príjemcu ukladá po overení platnosti jednu alebo viac prevodných elektronických poukážok v adresári poukážok:
- kde každá prevodná poukážka zo zmienenej jednej alebo viacej prevodných elektronických poukážok obsahuje jedinečné identifikátory všetkých peňažných modulov

príjemcu po celú dobu prevodu zmienenej elektronickej poukážky: a kde pre prípady, že zmienený prevodný peňažný modul príjemcu je prevodný peňažný modul, ďalej obsahuje krok d) predstavujúci kontrolný krok, ktorý zisťuje či, každý zmienený jedinečný identifikátor je na zozname jedinečných identifikátorov pre neplatné peňažné moduly, ktorý je uložený vo zmienenom peňažnom module príjemcu.

51. Spôsob, zmeny elektronickej reprezentácie prvej cudzej meny, uchovávané v prvom prevodnom module, za elektronicnú reprezentáciu druhej cudzej meny, uchovávané v druhom prevodnom module pre prvého klienta, ktorý sa skladá z krokov v ktorých:
- (a) sa vytvorí šifrované bezpečné spojenie medzi zmieneným prvým prevodným modulom a zmieneným druhým prevodným modulom;
 - (b) zmienený klient vyberá, pomocou zmieneného prvého prevodného modulu, prvú čiastku zmienenej prvej cudzej meny, ktorá má byť predaná;
 - (c) kontroluje, či prvý prevodný modul má dostatočné fondy;
 - (d) zmienený prvý prevodný modul posiela zmienenú prvú čiastku zmienenému druhému prevodnému modulu, pomocou zmieneného šifrovaného bezpečného spojenia;
 - (e) zmienený druhý prevodný modul žiada svojho vlastníka, aby vybral výmenný kurz alebo druhú čiastku v zmienenej druhej mene;
 - (f) sa kontroluje, či zmienený druhý prevodný modul má dostatočné fondy;
 - (g) zmienený druhý prevodný modul posiela správu obsahujúcu zmienenú druhú čiastku alebo zmienený výmenný kurz zmienenému prvému prevodnému modulu zmieneným šifrovaným bezpečným spojením;

- (h) zmienený prvý klient potvrdí zmienenú druhú čiastku alebo zmienený výmenný kurz;
- (i) zmienený prvý prevodný modul posiela zmienenú elektronickú reprezentáciu prvej cudzej meny zmienenému druhému prevodnému modulu, vo výške zmienenej prvej čiastky zmieneným šifrovaným bezpečným spojením;
- (j) zmienený druhý prevodný modul posiela zmienenú elektronickú reprezentáciu zmienenej druhej cudzej meny zmienenému prvému prevodnému modulu vo výške zmienenej druhej čiastky, zmieneným šifrovaným bezpečným spojením; a
- (k) zmienený prvý prevodný modul realizuje prevod zmienenej prvej cudzej meny ku zmienenému druhému prevodnému modulu a zmienený druhý prevodný modul prijíma zmienenú cudziu menu od zmieneného prvého prevodného modulu, a zmienený druhý prevodný modul realizuje prevod zmienenej druhej cudzej meny ku zmienenému prvému prevodnému modulu, a zmienený prvý prevodný modul prijíma zmienenú druhú cudziu menu od zmieneného druhého prevodného modulu, v poradí, ktoré nie predvídateľné.

52. Spôsob zodpovedajúci nároku 51, v y z n a č u j ú c i s a t ý m, že krok k) sa skladá z krokov, v ktorých:
- a) zmienený prvý prevodný modul a zmienený druhý prevodný modul zdieľajú spoločnú náhodnú binárnu hodnotu, majúcu buď prvú hodnotu alebo druhú hodnotu;
 - (b) zmienený prvý prevodný modul sa podmienene prihlasuje k prevodu buď zmieneného prevodu zmienenej prvej cudzej meny zmienenému druhému prevodnému modulu alebo zmienené prijatie zmienenej druhej cudzej meny od zmieneného druhého prevodného modulu, pričom zmienená spoločná náhodná binárna hodnota má v prvom prípade zmienenú prvú hodnotu a v druhom prípade zmienenú druhú

hodnotu, takže spätný prevod môže nastať;

(c) zmienený prvý prevodný peňažný modul posiela správu zmienenému druhému prevodnému modulu, ktorá oznamuje, že zmienený prvý prevodný modul ukončil podmienené prihlásenie prevodu

(d) zmienený druhý prevodný modul v reakcii na zmienenú správu sa podmienene prihlasuje k prevodu buď zmieneného príjmu zmienenej prvej cudzej meny od zmieneného prvého prevodného modulu alebo zmieneného prevodu zmienenej druhej cudzej meny ku zmienenému prvému prevodnému modulu, pričom zmienená spoločná náhodná binárna hodnota sa rovná v prvom prípade zmienenej prvej hodnote alebo v druhom prípade druhej hodnote, takže spätný prevod môže nastať.

(e) zmienený druhý prevodný peňažný modul, v tých prípadoch, keď zmienená hodnota spoločného náhodného čísla sa rovná prvej hodnote, posiela správu začni realizáciu zmienenému prvému prevodnému modulu

(f) zmienený prvý prevodný modul v reakcii na zmienenú správu začni realizáciu priradí podmienenému prihláseniu prevodu štatút bezpodmienečného prihlásenia a zahájí protokol o realizáciu, kde zmienený prvý prevodný modul sa zaväzuje k nevybavenému prevodu takže zmienený prvý prevodný modul už nemôže prerušiť zmienený prevod návratom do pôvodného stavu a kde zmienený druhý peňažný modul sa realizuje zmienený prevod druhej cudzej meny zmienený príjem prvej cudzej meny prihlásením zmieneného prevodu a príjmu, takže zmienený druhý peňažný modul už nemôže prerušiť zmenu cudzej meny návratom do pôvodného stavu; a

(g) zmienený druhý prevodný modul, kde zmienená spoločná hodnota náhodného čísla sa rovná druhej hodnote tým, že priradenie podmienenému prihláseniu atribút nepodmieneného prihlásenia a zahájí realizačný

protokol, kde zmienený druhý prevodný modul realizuje nevybavený prevod, aby zmienený druhý prevodný modul nemohol už prerušiť zmienený prevod návratom do pôvodného stavu a kde zmienený prvý prevodný modul sa sa zaväzuje uskutočniť zmienený prevod prvej cudzej meny a príjem druhej cudzej meny aby zmienený prvý peňažný modul už nemohol prerušiť zmienenú zmenu cudzej meny návratom do pôvodného stavu.

53. Spôsob podľa nároku 52, v y z n a č u j ú c i s a t ý m, že zmienené spoločné náhodné číslo je generované ako spojovací kľúč v priebehu zmieneného kroku vytvárania šifrovaného bezpečného spojenia.
54. Spôsob podľa nároku 51, v y z n a č u j ú c i s a t ý m, že zmienený realizačný protokol zahájený daným peňažným modulom pre akýkoľvek nevybavený peňažný prevod voči inému peňažnému modulu sa skladá z krokov, v ktorých:
zmienený daný modul posiela správu "pripravený ku splneniu záväzku prevodu" zmienenému inému peňažnému modulu;
zmienený iný peňažný modul posiela vyrozumienie zmienenému danému peňažnému modulu ako odpoveď na zmienenú správu "pripravený ku splneniu záväzku prevodu";
zmienený daný peňažný modul realizujúci prihlásením akýkoľvek zmienený nevybavený peňažný prevod tak, aby zmienený daný peňažný modul už nemohol zrušiť akýkoľvek zmienený nevybavený peňažný prevod návratom do pôvodného stavu; a
zmienený iný peňažný modul realizujúci prihlásením akýkoľvek zmienený nevybavený peňažný prevod tak, aby zmienený iný peňažný modul nemôže už nemohol zrušiť

akýkoľvek zmienený nevybavený peňažný peňažný prevod návratom do pôvodného stavu.

55. Spôsob podľa nároku 51, v y z n a č u j ú c i s a t ý m, že v kroku b) zmienený klient vyberie zmienenú prvú čiastku zmienenej prvej cudzej meny, aby bola predaná podľa typu poukážky??
56. Systém pre prevod elektronických poukážok medzi elektronickými modulmi riadenými procesorom, kde každý procesorový elektronický modul je jedným z radu modulových typov a ktorý obsahuje:
procesorové elektronické moduly, kde každý procesorový elektronický modul ukladá jedinečný modulový identifikátor, a každý je schopný vytvoriť šifrovaný bezpečný kanál a prevádzať a prijímať elektronické poukážky zmieneným šifrovaným kanálom, a kde každý zmienený elektronický modul má pamäť pre uchovávanie zmienených elektronických poukážok;
kde každý zo zmieneného radu modulových typov je spojený s jedinečným rozsahom modulových typových premenných, a ďalej kde každý jedinečný modulový identifikátor zobrazuje v hodnote zmienenej typovej premennej vo vnútri zmieneného jedinečného rozsahu priradeného ku zmienenému modulovému typu mechanizmu zobrazenie bezpečne uloženého v každom zmienenom elektronickom module.
57. Systém podľa nároku 56, v y z n a č u j ú c i s a t ý m, že každý zmienený jedinečný identifikátor je jedinečná celočíselová hodnota menšia ako vopred určené prvočíslo, a kde zmienená hodnota zmienenej typovej premennej je generovaná podľa umocnenia primitívnej odmocniny zmieneného prvočísla na zmienený jedinečný

identifikátor modulárnej aritmetiky pre vopred určené prvočíslo, a kde každý zo zmieneného radu elektronických modulov, zmienený primárny bezpečnostný server a každý zo zmieneného radu sekundárnych bezpečnostných serverov má bezpečne uloženú zmienenú odmocninu a zmienené prvočíslo.

58. Spôsob, pri ktorom klient používa prevodný modul k aktualizácii úverovej poukážky pre zmienený klientov bankový účet vo vydávajúcej banke, ktorá má modul bankomatu, modul generátora peňazí, a účtovný systém zapojený na počítač (on-line), a zmienený spôsob sa skladá z krokov, v ktorých:
- (a) zmienený klient vyberá pomocou zmieneného prevodného modulu bankový účet, z ktorého bude aktualizovaná zmienená úverová poukážka a požadovaná čiastka určujúca požadovanú celkovú úverovú čiastku pre zmienenú úverovú poukážku;
 - (b) zmienený prevodný modul vytvorí prvý šifrované bezpečné spojenie so zmieneným modulom bankomatu;
 - (c) zmienený prevodný modul pošle správu so žiadosťou o úver ku zmienenému modulu bankomatu cestou zmieneného prvého šifrovaného bezpečného spojenia, kde zmienená správa s úverovou žiadosťou obsahuje úverovú aktualizovanú čiastku zodpovedajúcu čistej úverovej čiastke pre zmienenú úverovú poukážku a informáciu o bankovom účte zodpovedajúcu zmienenému bankovému účtu.
 - (d) kontroluje zmienenú informáciu o bankovom účte, aby sa overila jej platnosť;
 - (e) kontroluje úverové spojenie pridružené ku zmienenému bankovému účtu klienta, aby sa zistilo, či k poskytnutiu zmienenej požadovanej úverovej čiastky sú fondy dostatočné;

(f) v tých prípadoch, keď existujú súčasné úverové poukážky pre zmienený klientov bankový účet, zmienený prevodný modul posiela zmienenú súčasnú úverovú poukážku zmienenému modulu bankomatu;

(g) zmienený modul bankomatu vytvára druhé šifrované bezpečné spojenie so zmieneným modulom generátora peňazí;

(h) je aktualizované zmienené úverové spojenie pridružené ku zmienenému bankovému účtu podľa zmienenej požadovanej celkovej čiastky pre zmienenú úverovú poukážku;

(i) zmienený modul bankomatu posiela žiadosť o vytvorenie poukážky zmienenému modulu generátora peňazí, cestou zmieneného druhého šifrovaného bezpečného spojenia, kde zmienená žiadosť o vytvorenie poukážky obsahuje požadovanú poukážkovú hodnotu;

(j) zmienený modul generátora peňazí vytvára úverovú poukážku zmienenej požadovanej hodnoty;

(k) prevedenie zmienenej úverovej poukážky zmienenému modulu bankomatu cestou zmieneného druhého šifrovaného bezpečného spojenia;

(l) prevedenie zmienenej úverovej poukážky zmienenému prevodnému bankomatu cestou prvého šifrovaného bezpečného spojenia;

(m) sa záväzne potvrdí spojenie zmieneného prevodného modulu a zmieneného modulu bankomatu; a

(n) zmienený modul bankomatu sa záväzne prepojí s modulom generátora peňazí.

59. Spôsob aktualizácie úveru podľa nároku 58, v y z n a č u j ú c i s a t ý m, že v tých prípadoch, keď existuje zmienená úverová poukážka, potom v kroku (c) zmienená čistá úverová čiastka predstavuje rozdiel medzi zmienenou požadovanou celkovou čiastkou

a súčasnou úverovou čiastkou zmienenej súčasne úverovej poukážky.

60. Spôsob aktualizácie úveru podľa nároku 58, v y z n a č u j ú c i s a t ý m, že zmienená banková účtovná informácia obsahuje profil účtu, ktorý má číslo bankového účtu, ktoré je digitálne označené modulom zákazníckych služieb; kde zmienené kroky kontrolovania platnosti zmienenej bankovej účtovnej informácie obsahuje krok kontrolujúci zmienený digitálny podpis na zmienenom profile účtu s verejným kľúčom zmieneného modulu zákazníckych služieb.
61. Spôsob aktualizácie úveru podľa nároku 58, v y z n a č u j ú c i s a t ý m,, že krok f) ďalej obsahuje krok zmieneného prevodného modulu posielajúceho zmienenému modulu bankomatu ktorúkoľvek pokladničnú poukážku a ktorúkoľvek prevedenú úverovú poukážku uloženú vo zmienenom prevodnom module; krok f) je nasledovaný krokom zmieneného modulu bankomatu, ktorý aktualizuje zmienený on-line účtovný systém pripojený na centrálny počítač (on-line) podľa zmienených pokladničných poukážok a prevedených úverových poukážok; v kroku i) zmienená žiadosť o vytvorenie poukážky obsahuje požadovanú hodnotu pokladničnej poukážky zodpovedajúcej celkovej hodnote zmienenej prevedenej úverovej poukážky uchovanej v zmienenom prevodnom module; vydaný peňažný účet je úverovaný v zmienenom účtovnom systéme napojenom na centrálny počítač (on-line) hodnotou zmienenej vyžiadanej pokladničnej poukážky; krok j) obsahuje krok zmieneného modulu generátora vytvárajúceho pokladničnú poukážku bankovku zmienenej

požadovanej hodnoty pokladničnej poukážky;
krok k) obsahuje krok, prevádzajúci zmienenú pokladničnú poukážku zmieneného modulu bankomatu cestou zmieneného druhého šifrovaného bezpečného spojenia; a
krok l) obsahuje krok prevádzajúci zmienenú pokladničnú poukážku zmienenému prevodnému modulu cestou zmieneného prvého šifrovaného bezpečného spojenia.

62. Spôsob, ktorý umožňuje klientovi, pomocou modulu zákazníckych služieb pridruženého k hostiteľovi, ktorý má prístup k jednej i viacerým bankám, spojiť prevodný peňažný modul so zmieneným klientovým bankovým účtom klienta v banke, ktorá má modul bankomatu, modul generátora peňazí, a účtovný systém, pripojený na centrálny počítač (on-line) pritom tento spôsob sa skladá z krokov, v ktorých:
- (a) zmienený hostiteľ zmieneného modulu zákazníckych služieb získa prístup k bankovej informácii o účte zmieneného klienta v zmienenej jednej či viacej bankách v reakcii na prijatie identifikačnej informácie zmieneného klienta;
 - (b) je overená zmienená informácia o bankovom účte, a zmienený klient identifikuje svoj bankový účet zmienený pre spojenie so zmieneným prevodným peňažným modulom;
 - (c) je vytvorené spojenie medzi zmieneným prevodným peňažným modulom a zmieneným modulom zákazníckych služieb;
 - (d) zmienený modul zákazníckych služieb generuje účtovný profil pre zmienený klientov bankový účet;
 - (e) zmienený modul zákazníckych služieb posiela správu zmienenému prevodnému peňažnému modulu, a táto zmienená správa obsahuje zmienený účtovný profil a digitálny podpis zmieneného účtovného profilu označený súkromným

klúčom zmieneného modulu zákazníckych služieb;

(f) zmienený prevodný peňažný modul overí zmienený digitálny podpis;

(g) zmienený prevodný peňažný modul pripojí certifikát zmieneného modulu zákazníckych služieb ku zmienenému účtovnému profilu;

(h) zmienený prevodný peňažný modul uloží zmienený účtovný profil; a

(i) učiní záväzným spojenie zmieneného prevodného peňažného modulu a zmieneného modulu zákazníckych služieb.

63. Spôsob podľa nároku 62, v y z n a č u j ú c i s a t ý m, že krok f) ďalej obsahuje krok zmieneného klienta, v ktorom sa kontroluje profil účtu.

64. Spôsob podľa nároku 62, v y z n a č u j ú c i s a t ý m, že krok h) obsahuje kroky zmieneného prevodného peňažného modulu, ktorým zamieňa existujúci druhý profil účtu za zmienený bankový účet so zmieneným profilom účtu.

65. Spôsob pri ktorom klient pomocou modulu zákazníckych služieb pristupuje k jednej alebo viac bankám, aby obnovil platnosť spojenia prevodného peňažného modulu so zmienenými klientovými bankovými účtami u banky majúcej modul bankomatu, modul generátora peňazí a účtovný systém pripojený k centrálnemu počítaču (on-line) pričom tento spôsob obsahuje kroky, v ktorých:

(a) zmienený klient vyberie pomocou zmieneného prevodného peňažného modulu zmienenú banku, u ktorej obnoví platnosť spojenia;

(b) zmienený prevodný peňažný modul vytvorí šifrované

bezpečné spojenie so zmieneným modulom zákazníckych služieb;

(c) zmienený prevodný peňažný modul pošle zmienenému modulu zákazníckych služieb účtovný profil pre zmienené bankové účty, ktorý je uložený v zmienenom prevodnom peňažnom module;

(d) zmienený modul zákazníckych služieb overuje platnosť zmieneného účtovného profilu;

(e) zmienený modul zákazníckych služieb kontroluje u zmienenej banky, či sú aktívne zmienené klientove bankové účty obsiahnuté v zmienenom účtovnom profile;

(f) zmienený modul zákazníckych služieb vytvára účtovný profil pre zmienený klientov bankový účet;

(g) zmienený modul zákazníckych služieb posiela správu zmienenému prevodnému peňažnému modulu, ktorá obsahuje zmienený účtovný profil a digitálny podpis zmieneného účtovného profilu označeného súkromným kľúčom zmieneného modulu zákazníckych služieb;

(h) zmienený prevodný peňažný modul overuje zmienený digitálny podpis;

(i) zmienený prevodný peňažný modul pripojuje overenie zmieneného modulu zákazníckych služieb ku zmienenému účtovnému profilu; a

(j) učiní záväzným spojenie zmieneného prevodného peňažného modulu a zmieneného modulu zákazníckych služieb.

66. Spôsob podľa nároku 65, v y z n a č u j ú c i s a t ý m, že zmienený účtový profil obsahuje špecifické digitálne podpisy modulu zákazníckych služieb a certifikát zmieneného špecifického modulu zákazníckych služieb, kde zmienený krok d) overujúci platnosť zmienených účtovných profilov obsahuje krok, v ktorom sa kontrolujú zmienené špecifické digitálne

podpisy zákazníckeho modulu a uvádza v platnosť zmienený certifikát zmieneného modulu zákazníckych služieb.

67. Elektronický monetárny systém, v y z n a č u j ú c i s a t ý m, že obsahuje:
- vydávajúcu banku majúcu účtovný systém zapojený na centrálny počítač (on-line);
 - systém vyrovnania vydaných peňazí;
 - elektronické reprezentácie peňazí, ktoré sú účtované v zmienenom on-line účtovnom systéme;
 - modul generátora peňazí spojený so zmienenou vydávajúcou bankou, ktorý vytvára zmienené elektronické reprezentácie peňazí;
 - modul bankomatu spojený so zmienenou vydávajúcou bankou, schopný uchovávať zmienené elektronické reprezentácie peňazí;
 - prevodný peňažný modul schopný prevádzať zmienené elektronické reprezentácie peňazí;
 - a ďalej v prípadoch, v ktorých prevodný záznam je pripojený u zmienenej elektronickej reprezentácii peňazí po každom prevode medzi dvoma akýmikoľvek zmienenými modulmi, a kde zmienené elektronické poukážky sú periodicky postupované zmienenému systému vyrovnania vydaných peňazí;
 - zmienený systém vyrovnania vydaných peňazí má procesor pre analyzovanie zmienených prevodných záznamov pre každú poukážku za účelom identifikácie elektronických reprezentácií peňazí, ktoré sú stratené či duplikované;
 - a
 - tam, kde klient daného prevodného peňažného modulu predloží nárok stratených peňazí identifikujúci stratené elektronické reprezentácie peňazí zmienenej vydávajúcej banke, a zmienená vydávajúca banka odškodní

zmieneného klienta na základe zmieneného nároku stratených peňazí a na základe systému vyrovnaní vydaných peňazí, ktoré potvrdia platnosť zmienených nárokov stratených peňazí pre každú stratenú elektronickú reprezentáciu peňazí.

68. Elektronický monetárny systém podľa nároku 67, v y z n a č u j ú c i s a t ý m, že zmienené prevodné peňažné moduly sú všetky prispôsobené k ukladaniu informácie spojenej s elektronickými reprezentáciami peňazí, ktoré sú zahrnuté v prerušených prevodoch a kde zmienený nárok na stratené peniaze obsahuje zmienenú informáciu.
69. Elektronický monetárny systém podľa nároku 67, v y z n a č u j ú c i s a t ý m, že všetky zmienené prevodné peňažné moduly sú prispôsobené k ukladaniu zmienených nárokov stratených peňazí na nezávislom pamäťovom zariadení, kde zmienené nároky na stratené peniaze sú digitálne označené súkromným kľúčom zmienených prevodných peňažných modulov.
70. Elektronický monetárny systém podľa nároku 69, v y z n a č u j ú c i s a t ý m, že zmienené nároky na stratené peniaze obsahujú informáciu spojenú so všetkými elektronickými reprezentáciami peňazí, ktoré sú uložené v zmienenom prevodnom peňažnom module.
71. Spôsob, podľa ktorého vytvorí klient nárok na stratené poukážky, ktorý identifikuje stratené elektronické poukážky spojené s klientovým prevodným peňažným modulom pričom sa zmienená metóda skladá z krokov, v ktorých:
- (a) zmienený klient volí pomocou zmieneného prevodného

peňažného modulu možnosť vytvorenia nároku na stratené poukážky;

(b) zmienený prevodný peňažný modul generuje jedinečné poradové číslo nároku a formuluje zmienený nárok na stratené poukážky ako paket obsahujúci zmienené jedinečné poradové číslo nároku, informácia pre všetky prevoditeľné elektronické poukážky uložené v prevodnom peňažnom module, informácia o zlyhaní pri realizácii pre všetky elektronické poukážky spojené so zlyhaním pri realizácii pomocou zmieneného prevodného peňažného modulu, a digitálny podpis a certifikát zmieneného prevodného peňažného modulu; a

(c) uloží zmienený nárok na stratené poukážky na pamäťovom médiu, ktoré je nezávislé na zmienenom prevodnom peňažnom module.

72. Systém podľa nároku 71, v y z n a č u j ú c i s a t ý m, že nárok na stratené poukážky obsahuje:
- prvé a druhé dátové pole zašifrované zmieneným súkromným kľúčom prevodného peňažného modulu, kde zmienené prvé dátové pole obsahuje zmienené jedinečné poradové číslo nároku, zmienenou informáciou pre všetky prevoditeľné elektronické poukážky uchované v zmienenom prevodnom peňažnom module obsahujúce súčasnú hodnotu a kópiu každej zmienenej prevoditeľnej elektronickej poukážky, a zmienenú informáciu o nesplnení záväzku pre nereklamované nesplnené záväzky, a ďalej kde druhé dátové pole obsahuje zmienené prvé dátové pole digitálne označené zmieneným súkromným kľúčom prevodného peňažného modulu; a
- tretie dátové pole obsahujúce zmienené poradové číslo nároku, celkovú monetárnu hodnotu čiastky pre zmienený nárok na stratené poukážky, a zmienený certifikát zmieneného prevodného peňažného modulu.

73. Spôsob, v y z n a č u j ú c i s a t ý m, že pomocou modulu zákazníckych služieb majúceho prístup k jednej či viacej vydávajúcim bankám umožňuje klientovi nárokovat stratené poukážky združené s prevodným peňažným modulom pomocou použitia zmieneného prevodného peňažného modulu, pričom tento spôsob obsahuje kroky, v ktorých:

(a) zmienený klient poskytne identifikáciu hostiteľovi zmieneného modulu zákazníckych služieb;

(b) sa vytvorí šifrované bezpečné spojenie medzi zmieneným prevodným peňažným modulom a zmieneným modulom zákazníckych služieb;

(c) zmienený modul zákazníckych služieb príjme od zmieneného hostiteľa zmienenú identifikačnú informáciu zmieneného klienta;

(d) zmienený prevodný peňažný modul pošle zmienenému modulu zákazníckych služieb správu obsahujúcu informáciu o nereklamovaných nesplnených záväzkoch združenú so záznamom nenárokovaných nesplnených záväzkov uloženým v zmienenom prevodnom peňažnom module; a

(e) zmienený modul zákazníckych služieb vytvára nárok zo zmienenej informácie nenárokovaných zlyhaní odovzdaní, a posiela zmienený nárok cestou zmieneného hostiteľa do vyšetrovacieho systému vydaných peňazí združeného so zmienenou jednou alebo viac vydávajúcimi bankami.

74. Spôsob reklamácie stratených poukážok podľa nároku 73, v y z n a č u j ú c i s a t ý m, že ďalej obsahuje krok zmieneného klienta modulu zakázaných služieb, ktorý v reakcii na zmienenú správu posiela identifikátor nároku zmienenému prevodnému modulu, a zmienený prevodný peňažný modul označuje každý zo

zmienených záznamov nenárokovaných realizácií zmieneným identifikátorom nároku.

75. Spôsob realizácie stratených poukážok podľa nároku 73, v y z n a č u j ú j ú c i s a t ý m, že zmienená informácia o nenárokovaných nesplnených záväzkoch¹⁷ poslaná zmienenému modulu zákazníckych služieb v kroku d) je združená len so záznamami nenárokovaných záväzkov, ktoré neboli skôr nárokované.
76. Spôsob reklamácie stratených poukážok podľa nároku 73, v y z n a č u j ú c i s a t ý m, že pred krokom d) zmienený klient vyberie pomocou zmieneného prevodného peňažného modulu zmienené záznamy neplnených záväzkov zo zoznamu záznamov nesplnených záväzkov.
77. Spôsob umožňujúci klientovi pomocou modulu zákazníckych služieb majúceho prístup k jednej či viacerým vydávajúcim bankám nárokovať stratené poukážky združené s prevodným peňažným modulom pomocou použitia pamäťového zariadenia, ktoré obsahuje nároky stratených poukážok uložené od zmieneného prevodného modulu a zmienené pamäťové zariadenie je nezávislé na zmienenom prevodnom module; pričom tento spôsob obsahuje kroky, v ktorých:
 - (a) zmienený klient poskytne identifikáciu hostiteľovi zmieneného modulu zákazníckych služieb;
 - (b) zmienený modul zákazníckych služieb umožňuje prístup ku zmieneným nárokom na stratené poukážky v zmienenom úložnom zariadení;
 - (c) zmienený modul zákazníckych služieb prijíma zmienený nárok na stratených poukážkach od zmieneného pamäťového zariadenia;
 - (d) zmienený modul zákazníckych služieb overuje

platnosť zmieneného nároku stratených poukážok; a
(e) zmienený modul zákazníckych služieb vytvára nárok zo zmienenej informácie nenárokovaného nesplneného záväzku, a posiela zmenený nárok cestou zmieneného hostiteľa do vyšetrovacieho systému vydaných peňazí združeného so zmienenou jednou či viacerými bankou.

78. Spôsob reklamácie stratených poukážok podľa nároku 77, v y z n a č u j ú c i s a t ý m, že zmienený nárok na stratené poukážky obsahuje certifikát zmieneného prevodného peňažného modulu, a tým, že zmienený krok d) zmieneného modulu zákazníckych služieb, ktorý overuje platnosť zmieneného nároku na stratené poukážky zahrňuje overenie platnosti zmieneného certifikátu.
79. Spôsob reklamácie stratených poukážok podľa nároku 77, v y z n a č u j ú c i s a t ý m, že zmienený nárok na stratené poukážky obsahuje kópie stratených poukážok, každá kópia zo zmienených poukážok má skupinu dátových polí certifikátov, ktorá obsahuje zoznam každého peňažného modulu platcu, ktorý prevádzal originál zmienenej stratenej poukážky a obsahuje všetky digitálne podpisy zmieneného peňažného modulu platcu a certifikát, a kde krok d) ďalej obsahuje krok overujúci platnosť každého certifikátu a digitálneho podpisu peňažného modulu platcu.
80. Spôsob reklamácie stratených poukážok podľa nároku 77, v y z n a č u j ú c i s a t ý m, že zmienený nárok stratených poukážok obsahuje kópie stratených poukážok, kde každá kópia zo zmienených kópií stratených poukážok má dátové pole záznamu prevodu, ktoré obsahuje zoznam každej monetárnej hodnoty prevedenej v každom prevode originálu zmienenej stratenej poukážky, a kde krok d)

ďalej obsahuje krok kontrolujúci zmienené dátové pole záznamu prevodu, aby zistilo, či v každom prevode bola prevedená monetárna čiastka, ktorá nie je vyššia ako monetárna čiastka prevedená v bezprostredne predchádzajúcom prevode.

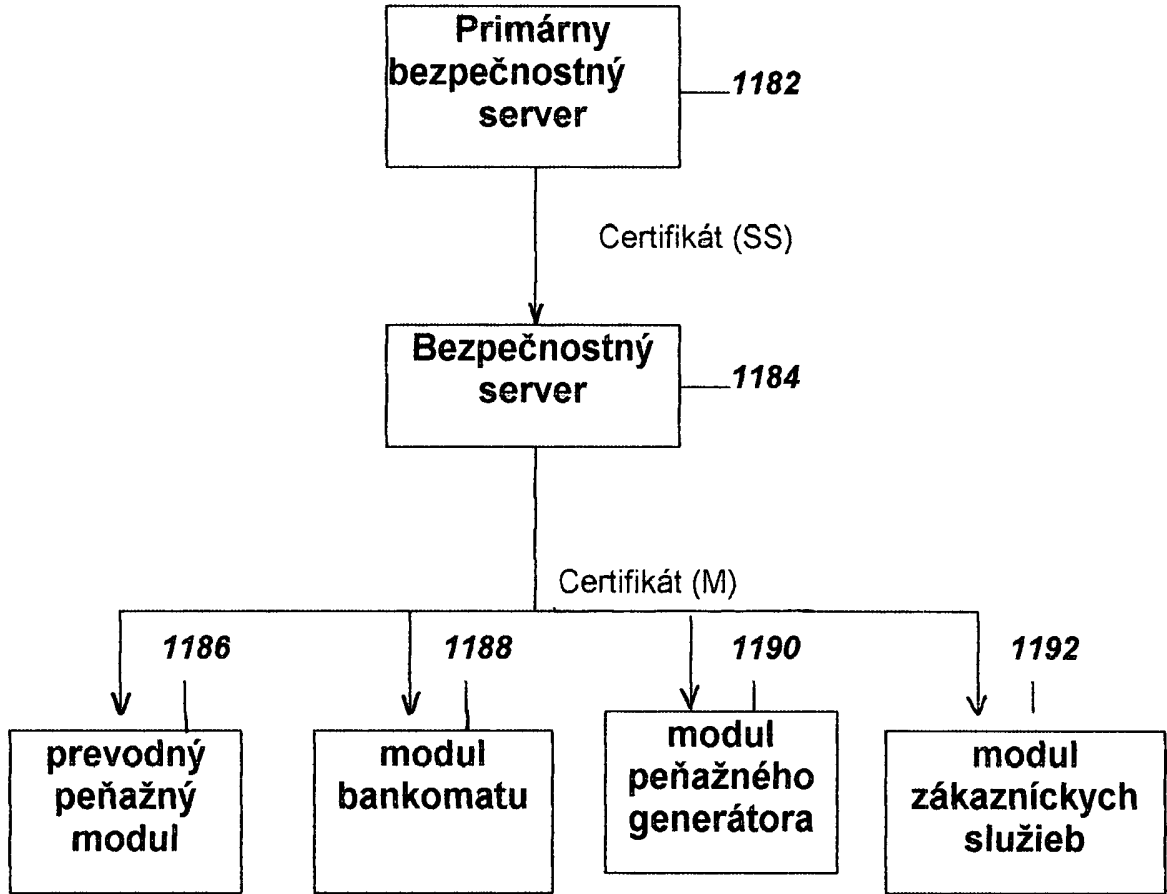
81. Spôsob reklamácie stratených poukážok podľa nároku 77, v y z n a č u j ú c i s a t ý m, že v kroku b) je vytvorené komunikačné spojenie medzi zmieneným modulom zákazníckych služieb a hostiteľským zariadením združeným so zmieneným pamäťovým zariadením, a zmienený modul zákazníckych služieb má prístup ku zmienenému nároku na stratené poukážky cestou zmieneného komunikačného spojenia.
82. Monetárny prevodný systém založený na elektronickom module, v y z n a č u j ú c i s a t ý m, že zmienený prevodný systém sa skladá z:
radu bezpečnostných serverov;
radu elektronických modulov odolných proti zneužitiu, z ktorých každý má jedinečný modulový certifikát, ktorý je digitálne označený jedným zo zmienených bezpečnostných serverov, pamäť na ukladanie elektronických reprezentácií peňazí, a procesor prispôsobený tak, aby zabezpečil šifrovaný bezpečný kanál pre prevod a príjem zmienených elektronických reprezentácií peňazí; a
kde zmienený modulový certifikát je uvedený v platnosť po spojení zmieneného elektronického modulu s iným zo zmienených elektronických modulov alebo zo zmienených bezpečnostných serverov; a
kde zmienený rad bezpečnostných serverov selektívne ovláda globálne opätovné overenie zmienených modulových certifikátov, vyžadujúce aby každý elektronický modul,

ktorý sa spojí s jedným zo zmienených bezpečnostných serverov opätovne overil zmienený modulový certifikát.

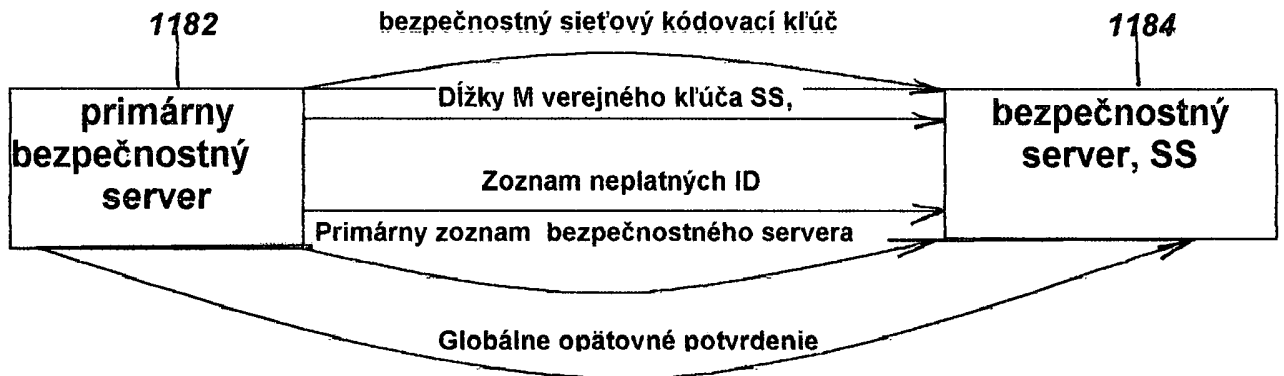
Poznámky prekladateľa

- 1 so vzormi
- 2 vo význame napáliť, prekonať, podviesť
- 3 vo význame všetky prevádzané alebo vydávané sumy peňazí
- 4 táto veta musí mať obrátený zmysel, teda namiesto
platný musí byť neplatný, chyba v originále
- 5 originál upravený tak, aby bol v súlade s obr. 8A
- 6 upravené podľa obr. 8A
- 7 MM znamená peňažný modul
- 8 tu bude asi chyba, pretože doplnok je obvykle
definovaný ako rozdiel množín
- 9 rozumie sa ako funkcia
- 10 tento text sa odkazuje na obrázok 12, ktorý nie je
v súbore. V súbore sú obr. 12A a 12B, ktoré však
neobsahujú prvok, ktorý je označený číslom 1186
- 11 slovo "prevod" doplnil prekladateľ
- 12 pravdepodobne má byť CSMHA
- 13 vo význame "zlučujú"
- 14 pravdepodobne má byť CSMHA
- 15 rozumie sa ukradnutý
- 16 zmenený singulár na plurál
- 17 v originále vypadlo slovo správne má asi byť
...unclaimed failed commit information...

1/54



Obr. 1A



Obr. 1B

2/54

1202

1204

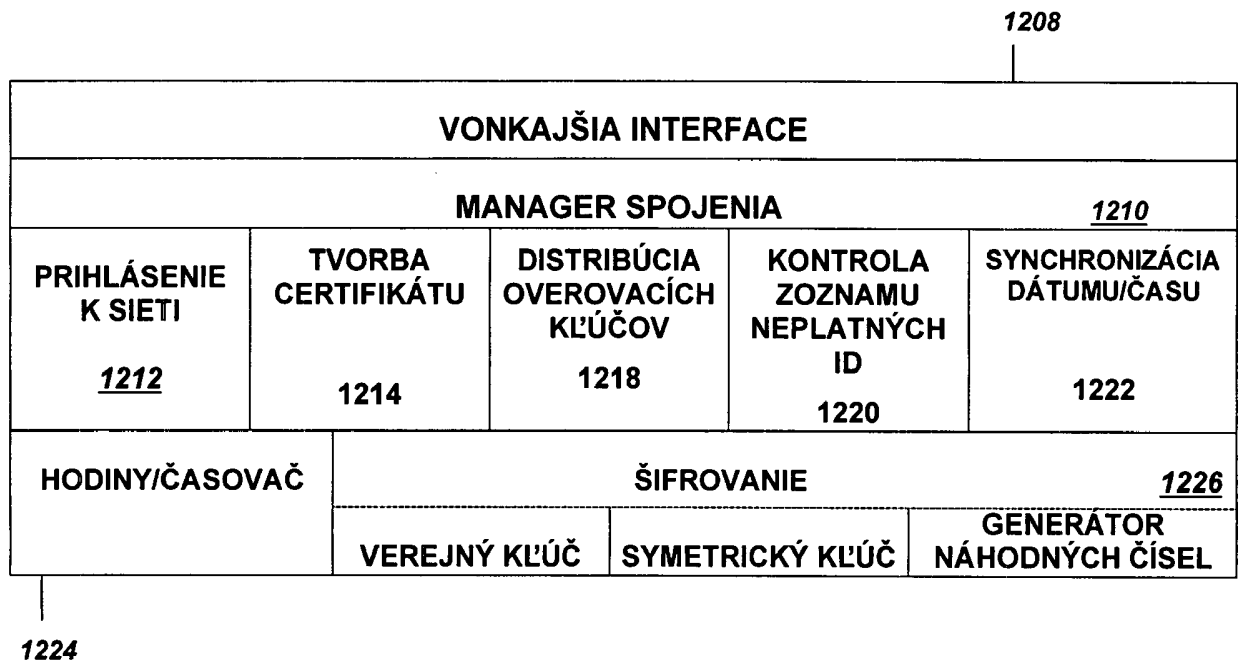
modul
výroby LANbezpečnostný
server výroby
LANbezpečnostný
serverprimárny
bezpečnostný
serverbezpečnostná
sieťmiestna
bezpečnostná
LANprimárny
bezpečnostný
serverbezpečnostný
serverbezpečnostný
serversieť
EMS

NS

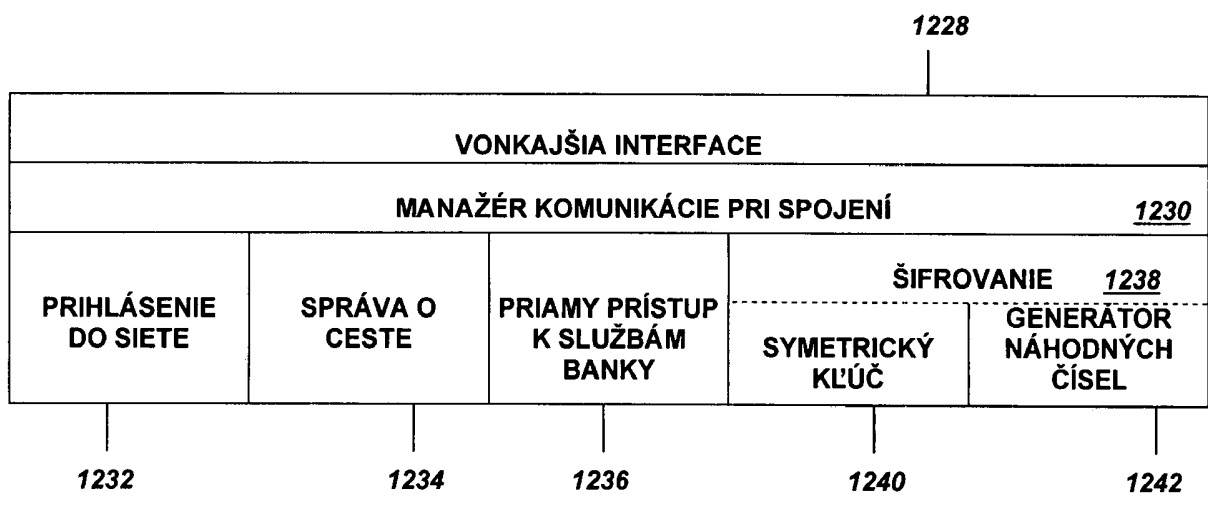
převodný
peňažný
modulmiestna
bankovná
LANmodul
peňažného
generátoramodul
zákazníckych
služiebmodul
bankomatu

Obr. 2

3/54



Obr. 3A



Obr. 3B

4/54

3000

VONKAJŠIA INTERFACE			
MANAŽÉR KOMUNIKÁCIE PRI SPOJENÍ <u>3001</u>			
VYTVOR PROFIL ÚČTU <u>3002</u>	ZAISTI BEZPEČNOSŤ <u>3004</u>	K HOSTITEĽOVI <u>3006</u>	POŽIADAVKA STRATENÝCH POZNÁMOK <u>3008</u>
HODINY/ČASOVAČ	ŠIFROVANIE <u>3010</u>		
	VEREJNÝ KĹÚČ	SYMETRICKÝ KĹÚČ	GENERÁTOR NÁHODNÝCH ČÍSEL

3012

Obr. 4A

3020

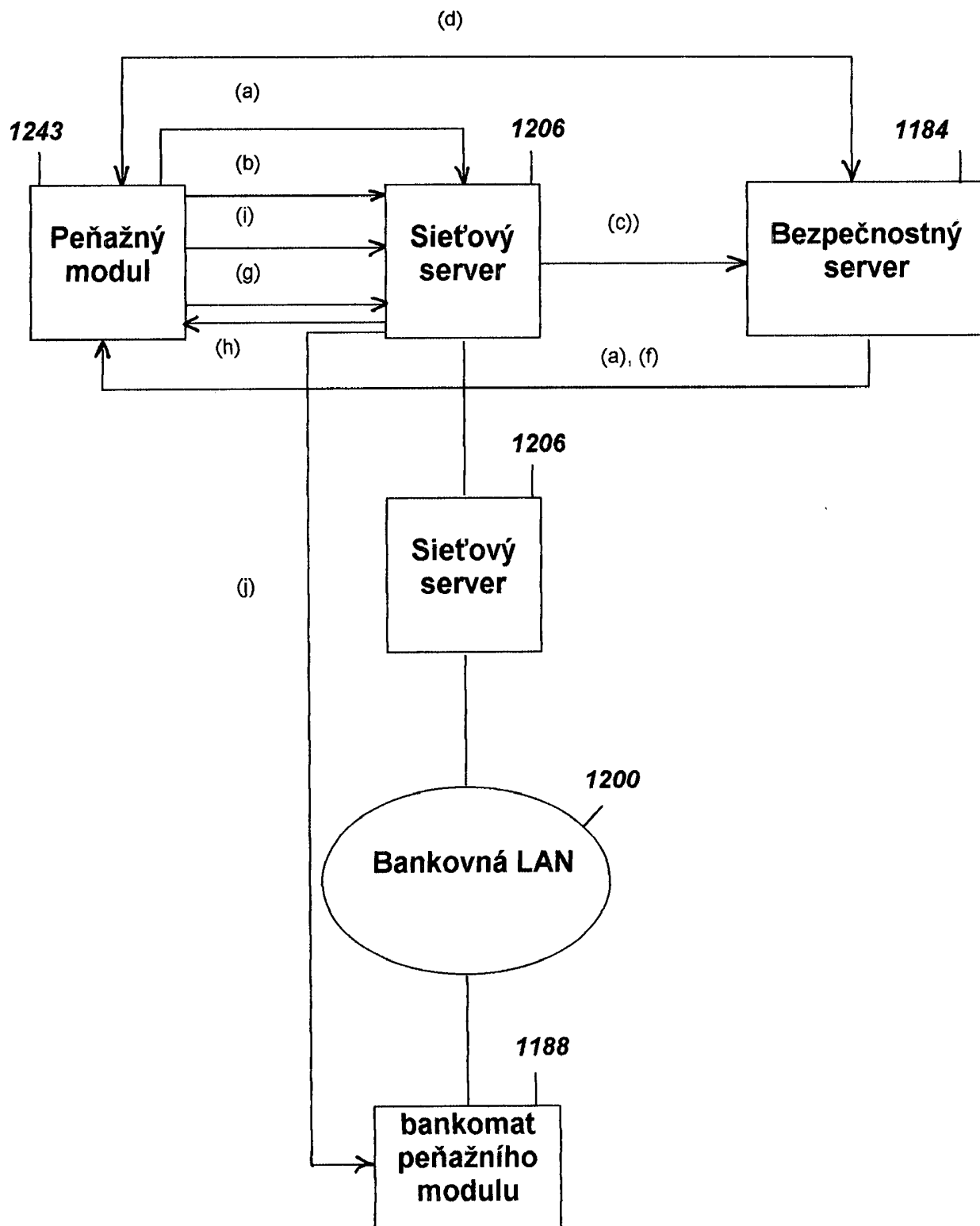
VONKAJŠIA INTERFACE				
MANAŽÉR KOMUNIKACE <u>3022</u>				
VYTVOR OVERENIE <u>3024</u>	ROZDEL OVEROVACIE KĹÚČE	ROZDEL ZOZNAM ŠPATNÝCH ID <u>3028</u>	NASTAV GLOBÁLNE OPÄTNÉ OVERENIE	ROZDEL BEZPEČNOSTNÉ SIEŤOVÉ KĹÚČE <u>3032</u>
HODINY/ČASOVAČ	ŠIFROVANIE <u>3036</u>			
	VEREJNÝ KĹÚČ	SYMETRICKÝ KĹÚČ	GENERÁTOR NÁHODNÝCH ČÍSEL	

3034

Obr. 4B

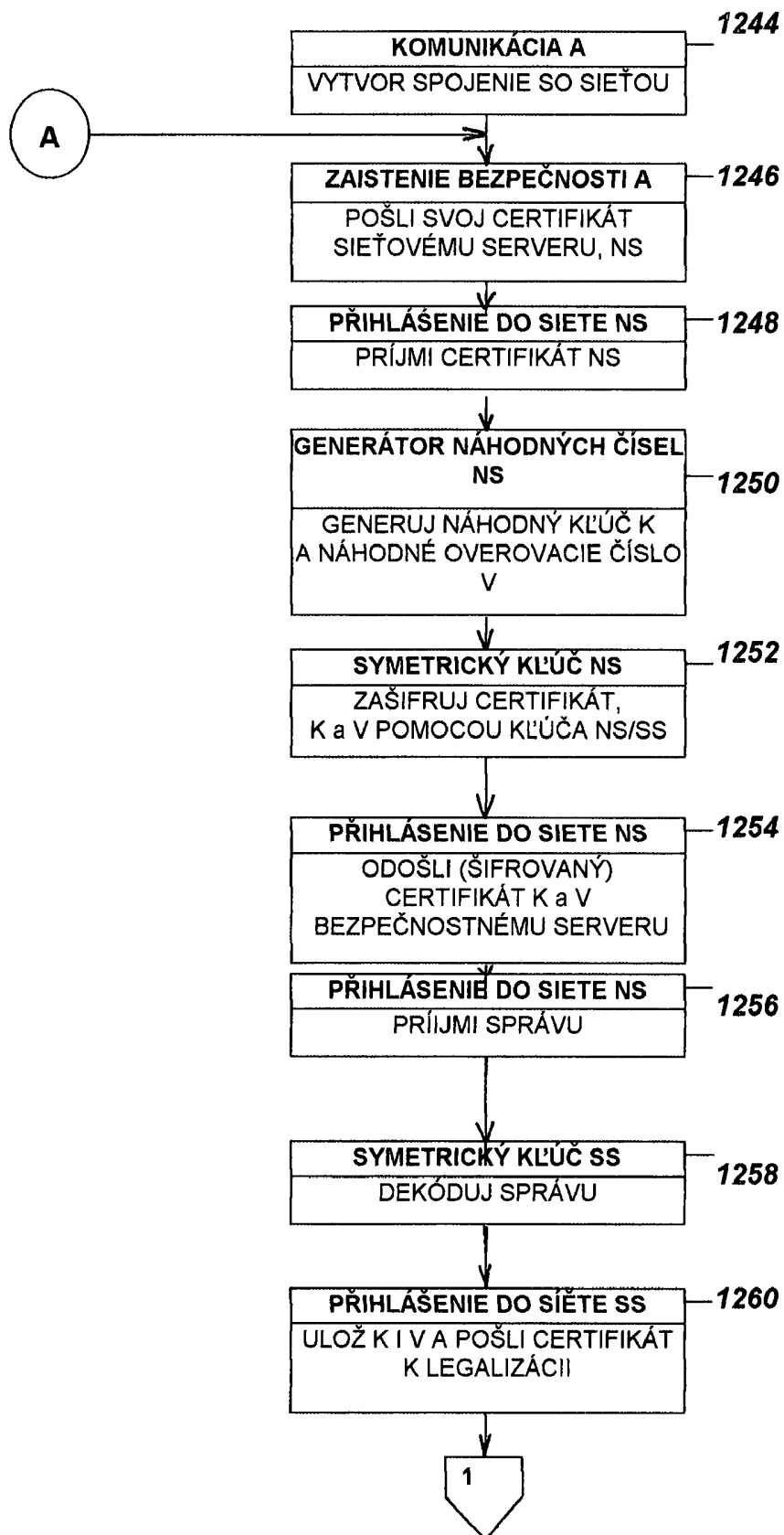
NÁHRADNÝ LIST (PRAVIDLO 26)

5/54



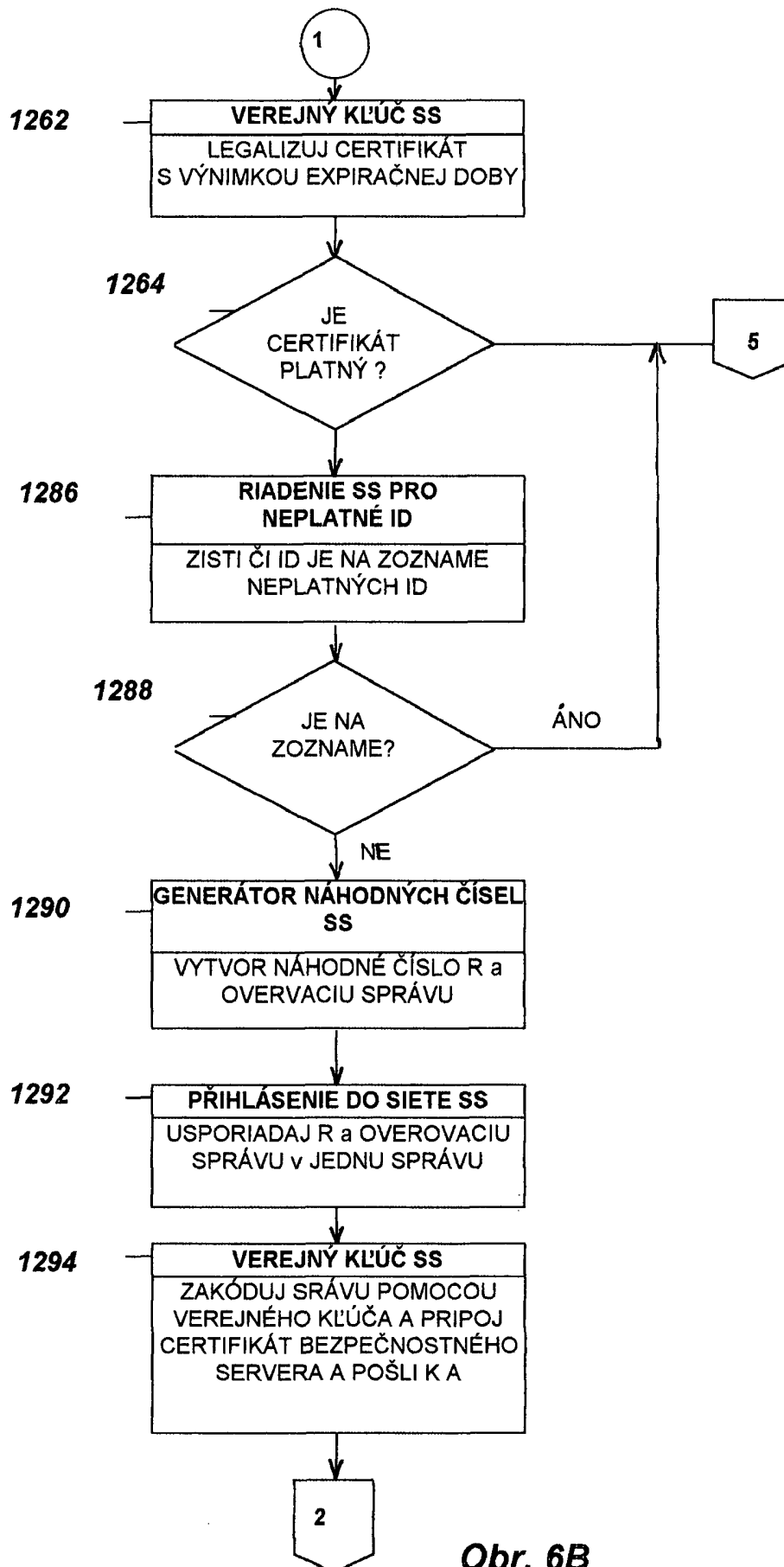
Obr. 5

6/54



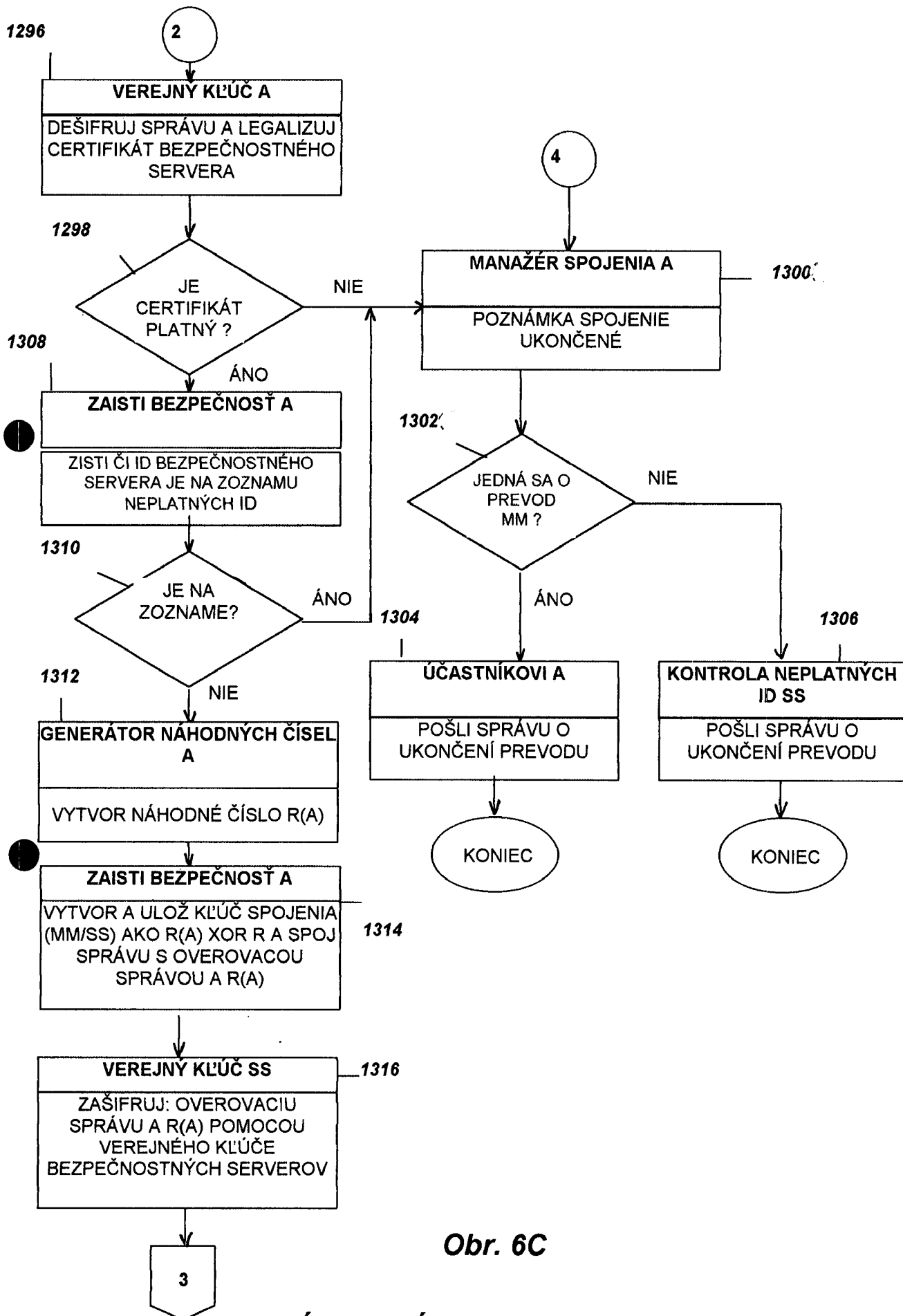
Obr. 6A

7/54



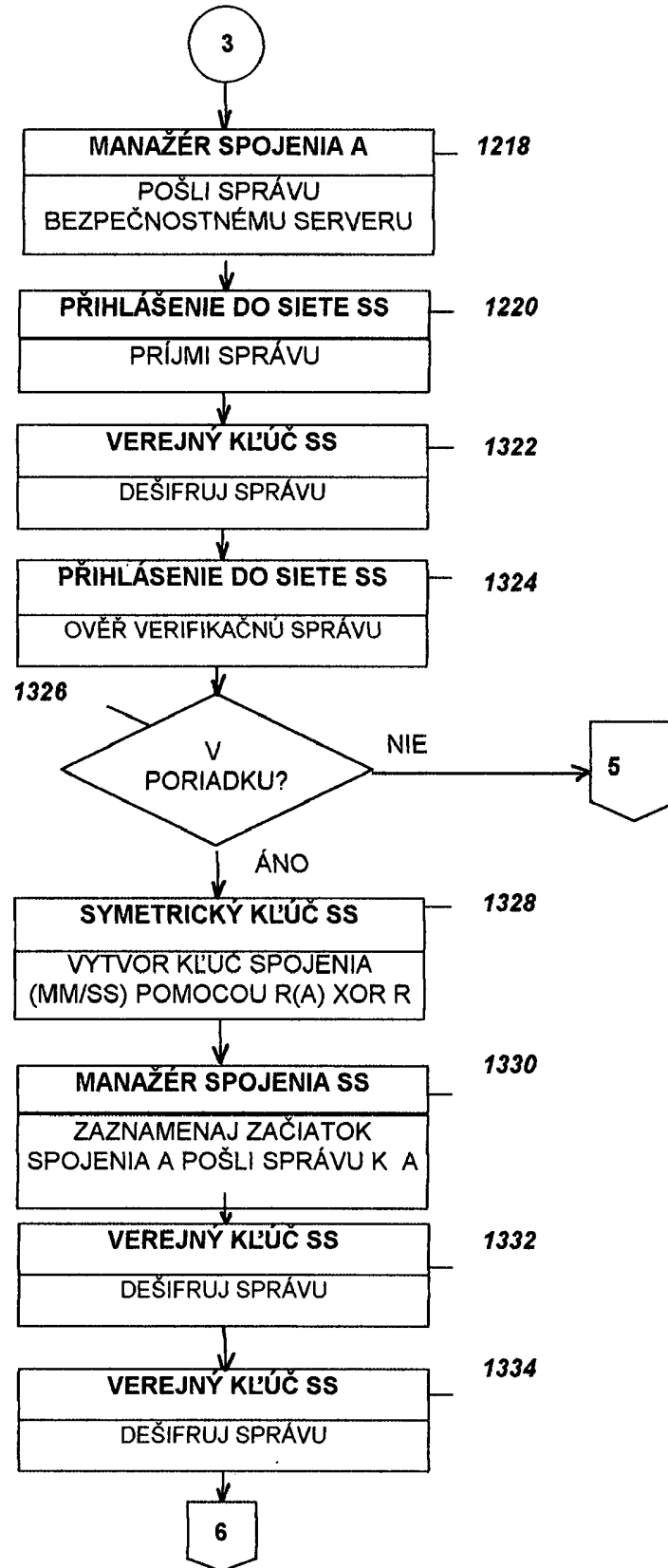
Obr. 6B

8/54



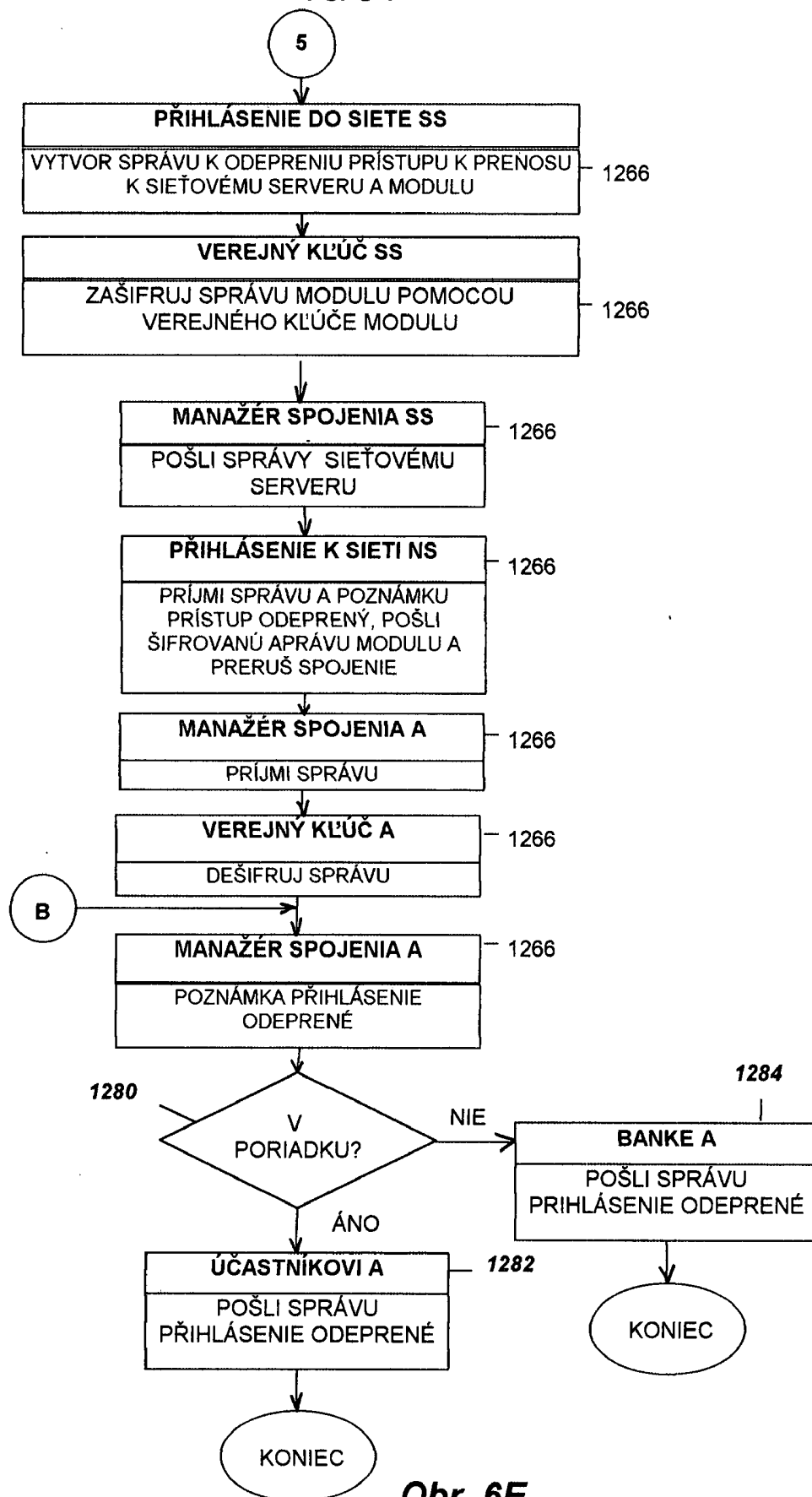
Obr. 6C

9/54



Obr. 6D

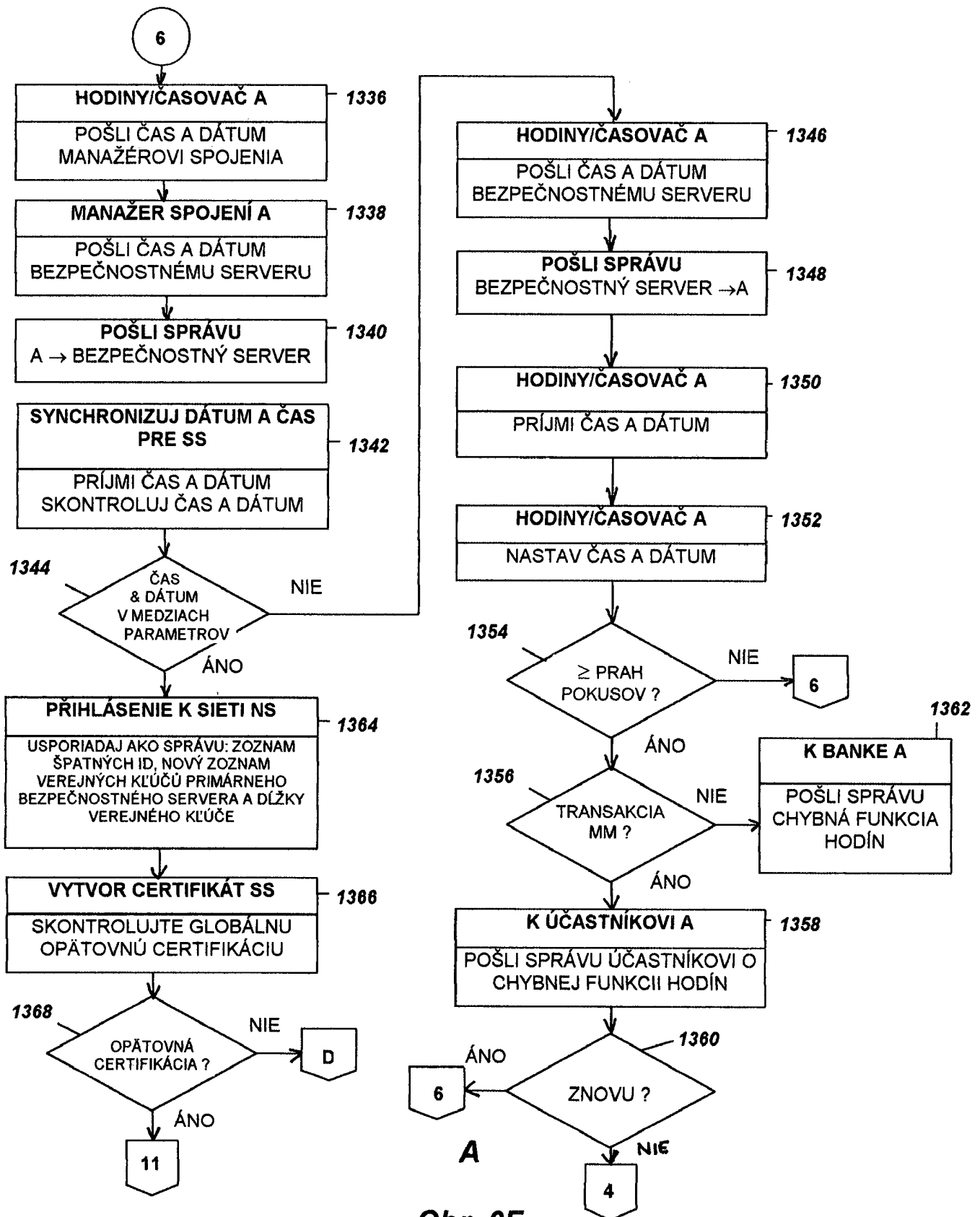
10/54



Obr. 6E

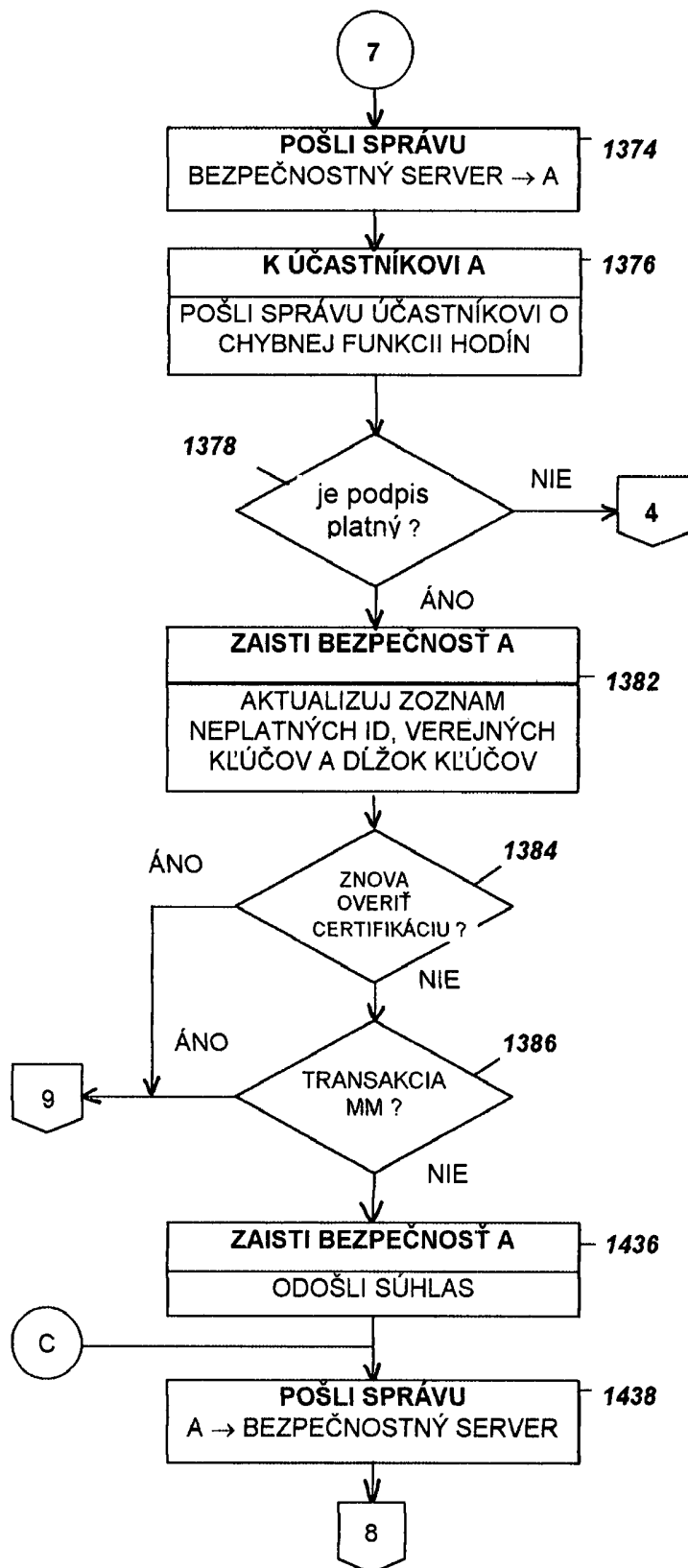
11/54

PV 1426-94



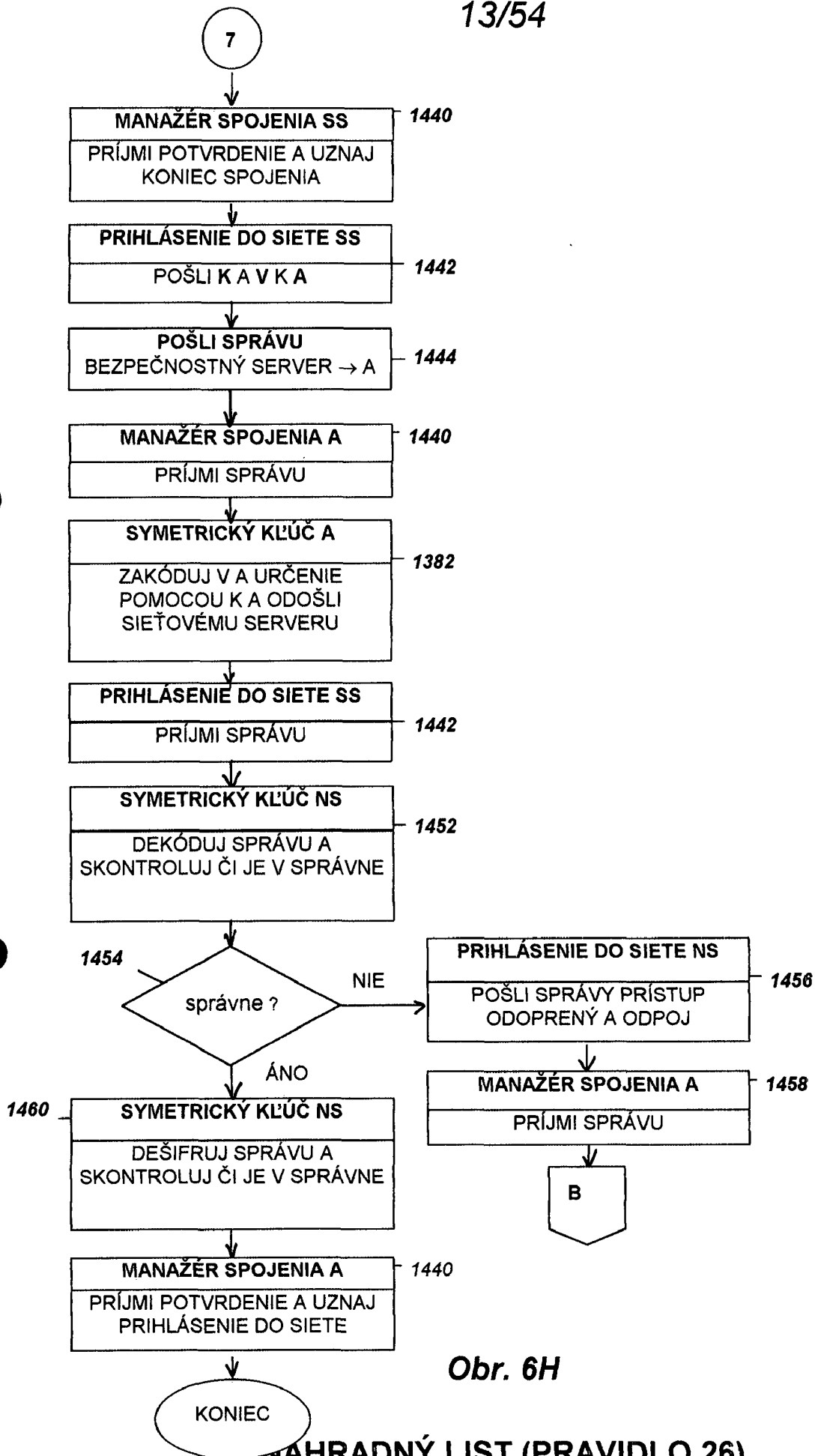
Obr. 6F

12/54



Obr. 6G

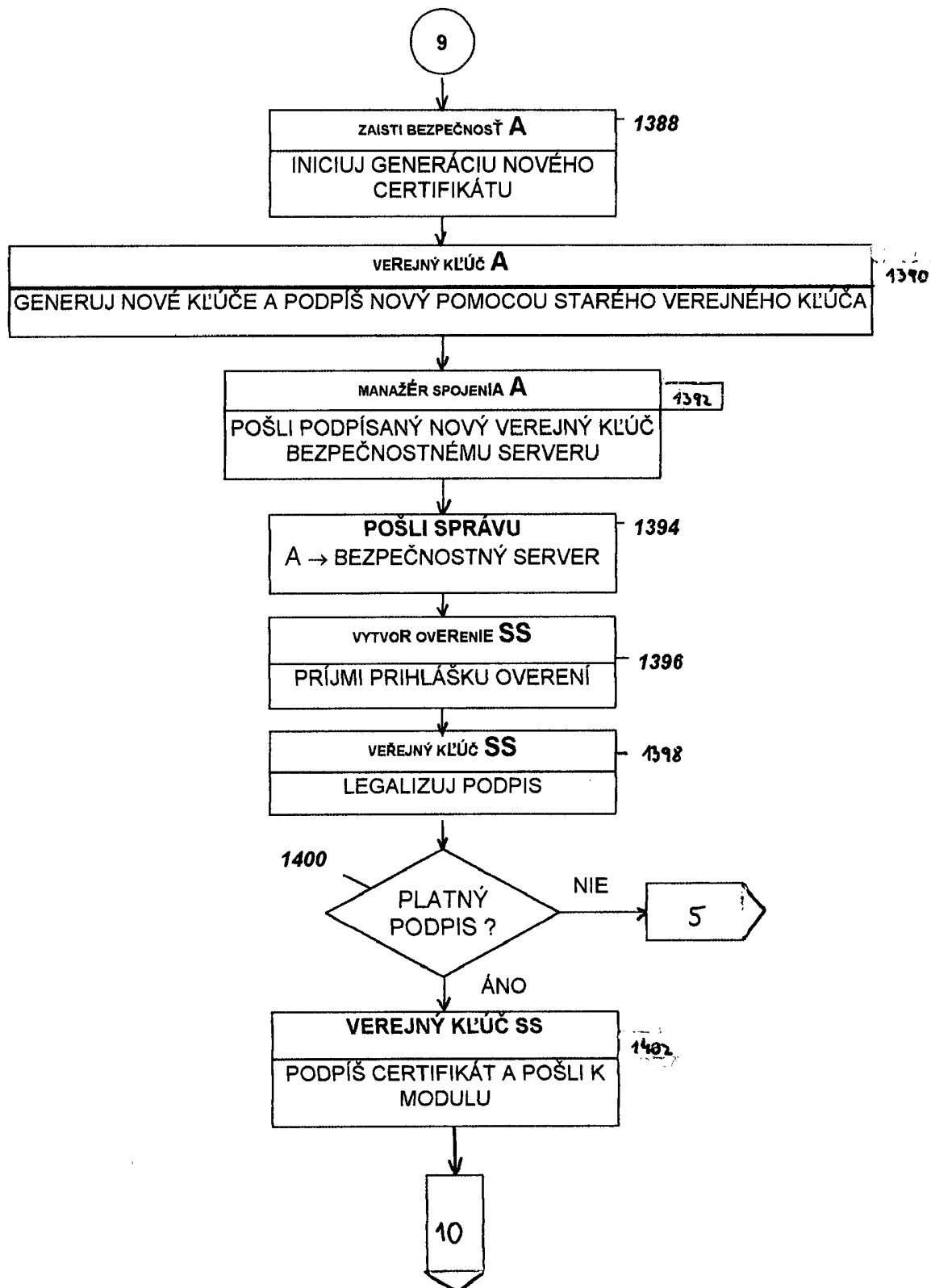
13/54



Obr. 6H

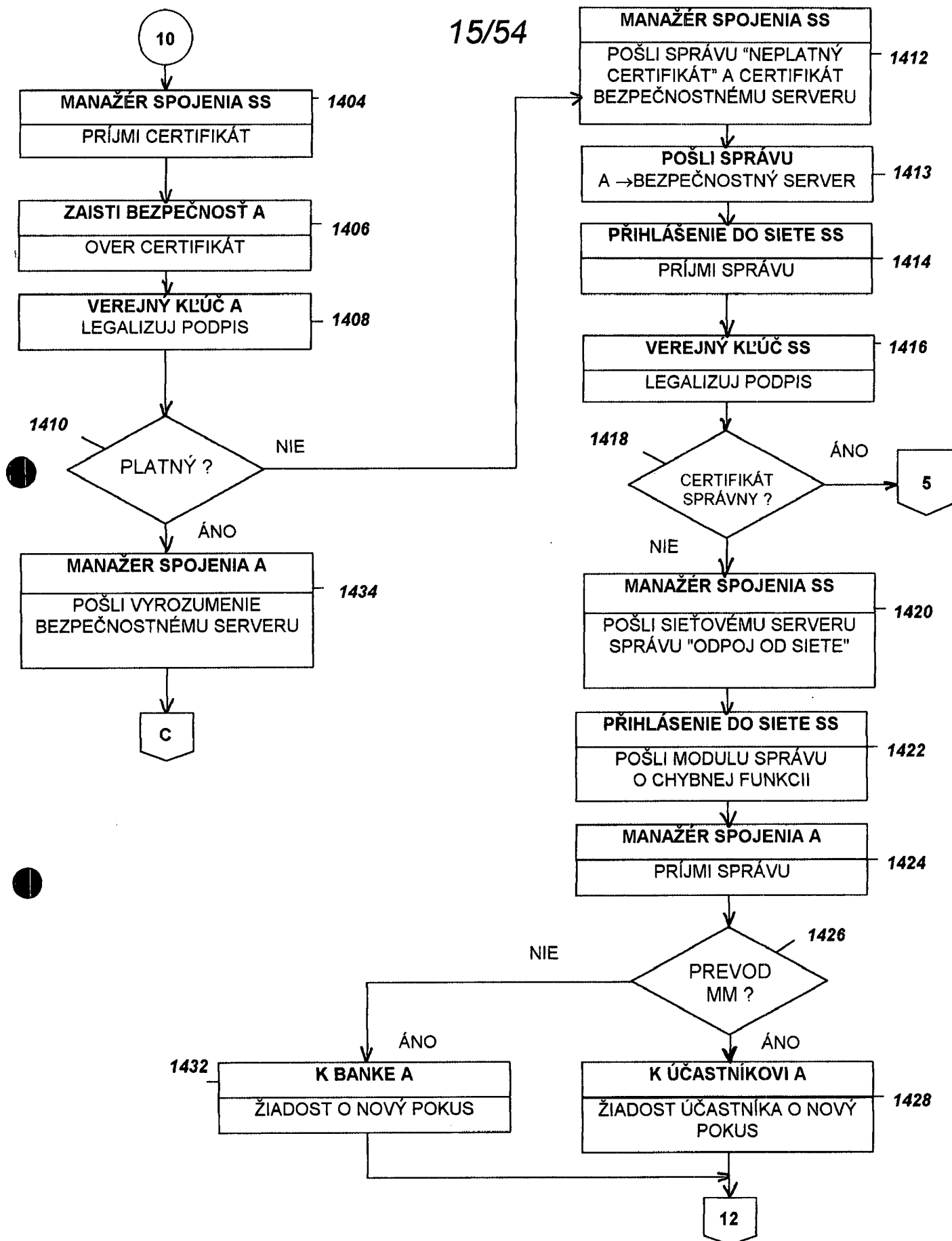
NAHRADNÝ LIST (PRAVIDLO 26)

14/54



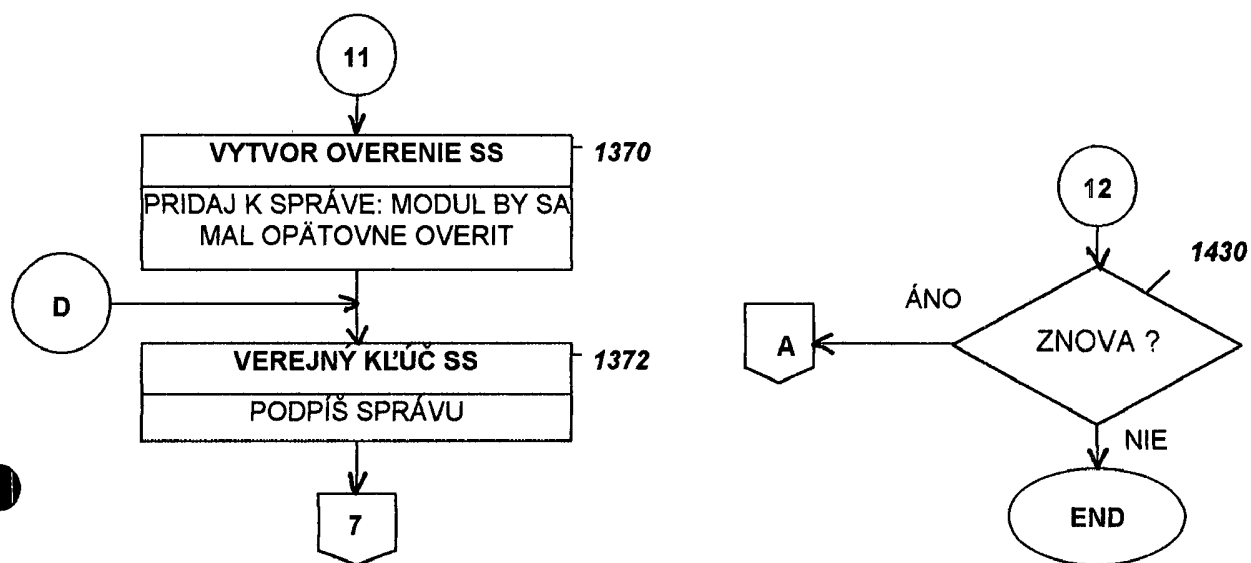
Obr. 6I

15/54



Obr. 6J

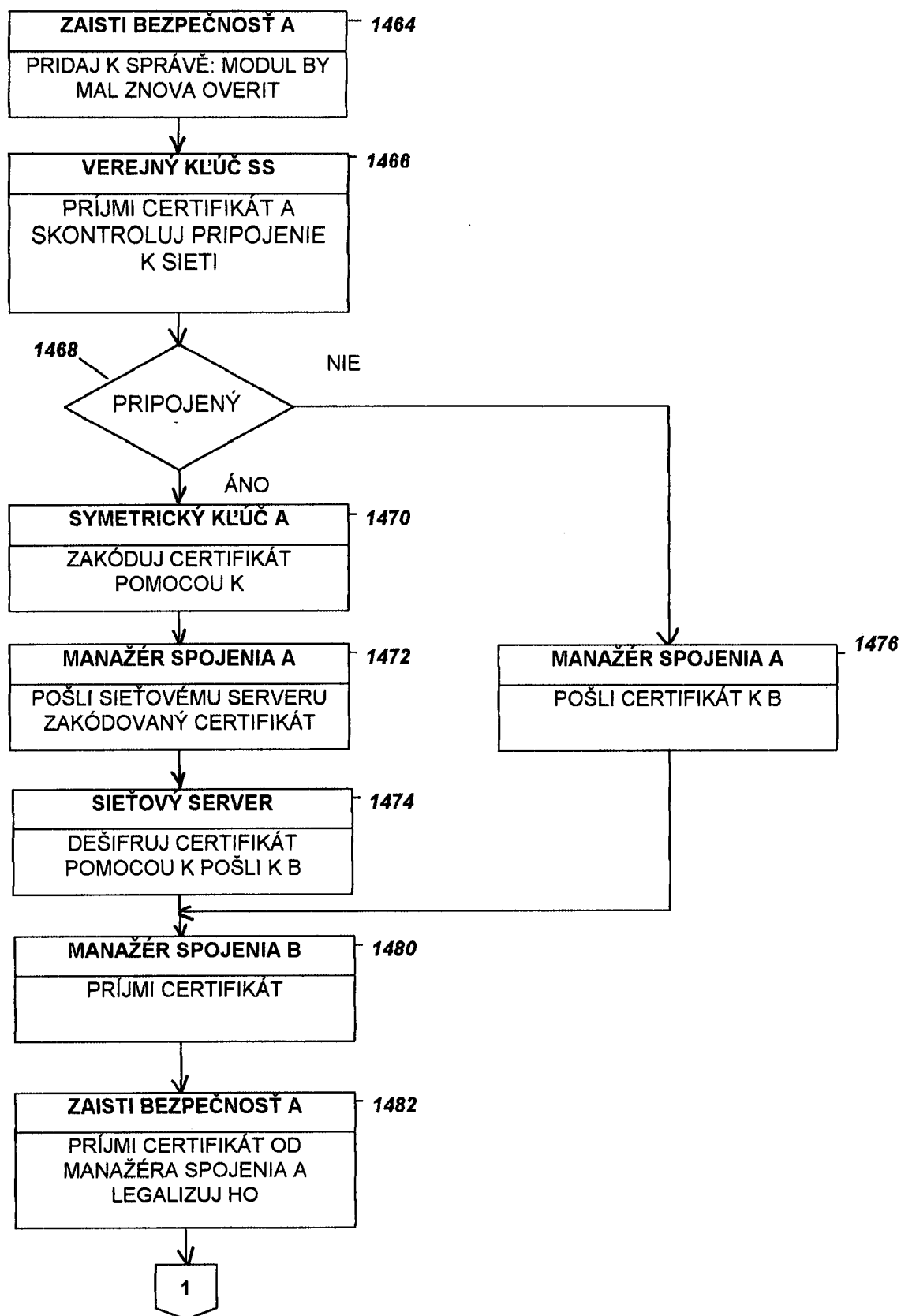
16/54



Obr. 6K

Obr. 6K

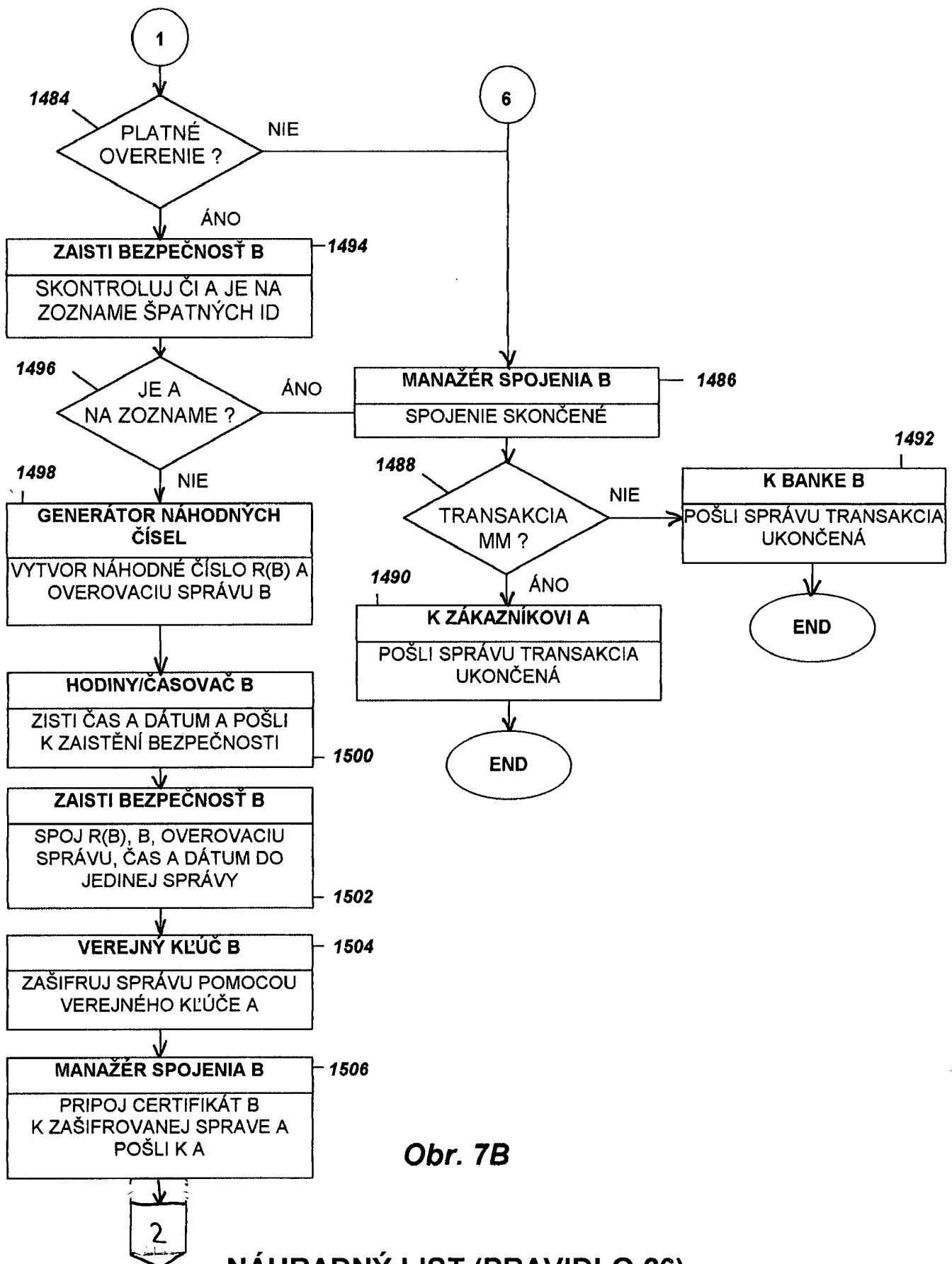
17/54



Obr. 7A

18/54

PV 1426-97

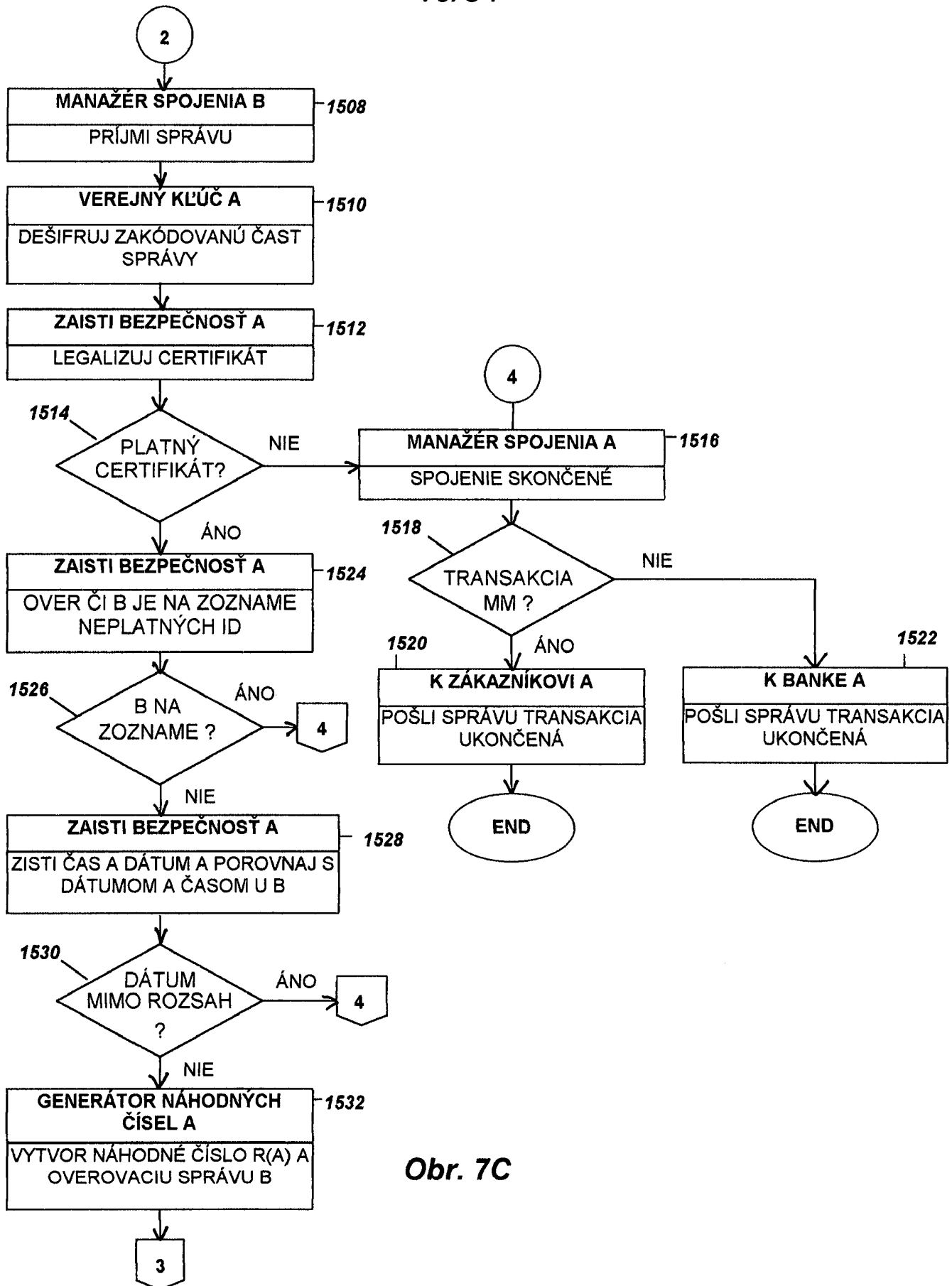


Obr. 7B

NÁHRADNÝ LIST (PRAVIDLO 26)

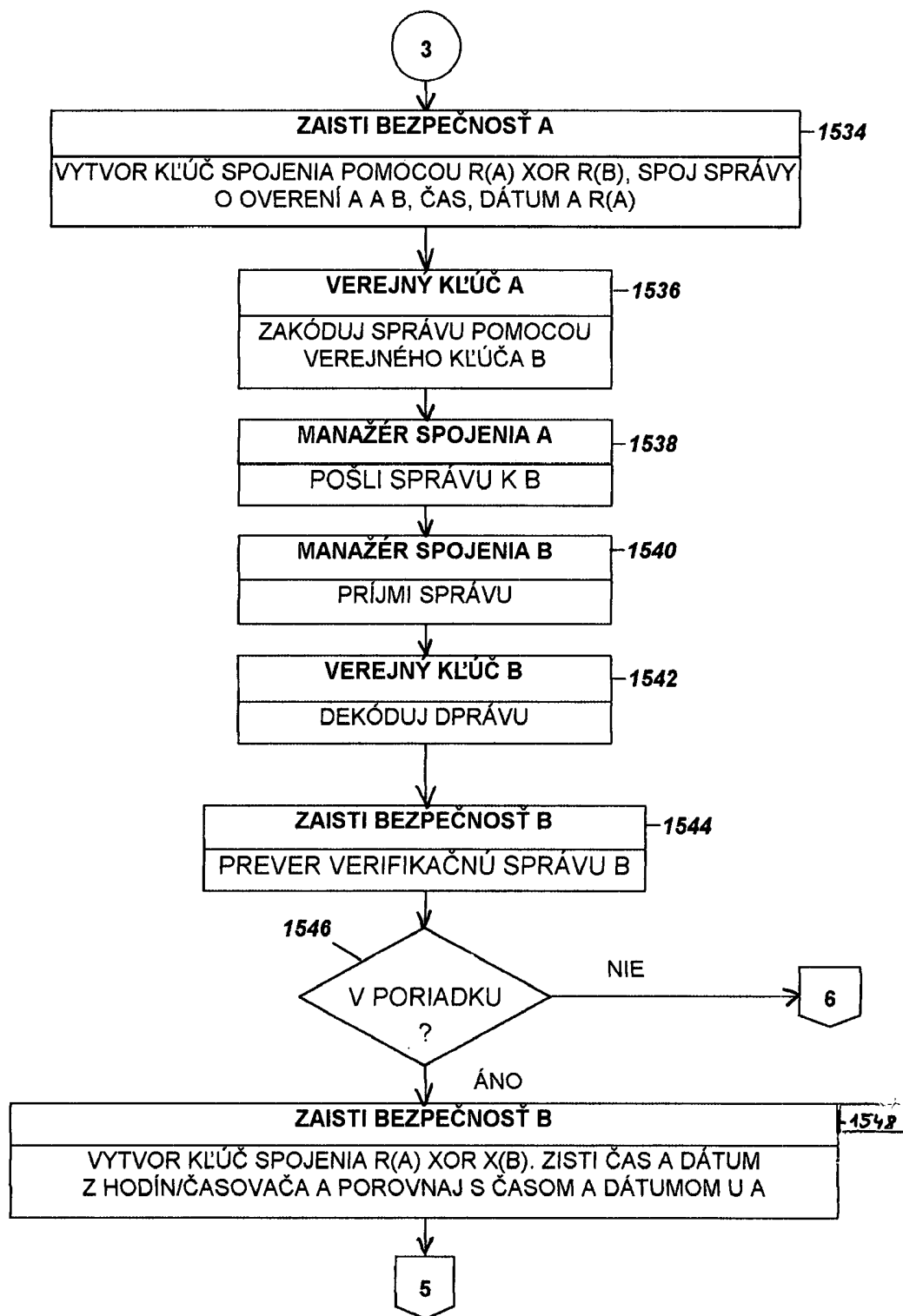
19/54

PI 1426-97



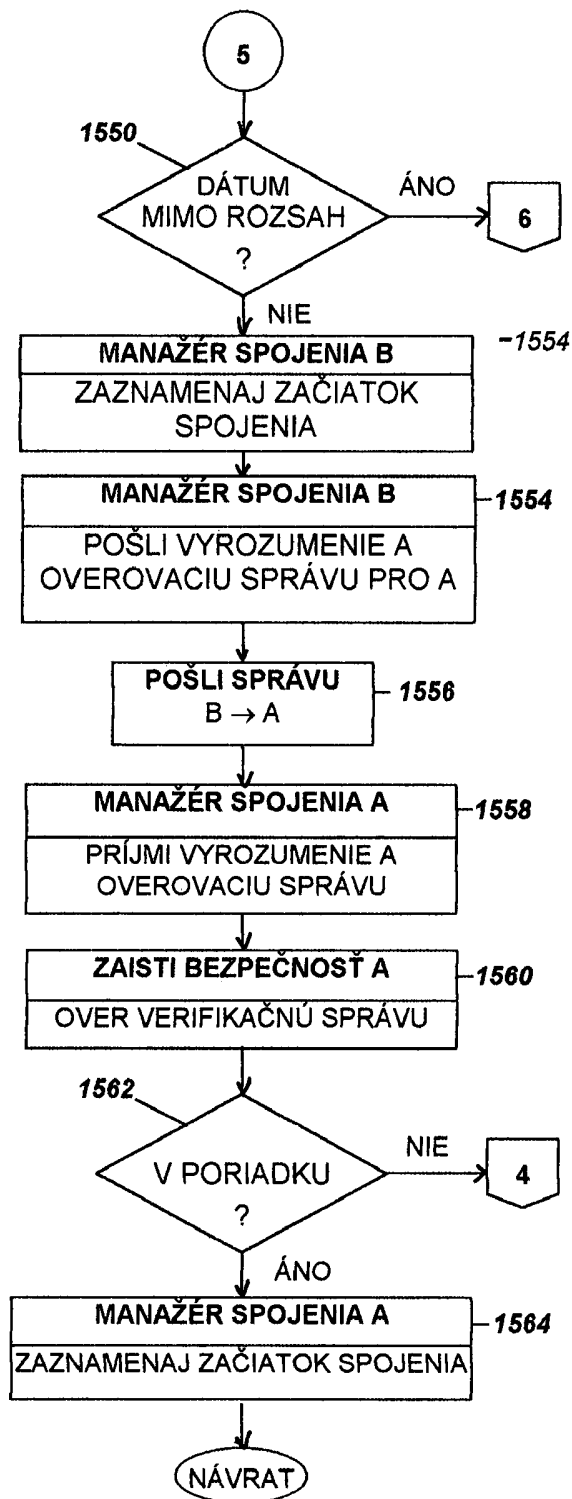
Obr. 7C

20/54



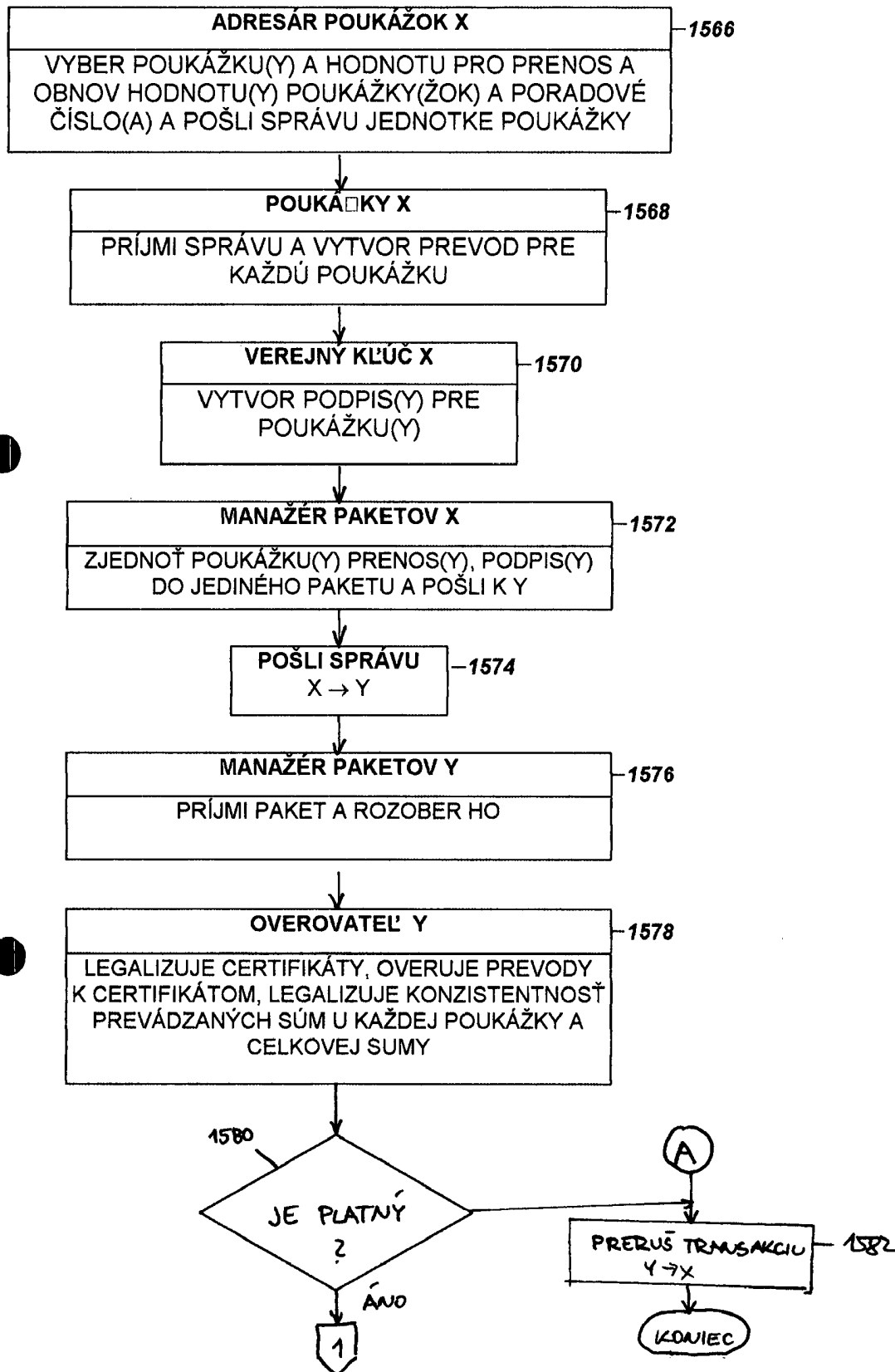
Obr. 7D

21/54



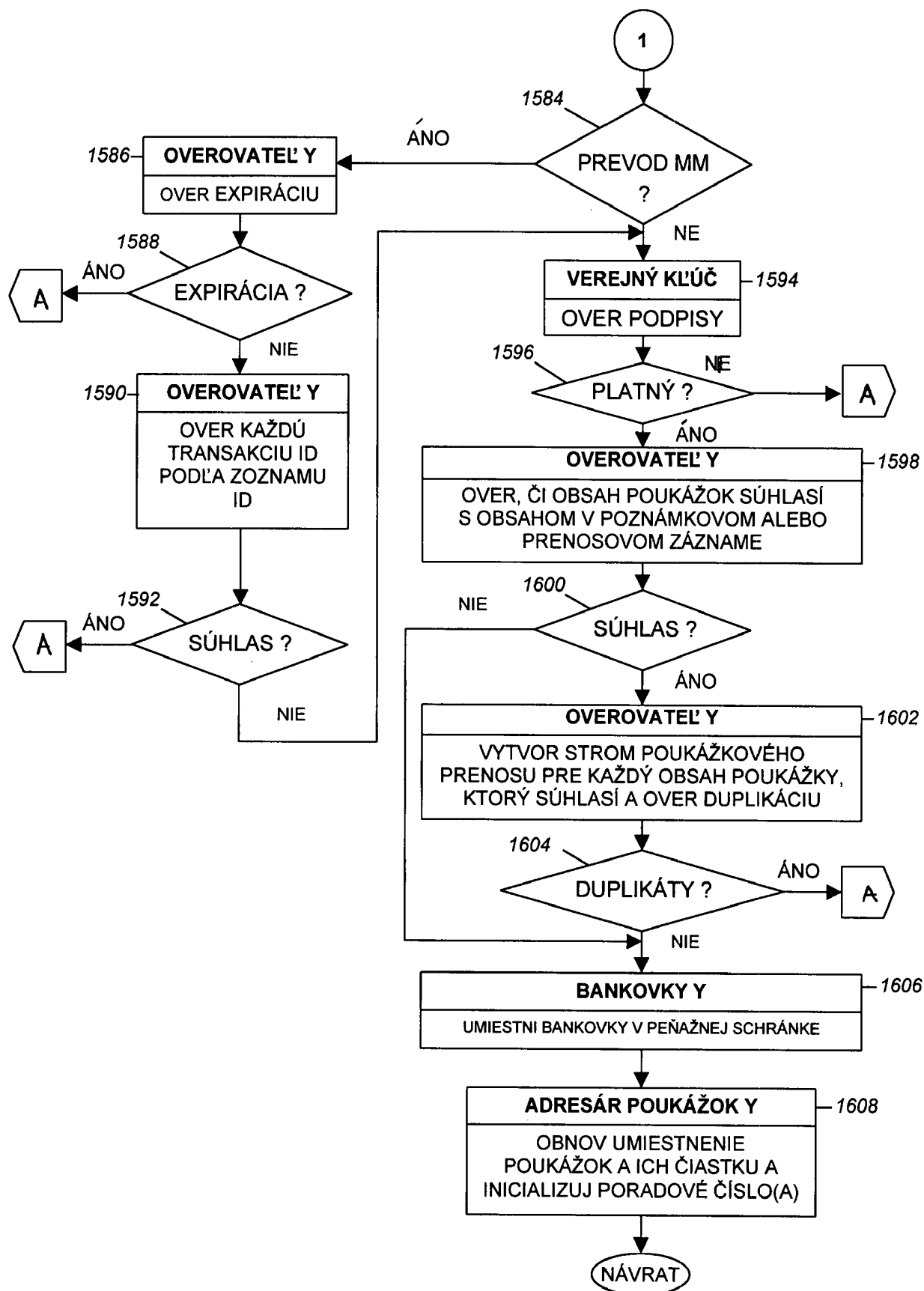
Obr. 7E

22/54



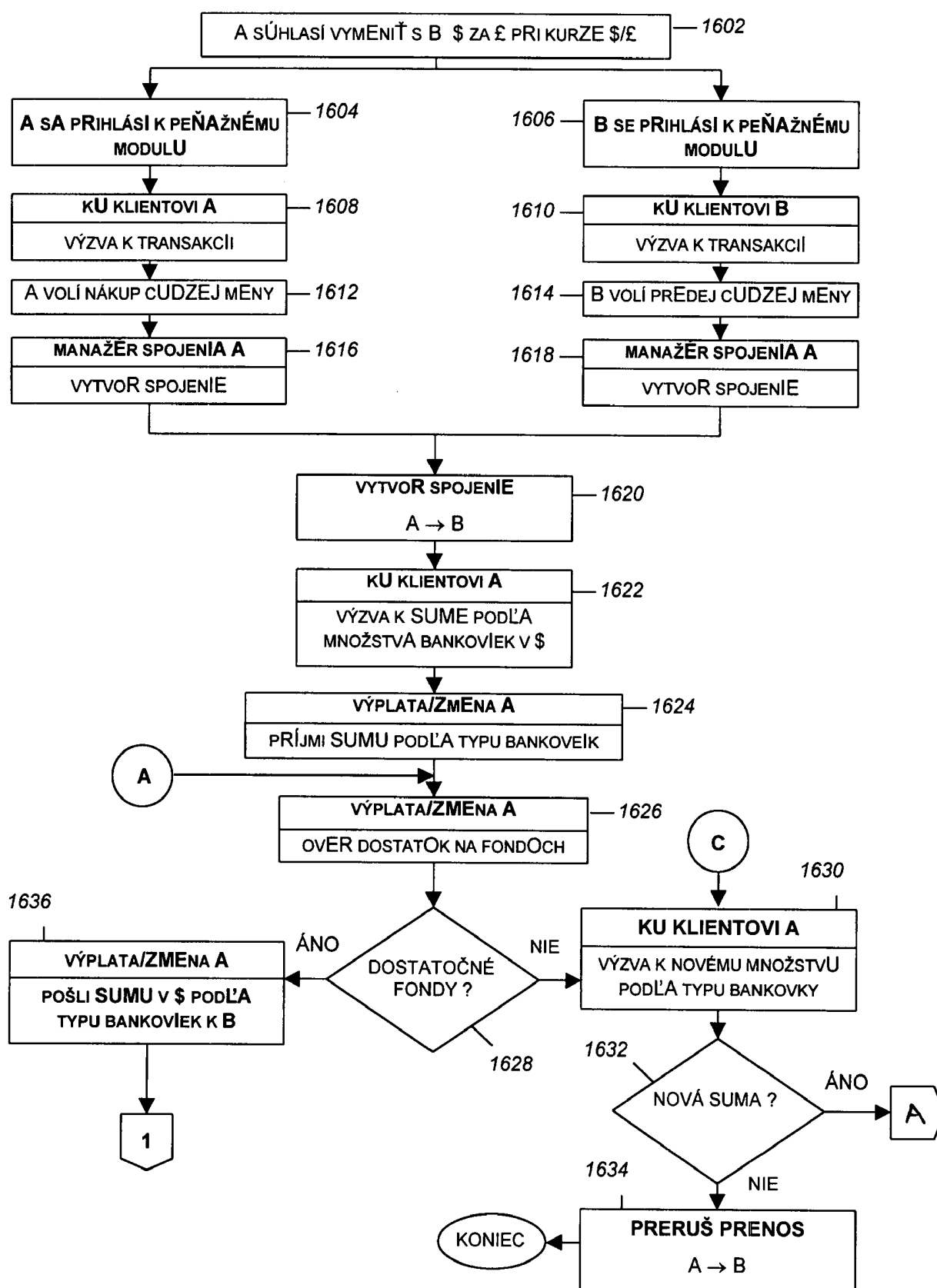
Obr. 8A

23/54



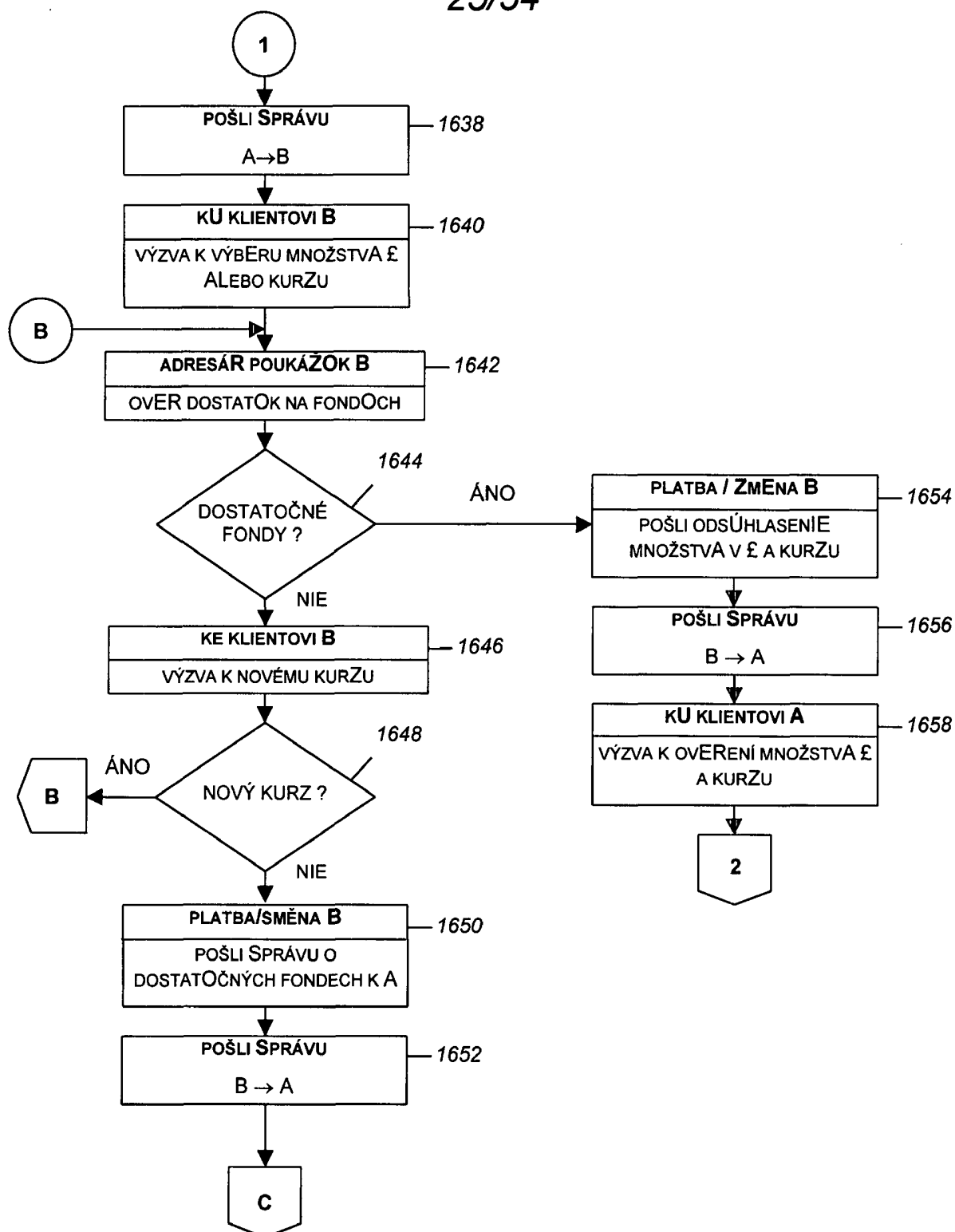
Obr. 8B

24/54



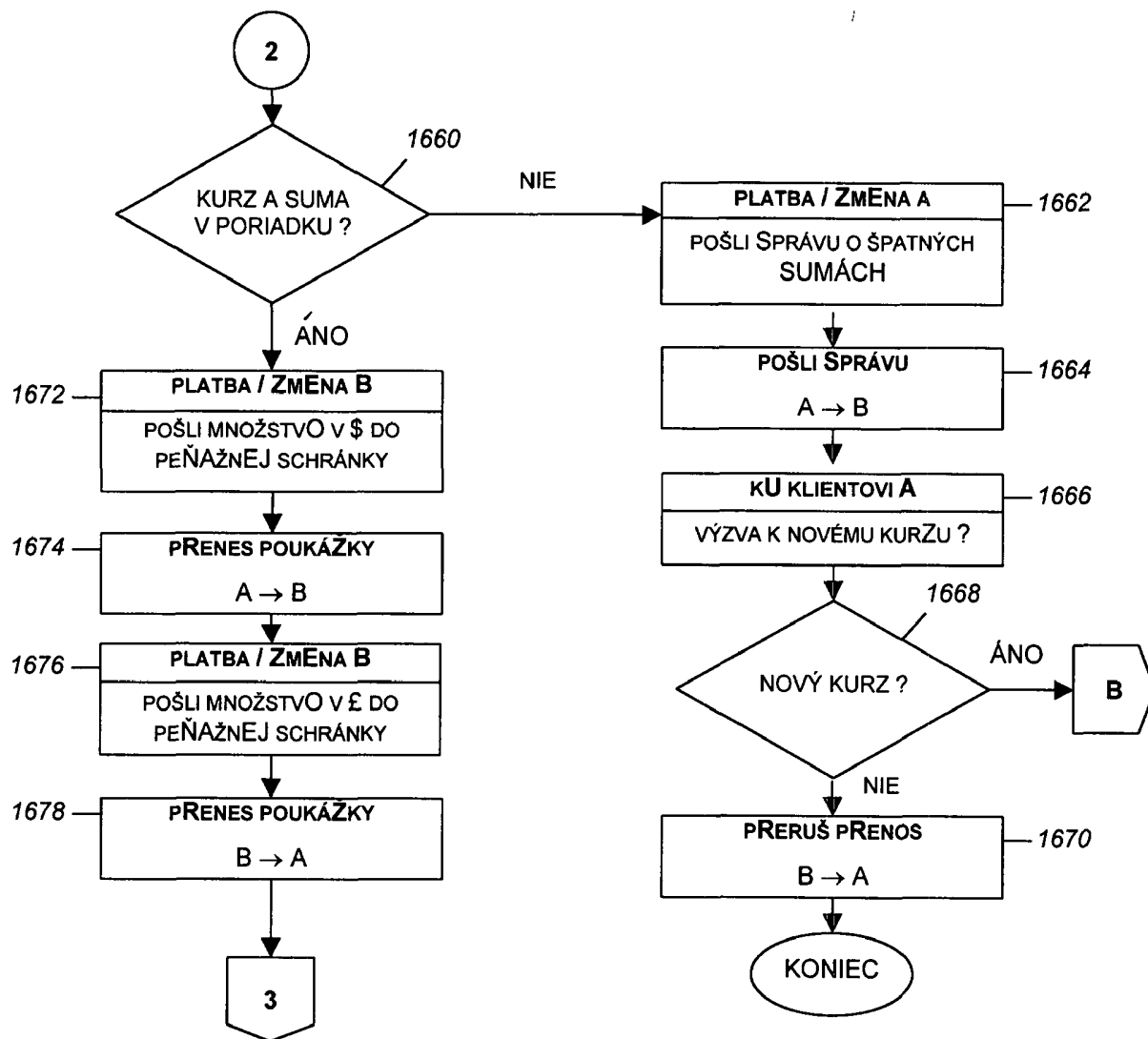
Obr. 9A

25/54



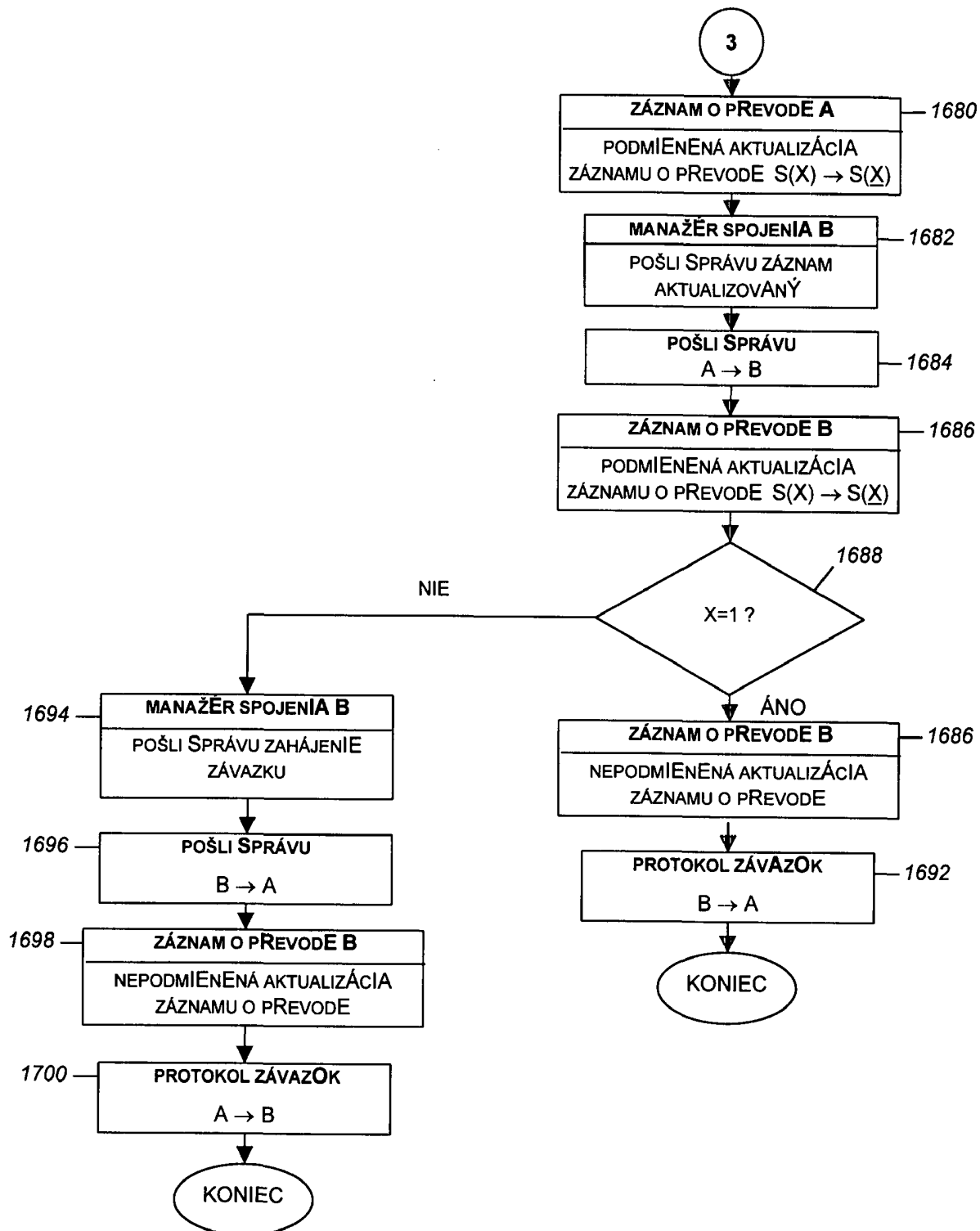
Obr. 9B

26/54



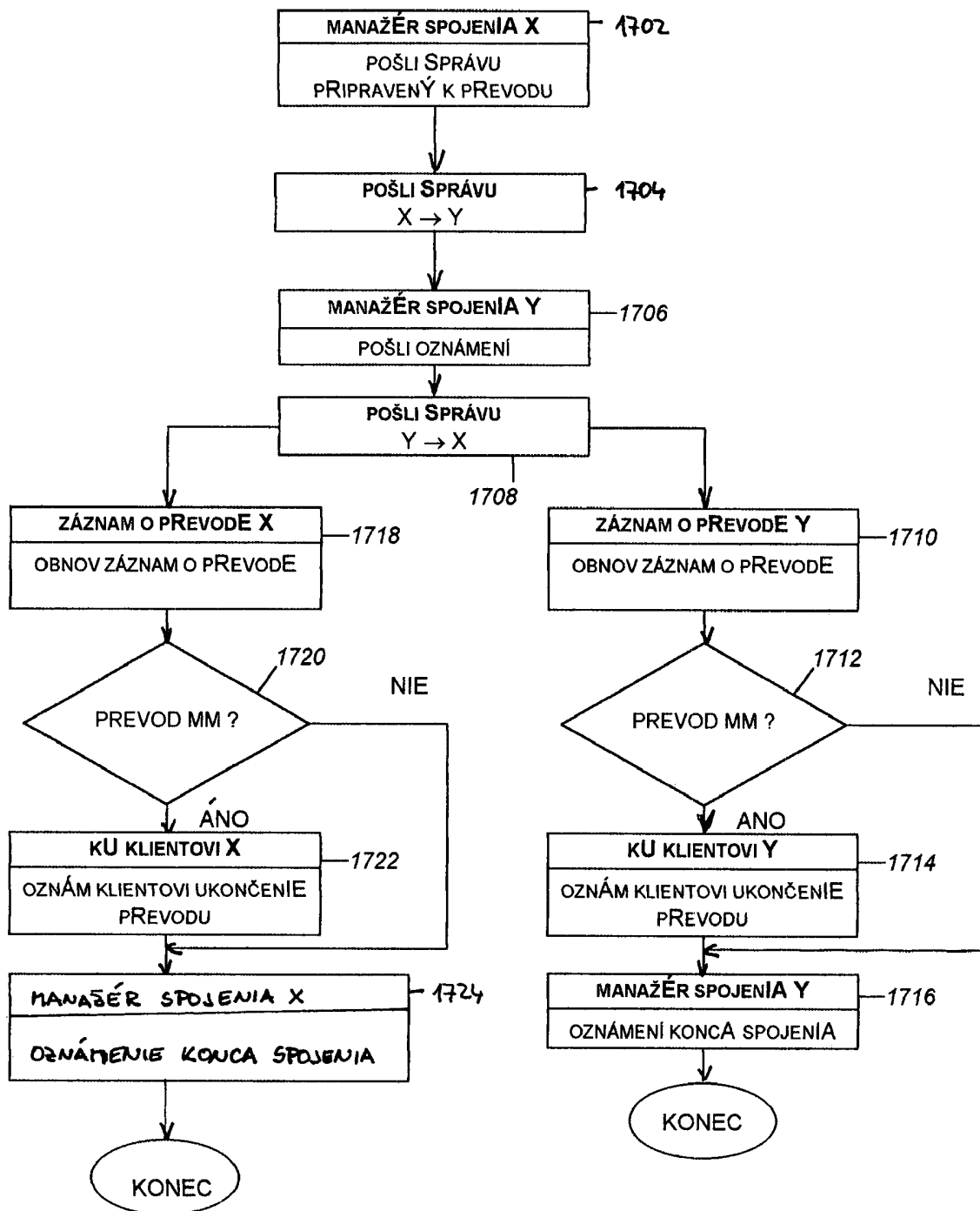
Obr. 9C

27/54



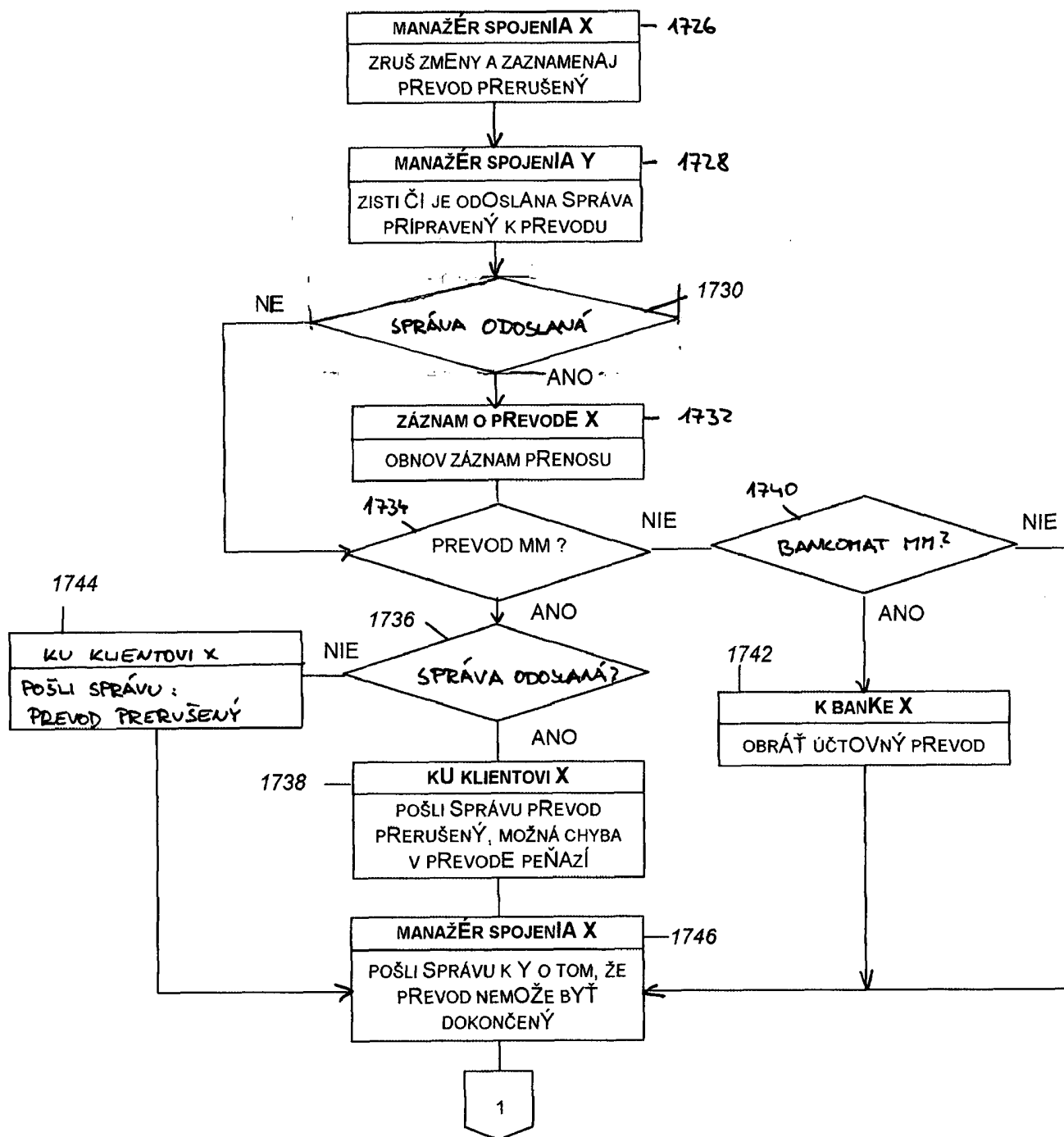
Obr. 9D

28/54



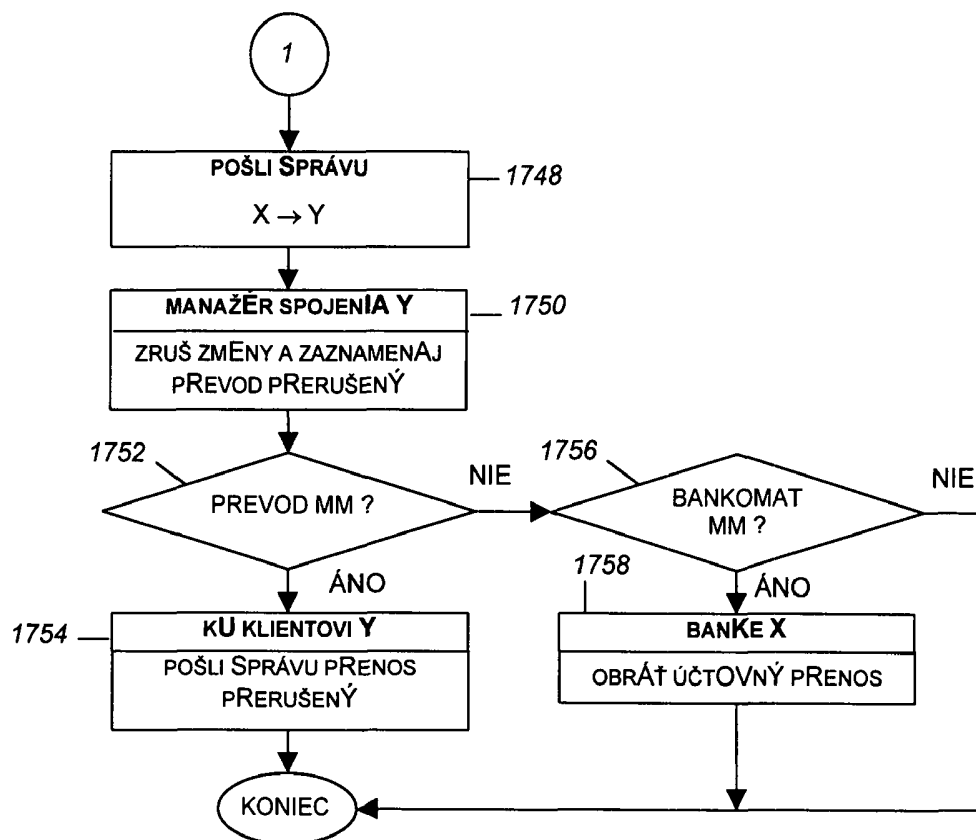
Obr. 10

29/54



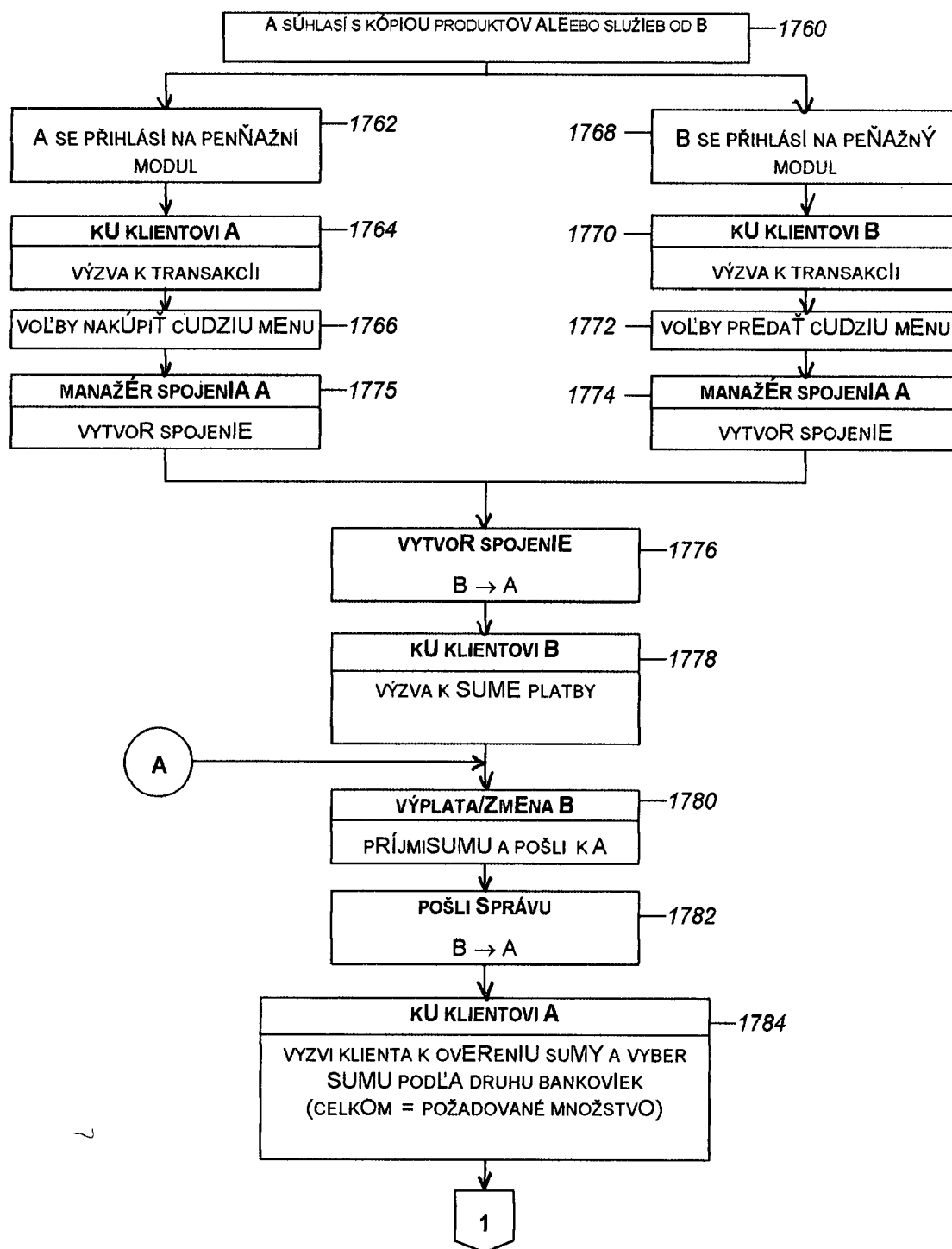
Obr. 11A

30/54



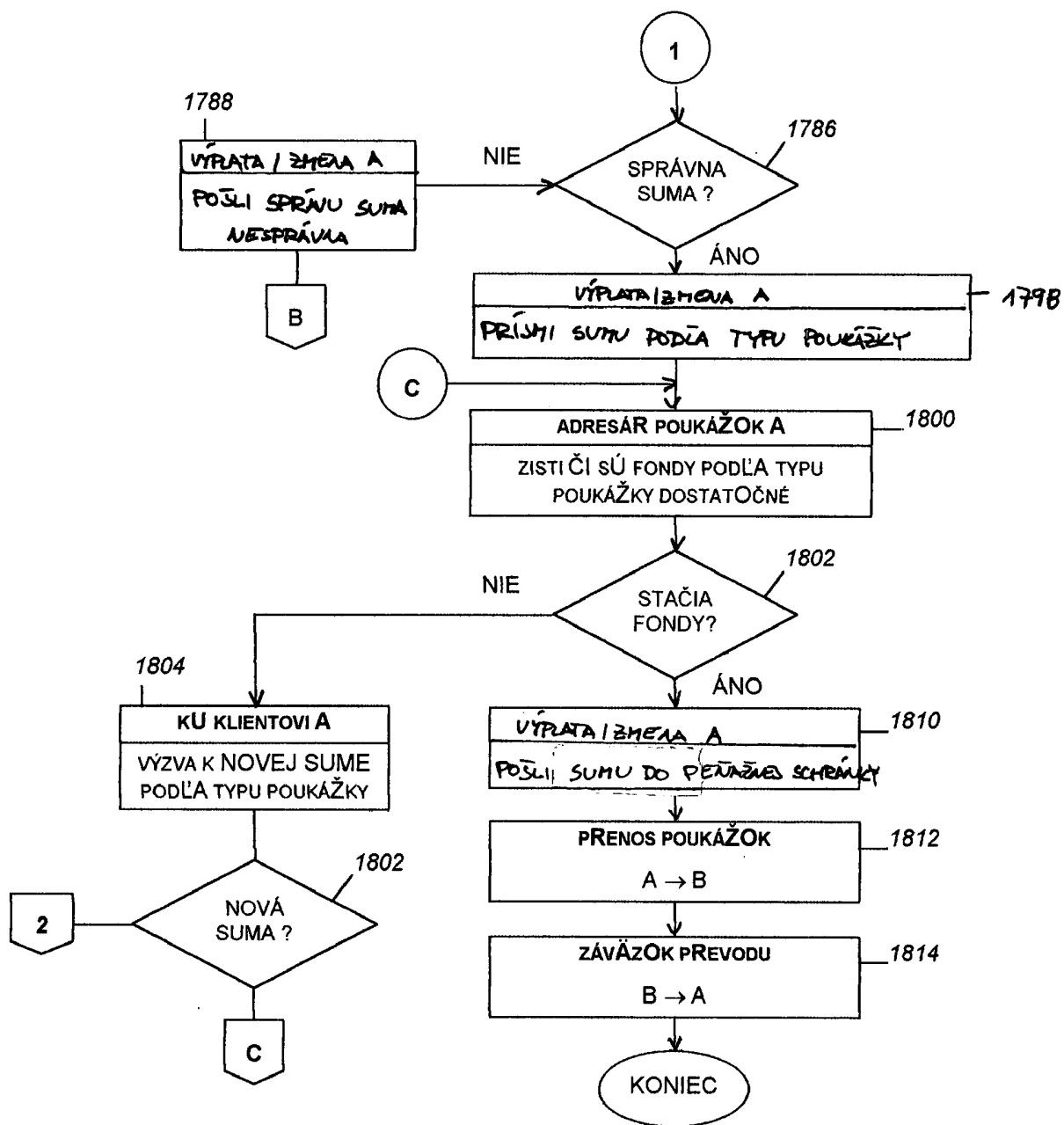
Obr. 11B

31/54



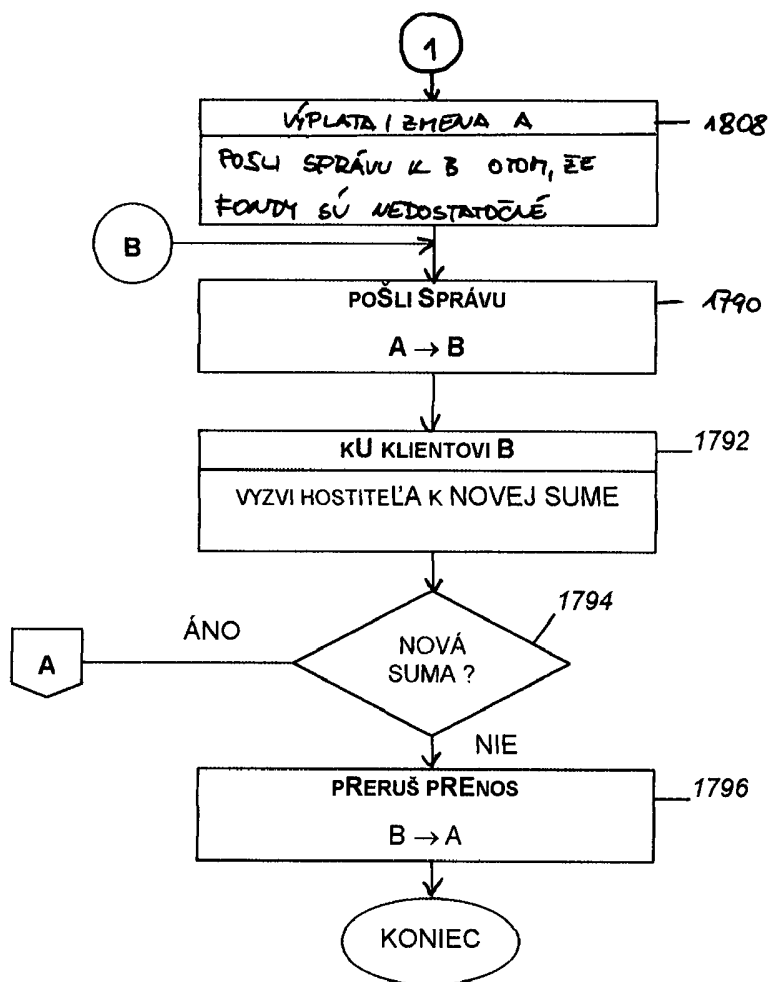
Obr. 12A

32/54



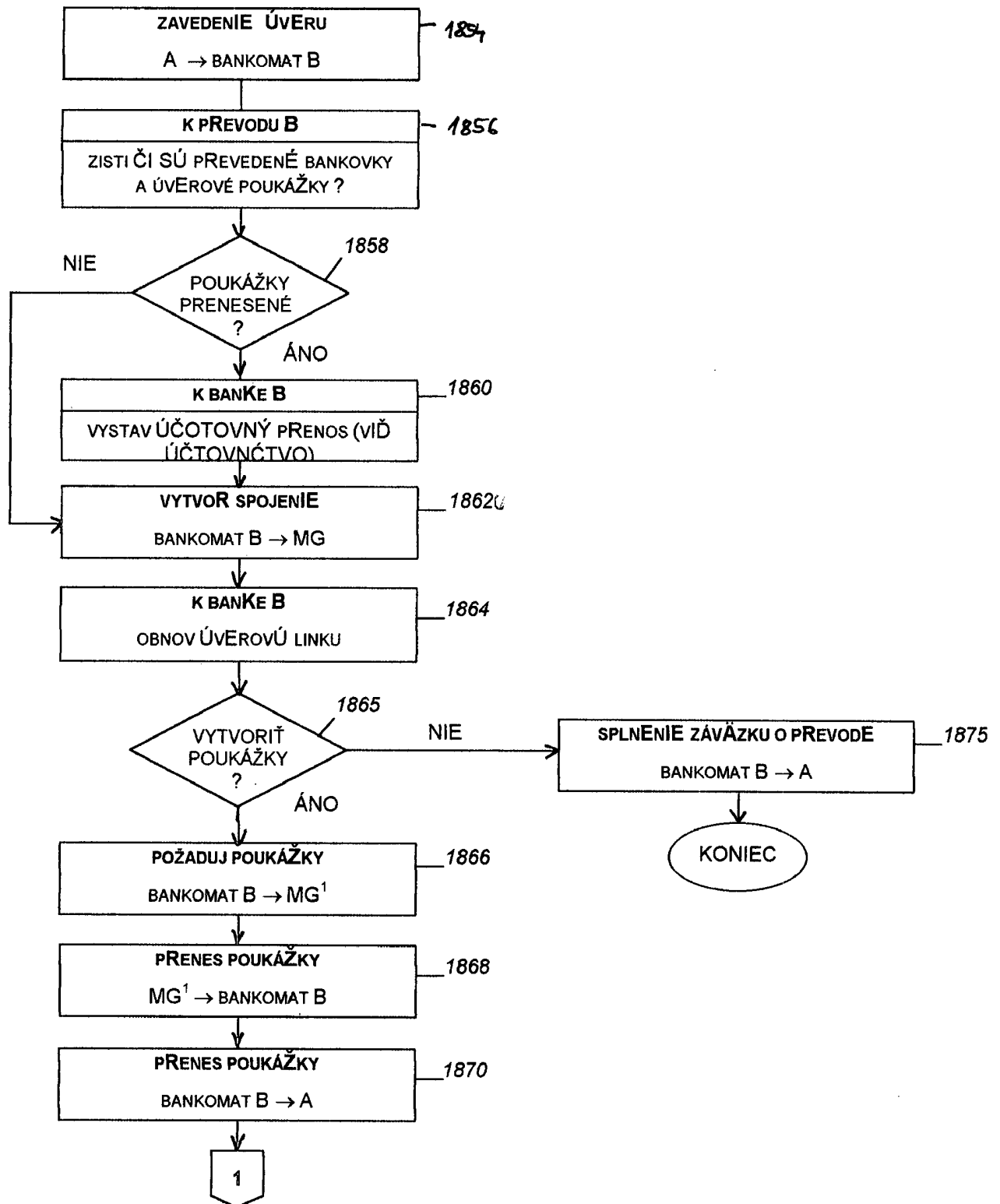
Obr. 12B

33/54



Obr. 12B

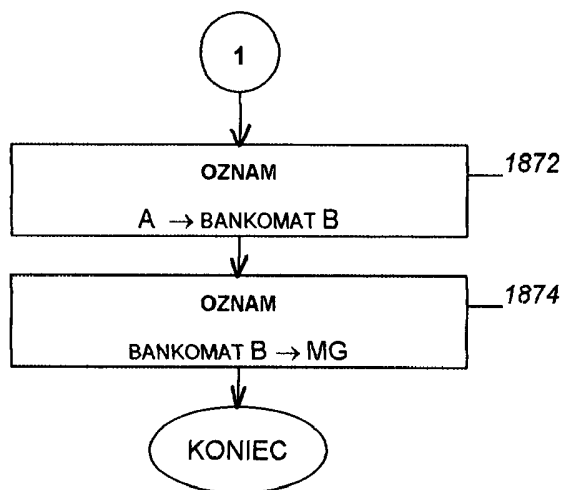
34/54



Obr. 13A

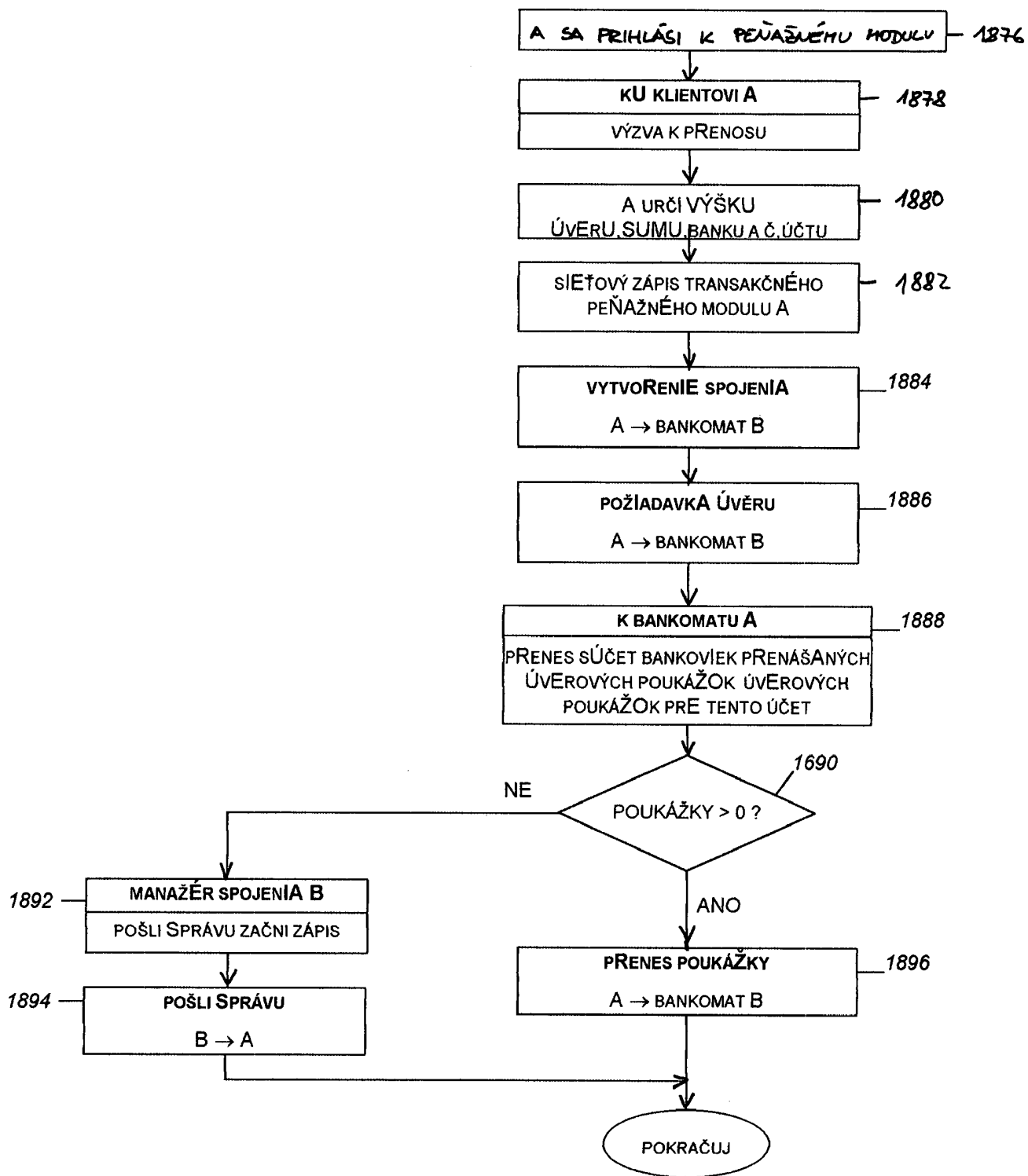
1 táto skratka nie je vysvetlená (pozn.prekl.)

35/54



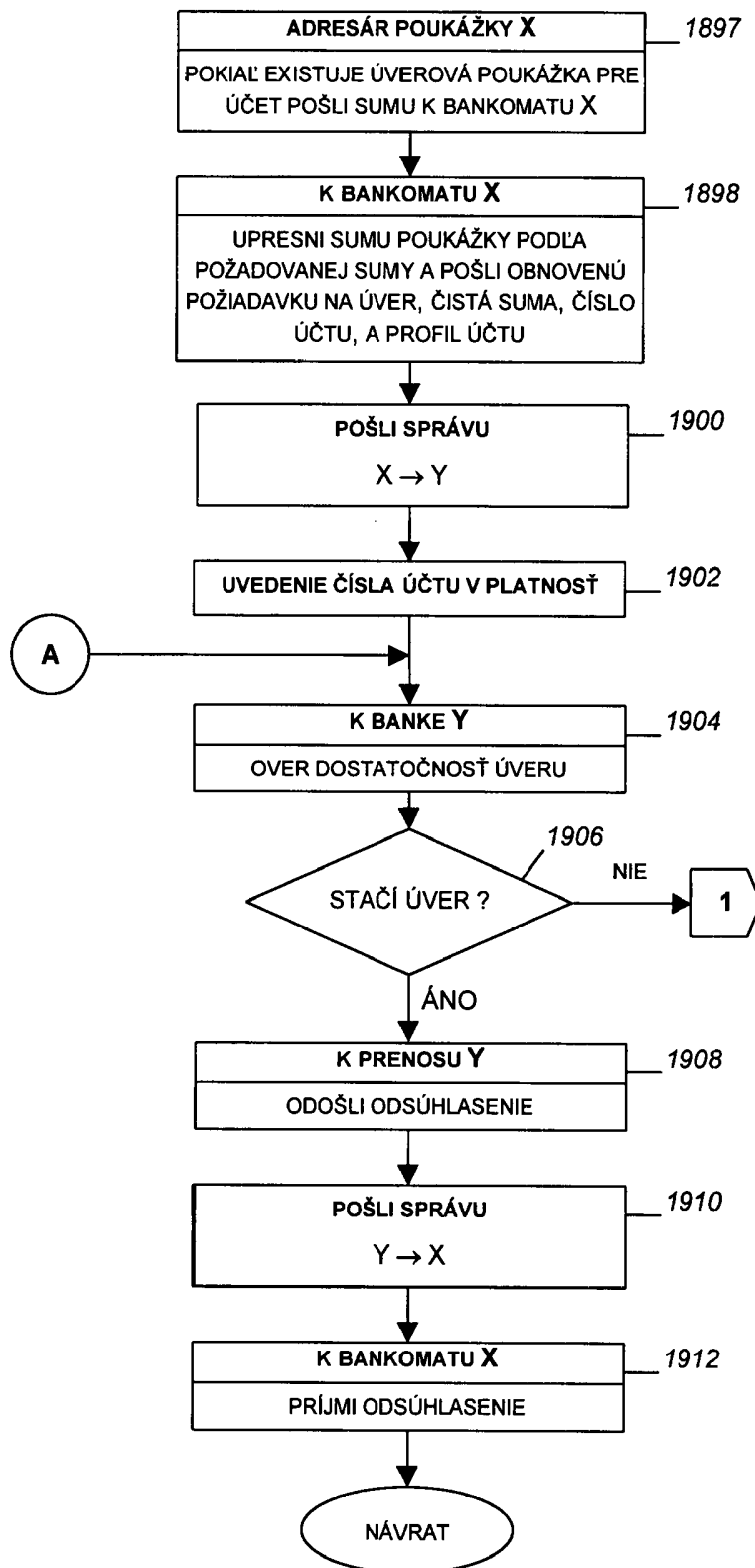
Obr. 13A

36/54



Obr. 14

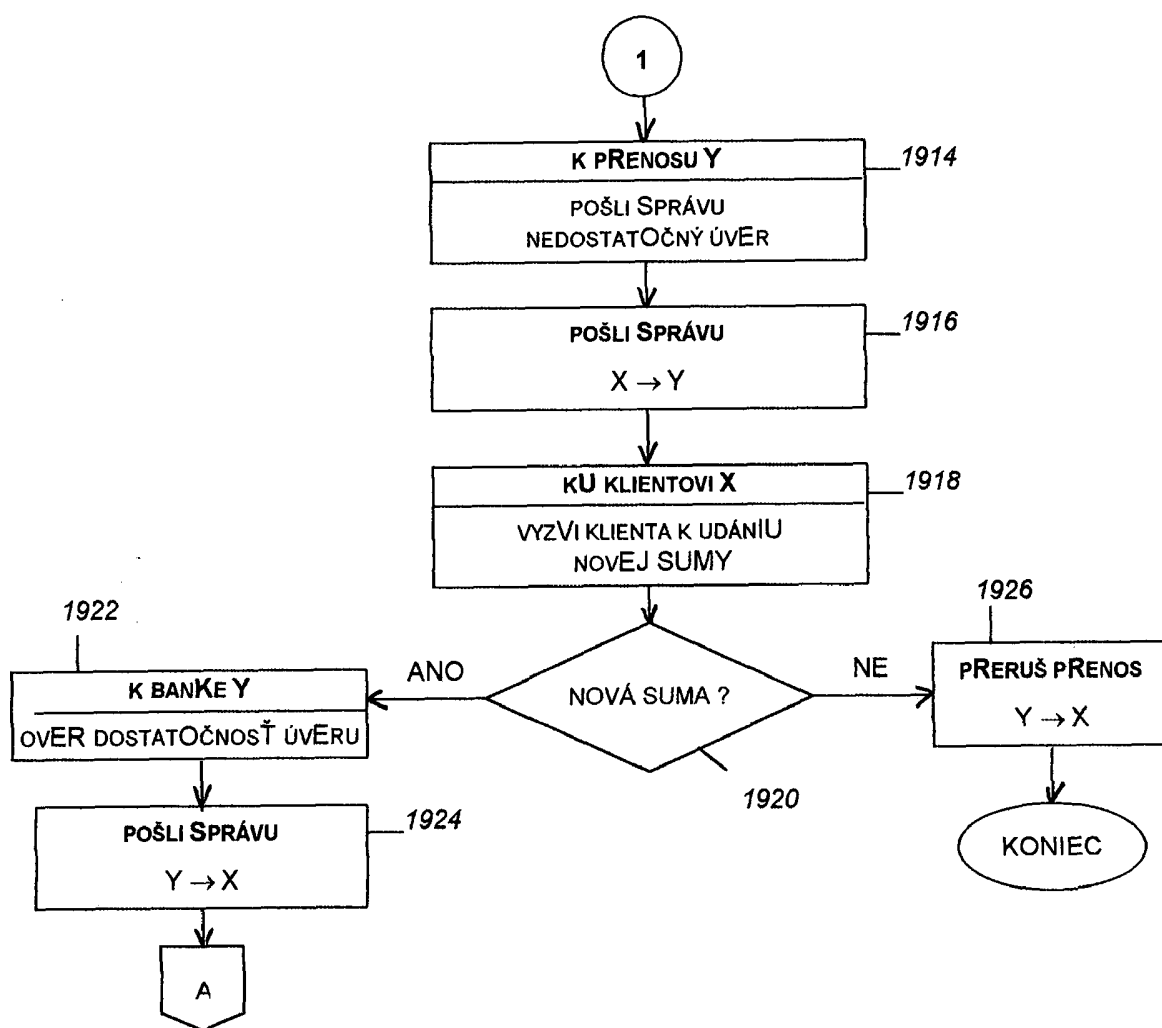
37/54



Obr. 15A

38/54

PV 1426-97



Obr. 15B

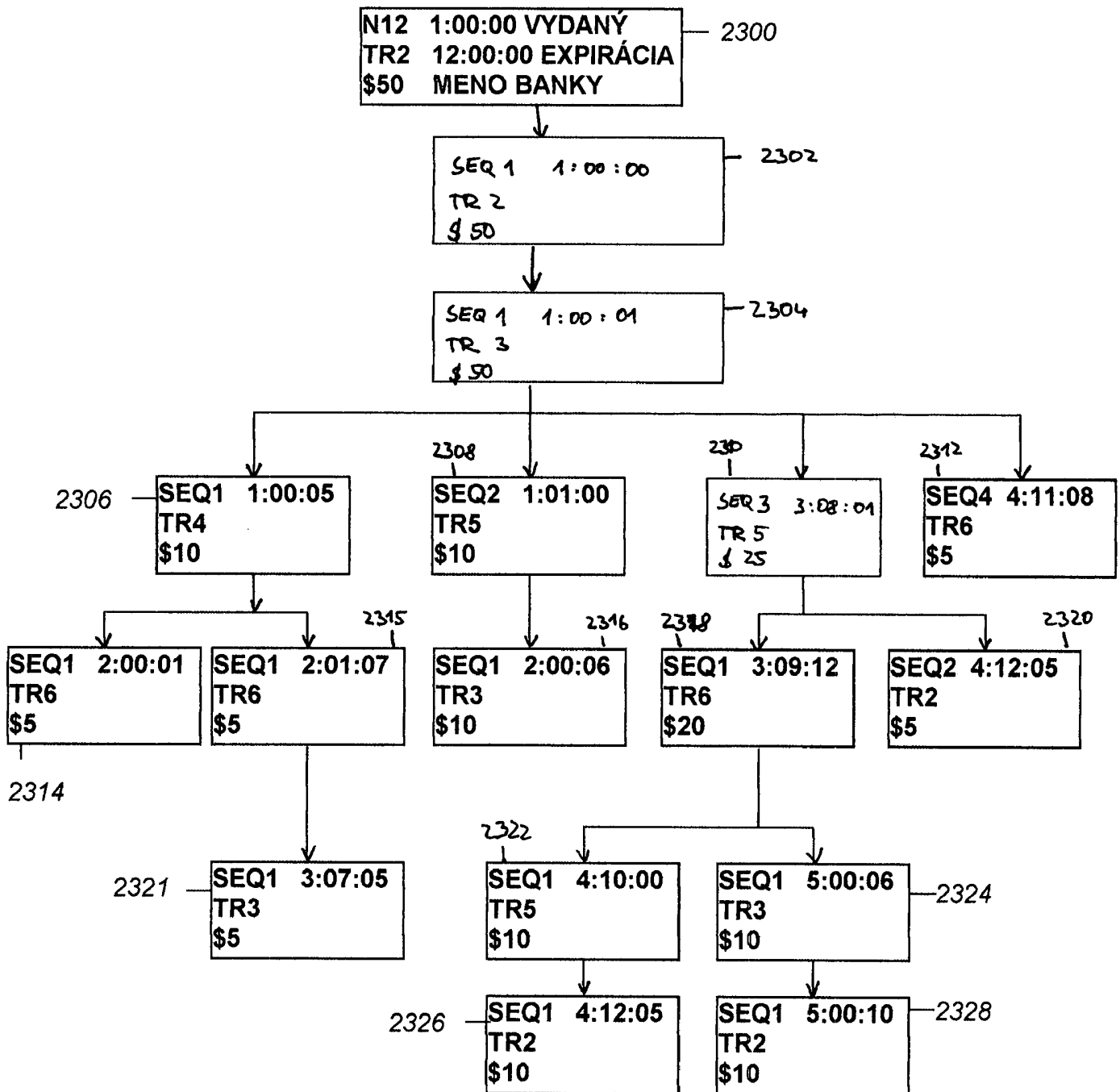
39/54

DÁTUM/ČAS	MG BANKOMAT		PRENOS			
	1	2	3	4	5	6
1:00:00	<u>VYTVOŘ</u> \$ 50 →					
1:00:01		<u>VYBER</u> \$ 50 →				
1:00:05			<u>VYPLATĚ</u> \$ 10 →			
1:01:00			<u>VYPLATĚ</u> \$ 10 →			
2:00:01				<u>VYPLATĚ</u> \$ 10 →		
2:00:06				<u>VYPLATĚ</u> \$ 10 ←		
2:01:07				<u>VYPLATĚ</u> \$ 5 →		
3:07:05				<u>VYPLATĚ</u> \$ 5 ←		
3:08:01				<u>VYPLATĚ</u> \$ 25 →		
3:09:12					<u>VYPLATĚ</u> \$ 20 →	
4:10:00					<u>VYPLATĚ</u> \$ 10 ←	
4:11:08				<u>VYPLATĚ</u> \$ 5 →		
4:12:05				<u>ZÁLOHA</u> \$ 5 ←		
5:00:06				<u>VYPLATĚ</u> \$ 10 ←		
5:00:10				<u>ZÁLOHA</u> \$ 10 ←		

Obr. 16

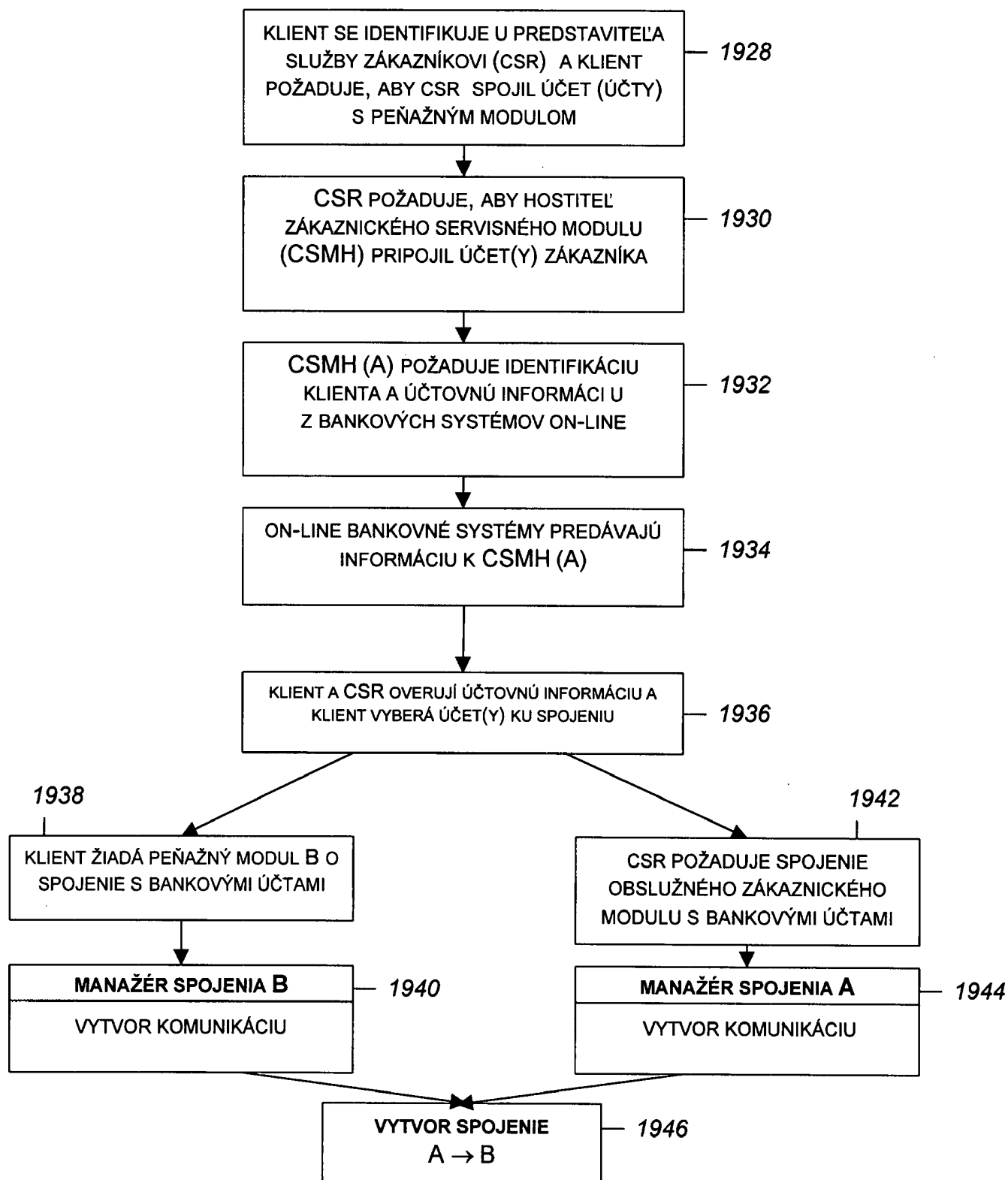
NÁHRADNÝ LIST (PRAVIDLO 26)

40/54



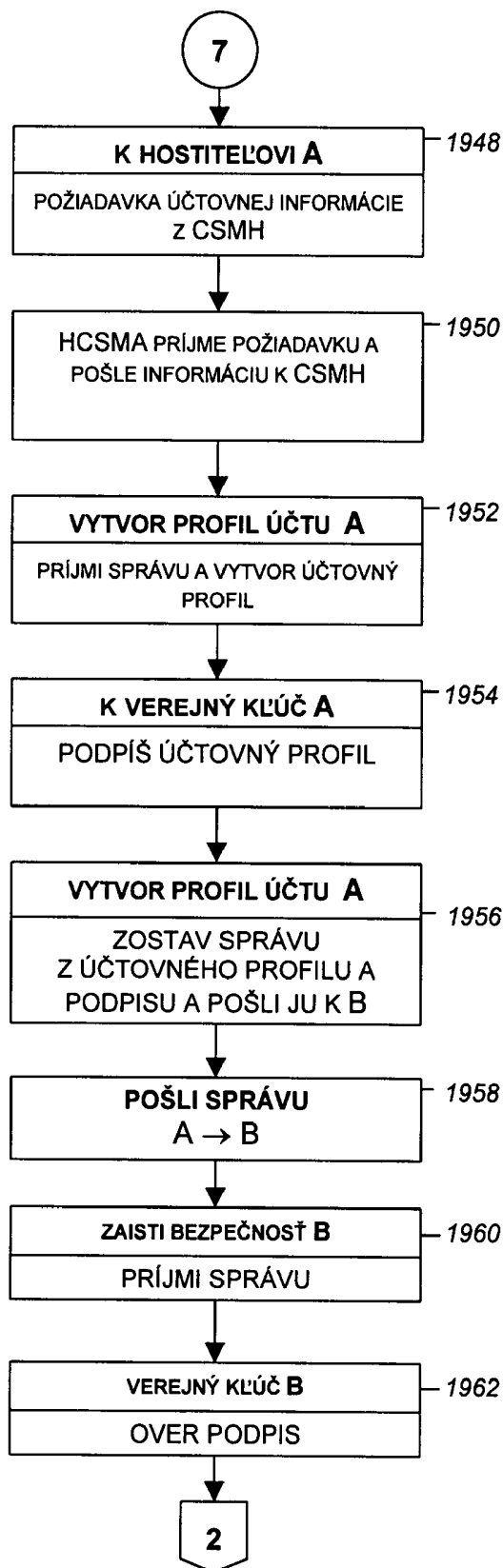
Obr. 17

41/54



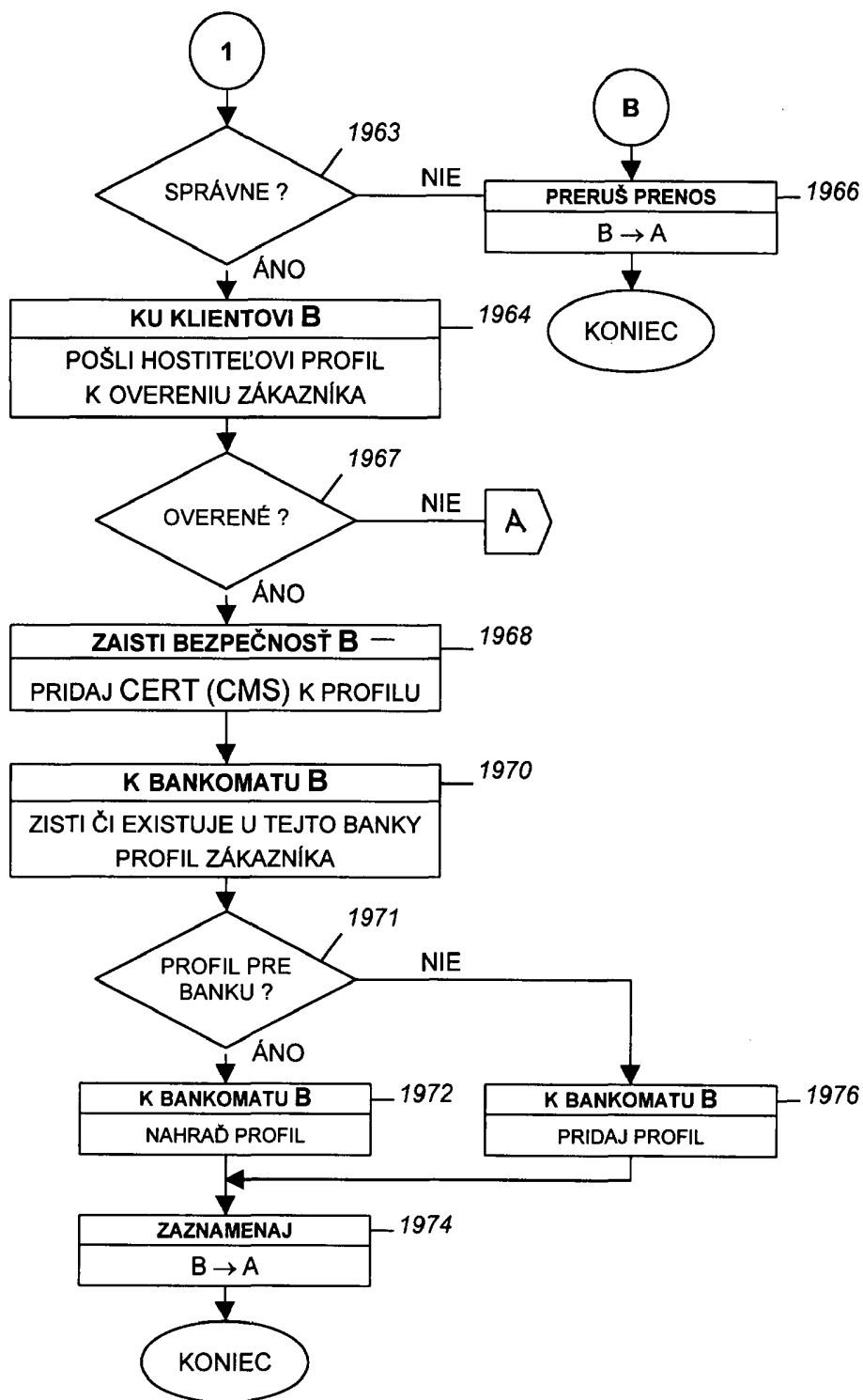
Obr. 18A

42/54



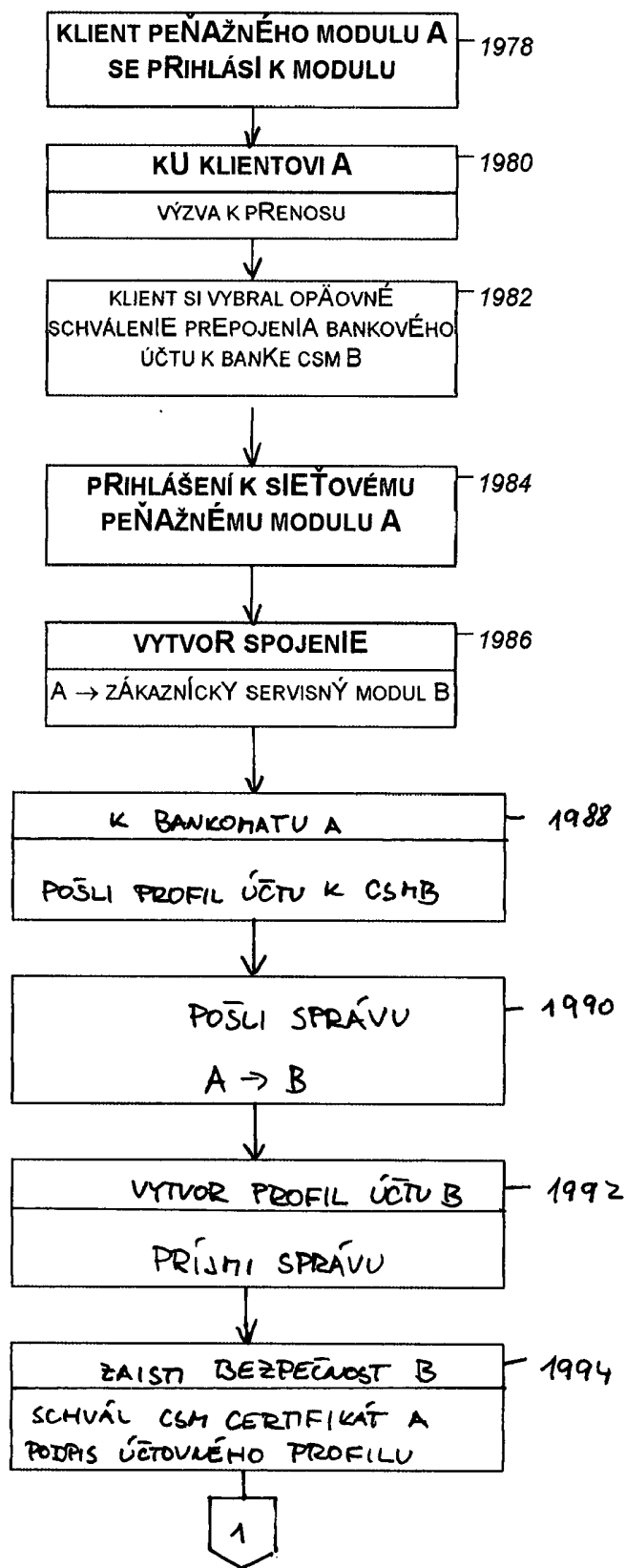
Obr.18B

43/54



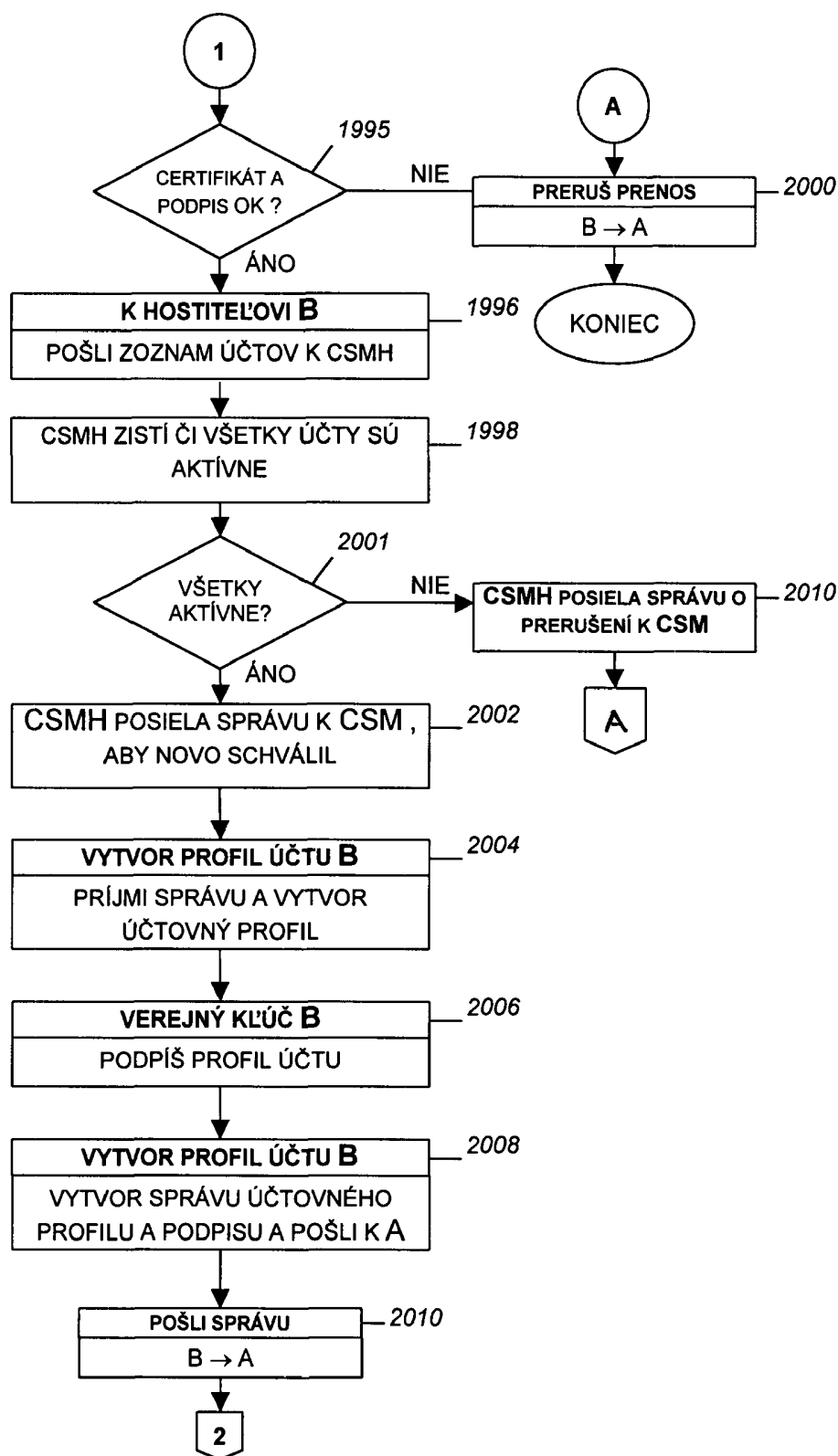
Obr. 18C

44/54



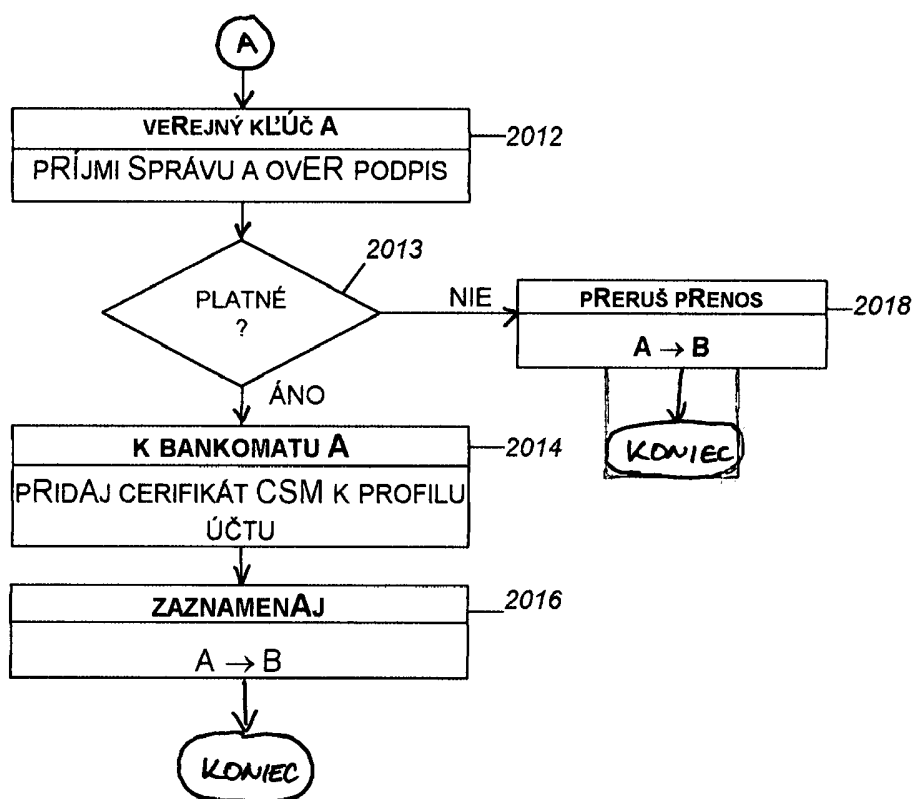
Obr. 19A

45/54



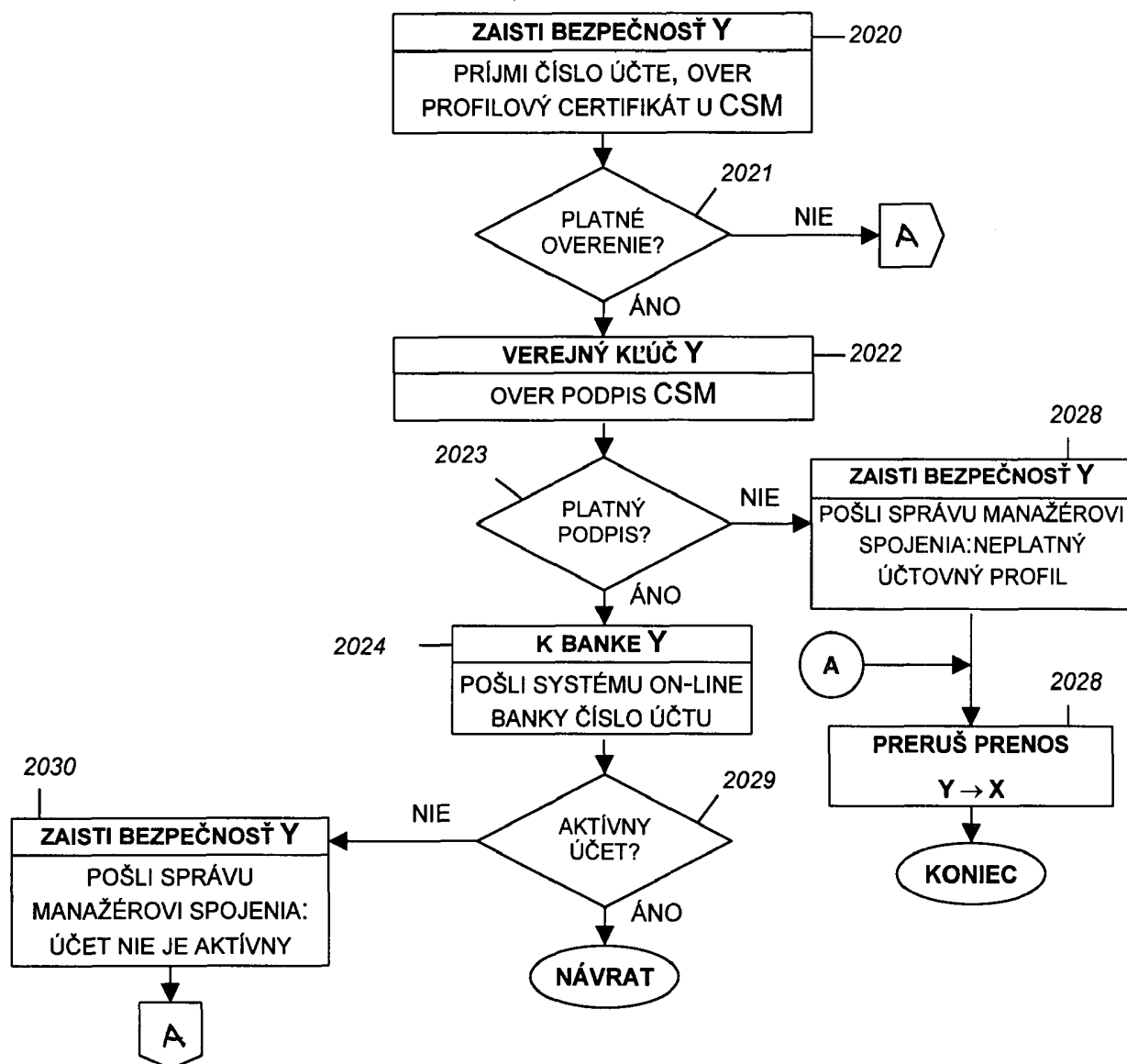
Obr. 19B

46/54



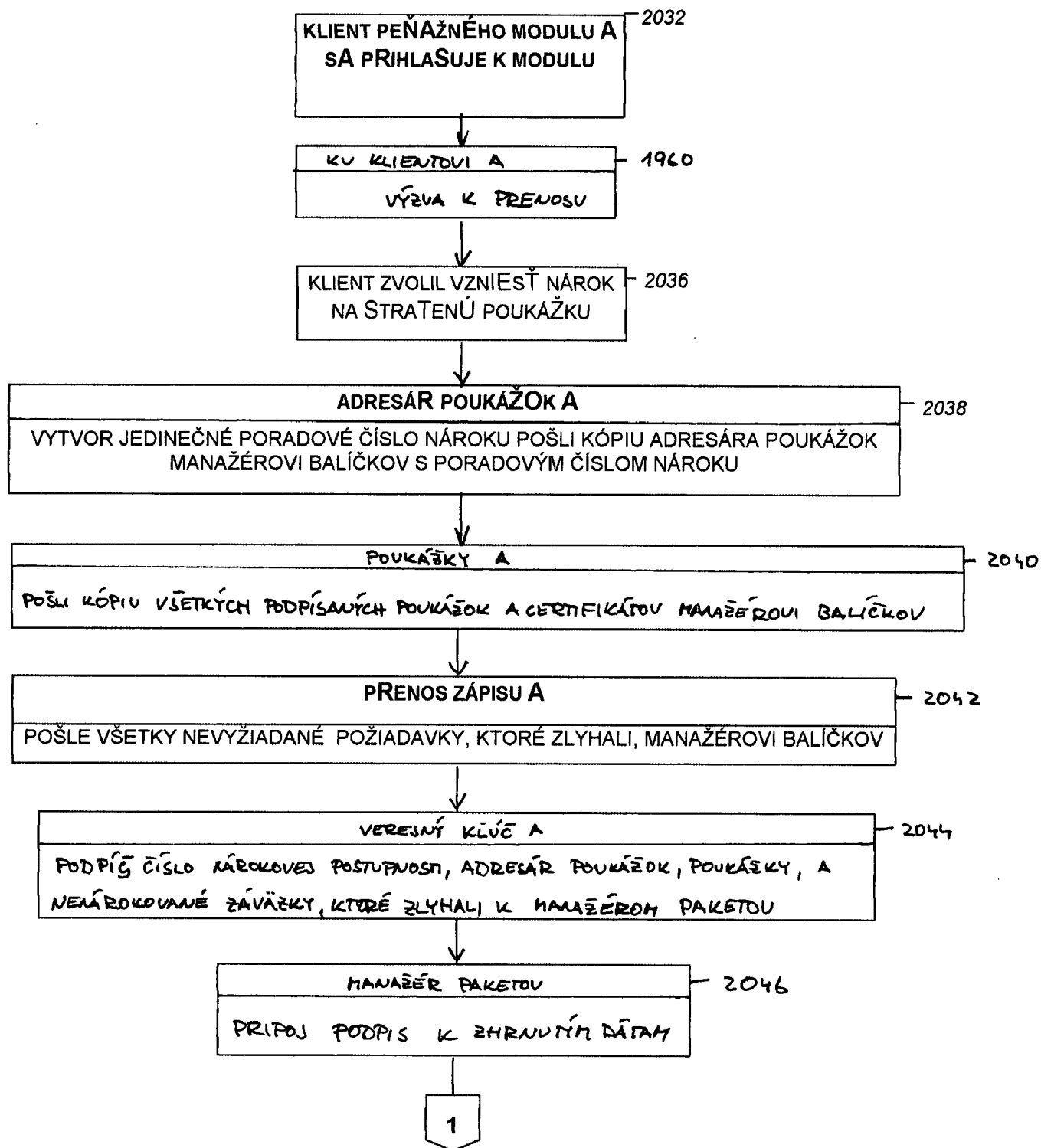
Obr. 19C

47/54



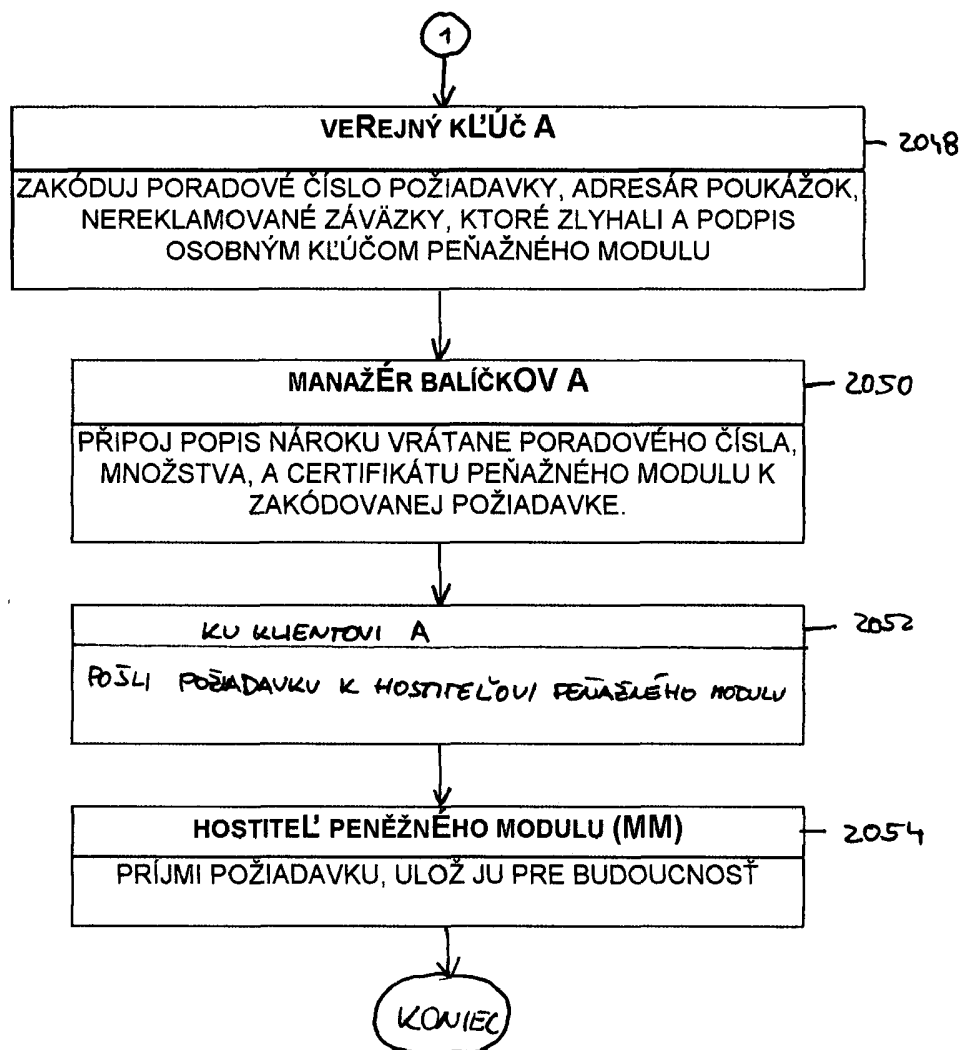
Obr. 20

48/54



Obr.21A

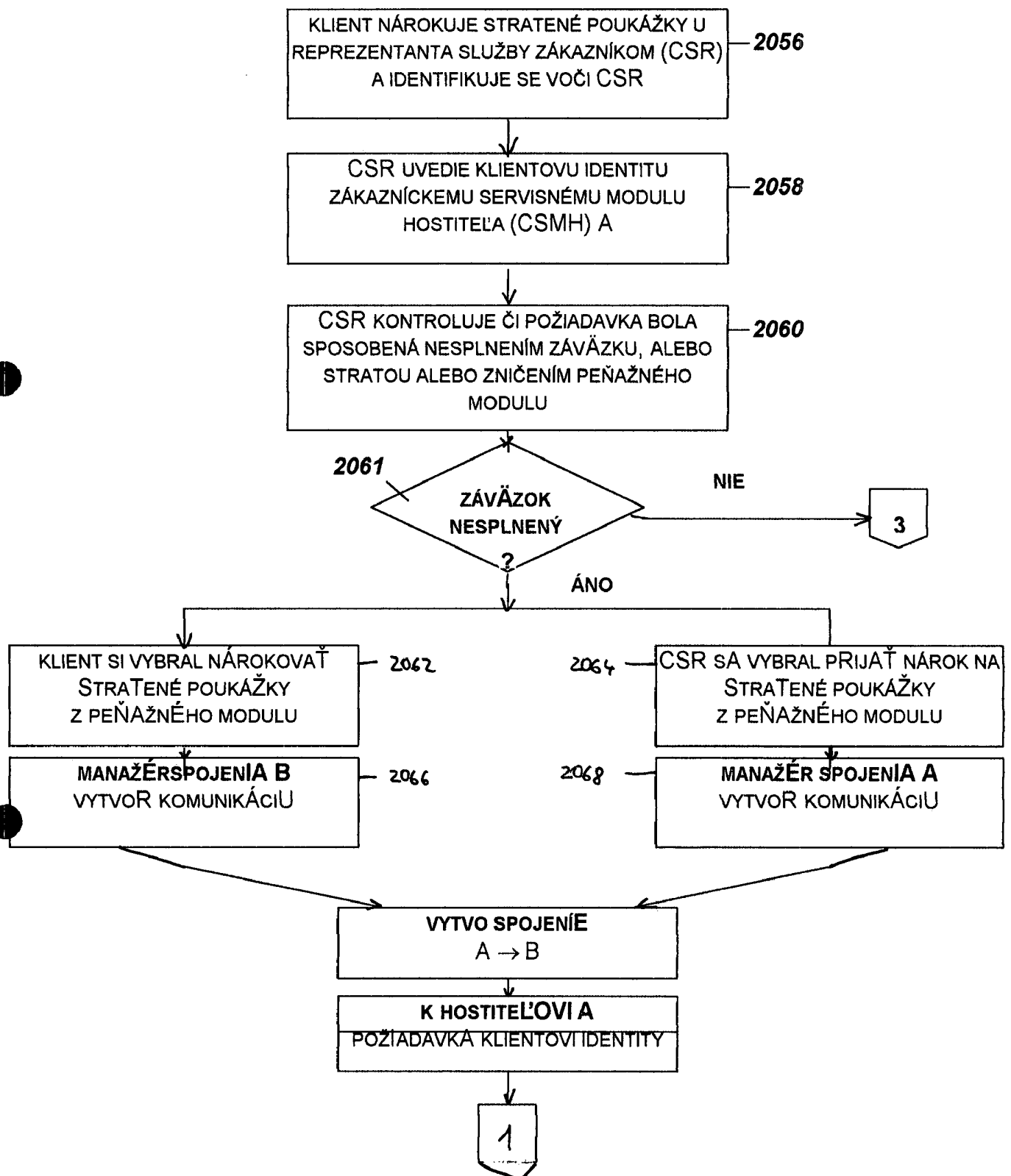
49/54



Obr.21B

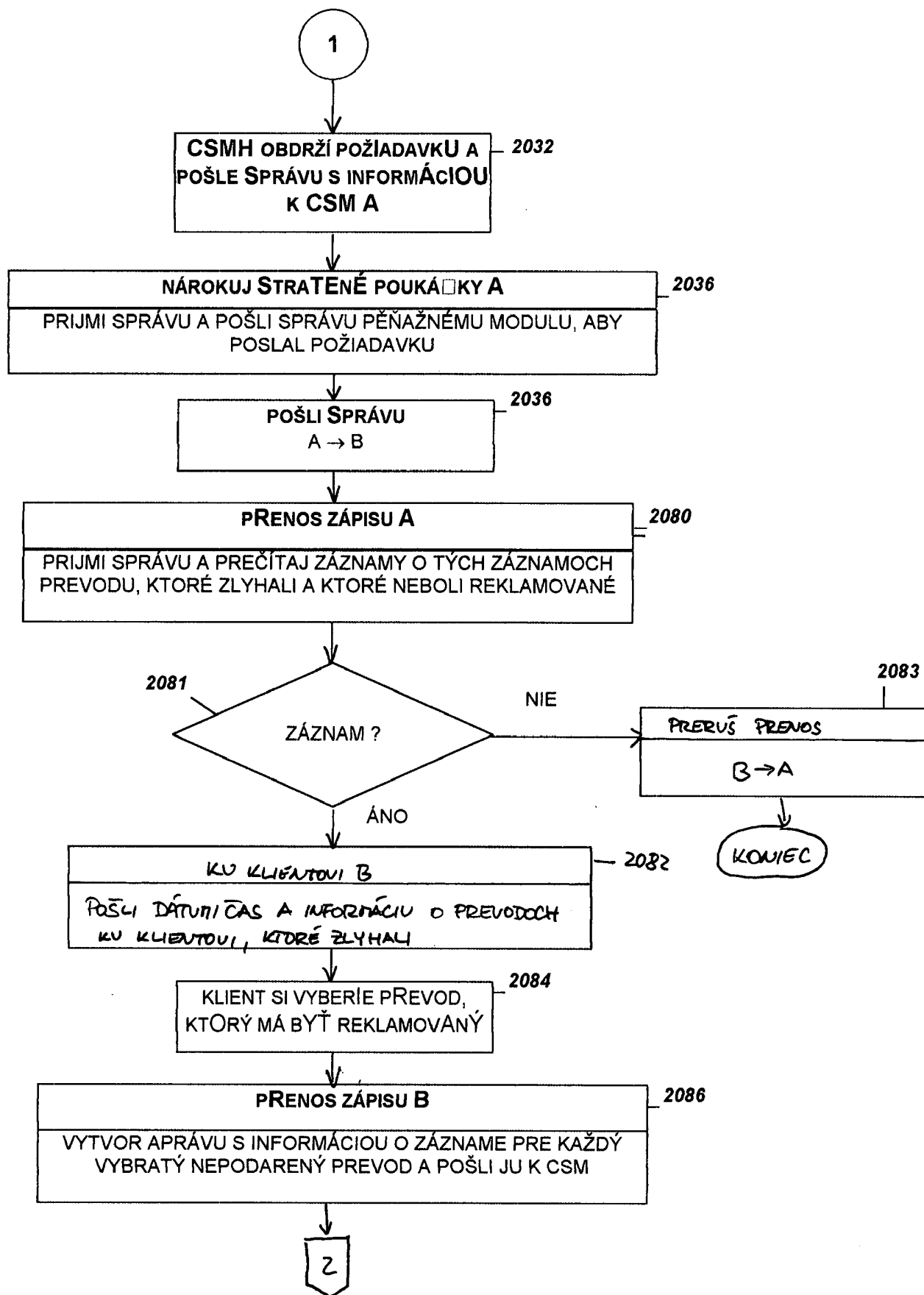
NÁHRADNÝ LIST (PRAVIDLO 26)

50/54



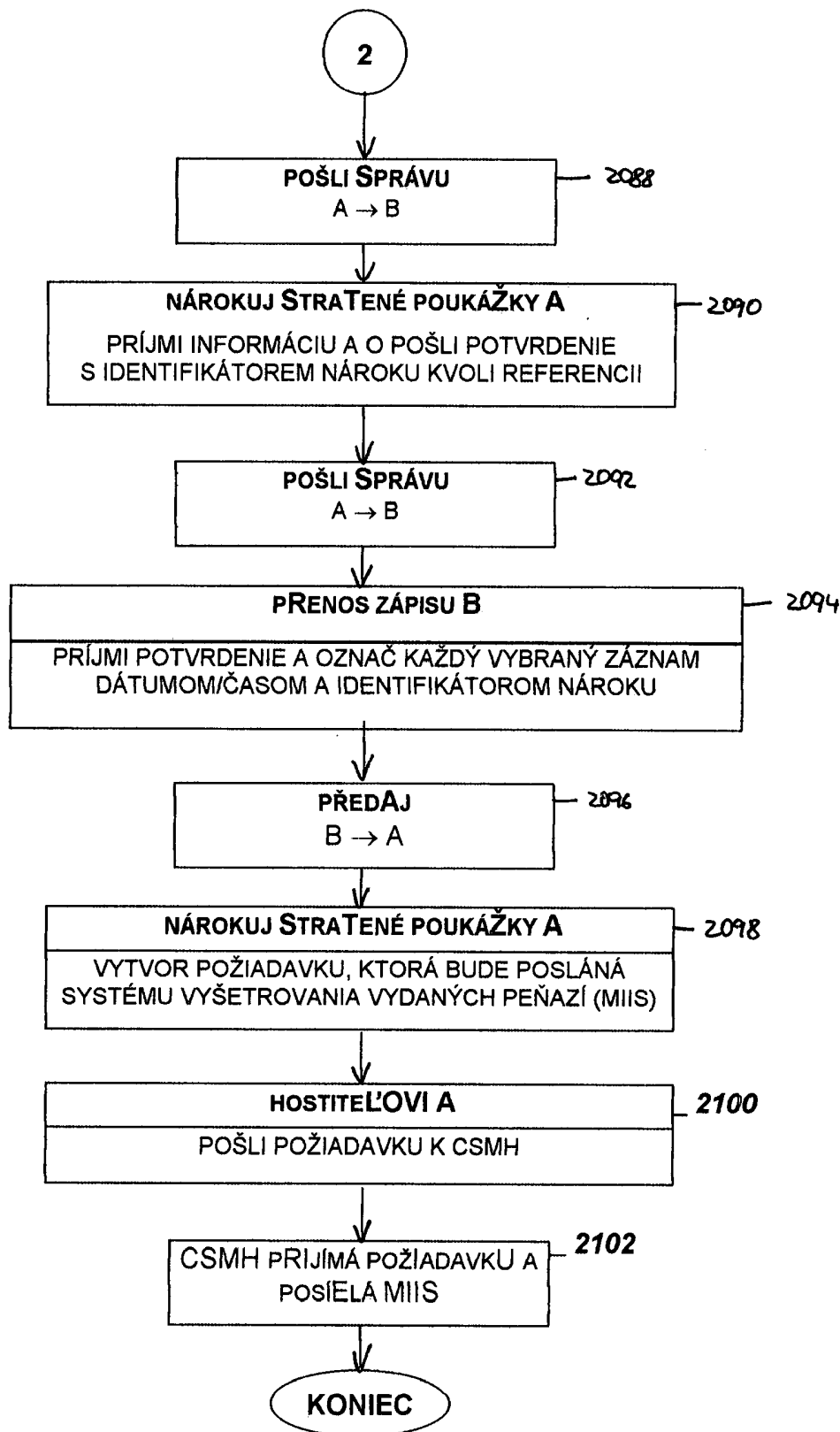
Obr. 22A

51/54



Obr.22B

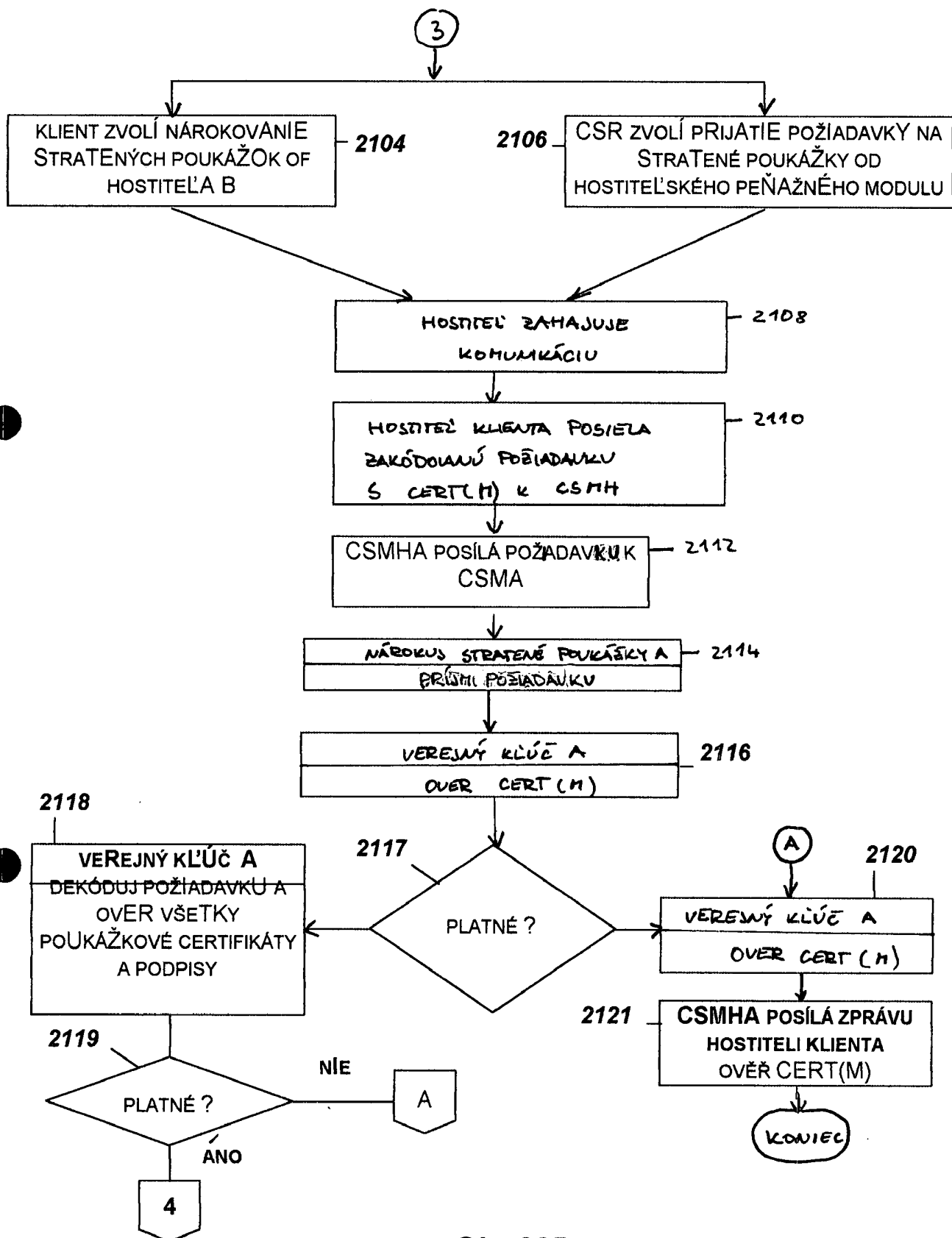
52/54



Obr.22C

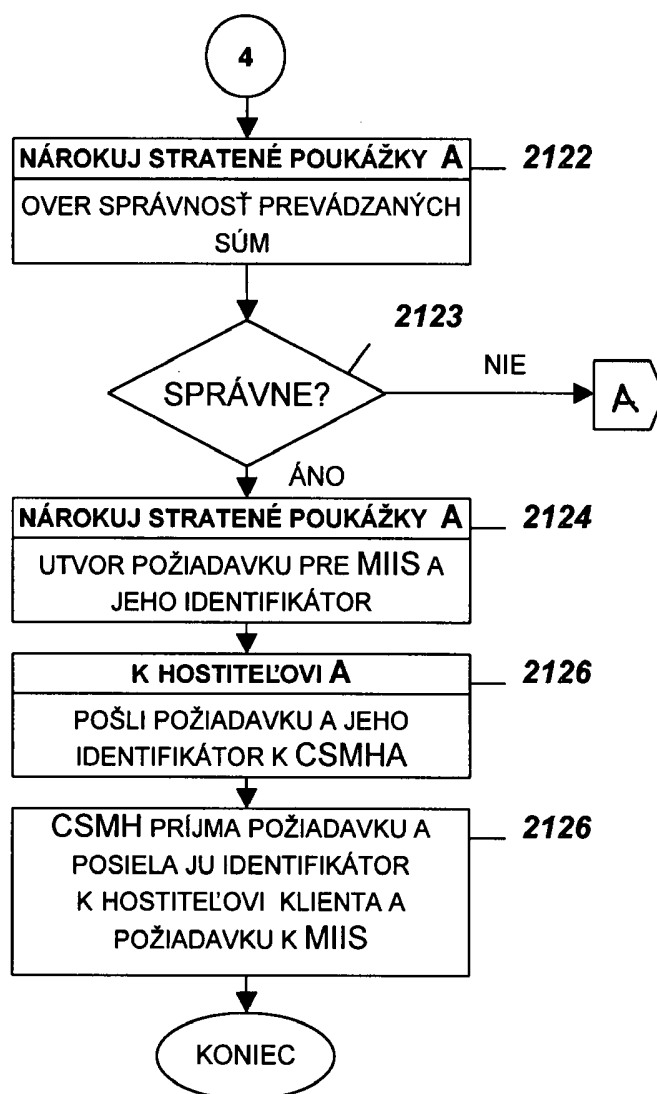
NÁHRADNÝ LIST (PRAVIDLO 26)

53/54



Obr.22D

54/54



Obr. 22E