PŘIHLÁŠKA VYNÁLEZU

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

(21) Číslo dokumentu:
1999 - 3319

(13) Druh dokumentu: **A3**

(51) Int. Cl.[7]:
H 04 N 7/16
H 04 N 7/173

(19)
ČESKÁ
REPUBLIKA

ÚŘAD
PRŮMYSLOVÉHO
VLASTNICTVÍ

(22) Přihlášeno: **25.04.1997**

(32) Datum podání prioritní přihlášky: **21.03.1997**

(31) Číslo prioritní přihlášky: **1997/97400650**

(33) Země priority: **EP**

(40) Datum zveřejnění přihlášky vynálezu: **14.06.2000**
(Věstník č. 6/2000)

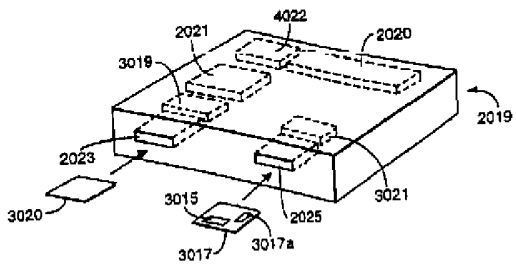
(86) PCT číslo: **PCT/EP97/02117**

(87) PCT číslo zveřejnění: **WO98/43427**

(71) Přihlašovatel:
CANAL+ SOCIETE ANONYME, Paris, FR;

(72) Původce:
Bastien Jean-Paul, Maisse, FR;
Declerck Christophe, Senantes, FR;
Bayassi Mulham, Paris, FR;

(74) Zástupce:
Korejzová Zdeňka JUDr., Spálená 29, Praha 1, 110 00;



(54) Název přihlášky vynálezu:

Vysílací a přijímací systém, přijímač/dekodér a vzdálená řídící jednotka

(57) Anotace:

Přijímač/dekodér (2020) pro použití v digitálním satelitním rádiovém nebo televizním systému zahrnuje dekodér (2020) a prostředek pro přijetí kreditní nebo bankovní karty, nesoucí mikroprocesor (3017a), a prostředek pro interakci s uvedeným mikroprocesorem (3017a), když je kreditní nebo bankovní karta vložena do pracovní polohy v uvedeném přijímači/dekodéru (2020) pro umožnění čtení dat nesených uvedenou kreditní nebo bankovní kartou a zadávání dat do mikroprocesoru (3017a), neseného uvedenou kreditní nebo bankovní kartou. Do přijímače/dekodéru (2020) může být vysíláno PIN číslo bezpečným způsobem prostřednictvím dálkového ovladače, který je rovněž popsán. Aplikace vynálezu zahrnují PPV televizi (platby po shlédnutí), teleshopping a telebanking.

CZ 1999 - 3319 A3

Vysílací a přijímací systém, přijímač/dekodér a vzdálená řídící jednotka

Oblast techniky

Předkládaný vynález se týká vysílacího a přijímacího systému, zejména, ale ne výhradně, digitálního interaktivního satelitního televizního systému pro hromadný trh. Vynález se rovněž týká přijímače/dekodéru a dálkového ovladače pro tento přijímač/dekodér.

Přesněji se předkládaný vynález týká v hlavním aspektu tak zvaného placeného rádiového a/nebo televizního systému, kde uživatel/divák volí program/film/hru pro sledování, za který má být provedena platba, což je označováno jako událost platby za shlédnutí (PPV) nebo v případě dat určených ke stažení jako tak zvaná událost platby za soubor (PPF).

Dosavadní stav techniky

S takovýmito známými PPV nebo PPF systémy je po koncovém uživateli/divákovi požadováno, aby nejprve interagoval se systémem za účelem nejen zvolení produktu, který má být dodán, ale v některých případech rovněž za účelem provedení platby za tuto dodávku. Termín "produkt" je zde použit pro označení jakéhokoliv programu, filmu nebo jiné události nebo dat, který má být přenášen buď do televizního zařízení koncového uživatele nebo do osobního počítače sdruženého se systémem.

Předkládaný vynález se rovněž týká systému nákupu prostřednictvím televize (teleshopping systém) nebo systému provádění bankovních operací prostřednictvím televize

(telebanking systém), ve kterých je ve spojení s vysílanou informací použita kreditní nebo bankovní karta pro provedení transakce, například nákupu položky nebo služby, která je předmětem reklamy.

Předkládaný vynález navrhuje zařízení zahrnující přijímač/dekodér pro použití při příjmu televizního nebo rádiového programu nebo datového souboru, přičemž toto zařízení zahrnuje prostředek pro interakci s kreditní nebo bankovní kartou uživatele pro čtení informace nesené touto kartou.

Takové uspořádání může usnadnit placení za produkty s minimálními požadavky na součinnost s uživatelem.

Bankovní nebo kreditní karta může nést data na magnetickém pásku (nebo jiném "pasivním" datovém nosiči). Zvláště výhodně ale kreditní nebo bankovní karta obsahuje mikroprocesor (nebo jiné "aktivní" zařízení pro ukládání dat) a zařízení je uspořádáno pro spolupráci s tímto mikroprocesorem a výhodně je uspořádáno pro poskytování informace tomuto mikroprocesoru. To může zajistit, aby byla udržena vysoká úroveň bezpečnosti, přičemž zároveň to může usnadnit přenos informace.

Zařízení výhodně dále zahrnuje prostředek pro vysílání do vzdáleného centra debetních instrukcí na základě informace nesené kartou pro provedení úhrady z kreditního nebo bankovního účtu uživatele.

V jednom výhodném provedení je zařízení výhodně uspořádáno pro příjem autorizační informace ze vzdáleného centra a pro řízení dekódování a/nebo dešifrování programu

nebo souboru v závislosti na autorizační informaci. To může usnadnit poskytování PPV nebo PPF služeb.

V dalším výhodném provedení zařízení dále zahrnuje prostředek pro interakci s inteligentní kartou obsahující účastnické informace (informace o účastníkovi a jeho předplatném), přičemž dekódování nebo dešifrování je řízeno v závislosti na účastnické informaci. Inteligentní karta může rovněž obsahovat informaci dekódovacího kliče a informaci týkající se kanálů, které má uživatel (účastník) předplacené.

Výhodně je zařízení uspořádáno pro uložení přijímané kreditní informace, reprezentující kredity dostupné pro nákup produktů, do paměťového prostředku inteligentní karty, přičemž výhodně zařízení zahrnuje prostředek pro modifikaci přijímané kreditní informace pro snížení dostupných kreditů o předem stanovené množství v odezvě na přijetí programu nebo souboru. Tímto způsobem uživatel může uložit kredity pro nákup produktů (PPV programů nebo PPF souborů) na inteligentní kartě.

V jednom výhodném provedení je zařízení uspořádáno pro vysílání debetních instrukcí, výhodně na žádost uživatele, do vzdáleného centra a pro modifikaci přijaté kreditní informace uložené v inteligentní kartě, výhodně při příjmu autorizační informace, pro zvýšení počtu kreditů uložených na inteligentní kartě v závislosti na platbě prostřednictvím bankovní nebo kreditní karty. Tímto způsobem uživatel může nakupovat kredity s použitím bankovní nebo kreditní karty, které budou uloženy na inteligentní kartě pro pozdější použití.

Zvláště výhodně je zařízení uspořádáno pro provádění nákupu dostatečného množství přijímaných kreditů pro umožnění nakupování množství produktů při každé transakci, ve které je do vzdáleného centra vysílána debetní instrukce. To může omezit počet požadovaných transakcí se vzdáleným centrem a může to zlepšit bezpečnost snížením počtu příležitostí, při kterých musí být vysílány detaily z bankovních nebo kreditních karet.

V uspořádání obzvláště vhodném pro teleshopping zařízení zahrnuje prostředek pro zpracování dat, reprezentativních pro bankovní nebo kreditní kartu uživatele, společně s přijímanými daty, reprezentativními pro nabízenou položku nebo službu, a pro vysílání objednávací žádosti do vzdáleného centra pro zpracování. S takovým systémem může být zjednodušeno objednávání a placení nabízených produktů. Výhodně je rovněž použit prostředek pro zadávání žádosti od uživatele pro nákup zobrazovaného produktu nebo služby. To může zjednodušit nakupování do té míry, že se pouze po uživateli požaduje, aby potvrdil svůj zájem o nákup specifikované položky.

Zařízení může dále zahrnovat prostředek pro příjem osobního identifikačního čísla (PIN), výhodně sdruženého s kreditní nebo bankovní kartou, výhodně vysílaného bezpečným způsobem z dálkového ovladače pro autorizaci transakce.

Zřízení výhodně má formu nastavovací řídící skříně (STB), která je výhodně sama obsažena v jednotce zahrnující jak dekodér tak i obvody pro čtení karet. Zařízení ale může být také integrováno do televize, video rekordéru nebo do počítače.

Předkládaný vynález je obzvláště výhodně použit pro příjem satelitně vysílaných programů a souborů a zejména digitálních satelitních programů, protože tyto poskytují vhodnou kapacitu pro přenos dat, ačkoliv je samozřejmě rovněž použitelný pro kabelové a pozemní aplikace.

Obzvláště výhodným znakem vynálezu je to, že zařízení obsahuje další interaktivní prostředek pro interakci s (přídavnou) kartou uživatele pro čtení informace nesené touto kartou, přičemž uvedený prostředek je oddělený od uvedeného prostředku pro interakci s kreditní nebo bankovní kartou uživatele. Tímto zajištění vlastně dvou zařízení pro čtení karet může být dále zvýšena využitelnost zařízení podle vynálezu.

Tento důležitý aspekt je zajištěn nezávisle. Tudíž podle odpovídajícího aspektu předkládaného vynálezu je navrženo zařízení zahrnující přijímač/dekodér pro použití při příjmu televizního nebo rádiového programu nebo datového souboru, přičemž zařízení zahrnuje prostředek pro interakci s kreditní nebo bankovní kartou uživatele pro čtení informace nesené touto kartou a odděleně od tohoto prostředku zahrnuje další interaktivní prostředek pro interakci s kartou uživatele pro čtení informace nesené touto kartou.

Výhodně je tento další interaktivní prostředek uspořádán pro interakci s kartou obsahující mikroprocesor, přičemž tato karta je tak zvaná "inteligentní karta". Zvláště výhodně je zařízení uspořádáno pro poskytování informací tomuto mikroprocesoru.

Podle dalšího aspektu předkládaného vynálezu přijímač/dekodér pro použití v digitálním satelitním

televizním systému zahrnuje dekodér a prostředek pro přijetí kreditní nebo bankovní karty nesoucí mikroprocesor, a prostředek pro interakci s uvedeným mikroprocesorem, když je kreditní nebo bankovní karta vložena do pracovní polohy v uvedeném přijímači/dekodéru pro umožnění čtení dat nesených uvedenou kreditní nebo bankovní kartou a zadávání dat do mikroprocesoru neseného uvedenou kreditní nebo bankovní kartou.

Podle výhodného znaku tohoto dalšího aspektu předkládaného vynálezu přijímač/dekodér rovněž zahrnuje prostředek pro přijetí inteligentní karty, přičemž vložení inteligentní karty koncovým uživatelem do přijímače/dekodéru umožňuje inteligentní kartě, aby interagovala v uvedeném přijímači/dekodéru, přičemž produkt zvolený koncovým uživatelem může být dodán do uvedeného přijímače/dekodéru a odtud do televizního zařízení nebo osobního počítače, se kterým je přijímač/dekodér spojen.

Podle dalšího aspektu předkládaného vynálezu je navržen digitální satelitní rádiový nebo televizní systém mající množství zakončení koncových uživatelů, z nichž každé zahrnuje přijímač/dekodér, který byl definován v kterémkoliv z předcházejících dvou odstavců.

Předkládaný vynález dále navrhuje použití čtecího zařízení kreditní nebo bankovní karty ve spojení se zařízením pro příjem nebo dekódování rádiových nebo televizních signálů, výhodně satelitních televizních signálů, pro poskytnutí informace umožňující provedení debetu na kreditním nebo bankovním účtu uživatele v odezvě na žádost o nabízený program, soubor, položku nebo službu.

Ve způsobovém aspektu předkládaný vynález navrhuje způsob zobrazení programu nebo zpřístupnění souboru pro stažení, který zahrnuje v přijímači/dekodéru, ve kterém je informace týkající se programu nebo souboru přijímána, čtení informace z bankovní nebo kreditní karty, zjištění zda uživatel je autorizován pro přijetí programu nebo souboru a, pokud uživatel je autorizován, zobrazení programu nebo zpřístupnění souboru a vydání debetní instrukce pro provedení debetu na kreditním nebo bankovním účtu uživatele. Ve výhodném provedení je provedení debetu na kreditním nebo bankovním účtu uživatele ve skutečnosti obvykle provedeno před zobrazením programu nebo zpřístupněním souboru.

V dalším způsobovém aspektu předkládaný vynález navrhuje způsob zajištění objednávky pro položku nebo službu, který zahrnuje v přijímači/dekodéru, ve kterém je informace týkající se položky nebo služby přijímána, čtení informace z bankovní nebo kreditní karty, vytvoření objednávací žádosti obsahující informaci identifikující položku nebo službu a informaci reprezentující informace bankovní nebo kreditní karty, a vysílání objednávací žádosti do vzdáleného centra pro zpracování.

Způsob výhodně dále zahrnuje ve vzdáleném centru zpracování objednávací žádosti a zjištění, zda transakci autorizovat na základě informace bankovní nebo kreditní karty.

Pokud s týká výše popisovaného zařízení, výhodně toto zařízení dále zahrnuje dálkový ovladač pro vysílání osobního identifikačního čísla (PIN) uživatele do přijímače/dekodéru. Zvláště výhodně tento dálkový ovladač zahrnuje zabezpečovací

prostředek pro zajištění bezpečnosti vysílání. Tyto znaky budou nyní diskutovány podrobněji níže.

V aspektu předkládaného vynálezu, který bude nyní popisován, se předkládaný vynález rovněž týká vzdálené řídíc jednotky, nebo jinak dálkového ovladače, pro komponent vybavení a zejména ručního dálkového ovladače použitého pro ovládání televizních zařízení, přijímačů/dekodéru pro satelitní televizní systémy a další taková zařízení.

Takové řídící jednotky (ovladače) pracují na základě vysílání signálu z ručního ovladače ke komponentu vybavení, přičemž jeden způsob tohoto přenosu je realizován prostřednictvím infra-červeného paprsku.

Jak bylo diskutováno dříve, za účelem umožnění uživateli provádět nákupní a bankovní transakce přes médium televizního systému, by bylo nutné, aby uživatel zadal tak zvané osobní identifikační číslo (PIN) za účelem vykonání finální transakce. Toto PIN číslo uživatele samozřejmě musí být udržováno tajné tak, aby třetí strany nemohly odebírat peníze z bankovního účtu uživatele neautorizovaným způsobem. Se známými dálkovými ovladači může být informace, vysílaná z ručního zařízení do televizního zařízení, zachycena, což představuje problém, pokud mají být vysílána důvěrná nebo tajná data. Předkládaný vynález má za cíle odstranit tento problém při současném udržení co nejjednodušší povahy operací prováděných uživatelem.

Tento aspekt předkládaného vynálezu se týká zejména navržení ručního dálkového ovladače (ruční vzdálené řídící jednotky), který bude možné použít s televizním systémem, se

kterým mohou být prováděny bankovní a jiné finanční transakce.

Podle tohoto aspektu předkládaného vynálezu má dálkový ovladače pro komponent vybavení prostředek, kterým může být osobní identifikační číslo uživatele vysíláno do komponentu vybavení, přičemž ovladač obsahuje zabezpečovací prostředek pro zajištění bezpečnosti uvedeného vysílání.

V blízkém aspektu předkládaný vynález navrhuje dálkový ovladač pro komponent vybavení, který zahrnuje prostředek definující tělo uvedeného ovladače, prostředek pro vysílání osobního identifikačního čísla uživatele do uvedeného komponentu vybavení a zabezpečovací prostředek pro zajištění bezpečnosti uvedeného vysílání.

Výhodně vysílací prostředek zahrnuje prostředek pro vytváření infra-červeného paprsku, což poskytuje výhodný prostředek vysílání, který může být méně náchylný k zachycení než jiná vysílací média.

Zabezpečovací prostředek výhodně zahrnuje prostředek pro kódování PIN čísla, což může zamezit detekci PIN čísla, pokud je vysílání zachyceno.

Kódovací prostředek může zahrnovat prostředek pro kombinování PIN čísla s náhodným číslem (nebo pseudo-náhodným číslem), což může způsobit, že neautorizované dekódování bude obtížnější.

Může být zajištěn prostředek pro umožnění uživateli zadávání náhodného čísla; přičemž toto zajištění uživatelského vstupu může způsobit, že zadání náhodného čísla bude méně náchylné na zachycení.

Výhodně zadávací prostředek zahrnuje alespoň jednu klávesu (tlačítko) pro zadání náhodného čísla a další klávesu, přičemž ovladače je uspořádán tak, že PIN číslo je přes vysílací prostředek vysíláno pouze tehdy, když je stlačena tato další klávesa. Takové uspořádání může být jednoduché na ovládání, ale zároveň spolehlivé, kompaktní a bezpečné.

Výhodné kódovací prostředek zahrnuje prostředek pro uložení náhodného čísla v ovladači, což umožňuje kódování následně zadaného PIN čísla.

Zabezpečovací prostředek může zahrnovat prostředek pro vytváření číselných charakteristik jednotlivého ovladače pro vysílání přes uvedený vysílací prostředek do komponentu vybavení. Takové uspořádání může nabízet vyšší bezpečnost a rovněž může sloužit pro zabránění použití neautorizovaných dálkových ovladačů.

Podobně pro zvýšení bezpečnosti může kódovací prostředek zahrnovat prostředek pro vytváření číselných charakteristik jednotlivého dálkového ovladače a prostředek pro kombinování uvedených číselných charakteristik s uvedeným náhodným číslem a uvedeným PIN číslem.

Ve výhodném uspořádání kódovací prostředek zahrnuje prostředek pro přijímání náhodného čísla z uvedeného komponentu vybavení a prostředek pro kombinování tohoto náhodného čísla s PIN číslem uživatele pro vysílání přes vysílací prostředek do uvedeného komponentu. To může učinit kódování bezpečnějším prostřednictvím vytvoření náhodného čísla pouze, když je potřebné pro kódování.

Ovladač výhodně rovněž zahrnuje prostředek pro vysílání řídících příkazů pro vybavení a výhodně má zadávací prostředek selektivně pracující, v závislosti na zadávacím stavu dálkového ovladače, buď pro zadávání uvedeného PIN čísla nebo pro zadávání řídícího příkazu pro vybavení, přičemž zadávací stav je výhodně nastavován podle dalšího zadávacího prostředku. Zadávací prostředek může zahrnovat číselnou vstupní klávesu a řídící příkaz může zahrnovat příkaz pro volbu programu nebo kanálu. Další zadávací prostředek může zahrnovat další funkční klávesu.

Vynález rovněž navrhuje kombinaci zahrnující dálkový ovladač podle výše uváděného popisu a komponent vybavení, přičemž uvedený komponent vybavení má prostředek pro přijímání PIN čísla uživatele. V takovéto kombinaci komponent vybavení může zahrnovat prostředek pro vytváření náhodného čísla a prostředek pro předávání náhodného čísla do zobrazovací jednotky, což usnadňuje zadávání náhodného čísla v čase kódování.

Komponent vybavení může zahrnovat prostředek pro vytváření náhodného čísla a prostředek pro vysílání uvedeného náhodného čísla do uvedeného dálkového ovladače, což může zamezit nutnosti ručního zadávání náhodného čísla.

Další aspekt předkládaného vynálezu navrhuje digitální televizní systém, který zahrnuje komponent televizního vybavení, přičemž uvedený komponent má prostředek pro přijímání PIN čísla uživatele, a dálkový ovladač podle výše uváděného popisu.

Blízký další aspekt předkládaného vynálezu navrhuje digitální televizní systém, který zahrnuje komponent

televizního vybavení, přičemž uvedený komponent má prostředek pro přijímání PIN čísla uživatele, a dálkový ovladač, přičemž uvedený dálkový ovladač zahrnuje prostředek pro definování těla uvedeného ovladače, prostředek pro vysílání PIN čísla uživatele do uvedeného komponentu vybavení a zabezpečovací prostředek pro zajištění bezpečnosti uvedeného vysílání.

Komponentem televizního vybavení může být televizní zařízení nebo přijímač/dekodér spojený s televizním zařízením.

Předkládaný vynález se rovněž týká způsobu zadávání PIN čísla do televizního systému, který zahrnuje použití dálkového ovladače podle výše uváděného popisu.

Výhodné znaky předkládaného vynálezu budou popsány v následujícím popisu, čistě prostřednictvím příkladu, ve spojení s odkazy na připojené výkresy.

Přehled obrázků na výkresech

Obr.1 znázorňuje celkovou architekturu digitálního televizního systému podle výhodného provedení předkládaného vynálezu;

Obr.2 znázorňuje architekturu systému podmíněného přístupu v digitálním televizním systému;

Obr.3 znázorňuje strukturu opravňovací řídící zprávy (EMM) použité v systému podmíněného přístupu;

Obr.4 znázorňuje schematický diagram hardwaru účastnického autorizačního systému (SAS) podle výhodného provedení předkládaného vynálezu;

Obr.5 znázorňuje schematický diagram architektury SAS;

Obr.6 znázorňuje architekturu interaktivního systému digitálního televizního systému podle obr. 1;

Obr.7 je schematické znázornění dálkového ovladače použitého v digitálním televizním systému;

Obr.8 je schematický perspektivní pohled na přijímač/dekodér podle předkládaného vynálezu;

Obr.9 je schematická reprezentace protokolů použitých při platbách koncového uživatele prostřednictvím kreditní nebo bankovní karty;

Obr.10 je pohled podobný obr. 7, ale znázorňující čárkovanými čarami klíčové vnitřní komponenty ovladače;

Obr.11 je schematický pohled znázorňující klíčové vnitřní komponenty přijímače/dekodéru;

Obr.12 je schematická reprezentace prvního kódovacího uspořádání podle předkládaného vynálezu;

Obr.13 je pohled podobný obr. 12, ale znázorňující druhé kódovací uspořádání;

Obr.14 je pohled podobný obr. 12, ale znázorňující třetí kódovací uspořádání; a

Obr.15 je pohled podobný obr. 12, ale znázorňující páté kódovací uspořádání.

Příklady provedení vynálezu

Celkový přehled digitálního televizního vysílacího a přijímacího systému 1000 podle předkládaného vynálezu je znázorněn na obr. 1. Vynález zahrnuje většinou běžný digitální televizní systém 2000, který využívá známý MPEG-2 kompresní systém pro vysílání komprimovaných digitálních signálů. Přesněji MPEG-2 komprimátor 2002 ve vysílacím centru přijímá tok digitálního signálu (obvykle tok video signálů). Komprimátor 2002 je spojen s multiplexorem a kodérem 2004 prostřednictvím spojení 2006. Multiplexor 2004 přijímá množství dalších vstupních signálů, sestavuje jeden nebo více vysílacích toků a vysílá komprimované digitální signály do vysílače 2008 vysílacího centra přes spojení 2010, které samozřejmě může být představováno velkým množstvím různých forem včetně telekomunikačních linek. Vysílač 2008 vysílá elektromagnetické signály přes vzestupné spojení 2012 směrem k satelitnímu odpovídači 2014, kde jsou tyto signály elektronicky zpracovány a vysílány přes teoretické sestupné spojení 2016 do pozemního přijímače 2018, běžně ve formě parabolické antény vlastněné nebo pronajímané koncovým uživatelem. Signály přijímané přijímačem 2018 jsou vysílány do integrovaného přijímače/dekodéru 2020 vlastněného nebo pronajímaného koncovým uživatelem a spojeného s televizním zařízením 2022 koncového uživatele. Přijímač/dekodér 2020 dekóduje komprimovaný MPEG-2 signál na televizní signál pro televizní zařízení 2022.

Systém 3000 podmíněného přístupu je spojen s multiplexorem 2004 a přijímačem/dekodérem 2020 a je umístěn částečně ve vysílacím centru a částečně v dekodéru. Tento systém umožňuje koncovému uživateli přístup k digitálním

televizním vysíláním (přenosům) od jednoho nebo více dodavatelů (poskytovatelů) vysílání. Inteligentní karta, schopná dekódování zpráv týkajících se komerčních nabídek (to jest jeden nebo několik televizních programů, které jsou prodávány dodavatelem vysílání), může být vložena do přijímače/dekodéru 2020. S použitím dekodéru 2020 a inteligentní karty může koncový uživatel nakupovat vysílané události buď v módu předplacení nebo v módu platby za shlédnutí.

S multiplexorem 2004 a přijímačem/dekodérem 2020 je rovněž spojen interaktivní systém 4000, který je opět umístěn částečně ve vysílacím centru a částečně v dekodéru a který umožňuje koncovému uživateli interagovat s různými aplikacemi přes modemový zpětný kanál 4002.

Systém podmíněného přístupu

Níže bude podrobněji popsán systém 3000 podmíněného přístupu.

Ze schématu obr. 2 je patrné, že systém 3000 podmíněného přístupu zahrnuje účastnický autorizační systém (SAS) 3002. SAS 3002 je spojen s jedním nebo s více účastnickými řídícími systémy (SMS) 3004, přičemž jeden SMS 3004 je pro každého poskytovatele vysílání, prostřednictvím příslušného TCP-IP spojení 3006 (ačkoliv jiné typy spojení by alternativně také mohly být použity). Alternativně by jeden SMS 3004 mohl být sdílen mezi dvěma poskytovateli vysílání, nebo by jeden poskytovatel vysílání mohl používat dva SMS 3004 a podobně.

První kódovací jednotky ve formě šifrovacích jednotek 3008, využívajících "mateřské" inteligentní karty 3010, jsou spojené se SAS 3002 spojením 3012. Druhé kódovací jednotky opět ve formě šifrovacích jednotek 3014, využívajících mateřské inteligentní karty 3016, jsou spojené s multiplexorem 2004 spojením 3018. Přijímač/dekodér 2020 přijímá "dceřinou" inteligentní kartu 3020. Přijímač/dekodér 2020 je spojen přímo se SAS 3002 prostřednictvím komunikačních obslužných kanálů 3022 přes modemový zpětný kanál 4002. SAS 3002 vysílá, kromě jiných informací, přihlašovací práva do dceřiné inteligentní karty 3020 podle požadavků.

Inteligentní karty obsahují tajné informace jednoho nebo více komerčních operátorů. "mateřská" inteligentní karta kóduje různé typy zpráv a "dceřiné" inteligentní karty dekódují tyto zprávy, pokud k tomu mají oprávnění.

První a druhé šifrovací jednotky 3008 a 3014 zahrnují rám, elektronickou VME (VME je ICL autorizovaný operační systém) kartu se softwarem uloženým na EEPROM, až 20 elektronických karet a jednu inteligentní kartu 3010 respektive 3016 na každou elektronickou kartu, jednu (karta 3016) pro kódování zpráv ECM a jednu (karta 3010) pro kódování zpráv EMM.

Činnost tohoto systému 3000 podmíněného přístupu digitálního televizního systému bude nyní níže popsáno poněkud podrobněji ve spojení s odkazy na různé komponenty digitálního televizního systému 2000 a systému 3000 podmíněného přístupu.

Multiplexor a kodér

Jak je patrné ze znázornění na obr. 1 a obr. 2, je ve vysílacím centru digitální video signál nejprve komprimován (nebo je mu snížena bitová rychlost) s použitím MPEG-2 komprimátoru 2002. Tento komprimovaný signál je potom vysílán do multiplexoru a kodéru 2004 přes spojení 2006, aby byl multiplexován s dalšími daty, jako jsou další komprimovaná data.

Kodér vytváří řídící slovo použité v kódovacím procesu a obsažené v toku MPEG-2 v multiplexoru 2004. Řídící slovo je vytvářeno vnitřně a umožňuje integrovanému přijímači/dekodéru 2020 koncového uživatele dekódovat program.

Přístupová kritéria, která indikují způsob komercionalizace programu, jsou rovněž přidávána do toku MPEG-2. Program může být komercionalizován kterýmkoliv jedním z množství "předplatitelských" módů a/nebo jedním z množství módů nebo událostí "placených za shlédnutí" (PPV). V předplaceném módu koncový uživatel předplácí (účastní se) jednu nebo více komerčních nabídek, nebo "souborů", což mu poskytuje práva sledovat každý kanál uvnitř těchto souborů. Ve výhodném provedení může být ze souboru kanálů zvoleno až 960 komerčních nabídek. V módu platby za shlédnutí je koncový uživatel vybaven možností kupovat události podle přání. To může být dosaženo buď předobjednáním události předem ("objednávkový mód"), nebo nákupem události, jakmile je vysílána ("impulzní mód"). Ve výhodném provedení jsou všichni uživatelé účastníci (předplatitelé), ať již sledují nebo nesledují v předplaceném nebo PPV módu, ale samozřejmě, že PPV diváci nemusí být nezbytné účastníci (předplatitelé).

Jak řídící slovo tak i přístupová kritéria jsou použita pro sestavení opravňovací řídící zprávy (ECM); což je zpráva vysílaná ve spojení s jedním kódovaným programem; přičemž tato zpráva obsahuje řídící slovo (které umožňuje dekódování programu) a přístupová kritéria vysílaného programu. Přístupová kritéria a řídící slovo jsou vysílány do druhé šifrovací jednotky 3014 přes spojení 3018. V této jednotce je zpráva ECM vytvářena, kódována a vysílána na multiplexor a kodér 2004.

Každá služba vysílaná poskytovatelem vysílání zahrnuje v datovém toku množství oddělených komponentů; například televizní program obsahuje komponent videa, komponent audia, komponent podtitulků a tak dále. Každý z těchto komponentů služby je jednotlivě kódován a šifrován pro následné vysílání k odpovídači 2014. Ve spojení s každým kódovaným komponentem služby je vyžadována samostatná zpráva ECM.

Vysílání programů

Multiplexor 2004 přijímá elektrické signály zahrnující kódované zprávy EMM ze SAS 3002, kódované zprávy ECM z druhé šifrovací jednotky 3014 a komprimované programy z komprimátoru 2002. Multiplexor 2004 kóduje programy a vysílá kódované programy, kódované zprávy EMM a kódované zprávy ECM jako elektrické signály do vysílače 2008 vysílacího centra přes spojení 2010. Vysílač 2008 vysílá elektromagnetické signály směrem k satelitnímu odpovídači 2014 přes vzestupné spojení 2012.

Přijímání programů

Satelitní odpovídač 2014 přijímá a zpracovává elektromagnetické signály vysílané vysílačem 2008 a vysílá tyto signály k pozemnímu přijímači 2018, obvykle ve formě parabolické antény vlastněné nebo pronajaté koncovým uživatelem, přes sestupné spojení 2016. Signály přijímané pozemním přijímačem 2018 jsou vysílány do integrovaného přijímače/dekodéru 2020 vlastněného nebo pronajatého koncovým uživatelem a spojeného s televizním zařízením 2022 koncového uživatele. Přijímač/dekodér 2020 demultiplexuje signály, aby získal kódované programy s šifrovanými zprávami EMM a s šifrovanými zprávami ECM.

Pokud program není kódován, to znamená, že nebyla vysílána jakákoliv zpráva ECM v toku MPEG-2, přijímač/dekodér 2020 dekomprimuje data a mění signál na video signál pro vysílání do televizního zařízení 2022.

Pokud program je kódován, přijímač/dekodér 2020 vybírá odpovídající zprávu ECM z toku MPEG-2 a předává tuto zprávu ECM "dceřiné" inteligentní kartě 3020 koncového uživatele. Ta je zasunuta do štěrbiny v pouzdru přijímače/dekodéru 2020. Dceřiná karta 3020 řídí, zda koncový uživatel má právo dekódovat zprávu ECM a právo přístupu k programu. Pokud ne je do přijímače/dekodéru 2020 předán negativní stav pro indikaci toho, že program nemůže být dekódován. Pokud koncový uživatel má příslušná práva, je zpráva ECM dekódována a je vyjmuto řídící slovo. Dekodér 2020 potom může dekódovat program s použitím tohoto řídícího slova. Tok MPEG-2 je dekomprimován a převeden na video signál pro následné vysílání do televizního zařízení 2022.

Účastnický řídící systém (SMS)

Účastnický řídící systém (SMS) 3004 zahrnuje databázi 3024, která spravuje, kromě jiného, všechny soubory koncových uživatelů, komerční nabídky (jako jsou tarify a reklamy), předplacení, detaily PPV, a data týkající se spotřeby koncových uživatelů a autorizace. SMS 3004 může být fyzicky vzdálený od SAS 3002.

Každý SMS 3004 vysílá zprávy do SAS 3002 přes odpovídající spojení 3006, které zahrnují modifikace nebo vytváření opravňovacích řídících zpráv (EMM), určených k vysílání ke koncovým uživatelům.

SMS 3004 rovněž vysílá zprávy do SAS 3002, které nezahrnují jakékoliv modifikace nebo vytváření zpráv EMM, ale zahrnují pouze změnu stavu koncového uživatele (týkající se autorizace přidělené koncovému uživateli při objednávání produktů nebo hodnoty, jaká bude koncovému uživateli účtována).

Jak je popsáno v popisu níže, vysílá SAS 3002 zprávy (obvykle vyžadující informace, jako je informace zpětného dotazu nebo fakturační informace) do SMS 3004, takže je zřejmé, že komunikace mezi těmito dvěma komponenty je dvoucestná.

Opravňovací řídící zprávy (EMM)

EMM je zpráva přidělená pouze jednotlivému koncovému uživateli (účastníkovi), nebo skupině koncových účastníků, (na rozdíl od zprávy ECM, která je přidělena pouze jednomu kódovanému programu nebo sadě kódovaných programů, pokud jsou

součástí stejné komerční nabídky). Každá skupina může obsahovat daný počet koncových uživatelů. Tato organizace do skupin má za cíl optimalizovat využití šířky pásma; to znamená, že přístup k jedné skupině může umožnit dosažení většího počtu koncových uživatelů.

Různé specifické typy zprávy EMM jsou používány při uvádění předkládaného vynálezu do praxe. Jednotlivé zprávy EMM jsou přiděleny jednotlivým účastníkům a jsou obvykle používány při zajišťování služeb placených za shlédnutí; tyto zprávy obsahujíc identifikátor skupiny a umístění účastníka v této skupině. Tak zvané "skupinové" účastnické zprávy EMM jsou přiděleny skupinám, řekněme o 256 jednotlivých účastnících, a jsou obvykle použity při spravování určitých účastnických služeb. Tato zpráva EMM má identifikátor skupiny a bitovou mapu skupiny účastníků. Publikové zprávy EMM jsou přiděleny celým publikům a mohou být, například, použity určitým operátorem pro poskytování určitých volných (bezplatných) služeb. "Publikum" je celek účastníků majících inteligentní karty, které obsahují stejný identifikátor operátora (OPI). Nakonec "specifická" zpráva EMM je adresována specifickému identifikátoru inteligentní karty.

Níže bude ve spojení s odkazy na obr. 3 popsána struktura typické zprávy EMM. Zpráva EMM, která je realizovaná jako série digitálních datových bitů, v zásadě zahrnuje záhlaví 3060, vlastní EMM 3062 a podpis 3064. Záhlaví 3060 dále zahrnuje identifikátor 3066 typu pro identifikaci zda zpráva je individuální, skupinová, publiková nebo je zprávou nějakého jiného typu, identifikátor 3068, který udává délku zprávy EMM, doplňkovou adresu 3070 pro zprávu EMM, identifikátor 3072 operátora a identifikátor 3074

klíče. Vlastní EMM 3062 se samozřejmě značně mění podle svého typu. Nakonec podpis 3064, který je obvykle 8 bytů dlouhý, zajišťuje určitý počet kontrol proti poškození zbývajících dat ve zprávě EMM.

Účastnický autorizační systém (SAS)

Zprávy vytvářené SMS 3004 jsou předávány přes spojení 3006 do účastnického autorizačního systému (SAS) 3002, který dále vytváří zprávy potvrzující příjem zpráv vytvořených SMS 3004 a předává tato potvrzení do SMS 3004.

Jak je znázorněno na obr. 4, na hardwarové úrovni SAS zahrnuje známým způsobem střediskový počítač 3050 (ve výhodném provedení DEC počítač) spojený s jednou nebo s více klávesnicemi 3052 pro zadávaní dat a příkazů, jednu nebo více zobrazovacích jednotek (VDU) 3054 pro zobrazování výstupní informace a prostředek 3056 pro ukládání dat. Může být zajištěna určitá záloha (nadbytečnost) v hardwaru.

Na softwarové úrovni SAS pracuje, ve výhodném provedení na standardním VMS operačním systému, podle softwarového schéma, jehož architektura bude nyní popsáno v přehledu ve spojení s odkazy na obr. 5; mělo by přitom být zcela zřejmé, že software by alternativně mohl být realizován v hardwaru.

V přehledu SAS zahrnuje oblast 3100 předplatitelského řetězce pro poskytování práv pro předplacený mód a pro obnovování práv automaticky každý měsíc, oblast 3200 řetězce plateb za shlédnutí pro poskytování práv pro PPV události, a zaváděč 3300 EMM pro předávání zpráv EMM, vytvářených oblastmi předplatitelského řetězce a řetězce PPV, do

multiplexoru a kodéru 2004 a tudíž pro plnění toku MPEG zprávy EMM. Pokud mají být udělena další práva, jako jsou práva při platbách za soubor (PPF) v případě stahování počítačového softwaru do osobního počítače uživatele, jsou rovněž vytvořeny další podobné oblasti.

Jednou funkcí SAS 3002 je spravovat přístupová práva k televizním programům, dostupným jako komerční nabídky v předplatitelském módu nebo prodávaným jako PPV události podle různých módů komercionalizace (například objednávkový mód, impulzní mód). SAS 3002 podle těchto práv a podle informace, přijaté ze SMS 3004, vytváří zprávy EMM pro účastníka.

Oblast 3100 předplatitelského řetězce zahrnuje příkazové rozhraní (CI) 3102, obslužný kanál 3104 technické správy účastníků (STM), generátor zpráv (MG) 3106 a šifrovací jednotku 3008.

Oblast 3200 PPV řetězce zahrnuje autorizační obslužný kanál (AS) 3202, relační (vztahovou) databázi 3204 pro ukládání relevantních detailů týkajících se koncových uživatelů, lokální databázi 3205 černého seznamu (seznam neplatičů), databázové obslužné kanály 3206 pro databáze, příkazově centralizovaný obslužný kanál (OCS) 3207, obslužný kanál 3208 pro programový vysílač (SPB), generátor zpráv (MG) 3210, jehož funkce je v zásadě stejná jako funkce generátoru zpráv pro oblast předplatitelského řetězce a tudíž na tomto místě dále nebude podrobněji popisována, a šifrovací jednotku 3008.

EMM zaváděč 3300 zahrnuje množství vysílačů 3302, 3304, 3306 a 3308 zpráv (ME) a softwarové multiplexory (SMUX) 3310 a 3312. Ve výhodném provedení předkládaného vynálezu

jsou použity dva ME 3300 a 3304 pro generátor 3106 zpráv, a další dva ME 3306 a 3308 pro generátor 3210 zpráv. ME 3302 a 3306 jsou spojené se SMUX 3312, zatímco ME 3304 a 3308 jsou spojené se SMUX 3312.

Interaktivní systém

S multiplexorem 2004 a přijímačem/dekodérem 2020 je rovněž spojen interaktivní systém 4000, který je opět umístěn částečně ve vysílacím centru a částečně v dekodéru a který umožňuje koncovému uživateli interagovat s různými aplikacemi přes modemový zpětný kanál 4002.

Obr. 6 znázorňuje obecnou architekturu interaktivního televizního systému 4000 digitálního televizního systému 1000 podle předkládaného vynálezu.

V přehledu zahrnuje interaktivní systém 4000 čtyři hlavní prvky:-

tvůrčí nástroj 4004 ve vysílacím centru nebo kdekoliv jinde pro umožnění poskytovateli vysílání vytvářet, vyvíjet, ladit a testovat aplikace;

aplikační a datový obslužný kanál 4006 ve vysílacím centru, spojený s tvůrčím nástrojem 4004 pro umožnění poskytovateli vysílání připravovat, ověřovat a formátovat aplikace a data pro dodání do multiplexoru a kodéru 2004 pro začlenění do MPEG-2 transportního datového toku (obvykle jeho privátní části), aby byla vysílána ke koncovému uživateli;

virtuální počítač včetně prováděcího prostředku (RTE) 4008, který je v proveditelném kódu nainstalován v přijímači/dekodéru 2020 vlastněném nebo pronajatém

koncovým uživatelem pro umožnění koncovému uživateli přijímat, ověřovat, dekomprimovat a stahovat (zavádět) aplikace do pracovní paměti 2024 dekodéru 2020 pro vykonání. Tento prováděcí prostředek 4008 rovněž realizuje rezidentní aplikace obecného účelu. Prováděcí prostředek 4008 je nezávislý na hardwaru a operačním systému;

modemový zpětný kanál 4002 mezi přijímačem/dekodérem 2020 a aplikačním a datovým obslužným kanálem 4006 pro umožnění signálům instruujícím tento aplikační a datový obslužný kanál 4006 zavádět data a aplikace do MPEG-2 transportního datového toku na žádost koncového uživatele.

Interaktivní televizní systém pracuje s použitím "aplikací", které řídí funkce přijímače/dekodéru a různých zařízení v něm obsažených. Aplikace jsou reprezentovány v prováděcím prostředku 4008 jako "zdrojové soubory". "Modul" je sestava zdrojových souborů a dat. Pro vytvoření aplikace může být požadováno několik modulů. "Objem paměti" přijímač/dekodéru je paměťový prostor pro moduly. Pro stanování nebo zavádění modulů je použito "rozhraní". Moduly mohou být stahovány do přijímače/dekodéru 2020 z MPEG-2 transportního datového toku.

Pro účely tohoto popisu je aplikace úsek strojového kódu pro řízení vysokoúrovňových funkcí výhodně přijímače/dekodéru 2020. Například, když koncový uživatel namíří ohnisko dálkového ovladače 2026 (jak je znázorněn podrobněji na obr. 7) na tlačítkový objekt viděný na obrazovce televizního zařízení 2022 a stlačí potvrzovací

klávesu, spustí se sekvence instrukcí, sdružená s tímto tlačítkem.

Interaktivní aplikace nabízí menu a vykonává příkazy na žádost koncového uživatele a poskytuje data týkající se účelu této aplikace. Aplikace mohou být buď rezidentními aplikacemi, to znamená, že jsou uloženy v ROM (nebo FLASH nebo jiné energeticky nezávislé paměti) přijímače/dekodéru 2020, nebo mohou být vysílány a stahovány do RAM (nebo FLASH) tohoto dekodéru 2020.

Příklady aplikací jsou:-

- Inicializační aplikace. Přijímač/dekodér 2020 je vybaven rezidentní inicializační aplikací, která je adaptabilním souhrnem modulů (tento termín je podrobněji definován níže), umožňujícím přijímači/dekodéru 2020 okamžitě pracovat v prostředí MPEG-2. Tato aplikace zajišťuje základní znaky, které mohou být modifikovány poskytovatelem vysílání, pokud je to žádoucí. Tato aplikace rovněž zajišťuje rozhraní mezi rezidentními aplikacemi a stahovanými aplikacemi.
- Spouštěcí aplikace. Spouštěcí aplikace umožňuje jakékoliv aplikaci, ať již stahované nebo rezidentní, pracovat v přijímači/dekodéru 2020. Tato aplikace působí jako samozaváděcí program vykonaný při vstupu do služby za účelem spuštění aplikace. Spouštěcí aplikace je stažena do RAM a tudíž může být snadno aktualizována. Může být uspořádána tak, že interaktivní aplikace dostupné na každém kanálu mohou být zvoleny a spuštěny buď bezprostředně po stažení nebo po stažení předem. V případě stažení předem je aplikace stažena do

paměti 2024 a je aktivována spouštěcí aplikací na požádání.

- Programový průvodce. Programový průvodce je interaktivní aplikace, která poskytuje ucelenou informaci o programech. Například může poskytovat informaci, řekněme, o televizních programech na jeden týden, které budou uváděny na každém kanálu souboru digitální televize. Stlačením klávesy na dálkovém ovladači 2026, koncový uživatel vstoupí do přídavné obrazovky, překrývající událost (relaci) znázorněnou na obrazovce televizního zařízení 2022 Tato přidaná obrazovka je vyhledávač (browser) poskytující informaci o současných a následujících událostech (relacích) na každém kanálu souboru digitální televize. Stlačením další klávesy na dálkovém ovladači 2026 koncový uživatel vstoupí do další aplikace, která zobrazí seznam informací o událostech během jednoho týdne. Koncový uživatel může rovněž vyhledávat a třídit události podle jednoduchých a přizpůsobených kritérií. Koncový uživatel může rovněž vstoupit přímo do zvoleného kanálu.
- Aplikace plateb za zhlédnutí. Aplikace plateb za shlédnutí je interaktivní služba dostupná na každém PPV kanálu souboru digitální televize ve spojení se systémem 3000 podmíněného přístupu. Koncový uživatel může vstoupit do této aplikace s použitím programového průvodce nebo vyhledávače kanálů. Navíc se aplikace spustí automaticky, jakmile je PPV událost zjištěna na PPV kanálu. Koncový uživatel potom může koupit probíhající událost buď prostřednictvím své dceřinné

inteligentní karty 3020 nebo přes komunikační obslužný kanál 3022 (s použitím modemu, telefonu a DTMF kódů, systému MINITEL nebo podobně). Tato aplikace může být buď rezidentní v ROM přijímače/dekodéru 2020 nebo stažitelná do RAM přijímače/dekodéru 2020.

- Aplikace PC stahování. Na žádost může koncový uživatel stahovat počítačový software s použitím této aplikace PC stahování.
- Aplikace časopisový vyhledávač. Tato aplikace časopisového vyhledávače zahrnuje cyklické video vysílání obrazů s navigací koncového uživatele prostřednictvím tlačítek znázorněných na obrazovce.
- Aplikace kviz. Kviz aplikace je výhodně synchronizována s vysíláním kviz programu. Například jsou na obrazovce televizního zařízení 2022 zobrazeny otázky s několika odpověďmi a koncový uživatel může zvolit odpověď s použitím dálkového ovladače 2026. Aplikace kviz může informovat uživatele, zda odpověď je správná nebo ne, a může počítat skóre uživatele.
- Aplikace teleshopping. V jednom příkladu tato aplikace teleshopping jsou nabídky zboží na prodej vysílány do přijímače/dekodéru 2020 a zobrazovány na televizním zařízení 2022. S použitím dálkového ovladače 2026 může uživatel zvolit určitou položku, kterou chce koupit. Objednávka této položky je vyslána přes modemový zpětný kanál 4002 do aplikačního a datového obslužného kanálu 4006 nebo do samostatného prodejního systému, jehož telefonní číslo bylo staženo do přijímače/dekodéru 2020, případně s příkazem pro zatížení účtu kreditní

karty, která byla vložena do jednoho zařízení 4036 pro čtení inteligentních karet v přijímači/dekodéru 2020.

- Aplikace telebanking. V jednom příkladu této aplikace telebanking uživatel vloží bankovní kartu do jednoho ze zařízení 4036 pro čtení inteligentních karet v přijímači/dekodéru 2020. Přijímač/dekodér 2020 zavolá banku uživatele s použitím telefonního čísla uloženého v bankovní kartě nebo uloženého v přijímači/dekodéru 2020, a potom tato aplikace poskytuje množství možností, které mohou být zvoleny s použitím dálkového ovladače 2026, například stažení přes telefonní linku stavu účtu, převod položek mezi účty, žádost o šekovou knížku a podobně.
- Aplikace internetovský vyhledávač. V jednom příkladu této aplikace internetovského vyhledávače jsou instrukce od uživatele, jako je žádost o sledování webové stránky mající určité URL, zadávány s použitím dálkového ovladače 2026 a tyto instrukce jsou vysílány prostřednictvím modemového zpětného kanálu 4002 do aplikačního a datového obslužného kanálu 4006. Příslušná webová stránka je potom začleněna do vysílání z vysílacího centra, přijata přijímačem/dekodérem 2020 přes vzestupné spojení 2012, odpovídač 2014 a sestupné spojení 2016, a je zobrazena na televizním zařízení 2022.

Aplikace jsou uloženy v paměťových místech přijímače/dekodéru 2020 a jsou reprezentovány jako zdrojové soubory. Zdrojové soubory zahrnují soubory jednotky popisu grafických objektů, soubory jednotky proměnných bloků,

soubory instrukčních sekvencí, aplikační soubory a datové soubory.

Soubory jednotek popisu grafických objektů popisují obrazovky, rozhraní mezi člověkem a počítačem aplikace. Soubory jednotek proměnných bloků popisují datové struktury zpracovávané aplikací. Soubory instrukčních sekvencí popisují zpracovatelské operace aplikace. Aplikační soubory zajišťují vstupní body pro aplikace.

Aplikace tvořené tímto způsobem mohou využít datové soubory, jako jsou knihovní soubory ikon, obrazové soubory, soubory znakových fontů, soubory tabulek barev a ASCII textové soubory. Interaktivní aplikace mohou rovněž získat přímá (on line) data provedením vstupů a/nebo výstupů.

Prováděcí prostředek 4008 zavádí do své paměti pouze ty zdrojové soubory, které potřebuje v daném okamžiku. Tyto zdrojové soubory jsou čteny ze souborů jednotek popisu grafických objektů, souborů instrukčních sekvencí a aplikačních souborů; soubory jednotek proměnných bloků jsou uloženy v paměti následně po vyvolání procedury pro stažení modulů a zde zůstávají zajištěny, dokud není provedeno specifické volání procedury pro vyjmutí modulů.

Zařízení kreditních karet pro nastavovací řídící skříň

Jak je patrné ze znázornění na obr. 8, je každý koncový uživatel systému, popsaného ve spojení s odkazy na předcházející výkresy, vybaven nastavovací řídící skříní 2019 (STB) zahrnující přijímač/dekodér 2020, prostřednictvím kterého koncový uživatel může interagovat s digitálním

satelitním televizním systémem a prostřednictvím kterého mohou být produkty zvolené koncovým uživatelem přenášeny do televizního zařízení 2022 uživatele nebo do osobního počítače uživatele, aby tam byly staženy.

Nastavovací řídící skříň 2019 zahrnuje, kromě jiných komponentů, dekodér 2020 a modem 2021, přičemž dekodér zahrnuje paměť 4022.

Na předku nastavovací řídící skříně 2019 jsou vytvořeny štěrbiny 2023 respektive 2025, do kterých může být vložena dceřinná inteligentní karta 3020 a/nebo kreditní/bankovní karta 3017. Tyto štěrbiny 2023 a 2025 mají se sebou sdružené prostředky 3019 respektive 3021 pro čtení karet.

Způsob, kterým "dceřinná inteligentní karta, která je specifická pro určitého uživatele, interaguje se systémem již byl popsán ve spojení s odkazy na obr. 2.

U tohoto provedení předkládaného vynálezu má koncový uživatel možnost platby za zvolený produkt prostřednictvím kreditní/bankovní karty, výhodně typu, který obsahuje mikroprocesor 3017a (tak zvaná "inteligentní karta"), obvykle v PPV a PPF režimech činnosti systému.

Toto použití kreditní/bankovní karty je umožněno prostřednictvím vytvoření nastavovací řídící skříně 2019 se štěrbinou 2025 a s přidruženým prostředkem uvnitř přijímače/dekodéru pro umožnění mikroprocesoru 3017a, aby interagoval se systémem jako celkem.

Přijímač/dekodér v tomto provedení zahrnuje běžné čtecí zařízení pro čtení karet, které je pod celkovým řízením stejným procesorem, který zajišťuje řízení dekódování a řídí

interakci s inteligentní kartou. Tímto způsobem mohu být debetní instrukce snadno spojeny s "nabíjením" inteligentní karty přídavnými kredity.

Tato interakce zahrnuje to, že kreditní/bankovní karta je vlastně dotazována pro poskytnutí její pravosti, data uplynutí platnosti a zda kreditní limit spojený s jejím držitelem již nebyl překročen, a potom pro provedení debetu na účtu, se kterým je karta spojena (přes její mikroprocesor, pokud se jedná o inteligentní kartu, a relevantní bankovní síť), o hodnotu účtovanou za zvolený produkt. V případě "neinteligentní" magnetické karty je použito podobné procedury.

Obr. 9 ilustruje ve schematickém znázornění protokol, který je použit pro umožnění kreditní/bankovní kartě 3017, aby interagovala se systémem, přičemž cílem těchto protokolů je zajištění finanční bezpečnosti. Tento protokol je založena na protokolu v současnosti používaném v systému MINITEL, který pracuje ve Francii.

Protokol pracuje ve vztahu se třemi odlišnými oblastmi, oblastí koncového uživatele nebo účastnického zakončení, obecně označenou jako oblast A, oblast poskytovatele systému, obecně označenou jako oblast B, a oblast bank, obecně označenou jako bankovní oblast C. Na obr. 9 jsou oblasti A, B a C určeny spíše pro označení provozního rozdělení systému, než pro označení jakýchkoliv fyzických vlastností.

Jak bylo naznačeno dříve, ve spojení s odkazy na obr. 8, má uživatel kreditní/bankovní kartu 3017, která zahrnuje mikroprocesor 3017a, ve formě čipu s integrovanými obvody.

Tato karta může rovněž mít tak zvaný privátní klíč 3015 mající podobnou bezpečnostní funkci, jako již bylo popsáno ve spojení s inteligentní kartou 3020 uživatele, pro použití při ověřování pravosti karty.

Ve spojení s jeho interaktivitou s kreditní/bankovní kartou 3017 je přijímač/dekodér 2020 koncového uživatele funkčně opatřen prostředkem pro zpracování dat reprezentujících samotnou transakci (znázorněno jako prostředek 3029) a prostředek pro zpracování dat týkajících se ověření pravosti a integrity (znázorněno jako prostředek 3031). Oblast A rovněž zahrnuje veřejný klíč 3027.

Oblast B, která je pod řízením poskytovatele systému, zahrnuje SMS 3004 a komunikační obslužný kanál 3022, popsané dříve ve spojení s odkazy na obr. 1 a obr. 2. Komunikační obslužné kanály 3022 rovněž zahrnují šifrovací obslužný kanál 3023, který začleňuje privátní klíč.

Oblast C zahrnuje privátní bankovní síť obvykle bankovních členů, kteří jsou na obrázku znázorněni jako členové 3033, 3034 a 3035. Bankovní síť zahrnuje správce 3036 dálkových plateb, který zahrnuje "mateřský" klíč 3037.

Sekvence událostí, které probíhají při jedné finanční transakci s použitím kreditní/bankovní karty 3017, bude nyní popsána ve spojení s odkazy na obr. 9, na kterém šipky naznačují různé kroky začleněné do provádění platby a uvonění/zadání příslušné EMM, aby byla přijata přijímačem/dekodérem 2020 koncového uživatele.

Vložení "inteligentní" kreditní/bankovní karty 3017 do přijímače/dekodéru 2020 způsobí následující události, jak je popsáno níže. Je třeba poznamenat, že všechny z kroků

obvykle probíhají v reálném čase, pokud níže není uvedeno jinak:

a) Prostřednictvím přijímače/dekodéru 2020 je z karty 3017 vybrána počáteční informace. Tato informace zahrnuje číslo karty, informaci o datu platnosti karty, jazyk země, měnovou jednotku a podobně. Tato informace je stažena do RAM paměti přijímače/dekodéru 2020.

b) Jakmile je stažena, je provedena kontrola této informace. Pokud je informace správná, procedura pokračuje; jinak je transakce přerušena.

c) S použitím dálkového ovladače 2026 je zadáno PIN číslo uživatele způsobem, který je popsán níže.

d) Karta 3017 potom ověřuje PIN číslo. Pokud je číslo správné, procedura pokračuje. Pokud je zadané PIN číslo nesprávné, poskytne karta 3017 řekněme dva nebo tři další pokusy. Pokud PIN číslo je stále nesprávné při těchto dalších pokusech, pak je transakce přerušena.

e) Pokud je PIN číslo správné, karta 3017 otevírá určité další paměťové oblasti a informace z těchto oblastí jsou staženy do RAM paměti přijímače/dekodéru 2020. Takovými informacemi mohou být transakce provedené s kartou 3017 a jejich peněžní hodnota.

f) Je provedena kontrola, zda transakce, které by provedl uživatel, by nepřekročily odpovídající kreditní limit.

g) Pokud je odpověď kladná (to jest nepřekročily by odpovídající limit), je kartě 3017 předána určitá informace o současné transakci, jako je cena, den, bankovní detaily a podobně.

h) S touto informací karta 3017 vypočítá první numerický certifikát potvrzující transakci. Numerický certifikát

je vytvořen mikroprocesorem karty prostřednictvím protokolu, který využívá cenu transakce, datum, číslo karty, datum uplynutí platnosti karty, označení produktu a podobné informace pro vytvoření certifikátu, který má obvykle délku 30 nebo 40 bytů.

i) Detaily o transakci jsou zapsány do bankovní/kreditní karty 3017.

j) Karta 3017 je potom uzavřena, což je důležité, protože není žádoucí, aby karta byla udržována otevřená v jakýchkoliv dalších krocích.

k) Je vytvořeno spojení s komunikačními obslužnými kanály 3022 systému SAS 3002 prostřednictvím modemového zpětného kanálu 4002.

l) Aby přijímač/dekodér 2020 ověřil SAS 3002, je přijímačem/dekodérem 2020 vytvořeno náhodné číslo (nebo ALEA), které je vysláno do komunikačních obslužných kanálů 3022.

m) Náhodné číslo je šifrováno s použitím šifrovacího algoritmu prostřednictvím šifrovacího obslužného kanálu 3023 a je vysláno zpět do přijímače/dekodéru 2020.

n) Přijímač/dekodér 2020 dešifruje náhodné číslo, aby zkontroloval, že je správné.

o) Při zajištění, že SAS 3002 je ověřen, kontroluje tento SAS 3002 (a zejména příkazově centralizovaný obslužný kanál 3027 (viz obr. 5)) se SMS 3004, aby potvrdil, že určitý účastník není na jakémkoliv černém seznamu (neplatičů).

p) Je provedena případná kontrola vzhledem k databázi udržované, například, ve vysílacím centru na to, zda požadovaný produkt je dostupný.

q) V případě, že nejsou zjištěny žádné problémy, jsou detaily o transakci a první certifikát vyslány komunikačními obslužnými kanály 3022 ke správci 3036 dálkových plateb v privátní bankovní síti 3032.

r) Kreditní stav koncového uživatele je ověřen a za předpokladu, že toto ověření je uspokojivé, vydá správce 3036 dálkových plateb numerický certifikát do komunikačních obslužných kanálů 3022, který byl vypočítán stejným způsobem jako první certifikát. Tento druhý certifikát je autorizací správce dálkových plateb pro nákup. Je třeba uvést, že druhý certifikát nemusí být vždy vyžadován, například, pokud hodnota transakce je pod určitou prahovou hodnotou, přičemž za těchto okolností nemusí být prováděno spojení se správce 3036 dálkových plateb.

s) Přijetí druhého certifikátu (obvykle ve formě elektrického signálu) operátorem je zárukou platby bankou pro operátora a tudíž SAS 3002 potom vysílá vhodnou zprávu EMM do přijímače/dekodéru 2020 pro autorizaci nákupu (pokud nákupem je programová událost a podobně).

t) Přijetí této zprávy EMM přijímačem/dekodérem 2020 umožňuje koncovému uživateli sledovat zvolený PPV produkt na jeho televizním zařízení 2022 nebo stahovat zvolený PPF produkt do osobního počítače koncového uživatele.

u) Mimo reálný čas SAS 3002 vysílá signál do SMS 3004, informující o transakci.

v) Mimo reálný čas SMS 3004 vysílá informaci o transakci relevantnímu členu 3033, 3034 nebo 3035 bankovní sítě

pro informování o tom, že platba byla přijata. banka provede potřebnou akci.

Výše byly uvedeny detaily o tom, jak může být realizován režim PPV nebo PPF s použitím kreditní nebo bankovní karty. Kromě toho může být stejné čtecí zařízení pro čtení bankovních nebo kreditních karet použito pro autorizaci dalších transakci, například nákupu zboží nebo služeb ve spojení s aplikací teleshopping, a pro umožnění koncovému uživateli sledovat a modifikovat detaily v jeho bankovním účtu ve spojení s aplikací telebanking.

Dálkový ovladač

Jak je patrné zejména z obr. 7 a obr. 10, zahrnuje infra-červený dálkový ovladač 2026 pouzdro 2030, na jehož horním povrchu je množství kláves nebo tlačítek, především zjevně řídící klávesy 2031, klávesa 2032 Mute (vypnutí zvuku) a numerická klávesnice 2034 s tlačítky očíslovanými "0" až "9".

Pouzdro 2030 obsahuje prostředek 2035 pro vytváření a vysílání infra-červeného paprsku (ve výhodném provedení infra-červené zařízení pracující podle standardu Phillips RC5), paměť 2036 zahrnující jak EEPROM (a/nebo FLASH paměť) tak i RAM, a řídící prostředek 2037 zahrnující šifrovací prostředek 2038. Paměť 2036, která je relativně malá, je použita pro uložení (v EEPROM) různých hesel a dalších identifikátorů (jak bude krátce popsáno níže) a (v RAM) proměnných použitých během různých výpočtů. Řídící prostředek je obecně běžný a zahrnuje, na hardwarové úrovni,

jedno-čipový mikroprocesor, jako je procesor dosažitelný od firmy Phillips pro dálkové ovladače, a ,na softwarové úrovni, software rezidentní v paměti 2036 a schopný funkcí, které budou krátce popsány (jako je funkce sčítání a funkce modulo).

V přehledu je ruční dálkový ovladač, podle zde uvedeného popisu, za prvé schopen vysílat PIN číslo uživatele do televizního systému, obvykle přes dekodér, a za druhé je tento dálkový ovladač rovněž opatřen prostředkem pro šifrování vysílaného čísla, zejména výpočtem sekvence náhodných čísel. Šifrování je obzvláště důležité v souvislosti s použitím kreditní nebo bankovní karty s přijímačem/dekodérem.

Pokud se týká zajištění bezpečnosti pro vysílané PIN číslo, existuje několik způsobů jak tato bezpečnost může být zajištěna. zejména mohou být použity různé protokoly a mohou být použity různé odlišné způsoby vlastního provádění šifrování.

Na tomto místě lze učinit odkaz na popis systému ve spojení s odkazy na obr. 2 a zejména na tu část systému, která popisuje tak zvané mateřské a dceřinné inteligentní karty. Na tomto místě je rovněž učiněn odkaz na schematické znázornění vnitřních komponentů přijímače/dekodéru 2020, jak je ilustrováno na obr. 11.

Určité znaky ručního infra-červeného dálkového ovladače, které jsou relevantní v kontextu předkládaného vynálezu, se týkají přístupu přijímače/dekodéru 2020 k dceřinné inteligentní kartě 3020 a/nebo kreditní/bankovní kartě 3017. Přijímač/dekodér 2020 je pod řízením řídícího

prostředku 2100, který je umístěn v dekodéru a je realizován v kombinaci hardwaru na bázi mikroprocesoru a softwaru. Řídící prostředek zahrnuje prostředek 2102 pro vyváření náhodného čísla a prostředek 20104 pro předávání náhodného čísla na televizní obrazovku, obvykle televizního zařízení 2022. Dekodér rovněž zahrnuje, v jednom výhodném provedení vynálezu, prostředek 2106 pro přijímání infra-červeného paprsku (ve výhodném provedení infra-červené zařízení pracující podle standardu Phillips RC5) pro komunikaci s infra-červeným dálkovým ovladačem. V jiném provedení vynálezu ale dekodér obsahuje jak prostředek pro přijímání tak i pro vysílání infra-červeného paprsku, pokud je požadováno vysílání k ovladači. Jak bylo zmiňováno dříve, přijímač/dekodér 2020 rovněž zahrnuje pracovní paměť 2024, která, stejně jako v případě dálkového ovladače, zahrnuje jak EEPROM/FLASH tak i RAM. Použití paměti je analogické k tomu, co bylo popsáno výše ve spojení s dálkovým ovladačem.

Obr. 12 až obr. 15 ilustrují množství šifrovacích protokolů, které mohu být použity.

Ve spojení s odkazy na obr. 12 v prvním šifrovacím protokolu dekodér 2020 pod řízením řídícím prostředkem 2100, umístěným v dekodéru, vysílá elektromagnetický signál do televizní obrazovky, která dále v odezvě zobrazí čtyř-číslicovou sekvenci a_1, a_2, a_3, a_4 od 0000 do 9999, přičemž tento krok je znázorněna na obr. 12 jako krok 500 vysílání čtyřčíslicového pseudo-náhodného čísla.

Toto čtyřčíslicové číslo může být buď zcela náhodně vytvořeným čtyřčíslicovým číslem, které je měněno pokaždé, když je do systému vstoupeno koncovým uživatelem, nebo může být předem stanoveným číslem z předem stanovených náhodných

čísel. Je zobrazena přidružená zpráva, která žádá uživatele, aby zadal toto náhodné číslo do ovladače 2026.

Zobrazení uvedeného čísla a přidružené zprávy je naznačeno krokem 501.

Uživatel potom sleduje náhodné číslo a_1, a_2, a_3, a_4 na televizní obrazovce 2022 v kroku 502 a v kroku 503 zadává toto číslo do dálkového ovladače 2026 při současném stlačení klávesy 2032 Mute.

Ve výhodném provedení je toto zadávání prováděno prostřednictvím numerické klávesnice 2034. Alternativně může být toto zadávání provedeno prostřednictvím jakéhokoliv vhodného vstupního prostředku, jako je prostřednictvím hlasové aktivace.

Opět v reakci na zprávu na televizní obrazovce uživatel potom v kroku 504 zadává do dálkového ovladače 2026 své vlastní PIN číslo s použitím numerické klávesnice 2034. Toto PIN číslo je rovněž čtyřčíslicové číslo c_1, c_2, c_3, c_4 a je PIN číslem, které rovněž platí pro dceřinnou inteligentní kartu 3020 a/nebo bankovní/kreditní kartu 3017. Kroky 503 a 504 jsou prováděny, zatímco je uživatelem držena stlačená klávesa 2032 Mute.

Následující krok zahrnuje to, že ovladač 2026 vlastně kombinuje tato dvě čtyřčíslicová čísla a_1, a_2, a_3, a_4 a c_1, c_2, c_3, c_4 pro vytvoření kódovaného čtyřčíslicového čísla t_1, t_2, t_3, t_4.

Nyní bude popsán způsob, kterým jsou vypočítány číslice t_1, t_2, t_3 a t_4.

Každá z číslic je vypočítána stejným způsobem, takže popsán bude pouze výpočet číslice t_1.

t_1 je vypočítána z číslic a_1 a c_1 podle následujícího výrazu:

$$t_1 = (a_1 + c_1) \bmod 10$$

kde "mod 10" znamená, že je brán základní 10 (desítkový) modulu z $(a_1 + c_1)$; jinými slovy je brána nejméně významná číslice z výsledku součtu.

Jak bylo uvedeno výše, jsou podobné výpočty provedeny pro číslice t_2, t_3 a t_4. Číslice c_1, c_2, c_3 a c_4 jsou tedy šifrovány tak, aby byly zabezpečeny proti jejich zachycení v důsledku toho, že dálkový ovladač 2026 vysílá PIN číslo uživatele do dekodéru 2020.

Právě popsaný krok je naznačen jako krok 505 na obr. 12.

Kódované číslo t_1, t_2, t_3, t_4 je potom vysíláno z dálkového ovladače 2026 do dekodéru 2020, jak je naznačeno krokem 506 na obr. 12.

Po přijetí kódovaného čtyřčíslicového čísla dekodér 2020 vyjímá původní čtyřčíslicové PIN číslo c_1, c_2, c_3, c_4. To je provedeno výpočtem každé z číslic c_1, c_2, c_3 a c_4 z t_1, t_2, t_3 a t_4, přičemž tento krok je na obr. 12 znázorněn jako krok 507. Výpočet je prováděn, ve spojení s popisem výpočtu číslice c_1, následovně:

$$c_1 = (t_1 - a_1 + 10) \bmod 10$$

Odpovídající vzorec platí i pro ostatní číslice.

V případě dceřinné inteligentní karty 3020 je následujícím krokem pro přijímač/dekodér 2020 porovnání

vyjmutého PIN čísla s již uloženým PIN číslem v dekodéru, které reprezentuje dceřinnou inteligentní kartu 3020. Ve skutečnosti je každá z číslic c_1, c_2, c_3 a c_4 porovnáván s odpovídající číslicí uloženou v dekodéru. Tento krok je na obr. 12 znázorněn jako krok 508.

Poslední kroky, znázorněné jako kroky 509 a 510 na obr. 12, zahrnují to, že přístup je do systému povolen, pokud si čtyřčíslicová čísla odpovídají (krok 509), nebo je přístup do systému odmítnut, pokud si čtyřčíslicová čísla neodpovídají (krok 510).

V případě, že bankovní nebo kreditní karta 3017 má svůj vlastní mikroprocesor (je tedy tak zvanou "inteligentní kartou"), je postupováno podle odlišné procedury. V kroku 508 je vyjmuté PIN číslo předáno do inteligentní karty pro ověření, zda PIN číslo je platné. Pokud toto PIN číslo je platné, je (v kroku 509) udělena autorizace pro příslušnou transakci a je vydán relevantní (první) certifikát, jak je popsáno výše. Pokud PIN číslo platné není, pak je (v kroku 510) autorizace odmítnuta.

Způsob, kterým jsou vykonávány kroky 503 až 506 bude nyní popsán poněkud podrobněji ve spojení s následující tabulkou, ve které jsou a_1, a_2, a_3, a_4, c_1, c_2, c_3 a c_4 desítkovými kódy, z nichž každý má hodnotu mezi "0" a "9". Pokud uživatel uvolní klávesu 2032 Mute v průběhu následujících kroků, znázorněných v tabulce, je rozkrývání sekvence zastaveno. Potom je nezbytné opětovně začít celou operaci. Je třeba uvést, že při uvolnění klávesy Mute na straně uživatele je vysílán zkušební Mute kód.

Zvolená klávesa	**Kód vysílaný dálkovým ovladačem**
Mute	Mute
Mute + (a_1)	Žádný
Mute + (a_2)	Žádný
Mute + (a_3)	Žádný
Mute + (a_4)	Žádný
Mute + (c_1)	t_1 = modulo 10 z (a_1 + c_1)
Mute + (c_2)	t_2 = modulo 10 z (a_2 + c_2)
Mute + (c_3)	t_3 = modulo 10 z (a_3 + c_3)
Mute + (c_4)	t_4 = modulo 10 z (a_4 + c_4)
Žádná (uvolnění klávesy Mute)	Mute

Ve spojení s odkazy na obr. 13 je nyní ilustrován druhý šifrovací protokol, který je v zásadě stejný jako již popsaný protokol ve spojení s odkazy na obr. 12. V protokolu podle obr. 13 je ale přidán přídavný bezpečnostní krok.

Tento krok je na obr. 13 označen jako krok 511 a zahrnuje uložení dalšího náhodného čísla do paměti jak dálkového ovladače 2026 tak i řídícího prostředku 2100 přijímače/dekodéru 2020. Takové číslo by ve skutečnosti bylo uloženo obvykle pouze při prvním použití dálkového ovladače 2026.

Toto přídavné náhodné číslo d_1, d_2, d_3, d_4 je kombinováno s prvním náhodným číslem a_1, a_2, a_3, a_4 a s PIN

číslem c_1, c_2, c_3, c_4 pro vytvoření kódovaného čísla t_1, t_2, t_3, t_4.

Tento přídavný krok 511 tudíž zajišťuje zvýšenou bezpečnost ve srovnání s protokolem podle obr. 12.

Obr. 14 ilustruje třetí šifrovací protokol, který je v podstatě stejný jako protokol na obr. 12. ale s dalším krokem 512.

V tomto protokolu paměť 2036 dálkového ovladače má v sobě předem uložené čtyřčíslicové číslo e_1, e_2, e_3, e_4, které je charakteristickou identitou tohoto určitého dálkového ovladače 2026.

Toto přídavné identifikační číslo je kombinováno v kroku 505 s náhodným číslem a_1, a_2, a_3, a_4 a s PIN číslem c_1, c_2, c_3, c_4 uživatele pro vytvoření kódovaného čísla t_1, t_2, t_3, t_4.

Řídící prostředek 2100 přijímače/dekodéru 2020 má prostředek, kterým toto identifikační číslo e_1, e_2, e_3, e_4 určitého dálkového ovladače 2026 může být porovnáno s číslem přijímače/dekodéru 2020 v systému, takže pokud si tato čísla neodpovídají, znamená to, že ovladač 2026 není správný pro tento určitý přijímač/dekodér 2020, což dále znamená, že dceřinná inteligentní karta 3020 a/nebo bankovní nebo kreditní karta 3017 (podle toho o kterou se jedná) nemohou být zpřístupněny tímto přijímačem/dekodérem 2020.

Ačkoliv protokol na obr. 14 ilustruje přidání kroku 512 ke krokům znázorněným na obr. 12, mohl by rovněž zajistit přídavný krok k protokolu znázorněnému na obr. 13, což by dokonce ještě dále zvýšilo poskytovanou bezpečnost. Šifrovací

protokoly ilustrované na obr. 12, obr. 13 a obr. 14 tudíž zajišťují podstatné zvýšení stupně bezpečnosti.

Nyní bude popsán čtvrtý šifrovací protokol, který kombinuje znak přídavného náhodného čísla a znak přídavného identifikačního číslo, podle výše uvedeného popisu. Jednou obzvláštní výhodou této kombinace je to, že umožňuje použití více než jen jednoho dálkového ovladače (každého s odlišným přídavným náhodným číslem) se stejným přijímačem/dekodérem při zajištění, že pro každý takový ovladač je dostupné odlišné přídavné identifikační číslo.

Způsob, kterým jsou uvedené dva znaky kombinovány bude nyní popsán ve spojení s odkazy na sekvenci operací kláves dálkového ovladače, jak je znázorněno v následující tabulce.

Zvolená klávesa	**Kód vysílaný dálkovým ovladačem**
Mute	Mute
Mute + (a_1)	Žádný
Mute + (a_2)	Žádný
Mute + (a_3)	Žádný
Mute + (a_4)	Žádný
Mute + (c_1)	t_1 = modulo 10 z (a_1 + c_1 + d_1)
Mute + (c_2)	t_2 = modulo 10 z (a_2 + c_2 + d_2)
Mute + (c_3)	t_3 = modulo 10 z (a_3 + c_3 + d_3)
Mute + (c_4)	t_4 = modulo 10 z (a_4 + c_4 + d_4)
Mute	jednou Mute
Mute	jednou e_1

Mute	jednou e_2
Mute	jednou e_3
Mute	jednou e_4
Žádná (uvolnění klávesy Mute)	jednou Mute

Je třeba si nejprve všimnout, že je zajištěna kompatibilita s prvním šifrovacím protokolem (popsaným ve spojení s odkazy na obr. 12), takže dálkový ovladač 2026 může, pokud je to žádoucí, komunikovat s přijímačem/dekodérem 2020, který je schopen pracovat pouze podle prvního šifrovacího protokolu (nastavením číslic d_1 až d_4 na nulu). Kompatibilita je zajištěna prostřednictvím automatického vysílání kódu Mute bezprostředně poté, co bylo vysláno t_1, t_2, t_3, t_4. Dekodér pracující podle prvního šifrovacího protokolu tedy bude přijímat všechny kódy potřebné pro jeho úspěšnou funkci.

Po přenosu příkazu Mute po druhé vysílá ovladač přídavné identifikační číslo e_1, e_2, e_3, e_4, před případným vysíláním konečného kódu Mute při uvolnění klávesy Mute na straně uživatele.

V tomto čtvrtém šifrovacím protokolu je kombinováno přídavné náhodné číslo d_1, d_2, d_3, d_4 s prvním náhodným číslem a_1, a_2, a_3, a_4 a PIN číslem c_1, c_2, c_3, c_4 následujícím způsobem (s příkladnou ilustrací pro t_1):

$$\mathbf{t_1 = (a_1 + c_1 + d_1) \bmod 10}$$

Přídavné náhodné číslo je zjištěno přijímačem/dekodérem 2020 následujícím způsobem (s příkladnou ilustrací pro c_1):

$$c_1 = (t_1 - (a_1 + d_1) + 10) \bmod 10$$

Stále ve spojení s odkazy na shora uvedenou tabulku bude nyní uveden popis toho, jak jsou přídavné náhodné číslo a přídavné identifikační číslo nejprve vytvořeny a uloženy.

Náhodné číslo je vytvořeno přijímačem/dekodérem 2020 stejným způsobem jako první náhodné číslo (a_1, a_2, a_3, a_4). Toto přídavné náhodné číslo (d_1, d_2, d_3, d_4) je ale vytvořeno pouze jednou, následně je uloženo ve Flash paměti 4024 dekodéru pro použití, kdykoliv je žádáno zadat PIN číslo s použitím dálkového ovladače 2026.

Přídavné identifikační číslo (e_1, e_2, e_3, e_4) je přijímačem/dekodérem 2020 vytvořeno jako další náhodné číslo a opět je uloženo ve Flash paměti 4024 pro budoucí použití.

Když je dálkový ovladač 2026 použit poprvé (a v jakýkoliv počáteční okamžik po výměně baterií, které vymazalo paměť 2036) jsou d_1, d_2, d_3, d_4 a e_1, e_2, e_3, e_4 nastaveny na nulu. Řídící prostředek 2100 přijímače/dekodéru 2020 porovnává hodnotu e_1, e_2, e_3, e_4 s nulou a výsledek porovnání je kladný. Řídící prostředek tudíž vytváří zprávu pro zobrazení na televizní obrazovce, která žádá uživatele, aby zadal hodnoty, vždy se stlačenou klávesou Mute, podle následující tabulky.

Zvolená klávesa	Kód vysílaný dálkovým ovladačem
Mute	Mute
Mute + pilote	Pilote
Mute + (d_1)	d_1
Mute + (d_2)	d_2
Mute + (d_3)	d_3
Mute + (d_4)	d_4
Mute + (e_1)	e_1
Mute + (e_2)	e_2
Mute + (e_3)	e_3
Mute + (e_4)	e_4
Mute + Progr	Progr
Žádná (uvolnění klávesy Mute)	jednou Mute

Řídicí klávesy 2031 "Pilote" a "Progr" jsou zvoleny proto, že nemají žádnou funkci vztahující se k předkládanému příkladu. Samozřejmě by mohly být zvoleny jakékoliv jiné vhodné klávesy.

Z tabulky je možné vypozorovat, že na uživateli je požadováno, aby zadal hodnoty d_1, d_2, d_3, d_4 a e_1, e_2, e_3, e_4 jako výstup z řídicího prostředku a čtené z televizní obrazovky. Při stlačení klávesy Progr pod druhé paměť 2036 dálkového ovladače 2026 uloží tyto dvě sady hodnot (to jest přídavné heslo a přídavné identifikační číslo).

Když je dálkový ovladač 2026 potom použit podruhé a pokaždé později, jsou z tohoto dálkového ovladače 2026 vysílány uložené, ne-nulové hodnoty přídavného hesla a přídavného identifikačního čísla. Řídící prostředek přijímače/dekodéru 2020 porovnává přídavné identifikační číslo s nulou a získává negativní výsledek. Pokud je tedy výsledek negativní, řídící prostředek pokračuje s vyhodnocováním c_1, c_2, c_3, c_4 z daných hodnot a_1, a_2, a_3, a_4, t_1, t_2, t_3, t_4 a d_1, d_2, d_3, d_4. Při ověření, že hodnoty c_1, c_2, c_3, c_4 jsou správné, řídící prostředek potvrzuje PIN číslo a další zpracování pokračuje, jako bylo popsáno v předcházejícím. Jinak je potvrzení odmítnuto.

Mělo by být zřejmé, že čtvrtý šifrovací protokol poskytuje několik výhod. Za prvé je mnohem bezpečnější v důsledku použití přídavného hesla (které je přitom měněno pouze relativně málo často) a v důsledku použití přídavného identifikačního čísla. Za druhé si tento protokol může poradit s použitím mnoha ovladačů pro jeden přijímač/dekodér; procedura pro uložení přídavného hesla a přídavného identifikačního čísla v dálkovém ovladači může být aplikována pro více než jen jeden dálkový ovladač. Za třetí dálkový ovladač může komunikovat účinně s přijímačem/dekodérem, který může pracovat pouze podle prvního protokolu v důsledku použití společných kódů.

Jak bylo uvedeno výše, je jedním z cílů vynálezu zjednodušit život uživatel na nejvyšší možnou míru prostřednictvím omezení počtu akcí, které uživatel musí provést, aby vykonal finanční transakci s použitím dálkového ovladače 2026. Obr. 15 ilustruje další (pátý) šifrovací protokol, který zjednodušuje akce, které musí být provedeny

uživatelem. V tomto protokolu přijímač/dekodér 2020 nejprve vytváří náhodné číslo a_1, a_2, a_3, a_4 v kroku 500. Ovšem, na rozdíl k protokolům ilustrovaným na obr. 12 až obr. 14, dekodér 2020 potom vysílá prostřednictvím infra-červeného paprsku náhodné číslo a_1, a_2, a_3, a_4 do ovladače 2026, kde je uloženo v paměti 2036 ovladače. To je namísto zobrazení náhodného čísla a_1, a_2, a_3, a_4 na televizní obrazovce.

Zbývající kroky tohoto protokolu jsou stejné, jako kroky 504 až 510 v protokolu ilustrovaném na obr. 14.

S tímto uspořádáním uživatel musí pouze zadat jedno čtyřčíslicové číslo, jmenovitě PIN číslo c_1, c_2, c_3, c_4 uživatele, namísto toho, aby musel zadávat dvě čtyřčíslicová čísla, jako v protokolu podle obr. 14. Je ovšem poněkud snížena bezpečnost tím, že dekodér vysílá náhodné číslo infra-červeným paprskem. Toto vysílání by mohlo být případně zachyceno.

Pro šifrování čtyřčíslicového čísla, určeného k vysílání z dálkového ovladače 2026 do dekodéru 2020, může být použito množství různých způsobů. Funkce modulo je ale patrně dostatečně bezpečná pro účely předkládaného vynálezu.

Mělo by být zcela zřejmé, že předkládaný vynález byl popsán výše čistě prostřednictvím příkladu, a že v rozsahu tohoto vynálezu mohou být provedeny modifikace jednotlivých detailů.

Každý znak popisovaný v popisu a (kde je to vhodné) v nárocích a na výkresech může být vytvořen nezávisle nebo v jakékoliv vhodné kombinaci.

Ve shora zmiňovaných výhodných provedeních byly určité znaky předkládaného vynálezu realizovány s použitím

počítačového softwaru. Ovšem osobám v oboru znalým je přirozeně zcela zřejmé, že jakýkoliv z těchto znaků může být realizován s použitím hardwaru. Navíc by mělo být zcela zřejmé, že funkce prováděné hardwarem, počítačovým softwarem a podobně jsou prováděny na nebo s použitím elektrických a podobných signálů.

Na tomto místě je učiněn odkaz na souběžné patentové přihlášky stejného přihlašovatele, které mají stejné datum podání a následující názvy: vytváření a vysílání signálů (značka zástupce: 73142/PT), Inteligentní karta pro použití s přijímačem kódovaných vysílaných signálů a přijímač (značka zástupce: 73143/PT), Vysílací a přijímací systém a systém s podmíněným přístupem (značka zástupce: 73145/PT), Stahování počítačového souboru z vysílače přes přijímač/dekodér do počítače (značka zástupce: 73146/PT), Vysílání a příjem televizních programů a jiných dat (značka zástupce: 73147/PT), Způsob zavádění dat do MPEG přijímače/dekodéru a MPEG vysílací systém pro jeho realizaci (značka zástupce: 73148/PT), Organizace počítačové paměti (značka zástupce: 73149/PT), Způsob vývoje a testování řídícího programu (značka zástupce: 73150/PT), Vybírání datových úseků z vysílaného datového toku (značka zástupce: 73151/PT), Systém řízení přístupu (značka zástupce: 73152/PT), Systém pro zpracování dat (značka zástupce: 73153/PT), Vysílací a přijímací systém, přijímač/dekodér a vzdálená řídící jednotka (značka zástupce: 73154/PT). Popisy těchto dokumentů jsou začleněny do tohoto popisu prostřednictvím odkazu. Seznam přihlášek obsahuje předkládanou přihlášku.

Zastupuje :

P A T E N T O V É N Á R O K Y

1. Zařízení zahrnující přijímač/dekodér pro použití při příjmu televizního nebo rádiového programu nebo datového souboru, v y z n a č u j í c í s e t í m , že zahrnuje prostředek pro interakci s kreditní nebo bankovní kartou uživatele pro čtení kreditní nebo bankovní informace nesené touto kartou, a, odděleně od tohoto prostředku, další interaktivní prostředek pro interakci s kartou uživatele pro čtení informace nesené touto kartou.

2. Zařízení podle nároku 1, v y z n a č u j í c í s e t í m , že je uspořádáno pro interakci s kreditní nebo bankovní kartou zahrnující mikroprocesor.

3. Zařízení podle nároku 2, v y z n a č u j í c í s e t í m , že je uspořádáno pro poskytnutí informace do mikroprocesoru.

4. Zařízení podle kteréhokoliv z předcházejících nároků, v y z n a č u j í c í s e t í m , že dále zahrnuje prostředek pro vysílání do vzdáleného centra debetní instrukce na základě informace nesené kreditní nebo bankovní kartou.

5. Zařízení podle kteréhokoliv z předcházejících nároků, v y z n a č u j í c í s e t í m , že dále zahrnuje prostředek uspořádaný pro přijetí autorizační informace ze vzdáleného centra.

6. Zařízení podle nároku 5, v y z n a č u j í c í s e t í m , že je uspořádáno pro řízení dekódování nebo dešifrování programu nebo souboru v závislosti na autorizační informaci.

7. Zařízení podle kteréhokoliv z předcházejících nároků, v y z n a č u j í c í s e t í m , že dále zahrnuje prostředek pro uložení přijaté kreditní informace, reprezentující kredity dostupné pro nákup produktů, do paměťového prostředku karty uživatele.

8. Zařízení podle nároku 4, v y z n a č u j í c í s e t í m , že je uspořádáno pro vyslání debetních instrukcí do vzdáleného centra a pro modifikaci přijaté kreditní informace, uložené v kartě uživatele, prostřednictvím zvýšení počtu kreditů uložených na kartě uživatele v odezvě na platbu prostřednictvím bankovní nebo kreditní karty.

9. Zařízení podle nároku 8, v y z n a č u j í c í s e t í m , že je uspořádáno pro provádění nákupu kreditů postačujících pro umožnění nákupu množství produktů při každé transakci, ve které je debetní instrukce vyslána do vzdáleného centra.

10. Zařízení podle kteréhokoliv z předcházejících nároků, v y z n a č u j í c í s e t í m , že dále zahrnuje prostředek pro zpracování dat, reprezentujících bankovní nebo kreditní kartu uživatele, společně s přijatými daty, reprezentujícími nabízenou položku nebo službu, a pro vysílání objednávkové žádosti do vzdáleného centra pro zpracování.

11. Zařízení podle nároku 10, v y z n a č u j í c í s e t í m , že zahrnuje prostředek pro zadání žádosti od uživatele pro nákup nabízené položky.

12. Zařízení podle kteréhokoliv z předcházejících nároků, v y z n a č u j í c í s e t í m , že dále zahrnuje prostředek přijetí PIN čísla.

13. Zařízení podle kteréhokoliv z předcházejících nároků, v y z n a č u j í c í s e t í m , že má formu nastavovací řídící skříně.

14. Zařízení podle kteréhokoliv z předcházejících nároků, v y z n a č u j í c í s e t í m , že je upraveno pro příjem satelitně vysílaných programů nebo souborů, výhodně digitálních satelitních programů nebo souborů.

15. Přijímač/dekodér pro použití v digitálním satelitním televizním systému, v y z n a č u j í c í s e t í m , že zahrnuje dekodér, prostředek pro přijetí kreditní nebo bankovní karty nesoucí mikroprocesor, prostředek pro interakci s uvedeným mikroprocesorem, když je kreditní nebo bankovní karta vložena do pracovní polohy v uvedeném přijímači/dekodéru pro umožnění čtení dat nesených uvedenou kreditní nebo bankovní kartou a pro zadání dat do mikroprocesoru neseného uvedenou kreditní nebo bankovní kartou, a prostředek pro přijetí inteligentní karty, přičemž vložení inteligentní karty koncovým uživatelem do přijímače/dekodéru umožní této inteligentní kartě interagovat s prostředkem v uvedeném přijímači/dekodéru, přičemž produkt zvolený koncovým uživatelem může být dodán do uvedeného přijímače/dekodéru a odtud do televizního zařízení nebo osobního počítače, se kterými je přijímač/dekodér spojen.

16. Digitální satelitní rádiový nebo televizní systém mající množství zakončení koncových uživatelů, v y z n a č u j í c í s e t í m , že každé zakončení zahrnuje přijímač/dekodér podle nároku 15.

17. Způsob zajištění objednávky pro položku nebo službu, v y z n a č u j í c í s e t í m , že zahrnuje v přijímači/dekodéru, ve kterém je přijata informace týkající se položky nebo služby, čtení informace z bankovní nebo kreditní karty, vytvoření objednávkové žádosti obsahující informaci identifikující položku nebo službu a informaci reprezentující informaci o bankovní nebo kreditní kartě, ověření vzdáleného centra a následně vysílání objednávkové informace do vzdáleného centra pro zpracování.

18. Způsob podle nároku 17, v y z n a č u j í c í s e t í m , že krok ověření vzdáleného centra zahrnuje kroky předání náhodného čísla do vzdáleného centra, přijetí náhodného číslo v šifrované formě ze vzdáleného centra, a dešifrování šifrovaného náhodného čísla pro ověření vzdáleného centra.

19. Způsob podle nároku 17 nebo 18 , v y z n a č u j í c í s e t í m , že dále zahrnuje ve vzdáleném centru zpracování objednávkové informace a určení, zda autorizovat transakci na základě informace o bankovní nebo kreditní kartě.

20. Zařízení podle kteréhokoliv z nároků 1 až 14, v y z n a č u j í c í s e t í m , že dále zahrnuje dálkový ovladač pro vysílání Osobního identifikačního čísla (PIN) uživatele do přijímače/dekodéru.

21. Zařízení podle nároku 20, v y z n a č u j í c í s e t í m , že dálkový ovladač zahrnuje bezpečnostní prostředek pro zajištění bezpečnosti vysílání.

22. Dálkový ovladač pro komponent vybavení, mající prostředek, kterým může být osobní identifikační číslo (PIN) uživatele vysílání do komponentu vybavení, v y z n a č u j í c í s e t í m , že zahrnuje bezpečnostní prostředek pro zajištění bezpečnosti uvedeného vysílání.

23. Dálkový ovladač pro komponent vybavení, který zahrnuje:
prostředek definující tělo uvedeného ovladače;
prostředek pro vysílání osobního identifikačního čísla (PIN) do uvedeného komponentu vybavení; a,
v y z n a č u j í c í s e t í m , že zahrnuje bezpečnostní prostředek pro zajištění bezpečnosti uvedeného vysílání.

24. Dálkový ovladač podle kteréhokoliv z nároků 22 až 23, v y z n a č u j í c í s e t í m , že vysílací prostředek zahrnuje prostředek pro vytváření infra-červeného paprsku.

25. Dálkový ovladač podle kteréhokoliv z nároků 22 až 24, v y z n a č u j í c í s e t í m , že uvedený bezpečnostní prostředek zahrnuje prostředek pro šifrování PIN čísla.

26. Dálkový ovladač podle nároku 25, v y z n a č u j í c í s e t í m , že uvedený šifrovací prostředek zahrnuje prostředek pro kombinování PIN čísla s náhodným číslem.

27. Dálkový ovladač podle nároku 26, v y z n a č u j í c í s e t í m , že dále zahrnuje prostředek pro umožnění uživateli zadat náhodné číslo.

28. Dálkový ovladač podle nároku 27, v y z n a č u j í c í s e t í m , že uvedený zadávací prostředek zahrnuje alespoň jednu klávesu pro zadání náhodného čísla a další klávesu, přičemž ovladač je uspořádán tak, že PIN číslo je vysíláno přes vysílací prostředek pouze při stlačení této další klávesy.

29. Dálkový ovladač podle kteréhokoliv z nároků 25 až 28, v y z n a č u j í c í s e t í m , že uvedený šifrovací prostředek zahrnuje prostředek pro uložení náhodného čísla v ovladači.

30. Dálkový ovladač podle kteréhokoliv z nároků 22 až 29, v y z n a č u j í c í s e t í m , že uvedený bezpečnostní prostředek zahrnuje prostředek pro vytváření číselných charakteristik jednotlivého ovladače pro vysílání přes uvedený vysílací prostředek do komponentu vybavení.

31. Dálkový ovladač podle kteréhokoliv z nároků 25 až 29, v y z n a č u j í c í s e t í m , že uvedený šifrovací prostředek zahrnuje prostředek pro vytváření číselných charakteristik jednotlivého dálkového ovladače a prostředek pro kombinování uvedených číselných charakteristik s uvedeným náhodným číslem a uvedeným PIN číslem.

32. Dálkový ovladač podle kteréhokoliv z nároků 25 až 31, v y z n a č u j í c í s e t í m , že uvedený šifrovací prostředek zahrnuje prostředek pro přijetí náhodného čísla od uvedeného komponentu vybavení a prostředek

pro kombinování tohoto náhodného čísla s PIN číslem uživatele pro vysílání přes vysílací prostředek do uvedeného komponentu vybavení.

33. Kombinace, v y z n a č u j í c í s e t í m , že zahrnuje dálkový ovladač podle kteréhokoliv z nároků 22 až 32 a uvedený komponent vybavení, přičemž tento komponent vybavení má prostředek pro přijetí PIN čísla uživatele.

34. Kombinace podle nároku 33, v y z n a č u j í c í s e t í m , že uvedený komponent vybavení zahrnuje prostředek pro vytváření náhodného čísla a prostředek pro předání uvedeného náhodného čísla do zobrazovací jednotky.

35. Kombinace podle nároku 33 nebo 34, v y z n a č u j í c í s e t í m , že uvedený komponent vybavení zahrnuje prostředek pro vytváření náhodného čísla a prostředek pro vysílání uvedeného náhodného čísla do uvedeného dálkového ovladače.

36. Kombinace podle kteréhokoliv z nároků 33 až 35, v y z n a č u j í c í s e t í m , že uvedený komponent vybavení zahrnuje zařízení podle kteréhokoliv z nároků 1 až 14.

37. Digitální televizní systém, v y z n a č u j í c í s e t í m , že zahrnuje komponent televizního vybavení, přičemž uvedený komponent má prostředek pro přijetí PIN čísla uživatele, a dálkový ovladač podle kteréhokoliv z nároků 22 až 32.

38. Digitální televizní systém, v y z n a č u j í c í s e t í m , že zahrnuje:

komponent televizního vybavení, přičemž uvedený

komponent má prostředek pro přijetí PIN čísla; a dálkový ovladač, přičemž uvedený ovladač zahrnuje: prostředek definující tělo uvedeného ovladače; prostředek pro vysílání PIN čísla uživatele do uvedeného komponentu vybavení; a bezpečnostní prostředek pro zajištění bezpečnosti uvedeného vysílání.

39. Způsob zadávání PIN čísla do televizního systému, v y z n a č u j í c í s e t í m , že zahrnuje použití dálkového ovladače, definovaného podle kteréhokoliv z nároků 22 až 32, pro vysílání uvedeného PIN čísla do televizního zařízení.

40. Přijímač/dekodér v podstatě podle zde uvedeného popisu a podle znázornění na připojených výkresech.

41. Digitální satelitní televizní systém v podstatě podle zde uvedeného popisu a podle znázornění na připojených výkresech.

42. Dálkový ovladač v podstatě podle zde uvedeného popisu a podle znázornění na obr. 7, obr. 10 a obr. 11 až obr. 15 připojených výkresů.

Zastupuje :

Fig.1.

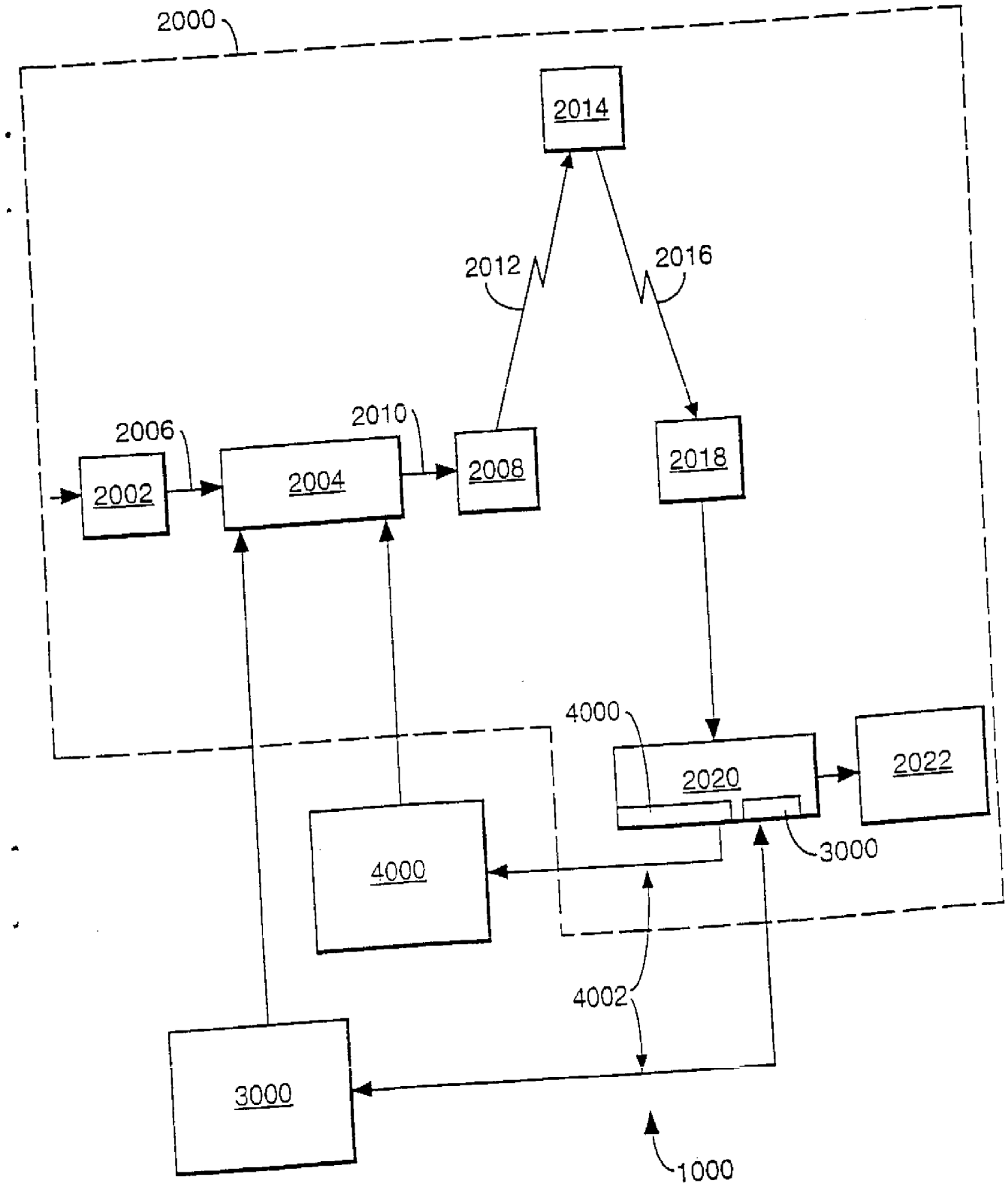
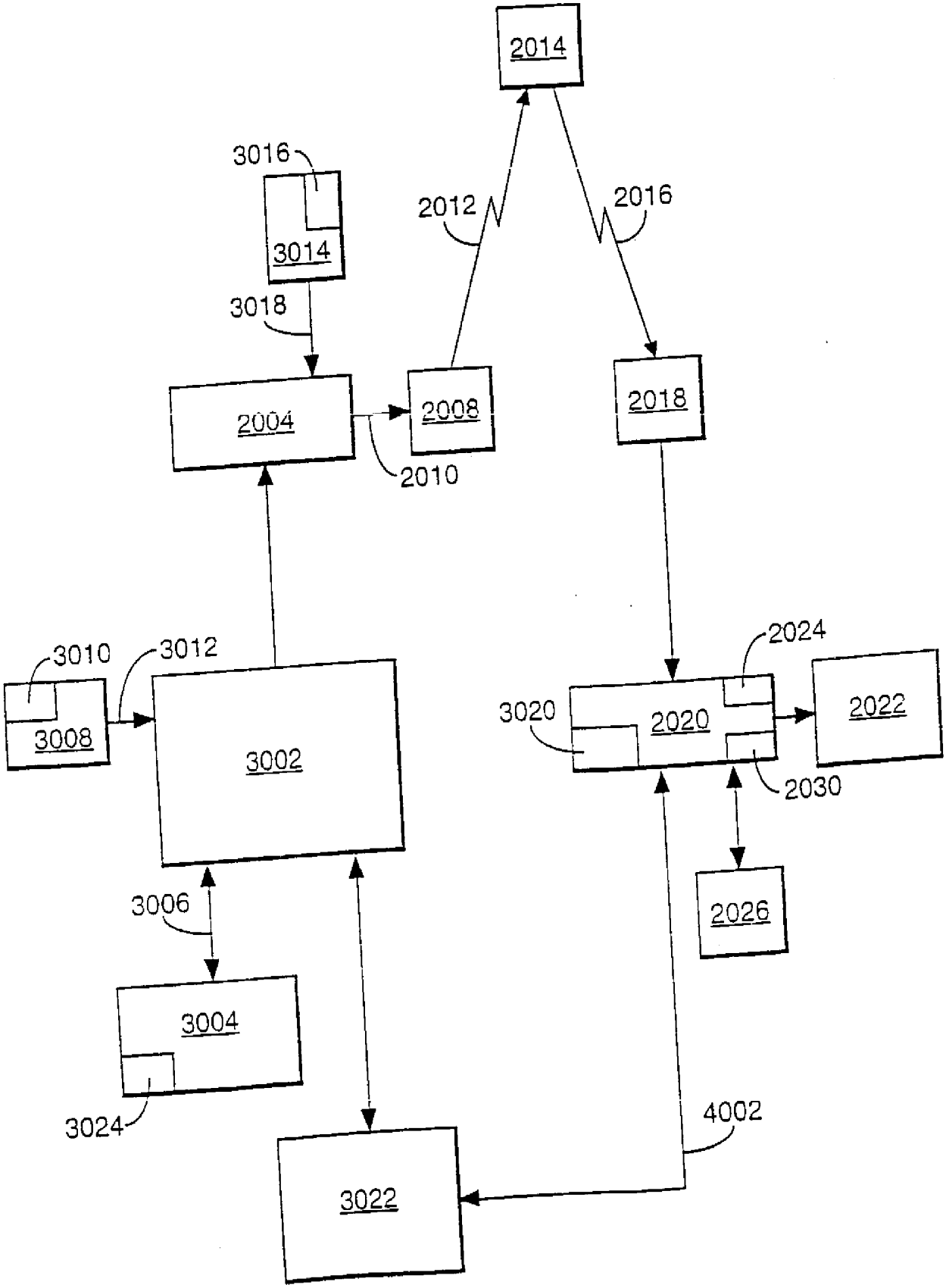

2000
2014
2012
2016
2006
2010
2002
2004
2008
2018
4000
2020
2022
3000
4000
4002
3000
1000

Fig.2.


2014
3016
3014
2012
2016
3018
2004
2008
2018
2010
3010
3012
3008
3002
2024
3020
2020
2022
2030
2026
3006
3004
3024
4002
3022

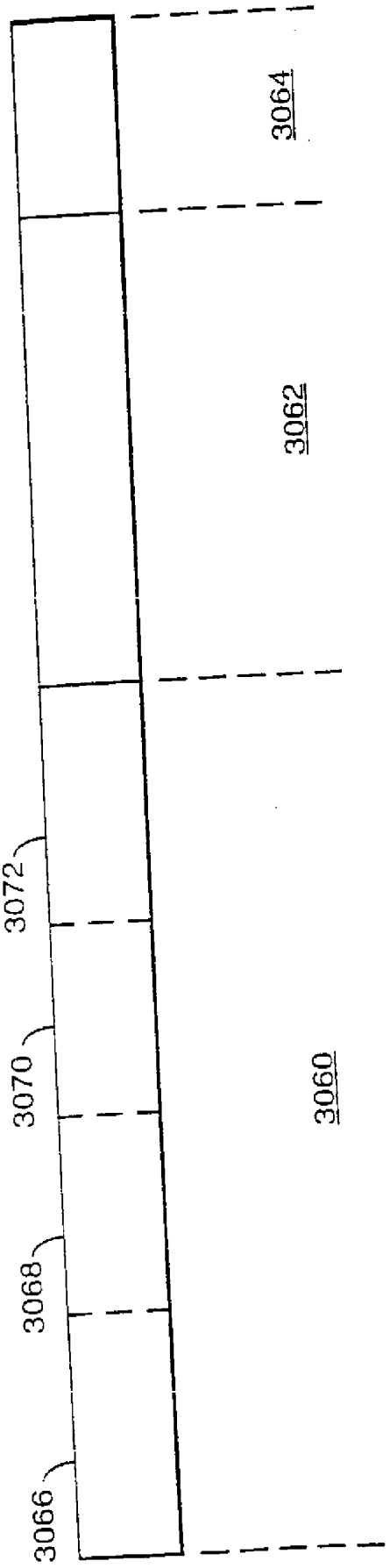


Fig.3.

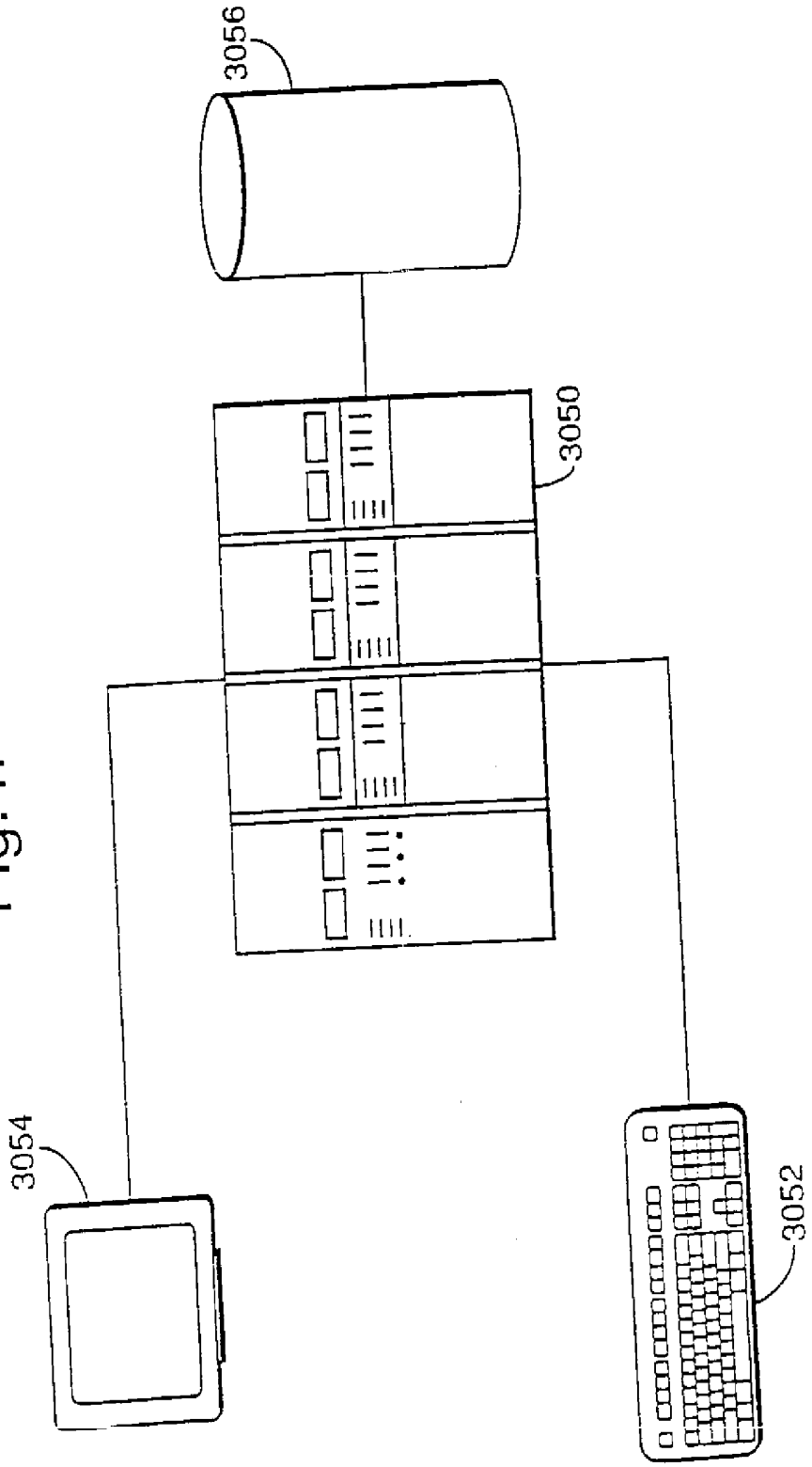


Fig.4.

Fig.5.

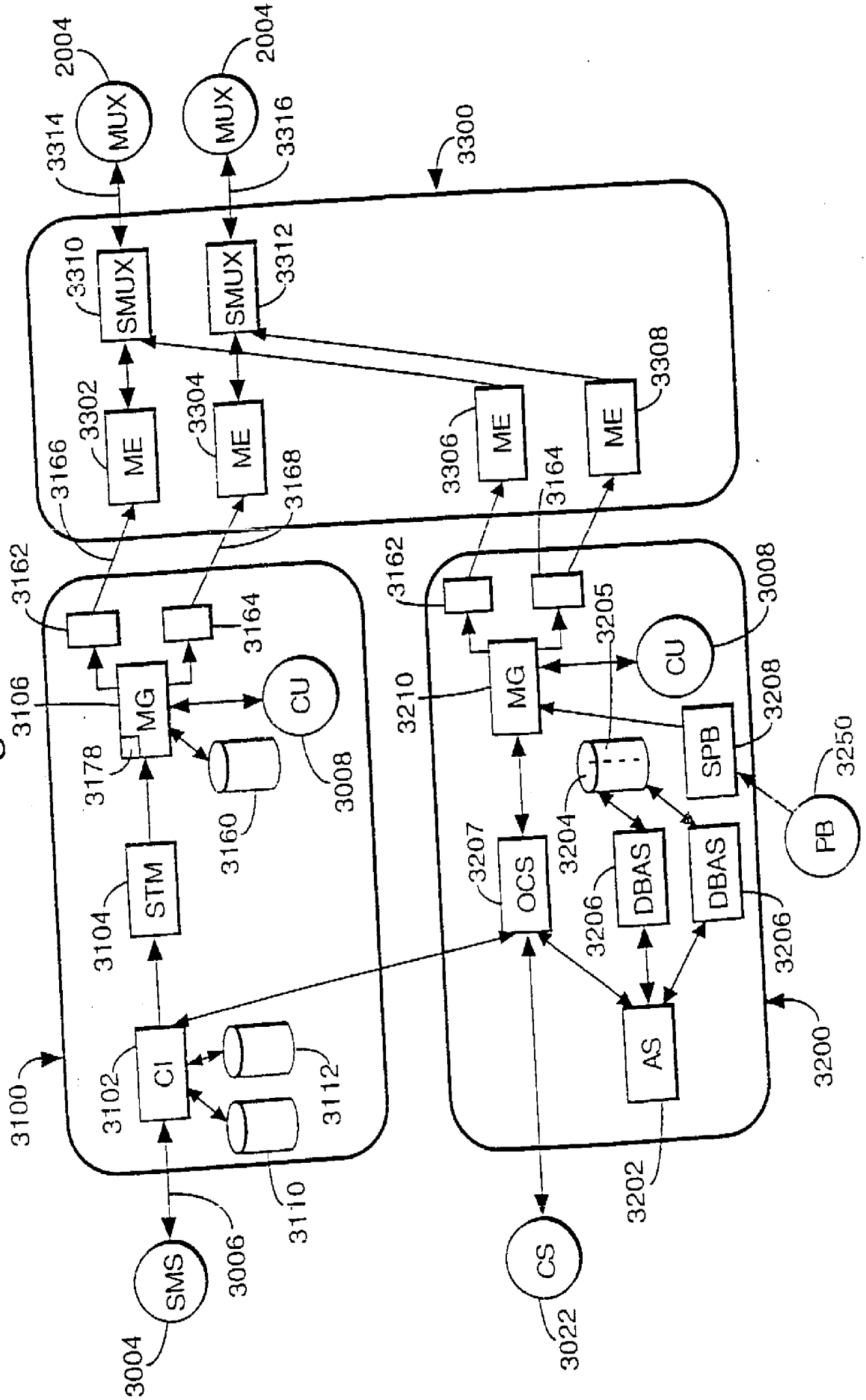

2004
MUX
3314
2004
MUX
3316
3300
3310
SMUX
3312
SMUX
3302
ME
3304
ME
3166
3168
3306
ME
3308
ME
3164
3162
3162
3106
MG
3164
3178
CU
3008
3160
3100
3102
CI
3112
3104
STM
3110
3006
SMS
3004
3210
MG
3205
CU
3008
3208
SPB
3250
PB
3204
3207
OCS
DBAS
DBAS
3206
3206
AS
3200
3202
CS
3022

Fig.6.

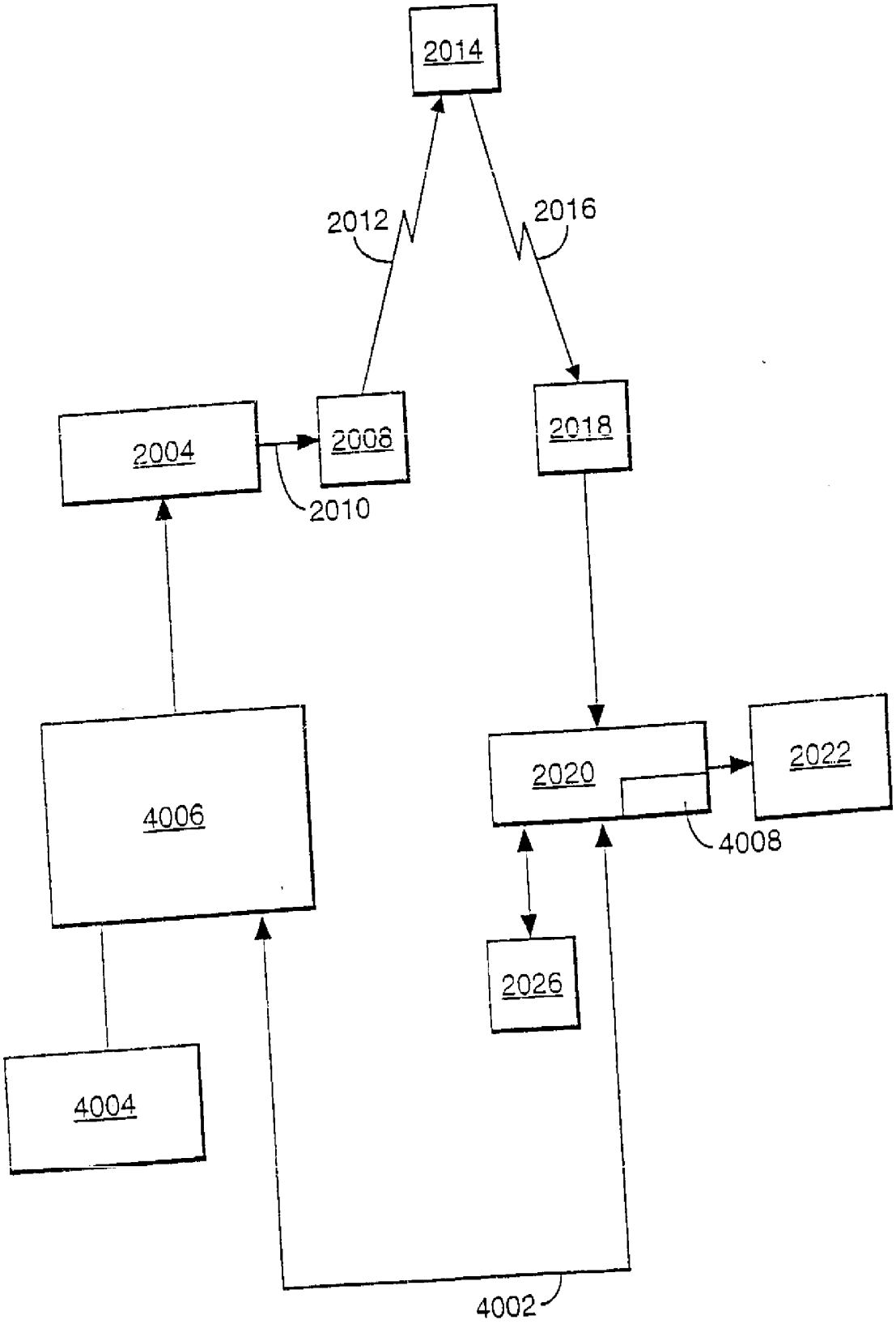

2014
2012
2016
2004
2008
2010
2018
4006
2020
2022
4008
2026
4004
4002

Fig.7.

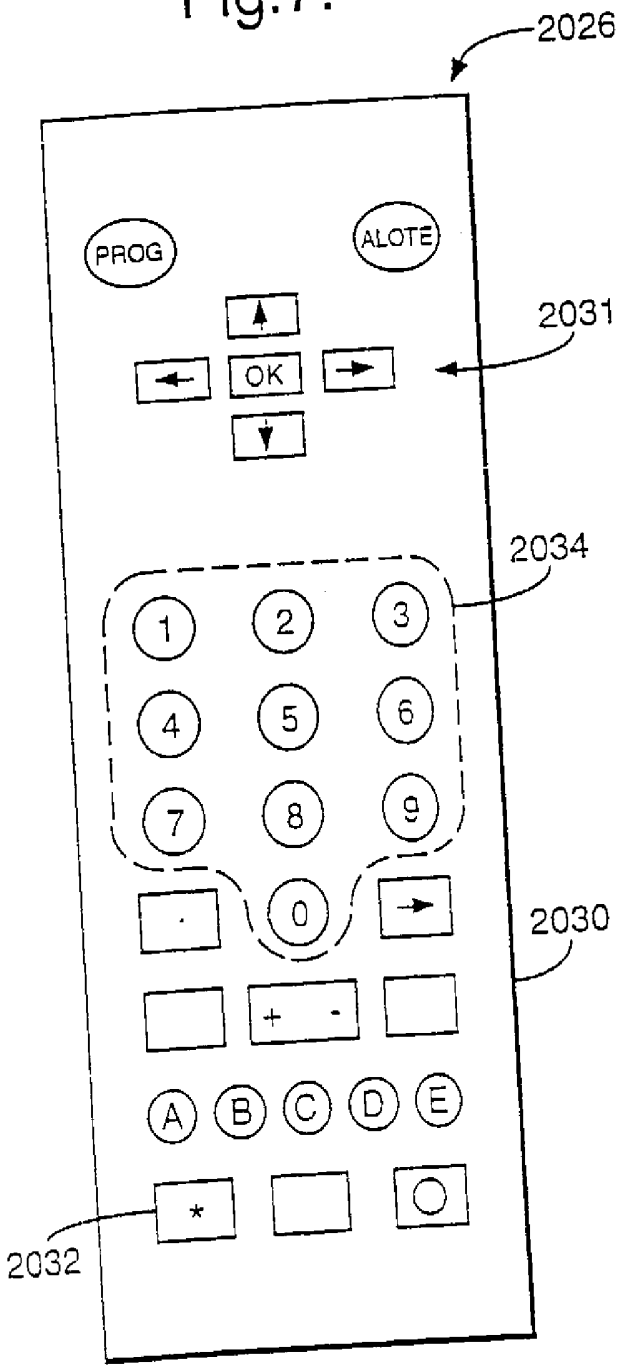


Fig.8.

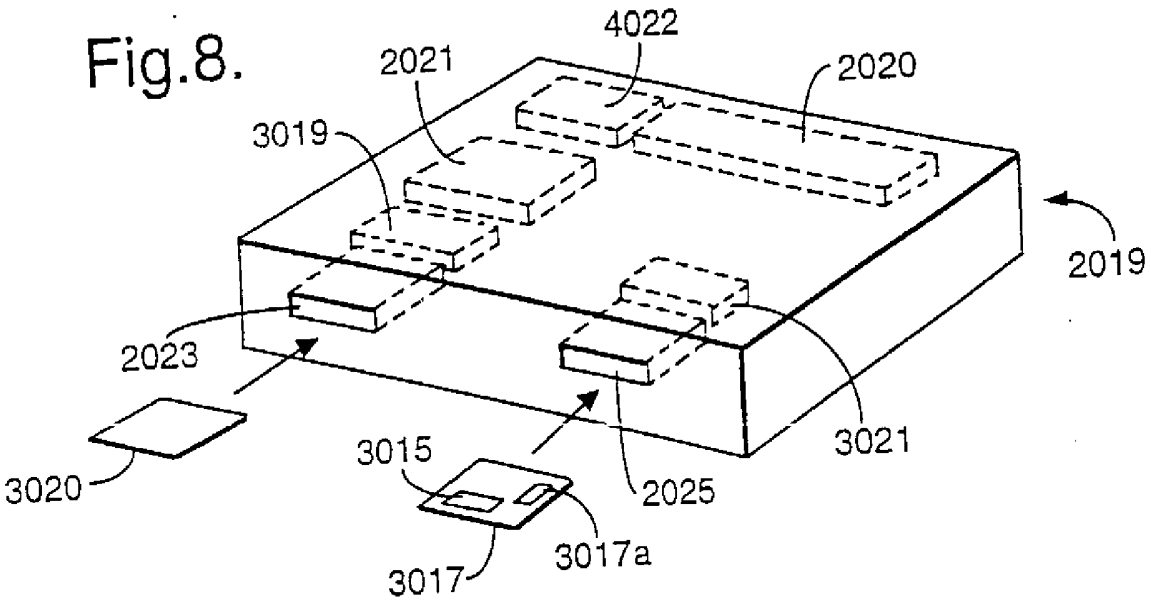

4022
2021
2020
3019
2019
2023
3021
3015
2025
3020
3017a
3017

Fig.9.

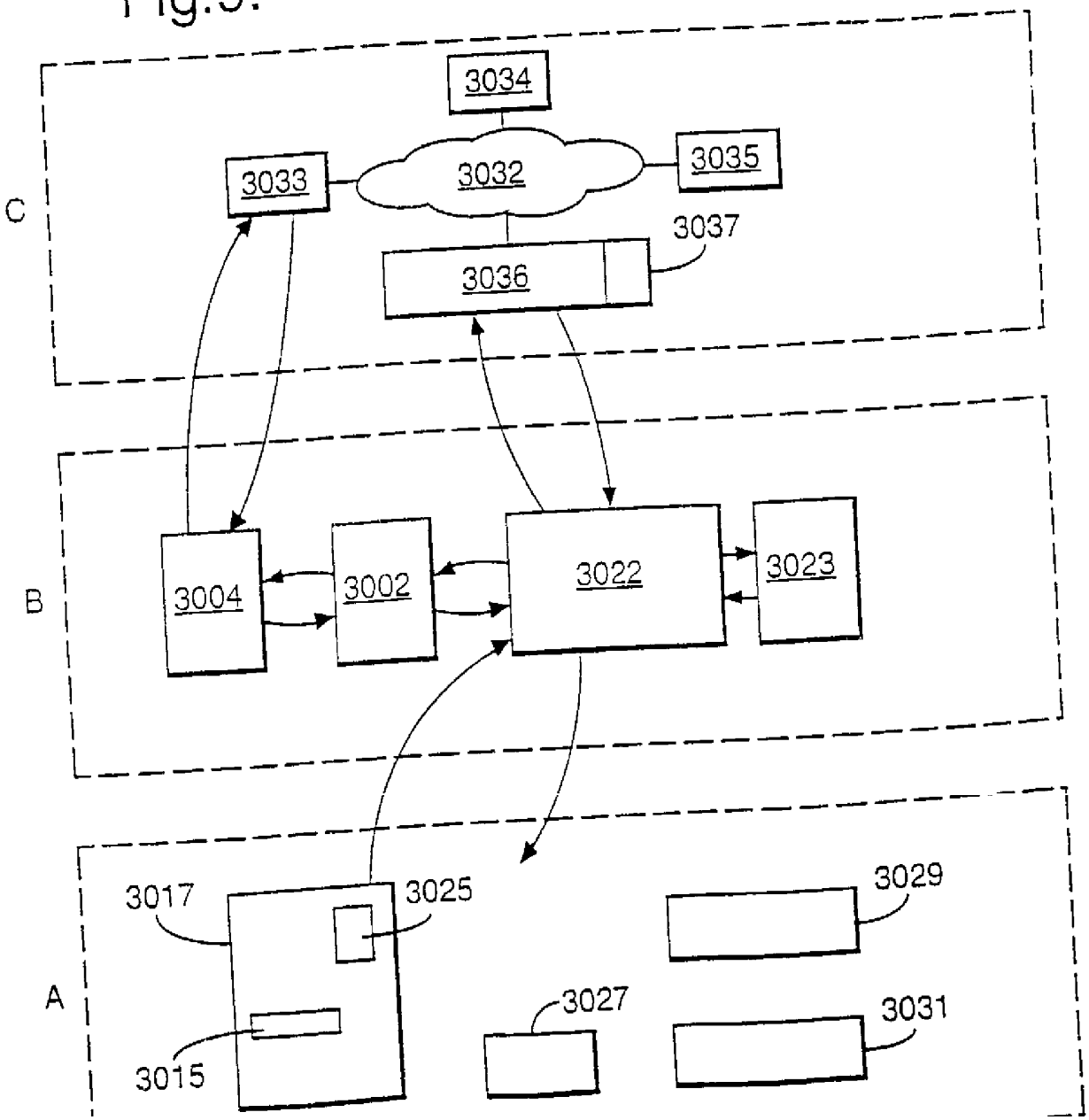

3034
3033
3032
3035
C
3037
3036
3004
3002
3022
3023
B
3017
3025
3029
A
3027
3031
3015

Fig.10.

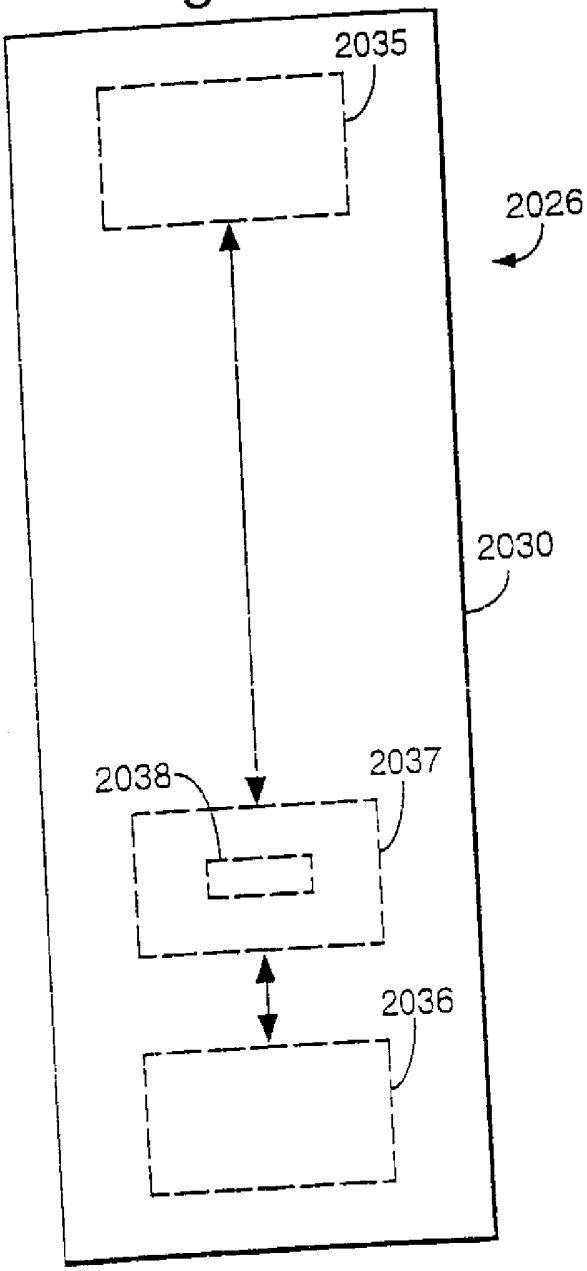


Fig.11.

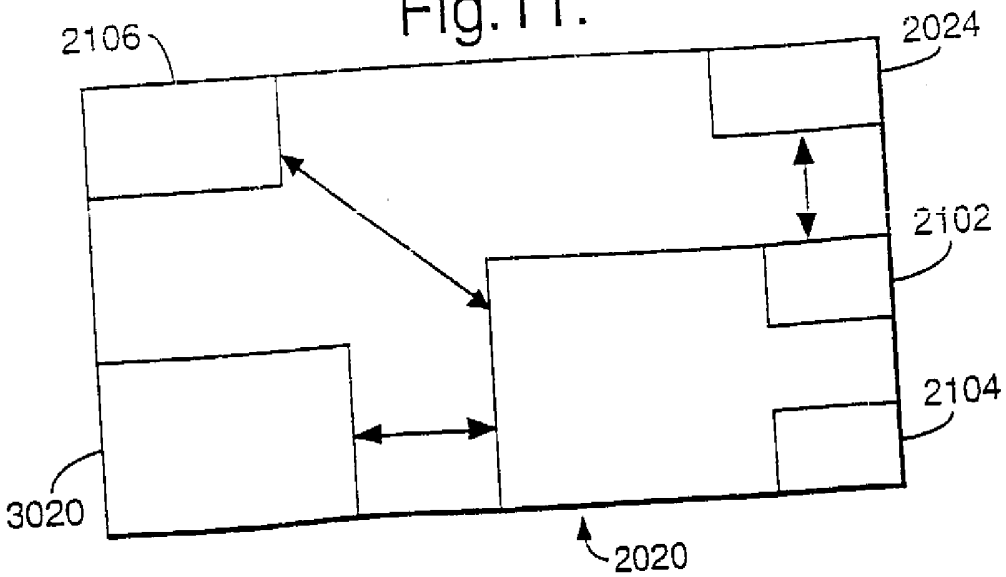


Fig.12.

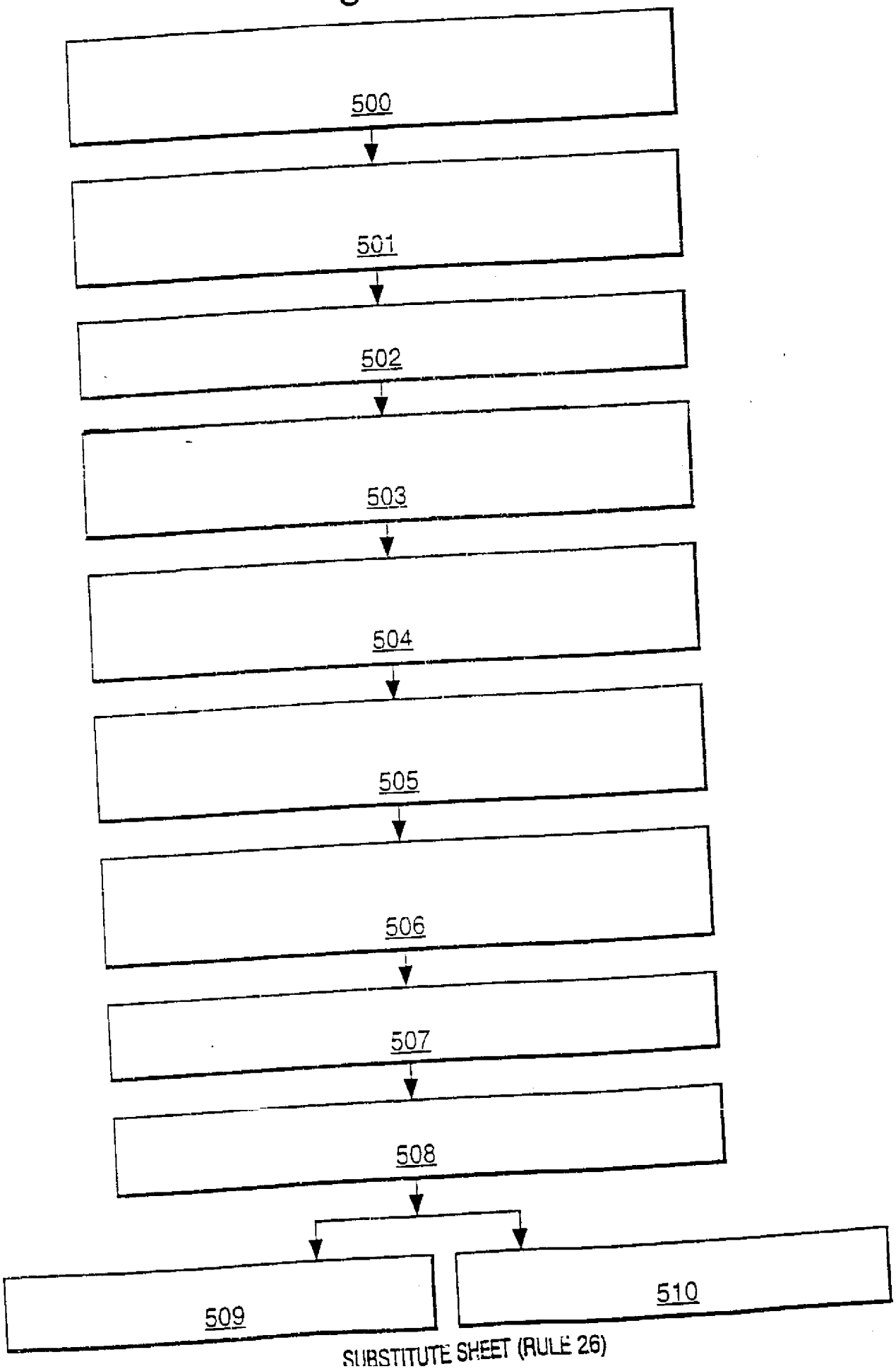


Fig.13.

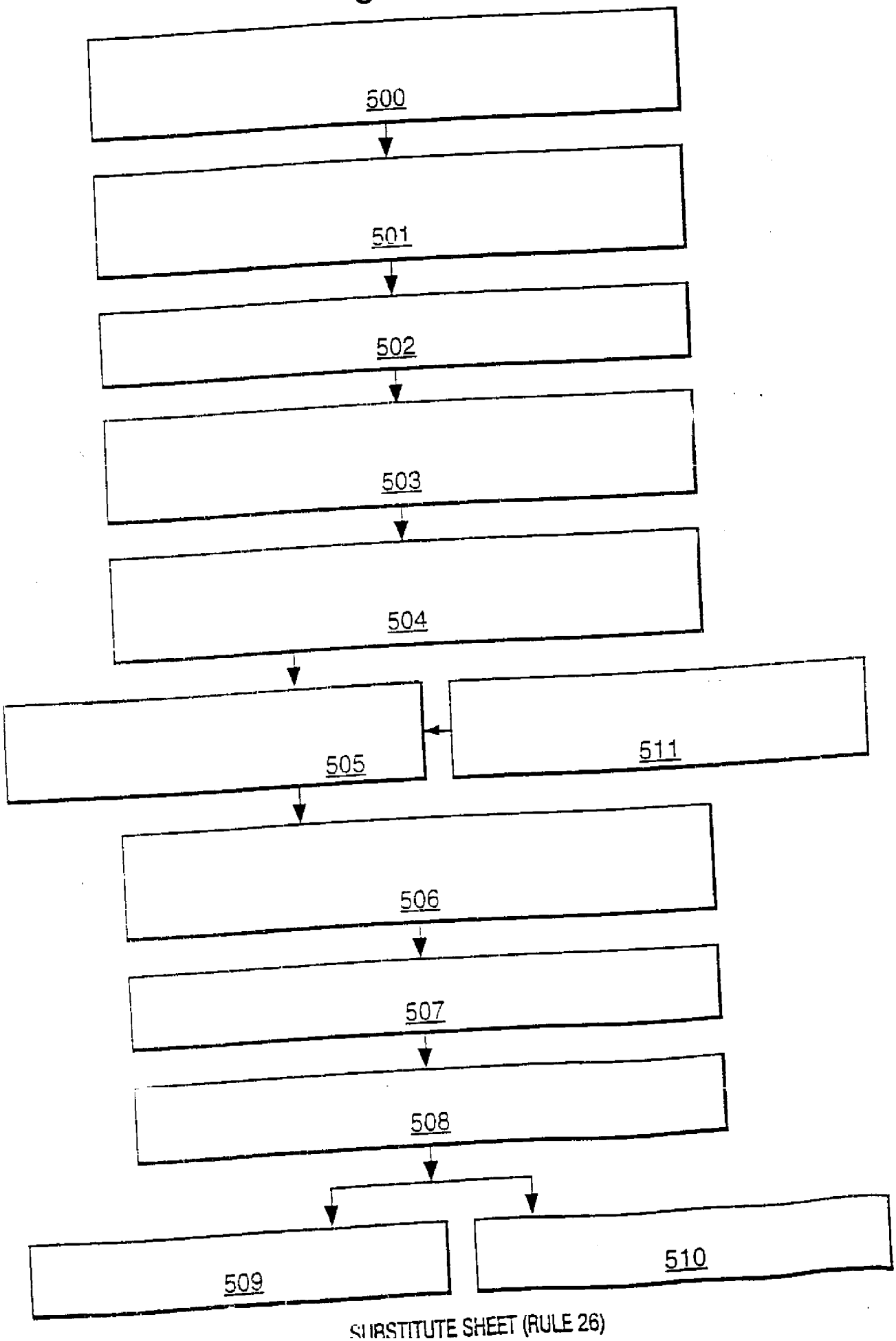


Fig.14.

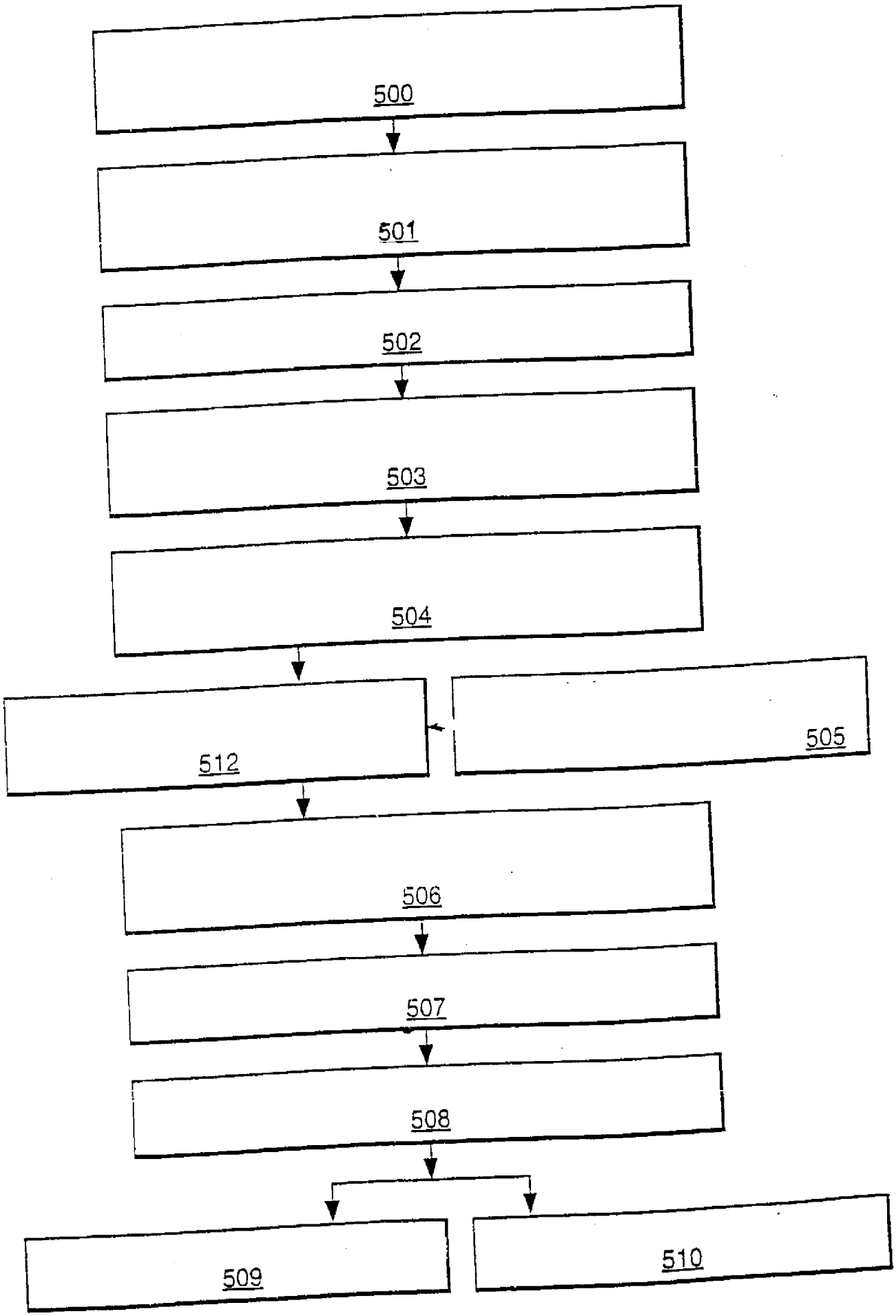


Fig.15.