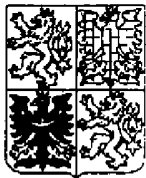


PŘIHLÁŠKA VYNÁLEZU

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

(19)
ČESKÁ
REPUBLICA



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: 12.07.2000
(Věstník č. 7/2000)
(86) PCT číslo: PCT/EP97/02108
(87) PCT číslo zveřejnění: WO98/43426

(21) Číslo dokumentu:

1999 - 3310

(13) Druh dokumentu: A3

(51) Int. Cl. 7:

H 04 N 7/16

H 04 N 7/167

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

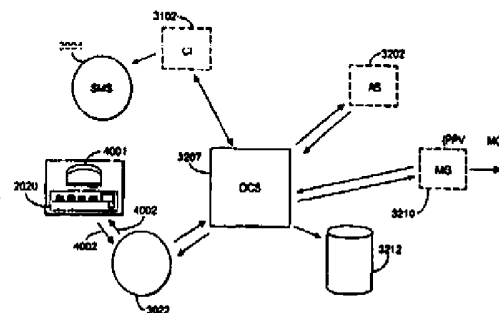
(72) Původce:
Bayassi Mulham, Paris, FR;
De La Tullaye Pierre, Rueil Malmaison, FR;
Jezequel Jean-Francois, Cormeille en Parisis, FR;

(74) Zástupce:
Korejzová Zdeňka JUDr., Spálená 29, Praha 1, 11000;

(54) Název přihlášky vynálezu:
**Vysílací a přijímací systém a systém s
podmíněným přístupem**

(57) Anotace:

Digitální televizní systém má množství nastavovacích řídicích skříní (STB) s množstvím televizních přijímačů koncových uživatelů, s modemem a dekodérem umístěným v každé (STB), účastnický autorizační systém (SAS), zahrnující nebo mající se sebou sdružené množství komunikačních obslužných kanálů, prostředek začleněný v (SAS) pro vytváření elektronických řídicích zpráv (EMM), zpětný kanál propojující každou z (STB) jednotlivě se (SAS), prostředkem začleněným v (SAS) a každou (STB), takže potřebná informace, vyžadovaná pro zavedení relevantní řídicí zprávy (EMM) do systému, je dodána přímo do relevantního komunikačního obslužného kanálu, začleněného v nebo sdruženého se (SAS), pro autorizaci uvolnění uvedené řídicí zprávy (EMM) a/nebo prostředku pro spojení modemu se zpětným kanálem, přičemž řídicí zprávy (EMM) lze vysílat do dekodéru přímo z relevantního komunikačního kanálu, začleněného v nebo sdruženého se (SAS).





Vysílací a přijímací systém a systém s podmíněným přístupem

Oblast techniky

5

Předkládaný vynález se týká vysílacího a přijímacího systému, zejména digitálního, interaktivního, satelitního televizního systému hromadného trhu, a systému s podmíněným přístupem pro tento systém.

Dosavadní stav techniky

10

Zejména, ale ne výhradně, se předkládaný vynález týká vysílacího systému hromadného trhu, který má některé nebo všechny z následujících výhodných znaků:-

15

- Je informačním vysílacím systémem, výhodně rádiovým a/nebo televizním vysílacím systémem.
- Je satelitním systémem (přestože by mohl být použitelný pro kabelový nebo pozemní přenos).
- Je digitálním systémem, výhodně využívajícím MPEG, zvláště výhodně MPEG-2, kompresní systém pro datový/signálový přenos.
- Poskytuje možnost interaktivity.

20

25

Mnohem přesněji se předkládaný vynález týká tak zvané placené televize (nebo placeného rádia), kde uživatel/divák volí program/film/hru pro sledování, za kterou je třeba provést platbu, to je označováno jako systém plateb za shlédnutí (PPV) nebo v případě, že mají být stahována (zaváděna) data, je to tak zvaný systém plateb za soubor (PPF).

30



U takovýchto známých PPV nebo PPF systémů je vyžadován značný časový interval, který musí být stráven uživatelem/divákem kvůli tomu, aby provedl akce potřebné pro vlastní přístup ke zvolenému produktu.

5 Například u jednoho známého systému je sekvence kroků, které musí být provedeny, následující:-

10 I) Uživatel telefonuje do tak zvaného účastnického řídicího systému (SMS), který v tomto známém systému zahrnuje určitý počet živých operátorů, kteří odpovídají na účastnický hovor a se kterými účastník komunikuje ohledně potřebných informací týkajících se zvoleného produktu a týkajících se finančního stavu účastníka pro tak zvaný účastnický autorizační systém (SAS), který v
15 sobě obsahuje nebo je sdružen s množstvím komunikačních obslužných kanálů.

20 II) Operátor v SMS potom musí zkontrolovat finanční stav uživatele před autorizací připojení od komunikačních obslužných kanálů k televiznímu zařízení účastníka, takže produkt může být dodán k uživateli a sledován tímto uživatelem.

25 V jiném známém systému živý operátor je nahrazen automatickým hlasovým obslužným kanálem, takže když uživatel telefonuje do SMS slyší hlasově aktivované záznamy, se kterými uživatel komunikuje stejné informace jako v systému podle I) výše.

30 Toto druhé uspořádání zmenšuje zpoždění, které je vlastní prvnímu popisovanému uspořádání, které může být mnohem snáze přetíženo, když si velké množství uživatelů přeje objednat produkt ve stejném okamžiku.

Ovšem dokonce i s tímto druhým uspořádáním je na uživateli žádáno, aby zadával značné množství informací ve formě dlouhých sériových čísel, přičemž tato činnost poskytuje značný prostor pro chyby a rovněž je časově náročná.

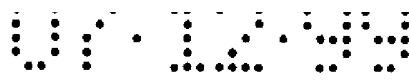
Třetí známé uspořádání vyžaduje na uživateli, aby používal existující systémy na bázi obrazovek, jako je MINITEL ve Francii a PRESTEL ve Velké Británii, přičemž tyto systémy nahrazují hlasově aktivovaný obslužný kanál popisovaný výše ve spojení s druhým uspořádáním. Systémy MINITEL a PRESTEL samy zahrnují modem na výstupu u spotřebitele.

Ve všech těchto známých uspořádáních je na uživateli žádáno, aby vynaložil značné množství času a snažil se zadat všechny informace potřebné pro aktivaci systému, aby docílil autorizace vysílání zvoleného produktu do televizního zařízení uživatele.

V případě satelitního televizního systému zde dochází k dalšímu zpoždění, se kterým uživatel skutečně přijímá zvolený produkt.

V PPV a PPF systémech jsou klíčovým elementem při řízení přístupu uživatele k produktům tak zvané opravňovací řídicí zprávy (EMM), které musí být zaváděny do systému, aby byl poskytnut uživateli přístup k produktům. Mnohem přesněji jsou zprávy EMM mechanismem, prostřednictvím kterého jsou kódovaná data reprezentující produkt dekodována pro určitého jednotlivého uživatele.

Ve známých satelitních televizních systémech jsou zprávy EMM vysílány do televizních zařízení uživatelů přes



satelitní spojení v pravidelných intervalech v MPEG-2 datovém toku. Tedy v případě EMM pro určitého uživatele zde může docházet ke značnému zpoždění o velikosti možná několika minut, než následující vysílání EMM pro uživatele dorazí do příslušného televizního zařízení tohoto uživatele.

Toto zpoždění při vysílání se přidává ke zpoždění popisovanému výše, ke kterému dochází v důsledku toho, že uživatel musí ručně zadávat určitá data do systému. Kumulativní účinek těchto dvou zpoždění může představovat obvykle pět minut pro uživatele, aby byl schopen získat přístup ke zvolenému produktu.

Předkládaný vynález se zabývá překonáním tohoto problému.

Podstata vynálezu

Podle prvního aspektu předkládaného vynálezu je vytvořen systém s podmíněným přístupem, který zahrnuje:

prostředek pro vytváření množství zpráv (výhodně podmíněného přístupu); a

prostředek pro přijímání zpráv, přičemž tento přijímací prostředek je upraven pro komunikaci s uvedeným prostředkem pro vytváření zpráv přes komunikační obslužný kanál spojený přímo s uvedeným prostředkem pro vytváření zpráv.

Výhodně je zprávou opravňovací zpráva pro vysílání (například prostřednictvím vysílání výzev) do přijímacího prostředku, přičemž uvedený prostředek pro vytváření zpráv je upraven pro vytváření opravňovacích zpráv v odezvě na data přijatá z uvedeného přijímacího prostředku.

Prostředek pro vytváření zpráv může být uspořádán pro vysílání zprávy jako paketu digitálních dat do uvedeného přijímacího prostředku přes uvedený komunikační obslužný kanál nebo přes satelitní odpovídač.

5 Přijímací prostředek může být spojitelný s uvedeným komunikačním obslužným kanálem prostřednictvím modemu a telefonní linky.

10 Ve spojení se shora uvedeným popisem předkládaný vynález rovněž navrhuje systém s podmíněným přístupem pro poskytnutí podmíněného přístupu účastníkům, který zahrnuje:

 účastnický řídicí systém;

 účastnický autorizační systém spojený s účastnickým řídicím systémem; a

15 komunikační obslužný kanál; přičemž tento obslužný kanál je spojen přímo s účastnickým autorizačním systémem.

20 Systém může dále zahrnovat přijímač/dekodér pro účastníka, přičemž tento přijímač/dekodér je spojitelný s uvedeným komunikačním obslužným kanálem a tudíž s uvedeným účastnickým autorizačním systémem prostřednictvím modemu a telefonní linky.

Podle druhého aspektu předkládaného vynálezu je vytvořen vysílací a přijímací systém zahrnující systém s podmíněným přístupem podle výše uvedeného popisu.

25 Podle třetího aspektu předkládaného vynálezu je vytvořen vysílací a přijímací systém, který zahrnuje:

 prostředek pro vytváření množství opravňovacích zpráv týkajících se vysílaných programů;

30 prostředek pro přijímání uvedených zpráv od uvedeného prostředku pro vytváření zpráv; a

prostředek pro spojení přijímacího prostředku s prostředkem pro vytváření zpráv pro přijetí uvedených zpráv, přičemž tento spojovací prostředek je schopen realizovat vyhrazené spojení mezi přijímacím prostředkem a prostředkem pro vytváření zpráv.

Vyhrazeným spojením by obvykle mělo být pevně zapojené spojení a/nebo modemové spojení s tou možností, že toto spojení bude provedeno přes celulární telefonní systém. Jinými slovy vyhrazené spojení je schopné vytvořit kanál pro spojení (dvoubodové spojení). To je rozdíl oproti vysílání informace přes vzduch nebo okolní prostředí. Tímto spojovacím prostředkem by tedy měl být obvykle modem v přijímacím prostředku.

Tudíž v souvislosti se shora uvedeným předkládaný vynález rovněž navrhuje vysílací a přijímací systém, který zahrnuje:

prostředek pro vytváření množství opravňovacích zpráv týkajících se vysílaných programů;

prostředek pro přijímání uvedených zpráv z uvedeného prostředku pro vytváření zpráv přes modem; a

prostředek pro spojení uvedeného modemu s uvedeným prostředkem pro vytváření zpráv a uvedeným přijímacím prostředkem.

Shora uvedené znaky mohou poskytnout výhodu zajištění uživatele potřebnou autorizací pro sledování (přes zprávu EMM) mnohem rychleji než doposud vůbec bylo možné, částečně z toho důvodu, že SAS obvykle využívá menší množství strojového kódu než SMS, takže SAS může pracovat mnohem účinněji (a v reálném čase), částečně z toho důvodu, že SAS může sám, přímo vytvářet potřebné zprávy EMM, a částečně z toho důvodu, že

zprávy EMM mohou být předávány uživateli nebo účastníkovi přes vyhrazenou (zpravidla modemovou) linku.

Výhodně je prostředek pro vytváření zpráv spojen s uvedeným modemem přes komunikační obslužný kanál, který je výhodně začleněn v nebo sdružen s tímto prostředkem pro vytváření zpráv.

Přijímací prostředek může být dále upraven pro přijímání opravňovacích zpráv přes satelitní odpovídač.

Přijímacím prostředkem může být přijímač/dekodér zahrnující prostředek pro přijímání komprimovaných signálů MPEG typu, prostředek pro dekódování přijatých signálů pro vytvoření televizního signálu a prostředek pro přivedení televizního signálu do televize.

Výhodně je přijímací prostředek upraven pro komunikaci s uvedeným prostředkem pro vytváření zpráv přes uvedený modem a spojovací prostředek. Přijímací prostředek může zahrnovat prostředek pro čtení inteligentní karty, která je do něj zasunuta koncovým uživatelem, přičemž tato inteligentní karta má v sobě uložena data pro automatickou inicializaci vysílání zprávy z uvedeného přijímacího prostředku do uvedeného prostředku pro vytváření zpráv po vložení inteligentní karty koncovým uživatelem.

Navíc systém může dále zahrnovat hlasovou linku pro umožnění koncovému uživateli vysílacího a přijímacího systému komunikovat s prostředkem pro vytváření zpráv.

Ze shora uvedeného popisu by mělo být zcela zřejmé, že předkládaný vynález navrhuje dvě uspořádání, prostřednictvím kterých je snížena doba potřebná k tomu, aby koncový uživatel dosáhl přístupu k požadovanému produktu.

Výhodně jsou pro dosažení maximální úspory času použita obě tato uspořádání, ale kterékoliv z těchto uspořádání může být použito individuálně.

Podle dalšího aspektu předkládaného vynálezu je
5 vytvořen vysílací a přijímací systém, který zahrnuje:

na vysílacím konci:

vysílací systém zahrnující prostředek pro vysílání
zpětné žádosti; a

na přijímacím konci:

10 přijímač zahrnující prostředek pro zpětné volání
vysílacího systému v odezvě na zpětnou žádost.

Prostřednictvím zajištění, že vysílací systém může
žádat přijímač o zpětné zavolání, je poskytnuta možnost, aby
vysílací systém získal informaci z přijímače o stavu tohoto
15 přijímače.

Výhodně prostředek pro zpětné volání vysílacího
systému zahrnuje modem spojitelný s telefonním systémem.
Prostřednictvím použití modemového zpětného kanálu může být
20 zajištěn jednoduchý způsob uvedení předkládaného vynálezu do
praxe.

Výhodně rovněž je prostředek pro zpětné volání
vysílacího systému uspořádán pro přenos do vysílacího systému
informace týkající se přijímače. Tato informace by mohla
25 zahrnovat počet zbývajících jednotek, počet objednaných
relací a podobně.

Výhodně vysílací systém zahrnuje prostředek pro
uložení informace, takže tato informace může být zpracována
30 později, pokud je to žádoucí.

Výhodně je vysílací prostředek uspořádán pro vysílání zpětné žádosti, která zahrnuje příkaz, že zpětné volání bude provedeno v danou dobu, a prostředek pro zpětné volání vysílacího systému je uspořádán pro odezvu na tento příkaz. Prostřednictvím uspořádání zpětného volání na pozdější dobu, než je vlastní žádost, může být systému poskytnuta větší pružnost.

Vysílací prostředek může být uspořádán pro vysílání zpětné žádosti jako jedné nebo více opravňovacích zpráv pro vysílání.

Výhodně vysílací systém zahrnuje prostředek pro vytváření kontrolní zprávy (jako je náhodné číslo) a pro její předání do přijímače, přičemž přijímač zahrnuje prostředek pro kódování kontrolní zprávy a pro její předání vysílacímu systému, a vysílací systém dále zahrnuje prostředek pro dekódování kontrolní zprávy přijaté z přijímače a pro její porovnání s původní kontrolní zprávou. Tímto způsobem může být zkontrolováno, zda přijímač je pravý.

Jakékoliv ze shora uvedených znaků mohou být spolu kombinovány v jakékoliv vhodné kombinaci. Uvedené znaky mohou být rovněž realizovány, pokud je to vhodné, jako aspekty způsobu.

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

Přehled obrázků na výkresech

- 5
Obr.1 znázorňuje celkovou architekturu digitálního televizního systému podle výhodného provedení předkládaného vynálezu;
- Obr.2 znázorňuje architekturu systému podmíněného přístupu v digitálním televizním systému;
- 10
Obr.3 znázorňuje strukturu opravňovací řídicí zprávy (EMM) použité v systému podmíněného přístupu;
- Obr.4 znázorňuje schematický diagram hardwaru účastnického autorizačního systému (SAS) podle výhodného provedení předkládaného vynálezu;
- 15
Obr.5 znázorňuje schematický diagram architektury SAS;
- Obr.6 znázorňuje schematický diagram obslužného kanálu účastnického technického řízení, který tvoří část SAS;
- 20
Obr.7 znázorňuje vývojový diagram procedury pro automatické obnovování připojení účastníků, jak je realizováno prostřednictvím SAS;
- Obr.8 znázorňuje schematický diagram bitové mapy skupiny připojení účastníků, která je použita v automatické obnovovací proceduře;
- 25
Obr.9 znázorňuje strukturu EMM, která je použita v automatické obnovovací proceduře;
- 30
Obr.10 znázorňuje detailně strukturu EMM;

- Obr.11 znázorňuje schematický diagram příkazově centralizovaného obslužného kanálu, když je použit pro přijímání příkazů přímo přes komunikační obslužné kanály;
- 5
- Obr.12 schematicky ilustruje část obr. 2, která znázorňuje jedno provedení předkládaného vynálezu;
- Obr.13 znázorňuje schematický diagram příkazově centralizovaného obslužného kanálu, když je použit pro přijímání příkazů z účastnického autorizačního systému pro žádost o zpětný dotaz;
- 10
- Obr.14 znázorňuje schematický diagram komunikačních obslužných kanálů;
- 15
- Obr.15 znázorňuje způsob, kterým je měněna rychlost vysílacího cyklu zpráv EMM podle časování PPV události;
- Obr.16 znázorňuje schematický diagram vysílače zpráv, použitého pro vysílání zpráv EMM;
- 20
- Obr.17 znázorňuje schematický diagram ilustrující způsob uložení zpráv EMM ve vysílači zpráv;
- Obr.18 znázorňuje schematický diagram inteligentní karty;
- 25
- Obr.19 znázorňuje schematický diagram uspořádání zón v paměti inteligentní karty; a
- Obr.20 znázorňuje schematický diagram popisu PPV události.
- 30

Příklady provedení vynálezu

Celkový přehled digitálního televizního vysílání 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 odpovídáči 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.

System 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
5 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.

10 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.

15 Níže bude podrobněji popsán systém 3000 podmíněného
přístupu.

Ze schématu obr. 2 je patrné, že systém 3000
podmíněného přístupu zahrnuje účastnický autorizační systém
20 (SAS) 3002. SAS 3002 je spojen s jedním nebo s více
účastnickými řídicími 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
25 SMS 3004 mohl být sdílen mezi dvěma poskytovateli vysílání,
nebo by jeden poskytovatel vysílání mohl používat dva SMS
3004 a podobně.

30 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 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.

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

10 Přístupová kritéria, která indikují způsob komercializace programu, jsou rovněž přidávána do toku MPEG-2. Program může být komercializován 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 15 960 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 20 vysílána ("impulzní mód"). Ve výhodném provedení jsou všichni uživatelé účastníci (předplatitelé), ať již sledují nebo nesledují v předplaceném nebo PPV módu, ale samozřejmě, že 25 PPV diváci nemusí být nezbytné účastníci (předplatitelé).

Jak řídicí slovo tak i přístupová kritéria jsou použita pro sestavení opravňovací řídicí zprávy (ECM); což je zpráva vysílaná ve spojení s jedním kódovaným programem; 30 přičemž tato zpráva obsahuje řídicí slovo (které umožňuje



dekódování programu) a přístupová kritéria vysílaného programu. Přístupová kritéria a řídicí slovo jsou vysílány do druhé šifrovací jednotky 3014 přes spojení 3018. V této jednotce je zpráva ECM vytvářena, kódována a vysílána na
5 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
10 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
20 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
25 spojení 2012.

Přijímání programů

Satelitní odpovídač 2014 přijímá a zpracovává elektromagnetické signály vysílané vysílačem 2008 a vysílá
30 tyto signály k pozemnímu přijímači 2018, obvykle ve formě



parabolické antény vlastněné nebo pronajaté koncovým
uživatelé, přes sestupné spojení 2016. Signály přijímané
pozemním přijímačem 2018 jsou vysílány do integrovaného
přijímače/dekodéru 2020 vlastněného nebo pronajatého koncovým
5 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.

10 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.

15 Pokud program je kódován, přijímač/dekodér 2020
vybírám odpovídající zprávu ECM z toku MPEG-2 a předává tuto
zprávu ECM "dceřiné" inteligentní kartě 3020 koncového
uživatele. Ta je zasunuta do štěrby v pouzdru
přijímače/dekodéru 2020. Dceřiná karta 3020 řídí, zda koncový
uživatel má právo dekódovat zprávu ECM a právo přístupu k
20 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 vyjmuta řídicí slovo. Dekodér 2020
potom může dekódovat program s použitím tohoto řídicího
25 slova. Tok MPEG-2 je dekomprimován a převeden na video signál
pro následné vysílání do televizního zařízení 2022.

Účastnický řídicí systém (SMS)

30 Účastnický řídicí 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.

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

10 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).

15 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
20 dvoucestná.

Opravňovací řídicí zprávy (EMM)

25 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
30 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 shlednutí; tyto zprávy obsahují 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)

5

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.

10

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 zadávání 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.

15

20

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.

25

30

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 shlednutí 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.

5 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 komercializace (například objednávkový mód, impulzní mód). SAS 3002 podle těchto práv a podle informace, přijaté ze SMS 3004, vytváří zprávy EMM pro účastníka.

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

15 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, 20 příkazově centralizovaný obslužný kanál (OCS) 3207, obslužný kanál 3208 pro programový vysílač (SPB), generátor zpráv (MG) 33210, 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 25 3008.

30 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.

Každý z uvedených tří hlavních komponentů SAS (oblast předplatitelského řetězce, oblast PPV řetězce a EMM zaváděč)
5 bude nyní popsán poněkud podrobněji.

Oblast předplatitelského řetězce

Nejprve bude popsána oblast 3100 předplatitelského
10 řetězce, ve které je příkazové rozhraní 3102 určeno primárně pro přidělování zpráv ze SMS 3004 do STM obslužného kanálu 3104 a také do OCS 3206, a z OCS 3206 do SMS 3004. Příkazové rozhraní 3102 bere jako vstup ze SMS 3004 buď přímé příkazy nebo dávkové soubory obsahující příkazy. Toto rozhraní
15 provádí syntaktickou analýzu zpráv přicházejících z STM obslužného kanálu 3104 a je schopné vysílat správné zprávy, když ve zprávě dojde k chybě (parametr mimo rozsah, chybějící parametr a podobně). Toto rozhraní dále sleduje přicházející příkazy v textové formě ve sledovacím souboru 3110 a rovněž v
20 binární formě v přehrávacím (opakovacím) souboru 3112, aby bylo schopno přehrávat (opakovat) série příkazů. Sledování může být vyřazeno z provozu a velikost souborů může být omezená.

V následujícím popisu bude provedena detailní diskuse
25 o STM obslužném kanálu 3104 ve spojení s odkazy zejména na obr. 6. STM obslužný kanál 3104 je v podstatě hlavním prvkem oblasti 3100 předplatitelského řetězce a jeho účelem je spravování volných práv, vytváření nových účastníků a obnovování existujících účastníků. Jak je znázorněno na
30 obrázku, jsou příkazy předávány do generátoru 3106 zpráv,



ačkoliv v odlišném formátu než je formát, ve kterém jsou tyto příkazy předávány do STM obslužného kanálu 3104. Pro každý příkaz je STM obslužný kanál 3104 uspořádán tak, aby vyslal potvrzovací zprávu do CI 3102 pouze tehdy, když relevantní příkaz již byl úspěšně zpracován a vyslán do MG 3106.

STM obslužný kanál 3104 obsahuje účastnickou databázi 3120, ve které jsou uloženy všechny relevantní parametry týkající se účastníků (číslo inteligentní karty, komerční nabídky, stav, skupina a umístění v této skupině, a podobně). Tato databáze 3120 provádí sémantické kontroly příkazů vysílaných CI 3102 vzhledem k obsahu databáze 3120 a aktualizuje databázi 3120, když jsou příkazy platné.

STM obslužný kanál 3104 dále spravuje vyrovnávací paměť 3122, typu první dovnitř první ven (FIFO), mezi STM obslužným kanálem 3104 a MG 3106 a rovněž záložní FIFO disk 3124. Účelem těchto FIFO prvků je zprůměrovat tok příkazů z CI 3102, pokud MG 3106 není z jakéhokoliv důvodu schopen po určitou dobu odpovídat. Tyto FIFO prvky mohou rovněž zajistit, že v případě kolize STM obslužného kanálu 3104 nebo MG 3106 nebude žádný příkaz ztracen, protože STM obslužný kanál 3104 je uspořádán pro vyprázdnění (to jest vyslání do MG 3106) jeho FIFO prvku, když je restartován. FIFO prvky jsou realizovány jako soubory.

STM obslužný kanál 3104 ve svém paměťovém jádru obsahuje obslužný kanál 3126 automatického obnovování, který automaticky vytváří obnovení a, pokud je to požadováno operátory, volná práva. V této souvislosti je možné o vytváření obnovení uvažovat tak, že zahrnuje i vytváření práv poprvé, ačkoliv je zcela zřejmé, že vytváření nových práv je

inicializováno v SMS 3004. Jak bude patrné, mohou být tyto dvě věci ošetřeny zhruba stejnými příkazy a zprávami EMM.

To, že STM obslužný kanál 3104 je oddělen od SAS 3002 a obslužný kanál automatického obnovení uvnitř SAS 3002 spíše než (ve známých systémech) v SMS 3004, je obzvláště důležitým znakem, protože to může podstatně omezit počet příkazů, které musí být předány ze SMS 3004 do SAS 3002 (při vzetí do úvahy, že SMS a SAS mohou být na různých místech a provozovány různými operátory). Ve skutečnosti dva hlavní příkazy vyžadované ze SMS 3004 jsou pouze příkazy, že nové předplácení by mělo být započato a že existující předplácení by mělo být zastaveno (například v případě neplacení). Prostřednictvím minimalizace výměny příkazů mezi SMS 3004 a SAS 3002 je rovněž snížena možnost selhání přenosu příkazů ve spojení 3006 mezi těmito dvěma prvky; a rovněž konstrukce SMS 3004 nemusí brát obecně do úvahy znaky systému 3000 podmíněného přístupu.

Automatické obnovování je realizováno způsobem naznačeným ve vývojovém diagramu podle obr. 7. Aby se omezila šířka pásma a vzhledem k tomu, že velký procentní podíl všech obnovení je standardní, je obnovení realizováno ve skupinách účastníků; ve výhodných provedeních vynálezu je 256 jednotlivých účastníků na skupinu. Vývojový diagram začíná zahajovacím krokem 3130 a pokračuje do kroku 3132, ve kterém je prováděna měsíční aktivace obnovovací funkce (ačkoliv by samozřejmě mělo být zcela zřejmé, že jiné frekvence obnovení jsou také možné). S měsíční frekvencí obnovování jsou práva poskytována koncovému uživateli pro právě probíhající měsíc a celý následující měsíc, na jehož konci přestanou platit, pokud nebudou obnovena.

V kroku 3134 je vstupováno do účastnické databáze 3120 vzhledem ke každé skupině a každému jednotlivci uvnitř této skupiny pro určení, zda práva pro určitého jednotlivce mají být obnovena.

5 V kroku 3136 je, jak je znázorněno na obr. 8, podle obsahů účastnické databáze 3120 sestavena bitová mapa předplacení skupiny. Tato bitová mapa zahrnuje identifikátor 3138 skupiny (v tomto případě skupina 1 - "G1") a 256 zón 3140 jednotlivých účastníků. Jednotlivé bity v této bitové mapě jsou nastaveny na 1 nebo nulu podle toho, zda má či nemá mít určitý účastník obnovena jeho práva. Typická sestava binárních dat je znázorněna na obrázku.

10 V kroku 3142 jsou do generátoru 3106 zpráv předávány vhodné příkazy, včetně bitové mapy předplacení skupiny. V kroku 3143 generátor 3106 zpráv nastavuje datum zastarání pro indikaci inteligentní kartě data, za kterým určitá účastnická EMM již není platná; obvykle je toto datum nastaveno jako konec následujícího měsíce.

15 V kroku 3144 generátor 3106 zpráv vytváří z příkazů vhodné zprávy EMM pro skupinu účastníků a žádá šifrovací jednotku 3008, aby zašifrovala tyto zprávy EMM, přičemž šifrované zprávy EMM jsou potom předávány do zaváděče 3300 EMM, který v kroku 3146 zavádí tyto zprávy EMM do datového toku MPEG-2.

20 Krok 3148 naznačuje, že shora popisovaná procedura je opakována pro každou skupinu. Proces je nakonec ukončen v ukončovacím kroku 3150.

25 Vývojový diagram, popisovaný výše ve spojení s odkazy na obr. 7, se ve skutečnosti týká specificky obnovování



předplacení. STM kanál 3104 rovněž spravuje podobným způsobem volná publiková práva a nové účastníky.

5 V případě volných publikových práv, dostupných pro specifické programy nebo skupiny takových programů, jsou tato práva vytvořena dostupnými prostřednictvím STM obslužného kanálu 3104, který tedy vydává příkaz do generátoru 3106 zpráv pro vytvoření vhodných publikových zpráv EMM (pro celé publikum) s datem zastarání po daném počtu dnů (nebo týdnů). MG 3106 vypočítá přesné datum zastarání na základě příkazu z STM obslužného kanálu 3104.

10 Pokud se týká nových účastníků, jsou tito účastníci zpracováni ve dvou fázích. Nejprve při nákupu inteligentní karty do přijímače/dekodéru 2020 (pokud je to žádáno operátorem) získává účastník volná práva pro danou časovou periodu (obvykle několik dnů). To je dosaženo prostřednictvím vytvoření bitové mapy pro účastníka, která obsahuje relevantní datum zastarání. Účastník potom předá přihlášku operátorovi spravujícímu tohoto účastníka (v SMS). Jakmile je tato přihláška zpracována, SMS dodá do SAS zahajovací příkaz pro tohoto určitého účastníka. Po přijetí tohoto zahajovacího příkazu v SAS přikáže STM obslužný kanál MG, aby přidělil jednoznačnou adresu tomuto novému účastníkovi (s určitým číslem skupiny a umístěním v této skupině) a aby vytvořil speciální, tak zvanou zprávu EMM předplacení "komerční nabídky" (oproti běžnější zprávě EMM předplacení "skupiny", která je používána pro obnovování) pro zajištění tomuto určitému účastníkovi práv až do konce následujícího měsíce. Od tohoto okamžiku může obnovování nového účastníka probíhat automaticky podle shora uváděného popisu. Prostřednictvím

15

20

25

30



tohoto dvoufázového procesu je možné udělovat novým účastníkům práva, dokud SMS nevydá zastavovací příkaz.

Je třeba uvést, že zpráva EMM předplacení komerční nabídky je použita pro nové účastníky a pro opětovnou aktivaci existujících účastníků. Zpráva EMM předplacení skupiny je použita pro účely obnovování a zastavování.

Jak je patrné z obr. 9, typická vlastní zpráva EMM (to jest při ignorování záhlaví a podpisu) předplacení, která je vytvořena prostřednictvím výše popisované procedury, zahrnuje následující hlavní části, zejména obvykle 256 bitů bitové mapy 3152 předplacení (nebo skupiny účastníků), 128 bitů řídicích šifrovacích klíčů 3154 pro šifrování zprávy EMM, 64 bitů každého použitého šifrovacího klíče 3156 pro umožnění inteligentní kartě 3020 dešifrovat řídicí slovo pro zajištění přístupu k vysílaným programům, a 16 bitů data 3158 zastarání pro indikaci data, za kterým inteligentní karta bude ignorovat tuto EMM. Ve skutečnosti jsou ve výhodném provedení vynálezu zajištěny tři použité klíče, jeden je nastaven pro současný měsíc, jeden je nastaven pro následující měsíc a jeden je nastaven pro účely obnovení v případě selhání systému.

Přesněji vlastní zpráva EMM předplacení skupiny má všechny ze shora uvedených komponentů, až na řídicí šifrovací klíče 3154. Vlastní zpráva předplacení komerční nabídky (která je pro jednotlivého účastníka) zahrnuje, namísto úplné bitové mapy 3152 skupiny účastníků, identifikátor skupiny následovaný umístěním v této skupině, a potom řídicí šifrovací klíče 3154 a tři použité klíče 3156 následované relevantním datem 3158 zastarání.

Generátor 3106 zpráv slouží pro přeměnu příkazů vydávaných STM obslužným kanálem 3104 na zprávy EMM pro předání do vysílače 3302 zpráv. Jak je patrné na obr. 5, MG 3106 nejprve vytvoří vlastní zprávy EMM a předá je do
5 šifrovací jednotky 3008 pro šifrování vzhledem k řídicím a použitým klíčům. CU 3008 dokončí podpis 3064 na EMM (viz obr. 3) a předá EMM zpět do MG 3106, kde je přidáno záhlaví 3060. Zprávy EMM, které jsou předány do vysílače 3302 zpráv, jsou tudíž úplné zprávy EMM. Generátor 3106 zpráv rovněž určuje
10 dobu započetí a zastavení vysílání a rychlost vysílání zpráv EMM, a předává tyto informace jako vhodné příkazy společně se zprávami EMM do vysílače 3302 zpráv. MG 3106 vytváří danou zprávu EMM pouze jednou; tím prvkem, který provádí její cyklické vysílání, je ME 3302.

15 Jak je opět patrné z obr. 5, zahrnuje generátor 3106 zpráv svoji vlastní databázi 3160 EMM, která po dobu aktuálnosti relevantní EMM tuto zprávu EMM ukládá. Tato zpráva EMM je vymazána, jakmile již uplynula doba jejího vysílání. Tato databáze 3160 je použita pro zajištění
20 konzistence mezi MG 3106 a ME 3302, takže například při vyloučení (zastavení) koncového uživatele ME 3302 nebude pokračovat s vysíláním obnovení. V této souvislosti MG 3106 vypočítává relevantní operace a vysílá je do ME 3302.

25 Při vytváření zprávy EMM přiděluje MG 3106 této zprávě EMM jednoznačný identifikátor. Když MG 3106 předává zprávu EMM do ME 3302 rovněž předává tento jednoznačný identifikátor (ID) pro EMM. To umožňuje identifikaci určité zprávy EMM jak v MG 3106 tak i v ME 3302.

30 Rovněž pokud se týká oblasti 3100 předplatitelského řetězce zahrnuje generátor 3106 zpráv dvě FIFO paměti 3162 a



3164, jednu pro každý z relevantních vysílačů 3302 a 3304
 zpráv v zaváděči 330 EMM, pro ukládání šifrovaných EMM.
 Protože oblast 3100 předplatitelského řetězce a zaváděč 330
 EMM mohou být vzdáleny o značnou vzdálenost, umožňuje použití
 5 těchto FIFO pamětí úplnou kontinuitu ve vysílání EMM, dokonce
 i když spoje 3166 a 3168 mezi těmito dvěma prvky selžou.
 Podobné FIFO paměti jsou použity v oblasti 3200 řetězce
 plateb za shlédnutí.

Jeden zvláštní znak generátoru 3106 zpráv zejména a
 10 systému 3000 podmíněného přístupu obecně se týká způsobu,
 kterým omezuje délku vlastní zprávy EMM 3062 prostřednictvím
 směřování parametru délku a identifikátoru pro úsporu
 prostoru. To bude v následujícím popisu popsáno ve spojení s
 odkazy na obr. 10, který ilustruje příkladnou EMM (ve
 15 skutečnosti PPV EMM, která je nejjednodušší EMM). Ke snížení
 délky dochází v Pid (identifikátor paketu nebo "parametru")
3170. Ten zahrnuje dvě části, vlastní ID (identifikátor) 3172
 a parametr 3174 délky pro paket (potřebný k tomu, aby mohl
 být identifikován začátek následujícího paketu). Celý Pid
 20 3170 je vyjádřen v právě jednom bytu informace, kde 4 bity
 jsou rezervovány pro ID a čtyři bity jsou rezervovány pro
 parametr délky. Protože 4 bity nejsou dostatečné pro
 definování délky skutečně binárním způsobem, je použito
 odlišného vztahu mezi bity a vlastní délkou, tento vztah je
 25 reprezentován ve vyhledávací tabulce uložené v paměťové
 oblasti 3178 v generátoru 3106 zpráv (viz obr. 5). Vztah je
 obvykle následující:-

0000 = 0

0001 = 1



	0010	=	2	
	0011	=	3	
	0100	=	4	
5	0101	=	5	-
	0110	=	6	=
	0111	=	7	
	1000	=	8	
10	1001	=	9	
	1010	=	10	
	1011	=	11	
	1100	=	12	
15	1101	=	16	
	1110	=	24	
	1111	=	32	

20 Mělo by být patrné, že parametr délky není přímo úměrný skutečné délce paketu; vztah je částečně více kvadratický, spíše než aby byl lineární. To umožňuje větší rozsah délky paketu.

25 Oblast řetězce plateb za shlédnutí

Pokud se týká oblasti 3200 řetězce plateb za shlédnutí, jak je podrobněji patrné na obr. 5, má autorizační obslužný kanál 3202 za svého klienta příkazově centralizovaný obslužný kanál 3207, který si žádá informace o každém

účastníkovi, který se připojuje ke komunikačním obslužným kanálům 3022 za účelem nákupu PPV produktu.

Pokud je účastník známý z AS 3202, proběhne sada transakcí. Pokud je účastník autorizován pro objednávku, vytváří AS 3202 fakturu (účet) a posílá ji do OCS 3207. V opačném případě AS 3202 signalizuje do OCS 3207, že objednávka není autorizována.

Pouze na konci této sady transakcí dochází k tomu, že AS 3202 aktualizuje relační databázi 3204 koncových uživatelů přes databázové obslužné kanály (DBAS) 3206, pokud alespoň jedna transakce byla autorizována; což optimalizuje počet přístupů do databáze.

Kritéria, podle nichž AS 3202 autorizuje nákupy, jsou uloženy v databázi, do níž je vstupováno přes DBAS procesy. V jednom provedení vynálezu je tato databáze stejná jako databáze, do níž vstupuje STM.

V závislosti na profilu spotřebitele může být autorizace odepřena (PPV_zakázáno, Casino_zakázáno ...). Tyto typy kritérií jsou aktualizovány prostřednictvím STM 3104 v zastoupení SMS 3004.

Jsou kontrolovány také další parametry, jako jsou limity povolené pro nákup (buď kreditní karta, automatická platba, nebo počet autorizovaných, provedených nákupů za den).

V případě platby kreditní kartou je kontrolováno číslo této karty vzhledem k lokálnímu černému seznamu (seznam neplatičů nebo nekrytých karet) uloženému v lokální databázi 3205 černého seznamu.



Když jsou všechna ověření úspěšná, pak AS:-

5 1. Vytváří fakturu (účet) a vysílá ji do OCS, který doplní tuto fakturu a uloží ji do souboru, tento soubor je později vyslán do SMS pro zpracování (aktuální fakturace zákazníka; a

2. Aktualizuje databázi, převážně pro nastavení nových nákupních limitů.

10 Tento mechanismus zkontroluj-a-vytvoř-fakturu-pokud-OK je aplikován pro každý příkaz, který účastník může žádat v průběhu jednoho spojení (je možné objednat, například, 5 filmů (pořadů) při jednom spojení).

15 Je třeba uvést, že AS má omezené množství informací týkajících se účastníka ve srovnání s tím, co má k dispozici SMS. Například AS nemá k dispozici jméno nebo adresu účastníka. Na druhou stranu AS má k dispozici číslo inteligentní karty účastníka, spotřebitelskou kategorii zákazníka (takže odlišné objednávky mohou být provedeny pro 20 odlišné účastníky) a různé příznaky, které udávají, například, zda účastník může nakupovat na kredit, nebo je vyloučen nebo byla ukradena jeho inteligentní karta. Použití omezeného množství informací může napomoci omezit dobu potřebnou pro autorizaci určitého požadavku účastníka.

25 Hlavním účelem DBAS 3206 je zvýšit výkon databáze z hlediska AS 3202 prostřednictvím paralelních přístupů (takže vlastně nemá velký smysl definovat uspořádání s pouze jedním DBAS 3206). Parametr AS 3202 určuje kolik DBAS 3206 by měl spojit. Daný DBAS 3026 může být spojen pouze s jedním AS 30 3202.



OCS 3207 převážně pracuje s PPV příkazy a pracuje v několika módech.

5 Za první OCS 3207 pracuje pro zpracování příkazů vydávaných SMS 3004, jako je obnova produktů (například, pokud je faktura již uložena prostřednictvím SMS 3004, není faktura vytvořena prostřednictvím OCS 3207), aktualizace "peněženky" v inteligentní kartě 3020, a zrušení/aktualizace spojení.

10 Různými kroky v této proceduře jsou:-

1. Identifikace relevantního účastníka (s použitím AS 3202);

2. V případě platnosti vytvoření odpovídajících příkazů do generátoru zpráv, aby vyslal vhodnou zprávu EMM.

15 Příkazy mohou být:

příkazy o produktech,
aktualizace peněženky,
vymazání spojení.

20 Je třeba si všimnout, že tyto operace nezahrnují vytvoření fakturačních informací, protože fakturace je již známá ze SMS. Tato operace jsou přizpůsobeny pro nákup "volných produktů".

25 Za druhé OCS 3207 pracuje s příkazy přijatými od účastníků přes komunikační obslužné kanály 3022. Tyto příkazy mohou být přijímány buď přes modem připojený k přijímači/dekodéru 2020, nebo prostřednictvím hlasové aktivace přes telefon 4001, nebo prostřednictvím aktivace klávesami přes MINITEL, PRESTEL nebo podobný systém v případě jeho dostupnosti.

30



Za třetí OCS 3207 pracuje se zpětnými žádostmi vydávanými ze SMS. Tyto poslední dva módy činnosti budou nyní níže podrobněji diskutovány.

5 V druhém typu módu popisovaného výše bylo uvedeno, že OCS 3207 pracuje s příkazy přijatými přímo od koncového uživatele (účastníka) přes komunikační obslužné kanály 3022. Tyto příkazy zahrnují objednávky produktů (například pro určitou PPV událost), modifikace předplatného, vyžadované účastníkem a znovunastavení rodičovského kódu (rodičovský kód je kód, prostřednictvím kterého rodiče mohou omezit právo 10 přístupu k určitým programům nebo třídám programů).

Způsob, kterým jsou tyto příkazy zpracovávány, bude nyní podrobněji popsán ve spojení s odkazy na obr. 11.

15 Objednávky produktů, zadávané účastníkem, zahrnují následující kroky:-

1. Přes AS 3202 identifikace volajícího, který provádí hovor přes CS 3022 a objednává určitý produkt;
2. Ověření platnosti žádosti volajícího, opět s použitím 20 AS 3202 (tam, kde je objednávka podávána s použitím přijímače/dekodéru 2020, je to dosaženo ověřením detailů inteligentní karty 3020);
3. Zjištění ceny nákupu;
4. Ověření, že cena nepřekročila kreditní limit volajícího a podobně;
- 25 5. Přijetí částečné faktury od AS 3202;
6. Vyplnění doplňkových polí ve faktuře pro vytvoření úplné faktury;
7. Přidání úplné faktury do paměťového souboru 3212 30 fakturačních informací pro pozdější zpracování; a



8. Vyslání odpovídajících příkazů do generátoru 3210 PPV zpráv pro vytvoření relevantních zpráv EMM.

5 Zprávy EMM jsou vyslány buď na modemové lince 4002,
pokud spotřebitel podal objednávku na produkt s použitím
přijímače/dekodéru 2020 (více detailů bude popsáno později),
anebo jsou vysílány. Jednou výjimkou je případ, ve kterém
10 dochází k nějakému selhání modemového spojení (v případě, kdy
spotřebitel podává objednávku s použitím přijímače/dekodéru
2020); za těchto okolností jsou EMM vysílány vzduchem.

Modifikace předplacení, vyžadovaná účastníkem,
zahrnuje:

1. Identifikaci volajícího (s použitím AS 3202);
- 15 2. Vyslání informace do příkazového rozhraní 3102; přičemž
toto CI 3102 dále předá tuto informaci do SMS 3004; a
3. Přes CI 3102 potom OCS 3207 přijímá odpověď ze SMS 3004
(týkající se modifikace ceny, pokud je modifikace
možná).

20 Pokud modifikace byla požadována s použitím přijímače
dekodéru 2020, OCS 3207 vytváří potvrzení do SMS 3004. Jinak,
například v případě telefonu nebo systému MINITEL, je
účastník požádán o potvrzení a tato odpověď je vyslána do SMS
25 3004 přes OCS 3207 a CI 3102.

Znovunastavení rodičovského kódu zahrnuje:

1. Identifikaci volajícího (s použitím AS 3202); a
2. Vyslání příkazu do MG 3210 pro vytvoření vhodné zprávy
EMM nesoucí vhodné heslo pro znovunastavení.

V případě znovunastavení rodičovského kódu není z důvodu bezpečnosti povoleno, aby příkaz pro znovunastavení kódu pocházel z přijímače/dekodéru 2020. Takovýto příkaz může pocházet pouze ze SMS 3004, telefonu a systému MINITEL nebo podobně. Tudíž v tomto zvláštním případě jsou zprávy EMM vysílány pouze vzduchem, nikdy ne na telefonní (modemové) lince.

Ze shora uvedených příkladů různých módů činnosti OCS 3207 by mělo být zcela zřejmé, že uživatel může mít přímý přístup do SAS 3002, a zejména do OCS 3207 a AS 3202, tím, že komunikační obslužné kanály 3022 jsou přímo spojené se SAS 3002 a přesněji s OCS 3207. Tento důležitý znak je spojen se snížením doby, která je nutná k tomu, aby uživatel předal svůj příkaz do SAS 3002.

Tento znak je dále ilustrován ve spojení s odkazy na obr. 12, ze kterého může být patrné, že nastavovací řídicí skříň (STB) koncového uživatele a zejména její přijímač/dekodér 2020 má možnost komunikovat přímo s komunikačními obslužnými kanály 3022 sdruženými se SAS 3002. Namísto toho, aby spojení od koncového uživatele ke komunikačním obslužným kanálům 3022 systému SAS 3002 bylo realizováno přes SMS 3004, je toto spojení realizováno přímo se SAS 3002.

Ve skutečnosti, jak bylo uvedeno výše, jsou vytvořena dvě přímá spojení.

První přímé spojení je realizováno prostřednictvím hlasového spoje přes telefon 4001 a vhodnou telefonní linku (a/nebo systém MINITEL nebo podobné spojení, kde je dostupné), přičemž koncoví uživatelé stále ještě musí zadat

série hlasových příkazů nebo číselných kódů, ale čas je přesto uspořen ve srovnání s komunikací realizovanou přes SMS 3004.

5 Druhé přímé spojení je realizováno z
přijímače/dekodéru 2020 a zadávání dat je dosaženo
automaticky tím, že koncový uživatel vloží svoji vlastní
10 dceřinou inteligentní kartu 3020, což tohoto koncového
uživatele uvolní od nutnosti zadávat relevantní data, což
dále zkracuje potřebnou dobu a snižuje pravděpodobnost chyb
při provádění tohoto zadávání.

15 Dalším důležitým znakem, který vyplývá ze shora
uváděného popisu, je spojen s omezením doby potřebné k tomu,
aby výsledná zpráva EMM byla vyslána ke koncovému uživateli,
aby iniciovala sledování zvoleného produktu tímto koncovým
uživatelem.

20 V širším smyslu a ve spojení s odkazy na obr. 12, je
tento znak opět dosažen prostřednictvím zajištění toho, že
přijímač/dekodér 2020 koncového uživatele má schopnost
komunikovat přímo s komunikačními obslužnými kanály 3022
sdruženými se SAS 3002.

25 Jak je popsáno v předcházejícím popisu, je
integrováný přijímač/dekodér 2020 spojen přímo s
komunikačními obslužnými kanály 3022 prostřednictvím
modemového zpětného kanálu 4002, takže příkazy z dekodéru
2020 jsou zpracovávány SAS 3002, zprávy (včetně zpráv EMM)
jsou vytvářeny a potom vysílány zpět přímo do dekodéru 2020
přes tento modemový zpětný kanál 4002. Při komunikaci mezi CS
3022 a přijímačem dekodérem 2020 je použit protokol (jak je
30 popsáno v popisu níže), takže CS 3022 přijímá potvrzení o



přijetí relevantní zprávy EMM, čímž proceduře přidává na spolehlivosti.

5 Tak například v případě objednávkového módu SAS 3002 přijímá zprávy od koncového uživatele přes inteligentní kartu a dekodér 2020 přes svůj modem a přes telefonní linku 4002, žádající přístup ke specifické události/produktu, a vrací vhodnou zprávu EMM přes telefonní linku 4002 a modem do dekodéru 2020, přičemž modem a dekodér jsou výhodně umístěny společně v nastavovací řídicí skříni (STB). To je tedy 10 dosaženo bez nutnosti vysílat zprávu EMM v MPEG-2 datovém toku přes komprimátor 2002 a přes multiplexor a kodér 2004, vzestupné spojení 2012, satelitní odpovídač 2014 a datové sestupné spojení 2016 pro umožnění koncovému uživateli, aby sledoval vybranou událost/produkt. Takto lze uspořít 15 podstatně na potřebné době a na šířce pásma. Je také zajištěna faktická spolehlivost tím, že, jakmile účastník již zaplatil za svůj nákup, zpráva EMM dorazí do přijímače/dekodéru 2020.

20 Ve třetím typu módu činnosti OCS 3207 podle shora uváděného popisu pracuje OCS 3207 se zpětnými žádostmi vydávanými systémem SAS 3002. To je ilustrováno ve spojení s odkazy na obr. 13. Obvyklé zpětné žádosti mají za účel zajištění, že přijímač/dekodér 2020 volá zpět SAS 3002 přes 25 modemový zpětný kanál 4002 s informací, kterou SAS 3002 vyžaduje od přijímače/dekodéru 2020.

30 Jak je instruován příkazovým rozhraním 3102 vytváří generátor 3106 zpráv v předplatitelském řetězci zpětnou zprávu EMM a vysílá ji do přijímače/dekodéru 2020. Tato zpráva EMM je z bezpečnostních důvodů šifrována prostřednictvím šifrovací jednotky 3008. Zpráva EMM může

obsahovat čas/datum, ve kterém by se měl přijímač/dekodér 2020 aktivovat a provést zpětný hovor sám od sebe, aniž by byl explicitně vyzván; zpráva EMM může rovněž obvykle obsahovat telefonní čísla, která terminál musí vytočit, počet
5 dalších pokusů po neúspěšných voláních a zpoždění mezi dvěma voláními.

Při přijetí zprávy EMM, nebo ve specifikovaném čase-datu, se přijímač/dekodér 2020 spojuje s komunikačními
10 obslužnými kanály 3022. OCS 3207 nejprve identifikuje volajícího s využitím AS 3202 a ověřuje určité detaily, jako je operátor inteligentní karty a detaily o účastníkovi. OCS 3207 potom žádá inteligentní kartu 3020, aby vyslala různé šifrované informace (jako jsou relevantní počty relací, kdy
15 relace byla sledována, kolikrát je účastníkovi umožněno opět sledovat relaci, způsob, kterým relace byla sledována, počet zbývajících využitelných jednotek, počet objednaných relací a podobně). Tato informace je dešifrována prostřednictvím generátoru 3210 zpráv PPV řetězce, opět s využitím šifrovací
20 jednotky 3008. OCS 3207 přidává tuto informaci do paměťového souboru 3214 zpětných informací pro pozdější zpracování a předání do SMS 3004. Tato informace je z bezpečnostních důvodů šifrována. Celá procedura je opakována tak dlouho, až inteligentní karta již neobsahuje nic určeného k přečtení.

Jedním obzvláště výhodných znakem tohoto uspořádání
25 zpětného volání je to, že před přečtením inteligentní karty (to jest okamžitě po identifikaci volajícího s využitím AS 3202, jak bylo popsáno výše) je provedena systémem SAS 3002 kontrola, že přijímač/dekodér 2020 je skutečný a nefalšovaný, spíše než aby byl pirátskou verzí nebo počítačovou simulací.
30 Taková kontrola je prováděna následujícím způsobem. SAS 3002



vytváří náhodné číslo, které je přijato přijímačem/dekodérem 2020, šifrováno a potom vráceno do SAS 3002. SAS 3002 dešifruje toto číslo. Pokud je dešifrování úspěšné a původní náhodné číslo je získáno, lze z toho vyvodit, že

5 přijímač/dekodér 2020 je nefalšovaný, a procedura pokračuje. V opačném případě je procedura přerušena.

Další funkce, které mohou proběhnou během zpětného volání, jsou vymazání zastaralých relací na inteligentní kartě nebo naplnění peněženky (tato posledně uvedená funkce

10 je rovněž popsána v popisu níže v části pojmenované "Inteligentní karta").

Rovněž ve spojení s oblastí 3200 řetězce plateb za shlednutí je nyní níže proveden popis komunikačních

15 obslužných kanálů 3022. Na hardwarové úrovni zahrnují tyto kanály ve výhodném provedení paralelní procesor DEC Four. Na úrovni softwarové architektury, jak je patrné z obr. 14, jsou komunikační obslužné kanály v mnoha ohledech zcela běžné. Jedna určitá odlišnost od běžných konstrukcí vyplývá ze

20 skutečnosti, že obslužné kanály musí obsluhovat jak přijímače/dekodéry 2020 tak i hlasovou komunikaci s běžnými telefony 4001 a rovněž případně se systémem MINITEL nebo s podobnými systémy.

V následujícím popisu bude uvedeno, že dva příkazově

25 centralizované obslužné kanály 3207 jsou znázorněné na obr. 14 (jako "OCS1" a OCS2"). Přirozeně může být použit jakýkoliv požadovaný počet.

Komunikační obslužné kanály zahrnují dva hlavní

30 obslužné kanály CS1 a CS2 a také určitý počet předních obslužných kanálů, například přední obslužné kanály Přední 1



a Přední 2; přičemž přestože jsou na obrázku znázorněny dva přední obslužné kanály, může jich být na jeden hlavní obslužný kanál vytvořeno obvykle 10 nebo 12. Rovněž, přestože na obrázku byly znázorněny dva hlavní obslužné kanály CS1 a CS2 a dva přední obslužné kanály Přední 1 a Přední 2, mohl by být použit jakýkoliv počet těchto kanálů. Obvykle je žádoucí určitá nadbytečnost.

Hlavní obslužné kanály CS1 a CS2 jsou spojené s příkazově centrovanými obslužnými kanály OCS1 a OCS2 přes vysokoúrovňové TCP/IP spojení 3230, zatímco hlavní obslužné kanály CS1 a CS2 jsou spojené s předními obslužnými kanály Přední 1 a Přední 2 přes další TCP/IP spojení 3232.

Jak je ilustrováno, zahrnují hlavní obslužné kanály CS1 a CS2 obslužné kanály pro "SENDER" (vysílání), "RECVR" (příjem), "VTX" (MINITEL, PRESTEL nebo podobně), "VOX" (hlasová komunikace), a "TRM" (komunikace s přijímačem/dekodérem). Tyto obslužné kanály jsou spojeny se sběrnicí "BUS" pro komunikaci signálů k předním obslužným kanálům.

Hlavní obslužné kanály CS1 a CS2 komunikují přímo s přijímači/dekodéry 2020 přes jejich modemové zpětné kanály 4002 s použitím společného protokolu veřejné sítě X25. Relativně nízkourovňový protokol mezi komunikačními obslužnými kanály 3022 a přijímači/dekodéry 2020 je v jednom výhodném provedení založen na mezinárodním protokolu CCITT standardu V42, který poskytuje spolehlivost tím, že má funkce chybové detekce a opětovného vysílání dat, a že využívá program pro provádění kontrolních součtů pro kontrolu integrity opětovného vysílání. Je rovněž zajištěn únikový mechanismus, jehož účelem je zabránění vysílání nepovolených znaků.

Na druhou stranu je hlasová telefonní komunikace prováděna přes přední komunikační obslužné kanály, z nichž každý je schopen realizovat řekněme 30 současně probíhajících hlasových přenosů ze spojení 3234 do lokální telefonní sítě přes vysokorychlostní "T2" (E1) standardní telefonní ISDN linky.

Třemi určitými funkcemi softwarové části komunikačních obslužných kanálů (které by mohly samozřejmě alternativně být realizovány zcela v hardwaru) jsou: za prvé měnit informace relativně nízkourovňového protokolu, přijaté z přijímače/dekodéru, na informační výstup relativně vysokourovňového protokolu do OCS, za druhé utlumit (omezit) nebo řídit počet současně prováděných spojení, a za třetí vytvořit několik souběžných kanálů bez jakéhokoliv směšování. V tomto posledním ohledu hrají komunikační obslužné kanály úlohu určité formy multiplexoru, přičemž interakce v určitém kanálu jsou definovány daným identifikátorem relace, který je ve skutečnosti použit v celém komunikačním řetězci.

Nakonec, pokud se týká oblasti 3200 řetězce plateb za shlednutí, a ve spojení opět s odkazy na obr. 5, je obslužný kanál 3208 pro programový vysílač (SPB) spojen s jedním nebo více programovými vysílači 3250 (které by obvykle mohly být umístěny vzdáleně od SAS 3002) pro přijetí programových informací. SPB 3208 filtrují informaci, odpovídající PPV událostem (relacím), pro další použití.

Obzvláště důležitým znakem je to, že filtrovaná informace o programových událostech je předána prostřednictvím SPB 3208 do MG 3210, který dále vysílá pseudoinstrukci (řídící příkaz) do ME 3306 nebo 3308 pro změnu rychlosti cyklického vysílání zpráv EMM za daných

okolností; to je provedeno tak, že ME nalézá všechny zprávy EMM s relevantním identifikátorem relace a mění rychlost cyklu vysílání, přidělenou těmto zprávám EMM. Tento znak by mohl být chápán jako dynamické přidělování šířky pásma pro specifické zprávy EMM. Cyklické vysílání zpráv EMM je diskutováno podrobněji v popisu níže v úseku zabývajícím se zaváděčem EMM.

Okolnosti, ve kterých je měněna rychlost cyklu vysílání, budou nyní popsány ve spojení s odkazy na obr. 15, který demonstruje, jak je rychlost 3252 cyklu zvýšena krátkou chvílí (řekněme 10 minut) před určitou PPV programovou událostí až do konce této události z pomalé rychlosti cyklu, řekněme jednou každých 30 minut, na rychlou rychlost cyklu, řekněme jednou každých 30 sekund nebo každou 1 minutu, aby splnila předpokládána zvýšené nároky uživatelů na PPV události v těchto okamžicích. Tímto způsobem může být šířka pásma přidělována dynamicky podle předpokládaných nároků uživatelů. To může napomáhat při omezení celkových nároků na šířku pásma.

Rychlost cyklu dalších zpráv EMM může být rovněž měněna. Například rychlost cyklu zpráv EMM týkajících se předplacení může být měněna multiplexorem a kódérem 2004 vysílajícím vhodnou pseudoinstrukci týkající se bitové rychlosti.

Zaváděč EMM

Pokud se týká zaváděče 3300 EMM budou nyní ve spojení s odkazy na obr. 16 popsány detaily vysílačů 3302 až 3308 zpráv, které tvoří část zaváděče 3300 EMM a působí jako

výstupní prostředek generátoru zpráv. Jejich funkcí je odebírat zprávy EMM a předávat je cyklicky (na způsob karuselu) přes odpovídající spoje 3314 a 3316 do softwarových multiplexorů 3310 a 3312 a tudíž do hardwarových multiplexorů a kodérů 2004. V odezvě softwarové multiplexory a kodéry 2004 vytvářejí globální pseudoinstrukci týkající se bitové rychlosti pro řízení celkové rychlosti cyklu zpráv EMM; aby to mohly provádět, berou ME 3302 až 3308 do úvahy různé parametry, jako je doba cyklu, velikost zprávy EMM a tak dále. Na obrázku EMM_X a EMM_Y jsou skupiny zpráv EMM pro operátory X a Y, zatímco EMM_Z jsou další zprávy EMM buď pro operátora X nebo pro operátora Y.

Další popis pokračuje prostřednictvím příkladného provedení jednoho z vysílačů zpráv; je třeba uvést, že zbývající ME pracují podobným způsobem. ME pracuje pod řízením pseudoinstrukcemi z MG, které řídí zejména začátek vysílání a okamžik ukončení a rychlost vysílání a rovněž číslo relace, pokud zpráva EMM je zprávou PPV EMM. Pokud se týká rychlosti vysílání, může ve výhodném provedení relevantní pseudoinstrukce nabývat jedné z pěti hodnot od velmi rychlé do velmi pomalé. Číselné hodnoty nejsou specifikovány v pseudoinstrukci, ale ME spíše přiřazuje pseudoinstrukci aktuální číselné hodnotě, která je dodávána prostřednictvím příslušné části SAS. Ve výhodném provedení má 5 rychlostí vysílání následující hodnoty:-

1. velmi rychle - každých 30 sekund
2. rychle - každou minutu
3. středně - každých 15 minut

- 4. pomalu - každých 30 minut
- 5. velmi pomalu - každých 30 minut

5 ME má první a druhou databázi 3320 a 3322. První
databáze 3320 je pro ty zprávy EMM, které ještě nedosáhly
svého data vysílání; tyto zprávy jsou uloženy v sériích
chronologických souborů v této databázi 3320. Druhá databáze
10 3322 je pro zprávy EMM určené k bezprostřednímu vysílání. V
případě selhání systému je ME uspořádán tak, aby měl možnost
opětovně přečíst relevantní uložený soubor a provést opravné
vysílání. Všechny soubory uložené v databázích 3320 a 3322
jsou aktualizovány podle žádostí z MG, když MG potřebuje
15 udržet konzistenci mezi přicházejícími pseudoinstrukcemi a
zprávami EMM již vyslanými do ME. Zprávy EMM aktuálně již
vysílané jsou rovněž uloženy v paměti s přímým přístupem 3324
(RAM).

20 Kombinace pamětí FIFO 3162 a 3164 v generátoru zpráv
a databází 3320 a 3322 ve vysílači zpráv znamená, že tyto dva
komponenty mohou pracovat v samostatném módu, pokud spoj 3166
mezi nimi je dočasně přerušen; ME potom může stále ještě
vysílat zprávy EMM.

25 Softwarové multiplexory (SMUX) 3310 a 3312 vytvářejí
rozhraní mezi vysílači ME a hardwarovými multiplexory 2004.
Ve výhodném provedení každý z nich přijímá zprávy EMM ze dvou
ME, ačkoliv obecně zde není žádné omezení týkající se počtu
vysílačů ME, které mohou být spojené s jedním SMUX. SMUX
soustřeďují zprávy EMM a potom je předávají podle typu EMM do
vhodného hardwarového multiplexoru. To je nezbytné, protože
30 hardwarové multiplexory přebírají různé typy zpráv EMM a



umístují je na různá místa v datovém toku MPEG-2. SMUX rovněž předávají globální pseudoinstrukce týkající se bitové rychlosti z hardwarových multiplexorů do vysílačů ME.

5 Jedním obzvláště důležitým znakem ME je to, že vysílá zprávy EMM v náhodném pořadí. Důvod pro takové uspořádání je následující. Vysílač zpráv nemá možnost snímat nebo řídit obsah toho, co vysílá do multiplexoru. Tudíž je možné, že může vysílat dvě zprávy EMM, které mají být přijaty a 10 dekódovány prostřednictvím přijímače/dekodéru 2020, ve zkráceném módu. Za takových okolností je dále možné, že, pokud zprávy EMM jsou nedostatečně odděleny, budou přijímač/dekodér a inteligentní karta neschopny snímat a dekódovat správně druhou z těchto zpráv EMM. Cyklické vysílání zpráv EMM v náhodném pořadí může tento problém 15 vyřešit.

Způsob, kterým je dosaženo náhodného rozdělování, bude nyní popsán ve spojení s odkazy na obr. 17; ve výhodném provedení je potřebná softwarová logika realizována ve 20 strojovém jazyku ADA. Obzvláště důležitou částí náhodného rozdělování je správné uložení zpráv EMM v databázích 3320 a 3322 (které jsou použity pro záložní účely) a v RAM 3324. Pro určitou rychlost cyklu vysílání a operátora jsou zprávy EMM uloženy ve dvojrozměrném poli prostřednictvím úrovně 3330 (jdoucí řekněme od A do Z) a počtu v úrovni 3332 (jdoucí od 0 25 do N). Třetí rozměr je přidán prostřednictvím rychlosti 3334 cyklu, takže je vytvořeno tolik dvojrozměrných polí kolik je použito rychlostí cyklu vysílání. Ve výhodném provedení je použito 256 úrovní a obvykle 200 nebo 300 zpráv EMM v každé 30 úrovni; a je použito 5 rychlostí cyklu vysílání. Poslední rozměr pole je přidán existencí různých operátorů; existuje

tedy tolik třírozměrných polí kolik je operátorů. Ukládání dat tímto způsobem může umožnit rychlé vyhledávání v případě, že MG žádá vymazání určité zprávy EMM.

Ukládání zpráv EMM probíhá podle algoritmu "s kontrolním součtem" (který je jinak známý jako "jednocestná funkce s kontrolním součtem"). Ten pracuje na modlovém přístupu, takže po sobě jdoucí úrovně jsou plněny předtím, než je použito vyšší číslo v úrovni, a počet zpráv EMM v každé úrovni zůstává zhruba konstantní. V tomto příkladu se uvažuje o použití 256 úrovní. Když MG vysílá do ME zprávu EMM s identifikátorem (ID) 1, je této EMM přiřazena úroveň "1" a zaujímá první číslo v úrovni 3332 pro úroveň 3330. Zprávě EMM s ID 2 je přiřazena úroveň "2" a tak dále až do úrovně 256. Zprávě EMM s ID 257 je přiřazena opět úroveň "1" (na základě funkce modulo) a zaujímá druhé číslo v první úrovni a tak dále.

Vyhledání specifické zprávy EMM, například když je prostřednictvím MG žádáno vymazání této specifické zprávy EMM, je prováděno prostřednictvím obrácení shora uvedeného postupu. Algoritmus s kontrolními součty je aplikován na ID zprávy EMM, aby se získala úroveň, načež je nalezeno číslo v této úrovni.

Vlastní náhodné rozdělování probíhá, když zprávy EMM jsou na cyklické bázi uvolňovány z RAM 3324 s použitím prostředku 3340 náhodného rozdělování, který je realizován v hardwaru a/nebo softwaru vysílače zpráv. Vyhledávání je přímé a opět je založeno na algoritmu s kontrolním součtem. Nejprve je zvoleno náhodné číslo (ve shora uvedeném příkladu nejprve v rozsahu 1 až 256) pro zjištění určité úrovně, která bude použita. Za druhé je zvoleno další náhodné číslo pro zjištění

určitého čísla v úrovni. Toto další náhodné číslo je zvoleno podle celkového počtu zpráv EMM v dané úrovni. Jakmile již byla daná zpráva EMM zvolena a odvysílána, je přesunuta do druhé identické paměťové oblasti v RAM 3324 opět s použitím funkce s kontrolním součtem. Tudiž první oblast zmenšuje svoji velikost, jak jsou zprávy EMM vysílány, do té míry, že při využití celé úrovně je tato oblast vymazána. Jakmile je první paměťová oblast zcela prázdná, je nahrazena druhou paměťovou oblastí před novým kolem vysílání zpráv EMM a obráceně.

Ve shora uvedeném postupu je po dvou nebo třech cyklech vysílání zpráv EMM šance, že jakékoliv dvě zprávy EMM určené pro stejného koncového uživatele budou vysílány zkráceně, statisticky zanedbatelná.

V pravidelných intervalech, zatímco jsou zprávy EMM ukládány, střediskový počítač 3050 vypočítává počet bytů v paměti a z této hodnoty vypočítává bitovou rychlost vysílání danou globální pseudoinstrukcí pro bitovou rychlost z multiplexoru a softwarového multiplexoru.

Ve shora uvedeném popisu byly uváděny záložní databáze 3320 a 3322. Tyto databáze jsou ve skutečnosti ve výhodném provedení sekvenčními paměťmi souborů, které obsahují záložní verzi toho, co je obsaženo v RAM 3324. V případě selhání vysílače zpráv a při následném restartu, nebo obecněji, když je ME restartován (opětovně spuštěn) z jakéhokoliv důvodu, je mezi RAM a databázemi vytvořeno spojení, přes které jsou zprávy EMM zavedeny do RAM. Tímto způsobem může být odstraněno riziko ztráty zpráv EMM v případě selhání systému.

Pro zprávy PPV EMM probíhá podobné ukládání, jako bylo popsáno výše ve spojení s předplatitelskými zprávami EMM, přičemž úroveň obvykle odpovídá danému operátorovi a číslo v úrovni odpovídá číslu relace.

5

Inteligentní karta

Dceřiná nebo "účastnická" inteligentní karta 3020 je schematicky znázorněna na obr. 18 a zahrnuje 8 bitový mikroprocesor 110, jako je mikroprocesor Motorola 6805, který má vstupní/výstupní sběrnici spojenou se standardním polem kontaktů 120, které jsou při použití spojeny s odpovídajícím polem kontaktů ve čtecím zařízení karty v přijímači/dekodéru 2020, přičemž toto čtecí zařízení karet je zcela běžné konstrukce. Mikroprocesor 110 je rovněž opatřen sběrnicovými spojeními s výhodně maskovanými ROM 130, RAM 140 a EEPROM 150. Inteligentní karta vyhovuje standardním protokolům ISO 7816-1, 7816-2 a 7816-3, které určují určité fyzické parametry inteligentní karty, polohy kontaktů na čipu a určité komunikace mezi vnějším systémem (a zejména přijímačem/dekodérem 2020) respektive inteligentní kartou a které v tomto popisu tudíž nebudou podrobněji popisovány. Jednou funkcí mikroprocesoru 110 je spravovat paměť v inteligentní kartě, jak bude popsáno níže.

20

25

EEPROM 150 obsahuje určité dynamicky vytvářené operátorové zóny 154, 155, 156 (ID operátora) a dynamicky vytvářené datové zóny, které nyní budou níže popsány ve spojení s odkazy na obr. 19.

30

Jak je patrné z obr. 19, EEPROM 150 zahrnuje permanentní zónu 151 trvalého "ID karty" (nebo výrobce) o 8



bytech, která obsahuje trvalý identifikátor účastnické inteligentní karty, zadaný výrobcem této inteligentní karty 3020.

5 Když je inteligentní karta znovunastavena, vydává mikroprocesor 110 signál do přijímače/dekodéru 2020, přičemž tento signál zahrnuje identifikátor systému s podmíněným přístupem, který je používán touto inteligentní kartou, a data vytvořená z dat uložených v inteligentní kartě, včetně ID (identifikátor) karty. Tento signál je uložen
10 přijímačem/dekodérem 2020, který následně využívá tento uložený signál pro kontrolu, zda inteligentní karta je kompatibilní se systémem podmíněného přístupu, který je použit tímto přijímačem/dekodérem 2020.

15 EEPROM 150 rovněž obsahuje permanentní zónu 152 "generátoru náhodných čísel", která obsahuje program pro vytváření pseudonáhodných čísel. Tato náhodná čísla jsou používána pro rozdělovací transakce výstupních signálů, vyvářených inteligentní kartou 3020 a vysílaných zpět do vysílače.
20

Pod permanentní zónou 152 generátoru náhodných čísel je vytvořena permanentní "řídící" zóna 153 o 144 bytech. Tato permanentní řídící zóna 153 je specifická operátorová zóna využívaná programem V ROM 130 při dynamickém vytváření (a
25 odstraňování) zón 154, 155, 156 ..., jak je podrobněji popsáno níže. Permanentní řídící zóna 153 obsahuje data týkající se práv inteligentní karty pro vytváření nebo odstraňování zón.

30 Program pro dynamické vytváření a odstraňování zón pracuje v odezvě na specifické zprávy EMM pro vytváření (nebo



odstraňování) zón, které jsou vysílány systémem SAS 3002 a přijímány přijímačem/dekodérem 2020 a předávány do účastnické inteligentní karty 3020. Aby bylo možné vytvářet zprávy EMM, vyžaduje operátor, že řídicí zóně mají být přiděleny

5 specifické klíče. To brání jednomu operátorovi ve smazání zón týkajících se jiného operátora.

Pod řídicí zónou 153 je řada zón 154, 155, 156 "ID operátora" pro operátory 1, 2, ..., respektive N. Obvykle alespoň jedna zóna ID operátora bude předem zavedena do

10 EEPROM účastnické inteligentní karty 3020, takže koncový uživatel může dekódovat programy vysílané tímto operátorem. Ovšem další zóny ID operátora mohou být následně dynamicky vytvářeny s použitím permanentní řídicí zóny 153 v odezvě na výstupní signál transakce, vytvářený přes inteligentní kartu

15 3020 koncovým uživatelem (účastníkem), jak bude podrobněji popsáno níže.

Každá operátorová zóna 154, 155, 156 obsahuje identifikátor skupiny, ke které inteligentní karta 3020 přísluší, a umístění inteligentní karty uvnitř této skupiny.

20 Tento údaj umožňuje inteligentní kartě (společně s dalšími inteligentními kartami v její skupině), aby mohla reagovat na vysílání "skupinové" předplatitelské EMM mající adresu skupiny (ale ne umístění inteligentní karty ve skupině) a rovněž "individuální" (nebo předplacení komerčních nabídek)

25 EMM adresované pouze této inteligentní kartě uvnitř skupiny. V každé takové skupině může být 256 členských inteligentních karet a tento znak tudíž podstatně omezuje šířku pásma, která je vyžadována pro vysílání zpráv EMM.

30 Aby se dále omezila šířka pásma, vyžadovaná pro vysílání "skupinových" předplatitelských zpráv EMM, jsou

skupinová data v každé operátorové zóně 154, 155, 156 a ve všech podobných zónách v EEPROM inteligentní karty 3020 a dalších dceřiných inteligentních karet kontinuálně aktualizována pro umožnění určité inteligentní kartě změnit svoje umístění v každé skupině pro vyplnění jakýchkoliv mezer vytvořených, například, vymazáním člena skupiny. Mezery jsou vyplněny prostřednictvím SAS 3002, protože v STM obslužném kanálu 3104 je seznam těchto mezer.

Tímto způsobem je značně omezeno segmentování a počet členů v každé skupiny je udržován na hodnotě nebo v blízkosti hodnoty 256 členů.

Každá operátorová zóna 154, 155, 156 je sdružena s jedním nebo s více "operátorovými datovými objekty" (objekty dat operátora) uloženými v EEPROM 150. Jak je znázorněno na obr. 19, jsou série dynamicky vytvářených "operátorových datových" objektů 157 až 165 umístěny pod zónami ID operátora. Každý z těchto objektů je označen:

- a) "identifikátorem" 1, 2, 3 ... N odpovídajícím odpovídajícímu operátorovi 1, 2, 3 ... N, jak je znázorněno v jeho levé části na obr. 19;
- b) "ID" (identifikátorem) indikujícím typ objektu; a
- c) "datovou" zónou rezervovanou pro data, jak je znázorněno v pravé části každého relevantního operátorového datového objektu na obr. 19.

Mělo by být zcela zřejmé, že každý operátor je sdružen s podobnou sadou datových objektů, takže následující popis typu dat v datových objektech operátora 1 je rovněž použitelný pro datové objekty všech ostatních operátorů. Rovněž bude zcela zřejmé, že datové objekty jsou umístěny v



souvislých fyzických oblastech EEPROM a že jejich pořadí není podstatné.

Vymazání datových objektů vytváří "mezeru" 166 v inteligentní kartě, to znamená, že určitý počet bytů, které
 5 vymazané objekty předtím zaujímaly, nejsou nyní obsazené.
 Takto "uvolněný" počet bytů nebo "mezera" se označuje: —

a) "identifikátorem" 0; a

b) "ID" (identifikátorem) indikujícím, že tyto byty
 10 jsou volné pro přijetí objektu.

Příští vytvořený datový objekt vyplňuje tuto mezeru, která je označena identifikátorem 0. Tímto způsobem je omezená paměťová kapacita (4 kilobyty) EEPROM 150 účinně využita.

15 Pokud se nyní týká sady datových objektů sdružených s každým operátorem, budou níže popsány příklady těchto datových objektů.

Datový objekt 157 obsahuje EMM klíč použitý pro dekódování zakódovaných zpráv EMM přijatých
 20 přijímačem/dekodérem 2020. Tento EMM klíč je permanentně uložen v datovém objektu 157. Tento datový objekt 157 může být vytvořen před distribucí inteligentní karty 3020 a/nebo může být vytvořen dynamicky, když je vytvářena nová operátorová zóna (jak je popsáno výše).

25 Datový objekt 159 obsahuje ECM klíče, které jsou vyslány odpovídajícím operátorem (v tomto případě operátorem 1) pro umožnění koncovému uživateli dekódování určitého "souboru" programů, ke kterému se přihlásil (který si
 30 předplatil). Nové ECM klíče jsou vysílány obvykle každý měsíc

společně s (obnovovací) zprávou EMM skupinového předplacení, která obnovuje celkové právo koncového uživatele pro sledování vysílání od (v tomto případě) operátora 1. Použití samostatné zprávy EMM a ECM klíčů umožňuje, aby sledovací práva byla nakupována různými způsoby (v tomto případě prostřednictvím předplacení a jednotlivě (platba za shlednutí)), a rovněž zvyšuje bezpečnost. Mód platby za shlednutí (PPV) bude podrobněji popsán níže.

Protože nové ECM klíče jsou vysílány periodicky, je podstatné zabránit uživateli v používání starých ECM klíčů, například prostřednictvím vypínání přijímače/dekodéru nebo opětovným nastavením hodin pro zabránění uplynutí platnosti starého ECM klíče, takže časovač v přijímači/dekodéru 2020 by mohl být přeskočen. Proto tedy operátorová zóna 154 zahrnuje oblast (obvykle mající velikost 2 byty) obsahující datum zastarání ECM klíčů. Inteligentní karta 3020 je uspořádána pro porovnání tohoto data se současným datem, které je obsaženo v přijímaných zprávách ECM, a pro zabránění v dekódování, pokud je současné datum pozdější než datum zastarání. Datum zastarání je vysíláno přes zprávy EMM, jak je popsáno výše.

Datový objekt 161 obsahuje 64 bitovou účastnickou bitovou mapu, která je přesnou reprezentací vysílaných programů operátora, ke kterým se účastník přihlásil (které si předplatil. Každý bit reprezentuje program a je nastaven na hodnotu "1", pokud je předplacen, a na hodnotu "0", pokud není předplacen.

Datový objekt 163 obsahuje množství jednotek, které mohou být použity spotřebitelem v PPV módu pro nákup sledovacích práv pro bezprostřední vysílání, například v

odezvě na volné ukázky nebo jinou reklamu. Datový objekt 163 rovněž obsahuje limitní hodnotu, která může být nastavena, například na zápornou hodnotu, pro umožnění kreditu spotřebitelům. Jednotky mohou být nakupovány, například prostřednictvím kreditu a přes modemový zpětný kanál 4002, nebo, například, prostřednictvím použití hlasového obslužného kanálu v kombinaci s kreditní kartou. Určitá událost může být účtována jako jedna jednotka nebo určitý počet jednotek.

Datový objekt 165 obsahuje popis PPV události, jak je znázorněno ve spojení s odkazy na tabulku 167 znázorněnou na obr. 20.

Tabulka 167, popisující PPV událost, obsahuje "ID 168 relace", identifikující relaci určenu ke sledování (odpovídající programu a času a datu vysílání) "mód 169 relace", indikující jak jsou nakupována sledovací práva (například v objednávkovém módu), "index 171 relace" a sledování 171 relace".

Pokud se týká přijímání programu v PPV módu, přijímač/dekodér 2020 určuje zda program je programem prodáváním v PPV módu. Pokud ano, pak dekodér 2020 kontroluje s použitím položek uložených v tabulce 167, popisující PPV událost, zda je v ní uložen ID relace pro tento program. Pokud je zde ID relace uložen, pak je ze zprávy ECM vyjmuto řídicí slovo.

Pokud zde ID relace není uložen, pak prostřednictvím specifické aplikace přijímač/dekodér 2020 zobrazí zprávu koncovému uživateli, která indikuje, že uživatel má právo sledovat relaci za cenu řekněme 25 jednotek, jak je přečteno ze zprávy ECM, nebo se může spojit s komunikačními obslužnými



kanály 3022, aby událost nakoupil. Při použití jednotek, pokud koncový uživatel odpoví "ano" (prostřednictvím vzdálené řídicí jednotky 2026 (viz obr. 2)), dekodér 2020 vysílá zprávu ECM do inteligentní karty, inteligentní karta snižuje obsah peněženky v inteligentní kartě 3020 o 25 jednotek, zapisuje ID 168 relace, mód 169 relace, index 170 relace a sledování 171 relace do tabulky 167, popisující PPV událost, a vyjímá a dešifruje řídicí slovo ze zprávy ECM.

V "objednávkovém módu" bude do inteligentní karty 3020 předána zpráva EMM, takže inteligentní karta zapíše ID 168 relace, mód 169 relace, index 170 relace a sledování 171 relace do tabulky 167, popisující PPV událost, s použitím této zprávy EMM.

Index 170 relace může být nastaven pro odlišení jednoho vysílání od druhého. Tento znak umožňuje autorizaci, aby byla dána pro podskupinu vysílání, například, 3 krát z 5 vysílání. Jakmile je do inteligentní karty předána zpráva EMM s indexem relace odlišným od současného indexu 170 relace, uloženého v tabulce 167, popisující PPV událost, je počet sledování 171 relace snížen o jednu. Když sledování 171 relace dosáhne hodnoty nula, inteligentní karta odmítne dešifrovat zprávu ECM s jiným indexem relace, než je současný index relace.

Počáteční hodnota sledování relace závisí pouze na způsobu, kterým si poskytovatel vysílání přeje definovat událost, které se sledování týká; sledování relace pro příslušnou událost může mít jakoukoliv hodnotu.



Mikroprocesor 110 v inteligentní kartě realizuje počítání a porovnávací program pro detekci toho, kdy již bylo dosaženo limitu počtu sledování určitého programu.

5 Všechny složky ID 168 relace, mód 169 relace, index 170 relace a sledování 171 relace v tabulce 167, popisující PPV událost, mohou být vyjmuty z inteligentní karty s použitím "zpětné" procedury, jak bylo popsáno v předcházejícím popisu.

10 Každý přijímač/dekodér 2020 obsahuje identifikátor, který může buď identifikovat jednoznačně tento přijímač/dekodér nebo může identifikovat jeho výrobce nebo jej může klasifikovat nějakým jiným způsobem, aby mu umožnil pracovat pouze s určitou individuální inteligentní kartou, určitou třídou inteligentních karet vyrobených stejným nebo 15 odpovídajícím výrobcem nebo jakoukoliv jinou třídou inteligentních karet, které jsou určeny pro použití výhradně s touto třídou přijímačů/dekodérů.

20 Tímto způsobem přijímače/dekodéry 2020, které byly spotřebiteli dodány jedním dodavatelem vysílání, jsou chráněny proti používání neautorizovaných dceřiných karet 3020.

25 Přidavně nebo alternativně k tomuto prvnému "potvrzení spolupráce" mezi inteligentní kartou a přijímačem by EEPROM inteligentní karty 3020 mohla obsahovat pole nebo bitovou mapu popisující kategorie přijímačů/dekodérů 2020, se kterými může fungovat. Tyto kategorie by mohly být specifikovány buď v průběhu výroby inteligentní karty 3020 nebo prostřednictvím specifické zprávy EMM.

Bitová mapa uložená v inteligentní kartě 3020 obvykle zahrnuje seznam až 80 přijímačů/dekodérů, z nichž každý je identifikován odpovídajícím ID přijímače/dekodéru, se kterými tato inteligentní karta může být použita. S každým

5 přijímačem/dekodérem je sdružena úroveň "1" nebo "0", která indikuje, zda inteligentní karta může respektive nemůže být použita s tímto přijímačem/dekodérem. Program v paměti 2024 přijímače/dekodéru vyhledává identifikátor přijímače/dekodéru v bitové mapě uložené v inteligentní kartě. Pokud je tento

10 identifikátor nalezen a hodnota sdružená s tímto identifikátorem je "1", pak je tato inteligentní karta "aktivována", pokud ne, pak inteligentní karta nebude fungovat s tímto přijímačem/dekodérem.

Navíc, pokud, obvykle z důvodu dohody mezi operátory, je žádoucí autorizovat použití jiných inteligentních karet v určitém přijímači/dekodéru, budou do těchto inteligentní karet vyslány speciální zprávy EMM pro změnu jejich bitových map přes odpovídač 2014.

15

Každý poskytovatel vysílání může rozlišovat své účastníky podle určitého předem stanoveného kritéria. Například určitý počet účastníků může být klasifikován jako "VIP". Každý poskytovatel vysílání tedy může rozdělit své účastníky do množství podskupin, přičemž každá podskupina zahrnuje jakýkoliv počet účastníků.

20

25

Podskupina, ke které určitý účastník náleží, je nastavena v SMS 3004. Dále SAS 3002 vysílá zprávu EMM k účastníkovi, která zapisuje informaci (obvykle o délce 1 byte) týkající se podskupiny, ke které účastník náleží, do relevantní zóny dat operátora, řekněme do zóny 154, EEPROM v inteligentní kartě. Dále, jak jsou události vysílány

30



poskytovatelem vysílání, je vysílána zpráva EMM, obvykle o délce 256 bitů, s událostí, přičemž tato zpráva EMM indikuje, které z podskupin účastníků mohou sledovat tuto událost.

Pokud podle informace uložené v operátorové zóně účastník nemá práva pro sledování události, jak je určeno zprávou ECM, je sledování programu odepřeno.

Toto uspořádání může být využito, například, pro odpojení všech daných inteligentních karet operátora v určité geografické oblasti v průběhu vysílání určitého programu, zejména programu týkajícího se sportovní události probíhající v této geografické oblasti. Tímto způsobem mohou fotbalové kluby a jiná sportovní tělesa prodávat vysílací práva vně jejich lokality, přičemž současně brání místním fanouškům ve sledování události v televizi. Takto jsou místní fanoušci povzbuzeni k nákupu lístků a návštěvě události.

Každý ze znaků sdružených s zónami 151 až 172 je považován za samostatný vynález nezávisle na dynamickém vytváření zón.

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.

5 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 řídicího 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 řídicí 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. Systém s podmíněným přístupem, v y z n a č u j í c í
s e t í m , že zahrnuje:

5 prostředek pro vytváření množství zpráv;

 prostředek pro přijímání zpráv; a

 komunikační obslužný kanál spojený přímo s uvedeným
prostředkem pro vytváření zpráv, přičemž uvedený prostředek
pro vytváření zpráv je upraven pro komunikaci s uvedeným
přijímacím prostředkem přes tento komunikační obslužný kanál;

10 přičemž uvedený prostředek pro vytváření zpráv je
upraven pro vytváření zpráv v odezvě na data komunikovaná do
prostředku pro vytváření zpráv z uvedeného přijímacího
prostředku přes uvedený komunikační obslužný kanál.

15 2. Systém s podmíněným přístupem podle nároku

1, v y z n a č u j í c í s e t í m , že zprávami
vytvářenými prostředkem pro vytváření zpráv jsou opravňovací
zprávy.

3. Systém s podmíněným přístupem podle nároku 1 nebo

20 2, v y z n a č u j í c í s e t í m , že dále zahrnuje
satelitní odpovídač, přičemž prostředek pro vytváření zpráv
je uspořádán pro vysílání zprávy jako paketu digitálních dat
do uvedeného přijímacího prostředku buď přes uvedený
komunikační obslužný kanál nebo přes uvedený satelitní
25 odpovídač.

4. Systém s podmíněným přístupem podle kteréhokoliv z
předcházejících nároků, v y z n a č u j í c í s e t í m ,
že uvedený přijímací prostředek je spojitelný s uvedeným
komunikačním obslužným kanálem prostřednictvím modemu a
30 telefonní linky.



5. Systém s podmíněným přístupem podle kteréhokoliv z předcházejících nároků, v y z n a č u j í c í s e t í m , že zprávy jsou vytvářeny prostředkem pro vytváření zpráv v odezvě na příkaz z přijímacího prostředku.

5 6. Vysílací a přijímací systém, v y z n a č u j í c í s e t í m , že zahrnuje systém s podmíněným přístupem podle kteréhokoliv z předcházejících nároků.

10 7. Vysílací a přijímací systém podle nároku 6, v y z n a č u j í c í s e t í m , že komunikační obslužný kanál je schopen realizovat vyhrazené spojení mezi přijímacím prostředkem a prostředkem pro vytváření zpráv.

15 8. Vysílací a přijímací systém podle nároku 6, v y z n a č u j í c í s e t í m , že dále zahrnuje modem, přičemž uvedený prostředek pro vytváření zpráv je spojen s tímto modemem přes uvedený komunikační obslužný kanál.

20 9. Vysílací a přijímací systém podle kteréhokoliv z nároků 6 až 8, v y z n a č u j í c í s e t í m , že přijímací prostředek zahrnuje prostředek pro čtení inteligentní karty, která je do něj zasunuta koncovým uživatelem, přičemž tato inteligentní karta má v sobě uložena data pro automatickou inicializaci vysílání zprávy z uvedeného přijímacího prostředku do uvedeného prostředku pro vytváření zpráv po vložení inteligentní karty koncovým uživatelem.

25 30 10. Vysílací a přijímací systém podle kteréhokoliv z nároků 6 až 9, v y z n a č u j í c í s e t í m , že dále zahrnuje hlasovou linku pro umožnění koncovému uživateli

vysílacího a přijímacího systému komunikovat s prostředkem pro vytváření zpráv.

5 11. Vysílací a přijímací systém podle kteréhokoliv z nároků 6 až 10, v y z n a č u j í c í s e t í m , že přijímací prostředek zahrnuje přijímač/dekodér zahrnující prostředek pro přijímání komprimovaných signálů MPEG typu, prostředek pro dekódování přijatých signálů pro vytvoření televizního signálu a prostředek pro přivedení televizního signálu do televize.

10 12. Systém s podmíněným přístupem pro poskytnutí podmíněného přístupu účastníkům, v y z n a č u j í c í s e t í m , že zahrnuje:

účastnický řídicí systém;

15 účastnický autorizační systém spojený s účastnickým řídicím systémem; a

komunikační obslužný kanál; přičemž tento obslužný kanál je spojen přímo s účastnickým autorizačním systémem, to jest ne přes účastnický řídicí systém;

20 přičemž uvedený účastnický autorizační systém je upraven pro vytváření zpráv v odezvě na data přijatá přes uvedený komunikační obslužný kanál..

25 13. Systém s podmíněným přístupem podle nároku 12, v y z n a č u j í c í s e t í m , že dále zahrnuje přijímač/dekodér pro účastníka, přičemž tento přijímač/dekodér je spojitelný s uvedeným komunikačním obslužným kanálem a tudíž s uvedeným účastnickým autorizačním systémem prostřednictvím modemu a telefonní linky.

30 14. Systém s podmíněným přístupem podle nároku 13, v y z n a č u j í c í s e t í m , že dále zahrnuje

satelitní odpovídač, přičemž účastnický autorizační systém je uspořádán pro vysílání zprávy jako paketu digitálních dat do uvedeného přijímače/dekodéru buď přes uvedený komunikační obslužný kanál nebo přes uvedený satelitní odpovídač.

5 15. Systém s podmíněným přístupem podle nároku 13 nebo 14, v y z n a č u j í c í s e t í m , že uvedený přijímač/dekodér je spojitelný s uvedeným komunikačním obslužným kanálem prostřednictvím modemu a telefonní linky.

10 16. Systém s podmíněným přístupem podle kteréhokoliv z nároků 13 až 15, v y z n a č u j í c í s e t í m , že zprávy jsou vytvářeny účastnickým autorizačním systémem v odezvě na příkaz z přijímače/dekodéru.

15 17. Systém s podmíněným přístupem podle kteréhokoliv z nároků 12 až 16, v y z n a č u j í c í s e t í m , že zprávy vytvářené účastnickým autorizačním systémem jsou opravňovací zprávy.

20 18. Systém s podmíněným přístupem, v y z n a č u j í c í s e t í m , že zahrnuje:

komunikační obslužný kanál spojitelný s účastnickým přijímačem/dekodérem;

účastnický řídicí systém pro uložení předplatitelské informace; a

25 účastnický autorizační systém pro vytváření zpráv v odezvě na příkazy přijaté přes komunikační obslužný kanál, a zahrnující:

30 příkazově centralizovaný obslužný kanál spojený s komunikačním obslužným kanálem pro přijímání příkazů z přijímače/dekodéru a informací z účastnického řídicího systému;

autorizační obslužný kanál spojený s příkazově centralizovaným obslužným kanálem pro identifikaci a ověření účastníka v odezvě na autorizační žádost z příkazově centralizovaného obslužného kanálu; a

5 generátor zpráv spojený s příkazově centralizovaným obslužným kanálem pro vytváření opravňovacích zpráv v odezvě na příkaz přijatý z příkazově centralizovaného obslužného kanálu;

10 přičemž uvedený příkazově centralizovaný obslužný kanál je upraven pro vydání uvedeného příkazu do generátoru zpráv v odezvě na data přijatá z alespoň jednoho z uvedeného autorizačního obslužného kanálu a uvedeného účastnického řídicího systému, a pro vysílání uvedených opravňovacích zpráv do přijímače/dekodéru přes komunikační obslužný kanál.

15 19. Vysílací a přijímací systém, v y z n a č u j í c í s e t í m , že zahrnuje:

na vysílacím konci:

20 vysílací systém zahrnující prostředek pro vysílání zpětné žádosti; a

na přijímacím konci:

přijímač zahrnující prostředek pro zpětné volání vysílacího systému v odezvě na zpětnou žádost;

25 přičemž vysílací systém je uspořádán pro ověření platnosti přijímače přes uvedenou zpětnou žádost.

30 20. Vysílací a přijímací systém podle nároku 19, v y z n a č u j í c í s e t í m , že vysílací systém zahrnuje prostředek pro vytváření kontrolní zprávy a pro její předání do přijímače, přičemž přijímač zahrnuje prostředek pro kódování této kontrolní zprávy a pro její předání vysílacímu systému, a vysílací systém dále zahrnuje

prostředek pro dekodování kontrolní zprávy přijaté z přijímače a pro její porovnání s původní kontrolní zprávou.

21. Vysílací a přijímací systém podle nároku 19 nebo 20, v y z n a č u j í c í s e t í m , že vysílací prostředek uspořádán pro vysílání zpětné žádosti, která zahrnuje příkaz, že zpětné volání bude provedeno v danou dobu, a prostředek pro zpětné volání vysílacího systému je uspořádán pro odezvu na tento příkaz.

22. Vysílací a přijímací systém, v y z n a č u j í c í s e t í m , že zahrnuje:
na vysílacím konci:

vysílací systém zahrnující prostředek pro vysílání zpětné žádosti; a

na přijímacím konci:

přijímač zahrnující prostředek pro zpětné volání vysílacího systému v odezvě na zpětnou žádost;

příčemž zpětná žádost zahrnuje příkaz, že zpětné volání bude provedeno v danou dobu, a prostředek pro zpětné volání vysílacího systému je uspořádán pro odezvu na tento příkaz.

23. Vysílací a přijímací systém podle kteréhokoliv z nároků 19 až 22, v y z n a č u j í c í s e t í m , že prostředek pro zpětné volání vysílacího systému zahrnuje modem spojitelný s telefonním systémem.

24. Vysílací a přijímací systém podle kteréhokoliv z nároků 19 až 23, v y z n a č u j í c í s e t í m , že prostředek pro zpětné volání vysílacího systému je uspořádán pro přenos do vysílacího systému informace týkající se přijímače.

25. Vysílací a přijímací systém podle nároku 24, v y z n a č u j í c í s e t í m , že vysílací systém zahrnuje prostředek pro uložení informace.

5 26. Vysílací a přijímací systém podle kteréhokoliv z nároků 19 až 25, v y z n a č u j í c í s e t í m , že vysílací prostředek je uspořádán pro vysílání zpětné žádosti jako alespoň jedné opravňovací zprávy.

10 27. Vysílací a přijímací systém podle kteréhokoliv z nároků 19 až 26, v y z n a č u j í c í s e t í m , že zpětná žádost zahrnuje příkaz, že pokus o zpětný hovor bude realizován s daným počtem pokusů, přičemž tento příkaz specifikuje dobu mezi pokusy o zpětný hovor.

15 28. Vysílací a přijímací systém podle kteréhokoliv z nároků 19 až 27, v y z n a č u j í c í s e t í m , že zpětná žádost zahrnuje příkaz specifikující alespoň jedno telefonní číslo, které má být vytočeno přijímacím prostředkem při odezvě na zpětnou žádost.

20 29. Systém s podmíněným přístupem a vysílací a přijímací systém v podstatě podle zde uvedeného popisu ve spojení s připojenými výkresy, zejména s obr. 12, obr. 13 a obr. 14.

Zastupuje :

25

30

Fig.1.

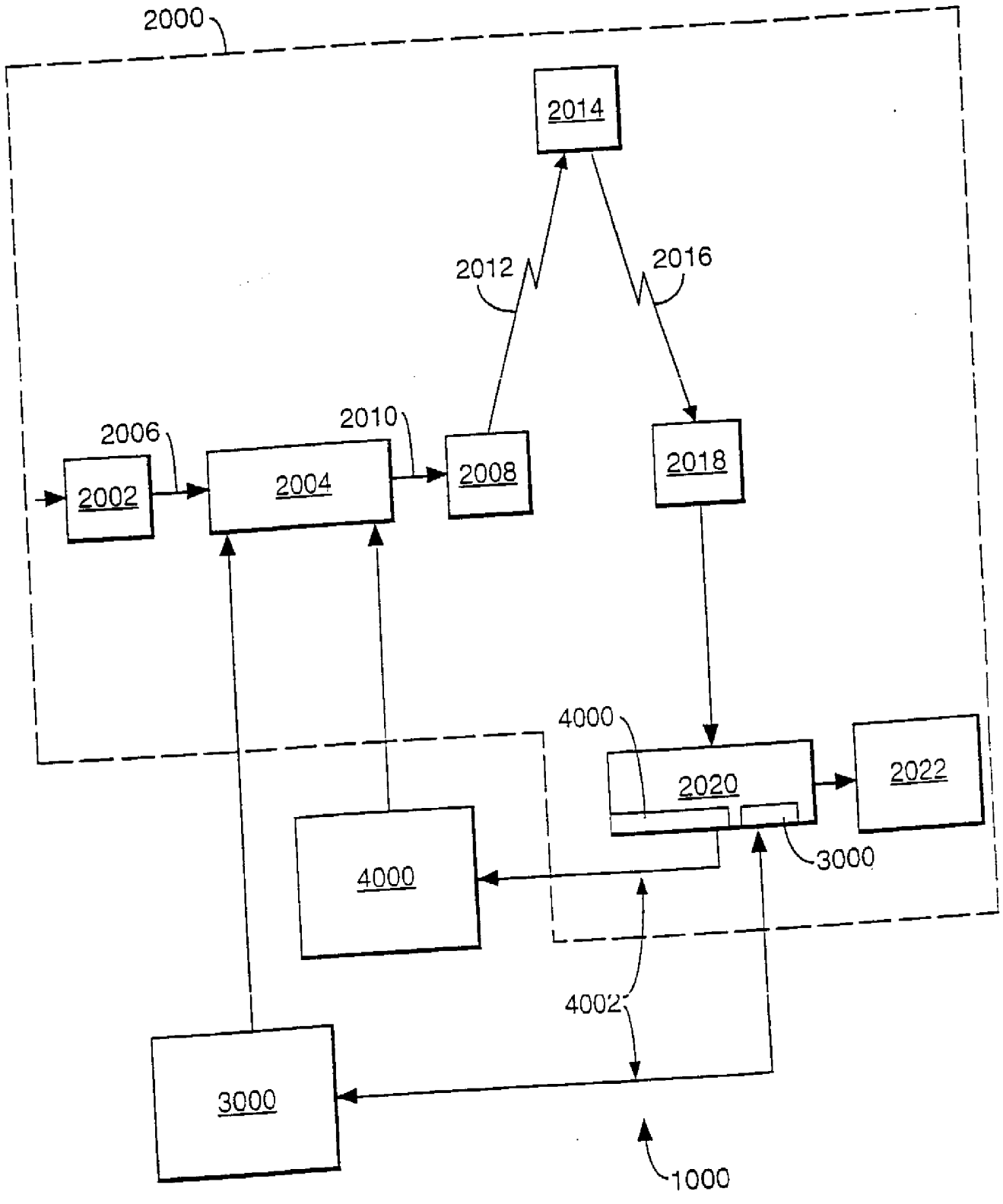


Fig.2.

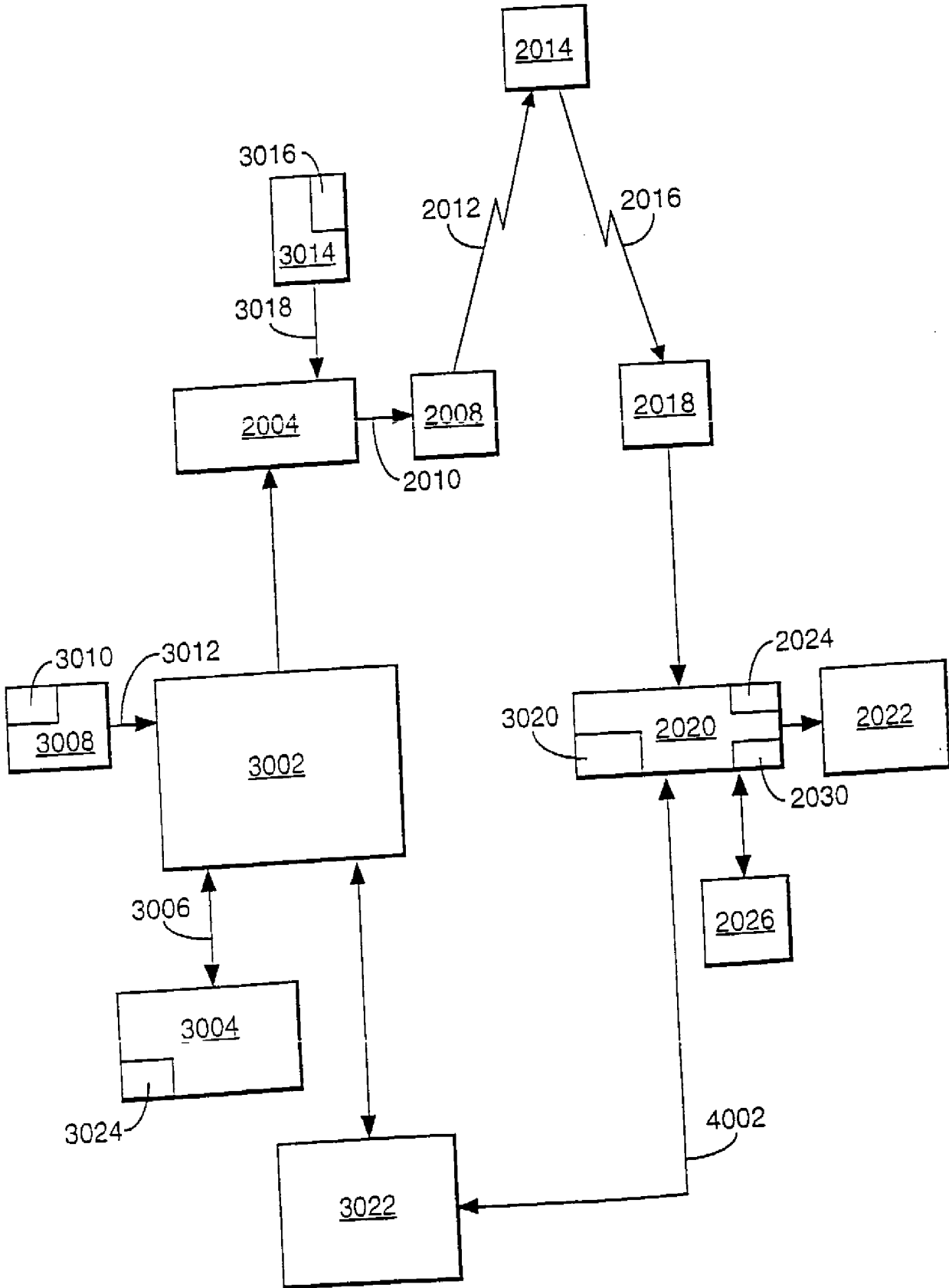


Fig.3.

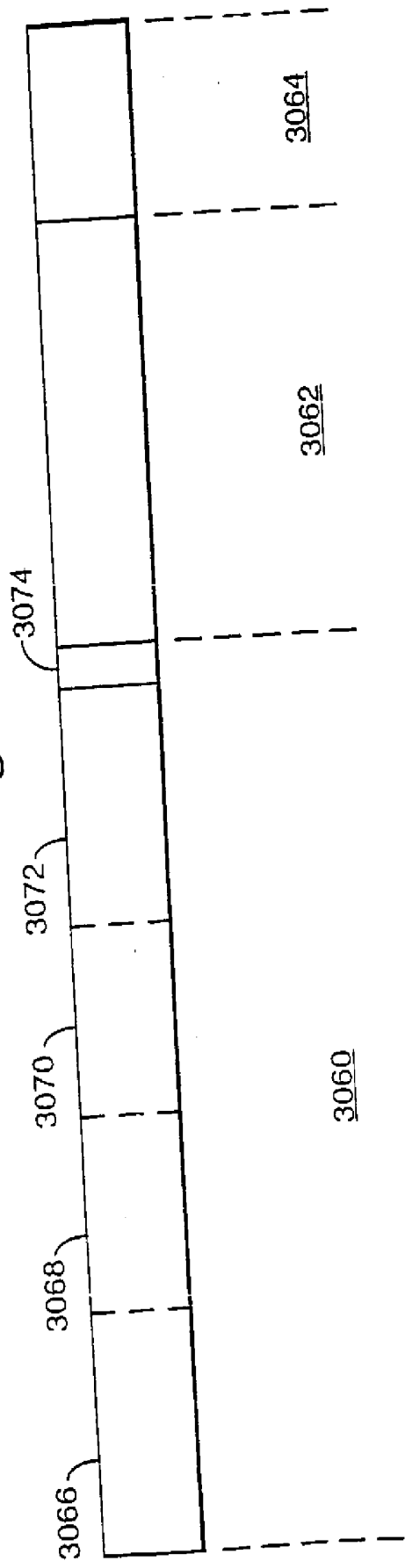


Fig. 4.

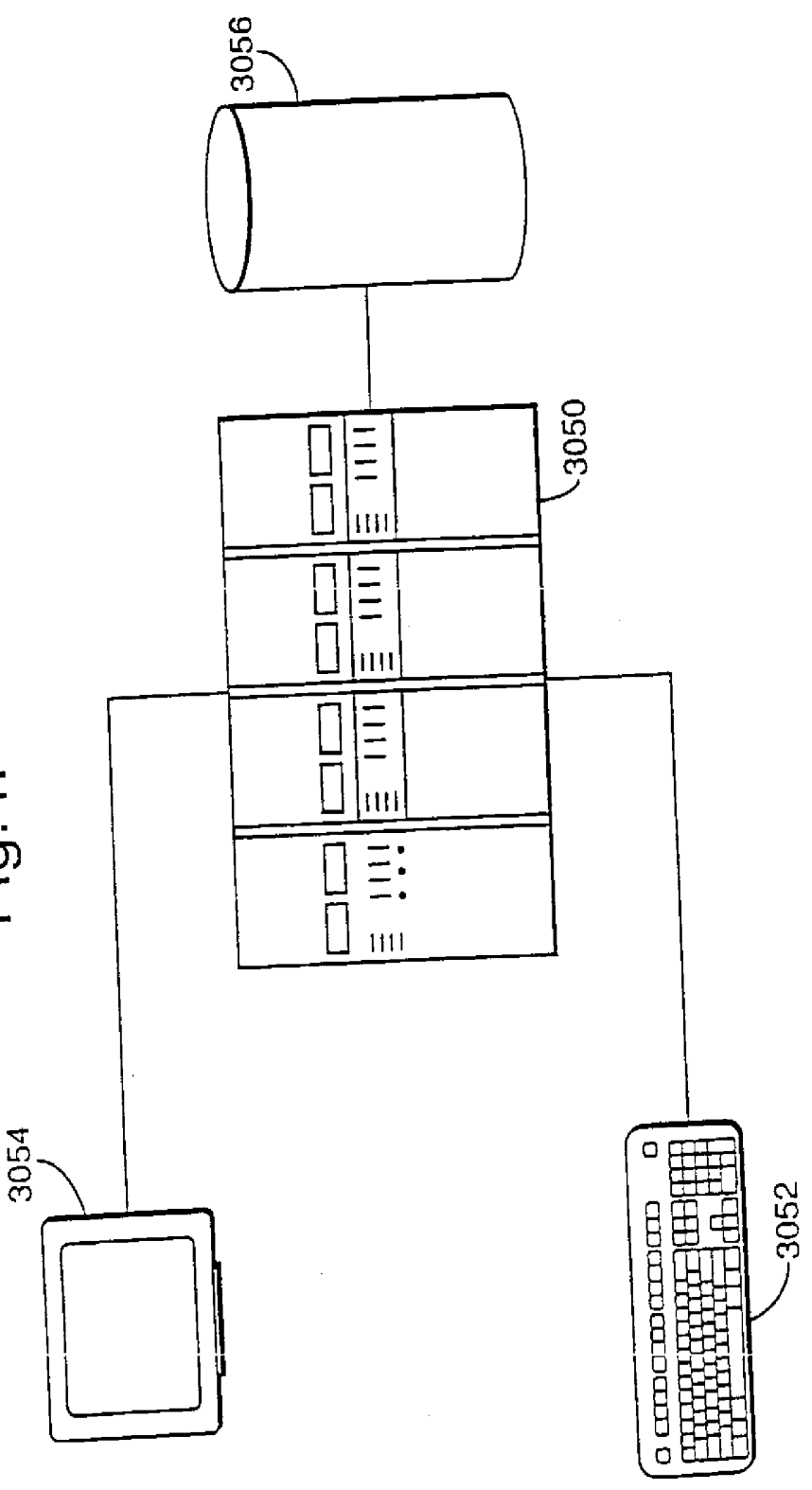
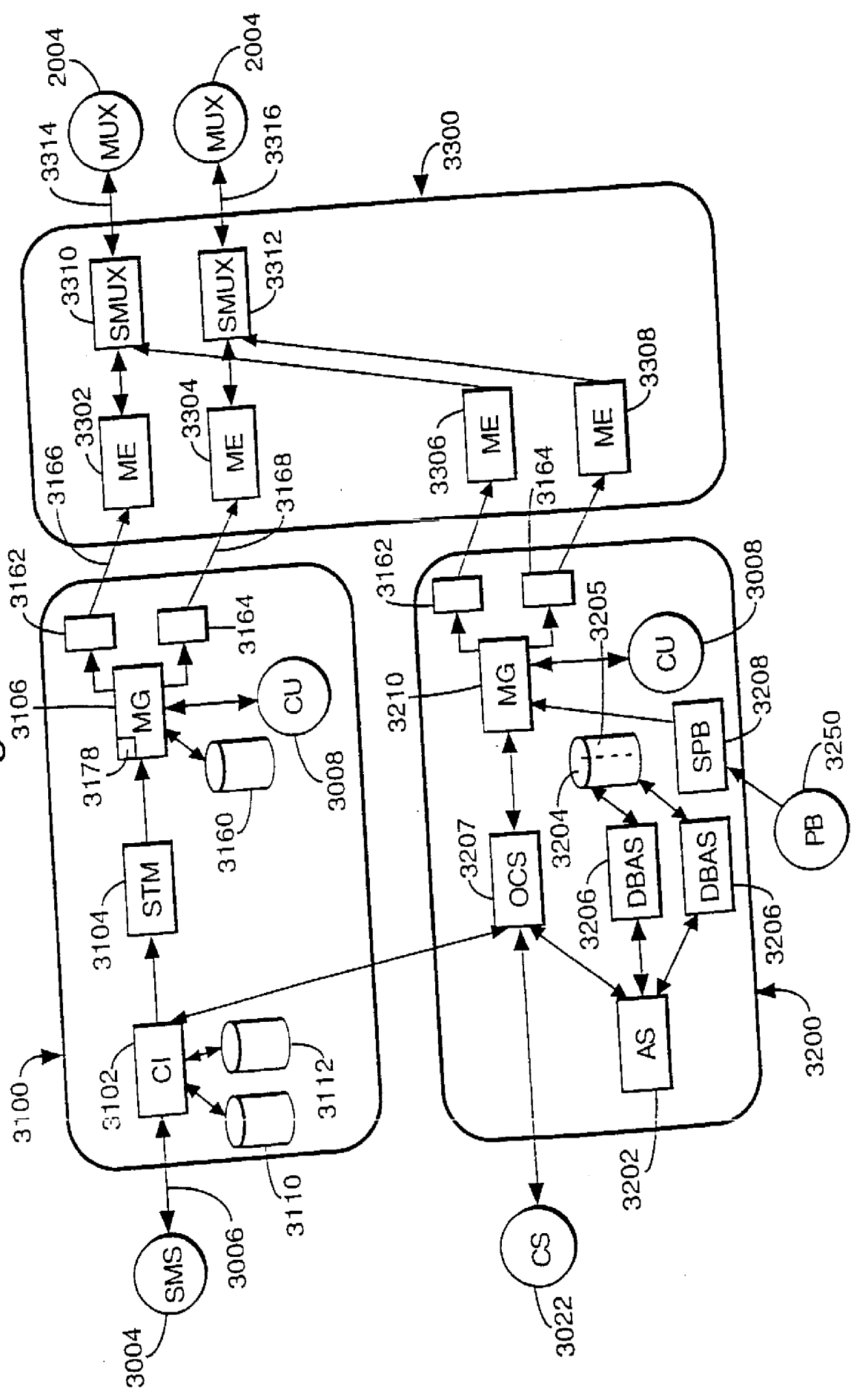


Fig. 5.



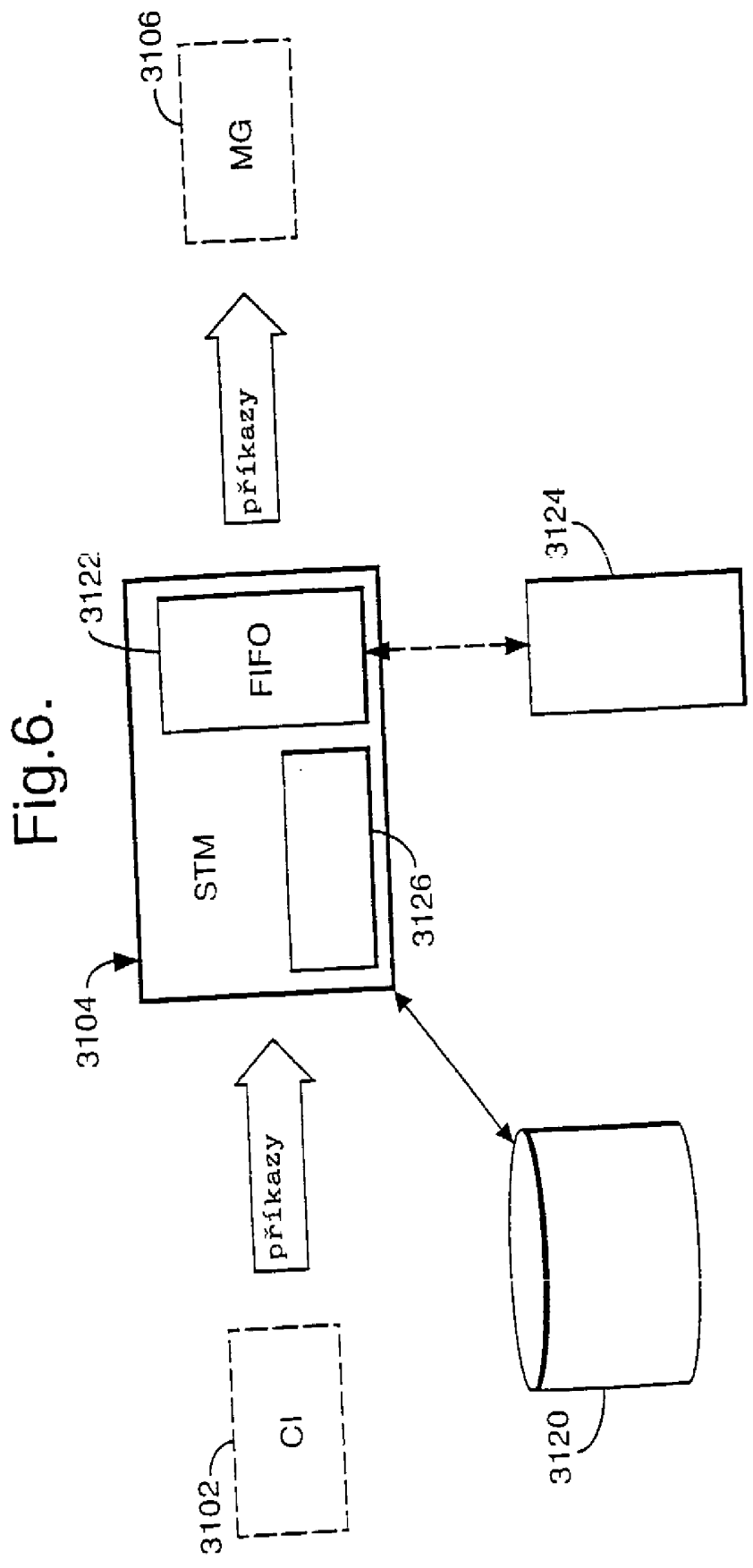


Fig. 7.

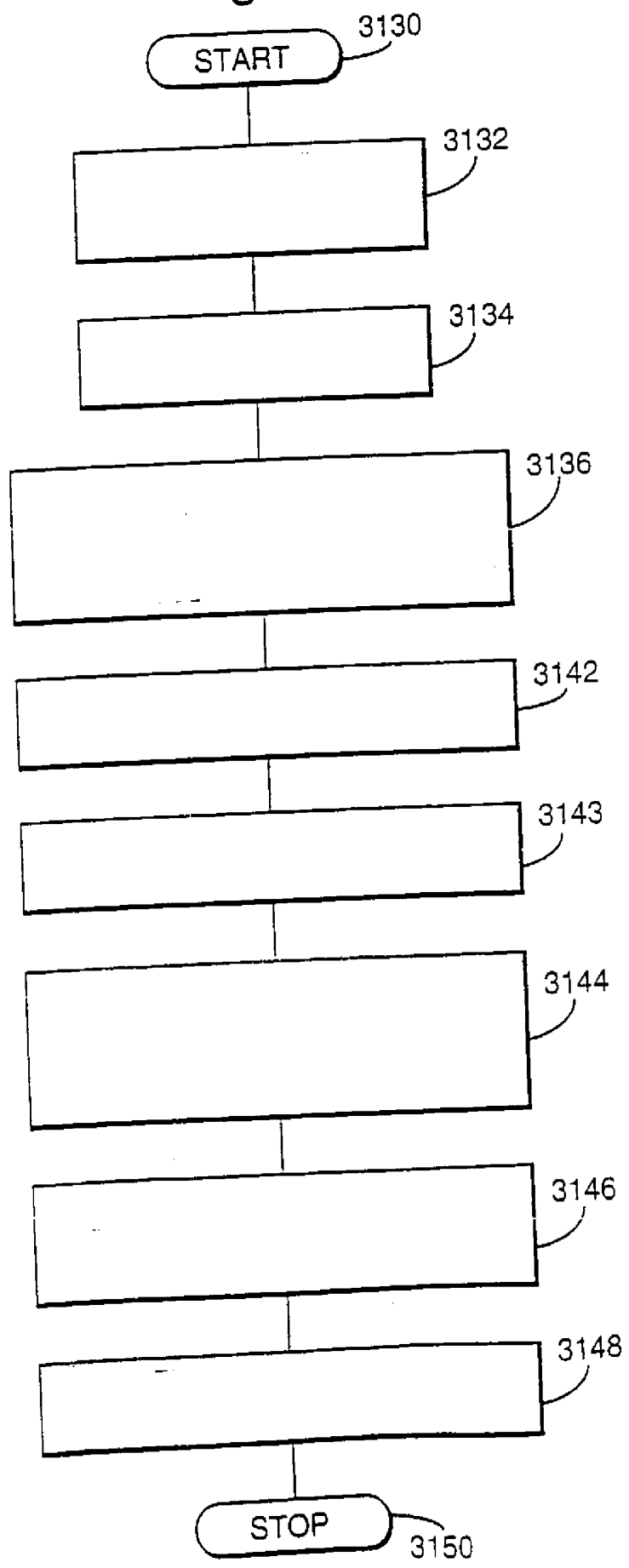


Fig.8.

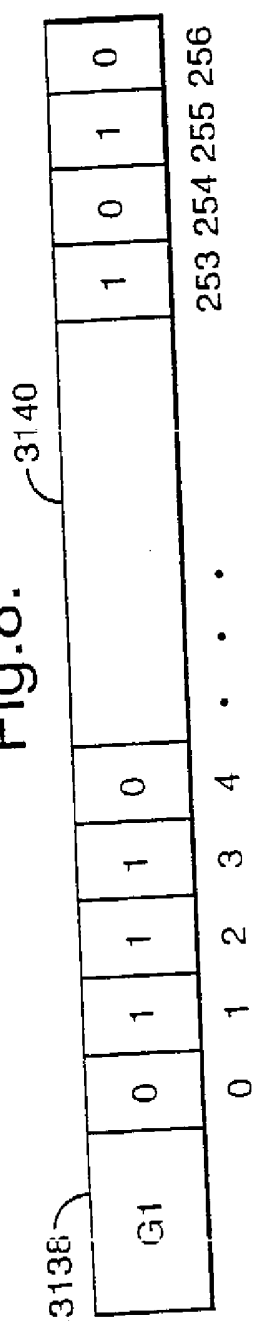


Fig.9.

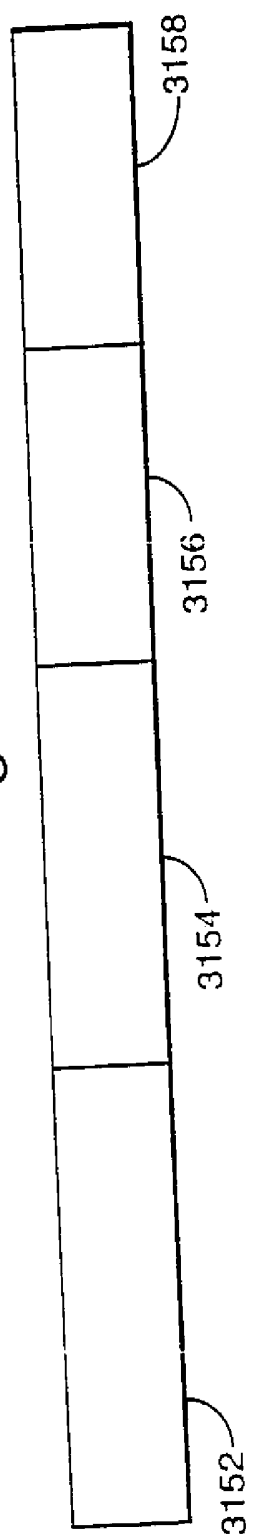


Fig.10.

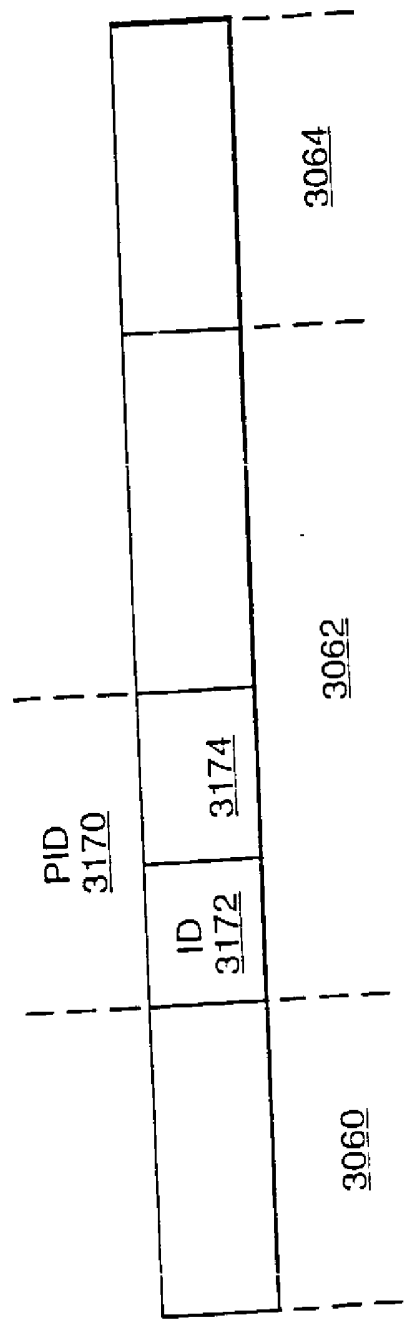


Fig.11.

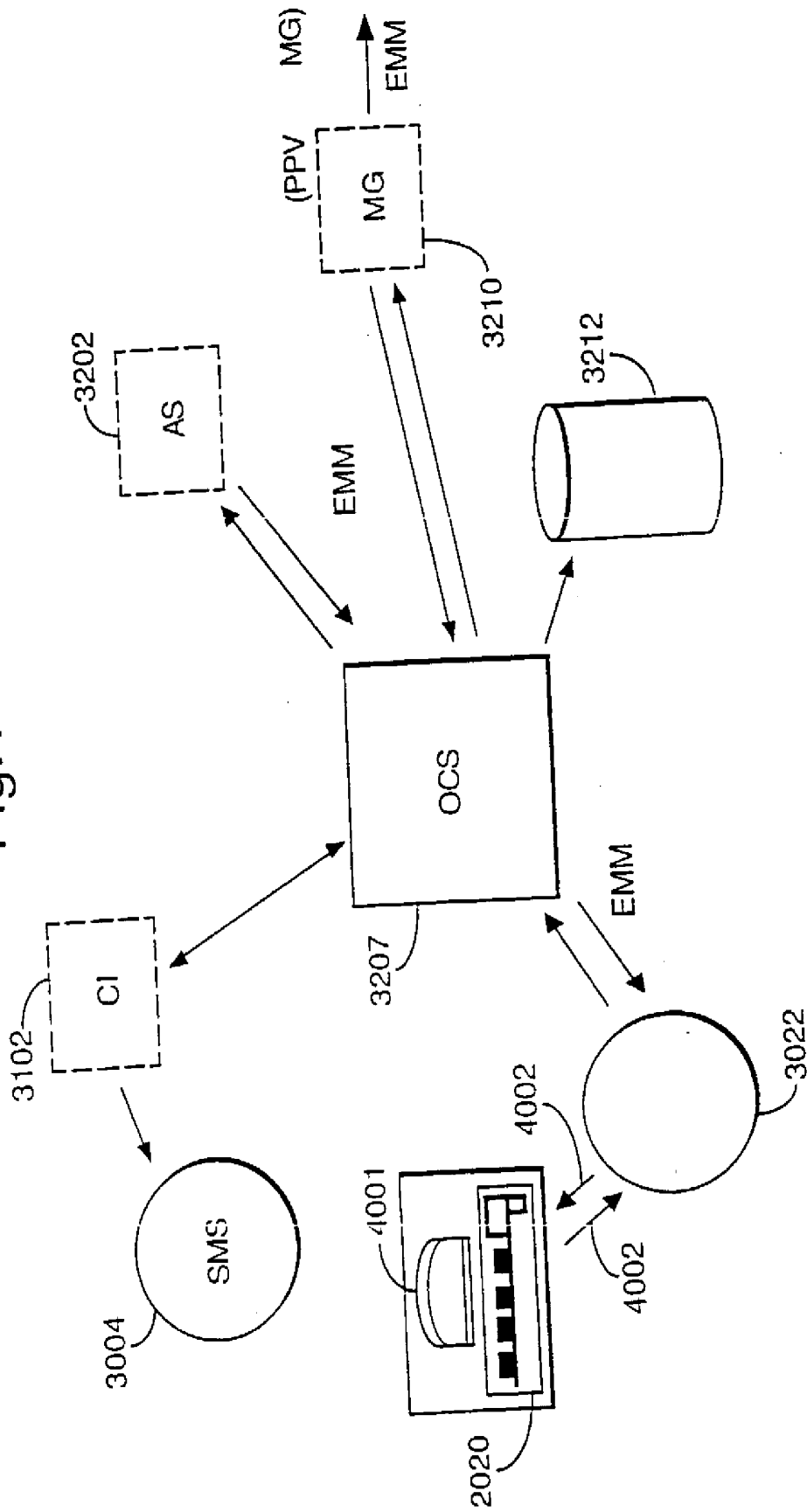


Fig.12.

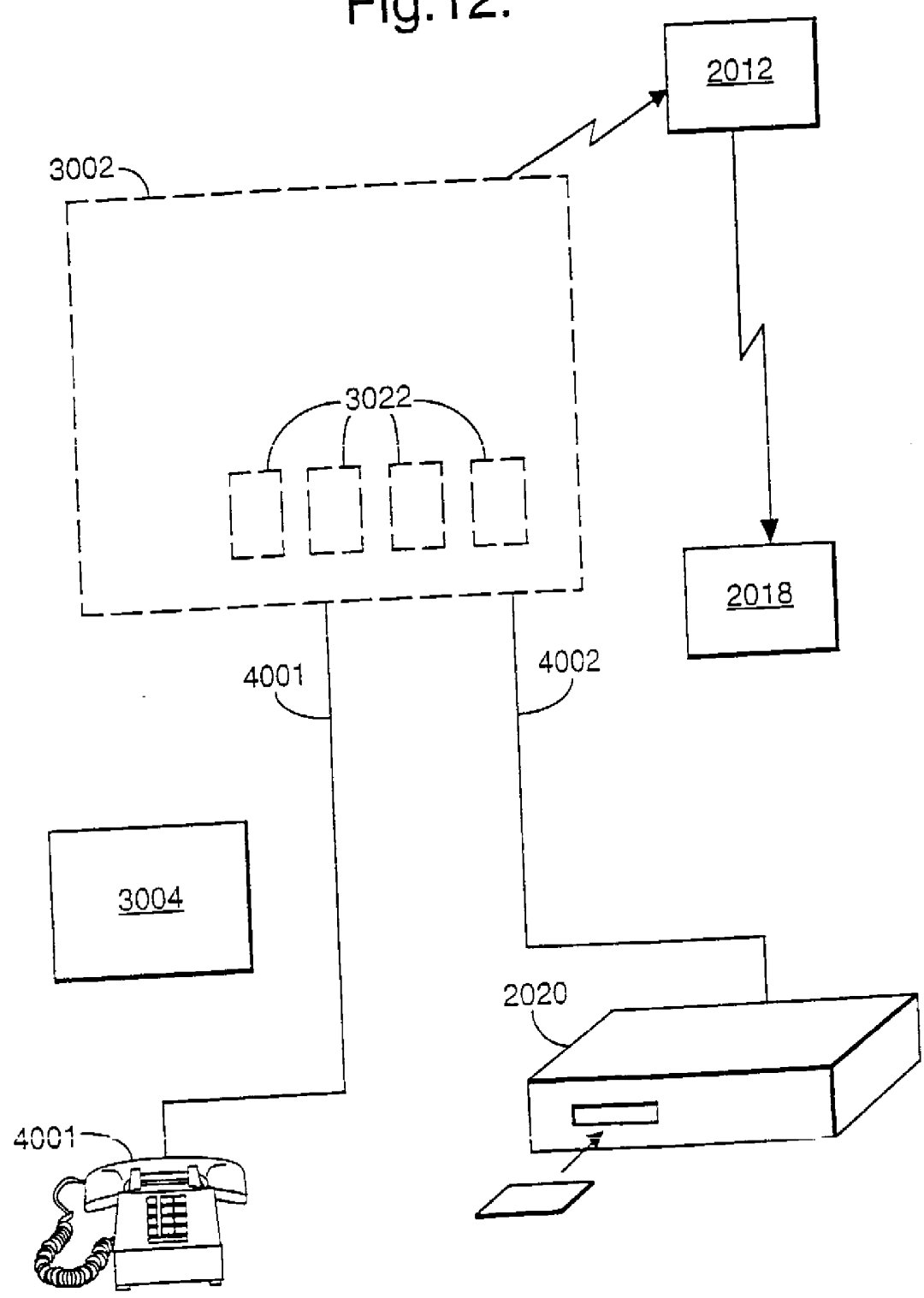


Fig. 13.

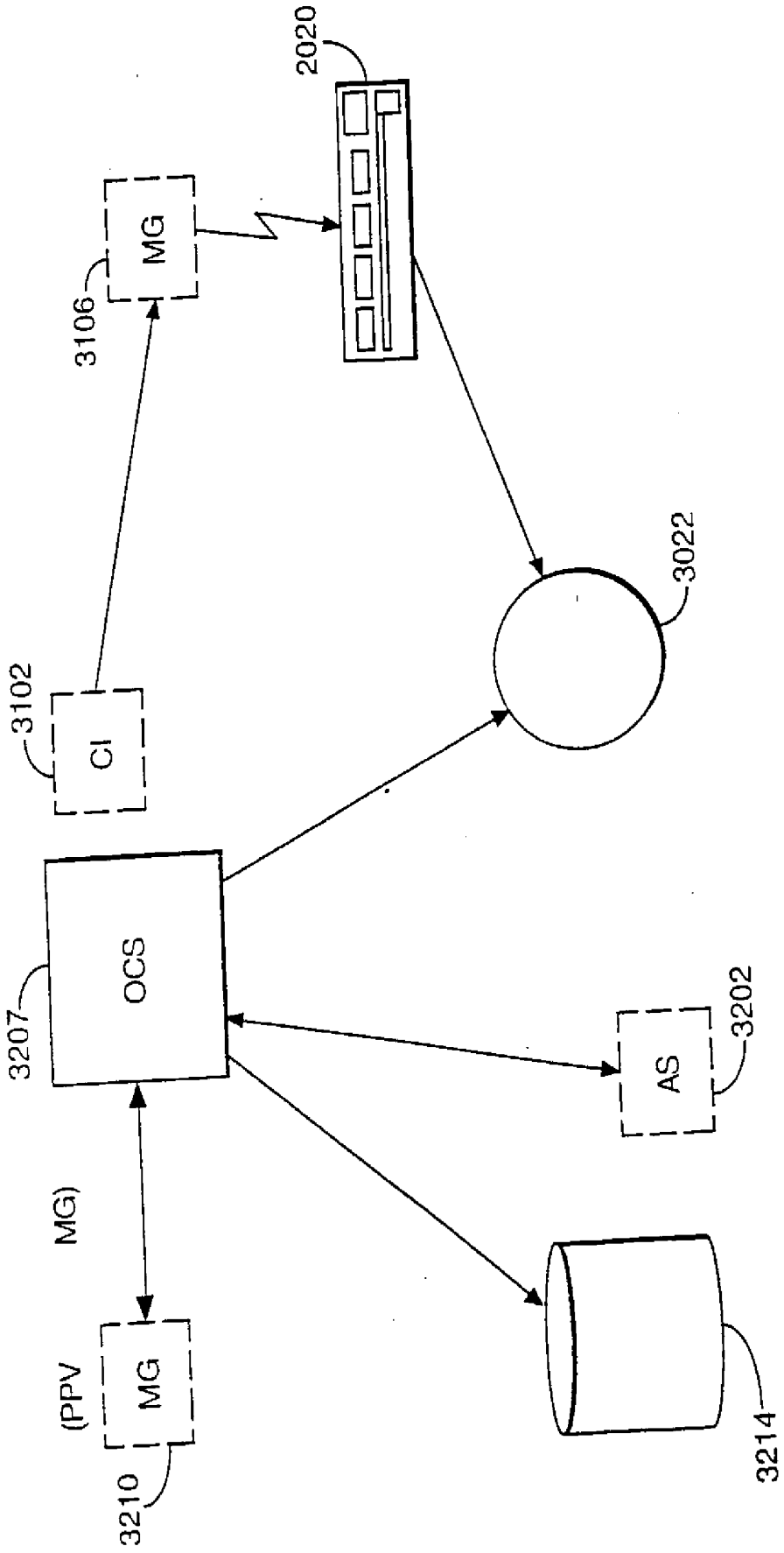


Fig. 14.

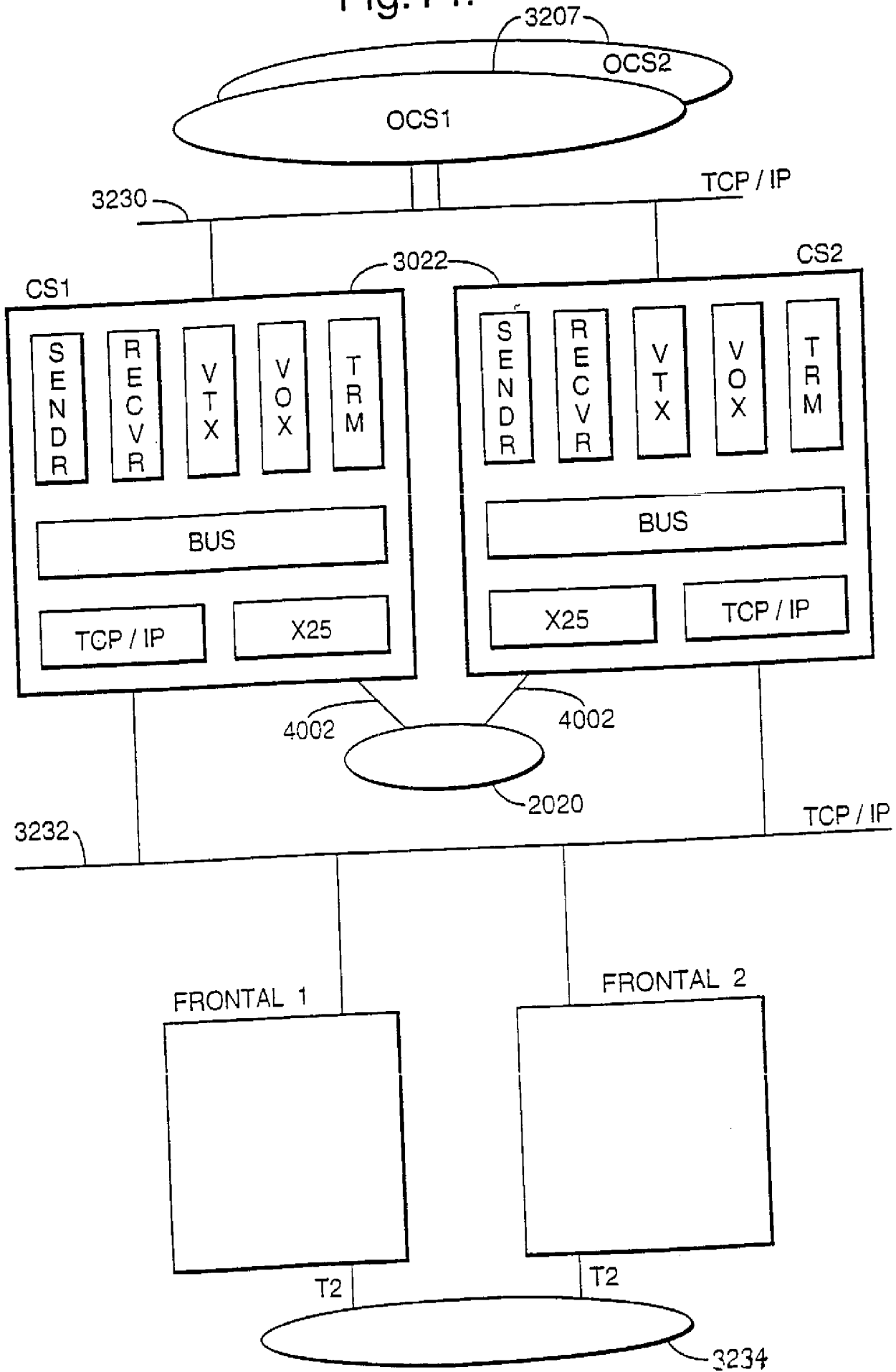


Fig.15.

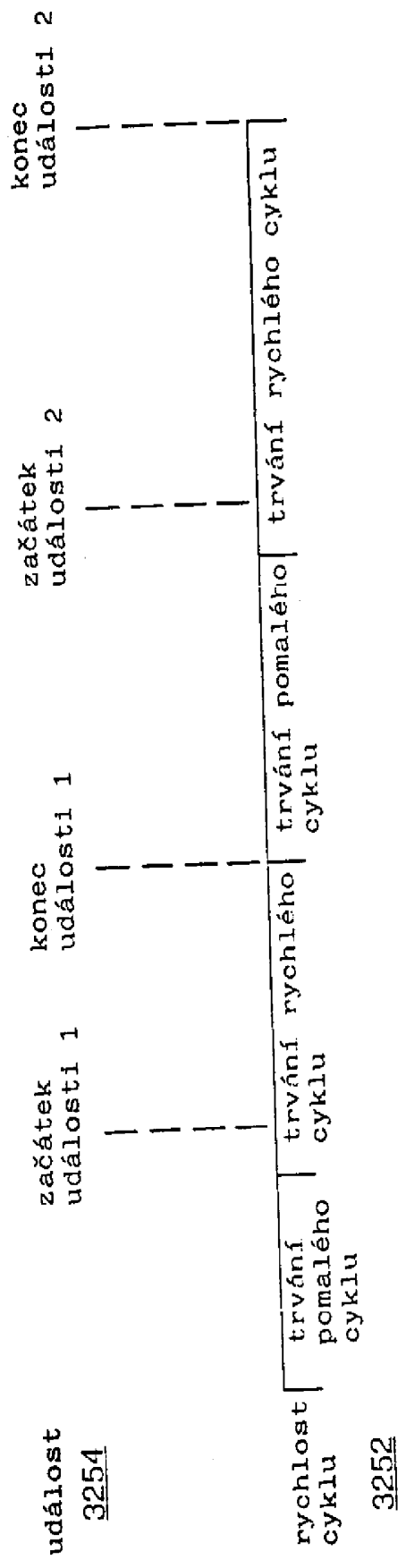


Fig.16.

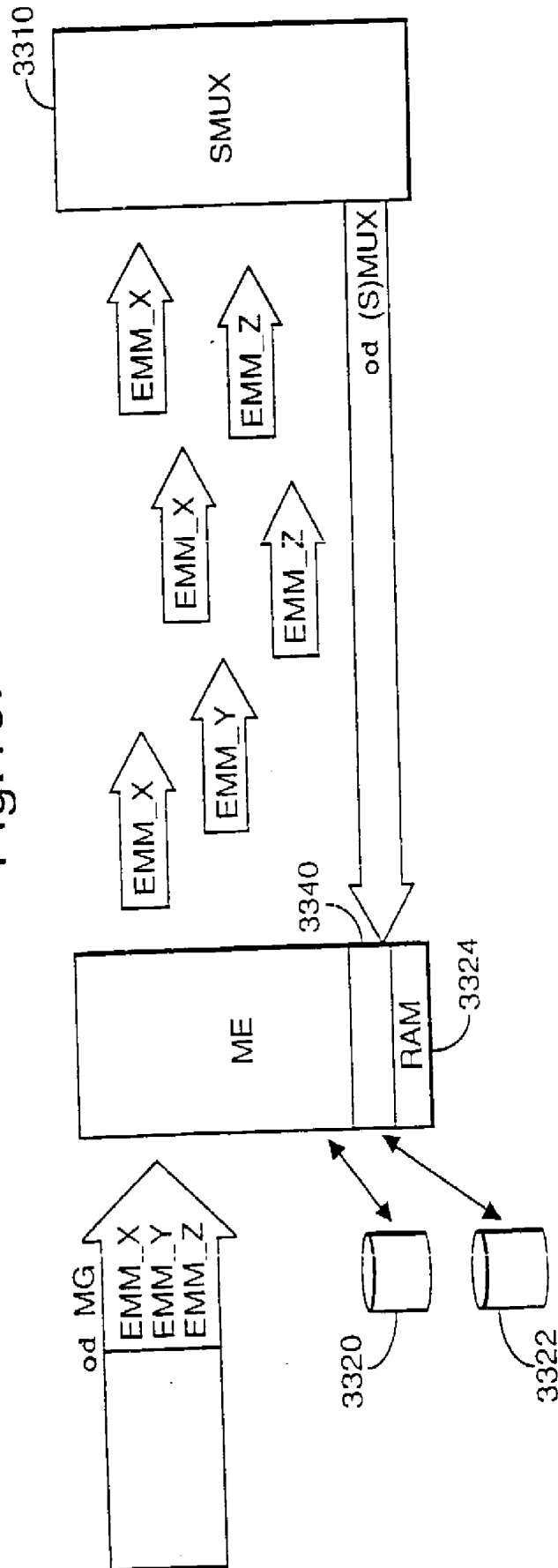


Fig.18.

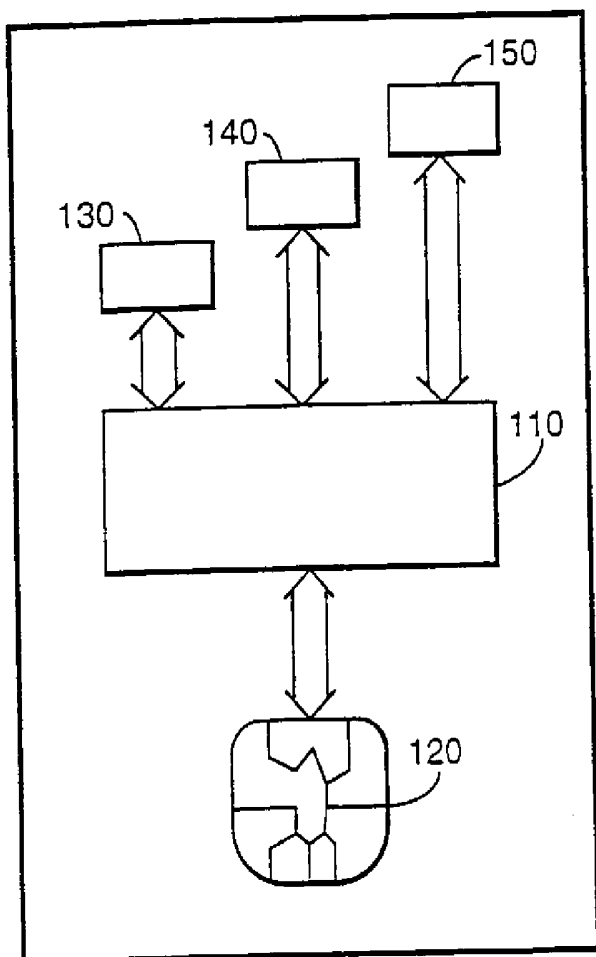


Fig.20.

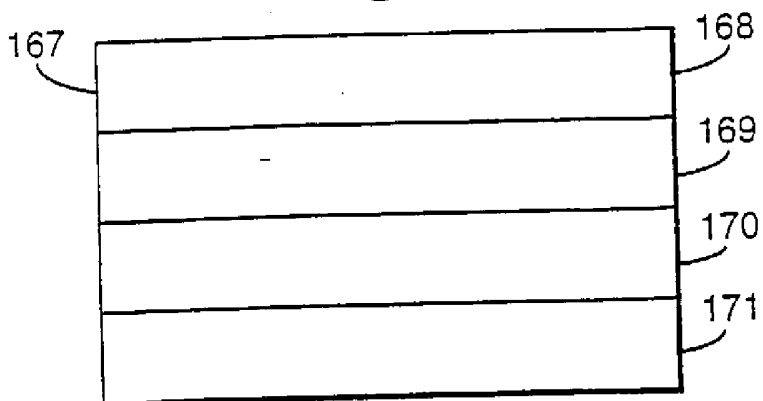


Fig.19.

151		
152		
153		
154		
155		
156		
1		157
1		159
2		
1		161
0		166
3		
1		163
1		165
N	ECM KLÍČ	DATA