P0303932

77.858/BT

KIVONAT

Terminál, ilyen terminállal ellátott adatterjesztő rendszer, és eljárás digitális adat továbbküldéséhez

Irdeto Access B.V., Hoofddorp, NL

A találmány tárgya terminál információ fogadásához és továbbküldéséhez. A terminálnak van első hálózati csatolója (31, 36) az elsődleges küldőtől (25, 26, 27) első hálózaton keresztül, első formátumban érkező kódolt, kulcs séma szerint titkosított információval ellátott elsődleges adatfolyam fogadásához. Van továbbá berendezése feljogosító üzenetek fogadásához, amelyek engedélyezik a felhatalmazott fogadót, hogy a titkosított adatfolyamot megfejtse. Végül van legalább egy további hálózati csatolója (37) a másodlagos hálózathoz (2) való csatlakozáshoz. A terminál úgy van beállítva, hogy az információ legalább egy részét legalább egy – az első formátumtól eltérő második formátumú - másodlagos adatfolyamban a második hálózaton (2) keresztül továbbküldje a második hálózathoz (2) csatlakozó legalább egy másodlagos terminálnak (3, 5, 6). A terminál ezután a másodlagos terminálnak (3, 5, 6) elküldi a másodlagos adafolyamo(ka)t - ugyanazon kulcs séma szerint titkosítva- , és továbbítja a fogadott feljogosító üzenetet, amely engedélyezi a felhatalmazott fogadót, hogy a második adatfolyamo(ka)t megfejtse.

A találmány tárgya továbbá digitális adat terjesztő rendszer, melynek van elsődleges hálózata és az elsődleges hálózathoz csatlakozó elsődleges adat küldője (25, 26, 27), amely úgy van kialakítva, hogy az elsődleges hálózaton keresztül kulcs sémának megfelelően titkosított elsődleges adatfolyamba kódolt információt küldjön. A rendszernek van továbbá feljogosító üzenet küldője (25, 26, 27). Ezeken kívül a rendszernek van másodlagos hálózata (2) és a másodlagos hálózathoz (2) csatlakozó egy vagy több másodlagos terminálja (3, 5, 6), valamint az első és a második (2) hálózathoz csatlakozó , fenti ismertetés szerinti elsődleges terminálja (1).

P0303932

77.858/BT

S. B. G. & K.
Szabadalmi Ügyvivői Iroda
H-1062 Budapest, Andrássy út 113.
Telefon: 461-1000, Fax: 461-1099

KÖZZÉTÉTELI PÉLDÁNY

A1

Terminál, ilyen terminállal ellátott adatterjesztő rendszer, és eljárás digitális adat továbbküldéséhez

Irdeto Access B.V., Hoofddorp, NL

A találmány hálózatok határain átnyúló vezérlés (transcontrol) területéhez kapcsolódik.

Részletesebben, a találmány tárgya terminál információ fogadásához és továbbküldéséhez, amely terminálnak van első hálózati csatolója az elsődleges küldőtől első hálózaton keresztül, első formátumban érkező kódolt, kulcs séma szerint titkosított információval ellátott elsődleges adatfolyam fogadásához,
berendezése feljogosító üzenetek fogadásához, amelyek engedélyezik a felhatalmazott fogadót, hogy a titkosított adatfolyamot megfejtse, valamint legalább egy további hálózati csatolója a másodlagos hálózathoz való csatlakozáshoz, ahol a terminál úgy van beállítva, hogy az információ legalább egy részét legalább egy – az első formátumtól eltérő második formátumú - másodlagos adatfolyamban a második hálózaton keresztül továbbküldje a második hálózathoz csatlakozó legalább egy másodlagos terminálnak.

A találmány tárgya továbbá digitális adatterjesztő rendszer, melynek van elsődleges hálózata, az elsődleges hálózathoz csatlakozó elsődleges adat küldője, amely úgy van kialakítva, hogy az elsődleges hálózaton keresztül kulcs sémának megfelelően titkosított elsődleges adatfolyamba kódolt információt küldjön,
feljogosító üzenet küldője, amely úgy van kialakítva, hogy olyan feljogosító üzeneteket küldjön, melyek felhatalmazzák az engedélyezett fogadót, hogy megfejtse a titkosított adatfolyamot,
másodlagos hálózata,

a másodlagos hálózathoz csatlakozó egy vagy több másodlagos terminálja, valamint az első és a második hálózathoz csatlakozó első terminálja, mely úgy van kialakítva, hogy az elsődleges adat küldőtől az első hálózaton keresztül fogadja a titkosított adatfolyamot, és az információ legalább egy részét legalább egy – az első formátumtól eltérő második formátumú - másodlagos adatfolyamba kódolva továbbítsa a második hálózathoz csatlakozó egy vagy több másodlagos terminálnak.

A találmány tárgya továbbá eljárás digitális adat fogadásához és továbbküldéséhez, mely eljárás során:
az elsődleges hálózaton keresztül fogadjuk az elsődleges küldőtől a kulcs séma szerint titkosított, első formátumú elsődleges adatfolyamba kódolt információt,
fogadjuk a feljogosító üzeneteket, amelyek felhatalmazzák ez engedélyezett fogadót, hogy megfejtse a titkosított adatfolyamot,
az információ legalább egy részét legalább egy – az első formátumtól eltérő második formátumú - másodlagos adatfolyamba kódolva a második hálózaton keresztül továbbítjuk legalább egy másodlagos terminálnak.

A találmány tárgya továbbá számítógép program, mely digitális adat fogadásához és továbbküldéséhez betölthető olyan terminálba, amelynek van
processzora, memóriája, első hálózati csatolója az első hálózaton keresztül első formátumban az elsődleges küldőtől érkező adatfolyam fogadásához, berendezése olyan feljogosító üzenetek fogadásához, melyek felhatalmazzák az engedélyezett fogadót, hogy megfejtsen egy titkosított adatfolyamot, valamint legalább egy további hálózati csatolója a másodlagos hálózathoz való csatlakozáshoz.

Ilyen terminál, rendszert és eljárás ismeretes például az EP-A-1 089 470 sz. szabadalmi leírásból is. Ez a bejelentés olyan beltéri egységet (set-top box) ismertet, amely videó kábellel és IEEE (Institute of Electrical & Electronics Engineers) 1394-es kábellel van a tévékészülékhez csatlakoztatva. A fogadó áramkör (front end circuit) az antennából származó DSS (Direct Satellite System, közvetlen műholdas rendszer) bemenetből kinyeri a felhasználó által kiválasztott csatorna műsor jelét és továbbítja azt a dekódoló (descrambler) áramkörnek. A dekódoló áramkört a töltőáramkör látja el a kód

megfejtéséhez szükséges dekódoló kulccsal. A többcsatornás szerkesztő (multiplex editing) áramkör a dekódoló áramkörből érkező MPEG (Motion Picture Experts Group) kódolású félduplex (Half Duplex, HD) műsorjel időbélyegét és csomaghosszúságát átszervezi az IEEE 1394 szabvány által meghatározott átviteli folyam struktúrájának megfelelően, majd továbbítja a titkosító áramkörnek. Fizetős műsor jel vételekor a titkosító áramkör titkosítja a többcsatornás szerkesztő áramkörtől érkező folyamot. A vezérlő meghajtót vezérel a mágneslemezre, optikai lemezre, mágneses-optikai lemezre, vagy félvezető memóriára rögzített vezérlő program kiolvasásához. A vezérlő program így kiolvasás, a felhasználó által kiadott utasítás beolvasása, vagy hasonló alapján vezérli a beltéri egység minden áramkörét. A töltőáramkör és a titkosító áramkör nincs összekötve.

Az ismertetett terminál működésekor az elsődleges küldő adatküldő egysége attól a pillanattól kezdve, hogy az adatot megfejtik az elsődleges terminálban, nem képes már a terjesztést vezérelni. Ebből következően ez az egység már nem képes vezérelni az adathoz való hozzáférést, még akkor sem, ha a megfejtett adatot újratitkosítják. Az elsődleges terminál üzemeltetője, amely az adatokat a másodlagos hálózaton keresztül fogadja és továbbítja, az adatfolyam újratitkosításához szükséges kulcs elküldésével meghatározhatja, melyik másodlagos fogadóknak engedélyezi az újratitkosított adatfolyam megfejtését.

A találmány fent ismertetett terminált, rendszert, és eljárást biztosít, melyek a digitális adat elsődleges szolgáltatójának lehetővé teszik, hogy megtartsák a másodlagos hálózatokon keresztül továbbított adatok feletti vezérlést.

A találmány ezt úgy éri el, hogy terminált biztosít információ fogadásához és továbbításához, amelynek van első hálózati csatolója az elsődleges küldőtől első hálózaton keresztül, első formátumban érkező kódolt, kulcs séma szerint titkosított információval ellátott elsődleges adatfolyam fogadásához,
berendezése feljogosító üzenetek fogadásához, amelyek engedélyezik a felhatalmazott fogadót, hogy a titkosított adatfolyamot megfejtse, valamint legalább egy további hálózati csatolója a másodlagos hálózathoz való csatlakozáshoz, ahol a terminál úgy

van beállítva, hogy az információ legalább egy részét legalább egy – az első formátumtól eltérő második formátumú - másodlagos adatfolyamban a második hálózaton keresztül továbbítsa a második hálózathoz csatlakozó legalább egy másodlagos terminálnak, ahol a terminál úgy van beállítva, hogy a másodlagos terminálnak küldje el a másodlagos adatfolyamo(ka)t - ugyanazon kulcs séma szerint titkosítva - , és továbbküldje a fogadott feljogosító üzenetet, amely engedélyezi a felhatalmazott fogadót, hogy a második adatfolyamo(ka)t megfejtse.

Az elsődleges adatszolgáltató - azzal, hogy feljogosító üzenetek (azaz a terminál részére információt biztosító forrás által generált üzenetek) továbbításával engedélyezi a másodlagos fogadók számára, hogy azok megfejtsék a továbbküldött adatfolyamot - mindvégig kézben tartja az adat további terjesztését.

Ideális esetben a terminál úgy van kialakítva, hogy megfejtse a fogadott elsődleges adatfolyamot és a kulcs sémának megfelelően titkosítsa a másodlagos adatfolyamo(ka)t.

Így a terminál hozzáférhet a fogadott adatfolyamban lévő adathoz, például egy multiplexált folyam bizonyos elemi folyamaihoz. Ezáltal hozzáférhet az információhoz, például az elemi folyamokat azonosító azonosítókat tartalmazó táblákhoz, amelyek alapján eldöntheti, hogy a fogadott adatfolyam mely részeit továbbítsa.

A találmány egy másik szempont szerint digitális adattovábbító hálózatot biztosít, melynek van elsődleges hálózata, az elsődleges hálózathoz csatlakozó elsődleges adat küldője, amely úgy van kialakítva, hogy az elsődleges hálózaton keresztül a kulcs sémának megfelelően titkosított elsődleges adatfolyamba kódolt információt küldjön,
feljogosító üzenet küldője, amely úgy van kialakítva, hogy olyan feljogosító üzeneteket küldjön, melyek felhatalmazzák az engedélyezett fogadót, hogy megfejtse a titkosított adatfolyamot,
másodlagos hálózata,
a másodlagos hálózathoz csatlakozó egy vagy több másodlagos terminálja, valamint

az első és a második hálózathoz csatlakozó elsődleges terminálja, mely úgy van kialakítva, hogy az elsődleges adat küldőtől az első hálózaton keresztül fogadja a titkosított adatfolyamot, és az információ legalább egy részét legalább egy – az első formátumtól eltérő második formátumú - másodlagos adatfolyamba kódolva továbbküldje a második hálózathoz csatlakozó egy vagy több másodlagos terminálnak, ahol az elsődleges terminál úgy van beállítva, hogy a második terminál(ok)nak elküldje az ugyanazon kulcs séma szerint titkosított másodlagos adatfolyamot és továbbítsa azokat a fogadott feljogosító üzeneteket, amelyek felhatalmazzák az engedélyezett fogadót, hogy megfejtse a második adatfolyamot.

A rendszer az elsődleges adat küldőt használó egység számára lehetővé teszi, hogy a másodlagos terminál(ok)nak továbbküldött adat feletti vezérlést végig megtartsa.

A találmány egy másik szempont szerint eljárást biztosít digitális adat fogadásához és továbbküldéséhez, mely eljárás során:
az elsődleges hálózaton keresztül fogadjuk az elsődleges küldőtől a kulcs séma szerint titkosított, első formátumú elsődleges adatfolyamba kódolt információt,
fogadjuk a feljogosító üzeneteket, amelyek felhatalmazzák ez engedélyezett fogadót, hogy megfejtse a titkosított adatfolyamot,
az információ legalább egy részét legalább egy – az első formátumtól eltérő második formátumú - másodlagos adatfolyamba kódolva a második hálózaton keresztül továbbítjuk legalább egy másodlagos terminálnak, ahol a másodlagos adatfolyam(ok)at ugyanazon kulcs séma szerint titkosítjuk és azokat az üzeneteket, amelyek felhatalmazzák az engedélyezett fogadót, hogy megfejtsék a titkosított másodlagos adatfolyamo(ka)t, továbbítjuk a másodlagos terminál(ok)nak.

A találmány szerinti terminál ezt az eljárást valósítja meg.

A találmány az utolsó szempont szerint számítógép programot biztosít, mely digitális adat fogadásához és továbbküldéséhez betölthető egy terminálba, amelynek van processzora, memóriája, első hálózati csatolója az első hálózaton keresztül első formátumban az elsődleges küldőtől érkező adatfolyam fogadásához, berendezése

olyan feljogosító üzenetek fogadásához, melyek felhatalmazzák az engedélyezett fogadót, hogy megfejtsen egy titkosított adatfolyamot, valamint legalább egy további hálózati csatolója a másodlagos hálózathoz való csatlakozáshoz, ezáltal az így felprogramozott terminál el van látva az 1-12. igénypontok bármelyike szerinti terminál funkciókkal.

Így a megfelelő hardverrel ellátott terminál könnyen átalakítható a találmány szerinti terminál funkcióinak megfelelő működéshez, nagyobb biztonsággal biztosítva a tartalomszolgáltatókat arról, hogy mindvégig kézben tartják a tartalom végfelhasználóig történő terjesztése feletti vezérlést.

A találmányt a következőkben a mellékelt ábrákra való hivatkozással részletesen ismertetjük, ahol az

1. ábra annak a digitális adatterjesztő architektúrának a sematikus rajza, amelyben a találmányt megvalósítjuk, a
2. ábra az Átviteli Folyam Csomagok összetételét mutató sematikus rajz, a
3. ábra a találmány szerinti terminál néhány összetevőjét mutató sematikus rajz, és a
4. ábra a találmány szerinti terminál által előállított adatcsomag összetételét mutató sematikus rajz.

Az 1. ábrának megfelelően a találmány 1 elsődleges fogadót biztosít, mely két hálózat között - ebben a példában a szállító hálózat és a 2 otthoni hálózat között - átjáróként funkcionál. Az 1 elsődleges fogadó az első formátumban fogadja az adatot és egy második formátumban küldi tovább. Annak ellenére, hogy a találmány nem korlátozódik egy fajta adattípusra, az ismertetés olyan példára szorítkozik, melyben MPEG-2 Átviteli Folyam csomagokat terjesztünk az 1 elsődleges fogadóig, amely a 2 otthoni hálózaton keresztül másodlagos fogadóknak küldi tovább a csomagokat. Az 1. ábrán látható példában másodlagos fogadó a 4 analóg televízióhoz kötött 3 beltéri egység, az 5 digitális televízió, és a hálózati kártyával, médialejátszóval és a 7 intelligens (smart) kártya olvasóval ellátott 6 számítógép. A találmány nem korlátozó-

dik csupán adatterjesztő környezetre, az 1 elsődleges fogadó a forrástól fogadhat digitális adatot pont-pont kapcsolaton keresztül is.

Az MPEG-2 szabványú ISO/IEC 13818 viszonylag részletesen ismerteti az adat kódolás és adatátvitel eljárását. Az alábbi leírás elsősorban azokat a szempontokat ismerteti, amelyek találmányhoz kapcsolódnak. A további részletek a szabványból megismerhetők.

Az 1. ábrán a 8 terjesztő forrás a 9 elemi folyamot egyszerű MPEG-2 csatorna 10 átviteli folyamába kódolja. Az elemi folyam egy csatorna, például video vagy audio jel egyszerű, digitálisan kódolt és esetleg MPEG eljárással tömörített összetevője. A csatornához tartozó különféle elemi folyamokból származó adatokat 11 PES (Program Elementary Stream, csatorna elemi folyam) csomagok formájában szállítjuk. A csatorna az analóg terjesztés egy csatornájának felel meg. A 11 PES csomagnak 12 PES csomag fejrésze és 13 PES csomag adatrésze (payload) van. Az elemi folyamokból származó adatokat 11 PES csomagokba multiplexáljuk és a 12 PES csomag fejrésszel jelöljük, hogy a 13 PES csomag adatrész melyik elemi folyamhoz tartozik.

A 11 PES csomagokat 14 MPEG-TS (Transport Stream, átviteli folyam) csomagokként szállítjuk (2. ábra). A 15 MPEG multiplexer (1. ábra) több átviteli folyamot multiplexál egy többcsatornás átviteli folyamba, így több csatornát egy folyamként szállítunk. Minden 14 TS csomagnak (2. ábra) 16 TS csomag fejrésze és 17 TS csomag adatrésze van. Ezen felül a 18 adaptációs mező biztosítja, hogy az összes 14 TS csomag ugyanolyan hosszúságú, függetlenül az általuk szállított 11 PES csomagok hosszától. A 16 TS csomag fejrésznek egyebek mellett 19 csomag azonosítója (Packet Idendifier, PID) van. A 19 csomag azonosító egy egyedi egész szám, melyet az egyszerű vagy többcsatornás átviteli folyam egy csatornájához tartozó elemi folyamok beazonosítására használunk.

A 0 PID értékű 14 TS csomagokban lévő program hozzárendelési tábla (Programme Association Table, PAT) az átviteli folyamban elérhető összes program listáját takarja.

A PAT-ben szereplő összes program a program leképezési táblához (Programme Map Table, PMT) van hozzárendelve, amely a programról és az őt alkotó elemi folyamokról szolgáltat részleteket.

Visszatérve az 1. ábrához, a 20 hálózati csatoló a 22 regionális központ számára átalakítja a 14 TS csomagokat a 21 elsődleges hálózaton keresztüli átvitelnek megfelelő formátumba. A regionális központ a 23 hálózati csatolón keresztül fogadja az átviteli folyamot. A 24 bitfolyam összeillesztő(splicer)/multiplexer arra szolgál, hogy más átviteli folyamokat, köztük szolgáltatás információt (Service Information, SI), elektronikus program ismertetőt (Electronic Program Guide, EPG), és teletextet szúrjon be. A 24 bitfolyam összeillesztő/multiplexer felülírja a PID értékeket, valamint a PMT-t és PAT-et is, hogy ne legyenek konfliktusban álló értékek. Az eredményként előálló MPEG átviteli folyamot a megfelelő 28 és 29 hálózati csatolók használatával ezután továbbítjuk a 25 műholdas küldőnek, a 26 földközeli küldőnek, vagy a 27 kábeles küldőnek.

A műholdas, földközeli vagy kábeles hálózatok szállító hálózatot alkotnak a fogadók otthonáig történő adatterjesztéshez. Más, például háztól-házig tartó optikai (Fiber to the home, FTTH), ADSL (Asyncronous Digital Subscriber Line, aszinkron digitális előfizetői vonal), vagy Ethernet kapcsolatokat alkalmazó hálózatok is igénybevehetők. A jelen találmány ismertetése során a szállító hálózatra, mint első hálózatra fogunk hivatkozni.

A 8 terjesztő forrás, a 22 regionális központ, vagy mindkettő használhat feltételes hozzáférésű rendszert a továbbított adatfolyam tartalmához való illetéktelen hozzáférés megelőzéséhez. E célból vagy a 13 PES csomag adatrészét, vagy a 17 TS csomag adatrészét titkosítjuk. Felhívjuk rá a figyelmet, hogy egy multiplexált átviteli folyamban, amelyben valójában több átviteli folyam van és mindegyük egy elemi folyamot szállít, az átviteli folyamoknak csak egy része titkosítható. A 12 PES csomag fejrész vagy a 16 TS csomag fejrész jelöli, hogy az adott csomag titkosított-e, vagy sem. Azért, hogy az ismertetés ne legyen túlságosan bonyolult, feltételezzük, hogy a titkosítást az átviteli folyam szintjén hajtjuk végre. A 17 TS csomag adatrészek

titkosításához ideális esetben szimmetrikus titkosító algoritmust, például DES-t (Data Encryption Standard) használunk.

Fontos, hogy a 17 TS csomag adatrészeket titkosíthatjuk ugyanazzal a kulccsal és/vagy algoritmussal a PID-értékektől függetlenül, illetve használhatunk különböző kulcsot és/vagy algoritmust is az egy csatornához tartozó elemi folyamok halmazának titkosításához. Feltételezve, hogy a 22 regionális központ egyben a hitelesítő központ (Certificate Authority, CA) is, be fog szúrni egy vagy több átviteli folyamot is, amelyek feljogosító üzeneteket tartalmaznak. Ezen felül módosítani fogja a titkosított csatornához tartozó PMT-t úgy, hogy a hozzáadja a csatornát a CA-leíróhoz, egyben meghatározva az alkalmazott CA rendszer típusát és a feljogosító üzenetek PID-jét. A feljogosítást vezérlő üzenetekben szerepel a vezérlő szó, valamint a titkosításhoz és megfejtéshez használt kulcs. Maguk a feljogosítást vezérlő üzenetek (Entitlement Control Message, ECM) is egy eltérő kulccsal titkosítottak. Egy másik adatfolyamban feljogosítást kezelő üzenetek (Entitlement Management Message, EMM) vannak, amelyek felhatalmazzák az engedélyezett előfizetőket vagy előfizetői csoportokat arra, hogy megfejtsék az ECM-eket, és azokból előhozzák a vezérlő szót.

Visszatérve az 1. ábra ismertetéséhez, az 1 elsődleges fogadó a hozzá kapcsolódó 30 parabola antennával fogadja az MPEG-2 átviteli folyamot. Az átviteli folyam olyan formátumban van, amely megfelel a műholdas szállító hálózaton keresztüli továbbításnak, például a DVB-S (Digital Video Broadcasting Satellite, digitális videojelet terjesztő műhold) formátumban. Az 1 elsődleges fogadó az adat részét vagy egészét a végberendezések számára a 2 otthoni hálózaton keresztül teszi elérhetővé, amelyen az adatot másfajta formátumban továbbítjuk. Az 1 elsődleges fogadó ezért szállító hálózati átjáró: olyan eszköz, amely egy vagy több szállító hálózathoz és egy vagy több hálózati szegmenshez van csatlakoztatva. Mivel egy vagy több csatlakozó összetevője van, bármely OSI (Open System Interconnection, nyílt rendszerek összekapcsolása) rétegben összekötheti a szállító hálózatot (azaz a műholdas hálózatot) az otthoni hálózati szegmensekkel. Működhet hídként vagy routerként, különböző kapcsolati réteg technológiákat összekötve, vagy átjáróként, az OSI 4. rétegének és felette lévő rétegeknek is nyújtva szolgáltatásait. Ebből következően a formátum

kifejezés arra a módra utal, ahogy az adatot hozzáigazítjuk az adott hálózat típusához tartozó protokollkészlethez. Az első hálózatnak (a műholdas hálózatnak) más protokollkészlete van, mint a 2 otthoni hálózatnak, azaz egy vagy több kapcsolati rétegben, hálózati rétegben, vagy szállítási rétegben különbözik tőle. Megjegyezzük, hogy ez azt jelenti, hogy az 1 elsődleges fogadónak ott, ahol az adat küldése keretekben és/vagy csomagokban történik, hozzá kell adnia, el kell távolítania, vagy módosítania kell a csomag fejrészeket, és/vagy újra kell osztania a csomag adatrészeket, hogy azok a 2 otthoni hálózat protokoll készletének megfeleljenek. A csomag kifejezés az adat egy kis részére utal, amelyet a kommunikációs hálózaton egy egységként továbbítunk. A csomag a hálózati réteg alatti rétegek csomagjait, szokásos nevükön kereteket, valamint cellákat tartalmaz. A csomagnak fejrésze vagy felvezető része (trailer), és adat része van. A csomagformátum a csomag összetételére utal, amelyet az adatrész mérete és a fejrészben/felvezető részben lévő különféle mezők határoznak meg.

A 3. ábra az 1 elsődleges fogadó összetevőinek sematikus rajza. A fogadónak van 31 tunere/demodulátora, amely eltávolítja a vivőhullámot az MPEG átviteli folyamot tartalmazó alapsáv jel előhozásához. Az 1 elsődleges fogadó a 32 processzort és a 33 memóriát használja a csomagok feldolgozásához. A 32 processzor a 34 buszhoz csatlakozik. Ebben a példában a 34 buszhoz csatlakozik a 35 intelligens kártya olvasó, a 36 modem, és a 37 Ethernet kártya is. A 36 modem és a 37 Ethernet kártya hálózati csatolóként funkcionál, azaz a processzoron futó megfelelő szoftverrel együtt kapcsolati réteget valósítanak meg, amely lehetővé teszi az adott hálózaton keresztüli, annak protokolljának megfelelő adatcserét. A 38 intelligens kártyát a 35 intelligens kártya olvasóba helyezzük egy vagy több csatorna fogadásának engedélyezéséhez. A 38 intelligens kártya helyett használhatunk más hordozható biztonsági eszközt, például USB (Universal Serial Bus, univerzális soros busz) eszközt (dongle) vagy PCMCIA (Personal Computer Memory Card International Association, személyi számítógép memória kártya nemzetközi szervezet) kártyát is. Az engedélyezés elképzelhető szoftverrel implementált biztonsági egységgel is. Ebben a példában a 2 otthoni hálózat Ethernet hálózat, azaz a 3 beltéri egységnek, az 5 digitális televíziónak, és a 6 számítógépnek is van Ethernet hálózati kártyája. Hangsúlyozzuk azonban, hogy

másfajta otthoni hálózat is elképzelhető, például olyan, amely USB csatlakozókkal, IEEE 1394, IEEE 802.11, vagy más típusú csatlakozókkal van kialakítva.

A találmánynak megfelelően az 1 elsődleges fogadó az átviteli folyamot DVB-S formátumban fogadja. Ezután, a PAT-ben és a PMT-ben lévő PID-ek használatával eldönti, hogy mely elemi folyamok tartalmazzák az EMM-eket és az ECM-eket, és mely elemi folyamokban vannak a tartalmat jelentő adatok, EPG adatok, esetleg IP (Internet Protocol, internetes protokoll) adatok, stb. Az utóbbit tartalmazó átviteli folyamok részét vagy egészét megfejtjük, ha a 38 intelligens kártyán van olyan információ, amely az 1 elsődleges fogadónak engedélyezi a megfelelő vezérlő szó előhozatalát. E célból a 38 intelligens kártya feldolgozza az ECM-eket, hogy továbbíthassa a vezérlő szót a megfejtést végrehajtó 32 processzornak.

Ezután a megfejtett adatfolyamok csomagjai újraütemezzük. Ez azt jelenti, hogy a csomagokat megfelelően hosszú részekre osztjuk és a szükséges fejrészeket – amelyeket a 2 otthoni hálózatban használt protokollok határoznak meg – hozzáadjuk. Ezeket a csomagokat ezután újratitkosítjuk. Ugyanazokat a vezérlő szavakat használjuk a 2 otthoni hálózat adatcsomag formátumában lévő csomagok újratitkosításához. Mivel ugyanazt a kulcs sémát használjuk, a feljogosító üzeneteket tartalmazó átviteli folyamokban lévő adatokat egyszerűen továbbítjuk. Nem alkotunk újabb feljogosító üzeneteket.

Megjegyezzük, hogy az 1 elsődleges fogadó nem különbözik lényegesen a másodlagos fogadóktól, abban az értelemben, hogy a 38 intelligens kártya nélkül nem képes a feljogosító üzeneteket vagy a tartalom adatokat megfejteni. Nem képes arra sem, hogy saját feljogosító üzeneteket alkosson. Ebből két előny származik, először is az, hogy az 1 elsődleges fogadó viszonylag egyszerű, másodszor pedig az, hogy a regionális központ biztos lehet abban, hogy a CA rendszere végig megfelelően védi a tartalom adatokat az illetéktelen hozzáféréstől.

Az 1 elsődleges fogadó újraütemezi a 14 TS csomagokat a 2 otthoni hálózat formátumának megfelelően. Ebben a példában az otthoni hálózat protokollkészlete

Ethernetet használ a kapcsolati rétegben, IP-t a hálózati rétegben és UDP-t (User Datagram Protocol, felhasználói adatcsomag protokoll) a szállítási rétegben. A 4. ábra a 2 otthoni hálózaton keresztül továbbított csomagok összetételét mutatja. Néhány, körülbelül hét 14 TS csomag alkotja egy 39 IP csomag (vagy IP datagram) adatrészét. A 39 IP csomagnak van továbbá 40 UDP fejrésze és 41 IP fejrésze. A 41 IP fejrészben a 39 IP csomag címzettjét jelentő másodlagos fogadónak az IP címe vagy csoportcím van. A 39 IP csomag egy 42 Ethernet keret adatrészét alkotja, amelyben 43 szinkronizációs jelsorozat (preamble), a 44 célállomás cím, a 45 forrás cím, a 46 típus, és a 47 CRC (Cyclic Redundancy Code, ciklikus redundáns kódolás) ellenőrző összeg van. A 44 célállomás cím üzenetszórás, csoportos címzés, vagy egyedi címzés típusú cím, amelyet a másodlagos fogadók használnak a nekik szánt Ethernet keretek előhozásához. Megjegyezzük, hogy lehetséges lett volna az is, hogy a 14 TS csomagokat közvetlenül a 42 Ethernet keretekbe ágyazzuk, anélkül, hogy 41 IP és 42 UDP fejrészeket adunk hozzá. Azonban az IP Ethernet feletti használata lehetővé teszi, hogy az adatot szélesebb körben terjeszthessük.

Ideális esetben az 1 elsődleges fogadó a titkosítás valamilyen formáját használja a protokollkészlet mellett, ahogyan azt a szabadalmaztató WO 02/07378 sz. nemzetközi beadványa részletesen ismerteti.

A találmány egy előnyben részesített megvalósításában a másodlagos fogadók képesek arra, hogy a 2 otthoni hálózaton keresztül kiválasztási utasításokat küldjenek az 1 elsődleges fogadónak. Az 1 elsődleges fogadó a kiválasztási utasítások hatására kiszűri a többcsatornás átviteli folyam azon elemi folyamait, amelyeket egyik másodlagos fogadó sem kért. Így képes arra is, hogy az egyes másodlagos fogadóknak az elemi folyamok csak egy részhalmazát küldje el.

A másodlagos fogadók mindegyikének van intelligens kártya olvasója is. Az olvasóba helyezett intelligens kártya engedélyezi őket arra, hogy az 1 elsődleges fogadótól kapott adatfolyamból előhozhassák az ECM-eket és megfejthessenek bizonyos elemi folyamokat.

Az 1 elsődleges fogadó a 36 modem használatával is fogadhat TS csomagokat. Ebben az esetben a TS csomagok már lehetnek IP csomagokba ágyazva. Ahelyett azonban, hogy Ethernet keretekbe lennének ágyazva, a fogadott IP csomagok tipikusan PPP (Point-to-Point Protocol, pont-pont közötti protokoll) csomagok vagy ATM (Asynchronous Transfer Mode,, aszinkron Átviteli Mód) cellák formájában érkeznek a kapcsolati réteg szintjén. Az 1 elsődleges fogadónak ezért a találmány szerinti eljárást kell végrehajtania, hogy a fogadott adatokat Ethernet keretformátumban küldhesse tovább.

Ahogyan az a korábbi ismertetésből is kiderült, az 1 elsődleges fogadó újraütemezi a megfejtett adatfolyamok csomagjait. A találmány lényegétől való eltérés nélkül elképzelhető az 1 elsődleges fogadó más változata is. Ebben a változatban az 1 elsődleges fogadó úgy van kialakítva, hogy fogadja az első formátumban kódolt információt tartalmazó elsődleges adatfolyamot, második formátumban újrakódolja az információt, és az újrakódolt információt tartalmazó adatot legalább az egyik másodlagos adatfolyamba beletegye. Ez az úgynevezett átkódolás a fogadott adat kitömörítésével és újratömörítésével is együtt járhat. Az 1 elsődleges fogadó például felbonthatja az átviteli folyamot az MPEG-4 szabvány szerint kódolt és tömörített elemi csatorna folyam előhozásához, kitömörítheti a kódolt videó adatot, és MPEG-2 szabványnak megfelelően újratömörítheti és kódolhatja a videó adatot. Az átkódolt videó adatot ezután más, audio és videó adatot tartalmazó elemi csatorna folyamokkal együtt átviteli folyamba multiplexálja, melyet ezután csomagokra osztja és elküldi egy vagy több másodlagos fogadónak. Természetesen az MPEG-4-ről MPEG-2-re történő átkódolás csak egy előnyös példa. Ahol adatot küldünk tovább, ott az 1 elsődleges fogadó kialakítható úgy is, hogy állóképeket kódoljon át, például JPEG (Joint Photograpics Experts Group) képeket GIF (Graphic Interchange Format) képekké. Ezek a megvalósítások előnyösek, mert lehetővé teszik a szokásos fogadók másodlagos fogadókként történő használatát, ha az adat terjesztő olyan formátumot kezd használni, amelyet a másodlagos fogadók nem támogatnak. Ebben az esetben csak az 1 elsődleges fogadót kell kicserélni. Elsősorban az újratömörítésből adódik a másik előny, hogy figyelembe vehető a 2 otthoni hálózaton és a szállító hálózaton rendelkezésre álló sávszélesség.

Ideális esetben az elsődleges adatfolyam szolgáltatóját ellátjuk még egy eszközzel az információ másodlagos terjesztésének vezérléséhez. Ennek egyik módja az, hogy különböző feljogosító üzeneteket biztosítunk, amelyek felhatalmaznak egy engedélyezett fogadót arra, hogy a kulcs séma szerint titkosított adatfolyamot megfejtsen, ez esetben minden feljogosító üzenetben legalább egy terminál specifikációja van. Más szavakkal, a 8 terjesztő forrás által az 1 elsődleges fogadónak küldött ECM-ek közül néhányban ugyanaz a vezérlő szó van, de a fogadó specifikációja (a típusa, illetve egy vagy több eszközének azonosítója) különbözik. Az elsődleges fogadó előhozza az őt címző ECM-eket, hogy megfejtse a fogadott adatfolyamot. A másodlagos fogadóknak csak azokat az ECM-eket továbbítja, amelyek a másodlagos fogadókra illő specifikációkat tartalmaznak.

A terjesztés vezérlésének másik eszköze olyan üzeneteket küld, amelyek engedélyezik a legalább egy másodlagos adatfolyam legalább egy másodlagos terminálnak való küldését. Az üzenet lehet egyszerű üzenet, amely csak azt határozza meg, hogy a továbbküldés engedélyezve van-e vagy sem, illetve korlátozhatja a másodlagos fogadók egy adott típusának vagy egy adott maximális számának való továbbküldést. Az 1 elsődleges fogadó úgy van kialakítva, hogy a másodlagos adatfolyamokat csak azoknak a másodlagos fogadóknak továbbítsa, melyekre megérkezett az engedély. Az eszköz-specifikus ECM-ek használatával kombinálva az 1 elsődleges fogadó például kiszűrhet bizonyos ECM-eket, hogy korlátozza azon másodlagos fogadók számát, melyek egy időben hozzáférhetnek az adathoz.

A találmány nem korlátozódik az ismertetett megvalósításokra, a csatolt igénypontok lényegétől való eltérés nélkül számos módon változtatható. Például a titkosított adatban lehetnek IP csomagok. Ebben az esetben az 1 elsődleges fogadó az adat továbbküldése előtt eltávolíthatja a TS csomagokba ágyazott csomagokat.

Szabadalmi igénypontok

1. Terminál információ fogadásához és továbbküldéséhez, amelynek van első hálózati csatolója (31, 36) az elsődleges küldőtől (25, 26, 27) első hálózaton keresztül, első formátumban érkező kódolt, kulcs séma szerint titkosított információval ellátott elsődleges adatfolyam fogadásához,
berendezése feljogosító üzenetek fogadásához, amelyek engedélyezik a felhatalmazott fogadót, hogy a titkosított adatfolyamot megfejtse, valamint legalább egy további hálózati csatolója (37) a másodlagos hálózathoz (2) való csatlakozáshoz, azzal jellemezve, hogy a terminál úgy van beállítva, hogy az információ legalább egy részét legalább egy – az első formátumtól eltérő második formátumú - másodlagos adatfolyamban a második hálózaton (2) keresztül továbbküldje a második hálózathoz (2) csatlakozó legalább egy másodlagos terminálnak (3, 5, 6), továbbá azzal, hogy a terminál úgy van beállítva, hogy a másodlagos terminálnak (3, 5, 6) küldje el a másodlagos adafolyamo(ka)t - ugyanazon kulcs séma szerint titkosítva- , és továbbítsa a fogadott feljogosító üzenetet, amely engedélyezi a felhatalmazott fogadót, hogy a második adatfolyamo(ka)t megfejtse.

2. Az 1. igénypont szerinti terminál, azzal jellemezve, hogy a terminál úgy van kialakítva, hogy a kulcs séma alapján megfejtse a fogadott elsődleges adatfolyamot és titkosítsa a másodlagos adatfolyamo(ka)t.

3. A 2. igénypont szerinti terminál, azzal jellemezve, hogy a terminál úgy van kialakítva, hogy felbontsa (demultiplexálja, de-multiplex) a több elemi adatfolyamból álló megfejtett adatfolyamot és továbbküldje az elemi adatfolyamok egy részhalmazában kódolt információt.

4. A 3. igénypont szerinti terminál, azzal jellemezve, hogy a terminál úgy van kialakítva, hogy kiválasztási utasításokat fogadjon a másodlagos terminálóktól és a kiválasztási utasításoknak megfelelően válassza ki a részhalmazból az elemi adatfolyamokat.

5. Az 1-4. igénypontok bármelyike szerinti terminál, azzal jellemezve, hogy a terminál úgy van kialakítva, hogy a titkosított elsődleges adatfolyamot első adatcsomag formátumban fogadja és a másodlagos adatfolyamok legalább egyikét második adatcsomag formátumban küldje el.

6. Az 1-4. és 5. igénypontok bármelyike szerinti terminál, azzal jellemezve, hogy a terminál úgy van kialakítva, hogy az első adatcsomag formátumban fogadott titkosított adatcsomag (14, 39, 42) egy adatrészét (13, 17) fejti meg egyszerre, hogy a megfejtett adatrészből tiszta adatot nyerjen ki és azt utána újracsomagolja a második adatcsomag formátumnak megfelelően.

7. A 2. igénypont vagy a 2. és az 5. vagy 6. igénypont szerinti terminál, azzal jellemezve, hogy a terminál úgy van kialakítva, hogy felbontsa a több titkosított elemi adatfolyamból álló titkosított adatfolyamot és továbbküldje az elemi adatfolyamok egy részhalmazát.

8. Az 1-7. igénypontok bármelyike szerinti terminál, azzal jellemezve, hogy a terminál úgy van kialakítva, hogy az általuk elküldött második adatfolyam(ok)nak legyen egy vagy több címük (44), melyek egy vagy több másodlagos terminált (3, 5, 6) azonosítanak.

9. Az 1-8. igénypontok bármelyike szerinti terminál, azzal jellemezve, hogy a terminál úgy van kialakítva, hogy fogadja az első formátumban kódolt információval ellátott első adatfolyamot, újrakódolja az információt a második formátumnak megfelelően, és az újrakódolt információt a másodlagos adatfolyamok legalább egyikébe foglalja.

10. A 9. igénypont szerinti terminál, azzal jellemezve, hogy a terminál úgy van kialakítva, hogy fogadja az első sémának megfelelően tömörített adattal ellátott első adatfolyamot, kibontsa az adatot, és az újratömörített adatot a másodlagos adatfolyamok legalább egyikébe foglalja.

11. Az 1-10. igénypontok bármelyike szerinti terminál, amely úgy van kialakítva, hogy üzeneteket fogadjon, melyek engedélyezik a másodlagos adatfolyamok legalább egyikének legalább egy másodlagos terminálhoz (3, 5, 6) való küldését, és csak azokat a másodlagos adatfolyamokat küldje el az adott másodlagos terminálóknak (3, 5, 6), amelyekre az engedélyezés megérkezett.

12. Az 1-11. igénypontok bármelyike szerinti terminál, melynek van berendezése a különböző feljogosító üzenetek fogadásához, melyek mindegyike egy engedélyezett fogadót hatalmaz fel arra, hogy megfejtsen egy - a kulcs séma szerint rejtjelezett - titkosított adatfolyamot, és ahol az egyes feljogosító üzeneteknek van legalább egy terminált meghatározó specifikációjuk, azzal jellemezve, hogy a terminál úgy van kialakítva, hogy csak azokat a feljogosító üzeneteket továbbítsa a másodlagos terminál (3, 5, 6), amelyek megfelelnek a feljogosító üzenetben lévő specifikációnak.

13. Digitális adat terjesztő rendszer, melynek van elsődleges hálózata, az elsődleges hálózathoz csatlakozó elsődleges adat küldője (25, 26, 27), amely úgy van kialakítva, hogy az elsődleges hálózaton keresztül kulcs sémának megfelelően titkosított elsődleges adatfolyamba kódolt információt küldjön,
feljogosító üzenet küldője (25, 26, 27), amely úgy van kialakítva, hogy olyan feljogosító üzeneteket küldjön, melyek felhatalmazzák az engedélyezett fogadót, hogy megfejtse a titkosított adatfolyamot,
másodlagos hálózata (2),
a másodlagos hálózathoz (2) csatlakozó egy vagy több másodlagos terminálja (3, 5, 6), valamint
az első és a második (2) hálózathoz csatlakozó elsődleges terminálja (1), mely úgy van kialakítva, hogy az elsődleges adat küldőtől (25, 26, 27) az első hálózaton keresztül fogadja a titkosított adatfolyamot, és az információ legalább egy részét legalább egy – az első formátumtól eltérő második formátumú - másodlagos adatfolyamba kódolva továbbítsa a második hálózathoz (2) csatlakozó egy vagy több másodlagos terminálnak (3, 5, 6),
azzal jellemezve, hogy az elsődleges terminál (1) úgy van beállítva, hogy a második terminál(ok)nak elküldje az ugyanazon kulcs séma szerint titkosított másodlagos

adatfolyamot és továbbítsa azokat a fogadott feljogosító üzeneteket, amelyek felhatalmazzák az engedélyezett fogadót, hogy megfejtse a második adatfolyamot.

14. Eljárás digitális adat fogadásához és továbbküldéséhez, mely eljárás során:
az elsődleges hálózaton keresztül fogadjuk az elsődleges küldőtől a kulcs séma szerint titkosított, első formátumú elsődleges adatfolyamba kódolt információt (25, 26, 27),
fogadjuk a feljogosító üzeneteket, amelyek felhatalmazzák ez engedélyezett fogadót, hogy megfejtse a titkosított adatfolyamot,
az információ legalább egy részét legalább egy – az első formátumtól eltérő második formátumú - másodlagos adatfolyamba kódolva a második hálózaton (2) keresztül továbbítjuk legalább egy másodlagos terminálnak (3, 5, 6), ahol a másodlagos adatfolyam(ok)at ugyanazon kulcs séma szerint titkosítjuk és azokat az üzeneteket, amelyek felhatalmazzák az engedélyezett fogadót, hogy megfejtsék a titkosított másodlagos adatfolyamo(ka)t, továbbítjuk a másodlagos terminál(ok)nak (3, 5, 6).

15. Számítógép program, mely digitális adat fogadásához és továbbküldéséhez betölthető olyan terminálba (1), amelynek van
processzora (32), memóriája (33), első hálózati csatolója (31, 36) az első hálózaton keresztül első formátumban az elsődleges küldőtől (25, 26, 27) érkező adatfolyam fogadásához, berendezése olyan feljogosító üzenetek fogadásához, melyek felhatalmazzák az engedélyezett fogadót, hogy megfejtsen egy titkosított adatfolyamot, valamint legalább egy további hálózati csatolója (37) a másodlagos hálózathoz (2) való csatlakozáshoz, ezáltal az így felprogramozott terminál (1) el van látva az 1-12. igénypontok bármelyike szerinti terminál funkciókkal.

A meghatalmazott

Dr. Bokor Tamás
szabadalmi ügyvivő
az S.B.G. & K. Szabadalmi Ügyvivői Iroda
tagja
H-1062 Budapest, Andrássy út 113.
Telefon: 461-1000 Fax: 461-1099

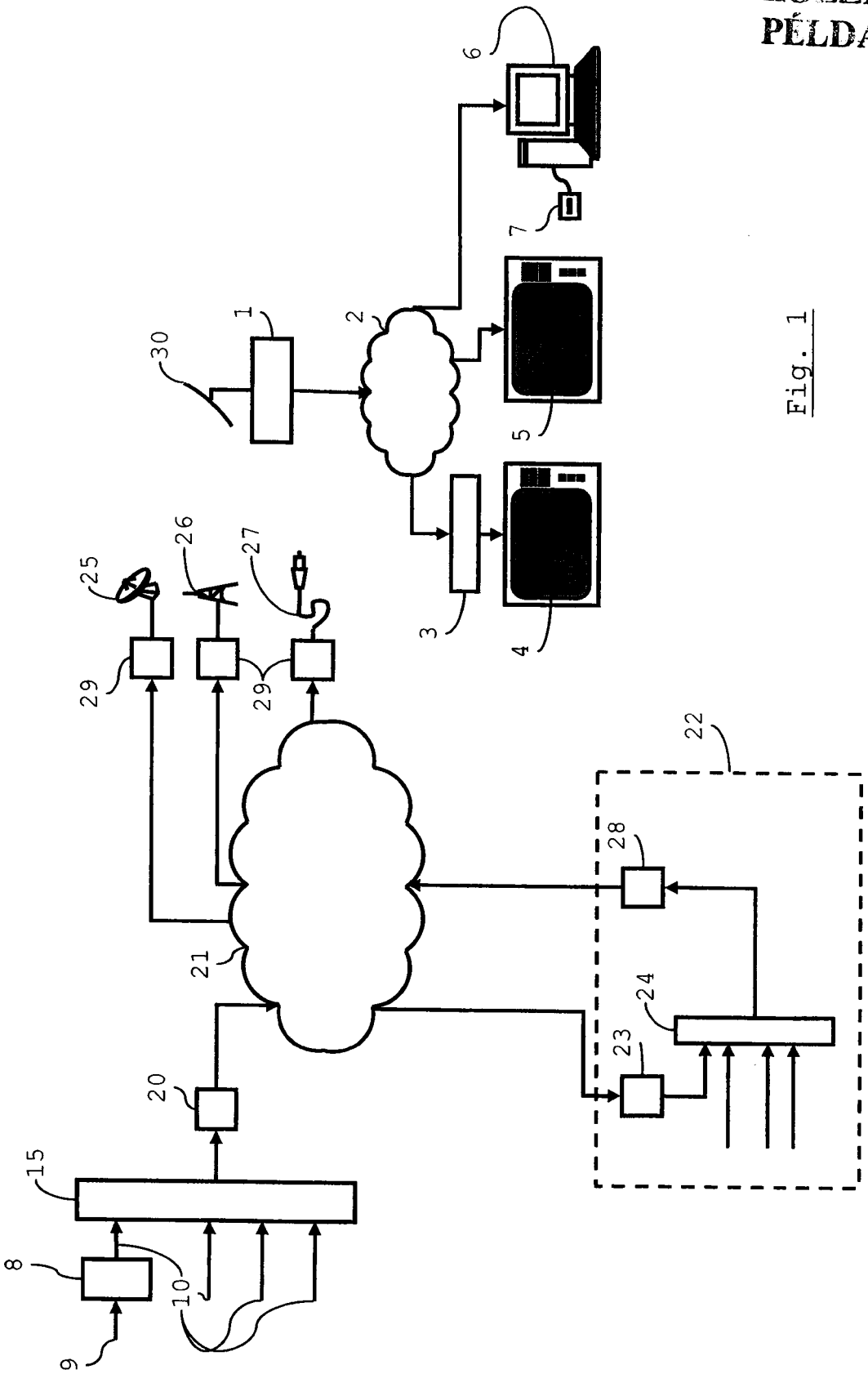

Fig. 1

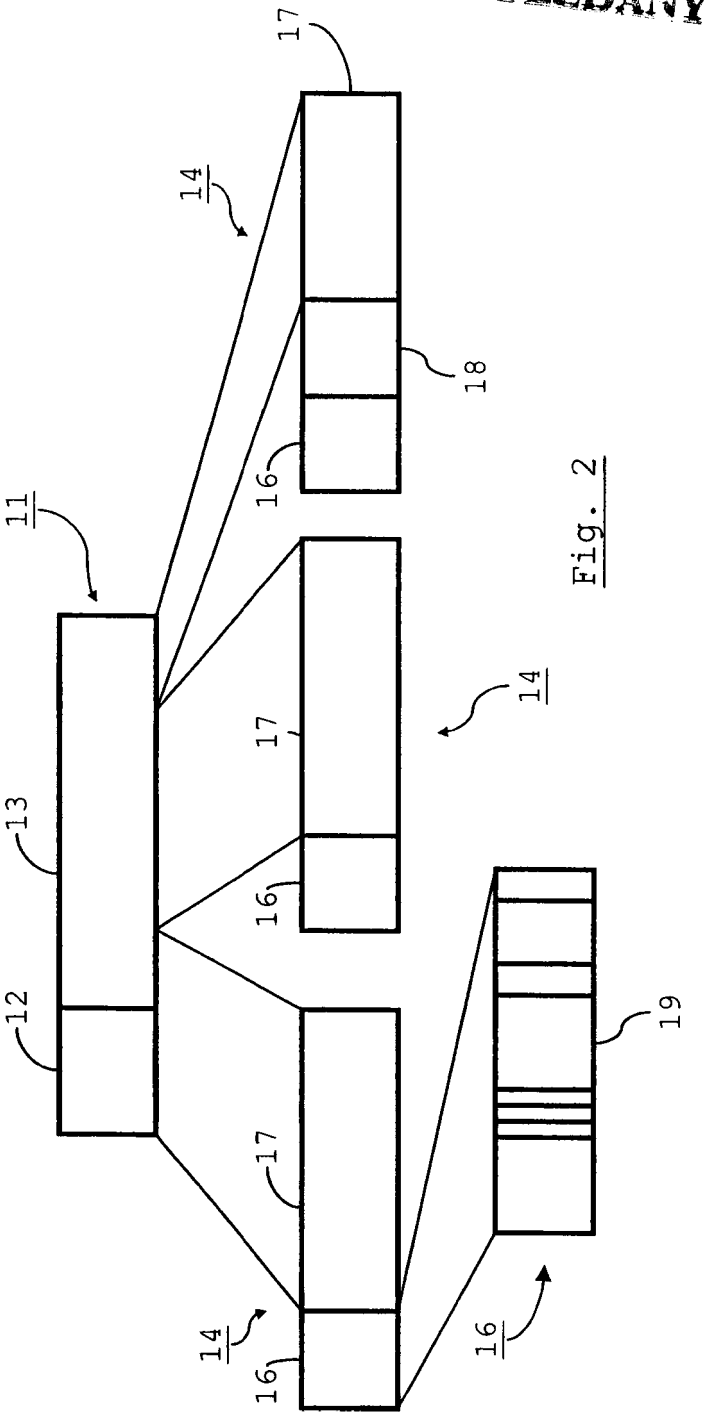

Fig. 2

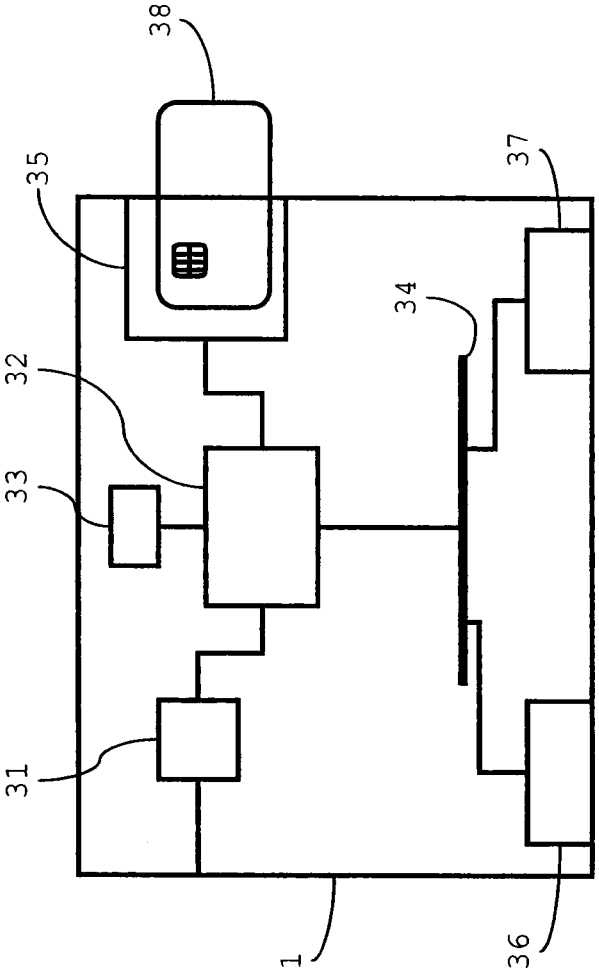

Fig. 3

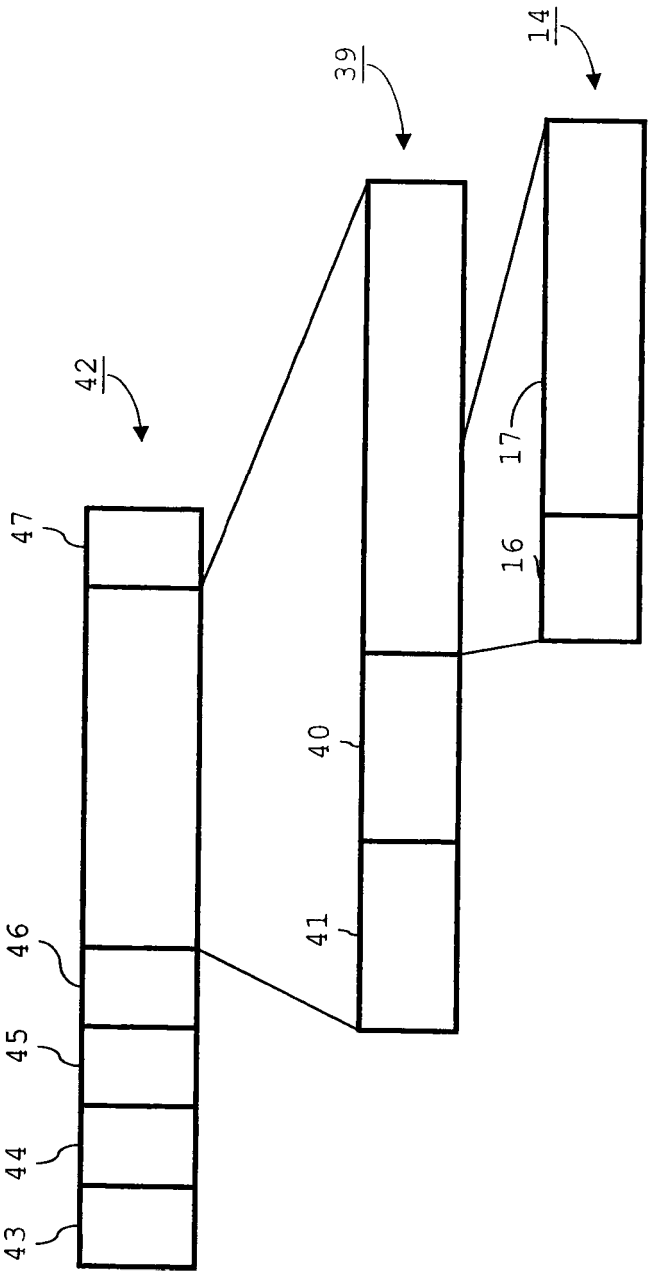

Fig. 4