



FI000097007B

(B) (11) KUULUTUSJULKAISU
UTLAGGNINGSSKRIFT
C (45) Patentti myönnetty
Patent meddelat 25 09 1996

97007

(51) Kv.1k.6 - Int.c1.6

H 04N 7/167

SUOMI-FINLAND

(FI)

Patentti- ja rekisterihallitus
Patent- och registerstyrelsen

(21) Patenttihakemus - Patentansökning	943582
(22) Hakemispäivä - Ansökningsdag	01.08.94
(24) Alkupäivä - Löpdag	01.08.94
(41) Tullut julkiseksi - Blivit offentlig	02.02.96
(44) Nähtäväksipanon ja kuul.julkaisun pvm. - Ansökan utlagd och utl.skriften publicerad	14.06.96

(71) Hakija - Sökande

1. Nokia Kulutuselektroniikka Oy, Radiomiehenkatu 3, 20320 Turku, (FI)

(72) Keksijä - Uppfinnare

1. Kangas, Mauri, Sporentie 21, 21530 Paimio, (FI)

(74) Asiamies - Ombud: Berggren Oy Ab

(54) Keksinnön nimitys - Uppfinningens benämning

Järjestelmä video-, audio- ja datapalveluja lähettävien eri hallintajärjestelmien
kontrolloimiseksi sekä järjestelmässä käytettävä vastaanotin
System för kontrollera olika styrningssystem som sänder video-, audio- och datatjänster
samt i systemet användbar mottagare

(56) Viitejulkaisut - Anförda publikationer

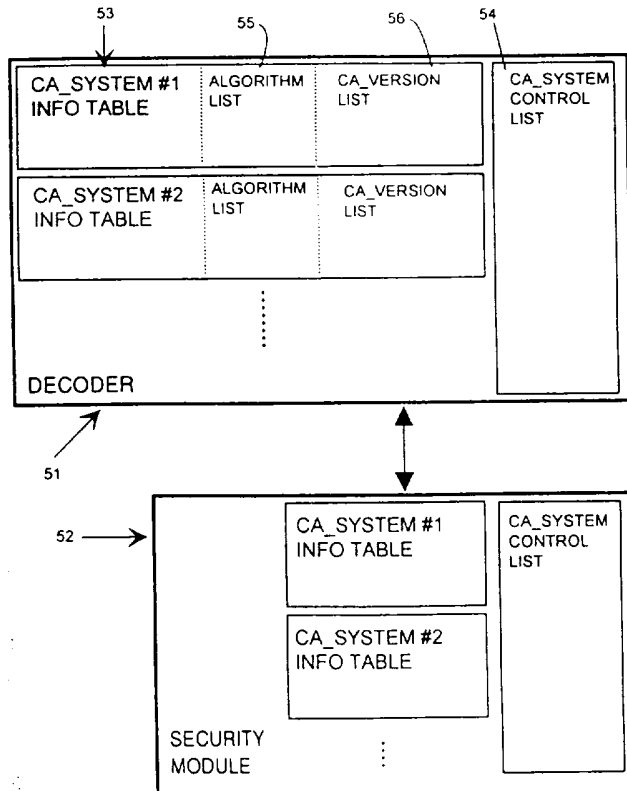
EP A 585833 (H 04N 7/167), EP A 506435 (H 04N 7/167), EP A 562295 (H 04N 7/167),
EP A 588184 (H 04N 7/167), US A 4736422 (H 04N 7/167)
Cutts, D.J.: "A Complete System for Controlled Access Television"
IBC 1990, International Broadcasting Convention, p. 266-269, Lontoo (engl. tiivistelmä)
Cruselles, E. et al.: "An Overview of Security in Eurocrypt Conditional Access System",
Proceedings of Globecom, 1993. IEEE Global Communications Conference (engl. tiivistelmä),
Saini, J.S.: "BBC Select Decoder", IBC 1992. International Broadcasting Convention,
p. 410-413, Lontoo 3-7.7.1993 (engl. tiivistelmä)

(57) Tiivistelmä - Sammandrag

Keksintö koskee järjestelmää video-, audio- ja datapalveluja niiden vastaanottoon oikeutetuille vastaanottimille lähettävien eri hallintajärjestelmien (engl. Conditional Access Systems) kontrolloimiseksi, jossa kukin hallintajärjestelmä suorittaa lähettämänsä palvelun salauksen, salauksen purkamiseen vastaanotimessa tarvittavien avainten lähettämisen salattuna ja valtuutusviestien lähetyksen. Ainakin yksi hallintajärjestelmä on nimetty kontrollijärjestelmäksi, jolla on oikeus kontrolloida muiden hallintajärjestelmien käyttämiä salausalgoritmeja ja avainten sekä valtuutusviestien lähetystä, jolloin kontrollijärjestelmä voi muuttaa muiden hallintajärjestelmien käyttöoikeuksia vastaanotimessa. Keksintö koskee myös järjestelmässä käytettävää vastaanotinta, joka käsittää dekooderin (51) salattujen video-, audio- ja datapalvelujen vastaanottamiseksi ja salauksen purkamiseksi, joka sisältää eri hallintajärjestelmiin liittyviä taulukoita (53), joista kukin sisältää hallintajärjestelmän käyttämän algoritmilistan (55), joka käsittää luettelon käytössä olevista salausalgoritmeista, joilla hallintajärjestelmän viestit ja palvelut on salattu.

Lisäksi dekooderi (51) sisältää hallintajärjestelmien kontrollitaulukon (54), joka sisältää luettelon kontrollijärjestelmistä. Vastaanottimeen voidaan salaustietojen antamiseksi liittää irrotettava turvamoduli (52), jonka taulukot ovat rakenteeltaan dekooderin (51) kaltaisia.

Uppfinningen avser ett system för att kontrollera olika hanteringssystem som sänder video-, audio- och datatjänster till behöriga mottagare, i vilket varje hanteringssystem utför chiffrering av den tjänst det sänder, utsändning av nycklar i chiffrerad form som behövs för dechiffrering i mottagaren och utsändning av behörighetssignaler. Åtminstone ett hanteringssystem har utsetts till kontrollsystem, som har rätt att kontrollera de av de övriga hanteringssystemen använda chiffreringsalgoritmerna och utsändningen av nycklar och behörighetssignaler, varvid kontrollsystemet kan ändra de övriga hanteringssystemens behörighet i mottagaren. Uppfinningen avser även en mottagare att användas i systemet, som omfattar en dekodare (51) för mottagning och dechiffrering av chiffrerade video-, audio- och datatjänster, som innehåller tabeller (53) i anslutning till de olika hanteringssystemen, av vilka var och en innehåller den av hanteringssystemet använda algoritmlistan (55), som omfattar en förteckning över chiffreringsalgoritmer i bruk, med vilka hanteringssystemets signaler och tjänster chiffrerats. Dessutom innehåller dekodaren (51) hanteringssystemens kontrolltabell (54), som innehåller en förteckning över kontrollsystemen. För att ge chiffreringsdata kan till mottagaren anslutas en löstagbar säkerhetsmodul (52), vars tabeller har likadan sammansättning som dekodern (51).



Järjestelmä video-, audio- ja datapalveluja lähettävien eri hallintajärjestelmien kontrolloimiseksi sekä järjestelmässä käytettävä vastaanotin - System för att kontrollera olika styrningssystem som sänder video-, audio- och datatjänster samt i systemet användbar mottagare

5

Tämä keksintö koskee järjestelmää video-, audio- ja datapalveluja niiden vastaanottoon oikeutetuille vastaanottimille lähettävien eri hallintajärjestelmien (engl. Conditional Access Systems) kontrolloimiseksi, jossa kukin hallintajärjestelmä suorittaa
10 lähettämänsä palvelun salauksen, salauksen purkamiseen vastaanottimessa tarvittavien avainten lähettämisen salattuna ja valtuutusviestien lähetyksen. Keksintö koskee myös järjestelmässä käytettävää vastaanotinta.

15 Digitaalisten video-, audio- ja datasignaalien siirtoon voidaan käyttää joko ilmateitse tapahtuvaa lähetystä, satelliittiyhteyttä, kaapeli-TV-verkkoa, puhelin/televerkkoa tai valokaapeliverkkoa, joissa digitaalista informaatiota lähetetään suurelle määrälle vastaanottimia. Usein kyseinen digitaalinen informaatio on tarkoitettu kaikkien vastaanottimien vapaasti käytettäväksi, mutta toisaalta halutaan käyttää menetelmiä, joilla voidaan kontrolloida sitä, kuka/ketkä vastaanottajista voivat tiedon saada.
20 Tällaisessa lähetysjärjestelmässä on kaksi periaatteellista toimintalinjaa: 1) digitaalista informaatiota lähetetään ennalta määritellyn suunnitelman mukaan, jolloin kukin vastaanottaja voi etukäteen tai lähetyksen aikana ilmaista halukkuutensa ko. informaation vastaanottoon, 2) digitaalista informaatiota lähetetään vain siinä tapauksessa, että joku vastaanottajista ilmaisee haluavansa vastaanottaa tällaista informaatiota.
25 Jälkimmäisessä tapauksessa voidaan myös sallia muiden kuin tilauksen tehneen vastaanottaa ko. informaatiota, jolloin näillä muilla vastaanottajilla voi olla ennestään oikeus vastaanottaa ko. lähetettä tai he voivat tilata sen lähetyksen aikana tai sen alkamista odotellessaan. Koska tällaisessa digitaalisen signaalin siirrossa halutaan estää luvaton signaalin vastaanotto, muutetaan bittivirta sellaiseen muotoon, että vastaanottimien on mahdotonta selvittää lähetetyn datan sisältöä, ellei
30 niillä ole käytettävissään datan salauksen purkamiseen tarvittavia avaimia. Digitaalisen bittivirran salaamiseen on käytettävissä monia menetelmiä, joita käyttävien järjestelmien tulisi olla mahdollisimman monimutkaisia ja varmoja, etteivät järjestelmän käyttöönoton jälkeen mahdollisesti tapahtuvat luvattomat datan purkuyritykset
35 onnistuisi.

· Digitaalisen videosignaalin siirtoon liittyy olennaisena osana audiosignaalin siirto ja lisäksi järjestelmien toteuttamisen yhteydessä täytyy lähettää myös ns. kontrollida-

taa. Palvelujen monipuolistamiseksi on tulevaisuudessa tarpeellista lähettää myös eri sovelluksia varten datainformaatiota, joka voi siirtojärjestelmän kannalta sisältää melkein mitä tahansa informaatiota. Näitä kaikkia informaation osia on tarpeen ainakin soveltuvien osin lähettää salattuna, jotta voidaan varmistaa niiden vastaanottaminen vain haluttujen vastaanottajien toimesta.

Tulevaisuuden digitaaliset televisiojärjestelmät mahdollistavat useiden ohjelmien samanaikaisen siirtämisen yhdessä siirtokanavassa. Tällöin siirrettävä signaali on pakettimuotoinen, ja siirtokanavassa kulkee vuorotellen eri ohjelmien audio- ja videoinformaatiota sisältäviä paketteja. Video-, audio- ja datasiinaalien välittämiseen paketteina on kehitetty useampiakin kompressiostandardeja, joista MPEG-2 (Moving Picture Experts Group) on yksi. Tämä standardi on syntynyt ISO:n (International Standards Organisation) ja IEC:n (International Electrotechnical Commission) yhteisessä työryhmässä. MPEG-standardeja on kehitelty useitakin, ja niiden määrittelemien spesifikaatioiden mukaan em. informaation lähettäminen tapahtuu tulevaisuudessa useissa eri sovelluksissa. Standardien suhteen viitataan ammattimiehen tuntemaan MPEG-standardiin ISO/IEC 13818. Sen mukaisesti pakataan koodattu video-, audio- ja datainformaatio ns. PES (Packetized Elementary Stream) -paketeiksi. Paketti, jonka pituus voi vaihdella, sisältää otsakkeen ja dataosan.

Kuvassa 1 on esitetty PES-paketin rakenne. Paketin otsake (header) käsittää paketin aloituskoodin (packet start code prefix), virtatunnisteen (stream ID), paketin pituuden osoituksen (packet length), optionaalisen otsakkeen sekä joukon täytetäviä (stuffing bytes). Tämän jälkeen tulee paketin datatavuja sisältävä informaatio-osa, joka aiemmin sanotun mukaisesti voi käsittää lohkon koodattua ohjelman audio-, video- tai datasiinaalia, kuitenkin niin, että yhdessä paketissa on vain yhdenlaista signaalia. Yhden paketin pituus voi olla useita kilotavuja.

MPEG-standardi määrittelee kaksi erityyppistä bittivirran muotoa: 1) ohjelmavirta (engl. Program Stream) ja 2) siirtovirta (engl. Transport Stream). Ohjelmavirta sisältää koodatun video- ja audiosignaalin edellä mainittuina PES-paketteina (Packetized Elementary Stream), joista kukin sisältää aina tietyn kokoisen koodatun bittivirran lohkon, ts. ohjelmälähteen video-, audio- ja datasiinaali koodataan erikseen ja pätkitään tietyn pituisiksi lohkoiksi, jotka kukin sijoitetaan PES-paketin informaatio-osaan. Sen pituus ja siten PES-paketin pituus voi olla vaihteleva. Siten ohjelman videosignaali koostuu peräkkäisistä video-PES-paketeista, audiosignaali

peräkkäisistä audio-PES-paketeista jne. Esimerkiksi elokuvan kaikki informaatio voidaan tallentaa ohjelmavirtana.

5 Kuvat 2a ja 2b esittävät, kuinka kuvan 1 PES-paketit sijoitetaan ohjelmavirtapaketeiksi. Ohjelmavirta, kuva 2a, koostuu peräkkäisistä paketeista, joissa on paketin otsake ja informaatio-osa PACK. Kuva 2b, joka esittää ohjelmavirran yhden paketin rakennetta, ns. pakettikerrosta, havainnollistaa, että ohjelmavirran paketti PACK sisältää useita PES-paketteja, joita on merkitty #1, #2, ..., #n ja jotka voivat sisältää ohjelmaan liittyvää kuvaa, ääntä, dataa jne. Havainnollisuuden vuoksi voidaan ajatella, että kuvan 2a pakettijono esittää esim. yhtä elokuvaa, jonka PES-paketoidut audio- ja videosignaalit on sijoitettu ohjelmavirtapakettien informaatio-osiin. Ohjelmavirta loppuu loppukoodiin "program end code".

15 Kun on lähetettävä ohjelmälähteen informaatio siirtotielle, muodostetaan ns. siirtovirta, joka on tarkoitettu video- ja audiosignaalien siirtämiseen jollain siirtotiellä, kuten TV-lähetys, satelliitti, kaapeli-TV, puhelin/telekaapelit, valokaapelit, jne. Jos ohjelmälähde on ohjelmavirran muodossa taltioitu tallenne, esim. CD-levylle tallennettu elokuva, demultipleksoidaan ohjelmavirta ensin erillisiksi audio-, video- ja data-PES-paketeiksi. Jos taas ohjelmälähteestä saadaan audio-, video- ja datasignaalia, ne dekodataan ja muodostetaan PES-paketteja. Oli lähde mikä tahansa, niin niistä saadut PES-paketit sijoitetaan siirtovirtaan. Siirtovirran rakenne on esitetty kuvissa 3a ja 3b. Siirtovirta koostuu kiinteän mittaisista esim. 188 tavun siirtovirtapaketeista, kuva 3a. Paketti käsittää vaihtuvan pituisen otsakkeen (header) ja hyötyinformaatiota sisältävän dataosan eli hyötykuorman (payload). Kuvassa 3b on esitetty yhden siirtovirtapaketin rakenne. Paketin otsake käsittää 9 kenttää, joista viimeinen on ns. adaptaatiokenttä (adaptation field). Paketin kuormaosaan (payload) sijoitetaan PES-paketin tavuja.

30 Jokaiselle digitaalisten signaalien siirron piiriin kuuluvalla järjestelmälle on yhteistä digitaalisignaalien salaaminen, jossa digitaalisen bittivirran sisältämä video-, audio- ja datainformaatio salataan ensin salauslaitteessa ja puretaan vastaanottolaitteessa. Kunkin järjestelmän käyttöön liittyy olennaisena osana hallintajärjestelmä (Conditional Access System), joka lähettää vastaanottimille salattua ohjausdataa, jota käytetään vastaanottimien vastaanotto-oikeuksien jakeluun sekä bittivirtakohtaisten avainten jakeluun. Käytössä voi olla useita hallintajärjestelmiä ja siten niiden ohjausdatan siirtoon käytettäviä, toisistaan poikkeavia salausalgoritmeja ja lisäksi samalla hallintajärjestelmällä voi olla käytössään useita eri algoritmeja ohjausdatan salaamiseen. Yleensä yhdellä ohjelmatoimittajalla on käytössään vain yksi hallinta-

järjestelmä mutta sen lähettämiin palveluihin voidaan liittää muidenkin hallintajärjestelmien (siis käytännössä ohjelmatoimittajien) valtuutusviestejä ja avainten jakeluviestejä, jolloin palvelun salaaminen suoritetaan vain yhden hallintajärjestelmän toimesta ja muille järjestelmille kerrotaan käytetyt avaimet, jotta ne voivat lähettää
5 avaimet salattuina niiden omilla salausalgoritmeilla. Vastaanottimen kannalta on yleistä tilanne, jossa useat eri hallintajärjestelmät tarjoavat palveluitaan samalle vastaanottimelle. Vastaanottimella pystytään siten vastaanottamaan palveluja useilta eri ohjelmatoimittajilta, koska on vastaanotettu useiden eri hallintajärjestelmien kontrolloimia valtuutus- ja avainten jakeluviestejä.

10

Edellä mainittu hallintajärjestelmä (Conditional Access System) tarkoittaa käytännössä siten minkä tahansa maksu-TV-järjestelmän hallintajärjestelmää, jonka tarkoituksena on jakaa ohjelmia ja muita palveluja maksaville asiakkaille korvausta vastaan siten, että voidaan turvallisesti jakaa kaikille halukaille vastaanotto-oikeuksia ja toisaalta estää palvelujen vastaanotto sellaisilta vastaanottajilta, jotka eivät ole tilanneet eivätkä tilaa ko. vastaanotto-oikeuksia. Hallintajärjestelmän, josta voidaan käyttää nimitystä CA-järjestelmä, toimintaan kuuluvat näin ollen olennaisina osina seuraavat toiminnot:

1. Maksullisena lähetetyn palvelun salaus.
- 20 2. Salatun palvelun purkamiseen vastaanottimessa tarvittavien avaimien jakelu.
3. Valtuutusviestein lähetys vastaanottajille.

Maksullisena lähetetyn palvelun salauksen purkamiseksi on lähetettävä tilaajalle salauksen purkuavaimet turvallisesti, joten niitä välittävät viestit on salattu CA-järjestelmän käyttämällä algoritmeilla. Nämä algoritmit ovat eri algoritmeja kuin varsinaisen palvelun eli video-, audio- ja datasiirtovirtapakettien salaamiseen käytettävät algoritmit ja yleensä kullakin CA-järjestelmällä on käytössä omat salausalgoritmit. Valtuutusviesti tarkoittaa sitä, että kaikille vastaanottajille lähetetään ns. valtuutusviestejä, jotka sisältävät tiedot niistä ohjelmista, joita kukin vastaanottaja voi purkaa.
25 Nämä tiedot lähetetään kullekin vastaanottajalle yksilöllisinä eli kullekin vastaanottajalle voidaan lähettää mikä tahansa valikoima vastaanotettavista palveluista. Toisaalta voidaan käyttää vastaanottajien ryhmittelyä siten, että kokonainen ryhmä vastaanottajia saa samalla valtuutusviestillä valtuudet. Valtuutusviestien sisältämät tiedot sisältävät kullekin palvelulle oman koodin, jonka täytyy vastata avaimien
30 yhteydessä lähetettyä koodia, jotta todetaan, että valtuutus on voimassa. Valtuutusviestit voidaan lähettää yksilöllisesti, sillä jokaisen vastaanottimen dekooderilla on oma yksilöllinen osoitenumero.

Koska bittivirtojen salaus tapahtuu suuresta nopeudesta johtuen mikropiiritoteutuksena eikä sen toteuttaminen ole nykytekniikalla mahdollista suorittaa ohjelmallisesti, on useissa tapauksissa edullista toteuttaa bittivirran tasolla tapahtuva salaus käyttäen hallintajärjestelmissä samaa salausalgoritmia, jolloin eri hallintajärjestelmiä varten toteutettavat salauslaitteet ja salauksen purkulaitteet ovat laitteistotasolla tältä osin samanlaisia.

Vastaanotettaessa useiden eri hallintajärjestelmien ohjelmia syntyy lukuisia ongelmia. Olipa bittivirran tasolla tapahtuva salaus samanlaista kaikkien digitaalisten signaalien osalta tai ei, ollaan nimittäin tulevaisuudessa hyvin pian sellaisessa tilanteessa, että digitaalisten signaalien lähettämistä kontrolloi suuri joukko toisistaan riippumattomia hallintajärjestelmiä, joilla kullakin on käytössään päivityksistä tai versioinneista johtuen useita eri ohjausdatan algoritmeja. Kullakin hallintajärjestelmällä on tosin tavallisesti yksi sille ominainen ohjausdatan siirtotapa, mutta siitä voi olla useita eri versioita. On myös mahdollista, joskin harvemmin käytännössä, että yhdellä hallintajärjestelmällä on käytössään useita algoritmeja ohjausdatan siirrossa.

Tunnetuissa järjestelmissä käytetään salauksen purkamiseen turvallisuussyistä salausavaimet sisältävää älykorttia (smart card), jonka tarkoituksena on toimia ns. hallittuna keinona vastaanottaa maksullisia, salattuna lähetettyjä palveluja. Yleensä palvelujen tarjoajia on useita, jolloin kyseeseen voi tulla useiden eri älykorttien käyttö joko samanaikaisesti tai älykorttia vaihtamalla. Yksi älykortti on yleensä aktivoituna kerrallaan palvelun vastaanottamiseen ja muut voivat olla vain tiedon vastaanottajina tai valmiudessa aktivoitumaan, kun vastaava palvelu valitaan vastaanottimesta. Älykortit ovat turvallisia, sillä ne on tehty rakenteellisesti sellaisiksi, että niiden kopioiminen tai väärinkäyttö on erittäin vaikeaa tai mahdotonta. Älykortti-käsitteellä tarkoitetaan tällä hetkellä korttia, joka sisältää yhden mikroprosessoripiirin, joka kytkeytyy varsinaiseen laitteeseen sarjalinjan välityksellä. Laite syöttää sähköä sekä kellosignaalin (oskillaattori) älykortille RESET-signaalin lisäksi. Tulevaisuudessa valmistetaan varmasti myös useitakin piirejä sisältäviä älykortteja, joissa liitäntä varsinaiseen laitteeseen on monimutkaisempi sisältäen esim. rinnakkaismuotoisen liitännän.

Edellä kuvatussa tilanteessa ongelmaksi tulee, miten ratkaista tarve hallita yksiselitteisesti tietyn hallintajärjestelmän käyttämiä ohjausdatan algoritmeja sekä eri hallintajärjestelmien mahdollisuuksia jakaa vastaanotto-oikeuksia tai vastaavasti bittivirtojen salaamiseen liittyviä avaimia. Tällainen tarve ilmenee silloin, kun halutaan estää salattujen digitaalisten signaalien luvaton vastaanotto, joka voisi perustua esim.

- vastaanotto-oikeuksien tai avaimien luvattomaan edelleen jakeluun tai sellaisen huonosti suunnitellun ohjausdatan salausalgoritmin käyttöön, jota voidaan jostain syystä käyttää suunniteltua laajemmin myös tulevien algoritmien ohittamiseen tai salauksen purkamiseen ainakin osittain. Toisaalta markkinatilanne voi joskus johtaa siihen, että ohjelmatoimittaja markkinoi digitaalisia palvelujaan kompensoimalla vastaanottimien hintoja tai vuokraa, jolloin se samalla haluaa varmistua siitä, että kukaan muu ohjelmatoimittaja ei pysty käyttämään ainakaan veloituksetta ko. vastaanottimia vapaasti omien palvelujen välittämiseen. Vastaanottimen käytön kontrollointi tulee tällaisessa tilanteessa tarpeelliseksi niiden hintaa tai vuokraa kompensoineen ohjelmatoimittajan kannalta katsoen. Voi myös käydä siten, että jokin toinen taho kopio ohjelmatoimittajan käyttämän hallintajärjestelmän siirtovirtapakettien otakskeisiin liittyvät ohjelmisto- ja algoritmitiedot ja lähettää sitten luvatta ohjelmia. Tämä halutaan estää.
- 15 Älykorttien käyttö turvallisuusriskien pienentämisessä on myös ongelmallista. Ne ovat liitännöjensä puolesta standardoituja ja siten helposti jaettavissa vastaanottajille esim. postitse. Tällöin kortti voi joutua väärin käsiin ja sen tiedot voidaan kopioida ja käyttää niitä luvattomaan palvelun vastaanottoon.
- 20 Tämän keksinnön tavoitteena on luoda järjestelmä, jolla edellä mainitut lukuisten eri hallintajärjestelmien käytöstä johtuvat ongelmat voidaan poistaa. Tavoitteena on luoda hallintajärjestelmien yläpuolella oleva järjestelmä, joka määrittelee mihin vastaanotinta voidaan käyttää ja mihin ei.
- 25 Järjestelmälle on tunnusomaista se, että ainakin yksi hallintajärjestelmä on nimetty kontrollijärjestelmäksi, jolla on oikeus kontrolloida muiden hallintajärjestelmien käyttämiä salausalgoritmeja ja avainten sekä valtuutusviestien lähetystä, jolloin kontrollijärjestelmä voi muuttaa muiden hallintajärjestelmien käyttöoikeuksia vastaanottimessa. Järjestelmässä käytettävälle vastaanottimelle, joka käsittää välineet salattujen video-, audio- ja datapalvelujen vastaanottamiseksi ja salauksen purkamiseksi, on tunnusomaista se, että mainitut välineet sisältävät
- 30 - eri hallintajärjestelmiin liittyviä taulukoita, joista kukin sisältää hallintajärjestelmän käyttämän algoritmilistan, joka käsittää luettelon käytössä olevista salausalgoritmeista, joilla hallintajärjestelmän viestit ja palvelut on salattu,
- 35 - hallintajärjestelmien kontrollitaulukon, joka sisältää luettelon kontrollijärjestelmistä.

Keksinnön mukainen hallintajärjestelmien yläpuolella oleva järjestelmä on yksi tai useampi hallintajärjestelmä, jolle annetaan enemmän oikeuksia kuin muille hallintajärjestelmille eli annetaan oikeus kontrolloida muiden hallintajärjestelmien käyttöoikeuksia ja käyttötapoja. Järjestelmää kutsutaan jäljempänä kontrollijärjestelmäksi.

5

Kuten edellä esitetystä käy ilmi, voidaan vastaanottimien käytön hallinta jakaa kahteen osaan: 1) ohjausdatan algoritmien käytön hallinta ja 2) hallintajärjestelmien käytön hallinta. Keksintönä on siten kontrollijärjestelmä, joka hallitsee hallintajärjestelmiä näiden ominaisuuksien suhteen. Kumpaakin edellä mainittua käytön hallinnan aluetta voidaan ajatella kontrolloitavan ainakin neljällä periaatteella: 1) perustuen dekooderin numeroon, 2) perustuen hallintajärjestelmän tunnuksen, 3) perustuen edellä mainittujen yhdistelmään ja 4) perustuen erilaisten kontrollointimekanismien luetteloon. Koska hallintajärjestelmän tunnus standardiehdotuksen mukaan tulee sisältämään 256 vaihtoehtoa kullekin hallintajärjestelmälle sisältäen mahdolliset tulevaisuuden variaatiot hallintajärjestelmästä tai sen alijärjestelmät, voidaan vastaanottimen käytön hallinta kohdistaa kaikkiin 256 hallintajärjestelmän vaihtoehtoon, hallintajärjestelmän alijärjestelmistä tai kullekin hallintajärjestelmälle voidaan antaa tarvittava maskisana, jonka avulla yhden hallintajärjestelmän alijärjestelmät voidaan tunnistaa. Lisäksi eri hallintajärjestelmiä varten voi vastaanottimessa olla luettelo, johon voidaan tallettaa haluttu määrä joko käytössä olevia hallintajärjestelmiä, sisältäen em. variaatiot kunkin hallintajärjestelmän osalta, tai vastaavasti luettelo niistä hallintajärjestelmistä, joita vastaanotin ei saa käyttää hyväkseen.

20

Keksinnön mukaisesta käytön hallinnasta tehdään luotettava siten, ettei käytön hallinnan kontrollointiin päästä vaikuttamaan hallitsemattomasti, eli laitteen valmistusvaiheessa luodaan peruskriteerit, joiden avulla käytön hallintaa voidaan tulevaisuudessa kontrolloida. Yksinkertaisimmillaan käytön hallinnan kontrolli voidaan ensimmäisen suorituserityksen mukaan kohdentaa ainoastaan siihen hallintajärjestelmän tunnuksen tai tunnuksiin, jotka ovat käytössä laitevalmistajalla tai hänen asiakkaallaan, eikä kyseistä käytön hallintaoikeutta voi enää jälkikäteen muuttaa kuin avaamalla vastaanotin ja korvaamalla käytön hallintaoikeudesta vastaava osa uudella. Toisin sanoen vastaanottimeen asennetaan valmistusvaiheessa luettelo sen hallintajärjestelmän tai niiden hallintajärjestelmien tunnuksista, joilla on oikeus kontrolloida muiden hallintajärjestelmien käyttöoikeuksia.

35

Toinen suorituserityksen käyttöön hallintaoikeuden kontrolloinnin toteuttamiseksi on tehdä siitä sillä tavalla joustava, että valmistusvaiheessa voidaan laitteelle antaa yhden tai useamman hallintajärjestelmän tunnus, joilla on mahdollisuus paitsi käytön

hallintaoikeuden kontrollointiin myös mahdollisuus muuttaa käytön hallintaoikeuksien kontrollointiin oikeuttavia tunnuksia. Toisin sanoen valmistusvaiheessa vastaanottoon syötettävään luetteloon kuuluvien kontrollijärjestelmien avulla voidaan myöhemmin lisätä tai poistaa uusia ohjausjärjestelmien tunnuksia eli voidaan
 5 muuttaa luetteloa, kun taas ensimmäisen suoritusmuodon mukaan luettelo pysyy aina muuttumattomana.

Keksinnön erään ominaispiirteen mukaan käytetään vastaanottimessa erillistä siihen liitettävää osaa, ns. turvamodulia. Se voi sisältää edellä mainittujen luetteloiden lisäksi muita turvallisuuteen liittyviä elektronisia osia kuten bittivirran salauksen purkamisessa tarvittavat osat. Siihen voidaan sijoittaa myös vastaanottimen mikroprosessori salauksenpurkupiirin ohella. Turvamodulin etu on se, että turvallisuusriskin ilmetessä esim. laajamittaisen laittoman kopioinnin yhteydessä voidaan moduli vaihtaa rakenteeltaan tai sisällöltään uuteen. Moduli voidaan tarvittaessa tehdä niin, ettei
 10 se ole minkään standardin mukainen vaan laitekohtainen. Tämä on turvallisuuden kannalta tehokkaampi vaihtoehto kuin pelkän älykortin vaihtaminen. Vastaanotinta voidaan käyttää siten joko ilman turvamodulia tai sen kanssa siten, että tiettyä palvelua vastaanotettaessa käytetään viestien purkamiseen pelkästään turvamodulia, pelkästään vastaanotinta tai turvamodulia ja vastaanotinta yhdessä. Tieto siitä, mitä
 15 yhdistelmää käytetään, sijoitetaan dekooderin ja/tai modulin sopiviin taulukoihin.
 20

Keksintöä selostetaan seuraavassa yksityiskohtaisesti viittaamalla oheisiin kuviin, joissa

- | | |
|-------------------|---|
| kuva 1 | esittää PES-paketin rakenteen, |
| 25 kuvat 2a ja 2b | esittävät ohjelmavirran rakenteen, |
| kuvat 3a ja 3b | esittävät siirtovirran rakenteen, |
| kuva 4 | esittää siirtovirran peräkkäisten pakettien sisältöä, |
| kuva 5 | esittää keksinnön mukaisen vastaanottimen rakenteen, |
| kuva 6 | esittää algoritmiluettelon, ja |
| 30 kuva 7 | esittää hallintajärjestelmien luettelon. |

Kuvia 1-3 on jo selostettu yleisessä osassa. Kuvan 3a siirtovirtaa on esitetty myös kuvassa 4, joka esittää osan tyypillisestä siirtovirrasta. Se koostuu allekkain esitetynä peräkkäisistä paketeista, joiden rakenne perussyntaksiltaan on kaikissa samanlainen. Kukin paketti käsittää otsakeosan (HEADER), joka on MPEG2-standardin mukainen, ja informaatio-osan (PAYLOAD). Sisältämänsä informaation mukaan
 35 paketit voidaan jakaa videopaketteihin (VIDEO), audiopaketteihin (AUDIO), hallintajärjestelmän ohjauksen välittäviin paketteihin (CA_CTRL MESSAGE) sekä hal-

15

25

35

ALG#2 on hallintajärjestelmien kontrollointijärjestelmän käytössä kun taas on algoritmit ALG#1 ja ALG#3 ovat sekä hallintajärjestelmän omassa käytössä että hallintajärjestelmien kontrollointijärjestelmän käytössä. Luettelon alalaidassa oleva algoritmivalintaosa ALG_SELECTION on kontrollijärjestelmän aseteltavissa. Tämä tarkoittaa, että algoritmien valinta suoritetaan joko kontrollijärjestelmän toimesta tai hallintajärjestelmän toimesta, mutta valinnan tästä tekee hallintajärjestelmien kontrollointijärjestelmä. Kontrollijärjestelmä voi esim. antaa hallintajärjestelmän CA-SYSTEM#1, kuva 5, päättää, että käytetään algoritmia ALG#3 sen lähettämien viestien salaamiseen. Kuvan 6A tapauksessa on algoritmivalintaosan ALG_SELECTION arvo CTRL_SYS, jolloin algoritmien valinta suoritetaan kontrollijärjestelmän toimesta.

Vastaavasti kuvassa 6 B on esitetty kuvan 5 versioluettelon 56 tarkempi sisältö. Kuva esittää siten hallintajärjestelmien versiotaulukkoa CA_VERSION LIST, jossa on hallintajärjestelmää varten oma sarake OWN_SEL sekä hallintajärjestelmien kontrollointijärjestelmää varten oma sarake CTRL_SYS SELECTION. Vastaavalla tavalla kuin kuvassa 6A on alalaidassa kontrollijärjestelmän suorittama valinta hallintajärjestelmän tai kontrollijärjestelmän välillä. Version valinta suoritetaan joko kontrollijärjestelmän toimesta tai hallintajärjestelmän toimesta, mutta päätöksen siitä, kumpi valitsee, tekee hallintajärjestelmien kontrollointijärjestelmä. Kontrollijärjestelmä voi esim. antaa hallintajärjestelmän CA-SYSTEM#1, kuva 5, päättää, että käytetään hallintajärjestelmän versiota VER#1. Versiointi sisältää paitsi erilaisia hallintajärjestelmän versioita myös ohjelmallista eroavuutta eri versioiden välillä, eli tällä valinnalla suoritetaan hallintajärjestelmien versioiden valinnan ohella myös valinta eri ohjelmaversioiden välillä. Kuvan 6B tapauksessa on versionvalintaosan VER_SELECTION arvo CTRL_SYS, jolloin versionvalinta suoritetaan kontrollijärjestelmän toimesta, eli hallintajärjestelmän käyttöön voidaan valita joko versio VER#1 tai VER#3.

Kuvassa 7 on esitetty kuvan 5 hallintajärjestelmien kontrollitaulukon 54 (CA_system control list) sisältö. Se on luettelo mahdollisista hallintajärjestelmistä SYS#1, ..., SYS#n kahdessa sarakkeessa, joista toisessa CA_SYS IN USE ilmoitetaan hallintajärjestelmät, jotka ovat käytössä, kuvassa järjestelmät 1, 3, 5 ovat käytössä ja toisessa CA_SYS NOT IN USE ilmoitetaan ne hallintajärjestelmät, joiden käyttö on ehdottomasti suljetaan pois, kuvassa järjestelmät 2, 4 ja 6 jne. Lisäksi luettelossa on kolmas sarake CONTROL CA_SYSTEM IN USE, jossa on luettelo hallintajärjestelmistä, jotka toimivat kontrollointijärjestelminä. Tälle luettelolle on tehtävä turvajärjestelyt siten, että valmistusvaiheessa jää voimaan ainakin yksi kont-

rollijärjestelmä, jota ei voi listalta poistaa. CA_SYSTEM IN USE ja CA_SYSTEM NOT IN USE -tiedot sisältävät myös tiedon siitä, mitä turvamoduleja/älykortteja voidaan liittää ko. vastaanottimeen ja vastaavasti turvamodulin tapauksessa tämä tieto sisältää tiedon siitä, minkä systeemin vastaanottimeen turvamoduli voidaan
5 liittää (kyseistä tietoa ei ole esitetty kuvassa 7). Tällöin voidaan hallita tilanne, jossa tiettyyn vastaanottimeen voidaan kytkeä vain haluttuja turvamoduleja tai älykortteja.

Seuraavassa viitataan uudelleen kuvaan 5 ja selostetaan tarkemmin turvamodulia 52, jota käytetään älykortin ohella vastaanottimeessa. Turvamoduli 52 sisältää samoista
10 lähtökohdista olevia asioita kuin dekooderin 53 sisällä olevat taulukot, mutta turvamodulin ja dekooderin sisällä olevilla taulukoilla ei tarvitse olla mitään keskinäistä yhteyttä vaan taulukot voivat sisältää aivan eri asioita kuin dekooderin sisällä olevat vastaavat taulukot. Turvallisuusriskin ilmetessä esim. laajamittaisen piratoinnin tapauksessa voidaan turvamoduli vaihtaa rakenteeltaan/sisällöltään uuteen, jolloin
15 laiton kopiointi saadaan estettyä tai vaikeutettua ja voidaan siten taata turvallinen järjestelmä. Koska tunnetut älykortit ovat liitännän puolesta standardoituja ja helposti esim. postitse jaettavia, on älykortteihin liittyvä turvallisuusriski suurempi kuin varsinaisiin suurempiin turvamoduleihin. Erillinen turvamoduli voidaan suunnitella sellaiseksi, että sen liitäntä laitteeseen ei noudata mitään standardia, toisin kuin äly-
20 korttitapauksessa, jolloin yhden laitevalmistajan turvamodulin tutkiminen ei auta toisen laitevalmistajan turvamodulin tutkimiseen tai piratointiin. Lisäksi turvamoduli voi sisältää sellaisia ASIC-piirejä, joiden luvaton kopioiminen on hankalaa, koska niiden suorittama toimintafunktio voi olla hyvin monimutkainen.

25 Keksinnön turvamoduli on irrotettava moduli, joka kytkeytyy varsinaiseen laitteeseen liittimen välityksellä. Kun puhutaan sellaisesta turvamodulista, joka sisältää enemmän kuin älykortin, on kyseessä moduli, jossa on hyvin moninapainen liitäntä (sovelluksesta riippuen) vastaanottimeen. Tällainen turvamoduli voi sisältää periaatteessa samanlaista elektroniikkaa kuin mihin nykyteknologioilla on totuttu esim.
30 vastaanotinlaitteissa. Koska turvamodulin fyysisellä koolla tai sen sisältämällä elektroniikalla ei ole sellaisia rajoituksia kuin älykortin tapauksessa (taipuminen, kortin paksuus, jne.), voidaan sille sijoittaa turvallisuuteen liittyviä elektronisia osia, esim. digitaalisen signaalin siirron tapauksessa bittivirran salauksen purkamisen sisältämät osat. Koska toisaalta voi olla hankalaa tehdä riittävän turvallista kytkentää vastaan-
35 ottimen mikroprosessorin ja bittivirran salauksenpurkupiirin välille turvallisuusmielessä, voidaan nämäkin osat tarvittaessa sijoittaa turvamodulille. Näiden toimenpiteiden lisäksi pyritään turvamoduli rakenteellisesti tekemään sellaiseksi, että sen osien tutkiminen elektronisilla laitteilla tulisi mahdollisimman hankalaksi.

Kuten aiemmin on sanottu, sisältää turvamoduli rakenteellisesti samoja taulukoita kuin mitä on dekooderissakin. Tosin turvamodulin ajatuksen mukaisesti sen sisältämät tiedot eroavat tavallisesti dekooderiin valmistuksessa asetetuista tiedoista. Sen avulla saadaan vastaanottimelle siten lisättyä uusia hallintajärjestelmiä ja salausalgoritmeja ja vaikeutettua laiton kopiointi. Erillinen turvamoduli ja siihen liitetty älykortti voivat molemmat sisältää em. taulukoita, mutta käsitteellisesti ja asioiden yksinkertaistamiseksi turvamoduli-käsitteeseen on yhdistetty kaikki em. tapaukset. Tällöin turvamodulin taulukot voivat olla yhdistelmä erillisen modulin ja älykortin taulukoista. Taulukoiden tarkoituksena on pyrkiä hallitsemaan tilanteita, jossa vastaanotinta pyritään käyttämään eri hallintajärjestelmien hallitsemien lähteiden vastaanottamiseen.

Vastaanotinta voidaan käyttää joko ilman turvamodulia tai sen kanssa siten, että tiettyä palvelua vastaanotettaessa käytetään viestien purkamiseen a) pelkästään turvamodulia, b) pelkästään vastaanotinta tai c) turvamodulia ja vastaanotinta yhdessä. Tieto siitä, mitä yhdistelmää käytetään, sijoitetaan dekooderin ja/tai turvamodulin joihinkin taulukoihin.

Keksinnön mukaisella järjestelmällä sekä vastaanottimella ja turvamodulilla saadaan toteutettua paremmin hallittavissa oleva video-, audio- ja datapalvelujen lähetys- ja vastaanottojärjestelmä, joka samalla vaikeuttaa salattujen palveluiden luvaton vastaanottoa.

∴

Patenttivaatimukset

1. Järjestelmä video-, audio- ja datapalveluja niiden vastaanottoon oikeutetuille vastaanottimille lähettävien eri hallintajärjestelmien kontrolloimiseksi, jossa kukin hallintajärjestelmä suorittaa lähettämänsä palvelun salauksen, salauksen purkamiseen vastaanottimessa tarvittavien avainten lähettämisen salattuna ja valtuutusviestien lähetyksen, jotka valtuutusviestit sisältävät ainakin tiedot niistä ohjelmista, jotka vastaanottaja voi purkaa, **tunnettu** siitä, että ainakin yksi hallintajärjestelmä on nimetty kontrollijärjestelmäksi, jolla on oikeus kontrolloida muiden hallintajärjestelmien käyttämiä salausalgoritmeja ja avainten sekä valtuutusviestien lähetystä, jolloin kontrollijärjestelmä voi muuttaa muiden hallintajärjestelmien käyttöoikeuksia vastaanottimessa.
2. Patenttivaatimuksen 1 mukainen järjestelmä, **tunnettu** siitä, että mainitulla ainakin yhdellä kontrollijärjestelmällä voidaan hallita myös kontrollijärjestelmiä, jolloin mainituilla kontrollijärjestelmillä voidaan nimetä uusia kontrollijärjestelmiä ja niitä voidaan poistaa.
3. Video-, audio- ja datapalveluja vastaanottava vastaanotin, joka käsittää dekooderin (51) salattujen video-, audio- ja datapalvelujen vastaanottamiseksi ja salauksen purkamiseksi, **tunnettu** siitä, että mainittu dekooderi (51) sisältää
- eri hallintajärjestelmiin liittyviä taulukoita (53), joista kukin sisältää hallintajärjestelmän käyttämän algoritmilistan (55), joka käsittää luettelon käytössä olevista salausalgoritmeista, joilla hallintajärjestelmän viestit ja palvelut on salattu,
 - hallintajärjestelmien kontrollitaulukon (54), joka sisältää luettelon kontrollijärjestelmistä.
4. Patenttivaatimuksen 3 mukainen vastaanotin, **tunnettu** siitä, että se käsittää irrotettavan turvamodulin (52), joka sisältää myös
- eri hallintajärjestelmiin liittyviä taulukoita (53), joista kukin sisältää hallintajärjestelmän käyttämän algoritmilistan (55), joka käsittää luettelon käytössä olevista salausalgoritmeista, joilla hallintajärjestelmän viestit ja palvelut on salattu,
 - hallintajärjestelmien kontrollitaulukon (54), joka sisältää luettelon kontrollijärjestelmistä.
5. Patenttivaatimuksen 3 tai 4 mukainen vastaanotin, **tunnettu** siitä, että kukin hallintajärjestelmään liittyvä taulukko (53) sisältää lisäksi hallintajärjestelmän versioluettelon (56), joka sisältää luettelon niistä siihen liittyvän hallintajärjestelmän (53) versioista, jotka ovat käytössä.

6. Patenttivaatimuksen 3 tai 4 mukainen vastaanotin, **tunnettu** siitä, että algoritmiluettelon (55) jokaiseen algoritmiin liittyy ensimmäinen tieto (OWN SEL) siitä, onko algoritmi hallintajärjestelmän omassa käytössä, ja toinen tieto (CTRL_SYS SELECTION) siitä, onko algoritmi kontrollijärjestelmän käytössä.

5

7. Patenttivaatimuksen 6 mukainen vastaanotin, **tunnettu** siitä, että kontrollijärjestelmä päättää, suoritetaanko algoritmin valinta kontrollijärjestelmän toimesta vai hallintajärjestelmän toimesta.

10 8. Patenttivaatimuksen 5 mukainen vastaanotin, **tunnettu** siitä, että jokaiseen hallintajärjestelmän versioluettelossa (56) mainittuun hallintajärjestelmän (53) versioon liittyy ensimmäinen tieto (OWN SEL) siitä, onko versio valittavissa hallintajärjestelmän käyttöön hallintajärjestelmän toimesta, ja toinen tieto (CTRL_SYS SELECTION) siitä, onko versio valittavissa hallintajärjestelmän käyttöön kontrollijärjestelmän toimesta.

15

9. Patenttivaatimuksen 3 tai 4 mukainen vastaanotin, **tunnettu** siitä, että kontrollijärjestelmä päättää, suoritetaanko version valinta kontrollijärjestelmän toimesta vai hallintajärjestelmän toimesta.

20

10. Patenttivaatimuksen 3 tai 4 mukainen vastaanotin, **tunnettu** siitä, että hallintajärjestelmien kontrollitaulukko (54) sisältää ensimmäisen luettelon (CA_SYSTEM NOT IN USE), joka ilmaisee ne hallintajärjestelmät, jotka eivät ole vastaanottimen käytössä, ja toisen luettelon (CA_SYSTEM IN USE), joka ilmaisee hallintajärjestelmät, jotka ovat vastaanottimen käytössä.

25

11. Patenttivaatimuksen 3, 4 tai 10 mukainen vastaanotin, **tunnettu** siitä, että hallintajärjestelmien kontrollitaulukko (54) sisältää luettelon (CONTROL CA_SYSTEM IN USE), joka ilmaisee ne hallintajärjestelmät, jotka ovat kontrollijärjestelmiä.

30

12. Patenttivaatimuksen 11 mukainen vastaanotin, **tunnettu** siitä, että mainittuun kontrollijärjestelmäluetteloon liittyy turvajärjestely, joka varmistaa, että ainakin yksi kontrollijärjestelmä on sellainen, jota ei voi poistaa luettelosta.

35

13. Patenttivaatimuksen 3 tai 4 mukainen vastaanotin, **tunnettu** siitä, että hallintajärjestelmien taulukkojen (53) tiedot ja hallintajärjestelmien kontrollitaulukon (54) tiedot tallennetaan vastaanottimeen sen valmistuksen yhteydessä.
- 5 14. Patenttivaatimuksen 13 mukainen vastaanotin, **tunnettu** siitä, että hallintajärjestelmien taulukkojen (53) tiedot ja hallintajärjestelmien kontrollitaulukon (54) tiedot voidaan päivittää vastaanotetun datan mukana tulevilla salatuilla viesteillä.
- 10 15. Patenttivaatimuksen 13 mukainen vastaanotin, **tunnettu** siitä, että hallintajärjestelmien taulukkojen (53) tiedot ja hallintajärjestelmien kontrollitaulukon (54) tiedot voidaan päivittää vastaanottimeen kytkettävällä älykortilla.
- 15 16. Patenttivaatimuksen 15 mukainen vastaanotin, **tunnettu** siitä, että se käsittää liitännän älykortin kytkemiseksi turvamoduliin (52).
17. Patenttivaatimuksen 4, 15 tai 16 mukainen vastaanotin, **tunnettu** siitä, että vastaanotin (51) sisältää tiedon siitä, minkälaisia turvamoduleja ja älykortteja vastaanottimeen voidaan liittää.
- 20 18. Jonkin patenttivaatimuksen 3 - 17 mukainen vastaanotin, **tunnettu** siitä, että tiettyä palvelua vastaanotettaessa käytetään viestien purkamiseen pelkästään vastaanottimeen (51) tallennettuja tietoja.
- 25 19. Jonkin patenttivaatimuksen 3 - 17 mukainen vastaanotin, **tunnettu** siitä, että tiettyä palvelua vastaanotettaessa käytetään viestien purkamiseen pelkästään turvamoduliin (52) tallennettuja tietoja.
- 30 20. Jonkin patenttivaatimuksen 3 - 17 mukainen vastaanotin, **tunnettu** siitä, että tiettyä palvelua vastaanotettaessa käytetään viestien purkamiseen sekä turvamoduliin (52) että vastaanottimeen (51) tallennettuja tietoja.
- 35 21. Irrotettava turvamoduli (52) video-, audio- ja datapalveluja vastaanottavaa vastaanotinta varten, joka käsittää dekooderin (51) salattujen video-, audio- ja datapalvelujen vastaanottamiseksi ja salauksen purkamiseksi, joka turvamoduli käsittää tietoja dekooderia varten salatun palvelun salauksen purkamiseksi, **tunnettu** siitä, että se sisältää
- eri hallintajärjestelmiin liittyviä taulukoita (53), joista kukin sisältää hallintajärjestelmän käyttämän algoritmilistan (55), joka käsittää luettelon käytössä olevista sa-

lausalgoritmeista, joilla hallintajärjestelmän viestit ja palvelut on salattu,
 - hallintajärjestelmien kontrollitaulukon (54), joka sisältää luettelon kontrollijärjestelmistä.

- 5 22. Patenttivaatimuksen 21 mukainen turvamoduli, **tunnettu** siitä, että se sisältää tiedon siitä, minkälaiseen vastaanottimeen se voidaan liittää.

Patentkrav

1. System för att kontrollera olika hanteringssystem som sänder video-, audio-
 10 och datatjänster till behöriga mottagare, vid vilket respektive hanteringssystem utför chiffrering av den tjänst den utsänt, utsändning av nycklar i chiffrerad form som behövs för dechiffrering i mottagaren och utsändning av behörighetssignaler, vilka innehåller åtminstone data om de program som mottagaren kan dekodera, **kännetecknat** av att åtminstone ett hanteringssystem utsetts till kontrollsystem, som har rätt att
 15 kontrollera chiffreringsalgoritmer som de övriga hanteringssystemen använder och utsändning av nycklar och behörighetssignaler, varvid kontrolsystemet kan ändra de övriga hanteringssystemens behörighet i mottagaren.

2. System enligt patentkrav 1, **kännetecknat** av att med nämnda åtminstone ena
 20 kontrollsystem kan man hantera även de övriga kontrollsystemen, så att man med nämnda kontrollsystem kan utse och avskriva nya kontrollsystem.

3. Mottagare som mottar video-, audio- och datatjänster, omfattande en dekodare
 (51) för att motta chiffrerade video-, audio- och datatjänster och för att dechiffrera
 25 dem, **kännetecknad** av att nämnda dekodare (51) innehåller
 - tabeller (53) i anslutning till de olika hanteringssystemen, av vilka var och en innehåller en av hanteringssystemet anlitad algoritmlista (55) omfattande en förteckning av använda chiffreringsalgoritmer, med vilka hanteringssystemets signaler och tjänster chiffrerats,
 30 - en kontrolltabell (54) för hanteringssystemet, som innehåller en förteckning av kontrollsystemen.

4. Mottagare enligt patentkrav 3, **kännetecknad** av att den omfattar en löstagbar säkerhetsmodul (52), som även innehåller
 35 - tabeller (53) i anslutning till hanteringssystemen av vilka var och en innehåller en av hanteringssystemet anlitad algoritmlista (55) som omfattar en förteckning över använda chiffreringsalgoritmer, med vilka hanteringssystemets signaler och tjänster chiffrerats,

- hanteringssystemens kontrolltabell (54), som innehåller en förteckning över kontrollsyste-
rollsystemen.

- 5 5. Mottagare enligt patentkrav 3 eller 4, **kännetecknad** av att varje tabell (53) i
anslutning till hanteringssystemet innehåller även hanteringssystemets versionsför-
teckning (56) som innehåller en förteckning över de versioner av hanteringssystemet
(53) som är i användning.
- 10 6. Mottagare enligt patentkrav 3 eller 4, **kännetecknad** av att till varje algoritm i
algoritmförteckningen (55) hör ett första data (OWN SEL) som anger om algoritmen
är i hanteringssystemets eget bruk, och ett andra data (CTRL_SYS SELECTION)
som anger om algoritmen är i kontrollsysteemets bruk.
- 15 7. Mottagare enligt patentkrav 6, **kännetecknad** av att kontrollsysteemet avgör om
valet av algoritim skall göras av kontrollsysteemet eller hanteringssystemet.
- 20 8. Mottagare enligt patentkrav 5, **kännetecknad** av att till varje version av han-
teringssystemet (53) nämnt i hanteringssystemets versionförteckning (56) hör ett
första data (OWN SEL) som anger om versionen kan väljas i hanteringssystemets
bruk av hanteringssystemet, och ett andra data (CTRL_SYS SELECTION) som
25 anger om versionen kan väljas i hanteringssystemets bruk av kontrollsysteemet.
- 30 9. Mottagare enligt patentkrav 3 eller 4, **kännetecknad** av att kontrollsysteemet
avgör om valet av version skall göras av kontrollsysteemet eller hanteringssystemet.
- 35 10. Mottagare enligt patentkrav 3 eller 4, **kännetecknad** av att hanteringssyste-
mens kontrolltabell (54) innehåller en första förteckning (CA_SYSTEM NOT IN
USE) som anger de hanteringssystem som inte är i mottagarens bruk, och en andra
förteckning (CA_SYSTEM IN USE) som anger de hanteringssystem som är i mot-
tagarens bruk.
- 35 11. Mottagare enligt patentkrav 3 eller 4, **kännetecknad** av att hanteringssyste-
mens kontrolltabell (54) innehåller en förteckning (CONTROL CA_SYSTEM IN
USE) som anger de hanteringssystem som är kontrollsysteem.
- 35 12. Mottagare enligt patentkrav 11, **kännetecknad** av att till nämnda kontrollsys-
temförteckning hör ett säkerhetssystem, som säkerställer att åtminstone ett kontroll-
system är sådant som inte kan strykas ur förteckningen.

13. Mottagare enligt patentkrav 3 eller 4, **kännetecknad** av att data i hanteringssystemens tabeller (53) och data i hanteringssystemens kontrolltabell (54) registreras i mottagaren vid tillverkningen.
- 5 14. Mottagare enligt patentkrav 13, **kännetecknad** av att data i hanteringssystemens tabeller (53) och data i hanteringssystemens kontrolltabell (54) kan uppdateras med chiffrerade meddelanden som följer med mottagna data.
- 10 15. Mottagare enligt patentkrav 13, **kännetecknad** av att data i hanteringssystemens tabeller (53) och data i hanteringssystemens kontrolltabell (54) kan uppdateras med ett smartkort kopplat till mottagaren.
- 15 16. Mottagare enligt patentkrav 15, **kännetecknad** av att den omfattar ett gränssnitt för att koppla smartkortet till säkerhetsmodulen (52).
- 20 17. Mottagare enligt patentkrav 4, 15 eller 16, **kännetecknad** av att mottagaren (51) innehåller data som anger vilket slags säkerhetsmoduler och smartkort som kan anslutas till mottagaren.
- 20 18. Mottagare enligt något av patentkraven 3-17, **kännetecknad** av att vid mottagning av en viss tjänst används endast data lagrade i mottagaren (51) för dekodning av signalerna.
- 25 19. Mottagare enligt något av patentkraven 3-17, **kännetecknad** av att vid mottagning av en viss tjänst används endast data lagrade i säkerhetsmodulen (51) för dekodning av signalerna.
- 30 20. Mottagare enligt något av patentkraven 3-17, **kännetecknad** av att vid mottagning av en viss tjänst används såväl data lagrade i säkerhetsmodulen (51) som data lagrade i mottagaren (51) för dekodning av signalerna.
- 35 21. Löstagbar säkerhetsmodul (52) för en mottagare av video-, audio- och data-tjänster, omfattande en dekodare (51) för att ta emot och dechiffrera chiffrerade video-, audio- och datatjänster, varvid säkerhetsmodulen omfattar data för dekodaren för dechiffrering av en chiffrerad tjänst, **kännetecknad** av att den innehåller - tabeller (53) i anslutning till de olika hanteringssystemen, av vilka var och en innehåller en av hanteringssystemet använd algoritmlista (55), som omfattar en förteck-

ning över chiffreringsalgoritmer i bruk, med vilka hanteringssystemets signaler och tjänster chiffrerats,

- hanteringssystemens kontrolltabell (54), som innehåller en förteckning över kontrollsyste-
men.

5

22. Säkerhetsmodul enligt patentkrav 21, kännetecknad av att den innehåller data som anger till vilket slags mottagare den kan anslutas.

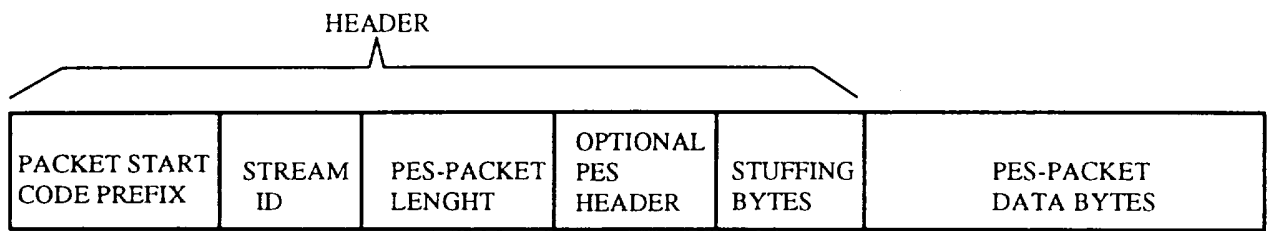


FIG. 1

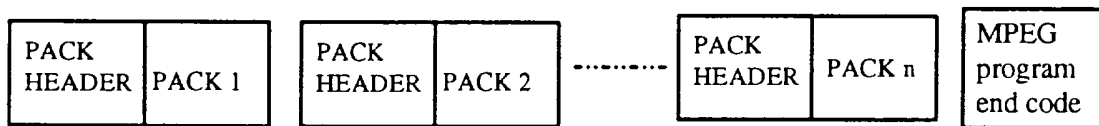


FIG. 2 a

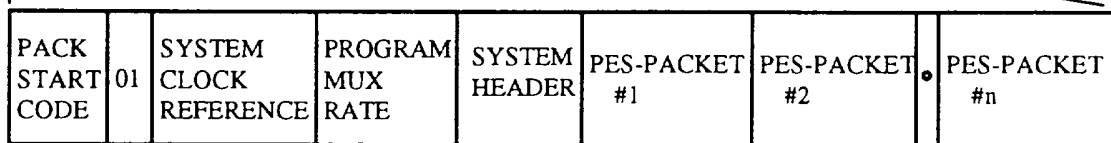


FIG. 2 b

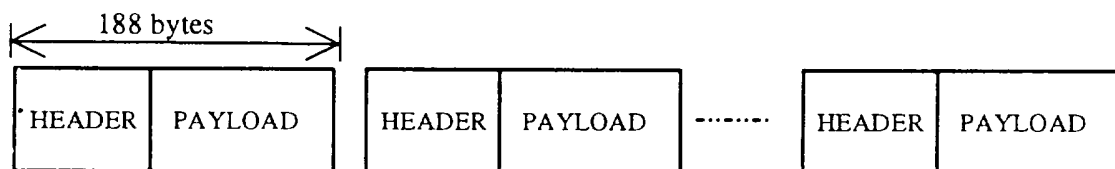


FIG. 3 a

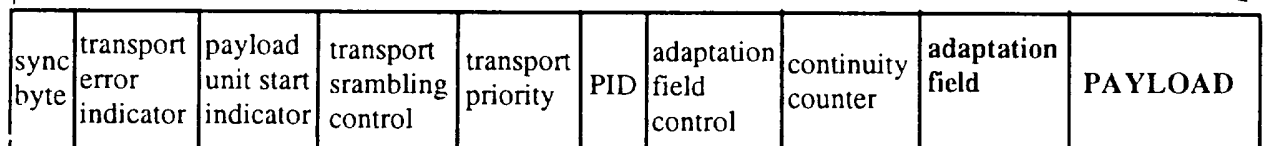


FIG. 3 b

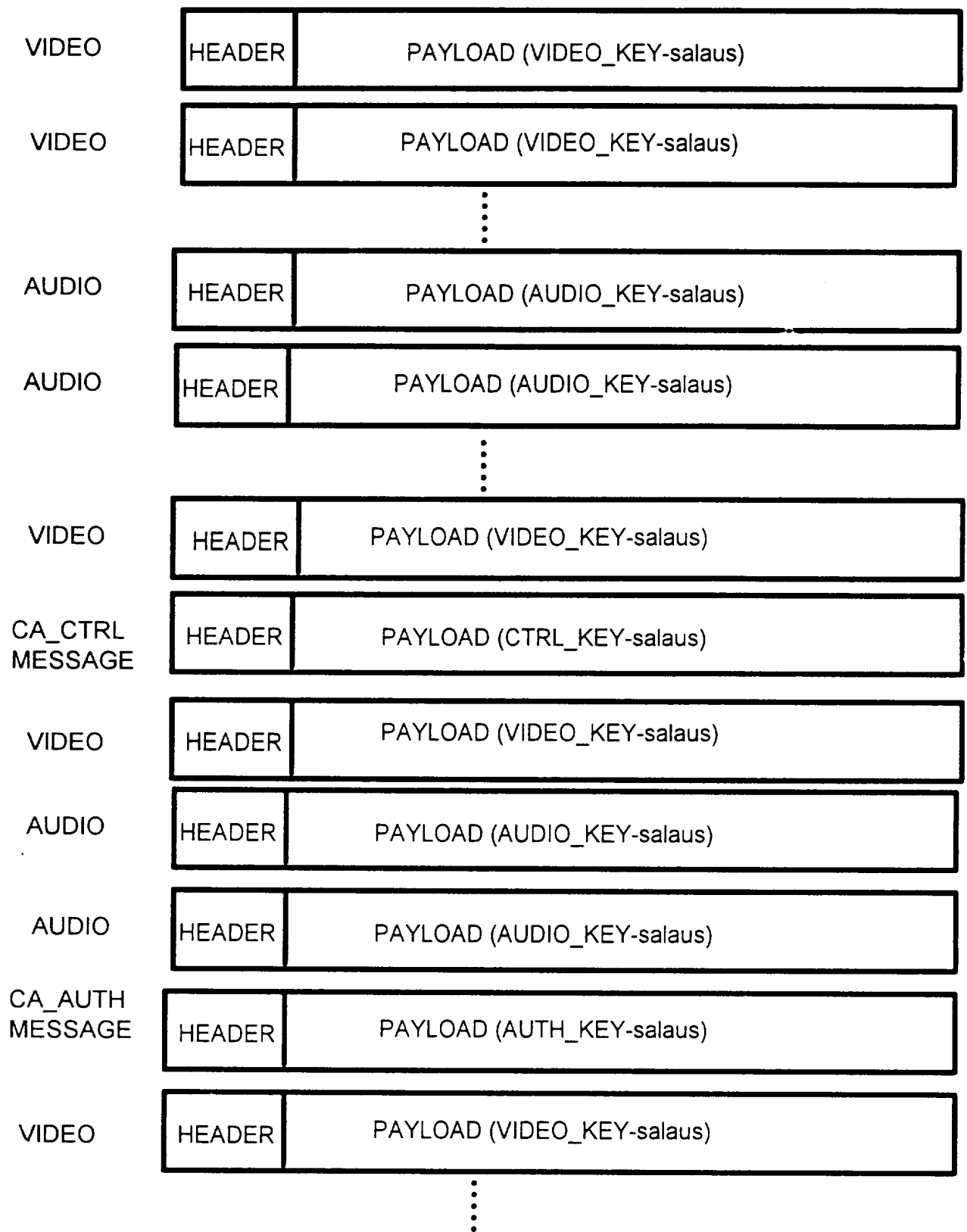


FIG. 4

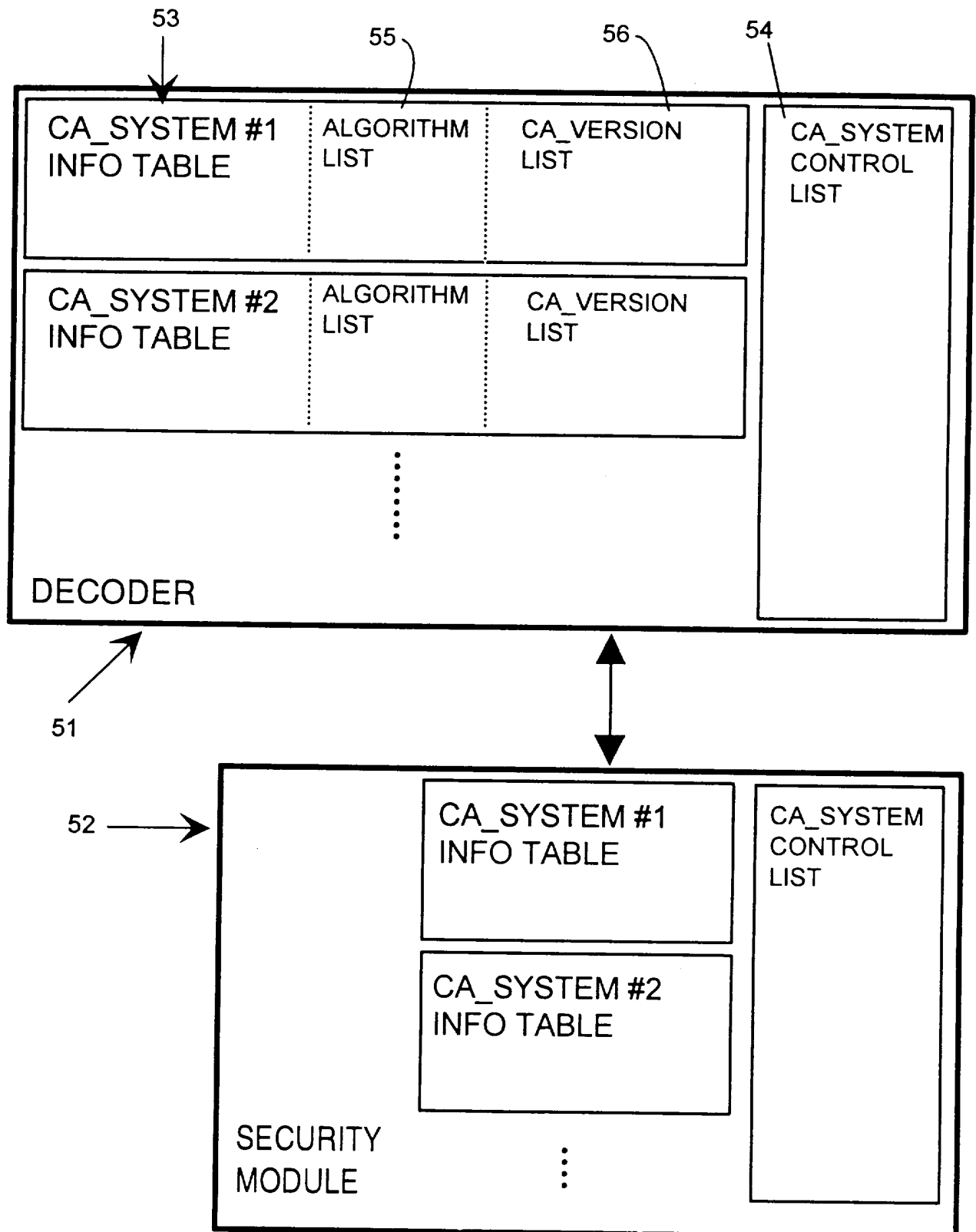


FIG. 5

55

CA_SYSTEM INFO TABLE, ALGORITHM LIST		
ALGORITHM	OWN SEL	CTRL_SYS SELECTION
ALG #1	X	X
ALG #2		X
ALG #3	X	X
⋮		
ALG_SELECTION		CTRL_SYS

FIG. 6 A

56

CA_SYSTEM INFO TABLE, CA_VERSION LIST		
CA_SYSTEM VERSION	OWN SEL	CTRL_SYS SELECTION
VER #1	X	X
VER #2		
VER #3		X
⋮		
VER_SELECTION		CTRL_SYS

FIG. 6 B

54

CA_SYSTEM CONTROL LIST		
CA_SYSTEM IN USE	CA_SYSTEM NOT IN USE	CONTROL CA_SYSTEM IN USE
SYS #1	SYS #2	SYS #1
SYS #3	SYS #4	SYS #5
SYS #5	SYS #6	
⋮	⋮	⋮

FIG. 7