Mikko Hänninen

# Ohjelman välitys ja salaus IPTV-järjestelmässä

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

23.5.2017

Metropolia

| | |
|---|---|
| Tekijä(t)<br>Otsikko<br><br>Sivumäärä<br>Aika | Mikko Hänninen<br>Ohjelman välitys ja salaus IPTV-järjestelmässä<br><br>30 sivua<br>23.5.2017 |
| Tutkinto | Insinööri (AMK) |
| Koulutusohjelma | Tietotekniikka |
| Suuntautumisvaihtoehto | Ohjelmistotekniikka |
| Ohjaaja | yliopettaja Jouko Kurki |


IPTV on internetprotokollan käyttöön perustuva television jakelutapa. Televisioverkkojen kehitys analogisista digitaalisiin ja internetyhteyksien tiedonsiirtonopeuksien kasvu ovat mahdollistaneet IPTV-järjestelmien toteuttamisen. IPTV:ssä voidaan välittää tavallisia televisiokanavia sekä teräväpiirtokanavia.

Tässä insinöörityössä on perehdytty IPTV-järjestelmissä käytettäviin salausmenetelmiin. Salauksella estetään välitettävän sisällön laiton kopiointi. IPTV-ssä käytetään AES-salaustekniikkaa. Työssä on tutkittu symmetristä ja epäsymmetristä salaustekniikkaa ja avainten hallintaa sekä perehdytty sisällön oikeuksienhallintajärjestelmään (DRM). DRM on yleiskäsite IPTV-järjestelmissä käytetyille suojausmenetelmille.

Symmetrisen salauksen etuna on salauksen nopeus. Avainten jakelu on symmetrisessä salauksessa ongelmallinen. Mikäli avainta joudutaan jostakin syystä vaihtamaan, avainten toimittaminen kaikille käyttäjille erikseen on hankalaa ja kallista. Epäsymmetrisessä salauksessa salaiset avaimet luodaan paikallisesti, jolloin vastaavaa ongelmaa ei ole. Hybrid Encryption on symmetrisen ja epäsymmetrisen salaustekniikan yhdistelmä. Tämä salaus käyttää sattumanvaraisesti luotua symmetristä avainta, joka salataan vastaanottajan julkisen avaimen kanssa. Tällä menettelyllä varmistetaan, että vain vastaanottajalla on salauksen purkamiseen tarvittava salainen avain. Symmetrisellä salauksella saadaan tehostettua salausta. Epäsymmetrisen salauksen ansiosta avaimenhallinta on helppoa.



| | |
|---|---|
| Avainsanat | IPTV, Symmetrinen salaus, PKE, PKI, ECM, EMM, DRM |

| | |
|---|---|
| Author(s)<br>Title<br><br>Number of Pages<br>Date | Mikko Hänninen<br>Program distribution and encryption at IPTV systems<br><br>35 pages<br>23, May 2017 |
| Degree | Bachelor of Engineering |
| Degree Programme | Information technology |
| Specialisation option | Software technology |
| Instructor(s) | Jouko Kurki, Principal Lecturer |

This Bachelor thesis examines encryption methods that are used in IPTV-systems. The study also introduces the IPTV-system architecture. Both symmetrical and asymmetrical encryption methods and encryption key management are examined. Encryption is important because it prevents illegal copying of valuable data. The IPTV-system uses an efficient encryption algorithm called Advanced Encryption Standard (AES). AES is a reliable encryption method.

Digital Rights Management (DRM) is also studied. DRM is a universal term for protection methods used in IPTV-systems. The IPTV system architecture is presented.

| | |
|---|---|
| Keywords | IPTV, Symmetrical encryption, PKE, PKI, ECM, EMM, DRM |

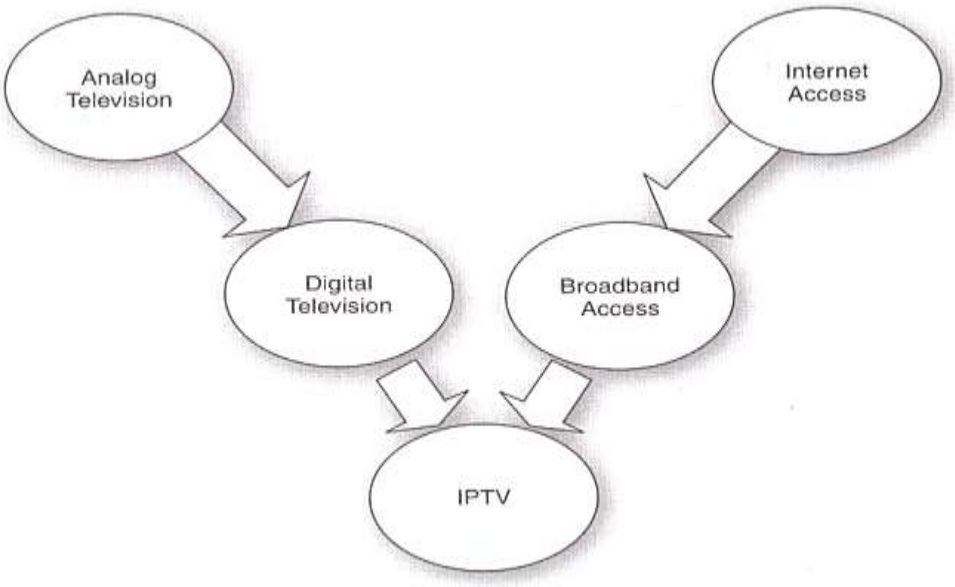
## Sisällys

## Lyhenteet

| | |
|---|---|
| AES | Advanced Encryption Standard |
| CAM | Conditional Access module |
| CA | Certificate Authority |
| CAS | Conditional Access System |
| CRL | Certificate Revocation List |
| DES | Data Encryption Standard |
| DRM | Digital Rights Management |
| ECM | Entitlement Control Message |
| EMM | Entitlement Management Message |
| HTTP | Hypertext Transfer Protocol |
| MAC | Message Authentication Code |
| P2P | Peer to Peer |
| PC | Personal Computer |
| PDA | Personal Digital Assistant |
| PKE | Public Key Encryption |
| PKI | Public Key Infrastructure |
| REL | Rights Expression Language |
| SSL | Secure Socket Layer |
| STB | Set-top Box |
| VOD | Video On Demand |

# 1 Johdanto

IPTV (Internet Protocol TV) on internetprotokollan käyttöön perustuva television jakelutapa. Televisioverkkojen kehitys analogisista digitaalisiin ja internetyhteyksien tiedonsiirtonopeuksien kasvu ovat mahdollistaneet IPTV-järjestelmien toteuttamisen. IPTV:ssä voidaan välittää tavallisia televisiokanavia (Standard Definition, SD) sekä teräväpiirtokanavia (High Definition, HD). Kuvassa 1 on havainnollistettu IPTV:n kehitystä.




Kuva 1. IPTV:n kehitys [4, XIV]

Tässä työssä käsitellään IPTV:n salausmenetelmiä. Työssä perehdytään symmetriseen ja epäsymmetriseen salaukseen, yksityisen ja julkisen avaimen toimintaperiaatteisiin sekä keskeisiin salaustekniikoihin: SSL (Secure Socket Layer, SSL) ja TLS (Transport Layer Security, TLS). Työssä käsitellään myös sisällön oikeuksienhallintajärjestelmää (Digital Rights Management, DRM). Menetelmää käytetään tiedon suojaamiseen IPTV-järjestelmissä.

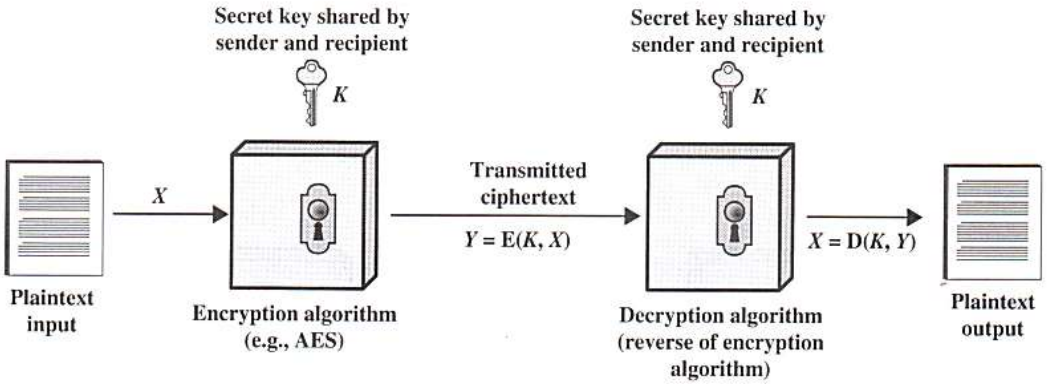
# 2 Salaustekniikat

Tässä luvussa perehdytään symmetriseen ja epäsymmetriseen salaukseen ja käydään läpi salauksen perusperiaatteita. Luvussa selvitetään myös salaustekniikoiden hyviä ja huonoja ominaisuuksia.

## 2.1 Symmetrinen ja epäsymmetrinen salaus

Symmetrinen salaus kehitettiin 1970-luvulla ja oli pitkään käytetyin salausalgoritmi. Käytetyimpiä symmetrisiä salausmenetelmiä ovat mm. DES-salausalgoritmi (Data Encryption Standard, DES) ja AES-salausalgoritmi (Advanced Encryption Standard, AES). [9, 48.]

Symmetrisen salauksen etuna on salaamisen nopeus. Salaus on kymmenen kertaa nopeampi verrattuna epäsymmetriseen salaukseen. Symmetrisen salauksen huonoina puolina ovat avainten hallinta ja niiden jakelu. Järjestelmän päivittämisen ja teknologian skaalautuvuuden toteuttaminen ovat ongelmallisia symmetrisessä salauksessa, jolloin järjestelmien uudistaminen on hankalaa. [8, 73.] Kuvassa 2 on esitetty symmetrisen salauksen toiminta.




Kuva 2. Symmetrinen salauskaavio [4, s. 49]

**Selkoteksti (Plaintext):** Selkokielinen teksti, joka halutaan lähettää (merkintä *X*)

**Salausalgoritmi:** Algoritmi, joka suorittaa salaukseen tarvittavat muutokset ja siirrot selkotekstiin (vasemmanpuoleinen laatikko).

**Salainen avain:** Avain on riippumaton salausalgoritmista ja selkotekstistä. Avaimen vaihtuessa algoritmi tuottaa eri lopputuloksen. Kuvassa tämä on merkitty kirjaimella *K*.

**Salattu teksti:** Teksti on salattu salausalgoritmilla. Kahdella eri avaimella saadaan erilainen lopputulos. Kuvassa tämä on merkitty kirjaimella *Y*.

**Salauksen purkualgoritmi:** Algoritmi, joka purkaa salatun tekstin takaisin selkotekstiksi (oikeanpuoleinen laatikko).

Salauksen pitää olla minimissään niin vahva, että salakuuntelija ei voi päätellä kaappaamistaan salatuista viesteistä salausavainta. Lähettäjän ja vastaanottajan pitää lähettää salausavain turvallista väylää pitkin ja pitää avain salassa. Mikäli avain paljastuu ja algoritmi on tiedossa, kaikki salattu liikenne on tämän jälkeen luettavissa.

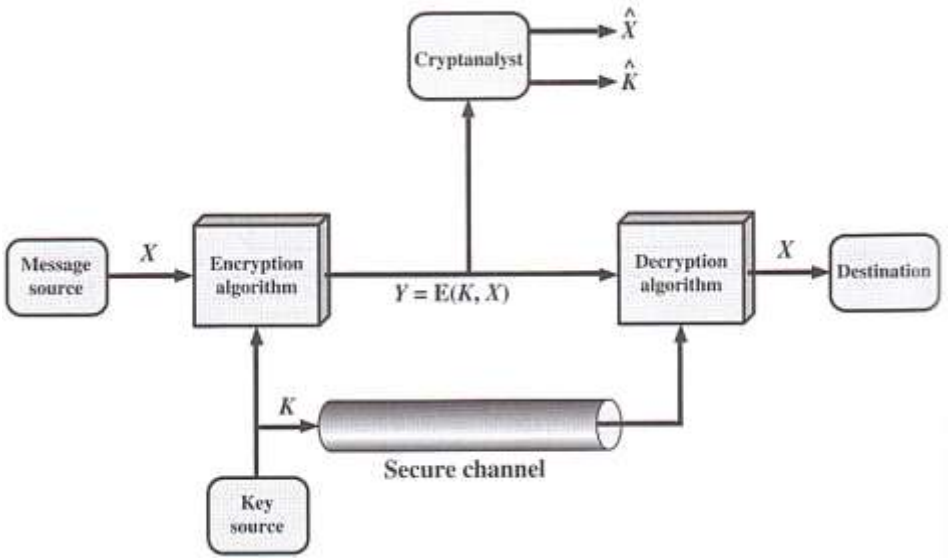
Kuvassa 3 on selvitetty selkotekstin eri vaiheet. Viesti *X* ja salausavain *K* syötetään salausalgoritmiin E, ja se muodostaa salatun tekstin, jota merkitään *Y*:llä.

$$Y = E(K, X)$$

Vastaavasti salatun tekstin purku merkitään *X*:llä. *D* symboloi salauksen purkualgoritmia.

$$X = D(K, Y)$$

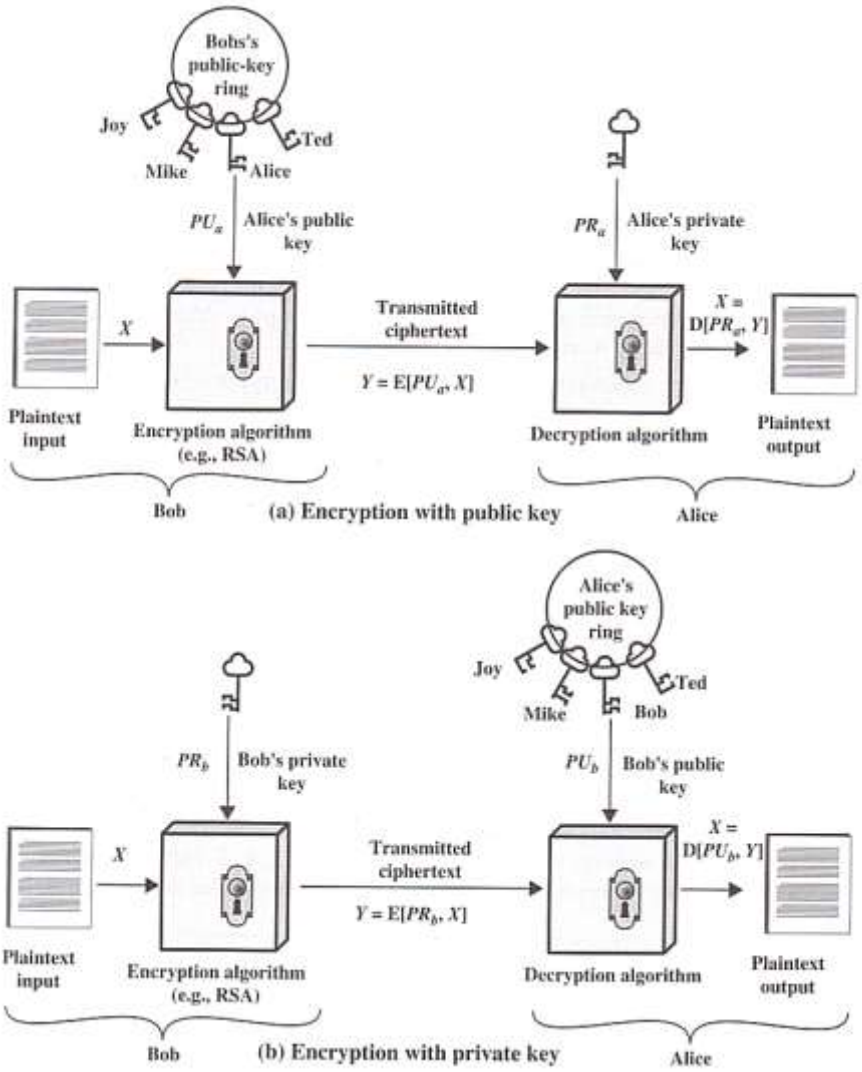
Lähettäjä tai kolmas osapuoli luo salausavaimen *K*. Avain toimitetaan turvallista kanavaa pitkin lähettäjälle. Tähän voidaan käyttää salausprotokollaa (Secure Socket Layer,SSL). Jos salakuuntelija haluaa saada yksittäisen viestin selville, hän käyttää salausanalyysia. Tätä varten luodaan arvioitu selkoteksti X^. Mikäli salakuuntelija haluaa saada selville kaiken liikenteen lähettäjän ja vastaanottajan välillä, tätä tarkoitusta varten luodaan arvioitu avain K^. Salausavain saattaa olla mahdollista selvittää kokeilemalla valtava määrä vaihtoehtoja. Nykyisillä tietokonetehoilla tämä ei ole käytännössä mahdollista.




Kuva 3. Symmetrinen salausjärjestelmä [4, s. 50]

## 2.2 Julkisen avaimen periaate

Symmetristä salaustekniikkaa käytettiin 1970:lle saakka, jolloin keksittiin julkisen avaimen salaus. Tässä salauksessa julkinen avain on kaikkien tiedossa, mutta salaiset avaimet ovat vain lähettäjän ja vastaanottajan tiedossa. Asymmetriset salaustekniikat käyttävät salaukseen yhtä avainta ja viestin salauksen purkamiseen eri mutta samaa sukua olevaa avainta. Purkuavaimen määrittäminen salausavaimen ja salausalgoritmin avulla on laskennallisesti mahdotonta. Lisäksi kumpaakin kahdesta samaa sukua olevasta avaimesta voidaan käyttää salaamiseen, kun toista käytetään salauksen purkuun. Kuvassa 4 on esitetty julkisen avaimen salaus kahdella eri tavalla: salaaminen käyttäen julkista avainta ja salaaminen käyttäen salaista avainta.




Kuva 4. Julkisen avaimen salaus [4, s. 277]

Kuvan 4 esimerkissä (a) Bob haluaa lähettää viestin Alicelle käyttäen salauksessa julkista avainta. Selkokielinen teksti merkitään kirjaimella $X$. Salausalgoritmi salaa selkokielisen tekstin käyttäen Alicen julkista avainta, jota merkitään kirjainyhdistelmällä $PU_a$. Muodostettuna on avainpari, josta toinen on salausta varten ja toinen salauksen purkua varten. Salatun tekstin muoto vaihtelee käytettävän avaimen ja selkotekstin mukaan. Eri avainta käytettäessä salatun tekstin muoto tulee muuttumaan.

Salattua tekstiä merkitään kirjaimella *Y* muodossa:

$$Y = E[PU_{a,}X]$$

Alice vastaanottaa viestin ja käyttää omaa salaista avaintaan salatun viestin salauksen purkamiseen. Alicen salaista avainta merkataan $PR_a$. Salauksen purkaminen merkitään muodossa

$$X = D[PR_a, Y]$$

Kuvan 4 esimerkissä (b) Bob haluaa lähettää viestin Alicelle käyttäen salaukseen salaista avaintaan $PR_b$. Selkokielistä tekstiä merkitään samalla kirjaimmella $X$. Salausalgorimi salaa selkotekstin ja salattua viestiä merkitään

$$Y = E[PR_b, X]$$

Alice valitsee Bobin julkisen avaimen, syöttää sen salauksen purkualgoritmille ja purkaa salauksen. Tämän jälkeen alkuperäinen teksti on Alicen luettavissa. Purkua kuvataan muodossa

$$X = D[PU_b, Y]$$

Jokainen käyttäjä luo avainparit, joita käytetään viestien salaamiseen ja salauksen purkamiseen. Käyttäjä toimittaa toisen avaimista julkiseen rekisteriin tai vastaavaan. Tästä avaimesta tulee käyttäjän julkinen avain. Kuvassa 4 julkisia avaimia ovat Alicen $PU_a$ ja Bobin $PU_b$. Alicen on turvallista purkaa viesti omalla salaisella avaimellaan $PR_a$, koska avain on vain Alicen itsensä tiedossa.

Kaikilla osapuolilla on mahdollisuus päästä käsiksi julkisiin avaimiin. Yksityiset avaimet luodaan paikallisesti, eikä yksityisiä avaimia tarvitse jakaa kuten symmetrisessä salauksessa. Yksityinen avain pystytään pitämään salassa muilta käyttäjiltä, jolloin tietoliikenne on turvallista. Jos yksityinen avain paljastuu, tietoliikenne ei ole enää turvallinen. Yksityistä avainta voidaan vaihtaa tarvittaessa, jolloin systeemi korvaa vanhan julkisen avaimen uudella julkisella avaimella.

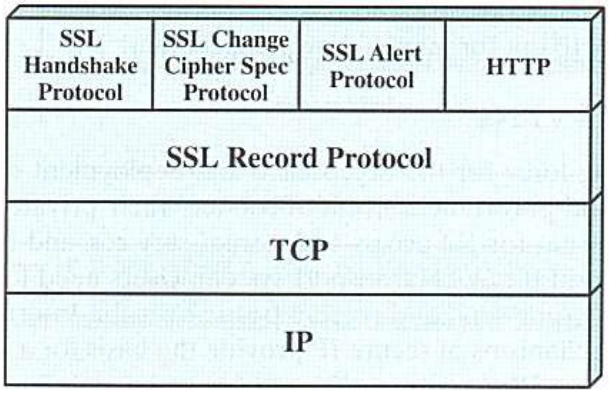
Taulukko 1. Symmetrisen ja asymmetrisen salauksen erot [4, 279]

| **Symmetrinen salaus** | **Asymmetrinen salaus** |
|---|---|
| **Toimimisen edellytykset** | **Toimimisen edellytykset** |
| Sama algoritmi käyttäen samaa avainta salaa ja purkaa salauksen. | Yhtä algoritmia käytetään salaukseen ja samaa sukua olevaa algoritmia salauksen purkamiseen käyttäen avainparia. Yksi avaimista on salaamista varten ja toinen salauksen purkamista varten. |
| Lähettäjällä ja vastaanottajalla täytyy olla sama algoritmi ja avain. | Lähettäjällä ja vastaanottajalla täytyy olla yksi avain yhteensopivasta avainpareista (Ei tarvitse olla sama). |
| **Yhteyden pysyminen turvallisena: edellytykset** | **Yhteyden pysyminen turvallisena: edellytykset** |
| Avaimen pitää pysyä salassa | Toisen kahdesta avaimesta pitää pysyä salassa. |
| On mahdotonta tai epäkäytännöllistä purkaa salausta, jos avain pysyy salassa. | On mahdotonta tai epäkäytännöllistä purkaa salaus jos yksi avaimista pysyy salassa. |
| Avaimen selvittämiseen ei riitä tiedossa oleva algoritmi ja salatusta tekstistä otetut näytteet. | Toisen avaimen selvittämiseen ei riitä tiedossa oleva algoritmi ja salatusta tekstistä otetut näytteet. |

## 2.3 SSL-salausprotokolla

Salausprotokolla Secure Socket Layer (SSL), joka tunnetaan myös nimellä Transport Layer Security (TLS), on käytetyimpiä salausprotokollia maailmassa.

SSL tallennusprotokolla (SSL Record Protocol) tuottaa turvapalveluita korkean tason protokollille. Näistä esimerkkinä (Hypertext Transfer Protocol, HTTP), joka tuottaa välityspalveluista Web-asiakkaalle (Client) / palvelimelle. Tämän tason yläpuolella ovat kättelyprotokolla (SSL Handshake Protocol), salaimenvaihtoprotokolla (SSL Change Cipher Spec Protocol) ja hälytysprotokolla (SSL Alert Protocol). Kaikki edellä mainitut protokollat on esitetty kuvassa 5.




Kuva 5. SSL-Protokolla pino [5. s. 800]

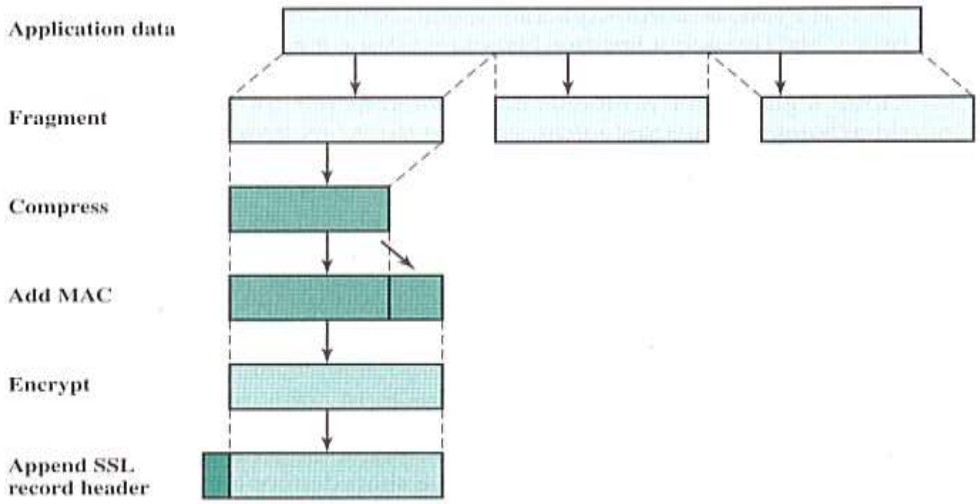
Kaksi tärkeintä käsitettä ovat SSL-sessio (SSL Session) ja SSL-yhteys (SSL Connection). SSL-yhteys on siirtokerroksen (Transport layer OSI-malli) tarjoaja, joka tuottaa tarvittavaa palvelua. Yhteydet voivat olla vertaisverkko (Peer to Peer, P2P) -yhteyksiä, jotka ovat tilapäisiä. Jokainen yhteys kommunikoi yhden session kanssa. SSL-sessio toimii asiakkaan ja palvelimen välillä. Kättelyprotokolla luo sessiot, jotka sisältävät kryptisiä parametrejä. Sessioissa käytetään samoja parametrejä, jotta vältytään uusien parametrien välitykseltä uusissa yhteyksissä.

Tallennusprotokolla

SSL-tallennusprotokolla tuottaa kahdenlaisia palveluita SSL-yhteyksiin.

**Tietosuoja (Confidentiality):** Kättelyprotokolla määrittää jaetun salaisen avaimen, jota käytetään SSL-kuorman epäsymmetriseen salaukseen.

**Viestin koskemattomuus (Message Integrity):** Kättelyprotokolla määrittää jaetun salaisen avaimen, jota käytetään muodostamaan MAC (Message Authentication Code, MAC). Kuvassa 6 on esitetty tallennusprotokolla.




Kuva 6. SSL-tallennusprotokolla [5. s. 802]

Ensimmäinen askel on tiedon jakaminen osiin (Fragmentation). Jokaisessa ylemmän tason viesti on jaettu 16,384 tavun lohkoihin. Lohkon koko voi olla myös tätä pienempi. Seuraava taso on pakkaaminen, jota ei aina välttämättä käytetä. Tämän jälkeen lasketaan MAC pakatusta datasta. Tämän jälkeen pakattu data ja MAC salataan käyttäen epäsymmetristä salausta. Lopuksi lisätään otsikko (SSL Record Header), joka sisältää seuraavat osat:

- Sisältötyyppi (Content Type) 8 bittiä: Ylätason protokolla käyttää fragmentin prosessoimiseen.

- Yläversio (Major Version) 8 bittiä: Kertoo mikä yläversio SSL:ssä on käytössä. SSLv3-arvo on 3.

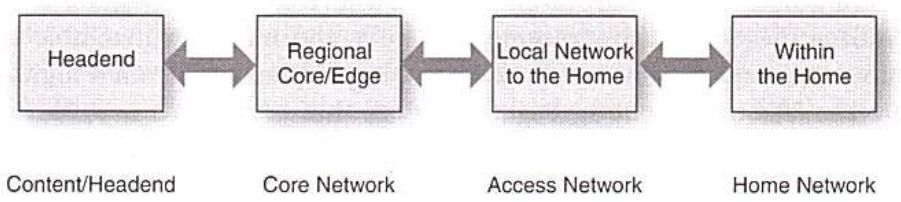
- Alaversio (Minor version) 8 Bittiä: Kertoo mikä alaversio SSL:ssä on käytössä. SSLv3- arvo on 0.

- Tiivistetty pituus (Compressed Length) 16 bittiä: Osiin jaetun selkotekstin pituus tavuissa (tai tiivistetty fragmentti, jos tiivistystä on käytetty) on maksimissan 16386 + 2048 tavua. [5, 800 – 802.]

# 3 IPTV:n salaustekniikat

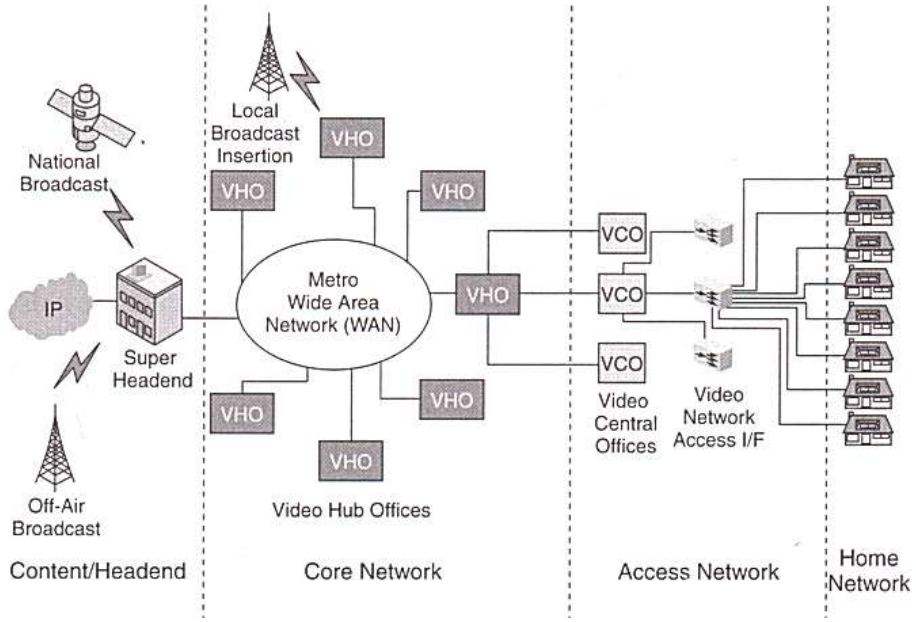
## 3.1 IPTV-järjestelmä

IPTV-järjestelmä koostuu monista erilaisista palveluista sekä kaapeli- sekä satelliitti-TV-lähetysten muokkaamisesta IPTV-muotoon katseltavaksi laitteilla, jotka on yhdistetty internetiin. IPTV-järjestelmässä käytetään monilähetyspalvelua (Multicast) TV-kanavien välitykseen. Palveluna voidaan käyttää täsmälähetyspalvelua (Unicast) tilausvideoiden (Video on Demand, VOD) välittämiseen (esimerkiksi sähköinen videovuokraamo). IPTV-lähetysverkko voidaan jakaa seuraaviin osioihin: lähetysasema (Headend), runkoverkko (Core Network), pääsyverkot (Access Network) ja kotiverkko (Home Network), jotka on esitetty kuvassa 7.




Kuva 7. IPTV lähetysverkko [3, s. 39]

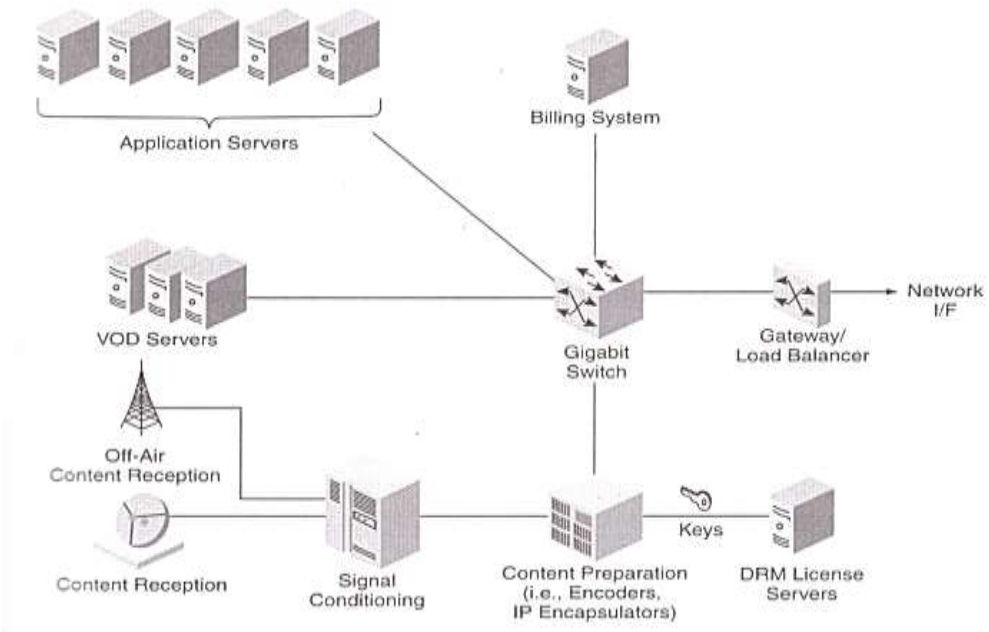
Lähetysasema (Headend) on paikka, jossa lähetettävä sisältö vastaanotetaan ja muokataan oikeaan muotoon IPTV-järjestelmää varten. Runkoverkko on järjestelmän selkäranka, joka välittää lähettämön tuottaman datan eteenpäin. Paikalliset mainokset ja asiasisällöt (mm. hätäviestit) välitetään runkoverkon kautta. Pääsyverkko (Access network) on niin sanottu Last mile -verkko, joka tarjoaa IPTV-palvelua kuluttajien koteihin. Kotiverkko välittää IPTV-palvelua asiakkaan kotona esimerkiksi reitittimen kautta. [3, 36 - 41.] Kuvassa 8 on esitetty IPTV-järjestelmäverkko yksityiskohtaisemmin.




Kuva 8. IPTV-Järjestelmäverkko [3, s. 39]

Lähetysasema (Headend)

Lähetysasemaa (Headend) voidaan kutsua IPTV-järjestelmän hermokeskukseksi, joka sisältää laitteistot kaapeli- ja satelliitti- lähetyksien vastaanottamiseen. Lähetysasema muokkaa saadun materiaalin IP-paketeiksi, jotka välitetään runkoverkkoon. Kalustona lähetysasemalla käytetään yleensä PC-palvelimia. Kuvassa 9 on esitetty lähetysaseman (Headend) laitteistokaavio.

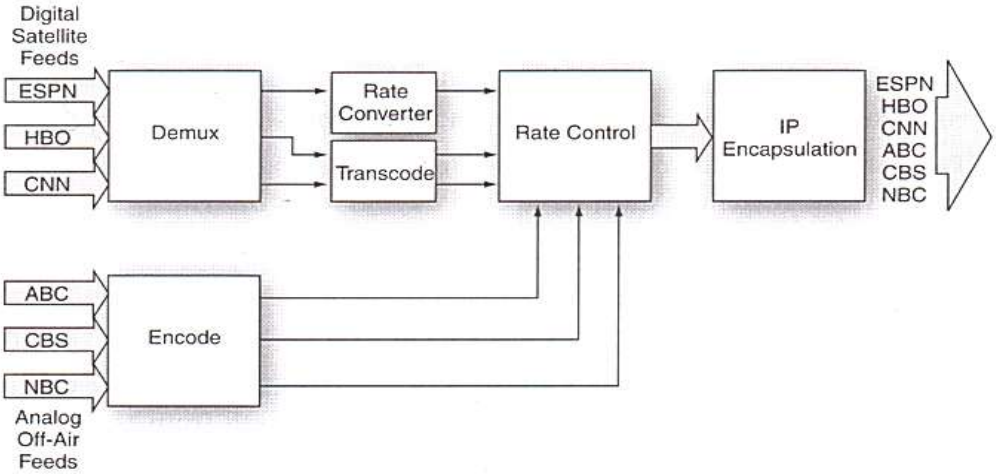



Kuva 9. IPTV Headend laitteisto [3, s. 41]

Aloitetaan lähetyaseman laitteistokaavion tarkastelu vasemmalla alareunassa olevasta sisällön vastaanotto (Content Reception) -yksiköstä. Sisältöä voidaan ottaa vastaan digitaalisia kaapeli- ja satelliittiyhteyksiä pitkin joko suoraan sisällöntuottajalta tai epäsuorasti muilta tahoilta. Sisältö voi olla TV-kanavamuodossa tai tilausvideopalvelu (Video On Demand, VOD). Seuraavaksi kätellään signaalinparannusyksikköä (Signal Conditioning), joka on kuvassa alareunassa toisena vasemmalla. Tämän yksikön tarkoituksena on parantaa vastaanotettujen sisältöjen signaalin laatua. Tähän tarkoitukseen käytetään vastaanotin-dekoodereita (Integrated Receiving Decoder, IRD), kohinan vaimentimia (Noise Reduction) ja digitaalisia videoprosessointilaitteistoja.

Seuraavaksi käsitellään sisällön valmistelijayksikköä (Content Preparation), joka on alarivillä kolmantena vasemmalla. Sisällön valmistelija koostuu enkoodereista ja IP-kapsulaattorista, jotka muokkaavat saamansa videovirran (Video Transport Stream, Video TS) IP-paketeiksi. Lisäksi tässä vaiheessa lisätään DRM-komponentti, jolla estetään asiaton materiaalin käyttö. IP-digiboksit (IP-STB) vastaanottavat IP-paketteja. Normaalin lähetyksen (Standard Definition Television, SDTV) bittinopeus on noin 1.5 Mbps ja teräväpiirtolähetyksen (High Definition Television, HDTV) bittinopeus on noin 8 Mbps. Kuvassa 10 on esitetty TV-kanavien vastaanottaminen digitaalisesti satelliitilla ja analogisia antenniverkkoja pitkin sekä niiden muokkaaminen. Demux vastaanottaa digitaaliset TV-kanavat (ESPN, HBO ja CNN). Enkooderi muokkaa analogiset

antennikanavat (ABC, CBS ja NBC) pakattuun digitaaliseen muotoon. Transkooderi muokkaa MPEG-2 koodatun videon tiiviimpään AVC tai VC-1 formaattiin. Bittinopeuden muunnin (Rate Converter) muokkaa MPEG-2-pakkausta tiiviimmäksi. Bittinopeuden kontrolloija (Rate Controller) luo lopullisen muodon, johon liitetään lähetystiedot ja kellon uudelleensynkronointi (Resync). IP-enkapsulaattori (IP Encapsulation) lisää formaatit IP-kuormaan (IP Payload), joka voidaan toimittaa IP-verkkoon.



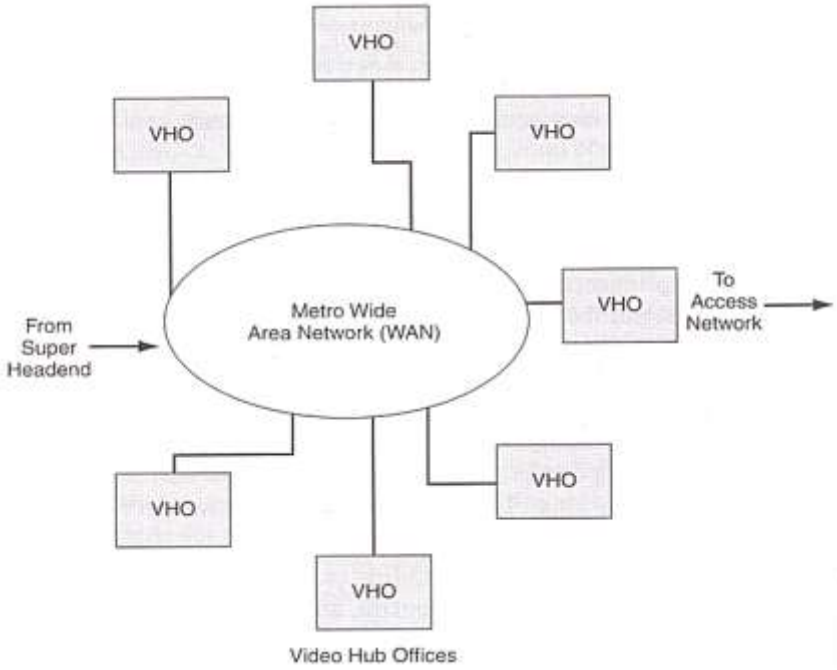

Kuva 10. Aineiston valmistelujärjestelmä [3, s. 43]

Seuraavaksi tarkastellaan DRM-lisenssipalvelin yksikköä, joka on kuvassa alarivissä oikeanpuoleisin. DRM-lisenssipalvelin (DRM License Server) hallinnoi, autentikoi ja raportoi sisällön siirtämisestä ja hallinnoi materiaalin salausta. Lisäksi palvelin tarkastaa lisenssipyynnöt ja toimittaa lisenssit luotettavalle DRM-loppukäyttäjälle. Tämän lisäksi se tuottaa käyttäjäinformaatiota tekijänoikeusmaksuja varten. VOD-palvelimet on optimoitu palvelemaan monia tietovirtoja samanaikaisesti. Laajakaistassa käytettävä kaistan-leveys säätelee käyttäjien määrää. Aineisto voidaan välittää multicastina (yksi bittivirta jaetaan monelle katselijalle) tai unicastina (jokaiselle käyttäjälle lähetetään oma bittivirta). Arkkitehtuuri mahdollistaa VOD-palvelimen sijoittamisen myös runkoverkkoon. Paikallisen lähetysaseman (Video Home Office, VHO) aplikaatiopalvelimet (Application Server) sisältävät systeeminhallinnan väliohjelmiston (Middleware), sähköisen ohjelmaoppaan (Electronic Program Guide, EPG) ja CAS/DRM-palvelimet. Se voidaan arkkitehtuurista riippuen sijoittaa runkoverkon paikalliselle lähetysasemalle. Laskutusjärjestelmässä on tietokanta, joka sisältää tarkat tiedot käyttäjistä. Tietokanta

sisältää tiedon siitä, mitä palveluita asiakkaan on lupa käyttää. Gateway/Load balancer tuottaa kuorman tasausta ja sessionohjausta sekä lähettää dataa verkkorajapinnalle. [3, 36 - 44.]

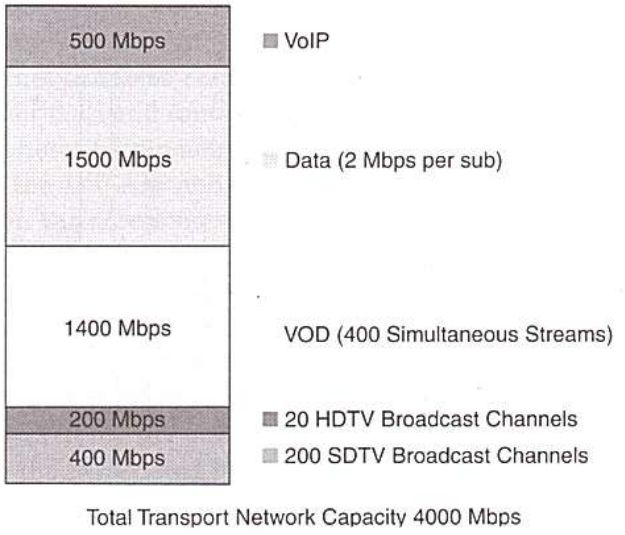
Runkoverkko (Core Network)

Runkoverkko koostuu laajaverkosta (Wide Area Network, WAN) ja paikallisesta lähetysasemasta (Video Hub Offices, VHO), jonka tarkoituksena on välittää dataa lähetysaseman (Headend) ja liityntäverkkojen (Access Network) välillä. Tärkein tehtävä on ylläpitää yhteyksillä tarvittava kaistanleveys. Runkoverkko pitää myös yllä hälytysjärjestelmää (Emergency Alert System, EAS). Kuvassa 11 on havainnollistettu runkoverkkoa.



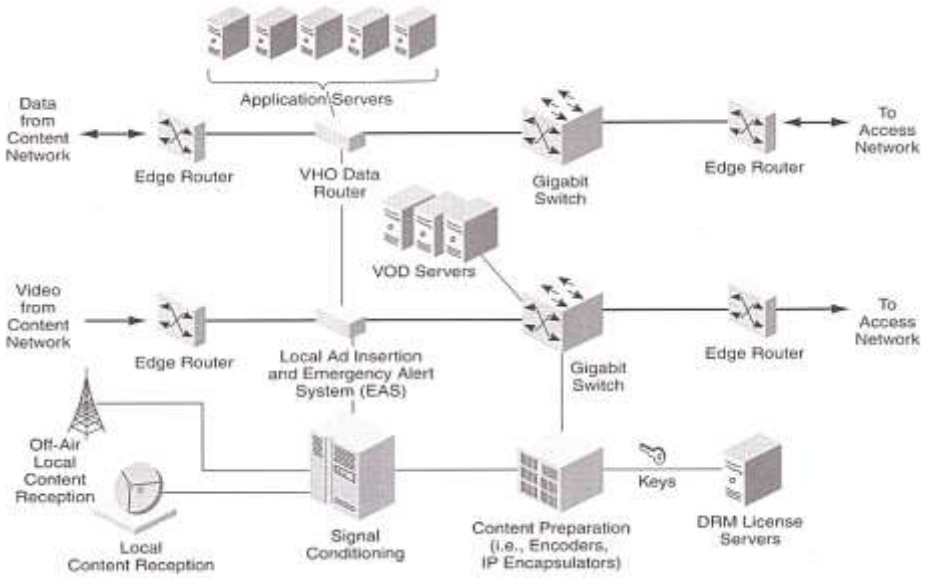

Kuva 11. Korkean tason arkkitehtuuri runkoverkosta [3, s. 44]

Kuvassa 12 on esitetty erään paikallisen lähetysaseman kapasiteettianalyysi. Esitettävät kapasiteetit voivat vaihdella eri järjestelmissä. Kuvassa näkyvä paikallisen lähetysaseman kokonaiskapasiteetti on noin 4 Gbps [3, 45].




Kuva 12. Esimerkki paikallisen lähetysaseman IP kapasiteetteistä [3, s. 45]

Kuvassa 13 on esitetty paikallisen lähetysaseman rakenne. Datan käsittelyosa (Local Content Reception, Signal Conditioning, Content Preparation, DRM Licence Server) on hyvin samanlainen kuin kuvassa 9. Siinä on myös VOD-palvelin ja applikaatiopalvelimet. Uutena osana on paikallinen mainos- ja hätävaroitusjärjestelmä (Local Ad Insertion and Emergency Alert System, EAS). Datan määrä on paljon pienempi paikallisessa lähetysasemassa (VHO) kuin päälähetysasemassa (Headend) [3, 45].




Kuva 13. Paikallisen lähetysaseman rakenne kuva [3, s. 46]

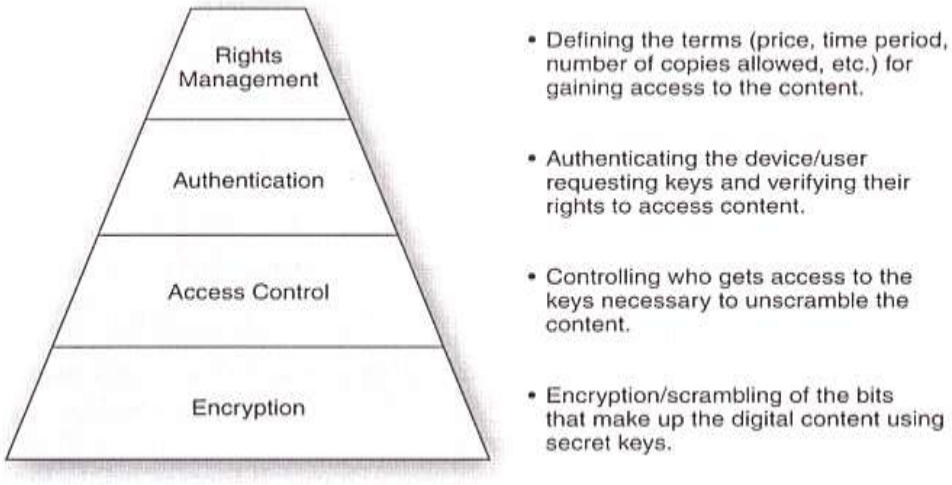
Salauksen purkuun tarvittavat tiedot välitetään CAM-viestissä (Conditional Access Message, CAM), joka sisältää ECM-viestin (Entitlement Control Message, ECM) ja EMM-viestin (Entitlement Management Message, EMM). Nämä koostuvat kolmesta erilaisesta datasta. Kontrollisanaa (Control_word) käytetään salauksen purkuketjun luomiseen. Palveluavain (Service_key) piilottaa kontrollisanan käyttäjäryhmään. Käyttäjäryhmiä voi olla useita. Käyttäjäavainta (User_key) käytetään palveluavaimen piilottamiseen.

## 3.2 Tekniikat IPTV-järjestelmässä

### 3.2.1 Sähköinen oikeuksienhallintajärjestelmä (DRM)

Sähköinen oikeuksienhallintajärjestelmä DRM (Digital Rights Management) on yleiskäsite, jota käytetään digitaalisessa muodossa olevan datan tekijänoikeuksien suojaamiseen. Piratismi ja tekijänoikeudella suojattujen tallenteiden levitys internetissä on ajanut viihdeteollisuuden käyttämään DRM-tekniikkaa sisältöjen suojaamiseen. DRM-järjestelmä koostuu monista tasoista, jotka estävät laittoman kopioinnin ja tarjoavat sekä aineistoa käyttävän että aineiston omistajan oikeudet. Nämä tasot esitellään kuvassa 20.

Digitaalisen oikeuksienhallintajärjestelmän alin taso on salaus (Encryption), joka salaa sisällön käyttäen salaisia avaimia. Pääsynvalvontataso (Access Control) kontrolloi, kuka pääsee sisältöön käsiksi. Autentikointitaso (Authentication) määrittelee sallittavat käyttäjät ja laitteet, pyytää avaimet alemmalta tasolta ja hyväksyy käyttöoikeudet. Oikeuksienhallintataso (Rights Management) määrittelee oikeudet käytettävään sisältöön (hinta, voimassaoloaika, kopioiden määrä jne.). Kuvassa 14 on esitetty yleiskuva järjestelmän toiminnasta.



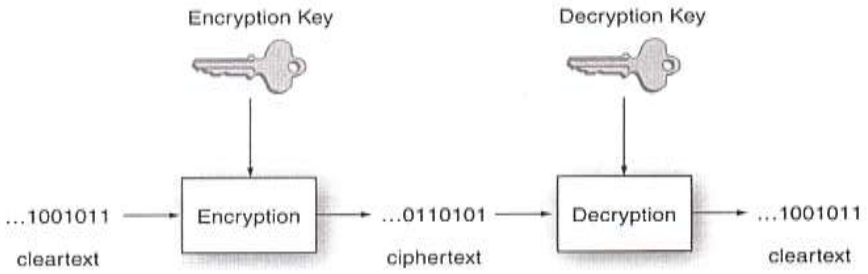

Kuva 14. Digitaalisen oikeuksienhallinta-järjestelmän tasot [3, s. 211]

Seuraavaksi käydään läpi yksityiskohtaisemmin tasoja aloittaen salauksesta.

Salaus

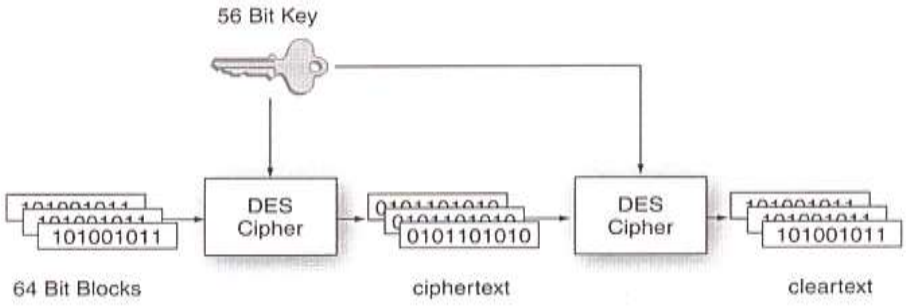
Digitaalinen salaus on sarja muutoksia, jotka muokkaavat selkokielisen tiedon lukukelvottomaan muotoon. Kuvassa 15 havainnollistetaan, kuinka olemassa olevalla avaimella muokataan selkoteksti salatuksi ja samalla avaimella salattu teksti puretaan takaisin luettavaan muotoon. Symmetrisessä salauksessa salaus- ja purkuavain on sama. Avainkoko on yleensä 64 - 512 bittiä. Avaimen selvittäminen kokeilemalla jokaista mahdollista avainta on liian aikaa vievää, koska avaimia on valtavasti. Salaamiseen voidaan käyttää DES-algoritmia (Data Encryption Standard, DES), jota on käytetty

salaukseen 1970-luvulta lähtien. Nykyisin käytetään yleisesti AES-salaustekniikkaa (Advanced Encryption Standard).



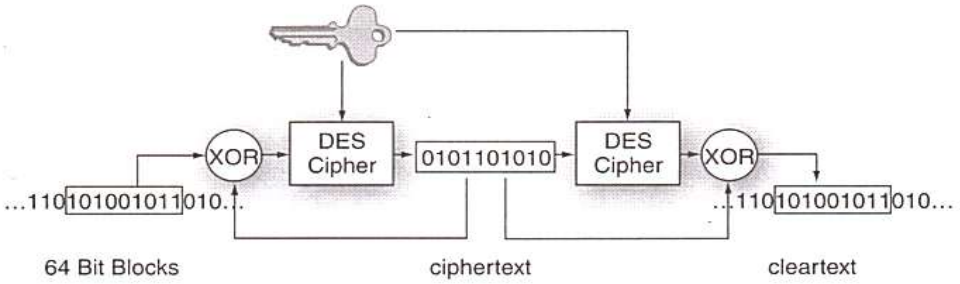

Kuva 15. Digitaalinen salaus [3, s. 212]

DES on ryhmäsalain (Block), joka käyttää 56 bitin kokoista avainta. Ryhmän (Block) koko on 64 bittiä. Mikäli viesti on tätä isompi, viesti pitää jakaa useampiin 64 bitin ryhmiin, jotka syötetään erikseen salaimeen. DES-salain on esitetty kuvassa 16.




Kuva 16. DES-salain [3, s. 213]

DES-salainta voidaan käyttää myös ketjutettuna (Cipher Block Chaining), jolloin salauksesta tulee vahvempi. Ketjutuksessa käytetään Exclusive OR (XOR) -toimintoa, joka kääntää binäärisen koodin järjestyksen. Kuvassa 17 on mallinnettu DES-ketjutus.



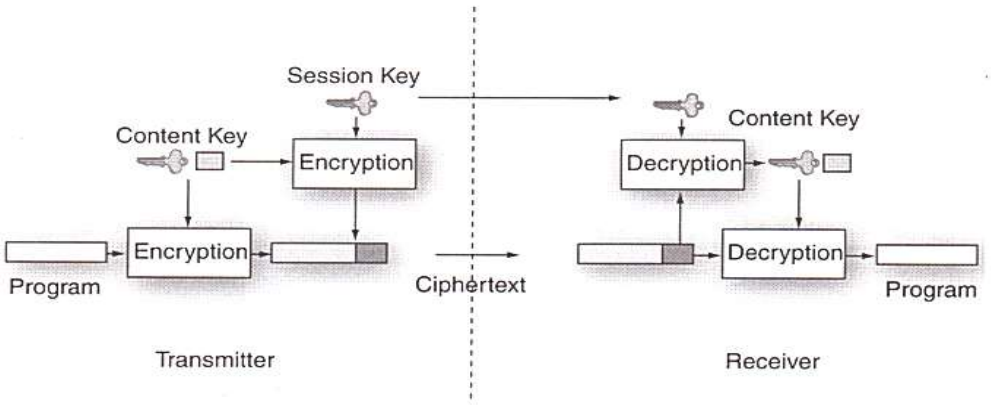

Kuva 17. DES-ketjutus [3, s. 214]

Käytössä myös parannettu versio kolmois-DES (Triple-DES), jossa käytetään yhden avaimen sijaan kolmea eri avainta, jolloin avaimen koko nousee 168 bittiin. DES:n tilalla on alettu käyttää Advanced Encryption Standard (AES) -algoritmia. [3, 211 - 214.]

Pääsynvalvonta (Access Control)

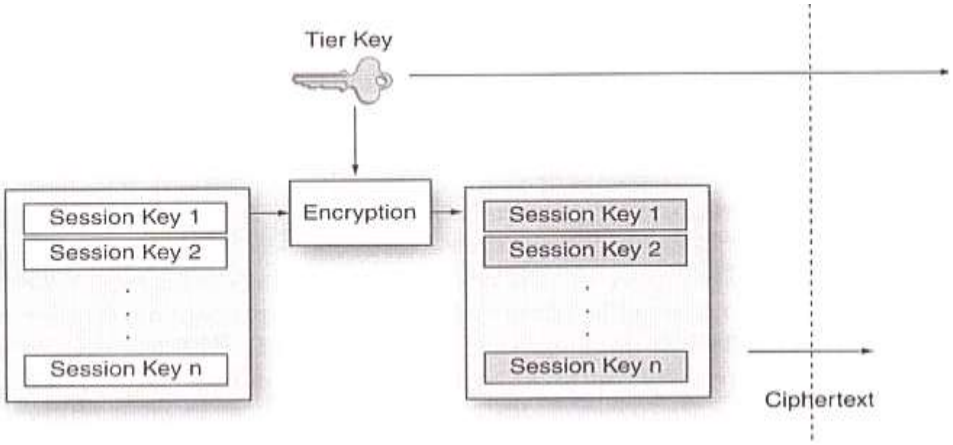
Siirrytään kuvan 14 seuraavalle tasolle, joka on pääsynvalvonta (Access Control). Kun audio- ja videovirrat on saatu salattua, ne välitetään miljooniin asiakkaiden koteihin. Tähän tarkoitukseen käytetään CAS-järjestelmää (Conditional Access System, CAS). CAS-periaatteet halutaan pitää salaisina, koska CAS toimittaa avaimet salauslaitteille.

Tuhansien eri avaimien hallintaan tarvitaan avainhierarkiaa, jotta avaimia voidaan hallita helpommin. Ylemmän tason avaimia käytetään purkamaan alemman tason avaimista tehtyjä avainryhmiä. Avainten vaihtuessa muutaman sekunnin välein on luotu sessioavain (Session Key), joka on sama koko käytettävän session ajan. Kuvassa 18 on havainnollistettu tätä toimintaa. Sessioavain lähetetään kerran salattua kanavaa pitkin vastaanottajalle. Sisältöavain (Content Key) salataan ohjelman bittivirran seassa.




Kuva 18. Sessioavain [3, s. 217]

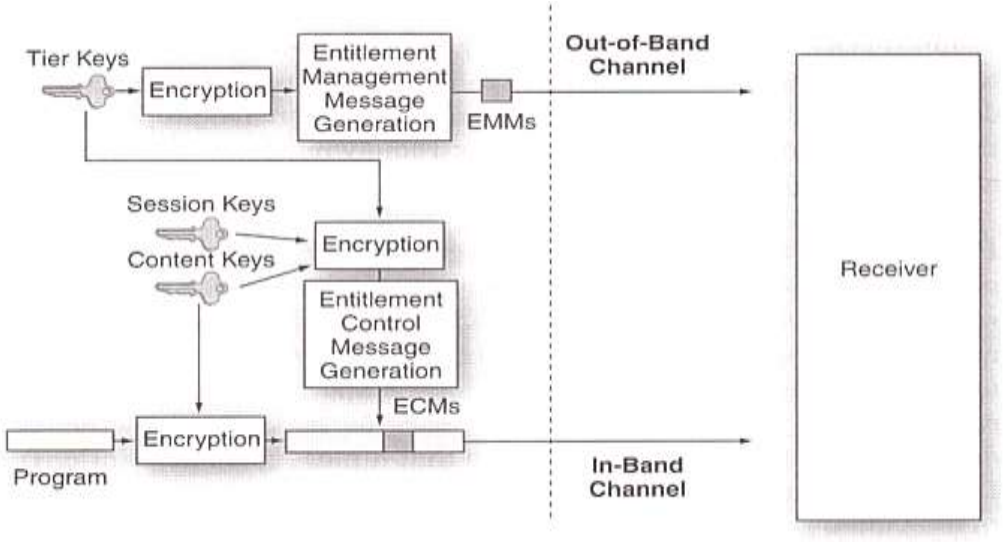
Kuvan 19 esimerkki havainnollistaa ohjelman välitystä. IPTV-järjestelmissä on monia ohjelmia, ja jokaisella ohjelmalla on oma sessioavain. Sessioavaimet voidaan niputtaa yhdeksi tasoavaimeksi (Tier Key). Kuvassa 19 eri ohjelmien sessioavaimet sijoitetaan ryhmiin ja salataan. Tasoavain lähetetään erikseen.




Kuva 19. Tasoavainsalaus [3, s. 218]

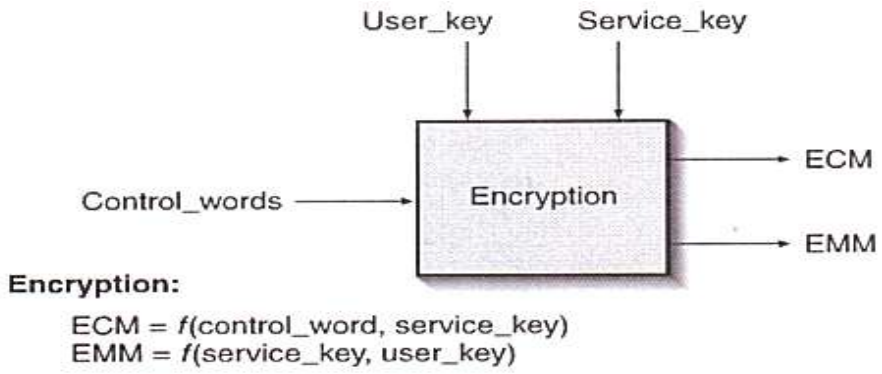
Tiedon kuljetukseen on olemassa kaksi erilaista menetelmää, jotka ovat nimeltään sisäinen kanava (in-band channel) ja ulkoinen kanava (out-band channel). Ulkoista kanavaa käytetään kiireettömän datan (Non-time critical) käsittelyyn. Sisäisellä kanavalla välitetään tiedot, jotka ovat kiireellisiä.

Kiireellisistä tiedoista käytetään nimitystä ECM (Entitlement Control Messages, ECM) ja kiireettömistä tiedoista nimitystä EMM (Entitlement Manage Messages, EMM). Kuvassa 20 kuvataan sisäistä ja ulkoista kanavaa. ECM välittää sisäistä kanavaa pitkin sessio- ja sisältöavaimet, jotka ovat kiireisiä sisältönsä takia. EMM välittää tiedot niistä laitteista, joita voidaan käyttää salauksen purkuun. Nämä tiedot eivät muutu niin usein kuin ohjelmatiedot. Tämän vuoksi käytetään ulkoista kanavaa. [3, 215 - 218.]



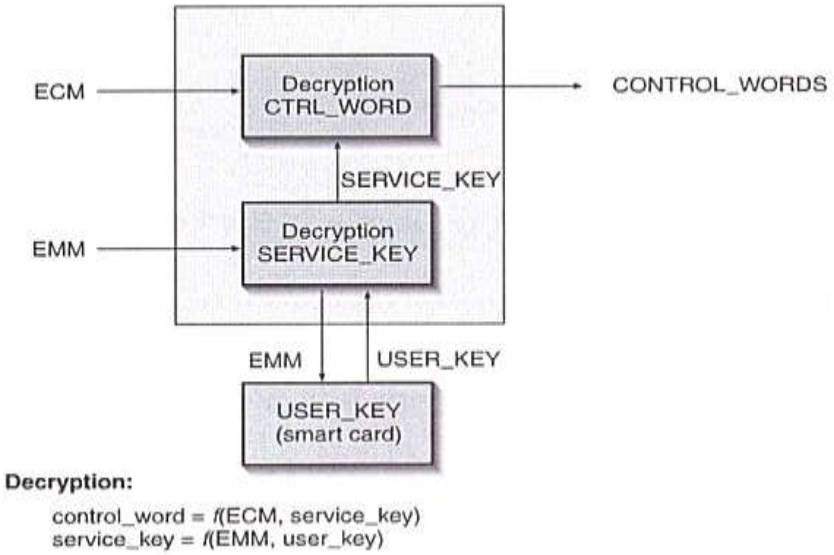

Kuva 20. Sisäinen ja ulkoinen kanava [3, s. 219]

Kuvassa 21 on esitetty ECM- ja EMM-salausprosessi, jossa ECM käyttää kontrollisanaa ja palveluavainta funktiona. EMM käyttää palveluavainta ja käyttäjäavainta funktiona. ECM lähettää funktiot kahden sekunnin välein, kun EMM lähettää funktiot kymmenen sekunnin välein.

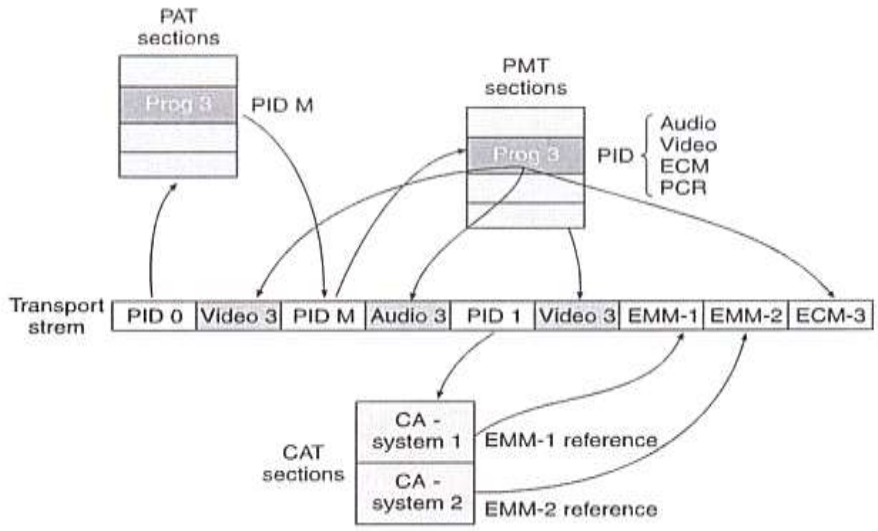



Kuva 21. ECM ja EMM salausprosessi [2, s. 102]

Salauksen purkamiseen digiboksi käyttää EMM-palveluavainta ja käyttäjäavainta. Näitä säilytetään lukijakortilla (Smart Card, SC). Palveluavainta käytetään ECM-salauksen purkamiseen. ECM käytetään kontrollisanan salauksen purkamiseen. Kontrollisana sallii laitteen salauksen purkuprosessin aloittamisen. Kuvassa 22 esitetään visuaalisesti salauksen purku.




Kuva 22. Salauksen purkuperiaate [2, s. 102]



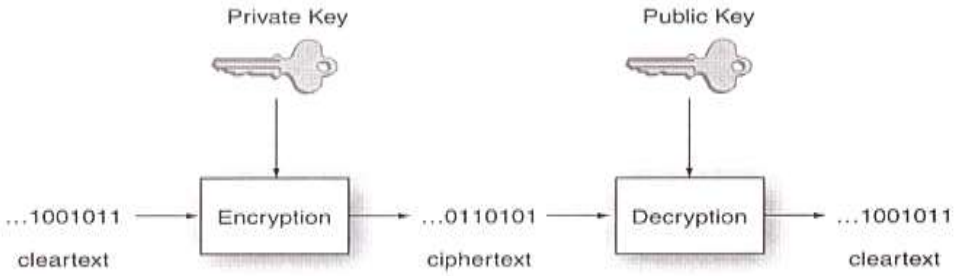

Kuva 23. ECM:n ja EMM:n sijainti siirtovirrassa [2, s. 103]

Autentikointi

Autentikoinnin tehtävänä on hallinnoida salaista tietoa sisältävää informaatiota ja identifioida oikea käyttäjä. IPTV-järjestelmässä välitetään paljon salaista tietoa. DRM-systeemin autentikointiosa hallinnoi salausavaimia, joilla salataan digitaalista aineistoa. Tällöin tunnistetaan viestin aitous ja lähettäjä. Monissa DRM-järjestelmissä käytetään yksisuuntaisia laajakaistaverkkoja. Näissä verkoissa avaininformaatio jaetaan kaikille vastaanottajille. Koska liikenne on yksisuuntaista, ei voida varmistaa, onko vastaanottava laite oikea. Tämän vuoksi luotetaan jaettuihin salaisuuksiin, jotka on toteutettu esimerkiksi sirulla digiboxissa (Set-Top Box, STB) tai salausmoduulilla (Conditional Access Module, CAM).

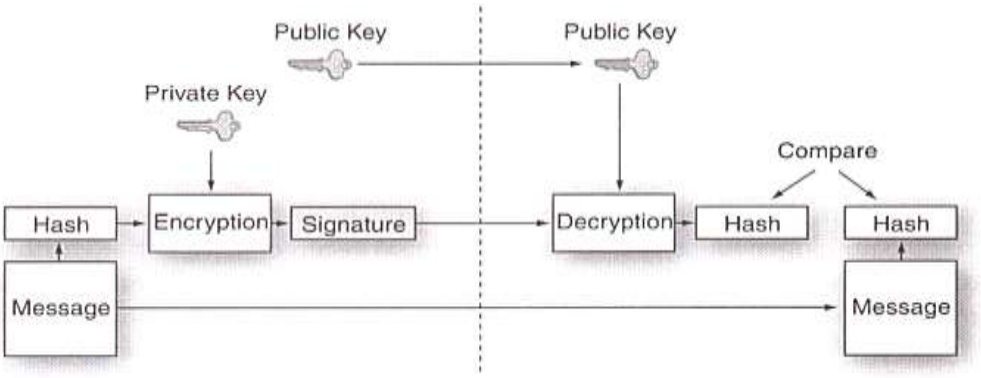
Näissä verkoissa on seuraavanlainen ongelma. Mikäli hakkerit selvittävät globaalin salausavaimen, sillä pystyy murtamaan jokaisen salauksen DRM-järjestelmissä. Tämän lisäksi järjestelmä ei voi tunnistaa, onko salaus murrettu. Tästä johtuen salausavaimia pitää vaihtaa säännöllisesti. Avaimet pitää toimittaa asiakkaille manuaalisesti, mikä on erittäin kallista. Tämän vuoksi on alettu käyttää kaksisuuntaisia verkkoja, jotka ovat kehittyneempiä eivätkä tarvitse globaaleja salaisuuksia, jotka olisivat kaikkien päätelaitteiden tiedossa. Lähettäjän ja vastaanottajan välillä käytetään julkisen avaimen salausta (Public Key Encryption, PKE) ja digitaalista allekirjoitusta. Näillä varmistetaan

turvallinen yhteys lähettäjän ja vastaanottajan välille. PKE käyttää kahta erilaista avainta: julkista ja salaista. Kuvassa 24 on esitetty avaimien käyttöä. Salaisella avaimella salataan tieto ja julkisella avaimella puretaan salaus. PKE tunnetaan myös nimellä epäsymmetrinen salaus. Salauksen voi purkaa vain tietyllä julkisella avaimella. Julkinen avain ei anna mitään viitteitä siitä, millainen salainen avain on. Julkinen avain on kaikkien nähtävillä. Kun lähettäjä pitää salaisen avaimen salaisena, tiedetään viestin olevan autenttinen.



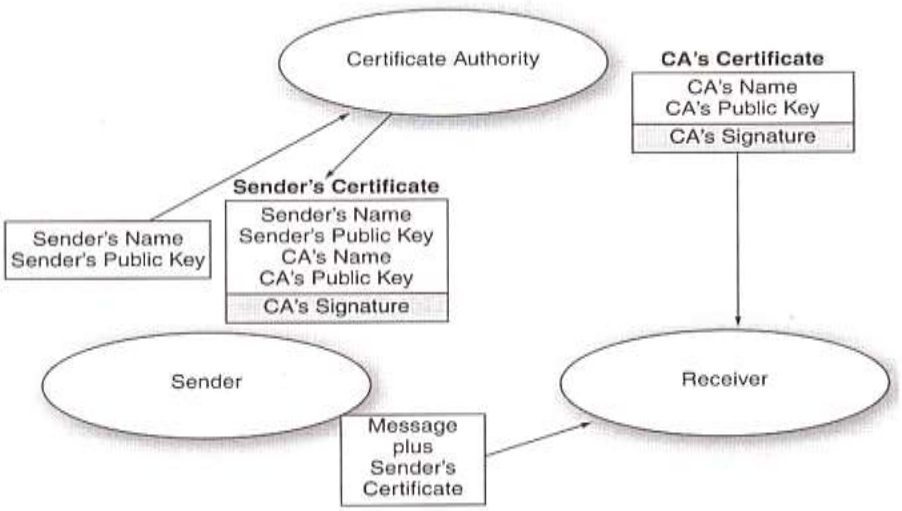

Kuva 24. Salainen ja julkinen avain [3, s. 221]

Digitaalinen allekirjoitus varmistaa, että lähettäjä on luonut viestin eikä salakuuntelija, joka väittää olevansa lähettäjä. Allekirjoitus luodaan PKE:n avulla, ja se on tiivistelmä viestistä, jota kutsutaan nimellä hash. Alkuperäinen teksti on paljon suurempi kuin hash-viesti. Mikäli joku taho muokkaa alkuperäistä tekstiä vertailemalla hash-viestejä keskenään, voidaan todeta, että tekstiä on muokattu matkan varrella. Lähettäjä salaa hash-viestin lähettäjän salaisella avaimella. Tämä salattu tiivistelmä on viestin allekirjoitus, joka voidaan luoda vain lähettäjän salaisella avaimella. Tämän jälkeen vastaanottajalle lähetetään viesti, allekirjoitus ja julkinen avain. Vastaanottaja purkaa allekirjoituksen julkisella avaimella, lukee viestin ja vertaa sitä purettuun hash-viestiin. Mikäli hash-viestit täsmäävät, viesti on autenttinen. Jos viestit eivät täsmää, tiedetään, että viestiä on muokattu. Kuvassa 25 on havainnollistettu PKE-allekirjoituksen välitys.




Kuva 25. PKE allekirjoituksen välitys [3, s. 221]

Kuvassa 26 on esitetty toimenpiteet, jotka tarvitaan luotettavuuden varmistamiseksi. PKE:n avulla kuka tahansa voi luoda julkinen/salainen-avainparin ja allekirjoittaa viestit salaisella avaimella. Tästä johtuen ei voida varmuudella luottaa lähettäjään. Ratkaisuksi tähän ongelmaan on luotu digitaaliset sertifikaatit. Sertifikaattiin liitetään lähettäjän nimi ja lähettäjän julkinen avain. Lähettäjä luo myös hash-viestin, joka liitetään sertifikaattiin. Tällä varmistetaan, että lähettäjä on luonut nämä osat sertifikaatista. Seuraavaksi sertifikaatti lähetetään luotettavalle kolmannelle osapuolelle. Näitä kutsutaan nimellä sertifikaattiauktoriteetti (Certificate Authority, CA). CA saa sertifikaatista lähettäjän osan, joka sisältää lähettäjän nimen ja lähettäjän julkisen avaimen. Tämän jälkeen CA lisää sertifikaattiin oman nimensä (CA’s Name), oman julkisen avaimensa (CA’s Public Key) ja allekirjoituksen (CA’s Signature), joka luodaan CA:n salaisella avaimella. Tämän jälkeen lähettäjän sertifikaatti on valmis, ja se lähetetään takaisin lähettäjälle. Lähettäjä todistaa aitoutensa sertifikaatin avulla. Lähettäjä luo viestinsä, liittää sertifikaatin ja lähettää ne vastaanottajalle. Tämän jälkeen vastaanottaja purkaa viestin salauksen, lukee sertifikaatin CA:n julkisella avaimella (CA’s Public Key) ja varmistaa lähettäjän allekirjoituksen. Vastaanottaja vertaa CA-sertifikaatin allekirjoitusta lähettäjän allekirjoitukseen ja toteaa viestit autenttisiksi.



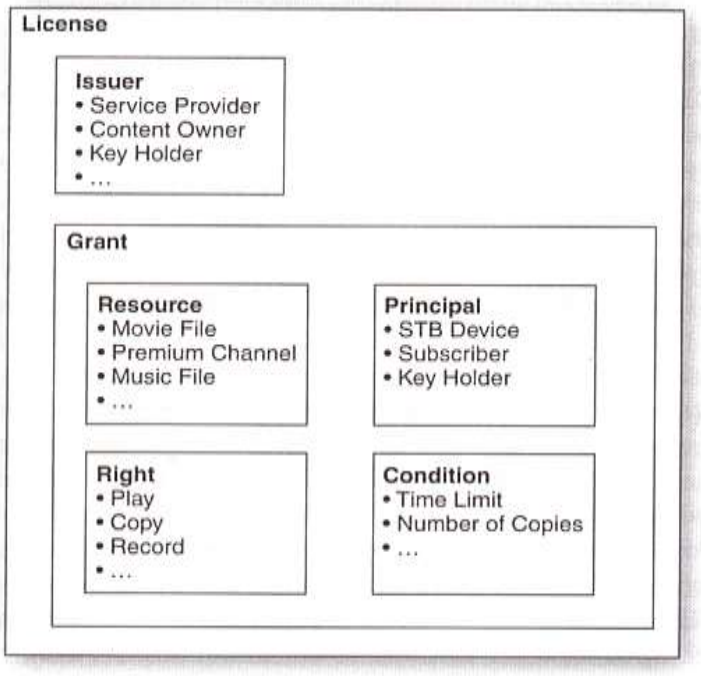

Kuva 26. Sertifioidun auktoriteetin toiminta [3, s. 223]

Niin kauan kuin CA-salaimen avain pysyy salassa, lähettäjä ja vastaanottaja voivat luottaa CA:han. Varmistaakseen aitoutensa CA ylläpitää sertifikaattiperuutuslistaa (Certificate Revoke List, CRL), jossa yleensä käytetään International Telecommunication Union (ITU-T) X.509 -standardia. CRL-sertifikaattia käytetään, koska lähettäjän salainen avain on voinut paljastua, jolloin lähettäjä ei ole enää luotettava. Vastaanottaja tarkistaa CRL- sertifikaatin aitouden. X.509-formaatti sisältää tietoja sertifikaatin aikarajoista, jotka CA voi asettaa.

CA:t käsittelevät satojatuhansia ellei miljoonia eri sertifikaatteja. Tätä varten on luotu julkisen avaimen infrastruktuuri (Public Key Infransructure, PKI), jota lähettäjät ja vastaanottajat käyttävät. DRM-järjestelmä käyttää omaa PKI:tä tai ottaa jonkun toisen PKI:n (esim. Verisign) ylläpitämään sertifikaattitietokantoja. DRM käyttää PKI:tä jokaisen laitteen sertifikaatin luomiseen. Valmistajilta vaaditaan tarkkuutta, jotta salainen avain ei paljastuisi. Jokaisessa PKE-laitteessa on uniikki salainen avain. Jos tämä avain paljastuu, vain tämän laitteen salaus paljastuu. Tämän vuoksi kaksisuuntaista verkkoa on helppo hallita. [3, 218 - 223.]

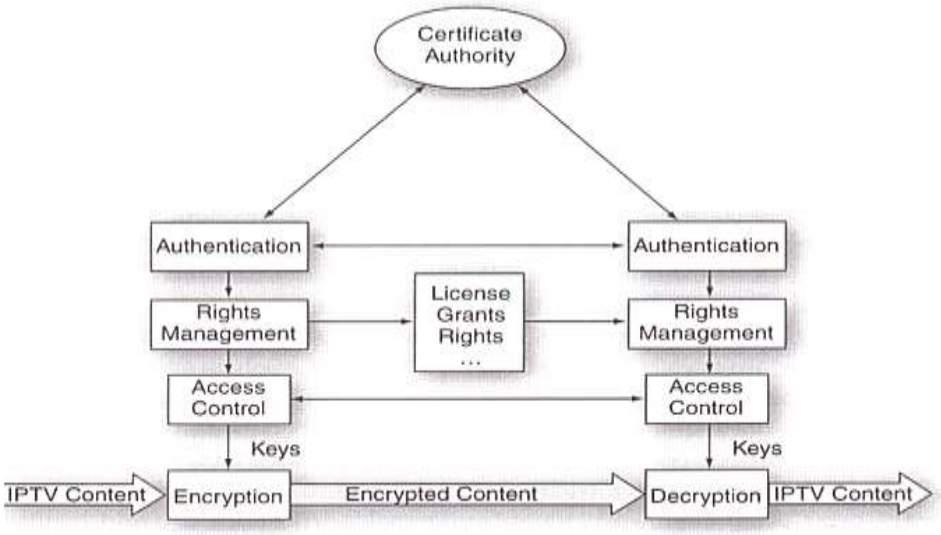
Oikeuksien hallinta (Rights management, DRM)

Kaikkien edeltävien toimien jälkeen tarvitaan DRM, jonka täytyy ilmaista, mitä asiakaslaite voi tehdä vastaanottamallaan sisällöllä, eli voidaanko materiaalia siirtää esimerkiksi PC:lle tai kannettavalle laitteelle (Personal Digital Assistant, PDA), esimerkiksi iPadille. Tähän tarkoitukseen on luotu oikeuksien ilmaisukieli (Rights Expression Language, REL), jolla kontrolloidaan materiaalin käyttöä. REL on osa DRM-järjestelmää. REL käyttää XrML-versiota, joka on Xerox Palo Alto Research Centerin luoma versio XML-kielestä. XrML sisältää oikeuksien periaatteet, resurssit, edellytykset, oikeudet, liikkeellelaskijat ja lisenssit. Kuvassa 27 on esitetty nämä asiat.




Kuva 27. XrML-oikeusmalli [3. s. 226]

DRM-järjestelmä, joka on tehty IPTV:tä varten, sisältää kaikki edellä esitetyt tasot. Salaamiseen käytetään digitaalista salainta (Cipher) ja salausavaimia (Encryption Key). Pääsynvalvontajärjestelmä (Access Control) hallinnoi käytettäviä avaimia, avain-informaatiota ja palvelutasoinformaatiota sekä kommunikoi suojatusti vastaanottavan laitteen kanssa. Oikeuksienhallintajärjestelmä (Rights Management) selvittää, mitä oikeuksia vastaanottajan laitteella on REL:n mukaan. Autentikointitaso selvittää oikeutettujen laitteiden pääsyn järjestelmään selvittäen sen CA:ta. Kuvassa 28 on havainnollistettu eri DRM-tasojen toimintaa IPTV-palvelussa.




Kuva 28. IPTV komponentit DRM-järjestelmässä [3, 228 - 232]

### 3.2.2 Esimerkki IPTV-järjestelmän vastaanottolaitteesta

DNA:n tarjoama DNA TV -palvelu on esimerkki käytössä olevasta IPTV-järjestelmästä. Ohjelmien vastaanottamiseen käytetään WBOX HD3 -digiboksia (kuva 32). TV-kanavien salauksen purkuun käytetään Conax CI+ -salausmodulia. TV-kortti (Smartcard) liitetään salausmoduulin sisään, joka purkaa salauksen. Kuvassa 29 on esitetty salausmoduuli ja TV-kortti.


Kuva 29. Kuva WBOX HD3 digiboksista [6]

Kuva 30. DNA Conax CI+-kortinlukija ja DNA TV -kortti [7]

## 4 Yhteenveto

Tässä opinnäytetyössä käsiteltiin IPTV-järjestelmän arkkitehtuuria ja ohjelman välitystä. Työssä on myös tutkittu, miten sisällönhallinta ja salaus on toteutettu. Symmetrisistä salausmenetelmistä DES ja 3DES ovat vanhentuneita. Nykyisin IPTV-järjestelmissä käytetään AES-salausta. Symmetrisen salauksen etuna on salauksen nopeus: salaus on kymmenen kertaa nopeampi kuin epäsymmetrisessä salauksessa. Symmetrisen salauksen huonona ominaisuutena voidaan pitää avainten jakelua. Mikäli avainta joudutaan jostakin syystä vaihtamaan, avaimien toimittaminen kaikille käyttäjille erikseen on hankalaa ja kallista. Epäsymmetrisessä salauksessa ei ole tätä ongelmaa, koska salaiset avaimet luodaan paikallisesti.

Näiden salaustekniikoiden lisäksi on kehitetty yhdistelmäsalaus (Hybrid Encryption), joka on yhdistelmä symmetristä ja epäsymmetristä salaustekniikasta. Salaus käyttää sattumanvaraisesti luotua symmetristä avainta, joka salataan vastaanottajan julkisen avaimen kanssa. Tällä menettelyllä varmistetaan, että vain vastaanottajalla on salauksen purkamiseen tarvittava salainen avain. Symmetrisellä salauksella saadaan tehostettua salausta. Epäsymmetrisen salauksen ansiosta avaimenhallinta on helppoa. Yhdistelmäsalausta käytetään SSL:ssä. CA:n ylläpitämät sertifikaatit ja niiden peruutuslistat vähentävät väärinkäytöksien riskiä.

## Lähdeluettelo

[1] Ramirez, D. 2008. IPTV Security, Protecting High-Value Digital Contents., Chichester, England: John Wiley & Sons Ltd.

[2] Benoit, H. 2008. digital television, Satellite, Cable, terrestrial, IPTV, Mobile TV in the DVB Framework. Burlington, MA 01803, USA: Elsevier Inc.

[3] Weber, J. & Newberry, T. 2007. IP-TV Crash Course. New York, NY, USA: McGraw-Hill.

[4] Stallings, W. 2014. Cryptography and Network Security. Pearson, Harlow, Essex CM20 2JE, England

[5] Stallings, W. 2011. Data and Computer Communications. Pearson, New Jersey, USA

[6] Wbox HD3 -digiboksi + USB kovalevy (500 Gt) [Viitattu 21.5.2017] https://kauppa4.dna.fi/DNA-Open/TV/Televisiot-ja-oheislaitteet/Wbox-HD3--digiboksi-%2B-USB-kovalevy-%28500-Gt%29/p/VDIGIBOX00002

[7] CI+-kortinlukija. [Viitattu 21.5.2017] https://kauppa4.dna.fi/DNA-Open/TV/Televisiot-ja-oheislaitteet/CI%2B--kortinlukija/p/VKOR00101