UNIVERZA V LJUBLJANI

FAKULTETA ZA ELEKTROTEHNIKO

UNIVERZITETNI ŠTUDIJ

MAGISTRSKO DELO

Digitalna zaščita multimedijskih vsebin in terminalna oprema

Jože Guna

Mentor: prof. dr. Janez Bešter

LJUBLJANA, 2005

Zahvala

V prvi vrsti gre zahvala mojemu mentorju prof. dr. Janezu Beštru za strokovno vodenje in pomoč pri izdelavi tega magistrskega dela.

Posebna zahvala gre mojim staršem, ki so mi omogočili študij in me vedno v vseh pogledih podpirali.

Hvala tudi vsem kolegom in sošolcem iz Laboratorija za telekomunikacije ter vsem ostalim za koristne pripombe in nasvete.

Posvetilo

Staršema, očetu Jožefu in materi Ljudmili.

VSEBINA

SEZNAM SLIK

SEZNAM TABEL

1. POVZETEK

Magistrsko delo se osredotoča na področja digitalne zaščite vsebin, pogojnega dostopa ter večpredstavne širokopasovne terminalne opreme.

Največji poudarek je na sistemih digitalne zaščite vsebin, kjer je podana definicija, širši dejavniki okolja ter klasificirane in opisane glavne vrste nevarnosti, pred katerimi skušajo ti sistemi varovati vsebine. Opisani so akterji in njihove vloge v življenjskem ciklu vsebin. Podane so zahteve, tehnologije ter elementi sistemov DRM. Podana je arhitektura splošnega sistema DRM, opisana standardizacija ter navedeni in podrobneje predstavljeni nekateri najpomembnejši produkti in projekti na tem področju.

Sistemom digitalne zaščite vsebin so komplementarni sistemi pogojnega dostopa. Opisana je njihova arhitektura in bistveni mehanizmi delovanja ter izpostavljena njihova vloga v primerjavi s sistemi DRM.

Zadnji del je namenjen področju večpredstavne terminalne opreme. Klasificirani in opisani so predstavniki s tega področja ter njihov pomen za uporabnike. Podana je arhitektura sodobnega večpredstavnega terminala, ki je primer strojne in programske konvergence. V eni napravi združuje funkcionalnosti osebnega računalnika, TV komunikatorja, večpredstavnega predvajalnika ter igralne konzole. Opisana je konkretna zasnova predlaganega terminala in njegova umestitev v IPTV okolje. Predstavljena in preizkušena je konkretna rešitev sistema DRM, povezava z okoljem IPTV in predlagano zasnovo večpredstavnega terminala.

Ključne besede:

sistemi digitalne zaščite vsebin, sistemi pogojnega dostopa, večpredstavna terminalna oprema

Abstract

In a modern information society connected by telecommunications networks appropriate and accurate information is often more important than material goods. Proper and secure protection of valuable information is therefore of great importance.

Main goals of this paper are focused on three subjects: digital rights management systems (DRM), conditional access systems and end-user multimedia terminal equipment with DRM functionalities.

The greatest emphasis is on digital rights management systems and technologies. Definition, classification and decomposition in accordance to the ISO-OSI layered model of DRM systems are given. Important technologies and basic elements of DRM systems are described. An overview of a generic DRM system and its information flow are presented. Some examples of specific commercial and academic DRM systems are described.

Conditional access systems, technologies involved and specific examples of those systems are presented. A comparison of functions between DRM and conditional systems is given.

The last part introduces, describes and categorizes the field of multimedia terminal equipment. A specification of a technologically advanced multimedia terminal is described. Real implementation of a DRM system is tested and its strengths and weaknesses exposed.

Keywords:

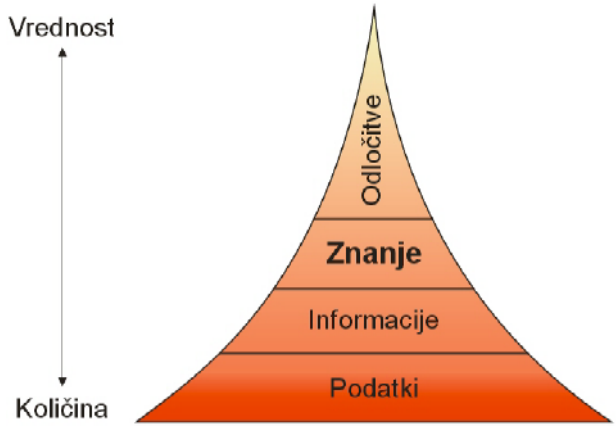
digital rights management systems, conditional access systems, multimedia terminal equipment

2. UVOD

Družba, v kateri živimo, počasi prehaja iz klasične industrijske v sodobno informacijsko družbo. Osnova informacijske družbe niso več materialne dobrine, temveč informacije. Vrednost informacij je relativna, odvisna od ciljnega področja in uporabnikov ter pogosto časovno in krajevno omejena. Najpomembnejše in najbolj dragocene so kvalitetne in prave informacije na pravem mestu ter ob pravem času. Takšne informacije omogočajo obogatitev in razširitev znanja ter posledično možnost sprejemanja strateških in pravih odločitev, ki imajo največjo vrednost v informacijski piramidi.

Drugi temelj informacijske družbe predstavljajo telekomunikacije, ki omogočajo učinkovito izmenjavo informacij preko različnih poti in medijev. Telekomunikacije so ena najhitrejše rastočih in najmočnejših gospodarskih panog v svetu in pri nas ter so strateškega pomena za vsako razvito družbo.

Osnovo telekomunikacij predstavljajo telekomunikacijska omrežja, ki so podlaga različnim uporabniškim storitvam. Najpomembnejši člen danes ni več tehnologija, temveč kvalitetne vsebine in storitve, zadnjo besedo pa imajo uporabniki. Od njih sta v največji meri odvisna ekonomski uspeh ali neuspeh določenih storitev, nove tehnologije ali celotnega sistema.



Sl. 1: Pomen informacij v informacijski piramidi

Pomemben pojem v telekomunikacijah predstavlja zlivanje oz. konvergenca (ang. Convergence, to converge). V splošnem izraz pomeni združitev, prekrivanje oz. zbliževanje več različnih elementov ali področij med seboj. Pri telekomunikacijah opazimo predvsem zlivanje na področjih storitev, tehnologij, omrežij ter terminalne opreme.

Zaradi izjemnega pomena informacij (pomembnih, nepomembnih) v informacijski in telekomunikacijsko povezani družbi je le-te potrebno ustrezno zaščititi. Pri tem sta pomembna predvsem dva segmenta in sicer:

- zaščita pred nelegalno pridobitvijo informacij in
- zaščita pred nelegalno uporabo (zlorabo) informacij.

Pod pojmom pomembna oz. vredna informacija lahko štejemo različne elemente oz. vsebine, ki imajo neko vrednost. Vsebinsko so pripadniki različnih področij, kot so npr. avtorska dela, poslovne skrivnosti in drugo ter so različnih oblik, kot npr. dokumenti, programska oprema, zabavne aplikacije in večpredstavno gradivo v obliki zvočnega in slikovnega materiala. Pomembna skupna lastnost vseh teh elementov je digitalna oblika. V primeru klasičnih informacij v analogni obliki je lete mogoče s procesom digitalizacije pretvoriti v njihovo ekvivalentno digitalno obliko.

V splošnem za zaščito in upravljanje z vsebinami v digitalni obliki skrbijo sistemi za digitalno upravljanje pravic oz. sistemi DRM (ang. Digital Rights Management). Drugi izraz, ki se uporablja, je sistem za digitalno varovanje avtorskih pravic, saj so navadno ščitena avtorska dela. Namenjeni so zaščiti in upravljanju različnih vrst vsebin, največkrat pa so namenjeni zaščiti večpredstavnih[1] vsebin. Izhajajo iz računalniškega sveta in v nasprotju s televizijskim pristopom omogočajo tudi shranjevanje in distribucijo vsebin v digitalni obliki. Zaščitene vsebine se ob nastanku kodirajo, uporaba je možna z licencami. Posamezna licenca vsebuje dekodirni ključ in predpisuje pogoje uporabe. Pri tem vsebine ni potrebno ponovno kriptirati, generacija različnih licenc ter s tem povezanih pogojev uporabe pa je poljubna. Primera značilnih sistemov DRM sta Microsoft DRM in Real Networks Helix DRM.

Podobno vlogo imajo sistemi pogojnega dostopa (ang. Conditional Access, CA), ki izhajajo iz klasičnega televizijskega sveta in so bili primarno namenjeni zaščiti vsebin v okviru digitalne (ang. Broadcast) televizije (DVB). Zaščitene vsebine so kriptirane in dostopne z uporabo kombinacije strojne in programske opreme v obliki dekodirnikov in pametnih kartic. Sodobni sistemi pogojnega dostopa se po funkcionalnosti približujejo sistemom DRM, tako da je tudi na tem področju mogoče opaziti efekt konvergence oz. zlivanja. Najbolj znani produkti s tega področja so izdelki podjetij Irdeto Access, Philips Cryptoworks, Viaccess in drugi. Zanimiva sta tudi sistema podjetij WideVine technologies in SecureMedia, ki spadata v sisteme pogojnega dostopa, vendar sta že v osnovi načrtovana kot DRM sistema in sta nekakšen hibrid med obema pristopoma.

V magistrski nalogi je poudarek na sistemih pogojnega dostopa in sistemih DRM za zaščito večpredstavnih vsebin, predvsem videa v digitalni obliki.

Pri uporabi storitev, vsebin in dostopu do informacij je pomembna tudi terminalna oprema. Pod tem pojmom se skriva praktično vsa strojna in programska oprema, ki je v vlogi posrednika med uporabnikom in sistemom za nudenje storitev. Uporabnik neposredno komunicira s terminalno opremo, ki predstavlja standardno uporabniško dostopovno točko. Terminalna oprema mora biti zato premišljeno in skrbno načrtovana, prijazna in predvsem enostavna za uporabo, kar je ključnega pomena. V splošne lahko terminalno opremo razdelimo po številnih kriterijih, od katerih so zanimivi predvsem zmogljivost, stopnja mobilnosti ter način interakcije z uporabnikom. Prav tako je na področju terminalne opreme opaziti trend zlivanja različnih vrst terminalne opreme in pojav kvalitativno nove terminalne opreme, ki je

[1] Avtor za izraz multimedija (multimedijski) predlaga in uporablja lep slovenski prevod večpredstavnost.

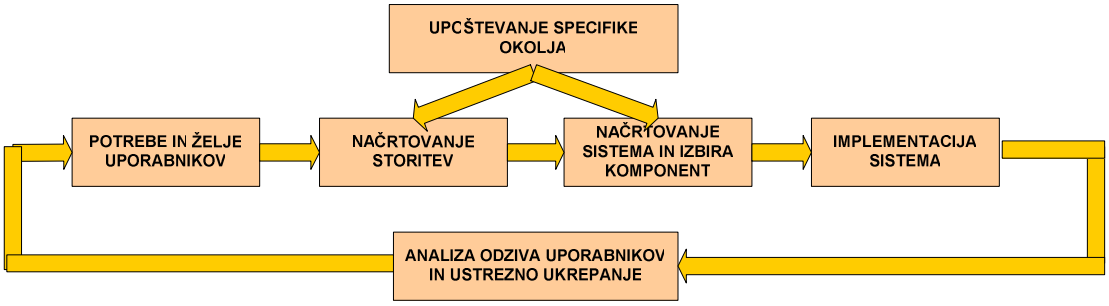
namenjena konzumiranju sodobnih večpredstavnih storitev preko širokopasovnih podatkovnih omrežij. Drugi, manjši, poudarek magistrskega dela je zato na sodobni širokopasovni terminalni opremi.

2.1. Načrtovanje storitev

Pri komercialnih sistemih za ponujanje vsebin in storitev v splošnem nastopajo trije akterji in sicer lastniki (vsebin in storitev), operaterji in uporabniki. Uporabniki so v tem modelu najbolj pomembni, saj predstavljajo vir dohodka za ostale akterje. Tudi sistem DRM se mora v tem pogledu prilagajati uporabnikom in prav tako prispeva k uspehu celotne rešitve.

Pri splošnem pristopu k načrtovanju storitev in ustreznega sistema za implementacijo je zato priporočljivo izhajati iz potreb in želja uporabnikov. Na podlagi le-teh ter ob upoštevanju specifike ciljnega okolja se nato oblikujejo ustrezne nove storitve ter načrtuje in implementira sistem. Po uspešni vzpostavitvi celotnega sistema za nadzor in strežbo vsebin je prav tako pomembno spremljanje odziva uporabnikov ter ustrezno ukrepanje.

S stališča uporabnikov sta pomembni kvaliteta in raznolikost ponujenih vsebin in storitev ter njihova enostavna uporaba, manj pomembna pa je sama tehnična izvedba.



Sl. 2: Pristop k načrtovanju storitev

2.2. Sistem za strežbo večpredstavnih storitev

Obe izbrani temi magistrske naloge, tako sistemi za zaščito vsebin kot tudi terminalna oprema, sta del večjega sistema, ki skrbi za hrambo, distribucijo ter upravljanje s storitvami in vsebinami. Sistemi za zaščito vsebin so v večji meri pomembnejši za ponudnika storitev in ne smejo biti ovira uporabnikom. Na drugi strani pa je terminalna oprema zelo pomembna za uporabnike, saj predstavlja osnovni stik med uporabniki in sistemom.

2.2.1. Koncept »3 Play« storitev

Koncept »triple play« oz. »3 Play« storitev je pravzaprav primer konvergence različnih storitev na eni tehnološki platformi. Za uporabnike je pomembna predvsem možnost enotnega pristopa do storitev ter enoten uporabniški vmesnik.

Koncept je mogoče poljubno razširiti v »X Play«, kar se bo v prihodnosti gotovo zgodilo. Trenutno »3 Play« storitve obsegajo tri glavne skupine in sicer:

- internetne,
- video in
- telefonske storitve.

Osnovne in najbolj pogoste storitve posameznih skupin prikazuje spodnja preglednica.

Triple Play Storitve		
Internetne	**Video**	**Telefonske**
• splošno brskanje po internetu, spletu • uporaba E-pošte • neposredno sporočanje • uporaba storitev prenosa datotek (FTP, omrežja P2P)	• TV v živo • video (vsebine) na zahtevo, bližnji video na zahtevo • EPG vodnik • PVR funkcionalnost • videokonference, videofonija • teletekstne informacije	• telefonija • dodatne telefonske storitve

Tab. 1: Razdelitev »3 Play« storitev

2.2.2. Tehnološka platforma

Tehnološka platforma je osnova celotnega sistema ter vsebuje vso potrebno strojno in programsko opremo. Razdeliti jo je mogoče v tri dele:

- strežniški del,
- povezovalno omrežje in
- terminalno opremo.

Strežniški del vsebuje vso potrebno opremo za izvajanje storitev. Značilni strežniki internetnih storitev so spletni strežnik, strežnik za elektronsko pošto, aplikacijski in datotečni strežnik, strežnik za neposredno sporočanje. Za telefonske storitve v primeru klasične telefonije skrbi telefonska centrala, v primeru NGN omrežij pa kombinacija klicnega strežnika in aplikacijskega strežnika. Komunikacijo med klasično in NGN telefonijo omogočata signalizacijski in medijski prehod.

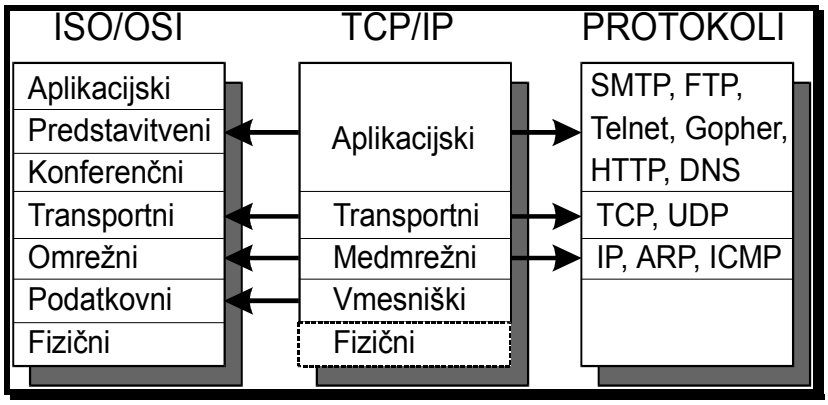
Tehnološko najbolj zahtevni in zanimivi so strežniki za večpredstavne storitve. Tipični predstavniki so večpredstavni strežnik, enkoderji, ki vsebine digitalizirajo in kompresirajo ter ostali posebni strežniki. Med te spadajo strežniki za nadzorno programsko opreme oz. middleware, strežniki za sisteme DRM in pogojnega dostopa ter ostali posebni strežniki, npr. za integracijo z drugimi sistemi.

Funkcijsko so strežniške naloge ločene, fizično pa so lahko implementirane v isti napravi. Kot strojna osnova se največkrat uporablja PC oz. kompatibilna platforma, pri večjih in bolj zahtevnih postavitvah pa se uporabljajo tudi posebne rešitve.

Omrežje med seboj povezuje strežniško opremo in uporabniško terminalno opremo. V splošnem se geografsko deli v dostopovno in hrbtenično. Dostopovno omrežje agregira vse naprave, hrbtenično omrežje pa zagotavlja hitro komunikacijo med njimi.

Skupen imenovalec, na katerem temeljijo sodobni sistemi za nudenje »3 Play« storitev, je IP platforma. Iz te povezave izvira drugo ime za takšne sisteme – IPTV oz. internetna televizija, televizija preko omrežij z internetnim protokolom.

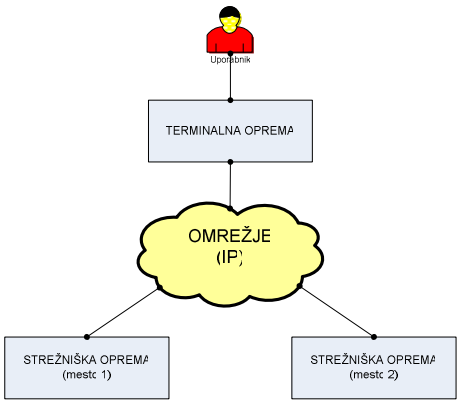
IP platforma temelji na družini internetnih protokolov TCP/IP oz. TCP/IP protokolnem skladu. V primerjavi s standardnim sedem slojnim ISO-OSI telekomunikacijskim modelom protokolni sklad TCP/IP definira le štiri sloje: dostopovnega, mrežnega, transportnega in aplikacijskega.



Sl. 3: Arhitektura protokolnega sklada TCP/IP

TCP/IP protokolni sklad je lahko implementiran preko različnih dostopovnih tehnologij, pri čemer se najpogosteje uporablja tehnologija Ethernet.

Terminalna oprema v okviru IPTV platforme med seboj povezuje dva svetova in sicer klasičnega računalniškega ter televizijskega. V ta namen je bila razvita posebna vrsta terminalne opreme – televizijski komunikator oz. TV komunikator (ang. Set-Top-Box, STB). TV komunikator vsebuje tako vmesnike za priključitev na širokopasovna telekomunikacijska omrežja (Ethernet, xDSL) kot tudi klasične televizijske vmesnike (SCART, video). Zmogljivosti TV komunikatorjev z razvojem tehnologije naraščajo in omogočajo uporabo praktično vseh vrst storitev na eni sami fizični napravi.



Sl. 4: Splošna arhitektura IPTV sistema

2.2.3. Arhitektura sodobnega sistema za video storitve

Celoten sistem za strežbo storitev iz koncepta »3 Play« sestavljajo trije sklopi, ki so med seboj tehnološko in storitveno povezani. Ti sklopi so:

- sistem za implementacijo internetnih storitev,
- sistem za implementacijo telefonskih storitev in
- sistem za implementacijo video storitev.

Tehnološko najbolj zahteven element je navadno sistem za implementacijo video storitev. Odvisno od izvedbe, je lahko problematičen tudi sistem za telefonske storitve, predvsem v smislu povezave klasične telefonije z IP platformo. Vsi sklopi temeljijo na IP platformi od koder podedujejo tudi večino prednosti in prav tako slabosti te platforme. Glavni problemi se pokažejo na področjih zagotavljanja kvalitete storitev in varnosti in se rešujejo z različnimi mehanizmi preko več slojev TK komunikacijskega modela. Sistem DRM in sistem pogojnega dostopa sta tipična mehanizma za reševanje varnostnih problemov in spadata v aplikacijski sloj.

V okviru strežniškega dela se izključno za večpredstavne (video) storitve uporabljajo nekateri novi funkcionalni elementi. Najbolj značilna sta večpredstavni strežnik in enkoder večpredstavnih vsebin. Večpredstavni strežnik skrbi izključno za hrambo večpredstavnih vsebin in učinkovito ter kvalitetno strežbo le-teh velikemu številu uporabnikov. Takšne večpredstavne vsebine so v naprej pripravljene in omogočajo izvedbe storitev na zahtevo (npr. video na zahtevo). Tipično se prenašajo v realnem času z metodo strujanja[2]. V primeru živih virov vsebin je le-te potrebno primerno obdelati, kar je naloga enkoderja vsebin. Poleg digitalizacije enkoder večpredstavne vsebine tudi kompresira, s čimer se zmanjša fizična velikost teh vsebin. Pri tem je potrebno paziti na razmerje med stopnjo kompresije in želeno izhodno kvaliteto vsebin. Tipični sodobni formati večpredstavnih vsebin v kompresirani obliki so MPEG-2, MPEG-4, Windows Media in Real.

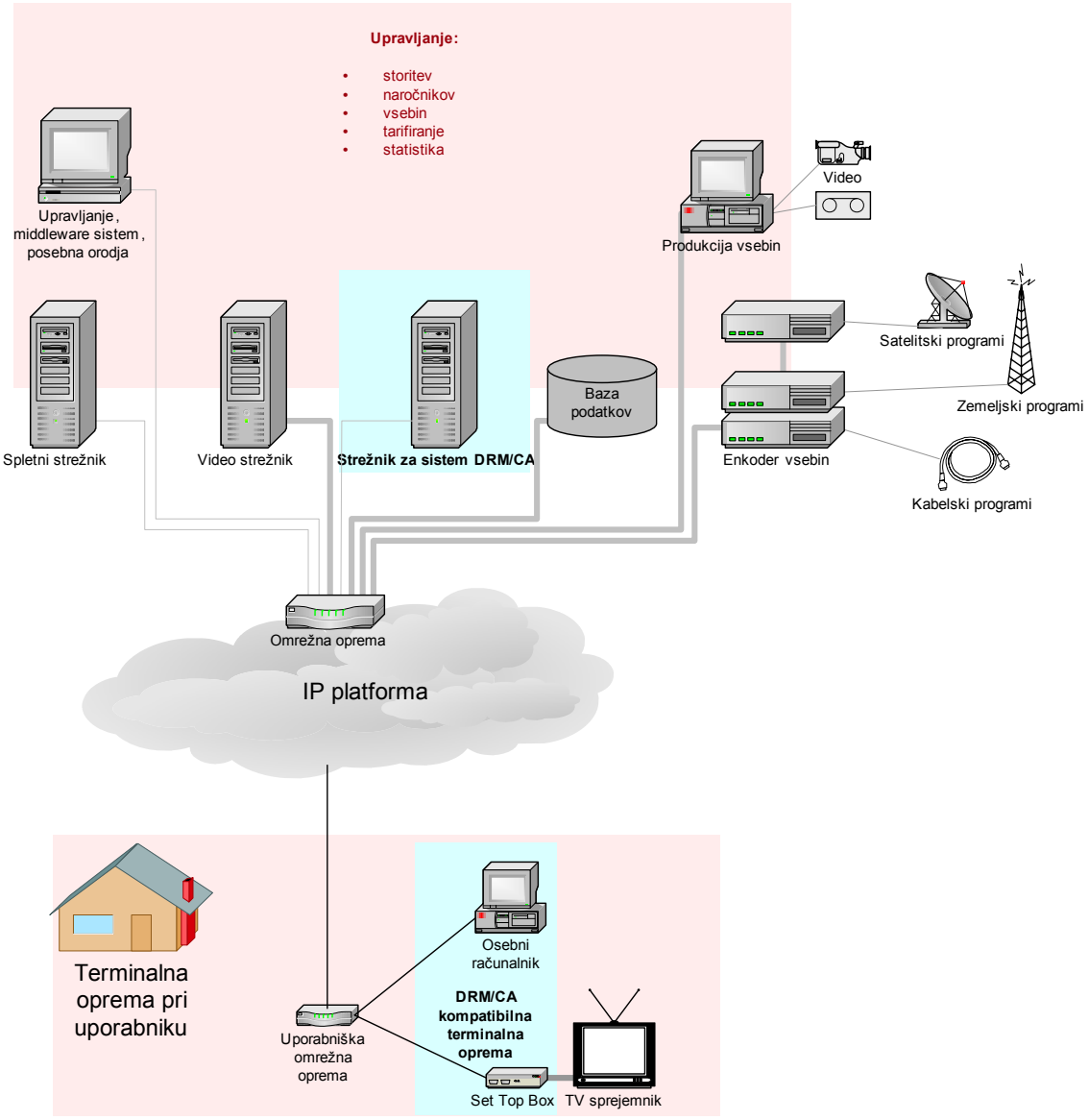
Sistema za zaščito večpredstavnih vsebin DRM oz. CA nudita dodatno varnost v smislu preprečevanja nelegalnega dostopa do vsebin in njihove zlorabe. Fizično so elementi teh sistemov lahko samostojni ali pa razporejeni po obstoječi strežniški infrastrukturi (npr. del večpredstavnega strežnika in enkoderja vsebin). Zaščita vsebin je navadno zadnji korak priprave vsebin. Primer predstavljajo vsebine na zahtevo, ki se najprej digitalizirajo, obdelajo, kompresirajo in nato zaščitijo (kriptirajo).

Za pravilno in učinkovito delovanje, nadzor in upravljanje s sistemom za strežbo video storitev skrbi dodatna programska oprema oz. middleware. Middleware deluje kot posrednik med vsemi ostalimi elementi in jih med seboj povezuje. Zaradi tega morajo biti vse specifične tehnologije neposredno podprte v middleware sistemu. Najbolj znani predstavniki teh sistemov so: ORCA, InfoGate OnDema, YesTV in drugi.

---

[2] Avtor namesto izraza »strujanje« predlaga »izraz pretočni« prenos. V angleškem jeziku se uporablja izraz »streaming«.

Terminalna oprema pri uporabniku deluje kot posrednik med uporabnikom in ponudnikom storitev ter mora podpirati vse želene storitve. Nekatere od teh storitev so generične in potrebujejo splošne elemente, kot je npr. spletni brskalnik. Druge, predvsem večpredstavne, imajo zelo specifične zahteve, kot je npr. podpora določenemu video formatu. Del sistemov za zaščito večpredstavnih vsebin mora biti prav tako implementiran v terminalni opremi, saj le-ta skrbi za dekodiranje zaščitenih vsebin.



Sl. 5: Funkcionalna arhitektura značilnega IPTV sistema za video storitve

3. DIGITALNA ZAŠČITA VSEBIN

Digitalno upravljanje s pravicami in zaščita vsebin v digitalni obliki je relativno nov koncept, ki šele prehaja v zrelo obdobje. Sam pojem DRM sistema je še precej nedoločen in ima različne pomene, ki se razlikujejo po obsegu in namenu. Sistemi DRM so lahko fokusirani samo na zelo ozko področje delovanja, kot je npr. DRM sistem za zaščito digitalnih video vsebin, ali pa obsegajo celotno verigo dejavnikov, ki so povezani z identifikacijo, trženjem in zaščito vsebin. Na ta način je mogoče izpeljati definicijo sistemov DRM v ožjem in v širšem pomenu.

Uspeh sistema DRM ni odvisen samo od tehnoloških dejavnikov, temveč nanj vplivajo tudi pravni vidiki, poslovni model ter ekonomski vidiki in socialni vidiki. Netehnološki dejavniki so lahko celo pomembnejši od tehnoloških za uspeh specifične implementacije sistema DRM.

Med tehnološke dejavnike lahko štejemo tudi specializiranost DRM sistema na določene vrste vsebin, kot so npr. dokumenti v digitalni obliki, programska oprema, elektronske igre in večpredstavne vsebine. Kljub temu, da je vse DRM sisteme mogoče opisati z nekaterimi skupnimi značilnostmi, se konkretna implementacija razlikuje glede na specifične potrebe posameznih vrst vsebin.

Zaradi kompleksnosti DRM sistema in sodelovanja z drugimi sistemi je pomembna uvrstitev DRM sistema v splošni telekomunikacijski model in na podoben način razslojitev samega sistema DRM po funkcionalnostih.

Opisane so najbolj značilne nevarnosti, ki pretijo vsebinam in sistemom DRM. Predstavljene so najpomembnejše tehnologije in elementi sistemov DRM. Podana je arhitektura in potek dogajanja v okviru generičnega sistema DRM.

Poseben problem predstavlja standardizacija in s tem povezana interoperabilnost oz. kompatibilnost različnih specifičnih implementacij med seboj. Opisanih je nekaj primerov standardizacije na tem področju ter primerov konkretnih implementacij sistemov DRM.

3.1. Definicija in dejavniki okolja na sistem DRM

3.1.1. Definicija

V literaturi in na spletu najdemo različne definicije sistema DRM. Nekatere zanimivejše so:

Webopedia,

»*Short for digital rights management,* ***a system for protecting the copyrights of data circulated via the Internet or other digital media by enabling secure distribution and/or disabling illegal distribution of the data****. Typically, a DRM system protects intellectual property by either encrypting the data so that it can only be accessed by authorized users or marking the content with a digital watermark or similar method so that the content can not be freely distributed.*«

[W1]

Wikipedia,

»*Digital Rights Management (DRM) is an umbrella term referring to any of several technical* ***methods used to control or restrict the use of digital media content on electronic devices with such technologies installed****. The media most often restricted by DRM techniques include music, visual artwork, and movies.*

Some digital media content publishers claim DRM technologies are necessary to prevent revenue loss due to illegal duplication of their copyrighted works. Civil libertarians, in contrast, argue that transferring control of the use of media from consumers to a consolidated media industry will lead to loss of existing end-user rights, as well as stifling innovation in software and cultural productions.

No current DRM technology includes a mechanism to enable fair use rights per se, though some DRM methods allow acts of copying which may coincidentally align with legal use rights. Arguably, a technology cannot, in principle, know what legal restrictions and rights apply in a specific jurisdiction, usage context, under an external contract, or to an individual author, owner, or publisher...«

[W2]

Encarta,

»*digital rights management* ***payment of royalties on Internet***«

[W3]

WhatIs,

»*Digital rights management (DRM) is a systematic approach to copyright protection for digital media.* ***DRM's purpose is to prevent illegal distribution of paid content over the Internet.*** *DRM products were developed in response to the rapid increase in online piracy of commercially marketed material, which proliferated through the widespread use of Napster and other peer-to-peer file exchange programs...*«

Iz navedenih virov lahko povzamemo:

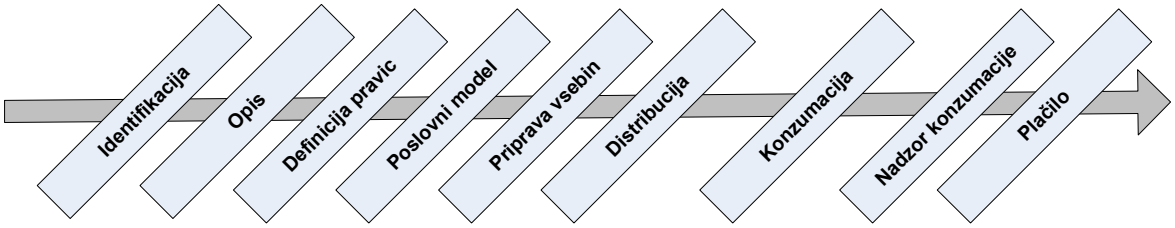
»***Sistem DRM je odgovoren za zaščito in varno distribucijo vsebin v digitalni obliki med ponudniki vsebin in uporabniki.***«

Termin DRM je neločljivo povezan z digitalnimi mediji, digitalnimi vsebinami ter internetom. Povezava med temi elementi ima največkrat celo negativen prizvok, saj gre za omejevanje svobode dela z zaščitenimi vsebinami. Večina definicij, ki jih najdemo predvsem na spletu, se opira na to povezavo ter predstavlja dominanten pogled na sistem DRM. Tak pogled bi lahko definirali kot **definicijo sistema DRM v ožjem pomenu** in ga v takšni obliki najdemo tudi v strokovni literaturi [K3].

Sistem DRM pa je lahko bistveno širši pojem, ki ima opravka s celotnim življenjskim krogom vsebine. Širša definicija tega pojma bi se lahko glasila:

Definicija sistema DRM v širšem pomenu:

»***Sistem DRM je odgovoren za vse procese, ki imajo opravka z vsebinami. Posega na področja identifikacije, opisa (metapodatki), zaščite, distribucije, nadzora uporabe ter plačila vsebin.***«



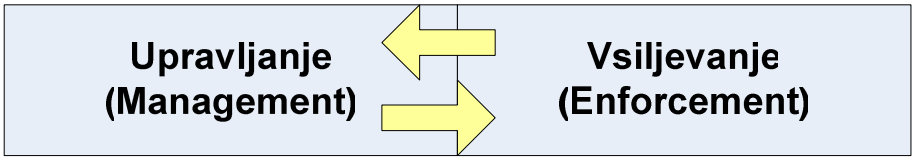
Sl. 6: Procesi v življenjskem krogu vsebin

Z vsebinami se v splošnem ukvarjajo sistemi za upravljanje z vsebinami, ki so znani pod terminom CMS (ang. Content Management System). V splošnem sistem DRM predstavlja neko vrsto takega sistema oz. je njegov sestavni del. Pri tem je operacije nad vsebinami mogoče razdeliti v dva dela in sicer:

- funkcije upravljanja (ang. Management) in
- funkcije vsiljevanja omejitev (ang. Enforcement).

Funkcije upravljanja se osredotočajo na upravljanje digitalnih pravic (ang. Managing Digital Rights) oz. vsebin. V to skupino spadajo identifikacija in opis zanimivih vsebin, dodajanje metapodatkov, definicija pravic nad vsebinami, distribucija ter vzpostavitev primernega poslovnega modela. Ta del se nanaša na upravljanje z vsebinami in posega na področje CMS sistemov. Predstavlja del definicije sistemov DRM, ki klasično ožjo definicijo spremeni v bolj splošno in širšo definicijo tega pojma.

Funkcije vsiljevanja se osredotočajo na digitalno upravljanje pravic (ang. Digitally Managing of Rights). Sem spadajo mehanizmi za zaščito vsebin in vsiljevanje omejitev, kot jih določajo pravice in pravila uporabe posameznih vsebin. Za zaščito se uporablja dvonivojski pristop s tehnikami kriptiranja in sekundarni varnostni mehanizmi. Ta del opisuje definicija sistema DRM v ožjem pomenu. Današnji DRM sistemi, predvsem tisti, ki so osredotočemi na večpredstavne vsebine, so znani po tej ožji definiciji. Večina uporabnikov in ponudnikov vsebin ob pojmu DRM največkrat pomisli na vsiljevanje in restrikcije, kar pa je le del funkcionalnosti sodobnega splošnega sistema DRM. [K3]



Sl. 7: Dva aspekta splošnega sistema DRM

3.1.2. Dejavniki okolja na sistem DRM

Splošen sistem DRM se dotika praktično vseh procesov in akterjev, ki sodelujejo v življenjskem krogu vsebin. Poleg tehnoloških dejavnikov na sisteme DRM vplivajo tudi drugi dejavniki, od katerih je odvisen uspeh določenega sistema DRM. Vpliv ne-tehnoloških dejavnikov je včasih celo pomembnejši od tehnoloških.

Dejavnike okolja na sistem DRM lahko povzamemo v:

- tehnološke,
- ekonomske,
- pravne in
- socialne.

Tehnološki dejavniki so neposredno povezani s tehnično zasnovo in izvedbo posameznega sistema DRM. Med njimi so najbolj pomembni stopnja varnosti oz. zaupanja sistema, razširljivost in fleksibilnost, enostavnost implementacije ter odprtost. Tehnološki dejavniki so natančneje opisani v nadaljevanju (poglavje 3.3.1).

Pravni vidik je pomemben s stališča definiranja legalnosti uporabljenih mehanizmov za zagotavljanje varnosti in sledljivosti vsebin. Konzumirane vsebine je mogoče neposredno povezati z identiteto uporabnikov in njihovimi navadami, kar že posega na področje varovanja osebnih podatkov. DRM sistem ne sme kršiti teh pravic ter sme občutljive podatke uporabljati samo za potrebe delovanja sistema, nikakor se pa ti podatki ne smejo zlorabiti. V tem pogledu pravni vidik vpliva tudi na socialni vidik.

Med dejavniki ekonomskega vidika je prav gotovo najpomembnejša cena oz. uravnoteženo razmerje med ceno dovolj zmogljivega DRM sistema glede na vrednost ščitenih vsebin. Nesmiselna je uporaba zelo zmogljivega in dragega sistema za zaščito nepomembnih vsebin. V angleški literaturi za to primerjavo

najdemo izraz »A 1000 $ lock for a 1 $ worth content.« oz. ključavnica za 1000 $, ki ščiti vsebino vredno 1 $, kar ekonomsko ni upravičeno.

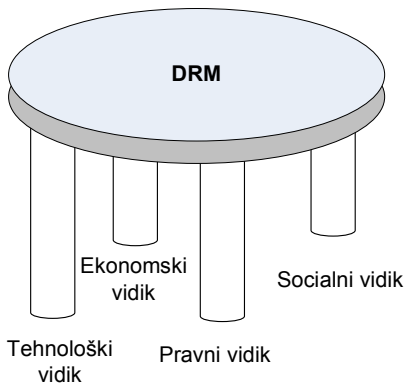
Socialna vidika sta predvsem dva in sicer odnos uporabnikov ter odnos ponudnikov vsebin do sistema DRM.

Za uporabnike je sistem DRM praktično skoraj nepotreben oz. je dodatek, ki ga pri konzumiranju vsebin in uporabi storitev nujno ne potrebujejo. Takšen pogled na to področje ima večina uporabnikov. Pri tem je posebno pomemben dejavnik uporabniške prijaznosti in enostavnosti uporabe. DRM komponenta pri konzumiranju vsebin nikakor ne sme biti moteča. Socialni vidik je pri komercialnih sistemih mogoče še najbolj pomemben od vseh navedenih dejavnikov. Uporabniki so namreč končni člen v verigi in neposredno odgovorni za tržni uspeh celotne rešitve (slika št. 2). DRM sistem pri tržno-orientiranih sistemih za uporabnike ne sme predstavljati ovire.

Izjemo tega pravila predstavljajo ne-tržno usmerjeni projekti, kjer so od ekonomskih pomembnejši drugi interesi kot so npr. nacionalna varnost, varovanje osebnih podatkov, dostop do uradnih dokumentov v digitalni obliki in drugi. Varovane vsebine in informacije so posebno občutljive, njihova učinkovita zaščita je bolj pomembna od ugodja uporabnikov. Postopki za zaščito so zakonsko predpisani in nadzorovani preko ustreznih državnih organov in institucij. Primer takšnega pristopa je npr. dostop do osebnih podatkov preko spletnega portala. Pri tem se morajo podatki od ustrezne državne institucije prenesti do uporabnika preko nenadzorovanega internetnega omrežja. Za zaščito skrbi sistem DRM in pravila uporabe ter varnostnih mehanizmov so strogo predpisana. Kljub morebitni neprijaznosti in težavnemu uporabniškemu vmesniku bo takšen sistem še vedno funkcioniral, ker ni odvisen izključno od ekonomskih dejavnikov.

Na drugi strani sistem DRM ščiti avtorje in ponudnike vsebin ter skuša onemogočati nelegalno uporabo. Za ponudnike vsebin je pri tem od tehnoloških dejavnikov zelo pomembna stopnja varnosti sistema. Noben sistem ni 100 % varen. Mora pa biti dovolj varen, da razumljivo dobro ščiti vsebine pred napadi in je ob tem še ekonomsko upravičen.

Vpliv navedenih dejavnikov okolja na sistem DRM lahko ponazorimo s sliko »mize oz. stola«, ki ima štiri noge. Vsaka noga predstavlja enega od dejavnikov, katerih vpliv ne sme biti ne prešibek ne premočan. Da bo miza povsem stabilna, morajo biti vsi dejavniki uravnoteženi oz. »noge« mize enako dolge. [K3]



Sl. 8: Ponazoritev vpliva dejavnikov okolja na sistem DRM

3.2. Klasifikacija sistemov DRM

Sistemi DRM so si glede osnovnih zahtev in nalog med seboj presenetljivo podobni. Vsem je skupna velika skrb za varovanje dostopa do vsebin, varna distribucija ter nadzor nad uporabo. Kljub temu jih je mogoče deloma razvrstiti po nekaterih kriterijih.

3.2.1. Po vrsti vsebin

Sistemi DRM so namenjeni zaščiti različnih vrst vsebin, pri čemer so lahko specializirani na določen tip vsebine. Največkrat so to večpredstavne vsebine, predvsem video. S stališča sistemov DRM lahko vsebine razdelimo v tri logične skupine:

- dokumenti,
- posamezni večpredstavni elementi in
- programska oprema.

Vrsta vsebine		Značilnosti
dokumenti	skupek večpredstavnih elementov	V to skupino spadajo dokumenti v elektronski obliki. Sestavljajo jih različni večpredstavni elementi, med katerimi sta najbolj tipična tekst in slikovno gradivo. Skupna značilnost dokumentov je, da se tekstovni del med procesi priprave in obdelave, vključno z DRM mehanizmi, nikakor ne sme popačiti oz. spremeniti pomena. Vrste dokumentov, ki so zanimive za zaščito s sistemi DRM: avtorska dela v elektronski obliki (npr. E-knjige), pravni dokumenti (npr. pogodbe), tajni dokumenti, dokumenti s poslovnimi skrivnostmi in drugo.
večpredstavni elementi	tekst	Čisti tekst je najmanj zahtevna vrsta večpredstavnih elementov glede na potrebne strojne zmogljivosti (terminalne) opreme ter prenosnih kapacitet. Potrebna pasovna širina za strujanje je odvisna od načina zapisa tekstovnih podatkov, vendar je v splošnem zelo majhna, reda cca. 50 kbit/s. Tekstovne informacije je mogoče zelo učinkovito kompresirati, pri čemer se vedno uporablja breizgubne kompresijske postopke, kar je pogoj za ohranitev celotne informacije.
	slike	V to skupino spadajo statične slike v različnih formatih. Najpogostejši formati so JPG, GIF in PNG. Uporabljajo se breizizgubni in izgubni kompresijski postopki. Dosežena kompresijska razmerja so v prvem primeru v povprečju 2:1 in v drugem do 100:1 ob še uporabni kvaliteti.
	zvok	Sem uvrščamo vse oblike avdio vsebin. Uporabljena kompresija je brezizgubna ali izgubna, pri čemer se za potrebe večpredstavnih storitev večinoma uporablja slednja. Potrebna pasovna širina za strujanje za kompresirano obliko zvočnih vsebin se giblje od 16 kbit/s (slaba kvaliteta) do 512 kbit/s (zelo kvaliteten večkanalni zvok).

	video	Video je trenutno najzahtevnejši večpredstavni element. Zaradi izjemno velike količine informacij se skoraj vedno za zapis uporabljajo izgubni kompresijski postopki. Izhodna kvaliteta in potrebna pasovna širina za strujanje je odvisna tako od same vsebine ter od izbranega kompresijskega postopka. Za video standardne definicije (klasična TV kakovost) ob uporabi starejših kompresijskih postopkov (MPEG 2) je potrebna pasovna širina reda 4 Mbit/s do 10 Mbit/s. Z novejšimi kompresijskimi postopki (MPEG-4 AVC, Real 10, MS Windows Media 9) je ob približno enaki izhodni kvaliteti potreba pasovna širina za strujanje bistveno nižja, reda 1 Mbit/s do 2 Mbit/s. Video visoke definicije (HDTV) zahteva višje pasovne širine. V primeru zapisa MPEG-2 je to reda vsaj 20 MBit/s in pri novejših zapisih (MPEG-4 AVC, MS WM9) reda 7 Mbit/s.
programska oprema	aplikacije	Sem uvrščamo klasično programsko opremo.
	igre	V to skupino spadajo zabavna programska oprema, kar večinoma predstavljajo računalniške igre.

Tab. 2: Razvrstitev vrst vsebin in njihove najbolj značilne lastnosti

Razlike med sistemi DRM se pokažejo v sklopu funkcij vsiljevanja omejitev glede na implementacijo specifičnih mehanizmov zaščite vsebin. Pri tem se uporablja kombinacija več mehanizmov, ki se med seboj dopolnjujejo. Primarno se zaščita doseže s kriptiranjem vsebin. V primeru zlorabe in razbitja kode sama enkripcija ni zadostna. Sekundarno se zato uporablja še mehanizem dodajanja vodnega žiga in mehanizem določanja prstnega odtisa vsebin, kar omogoča sledljivost vsebin. Prilagojenost posameznega sistema DRM se navadno pokaže prav pri tem mehanizmu.

V primeru dokumentov in teksta kot večpredstavnega elementa se izvorna informacija ne sme spremeniti. To velja tudi za mehanizme sistemov DRM.

V primeru ostalih večpredstavnih elementov ohranjanje popolnoma originalne oblike zapisa ni več nujno. Dovolj dobro se mora ohraniti le izhodna oblika vsebine, kot jo dojema uporabnik. Ta lastnost je dvorezen meč, saj poleg dodatnega manevrskega prostora zahteva tudi dodatno robustnost od uporabljenih varnostnih mehanizmov. V primeru vodnega žiga mora le-ta bit odporen na različne posege, kot je kompresija, spreminjanje parametrov vsebine (skaliranje, sprememba barvne globine, degradacija, ...) in v skrajnem primeru analogna reprodukcija in ponovna digitalizacija vsebine.

Programska oprema predstavlja posebno vrsto vsebin, ki se prav tako lahko ščiti s sistemi DRM. Pri tem je še bolj kot pri dokumentih pomembna uporaba brezizgubnih postopkov, saj v nasprotnem primeru programska oprema ni več funkcionalna oz. postane celo škodljiva. Najbolj radikalne pristope zaščite in omejevanja zlorab zasledimo pri računalniških igrah. Standardni mehanizmi omejevanja so vnos gesel ali serijskih številk in spletna registracija pri čemer se neavtorizirana uporaba vsebine zavrne. Naprednejši mehanizmi omogočajo drugačne pristope, kjer uspešno detektirana zloraba ne povzroči takojšnje zavrnitve dostopa do vsebine. Primer takšnega sistema je zaščita FADE [W4], ki jo je razvilo podjetje Code Masters in je bila prvič uporabljena v računalniški igri Operation Flashpoint. Pri nelegalnih kopijah se uporabniška izkušnja časovno

čedalje bolj slabša. V primeru igre Operation Flashpoint, ki spada v zvrst prvoosebnih strelskih iger, to pomeni časovno stalno slabšanje uporabniškega nadzora. Postopek se nadaljuje dokler normalna uporaba ni več mogoča, kljub temu da je igro še vedno mogoče zagnati. Takšen pristop omogoča demonstracijo vsebin (iger) ter naj bi prisilil uporabnike k nakupu legalne različice.

3.2.2. Po načinu izvedbe

Sistemi DRM so rešitve tipično programske (»softverske«) narave. Varnost se dosega z različnimi mehanizmi zaščite vsebin ter skrivanjem vitalnih delov za odklepanje vsebin – ključev. Varnostno kritični del predstavljata distribucijski kanal in uporabniška terminalna oprema.

Za uporabo vsebin mora uporabnik posedovati tako zaščiteno vsebino kot tudi ključe za odklepanje. Oba elementa sta seveda zaščitena. Ne glede na mehanizme zaščite ključev se ti morajo ob uporabi vsebin pretvoriti v nezaščiteno obliko, kar pa predstavlja določen varnostni problem. Zaščita ključev je zato vitalnega pomena. V primeru samo programskih rešitev se ta problem največkrat rešuje s skrivanjem ključev na uporabniški terminalni opremi, kar je znano pod izrazom varnost s skrivanjem (ang. Security by Obscurity). V primeru razkritja ključev vsebine niso več varne in pogosto nezakonito preidejo v »javno last«. Na stopnjo nevarnosti tega problema vpliva tudi vrsta terminalne opreme. Najmanj verjetno zlorabo predstavljajo manj poznane in zaprte vrste terminalne opreme, kot so npr. mobilni terminali, TV komunikatorji in namenski večpredstavni predvajalniki. Večji problem predstavljajo klasični PC kompatibilni osebni računalniki in naprave, ki so narejene na podlagi te platforme. Značilna primera programskih sistemov DRM sta produkta podjetij Microsoft DRM in Real DRM.

Drugi način izvedbe je kombinacija programske in posebne strojne opreme, ki skuša biti delno ali v celoti zaščitena pred zlorabo (ang. Tamper Resistant HardWare, Tamper Free HardWare). Varnostno kritični elementi so skriti v okviru dodatne strojne opreme v terminalni opremi in zlorabe so na ta način bistveno težje. Slabost tega pristopa je v večji ceni sistema (predvsem terminalne) opreme ter težji implementaciji na določenih področjih, kot je npr. PC platforma. Značilen primer takšnega pristopa so sistemi pogojnega dostopa, na področju PC platforme pa iniciativa Trusted Computing.

3.3. Uvrstitev v TK model

ISO-OSI (ang. International Organization for Standardization, ang. Open Systems Interconnect) predstavlja standardni model za načrtovanje telekomunikacijskih sistemov in storitev. Potreba po takšnem načinu načrtovanja se je pokazala zaradi izjemne kompleksnosti TK sistemov.

Model je sestavljen iz sedmih slojev (ang. Layer), ki logično grupirajo posamezne funkcije TK sistemov. Primeri specifičnih implementacij TK sistemov po OSI modelu se imenujejo protokolni skladi. Različni protokoli so po funkcijah grupirani po slojih in so urejeni v obliki sklada, od koder izvira ime takšne strukture. Pomembna lastnost posameznih slojev je, da so hierarhično organizirani od najnižjega do najvišjega, pri čemer spodnjeležeči sloj svoje storitve višjeležečemu sloju ponuja preko storitvene dostopovne točke (ang. Service Access Point, SAP). Posamezni sloji so med seboj neodvisni, kar omogoča lažje načrtovanje, upravljanje in nadgradnjo sistema. Najnižji sloj v modelu je fizični, ki zajema vse fizične elemente TK sistemov. Najvišji sloj je aplikacijski, ki preko storitvene dostopovne točke svoje storitve neposredno nudi uporabniku. Podatki so vsebovani v protokolnih podatkovnih enotah (ang. Protocol Data Unit, PDU), ki imajo različna imena glede na specifičen sloj. Med posameznimi sloji se podatki pošiljajo s pomočjo mehanizma ovijanja oz. enkapsulacije. Višjeležeči sloj (npr. sloj 4) svoj PDU preda nižjeležečemu sloju (npr. sloj 3), pri čemer ga le-ta obravnava kot podatek. V primeru medslojne komunikacije se tako interpretirani podatki opremijo še z dodatnimi informacijami v obliki glave in repa. Postopek se postopoma ponavlja preko vseh slojev protokolnega sklada. Opisani način komunikacije se imenuje vertikalna ali fizična komunikacija in predstavlja dejanski potek komunikacije med posameznimi sloji. Logično gledano pa posamezni sloji komunicirajo le med istoležečimi sloji, kar se imenuje horizontalna ali logična komunikacija.

Sistem DRM lahko glede na model ISO-OSI uvrstimo v najvišji, aplikacijski sloj. DRM funkcionalnosti predstavljajo del nalog uporabniške **aplikacije** za dostop do storitev, ki se izvaja na uporabniški terminalni opremi. Kljub uvrstitvi v aplikacijski sloj je mogoče funkcije sistema DRM nadalje razvrstiti v več slojev, analogno OSI modelu. Na ta način se poveča jasnost zasnove in izpostavijo skupne značilnosti sistemov DRM.

Predlagani slojni model sistema DRM:

- Višja DRM sloja – visokonivojske DRM storitve
    - aplikacijski sloj
    - posredovalni sloj
- Srednja DRM sloja – vmesni povezovalni člen med višjimi in nižjimi sloji
    - sloj opisa pravic (REL)
    - sloj interpretacije pravic REL
- Nižji DRM sloji – nizkonivojske implementacijsko specifične DRM funkcije in mehanizmi
    - višji servisni sloj
    - nižji servisni sloj
    - fizični sloj

Višji sloji sistema DRM so neposredno povezani z ostalimi aplikacijami za dostop do storitev in uporabo vsebin. Aplikacijski DRM sloj omogoča čim bolj enostaven in transparenten način uporabe splošnih DRM funkcionalnosti ter pravilno upodabljanje vsebin, ki so zaščitene preko sistemov DRM. Lahko je implementiran v obliki samostojne aplikacije ali pa je del drugih ne-DRM aplikacij ter jim s tem omogoča uporabo DRM storitev. Posredovalni DRM sloj neposredno povezuje aplikacijski DRM sloj z ostalimi sloji. Med njegove naloge lahko spadajo identifikacija vsebin, zahtevan nivo zaščite, določanje vrste pravic do vsebin in mehanizmi avtentikacije uporabnika in uporabniške terminalne opreme.

Srednja sloja predstavljata vmesni člen in višjim slojem zakrivata kompleksnosti specifičnih implementacij določenih mehanizmov DRM v nižjih slojih. Takšen pristop bistveno pripomore k večji preglednosti in boljši kompatibilnosti med različnimi implementacijami sistemov DRM z ostalimi sistemi.

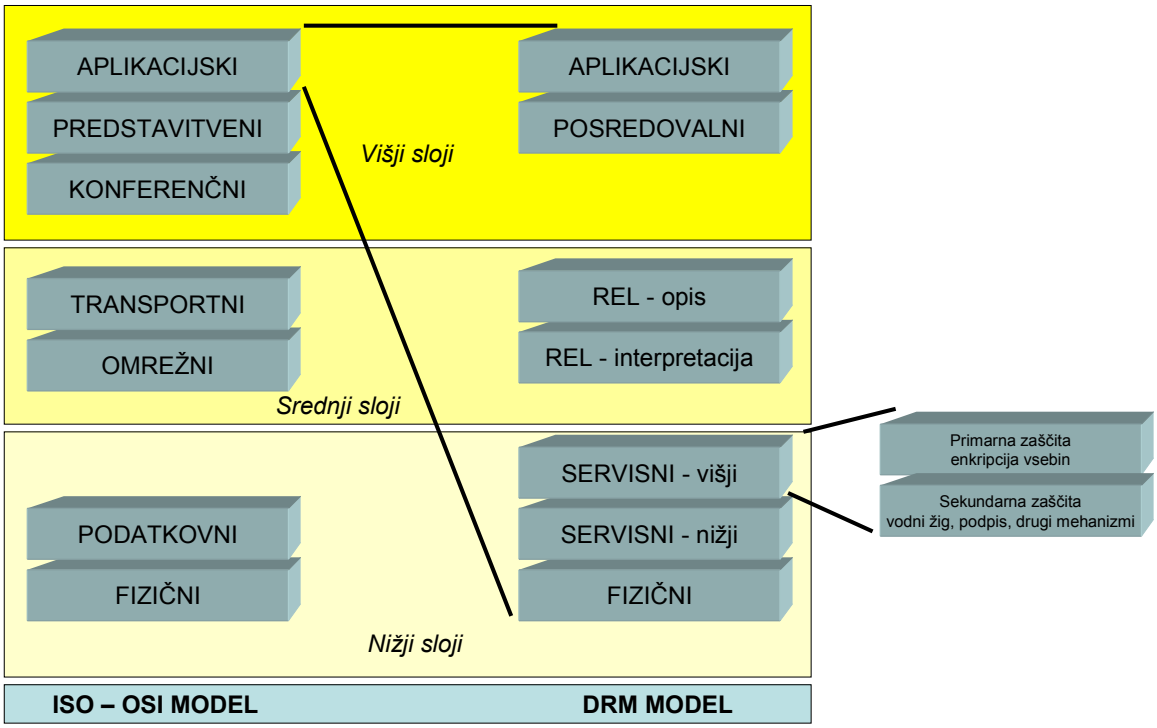
Termin REL (ang. Rights Expression Language) označuje jezik za opis pravic in predstavlja najbolj pogost pristop za definicijo pravic pri sistemih DRM. Sloj opisa pravic je zadolžen za zbiranje informacij o vsebinah in pravicah o njihovi uporabi. Konkretna interpretacija pravic se vrši v sloju interpretacije pravic.

Nižji DRM sloji definirajo specifično implementacijo DRM mehanizmov ter nudijo ustrezno okolje za njihovo izvajanje. Pri tem gre večinoma za vključitev funkcionalnosti sistemov DRM v konkretno izvajalno okolje, ki ga sestavljajo operacijski sistem in sistemska sredstva.

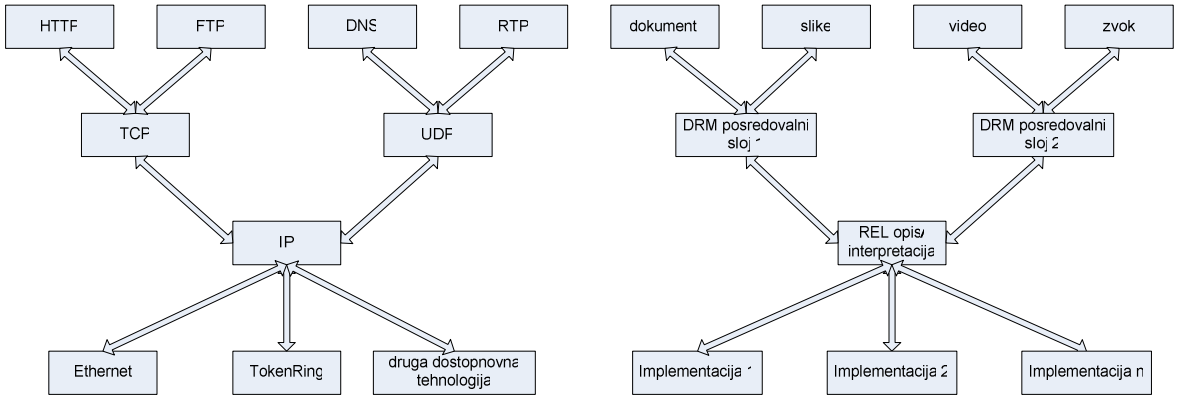
Med naloge višjega servisnega DRM sloja spadajo mehanizmi za zagotavljanje varnosti. Logično gledano je te mehanizme po funkciji mogoče razdeliti v primarni in sekundarni sloj zaščite. Primarno zaščito predstavlja enkripcija vsebin, sekundarno pa mehanizmi dodajanja vodnega žiga, digitalni certifikati, generacija prstnega odtisa in drugi.

Nižji servisni sloj definira način zapisa DRM vsebin in omogoča komunikacijo z drugimi sistemskimi aplikacijami in napravami preko ustreznih gonilnikov. Fizični DRM sloj specifično implementacijo sistema DRM povezuje z izvajalnim okoljem. Na ta nivo lahko uvrstimo elemente kot je npr. datotečni sistem in ostali osnovni sistemski servisi.

[K1]



Sl. 9: Slojni model sistema DRM



Sl. 10: Vizualna predstavitev odnosa med sloji in funkcionalna primerjava med slojnima modeloma TCP/IP in DRM

Sodobni sistemi DRM so dovolj zanesljivi, da lahko delujejo samostojno. Kljub temu pa se učinkovitost in stopnja varnosti bistveno poveča, če se uporabi večnivojski pristop, kjer se med seboj dopolnjuje več različnih mehanizmov zagotavljanja varnosti na različnih slojih OSI modela. Nekateri najbolj značilni mehanizmi, predvsem za zaščito večpredstavnih vsebin v okolju IPTV, so opisani v nadaljevanju.

Dostopovni sloj

Na dostopovnem sloju je primerna uporaba mehanizmov navideznih lokalnih omrežij (ang. Virtual LAN), dostopovnih list (ang. Access List) in drugih specifičnih mehanizmov, kot sta avtentikacija po MAC naslovu in varovanje porta (ang. Port Security).

Mehanizem navideznih lokalnih omrežij omogoča navidezno kreiranje več lokalnih omrežij. Uporabniki različnih VLAN omrežij so privzeto popolnoma ločeni med seboj. Komunikacija med njimi poteka preko omrežnih usmerjevalnikov. Prednost tega je realizacija več VLAN omrežij na isti omrežni opremi, kot je npr. omrežno stikalo z vgrajeno podporo VLAN. Omrežja so med seboj ločena, prav tako je omejen promet tipa broadcast.

Dostopovno listo v splošnem sestavlja množica pogojev, ki dovoljuje ali pa preprečuje komunikacijo. Mehanizem dostopovnih list je uporaben praktično na večini slojev komunikacijskega modela (od L2 do L7). Ob pravilni uporabi omogoča zagotavljanje visoke stopnje varnosti.

Mehanizem avtentikacije po MAC naslovu omogoča dostop do omrežja le določeni terminalni opremi, ki je registrirana v sistem. Samo uporaba avtentikacije po MAC naslovu danes ni več dovolj močna zaščita, je pa učinkovita v zaprtih okoljih in v kombinaciji z ostalimi mehanizmi.

Avtentikacija po portu oz. varovanje porta omogoča ugotavljanje izvora prometa glede na priključitveni port na omrežni opremi (npr. TV komunikator v sobi 1 je priključen na port 3 na omrežnem stikalu dostopovnega omrežja). Mehanizem onemogoča napade prisluškovanja in ugrabljanja identitete drugih uporabnikov. Gre za nestandardno in konkretno rešitev podjetja CISCO.

Omrežni in transportni sloj

V splošnem so primerni mehanizmi dostopovnih list ter različnih načinov tuneliranja in kriptiranja komunikacije, kot so IPSEC, SSL (ang. Secure Socket Layer) in TSL (ang. Transport Layer Security).

Aplikacijski sloj

Na aplikacijskem sloju se uporabljajo različni sistemi, kot so požarni zidovi (ang. Firewall), sistemi za detekcijo in preprečevanje zlorab (ang. Intrusion Detection System, Intrusion Prevention System), filtri za odstranjevanje neželene pošte, anti-virusni in anti-spyware sistemi ter različni vmesni strežniki (ang. Proxy Server). Pravilno nastavljena politika na požarnem zidu lahko prepreči večino napadov, specializirane naloge pa opravljajo ostali sistemi. Za zaščito pri splošni uporabi spleta je primerna uporaba filtrirnih vmesnih proxy strežnikov. Omogočajo tudi dodatne funkcionalnosti, kot je npr. tematsko filtriranje vsebine (npr. storitev starševska kontrola).

3.4. Nevarnosti in okolja sistemov DRM

Različna okolja in pripadajoče vrste nevarnosti predstavljajo izziv za načrtovalce sistemov DRM. V določenih kombinacijah okolij in nevarnosti, ki jih vnašajo, so sistemi DRM prva in edina obrambna linija. Velja pravilo, da je celota tako močna, kot je močan njen najšibkejši člen. Izbira optimalnega sistema DRM in njegovih elementov je v tem primeru izjemnega pomena.

3.4.1. Vrste nevarnosti

V splošnem lahko vrste nevarnosti, ki ogrožajo vsebine, razdelimo v dve veliki skupini in sicer na:

- nevarnosti digitalne luknje in
- nevarnosti analogne luknje.

Ena izmed pomembnejših skupnih značilnosti vsebin, ki so ščitene z sistemi DRM, je digitalna oblika. Vsebine v digitalni obliki imajo vrsto prednosti kot so popolna reprodukcija, hramba na digitalnih nosilcih, uporaba kompresijskih postopkov za zmanjšanje obsega, relativna neobčutljivost na zunanje vplive in na staranje. Iste vsebine je mogoče ekvivalentno predstaviti tudi v klasični analogni obliki. V primeru dokumentov in slikovnega gradiva je to papirna različica, v primeru zvoka in v videa pa reprodukcija na analognih medijih.

3.4.1.1. Digitalna luknja

Pojem *digitalna luknja* (ang. Digital Hole) opredeljuje vse možne načine nelegalne zlorabe vsebin v digitalni obliki. Najpogostejši napadi so v obliki nelegalnega dekodiranja vsebine oz. »razbitja kode«. Večina zlorab zaradi prednosti digitalne oblike spada v to kategorijo. Pri sistemih DRM za zaščito na tem nivoju skrbijo različni mehanizmi kriptiranja. Kljub temu je pri načrtovanju potrebno nameniti posebno skrb celotni verigi, drugače lahko pride do zlorab, kot kaže naslednji primer.

Primer tovrstne zlorabe predstavlja metoda DeCSS, ki omogoča nelegalno reprodukcijo video vsebin na DVD nosilcih po standardu DVD-video. Video vsebine po tem standardu so kriptirane po postopku CSS (ang. Content Scrambling System) in varovane na treh nivojih. Varnostni mehanizmi so vgrajeni v DVD predvajalno strojno opremo, v DVD predvajalno programsko opremo in na sam optični podatkovni nosilec. Legalna uporaba je mogoča le s kombinacijo vseh treh elementov. Standard DVD-video pri tem že v osnovi skuša onemogočiti nelegalno reprodukcijo v smislu presnemavanja vsebin, nelegalno gledanje vsebin in omejitev vsebin na določeno geografsko področje. V primeru uspešne zlorabe digitalne reprodukcije in pridobitja vsebine iz optičnega nosilca je vsebina še vedno neuporabna, ker je kriptirana. Pri tem se pojavijo značilni artefakti v obliki zelenih kock, ki so znani pod angleškim izrazom »green marsians«.

Kljub zaščiti na več nivojih so le-to z metodo vzvratnega inženiringa (ang. Reverse Engineering) kmalu (leta 1999) uspeli popolnoma onemogočiti. Šibki člen v verigi so tokrat predstavljali ključi za dekodiranje. Pri postopku CSS je nabor možnih ključev precej omejen. Ključi so fizično shranjeni v strojni DVD predvajalni opremi.

Mediji z zaščitenimi vsebinami so kriptirani po enem iz omejenega nabora možnih ključev, pravilnega ugotovi strojni predvajalnik. Zaradi ameriške zakonodaje o izvozu varnostnih mehanizmov je velikost ključev omejena na 40 bitov. To za današnje procesorske zmogljivosti osebnih računalnikov ni več pretirana ovira in uspešen je tudi napad z grobo silo (ang. Brute Force), pri katerem se pač preveri vse možne kombinacije. V primeru CSS je bilo to zaradi slabe izkoriščenosti 40 bitnega nabora kombinacij še nekoliko lažje. Kmalu po tem so se pojavila programska orodja za razbitje CSS kode in popolno digitalno reprodukcijo vsebin. DeCSS je v kombinaciji z sodobnimi video kompresijskimi postopki, kot so MPEG-4, DivX in XVID, omogočil eksplozijo nelegalne distribucije video vsebin. Na področju videa je kodek DivX po pomenu podoben nelegalni distribuciji audio vsebin v formatu MP3.

Za avtorja prvega uspešnega algoritma za razbitje kode CSS, ki se imenuje DeCSS (ang. DEcrypt CSS), velja norveški najstnik Jon Johansen. Algoritem DeCSS je javno objavil na spletu oktobra leta 1999. Zanimive so bile tudi pravne posledice tega dejanja. Leta 2000 so norveški policisti vdrli v njegovo hišo in preiskali prizorišče. Proti avtorju so postavili obtožbo in ga postavili pred sodišče. Vse obtožbe so leta 2003 zavrnili in zgodba je dobila epilog januarja leta 2004, ko so opustili nadaljnji pregon. Odločitev sodišča je bila, da je sam algoritem DeCSS še legalen, njegova uporaba pa ne. Vprašljiva je bila potem tudi pot razvoja algoritma, o čemer se niso natančno izjasnili.

Zanimiva je tudi implementacije algoritma DeCSS. Realiziran je bil v številnih programskih jezikih, pri čemer najmanjše implementacije obsegajo le nekaj sto byte-ov.

[W5]

```
void CSSdescramble(unsigned char *sec,unsigned char *key)
{
  unsigned int t1,t2,t3,t4,t5,t6;
  unsigned char *end=sec+0x800;

  t1=key[0]^sec[0x54]|0x100;
  t2=key[1]^sec[0x55];
  t3=(*((unsigned int *)(key+2)))^(*((unsigned int *)(sec+0x56)));
  t4=t3&7;
  t3=t3*2+9-t4;
  sec+=0x80;
  t5=0;
  while(sec!=end)
    {
      t4=CSStab2[t2]^CSStab3[t1];
      t2=t1>>1;
      t1=((t1&1)<<8)^t4;
      t4=CSStab5[t4];
      t6=(((((((t3>>3)^t3)>>1)^t3)>>8)^t3)>>5)&0xff;
      t3=(t3<<8)|t6;
      t6=CSStab4[t6];
      t5+=t6+t4;
      *sec++=CSStab1[*sec]^(t5&0xff);
      t5>>=8;
    }
}
```

Sl. 11: Implementacija DeCSS v jeziku C

```
#!/usr/bin/perl
# 472-byte qrpff, Keith Winstein and Marc Horowitz <sipb-iap-dvd@mit.edu>
# MPEG 2 PS VOB file -> descrambled output on stdout.
# usage: perl -I <k1>:<k2>:<k3>:<k4>:<k5> qrpff
# where k1..k5 are the title key bytes in least to most-significant order

s''$/=\2048;while(<>){G=29;R=142;if((@a=unqT="C*",_)[20]&48){D=89;_=unqb2
4,qT,@
b=map{ord qB8,unqb8,qT,_^$a[--
D]}@INC;s/...$/1$&/;Q=unqV,qb25,_;H=73;O=$b[4]<<9
|256|$b[3];Q=Q>>8^(P=(E=255)&(Q>>12^Q>>4^Q/8^Q))<<17,O=O>>8^(E&(F=(S=O>>1
4&7^O)
^S*8^S<<6))<<9,_=(map{U=_%16orE^=R^=110&(S=(unqT,"\xb\ntd\xbz\x14d")[_/16
%8]);E
^=(72,@z=(64,72,G^=12*(U-
2?0:S&17)),H^=_%64?12:0,@z)[_%8]}(16..271))[_]^((D>>=8
)+=P+(~F&E))for@a[128..$#a]}print+qT,@a}';s/[D-HO-
U_]/\$$&/g;s/q/pack+/g;eval
```

Sl. 12: Ena izmed najkrajših implementacij, napisana v interpreterskem jeziku Perl (472 byte-ov)

3.4.1.2. Analogna luknja

Pojem *analogna luknja* (ang. Analog Hole) opisuje, podobno kot pri pojmu digitalne luknje, vse možne načine zlorabe vsebin, ko se le-te pretvorijo v analogno obliko. Ta korak se mora zgoditi najkasneje ob trenutku uporabe vsebin. Vsebine so najbolj izpostavljene prav v tem trenutku, to je, ko se nahajajo na uporabniški terminalni opremi oz. so v postopku upodabljanja (uporabe). Ljudje imamo analogna čutila in ne znamo uporabljati vsebin neposredno v digitalni obliki. Analogna oblika pri dokumentih največkrat pomeni papirno različico ali prikaz na prikazovalni enoti, kot je televizijski sprejemnik, računalniški monitor, projektor ali kakšna druga naprava. Video vsebine se prav tako upodabljajo na prikazovalnih enotah, zvočne vsebine pa se reproducirajo na audio reprodukcijskih napravah. Če odpovejo napadi v digitalni obliki, je vsebine še vedno mogoče nelegalno pridobiti v analogni obliki. V primeru dokumentov je možno fotokopiranje in optično branje (skeniranje), pri zvočnih in video vsebinah pa analogno presnemavanje ter ponovna digitalizacija. Velja pravilo »*Kar lahko vidim in slišim, lahko skopiram.*«. Tako pridobljene vsebine so zaradi vmesnih konverzij in drugih postopkov nekoliko slabše kakovosti, vendar še vedno zadosti uporabne, da so zanimive.

Preprečevanje tovrstnih zlorab je precej težje kot pri zlorabah digitalne luknje. Pri tem se skušata doseči dva cilja in sicer:

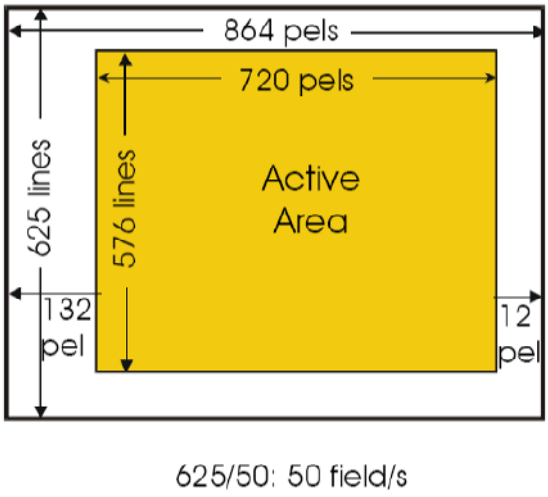
- sledenje vsebine in
- preprečevanje zlorabe vsebine preko analogne luknje.

Za dosego teh ciljev skrbijo sekundarni varnostni mehanizmi sistemov DRM, ki predstavljajo drugi nivo obrambe. Gre za precej kompleksne mehanizme, ki se šele začenjajo uporabljati v sodobnih sistemih DRM.

Za sledenje vsebine se uporablja mehanizem dodajanja vodnega žiga. V originalno vsebino se pred uporabo ostalih postopkov doda unikaten podpis. Pri tem vgrajeni podpis ne sme spremeniti vsebine ter mora biti odporen na različne napade oz. spremembe vsebine. Glavni cilj dodajanja vodnega žiga ni onemogočenje nelegalne uporabe vsebine, temveč ugotovitev identitete uporabnika, ki je vsebino zlorabil in neavtorizirano distribuiral naprej v omrežje.

Naslednji korak predstavlja aktivno preprečevanje zlorabe vsebin preko analogne luknje. V originalno vsebino se skuša vnesti motilni signal, ki v primeru zlorabe vsebino tako popači, da je neuporabna. Rešitve tega tipa so večinoma zaprte narave (ang. Proprietary). Bolj radikalen pristop napoveduje iniciativa Trusted Computing kjer je predvidena striktna uporaba dodatne strojne opreme za vsiljevanje predpisanih pravic. V skrajnem primeru bo uporabnik poleg licence potreboval tudi certificirano reprodukcijsko strojno opremo. To vključuje npr. zvočnike in zvočne vmesnike ter monitorje in grafične vmesnike z zmožostjo overovitve in ugotavljanja poskusov zlorab vsebin. Posledično to pomeni, da monitor kot samostojna enota ne bo prikazal vsebine, za katero bo menil, da je nelegalna.

Kot primer navedimo rešitev podjetja Macrovision. Tehnologija Macrovision ACP (ang. Analog Content Protection) skuša preprečevati nelegalno reprodukcijo DVD vsebin z uporabo analognih video snemalnih naprav, kot so VHS videorekorderji, naprave PVR in osebni računalniki z video-zajemalnimi vmesniki. Za analogno obliko video vsebin se uporablja več standardov, od katerih so najbolj razširjeni evropska sistema PAL (ang. Phase Alternation by Line) in SECAM (ang. Séquential Couleur à Mémorie) ter ameriški NTSC (ang. National Television Systems Committee). Zaradi analogne oblike posamezni slikovni elementi (ang. Pixel oz. Picture ELement, PEL) niso natančno definirani, določa jih analogna pasovna širina video signala. Definirano je število vrstic, posamezni elementi v vrstici pa ne. Kljub temu lahko signalu določimo določeno ekvivalentno ločljivost. Pri tem ločimo celotno ločljivost slike in aktivno ločljivost (aktivni del), ki določa dejansko prikazano sliko. Celotno ločljivost definira 625 vrstic z 864 slikovnimi elementi. Aktivni del določa 576 vrstic z 720 slikovnimi elementi. Razmere ilustrira slika št. 13.



Sl. 13: Celotni del in aktivni del slike pri PAL standardu

V neaktivni del slike (»temne vrstice«) se doda moteči signal, ki pri ogledu vsebin ne povzroča motenj, saj neaktivne vrstice slike niso prikazane. Pri poskusu reprodukcije pa moteči signal tako zmede analogne snemalne naprave, da vsebina ni uporabna. Motilni signal v neaktivnem delu je izbran tako, da po amplitudi zelo varira. Snemalna naprava zajema celoten signal in ga pri tem analizira. Zaradi velikih amplitudnih odstopanj motilnega signala pride do prekomerne kompenzacije signala, kar se v praksi odraža v zelo hitrih spremembah svetlosti slike. Velja tudi omeniti dejstvo, da so do sedaj bile uspešno onemogočene še vse rešitve podjetja Macrovision, kar ni zelo vzpodbudno za to področje.

[W6]

Sl. 14: Karikiran prikaz nevarnosti analogne luknje

3.4.2. Vrste okolij

Pojem *okolje* opisuje dejansko okolje, kjer vsebine »živijo« in se izvajajo operacije nad njimi. Klasifikacija okolij je pomembna, ker iz njihovih lastnosti izvirajo vrste potencialnih nevarnosti, iz tega pa posledično sledi ocena potrebne stopnje varnosti. V groben je okolja mogoče razdeliti na dve skupini – na nadzorovana in na nenadzorovana. Prvi tip opisujeta tudi izraza zaseben (ang. Private) in zaupanja vredna (ang. Trusted), drugi tip pa javen (ang. Public) ter zaupanja nevreden (ang. Untrusted). Določene kombinacije okolij, njihovih potencialnih nevarnosti in zahtevane stopnje varnosti potrebujejo več slojev zaščite vključno z sistemom DRM, druge pa sistema DRM sploh ne potrebujejo. Pobarvana polja v tabeli označujejo za sisteme DRM najbolj zanimiva okolja.

Vrste okolij			
Okolje	**Značilnosti**	**Ocena stopnje nevarnosti (1-5)**	**Ocena potrebnih varnostnih mehanizmov**
splošno internetno	Predstavlja splošno nenadzorovano javno internetno okolje.	Prenos informacij med dvema akterjema je popolnoma nenadzorovan in izpostavljen najvišji stopnji nevarnosti. Dovoljene so vse vrste terminalne opreme. Ocena nevarnosti: 5 Opisno: zelo nevarno okolje	Zaradi javnega omrežja, kjer posamezen operater nima popolnega nadzora, je zelo priporočena uporaba varnostnih mehanizmov na aplikacijskem sloju - sistem DRM. Dober sistem DRM lahko pri tem deluje samostojno. Na omrežnem sloju je možna uporaba navideznih zasebnih omrežij (npr. tehnologija IPSEC) in na transportnem Transport Layer Security (TSL). Problem analogne luknje rešujejo sekundarni varnostni mehanizmi sistemov DRM in specialna strojna oprema.
operatersko internetno	Predstavlja delno nadzorovano okolje, ki je pod neposrednim vplivom enega operaterja. Primer takšnega okolja je omrežje za prenos večpredstavnih vsebin v sklopu IPTV platforme preko nadzorovane dostopovne tehnologije (npr. xDSL).	Operater ima dober nadzor nad svojim celotnim omrežjem in nad dostopom uporabnikov do storitev. Poleg osebnih računalnikov je možna uporaba specializiranih in bolj zaprtih vrst terminalne opreme, ki so zato potencialno bolj varne. Tipično gre za predstavnike iz skupine TV komunikatorjev. Ocena nevarnosti: 3-5 Opisno: srednje do visoko nevarno okolje	V primeru osebnih računalnikov kot terminalne opreme je zelo priporočena uporaba sistemov DRM. Pri specializiranih napravah (TV komunikatorjih) sistem DRM ni nujno potreben. Zaradi zaprtosti in dobre identifikacije teh naprav v operaterjevo omrežje v skrajnem primeru varnostni sistem sploh ni potreben, je pa priporočen. Namesto sistemov DRM so primerni tudi sistemi pogojnega dostopa. Problem analogne luknje ostaja.

zaprto okolje	Predstavlja popolnoma zaprto in nadzorovano okolje. Dovoljene vrste terminalne opreme in način dostopa sta nadzorovana. Primeri takšnih okolij so: interno operatersko omrežje, omrežja v okviru hospitality okolij (hoteli, bolnice, zavodi), druga zasebna lokalna omrežja.	Upravljalec ima popoln nadzor nad dogajanjem v omrežju ter načinom dostopa do njega. Zelo pogosta je uporaba specializiranih vrst terminalne opreme, ki so lahko celo edino dovoljene. V primeru dostopa z osebnimi računalniki ali drugimi vrstami bolj kritične terminalne opreme je dostop do omrežnih storitev ločen že z varnostnimi mehanizmi na nižjih slojih. Ocena nevarnosti: 1-3 Opisno: nizko do srednje nevarno okolje	Doseže se lahko zelo visoka stopnja varnosti. Zelo učinkoviti so varnostni mehanizmi na dostopovnem sloju (virtualni LAN, dostopovne liste) in omrežnem sloju (dostopovne liste). Sistemi DRM večinoma sploh niso potrebni, so pa priporočljivi, če se kot terminalna oprema uporablja osebni računalnik. Problem analogne luknje zaradi tujega okolja ni več izrazit (redkokateri uporabnik bo skušal zlorabiti večpredstavne vsebine v hotelu).
mobilno okolje	Predstavlja zavarovana omrežja operaterjev mobilne telefonije. Novejša in bolj zmogljiva mobilna omrežja nudijo udobno uporabo večpredstavnih storitev. Zelo zanimiva je tehnologija DVB-H, ki združuje enosmerno (broadcast) omrežje z veliko zmogljivostjo za prenos vsebin ter mobilno omrežje za prenos povratnih informacij.	Dostop do storitev je možen le preko mobilnega terminala. Identiteta uporabnika je jasno določena (pametna kartica). Možnosti zlorab so majhne, saj natančno delovanje terminalne opreme ni javno znano. Mobilni terminal lahko pojmujemo kot odpornega na zlorabe (tamper resistant, tamper free). Ocena nevarnosti: 1-2 Opisno: nizko nevarno okolje	Varnostni mehanizmi so implementirani v okviru sistemske programske opreme mobilnega terminala in jih je zato težje onemogočiti. Pri novejših tehnologijah (DVB-H) je smiselna uporaba sistemov DRM ali sistemov pogojnega dostopa. Problem analogne luknje ostaja vendar njegova izraba ni smiselna. Kvaliteta večpredstavnih vsebin je prirejena (omejenim) zmogljivostim terminalne opreme.

Tab. 3: Klasifikacija okolij, njihove osnovne značilnosti, ocena stopnje nevarnosti in ocena potrebnih varnostnih mehanizmov

3.5. Arhitektura splošnega sistema DRM

3.5.1. Zahteve

Sistem DRM je vpet v širše okolje in ni odvisen samo od tehnoloških dejavnikov. Pomembno je upoštevati širše kriterije izbire, ki vplivajo na dejavnike okolja na sisteme DRM, kot je opisano v uvodnih poglavjih (poglavje 3.1.2).

Uporabniška prijaznost (ang. User Friendliness) – je potencialno najpomembnejši kriterij. Sistem DRM je s stališča uporabnikov nepotreben dodatek (»nujno zlo«) pri uporabi vsebin. Kompliciran in neprijazen način dostopa do vsebin bo odvrnil veliko večino uporabnikov. Podobno se morajo med uporabniškim zadovoljstvom in restriktivno politiko odločiti ponudniki vsebin.

Zaupanje (ang. Trust) – označuje stopnjo zaupanja vseh akterjev v verigi odnosov v sistem DRM. S stališča avtorjev in ponudnikov vsebin je to povezano s stopnjo varnosti njihovih vsebin in minimiziranjem možnosti zlorab. Za uporabnike zaupanje pomeni, da se njihovi podatki in navade ne bodo zlorabile.

Stopnja varnosti (ang. Security) – je kriterij, ki se najbolj izpostavlja. Potrebno je poudariti, da popolnoma varnega in nezlomljivega sistema ni oz. njegov približek ni ekonomsko upravičen. Sistem DRM skuša vsebine zavarovati pred nevarnostmi tako digitalne in kot tudi analogne luknje, pri čemer je slednje bistveno težje. Stopnja varnosti mora biti primerna vrednosti vsebin.

Ne glede na izbrano okolje ali tehnologijo je mogoče ugotoviti in opisati kriterije, ki bistveno vplivajo na stopnjo varnosti celotnega sistema, z nekaj preprostimi načeli. Ta načela so splošno veljavna in so:

- izogibanje globalnim skrivnostim – pri varnostnih mehanizmih in postopkih se je v največji meri potrebno izogibati globalnim varnostnim parametrom. Varnostno kritični parametri, kot so v primeru sistemov DRM npr. dekodirni/dekriptirni ključi, morajo biti čim bolj lokalizirani. Izogibati se je potrebno globalnim ključem, ki odklepajo vse vsebine ali celo celoten sistem.
- izogibanje centralnim potencialnim točkam odpovedi – potrebno se je izogibati arhitekturi in situacijam, kjer obstajajo ključni centralni elementi, ki v primeru odpovedi privedejo do odpovedi celotnega sistema. To posledični privede do distribuiranosti in uvedbe redundance komponent.
- ukrepanje v primeru zlorab – sistem mora omogočati ukrepanje v primeru zlorab, vdorov ali razbitja varnostnih algoritmov in ključev, posebno če se zgodijo na globalni ravni. V primeru sistemov DRM so varnostno kritični elementi vsebine same ter uporabniška terminalna oprema. Pri zlorabi mora biti mogoča programska nadgradnja varnostnega dela terminalne opreme z novimi izboljšanimi varnostnimi algoritmi in ključi (tudi ena izmed zahtev uporabniške DRM terminalne opreme).

Razširljivost in fleksibilnost (ang. Extensibility, Flexibility) – označuje možnosti prilagajanja sistemov DRM različnim tipom vsebin in potrebam razvoja novih storitev.

Implementacija (ang. Implementability) – opisuje zahtevnost implementacije v smislu potrebnih strojnih sredstev.

Odprtost (ang. Openness) – označuje stopnjo odprtosti sistema v smislu razkritja celote ali dela programske kode javnosti in s tem omogočanja javnega razvoja in izboljšav sistema. Pod ta kriterij spada tudi uporaba (odprtih) standardov.

Interoperabilnost, kompatibilnost (ang. Interoperability, Compatibility) – opisuje zmožnost delovanja v različnih okoljih in sodelovanja s komponentami drugih sistemov. Primer je uporaba zaščitene vsebine X s sistemom DRM A na uporabniški terminalni opremi B preko omrežja C.

Cena (ang. Cost) – označuje celotno ceno sistema, ki vključuje stroške nakupa, implementacije in vzdrževanja sistema DRM za ponudnike storitev ter posledično povišanje cene vsebin in storitev za uporabnike. [K3], [K4]

3.5.2. Akterji

V verigi odnosov pri delu z vsebinami pri sistemih DRM zasledimo tri značilne akterje. To so:

- avtorji vsebin oz. lastniki vsebin (ang. Content Owner),
- ponudniki vsebin (ang. Content Provider) oz. posredniki (ang. Content License Broker) in
- uporabniki.

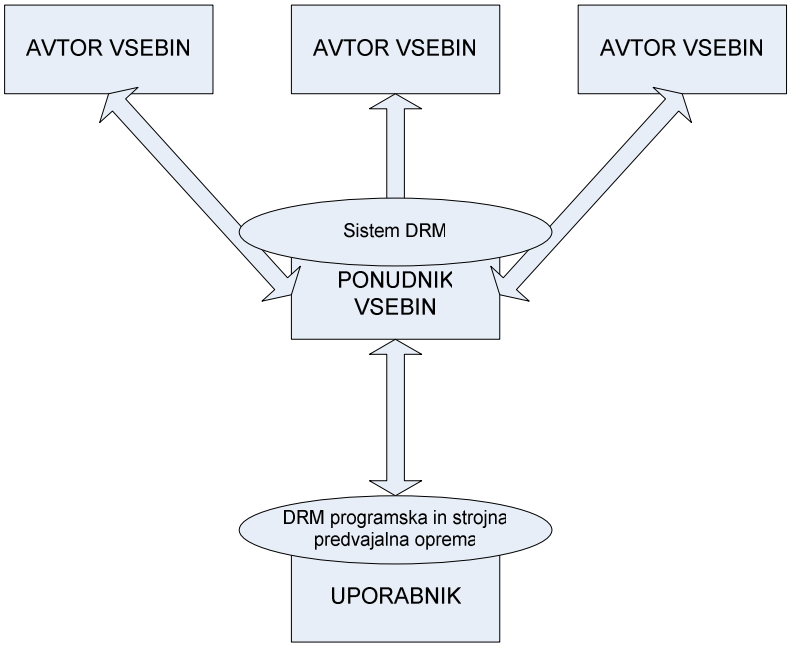
Avtorji in lastniki vsebin imajo navadno vse pravice do vsebin in prav tako definirajo osnovna pravila uporabe (licenco). Ponudniki vsebin oz. posredniki v njihovem imenu vsebine hranijo, ščitijo in ponujajo uporabnikom, ki so končni člen verige. Naloge ponudnikov vsebin so varen dostop in distribucija vsebin, opravljanje finančnih transakcij ter zagotavljanje spoštovanja pogojev uporabe skladno z pravili licence.

Vsebine so najbolj izpostavljene, ko so v okolju uporabnika. Ključen del sistema DRM je del uporabniške terminalne opreme, ki skrbi za zagotavljanje funkcionalnosti DRM – *DRM agent* oz. *uporabniški predvajalnik vsebin* (ang. End-User Player). Ta je lahko implementiran v obliki programske rešitve ali pa vsebuje tudi posebno proti napadom odporno strojno opremo (strojni dekodirnik, pametna kartica). Sistem DRM namreč ne zaupa neposredno uporabniku samemu, temveč njegovemu DRM agentu. DRM agent je odgovoren za vsiljevanje pogojev uporabe in za zagotavljanje legalne uporabe vsebin. Primer programskega DRM agenta je Microsoft Media Player z DRM funkcionalnostmi, primer strojnega pa npr. Apple iPod glasbeni predvajalnik.

DRM agent mora upoštevati naslednje zahteve:

- **pravilno delovanje** – agent mora delovati v skladu z DRM pogoji uporabe in preprečevati zlorabe.
- **individualizacija** – vsebine morajo biti vezane na točno določenega uporabnika in točno določeno terminalno opremo.
- **odpornost na zlorabe** (ang. Tamper Resistant, Tamper Free) – agent mora biti odporen na zlorabe. Poskusi obratnega inženiringa (ang. Reverse Engineering) naj bodo težko izvedljivi.

- **nadgradljivost** – agent mora biti nadgradljiv v smislu podpore različnim formatom vsebin, novim storitvam ter, kar je najpomembnejše – novim varnostnim mehanizmom. V primeru zlorabe in »razbitja« kode je tako možna nadgradnja sistema brez zamenjave uporabniške terminalne opreme.
- **detekcija zlorab** – agent mora imeti možnost zaznavanja poskusa zlorab in ustreznega ukrepanja.



Sl. 15: Odnosi med akterji pri sistemih DRM

3.5.3. Tehnologije

Prva asociacija, ki se nam porodi ob pojmu DRM, je vsiljevanje določenih pravil in skrivanje koristne vsebine. Vsebina je skrita s pomočjo kriptografskih metod, ki predstavljajo prvo obrambno črto zaščite sistemov DRM. Brez ustreznih dekodirnih informacij je do koristne vsebine mogoče dostopati le z uporabo neposrednega napada, kar pri sodobnih kriptografskih metodah in trenutni zmogljivosti računalniške opreme traja nepraktično dolgo časa. Za zagotavljanje razumljive stopnje varnosti celotnega sistema je izbira dovolj varne in učinkovite kriptografske metode ter zagotavljanja varnosti dekodirne informacije ključnega pomena.

Drugo obrambno črto sodobnih sistemov DRM predstavljajo metode dodajanja vodnega žiga in generiranja podpisa vsebin, ki so relativno nove in se šele uvajajo. Osnovna naloga teh sekundarnih varnostnih mehanizmov je preprečevanje nevarnosti analogne luknje.

3.5.3.1. Kriptiranje vsebin

Kriptografija (ang. Cryptography) je veda o šifriranju, ki se ukvarja z zaščito sporočil. Skladno s kriptografijo obstaja komplementarna veda *analiza šifriranja*,

katere naloga je iskanje pomanjkljivosti kriptografskih metod. Obe vedi slonita na matematičnih metodah in ju zato uvrstimo med matematične vede.

Sam pojem šifriranja lahko opredelimo kot storitev. Ne glede na specifično implementacijo, morajo pri tem biti upoštevane določene osnovne zahteve, ki predstavljajo tudi osnovne šifrirne storitve. Le-te lahko združimo v naslednje skupine:

- **Zaupnost** (ang. Confidentiality) – preprečuje nepooblaščeno prebiranje in kopiranje vsebin pred vsemi nepooblaščenimi osebami. Sinonim za storitev zaupnosti je tajnost. To je možno doseči na različne načine, vse od fizične zaščite prenosnega medija do uporabe šifrirnih algoritmov.
- **Celovitost** (ang. Integrity) - preprečuje kakršnokoli spremembo sporočila, pod čemer lahko razumemo brisanje, zamenjavo ali dodajanje dela sporočila k prvotnemu sporočilu. Vsak nepooblaščen poseg v sporočilo mora biti jasno razviden.
- **Avtentikacija oz. overovljanje** (ang. Authentication) – omogoča prepoznavanje udeležencev pri varni komunikaciji. Prepoznati se morajo obe sodelujoči strani pri komunikaciji in sporočilo. Pojem sodelujoča stran označuje uporabnike in njihovo terminalno opremo. S tem se zajamči točnost izvora podatkov z vidika »kdo in od kod«.
- **Nadzor dostopa** (ang. Access Control) – preprečuje neavtoriziran dostop do vsebin in storitev.
- **Nezanikanje** (ang. Non-repudiation) – onemogoča zanikanje opravljenih storitev in akcij. Ta storitev postaja vse bolj pomembna, saj so kriptografske metode vse bolj pomembne pri poslovnih in pravnih transakcijah.

Kriptografske metode ločimo na t.i. šibke in močne. Razlikujejo se po ocenjeni težavnosti »razbitja metode« oz. dosega nepooblaščenega dostopa do zaščitenih vsebin, kar je povezano s pojmom »moči«. Težavnost »razbitja kode« ni konstantna, temveč je odvisna od zmogljivosti računalniške opreme, pri čemer so zaradi cenovne ugodnosti in velike razširjenosti največkrat merilo osebni računalniki. »Moč« določene kriptografske metode je odvisna tako od samega kriptografskega algoritma ter od dolžine izbranega ključa. Za praktično uporabo je zanimiva samo »močna« kriptografija.
Z zaporednim preizkušanjem vseh možnih ključev je teoretično mogoče razbiti katerokoli šifrirno metodo, ki uporablja ključ. Takšen način napada se imenuje napad z grobo silo (ang. Brute Force). Pri tej obliki napada potrebna računska moč eksponentno narašča z dolžino ključa in je odvisna seveda tudi od zahtevnosti samega šifrirnega postopka. Za 32 bitni ključ bi tako potrebovali 2^{32} (približno 10^9) korakov. Ob upoštevanju današnje strojne zmogljivosti povprečnega osebnega računalnika to ne predstavlja posebne ovire. Za ključe dolžine 40 bitov je potrebno 2^{40} korakov, za kar bi potrebovali približno 7 dni na modernem domačem računalniku. Ključi dolžine 64 bitov so verjetno zlomljivi s strani večjih svetovnih vlad, svetovnih multinacionalk in v bližnji prihodnosti verjetno še komu. Za 128 bitne ključe lahko predvidevamo, da bodo ostali nezlomljivi še kar nekaj časa. Najnovejši šifrirni algoritmi (AES, Twofish) pa lahko uporabljajo tudi 192 in 256 bitne ključe. [K34],[K35], [W27], [W46]

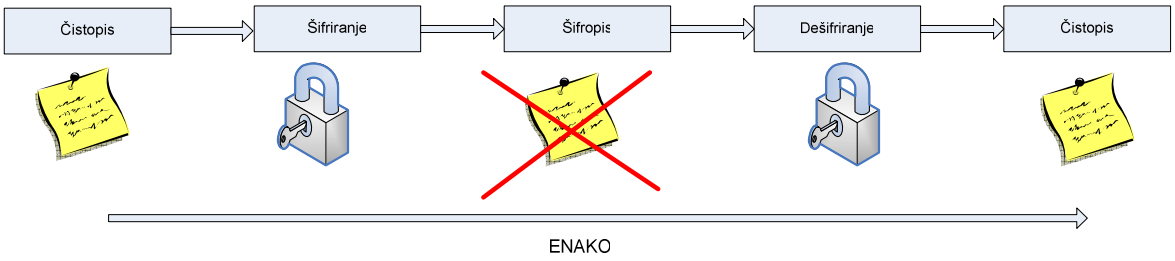
3.5.3.1.1. Analiza šifriranja in klasifikacija napadov

Cilj šifriranja je preprečiti, da bi do čistopisa ali šifrirnega ključa prišli *napadalci sistema*. Komplementarno je cilj analize šifriranja, kako priti do šifrirnega ključa in s tem tudi do vseh sporočil, ki se prenašajo preko komunikacijskega kanala. Vsak poskus analize šifriranja z namenom zlorabe se imenuje: *napad na sistem*. Napade je mogoče klasificirati v dve skupini:

- **Pasivni napad**, pri katerem napadalec samo opazuje komunikacijski kanal, pri tem pa je lahko ogrožena storitev zaupnosti podatkov. To se zgodi v primeru, da napadalec ugotovi šifrirni ključ.
- **Aktivni napad**, kjer napadalec na kakršenkoli način spremeni podatke, ki se prenašajo preko komunikacijskega kanala. Pri tem sta poleg zaupnosti ogroženi še storitvi celovitosti in overovljenja.

3.5.3.1.2. Terminologija

V kriptografski terminologiji se osnovno sporočilo oz. podatki, ki se lahko preberejo in so razumljivi brez posebnih postopkov, navadno imenujejo *čistopis* (ang. Plaintext, Cleartext). *Šifriranje* oz. enkripcija ali kriptiranje (ang. Encryption) označuje metodo prikrivanja vsebine čistopisa. Rezultat uporabe metode šifriranja nad čistopisom je nerazumljiv niz znakov, ki se imenuje *šifropis* ali *tajnopis*. Z uporabo šifriranja se informacije zavarujejo pred nepooblaščenimi elementi. Obraten postopek šifriranju se imenuje *dešifriranje (*ang. Decryption). Šifropis se prevede nazaj v originalno berljivo obliko – čistopis. Osnovno verigo dogodkov ilustrira spodnja slika.



Sl. 16: Splošen postopek šifriranja in dešifriranja

Postopka šifriranja in dešifriranja v sami metodi uporabljata določene parametre, ki so znani pod izrazom *ključ*. Ključ predstavlja začetne vrednosti šifrirnega algoritma s katerim izvedemo postopek šifriranja. Brez uporabe pravilnega ključa legalno naj ne bi bilo mogoče pravilno izvesti postopka dešifriranja.

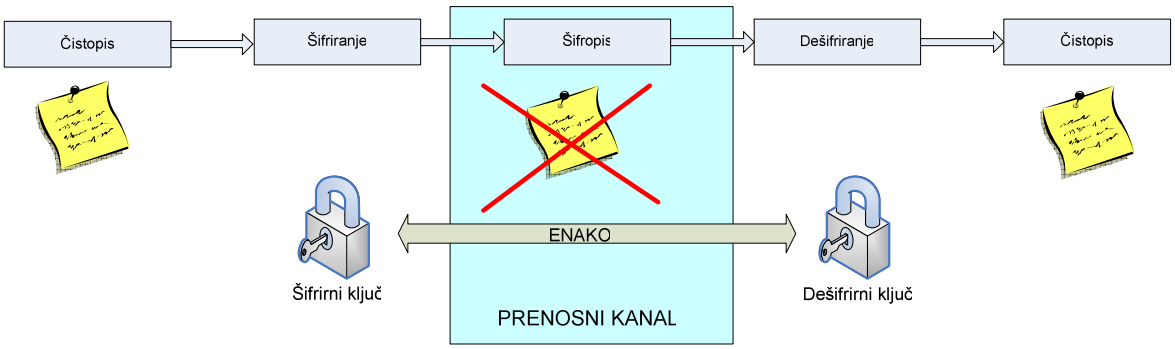
Sam postopek šifriranja in dešifriranja se izvaja s pomočjo *šifrirnega (kriptografskega) algoritma, postopka* oz. kode (ang. Cipher). Večina sodobnih in priznanih kriptografskih metod temelji na pricipu javnih in standardiziranih šifrirnih algoritmov. Celoten algoritem je javen in dobro definiran, kar omogoča preizkušanje varnosti algoritma bistveno širši množici razvijalcev in uporabnikov in posledično vpliva na večjo stopnjo varnosti ter dviguje zaupanje v algoritem. V primeru javnih šifrirnih algoritmov edino skrivnost predstavlja ključ, ki ga je zato potrebno skrbno varovati. Na določenih področjih uporabe se zaradi višjih ciljev

uporabljajo tajni šifrirni algoritmi. Takšna področja so npr. varovanje vojaških skrivnosti, državnih skrivnosti in nekaterih posebnih industrijskih in poslovnih skrivnosti. V tem primeru ni znan niti ključ niti šifrirni algoritem. Posledično to pomeni večjo stopnjo varnosti ter, hkrati zaradi zaprtosti, manjšo možnost predčasnega odkritja morebitnih slabosti algoritma.

V osnovi lahko glede na lastnosti kriptografske metode oz. šifrirne algoritme razdelimo v dve skupini in sicer na:

- simetrične in
- asimetrične.

Simetrični algoritmi so znani tudi kot metoda skrivnega ključa (ang. Secret Key). Tako za šifriranje kot tudi za dešifriranje se uporablja enak ključ oz. je dešifrirni ključ mogoče pridobiti iz šifrirnega ključa. Prednost simetrične kriptografije se kaže v večji enostavnosti in hitrosti metod v primerjavi z asimetrično kriptografijo. Posledično to pomeni manj zahtevno implementacijo. Glavna slabost simetrične kriptografije prav tako izhaja iz dejstva o enakih šifrirnih in dešifrirnih ključih. Problem se pojavi v varni izmenjavi ključev, saj celotna varnost sporočil temelji na tajnosti ključev. Problem varne izmenjave ključev se rešuje z uporabo asimetrične kriptografije, pri čemer je zelo znan postopek Diffie-Helman. Najbolj znani in uporabljani algoritmi simetrične kriptografije so DES (ang. Data Encryption Standard), 3DES (ang. Triple DES) in Rijndael oz. AES (ang. Advanced Encryption Standard). Njihov zgodovinski razvoj in ocenjena moč si prav tako sledita v navedenem zaporedju.

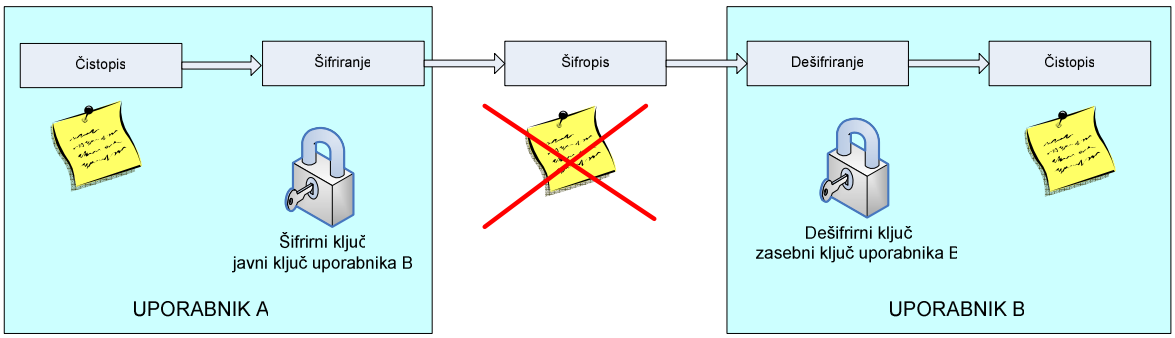


Sl. 17: Simetrični kriptografski postopek

Asimetrični algoritmi so znani pod izrazom metoda javnega/tajnega (privatnega) ključa (ang. Public / Private Key). Šifrirni in dešifrirni ključ nista enaka. Prednosti tega pristopa sta visoka stopnja varnosti in eliminacija problema izmenjave ključev. Slabosti so višja kompleksnost algoritmov, bolj zahtevna implementacija ter posledično počasnejše delovanje v primerjavi s simetričnimi kriptografskimi algoritmi. Zelo znani predstavniki iz te skupine so postopki Elgamal (imenovan po izumitelju, Taher Elgamal), RSA (imenovan po izumiteljih Ron Rivest, Adi Shamir in Leonard Adleman), Diffie-Hellman (imenovan po izumiteljih), in DSA (Digital Signature Algorithm), ki ga je izumil David Kravitz.

Pri asimetrični kriptografiji se uporablja par ključev za šifriranje in dešifriranje. Javni ključ, ki se uporablja za šifriranje podatkov in pripadajoči zasebni ključ,

oziroma tajni ključ za dešifriranje. Vsak uporabnik sistema, posreduje v javnost svoj javni ključ, medtem, ko obdrži zasebni ključ kot skrivnost. Vsi udeleženci, ki razpolagajo z našim javnim ključem, lahko zaščitijo informacije. Prebere jih lahko le imetnik svojega zasebnega ključa. Prav tako velja, da iz javnega ključa in šifropisa ni mogoče ugotoviti tajnega zasebnega ključa. [K6], [K34], [K35]



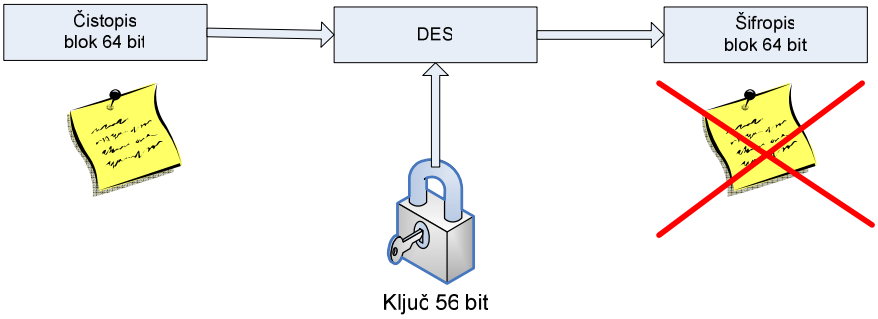
Sl. 18: Asimetrični kriptografski postopek

3.5.3.1.3. DES

Simetrični šifrirni postopek DES je naslednik algoritma Lucifer, ki so ga razvili in patentirali pri IBM. Leta 1976 je bil sprejet kot standardni kriptografski algoritem v ZDA in je vključen v veliko število aplikacij. Do leta 1997 je bila dovoljena splošna uporaba znotraj ZDA, prepovedan pa izvoz. Leta 1999 so dovolili izvoz opreme z algoritmom s 56-bitnim ključem, od januarja 2000 pa so te omejitve še zmanjšane (v brskalnikih lahko uporabljamo trojni DES).

Julija 2004 je ameriška organizacija NIST (National Institute of Standards and Technology) objavila predlog, da se DES s 56-bitnim ključem ne bi več uporabljal. Obrazložitev: »*DES is now vulnerable to key exhaustion using massive, parallel computations.*«, kar pa še ne velja za trojni DES. Postopek DES je bil v uporabi tri desetletja, pri čemer ostaja vprašanje, kako bo z novejšimi šifrirnimi postopki in napredkom tehnologije.

Pri postopku DES se šifrirajo 64 bitov dolgi bloki z uporabo 56 bitov dolgega ključa in operacij permutacije, substitucije ter operacije XOR. 64 bitov dol blok se na začetku permutira ter preuredi s pomočjo posebnih tabel (S-boxes) in ključa. Ta del postopka se 16-krat ponovi - vsakokrat z drugače preurejenim ključem. Postopek DES pozna več načinov delovanja, pri čemer je opisani najpogostejši.



Sl. 19: Osnovna arhitektura postopka DES

Opis postopka za šifriranje 64-bitnega bloka:

1. Blok permutiramo z začetno permutacijo IP.

2. Blok razdelimo na dva 32-bitna bloka (levi gre v register L, desni v register R).

Začetek zanke

3. V vsakem bajtu bloka R podvojimo prvi, četrti, peti in osmi bit (32 + 4.4 = 48 bitov).

4. Ta rezultat seštejemo z operacijo XOR s ključem, ki je v vsaki ponovitvi zanke drugačen.

5. Vsoto razdelimo na 8 x 6 bitov. Vsak tak sekstet bitov zamenjamo z elementom iz substitucijske tabele, ki ima dimenzije 4 x 16 in vsebuje elemente od 0 do 15. Pozicijo elementa dobimo tako: vrstico določa 1. in 6. bit (0 - 3), stolpec pa 2. - 5.bit (0 - 15).

6. Osemkrat po 4 bite premešamo s permutacijo P.

7. Rezultat seštejemo z vsebino registra L z XOR in shranimo v začasni register.

8. Vsebino registra R prenesemo v L, vsebino iz začasnega registra pa v R.

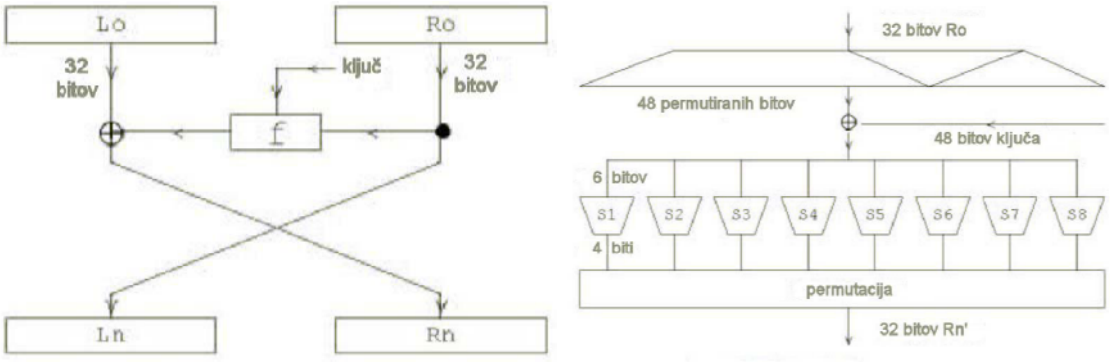
Zanko ponovimo 16-krat.

9. Bloka iz L in R združimo v obratnem vrstnem redu in premešamo z inverzom začetne permutacije IP.

Določitev 48-bitnega ključa, ki ga uporabimo v 4. koraku:

Izmed 64 bitov izločimo vsakega 8., preostalih 56 bitov razdelimo in vpišemo v registra C in D. V 16 korakih ju ciklično premaknemo za eno ali dve mesti v levo (koraki 1, 2, 9, 16 premik za eno mesto, sicer 2). Bloka združimo, 8 bitov izpustimo in preostanek premešamo.

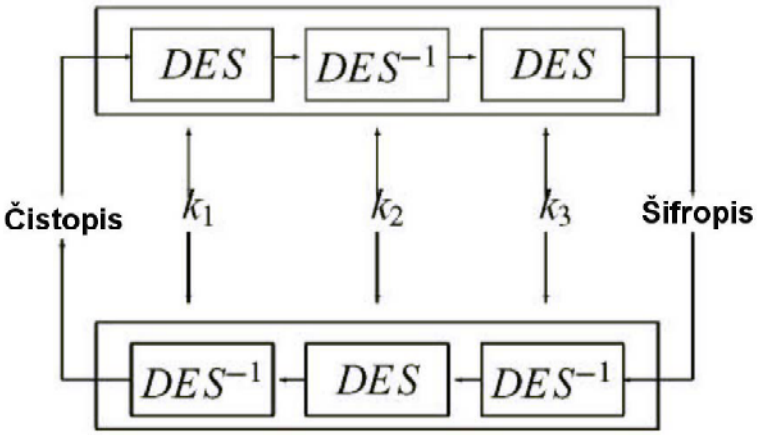
Algoritem učinkuje tako, da sprememba enega samega vhodnega bita bloka spremeni skoraj vse bite v rezultatu bloka. Dešifriranje poteka z istim ključem in skoraj enakim postopkom. [K34], [K35], [W23]



Sl. 20: Zanka DES (levo) in zgradba funkcije f (desno) [K34]

3.5.3.1.4. Trojni DES

Trojni DES temelji na večkratni ponovitvi postopka DES. Postopek šifriranja poteka z uporabo DES in šifriranja s ključem 1, dešifriranjem s ključem 2 ter končno s šifriranjem s ključem 3. Postopek dešifriranja poteka v obratnem vrstnem redu: dešifriranje s ključem 3, šifriranje s ključem 2 in končno dešifriranje s ključem 1. [K34], [W24]



Sl. 21: Postopek 3DES šifriranja in dešifriranja [K34]

Ocenjujejo, da je tako uporabljen algoritem ekvivalenten uporabi z 112 bitov dolgim ključem. V primeru računalnika z zmogljivostjo testiranja 10^{12} celotnih postopkov enkripcij v sekundi, znaša izračun: 2^{112} operacij ustreza 5.19 x 10^{33} testiranj. Ob upoštevanju zmogljivosti testnega računalnika znaša najneugodnejši čas razbitja kode: 5.19 x 10^{33} testiranj / 10^{12} operacij znaša 10^{21} sekund, kar je 10^{14} let.

3.5.3.1.5. AES

Postopek Advanced Encryption Standard je po funkciji naslednik postopkov DES in 3DES. Leta 2001 je bil uradno potrjen s strani organizacije NIST. Temelji na algoritmu Rijndael, avtorjev Joan Daemen in Vincent Rijmen. Predstavlja novo generacijo simetričnih šifrirnih algoritmov z glavnimi odlikami:

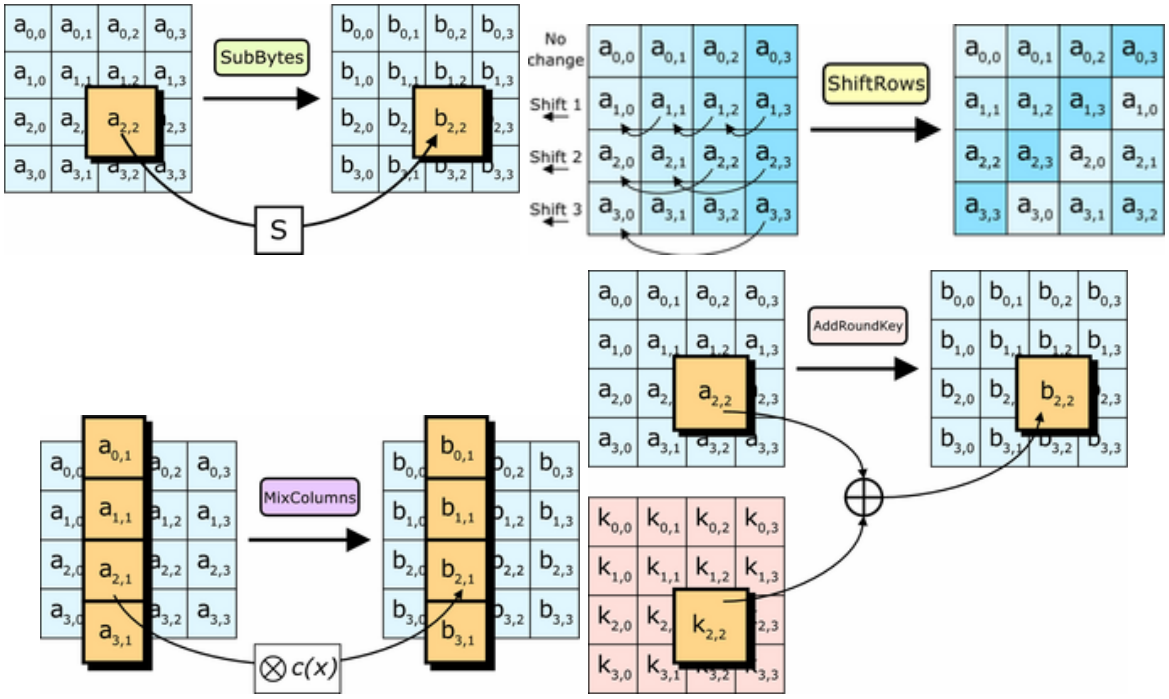
- odpornost proti vsem poznanim napadom,
- enostaven model,
- kompaktnost kode in hitrost na raznolikih platformah.

AES podatke obdeluje po blokih velikosti 128 bitov in uporablja ključe dolžin 128, 192 ali 256 bitov. Temelji zgolj na uporabi operacij bitne substitucije, permutacije in operacije XOR.

AES operira nad vhodnimi podatki v obliki matrike 4x4 byte-ov. Vrednosti te matrike v določenem času določajo stanje (ang. State) algoritma. Šifriranje se izvaja po korakih, pri čemer se vsakič, razen pri zadnjem koraku, izvedejo naslednje operacije nad trenutnim stanjem:

1. Operacija zamenjave elementov (ang. SubBytes) – nelinearna preslikava, kjer se elementi stanja (byte) zamenjajo glede na pravila v zamenjalni tabeli (ang. Lookup Table).
2. Operacija premika vrstic (ang. ShiftRows) – vsaka vrstica v stanju se rotira za določen premik.
3. Mešanje stolpcev (ang. MixColumns) – celoten stolpec se transformira s pomočjo linearne transformacije.
4. Krožni ključ (ang. AddRoundKey) – vsak element stanja se kombinira s krožnim ključem (ang. Round Key), ki izhaja iz kodirnega ključa.

Izvede se deset korakov, končni šifropis predstavlja vrednost elementov zadnjega stanja po končanem postopku.



Sl. 22: Ilustracija operacij pri postopku AES (zamenjava elementov – levo zgoraj, premik vrstic – desno zgoraj, mešanje stolpcev – levo spodaj, krožni ključ – desno spodaj) [W25]

AES postopek trenutno velja za zelo varnega in učinkovitega. [W25]

3.5.3.1.6. RSA

RSA je en izmed najbolj znanih in splošno uporabljenih šifrirnih algoritmov z javnim ključem. Uporablja se za šifriranje in za digitalne podpise. Varnost RSA-ja naj bi bila ekvivalentna problemu faktorizacije, kar pa še ni dokazano. Temelji na predpostavki, da je zelo težko ugotoviti posamezne množilne faktorje iz znanega zmnožka. Pri tem se v postopku uporabljajo zelo velika praštevila, reda 100 do 200 digitov.

RSA uporablja za računanje cela števila modula n = p*q, kjer sta p in q veliki skrivni praštevili. Za šifriranje sporočila m se uporabi eksponentna funkcija z majhnim javnim eksponentom e. Pri dešifriranju prejemnik šifropisa ($c = m^e \pmod n$) izračuna obratno množenje $d=e^{-1} \pmod{(p-1)*(q-1)}$ in dobi $c^d = m^{e*d} = m \pmod n$. Tajni ključ vsebuje n, p, q, e, d; javni ključ pa vsebuje n in e. V primeru napada se predvideva, da je za napadalca obratni izračun d iz e enako zahteven kot faktorizacija n.

Element	Vrednost/Opis
javni ključ	n = p*q, kjer sta p in q veliki tajni praštevili e = (p-1)*(q-1)
tajni ključ	$d = e^{-1} \bmod ((p-q)*(q-1)$
šifriranje	$c = m^e \bmod n$, kjer je m sporočilo
dešifriranje	$m = c^d \bmod n$

Tab. 4: Postopek RSA

Za zagotavljanje solidne stopnje varnosti, je priporočljiva velikost ključa večja od 1024 bitov (razred 10^{300}). Velikost ključa 2048 bitov naj bi bila razumljivo varna še nekaj časa. [W26], [W28]

3.5.3.1.7. Pomen šifriranja pri sistemih DRM

Sistemi DRM so tesno povezani z uporabo kriptografskih metod. Pri tem je pomembno dejstvo, da sama moč uporabljene kriptografske metode NE zagotavlja neposredno varnost celotnega sistema DRM. To je le potreben, ne pa zadosten pogoj. V primeru razkritja ključa ne bo pomagal še tako močan kriptografski postopek. Pomemben je tudi način uporabe kriptografije, saj globalne skrivnosti zelo znižujejo celotno stopnjo varnosti. Vsi sistemi DRM ne uporabljajo standardnih kriptografskih metod, kar je dvorezen meč.

V okviru terminologije sistemov DRM po funkciji šifriranja ločimo dva pojma in sicer kodiranje (mešanje) ter kriptiranje (šifriranje). Prvi se nanaša na šifriranje vsebin in drugi na šifriranje vseh ostalih informacij. V primeru sistemov DRM se kodirajo npr. večpredstavne vsebine in kriptirajo podatki o licenci. Podobno, se pri sistemih pogojnega dostopa kodirajo video tokovi in kriptirajo sporočila o pravicah.

Simetrični in asimetrični kriptografski postopki imajo svoje prednosti in slabosti. Pri realnih sistemih se zato uporablja kompromis med obema skrajnostima. Za šifriranje vsebinskega dela informacij se uporabljajo hitri simetrični postopki. Ključne informacije v obliki licenc in dekodirnih ključev se ščitijo z močnimi asimetričnimi kriptografskimi postopki. Na ta način se doseže visoka stopnja varnosti ob sprejemljivih zahtevah po zmogljivosti opreme.

3.5.3.2. Identifikacija uporabnikov

Pri vseh sistemih, ki se ukvarjajo s transakcijami vrednih informacij, kamor spadajo tudi sistemi DRM, je pomembna identifikacija uporabnikov. Identifikacija omogoča

ugotovitev identitete komunicirajočih entitet oz. uporabnikov. Tako je mogoče določene akcije in zahteve pripisati ustreznim akterjem.

Sam pojem *identifikacije* označuje samo predvideno, predlagano identiteto uporabnika. Pri poštenih uporabnikih je to dovolj, v primeru zlorabe identitete pa ne zadošča. Napadalec se lahko predstavlja kot legalen uporabnik in brez dodatnih mehanizmov sistem ne bo ločil razlike. Za ugotovitev resnične identitete je potrebno preverjanje identifikacijskih informacij. Temu služi mehanizem *avtentikacije*. Avtenikacija se osredotoča na dve področji in sicer:

- avtentikacijo uporabnikov in njihove terminalne opreme in na
- avtentikacijo komunikacije.

3.5.3.2.1. Avtentikacija uporabnikov

Pri sistemih DRM se z avtentikacijo uporabnikov največkrat označuje avtentikacija njihove terminalne opreme oz. varnostnega agenta. Sistem zaupa le terminalni opremi. Najpogostejši pristop je uporaba asimetrične kriptografije z javnimi in tajnimi ključi. Na podlagi tega so bili razviti *certifikati z javnim ključem* (ang. Public Key Certificate), danes zelo uporabljana metoda, ki velja za zelo varno.

Mednarodna organizacija za standardizacijo ISO je leta 1993 razvila standard X.509 za avtentikacijo (uporabnikov, opreme) preko javnih in nezavarovanih omrežij. Standard predvideva uporabo kateregakoli kriptografskega postopka z javnim/privatnim ključem, pri čemer je priporočen mehanizem RSA. Najpomembnejši del standarda opisuje mehanizem certifikatov z javnim ključem. Pri tem neka javna in zaupanja vredna organizacija za izdajanje certifikatov (ang. Certification Authority, CA) posameznikom oz. organizacijam izda unikaten certifikat. Ta vsebuje podatke o uporabniku in uporabnikov javni ključ. Certifikatu je dodan podpis s strani organizacije CA, ki ga je izdala, ki je podpisan s tajnim ključem te organizacije. Certifikat si lahko s pomočjo orodij izdela vsak posameznik oz. organizacija, vendar je v tem primeru takšen certifikat uporaben samo lokalno. Obstaja več organizacij za izdajanje certifikatov, ki so v hierarhičnem odnosu.

<table>
<tr><td rowspan="2">Verzija</td><td rowspan="2">Serijska številka</td><td>ID šifrirnega algoritma</td><td rowspan="2">Izdajalec certifikata (CA)</td><td>Veljavnost</td><td rowspan="2">Uporabnik</td><td>Uporabnikov javni ključ</td><td rowspan="2">Podpis</td></tr>
<tr><td>Parametri šifrirnega algoritma</td><td>Časovni interval
OD - DO</td><td>Parametri šifrirnega algoritma za javni ključ</td></tr>
</table>

Tab. 5: Zgradba X.509 certifikata

Zgradbo X.509 certifikata prikazuje tabela št. 5. Polje »verzija« označuje format certifikata. Polje »serijska številka« označuje unikatno oznako certifikata v okviru organizacije, ki ga je izdala. Polji »ID šifrirnega algoritma« in »parametri šifrirnega algoritma« označujeta podatke o uporabljenem šifrirnem algoritmu s strani organizacije CA pri izdaji certifikata. Polji »veljavnost« in »časovni interval« opisujeta veljavnost certifikata. Polja »uporabnik«, »uporabnikov javni ključ« in

»parametri šifrirnega algoritma za javni ključ« opisujejo uporabnika certifikata in njegov javni ključ. Zadnje polje »podpis« vsebuje podpis s strani organizacije za izdajo certifikata. [K6]

3.5.3.2.2. Avtentikacija komunikacije

Avtentikacija komunikacije zagotavlja integriteto sporočil. Skuša se ugotoviti vsako spremembo ali poneverbo sporočil. Za to se uporablja simetrična in asimetrična kriptografija, v primeru nešifriranih sporočil pa metoda z zgoščevalnimi funkcijami.

Zgoščevalne funkcije (ang. Hash Function) so matematične funkcije, ki ne glede na obseg sporočil generirajo izhodno številsko vrednost fiksne dolžine. Ta vrednost je odvisna od vsebine sporočila. Zgoščevalne funkcije morajo zadoščati naslednjim zahtevam:

- različna sporočila morajo generirati različne vrednosti zgoščevalne funkcije,
- napad z grobo silo naj bo edina učinkovita oblika napada,
- enostavnost postopka zgoščevalne funkcije,
- enostavna implementacija in hitro izvajanje.

Najbolj znana zgoščevalna postopka sta MD5 (Message Digest Number 5) in SHA (Secure Hash Algorithm). Postopek SHA je odobren s strani organizacij NIST in NSA in velja za zelo zanesljivega.

3.5.3.3. Vodni žig

Tehnologija vodnega žiga (ang. Watermarking) v splošnem opisuje postopek dodajanja dodatnih informacij v originalne vsebine ob upoštevanju določenih pogojev. Izraz vodni žig (ang. Watermark) izhaja iz prvih oblik uporabe te tehnologije pred približno 700 leti, ko so na ta način izdelovalci papirja podpisali in v nekem pomenu zaščitili svoj izdelek. Podpis je bil odtisnjen na papir v postopku izdelave in ni oviral normalne uporabe papirja ter je bil viden le pod določenim kotom. Od takrat naprej se uporablja za zaščito vrednejših papirnatih dokumentov, kot so denar, listine in delnice ter še danes predstavlja enega pomembnejših mehanizmov za preprečevanje ponarejanja. Vodni žig je uporaben tako pri materialnih vsebinah kot tudi pri vsebinah v elektronski obliki.

Vodnemu žigu je na prvi pogled podobna veda o steganografiji (ang. Steganography), ki prav tako dodaja informacije v originalne vsebine. Izraz izhaja iz grščine in pomeni »zakrito pisanje« oz. z lepim slovenskim izrazom tajnopisje. Veda je precej mlada, z začetki v letu 1996, in v splošnem operira nad vsebinami v elektronski obliki. Po tehnološki izvedbi sta si metodi zelo podobni in se dopolnjujeta. Bistvena razlika se pokaže v konceptu in razlogih za dodajanje informacij. Glavni razlog pri tajnopisju je dodajanje skrite informacije v originalne vsebine zaradi posebnih (skrivnostnih) razlogov. Sama informacija ter vednost, da je v vsebini skrita dodatna informacija, morata ostati skrita. Dodana informacija ni nujno povezana z vsebino. Pri vodnemu žigu je dodana informacija vedno povezana z vsebino in dodana s točno definiranimi cilji. Vednost o obstoju vodnega žiga v vsebini je javna in uporabniki so o tem obveščeni. [W21]

Tehnologija vodnega žiga v okviru sistemov DRM se uporablja za preprečevanje nevarnosti analogne luknje. V tem smislu se skoraj vedno uporablja nad vsebinami v digitalni obliki.

Glavne naloge vodnega žiga so:

- identifikacija vsebin,
- sledenje vsebinam in
- preprečevanje zlorabe vsebin.

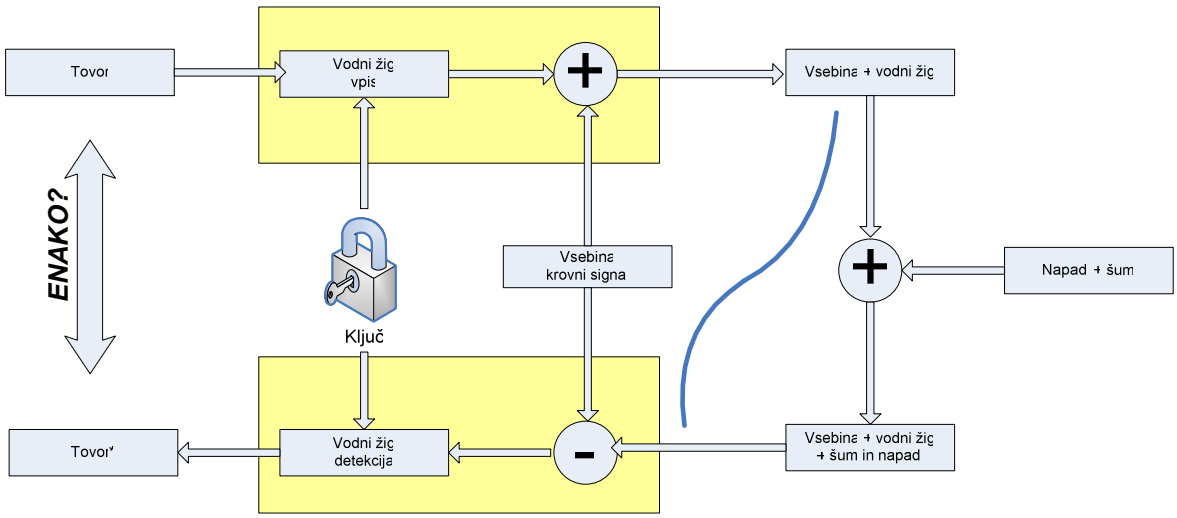
Prvi dve nalogi sta pasivni in služita ugotavljanju točke zlorabe oz. izlitja (ang. Leak). Zadnja naloga opisuje aktivno preprečevanje zlorabe z različnimi mehanizmi (npr. tehnologije podjetja Macrovision). Ne glede na specifični implementacijo mehanizmov vodnega žiga je potrebno upoštevati naslednje zahteve:

- **nevidnost, nezaznavnost** (ang. Imperceptibility) – niti informacije, dodane z vodnim žigom, niti sam mehanizem vodnega žiga ne smeta spremeniti vsebin tako da, ne nudijo kvalitetne uporabniške izkušnje ob legalni uporabi. Z drugimi besedami, pri legalni uporabi uporabnika vodni žig ne sme v nobenem primeru motiti.
- **varnost** (ang. Security) – informacije, dodane z vodnim žigom, morajo biti zavarovane in dostopne le pooblaščenim osebam. Pri tem se ne sme zlorabiti pravic uporabnikov v smislu zlorabe podatkov, zasebnosti in sledenja uporabniškim navadam.
- **robustnost** (ang. Robustness) – vodni žig mora biti odporen na zlorabe in spremembe vsebine. To se nanaša na poskuse nelegalnega izbrisa, dodajanja ali spreminjanja informacij v vodnem žigu. Onemogočeno mora biti nepooblaščeno spreminjanje, kar je povezano s kriterijem o varnosti.

V okviru terminologije pri tehnologiji vodnega žiga se z izrazom *tovor* (ang. Payload) imenuje dodana informacija ter izrazom *krovni, prekrivni signal* (ang. Cover Signal) originalna vsebina, v katero se dodaja informacija. Količina možne dodane informacije je seveda odvisna od velikosti in oblike originalne vsebine. V slikovno originalno vsebino velikosti 1000x1000 slikovnih elementov je mogoče dodati bistveno več informacije kot v sliko velikosti 10x10 slikovnih elementov. Pri tem je seveda potrebno upoštevati zgoraj navedene zahteve za tehnologijo vodnega žiga.

Pri konceptu izvedbe se večinoma uporabljajo metode razpršenega spektra za vnos informacije (podobno konceptom v sistemu UMTS) ter korelacijske metode na podlagi kod (ključev) za detektiranje. Postopek vodnega žiga lahko operira nad vsebino v nekompresirani obliki (»surova oblika«) ali nad vsebino v kompresirani obliki. Ker se pri večpredstavnih vsebinah uporabljajo večinoma izgubni kompresijski postopki, se pri tem del informacije izgubi. Zato se vodni žig dodaja v nekompresirano obliko vsebine, kjer je sam postopek dodajanja vodnega žiga tudi enostavnejši. Pri tem se za zahtevna izkažeta kriterija nezaznavnosti in predvsem robustnosti. Slednji v idealnem pomenu zahteva, da je vodni žig odporen na vse možne napade. To vključuje napade v digitalni in analogni obliki. Primeri digitalnih napadov so prekodiranje vsebine, skaliranje vsebine, spreminjanje barvne globine in celo rezanje dela vsebine. Analogni napadi so še težji, saj kombinirajo obe vrsti napadov in temeljijo na konverziji iz digitalne v analogno obliko ter ponovno v

digitalno obliko. Primer takšnega napada je npr. zajem avdio signala iz zvočnega izhoda (Line-Out) ali pa zajem slikovnega signala iz video izhoda (kompozitni, S-VHS, RBG) ali celo z uporabo kamere. Kljub celotni verigi napadov in dogodkov mora biti razvidno dovolj informacije vodnega žiga, da je le-ta še vedno zanesljiva in uporabna.



Sl. 23: Princip vnosa in detekcije vodnega žiga

Sama specifična izvedba mehanizmov vodnega žiga je odvisna od vrste in formata zapisa originalne vsebine. Tipične vrste vsebin so tekst, statične slike, avdio in video. Pri večpredstavnih vsebinah se večinoma izkoriščajo psihofizične lastnosti človeških čutil. Formati vsebin se nanašajo na način zapisa v digitalni obliki ter na obliko kompresije. Tipični predstavniki za večpredstavne vsebine so formati iz družine MPEG, MS Windows Media in Real. Nekatere značilne pristope pri večpredstavnih vsebinah opisuje spodnja preglednica. [K7], [W30]

Vsebina	Princip vnosa vodnega žiga
slike	Dodatne informacije so razpršene po celotni sliki ali delu slike. Skrite so v rahlo spremenjen barvni informaciji posameznih slikovnih elementov.
avdio	Izkoriščajo se posebnosti zaznavanja zvoka slušnih čutil. Izkorišča se efekt maskiranja v časovnem in frekvenčnem prostoru. Pri frekvenčnem maskiranju se izkorišča nezmožnost hkratnega zaznavanja določenih kombinacij tonov. Če se v določenem časovnem intervalu hkrati pojavita šibek in močan ton, se šibek prekrije in ni zaznaven. Pri časovnem maskiranju se izkaže, da v primeru močnega tona (velika amplituda) uho ne zazna šibkejšega tona, ki sledi za močnim oz. se pojavi celo pred njim. V nezaznavne dele je mogoče dodati drugo informacijo, ki je del vsebine in ne moti uporabnika.
video	Dodatne informacije so skrite v posameznih slikah ter v spremembah med slikami.

Tab. 6: Tipični principi dodajanja vodnega žiga pri večpredstavnih vsebinah

3.5.3.4. Ugotavljanje podpisa vsebine

Tehnologija ugotavljanja podpisa oz. prstnega odtisa vsebine (ang. Fingerprinting) se nanaša na področje identifikacije vsebin (ang. Content Based Identification). Ime izhaja iz izraza prstni odtis (ang. Fingerprint), ki označuje značilen podpis oz. opis vsebine. Na prvi pogled je tehnologija prstnega odtisa podobna vodnemu žigu, vendar obstaja bistvena razlika. Pri vodnemu žigu gre za invaziven postopek, ki vpliva na originalno vsebino. Pri prstnemu odtisu gre za neinvaziven postopek, ki v ničemer ne spreminja originalne vsebine. Glavna naloga tehnologije prstnega odtisa je analiza vsebin (predvsem večpredstavnih) in izločitev informacije, ki unikatno identificira originalno vsebino z vsebinskega vidika (kaj je dejanska vsebina). To pomeni, da se skuša opredeliti vsebino s stališča uporabnika in ne s stališča formata vsebine. Rezultat analize – prstni odtis vsebine je kasneje mogoče uporabiti za iskanje. Druga naloga tehnologije prstnega odtisa je namreč organizacija in zbiranje unikatnih podpisov ter možnost ponovnega iskanja originalne vsebine ali njej vsebinsko podobnih vsebin. V primeru video vsebin se določena vsebina, npr. anime Mononoke Hime, analizira in vpiše v bazo prstnih odtisov. Uporabnik lahko to vsebino kasneje s pomočjo znanega vzorca, kar je npr. izsek iz originalne vsebine, ponovno poišče oz. poišče njej podobne vsebine. Sistem navadno navede tudi stopnjo uspešnosti razpoznave.

Tehnologija vodnega žiga	Tehnologija prstnega odtisa
Invaziven postopek, ki originalno vsebino spremeni.	Neinvaziven postopek, ki v ničemer ne spremeni originalne vsebine.
Obstaja možnost popačenja in spremembe vsebinskega dela – izgleda – vsebine.	Ni nevarnosti popačenja vsebin.
Rezultat – vnesena informacija pri vodnem žigu – ni odvisen od vsebine (ni funkcija vsebine).	Rezultat – unikaten prstni odtis vsebine – je odvisen od vsebine (je funkcija vsebine).
Potreben je dostop do točno določene vsebine.	Potreben je dostop le do vsebinsko podobne vsebine in ne do točno določenega primerka vsebine.
Možna je identifikacija in označitev točno določene vsebine.	Možna je identifikacija vsebinsko podobnih vsebin.
V primeru spremembe tehnologije je potrebna ponovna obdelava vseh vsebin.	V primeru spremembe tehnologije ni potrebna ponovna obdelava vsebin (vsebina se ne spremeni).
Vsaka vsebina in kopija vsebine je unikatno podpisana.	Potrebna je obdelava vseh vsebinsko (s stališča uporabnika) novih vsebin. Vsaka vsebina je določena le do nivoja vsebinske podobnosti – posamezne različne kopije iste vsebine ni mogoče ločiti.

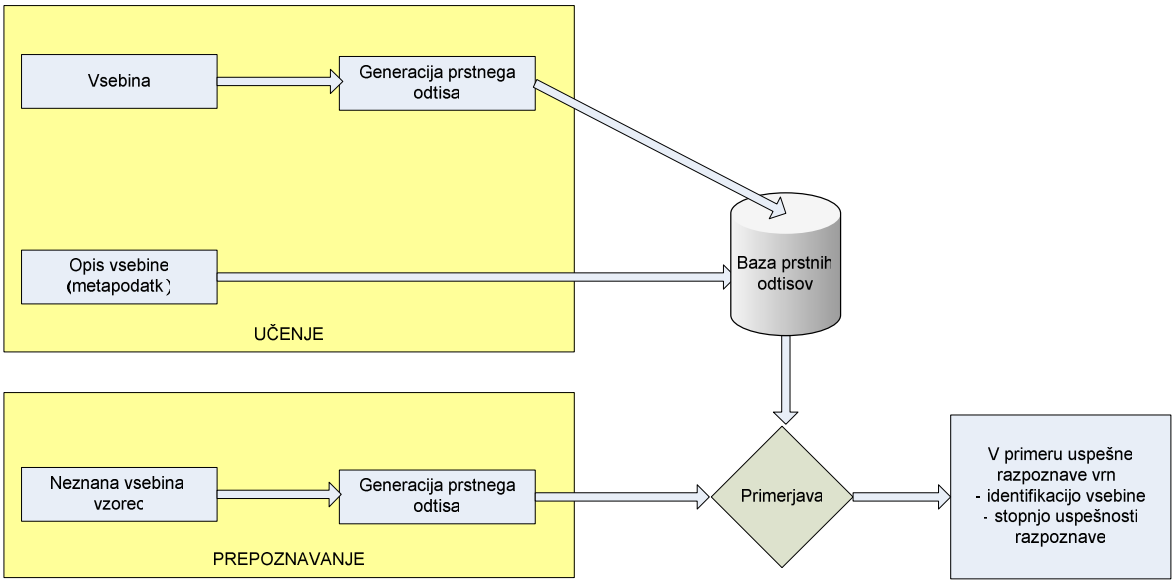
Tab. 7: Primerjava lastnosti tehnologij vodnega žiga in prstnega odtisa vsebin

Obe tehnologiji sta komplementarni in dajeta najboljše rezultate v kombinaciji. Pri sistemih DRM in večpredstavnih vsebinah se pristop izkaže v primeru uspešnega napada na vodni žig in njegove odstranitve iz vsebine. Ponudnik vsebin ima od komprimitirane vsebine spravljen tudi prstni odtis. Napad na prstni odtis ni mogoč, ker ni del vsebine. Sprememba prstnega odtisa je možna le v primeru spremembe

vsebinskega dela vsebine, kar ni v interesu napadalcev. S pomočjo iskanja vsebin po nelegalnih omrežjih s tehnologijo prstnega odtisa je mogoče detektirati zlorabljene vsebine. Primer je npr. uspešna detekcija najnovejšega filma na medmrežju, ki legalno sploh še v obtoku. V tem primeru je zloraba očitna.

Ugotavljanje prstnega odtisa vsebin temelji na metodi razpoznavanja vzorcev (ang. Pattern Recognition) in poteka v dveh korakih:

- **Faza učenja** (ang. Training Phase) – iz vsebinskega vidika se poiščejo karakteristične značilnosti elementov (i.e. značilke), ki nastopajo v vsebini. Te značilnosti se matematično opišejo v izjemno kompaktni obliki in shranijo v bazi podatkov.
- **Faza prepoznavanja** (ang. Recognition Phase) – testni vsebini se določi prstni odtis in nato se s pomočjo primerjave znanih prstnih odtisov v bazi skuša poiskati najbolj podobne. S tem je mogoče identificirati neznano vsebino oz. poiskati njej podobne.



Sl. 24: Princip delovanja tehnologije prstnega odtisa

Tehnologija prstnega odtisa mora prav tako izpolnjevati določene zahteve. V primerjavi s tehnologijo vodnega žiga odpadejo zahteve po nevidnosti postopka, saj le-ta ni invaziven.

- **Zahtevnost postopka** – postopek določanja in detekcije prstnih odtisov vsebin mora biti dovolj preprost, da je možna dovolj hitra implementacija in uporaba.
- **Robustnost** – postopek mora biti dovolj odporen na spremembe vsebine. Stopnja pravilne razpoznave mora biti uporabna.

[K8]

Vsebina	Princip določanja prstnega odtisa vsebin
slike, video	Uporablja se metoda razpoznavanja vzorcev (določanja značilk) in različni zgoščevalni postopki.
avdio	Uporabljata se dva pristopa. Prvi temelji na detekciji značilnih avdio parametrov, kot so spremembe glasnosti, tempa in spektralne podobe signala. Primere te metode opisuje standard MPEG-7. Druga metoda se osredotoča na samo vsebino avdio vsebin, kot jih zaznavajo uporabniki. Primer teh metod je sistem MusicDNA.
tekst	Upoštevajo se jezikovne značilnosti, skladnja in semantika jezika.

Tab. 8: Tipični principi določanja prstnega odtisa vsebin

3.5.4. Elementi in arhitektura splošnega sistema DRM

3.5.4.1. Označevanje vsebin

Poleg vsebine same je enako pomemben primeren način opisa te vsebine. Opis različnih elementov, objektov in vsebin je kompleksno področje s svojimi metodami in terminologijo. Ločimo pojma identifikator (ang. Identifier) in metapodatki (ang. Metadata), ki predstavljata dva obraza istega kovanca. Identifikator je jasen in nedvoumen (ang. Unambigious) niz, ki označuje entiteto. Slednja označuje nekaj (objekt, stvar, pojem, vsebina, ...), kar se opisuje. Identifikator mora poleg nedvoumnosti biti unikaten in persistenten. Identifikatorji se po pomenu združujejo v t.i. imenske prostore (ang. Namespace). Obstaja več standardiziranih sistemov in shem za identifikatorje, ki se uporabljajo tudi pri sistemih DRM. Najbolj znani so: ISO ISBN, ISO ISSN, ISO ISRC, ISO ISAN in ANSI/NISO Z39.84 Digital Object Identifier. Izraz ontologija (ang. Ontology) označuje orodje za opis odnosov med posameznimi entitetami v okviru določenega okolja. [K5]

Sami identifikatorji so samo dobro definirani alfanumerični nizi in sami zase nimajo pomena. Pomen jim dajejo metapodatki, ki dodatno opisujejo entitete. Izraz metapodatki v splošnem pomeni podatke o podatkih oz. podatke, ki opisujejo druge podatke. Primer je npr. identifikator ISBN 2-769754-55-3, ki označuje knjižno gradivo. Točno za katero knjigo v tem primeru gre povedo pripadajoči metapodatki. Zelo znano orodje za opis metapodatkov je ogrodje <indecs> Framework [W22].

V okviru sistemov DRM se podatki o vsebini nanašajo na več področij. Tipično gre za opis same vsebine, podatke o oceni, podatke za lažje iskanje vsebine in drugo. Podatki za opis niso nujno zgolj tekstovni, temveč so lahko po obliki v različnih večpredstavnih elementih. Primerni podatki za opis neke večpredstavne vsebine, npr. filma, so:

- podatki o filmu: naslov, avtor, igralci, zvrst, podzvrst, letnica, ...
- opis filma v tekstovni obliki z dodanim slikovnim gradivom in predoglednimi video izseki,
- ocena filma,
- podatki za iskanje: prstni odtis te vsebine, drugi identifikatorji.

3.5.4.2. Jezik za opis pravic

Jezik za opis pravic REL (ang. Rights Expression Language) je bistven del sistema DRM. Po razslojitvi sistema DRM po funkcijah (poglavje 3.1.4) spada med srednje DRM sloje, ki med seboj povezujejo višje aplikacijske in nižje implementacijske fizične DRM sloje. Jezik za opis pravic se uporablja za artikulacijo opisa načina uporabe ter uporabniških pravic do vsebin. Jezik za opis pravic mora zadostiti naslednjim pogojem:

- **razširljivost, neomejenost** (ang. Extensibility) – REL mora imeti dovolj bogat nabor možnosti za potrebe definicije in opisa različnih pravic v različnih okoljih ter pri različnih poslovnih modelih. Ne sme biti omejen s stalnim naborom, temveč mora dopuščati razširitve.
- **strojna razumljivost** (ang. Machine Readability) – mora biti strojno razumljiv.
- **interoperabilnost** – mora biti prenosljiv in kompatibilen z različnimi sistemi.

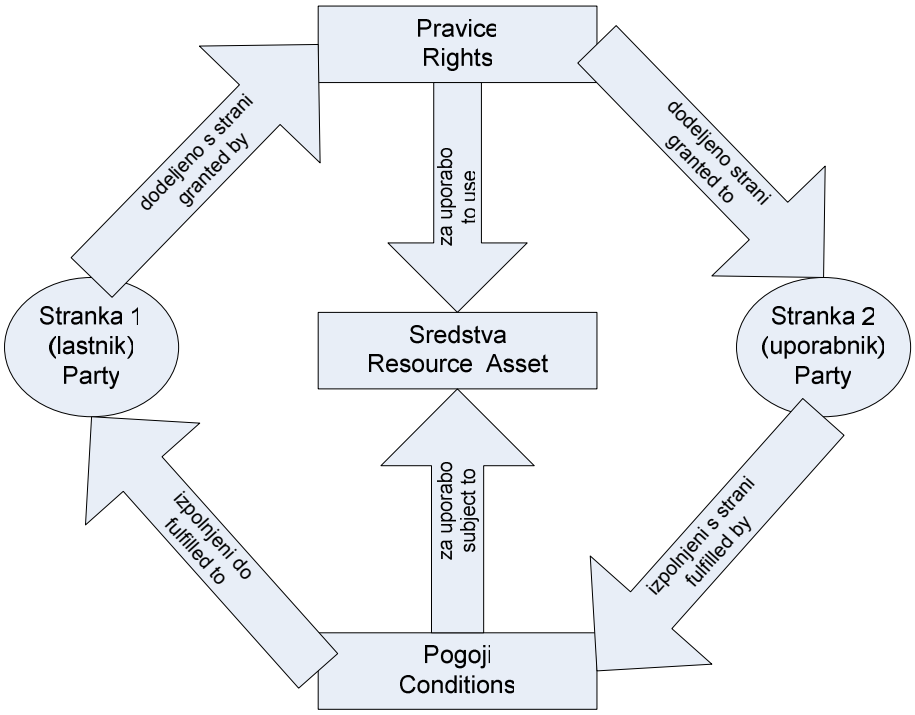
Na podlagi zgornjih zahtev je logična izbira zapisa na podlagi XML (eXtesible Markup Language) tehnologije. XML zapis je človeško in strojno berljiv, prenosljiv ter dobro definiran.

Jezike REL v splošnem sestavljata dve komponenti. To sta koncept jezika (ang. Rights Language Concept, RLC) in slovar (ang. Rights Data Dictionary, RDA). Koncept jezika določa pravila skladnje (sintakso), slovar pa nabor definiranih in možnih elementov jezika (definira pomen oz. semantiko). Kombinacija pravilnih elementov jezika, kot jih določa slovar, in pravilne postavitve v skladu s konceptom jezika dajeta veljavne izraze v REL jeziku.

Osnovni elementi oz. gradniki jezikov za opis pravic so:

- **pravice** (ang. Rights) – definirane so v obliki izrazov, ki določajo pogoje dostopa in uporabe sredstev. Pogoji uporabe so podrobneje definirani kot pravice oz. omejitve uporabe sredstev.
- **pogoji** (ang. Condition) - določajo predpogoje, ki morajo biti izpolnjeni preden se smejo koristiti pravice uporabe sredstev.
- **sredstva, premoženje** (ang. Resources, Assets) – določajo dejanske vsebine ali storitve, ki se lahko koristijo.
- **stranka** (ang. Party) – določa pravne ali fizične stranke, ki so udeležene v odnosih pri operacijah z vsebinami in storitvami (akterji).

Tipično razporeditev zgoraj opisanih elementov pri jezikih za opis pravic in odnose med njimi ilustrira naslednja slika št. 25.



Sl. 25: Osnovni gradniki jezikov za opis pravic (REL) in odnosi med njimi

Dva najbolj znana predstavnika jezikov za opis pravic sta XrML in ODRL. XrML se uporablja pri DRM sistemih v okviru standarda MPEG-21, OASIS Rights Language Techical Committee in Open eBook Forum. ODRL uporablja organizacija Open Mobile Alliance (OMA). Oba jezika REL temeljita na XML tehnologiji. [K9], [W31]

3.5.4.2.1. ODRL

Odprti jezik za opis digitalnih vsebin ODRL (ang. The Open Digital Rights Language) se razvija v okviru iniciative ODRL z namenom uspešno razviti odprto različico jezika REL, specifično namenjenega potrebam sistemov DRM. Ključen poudarek je na besedi odprt, kar pomeni, da je prosto dosegljiv in dostopen veliki množici potencialnih razvijalcev in uporabnikov. Zadnja različica (1.1) je izšla tudi pod okriljem organizacije W3C in predstavlja privzeti REL jezik pri DRM sistemu organizacije OMA ter pri projektu OpenIPMP (ang. Open Source Rights Management Project). [K9], [W34]

```
<rights>
 <agreement>
  <party>
   <context>
    <uid>urn:univ:us-wuw-deptIS </uid>
    <name>Department of IS, Vienna University of Economics and BA</name>
   </context>
   <rightsholder/>
  </party>
  <asset>
   <context>
    <uid>urn:univ:lr-wuw-vid-1</uid>
    <name>Marketing strategies for Universal</name>
   </context>
  </asset>
  <party>
   <context>
    <uid>urn:univ:us-wuw-uniBrux</uid>
    <name>Université Libre de Bruxelles</name>
   </context>
  </party>
  <permission>
   <play>
    <requirement>
     <prepay>
      <amount currency=EUR>10.00</amount>
     </prepay>
    </requirement>
    <constraint>
     <count> 5 </count>
    </constraint>
   </play>
  </permission>
 </agreement>
</rights>
```

Sl. 26: Primer zapisa opisa pravic v jeziku ODRL

3.5.4.2.2. XrML

XrML (ang. eXtensible Rights Markup Langugage) razvija podjetje ContentGuard, ki je skupni projekt podjetij Xerox in Microsoft. V primerjavi z ODRL XrML ni odprt jezik in ga je potrebno licencirati, kar je slabost. ContentGuard je z razvojem jezika XrML končal pri verziji 2.0 ter ga predal organizaciji OASIS. Najbolj znan uporabnik jezika XrML je standard MPEG-21 Part 5. [K9], [W35]

```
<?xml version="1.0" encoding="UTF-8"?>
<license xmlns="http://www.xrml.org/schema/2001/11/xrml2core"
         xmlns:sx="http://www.xrml.org/schema/2001/11/xrml2sx"
         xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
         xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xmlns:cx="http://www.xrml.org/schema/2001/11/xrml2cx"
         xsi:schemaLocation="http://www.xrml.org/schema/2001/11/xrml2cx
                                        ..\schemas\xrml2cx.xsd">
  <grant>
   <keyHolder>
    <info>
     <dsig:x509Data>
      <dsig:X509IssuerSerial>
       <dsig:X509IssuerName>CN=Guth Susanne,
                OU=Dept. of Information Systems,
                O=Vienna University of BA, L=Vienna,
                ST=Vienna, C=Austria
       </dsig:X509IssuerName>
       <dsig:X509SerialNumber>12345678</dsig:X509SerialNumber>
      </dsig:X509IssuerSerial>
      <dsig:X509Certificate>MIIEODCCA6GgAwIBAgIBEDANBgkqhki...
             ...Zos6NAm8m6UQBA== </dsig:X509Certificate>
     </dsig:x509Data>
    </info>
   </keyHolder>
   <cx:print/>
   <cx:digitalWork>
     <cx:locator>
       <nonSecureIndirect URI="http://www.wu-wien.ac.at/someResource"/>
     </cx:locator>
   </cx:digitalWork>
   <validityInterval>
     <notAfter>2005-12-24T23:59:59</notAfter>
   </validityInterval>
  </grant>
</license>
```

Sl. 27: Primer zapisa opisa pravic v jeziku XrML

3.5.4.2.3. Licenca

Pri sistemu DRM in tovrstnemu načinu zaščite sredstev (vsebin in storitev) uporabnik načeloma ni lastnik vsebin temveč samo pridobi pravico do njihove uporabe v skladu z določenimi pogoji. Ti pogoji so zapisani v licenci, ki je neke vrste pogodba med uporabnikom in lastnikom sredstev. Licenca je formulirana v jeziku za opis pravic in navadno vsebuje naslednje elemente:

- unikatno oznako sredstva (vsebine, storitve),
- informacije o ponudniku sredstev,
- informacije o uporabniku,
- pravice in omejitve uporabe,
- informacije o stanju vsebine – za potrebe sledenja vsebini (potrebno v primeru omejitve uporabe vsebine po npr. maksimalnemu številu uporabe) in uporabniškim navadam (če je to dovoljeno),
- varnostne informacije – dekodirni ključi, ki so potrebni za legalno uporabo vsebin, morajo biti kriptirani in ostati zaščiteni,
- avtentikacijske informacije – informacije za identifikacijo in avtentikacijo uporabnikov oz. njihove terminalne opreme. Na podlagi zadostitve predpogojev uporabe (npr. legalen uporabnik, izvedeno plačilo) se vsebina dešifrira in dovoli njena uporaba v skladu s pravili v licenci,
- druge varnostne informacije – zagotavljajo, da se vsebina licence ni spremenila, če le-ta ni kriptirana. Nekatere informacije morajo biti prosto berljive, da je sploh mogoča komunikacija med ponudnikom in uporabnikom. Primer takšne informacije je npr. naslov ponudnika storitev, če sta vsebina in licenca ločena elementa.

Uporaba licenc je bistvena lastnost in prednost sistemov DRM. Vsaka licenca je izdana za določeno vsebino in vezana na točno določenega uporabnika. Takšen način omogoča nedvoumno in izjemno natančno opredelitev individualizacije uporabe vsebin. Licenca prav tako veže določeno vsebino v smislu neprenosljivosti med različnimi uporabniki in terminalno opremo. Pomembna lastnost licenc je izjemen nabor možnosti opredelitve načina uporabe vsebin. To je tudi ena izmed glavnih prednosti pred drugimi sistemi zaščite vsebin, kot so npr. sistemi pogojnega dostopa. Uporabniki imajo na voljo možnost sami definirati, kako želijo konzumirati vsebino. Izbrani način seveda vpliva tudi na ceno storitve. V primeru večpredstavnih vsebin so pogoji uporabe vezani lahko na:

- časovne omejitve: uporaba je možna v določene časovnem intervalu,
- število ponovitev: uporaba vsebine je omejena na določeno število ponovitev,
- terminalno opremo: uporaba je možna na TV komunikatorju in ni mogoča na mobilnem terminalu,
- druge pogoje,
- kombinacijo pogojev.

Druga prednost pristopa z licencami je v ločitvi postopkov zaščite vsebin in načina definicije pogojev uporabe. Vsebine je potrebno le enkrat kriptirati, načinov uporabe (licenc) pa je neskončno mnogo. Glavni problem pri tem je v varovanju dekriptiranih informacij (glavnih ključev). Glavni ključi se morajo prenesti k uporabniku, da le-ta lahko sploh konzumira vsebine. Glavni ključi se tipično prenašajo v okviru licenc. Problem se največkrat rešuje z dvojnim kriptirnim modelom, kjer se glavni ključ še dodatno kriptira. V idealnem primeru se licenca in glavni ključi v celoti obdelajo v strojni varnostni opremi in nikoli niso izpostavljeni zunanjemu okolju. Zloraba namenske varnostne strojne opreme je bistveno težja kot zloraba DRM agenta v samo programski obliki.

3.5.4.3. Varni vsebovalnik

Na poti skozi omrežje in v okolju uporabnika so vsebine izpostavljene različnim nevarnostim. Njihova zaščita se doseže z ovijanjem originalne oblike vsebin v posebne objekte, ki se imenujejo varni vsebovalniki[3] (ang. Secure Container). Varni vsebovalniki so šifrirani z različnimi kriptografskimi postopki. Med standardnimi so najbolj uporabljeni simetrični šifrirni postopki (3DES in AES) za zaščito samih vsebin ter asimetrični šifrirni postopki (RSA) za zaščito dodatnih informacij (ključi, licence). Varni vsebovalnik zagotavlja tako integriteto (nespremenjenost) kot tudi varnost in izvornost (avtoriziranost vseh udeležencev) vsebin.

Manj priporočena, vendar zelo uporabljena, je tudi uporaba nestandardnih in skrivnih kriptografskih postopkov. Ta način se uporablja predvsem pri zaprtih in komercialnih DRM rešitvah, kot je npr. Microsoft DRM. Nestandardni kriptografski postopki niso nujno bolj varni od standardnih in znanih, saj nimajo možnosti tako obširnega testiranja s strani laične in strokovne javnosti. Ranljivosti v samem postopku in načinu uporabe dekodirne informacije lahko privedejo do kompromitiranja celotnega sistema.

3.5.4.4. Obdelava vsebin v okviru sistema DRM

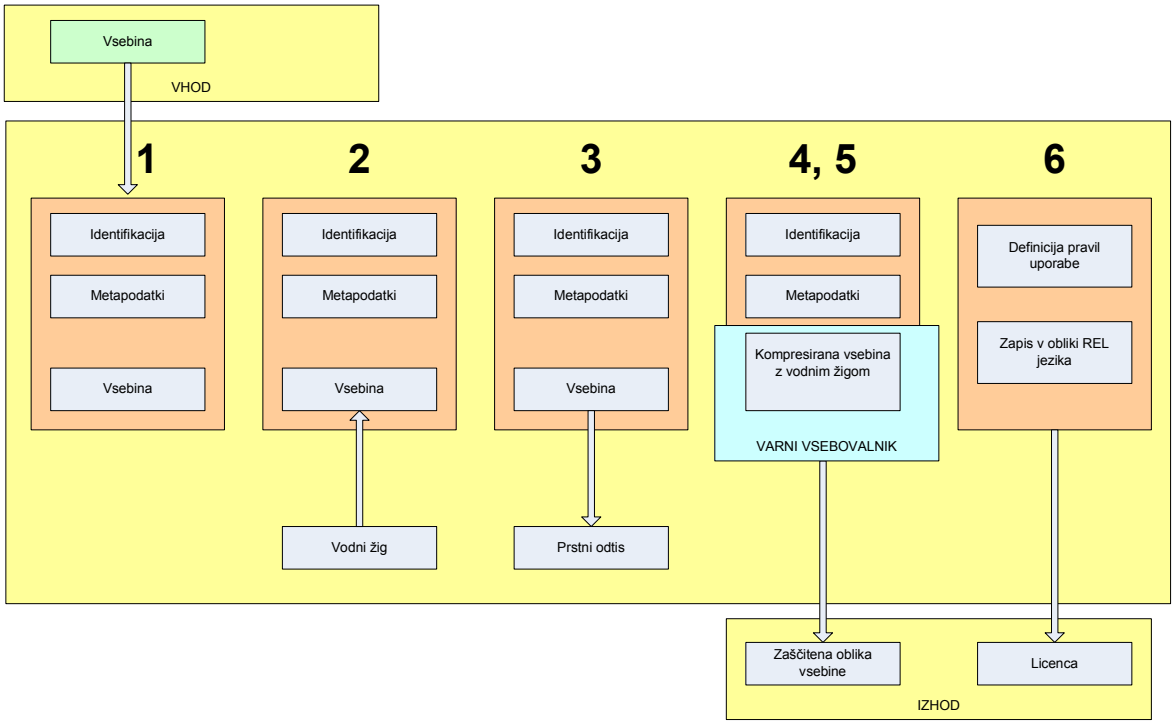
Vsebine gredo pri sistemih DRM skozi nekaj značilnih faz obdelave, preden so primerne za varno distribucijo in uporabo. Te faze so:

1. **opis vsebine** – vsebini se doda unikatna oznaka (identifikator) in se opremi z metapodatki.
2. **vodni žig** – vsebino se opremi z vodnim žigom. V splošnem je ta korak mogoče izvesti nad vsebino v originalni nekompresirani obliki ali pa v kompresirani obliki, pri čemer je prvi način bolj enostaven in najpogostejši.
3. **prstni odtis** – nad originalno vsebino v nekompresirani obliki se izdela prstni odtis. Uporablja se kot pomoč pri identifikaciji v kombinaciji s tehnologijo vodnega žiga. Ta korak se lahko izvede tudi nad vsebino, kateri je prej bil dodan vodni žig.

[3] Avtor predlaga za izraz Secure Container slovenski izraz varni vsebovalnik.

4. **kompresija vsebine** – vsebine, posebno večpredstavne, se zapišejo v bolj kompaktni kompresirani obliki.
5. **zaščita vsebine** – vsebina se ovije v obliko varnega vsebovalnika, ki je kriptiran.
6. **licenca** – sestavi se licenca za uporabo vsebine, ki je najpogosteje zapisana v enem izmed jezikov za opis pravic.

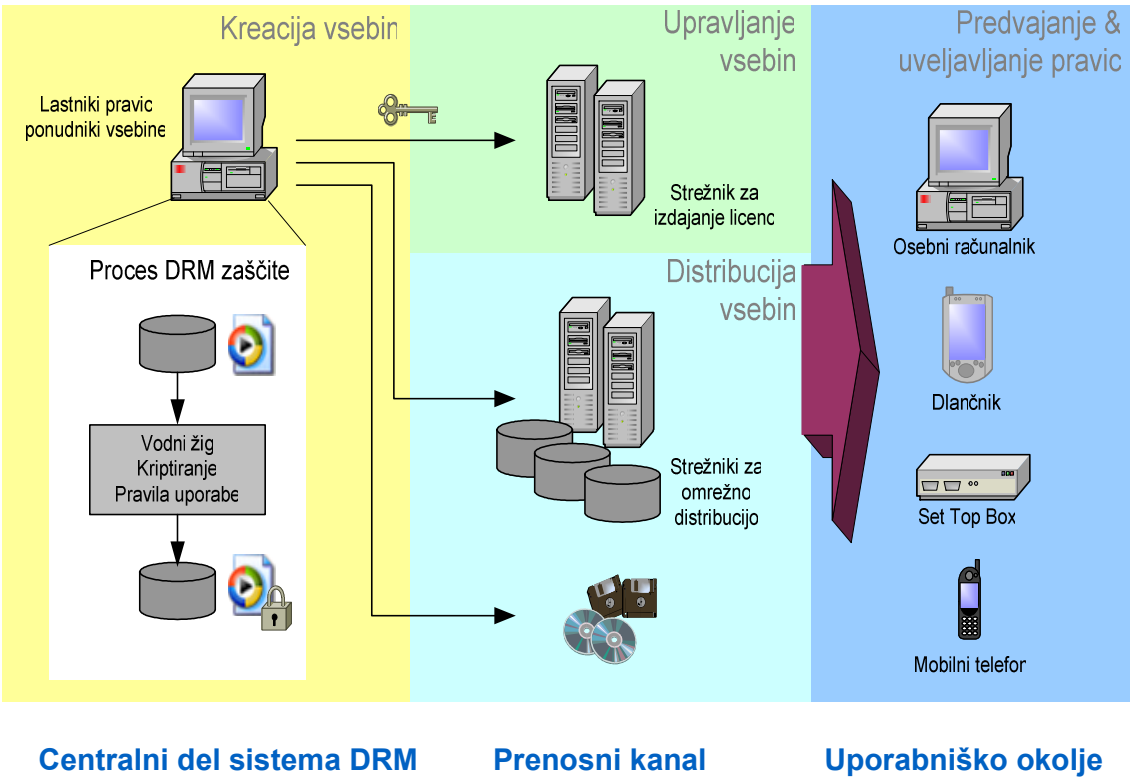
Sama licenca je lahko del varnega vsebovalnika ali pa je samostojna. V vsakem primeru sta oba elementa zaščitena.



Sl. 28: Procesi obdelave vsebin v okviru sistema DRM

3.5.4.5. Arhitektura sistema DRM

Vsak sistem DRM v grobem deluje na treh področjih in sicer na centralnem delu sistema pri ponudniku storitev, na vmesnem distribucijskem delu in v okolju uporabnika. Vsebine se v celoti pripravijo v centralnem delu, v različnih oblikah distribuirajo in konzumirajo pri uporabnikih. Oblike distribucije so lahko raznolike, od prenosa preko različnih omrežij v realnem času (pretočni prenos, strujanje) do prenosa na različnih digitalnih medijih. Poleg distribucije vsebin poseben problem predstavlja varna distribucija licenc in izmenjava dekriptirnih informacij (dekodirnih ključev). Pomembno dejstvo je, da so vsebine ves čas zaščitene in neuporabne brez ustrezne licence za uporabo (in seveda plačila storitve). Splošen sistem DRM je v grobi obliki ilustriran na sliki št. 29.



Sl. 29: Groba arhitektura splošnega sistema DRM

Do sedaj opisane tehnologije in elementi so deli sistema DRM. V tem poglavju jih bom povezal v celoto in predstavil potek dogajanja na primeru arhitekture splošnega sistema DRM. Posamezne aktivnosti se ujemajo s predstavitvijo na sledeči sliki arhitekture, slika št. 30.

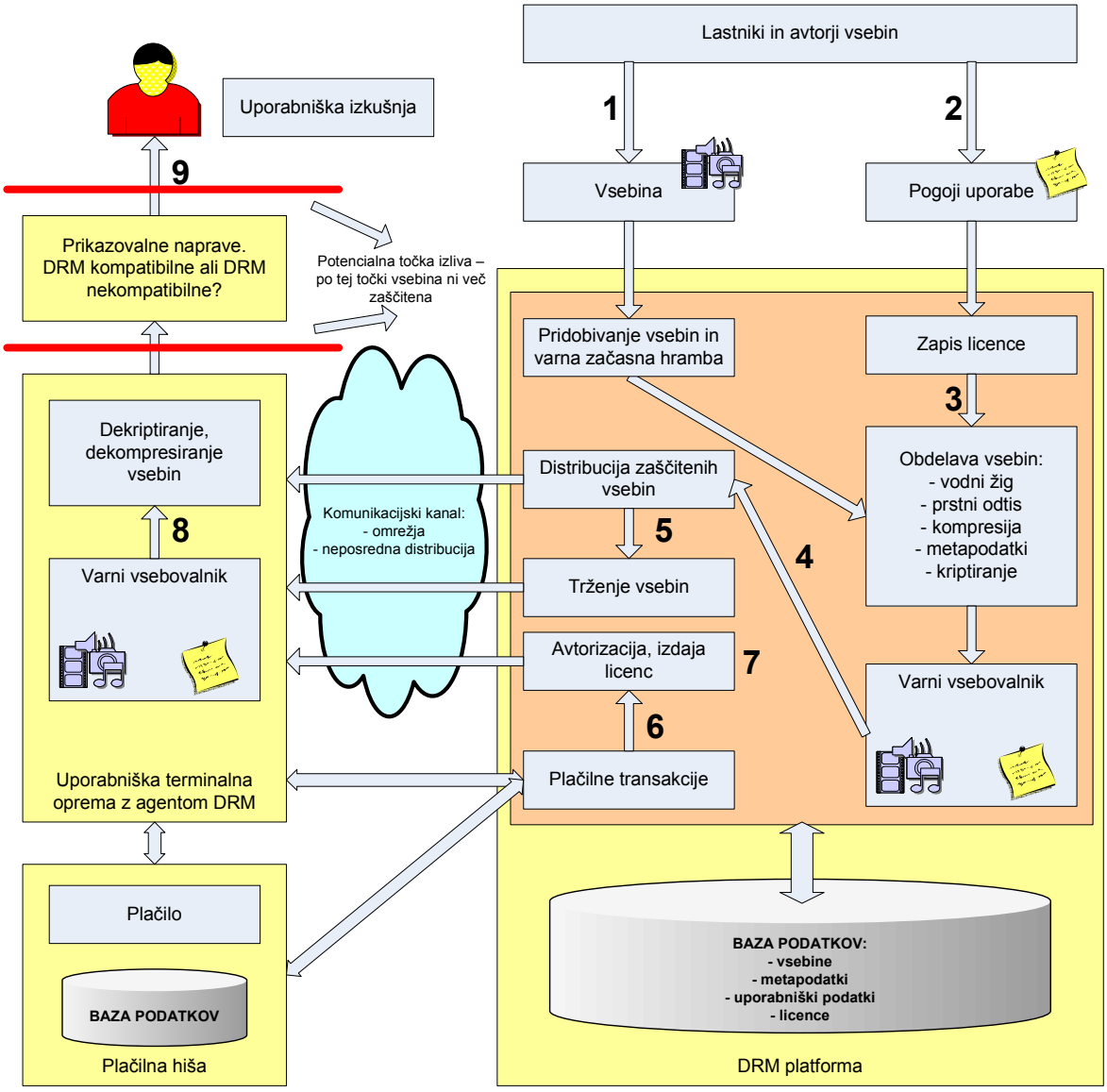
1. **Pridobitev vsebin** – avtorji in lastniki vsebin le-te dajo v uporabo preko ponudnikov vsebin. Prenos vsebin lahko poteka preko več kanalov, od omrežnega prenosa do dostave na prenosnih nosilcih. Zavedati se je potrebno, da vsebine v tem koraku še niso zaščitene s sistemom DRM, saj vanj šele vstopajo. Prenosni kanali morajo biti zato ustrezno varovani. V primeru omrežne distribucije so primerni varnostni mehanizmi na omrežnem in transportnem sloju. Najpogostejše oblike zaščite sta uporaba tehnologij IPSEC (omrežni sloj) in TLS (transportni sloj). Vsebina se začasno varno shrani na ponudnikovem strežniku.
2. **Oblikovanje pravil uporabe, kreiranje ponudbe** – avtorji in lastniki vsebin določijo osnovna pravila uporabe. Tako prenos vsebin kot tudi oblikovanje pravil uporabe morata biti za avtorje vsebin enostavna. Najprimernejše za to so namenske ali spletne aplikacije z prijaznim uporabniškim vmesnikom. Čeprav so kasneje pravila uporabe zapisana v drugačni obliki, ponudnikom vsebin za to ne sme biti potrebno obvladovanje računalniških tehnologij. Glede na poslovni model in posebne ponudbe ponudnik vsebin nato oblikuje svoja pravila uporabe. Le-ta so lahko zgolj bolj omejujoča nadgradnja osnovnih pravil, kot so jih določili avtorji vsebin. Pravila uporabe se nato zapišejo kot licenca v enem izmed jezikov za opis pravic, ustrezno zaščitijo in shranijo na licenčnem strežniku.

3. **Obdelava vsebin** – vsebine se obdelajo skladno s postopki DRM sistema. To vključuje opis vsebin, dodajanje vodnega žiga, generacija prstnega odtisa, postobdelava in kompresija ter končno kriptiranje in ovijanje v varni vsebovalnik. Licenca je lahko del same vsebine ali pa je samostojna. Vsebina je po končani obdelavi enoznačno določena, podpisana in zavarovana. Zloraba je mogoča zgolj s pridobitvijo licence oz. z napadom na kriptografski postopek.
4. **Distribucija vsebin** – vsebine se distribuirajo preko različnih kanalov. To so lahko prenosna omrežja, digitalni mediji in drugi načini. Večpredstavne vsebine so navadno shranjene na večpredstavnih strežnikih, ki so del IPTV platforme.
5. **Trženje vsebin** – opisuje dejansko ponujanje vsebin uporabnikom pod določenimi pogoji. Ta faza opisuje zahtevo po licenci. Za to obstaja več različnih pristopov:
    a. Uporabnik najprej pridobi vsebino neposredno od ponudnika in šele nato licenco. Uporabnikov agent DRM ob prvem poskusu uporabe kontaktira ustreznega ponudnika te vsebine in iz njegovega licenčnega strežnika pridobi licenco, ki se oblikuje glede na želje uporabnika.
    b. Uporabnik (A) pridobi vsebino od drugega (B) uporabnika. Metoda je znana tudi po izrazom »super distribution«. Drug uporabnik (B) ima že licenco in pravico do uporabe vsebine. Ta licenca je seveda vezana na drugega (B) uporabnika in ni primerna za uporabnika (A). Ko vsebino želi konzumirati prvi uporabnik (A), se zopet ponovi postopek pridobivanja licence.
    c. Uporabnik najprej pridobi licenco in šele nato vsebino.
6. **Plačilne transakcije** – naslednji logični korak je plačilo, ki se izvrši preko ustreznega plačilnega modela (npr. uporaba zunanje plačilne hiše). Najpogostejši načini so predplačniški model, pavšalni model in plačilo po uporabi vsebin.
7. **Avtorizacija uporabe vsebine** – šele po uspešni zahtevi licence in plačilu se licenca dejansko prenese k uporabniku. Možen je zadnji korak – uporaba vsebin.
8. **Uporaba (konzumacija) vsebin** – po pridobitvi vsebine in ustrezne licence je možna konzumacija vsebine. Pri tem se (odvisno od načina pridobitve licence v fazi trženja) izvedejo naslednji koraki:
    a. Uporabnik zahteva dostop do določene zaščitene vsebine.
    b. Terminalna oprema z agentom DRM preveri, če je dostop možen oz. če ima uporabnik ustrezne pravice. Če jih nima, se v tej fazi lahko sproži postopek za pridobitev licence oz. se v negativnem primeru zavrne dostop do vsebine.
    c. Če je vse v redu, identifikacija in avtorizacija uporabnika sta uspešni, licenca je pravilna, se želena vsebina dekriptira. To je naloga agenta DRM, ki je realiziran v programski ali strojni obliki.
    d. Dekriptirana vsebina se dekompresira.

e. Terminalna oprema končno upodobi vsebino. Ves postopek je potekal v skladu s pravili DRM. S tem se izognemo nevarnostim digitalne luknje, nevarnosti analogne luknje pa v določeni meri ostajajo. Nekateri DRM sistemi (npr. Trusted Computing) rešujejo tudi to področje s precej radikalnimi prijemi. Za uporabo vsebin ne zadošča samo ustrezna licenca in DRM kompatibilna terminalna oprema, temveč tudi DRM kompatibilna predvajalna oprema, kot so npr. TCP kompatibilni sprejemniki, avdio predvajalniki in računalniški monitorji.

9. **Uporabniška izkušnja** – opisuje uporabniško končno izkušnjo v smislu zadovoljstva pri uporabi vsebin in storitev. Za to je tako odgovoren celoten sistem strežbe vsebin kot tudi same vsebine. Sistem DRM mora biti čim manj opazen in moteč.

[K12]



Sl. 30: Arhitektura in potek dogajanja na primeru splošnega sistema DRM

3.6. Standardizacija

Sistemi DRM so zelo kompleksen sistem, zato je razumljiva težnja po standardizaciji celotnih sistemov oz. vsaj njihovih elementov. Zanimiva primera standardizacije sta projekta OMA in IPMP.

3.6.1. OMA

Organizacija OMA (ang. Open Mobile Alliance) je odprto standardizacijsko telo, ki se ukvarja z razvojem odprtih standardov in ogrodij na področju mobilnih tehnologij. Glavni cilji so promocija novih in sodobnih podatkovnih mobilnih storitev na podlagi zagotavljanja čim večje interoperabilnosti med vsemi akterji. V okviru dela organizacije OMA je velik poudarek tudi na razvoju mobilnih sistemov DRM, kjer trenutno obstajata standarda OMA DRM različica 1 in OMA DRM različica 2. Oba standarda sta prosto dostopna. Velja poudariti dejstvo, da so vsi prejšnji poskusi razvoja mobilnih sistemov DRM s strani organizacij WAP Forum in 3GPP sedaj združeni pod okriljem organizacije OMA, ki predstavlja (najbolj) pomembnega igralca na tem področju.

3.6.1.1. OMA DRM v1

OMA DRM različica 1 je bila razvita in objavljena leta 2002. Standard je sestavljen iz treh sklopov:

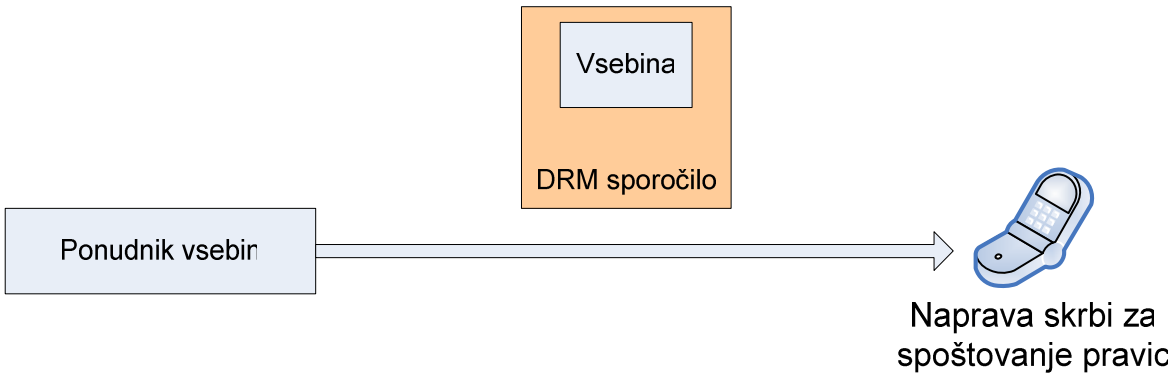
- splošna arhitektura,
- specifikacija jezika OMA REL,
- specifikacija DRM načina zapisa vsebin (vsebovalnik).

Pri različici je poudarek na specifikaciji načina zapisa in ne na varnostnih mehanizmih. Sam način zapisa vsebin je večinoma slabo oz. celo nekriptiran. Vsebinsko je poudarek na vsebinah majhne vrednosti, kot so klicne melodije in slikovno gradivo (e.g. logotipi). Po načinu varovanja in distribucije vsebin OMA v1 definira tri različne metode. Metoda »Forward-Lock« je obvezna, metodi »Combined Delivery« in »Separate Delivery« pa sta opcijski.

Specifikacija OMA DRM predpisuje le način zapisa, distribucije in opisa pravic, ne predpisuje pa samo implementacijo teh mehanizmov. Tak pristop omogoča določeno stopnjo fleksibilnosti posameznim proizvajalcev opreme. OMA DRM se zanaša na urejenost mobilnega okolja in spoštovanja pravil DRM s strani proizvajalcev mobilne (terminalne) opreme, kjer zaradi zaprtosti sam mobilni terminal lahko označimo kot napravo, odporno na zlorabe.

3.6.1.1.1. Metoda Forward-Lock

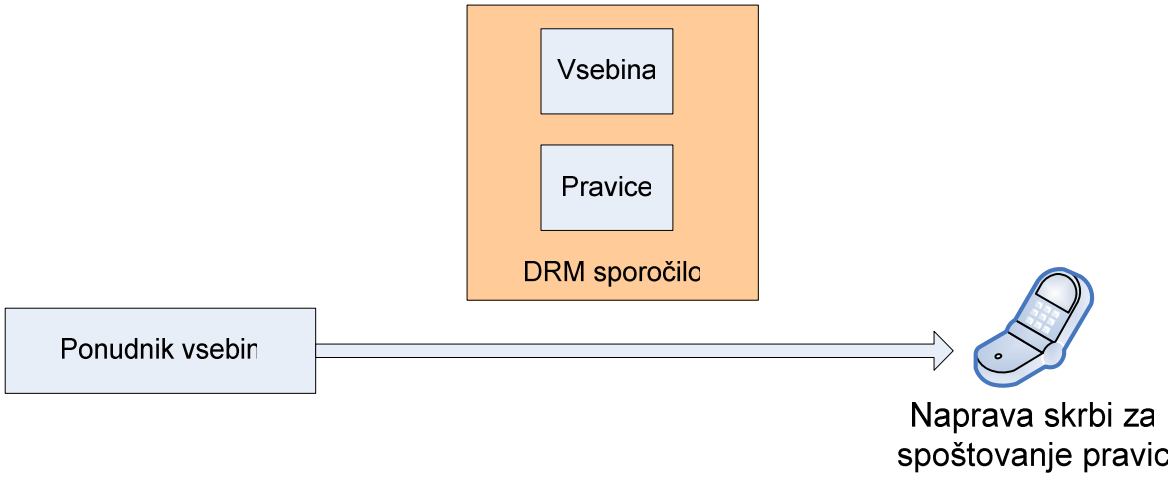
Vsebina je zapisana v vsebovalnikih, ki se imenujejo DRM sporočila (ang. DRM Message) in niso kriptirana. Za zagotavljanje restrikcij je odgovorna terminalna oprema. Glavna omejitev te metode je, da vsebina ne sme zapustiti končne terminalne naprave – je omejena na enega uporabnika. Za prenos je odgovoren protokol »OMA Download Mechanism«.



Sl. 31: OMA »Forward-Lock« metoda distribucije vsebin

3.6.1.1.2. Metoda Combined Delivery

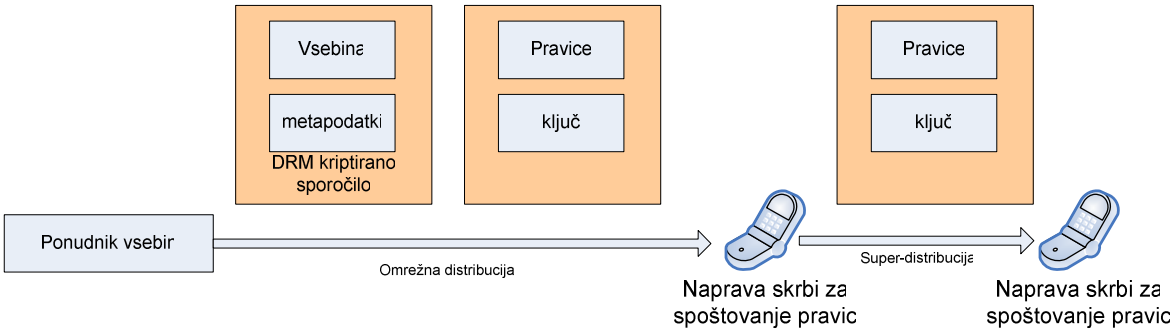
V primerjavi s prejšnjo metodo je tu mogoča bolj natančna definicija pogojev uporabe. DRM sporočilo vsebuje dodaten element, ki opisuje pravice in je opisan z OMA REL jezikom. Tudi tukaj DRM sporočilo ni kriptirano.



Sl. 32: OMA »Combined Delivery« metoda distribucije vsebin

3.6.1.1.3. Metoda Separate Delivery

Vsebina in opis pravic se distribuirata ločeno. Vsebina je pri tej metodi vedno kriptirana. Izbran kriptografski postopek je AES s ključem dolgim 128 bitov. Vsebina se na terminalno opremo prenese po protokolu »OMA Download Mechanism«, datoteka s pravicami pa se prenese posebej preko WAP push metode. Ta metoda distribucije je edina, ki omogoča nadaljno distribucijo vsebin. Uporabniki si lahko preko različnih kanalov med seboj izmenjajo tako zaščitene vsebine. Seveda je pri tem potrebna pridobitev ustreznih pravic za vsakega uporabnika posebej.



Sl. 33: OMA »Separate Delivery« metoda distribucije vsebin

3.6.1.1.4. Arhitektura OMA kompatibilnega sistema

Čeprav standard sam ne predpisuje natančne arhitekture, morajo OMA kompatibilni sistemi vsebovati naslednje komponente:

- pakirni strežnik (ang. Packaging Server) – preoblikuje vsebine v OMA DRM format,
- licenčni strežnik – izdaja licence,
- vsebinski strežnik – hrani OMA DRM vsebine,
- plačilna funkcija – infrastruktura za izvajanje denarnih transakcij za plačevanje,
- terminalna oprema – OMA DRM kompatibilna terminalna oprema.

3.6.1.2. OMA DRM v2

OMA DRM različica 2 je bila izdana julija 2005. Ponuja številne novosti, od katerih so pomembnejše:

- podpora močnejši kriptografiji – poleg simetrične je podprta tudi asimetrična kriptografija z javnim ključem,
- močnejša identifikacija in avtentikacija terminalne opreme,
- podpora jeziku za opis pravic ODRL,
- podpora bogatejšim vsebinam – podprte so večpredstavne vsebine večje kvalitete (zvok, slike, video), podpora strujanju (pretočnemu prenosu) vsebin, vsebine drugih tipov, npr. ohranjevalniki zaslona, lepotni dodatki, itd.
- novi modeli distribucije vsebin – npr. uporabnik, ki vsebino legalno poseduje, lahko le-to prenese na svojo drugo terminalno opremo. [K11], [W32]

3.6.2. IPMP

Kratica IPMP (ang. Intellectual Property Management & Protection) v splošnem označuje sistem za zaščito in upravljanje z avtorsko zaščitenimi vsebinami (i.e. DRM). Primer IPMP pri standardu MPEG-2 so klasični sistemi pogojnega dostopa. Koncept IPMP je resneje zaživel v okviru standarda MPEG-4 z definicijo t.i. priponk (ang. Hooks), ki predstavljajo standardiziran način vključevanja (tudi

nestandardiziranih) IPMP orodij v celotno arhitekturo uporabe večpredstavnih vsebin. Strokovnjaki so kmalu po objavi standarda začeli opozarjati na nepopolnost tako predlaganega sistema zaščite zaradi možne medsebojne nepovezljivosti različnih novih IPMP orodij pri razvoju MPEG-4 naprav.

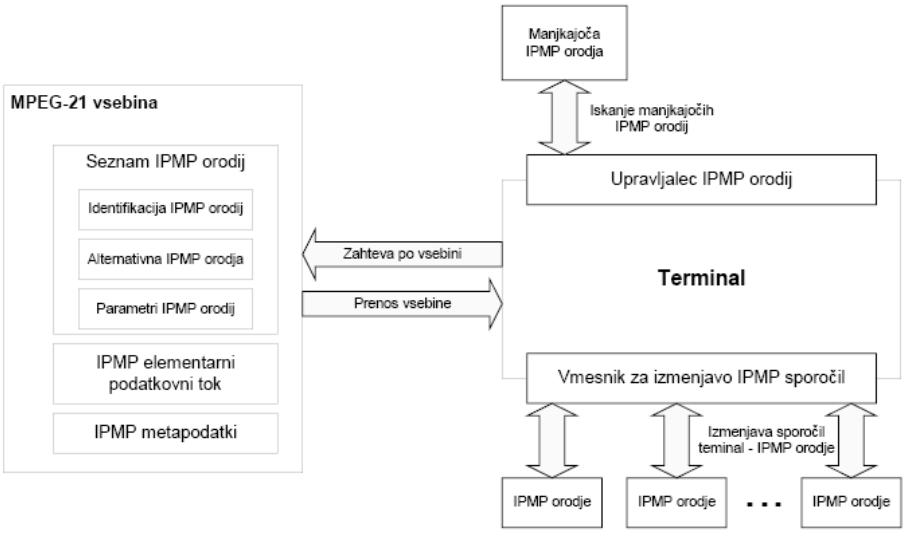
MPEG-21 nadaljuje delo na tem področju, začeto v standardu MPEG-4, z izgradnjo interoperabilnega ogrodja IPMP z uporabo IPMP orodij. Uporablja se termin IPMP orodje, ki je osnovni gradnik celotne IPMP rešitve. IPMP orodje je v osnovi zaprt gradnik oz. modul, ki opravlja določeno funkcijo, npr. avtentikacijo, kriptiranje, itd. IPMP vključuje standardiziran dostop do IPMP orodij, ne glede na njihovo lokacijo v informacijski infrastrukturi, definicijo protokola za izmenjavo sporočil med različnimi orodji IPMP in terminalno opremo. Poleg tega se posveča verodostojnosti orodij IPMP ter omogoča integracijo formul za opis pravic (ang. Rights Expressions) v skladu s slovarjem pravic in jezikom za opis pravic.

Najpomembnješi deli standarda MPEG-21, ki se nanašajo na področja sistemov DRM (IPMP), so:

- MPEG-21 Part 4: Intellectual Property Management and Protection (IPMP), ki definira arhitekturo rešitve,
- MPEG-21 Part 5: Rights Expression Language, ki definira jezik za opis pravic, ter
- MPEG-21 Part 6: Rights Data Dictionary, ki definira slovar.

Kot pri drugih standardih iz družine MPEG je tudi tu velik poudarek na interoperabilnosti. Na ta problem je mogoče gledati z vidika proizvajalcev orodij IPMP in z vidika uporabnikov. Sistem naj omogoča uporabo ene zaščitene vsebine na terminalni opremi različnih proizvajalcev ter več vsebin, zaščitenih z različnimi IPMP orodji, na isti terminalni opremi.

Gledano z arhitekturnega vidika upravljavec orodij IPMP analizira podatke IPMP, ki jih je prejel z vsebino ter uporabi ustrezna orodja IPMP. Če zahtevanega orodja IPMP ni na terminalu, ga poišče na mestu, ki je podano v opisu IPMP, ali pa uporabi nadomestno orodje IPMP, prav tako specificirano v opisu IPMP. Orodja IPMP komunicirajo tako s terminalom kot tudi med seboj, z uporabo vmesnika za izmenjavo sporočil IPMP.



Sl. 34: Arhitektura MPEG-21 IPMP [K37]

```
<License>
<!-- hipotetičen primer, dejanski primer vsebuje 'namespace' informacijo -->
<grant>
<!-- 'grant' pomeni podelitev pravice, medtem ko 'revoke' pomeni njen preklic -->
<Keyholder LicensePartID="Max">
<!-- definicija prejemnika pravice -->
<info>
<KeyValue>
<RSAKeyValue>
<Modulus>KTdTfdEsdfWf454sQEyZA</Modulus>
<Exponent>AQABCC==</Exponent>
</RSAKeyValue>
</KeyValue>
</info>
</Keyholder>
<!-- definicija pravice -->
<play/>
<diReference>
<!-- definicija objekta, na katerega se pravica nanaša -->
<Identifier>urn:mpegRA:mpeg21:dii:isrc:US-ZO3-99-32476</Identifier>
</diReference>
<validityInterval>
<!-- pogoj izvrševanja pravice -->
<notBefore>2005-06-01T00:00:00</notBefore>
<notAfter>2005-08-31T23:59:59</notAfter>
</validityInterval>
</grant>
<issuer>
<Keyholder LicensePartID="Jože">
<!-- identfikacija izdajatelja pravice -->
<info>
<KeyValue>
<RSAKeyValue>
<Modulus>KAdTfd34fEfdwQaQEyjA</Modulus>
<Exponent>AQABCC==</Exponent>
</RSAKeyValue>
</KeyValue>
</info>
</Keyholder>
</issuer>
</License>
```

Sl. 35: Primer opisa pravic pri MPEG-21 IPMP

Slika št. 35 prikazuje primer opisa licence v zapisu XML in skladu z MPEG-21 IPMP priporočili. Razvidni so nekateri elementi jezika za opis pravic (poglavje 3.3.4.2). Element *grant* definira: prejemnika pravice, vrsto pravice, identifikacijo vsebine, na katero se nanaša in pogoje za izvršitev pravic. Element *issuer* podaja informacijo o izdajatelju pravice. Opisan primer se v človeško razumljivi obliki glasi: "Izdajatelj pravice Jože, identificiran z navedenim ključem RSA, dovoljuje prejemniku pravice Maxu, identificiranim z navedenim ključem RSA, predvajanje vsebine, identificirane z URN identifikacijo, v času od 1.junija 2005 do vključno 31 avgusta 2005". Opazimo lahko, da je že najbolj enostaven primer za človeka dokaj zapleten, kar je pravzaprav razumljivo, saj je opis pravic namenjen avtomatskemu branju. Zaradi tega pa je zelo pomembno, da se pri izdelavi licenc strogo držimo opisne sheme REL. [K37], [W33]

3.6.3. Standardi v povezavi s sistemi DRM

Družina standardov, razvitih pod okriljem organizacije MPEG (ang. Moving Picture Experts Group), ki deluje v okviru organizacije za standardizacijo ISO/IEC, trenutno obsega predstavnike MPEG-1, MPEG-2, MPEG-4, MPEG-7 in MPEG-21. Prvi trije so namenjeni vsebinam samim v smislu razvoja učinkovitih kompresijskih postopkov in različnih načinov zapisa in dekompozicije vsebin v osnovne večpredstavne elemente (MPEG-4). Zadnja dva, MPEG-7 in MPEG-21, obravnavata načine opisa vsebin in njihove uvrstitve v širše okolje. Nekateri elementi standardov MPEG-7 in MPEG-21 se uporabljajo tudi pri gradnikih sistemov DRM in njihovih konkretnih implementacijah. Oba za način zapisa uporabljata XML tehnologije.

3.6.3.1. MPEG – 7

Standard MPEG-7, ki je formalno znan pod imenom »Vmesnik za opis večpredstavnih vsebin« (ang. Multimedia Content Description Interface), je namenjen izključno *opisu* vsebin. Definira različna orodja, postopke in sheme za opis vsebin. Način zapisa je v človeško in strojno berljivi obliki. Način opisa elementov pri standardu MPEG-7 ni odvisen od oblike vsebine. Mogoče je opisati tako digitalne vsebine kot tudi materialne vsebine (npr. papirnati dokument, vsebina na videokaseti, itd.).

Osnovni elementi MPEG-7 standarda so:

- opisna orodja:
    - deskriptorji (ang. Descriptors, D) – definirajo sintakso in semantiko vsakega opisnega elementa (metapodatek),
    - opisne sheme (ang. Description Schemes, DS) – definirajo strukturo in semantiko relacij med opisnimi orodji (D ali DS).
- jezik za definicijo opisa (ang. Description Definition Language, DDL) – definira sintakso obstoječih MPEG-7 opisnih orodij ter predpisuje načine kreacije novih deskriptorjev in opisnih shem.
- sistemska orodja – orodja za zapis MPEG-7 elementov v binarni in tekstovni obliki za potrebe shranjevanja in prenosa, multipleksiranje opisov, sinhronizacija opisov z vsebino, itd.

V okviru sistemov DRM je zanimiv kot standardiziran način opisa vsebin ter na področju izdelave prstnega odtisa vsebin, ki je tudi pomemben del standarda MPEG-7.

3.6.3.2. MPEG – 21 Multimedia Framework

Standard MPEG-21, znan pod imenom »Večpredstavno ogrodje« (ang. Multimedia Framework), je najmlajši v družini MPEG standardov. Zaradi uvajanja nekaterih popolnoma novih konceptov v verigo ponudbe in povpraševanja je MPEG-21 neke vrste lepilo, ki povezuje in zaokrožuje dosedanje dosežke skupine MPEG standardov. Njegova naloga je z uporabniškega vidika vzpostaviti resnično interoperabilno večpredstavno ogrodje. V povezavi s standardoma MPEG-4 in MPEG-7 ustvarja plodno podlago za razvoj novih večpredstavnih tehnologij.

MPEG-21 stremi k definiciji odprtega večpredstavnega ogrodja za identifikacijo, lociranje, prenos, uporabo in zaščito večpredstavnih vsebin, namenjenega vsem akterjem v verigi ponudbe in povpraševanja teh vsebin. Ponudnikom vsebin in storitev bo v takem okolju omogočen enakovreden nastop na z MPEG-21 podprtem odprtem trgu večpredstavnih vsebin in storitev. Končni uporabnik bo tako imel možnost transparentnega dostopa do širokega spektra vsebin in storitev, pri čemer pa bo zagotovljena tudi interoperabilnost različnih omrežnih in MPEG-21 kompatibilnih terminalnih naprav.

Cilje standarda MPEG-21 lahko zgoščeno zapišemo kot: definirati večpredstavno ogrodje, ki omogoča transparentno in izboljšano rabo večpredstavnih virov, ki so dosegljivi iz širokega spektra omrežij in naprav, uporabljenih v različnih uporabniških skupinah.

Med naloge standarda MPEG-21, ki jih mora le-ta izpolniti, sodijo identifikacija in definicija:

• posameznih mehanizmov in elementov opisane verige ponudbe in povpraševanja,

• medsebojne odvisnosti med temi mehanizmi in elementi,

• operacij, ki jih le-ti podpirajo.

V okviru posameznih delov MPEG-21 standarda so opisane naloge izvedene z definicijo in standardizacijo sintakse in semantike sestavnih elementov. MPEG-21 arhitektura je zgrajena na dveh osnovnih konceptih, ki izvirata na definiciji predmeta in osebka načrtovanega večpredstavnega ogrodja.

- **Digitalni predmet** (ang. Digital Item, DI) – predstavlja osnovni element transakcij v večpredstavni informacijski verigi, zato se smatra za predmet (»kaj?«) večpredstavnega ogrodja.
- **Transakcije z digitalnimi predmeti** – potekajo med MPEG-21 uporabniki, ki se zato smatrajo za osebek (»kdo?«) večpredstavnega ogrodja.

Prvega zato imenujemo tudi koncept digitalnega predmeta, drugega pa koncept interakcij uporabnikov z digitalnimi predmeti. Standard MPEG-21 sestavlja več delov. To so: MPEG-21 Multimedia Framework Part 1: Vision, Technologies and Strategy, MPEG-21 Part 2 – Digital Item Declaration, MPEG-21 Part 3 – Digital Item Identification, **MPEG-21 Part 4 – Intellectual Property Management and Protection (IPMP), MPEG-21 Part 5 – Rights Expression Language, MPEG-21 Part 6 – Rights Data Dictionary**, MPEG-21 Part 7 – Digital Item Adaptation, MPEG-21 Part 8 – Reference Software in MPEG-21 Part 9 – File Format.

V okviru problematike sistemov DRM so zanimivi deli Part 4, Part 5 in Part 6, ki se neposredno ukvarjajo z nekaterimi osnovnimi elementi sistemov DRM.

[K37], [W33]

3.7. Obstoječe rešitve

Na koncu analize sistemov DRM so predstavljeni še nekateri tipični predstavniki iz tega področja. Sistem Microsoft DRM sem izbral kot predstavnika tipične komercialne rešitve, iniciativo Trusted Computing kot možen (črn) scenarij prihodnjega razvoja sistemov za zaščito pravic (podobno sistemom DRM) ter projekt Tiramisu kot predstavnika odprtega sistema DRM, ki za osnovne elemente uporablja priznane standarde.

3.7.1. Microsoft DRM

Microsoftov sistem DRM je primer komercialne rešitve, ki je močno vpeta v obstoječo MS platformo za izvedbo IPTV storitev. Gre za popolnoma programsko rešitev, ki jo je v grobem mogoče razdeliti na centralno komponento in komponente terminalne opreme. Centralna komponenta dejansko predstavlja sistem DRM, terminalne komponente pa so namenjene razvoju in vključitvi funkcionalnosti sistema MS DRM v predvajalno programsko opremo na različni terminalni opremi. Zadnja različica MS DRM je verzija 10.

- Centralna komponenta: Windows Media Rights Manager 10 SDK
- Terminalne komponente:
    - Windows Media DRM 10 for Portable Devices – orodja za dodajanje MS DRM funkcionalnosti prenosni večpredstavni terminalni opremi (prenosni video predvajalniki, mobilni telefoni, itd.)
    - Windows Media DRM 10 for Network Devices – orodja za dodajanje MS DRM funkcionalnosti stacionarni terminalni opremi (TV komunikatorji, video predvajalniki, itd.)
    - Windows Media Format 9.5 SDK – orodja za razvoj predvajalne programske opreme
    - Windows Media Data Session Toolkit – orodja za zaščito vsebin pri prenosu na fizičnih digitalnih medijih (optični disk, disk, spominske kartice, itd.)

3.7.1.1. WM Rights Manager

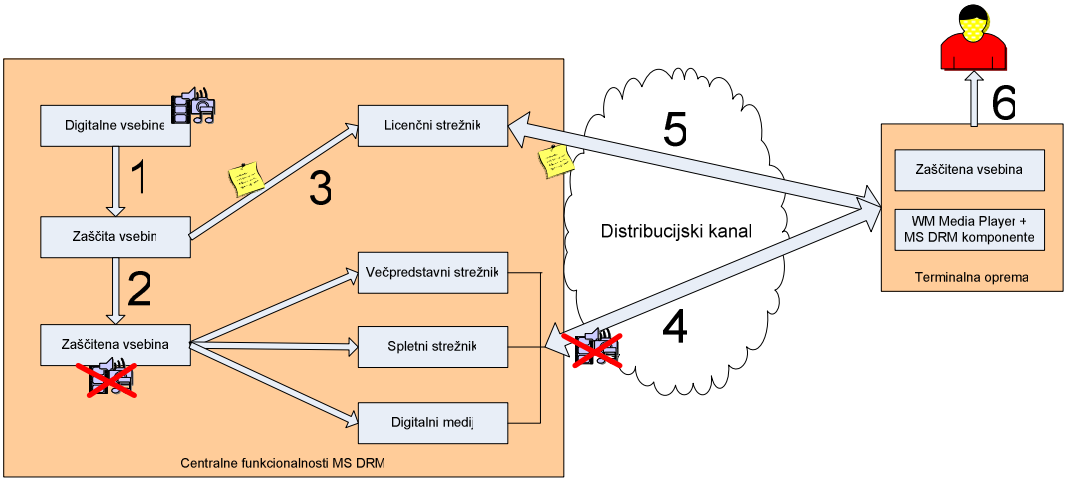
WM Rights Manager dejansko je MS DRM sistem in vsebuje vse potrebne komponente. Microsoft uporablja svojo terminologijo pri procesih DRM, ki pa funkcijsko ustreza procesom splošnega sistema DRM, kot je bilo opisano v prejšnjih poglavjih. Značilen pretok informacij skozi MS DRM sistem prikazuje slika št. 36.

1. **Pakiranje vsebin** – večpredstavne vsebine se zaščitijo v procesu pakiranja (ang. Packaging) s kriptografskimi postopki. Žive vsebine se kriptirajo v realnem času, pri vsebinah na zahtevo pa to ni nujno. Microsoft pri tem uporablja svoje kriptirne postopke, kar je dvorezen meč. Hkrati se kreira (glede na definicijo pogojev uporabe) ustrezna licenca, ki med drugim vsebuje tudi dekriptirni ključ. Vsebina je opisana z metapodatki in ima

določen naslov (URL) licenčnega strežnika. Vse vsebine so v formatu Windows Media.

2. **Distribucija** – zaščitene vsebine se distribuirajo na različne načine. Večpredstavne vsebine so tipično shranjene na večpredstavnem strežniku, kjer se s pomočjo pretočnega načina (strujanja) v realnem času prenašajo k uporabnikom. Prav tako je možna distribucija na digitalnih medijih.
3. **Licenca** – licenca določa pogoje uporabe. Kreira se v postopku pakiranja vsebin ter se shrani na licenčnem strežniku, ki je v celoti odgovoren za transakcije z licencami.
4. in 5**. Zahteva po uporabi vsebin** – uporabnik oz. njegova z MS DRM sistemom kompatibilna oprema pridobi zaščiteno vsebino. Podprtih je večina možnih metod izmenjave. Sama metoda pridobivanja licenc je lahko aktivna (uporabnik aktivno sodeluje pri procesu) ali pasivna (sistem sam poskrbi za pridobivanje licence brez interakcije uporabnika).
    a. licenca -> vsebina – uporabnik najprej pridobi licenco in šele nato vsebino,
    b. vsebina -> licenca – uporabnik najprej pridobi vsebino in nato licenco,
    c. vsebina + licenca – licenca je že del vsebine.

Y- **Konzumacija vsebine** – za konzumacijo vsebine je potrebna vsebina sama ter ustrezna in veljavna licenca.



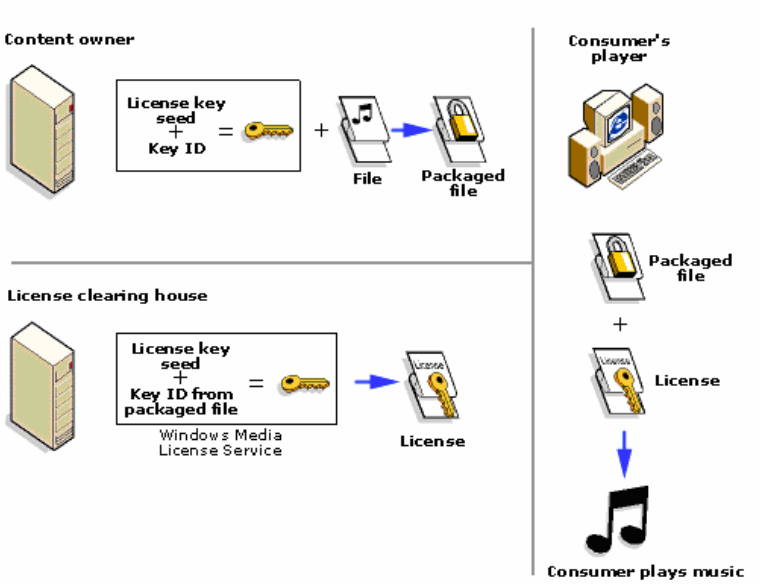
Sl. 36: Funkcionalna arhitektura MS DRM

3.7.1.1.1. Zaščita vsebin – pakiranje

Vsebine se zaščitijo s kriptiranjem, pri čemer se uporabi glavni ključ. Za generacijo glavnega ključa se uporablja dva parametra:

- License Key Seed – je enoten za določenega avtorja vsebine in ga enopomensko definira. Poznan je le avtorju in licenčnemu strežniku.
- Key ID – je spremenljiv in pri vsaki vsebini drugačen. Zapiše se tudi v zaščiteno vsebino (ang. Packaged File).

Pri dekriptiranju vsebin se glavni ključ ponovno generira in varno shrani v licenci. Pri tem se za generacijo uporabi Key ID, ki je del zaščitene vsebine in License Key Seed, ki ga pozna licenčni strežnik. License Key Seed nikoli ne zapusti licenčnega strežnika temveč ga le-ta uporabi pri generaciji glavnega ključa in licence.



Sl. 37: Proces generacije ključev

3.7.1.1.2. Licenca

Bistvena dela licence sta ključ za dekriptiranje vsebine ter pogoji uporabe. Možnosti definicije pogojev so zelo obširne, najbolj tipični scenariji so:

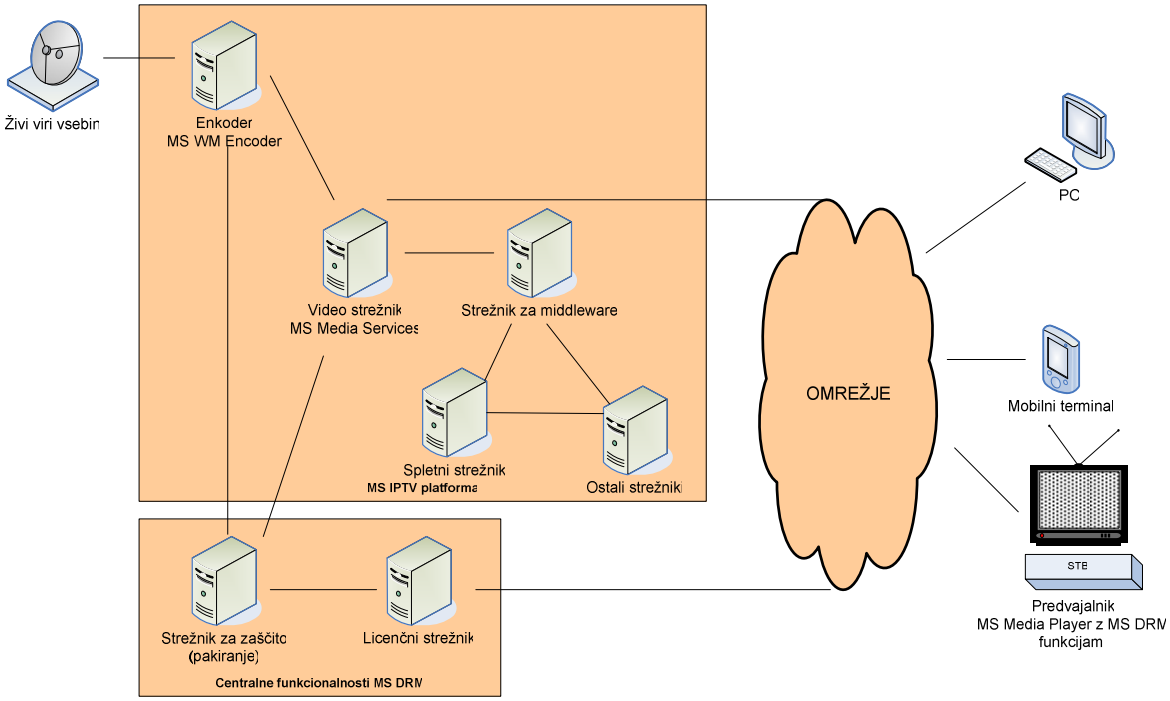
- omejitev po maksimalnem številu uporabe vsebine (npr. predvajanj filma),
- omejitev in definicija vsebine na specifično terminalno opremo (npr. možno je predvajanje z računalnikom, a ne s prenosnim predvajalnikom),
- časovne omejitve,
- omejitve glede distribucije same licence in prenosa pravic na tretjo osebo,
- definicija minimalnega zahtevanega nivoja varnostnih mehanizmov na terminalni opremi,
- drugi pogoji in njihova kombinacija.

Vsebine se v svojem življenjskem krogu kriptirajo le enkrat, njihove načine uporabe pa določajo različne licence, ki se sproti generirajo in prilagajo uporabnikom.

3.7.1.2. Vključitev MS DRM v MS IPTV platformo

Microsoftovo implementacijo IPTV platforme gradijo standardni gradniki. Vse komponente so programske in tečejo na MS Windows operacijskih sistemih teh PC kompatibilni strojni opremi. Vsebine, tako žive kot tudi na zahtevo, se kompresirajo in tudi kriptirajo na enkoderju vsebin (MS Windows Media Encoder). Interakcijo z uporabniki v smislu strežbe vsebin skrbi večpredstavni strežnik (MS

Windows Media Server). Gradnike DRM sistema predstavljata strežnik za pakiranje vsebin in licenčni strežnik. Prvi pri obdelavi vsebin tesno sodeluje z enkoderjem in večpredstavnim strežnikom, drugi pa je odgovoren za transakcije z licencami. [W36]



Sl. 38: Arhitektura MS IPTV platforme z MS DRM sistemom

3.7.2. Trusted Computing

Izraz *zaupanja vredno računalništvo* (ang. *Trusted Computing, TC)* se nanaša na družino specifikacij za doseganje določene stopnje varnosti oz. zaupanja na različni terminalni in strežniški opremi z uporabo varnostnih mehanizmov. Glavni cilji so povečanje splošne stopnje varnosti uporabe strojne in programske opreme, omejevanje škodljivega delovanja virusov, trojanskih konjev in podobnih zlorab programske opreme ter implementacija mehanizmov zaščite avtorsko zaščitenih vsebin. Sam pristop k reševanju teh problemov je precej radikalen in povzroča polemike, predvsem pri odnosu do razvoja programske opreme pod licenco odprte kode.

Kontroverzno je že samo ime tehnologije – zaupanja vredno (ang. Trusted), ki v različnih kontekstih pomeni različne stvari. Pri platformi Trusted Computing izraz zaupanja vreden ne pomeni vedno, da sistemu res lahko zaupamo, temveč da gre za sistem, ki smo ga prisiljeni uporabljati in mu zato posredno moramo zaupati. Primer je npr. grafični vmesnik, ki ne daje nobene garancije oz. nima nobenih posebnih mehanizmov zagotavljanja, da je dejanska prikazana slika na zaslonu res rezultat pričakovanega slikovnega upodabljanja informacij programske opreme. Grafičnemu vmesniku pač zaupamo, ker nimamo druge izbire oz. dokaza, da temu ni tako.

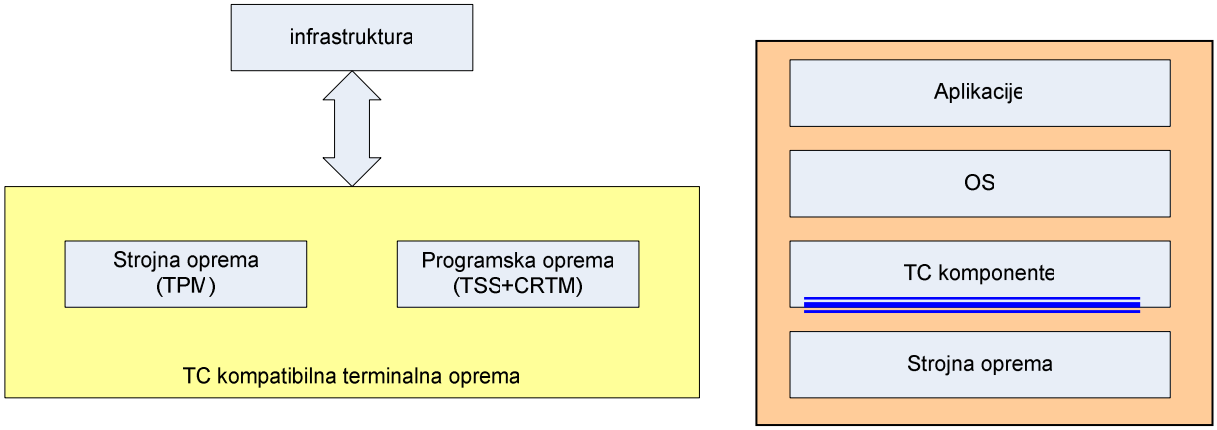
S platformo Trusted Computing se ukvarja organizacija TCPA (ang. The Trusted Platform Computing Alliance), ki je bila ustanovljena leta 1999 s strani največjih ICT podjetij, kot so: HP&Compaq, IBM, Intel, Motorola, Microsoft in druga. V organizacijo spadajo tudi podjetja, ki razvijajo strojno opremo PC platforme, osnovno programsko opremo (BIOS), zabavno elektroniko, programsko opremo, storitve, idt. V okviru organizacije TCPA deluje skupina Trusted Computing Group, ki je neke vrste naslednik TCPA in nadaljuje delo na tem področju. Sestavljajo jo ista velika podjetja kot TCPA: Microsoft, Intel, IBM, HP, AMD in drugi.

Osnovni koncepti Trusted Computing platforme so:

- potrebna je enopomenska identifikacija naprav in sestavnih delov naprav (npr. CPU in izvedena s certifikati,
- uporaba posebne strojne opreme za kritične varnostne mehanizme.

Osnovni elementi Trusted Computing arhitekture so:

- TCPA/TCG strojna oprema,
- TCPA/TCG programska oprema (podpora) in
- TCPA/TCG infrastruktura.



Sl. 39: TCPA/TCG elementi in pripadajoč slojni model

3.7.2.1. Strojna oprema – TPM modul

TCPA oz. TCG predvideva uporabo posebne varnostne strojne opreme, ki se imenuje modul zaupanja vredne platforme (ang. Trusted Platform Module, TPM). Modul TPM predstavlja visoko tehnološko na zlorabe odporno strojno komponento, ki je namenjena pomoči pri izvajanju varnostno kritičnih postopkov. Modul TPM tipično vsebuje generator naključnih števil, generator (RSA) ključev in poseben zavarovan NVRAM (ang. Non Volatile RAM) trajni pomnilnik. Ta pomnilnik je en izmed ključnih delov TPM modula. Vsebuje varnostno kritične informacije – ključe in se smatra za varnega. TPM modul prav tako omogoča beleženje varnostno pomembnih sistemskih dogodkov na način, ki je odporen na zlorabe. Večina bolj zahtevnih in višjenivojskih operacij se izvaja v programski opremi.

Ob prvi uporabi nove naprave uporabnik vzpostavi varen odnos z napravo preko t.i. avtorizacijske skrivnosti (i.e. z uporabo gesel). To geslo se tudi shrani v TPM modulu.

3.7.2.2. Programska podpora

TCPA kompatibilna terminalna oprema potrebuje dve vrsti programske opreme in sicer podporne storitve (ang. Trusted Platform Support Service, TSS) in jedro zaupanja (ang. Core Root of Trust for Measurement, CRTM). Prva skrbi za izvajanje kompleksnejših operacij in kriptografskih postopkov. Druga je del osnovne programske opreme terminalne naprave (tipično shranjena v BIOS) in se izvede v začetnih fazah zagona naprave. Naloga CRTM je izvajanje neke vrste varnostnih meritev programske sistemske opreme z zajemanjem karakterističnih informacij, kot so npr. »hash« vsote in vpisom teh informacij v TPM modul. S pomočjo teh vrednosti lahko višjenivojske varnostne funkcije preverijo spremembe (in pristnost) programske kode. Idejo »merjenja zaupanja« je mogoče razširiti tudi na nivo operacijskega sistema in aplikacij.

3.7.2.3. Infrastruktura

Infrastruktura med seboj povezuje TCPA kompatibilno opremo. Uporabniki imajo možnost ugotoviti stopnjo zaupanja v določeno okolje glede na izjave o zaupanju drugih akterjev (uporabnikov, opreme). Za to se uporabljajo mehanizmi digitalnih podpisov, certifikatov in kriptografije na podlagi javnih ključev.

3.7.2.4. Implementacije

V okvir TC platforme spadajo tudi posamezne iniciative nekaterih največjih podjetij s tega področja. Poleg skupne strategije vsako izmed teh podjetij razvija svojo TC rešitev, ki se dopolnjujejo. Bolj znane so:

- Microsoft: Palladium/NGSCB,
- Intel: LaGrande Technology (LT),
- AMD: Secure Execution Mode (SEM).

V okviru razvoja svojih rešitev glede na TCPA/TCG iniciativo predlagajo dodatne razširitve strojne in programske opreme. To so:

- Secure I/O – zavarovanje poti prenosa podatkov po vhodno/izhodnih vmesnikih z kontrolnimi vsotami in namenom zaznave poskusa zlorab (npr. video vmesniki, vmesnik za tipkovnico, itd.).
- Memory Curtaining – strojno podprto ločevanje pomnilniškega prostora.
- Sealed Storage – personalizirano kriptiranje vsebin na podlagi ključev, ki izhajajo iz specifičnih lastnosti programske in strojne opreme. Vsebino je mogoče dekriptirati le na izvorni strojni in programski opremi. Predlagana razširitev omogoča zelo visoko stopnjo varnosti in zasebnosti.
- Remote Attestation – omogoča zaznavanje sprememb na terminalni opremi. Varnostna strojna oprema popiše in izda certifikate za avtorizirano programsko opremo, ki jo uporablja uporabnik. To lahko na drugem sistemu služi kot dokaz, da je programska oprema nespremenjena.

Predlagani dodatni mehanizmi lahko delujejo v kombinaciji. Primer predstavlja npr. uporabnik, ki ima svoj osebni dnevnik. Mehanizem secure I/O ga zavaruje na vhodno/izhodnih vmesnikih, memory curtaining ga zavaruje v času uporabe dnevniške aplikacije pred drugimi aplikacijami, sealed storage garantira varno hrambo na disku, remote attestation pa omogoča branje dnevnika na drugi terminalni opremi le v primeru, če na njej teče predpisana dnevniška aplikacija.

[W37]

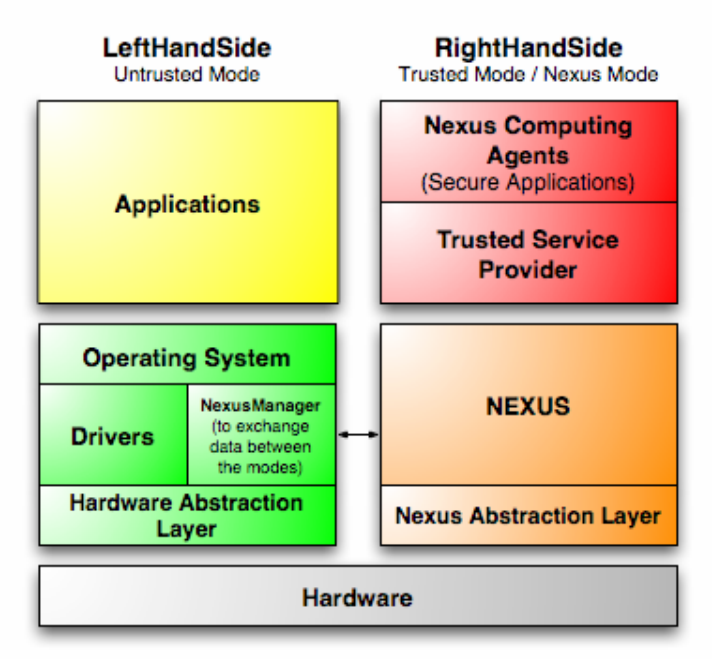
3.7.2.4.1. MS Palladium/NGSCB

Čeprav je Microsoft dejaven v iniciativi TCPA/TCG, vseeno razvija svoje rešitve. Idejno podobno (komplementarno) rešitev iniciativi TC predstavlja Palladium (imenovan po kemijskem elementu), ki se po novem imenuje NGSCB (ang. Next Generation Secure Computing Base).

Palladium/NGSCB prav tako temelji na posebni strojni in programski opremi, ki pa je nekoliko zahtevnejša. Palladium/NGSCB je pri strojni opremi tesno povezan z Intelovo rešitvijo LaGrande Technology.

Strojna komponenta pri Palladium/NGSCB se imenuje Security Support Component in je po funkcionalnostih podobna modulu TPM. Druga potrebna strojna komponenta je procesorska enota (i.e. CPU) z nekaterimi dodatnimi funkcijami (npr. podpora strojnemu ločevanje procesov in pomnilniškega prostora). Pri programski opremi je definirano novo izvajalno okolje – Nexus in agenti nexus (ang. Nexus Computing Agents, NCAs). Nexus predstavlja varni del jedra operacijskega sistema, agenti NCA pa varne module znotraj varnih aplikacij. Agent NCA predstavlja povezavo med varno aplikacijo in varnim delom operacijskega sistema (Nexus).

Podprta sta t.i. standardni in zavarovani način izvajanja. Pri slednjem je možno izvajanje le posebej podpisane programske opreme. [W37]



Sl. 40: Arhitektura Palladium/NGSCB [W37]

3.7.2.4.2. HDCP

HDCP (ang. High-bandwidth Digital-Content Protection) je tehnologija, ki jo razvija podjetje Intel in jo lahko uvrstimo v iniciativo TC. HDCP definira načine zaščite digitalnih vsebin pri prenosu preko digitalnih A/V vmesnikov DVI (ang. Digital Visual/Video Interface) in HDMI (ang. High Definition Multimedia Interface). Gre za reševanje problema analogne luknje in obliko DRM zaščite predvsem video vsebin visoke definicije.

Osnovna ideja HDCP je v kriptiranju prenosa med napravo za upodabljanje oz. predvajanje vsebin (npr. grafični vmesnik, HD-DVD ali Blu-Ray video predvajalnik) in za prikaz vsebin (HDTV monitor ali plasma TV). Prikaz vsebin v polni kvaliteti je možen le, če je medij legalen in, če sta obe napravi v odnosu (upodabljanje, prikaz) HDCP kompatibilni ter imata ustrezno licenco. V nasprotnem primeru naprava za predvajanje vsebin le-to upodobi v manjši kvaliteti (DVD video namesto HDTV in DAT zvok namesto polnega DVD-audio zvoka) oz. sploh ne. Z drugimi besedami to pomeni, da bomo poleg novih predvajalnikov in strojnih komponent v računalnikih potrebovali tudi nove HDCP kompatibilne monitorje, televizorje in celo zvočnike.

3.7.2.5. Kritika TC

Trusted Computing in sorodne rešitve so deležne veliko kritik, predvsem med razvijalci odprte programske kode. Sama ideja je sicer dobra in načeloma lahko ponudi večjo stopnjo varnosti, vendar je to dvorezen meč, ki lahko uporabnike priklene na določene proizvajalce strojne in programske opreme. Najbolj črn scenarij je tako scenarij »velikega brata«, kjer vse prednosti TC uživajo državne institucije in velike korporacije. Kritike je mogoče združiti na naslednja področja:

1. TC je (lahko) enako DRM

TC je podoben sistemom DRM, ki imajo včasih negativen prizvok. Veliko uporabnikov ne loči med njima. Če TC nastopa v vlogi sistema DRM, je še bolj strikten, saj je uporaba varnostne strojne opreme pogoj.

2. TC (lahko) pomeni manj svobode

Manj svobode je mišljeno v smislu možnosti izbire proizvajalcev strojne in programske opreme. V obeh primerih bo izbira pogojena z vrsto vsebin. Pri programski opremi bo uporabnik omejen z prevladujočimi predstavniki in načini zapisa (npr. podjetje ali država se bo odločila za uporabo zapisa dokumentov v formatu MS Office in ti bodo uporabni le v paketu Office in ne z drugimi programi). Pri vsebinah bo npr. večina filmov v zaščitenem formatu, ki ga favorizira predvajalna oprema določenega proizvajalca.

3. TC (lahko) pomeni manj zasebnosti

Strojni moduli pri TC vsebujejo podatke, ki enoznačno povezujeo uporabnika s terminalno opremo. Na ta način je mogoče slediti uporabniškim navadam in te podatke zlorabiti.

4. TC (lahko) pomeni manjšo stopnjo varnosti

Kontroverzna trditev, ki izhaja iz dejstva o vsiljevanju predpisanih varnostnih mehanizmov. Noben varnostni sistem ni nezlomljiv. V primeru »razbitja« je obseg zlorab zaradi velikega števila potencialno prizadetih naprav lahko zelo velik.

5. TC (lahko) onemogoča konkurenco

Uporaba zaščitenih vsebin bo mogoča le na TC kompatibilni opremi, ki uporablja tudi licenčne tehnologije. Ta način najbolj prizadene razvijalce proste programske opreme, kjer je strošek licenc lahko prevelik. V najslabšem slučaju bo mogoče uporabljati le zaščitene vsebine (in TC kompatibilne).

Zaradi precejšnjih kritik so zagovorniki TC iniciative predlagali tudi možnost izklopa TC funkcionalnosti. Vsak uporabnik bo imel možnost (v celoti) onemogočiti varnostne mehanizme TC na svoji terminalni opremi. Novo pridobljena svoboda je varljiva, saj bo uporaba zaščitenih vsebin možna le z vklopljenimi TC funkcionalnostmi.

3.7.2.6. Povezava s sistemi DRM

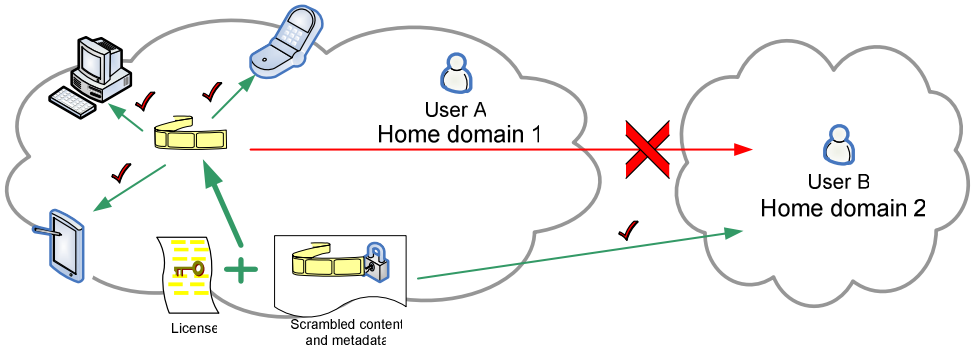
Kriterij	DRM	TC
povezava	je sistem DRM	je podlaga, se dopolnjuje s sistemi DRM
usmeritev	vsebinsko naravnan	bolj splošen
pravni status	obstajajo pravni akti (npr. Digital Millenium Copyright Act)	še ni posebnih pravnih aktov
kontrola izklopa	v primeru uporabe ni možen izklop	možen strojni izklop (zaščitene vsebine potem ne delujejo)
standardizacija	DRM oz. njegovi elementi se skušajo standardizirati, vendar je področje manj homogeno kot pri TC	večina dogajanja je združenega pod okriljem TC
stopnja varnosti	različna (lahko zelo visoka, lahko nizka)	splošno je lahko zaradi uporabe strojnih dodatkov zelo visoka
zrelost, dostopnost	sistemi so dostopni, prehajajo v zrelo obdobje	sistemi so v razvoju, splošna uporaba je negotova (izrazito negativen odnos javnosti)

Tab. 9: Primerjava lastnosti sistemov DRM in področja TC

3.7.3. Tiramisu

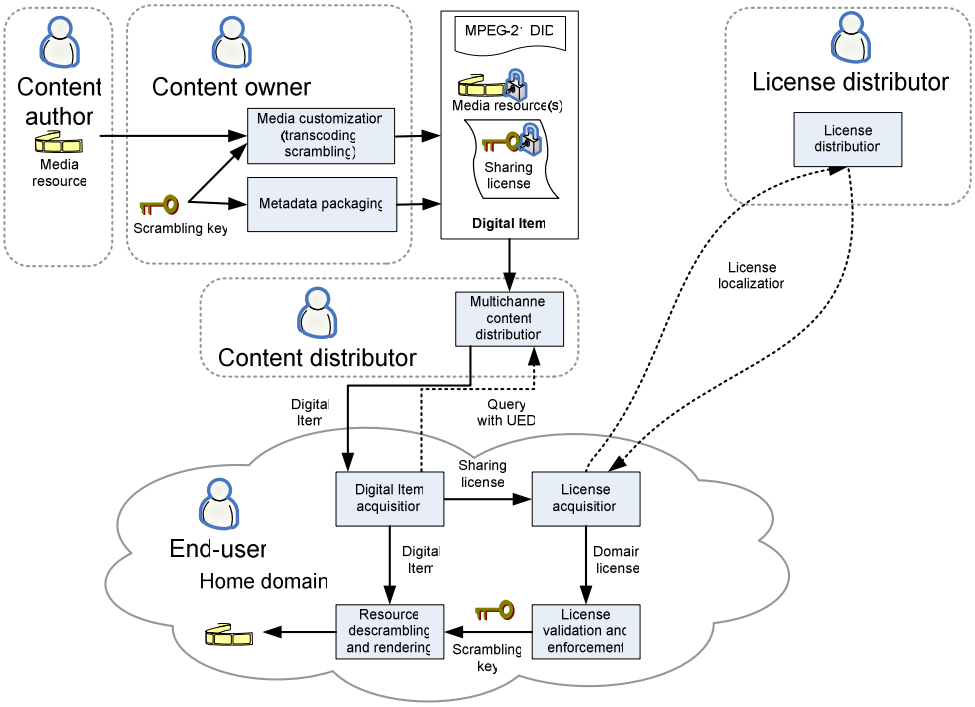
TIRAMISU (ang. The Innovative Rights and Access Management Inter-platform Solution) je evropski projekt s področja zaščite in distribucije večpredstavnih vsebin. Podpirajo ga številni svetovno priznani partnerji na tem področju, kot sta npr. Optibase in NagaraVision ter akademske ustanove, med drugimi tudi naša univerza in fakulteta (FE). Glavni cilj projekta je razvoj celotnega ogrodja za pripravo, distribucijo, zaščito in uporabo različnih večpredstavnih vsebin preko različnih prenosnih poti in medijev. Velik poudarek je na zaščiti avtorskih vsebin (sistem DRM) ter na uporabi standardov, predvsem MPEG-7 in MPEG-21. Tiramisu je ena izmed prvih celovitih implementacij na podlagi MPEG-21 standarda za večpredstavna ogrodja.

Zanimiva je ideja t.i. domačih domen (ang. Home Domain). Domača domena obstaja v okviru povezane skupine uporabnikov (npr. družinski člani). Vanjo spadajo različne vrste terminalne opreme, ki jo imajo ti uporabniki. Uporaba, prenos in hramba vsebin je možna na katerikoli terminalni opremi v domači domeni z enim naborom pravic (licence). Prenos med različnimi domenami zahteva pridobitev ustreznih novih licenc. Takšen pristop naj bi vzpodbudil večjo uporabo DRM sistemov in manj odpora do njih pri uporabnikih.



Sl. 41: Koncept domače domene [K36]

V okviru projekta TIRAMISU je bil razvit tudi sistem DRM za zaščito vsebin. Dodatno stopnjo varnosti zagotavlja uporaba strojnih komponent v obliki pametnih kartic, ki skrbijo za varnostno kritične funkcije (hramba ključev in dekodiranje vsebine). Sistem enakovredno ponuja orodja za pripravo in zaščito vsebin tako »velikim« avtorjem, kot tudi domačim uporabnikom. Vsak uporabnik lahko ustvari in zaščiti svoje vsebine ter jih da v uporabo ostalim uporabnikom. Osnovni potek delovanja in arhitekture sistema ilustrira spodnja slika. [K36]



Sl. 42: Arhitektura TIRAMISU [K36]

4. SISTEMI POGOJNEGA DOSTOPA

Tehnologija pogojnega dostopa (ang. Conditional Access – CA, ang. Authentication, Access Control System – AACS) omogoča selektiven dostop do vsebin digitalne televizije (ang. Digital TV) in ITV storitev. Pogojni dostop izhaja iz »televizijskega« sveta in je v zelo omejeni vlogi podoben sistemom DRM, vendar med njima obstaja nekaj pomembnih razlik (poglavje 5).

Sistem pogojnega dostopa je najbolj zaživel pri digitalni televiziji (ang. Digital Video Broadcast – DVB), vendar je uporaben za zaščito vsebin tudi na drugih sorodnih področjih, kot so digitalni radio (ang. Digital Audio Broadcast – DAB), IPTV in druge digitalne interaktivne večpredstavne storitve.

4.1. Definicija

V literaturi in na spletu zasledimo naslednje pomembnejše opise in definicije tega pojma:

The ITV dictionary,

»***Conditional Access – (CA) – (May also be known as: Authentication, Access Control System,) – CA is an encryption/decryption management method (security system) where the broadcaster controls the subscriber's access to digital and ITV services. This can ensure that the person is who he/she says he/she is (authenticity). It also offers security in purchase and other transactions. The end-users (subscribers) have a receiver/Set-top Box that allows reve her »Conditional Access« to the services available through that service.*** *»Smart cards« and/or a private PIN number are most often used to access the services, and/or premium services, by the end-user (subscriber.) The system is primarily made up of 3 parts: (1) signal scrambling, (2) encryption of electronic »keys« which the viewer will need, and the (3) Subscriber Management System – ensuring those who have bought the scrambled programming, are able to receive and watch it.*

The Subscriber Management System (SMS) is a combination of hardware and software as well as human activities that help organize and operate the company business. The SMS contains all customer relevant information and is responsible for keeping track of placed orders, credit limits, invoicing and payments, as well as the generation of reports and statistics. The SMS is part of the Customer Management System (CMS) and includes:

Entitlement Control Messages – (ECMs) – Data (probably encrypted) in the broadcast stream (which is the signal that travels to and from the subscriber and content provider) that contains information and directions from the subscriber such as the movie they want to see. This data doesn't necessarily have what would be considered more personal information, such as the number of months of service they want to pay for.

Entitlement Management Messages – (EMMs) – Data (probably encrypted) in the broadcast stream that contains information and directions from the subscriber that more directly deals with their account and personal listings, such as how much of the outstanding balance of their account they now want to pay. It doesn't deal with things such as what movie they want to see or what time they want to see that movie.

Subscriber Authorization System – (SAS) – It takes the SMS (Subscriber Management System) data and translates it into data the operational software can understand.

If the customer's set-top Box or built-in, has a "Common Interface" (CI), and it's often best if it does, the Set-top Box or built-in can be used on more than one encryption system. Consumers can use detachable hardware, which allows them to receive encrypted services they pay subscription fee(s) for. The interface between the set-top box and the CI hardware is standardized so that the same set-top box can be used to handle a variety of encryption systems.«

[W7]

WhatIs.com,

»***Conditional access (CA) is a technology used to control access to digital television (DTV) services to authorized users by encrypting the transmitted programming.*** *CA has been used for years for pay-TV services. There are numerous ATSC and DVB-compliant CA systems available for a broadcaster to choose from. The CA system provider provides the equipment and software to the broadcaster who then integrates the CA system into his equipment.* ***CA is not designed solely for DTV. It can be used for digital radio broadcasts, digital data broadcasts, and non-broadcast information and interactive services.*** *A CA system consists of several basic components:*

Subscriber Management System (SMS): The SMS is a subsystem of the CA system that manages the subscriber's information and requests entitlement management messages (EMM) from the Subscriber Authorization System (SAS). An EMM provides general information about the subscriber and the status of the subscription. The EMM is sent with the ECM. The ECM is a data unit that contains the key for decrypting the transmitted programs.

Subscriber Authorization System (SAS): The SAS is a subsystem of the CA system that translates the information about the subscriber into an EMM at the request of the SMS. The SAS also ensures that the subscriber's security module receives the authorization needed to view the programs, and the SAS acts as a backup system in case of failure.

Security module: The security module, usually in the form of a smart card, extracts the EMM and ECM necessary for decrypting the transmitted programs. The security module is either embedded within the set-top box or in a PC Card that plugs into the set-top box.

Set-top box: The set-top box houses the security module that gives authorization for decrypting the transmitted programs. The set-top box also converts the digital signal to an analogue signal so an older television can display the programs.

There are two DVB protocols used by CA systems: SimulCrypt and MultiCrypt. SimulCrypt uses multiple set-top boxes, each using a different CA system, to

authorize the programs for display. The different ECMs and EMMs required by each CA system are transmitted simultaneously. Each set-top box recognizes and uses the appropriate ECM and EMM needed for authorization. The ATSC standard uses SimulCrypt. MultiCrypt allows multiple CA systems to be used with one set-top box by using a PC card with an embedded smart card for each CA system used. Each card is then plugged into a slot in the set-top box. Each card recognizes the ECM and EMM needed for authorization.«

[W8]

Wikipedia,

»***Conditional access (»CA«) is the protection of content by requiring certain criteria to be met before granting access to the content. The term is commonly used in relation to digital television systems, most notable satellite television.***

Under the DVB, conditional access system standards are defined in the specification documents for DVB-CA (Conditional Access), DVB-CSA (the Common Scrambling Algorithm) and DVB-CI (the Common Interface). These standards define a method by which a digital television stream can be scrambled, with access provided only to those with valid decryption cards. These cards are read, and even sometimes rewritten with access rights, through a Conditional Access Module (CAM), a PCMCIA format card reader, rev onboard card reader meeting DVB-CI standards, such as that in the Sky Digibox.

Due to the common usage of CA in DVB systems, many tools to aid even directly circumvent encryption exist. CAM emulators and multiple-format CAM's exist which can either read many formats of cards even directly decrypt a compromised encryption scheme. Most multiple format CAM's, and all CAM's which directly decrypt a signal are based on reverse-engineering of the CA system.

A large number of companies provide competing CA systems, and the DVB standard allows the encryption of a channel in more than one system at once (Simulcryption). VideoGuard, Irdeto Access, Conax, Nagravision and Viaccess are among the most commonly used CA systems.«

[W9]

Tehnologija pogojnega dostopa je »zrela« in dobro definirana. Iz navedenih virov je razvidno, da so si definicije in opisi vsebinsko zelo podobni. Podoben opis zasledimo tudi v strokovni literaturi in v dokumentaciji znanih razvijalcev sistemov pogojnega dostopa. V primerjavi z definicijo sistemov DRM, kjer je bilo skupno definicijo nekoliko težje poiskati, lahko pri sistemih pogojnega dostopa povzamemo:

»Sistem pogojnega dostopa je tehnologija, ki omogoča nadzorovan, selektiven in varen dostop do vsebin digitalne televizije (ang. Digital TV) in ITV storitev, če so izpolnjeni določeni pogoji (ime –> pogojni dostop). Vsebine so zaščitene z kriptiranjem. Dostop do vsebin je možen z uporabo namenske strojne opreme, ki je največkrat v obliki dekodirnih modulov in pametnih kartic.«

4.2. Princip delovanja in arhitektura

Sistem pogojnega dostopa je v osnovi razdeljen na dva dela:

- sistemski – ponudnikov del (t.i. »Head-End«) in na
- uporabniški del (t.i. »User-End«).

Sistemski del vsebuje vse potrebne elemente za zaščito (kriptiranje) in distribucijo vsebin ter za nadzor nad sistemom in uporabniki. Uporabniški del je primarno namenjen avtentikaciji in avtorizaciji uporabnikov ter dekodiranju vsebin. Tipično je del uporabniške terminalne opreme (npr. TV komunikatorja) in ga sestavljata dekodirni modul (ang. Decoding Module, Decoder) ter pametna kartica (ang. Smart Card).

Glavne naloge in zahteve sodobnih sistemov pogojnega dostopa so:

- zagotavljanje plačevanja uporabljenih storitev,
- omejevanje dostopa do vsebin glede na geografski položaj,
- omejevanje dostopa do vsebin po različnih kriterijih (vrsta vsebine, vrsta uporabnika) in izvajanje t.i. starševske kontrole (ang. Parental Control),
- varovanje vsebin in odpornost na zlorabe,
- kodiranje vsebin v realnem času,
- enostavnost uporabe in neobremenjevanje uporabnikov,
- podpora velikemu številu uporabnikov,
- različne metode zaračunavanja,
- neproblematična uporaba različnih CA sistemov na isti terminalni opremi,
- upravljanje s pametnimi karticami (vklop/izklop kartice ali določenih storitev),
- pošiljanje sporočil na terminalno opremo,
- daljinska nadgradnja programske opreme terminalne opreme,
- primerna cena sistema za ponudnika (centralni del) in uporabnika (terminalna oprema).

4.2.1. Elementi sistema pogojnega dostopa

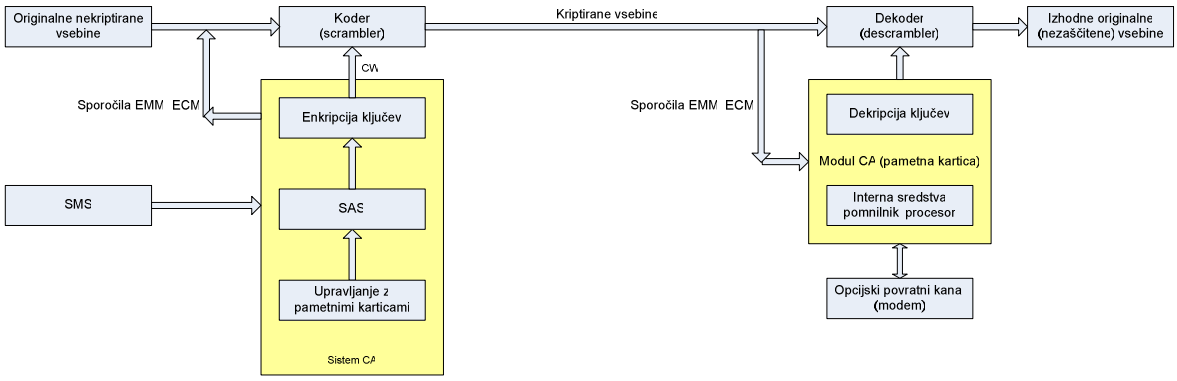
Varnost vsebin se podobno kot pri sistemih DRM zagotavlja z metodami kriptiranja. Pri tem natančneje ločimo pojem mešanja (ang. Scrambling), ki označuje kriptiranje vsebinskega dela signala (audio, slike, video, podatki) in pojem kriptiranja (ang. Encryption), ki označuje kriptiranje vseh ostalih vrst podatkov.

Sistemi pogojnega dostopa vsebine ščitijo z metodama mešanja vsebin in kriptiranja dekodirnih ključev. Z metodo mešanja (kodiranja) signala se izbrane vsebine zaščitijo tako, da so neberljive brez ustreznega dekodirnega ključa. Dekodirni ključi se prenašajo sprotno v okviru zaščitenega signala. Ker so

dekodirni ključi ključni in vitalni element za dekodiranje signala, so dodatno zaščiteni s postopkom kriptiranja.

Glavni funkcionalni elementi sistema pogojnega dostopa so:

- mešanje (kodiranje) signala (ang. Signal Scrambling),
- kriptiranje dekodirnih ključev,
- uporabniški nadzorni sistem,
- uporabniška terminalna oprema z ustreznim dekoderjem.



Sl. 43: Elementi sistema pogojnega dostopa

4.2.2. Kodiranje in dekodiranje signala

Pri digitalni televiziji (DVB, DAB) se vsebine prenašajo v okviru transportnega toka podatkov (ang. Transport Stream). Kodirnik (ang. Scrambler) vhodni transportni tok pretvori v obliko, ki je brez ustreznega ključa in dekodiranja neuporabna. Kodiranje se izvaja s pomočjo posebnega algoritma in nadzoruje z uporabo ključev oz. kontrolnih besed (ang. Control Word, CW). Kodirani paketi v transportnem toku so posebej označeni z ustreznim zapisom v njihovi glavi. Kodirani transportni tok podatkov se po potrebi multipleksira in distribuira preko različnih medijev. Dekodirni ključi oz. kontrolne besede se dodatno kriptirajo in pošljejo v okviru transportnega toka.

4.2.2.1. Common Scrambling Algorithm

Navaden (javen, skupen) kodirni algoritem (ang. Common Scrambling Algorithm – CSA) je bil razvit v okviru organizacije DVB (ang. Digital Video Broadcast-ing) za potrebe sistemov pogojnega dostopa pri digitalni televiziji (DVB). Je standardiziran in tudi t.i. »de facto« standard, ki se uporablja pri večini CA sistemov. Trenutno je bilo podeljenih 117 licenc izdelovalcem dekodirne opreme (večinoma izdelovalcem TV komunikatorjev) in 55 licenc izdelovalcem kodirne opreme (CA sistemi).

Algoritem CSA sestavljata dva dela in sicer:

- kodirna tehnologija – Scrambling Technology in
- dekodirna tehnologija/ sistem – Common Descrambling System (CDS).

Kodirno tehnologijo licencirajo izdelovalci CA sistemov, dekodirno tehnologijo pa izdelovalci terminalne opreme. Tehnologija CSA je dostopna kot standard v okviru organizacije ETSI.

4.2.3. Kriptiranje in dekriptiranje ključev

V okviru sistemskega dela sistema CA se generirajo in kriptirajo dekodirni ključi (CW) ter sporočila ECM (ang. Entitlement Control Messages) in EMM (ang. Entitlement Management Messages).

Sporočila ECM vsebujejo informacije o željenih vsebinah in so relativno neosebnega značaja. Prenašajo se v okviru t.i. broadcast podatkovnega toka.

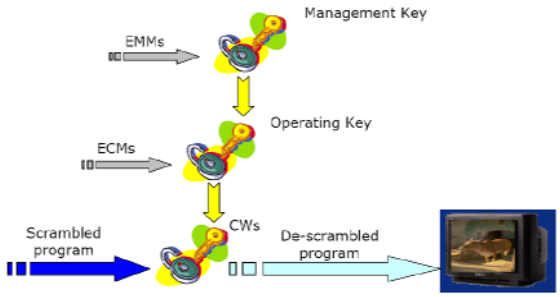
Sporočila EMM vsebujejo informacije o uporabnikih, njihovih pravicah, osebnih nastavitvah in plačevanju storitev ter so osebnega značaja. Prav tako se prenašajo v okviru t.i. broadcast podatkovnega toka.

Dekodirni ključi (CW) se kriptirajo in pošiljajo v sporočilih ECM. Dekodirni sistem v uporabniški terminali opremi dekriptira dekodirne ključe v skladu s pravicami uporabnika. Le-te so natančno določene v sporočilih EMM.

Varnost dekodirnih ključev in sporočil ECM in EMM je ključnega pomena za varnost celotnega sistema CA. Zaradi preprečevanja zlorab se ti parametri redno menjajo. Dekodirni ključi (CW) se tipično menjavajo v intervalih 10 s, sporočila ECM pa mesečno.

V uporabi sta dva načina enkripcije dekodirnih ključev in sicer algoritemski pristop (ang. Algorithm-Based Systems) in pristop na podlagi ključev (ang. Key-Based Systems). Delovanje in primerjavo med obema metodama razlaga spodnja tabela št. 10.

ALGORITEMSKI PRISTOP	**PRISTOP S KLJUČI**
DELOVANJE	
• pametna kartica sprejme ustrezna sporočila ECM, EMM, ki ne vsebujejo dekodirnega ključa (CW) • pametna kartica ima vgrajen nabor različnih dekripcijskih algoritmov • če je uporabnik upravičen do plačljive vsebine, se za dekripcijo dekodirnega ključa uporabi izbrani algoritem na pametni kartici • ostali dekripcijski algoritmi so rezerva in se uporabijo, če trenutni algoritem ni več varen	• vsaka pametna kartica ima svoj unikaten ključ (ang. management key), ki je kriptiran • za določeno storitev se v sporočilu EMM pošlje kriptiran ključ (ang. product key, ang. operating key). Le-ta se dekriptira s pomočjo dekriptirnega algoritma in unikatnega ključa pametne kartice. Rezultat je dekriptiran ključ, ki je bil poslan v EMM sporočilu. • Ta ključ se uporabi za dekriptiranje dekodirnega ključa, ki je bil poslan v ECM sporočilu. Pridobljeni ključ je t.i. kontrolna beseda (CW) in se uporabi za dekodiranje signala.

	
PREDNOSTI	
• nizka režija pri sporočilih ECM, EMM • večji nabor možnih načinov zaračunavanja storitev (različne uporabniške pravice)	• pogosto menjavanje ključev pripomore k varnosti sistema • enostavna izločitev in izklop »razbitih« kartic • hierarhična struktura ključev
SLABOSTI	
• omejen nabor dekripcijskih algoritmov; zamenjava kartice je nujna, če so »razbiti« vsi razpoložljivi algoritmi • tajnost algoritmov • vse pametne kartice vsebujejo isti nabor algoritmov, ni možno izločevanje »razbitih« kartic	• večja režija pri sporočilih ECM, EMM • hierarhičen pristop s ključi je bolj zahteven • določevanje različnih načinov zaračunavanja storitev je bolj omejeno

Tab. 10: Lastnosti različnih načinov enkripcije ključev in dekodiranja vsebin

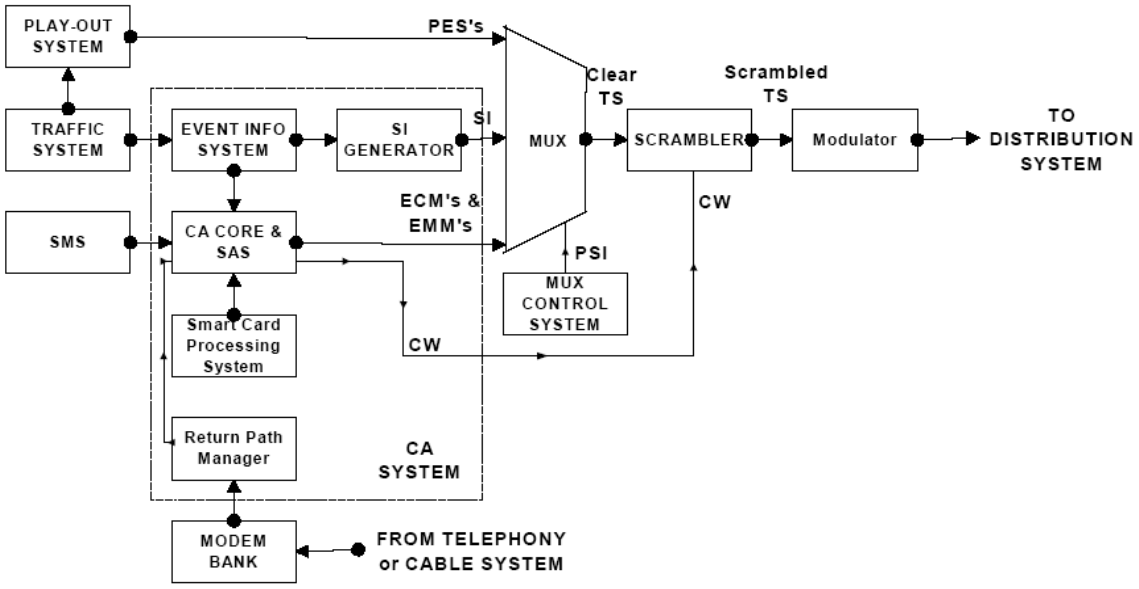
4.2.4. Uporabniški nadzorni sistem

Uporabniški nadzorni sistem oz. SMS (ang. Subscriber Management System) vsebuje informacije o naročnikih. Upravlja z naročniki, opravlja naloge zaračunavanja (ang. Billing) ter nadzoruje delovanje sistem CA (npr. vklop/izklop uporabnika). SMS pridobiva informacije o uporabniških pravicah iz sistema SAS.

Uporabniški avtorizacijski sistem oz. SAS (ang. Subscriber Authorization System) vsebuje informacije o uporabniških pravicah in njihovih pametnih karticah. Ti parametri so lahko serijska številka kartice, unikaten identifikator kartice, dodeljene pravice in drugo. Uporabnik oz. njegova pametna kartica se najprej registrira v sistemu SAS in se šele nato vključi preko sistema SMS (serijska številka kartice). Po tem postopku uporabnik že lahko spremlja plačljivo televizijo (ang. PayTV, PTV). Sistem SAS generira ustrezna sporočila EMM in neposredno komunicira z uporabniškim dekodirnim sistemom. V primeru okvar služi kot pomožni oz. »backup« sistem in prevzame tudi funkcije nadzornega sistema SMS.

4.2.5. Elementi »Head-End« sistema CA

Tabela št. 11 in slika št. 44 opisujeta glavne elemente generičnega DVB-CA sistema in odnose med njimi.



Sl. 44: Elementi »Head-End« sistema CA

ELEMENT	OPIS/NALOGA
Play-Out System	shranjevanje in priprava vsebin
Traffic Management System	avtomatizacija predvajanja vsebin glede na programsko shemo (spored)
SI Generator	generator informacij DVB-SI
Subscriber Management System	vsebuje podatke o naročnikih, zaračunavanje, vklop/izklop naročnikov
Subscriber Authorization System	podatki o uporabniških pravicah in njihovih pametnih karticah
CA Core	generiranje dekodirnih ključev, sporočil ECM in EMM
Smart Card Processing System	registracija pametnih kartic v sistem (SAS), določanje pravic uporabnikov
Return-Path Management System	nadzor nad povratnim komuniciranjem med STB in CA sistemom
Multiplexer (MUX)	multipleksiranje podatkovnih tokov
MUX Control System	nadzira multipleksno enoto, generira PSI (ang. Programme Specific Information) informacije
Scrambler	kodiranje izhodnega multipleksiranega podatkovnega toka na osnovi posebnega algoritma in dekodirnih ključev (CW), v primeru DVB standarda se uporablja algoritem CSA

Tab. 11: Značilnosti elementov generičnega CA sistema

4.2.6. Terminalna oprema

Uporabniško terminalno opremo navadno predstavlja TV komunikator, ki služi kot vmesnik med digitalnim in analognim svetom. Preko širokopasovnih vmesnikov sprejema podatke v digitalni obliki, jih preoblikuje, dekodira in pretvori v obliko, ki je primerna za prikaz na TV sprejemniku. V primeru uporabe zaščitenih storitev TV komunikator vsebuje tudi primeren dekodirnik.

Dekodirnik oz. t.i. varnostni modul (ang. Security Module) je navadno realiziran v obliki pametne kartice (ang. Smart Card). Iz sporočil EMM in ECM dekriptira ustrezne dekodirne ključe in jih posreduje enoti za dekodiranje (ang. Descrambling) signala. Dostop do pametne kartice je lahko dodatno zaščiten preko PIN kode.

V primeru različnih CA sistemov je zgornji pristop nepraktičen, saj potrebujemo za vsak CA sistem drug TV komunikator. V ta namen je bil razvit standardni vmesnik med terminalno opremo in uporabniško CA opremo. Vmesnik se imenuje skupni vmesnik (ang. Common Interface, CI) in omogoča uporabo različnih CA sistemov na isti terminalni opremi.

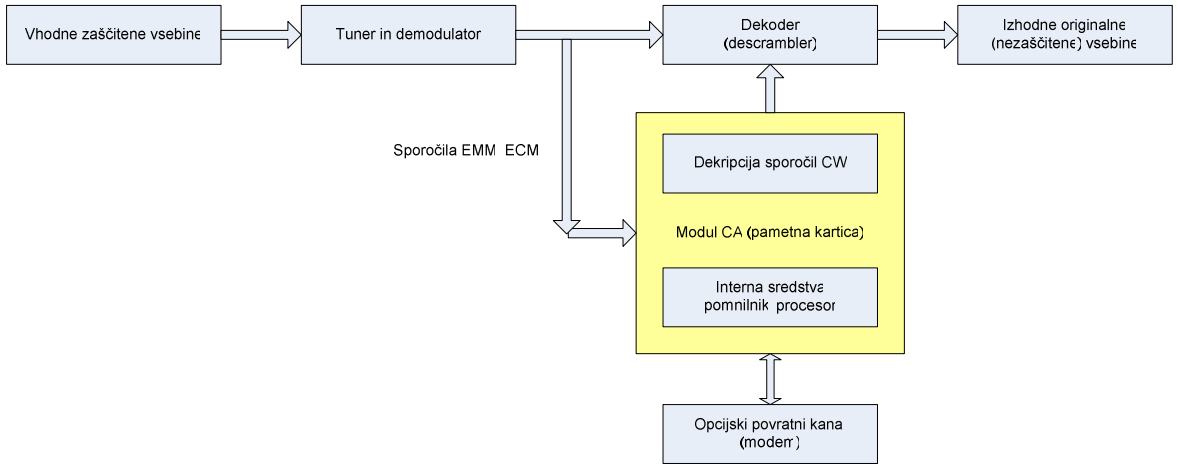
V okviru DVB standarda sta možna dva različna scenarija oz. pristopa uporabe CA sistemov. To sta SimulCrypt in MultiCrypt. Omogočata združevanje različnih sistemov pogojnega dostopa s stališča ponudnika in s stališča uporabnika.

Pristop SimulCrypt omogoča uporabo različnih CA sistemov v okviru enega transportnega toka podatkov. Ustrezni ključi se za različne sisteme pošiljajo simultano. Za vsak CA sistem potrebujemo drugo terminalno opremo, ki iz skupnega transportnega toka razbere ustrezne podatke.

Pristop MultiCrypt omogoča uporabo različnih CA sistemov na isti terminalni opremi. Terminalna oprema ima ločen prikazni in dekodirni sistem. Različni CA dekodirniki se na terminalno opremo priključujejo preko vmesnika CI. Ta pristop je za uporabnike primernejši, saj potrebujejo le en TV komunikator.

4.2.6.1. Elementi »User-End« sistema CA

Tabela št. 12 in slika št. 45 opisujeta glavne elemente generičnega DVB-CA uporabniškega sistema in odnose med njimi.



Sl. 45: Elementi »User-End« sistema CA

ELEMENT	OPIS/NALOGA
Descrambler	dekodira kodiran transportni tok podatkov na osnovi dekodirnih ključev
CA Module	na podlagi uporabniških pravic dostopa do vsebin dekriptira ustrezne dekodirne ključe in jih posreduje dekodirni enoti
modem, mrežni vmesnik	skrbi za povraten kanal

Tab. 12: Značilnosti elementov uporabniškega dela CA sistema

[W11]

4.3. Standardizacija

Tehnologija pogojnega dostopa je standardizirana v okviru standardov digitalne televizije DVB. Pri tem so pomembni naslednji standardi:

- DVB-CA – krovni standard za pogojni dostop,
- DVB-CSA – standard za način mešanja vsebin (Common Scrambling Standard),
- DVB-CI – standard za specifikacijo skupnega vmesnika (Common Interface),
- DVB-SIM – standard za metodo SimulCrypt.

Ena izmed pomembnejših posledic standardizacije tehnologije pogojnega dostopa je možnost medsebojnega delovanja sistemskega in uporabniškega dela implementacij različnih ponudnikov teh sistemov. Tako lahko ena terminalna oprema preko skupnega vmesnika podpira več različnih sistemov. Prav tako je pomembna standardizacija enotnega načina mešanja vsebinskega dela signala, kar omogoča ponovno uporabo enotne terminalne opreme za dekodiranje vsebin, zaščitenih preko različnih sistemov pogojnega dostopa.

4.4. Obstoječe rešitve

Sistemi pogojnega dostopa so tipična »televizijska« tehnologija. V osnovi omogočajo precej omejen nabor funkcionalnosti. S pridobivanjem na pomenu internetne televizije pa se tudi dosedaj klasični sistemi pogojnega dostopa preoblikujejo v smeri zaščite teh vsebin. Večina najbolj priznanih proizvajalcev sistemov pogojnega dostopa danes ponuja hibridne rešitve, ki omogočajo tako zaščito DVB vsebin kot tudi IPTV vsebin.

Najbolj znani ponudniki rešitev s področja pogojnega dostopa, ki izhajajo iz »televizijskega« sveta, so:

- Irdeto Access,
- Nagravision in Mediaguard,
- Viaccess,
- Philips CryptoWorks,
- Conax in
- NDS.

Obstajajo tudi rešitve, ki primarno izhajajo iz »računalniškega« sveta in so namenjene zaščiti IPTV vsebin. V osnovi gre za sisteme DRM, ki se po funkcionalnostih približujejo sistemom pogojnega dostopa. Zanimiv je način pristopa, ki je obraten kot pri razvijalcih klasičnih sistemov pogojnega dostopa. Primera tovrstnih rešitev ponujata podjetji:

- SecureMedia in
- WideVine Technologies.

Kot primer arhitekture specifičnega sistema pogojnega dostopa sem izbral podjetji Irdeto Access in WideVine Technologies. Oba predstavnika sta med najbolj priznanimi na tem področju.

4.4.1. Irdeto Access

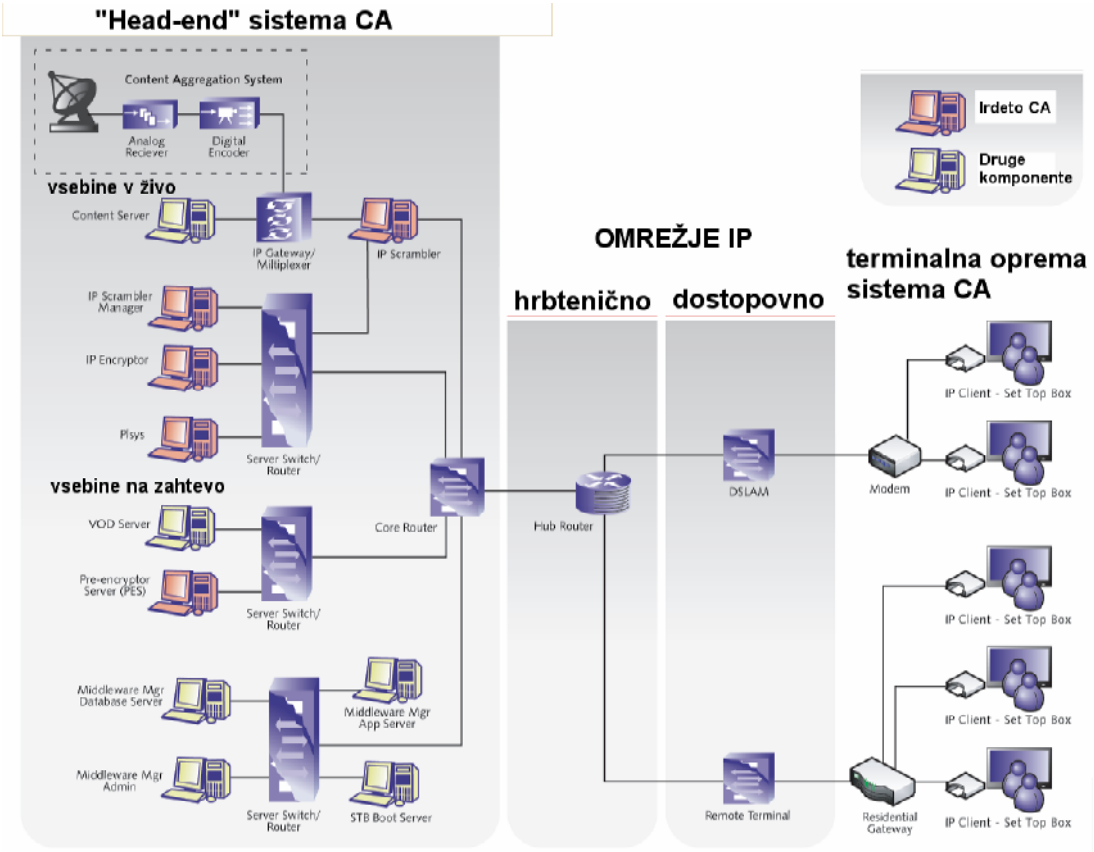
Irdeto Access je tipični ponudnik klasičnih rešitev na področju sistemov DVB pogojnega dostopa. Poleg tega ponujajo tudi IP rešitev, ki je nadgradnja klasične rešitve. V splošnem lahko njihove rešitve razdelimo na štiri segmente, in sicer:

- veliki sistemi – Irdeto Pisys,
- manjši sistemi – Irdeto M-Crypt,
- IP rešitev – Irdeto Piright in
- dekodirna CA terminalna oprema.

Produkt Pisys je namenjen srednjim in velikim postavitvam, ki imajo do nekaj milijonov naročnikov (do 5 milijonov v maksimalni izvedbi). Vsebuje vse potrebne elemente sistema pogojnega dostopa ter je modularno sestavljen. Omogoča različne metode dostopa do vsebin ter metode plačevanja, kot so naročniški in predplačniški paketi. Med posebnosti spadata možnost deljenja funkcionalnosti

ene postavitve Irdeto Pisys sistema pogojnega dostopa več operaterjem ter možnost hkratnega dekodiranja več tokov zaščitenih vsebin (do dva DVB MPEG-2 tokova) na strani terminalne opreme pri uporabniku. Produkt M-Crypt je nekoliko bolj omejen in namenjem nekoliko manjšim postavitvam do maksimalno stotisoč naročnikov. Pri tem obstaja možnost popolne nadgradnje v večji sistem Pisys.

Produkt z imenom Piright je namenjen zaščiti IPTV vsebin in je nadgradnja obeh prejšnjih produktov. Jedro sistema predstavlja izvedenka Pisys sistema z dodatnimi elementi. To so upravljalec transakcij (Irdeto IP Transaction Manager), Irdeto GigaCrypt, predkodirnik (Irdeto Pre-encryption station), licenčni strežnik (Irdeto Key Manager) ter komponente terminalne opreme in nadzora dekodiranja vsebin. Pri tem IP Transaction Manager skrbi za nadzor prenosa (unicast in multicast) preko omrežij IP, GigaCrypt za kodiranje (mešanje) vsebin v realnem času, predkodirnik za kodiranje vsebin na zahtevo, licenčni strežnik pa za upravljanje s ključi in licencami. Podprte so različne vrste večpredstavnih vsebin v obliki videa, avdia in podatkov ter v formatih MPEG-2 in MPEG-4. Postopek zaščite vsebin (mešanje, kriptiranje) lahko poteka v realnem času za žive vsebine ter v nerealnem (predkodiranje) času za vsebine na zahtevo. Relativno omejenim načinom nadzora nad vsebinami iz področja klasičnih sistemov pogojnega dostopa so dodani novi načini definicije pravic, kot so značilni za sisteme DRM. Piright je v primerjavi s samo programskimi izvedenkami sistemov DRM od sistemov pogojnega dostopa za dekodiranje podedoval pristop s pametnimi karticami, kar omogoča relativno visoko stopnjo varnosti. Odnose med posameznimi elementi IP CA rešitve ilustrira spodnja slika. [W12]



Sl. 46: Arhitektura Irdeto Piright sistema pogojnega dostopa za zaščito vsebin v okolju IPTV

Podjetje Irdeto Access svoje rešitve aktivno izboljšuje in vse bolj prodira na segment zaščite vsebin platforme internetne televizije. To dokazujejo skupni projekti in sodelovanje s priznanimi podjetji s področja IPTV, kot so Kasena, Minerva, Amino in drugi.

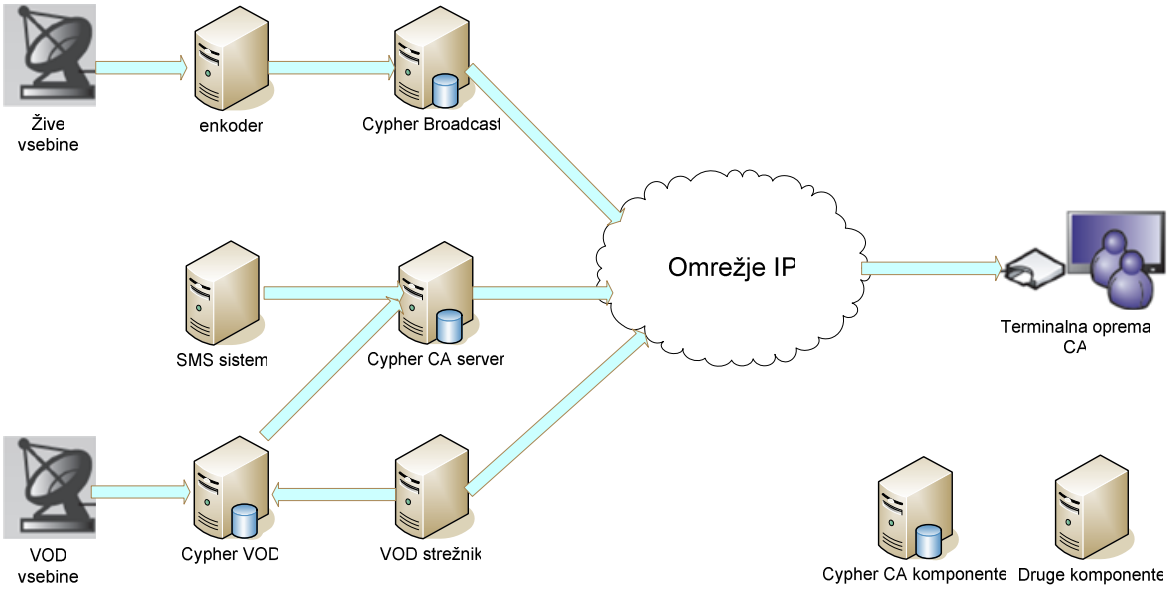
4.4.2. WideVine Technologies

Podjetje WideVine Technologies je relativno novo na področju sistemov pogojnega dostopa, saj je bilo ustanovljeno šele leta 1999. Kljub temu so se že v začetku usmerili k sistemom zaščite digitalnih vsebin pri prenosu preko širokopasovnih telekomunikacijskih omrežij in imajo pri tem podporo nekaterih največjih ameriških podjetij zabavne industrije, kot so NBC, Viacom, Time Warner, Sony in drugi. V primerjavi s pristopom podjetja Irdeto njihova rešitev ne temelji na nadgradnji klasičnega sistema pogojnega dostopa za potrebe platforme IPTV, temveč je že v osnovi takšna. Pristop prinaša nekatere prednosti in slabosti. Med glavne prednosti spada boljša zasnova sistema, ki je bolj prilagojena IPTV platformi, med slabosti pa relativno slaba poznanost podjetja. WideVine Technologies ponuja celotno rešitev tipa »end-to-end«, ki je sestavljena iz naslednjih komponent:

- Cypher CA - upravljanje z uporabniškimi pravicami (licencami),
- Cypher VOD – kodiranje in dekodiranje VOD vsebin,
- Cypher Broadcast – kodiranje in dekodiranje živih (ang. Broadcast) ITV vsebin,
- Cypher DCP – terminalna programska oprema za dodatno zaščito vsebin pred zlorabo,
- Cypher S-Chip – kombinacija programske in strojne opreme za dekodiranje in zaščito vsebin pred zlorabami in nepooblaščeno uporabo.

Komponenta Cypher CA predstavlja jedro celotnega sistema in omogoča upravljanje z licencami in uporabniškimi pravicami. Podprti načini zapisa so MPEG-2, MPEG-4, ISMA in drugi v unicast in multicast načinu prenosa. Komponenta Cypher VOD je odgovorna za zaščito lokalno shranjenih vsebin in vsebin na zahtevo. Podprt je tudi SimulCrypt standard. Komponenta Cypher Broadcast skrbi za sprotno zaščito vsebin v realnem času. Komponenti Cypher DCP in Cypher S-Chip sta del uporabniške dekodirne terminalne opreme. Posebnost je t.i. programska navidezna pametna kartica (ang. Software Based Virtual Smart Card), ki omogoča simulacijo funkcionalnosti pametne kartice zgolj preko programske opreme. Sistem za upravljanje z naročniki (SMS) ni del arhitekture. Arhitekturo rešitve prikazuje slika št. 47.

[W16]



Sl. 47: Arhitektura IP CA rešitve podjetja WideVine

5. PRIMERJAVA KLJUČNIH LASTNOSTI SISTEMOV DRM IN POGOJNEGA DOSTOPA

Osnovne naloge sistemov DRM in pogojnega dostopa so si zelo podobne. V ožjem pomenu gre v osnovi za nadzor dostopa do vsebin ter določanje pogojev uporabe. Sistemi DRM so že v osnovi namenjeni zaščiti vsebin preko omrežij IP, sistemi pogojnega dostopa pa se jim počasi približujejo. Tako lahko danes pri sodobnih sistemih pogojnega dostopa ločimo dve podzvrsti, ki sta med seboj povezani. To so klasični sistemi pogojnega dostopa (CA) ter pogojni dostop za zaščito vsebin, ki se prenašajo preko omrežij IP (IPCA). Pri sistemih IPCA gre največkrat za nadgradnjo klasičnega CA sistema.

Med obema pristopoma obstaja nekaj ključnih razlik. Prva se kaže v načinu prenosa vsebin. Pri klasičnih CA sistemih gre vedno za prenos tipa broadcast, kjer se ena vsebina oddaja množici potencialnih prejemnikov. Pri ostalih dveh predstavnikih so možni tudi drugi načini prenosa, kot je prenos na zahtevo (unicast) in celo zaščita lokalno shranjenih vsebin.

Glede vrste vsebin so sistemi DRM najbogatejši. Možna je zaščita praktično vseh oblik vsebin, vključno s programsko opremo. Sistemi pogojnega dostopa so omejeni na večpredstavne vsebine, kar v veliki večini predstavljajo video vsebine.

Format vsebin je pri sistemih DRM lahko skoraj poljuben. Potencialno od formata vsebin odvisni elementi so edino specifični sekundarni varnostni mehanizmi, kot je npr. vodni žig. Klasični sistemi pogojnega dostopa so omejeni na format MPEG-2, sistemi IPCA pa lahko podpirajo tudi MPEG-4.

Pomembna razlika se kaže pri načinu kontrole nad vsebinami in načinom oblikovanja pravil uporabe. Najširše možnosti so pri sistemih DRM, nekoliko bolj omejene pri sistemih IPCA ter najbolj omejene pri klasičnih sistemih pogojnega dostopa. V tem primeru je mogoča samo kontrola dostopa do vsebin glede na določene (omejene) pogoje.

Povratni kanal je za izmenjavo licenc potreben pri sistemih DRM in IPCA, pri klasičnih CA sistemih pa ne. To je hkrati prednost in slabost. Slabost je zato, ker je nabor možnih ključev za kodiranje in dekodiranje vsebin omejen, kar v primeru zlorab pomeni zamenjavo varnostnega dela terminalne opreme (i.e. pametne kartice).

Sistemi DRM so večinoma samo programske rešitve z opcijo strojne nadgradnje. Sistemi pogojnega dostopa skoraj vedno pri terminalni opremi vsebujejo tudi posebno dekodirno strojno opremo, kar bistveno poveča stopnjo varnosti sistema.

Kot zadnjo razliko bi izpostavil pristop k zaščiti vsebin. Sistemi pogojnega dostopa se osredotočajo zgolj na reševanje problemov digitalne luknje, medtem ko sistemi DRM skušajo reševati celoten problem.

Lastnost	DRM	Sistem CA	Sistem IPCA
vrsta prenosa	vse oblike	samo broadcast	vse oblike
vrsta vsebin	vse vrste vsebin, žive in na zahtevo (podatki, večpredstavne vsebine, programska oprema, dokumenti)	večpredstavne žive vsebine	večpredstavne vsebine, žive in na zahtevo
format vsebin	večina poznanih formatov, sistem DRM ni (pretirano) odvisen od formata vsebin	tipično MPEG-2	tipično MPEG-2, možni so tudi drugi formati (npr. MPEG-4)
način kontrole	izjemno širok nabor možnosti oblikovanja pravil uporabe	zelo omejen nabor možnosti oblikovanja pravil uporabe, tipično gre samo za kontrolo dostopa (dovoljen, ni dovoljen)	podobno sistemom DRM z določenimi omejitvami
povratni kanal	potreben	ni potreben (opcijski)	potreben
dekodirna terminalna oprema	tipično samo programska rešitev, možna kombinacija s posebno strojno opremo	tipično kombinacija programske in strojne opreme	tipično kombinacija programske in strojne opreme
problem digitalne/analogne luknje	rešuje oboje	rešuje probleme digitalne luknje	rešuje probleme digitalne luknje

Tab. 13: Primerjava pomembnejših lastnosti sistemov DRM in pogojnega dostopa

6. TERMINALNA OPREMA

6.1. Definicija in pomen

Pod izrazom *terminalna oprema* v splošni obliki lahko razumemo praktično vsako obliko kombinacije strojne (in programske opreme), ki uporabnikom omogoča dostop oz. uporabo različnih vsebin in storitev. Na področju telekomunikacij zasledimo nekoliko bolj natančno definicijo. Za ilustracijo sem izbral definicijo iz spletne enciklopedije, ki pravi:

Wikipedia,

»***Communications equipment at either end of a communications link, used to permit the stations involved to accomplish the mission for which the link was established.***

In radio-relay systems, equipment used at points where data are inserted or derived, as distinct from equipment used only to relay a reconstituted signal.

Telephone and telegraph switchboards and other centrally located equipment at which communications circuits are terminated.« [W47]

Na področju telekomunikacij ima izraz terminalna oprema podoben pomen, le da je povezan še s prenosom informacij. V okviru tega poglavja se bomo omejili na področje širokopasovne večpredstavne terminalne opreme.

6.2. Razdelitev

Na področju širokopasovne večpredstavne terminalne opreme danes zasledimo več tipičnih predstavnikov, ki so prilagojeni določenemu okolju in načinu uporabe. Razvrstimo jih lahko po več kriterijih, pri čemer sem izbral kriterija zmogljivosti in mobilnosti.

Sl. 48: Razdelitev večpredstavne terminalne opreme

Izbrani predstavniki so grupirani glede na tipični način dostopa do komunikacijskih omrežij. Pri prvih treh predstavnikih primarni način dostopa predstavljajo fiksna omrežja, pri zadnjih treh pa mobilna. Možne so seveda tudi kombinacije, npr. tablični računalnik ima poleg brezžičnih vmesnikov tudi žične (ima tako WLAN kot tudi Ethernet vmesnika).

6.2.1. Osebni računalnik

Osebni računalnik (ang. Personal Computer, PC) je izmed vseh naštetih predstavnikov najbolj poznan. Zasnovo je v 70. letih prejšnjega stoletja razvilo podjetje IBM, ko so skušali izdelati poceni alternativo takrat velikim in dragim računalniškim sistemom. Danes gre za najbolj razširjenega in dominantnega predstavnika na tem področju. Ključni razlogi za uspeh so bili odprtost, razširljivost in cenovna ugodnost platforme.

Osebni računalniki so se čez čas razvijali in dobivali kvalitativno nove predstavnike. Po obliki in namenu uporabe jih je mogoče razdeliti na:

- klasične, namizne modele,
- prenosne modele in
- specializirane, domače večpredstavne modele.

Navadni, klasični modeli se po obliki niso veliko spreminjali od prvih predstavnikov osebnih računalnikov. Po obliki so tipično v velikih ležečih ali pokončnih ohišjih. V splošnem so najbolj zmogljivi izmed vseh predstavnikov večpredstavne terminalne opreme, vendar zato najmanj prenosni ter energijsko zelo potratni.

Prenosni računalniki so v primerjavi z namiznimi samostojne naprave, ki vključujejo vnosne vmesnike (tipkovnica, miška, sledna tablica) in prikazovalno enoto (zaslon). Glavna poudarka sta mobilnost in energijska učinkovitost, kar omogoča visoko stopnjo avtonomnosti. Po zmogljivosti so tipično za odtenek manj zmogljivi od namiznih modelov, predvsem pri procesorski moči, grafični moči ter kapaciteti pomnilniških enot. Kljub temu vrhunski modeli v ničemer ne zaostajajo za namiznimi modeli.

Tretja podzvrst specializiranih večpredstavnih računalnikov je najmlajša in se pojavlja šele v zadnjem času. Ti predstavniki so znani tudi pod imenom HTPC (ang. Home Theater PC). Bistvena razlika se kaže v namenu in posledično obliki HTPC računalnikov. Njihov namen je v eni napravi zadovoljevati potrebe po dostopu do vseh večpredstavnih vsebin in storitev ter tako postati center domače zabave. Tipično sodijo v okolje t.i. dnevne sobe. Po obliki skušajo biti čim manj podobni klasičnim računalnikom in čim bolj podobni A/V napravam. Za upravljanje se primarno uporablja TV upravljalec in sekundarno računalniška tipkovnica, ki je brezžična. Po zmogljivosti so nekoliko manj zmogljivi od namiznih modelov, čeprav to ni tehnološka ovira in so v tem smislu lahko tudi povsem enakovredni. Razlogi za manjšo zmogljivost so predvsem v zagotavljanju čim manj motenj do uporabnikov v smislu prevelikih naprav, prekomernega segrevanja ter povzročanja hrupa. HTPC po funkcijah posegajo tudi na področja drugih predstavnikov terminalne opreme, predvsem TV komunikatorjev in igralnih konzol. Prikazovalna enota je lahko računalniški monitor ali pa TV sprejemnik.

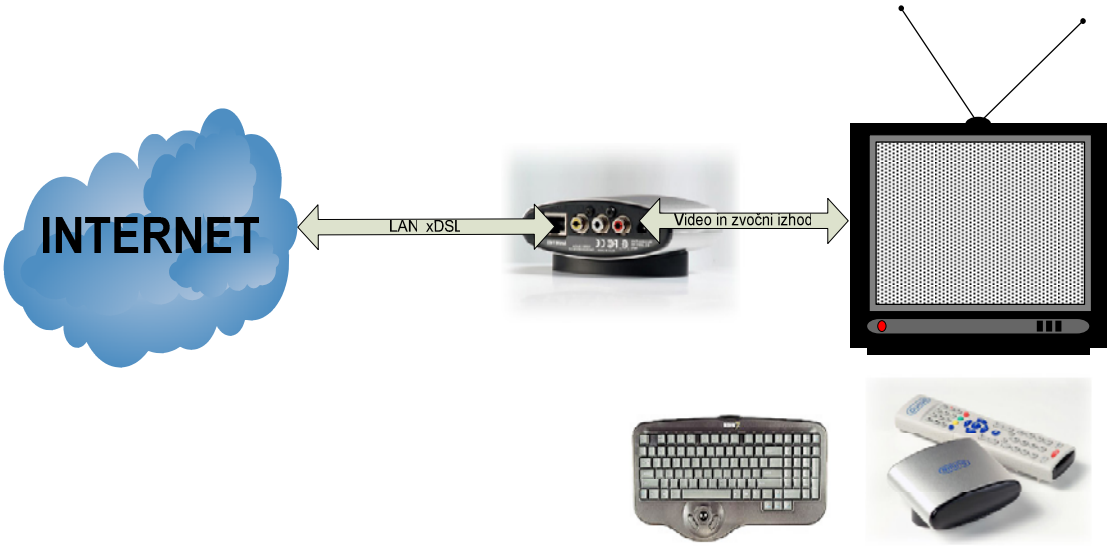
Opisane podzvrsti osebnih računalnikov se razlikujejo predvsem po obliki in stopnji mobilnosti ter deloma po zmogljivosti. Kljub temu po zmogljivosti med njimi ni več tako velikih razlik in je mogoče poiskati primerke izmed vsake podzvrsti, ki so si povsem enakovredni.

Po tehnoloških značilnostih platforma osebnih računalnikov napreduje z eksponentno rastjo. Še vedno namreč velja t.i. Moorov zakon, ki v originalni obliki pravi: »*Stopnja integracije v smislu števila transistorjev na enoto površine polprevodnika se mora podvojiti vsakih 18 mesecev.*«. To posledično pomeni tudi približno enako povečanje zmogljivosti. Zmogljivost sodobnih osebnih računalnikov je odvisna predvsem od procesorske zmogljivosti, osnovne plošče in veznega nabora, kapacitete delovnega pomnilnika in trajnih spominskih enot ter zmogljivosti dodatnih vmesnikov, predvsem grafičnega. Tako vrhunski osebni računalniki danes vsebujejo procesorje frekvenc do 4 GHz, do 16 GB delovnega pomnilnika ter 500 GB pomnilniškega prostora po kosu trdih diskov. Pri tem je seveda potrebno upoštevati dejstvo, da samo podatek o frekvenci procesorja še ne označuje celotne zmogljivosti procesorja. Vsi procesroji niso strukturno enaki in zato tudi po zmogljivosti ne. Pomemben podatek je zmogljivost/Hz.

Sl. 49: Klasični, namizni osebni računalnik (levo), prenosnik (sredina) in HTPC (desno)

6.2.2. TV komunikator

TV komunikator (ang. Set-Top-Box, STB) predstavlja novejšega predstavnike terminalne opreme, ki se je pojavil z razmahom IPTV storitev. Predstavlja most med računalniškim in televizijskim svetom. Na eni strani vsebuje klasične računalniške komunikacijske vmesnike (WLAN, Ethernet, modem xDSL) in na drugi televizijske (A/V vmesniki).



Sl. 50: TV komunikator ter njegova vloga in umestitev v okolje

Glavna naloga TV komunikatorja je zagotavljanje dostopa do vsebin in storitev IPTV platforme. Namenjen je vsem uporabnikom, predvsem tudi računalniško manj veščim in tistim, ki se računalnikov bojijo. Po obliki v ničemer ne spominja na osebne računalnike in je podoben A/V napravam oz. je celo bolj eksotičnih oblik (npr. Amino). Za upravljanje se v prvi vrsti uporablja TV upravljalec in za nekatere dodatne storitve tudi brezžična tipkovnica. Uporabniški vmesnik in sam način upravljanja sta čim bolj enostavna in podobna televizijskemu pristopu. Kot prikazovalna enota se uporablja izključno TV sprejemnik.

Po tehnološki zasnovi lahko TV komunikatorje razdelimo v dve skupini in sicer:

- na osnovi specializiranih komponent in na
- osnovi PC platforme.

V prvo skupino spada številčno največ predstavnikov TV komunikatorjev. Izdelani so na osnovi popolnoma specializiranih vezij, ki omogočajo visoko stopnjo integracije. Pogosto je celoten TV komunikator realiziran v fizično enem samem vezju. Glavne odlike tega pristopa so majhna poraba energije, posledično enostavno hlajenje ter majhna hrupnost naprave, visoka zanesljivost ter potencialno najpomembnejše – izjemna cenovno ugodnost. Strošek terminalne opreme pri IPTV platformi je namreč zaradi visokega števila uporabnikov največji strošek in večji celo tudi od stroška najbolj sofisticirane strežniške opreme. Slabosti, ki izhajajo iz specializirane zasnove, se kažejo v manjši zmogljivosti, omejenih funkcionalnostih ter slabih možnostih nadgradnje. Vgrajena programska oprema lahko hitro zastari, izvedba sodobnejših in strojno bolj zahtevnih storitev ni mogoča. Primer je npr. storitev prenosa videa, pri čemer nadgradnja

kompresijskega postopka lahko pomeni resno oviro (prehod iz MPEG-2 na MPEG-4 AVC).

Drugi tip TV komunikatorjev za strojno zasnovo uporablja PC platformo. Pri tem podeduje večino prednosti in tudi slabosti. Glavne prednosti so velika zmogljivost, razširljivost in nadgradljivost, slabosti pa potencialno manjša stabilnost in težje upravljanje. Po namenu in deloma obliki se prekrivajo s HTPC tipom osebnih računalnikov.

Po zmogljivosti TV komunikatorji na osnovi specializiranih komponent dosegajo frekvence do 600 Mhz, imajo 64 – 128 MB delovnega pomnilnika ter opcijsko (za storitve PVR) vgrajene dodatne pomnilniške kapacitete (trdi disk).

TV komunikatorji na osnovi PC platforme se po zmogljivosti uvrščajo v več razredov. Osnovni razred je na nivoju zmogljivejših predstavnikov iz prejšnje skupine in vsebuje procesorje reda 1000 Mhz – 1300 Mhz ter 128-256 RAM. Te procesorske enote so zelo osnovne in po zmogljivosti na 1 Hz precej slabše.

Srednji razred TV komunikatorjev je podoben srednjemu razredu klasičnih PC računalnikov. Vsebuje srednje zmogljive procesorje tipa Intel Celeron ali AMD Sempron frekvenc reda 1000 Mhz – 2400 Mhz.

Najvišji razred TV komunikatorjev je po zmogljivosti povsem enakovreden vrhunskim osebnim računalnikom, kar se odraža tudi na ceni.

6.2.3. Igralna konzola

Igralne konzole so primarno namenjene zabavi in igranju t.i. videoiger na TV sprejemniku. Zabavamo se seveda tudi z osebnim računalnikom, kjer lahko igramo že zelo dodelane in sofisticirane igre s čudovito 3D grafiko in prostorskim zvokom. Vendar imajo konzole pred njim nekaj pomembnih prednosti. Strojna oprema je znana, zato so lahko igre in aplikacije bolj dodelane in delujejo brez vsakršnih problemov, kar pri PC platformi ni slučaj. Konzole se navadno ne menjajo zelo hitro, zato isto napravo uporabljamo več let in hkrati uživamo podporo razvijalcev strojne (igralni dodatki in pripomočki) in programske opreme. V tem času se pri PC zamenja že nekaj generacij strojne opreme. Nadalje so pomembne postavke še enostavnost uporabe, razširjenost ter cena, saj le za delček zneska sodobnega računalnika dobimo zmogljivo igralno napravo, ki je uporabna še za kaj drugega kot le za igranje videoiger.

Kot vhodni medij se uporabljajo razni optični nosilci (CD, DVD) ali pomnilniške kartice. Vsebujejo zelo zmogljive zvočne in grafične procesorje (vektorske enote, DSP procesorje, MPEG dekoderje), ki se lahko kosajo z najsodobnejšimi osebnimi računalniki. V zadnjem času se v vse sodobne konzole vgrajuje možnost povratnega kanala preko mrežnega vmesnika ali analognega modema. Nekatere prav tako vsebujejo trdi disk (npr. X-Box).

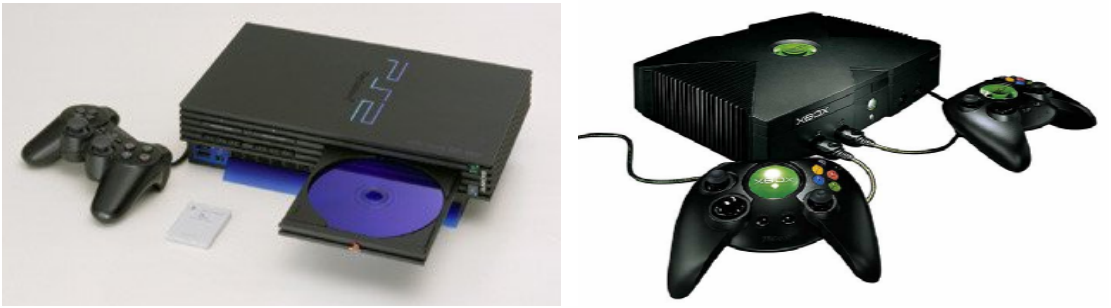
Igralne konzole so v primerjavi z osebnimi računalniki zelo razširjene predvsem v Aziji in Ameriki. Trg trenutno obvladujejo podjetja SONY, NINTENDO in MICROSOFT. Najbolj znani predstavniki so SONY PlayStation (PSX prodanih več kot 80 mil. kosov, PS2 prodanih tudi že več kot 30 mil. kosov), SEGA Dreamcast, Nintendo 64 in Gamecube ter Microsoftov X-Box. Proizvajalci jih ponavadi prodajajo pod ceno in ustvarjajo dobiček s prodajo iger in dodatkov. Za konzole so

na voljo številni dodatki, kot so razni emulatorji (posnemovalci), predvajalniki zvočnih MP3 datotek, predvajalniki video datotek, spletni brskalniki in drugi.

Trenutno najbolj zanimivi igralni konzoli sta SONY PlayStation 2 in Microsoft X-box. Poleg namenske programske opreme je nanje mogoče naložiti tudi prave operacijske sisteme, kot je npr. Linux (Sony PS2). Nabor možni aplikacij se močno poveča in posega tudi na področje IPTV.

Posebno zanimiv predstavnik je X-Box, saj temelji na PC osnovi. Vsebuje Intel Pentium III 733 MHz procesor, 64 MB RAM, trdi disk in neokrnjen nForce vezni nabor z integrirano grafiko (Geforce 3), zvokom in mrežnim vmesnikom. Kot operacijski sistem je uporabljeno Windows 2000 jedro, za večpredstavnost skrbi knjižnica DirectX 8. Prav to je stična točka s PC svetom, ki omogoča lahko prenosljivost z ostalimi Windows sistemi.

Danes smo priča prehodu na naslednjo generacijo konzol, ki se bo zgodil naslednje leto. Najbolj zanimivi predstavniki so nasledniki sedanjih konzol. To so Sony Playstation 3, Microsoft X-Box 360 in Nintendo Revolution. Konzole so v primerjavi z razvojem osebnih računalnikov bistveno bolj stalne. Trenutna generacija je bila v uporabi 5 let, kar je izjemno dolgo obdobje. Sodobne konzole so zato načrtovane za prihodnost in so po zmogljivosti bistveno boljše kot osebni računalniki. Zaradi splošnega trenda konvergence bodo tako zaradi tehnoloških odlik in cene hud konkurent osebnim računalnikom ter prav tako TV komunikatorjem na področjih zabave, internetnih in IPTV storitev.



Sl. 51: Igralni konzoli Sony PlayStation 2 (levo) in MS X-Box (desno)

6.2.4. Tablični računalnik

Tablični računalnik (ang. Tablet PC) je hibrid med prenosnim računalnikom in dlančnikom. Po zmogljivostih sodijo med prenosnike, po načinu vnosa pa med dlančnike. Po zmogljivosti in velikosti jih je mogoče razdeliti na:

- čiste tablične računalnike (ang. Slate TabletPC),
- hibridne tablične računalnike,
- posebne tablične računalnike in
- pametne zaslone (ang. Smart Display).

Čisti tablični računalniki v osnovi nimajo vgrajene tipkovnice in se krmilijo izključno preko elektronskega pisala. Možna je dodatna oprema v obliki »dock« postaje in zunanje tipkovnice.

Hibridni tablični računalniki imajo vgrajeno tudi tipkovnico in so v resnici klasični prenosniki z možnostjo krmiljenja z elektronskim peresom in obračanjem zaslona.

Posebni tablični računalniki so namenjeni za specialne namene in so lahko v bolj robustnih ohišjih.

Po zunanji obliki so tabličnim računalnikom podobni tudi t.i. pametni zasloni (ang. Smart Display). Po konceptu so približno enaki, vendar so strojno bistveno manj zmogljivi. Strojna zanova izvira iz dlančniške platforme, operacijski sistem pa je navadno Windows CE.

Tablični računalniki se upravljajo s pomočjo elektronskega peresa, ki lahko deluje na dva osnovna načina in sicer:

- aktivno preko elekromagnetnega principa in
- pasivno preko matrike, občutljive na dotik.

Prvi način je načeloma boljši, ker omogoča tudi brezkontaktno krmiljenje in je fizično vgrajen za LCD zaslonom. Pri drugem načinu se je potrebno zaslona dotakniti, matrika, občutljiva na dotik, pa je praviloma nameščena na zgornji strani LCD zaslona, kar poslabša vidljivost in čitljivost.

Sl. 52: Čisti tablični računalnik (levo) in hibridni (desno)

6.2.5. Dlančnik

Dlančnik (ang. HandHeld, Personal Data Assistant, PDA) je v osnovi pomanjšan tablični računalnik. Primarni način vnosa je uporaba elektronskega peresa, nekateri modeli imajo vgrajeno tudi tipkovnico. Najbolj znani dlančniki so narejeni na osnovi Palm OS operacijskega sistema ali pa na osnovi MS Windows CE operacijskega sistema.

Po zmogljivosti so povsem primerni za večino IPTV storitev. Najboljši predstavniki vsebujejo procesorje reda 600 Mhz, 128 MB delovnega spomina in možnost

razširitev preko vmesnikov PCMCIA. Nekateri modeli imajo dodatke v obliki večpredstavnih kamer in GPS sprejemnikov.

Dlančniki se uporabljajo v glavnem kot osebni organizator, večpredstavni predvajalnik in terminala za dostop do internetnih storitev. Prednosti so fizična majhnost, naraven način vnosa podatkov in odlična mobilnost ter povezljivost. Slabosti sta potencialna omejenost zaradi specializiranosti in omejena avtonomnost (poraba energije).

Sl. 53: Dlančnik Sony Clie na osnovi Palm OS (levo) in HP-Compaq Ipaq na osnovi MS Windows CE (desno)

6.2.6. Mobilni telefon

Osnovna funkcija mobilnega telefona je na začetku bila zgolj zagotavljanje prenosa govora in nekaterih zelo omejenih govornih in podatkovnih storitev. Sodobni mobilni telefoni, ki se označujejo s pridevnikom »pameten«, znajo bistveno več in so po naboru storitev praktično skoraj enaki prej opisanim predstavnikom večpredstavne terminalne opreme.

Sodobni pametni mobilni telefoni so po strojni zasnovi narejeni na podlagi namenskih komponent. S tega vidika so zelo robustni in varni. Zmogljivejši predstavniki, ki so označeni kot pametni, temeljijo na pravih operacijskih sistemih, kot sta Symbian in MS Windows CE Phone Editon. Pravi operacijski sistem omogoča neomejene možnosti razširitve in razvoj novih aplikacij. Po zmogljivosti najboljši modeli vsebujejo namenska procesorska vezja frekvenc reda 100 Mhz, 200 Mhz ali celo več ter 10 – 64 MB centralnega delovnega pomnilnika ter možnost razširitev preko dodatnih vmesnikov.

Trenutni trendi na tem področju so večpredstavne zmožnosti, vgrajeni digitalni fotoaparati in videokamere visokih ločljivosti ter celo možnost sprejema televizijskega signala. Nova in zanimiva tehnologija, ki povezuje televizijski in mobilni svet, je tehnologija DVB-H. Pri tem bo mogoče preko namenskega DVB-H omrežja (tipa broadcast) oddajanje televizijskih vsebin in storitev v visoki kakovosti

(z ozirom na fizične omejitve mobilnih telefonov). Povratni kanal bo potekal preko podatkovnih povezav preko mobilnih omrežij (GSM GPRS, UMTS).

Glavne odlike pametnih mobilnih telefonov so fizična majhnost, izjemna mobilnost in možnost povezave v globalna omrežja od praktično koderkoli. Slabosti so manjša strojna zmogljivost in potencialna omejenost zaradi specializiranosti.

Sl. 54: Pametni mobilni telefon Sony-Ericsson P900 (levo) Nokia 7710 z DVB-H podporo (desno)

6.3. Konvergenca na področju terminalne opreme

Na področju večpredstavne terminalne opreme bi izpostavil dve obliki konvergence – strojno in funkcionalno konvergenco.

S *strojno konvergenco* opisujemo pojav zlivanja terminalne opreme s fizičnega, strojnega vidika. Oblikovno se prej strogo ločeni predstavniki združijo in tako nastanejo kvalitativno nove vrste terminalne opreme. Kot primer naj služijo večpredstavni domači računalnik HTPC, TV komunikator in tablični računalnik. HTPC svoje računalniške korenine zakriva v podobi klasične A/V oblike naprav (avdio, video naprave, e.g. videorekorder). Ohranjajo se prednosti računalniške platforme (zmogljivost, razširljivost) pri drugačnem načinu uporabe. Spremeni se oblika, poenostavi se način upravljanja. Podobno velja za TV komunikatorje, ki pa so že osnovi načrtovani za potrebe izvajanja večpredstavnih storitev v okviru neračunalniškega domačega okolja.

Drug primer strojne konvergence so tablični računalniki, ki imajo svoje korenine pri prenosnikih in dlančnikih. Od prenosnih računalnikov so podedovali večjo zmogljivost in fleksibilnost, od dlančnikov pa bolj naraven način vnosa podatkov.

Funkcionalna konvergenca opisuje pojav združevanja na aplikacijskem nivoju. Nabor aplikacij in možnosti uporabe se poveča, prej ekskluzivne aplikacije so možne tudi na drugih vrstah terminalne opreme. Primere funkcionalne konvergence najdemo praktično pri vseh opisanih predstavnikih terminalne opreme. Glavno gonilo pri tem je večpredstavnost in uporaba večpredstavnih storitev. Dober konkreten primer so pametni mobilni telefoni, ki še pred nekaj leti niso omogočali kaj več od govornih storitev. Danes so v skladu s fizičnimi omejitvami (i.e. velikost zaslona) na področju večpredstavnosti enakovredni ostalim »velikim« bratom.

6.4. Zasnova sodobnega širokopasovnega terminala

Za osnovo sodobnega širokopasovnega večpredstavnega terminala sem izbral pristop na osnovi HTPC, ki temelji na PC platformi. Programski del sestavlja operacijski sistem (Windows, Linux) in posebna upravljavska večpredstavna aplikacija, ki neposredno komunicira z uporabnikom in omogoča izvedbo vseh želenih večpredstavnih storitev in podpira DRM funkcionalnosti. Gre za konvergenčno napravo, ki združuje funkcionalnosti osebnega računalnika, TV komunikatorja in igralne konzole, ter ima namen postati centralna enota hišne zabave.

6.4.1. Strojna zasnova

Predlagani večpredstavni širokopasovni terminal temelji na HTPC platformi od koder podeduje dobre in slabe lastnosti. Skušajo se maksimizirati dobre lastnosti v smislu velike zmogljivosti in razširljivosti, slabe, predvsem v smislu energijske neučinkovitosti in fizične velikosti, pa minimizirati.

Ne glede na specifično implementacijo, so naprave na osnovi PC platforme (velja tudi za TV komunikatorje) sestavljene iz funkcijsko enakih komponent. Glavno izvajalno breme nosi centralna procesorska enota, ki ji pomagajo specializirana vezja za dekodiranje in dekompresijo večpredstavnih elementov (video, zvok, slike), za delo z grafiko in zvokom ter za vhodno/izhodne operacije. Specializirana vezja so arhitekturno gledano nekoliko okrnjeni procesorji, ki so namenjeni točno določenim opravilom in so zato lahko bistveno učinkovitejša. Poznana so tudi pod izrazom signalni procesor (ang. Digital Signal Procesor, DSP).

6.4.1.1. Komponente

Ohišje

Ohišje fizično povezuje vse komponente med seboj ter določa zunanji izgled naprave. Tipična sestavna elementa ohišij sta tudi napajalnik in osnovni hladilni sistem.

Pri domačih večpredstavnih napravah ima ohišje bistveno večji pomen, kot pri klasičnih osebnih računalnikih. Oblika je lahko celo ključna za celoten uspeh naprave, kljub očitnim pomanjkljivostim, kar je primer pri TV komunikatorju podjetja Amino. Pomembni sta oblika in funkcionalnost. Po obliki mora biti prijetno in enostavno ter ne sme spominjati na klasični namizni osebni računalnik. Po funkcionalnosti so zaželeni dodatki v smislu dodatnih vmesnikov (USB, FW, bralnik za pomnilniške kartice, itd.) in večpredstavnih komponent (radijski sprejemnik, LCD zaslon, itd.) ter enostavne uporabe in dostopa do njih.

Drug pomemben element je napajalnik in hladilni sistem. Večpredstavni terminal sodi v domače okolje dnevne sobe in mora zato zagotavljati čim bolj zanesljivo in predvsem tiho delovanje ter oddajati čim manj toplote. Napajalnik mora biti zadosti zmogljiv (cca. 200 W – 300 W), hladilni sistem pa učinkovit. Vsem zastavljenim pogojem najbolj ustrezajo pasivni hladilni sistemi.

Primerne tehnologije hladilnega sistema so:

- popolnoma pasivni hladilni sistem na osnovi hladilnih reber,
- pasivni hladilni sistem z visoko kvalitetnimi in tihimi ventilatorji,
- hladilni sistem na osnovi tehnologije vročih cevk (ang. HeatPipe).

Od naštetih je najboljša tehnologija vročih cevk, ki omogoča premeščanje toplotne energije iz enega mesta (npr. CPU) na drugo (hladilna rebra) brez večjih izgub. Zaradi dislokacije toplotne energije je možna uporaba velikih pasivnih hladilnih elementov, kar omogoča popolnoma pasivno izvedbo hladilnega sistema, ki je prilagojen fizičnim zahtevam ohišja. Glavni generatorji toplote v sistemu so procesorska enota, grafični procesor, napajalnik, v manjši meri pa še vezni nabor in diskovne enote. Pri predlaganem sistemu je potrebno posebej hladiti le centralni procesor in napajalnik ter zagotavljati normalno ambientno delovno temperaturo v notranjosti naprave (idealno cca. 35 °C ali manj).

Sl. 55: Pasivni hladilni sistem z vročimi cevkami (izdelek podjetja Thermaltake)

Za potrebe predlaganega večpredstavnega terminala sta primerna dva tipa ohišij:

- večpredstavna ohišja in
- t.i. goli (ang. Barebone) sistemi.

Prvi tip ohišij je opremljen z večpredstavnimi dodatki, je nekoliko večjih fizičnih dimenzij, podoben A/V napravam in podpira večino klasičnih PC kompatibilnih komponent. V strojnem smislu je najbolj fleksibilen in cenovno primerljiv z boljšimi klasičnimi računalniškimi ohišji.

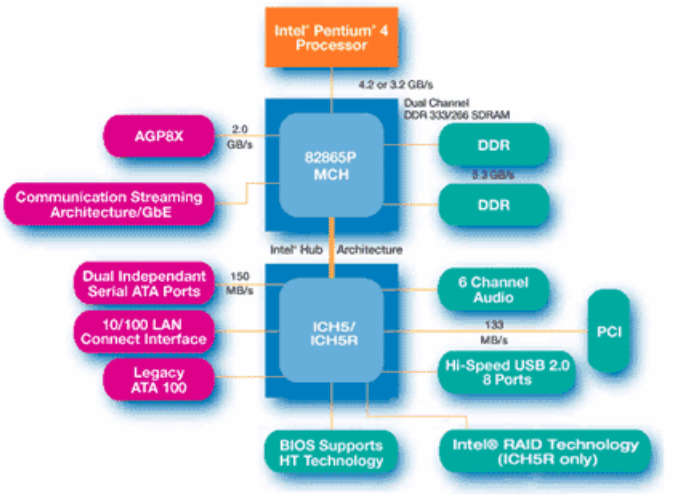
Drugi tip ohišij je že v osnovi načrtovan za potrebe domače večpredstavne terminalne opreme. Gre za fizično zelo majhna ohišja z večpredstavnimi dodatki (zaslon, TV tuner, daljinski upravljalec, itd.). Zaradi fizičnih omejitev je sestavni del ohišja tudi primerna matična plošča in sofisticiran napajalni in hladilni sistem, največkrat na osnovi tehnologije vročih cevk. Najbolj znani izdelovalci golih sistemov so podjetja Shuttle, Asus, MSI in druga.

Sl. 56: Primer večpredstavnega ohišja (levo: nmedia HTPC 100) in barebone ohišja (desno: Asus S-presso)

Matična plošča

Matična plošča logično povezuje vse komponente. Določa splošne značilnosti sistema v smislu usmerjenosti na določen tip centralnega procesorja ter je v največji meri odgovorna za stabilnost sistema.

Jedro matične plošče predstavlja vezni nabor (ang. Chipset), ki je fizično implementiran kot par integriranih vezij oz. kot samostojno integrirano vezje. Pri izvedbi v dveh vezjih se prvo imenuje severni most in drugo južni most oz. spojnik (ang. Hub). Naloge severnega mostu so povezava s procesorsko enoto, pomnilnikom, z zunanjim grafičnim vmesnikom (AGP) in z južnim mostom. Del severnega mostu je lahko tudi integriran grafični vmesnik. Južni most skrbi za vse ostale funkcije. Tipično so v njem implementirana sistemska vodila (PCI, PCI eXpress), vhodno/izhodni vmesniki (USB, FireWire), diskovni krmilnik in mrežni vmesnik. Zvočni vmesnik je prav tako lahko del južnega mostu. Del matične plošče je tudi BIOS (ang. Basic Input Output System), ki vsebuje osnovni zagonski program sistema.



Sl. 57: Primer arhitekture veznega nabora za platformo Intel Pentium 4 in naloge severnega (MCH) ter južnega (ICH) mostu

Procesorska enota

Če kot jedro sistema označimo matično ploščo, potem je centralni procesor srce sistema, ki v največji meri določa splošno strojno zmogljivost. Centralni procesor je odgovoren za izvajanje večine nalog, pri čemer mu pri specializiranih opravilih pomagajo koprocesorske enote (npr. za dekompresijo videa, grafični pospeševalnik, itd.).

Glavni izdelovalci procesorskih enot so:

- Intel:
  - družina Pentium,
  - družina Celeron,
  - družina Pentium-M.
- AMD:
  - družina Athlon,
  - družina Sempron.
- drugi:
  - Via Eden,
  - Motorola,
  - IBM.

Osnovno merilo zmogljivosti je notranji takt procesorskega jedra, ki pri najzmogljivejših predstavnikih dosega frekvence do 4 Ghz. Sam podatek o taktu ne daje povsem točne informacije o zmogljivosti, saj vsi procesorji niso enako učinkoviti. Prav tako je pomemben podatek o učinkovitosti (zmogljivost na 1 Hz). Družini Intel Pentium in AMD Athlon spadata med bolj zmogljive predstavnike, primerne za računalnike višjega razreda. Družini Intel Celeron in AMD Sempron sta komplementarno primerni za cenejše in manj zmogljive računalnike. Za ilustracijo učinkovitosti naj navedemo, da je procesor AMD Athlon pri taktu 2 Ghz približno enako zmogljiv kot procesor Intel Pentium 4 pri taktu 3 Ghz.

Zelo zanimivi so procesorji Intel Pentium M (Centrino platforma), ki so primarno namenjeni uporabi v prenosnikih. So izjemno varčni in v primerjavi z namiznimi modeli bistveno bolj zmogljivi. Procesor Pentium-M pri taktu 1.5 Ghz je približno enako hiter kot Pentium 4 pri taktu 2.5 Ghz. Pentium-M procesorji so zaradi navedenih prednosti zelo primerni za predlagani večpredstavni terminal.

Pomnilniške enote

V grobem ga delimo na tri dele. RAM (Random Access Memory) je hiter delovni pomnilnik, namenjen hrambi tekočih aplikacij in podatkov. Po izklopu napajanja se vsebino izgubi. V ROM (Read Only Memory) je trajno shranjen zagonski program (BIOS ali celoten OS – Windows CE, Linux). Na željo uporabnika ga je možno prepisati z novejšo različico programske opreme (FLASH ROM, EEPROM). Tretji tip predstavljajo masovni pomnilniški nosilci, kot so trdi disk, diskete, optični in magnetni mediji. Na njih hranimo vse ostale podatke in programe, ker so najbolj zmogljivi in glede na kapaciteto cenovno najbolj ugodni. Po hitrosti je najhitrejši predpomnilnik – posebno hiter RAM v CPU, sledi delovni pomnilnik (RAM) in nazadnje še masovni mediji. Povprečna današnja velikost se giblje med 512 in 1024 MB za delovni pomnilnik RAM in med 160 in 250 GB za trdi disk.

Osnovni parametri pomnilniških enot so dostopni čas, hitrost prenosa in kapaciteta.

Grafični in zvočni vmesnik

Skrbita za generiranje video in avdio signala. Sodobne igre in multimedijske aplikacije, kjer se prepletajo video, statične slike, grafični učinki, zvok ter tekst, zahtevajo precej zmogljive izvedbe. Poseben problem predstavlja zajemanje in predvajanje videa v polni ločljivosti in hitrosti, ki je rešen s pomočjo namenskih vezij (samostojna ali del grafičnega procesorja). Ponavadi je uporabljen kateri izmed MPEG družine kodekov (MJPEG, MPEG-2, MPEG-4). Posebnega pomena je t.i. prekrivni način (overlay), kjer za prikaz, raztegovanje in pretvarjanje med barvnimi prostori skrbi grafični vmesnik. Za prikaz na TV prikazovalnih enotah mora grafični vmesnik podpirati t.i. TV izhod, kjer se video signal prilagodi in kodira v TV obliko (standard PAL za Evropo).

Naloga zvočnega vmesnika je generacija in obdelava zvočnih signalov. Podpirati mora hkratno predvajanje več virov glasbe (vgrajen mešalnik), zvočne učinke, sodobno sintezo zvoka z zvočnimi tabelami (MIDI) in zmožnost predvajanja t.i. 3D zvoka, kjer lahko posamezne vire postavimo kjerkoli v prostoru. Poleg stereo (dva kanala) načina mora podpirati tudi večkanalni filmski zvok, tipično Dolby AC3 5.1 (stereo spredaj in zadaj, center ter bas).

Razširitveni vmesniki

V to skupino uvrščamo vse ostale vmesnike, ki razširjajo osnovne funkcionalnosti. Pri večpredstavnih terminalih je pomembna razširitev s TV sprejemniškimi karticami (vmesniki). Le-te omogočajo zajem, obdelavo in prikaz TV signalov. Boljše izvedenke omogočajo tudi strojno zajemanje in kompresiranje (tipično v format MPEG-2) video signala v digitalni obliki na pomnilniške enote. Nekateri boljši TV sprejemniški vmesniki imajo za kompresijo specializirana DSP vezja, ki razbremenijo glavni procesor. Funkcionalnost se na ta način razširi v smislu funkcij digitalnega snemanja video vsebin ter zakasnjenega predvajanja (ang. Time Shifting). Pri zakasnjenem se žive vsebine vseskozi shranjujejo na disk in uporabnik ima možnost pavziranja živega programa. Ob nadaljevanju se program prične predvajati na mestu, kjer je prišlo do prekinitve. Storitev je zanimiva, ker je možna nad živimi vsebinami.

Komunikacijski vmesniki

Predlagan večpredstavni terminal je vpet tako v računalniško kot tudi televizijsko okolje. Za povezavo s širokopasovnimi omrežji se uporabljajo vmesnik Ethernet (10/100/1000) in brezžični WLAN vmesniki (802.11b/g z 54 Mbit/s pasovne širine). Za povezavo s televizijskim svetom skrbijo analogni A/V vmesniki in digitalni (DVI, HDMI) vmesniki.

Krmilne enote

Klasično tipkovnico iz računalniškega sveta nadomestita daljinski upravljalec in daljinsko namizje, sestavljeno iz prilagojene tipkovnice z vgrajeno sledno ploščico ali miško in (po želji) zunanje miške. Povezava poteka preko IR (Infra Red) vmesnika ali preko radijske zveze, kar je boljše. Tipkovnica je navadno opremljena z dodatnimi gumbi za krmiljenje večpredstavnih aplikacij (video, zvok, spletne aplikacije…), dodatna miška pa naj temelji na optični tehnologiji.

Prikazovalne enote

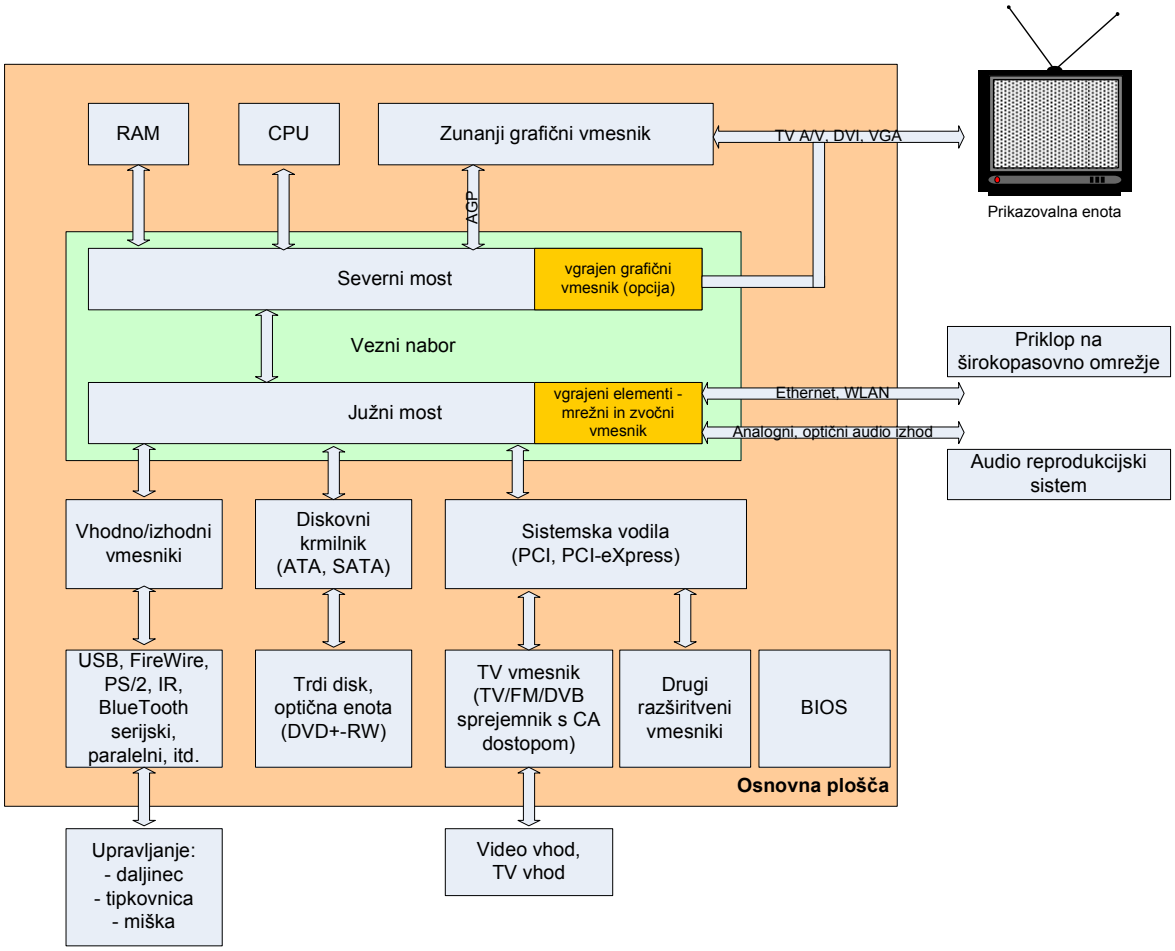
Za prikaz so primerne naslednje enote:

- računalniški svet – računalniški monitor,
- televizijski svet:
    - klasični TV sprejemnik na osnovi CRT tehnologije,
    - TV sprejemnik na osnovi LCD ali plasma tehnologije,
    - digitalni projektor (LCD, DLP).

Med prikazovalnimi enotami so zaradi cenovne ugodnosti najbolj razširjeni klasični televizijski sprejemniki na podlagi CRT tehnologije. Povezava med terminalno opremo je izvedena preko analognega TV video izhoda (kompozitni, S-VHS, RGB). Pri tem zaradi tehničnih omejitev in specifike prikaza na TV zaslonu pride do izgube informacije in popačitev. Sodobnejše LCD in plazma prikazovalne tehnologije so v tem pogledu bolj podobne računalniškemu načinu prikaza slike ter bistveno boljše. LCD in plazma zasloni so diskretni, brez geometrijskih napak ter uporabljajo digitalni način prenosa slike (e.g. VGA, DVI, HDMI). Možen je tudi višji nabor ločljivosti, ki sega od klasične televizijske (PAL – 720x576i oz. NTSC – 720x480i) do ločljivosti televizije visoke definicije (HDTV – 1280x720p, 1920x1080i). Prikaz na kvalitetnih plazma in LCD televizijskih sprejemnikih ter LCD oz. DLP računalniških projektorjih je brezhiben in primeren kot popoln nadomestek računalniškega monitorja.

6.4.1.2. Arhitektura

Vse komponente so med seboj povezane preko osnovne plošče. Centralni procesor je odgovoren za večino opravil (izvajanje operacijskega sistema in aplikacij). Grafični vmesnik je odgovoren za generacijo in procesiranje slikovnega signala ter pomaga tudi pri dekompresiji videa. Za generiranje in obdelavo zvoka skrbi zvočni vmesnik. Povezava s širokopasovnimi omrežji poteka preko Ethernet omrežnega vmesnika. Klasičen televizijski signal se v sistem prenese preko TV vmesnikov. Le-ti omogočajo prikaz, dekodiranje (v primeru zaščitenih DVB programov) in strojno kompresijo TV programov. Če sistem vsebuje več TV vmesnikov, je mogoče hkrati snemati oz. spremljati več televizijskih programov. Za shranjevanje vsebin skrbijo pomnilniški mediji v obliki trdih diskov in optičnih zapisovalnih enot (DVD +-RW). Strojno arhitekturo prikazuje slika št. 58.



Sl. 58: Strojna arhitektura

6.4.2. Programska zasnova

Po programski zasnovi ločimo dva osnovna dela in sicer operacijski sistem ter aplikacije. Primerni operacijski sistemi so družina Windows (Windows XP, Windows Media Center in Windows CE) in Linux. Od naštetih sta strojno manj zahtevna Windows CE in nekatere okrnjene distribucije Linux OS.

Na aplikacijskem sloju sta za potrebe upravljanja večpredstavnih storitev primerna Windows Media Center in namenske aplikacije. Operacijski sistem Windows Media Center temelji na operacijskem sistemu Windows XP, ki je že v osnovi načrtovan za to nalogo in vsebuje primeren in prirejen uporabniški vmesnik. Druga možnost je uporaba klasičnega operacijskega sistema in namenskih aplikacij, ki služijo v vlogi nadzorne aplikacije za dostop do vsebin in storitev ter imajo primeren uporabniški vmesnik.

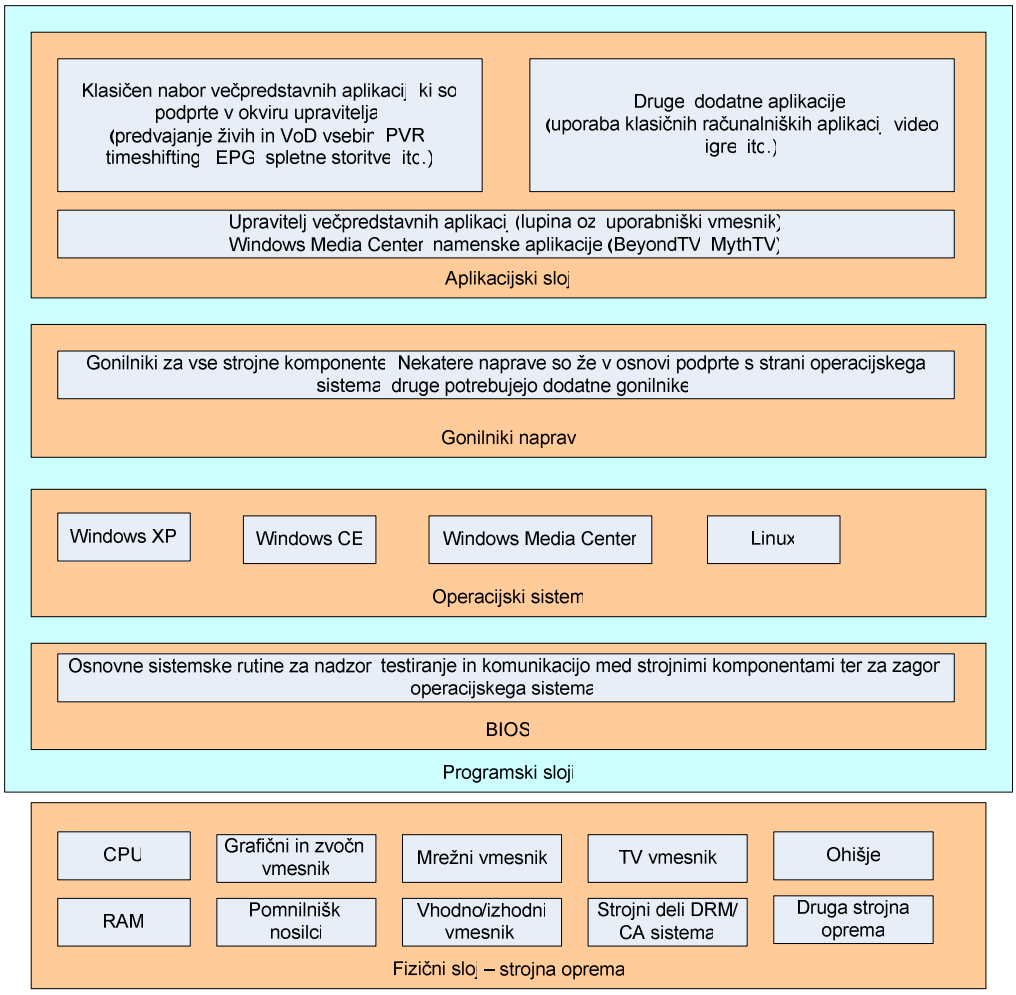
Logično arhitekturno zgradbo sestavlja 5 slojev. Najnižji je namenjen vsej fizični in strojni opremi, vsi ostali pokrivajo programsko opremo. Tak pristop omogoča neodvisnost programskih rešitev od strojne izvedbe naprave.

Drugi sloj predstavlja osnovni zagonski sistem BIOS, ki med seboj povezuje strojno opremo z višjimi sloji (operacijskim sistemom).

Sledi sloj operacijskega sistema, ki gradi izvajalno okolje za aplikacije. Tako kot strojna oprema v največji meri vpliva na strojno zmogljivost sistema, operacijski sistem vpliva na programske zmožnosti sistema. Pri specializiranih in okrnjenih napravah (e.g. TV komunikatorji na osnovi specializirane platforme) se uporabljajo okrnjene verzije OS, ki omogočajo samo osnovne funkcije (Windows CE, okrnjene distribucije Linux). Pri zmogljivejših sistemih je možna uporaba pravih operacijskih sistemov (Windows, Linux), kar omogoča veliko fleksibilnost in polno funkcionalnost, kot jo poznamo pri osebnih računalnikih. Ne glede na izbran OS je zaželeno, da naprava kar najhitreje preide v stanje pripravljenosti za delo. Za to je primerna uporaba naprednejših načinov zagona (hibernacija na disk oz. RAM), optimizacija OS (odstranitev nepotrebnih komponent) in zagon iz hitrejših medijev.

Sloj gonilnikov je umeščen med sloja operacijskega sistema in aplikacij. Naprave, ki neposredno niso podprte s strani OS, potrebujejo za pravilno delovanje dodatno programsko podporo – gonilnik. Le-ti predstavljajo vez med OS in temi napravami.

Najvišji nivo je namenjen uporabniškim aplikacijam, ki predstavljajo neposreden uporabniški stik s celotnim sistemom. Posebnega pomena je program UPRAVITELJ APLIKACIJ oz. lupina sistema, ki vse aplikacije in storitve povezuje v konsistentno celoto in predstavlja uporabniški vmesnik. Biti mora enostaven za uporabo, dovolj odziven (hiter) in zmogljiv. Mogoče ima še največji pomen, saj se z njim uporabnik sreča že takoj ob vklopu naprave in ga vseskozi uporablja.



Sl. 59: Logična arhitektura

6.4.3. Uporabniški vmesnik

Uporabniški vmesnik (ang. User Interface) - UI je s stališča uporabnika najpomembnejši del celotnega sistema. Razdelimo ga lahko na dve komponenti:

- strojni uporabniški vmesnik in
- programski uporabniški vmesnik.

V strojni del UI prištevamo vse fizične komponente, ki služijo za upravljanje in nadzor terminalne opreme. Sem tipično spadajo daljinski upravljalec, brezžična tipkovnica, miška in drugi dodatki (npr. igralni pripomočki). Nenazadnje tudi sama fizična naprava predstavlja fizični uporabniški vmesnik. Za televizijsko okolje je najpomembnejši daljinski upravljalec, ki mora imeti funkcijo primarnega načina upravljanja z napravo. Njegovi obliki in zasnovi je potrebno posvečati veliko pozornosti s ciljem doseči funkcionalen in predvsem preprost izdelek. Nekaj primerov dobrih in slabih (po mojem mnenju) predstavnikov prikazuje slika št. 60.

Sl. 60: Primeri daljinskih upravljalcev za IPTV storitve (levo) in skica zasnove (desno)

Prikazana je skica moje zasnove primernega daljinskega upravljalca za IPTV storitve. Menim, da je večino opravil mogoče izvesti z smernim križem, barvnimi tipkami ter nekaterimi dodatnimi tipkami. Numerični del je opcija.

Programski del UI predstavlja UI aplikacija. Pri tem je najpomembnejši UI upravitelja aplikacij. Posebno problematično okolje predstavlja klasičen televizijski sprejemnik na CRT osnovi. Izgled UI mora biti posebno načrtovan, pri čemer je nekaj glavnih vodil in omejitev:

- **omejena ločljivost prikaza** – PAL: 720x576i,
- **omejen prikaz barvnih vzorcev** – nekatere barvne kombinacije so izjemno slabo vidne (rdeča barva), priporočena je uporaba vsebin (teksta) v svetlejših

odtenkih na temnejši podlagi (zelo primerna kombinacija je bel ali rumen tekst na temno modri podlagi), prepodrobne slikovne vsebine niso zaželene.

- **velikost in oblika teksta** – tekst mora biti v primerno veliki tipografiji, pri čemer je pomembna tudi oblika. Najbolj znana tipografija je tipa Tiresias.

Sodobnejše tehnologije prikaza teh omejitev nimajo oz. niso tako izrazite. V to skupino spadajo LCD in plazma TV sprejemniki ter digitalni projektorji.

Nekaj najbolj znanih upraviteljev večpredstavnih aplikacij je MS Windows Media Center, MythTV in BeyondTV. Prednost zadnjih dveh predstavnikov je v nevezanosti na določen operacijski sistem (delujeta v Windows OS in Linux OS). Uporabniški vmesniki so enostavni in načrtovani v skladu z omejitvami prikaza na CRT TV zaslonih. Nekaj primerov izgleda (UI) je prikazanih na sliki št. 61.

Sl. 61: Uporabniški vmesnik Windows Media Center 2005 (zgoraj) in BeyondTV spodaj)

6.5. Primer terminalne opreme

Kot primer zanimivega in zelo uspešnega predstavnika terminalne opreme s področja TV komunikatorjev sem izbral TV komunikator AMINO AmiNET 110, podjetja Amino Communications. [W41]

Po strojni zasnovi gre za predstavnika TV komunikatorjev na osnovi specializiranih komponent. V celoti temelji na DSP procesorju IBM PowerPC (frekvence reda 400 Mhz), ki je odgovoren tudi za dekompresiranje video signala. Vsebuje omejen nabor vmesnikov, širokopasovni 10/100 Mbit Ethernet vmesnik in A/V televizijske vmesnike (cinch, scart). Za upravljanje služita daljinski upravljalec in tipkovnica na IR principu prenosa informacij.

Po programski opremi temelji na okrnjeni in specializirani različici Linux operacijskega sistema z dodatnimi aplikacijami, od katerih je najbolj pomemben spletni brskalnik (podjetja Ant Fresco). Funkcionalno je Amino TV komunikator zelo omejena naprava. Glavni namen je uporaba video storitev (video v živo, video na zahtevo) in omejena uporaba spletnih storitev. Video predvajalnik podpira le video v formatu MPEG-2, spletni brskalnik pa je zelo omejen.

Opisani TV komunikator je zanimiv primer, ker je kljub omejenosti izredno uspešen. Razlogi za njegov uspeh so:

- zelo prijetna zunanja oblika in fizična majhnost naprave,
- prijazen daljinski upravljavec,
- zanesljivo delovanje,
- cenovna ugodnost.

Amino TV komunikatorji se uporabljajo v konkretnih komercialnih IPTV postavitvah, med drugim tudi pri nas v okviru rešitve SiOL TV.

Sl. 62: Amino AmiNET110

6.6. Praktični del

Praktični del se osredotoča na dva segmenta in sicer na specifikacijo konkretnega večpredstavnega terminala in na postavitev ter preizkus realnega sistema DRM in njegovih funkcionalnosti.

6.6.1. Zasnova večpredstavnega terminala

V okviru konkretne specifikacije terminala so v tabeli št. 14 orisani trije različni sistemi. Sistem »ZMOGLJIVI – MSI« je primer t.i. golega sistema. Temelji na večpredstavnem ogrodju podjetja Microstar International [W40], ki ga sestavlja ohišje z večpredstavnimi dodatki, napajalnik, hladilni sistem ter osnovna plošča, ki ima večino komponent že integriranih. Sistem temelji na Intel Pentium 4 procesorju, Nvidia grafičnemu vmesniku ter TV vmesniku. Posebnosti sistema so vgrajena podpora daljinskemu upravljalcu ter poseben »InstantON« način delovanja. V slednjem naprava deluje kot radijski sprejemnik in glasbeni predvajalnik brez potrebe po popolnem zagonu sistema. Tehnično je to rešeno z dodatki na matični plošči ter uporabo posebne namenske Linux distribucije. S programskega stališča na predlaganem sistemu lahko tečejo različni operacijski sistemi in aplikacije. Izbrana operacijska sistema sta Windows XP in Windows Media Center.

Sistem »ZMOGLJIVI – Shuttle« [W39] je podoben prejšnjemu sistemu pri čemer je že v osnovi načrtovan kot platforma za Windows Media Center operacijski sistem. Temelji na večpredstavno opremljenem ohišju in matični plošči podjetja Shuttle. Posebnost je procesor Intel Pentium M, ki je predstavnik procesorjev mobilne platforme. Je izredno energijsko učinkovit in zmogljiv. Celoten sistem deluje kot A/V naprava in vse vgrajene komponente so lepo zaokrožene in podrejene temu cilju. Primarni operacijski sistem je Windows Media Center.

Sistem »ENOSTAVNI – VIA« [W42] je manj zmogljiv in temelji na mini ITX platformi podjetja VIA, ki jo sestavlja VIA EDEN matična plošča ter x86 kompatibilen VIA C3 procesor. Glavne posebnosti so izjemno majhne dimenzije plošče ter posledično ohišja, majhna poraba energije (še manj kot Pentium M) ter izjemno visoka stopnja integracije.

Vse predlagane zasnove so primer strojne konvergence in posegajo na področja uporabe v vlogi osebnega računalnika, TV komunikatorja ter igralne konzole. Zmogljivejši zasnovi sta primerni za vse vrste računalniških, televizijskih in IPTV ter igralnih storitev. Omejitev enostavnejšega sistema je predvsem manjša strojna zmogljivost, kar nekoliko okrni uporabnost pri predvajanju in shranjevanju zahtevnejših video vsebin ter uporabi zahtevnejših zabavnih aplikacij (i.e. 3D iger).

Področja uporabe:

- Internetne storitve:
  - brskanje po svetovnem spletu (WWW),
  - elektronska pošta,
  - dostop do novic (NewsGroup).

- Večpredstavne storitve (televizijske, IPTV):
  - vsebine na zahtevo,
  - vsebine v živo,
  - EPG,
  - PVR,
  - uporaba naprave kot večpredstavni predvajalnik vsebin vseh vrst formatov.
- Uporaba PC aplikacij.
- Zabava – računalniške (video) igre in emulacija (posnemanje) drugih igralnih sistemov.

KOMPONENTA	SISTEM		
	ZMOGLJIVI-MSI	ZMOGLJIVI-Shuttle	ENOSTAVNI-Via
ohišje	MSI MEGA 865 202mm (w) x 151mm (h) x 320mm (d)	Shuttle XPC M1000, 442mm (w) x 78mm (h) x 350mm (d)	ITX ohišje majhne dimenzije reda cca. 250mm (w) x 65mm (h) x 200mm (d)
matična plošča	namenska MSI, vezni nabor: Intel 865G+ICH5 PCI in AGP razširitveno mesto	namenska Shuttle, vezni nabor: Intel 915PM+ICH6M	VIA EPIA x86 platfoma, mini ITX (170mm x 170mm), VIA vezni nabor PCI razširitveno mesto
CPU	Intel Pentium4 2.66 HT, Prescott	Intel Pentium M 740 (1.73 GHz, 2 MB cache)	VIA C3, 1.3 Ghz
RAM	512 MB DDR	512 MB DDR	512 MB DDR
grafični vmesnik	integriran Intelov 865G, dodatni samostojni Nvidia Geforce 6600 ali ATI x600	samostojni Nvidia Geforce 6600	integrirana VIA z MPEG-2 strojnim dekoderjem
zvočni vmesnik	integriran, 5.1 kanalni	Creative Soundblaster Live! 24-bit HD7.1	integrirana VIA, AC'97
TV vmesnik	Hauppage, Leadtek, Asus, MSI s strojnim MPEG-2 enkoderjem	AverMedia s strojnim MPEG-2 enkoderjem	Hauppage, Leadtek, Asus, MSI s strojnim MPEG-2 enkoderjem
trajni pomnilnik	ATA HDD, 160-250 GB	SATA HDD, 250GB	ATA HDD, 160-250 GB
I/O vmesniki	USB, FW, VGA, DVI, kompozitni TV, avdio (analogni in digitalni), IR, PS/2, paralelni	USB, FW, VGA, DVI, kompozitni TV, avdio (analogni in digitalni), IR	USB, FW, VGA, DVI, kompozitni TV, avdio (analogni in digitalni), IR (v okviru TV vmesnika)
LAN	integriran 10/100 Ethernet, 802.11b/g WLAN, 56k modem	integriran 10/100/1000 Ethernet, 802.11b/g WLAN	integriran 10/100 Ethernet
nadzor	IR daljinec, daljinsko namizje	IR daljinski upravljalec in tipkovnica z vgrajeno miško	IR daljinec, daljinsko namizje
dodatki, posebnosti	bralnik pomnilniških kartic, ohišje ima LCD zaslon in samostojne funkcionalnosti radija in glasbenega predvajalnika (CD, MP3)	bralnik pomnilniških kartic	izjemno fizično majhne dimenzije sistema, majhna poraba energije, pasivno hlajenje komponent, visoka stopnja integracije (večina komponent je integriranih na osnovni plošči)
OS	Windows XP z MSI Media Center aplikacijo, Windows Media Center Linux	Windows Media Center	Windows XP, Linux

Tab. 14: Specifikacija predlaganih HTPC sistemov

Sl. 63: Izgled sistemov MSI (levo) in Shuttle (desno)

6.6.2. Laboratorijska postavitev sistema DRM

Za preizkus sistema DRM in njegovih funkcionalnosti sem izbral MS IPTV in MS DRM platformo. Gre za tipičnega predstavnika komercialne rešitve. Preizkusil sem zadnjo, 10. različico sistema.

Pri predlaganih specifikacijah sistemov je na programskem sloju zaradi povezave z izbranim DRM sistemom predlagan tudi Windows XP oz. Media Center operacijski sistem, ki vsebuje potrebne MS DRM uporabniške komponente (MS Media Player z DRM agentom).

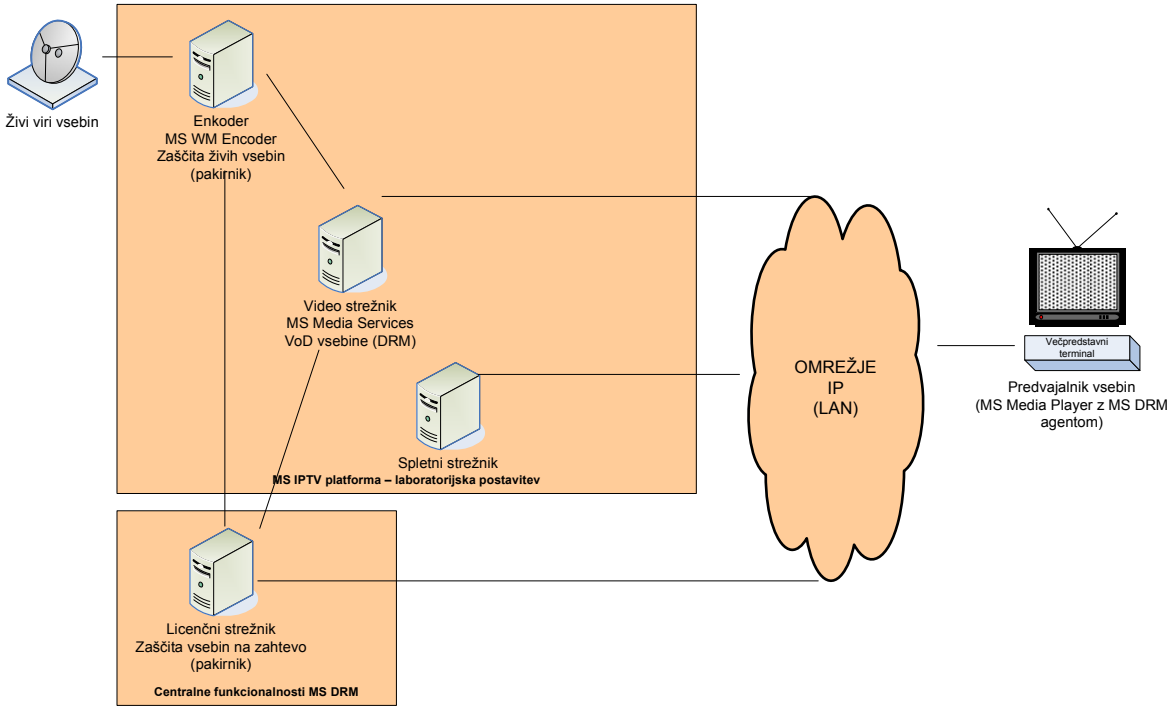
MS DRM sistem je del MS IPTV platforme, ki jo na strežniški strani sestavljajo enkoder vsebin, večpredstavni strežnik ter spletni strežnik in na odjemalski strani večpredstavni terminal z MS Media Player predvajalnikom. Enkoder je namenjen obdelavi in pripravi vseh vrst večpredstavnih vsebin, da so primerne za vključitev v MS IPTV platformo. Posebno vlogo ima pri živih vsebinah, kjer priprava poteka v realnem času. Vloga večpredstavnega strežnika je hranjenje in strežba vsebin (tudi zaščitenih) na zahtevo ter delovanje v vlogi posrednika v primeru živih vsebin. Spletni strežnik gosti splošne spletne aplikacije.

MS DRM v trenutni obliki temelji samo na programskih elementih. V osnovi gre za precej enostavno implementacijo, ki temelji na nekaj zaprtih in zavarovanih programskih knjižnicah – API (ang. Application Programming Interface). Te so osnova za vse DRM funkcije. Microsoft je zelo dejaven tudi na področju iniciative Trusted Computing, kjer sodeluje z drugimi podjetji (npr. Intel), ki se ukvarjajo z razvojem strojnih varnostnih komponent. V prihodnosti lahko pričakujemo tudi korake v tej smeri.

DRM del sestavlja samostojna komponenta v obliki licenčnega strežnika ter komponente, ki so del ostalih elementov (enkoder, večpredstavni strežnik, odjemalec). Licenčni strežnik predstavlja jedro sistema in nastopa v več vlogah. V primeru ponudnika storitev, ki ima sistem MS DRM, omogoča oblikovanje licenc ter zaščito (kriptiranje) vsebin na zahtevo. V primeru uporabnikov zaščitenih vsebin skrbi za interakcijo z njihovo terminalno opremo ter za izdajanje licenc. Pri vsebinah v živo se te fizično sproti zaščitijo na enkoderju vsebin, pri čemer se upošteva pravila uporabe, kot so določena na licenčnem strežniku.

Na uporabniški strani za dekriptiranje in delo z licencami skrbi DRM agent v okviru MS Media Player predvajalnika vsebin. DRM agent je izveden programsko in je zaščiten (kriptiran). Njegove funkcije lahko uporablja le certificirana programska oprema. To je pomembno, ker je DRM agent odgovoren za spoštovanje pogojev uporabe skladno z licenco ter ima dostop do občutljivih informacij (dekriptirnih ključev).

Arhitekturo testne laboratorijske postavitve ilustrira slika št. 64. Prikazana je logična postavitev komponent in odnosov med njimi. Fizično so vse komponente povezane v omrežje na osnovi protokolnega sklada TCP/IP. Kot dostopovna tehnologija je izbran Ethernet.



Sl. 64: Arhitektura laboratorijske postavitve sistema MS DRM

Oba scenarija, to je zaščita živih vsebin ter vsebin na zahtevo, smo praktično preizkusili. Ne glede na vrsto vsebin se na licenčnem strežniku najprej oblikujejo pravila uporabe. Pri vsebinah na zahtevo se sama zaščita vsebin nato izvede fizično na licenčnem strežniku z uporabo programskih skript in knjižnic. Sam postopek zaščite je nestandarden (skrit) in zelo hiter. Rezultat je kriptirana oblika vsebine, ki po količini podatkov ni bistveno daljša od originala (dolžina datoteke). Rezultati so razvidni iz tabele št. 15. Zaščiteno vsebino je potrebno le še prenesti na večpredstavni strežnik, kjer se obravnava kot vsaka druga vsebina.

V primeru živih vsebin se na licenčnem strežniku kreira poseben profil, ki se prenese na enkoder vsebin ter uporabi pri njihovi zaščiti. Sam postopek zaščite poteka v realnem času in za izvajanje ne zahteva veliko strojnih sredstev.

V okviru testiranja smo pripravili, kompresirali in zaščitili nekaj video vsebin, v različnih kvalitetah ter dolžinah. Kot pogoj uporabe je bilo določeno omejeno število predvajanj. Za uporabo vsebin je bila potrebna veljavna licenca, ki jo je bilo

potrebno po izteku pogojev obnoviti. Primer legalno predvajane vsebine prikazuje slika št. 65, uporabniške razlage pogojev (preostalih) uporabe pa slika št. 66.

Vsi dodatni postopki zaščite v nobenem primeru niso vplivali na izhodno kvaliteto vsebine. Uporaba in delo z licencami sta z uporabniškega stališča neproblematična in relativno prijazna. Dodatno dekriptiranje vsebin na uporabniški terminalni opremi ne povzroča bistveno povečane obremenitve sistema. Testna terminalna oprema je uporabljala Windows XP operacijski sistem in naslednjo strojno konfiguracijo:

- CPU: Intel Pentium 4, 2Ghz,
- RAM: 768 MB Rambus,
- Osnovna plošča: Intel 850,
- Grafični vmesnik: Nvidia Geforce Titanium 4200, AGP 8x.

Pribitek zaradi potrebnega dekriptiranja je bil reda 1-3% procesorskega časa. Meritve smo izvedli z v tabeli navedenimi testnimi vsebinami.

Vsebina	Parametri	Original	Zaščitena vsebina
Vsebina 1	dolžina: 3:07 pasovna širina: 755 kbit/s format: 640x480x25, WM9	19.129.748 bytes	19.131.466 bytes
Vsebina 2	dolžina: 2:00 pasovna širina: 755 kbit/s format: 640x480x25, WM9	10.835.653 bytes	10.837.371 bytes
Vsebina 3	dolžina: 4:50 pasovna širina: 539 kbit/s format: 320x240x25, WM9	19.562.154 bytes	19.563.872 bytes

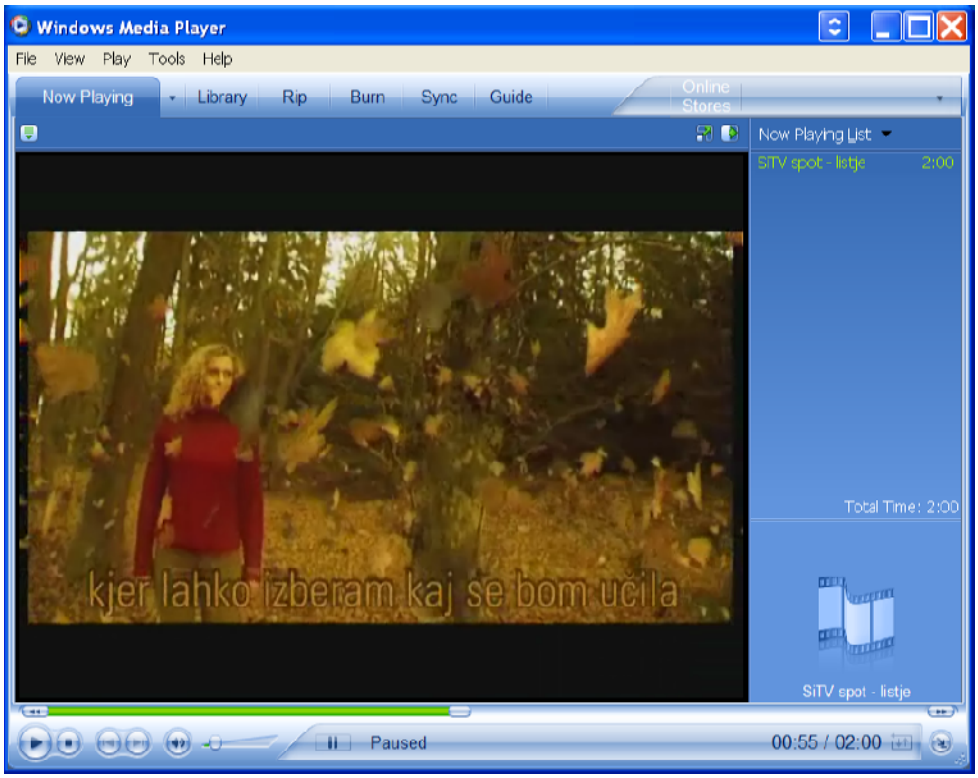
Tab. 15: Primerjava pribitka dolžine vsebin zaradi postopka zaščite

MS DRM sistem se zelo dobro vklaplja v obstoječo MS IPTV platformo. Kljub temu je na mestu kritika trenutne različice. Izpostavil bi naslednje točke:

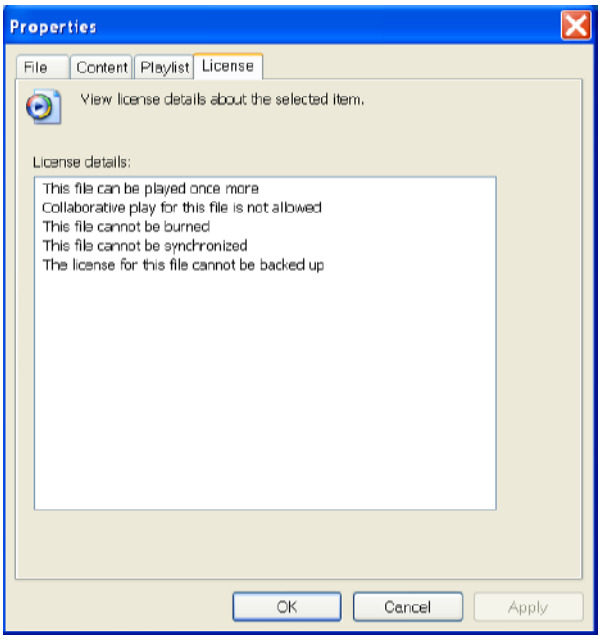
- neznan kriptirni mehanizem,
- gola funkcionalnost,
- trenutna podpora samo Windows operacijskemu sistemu in predvajalni opremi na osnovi MS Media Player predvajalnika.

Zagotavljanje varnosti s skrivanjem zaradi potencialnih slabosti kriptirnega mehanizma dolgoročno ni nujno dober pristop. Trenutna različica MS DRM ne predstavlja celotnega sistema za delo z vsebinami. Manjka praktično celoten del za upravljanje z vsebinami (CMS). Realizirana je le gola funkcionalnost v smislu zaščite vsebin in vsiljevanja predpisanih pogojev. Zadnja kritika gre omejeni podpori. Microsoft sicer preko izpostavljenih programskih orodij in knjižnic omogoča implementacijo agenta DRM na poljubni terminalni opremi. Vendar gre

pri tem za zasebno rešitev, ki jo je potrebno licencirati. Razlog za tako skrben nadzor nad programsko kodo je sicer razumljiv (agent DRM je najbolj izpostavljen del celotnega sistema), vendar takšen pristop lahko omeji razmah njihove rešitve.



Sl. 65: Predvajanje zaščitene vsebine v predvajalniku MS Media Player



Sl. 66: Uporabniška razlaga pripadajoče licence – opis pravic

7. SKLEP

Nematerialne dobrine v obliki informacij in vsebin imajo v informacijski in telekomunikacijsko povezani družbi veliko vrednost. V interesu njihovih lastnikov in ponudnikov je, da jih zaščitijo. Prav tej nalogi so namenjeni sistemi za digitalno zaščito in upravljane s vsebinami (DRM).

Pri zaščiti vsebin se iz tehničnega vidika uporabljata dva elementa in sicer mehanizmi zaščite vsebin ter opis pravil in pogojev uporabe. Vsebine se skuša zaščititi na celotni poti od ponudnikov do uporabnikov ter pri tem izogniti nevarnostim analogne in digitalne luknje. Za samo zaščito se primarno uporabljajo različni kriptografski postopki ter sekundarno dodatni mehanizmi, ki vsebine ščitijo v primeru zlorabe oz. zaobitja kriptografije. Drugi element je opis pogojev uporabe vsebin, ki je zapisan v obliki licence ter predstavlja pogodbo med lastnikom vsebin in uporabniki. Uporabnik namreč ni lastnik vsebine, temveč pridobi le pravico do uporabe v skladu z določenimi pogoji.

Magistrsko delo opisuje tehnologije in elemente sodobnih sistemov DRM ter tematiko zaokrožuje z arhitekturo in prikazom toka dogodkov v primeru splošnega sistema DRM.

Sistemi digitalne zaščite vsebin pogosto niso odvisni samo od tehnoloških dejavnikov, temveč tudi od drugih, kjer največkrat prevladujejo socialni. Uporabniki so zadnji in odločilni člen verige. Sistem DRM je zanje nepotreben dodatek, ki jim omejuje možnosti pri delu z vsebinami. Nikakor pri tem sistem DRM ne sme biti moteč ali preveč zahteven dejavnik. V nasprotnem primeru bodo uporabniki raje posegli po prostih, nelegalnih različicah vsebin. V okviru sklepa o sistemih DRM bi navedel še naslednje tri ugotovitve.

Dober poslovni model je prva in pogosto zelo učinkovita obrambna linija pred nelegalno pridobitvijo in zlorabo ter distribucijo vsebin. Primerna cena (poštena s stališča uporabnikov) veliko večino navadnih uporabnikov odvrne od zlorabe vsebin. Pri tem dobijo originalno različico vsebin, podprejo avtorje ter imajo dober »občutek« ob nakupu.

Sistem DRM, posebno njegov del, ki je odgovoren za vsiljevanje pravic, ne sme biti moteč ali celo vsiljiv za uporabnike. Preveč kompliciran ali restriktivni sistemi DRM, ki niso pogojeni z drugimi dejavniki (npr. zakonsko predpisani sistemi), ne bodo uspešni. Uporabniki bodo v tem primeru raje posegli po nelegalnih vsebinah.

100 % varnega sistema ni, sistem, ki se temu idealu skuša približati v njegovi skrajni limiti (stopnja varnosti = $lim_{n->0}[100\%-n]$, v komercialnih postavitvah največkrat ni ekonomsko upravičen. Stopnja varnosti sistema DRM se lahko zelo poveča, če je uporabljen v kombinaciji z drugimi smiselnimi varnostnimi mehanizmi na nižjih slojih TK modela.

Znani predstavniki sistemov DRM so Microsoft DRM in Real Helix DRM, akademski Tiramisu ter iniciativa Trusted Computing. Prva dva predstavnika sta primera komercialnih rešitev, projekt Tiramisum pa je zanimiv, ker temelji na odprtih standardih. Iniciativa Trusted Computing nakazuje možen prihodnji razvoj v tej smeri. Osebno upam, da inciativa Trusted Computing v prihodnosti ne bo

prevladala v takšni obliki, kot je bila načrtovana. Gre za zelo restriktiven sistem, ki posega na večino področij dela z vsebinami in kaže na relativno »črn« scenarij razvoja.

Sistemi pogojnega dostopa so bili v osnovi namenjeni zaščiti vsebin digitalne (DVB) televizije. Pri tem so bili zelo omejeni, saj je največkrat šlo le za omejevanje dostopa do vsebin, od koder izvira ime tehnologije. Sodobni sistemi pogojnega dostopa te omejitve preraščajo in se po funkcionalnostih približujejo sistemom DRM. Najbolj znani predstavniki s tega področja so rešitve podjetij Irdeto, Philips CryptoWorks, NDS in WideWine Technologies.

Izpostavljene so ključne lastnosti sistemov DRM in pogojnega dostopa ter podana je primerjava med njimi. Menim, da sistemi DRM šele prehajajo v svoje zrelo obdobje. Gre za zelo kompleksne sisteme, ki so sestavljeni iz številnih elementov, ki temeljijo na različnih tehnologijah. Razumljiva je težnja po standardizaciji celotnega sistema DRM ali vsaj njegovih osnovnih komponent. Pri tem se za kamen spotike izkažejo uporabljeni kriptografski postopki, kjer se posebno pri komercialnih rešitvah razvijalci zaradi potencialno večje stopnje varnosti raje odločajo za lastne, skrite algoritme. Kljub temu obstaja nekaj primerov poskusov standardizacije sistema DRM v celoti. Na mobilnem področju je tako zanimiva rešitev organizacije Open Mobile Alliance, na fiksnem pa rešitev IPMP, ki je definirana v okviru standarda MPEG-21 »Večpredstavno ogrodje«.

Klasični sistemi pogojnega dostopa so nekoliko starejši ter danes predstavljajo zrelo, dobro definirano ter standardizirano tehnologijo. V primerjavi s sistemi DRM, ki izvirajo iz računalniškega sveta, so klasični sistemi pogojnega dostopa tipično televizijska tehnologija. Izzivom zaščite sodobnih, večpredstavnih vsebin in storitev se približujejo s svojega zornega kota ter bodo, po mojem mnenju, kmalu predstavljali resno konkurenco sistemom DRM.

Področje terminalne opreme in uporabniškega vmesnika je najbolj pomembno za uporabnike. Ker so uporabniki tudi končni porabniki vsebin in storitev, mora biti to področje prav tako pomembno za vse ostale akterje. V okviru magistrskega dela sem raziskal področje sodobne širokopasovne večpredstavne terminalne opreme ter predlagal zasnovo konvergenčnega terminala. V eni napravi se združujejo področja uporabe osebnega računalnika, TV komunikatorja, večpredstavnega predvajalnika ter igralne konzole. Namenjen je uporabi v domačem okolju dnevne sobe. Namen predlaganega večpredstavnega terminala je prevzeti vlogo centra hišne zabave ob podpori funkcionalnosti sistemov DRM.

Funkcionalnosti sistema DRM sem preizkusil na realnem primeru. Za osnovo je služila implementacija podjetja Microsoft (MS DRM), ki sem jo postavil v laboratorijskem okolju. Sistem MS DRM se dobro vključuje v obstoječo MS IPTV platformo, vendar pokriva le precej osnovne DRM funkcionalnosti. Preizkusil sem tako zaščito živih vsebin, kot tudi vsebin na zahtevo. Oba scenarija sta delovala v skladu s specifikacijami.

SLOVAR KRATIC IN IZRAZOV

IZRAZ	ANGLEŠKO	SLOVENSKO
3DES	Triple DES	trojni DES
3PLAY	Triple Play	storitev »trojček«
A		
ADSL	Asymmetric Digital Subscriber Line	nesimetrični digitalni naročniški vod
AES	Advanced Encryption Standard	napredni kriptirni standard
AGP	Accelerated Graphics Port	pospešeni grafični vmesnik
API	Application Programming Interface	aplikacijski program(er)ski vmesnik
ASF	MS Advanced Streaming Format	MS napredni pretočni format
ATM	Asynhronous Transfer Mode	asinhroni prenosni način
B		
BIOS	Basic Input/Output System	osnovni sistem pri PC računalniku
BR	Bit Rate	bitna hitrost
C		
CA	Conditional Access	sistem pogojnega dostopa
CBR	Constant Bit Rate	konstantna bitna hitrost
Chipset		vezni nabor osnovne plošče
CMS	Content Management System	sistem za upravljanje vsebin
Compression		kompresija, stiskanje
CPU	Central Processing Unit	procesor
CRT	Cathode Ray Tube	katodni zaslon, tudi monitor s katodnim zaslonom
CSMA/CD	Carrier Sense Multiple Access/Collission Detection	Ethernet način za dostop do skupnega medija
D		
DAB	Digital Audio Broadcast	digitalni prenos zvoka

DDR	Double Data Ram	podatki se prenašajo ob obeh urinih frontah
DES	Data Encryption Standard	
DRM	Digital Rights Management	sistem digitalne zaščite pravic
DSL	Digital Subscriber Line	digitalni naročniški vod
DV	Digital Video	video v digitalni obliki (MPEG-2)
DVB	Digital Video Broadcast	digitalna televizija, video
DVD	Digital Video/Versalatile Disk	digitalni video/večnamenski disk
DVI	Digital Video Interface	digitalni video vmesnik (za LCD)
DVR	Digital Video Record(er)ing	digitalno zapisovanje TV signala
E		
Ethernet		standard računalniškega omrežja
F		
Flash ROM	Flash Read Only Memory	vpisljiv bralni pomnilnik
Fps	Frames Per Second	št. slik na sekundo
FTP	File Transfer Protocol	protokol za prenos datotek
G		
GPU	Graphics Processing Unit	grafični procesor
H		
HDMI	High Definition Multimedia Interface	digitalni vmesnik za HDTV
HDSL	High-Speed Digital Subscriber Line	hitri digitalni naročniški vod
HDTV	High Definition Television System	televizija visoke razločljivosti
HTML	Hypertext Markup Language	hipertekstovni jezik
HTPC	Home Theater PC	domači večpredstavni PC
HW	HardWare	strojna oprema
I		
Igralna konzola		naprava za igranje iger na televizijskem sprejemniku
internet		več računalniških omrežij

Internet		svetovno rač. omrežje (medmrežje)
IP	Internet Protocol	protokol internet
ISDN	Integrated Services Digital Network	integrirano omrežje z digitalnimi storitvami
ISO	International Standard Organization	mednarodna organizacija za standarde
J		
JPEG	Joint Pictures Expert Group	ekspertna skupina za slike
K		
KF	Key Frame	ključna slika
Kodek, codec	Compressor Decompressor	program za kodiranje/kompresijo
L		
LAN	Local Area Network	lokalno omrežje
LCD	Liquid Crystal Display	zaslon na tekoče kristale
M		
MAC	Media Access Control	metoda dostopa do medija
MJPEG	Motion JPEG	
MMS	Microsoft Media Server Protocol	MS media strežniški protokol
Modem	Modulator-Demodulator	
MPEG	Moving Pictures Experts Group	ekspertna skupina za gibajoče slike
Multicast(ing)		oddajanje več prejemnikom
Multimedia		multimedija, večpredstavnost
N		
NTSC	National Televison Standard Committee	ameriški TV standard
O		
OS	Operating System	operacijski sistem
OSI	Open System Interconnection	mednarodni TK standard
P		
PAL	Phase Alternating Line	evropski TV standard

PC	Personnal Computer	osebni računalnik
PCI	Peripheral Component Interconnect	računalniško vodilo
Pixel, pel	picture element	slikovni element
Port	port	komunikacijska vrata
PSTN	Public Switchwed Telephone Network	javno komutirano telefonsko omrežje
PVR	Personal Video Recording	osebni videorekorder
Q		
QoS	Quality of Service	kakovost storitev (storitve)
R		
RAM	Random Access Memory	bralno/pisalni pomnilnik
REL	Rights Expression Language	jezik za opis pravic
RGB	Red Green Blue	barvni sistem
ROM	Read Only Memory	samo bralni pomnilnik
RTCP	Real Time Control Protocol	
RTP	Real-time Transport Protocol	
RTSP	Real Time Streaming Protocol	
S		
S/PDIF	Sony/Philips Digital Interface	digitalni vmesnik za prenos zvoka
SCSI	Small Computer System Interface	sistemski vmesnik malih računalnikov
Server		strežnik
STB	Set-Top-Box	televizijski komunikator
SW	SoftWare	programska oprema
T		
TC	Trusted Computing	
TCG	Trusted Computing Group	
TCP	Transfer Control Protocol	kontrolni protokol prenosa
TCP	Trusted Computing Platform	platforma zaupanja vrednega računališтva
TCPA	Trusted Platform Computing Alliance	

TE	Terminal Equipment	terminalna oprema
U		
UDP	User Datagram Protocol	uporabniški datagramski protokol
Unicast(ing)		povezava tipa točka-točka
USB	Universal Serial Bus	univerzalno serijsko vodilo
UTP	Unshielded Twisted Pair	neoklopljena parica, par
V		
VBR	Variable Bit Rate	spremenljiva bitna hitrost
VCR	Video Cassete Recorder	video rekorder
VHS, SVHS	Video Home System, SuperVHS	način zapisa videosignala (VCR)
VoD	Video on Demand	video na zahtevo
W		
WAN	Wide Area Network	omrežje na širokem področju (npr. države)
WM	Windows Media	
WMA	Windows Media Audio	zvočni kodek
WMV	Windows Media Video	slikovni kodek
WWW	World Wide Web	svetovni splet (del Interneta)
X		
XML	eXtended Markup Language	razširjen hipertekstovni jezik
Y		
YUV	Y-svetlost; U,V barva	barvni sistem

SEZNAM VIROV

	SPLETNI VIRI
[W1]	Webopedia: Sistem DRM, definicija, http://www.webopedia.com/ http://www.webopedia.com/TERM/D/DRM.html
[W2]	Wikipedia: Sistem DRM, definicija, http://en.wikipedia.org/ http://en.wikipedia.org/wiki/Digital_rights_management
[W3]	Encarta: Sistem DRM, definicija, http://encarta.msn.com/artcenter_/browse.html http://encarta.msn.com/encnet/refpages/search.aspx?q=DRM&Submit2=Go
[W4]	Mehanizem zaščite zabavne programske opreme (iger) s tehnologijo FADE, http://www.gameburnworld.com/protections_fade.shtml
[W5]	DVD-video in zaščita CSS, http://www.lemuria.org/DeCSS/decss.html http://en.wikipedia.org/wiki/DeCSS http://www.cs.cmu.edu/~dst/DeCSS/Gallery/ http://www.cs.cmu.edu/~dst/DeCSS/FrankStevenson/analysis.html
[W6]	Macrovision zaščita, http://www.macrovision.com/products/macrovision_acp/index.shtml http://en.wikipedia.org/wiki/Macrovision
[W7]	The ITV Dictionary: Pogojni dostop, definicija, http://www.itvdictionary.com/conditional_access.html
[W8]	What IS: Pogojni dostop, definicija, http://www.itvdictionary.com/conditional_access.html
[W9]	Wikipedia: Pogojni dostop, definicija, http://en.wikipedia.org/wiki/Conditional_access
[W10]	Konzorcij DVB, http://www.dvb.org/
[W11]	Sistemi pogojnega dostopa Conditional Access: Splošni viri, http://www.dtg.org.uk/reference/tutorial/ca.htm http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci331380,00.html http://www.itvdictionary.com/conditional_access.html http://www.dvb.org/index.php?id=50
[W12]	Irdeto, http://www.irdetoaccess.com/

[W13]	NDS, http://www.nds.com/
[W14]	Philips Cryptoworks, http://www.software.philips.com/InformationCenter/Global/FArticleSummary.asp?lNodeId=870&channel=870&channelId=N870A2300
[W15]	SecureMedia, http://www.securemedia.com/index.php
[W16]	Widewine Technologies, http://www.widevine.com/default.asp
[W17]	Nagravision, http://www.nagravision.com/
[W18]	Viaccess, http://www.viaccess.com/
[W19]	Mediaguard, http://www.nagra.fr/index.php
[W20]	Conax, http://www.conax.com/
[W21]	Tajnopisje, http://www.ljudmila.org/matej/privacy/kripto/stego.html
[W22]	<indecs> Framework, http://www.indecs.org
[W23]	Kriptografija – DES, http://en.wikipedia.org/wiki/Data_Encryption_Standard
[W24]	Kriptografija – 3DES, http://en.wikipedia.org/wiki/3DES
[W25]	Kriptografija – AES, http://en.wikipedia.org/wiki/AES
[W26]	Kriptografija – RSA, http://en.wikipedia.org/wiki/Data_Encryption_Standard
[W27]	National Institute of Standards and Technology, http://www.nist.gov/
[W28]	RSA Laboratories, http://www.rsasecurity.com/rsalabs/node.asp?id=2152
[W29]	ISO, http://www.iso.org/iso/en/ISOOnline.frontpage
[W30]	Watermarking, http://www.watermarkingworld.org/ http://en.wikipedia.org/wiki/Digital_watermarking

[W31]	Rights Expression Language, http://xml.coverpages.org/mpegRights.html
[W32]	OMA, http://www.openmobilealliance.org/
[W33]	MPEG, MPEG-7, MPEG-21, http://www.mpegif.org/resources.php#section42 http://mpeg-21.itec.uni-klu.ac.at/cocoon/mpeg21/ http://www.chiariglione.org/mpeg/standards/mpeg-21/mpeg-21.htm
[W34]	ODRL, http://odrl.net/
[W35]	XrML, http://www.xrml.org/
[W36]	Microsoft DRM, http://www.microsoft.com/windows/windowsmedia/drm/default.aspx http://www.microsoft.com/windows/windowsmedia/drm/faq.aspx http://www.microsoft.com/windows/windowsmedia/howto/articles/drmarchitecture.aspx?pf=true
[W37]	Trusted Computing, https://www.trustedcomputinggroup.org/home http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html http://en.wikipedia.org/wiki/NGSCB
[W38]	Tiramisu, http://www.optibase.com/Content.aspx?id=1748 http://www.dmpf.org/open/dmp0086.doc http://www.rose.es/docs/TIRAMISU%20DRM%20Requirements%20and%20Beyond.ppt
[W39]	Shuttle, http://us.shuttle.com/
[W40]	MSI, http://www.msi.com.tw/
[W41]	Amino, http://www.aminocom.com/
[W42]	VIA Epia, http://www.viaembedded.com/index.jsp http://www.viavpsd.com/product/epia_m_spec.jsp?motherboardId=81
[W43]	MS Windows Media Center, http://www.microsoft.com/windowsxp/mediacenter/default.mspx
[W44]	Microsoft Windows Media, http://www.windowsmedia.com,

[W45]	BeyondTV, http://www.snapstream.com/products/beyondtv/
[W46]	Kriptografija splošni viri, http://en.wikipedia.org/wiki/Cryptography
[W47]	Wikipedia: Terminalna oprema, definicija, http://en.wikipedia.org/wiki/Terminal_equipment

🕮	**ČLANKI IN KNJIŽNI VIRI**
[K1]	Pramod A. Jamkhedkar, Gregory L. Heileman: DRM as a Layered System, The Fourth ACM Workshop on Digital Rights Management, DRM 2004, http://www.cse.uconn.edu/~drm2004/ http://www.cse.uconn.edu/~drm2004/talks/heileman.pdf
[K2]	Eberhard Becker, Willms Buhse, Dirk Guennewig, *et al.:* Digital Rights Management: Technological, Economic, Legal and Political Aspects, Springer-Verlag GmbH, 2003 Eberhard Becker, Willms Buhse, Dirk Günnewig, et al.: DRM as an Interlocking Challenge for Different Scientific Disciplines: Introduction, str. 1-2
[K3]	Eberhard Becker, Willms Buhse, Dirk Guennewig, *et al.:* Digital Rights Management: Technological, Economic, Legal and Political Aspects, Springer-Verlag GmbH, 2003 Niels Rump: Definition, Aspects, and Overview, str. 3-15
[K4]	Eberhard Becker, Willms Buhse, Dirk Guennewig, *et al.:* Digital Rights Management: Technological, Economic, Legal and Political Aspects, Springer-Verlag GmbH, 2003 Richard Gooch: Requirements for DRM Systems Introduction – The Requirement for DRM, str. 16-25
[K5]	Eberhard Becker, Willms Buhse, Dirk Guennewig, *et al.:* Digital Rights Management: Technological, Economic, Legal and Political Aspects, Springer-Verlag GmbH, 2003 Norman Paskin: Components of DRM Systems Identification and Metadata, str. 26-61
[K6]	Eberhard Becker, Willms Buhse, Dirk Guennewig, *et al.:* Digital Rights Management: Technological, Economic, Legal and Political Aspects, Springer-Verlag GmbH, 2003 Gabriele Spenger: Authentication, Identification Techniques, and Secure Containers – Baseline Technologies, str. 62-80
[K7]	Eberhard Becker, Willms Buhse, Dirk Guennewig, *et al.:* Digital Rights Management: Technological, Economic, Legal and Political Aspects, Springer-Verlag GmbH, 2003 Fabien A.P. Petitcolas: Digital Watermarking, str. 81-92
[K8]	Eberhard Becker, Willms Buhse, Dirk Guennewig, *et al.:* Digital Rights Management: Technological, Economic, Legal and Political Aspects, Springer-Verlag GmbH, 2003 Jürgen Herre: Content Based Identification (Fingerprinting), str. 93-100
[K9]	Eberhard Becker, Willms Buhse, Dirk Guennewig, *et al.:* Digital Rights Management: Technological, Economic, Legal and Political Aspects, Springer-Verlag GmbH, 2003 Susanne Guth: Rights Expression Languages, str. 101-112
[K10]	Eberhard Becker, Willms Buhse, Dirk Guennewig, *et al.:* Digital Rights Management: Technological, Economic, Legal and Political Aspects, Springer-Verlag GmbH, 2003 Ahmad-Reza Sadeghi and Markus Schneider: Electronic Payment Systems, str. 113-137
[K11]	Eberhard Becker, Willms Buhse, Dirk Guennewig, *et al.:* Digital Rights Management: Technological, Economic, Legal and Political Aspects, Springer-Verlag GmbH, 2003 Frank Hartung: Mobile DRM Introduction: The Need for Mobile DRM, str. 138-149
[K12]	Eberhard Becker, Willms Buhse, Dirk Guennewig, *et al.:* Digital Rights Management: Technological, Economic, Legal and Political Aspects, Springer-Verlag GmbH, 2003 Susanne Guth: A Sample DRM System, str. 150-161

[K13]	Eberhard Becker, Willms Buhse, Dirk Guennewig, *et al.:* Digital Rights Management: Technological, Economic, Legal and Political Aspects, Springer-Verlag GmbH, 2003 Spencer Cheng and Avni Rambhia: DRM and Standardization – Can DRM Be Standardized?, str. 162-177
[K14]	Eberhard Becker, Willms Buhse, Dirk Guennewig, *et al.:* Digital Rights Management: Technological, Economic, Legal and Political Aspects, Springer-Verlag GmbH, 2003 Dirk Kuhlmann and Robert A. Gehring: Trusted Platforms, DRM, and Beyond, str. 178-205
[K15]	Eberhard Becker, Willms Buhse, Dirk Guennewig, *et al.:* Digital Rights Management: Technological, Economic, Legal and Political Aspects, Springer-Verlag GmbH, 2003 Tobias Hauser and Christian Wenz: DRM Under Attack: Weaknesses in Existing Systems, str. 206-223
[K16]	Eberhard Becker, Willms Buhse, Dirk Guennewig, *et al.:* Digital Rights Management: Technological, Economic, Legal and Political Aspects, Springer-Verlag GmbH, 2003 Stuart Haber, Bill Horne, Joe Pato, et al.: If Piracy Is the Problem, Is DRM the Answer?, str. 224-233
[K17]	Eberhard Becker, Willms Buhse, Dirk Guennewig, *et al.:* Digital Rights Management: Technological, Economic, Legal and Political Aspects, Springer-Verlag GmbH, 2003 Tobias Bauckhage: Digital Rights Management: Economic Aspects The Basic Economic Theory of Copying, str. 234-249
[K18]	Eberhard Becker, Willms Buhse, Dirk Guennewig, *et al.:* Digital Rights Management: Technological, Economic, Legal and Political Aspects, Springer-Verlag GmbH, 2003 Rolf T. Wigand: Facing the Music: Value-Driven Electronic Markets, Networks and Value Webs in Economic Integration of Digital Products, str. 250-270
[K19]	Eberhard Becker, Willms Buhse, Dirk Guennewig, *et al.:* Digital Rights Management: Technological, Economic, Legal and Political Aspects, Springer-Verlag GmbH, 2003 Willms Buhse and Amélie Wetzel: Creating a Framework for Business Models for Digital Content – Mobile Music as Case Study, str. 271-287
[K20]	Eberhard Becker, Willms Buhse, Dirk Guennewig, *et al.:* Digital Rights Management: Technological, Economic, Legal and Political Aspects, Springer-Verlag GmbH, 2003 Arnold Picot and Marina Fiedler: Impacts of DRM on Internet Based Innovation, str. 288-300
[K21]	Eberhard Becker, Willms Buhse, Dirk Guennewig, *et al.:* Digital Rights Management: Technological, Economic, Legal and Political Aspects, Springer-Verlag GmbH, 2003 Marc Fetscherin: Evaluating Consumer Acceptance for Protected Digital Content, str. 301-320
[K22]	Eberhard Becker, Willms Buhse, Dirk Guennewig, *et al.:* Digital Rights Management: Technological, Economic, Legal and Political Aspects, Springer-Verlag GmbH, 2003 Michel Clement: Lessons from Content-for-Free Distribution Channels, str. 321-333
[K23]	Eberhard Becker, Willms Buhse, Dirk Guennewig, *et al.:* Digital Rights Management: Technological, Economic, Legal and Political Aspects, Springer-Verlag GmbH, 2003 Oliver Bremer and Willms Buhse: Standardization in DRM – Trends and Recommendations, str. 334-343
[K24]	Eberhard Becker, Willms Buhse, Dirk Guennewig, *et al.:* Digital Rights Management: Technological, Economic, Legal and Political Aspects, Springer-Verlag GmbH, 2003 Peter Biddle, Paul England, Marcus Peinado, et al.: The Darknet and the Future of Content Protection, str. 344-365

[K25]	Eberhard Becker, Willms Buhse, Dirk Guennewig, *et al.:* Digital Rights Management: Technological, Economic, Legal and Political Aspects, Springer-Verlag GmbH, 2003 Mathias Lejeune: Protection of Digital Content and DRM Technologies in the USA, str. 366-382
[K26]	Eberhard Becker, Willms Buhse, Dirk Guennewig, *et al.:* Digital Rights Management: Technological, Economic, Legal and Political Aspects, Springer-Verlag GmbH, 2003 Barbara Simons: The Copyright Wars – A Computer Scientist's View of Copyright in the U.S., str. 383-404
[K27]	Eberhard Becker, Willms Buhse, Dirk Guennewig, *et al.:* Digital Rights Management: Technological, Economic, Legal and Political Aspects, Springer-Verlag GmbH, 2003 Jörg Reinbothe: Protection of Digital Content and DRM Technologies in the European Union, str. 405-417
[K28]	Eberhard Becker, Willms Buhse, Dirk Guennewig, *et al.:* Digital Rights Management: Technological, Economic, Legal and Political Aspects, Springer-Verlag GmbH, 2003 Lee A. Bygrave: Digital Rights Management and Privacy – Legal Aspects in the European Union, str. 418-446
[K29]	Eberhard Becker, Willms Buhse, Dirk Guennewig, *et al.:* Digital Rights Management: Technological, Economic, Legal and Political Aspects, Springer-Verlag GmbH, 2003 Séverine Dusollier: Tipping the Scale in Favor of the Right Holders: The European Anti-Circumvention Provisions, str. 462-478
[K30]	Eberhard Becker, Willms Buhse, Dirk Guennewig, *et al.:* Digital Rights Management: Technological, Economic, Legal and Political Aspects, Springer-Verlag GmbH, 2003 Thomas Dreier and Georg Nolte: Protection of Digital Content and DRM Technologies in German Copyright, str. 479-501
[K31]	Eberhard Becker, Willms Buhse, Dirk Guennewig, *et al.:* Digital Rights Management: Technological, Economic, Legal and Political Aspects, Springer-Verlag GmbH, 2003 Stefan Bechtold: The Present and Future of Digital Rights Management – Musings on Emerging Legal Problems, str. 597-654
[K32]	Frank Hartung, Friedhelm Ramme: Digital Rights Management and Watermarking of Multimedia Content for M-Commerce Applications, IEEE Communications Magazine, November 2000
[K33]	*William Luh, Deepa Kundur:* New Paradigms for Effective Multicasting and Fingerprinting of Entertainment Media, IEEE Communications Magazine, Junij 2005
[K34]	Aleš Zavec: Protokoli za zaščito elektronske pošte, diplomsko delo, FE, Ljubljana 2002
[K35]	Radoslav Smrekar: Samosinhronizirni sprotni šifrirni algoritem, diplomsko delo, FE, Ljubljana 2001
[K36]	Boštjan Marušič, Štefan Dobravec, Philippe de Cuetos, Cyril Concolato, Laurent Piron, Jurij F. Tasič: TIRAMISU: A Novel Approach to Content Representation and Key Management for Seamless Super-Distribution of Protected Media, Signal Processing: Image Communication, Vol 20, Issue 9-10, str. 947-971
[K37]	Štefan Dobravec: Ogrodje novih multimedijskih tehnologij-MPEG-21, magistrsko delo, FE, Ljubljana 2003
[K38]	P. Meše, Internet: pojmovnik, angleško-slovenski slovar, slovar kratic in slovensko-angleški slovar, Elektrotehniška zveza Slovenije, 1999
[K39]	J. Bešter, M. Jagodič, M. Krišelj, P. Meše, M. Šubic, Zlivanje telekomunikacijskih omrežij in storitev, Elektrotehniška zveza Slovenije, Ljubljana, 1998
[K40]	Jože Guna: Video storitve prek internetnih omrežij, diplomsko delo, FE, Ljubljana 2002

Izjava o avtorstvu

Izjavljam, da sem magistrsko delo samostojno izdelal pod vodstvom mentorja prof. dr. Janeza Beštra.

Izkazano pomoč drugih sodelavcev sem v celoti navedel v zahvali.

V Ljubljani, 17. 10. 2005

Jože Guna