УНИВЕРЗИТЕТ У НОВОМ САДУ
ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА У НОВОМ САДУ

Немања Фимић

Заштита плаћеног садржаја при дистибуцији на уређаје додатног екрана

МАСТЕР РАД

Нови Сад, 2014.

	УНИВЕРЗИТЕТ У НОВОМ САДУ ● **ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА** 21000 НОВИ САД, Трг Доситеја Обрадовића 6	Број:
	ЗАДАТАК ЗА МАСТЕР РАД	Датум:

(Податке уноси предметни наставник - ментор)

СТУДИЈСКИ ПРОГРАМ:	Рачунарство и аутоматика
РУКОВОДИЛАЦ СТУДИЈСКОГ ПРОГРАМА:	Никола Јорговановић

Студент:	Немања Фимић	Број индекса:	Е2 20/2013
Област:	Архитектуре и алгоритми у дигиталним сигналним процесорима 1		
Ментор:	Јелена Ковачевић		

НА ОСНОВУ ПОДНЕТЕ ПРИЈАВЕ, ПРИЛОЖЕНЕ ДОКУМЕНТАЦИЈЕ И ОДРЕДБИ СТАТУТА ФАКУЛТЕТА ИЗДАЈЕ СЕ ЗАДАТАК ЗА МАСТЕР РАД, СА СЛЕДЕЋИМ ЕЛЕМЕНТИМА:

- проблем – тема рада;
- начин решавања проблема и начин практичне провере резултата рада, ако је таква провера неопходна;

НАСЛОВ МАСТЕР РАДА:

Заштита плаћеног садржаја при дистибуцији на уређаје додатног екрана

ТЕКСТ ЗАДАТКА:

Обезбедити заштиту плаћеног садржаја при дистрибуцији на уређаје додатног екрана коришћењем ЦИ+ програмске јединице и ДТЦП-ИП протокола. Потребно је извршити анализу ЦИ+ и ДТЦП-ИП програмских јединица и одредити који делови морају да буду у заштићеним регионима. Такође је потребно извршити имплементацију ових програмских јединица и репродуковати садржај на додатном екрану у циљу верификације решења.

Руководилац студијског програма:	Ментор рада:

Примерак за: o - Студента; o - Ментора

УНИВЕРЗИТЕТ У НОВОМ САДУ ● **ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА**
21000 НОВИ САД, Трг Доситеја Обрадовића 6

КЉУЧНА ДОКУМЕНТАЦИЈСКА ИНФОРМАЦИЈА

Редни број, **РБР**:	
Идентификациони број, **ИБР**:	
Тип документације, **ТД**:	Монографска документација
Тип записа, **ТЗ**:	Текстуални штампани материјал
Врста рада, **ВР**:	Дипломски – мастер рад
Аутор, **АУ**:	Немања Фимић
Ментор, **МН**:	др Јелена Ковачевић
Наслов рада, **НР**:	Заштита плаћеног садржаја при дистибуцији на уређаје додатног екрана
Језик публикације, **ЈП**:	Српски / латиница
Језик извода, **ЈИ**:	Српски
Земља публиковања, **ЗП**:	Република Србија
Уже географско подручје, **УГП**:	Војводина
Година, **ГО**:	2014.
Издавач, **ИЗ**:	Ауторски репринт
Место и адреса, **МА**:	Нови Сад; трг Доситеја Обрадовића 6
Физички опис рада, **ФО**: (поглавља/страна/ цитата/табела/слика/графика/прилога)	7/61/0/4/31/0/0
Научна област, **НО**:	Електротехника и рачунарство
Научна дисциплина, **НД**:	Рачунарска техника
Предметна одредница/Кључне речи, **ПО**:	ЦИ+, ДТЦП-ИП, заштита, дистрибуција, ДТВ пријемник
УДК	
Чува се, **ЧУ**:	У библиотеци Факултета техничких наука, Нови Сад
Важна напомена, **ВН**:	
Извод, **ИЗ**:	У овом раду је приказано решење за заштиту плаћеног садржаја при дистрибуцији на уређаје додатног екрана. У циљу реализације коришћене су ЦИ+ програмска јединица, за контролу модула за условни приступ, и ДТЦП-ИП програмска јединица за управљање дигиталним правима. Реализовано решење је тестирано на три различита уређаја додатног екрана. Критеријум успешности теста је успешна репродукција плаћеног садржаја на уређају додатног екрана.
Датум прихватања теме, **ДП**:	
Датум одбране, **ДО**:	

Чланови комисије, **КО**:			
	Председник:	проф др Никола Теслић	
	Члан:	др Растислав Струхарик	Потпис ментора
	Члан, ментор:	др Јелена Ковачевић	

UNIVERSITY OF NOVI SAD ● **FACULTY OF TECHNICAL SCIENCES**
21000 NOVI SAD, Trg Dositeja Obradovića 6

KEY WORDS DOCUMENTATION

Accession number, **ANO**:			
Identification number, **INO**:			
Document type, **DT**:		Monographic publication	
Type of record, **TR**:		Textual printed material	
Contents code, **CC**:		Master Thesis	
Author, **AU**:		Nemanja Fimić	
Mentor, **MN**:		Jelena Kovačević, PhD	
Title, **TI**:		Secured Streaming of Premium Content in Second Screen Environment	
Language of text, **LT**:		Serbian	
Language of abstract, **LA**:		Serbian	
Country of publication, **CP**:		Republic of Serbia	
Locality of publication, **LP**:		Vojvodina	
Publication year, **PY**:		2014.	
Publisher, **PB**:		Author's reprint	
Publication place, **PP**:		Novi Sad, Dositeja Obradovica sq. 6	
Physical description, **PD**: (chapters/pages/ref./tables/pictures/graphs/appendixes)		7/61/0/4/31/0/0	
Scientific field, **SF**:		Electrical Engineering	
Scientific discipline, **SD**:		Computer Engineering, Engineering of Computer Based Systems	
Subject/Key words, **S**/**KW**:		CI+, DTCP-IP, Security, Streaming, STB	
UC			
Holding data, **HD**:		The Library of Faculty of Technical Sciences, Novi Sad, Serbia	
Note, **N**:			
Abstract, **AB**:		This paper presents a solution for secured streaming of premium content in second screen environment. For this purpose, CI+ stack and DTCP-IP protocol were used. CI+ stack was used in order to control the CAM, while the job of DTCP-IP protocol was to provide DRM. Implemented solution was tested with three different second screen devices. Tests were rendered successful in case of successful playback on the second screen device.	
Accepted by the Scientific Board on, **ASB**:			
Defended on, **DE**:			
Defended Board, **DB**:	President:	Nikola Teslić, PhD	
	Member:	Rastislav Stuharik, PhD	Menthor's sign
	Member, Mentor:	Jelena Kovačević, PhD	

Zahvalnost

Zahvaljujem se institutu RT-RK na pruženoj mogućnosti za realizaciju ovog rada.

Takođe se zahvaljujem mentoru dr Jeleni Kovačević, stručnom saradniku Goranu Miljkoviću, kao i kolegama iz AMUSE tima na savetima i stručnoj pomoći prilikom izrade ovog rada.

Na kraju, zahvaljujem se svojoj porodici na pruženoj podršci tokom mog školovanja.

SADRŽAJ

SPISAK SLIKA

SPISAK TABELA

SKRAĆENICE

DTV	*- Digitalna televizija*
DVB	**-** *Digital Video Broadcasting*
TS	**-** *Transport Stream, Prenosni tok*
PID	**-** *PacketIdentifier, Identifikator paketa*
PSI	**-** *Program Specific Information, Informacije specifične za program*
PAT	**-** *Program Association Table, Tabela asocijacije programa*
PMT	**-** *Program Map Table, Tabela mapiranja programa*
CAT	**-** *Conditional Access Table, Tabela uslovnog pristupa*
NIT	**-** *Network Information Table, Tabela mrežnih informacija*
CI+	*- Common Interface Plus*
DES	**-** *Data Encryption Standard*
AES	**-** *Advanced Encryption Standard*
SAC	**-** *Secure Authenticated Channel, Sigurni autentifikovani kanal*
PCMCIA	**-** *Personal Computer Memory Card International Association*
DTCP-IP	*- Digital Transmission Content Protection over Internet Protocol*
DTLA	**-** *Digital Transmission Licensing Administrator*
DRM	**-** *Digital Rights Management, Upravljanje digitalnim pravima*
AKE	**-** *Authentication and Key Exchange, Autentifikacija i razmena ključeva*
EMI	**-** *Encryption Mode Indicator, Indikator moda enkripcije*
SRM	**-** *System Renewability Message, Poruka obnovljivosti sistema*
SHA-1	**-** *Secure Hash Algorithm*
RNDG	**-** *Random Number Generator, Generator slučajnog broja*
ECC	**-** *Elliptic Curve Cryptography, Kriptografija eliptične krive*
EC-DHA	**-** *Elliptic Curve Diffie-Hellman Algorithm*

EC-DSA - *Elliptic Curve Digital Signature Algorithm*

EBC - *Electronic Code Book*

CBC - *Cipher-block chaining*

HAL - *Hardware Abstraction Layer, Apstrakcioni sloj fizičke arhitekture*

CCK - *Content Control Key, Ključ za kontrolu sadržaja*

DMS - *Digital Media Server, Digitalni medija poslužilac*

1. Uvod

U ovom radu je predstavljeno rešenje za sigurnu distribuciju plaćenog sadržaja u okruženju dodatnog ekrana u kućnoj mreži. Opisano rešenje za sigurnu distribuciju obuhvata faze prihvata signala od emitera, boravka sadržaja na digitalnom TV prijemniku i samu distribuciju na uređaj dodatnog ekrana.

Razvoj digitalne televizije, kao i prenosnih uređaja i infrastrukture kućnih mreža doveo je do promene u načinu gledanja televizije. Usled postojanja sve većeg broja uređaja sposobnih za reprodukciju multimedijalnog sadržaja u prosečnoj kući, televizor više ne zaokuplja celokupnu pažnju gledaoca. Čest je slučaj kada se paralelno sa gledanjem televizijskog programa traže dodatne informacije na internetu korištenjem mobilnog telefona ili tablet računara. Naime, istraživanje kompanije „Gugl" je pokazalo da čak 77% gledalaca koristi i dodatni uređaj za vreme gledanja televizije [1]. Takodje, razvoj prenosnih uređaja, omogućio je reprodukciju multimedijalnog sadržaja, pa tako sve češće se prenosni uređaji koriste i za gledanje emisija, a ne samo za pretragu interneta. U situaciji kada se televizijski signal distirbuira na prenosne uređaje, sa digitalnog TV prijemnika, te uređaje nazivamo uređajima dodatnog ekrana [2].

Dodatni ekrani se ne koriste samo za pretraživanje interneta u cilju prikupljanja dodatnih informacija već se sve veći broj funkcionalnosti digitalnog TV prijemnika prebacuje na uređaje dodatnog ekrana. Kao posledica, dodatni ekran ima široku upotrebu, pa tako možemo da ga koristimo u funkciji daljinskog upravljača, da kontrolišemo digitalni TV prijemnik, da pregledamo elektronski programski vodič, postavljamo podsetnike, zakazujemo snimanja, pretražujemo multimedijalne sadržaje na digitalnom TV prijemniku, pa čak i da gledamo televizijske servise.

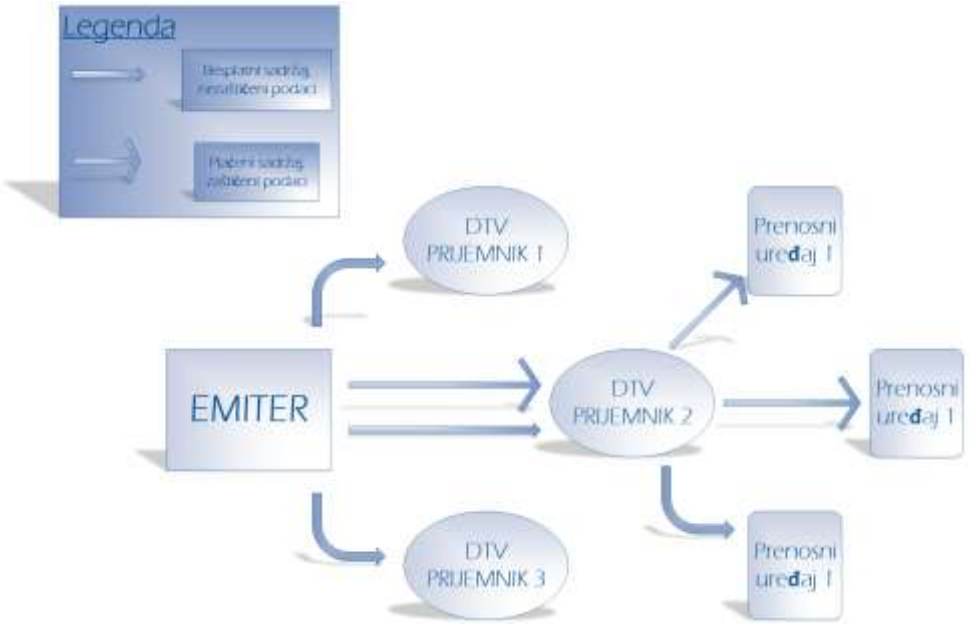
Kada je reč o televizijskim servisima razlikujemo dve grupe TV servisa:

- besplatni sadržaj – dostupan svima, prenosi se bez enkripcije

- plaćeni sadržaj – dostupan samo korisnicima koji su se pretplatili na ove sadržaje, prenosi se enkriptovan

Prema DVB standardima koji određuju emitovanje televizijskog signala utvrđeno je kako se prenose besplatni, a kako plaćeni sadržaji. Ipak ovim standardima nije pokriven slučaj korišćenja kada želimo da primljeni sadržaj prosledimo na uređaj dodatnog ekrana. Dok besplatne sadržaje možemo da distribuiramo na dodatne uređaje bez ikakvih ograničenja, sa plaćenim sadržajima je situacija drugačija. Pošto je pristup plaćenim sadržajima dostupan samo pretplaćenim korisnicima, ovi sadržaji se emituju enkriptovani, a uputstvo za dekripciju kao i svi potrebni resursi za samo dekriptovanje sadržaja se isporučuju pretplaćenim korisnicima. Na taj način se sadržaj štiti od neželjenog pristupa, odnosno onemogućava se pristup plaćenim sadržajima korisnicima koji se nisu pretplatili na njih.

Kada se u sistem uvedu i uređaji dodatnog ekrana zaštita sadržaja se dodatno komplikuje, jer sadržaj više nije potrebno zaštititi samo na digitalnom TV prijemniku, već se zaštita mora obezbediti i tokom distribucije kroz kućnu mrežu kao i na samom uređaju dodatnog ekrana.



Slika 1.1 Protok podataka od emitera do DTV prijemnika i prenosnih uređaja

Naredno poglavlje opisuje neke od standarda i algoritama koji se koriste u zaštiti sadržaja, a koje je potrebno poznavati da bi se razumeo rad.

U trećem poglavlju je izložen koncept predstavljenog rešenja, dok je u četvrtom poglavlju detaljnije opisano programsko rešenje.

Peto poglavlje prezentuje rezultate ovog rada, a zaključak je dat u šestom poglavlju.

Poslednje, sedmo poglavlje daje pregled korišćene literature.

2. Teorijske osnove

U ovom poglavlju su predstavljene teorijske osnove potrebne za razumevanje ostatka rada. Opisane su osnove digitalne televizije i digitalnog TV prijemnika, kao i prenosnog toka koji se koristi za emitovanje sadržaja u okviru digitalne televizije. Takođe su opisane CI+ programska jedinica i DTCP-IP protokol koji su korišćeni za obezbeđivanje sigurne distribucije, kao i neki od najvažnijih kriptografskih algoritama i funkcija.

2.1 Digitalna televizija

Digitalna televizija predstavlja prenos audio i video zapisa, kao i dodatnih informacija u digitalnom format. Prednosti digitalne televizije u odnosu na analognu su pre svega kvalitetniji zvuk i slika. Takođe, digitalna televizija omogućuje prenos više TV servisa na jednoj frekvenciji i uopšte veću količinu informacija. Digitalni TV prijemnici uglavnom poseduju i pristup internet, kao i mogućnost izvršavanja mnogobrojnih aplikacija pisanih u Javi, HTML-u i drugim programskim jezicima, što dovodi do postojanja interaktivne televizije. Takođe, kao posledica veće količine informacija koje se prenose tokom podataka u digitalnoj televiziji gledalac je u mogućnosti da bira između različitih video ili audio zapisa, jezika prevoda na jednom TV servisu, kao i da koristi TV aplikacije poput programskog vodiča ili ličnog video snimača.

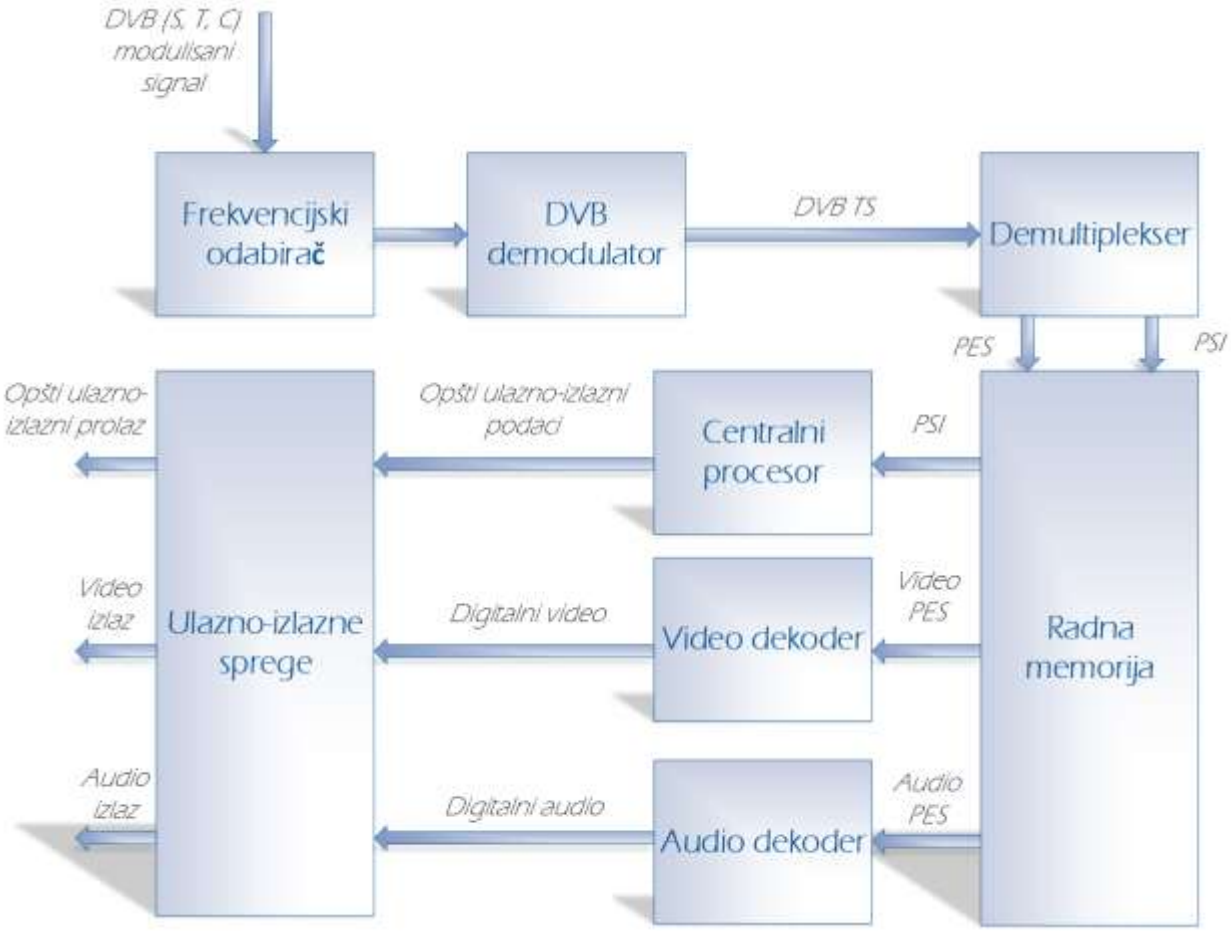
Najznačajniji standardi digitalne televizije su:

- DVB – grupa standarda koja se koristi u Evropi ali i u većem delu sveta
- ATSC – standardi koji se primenjuju u digitalnom TV prenosu zemaljskim vezama u SAD, Kanadi, Meksiku, Južnoj Koreji
- OCAP – standard koji se koristi u SAD u kablovskoj digitalnoj televiziji

ISDB – grupa DTV standarda nastala u Japanu

2.1.1 Digitalni TV prijemnik

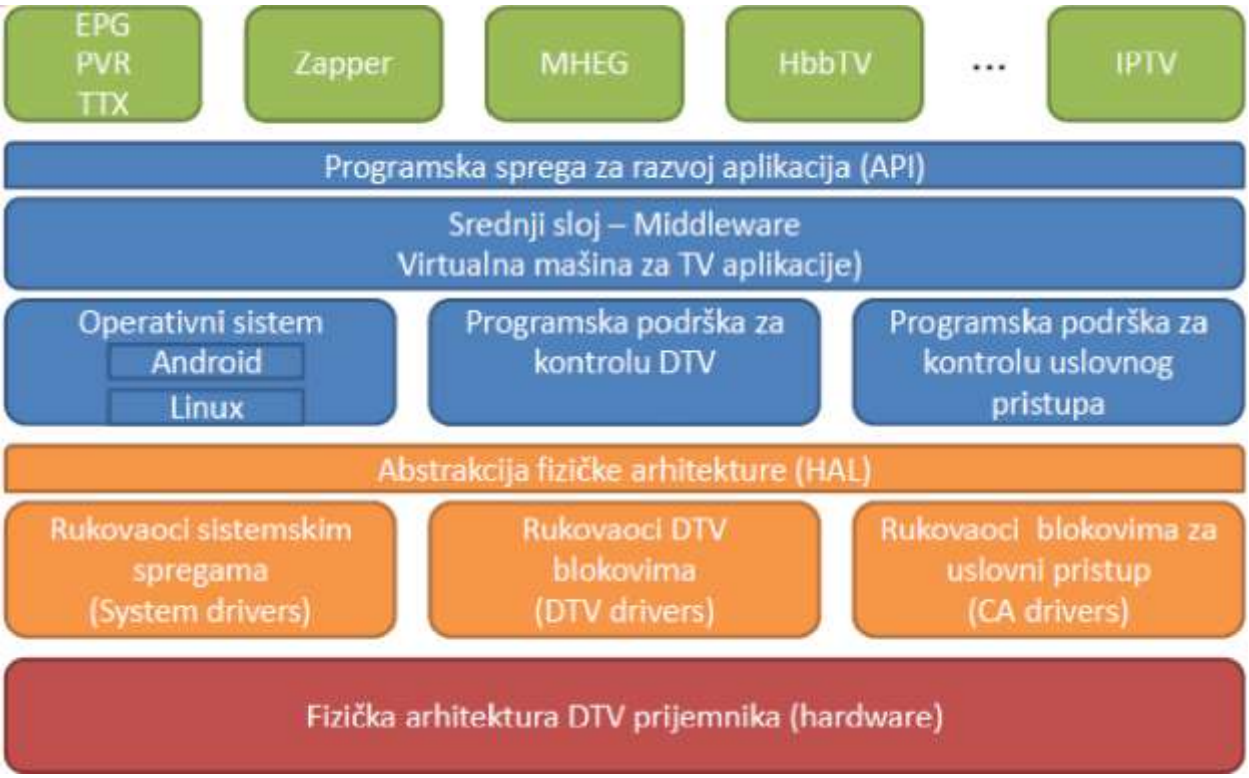
Uobičajena arhitektura DTV prijemnika je prikazana na slici 2.1.



Slika 2.1 Arhitektura DTV prijemnika

Rad svih blokova je kontrolisan i koordinisan od strane centralnog procesora. Modulisani signal stiže u frekvencijski birač čiji je zadatak da izdvoji signal emitovan na frekvenciji zadatoj od strane centralnog procesora. Signal se zatim prosleđuje u odgovarajući demodulator, na osnovu tipa signala (satelitski, kablovski, zemaljski), na čijem izlazu se dobija digitalni signal. Frekvencijski birač i demodulator zajedno čine mrežni sprežni modul (engl. Network interface module – NIM) i često se nalaze u zajedničkom kućištu. Zatim se vrši demultipleksiranje transportnog toka podataka gde se prvo izdvajaju paketi koji sadrže PID-ove zadate od strane centralnog procesora, a zatim se organizuju u elementarne tokove podataka i prosleđuju audio ili video dekoderu ukoliko je reč o audio ili video zapisima, ili centralnom procesoru ukoliko je reč o tabelama.

Što se tiče programske podrške za DTV prijemnike, uobičajeni izgled slojeva programske spodrške je dat na slici 2.2.



Slika 2.2 Programska podrška DTV prijemnika

Najvažniji deo programske podrške, koji sadrži gotovo kompletnu DTV funkcionalnost i omogućava izvršavanje aplikacija, je srednji sloj (engl. Middleware). Uloga srednjeg sloja je da realizuje najvažnije operacije kao što su raščlanjavanje DVB podataka, kontrola pristupa i organizacija servisa, prikupljanje podataka o programima (engl. Event Information Table – EIT), podrška za snimanje, kontrola podsetnika, dekodovanje multimedijalnih sadržaja i drugi, kao i da kontroliše fizičku arhitekturu kroz komunikaciju sa nižim slojevima i da obezbedi potrebne programske sprege ka višim programskim slojevima. Važna osobina sredjeg sloja je da on apstrakuje funkcionalnosti DTV uređaja, fizičke arhitekture i operativnog sistema i na taj način obezbeđuje da proizvođač aplikativne DTV programske podrške ne mora da bude upoznat sa specifičnostima fizičke arhitekture. Drugim rečima srednji sloj formira virtuelnu mašinu na kojoj se izvršava aplikativni deo programske podrške. Ovo takođe garantuje identično izvršavanje iste aplikacije na različitim fizičkim arhitekturama ukoliko se koristi isti srednji sloj.

2.1.2 Prenosni tok

Prenosni tok (eng. Transport Stream, TS) je standardan format za prenos i skladištenje audio i video podataka, kao i podataka vezanih za informacije o programima. TS se koristi u

standardima digitalne televizije kao što su DVB, ATSC i IPTV. Prenosno tok specificira prenosni oblik za enkapsulaciju paketizovanih elementarnih tokova.

Osnovna jedinica za prenos podataka u prenosnom toku je paket. Svaki paket započinje sa sinhronizacionim bajtom i zaglavljem. Dalje može da sledi adaptaciono polje ukoliko postoji i podaci koji se prenose. Dužina paketa je 188 bajta.

Svaka tabela i elementarni tok u okviru transportnog toka su identifikovani pomoću 13-o bitnog identifikatora paketa (eng. Packet Identifier, PID), koji se nalazi u zaglavlju paketa prenosnog toka. Uloga PID-a je da se željeni paket pronađe u okviru prenosnog toka i da se izdvoji od ostalih. Svi paketi koji sadrže podatke vezane za isti elementarni tok ili istu tabelu imaju isti PID.

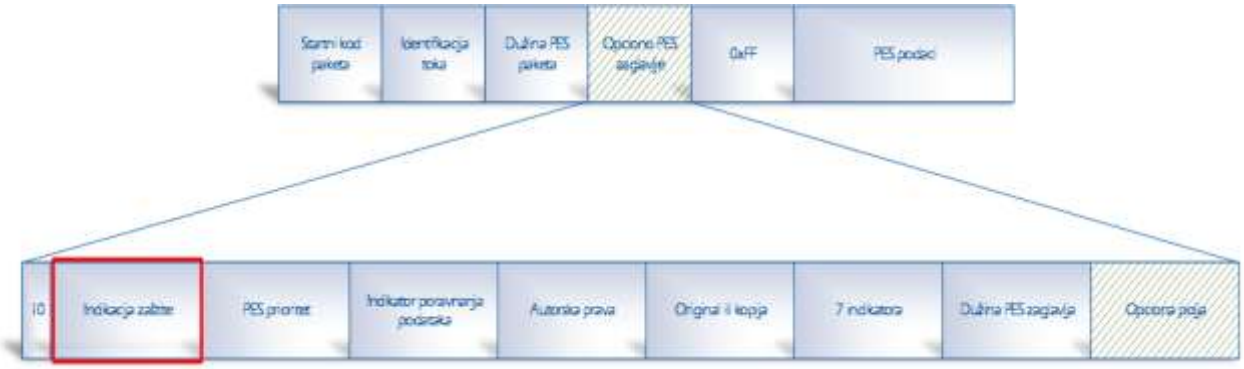
Prenosni tok funkcioniše na konceptu programa. Svaki program je opisan u tabeli mapiranja programa (eng. Program Map Table, PMT) koja poseduje jedinstveni PID. U PMT tabeli se nalaze PID-ovi elementarnih tokova vezanih za program. Spisak svih PMT tabela, kao i njihovi PID-ovi se nalaze u tabeli asociranja programa (eng. Program Association Table, PAT). PAT tabela uvek ima PID 0. PAT i PMT tabele spadaju u tabele informacija specifičnih za programe (eng. Program Specific Information, PSI), a postoje jos dve tabele koje spadaju u ovu grupu i to su tabela uslovnog pristupa (eng. Confitional Access Table, CAT) i tabela mrežnih informacija (eng. Network Information Table).

2.1.3 Indikacija zaštićenog sadržaja u okviru prenosnog toka

U okviru prenosnog toka zaštita može biti uvedena ili na nivou paketa transportnog toka ili na nivou paketizovanog elementarnog toka [3]. Ukoliko je zaštita uvedena na nivou paketa transportnog toka, tada se indikacija o zaštiti sadržaja nalazi u zaglavlju paketa transportnog toka kao sto se može videti na slici 2.3.

Slika 2.3 Zaglavlje paketa transportnog toka

U drugom slučaju, ako je zaštita sadržaja uvedena na nivou paketizovanog elementarnog toka, indikacija o zaštiti se nalazi u opcionom polju zaglavlja paketa kao što se može videti na slici 2.4.



Slika 2.4 Zaglavlje paketa paketizovanog elementarnog toka

U oba slučaja polje za indikaciju zaštite sadržaja je dugačko dva bajta i može imati određene vrednosti čija značenja su prikazana u tabeli 2.1.

Vrednost polja za indikaciju zaštićenog sadržaja	Značenje
00	**Nezaštićen sadržaj**
01	**Rezervisano za buduću upotrebu**
10	**Sadržaj enkriptovan parnim ključem**
11	**Sadržaj enkriptovan neparnim ključem**

Tabela 2.1 Moguće vrednosti polja za indikaciju zaštite sadržaja i njihova značenja

Kao što možemo da vidimo iz tabele, prvi bajt pokazuje da li je sadržaj enkriptovan ili ne, a drugi pokazuje koji ključ je korišćen prilikom enkripcije ukoliko je sadržaj enkriptovan.

2.2 CI+ programska jedinica

CI+ je proširenje CI standarda za zaštitu sadržaja na digitalnim TV prijemnicima[7]. Glavna uloga CI+ programske jedinice je da komunicira sa i kontroliše modul za uslovni pristup. Takodje uloga CI+ programske jedinice je i da zaštiti sadržaj prilikom razmene između modula za uslovni pristup i srednjeg sloja programske podrške digitalnog TV prijemnika, koji se obično odvija preko nezaštićenih fizičkih veza. Baš iz tog razloga se ovaj sadržaj prenosi enkriptovan, jer bi u suprotnom lako moglo da dođe do neželjenog pristupa sadržaju. Pored same zaštite sadržaja, uloga CI+ programske jedinice je i da obezbedi spregu za komunikaciju sa korisnikom.

Kako bi se koristila CI+ programska jedinica neophodno je posedovati CI+ sertifikovan uređaj kojem su dodeljeni validni sertifikati kako bi se uspešno izvršila međusobna autentifikacija između uređaja na kom se nalazi CI+ programska jedinica i modula za uslovni pristup, što je prvi i osnovni korak u funkcionisanju CI+ zaštite. U slučaju da autentifikacija ne može da se izvrši uspešno sva dalja aktivnost se prekida i nije moguće reprodukovati zaštićeni sadržaj.

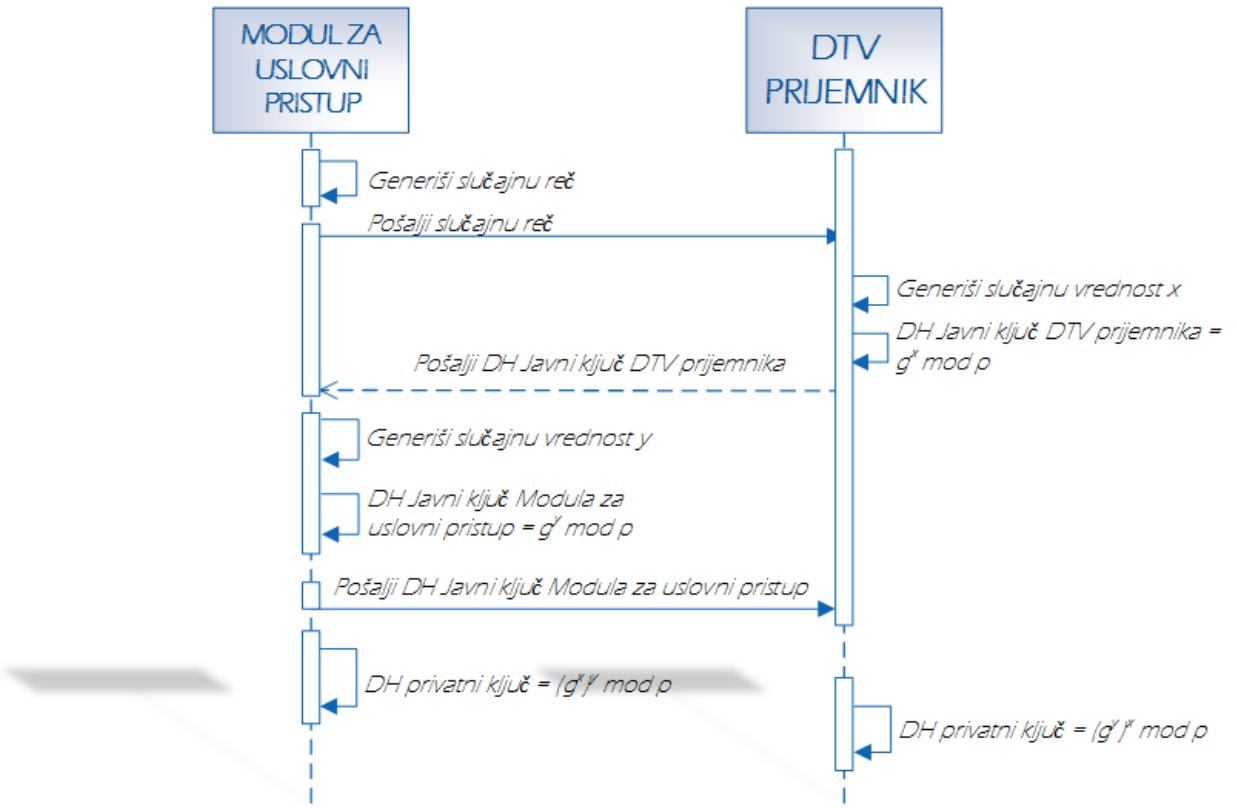
Podržani standardi enkriptovanja podataka od strane CI+ programske jedinice su DES (eng. *Data Encryption Standard*) i AES (eng. *Advanced Encryption Standard*) čiji će načini rada biti objašnjeni u daljem tekstu.

2.2.1 Autentifikacija u okviru CI+

CI+ specifikacija zahteva obostranu autentifikaciju DTV prijemnika i modula za uslovni pristup. Pre nego što se počne sa dekripcijom sadržaja DTV prijemik i modul za uslovni pristup moraju da uspešno da prođu autentifikaciju koja se sastoji iz sledećih koraka:

- modul za uslovni pristup zahteva od DTV prijemnika njegove sertifikate i DTV prijemnik mu ih šalje. Zatim modul za uslovni pristup potvrđuje ispravnost sertifikata uređaja (eng. Device Certificate) koji sadrži jedinstveni identifikacioni kod uređaja i sertifikata grupe (eng. Brand Certificate) kontrolom potpisa.
- DTV prijemnik zahteva od modula za uslovni pristup njegove sertifikate i modul za uslovni pristup mu ih šalje. Zatim DTV prijemnik potvrđuje ispravnost sertifikata uređaja (eng. Device Certificate) koji sadrži jedinstveni identifikacioni kod uređaja i sertifikata grupe (eng. Brand Certificate) kontrolom potpisa.
- modul za uslovni pristuo i DTV prijemnik dokažu da poseduju privatni ključ koji odgovara javnom ključu ugrađenom u sertifikate potpisujući Difi-Helman (eng. Diffie-Hellman, DH) javni ključ i ostale podatke i šaljući potpisane podatke drugoj strani.
- modul za uslovni pristup i DTV prijemnik dokažu da mogu da izračunaju autentifikacioni ključ.

Proces međusobne autentifikacije je zasnovan na DH algoritmu. CI+ programska jedinica koristi DH algoritam u tri prolaza za razmenu ključeva. Uprošćena verzija ovog algoritma je predstavljena na slici 2.5.



Slika 2.5 DH algoritam

Na slici se vidi da obe strane zasebno računaju DH privatni ključ. Pri tom koriste različite privatne vrednosti (x, y) a na kraju izračunaju isti ključ.

Mere zaštite sadržaja prilikom razmene poruka koje sadrže DH parametre između modula za uslovni pristup i DTV prijemnika su:

- modul za uslovni pristup započinje komunikaciju slanjem slučajne reči (eng. nonce), vrednosti koja se generiše na slučajan način i koristi se samo jednom, odnosno samo tokom komunikacije sa jednim uređajem. Ova slučajna reč se koristi tokom celog trajanja komunikacije u potpisu razmenjivanih podataka. Na taj način se uređaji štite od napada ponavljanja (eng. replay attacks).
- modul za uslovni pristup i DTV prijemnik međusobno provere validnost sertifikata drugog uređaja. Na taj način se obezbeđuju da komuniciraju samo sa CI+ sertifikovanim uređajima i takođe potvrđuju da se drugi uređaj koji učestvuje u komunikaciji ne nalazi na listi povučenih uređaja (eng. revoked device).
- poruke koje se razmenjuju između modula za uslovni pristup i DTV prijemnika su zaštićene parom javni-privatni ključ. Pošiljaoc potpisuje svaku poruku svojim privatnim ključem, a primalac potvrđuje uspešan prijem poruke koristeći javni ključ iz sertifikata pošiljaoca.

Nakon uspešne autentifikacije sledi uspostavljanje sigurnog autentifikovanog kanala

(eng. Secure Authenticated Channel, SAC) koji služi za razmenu ključeva i kontrolnih poruka. Po uspostavljanju SAC moguće je pristupiti računanju ključeva za zaštitu sadržaja kojima se kriptuju sami podaci. Kada su uspešno izvršeni svi prethodni koraci sadržaj je zaštićen, i kažemo da se prenosi po ruti poverenja koja je dogovorena između modula za uslovni pristup i DTV prijemnika. Ukoliko jedan od prethodnih koraka nije mogao da sa izvrši uspešno, ceo proces autentifikacije se prekida i modul za uslovni pristup prestaje sa dekriptovanjem sadržaja, odnosno nije moguće reprodukovati sadržaj.

2.3 DTCP-IP

DTCP-IP je tehnologija za upravljanje digitalnim pravima (eng. Digital Rights Management, DRM) koja obezbeđuje sadržaj od neželjenog pristupa u kućnim mrežama [8]. Prvobitno definisana specifikcija se odnosila na zaštitu multimedijalnog sadržaja prilikom razmene između uređaja povezanih serijskim magistralama. Ovu specifikaciju kao i njeno proširenje na internet protokol (DTCP-IP) je definisala grupa DTLA (Digital Transmission Licensing Administrator) koja je i zadužena za izdavanje licenci.

Slično kao i kod CI+, i u komunikaciji između dva DTCP-IP kompatibilna uređaja potrebno je da se uspešno prođe sistem autentifikacije pre nego što se razmeni korisni sadržaj. Kod DTCP-IP postoje dve vrste autentifikacije:

- potpuna autentifikacija i
- ograničena autentifikacija

U ovom radu ćemo se baviti potpunom autentifikacijom koja je iskorišćena u realizaciji rešenja.

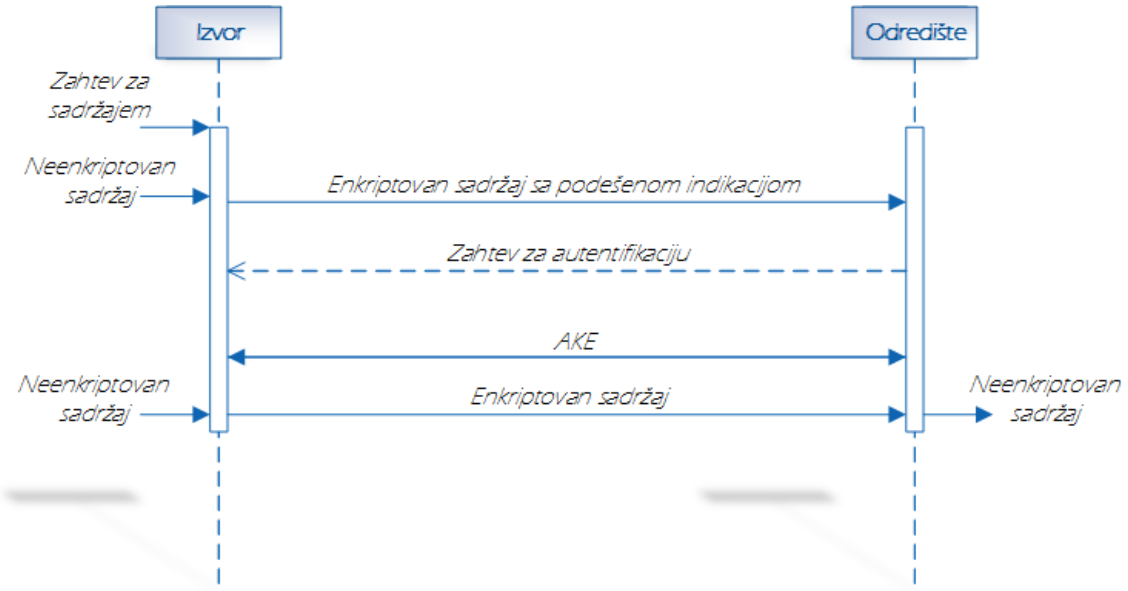
Pored dela koji se bavi autentifikacijom i razmenom ključeva (AKE – Authentication and Key Exchange), DTCP-IP se sastoji i od modula za kontrolu kopiranja, enkripciju sadržaja i obnavljanje sistema.

Modul za kontrolu kopiranja pruža vlasniku sadržaja da ograniči prava u pogledu kopiranja sadržaja, pa tako može da dopusti da se sadržaj iskopira samo jednom ili da potpuno zabrani kopiranje sadržaja. Informacije o kontroli kopiranja se ugrađuju ili u EMI (eng. Encryption Mode Indicator) poruke ili u sam tok podataka, npr. MPEG-TS.

Sadržaj se prenosi u enkriptovanom obliku i iz tog razloga svaki uređaj sa DTCP-IP licencom mora da podržava osnovne kriptografske algoritme propisane specifikacijom kako bi bio sposoban da enkriptuje i dekriptuje sadržaj. Pored osnovnih algoritama, moguća je i podrška za dodatne algoritme, a dogovor o korišćenim kriptografskim algoritmima se postiže između uređaja koji učestvuju u DTCP-IP komunikaciji.

Uređaji koji podržavaju potpunu autentifikaciju imaju mogućnost da primaju SRM (eng. System Renewability Messages) koje kreira DTLA i koje im pružaju dugoročnu sigurnost. Kroz ove poruke se prosleđuju informacije o kompromitovanim uređajima i na taj način se ti uređaji, kao i njihovi sertifikati, označavaju kao nevalidni, čime se štite ostali korisnici.

Pregled zaštite podataka je dat na slici 2.6.



Slika 2.6 Zaštita podataka DTCP-IP protokolom

Kao što se može videti na slici komunikacija se odvija između dva uređaja. Uređaj koji obezbeđuje podatke se naziva izvor (eng. Source), a uređaj koji prima podatke se naziva odredište (eng. Sink). Odredište započinje komunikaciju slanjem zahteva za podacima. Izvor odgovara slanjem enkriptovanih podataka i indikacije o kontroli kopiranja od strane izvora ka odredištu. U slučaju da su zahtevani podaci zaštićeni, izvor može da šalje prazne poruke uz indikaciju o kontroli kopiranja dok se ne prođe autentifikacija. Po prijemu paketa odredište ispituje bite koji nose indikaciju o kontroli kopiranja i zatim šalje izvoru zahtev za potpunom ili ograničenom autentifikacijom. Posle uspešne autentifikacije izvor i odredište razmenjiju ključ koji će se koristiti sa jedne strane za enkripciju, a sa druge za dekripciju sadržaja.

2.3.1 Autentifikacija u okviru DTCP-IP

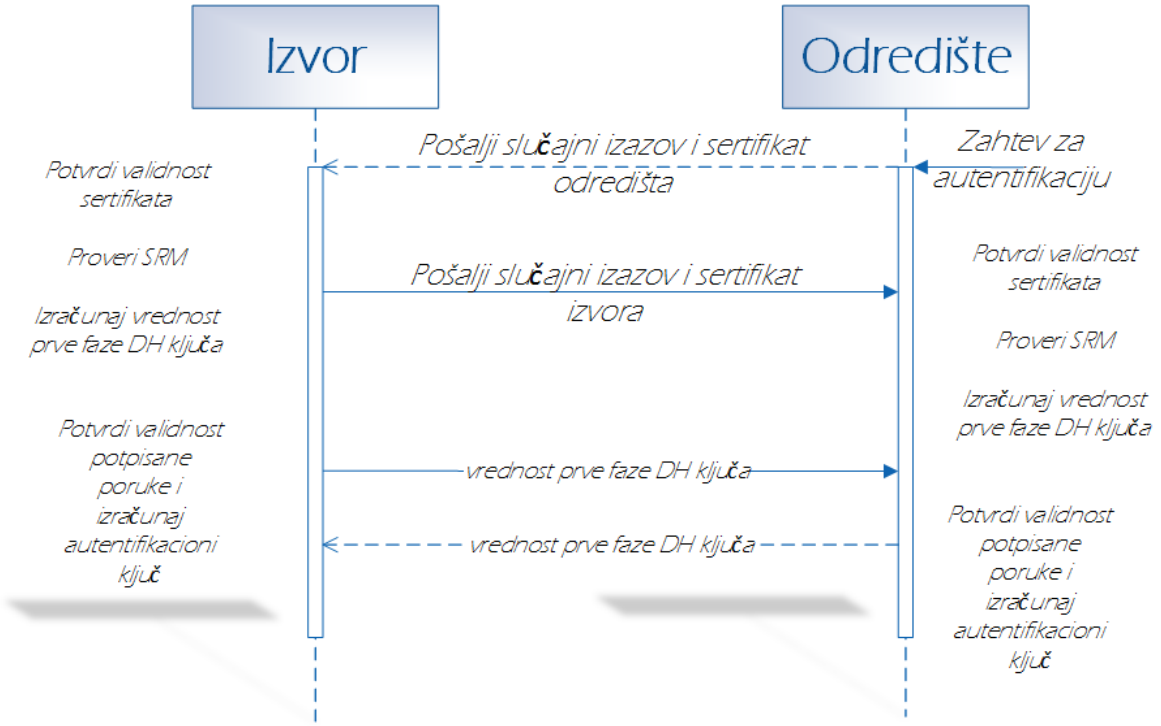
Kao što je već pomenuto u ovom radu će biti razmotrena samo potpuna autentifikacija koja je iskorišćena u realizaciji. Potpuna autentifikacija koristi sledeće kriptografske algoritme i funkcije:

- SHA-1 (Secure Hash Algorithm)
- RND (Random) generator - generator slučajnog broja

- EC-DH algoritam
- EC-DSA algoritam

Ovi algoritmi i funkcije će biti detaljnije objašnjeni u daljem tekstu.

Slika 2.7 prikazuje dijagram toka potpune autentifikacije.



Slika 2.7 DTCP-IP potpuna autentifikacija

Odredišni uređaj započinje autentifikaciju slanjem slučajnog izazova i svog sertifikata. Ovo može da se desi kao posledica pokušaja pristupu sadržaja koji ima podešenu kontrolu kopiranja ili zahtev za autentifikaciju može da stigne unapred, pre zahteva za bilo kakvim sadržajem. U drugom slučaju, ako zahtev za autentifikaciju prethodi zahtevu za podacima, izvor može da odbije zahtev.

Ukoliko je zahtev prihvaćen, izvor odgovara sa slučajnim izazovom i svojim sertifikatom. Nakon razmene slučajnih izazova i sertifikatasvaki uređaj proverava integritet drugog uređaja pomoću EC-DSA. Ukoliko se potpisi sertifikata pokažu kao ispravni prema DTLA, sledeći korak je da se proveri da li se dati uređaj nalazi na listi opozvanih uređaja koja se nalazi u okviru poruka o obnovljivosti sistema (SRM). Ukoliko nijedan od uređaja koji učestvuju u komunikaciji nije opozvan, pristupa se računanju vrednosti prve faze EC-DH ključa.

Po izračunavanju ove vrednosti razmenjuju se poruke koje sadrže pomenutu vrednost kao i verziju poruke o obnovljivosti sistema i slučajni izazov drugog uređaja. Ove poruke su potpisane prema EC-DSA. Po prijemu datih poruka svaki uređaj proverava validnost potpisa na osnovu javnog ključa drugog uređaja. Ukoliko se ispostavi da potpisi nisu validni, komunikacija se prekida. U suprotnom izračunava se do kraja EC-DH ključ.

Takođe, ukoliko se ustanovi da neki od uređaja poseduje noviju verziju SRM poruke dolazi i do razmene ovih poruka kako bi oba uređaja posedovala najnoviju SRM poruku.

Posle uspešno završene autentifikacije može se pristupiti razmeni podataka. Ovi podaci se prenose enkriptovani AES standardom.

2.3.2 DTCP-IP sertifikat

Kao što se može videti glavni indikator da uređaj podržava DTCP-IP je posedovanje sertifikata. Sertifikati se izdaju od strane DTLA i svaki uređaj čuva svoj sertifikat i koristi ga prilikom autentifikacije. Format sertifikata je prikazan na slici 2.8.

Slika 2.8 DTCP-IP sertifikat

DTCP-IP sertifikat se sastoji od sledećih polja:

- Tip sertifikata (4 bita) – za sada jedina definisana vrednost je 0 koja označava DTCP sertifikat. Ostale vrednosti su rezervisane za buduću upotrebu.
- Format sertifikata (4 bita) – za sada su definisane tri vrednosti:
  1. 0 – ograničena autentifikacija
  2. 1 – osnovna potpuna autentifikacija
  3. 2 – proširena potpuna autentifikacija

  ostale vrednosti su rezervisane za budućnost
- Generacija uređaja (4 bita) – ovo polje označava koju generaciju SRM poruka uređaj može da primi
- Rezervisana polja (11 bita) – rezervisana za budućnost, trenutno definisana na vrednost 0
- Dodatna lokalizacija (1 bit) – ukoliko uređaj podržava testove dodatne lokalizacije postavi se na 1, u suprotnom na 0
- Autentifikacioni prenosnik (1 bit) – ukoliko je ovo polje postavljeno na 1 to označava da dati uređaj ima ulogu prenosnika između druga dva DTCP-IP uređaja, odnosno da ono što primi od jednog uređaja prema kome se odnosi kao odredište, prosledi drugom prema kome se odnosi kao izvor

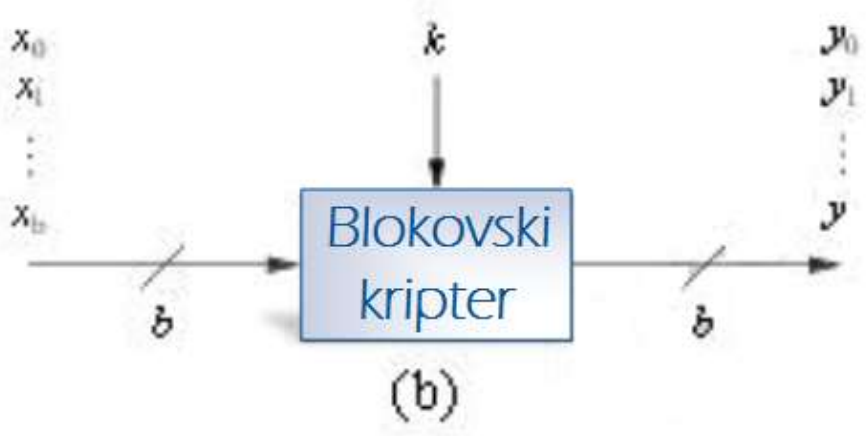
- Identifikacioni broj uređaja (40 bita) – dodeljuje ga DTLA
- EC-DSA javni ključ (320 bita)
- EC-DSA potpis svih prethodnih podataka (320 bita)

2.4 Kriptografski algoritmi i funkcije

U ovom poglavlju je dat pregled nekih osnovnih kriptografskih funkcija i algoritama koje se koriste u sklopu CI+ i DTCP-IP.

2.4.1 Blokovski kripteri

Blokovski kripteri spadaju u simetrične kriptere, što znači da koriste isti ključ za enkodovanje i dekodovanje podataka. Iz samog imena, blokovski je jasno da rade na bloku podataka predefinisane veličine. Za svaki blok podataka, koristi se drugi ključ. Najčešće dužine blokova su 128 bita, što je slučaj kod AES ili 64 bita što je slučaj kod DES [9].



Slika 2.9 Blokovki kripter

2.4.1.1 DES-56-EBC

DES standard je jedan od najpopulanijih kriptografskih standarda poslednjih 30 godina. Iako danas nije najsigurniji, i dalje se koristi u nekim starijim aplikacijama. Takođe trostruka uzastopna upotreba DES standarda za kriptovanje predstavlja jaku zaštitu. Ovaj metod se naziva 3DES (Triple DES). Pored toga DES standard je uticao na razvoj mnogih drugih standarda.

DES standard koristi ključ dužine 56 bita i radi nad blokom veličine 64 bita. Enkripcija se odigrava u 16 prolaza i u svakom se vrše iste operacije, ali sa drugim ključevima. Svi ključevi su ipak izvedeni iz istog glavnog ključa.

Blokovski kripteri mogu da rade u različitim modovima. Tako DES kripter koji se koristi u CI+ radi u EBC modu. To znači da se podaci podele na blokove dužine 64 bita i svaki blok se kriptuje zasebno, bez uticaja ostalih blokova.

Enkripciju podataka sa DES-56-EBC kripterom se može opisati sledećom formulom:

- $S(m) = E_{DES\text{-}56\text{-}EBC}\ \{CCK\}b(m)$

gde je:

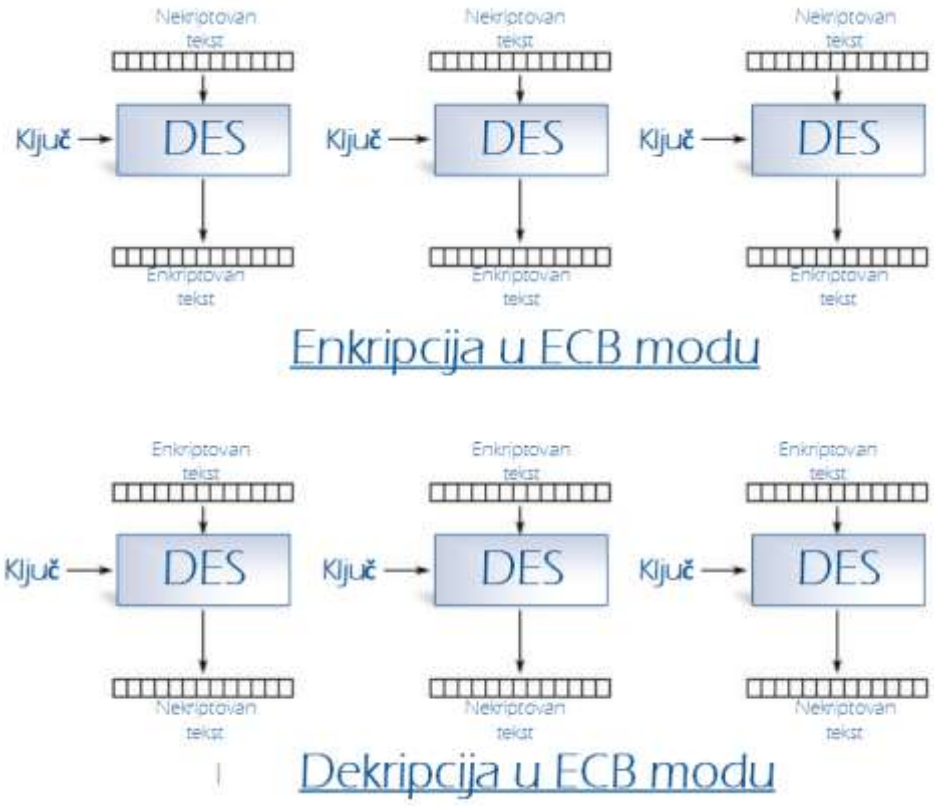
- S(m) m-ti blok enkriptovanih podataka
- $E_{DES\text{-}56\text{-}EBC}$ operacija enkriptovanja
- CCK ključ koji se koristi za enkripciju
- b(m) m-ti blok početnih podataka

Dekripcija se može predstaviti formulom:

- $b(m) = D_{DES\text{-}56\text{-}EBC}\ \{CCK\}S(m)$

gde je $D_{DES\text{-}56\text{-}EBC}$ operacija dekriptovanja, a ostalo je isto kao i u prethodnom primeru.

Grafički prikaz enkriptovanja i dekriptovanja podataka sa DES-56-EBC je dat na slici 2.10.



Slika 2.10 Enkriptovanje i dekriptovanje podataka korišćenjem DES-56-EBC

2.4.1.2 AES-128-CBC

AES standard je danas najrasprostranjeniji standard za kriptovanje koji radi sa simetričnim ključevima. Kao takav koristi se i u mnogim komercijalnim standardima kao što su IPsec (Internet security standard), TLS, IEEE 802.11 i drugi.

Prema standardu AES mora da podržava tri dužine ključa, 128, 192 i 256 bita. Radi nad blokom dužine 128 bita. Broj prolaza je funkcija dužine ključa i predstavljen je u tabeli 2.2.

Dužina ključa u bitima	Broj prolaza
128	10
192	12
256	14

Tabela 2.2 Zavisnost broja prolaza od dužine ključeva u AES

Kao i DES i AES može da radi u različitim modovima, a u okviru CI+ i DTCP-IP se koristi CBC mod sa dužinom ključa od 128 bita. U ovom modu izlaz enkriptovanja bloka se koristi pri enkripciji sledećeg bloka. Za prvi blok koji se enkriptuje koristi se vektor za inicijalizaciju (eng. Initialization Vector, IV).

Enkripciju podataka sa AES-128-CBC kripterom se može opisati sledećim formulama:

- $S(1) = E_{AES\text{-}128\text{-}CBC}\ \{CCK\}[b(1) \oplus IV]$
- $S(m) = E_{AES\text{-}128\text{-}CBC}\ \{CCK\}[b(m) \oplus S(m-1)]$ za $m=2,...,M$

gde je:

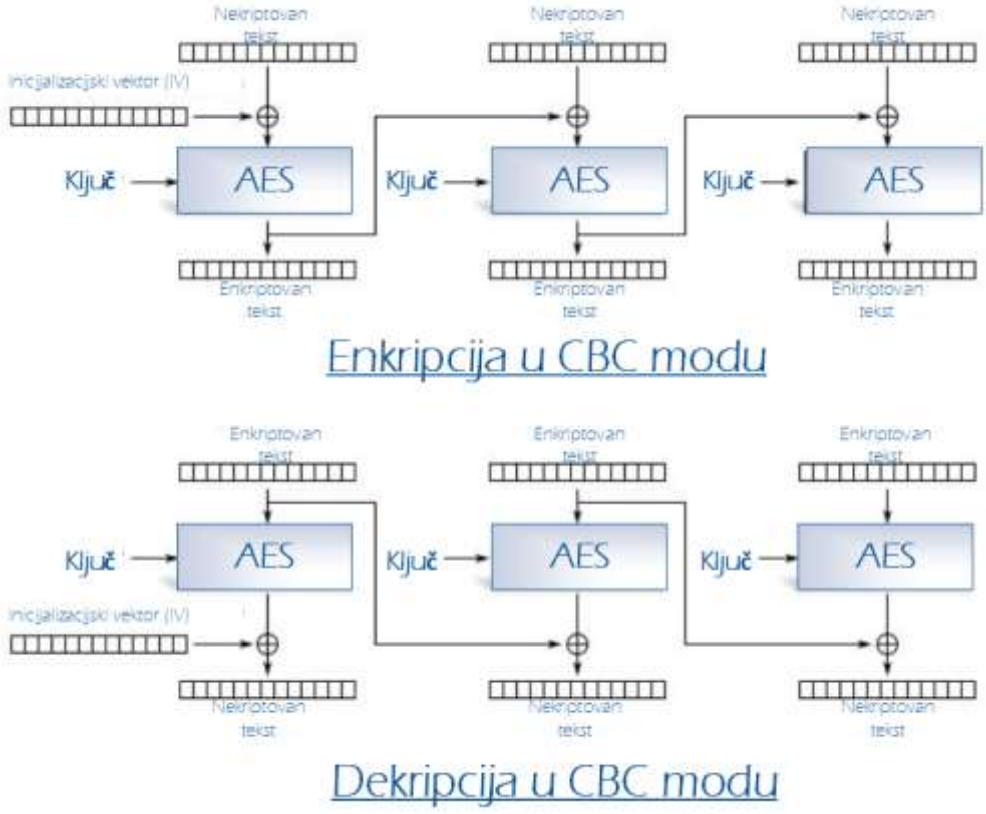
- S(m) m-ti blok enkriptovanih podataka
- $E_{AES\text{-}128\text{-}CBC}$ operacija enkriptovanja
- CCK ključ koji se koristi za enkripciju
- b(m) m-ti blok početnih podataka
- S(m-1) prethodni blok enkriptovanih podataka
- IV vektor za inicijalizaciju

Dekripcija se može predstaviti sledećim formulama:

- $S(1) = D_{AES\text{-}128\text{-}CBC}\ \{CCK\}[b(1) \oplus IV]$
- $S(m) = D_{AES\text{-}128\text{-}CBC}\ \{CCK\}[b(m) \oplus S(m-1)]$ za $m=2,...,M$

gde je $D_{AES\text{-}128\text{-}CBC}$ operacija dekriptovanja, a ostalo je isto kao u prethodnom primeru.

Grafički prikaz enkriptovanja i dekriptovanja podataka sa AES-128-CBC je dat na slici 2.11.



Slika 2.11 Enkriptovanje i dekriptovanje podataka korišćenjem AES-128-CBC

2.4.1.3 Enkriptovanje blokovskim kripterima u okviru CI+ i DTCP-IP

U okviru CI+ i DTCP-IP ne enkriptuju se celi TS paketi, već samo podaci, dok se zaglavlja i adaptaciona polja prenose neenkriptovana. Kako blokovski kripteri rade sa predefinisanim veličinama blokova, može da se desi da količina podataka koja treba da se enkriptuje nije deljiva sa veličinom bloka, odnosno da postoji određen broj celih blokova i ostatak. U tom slučaju se deo podataka koji predstavlja ostatak prenosi neenkriptovan, dok ostali podaci enkriptuju na prethodno opisan način.

2.4.2 Kriptografija eliptične krive

Kriptografija eliptične krive (ECC) je pristup kriptografiji javnih ključeva zasnovana na algebarskim strukturama eliptičnih krivih nad konačnim poljima. Od funkcija ECC u CI+ i DTCP-IP se koriste EC-DH i EC-DSA.

2.4.2.1 EC-DH

Difi-Helman razmena ključeva omogućava korisnicima koji nemaju nikakvog predznanja jedan o drugom da se dogovore o tajnom ključu preko javnog kanala [10].

- Algoritam započinje tako što se učesnici u komunikaciji dogovore o dva slučajna broja p i g koje će koristiti.
- Sledeći korak je da svaki od korisnika, korisnik 1 i korisnik 2, izabere svoj tajni broj a i b respektivno. Ovi brojevi se čuvaju kao tajni.
- Zatim sledi računanje vrednosti prve faze DH razmene ključeva po formuli A= $g^a \bmod p$ i B= $g^b \bmod p$ i njihova razmena.
- Po prijemu A odnosno B korisnici računaju tajni broj S po formuli S= $B^a \bmod p$ za korisnika 1, odnosno S= $A^b \bmod p$ za korisnika 2.

Posle ovih koraka korisnici 1 i 2 dele tajnu S koja se može iskoristiti kao ključ u daljoj komunikaciji. Tabela 2.3 daje pregled tajnih i javnih podataka u okviru DH razmene ključeva u svakom koraku algoritma.

Korisnik 1				Korisnik 2		
Tajno	Javno	Računa	Šalje	Računa	Javno	Tajno
a	p, g		p, g →			b
a	p, g, A	A= $g^a \bmod p$	A→		p,g	b
a	p, g, A		←B	B= $g^b \bmod p$	p,g,A,B	b
a, S	p,g,A,B	S= $B^a \bmod p$		S= $A^b \bmod p$	p,g,A,B	b, S

Tabela 2.3 DH razmena ključeva

2.4.2.2 EC-DSA

DSA je standard za digitalne potpise[11].

Prva faza algoritma digitalnog potpisa je generisanje ključeva. Ova faza se sastoji iz dve pod faze:

- izbor parametara
  - izbor heš (eng. Hash) funkcije H, npr SHA-1
  - izbor dužine ključeva L i N
  - izbor N-bitnog broja q, gde N mora biti manji ili jednak izlazu H

  - izbor L-bitnog broja p, koji će se koristiti za osnovu brojnog sistema, takvog da je p-1 umnožak od q
  - izbor broja g, koji kada se podigne na stepen q po modulu p iznosi 1
- generisanje ključeva
  - izbor slučajnog broja x, gde je $0<x<q$
  - računanje $y=g^x \bmod p$
  - privatni ključ je uređena četvorka (p,q,g,y), a privatni ključ je x

Druga faza je samo potpisivanje poruke.

- generisanje slučajne vrednosti k po poruci, gde je $0<k<q$
- računanje $r=(g^k \bmod p) \bmod q$
- ukoliko je r=0, izabrati drugo k i početi iz početka
- računanje $s=k^{-1}(H(m)+xr) \bmod q$, gde je m poruka koja se potpisuje
- ukoliko je s=0, izabrati drugo k i početi iz početka
- potpis je uređeni par (r,s)

Treća faza je verifikacija ispravnosti potpisa po prijemu poruke.

- odbaciti potpis ukoliko neki od uslova $0<r<q$ i $0<s<q$ nije zadovoljen
- računanje $w=s^{-1} \bmod q$
- računanje $u_1=H(m)*w \bmod q$
- računanje $u2=r*w \bmod q$
- računanje $v=((g^{u}{}_1 y^{u}{}_2) \bmod p) \bmod q$
- ako je v=r potpis je validan

2.4.3 SHA-1 i RNDG

SHA-1 je kriptografka funkcija definisana u [12]. Uloga SHA funkcija je da izmene podatke koji im se pošalju i vrate kao izlaz nove podatke određene dužine.

Pored SHA funkcija u okviru ostalih kriptografskih funkcija se često koriste i generatori slučajnih brojeva (RNDG).

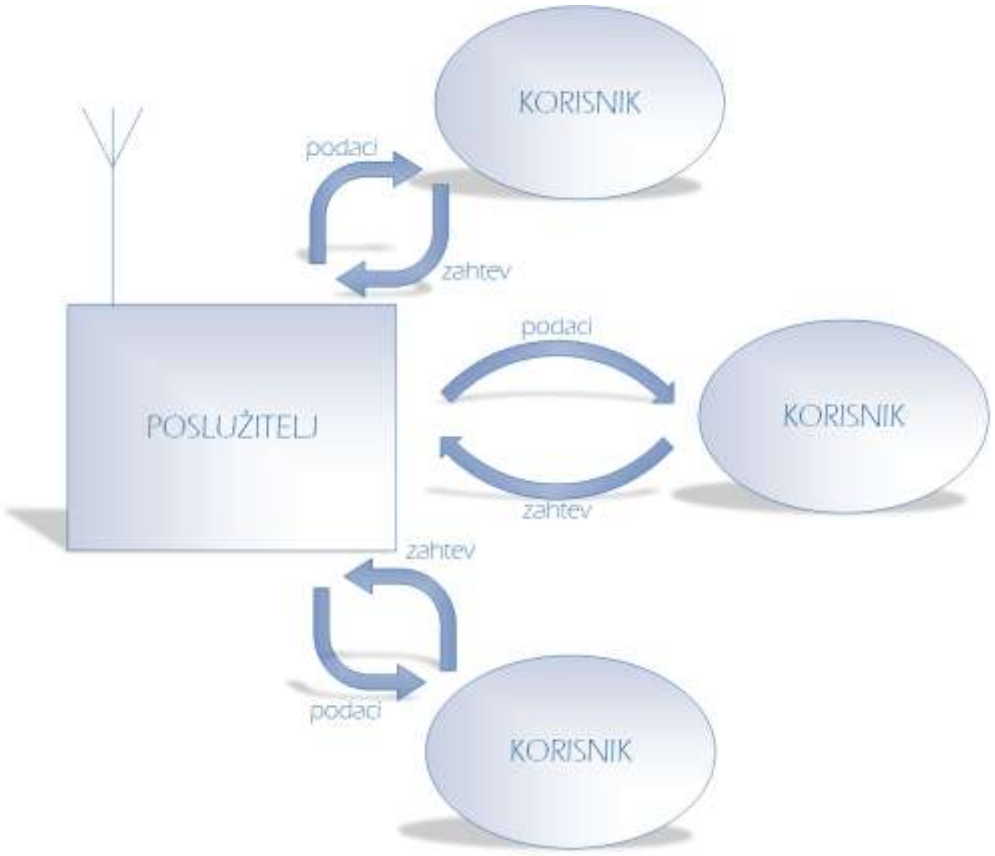
3. Koncept rešenja

U ovom poglavlju je predstavljen koncept rešenja sigurne distribucije plaćenog sadržaja u okruženju dodatnog ekrana koje je predloženo u ovom radu. Pomenuto rešenje treba da obezbedi sigurnu distribuciju sadržaja od modula za uslovni pristup, koji predstavlja ulaznu tačku sistema u slučaju zaštićenog sadržaja, do modula za reprodukciju ili distribucionog poslužitelja ukoliko se sadržaj prosleđuje na dodatni ekran.

3.1 Arhitektura sistema

Sistem za distribuciju plaćenog sadržaja na uređaje dodatnog ekrana se sastoji od digitalnog TV prijemnika koji ima ulogu poslužioca i dodatnog ekrana koji ima ulogu korisnika. Modul za uslovni pristup može da bude sastavni deo digitalnog TV prijemnika, a može kao u slučaju koji je opisan u ovom radu da predstavlja dodatak na digitalni TV prijemnik povezan preko USB-a. Najčešći slučaj povezivanja modula za uslovni pristup sa digitalnim TV prijemnikom je preko CI (eng. Common Interface) sprege koja predstavlja specijalni slučaj PCMCI sprege, pa je u našem slučaju bilo potrebno napisati poseban rukovaoc za komunikaciju sa modulom za uslovni pristup preko USB-a posredstvom libusb biblioteke. Dodatni dodatak na programsku podršku predstavlja i CI+ programska jedinica koja ima zadatak da komunicira sa modulom za uslovni pristup i da ga kontroliše. Takođe, u okviru srednjeg sloja programske podrške digitalnog TV prijemnika se nalaze distribucioni poslužilac i DLNA poslužilac koji imaju ulogu u komunikaciji sa uređajem dodatnog ekrana pri DTCP-IP prenosu. Naime, indikacija o zaštićenom sadržaju DTCP-IP-om se propagira kroz DLNA, a sam prenos podataka se obavlja putem distibucionog servera. Na slici 3.1 je predstavljen sistem u okreženju dodatnog

ekrana sa najvišeg nivoa apstrakcije. Kao što se jasno vidi sa slike u pitanju je arhitektura poslužilac-korisnik.

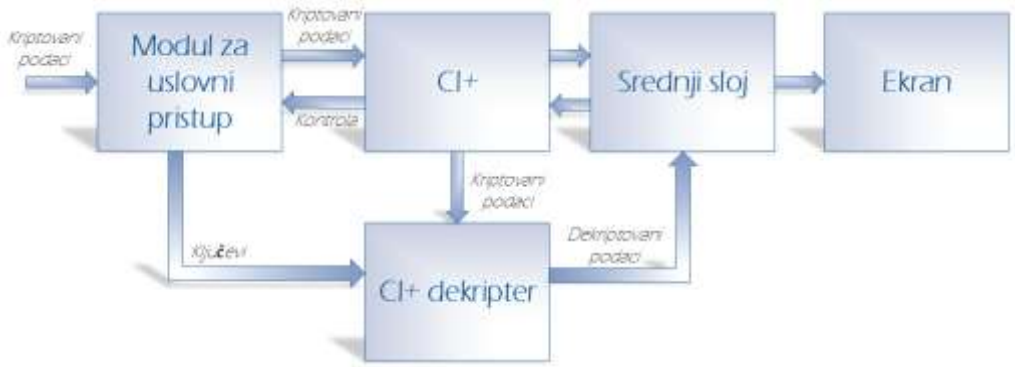


Slika 3.1 Arhitektura sistema poslužilac-korisnik

3.2 Arhitektura digitalnog TV prijemnika

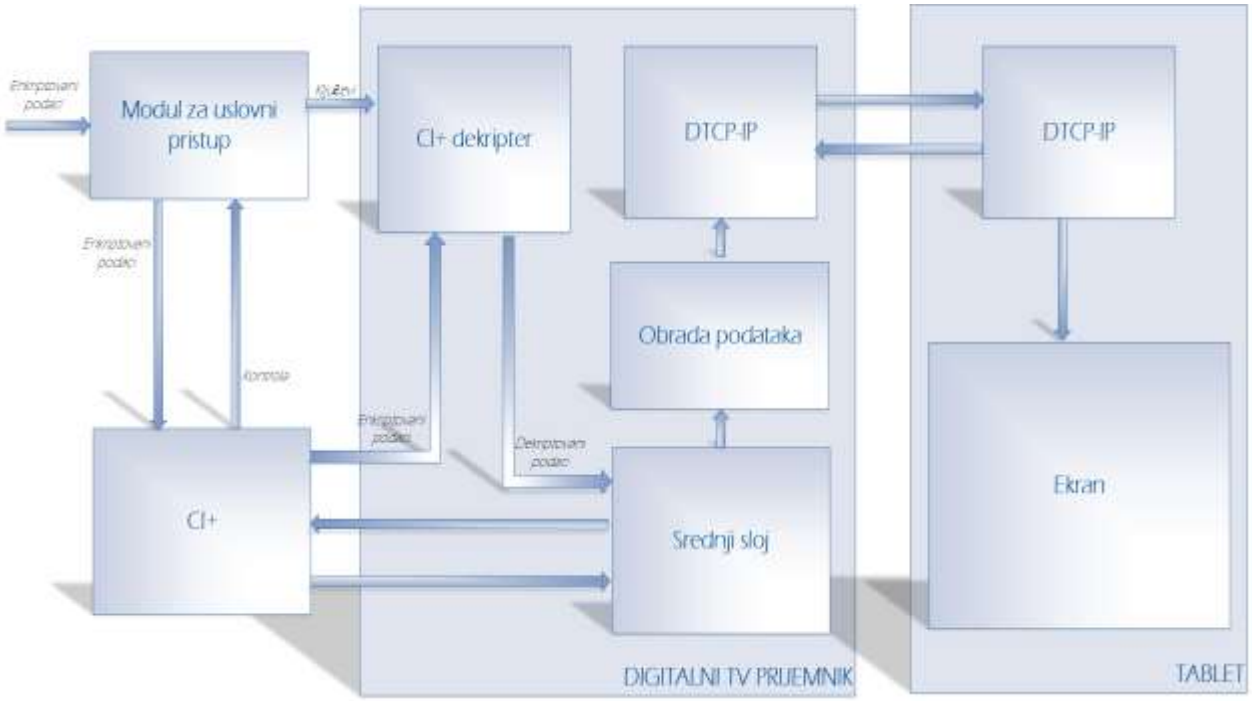
Za razliku od uobičajene realizacije CI+ programske jedinice na digitalnom TV prijemniku koji ne podržava okruženje dodatnog ekrana, koja je prikazana na slici 3.2, realizacija u okruženju dodatnog ekrana zahteva određena proširenja. Kao što se može videti na slici enkriptovani podaci dolaze do modula za uslovni pristup, koji predstavlja ulaznu tačkuu sistema, zatem se kroz komunikaciju između CI+ programske jedinice I modula za uslovni pristup, podaci dekriptuju. Za dekriptovanje podataka je zadužen CI+ dekripter. Njegova uloga je da dekriptuje podatke enkriptovane DVB enkripcijom, ali i da ih opet enkriptuje, ovog puta prema AES standard, kako bi se podaci preneli zaštićeni do ostatka srednjeg sloja programske podrške. Odatle se podaci usmeravaju na dekoder, koji uglavnom sadrži realizaciju u fizičkoj arhitekturi za dekriptovanje AES enkriptovanih podataka. Krajnji rezultat je prikaz izdekodovanog sadržaja na izabranom izlazu. Za ovakav prenos sadržaja kažemo da je prenos po ruti poverenja. Ruta

poverenja se unapred dogovara, i u ovom dogovoru učestvuju modul za uslovni pristup, CI+ programska jedinica i srednji sloj programske podrške DTV prijemnika.



Slika 3.2 Uobičajena realizacija CI+ programske jedinice na DTV prijemniku

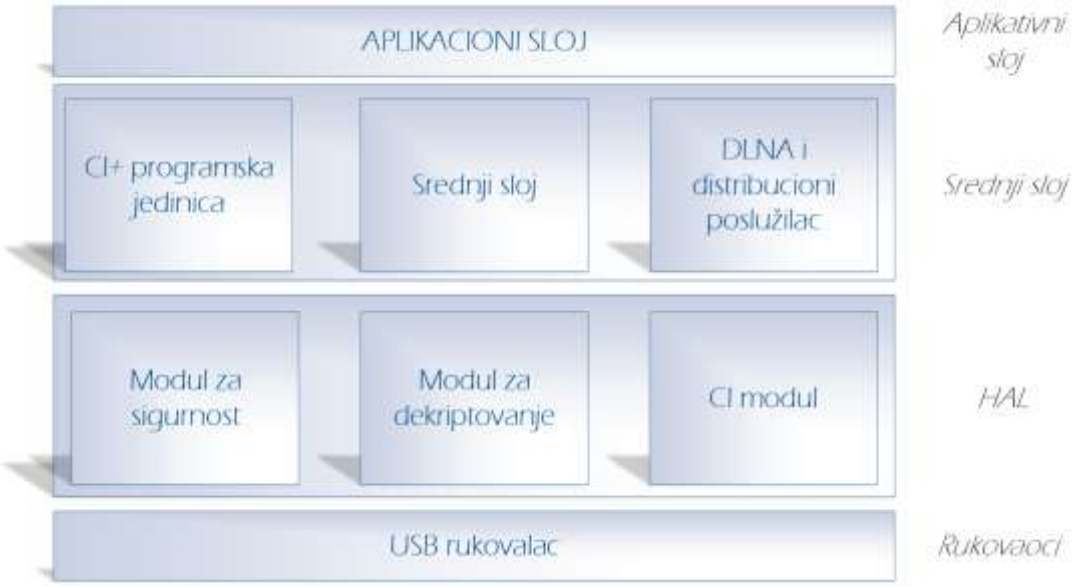
Za razliku od ovog rešenja arhitektura digitalnog TV prijemnika se menja u okruženju dodatnog ekrana samim tim što se mora proširiti sa distribucionim serverom koji predstavlja osnovnu spregu za komunikaciju sa uređajem dodatnog ekrana. Ukoliko se radi o zaštićenom sadržaju koji treba proslediti do korisnika, potrebno je uvesti I dodatnu zaštitu tokom samog prenosa korišćenjem nekog DRM-a kao što je DTCP-IP. Nekoliko načina realizacije CI+ programske jedinice i DTCP-IP protokola na digitalnom TV prijemniku u okruženju dodatnog ekrana su predstavljeni u [15]. Osnovni gradivni blokovi rešenja čija je realizacija prikazana u ovom radu su prikazani na slici 3.3.



Slika 3.3 Arhitektura digitalnog TV prijemnika u okruženju dodatnog ekrana

Sa slike se vide da kao i u slučaju kod digitalnog TV prijemnika koji se ne nalazi u okruženju dodatnog ekrana, ulaznu tačku sistema predstavlja modul za uslovni pristup. Takođe putanja kojom se prenose podaci se ne razlikuje do dela kada se podaci prosleđuju programskoj podršci srednjeg sloja. U ovom slučaju podaci se od srednjeg sloja prenose do bloka za prenos DTCP-IP protokolom. Treba istaći i blok za obradu podataka koji može da prethodi transferu podataka DTCP-IP protokolom. Ovaj blok je veoma značajan. Njegova uloga je da prevede podatke u oblik pogodan za reprodukciju na uređaju dodatnog ekrana. Ovo je posebno važno ako se uzme u obzir ograničen broj kodeka i formata podržanih od uređaja dodatnog ekrana. Sa slike se može videti da je potrebno realizovati i DTCP-IP blok na korisničkoj strain, kako bi uređaj dodatnog ekrana mogao da prihvati podatke prenesene ovim protokolom, da ih dekriptuje i na kraju prikaže. U ovom slučaju ruta poverenja po kojoj se prenose podaci se proširuje da obahvati i DTCP-IP blok, kao i blok za obradu podataka ukoliko se on koristi. To znači da se podaci enkriptovani AES algoritmom sa izlaza modula za uslovni pristup prenose do DTCP-IP bloka ili bloka za obradu podataka u takvom obliku. Ukoliko se ne koristi blok za obradu podatka podaci se dekriptuju u okviru DTCP-IP bloka, a zatim ponovo enkriptuju AES algoritmom, ali ovaj put ključevima dogovorenim između DTCP-IP izvora i odredišta. Ukoliko se koristi blok za obradu podataka, putanja je nešto drugačija. Ovaj blok se sastoji od dekodera i enkodera na kojima se nalaze delovi fizičke arhitekture zaduženi za dekriptovanje i enkriptovanje i ovi delovi fizičke arhitekture su fizički zaštićeni od neželjenog pristupa. Iz tog razloga možemo da izvršimo dekripciju, dekodujemo podatke, zatim ih enkodujemo u drugi format, pa ponovo enkriptujemo istim ključevima, bez narušavanja sigurnosti podataka. U ovom slučaju ruta poverenja je modifikovana u odnosu na prethodni slučaj, jer je produžena da obuhvati i DTCP-IP blok, odnosno i prenos podataka do korisnika. Samim tim, u dogovoru o ruti poverenja učestvuje i DTCP-IP blok.

Kako je akcenat ovog rada na sigurnosti podataka tokom distribucije, najvažniji delovi sistema sa tog aspekta su modul za uslovni pristup, CI+ programska jedinica i DTCP-IP. Na slici 3.4 je prikazana slojevita programska podrška, na kojoj su prikazani najvažniji delovi sistema, a posebno su istaknuti delovi koji su potrebni za realizaciju CI+ programske jedinice i DTCP-IP-a.



Slika 3.4 Slojeviti prikaz programske podrške sa istaknutim modulima od značaja za CI+ i DTCP-IP

Kao što je već pomenuto, umesto uobičajenih CI veza za komunikaciju sa modulom za uslovni pristup, korišćene su USB veze, pa je stoga potrebno da se koristi libusb biblioteka za tu komunikaciju. Što se tiče sloja apstrakcije fizičke arhitekture (eng. Hardware Abstraction Layer, HAL), moduli bitni za CI+ i modul za uslovni pristup su sigurnosni modul, modul za dekriptovanje koji su potrebni CI+ programskoj jedinici, i CI modul koji predstavlja rukovaoca za modul za uslovni pristup odnosno kroz ovaj modul se komunicira sa modulo za uslovni pristup posredstvom libusb biblioteke.

Kao dodaci na srednji sloj su dodati CI+ programska jedinica, DTCP-IP programska jedinica. DTCP-IP programska jedinica je usko povezana sa DLNA programskom jedinicom, koja je zadužena za prikazivanje sadržaja korisnicima kao i indikaciju zaštićenog sadržaja korišćenjem DTCP-IP-a, i distribucionog poslužioca preko kog se odvija sam prenos podataka.

3.3 Pribavljanje DTV sadržaja

Prenos sadržaja od emitera do digitalnog TV prijemnika je prikazan na slici 3.5.

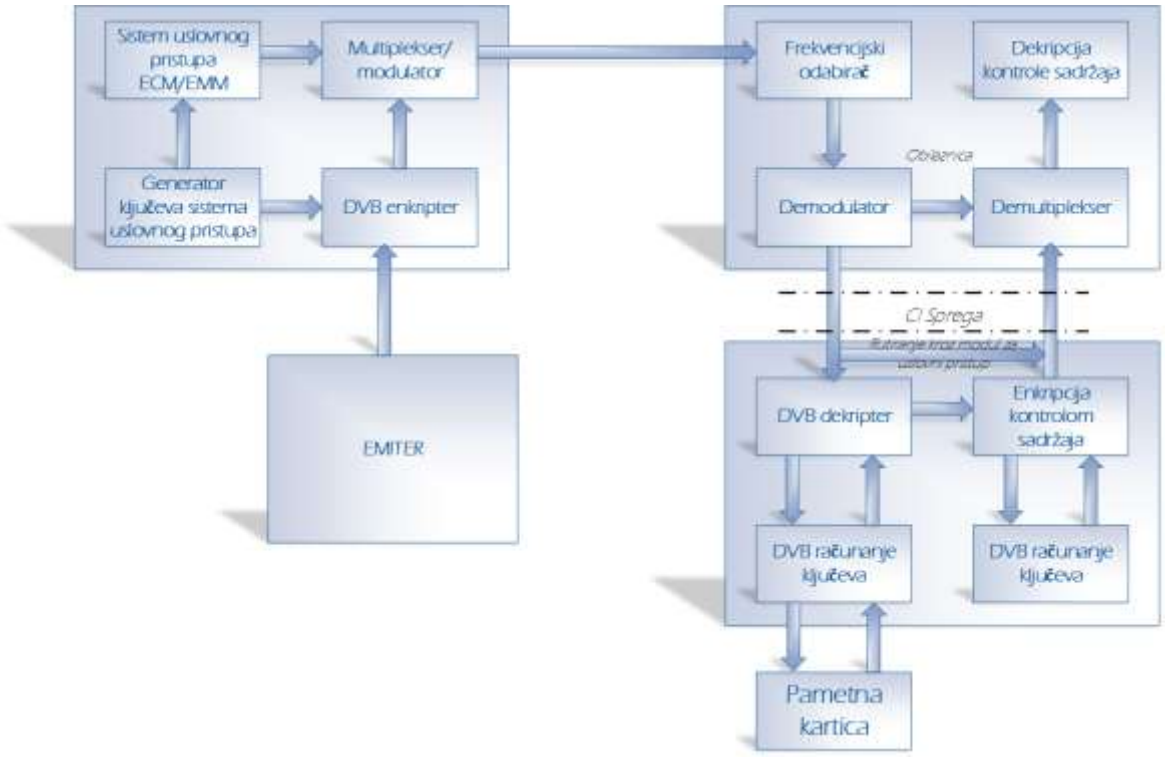
Kada pričamo o pribavljanju DTV sadržaja od emitera možemo razlikovati dve faze [13]:

- akvizicionu fazu
- post-akvizicionu fazu

Tokom akvizicione faze za zaštitu sadržaja je zadužen emiter i tokom tog prenosa sadržaj se štiti prema DVB standardima [3]-[6]. U zavisnosti od medijuma kojim se sadržaj prenosi razlikujemo tri grupe DVB standarda, a to su:

- DVB-C koji se primenjuje u kablovskoj televiziji
- DVB-S koji se primenjuje u satelitskoj televiziji
- DVB-T koji se primenjuje u zemaljskoj televiziji

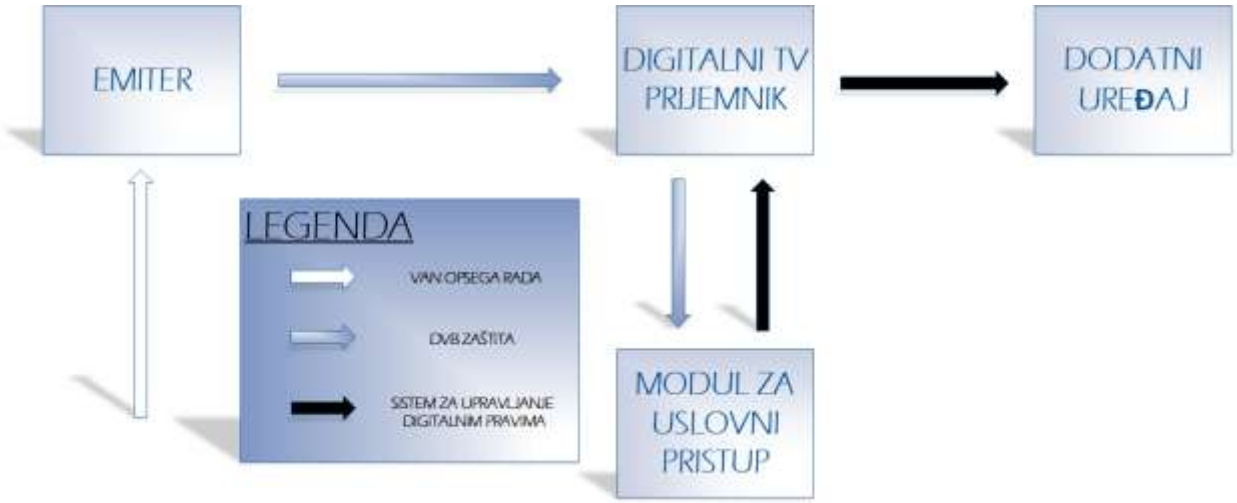
Sa druge strane, tokom post.akvizicione faze zaštitu sadržaja mora da ostvari programska podrška i u tu svrhu se koriste razni sistemi za upravljanje digitalnim pravima [14]. Jedan od tih sistema je i DTCP-IP koji je široko rasprostranjen jer je sastavni deo DLNA (eng. Digital Living Network Alliance) koji predstavlja jedan od standarda za deljenje sadržaja u kućnim mrežama. Takođe DTCP-IP je preporučen i od strane CI+ standarda.



Slika 3.5 Blokovi koji učestvuju u distribuciji signala sa strane emitera i DTV prijemnika

Sa slike 3.5 se vidi da se sadržaj najpre enkriptuje na strani emitera, potom se tako zaštićen sadržaj distribuira do digitalnog TV prijemnika. Po prijemu i demodulaciji sadržaja, sadržaj je i dalje enkriptovan te stoga neupotrebljiv za reprodukciju, pa je neophodno da se sadržaj najpre preda modulu za uslovni pristup kako bi se preveo u oblik pogodan za reprodukciju. Nakon izvršene DVB dekripcije u okviru modula za uslovni pristup, sadržaj je potrebno vratiti do modula za reprodukciju digitalnog TV prijemnika. I tokom ovog prenosa sadržaj mora da bude zaštićen, pa stoga se u okviru modula za uslovni pristup sadržaj nakon DVB dekripcije ponovo enkriptuje, al ovaj put drugim algoritmima i sa drugim ključevima i u takvom obliku se prenosi dalje. Ova enkripcija sadržaja se naziva kontrola sadržaja. Kontrola sadržaja prestaje na samom

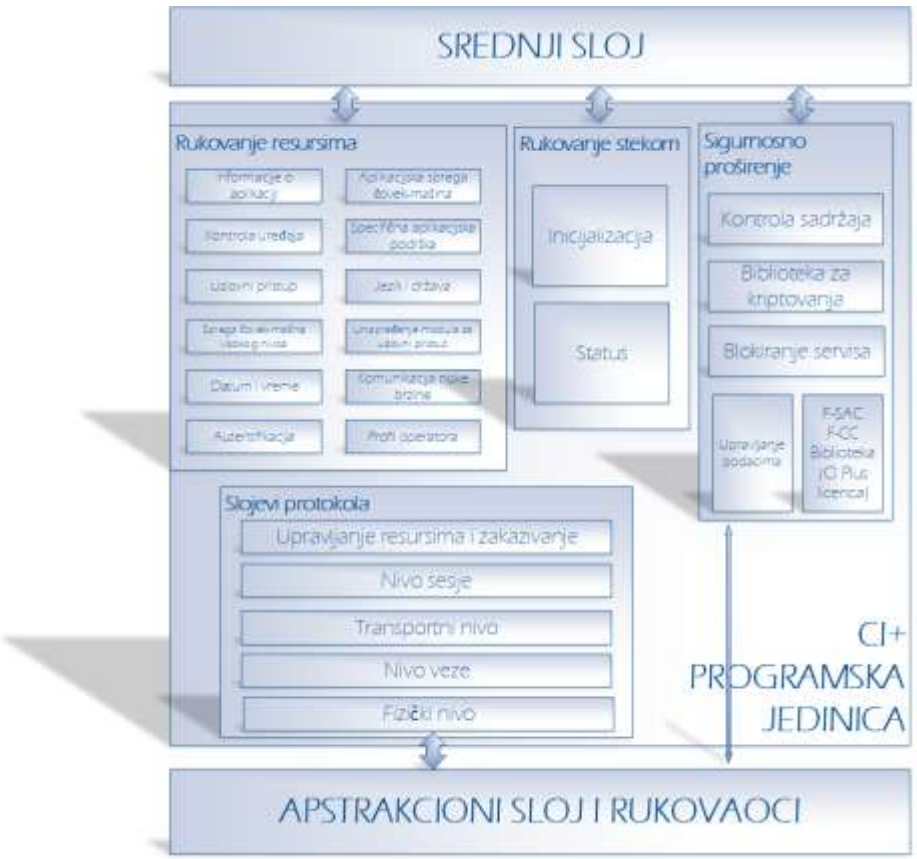
dekoderu, gde obično postoje moduli fizičke arhitekture za dekriptovanje sadržaja zaštićenog kontrolom sadržaja. Svim pomenutim enkripcijama i dekripcijama, kao i samim prenosima upravlja CI+ programska jedinica. Faze prenosa sadržaja kao i zaduženja u pogledu zaštite tokom ovih faza su prikazani na slici 3.6.



Slika 3.6 Faze prenosa sadržaja i zaduženja u pogledu zaštite

3.4 CI+ programska jedinica

CI+ programska jedinica je zadužena za kontrolu i komunikaciju sa modulo za uslovni pristup. CI+ programska jedinica korišćena u ovom rešenju se sastoji od modula za inicijalizaciju programske celine, status programske jedinice, kontrolu sadržaja i blokiranja servisa od strane digitalnog TV prijemnika, kao i modula za kontrolu resursa koji obezbeđuju informacije o aplikaciji, aplikacijsku spregu čoveka i mašine, uslovni pristup, informacije o vremenu i datumu, spregu čoveka i mašine visokog nivoa, kontrolu digitalnog TV prijemnika, informacije o jeziku i državi digitalnog TV prijemnika, komunikaciju niske brzine, specifičnu aplikacijsku podršku, unapređenje modula za uslovni pristup i operatorski profil, kao što je prikazano na slici 3.7.



Slika 3.7 CI+ programska jedinica

Kroz komunikaciju sa modulom za uslovni pristup CI+ programska jedinica treba da obezbedi da se najpre izvrši autentifikacija između modula za uslovni pristup i srednjeg sloja programske podrške digitalnog TV prijemnika, čiji je deo CI+ programska jedinica, na način kako je objašnjeno u poglavlju teorijske osnove. Zatim sledi uspostava sigurnog autentifikovanog kanala (SAC) koji u daljoj komunikaciji služi za razmenu ključeva i kontrolnih poruka. Kada je SAC uspostavljen može da se pristupi računanju ključeva za kontrolu podataka (Content Control Key, CCK), kojim se dekriptuju sami podaci. Kao što je već ranije pomenuto posle dekripcije DVB enkriptovanog sadržaja potrebno je enkriptovati podatke AES standardom. Ključevi koji se koriste za ovu enkripciju se dogovaraju između CI+ programske jedinice i ostatka programske podrške srednjeg sloja DTV prijemnika u okviru dogovora o ruti poverenja.

Pored same dekripcije sadržaja CI+ programska jedinica mora da propagira i podatke o kontroli kopiranja. Ovo se postiže kroz EMI poruke koje kasnije koristi i DTCP-IP kako bi informacije o kontroli kopiranja dostavio i do uređaja dodatnog ekrana.

Uz to, uloga CI+ programske jedinice je i da obezbedi spregu za komunikaciju sa korisnikom. Kroz tu spregu se korisniku pružaju neke osnovne informacije o uređaju i pruža mu se delimična kontrola nad uređajem.

Kako su različiti delovi CI+ programske jedinice zaduženi za različite stvari dolazi se do zaključka da ne moraju svi delovi CI+ programske jedinice da se nalaze u sigurnom delu

memorije. Svi delovi koji su vezani za kriptografske funkcije, autentifikaciju, uslovni pristup ili dolaze u kontakt sa CI+ sertifikatima moraju da se nalaze u zaštićenom delu. Takođe sami sertifikati koji sadrže privatni i javni ključ i ostale kriptografske tajne potrebne za uspešno izvršenje autentifikacije moraju da se nalaze u sigurnoj memoriji. Iz prethodnog sledi da sigurnosno proširenje CI+ programske jedinice prikazano na slici 3.7 mora da se nalazi u sigurnoj zoni, kao i moduli koji se bavi autentifikacijom i uslovnim pristupom. Ostali moduli ne moraju da se nalaze u sigurnim zonama jer se informacije koje moraju da ostanu tajne prenose enkriptovane kroz ove module.

3.5 DTCP-IP

DTCP-IP treba da obezbedi siguran prenos sadržaja između dva DTCP-IP kompatibilna uređaja, izvora i odredišta. Pored toga DTCP-IP mora da podržava i kontrolu kopiranja, a takođe i da razmenjuje poruke o obnovljivosti sistema (SRM) sa drugim DTCP-IP uređajima. Dodatna uloga je koju DTCP-IP ima u ovom sistemu je da kroz komunikaciju sa CI+ programskom jedinicom i srednjim slojem programske podrške DTV prijemnika dobavi potrebne ključeve za dekriptovanje AES enkriptovanog sadržaja koji stiže rutom poverenja.

Po dolasku zahteva za zaštićenim sadržajem od strane odredišnog uređaja, prvo se izvrši potpuna autentifikacija kao što je to opisano u poglavlju teorijske osnove. Po uspešno izvršenoj autentifikaciji sledi dogovor o ključevima za enkripciju sadržaja AES standardom. Zatim sesadržaj pripremi za slanje, što podrazumeva dekriptovanje ključevima dogovorenim u komunikaciji sa CI+ programskom jedinicom i enkriptovanje sa ključevima dogovorenim između DTCP-IP izvora i odredišta. U ovom radu je korištena realizacija DTCP-IP protokola razvijena u sklopu [16]. Arhitektura DTCP-IP-a korišćenog u ovom rešenju je prikazana na slici 3.8.

Slika 3.8 DTCP-IP arhitektura

Sadržaj koji se šalje uz DTCP-IP zaštitu se prikazuje korisnicima kroz DLNA. Korisnik pretraživanjem sadržaja DMS-a (eng. Digital Media Server) dobija informaciju o postojanju sadržaja koji može da se distribuira. Ukoliko se radi o sadržaju koji nosi sa sobom informaciju o kontroli kopiranja tada postoji indikacija da se sadržaj mora preneti zaštićen, odnosno da mora da se koristi DTCP-IP. U tom slučaju se uspostavlja već ranije opisana DTCP-IP sesija. Zatim se sadržaj priprema za prenos, odnosno prevodi se u enkriptovan oblik. Takav sadržaj može da se prenese do uređaja dodatnog ekrana posredstvom distribucionog poslužioca. Sa korisničke strane mora da postoji realizacija DTCP-IP-a kako bi pristigli sadržaj mogao da se dekriptuje i prikaže.

3.6 Distribucioni poslužilac i korisnička strana DTCP-IP

Kao što se moglo videti iz opisa DTCP-IP-a za njegovo funkcionisanje neophodno je posedovati distribucioni poslužilac na strain digitalnog TV prijemnika, a takođe je potrebno realizovati DTCP-IP korisnika na uređaju dodatnog ekrana. Ovi delovi sistema nisu cilj ovog rada, ali će radi sticanja ispravnije slike o celokupnom sistemu biti ukratko opisani.

Distribucioni poslužilac podržava nekoliko načina distribucije podataka. Pored običnog http poslužioca, može da funkcioniše i kao adaptivni distribucioni poslužilac i podržava dva tipa adaptivne distribucije podataka:

- HLS (HTTP Live Streaming)
- Mpeg-dash

Treba napomenuti da distribucioni poslužilac nema ulogu u enkriptovanju podataka, već samo prenosi unapred pripremljene podatke od strane DTCP-IP-a.

Na strain uređaja dodatnog ekrana je potrebno posedovati DTCP-IP kompatibilnu aplikaciju kao što je ranije istaknuto. U tu svrhu je razvijen DTCP-IP posrednik koji može da prima i dekriptuje podatke na strani uređaja dodatnog ekrana i da ih prosleđuje modulu za reprodukciju sadržaja[17]. Pored ovog rešenja moguće je koristiti i neko od komercijalnih rešenja za DTCP-IP o čemu će biti više reči u poglavlju ispitivanje i verifikacija.

4. Programsko rešenje

U ovom poglavlju je dat detaljniji prikaz programskog rešenja sistema za sigurnu distribuiju plaćenog sadržaja na uređaje dodatnog ekrana u kućnoj mreži. Akcenat je stavljen na realizaciji CI+ programske jedinice, kao i svih dodatnih potrebnih modula za ispravno funkcionisanje CI+ programske jedinice i modula za uslovni pristup.

4.1 Moduli HAL-a

U cilju pravilnog funkcionisanja CI+ programske jedinice neophodno je bilo isportovati tri HAL modula:

- Modul za sigurnost
- Modul za dekriptovanje
- Modul za kontrolu modula za uslovni pristup – CI modul

Slika 4.1 HAL moduli potrebni za CI+ programsku jedinicu

Kako se kroz komunikaciju sa ovim modulima razmenjuju kriptografske tajne, ta komunikacija mora da bude zaštićena. To znači da se podaci moraju prenositi enkriptovani ili po enkriptovanim vezama.

4.1.1 Modul za sigurnost

Osnovna uloga ovog modula je da omogući prepoznavanje grupe uređaja kojoj digitalni TV prijemnik pripada, kao i prepoznavanje baš tog uređaja u okviru grupe. S toga najvažnije funkcije ovog modula su:

- Funkcija koja vraća jedinstvenu identifikaciju uređaja
- Funkcija koja vraća identifikaciju grupe uređaja kojoj digitalni TV prijemnik pripada

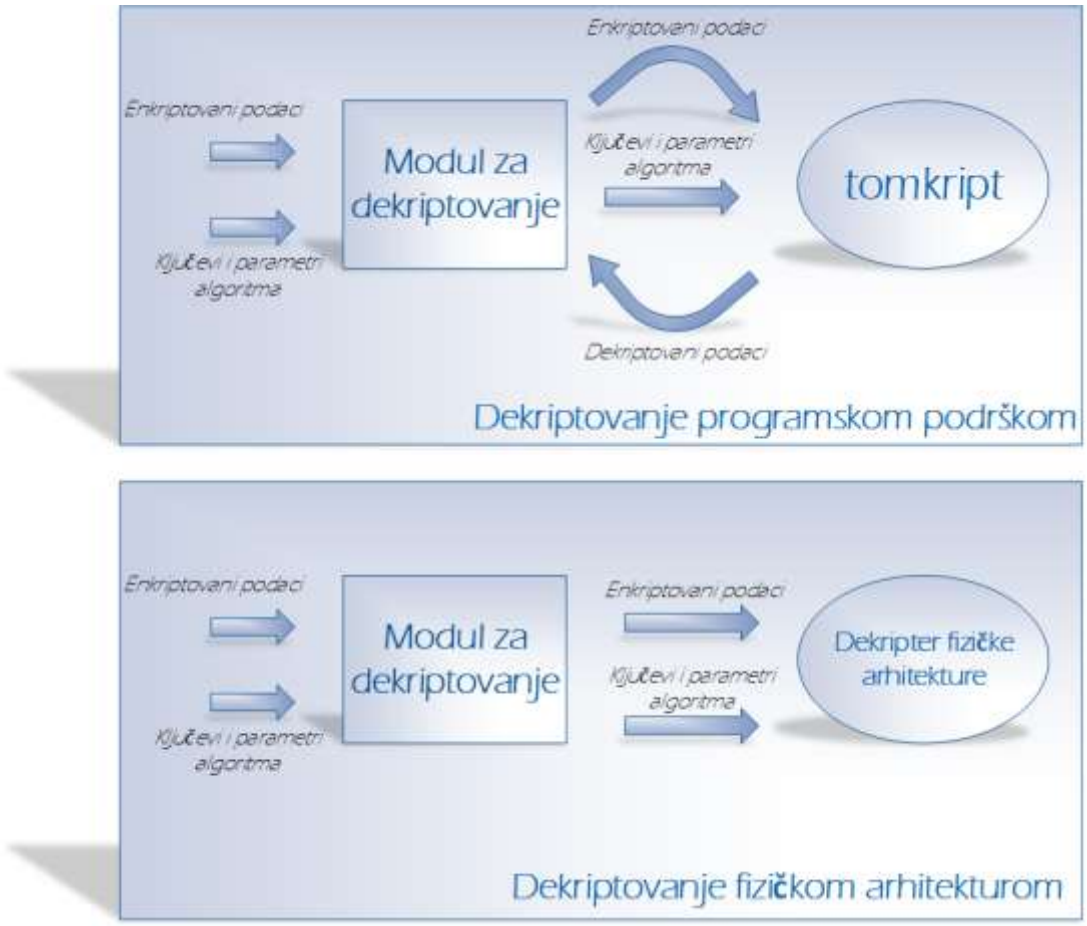
Ove informacije su potrebne CI+ programskoj jedinici da bi se uspešno povezao uređaj sa njegovim CI+ sertifikatima. Takođe, ove informacije se koriste kod povlačenja iz upotrebe jednog uređaja ili grupe uređaja od strane CI+.

4.1.2 Modul za dekriptovanje

Ovaj modul je zadužen za dekriptovanje AES enkriptovanog sadržaja. Uloga ovog modula je da prihvati ključeve za dekriptovanje od CI+ programske jedinice i da izvrši samo dekriptovanje podataka. Kako ključevi predstavljaju kriptografsku tajnu i ne smeju da budu dostupni svima oni se prenose enkriptovani. U zavisnosti od slučaja korišćenja, ovaj modul usko sarađuje ili sa modulom zaduženim za dekodere i enkodere ukoliko se vrši transkodovanje sadržaja ili sa DTCP-IP modulom ako se sadržaj priprema za distribuciju na uređaj dodatnog ekrana.

Realizacija ovog modula može da se izvrši u programskoj podršci korišćenjem biblioteke tomkript (eng. tomcrypt), a bolji način je da se iskoristi podrška za dekriptovanje realizovana u fizičkoj arhitekturi ukoliko ona postoji. Ukoliko se vrši realizacija u programskoj podršci korišćenjem tomkript biblioteke mora se voditi računa da se ne naruši ruta poverenja. Naime, dekriptovani podaci ne smeju da se pojave ni jednog trenutka u radnoj memoriji odakle može da im se pristupi. Dekriptovanje treba izvršiti neposredno pre dekodovanja ili pre predavanja podataka DTCP-IP modulu. Iz tog razloga je bolje koristiti podršku za dekriptovanje realizovanu u fizičkoj arhitekturi. Tada se sva odgovornost za rutu poverenja prenosi na fizičku arhitekturu. Uloga modula za dekriptovanje je da podesi sve parameter koji su potrebni da bi se sadržaj dekriptovao. Tu pored ključeva za dekriptovanje spadaju i algoritmi koji su korišćeni, u našem slučaju AES, i režim rada dekriptera što je u našem slučaju CBC. Ukoliko se koristi podrška za

dekriptovanje realizovana u fizičkoj arhitekturi tada se sadržaj prenosi enkriptovan skroz do dekodera na kojima postoji deo za dekriptovanje sadržaja fizički zaštićen od neželjenog pristupa. Takođe ukoliko se sadržaj ni ne transkoduje ni ne reprodukuje na digitalnim TV prijemnicima, odnosno nema potrebe da se koriste dekoderi, tada se neposredno pre slanja sadržaja DTCP-IP modulu sadržaj dekriptuje specijalnim alatima fizičke arhitekture koji vode računa o tome da dekriptovan sadržaj ni jednog trenutka ne dospe na memorijske lokacije kojima može da pristupi bilo ko. Na taj način sadržaj je zaštićen sve vreme boravka na digitalnom TV prijemniku i ruta poverenja je u potpunosti sačuvana. Dodatna prednost korišćenja podrške za dekriptovanje realizovane u fizičkoj arhitekturi je što se na taj način centralni processor ne opterećuje dodatno. Naime, kroz merenja se pokazalo da je za dekriptovanje sadržaja korišćenjem tomkript biblioteke potrebno oko 20% procesorskog vremena. To predstavlja značajno opterećenje za ceo sistem pogotovo ako je istovremeno potrebno dekriptovati nekoliko servisa, na primer kada želimo i da gledamo jedan servis na digitalnom TV prijemniku, i da distribuiramo još nekoliko različitih servisa na uređaje dodatnog ekrana. Ukoliko koristimo podršku za dekriptovanje realizovanu u fizičkoj arhitekturi pomenuti problem ne postoji. Ova razlika je prikazana na slici 4.2.



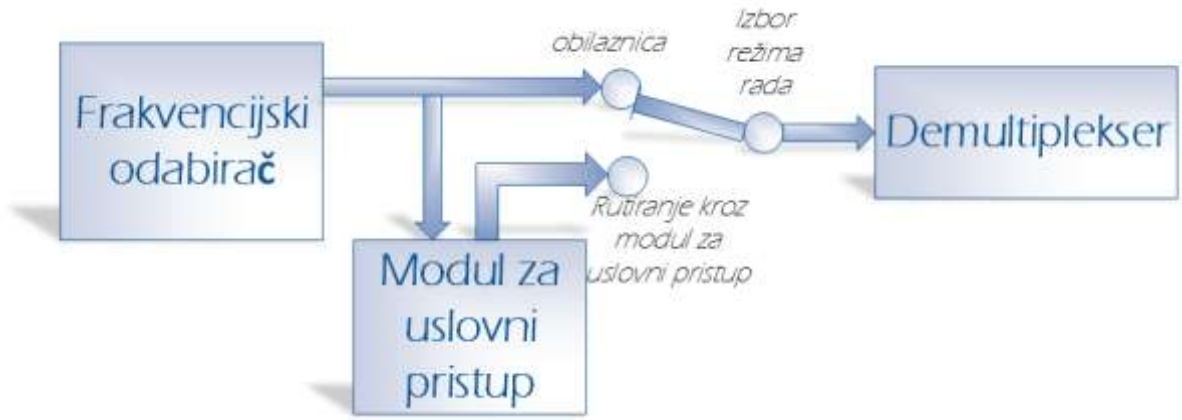
Slika 4.2 Razlika između dekriptovanja u programskoj podršci i fizičkoj arhitekturi

U ovde opisanom rešenju prvo je napravljeno rešenje sa dekriptovanjem sadržaja korišćenjem tomkript biblioteke. Pri tome nije vođeno računa o ruti poverenja, već je sadržaj dekriptovan čim bi se skupili svi potrebni parametri za dekriptovanje i tako dekriptovan usmeravan dalje na dekodere ili predavan DTCP-IP modulu. Takva realizacija je poslužila samo kao dokaz ispravnog funkcionisanja sistema u celini, a naknadno je iskorišćena fizička arhitektura za dekriptovanje sadržaja i na taj način je uspostavljena ruta poverenja na digitalnom TV prijemniku.

Realizacija kroz programsku podršku je nezavisna od platforme na kojoj se rešenje realizuje, pa je stoga lako prenosiva i može se uvek koristiti kao dokaz funkcionisanja ostatka sistema pri brzom razvoju. Naknadno je potrebno realizovati dekriptovanje kroz podršku u fizičkoj arhitekturi ciljnog uređaja kako bi se ispunili svi uslovi standarda i obezbedila potpuna zaštita sadržaja. Ukoliko platforma na kojoj se vrši realizacija zaštite sadržaja ne poseduje podršku u fizičkoj arhitekturi za dekriptovanje, tada je potrebno dodatno obezbediti realizaciju rešenja kroz programsku podršku vodeći računa da se ni u jednom trenutku ne dopusti pristup dekriptovanom sadržaju ostalim korisnicima i aplikacijama.

4.1.3 Modul za kontrolu modula za uslovni pristup – CI modul

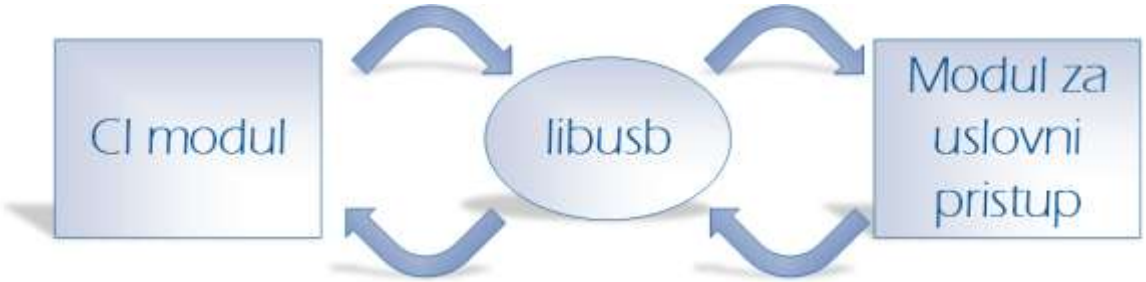
Ovaj modul je zadužen za kontrolu modula za uslovni pristup. Njegov zadatak je da na početku, po ubacivanju pametne kartice u modul za uslovni pristup izvrši inicijalizaciju modula za uslovni pristup. U inicijalizaciju spada autentifikacija uređaja, uspostavljanje sigurnog autentifikovanog kanala i dogovor o ključevima kojima će se kriptovati buduće poruke. Pored ključeva, razmenjuju se i kontrolne poruke koje upravljaju radom modula za uslovni pristup. U zavisnosti od servisa koji se zahteva, modul za uslovni pristup može da radi u dva različita režima. Ukoliko se zahteva besplatni TV sadržaj modul za uslovni pristup radi u režimu obilaznice, odnosno ne vrši nikakvu obradu podataka, već se podaci usmeravaju sa frekvencijskog odabirača i demodulatora digitalnog TV prijemnika pravo na demultiplekser. U suprotnom, ako se zahteva plaćeni TV sadržaj modul za uslovni pristup radi u režimu rutiranja podataka kroz modul za uslovni pristup. U tom slučaju se podaci sa frekvencijskog odabirača i demodulatora usmeravaju na modul za uslovni pristup. Tu se vrši dekriptovanje DVB enkripcije, a zatim enkriptovanje AES podacima. Tako zaštićeni podaci se dalje usmeravaju na demultiplekser kao i u prethodnom slučaju. Sve ove radnje su praćene pregovorima između CI+ programske jedinice i modula za uslovni pristup o ključevima kojima se dekriptuje i enkriptuje sadržaj. Slika 4.2 prikazuje različite režime rada modula za uslovni pristup.



Slika 4.3 Režimi rada modula za uslovni pristup

Komunikacija sa modulom za uslovni pristup posle izvršene autentifikacije se uglavnom svodi na promene režima rutiranja podataka. Ova komunikacija se odvija upisivanjem određenih vrednosti u register modula za uslovni pristup. Ove vrednosti su specifične za ubačenu karticu i mogu se pročitati iz specifikacije. Pošto je nemoguće napisati jedno rešenje za sve pametne kartice ovaj modul mora da se menja ukoliko želimo da proširimo podršku na novi tip pametne kartice, odnosno kartice drugog proizvođača. Zaključak je da ovaj modul pruža univerzalni okvir za komunikaciju sa modulom za uslovni pristup, a same poruke koje se šalju se menjaju od slučaja do slučaja u zavisnosti od pametne kartice koja se koristi.

Uobičajeni način slanja ovih poruka je preko CI veza, pošto se modul za uslovni pristup uglavnom tako povezuje sa digitalnim TV prijemnikom. Iz tog razloga CI modul uglavnom treba da se oslanja na PCMCI rukovaoc. Ipak, u našem slučaju situacija je nešto drugačija. Pošto ne postoje CI veze do modula za uslovni pristup već se on povezuje preko USB-a, modul za kontrolu modula za uslovni pristup se oslanja na libusb biblioteku pomoću koje se upisuju i isčitavaju podaci iz registara modula za uslovni pristup. Ova komunikacija je predstavljena na slici 4.3.



Slika 4.4 Komunikacija između CI modula i modula za uslovni pristup

Biblioteka libusb je biblioteka koja pruža aplikacijama pristup i kontrolu nad prenosom podataka na i sa USB prolaza na uređajima sa i bez UNIX baziranim operativnim sistemima.

Prednost ove biblioteke je što ne zahteva pisanje modula jezgra. Biblioteka je napisana u C programskom jeziku i dostupna je na raznim platformama[19].

4.2 CI+ programska jedinica

CI+ programska jedinica služi za koordinaciju rada modula za uslovni pristup. U slojevitom prikazu programske podrške digitalnog TV prijemnika nalzi se u ravni sa srednjim slojem programske podrške digitalnog TV prijemnika. Faktički, CI+ programska jedinica predstavlja proširenje za srednji sloj programske podrške digitalnog TV prijemnika za komunikaciju i kontrolu modula za uslovni pristup. U svom radu koristi prethodno opisane module apstrakcionog sloja fizičke arhitekture digitalnog TV prijemnika.

Kao što je prikazano na slici 3.5 CI+ programska jedinica se može podeliti na nekoliko podmodula i to su:

- Modul za rukovanje resursima
- Modul za rukovanje CI+ programskom jedinicom
- Sigurnosno proširenje
- Slojevi protokola

Ti moduli će u daljem tekstu biti nešto detaljnije opisani.

4.2.1 Modul za rukovanje CI+ programskom jedinicom

Modul za rukovanje CI+ programskom jedinicom omogućava aplikacijama da pokrenu inicijalizaciju CI+ programske jedinice, kao i da provere njen status. Ovaj modul se poziva na samom startu izvršavanja programa kada je potrebno izvršiti inicijalizaciju, a u daljem radu obaveštava aplikaciju u kom stanju se nalazi CI+ programska jedinica i da li je došlo do neke greške tokom rada. Izgled ovog modula je predstavljen na slici 4.5.

Slika 4.5 Modul za rukovanje CI+ programskom jedinicom

Najvažnije funkcije ovog modula, koje služe za samo upravljanje i kontrolu CI+ programske jedinice su:

```
tCI_EX_INIT_Error CI_EX_INIT_Init
(
    tCI_EX_INIT_CI_Type       ci_type,
    tCI_EX_INIT_Res_Activation  lsc_activation,
    tCI_EX_INIT_Res_Activation  sas_activation,
    tCI_EX_INIT_Res_Activation  auth_activation
)
```

Ova funkcija vrši inicijalizaciju svih podmodula CI+ programske jedinice. Poziv ove funkcije mora da prethodi svim ostalim pozivima funkcija CI+ programske jedinice.

```
tCI_EX_INIT_Error CI_EX_INIT_Activate(void)
```

Ova funkcija pokreće autentifikaciju. Po ubacivanju pametne kartice u modul za uslovni pristup, poziva se ova funkcija kako bi se izvršavanjem autentifikacije CI+ programska jedinica prevela u aktivno stanje.

```
tCI_EX_INIT_Error CI_EX_INIT_SwitchTs(unsigned short slotnumber, unsigned char
TsRoute)
```

Ova funkcija služi da se izabere modul za uslovni pristup koji će se koristiti u slučaju kad je povezano više ovih modula, kao i da se podesi režim rada izabranog modula za uslovni pristup, odnosno da li će podaci ići obilaznicom, kada se gleda besplatni TV sadržaj, ili će se rutirati kroz modul za uslovni pristup, kada je u pitanju plaćeni TV sadržaj.

Kada se izvrše pozivi ovih funkcija CI+ programska jedinica je funkcionalna i korisnik nema veliki uticaj na dalji rad. Ipak kroz podmodul za promenu statusa korisniku je omogućeno da proverava stanje CI+ programske jedinice. Kako bi se podesila funkcija povratnog poziva koja će služiti za vezu sa korisnikom poziva se funkcija:

```
tCI_EX_STA_Error CI_EX_STA_Register(tCI_EX_STA_NotifyFn notifyFn)
```

gde je parametar upravo funkcija koja treba da se pozove na promenu stanja CI+ programske jedinice.

4.3 Konfiguracija i kontrola DTCP-IP modula

Za uspešnu konfiguraciju i korišćenje DTCP-IP modula korišćenog u ovom rešenju bilo je potrebno izvršiti sledeću sekvencu poziva. Prvi korak je da se po startovanju sistema pozove funkcija koja će inicijalizovati DTCP-IP modul. Prototip ove funkcije je:

```
dtcp_ip_error_t dtcp_ip_init(void);
```

Ova funkcija nema ulazne parametre, a vraca gresku ukoliko do nje dođe ili obaveštenje da je sve dobro prošlo. Neophodno je pozvati ovu funkciju pre bilo kog drugog poziva ovog modula.

Sledeća funkcija koja se poziva na strani poslužioca je funkcija koja kreira DTCP-IP izvor. Prototip funkcije je:

```
dtcp_ip_error_t dtcp_ip_source_create(dtcp_ip_source_t* source);
```

Ova funkcija prima kao ulazni parametar pokazivač na strukturu `dtcp_ip_source_t` koji se u okviru funkcije popuni sa adresom instancirane strukture i ova vrednost se koristi za dalje pozive funkcija vezanih za DTCP-IP izvor.

Posle kreiranja potrbno je i startovati DTCP-IP izvor pozivom funkcije:

```
dtcp_ip_error_t dtcp_ip_source_start(dtcp_ip_source_t source, char* host, int port);
```

Uz prethodno pomenutu strukturu `dtcp_ip_source_t` dodatni ulaznui parametri ove funkcije su ip adresa poslužioca na kom se izvršava ovaj program i prolaz na kom se čekaju konekcije. Po izvršavanju ovih funkcija strana DTCP-IP poslužioca je spremna i dalji rad zavisi od pristizanja zahteva od korisničke strane.

Kada stigne zahtev za podacima poziva se funkcija:

```
dtcp_ip_error_t dtcp_ip_http_enc_create(dtcp_ip_source_t source, dtcp_ip_stream_t
*stream, dtcp_stream_params_t *params);
```

Kojoj se kao dodatni ulazni parametri proslede struktura sa parametrima vezanim za tip enkriptera, kao i adresa promenljive u koju se upiše identifikator konekcije.

Nakon kreiranja enkriptera dalji rad se zasniva na uzastopnim pozivima funkcija:

```
dtcp_ip_error_t dtcp_ip_http_enc_out_len(dtcp_ip_source_t source, dtcp_ip_stream_t
stream, size_t in_len,size_t *out_len, size_t *handled_len);
```

koja računa tačnu veličinu paketa koji će se slati zaštićen DTCP-IP zaštitom po dodavanju svih potrebnih zaglavlja i provere grešaka i

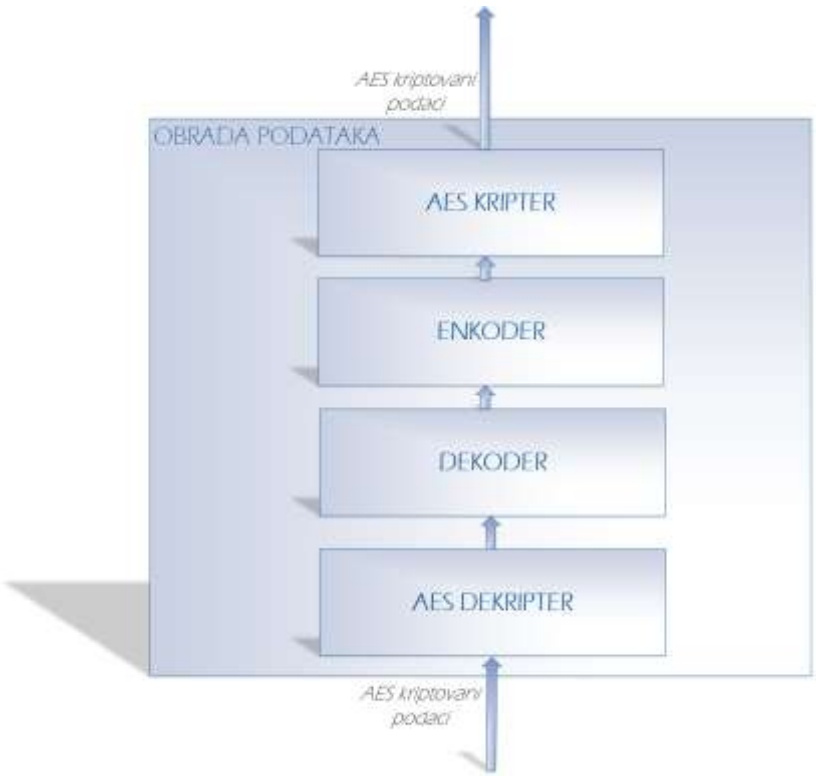
```
   dtcp_ip_error_t dtcp_ip_http_enc(dtcp_ip_source_t source, dtcp_ip_stream_t stream,
char* peer_addr, void* in_data, size_t in_len,void* out_data, size_t *out_len, size_t
*encrypted);
```

koja vrši samo enkripciju podataka.

Posle izvršenja ovih funkcija podaci zaštićeni DTCP-IP zaštitom se mogu poslati korisniku posredstvom distibucionog poslužioca.

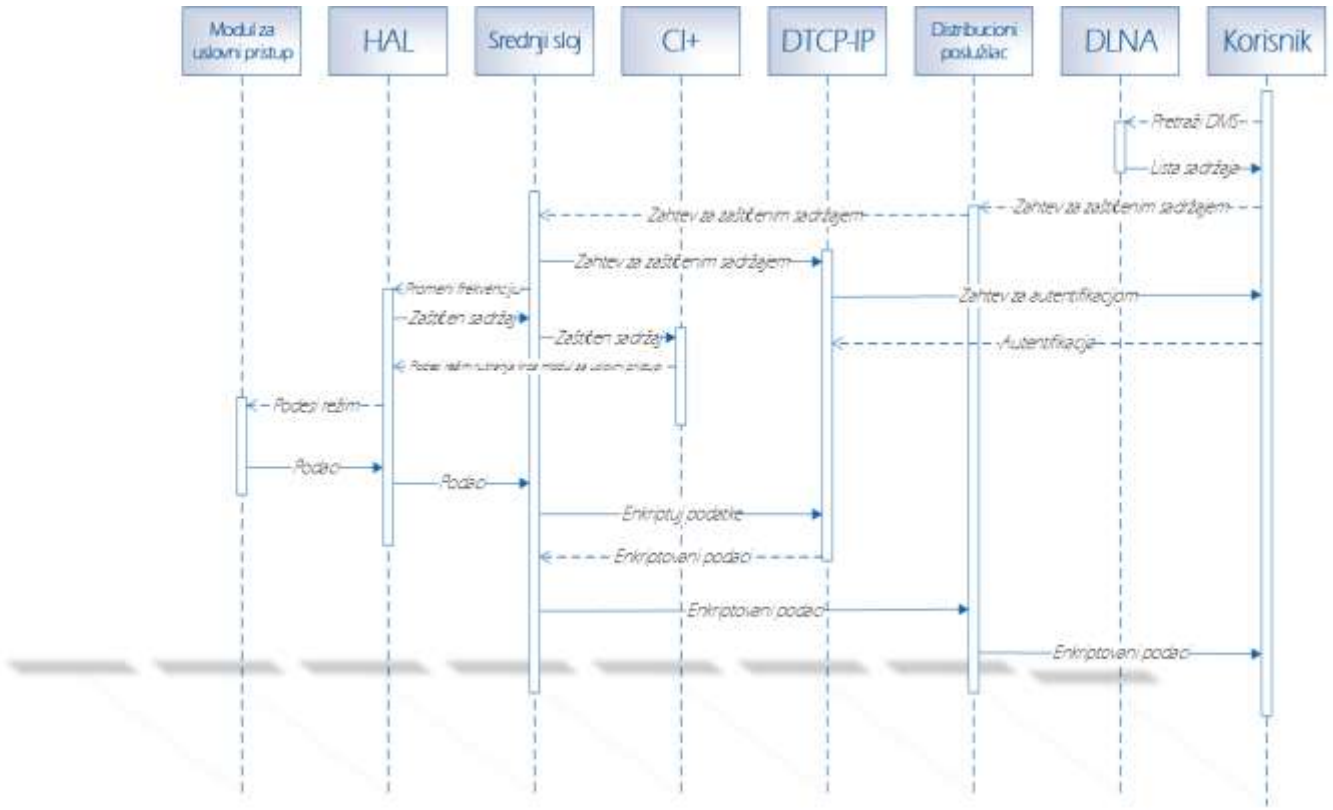
4.4 Pregled kompletnog sistema i propagacija zahteva za podacima kroz sistem

Arhitektura kompletnog sistema je već prikazana na slici 3.3. Na pomenutoj slici možemo da vidimo koji sve blokovi učestvuju u slanju podataka do uređaja dodatnog ekrana. Komunikacija započinje na zahtev korisnika, u ovom slučaju uređaja dodatnog ekrana, za podacima vezanim za servis koji je zaštićen CI+ zaštitom. Korisnik dobija uvid u dostupne podatke pretraživanjem DMS-a koji se nalazi na digitalnom TV prijemniku. Zahtev koji klijent šalje se prihvata od strane distribucionog poslužioca, zatim se prosleđuje srednjem sloju koji pokreće promenu frekvencije frekvencijskog odabirača ukoliko je to potrebno. Ukoliko se ispostavi da je stigao zahtev za zaštićenim servisom o tome se obaveštava CI+ programska jedinica, koja posredstvom CI modula apstrakcionog sloja fizičke arhitekture obaveštava modul za uslovni pristup da treba da pređe u režim rutiranja kroz modul za uslovni pristup. Jednom kada su ove operacije izvršene, na već ranije opisan način podaci se dekriptuju od DVB enkripcije i enkriptuju AES enkripcijom u okviru modula za uslovni pristup i stižu do demultipleksera. Tu se vrši rasčlanjavanje podataka i elementarni tokovi se usmeravaju ka bloku za obradu podataka ukoliko je sadržaj potrebno transkodovati kako bi se omogućila reprodukcija na uređaju dodatnog ekrana. U okviru bloka za obradu podataka podatke je najpre potrebno dekriptovati, zatim izdekodovati, potom se može pristupiti enkodovanju u drugi kodek i pakovanju u odgovarajući prenosni oblik. Posle toga se podaci, sad u odgovarajućem prenosnom obliku i odgovarajućeg kodeka, moraju ponovo enkriptovati kako bi se održala sigurnost. Arhitektura ovog bloka je prikazana na slici 4.9.



Slika 4.6 Blok za obradu podataka

Podaci se dalje prosleđuju DTCP-IP modulu. Kako je ranije objašnjeno DTCP-IP autentifikacija je već prethodno obavljena, odmah po prijemu zahteva za podacima, pa ovaj modul poseduje ključeve za enkriptovanje sadržaja. Ipak kako su podaci već enkriptovani AES standardom, potrebno ih je najpre dekriptovati, pre nego što se pristupi enkripciji. Po završenoj enkripciji, podaci se prosleđuju distribucionom poslužiocu koji ih prenosi do uređaja dodatnog ekrana jednim od podržanih protokola. Na korisničkoj strani podaci se prihvataju, šalju DTCP-IP posredniku koji vrši dekriptovanje i konačno prosleđuje podatke modulu za reprodukciju. Rezultat svega je reprodukovan željeni servis na uređaju dodatnog ekrana. Slika 4.10 predstavlja dijagram toka propagacije zahteva za zaštićenim servisom i odgovor digitalnog TV prijemnika u vidu isporuke zaštićenih podataka.



Slika 4.7 Zahtev za zaštićenim servisom i odgovor

5. Ispitivanje i verifikacija

U cilju ispitivanja i verifikacije realizovanog rešenja razvijene su dve test aplikacije, a korišćena je i komercijalna android aplikacija Tvonki bim (eng. Twonky beam). Testirana je funkcionalnost CI+ programske jedinice kao i deo za transport podataka koji se sastoji od DTCP-IP-a i distribucionog servera.

Za testove je korišćena platforma brcm7445 kao digitalni TV prijemnik, a uređaj dodatnog ekrana je bio tablet računar samsung galaksi tab 2 sa android platformom.

Prvi test se odnosi na CI+ programsku jedinicu. Za ovaj test potrebno je koristiti testni tok podataka sa CI+ enkripcijom. Kriterijum uspešnosti testa je prikaz dekriptovane slike na izlazu digitalnog TV prijemnika kada je CI+ pametna kartica ubačena u modul za uslovni pristup, a kada kartica nije ubačena u modul za uslovni pristup, na izlazu treba da bude enkriptovana slika, odnosno ne sme se dopustiti gledanje TV servisa. Test se sastojao iz sledećih koraka:

1. Uključiti digitalni TV prijemnik sa povezanim modulom za uslovni pristup ali bez ubačene CI+ pametne kartice
2. Prebaciti na servis koji se prenosi u enkriptovanom obliku kroz tok podataka
3. Potvrditi da je prikaz na ekranu enkriptovan, odnosno da nemamo pravo da gledamo dati servis
4. Ubaciti CI+ pametnu karticu u modul za uslovni pristup i sačekati da se modul za uslovni pristup inicijalizuje i rekonfiguriše
5. Potvrditi da je prikaz na ekranu validan, odnosno da smo posle ubacivanja kartice stekli pravo gledanja datog servisa

Ovaj test je prošao uspešno. Na slici 5.1 su prikazani rezultati ovog testa. Na slici se vidi izlaz kada pametna kartica nije ubačena levo, i kada je ubačena desno.

Pametna kartica nije ubacena

Pametna kartica je ubačena

Slika 5.1 Rezultati prvog testa

Posle prvog testa ustanovljeno je da CI+ programska jedinica ispravno dekriptuje sadržaj. Ostali testovi su se odnosili na testiranje distribucije zaštićenih servisa na uređaje dodatnog ekrana. U tu svrhu korišćene su tri različite aplikacije:

- Prva je DTCP-IP korisnik za Linux operativni sistem. Treba napomenuti da je uloga ove aplikacije samo da dobavi i dekriptuje podatke, a ne i da ih reprodukuje. Za reprodukciju je korišćen avplej (eng. avplay) program.
- Druga aplikacija je SARimout (eng. SARemote)[18]. Ova aplikacija se izvršava na Android platformi.
- Treća aplikacija je Tvonki bim takođe na Android platformi. Razlika u odnosu na SARemote je ta što je Tvonki bim komercijalna aplikacija.

I u ovim testovima se koristio isti testni tok podataka.

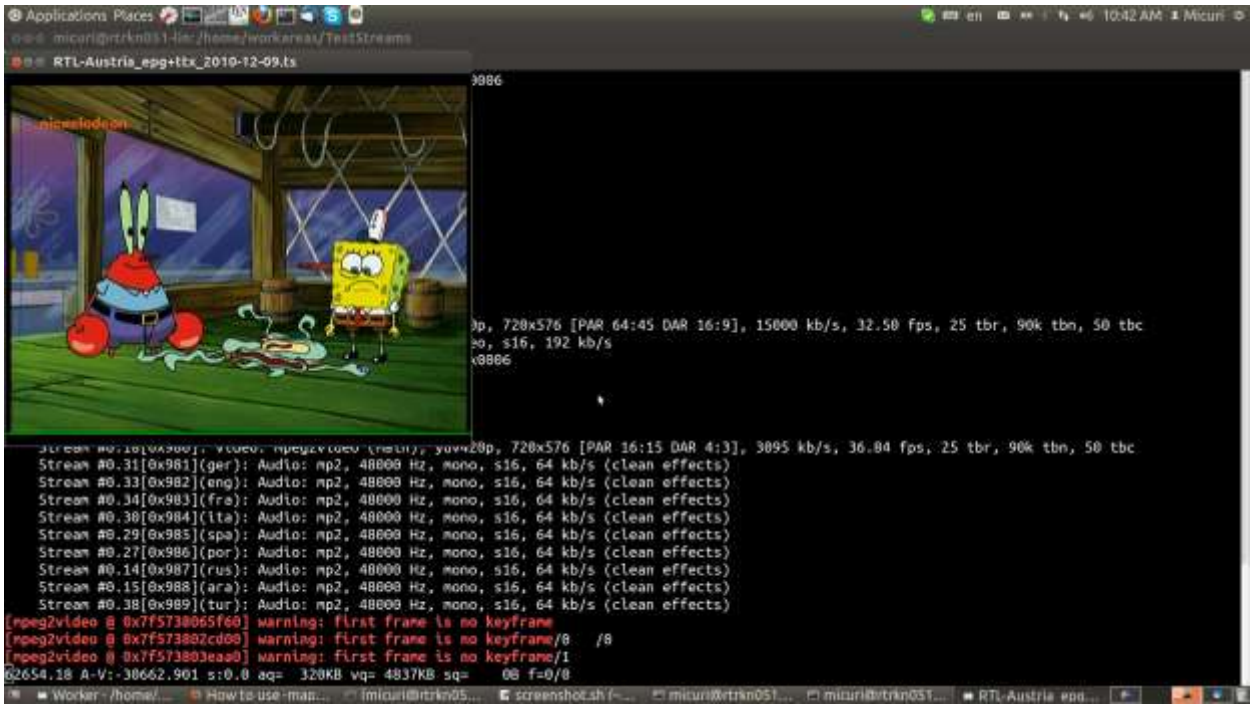
Drugi test je služio da se proveri validnost kontrole kopiranja postavljene od CI+ programske jedinice. Kriterijum uspešnosti testa je potvrda neophodne DTCP-IP autentifikacije pre dobavljanja podataka vezanih za zaštićen servis i uspešna reprodukcija dobavljenog sadržaja na uređaju dodatnog ekrana.

Test se sastojao iz sledećih koraka:

1. Pokrenuti digitalni TV prijemnik sa povezanim modulom za uslovni pristup i ubačenom pametnom karticom.
2. Poslati zahtev za zaštićenim TV servisom sa uređaja dodatnog ekrana koji ne podržava DTCP-IP, npr avplej.
3. Potvrditi da nije moguće dobiti podatke pre nego što se izvrši DTCP-IP autentifikacija.

4. Poslati zahtev za zaštićenim TV servisom sa uređaja dodatnog ekrana koji podržava DTCP-IP. u ovom testu je korišćen Linux DTCP-IP korisnik.
5. Potvrditi pristizanje podataka proverom veličine snimljene datoteke.
6. Prekinuti Linux DTCP-IP korisnika u dobavljanju podataka i reprodukovati snimljenu datoteku upotrebom avpleja
7. Potvrditi da je reprodukovani sadržaj isti kao i sadržaj reprodukovan na digitalnom TV prijemniku u prvom testu.

Ovaj test je prošao uspešno. Na slici 5.2 su prikazani rezultati ovog testa. Može se videti reprodukcija datoteke koja je prenesena pomoću Linux DTCP-IP aplikacije.



Slika 5.2 Rezultati testa 2

Treći test je izvršen sa dve android aplikacije koje su već pomenute, SARimout i Tvonki bim. Kriterijum uspešnosti testa je reprodukcija validnog sadržaja na uređaju dodatnog ekrana. U oba slučaja testni koraci su sledeći:

1. Pokrenuti digitalni TV prijemnik sa povezanim modulom za uslovni pristup i ubačenom pametnom karticom.
2. Poslati zahtev za zaštićenim TV servisom sa uređaja dodatnog ekrana
3. Potvrditi da je reprodukovani sadržaj na uređaju dodatnog ekrana validan (isti kao i reprodukovani sadržaj u prethodnim testovima)

Ovaj test je prošao uspešno u oba slučaja. Na slici 5.3 su prikazani rezultati testa izvršenog sa SARimout aplikacijom.

Slika 5.3 Rezultati testa 3 izvršenog sa SARimout aplikacijom

Na slici 5.4 su prikazani rezultati testa izvršenog sa Tvonki bim aplikacijom.

Slika 5.4 Rezultati testa 3 izvršenog sa Tvonki bim aplikacijom

Tabela 5.1 daje pregled svih izvršenih testova kao i njihovih rezultata.

TEST	REZULTAT
Provera dekriptovanja TV servisa posredstvom CI+ programske jedinice	Prošao
Provera propagacije kontrole kopiranja od strane CI+ programske jedinice i DTCP-IP prenosa podataka	Prošao
Reprodukcija zaštićenog sadržaja na uređaju dodatnog ekrana korišćenjem SARimout aplikacije	Prošao
Reprodukcija zaštićenog sadržaja na uređaju dodatnog ekrana korišćenjem Tvonki bim aplikacije	Prošao

Tabela 5.1 Izvršeni testovi i njihovi rezultati

6. Zaključak

U ovom radu je predstavljeno rešenje za sigurnu distribuciju plaćenog sadržaja na uređaje dodatnog ekrana na digitalnom TV prijemniku brcm7445. Pomenuto rešenje je realizovano pomoću CI+ programske jedinice i DTCP-IP protokola. Za uređaje dodatnog ekrana su korišćeni tablet računar na Android platformi i personalni računar na Linuks platformi.

Pošto pristup plaćenim sadržajim imaju samo pretplaćeni korisnici ovi sadržaji moraju svo vreme boravka na digitalnom TV prijemiku da budu zaštićeni od neželjenog pristupa. Za zaštitu tokom samog prenosa sadržaja od emitera do digitalnog TV prijemnika je zadužen modul za uslovni pristup. Modul za uslovni pristup radi pod kontrolom CI+ programske jedinice. CI+ programsku jedinicu je moguće relizovati samo na CI+ sertfikovanim uređajima, odnosno za korišćenje CI+ programske jedinice potrebno je posedovati CI+ pametnu karticu koja sadrži sve potrebne sertifikate. CI+ programska jedinica i modul za uslovni pristup zajedno sa srednjim slojem programske podrške digitalnog TV prijemnika obezbeđuju sadržaj od neželjenog pristupa tokom celog boravka sadržaja na digitalnom TV prijemniku. Sa druge strane, kada želimo da plaćeni sadržaj prenesemo na uređaj dodatnog ekrana, moramo obezbediti dodatnu zaštitu tokom samog prenosa. U tu svrhu se koriste razni DRM-ovi. U ovom rešenju izabrani DRM je DTCP-IP. DTCP-IP je izabran zato što je sastavni deo DLNA koji predstavlja jedan od najrasprostranjenijih načina deljenja multimedijalnih sadržaja u kućnim mrežama, a takođe i sam CI+ standard preporučuje upotrebu DTCP-IP-a.

Realizacijom rešenja predstavljenog u ovom radu uspešno je omogućena sigurna distribucija plaćenog sadržaja na uređaje dodatnog ekrana, što je i potvrđeno izvršenim testovima. Testovi su potvrdili ispravno funkcionisanje CI+ programske jedinice u pogledu dekriptovanja i enkriptovanja sadržaja, kao i propagacije kontrole kopiranja. Takođe testiran je i prenos preko DTCP-IP protokola koji se pokazao kao funkcionalan kako sa namenski razvijenim

testnim aplikacijama tako i sa komercijalnim rešenjima DTCP-IP korisnika koja postoje na tržištu. Pored same zaštite sadržaja značaj ovog rešenja je i u tome što omogućava obradu podataka na strani digitalnog TV prijemnika, pa se sadržaj koji se šalje uvek može prilagoditi potrebama korisničke aplikacije. Iz tog razloga ovo rešenje može da radi praktično sa bilo kojom korisničkom aplikacijom.

7. Literatura

[1] Google, "The New Multi-screen World: Understanding Cross-platform Consumer Behaviour", http://services.google.com/fh/files/misc/multiscreenworld_final.pdf, August 2012.

[2] N. Soskic, D. Popov Tapavicki, M. Subotic, N. Kuzmanovic, M. Savic, "A proposal for second screen DTV and remote control application", ICCE Berlin, pp.391-393, 2013.

[3] ETR 289: "Digital Video Broadcasting (DVB); Support for use of scrambling and Conditional Access (CA) within digital broadcasting systems", European Telecommunications Standards Institute, October 1996.

[4] EN 50221: "Common Interface Specification for Conditional Access and other Digital Video Broadcasting Decoder Applications", CENELEC, CENELEC TC 206, February 1997

[5] TS 101 699 V1.1.1: "Digital Video Broadcasting (DVB); Extensions to the Common Interface Specification". European Telecommunications Standards Institute, November 1999

[6] ETSI TS 100 289 V1.1.1 (2011-09), Digital Video Broadcasting (DVB); Support for use of the DVB Scrambling Algorithm version 3 within digital broadcasting systems

[7] CI Plus Specification v1.3.1 (2011-09)

[8] Digital Transmission Content Protection Specification, revision 1.7, Digital Transmission Licensing Administrator, December 2011.

[9] Understanding Cryptography by C. Paar and J. Pelzl, Copyright Springer-Verlag

[10] RFC 2631 - Diffie-Hellman Key Agreement Method, E. Rescorla June 1999.

[11] NIST, Digital Signature Standard (DSS)

[12] NIST, Secure Hash Standard (SHS)

[13] Diaz-Sanchez, D.; Marin, A.; Almenarez, F.; Cortes, A., "Sharing Conditional Access Modules through the Home Network for Pay TV Access", Consumer Electronics, IEEE Transactions on (Volume:55 , Issue: 1), February 2009, pp 88-96.

[14] Sakamoto, N.; Muguruma, K. ; Koshino, N. ; Chiba, S. ; Sakurai, M., "A digital HDTV receiver with home networking function and digital content storage", Consumer Electronics, IEEE Transactions on (Volume:51 , Issue: 3), September 2005, pp 831-835.

[15] N. Fimić, M.Subotić, D. Dejanović, G. Miljković, " A Proposal for Secured Streaming of Premium Content in Second Screen Environment", MECO Budva, June 2014., pp 275-278

[16] R. Vulin, Jedno rešenje realizacije programske podrške za zaštitu multimedijalnog sadržaja pomoću DTCP-IP protokola

[17] D. Popov Tapavički, N. Špirić, S. Tanacković, N. Fimić, J. Kovačević, "Implementation of DTCP-IP Protected Content on Android Devices", MECO Budva, June 2014., pp 279-281

[18] N. Soskic, N. Kuzmanovic, M. Vidakovic, G. Miljkovic, "Second Screen User Experience: A New Digital Television Frontier", 37th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO, May 2014.

[19] Libusb, http://www.libusb.org/

[20] N. Fimić, M.Subotić, D. Dejanović, G. Miljković, "Jedno rešenje zaštićene distribucije plaćenog sadržaja na uređaje dodatnog ekrana", 58. Konferencija za elektroniku, telekomunikacije, računarstvo, automatiku i nuklearnu tehniku (ETRAN), Jun 2014.