



УНИВЕРЗИТЕТ У НОВОМ САДУ ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА



УНИВЕРЗИТЕТ У НОВОМ САДУ
ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА
НОВИ САД
Департман за рачунарство и аутоматику
Одсек за рачунарску технику и рачунарске комуникације

ЗАВРШНИ (BACHELOR) РАД

Кандидат: Ксенија Попов
Број индекса: РА 151/2014

Тема рада: Подршка за динамички генерисане кључеве у систему са условним приступом у дигиталној телевизији

Ментор рада: проф. др Илија Башичевић

Нови Сад, април, 2021



КЉУЧНА ДОКУМЕНТАЦИЈСКА ИНФОРМАЦИЈА

Редни број, РБР:			
Идентификациони број, ИБР:			
Тип документације, ТД:	Монографска документација		
Тип записа, ТЗ:	Текстуални штампани материјал		
Врста рада, ВР:	Завршни (Bachelor) рад		
Аутор, АУ:	Ксенија Попов		
Ментор, МН:	проф. др Илија Башичевић		
Наслов рада, НР:	Подршка за динамички генерисане кључеве у систему са условним приступом у дигиталној телевизији		
Језик публикације, ЈП:	Српски / латиница		
Језик извода, ЈИ:	Српски		
Земља публиковања, ЗП:	Република Србија		
Уже географско подручје, УГП:	Војводина		
Година, ГО:	2021.		
Издавач, ИЗ:	Ауторски репрингт		
Место и адреса, МА:	Нови Сад; трг Доситеја Обрадовића 6		
Физички опис рада, ФО: (поглавља/страница/цитата/табела/слика/графика/прилога)	7/31/7/1/18/0/0		
Научна област, НО:	Електротехника и рачунарство		
Научна дисциплина, НД:	Рачунарска техника		
Предметна одредница/Кључне речи, ПО:	Дигитална телевизија, Защита садржаја, CAS, Widevine, Лиценце		
УДК			
Чува се, ЧУ:	У библиотеци Факултета техничких наука, Нови Сад		
Важна напомена, ВН:			
Извод, ИЗ:	У овом раду је описано проширење за CAS систем заштите садржаја како би се добавио одговарајући идентификатор кључа на основу којег Widevine сервис за лиценцу одговара ЕММ поруком. Након примања ЕММ поруке (лиценце), сет-топ бокс је у стању да дескремблује садржај и користи га.		
Датум прихватања теме, ДП:			
Датум одбране, ДО:			
Чланови комисије, КО:	Председник:	проф. др Мирослав Поповић	
	Члан:	проф. др Иван Каштелан	Потпис ментора
	Члан, ментор:	проф. др Илија Башичевић	



KEY WORDS DOCUMENTATION

Accession number, ANO:		
Identification number, INO:		
Document type, DT:	Monographic publication	
Type of record, TR:	Textual printed material	
Contents code, CC:	Bachelor Thesis	
Author, AU:	Ksenija Popov	
Mentor, MN:	Ilija Bašičević, PhD	
Title, TI:	Support for dynamically generated keys in a conditional access system in digital television	
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:	2021.	
Publisher, PB:	Author's reprint	
Publication place, PP:	Novi Sad, Dositeja Obradovica sq. 6	
Physical description, PD: <small>(chapters/pages/ref./tables/pictures/graphs/appendices)</small>	7/30/7/1/18/0/0	
Scientific field, SF:	Electrical Engineering	
Scientific discipline, SD:	Computer Engineering, Engineering of Computer Based Systems	
Subject/Key words, S/KW:	Digital television, Content protection, CAS, Widevine, Licenses	
UC		
Holding data, HD:	The Library of Faculty of Technical Sciences, Novi Sad, Serbia	
Note, N:		
Abstract, AB:	This paper describes implementation of CAS system in order to supply key id based on which Widevine license service replies with EMM message. After getting EMM message (license), set-top box can descramble content and use it.	
Accepted by the Scientific Board on, ASB:		
Defended on, DE:		
Defended Board, DB:	President:	Miroslav Popović, PhD
	Member:	Ivan Kaštelan, PhD
	Member, Mentor:	Ilija Bašičević, PhD
		Menthor's sign

Zahvalnost

Zahvaljujem se Institutu RT-RK na pruženoj prilici za realizaciju ovog rada.

Takođe, zahvaljujem se mentoru, prof. dr Iliji Bašičeviću i tehničkom mentoru, Radenku Banoviću na stručnoj pomoći i savetima prilikom izrade rada.

Na kraju, posebno se zahvaljujem svojoj porodici i prijateljima na neizmernoj podršci koju su mi pružili tokom čitavog školovanja.



УНИВЕРЗИТЕТ У НОВОМ САДУ

ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА



SADRŽAJ

1.	Uvod	1
2.	Teorijske osnove.....	3
2.1	Digitalna televizija	3
2.2	MPEG-2, PES i TS paketi.....	5
2.3	Zaštita sadržaja.....	7
2.3.1	Skremblovanje.....	7
2.3.2	Deskremblovanje	8
2.3.3	Enkripcija	8
2.3.4	Dekripcija	8
2.3.5	ECM i EMM poruke.....	8
2.3.6	Sistem sa uslovnim pristupom.....	9
2.4	<i>Widewine</i>	10
2.4.1	<i>Widewine CAS</i>	11
2.4.1.1	<i>Widewine CAS za Android TV</i>	13
2.4.2	<i>Widewine DRM</i>	13
2.5	HTTP	13
2.6	JSON	14
3.	Koncept rešenja	15
3.1	Predajna i prijemna strana.....	15
3.2	Opis ciljne platforme.....	17
4.	Programsko rešenje.....	18
4.1	ECM generator.....	18
4.2	CAS <i>Proxy</i>	20

4.3	MediaCAS.....	23
4.4	TSDuck	24
5.	Rezultati.....	25
6.	Zaključak	28
7.	Literatura	30

SPISAK SLIKA

Slika 2.1 Tipovi prenosnog puta i faze isporuke TV sadržaja	4
Slika 2.2 Mapa sveta sa korišćenim standardima	5
Slika 2.3 Struktura PES paketa	6
Slika 2.4 Struktura TS paketa	6
Slika 2.5 Simultano kriptovanje i multikriptovanje.....	10
Slika 2.6 <i>Widevine</i> logo	11
Slika 2.7 Funkcionalne celine u okviru <i>Widevine</i> CAS rešenja	12
Slika 2.8 Primer JSON poruke.....	14
Slika 3.1 Komunikacija sa predajne strane	16
Slika 3.2 Komunikacija sa prijemne strane	16
Slika 3.3 Razvojna platforma.....	17
Slika 4.1 Generisanje zahteva za licencu	21
Slika 4.2 Generisanje zahteva za licencu	22
Slika 4.3 Slanje zahteva za licencu	22
Slika 4.4 Funtcionisanje CAS <i>plugin-a</i>	24
Slika 5.1 Primer sadržaja ECM poruke	25
Slika 5.2 Informacije ključeva, JSON poruka i odgovora	26
Slika 5.3 Izgenerisan zahtev	26

SPISAK TABELA

Tabela 5.1 Testni slučajevi 27

SKRAĆENICE

API - *Application Programming Interface* - Aplikativni programski interfejs

CA - *Conditional Access* - Uslovni pristup

CAS - *Conditional Access System* - Sistem sa uslovnim pristupom

DRM - *Digital Rights Management* - Sistem za zaštitu digitalnih prava

ECM - *Entitlement Control Message* - Poruka za kontrolu pristupa

EMM - *Entitlement Management Message* - Poruka za upravljanje pristupom

HTTP - *Hypertext Transfer Protocol* - Protokol za prenos hiperteksta

JSON - *JavaScript Object Notation* - Tekstualni format za razmenu podataka

OTT - *Over the Top* - Servis za emitovanje sadržaja putem interneta

SCS - *Simulcrypt Synchronizer* - Sinhronizator za simultano kriptovanje

SDK - *Software Development Kit* - Okruženje za razvoj programske podrške

SoC - *System on Chip* - Integracija većine računarskih komponenti pomoću čipa

1. Uvod

Pod uticajem razvoja novih tehnologija, digitalna televizija je postala jedan od masovnijih medija. Tome su doprineli veća pouzdanost uređaja i sistema za digitalnu televiziju i njegove operativne mogućnosti, lakši prenos i obrada digitalnog signala, kvalitetnija slika i dr. Samim tim, veća dostupnost sadržaja ukazala je na potrebu adekvatne zaštite, od neželjenih korisnika i piraterije. U tu svrhu, kompanija *Google* razvila je *Widevine*, tehnologiju koja omogućava besplatnu i efikasnu zaštitu za video i audio sadržaj visokog kvaliteta.

Od značaja za ovaj projekat predstavljen je CAS sistem. Dato je i njegovo poređenje sa DRM sistemom, mada razlike između ova dva sistema za zaštitu sadržaja polako nestaju. Razlika između CAS i DRM sistema je u tome što se prvi koristi samo za zaštitu sadržaja tokom transporta, a drugi štiti sadržaj i tokom transporta i na uređaju.

U ovom zadatku je opisano proširenje za CAS sistem zaštite sadržaja kod koga se ključevi za dešifrovanje dobavljaju u okviru prenosnog toka podataka, dok se kod DRM sistema ključevi za dešifrovanje dobavljaju van prenosnog toka podataka.

Cilj realizacije ovog rada je proširenje postojećeg rešenja za emitovanje TV sadržaja na bazi *Google Widevine* algoritma. Trenutno rešenje koristi fiksni ključ, dok proširenje treba da omogući dinamičko preuzimanje ključa na bazi identifikatora sadržaja.

Ovaj rad je sačinjen od 7 poglavlja:

1. Uvod - u ovom poglavlju nalaze se osnovne informacije o radu i kratak opis rada.
2. Teorijske osnove - drugo poglavlje sadrži teorijske osnove koje su neophodne za razumevanje načina funkcionisanja digitalne televizije, formata za prenos

digitalnih TV podataka, kao i najznačajnije stavke koje se tiču zaštite sadržaja, CAS sistema i tehnologije *Widevine* sa svojim rešenjima.

3. Koncept rešenja - treće poglavlje sadrži opšti koncept rešenja i analizu zadatog problema. Dat je opis komunikacije između komponenti kako bi se dobavili odgovarajući ključevi koji su potrebni da se zaštiti prenosni tok.
4. Programsко rešenje - u četvrtom poglavlju je detaljnije opisana realizacija programskih modula.
5. Rezultati - u petom poglavlju su opisani postupci ispitivanja i data je evaluacija rada rešenja.
6. Zaključak - šesto poglavlje sadrži kratak pregled šta je realizovano u radu.
7. Literatura - sedmo poglavlje sadrži spisak literature koja se koristila za pisanje rada.

2. Teorijske osnove

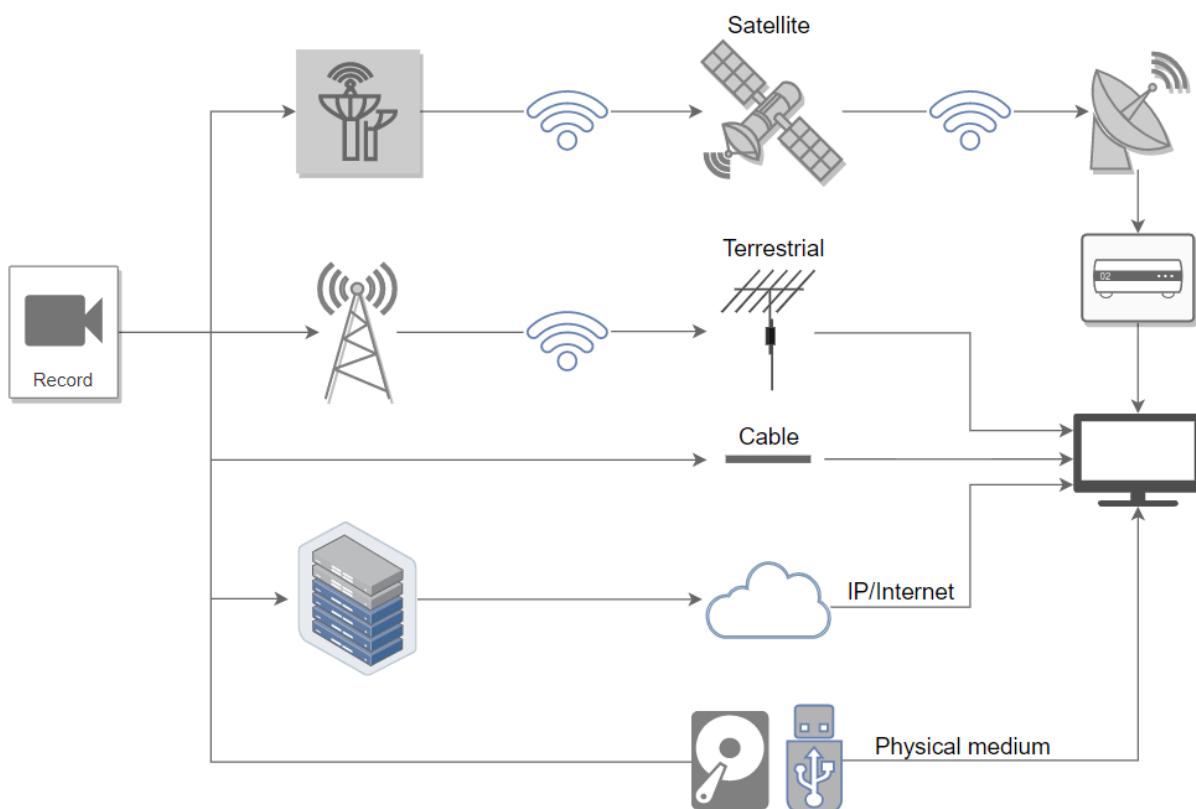
U ovom poglavlju opisane su teorijske osnove na kojima je ovaj rad zasnovan. Dat je koncept digitalne televizije, formata za prenos digitalnih TV podataka, opis zaštite sadržaja sa svojim operacijama i opis CAS sistema. Zatim je objašnjena namena tehnologije *Widevine*, njegovih rešenja *Widevine DRM* i *Widevine CAS* sa akcentom na *Widevine CAS* i njegova podrška za *Android TV*. Na samom kraju, ono što je takođe značajno za projekat predstavlja opis HTTP protokola i JSON poruke.

2.1 Digitalna televizija

Digitalna televizija predstavlja prenos pokretnih slika, zvuka i dodatnih informacija od emitera do gledalaca digitalnim putem. Dodatne informacije obuhvataju: metapodatke kako bi se razvrstali audio i video sadržaj po programima, nazine programa, tekstualne opise, žanrove, vreme, datum i drugo. Neke od značajnih prednosti koje pruža digitalna televizija podrazumevaju kvalitetniju sliku i zvuk, mogućnost gledanja u pokretu na bilo kom mestu, izbor audio jezika i jezika za prevod, roditeljsku kontrolu, digitalni teletekst, izbor audio i video formata od strane korisnika, interaktivnu televiziju i pristup internetu [1].

Televiziju, prema tipu prenosnog puta, klasifikujemo kao:

- Satelitsku (eng. *Satellite*)
- Zemaljsku (eng. *Terrestrial*)
- Kablovsku (eng. *Cable*)
- Televiziju putem interneta (eng. *IPTV*)
- Televiziju na fizičkom medijumu (eng. *TV on physical medium*)



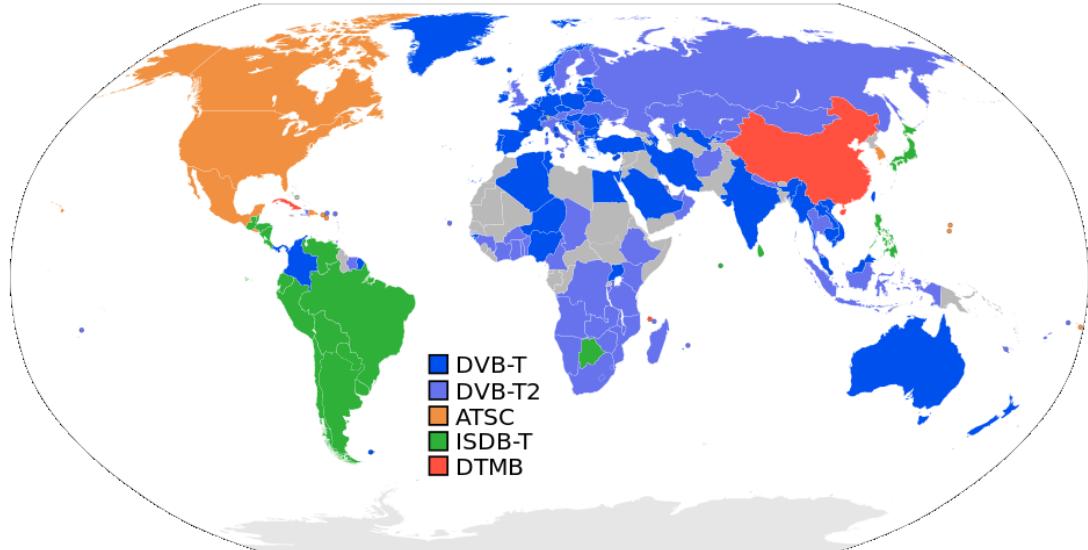
Slika 2.1 Tipovi prenosnog puta i faze isporuke TV sadržaja

Da bi se digitalni TV sadržaj preneo, postoje unapred definisana pravila prenosa. Ta pravila prenosa se nazivaju standardi. Najznačajniji standardi digitalne televizije su:

- **DVB (Digital Video Broadcasting)** - standardi za isporuku digitalnog audio i video sadržaja. Iz DVB standarda je proizašao veliki broj standarda za digitalno TV emitovanje. Najznačajniji su standardi za digitalnu zemaljsku televiziju (DVB-T i DVB-T2), digitalnu kablovsku televiziju (DVB-C) i digitalnu satelitsku televiziju (DVB-S). Koriste se u Evropi, Rusiji, Australiji i većem delu Afrike.
- **ATSC (Advanced Television Systems Committee)** - standardi za satelitsku, zemaljsku i kablovsku digitalnu televiziju. Zastupljeni u SAD, Kanadi, Meksiku, Južnoj Koreji, Dominikanskoj Republici, Gvatemali, El Salvadoru, Hondurasu, Antigvi i Barbudi. Razvoj ATSC standarda je pod kontrolom Sjedinjenih Američkih Država od njegovog početka do danas.
- **ISDB (Integrated Services Digital Broadcasting)** - ovu grupu standarda čine standardi za zemaljsko i mobilno emitovanje (ISDB-T), standardi za satelitsko emitovanje (ISDB-S) i standardi za kablovsko emitovanje (ISDB-C). Zastupljeni

su u Japanu. Prelazak na ISDB-T standard u Brazilu, Argentini, Čileu, Kosta Riki, Ekvadoru, Filipinima, Maldivima, Boliviji i dr. je još uvek u toku.

- DTMB (*Digital Terrestrial/Television Multimedia Broadcasting*) - standard za digitalno zemaljsko TV emitovanje. Razvijen je u Kini.



Slika 2.2 Mapa sveta sa korišćenim standardima

2.2 MPEG-2, PES i TS paketi

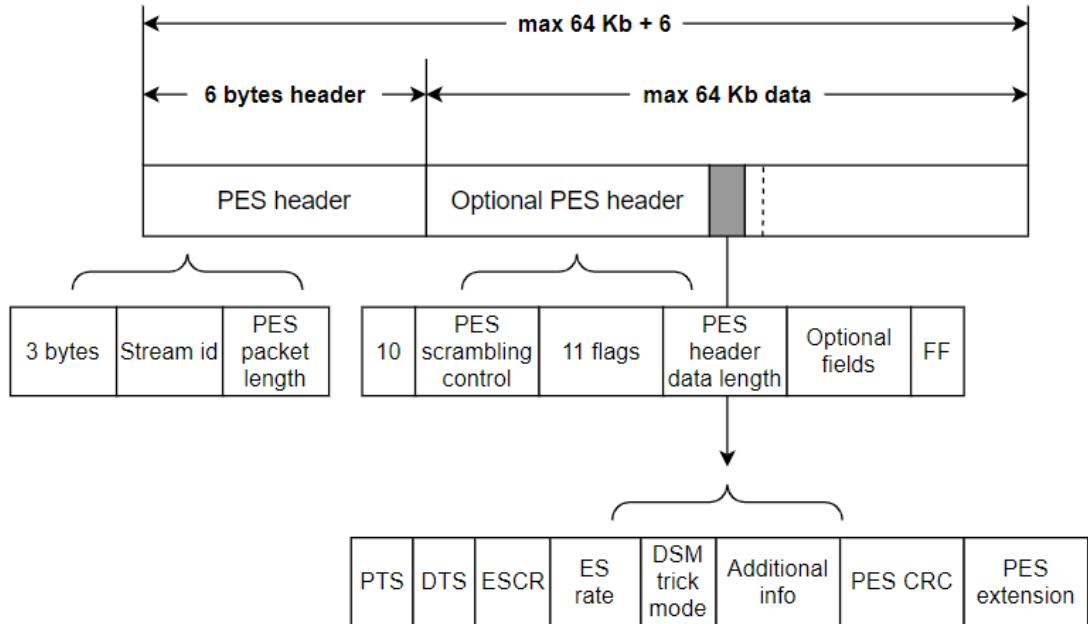
U digitalnoj televiziji, najčešće korišćen standard za kontejnerske formate je MPEG-2 (eng. *Moving Picture Experts Group*) koji definiše način formatiranja delova TV sadržaja i njihovo kombinovanje u jedan bitski tok. Neki od ostalih korišćenih standarda su: ASF (eng. *Advanced Systems Format*), AVI (eng. *Audio Video Interleave*), 3GP (eng. *Third Generation Partnership Project*), IFF (eng. *Interchange File Format*) i dr.

Postoje dva tipa kontejnerskih formata u okviru MPEG-2 standarda:

1. Prenosni tok (eng. *MPEG Transport Stream*, MPEG-TS) - može da sadrži jedan ili više kanala. Koristi se kod prenosa emisionim putem, ali i u slučaju nepouzdanog prenosa na transportnom nivou.
2. Programski tok (eng. *MPEG Program Stream*, MPEG-PS) - može da sadrži samo jedan kanal. Za razliku od prenosnog toka, programski tok se koristi kod skladištenja na fizičku memoriju.

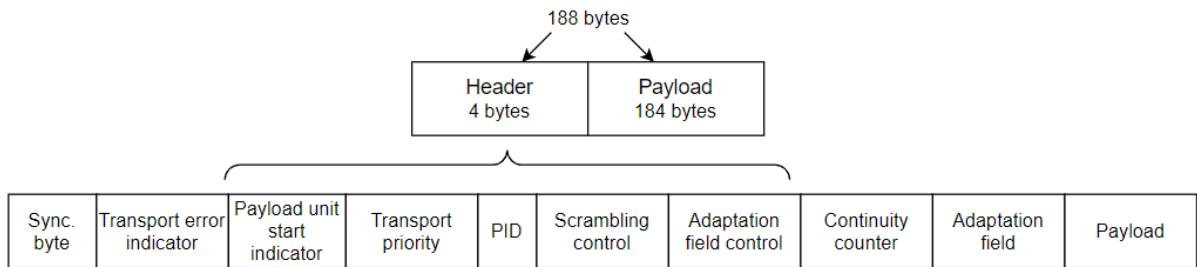
Prenosni ili programski tokovi se sastoje od elementarnih tokova. Jedan elementarni tok prenosi jednu komponentu servisa kao što je video tok, prevod, teletekst i slično. Proces u kojem se više elementarnih tokova prenosi u jedan bitski tok tako što se elementarni tokovi

dele u najmanje jedinice prenosa tj. pakete, koji se naizmenično šalju u vremenu, naziva se multipleksiranje (eng. *multiplexing*). Najmanja jedinica prenosa koja je i osnova za postupak multipleksiranja predstavlja paket prenosnog toka (eng. *Packetized Elementary Stream Packet*, PES).



Slika 2.3 Struktura PES paketa

Pre procesa multipleksiranja svi elementarni tokovi se dele u PES pakete koji su promenljive veličine. Maksimalna veličina paketa je definisana i potrebna u slučaju vremenskog multipleksiranja elementarnih tokova koji za cilj imaju reprodukciju u realnom vremenu. S obzirom na promenljivu veličinu, PES paketi nisu pogodni za prenos emisionim putem. Svaki PES paket se iz tog razloga deli na pakete prenosnog toka (eng. *Transport Stream Packets*, TS), koji imaju konstantnu veličinu manjeg broja bita što ih čini pogodnijim za emisioni prenos.



Slika 2.4 Struktura TS paketa

TS paket sadrži zaglavje (eng. *Header*) veličine 4 bajta i deo za podatke (eng. *Payload*) veličine 184 bajta. Najznačajnije polje u TS zaglavljtu je paketski identifikator (PID) koji definiše sadržaj TS paketa i omogućava demultiplexiranje prenosnog toka na prijemnoj strani. Osim navedenog, zaglavje sadrži polja kao što su: indikator početka jedinice podataka (eng. *Payload Unit Start Indicator*), brojač kontinuiteta (eng. *Continuity Counter*), adaptaciono polje (eng. *Adaptation Field*), polje za kontrolu adaptacionog polja (eng. *Adaptation Field Control*) itd.

2.3 Zaštita sadržaja

Kompletan put od proizvodjača sadržaja, ili nosioca prava za prenos sadržaja i njegovo emitovanje, pa do krajnjeg korisnika zahteva zaštitu u svim njegovim delovima. Obično se zaštita sadržaja (eng. *content protection*) poverava kompanijama koje nude uređaje koji služe za skremblovanje, deskremblovanje, enkripciju, dekripciju i sigurne razmene pristupnih ključeva. Prethodno nabrojane operacije su veoma bitne za zaštitu sadržaja i o njima je dat opis u nastavku, kao i opis CAS sistema.

2.3.1 Skremblovanje

Skremblovanje (eng. *scrambling*) je proces zaštite digitalnog TV signala koji se postiže tako što se dodaju ili se menjaju neke važne komponente originalnog signala i time se onemogućava njegova nedozvoljena reprodukcija.

Algoritmi za skremblovanje se sastoje od algoritma za šifrovanje na dva nivoa:

1. Blokovskog nivoa - realizuje se tako što se podaci organizuju u blokove fiksne veličine, nakon čega se vrši manipulacija bajtovima po određenom algoritmu unutar blokova, npr. zamena kolona sa vrstama, čitanje po dijagonali i slično. Ovaj nivo se može dodatno osigurati tako što se već skremblovani blok kombinuje sa blokom koji tek treba da se skrembluje.
2. Nivoa toka podataka - definiše pravilo čitanja kolona iz svakog bloka. Pomoću ključa odnosno kontrolne reči određuje se rezultujući poredak bajtova. Duža kontrolna reč dovodi do većeg broja kombinacija izlaznih bajtova te samim tim i veće sigurnosti, ali i potrebe za većom procesorskom snagom.

2.3.2 Deskremblovanje

Deskremblovanje (eng. *descrambling*) se obavlja u uređaju koji se naziva deskrembler i koji je smešten na prijemnoj strani. Proces deskremblovanja se vrši tako što se od skremblovanog odnosno zaštićenog signala dobija originalni signal koji se dalje prosleđuje audio i video dekoderima. Da bi deskremblovanje bilo uspešno, deskrembler mora imati informacije o algoritmu na osnovu kojeg je izvršeno skremblovanje [2].

2.3.3 Enkripcija

Za razliku od skremblovanja, enkripcija (eng. *encryption*) se koristi da opiše proces zaštite ključeva koji se takođe štite prilikom prenosa. Proces funkcioniše tako što se uzmu podaci koje je moguće pročitati i zatim se oni menjaju po određenom algoritmu. Ključevi enkriptuju (zaključavaju) podatke tako da samo onaj korisnik sa odgovarajućim ključem može da pristupi tim podacima odnosno da ih dekriptuje [3].

2.3.4 Dekripcija

Dekripcija (eng. *decryption*) predstavlja proces koji je obrnut enkripciji. To znači da se obavlja konverzija enkriptovanih podataka u njihov originalni oblik koji je moguće razumeti. Podatke je moguće dekriptovati pomoću odgovarajućeg ključa ili šifre. Dekripcija se odvija na prijemnoj strani [4].

2.3.5 ECM i EMM poruke

Postizanje deskremblovanja prenosnog toka i njegovo dalje korišćenje u okviru digitalnog TV prijemnika, zahteva pristup odgovarajućim ključevima koji se emituju u okviru ECM i EMM poruka.

ECM poruku generiše ECM generator na predajnoj strani. Nju koristi skrembler da bi izvršio skremblovanje sadržaja i smešta je u prenosni tok koji se dalje šalje prijemnim stranama. Najvažnija informacija koja se nalazi u ECM poruci predstavlja ključ ili kontrolna reč. Ta informacija je bitna kako bi uređaj (npr. set-top boks) upotrebom ključeva mogao da deskrembluje prenosni tok. Ključevi se menjaju učestalo da bi se otežalo pristupanje porukama od strane korisnika koji nemaju pravo pristupa. Unutar ECM poruke, kontrolne reči su enkriptovane kako bi se postiglo da i ako se dobavi ECM poruka, ne može se iskoristiti kontrolna reč za deskremblovanje prenosnog toka. Da bi se enkriptovana kontrolna reč unutar ECM poruke dekriptovala, potreban je poseban ključ koji se nalazi u EMM poruci. Nakon toga, EMM poruku prima uređaj i pomoću nje dekriptuje sadržaj. Ovakve poruke se mogu

prenositi emisionim putem, ali i na druge načine, kao što su telefonske linije, internet, pametne kartice itd [5].

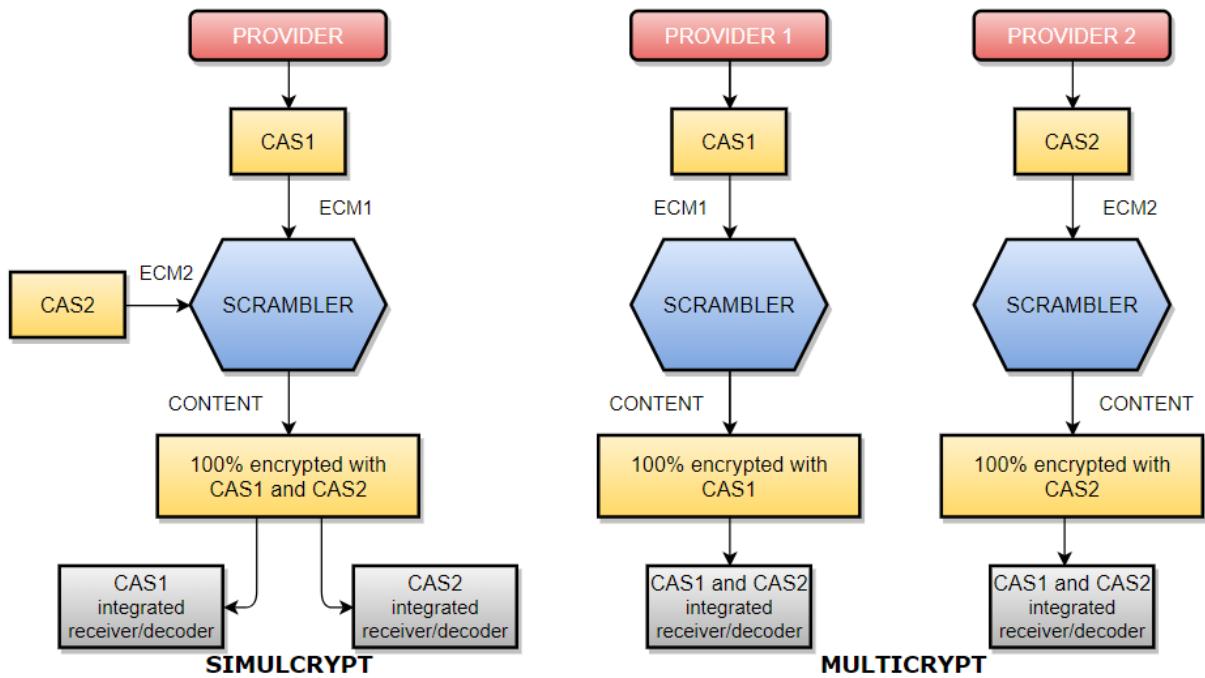
2.3.6 Sistem sa uslovnim pristupom

CAS sistem ili CA sistem koristi skremblovanje i enkripciju da zaštitи sadržaj tokom transporta. Osnovna svrha CAS sistema jeste da odredi koji set-top boks dekoderi i prijemnici će biti u mogućnosti da isporuče određene programske servise do krajnjeg korisnika. Cilj je da se osigura da servisi budu pristupačni samo onima koji imaju odgovarajuća prava. Razlozi zbog kojih je potrebno da sadržaj bude ograničen: da se izvrši plaćanje od strane korisnika kako bi se omogućio pristup kanalima i da se ograniči pristup određenom geografskom području zbog razmatranja programskih prava (što se može postići ako uređaj ima ugrađeni GPS sistem). Operateri TV kanala koriste ovakav sistem da omoguće preplatnicima pristup sadržaju, a oni koji nisu preplaćeni nemaju takvih prava. Korisnici mogu da pristupe sadržaju putem pametnih kartica koje su slične kreditnim karticama ili autorizacijom uređaja od strane korisničkog servisa operatera. Korisnici mogu da menjaju kanale bez potrebe za autentifikacijom pri promeni kanala i u svakom trenutku imaju pristup svim servisima tog prenosnog toka [6].

Da gledaoci ne bi posedovali više sistema sa uslovnim pristupom, DVB standard uvodi dve realizacije sistema za uslovni pristup:

1. Simultano kriptovanje (eng. *Simulcrypt*) - enkriptuje se sadržaj upotrebom jednog ključa koji dele dva različita CAS sistema koji moraju generisati dve različite ECM poruke za korisnike. Koristi se najviše u Evropi [7].
2. Multikriptovanje (eng. *Multicrypt*) - enkripcija sadržaja se vrši tako što svaki CAS sistem poseduje svoj ključ i generiše jedinstvenu ECM poruku za korisnika. Multikriptovanje je zakonom propisano u Španiji [7].

Prednost multikriptovanja u odnosu na simultano kriptovanje je u tome što ne zahteva pisane ugovore između operatera, a prednost simultanog kriptovanja je u tome što je njegova implementacija jeftinija. U slučaju multikriptovanja potrebna su veća ulaganja koja se tiču izrade posebnih modula i slično. Na slici 2.5 je prikazana funkcionalnost simultanog kriptovanja i multikriptovanja.



Slika 2.5 Simultano kriptovanje i multikriptovanje

2.4 *Widevine*

Widevine je osnovan 1999. godine sa ciljem da postane internacionalni operater za optimizaciju videa i zaštitu sadržaja. U decembru 2010. godine kompanija *Google* ga je preuzeila. Njegove usluge koriste mnoge kompanije: *Netflix*, *HBO*, *Google Chrome*, *Firefox*, *Facebook*, *Android*, *LG*, *Sony*, *Warner Bros*, *Disney* i druge.

Widevine predstavlja jednu od vodećih platformi za isporuku sistema za zaštitu sadržaja visoke definicije i trenutno je dostupan na 5 biliona uređaja, kao što su npr. mobilni telefoni, set-top boksevi, televizori i računari. Pruža besplatno rešenje (eng. *open source*) koje predstavlja prekretnicu u polju digitalne zaštite sadržaja. Mnogi operateri i vlasnici sadržaja koriste *Widevine*-ova rešenja kako bi njihove usluge bile osigurane na putu do uređaja koje potrošači koriste. Podržava razne enkripcione šeme i zaštitu hardvera u skladu sa pravilima koja određuju vlasnici sadržaja kako bi se ograničio pristup potrošača tom sadržaju. Bilo koji uređaj koji podržava *Widevine* mora podržavati nivoe zaštite L1, L2 i L3 (najviši nivo zaštite). Da bi se omogućilo prikazivanje kvalitetnijeg sadržaja (npr. HD rezolucija), uređaj mora da poseduje L3 zaštitu [8] [9].

Widevine pruža dva rešenja: *Widevine CAS* i *Widevine DRM* koji su opisani u nastavku.



Slika 2.6 *Widevine* logo

2.4.1 *Widevine CAS*

Widevine-ovo CAS rešenje predstavlja veliki napredak u okviru industrije za emitovanje TV sadržaja i podstiče narednu generaciju operatera, pružajući besplatno rešenje za zaštitu sadržaja. U poslednje vreme, prenos TV sadržaja emisionim putem se postepeno zamenjuje prenosom putem interneta. Potreban korak koji doprinosi tome predstavlja spajanje tehnologija za emitovanje TV sadržaja sa OTT¹ tehnologijom, zbog čega *Widevine* CAS pruža saradnju sa ovom tehnologijom [10].

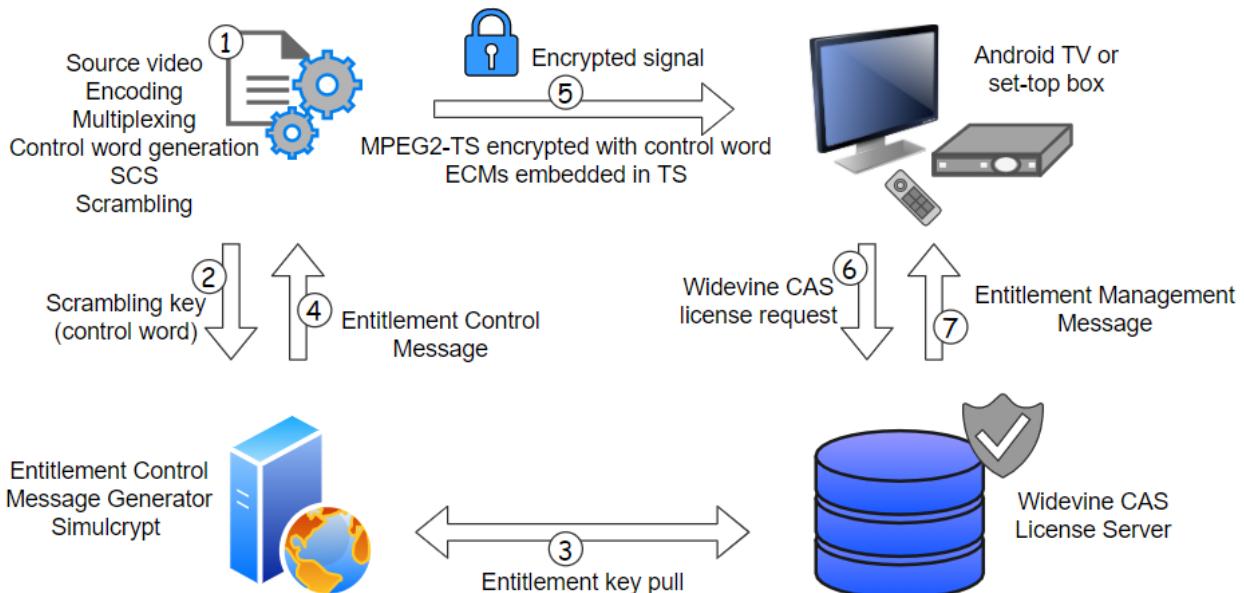
Widevine CAS rešenje [11] uključuje:

- *Widevine* uređaje (eng. *Widevine Devices*) - bezbednost uređaja je pouzdana. Koriste se postojeće sigurnosne arhitekture L1. Omogućuje brz ravoj i sertifikaciju. Podržava postojeća SoC² rešenja. Ima podršku za rad sa Android TV-om.
- *Widevine* hibrid (eng. *Widevine Hybrid*) - CAS se nadovezuje na postojeći OTT sigurnosni stek. Omogućava brzu integraciju Android TV-a preko MediaCAS API-a. Pravi fuziju CAS i DRM rešenja.
- *Widevine* uslugu (eng. *Widevine Provisioning*) - fleksibilan i skalabilan SDK. Dostupno za bilo koji *middleware*³.
- *Widevine* licence (eng. *Widevine Licenses*) - bez naknade za *Widevine* klijentske ili serverske proizvode. Skalabilan i fleksibilan SDK.

¹ OTT (Over-the-Top) predstavlja servis za emitovanje sadržaja putem interneta, pri čemu se sadržaju pristupa preko mobilnih telefona, računara, pametnih TV- a itd.

² SoC (System on Chip) predstavlja čip koji integriše većinu računarskih komponenti ili drugih elektronskih sistema.

³ Middleware je softver koji omogućava servise softverskim aplikacijama izvan okvira operativnog sistema.



Slika 2.7 Funkcionalne celine u okviru *Widevine* CAS rešenja

Funkcionalne celine unutar *Widevine* CAS rešenja (slika 2.7):

1. Na strani operatera, skrembler enkriptuje video sa ključevima za skremblovanje (kontrolne reči) koji se učestalo menjaju. Ova funkcionalnost se obično obavlja od strane multipleksera.
2. SCS šalje ključeve do ECM generatora i on ih spaja zajedno sa drugim *entitlement* ključem koji se povremeno menja.
3. ECM generator komunicira sa *Widevine* serverom za licencu kako bi izdvojio *entitlement* ključeve.
4. ECM generator stavlja spojene ključeve zajedno sa metapodacima u ECM poruku i šalje nazad do SCS-a.
5. Operater šalje ECM poruku do prijemnog uređaja (npr. Android TV ili set-top boks) zajedno sa enkriptovanim videom.
6. Set-top boks ili Android TV komunicira sa serverom za licencu i zahteva *entitlement* ključ preko HTTP protokola.
7. Ako je korisnik ovlašćen, dostavljaju mu se EMM poruke iz kojih se izdvajanjem *entitlement* ključeva dekriptuju kontrolne reči u okviru ECM poruke. Na osnovu toga uređaj može da dekriptuje sadržaj i pusti ga korisniku.

2.4.1.1 **Widevine CAS za Android TV**

Widevine CAS je otvorenog koda i ima podršku za rad sa *Android TV*-om. Kompanija *Google* nudi komponente *Widevine* CAS rešenja, koje se oslanjaju na *Widevine* DRM rešenje, kao deo *Android TV*-a, što dosta smanjuje primene i troškove usluga emitovanja i televiziju putem interneta. *Widevine* CAS pruža zaštitu na *Android TV* 9+ set-top boksevima. Takođe, podržava 4K Ultra HD rezoluciju [12].

2.4.2 **Widevine DRM**

Widevine-ovo DRM rešenje omogućava bezbednu distribuciju, licenciranje i zaštitu sadržaja na bilo kom potrošačkom uređaju. Opremljen je sa HTML5 video plejerom koji podržava adaptivni striming. Omogućava reprodukciju sadržaja bilo gde, jer koristi široko zastupljene medijske formate kao što su ISO BMFF (npr. MP4) i WebM. Proces komunikacije između različitih *Widevine* uređaja je jednostavan. Rešenje je fleksibilno što ga čini pogodnim za adaptaciju u narednim generacijama uređaja [13].

2.5 HTTP

HTTP je najkorišćeniji protokol za prenos informacija putem interneta, a njegova osnovna namena je prenos hiper teksta odnosno isporučivanje veb stranica koje su napisane HTML programskim jezikom i koristi se pri radu sa *World Wide Web*-om. HTTP predstavlja zahtev/odgovor protokol za obavljanje komunikacije između servera i klijenta. Server konstantno osluškuje zahteve na odgovarajućem portu (uglavnom se koristi port 80, a može i port 8080) i čeka da se klijent poveže i pošalje zahtev. Ranije nije postojala stalna konekcija između servera i klijenta, nego nakon što klijent odgovori, prekidala se konekcija sve do sledećeg zahteva. Sa verzijom HTTP 1.1 podržana je mogućnost stalne konekcije. Prva verzija HTTP protokola je posedovala samo jednu vrstu zahteva sa kojom se zahtevala stranica sa servera, ali dodavanjem novih operacija i linija u zaglavlju, nastao je poboljšan HTTP protokol koji je od 1996. godine podržan od strane svih poznatih veb pregledača. Protokol koristi odgovarajuće metode pomoću kojih definiše zahtev i parametre serveru, a neke od njih su: GET, POST, PUT, HEAD, DELETE [14].

Uopšteni izgled prve linije HTTP zahteva: metod /putanja HTTP/verzija, primer GET /home/index.html HTTP/1.1

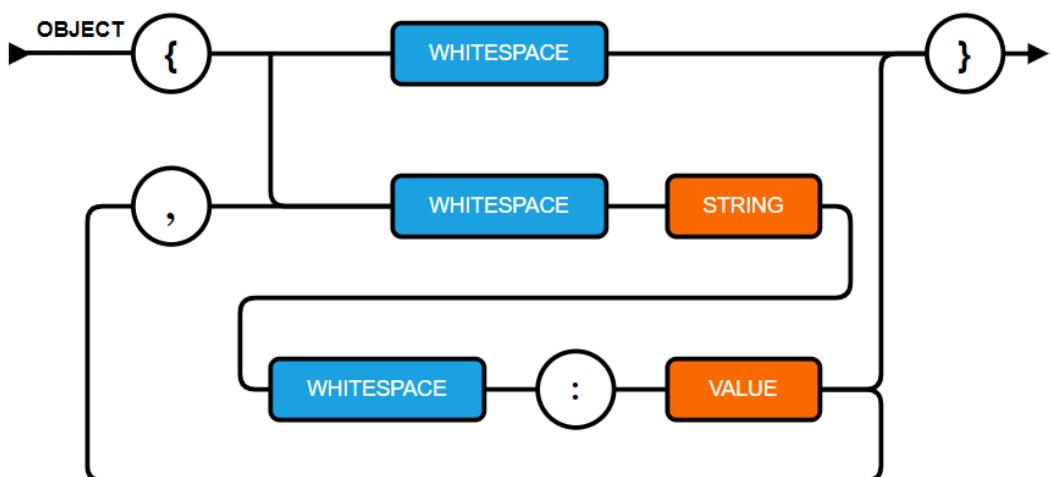
Uopšteni izgled prve linije HTTP odgovora: HTTP/verzija statusni kod, primer HTTP/1.1 200 OK

Ukoliko se putem HTTP zahteva prosleđuju određeni resursi i ukoliko server vraća određene resurse klijentu, oni se skladište u telu HTTP poruke.

2.6 JSON

JSON predstavlja tekstualni standard za prenos podataka baziran na *JavaScript* sintaksi objekta. JSON je tekst koji može da se lako konvertuje i parsira u odgovarajući oblik. Najčešće se koristi za prenos podataka preko mreže, npr. u veb aplikacijama kao što je slanje podataka od servera prema klijentu kako bi se sadržaj prikazao na određenoj veb stranici ili obrnuto. Koristi konvencije koje su poznate programerima *C* grupe programskega jezika kao što su *C*, *C++*, *Java*, *JavaScript*, *Python* i mnogi drugi. Opšti oblik JSON-a je: {"key1": "value1", "key2": "value2"} [15].

Na slici 2.8 je prikazan jedan primer kako izgleda JSON poruka sa objektom koji se sastoji od parova imena i vrednosti, gde svako ime ide uz dvotačku i svaki par je odvojen zarezom.



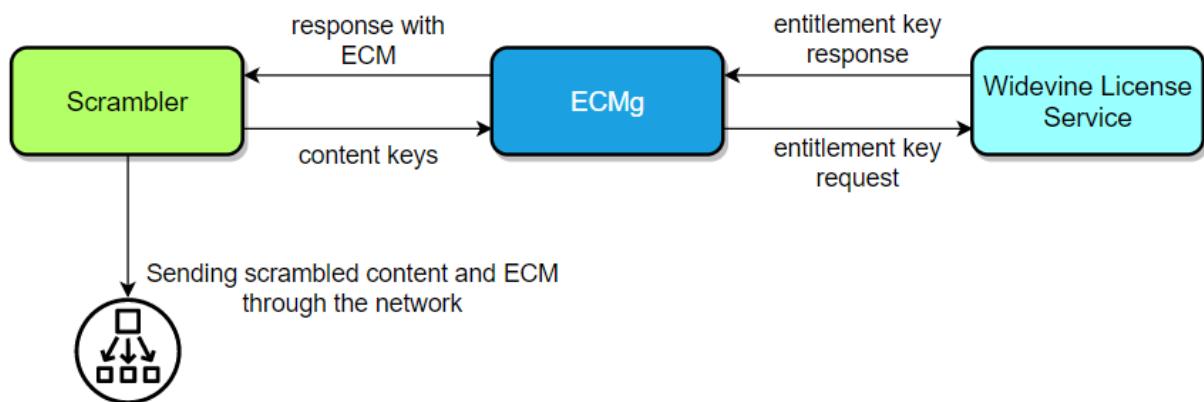
Slika 2.8 Primer JSON poruke

3. Koncept rešenja

U ovom poglavlju dat je koncept rešenja koji se sastoji od četiri glavne celine: *Widevine* servisa za licencu, ECM generatora, CAS *Proxy*-a i set-top boks uređaja, čije funkcionalnosti i komunikacije su opisane u nastavku.

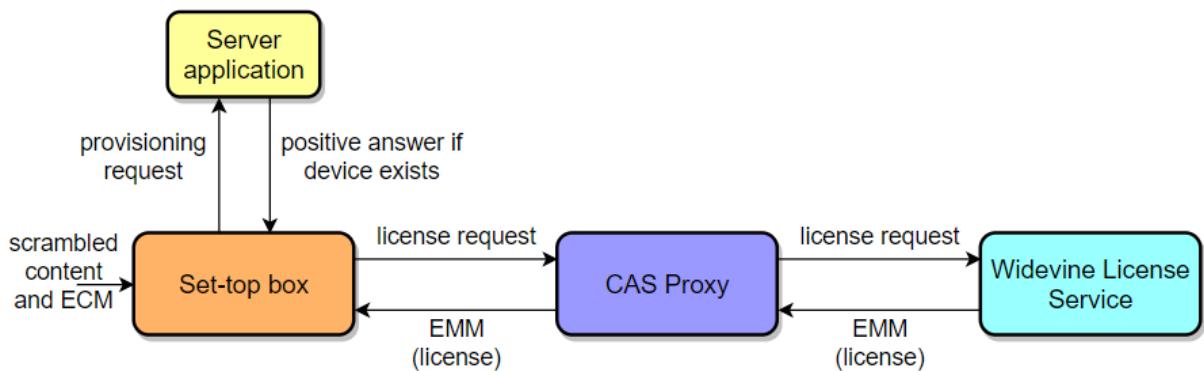
3.1 Predajna i prijemna strana

Na predajnoj strani nalazi se skrembler koji komunicira sa ECM generatorom koji komunicira sa *Widevine* servisom za licencu sa ciljem da se dobave *entitlement* ključevi koji su potrebni za enkriptovanje *content* ključeva kako bi skrembler mogao da zaštitи sadržaj. Skrembler prvo generiše *content* ključeve i šalje ključeve ECM generatoru. Zatim ECM generator šalje zahtev za *entitlement* ključeve (*entitlement key request*) *Widevine* servisu za licencu. Kao odgovor dobijaju se *entitlement* ključevi, pomoću kojih ECM generator enkriptuje *content* ključeve, takođe u odgovoru se dobija identifikator *entitlement* ključa. Nakon enkriptovanja *content* ključeva, ECM generator ključeve smešta u ECM poruku zajedno sa identifikatorom i to prosleđuje skrembljeru. Skrembler zatim vrši skremblovanje prenosnog toka *content* ključevima koji su na početku generisani, nakon čega se skremblovan sadržaj šalje kroz mrežu zajedno sa ECM porukom. Na slici 3.1 je prikazana komunikacija sa predajne strane, odnosno komunikacija između skremблера, ECM generatora i *Widevine* servisa za licencu.



Slika 3.1 Komunikacija sa predajne strane

Sa prijemne strane nalazi se set-top boks uređaj koji prima skremblovan sadržaj i ECM poruku. Da bi mogao da deskrembluje sadržaj, potrebna mu je EMM poruka odnosno licenca. Set-top boks prvo šalje *provisioning request*, sa kojim proverava da li uređaj ima prava pristupa, prema server aplikaciji koji je odgovoran za rukovanje uređajima. Ukoliko je uređaj prisutan u sistemu i pretplaćen, dobija se pozitivan odgovor. Nakon toga set-top boks šalje zahtev za licencu (*license request*) zajedno sa identifikatorom *entitlement* ključa (koji se nalazi u ECM poruci) ka CAS Proxy serveru koji zatim to prosleđuje Widevine servisu za licencu. Na osnovu identifikatora *entitlement* ključa, Widevine servis za licencu odgovara odgovarajućom EMM porukom koju *Proxy* prosleđuje ka set-top boksu. Nakon primanja EMM poruke, set-top boks pomoću *entitlement* ključeva iz EMM poruke dekriptuje *content* ključeve iz ECM poruke, nakon čega je u stanju da deskrembluje sadržaj i koristi ga. Na slici 3.2 je prikazana komunikacija sa prijemne strane, odnosno komunikacija između set-top boks uređaja, CAS Proxy-a i Widevine servisa za licencu.



Slika 3.2 Komunikacija sa prijemne strane

3.2 Opis ciljne platforme

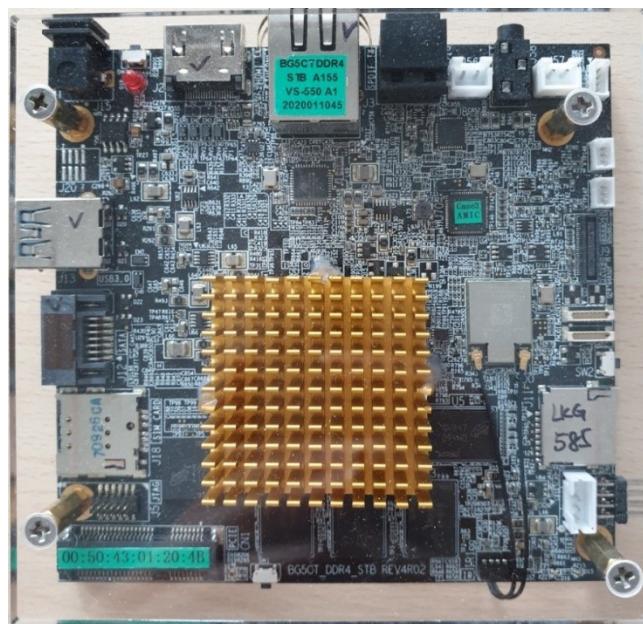
Za izradu zadatka koristila se platforma naziva *Synaptic BG5CT Android Q Platform*.

Specifikacije platforme:

- Centralni procesor: *Quad Core ARM Cortex A53 CPU, NEON CPU subsystem*
- Grafički procesor: *Imagination Technologies, PowerVR Rogue GE8310, 2.8 Gpixel per second GPU*
- RAM memorija: 1.5 GB
- *Marvell* čipset

Platforma sadrži veliki broj analognih i digitalnih ulaza i izlaza, a to su:

- USB port 3.0
- *Display port*
- SATA port
- JTAG port
- HDMI izlaz
- *spdif* izlaz
- UART *connector*
- IR *detector*
- Podrška za memorijsku karticu i SIM karticu
- Ethernet
- PCI-Express



Slika 3.3 Razvojna platforma

4. Programsко rešenje

U ovom poglavlju je opisano programsko rešenje za zadati problem. Rešenje je realizovano korišćenjem *C++* programskog jezika, na operativnom sistemu *Linux*.

4.1 ECM generator

Widevine pruža ECM generator biblioteku koja se integriše u postojeći sloj pristupa podacima skremblera kako bi se obavila enkripcija sadržaja. ECM generator i TS multiplekser kontrolišu vreme rotacije ključeva, pri čemu svaka promena ključa uzrokuje početak nove rotacije. Ako je rotacija ključeva *enable*, tada ECM sadrži par ključeva, parni (eng. *even*, *single*) i neparni (eng. *odd*) ključ.

Parni ključ sadrži sledeća polja (neparni ključ sadrži ista polja):

- *Entitlement_Key_ID* - identifikator ključa koji se koristi za dobavljanje EMM poruke
- *Content_Key_ID* - identifikator *content* ključa
- *Wrapped_Key_Data* - kontrolna reč
- *Wrapped_Key_IV* - inicijalni vektor za dekriptovanje enkriptovane kontrolne reči
- *Content_IV* - inicijalni vektor za dekriptovanje toka podataka

Opis programskih modula koji su se koristili za realizaciju ovog rada:

Klasa **WvCasKeyFetcher** omogućava komunikaciju sa *Widevine* servisom za licencu kako bi se dobavili *entitlement* ključevi. Argumenti (sadrže kredencijale *Widevine* servisa za licencu):

- *signing_provider* - ime operatera koji potpisuje enkriptovan CAS zahtev

- signing_key - ključ (u heksa obliku) za potpisivanje enkriptovanog CAS zahteva
- signing_iv - inicijalni vektor (u heksa obliku) za potpisivanje enkriptovanog CAS zahteva

Struktura **EntitlementRequestParams** sadrži polja koja su potrebna da bi se napravila poruka koja zahteva *entitlement* ključeve. Polja (sadrže kredencijale *Widevine* servisa za licencu):

- content_id - identifikator sadržaja
- content_provider - operater (u ovom slučaju operater je *iwedia*)
- track_types - željena rezolucija
- key_rotation - rotacija ključeva (tačno ili netačno)

Funkcija **CreateEntitlementRequest** omogućava pravljenje odgovarajuće poruke koja se koristi da zahteva *entitlement* ključeve od *Widevine* servisa za licencu. Argumenti:

- request_params - parametri potrebni za zahtevanje *entitlement* ključeva od servera
- signed_request_json - napravljena odgovarajuća poruka

Funkcija **MakeHttpRequest** pravi HTTP zahtev koji se šalje do *Widevine* servisa za licencu kako bi se dobavili *entitlement* ključevi. Argumenti:

- signed_request_json - HTTP zahtev koji se šalje do servera
- http_response_json - HTTP odgovor u JSON formatu

Funkcija **ParseEntitlementResponse** parsira poruku u kojoj se nalaze *entitlement* ključevi. Argumenti:

- http_response_json - poruka dobijena od servera u kojoj se nalaze *entitlement* ključevi
- entitlements - *entitlement* ključevi isparsirani iz niza znakova dobijenog od servera

Struktura **EntitlementKeyInfo** sadrži informacije potrebne kako bi se ubacili *entitlement* ključevi. Polja:

- is_even_key - ako je true, *entitlement* je paran ključ
- key_id - identifikator za *entitlement* ključ
- key_value - vrednost *entitlement* ključa
- track_type - rezolucija koja se koristi

Klasa **WvCasEcm** se koristi da se generišu ECM poruke. Argumenti:

- ecm_init_parameters - parametri za konfigurisanje ECM toka
- injected_entitlement - informacija o *entitlement* ključu

Funkcija **GenerateEcm** se koristi da se napravi ECM poruka koja će se ubaciti u polje za podatke TS paketa. Parametri:

- even_key - informacija o parnom ključu
- odd_key - informacija o neparnom ključu
- track_type - rezolucija koja se koristi
- serialized_ecm - pokazivač na memoriju lokaciju gde će se sačuvati generisana ECM poruka

Funkcija **GenerateTsPacket** generiše TS paket sa datim ECM porukama. Parametri:

- ecm - serijalizovana ECM poruka
- pid - identifikator programa za ECM tok
- table_id - identifikator tabele koji se nalazi u zaglavju TS paketa
- continuity_counter - brojač redosleda ECM paketa
- packet - bafer za generisane TS pakete

Struktura **WvCasContentKeyInfo** sadrži polja potrebna da bi se generisao deo ECM poruke zadužen za *content* ključeve. Polja:

- key_id - identifikator *content* ključa
- key - kontrolna reč
- content_iv - *content* inicijalni vektor
- wrapped_key_iv - inicijalni vektor koji se koristi za enkriptovanje ključa

Korišćena je *libcurl* biblioteka koja je otvorenog koda i koristi se za kreiranje i slanje HTTP zahteva.

4.2 CAS Proxy

CAS Proxy omogućuje operaterima sledeće:

- ispitivanje zahteva za licencu od strane CAS uređaja
- promenu i korišćenje specifičnih pravila za bilo koji CAS zahtev za licencu
- dobijanje CAS licence od *Widevine* servisa za licencu

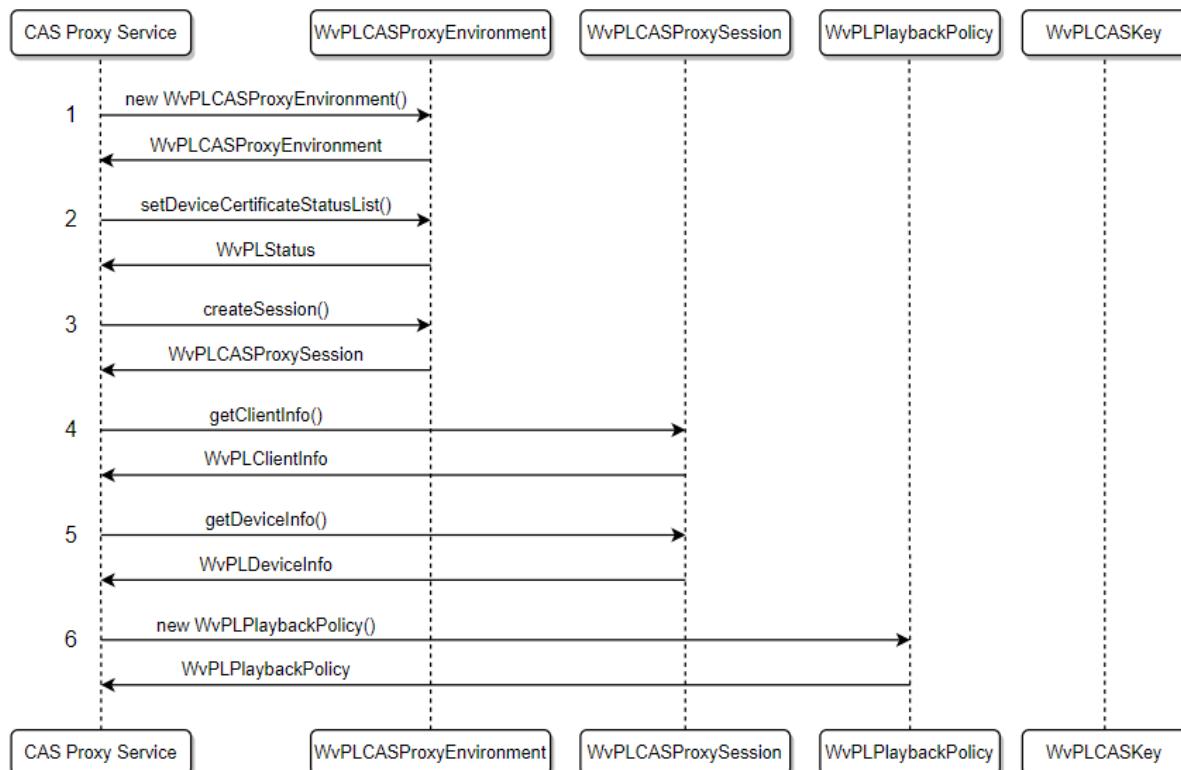
Ovakav *Proxy* će obezbediti funkcionalnost koja će omogućiti operaterima da naprave CAS zahtev za licencu do *Widevine* servisa za licencu.

Opis koraka na osnovu kojih se generiše zahtev za licencu koji se zatim šalje *Widevine* servisu za licencu:

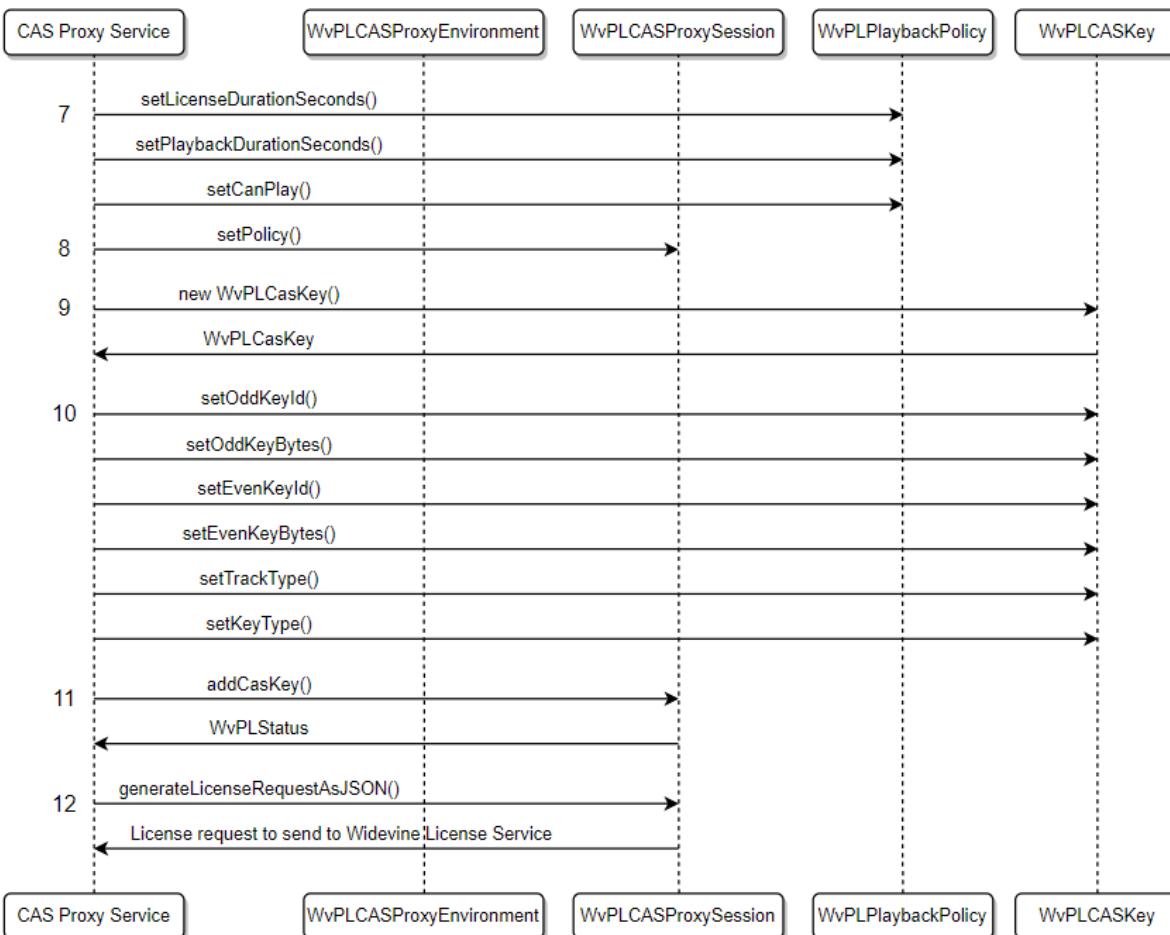
1. Prvo je potrebno izvršiti inicijalizaciju CAS *Proxy* okruženja.
2. Zatim se postavlja statusna lista uređaja koji mogu da dobave CAS licence.
3. Pravi se sesija, pri čemu svaki klijent zahteva posebnu sesiju.

4. Dobavljaju se i proveravaju informacije o klijentu.
5. Dobavljaju se i proveravaju informacije o uređaju.
6. Pravljenje objekta za pravila koji se primenjuje u sesiju.
7. Podešavanje pravila trenutnog klijenta.
8. Primjenjivanje pravila trenutnog klijenta na sesiju.
9. Pravljenje objekta ključa.
10. Podešavanje pravila ključa.
11. Primjenjivanje konstruisanog ključa na sesiju.
12. Generisanje zahteva za licencu koji treba da se pošalje *Widevine* servisu za licencu.
13. Slanje zahteva za licencu preko HTTP protokola POST metodom.
14. Primanje CAS *license* odgovora od *Widevine* servisa za licencu.
15. Primanje *Widevine license response* objekta.
16. Primanje bajtova licence koja će se kasnije proslediti klijentu.
17. Primanje sertifikovanog serijskog broja uređaja.
18. Slanje bajtova licence *Widevine* klijentu.

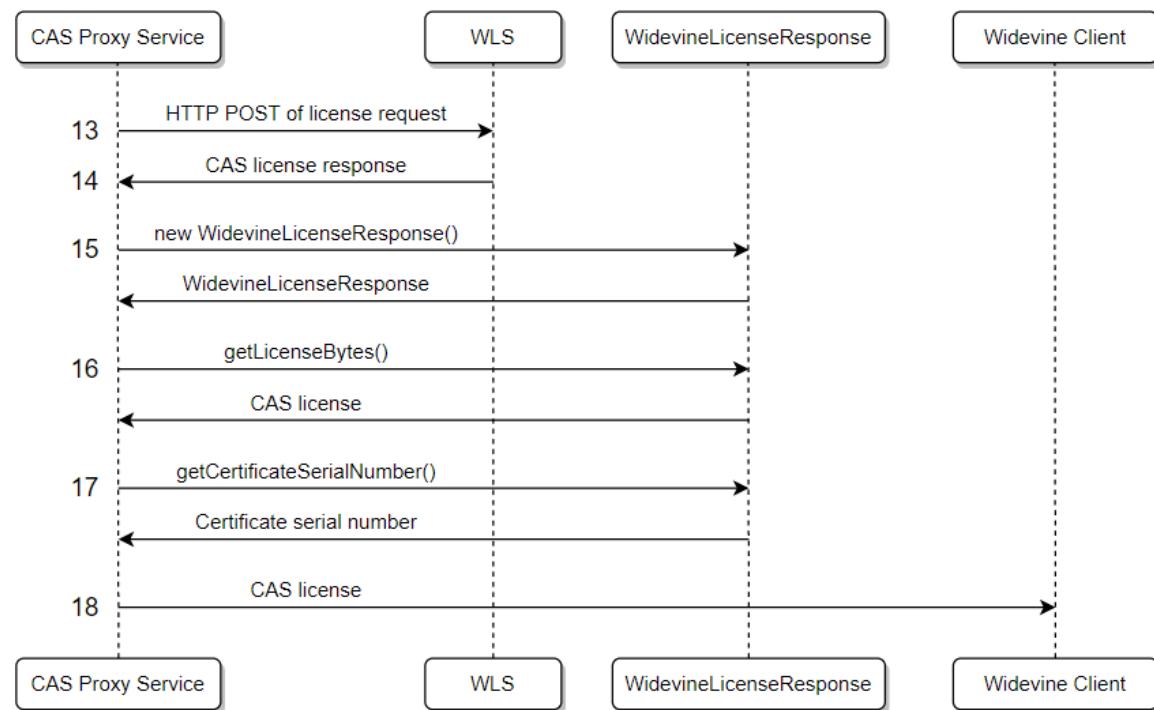
Na slikama 4.1, 4.2 i 4.3 su prikazani opisani koraci sa odgovarajućim funkcijama.



Slika 4.1 Generisanje zahteva za licencu



Slika 4.2 Generisanje zahteva za licencu



Slika 4.3 Slanje zahteva za licencu

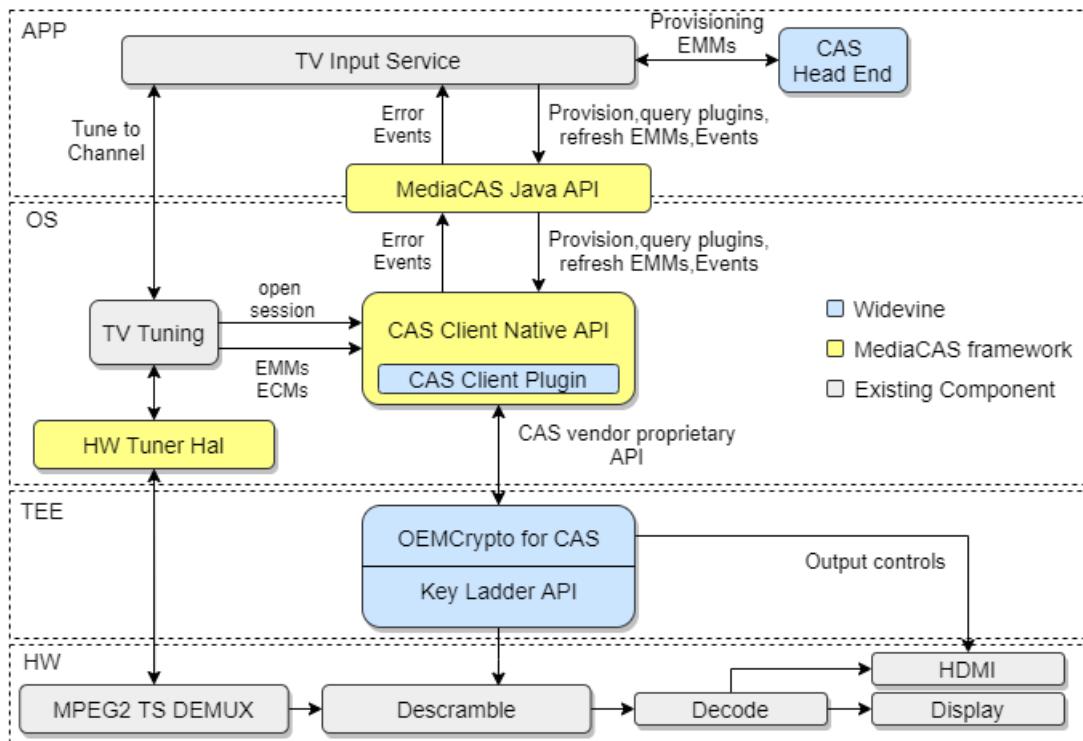
4.3 MediaCAS

MediaCAS API predstavlja interfejs između aplikativnog sloja i sloja operativnog sistema. MediaCAS radni okvir koristi događaje (eng. *events*) da bi implementirao *Widevine* CAS EMM *request* protokol. Događaji prave osnovu za zahtev/odgovor poruke koje se mogu koristiti da se implementiraju specifične notifikacije i API metode.

Naziv događaja, njihov ID i opis:

- INDIVIDUALIZATION_REQUEST (ID 1000) - generiše ga CAS *plugin* kao odgovor na poziv za *provision* ako uređaj već nije izdvojen.
- INDIVIDUALIZATION_RESPONSE (ID 1001) - generiše ga aplikacija i šalje do *plugin-a*. Sadrži odgovor na INDIVIDUALIZATION_REQUEST.
- INDIVIDUALIZATION_COMPLETE (ID 1002) - generiše ga CAS *plugin* da se uspešno izvršio *provision*.
- LICENSE_REQUEST (ID 2000) - generiše ga CAS *plugin* da bi se poslao EMM zahtev ako je uređaj izdvojen. Nakon aktiviranja ovog događaja, on se prosleđuje serveru da bi se dobio *entitlement* za traženi tok.
- LICENSE_RESPONSE (ID 2001) - generiše ga aplikacija i šalje do *plugin-a*. Sadrži odgovor na LICENSE_REQUEST.
- LICENSE_RENEWAL_REQUEST (ID 2003) - generiše ga CAS *plugin* da se zahteva obnavljanje licence.
- LICENSE_RENEWAL_RESPONSE (ID 2004) - generiše ga aplikacija i šalje do *plugin-a*. Sadrži odgovor na LICENSE_RENEWAL_REQUEST.
- LICENSE_CAS_READY (ID 2006) - generiše ga CAS *plugin* da obavesti da je spremna obrada ECM poruka.
- LICENSE_CAS_RENEWAL_READY (ID 2007) - generiše ga CAS *plugin* da obavesti da je obnova licence uspešno primljena.
- CAS_SESSION_ID (ID 3000) - generiše ga CAS *plugin* tokom poziva MediaCas.openSession(), u kojoj se *program id* postavlja na *cas_session_id* što se može koristiti da se napravi više sesija. Povratna vrednost predstavlja token koji se koristi prilikom slanja događaja pojedinačnim sesijama.
- SET_CAS_SOC_ID (ID 3001) - generiše ga demultiplexer da se identificuje kojem MediaCas.Session pripada koji ECM tok. Ovom događaju se moraju pridružiti *program id* i *session id* toka koji treba da bude procesuiran od strane te sesije.
- CAS_ERROR (ID 5000) - generiše ga CAS *plugin* da obavesti o pojavi greške.

Na slici 4.4 je prikazan način funkcionisanja CAS *plugin-a* gde je naznačen i MediaCAS radni okvir.



Slika 4.4 Funkcionisanje CAS *plugin-a*

4.4 TSDuck

Tokom izrade zadatka korišćen je TSDuck koji predstavlja skup programskih alata za manipulaciju MPEG prenosnim tokovima. Neke od funkcionalnosti TSDuck-a su:

- transmodulacija prenosnog toka (DVB, ATSC, ISDB itd.)
- analiziranje prenosnog toka
- promena, brisanje, preimenovanje servisa
- rad sa direktnim prenosnim tokovima
- razmena podataka sa hardverom (DVB, ISDB tjuneri, modulatori itd.)
- izdvajanje karakterističnih podataka kao što je teletekst i slično

Najznačajniji TSDuck alat je *tsp* (eng. *transport stream processor*), radni okvir koji se koristi za obradu prenosnih tokova. Svaki put kad se *tsp* pokrene, postoji: jedan ulazni dodatak koji dobija od različitih izvora prenosni tok, bilo koji broj dodataka za obradu paketa koji mogu izvršiti transformaciju paketa u toku prenosa i jedan izlazni dodatak koji šalje prenosni tok do različitih destinacija.

5. Rezultati

U ovom poglavlju opisani su testni slučajevi koji su potrebni kako bi zadatak bio kompletno odrđen. Zadatak je testiran na platformi *Synaptic BG5CT Android Q Platform* koja je detaljno opisana u poglavlju 3.2.

Alat *tsp* generiše *content* ključeve koji se prosleđuju ECM generatoru koji čeka na odgovarajućem portu. Nakon što ECM generator izvrši enkriptovanje *content* ključeva *entitlement* ključevima dobijenih od *Widevine* servisa za licencu, smešta ključeve u ECM poruku koju prosleđuje TSDuck-u koji zatim skrembluje TS paket. Formirani sadržaj zajedno sa ECM porukom se šalje set-top boksu koji prvo komunicira sa server aplikacijom da bi se proverilo da li uređaj ima prava pristupa.

Slika 5.1 Primer sadržaja ECM poruke

```

KEY VALUE SIZE 001144161a096f90ffdf37f1d4135e81b255 0012040fab6f0142b485e169ea9
987282eb9
040fab6f0142b485e169ea9987282eb9 44161a096f90ffdf37f1d4135e81b255
20:37:39.660931 32 wv_cas_key_fetcher.cc:85]
Json CasEncryptionRequest: {"content_id":"MTIzNDU2Nzg=","provider":"iwedia","track_types":["SD"],"key_rotation":true}
20:37:39.660960 32 wv_cas_key_fetcher.cc:107]
Json SignedCasEncryptionRequest: {"request":"eyJjb250ZW50X2lkIjoiTVRJek5EVTFJ0emc9IiwiCJHJvdmlkZXiiOijpd2V
kaWEiLCJ0cmFja190eXBlcI6WyJTRCjdLCJrZLfc90YXRp24iOn
RydWV9","signature":"/V8eN796KkPPkStu0Tlroug0tS35RxMwqKSZVSzihs=","signer":"iwedia"]
Request: {"request":"eyJjb250ZW50X2lkIjoiTVRJek5EVTFJ0emc9IiwiCJHJvdmlkZXiiOijpd2V
kaWEiLCJ0cmFja190eXBlcI6WyJTRCjdLCJrZLfc90YXRp24iOn
RydWV9","signature":"/V8eN796KkPPkStu0Tlroug0tS35RxMwqKSZVSzihs=","signer":"iwedia"]
Response: {"response":"eyJzdGFnDxMioiJPSyIsImNvbnRlbnRfaQoIjNVEl6TkRVMk56Zz0iL
CJlbnRpdGxlbwVudF9rZxLz1jpbeYrZXLfaWQoIj5aWVsc1llSFhFZVLCyJbh0Fwah3PT0LLCJrZ
Xk10iJCOH2rBxJzQzdSwLdBK09EVStwNTzNUpRnRFwZzZYkUzP0u1mY3V3TjRjPSIsInRyYWRNRX3R5c
GU10iJTRCisImtleV9zbG90IjoiRVZfTj9LHSia2V5X2lkiJoidG01dXBBlhYL2VTY28wZnRuYmZwU
T09iwiLa2V5IjoiNDhJbuZJLzE4RDR150cTwVh6XvhMEY3cHRPTFoc9YMLJFYTVUEmJkUT0LLCJ0c
mFja190eXBlijoiU0QiLCJrZLfc2xvdCI6Ik9ERCJ9XX0="}
20:37:39.844539 32 wv_cas_key_fetcher.cc:124]
Json HTTP response: {"response":"eyJzdGFnDxMioiJPSyIsImNvbnRlbnRfaQoIj5aWVsc1llSFhFZVLCyJbh0Fwah3PT0LLCJrZ
RBNE5EUT0iLCJlbnRpdGxlbwVudF9rZxLz1jpbeYrZXLfaWQoIj5aWVsc1llSFhFZVLCyJbh0Fwah3PT0LLCJrZ
NBPT0iLCJrZxk10iJ0z1JycmdqeU4Nj0ycjY3Vhd0OHJicUSMUGNMRMtKcWRVSUROdm5GZDBNPSIsIn
RyYWRNRX3R5cGU10iJTRCisImtleV9zbG90IjoiU0l0R0xFIn1dfQ="}
20:37:39.844607 32 wv_cas_key_fetcher.cc:130]
Json CasEncryptionResponse: {"status":"OK","content_id":"MjExNDA4NDQ=","entitlement_keys":[{"key_id":"MPaguMoX6E1S8D9AwFCA==","key":"hgRrrgjyH8642r67Twt8ruqN
LPclFkQqdUDNvnFd0M=","track_type":"SD","key_slot":"SINGLE"}]}
Parsed: 1 entitlement keys.

```

Slika 5.2 Informacije ključeva, JSON poruka i odgovora

Nakon toga se na set-top boksu generiše zahtev za licencu koji se zatim prosleđuje *Proxy*-u. Ukoliko je zahtev od set-top boksa validan, *Proxy* izgeneriše JSON zahtev (slika 5.3) na osnovu kojeg se dobija licenca. JSON zahtev sadrži potrebne informacije kao što su poruka, potpis i operater, a na samom kraju se nalazi link sa zadatim operatorom (*iwedia*). Na osnovu toga dobija se licenca sa .lic ekstenzijom.

```

curl -d '[{"request":"eyJwYXlsb2FkIjoiQ0FjU3VRc0toQXNJQVJMd
ENRCXBZ2dRWhDTGleTDDu0d6NwRNhoRXZsdEhPr09UdFPRUzRbRDTULjQknNs0NBuUVBchlubkRr
TLjWd2lcbitiR0w1LNicW55TF2VnpLZVJNYlJwbh3b0lxaEhtbGpxS0h0XpxMm10M0tReLEzejk2bUW
xT2taqjQNYl9F0mxYK2s3q1BsVVY1b1jNPukpTM21v0UNNvMFY0Vxd69dRlBjZGVyc180UTRXTU1p0HNCZ0
Y5UWptpNa20FvJuctPcmd3cxdUvkpfWwNy5rSHNsAgV5M2J0UhlickFsbw01c0VzdFyZUXBZXFkRDbwV
100bEdtcTayN20rb0FFU2U5t1ha5b2J3zanVJ3hDcnrdwcmQ0WE1SdVFLVkJavndrMjhPNWV4cjybw0
SHjL3pCUVZkdmeeFFMnzsCdv0ZgdBazlQnds2Vgmv2pxbUpsRzfCtdxew5rpb0xzPz3dByWtV2RudnJ
PZm0Wnxacs1VGF6eE10VdVYT3pru2pRSRBUUFC50prZ0vQUNNakd2czdRZuMnpDV19jby82TjLKNH
BuU3NaL3AybnEx0G9idklyb0ljbXZRMVREcFGFkzd1TzNzRmWtNzWe4yThcvSDVyuQUsT28xSUFWd1BTUXBx0hdHO
w9utVClk1LFQ2Fx2b1heTZTkvk9sfPMQXQ003hnZG9SVhp1Mfh0dkh1NnZ0MzibG1wQ09dnpmB1J1CzYr
dTREK3h6Noxy1lnldnpddekRbdhmuxThiaHvUxkSKYzUy0cxaWm0Ykc0UFRIaE51U0p0MUtqskRhdEcsYm9
0cGh0d1Fw5UJ6aH0l0VFNSSDhqcits0zdmFxhTixFVib2CfppLeHdqVUV3NUdoz0lQaTfENT
Zqa1RK01Fw1LzYNe42adyvFAwRTvPMU12NEi0b3RROtiwMu5KzZnB2nvBh81cLoyV9z0Hd3cXYNU2nMl
300YkhKWhxMk3RcxDbZ2dCrhBSVRXQzhawk45dHf4L21TdE1SiUfH0tMVGlvvd0zJbzRDTULjQknNs0NB
UUFBbVjzMuW3Y1Uc3JNx2cU505FFnMuN50Uz0wU5wK1FvaWmWbzvXszY4ejhKREs5MRX6U185ZFdtyNb
XQ01sRmVYTNmRwYe19qSwlpobvFDVdGdtQzR5RMWT5zCtD6b2RzbjZmbglbnuFmwdMr3AweHGRHbduM
1TaGFoeVBSh1MnNKQ3pyYllyZw5FMUzRdxZUN3AwcUnuShJla3pQa1c0QzhtZVRzTUU2U1NIR0d0u2NYS
mJOUlZxWtDlqkf6aH0lNyQzXtqM6vN0MuvdjBaBktduE3SFFwdzvRglLSE91K1jpdzE2Vndt
VFRZelte4T3R1VVQ2S3Fy9mQodGh4Quo1zFyj3ZvC5zcrkennp0NxlZadc2wZtRHn2TEJNvo1V1Q4t3R
MRXVHRDNDcVjKzJiRw9uvis3SzFzhM29tovlpVjBESnBRsURBUUC50prZ01BRVNnQu1oTGVGQnduQlh3Wm
h5R04x13ZDM0orRxLDK1i5YKzMerjTNWHzarMsSERKRCERZggQkZj0gJndlRyT1F1L0RxM3Nr25mVGn6T
wsxbkNwcuGZU2b1JwsZfAbxFw1kmvBue5MMU85ZGwWeu91n0F3Q0WdhZHWBm0hPSUR42zLMVbka3JwWfqW
Qn1x0W0xdnRzVtLHu2ltQ3RCQTE5U09uSVBxAep3a2prWeErVnU3ak5DeC91NUVXTvhHQ3jeVxoK3crTzZ
ZZG1yNx01TxdkwGhsZm9BwHeDrn1Q5cUfpaVzHeuZouZ60hd2znw1y3znduCusrTktxtjFKNj1LTVLzd1
VCT01J5lg1uUfxtel4Q4FTTCUpoVeF1L2w1dVFMNTzHTtHeVXBzNzUddDjdgtV2x0vnAz1BkeFhQjFV
0pLW0xbzJcbuZlNnVTSs1tlzNsjNDSjc3QncrrejluagrizdrLiu0cyE10s1Qzb2ftNhdtt05itVpk2zu
bFvLW0e350s0auVnlwLvgvceno5b2xnVxhabdjuVG5BbbZYSVrckhkhMZElRfRQSgF2bzF3YwZp5kwDz
RQ130C9B1updEp3n91SLB4a0NrWtNuV3rdkgwcmxZvMwUj9s0dxhNphQ0UdHqXdrUersZel2R3A1UG
F35WFd29NWT15dGNHnrlVlj1lWvcxbEvntjNkm2NhrFvS2JX0WtaV3hym1GdfpSSURkM2QzR2LBS0RIq
nl1mlIxwTNSzJtRnRaB1rVjjs9NByB1wZewh0Vv0PytjBjeG9t2hGaGntTm9hfJsWtnsmwntVmZi
bUZ0WlJ3JUllYSpHr2wwWld0MGRY5mxYmJy0V0lyYdnh0xa1YyV0dbYghWnh1v1VTQz3SbGrtbgpavjl
1WVcxbe1n5W9EaElNQ2g0s5hCb0s5KmxrWlhacJtvmzkr126ZENJSLEYrNpnsE5HwD0fbdbSvLbuOrRn2
RUaEjUqvZPtK9pKy80Q0dqvQNCWERYZ0pvcGZhUu4v0kweivtMngrZEg2TctPyk1nbnttb1Jbdjdjnust4b
lrbTgx5T15Q2FcZ25seTfMMFnTc3JRRXB0SmplN2hCnRaRGuRvVE3NnZj3CFMzuhuTk9CWHVheGw3c1ky
R3Zyen40ehUl04wSe0ZnQv0SaFcxTcsrenZgdzBsmwn0akc40HnhVbtrLdrZ29XrvowTkdUZ2Mxhhlz0s
2Mnr1V3o1Q2ZJRvh2af43wm1NeW9hz1BTT1daWjFnbhRlaXYxQUvQZUZDNk15K25qcTh0M3U5d2hva016aG
xHTWQ00JjdEzTbjrM0FJ0wVWSN3psTGRQdutjcdbcQkxBt0Y3bmdYrfDk3NraItzMuRydhh3cxdjeKE1N
nlMehhbGg1Rmh3aGFGTvnwck9IyKfg0lRk2vLnjzhRelivlor0s9Qk1psu4m1E9PS1sInByb3ZpZGvY
X2lkIjoid2lkZxZpbmVfdGVzdcIsImNvbnRlbnRfaQoIjRmkz6vkh0R1lx0Gw1LCJvdmVycmlkZv9wcm92aWrlc19jbGllbnRfdG9rzW
4iomzhbHNlfX0=","signer":"iwedia","provider":"iwedia"]' https://license.uat.widevin
e.com/cas/getlicense/iwedia

```

Slika 5.3 Izgenerisan zahtev

Testni slučajevi sa redosledom izvršenih koraka kako bi se postigao odgovarajući rezultat su prikazani u tabeli ispod (tabela 5.1).

TEST	REZULTAT
Uspostavljanje komunikacije između ECM generatora i TSDuck-a	PROŠAO
Slanje zahteva za ključeve <i>Widevine</i> servisu za licencu	PROŠAO
Primanje ključeva od <i>Widevine</i> servisa za licencu	PROŠAO
Smeštanje ključeva u ECM poruku	PROŠAO
Slanje skremblovanog sadržaja	PROŠAO
Uspostavljanje komunikacije sa server aplikacijom	PROŠAO
Dobijanje odgovarajućeg odgovora od server aplikacije	PROŠAO
Uspostavljanje komunikacije između set-top boksa i <i>Proxy</i> -a	PROŠAO
Generisanje zahteva za licencu pomoću <i>Proxy</i> -a	PROŠAO
Slanje zahteva do <i>Widevine</i> servisa za licencu	PROŠAO
Dobijanje licence	PROŠAO

Tabela 5.1 Testni slučajevi

6. Zaključak

U ovom radu je opisano proširenje za CAS sistem sa ciljem da se dobavi licenca odnosno EMM poruka pomoću identifikatora *entitlement* ključa kako bi set-top boks deskremblovao sadržaj. Na predajnoj strani, pomoću *entitlement* ključeva dobijenih od *Widevine* servisa za licencu, enkriptuju se *content* ključevi koji se smeštaju u ECM poruku. U ECM poruku se smešta i identifikator *entitlement* ključa koji se takođe dobija u odgovoru od *Widevine* servisa za licencu. Zatim se ECM poruka prosleđuje skrembleru koji vrši skremblovanje čitavog prenosnog toka *content* ključevima koji su na početku generisani i takav skremblovan sadržaj se šalje kroz mrežu zajedno sa ECM porukom. Na prijemnoj strani, šalje se zahtev za licencu *Widevine* servisu za licencu i identifikator *entitlement* ključa. Na osnovu identifikatora, *Widevine* servis za licencu odgovara EMM porukom koju CAS *Proxy* prosleđuje do set-top boksa. Nakon primanja EMM poruke, set-top boks pomoću *entitlement* ključeva iz EMM poruke dekriptuje *content* ključeve iz ECM poruke. Na osnovu toga je u stanju da deskrembluje sadržaj.

Prednosti CAS sistema su svakako u tome što su veoma pogodni, jer sprečavaju korisnike koji nisu pretplaćeni da pristupe podacima. Sigurni čipset u okviru set-top boksa predstavlja pogodno i isplativo rešenje, jer je omogućio da proces pretplate funkcioniše zasebno od ostatka preduzeća i hardvera. CAS sistem omogućava korisnicima da prilagode svoje kanale i plaćaju samo ono što ih zanima.

Nedostaci CAS sistema su što vrše zaštitu sadržaja samo tokom transporta i za razliku od DRM tehnologije, koriste jednosmerne (eng. *one-way*) mreže odnosno nema nikakve povratne informacije od strane prijemnog uređaja. U tu svrhu korišćene su pametne kartice koje su se ispostavile kao nepouzdano i skupo rešenje, jer su bile podložne kloniranju, te su morale biti menjane na svakih nekoliko godina o trošku operatera. Ovaj problem je rešen

pojavom modernijih SoC komponenti koje pružaju mogućnost za sigurno rešenje unutar set-top boksa. CAS sistem je ograničen na uređaje za emitovanje i odnosi se samo na video/audio sadržaj što je u današnje vreme, s obzirom na napredak televizije, potencijalni problem.

Prema izveštaju *Nielsen's Total Audience Report* iz novembra 2020. godine [16], televizija i dalje predstavlja najupotrebljiviji medij uz koga u proseku ljudi provedu od 4 do 7 sati dnevno. Samim tim zbog velike upotrebe, digitalni sadržaj postaje sve češće meta napada. U tu svrhu, CAS sistem mora posedovati što bezbedniji sistem kako bi se izborio od neželjenih pojava i zadržao status pouzdanog sistema za zaštitu sadržaja. Dokle god postoji prenos videa i hardverska rešenja koja to podržavaju, CAS sistem za zaštitu sadržaja će opstati još dugo vremena.

7. Literatura

- [1] dr Milan Z. Bjelica, dr Nikola Teslić, mr Velibor Mihić, Softver u digitalnoj televiziji 1, Univerzitet u Novom Sadu, Fakultet Tehničkih Nauka, 2017.
- [2] *Descramble*, dostupno na: <https://en.wikipedia.org/wiki/Scrambler/> , pristupano februar 2021.
- [3] *What is encryption*, dostupno na: <https://www.cloudflare.com/learning/ssl/what-is-encryption/> , pristupano februar 2021.
- [4] *Decryption*, dostupno na: <https://www.techopedia.com/definition/1773/decryption> , pristupano februar 2021.
- [5] ECM EMM, dostupno na: https://www.itu.int/dms_pubrec/itu-r/rec/bt/R-REC-BT.1852-1-201701-I!!PDF-E.pdf , pristupano februar 2021.
- [6] *Conditional access (CA)*, dostupno na:
https://tech.ebu.ch/docs/techreview/trev_266-ca.pdf , pristupano februar 2021.
- [7] *Simulcrypt Multicrypt*, dostupno na: <https://www.headendinfo.com/simulcrypt-multicrypt/> , pristupano februar 2021.
- [8] *Widevine*, dostupno na: <https://www.widevine.com/> , pristupano februar 2021.
- [9] *Widevine*, dostupno na: <https://en.wikipedia.org/wiki/Widevine> , pristupano februar 2021.
- [10] *Widevine CAS*, dostupno na: <https://castlabs.com/news/widevine-cas-to-disrupt-broadcast-industry/> , pristupano februar 2021.
- [11] *Widevine CAS*, dostupno na: <https://www.widevine.com/solutions/widevine-cas> , pristupano februar 2021.
- [12] *Simplified security on Android TV*, dostupno na:
<https://castlabs.com/drmtoday/widevine-cas/> , pristupano februar 2021.

- [13] *Widevine DRM*, dostupno na: <https://www.widevine.com/solutions/widevine-drm> , pristupano februar 2021.
- [14] *Hypertext Transfer Protocol*, dostupno na:
https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol , pristupano februar 2021.
- [15] JSON, dostupno na: <https://developer.mozilla.org/en-US/docs/Learn/JavaScript/Objects/JSON> , pristupano februar 2021.
- [16] *The Generation Gap in TV Consumption*, dostupno na:
<https://www.statista.com/chart/15224/daily-tv-consumption-by-us-adults/> , pristupano februar 2021.