Техничко решење

БЕЗБЕДНО СТАРТОВАЊЕ ЦЕНТРАЛНОГ ПРОЦЕСОРСКОГ МОДУЛА ЗА ТЕЛЕЗАШТИТНИ ТЕРМИНАЛ

Аутори:
Миленко Кабовић, Јована Новаковић, Анка Кабовић, Владимир Челебић, Ива Салом, Владислав Миленковић

Година: 2022.

Корисник:
Електромрежа Србије – ЕМС АД

Начин коришћења:
У телезаштитном терминалу TZ-600

Рецензенти:

ТЕХНИЧКО РЕШЕЊЕ

Назив	**БЕЗБЕДНО СТАРТОВАЊЕ ЦЕНТРАЛНОГ ПРОЦЕСОРСКОГ МОДУЛА ЗА ТЕЛЕЗАШТИТНИ ТЕРМИНАЛ**
Аутори	Миленко Кабовић, Јована Новаковић, Анка Кабовић, Владимир Челебић, Ива Салом, Владислав Миленковић Институт „Михајло Пупин“ Београд
Категорија	Битно побољшано техничко решење Доказ: Рачун
Кључне речи	Телезаштита, Етернет, IEC 61850

За кога је решење рађено (правно лице или грана привреде):
Техничко решење је рађено за потребе, ЕМС АД Београд
Година када је решење комплетирано:
2022.
Година када је почело да се примењује и од кога:
Примена техничког решења је почела у 2022. години, Корисник: ЕМС АД Београд
Област и научна дисциплина на коју се техничко решење односи:
Техничко-технолошке науке; електроника, информационо-комуникационе технологије
Рецензенти техничког решења:

Технички елаборат:

- Проблем који се техничким решењем решава
- Стање решености тог проблема у свету
- Опис техничког решења са карактеристикама, укључујући пратеће илустрације и техничке цртеже
- Референце
- Рецензије техничког решења

БЕЗБЕДНО СТАРТОВАЊЕ ЦЕНТРАЛНОГ ПРОЦЕСОРСКОГ МОДУЛА ЗА ТЕЛЕЗАШТИТНИ ТЕРМИНАЛ

ТЕХНИЧКИ ЕЛАБОРАТ

Проблем који се техничким решењем решава:

Електроенергетска индустрија је једна од најкритичнијих инфраструктурних индустрија која високо утиче на живот људи и њихову економску активност. Телезаштитни уређаји су део критичне инфраструктуре у електропривредним системима. У периоду од 2008. до 2022. године у Републици Србији (ЕМС АД), као и земљама из региона (Северна Македонија, Босна и Херцеговина и Црна Гора) Институт „Михајло Пупин“ је произвео и пустио у рад преко 100 телезаштитних уређаја типа TZ-600 намењених за пренос сигнала релејне заштите (по стандарду IEC 60834-1 [1]) са једне стране штићеног далековода (напонске равни 400 kV, 220 kV и 110 kV) на другу, и то: сигнала за рад дистантне и усмерене земљоспојне заштите, заштите сабрница, отказа прекидача и слично. С обзиром на све већу разноврсност телекомуникационих система који се примењују у електропривреди, од савремених телезаштитних уређаја захтева се адаптивност и флексибилност, тако да могу да обезбеде брз и сигуран пренос телезаштитних команди преко различитих медија преноса и комуникационих технологија. Како би се пратили савремени трендови у електропривредним системима, а пре свега могућност примене у дигиталним трафо станицама, неопходно је било извршити значајно унапређење терминала TZ-600. Да би се то постигло, покренута је реализација нове централне јединице (CPU) која мора да буде компатибилна са постојећом архитектуром уређаја TZ-600, а такође и да омогући нове функционалности и да буде основа новог, унапређеног уређаја.

Централна јединица представља процесорски део уређаја TZ-600, тако да је било веома важно посветити пажњу аспектима сајбер безбедоности (заштити) при изради ове јединице. Због сталног рада у реалном времену и строгих захтева за поузданост, безбедност код телезаштитних уређаја се остварује по следећем приоритету: (1) расположивост података, (2) интегритет и (3) поверљивост. Стога је приликом пројектовања овог система изабран процесорски систем Zynq 7000 SoC који пружа подршку за примену различитих безбедносних механизама, на различитим нивоима: криптографске функције, односно модули који их извршавају (AES/HMAC и RSA алгоритми), подршка за безбедно стартовање система, заштита извршавања софтвера.

Модерни телезаштитни терминали треба да омогуће обављање више различитих комуникационих задатака у реалном времену, и због тога морају да садрже јаке процесорске системе који имају могућност промене основног софтвера. Дужи животни век оваквих

система може се омогућити ажурирањем верзије софтвера (фирмвера) које се мора обавити преко безбедних канала, при том не мењајући позицију уређаја који се налази на терену. Због тога се као један од најзначајнијих безбедносних механизама намеће процес безбедног стартовања (Secure Boot) који треба да осигура претпоставку да основна конфигурација система представља легитимну верзију произвођача, и да их ниједан злонамерни актер или процес није мењао. Применом процеса безбедног стартовања, који се извршава приликом сваког новог покретања процесорског система телезаштитног терминала, омогућава се идентификација неовлашћених извршних датотека, спречава њихово покретање, и извршавају се корективне радње. Процес безбедног стартовања састоји се од неколико корака којима се обезбеђује интегритет и аутентичност инсталације како би уређај радио исправно и безбедно, и због тога представља основу за све касније примењене безбедносне механизме (*Root of Trust* концепт).

Стање решености тог проблема у свету:

Телезаштитни уређаји пројектовани су за пренос команди заштите преко различитих врста комуникационих медија у електроенергетским (ЕЕ) мрежама. За заштитне шеме су, због своје важности, коришћени наменски комуникациони путеви, па су се основни акценти код пројектовања уређаја за пренос сигнала релејне заштите заснивали на примени стандарда IEC 60834-1 (висока поузданост, сигурност и расположивост, време преноса испод 10 ms). Потенцијалне добити увођењем Етернет комуникационе технологије, као и потреба за обезбеђивањем интероперабилности (могућност да уређаји различитих произвођача међусобно комуницирају) уређаја довели су до развоја стандарда IEC 61850 [2]. Иако је у почетку замишљен као стандард за аутоматизацију унутар једне трафостанице, стандард је еволуирао на цео електропривредни домен, што је довело до потребе за развојем и увођењем механизама заштите од сајбер напада. Због тога је развијен посебан стандард, IEC 62351 [3] који се, између осталог, бави проблемом сајбер безбедности IEC 61850 порука, а дефинише поруке, процедуре и алгоритме за безбедну комуникацију од једног до другог краја (E2E, End-to-End) везе.

Постоји више познатих произвођача телекомуникационе опреме за пренос сигнала телезаштите, као што су ABB (NSD 700), RFI (*Guard* 8000), *Siemens* (SWT 3000), DIMAT (TPU-1), *General Electric* (*Gridcom* DIP), *Valiant* (VCL TP) итд. Сви уређаји су модуларног типа, што омогућава флексибилност уређаја у зависности од потреба корисника. Правци развоја у електропривредама у свету показују последњих година интезивну примену Етернет технологије, посебно у контексту примене стандарда IEC 61850. У складу са тим, од уређаја се захтева да поседују свеобухватан сет мера заштите од сајбер напада, а као део тих мера је и безбедно стартовање централног процесорског модула, које обезбеђује да се без мењања позиције уређаја на терену конфигурација уређаја обави преко безбедних канала. С друге стране, са порастом развоја и продаје прилагођених IP модула, различита тржишта све већу пажњу посвећују имплементирању уређаја који пружају могућност заштите софтвера и хардверских IP модула са становишта безбедности, а самим тим,

примена оваквих уређаја, односно чипова, доста олакшава процес заштите једног сложеног система, какав је процесорски модул телезаштитног терминала.

Опис техничког решења:

Процесорски модул за телезаштитни терминал TZ-600 је заснован на Xilinx Zynq 7000 SoC (System on Chip) компоненти, која се састоји од програмабилне логике FPGA (PL) и процесорског система (PS) са дуалним ARM Cortex-A9 микропроцесором [4]. Ради што веће безбедности, што бољих перформанси и искористивости ресурса, пројектовање система укључује примену безбедносних мера на сваки од његових делова, што у случају коришћеног чипа подразумева обезбеђивање како PS подсистема, тако и PL дела система.

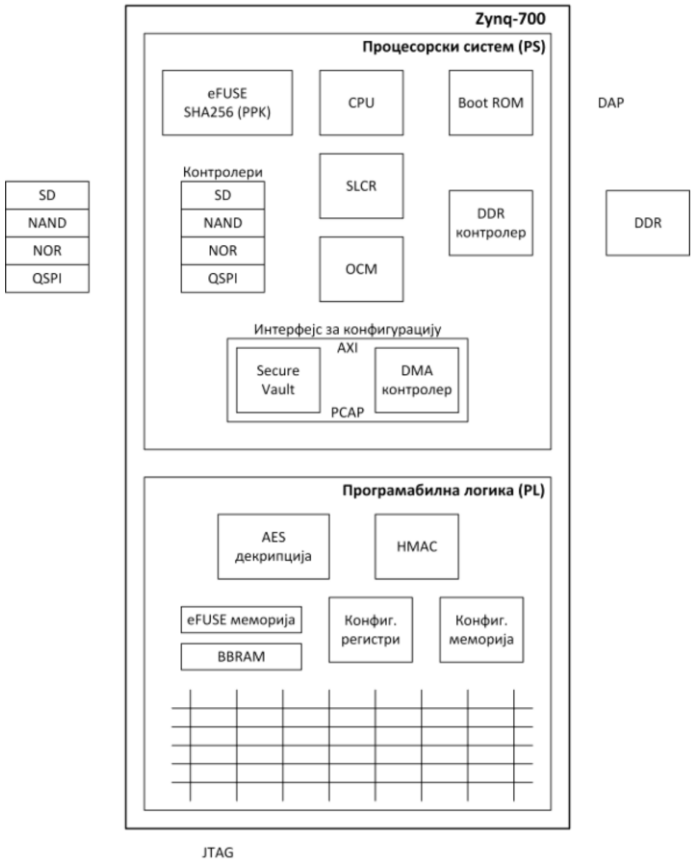
Zynq 7000 је интегрисано коло последње генерације који пружа могућност коришћења различитих безбедносних механизама и обезбеђује различите нивое заштите:

- BootROM код
- 256 kB OCM за смештање FSBL-а и осетљивог SW
- Secure Boot и уграђени HW блокови, модули који обезбеђују крипто функције (AES/HMAC, RSA)
- ARM TrustZone технологија - партиционисање система на различите безбедносне зоне
- Асиметрични мултипроцесорски систем (AMP)
- Подршка за подизање Linux-а (PetaLinux)
- Anti-tamper технологија (брисање свих података уколико систем детектује покушај напада)

На једном језгру Cortex-A9 Zynq-7000 SoC-а се реализују временски мање критични сервиси у оквиру Linux оперативног система (нпр. конфигурација и надгледање уређаја, рад са базама података). На другом језгру Cortex-A9 Zynq-а се реализују временски критични сервиси, који се извршавају у реалном времену под Free RTOS оперативним системом (нпр. рад са GOOSE порукама, реализација преноса команди преко Етернет интерфејса, рад са графичким дисплејом, реализација сервисног говорног канала). На компоненти постоји и мала (256 KB) RAM меморија, OCM (On Chip Memory) за смештање FSBL (First Stage Bootloader) кода на почетку подизања система, или касније за складиштење осетљивих информација или кода, док се преко меморијских контролера приступа већој спољашњој DDR RAM меморији.

Овај систем се у принципу стартује, када је реч о теренским условима, помоћу меморије са постојаним садржајем (Non-Volatile Memory - NVM), као што је нпр. SD картица. Хардверске компоненте које учествују у стартовању система су: централна процесорска

јединица (CPU0), системски контролни регистри (System Level Control Register - SLCR), интерфејс за конфигурацију уређаја, меморија са постојаним садржајем (NVM), JTAG, AES/HMAC (Advanced Encryption Standard/Hashed Message Authentication Code), OCM меморија (On-Chip Memory), DDR меморија, BootROM меморија (слика 1).



Слика 1 – Хардверске компоненте Zynq 7000 које се користе за стартовање система [5]

Хардверске компоненте које учествују у стартовању процесорског система Zynq 7000

CPU0 контролише стартовање система писањем/читањем регистра конфигурације уређаја (Device Configuration – DEVCFG) и других системских контролних регистара (SLCR). Интерфејс за конфигурацију уређаја садржи контролер за директан приступ меморији (DMAC), који се користи за пребацивање кода у току стартовања система из NVM меморије у DDR меморију. Безбедно складиште је део меморије у оквиру процесорског система који је недоступан. Пројектант система контролише приступ његовим деловима, тако да су уобичајено безбедни делови: OCM меморија, L1 и L2 кеш меморија, меморија за конфигурисање PL (програмабилне логике), BBRAM и eFUSE. NVM меморија која се користи за стартовање система може бити SD картица, меморија са серијским интерфејсом – QSPI, NAND или NOR флеш меморија. BootROM меморија је капацитета 128 kB и садржи софтверски код (BootROM code) који није видљив од стране корисника, и не може се мењати. Улога овог кода је да прочита регистар у коме се чува податак о начину стартовања

система, те да на основу тога изврши пребацивање првог дела софтвера за стартовање система FSBL-а из NVM меморије у OCM меморију. Регистар у коме се чува податак о начину стартовања система се зове BOOT_MODE регистар, а његов садржај зависи од стања на Boot Mode пиновима процесора који се читају при ресетовању процесора код укључења напајања (Power on Reset). Начини стартовања система могу бити: JTAG, PS мастер небезбедни и PS мастер безбедни. PS мастер модови могу да користе различите типове флеш меморија (NOR, NAND, QSPI) или SD картицу. У табели I приказана је зависност врсте уређаја за стартовање система од стања на поменутим Boot Mode пиновима [6].

Табела I - Зависност врсте уређаја за стартовање од стања на Boot Mode пиновима

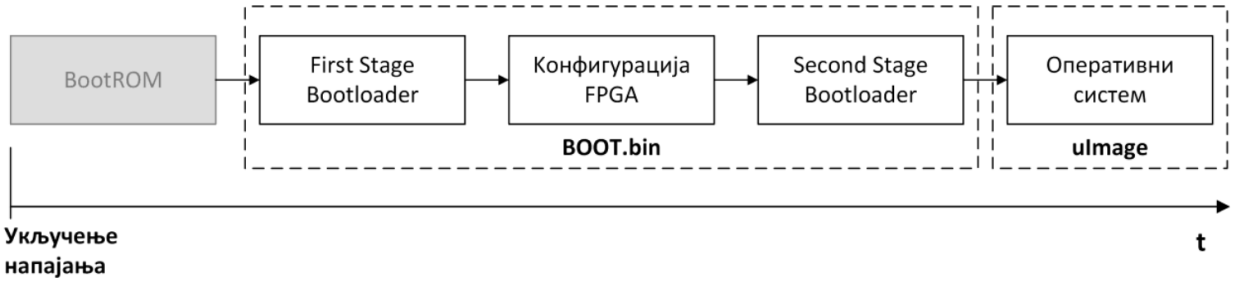
Boot Mode пинови процесора / Boot уређај	MIO[5]	MIO[4]	MIO[3]	MIO[2]
Каскадни JTAG	0	0	0	0
Независни JTAG	0	0	0	1
NOR флеш меморија	0	0	1	x
NAND флеш меморија	0	1	0	x
QSPI флеш меморија	1	0	0	x
SD картица	1	1	0	x

OCM меморија је типа RAM, и капацитета 256 KB. Она није повезана са спољашњим пиновима Zynq 7000 процесора, тако да представља безбедну меморију. Код стартовања система служи за чување FSBL-а (део кода за стартовање система у првој фази стартовања). Може се користити и за чување осетљивог софтвера након стартовања. У случају безбедног стартовања процесорског система за криптовање/декриптовање се користи напредни стандард – AES, док се за аутентификацију користи HMAC. За чување AES кључа се користи или eFUSE меморија у PL-у или BBRAM (Battery Backed RAM) меморија. Прва поменута меморија се само једном програмира, а друга захтева батерију да би се кључ трајно чувао. Алат за развој софтвера – SDK користи Bootgen апликацију за криптовање софтвера у току његовог развоја. Декриптовање се обавља у процесору уређаја код стартовања система, тј. користи се поменути AES кључ записан у eFUSE меморији или BBRAM-у.

Софтверске компоненте које су укључене у стартовање процесорског система Zynq 7000

Стартовање система после укључења напајања се састоји из пет фаза (слика 2), за чије извршавање су задужени следећи делови софтвера:

- BootROM (код коме се не може приступити)
- FSBL (First Stage Bootloader)
- FPGA конфигурација (bitstream)
- Second Stage Bootloader (нпр. U-Boot)
- Оперативни систем



Слика 2 – Преглед процеса стартовања система Zynq 7000 [2]

Са слике 2 се види да је софтвер за другу, трећу и четврту фазу спакован у један фајл (BOOT.bin) као посебне партиције. Свакој партицији у оквиру поменутог фајла се посебно одређује аутентичност.

Заглавље за стартовање система (Boot Header) дефинише карактеристике FSBL-a (First Stage Bootloader). Поља за ID слику и контролну суму (Checksum) омогућавају BootROM коду да покрене проверу интегритета и аутентичности инсталације. BootROM код је први софтвер који се покреће одмах по успостављању напајања на процесорском систему. Главни задаци овог кода су конфигурација система, копирање слике FSBL корисничког кода са SD картице на OCM меморију на чипу (On-Chip Memory) и пребацивање извршавања кода на OCM [3]. OCM је брза и сигурна меморија пошто нема адресне линије и линије података на пиновима Zynq 7000 компоненте. FSBL код надаље врши конфигурацију FPGA дела процесорског система (фаза 3), и затим у наредној фази учитава SSBL (Second Stage Boot Loader) код у DDR меморију. У завршној фази 5 SSBL код учитава слику оперативног система или код апликације у DDR меморију и препушта контролу рада оперативном систему (блок 5 на слици 2).

FSBL је код који обезбеђује Xilinx, а који се може по потреби модификовати од стране корисника за обављање додатних функција. Он врши иницијализацију периферијских (Ethernet, USB, I2C, SPI, CAN, GPIO) и меморијских контролера (DDR), као и блокова за генерисање тактова који нису иницијализовани помоћу BootROM кода. Као што је већ речено, FSBL код се учитава из NV меморије у OCM меморију, међутим ако је у заглављу фајла за стартовање система (BOOT.bin фајл, слика 2), омогућена опција извршавања из места (XIP – execute in place), код се извршава директно из QSPI или NOR флеш меморије. Ова опција није подржана за NAND флеш меморију и SD картицу. У Табели II приказани су делови заглавља BOOT.bin фајла [6].

Табела II – Делови заглавља BOOT.bin фајла

Ознака поља у заглављу	Позиција – офсет поља	Садржај поља
Детекција типа QSPI меморије	0x020	0xAA995566 = Single QSPI 0xACCA50AF = Dual QSPI
Идентификација фајла	0x024	0x584C4E58(‘XLNX’) означава исправно заглавље
Статус шифровања	0x028	0xA5C3C5A3 = eFUSE 0x3A5C3C5A = BBRAM 0x00000000 = без шифровања
Дужина FSBL кода који се копира у OCM меморију	0x034	Дужина FSBL кода за копирање, 0x0 = омогућено је извршавање из меморије без копирања – XIP опција
Иницијализација процесорских контролних регистара	0x0A0 – 0x89C	Користи се 2048 бајтова за иницијализацију 256 процесорских регистара пре копирања FSBL кода

Карактеристични напади за део кода за стартовање који врши конфигурацију програмабилне логике

Zynq 7000 представља SoC компоненту, чија архитектура је карактеристична за модерне системе као што је процесорска јединица телезаштитног терминала TZ-600. Интегритет једног оваквог сложеног система подразумева интегритет његових различитих делова, као што су FSBL, SSBL, кернел, корисничке апликације, мрежни сервиси итд. Са функционалног аспекта оваквог система најкритичнији су напади на део софтвера за конфигурацију FPGA (bitstream), и могу се подвести под неколико основних:

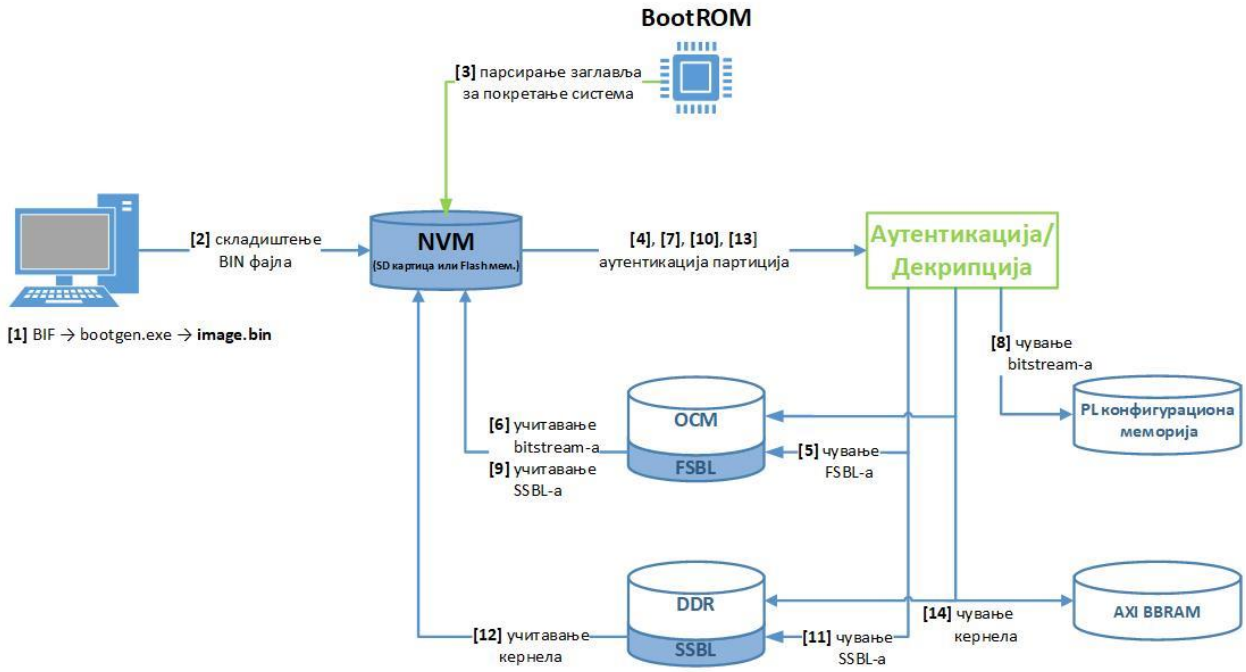
- Лажирање података за конфигурацију FPGA тако да они изгледају као ауторизовани, да би се са неауторизованим подацима извршило конфигурисање FPGA. Нападач се понаша као „човек између“ провајдера података за конфигурацију и FPGA дела процесора. Након извршене промене аутентичности, нападач мења оригиналне податке за конфигурисање лажним, и тиме нарушава интегритет система.
- Злонамерна модификација података за конфигурацију FPGA у току рада уређаја. Ова ситуација се дешава када FPGA након конфигурације има интерфејсе према спољашњем свету који се могу користити за злонамерни приступ.
- Ажурирање конфигурације FPGA се често ради даљински преко мреже, *OTA* ажурирање (Over-The-Air update). Уколико је комуникациона мрежа несигурна, нападач може да лажира свој идентитет и тако убаци неисправне податке како би изменио конфигурацију програмабилне логике и тиме малициозно утицао на основну функционалност система [7].

Пошто све модерне FPGA компоненте садрже у себи криптографске системе, у новије време се све чешће примењују напади коришћењем анализе бочних канала (Side-Channel Attack – SCA) [8]. Ови напади се заснивају на информацијама о физичким процесима који се дешавају у току имплементације криптовања и декриптовања. Параметри који се користе код ове врсте напада су: време извршавања појединих операција, потрошња, електромагнетско зрачење или емитовање звука. Дакле, генерално говорећи, свака физички опсервабилна појава која може бити повезана са конфигурацијом и активношћу криптографског система, може бити извор информација за злонамерног нападача.

Безбедно стартовање Xilinx Zynq 7000 компоненте

Процесорски систем Zynq 7000, као што је већ речено, поред небезбедног старта омогућава и безбедно стартовање. Безбедно стартовање система које се нуди од произвођача компоненте Zynq 7000 се обавља у неколико корака, и повећава безбедност стартовања уз минималне трошкове. Главни циљ безбедности код Zynq 7000 компоненте лежи у основама поверења (“Root of Trust” концепт) заснованих на поверљивости, интегритету и аутентичности почев од момента укључивања напајања до тренутка преузимања контроле од стране корисника. Самим тим подразумева заштиту основног софтвера на ком се заснива систем, односно софтвера који учествује у креирању слике, од неовлашћеног приступа. Ово се на Zynq платформи може постићи потписивањем сваке од партиција које учествују у креирању слике са приватним кључем асиметричнг пара кључева.

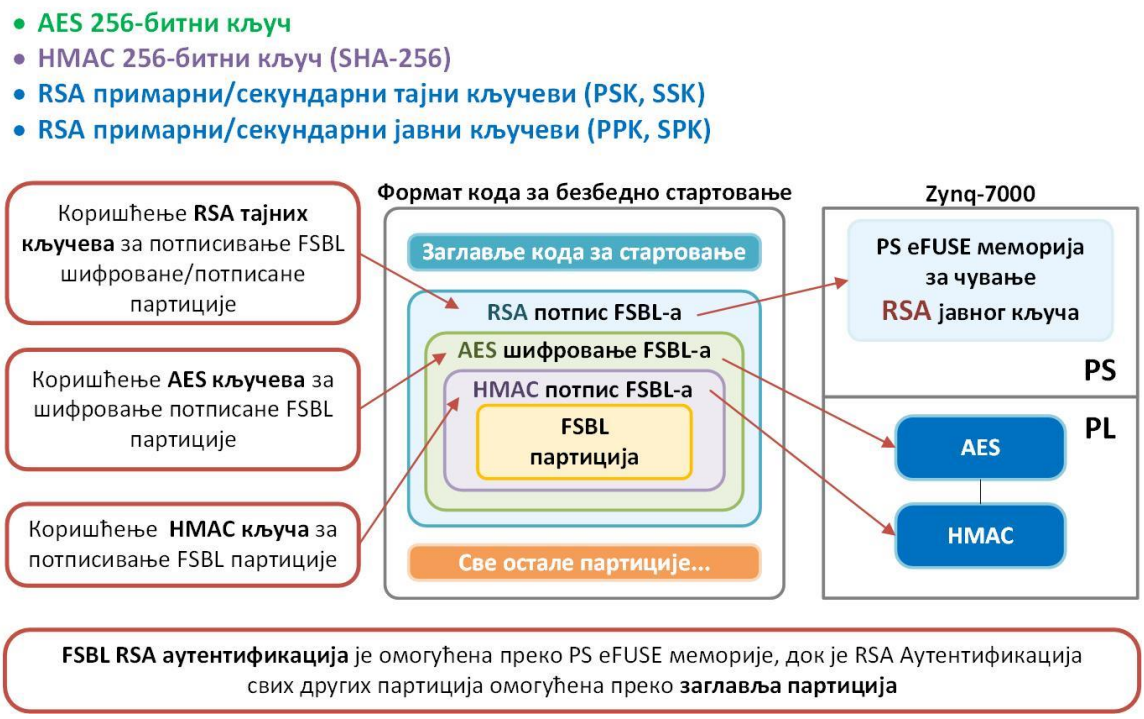
Безбедно стартовање уређаја почиње када BootROM код учита FSBL, и затим се наставља серијски са учитавањем података за конфигурацију FPGA (bitstream) и SSBL софтвера, стварајући ланац поверења са сукцесивном провером аутентичности целокупног софтвера учитаног у уређају [5] (слика 3). Одржавање ланца поверења постаје од виталног значаја у моменту када се уређај нађе на терену.



Слика 3 – Приказ фаза безбедног стартовања и системских меморија које учествују у том процесу

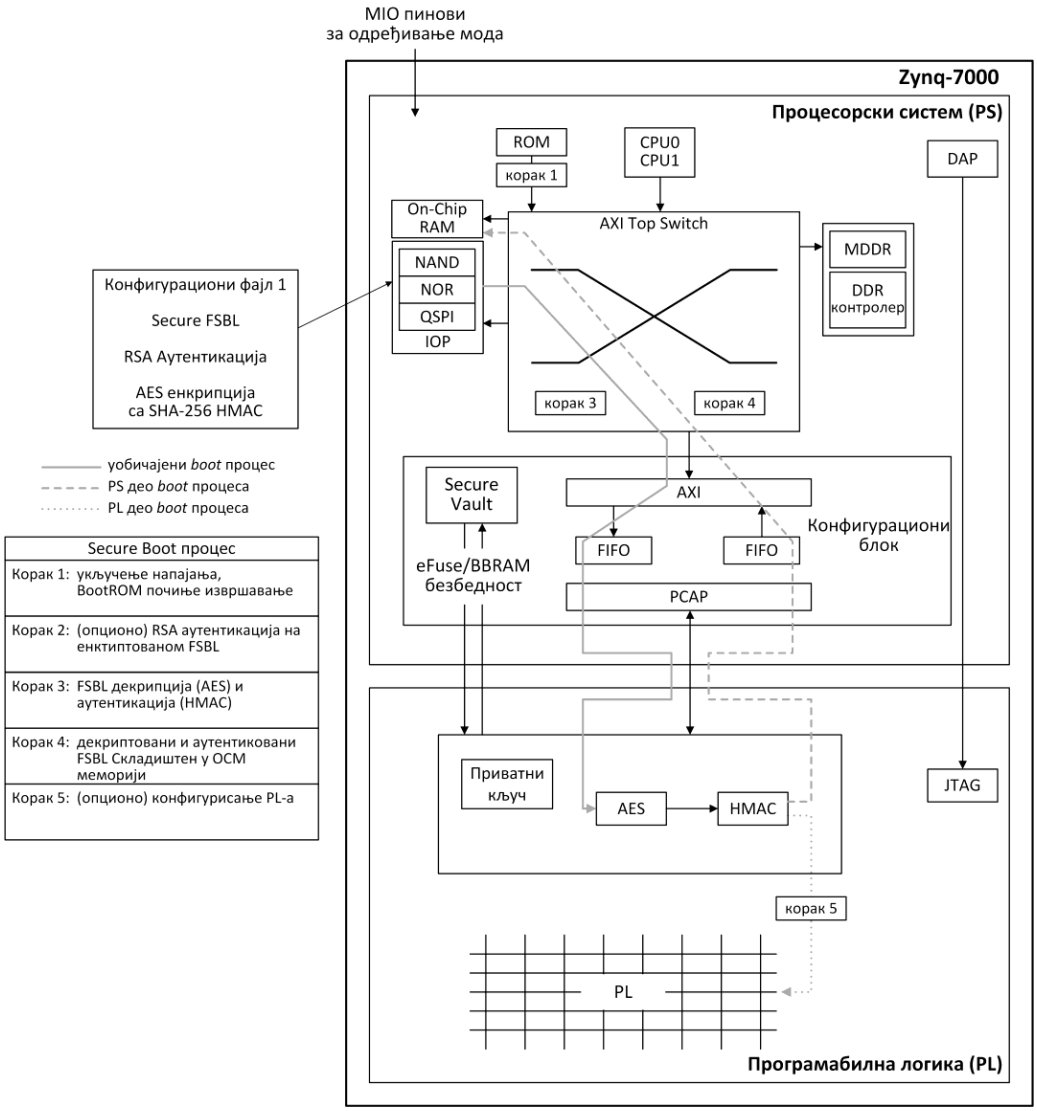
Селектовање система безбедног стартовања постиже се конфигурацијом Boot mode пинова, као и избором мода за шифровање у заглављу кода за стартовање система. Од безбедносних функција у Zynq 7000 компоненти обезбеђено је шифровање засновано на AES стандарду (Advanced Encryption Standard) са 256 бита. AES шифровање се користи за одржавање поверљивости података, али не омогућава чување интегритета података. За чување интегритета података користи се HMAC (Hash-based Message Authentication Code) алгоритам, који користи функцију сажимања (Hash) у оквиру MAC кода.

Додатно се може користити за обезбеђивање аутентичности извора RSA (Rivest-Shamir-Adleman) криптографска функција заснована на асиметричној техници шифровања. RSA приватни кључ се користи за прорачун дигиталног потписа, док се јавни кључ користи за верификацију дигиталног потписа. Основна снага RSA алгоритма се заснива на чињеници да је тешко факторизовати велику целобројну вредност. Јавни кључ се састоји од два броја где један број представља производ два велика примарна броја. Приватни кључ се такође изводи од иста два примарна броја и због тога снага енкрипције лежи у величини кључа (у нашем случају користи се кључ од 2048 бита дужине). Кључеви су математички повезани, али се не може извести приватни кључ на основу јавног кључа. На слици 4 приказани су разни кључеви који се користе у случају безбедног стартовања процесорског система Zynq 7000.



Слика 4 – Приказ разних кључева који се користе за генерисање и декриптовање FSBL кода[6]

Извршавање фаза код безбедног стартовања Zynq 7000 компоненте приказано је на слици 5.



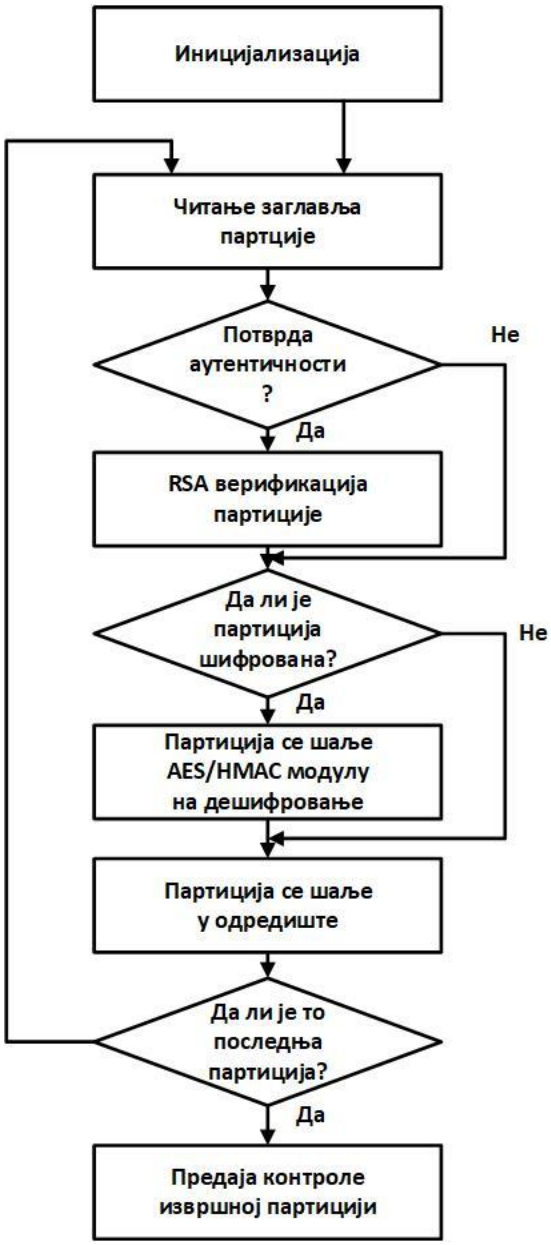
Слика 5 – Блок дијаграм безбедног стартовања [7]

Процес безбедног стартовања оперативног система иницран је од стране BootROM кода који се налази у ROM меморији процесорског система. Уколико је омогућена RSA провера аутентичности, она се извршава у другој фази (слика 5) уз коришћење јавног кључа. Овај процес се извршава на следећи начин: BootROM код учитава заглавље BOOT.bin фајла (слика 2), као и FSBL део истог фајла у првих 192 kB OCM меморије. Затим се учитава јавни кључ из BOOT.bin фајла, израчунава се његов SHA-256 потпис који се пореди са вредношћу која се налази у eFUSE меморији (слика 4 блок са десне стране). Уколико се вредности поклапају, BootROM код врши проверу аутентичности FSBL дела кода за стартовање система са јавним кључем. Ако је поређење кључева неуспешно, или је неуспешна провера аутентичности FSBL-а, BootROM код трага за новим FSBL-ом уколико се ради о флеш меморији, или улази у стање грешке уз омогућавање JTAG-а, или у закључано стање уколико је BOOT.bin фајл криптован.

После фазе провере аутентичности FSBL-а уколико заглавље BOOT.bin фајла показује да је реч о безбедном стартовању система, долази фаза декриптовања FSBL-а. Трећа фаза се извршава помоћу AES и HMAC модула који се налазе у PL делу процесорског система (доњи део слике 5). Да би се она извршила неопходан услов је да PL део система има напајање. После провере статуса напајања од стране BootROM кода, тј. пошто је напајање детектовано, врши се слање криптованог FSBL-а преко PCAP (Processor Config Access Port) интерфејса у AES и HMAC модуле. У четвртој фази безбедног стартовања, декриптовани FSBL код се шаље натраг у OCM меморију, и контрола стартовања система се предаје FSBL-у. У зависности од апликације овај код може да изврши конфигурацију PL-а, учита додатно софтвер, или чека инструкције из спољашњег извора. Да би се то безбедно урадило, FSBL мора да обезбеди проверу аутентичности наредних фаза подизања система. Софтвер који се надаље учитава мора да користи исти извор за кључ као и FSBL. Учитавање некриптованог софтвера је могуће, али није препоручљиво. На слици 6 приказан је дијаграм тока FSBL кода. FSBL врши проверу партиција кода који треба стартовати у процесорском систему [5]. Из заглавља сваке партиције чита се информација да ли треба вршити RSA проверу аутентичности, као и да ли је она шифрована. Уколико је партиција шифрована, она се шаље у AES/HMAC модул за дешифровање у PL-у, и тек након тога се смешта у радну меморију процесора. Провера аутентичности се врши помоћу аутентикационог сертификата који садржи јавни кључ и потпис.

Други начин за учитавање партиција у радну меморију је да FSBL учита SSBL, односно U-Boot код (u-boot.elf) и да преда контролу њему, тј. овај код надаље врши смештање партиција у меморију, и обавља сличне функције као и FSBL. U-Boot има и додатне функције као што су читање и упис NVM и DDR меморије. Може да ради интерактивно, када корисник прекине стартовање система, и када се јавља zynq-uboot „prompt“ ознака. Функционалност овог кода се може мењати изменама у zynq_common.h фајлу који се налази у include/configs директоријуму. Након измене конфигурације U-Boot код се мора поново компајлирати [5].

Zynq 7000 SoC процесорски систем после безбедног стартовања се налази у тзв. сигурном стању. У несигурно стање се прелази само ако је BootROM код детектовао да FSBL није криптован [4].

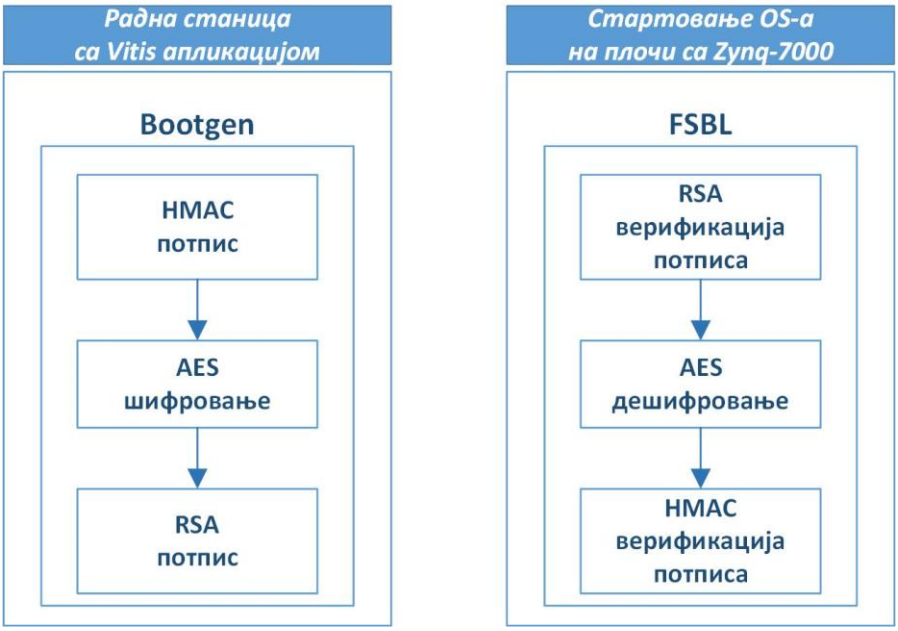


Слика 6 – Ток извршавања FSBL кода [5]

AES енкриптовање и RSA аутентификација

Bootgen и FSBL софтвер подржавају AES енкриптовање, као и HMAC и RSA аутентикацију. За AES/HMAC се користе приватни кључеви, док се за RSA аутентификацију користе парови приватно/јавних кључева. За RSA аутентификацију Bootgen код потписује партиције, док их BootROM и FSBL кодови верификују. Код RSA аутентификације приватни кључ се користи у току производње софтвера, док се јавни кључ смешта у оквиру процесорског система, тачније у eFUSE меморију. Овај пар кључева се може мењати по потреби.

На слици 7 приказана је интеракција између Bootgen и FSBL софтвера који се извршавају у оквиру радне станице и Zynq процесорског система респективно [5].



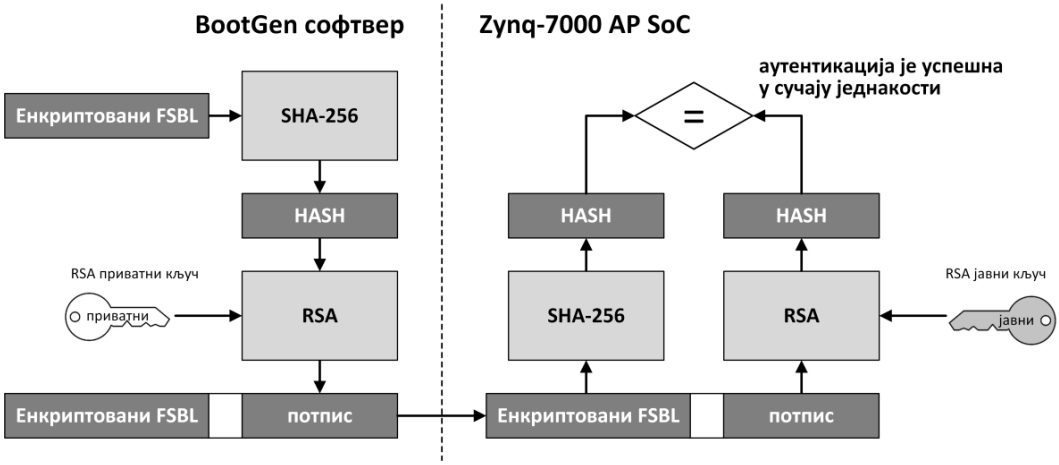
Слика 7 – Редослед извршавања функција Bootgen и FSBL кода [5]

Као што се са слике 7 види, Bootgen код генерише најпре HMAC потпис, затим следи AES шифровање (енкрипција) и на крају RSA потписивање. У оквиру безбедног стартовања Zynq процесорског система FSBL код извршава поменуте функције обрнутим редоследом: RSA верификација, AES декриптовање и HMAC верификација.

Као што је већ речено код Zynq 7000 архитектуре се користе два начина за смештање кључа: батеријски подржани RAM (BBRAM) или једнократно програмабилни осигурач (eFUSE). Недостатак код једнократно програмабилних осигурача је што једном програмиран кључ није могуће поново програмирати, док са друге стране коришћење BBRAM-а може да изазове проблеме у одржавању (услед флуктуације напона напајања може доћи до губитка кључа, као и услед истрошености батерије). За смештање кључа у меморију користи се 256-битска функција сажимања (SHA-256). Пошто је FSBL први део корисничког кода који се учитава из спољњег извора, веома је важно да се у овој тачки обезбеди ауторизација и на тај начин иницира „ланац поверења“ [9]. Обезбеђивање аутентичности коришћењем асиметричне технике шифровања приказано је на слици 8.

Асиметрична провера аутентичности (дигитални потпис) уз коришћење RSA-2048 је криптографска функција која користи два различита типа кључа: приватни за генерисање дигиталног потписа и јавни за његово проверавање. Генерисање потписа се врши помоћу Bootgen софтвера, а верификација се врши у самом Zynq 7000 уређају у току процеса безбедног стартовања (слика 8). 256-битни хеш запис јавног кључа се програмира у оквиру eFUSE вектора унутар процесорског дела Zynq 7000 SoC-а. Корисник Xilinx-ових модула

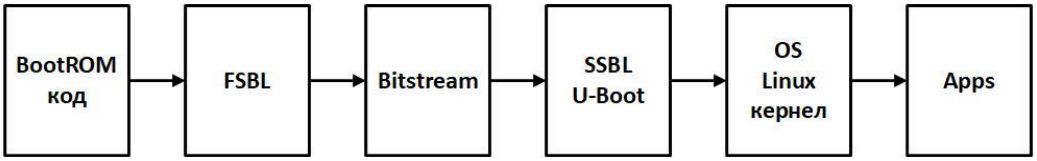
је одговоран за генерисање приватног и јавног кључа, омогућавање RSA као и програмирање јавног кључа у Zynq 7000 SoC [9].



Слика 8 – Обезбеђивање аутентичности коришћењем асиметричне технике шифровања

Пошто функцију RSA аутентификације за FSBL извршава BootROM код, неопходно је да она буде убачена и у FSBL или U-Boot, да би се извршила на исти начин и аутентификација остатка софтвера који се учитава помоћу осталих делова кода из ланца за подизање система (FSBL/SSBL).

Методе које се користе код безбедног стартовања процесорског система Zynq 7000 имају за циљ да спрече учитавање модификоване партиције у радну меморију, као и да сачувају поверљивост података у њима. У току извршавања Bootgen кода корисник одлучује које ће партиције бити шифроване, као и на којима ће се извршити аутентификација коришћењем RSA пара јавног/приватног кључа. Тако се формира тзв. ланац поверења који је приказан на слици 9 [5].



Слика 9 – Ланац поверења који се формира у току безбедног стартовања процесорског система

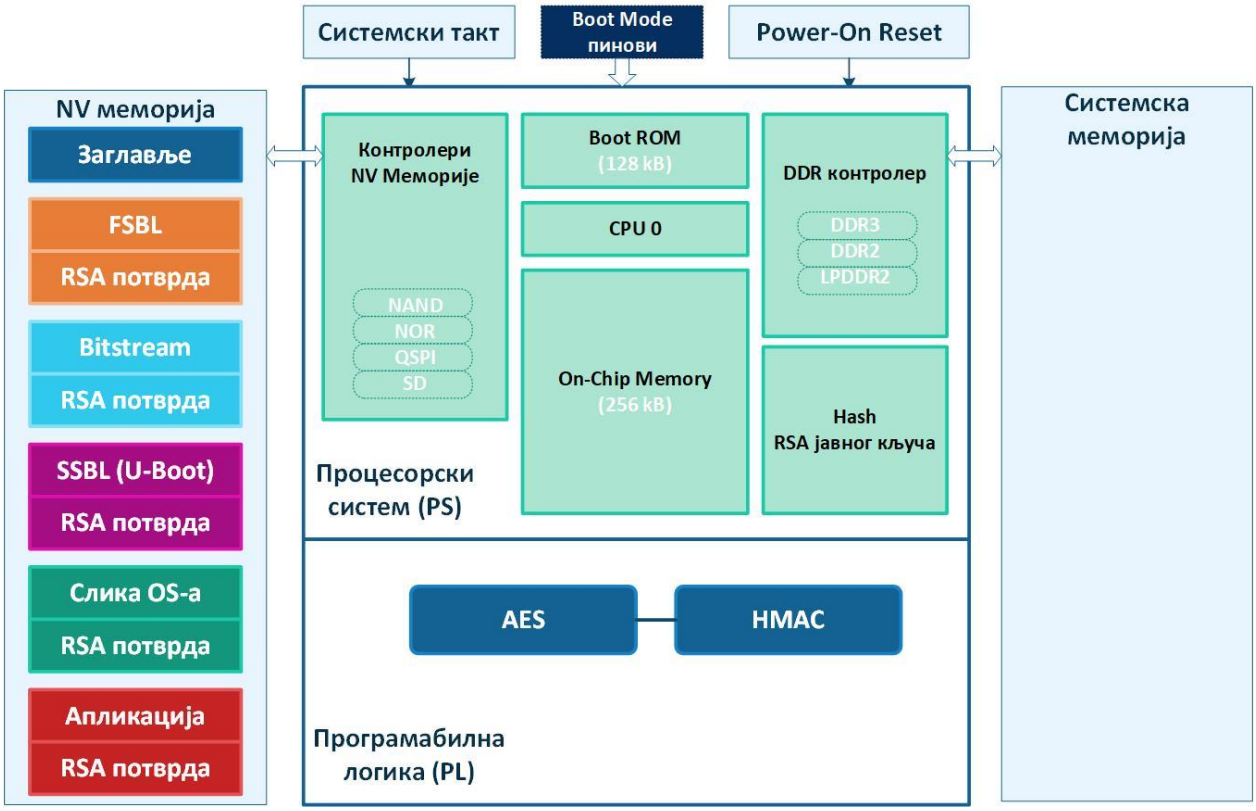
Веома важан део сигурности процесорских система овог типа је сигурност кључева. Предност RSA аутентификације је да се приватни кључеви не смештају у уређају, затим да се за различите партиције генеришу различити кључеви, као и да се RSA кључеви могу мењати у току ажурирања партиција. Додатно Zynq 7000 процесорски систем има релативно велику тзв. сигурну меморију, која се користи за складиштење осетљивих података и делова кода. Линкер скрипт фајл као и одређени атрибути омогућавају

извршавање „open source“ кода из DDR меморије, и „осетљивих“ апликација из сигурне меморије на чипу (OCM).

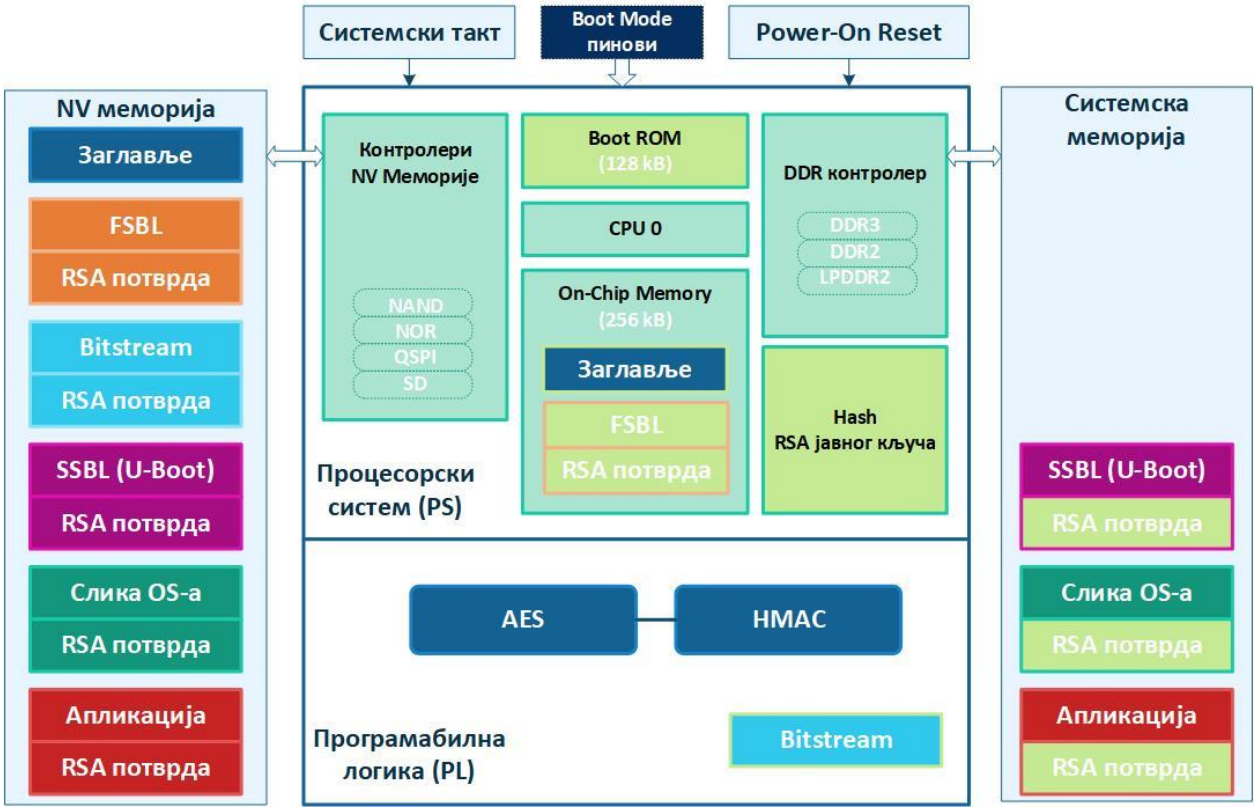
Процес генерисања кода за безбедно стартовање процесорског система Zynq 7000 се састоји из следећих фаза:

1. Генерисање AES/HMAC кључа
2. Генерисање јавног и тајног кључа за RSA аутентификацију
3. Заштита RSA јавног кључа применом „hash“ поступка
4. Коришћење поменутих кључева за шифровање и потпис партиција слике за стартовање процесорског система
5. Програмирање AES/HMAC кључа у PL део процесорског система (у неку од сигурних меморија процесорског система eFUSE или BBRAM)
6. Програмирање RSA јавног кључа који је обрађен hash поступком у eFUSE вектор PS дела процесорског система
7. Програмирање шифрованих/потписаних партиција слике за стартовање процесорског система у NV меморију.

На сликама 10 и 11 приказане су блок шеме стања процесорског система Zynq 7000 на почетку и на крају процеса безбедног стартовања.



Слика 10 – Стање процесорског система на почетку процеса безбедног стартовања [6]

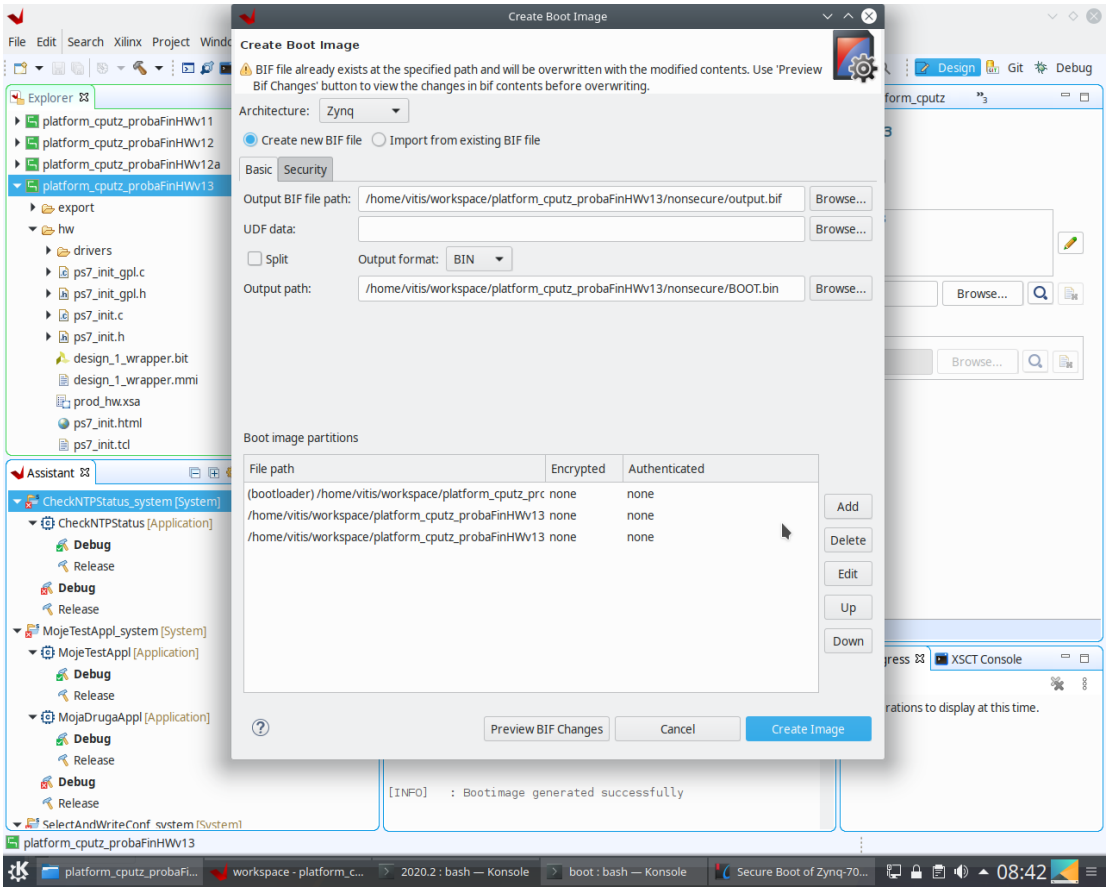


Слика 11 – Стање процесорског система на крају процеса безбедног стартовања [6]

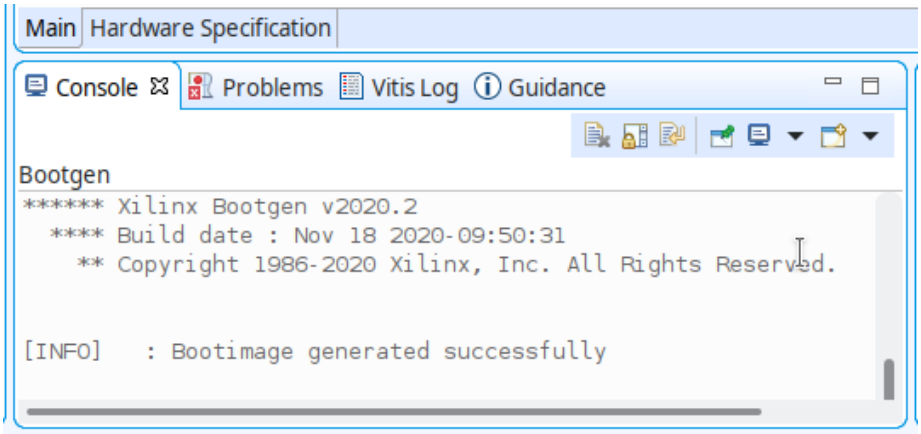
Реализација кода за безбедно стартовање

Реализација поменутих фаза за генерисање кода за безбедно стартовање Zynq 7000 процесора се обавља помоћу софтвера Xilinx-овог развојног окружења Vivado Design Suite и Vitis. Vivado Design Suite служи за генерисање .xsa ајла, док Vitis софтверски пакет служи за генерисање софтверских пројеката на основу хардверских платформи које се креирају на основу XSA фајла. Помоћу Vitis софтвера се може креирати и BOOT.bin фајл тј. слика за стартовање система у свом базичном облику без криптовања, као и са криптовањем.
Креирање BOOT.bin без криптовања приказано је на примеру платформског пројекта „platform_cputz_probaFinHWv13“ на слици 12. Да би се задале путање за излазни фајл, као и улазни фајлови, потребно је у оквиру платформског пројекта изабрати из главног менија опцију „Xilinx“, затим из подменија опцију „Create Boot Image“ након чега се отвара прозор приказан на слици 12. Са слике се види да је изабрано генерисање BOOT.bin фајла без криптовања, као и да су задате путање за фајлове који ће бити генерисани (.bif и .bin). BIF (bootgen image format) фајл служи за спецификацију како ће поједине партиције бити заштићене, као и где ће бити смештене у радној меморији. У доњем делу прозора са насловом „Boot image partitions“ , помоћу опције „Add“ врши се додавање партиција које треба да уђу у састав BOOT.bin фајла. Ту треба додати fsbl.elf фајл који представља FSBL партицију, затим design_1_wrapper.bit фајл који представља Bitstream партицију, која служи за конфигурацију FPGA дела система, и на крају u-boot.elf фајл којим је представљена SSBL

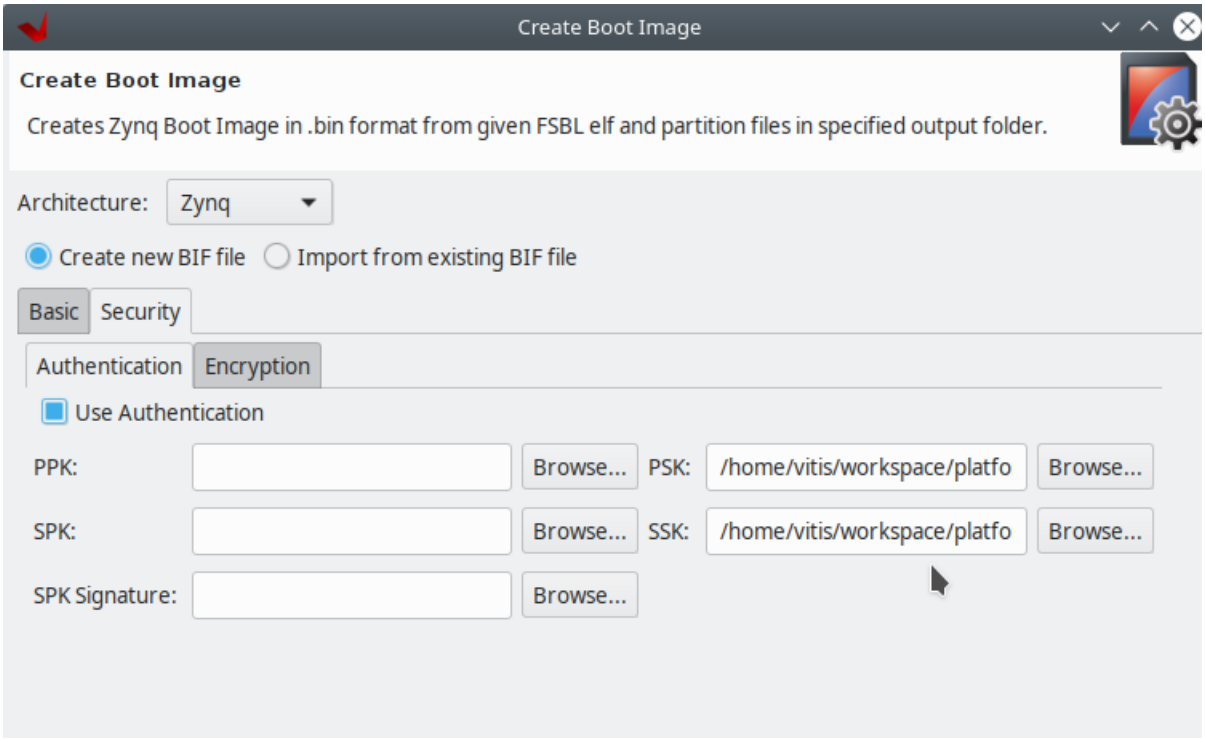
(Second Stage Bootloader) партиција (слика 9). За поменуте партиције није изабрана ни опција криптовања, ни аутентикације. На крају треба изабрати опцију за креирање слике за стартовање система – „Create Image“. Резултат поменуте операције је приказан на слици 13. Креирање BOOT.bin фајла са криптовањем је приказано на сликама 14, 15 и 16. Поступак је у свом почетном делу исти као код генерисања слике за стартовање без криптовања. У оквиру прозора „Create Boot Image“, са изабраном картицом „Security“ и поткартицом „Authentication“ треба означити опцију „Use Autentication“ и задати путање до „rsa“ тајних кључева: PSK – примарни тајни кључ и SSK – секундарни тајни кључ као што је приказано на слици 14, а потом преласком на поткартицу „Encryption“ означити и опцију „Use Encryption“ као што је приказано на слици 15. На крају у оквиру поменутог прозора треба додати фајлове који чине слику за стартовање система, али са сетованим опцијама за „aes“ енкрипцију и „rsa“ аутентикацију као што је приказано на слици 16 и изабрати опцију за креирање слике „Create Image“. На слици 17 приказан је резултат креирања BOOT.bin фајла.



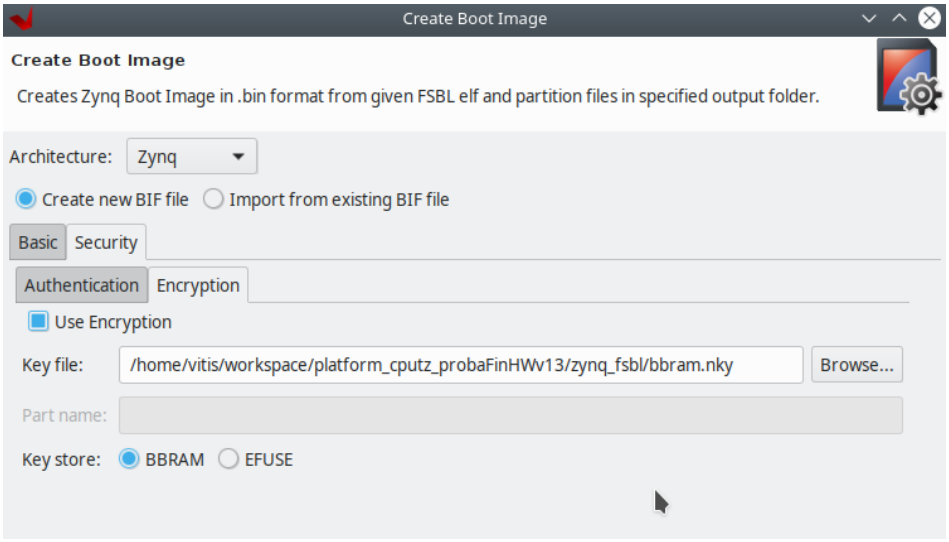
Слика 12 – Креирање некриптованог BOOT.bin фајла у оквиру платформског пројекта у Vitis развојном окружењу



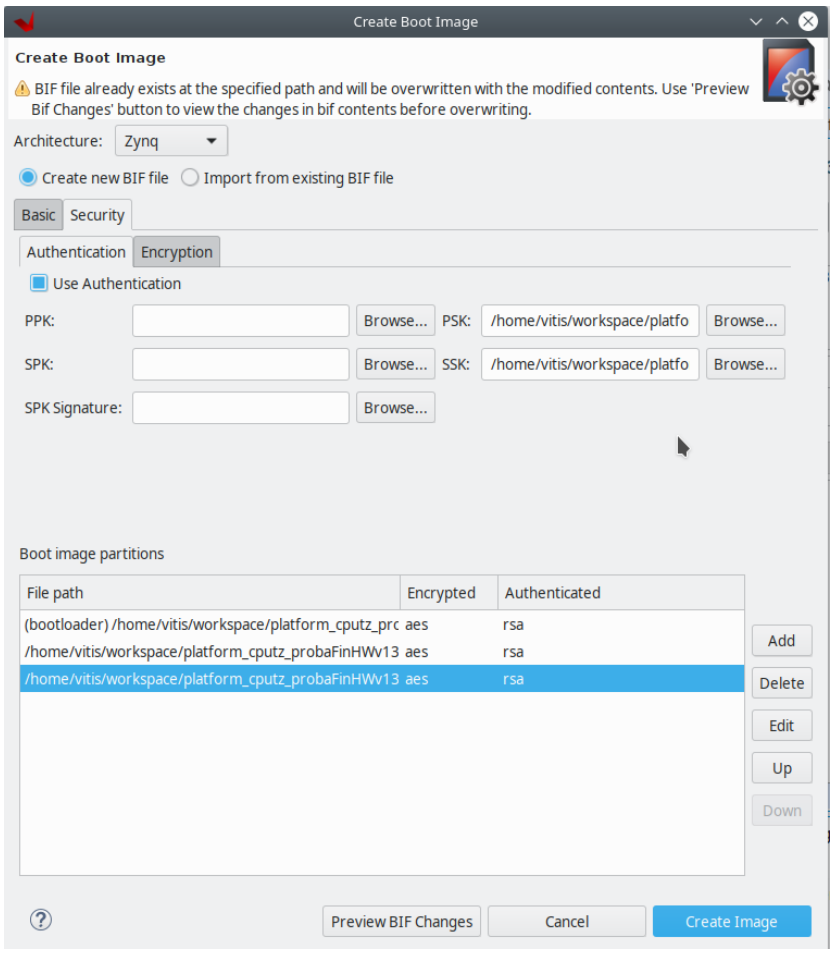
Слика 13 – Резултат креирања BOOT.bin фајла у конзолном прозору Vitis развојног окружења



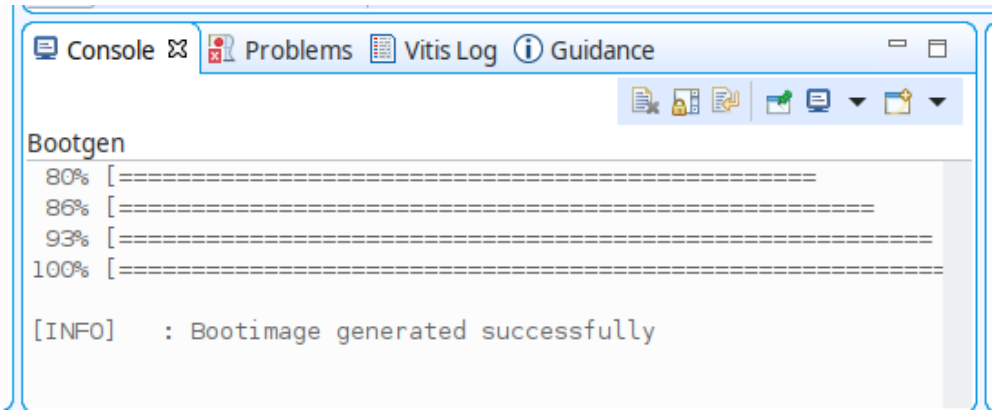
Слика 14 – Изабрана опција „Use Authentication“ у прозору „Create Boot Image“ и путање до тајних „rsa“ кључева



Слика 15 – Изабрана опција „Use Encryption“ у прозору „Create Boot Image“ и путање до „aes“ кључа



Слика 16 –Креирање криптоване слике за стартовање система, уз измену опција „encrypted“ и „authenticated“ за додате партиције које чине излазни BOOT.bin фајл



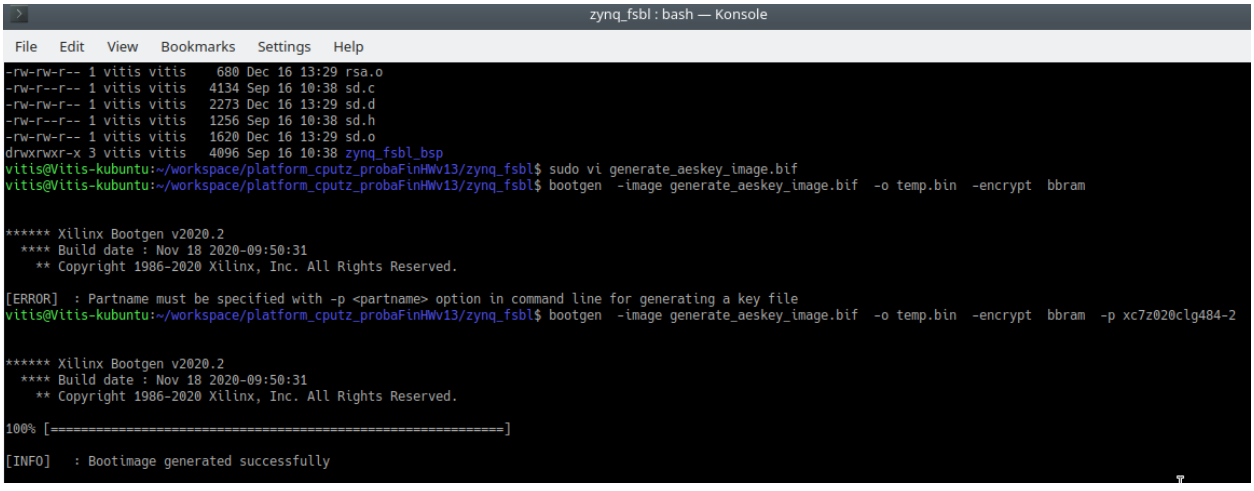
Слика 17 – Резултат креирања криптованог BOOT.bin фајла у конзолном прозору Vitis развојног окружења

Као што се из претходног текста може видети за генерисање криптованог BOOT.bin фајла неопходно је најпре генерисати потребне кључеве за „aes“ криптовање и „rsa“ аутентификацију. За генерисање „aes“ кључа помоћу Xilinx-овог Bootgen алата из Vitis развојног окружења најпре је потребно креирати фајл чији је садржај приказан на слици 18.

```
generate_aeskey_image:
{
[aeskeyfile] bbram.nky
[bootloader, encryption=aes] fsbl.elf
}
```

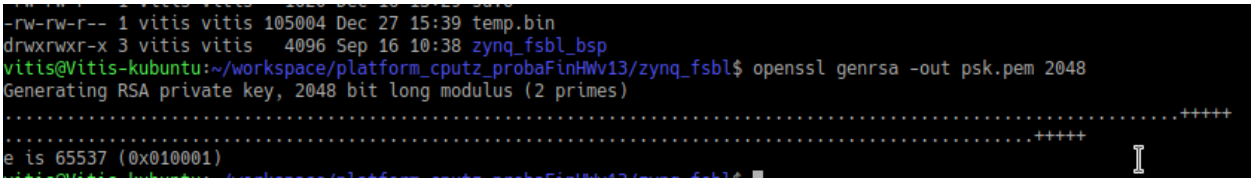
Слика 18 – Улазни фајл за генерисање „aes“ кључа

Затим треба из командне линије стартовати Bootgen програм са одређеним опцијама као што је приказано на слици 19.



Слика 19 – Генерисање „aes“ кључа тј. фајла bbram.nky

За генерисање „rsa“ кључа потребно је такође из командне линије стартовати „openssl“ програм са одговарајућим опцијама као што је приказано на слици 20



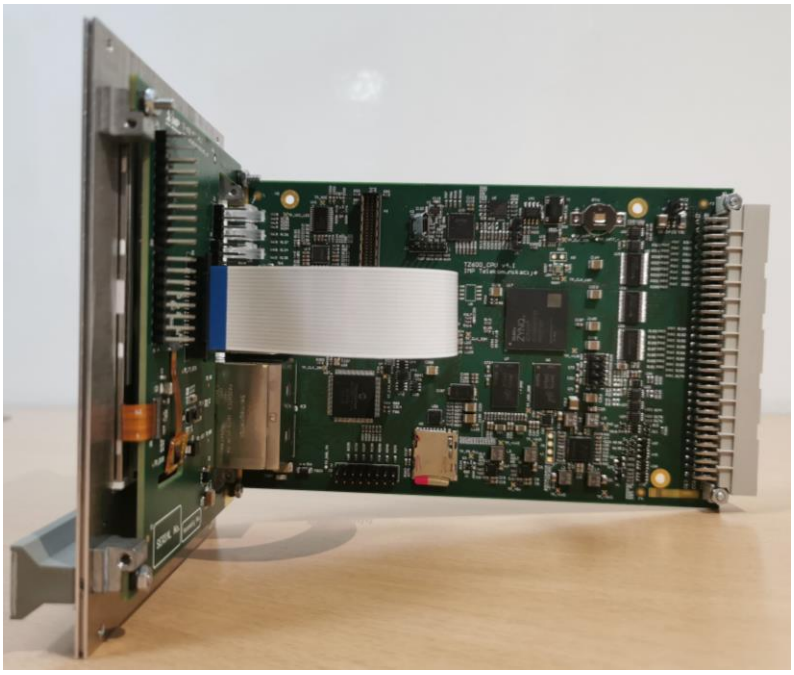
Слика 20 – Генерисање примарног тајног „rsa“ кључа – psk.pem

Програмирање „aes“ кључа се врши помоћу HW Manager програма (у оквиру Vivado развојног окружења) или Secure Key Driver програма. HW Manager се може користити и за програмирање у BBRAM или у eFUSE меморију. Опција Bootgen програма „encrypt“ специфицира који се кључ користи. У заглавље слике за стартовање система уписује се место где се налази кључ. Код стартовања система након укључивања напајања BootROM код чита ово заглавље да би се одредило место кључа.

За покретање система са SD картице креирани BOOT.bin фајл треба уписати на картицу, у њену BOOT партицију.

Закључак

У овом техничком решењу приказана је метода којом се обезбеђује реализација безбедног стартовања оперативног система и софтвера који ради на централном процесорском модулу телезаштитног терминала (приказаном на слици 20). Код креирања слике система, како би се обезбедило безбедно стартовање, треба одредити које ће партиције бити шифроване, и/или аутентификоване. Такође је потребно одредити који делови софтвера и подаци морају бити заштићени, тј. смештени у сигурну меморију Zynq процесорског система, јер само нужно осетљиве информације треба да буду обезбеђене како перформансе система не би опале. FSBL партиција мора бити шифрована и аутентификована. Партиције које садрже ауторски заштићене податке као што су конфигурациони подаци за PL део процесорског система свакако морају бити шифроване, а партиције које садрже тзв. доступни софтвер (open source software) као нпр. U-Boot и Linux не требају бити шифроване, већ само аутентификоване, да би се осигурало да нису злонамерно модификоване. Реализација начина заштите појединих партиција се врши помоћу Bootgen програма из Xilinx-овог развојног окружења. У оквиру овог програма користи се специјални фајл тзв. BIF фајл за спецификацију криптовања и смештања партиција у меморију. Излазни фајл Bootgen програма може бити у бинарном или MCS формату у зависности од врсте меморије која се користи за смештање кода за стартовање система (SD картица или QSPI флеш меморија).



Слика 21 – Реализовани централни процесорски модул телезаштитног терминала TZ-600

Нови централни модул, уграђен у постојећи телезаштитни уређај TZ-600, приказан је на слици 22, на којој се могу видети и придодати Етернет прикључци.

Слика 22 – Нова централна процесорска јединица у уређају TZ-600

Референце:

[1] IEC 60834-1: “Teleprotection Equipment of Power Systems - Performance and Testing - Part 1: Command Systems,” 2nd edition, October 1999

[2] IEC/TR 61850-90-1: “Communication networks and systems for power utility automation - Part 90-1: Use of IEC 61850 for the communication between substations,” March 2010

[3] IEC 62351-6, Power systems management and associated information exchange – Part 6: Security for IEC 61850, Edition 1.0, International Electrotechnical Commission, Geneva, Switzerland, 2020.

[4] Zynq-7000 SoC Technical Reference Manual, XILINX, UG585 (v1.13) April 2, 2021.

[5] Ed Peterson: „Secure Boot of Zynq-7000 SoC“, XILINX XAPP1175 (v2.2), 2021.

[6] Nasser Poureh: „Zynq Boot and Configuration Procedures“, Xfest presentation, Avnet, 2014.

[7] Ali Shuja Siddiqui, Yutian Gui, Fareena Saqib: „Secure Boot for Reconfigurable Archiectures“, Cryptography Journal, September 2020.

[8] Unterstein, F., Jacob, N., Hanley, N. et al. SCA secure and updatable crypto engines for FPGA SoC bitstream decryption: extended version. J Cryptogr Eng 11, 257–272 (2021).

[9] Ed Peterson: „Leveraging Asymmetric Authentication to Enhance Security-Critical Applications Using Zynq-7000 All Programmable SoCs”, WP468 (v1.0) October 20, 2015.

[10] Ali Shuja Siddiqui, Yutian Gui and Fareena Saqib: „Secure Boot for Reconfigurable Architectures“, Cryptography 2020, 4, 26.

Допринос аутора:

Руковођење пројектом: Владимир Челебић
Дизајн архитектуре и спецификација функција: Владимир Челебић, Миленко Кабовић, Јована Новаковић
Реализација система: Миленко Кабовић, Јована Новаковић, Ива Салом
Тестирање система: Анка Кабовић, Владислав Миленковић

Листа претходних техничких решења по ауторима

АНКА КАБОВИЋ

2021.

1. Владимир Челебић, Миленко Кабовић, Ива Салом, Анка Кабовић, Јована Новаковић, Горан Димић, " Унапређење мрежних интерфејса централног модула за телезаштитни терминал " – М83
https://www.pupin.rs/code/wp-content/uploads/2022/01/TR-2021-IMP-T-1-M83.pdf

2020.

2. Владимир Челебић, Ива Салом, Миленко Кабовић, Анка Кабовић, Јованка Гајица, Миливоје Ралевић, "Обједињени систем за централизовано надгледање и синхронизацију тачног времена телезаштитних терминала" – М84
http://www.pupin.rs/code/wp-content/uploads/2020/12/TR-2020-IMP-T-1-M84.pdf
3. Владимир Челебић, Миленко Кабовић, Ива Салом, Анка Кабовић, Јована Новаковић, Горан Димић, "Нови централни модул за телезаштитни терминал" – М85
http://www.pupin.rs/code/wp-content/uploads/2020/12/TR-2020-IMP-T-2-M85.pdf
4. Анка Кабовић, Миленко Кабовић, Јованка Гајица, Иван Кокић, Ненад Антонић, Славица Бошtјанчич Ракас, Валентина Тимченко, „Систем за динамичко праћење сигурносног растојања проводника на далеководу 110kV бр. 176/3" – М84
http://www.pupin.rs/code/wp-content/uploads/2020/12/TR-2020-IMP-T-3-M84.pdf

2019.

5. Владимир Челебић, Миленко Кабовић, Анка Кабовић, Ива Салом, Јованка Гајица, "Сервер за централизовано надгледање и синхронизацију времена телезаштитних терминала у мрежи ЕМС АД" – М84
http://www.imptelecom.com/media/TehnickaResenja/2019/TR32037_2019A1.pdf
6. Владимир Челебић, Ива Салом, Миленко Кабовић, Анка Кабовић, Јованка Гајица, "Мерне методе за одређивање тачности процеса синхронизације времена на уређају за пренос сигнала телезаштите" – М84
http://www.imptelecom.com/media/TehnickaResenja/2019/TR32037_2019A2.pdf
7. Анка Кабовић, Миленко Кабовић, Јованка Гајица, Славица Бошtјанчич Ракас, Валентина Тимченко "Софтвер за краткорочно предвиђање максималног дозвољеног струјног оптерећења далековода" – М85.
http://www.imptelecom.com/media/TehnickaResenja/2019/TR32037_2019A3.pdf

2018.

8. Владимир Челебић, Миленко Кабовић, Анка Кабовић, Ива Салом, Јованка Гајица, "Надоградња система за пренос сигнала телезаштите у мрежи преноса ЕМС АД имплементацијом синхронизације тачног времена" – М84
http://www.imptelecom.com/media/TehnickaResenja/2018/TR32037_2018A1.pdf
9. Владимир Челебић, Миленко Кабовић, Анка Кабовић, Ива Салом, Јованка Гајица, Братислав Планић, "Унапређени телезаштитни терминал TZ-600 за повећање расположивости и убрзање преноса сигнала дистантне заштите за потребе ЈП ЕПС, огранак ХЕ Ђердап" – М84
http://www.imptelecom.com/media/TehnickaResenja/2018/TR32037_2018A2.pdf

2017.

10. Анка Кабовић, Иван Кокић, Јованка Гајица, Славица Бошtјанчич Ракас, Валентина

Тимченко, “Апликација за пријем података са метео-ролошких станица реализована у оквиру система за праћење температуре проводника далековода у мрежи ЕМС-а” – М85
http://www.imptelecom.com/media/TehnickaResenja/2017/TR32037_2017A4.pdf

11. Анка Кабовић, Миленко Кабовић, Јованка Гајица, “Апликација за прорачун максималног дозвољеног струјног оптерећења далековода” – М85
http://www.imptelecom.com/media/TehnickaResenja/2017/TR32037_2017A3.pdf

2016.

12. Владимир Челебић, Анка Кабовић, Миленко Кабовић, Јованка Гајица, Ива Салом, Јелена Васиљевић, Драгослав Мијић, “Повезивање телезаштитног терминала на резервни преносни пут преко Етернет интерфејса у мрежи ЕМС-а” – М84;
http://www.imptelecom.com/media/TehnickaResenja/2016/TR32037-2016A2.pdf

2015.

13. Анка Кабовић, Миленко Кабовић, Јелена Васиљевић, Ива Салом, Владимир Челебић, Јованка Гајица, “Софтвер за симулацију размене GOOSE поруке између заштитног релеа и телезаштитног уређаја у подстаници” – М85
http://www.imptelecom.com/media/TehnickaResenja/2015/TR32037-2015A2.pdf

ВЛАДИМИР ЧЕЛЕБИЋ

2021.

1. Владимир Челебић, Миленко Кабовић, Ива Салом, Анка Кабовић, Јована Новаковић, Горан Димић, " Унапређење мрежних интерфејса централног модула за телезаштитни терминал " – М83
https://www.pupin.rs/code/wp-content/uploads/2022/01/TR-2021-IMP-T-1-M83.pdf

2020.

2. Владимир Челебић, Ива Салом, Миленко Кабовић, Анка Кабовић, Јованка Гајица, Миливоје Ралевић, "Обједињени систем за централизовано надгледање и синхронизацију тачног времена телезаштитних терминала" – М84
http://www.pupin.rs/code/wp-content/uploads/2020/12/TR-2020-IMP-T-1-M84.pdf
3. Владимир Челебић, Миленко Кабовић, Ива Салом, Анка Кабовић, Јована Новаковић, Горан Димић, "Нови централни модул за телезаштитни терминал" – М85
http://www.pupin.rs/code/wp-content/uploads/2020/12/TR-2020-IMP-T-2-M85.pdf

2019.

4. Владимир Челебић, Миленко Кабовић, Анка Кабовић, Ива Салом, Јованка Гајица, "Сервер за централизовано надгледање и синхронизацију времена телезаштитних терминала у мрежи ЕМС АД" – М84
http://www.imptelecom.com/media/TehnickaResenja/2019/TR32037_2019A1.pdf
5. Владимир Челебић, Ива Салом, Миленко Кабовић, Анка Кабовић, Јованка Гајица, "Мерне методе за одређивање тачности процеса синхронизације времена на уређају за пренос сигнала телезаштите" – М84
http://www.imptelecom.com/media/TehnickaResenja/2019/TR32037_2019A2.pdf
6. Владимир Ћатић, Ива Салом, Владимир Челебић, Дејан Тодоровић, Јована Новаковић, Братислав Планић, Вељко Јанић, Марко Ралић, Ивана Николић, Наталија Кокић, "Унапређена акустичка камера за посебне намене" – М84
http://www.imptelecom.com/media/TehnickaResenja/2019/TR32038_2019A1.pdf

2018.

7. Јована Новаковић, Ива Салом, Владимир Челебић, Дејан Тодоровић, Владимир Ћатић, Вељко Јанић, Братислав Планић, "Акустичка камера за посебне намене" – М82
http://www.imptelecom.com/media/TehnickaResenja/2018/TR32038_2018A1.pdf
8. Владимир Челебић, Миленко Кабовић, Анка Кабовић, Ива Салом, Јованка Гајица, Братислав Планић, "Унапређени телезаштитни терминал TZ-600 за повећање расположивости и убрзање преноса сигнала дистантне заштите за потребе ЈП ЕПС, огранак ХЕ Ђердап" – М84
http://www.imptelecom.com/media/TehnickaResenja/2018/TR32037_2018A2.pdf
9. Владимир Ћатић, Ива Салом, Владимир Челебић, Дејан Тодоровић, Наталија Лукић, Ивана Николић, "Софтверска симулација акустичке камере са beamforming алгоритмом" – М85
http://www.imptelecom.com/media/TehnickaResenja/2018/TR32038_2018A2.pdf
10. Владимир Челебић, Миленко Кабовић, Анка Кабовић, Ива Салом, Јованка Гајица, "Надоградња система за пренос сигнала телезаштите у мрежи преноса ЕМС АД имплементацијом синхронизације тачног времена" – М84
http://www.imptelecom.com/media/TehnickaResenja/2018/TR32037_2018A1.pdf

2017.

11. Владислав Миленковић, Владимир Челебић, Братислав Планић, Ива Салом, Вукашин Ристић, Бојан Косић, Горан Димић, Ненад Антонић, “Реализација уређаја за тестирање и анализу рада система за пренос сигнала телезаштите” – М85 http://www.imptelecom.com/media/TehnickaResenja/2017/TR32043-2017-IMP-M85-TTZ.pdf
12. Вукашин Ристић, Братислав Планић, Ива Салом, Жељко Стојковић, Владимир Челебић, Горан Димић, Ненад Антонић, Бојан Косић, Владислав Миленковић, “Самостални Bluetooth микрофон студијског квалитета – MIKME” – М81 http://www.imptelecom.com/media/TehnickaResenja/2017/TR32043-2017-IMP-M81-MIKME.pdf
13. Наталија Лукић, Владимир Ћатић, Вељко Јанић, Владислав Миленковић, Ненад Антонић, Вукашин Ристић, Братислав Планић, Жељко Стојковић, Владимир Челебић, Горан Димић, Иван Кокић, “Окружење за аутоматско тестирање система за аквизицију и обраду података” – М84 http://www.imptelecom.com/media/TehnickaResenja/2017/III44003-2017-M84-ATE.pdf

2016.

14. Владимир Челебић, Анка Кабовић, Миленко Кабовић, Јованка Гајица, Ива Салом, Јелена Васиљевић, Драгослав Мијић, “Повезивање телезаштитног терминала на резервни преносни пут преко Етернет интерфејса у мрежи EMC-а” – М84 http://www.imptelecom.com/media/TehnickaResenja/2016/TR32037-2016A2.pdf
15. Ива Салом, Владимир Челебић, Миленко Кабовић, Наталија Лукић, Владимир Ћатић, Вукашин Ристић, Јованка Гајица, Марко Оклобџија, Ненад Карталовић, Миомир Мијић, “Решење проблема нелинеарности напонски контролисаног појачавача са JFET транзистором” – М85 http://www.imptelecom.com/media/TehnickaResenja/2016/TR32038-2016A1.pdf
16. Ива Салом, Вукашин Ристић, Миленко Кабовић, Владимир Челебић, Жељко Стојковић, Наталија Лукић, Владимир Ћатић, Лазар Бербаков, Бојан Косић, “Алгоритамска компензација разлике компоненти JFET-а за контролу појачања у напонски контролисаном појачавачу” – М85 http://www.imptelecom.com/media/TehnickaResenja/2016/TR32043-2016-M85-IMP-JFET.pdf

2015.

17. Владимир Челебић, Миленко Кабовић, Ива Салом, Јованка Гајица, “Оптички интерфејс ИМП терминала за телезаштиту са мултиплексерском опремом” – М84 http://www.imptelecom.com/media/TehnickaResenja/2015/TR32037-2015A1.pdf
18. Анка Кабовић, Миленко Кабовић, Јелена Васиљевић, Ива Салом, Владимир Челебић, Јованка Гајица, “Софтвер за симулацију размене GOOSE поруке између заштитног релеа и телезаштитног уређаја у подстаници” – М85 http://www.imptelecom.com/media/TehnickaResenja/2015/TR32037-2015A2.pdf

ВЛАДИСЛАВ МИЛЕНКОВИЋ

2021.

1. Владислав Миленковић, Иван Тодоровић, Марко Ралић, Вукашин Ристић, Анастасија Николић, Жељко Стојковић, Горан Димић, „Унапређење реализације web сервиса и локалног апликативног софтвера за управљање GIVA IPC паметним модуларним аудио појачалом“, М83
https://www.pupin.rs/code/wp-content/uploads/2022/01/TR-2021-IMP-T-2-M83.pdf

2020.

2. Владислав Миленковић, Иван Тодоровић, Вукашин Ристић, Наталија Кокић, Ива Салом, Анастасија Перић, „Развој GIVA IPC паметног модуларног аудио појачала заснованог на DSP процесору Allwinner H2+ и оперативном систему Linux“, М81
http://www.pupin.rs/code/wp-content/uploads/2020/12/TR-2020-IMP-T-5-M81.pdf

2018.

3. Братислав Планић, Вељко Јанић, Ива Салом, Вукашин Ристић, Горан Димић, Владислав Миленковић, Лазар Бербаков, “Побољшање квалитета аудио сигнала самосталног Bluetooth микрофона MIKME студијског квалитета” – М83
http://www.imptelecom.com/media/TehnickaResenja/2018/TR32043_2018A2.pdf

2017.

4. Владислав Миленковић, Владимир Челебић, Братислав Планић, Ива Салом, Вукашин Ристић, Бојан Косић, Горан Димић, Ненад Антонић, “Реализација уређаја за тестирање и анализу рада система за пренос сигнала телезаштите” – М85
http://www.imptelecom.com/media/TehnickaResenja/2017/TR32043-2017-IMP-M85-TTZ.pdf
5. Марјан Ђурић, Вукашин Ристић, Бојан Косић, Горан Димић, Ненад Антонић, Владислав Миленковић, Ина Масникоса, “Модификован регистрофонски систем за потребе железнице” – М85
http://www.imptelecom.com/media/TehnickaResenja/2017/TR32043-2017-IMP-M85-REG-ZEL.pdf
6. Вукашин Ристић, Братислав Планић, Ина Салом, Жељко Стојковић, Владимир Челебић, Горан Димић, Ненад Антонић, Бојан Косић, Владислав Миленковић, “Самостални Bluetooth микрофон студијског квалитета – MIKME” – М81
http://www.imptelecom.com/media/TehnickaResenja/2017/TR32043-2017-IMP-M81-MIKME.pdf
7. Наталија Лукић, Владимир Ћатић, Вељко Јанић, Владислав Миленковић, Ненад Антонић, Вукашин Ристић, Братислав Планић, Жељко Стојковић, Владимир Челебић, Горан Димић, Иван Кокић, “Окружење за аутоматско тестирање система за аквизицију и обраду података” – М84
http://www.imptelecom.com/media/TehnickaResenja/2017/III44003-2017-M84-ATE.pdf

ИВА САЛОМ

2021.

1. Владимир Челебић, Миленко Кабовић, Ива Салом, Анка Кабовић, Јована Новаковић, Горан Димић, " Унапређење мрежних интерфејса централног модула за телезаштитни терминал " – М83
https://www.pupin.rs/code/wp-content/uploads/2022/01/TR-2021-IMP-T-1-M83.pdf

2020.

2. Владимир Челебић, Ива Салом, Миленко Кабовић, Анка Кабовић, Јованка Гајица, Миливоје Ралевић, "Обједињени систем за централизовано надгледање и синхронизацију тачног времена телезаштитних терминала" – М84
http://www.pupin.rs/code/wp-content/uploads/2020/12/TR-2020-IMP-T-1-M84.pdf
3. Владимир Челебић, Миленко Кабовић, Ива Салом, Анка Кабовић, Јована Новаковић, Горан Димић, "Нови централни модул за телезаштитни терминал" – М85
http://www.pupin.rs/code/wp-content/uploads/2020/12/TR-2020-IMP-T-2-M85.pdf
4. Владислав Миленковић, Иван Тодоровић, Вукашин Ристић, Наталија Кокић, Ива Салом, Анастасија Перић, „Развој GIVA IPC паметног модуларног аудио појачала заснованог на DSP процесору Allwinner H2+ и оперативном систему Linux", М81
http://www.pupin.rs/code/wp-content/uploads/2020/12/TR-2020-IMP-T-5-M81.pdf
5. Дејан Тодоровић, Ива Салом, Братислав Планић, Горан Димић, Владимир Ћатић, Мина Косић (Радивојевић), „Мерни систем за in situ мерење акустичких карактеристика звучних баријера према стандардима EN 1793-5 и EN 1793-6", М82
http://www.pupin.rs/code/wp-content/uploads/2020/12/TR-2020-IMP-T-6-M82.pdf

2019.

6. Вељко Јанић, Валентина Тимченко, Славица Боштјанчич Ракас, Ива Салом, Иван Кокић, Владимир Ћатић, Братислав Планић, Вукашин Ристић, "MIKME Pocket – бежични аудио снимач" – М83.
http://www.imptelecom.com/media/TehnickaResenja/2019/III44003-2019-M83-MIKME_Pocket.pdf
7. Владимир Челебић, Миленко Кабовић, Анка Кабовић, Ива Салом, Јованка Гајица, "Сервер за централизовано надгледање и синхронизацију времена телезаштитних терминала у мрежи ЕМС АД" – М84
http://www.imptelecom.com/media/TehnickaResenja/2019/TR32037_2019A1.pdf
8. Владимир Челебић, Ива Салом, Миленко Кабовић, Анка Кабовић, Јованка Гајица, "Мерне методе за одређивање тачности процеса синхронизације времена на уређају за пренос сигнала телезаштите" – М84
http://www.imptelecom.com/media/TehnickaResenja/2019/TR32037_2019A2.pdf
9. Владимир Ћатић, Ива Салом, Владимир Челебић, Дејан Тодоровић, Јована Новаковић, Братислав Планић, Вељко Јанић, Марко Ралић, Ивана Николић, Наталија Кокић, "Унапређена акустичка камера за посебне намене" – М84
http://www.imptelecom.com/media/TehnickaResenja/2019/TR32038_2019A1.pdf

2018.

10. Јована Новаковић, Ива Салом, Владимир Челебић, Дејан Тодоровић, Владимир Ћатић, Вељко Јанић, Братислав Планић, "Акустичка камера за посебне намене" –

M82
http://www.imptelecom.com/media/TehnickaResenja/2018/TR32038_2018A1.pdf

11. Владимир Челебић, Миленко Кабовић, Анка Кабовић, Ива Салом, Јованка Гајица, Братислав Планић, "Унапређени телезаштитни терминал TZ-600 за повећање расположивости и убрзање преноса сигнала дистантне заштите за потребе ЈП ЕПС, огранак ХЕ Ђердап" – М84
http://www.imptelecom.com/media/TehnickaResenja/2018/TR32037_2018A2.pdf
12. Владимир Ћатић, Наталија Лукић, Ива Салом, Братислав Планић, Горан Димић, Иван Кокић, "Унапређење система за аутоматско тестирање хардверских јединица уређаја MIKME у процесу производње са проширењем примене на нове верзије уређаја и са додавањем нових опција" – М83
http://www.imptelecom.com/media/TehnickaResenja/2018/III44003-2018A1.pdf
13. Владимир Ћатић, Ива Салом, Владимир Челебић, Дејан Тодоровић, Наталија Лукић, Ивана Николић, "Софтверска симулација акустичке камере са beamforming алгоритмом" – М85
http://www.imptelecom.com/media/TehnickaResenja/2018/TR32038_2018A2.pdf
14. Владимир Челебић, Миленко Кабовић, Анка Кабовић, Ива Салом, Јованка Гајица, "Надоградња система за пренос сигнала телезаштите у мрежи преноса ЕМС АД имплементацијом синхронизације тачног времена" – М84
http://www.imptelecom.com/media/TehnickaResenja/2018/TR32037_2018A1.pdf
15. Братислав Планић, Вељко Јанић, Ива Салом, Вукашин Ристић, Горан Димић, Владислав Миленковић, Лазар Бербаков, "Побољшање квалитета аудио сигнала самосталног Bluetooth микрофона MIKME студијског квалитета" – М83
http://www.imptelecom.com/media/TehnickaResenja/2018/TR32043_2018A2.pdf

2017.

16. Владислав Миленковић, Владимир Челебић, Братислав Планић, Ива Салом, Вукашин Ристић, Бојан Косић, Горан Димић, Ненад Антонић, "Реализација уређаја за тестирање и анализу рада система за пренос сигнала телезаштите" – М85
http://www.imptelecom.com/media/TehnickaResenja/2017/TR32043-2017-IMP-M85-TTZ.pdf
17. Вукашин Ристић, Братислав Планић, Ива Салом, Жељко Стојковић, Владимир Челебић, Горан Димић, Ненад Антонић, Бојан Косић, Владислав Миленковић, "Самостални Bluetooth микрофон студијског квалитета – MIKME" – М81
http://www.imptelecom.com/media/TehnickaResenja/2017/TR32043-2017-IMP-M81-MIKME.pdf

2016.

18. Владимир Челебић, Анка Кабовић, Миленко Кабовић, Јованка Гајица, Ива Салом, Јелена Васиљевић, Драгослав Мијић, "Повезивање телезаштитног терминала на резервни преносни пут преко Етернет интерфејса у мрежи ЕМС-а" – М84;
http://www.imptelecom.com/media/TehnickaResenja/2016/TR32037-2016A2.pdf
19. Ива Салом, Владимир Челебић, Миленко Кабовић, Наталија Лукић, Владимир Ћатић, Вукашин Ристић, Јованка Гајица, Марко Оклобџија, Ненад Карталовић, Миомир Мијић, "Решење проблема нелинеарности напонски контролисаног појачавача са JFET транзистором" – М85
http://www.imptelecom.com/media/TehnickaResenja/2016/TR32038-2016A1.pdf
20. Ива Салом, Вукашин Ристић, Миленко Кабовић, Владимир Челебић, Жељко

Стојковић, Наталија Лукић, Владимир Ћатић, Лазар Бербаков, Бојан Косић, “Алгоритамска компензација разлике компоненти JFET-а за контролу појачања у напонски контролисаном појачавачу” – М85
http://www.imptelecom.com/media/TehnickaResenja/2016/TR32043-2016-M85-IMP-JFET.pdf

21. Владимир Ћатић, Наталија Лукић, Ива Салом, Вукашин Ристић, Миленко Кабовић, Никола Ненадић, Жељко Стојковић, Горан Димић, Ненад Антонић, Бојан Косић, “Систем за аутоматско тестирање хардверских јединица уређаја MIKME у процесу производње” – М81
http://www.imptelecom.com/media/TehnickaResenja/2016/TR32043-2016-M81-IMP-MIKMEATE.pdf

2015.

22. Владимир Челебић, Миленко Кабовић, Ива Салом, Јованка Гајица, “Оптички интерфејс ИМП терминала за телезаштиту са мултиплексерском опремом” – М84
http://www.imptelecom.com/media/TehnickaResenja/2015/TR32037-2015A1.pdf
23. Анка Кабовић, Миленко Кабовић, Јелена Васиљевић, Ива Салом, Владимир Челебић, Јованка Гајица, “Софтвер за симулацију размене GOOSE поруке између заштитног релеа и телезаштитног уређаја у подстаници” – М85
http://www.imptelecom.com/media/TehnickaResenja/2015/TR32037-2015A2.pdf

ЈОВАНА НОВАКОВИЋ

2021.

1. Владимир Челебић, Миленко Кабовић, Ива Салом, Анка Кабовић, Јована Новаковић, Горан Димић, " Унапређење мрежних интерфејса централног модула за телезаштитни терминал " – М83
https://www.pupin.rs/code/wp-content/uploads/2022/01/TR-2021-IMP-T-1-M83.pdf

2020.

2. Владимир Челебић, Миленко Кабовић, Ива Салом, Анка Кабовић, Јована Новаковић, Горан Димић, "Нови централни модул за телезаштитни терминал" – М85
http://www.pupin.rs/code/wp-content/uploads/2020/12/TR-2020-IMP-T-2-M85.pdf

2019.

3. Ивана Николић, Бојан Косић, Мина Радивојевић, Јована Новаковић, "Успостављање комуникације између процесорских јединица у асиметричним вишепроцесорским системима" – М85
http://www.imptelecom.com/media/TehnickaResenja/2019/TR32037_2019A4.pdf
4. Владимир Ћатић, Ива Салом, Владимир Челебић, Дејан Тодоровић, Јована Новаковић, Братислав Планић, Вељко Јанић, Марко Ралић, Ивана Николић, Наталија Кокић, "Унапређена акустичка камера за посебне намене" – М84
http://www.imptelecom.com/media/TehnickaResenja/2019/TR32038_2019A1.pdf

2018.

5. Јована Новаковић, Ива Салом, Владимир Челебић, Дејан Тодоровић, Владимир Ћатић, Вељко Јанић, Братислав Планић, "Акустичка камера за посебне намене" – М82
http://www.imptelecom.com/media/TehnickaResenja/2018/TR32038_2018A1.pdf

МИЛЕНКО КАБОВИЋ

2021.

1. Владимир Челебић, Миленко Кабовић, Ива Салом, Анка Кабовић, Јована Новаковић, Горан Димић, " Унапређење мрежних интерфејса централног модула за телезаштитни терминал " – М83
https://www.pupin.rs/code/wp-content/uploads/2022/01/TR-2021-IMP-T-1-M83.pdf

2020.

2. Владимир Челебић, Ива Салом, Миленко Кабовић, Анка Кабовић, Јованка Гајица, Миливоје Ралевић, "Обједињени систем за централизовано надгледање и синхронизацију тачног времена телезаштитних терминала" – М84
http://www.pupin.rs/code/wp-content/uploads/2020/12/TR-2020-IMP-T-1-M84.pdf
3. Владимир Челебић, Миленко Кабовић, Ива Салом, Анка Кабовић, Јована Новаковић, Горан Димић, "Нови централни модул за телезаштитни терминал" – М85
http://www.pupin.rs/code/wp-content/uploads/2020/12/TR-2020-IMP-T-2-M85.pdf
4. Анка Кабовић, Миленко Кабовић, Јованка Гајица, Иван Кокић, Ненад Антонић, Славица Боштјанчич Ракас, Валентина Тимченко, „Систем за динамичко праћење сигурносног растојања проводника на далеководу 110kV бр. 176/3" – М84
http://www.pupin.rs/code/wp-content/uploads/2020/12/TR-2020-IMP-T-3-M84.pdf

2019.

5. Владимир Челебић, Миленко Кабовић, Анка Кабовић, Ива Салом, Јованка Гајица, "Сервер за централизовано надгледање и синхронизацију времена телезаштитних терминала у мрежи ЕМС АД" – М84
http://www.imptelecom.com/media/TehnickaResenja/2019/TR32037_2019A1.pdf
6. Владимир Челебић, Ива Салом, Миленко Кабовић, Анка Кабовић, Јованка Гајица, "Мерне методе за одређивање тачности процеса синхронизације времена на уређају за пренос сигнала телезаштите" – М84
http://www.imptelecom.com/media/TehnickaResenja/2019/TR32037_2019A2.pdf
7. Анка Кабовић, Миленко Кабовић, Јованка Гајица, Славица Боштјанчич Ракас, Валентина Тимченко "Софтвер за краткорочно предвиђање максималног дозвољеног струјног оптерећења далековода" – М85.
http://www.imptelecom.com/media/TehnickaResenja/2019/TR32037_2019A3.pdf

2018.

8. Владимир Челебић, Миленко Кабовић, Анка Кабовић, Ива Салом, Јованка Гајица, "Надоградња система за пренос сигнала телезаштите у мрежи преноса ЕМС АД имплементацијом синхронизације тачног времена" – М84
http://www.imptelecom.com/media/TehnickaResenja/2018/TR32037_2018A1.pdf
9. Владимир Челебић, Миленко Кабовић, Анка Кабовић, Ива Салом, Јованка Гајица, Братислав Планић, "Унапређени телезаштитни терминал TZ-600 за повећање расположивости и убрзање преноса сигнала дистантне заштите за потребе ЈП ЕПС, огранак ХЕ Ђердап" – М84
http://www.imptelecom.com/media/TehnickaResenja/2018/TR32037_2018A2.pdf

2017.

10. Анка Кабовић, Миленко Кабовић, Јованка Гајица, “Апликација за прорачун максималног дозвољеног струјног оптерећења далековода” – М85 http://www.imptelecom.com/media/TehnickaResenja/2017/TR32037_2017A3.pdf

2016.

11. Владимир Челебић, Анка Кабовић, Миленко Кабовић, Јованка Гајица, Ива Салом, Јелена Васиљевић, Драгослав Мијић, “Повезивање телезаштитног терминала на резервни преносни пут преко Етернет интерфејса у мрежи EMC-а” – М84; http://www.imptelecom.com/media/TehnickaResenja/2016/TR32037-2016A2.pdf
12. Владимир Ћатић, Наталија Лукић, Ива Салом, Вукашин Ристић, Миленко Кабовић, Никола Ненадић, Жељко Стојковић, Горан Димић, Ненад Антонић, Бојан Косић, “Систем за аутоматско тестирање хардверских јединица уређаја MIKME у процесу производње” – М81 http://www.imptelecom.com/media/TehnickaResenja/2016/TR32043-2016-M81-IMP-MIKMEATE.pdf
13. Ива Салом, Владимир Челебић, Миленко Кабовић, Наталија Лукић, Владимир Ћатић, Вукашин Ристић, Јованка Гајица, Марко Оклобџија, Ненад Карталовић, Миомир Мијић, “Решење проблема нелинеарности напонски контролисаног појачавача са JFET транзистором” – М85 http://www.imptelecom.com/media/TehnickaResenja/2016/TR32038-2016A1.pdf
14. Ива Салом, Вукашин Ристић, Миленко Кабовић, Владимир Челебић, Жељко Стојковић, Наталија Лукић, Владимир Ћатић, Лазар Бербаков, Бојан Косић, “Алгоритамска компензација разлике компоненти JFET-а за контролу појачања у напонски контролисаном појачавачу” – М85 http://www.imptelecom.com/media/TehnickaResenja/2016/TR32043-2016-M85-IMP-JFET.pdf

2015.

15. Владимир Челебић, Миленко Кабовић, Ива Салом, Јованка Гајица, “Оптички интерфејс ИМП терминала за телезаштиту са мултиплексерском опремом” – М84 http://www.imptelecom.com/media/TehnickaResenja/2015/TR32037-2015A1.pdf
16. Анка Кабовић, Миленко Кабовић, Јелена Васиљевић, Ива Салом, Владимир Челебић, Јованка Гајица, “Софтвер за симулацију размене GOOSE поруке између заштитног релеа и телезаштитног уређаја у подстаници” – М85 http://www.imptelecom.com/media/TehnickaResenja/2015/TR32037-2015A2.pdf

ИНСТИТУТ МИХАЈЛО ПУПИН
ТЕЛЕКОМУНИКАЦИЈЕ д.о.о.
БЕОГРАД
Број 2176/4-21
Датум: 25 NOV 2021 год.

АКЦИОНАРСКО ДРУШТВО
„ЕЛЕКТРОМРЕЖА СРБИЈЕ" БЕОГРАД
Број 500-00-0x0-MAB-262/2021-001
19-11-2021 год.
БЕОГРАД, Кнеза Милоша 11

УГОВОР бр. 204 21

Уговорне стране:
Акционарско друштво „Електромрежа Србије" Београд
улица Кнеза Милоша бр. 11, Београд
кога заступа директор Јелена Матејић, дипл.економиста
(у даљем тексту: Наручилац)

и

ИМП Телекомуникације Д.О.О. Београд
улица Волгина 15, Београд (Звездара), Београд
кога заступа директор Владимир Челебић
(у даљем тексту: Испоручилац)

Уговорне стране сагласно констатују:

- да је Наручилац на основу чл. 61. Закона о јавним набавкама („Сл. Гласник РС", бр. 91/2019) спровео преговарачки поступак без објављивања јавног позива за јавну набавку бр. 204 21 - Унапређење система за пренос сигнала дистантне заштите – Т3600;
- да је Испоручилац доставио понуду број 2176/2-21 од 05.10.2021. године, која се налази у прилогу Уговора и саставни је део овог Уговора;
- да је Наручилац, на основу понуде Испоручиоца и Одлуке о додели уговора бр.700-00-ЈН-174/2021-009 од 21.10.2021. године, изабрао Испоручиоца за испоруку добара која су предмет овог Уговора.

Члан 1.

Предмет овог Уговора је унапређење система за пренос сигнала дистантне заштите – Т3600 односно испорука и пуштање модула у рад (у даљем тексту: опрема), у свему према Понуди Испоручиоца бр. 2176/2-21 од 05.10.2021. године (Прилог 1. Уговора), техничком делу конкурсне документације (Прилог 2. Уговора) и Споразуму о безбедности и здрављу на раду (Прилог 3. Уговора).

Члан 2.

Укупна уговорена вредност предмета угвора из члана 1. овог Уговора износи [redacted] а према јединичним ценама датим у Прилогу 1. овог Уговора.

Цена је исказана без ПДВ и не може се повећавати до краја реализације уговора.

Ценом је обухваћена испорука, уградња и пуштање опреме у рад, као и сви зависни трошкови за извршење предмета Уговора, укључујући, али не ограничавајући се на трошкове дневница, путне трошкове, трошкове боравка и смештаја, трошкове осигурања за ангажовано особље Испоручиоца, као и било који други трошкови из или у вези са извршењем предмета уговора.

Уколико Испоручилац у уговореном року не достави тражену документацију, Наручилац задржава право да раскине уговор и наплати средство финансијског обезбеђења за добро извршење посла.

Члан 14.

Уговор је сачињен у два (2) истоветна примерка, од којих свака уговорна страна задржава по један (1) примерак.

ИСПОРУЧИЛАЦ
ИМП Телекомуникације Д.О.О. Београд

Директор

Владимир Челебић

НАРУЧИЛАЦ
Акционарско друштво
Електромрежа Србије“ Београд

Директор

Јелена Матејић, дипл.економиста