

Upotrebom digitalnih sertifikata do sigurnog pristupa servisima

**Dokument najbolje prakse
(smernice i preporuke)**

Izrađen u okviru AMRES tematske grupe za oblast sigurnost
(AMRES BPD9 106)

Autor: Milica Kovinić
Saradnici: Dušan Pajin, Mara Bukvić, Marko Stojaković,
Ivica Barišić, Bojan Jakovljević

April, 2011

© TERENA 2010. All rights reserved. (Sva prava zadržana.)

Dokument broj: GN3-NA3-T4-AMRES-BDP-106
Verzija / datum: April 2011.
Izvorni jezik : Srpski
Originalni naslov: "Upotrebom digitalnih sertifikata do sigurnog pristupa servisima"
Originalna verzija / datum: Revizija 1 (dokumenta iz septembra 2010.)/ 21. april .2011.
Kontakt: milica.kovinic@rcub.bg.ac.rs, dpajin@rcub.bg.ac.rs

AMRES/RCUB snosi odgovornost za sadržaj ovog dokumenta. U izradi dokumenta učestvovala je tematska grupa za oblast sigurnost organizovana u AMRESu radi sprovođenja zajedničkih aktivnosti na razvoju i širenju dokumenata sa tehničkim smernicama i preporukama za mrežne servise u višokoškolskim obrazovnim i istraživačkim ustanovama u Srbiji.

Delovi dokumenta mogu se slobodno kopirati, nepromenjeni, pod uslovom da je originalni izvor naveden i autorska prava sačuvana.

Dokument je nastao kao rezultat istraživanja koja su finansirana sredstvima Sedmog okvirnog programa Evropske zajednice (FP7/2007-2013) po ugovoru br. 238875, koji se odnosi na projekat „Multi-Gigabit European Research and Education Network and Associated Services (GN3)“.



Sadržaj

Executive Summary	5
Rezime	6
Uvod	7
1 Osnovni pojmovi vezani za sigurnu komunikaciju i PKI	8
2 Kriptografski protokoli i tehnike	11
2.1 Obezbeđivanje tajnosti - sistemi za šifrovanje	11
2.1.1 Sistemi za šifrovanje sa simetričnim ključevima	12
2.1.2 Sistemi za šifrovanje sa asimetričnim ključevima	12
2.1.3 Kombinovani sistemi za šifrovanje	12
2.2 Provera integriteta – Heš funkcije	13
2.3 Provera integriteta sa autentifikacijom – MAC kod	14
2.4 Provera integriteta sa autentifikacijom i neporecivošću - Digitalni potpis	15
2.5 Digitalni sertifikat i infrastruktura javnih ključeva	16
3 Infrastruktura javnih ključeva PKI	18
3.1 PKI - komponente i osnovne funkcije	18
3.1.1 Registracija, proces prijavljivanja institucija/korisnika	19
3.1.2 Inicijalizacija	19
3.1.3 Sertifikacija	19
3.1.4 Opoziv sertifikata	19
3.1.5 Provera lanca poverenja	20
3.1.6 Provera validnosti sertifikata	20
3.2 Format digitalnog sertifikata	20
4 TCS – TERENA Certificate Service	24
4.1 Tipovi sertifikata koje nudi TCS	24
4.2 Prednosti korišćenja TCS sertifikata	25
4.3 Servisi koje je potrebno obezbediti digitalnim sertifikatima	25
4.3.1 Web server	26
4.3.2 RADIUS server	27
4.3.3 Email server	28
4.3.4 Zaštita elektronske pošte	28
5 AMRES usluga izdavanja TCS sertifikata	30

5.1	Registracija institucije	30
5.2	Prijavljivanje za korišćenje TCS servisa	31
5.3	Kreiranje asimetričnog para ključeva i zahteva za potpisivanje sertifikata	31
5.3.1	Linux OpenSSL	32
5.3.2	Microsoft IIS 4.x	36
5.3.3	Microsoft IIS 5.x / 6.x	37
5.4	Podnošenje zahteva	43
6	Instalacija sertifikata	45
6.1.1	Web server pod Linux-om (Apache/mod_ssl)	45
6.1.2	Java Web server (Tomcat, JBoss...)	46
6.1.3	RADIUS server	47
6.1.4	Email na Linux serveru	48
6.1.5	Microsoft IIS 5.x i 6.x	48
7	Reference	55
8	Rečnik	56

Executive Summary

This document promotes the adoption of digital certificate in AMRES high education and research community.

In order to establish secure communication, users must be sure that they are indeed accessing to the resources which they are intended to access and that no one can read and/or change data that is sent or received between users and resources. The use of digital certificates in conjunction with SSL technology provides us such type of security.

Document outlines the components of PKI infrastructure, and also the implementation of PKI functions in the case of AMRES association in TCS (TERENA Certificate Service) service. Different needs for using PKI in NREN are also induced, they require different types of digital certificates, and special attention is paid to the use of PKI infrastructure and digital certificates in combination with SSL technology for the purpose of mutual authentication of services and their users.

The document explains the procedure of obtaining a server certificate - key generation, creation of certificates, preparation and submission of the request for signing a server certificate. The final part of the document contains the instructions for installing digital certificates on Linux servers.

Rezime

Dokument promoviše usvajanje digitalnih sertifikata u institucijama članicama Akademske mreže Srbije kao načina za uspostavljanje sigurnih kanala komunikacije.

Da bi korisnici prilikom preuzimanja ili slanja podataka na neki server imali zaštićenu komunikaciju, moraju biti sigurni da su zaista pristupili onom serveru kojem su imali nameru da pristupe i da niko ne može pročitati i/ili promeniti podatke koji se šalju ili primaju. Upotreba digitalnih sertifikata u kombinaciji sa SSL tehnologijom omogućava pomenutu sigurnost.

Opisane su komponente PKI infrastrukture, ali i način realizacije PKI funkcija na primeru uključivanja AMRES-a u TCS (*TERENA Certificate Service*) servis. Navedene su i različite potrebe za korišćenjem PKI u NREN-u, koje zahtevaju različite tipove digitalnih sertifikata, ali je posebna pažnja posvećena korišćenju PKI infrastrukture, odnosno digitalnih sertifikata u kombinaciji sa SSL tehnologijom u svrhu međusobne autentifikacije servisa i njihovih korisnika.

U dokumentu je objašnjen postupak pribavljanja serverskog sertifikata – generisanje ključa, formiranje sertifikata, priprema za/i podnošenje zahteva za potpisivanje serverskog sertifikata. U završnom delu dokumenta nalaze se uputstva za instalaciju digitalnih sertifikata na Linux serverima.

Uvod

Razvoj elektronskih komunikacija doveo je do toga da se razmena informacija poverljive sadržine odvija svakodnevno. Da bi korisnici prilikom pristupa web, mail ili RADIUS serverima preuzeli ili dali na uvid osetljive podatke (npr. korisnička imena) moraju biti sigurni da su pristupili pravom serveru te da je komunikacija sa serverom sigurna, da niko ne može da presretne/pročita i/ili promeni podatke. Korišćenje SSL tehnologije na serverima (HTTPS, POP3S i sl.) omogućava traženu sigurnost, ali zahteva da serveri imaju odgovarajuće digitalne sertifikate.

AMRES omogućava izdavanje serverskih SSL sertifikata u saradnji sa TERENA-om, a preko servisa *TERENA Certificate Service* (TCS). Servis je besplatan za sve institucije članice AMRES-a.

Svrha dokumenta je da promoviše upotrebu serverskih sertifikata koji omogućavaju uspostavljanje sigurnijih kanala komunikacije. Dokument je namenjen IT administratorima u institucijama članicama AMRES-a.

U prvom delu su date definicije termina i pojmova, kriptografskih sistema, protokola i tehnika vezanih za upotrebu digitalnih sertifikata i infrastrukture javnih ključeva. Opisan je format i tipovi digitalnih sertifikata za različite potrebe u NREN-u (Akademske mreži).

U drugom delu dokumenta, objašnjen je postupak pribavljanja serverskog sertifikata – generisanje ključa, formiranje sertifikata, priprema za/ i podnošenje zahteva za potpisivanje serverskog sertifikata. U završnom delu dokumenta nalaze se uputstva za instalaciju digitalnih sertifikata na Linux serverima.

1 Osnovni pojmovi vezani za sigurnu komunikaciju i PKI

U ovom dokumentu se koriste tehnički termini iz oblasti sigurnosti, vezani za upotrebu infrastrukture javnih ključeva radi omogućavanja bezbedne komunikacije u računarskim mrežama. Da bi se olakšalo razumevanje dokumenta, definicije najvažnijih pojmova su izdvojene i navedene u nastavku.

Računarska sigurnost (*computer security*) se bazira na poverljivosti (*confidentiality*), integritetu (*integrity*) i dostupnosti (*availability*) podataka, dok bezbedna komunikacija podrazumeva očuvanje tajnosti (*confidentiality*), integriteta (*integrity*) i autentifikaciju sa neporecivošću (*authentication with non-repudiation*).

- **Autentifikacija (*Authentication*)** je proces u kome se dokazuju identiteti krajnjih učesnika u komunikaciji (npr. korišćenjem digitalnih potpisa).
- **Integritet (*Integrity*)** podataka garantuje da nije došlo do izmene podataka ili sadržaja poruke na njenom putu od izvora do odredišta, najčešće tako što se generiše *heš (hash)* poruke (niz bita fiksne dužine) koji se zajedno sa njom šalje. Na prijemu se istim algoritmom korišćenim pri slanju poruke formira heš i poredi sa hešom koji je primljen uz poruku. Ako se te dve vrednosti ne poklapaju znači da je došlo do izmene originalnog sadržaja poruke.
- **Tajnost ili poverljivost (*Confidentiality*)** podataka omogućava da podatak ili sadržaj poruke bude dostupan samo onome kome je poruka i namenjena, što se postiže šifrovanjem.
- **Neporicanje (*Non-repudiation*)** onemogućava da onaj ko je poslao poruku kasnije tvrdi da je nije poslao. Kada pošiljalac potpiše poruku svojim digitalnim potpisom, zna se da je on koristio svoj privatni ključ kako bi formirao digitalni potpis. Kako samo pošiljalac ima pristup svom privatnom ključu to znači da je samo on mogao da pošalje odgovarajuću digitalno potpisanu poruku.

Kriptografskim ključevima nazivaju se:

- **Asimetrični par ključeva (*Key Pair*)** – čine privatni i javni ključ, kao matematički par koji se koriste za potrebe rada asimetričnog kriptografskog algoritma, kao što je na primer RSA algoritam. Poruku šifrovanu javnim ključem može da pročita samo vlasnik privatnog ključa, dok poruku šifrovanu privatnim ključem mogu da pročitaju svi kojima je poznat javni ključ.
- **Privatni ključ (*Private Key*)** – matematički podatak koji može da se koristi za kreiranje elektronskog potpisa ili za dešifrovanje dokumenta koji je šifrovan, primenom asimetričnog kriptografskog algoritma,

da bude dostupan samo vlasniku privatnog ključa. Privatni ključ je tajni podatak, dostupan samo njegovom vlasniku.

- **Javni ključ (*Public Key*)** – matematički podatak koji može biti javno objavljen (najčešće se objavljuje u formi X.509v3 elektronskog sertifikata). Koristi se za verifikaciju elektronskog potpisa, kreiranog pomoću odgovarajućeg privatnog ključa koji je matematički par sa datim javnim ključem, kao i za šifrovanje podataka za korisnika koji poseduje odgovarajući privatni ključ.
- **Deljeni tajni ključ (*Shared Secret Key*)** – matematički podatak koji se koristi za šifrovanje i dešifrovanje dokumenta koji je šifrovan primenom simetričnog kriptografskog algoritma. Takođe se koriste i termini simetrični ključ ili samo tajni ključ.

Infrastrukturu javnih ključeva (PKI - *Public Key Infrastructure*) čine hardver, softver, polise i procedure koje su neophodne za upravljanje, generisanje, skladištenje i distribuciju kriptografskih ključeva i digitalnih sertifikata. PKI je sigurnosna infrastrukturu čije su usluge implementirane uz pomoć koncepata sistema za enkripciju koji koriste asimetrične algoritme. U vezi sa PKI infrastrukturom koriste se sledeće definicije:

- **Sertifikaciono telo (CA – *Certification Authority*)** – Pravno lice koje izdaje digitalne sertifikate.
- **Registraciono telo (RA – *Registration Authority*)** – Entitet koji je odgovoran za inicijalnu identifikaciju i proveru podataka o korisniku/vlasniku sertifikata, ali koje ne izdaje i ne potpisuje sertifikat. RA je delegirano od CA da vrši odgovarajuće poslove vezane za proveru identiteta krajnjih korisnika.
- **Digitalni sertifikat** – Elektronski dokument koji potvrđuje da javni ključ pripada određenom entitetu (RFC 5280). Koristi se i naziv elektronski sertifikat.
- **CA sertifikat** – Sertifikat samog sertifikacionog tela. Potvrđuje da je CA upravo ono CA koje tvrdi da je. Može biti samopotpisan (kada je CA ujedno i koreno sertifikaciono telo - *Root CA*) ili biti izdat (digitalno potpisan) od strane drugog sertifikacionog tela – izdavaoca sertifikata.
- **Lanac sertifikata (*Certificate chain*)** – Uređena sekvenca sertifikata koja se, zajedno sa javnim ključem inicijalnog objektu u lancu, procesira u cilju provere istog u poslednjem objektu u lancu. Formira hijerarhijski lanac poverenja, gde jedan digitalni sertifikat potvrđuje autentičnost prethodnog digitalnog sertifikata.
- **Politika sertifikacije (CP – *Certificate Policy*)** – Imenovan skup pravila koji definiše primenljivost sertifikata na određeno okruženje i/ili na klasu aplikacija sa zajedničkim bezbednosnim zahtevima.
- **Praktična pravila rada sertifikacionog tela (CPS - *Certificate Practice Statement*)** – Javna praktična pravila i procedure koje sertifikaciono telo primenjuje u proceduri izdavanja sertifikata.
- **Treća strana** – Primalac sertifikata koji prihvata sertifikat i proverava njegovu validnost. Pored toga, proverava digitalni potpis elektronskih dokumenata koja su potpisana sertifikatom koristeći javni ključ vlasnika sertifikata koji se nalazi u samom sertifikatu. U cilju provere validnosti digitalnog sertifikata, treća strana mora da proveri status opozvanosti sertifikata proverom odgovarajuće CRL liste.
- **Potpisnik** – Entitet koji poseduje sredstvo za elektronsko potpisivanje i vrši elektronsko potpisivanje u svoje ime. To može biti fizičko lice ili entitet u pravnom licu kojem je izdat digitalni sertifikat.
- **Korisnik (krajnji entitet, vlasnik sertifikata)** – fizičko lice ili entitet u pravnom licu kojem se izdaje digitalni sertifikat. Fizička lica su krajni korisnici. Pravna lica su institucije, koje digitalne sertifikate potražuju za svoje entitete, najčešće za svoje servere ili servise.
- **Lični korisnički sertifikat (personalni ili klijentski sertifikat)** – elektronski sertifikat izdat fizičkom licu, odnosno krajnjem korisniku radi potvrde njegovog identiteta i za bezbedno slanje elektronske pošte (digitalno potpisivanje mejlova i enkripcija njihovog sadržaja). Sadrži podatke koje identifikuju to lice, kao što su korisničko ime u okviru federacije identiteta, puno ime korisnika, e-mail adresa.

- **Serverski sertifikat – elektronski sertifikat izdat pravnom licu**, odnosno instituciji za potvrdu identiteta servera ili servisa u njegovom vlasništvu. Sadrži podatke koje identifikuju servis, najčešće jednoznačni DNS naziv servera.
- **Zahtev za dobijanje sertifikata (CSR – Certificate Service Request)** – Standardni format (po PKCS #10 preporuci) koji se koristi za slanje zahteva za dobijanje sertifikata.
- **Sertifikacija** – process izdavanja digitalnog sertifikata.
- **Serijski broj sertifikata** – Pridruženi broj sertifikatu koji jedinstveno identifikuje sertifikat u domenu datog CA.
- **Lista opozvanih sertifikata (CRL – Certificate Revocation List)** – Lista izdata i elektronski potpisana od strane CA koja sadrži serijske brojeve opozvanih sertifikata i vreme kada je opoziv izvršen. Takva lista se mora uzeti u obzir prilikom provere validnosti sertifikata.
- **Opoziv sertifikata** – Trajno ukidanje validnosti datog sertifikata i njegovo smeštanje na CRL listu.
- **Repozitorijum** – Baza podataka i/ili direktorijum na kome su objavljeni osnovni dokumenti rada CA, kao i eventualne druge informacije koje se odnose na pružanje sertifikacionih usluga od strane datog CA (kao na primer objavljivanje svih izdatih sertifikata...).
- **PKCS (Public-Key Cryptography Standards)** – Obuhvata grupu standarda za kriptografiju sa javnim ključevima. Definisali su ih RSA Laboratories.

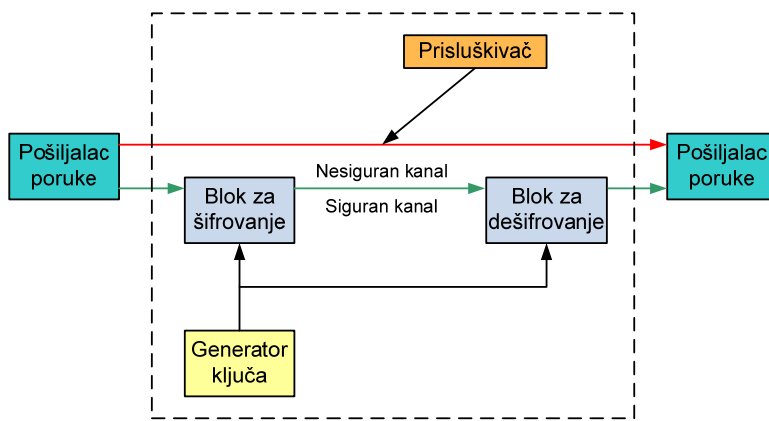
2 Kriptografski protokoli i tehnike

U ovom poglavlju je opisano na koji način se obezbeđuje sigurna komunikacija kroz računarske mreže, odnosno kako se postiže tajnost komunikacije, očuvanje integriteta i autentifikacija učesnika u komunikaciji.

2.1 Obezbeđivanje tajnosti - sistemi za šifrovanje

Samo učesnici u komunikaciji (pošiljalac i primalac) bi trebalo da razumeju komunikaciju u kojoj je očuvana tajnost ili poverljivost. Tajnost komunikacije postiže se šifrovanjem (enkripcijom) poruka.

Na slici 1 je prikazana opšta blok šema sistema za šifrovanje. Sistem za šifrovanje se sastoji od bloka za šifrovanje, bloka za dešifrovanje, generatora ključa i skupa poruka koje oni emituju. U bloku za šifrovanje se primenjuje matematička funkcija (algoritam za šifrovanje) koja transformiše skup poruka koje se prenose u neprepoznatljiv oblik. Algoritam za šifrovanje se primenjuje na originalnu poruku u kombinaciji sa ključem, koji predstavlja niz simbola čiji je zadatak da dodatno doprinese promeni izvorne poruke. Ključ je nezavisan od izvorne poruke i od same funkcije i generiše se u generatoru ključa. Algoritam za šifrovanje može se smatrati sigurnim ukoliko sigurnost šifrovane poruke zavisi samo od tajnosti ključa, ali ne i od tajnosti algoritma. Ovako izmenjena (šifrovana) poruka se potom šalje preko nesigurnog telekomunikacionog kanala ka odredištu. Poruku u kanalu može presresti prislušivač u cilju dobijanja koristi bilo kroz samu informaciju koju poruka sadrži ili kroz izmenu originalne poruke i podmetanja lažne informacije.



Slika 1 Opšta blok šema sistema za šifrovanje

2.1.1 Sistemi za šifrovanje sa simetričnim ključevima

Sistemi za šifrovanje sa simetričnim ključevima (algoritmi simetrične kriptografije) predstavljaju sisteme kod kojih su ključ za šifrovanje i dešifrovanje isti, pa je neophodno da se pošiljalac i primalac unapred dogovore o vrednosti ključeva koji će se koristiti za enkripciju/dekripciju podataka. Ovde se javlja problem distribucije i skalabilnosti simetričnog (deljenog) ključa.

Algoritmi simetrične kriptografije obezbeđuju tajnost komunikacije, ali ne omogućavaju ni proveru integriteta poruke ni autentifikaciju njenog pošiljaoca.

2.1.2 Sistemi za šifrovanje sa asimetričnim ključevima

Rešavanje problema skalabilnosti i distribucije ključeva između učesnika u komunikaciji dovelo je do pojave sistema sa asimetričnim ključevima (algoritmi asimetrične kriptografije). U ovim sistemima svaka strana poseduje par ključeva, privatni i javni ključ, pri čemu, podaci šifrovani javnim ključem dešifruju se privatnim, i obrnuto. Privatni ključ je tajni i poseduje ga samo njegov vlasnik, dok je javni ključ dostupan svima. Ovi ključevi se generišu tako da iako su matematički povezani, računarski je neisplativo (u razumnom vremenskom periodu) pronalaženje privatnog ključa iz poznatog javnog. Privatni ključ se nikada ne prenosi nesigurnim kanalom.

Korišćenje sistema sa asimetričnim ključevima obezbeđuje ne samo poverljivost podataka i tajnost komunikacije, već i autentifikaciju pošiljaoca.

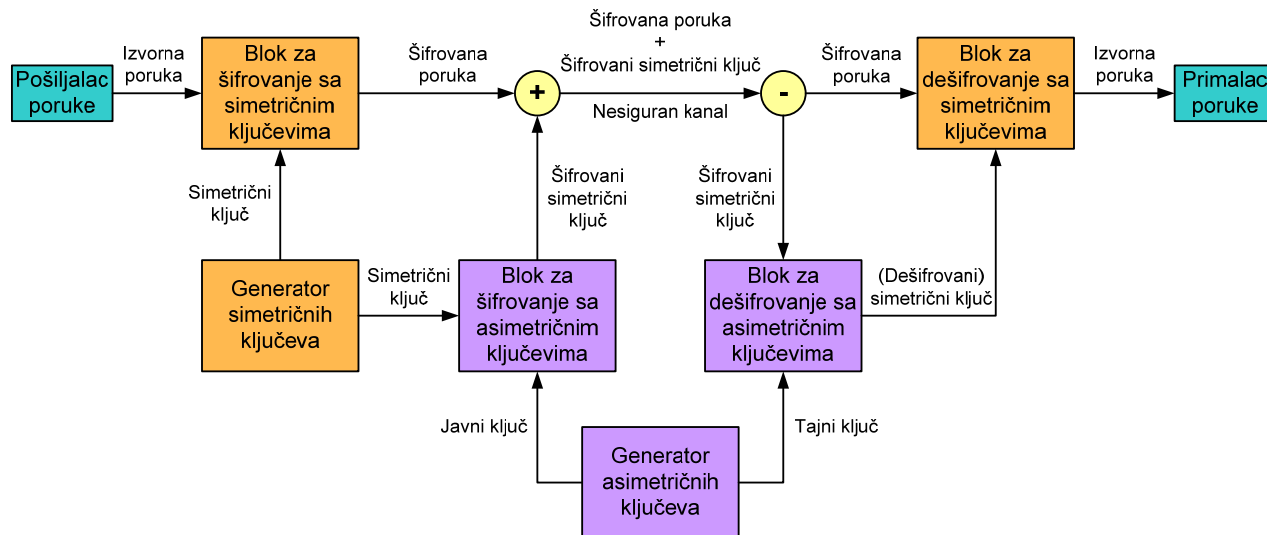
Poverljivost podataka se obezbeđuje tako što pošiljalac vrši enkripciju koristeći javni ključ primaoca. Na taj način samo onaj kome je poruka namenjena može da je dešifruje jer samo on poseduje odgovarajući privatni ključ.

Kako bi se obezbedila autentifikacija, pošiljalac vrši enkripciju podataka koje šalje svojim privatnim ključem. Kada primalac primi poruku, vrši njenu dekripciju javnim ključem pošiljaoca. Na taj način primalac je siguran da je poruku poslao samo onaj ko ima odgovarajući privatni ključ. Ovaj postupak leži u osnovi digitalnog potpisa.

2.1.3 Kombinovani sistemi za šifrovanje

Kombinovanjem sistema za šifrovanje sa simetričnim i asimetričnim ključevima na odgovarajući način, dobijaju se kombinovani sistemi za šifrovanje koji objedinjuje njihove najbolje osobine. Algoritmi simetrične kriptografije su jednostavniji pa omogućavaju veće brzine rada koristeći ključeve manjih veličina dok se skalabilnost i distribucija ključeva realizuju korišćenjem algoritama asimetrične kriptografije koji su složeniji i zahtevaju duže vreme obrade.

Na slici 3 je prikazana blok šema kombinovanog sistema za šifrovanje.



Slika 3 Blok šema kombinovanih sistema za šifrovanje

2.2 Provera integriteta – Heš funkcije

Primalac mora biti siguran da je primljena poruka upravo onakva kakva je bila poslata. To utvrđuje proverom integriteta poruke. Jednosmerna heš funkcija je kriptografska tehnika koja se koristi u svrhu provere integriteta poruke i kao gradivna celina čini deo mnogih sigurnosnih protokola.

Primenom kriptografske heš funkcije na blok podataka proizvoljne dužine dobija se niz bita fiksne dužine koji se naziva heš vrednost poruke (*hash value, message digest, digest*). Osnovna karakteristika heš funkcije je da i najmanja promena u originalnoj poruci dovodi do promene njene heš vrednosti.

Idealna kriptografska heš funkcija treba da poseduje sledeće karakteristike:

- izračunavanje heš vrednosti neke poruke je jednostavno
- nemoguće je (u konačnom broju koraka) pronaći poruku koja ima datu heš vrednost. Algoritmi koji imaju ovakvu osobinu nazivaju se jednosmerni (*one-way*)
- ako je poznata poruka m , nemoguće je (u konačnom broju koraka) pronaći drugu poruku m' tako da se njihove heš vrednosti poklapaju (*weak collision resistance*)
- nemoguće je (u konačnom broju koraka) pronaći dve različite poruke koje imaju istu heš vrednost (*strong collision resistance*)

Kriptografske heš funkcije se koriste kako bi se potvrdio integritet podataka koji se prenose nesigurnim kanalom.

U tabeli 1 je data lista heš funkcija koje su u upotrebi, i (uz naziv algoritma navedene su dužine njihovih heš vrednosti). Što je dužina heša veća, algoritam je otporniji na razne vrste napada provale i time pruža veću sigurnost.

Naziv algoritma	Dužina heša
GOST	256 bita
HAS-160	160 bita
HAVAL	128-256 bita
MD2	128 bita
MD4	128 bita
MD5	128 bita
RadioGatun	Do 1216 bita
RIPEND-64	64 bita
RIPEND-160	160 bita
RIPEND-320	320 bita
SHA-1	160 bita
SHA-224	224 bita
SHA-256	256 bita
SHA-384	384 bita
SHA-512	512 bita
Skein	256, 512, 1024 bita
Snefru	128, 256 bita
Tiger	192 bita
Whirlpool	512 bita
FSB	160-512 bita
ECOH	224-512 bita
SWIFFT	512 bita

Tabela 1 Heš funkcije

2.3 Provera integriteta sa autentifikacijom – MAC kod

MAC (*Message Authentication Code*) kod ili kod za autentifikaciju poruke u osnovi ima osobine heš funkcija, uz dodatak deljenog ključa, kojim se, pored provere integriteta poruke, omogućava i autentifikacija pošiljaoca. MAC, slično kao i heš, predstavlja niz bita fiksne dužine koji se dobija tako što se na poruku i tajni ključ, koji poseduju obe strane u komunikaciji, primeni MAC algoritam. Upotreba ključa omogućava da samo onaj ko ima identičan ključ može proveriti heš funkciju. Tako vlasnik poruke/datoteke može da potvrdi njenu autentičnost ako želi da bude siguran da datoteka nije izmenjena usled napada (aktivnosti virusa i sl.), a sa druge strane, primalac poruke može da autentifikuje njenog pošiljaoca.

Postoje dve kategorije MAC koda u zavisnosti od tipa algoritma koji se koristi:

- **HMAC** (*Hash-based Message Authentication Code*) – nastaje kada se primeni neki od poznatih heš algoritama u realizaciji MAC algoritma (HMAC-MD5, HMAC-SHA1),
- **CMAC** (*Cipher-based Message Authentication Code*) – nastaje kada se primeni ulančani simetrični blokovski algoritmi (*symmetric block cipher in a cipher block chaining mode*).

Heš i MAC vrednost poruke omogućavaju proveru njenog integriteta, pri čemu MAC omogućava i autentifikaciju pošiljaoca poruke. Međutim, ni MAC ni heš ne pružaju zaštitu sa neporecivošću, odnosno da

onaj ko je poslao poruku kasnije ne može da tvrdi da je nije poslao ili da je neko drugi poslao umesto njega. Kako bi se obezbedila zaštita sa neporecivošću koristi se digitalni potpis.

2.4 Provera integriteta sa autentifikacijom i neporecivošću - Digitalni potpis

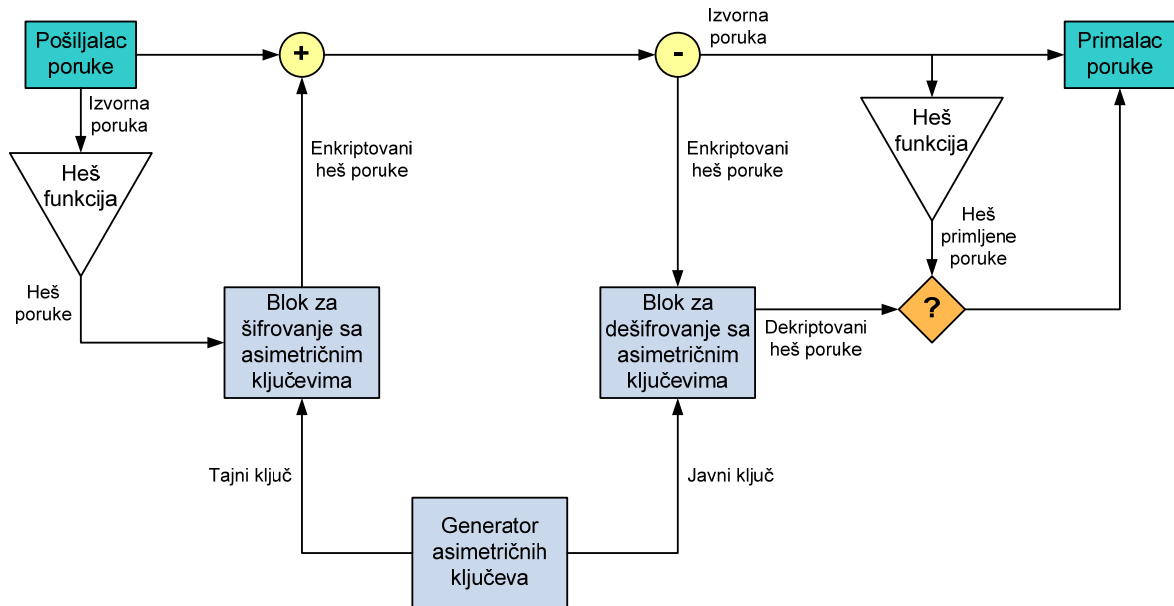
Autentifikacija sa neporecivošću obezbeđuje da su učesnici u komunikaciju upravo oni koji tvrde da su to. Algoritmi za šifrovanje sa asimetričnim ključem mogu obezbediti proveru integriteta i ideniteta (autentifikaciju) upotrebom digitalnih potpisa.

Digitalni potpis elektronskih podataka može da se posmatra u analogiji sa potpisom ili pečatom štampanih dokumenta. On omogućava da primalac poruke bude siguran da nije došlo do izmene originalnog sadržaja poruke, kao i da bude siguran u identitet pošiljaoca poruke. Drugim rečima, garantuje integritet poruke i identit/autentifikaciju pošiljaoca iste. Pored toga, digitalni potpis ne može da se porekne, tako da onaj ko je poslao poruku kasnije ne može da tvrdi da je nije poslao ili da je neko drugi poslao umesto njega.

Digitalni potpis poruke se formira korišćenjem tehnike asimetričnih ključeva. Pošiljalac kreira heš (šifrovani sažetak poruke) tako što na originalnu poruku primenjuje heš algoritam. Heš poruke predstavlja „digitalni otisak prsta“ poruke. Ako bi došlo do najmanje promene u originalnoj poruci, promenio bi se i rezultujući heš poruke. Pošiljalac zatim vrši enkripciju heša svojim privatnim ključem. Ovako enkriptovan heš predstavlja digitalni potpis poruke.

Pošiljalac dodaje na kraj originalne poruke i njen digitalni potpis i tako digitalno potpisanu poruku šalje. Na prijemu, primalac pomoću javnog ključa pošiljaoca vrši dešifrovanje digitalnog potpisa poruke kako bi dobio heš poslate poruke i poredi ga sa vrednošću heša koji on dobija primenjujući isti heš algoritam na samu primljenu poruku. Ako se dobijene heš vrednosti ne razlikuju primalac može da bude siguran da poruka nije izmenjena. Ako se vrednosti razlikuju znači da je došlo do neovlašćenog menjanja sadržaja poruke i/ili da je neko drugi poslao poruku od onog za koga se izdaje.

Na slici 4 je prikazana blok šema sistema sa digitalnim potpisom.



Slika 4 Blok šema sistema sa digitalnim potpisom

2.5 Digitalni sertifikat i infrastruktura javnih ključeva

Pri korišćenju tehnike asimetrične kriptografije, bilo za obezbeđivanje poverljivosti informacije šifrovanjem ili primenom digitalnog potpisa za autentifikaciji pošiljaoca i obezbeđivanja integriteta, javlja se problem autentifikacije samog para asimetričnih ključeva. Osnovno pitanje koje se postavlja je kako se može garantovati da javni ključ stvarno pripada onoj osobi za koju mi verujemo da pripada. Potencijalni napadač može da podmentne svoj javni ključ kako bi čitao poruke namenjene nekom drugom ili da naruši integritet poruke potpisivanjem iste svojim privatnim ključem. Ovaj problem rešavaju digitalni sertifikati i infrastruktura javnih ključeva.

Digitalni sertifikati (*Public Key Certificate - PKC*) omogućavaju potvrdu identiteta učesnika u elektronskoj komunikaciji, slično kao što to čine lične karte u međuljudskim interakcijama. On povezuje podatke o identitetu učesnika u komunikaciji sa parom asimetričnih ključeva koji se koriste za enkripciju i potpisivanje digitalne informacije čime potvrđuje nečije pravo na korišćenje para kriptografskih ključeva. Dakle, potvrđuje se da određeni javni ključ pripada određenom krajnjem entitetu (krajnjem korisniku, ali i korisničkom serveru). Na taj način se sprečava zloupotreba ključeva i da se neko neovlašćeno predstavlja tuđim identitetom.

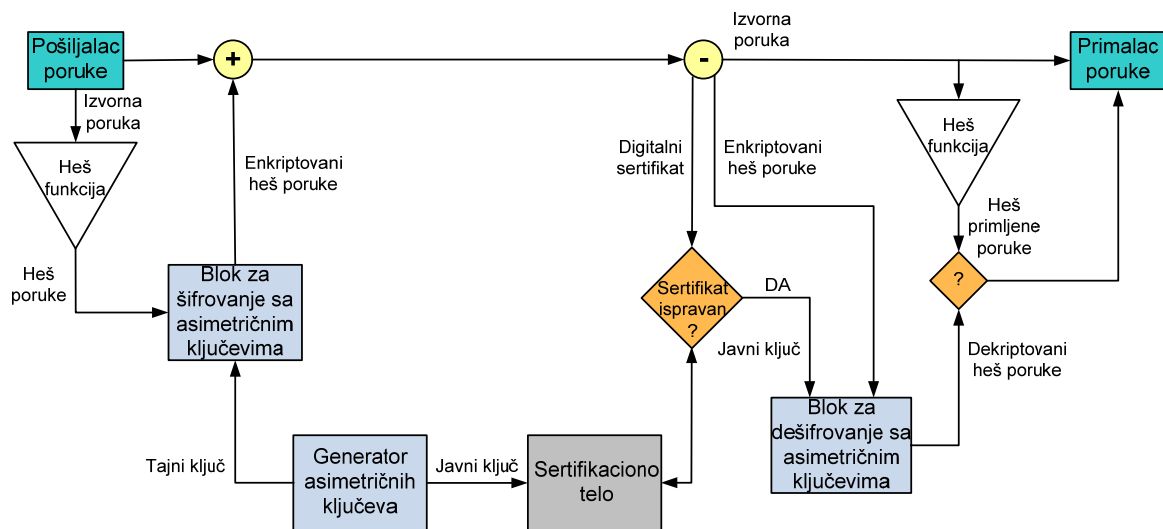
Informacija u digitalnom sertifikatu je digitalno potpisana i na taj način potvrđena od strane sertifikacionog tela (CA – Certification Authority). Sertifikaciono telo je zaduženo za izdavanje sertifikata i predstavlja neosporan autoritet kome veruju svi učesnici u komunikaciji. Koncept koji objedinjuje korišćenje digitalnih sertifikata i ulogu sertifikacionih tela naziva se infrastruktura javnih ključeva i objašnjen je u sledećem poglavlju.

Digitalni sertifikat sadrži podatke o vlasniku/krajnjem entitetu sertifikata, javni ključ vlasnika/krajnjeg entiteta sertifikata, period važenja sertifikata, ime izdavača (sertifikaciono telo koje je izdalo sertifikat), serijski broj sertifikata, digitalni potpis izdavača.

Najčešće korišćen format digitalnog sertifikata je definisan ITU-T X.509 standardom, verzija 3. Može se čuvati odvojeno od privatnog ključa (PEM format), ili se može čuvati spojen sa privatnim ključem u različitim formatima (npr. PKCS #12, JKS, ...).

Pri slanju poruke pošiljalac digitalno potpisuje poruku i uz nju šalje i svoj digitalni sertifikat kako bi primalac mogao da bude siguran u identitet pošiljaoca. Uz poruku može da bude poslato i više digitalnih sertifikata koji formiraju lanac sertifikata, odnosno hijerarhijski lanac poverenja, gde jedan digitalni sertifikat potvrđuje autentičnost prethodnog digitalnog sertifikata. Na samom vrhu u hijerarhiji poverenja nalazi se *root (top-level)* sertifikaciono telo tzv. koreno sertifikaciono telo, kome veruju sva ostala sertifikaciona tela. Javni ključ *root* sertifikacionog tela mora da bude javno poznat i dostupan. Dodatak A sadrži prikaz jednog takvog lanca poverenja uspostavljenog na realnom primeru lanca CA sertifikata za TCS servis.

Na slici 5 je prikazana blok šema sistema sa digitalnim sertifikatima.



Slika 5 Blok šema sistema sa digitalnim sertifikatima

3 Infrastruktura javnih ključeva PKI

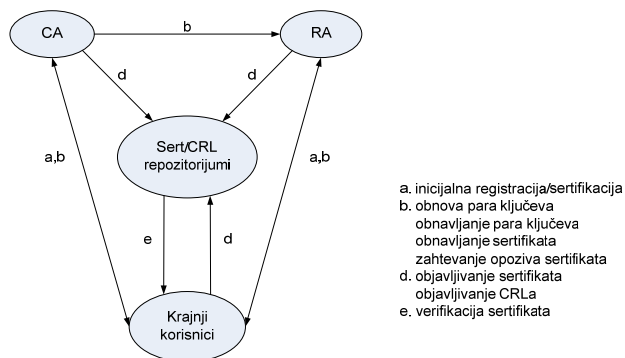
Infrastruktura javnih ključeva (PKI – *Public Key Infrastructure*) čine hardver, softver, polise i procedure koje su neophodne za upravljanje, generisanje, skladištenje i distribuciju kriptografskih ključeva i digitalnih sertifikata. Ona definiše model za sveobuhvatnu sigurnosnu infrastrukturu čije su usluge implementirane uz pomoć koncepata sistema za enkripciju koji koriste asimetrične algoritme.

Infrastruktura javnih ključeva definisana je standardom ITU-T X.509. Prati ga IETF dokument RFC 5280, u kome su definisane jasnije preporuke za Internet zajednicu.

3.1 PKI - komponente i osnovne funkcije

Infrastrukturu javnih ključeva čine hardver, softver, polise i procedure koje su neophodne za upravljanje, generisanje, skladištenje, distribuciju, korišćenje i povlačenje kriptografskih ključeva i digitalnih sertifikata.

Na slici 6 je prikazana međusobna povezanost osnovnih PKI elemenata.



Slika 6 Odnosi PKI elemenata

Upravljanje, generisanje, skladištenje i distribucija kriptografskih ključeva i digitalnih sertifikata se odvija kroz **Sertifikaciona (CA) i Registraciona (RA) tela**.

Učesnici u komunikaciji, koji međusobno nemaju uspostavljen lanac poverenja, veruju trećoj strani - Sertifikacionom telu CA. CA kao autoritativno telo kome se veruje, ima kapacitet da izdaje i povlači digitalne

sertifikate (*Public Key Certificate* - PKC). CA, pre izdavanja sertifikata, vrši potpunu proveru podataka o vlasniku/krajnjem entitetu za koga je podnet zahtev za izdavanje sertifikata. Ove provere CA može da vrši direktno ili posredstvom jednog ili više RA. Posle uspešne provere, CA izdaje digitalni sertifikat njegovom vlasniku/krajnjem entitetu. Izdati sertifikat garantuje da javni ključ pripada tom vlasniku/krajnjem entitetu. Krajnji entitet može biti krajnji korisnik (fizičko lice) ili server, a digitalni sertifikat može da veže javni ključ za identitet ili DNS-zapis krajnjeg entiteta. Digitalni sertifikat izdat krajnjem korisniku garantuje njegov identitet, a potpisan je digitalnim sertifikatom samog Sertifikacionog tela. Krajnji korisnici sada koriste svoje digitalne sertifikate, izdate od strane Sertifikacionog tela kome veruju, kako bi dokazali svoj identitet jedan drugom i uspostavili sigurnu komunikaciju.

Digitalni sertifikati se izdaju i fizičkim i pravnim licima. Fizičkim licima (krajnjim korisnicima) se izdaju lični sertifikati. Pravnim licima tj. institucijama se izdaju sertifikati za krajnje entitete u njihovom vlasništvu, a to su najčešće serverski SSL sertifikati za korisničke servere (web, mail, radius i sl.).

3.1.1 Registracija, proces prijavljivanja institucija/korisnika

Da bi koristili usluge infrastrukture javnih ključeva, institucije/krajnji korisnici prvo moraju da prođu proces prijavljivanja koji obuhvata proveru njihovog identiteta i razmenu informacija sa za to zaduženom komponentom infrastrukture **Registracionim telom (RA)**. Prvi korak u procesu prijavljivanja je registracija, koja podrazumeva proveru identiteta krajnjeg entiteta koji podnosi zahtev za sertifikatom. Registracija za krajnjeg korisnika znači proveru identiteta krajnjeg korisnika koji podnosi zahtev za sertifikatom. U slučaju institucija, sertifikat se izdaje njenim korisničkim serverima. Zato za institucije postoji faza predregistracije u kojoj se proveravaju podaci o instituciji i dostavljaju se imena osoba (u proceduri imenovanja predstavnika institucije) koje će biti ovlašćene da podnose zahtev za sertifikatom za potrebe te institucije. Nivo provere identiteta krajnjeg korisnika ili institucije zavisi od tipa sertifikata za koji se podnosi zahtev (sertifikati koji se koriste kako bi obezbedili elektronske transakcije novca zahtevaju stroži nivo provere od ostalih tipova sertifikata). Za svaki tip sertifikata je definisan odgovarajući nivo provere, dokumentom koji se naziva **politika sertifikacije**.

3.1.2 Inicijalizacija

Inicijalizacije je sledeći korak u registraciji u okviru koga predstavnik institucije/krajnji korisnik i sertifikaciono telo razmenjuju neophodne informacije za dalju komunikaciju: kako će se odvijati sama komunikacija, kako će se distribuirati sertifikati, na koji način se uspostavlja sigurna komunikacija između predstavnika institucije/krajnjih korisnika i sertifikacionog tela, kako se generiše i dostavlja par asimetričnih ključeva, itd.

3.1.3 Sertifikacija

Sertifikacija obuhvata proces izdavanja i dostavljanja sertifikata predstavnicima institucija/krajnjim korisnicima i obavlja je CA.

3.1.4 Opoziv sertifikata

Iako je period važenja digitalnog sertifikata definisan datumima u odgovarajućim polja samog sertifikata dešava se da dođe do kompromitovanja tajnog ključa ili promene nekog od osnovnih ličnih podataka koji se nalaze u

sertifikatu što ima za posledicu opozivanje sertifikata, odnosno njegovo povlačenje iz upotrebe. Opozvani sertifikati se objavljuju preko lista opozvanih sertifikata (**Certificate Revocation List - CRL**) koje objavljuje sertifikaciono telo koje je izdalo sertifikat. Koristeći **Repozitorijum** – bazu podataka i/ili direktorijum sa osnovnim dokumentima rada CA, CA objavljuje i eventualne druge informacije koje se odnose na pružanje sertifikacionih usluga od strane datog CA (kao na primer objavljivanje svih izdatih sertifikata, ...).

U nekim slučajevima, umesto lista opozvanih sertifikata, se koriste protokoli za proveru stanja sertifikata u realnom vremenu koji daju pozitivan ili negativan odgovor o statusu sertifikata. Primer takvog protokola je OSCP – *Online Certificate Status Protocol*.

Primalac sertifikata je svakako dužan da proveri sertifikat, pre nego što ga prihvati. Provere sertifikata nije jednostavan proces, jer potpisnik poruke može umesto jednog vlastitog sertifikata dati lanac sertifikata, u kome je svaki sertifikat potpisan sertifikatom nadređenog CA. To podrazumeva proveru lanca poverenja i validnosti svakog sertifikata u tom lancu.

3.1.5 Provera lanca poverenja

Provera sertifikata za svaki pojedinačni sertifikat mora da odgovori na sledeća pitanja: Da li postoji poverenje u dati sertifikat? Da li je sertifikat zaista potpisan od strane određenog CA?

Ako primalac sertifikata nema poverenje u prvi sertifikat u lancu, mora preći na proveru sledećeg sertifikata u lancu (odnosno sertifikata CA koje ga je potpisao). Proces se nastavlja sve dok primalac, u lancu sertifikata ne pronađe sertifikat u koji ima poverenja, odnosno u CA kome pripada sertifikat. Dodatak A sadži prikaz lanca poverenja uspostavljenog na realnom primeru lanca CA sertifikata za TCS servis.

3.1.6 Provera validnosti sertifikata

Provera sertifikata za svaki pojedinačni sertifikat mora da odgovori i na pitanja da li je sertifikat istekao? Da li je sertifikat važeći ili je opozvan? Kao što je već gore pomenuto, nevažeći (opozvani sertifikati) se objavljuju preko lista opozvanih sertifikata ili se koriste protokoli za proveru stanja sertifikata. Svaki sertifikat sadrži polje koje označava period njegovo važenja (*Validity*) i pokazuje da li je sertifikat istekao. Sertifikati se obično izdaju na 1 do 2 godine.

3.2 Format digitalnog sertifikata

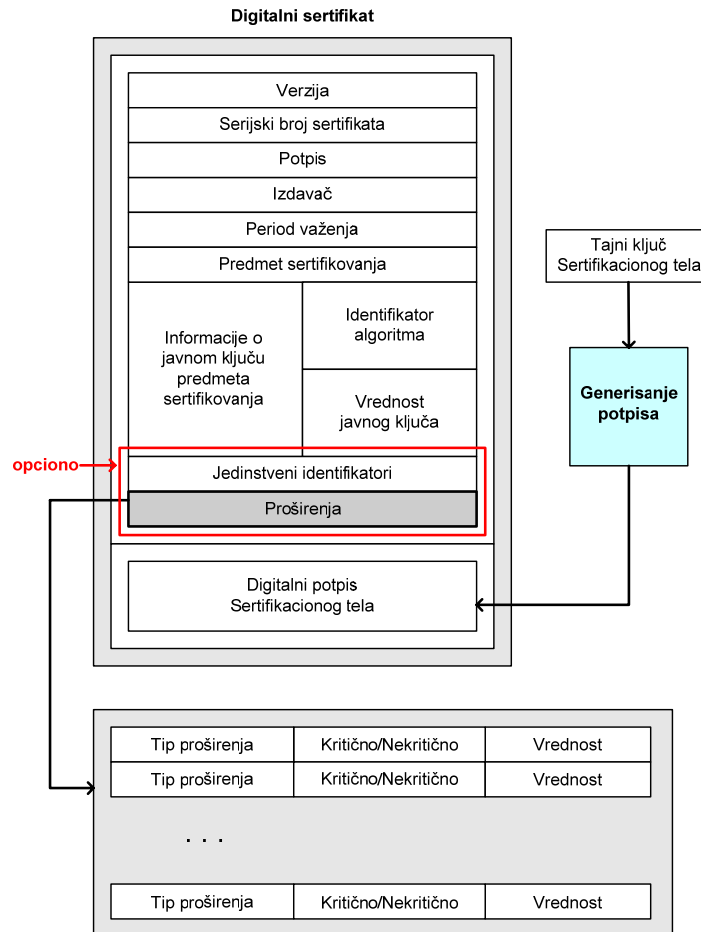
Format digitalnog sertifikata je definisan ITU-T X.509 standardom. Danas se najčešće koristi verzija 3.

Prema preporukama IETF RFC 5280 (*Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*) digitalni sertifikat treba da sadrži sledeća polja (slika 7):

- **Version** – informacija o verziji sertifikata. Trenutna verzija (i ona koja se najčešće koristi) je 3.
- **Serial number** – serijski broj sertifikata predstavlja jedinstveni identifikator sertifikata izdatih od određenog sertifikacionog tela.

- **Signature** – identifikator u OID (identifikator objekta) formatu. Identifikuje algoritam koji je sertifikaciono telo koristilo za potpisivanje sertifikata.
- **Issuer** – jedinstveno ime sertifikacionog tela koje je izdalo sertifikat. Daje se u formatu jedinstvenog imena (Distinguishing name - DN).
- **Validity** – označava period važenja sertifikata i sadrži dva datuma od kojih jedan označava trenutak od kada se sertifikat može smatrati važećim (polje *Not Valid Before*), a drugi, trenutak do kog se sertifikat može smatrati važećim (polje *Not Valid After*).
- **Subject** – identifikuje korisnika/entitet kome je izdat sertifikat. Kao i polje *Issuer*, daje se u formatu jedinstvenog imena (Distinguishing name - DN) entiteta, npr. "C=RS, O=Univerzitet u Beogradu OU=RCUB, CN=Milica Kovinic".
- **Subject public key info** – sadrži javni ključ korisnika/entiteta, kao i identifikaciju algoritma koji je korišćen pri kreiranju istog (RSA, DSA, Diffie-Hellman i slično).
- **Unique identifiers** – dodatni identifikator sertifikata čija se upotreba ne preporučuje u verzijama 2 i 3.
- **Extensions** – sadrži listu jednog ili više proširenja sertifikata koja se koriste za specificiranje dodatnih informacija o sertifikatu. Svaki član liste sadrži informaciju o tipu proširenja, oznaku kritičnosti proširenja i sadržaj proširenja. Kada korisnički softver, prilikom procesiranja, ne ume da prepozna proširenje, ako je ono označeno kao kritično proširenje, sertifikat će biti označen kao nevažeći. (ako je proširenje označeno kao nekritično, moguće je ignorisati dato proširenje i uvažiti ponuđeni sertifikat). Proširenja koja su u upotrebi pripadaju sledećim kategorijama:
 - Standardna proširenja:
 - **Authority key identifier - AKI** – omogućava identifikovanje javnog ključa koji odgovara privatnom ključu sertifikacionog tela kojim je potpisan sertifikat. Obično se koristi ako sertifikaciono telo ima više od jednog ključa za potpisivanje.
 - **Subject key identifier - SKI** – jedinstveni identifikator koji se koristi se za identifikovanje sertifikata koji sadrže odgovarajući javni ključ.
 - **Key usage** – definiše namenu ključa sadržanog u konkretnom sertifikatu, tj. da li on može da se koristi za potpisivanje, za šifrovanje, za verifikaciju lista opozvanih sertifikata i sl.
 - **Certificate policies** – sadrži listu identifikatora politika sertifikacije (datih u OID formi identifikatora objekta) i dodatnih opcionih tekstualnih parametara koji svedoče da je konkretan sertifikat izdat pod odgovarajućim skupom pravila objedinjenih u naznačenim politikama sertifikacije. Opcioni parametri su *Certification Practice Statement pointer* (definiše lokaciju na kojoj mogu da se pronađu Praktična pravila rada Sertifikacionog tela) i *User notice* (sadrži tekst poruke za krajnjeg korisnika).
 - **Policy mappings** – koristi se u sertifikatima sertifikacionih tela iz različitih administrativnih domena da označi skup parova politika sertifikacije koje se smatraju ekvivalentnim. Par politika sertifikacije, koji se želi specificirati u ovom proširenju, navodi se u poljima *Issuer domain policy* i *Subject domain policy*.
 - **Subject alternative name** – sadrži dodatne podatke o subjektu/objektu sertifikacije (npr. email krajnjeg korisnika, URL, IP adresu, alternativno DNS ime servera i sl.).
 - **Issuer alternative name** – sadrži dodatne podatke o sertifikacionom telu koje je izdalo sertifikat (npr. email, URI, IP adresu i sl.).
 - **Subject directory attributes** – daje dodatne informacije o predmetu sertifikovanja (npr. nacionalnost) i nije od velikog značaja.
 - **Basic constraints** – govori da li je predmet sertifikacije sertifikaciono telo ili krajnji korisnik/entitet. Za sertifikaciono telo, proširenje može da sadrži i parametar *Path length* (pokazuje broj sertifikata sertifikacionih tela koje mogu da ga slede).

- **Name constraints** – koristi se samo u sertifikatima sertifikacionih tela i definiše prostor imena dat u formi stabla dozvoljenih/zabranjenih imena (*Permitted subtrees and/or Excluded subtrees*), kome moraju/ne smeju da pripadaju tipovi imena u sertifikatima krajnjih korisnika izdatih od strane istih sertifikacionih tela.
- **Policy constraints** – koristi se u sertifikatima sertifikacionih tela da zabrani preslikavanje politika sertifikacije ili da označi neophodnost pojavljivanja određene politike sertifikacije u svim sertifikatima koji se proveravaju nakon ovog (sertifikata sa ovim proširenjem). Prisustvo polja *InhibitPolicyMapping* sugeriše da je nakon određenog broja (definisanog vrednošću ovog polja) sertifikata zabranjeno preslikavanje politika sertifikacije, dok prisustvo polja *Require explicit policy* sugeriše upotrebu određene politike sertifikovanja u određenom broju (definisanom ovom vrednošću) narednih sertifikata.
- **Extended key usage** – koristi se u sertifikatima krajnjih korisnika/entiteta da označi dodatne mogućnosti upotrebe ključa (pored onih koje su definisane u proširenju *Key usage*).
- **CRL distribution points** - ukazuje na lokacije na kojima se nalazi lista opozvanih sertifikata.
- **Inhibit anyPolicy** – koristi se u sertifikatima sertifikacionih tela da definiše odnos prema specijalnoj vrednosti politike sertifikacije *anyPolicy* (koja označava mogućnost upotrebe bilo koje politike sertifikacije) u narednim sertifikacionim telima. Vrednost označava broj dodatnih sertifikata koji se mogu pojaviti u lancu pre nego što *anyPolicy* više nije dozvoljena, odnosno broj sertifikacionih tela posle ovog, nakon koga se *anyPolicy* se ne smatra važećom za uparivanje sa nekom drugom konkretnom politikom.
- **Freshest CRL pointer** – predstavlja pokazivač na „najsvežije“ informacije vezane za opozvane sertifikate. U praksi, ovo je najčešće pokazivač na *Delta* listu opozvanih sertifikata.
- Privatna proširenja se definišu prilikom korišćenja sertifikata u specifičnim oblastima. Tako, na primer, RFC 5280 specificira dva proširenja ove vrste za primenu na Internetu:
 - **Authority information access** - definiše način pristupa uslugama (i informacijama) koje pruža sertifikaciono telo izdavalac sertifikata (npr. o usluzi za *online* proveru ispravnosti sertifikata, dodatnim informacijama o politici sertifikovanja...).
 - **Subject information access** - definiše način pristupa uslugama (i informacijama) koje pruža predmet sertifikovanja (npr. mesto skladištenja sertifikata kad je reč sertifikacionom telu kao predmetu sertifikovanja).



Slika 7 Digitalni sertifikat prema RFC 5280

Primeri formata i realan sadržaj polja digitalnog sertifikata se mogu naći u prilogu Dodatak A, u kome je pokazan lanac CA sertifikata za TCS servis.

Digitalni sertifikat se može čuvati u PEM formatu odvojeno od privatnog ključa, ili se može čuvati spojen sa privatnim ključem u različitim formatima (npr. PKCS #12, JKS, ...).

Najčešće korišćene fajl ekstenzije za X.509 sertifikate su:

- .CER, .CRT, .DER: DER (*Distinguished Encoding Rules*) format, najčešće u binarnoj formi, ali može da bude i Base64.
- .PEM: Base64 kodirani DER sertifikat, smešten između "-----BEGIN CERTIFICATE-----" i "-----END CERTIFICATE-----".
- .P7B: videti .P7C.
- .P7C: PKCS #7 format, sadrži samo sertifikat (jedan ili više), ali može da se koristi i za CRL.
- .PFX: videti P12.
- .P12: PKCS #12 format, sadrži sertifikat i odgovarajući privatni ključ (zaštićen je šifrom).
- .CSR: PKCS #10 format, sadrži zahtev za dobijanje sertifikata (CSR).

4 TCS – TERENA Certificate Service

TCS (*TERENA Certificate Service*) predstavlja servis za izdavanje digitalnih sertifikata naučno-istraživačkim i obrazovnim institucijama posredstvom njihovih matičnih akademskih mreža na koje su povezane. TERENA ima ulogu sertifikacionog tela, a ulogu registracionog tela propagira na NREN članice koje su se registrovale za korišćenje TCS servisa. Sertifikati dobijeni preko TCS servisa su izdati od strane *Comodo CA Limited*, jednog od vodećih, globalno priznatih sertifikacionih tela.

4.1 Tipovi sertifikata koje nudi TCS

TCS servis nudi pet različitih tipova digitalnih sertifikata :

- **Serverski SSL sertifikati (*Server Certificate*)** – nazivaju se još i SSL sertifikati, za autentifikaciju servera i uspostavljanje sigurne sesije sa krajnjim klijentima. Ovi sertifikati imaju period važenja do 3 godine. Među njima se razlikuju tri vrste serverskih sertifikata i to u zavisnosti od registrovanog DNS imena servera koje se nalazi u sertifikatu:
 - **TERENA Single SSL Certificate** – ovaj tip sertifikata se vezuje za samo jedno registrovano DNS ime servera, koje se nalazi u sertifikatu kao vrednost CN (*Common Name*) atributa.
 - **TERENA Multi-Domain SSL Certificate** – ovaj tip sertifikata može da obezbedi više od jednog registrovanog DNS imena i to tako što se jedno ime definiše kao primarno i smešta se u CN polje sertifikata, a sva dodatna imena se definišu kao vrednost SAN (*Subject Alternative Name*) polja. Sertifikat može da sadrži do 100 različitih DNS imena servisa koji se nalaze na **jednoj** fizičkoj mašini (serveru).
 - **TERENA Wildcard SSL Certificate** – omogućava da jedan sertifikat obezbedi neograničen broj poddomena koji se nalaze na različitim fizičkim mašinama (serverima). Ovaj sertifikat sadrži u CN polju ime domena oblika *.neki_domen (npr. *.rcub.bg.ac.rs) i na taj način štiti sve poddomene koji se nalaze pod definisanim domenom. Zbog stavljanja bezbednosti celog domena u jedan sertifikat, korišćenje Wildcard sertifikata je opravdano samo u sledećim slučajevima:
 - farme web servera
 - klasteri
 - *load balancers*
 - *failover* serveri
- **e-Istraživački serverski sertifikati (*e-Science Server Certificate*)** – za autentifikaciju GRID hostova i servisa. Cilj je da oni budu IGTF akreditovani. Ovi sertifikati imaju period važenja do 13 meseci.

- **Lični korisnički sertifikati (*Personal Certificate*)** – nazivaju se još i klijentski sertifikati, za autentifikaciju odnosno identifikaciju krajnjih korisnika tokom pristupa korisničkim serverima/servisima i zaštitu elektronske pošte (digitalno potpisivanje mejlova i enkripcija njihovog sadržaja). Sadrži podatke koji identifikuju krajnjeg korisnika, kao što su korisničko ime u okviru federacije identiteta (AMRES federacija identiteta je u procesu uspostavljanja), puno ime korisnika, e-mail adresu. Ovi sertifikati imaju period važenja do 3 godine.
- **e-Istraživački lični sertifikati (*e-Science Personal Certificate*)** – za autentifikaciju odnosno identifikaciju krajnjih korisnika prilikom pristupa Grid servisima. Namera je da budu IGTF akreditovani. Ovi sertifikati imaju period važenja do 13 meseci.
- **Sertifikati za potpisivanje koda (*Code-signing Certificate*)** – za autentifikaciju softvera koji se distribuira preko Interneta. Ovi sertifikati imaju period važenja do 5 godina.

4.2 Prednosti korišćenja TCS sertifikata

Sertifikati dobijeni preko TCS servisa su potpisani TERENA CA sertifikatom koji je dalje potpisan od strane *UserTrust*, prelaznog sertifikacionog tela koje je potpisano od strane *AddTrust External root* sertifikacionog tela. Taj *root* sertifikat je preinstaliran u većini SSL klijenata (na primer, prilikom pristupanja sajtu preko https-a, koji se nalazi na web serveru koji ima TERENA sertifikat, nije potrebna intervencija korisnika kako bi sertifikat bio prihvaćen jer se odgovarajući *Root CA* sertifikat već nalazi preinstaliran u većini često korišćenih *web browser*-a: Internet Explorer, Mozilla Firefox, Google Chrome, Opera).

U prilogu Dodatak A je dat lanac CA sertifikata za TCS serverske sertifikate. Prvi u nizu je sertifikat korenog sertifikacionog tela (*root CA*), *AddTrust External CA Root*, kojim je potpisan sledeći sertifikat prelaznog sertifikacionog tela (*intermediate CA*), *UTN-USERFirst-Hardware*. Na kraju sledi sertifikat TERENA sertifikacionog tela, *TERENA SSL CA*, koji je potpisan navedenim prelaznim sertifikatom.

Preko AMRES usluge izdavanja TCS sertifikata, institucijama članicama AMRESa raspoloživi su svi tipovi TCS sertifikata sem sertifikata za potpisivanje koda i autentifikaciju softvera. Ipak, treba imati u vidu da politika sertifikacije zahteva uspostavljanje jasnih i efikasnih procedure provere podataka prilikom izdavanja i korišćenja sertifikata. Ove procedure su trenutno uspostavljene za serverske SSL sertifikate. Planirano je da se izdavanje ličnih korisničkih sertifikata uskoro uredi na sličan način, preko AMRES federacije identiteta koja je u razvoju.

Serverski SSL sertifikati se mogu koristiti na svim serverima u AMRESu, koji nisu deo GRID infrastrukture. Izdavanje e-Istraživačkih tipova sertifikata (serverskih i ličnih) za zaštitu i pristup GRID instalacijama, trenutno je uspostavljeno kroz AEGIS CA. AEGIS CA je formiran da bi pružio PKI servis za GRID istraživačku zajednicu u Srbiji. AEGIS politika je objavljena u dokumentu <http://aegis-ca.rcub.bg.ac.rs/documents/AEGIS-CP-CPSv1-2.doc>, koji sadrži i Praktična pravila rada AEGIS CA.

4.3 Servisi koje je potrebno obezbediti digitalnim sertifikatima

Digitalne sertifikate treba koristiti za:

- **Autentifikaciju servera** (web, mejl ...) od strane klijenta ili drugog servera. U ovom slučaju se koriste serverski SSL sertifikati koji potvrđuju identitet servera klijentu koji mu pristupa. Na ovaj način klijent može da bude siguran da je pristupio pravom serveru, što je važno ako se šalju osetljivi podaci kao što

su korisnički kredencijali. Takođe, pored autentifikacije servera, obezbeđuje se i poverljivost komunikacije tako što klijent šalje ključ, koji će se koristiti za enkripciju podataka, enkriptovan javnim ključem servera.

- **Autentifikaciju krajnjih korisnika, klijenata** od strane servera kome pristupaju. U ovom slučaju klijent poseduje svoj lični korisnički sertifikat koji server proverava kako bi potvrdio identitet klijenta. Primer je autentifikacija klijenata u GRID infrastrukturi, gde svaki krajnji korisnik poseduje svoj lični sertifikat kojim se autentifikuje za pristup GRID servisima.
- **Sigurnu razmenu elektronske pošte** u kojoj su očuvani integritet poruke i poverljivost komunikacije. Pošiljalac digitalno potpisuje email poruku svojim privatnim ključem čime se garantuje integritet poruke. Da bi se obezbedila tajnost, potrebno je da učesnici u komunikaciji prethodno razmene svoje lične korisničke sertifikate.
- **Uspostavljanje IPsec/TLS VPN tunela** i autentifikaciju krajnjih korisnika koji iniciraju uspostavu VPN tunela. Pored toga, kod SSL VPN-ova, sertifikati se koriste i za autentifikaciju samog SSL VPN servera od strane VPN klijenata. Dakle, u ovom slučaju su potrebni serverski SSL sertifikat, kao i lični korisnički sertifikati.
- **Digitalno potpisivanje softvera** obezbeđuje dokaz o poreklu i integritetu softverskog koda. Kada je softver digitalno potpisan sertifikatom koje je izdalo sertifikaciono telo od poverenja, korisnik može da bude siguran da kod nije maliciozno izmenjen i da je bezbedno da ga instalira na svom sistemu. U ovom slučaju potrebni su sertifikati za potpisivanje koda.

Obzirom da je u institucijama članicama AMRES-a upotreba digitalnih sertifikata u začetku, u nastavku je data preporuka za najčešće korišćene servere/servise koje je potrebno obezbediti serverskim SSL sertifikatima. Takođe, objašnjena je zaštita elektronske pošte korišćenjem personalnih sertifikata.

4.3.1 Web server

HTTPS (*Hypertext Transfer Protocol Secure*) protokol se koristi kako bi se obezbedila zaštićena komunikacija između web servera i web klijenta preko nezaštićene mreže kao što je Internet. Sigurna komunikacija, uspostavljena na ovaj način, omogućava klijentu da autentifikuje server kojem pristupa, kao i enkripciju podataka koji se razmenjuju između klijenta i servera. HTTPS je HTTP protokol koji koristi usluge TLS/SSL protokola na nižem sloju.

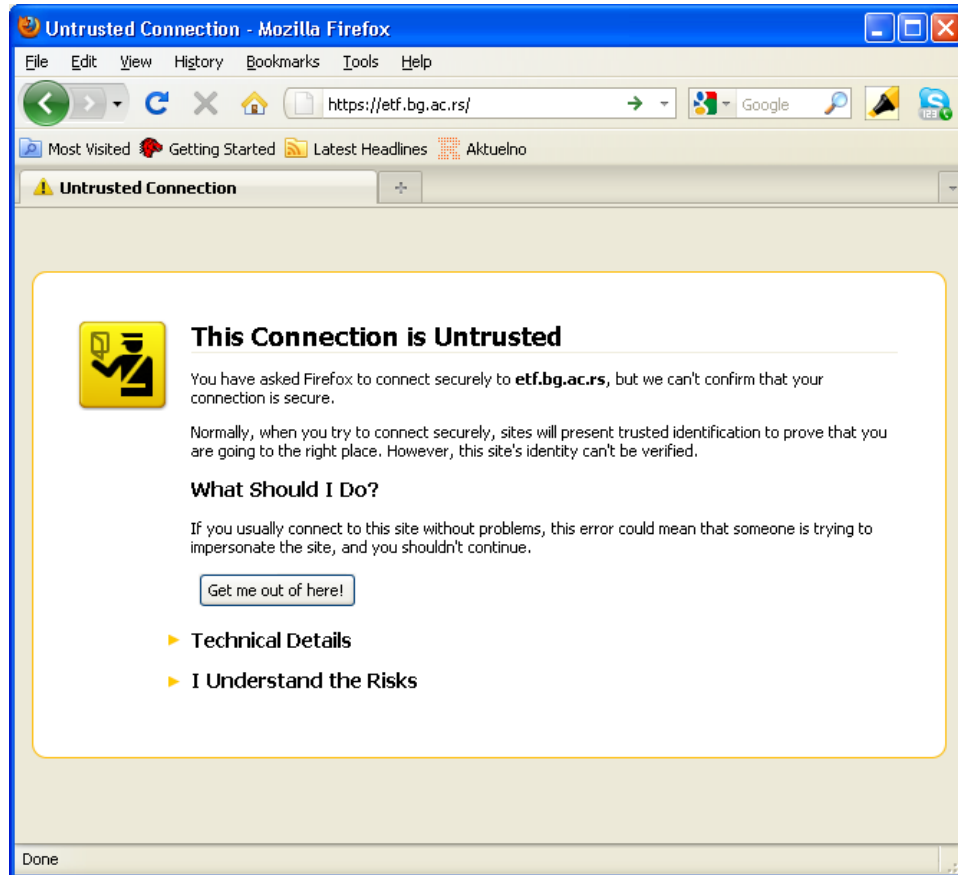
Za HTTPS komunikaciju, web server mora biti konfigurisan da sluša na portu 443 i da koristi serverski SSL sertifikat. Serverski sertifikat sadrži informacije koje omogućavaju klijentu da potvrdi identitet servera pre slanja poverljivih informacija (kao što su korisnička imena i lozinke).

Uspostava HTTPS konekcije se sastoji iz sledećih koraka:

- Klijent pristupa web strani preko koje unosi neke osetljive podatke kao što su korisnički kredencijali.
- Web server šalje svoj serverski sertifikat klijentu.
- Da bi proverio sertifikat, web klijent proverava lokalnu bazu sertifikata na korisnikovom računaru, kako bi pronašao sertifikat sertifikacionog tela koje je izdalo sertifikat web servera. U slučaju da ga je pronašao, može da veruje sertifikacionom telu koje je izdalo sertifikat. Dalje, klijent proverava ime servera u sertifikatu, koje mora da se poklapa sa DNS imenom preko koga je klijent pristupio serveru.
- Web klijent pomoću javnog ključa, koji se nalazi u serverskom sertifikatu koji je primio, vrši enkripciju podataka koje šalje serveru.

- Kako bi server mogao da šalje kriptovane podatke klijentu, klijent mu šalje ključ, koji je generisao za tu sesiju, kriptovan javnim ključem servera. Od ovog trenutka može da počne sigurna razmena podataka između klijenta i servera.

U slučaju da sertifikat servera nije potpisan od sertifikacionog tela kome klijent veruje, pojavljuje se pop-up poruka (slika 8) sa upozorenjem korisniku da sajt kome pristupa nije siguran i sa pitanjem da li želi da nastavi sa daljom komunikacijom (što često zna da zbuni korisnika).



Slika 8 Poruka sa upozorenjem korisniku da sajt kome pristupa nije siguran

Kod HTTPS komunikacije i klijenti mogu da koriste svoje personalne sertifikate. Sertifikat klijenta sadrži lične podatke o korisniku i omogućavaju serveru da autentifikuje korisnika.

4.3.2 RADIUS server

RADIUS serverima korisnici šalju svoje kredencijale kako bi se autentifikovali za pristup mrežnim resursima. U AMRES mreži upotreba sertifikata na RADIUS serverima u okviru eduroam servisa je obavezna. Za autentifikaciju klijenata koristi se standard IEEE 802.1x. Za prenos autentifikacionih poruka koristi se EAP (*Extensible Authentication Protocol*) protokol u kombinaciji sa TLS, TTLS (*Tunneled TLS*) ili PEAP (*Protected EAP*) protokolom.

Pri procesu autentifikacije, RADIUS server dobija poruku od klijenta koja označava početak autentifikacije. Server odgovara šaljući svoj digitalni sertifikat klijentu. Klijent proverava ispravnost digitalnog sertifikata servera tako što u svojoj lokalnoj bazi pronalazi sertifikat sertifikacionog tela koje je izdalo serverski sertifikat. Ako je ishod pozitivan, klijent šalje svoje kredencijale (identitet i lozinku) kriptovane javnim ključem servera. RADIUS server, dobijene podatke dekriptuje svojim privatnim ključem i proverava kredencijale korisnika u svojoj bazi podataka.

Detaljnije objašnjenje EAP-TTLS protokola nalazi se u dodatku prilogu Dodatak C.

4.3.3 Email server

STARTTLS predstavlja ekstenziju SMTP, IMAP i POP3 protokola (SMTPS, IMAPS, POP3S) koja omogućava uspostavu kriptovane konekcije uz podršku SSL/TLS protokola. Kako je STARTTLS nadogradnja postojećih protokola, nije potreban poseban port za kriptovanu komunikaciju. Za protokole SMTPS, IMAPS i POP3S registrovani su posebni portovi, pri čemu RFC ne preporučuje njihovo korišćenje, jer upotreba STARTTLS omogućava korišćenje istog porta i za zaštićenu i za nezaštićenu komunikaciju.

Pored toga što omogućava poverljivu, enkripcijom zaštićenu, razmenu podataka, STARTTLS nudi mogućnost autentifikacije između servera, kao i između klijenta i servera. Da bi se uspostavila kriptovana/autentifikovana komunikacija, strana koja inicira komunikaciju šalje *starttls* poruku kako bi označila prebacivanje na zaštićenu razmenu podataka.

Autentifikacija može da bude obostrana ili jednostrana. Najčešće se konfigurise tako da klijent autentifikuje server kome pristupa (u slučaju POP3, IMAP i SMTP protokola) i između servera (u slučaju SMTP protokola). Strana koja se autentifikuje mora da poseduje svoj digitalni sertifikat koji druga strana proverava.

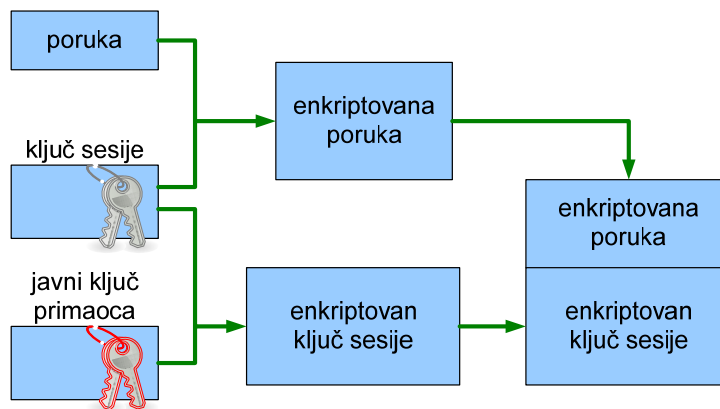
U slučaju kriptovane komunikacije, između klijenta i servera ili servera i servera, strana koja šalje koristi javni ključ iz digitalnog sertifikata druge strane kako bi poslala šifrovanu poruku. Na prijemu, druga strana vrši dešifrovanje pomoću svog privatnog ključa.

Ovde je bitno naglasiti da se zaštićena komunikacija ne odvija s kraja na kraj, već samo između onih servera/klijenata koji su konfigurisani da koriste STARTTLS. Jedan od načina da se obezbedi poverljivost komunikacije između krajnjih klijenata je korišćenjem S/MIME standarada što je objašnjeno u nastavku.

4.3.4 Zaštita elektronske pošte

MIME je Internet standard koji definiše prošireni format email poruke. S/MIME (*Secure/ Multipurpose Internet Mail Extensions*) predstavlja proširenje MIME standarda i omogućava zaštićenu razmenu elektronske pošte koja omogućava autentifikaciju pošiljaoca, dokaz integriteta poruke kao i enkripciju njenog sadržaja. Ovde je potrebno da obe strane komunikacije poseduju digitalne sertifikate i da ih međusobno razmene.

Na slici 9 je prikazana S/MIME enkripcija/dekripcija poruke. Da bi se izvršila enkripcija poruke, pošiljalac generiše simetrični ključ za tu sesiju kojim enkriptuje telo poruke. Zatim, pošiljalac enkriptuje simetrični ključ javnim ključem primaoca. Na prijemu, primalac koristeći svoj privatni ključ dešifruje simetrični ključ sesije, pomoću koga dekriptuje telo poruke. Na ovaj način se dobija poverljiva razmena email poruka, pri čemu je ceo proces potpuno transparentan za same krajnje korisnike.



Slika 9 S/MIME enkripcija/dekripcija poruke

Da bi se obezbedio integritet poruke, kreira se digitalni potpis poruke, koji se zajedno sa njom šalje. Digitalni potpis poruke se dobija računanjem njene heš vrednost. Kako se za dešifrovanje heša koristi javni ključ pošiljaoca, to potvrđuje da je samo onaj sa odgovarajućim privatnim ključem mogao da pošalje poruku, čime je izvršena autentifikacija strane koja je poslala poruku.

5 AMRES usluga izdavanja TCS sertifikata

AMRES je u saradnji sa TERENA-om uspostavio servis izdavanja digitalnih sertifikata, gde TERENA ima ulogu sertifikacionog tela (*CA – Certification Authority*), a AMRES registracionog tela (*RA – Registration Authority*). TCS servis je potpuno besplatan za sve AMRES članice koje prethodno prođu kroz proces registracije.

Politika sertifikacije propisuje procedure provere podataka prilikom izdavanja i korištenja sertifikata. Procedure definisane za pribavljanje serverskih SSL sertifikata su objašnjene u nastavku.

Da bi institucija dobila serverski SSL sertifikat, potrebno je da uradi sledeće:

1. Registraciju institucije u ac.rs
2. Prijavljivanje za korišćenje TCS servisa
3. Kreiranje para ključeva i zahteva za sertifikatom
4. Podnošenje zahteva

Instalacija sertifikata i konfiguracija servera je opisana u poglavlju 6 Instalacija sertifikata.

5.1 Registracija institucije

Registracija institucije se obavlja preko [portala Registra domena ac.rs](http://portal.registra.ac.rs).

Smatra se da je institucija registrovana u ac.rs kada ima registrovan bar jedan domen na [portalu Registra domena ac.rs](http://portal.registra.ac.rs). Registracija domen institucije u ac.rs (bilo da je domen već aktivan ili potpuno nov) se radi jednom. Time domen institucije postaje administrativno ozvaničen u ac.rs. Institucije koje imaju domen registrovan u ac.rs su, kao institucije akademske i istraživačke zajednice, automatski kvalifikovane za korišćenje dugih servisa akademske mreže. Između ostalog, registrovana institucija se može prijaviti za korišćenje TCS usluge (tako što će potpisati odgovarajući ugovor i priložiti ga preko Portala).

Podaci o instituciji na portalu moraju biti tačni i ažurni. Oni se koriste se za proveru podataka o samoj instituciji u državnim registrima preduzeća, zatim u dokumentu koji institucija potpisuje i prilaže u prijavi za korišćenje TCS servisa, ali i kasnije za proveru informacije koju sadrži zahtev za izdavanje sertifikata koji institucija podnosi AMRES-u u procesu dobijanja TCS sertifikata.

5.2 Prijavljivanje za korišćenje TCS servisa

Registrovane institucije u *ac.rs* mogu se prijaviti za korišćenje TCS servisa tako što će popunjeni i od ovlašćene osobe potpisani dokument [Saglasnost za korišćenje TCS](#) upload-ovati preko portala Registra *ac.rs* domena (slika 10). Dokument o saglasnosti može se preuzeti na sajtu [AMRES-a](#). Njegovim potpisivanjem, institucija imenuje osobu, koja će je kao administrativni kontakt zastupati u postupcima zahtevanja, dobijanja, obnavljanja i opozivanja digitalnih sertifikata. Uslovi, prava i obaveze za korišćenje digitalnih sertifikata (definisani od strane TERENA-e) propisuju da svaka institucija, odnosno njen imenovani administrativni kontakt, mora biti upoznat sa osnovnim preduslovima korišćenja digitalnih sertifikata (koji se mogu preuzeti sa sajta [AMRES-a](#)). Posle provere podataka od strane AMRES-a, imenovani administrativni kontakt biće email-om obavešten o rezultatu prijave.



Ovde treba da dostavite potpisani dokument 'Saglasnost za korišćenje usluge izdavanja TERENA sertifikata' potpisan od strane ovlašćenog lica Vaše institucije. U njemu, za osobu koja će vršiti ulogu administrativnog kontakta, trebate popuniti vaše podatke (to mora biti ista osoba koja je već imenovana kao administrativni kontakt pri registraciji prvog domena institucije u *ac.rs*).

*Kako biste dodali dokumenta potrebno je da kliknete na dugme 'Add', potom da izaberete dokument i onda kliknete na dugme 'Upload'. Prihvataju se fajlovi tipa: .jpg, .gif, .bmp, .png, .pdf, .doc i .docx!

Tehnički kontakt za uslugu izdavanja TERENA sertifikata ispred Vaše institucije je: _____

Pošalji zahtev

Slika 10 Slanje ugovora za registraciju za TCS preko Portala

Institucija koja postane korisnik TCS servisa, dalje preko svog administrativnog kontakta ostvaruje pravo na podnošenje zahteva i dobijanje serverskih SSL sertifikata.

5.3 Kreiranje asimetričnog para ključeva i zahteva za potpisivanje sertifikata

Zahtev za dobijanje serverkog SSL sertifikata podnosi se u formi zahteva za potpisivanje sertifikata (CSR – *Certificate Signing Request*), tzv. CSR zahteva koji se šalje email-om na adresu tcs@amres.ac.rs.

Kreiranju CSR zahteva, predhodi postupak generisanja asimetričnog para RSA ključeva, tj. privanog ključa i njemu odgovarajućeg javnog ključa, pomoću alata koji je raspoloživ na serveru. Na Linux serverima treba koristiti OpenSSL paket (može se naći na <http://www.openssl.org>). Na Microsoft platformama odgovarajući paket je raspoloživ u grupi *Internet (Information) Service Manager* alata. Tek pošto su generisani ključevi, korištenjem istog alata, kreira se serverski sertifikat, odnosno CSR zahtev za potpisivanjem sertifikata.

Napomena: Zbog veće sigurnosti, AMRES je usvojio da minimalna dužina para asimetričnih ključeva, koji se generišu pri kreiranju zahteva za sertifikatom, mora biti 2048 bita.

Serverski sertifikat veže javni ključ za identitet servera, odnosno DNS zapis o serveru, pa se u CSR zahtevu sem javnog ključa moraju dostaviti i informacije koje opisuju identitet servera. Pre svih, to je registrovano DNS ime servera (koje će biti smešteno u polju *Common name* sertifikata). Ako se na istoj fizičkoj mašini (serveru) koristi više DNS imena (npr. za različite servise), jedno od registrovanih DNS imena mora biti određeno za primarno DNS ime servera. Sva ostala imena koje pokriva sertifikat se navode kao dodatna/alternativna DNS imena servera.

Serverski sertifikat koji štiti jedan server može da sadži jedno ili više (maksimalno 100) njegovih DNS imena. Svako DNS ime severa (bilo primarno ili alternativno) se mora navesti u FQDN (*Fully Qualified Domain Name*) obliku, tj. mora biti dato puno DNS ime servera (npr. www.sf.bg.ac.rs, www.uns.rs.ac i sl.).

Kao što je objašnjeno u poglavlju 4, Terena Single SSL Certificate pokriva samo jedno DNS ime servera, dok TERENA Multi-Domain SSL Certificate pokriva više DNS imena istog servera. Prema tome, TERENA Multi-Domain SSL Certificate treba zahtevati kada je u instituciji podignuto više servisa na istom serveru, pri čemu svaki od servisa koristi svoje DNS ime. Primer, server sa primarnim imenom glavni_server.na_domenu.ac.rs na kome se nalaze web servis, webmail servis, mail servis, pop3 servis kojima se pristupa preko imena www.na_domenu.ac.rs, webmail.na_domenu.ac.rs, mail.na_domenu.ac.rs i pop3.na_domenu.ac.rs.

Konkretna procedura kreiranja CSR zahteva zavisi od karakteristika servera za koji je SSL sertifikat predviđen: (operativnog sistema, alata raspoloživog za kreiranje zahteva na toj platformi, te broja različitih DNS imena za dati server). U nastavku je opisan postupak kreiranja zahteva na dve najčešće platforme u AMRESu: Linux serverima (sa OpenSSL paketom) i Microsoft IIS serverima (4.x, 5.x/6.x). Uputstva za druge serverske platforme mogu se naći na adresi: http://www.instantssl.com/ssl-certificate-support/csr_generation/ssl-certificate-index.html.

5.3.1 Linux OpenSSL

Za kreiranje CSR zahteva na Linux serverima trebalo bi koristiti OpenSSL paket. Paket je potrebno preuzeti sa <http://www.openssl.org> i instalirati na server.

Za dve najčešće situacije, pripremljena su dva predefinisana OpenSSL konfiguraciona fajla: *SCSReq.cnf* i *MultiSCSReq.cnf*. Treba odabrati i koristiti jedan od njih u zavisnosti od toga da li se podnosi zahtev za TERENA Single SSL Certificate (*SCSReq.cnf*) ili TERENA Multi-Domain SSL Certificate (*MultiSCSReq.cnf*).

Kao što je objašnjeno u poglavlju 4, Terena Single SSL Certificate pokriva samo jedno DNS ime servera, dok TERENA Multi-Domain SSL Certificate pokriva više DNS imena istog servera. Gotovo uobičajeno je da se

Linux serveri koriste tako da se na jednom Linux serveru (jednoj IP adresi) nalazi više servisa sa različitim simboličkim adresama. Na primer, kada se više različitih *web* sajtova ili servisa hostuje na jednom serveru, različita DNS imena sajtova/servisa se mapiraju u istu IP adresu servera. Pogrešno je zahtevati poseban serverski sertifikati za svaki *web* sajt ili servis. Za takav server treba zahtevati samo jedan sertifikat koji važi za sva DNS imena tog servera, i to sertifikat TERENA Multi-Domain SSL Certificate (*MultiSCSreq.cnf*).

Sadržaj odabranog konfiguracionog fajla, *SCSreq.cnf* ili *MultiSCSreq.cnf*, prebaciti u tekstualni fajl na serveru i sačuvati ga pod odgovarajućim imenom. Ime fajla se navodi u pozivu OpenSSL-a za kreiranje CSR zahteva. U primeru ćemo nastaviti da koristimo ista imena *SCSreq.cnf*, za kreiranje zahteva za sertifikatom koji sadrži jedno DNS ime servera, odnosno *MultiSCSreq.cnf* za kreiranje zahteva za više DNS imena.

SCSreq.cnf – konfiguracioni fajl koji se poziva kada se kreira zahtev za sertifikatom koji sadrži jedno DNS ime servera (u FQDN obliku, npr. *rcub.bg.ac.rs*):

```
[ req ]
default_bits          = 2048
default_keyfile       = keyfile.pem
distinguished_name    = req_distinguished_name
encrypt_key           = no

[ req_distinguished_name ]
countryName           = Oznaka zemlje (2 znaka)
countryName_default   = RS
countryName_min       = 2
countryName_max       = 2
localityName          = Naziv lokacije (grad)
organizationName      = Pun naziv institucije
organizationalUnitName = Naziv organizacione jedinice
commonName            = DNS (FQDN) ime servera
commonName_max        = 64
```

MultiSCSreq.cnf – konfiguracioni fajl koji se poziva kada se kreira zahtev za sertifikatom koji sadrži više od jednog DNS imena servera:

```
[ req ]
default_bits          = 2048
default_keyfile       = keyfile.pem
distinguished_name    = req_distinguished_name
encrypt_key           = no
req_extensions        = v3_req

[ req_distinguished_name ]
countryName           = Oznaka zemlje (2 znaka)
countryName_default   = RS
countryName_min       = 2
countryName_max       = 2
localityName          = Naziv lokacije (grad)
organizationName      = Pun naziv institucije
organizationalUnitName = Naziv organizacione jedinice
0.commonName         = Primarno DNS (FQDN) ime servera
0.commonName_max      = 64

[ v3_req ]
subjectAltName        = @alt_names
```

```
[ alt_names ]
DNS.1          = www.na_domenu.ac.rs
DNS.2          = webmail.na_domenu.ac.rs
DNS.3          = pop3.na_domenu.ac.rs
```

Kada se generiše zahtev za sertifikatom koji sadrži više od jednog DNS imena, sva dodatna DNS imena moraju se uneti direktno u konfiguracioni fajl *MultiSCSreq.cnf* u delu `[alt_names]` kao vrednosti elemenata `DNS.x` ($x=1,2,3, \dots$). Dati konfiguracioni fajl je formiran za tri dodatna DNS imena, pri čemu taj broj, u zavisnosti od potrebe, može da bude manji ili veći. Ako je broj dodatnih DNS imena manji od tri potrebno je obrisati suviše `DNS.x` elemente (obrisati celu liniju koja počinje sa `DNS.x`).

Zahtev za sertifikatom generisati pozivanjem *openssl* komande ([OpenSSL](#) paket mora biti predhodno instaliran).

Pre zadavanja *openssl* komande, *umask* komandom definistati *read* privilegije za sve što će biti potom kreirano. Svrha je zaštita privatnog ključa servera, koji treba ostati tajni i ne sme da bude javno dostupan.

U pozivu *openssl* komande navodi se ime konfiguracionog fajla (sa putanjom do njega ukoliko se nalazi u direktorijumu različitom od onog iz koga se komanda poziva), ime fajla u koji će biti smešten privatni ključ i ime fajla u koji će biti smešten zahtev za potpisivanje sertifikata (alternativno korisimo i skraćeni naziv zahtev za sertifikatom). U dole navedenoj komandi koristi se *SCSreq.cnf* konfiguracioni fajl, dok *myserver.key* i *server.csr* predstavljaju nazive fajlova u koje će biti smešteni privatni ključ servera i zahtev za sertifikatom, respektivno. Pri tome imena *myserver.key* i *server.csr* mogu da se promene i zgodno je da nose ime samog servera za koji se zahtev generiše.

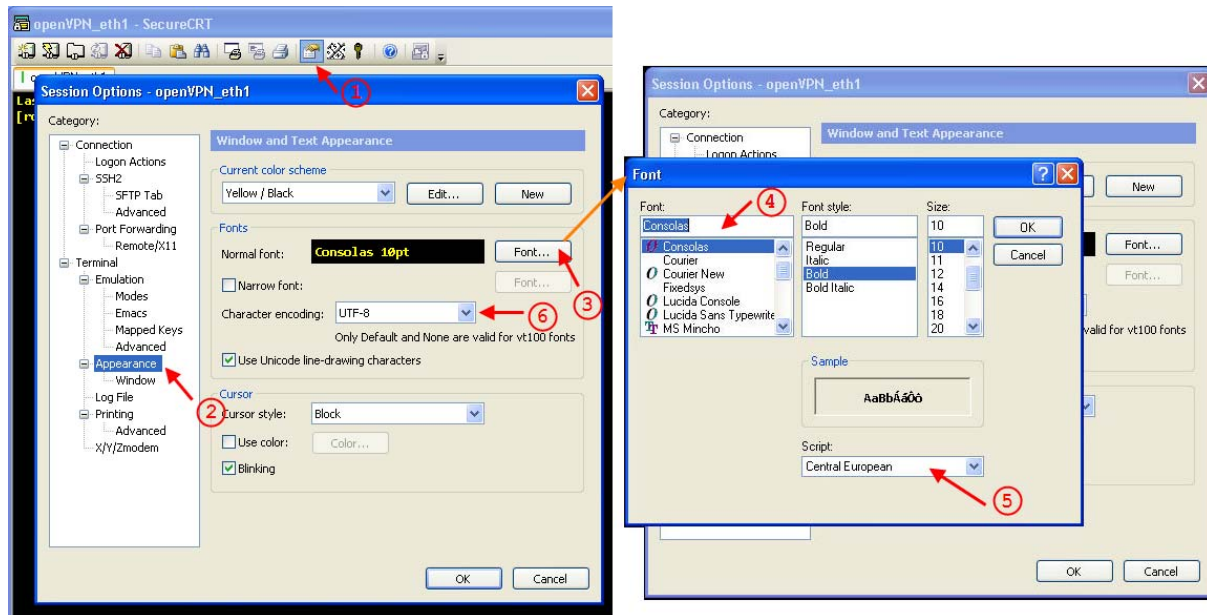
```
umask 0377
openssl req -new -config SCSreq.cnf -utf8 -keyout myserver.key -out server.csr
```

Pokretanjem navedene *openssl* naredbe ulazi se u dijalog prikazan na slici 11. Komanda će tražiti odgovarajuću informaciju na svako pitanje. Pri tome će, *default* odgovore ponuditi u zagradama `[]`, ako ih ima predefinisane. Tražene podatke uneti tačno i u skladu sa podacima koji su podneti u procesu registracije (npr. koristiti zvaničan naziv institucije pod kojim je ona registrovana na portalu i sl.).

```
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to "myserver.key"
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Oznaka zemlje (2 znaka) [RS]:
Naziv lokacije (grad) []:Beograd
Pun naziv institucije [Univerzitet u Beogradu]:
Naziv organizacione jedinice []: RCUB
Primarno DNS (FQDN) ime servera []:imeservera.rcub.bg.ac.rs
```

Slika 11

Napomena: U slučaju da neki od unosa sadrži latinična slova (č, ć, š, ž, đ), podesiti podršku za UTF-8. Podešavanje zavisi od terminala koji se koristi. Za korisnike SecureCRT terminala (verzija 5.5.3.536) podešavanje uraditi u šest koraka redosledom prikazanim na slici 12.



Slika 12 Podešavanje podrške za UTF-8 kod SecureCRT terminala

Po uspešnom izvršenju komande, dobili smo zahtev za potpisivanje sertifikata (u fajlu `server.csr`) i par ključeva (od kojih se privatni ključ nalazi u fajlu `myserver.key`, a javni u fajlu `server.csr`, zapakovan sa samim zahtevom).

Sadržaj kreiranog zahteva za sertifikatom može da se proveri sledećom komandom (slika 13):

```
openssl req -in server.csr -text
```

```

Certificate Request:
  Data:
    Version: 0 (0x0)
    Subject: C=RS, L=Beograd, O=University of Belgrade, OU=RCUB,
CN=openvpn-server.rcub.bg.ac.rs
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (2048 bit)
      Modulus (2048 bit):
        00:e:f:fa:67:16:c9:e4:fc:65:2e:d2:0a:3b:3c:cc:
        06:d7:3e:cb:fl:f1:81:e3:ae:4e:3c:lf:5e:0c:f9:
        87:fd:79:73:43:d9:9f:c5:2e:25:58:4d:ac:7f:4b:
        ...
        df:5f:ab:86:22:40:c2:08:02:ed:2c:c6:9c:9c:5f:
        ab:17:22:ec:d6:45:4b:a2:9b:4a:07:90:26:2e:23:
        15:fc:c7:15:4b:eb:4a:05:7c:0a:9a:6d:e4:73:7b:
        08:21:e3:02:f9:db:49:24:12:e7:16:6d:e3:50:92:
        29:f0:77:8d:54:3c:a7:aa:la:aa:cf:d7:a9:6d:bf:
        a8:r/
      Exponent: 65537 (0x10001)
      Attributes:
      Requested Extensions:
        X509v3 Subject Alternative Name:
          DNS:openvpn-server.rcub.bg.ac.rs, DNS:ejbca.rcub.bg.ac.rs,
DNS:openvpn.rcub.bg.ac.rs
      Signature Algorithm: sha1WithRSAEncryption
        2:d6:d5:b7:7f:7c:86:a1:8d:24:ce:73:l2:cb:ff:81:e9:7c:
        e9:2c:b8:2b:01:24:a7:2d:9e:83:5b:9e:ce:3c:d0:04:48:b9:
        lf:b0:24:8e:24:f2:d2:3b:fd:59:ec:fd:81:44:97:1a:c5:11:
        ...
        9b:3d:f7:a4:f3:c7:cd:40:88:3f:91:d9:7f:8b:e1:19:c6:47:
        6d:39:a3:ea:73:c9:d9:e7:45:62:0b:42:58:bc:81:d1:30:9a:
        f2:18:ba:a3:60:91:7a:8d:24:b9:2d:a8:07:11:29:4f:1e:dd:
        b2:cc:f2:3c:6e:25:aa:8d:15:50:7c:6f:e6:cd:c8:5d:fe:35:
        e7:63:40:39
    -----BEGIN CERTIFICATE REQUEST-----
    MIIDITCAgkCAQAwdjELMAkGALUEBhMCU1MxEDA0BgNVBAcTBOJlb2dyYWQxHZAAd
    ...
    DQEBAQUAA4IBDwAwggEKAoIBAQDv+mcWyeT8Z378Cjs8zAbXPsvx8YHjrk48H14M
    FL/LWVThxqWxmz33pPPHzUCIP5HZf4vhGcZhbTmj6nPJ2edFYgtCWLYBOTCa8hi6
    o2CReo0kuS2oBxEpTx7dsszyPG4lqo0VUHxv5s3IXf4151PQ0Q==
    -----END CERTIFICATE REQUEST-----

```

Slika 13 Zahtev za sertifikatom

Vidimo da zahtev za potpisivanje sertifikata sem javnog ključa servera, sadrži i druge podatke koji treba da se nalaze u sertifikatu, poput podataka o instituciji, primarnog DNS imena i opciono više dodatnih DNS imena servera. Svi podaci koji treba da se nalaze u sertifikatu, digitalno potpisani privatnim ključem servera, upisani su u odgovarajućem formatu, između „-----BEGIN CERTIFICATE REQUEST-----” i „-----END CERTIFICATE REQUEST-----”, na kraju fajla (*server.csr*).

Privatni ključ u fajlu *myserver.key* ostaje na serveru, i ne sme da bude javno dostupan. U poglavlju 6 Instalacija sertifikata su date preporuke za odabir i zaštitu direktorijuma u kojima se čuvaju sertifikati i ključevi.

5.3.2 Microsoft IIS 4.x

Za Microsoft platforme naveden je samo postupak zahtevanja *TERENA Single SSL Certificate* -, za jedno DNS ime servera, ne i postupak zahtevanja *TERENA Multi-Domain SSL Certificate*, koji pokriva više od jednog DNS imena istog servera (pogledati poglavlja 4.1 Tipovi sertifikata koje nudi TCS i 5.3.1 Linux OpenSSL). Za razliku od Linux servera, Microsoft IIS serveri u AMRESu se ređe koriste tako da se na jednom IIS serveru (jednoj IP adresi) nalazi više servisa sa različitim simboličkim adresama.

Generisanje para ključava i IIS SSL zahteva za sertifikatom (CSR) se sastoji iz sledećih koraka:

- Otvoriti **Microsoft Management Console (MMC)** za IIS (Option Pack > Microsoft Internet Information Server > Internet Service Manager).
- U okviru MMC, kliknuti na **Internet Information Server** folder i odabrati **Computer name**.
- Otvoriti **Properties** prozor, za sajt za koji se kreira CSR, desnim klikom na ime sajta.
- Otvoriti **Directory Security Folder**.
- U delu **Secure Communications**, kliknuti na **Key Manager**, a zatim izabrati „**Create New Key...**”.
- Izabrati „**Put the request in a file that you will send to an authority**”. Uneti odgovarajuće ime fajla (ili koristiti predefinisano ime) u koji će biti smešten kreirani zahtev.
- Popuniti odgovarajuće podatke
 - Popuniti sva polja, ne koristeći sledeće karaktere: ! @ # \$ % ^ * () ~ ? > < & / \

Napomena: Zbog veće sigurnosti, AMRES je usvojio da minimalna dužina para asimetričnih ključeva, koji se generišu pri kreiranju zahteva za sertifikatom, mora biti 2048 bita.

Međutim, ako je IIS server 40-bitni (40 bit enabled), dužina generisanih ključeva ne može biti iznad 512 bita, a ako je server 128-bitni, dužina ključa može da bude do 2048 bita. Za 40-bitne servere se može napraviti izuzetak od opšteg pravila da ne treba koristiti ključeve manje od 2048, mada to pruža manji stepen zaštite.

- Kliknuti **Next** potreban broj puta, zatim kliknuti **Finish**.
- **Key Manager** će prikazati ikonu ključa ispod **www** ikone. Ključ će biti precrtan narandžastom crticom, označavajući da postupak nije gotov.
- U meni-u **Computers** izabrati **Exit**. Izabrati **YES** za potvrdu unetih izmena.
- Dobijeni zahtev za sertifikatom se nalazi u fajlu (čije ime ste odredili u jednom od predhodnih koraka) između redova „-----BEGIN CERTIFICATE REQUEST-----” i „-----END CERTIFICATE REQUEST-----” uključujući i njih.
- Kliknite **Next**

Napomena: password kojim je zaštićen privatni ključ, kao i sam ključ bi trebalo da budu poznati samo administrativnom kontaktu institucije.

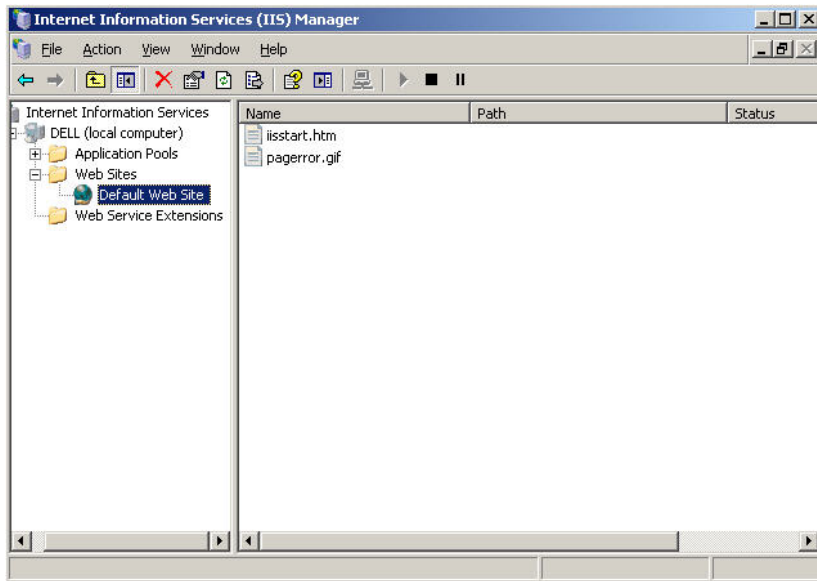
5.3.3 Microsoft IIS 5.x / 6.x

Za Microsoft platforme naveden je samo postupak zahtevanja *TERENA Single SSL Certificate* -, za jedno DNS ime servera, ne i postupak zahtevanja *TERENA Multi-Domain SSL Certificate*, koji pokriva više od jednog DNS imena istog servera (pogledati poglavlja 4.1 Tipovi sertifikata koje nudi TCS i 5.3.1 Linux OpenSSL). Za razliku od Linux servera, Microsoft IIS serveri u AMRESu se ređe koriste tako da se na jednom IIS serveru (jednoj IP adresi) nalazi više servisa sa različitim simboličkim adresama.

Napomena: Pre generisanja zahteva, instalirati *hotfix* dostupan na <http://support.microsoft.com/kb/975701>, koji rešava problem oznake zemlje (country code) za Srbiju. Zbog greške u samom Web Server Certificate Wizard-u, kao oznaka zemlje za Srbiju stoji SP umesto RS.

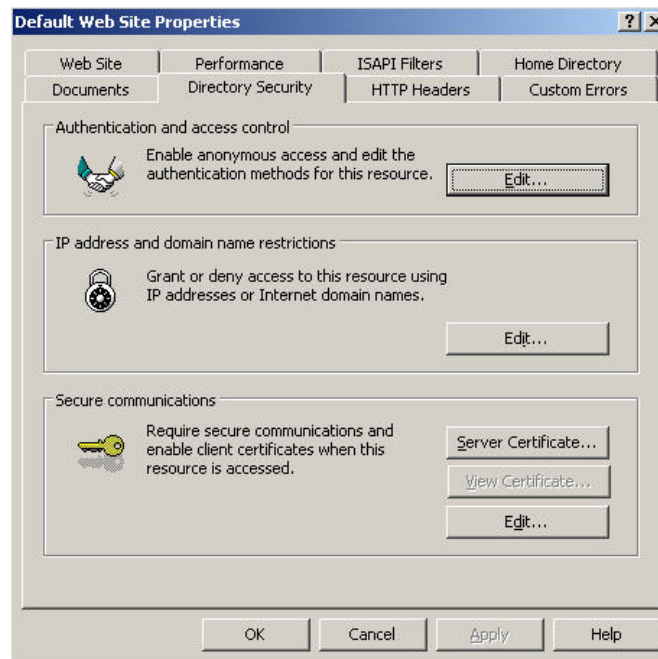
Generisanje para ključeva i IIS SSL zahteva za sertifikatom (CSR) se sastoji iz sledećih koraka:

- Izabrati **Administrative Tools** i startovati **Internet Services Manager**.



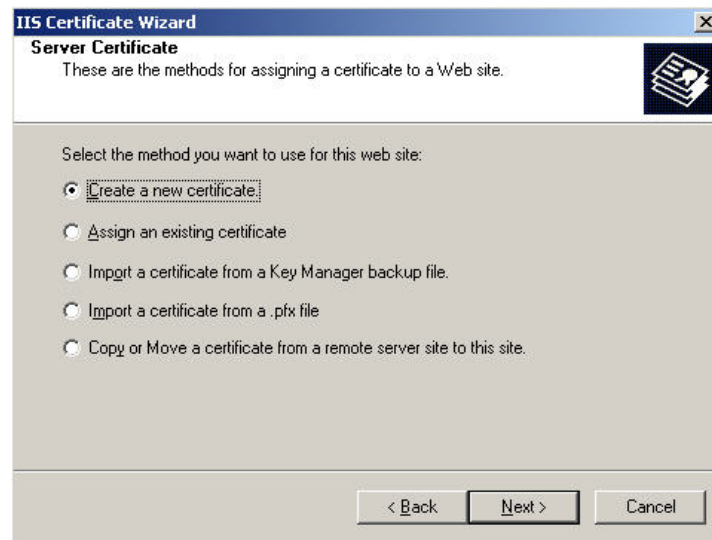
Slika 14

- Otvoriti **Properties** prozor sajta za koji se kreira CSR (desnim klikom na **Default Website** otvara se meni u kome se bira **Properties**).
- Otvoriti **Directory Security** desnim klikom na **Directory Security** tab.



Slika 15

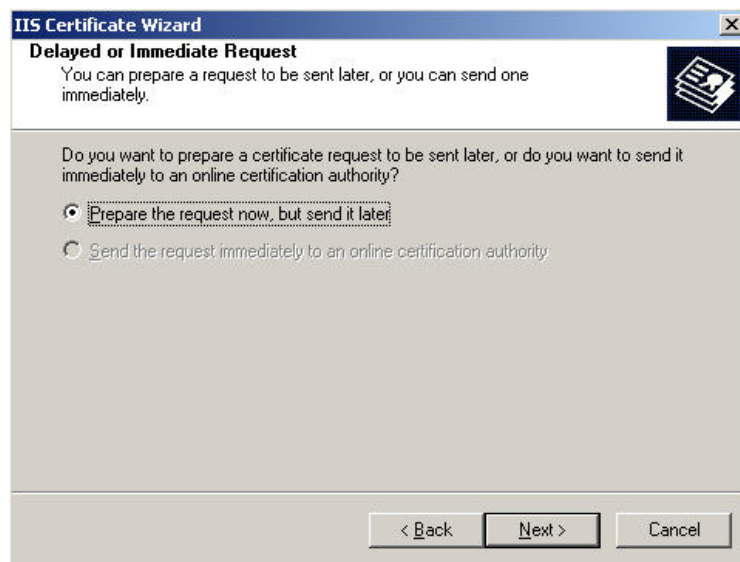
- Klikom na **Server Certificate** otvara se sledeći *Wizard*:



Slika 16

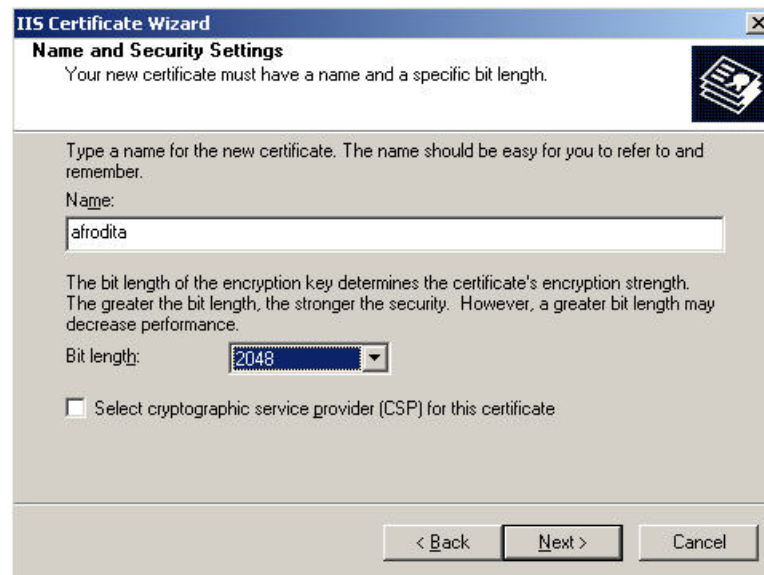
- Kliknuti **Create a new certificate**, a zatim **Next**.

Napomena: Ukoliko se ne dobije prikaz kao na slici 16, koji dozvoljava kreiranje novog zahteva, najverovatnije je da sajt već poseduje SSL sertifikat. U tom slučaju, koristiti postupak koji omogućava da se kreira zahtev za potpisivanje novog sertifikata, a da se ne ukloni postojeći sertifikat. Uputstvo se nalazi na adresi https://support.comodo.com/index.php?_m=knowledgebase&_a=viewarticle&kbarticleid=456.



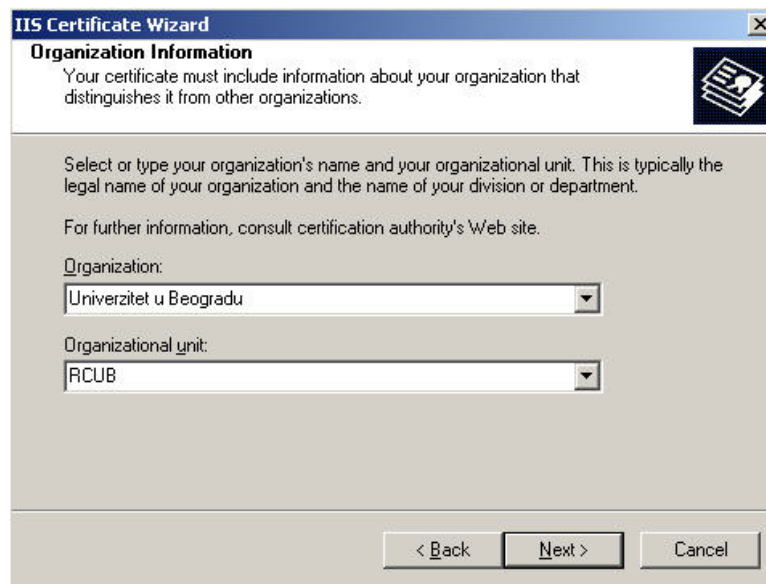
Slika 17

- Izabrati **Prepare the request** i kliknuti **Next**.



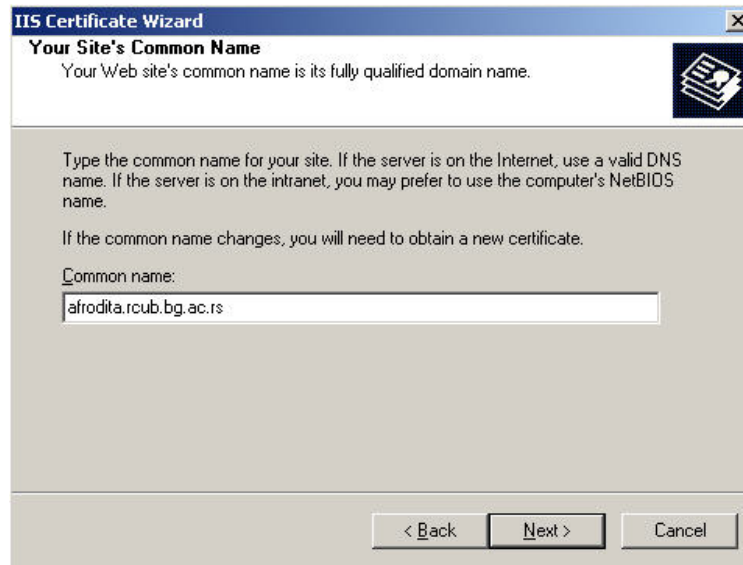
Slika 18

- Uneti naziv za sertifikat. Naziv ima samo lokalno značenje, i treba da asocira na konkretan sertifikat kada se koristi više njih na domenu.
- Za **Bit length** izabrati **2048**, a zatim kliknuti **Next**.



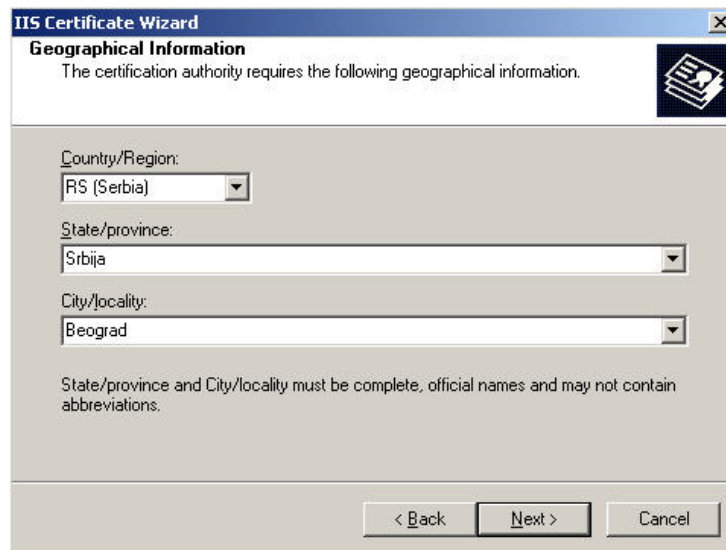
Slika 19

- Uneti **Organization** (pun naziv institucije) i **Organization Unit** (naziv organizacione jedinice). Od ove pozicije pa nadalje, sve tražene podatke unositi tačno i u skladu sa podacima koji su podneti u procesu registracije (npr. koristiti zvaničan naziv institucije pod kojim je ona registrovana na portalu i sl.).
- Kliknuti **Next**.



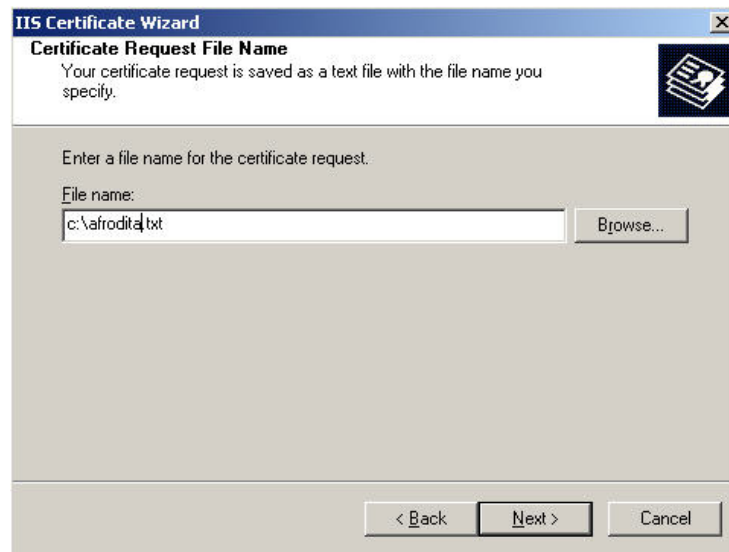
Slika 20

- U polje **Common Name** uneti puno DNS ime servera za koji se traži sertifikat. Kliknuti **Next**.



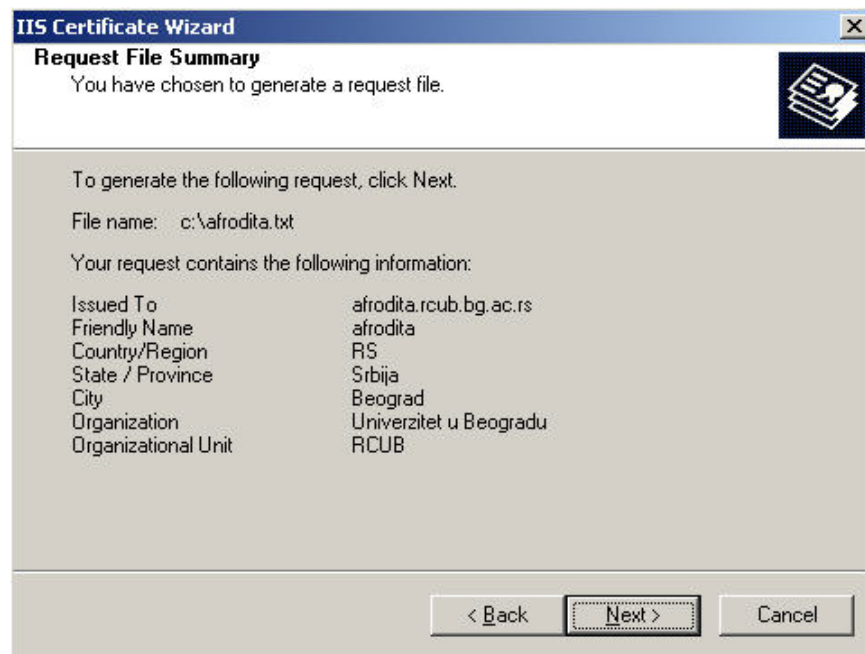
Slika 21

- Uneti vrednosti 2-značnu skraćenicu za Srbiju, naziv države i grada u polja **Country**, **State** and **City**.
- Kliknuti **Next**.



Slika 22

- Uneti naziv fajla (koristiti ekstenziju *txt*) i direktorijum u kome će biti smešten zahtev za sertifikatom. Kliknuti **Next**.



Slika 23

- Proveriti unete podatke. U slučaju greške, kliknuti **Back** i uneti odgovarajuće izmene. Po uspešnoj proveri, kliknuti **Next**.
- Dobijeni zahtev za sertifikatom se nalazi u *.txt* fajlu između redova „-----BEGIN CERTIFICATE REQUEST-----” i „-----END CERTIFICATE REQUEST-----” uključujući i njih.

- Kliknuti **Next**.

Sačuvati privatni ključ na sledeći način:

- Otići na: **Certificates snap in** u okviru MMC (*Microsoft Management Console*)
- Izabrati **Requests**
- Izabrati **All tasks**
- Izabrati **Export**

Napomena: password kojim je zaštićen privatni ključ, kao i sam ključ bi trebalo da budu poznati samo administrativnom kontaktu institucije.

5.4 Podnošenje zahteva

Zahtev za sertifikatom, u ime institucije korisnika TCS servisa, podnosi ovlašćena osoba institucije (administrativni kontakt) određena u toku registracije institucije i podnošenja zahteva za korištenje TCS servisa. Zahtev se podnosi mailom na adresu tcs@amres.ac.rs. Pri tome se u telo e-mail poruke kao tekst kopira sadržaj između redova „-----BEGIN CERTIFICATE REQUEST-----” i „-----END CERTIFICATE REQUEST-----” iz fajla u kome je sačuvan zahtev za potpisivanjem sertifikata (*myserver.csr* na *Linux* serverima, odnosno *ime_fajla.txt* na *Microsoft IIS* serverima). Fajl sa ekstenzijom *.csr*, kao i onaj sa ekstenzijom *.txt* može da se otvori bilo kojim tekstualnim editorom. Zahtev za potpisivanjem sertifikata se nalazi u *base-64* kodiranom PEM formatu između redova „-----BEGIN CERTIFICATE REQUEST-----” i „-----END CERTIFICATE REQUEST-----” uključujući ti njih.

Primer sadržaja fajla *myserver.csr*:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDITCCAgkCAQAwZjELMAkGA1UEBhMCU1MxEDAQOBgNVBACTB0Jlb2dyYWQxHzAd
BgNVBAoTF1VuaXZlcnNpdHkgb2YgQmVsZ3JhZGUxDTALBgNVBAsTBFBFJDVUIxJTAj
BgNVBAMTHG9wZW52cG4tc2VydMvYLnJjdWlUyYmcuYWMucnMwggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQDv+mcWyeT8ZS7SCjs8zAbXPsvx8YHjrk48H14M
+Yf9eXND2Z/FLiVYTax/S59YuFKilv1mkxEFusspaDCnPs8dQovX2UYHZt9tNGXS
fzk2x7rviI/mGly3o15Y0QH96Ov6+R2aGBAPcimjLtWh17KaAE0Xon4V6QWExNU6
0TkP73/krflXTehJh2GdT7OvPCbJnwXUTN/RxLqETyL/B1bQr0mmi7Kqdy3xQLJM
ng5kBQ+fkD9fq4YiQMIIAu0sxpYcX6sXIuzWRUuim0oHkCYuIxX8xxVL60oFfAqa
OiQyonjCG7ZJXngh7OteSeJEETCniy+fzzweedv62kLTjMx5Osw6FzUMuXCugzg
8kDH3DS607iv4Gn3IhYk/aV6H6hJtwUZaA/vsst6MvM6SJ0eePZbpvGbYbnUAXU
FL/LWVThxqWXmz33pPPHzUCIP5HZf4vhGcZHbTmj6nPJ2edFYgtCWLyB0TCa8hi6
o2CReo0kuS2oBxEpTx7dsszyPG4lqo0VUHxv5s3IXf4151PQQQ==
-----END CERTIFICATE REQUEST-----
```

Takođe, u mejlu koji se upućuje na adresu tcs@amres.ac.rs je potrebno navesti i sledeće podatke:

- pun zvaničan naziv institucije pod kojim je ona registrovana na portalu registra domena [ac.rs](https://registar.ac.rs) (<https://registar.ac.rs>), i adresu institucije, tj. ulicu i broj, poštanski broj i ime grada u kojoj se institucija nalazi.

- sva DNS imena servera koje pokriva sertifikat koji se nalazi u zahtevu za potpisivanje (ako se navodi više simboličnih imena u jednom sertifikatu, naglasiti koje ime je primarno).
- period važenja sertifikata za koji se podnosi zahtev – 1, 2 ili 3 godine.
- serverski softver korišćen za generisanje zahteva.
- podatke o ovlašćenoj osobi/administrativnom kontaktu institucije koja podnosi zahtev.
- e-mail adresu na koju će biti poslat potpisani sertifikat.

Posle uspešne provere podataka iz zahteva od strane AMRES-a, sertifikat će biti izdat i poslat na mejl adresu koja je navedena u zahtevu za sertifikatom.

6 Instalacija sertifikata

Serverski SSL sertifikat zajedno sa fajlom u kome se nalazi njegov *ca-chain* stiže na mejl poručioaca u jednom *.zip* fajlu. Ime *.zip* fajla može biti ili sedmocifreni broj (na primer 9026687.zip) ili primarno DNS ime servera definisano u zahtevu za potpisivanjem sertifikata (npr. sf.bg.ac.rs.zip).

Dobijeni sertifikat instalirati na server i server konfigurisati tako da server, sem svog SSL sertifikata, šalje i *ca-chain* kojim se uspostavlja lanac poverenja za taj sertifikat. TERENA SSL CA sertifikat kojim se potpisuju svaki SSL serverski sertifikati je potpisan od strane *UserTrust* prelaznog sertifikacionog tela koje je potpisano od strane *AddTrust External root* sertifikacionog tela. Prelazni i *root* sertifikati su smešteni zajedno i nalaze se u *ca-chain* fajlu. Mada većina *ssl* klijenata ima preinstalirane najšire zastupljene *root* sertifikate, da bi serverski SSL sertifikat mogao da se proveriti, klijentu je potreban i podatak o prelaznom sertifikatu koji je potpisan CA *root* sertifikatom.

U nastavku je opisan postupak instalacije serverskih SSL sertifikata za najšire zastupljene servise/serve u AMRESu – sertifikata za zaštitu servisa/servera na Linux platformam (sa Apache/mod_ssl paketom) i Microsoft IIS serverima.

Ako je institucija zahtevala TERENA Single SSL Certificate, treba pratiti postupak za odgovarajuće okruženje iz (isključivo) jednog od ponuđenih podpoglavlja.

Ako je institucija zahtevala TERENA Multi-Domain SSL Certificate, što znači da se u instituciji koristi platforma na kojoj je podignuto više servisa na istom serveru (pri čemu svaki od servisa koristi svoje DNS ime), treba proći kroz sva potpoglavlja za pojedinačne servise.

6.1.1 Web server pod Linux–om (Apache/mod_ssl)

Raspakovati dobijeni *.zip* fajl, čime će se dobiti dva fajla sa ekstenzijama *.crt* i *.ca-bundle*. U fajlu sa *.crt* ekstenzijom nalazi se sertifikat servera, dok se u fajlu sa ekstenzijom *.ca-bundle* nalazi lanac sertifikata za uspostavljanje lanca poverenja za izdati serverski sertifikat. Za Linux distribucije nastale od Redhat-a (CentOS, Fedora, Mandriva) uobičajeno je da se sertifikati i ključevi čuvaju na sledećim lokacijama, respektivno:

```
unzip 9026687.zip

/etc/pki/tls/certs/
/etc/pki/tls/private/
```

Editovati konfiguracioni fajl *ssl.conf* i uneti odgovarajuće putanje do sertifikata servera, lanca sertifikata, kao i ključa servera:

```
#(putanja do serverskog SSL sertifikata)
SSLCertificateFile /etc/pki/tls/certs/9026687.crt

#(putanja do privatnog ključa servera)
SSLCertificateKeyFile /etc/pki/tls/private/myserver.key

#(putanja do prelaznog sertifikata)
SSLCertificateChainFile /etc/pki/tls/certs/9026687.ca-bundle
```

Na kraju je potrebno restartovati web server:

```
/etc/init.d/httpd stop
/etc/init.d/httpd start
```

U slučaju da želite da vidite instaliran sertifikat, to možete da uradite pomoću sledeće komande:

```
openssl x509 -in 9026687.crt -text
```

Kada se instalira *Multi-Domen SSL Sertifikat*, preći na sledeći servis koji se štiti sertifikatom i u njegov pripadajući konfiguracioni fajl ubaciti podatke o putanji do direktorijuma u kome se sertifikati nalaze.

6.1.2 Java Web server (Tomcat, JBoss...)

Raspakivanjem *.zip* fajla, dobiće se tri fajla koja sadrže sertifikate. Sertifikati moraju da se importuju u odgovarajućem redosledu: koreni (*Root*), prelazni (*Intermediate CA*) i serverski sertifikati (*domain/site certificate*).

Sertifikati se importuju korišćenjem sledećih *keytool* komandi:

```
#importovati koreni (root) sertifikat
keytool -import -trustcacerts -alias root -file (ROOT CERTIFICATE FILE NAME) -
keystore domain.key

#importovati prelazni sertifikat
keytool -import -trustcacerts -alias INTER -file (INTERMEDIATE CA FILE NAME) -
keystore domain.key

#importovati serverski SSL sertifikat
#yyy je alias odabran prilikom generisanja CSR zahteva za sertifikatom
keytool -import -trustcacerts -alias yyy (where yyy is the alias specified during
CSR creation) -file domain.crt -keystore domain.key
```

Obratiti pažnju da se prilikom poslednjeg importa mora koristiti *alias* koji je odabran prilikom generisanja zahteva za sertifikatom, nakon čega *keytool* potvrđuje uparivanje porukom: "*Certificate reply was installed in keystore*".

Kada se instalira *Multi-Domen SSL Sertifikat*, preći na sledeći servis koji se štiti sertifikatom i u njegov pripadajući konfiguracioni fajl ubaciti podatke o putanji do direktorijuma u kome se sertifikati nalaze.

6.1.3 RADIUS server

Ovo uputstvo opisuje postupak instalacije i upotrebe serverskog SSL sertifikata na RADIUS serveru (koji je podignut na *FreeRadius* platformi) koji koristi EAP-TTLS protokol za autentifikaciju korisnika. Opisano okruženje standardno se koristi u AMRESu kada se RADIUS server u instituciji članici uključuje u eduroam servis.

Obezbediti serverski sertifikat na način opisan u poglavlju 5 AMRES usluga izdavanja TCS sertifikata. Dobijeni *.zip* fajl u kome se nalazi sertifikat (npr. *8866644.zip*) prebaciti na RADIUS server (npr. korišćenjem programa WinSCP) u direktorijum */etc/raddb/certs*, u kome se obično drže sertifikati vezani za FreeRadius server. Isti direktorijum koristiti za čuvanje privatnog serverskog ključa koji je generisan u procesu zahtevanja datog serverskog sertifikata (pretpostavimo da se privatni ključ čuva u fajlu *privatnikljuc.key*). Koristiti sledeće komande:

```
$(prebaciti zip fajl u odgovarajući direktorijum)
cp 8866644.zip /etc/raddb/certs/8866644.zip

$(prebaciti privatni ključ )
cp privatnikljuc.key /etc/raddb/certs/privatnikljuc.key

$(raspakovati zip fajl)
unzip 8866644.zip
```

Raspakivanjem *.zip* fajla, dobijaju se dva fajla sa ekstenzijama *.crt* i *.ca-bundle*. U fajlu sa *.crt* ekstenzijom nalazi se sertifikat servera. Sertifikat iz *.crt* fajla prebaciti u *.pem* format sledećim komandama:

```
openssl x509 -in 8866644.crt -out 8866644.der -outform DER
openssl x509 -in 8866644.der -inform DER -out 8866644.pem -outform PEM
```

Privatni ključ servera mora imati ograničen pristup, što mu obezbeđuje „r-----“, (read only) dozvola. Postaviti „r-----“, (read only) dozvolu komandom:

```
chmod 400 /etc/raddb/certs/privatnikljuc.key
```

Da bi autentifikacija kroz *ttls* protokol mogla da funkcioniše, potrebno je prvo konfigurisati *ttls* u konfiguracionom fajlu *eap.conf*. Editovati konfiguracioni fajl *eap.conf* i upisati informacije o sertifikatima sledećim komandama:

```
certdir = /etc/raddb/certs
cadir = /etc/raddb/certs
private_key_file = /etc/raddb/certs/privatnikljuc.key
certificate_file = /etc/raddb/certs/8866644.pem
CA_file = /etc/raddb/certs/8866644.ca-bundle
```

Sada je potrebno restartovati RADIUS proces da bi promene u konfiguraciji postale aktivne:

```
killall radiusd
radiusd
```

Da bi klijent uspešno proverio sertifikat servera, mora da instalira sam sertifikat na svoj računar.

6.1.4 Email na Linux serveru

Postupak instalacije sertifikata za *email* servis na Linux serveru je sličan postupku instalacije sertifikata za *web* server opisan u poglavlju 6.1.1 Web server pod Linux–om (Apache/mod_ssl), samo što se konfiguriraju drugi konfiguracioni fajlovi. Odgovarajući konfiguracioni fajl se bira u zavisnosti od konkretnog email softvera koji se koristi za razmenu maila. Generalno pravilo je da se u svaki konfiguracioni fajl servisa, koji se obezbeđuje sertifikatom, moraju uneti putanje do SSL serverskog i prelaznog sertifikata, kao i privatnog ključa (koji odgovara javnom ključu iz sertifikata).

Sledeće komande pokrivaju slučaj Linux servera na kome je instaliran *postfix* paket da bi omogućio razmenu mailova po **smtp** protokolu i *dovecot* paket za preuzimanje poruka preko *imap* i *pop3* protokola od strane korisnika.

- Za **postfix smtp** server, editovati konfiguracioni fajl **main.cf** (*/etc/postfix/main.cf*):

```
smtpd_use_tls = yes

# (putanja do prelaznog sertifikata)
smtpd_tls_CAfile = /etc/pki/tls/certs/8866644.ca-bundle

# (putanja do direktorijuma u kome su sertifikati)
smtpd_tls_CApath = /etc/pki/tls/certs

# (putanja do sertifikata servera)
smtpd_tls_cert_file = /etc/pki/tls/certs/8866644.crt

# (putanja do privatnog ključa)
smtpd_tls_key_file = /etc/pki/tls/private/myserver.key
```

- Za **imap** i **pop3** na serveru editovati konfiguracioni fajl **dovecot.conf** (*/etc/dovecot.conf*):

```
# (putanja do sertifikata servera)
ssl_cert_file= /etc/pki/tls/certs/8866644.crt

# (putanja do privatnog ključa servera)
ssl_key_file = /etc/pki/tls/private/myserver.key

# (putanja do prelaznog sertifikata)
ssl_ca_file = /etc/pki/tls/certs/8866644.ca-bundle
```

Kada se instalira *Multi-Domen SSL Certifikat*, preći na sledeći servis koji se štiti sertifikatom i u njegov pripadajući konfiguracioni fajl ubaciti podatke o putanji do direktorijuma u kome se sertifikati nalaze.

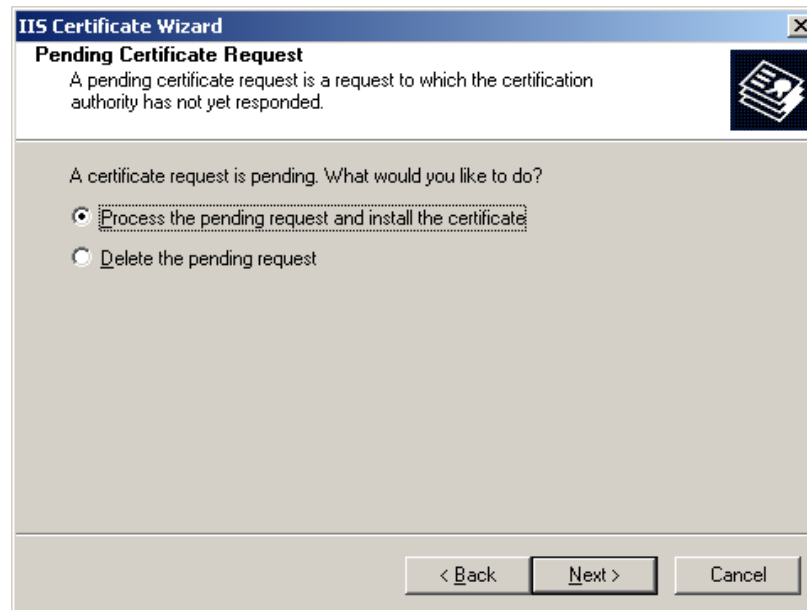
6.1.5 Microsoft IIS 5.x i 6.x

U ovom slučaju, ime fajla u kome se nalazi sertifikat servera može biti oblika ime_domena.cer. Sadrži koreni (*Root*), prelazni (*Intermediate CA*) i serverski sertifikat.

Instalacija sertifikata se sastoji od prolaza kroz sledeće korake:

- Otvoriti *Control Panel* i izabrati **Administrative Tools**.

- Startovati **Internet Services Manager** čime se ulazi u *wizard* sa slike 14.
- Desnim klikom miša izabrati *website* i levim klikom **Properties**.
- Izabrati **Directory Security** tab u *wizard*-u prikazanom na slici 15.
- Izabrati **Server Certificate**.



Slika 26

- Izabrati **Process the Pending Request and Install the Certificate**. Kliknuti **Next**.
- Uneti putanju do lokacije sertifikata servera. Kliknuti **Next**.
- Proveriti ispravnost prikazanih podataka na ekranu. Kliknuti **Next**.
- Prikazaće se potvrda (**confirmation screen**). Kliknuti **Next**.
- Stopirati i startovati odgovarajući web sajt.

Dodatak A Lanac TCS sertifikata

U nastavku je pokazan lanac CA sertifikata za TCS serverske sertifikate. Prvi u nizu je sertifikat korenog certifikacionog tela (*root CA*), AddTrunst External CA Root. Njime je potpisan sledeći sertifikat u lancu. To je sertifikat prelaznog certifikacionog tela (*intermediate CA*), UTN-USERFirst-Hardware. Na kraju je sertifikat TERENA certifikacionog tela, TERENA SSL CA (potpisan navedenim prelaznim sertifikatom).

Sertifikat korenog certifikacionog tela je samopotpisan, pa su vrednosti polja *Issuer* i *Subjest* iste. U polju *Issuer*, sertifikata prelaznog certifikacionog tela, nalaze se podaci korenog certifikacionog tela, kao tela koje je izdalo sertifikat. TERENA CA sertifikat je izdat od strane prelaznog certifikacionog tela, čiji se podaci nalaze u polju *Issuer*.

AddTrust External CA Root (koreni sertifikat):

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 1 (0x1)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=SE, O=AddTrust AB, OU=AddTrust External TTP Network, CN=AddTrust
External CA Root
    Validity
      Not Before: May 30 10:48:38 2000 GMT
      Not After : May 30 10:48:38 2020 GMT
    Subject: C=SE, O=AddTrust AB, OU=AddTrust External TTP Network,
CN=AddTrust External CA Root
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (2048 bit)
      Modulus (2048 bit):
        00:b7:f7:1a:33:e6:f2:00:04:2d:39:e0:4e:5b:ed:
        1f:bc:6c:0f:cd:b5:fa:23:b6:ce:de:9b:11:33:97:
        a4:29:4c:7d:93:9f:bd:4a:bc:93:ed:03:1a:e3:8f:
        cf:e5:6d:50:5a:d6:97:29:94:5a:80:b0:49:7a:db:
        2e:95:fd:b8:ca:bf:37:38:2d:1e:3e:91:41:ad:70:
        56:c7:f0:4f:3f:e8:32:9e:74:ca:c8:90:54:e9:c6:
        5f:0f:78:9d:9a:40:3c:0e:ac:61:aa:5e:14:8f:9e:
        87:a1:6a:50:dc:d7:9a:4e:af:05:b3:a6:71:94:9c:
        71:b3:50:60:0a:c7:13:9d:38:07:86:02:a8:e9:a8:
        69:26:18:90:ab:4c:b0:4f:23:ab:3a:4f:84:d8:df:
```

```

ce:9f:e1:69:6f:bb:d7:42:d7:6b:44:e4:c7:ad:ee:
6d:41:5f:72:5a:71:08:37:b3:79:65:a4:59:a0:94:
37:f7:00:2f:0d:c2:92:72:da:d0:38:72:db:14:a8:
45:c4:5d:2a:7d:b7:b4:d6:c4:ee:ac:cd:13:44:b7:
c9:2b:dd:43:00:25:fa:61:b9:69:6a:58:23:11:b7:
a7:33:8f:56:75:59:f5:cd:29:d7:46:b7:0a:2b:65:
b6:d3:42:6f:15:b2:b8:7b:fb:ef:e9:5d:53:d5:34:
5a:27
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Subject Key Identifier:
AD:BD:98:7A:34:B4:26:F7:FA:C4:26:54:EF:03:BD:E0:24:CB:54:1A
X509v3 Key Usage:
Certificate Sign, CRL Sign
X509v3 Basic Constraints: critical
CA:TRUE
X509v3 Authority Key Identifier:
keyid:AD:BD:98:7A:34:B4:26:F7:FA:C4:26:54:EF:03:BD:E0:24:CB:54:1A
DirName:/C=SE/O=AddTrust AB/OU=AddTrust External TTP
Network/CN=AddTrust External CA Root
serial:01

Signature Algorithm: sha1WithRSAEncryption
b0:9b:e0:85:25:c2:d6:23:e2:0f:96:06:92:9d:41:98:9c:d9:
84:79:81:d9:1e:5b:14:07:23:36:65:8f:b0:d8:77:bb:ac:41:
6c:47:60:83:51:b0:f9:32:3d:e7:fc:f6:26:13:c7:80:16:a5:
bf:5a:fc:87:cf:78:79:89:21:9a:e2:4c:07:0a:86:35:bc:f2:
de:51:c4:d2:96:b7:dc:7e:4e:ee:70:fd:1c:39:eb:0c:02:51:
14:2d:8e:bd:16:e0:c1:df:46:75:e7:24:ad:ec:f4:42:b4:85:
93:70:10:67:ba:9d:06:35:4a:18:d3:2b:7a:cc:51:42:a1:7a:
63:d1:e6:bb:a1:c5:2b:c2:36:be:13:0d:e6:bd:63:7e:79:7b:
a7:09:0d:40:ab:6a:dd:8f:8a:c3:f6:f6:8c:1a:42:05:51:d4:
45:f5:9f:a7:62:21:68:15:20:43:3c:99:e7:7c:bd:24:d8:a9:
91:17:73:88:3f:56:1b:31:38:18:b4:71:0f:9a:cd:c8:0e:9e:
8e:2e:1b:e1:8c:98:83:cb:1f:31:f1:44:4c:c6:04:73:49:76:
60:0f:c7:f8:bd:17:80:6b:2e:e9:cc:4c:0e:5a:9a:79:0f:20:
0a:2e:d5:9e:63:26:1e:55:92:94:d8:82:17:5a:7b:d0:bc:c7:
8f:4e:86:04

```

UTN-USERFirst-Hardware (prelazni sertifikat):

```

Certificate:
Data:
Version: 3 (0x2)
Serial Number:
48:4b:ac:f1:aa:c7:d7:13:43:d1:a2:74:35:49:97:25
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=SE, O=AddTrust AB, OU=AddTrust External TTP Network, CN=AddTrust
External CA Root
Validity
Not Before: Jun 7 08:09:10 2005 GMT
Not After : May 30 10:48:38 2020 GMT
Subject: C=US, ST=UT, L=Salt Lake City, O=The USERTRUST Network,
OU=http://www.usertrust.com, CN=UTN-USERFirst-Hardware
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (2048 bit)
Modulus (2048 bit):
00:b1:f7:c3:38:3f:b4:a8:7f:cf:39:82:51:67:d0:

```

```
6d:9f:d2:ff:58:f3:e7:9f:2b:ec:0d:89:54:99:b9:
38:99:16:f7:e0:21:79:48:c2:bb:61:74:12:96:1d:
3c:6a:72:d5:3c:10:67:3a:39:ed:2b:13:cd:66:eb:
95:09:33:a4:6c:97:b1:e8:c6:ec:c1:75:79:9c:46:
5e:8d:ab:d0:6a:fd:b9:2a:55:17:10:54:b3:19:f0:
9a:f6:f1:b1:5d:b6:a7:6d:fb:e0:71:17:6b:a2:88:
fb:00:df:fe:1a:31:77:0c:9a:01:7a:b1:32:e3:2b:
01:07:38:6e:c3:a5:5e:23:bc:45:9b:7b:50:c1:c9:
30:8f:db:e5:2b:7a:d3:5b:fb:33:40:1e:a0:d5:98:
17:bc:8b:87:c3:89:d3:5d:a0:8e:b2:aa:aa:f6:8e:
69:88:06:c5:fa:89:21:f3:08:9d:69:2e:09:33:9b:
29:0d:46:0f:8c:cc:49:34:b0:69:51:bd:f9:06:cd:
68:ad:66:4c:bc:3e:ac:61:bd:0a:88:0e:c8:df:3d:
ee:7c:04:4c:9d:0a:5e:6b:91:d6:ee:c7:ed:28:8d:
ab:4d:87:89:73:d0:6e:a4:d0:1e:16:8b:14:e1:76:
44:03:7f:63:ac:e4:cd:49:9c:c5:92:f4:ab:32:a1:
48:5b
Exponent: 65537 (0x10001)
X509v3 extensions:
  X509v3 Authority Key Identifier:
    keyid:AD:BD:98:7A:34:B4:26:F7:FA:C4:26:54:EF:03:BD:E0:24:CB:54:1A

  X509v3 Subject Key Identifier:
    A1:72:5F:26:1B:28:98:43:95:5D:07:37:D5:85:96:9D:4B:D2:C3:45
  X509v3 Key Usage: critical
    Certificate Sign, CRL Sign
  X509v3 Basic Constraints: critical
    CA:TRUE
  X509v3 CRL Distribution Points:
    URI:http://crl.usertrust.com/AddTrustExternalCARoot.crl

Signature Algorithm: sha1WithRSAEncryption
3c:ec:7b:e0:ae:a3:0e:96:6d:30:d7:85:c6:d2:68:5b:45:5a:
82:a6:34:0f:b0:c9:92:23:5e:11:6d:08:11:b2:74:09:23:3a:
35:25:73:58:5e:ca:b9:7c:28:fa:47:ec:f9:a0:03:58:50:b6:
53:ef:8c:db:39:e4:67:e9:d8:ca:28:46:d4:a7:e0:f5:38:75:
f8:e7:cb:5c:bf:1d:11:3c:6a:40:9b:2d:44:56:d3:f7:ff:05:
28:32:0c:15:c8:64:45:93:e8:21:24:8f:2d:da:7a:84:7b:4f:
cf:cd:b2:25:7c:77:10:d3:94:d1:04:91:a8:25:1c:09:22:0f:
7d:44:35:11:14:ef:af:00:fe:5e:ea:5f:8e:b0:d9:92:59:ba:
fc:13:96:a0:18:01:56:ce:da:f6:28:0b:b1:af:dd:5c:4f:5c:
b2:f3:8f:5a:71:cf:ed:18:ad:63:88:1d:8e:95:f7:ea:95:e7:
1f:ad:90:b8:84:08:47:85:7f:22:2f:1a:1d:48:30:d6:4c:08:
d8:37:19:67:32:2b:eb:5c:d0:b2:fc:6e:57:9f:04:35:5e:90:
00:7e:11:c7:de:13:2a:cd:a4:6d:45:26:c7:88:56:a0:f0:6a:
f7:d8:e7:fc:27:7e:67:08:d0:bd:fa:b6:c3:61:02:01:65:b9:
b8:2f:cf:5a
```

TERENA SSL CA (TERENA CA sertifikat):

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      4b:c8:14:03:2f:07:fa:6a:a4:f0:da:29:df:61:79:ba
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=US, ST=UT, L=Salt Lake City, O=The USERTRUST Network,
    OU=http://www.usertrust.com, CN=UTN-USERFirst-Hardware
    Validity
```

```
Not Before: May 18 00:00:00 2009 GMT
Not After : May 30 10:48:38 2020 GMT
Subject: C=NL, O=TERENA, CN=TERENA SSL CA
Subject Public Key Info:
  Public Key Algorithm: rsaEncryption
  RSA Public Key: (2048 bit)
    Modulus (2048 bit):
      00:c3:e3:48:c4:2f:5c:c1:cb:a9:99:fd:1b:a2:83:
      5d:8a:3d:ad:3a:d0:e2:a4:43:1f:4d:0e:fe:35:25:
      30:a5:69:1b:c4:e8:e5:c1:8f:54:7e:e1:6a:a2:9a:
      5c:5c:de:3d:fc:02:ce:96:b8:5f:8f:83:5b:cc:60:
      40:90:f8:e4:b6:3a:25:9c:5f:14:51:ec:b1:e7:af:
      9e:50:a1:31:55:c7:02:bd:ac:52:8a:7f:35:8e:82:
      fa:84:ad:15:fe:a2:7f:83:10:3a:55:53:94:2c:01:
      16:74:94:54:63:28:a3:f2:5b:29:3d:94:88:80:20:
      e2:14:59:21:19:b4:a4:98:e1:60:e6:f2:eb:a2:80:
      83:43:e0:ad:68:f3:79:19:8b:68:43:51:3f:8a:9b:
      41:85:0c:35:8c:5d:b5:f1:b6:e5:a7:c3:83:b5:6b:
      23:6f:d4:a5:eb:50:e5:94:f1:4a:5f:ee:27:4b:14:
      12:15:24:4c:0d:cf:62:8d:b7:00:21:ad:3a:32:0f:
      58:0b:5f:1e:9b:d1:df:9d:8e:a9:19:35:50:2f:41:
      a9:ad:3b:c6:e0:45:b2:53:39:7f:21:bf:22:1a:87:
      5c:34:ae:52:6f:07:7d:a2:0b:4e:9f:2b:79:a6:7d:
      13:dd:f5:7f:83:7c:2f:5a:5d:77:78:78:91:a0:14:
      bf:7d
    Exponent: 65537 (0x10001)
X509v3 extensions:
  X509v3 Authority Key Identifier:
    keyid:A1:72:5F:26:1B:28:98:43:95:5D:07:37:D5:85:96:9D:4B:D2:C3:45

  X509v3 Subject Key Identifier:
    0C:BD:93:68:0C:F3:DE:AB:A3:49:6B:2B:37:57:47:EA:90:E3:B9:ED
  X509v3 Key Usage: critical
    Certificate Sign, CRL Sign
  X509v3 Basic Constraints: critical
    CA:TRUE, pathlen:0
  X509v3 Certificate Policies:
    Policy: 1.3.6.1.4.1.6449.1.2.2.29

  X509v3 CRL Distribution Points:
    URI:http://crl.usertrust.com/UTN-USERFirst-Hardware.crl

  Authority Information Access:
    CA Issuers - URI:http://crt.usertrust.com/UTNAddTrustServer_CA.crt
    OCSP - URI:http://ocsp.usertrust.com

Signature Algorithm: sha1WithRSAEncryption
4e:23:ee:48:9c:f6:85:8b:71:c4:0a:6e:73:93:72:c0:3a:8e:
80:8a:d9:b3:ca:b2:d4:01:9c:28:cf:f2:5c:0e:21:44:93:0b:
b6:1a:21:e3:98:01:94:0e:67:49:81:1e:be:3d:0d:4e:60:da:
ef:a0:31:4e:95:ef:f3:dd:7a:5a:82:20:43:b6:a1:63:43:b3:
50:69:43:62:4b:56:62:b0:34:8a:b9:13:43:59:93:ec:14:79:
88:f3:48:93:e8:9d:c9:fa:87:72:0c:6b:56:a0:c3:15:8d:68:
a5:87:1f:71:2d:e6:5a:6d:3c:69:71:40:04:55:dc:a0:43:94:
20:45:38:78:d7:bd:8a:d8:39:c6:df:09:b7:5a:9a:a9:03:b8:
28:10:78:cd:bf:01:1b:5a:11:3e:38:f4:d8:1b:34:79:cf:33:
d2:01:fd:ac:98:cd:6d:47:11:90:4c:bb:b9:5b:d8:70:e7:d5:
af:b6:cc:c4:86:e6:75:c0:9e:29:b6:2b:0f:2a:a5:69:02:0d:
e3:e9:a2:b4:5d:c0:f3:ce:2c:6a:85:38:76:61:c6:49:82:ab:
51:b3:82:a6:b9:41:98:28:98:fb:6b:fe:8a:16:ff:31:7e:54:
47:a8:3c:dc:43:26:a9:9b:05:b7:9e:c0:34:43:91:30:d4:32:
```

Dodatak B **SSL protokol**

Sadržaj je dostupan samo na srpskom jeziku u on-line verziji dokumenta na AMRES wikiju
https://www.bpd.amres.ac.rs/doku.php?id=amres_cbp_wiki:start.

Dodatak C **EAP-TTLS**

Sadržaj je dostupan samo na srpskom jeziku u on-line verziji dokumenta na AMRES wikiju
https://www.bpd.amres.ac.rs/doku.php?id=amres_cbp_wiki:start.

7 Reference

- [1] William Stallings, „Network and internetwork security principles and practice“
- [2] Pascal Steichen, “PKI applications, standards and protocols”
http://pst.libre.lu/mssi-luxmbg/p3/02_std-prot-art.html
- [3] <http://www.itu.int/rec/T-REC-X.509-200508-I>
- [4] <https://support.comodo.com/>
- [5] <http://tools.ietf.org/html/rfc2595>
- [6] <http://www.rfc-editor.org/rfc/rfc2487.txt>
- [7] http://en.wikipedia.org/wiki/Public_key_infrastructure
- [8] Stephen A. Thomas, „SSL and TLS essentials: securing the Web“
- [9] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, „Handbook of Applied Cryptography“
<http://www.cacr.math.uwaterloo.ca/hac/>
- [10] Portal registra domena ac.rs <https://registar.ac.rs/DNS-web/pages/home.jsf>

8 Rečnik

CRL	Certificate Revocation List - Lista opozvanih sertifikata
FQDN	Fully Qualified Domain Name
IETF	The Internet Engineering Task Force
IGTF	International Grid Trust Federation
PKI	Public Key Infrastructure
TERENA	The Trans-European Research and Education Networking Association
TCS	TERENA Certificate Service
X.509 standard	ITU-T standard za Infrastrukturu javnih ključeva (PKI). Standard X.509 specificira, između ostalog, standardne formate za digitalne sertifikate , listu opozvanih sertifikata i karakteristike sertifikata
RADIUS	Remote Authentication Dial In User Service