

# Kako koristiti certifikat u radu RADIUS poslužitelja

RADIUS poslužitelji obrađuju zahtjeve koji dolaze putem RADIUS protokola, te u svom radu mogu upotrebljavati certifikate. Certifikati se koriste u slučaju korištenja 802.1x/EAP autentikacijskih procedura EAP-TLS i EAP-TTLS, te sa stanovišta RADIUS poslužitelja služe kako bi se na siguran način zatvorio /kriptirao tunel kojim se prenose autentikacijski parametri.

RADIUS poslužitelji obrađuju zahtjeve koji dolaze putem RADIUS protokola, te u svom radu mogu upotrebljavati certifikate.

Certifikati se koriste u slučaju korištenja 802.1x/EAP autentikacijskih procedura EAP-TLS i EAP-TTLS, te sa stanovišta RADIUS poslužitelja služe kako bi se na siguran način zatvorio/kriptirao tunel kojim se prenose autentikacijski parametri.

## EAP-TLS

EAP-TLS u svom radu koristi isključivo certifikate i smatra se jednim od najsigurnijih autentikacijskih protokola.

Certifikati se koriste kako bi se prvo provjerio sam RADIUS poslužitelj od strane klijenta pri uspostavi kriptiranog tunela između klijenta i RADIUS poslužitelj. Nakon ove provjere slijedi autentikacijska procedura u kojoj se korisnik putem svog klijenta predstavlja svojim certifikatom ([PKI\(link is external\)](#)), a RADIUS poslužitelj obavlja autentikaciju istoga. Uobičajeno je da se korisnički certifikat nalazi na prenosivom mediju kao što su SMART kartice ili sigurne USB memorije.

## EAP-TTLS

EAP-TTLS u svom radu koristi certifikat za uspostavu sigurnog i provjerenoga tunela između klijenta RADIUS poslužitelja koji će provjeriti autentikacijske elemente, slično EAP-TLS proceduri.

Za razliku od EAP-TLS, autentikacijski parametri mogu biti jako različiti (PAP, PEAP, MSCHAP, MSCHAP2, GTC, ...) što je glavna prednost pred EAP-TLS procedurom. Ovo omogućuje da se autentikacijski parametri provjere putem različitih baza podataka, čime se postiže veća fleksibilnost sa stajališta korisnika i same administracije.

Kriptiranje tunela certifikatom obavezan je element autentikacije unutar sustava [eduroam](#), a više o autentikacijskim mehanizmima u tom sustavu moguće je pročitati u članku [Autentikacijski mehanizmi u eduroamu](#).

## Potrebne informacije u radu s certifikatima

Pri radu s certifikatima koriste se sljedeći pojmovi:

- **privatni ključ** - privatni (tajni) ključ kojim je potpisana zahtjev za certifikatom;
- **zahtjev za certifikatom** - tekstualna datoteka u kojoj su navedeni potrebni podaci koji će se naći u samom certifikatu, te je ista potpisana privatnim ključem koji će se koristiti u radu s certifikatom;
- **certifikat** - datoteka u kojoj se nalazi certifikat nastao uporabom datoteke zahtjeva za certifikatom i potpisom odgovarajućim vršnim (root CA) certifikatom. Ova datoteka se koristi u radu uz korištenje privatnog ključa;
- **vršni certifikat (root CA)** - javni certifikat vjerodostojnog izdavatelja certifikata (CA) kojim je potpisana certifikat;
- **povezni certifikati** - datoteka poveznih certifikata s vršnim certifikatom; opisuju nad certifikate (koristi se u strukturiranim certifikatima);

Da bi mogli uspješno implementirati certifikate u rad RADIUS poslužitelja potrebne su nam sljedeće komponente, tj. datoteke:

- **privatni ključ**
- **certifikat**
- **vršni certifikat** (pri radu s EAP-TLS)

Sve navedene datoteke moraju biti odgovarajućeg formata zapisa (uobičajeno se koristi PEM). Više o formatima zapisa certifikata može se pronaći na linku [X.509 Certificate\\_filename\\_extensions](#).

## Načini dobivanja certifikata

U osnovi postoje dva načina dobivanja certifikata: samopotpisani (*selfsigned*) certifikat i certifikat izdan od ovlaštenog izdavatelja. Razlika je u činjenici da današnji klijenti u svojim konfiguracijskim datotekama sa sobom nose vršne certifikate od ovlaštenih izdavatelja certifikata, dok se kod samopotpisanih certifikata vršni samogenerirani CA certifikat mora na neki način postaviti u konfiguraciju klijenta, jer se u suprotnom javlja greška o mogućoj zlouporabi. Također, zbog sigurnosnih i organizacijskih razloga, certifikati koji su potpisani od ovlaštenih izdavatelja imaju veću sigurnosnu vrijednost te se preporučaju u većini slučajeva.

Pri primjeni samopotpisanih certifikata nužno je da vršni CA certifikat bude slobodno dostupan korisnicima kako bi ga mogli prenijeti u svoje klijente.

Postupak izrade samoptisanog certifikata moguće je pronaći na linku [Creating Certificate Authorities and self-signed SSL certificates](#).

Postupak dobivanja certifikata od ovlaštenog izdavatelja može se razlikovati od izdavatelja do izdavatelja, no u osnovi se svodi na:

1. stvaranje privatnog ključa;
2. stvaranje zahtjeva za certifikatom;
3. podnošenje zahtjeva za certifikatom;
4. dobivanje certifikata pod pred definiranim uvjetima;
5. postavljanje certifikata;

Za akademsku zajednicu u Hrvatskoj dostupni su certifikati ovlaštenog izdavatelja putem [TERENA Certificate Service](#) (TCS), koji se mogu zatražiti na linku [Poslužiteljski certifikati](#).

Na gore navedenom linku opisan je i način stvaranja zahtjeva za certifikatom te njegovo unošenje u konfiguraciju. Također je opisan i postupak dobivanja certifikata, kao i uvjeti pod kojima se isti mogu zatražiti, odnosno dobiti.

## Implementacija certifikata u FreeRADIUS poslužitelj

Po dobivanju certifikata potrebno je ažurirati `eap` područje unutar konfiguracijske datoteke (uobičajeno se to područje nalazi u zasebnoj datoteci `eap.conf`). S obzirom da je proces uspostave tunela, kako je objašnjeno na početku, jednak za EAP-TLS i EAP-TTLS, dodavanje certifikata se obavlja samo u podpodručju `tls`.

Prvo je potrebno provjeriti sljedeće postavke:

```
certdir = ${confdir}/certs
cadir = ${confdir}/certs
```

Te nam postavke govore u kojem direktoriju FreeRADIUS poslužitelj očekuje potrebne datoteke s certifikatima. Kako bi osigurali ispravan rad s certifikatima, u te direktorije treba postaviti certifikate kako bi bili dostupni pri pokretanju poslužitelja.

Potom je potrebno podesiti slijedeće postavke:

```
private_key_password = TyfKNYA5Lz
private_key_file = ${certdir}/key-srv.pem
certificate_file = ${certdir}/cert-srv.pem
```

Nakon promjene konfiguracije potrebno je restartati FreeRADIUS poslužitelj.

U slučaju instalacije FreeRADIUS poslužitelja nekim od paketnih sustava, uobičajeno je da se automatski generira samopotpisani certifikat te se isti automatski upisuje u samu konfiguraciju. Kod tako generiranog certifikata u direktoriju `/etc/freeradius/certs` nalazi se **root CA** certifikat (datoteka naziva `root.der`) koji mora biti slobodno dostupan korisnicima.

## Provjera certifikata RADIUS poslužitelja na strani klijenta

Kako bi se spriječila mogućnost zlouporabe sustava metodom [MITM](#) napada, poželjno je da klijent provjerava certifikat RADIUS poslužitelja.

Provjera se obavlja na način da se provjeri izdavatelj certifikata s **root CA** certifikatom kojeg ima klijent na svom popisu te se usporedi CN polje u certifikatu s predefiniranom vrijednošću koju je specificirao održavatelj RADIUS poslužitelja, a zapisana je u samom certifikatu RADIUS poslužitelja.

Ove provjere se definiraju na klijentima u području za certifikate i razlikuju se od klijenta do klijenta.