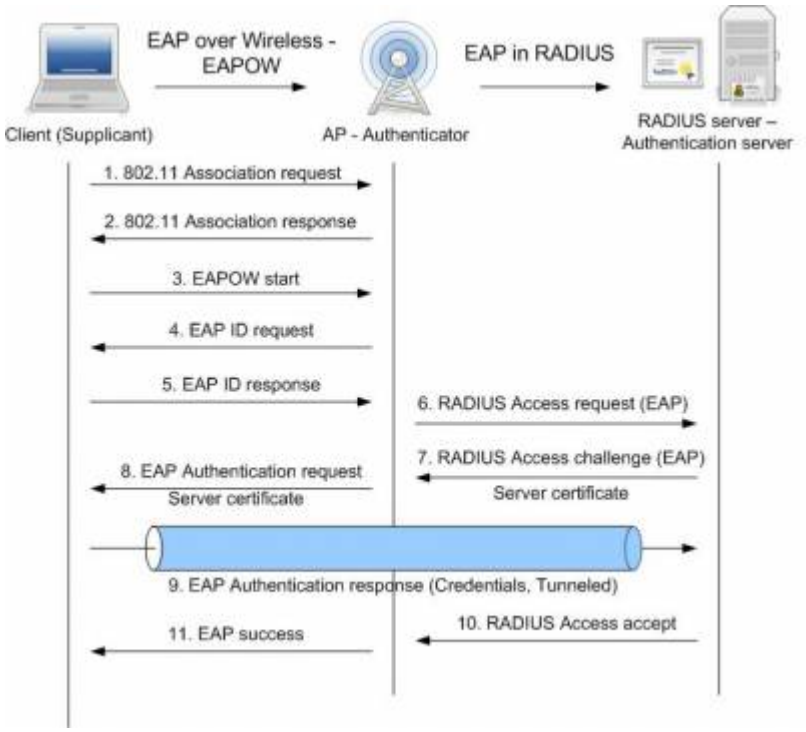
EAP-TTLS protokol

EAP (*Extensible Authentication Protocol*) predstavlja *framework* protokol za autentifikaciju u okviru 802.1x standarda. EAP poruke se prenose po sloju iznad MAC sloja protokola PPP, Ethernet, Token Ring ili 802.11 wireless protokola. U EAP poruke pakuju se paketi protokola za autentifikaciju: TLS, TTLS ili PEAP.

Razmena poruka izme?u klijent i server strane prilikom autentifikacije koriš?enjem EAP-TTLS protokola na wireless mreži je prikazan na slici C.1.



Slika C.1 Razmena poruka EAP-TTLS

1. Klijent zahteva asocijaciju na pristupnu ta?ku (AP - *access point*), ?ime želi da alocira resurse i da se sinhronizuje sa AP-om. U toj poruci šalje informacije o svojoj NIC (*Network Interface Card*) kartici (protoke koje ona podržava) i SSID (*Service Set Identifier*) mreže na koju želi da se poveže.
2. AP odgovara *Association Response* porukom u kojoj prihvata ili odbija zahtev za asocijacijom. Ako odlu?i da prihvati zahtev, AP alocira memorijski prostor i generiše *Association ID*, koji prosle?uje u poruci.
3. Klijent šalje prvu EAP poruku, odnosno zahtev, ?ime po?inje EAP-TTLS autentifikacija.
4. AP zaheva podatke o identitetu klijenta.
5. Klijent šalje svoje kredencijale u odgovoru na prethodu poruku, ali ne šalje svoj pravi identitet, jer je veza sa AP još nezašti?ena, tj. na njoj se ne koristi nikakva enkripcija za zaštitu podataka. Klijent šalje samo svoj tzv. spoljni (*outer*) identitet koji je obi?no u formi *autonomous@ream*. Dakle, ne šalje svoje pravo korisni?ko ime.
6. AP preuzima klijentovu EAP poruku, enkapsulira je u RADIUS protokol i prosle?uje RADIUS

serveru za autentifikaciju.
7. Server vra?a poruku u kojoj od klijenta zahteva informaciju o identitetu i lozinku, i u njoj svoj sertifikat, koji sadrži javni klju? servera i *hash* samog sertifikata kriptovan javnim klju?em tela koje je izdalo sertifikat (CA – *Certification Authority*).
8. AP dekapsulira EAP poruku RADIUS servera, a zatim je enkapsulira u 802.11 protokol i posle?uje ka klijentu.
9. Klijent proverava identitet servera na slede?i na?in:
   1. uz predpostavku da klijent poseduje javni klju? CA-a (predefinisan u okviru *Supplicant* softvera instaliranog na klijentu), klijent dekriptuje digitalni potpis sertifikata javnim klju?em CA-a i dobija *hash* sertifikata;
   2. sertfikat servera se zatim ubacuje u *hash* funkciju koja je navedena u sertifikatu, a rezultat se upore?uje sa *hash*-om dobijenim dekriptovanjem digitalnog potpisa iz njegovog serverskog sertifikata. Ako su ta dva *hash*-a jednaka, klijent može da veruje serveru i da njegovim javnim klju?em kriptuje svoje kredencijale;
   3. ako je ishod prethodnog postupka pozitivan, klijent vrši kriptovanje svojih kredencijala (identiteta i lozinke) koriste?i javni klju? servera, na taj na?in prave?i tunel izme?u njega i servera.
10. Server dekriptuje poruku svojim privatnim klju?em i proverava kredencijale korisnika u bazi podataka. Ako je autentifikacija uspešna, server šalje Access accept poruku ka klijentu.
11. AP prosle?uje poruku klijentu o uspešnoj autentifikaciji, ?ime je proces završen.