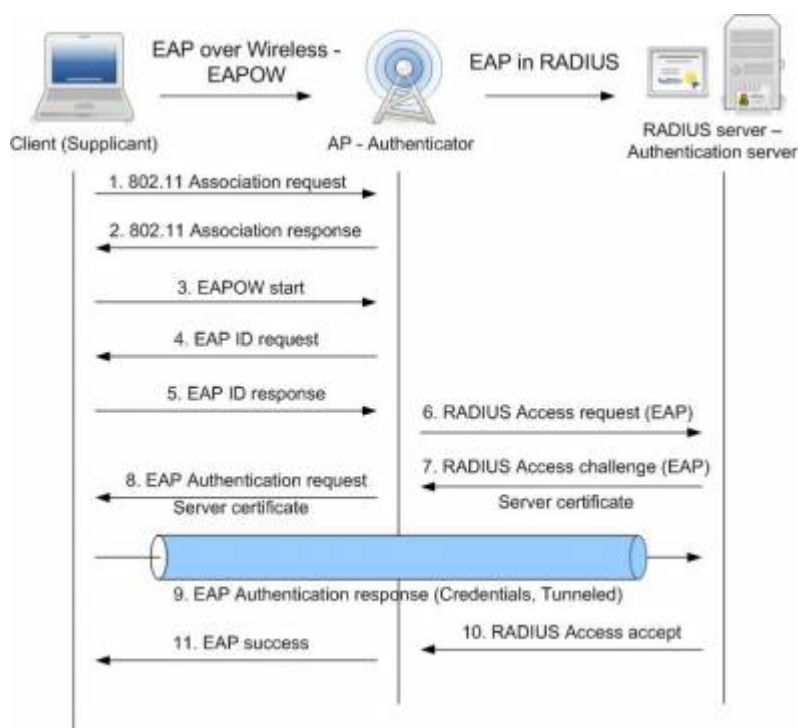


# EAP-TTLS protokol

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 između klijent i server strane prilikom autentifikacije korišćenjem 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 tačku (AP - *access point*), želi da alokira resurse i da se sinhronizuje sa AP-om. U toj poruci šalje informacije o svojoj NIC (*Network Interface Card*) kartici (protokole 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 odluži da prihvati zahtev, AP alokira memorijski prostor i generiše *Association ID*, koji prosleđuje u poruci.
3. Klijent šalje prvu EAP poruku, odnosno zahtev, želi počinje EAP-TTLS autentifikacija.
4. AP zahteva 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 nezaštićena, tj. na njoj se ne koristi nikakva enkripcija za zaštitu podataka. Klijent šalje samo svoj tzv. spoljni (*outer*) identitet koji je obično u formi *autonomous@realm*. Dakle, ne šalje svoje pravo korisničko ime.
6. AP preuzima klijentovu EAP poruku, enkapsulira je u RADIUS protokol i prosleđuje RADIUS

- serveru za autentifikaciju.
7. Server vraća poruku u kojoj od klijenta zahteva informaciju o identitetu i lozinku, i u njoj svoj sertifikat, koji sadrži javni ključ servera i *hash* samog sertifikata kriptovan javnim ključem tela koje je izdalo sertifikat (CA - *Certification Authority*).
  8. AP dekapulira EAP poruku RADIUS servera, a zatim je enkapsulira u 802.11 protokol i pošlje ka klijentu.
  9. Klijent proverava identitet servera na sledeći način:
    1. uz pretpostavku da klijent poseduje javni ključ CA-a (predefinisano u okviru *Supplicant* softvera instaliranog na klijentu), klijent dekriptuje digitalni potpis sertifikata javnim ključem CA-a i dobija *hash* sertifikata;
    2. sertifikat servera se zatim ubacuje u *hash* funkciju koja je navedena u sertifikatu, a rezultat se upoređuje 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 ključem kriptuje svoje kredencijale;
    3. ako je ishod prethodnog postupka pozitivan, klijent vrši kriptovanje svojih kredencijala (identiteta i lozinke) koristeći javni ključ servera, na taj način praveći tunnel između njega i servera.
  10. Server dekriptuje poruku svojim privatnim ključem i proverava kredencijale korisnika u bazi podataka. Ako je autentifikacija uspešna, server šalje Access accept poruku ka klijentu.
  11. AP pošlje poruku klijentu o uspešnoj autentifikaciji, čime je proces završen.

From:

<http://www.bpd.amres.ac.rs/> - AMRES wiki

Permanent link:

[http://www.bpd.amres.ac.rs/doku.php?id=amres\\_cbp\\_wiki:bpd\\_106\\_dodatakc\\_eap-ttls](http://www.bpd.amres.ac.rs/doku.php?id=amres_cbp_wiki:bpd_106_dodatakc_eap-ttls)

Last update: 2011/05/15 21:10