AMRES eduroam – tehnički uvod

AMRES

Akademska mreža Srbije

eduroam servis u AMRES-u

Sadržaj

- Institucije u okviru eduroam-a
- eduroam autentifikacija
  - 802.1x
  - Hijerarhijska struktura RADIUS servera
  - Sigurnost korisničkih kredencijala
  - Primer eduroam autentifikacije
- eduroam autorizacija

Institucije u okviru eduroam-a

- U zavisnosti od funkcije koju obavljaju, institucije u okviru eduroam-a mogu biti:

1. **Davalac servisa** *(Service Provider - SP)* – organizator nacionalnog eduroam servisa –AMRES
2. **Davalac identiteta** *(Identity Provider - IdP)* – matična institucija, obezbeđuje korisničke kredencijale i vrši autentifikaciju svojih korisnika
3. **Davalac resursa** *(Resource Provider - RP)* – obezbeđuje resurse za pristup Internetu (bežične ili žičane) i vrši kontrolu pristupa

Vaša institucija može biti IdP, RP ili IdP+RP

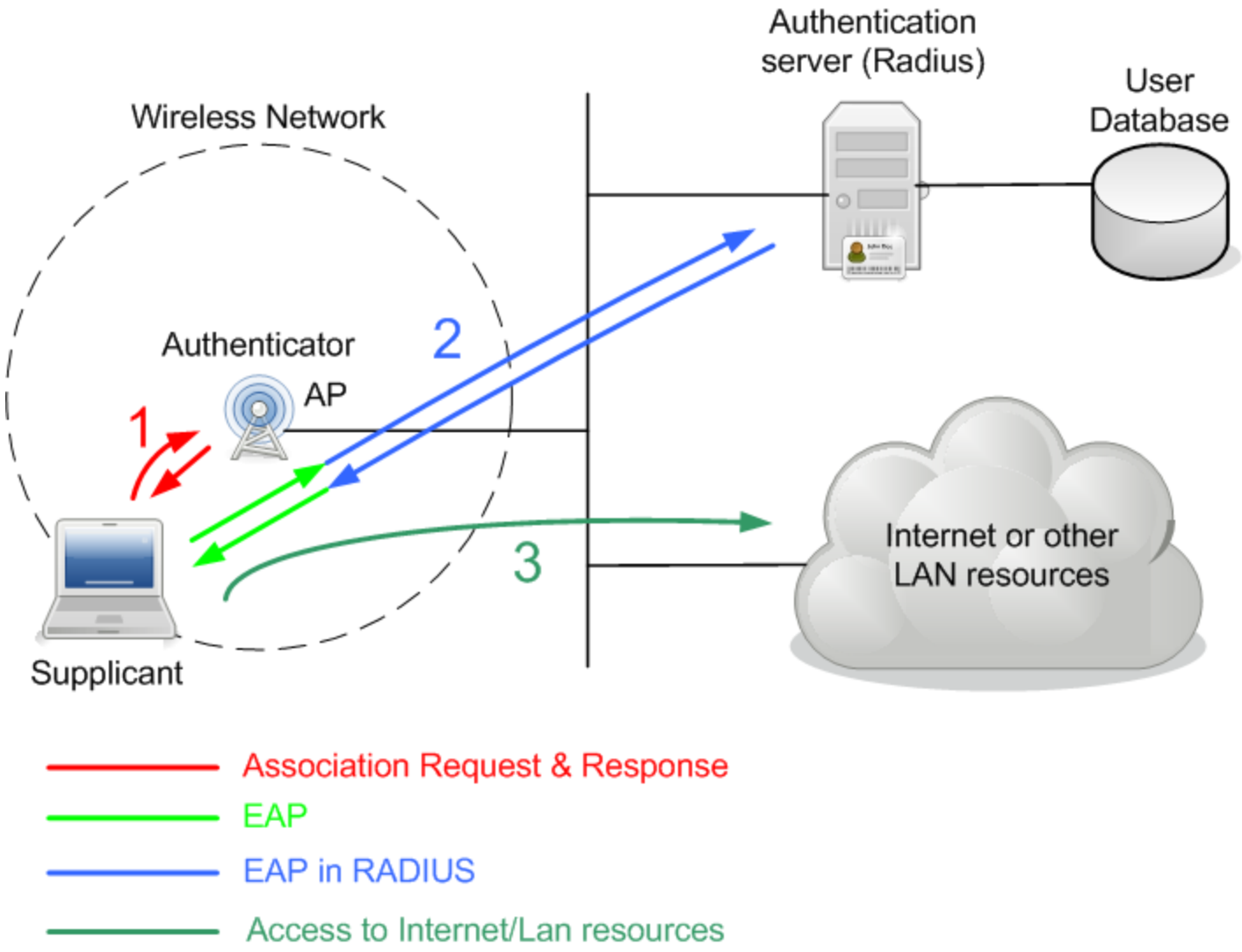
eduroam autentifikacija - 802.1x (1)

- Za kontrolu pristupa koristi **IEEE 802.1x** standard
  (Layer 2 port-based Network Access Control standard)
- Strane koje komuniciraju u okviru 802.1x standarda:
  - *Supplicant* - Korisnički uređaj
  - *Authenticator* - NAS – *Network Access Server* - (AP, WLC kontroler ili svič koji podržava 802.1x)
  - *Authentication server* – *defacto* standard RADIUS
- Dok se identitet korisnika ne proveri dozvoljena je razmena samo 802.1X EAP (*Extensible Authentication Protocol*) poruka između *supplicant-a* i NASa

eduroam autentifikacija - 802.1x (2)

- RADIUS - *Remote Access Dial In User Server*
  - rfc 2865
  - Mrežni protokol koji omogućava centralizovan AAA servis (*Authentication, Autorization, Accounting*)
  - Zahtev korisnika se preko mrežnih pristupnih tačaka prenosi do RADIUS servera
  - Provera korisničkih informacija – LDAP, SQL, AD, fajl ..
  - UDP portovi 1812 - autentifikacija i 1813 - accounting

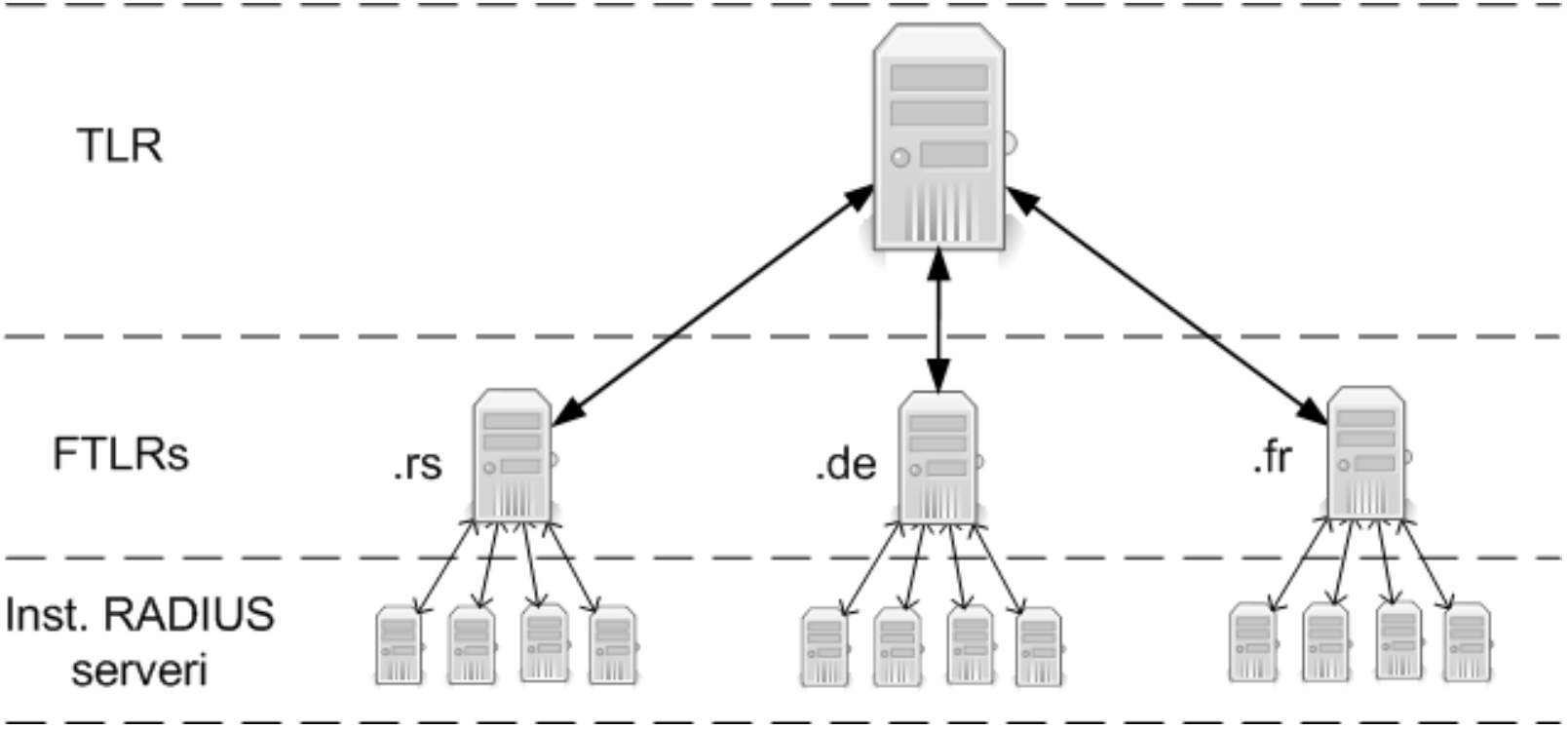
eduroam autentifikacija - 802.1x (3)



Hijerarhijska struktura RADIUS-a (1)

- Za prosleđivanje autentifikacionih zahteva koristi se 3-nivovska hijerarhija RADIUS servera:
  - ***Top-Level RADIUS Server*** **(TLR)** – konfederacioni serveri, povezuju nacionalne FTLR servere (sadrže listu nacionalnih domena nl, dk, de, pt, fr,rs..), vrše proksiranje zahteva
  - ***Federation Top-Level RADIUS Server*** **(FTLR)** – serveri na nacionalnom nivou, povezuju radius servere institucija, vrše proksiranje zahteva
  - ***Institutional RADIUS Server*** – odgovoran za autentifikovanje svojih korisnika i (u slučaju davaoca resursa) prosleđivanje autentifikacionih zahteva gostujućih korisnika ka njihovim matičnim institucijama

Hijerarhijska struktura RADIUS-a (2)



Hijerarhijska struktura RADIUS-a (3)

- Korisnička imena su u formi:

  korisnik@domen_institucije

- domen_institucije (*realm*) se koristi za prosleđivanje (proxy) zahteva sledećem serveru u hijerarhiji

Sigurnost korisničkih kredencijala (1)

- Sigurnost prilikom prenosa korisničkih kredencijala u eduroam-u je obavezna!
- Korisnički kredencijali se tuneluju (prenose enkriptovani) kroz hijerarhiju RADIUS servera
- Autentifikacioni metodi: EAP-TLS, EAP-TTLS i EAP-PEAP

Sigurnost korisničkih kredencijala (2)

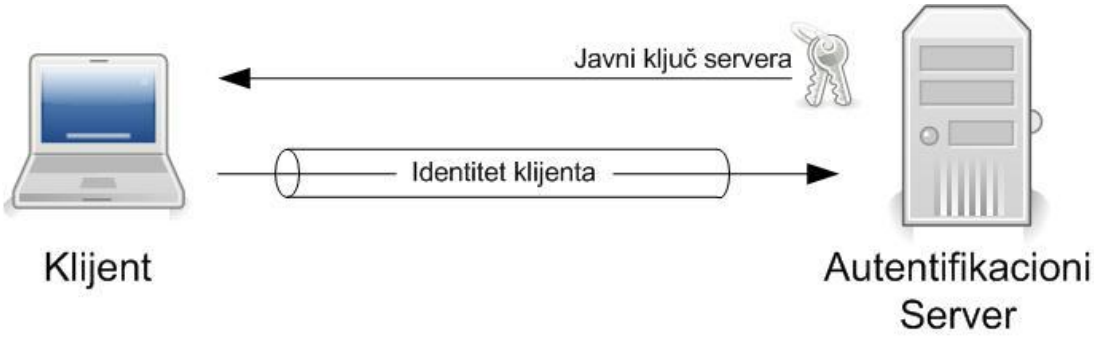
- EAP-TLS (*Transport Layer Security*) – protokol koji omogućava uzajamnu autentifikaciju dva krajnja uređaja na osnovu digitalnih sertifikata

Sigurnost korisničkih kredencijala (3)

- EAP TTLS (Tunneled TLS) i PEAP (Protected EAP)
- Autentifikacija sadrži dve faze

1. Klijent autentifikuje autentifikacioni server preko digitalnog sertifikata servera

2. Server autentifikuje klijenta preko korisničkog imena i lozinke



Sigurnost korisničkih kredencijala (4)

- Radi uspostavljanja tunela, korisnički uređaj šalje identitet korisnika u anonimnoj formi:

  anonymous@domen_institucije

- domen_institucije se koristi za rutiranje zahteva
- Kada se uspostavi TLS tunel, unutar tunela se šalju pravo korisničko ime i tek tada se šalje lozinka

Sigurnost korisničkih kredencijala (5)

- Unutar ttls/peap tunela se šalju pravi kredencijali, i mogući su različiti načini provere identiteta korisnika
  - PAP (*Password Authentication Protocol*)
  - CHAP (*Challenge Handshake Auth Protocol*)
  - MSCHAP (*Microsoft CHAP*)
  - EAP-GTC (*Generic Token Card*)
  - MD5-Challenge

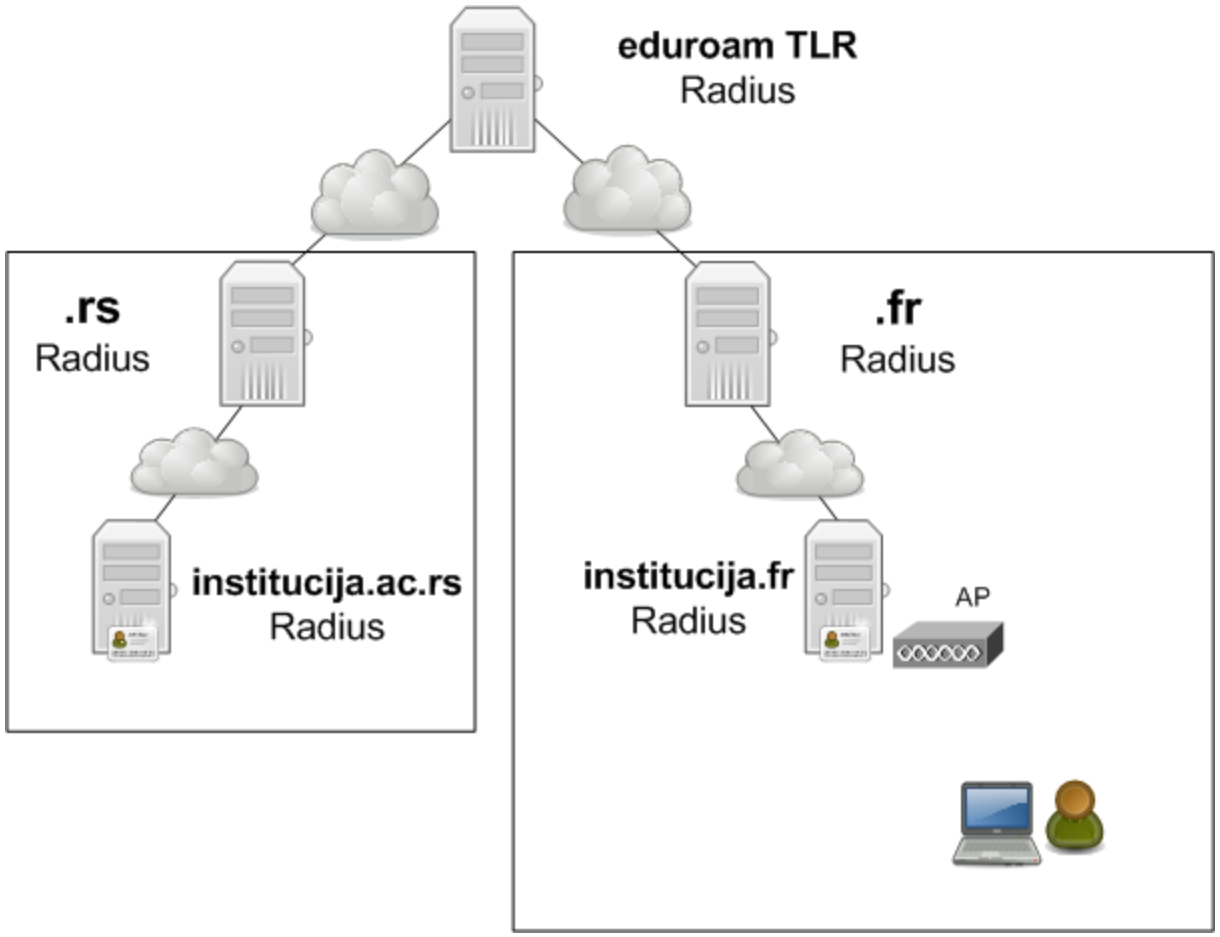
Sigurnost korisničkih kredencijala (6)

- Razlike između TTLS i PEAP
  - Nisu jednako podržani na *supplicant*-ima
  - Unutar tunela koriste različite autentifikacione metode:
    - TTLS: PAP, CHAP, MSCHAP, MD5-Challenge
    - PEAP: MSCHAP

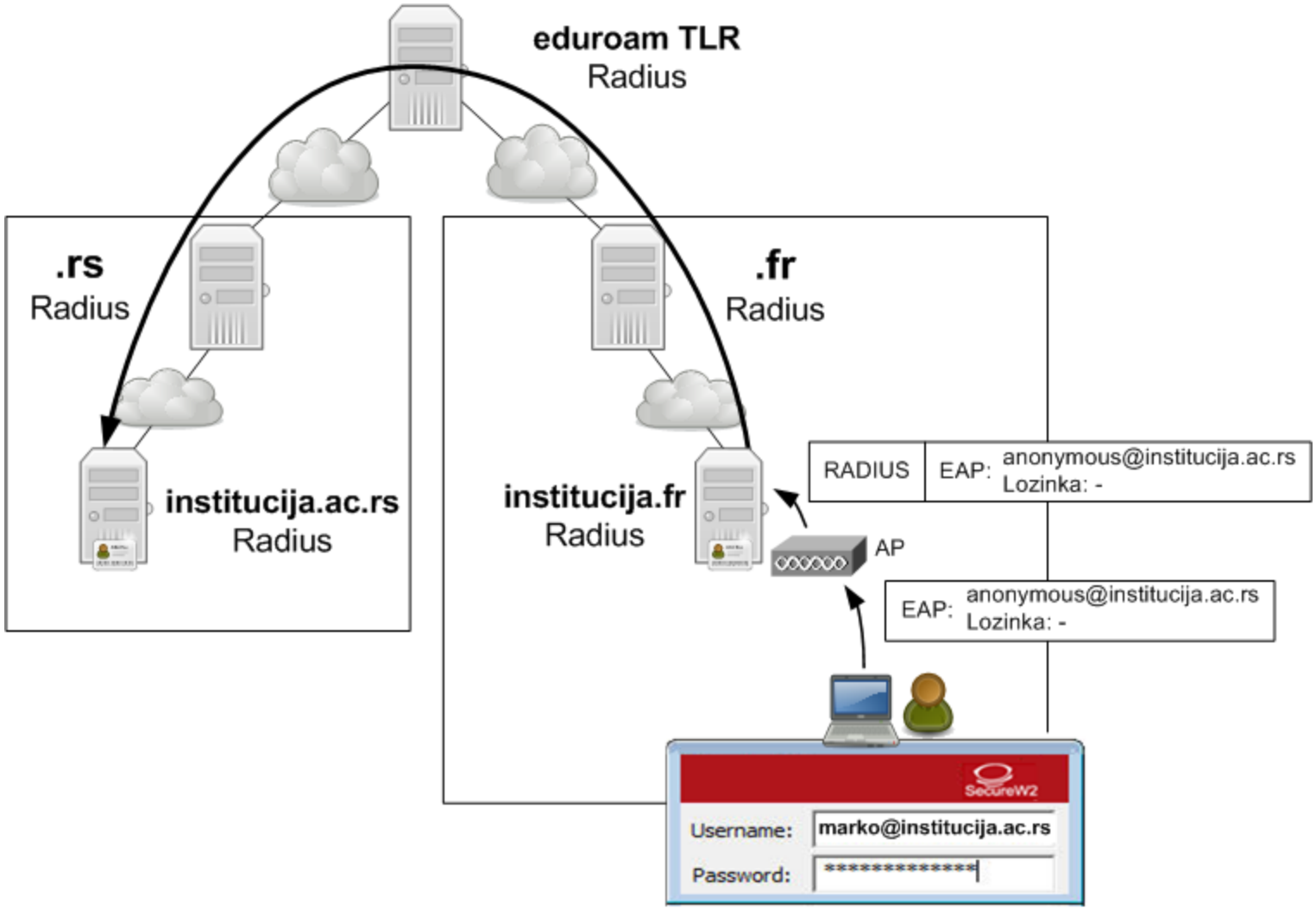
Sigurnost korisničkih kredencijala (6)

	clear-text	NT-hash	MD5 hash	Salted MD5 hash	SHA1 hash	Salted SH1 hash	Unix Crypt
PAP	o	o	o	o	o	o	o
CHAP	o	x	x	x	x	x	x
Digest	o	x	x	x	x	x	x
MS-Chap	o	o	x	x	x	x	x
PEAP	o	o	x	x	x	x	x
EAP-MSCHAPv2	o	o	x	x	x	x	x
Cisco LEAP	o	o	x	x	x	x	x
EAP-GTC	o	o	o	o	o	o	o
EAP-MD5	o	x	x	x	x	x	x
EAP-SIM	o	x	x	x	x	x	x

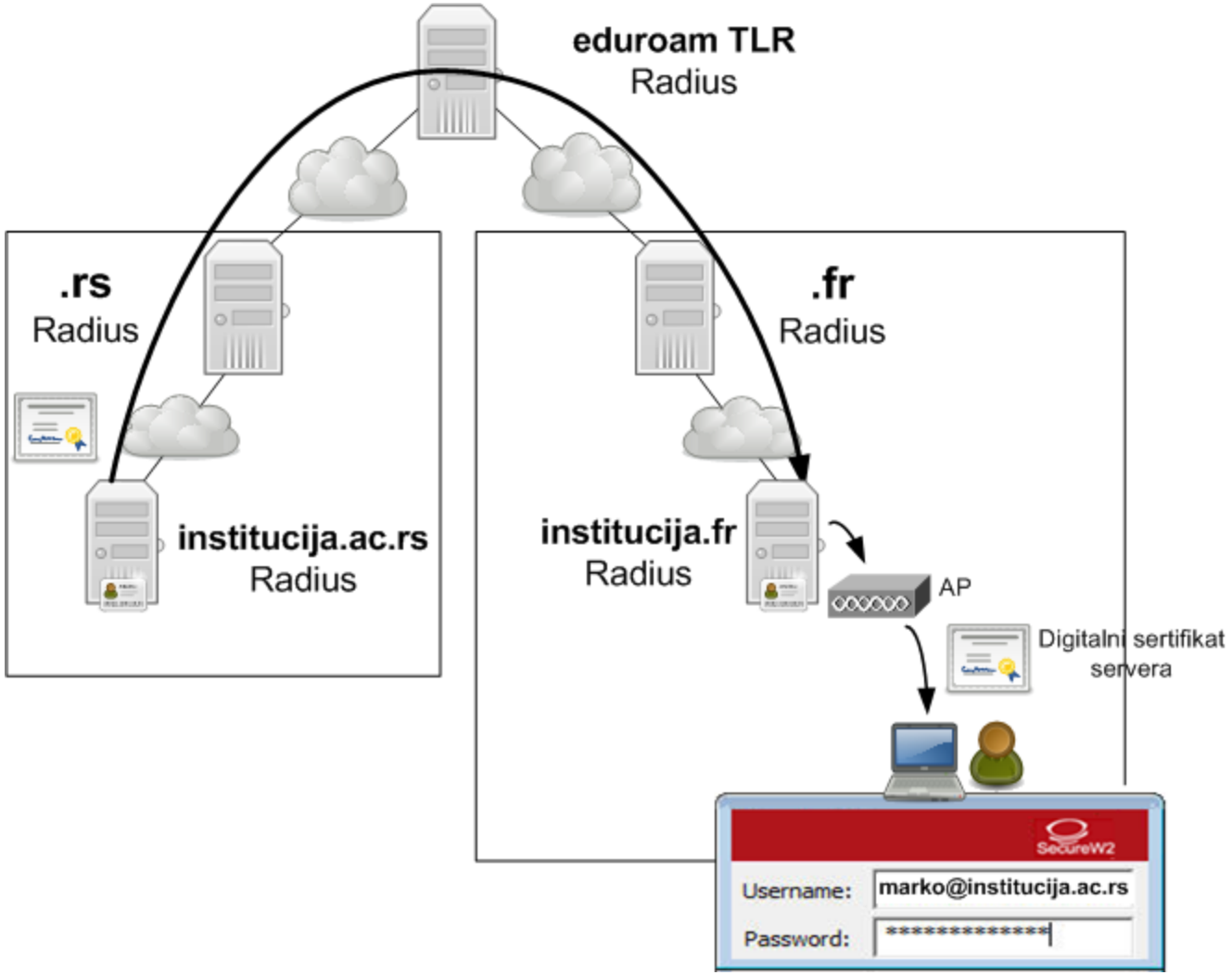
eduroam autentifikacija



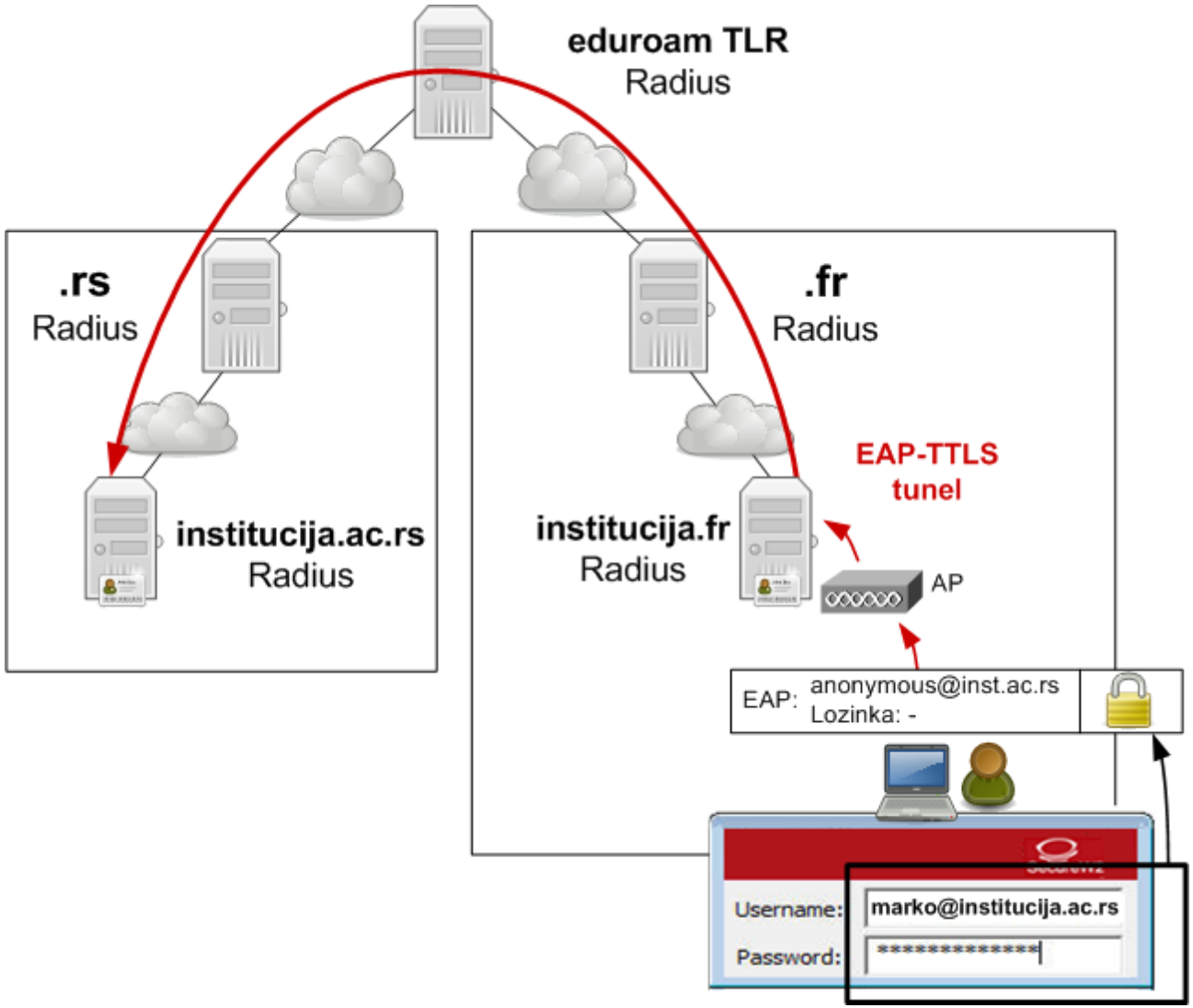
eduroam autentifikacija



eduroam autentifikacija



eduroam autentifikacija



eduroam autorizacija

- Korisniku je omogućeno korišćenje određenih servisa koje dozvoljava posećena organizacija
- Postoji minimalan set servisa koje posećena organizacija (Davalac resursa) mora ponuditi korisnicima (u skladu sa *eduroam* pravilnikom)