Če pregledamo naš koncept treh A-jev, je postopek pri katerikoli storitvi že, za *Identifikacijo in Avtentikacijo* enak, zato ju hočemo spraviti v nekakšno abstrakcijo, tako da jih lahko uporabljamo vedno kjerkoli in nas ne zanimajo detajli.

Za ta namen je bil definiran **RADIUS** protokol, ki je zapisan v RFC 2865, pomeni pa Remote Authentication Dial In User Service, in tudi definiram v RFC 2866 *RADIUS Accounting*.

Njegove osnovne funkcionalnosti so: - Omogočanje avtomatske **avtorizacije, avtentikacije in beleženja** - Fleksibilnost avtentikacije, kjer omogoča uporabo drugega protokola

RADIUS koristi tri komponente svoje storitve: - **Uporabnika** storitve - **Ponudnika** neke storitve, ki potrebuje za uporabnika AAA storitve, zato koristi RADIUS - **RADIUS strežnik**

> RADIUS strežnik je lahko samo vmesni člen pri dostopu do drugega RADIUS strežnika.

Arhitektura pogovora

![[Pasted image 20230112164037.png]]

Ali pa seveda lahko RADIUS strežnik lahko igra vlogo proxy-a, če ne vsebuje podatke o določenik zahtevi.

Zahteva za dostop

Prvo sporočilo RADIUS pogovora, vzpostavitev dostopa glede na identifikacijo uporabnika, ga lahko nato RADIUS avtenticira. Uporablja se razne portokole: - PAP - CHAP - MS-CHAP - EAP Zahtevo lahko strežnik zavrne ali pa sprejme. Po avtentikaciji, RADIUS server preko nekega API-a pošlje vse avtorizirane mikrostoritve svoji stranki, ki svojemu odjemalcu končno ponudi storitve.

Da bi uporabljali proxy storitve še posebaj za RADIUS moramo mi zaupati, da RADIUS strežnik zaupa tistemu RADIUS strežniku kamor pošilja podatke naprej oz. da le-ta jamči za nas.

Temu je potrebno tudi beleženje, kateri uporabnik se je kdaj prijavil, odjavil in vmes morda še kaj se je zgodilo pomembnega, brez da beležimo tistega, kar po zakonih ne smemo.

Torej beležimo lahko tri vrste dogodkov: - Začetek rabe storitve - Nadaljno rabo ali popraljene podatke - Zaključek rabe ![[Pasted image 20230112170558.png]]

> RADIUS kategoriziramo kot koračni protokol, seveda potem uprablja identifikator sporočil.

Za komunikacijo med storitvijo za katero zagotavlja AAA in RADIUS strežnikom, sam protokol seveda tudi zaščiti, to pomeni, da poskrbi za šifriranje (če ni v uporavi PAP protokol) in seveda za celovitost. RADIUS predvideva avtentikator, ki podpisuje te podatke, kateri se pošiljajo in je edini vir zagotavljanja celovitosti. Storitev in RADIUS strežnik imata skupno skrivnost.

Podpisovanje AA. paketov

Odjemalna storitev pošlje izziv, ki je naključno 128-bitno število, na kar strežnik odgovori z 128-bitnim številom, izračunano iz skrivnosti, vsebine paketa in izziva odjemalca. Podpis je uporabljen, kot avtentikacija odgovora in ne ščiti zahteve odjemalca. Isti izziv v odjemalčevem podpisu se uporabi za izziv za zaščito poslanega gesla.

Podpisovanje ..A paketov

Malce drugače, saj smo fleksibilni, četudi ni paket uredu, še dalje če ni uredu, akcijo samo ponovno zapišemo.

![[Pasted image 20230112173802.png]] Te atributi se lahko uporabijo recimo, da povemo do česa vse ima uporabnik dostop. Lahko vpišemo, kaj vse želimo beležit, seveda per-user basis. Vpisujejo se lahko tudi uporabniški podatki, gesla itd.