KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Sieťová a komunikačná bezpečnosť

04 Vzdialený prístup k lokálnej sieti

KCKB UPJS CSIRT UPJS

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Vzdialený prístup k lokálnej sieti

- EAP autentifikácia
- protokol RADIUS
- správa dôvery
- certifikačný proces

Vzdialený prístup k lokálnej sieti

- Bezpečnosť vzdialeného prístupu vyžaduje silnú autentifikáciu a šifrovanie
  - EAP autentifikácia (Extensible Authentication Protocol)
  - Protokol RADIUS (Remote Authentication Dial-In User Service)
  - Správa dôvery (Trust Management)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

EAP autentifikácia

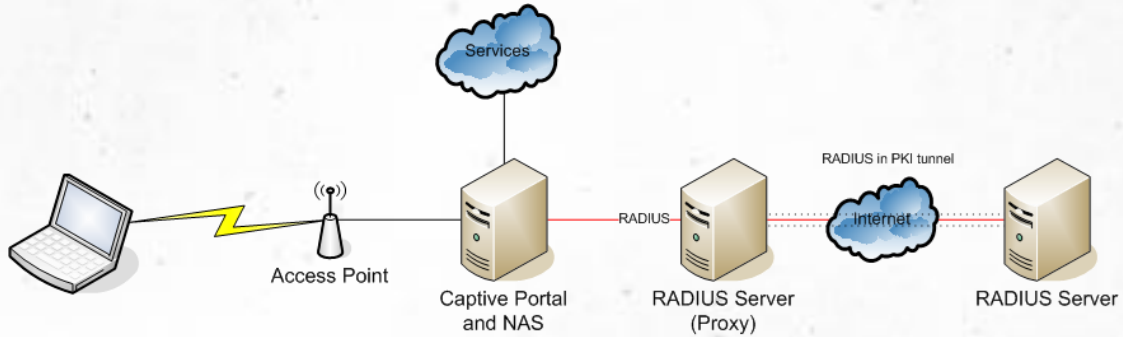
- EAP autentifikácia (802.1X Extensible Authentication Protocol)
- podporuje viaceré autentifikačné metódy
  - EAP-PSK
    - heslo
  - PEAP, EAP-MSCHAPv2 (WPA2 Enterprise pre eduroam)
    - TLS tunnel (Protected)
    - server certifikát, klient login + heslo
  - EAP-TLS
    - certifikáty pre server aj klientov
  - EAP-TTLS
    - certifikát pre klienta je nepovinný

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Remote Authentication Dial-In User Service (RADIUS)

Sieťový protokol (RFC 2865), ktorý zabezpečuje:

- overenie totožnosti (autentizáciu)
- prístupové práva (autorizáciu)
- prehľad o využívaní služieb (účtovanie)



https://upload.wikimedia.org/wikipedia/commons/e/e7/Drawing_Roaming_RADIUS.png

Slúži ako centrálna správa prístupov:

- k pripojeniu na switch/access point (firemná/školská sieť), aj roaming

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Radius

1. Používateľ sa pripája cez access point, switch alebo VPN bránu.
2. Zariadenie pošle na Radius server správu Access-Request s údajmi o používateľovi.
3. Server vráti Access-Accept alebo Access-Reject;
   pri účtovaní sa používajú aj záznamy Start, Interim-Update a Stop.

FreeRADIUS - najznámejšia open-source implementácia tohto protokolu

https://www.freeradius.org/img/wordmark.svg

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

FreeRadius

```
# clients.conf
client kckb01 {
        ipaddr = <IP.klienta>
        secret = kckb.skb
        shortname = kckb
}
```

```
# users
student1 Cleartext-Password := "UPJS-SKB"
        Reply-Message := "Ahoj, %{User-Name}"
```

```
#bash
radiusd –X
radtest student1 UPJS-SKB <IP.servera> 0 kckb.skb
```

FreeRadius

- Je možné napríklad:
  - nastaviť VLAN id podľa skupiny

```
DEFAULT LDAP-Group == "students"
        Tunnel-Type = VLAN,
        Tunnel-Medium-Type = IEEE-802,
        Tunnel-Private-Group-Id = "20"
```

  - nastaviť denný limit

```
Max-Daily-Session := 10800
```

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

FreeRadius

Je možné napríklad:

- uložiť len hash hesla

```
Student1 Password.MD5 := 71f02ecf95e1fbe5ab0ef7696b06ab62
```

- použiť CHAP (challenge-response)

```
authorize {
   chap
}
authenticate {
   chap
}
```

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

EAP-TTLS vo FreeRadius

```
eap {
        default_eap_type = ttls
        ttls {
                default_eap_type = pap
                copy_request_to_tunnel = yes
                use_tunneled_reply = yes
        }
}

tls-config tls-common {
        private_key_file = /etc/ssl/private/server.key
        certificate_file = /etc/ssl/certs/server.crt
        ca_file = /etc/ssl/certs/ca.crt
}
```

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

EAP-TTLS vo FreeRadius

- klient najprv overí serverový certifikát RADIUS servera
- vytvorí sa TLS tunel
- prebehne autentifikácia (typicky PAP)

- dôvera stojí na správnej reťazi certifikačných autorít a validácii certifikátu

Certifikácia FreeRadius servera

- vytvorenie/vybratie certifikačnej autority (CA)
- vygenerovanie CSR žiadosti a vydanie/podpísanie certifikátu CA
- nastavenie konfigurácie RADIUS servera
- distribúcia certifikátu CA na klienstké zariadenia

- Pri EAP-TLS je potrebné generovať certifikáty aj pre klientov

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

EAP-TLS

- Pri EAP-TLS je potrebné generovať certifikáty aj pre klientov, tie overuje server

```
eap {
        default_eap_type = tls
        tls-config tls-common {
                private_key_file = ${certdir}/server.key
                certificate_file = ${certdir}/server.crt
                ca_file = ${cadir}/ca.crt
        }
}
```

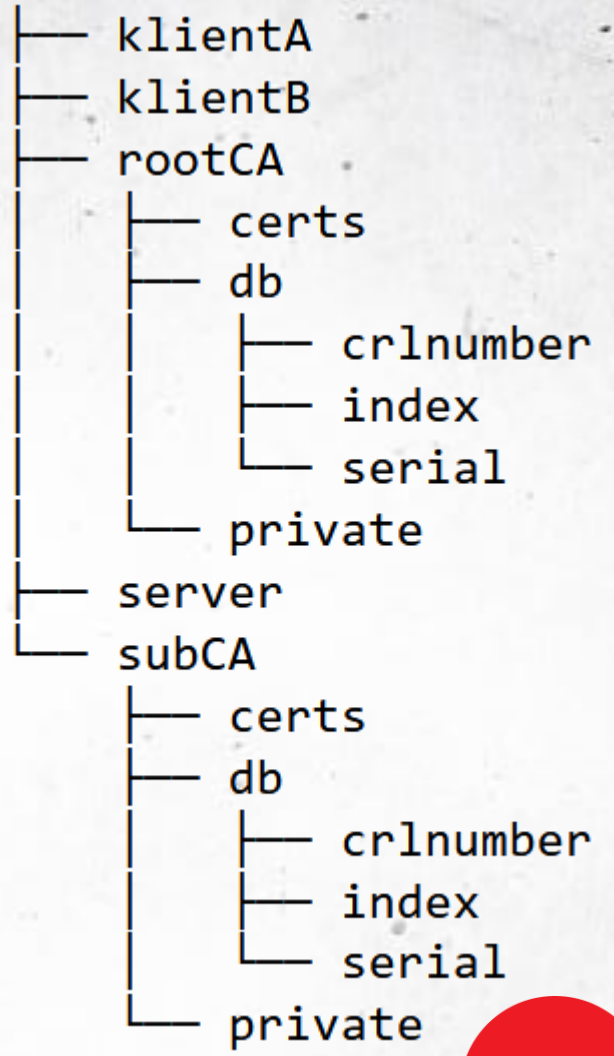
KERBEROS

- **ticket-based autentifikačný protokol**
  - typicky pre prihlásenie k službám a SSO v doméne
    overuje identitu používateľa alebo služby pomocou tiketov
    protokol na bezpečnú autentifikáciu v sieti,
    ktorý používa tikety namiesto opakovaného posielania hesla
- Na rozdiel od RADIUSu nerieši len prístup do siete, ale aj prístupy do jednotlivých služieb.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Certifikáty (I.)

```
mkdir -p {rootCA,subCA}/{db,certs} server klient{A,B}
mkdir -p -m 0700 {root,sub}CA/private
touch {root,sub}CA/db/index
openssl rand -hex 16  >"rootCA/db/serial"
openssl rand -hex 16  >"subCA/db/serial"
echo 1001 >"rootCA/db/crlnumber"
echo 1001 >"subCA/db/crlnumber"
```



Certifikáty (II.)

- Vytvorenie CSR požiadavky na certifikát
  - openssl req -new -config "rootCA.conf" -out "rootCA/ca.csr" -keyout "rootCA/private/ca.key"
- Samopodpísanie certifikátu autority
  - openssl ca -selfsign -config "rootCA.conf" -in "rootCA/ca.csr" -out "rootCA/ca.crt" -extensions ca_ext
- Vytvorenie požiavky na certifikát medziľahlej autority
  - openssl req -new -config "subCA.conf" -out "subCA/ca.csr" -keyout "subCA/private/ca.key"
- Podpísanie certifikátu medziľahlej autority
  - openssl ca -config "rootCA.conf" -in "subCA/ca.csr" -out "subCA/ca.crt" -extensions sub_ca_ext

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Certifikáty (III.)

- Vytvorenie požiadavky na certifikát servera
  - openssl req -new -config "server.conf" -out "server/server.csr" -keyout "server/server.key"
- Podpísanie certifikátu medziľalhou autoritou
  - openssl ca -config "subCA.conf" -in "server/server.csr" -out "server/server.crt" -extensions server_ext
- Vytvorenie reťaže certifikátov

```
cat "server/server.crt" {sub,root}CA/ca.crt |
sed -n '/-----BEGIN/,/-----END/{p}’ |
tee "server/chain.crt"
```

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Ďakujeme za pozornosť