Kako postaviti TCS certifikat AOSI web servisu?

TCS certifikat AOSI web servisa

Obzirom da AOSI web servis komunicira SOAP/HTTPS protokolom, umjesto self signed certifikata koji standardno dolazi s aosi-aai paketom za kriptiranje HTTPS prometa moguće je postaviti valjani TCS certifikat. Postavljanje valjanog TCS certifikata omogućit će klijentima koji se spajaju na AOSI da automatski provjere ispravnost certifikata i budu sigurni da pripada ustanovi na čiji se AOSI spajaju.

Prije primjene novog certifikata potrebno je posjedovati TCS certifikat izdan za poslužitelj na kojem se nalazi AOSI web servis. Upute za dobivanje takvog certifikata navedene su na web stranici http://certifikati.carnet.hr(link is external)

Da bi certifikat bio valjan, u polju **subject**, u atributu **CN** (ili u ekstenziji **Subject Alternative Name**) mora imati ispravan hostname. Ta vrijednost trebala bi biti jednaka vrijednosti koju vraća naredba:

```
hostname --fqdn
```

izvršena na poslužitelju na kojem se nalazi AOSI web servis.

Za primjenu certifikata AOSI web servisa potrebne su tri datoteke (ekstenzija nije bitna, bitno je da su PEM enkodirani):

hostname_cert.cer, hostname_interm.cer i hostname.key.

Napominjemo da su nazivi generički i ne odgovaraju nazivima tih datoteka na vašem poslužitelju pa stoga u nastavku donosimo objašnjenje što je u pojedinoj datoteci:

- **hostname_cert.cer**: datoteka koja sadrži vaš certifikat, obično se smješta u direktoriju **`/etc/ssl/certs/ ili direktorij /etc/ssl/ssl/`**. To je datoteka koju ste preuzeli putem CARNetove TCS usluge - (Certificate only, PEM encoded).
- **hostname_interm.cer**: datoteka s lancem povjerenja. Obično se smješta u direktoriju **`/etc/ssl/certs/ ili direktorij /etc/ssl/ssl/`**. I tu ste datoteku preuzeli posredstvom CARNetove TCS usluge - (Intermediate(s)/Root only, PEM encoded)
- **hostname.key**: ključ koji ste koristili za potpisivanje zahtjeva za certifikat. Obično se smješta u direktorij **`/etc/ssl/private/.`**

1. Instalirati paket certs-aai koji je zadužen za postavljanje certifikata.

Paket se instalira naredbom:

```
# apt-get install certs-aai
```

U potupku instalacije trebate znati:

Putanju do poslužiteljskog certifikata:
npr. /etc/ssl/certs/hostname_cert.cer

Putanju do certifikata s lancem povjerenja (tzv. *chain* ili *intermediate* certificate):
obično: /etc/ssl/certs/hostname_interm.cer

Putanja do ključa koji ste koristili za potpisivanje zahtjeva za certifikat (key):
obično: /etc/ssl/private/hostname.key

(Certifikat i prijelazni certifikat (chain) se na Debianu standardno postavljaju u direktori /etc/ssl/certs ili /etc/ssl/ssl/, a ključevi u /etc/ssl/private).

Ako imate instaliran paket certs-aai, paket aosi-aai će kod instalacije znati prepoznati i primjeniti ispravne certifikate.

2. Zamjenu certifikata obavit ćete pokretanjem naredbe:

```
# dpkg-reconfigure certs-aai
```

kojom će se upisati novi certifikati.

3. Nakon upisivanja novog certifikata, AOSI web servis treba primjeniti novi cerifikat. Zato je potrebno pokrenuti naredbu:

```
# dpkg-reconfigure aosi-aai
```

VAŽNA NAPOMENA!

Prilikom pokretanja gornje naredbe dpkg-reconfigure aosi-aai potrebno je unijeti zaporku LDAP administratorskog (sistemskog) korisnika čiji je dn: cn=admin, dc=domena, dc=hr (dakle, ne radi se o fizičkoj osobi/korisniku sa ovlastima ažuriranja podataka putem web sučelja već o "sistemskom korisniku"). Ta je zaporka zapisana u datoteci /etc/aosi/ldap_pwd.