Infrastruktura javnih ključeva

- specifikacija predmetnog projekta -

Informaciona bezbednost, SIIT, 2025

Korisničke uloge

- **Administrator (Admin aplikacije)**
- **CA korisnik (korisnik organizacije koja poseduje CA sertifikat)**
- **Običan korisnik**

Prava i funkcionalnosti po ulogama

Administrator

- Može da dodaje nove CA korisnike.
- Može da dodaje CA sertifikate za ove korisnike (za sisteme, servere itd).
- Može da izdaje sve tipove sertifikata:
    - Root (samopotpisani)
    - Intermediate
    - End-Entity (EE)
- Ima uvid u sve sertifikate u sistemu.
- Može da koristi bilo koji sertifikat iz bilo kog lanca za dalje izdavanje.
- Može da vidi, preuzme ili povuče sve sertifikate.

CA korisnik

- Može da izdaje intermediate i end-entity sertifikate **samo za svoju organizaciju**, koristeći svoj CA sertifikat ili bilo koji sertifikat iz prethodno kreiranog lanca.
- Može da vidi i preuzme samo sertifikate iz svog lanca.
- Može da kreira i koristi šablone vezane za svoje sertifikate.

Običan korisnik

- Može da:
    - uploaduje CSR i privatni ključ radi izdavanja sertifikata,
    - ili popuni formu za generisanje ključeva i sertifikata,
    - bira CA sertifikat koji će se koristiti za izdavanje njegovog sertifikata
    - preuzme dobijeni sertifikat i privatni ključ,
    - pregleda svoje sertifikate,
    - povuče sertifikat uz navođenje razloga (po X.509 standardu).

Funkcionalnosti sistema

Registracija

Samo obični korisnici mogu da se registruju, na početnoj stranici putem forme za registraciju. Običan korisnik od podataka mora da unese *email* adresu, lozinku, ime, prezime

i organizaciju. Lozinka mora da se unese dva puta, i mora da ispoštuje minimalne zahteve. Dodatno, potrebno je ugraditi funkcionalnost procene jačine lozinke. Korisnik mora da potvrdi svoj identitet nakon registracije, klikom na aktivacioni link iz mejla. Link je vremenski ograničen i može da se iskoristi samo jednom.

Prijava na sistem

Svi korisnici sistema imaju mogućnost prijave pomoću email adrese i lozinke. Ukoliko je korisnik uspešno prijavljen, potrebno je izgenerisati *access* token i *refresh* token koji će se poslati na klijentski deo aplikacije. Access token treba da ima kratak životni vek, dok refresh token ima značajno duži.

Dobijene tokene treba skladištiti na klijentskom delu; access token treba slati kroz zaglavlje prilikom narednih zahteva tog ulogovanog klijenta, dok ne istekne. Po isteku, kreirati novi access token koristeći refresh token.

Pročitajte više o bezbednoj implementaciji i bezbednom korišćenju:
https://auth0.com/blog/refresh-tokens-what-are-they-and-when-to-use-them/

Izdavanje sertifikata

Sistem treba da podrži centralizovano izdavanje sertifikata za digitalne entitete svih nivoa, uključujući proizvoljan broj **intermediate nivoa**. Za generisanje sertifikata korisnik unosi podatke o vlasniku (pogledati X500Name), definiše trajanje sertifikata i ekstenzije (npr. keyCertSign, BasicConstraints, …) i bira CA sertifikat koji će biti izdavalac. Prilikom generisanja sertifikata, potrebno je voditi računa o validnosti sertifikata izdavaoca. Validnost treba posmatrati u kontekstu perioda važenja, ispravnosti digitalnog potpisa i statusa povučenosti.

- Izdavanje:
    - Samopotpisanih (Root CA)
    - Intermediate (CA)
    - End-Entity (korisnici, uređaji)

Čuvanje sertifikata

- Poverljivost sertifikata mora biti očuvana kroz sistem. Preporučujemo da proučite kako bi takvo nešto u praksi moglo da izgleda:
  https://infisical.com/docs/internals/security#cryptography
- Minimalno je potrebno obezbediti sledeće:
    - Da se privatni ključevi izdatih sertifikata u bazi čuvaju enkriptovani
    - Da se oni enkriptuju pomoću ključa izdatog za pojedinačnu organizaciju
    - Da je konfiguracija kriptografskih algoritama dobro proučena, da su dobre prakse istražene i primenjene
    - Da je obezbeđena poverljivost i samih ključeva na nivou organizacija (što sugeriše postojanje glavnog (master) ključa, ali detalje ostavljamo na izbor timu)

Preuzimanje sertifikata:

Prilikom preuzimanja sertifikata i povezanog privatnog ključa, obezbediti da se oni na serverskoj strani zapakuju u keystore (pkcs12 ili jks).

CSR (Certificate Signing Request)

CSR je zahtev koji pravi entitet kako bi zatražio sertifikat of sertifikacionog tela (CA). CSR sadrži sve podatke o vlasniku sertifikata (pogledati X500Name), javni ključ i ekstenzije. End-entity korisnici prave CSR putem eksterne generacije - korisnik sam generiše ključeve i koristi alat za generisanje csr-a, poput openssl-a. Tako generisani csr se potom čuva u enkodovanom .pem formatu i upload-uje kroz formu na PKI sistemu. Pored upload-a je potrebno omogućiti korisniku da odabere CA za digitalni potpis. Na osnovu odabranog CA, korisnik može da unese trajanje sertifikata pri čemu se mora poštovati trajanje sertifikata odabranog CA. Druga opcija za generisanje EE sertifikata je *autogenerate* pri čemu PKI sistem generiše par ključeva, ali ne čuva privatni ključ. Privatni ključ može da se preuzme uz sertifikat u pkcs12 ili jks formatu (pogledati funkcionalnost preuzimanje sertifikata). U slučaju autogenerate opcije, korisnik popunjava formu za kreiranje sertifikata uključujući datume, odabir CA i lične podatke *(CN, O, OU, C, E).*

Pregled i pristup sertifikatima

- Administrator vidi sve sertifikate.
- CA korisnik vidi samo sertifikate iz svog lanca.
- Korisnik vidi samo svoje EE sertifikate (može da ih ima proizvoljno mnogo).

Povlačenje sertifikata (Revocation)

Svaki korisnik ima mogućnost povlačenja sertifikata uz obavezno navođenje razloga iz X.509 standarda. Povučeni sertifikati ne bi smeli da se ponude dalje za izdavanje novih sertifikata (isto važi i za privatni ključ vezan za povučeni sertifikat). Za proveru povučenosti, potrebno je obezbediti Revocation servis (CRL proveru) pomoću CRL Distribution Point ekstenzije u sertifikatu ili podršku za OCSP.

Šabloni (Templates) za sertifikate

Šablon definiše ekstenzije i politiku sertifikata. Prilikom izdavanja sertifikata, potrebno je olakšati CA korisniku popunjavanje forme time što će mu se u zavisnosti od odabranog issuera, ponuditi (i popuniti) odgovarajuće ekstenzije sa predefinisanim vrednostima. Automatsko definisanje ekstenzija na osnovu odabranog sertifikata izdavaoca predstavlja šablon. Šablon se kreira tako što CA korisnik definiše sledeće vrednosti:

- **Naziv šablona**
- **CA issuer -** CA koji će dalje izdavati sertifikate na osnovu ovog šablona
- **Common Name (CN)** – regularni izraz za validaciju (npr. `.*\.ftn\.com`)
  - ovo podrazumeva da će se prilikom upotrebe šablona CN novog sertifikata validirati na osnovu unetog regularnog izraza

    - **Subject Alternative Names (SANs)** – definiše regularni izraz za SAN ekstenziju (isto pravilo validacije važi kao i za CN)
    - **TTL (vreme važenja)** – maksimalno trajanje
    - **Key Usage** – podrazumevana vrednost ove ekstenzije
    - **Extended Key Usage** – podrazumevana vrednost ove ekstenzije

CA korisnik može ali i ne mora da iskoristi unapred definisani šablon za izdavanje novog sertifikata. Takođe, korisnik može da izabere i druge ekstenzije koje nisu obuhvaćene šablonom, ali tako da ukupan skup odabranih ekstenzija ne prevazilazi politiku sertifikata koji se koristi za potpisivanje.

Opšti zahtevi

Potrebno je obezbediti komunikaciju klijentskog i serverskog dela aplikacije putem HTTPS protokola. To podrazumeva da izgenerišete nov sertifikat, i iskonfigurišete aplikaciju tako da iskoristi taj sertifikat za HTTPS komunikaciju između svih servisa aplikacije. Ukoliko tim izgeneriše novi sertifikat pomoću svog PKI sistema, dobiće dodatne bodove za ovu funkcionalnost.

Neophodno je implementirati autentikaciju i kontrolu pristupa svih korisnika. Korisnici koji nisu autentifikovani nemaju prava pristupa ni jednoj stranici, osim stranici za registraciju i prijavu na sistem. Takođe nemaju prava pristupa nikakvim podacima sistema. Potrebno je obezbediti zaštitu pristupa za svaki ulaz u sistem (engl. endpoint) i na klijentskoj i na serverskoj strani aplikacije.

Funkcionalnosti za jednog studenta

- Stari studenti koji projekat rade samostalno treba da implementiraju sledeće funkcionalnosti: funkcionalnosti za administratora (izdavanje sertifikata svih nivoa, pregled i preuzimanje sertifikata)
- HTTPS
- rad sa tokenima (autentikacija i autorizacija)