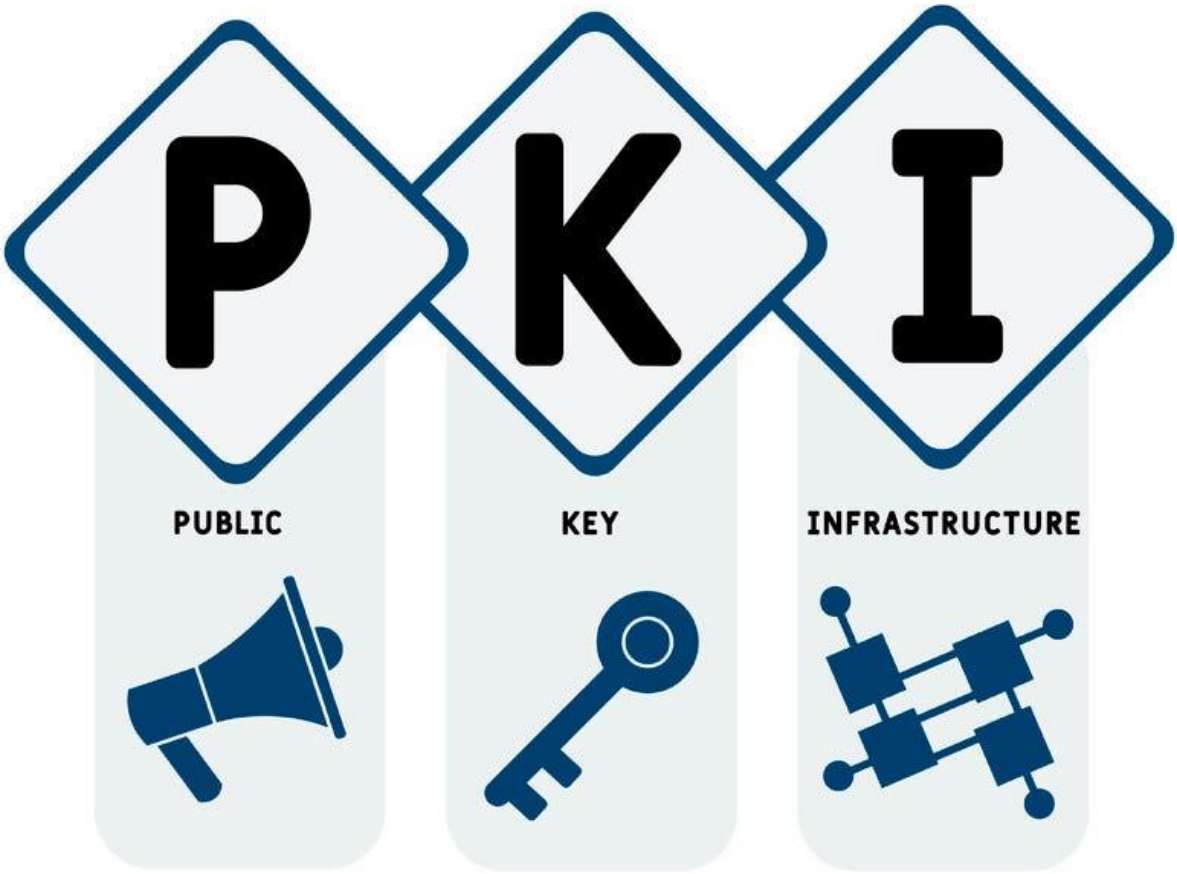

Zahtevi za KT 1

U aplikaciji Booking:

1. Za ulogu admina omogućiti zahtevanje sertifikata koji će vam služiti za izdavanje sertifikata u Booking aplikaciji.
2. Za ulogu vlasnik omogućiti zahtevanje sertifikata koji će služiti za digitalno potpisivanje poruka.
3. Sertifikate distribuirati na bezbedan način.
4. Omogućiti da korisnici *Booking* aplikacije koriste sigurnu verziju HTTP protokola.

U servisu PKI:

1. Admin može centralizovano da izdaje sertifikate za digitalne entitete u svom sistemu (PKI). Adminu treba omogućiti da izda bilo koji sertifikat u lancu sertifikata, što podrazumeva izdavanje samopotpisanih sertifikata, intermediate sertifikata (CA) i end-entity sertifikata. Neophodno je uzeti u obzir da može postojati proizvoljno mnogo nivoa intermediary sertifikata.
2. Admin treba da ima uvid u sertifikate koji postoje na sistemu.
3. Prilikom implemetacije voditi računa o:
    a. Ukoliko se izdaje end-entity sertifikat, potrebno je sprečiti čuvanje privatnih ključeva na PKI sistemu. Privatni i javni ključ za end-entity korisnike može biti izgenerisan eksterno (od strane korisnika), ili opcijom autogenerate, pri čemu PKI sistem generiše par ključeva, ali ih ne čuva.
    b. Pitanje za razmatranje: da li se svi sertifikati čuvaju u istom KeyStore fajlu?
    c. Da li treba čuvati informacije o tome kom tipu entiteta se sertifikat izdaje (servisu, podsistemu, korisniku)?
    d. Potrebno je omogućiti šablone za sertifikate, gde se šablonom definišu ekstenzije koje će ući u sertifikat, a pre svega namena sertifikata. Adminu treba što više olakšati popunjavanje svih podataka koji su potrebni za sertifikat.
    e. PKI treba da uzme u obzir validnost sertifikata u kontekstu izbora izdavaoca. Kada izdajem sertifikat koji nije root (nije samopotpisan) koje sertifikate mogu da ponudim kao opciju za njegovo potpisivanje? Kada je sertifikat validan? Da li je validnost sertifikata određena samo datumom njegovog isteka?
    f. Obratiti pažnju na best practice konfiguraciju bezbednosnih funkcija koje se koristite.
    g. Admin ima mogućnost da povuče sertifikat. PKI treba da pruži servis za proveru da li je sertifikat povučen. Koju tehniku za proveru povučenosti sertifikata treba koristiti? Šta se desi sa sertifikatima koje je intermediary sertifikat potpisao pošto je on povučen?
    h. Obratite pažnju na vreme trajanja sertifikata (root CA, subordinate/intermediate CA, end user). Isto tako razmislite o “trajanju” privatnog ključa CA, tj. do kada se može koristiti za potpisivanje sertifikata.

Napomena: Studenti koji rade sami, za prvu kontrolnu tačku implementiraju izdavanje sertifikata svih niova i proveru povučenosti. Nije potrebno voditi računa o čuvanju ključeva za end-entity sertifikate. Takođe, jednočlani timovi su oslobođeni autogenerate funkcionalnosti.