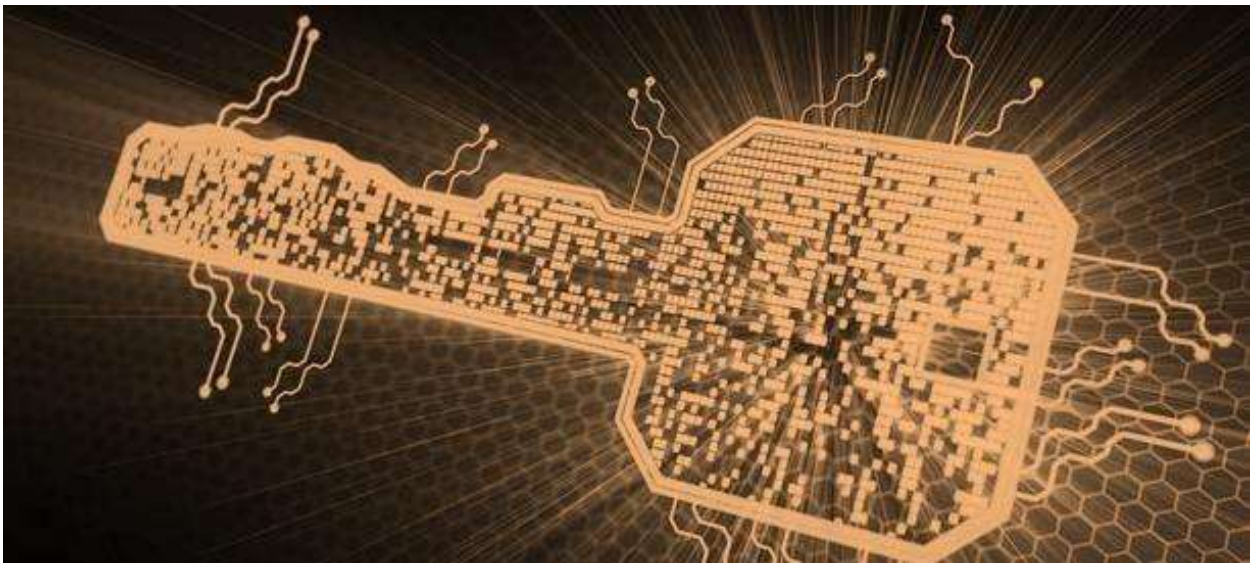

Infrastruktura javnih ključeva

Prva kontrolna tačka

Kontekst

Multinacionalna korporacija koja nudi svoje usluge mušterijama širom sveta. Kako bi podržala milione mušterija i hiljade zaposlenih, kao i očuvala položaj svetskog lidera na svom tržištu, koorporacija raspolaže sa značajnim brojem softverskih podsistema, od internih alata i informacionih sistema, do servisa dostupnih putem interneta. Zbog velike količine vrednih podataka i svoje pozicije na tržištu, softver ove korporacije predstavlja značajnu metu za napad od strane kriminalaca i konkurenata.

Bitan čvor za bezbednost ovog sistema predstavlja podsistem za infrastrukturu javnih ključeva (u daljem tekstu *PKI*). Uz pomoć ovog podsistema, security administrator (u daljem tekstu *admin*) može da poveća bezbednost. Pored security admin-a, PKI mogu da koriste intermediary i end entiteti, koji imaju prava da pregledaju svoje sertifikate i da ih preuzmu (ovo naročito treba uzeti u razmatranje i pri implementaciji narednih kontrolnih tačaka).

Cilj zadatka

Kao glavni rezultat ovog zadatka, svaki student treba da stekne jasnu sliku koju ulogu sertifikati i PKI podsistem igraju u distribuiranom softverskom sistemu, kako se integrišu sa istim, i koje komplikacije i problemi postoje u ovoj priči.

Specifikacija

Admin može centralizovano da izdaje sertifikate za digitalne entitete u svom sistemu. Adminu treba omogućiti da izda bilo koji sertifikat u lancu sertifikata, što podrazumeva izdavanje samopotpisanih sertifikata, intermediate sertifikata (CA) i end-entity sertifikata. Pitanje za razmatranje : da li se svi sertifikati čuvaju u istom KeyStore fajlu? Da li treba čuvati informacije o tome kom tipu entiteta se sertifikat izdaje (servisu, podsistemu, korisniku)? Neophodno je uzeti u obzir da može postojati proizvoljno mnogo nivoa intermediary sertifikata.

Pored admina, svaki CA (vlasnik intermediate sertifikata) može da izdaje nove intermediate ili end-entity sertifikate. Obratiti pažnju koje sertifikate CA može da ponudi za izdavanje.

Potrebno je omogućiti templejte za sertifikate, gde se templejtom definišu ekstenzije koje će ući u sertifikat, a pre svega namena sertifikata.

Admin treba da ima uvid u sertifikate koji postoje na sistemu.

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?

Adminu treba što više olakšati popunjavanje svih podataka koji su potrebni za sertifikat.

Obratiti pažnju na *best practice* konfiguraciju bezbednosnih funkcija koje se koristite.

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 (CRL koji pati od niza problema ili OCSP)? Šta se desi sa sertifikatima koje je intermediary sertifikat potpisao pošto je on povučen?

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.