Odlično! Ovo je složeniji zadatak koji kombinuje pronalaženje privatnog ključa i upravljanje CA (Certificate Authority) funkcijama (izdavanje, opoziv i obnova CRL-a).

Evo detaljnog pojašnjenja zadatka i skripte za rješavanje.

🧐 Pojašnjenje Zadatka 5

Zadatak se sastoji iz tri logička koraka:

Korak 1: Pronalaženje Ispravnog Privatnog Ključa (The Key Match)

1. **Imate:** Datoteku **cert.p12** (PKCS#12 format) i niz potencijalnih privatnih ključeva (**kljuc1.key** **do** **kljuc100.key**).
2. **PKCS#12:** Ova datoteka obično sadrži par ključeva (javni i privatni) i sertifikat u jednom fajlu. Lozinka za otvaranje datoteke je **"sigurnost"**.
3. **Cilj:** Odrediti koji od 100 datih privatnih ključeva (kljucX.key) je **identičan** privatnom ključu koji se nalazi unutar **cert.p12**.

- **Metoda:** Morate ekstrahovati javni ključ iz sertifikata unutar cert.p12 i uporediti ga sa javnim ključevima izvedenim iz svakog od 100 privatnih ključeva, ili (lakše) direktno uporediti ključeve.

Korak 2: Priprema za CA funkcije

1. **Cilj:** Koristeći pronađeni ispravan privatni ključ, potrebno je postaviti strukturu CA tijela.
2. **Ključno:** Zavisite od **konfiguracionog fajla (npr. openssl.cnf)** iz 6. zadatka. Za potrebe skripte, pretpostavićemo da je taj fajl dostupan i da se zove npr. ca.cnf.

Korak 3: Upravljanje CRL (Certificate Revocation List)

Ovaj dio je najkompleksniji i zahtijeva specifične OpenSSL komande za upravljanje bazom podataka opozvanih sertifikata.

- **Prva CRL Lista:**
  - **Potrebno:** Opozvati (revocirati) dva sertifikata.
    - Prvi sertifikat: Opozvan sa razlogom **"suspendovan"** (engl. cessationOfOperation).
    - Drugi sertifikat: Opozvan sa razlogom **"prestanak rada"** (engl. certificateHold).
- **Druga CRL Lista:**
  - **Potrebno:**
    - Drugi sertifikat: Ostaje opozvan.
    - Prvi sertifikat: **Vraćen iz suspenzije** (un-revoked, un-held).

💻 Generisanje Skripte za Rješavanje (skripta5.sh)

S obzirom na složenost, podijelićemo skriptu na tri dijela, kako bi pratila logiku zadatka.

Dio 1: Pronalaženje Ispravnog Ključa

Pouzdan način za pronalaženje podudarnosti je uporediti **modulus (modul)** privatnog ključa iz cert.p12 sa modulusom svakog od 100 ključeva.
Bash

```
#!/bin/bash

# --- KORAK 1: PRONALAZENJE KLJUCA ---

echo "--- 1. Pretraga ispravnog kljuca ---"
# Ekstrahovanje privatnog kljuca iz P12 i dešifrovanje (koristimo 'sigurnost')
# Zatim ekstrahovanje modula za poredjenje
openssl pkcs12 -in cert.p12 -nocerts -nodes -password pass:sigurnost | \
openssl rsa -modulus -noout > p12_modulus.txt

# Postavljanje CA fajlova
CERT_TO_REVOKE_1="clientcert_A.pem" # Imena sertifikata za opoziv, pretpostavljamo da su dostupni
CERT_TO_REVOKE_2="clientcert_B.pem"

FOUND_KEY=""

for k in kljuc*.key; do
    # Ekstrahovanje modula iz trenutnog kljuca
    kljuc_modulus=$(openssl rsa -in "$k" -modulus -noout 2>/dev/null)

    # Poredjenje sa modulusom iz P12
    if grep -q "$kljuc_modulus" p12_modulus.txt; then
        FOUND_KEY="$k"
        echo "☑ Ispravan kljuc je pronadjen: $FOUND_KEY"
        break
    fi
done

if [ -z "$FOUND_KEY" ]; then
    echo "❌ Kljuc nije pronadjen. Prekid."
    exit 1
fi

# Cleanup
rm p12_modulus.txt

# --- KORAK 2: PRIPREMA ZA CA (PRETPOSVLJENO) ---

# Pretpostavlja se da je CA sertifikat (CAcert.pem) kreiran i inicijalizovan (npr. iz zadatka 6)
# Pretpostavlja se postojanje ca.cnf, index.txt i serial fajlova.

CA_KEY="$FOUND_KEY" # Koristi pronadjeni kljuc
CA_CERT="CAcert.pem" # Pretpostavljeno CA ime
CA_CNF="ca.cnf"      # Pretpostavljeni config fajl iz Zadatka 6
INDEX_FILE="index.txt"
SERIAL_FILE="serial"

# Inicijalizacija baze podataka (ako nije vec uradjena od Zadatka 6)
```

```
touch "$INDEX_FILE"
echo 01 > "$SERIAL_FILE"
echo "--- CA Baza podataka inicijalizovana ---"

# --- KORAK 3: UPRAVLJANJE CRL LISTAMA ---

echo "--- 3. Generisanje CRL lista ---"

# 3.1 Opoziv (Revocation) za Prvu CRL Listu

# Opoziv 1: Suspendovan (certificateHold)
echo "Opoziv sertifikata 1 (Suspenzija)"
openssl ca -config "$CA_CNF" -keyfile "$CA_KEY" -cert "$CA_CERT" \
   -revoke "$CERT_TO_REVOKE_1" -crl_reason certificateHold -batch

# Opoziv 2: Prestanak rada (cessationOfOperation)
echo "Opoziv sertifikata 2 (Prestanak rada)"
openssl ca -config "$CA_CNF" -keyfile "$CA_KEY" -cert "$CA_CERT" \
   -revoke "$CERT_TO_REVOKE_2" -crl_reason cessationOfOperation -batch

# Generisanje PRVE CRL liste
echo "Generisanje prve CRL liste: crl1.pem"
openssl ca -config "$CA_CNF" -keyfile "$CA_KEY" -cert "$CA_CERT" \
   -gencrl -out crl1.pem

# 3.2 Opoziv (Revocation) za Drugu CRL Listu

# Vracanje Prvog sertifikata iz suspenzije (Un-revocation)
echo "Vracanje sertifikata 1 iz suspenzije (Undoing certificateHold)"
openssl ca -config "$CA_CNF" -keyfile "$CA_KEY" -cert "$CA_CERT" \
   -crl_hold off -revoke "$CERT_TO_REVOKE_1" -batch

# Napomena: Sertifikat 2 ostaje opozvan (cessationOfOperation je trajni opoziv)

# Generisanje DRUGE CRL liste
echo "Generisanje druge CRL liste: crl2.pem"
openssl ca -config "$CA_CNF" -keyfile "$CA_KEY" -cert "$CA_CERT" \
   -gencrl -out crl2.pem

echo "--- Završeno. Proverite crl1.pem i crl2.pem ---"
```

4. Sugestije i Važne Napomene

1. **Dostupnost Fajlova:** Skripta pretpostavlja da su sertifikati koji se opozivaju (clientcert_A.pem i clientcert_B.pem) i CA sertifikat (CAcert.pem) dostupni i validni. U stvarnosti, morate izvući sertifikat iz cert.p12 ili koristiti sertifikate iz drugih zadataka.
    - **Ekstrakcija sertifikata iz P12:**
      Bash
      openssl pkcs12 -in cert.p12 -clcerts -nokeys -out cert_from_p12.pem -password pass:sigurnost
2. **CA Konfiguracija:** Linije koje se tiču CA operacija (openssl ca -config...) **neće raditi** ako nemate ispravan ca.cnf i prateću CA strukturu (prazan index.txt i serial fajl sa

serijskim brojem). Zadatak 6 se bavi CA setupom i bez njega ovaj dio ne možete izvršiti.

3. **Razlozi za Opoziv:** OpenSSL koristi specifične ključne riječi za razloge opoziva:
    - suspendovan $\rightarrow$ certificateHold (Može se vratiti)
    - prestanak rada $\rightarrow$ cessationOfOperation (Trajan opoziv)
4. **Vraćanje iz Suspenzije:** Vraćanje iz suspenzije (un-revoking) se vrši ponovnim opozivanjem sa zastavicom -crl_hold off.

Da li želite da Vam pomognem sa analizom narednog zadatka (verovatno Z6, CA setup) ili da se fokusiramo na detalje oko generisanja CRL lista?