

# SİL Sorgulama Kütüphanesi

## Kullanım Kılavuzu

### Sürüm 0.1

- **SİL (Sertifika İptal Listesi) Bulma Servisi Nedir?**

- SİL yayınlayan bir Elektronik Sertifika Hizmet Sağlayıcısının (ESHS) önceden yayınlamış olduğu SİL'leri takip etmek yada bulmak çoğu zaman mümkün olmamaktadır. Herhangi bir tarihte hangi sertifikaların iptal edildiği araştırılırken ilgili SİL'i bulmak ve kullanmak gerekmektedir.
- Bu gibi sebeplerden ötürü Kamu Sertifikasyon Merkezi SİL Bulma Servisi kurulmuştur. Sistem, üzerinde önceden tanımlanmış olan ESHS'lerin SİL'lerini sürekli olarak toplayan, bunları depolayan ve yapılan sorgulara göre istenen SİL'in adresini kullanıcıya gönderen bir yapıda tasarlanmıştır.
- Servis, sorgulamak istediğiniz ESHS'nin sertifikasını ve istediğiniz sorgu kriterini girdiğinizde size sorgunuza en uygun SİL'in adresini döner (URL adresi olarak). Bu URL adresindeki dosyayı indirdiğinizde, istediğiniz SİL dosyasını elde etmiş olursunuz..

- **SİL Bulucu Arayüz ile Ne Şekilde Sorgulama Yapabilirim?**

- Sorgulamak istediğiniz ESHS'nin sertifikasını ve Sorgulama kriterlerini girmeniz gerekmektedir.
- **Sorgulama Kriterleri:** Sorgulanacak olan SM nin sertifikasının girilmesi zorunludur, bundan sonra tercihli olarak:
  - **SİL Numarası ile:** Verilen Belirtilen SİL numarasına sahip SİL'in adresini getirir.
  - **SİL Tarihi:** Verilen tarihten önceki yada sonraki ilk SİL'in adresini getirir.
  - **SİL Özeti ile:** Verilen SİL özetine sahip SİL'in Adresini getirir.
- İsteddiğiniz SİL'in adresini aldıktan sonra bu adresten mevcut SİL'i indirebilirsiniz.

## ○ SİL Bulucu Arayüz:

SİL Sorgulama Arayüzü

SİL Sunucusu:

Sorgulanacak SM nin

Sertifikasını Gir

SM Serial Number:

Sorgulama Tipi

SİL No ile Tarih ile Özet ile

SİL Numarası:

Sorgular:

- ✓ Arayüzde ilk olarak bağlanacak olduğumuz SİL Bulma Servisinin URL adresi girilir.
- ✓ Daha sonra "Sertifikasını Gir" Tuşu tıklanarak SİL'ini sorgulamak istediğimiz ESHS'nin Sertifikası seçilir.
- ✓ Sorgulama tipindeki 3 tane sekmeden sorgulamak istediğimiz kriterle ilgili sekme seçilerek gerekli alanlar doldurulur.
- ✓ En sonunda Sorgula tuşuna tıklanarak sorgulama işlemi yapılır.

## ○ SİL Sorgulama Kütüphanesi Kullanımı

Verilen "SilBulmaApi.jar" kütüphanesini projemize ekleyip Sillstemci sınıfını kullanarak sorgulama işlemi yapabiliriz. Örnek olarak Sertifikanın okunması, parametlerin ayarlanması aşağıdaki kodda gösterilmiştir. Özet ile sorgulama için geçerli özet tipleri: SHA1 ve SHA256 dır.

```

SilIstemci silIstemci = new SilIstemci();
silIstemci.setHostURL(new URL("http://localhost:8093"));
silIstemci.setTimeoutInSec(6);

Certificate certificate = new Certificate();
AsnIO.dosyadanOKU(certificate, "D:\\Projects\\SilBulmaServisi\\TestSertifikaMakamı.cer");

List silAdresleri;

BigInteger silNo = new BigInteger("179", 10);
silAdresleri = silIstemci.silSorgulaSilNumarasiile(certificate, silNo);

for (int i = 0; i < silAdresleri.size(); i++) {
    System.out.println("s1:" + silAdresleri.get(i));
}

Calendar date = Calendar.getInstance();
date.setTimeInMillis(System.currentTimeMillis());

silAdresleri = silIstemci.silSorgulaTarihindenOnceki(certificate, date);

for (int i = 0; i < silAdresleri.size(); i++) {
    System.out.println("s2:" + silAdresleri.get(i));
}
silAdresleri = silIstemci.silSorgulaTarihindenSonraki(certificate, date);

for (int i = 0; i < silAdresleri.size(); i++) {
    System.out.println("s3:" + silAdresleri.get(i));
}
byte[] silBytes = AsnIO.dosyadanOKU("D:\\Projects\\SilBulmaServisi\\SilDosyaları\\2\\2007-09\\2\\10121
MessageDigest messageDigest = MessageDigest.getInstance("SHA-256");
byte[] digest = messageDigest.digest(silBytes);

silAdresleri = silIstemci.silSorgulaSilOzetiile(certificate, "SHA-256", digest);

for (int i = 0; i < silAdresleri.size(); i++) {
    System.out.println("s4:" + silAdresleri.get(i));
}

```

Şekil 1- Örnek Kod

- ✓ SilIstemci sınıfından bir nesnesi instance oluşturularak kullanılır.
- ✓ Ulaşılabilecek servisin adresi **setHostURL** ile ayarlanır.
- ✓ Sorgulanacak SM nin sertifikası AsnIO yardımı ile dosya sisteminden okunur.
- ✓ Verilecek diğer kriterler belirlenir(tarih, sil numarası,özet vs)
- ✓ Silistemci Nesnemizin ilgili sorgula methodu çağırılır. Bu methodun geri döndüğü liste bize istediğimiz Sil lerin Url adreslerini gösterir. Sonuç boş ise aradığımız kriterlere uygun Sil bulunamamış demektir.
- ✓ Verilen sunucuya bağlanamama gibi durumlarda Silistemci nesnemiz hata atar.
- ✓ Fonksiyonlar ve Parametreleri:
  - **silSorgulaTarihindenOnceki**> Sertifika + Tarih
  - **silSorgulaTarihindenSonraki**> Sertifika + Tarih
  - **silSorgulaSilNumarasiile** > Sertifika + SilNumarası(BigInteger olarak)
  - **silSorgulaSilOzetiile** > Sertifika + Ozet Tipi(SHA-1, SHA-256) + Ozet(Byte Array olarak)
- ✓ **Proxy** kullanılıyor ise Java'nın standart proxy ayarlama yöntemi kullanılabilir.