



TÜBİTAK BİLGEM

KAMU SERTİFİKASYON MERKEZİ

**TASNİF DIŐI**

## SSL (GÜVENLİ CİHAZ) SERTİFİKASI İSTEK DOSYASI OLUŐTURMA VE YÜKLEME REHBERİ

Doküman Kodu	Yayın Numarası	Yayın Tarihi
REHB-001-016	02	07.06.2016

Uyarı : Yalnız Kamu SM dosya sunucudan erişilen elektronik kopyalar güncel ve kontrollü olup, elektronik ortamdan alınacak kağıt baskılar KONTROLSÜZ KOPYA'dır

**TASNİF DIŐI**



**SSL (GÜVENLİ CİHAZ) SERTİFİKASI İSTEK DOSYASI  
OLUŐTURMA VE YÜKLEME REHBERİ**

**DEĐİŐİKLİK KAYITLARI**

<b>Yayın No</b>	<b>Yayın Nedeni</b>	<b>Yayın Tarihi</b>
00	İlk Çıkıő	27.12.2011
01	İçerik Güncelleme	29.05.2013
02	İçerik Güncelleme	07.06.2016

UYARI: Yalnız Kamu SM doküman yönetim sisteminden erişilen elektronik kopyalar güncel ve kontrollü olup, elektronik ortamdan alınacak kâğıt baskılar KONTROLSÜZ KOPYADIR.



**SSL (GÜVENLİ CİHAZ) SERTİFİKASI İSTEK DOSYASI  
OLUŐTURMA VE YÜKLEME REHBERİ**

**KISALTMALAR**

<b>Kamu SM</b>	<b>Kamu Sertifikasyon Merkezi</b>
<b>SSL</b>	<b>Secure Sockets Layer</b>



# SSL (GÜVENLİ CİHAZ) SERTİFİKASI İSTEK DOSYASI OLUŐTURMA VE YÜKLEME REHBERİ

## İÇİNDEKİLER

<b>1 Giriő</b> .....	<b>5</b>
<b>2 Amaç ve Kapsam</b> .....	<b>5</b>
<b>3 SSL Sertifikası Üretimi İçin Temel Adımlar</b> .....	<b>5</b>
<b>4 OpenSSL ile SSL Sertifikası İşlemleri</b> .....	<b>7</b>
4.1 Anahtar Çifti Oluőturma .....	7
4.2 CSR Oluőturma .....	8
4.3 Kamu SM'den Gelen Sertifikayı Sunucuya Tanıtma .....	9
<b>5 Java Keytool ile SSL Sertifikası İşlemleri</b> .....	<b>9</b>
5.1 Keystore ve Anahtar Çifti Oluőturma.....	10
5.2 CSR Oluőturma .....	11
5.3 Kamu SM'den Gelen Sertifikayı Sunucuya Tanıtma .....	11
<b>6 Dikkat Edilmesi Gereken Hususlar</b> .....	<b>12</b>



## SSL (GÜVENLİ CİHAZ) SERTİFİKASI İSTEK DOSYASI OLUŐTURMA VE YÜKLEME REHBERİ

### 1 Giriő

Bu doküman, SSL yani güvenli cihaz sertifikası edinmek isteyen kurumlara genel itibariyle yol gösterici bir dokümandır.

### 2 Amaç ve Kapsam

Bu doküman, Kamu SM'den SSL sertifikası almayı planlayan kurumlara, SSL sertifikası edinmek için gerekli adımlar hakkında genel bilgi vermek amacıyla hazırlanmıştır. Sürekli deęişen teknoloji sebebiyle en doęru ve güncel bilgi kurumun sertifikayı yükleyeceęi uygulama sunucusu, web sunucusu vb tedarikçisinden edinilmelidir.

Kamu SM, SSL sertifikası talep edilen domain adresini sertifikalandırmak dışında herhangi bir ürün spesifik problemden sorumlu deęildir.

### 3 SSL Sertifikası Üretimi İçin Temel Adımlar

Kamu SM'den SSL sertifikası almayı planlayan kurumların yapması gereken 3 temel adım vardır. Bunlar;

1. SSL sertifikası için gerekli olan anahtar çiftini ve sertifika istek dosyasını (CSR) oluşturmak.
2. CSR dosyasını Kamu SM'ye göndermek.
3. CSR dosyasına karşılık Kamu SM tarafından üretilen SSL sertifikasını sunucuya tanıtmak.

Anahtar çifti **Açık anahtar** ve **Özel anahtar**dan oluşur (**Public/Private Key Pair**). **CSR** (Certificate Signing Request), dięer adıyla **PKCS#10 istek dosyası** ise SSL alan kurumun açık anahtarından ve kimlik bilgilerinden (CN, OU, O, L, S, C deęerleri) oluşturulan bir dosyadır.

UYARI: Yalnız Kamu SM doküman yönetim sisteminden erişilen elektronik kopyalar güncel ve kontrollü olup, elektronik ortamdan alınacak kâğıt baskılar KONTROLSÜZ KOPYADIR.



## SSL (GÜVENLİ CİHAZ) SERTİFİKASI İSTEK DOSYASI OLUŐTURMA VE YÜKLEME REHBERİ

SSL sertifikası, birinci adımda oluşturulan anahtar çifti ve sertifika istek dosyasına matematiksel olarak baėlıdır. Bundan dolayı sistemde oluşturulan anahtar çifti, CSR ve sisteme yüklenen SSL sertifikası uyuőmazsa sistem düzgün çalışmayacaktır.

SSL sertifikası sunucuya tanıtıldıktan sonra anahtar çiftiyle birlikte SSL sertifikasının yedeėinin alınması (**export**) ve güvenli bir ortamda saklanması önemle tavsiye edilir. Olası bir kayıp/çökme durumunda SSL yedeėinden herhangi bir sunucuya yeniden yükleme yapılabilir (**import**). Anahtarlar olmaksızın, sadece SSL sertifikasının yedeklenmesinin hiçbir fonksiyonu yoktur.

Kurum tarafından oluşturulan anahtarlar (özel anahtar) Kamu SM'ye gönderilmediėinden Kamu SM, SSL anahtarlarını kurtaramaz. Bu sebeple **export** işleminin önemi, kritik verilerin yedeėinin alınmasıyla eődeėerdir.

Joker SSL (wildcard SSL) sertifikası aynı alt alana sahip birden fazla web sayfasının SSL sertifikasıyla kimliklendirilmesi için kullanılır. Örneėin **\*.testdomain.com** şeklinde alınan joker SSL sertifikası; **mail.testdomain.com**, **portal.testdomain.com** vs gibi istenilen sayıda domain adı için kullanılabilir. Bu farklı domain adlarının sunuculardan hizmet verebilmesini sağlamak için tek bir joker SSL sertifikasının hepsine ayrı ayrı yüklenmesi gerekir. İşte bu noktada yine üst paragrafta sözü edilen **export-import** işleminin yapılması gerekir. Yani joker SSL sertifikası, CSR dosyasının ve dolayısıyla anahtar çiftinin oluşturulduėu sunucuya yüklendikten sonra bu sunucudan **export** alınarak bir **PFX** dosyası oluşturulur (PKCS#12 formatında anahtar çifti ve sertifikayı içeren dosyadır), daha sonra bu **PFX** dosyası diėer sunuculara **import**

UYARI: Yalnız Kamu SM doküman yönetim sisteminden erişilen elektronik kopyalar güncel ve kontrollü olup, elektronik ortamdan alınacak kâğıt baskılar KONTROLSÜZ KOPYADIR.



## SSL (GÜVENLİ CİHAZ) SERTİFİKASI İSTEK DOSYASI OLUŐTURMA VE YÜKLEME REHBERİ

edilir. Böylelikle diđer sunuculara da aynı SSL sertifikası (anahtarlarıyla birlikte) yüklenmiŐ olur.

Bu bölümün baŐında tanımlanan temel adımların uygulanmasında genel itibariyle izlenebilecek iki yöntem bulunmaktadır:

- Uygulama sunucusu, web sunucusu vb üreticisi Őirketler tarafından sađlanan **arayüzler** vasıtasıyla
- **OpenSSL, Java Keytool** gibi yaygın kullanılan araçlar vasıtasıyla

### 4 OpenSSL ile SSL Sertifikası İşlemleri

İnternette kolaylıkla bulunabilen ve Windows ortamında da çalışabilen OpenSSL, SSL yüklenecek olan sunucuya kurulur. Komut satırından programın kurulu olduđu dizine gidilir ve komutlar **openssl/bin** dizini altından çalıştırılır.

OpenSSL ilk çalıştırıldığında aŐađıdaki hata ile karşılaşılabılır:

**Warning: can't open config file: C:\Openssl\bin\openssl.cfg**

Hatadan da anlaşılacağı gibi program **openssl.cfg** dosyasını bulamadığı için hata veriyor ve çalışmıyor. AŐađıdaki komut çalıştırılarak sorun çözülür.

**set OPENSSL\_CONF=c:[OpenSSL Dizini]\bin\openssl.cfg**

#### 4.1 Anahtar Çifti OluŐturma

SSL sertifikasının yükleneceđi sunucu üzerinde öncelikle bir anahtar çifti oluŐturulmalıdır. **2048 bit RSA anahtar çifti** oluŐturmak için aŐađıdaki komutlardan biri çalıştırılır:

**openssl genrsa -out <anahtar\_dosyasi>.key 2048**

veya

**openssl genrsa -des3 -out <anahtar\_dosyasi>.key 2048**



## SSL (GÜVENLİ CİHAZ) SERTİFİKASI İSTEK DOSYASI OLUŐTURMA VE YÜKLEME REHBERİ

Yukarıdaki komutlarla oluşturulan anahtar çifti `\openssl\bin` dizini altına yazılır. İlk komut ile ikinci komut arasındaki tek fark ikinci komutun şifre istiyor olmasıdır. CSR oluştururken burada belirlenen şifre sorulacaktır. Bu şifre aynı zamanda anahtarı koruyacağı için güçlü bir şifre olmalıdır.

Örnek kullanım:

```
openssl genrsa -des3 -out ssl_anahtari.key 2048
```

### 4.2 CSR Oluőturma

Bir önceki bölümde oluşturulan anahtar çiftinin sertifikalandırılması için CSR dosyası aşağıdaki komut yardımıyla oluşturulur:

```
openssl req -new -key <anahtar_dosyasi>.key -out  
<istek_dosyasi>.csr
```

Örnek kullanım:

```
openssl req -new -key ssl_anahtari.key -out  
ssl_istek_dosyasi.csr
```

Yukarıdaki komut çalıştırıldığı zaman sertifikayı talep eden kuruma ait bilgiler sorulacaktır. Bilgiler, Kamu SM tarafından kontrol edilerek sertifika içerisine yazılacağından bu bilgilerin doğruluğu önemlidir. Kontrol sonucu olumsuz olan CSR dosyaları sertifikalandırılmayacaktır. Bu bilgiler girilirken dikkat edilmesi gereken hususlar Bölüm 0'da altında anlatılmaktadır.





## SSL (GÜVENLİ CİHAZ) SERTİFİKASI İSTEK DOSYASI OLUŐTURMA VE YÜKLEME REHBERİ

### 4.3 Kamu SM'den Gelen Sertifikayı Sunucuya Tanıtma

Bu aşamada farklı uygulama sunucusu, web sunucusu vb. için işlem farklılaşmaktadır. Bu sebeple uygun işlemlerin sırası ile yapılması gerekmektedir.

### 5 Java Keytool ile SSL Sertifikası İşlemleri

Java diliyle yazılmış web uygulamalarının çalışması için gerekli olan web sunucularda istemci ile sunucu arasında güvenli bir iletişim sağlamak için **Truststore** ve **Keystore** dosyaları kullanılmaktadır. Keystore dosyası özel anahtar kullanarak şifreleme ve imzalama işlemi yaparken, Truststore dosyası genellikle doğrulama işlemleri için kullanılır.

SSL sertifikasının yükleneceği sunucu üzerinde Java Runtime Environment (**JRE**) veya Java Development Kit (**JDK**) kurulu olmalıdır. CSR dosyası oluşturulmadan önce, CSR oluşumunda kullanılmak üzere bir keystore oluşturulmalıdır. Keystore, anahtar ve sertifika yönetim programı olan Java Keytool ile oluşturulur. Java Keytool programı, kullanıcıların kendi anahtar çiftlerini ve sertifikalarını yönetmelerine olanak sağlar.

Java Keystore'da tutulan her sertifika ilgili anahtar çiftiyle ilişkilidir. Bu ilişki benzersiz bir takma ad (alias) ile sağlanır.

Keystore ve Truststore oluşumu 3 adımda gerçekleştirilir:

1. Keystore ve anahtar çifti oluşturulur.
2. Keystore kullanılarak CSR oluşturulur ve Kamu SM'ye gönderilir.

UYARI: Yalnız Kamu SM doküman yönetim sisteminden erişilen elektronik kopyalar güncel ve kontrollü olup, elektronik ortamdan alınacak kâğıt baskılar KONTROLSÜZ KOPYADIR.



## SSL (GÜVENLİ CİHAZ) SERTİFİKASI İSTEK DOSYASI OLUŐTURMA VE YÜKLEME REHBERİ

- Truststore dosyası içerisine Kamu SM'den gelen SSL sertifikası ile bu sertifikanın üst makam sertifikaları import edilir.

### 5.1 Keystore ve Anahtar Çifti OluŐturma

Java keytool ile anahtarlar ve sertifikalar bir keystore (anahtar deposu) dosyası içinde saklanır. Windows sistemlerde keytool komutu Java bin dizininde çalıştırılır:

```
keytool -genkey -alias <takma_ad> -keyalg RSA -keysize 2048  
-keystore <domain_adi>.jks
```

Örnek kullanım:

```
keytool -genkey -alias takma_ad_ssl -keyalg RSA -keysize 2048  
-keystore mail.testdomain.com.jks
```

**NOT:** Bu komutta **takma\_ad\_ssl** sadece örnek bir takma addır. **RSA** anahtar algoritmasıdır. **2048** anahtar boyudur. **mail.testdomain.com** SSL ile kimliklendirmek istediğiniz domain adıdır. Eğer Joker (wildcard) SSL alıyorsanız domain adının başındaki \* karakterini dosya adına koymayınız çünkü dosya adında \* karakterine izin verilmez. Esasen dosya adının ne olduğunun önemi yoktur, sadece anlaşılır olması için örnekte domain adı dosya adı olarak kullanılmıştır.

**NOT:** **jks=java key store.**

Komut çalıştırıldığında, keystore için şifre ve sertifikada yer alacak bilgiler sorulacaktır, ardından keystore oluşacaktır. Bu örnekte keystore dosyası, özel olarak belirtilmediği için <JAVAHOME>\bin dizini



## SSL (GÜVENLİ CİHAZ) SERTİFİKASI İSTEK DOSYASI OLUŐTURMA VE YÜKLEME REHBERİ

altında oluşturulmuŐtur. CSR oluşturulurken ve Kamu SM'den gelen SSL sertifikası sisteme yüklenirken aynı takma adının (bu örnekte **takma\_ad\_ssl**) kullanılması gerekmektedir.

### 5.2 CSR OluŐturma

AŐağıdaki komut yardımıyla CSR oluşturulur ve Kamu SM'ye gönderilir.

```
keytool -certreq -keyalg RSA -alias <takma_ad> -file  
<domain_adi>.csr -keystore <domain_adi>.jks
```

Örnek kullanım:

```
keytool -certreq -keyalg RSA -alias takma_ad_ssl -file  
mail.testdomain.com.csr -keystore mail.testdomain.com.jks
```

### 5.3 Kamu SM'den Gelen Sertifikayı Sunucuya Tanıtma

Kamu SM'den gelen SSL sertifikasını import etmeden önce Kamu SM kök ve alt kök sertifikalarını sisteme tanıtmak gerekir. Kök sertifikayı tanıtmak için:

```
keytool -import -alias root -file koksertifika.cer -keystore  
mail.testdomain.com.jks
```

Alt kök sertifikayı tanıtmak için:

```
keytool -import -alias intermediate -file altkoksertifika.cer  
-keystore mail.testdomain.com.jks
```



## SSL (GÜVENLİ CİHAZ) SERTİFİKASI İSTEK DOSYASI OLUŐTURMA VE YÜKLEME REHBERİ

Kamu SM'den gelen sertifika dosyası (.cer veya .crt uzantılı bir dosya olacaktır, bu örnekte dosyanın **mail.testdomain.com.cer** olduğunu düşünelim) Truststore dosyası içerisine aşağıdaki komut yardımıyla import edilir.

```
keytool -import -alias takma_ad_ssl -file  
mail.testdomain.com.cer -keystore mail.testdomain.com.jks
```

### 6 Dikkat Edilmesi Gereken Hususlar

Anahtarlar oluşturulurken RSA olmasına ve uzunluğunun 2048 bit olmasına dikkat edilir.

CSR dosyası oluşturulurken SSL alan kuruma ait birtakım bilgilerin girilmesi gerekmektedir.

Bu bilgilerin neler olduğu ve girilirken nelere dikkat edilmesi gerektiği şöyle sıralanabilir:

- CN (Common Name) alanına SSL ile kimliklendirilecek web sayfasının adresi https veya http olmadan girilir (örneğin **mail.testdomain.com** veya **\*.testdomain.com** yazılır, **https://mail.testdomain.com** veya **https://\*.testdomain.com** yazılmaz)
- OU (Organizational Unit) alanına kurum departmanı yazılır (örneğin **Bilgi İşlem Departmanı**)
- O (Organization) alanına kurum adı yazılır (örneğin **Elazığ Belediyesi**)



**SSL (GÜVENLİ CİHAZ) SERTİFİKASI İSTEK DOSYASI  
OLUŐTURMA VE YÜKLEME REHBERİ**

- L (Location) alanına kurumun bulunduđu ilçe yazılır (örneğin **Elazig**)
- S (State or Province) alanına kurumun bulunduđu il yazılır (örneğin **Elazig**)
- C (Country) alanına kurumun bulunduđu ülkenin 2 karakterli kodu yazılır (Türkiye için **TR**)
- CN, OU, O, L, S ve C girilmesi zorunlu alanlardır. Bunların dışındaki alanlar isteđe bađlıdır. Tüm bu alanlar için deđerler girilirken Türkçe karakterler yerine İngilizce karakterler kullanılmalıdır. Örneđin:
  - **Elazıđ Belediyesi** yerine **Elazig Belediyesi**, (ı yerine i, đ yerine g)
  - **Bilgi İşlem Departmanı** yerine **Bilgi Islem Departmani** (ő yerine s, ı yerine i, İ yerine I)