TÜBİTAK BİLGEM
KAMU SERTİFİKASYON MERKEZİ

SSL (GÜVENLİ CİHAZ) SERTİFİKASI İSTEK DOSYASI OLUŞTURMA VE YÜKLEME REHBERİ

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

SSL (GÜVENLİ CİHAZ) SERTİFİKASI İSTEK DOSYASI OLUŞTURMA VE YÜKLEME REHBERİ

DEĞİŞİKLİK KAYITLARI

Yayın No	Yayın Nedeni	Yayın Tarihi
00	İlk Çıkış	27.12.2011
01	İçerik Güncelleme	29.05.2013
02	İçerik Güncelleme	07.06.2016

SSL (GÜVENLİ CİHAZ) SERTİFİKASI İSTEK DOSYASI OLUŞTURMA VE YÜKLEME REHBERİ

KISALTMALAR

Kamu SM	**Kamu** Sertifikasyon **M**erkezi
SSL	**S**ecure **S**ockets **L**ayer

TÜBİTAK BİLGEM

KAMU SERTİFİKASYON MERKEZİ

SSL (GÜVENLİ CİHAZ) SERTİFİKASI İSTEK DOSYASI OLUŞTURMA VE YÜKLEME REHBERİ

İÇİNDEKİLER

SSL (GÜVENLİ CİHAZ) SERTİFİKASI İSTEK DOSYASI OLUŞTURMA VE YÜKLEME REHBERİ

1 Giriş

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 değişen teknoloji sebebiyle en doğru ve güncel bilgi kurumun sertifikayı yükleyeceği uygulama sunucusu, web sunucusu vb tedarikçisinden edinilmelidir.
Kamu SM, SSL sertifikası talep edilen domain adresini sertifikalandırmak dışında herhangi bir ürün spesifik problemden sorumlu değildir.

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** (**C**ertificate **S**igning **R**equest), diğer adıyla **PKCS#10 istek dosyası** ise SSL alan kurumun açık anahtarından ve kimlik bilgilerinden (CN, OU, O, L, S, C değerleri) oluşturulan bir dosyadır.

SSL (GÜVENLİ CİHAZ) SERTİFİKASI İSTEK DOSYASI OLUŞTURMA VE YÜKLEME REHBERİ

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

SSL sertifikası sunucuya tanıtıldıktan sonra anahtar çiftiyle birlikte SSL sertifikasının yedeğinin alınması (**export**) ve güvenli bir ortamda saklanması önemle tavsiye edilir. Olası bir kayıp/çökme durumunda SSL yedeğinden 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 gönderilmediğinden Kamu SM, SSL anahtarlarını kurtaramaz. Bu sebeple **export** işleminin önemi, kritik verilerin yedeğinin alınmasıyla eşdeğerdir.

Joker SSL (wildcard SSL) sertifikası aynı alt alana sahip birden fazla web sayfasının SSL sertifikasıyla kimliklendirilmesi için kullanılır. Örneğin ***.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 oluşturulduğu 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 diğer sunuculara **import**

edilir. Böylelikle diğer sunuculara da aynı SSL sertifikası (anahtarlarıyla birlikte) yüklenmiş olur.

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

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

4 OpenSSL ile SSL Sertifikası İşlemleri

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

OpenSSL ilk çalıştırıldığında aşağıdaki hata ile karşılaşılabilir:

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. Aşağıdaki komut çalıştırılarak sorun çözülür.

set OPENSSL_CONF=c:\[OpenSSL Dizini]\bin\openssl.cfg

4.1 Anahtar Çifti Oluşturma

SSL sertifikasının yükleneceği sunucu üzerinde öncelikle bir anahtar çifti oluşturulmalıdır. **2048 bit RSA anahtar çifti** oluşturmak için aşağıdaki komutlardan biri çalıştırılır:

openssl genrsa -out <anahtar_dosyasi>.key 2048

veya

openssl genrsa -des3 -out <anahtar_dosyasi>.key 2048

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 Oluşturma

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.

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 anahtarı 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.

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

5.1 Keystore ve Anahtar Çifti Oluşturma

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=**j**ava **k**ey **s**tore.

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

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

5.2 CSR Oluşturma

Aşağıdaki 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**

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 Islem Departmani**)
- O (Organization) alanına kurum adı yazılır (örneğin **Elazig Belediyesi**)

- L (Location) alanına kurumun bulunduğu ilçe yazılır (örneğin **Elazig**)
- S (State or Province) alanına kurumun bulunduğu il yazılır (örneğin **Elazig**)
- C (Country) alanına kurumun bulunduğu ülkenin 2 karakterli kodu yazılır (Türkiye için **TR**)
- CN, OU, O, L, S ve C girilmesi zorunlu alanlardır. Bunların dışındaki alanlar isteğe bağlıdır. Tüm bu alanlar için değerler girilirken Türkçe karakterler yerine İngilizce karakterler kullanılmalıdır. Örneğin:
  - **Elazığ Belediyesi** yerine **Elazig Belediyesi**, (ı yerine i, ğ yerine g)
  - **Bilgi İşlem Departmanı** yerine **Bilgi Islem Departmani** (ş yerine s, ı yerine i, İ yerine I)