HSM CİHAZINA ANAHTAR VE SERTİFİKA YÜKLEME BİLGİ FORMU VE TAAHHÜTNAMESİ

Anahtar ve Sertifika Sahibi Kurum Bilgileri

Kurum Adı/ Ünvanı:	
Kurum DETSİS No:	
Kurum Adresi:	
Posta Kodu:	
Vergi Dairesi:	
Vergi Kimlik No:	
Telefon:	
Kurum E-posta:	

HSM Sahibi Kurum Bilgileri*

Kurum Adı/ Ünvanı:	
Kurum DETSİS No:	
Kurum Adresi:	
Posta Kodu:	
Vergi Dairesi:	
Vergi Kimlik No:	
Telefon:	
Kurum E-posta:	

**Anahtar ve Sertifika Sahibi Kurum ile HSM Sahibi Kurum aynı olduğu durumda doldurulmasına gerek yoktur.*

Kurum HSM Cihaz Sorumlusu

Adı Soyadı:	
T.C. Kimlik No:	
İş Adresi:	
İş Telefonu:	
Cep Telefonu:	
Kurumsal E-posta:	

Yukarıda belirtilen bilgilerin doğru olmaması durumunda doğacak bütün zararlardan sorumlu olduğumu beyan eder, kurumum adına HSM cihazına anahtar yükleme süreçlerinden sorumlu olduğumu taahhüt ederim.

◉ İşbu form ve taahhütnameye HSM Cihaz Sorumlusu e-imza atacaktır.

Hazırlanan form ve taahhütname üst yazısı ile birlikte EYP 2.0 dosyası oluşturularak iletilebilir. EYP dosyası bu bölümde bilgileri yer alan HSM Cihaz Sorumlusu ve kurum onayı kısmında yer alan kurum yetkilisi tarafından elektronik olarak imzalandıktan sonra kurum elektronik mührü kullanılarak mühürlenmelidir. Oluşturulan EYP dosyası kurumsal e-posta adresi veya KEP üzerinden Kamu SM'ye iletilmelidir.

○ İşbu form ve taahhütnameye HSM Cihaz Sorumlusu ıslak imza atacaktır.

Hazırlanan form ve taahhütname, bilgi@kamusm.gov.tr veya kurumsal_bilgi@kamusm.gov.tr adreslerinden birine e-posta ile iletilebilir. E-posta ile gönderim durumunda form ve taahhütnamenin ayrıca TÜBİTAK BİLGEM Gebze Yerleşkesi (İdari Bina) P.K. 74 41470, Gebze Kocaeli adresine posta yoluyla iletilmesi gerekmektedir.

Uyarı: Kamu SM dosya sunucudan erişilen elektronik kopyalar güncel ve kontrollü olup, diğer baskılar kontrolsüz kopyadır.

HSM CİHAZINA ANAHTAR VE SERTİFİKA YÜKLEME BİLGİ FORMU VE TAAHHÜTNAMESİ

HSM Cihazına Anahtar ve Sertifika Yükleme Bilgi Formu

HSM Cihazına Anahtar ve Sertifika Yüklemede Kullanılacak Yöntem

○ Yerinde* ● Uzaktan (Önerilen)

Yerinde Yükleme Sebebi:

Kurum HSM Cihazı

ESN No:	
Cihaz IP Adresi:	
Marka-Model Bilgisi:	
Milli HSM Cihazı:	○

(Kullanılacak cihaz yerli ve milli ise kutucuğu işaretleyiniz)

Kurum Yedek HSM Cihazı

ESN No:	
Cihaz IP Adresi:	
Marka-Model Bilgisi:	
Milli HSM Cihazı:	○

(Kullanılacak cihaz yerli ve milli ise kutucuğu işaretleyiniz)

- Elektronik mühür ve kurumsal şifreleme sertifikaları, kurumunuz tarafından temin edilen HSM cihazına yüklenir. İşbu form ve taahhütname ile kurumunuz, tüm yasal sorumluluğun kendisine ait olduğunu taahhüt eder.
- Bilgi Teknolojileri Dairesi Başkanlığınca hazırlanmış "Kurumsal Şifreleme ve Elektronik Mühür Sertifikalarına İlişkin Usul ve Esaslar"ın 11. maddesinin 3. fıkrasında "İşbu maddede belirlenen standartlara uygun milli veya yerli güvenli elektronik imza oluşturma aracı mevcut ise bu cihazın tercih edilmesi esastır" ibaresi yer almaktadır. Bu kapsamda yerli HSM cihazlarının tercih edilmesi önerilmektedir. Kurumunuz bünyesinde yerli olmayan HSM cihazı bulunuyorsa ya da yerli HSM cihazının temininde sorun yaşanıyorsa standartları karşılayan farklı marka/model HSM cihazları da tercih edilebilir.

"Uzaktan" seçiliyse aşağıdaki bilgileri doldurunuz

Kurum Uzak Erişim Bilgileri

VPN Erişimi için Kullanılacak Uygulama:	
VPN Bağlantısı Yapılacak IP Adresi:	
Bağlantı Yapılacak Uzak Masaüstü Uygulaması:	

** TÜBİTAK BİLGEM Kamu Sertifikasyon Merkezi (Kamu SM) HSM cihazına anahtar ve sertifika yükleme süreçleri; başvuru sonrası işlemlerin güvenle ve en kısa sürede tamamlanması için tasarlanmıştır. Kamu SM tarafından uzaktan yükleme seçeneğinin tercih edilmesi önerilmektedir. Zorunlu hallerde uygulanacak yerinde yükleme süreci için ekstra ücretlendirme yapılmaktadır. Yerinde yüklemenin zorunlu olduğu durumlar için kurumdan sebep belirtmesi talep edilmektedir.*

Uyarı: Kamu SM dosya sunucudan erişilen elektronik kopyalar güncel ve kontrollü olup, diğer baskılar kontrolsüz kopyadır.

HSM CİHAZINA ANAHTAR VE SERTİFİKA YÜKLEME BİLGİ FORMU VE TAAHHÜTNAMESİ

Amaç

İşbu form ve taahhütname, 2017/21 Sayılı Başbakanlık Genelgesi ve Bilgi Teknolojileri ve İletişim Kurulu tarafından yayımlanan 2019/DK-BTD/160 Sayılı Kurumsal Şifreleme ve Elektronik Mühür Sertifikalarına İlişkin Usul ve Esaslar'a göre TÜBİTAK BİLGEM Kamu Sertifikasyon Merkezinden kendi bünyesinde bulunan HSM cihazına anahtar oluşturma, anahtar yükleme ve sertifika yükleme talebi yapan tüzel kişiliğin (bundan sonra Kurum olarak anılacaktır) ilgili süreçlerin her aşamasında Kurum ve görevlendirilen HSM Cihaz Sorumlusu tarafından uyulması gereken usul ve esaslarını içermektedir.

Tanımlar

EAL (Evaluation Assurance Level): Değerlendirme Garanti Seviyesi.

Elektronik Mühür Sertifikası: Kamu kurum ve kuruluşları arasında elektronik ortamdaki belge paylaşımında yazışma yapan tarafların kurumsal kimliklerini güvenli bir şekilde tanımlamak ve doğrulamak amacıyla kullanılan elektronik sertifika.

FIPS (Federal Information Processing Standard): Federal Bilgi İşleme Standardı.

HSM (Hardware Security Module): Sertifikanın kriptografik anahtarlarının içinde bulunduğu harici aygıt; donanımsal güvenlik modülü.

Kamu SM: Kamu SM: TÜBİTAK BİLGEM bünyesinde bulunan Kamu Sertifikasyon Merkezi'ni (İşbu form ve taahhütname kapsamındaki hizmetler TÜBİTAK BİLGEM bünyesinde yer alan Kamu SM tarafından yürütülür).

Kurumsal Şifreleme Sertifikası: Elektronik ortamdaki belge paylaşımında şifreleme yapmak amacıyla kullanılan açık anahtarı içeren elektronik sertifika.

Kurum: TÜBİTAK BİLGEM Kamu Sertifikasyon Merkezinden Elektronik Mühür ve Şifreleme Sertifikası talep eden, DETSİS'te bilgileri bulunan ve Elektronik Mühür ve Şifreleme Sertifikası almaya yetkisi olan tüzel kişilik.

VPN (Virtual Private Network): Sanal Özel Ağ.

Açıklamalar

- Bu form ve taahhütname, elektronik mühür ve/veya kurumsal şifreleme sertifikasyon sürecinde Kurum tarafından temin edilen ve yukarıda bilgileri verilen HSM cihazında (Bundan sonra HSM cihazı olarak anılacaktır) anahtar çifti oluşturma, oluşturulan sertifika ve anahtar çiftini HSM cihazına yükleme talebinin yazılı olarak beyan edilmesi ve Kurum tarafından onaylanan bu talebin Kamu SM'ye iletilmesi amacıyla hazırlanmıştır.
- Kurum HSM Cihaz Sorumlusu, resmi olarak görevlendirilen işbu form ve taahhütnamede bilgileri yer alan; Kamu SM ile Kurum arasında HSM cihazına anahtar çifti ve sertifika yükleme ile ilgili süreci yürütecek kişidir.
- İşbu form ve taahhütname ile Kurum, sertifika işlemlerinin gerçekleştirileceği, yukarıda bilgileri verilen HSM cihazının Kurum bünyesinde var olduğunu ve kullanıma hazır durumda olduğunu taahhüt eder.
- Kurum HSM cihazının en az FIPS 140-2 Seviye 3 veya EAL 4+ sertifikasına veya bunlara eşdeğer güvenlik sertifikalarına sahip olması ve güvenlik mekanizmalarının açık olması gerekmektedir. Bunun için gerekli kontroller Kurum ve Kamu SM personeli tarafından sağlanacaktır.
- HSM cihazı, Kurum içerisinde güvenli bir ortamda konumlandırılmalı ve sadece yetkili personeller tarafından erişilebilmelidir. Kurum bunun için gerekli önlemlerin alınacağını taahhüt eder.
- HSM cihazının bulunduğu alan kamera ile izlenmeli ve kayıt altına alınmalıdır. Kurum bunun için gerekli kontrolleri yapacağını taahhüt eder.
- HSM cihazına erişimler sınırlandırılmalı ve bilgi güvenliği en az yetki prosedürüne göre belirlenmelidir. Kurum bunun için gerekli önlemleri alacağını taahhüt eder.
- HSM ile sunucular arasında yapılan erişimlere ait loglar en az 2 yıl süreyle saklanmalıdır. Kurum bunun için gerekli kontrolleri yapacağını taahhüt eder.
- Herhangi bir servis kesintisi yaşanmaması için yedekli HSM kullanımı Kamu SM tarafından tavsiye edilmektedir. Sistem yedekli hale getirilmediği takdirde oluşabilecek servis kesintileri ve kesinti süresinden Kurum sorumludur.
- İşbu form ve taahhütnameye onay veren kişiler, 6698 Sayılı Kişisel Verilerin Korunması Kanunu gereğince, kişisel verilerin işlenmesine ilişkin Kamu SM Web Sayfasında yer alan KVKK Aydınlatma Metni'ni okuduğunu beyan eder.
- Yüklenecek tüm sertifikalar için HSM üzerinde ayrı ayrı slotlar oluşturulmalıdır. Bu slotların güvenliği için HSM tarafından desteklenen en yüksek koruma yöntemleri kullanılmalıdır.
- HSM cihazı yerli ve milli değilse Kurum üretilecek anahtar çiftinin Kurum gözetimi altında HSM cihazı dışında güvenli yöntemlerle oluşturulup cihaza yüklenmesini kabul eder.

Uyarı: Kamu SM dosya sunucudan erişilen elektronik kopyalar güncel ve kontrollü olup, diğer baskılar kontrolsüz kopyadır.

HSM CİHAZINA ANAHTAR VE SERTİFİKA YÜKLEME BİLGİ FORMU VE TAAHHÜTNAMESİ

Açıklamalar

- HSM cihazına anahtar yüklemede Kurum'a Kamu SM tarafından "yerinde" ve "uzaktan" olmak üzere iki seçenek sunulmuştur:
    - "Yerinde" yükleme, Kurum tarafından belirtilen zorunlu hallerde Kamu SM personelinin Kurum yerleşkesine gidip HSM cihazına anahtar üretimi ve sertifika yükleme işlemlerini yerinde gerçekleştirdiği süreçlerdir.
    - "Uzaktan" yükleme, Kamu SM ve Kurum arasında yapılan güvenli uzak bağlantı sonrası Kamu SM personelinin HSM cihazına anahtar üretimi ve sertifika yükleme işlemlerini uzaktan gerçekleştirdiği süreçlerdir.
- Kurum, yükleme işlemleri öncesinde Kamu SM'ye HSM cihazının anahtar yüklemeye uygun ve hazır olduğunu gösteren delil (ekran alıntısı içeren e-posta) göndermelidir.
- Kurum, işlem tarihi öncesi HSM cihazı ile doğrudan iletişim halinde, HSM cihazına istemci olacak ve işletim sistemine sahip, anahtar yönetim yazılımı yüklemeye uygun, çalışır bir bilgisayar temin etmelidir.
- Bağlanılacak bilgisayarda Java 8 veya üstü sürümün kurulu olması gerekmektedir.
- Bağlanılacak istemci bilgisayarın güncellemelerinin yapılmış olduğunu ve güncel imza veri tabanlarına sahip antivirüs yazılımının yüklü olduğunu Kurum taahhüt eder.
- HSM cihazına anahtar üretimi ve sertifika yükleme işlemi öncesi Kamu SM personeli HSM cihazının cihaz ekranına, komut satırına, istemci uygulamasına erişerek HSM Cihazına Anahtar ve Sertifika Yükleme Bilgi Formu'nda verilen bilgilerin doğruluğunu ve geçerliliğini, HSM cihazının yukarıda yer alan Bullet 4'te belirtilen güvenlik şartlarına uygun olduğunu teyit eder.
- Uzaktan yükleme ile anahtar üretimi ve sertifika yüklenmesi yapılacağı durumlar için Kurum ile Kamu SM arasında VPN bağlantısı kurularak iletişim şifreli olarak gerçekleştirilecektir.
- VPN için gereken güvenli uygulama Kurum'un altyapısına uygun olarak Kurum tarafından belirlenecek ve sağlanacaktır.
- VPN ile bağlantı sağlanacak IP ve uygulama bilgisi Kurum tarafından başvuru esnasında Kamu SM personeline bildirilecektir. Sadece bildirilen IP adresine bağlantı gerçekleştirilecek olup farklı bir IP adresine bağlantı yapılmamalıdır. Bunun için gerekli kontroller Kurum tarafından sağlanmalıdır.
- VPN bağlantısı sonrasında HSM cihazına istemci olan bilgisayara uzak bağlantı yapılacaktır. Yapılacak uzak bağlantı uygulaması Kurum tarafından belirlenmelidir.
- İşlemi gerçekleştirecek Kamu SM personeli, bu form ve taahhütnamede yer alan herhangi bir maddeye uygunsuzluğun ya da HSM cihazına anahtar üretimi ve sertifika yükleme işleminde olumsuzluk yaratacak herhangi bir güvenlik ihlalinin tespiti halinde, gerekli azami şartlar sağlanana kadar işlemi durdurma yetkisine sahiptir.

Kurum Onayı

İşbu form ve taahhütname kapsamında bilgileri verilen kişinin kurumumuz adına "HSM Cihaz Sorumlusu" olarak yetkilendirilmiş olduğunu, yukarıda yazılı bilgilerin ve belirtilen HSM Cihaz bilgilerinin doğru olduğunu, doğru olmaması durumunda doğacak bütün zararlardan kurumumuzun sorumlu olduğunu, HSM cihazına anahtar ve sertifika yükleme işlemlerinin yukarıda belirtilen açıklamalara uygun olarak yapılacağını kabul, beyan ve taahhüt ederiz.

(●) İşbu form ve taahhütname EYP dosyası ile e-imzalı olarak gönderilecektir.

İşbu form ve taahhütname üst yazısı ile birlikte EYP 2.0 dosyası oluşturularak iletilebilir. EYP dosyası bu bölümde bilgileri yer alan Kurum Yetkilisi ve HSM Cihaz Sorumlusu tarafından elektronik olarak imzalandıktan sonra kurum elektronik mührü kullanılarak mühürlenmelidir. Oluşturulan EYP dosyası kurumsal e-posta adresi veya KEP üzerinden Kamu SM'ye iletilmelidir.

( ) İşbu form ve taahhütname ıslak imzalı gönderilecektir.

İşbu form ve taahhütname, bilgi@kamusm.gov.tr veya kurumsal_bilgi@kamusm.gov.tr adreslerinden birine e-posta ile iletilebilir. E-posta ile gönderim durumunda form ve taahhütnamenin ayrıca TÜBİTAK BİLGEM Gebze Yerleşkesi (İdari Bina) P.K. 74 41470, Gebze Kocaeli adresine posta yoluyla iletilmesi gerekmektedir.

Uyarı: Kamu SM dosya sunucudan erişilen elektronik kopyalar güncel ve kontrollü olup, diğer baskılar kontrolsüz kopyadır.