

İşbu doküman (bundan böyle "Taahhütname" olarak anılacaktır), Barış Mahallesi, Anibal Caddesi P.K.74, TÜBİTAK Gebze Yerleşkesi, 41470 Gebze, Kocaeli adresinde mukim Türkiye Bilimsel ve Teknolojik Araştırma Kurumu, Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (TÜBİTAK BİLGEM)'in SSL Sertifikasına yönelik olarak adresinde mukim firması/kurumuna (bundan böyle "Sertifika Sahibi" olarak anılacaktır) tanınan kullanım haklarını tanımlamaktadır.

İşbu Taahhütname, Sertifika Sahibine gönderilecek olan teklif mektubunun Sertifika Sahibi tarafından onaylandığını belirten yazısı ile birlikte imzalanarak TÜBİTAK BİLGEM'e gönderilecektir. Taahhütname, imzalandığı tarih itibarıyla yürürlüğe girmiş olacak ve Sertifika Sahibi işbu Taahhütnamenin tüm şart ve hükümlerinin tamamını okuduğunu, kabul ettiğini ve söz konusu bu şart ve hükümler ile yasal olarak bağlı olduğunu kabul etmiş olacaktır.

1 Tanımlar ve Kısaltmalar

- i. **SSL Sertifikası/Sertifika:** Sunucunun kimlik doğrulamasını sağlayan ve sunucu-istemci arasında akan verinin güvenliğini ve bütünlüğünü mümkün kılan sertifikadır.
- ii. **Sertifika Sahibi:** SSL Sertifikası başvurusunda bulunan ve talep ettiği alan adını kullanma yetkisine sahip tüzel kişidir.
- iii. **Alan Adı:** İnternette hizmet veren sunucuları tanımlamak için kullanılan ve kurumsal kimlik ya da marka ile özdeşleşmiş isimlerdir.
- iv. **Anahtar Çifti:** Özel anahtarı ve onunla ilişkili olan açık anahtarı ifade eder.
- v. **Özel Anahtar:** Anahtar Çiftinin sahibi tarafından gizli tutulan ve dijital imza oluşturmak ve/veya ilgili Açık Anahtarla şifrelenmiş elektronik kayıtların, dosyaların şifresini çözmek için kullanılan anahtardır.
- vi. **Açık Anahtar:** İlgili özel anahtarın sahibinin herkes ile paylaşabildiği, özel anahtarı ile oluşturduğu dijital imzaların doğrulanmasında ve/veya kendisine şifreli mesaj iletilmesinde kullanılan anahtar çiftinin gizli olmayan bileşenidir. Yalnızca ilişkili olduğu özel anahtar ile eşleşir.
- vii. **Kamu SM:** Kamu Sertifikasyon Merkezi, TÜBİTAK'a bağlı Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM) bünyesinde elektronik sertifika hizmeti sağlamak üzere oluşturulan birimdir.
- viii. **Sİ (Sertifika İlkeleri):** SSL Sertifikasının ve açık anahtar altyapısı mimarisinin güvenlik gereksinimlerini de sağlayacak şekilde oluşturulması/uygulanması adına gerekli kural setlerini içeren dokümandır.
- ix. **SUE (Sertifika Uygulama Esasları):** Güvenilir SSL Sertifikası ile ilgili düzenlemeleri tanımlamaktadır.



2 SSL Sertifika Sahibinin Yükümlülükleri

Sertifika Sahibine Sertifikanın devredilemez ve münhasır nitelikte kullanım hakkı sağlanmaktadır. Bu kapsamda Sertifika Sahibi;

- a. Sertifika başvurusu için bildirilen bilgilerinin doğruluğunu ve verilen bilgilerdeki yanlışlık veya hatalardan kaynaklı problemlerde tüm sorumluluğu üstleneceğini,
- b. Bilgilerin Kişisel Verilerin Korunması Kanunu kapsamında başvuru formu ile birlikte saklanmasına izin verdiğini,
- c. Bu Taahhütnameye istinaden aldığı/alacağı SSL Sertifikasını kullanma hak ve yükümlülüklerini bir başka kişi veya kuruma devretmeyeceğini,
- d. Sertifika başvurusunda, kurumunun resmi olarak sahip olduğunu belgeleyebildiği alan adı/alan adları dışında başka bir alan adı için Sertifika talebinde bulunmayacağını,
- e. Resmi olarak sahip olduğu kurum adı ve alan adlarının doğrulanabilmesi için aşağıdaki adımları ve doğrulama sürecinde yapılması gerekenleri tamamlayacağını;
 - Kamu SM, alan adı üzerinde kurumun kontrolünü test etmek amacıyla alan adında sunulan bir sayfada kurum tarafından sertifika imzalama isteğinde kullanılan bilgilerden oluşturulacak istek belirtecinin, alan adında .well-known/pki-validation/ dizini içerisinde "kamusmdv.txt" adlı dosyada yayımlanmasını talep eder.
 - Kamu SM tarafından yayımlanması istenen istek belirteci, kurum tarafından alan adının sertifikalandırılması için üretilen sertifika imzalama isteğinin (PKCS#10 CSR) SHA-256 özet değeri olarak belirlenmiştir.
 - Bu değerin yayımlanmasının ardından Kamu SM gerekli kontrolleri yapar ve alan adı sahipliği doğrulanır.
- f. Alınan SSL Sertifikasını yasal olarak suç teşkil edecek içerik bulunduran internet adresleri için kullanmayacağını,
- g. SSL Sertifikası başvurusunda kullanılacak özel anahtarın üretiminin başvuru sahibi tarafından yapılacağını üçüncü şahıslar tarafından oluşturulamayacağını veya üçüncü şahıslara teslim edilmeyeceğini, özel anahtarın korunması için gerekli önlemleri alacağını, özel anahtarın gizliliğini kaybetmesi durumunda sertifikanın iptali için Kamu SM'yi derhal bilgilendireceğini,
- h. Sertifika işlemlerini yapabilmesi için kullandığı parolaların gizliliğini ve güvenliğini sağlamak için gerekli önlemleri alacağını,



- i. Kamu SM, gerekli gördüğü durumlarda Sİ/SUE dokümanlarında deęişiklik hakkına sahiptir/yapabilir. SSL Sertifikasını Kamu SM Sİ ve SUE dokümanlarında belirtildięi şekilde kullanacağını,
 - j. Kurum, SSL Sertifikası hizmeti alımı sırasında verilmiş olan bilgilerde son bir sene içerisinde deęişiklik olmayacağını, SSL Sertifikası geçerlilik süresi boyunca her sene bir defaya mahsus Faaliyet Takip Formu ile Kamu SM'ye bildirimde bulunacağını,
 - k. Kurum, SSL Sertifikası hizmet alımı sırasında beyan edilmiş bilgilerin deęişmesi, yahut geçerliliğini yitirmesi durumunda kurum adına alınan SSL Sertifikası iptali için başvuruda bulunacağını,
 - l. Kurum kendine ait alan adının sahipliğini vekaleten devredebilir. Bu durumda başvuru belgelerine ek olarak, Kamu SM'nin yayımlamış olduęu "SSL Vekalet Formu" taraflarca imzalanarak Kamu SM'ye iletileceğini,
 - m. Verilen Sertifikadaki bilgilerin doğruluęunu kontrol etmek zorunda olduęunu,
 - n. Özel anahtar gizliliğinin kaybolması durumunda SSL Sertifika kullanımını derhal durduracağını,
- kabul ve taahhüt eder.

3 SSL Sertifikasının İptali

SSL Sertifikası iptal talebi, sadece Sertifika Sahibi tarafından yapılabilir. Kamu SM, Sertifika Sahibinin talebi üzerine SSL Sertifikasını iptal eder; ancak iptal durumunda Sertifika Sahibinin Sertifika bedelini ödeme yükümlülüęü devam eder. SSL Sertifikası aőağıda belirtilen hallerde, Kamu SM tarafından re'sen iptal edilir ve Sertifika Sahibine durum bildirilir:

- a. Sertifika Sahibinin SSL Sertifikasını, bu Taahhütname ve/veya Kamu SM Sİ ve SUE dokümanlarında belirtilen şartlara uygun olarak kullanmadığını tespit edilmesi.
- b. Kamu SM sisteminin, Kamu SM Sİ ve SUE dokümanlarında belirtildięi şekilde güvenliğini yitirmesi veya sertifika hizmetlerinin sonlandırılması.
- c. Kamu SM Sİ ve SUE dokümanlarında belirtilen, SSL Sertifikasının iptalini gerektiren dięer hallerin ortaya çıkması.

4 Taahhütname Süresi

SSL Sertifikasının geçerlilik süresi (en çok iki sene olacak şekilde), Cihaz Sertifikası Başvuru Formu'nda belirtilen geçerlilik sürelerinden birinin Sertifika Sahibi tarafından seçilmesi ile belirlenmektedir. Sertifika başlangıç ve bitiş tarihleri Sertifika içeriğinde belirtilecektir. Taahhütnamenin süresi SSL Sertifikasının geçerlilik süresi ile sınırlıdır. Taahhütname imzalandığı tarih itibarıyla yürürlüğe girmiş olacak ve Sertifika Sahibi işbu Taahhütnamenin tüm şart ve hükümlerinin tamamını okuduğunu, kabul ettiğini ve söz konusu bu şart ve hükümler ile yasal olarak baęlı olduęunu kabul etmiş olacaktır.