

1 Tanımlar ve Kısaltmalar

- i. **SSL Sertifikası/Sertifika:** Sunucunun kimlik doğrulamasını sağlayan ve sunucu-istemci arasındaki 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 birim.
- 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 Kamu SM aşağıdaki yükümlülükleri yerine getirmeyi taahhüt eder;

1. Sertifikalarla ilgili tüm işlemlerini Kamu SM Sİ ve SUE dokümanlarında belirtilen şartlar altında yerine getirir.
2. Kamu SM Sİ, SUE ve/veya ilgili belgelerin güncel sürümlerini kesintisiz olarak bilgi deposunda yayımlar.
3. Kök ve alt kök sertifikalarını üçüncü tarafların erişimine açık bilgi depolarında kesintisiz olarak yayımlar.
4. Sertifika başvurusunda bulunan kurum ve kişi bilgilerinin doğrulanmasını Kamu SM Sİ ve SUE dokümanlarında tanımlandığı şekilde yapar.
5. Kamu SM Sertifika Şeffaflığı (Certificate Transparency) ile uyumlu SSL sertifikaları üretmektedir. Bu sebeple sertifikaları herkese açık log sunucularına kaydetmek zorundadır.
6. Sertifika başvurusu sırasında Sertifika Sahibine ait kağıt üzerinde veya elektronik ortamdan verilen kişisel bilgileri sertifika hizmeti dışında başka herhangi bir amaç için kullanmaz, tutulan bilgilerin Kişisel Verilerin Korunması Kanunu çerçevesinde gizliliğinin korunması için gerekli önlemleri alır, bu bilgileri üçüncü kişilere mahkeme kararı veya Sertifika Sahibinin yazılı rızası olmaksızın vermez.



7. SSL Sertifikası iptal talebi, sadece Sertifika Sahibi tarafından yapılabilir. Sertifika aşağıda belirtilen hallerde, Kamu SM tarafından re'sen iptal edilir.
 - Sertifika Sahibinin SSL Sertifikasını, bu Taahhütname ve/veya Kamu SM Sİ ve SUE dokümanlarında belirtilen şartlara uygun olarak kullanmadığının tespit edilmesi.
 - Kamu SM sisteminin, Kamu SM Sİ ve SUE dokümanlarında belirtildiği şekilde güvenliğini yitirmesi veya sertifika hizmetlerinin sonlandırılması.
 - Kamu SM Sİ ve SUE dokümanlarında belirtilen, sertifikanın iptalini gerektiren diğer hallerin ortaya çıkması.
8. İptal edilen sertifikalar için sertifika iptal listesi yayımlar.
9. Kamu SM, Sertifika Sahibinin özel anahtar ve sertifika kullanımında, söz konusu şartları yerine getirmemesinden sorumlu değildir.
10. Kamu SM SSL Kök sertifikası Internet Explorer ve Mozilla Firefox'un güncel sürümlerinde; ayrıca Microsoft Windows tabanlı işletim sistemlerinde çalışması durumunda Yandex, Chrome ve Opera web tarayıcılarının güvenilir sertifikalar listesinde yer almaktadır.
11. Android işletim sisteminde; Kamu SM SSL Kök sertifikası, Mozilla SSL güvenilir kök yazılımı olan NSS'de yer aldığından Firefox tarayıcısı tarafından desteklenmektedir.
12. Kamu SM SSL Kök sertifikası, Android işletim sisteminin 8.1 öncesi sürümlerinde ve iOS işletim sisteminin güvenilir kökler listesinde ekli değildir.
13. Kamu SM tarafından, başvuru sırasında verilen tüm bilgi ve belgeler (başvuru ve taahhütname),
 - Sertifika üretimi ve iptal başvuruları sırasında elektronik veya kağıt ortamda alınan formlar,
 - Sertifika işlemleriyle ilgili yapılan önemli yazışmalar,
 - Üretilen tüm sertifikalar,
 - Geçerlilik süresi dolan tüm Kamu SM kök ve alt kök sertifikaları,
 - Yayımlanan tüm sertifika iptal durum kayıtları,
 - Sertifika İlkeleri dokümanı,
 - Sertifika Uygulama Esasları dokümanı,
 - Sertifika yönetim prosedürleri,
 - Sertifika Sahibi Taahhütnameleriarşivlenir ve arşivlenen bu belgeler 7 (yedi) yıl boyunca saklanır.