KAMU SM GÜVENLİ SUNUCU SERTİFİKA (SSL) HİZMETİ YÜKÜMLÜLÜKLERİ

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. SSL sertifika hizmetleri konusunda, "ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers Issuing Certificates; Part 1: General Requirements" standardının güncel sürümü ile https://www.cabforum.org adresinde yayımlanan "CA/Browser Forum Baseline Requirements (BR) for the Issuance and Management of Publicly-Trusted Certificates" dokümanının güncel sürümüne uyar.
3. Kamu SM Sİ, SUE ve/veya ilgili belgelerin güncel sürümlerini kesintisiz olarak bilgi deposunda yayımlar.
4. Kök ve alt kök sertifikalarını üçüncü tarafların erişimine açık bilgi depolarında kesintisiz olarak yayımlar.
5. Sertifika başvurusunda bulunan kurum ve kişi bilgilerinin doğrulanmasını Kamu SM Sİ ve SUE dokümanlarında tanımlandığı şekilde yapar.
6. Kamu SM Sertifika Şeffaflığı (Certificate Transparency) ile uyumlu SSL sertifikaları üretmektedir. Bu sebeple sertifikaları herkese açık log sunucularına kaydetmek zorundadır.
7. 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.
8. 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.

9. İptal edilen sertifikalar için sertifika iptal listesi yayımlar.
10. Kamu SM, Sertifika Sahibinin özel anahtar ve sertifika kullanımında, söz konusu şartları yerine getirmemesinden sorumlu değildir.
11. Kamu SM SSL Kök sertifikası; Windows, Mac OS 10.14.2+, IOS 12.1.1+, Linux Ubuntu, Pardus (Debian 17.2+) ve Android 8.1+ işletim sistemlerinde çalışan,
    - Mozilla Firefox (v56.0+)
    - Google Chrome ,
    - Internet Explorer,
    - Microsoft Edge ,
    - Opera,
    - Yandex

    tarayıcıları ile uyumlu olarak çalışmaktadır.
12. Kamu SM tarafından,

    - Sertifika sahibi tarafından başvuru sırasında verilen tüm bilgi ve belgeler,
    - 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,
    - Sİ dokümanı,
    - SUE dokümanı,
    - Sertifika yönetim prosedürleri,
    - Sertifika sahibi taahhütnameleri ve
    - Sertifikasyon süreçlerinde kullanılan sistemlerin NTP (ağ zaman protokolü) senkronizasyon logları

    arşivlenir ve arşivlenen bu belgeler 7 (yedi) yıl boyunca saklanır.