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:** Kurum ve markalara ait internette hizmet veren sunucuları tanımlamak için IP adresleri yerine kullanılan isimleri ifade eder.
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/SUE (Sertifika İlkeleri ve Sertifika Uygulama Esasları):** SSL sertifikasının ve açık anahtar altyapısı mimarisinin, güvenlik gereksinimlerini sağlayacak şekilde oluşturulması/uygulanması adına gerekli kural setlerini içeren ve bu kural setlerinin nasıl uygulanacağını detaylı olarak anlatan dokümandır.
ix. **SİL:** Sertifika İptal Listesi.
x. **OCSP (Online Certificate Status Protocol):** Çevrimiçi Sertifika Durum Protokolü.

2 Kamu SM Yükümlülükleri

1. Sertifikalarla ilgili tüm işlemlerini Kamu SM SSL Sİ/SUE dokümanında belirtilen şartlar altında yerine getirir.
2. Kamu SM, 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 TLS Certificates*" dokümanının güncel sürümüne uyar.
3. Kamu SM Sİ/SUE ve/veya ilgili belgelerin güncel sürümlerini kesintisiz olarak herkesin erişimine açık bilgi deposundan yayımlar.
4. Kamu SM Sİ/SUE dokümanlarının eski sürümlerini web sitesinde yayımlar.
5. Kök ve alt kök sertifikalarını üçüncü tarafların erişimine açık bilgi depolarında kesintisiz olarak yayımlar.
6. Sertifika başvurusunda bulunan kurum ve kişi bilgilerinin doğrulanmasını Kamu SM Sİ/SUE dokümanlarında tanımlandığı şekilde yapar.
7. Sertifika başvurusunda bulunulan alan adlarına sahipliğin doğrulanmasını Sİ/SUE dokümanında tanımlandığı şekilde yapar.
8. Kamu SM Sertifika Şeffaflığı (Certificate Transparency) ile uyumlu SSL sertifikaları üretmektedir. Bu sebeple sertifikaları herkese açık log sunucularına kaydeder.

9. 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 6698 Sayılı Kişisel Verilerin Korunması Kanunu çerçevesinde gizliliğinin korunması için gerekli önlemleri alır, bu bilgileri üçüncü kişilere mahkeme kararı veya Sertifika Sahibinin yazılı rızası olmaksızın vermez.
10. Sertifika iptal başvurularını Sİ/SUE'de belirtilen prosedürler çerçevesinde kabul eder ve Sİ/SUE'de belirtilen herhangi bir nedenin ortaya çıkması durumunda sertifikayı iptal eder.
11. İptal edilmiş sertifika bilgilerini SİL'de yayımlar ve OCSP aracılığıyla duyurur.
12. Kamu SM, Sertifika Sahibinin özel anahtar ve sertifika kullanımında, söz konusu şartları yerine getirmemesinden sorumlu değildir.
13. Üretilen SSL sertifikaları iOS, MAC OS, Windows ve Linux işletim sistemlerine ek olarak, Android işletim sistemi üzerinde çalışan Internet Explorer, Microsoft Edge, Google Chrome, Mozilla Firefox, Yandex, Opera, Safari ve 360 Browser tarayıcıları ile uyumlu şekilde çalışmaktadır.
14. Kamu SM tarafından,

- Sertifika sahibi kurum tarafından, başvuru sırasında verilen tüm bilgi ve belgeler ile bunların doğrulandığına ilişkin kayıtlar,
- Sertifika üretimi ve iptal başvuruları sırasında elektronik veya kağıt ortamda alınan formlar,
- Üretilen tüm sertifikalar,
- Geçerlilik süresi dolan tüm Kamu SM kök ve alt kök sertifikaları,
- Yayımlanan tüm sertifika iptal durum kayıtları,
- Sİ/SUE dokümanı,
- Sertifika yönetim prosedürleri,
- Sertifika sahibi taahhütnameleri ve
- Sertifikasyon süreçlerinde kullanılan sistemlerin NTP (ağ zaman protokolü) senkronizasyon logları

arşivlenir ve kayıt oluşturma zamanından itibaren en az 2 (iki) yıl süreyle veya yasalar ve/veya ETSI standartları uyarınca saklanmaları gereken süre boyunca (hangisi daha uzunsa) saklanır.