TASNİF DIŞI

TÜBİTAK BİLGEM
KAMU SERTİFİKASYON MERKEZİ

KAMU SM SSL SERTİFİKA İLKELERİ

Revizyon No
v.1.0.1
Revizyon Tarihi
16.10.2019

TASNİF DIŞI

Yasal Uyarı

Kamu Sertifikasyon Merkezi
TÜBİTAK Yerleşkesi, P.K. 74
Gebze 41470 Kocaeli, TÜRKİYE
http://www.kamusm.gov.tr

İÇİNDEKİLER

1. GİRİŞ

Kamu Sertifikasyon Merkezi (Kamu SM), Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) tarafından; 15 Ocak 2004 tarihli ve 5070 sayılı, Elektronik İmza Kanunu gereklilikleri yerine getirilerek ve uluslararası standartlara uygun olarak oluşturulmuş Elektronik Sertifika Hizmet Sağlayıcısı'dır (ESHS). Kamu SM devlete ait olarak hizmet veren bir ESHS'dir.

Sertifika İlkeleri (Sİ) olarak isimlendirilen bu doküman, Kamu SM'nin, Türkiye Cumhuriyeti Devleti'ne bağlı kamu kurum ve kuruluşlara OV SSL (Organization Validated SSL) sağlayıcılığı konusundaki faaliyetleri sırasında uyulması gereken kuralları ve çalışma ilkelerini anlatmak amacıyla, "IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" rehber kitapçığına uygun olarak hazırlanmıştır.

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,
- ETSI EN 319 411-1 standardında referans verilen ve 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.

Bu doküman ile belirtilen standartlar arasında herhangi bir uyuşmazlık olması durumunda ilgili dokümanlardaki gereklilikler geçerli olacaktır.

Bu doküman, sertifika başvurularının alınması, sertifika üretimi ve yönetimi, sertifika yenileme ve sertifika iptal işlemleriyle ilgili hizmetlerin, idari, teknik ve yasal gerekliliklere uygun olarak yürütülmesiyle ilgili esasları ortaya koyar; Kamu SM'nin, sertifika sahibinin ve üçüncü kişilerin uygulama sorumluluklarını belirler. Bu kapsamda oluşturulan sertifikalar 5070 sayılı Elektronik İmza Kanunu'nda sözü geçen nitelikli elektronik sertifika kapsamında değerlendirilmez.

1.1. GENEL BAKIŞ

Bu doküman, sistem bileşenlerinin rollerini, sorumluluklarını ve ilişkilerini; kayıt ve sertifika yönetim işlemlerini tanımlar.

Kayıt işlemleri, sertifika verilecek kurumların başvurularını, kimlik bilgilerini ve ilgili resmi belgeleri toplamak, doğrulamak, onaylamak; sertifika üretme ve iptal isteklerini almak, değerlendirmek, onaylanan sertifika başvuru ve iptal istekleri doğrultusunda gerekli işlemleri başlatmak gibi işlerden oluşur.

Sertifika yönetimi, sertifika sahipleri için sertifika üretmek, sertifikaları yayımlamak, iptal etmek, sertifika iptal bilgisini yayımlamak, sertifika işlemleri ile ilgili kurumları başvuru ve sertifikanın durumu hakkında bilgilendirmek, gerekli kayıtları tutmak gibi işlerden oluşur.

Bu doküman, "İnternet Açık Anahtar Altyapısı Sertifika İlkeleri ve Sertifika Uygulama Esasları Çerçeve Planı" [IETF - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 3647)] referans alınarak hazırlanmıştır.

1.2. DOKÜMAN ADI VE TANIMI

Doküman Adı: Kamu SM SSL Sertifika İlkeleri

Doküman Sürüm Numarası: 1.0.1

Tarih	Değişiklikler	Versiyon
07.08.2018	İlk doküman	1.0.0
16.10.2019	Yıllık doküman revizyonu kapsamında düzenlemeler yapıldı.	1.0.1

Yayın Tarihi: 16.10.2019

Nesne Tanımlama Numarası: 2.16.792.1.2.1.1.5.7.1.3

Bu doküman, Kamu SM'nin OV SSL sertifikası hizmeti verirken uyguladığı esasları tanımlayan Sİ dokümanıdır ve sunuculara yönelik verilen OV SSL sertifikalarını kapsar. OV SSL sertifikaları, ETSI EN 319 411-1 standardında tanımlanan "Organizational Validation Certificate Policy – Kurumsal Doğrulamalı Sertifika İlkeleri" uyarınca üretilir ve yönetilir.

Bu doküman http://depo.kamusm.gov.tr/ilke adresinde kamuya açık olarak yayımlanmaktadır.

1.3. SİSTEM BİLEŞENLERİ

Bu doküman kapsamında tanımlanan sistem bileşenleri, Kamu SM'nin ESHS faaliyetlerinde rol alan ve sertifika hizmetleriyle ilgili hak ve yükümlülükleri bulunan taraflardır. Bu taraflar, ESHS, kayıt birimleri, sertifika sahipleri ve üçüncü kişiler olarak tanımlanır. Kamu SM ESHS faaliyetlerinin tümü Kamu SM personeli tarafından yürütülmektedir.

1.3.1. Elektronik Sertifika Hizmet Sağlayıcısı

Kamu SM, ESHS olarak OV SSL sertifika hizmeti vermektedir. Kamu SM OV SSL hiyerarşisini oluşturan bileşenler: kök, kök tarafından yayımlanmış alt kök ve OCSP sertifikası; alt kök tarafından yayımlanmış OCSP sertifikası ve SSL son kullanıcı sertifikalarıdır. Alt kök makamı aşağıdaki hizmetleri yerine getirir:

- Sertifikaların üretilmesi, imzalanması ve ilgili kurumlara ulaştırılması
- Sertifikaların iptal edilmesi
- Sertifika durum bilgilerinin Sertifika İptal Listesi (SİL) şeklinde veya diğer yöntemlerle yayımlanması

1.3.2. Kayıt Birimleri

Tüm kayıt işlemleri doğrudan Kamu SM personeli tarafından yürütülmektedir. Kayıt Birimleri, Kamu SM'nin sertifika ve iptal başvurusu gibi doğrudan son kullanıcılara yönelik hizmetlerini yürüten birimidir. Bu birim, ilk müşteri kayıtlarını oluşturur, gerekli kimlik tanımlama ve doğrulama süreçlerini yürütür, ilgili sertifika taleplerini sertifika üretim birimine yönlendirir.

1.3.3. Sertifika Sahipleri

Kamu SM tarafından üretilen sertifikalarını sertifika ilkeleri ve uygulama esaslarına uygun olarak kullanmakla yükümlü olan kamu kurum ve kuruluşlarıdır.

1.3.4. Üçüncü Kişiler

Kamu SM tarafından oluşturulan sertifikaları doğrulamak suretiyle kabul eden ve bu sertifikalarla işlem yapan taraflardır.

1.4. SERTİFİKA KULLANIMI

1.4.1. Uygun Sertifika Kullanımı

SSL sertifikası, sunucu ile istemci arasında kimlik doğrulamanın gerçekleştirilmesi ve iletişimin şifreli olarak sağlanması amacıyla kullanılır. SSL sertifikası, sadece sertifikada bulunan alan adına hizmet veren sunucular için kullanılır. Tüm sertifikaların kullanım hakları sadece sertifika sahiplerine aittir.

1.4.2. Sertifika Kullanım Sınırları

Kamu SM tarafından oluşturulan SSL sertifikaları Bölüm 1.4.1'de belirtilen amaçlar dışında kullanılamaz.

1.5. İLKE VE UYGULAMA ESASLARININ YÖNETİMİ

1.5.1. Doküman Yönetimi

Bu doküman Kamu SM tarafından yazılmıştır. Kamu SM, gerekli gördüğü durumlarda dokümanda değişiklik yapabilir.

1.5.2. İletişim Bilgileri

Bu dokümanın uygulanması ve ilgili yönetim ilkeleri hakkındaki sorular Kamu SM'nin aşağıdaki erişim noktalarına yönlendirilebilir:

Adres : Kamu Sertifikasyon Merkezi, TÜBİTAK Yerleşkesi P.K. 74, 41470 Gebze-Kocaeli
Tel : 444 5 576
Faks : (262) 648 18 00
E-Posta : bilgi@kamusm.gov.tr
Web : http://www.kamusm.gov.tr

Kamu SM, bu dokümanı herkesin erişimine açık bulunan http://depo.kamusm.gov.tr/ilke internet adresinden yayımlar.

1.5.3. Sertifika Uygulama Esaslarının İlkelere Uygunluğunu Belirleyen Kişi

SUE dokümanın sertifika ilkelerine uygunluğu Kamu SM yönetimi ve yönetim tarafından yetki verilen kişiler tarafından belirlenir.

1.5.4. Sertifika Uygulama Esasları Onay Prosedürleri

Si/SUE dokümanlarının yayımlanma onayı, Kamu SM yönetimi ve yönetim tarafından yetki verilen kişiler tarafından gerçekleştirilen incelemelerden sonra verilir.

1.6. TANIMLAR VE KISALTMALAR

1.6.1. Tanımlar

Anahtar çifti: Elektronik imza oluşturmak ve doğrulamak ya da bir veriyi şifrelemek ve şifresini çözmek amacıyla kullanılan özel anahtar ve ilgili açık anahtar.

Bilgi deposu: Sertifikaların, sertifika iptal durum kayıtlarının ve sertifika işlemleri ile ilgili diğer bilgilerin yayımlandığı web sunucular gibi veri saklama ortamları.

Çevrimiçi sertifika durum protokolü: Sertifika iptal listesine alternatif olarak üçüncü kişilerin sertifika geçerlilik kontrol talebini yapıp, sertifikanın iptal durumunu kesintisiz olarak öğrenmelerine imkân tanıyan standart iletişim kuralı.

İptal durum kaydı: Kullanım süresi dolmamış sertifikaların iptal bilgisinin yer aldığı, iptal zamanının tam olarak tespit edilmesine imkân veren ve üçüncü kişilerin hızlı ve güvenli bir biçimde ulaşabileceği kayıt.

Kamu Sertifikasyon Merkezi: Türkiye Bilimsel ve Teknolojik Araştırma Kurumu bünyesinde, elektronik sertifika hizmeti sağlamak üzere oluşturulan birim.

Nesne tanımlama numarası (OID): Herhangi bir nesneyi eşsiz olarak tanımlayan, uluslararası standart belirleyen bir kuruluştan alınan numara.

OV SSL: ETSI EN 319 411-1 standardında tanımlanan "Organization Validation Certificate Policy – Kurumsal Doğrulamalı Sertifika İlkeleri" uyarınca üretilen ve idame edilen SSL sertifikası.

Sertifika İptal Listesi (SİL): İptal edilmiş sertifikaların kamuya duyurulması amacıyla ESHS tarafından oluşturulan, imzalanan ve yayımlanan elektronik dosyadır.

Sertifika sahibi: Kamu SM'den sertifika alan kamu kurum ve kuruluşu.

Kök makamı: Kamu Sertifikasyon Merkezi içinde oluşturulmuş, en yetkili imza derecesi verilmiş ve sertifikasını kendisi imzalamış olan sertifika makamı.

Kök sertifikası: Kök makamına ait sertifika.

Alt kök makamı: Kamu Sertifikasyon Merkezi içinde oluşturulmuş, sertifikası kök makam tarafından imzalanmış ve SSL sertifikalarını oluşturup imzalayan makam.

Alt kök sertifikası: Alt kök makamına ait sertifika.

Son kullanıcılar: Sertifika sahipleri ve sertifikaları kullanan üçüncü kişiler.

Üçüncü kişiler: Sertifikalara güvenerek işlem yapan gerçek veya tüzel kişiler.

Yetkilendirilmiş üçüncü kuruluş: Kamu SM tarafından sertifika yönetim sürecindeki gereksinimleri yerine getirmek üzere yetkilendirilmiş gerçek veya tüzel kişiler.

1.6.2. Kısaltmalar

BR (Baseline Requirements): CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates – CA/Browser Forum Temel Gereklilikler Dokümanı

CA (Certificate Authority): Sertifika Makamı

CEN (Comité Européen de Normalisation): Avrupa Standardizasyon Komitesi

CWA (CEN Workshop Agreement): CEN Çalıştay Kararı

EAL (Evaluation Assurance Level): Değerlendirme Garanti Düzeyi

ESHS: Elektronik Sertifika Hizmet Sağlayıcısı

ETSI (European Telecommunications Standards Institute): Avrupa Telekomünikasyon Standartları Enstitüsü

ETSI EN (ETSI European Standard): ETSI Avrupa Standardı

IETF RFC (Internet Engineering Task Force Request for Comments): İnternet Mühendisliği Görev Grubu Yorum Talebi

ISO/IEC (International Organization for Standardization / International Electrotechnical Commitee): Uluslararası Standardizasyon Teşkilatı / Uluslararası Elektroteknik Komitesi

Kamu SM: Kamu Sertifikasyon Merkezi

OCSP (Online Certificate Status Protocol): Çevrimiçi Sertifika Durum Protokolü

PKI (Public Key Infrastructure): Açık Anahtar Altyapısı

Sİ: Sertifika İlkeleri

SİL: Sertifika İptal Listesi

SSL (Secure Sockets Layer): Güvenli Soket Katmanı

SUE: Sertifika Uygulama Esasları

2. YAYIN VE BİLGİ DEPOSU SORUMLULUKLARI

Bilgi deposu, Kamu SM'nin kök ve alt kök sertifikalarını, iptal durum kayıtlarını, Sİ ve SUE gibi dokümanlarını herkesin ulaşabileceği şekilde kesintisiz, güvenli ve ücretsiz olarak yayımladığı ortamdır. Depodan yayımlanan bazı kritik dosyalar gerektiğinde güncellenir. Bu güncellemeler, güncellenen dosya üzerinde tutulan sürüm numarası ve güncelleme tarihi ile belirtilir.

2.1. BİLGİ DEPOSU

Kamu SM'nin bilgi deposuna internet üzerinden erişilir. Kamu SM, bilgi deposunu işletmek için üçüncü bir güvenilir kişi ya da kuruluş kullanmaz.

2.2. SERTİFİKA HİZMETİ İLE İLGİLİ BİLGİLERİN YAYIMLANMASI

Kamu SM'nin, herkesin erişimine açacağı bilgi deposunda sistemin iç işleyişi ile ilgili olanlar hariç olmak üzere aşağıdaki bilgiler bulunur:

- Kamu SM'ye ait kök ve alt kök sertifikaları,
- Kamu SM'ye ait sertifikaların özet değerleri ile özet değerlerinin hesaplanmasında kullanılan özetleme algoritmaları,
- Kamu SM tarafından kullanılan OID listesi,
- Kamu SM Sİ ve SUE dokümanları,
- Taahhütnameler, Formlar, Sertifika Sözleşmeleri, Sertifika Yönetim Prosedürleri,
- Güncel sertifika iptal durum kayıtları

Kamu SM'nin bilgi deposuna http://www.kamusm.gov.tr ve http://depo.kamusm.gov.tr adresleri üzerinden erişilir.

2.3. YAYIM ZAMANI VE SIKLIĞI

Sİ/SUE dokümanları içeriğinin değişmesi üzerine Taahhütnameler, Formlar, Sertifika Sözleşmeleri, Sertifika Yönetim Prosedürleri güncellenir. Güncellenen dokümanlar, güncelleme yapılmasına müteakip derhal yayımlanır.

Kamu SM'ye ait sertifikalar güncelleme yapılmasına müteakip derhal yayımlanır.

SİL'lerin yayımlanma sıklığı ve OCSP kayıtlarının güncellenme sıklığı SUE dokümanı Bölüm 4.9.7 ve 4.9.9'da belirtilmektedir.

Kamu SM Sertifika Uygulama Esasları dokümanları yıllık olarak düzenli bir şekilde güncellenmektedir.

2.4. BİLGİ DEPOSUNA ERİŞİM KONTROLLERİ

Kamu SM bilgi deposuna bilgi edinme amaçlı erişim herkese açıktır. Bilgi deposunun güncellenmesi, yetkisi olan Kamu SM personeli tarafından yapılmaktadır.

Kamu SM, bilgi deposu ile ilgili olarak aşağıdaki yükümlülükleri yerine getirir:

- Bilgi deposunda tutulan bilgilerin izinsiz silinmeye ve değiştirilmeye karşı bütünlüğünü korumak,
- Bilgi deposunda tutulan bilgilerin doğruluğunu ve güncelliğini sağlamak,
- Bilgi deposunu sürekli olarak erişime açık tutmak,
- Bilgi deposunun kesintisiz olarak erişilebilirliğini sağlamak için gerekli önlemleri almak,
- Bilgi deposuna erişimi ücretsiz sağlamak.

3. KİMLİK BELİRLEME VE DOĞRULAMA

Kamu SM, sertifika başvurusunda bulunan kamu kurum ve kuruluşlarının, kurum kimliklerini ve sertifika verilecek alan adı sahipliğini doğrular. Kamu SM doğrulama işlemini yasal ve teknik gerekliliklere göre gerekli görülen tüm belgelere ve resmi kaynaklara dayandırarak yapar.

3.1. İSİMLENDİRME

Kamu SM tarafından üretilen sertifikalarda, sertifika sahibine ait kimlik bilgileri SUE dokümanı Bölüm 3.1'de tanımlandığı şekilde belirtilir.

3.2. İLK KİMLİK DOĞRULAMA

Sertifika hizmetlerinden faydalanmak için ilk defa başvuruda bulunulduğunda, Kamu SM tarafından ilgili kurumun kimliğinin doğrulanabilmesi için SUE dokümanı Bölüm 3.2'de tanımlanan yöntemler uygulanır.

OV SSL sertifikasında yer alacak kamu kurum veya kuruluşunun ismi veya unvanı, yasal belgelere bağlı olarak doğrulanır. Burada yapılan doğrulama işlemi Kamu SM prosedürlerinde belirlendiği gibi yürütülür.

3.3. ANAHTAR YENİLEME İSTEĞİNDE KİMLİK BELİRLEME VE DOĞRULAMA

Sunucu sertifikaları için anahtar yenileme yapılmaz. Kurum talep ederse ilk kez başvuru yapılıyormuş gibi sertifika başvuru prosedürleri uygulanır. Bu durumda kimlik belirleme ve doğrulama işlemleri SUE dokümanı Bölüm 3.2'de belirtilen şekilde yapılır.

3.4. SERTİFİKA İPTAL İSTEĞİNDE KİMLİK BELİRLEME VE DOĞRULAMA

Kamu SM'ye sertifika iptal talebi gelmesi durumunda sertifika sahibi kurum sistemde tanımlı telefon numarasından aranarak kimlik belirleme ve doğrulaması yapılır, iptal talebinin teyidi alınır.

4. SERTİFİKA YAŞAM DÖNGÜSÜ İŞLEVSEL GEREKLİLİKLERİ

Bu bölümde sertifika yönetim süreçlerinde yapılan işlemler anlatılmaktadır. Süreçlerle ilgili ayrıntılar Kamu SM'nin internet sitesinde belirtilmektedir.

4.1. SERTİFİKA BAŞVURUSU

Sertifika başvurusunu kimlerin yapabildiği ve SSL sertifika başvurusu yapan kamu kurum veya kuruluşunun sorumlulukları SUE dokümanı Bölüm 4.1'de belirtilmiştir.

4.2. SERTİFİKA BAŞVURUSUNUN İŞLENMESİ

SSL başvuruları SUE dokümanı Bölüm 3.2'de ve 4.1'de açıklanan esaslar ve buna bağlı Kamu SM prosedürleri uyarınca yürütülür. Sertifika başvurusunun kabul/red edilmesi ve işlenme zamanı SUE dokümanı Bölüm 4.2'de belirtilmiştir.

4.3. SERTİFİKANIN ÜRETİLMESİ

SUE dokümanı Bölüm 4.2.2'de yer alan esaslar uyarınca kabul edilen sertifika başvuruları Kamu SM tarafından işlenir ve CSR dosyasının doğrulanmasının ardından sertifika üretilir. Bu işlemler esnasında gerçekleşen adımlar kayıt altına alınır.

Kamu SM ürettiği sertifikayı kurum yetkilisinin doğrulanmış e-posta adresine gönderir.

4.4. SERTİFİKANIN KABUL EDİLMESİ

Sertifika sahibi sertifika içerisindeki bilgilerin başvuru esnasında beyan ettiği bilgilerle aynı olup olmadığını kontrol eder ve herhangi bir uygunsuzluk durumunda derhal Kamu SM'yi bilgilendirir ve sertifikayı kullanmaz. Bu durumda sertifika, Kamu SM tarafından iptal edilir.

Kamu SM tarafından üretilen SSL sertifikaları Sertifika Şeffaflığı (Certificate Transparency - CT) log sunucularına kaydedilir.

4.5. SERTİFİKANIN VE ANAHTAR ÇİFTİNİN KULLANIMI

Sertifika sahibi ve üçüncü kişilerin sertifika ve özel anahtar kullanımıyla ilgili düzenlemeler SUE dokümanı Bölüm 4.5'de belirtilmiştir.

4.6. SERTİFİKA YENİLEME

Sertifika yenileme, aynı anahtar çifti kullanılarak sertifikanın yenilenmesi anlamına gelmektedir. Kamu SM, SSL sertifikaları için sertifika yenileme yapmaz. Sertifikasının yenilenmesini talep eden sertifika sahibi SUE dokümanı Bölüm 4.1'de anlatıldığı şekilde başvurur ve bu başvuru tamamen yeni bir sertifika başvurusu olarak değerlendirilir.

4.7. ANAHTAR YENİLEME

Anahtar yenileme, sistemde geçerli bir sertifikası bulunan sertifika sahibine, sertifikanın bitiş tarihinden önce, yeni bir anahtar çiftine sertifikanın içeriğinde bulunan bilgilerde değişiklik yapmadan, eskisinin yerine geçecek yeni bir sertifika verilmesi anlamına gelmektedir. SSL sertifikaları için anahtar yenilemesi yapılmaz. Sertifika sahibi tekrar sertifika başvurusunda bulunmak isterse SUE dokümanı Bölüm 4.1'de anlatıldığı şekilde başvurusunu gerçekleştirir. Bu başvuru sonucunda yeni bir anahtar çiftine sahip yeni bir sertifika üretilir.

4.8. SERTİFİKA DEĞİŞİKLİĞİ

Kamu SM tarafından üretilmiş bir sertifikanın içeriğindeki bilgilerde bir değişiklik olması durumunda, sertifika iptal edilir ve yeni bilgilerle birlikte yeni bir sertifika başvurusunda bulunulur. Yeni sertifika başvurusu SUE dokümanı Bölüm 4.1'de belirtilen esaslar uyarınca yürütülür.

4.9. SERTİFİKANIN İPTALİ VE ASKIYA ALINMASI

Son kullanıcı ve alt kök sertifikasının iptal edildiği durumlar, sertifika iptal başvuruları, iptal mekanizmaları ve özel anahtarın güvenliğini yitirmesine ilişkin özel gereklilikler SUE dokümanı Bölüm 4.9'da belirtilmiştir. SSL sertifikaları için askı işlemi uygulanmamaktadır.

4.10. SERTİFİKA DURUM SERVİSLERİ

Üçüncü kişiler, sertifika iptal durum kayıtlarına SİL ve OCSP aracılığıyla ulaşır. Sertifika durum servislerinin işletimsel özellikleri ve erişilebilirliği SUE dokümanı Bölüm 4.10'da belirtilmiştir.

4.11. SERTİFİKA SAHİPLİĞİNİN SONA ERMESİ

Sertifikanın kullanım süresinin dolması, iptal edilmesi veya Kamu SM'nin sertifika hizmetlerini sonlandırmasıyla sertifika sahipliği sona erer. Kamu SM, sertifikanın iptal edilmesi veya Kamu SM tarafından sertifika hizmetlerinin sonlandırılması durumunda sertifika sahibini ve varsa

taahhütnamede belirtilen kişileri bilgilendirir. Kullanım süresinin dolması durumunda Kamu SM sertifika sahibini bilgilendirmek zorunda değildir; sertifika sahibi, sertifikasının kullanım süresinin dolduğu zamanı kendisi takip etmekle yükümlüdür.

4.12. ANAHTAR SAKLAMA VE YENİDEN ÜRETME

Kamu SM, son kullanıcı anahtarlarını üretmediğinden sertifika sahiplerine ait anahtarların Kamu SM tarafından yeniden oluşturulması veya saklanması mümkün değildir.

5. YÖNETİM, İŞLEMSEL VE FİZİKSEL KONTROLLER

Kamu SM tarafından sertifika hizmeti verilirken yerine getirilmesi gereken teknik olmayan güvenlik kontrolleri SUE dokümanı Bölüm 5'de belirtilmiştir.

6. TEKNİK GÜVENLİK KONTROLLERİ

Kamu SM'nin kendi anahtar çiftleri ve erişim verilerini ürettiği, tüm sertifika yönetim işlemlerini gerçekleştirdiği sistemler CWA 14167-1, ETSI EN 319 411-1 ve CA/B Forum Baseline Requirements gereklerini sağlar. Kamu SM tarafından sertifika hizmeti verilirken yerine getirilmesi gereken teknik güvenlik kontrolleri SUE dokümanı Bölüm 6'da belirtilmiştir.

7. SERTİFİKA, SERTİFİKA İPTAL LİSTESİ VE OCSP PROFİLLERİ

Kamu SM tarafından üretilen sertifikalar ile SİL'lerin profilleri ve verilen OCSP hizmetinin yapısı SUE dokümanı Bölüm 7'de anlatılmaktadır.

7.1. SERTİFİKA PROFİLLERİ

Kamu SM,

- ISO/IEC 9594-8/ ITU-T Recommendation X.509 v.3: "Information Technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks",
- IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile",
- "CA/Browser Forum Baseline Requirements (BR) for the Issuance and Management of Publicly-Trusted Certificates" dokümanlarının güncel sürümlerine uygun olarak sertifika oluşturur.

Kamu SM devlet kurumlarına OV SSL hizmeti vermekte olduğundan devlet kurumlarına ait olan TLD'ler için kısıtlama getirmiştir. Sertifika verilecek TLD'ler, gov.tr, k12.tr, pol.tr, mil.tr, tsk.tr, kep.tr, bel.tr, edu.tr, org.tr olarak belirlenmiştir. Bunların dışındaki TLD'ler için SSL hizmeti verilmemektedir.

7.2. SİL PROFİLİ

Kamu SM, IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" dokümanına uygun olarak SİL oluşturur. Kamu SM tarafından yayımlanan SİL'lerde temel olarak yayımcı bilgileri, SİL numarası, SİL'in yayımlanma tarihi, bir sonraki SİL'in yayımlanacağı tarih ve iptal edilen sertifikaların seri numaraları ile iptal zamanları yer alır. SİL dosyaları Kamu SM tarafından imzalanmıştır.

7.3. OCSP PROFİLİ

Kamu SM, OCSP desteğini IETF RFC 6960: "Internet X.509 Public Key Infrastructure Online Certificate Status Protocol - OCSP" dokümanına uygun olarak kesintisiz şekilde sunar.

8. UYGUNLUK DENETİMLERİ VE DİĞER DEĞERLENDİRMELER

Kamu SM'nin Sİ ve SUE dokümanlarında belirtilen şartları sağlayıp sağlamadığı yılda en az bir kez olmak üzere denetlenir. Denetim raporlarının kapsamadığı zaman aralığı yoktur. Uygunluk denetimleri ETSI EN 319 411-1 standardı ve CA/B Forum Baseline Requirements kapsamında yetkili bir denetçi kurum tarafından yapılmaktadır.

Kamu SM'nin Sİ ve SUE dokümanlarına uygunluğunun denetlenmesiyle ilgili ayrıntılı bilgilendirme SUE dokümanı Bölüm 8'de yapılmaktadır.

9. DİĞER İŞLER VE HUKUKSAL MESELELER

Hukuksal meseleler ve genel iş süreçleriyle ilgili bilgilendirme SUE dokümanı Bölüm 9'da yapılmaktadır.

9.1. ÜCRETLENDİRME

Kamu SM tarafından üretilen sertifikalar için sertifika sahiplerinden ücret alınır. Ücretin miktarı ve ödeme şekli Kamu SM tarafından gönderilen teklif mektuplarında veya kurumsal web sayfasında bildirilir.

Sertifika yönetim prosedürleri içinde elektronik ortamdan ve çağrı merkezi üzerinden otomatik olarak gerçekleştirilen işlemler için ücret talep edilmez.

Kamu SM, bilgi deposundan yayımladığı dokümanlara erişim ve iptal durum kaydını SİL veya OCSP aracılığıyla duyurma hizmeti için sertifika sahibinden veya üçüncü kişilerden ücret talep etmez.

Sertifika sahibi, sertifikasını ilk teslim aldığında yaptığı kontrol neticesinde, sertifikasını kullanamadığını tespit ederse ve sorunun Kamu SM'den kaynaklanan bir hata sebebiyle ortaya çıktığı anlaşılırsa, talebi halinde sertifika sahibinin sertifika için ödediği ücret iade edilir.

9.2. FİNANSAL SORUMLULUK

Sertifika sahiplerine ve sertifikayı kullanan üçüncü taraflara yönelik finansal sorumluluklar SUE dokümanı Bölüm 9.2'de belirtilmiştir.

9.3. TİCARİ BİLGİNİN KORUNMASI

Kamu SM ve ilgili taraflar karşılıklı ticari bilgilerini üçüncü taraflarla paylaşmaz. Bu amaçla gerekli olan önlemleri alırlar.

9.4. KİŞİSEL BİLGİNİN GİZLİLİĞİ

Kamu SM verdiği sertifika hizmetleri kapsamında, sertifika başvuru sahiplerine, sertifika sahibi müşterilerine ya da diğer katılımcılara ait kişisel/kurumsal bilgilerin gizliliğini korur.

Kamu SM sertifika talep eden kurumdan, elektronik sertifika vermek için gerekli bilgiler hariç bilgi talep etmez. Kamu SM elde ettiği kişisel/kurumsal bilgileri sertifika hizmeti vermek dışında başka amaçlar

için kullanmaz, üçüncü kişilere vermez, sertifika sahibinin izni olmaksızın sertifikayı üçüncü kişilerin ulaşabileceği ortamlarda bulundurmaz.

Kamu SM sertifika sahibinin yazılı rızası ile bilgileri üçüncü kişilerle paylaşabilir.

Kamu SM sertifika sahiplerine ait gizli bilgileri, mahkeme kararı olması durumunda açıklayabilir.

9.5. TELİF HAKLARI

Kamu SM tarafından üretilen tüm sertifikalar ve dokümanlar ile Sİ ve SUE dokümanına bağlı olarak geliştirilen tüm bilgilerin fikri mülkiyet hakları Kamu SM'ye aittir.

9.6. BEYAN VE TAAHHÜTLER

Kamu SM, sertifika sahipleri ve üçüncü kişiler sertifika sözleşmeleri ile taahhütnamelerde sözü geçen yükümlülükleri yerine getirirler. ESHS, kayıt birimi, sertifika sahibi, üçüncü kişiler ve diğer katılımcıların beyan ve taahhütleriyle ilgili bilgilendirme SUE dokümanı Bölüm 9.6'da yapılmaktadır.

9.7. YÜKÜMLÜLÜKLERDEN FERAGAT

Kamu SM ile sertifika sahibi kamu kurum veya kuruluşları arasındaki yükümlülük, SSL Taahhütnamesinde belirtildiği şekilde sona erer.

9.8. SORUMLULUKLA İLGİLİ SINIRLAMALAR

Kamu SM ve sertifika hizmetlerini alan tarafların sorumluluklarıyla ilgili sınırlamalar SSL Taahhütnamesinde de belirlenir.

9.9. TAZMİNAT HALLERİ

Kamu SM ve sertifika hizmeti alan taraflar arasında yükümlülüklerin yerine getirilmemesinden kaynaklanan zararlar, tarafların o ana kadar somut olarak gerçekleşmiş hak ve alacakları korunmak suretiyle tasfiye edilir.

9.10. ANLAŞMA SÜRESİ VE ANLAŞMANIN SONA ERMESİ

Sertifika sahipleri SSL Taahhütnamesine uygun olarak Kamu SM ile işbirliği içinde çalışır.

Sertifika sahipleri sertifika hizmetlerini aldıkları süre boyunca Sİ ve SUE dokümanı ile sertifika yönetim prosedürlerinde belirtilen şartları yerine getirmeyi kabul ederler.

Kamu SM sertifika hizmeti verdiği süre boyunca Sİ ve SUE dokümanı, sertifika yönetim prosedürleri ve sertifika sahibine ilettiği SSL Taahhütnamesindeki şartları yerine getirir.

Sertifika sahibinin imzaladığı SSL Taahhütnamesinin süresi sertifikanın geçerlilik süresi kadardır. Ancak, sertifikanın iptal edilmesi durumunda taahhütnamenin süresi de sona erer.

SSL Sertifika Sahibi Taahhütnamesinin sona ermesiyle hizmeti alan kurumun, Sİ ve SUE dokümanında belirtilen şartları sağlamakla ilgili yükümlülükleri ortadan kalkar.

Sertifika sahibinin taahhütnameye uygun hareket etmemesinden dolayı uğrayacağı zararlardan Kamu SM sorumlu tutulamaz.

9.11. SİSTEM BİLEŞENLERİ İLE HABERLEŞME VE KİŞİSEL BİLGİLENDİRME

Kamu SM, sertifika yönetim prosedürlerinde sertifika başvurusunun sonucu, iptal, güncelleme ve yenileme taleplerinin sonuçları hakkında sertifika sahibini bilgilendirir.

Sertifika yönetim işlemleri sırasında sertifika sahipleri ile yapılan haberleşmenin hangi durumlarda, ne şekilde yapılacağı Kamu SM'nin sertifika yönetim prosedürlerinde detaylı olarak belirtilir.

9.12. DEĞİŞİKLİK HALLERİ

Bu doküman Kamu SM tarafından yazılmıştır. Dokümanda yapılabilecek değişiklikler ekleme ve değiştirme şeklinde olabileceği gibi, Kamu SM dokümanın tamamen yenilenmesine de karar verebilir.

Bu dokümanda yapılan değişiklikler dokümanın yenilenerek Kamu SM bilgi deposu üzerinden erişime açılması ile duyurulur. Yenilenen doküman en fazla 1 (bir) hafta sonra bilgi deposundan yayımlanır ve yayımlandığı tarihte yürürlüğe girer.

9.13. ANLAŞMAZLIK HALLERİ

Taraflar arasında çıkan tüm anlaşmazlıkların sulhen çözümü esastır. İhtilafların çözümünde karşılıklı imzalanan sözleşmeler, taahhütnameler, Kamu SM Sertifika İlkeleri ve Kamu SM Sertifika Uygulama Esasları dokümanlarına başvurulur. Herhangi bir anlaşmazlık çözüm mekanizmasına başvurmadan önce, tarafların Kamu SM'yi bilgilendirmesi ve anlaşmazlıkları doğrudan Kamu SM ile çözme girişiminde bulunması gerekir. İhtilafların sulhen çözümünün mümkün olmaması halinde, ihtilafların çözümünde görevli ve yetkili mahkeme Türkiye Cumhuriyeti Gebze Mahkemeleri'dir.

9.14. UYGULANACAK HUKUK

SUE'nin uygulanmasında ve yorumlanmasında Türkiye Cumhuriyeti Hukuku geçerlidir.

9.15. UYGULANABİLİR YASALARLA UYUM

Bu dokümanda geçen hükümlerin daha sonra yürürlüğe girecek ilgili mevzuata aykırı bulunması halinde dokümanda gerekli değişiklikler yapılarak uygun hale getirilir.