SSL SERTİFİKA İLKELERİ VE SERTİFİKA UYGULAMA ESASLARI

Kamu Sertifikasyon Merkezi
TÜBİTAK Yerleşkesi, P.K. 74
Gebze 41470 Kocaeli, TÜRKİYE
Tel: +90 (0) 262 648 18 18
Faks: +90 (0) 262 648 18 00
www.kamusm.gov.tr
Yayın Tarihi:Haziran 20,2017
Versiyon: 2.2.1

Yasal Uyarı

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 ve Sertifika Uygulama Esasları (Sİ/SUE) olarak isimlendirilen bu doküman, Kamu SM'nin, Türkiye Cumhuriyeti Devleti'ne bağlı kamu kurum ve kuruluşlara OV SSL (Organization Validated SSL) sağlayıcılığı konusundaki faaliyetlerini nasıl yürüttüğünü 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 TS 102 042 Electronic Signatures Infrastructure (ESI); Policy Requirements for Certification Authorities Issuing Public Key Certificates" standardının güncel sürümü ile ETSI TS 102 042 standardında referans verilen ve http://www.cabforum.org adresinde yayımlanan "CA/Browser Forum Baseline Requirements (BR) for the Issuance and Management of Publicly-Trusted Certificates" dokümanının güncel sürümüne uyar. Sİ/SUE dokümanı ile bu dokümanlar arasında herhangi bir uyuşmazlık olması durumunda ilgili dokümanlardaki gereklilikler geçerli olacaktır.

Bu Sİ/SUE dokümanı, 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 Bakış

Sİ/SUE dokümanı, sistem bileşenlerinin rollerini, sorumluluklarını ve ilişkilerini tanımlar; kayıt ve sertifika yönetim işlemlerinin gerçekleştirilme şeklini anlatır.

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 anahtar çifti ve 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.

Sİ/SUE dokümanı, "Internet 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. Doküman içeriğinde belirtilen bir kısım alt başlıkların altındaki "Düzenlenmesine gerek duyulmamıştır." ibaresi, ihtiyaç duyulmadığından düzenleme yapılmadığını ifade etmektedir.

1.2. Doküman Adı ve Tanımı

Doküman Adı: SSL Sertifika İlkeleri ve Sertifika Uygulama Esasları

Doküman Sürüm Numarası: 1.0.1

Tarih	Değişiklikler	Versiyon
30.03.2016	İlk doküman	**1.0.0**
07.03.2017	- 3.2.2 Kurumsal Kimliğin Doğrulanması bölümünde güncelleme yapıldı. - Versiyon tarihçesi eklendi. - Sertifika profilleri güncellendi. (seri numarası). - 4.9.3 Sertifika İptal Başvuru Yöntemleri güncellendi.	**1.0.1**
14.04.2017	- 3.2.2 Kurumsal Kimliğin Doğrulanması bölümü güncellenmiştir. - 2017 yıllık düzenli CPS güncellemeleri kapsamında değişiklikler yapılmıştır.	**2.1.1**
20.06.2017	- Kimlik doğrulama adımlarına CAA kayıtları incelemesi eklenmiştir.	**2.2.1**

Yayın Tarihi: 07.03.2017

Nesne Tanımlama Numarası: 2.16.792.1.2.1.1.5.7.1.3

Bu doküman, Kamu SM OV SSL sertifikası hizmeti verirken uyguladığı esasları tanımlayan Sİ/SUE dokümanıdır ve sunuculara yönelik verilen OV SSL sertifikalarını kapsar. OV SSL sertifikaları, ETSI TS 102 042 standardında tanımlanan "Normalized Certificate Policy – Standartlaştırılmış Sertifika İlkeleri" uyarınca üretilir ve yönetilir.

Sİ/SUE dokümanı http://depo.kamusm.gov.tr/ilke adresinde kamuya açık olarak yayımlanmaktadır.

1.3. Sistem Bileşenleri

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.

1.3.1. Elektronik Sertifika Hizmet Sağlayıcısı

Kamu SM, ESHS olarak OV SSL sertifika hizmeti vermektedir. Bunun için tepede bir kök ve altında tümü Kamu SM'ye ait alt kök makamlardan oluşan bir hiyerarşi mevcuttur. SSL sertifikaları alt kök makamından üretilmektedir. 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 başvuru ve iptal 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 bu Si/SUE dokümanına 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.

1.3.5. Diğer Bileşenler

Düzenlenmesine gerek duyulmamıştır.

1.4. Sertifika Kullanımı

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 Sınırıları

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

1.5. İlke ve Uygulama Esaslarının Yönetimi

1.5.1. Doküman Yönetimi

Bu Si/SUE dokümanı Kamu SM tarafından yazılmıştır. Kamu SM, gerekli gördüğü durumlarda dokümanda değişiklik yapabilir.

1.5.2. İletişim Bilgileri

Bu Si/SUE dokümanının 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, Sİ/SUE dokümanını herkesin erişimine açık bulunan http://depo.kamusm.gov.tr/ilke internet adresinden yayımlar.

1.5.3. Sertifika Uygulama Esaslarının İlkelere Uygunluğunu Belirleyen Kişi

Bu Sİ/SUE dokümanının uygunluğu Kamu SM yönetimi ve yönetim tarafından yetki verilen kişiler tarafından belirlenir.

1.5.4. Sertifika Uygulama Esasları Onay Prosedürleri

Bu Sİ/SUE dokümanının yayımlanma onayı, Kamu SM yönetimi ve yönetim tarafından yetki verilen kişiler tarafından gerçekleştirilen incelemelerden sonra verilir.

1.6. Tanımlar ve Kısaltmalar

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.

Çevrim içi 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.

DV SSL: ETSI TS 102 042 standardında tanımlanan "Domain Validation Certificate Policy – Alan Adı Doğrulamalı Sertifika İlkeleri" uyarınca üretilen ve idame edilen SSL sertifikası.

EV SSL: ETSI TS 102 042 standardında tanımlanan "Extended Validity Certificate Policy – Genişletilmiş Kurumsal Doğrulamalı Sertifika İlkeleri" uyarınca üretilen ve idame edilen SSL sertifikası.

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 TS 102 042 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.

Zaman damgası: Bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı ve/veya kaydedildiği zamanın tespit edilmesi amacıyla, ESHS tarafından elektronik imzayla doğrulanan kayıt.

1.6.2. Kısaltmalar

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

BS (British Standards): İngiliz Standartları

CA (Certificate Authority): Sertifika Makamı

CAA (Certificate Authority Authorization): Sertifika Makamı Yetkilendirmesi

CEN (Comité Européen de Normalisation): Avrupa Standardizasyon Komitesi

CP (Certificate Policy): Sertifika İlkeleri

CPS (Certificate Practise Statement): Sertifika Uygulama Esasları

CRL (Certificate Revocation List): Sertifika İptal Listesi

CWA (CEN Workshop Agreement): CEN Çalıştay Kararı

DSA (Digital Signature Algorithm): Sayısal İmza Algoritması

EAL (Evaluation Assurance Level): Değerlendirme Garanti Düzeyi

ECC: Elliptic Curve Cryptography

ECDSA: Elliptic Curve Digital Signature Algorithm

ESHS: Elektronik Sertifika Hizmet Sağlayıcısı

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

ETSI TS (ETSI Technical Specification): ETSI Teknik Özellikleri

FIPS PUB (Federal Information Processing Standards Publications): Federal Bilgi İşleme Standartları Yayınları

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

ISO/IEC (International Organisation for Standardisation / International Electrotechnical Commitee): Uluslararası Standardizasyon Teşkilatı / Uluslararası Elektroteknik Komitesi

ITU (International Telecommunication Union): Uluslararası Telekomünikasyon Birliği

Kamu SM: Kamu Sertifikasyon Merkezi

LDAP (Lightweight Directory Access Protocol): Dizin Erişim Protokolü

OCSP (Online Certificate Status Protocol): Çevrim İçi Sertifika Durum Protokolü

PKI (Public Key Infrastructure): Açık Anahtar Altyapısı

RSA: Rivest Shamir Adleman (Algoritmayı bulan kişilerin baş harfleri)

SAN: Subject Alternative Name

SHA (Secure Hash Algorithm): Güvenli Özet Algoritması

Sİ: Sertifika İlkeleri

SİL: Sertifika İptal Listesi

SSL: Secure Sockets Layer

SUE: Sertifika Uygulama Esasları

TLD (Top Level Domain): Üst Seviye Alan Adı

2. YAYIN VE BİLGİ DEPOSU SORUMLULUKLARI

Bilgi deposu, Kamu SM'nin kök ve alt kök sertifikalarını, iptal durum kayıtlarını, Sİ/SUE gibi dokümanları 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. Bilgi 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. Sertifika Hizmeti ile İlgili Bilgilerin Yayımlanması

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/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. Yayım Zamanı ve Sıklığı

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

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

SİL'lerin yayımlanma sıklığı ve OCSP kayıtlarının güncellenme sıklığı bu dokümanda Bölüm 4.9.7 ve 4.9.9'da belirtilmektedir.

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

2.4. Bilgi Deposuna Erişim Kontrolleri

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. İsimlendirme

3.1.1. İsim Alanı Tipleri

Kamu SM tarafından üretilen sertifikalarda, sertifika sahibine ait kimlik bilgilerinin belirtildiği DN (Distinguished Name-Ayırt edici isim) alanı boş olamaz ve DN içinde "ITU X.500" biçiminin desteklediği isim tipleri kullanılır.

3.1.2. İsim Bilgilerinin Teşhise Elverişli Olması

Kamu SM tarafından üretilen sertifikalardaki isimler net ve anlamlı olmalıdır. Sertifikalarda Kamu SM tarafından doğrulanmış alan adı ve kurum bilgileri bulunur.

3.1.3. Sertifika Sahibinin Takma İsim veya Lakap Kullanması

Sertifika içeriğinde takma isim veya lakap kullanılmasına izin verilmez.

3.1.4. Farklı İsim Alanı Tiplerinin Yorumlanması

Sertifika içeriğinde ITU X.500 biçimi dışında isim alanı tipi kullanılmaz.

3.1.5. İsim Bilgilerinin Tekilliği

Kamu SM tarafından oluşturulan sertifikaların içeriğindeki kimlik bilgileri her kamu kurumu için ayırt edici niteliktedir. Aynı kamu kurumuna ait sertifikaların içeriğindeki kimlik bilgilerinin aynı olmasına izin verilmektedir. Ancak farklı kurumlara ait elektronik sertifikaların içeriğindeki kimlik bilgilerinin aynı olması engellenmektedir. Sertifika içinde IP adreslerinin, kurum bilgisi olmaksızın yalnızca alan adlarının, sanal sunucu adlarının veya iç sunucu isimlerinin bulunmasına izin verilmez.

Kamu SM yalnızca Türkiye'deki kamu kurum ve kuruluşlarına OV SSL sertifikası vermektedir. Kamu kurum ve kuruluşlarına verilen OV SLL sertifikalardaki:

- CN alanı:
  - "CN" alanında DNS'te sertifika sahibi kamu kurum veya kuruluşu adına kayıtlı sunucu adı yazılır.
  - OV SSL wildcard sertifikalarında bu alana "*.<alan adı>" yazılır. Bu alan "*.com" veya "*.com.tr" gibi ayırt edici olmayan adlar içermez.
  - Bu alana IP adresi veya iç sunucu adı yazılmaz.
- "O" alanında sertifika sahibi kamu kurumu veya kuruluşunun teşkilat kanununda veya diğer mevzuatta yer alan açık unvanı veya anlaşılır şekilde kısaltılmış biçimi bulunur.
- "OU" alanında organizasyon birimi ya da marka adının bulunması halinde, Türk Standartları Enstitüsü'nde kayıtlı marka adı yazılır.
- "SERIALNUMBER" alanı, sertifika sahibi kamu kurumunun benzersiz vergi numarasıdır.
- "L" alanında, sertifika sahibi kamu kurumu veya kuruluşun bulunduğu il bilgisi bulunur.

- "C" alanında, başvuru sahibi kamu kurum ve kuruluşunun bulunduğu ülkenin ISO 3166-1 Alpha-2 standardında yer alan ülke kodu (TR) yer alır.
- "SAN" alanında, CN alanında bulunan DNS'te sertifika sahibi kamu kurum veya kuruluşu adına kayıtlı sunucu adı yazılır. Sunucu sertifikalarında her bir alan adının sertifika başvuru sahibi kuruma ait veya kontrolü altında olduğunun doğrulanması koşuluyla birden fazla alan adı da yazılabilir.

3.1.6. Markanın Tanınması, Doğrulanması ve Rolü

Sertifika başvuru sahipleri başvuru esnasında başkalarına ait fikri ve sınai mülkiyet haklarına zarar verecek isimleri kullanamazlar. Kamu SM sertifika başvurusu esnasında kullanılan isimlerin fikri ve sınai mülkiyet haklarının başvuru sahibine ait olup olmadığını doğrulamaz. Ortaya çıkabilecek herhangi bir fikri ve sınai mülkiyet hakkı problemi ile ilgili olarak Kamu SM sertifika başvurusunu reddetme veya ürettiği sertifikaları iptal etme hakkına sahiptir. Problemin giderilmesine yönelik olarak Kamu SM herhangi bir arabulucuk faaliyeti yürütmez.

3.2. İlk Kimlik Doğrulama

Sertifika hizmetlerinden faydalanmak için ilk defa başvuruda bulunulduğunda, Kamu SM tarafından ilgili kurumun kimliğinin doğrulanabilmesi için aşağıda tanımlanan yöntemler uygulanır.

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

3.2.1. Özel Anahtar Sahipliğinin Kanıtlanması

SSL Sertifika başvurusu esnasında başvuru sahibi tarafından oluşturulan sertifika imzalama isteği özel anahtar ile imzalanır. Bu sayede özel anahtara sahiplik doğrulanır.

3.2.2. Kurumsal Kimliğin Doğrulanması

Kamu SM'den OV SSL sertifikası talebinde bulunan kamu kurumlarının kimlik, adres ve alan adı doğrulamaları Kamu SM ve ilgili kamu kurumu arasında yapılan resmi yazışmalar ve sertifika imzalama isteğinde belirtilen alan adı sahipliğinin ilgili kanallardan (nic.tr) doğrulanması yoluyla yapılır.

Kamu SM'ye yapılan tüm başvurular aşağıdaki bilgileri doğrulayacak yasal belgeler ile desteklenir ve bu bilgilerin bir kısmı özne (Subject) alanı içinde yer alır:

- Kurumun yasal unvanı – Sertifikada O alanında yer alacak olan kurum adı(Yayımlanır)
- Kurumun alt birim adı - Sertifikada OU alanında yer alacak birim adı(Yayımlanır)
- Kurumun adresi (İl/ilçe/Posta kodu) (Yayımlanır)
- Vergi numarası (Yayımlanır)
- Kurum yetkilisi bilgisi
- Alan adının tamamı (FQDN – Fully Qualifed Domain Name) (Yayımlanır)
- Alan adına sahiplik yapan yöneticinin tam adı, email adresi ve iletişim bilgileri
- PKCS#10 Sertifika imzalama isteği
- Taahhütname

Yukarıda yer alan bilgilerin tamamı başvuru formunda zorunludur. Başvuru formu alındıktan sonra Kamu SM doğrulamayı temel olarak iki kısımda gerçekleştirir. Öncelikle başvuruda bulunan kamu kurumunun kimliği ve adresi doğrulanır. İkinci kısımda ise kamu kurumunun alan adı sahipliği doğrulanmaktadır. Her iki doğrulama yöntemi de CA/B Forum Baseline Requirements dokümanına uygun şekilde yapılır.

Kimlik ve adres doğrulama adımları:

- Sertifika talep eden kurumun kimliği ve adresi yasal belgelere göre doğrulanır, kimlik ve adres bilgilerinin sertifika imzalama isteği içerisindeki bilgilerle aynı olup olmadığı kontrol edilir.
- Sertifika başvurusunda bulunan kurum yetkilisinin kurum adına başvuru hakkına sahip olduğu yasal belgeler ile doğrulanır. Buna göre doğrulanan telefon numaralarından sertifika başvurusunda bulunan kurum yetkilisi aranarak başvurusunu teyit etmesi istenir.
- Kurum yetkilisince veya kamu kurumları adına resmi belge düzenlemeye yetkili kişilerce ibraz edilebilecek güncel bir resmi belge ile faaliyetinin devamlılığı teyit edilir.

Alan adı sahipliğini doğrulamak için:

- Alan adının Bölüm 7.1.5'de listesi verilen TLD'lere sahip bir devlet kurumu alan adı olduğu ilk olarak kontrol edilir.
- Başvuru formunda belirtilen alan adı "nic.tr" ile doğrulanır. "nic.tr", Türkiye' de ".tr" üst düzey etki alanındaki alan adlarının kaydını tutan devlet kurumudur. Başvuru formunda yazılı olan ve sahipliği belirtilen alan adı bilgilerinin nic.tr tarafından sağlanan bilgilerle aynı olup olmadığı kontrol edilir. Ayrıca başvuru formunda belirtilen alan adının, sertifika imzalama isteği içerisindeki alan adıyla aynı olup olmadığı kontrol edilir.
- Kamu SM, alan adı üzerinde kurumun kontrolünü test etmek amacıyla alan adında sunulan bir sayfada değişiklik talep eder. Talep edilen değişiklik, kurum tarafından sertifika imzalama isteğinde kullanılan bilgilerden oluşturulacak istek belirtecinin, alan adında hizmet veren bir sayfanın meta etiketi (meta tag) içinde yayımlanmasıdır. 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.
- Kamu SM doğrulama adımlarına ek olarak CAA kayıtlarını RFC 6844 (DNS Certification Authority Authorization (CAA) Resource Record) prosedürlerine uygun şekilde incelemektedir. "kamusm.gov.tr" alan adı CAA kayıtlarında issue ve issuewild property tag'leri içinde aranmaktadır.

Wildcard sertifikalarda alan adı doğrulamada ilk olarak "*.com" veya "*.com.tr" gibi ayırt edici olmayan adlar içermediği kontrol edilir. Wildcard sertifikalarda alan adı sahipliğini doğrulamak için yukarıda belirtilen maddelerin tamamı uygulanır. Bunun yanı sıra, "*.<alan adı>" 'na sahip bir web sitesi için Kamu SM tarafından belirlenen bir "xxx.<alan adı>" üzerinde istek belirtecinin yayımlanması talep edilir.

3.2.3. Kişisel Kimliğin Doğrulanması

Kamu SM kamu kurumlarına OV SSL hizmeti verdiğinden, bireysel değil kurumsal başvuru kabul etmektedir.

3.2.4. Doğrulanmayan Sertifika Sahibi Bilgileri

Kamu SM tarafından oluşturulan SSL sertifikaları doğrulanmayan bilgiler içermez.

3.2.5. Yetkinin Doğrulanması

3.2.2'de anlatıldığı şekilde yapılır.

3.2.6. Uyum Kriterleri

Düzenlenmesine gerek duyulmamıştır..

3.3. Anahtar Yenileme İsteğinde Kimlik Belirleme ve Doğrulama

3.3.1. Olağan Anahtar Yenileme İsteğinde Kimlik Belirleme 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 Bölüm 3.2'de belirtilen şekilde yapılır.

3.3.2. İptal Sonrası Anahtar Güncelleme İsteğinde Kimlik Belirleme 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 Bölüm 3.2'de belirtilen şekilde yapılır.

3.4. Sertifika İptal İsteğinde Kimlik Belirleme 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 teyyidi 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. Sertifika Başvurusu

4.1.1. Sertifika Başvurusunu Kimlerin Yapabildiği

SSL sertifikası için kamu kurum ve kuruluşları Kamu SM'ye başvuruda bulunabilir. Bu başvurular yetkilendirilmiş bir kurum çalışanı tarafından kurumsal olarak yapılır. Kurum, Kamu SM'den alacağı sertifika hizmetlerinin şartlarını belirleyen SSL Taahhütnamesi'ni ve Güvenli Sunucu Sertifikası Talep Formu'nu doldurup ıslak imzalı ve mühürlü olarak Kamu SM'ye gönderir. Kurum çalışanı, kurumun talebi olmadan bireysel olarak sertifika başvurusunda bulunamaz.

4.1.2. Kayıt İşlemleri ve Sorumluluklar

SSL sertifika başvurusu yapan kamu kurum veya kuruluşunun sorumlulukları şunlardır:

- Bu Sİ/SUE dokümanında gerekliliği belirtilen tüm bilgileri içerecek şekilde Güvenli Sunucu Sertifikası Talep Formu'nu ve SSL Taahhütnamesi'ni ıslak imzalı ve mühürlü olarak Kamu SM'ye gönderir. Kurum, Kamu SM'ye göndermiş olduğu bilgilerin doğruluğunu takip etmekle ve bu bilgilerde değişiklik olması halinde Kamu SM'yi bilgilendirmekle yükümlüdür.
- Kurum, anahtar çiftini kendisi üretir ve özel anahtarın kendisinde olduğunu ispat edecek şekilde sertifika istek dosyasını (Certificate Signing Request - CSR) oluşturur ve kurumsal e-posta adresinden Kamu SM'ye iletir.
- Özel anahtarın gizliliğini ve bütünlüğünü korumak için gerekli tüm tedbirleri alır.

4.2. Sertifika Başvurusunun İşlenmesi

4.2.1. Kimlik Tanımlama ve Doğrulama İşlevlerinin Yerine Getirilmesi

SSL başvuruları Bölüm 3.2'de ve 4.1'de açıklanan esaslar ve buna bağlı Kamu SM prosedürleri uyarınca yürütülür.

4.2.2. Sertifika Başvurusunun Kabul veya Reddi

Bölüm 3.2'de açıklanan esaslar ve Kamu SM başvuru prosedürlerine göre gerekli form ve belgelerin eksiksiz olarak tamamlanmış olması halinde sertifika başvurusu kabul edilir. Başvurusu kabul edilen kurum Kamu SM sisteminde tanımlanır ve sertifika üretim süreci başlatılır.

Kamu SM, aşağıdaki durumlardan herhangi birinin oluşması halinde sertifika başvurusunu reddeder:

- Bölüm 3.2'de açıklanan esaslar ve Kamu SM başvuru prosedürlerine göre gerekli form ve belgelerin tamamlanmaması,
- Bilgi ve belgelerin doğrulanmasına ilişkin sorgulamalara başvuru sahibinin zamanında veya tatminkar yanıt vermemesi,
- Kurumun herhangi bir resmi kaydının olmaması,
- SSL sertifikasının üretilmesinin, Kamu SM'nin itibarını zedeleyebileceğine ilişkin kuvvetli bir kanaatinin oluşması,

- Sertifika başvurusu sırasında beyan edilen belgelerde tahrifat, hata, eksik onay, eksik bilgi veya yanlış bilgi olması,
- Gönderilen CSR dosyasının teknik kriterleri sağlamaması.

Başvurusu kabul edilmeyenlerle ilgili bilgilendirme kuruma yazılı veya sözlü olarak yapılır. Yazılı bilgilendirme kuruma e-posta gönderme yoluyla yapılır. Sözlü bilgilendirme kuruma telefon açılarak yapılır. Kurum ve başvuru sahibine ait e-posta ve telefon bilgileri başvuru sırasında beyan edilen bilgilerdir. Gereken düzeltmeler yapılıp eksikler tamamlandıktan sonra başvuru tekrarlanabilir.

4.2.3. Sertifika Başvurusunun İşlenme Zamanı

Başvurunun, Bölüm 3.2'de yer alan esaslar ve Kamu SM prosedürlerine göre eksiksiz ve doğru olması halinde ilgili belgelerin Kamu SM'ye ulaşmasının ardından en geç 3 (üç) iş günü içinde başvuru işleme alınır.

İşlenmiş bir sertifika başvurusunun, Bölüm 4.2.2'de yer alan esaslar uyarınca kabul edilmesinden sonra üretimi en geç 2 (iki) iş günü içinde yapılır.

4.3. Sertifikanın Oluşturulması

4.3.1. Sertifika Oluşturulmasında ESHS'nin İşlevleri

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 loglanır.

4.3.2. Sertifika Oluşturulması ile İlgili Sertifika Sahibinin Bilgilendirilmesi

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

4.4. Sertifikanın Kabul Edilmesi

4.4.1. Kabulün Şekli

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.

SSL sertifikası, başvuru sahibine gönderilmesine müteakip 10 (on) işgünü içerisinde herhangi bir dönüş olmaması durumunda kabul edilmiş olur.

4.4.2. Sertifikanın ESHS Tarafından Yayımlanması

Kamu SM ürettiği SSL sertifikalarını yayımlamamaktadır.

4.4.3. Sertifikanın Oluşturulmasının Diğer Bileşenlere Duyurulması

Düzenlenmesine gerek duyulmamıştır.

4.5. Sertifikanın ve Anahtar Çiftinin Kullanımı

4.5.1. Sertifika Sahibinin Sertifika ve Özel Anahtar Kullanımı

Sertifika sahibi, sertifikasını ve sertifikaya ait özel anahtarını, tabi olunan standartlar ve diğer düzenlemeler ile Sİ/SUE dokümanında ve ilgili sertifika sahibi taahhütnamesinde yer alan koşullar ve belirlenmiş sınırlar içinde kullanmalıdır.

Sertifika sahibi, özel anahtarı yetkisiz kişilerin erişimine karşı korumakla yükümlüdür. SSL sertifikasına karşılık gelen özel anahtar yalnızca sertifikada "Anahtar Kullanımı" alanında belirtilen amaçlar dahilinde kullanılabilir.

4.5.2. Üçüncü Kişilerin Sertifika ve Açık Anahtarı Kullanımı

Sertifika sahibine ait sertifikaların içinde yer alan açık anahtar, üçüncü kişilerce doğrulama amacıyla kullanılır. Üçüncü kişiler, güvenecekleri sertifikanın ve sertifikayı oluşturan ESHS'nin sertifikasının geçerliliğini kontrol etmekle, sertifikanın "Anahtar Kullanımı" alanında belirtilen amaçlar doğrultusunda kullanıldığını doğrulamakla ve bu Sİ/SUE'de belirtilen kullanım koşullarına uymakla yükümlüdürler.

Sertifikalanın doğrulanamaması durumunda sertifikaya dayanarak işlem yapılmamalıdır.

Kamu SM, üçüncü kişilerin açık anahtar ve sertifika kullanımında, söz konusu şartları yerine getirmemelerinden sorumlu değildir.

4.6. Sertifika Yenileme

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

4.7. Anahtar Yenileme

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 Bölüm 4.1'de anlatıldığı şekilde başvurusunu gerçekleştirir. Bu başvuru sonucunda yeni bir anahtar çiftine sahip yeni bir sertifika üretilir.

4.8. Sertifika Değişikliği

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 Bölüm 4.1'de belirtilen esaslar uyarınca yürütülür.

4.8.1. Sertifika Değişikliğini Gerektiren Durumlar

Düzenlenmesine gerek duyulmamıştır.

4.8.2. Sertifika Değişiklik Talebinde Bulunabilecek Kişiler

Düzenlenmesine gerek duyulmamıştır.

4.8.3. Sertifika Değişiklik Talebinin İşlenmesi

Düzenlenmesine gerek duyulmamıştır.

4.8.4. Yeni Sertifikayla İlgili Sertifika Sahibine Bildirim Yapılması

Düzenlenmesine gerek duyulmamıştır.

4.8.5. Değişiklik Yapılmış Sertifikanın Kabul Şekli

Düzenlenmesine gerek duyulmamıştır.

4.8.6. ESHS Tarafından Değişiklik Yapılmış Sertifikanın Yayımlanması

Düzenlenmesine gerek duyulmamıştır.

4.8.7. Diğer Katılımcılarının Yeni Sertifika Üretimiyle İlgili Bilgilendirilmesi

Düzenlenmesine gerek duyulmamıştır.

4.9. Sertifikanın İptali ve Askıya Alınması

4.9.1. Sertifikanın İptal Edildiği Durumlar

Sertifika sahibi, aşağıdaki sebeplerin ortaya çıkması durumunda sertifikasının iptal edilmesi için Kamu SM'ye başvuruda bulunur:

- Özel anahtarın güvenliğinin kaybedildiğinden şüphelenilmesi,
- Sertifikanın içeriğinde yer alan bilgilerin değişmesi,
- Alan adı sahipliğinin sona ermesi.
- Kamu SM, aşağıdaki sebeplerin ortaya çıkması durumunda sertifika sahibine ait sertifikayı iptal eder:
- Sertifika içeriğindeki sertifika sahibine ait bilgilerin sahteliğinin veya yanlışlığının ortaya çıkması,
- Sertifikanın SSL Taahhütnamesi ve Sİ/SUE dokümanında belirtilen şartlara aykırı kullanımının tespit edilmesi,
- Bir mahkemenin veya bir yetkilinin sertifika sahibinin alan adı sahipliğini veya kullanma yetkisini ortadan kaldırdığına dair Kamu SM'ye bir bildirimde bulunulması veya bunun Kamu SM tarafından anlaşılması,
- Kamu SM'nin sertifikayı imzalamak için kullandığı özel anahtarın güvenliğinin bozulması,
- SSL sertifikalarının üretiminde kullanılan anahtar uzunluğunun veya kriptografik algoritmaların uygunluğunun ortadan kalkması,
- Kamu SM'nin işleyişine son vermesi ve verilen sertifikaların yönetim işlemlerinin başka bir ESHS tarafından devamlılığının sağlanamaması.

4.9.2. Sertifika İptal Başvurusunu Kimlerin Yapabildiği

Sertifika sahibi kurumun yetkilisi, Kamu SM tarafından verilen SSL sertifikalarının iptalini isteme yetkisine sahiptir. Bölüm 4.9.1'de belirtilen durumlarda Kamu SM'nin de sertifikayı iptal etme yetkisi vardır. Ancak sertifikayı Kamu SM iptal ettiğinde, sertifika sahibi kurumu bilgilendirir, iptal sebebini açıklar.

4.9.3. Sertifika İptal Başvuru Yöntemleri

SSL sertifikası iptal başvurusu, sertifika sahibi kurumun yetkilisi tarafından Kamu SM' ye "SSL Sertifika İptal Başvurusu" adında kurum onaylı resmi yazı ile yapılır. Başvuru yapacak kurumlar resmi yazı formunu Kamu SM web sitesinde bulabilirler. İlgili doküman tam bir şekilde doldurulmalıdır. Ancak iptal işleminin acil olduğu durumlarda kurum yetkilisi telefonla Kamu SM'yi arayarak ve kurumsal eposta adresinden taranmış onaylı resmi yazıyı göndererek iptal talebinde bulunabilir. Bu durumda, eposta ile gelen resmi yazı kontrol edildikten ve telefonda gerekli doğrulamalar yapıldıktan sonra sertifika iptal edilir.

Sertifikası iptal edilen kuruma e-posta yoluyla bilgi verilir ve iptal bilgisi SİL ve OCSP'ye Bölüm 4.9.5'de belirtilen sürede yansıtılır.

Kamu SM'ye ait kök ve alt kök sertifikaların iptal edilmesi durumunda iptal durumu, mümkün olan en kısa sürede ilgili taraflara duyurulur. İptal edilen kök veya alt kök sertifikalarının imzasını taşıyan tüm sertifikalar iptal edilir ve sahipleri e-posta veya SMS yoluyla bilgilendirilir.

4.9.4. İptal İsteği Erteleme Süresi

Sertifika sahibinin sertifika iptal talebini geciktirebileceği maksimum süreyi ifade eder. Sertifika sahibi iptal talebini en kısa sürede Kamu SM'ye iletmelidir. Sertifika sahibinin, iptal isteğini ertelemesinden kaynaklanan sorunlardan Kamu SM sorumlu tutulamaz.

4.9.5. İptal İsteğinin İşlenme Süresi

Kamu SM, kendisine gelen geçerli iptal başvurularını derhal işleme alır ve gerekli doğrulamanın ardından sertifikayı iptal eder. Bu iptal bilgisi OCSP sunucusuna hemen, SİL dosyasına ise en geç 24 saatte yansır.

4.9.6. Üçüncü Kişilerin Sertifika İptal Durumunu Kontrol Gerekliliği

Sertifika iptal durum kayıtları, kimlik doğrulaması gerektirmez ve herkesin erişimine ücretsiz olarak açıktır. Kamu SM, iptal durum kayıtlarına erişimin sürekliliğini sağlar.

Üçüncü kişiler, sertifikalara dayanarak işlem yapmadan önce sertifikaların geçerliliğini SİL ya da OCSP yöntemlerinden birini kullanarak kontrol etmekle yükümlüdür.

Üçüncü kişiler, sertifika geçerlilik kontrolünü yaptığı SİL dosyasının veya OCSP sunucusundan aldığı iptal durum kaydının Kamu SM'ye ait özel anahtarla imzalandığını kontrol eder. Üçüncü kişilerin yapması gereken geçerlilik kontrolleri Bölüm 9.6.4'te belirtilmiştir.

4.9.7. Sertifika İptal Listesi Yayımlama Sıklığı

Son kullanıcı sertifika iptal bilgisinin bulunduğu SİL günde en az 1 (bir) kere yayımlanır. Bu SİL'in geçerlilik süresi en fazla 36 (otuzaltı) saattir. Yenisi yayımlanmış olsa da SİL dosyası geçerlilik süresinin sonuna kadar geçerliliğini korur.

Kamu SM'ye ait alt kök sertifikalarının iptal bilgisinin bulunduğu SİL dosyası yılda en az 1 (bir) kere yayımlanır. Alt kök sertifikasının iptali durumunda SİL dosyası derhal yenilenir.

Kamu SM tarafından yayımlanan SİL dosyaları arşivlenir.

4.9.8. Sertifika İptal Listesi Yayımlama Gecikme Süresi

SİL, üretildiği andan itibaren en geç 10 (on) dakika içinde yayımlanır.

4.9.9. Çevrim İçi Sertifika İptal Durum Kontrol İmkanı

Kamu SM, SSL sertifikalarının iptal durum bilgisini OCSP üzerinden kesintisiz olarak yayımlar. OCSP desteği olan uygulamalar SSL sertifikasının iptal durum kontrolünü http://ocspssls1.kamusm.gov.tr adresi üzerinden, Kamu SM alt kök sertifikasının iptal durum kontrolünü ise http://ocspsslkoks1.kamusm.gov.tr adresi üzerinden sağlar.

4.9.10. Çevrim İçi Sertifika İptal Durum Kontrol Gereklilikleri

Üçüncü taraflar, bir sertifikaya güvenmeden önce Bölüm 4.9.6'da belirtilen esaslar doğrultusunda sertifikanın iptal kontrolünü yapmak durumundadır. Teknik imkanlar elveriyorsa sertifika iptal kontrolünün OCSP üstünden yapılması Kamu SM tarafından tavsiye edilen yöntemdir.

Kamu SM OCSP cevapları RFC 6069'a [X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP] uygun olarak HTTP üzerinden istek ve cevapları desteklemektedir. Kamu SM OCSP sunucuları müşteriler tarafından yapılan GET ve POST isteklerine cevap verebilmektedir. Kamu SM sisteminde var olmayan bir sertifika seri numarası için iptal sorgusu yapıldığında, OCSP sunucusu "UNKNOWN" cevabı dönmektedir.

4.9.11. Diğer Sertifika Durum Bildirim Yöntemleri

Kamu SM, SİL ve OCSP dışında iptal durum kaydı bildirim yöntemlerini uygulamamaktadır.

4.9.12. Özel Anahtarın Güvenliğini Yitirmesine İlişkin Özel Gereklilikler

Kamu SM kök veya alt kök sertifikasına ait özel anahtarın gizliliğinin veya güvenliğinin şüphe altında olması halinde bu anahtara bağlı Kamu SM sertifikası ve bu sertifika altındaki tüm sertifikalar iptal edilir ve bu durum sertifika sahiplerine en az e-posta yoluyla duyurulur.

Kamu SM, son kullanıcılara ait sertifikalarda güvenlik sorunu oluşması durumunda ilgili son kullanıcı sertifikasını iptal eder, sertifika sahibini bilgilendirir. Kamu SM kaynaklı tüm sertifika iptal işlemlerinde, iptal sonrası yeni sertifika üretim ve dağıtım işlemlerine en kısa sürede başlanır.

4.9.13. Sertifikanın Askıya Alındığı Durumlar

SSL sertifikaları için askı işlemi uygulanmamaktadır.

4.9.14. Sertifika Askıya Alma Başvurusunu Kimlerin Yapabildiği

Düzenlenmesine gerek duyulmamıştır.

4.9.15. Sertifika Askıya Alma Başvurusunun İşlenmesi

Düzenlenmesine gerek duyulmamıştır.

4.9.16. Askıda Kalma Süresi

Düzenlenmesine gerek duyulmamıştır.

4.10. Sertifika Durum Servisleri

Üçüncü kişiler, sertifika iptal durum kayıtlarına SİL ve OCSP aracılığıyla ulaşır.

4.10.1. İşletimsel Özellikler

Üçüncü kişiler, sertifika iptal durum kayıtlarına Kamu SM'nin yayımladığı SİL dosyalarından erişebilirler. SİL dosyalarına erişim bilgileri 2. Bölüm'de verilmiştir. Üçüncü kişiler, sertifikanın geçerlilik durumunu her kontrol etmek istediklerinde güncel SİL dosyasını Kamu SM bilgi deposundan kendi sistemlerine kopyalar ve gerekli kontrolleri yaparlar.

OCSP desteği olan üçüncü kişiler, sertifika iptal durumunu OCSP sunucudan öğrenebilirler. OCSP erişim adresi 2. Bölümde verilmiştir. Üçüncü kişiler sertifikanın geçerlilik durumunu her kontrol etmek istediklerinde, OCSP sunucusu üzerinden sorgulama yaparlar.

4.10.2. Servisin Erişilebilirliği

Kamu SM, SİL ve OCSP servislerini 7/24 kesintisiz olarak sunmak için gerekli tüm tedbirleri alır.

4.10.3. İsteğe Bağlı Özellikler

Düzenlenmesine gerek duyulmamıştır.

4.11. Sertifika Sahipliğinin Sona Ermesi

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 Yeniden Üretme

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

4.12.1. Anahtar Saklama ve Yeniden Oluşturma İlke ve Esasları

Düzenlenmesine gerek duyulmamıştır.

4.12.2. Oturum Anahtarı Zarflama ve Yeniden Oluşturma İlke ve Esasları

Düzenlenmesine gerek duyulmamıştır.

5. YÖNETİM, İŞLEMSEL VE FİZİKSEL KONTROLLER

Bu bölümde Kamu SM tarafından sertifika hizmeti verilirken yerine getirilmesi gereken teknik olmayan güvenlik kontrolleri anlatılmıştır.

5.1. Fiziksel Kontrol

Kamu SM sisteminin çalıştığı cihazların bulunduğu binalar ve odalar, giriş ve çıkışların kontrol edildiği, yetkisiz kişilerin girişini engelleyen güvenlik önlemleri ile donatılmıştır.

5.1.1. Tesis Yeri ve İnşaatı

Kamu SM sisteminin çalıştığı binanın bulunduğu mekan, yerleşim merkezinden uzak, yangın, su baskını, deprem, yıldırım ve hava kirliliğinden en az etkilenecek, giriş ve çıkışların kontrol edildiği bir bölgedir.

Bina, yüksek güvenlik gerektiren işlerin yapılmasına imkan sağlayan yapıdadır. Bina, esnek (çelik yapı) ve sert (çelik çatıyla desteklenmiş beton yapı veya desteklenmiş beton yapı) yapı şartlarını sağlamaktadır.

Kamu SM'nin kurulduğu yer ve binada güç kaynakları, haberleşme üniteleri, yedekli iklimlendirme üniteleri, gazlı yangın söndürme sistemleri, mevcut olup, deprem, su baskını ve afetlere karşı gerekli tedbirler alınmıştır.

5.1.2. Fiziksel Erişim

Kamu SM yazılım ve donanım sistemleriile arşivlere erişim denetim altındadır. Binaya girişler güvenlik görevlilerinin kontrolü altında, gelişmiş erişim kontrol cihazlarıyla sağlanmaktadır.

Bina içinde Kamu SM sistemine ait yazılım ve donanım araçlarının bulunduğu, elektronik veya kağıt ortamdaki bilgilerin tutulduğu, sistemin işletildiği ve yönetildiği odalara erişim biometrik kontroller yapangelişmiş erişim kontrol cihazlarıyla yapılmaktadır. Yetkisi olmayan kişiler sistemin kurulu olduğu odalara giriş yapamamaktadır. Yetkisiz kişilerin donanım bakımı veya bunun gibi sıra dışı bir amaçla sistemin kurulu olduğu odalara girişleri özel erişim talimatları uyarınca düzenlenir.

5.1.3. Güç Kaynağı ve Havalandırma

Aşağıdaki güç kaynakları Kamu SM işlevlerinin yerine getirilmesi ve sürekliliği için kullanılmaktadır:

- Güç alma ve devşirme (transformatör) birimleri
- Dağıtım paneli
- Trafo
- UPS
- Kuru akü
- Acil jeneratör

Bina aşırı ısınmayı önleyebilecek kapasitede ve uygun nem seviyesini ayarlayabilecek özelliklerde kesintisiz/yedekli iklimlendirme sistemleri ile donatılmıştır.

5.1.4. Su Baskınları

Kamu SM işlevlerinin yerine getirildiği ortamlarda su baskınlarından en az zarar görecek şekilde önlemler alınmıştır.

5.1.5. Yangın Önleme ve Korunma

Kamu SM sistem altyapılarının ve ofislerinin bulunduğu, operasyonun yerine getirildiği ortamlarda yangını önleyici ve olası yangınlarda zararı en aza indirecek önlemler alınmıştır.

5.1.6. Saklama ve Yedekleme Ortamlarının Korunması

Kullanılan veri saklama ortamları (disk, CD, kağıt vs.) bozulmaya, yıpranmaya karşı fiziksel ve elektronik olarak korunur. Buna ek olarak gerekli görülen ortamların yerinde yedeği alındığı gibi gerekli güvenlik kriterlerini sağlayan coğrafi olarak ayrı bir lokasyonda da yedekler alınmaktadır.

5.1.7. Atıkların Yok Edilmesi

Hassas bilgilerin bulunduğu ve kullanılmayan elektronik veya kağıt ortamda tutulan bilgiler geri dönüşümsüz olarak yok edilir.

5.1.8. Farklı Mekanlarda Yedekleme

Kamu SM, farklı mekanda yedekleme işi için coğrafi olarak tamamen ayrı, uzak bir felaket kurtarma merkezine sahiptir. Kamu SM, sisteminin sürekliliğini sağlayabilmek amacıyla gerekli gördüğü bileşenleri, farklı bir fiziksel mekanda güvenli kasalarda saklar. Yedek sistemin bulunduğu mekan, asıl sistemin sağladığı tüm güvenlik ve işlevsellik şartlarını sağlar. Yedekleme sunucu ve ortamlarına sadece yetkili personeller erişim sağlar.

5.2. Prosedürsel Kontroller

5.2.1. Güvenilir Roller

Kamu SM'de çalışan personelin rolleri CWA 14167-1 ve ETSI 101 456 standartlarına göre belirlenmiştir ve aşağıda belirtildiği şekilde sınıflandırılmıştır:

Kamu SM Yönetimi: Kamu SM'nin stratejik hedeflerinin gerçekleştirilmesi için gerekli tüm idari ve teknik faaliyetlerin yönetilmesinden sorumludur.

Güvenlik Personeli: Kamu SM güvenlik politikalarının uygulanmasından sorumludur.

Sistem Yöneticileri: Sertifika hizmetlerinin yürütülmesi için bilgi teknolojileri altyapısının yönetilmesinden sorumludur.

Sistem Operatörleri: Tüm sistem bileşenlerinin işletiminden, yedeklenmesinden ve kurtarma faaliyetlerinin yürütülmesinden sorumludur.

Sistem Denetçisi: Sertifika hizmetleriyle ilgili arşiv ve denetim kayıtlarının denetlenmesinden sorumludur.

Sertifika Kayıt Sorumlusu: Sertifika üretim ve iptaliyle ilgili kayıtları giren personeldir.

Sertifika Üretim Sorumlusu: Sertifika üretimini gerçekleştiren personeldir.

5.2.2. Her İşlem İçin Gereken Kişi Sayısı

Kamu SM, CA ve son kullanıcıya aitsertifikaların üretilmesi için birden fazla kişinin aynı anda hazır bulunmasını sağlar. Sertifika iptalleri için bölüm 4.9'da belirtilen şartların oluşması gerekmektedir. Bunun neticesinde CA sertifikasının iptali için birden fazla kişinin hazır bulunması gerekmektedir.

Kamu SM, CAözel anahtarlarının başka bir kriptografik modül içerisine yedeklenmesi için birden fazla kişinin aynı anda hazır bulunmasını sağlar.

5.2.3. Kimlik Doğrulama ve Yetkilendirme

Kamu SM işleyişinin her adımında, işlemleri yerine getirecek kişilerin kimlik tanımlaması ve doğrulaması yapılır. Böylece her sistem birimine sadece yetkili kişilerin erişimi sağlanır. Sistemdeki bazı birimlere erişim, farklı derecelerdeki yetkilendirme tanımlamalarıyla yapılır. Bu birimlere erişimin sağlanabilmesi için kimlik doğrulaması yapıldıktan sonra yetkilendirme tanımlamalarında verilen yetkiler çerçevesinde sistemde işlem yapılabilmektedir.

Kamu SM sistemi içinde kimlik doğrulama güvenli donanım araçları, parolalar, gizli sorular ve biyometrik veri kullanılarak güncel kriptografik yöntemlerle yapılır.

5.2.4. Görevlerin Ayrılmasını Gerektiren Roller

Güvenilir roller arasındaki görevler ayrılığı en az CWA 14167-1 standardını sağlayacak şekilde düzenlenir.

- Sertifika Üretim Sorumlusu ile Sertifika Kayıt Sorumlusu arasında,
- Sistem Denetçisi ile diğer roller arasında,
- Sistem Yöneticisi ile Güvenlik Personeli ve Sistem Denetçisi arasında

görevler ayrılığı vardır.

5.3. Personel Güvenlik Kontrolleri

5.3.1. Kişisel Geçmiş, Deneyim ve Nitelik Gerekleri

Çalışanlar sistemin işleyiş ve güvenlik gereklerini sağlayabilecek nitelikte, bilgili ve deneyimli kişilerden seçilir. Kamu SM'nin istihdam ettiği personel sistem güvenliği, veri tabanı yönetimi, elektronik imza teknolojileri ve uygulamaları, sertifika yönetimi ile ilgili konularda bilgi ve deneyimi olan nitelikli kişilerden oluşur.

5.3.2. Geçmiş Araştırması

Çalışanların Kamu SM'nin işletilmesinde güvenlik ihtiyaçlarının gerektirdiği güvenilirliğe sahip olması gerekmektedir. Personelin güvenilirliği geçmişine yönelik yapılan araştırmalar ile belirlenir. İşe alınmadan önce geçmişe yönelik yapılan araştırmalarda personelin herhangi bir sebepten dolayı hüküm giyip giymemiş olduğu araştırılır.

5.3.3. Eğitim Gerekleri

Çalışanlar Kamu SM'deki işlerine aktif olarak başlamadan önce gerekli eğitimden geçirilirler. Çalışanlara verilen eğitimde Kamu SM'de uygulanan güvenlik ilkeleri, sistemin teknik ve idari işleyişi, işleriyle ilgili süreçler, süreç içindeki görev ve sorumluluklar anlatılır.

5.3.4. Sürekli Eğitim Gerekleri ve Sıklığı

Kamu SM sisteminde yapılan değişikliklerin bildirilmesi amacıyla personele verilen eğitimler gerekli görüldükçe tekrarlanır. Yeni göreve başlayanlar için temel başlangıç eğitimi verilir.

5.3.5. Görev Değişim Sıklığı ve Sırası

Düzenlenmesine gerek duyulmamıştır.

5.3.6. Yetkisiz Eylemlerin Cezalandırılması

Kamu SM personelinin tamamen veya kısmen sahte elektronik sertifika oluşturması, geçerli olarak oluşturulan elektronik sertifikaları taklit veya tahrif etmesi, yetkisi olmadan elektronik sertifika oluşturması veya bu elektronik sertifikaları bilerek kullanması halinde ve diğer yetkisiz eylemlerde ilgili mevzuat gereğince işlem yapılır.

5.3.7. Anlaşmalı Personel Gereksinimleri

Kamu SM kendi personeli dışındaki kişilerle çalışmak durumunda olduğunda, bu kişilerle ilgili olarak, kendi personeline uyguladığı güvenlik kontrollerini yapar.

5.3.8. Sağlanan Dokümantasyon

Çalışanlara işleriyle ve süreçlerle ilgili gerekli kılavuz ve destek dokümanları sağlanır. Bunlar SUE ve Kamu SM'nin CA operasyonlarını yürütmesi için gerekli olan teknik ve operasyonel dokümanları içermektedir.

5.4. Denetim Kayıtları

Kamu SM işleyişi sırasında gerçekleştirilen anahtar ve sertifika yönetimi, sistemin güvenliği ile ilgili işlerin kayıtları tutulur. Tutulan kayıtların bir kısmı elektronik ortamda, diğer bir kısmı ise kağıt üzerindedir. Denetimler sırasında gerekli görüldüğü takdirde bu kayıtlar görevliler tarafından incelenir.

5.4.1. Kaydedilen İşlemler

Kamu SM sisteminde aşağıda yapılan işlemler ile ilgili elektronik veya kağıt ortamda yapılan işlerin kayıtları tutulur:

- Kamu SM anahtarlarının yaşam döngüsü yönetimi işlemleri
  - Anahtar üretimi
  - Anahtar yedekleme
  - Anahtar yok etme
  - Kriptografik modül yaşam döngüsü işlemleri
- Sertifika üretim ve iptal başvuruları
  - Başvuru sahibi tarafından sunulan belgelerin neler olduğu bilgisi
  - Başvuru sırasında alınan kimlik tanımlamaya yarayan belgeler

- Başvuru sırasında elektronik veya kağıt ortamda alınan form veya belgeler
- Kağıt belgelerin kopyalarının nerede saklandığı bilgisi
- Geçerli ve geçersiz alınan tüm başvuru bilgileri

- Sertifika yaşam döngüsü yönetimi işlemleri
  - Sertifika üretimi
  - Sertifika iptal etme
  - SİL yayımlanması
- Güvenlikle ilgili diğer işlemler
  - Sisteme başarılı veya başarısız tüm erişim denemeleri
  - Çalışanlar tarafından gerçekleştirilen güvenlik sistemi işlemleri
  - Güvenli tutulması gereken hassas dosyaların okunması, yazılması ve değiştirilmesi
  - Güvenlik profili değişiklikleri
  - Sistemin çökmesi, donanım hataları ve diğer bozukluklar
  - Güvenlik cihaz/yazılımişlemleri (Güvenlik Duvarları, IPS, HIDS, Router v.b.)
  - Kamu SM'ye ziyaretçi giriş ve çıkışı

Kayıtlarda kayıt zamanı ve kaydın oluşmasına sebep olan çalışanın ismi bulunur.

5.4.2. Kayıtların İncelenme Sıklığı

Sistemin işleyişiyle ilgili tutulan kayıtlar düzgün zaman aralıklarıyla incelenir. İncelemeler haftalık olarak yapılır ve herhangi bir güvenlik açığı oluşup oluşmadığı kontrol edilir. Buna ek olarak, sistemde olağandışı hareketlerin görülmesi ya da alarm durumlarında tutulan kayıtlar incelenir. Yapılan incelemeler sonucu gerek görülen ve başlatılan işlemler de belgelenir.

Sertifika başvurusu sırasında sertifika sahiplerinden gelen bilgilerin elektronik veya kağıt ortamda tutulan kayıtları, sertifika yaşam döngüsü süresi içinde gerek görüldükçe veya yasal işlemler sebebiyle incelenebilir.

5.4.3. Kayıtların Saklanma Süresi

Kayıtlar incelenmelerinden sonra, en az 2 (iki) ay sistemde tutulur. Ardından arşivlenir.

5.4.4. Kayıtların Korunması

Kamu SM'ye ait kayıtların elektronik ve fiziksel olarak güvenlik altında tutulması için aşağıdaki önlemler alınmıştır:

- Yetkisi olmayan kişiler elektronik kayıtların bulunduğu sistemlere erişemezler.
- Kağıt üzerindeki kayıtlar sadece yetkililerin girme izni bulunan kilitli odalarda bulunur.
- Kayıtların değiştirilmesine izin verilmez, bunun için gerekli güvenlik önlemleri alınmıştır.
- Elektronik olarak saklanan ve sistemin işleyişi açısından kritik olan kayıtlar, işlemi yapan personel tarafından gerektiğinde elektronik imza ile imzalanarak saklanır. Böylece kritik kayıtlarda oluşabilecek her değişiklik sistem tarafından fark edilir.
- Kritik bilgiler gerektiğinde Kamu SM'ye ait anahtarlarla şifreli olarak saklanır.

5.4.5. Kayıtların Yedeklenmesi

Sistemin kritikliği göz önüne alındığında her gün düzenli olarak, sistemin yoğun olarak kullanılmadığı bir saatte gerekli görülen kayıtların çevrim içi yedeği alınmaktadır. Yedekleme ihtiyacını gidermek üzere teyp kütüphanesi ve yedekleme işlemlerini otomatikleştirmek için yedekleme yönetim yazılımı mevcuttur. Kritik kayıtlar coğrafi olarak ayrı bir bir şehirde bulunan güvenli felaket kurtarma merkezlerine yedeklenmektedir.

5.4.6. Kayıtların Toplanması

Kayıtlar uygulama katmanında, ağ katmanında ve işletim sistemidüzeyinde otomatik olarak toplanır. Otomatik kayıt toplama işlemi sistemin başlamasından kapanmasına kadar çalışır.

5.4.7. Kayda Sebebiyet Veren Tarafın Bilgilendirilmesi

Kayıt oluşmasına sebep olan işlemi başlatan Kamu SM sistem kullanıcısı, kaydın yapıldığına dair sistem tarafından bilgilendirilir.

5.4.8. Saldırıya Açıklığın Değerlendirilmesi

Denetim kayıtlarının tutulduğu sistemler için Bölüm 6.5, 6.6 ve 6.7'de sözü geçen teknik güvenlik kontrolleri uygulanır.

Kamu SM periyodik olarak zaafiyet değerlendirmesi yapar ve bunları kayıt altına alır. Kayıt altına alınan zaafiyetler risk değerlendirme süreçlerine göre işlenir.

5.5. Kayıt Arşivleme

5.5.1. Arşivlenen Kayıt Bilgileri

Bölüm 5.4.1'de belirtilen kayıtlara ek olarak sertifika başvurusu ve sertifika yaşam döngüsüyle ilgili, elektronik olarak ya da kağıt üzerinde tutulan aşağıdaki belgeler arşivlenir:

- Sertifika sahibi kurum 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
- Sertifika İlkeleri dokümanı
- Sertifika Uygulama Esasları dokümanı
- Sertifika yönetim prosedürleri
- Sertifika Sahibi Taahhütnameleri

5.5.2. Arşivlerin Tutulma Süresi

Arşivlenen bilgiler ve belgeler en az 7 (yedi) yıl boyunca saklanır.

5.5.3. Arşivlerin Korunması

Arşivlenen bilgi ve belgeler izinsiz izlenmeyi, değiştirmeyi ve silinmeyi engelleyecek şekilde elektronik ve fiziksel olarak güvenli tutulur. Arşivler yetkisiz çalışanların erişimine kapalıdır. Arşivlerin tutulduğu ortam 5.5.2'de belirtilen süre boyunca arşivlerin zarar görmesini engelleyecek şekilde seçilir.

5.5.4. Arşivlerin Yedeklenmesi

Kritik bilgi içeren elektronik arşivler Kamu SM iş sürekliliği politikası gereğince yedeklenir.

5.5.5. Kayıtların Zaman Damgası Gereksinimleri

Kamu SM gerekli gördüğü kayıtlara zaman damgası ekler.

5.5.6. Arşivlerin Toplanması

Arşivler elektronik veya kağıt ortamda ilgili prosedürlere göre toplanır.

5.5.7. Arşiv Bilgilerinin Elde Edilme ve Doğrulanma Metodu

Arşiv bilgileri yetkili personelden edinilir. Aynı bilgiye ait birden fazla arşiv olması durumunda arşivler kıyaslanarak doğruluğu kontrol edilir.

5.6. Anahtar Değişimi

Kamu SM'ye ait anahtarlar ve sertifikalar geçerlilik süresinin dolması sebebiyle veya güvenlik gerekleriyle yenilenebilir. Kamu SM'ye ait sertifikanın kullanım süresinin dolmasından önce eski anahtar çiftinden yeni anahtar çiftine geçiş işlemleri yapılır. Anahtar değişimi işlemleri şunları gerektirir:

- Sertifika kullanım süresinin dolmasından en geç 3 (üç) yıl önce işlemler başlatılır. Eski anahtarlarla sertifika verilmesi durdurulur.
- Kamu SM'nin eski özel anahtarıyla imzalanmış sertifikaların doğrulanabilmesi için, eski Kamu SM sertifikası yayımlanmaya devam eder.
- SİL dosyası aynı Kamu SM özel anahtarıyla imzalanıyorsa, Kamu SM'nin eski özel anahtarıyla oluşturulmuş sertifikaların kullanım tarihleri dolana kadar, Kamu SM SİL'leri eski özel anahtarla imzalanmaya devam eder. Yeni üretilen sertifikalar için oluşturulan SİL dosyası yeni Kamu SM özel anahtarıyla imzalanır.
- Kamu SM anahtarlarının yenilendiği bilgisini http://www.kamusm.gov.tr internet adresi üzerinden duyurur ve sertifika hizmeti verdiği kurumları bilgilendirir.

5.7. Güvenilirliğin Yitirilmesi ve Arıza Durumlarında Yapılacaklar

5.7.1. Güvenilirliğin Yitirilmesi Durumunun Düzeltilmesi

Güvenilirliğin yitirilmesi durumlarında(olay veya güvenlik zayıflığı v.b.), sertifika yönetim sisteminin en kısa zamanda yeniden güvenilir olarak çalışmaya başlaması, durumdan etkilenen tarafların haberdar edilmesi ve zararlarının en aza indirgenmesi için belirlenen süreçler işletilir.

5.7.2. Donanım, Yazılım veya Veri Bozulması

Kamu SM, donanım, yazılım veya veri operasyonlarının gizliliğinin ihlal edildiğini tespit etmesi halinde olayın genişliğini ve etkilenen taraflar için sunulmuş riskleri soruşturur.

Donanım, yazılım veya veri bozulması durumları raporlanır ve arızanın/hatanın giderilmesi için gerekli süreç başlatılır.

İş sürekliliğini sağlamak için sistemde kullanılacak aktif cihazlar, sunucular ve depolama alan ağı bileşenleri yedekli yapıda çalışmaktadır. Depolama ünitesi fiziksel olarak farkı bir noktada bulunan veri depolama ünitesi ile veri senkronizasyonu yapabilecek niteliktedir. Arızanın giderilmesi süreci arıza sebebinin araştırılmasını, hatanın giderilmesini ve gerekli görüldüğünde Kamu SM hizmetlerini güvenilir yedek ortama aktarmayı içerir.

5.7.3. Özel Anahtarın Gizliliğini Kaybetmesi

Kamu SM'nin sertifika imzalamada kullandığı özel anahtarın gizliliğinin kaybedildiğinden şüphelenilmesi ya da bunun öğrenilmesi durumunda ilgili sertifika en kısa zamanda iptal edilir ve aşağıdaki işlemler yerine getirilir:

- Kamu SM kendisine ait sertifikanın iptal edildiğini, iptal sebebi ile birlikte en hızlı şekilde http://www.kamusm.gov.tr internet adresi üzerinden duyurur ve ilgili kurumları yazıyla bilgilendirir.
- Kamu SM, sertifika sahiplerinin durumdan ne şekilde etkileneceğini belirten açıklamayı yapar, eski özel anahtarıyla imzalanan sertifikalara güvenilmemesi için ilgili taraflara ihtarda bulunur.
- Kamu SM, kendisine ait sertifikanın iptal edildiği bilgisini yayımladığı SİL dosyasında belirtir.
- Kamu SM tarafından üretilen sertifikaların gerekli görülen bir kısmı veya hepsi iptal edilir. İptal bilgisi sertifika sahiplerine en kısa zamanda bildirilir.
- Kamu SM sertifika isteklerine yanıt vermeyi durdurur.
- İlgili taraflar Kamu SM'nin durumuyla ilgili sürekli bilgilendirilir.
- Kamu SM, özel anahtarın yok edilmesi sürecini işletir.
- Kamu SM, yeni bir anahtar çifti ve sertifika üreterek yeni sertifikayı taraflara bildirir.
- Kamu SM anahtarının yenilenmesiyle, iptal edilen sertifikaların yerine, kullanıcıdan gelen talep doğrultusunda, yenilerinin üretilmesi süreci başlatılır.

5.7.4. Arıza Sonrası Yeniden Çalışırlık

Kamu SM, arıza ya da afet sonrası sistemin en kısa zamanda yeniden ve güvenli olarak çalışmaya başlaması için gerekli yöntemleri ve süreçleri Kamu SM İş Sürekliliği Planı'nda tanımlar.

Kamu SM başka bir şehirde felaket kurtarma merkezine sahiptir. İş sürekliliğinin devamı için Kamu SM merkez ofiste saklanan verilerin yedekleri felaket kurtarma merkezinde de saklanmaktadır.

Kamu SM, arıza sonrası yeniden çalışırlığı sağlayacak Kamu SM İş Sürekliliği Planı'nı periyodik olarak gözden geçirir ve test eder.

5.8. Sertifika Hizmetlerinin Sonlandırılması

Kamu SM, bir sebeple işleyişine son vereceği zaman aşağıdaki işlemleri yerine getirir:

- Sertifika hizmetlerine son vereceği tarihten en az 3 (üç) ay önce durumu sertifika hizmeti verdiği kurumlara yazı ve/veya e-posta ile duyurur.
- Sertifika hizmetlerine son vereceği bilgisini internet sitesi üzerinden ve ulusal yayın yapan en yüksek tirajlı 3 (üç) gazetede ilan vermek suretiyle kamuoyuna duyurur.
- Sertifika hizmetlerine son vereceğini duyurmasından itibaren sertifika başvurusu kabul etmez ve yeni sertifika oluşturmaz.
- Dağıttığı sertifikaları iptal eder, iptal bilgisini SİL ve OCSP aracılığıyla üçüncü kişilere duyurur. İptal ettiği sertifikaların bilgisini sertifika sahiplerine e-posta ile ve/veya yazılı olarak duyurur.
- İptal ettiği sertifikaların kullanım süreleri dolana kadar en son ürettiği SİL dosyasını yayımlamaya devam eder.
- SİL dosyasını imzalamada kullandığı özel anahtara karşılık gelen sertifikasını, SİL dosyasının geçerlilik süresi boyunca yayımlamaya devam eder.
- Sertifikaları imzalamak için kullandığı özel anahtarı imha eder.
- İlgili tüm kayıtları ve arşivleri uygun bir şekilde en az 7 (yedi) yıl boyunca korur.

6. TEKNİK GÜVENLİK KONTROLLERİ

Kamu SM'nin kendi anahtar çiftleri ve erişim verilerini ürettiği, tüm sertifika yönetim işlemlerini gerçekleştirdiği sistemler CWA 14167-1, ETSI TS 102 042 ve CAB Forum Baseline Requirements gereklerini sağlar.

6.1. Anahtar Çifti Üretimi ve Kurulumu

6.1.1. Anahtar Çifti Üretimi

Kök ve alt kök makamlara ait anahtar çiftleri, yetkisi olmayan personelin giremeyeceği güvenli odada, birden fazla eğitimli personelin gözetiminde, ağ ortamına kapalı sistemlerde, güvenli anahtar üretimi için gereken testlerden geçmiş, FIPS-140 veya EAL4+ standartlarını sağlayan güvenli yazılım ve/veya donanım kullanılarak üretilir. Üretilen özel anahtar güvenli kriptografik modül içinde saklanır. Modül güvenli odadan dışarıya çıkarılmaz. Yapılan bütün işlemler kayıt altına alınır ve işlemi gerçekleştiren personel tarafından onaylanır.

Anahtar çiftlerinin üretimleri sırasında ETSI TS 102 042 ve Baseline Requirements dokümanlarının gereklilikleri yerine getirilir.

SSL sertifikaları için anahtar çifti üretimi sertifika talep eden tarafça gerçekleştirilir, Kamu SM son kullanıcı için PKCS#12 dosyası üretmez.

Özel anahtarın saklandığı kriptografik modül Bölüm 6.2.1'de belirtilen standartlara uyar.

6.1.2. Sertifika Sahibine Özel Anahtarın Ulaştırılması

SSL sertifikaları için anahtar çifti üretimi sertifika talep eden tarafından gerçekleştirildiğinden özel anahtarın sahibine ulaştırılması söz konusu değildir.

6.1.3. İmza Doğrulama Verisinin ESHS'ye Ulaştırılması

SSL sertifikası başvuru sahibi, başvurusunun kabul edilmesi sonrasında açık anahtarını PKCS#10 formatında sertifika imzalama isteği olarak kurumsal e-postasını kullanarak Kamu SM'ye ulaştırır.

6.1.4. Kamu SM İmza Doğrulama Verilerinin Taraflara Ulaştırılması

Kamu SM'ye ait kök ve alt kök sertifikaları Kamu SM bilgi deposu üzerinden yayımlanır. Ayrıca tarayıcılara tanıtılmış durumdadır.

6.1.5. Anahtar Uzunlukları

Kamu SM'ye ait kök ve alt köklerin RSA anahtar boyları 2048 bittir. OCSP cevaplarını imzalayan RSA anahtarının boyu 2048 bittir. Kamu SM tarafından üretilen SSL sertifikalarının RSA anahtar boyu 2048 bittir.

6.1.6. Anahtar Üretim Parametreleri ve Kalitesinin Kontrolü

Kamu SM anahtar üretiminde RSA with SHA-256 algoritması kullanmaktadır ve CAB Forum Baseline Requirements Bölüm 6.1.6'da RSA algoritması için belirtilen özelliklere uygun olarak anahtar üretimi gerçekleştirmektedir.

6.1.7. Anahtar Kullanım Amaçları

Kamu SM tarafından oluşturulan anahtarların hangi amaçlar için kullanılabileceği sertifikadaki "Anahtar Kullanımı" ve "Genişletilmiş Anahtar Kullanımı" uzantısı içerisinde belirtilir.

Kök ve alt kök anahtarları sertifika ve SİL imzalamak için kullanılır. Kamu SM OCSP sertifikaları OCSP cevaplarını imzalamak için kullanılır. SSL anahtarları kimlik doğrulama ve şifreleme için kullanılır.

Kamu SM SSL sertifikalarının imzalanmasında kullanılan Sertifika zinciri Ek-A'da detaylı olarak bulunmaktadır.

6.2. Özel Anahtarın Korunması

6.2.1. Kriptografik Modül Standartları ve Kontroller

Kamu SM'ye ait özel anahtarlar güvenli donanım ve/veya yazılımlar kullanılarak üretilir, güvenli kriptografik modül içinde saklanır ve asla bu modül dışına çıkmaz.

Kriptografik modül aşağıda belirlenen güvenlik işlevlerine sahiptir:

- Özel anahtarın geçerlilik süresi boyunca gizlilik ve bütünlüğünü sağlar.
- Modüle erişimde kimlik belirleme ve doğrulama işlevlerini yerine getirir.
- Erişim yetkisi birden fazla yetkili kişinin kontrolünde olacak şekilde tanımlanabilir.
- Kullanıcıya tanımlanan roller doğrultusunda verdiği hizmetlere erişimi sınırlar.
- Modüle izinsiz erişim ve kullanım ile tahrifata yol açabilecek her türlü fiziksel önlem alınmıştır.
- Yetkisiz erişime teşebbüs edilmesi durumunda modül, içindeki veriyi siler.
- Özel anahtarın yedeğinin güvenli biçimde alınmasına olanak verir.
- Kriptografik modül şu güvenlik standartlarından en azından birisini sağlar: FIPS 140-1, 140-2 or 140-3 seviye 3 veya üzeri.

6.2.2. Özel Anahtara Birden Fazla Kişi Kontrolünde Erişim

Kamu SM'ye ait özel anahtarın bulunduğu odaya erişim, en az 2 (iki) farklı personelin birlikte bulunmasıyla ve görevler ayrılığı prensibine riayet edilerek sağlanmaktadır. Yetkili kişiler dışında erişim gerekli kontroller vasıtasıyla engellenir.

6.2.3. Özel Anahtarın Yeniden Elde Edilmesi

Düzenlenmesine gerek duyulmamıştır.

6.2.4. Özel Anahtarın Yedeklenmesi

Kamu SM'ye ait özel anahtarların yedeğinin alınması birden fazla yetkili personel tarafından yapılır. Yedekleme işlemi hazırda kullanılmakta olan özel anahtar için sağlanan güvenlik ile eşdeğer güvenlik önlemleri altında yapılır. Yedeklenen özel anahtar yetkisiz kişilerin erişimine kapalı, fiziksel ve elektronik olarak güvenli kriptografik donanım cihazı içinde tutulur. Bu güvenli donanım cihazı aktif kullanılmakta olan özel anahtarın bulunduğu ortam ile aynı güvenlik şartlarına sahip ortamda saklanır.

Sertifika sahiplerine ait özel anahtarlar Kamu SM'de bulunmaz.

6.2.5. Özel Anahtarın Arşivlenmesi

Kamu SM'ye ait özel anahtarlar arşivlenmez.

6.2.6. Özel Anahtarın Kriptografik Modüle/Modülden Taşınması

Taşıma işlemi, güvenilir yöntemlerle şifreli olarak ve birden fazla yetkili personelin denetiminde yerine getirilir.

6.2.7. Özel Anahtarın Kriptografik Modülde Saklanması

Kamu SM'ye ait özel anahtarlar, yetkisiz kişilerin erişimine kapalı, FIPS 140 Seviye 3 sertifikasına sahip güvenli kriptografik donanım cihazı içinde tutulur. Özel anahtarın yedekleme amacı haricinde cihaz dışına çıkması engellenmiştir. Özel anahtar kriptografik modül içinde güvenli algoritma ve yöntemlerle şifreli olarak saklanır.

6.2.8. Özel Anahtarın Aktive Edilmesi

Kamu SM özel anahtarının aktive edilmesi birden fazla yetkili personelin ortak denetimi altında gerçekleştirilir. Özel anahtarın bulunduğu odaya giriş için, tanımlanan personelin aynı anda hazır bulunması ve elektronik olarak kimliklerinin ve yetkilerinin doğrulanması gerekir. Yeterli sayıda yetkili personelin hazır bulunmadığı ve kimliklerinin doğrulanamadığı durumlarda özel anahtarın bulunduğu odaya erişim sağlanamaz.

Özel anahtar kriptografik modül içinde şifreli durumdayken aktif durumda değildir. Aktifleştirilmesi için gerekli verinin modüle sunulması gerekir.

6.2.9. Özel Anahtarın Deaktive Edilmesi

Kamu SM'nin özel anahtarı kullanıldıktan sonra oturum kapandığında anahtara erişim otomatik olarak kesilir ve bir dahaki kullanıma kadar erişime kapalı tutulur. Anahtarın tekrar aktifleştirilmesi için Bölüm 6.2.8'de belirtilen yöntemin yeniden işletilmesi gerekir.

6.2.10. Özel Anahtarın Yok Edilmesi

Kamu SM'ye ait özel anahtar, kullanım süresinin dolmasının ardından, bütün yedekleriyle birlikte uygun yöntemlerle geri dönüşsüz şekilde silinir ve bu işlemler kayıt altına alınır. Kamu SM'ye ait özel anahtarın silinmesi işlemi için Bölüm 6.2.8'de belirtilen şekilde yeterli sayıda yetkili personelin aynı anda hazır bulunması gerekir.

6.2.11. Kriptografik Modülün Değerlendirilmesi

Kamu SM, bölüm 6.2.1 de belirtilen standartlara uygun kriptografik modül kullanır.

6.3. Anahtar Çifti Yönetimiyle İlgili Diğer Konular

6.3.1. Açık Anahtarın Arşivlenmesi

Özel anahtarın kullanım süresi, sertifikanın içeriğinde belirtilen kullanım süresi kadardır. Sertifikanın kullanım süresinin dolmasıyla ya da sertifikanın iptal edilmesiyle özel anahtarın kullanımı sona erer. Kamu SM'ye ve sertifika sahibine ait anahtar çiftlerinin kullanım süresi, anahtar uzunlukları ve kullanılan kripto algoritmasına göre belirlenir. Son kullanıcı sertifikaları 1 (bir), 2 (iki) veya 3 (üç) yıllık olabilir. Kamu SM'ye ait anahtar çiftlerinin geçerlilik süresi 30 (otuz) yılı aşamaz.

6.3.2. Anahtarların Kullanım Süreleri

Özel anahtarın kullanım süresi, sertifikanın içeriğinde belirtilen kullanım süresi kadardır. Sertifikanın kullanım süresinin dolmasıyla ya da sertifikanın iptal edilmesiyle özel anahtarın kullanımı sona erer. Kamu SM'ye ve sertifika sahibine ait anahtar çiftlerinin kullanım süresi, anahtar uzunlukları ve kullanılan kripto algoritmasına göre belirlenir. Son kullanıcı sertifikaları 1 (bir), 2 (iki) veya 3 (üç) yıllık olabilir. Kamu SM'ye ait anahtar çiftlerinin geçerlilik süresi 30 (otuz) yılı aşamaz.

6.4. Erişim Verileri

6.4.1. Erişim Verilerinin Oluşturulması ve Yüklenmesi

Kamu SM sistemi içinde kullanılan erişim verileri gerekli karmaşıklık gereksinimlerine sahip, yetkisiz kişilerin erişimine kapalı, fiziksel ve elektronik olarak güvenli ortamlarda üretilir.

Erişim verileri kriptografik modülün özelliklerine uygun olarak oluşturulur. Kamu SM'nin kullandığı kriptografik modüller en az FIPS 140-2 uyumludur.

6.4.2. Erişim Verilerinin Korunması

Kamu SM'de kullanılan erişim verileri yalnızca yetkili personel tarafından kullanılır. Bu verilerin korunmasında Kamu SM veri koruma politikaları doğrultusunda gerekli tedbirler alınır.

6.4.3. Erişim Verileri İle İlgili Diğer Konular

Düzenlenmesine gerek duyulmamıştır.

6.5. Bilgisayar Güvenliği Denetimleri

6.5.1. Bilgisayar Güvenliği İle İlgili Teknik Gerekler

Kamu SM'de kötü niyetli yazılımlara karşı gereken önlemler alınır. Sistemde ağ ve sunucu bazlı sensörler içeren saldırı tespit sistemi bulunmaktadır. Bütün sunucular üzerinde merkezden yönetilebilen virüs tespit ve temizleme ajanları kurulmuştur ve bunlar sürekli güncel tutulmaktadır. Kritik işlemlerin yapıldığı bilgisayarlar ağ ortamı dışında tutulur. Bilgilerinin tahrifata, silinmeye ve kaçağa karşı korunması ve işletimin sürekliliğinin sağlanması için gerekli güvenlik tedbirleri alınır. Her kurulan yazılımın yedek kopyası yaratılır ve sistemin güvenliği konusunda bütün iyileştirme eylemleri gecikmesiz uygulanır.

Kamu SM sistem altyapısında görevler ayrılığı prensibine aykırı düşecek yetkilendirmeler yapılmaz. Bu doğrultuda periyodik erişim gözden geçirme faaliyetleri yapılır. Sertifika yaşam döngüsüyle doğrudan ya da dolaylı ilişkili tüm sistemler için gerekli loglama faaliyetleri gerçekleştirilir.

6.5.2. Bilgisayar Sisteminin Sağladığı Güvenlik Seviyesi

Düzenlenmesine gerek duyulmamıştır.

6.6. Yaşam Döngüsü Teknik Kontrolleri

6.6.1. Sistem Geliştirme Kontrolleri

Sistem geliştirilirken gerçekleştirilen kontroller aşağıda verilmiştir:

- Yeterli düzeyde kalite ve güvenlik tedbirleri alınır.

- Belirlenen güvenlik kriterlerine uygun personel çalıştırılır.
- Her kurulan yazılımın yedek kopyası yaratılır.
- Sertifika işlemlerinin sürekliliğini sağlamak için sistem bilgilerini tutan bileşenlerin yedekleri oluşturulur.
- Sistemin açık ağa bağlantısında gerekli güvenlik önlemleri alınır.
- Kurulum sırasında dışarıdan gelen yazılımlar kullanılmadan önce virüs taramasından geçirilir ve resmi olmayan yazılımların sisteme girmesi engellenir. Bu konuda tüm güvenlik gerekleri yerine getirilir, bütün iyileştirme eylemleri gecikmesiz uygulanır.
- Anormal sistem koşullarını yakalamak için ilk dönemlerde sistem durumları yakından gözlemlenir.
- Geliştirilmekte olan sisteme erişim kimlik, parola gibi tanıtıcı bilgilerin doğrulanmasıyla yapılır.
- Sistemin geliştirilmesi sırasında yapılan denetimler ISO 27001'in güncel sürümünün gereklerini sağlar.
- Geliştirme faaliyetleri sırasında geliştirme, test ve canlı sistemler ayrılır. Canlıya alınma işlemi onay mekanizmalarından sonra gerçekleştirilir.
- Sistem bileşenlerine dair periyodik risk değerlendirmeleri yapılır ve yönetime sunulur.
- Sistemlerde gerçekleştirilen değişiklikler kayıt altına alınır ve izlenir.
- Uzaktan erişim dahil üçüncü tarafların sistemlere erişimine izin verilmez.
- Herhangi bir danışmanlık ya da ürün alınması gereken durumda tedarikçinin seçimi daha önceki referanslarına ve tedarikçinin iş bitirme kabiliyetine göre yapılır.

6.6.2. Güvenlik Yönetimi Kontrolleri

Sistem içinde kurulu olan yazılım ve donanım ürünleri ile ağ ortamının işleyişinin planlanan şekilde güvenli olarak sürdürüldüğünü göstermek için periyodik olarak güvenlik denetimleri yapılır. Kamu SM içinde güvenliğe uygun olmayan hareketler ve yetkilendirmeler denetleme sonucunda açıklanır ve düzeltici önlemler alınır. Güvenlik kontrolleri için temel dayanak ISO 27001'in güncel sürümüdür.

6.6.3. Yaşam Döngüsü Güvenlik Denetimleri

Düzenlenmesine gerek duyulmamıştır.

6.7. Ağ Güvenliği Kontrolleri

Son teknolojik gelişmeler göz önünde bulundurularak gerekli ağ güvenliği kontrolleri yapılır. Sistem, dış açık ağa bağlantısında saldırı engelleme özellikli yeni nesil güvenlik duvarları kullanır. Sistemdeki sunucu ve aktif cihazların durum ve performanslarını izlemek, geçmişe yönelik performans raporları çıkarmak ve geleceğe yönelik performans eğilimlerini saptamak amacı ile ağ ve sistem yönetimi altyapıları mevcuttur.

Sunucular üzerine ağ ve sistem yönetimi ve güvenliği ajanları kurulmuştur. Yönetim yazılımı bu ajanlardan disk, hafıza, işlemci kullanımı, dosya bütünlüğü, güvenlik log kayıtları, harici depolama üniteleri takibi vb. bilgileri çeker ve bu bilgileri gerçek zamanlı görüntüler. Sunucuların çalışması için

önem arz eden kaynaklar için eşik değerler belirlenir ve bu eşik değerlerin aşılması durumunda sistem yöneticisi otomatik olarak uyarılır. Ağ ve sistem yönetimi ve güvenliği altyapısı çektiği bilgileri merkezi bir veri tabanında saklar. Böylece herhangi bir anda verilerin sorgulanmasına ve geçmişe dönük rapor üretilmesine imkan tanınır.

Yüksek güvenlik gerektiren işlemlerin yapıldığı sistemler (kök ve alt kök sunucuları gibi) için farklı ağ segmentleri oluşturulmuştur. Kritik işlemlerin yapıldığı sistemler ağa bağlı değildir.

Sistemlerdeki ayrıcalıklı erişim hesaplarına yetkiler güvenlik ekibince kontrollü olarak verilir ve loglar üzerinden izlenir.

Ağ ve sistem güvenliğine dair tüm işlemler siber olaylara müdahale ekibi tarafından izlenir ve gerektiğinde olay müdahele süreçleri doğrultusunda aksiyon alınır.

Sistemler üzerinde periyodik olarak zaafiyet taramaları ve yılda en az bir kez penetrasyon testi yapılır.

6.8. Zaman Damgası

Kamu SM sistem ve servislerinin gizlilik, bütünlük ve erişilebilirliğine dair tutulan elektronik kayıtlar zaman damgalı olarak saklanır.

7. SERTİFİKA, SERTİFİKA İPTAL LİSTESİ VE OCSP PROFİLLERİ

Bu bölümde Kamu SM tarafından üretilen sertifikalar ile SİL'lerin profilleri ve verilen OCSP hizmetinin yapısı anlatılmaktadır.

7.1. Sertifika Profilleri

Bu bölümde Kamu SM tarafından oluşturulan kök, alt kök ve SSL sertifikaların içeriği anlatılmaktadır.

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" ve "CA/Browser Forum Baseline Requirements (BR) for the Issuance and Management of Publicly-Trusted Certificates" dokümanlarının güncel sürümlerine uygun olarak sertifika oluşturur. Sertifika seri numaraları 64 bit entropi kullanılarak oluşturulmaktadır.

Kamu SM tarafından oluşturulan kök, alt kök ve SSL sertifikalarının içeriği EK-A'da bulunmaktadır.

7.1.1. Sürüm Numarası

Kamu SM, IETF RFC 5280 uyarınca X.509 v3 sertifika standardını destekler.

7.1.2. Sertifika Uzantıları

Kamu SM tarafından üretilen sertifikalar IETF RFC 5280 uyarınca zorunlu alanların yanı sıra X.509 v.3 sertifika uzantılarını da içerir. Sertifikanın içeriğinde bulunan sertifika uzantıları sertifikanın kullanılacağı uygulamanın gereklerine bağlı olarak belirlenir.

Kamu SM tarafından oluşturulan kök, alt kök ve SSL sertifikalarının içeriği detaylı olarak EK-A'da belirtilmiştir.

Uzantılardan bazıları kritik olarak tanımlanmıştır. Kritik olarak belirtilen uzantıların sertifikayı kullanan uygulama tarafından tanımlanamaması durumunda sertifikanın kullanılmaması gerekir.

7.1.3. Algoritma Nesne Tanımlayıcıları

Kamu SM tarafından oluşturulan tüm sertifikaların imzalanmasında SHA-256 with RSA algoritması (OID = {1 2 840 113549 1 1 11}) kullanılır.

Kamu SM OCSP cevaplarının imzalanmasında da SHA-256 with RSA algoritması kullanmaktadır.

7.1.4. İsim Biçimleri

Kamu SM tarafından üretilen sertifikalardaki isim biçimleri Bölüm 3.1.1'de belirtilmiştir. Kamu SM tarafından oluşturulan kök, alt kök ve SSL sertifikalarının isim biçimleri EK-A'da bulunmaktadır. Kamu SM IP adreslerine, sanal sunucu isimlerine veya iç sunucu adreslerine sertifika vermemektedir.

7.1.5. İsim Kısıtları

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.

7.1.6. Sertifika İlkeleri Nesne Tanımlayıcısı

Kamu SM tarafından oluşturulan her sertifika içeriğinde, o sertifikanın hangi sertifika ilkelerine göre kullanılacağını belirtmek amacıyla, ilgili sertifika ilkesine ait nesne tanımlayıcısı bulunmaktadır. Kamu SM tarafından üretilen SSL sertifikalarında Bölüm 1.2'de belirtilen OID kullanılır. Kamu SM tarafından oluşturulan sertifikaların Sertifika İlkeleri Nesne Tanımlayıcıları EK-A'da ilgili sertifikalar altında bulunmaktadır.

7.1.7. İlke Kısıtları Uzantısının Kullanımı

Düzenlenmesine gerek duyulmamıştır.

7.1.8. İlke Niteleyicilerin Yazımı ve Anlamı

Kamu SM tarafından oluşturulan SSL sertifikalarında "Sertifika İlkeleri" uzantısı içeriğinde OID olarak Bölüm 1.2'de belirtilen OID ve ilke niteleyici olarak http://depo.kamusm.gov.tr/ilke yer alır. Kamu SM tarafından oluşturulan sertifikaların Sertifika İlke Niteleyicileri EK-A'da ilgili sertifikalar altında bulunmaktadır.

7.1.9. Kritik Sertifika İlkeleri Uzantısının İşlenme Semantiği

Düzenlenmesine gerek duyulmamıştır.

7.2. SİL Profili

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 yayımlayıcı 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.

7.2.1. Sürüm Numarası

Kamu SM'nin ürettiği SİL'ler IETF RFC 5280 uyarınca X.509 v.2 formatına uygundur.

7.2.2. SİL ve SİL Kayıt Uzantıları

Kamu SM tarafından üretilen SİL'lerde IETF RFC 5280'de tanımlanan uzantılar kullanılır.

Uzantı	Değer
SİL Numarası	Artan tamsayı
Otorite Anahtar Tanımlayıcısı	SİL'i imzalayan SM'nin sertifikasındaki Konu Anahtar Tanımlayıcısı
Sebep Kodu	İptal sebebi

7.3. OCSP Profili

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

7.3.1. Sürüm Numarası

Kamu SM tarafından verilen OCSP hizmeti IETF RFC 6960 dokümanına göre V.1'i destekler.

7.3.2. OCSP Uzantıları

Kamu SM tarafından verilen OCSP hizmetinde IETF RFC 6960'da belirtilen şekilde uzantılar kullanılabilir.

8. UYGUNLUK DENETİMLERİ VE DİĞER DEĞERLENDİRMELER

Bu bölümde Kamu SM'nin Sİ/SUE dokümanına uygunluğunun denetlenmesi ile ilgili bilgilendirme yapılmaktadır.

8.1. Uygunluk Denetiminin Sıklığı

Kamu SM'nin bu Sİ/SUE dokümanında belirtilen şartları sağlayıp sağlamadığı yılda en az bir kez olmak üzere denetlenir.

Bu denetimler, Türkiye Cumhuriyeti'nin ESHS'ler için kanunla yetkilendirdiği resmi denetim otoritesi olan Bilgi Teknolojileri ve İletişim Kurumu'nun yaptığı ETSI TS 102 042 ve CAB Forum Baseline Requirements kapsamlı dış denetimler, ISO 27001 kapsamında yapılan BGYS denetimleri ve güvenilir personel tarafından yapılan iç denetimlerden oluşur.

Bu denetimlerin kapsamı OV SSL ile sınırlıdır.

8.2. Denetçinin Nitelikleri

Bilgi Teknolojileri ve İletişim Kurumu tarafından yapılan ETSI TS 102 042 ve CAB Forum Baseline Requirements kapsamlı dış denetim, resmi görevlendirme yazılarıyla ve her sene yapılır.

Denetçiler, açık anahtar altyapı teknolojisi, bilgi güvenliği ve teknolojisi ve bilgi sistemleri denetimi konusunda yetkin kişilerdir.

Denetçiler, denetimlerini bağımsız bir şekilde gerçekleştirir.

ISO 27001 denetimleri için denetçide baş denetçi sertifikası şartı aranır.

8.3. Denetçinin Denetlenen Tarafla Olan İlişkisi

Denetçiler, herhangi bir çıkar çatışması olmaması ve bağımsızlığın zedelenmemesi için Kamu SM'den bağımsız kişilerden oluşur.

8.4. Denetimin Kapsamı

Denetimlerde, sertifika yönetim süreçlerini anlatan sertifika yönetim prosedürlerinin, Kamu SM'nin iç işleyişindeki güvenlik ve işlevsel süreçlerin incelenerek, işleyişin Sİ/SUE dokümanına uygunluğu denetlenir.

Bu kapsamda;

- Anahtar ve sertifika yaşam döngüsü süreçleri,
- ESHS sistemsel ve çevresel güvenlik kontrolleri,
- Süreçlerin dökümanlara uygun işletimi,
- Personel yetkinlikleri,
- Görevler ayrılığı prensiplerine uygunluklar,
- Sİ/SUE, ISO 27001, ETSI TS 102 042 ve CAB Forum Baseline Requirements'e uygunluk

denetlenir.

8.5. Eksikliğin Tespiti Durumunda Yapılacaklar

Denetim sırasında Kamu SM'nin, Sİ/SUE dokümanının gereklerini yerine getirmediğinin tespit edilmesi durumunda, denetçi hangi süreçlerdeki aşamaların uygunsuz olduğunu yazdığı raporla ilgililere bildirir. Kamu SM yönetiminin önderliğinde yetersizliği tespit edilen durumların giderilmesi için yapılacak işlemler belirlenir ve yetersizliğin giderilmesi için çalışma başlatılır.

Denetimde, sistemin kurulum, işletim veya bakım aşamaları sırasında, Sİ/SUE dokümanının gereklerinin yerine getirilmediğinin tespit edilmesi durumunda aşağıdaki işlemler gerçekleştirilir:

- Denetçi hangi süreçlerdeki aşamaların uygunsuz olduğunu not eder ve ilgili paydaşları bilgilendirir.
- Kamu SM denetim sonucu tespit edilen yetersizliklerini Sİ/SUE dokümanında belirtilen uygulama esaslarına uygun olarak giderir.
- Sertifika yönetimiyle ilgili kritik bulunan işlemlerde yetersizliğin tespit edilmesi durumunda, Kamu SM ilgili işlemleri düzeltmeler yapılıncaya kadar durdurur.

Ayrıca, Kamu SM personelinin tamamen veya kısmen kötü niyetli elektronik sertifika oluşturması, geçerli olarak oluşturulan elektronik sertifikaları taklit veya tahrif etmesi, yetkisi olmadan elektronik sertifika oluşturması veya bu elektronik sertifikaları bilerek kullanması halinde ve diğer yetkisiz eylemlerde ilgili mevzuat gereğince işlem yapar.

8.6. Sonucun Bildirilmesi

Denetim sonuçları rapor olarak Kamu SM yönetimine bildirilir. Kamu SM yönetimi raporda belirtilen uygunsuzlukların en kısa zamanda düzeltilmesini sağlar.

9. DİĞER İŞLER VE HUKUKSAL MESELELER

9.1. Ücretlendirme

9.1.1. Sertifika Oluşturma ve Yenileme Ücreti

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.

Kamu SM'nin özel anahtarının çalınması, kaybolması, gizliliğinin veya güvenilirliğinin ortadan kalkması, sertifika ilkelerinin değişmesi ya da sertifikanın hatalı üretilmesi gibi sertifika sahibinin kusurunun bulunmadığı durumların sonucunda sertifikaların Kamu SM tarafından iptal edilmesi ve yenilenmesi halinde, hiçbir ücret talep edilmez.

9.1.2. Sertifika Erişim Ücreti

Kamu SM, kendisine ait sertifikaları ücretsiz olarak yayımlar.

9.1.3. İptal Durum Kaydına Erişim Ücreti

Kamu SM, iptal durum kaydını SİL veya OCSP aracılığıyla duyurma hizmeti için, sertifika sahibinden veya üçüncü kişilerden ücret talep etmez.

9.1.4. Diğer Hizmetlerin Ücretleri

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

Kamu SM, bilgi deposundan yayımladığı bilgi ve dokümanlara erişim için sertifika sahibinden veya üçüncü kişilerden ücret talep etmez.

9.1.5. İade Ücreti

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 ödenen ücreti iade edilir.

9.2. Finansal Sorumluluk

9.2.1. Sigorta Kapsamı

OV SSL sertifikaları ile ilgili olarak sertifika sahiplerine ve sertifikayı kullanan üçüncü taraflara yönelik şu an için herhangi bir sigorta uygulamamaktadır.

9.2.2. Diğer Varlıklar

Düzenlenmesine gerek duyulmamıştır.

9.2.3. Sertifika Mali Sorumluluk Sigortası

Düzenlenmesine gerek duyulmamıştır.

9.3. Ticari Bilginin Korunması

9.3.1. Gizli Bilginin Kapsamı

Kamu SM ve sertifika hizmeti verdiği taraflarca paylaşılan iş planları, satış bilgileri, ticari sırlar ve yapılan gizli anlaşmalarda verilen bilgiler ticari bilgi olarak değerlendirilir. Ayrıca gizli olmadığı özel olarak bildirilmeyen tüm belge ve dokümanlar gizli olarak kabul edilir.

9.3.2. Gizlilik Kapsamında Olmayan Bilgileri

Kamu SM tarafından http://depo.kamusm.gov.tr adresinden yayımlanan her türlü döküman ve sertifikalar içerisinde yer alan bilgiler gizli olarak değerlendirilmezler.

9.3.3. Gizli Bilginin Korunma Sorumluluğu

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

9.4. Kişisel Bilginin Gizliliği

9.4.1. Gizlilik Planı

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

9.4.2. Özel Olarak Tanımlanan Bilgiler

Kişisel/kurumsal bilgiler, sertifika sahibinin, başvuru sırasında kimlik tanımlama ve doğrulama ile sertifika yönetim prosedürleri içinde kullanılmak üzere Kamu SM'ye beyan ettiği nüfus bilgileri ile adres ve telefon numarası gibi erişim bilgilerini kapsar.

9.4.3. Özel Olarak Tanımlanmayan Bilgiler

Kamu SM tarafında oluşturulan sertifikaların içeriğinde bulunan bilgiler gizli değildir.

9.4.4. Gizli Bilginin Korunma Sorumluluğu

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.

Sertifika sahiplerinden başvuru sırasında ve daha sonra sertifika yaşam döngüsü içinde istenen bilgilere erişimin ve yetkisiz kullanımın engellenmesi ve mahremiyetinin korunması için, Kamu SM tarafından gerekli güvenlik tedbirleri alınır. Sadece yetkilendirilmiş çalışanlar sertifika sahiplerinin bilgilerine erişirler.

9.4.5. Gizli Bilginin Kullanımına İzin Verilmesi

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

9.4.6. Yetkili Merciilerin Kararına Uygun Olarak Bilginin Açıklanması

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

9.4.7. Diğer Başlıklar

Düzenlenmesine gerek duyulmamıştır.

9.5. Telif Hakları

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

9.6. Beyan ve Taahhütleri

Kamu SM, sertifika sahipleri ve üçüncü kişiler sertifika sözleşmeleri ile taahhütnamelerde sözü geçen yükümlülükleri yerine getirirler.

9.6.1. ESHS Beyan ve Taahhütleri

ESHS olarak Kamu SM'nin OV SSL sertifika hizmeti için yükümlülükleri şunlardır:

- Hizmetin gerektirdiği nitelikte personel istihdam etmek,
- Belirlediği ilke ve esaslara uygun olarak sertifika işlemlerini yürütmek,
- Sİ ve SUE dokümanlarını herkesin erişimine açık bilgi deposundan yayımlamak,
- Kök ve alt kökler için anahtar çifti üretmek ve bu anahtar çiftleri için sertifikalar oluşturmak,
- Kök ve alt kök sertifikalarını son kullanıcıların erişebileceği ortamlarda yayımlamak,
- Sertifika verdiği kurum kimliğini resmi belgelere göre güvenilir bir biçimde tespit etmek,
- Kurumlardan gelen sertifika başvurularını usulüne uygun biçimde kabul etmek ve başvuruda bulunan kişilerin/kurumların belgeleri ile başvuru formlarını gerekli kontrollerden geçirmek suretiyle kimlik doğrulamalarını Bölüm 3.2.2'de belirtildiği şekilde yapmak,
- Sertifikaların içeriğindeki bilgilerin doğruluğunu beyan edilen belgelere dayanarak sağlamak,
- Gerekli başvuru şartlarını sağlamayan başvuru sahiplerine sertifika vermemek,
- Sertifika başvurularını değerlendirerek, başvurunun sonucu hakkında ilgili kurumları bilgilendirmek,
- Sertifika başvurusu kabul edilmiş kamu kurumları için sertifika üretmek,
- Sertifika yenileme başvurularını Sİ/SUE'de belirtilen şekilde kabul etmek ve değerlendirerek gerekli yenileme işlemlerini yapmak,
- Sertifika iptal başvurularını Sİ/SUE'de belirtilen şekilde kabul etmek ve değerlendirerek gerekli iptal işlemlerini zamanında yapmak,
- Yayımlanan Sİ/SUE dokümanı ile SSL Taahhütnamesi'ne uygun olmayan sertifika kullanımlarının tespit edilmesi durumunda ilgili sertifikayı iptal etmek,
- İptal edilmiş sertifika bilgilerini SİL'de yayımlamak ve OCSP aracılığıyla duyurmak,
- Sertifikaların ve iptal durum kayıtlarının bütünlüğünü ve erişilebilirliğini sağlamak için her türlü tedbiri almak,
- Sertifika sahiplerine ait elektronik veya kağıt ortamda tutulan bilgilerin gizliliğinin korunması için gerekli önlemleri almak, bu bilgileri üçüncü kişilere mahkeme kararı olmaksızın vermemek,
- Sertifika üretim, yönetim ve iptali ile ilgili yapılan tüm işlemlerin kaydını tutmak,

- İşleyiş sırasında kullanılan tüm kağıt ve elektronik kayıtları bu Sİ/SUE'de belirtilen süreler boyunca güvenli olarak saklamak,
- Kök sertifikasını mevzuatta belirtilen şekilde kamuya duyurmak.

9.6.2. Kayıt Birimi Beyan ve Taahhütleri

Kayıt birimlerinin sorumlulukları şunlardır:

- Sertifika başvurularının alınması,
- Sertifika başvuru sahibinin sertifika tipine göre bu dokümanda belirtilen kimlik bilgilerinin gerekli belgelere dayanarak tespiti,
- Sertifika sahibinden gerekli belgelerin ve bilgilerin alınması,
- Sertifika yenileme, askı ve iptal taleplerinin kabul edilmesi, ve KAMU SM'nin ilgili birimlerine iletilmesi.

9.6.3. Sertifika Sahibi Beyan ve Taahhütleri

Sertifika sahibinin yükümlülükleri şunlardır:

- Sertifika başvuru, iptal ve diğer işlemleri bu Sİ/SUE'de belirtildiği şekilde, detayları Kamu SM sertifika yönetim prosedürlerinde anlatılan usule uygun biçimde yerine getirmek,
- Sertifika başvurusu, yenileme ve iptal işlemleri sırasında doğru bilgi beyan etmek,
- Verilen sertifikadaki bilgilerin doğruluğunu kontrol etmek,
- Özel anahtarın güvenliğini sağlamak, özel anahtarın gizliliğinin yitirildiğinden şüphelenmesi durumunda sertifikanın iptal edilmesi için Kamu SM'ye en kısa zamanda başvurmak,
- Kamu SM tarafından oluşturulmuş sertifikanın içeriğinde bulunan bilgilerin değişmesi durumunda derhal sertifikanın iptal edilmesi için Kamu SM'ye başvurmak,
- Sertifika başvurusu sırasında ve sertifikanın geçerlilik süresi boyunca beyan ettiği bilgilerde meydana gelen değişiklikleri derhal Kamu SM'ye bildirmek,
- İptal olmuş veya geçerlilik süresi dolmuş sertifika ile işlem yapmamak,
- Özel anahtarı alt kök sertifikası imzalamak amacıyla kullanmamak,
- Kendisine verilen sertifikayı Sİ/SUE dokümanında belirtildiği biçimde, SSL Taahhütnamesi'nde belirtilen şartlar dahilinde kullanmak.

Yukarıda beyan edilen yükümlülüklerin ihlali nedeniyle üçüncü kişilerin zarara uğraması halinde TÜBİTAK'ın ödemek zorunda olduğu tazminatlarla ilgili sertifika sahibine rücu hakkı saklıdır.

9.6.4. Üçüncü Kişilerin Beyan ve Taahhütleri

Üçüncü kişiler, sertifikalarla ilgili işlem yapmadan önce sertifikanın aşağıda belirtilen geçerlilik kontrollerini yapmakla yükümlüdür:

- Sertifikanın, tanımlanan veriliş amacına uygun olarak kullanıldığını doğrulamak,
- Sertifikanın kullanım süresinin dolup dolmadığını kontrol etmek,
- Sertifikanın geçerliliğini SİL veya OCSP aracılığıyla kontrol etmek,
- SİL veya OCSP'den aldığı iptal durum kaydının bütünlüğünü Kamu SM'nin ilgili sertifikalarının içinde mevcut olan açık anahtarı kullanarak doğrulamak,

- Sertifikanın doğruluğunu Kamu SM alt kök sertifikasının içinde mevcut olan açık anahtarı kullanarak doğrulamak,
- Kamu SM alt kök sertifikasının doğruluğunu kök sertifikasının içinde mevcut olan açık anahtarı kullanarak doğrulamak,
- Kamu SM kök sertifikasının doğruluğunu sertifika özet değerini kontrol etmek suretiyle doğrulamak,
- Sertifika sahibinin, sertifikasının içindeki açık anahtara karşılık gelen özel anahtara sahip olduğunu doğrulamak.

9.6.5. Diğer Katılımcıların Beyan ve Taahhütleri

Kamu SM'nin OV SSL Sertifika hizmeti verirken hizmet aldığı tüm kişi ve kuruluşlardan oluşan diğer katılımcılar söz konusu hizmeti en doğru biçimde vereceklerini ve Kamu SM prosedürleri ve müşterileriyle ilgili gizli veya özel bilgileri açığa çıkarmayacaklarını garanti eder. Kamu SM ile hizmet aldığı kişi veya kuruluşlar arasında bu garantilerin açıkça belirtildiği hizmet sözleşmeleri imzalanır.

9.7. Yükümlülüklerden Feragat

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

9.8. Sorumlulukla İlgili Sınırlamalar

Kamu SM ve sertifika hizmetlerini alan tarafların sorumlulukları ilgili sınırlamalar SSL Taahhütnamesi'nde de belirlenir.

9.9. Tazminat Halleri

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 Süresi ve Anlaşmanın Sona Ermesi

Sertifika sahipleri SSL Taahhütnamesi'ne uygun olarak Kamu SM ile işbirliği içinde çalışır.

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

Kamu SM sertifika hizmeti verdiği süre boyunca Sİ/SUE dokümanı, sertifika yönetim prosedürleri, sertifika sahibine ilettiği SSL Taahhütnamesi'ndeki şartları yerine getirir.

9.10.1. Anlaşma Süresi

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

9.10.2. Anlaşmanın Sona Ermesi

SSL Sertifika Sahibi Taahhütnamesi aşağıdaki durumlarda sonlandırılabilir:

- Sertifika sahibinin sertifikasını iptal etmesi,

- Sertifikanın kullanım süresinin sona ermesi,
- Sertifika sahibinin Sertifika Sahibi Taahhütnamesi'ne aykırı davranması durumunda Kamu SM'nin sertifika sahibine ait sertifikayı iptal etmesi,
- Bölüm 5.7.3'te belirtilen güvenlik açığının ortaya çıkması sebebiyle Kamu SM'nin sertifika sahibine ait sertifikayı iptal etmesi,
- Kamu SM Bölüm 5.8'de belirtildiği biçimde sertifika hizmetlerini sonlandırırsa, Kamu SM'nin sertifika sahibine ait sertifikayı iptal etmesi.

9.10.3. Anlaşmanın Sona Ermesinin Etkileri

SSL Sertifika Sahibi Taahhütnamesi'nin sona ermesiyle hizmeti alan kurumun, Sİ/SUE dokümanında belirtilen şartları sağlamakla ilgili yükümlülükleri ortadan kalkar.

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

Taahhütnameler sona erse bile Kamu SM, dağıttığı sertifikalarla ilgili, yükümlülüklerini yerine getirmeye devam eder. Kamu SM, dağıttığı sertifikalara, iptal durum kayıtlarına taraflarca erişimin sağlanması, Bölüm 5.4 ve 5.5'de belirtilen kayıtların ve arşivlerin saklanması ile ilgili hizmetleri sürdürür.

9.11. Sistem Bileşenleri İle Haberleşme ve Kişisel Bilgilendirme

Kamu SM, sertifika yönetim prosedürlerinde sertifika başvurusunun sonucu, iptal, güncelleme ve yenileme taleplerinin sonuçları hakkında sertifika sahibini bilgilendirir. Bilgilendirmeler telefon, faks veya e-posta aracılığıyla olur. Kurumun sertifika başvuru formunda belirtilen e-posta adresine, değişmesi halinde yeni bildirdiği e-posta adresine yapılan bilgilendirmeler resmi bildirim olarak kabul edilir.

Sertifika yönetimiyle ilgili kritik görünen işlemlerle ilgili bilgilendirmeler resmi yazıyla yapılır.

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. Değişiklik Halleri

9.12.1. Değişiklik Metodları

Sİ/SUE dokümanı Kamu SM tarafından yazılmıştır. Bu Sİ/SUE dokümanında yapılabilecek değişiklikler ekleme ve değiştirme şeklinde olabileceği gibi, Kamu SM dokümanın tamamen yenilenmesine de karar verebilir. Bu Sİ/SUE dokümanının herhangi bir kısmının yanlış ya da geçersiz olduğu ortaya çıksa bile, Kamu SM Sİ/SUE'nin diğer kısımları, Sİ/SUE dokümanı güncellenene kadar geçerliliğini sürdürür.

9.12.2. Bilgilendirme Mekanizması ve Sıklığı

Sİ/SUE dokümanında 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.

9.12.3. Nesne Tanımlama Numarasının Değişmesini Gerektiren Durumlar

Düzenlenmesine gerek duyulmamıştır.

9.13. Anlaşmazlık Halleri

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. İhtilafların sulhen çözümünün mümkün olmaması halinde, ihtilafların çözümünde görevli ve yetkili mahkeme Türkiye Cumhuriyeti Gebze Mahkemeleri'dir.

9.14. Uygulanacak Hukuk

İhtilafların çözümünde görevli ve yetkili mahkeme Türkiye Cumhuriyeti Gebze Mahkemeleri'dir.

9.15. Uygulanabilir Yasalarla Uyum

Sİ/SUE dokümanında geçen hükümlerin daha sonra yürürlüğe girecek ilgili mevzuata aykırı bulunması halinde dokümanda gerekli değişiklikler yapılarak uygun hale getirilir.

9.16. Diğer Hükümler

Düzenlenmesine gerek duyulmamıştır.

10. EK-A SERTİFİKA PROFİLLERİ

10.1. Kamu SM SSL Kök Sertifikası

Alan	Değer
Sürüm	V3
Seri Numarası	01
İmza Algoritması	sha-256 with RSA {1 2 840 113549 1 1 11}
Sertifikayı Veren	CN = TUBITAK Kamu SM SSL Kok Sertifikasi – Surum 1 OU = Kamu Sertifikasyon Merkezi – Kamu SM O = Turkiye Bilimsel ve Teknolojik Arastirma Kurumu – TUBITAK L = Gebze – Kocaeli C = TR
Geçerlilik Başlangıcı	25 Kasım 2013 Pazartesi 11:25:55
Geçerlilik Sonu	25 Ekim 2043 Pazar 11:25:55
Konu	CN = TUBITAK Kamu SM SSL Kok Sertifikasi – Surum 1 OU = Kamu Sertifikasyon Merkezi – Kamu SM O = Turkiye Bilimsel ve Teknolojik Arastirma Kurumu – TUBITAK L = Gebze – Kocaeli C = TR
Açık anahtar	2048 bit RSA {1 2 840 113549 1 1 1}
Uzantılar	**Değer**
Konu Anahtarı Tanımlayıcısı	Critical=No; 65 3f c7 8a 86 c6 3c dd 3c 54 5c 35 f8 3a ed 52 0c 47 57 c8
Anahtar Kullanımı	**Critical=Yes**; Certificate Signing, Offline CRL Signing, CRL Signing
Temel Kısıtlamalar	**Critical=Yes**; Subject Type=CA; Path Length Constraint=None

10.2. Kamu SM SSL Alt Kök Sertifikası

Alan	Değer
Sürüm	V3
Seri Numarası	29
İmza Algoritması	sha-256 ile RSA {1 2 840 113549 1 1 11}
Sertifikayı Veren	CN = TUBITAK Kamu SM SSL Kok Sertifikasi – Surum 1 OU = Kamu Sertifikasyon Merkezi – Kamu SM O = Turkiye Bilimsel ve Teknolojik Arastirma Kurumu – TUBITAK L = Gebze – Kocaeli C = TR
Geçerlilik Başlangıcı	14 Mayıs 2015 Perşembe 16:32:27
Geçerlilik Sonu	11 Mayıs 2025 Pazar 16:32:27
Konu	CN = TUBITAK Kamu SM SSL Sertifika Hizmet Saglayicisi – Surum 1 OU = Kamu Sertifikasyon Merkezi – Kamu SM O = Turkiye Bilimsel ve Teknolojik Arastirma Kurumu – TUBITAK L = Gebze – Kocaeli C = TR
Açık anahtar	2048 bit RSA {1 2 840 113549 1 1 1}
Uzantılar	**Değer**
Yetkili Anahtarı Tanımlayıcısı	Kritik=Hayır; KeyID=65 3f c7 8a 86 c6 3c dd 3c 54 5c 35 f8 3a ed 52 0c 47 57 c8
Konu Anahtarı Tanımlayıcısı	Kritik=Hayır; KeyID=f6 35 35 17 ae 2e fb b7 7d f7 76 17 8a 65 64 eb 67 7a 40 ab
Anahtar Kullanımı	**Kritik=Evet**; Sertifika İmzalama, Çevrimdışı SİL İmzalama, SİL İmzalama
Temel Kısıtlar	**Kritik=Evet**; Konu Türü=CA; Yol Uzunluğu Kısıtlaması=0
Sertifika İlkeleri	[1]Sertifika İlkesi: İlke Tanımlayıcısı=All issuance policies [1,1]İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimliği=CPS Niteleyici: http://depo.kamusm.gov.tr/ilke/ [1,2] İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimliği =Kullanıcı Uyarısı Niteleyici: Uyarı Metni=Bu sertifika ile ilgili Sertifika Ilkelerini okumak için belirtilen web sitesini ziyaret ediniz.

SİL Dağıtım Noktaları	[1]SİL Dağıtım Noktası Dağıtım Noktası Adı: Tam Ad: URL=http://depo.kamusm.gov.tr/ssl/SSLKOKSIL.S1.crl
Yetkili Bilgi Erişimi	[1]Yetkili Bilgi Erişimi Erişim Yöntemi=Sertifika Yetkilisi Yayımcısı (1.3.6.1.5.5.7.48.2) Diğer Ad: URL=http://depo.kamusm.gov.tr/ssl/SSLKOKSM.S1.cer [2] Yetkili Bilgi Erişimi Erişim Yöntemi=OCSP (1.3.6.1.5.5.7.48.1) Diğer Ad: URL=http://ocspsslkoks1.kamusm.gov.tr

10.3. Son Kullanıcı SSL Sertifika Şablonu

Alan	Değer
Sürüm	V3
Seri Numarası	64 bit rastsal sayı içeren tam sayı
İmza Algoritması	sha-256 ile RSA {1 2 840 113549 1 1 11}
Sertifikayı Veren	CN = TUBITAK Kamu SM SSL Sertifika Hizmet Saglayicisi – Surum 1 OU = Kamu Sertifikasyon Merkezi – Kamu SM O = Turkiye Bilimsel ve Teknolojik Arastirma Kurumu – TUBITAK L = Gebze – Kocaeli C = TR
Geçerlilik Başlangıcı	Sertifikanın üretildiği zamandır
Geçerlilik Sonu	Sertifika geçerlilik sonu
Konu	CN = Web sitesi DNS adı O = Başvuru sahibi kurum adı ST = Başvuru sahibinin bulunduğu il C = Başvuru sahibinin bulunduğu ülke
Açık anahtar	2048 bit RSA {1 2 840 113549 1 1 1}
Uzantılar	**Değer**
Yetkili Anahtarı Tanımlayıcısı	Kritik=Hayır; KeyID=f6 35 35 17 ae 2e fb b7 7d f7 76 17 8a 65 64 eb 67 7a 40 ab
Konu Anahtarı Tanımlayıcısı	Kritik=Hayır; KeyID=Sertifikanın içeriğindeki “subjectPublicKey” alanının “BIT STRING” olarak değerinin SHA-1 özet çıktısından oluşur.
Anahtar Kullanımı	**Kritik=Evet**; Dijital imza, Anahtar Şifreleme
Temel Kısıtlar	Kritik=Hayır; Konu Türü=Son Varlık; Yol Uzunluğu Kısıtlaması=Yok
Sertifika İlkeleri	[1]Sertifika İlkesi: İlke Tanımlayıcısı=2.16.792.1.2.1.1.5.7.1.3 [1,1]İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimliği=CPS Niteleyici= http://depo.kamusm.gov.tr/ilke [1,2]İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimliği=Kullanıcı Uyarısı Niteleyici= Uyarı Metni=Bu sertifika ile ilgili sertifika ilkelerini okumak için belirtilen web sitesini ziyaret ediniz.

Gelişmiş Anahtar Kullanımı	Sunucu Kimlik Doğrulaması (1.3.6.1.5.5.7.3.1) İstemci Kimlik Doğrulaması (1.3.6.1.5.5.7.3.2)
SİL Dağıtım Noktaları	[1]SİL Dağıtım Noktası Dağıtım Noktası Adı: Tam Ad: URL=http://depo.kamusm.gov.tr/ssl/SSLSIL.S1.crl
Yetkili Bilgi Erişimi	[1]Yetkili Bilgi Erişimi Erişim Yöntemi=Sertifika Yetkilisi Yayımcısı(1.3.6.1.5.5.7.48.2) Diğer Ad: URL=http://depo.kamusm.gov.tr/ssl/SSLSM.S1.cer [2]Yetkili Bilgi Erişimi Erişim Yöntemi= OCSP (1.3.6.1.5.5.7.48.1) Diğer Ad: URL=http://ocspssls1.kamusm.gov.tr
Konu Alternatif Adı	DNS Name=<alan adı 1> DNS Name=<alan adı 2> ... DNS Name=<alan adı n>