TASNİF DIŞI

TÜBİTAK BİLGEM
KAMU SERTİFİKASYON MERKEZİ

KAMU SM SSL SERTİFİKA İLKELERİ VE SERTİFİKA UYGULAMA ESASLARI

Doküman Kodu
YON.01.06
Revizyon No
v.3.7.0
Revizyon Tarihi
13.12.2023

TASNİF DIŞI

Yasal Uyarı

Kamu Sertifikasyon Merkezi
TÜBİTAK Yerleşkesi, P.K. 74
Gebze 41470 Kocaeli, TÜRKİYE
https://kamusm.bilgem.tubitak.gov.tr

İÇİNDEKİLER

1. GİRİŞ

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

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

Kamu SM, SSL sertifika hizmetleri konusunda, https://www.cabforum.org adresinde yayımlanan "CA/Browser Forum Baseline Requirements (BR) for the Issuance and Management of Publicly-Trusted Certificates" dokümanının güncel sürümüne uyar. Ayrıca bu Sİ/SUE dokümanı, aşağıda belirtilen politikaların, yönergelerin ve gereksinimlerin güncel versiyonlarına uyum sağlamak amacıyla gerçekleştirilen uygulamaları açıklamaktadır:

- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
- CA/Browser Forum Network and Certificate System Security Requirements
- Microsoft Trusted Root Program Requirements
- Mozilla Root Store Policy
- Apple Root Certificate Program
- Chrome Root Program Policy
- 360 Browser CA Policy

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 BAKIŞ

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 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, "İnternet Açık Anahtar Altyapısı Sertifika İlkeleri ve Sertifika Uygulama Esasları Çerçeve Planı" [IETF - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 3647)] referans alınarak hazırlanmıştır. Doküman içeriğinde belirtilen bazı alt başlıkların altındaki "Düzenlenmesine gerek duyulmamıştır." ibaresi, bu bölümle ilgili herhangi bir şart bulunmadığını; "Uygulanmamaktadır." ibaresi bu bölüm altında bulunan uygulamanın Kamu SM politikaları tarafından yasaklandığını ifade etmektedir.

1.2. DOKÜMAN ADI VE TANIMI

Doküman Adı: Kamu SM SSL Sertifika İlkeleri ve Sertifika Uygulama Esasları

Doküman Sürüm Numarası: 3.7.0

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 güncellendi. - 2017 yıllık düzenli SUE güncellemeleri kapsamında değişiklikler yapıldı.	**2.1.1**
20.06.2017	- Kimlik doğrulama adımlarına CAA kayıtları incelemesi eklendi.	**2.2.1**
25.09.2017	- CA/B BR 1.5.0 ile uyumlu hale getirildi.	**3.0.0**
21.10.2017	- Alan adı doğrulamada meta tag kullanımı yerine dosya kullanımı getirildi.	**3.1.0**
26.01.2018	- BR Self Assesment doğrultusunda küçük değişiklikler yapıldı. - Bölüm 3.2.2 CAA Errata 5065 kontrolü eklenerek güncellendi.	**3.2.0**
07.07.2018	- Açık anahtar algoritmalarına ECC eklendi.	**3.2.1**
24.10.2018	- Denetim standardı ETSI EN 319 411-1 doğrultusunda güncelleme yapılmıştır. - CA/B BR 1.6.1 ile uyumlu hale getirildi.	**3.3.0**

16.10.2019	- Yıllık doküman revizyonu kapsamında düzenlemeler yapıldı.	**3.3.1**
11.06.2020	- 3.2.2.4.6 Alan adı doğrulama yöntemi 3.2.2.4.18 ile değiştirildi.	**3.3.2**
04.09.2020	- 1 Eylül 2020'den itibaren üretilen SSL sertifikalarının maksimum geçerlilik süresi güncellendi.	**3.3.3**
16.07.2021	- Bölüm 4.9.12'ye özel anahtarın ele geçirildiğinin ispatını bildirmek için kullanılabilecek yöntemler eklendi. - CA/B BR 1.7.6 ile uyumlu hale getirildi.	**3.3.4**
10.09.2021	- Denetim standardı ETSI EN 319 411-1 v.1.3.1 doğrultusunda güncelleme yapılmıştır.	**3.4.0**
01.12.2021	- Mevcutta kullanılan alan adı sahipliği doğrulama yöntemi yerine "Yapılandırılmış E-Mail" ve "DNS Kaydı Değişikliği" yöntemlerinin kullanımı devreye alınmıştır. - Son kullanıcı SSL sertifikalarında subject:organizationalUnitName alanının kullanımı kaldırılmıştır.	**3.5.0**
04.07.2022	- Son kullanıcı SSL sertifikalarında subject:Locality alanının kullanımı kaldırılmıştır. - Son kullanıcı sertifikalarının iptal nedenleri ile ilgili düzenleme yapılmıştır.	**3.6.0**
26.08.2022	- SSL Başvuru Formu ve SSL Kullanıcı Taahhütnamesinin birleştirilmesi kapsamında güncellemeler yapılmıştır.	**3.6.1**
16.08.2023	- Yıllık gözden geçirme kapsamında, doküman genelinde tutarlılığın sağlanması için minör editoryal düzenlemeler yapılmıştır. - İptal sebeplerinin CRLReasonCode karşılıkları eklenmiştir.	**3.6.2**
04.09.2023	- CA/B BR doğrultusunda SSL sertifikası profili güncellenmiştir.	**3.6.3**
13.12.2023	- ".tr" ccTLD ile biten alan adları için sertifika üretilmesiyle ilgili güncellemeler yapılmıştır. - Self Assessment doğrultusunda düzenlemeler yapılmıştır. - Kamu SM SSL Sertifika İlkeleri dokümanı ile birleştirilmiştir.	**3.7.0**

Yayın Tarihi: 13.12.2023

Nesne Tanımlama Numarası: 2.16.792.1.2.1.1.5.7.1.3

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

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

1.3. SİSTEM BİLEŞENLERİ

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

1.3.1. Elektronik Sertifika Hizmet Sağlayıcısı

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

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

1.3.2. Kayıt Birimleri

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

Tüm kayıt işlemleri doğrudan Kamu SM personeli tarafından yürütülmektedir. Kamu SM, Bölüm 3.2'de tanımlanan gerekliliklerinin tamamını veya bir kısmının yerine getirilmesini Yetkilendirilmiş Üçüncü Tarafa devretmez.

1.3.3. Sertifika Sahipleri

Kamu SM tarafından üretilen sertifikalarını bu Sİ/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

Uygulanmamaktadır.

1.4. SERTİFİKA KULLANIMI

1.4.1. Uygun Sertifika Kullanımı

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

1.4.2. Sertifika Kullanım Sınırları

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

1.5. İLKE VE UYGULAMA ESASLARININ YÖNETİMİ

1.5.1. Doküman Yönetimi

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

1.5.2. İletişim Bilgileri

Bu Sİ/SUE dokümanıyla ilgili bilgi talepleri Kamu SM'nin aşağıdaki iletişim noktalarına iletilmelidir:

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
Problem Raporlama E-Posta: kamusm.cainfo@tubitak.gov.tr
Web : https://kamusm.bilgem.tubitak.gov.tr

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. TANIMLAR VE KISALTMALAR

1.6.1. Tanımlar

Açık Anahtar: Anahtar sahibinin herkes ile paylaşabildiği ve ilgili özel anahtarı ile oluşturduğu dijital imzaların doğrulanmasında ve/veya kendisine şifreli mesaj iletilmesinde kullanılan anahtar çiftinin gizli olmayan bileşenidir. Yalnızca ilişkili olduğu özel anahtar ile eşleşir.

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.

Anahtar Çifti: Özel Anahtarı ve onunla ilişkili olan Açık Anahtarı ifade eder.

Başvuru Sahibi: Kamu SM'ye sertifika için başvuran kamu kurum ve kuruluşu. Sertifika üretildikten sonra Sertifika Sahibi olarak anılır.

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

Çevrimiçi Sertifika Durum Protokolü: Güvenen tarafların sertifikanın iptal durumunu belirlemesini sağlayan çevrimiçi sertifika kontrol protokolü.

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.

İş Günü: Resmi tatiller ve hafta sonu (Cumartesi-Pazar) tatil günleri hariç diğer günler.

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

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

Kök Sertifikası: Kök makamı tarafından yayımlanmış ve üzerinde kendi imzası bulunan sertifika.

Kurum Yetkilisi: SSL Başvuru Formu ve Taahhütnamesinde "Kurum İletişim Noktası" olarak belirtilen ve kurum adına SSL sertifikası başvuru süreçlerini yürütmekle görevlendirilen kişi.

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

Nitelikli Elektronik Sertifika: Teknik açıdan güvenli elektronik imza/mühür oluşturmak için uygun olan ve 5070 sayılı Elektronik İmza Kanunu'ndaki koşulları sağlayan elektronik sertifika.

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

Ön Sertifika (precertificate): RFC 6962'de tanımlandığı üzere; Sertifika Şeffaflığı log sunucularına gönderilebilen imzalı bir veri yapısıdır.

Özel Anahtar: Anahtar Çiftinin sahibi tarafından gizli tutulan ve dijital imza oluşturmak ve/veya ilgili Açık Anahtarla şifrelenmiş elektronik kayıtların, dosyaların şifresini çözmek için kullanılan anahtardır.

Rastgele Değer: Kamu SM tarafından oluşturulan ve en az 112 bit entropiye sahip değer.

Sertifika: Açık anahtar ile kimlik bilgilerini birbirine bağlamak için elektronik imza kullanan elektronik kayıt.

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

Sertifika Makamı: Sertifikaların oluşturulması, yayımlanması, iptal edilmesi ve yönetiminden sorumlu kuruluş.

Sertifika Sahibi: Kamu SM'den sertifika alan ve yasal olarak taahhütname ile bağlı olan kamu kurum ve kuruluşu.

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

Wildcard SSL: Talep edilen alan adına ait tüm alt alan adlarını kapsayan SSL sertifikası.

Yetkilendirilmiş Üçüncü Taraf: Kamu SM tarafından sertifika yönetim sürecindeki gereksinimleri yerine getirmek üzere yetkilendirilmiş 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

BGYS: Bilgi Güvenliği Yönetim Sistemleri

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

CA (Certificate Authority): Sertifika Makamı

CAA (Certificate Authority Authorization): Sertifika Makamı Yetkilendirmesi

CCADB (Common CA Database): Ortak Sertifika Makamı Veritabanı

ccTLD (Country Code Top-Level Domain): Ülke Kodu Üst Seviye Alan Adı

CEN (European Committee for Standardization): Avrupa Standardizasyon Komitesi

CRL (Certificate Revocation List): Sertifika İptal Listesi

CSR (Certificate Signing Request): Sertifika İmzalama İsteği

CWA (CEN Workshop Agreement): CEN Çalıştay Kararı

DNS (Domain Name System): Alan Adı Sistemi

EAL (Evaluation Assurance Level): Değerlendirme Garanti Düzeyi

ECC (Elliptic Curve Cryptography): Eliptik Eğri Kriptografi

ESHS: Elektronik Sertifika Hizmet Sağlayıcısı

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

ETSI EN (ETSI European Standard): ETSI Avrupa Standardı

ETSI TS (ETSI Technical Specification): ETSI Teknik Özellikleri

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

FQDN (Fully-Qualified Domain Name): Tam Nitelikli Alan Adı

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

ISO/IEC (International Organisation for Standardization/International Electrotechnical Commission): Uluslararası Standardizasyon Teşkilatı/Uluslararası Elektroteknik Komisyonu

ITU (International Telecommunication Union): Uluslararası Telekomünikasyon Birliği

Kamu SM: Kamu Sertifikasyon Merkezi

NIST (National Institute of Standards and Technology): (Amerika Birleşik Devletleri) Ulusal Standartlar ve Teknoloji Enstitüsü

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

OID (Object Identifier): Nesne Belirteci

PKI (Public Key Infrastructure): Açık Anahtar Altyapısı

SAN: Subject Alternative Name

SHA (Secure Hash Algorithm): Güvenli Özet Algoritması

SİL: Sertifika İptal Listesi

SSL (Secure Sockets Layer): Güvenli Soket Katmanı

Sİ/SUE: Sertifika İlkeleri ve Sertifika Uygulama Esasları

TLD (Top Level Domain): Üst Seviye Alan Adı

UTC (Coordinated Universal Time): Eş Güdümlü Evrensel Zaman

2. YAYIN VE BİLGİ DEPOSU SORUMLULUKLARI

Bilgi deposu, Kamu SM'nin kök ve alt kök sertifikalarını, iptal durum kayıtlarını, Sİ/SUE, Başvuru Formu ve Taahhütnameler gibi dokümanlarını uygun ve kolayca erişilebilen çevrimiçi ortamda 7 gün 24 saat kesintisiz, güvenli, ücretsiz ve herkesin erişimine açık olarak yayımladığı ortamdır. Depodan yayımlanan dokümanlar gerektiğinde güncellenir. Bu güncellemeler, güncellenen doküman üzerinde tutulan sürüm numarası ve güncelleme tarihi ile belirtilir.

2.1. BİLGİ DEPOSU

Kamu SM'nin bilgi deposuna https://kamusm.bilgem.tubitak.gov.tr ve http://depo.kamusm.gov.tr/ilke adresleri üzerinden erişilir.

Kamu SM, bilgi deposunu işletmek için Yetkilendirilmiş Üçüncü Taraflar kullanmaz.

2.2. SERTİFİKA HİZMETİ İLE İLGİLİ BİLGİLERİN YAYIMLANMASI

Kamu SM'nin, herkesin erişimine açacağı bilgi deposunda 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,
- Form ve Taahhütnameler,
- Güncel sertifika iptal durum kayıtları

SSL Başvuru Formu ve Taahhütnamesi ve Sİ/SUE dokümanı uluslararası erişime açık bir şekilde İngilizce ve Türkçe olarak yayımlanır.

Sİ/SUE dokümanının eski sürümlerine aşağıdaki adresten erişilir:

https://kamusm.bilgem.tubitak.gov.tr/depo/ilke_ve_uygulama_esaslari/eski_ilke_ve_uygulama_esaslari.jsp

Uygulama geliştiricilerin yazılımlarını Kamu SM tarafından üretilen SSL sertifikalarıyla test edebilmeleri için oluşturulmuş test web sayfalarının linkleri aşağıda verilmiştir:

Geçerli SSL sertifikası:	https://testssl.kamusm.gov.tr
İptal olmuş SSL sertifikası:	https://testsslrevoked.kamusm.gov.tr
Süresi dolmuş SSL sertifikası:	https://testsslexpired.kamusm.gov.tr

2.3. YAYIM ZAMANI VE SIKLIĞI

Sİ/SUE dokümanı içeriğinin değişmesi üzerine Form ve Taahhütnameler güncellenir. Güncellenen dokümanlar, güncelleme yapılmasına müteakip mümkün olan en kısa sürede bilgi deposundan yayımlanır.

Kamu SM'ye ait sertifikalar üretilmesine müteakip mümkün olan en kısa sürede bilgi deposundan 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 dokümanını yılda en az bir kez gözden geçirerek, operasyonlarının doğru kalmasını ve ETSI ve CA/B Forum gibi uluslararası kuruluşlar tarafından belirlenen harici gereksinimlere uygun olmasını sağlamak için gerekli değişiklikleri yapar.

Kamu SM, ETSI EN 319 401, ETSI EN 319 411-1 ve CA/B Forum Baseline Requirements standartları ile Kök Programlarındaki güncellemeleri takip eder; faaliyetlerinde gerekli düzenlemeleri yapar ve Sİ/SUE dokümanına gerekli güncellemeleri yansıtır.

2.4. BİLGİ DEPOSUNA ERİŞİM KONTROLLERİ

Kamu SM bilgi deposuna erişim salt-okunur şekilde 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, başvuru sahibinin kurum kimliğini, kurum yetkilisinin yetkisini ve sertifika verilecek alan adı sahipliğini doğrular. Kamu SM doğrulama işlemini yasal ve teknik gerekliliklere göre gerekli görülen tüm belgelere ve resmi kaynaklara dayandırarak yapar.

3.1. İSİMLENDİRME

3.1.1. İsim Alanı Tipleri

Kamu SM tarafından üretilen sertifikalarda, sertifika sahibine ait kimlik bilgilerinin belirtildiği DN (Distinguished Name-Ayırt Edici İsim) 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. 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 SSL sertifikalardaki:

- "CN (Common Name)" 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 (Organization)" alanında sertifika sahibi kamu kurumu veya kuruluşunun teşkilat kanununda veya diğer mevzuatta yer alan açık unvanı veya anlaşılır şekilde kısaltılmış biçimi bulunur.
- "ST (State or Province)" alanında, sertifika sahibi kamu kurumu veya kuruluşun bulunduğu il bilgisi bulunur.
- "C (Country)" alanında, sertifika 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 başvuru sahibi kuruma ait veya kontrolü altında olduğunun doğrulanması koşuluyla birden fazla alan adı da yazılabilir.

3.1.6. Markanın Tanınması, Doğrulanması ve Rolü

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 arabuluculuk faaliyeti yürütmez.

3.2. İLK KİMLİK DOĞRULAMA

İlk kimlik doğrulama sürecinde Kamu SM tarafından aşağıdaki alt başlıklarda tanımlanan yöntemler uygulanır.

3.2.1. Özel Anahtar Sahipliğinin Kanıtlanması

SSL sertifika başvurusu esnasında başvuru sahibi tarafından oluşturulan sertifika imzalama isteği özel anahtar ile imzalanır. Kamu SM CSR dosyasının imzasını doğrular, böylelikle başvuru sahibinin özel anahtara sahipliği doğrulanmış olur.

3.2.2. Kurumsal Kimliğin Doğrulanması

Kamu kurumunun kimliği ve adresi, devlete ait veri tabanları ve yasal belgeler kullanılarak doğrulanır. Kimlik doğrulaması Bölüm 3.2.2.1'de tanımlandığı gibi yapılır. Alan adı sahipliği Bölüm 3.2.2.4'de tanımlanan yöntemlerle doğrulanır. Kamu SM kurumsal kimliğin ve alan adı sahipliğinin doğrulanması sürecini BR dokümanına uyum sağlamak amacıyla düzenli olarak gözden geçirilen iç politika ve prosedürlerine göre yürütür.

3.2.2.1. Kimlik Doğrulama

Kimlik ve adres doğrulama adımları:

- Başvuru sahibinin kimliği ve adresi, periyodik olarak güncellenen devlet veritabanları kullanılarak doğrulanır. Buna ek olarak, başvuru formunda kurum mührünün olduğu kontrol edilir.
- Başvuru formunda yer alan kimlik ve adres bilgilerinin sertifika imzalama isteği içerisindeki bilgilerle aynı olup olmadığı kontrol edilir.
- Kurum kendine ait alan adının sahipliğini vekaleten devredebilir. Bu durumda başvuru belgelerine ek olarak, vekalete ilişkin resmi yazı taraflarca imzalanarak Kamu SM'ye iletilmelidir.

3.2.2.2. Marka İsmi

Kamu SM, özne (Subject) alanında marka isimlerine izin vermez.

3.2.2.3. Ülke Doğrulaması

Kamu SM, yalnızca ".tr" ccTLD ile biten alan adına sahip kamu kurum ve kuruluşlarına OV SSL sertifikası hizmeti vermektedir.

3.2.2.4. Alan Adı Sahipliğinin ve Kontrolünün Doğrulanması

Alan adı sahipliğini doğrulamak için:

- İlk olarak, alan adının ".tr" ccTLD ile bittiği kontrol edilir.
- Başvuru formunda belirtilen alan adının, sertifika imzalama isteği içerisindeki alan adıyla aynı olup olmadığı kontrol edilir.
- Kamu SM, alan adı üzerinde başvuru sahibinin kontrolünü test etmek amacıyla aşağıdaki yöntemlerden birini kullanmaktadır:
    - ***Yapılandırılmış E-Mail Yöntemi (CA/B BR Bölüm 3.2.2.4.4):***
        - Kamu SM, sertifikalandırılacak alan adına bağlı mail sunucusuna ait yönetici e-posta adreslerinden birine (*admin@alanadi, administrator@alanadi, webmaster@alanadi, hostmaster@alanadi, postmaster@alanadi*) rastgele değer gönderir.
        - Başvuru sahibi, yönetici e-posta adresine gelen rastgele değeri Kamu SM'ye geri iletir.
        - Kamu SM rastgele değerin kontrolünü yapar ve alan adı sahipliği doğrulanır.
        - Rastgele değer, her e-posta için eşsizdir ve oluşturulduğu tarihten itibaren 30 (otuz) gün geçerlidir.
        - İçeriği, alıcısı ve rastgele değer aynı kalmak koşuluyla e-postanın tamamı yeniden gönderilebilir.
    - ***DNS Kaydı Değişikliği Yöntemi (CA/B BR Bölüm 3.2.2.4.7):***
        - Başvuru sahibi, sertifikalandırılacak alan adı için Kamu SM tarafından üretilen rastgele değeri içeren bir DNS TXT veya CNAME kaydı oluşturur.
        - Kamu SM oluşturulan DNS kaydını kontrol eder ve alan adı sahipliği doğrulanır.
        - Rastgele değer, sertifika isteğine özeldir ve oluşturulduğu tarihten itibaren 30 (otuz) gün geçerlidir.

Alan adı sahipliğinin doğrulanması için BR 1.8.0 versiyonu Bölüm 3.2.2.4.4 ve Bölüm 3.2.2.4.7'de belirtilen yöntemler kullanılmaktadır. Alan adı sahipliği doğrulamada kullanılan yöntem ve ilgili BR versiyonunun kaydı tutulmaktadır.

3.2.2.5. IP Adres Doğrulaması

Kamu SM, doğrudan IP adreslerine SSL sertifikası vermez.

3.2.2.6. Wildcard Alan Adı Doğrulaması

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 Bölüm 3.2.2.4'te belirtilen kontrollerin tamamı uygulanır.

3.2.2.7. Veri Kaynağının Doğruluğu

Kamu SM, doğrulamada kullandığı veri kaynaklarının güvenilirliğini ve doğruluğunu değerlendirir. 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 adı veya unvanı (Sertifikada 'O' alanı içerisinde bulunur.)
- Kurumun adresi (İl/İlçe/Posta kodu) (Sertifika 'ST' alanı içerisinde il bilgisi bulunur.)
- Vergi numarası
- Kurum yetkilisine ait bilgiler
- Alan adı (Sertifikada 'CN' ve 'SAN' alanları içerisinde bulunur.)
- Sertifika başvurusunda kurum onayını veren yetkiliye ait bilgiler
- PKCS#10 sertifika imzalama isteği

Yukarıda yer alan bilgilerin tamamı başvuru sürecinde alınmak zorundadır. Başvuru formu alındıktan sonra Kamu SM doğrulamayı temel olarak iki kısımda gerçekleştirir. Öncelikle başvuruda bulunan kamu kurumunun kimliği ve adresi, devlete ait veri tabanları ve yasal belgeler kullanılarak doğrulanır. İkinci kısımda ise kamu kurumunun alan adı sahipliği doğrulanmaktadır. Her iki doğrulama süreci de CA/B Forum Baseline Requirements dokümanına uygun şekilde yapılır.

3.2.2.8. CAA Kayıtları

Kamu SM doğrulama adımlarına ek olarak CAA kayıtlarını RFC 8659 (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. CAA kaydı sorgulama sonucuna göre sertifika üretilmesinde herhangi bir sakınca yoksa sertifika, CAA kaydının geçerlilik süresi içerisinde veya 8 saat içerisinde (hangisi daha büyükse) üretilir. CAA kaydı sorgulanırken karşılaşılan hata Kamu SM altyapısından kaynaklanmıyorsa ve en az bir kez sorgu yapıldıysa sertifika üretilebilir. Her bir CAA sorgulamasının kaydı sertifika verildiği ya da verilmediği durumda tutulmaktadır.

3.2.3. Kişisel Kimliğin Doğrulanması

Kamu SM kamu kurumlarına OV SSL hizmeti verdiğinden, yalnızca 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

Sertifika talebinde bulunan kurum, kendi adına SSL sertifikası başvuru süreçlerini yürütmekle görevlendirdiği kurum yetkilisini başvuru esnasında belirtir. Kamu SM tanımlanan kurum yetkilisi dışında farklı bir kişiden gelen sertifika taleplerini kabul etmemektedir.

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.

3.2.6. Uyum Kriterleri

Kamu SM çapraz sertifikalandırma yapmamaktadır.

3.3. ANAHTAR YENİLEME İSTEĞİNDE KİMLİK BELİRLEME VE DOĞRULAMA

3.3.1. Olağan Anahtar Yenileme İsteğinde Kimlik Belirleme ve Doğrulama

SSL sertifikaları için anahtar yenileme yapılmaz. Anahtar yenileme taleplerinde ilk başvuru prosedürleri uygulanır. Bu durumda kimlik belirleme ve doğrulama işlemleri Bölüm 3.2'de belirtilen şekilde yapılır.

3.3.2. İptal Sonrası Anahtar Yenileme İsteğinde Kimlik Belirleme ve Doğrulama

SSL sertifikaları için anahtar yenileme yapılmaz. Anahtar yenileme taleplerinde ilk başvuru prosedürleri uygulanır. Bu durumda kimlik belirleme ve doğrulama işlemleri Bölüm 3.2'de belirtilen şekilde yapılır.

3.4. SERTİFİKA İPTAL İSTEĞİNDE KİMLİK BELİRLEME VE DOĞRULAMA

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

Sertifika iptal başvurusunu kimlerin yapabildiği Bölüm 4.9.2'de tanımlanmıştır.

Sertifika iptali sırasında zaman bilgisi tutarlılığının sağlanması için Kamu SM 24 saatte bir tüm sunucularını UTC ile senkronize eder.

4. SERTİFİKA YAŞAM DÖNGÜSÜ İŞLEVSEL GEREKLİLİKLERİ

Bu bölümde sertifika yönetim süreçlerinde yapılan işlemler anlatılmaktadır. Kamu SM, sertifika üretimi ve iptali ile ilgili sertifika politikalarına uygun hizmetlerin kurulması ve sürdürülmesi konusunda diğer kuruluşlardan bağımsızdır. Ayrıca sertifika üretimi ve iptali ile ilgili işlemlerin tarafsızlığını güvence altına alan belgelendirilmiş bir yapıya sahiptir. Sertifika üretimi ve iptal yönetimi ile ilgili Kamu SM personelinin, ESHS hizmetlerinin güvenliğini tehlikeye atacak ticari ve finansal işlemler yapmaları kanunen yasaklanmıştır.

4.1. SERTİFİKA 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 web sitesinden indireceği "Güvenli Sunucu Sertifikası (SSL) Başvuru Formu ve Taahhütnamesi" dokümanını doldurup imzalı ve mühürlü/kaşeli olarak Kamu SM'ye gönderir. Nitelikli elektronik sertifikalar ile oluşturulmuş elektronik imzalı/mühürlü başvurular da kabul edilmektedir. 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:

- Gerekli tüm bilgileri içerecek şekilde Güvenli Sunucu Sertifikası (SSL) Başvuru Formu ve Taahhütnamesini imzalı ve mühürlü/kaşeli 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.

Başvuru sahibi, Kamu SM'nin doğrulama sürecini başarıyla yürütebilmesi için gerekli bilgileri sağlamalıdır. Kamu SM gerek görmesi halinde ek belge talebinde bulunabilir.

4.2. SERTİFİKA BAŞVURUSUNUN İŞLENMESİ

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. Kamu SM, Bölüm 3.2 kapsamında edindiği alan adı doğrulama verisi dahil herhangi bir bilgi ve belgeyi sonraki başvurularda tekrar kullanmaz. Kimlik tanımlama ve doğrulama işlevleri sırasında yetkilendirilmiş üçüncü kuruluşlar yer almamaktadır.

Kamu SM yüksek riskli sertifika başvurularının doğrulanması için ilave doğrulama yöntemleri uygulayabilir.

Kamu SM, CAA kayıtlarını RFC 8659 prosedürlerine uygun şekilde incelemektedir. CAA kayıtlarının işlenmesi ile ilgili politika Bölüm 3.2.2.8'de ayrıntılı olarak verilmiştir.

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.

Kamu SM, IP adreslerine veya iç sunucu adreslerine sertifika vermemektedir.

Sertifika başvurusunun kabul edilmemesi durumunda kuruma e-posta aracılığıyla yazılı veya telefon aracılığıyla sözlü bilgilendirme 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. SERTİFİKANIN ÜRETİLMESİ

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 kayıt altına alınır.

Kök sertifikası tarafından imzalanmış bir sertifikanın üretimi, sertifika üretim sorumlusu ve sistem operatörünün kontrolü ile gerçekleştirilir.

4.3.2. Sertifika Oluşturulması ile İlgili Sertifika Sahibinin Bilgilendirilmesi

Kamu SM, ürettiği sertifikayı kurum yetkilisinin başvuru sırasında belirttiği kurumsal e-posta adresine gönderir.

4.4. SERTİFİKANIN KABUL EDİLMESİ

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, sahibine gönderilmesine müteakip 10 iş günü içerisinde herhangi bir dönüş olmaması durumunda kabul edilmiş olur.

4.4.2. Sertifikanın ESHS Tarafından Yayımlanması

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

4.4.3. Sertifikanın Oluşturulmasının Diğer Bileşenlere Duyurulması

Düzenlenmesine gerek duyulmamıştır.

4.5. SERTİFİKANIN VE ANAHTAR ÇİFTİNİN KULLANIMI

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 SSL Başvuru Formu ve Taahhütnamesinde yer alan koşullar ve belirlenmiş sınırlar içinde kullanmalıdır. Sertifika sahibi, SSL sertifikasını yalnızca sertifikanın "Subject Alternative Names" alanında belirtilen alan adları üzerinden erişilebilen sunuculara kurmalıdır.

Sertifika sahibi, özel anahtarın kontrolünü sağlamak, gizli tutmak ve her zaman uygun şekilde korumak için tüm makul önlemleri almakla yükümlüdür. SSL sertifikasına karşılık gelen özel anahtar yalnızca sertifikada "Anahtar Kullanımı" ve "Genişletilmiş Anahtar Kullanımı" alanlarında 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" ve/veya "Genişletilmiş Anahtar Kullanımı" alanında belirtilen amaçlar doğrultusunda kullanıldığını doğrulamakla ve Sİ/SUE'de belirtilen kullanım koşullarına uymakla yükümlüdürler.

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

4.6. SERTİFİKA YENİLEME

Sertifika yenileme, eski sertifikanın geçerlilik süresi dolduktan sonra aynı anahtar çifti ve sertifika bilgileri kullanılarak yeni bir geçerlilik süresiyle yeni bir sertifika yayımlanması anlamına gelmektedir. Kamu SM, SSL sertifikaları için sertifika yenileme yapmaz. Sertifika yenileme talepleri yeni bir sertifika başvurusu olarak değerlendirilir.

4.7. ANAHTAR YENİLEME

Anahtar yenileme, sistemde geçerli bir sertifikası bulunan sertifika sahibine, sertifikanın bitiş tarihinden önce, yeni bir anahtar çiftine sertifikanın içeriğinde bulunan bilgilerde değişiklik yapmadan, eskisinin yerine geçecek yeni bir sertifika verilmesi anlamına gelmektedir. SSL sertifikaları için anahtar yenilemesi yapılmaz. Anahtar yenileme talepleri yeni bir sertifika başvurusu olarak değerlendirilir.

4.8. SERTİFİKA DEĞİŞİKLİĞİ

Kamu SM tarafından üretilmiş bir sertifikanın içeriğindeki bilgilerde bir değişiklik olması durumunda, sertifika iptal edilir ve yeni bilgilerle birlikte yeni bir sertifika başvurusunda bulunulur. Sertifika değişikliği talepleri yeni bir sertifika başvurusu olarak değerlendirilir.

4.9. SERTİFİKANIN İPTALİ VE ASKIYA ALINMASI

4.9.1. Sertifikanın İptal Edildiği Durumlar

4.9.1.1. SSL Sertifikasının 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,
- Sertifikanın hatalı üretilmesi.

Kamu SM, aşağıdaki sebeplerin ortaya çıkması durumunda sertifika sahibine ait sertifikayı en geç 24 saat içinde iptal eder:

- Sertifika sahibinin sebep göstermeksizin yazılı olarak iptal talebinde bulunması (CRLReason: "unspecified (0)"),
- SSL başvuru sürecinde, Kamu SM'ye evrakları gönderen yetkili kişinin kurumun onayını almadığının tespit edilmesi veya ilgili kurum tarafından söz konusu durumun Kamu SM'ye bildirilmesi (CRLReason #9, privilegeWithdrawn),
- Sertifika sahibinin özel anahtarının güvenliğini kaybettiğinin tespit edilmesi (CRLReason #1, keyCompromise),
- SSL sertifikası özel anahtarının kolaylıkla hesaplanabilmesine olanak veren metot bulunduğunun tespit edilmesi (Örn: Debian zayıf anahtar) (CRLReason #1, keyCompromise),
- Alan adı sahipliği doğrulamasına güvenilmemesi gerektiğinin tespit edilmesi (CRLReason #4, superseded).

Kamu SM, aşağıdaki sebeplerin ortaya çıkması durumunda sertifika sahibine ait sertifikayı en geç 5 (beş) gün içinde iptal eder:

- Sertifikanın Sİ/SUE ve CA/B Forum Baseline Requirements dokümanlarına uygun üretilmediğinin tespit edilmesi (CRLReason #4, superseded),
- Sertifika içeriğindeki sertifika sahibine ait bilgilerin sahteliğinin veya yanlışlığının ortaya çıkması (CRLReason #9, privilegeWithdrawn),
- Sertifika içeriğindeki bilgilerin değiştiğinin ortaya çıkması (CRLReason #9, privilegeWithdrawn),
- Sertifikanın SSL Başvuru Formu ve Taahhütnamesi ve Sİ/SUE dokümanında belirtilen şartlara aykırı kullanımının tespit edilmesi (CRLReason #9, privilegeWithdrawn),
- Sertifikanın kötüye kullanıldığının tespit edilmesi (CRLReason #9, privilegeWithdrawn),
- Sahte veya yanıltıcı bir alt alan adını doğrulamak için wildcard SSL sertifikası kullanıldığının tespit edilmesi (CRLReason #9, privilegeWithdrawn),
- Bir mahkemenin veya bir yetkilinin sertifika sahibinin alan adı sahipliğini veya kullanma yetkisini ortadan kaldırdığına dair Kamu SM'ye bildirimde bulunması veya bunun Kamu SM tarafından anlaşılması (CRLReason #5, cessationOfOperation),

- SSL sertifikalarının üretiminde kullanılan anahtar uzunluğunun veya kriptografik algoritmaların uygunluğunun ortadan kalkması (CRLReason #4, superseded),
- SSL sertifikası özel anahtarı üretiminde kullanılan yöntemin hatalı/zayıf olduğuna dair kanıt elde edilmesi (CRLReason #1, keyCompromise),
- Kamu SM'nin işleyişine son vermesi ve verilen sertifikaların yönetim işlemlerinin başka bir ESHS tarafından devamlılığının sağlanamaması (CRLReason: "unspecified (0)").

4.9.1.2. Alt Kök Sertifikasının İptal Edildiği Durumlar

Kamu SM, aşağıdaki sebeplerin ortaya çıkması durumunda alt kök sertifikasını en geç 7 (yedi) gün içinde iptal eder:

- Sertifikanın; SSL Başvuru Formu ve Taahhütnamesi, Sİ/SUE ve CA/B Forum Baseline Requirements dokümanlarına uygun olarak üretilmediğinin ve/veya belirtilen şartlara aykırı kullanımının tespit edilmesi,
- Kamu SM'nin sertifikayı imzalamak için kullandığı özel anahtarın güvenliğinin yitirilmesi,
- SSL sertifikalarının üretiminde kullanılan anahtar uzunluğunun veya kriptografik algoritmaların uygunluğunun ortadan kalkması,
- Sertifika içeriğindeki bilgilerin yanlışlığının ortaya çıkması,
- 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

Bölüm 4.9.1.1'de belirtilen durumlarda sertifika sahibi veya Kamu SM sertifika iptal sürecini başlatabilir. Sertifikayı Kamu SM iptal ettiğinde, sertifika sahibi kurumu bilgilendirir, iptal sebebini açıklar.

Yalnızca sertifika sahibi veya kurum yetkilisi tarafından gerçekleştirilen yetkilendirilmiş iptal talepleri kabul edilir.

Ek olarak, üçüncü taraflar makul nedenler bildirmek suretiyle Kamu SM tarafından üretilen bir SSL sertifikasının iptalini talep etmek için Bölüm 4.9.5'te belirtildiği üzere problem raporları gönderebilir.

4.9.3. Sertifika İptal Başvuru Yöntemleri

SSL sertifikası iptal başvurusu, sertifika sahibi kurumun yetkilisi tarafından Kamu SM web sitesinde yer alan "SSL İptal Başvuru Formu" ile yapılır. Kurum yetkilisi imzalı ve mühür/kaşeli formun taranmış halini kurumsal e-posta adresinden Kamu SM web sayfasından yayımlanan iptal için belirlenen ssliptal@kamusm.gov.tr e-posta adresine göndererek iptal talebinde bulunur. 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. Alt kök sertifikasının iptal kontrolünde kullanılan SİL dosyası ve OCSP yanıtlarına, uygun iptal sebebini içeren "CRLReason/ReasonCode" iptal kodu eklenir. İptalin gerçekleştirilmesinin ardından sertifika 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, iptal başvurusunu en geç 24 saat içerisinde doğrulayarak sertifikayı iptal eder. Bu iptal bilgisi OCSP sunucusuna hemen yansır ve en geç 24 saat içerisinde yeni SİL dosyası yayımlanır. İptal başvurusunun doğrulanamaması durumunda sertifika iptal durum değişikliği SİL ve OCSP sunucusuna yansıtılmaz. İki iptal kontrol mekanizması arasında sertifika iptal durum bilgisinde fark olması durumunda OCSP cevabı dikkate alınmalıdır. İptal edilen sertifikalar yeniden kullanılabilir hale getirilemez.

Üçüncü taraflarca sertifikada hata görülmesi durumunda sertifikanın incelenmesi talep edilebilir. İlgili talep CPS Bölüm 1.5.2'de belirtilen problem raporlama e-posta adresi üzerinden iletilmelidir. Şüpheli durum 24 saat içerisinde incelenir ve sertifika sahibi ile sertifikanın incelenmesini talep eden tarafa ön bilgilendirme yapılır. Bölüm 4.9.1.1'e göre sertifikanın iptal durumu değerlendirilerek ilgili taraflara sonuç bildirilir ve iptal süreci işletilir.

Kamu SM, iptal taleplerini ve problem raporlarını kabul etme ve bunlara yanıt verme konusunda 7 gün 24 saat sürekli olarak hizmet vermektedir.

4.9.6. Üçüncü Kişilerin Sertifika İptal Durumunu Kontrol Gerekliliği

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

Üçüncü kişiler, sertifikalara dayanarak işlem yapmadan önce sertifikaların geçerliliğini doğrulamalı ve SİL ya da OCSP yöntemlerinden birini kullanarak iptal kontrolü yapmalıdır. Teknik imkanlar elveriyorsa sertifika iptal kontrolünün OCSP üstünden yapılması Kamu SM tarafından tavsiye edilen yöntemdir.

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

SSL sertifikalarının iptal bilgisinin bulunduğu SİL günde en az 1 (bir) kere yayımlanır. Bu SİL'in geçerlilik süresi en fazla 36 saattir. Yeni SİL dosyası, SİL içerisindeki *nextUpdate* alanında belirtilen zamandan önce yayımlanır.

Kamu SM'ye ait alt kök sertifikalarının iptal bilgisinin bulunduğu SİL dosyası yılda en az 1 (bir) kere yayımlanır. Bu SİL'in geçerlilik süresi en fazla 1 (bir) yıldır. Alt kök sertifikasının iptali durumunda derhal yeni SİL dosyası yayımlanır.

Kamu SM tarafından yayımlanan SİL dosyaları arşivlenir.

Kamu SM, alt kök sertifikasının süresi dolana/iptal olana kadar veya özel anahtarı imha edilene kadar SİL yayımlamaya devam eder.

4.9.8. Sertifika İptal Listesi Yayımlama Gecikme Süresi

SİL'ler oluşturulduktan sonra en kısa süre içinde depoda 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.

Kamu SM tarafından oluşturulan OCSP cevapları, iptal kontrolü yapılan sertifikanın yayımcı sertifikası tarafından verilen OCSP Yanıtlayıcı Sertifikaları kullanılarak imzalanır. OCSP Yanıtlayıcı Sertifikalarında RFC 6960'a uygun olarak *id-pkix-ocsp-nocheck* uzantısı bulunur.

4.9.10. Çevrim İçi Sertifika İptal Durum Kontrol Gereklilikleri

Kamu SM OCSP sunucuları RFC 6960'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.

OCSP cevapları, geçerlilik süresi 16 (on altı) saati aşmayacak şekilde üretilir. Her bir OCSP sorgusu için güncel bir OCSP cevabı üretilir.

Kamu SM, asıl sertifikası üretilmemiş olsa bile, ön sertifikalar [Precertificate; RFC 6962] için OCSP servisi ve yanıtı sağlar.

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 e-posta veya uygun iletişim kanalları yoluyla duyurulur.

Kamu SM, son kullanıcılara ait sertifikalarda güvenlik sorunu oluşması durumunda ilgili son kullanıcı sertifikasını iptal eder, sertifika sahibini bilgilendirir.

Üçüncü taraflar, Kamu SM tarafından üretilen bir SSL sertifikasının özel anahtarının ele geçirildiği gerekçesiyle iptalini talep edebilir. Bu durumda, özel anahtarın ele geçirildiğinin ispatlanması için "Common Name" alanında anahtarın ele geçirildiği ifadesi yer alan sertifika istek dosyası (CSR), ilgili özel anahtarla oluşturularak Bölüm 4.9.3'de belirtilen adrese e-posta ile gönderilmelidir. Kamu SM, kendi takdirine bağlı olarak alternatif yöntemlere izin verebilir.

4.9.13. Sertifikanın Askıya Alındığı Durumlar

SSL sertifikaları için askı işlemi uygulanmamaktadır.

4.9.14. Sertifika Askıya Alma Başvurusunu Kimlerin Yapabildiği

Uygulanmamaktadır.

4.9.15. Sertifika Askıya Alma Başvurusunun İşlenmesi

Uygulanmamaktadır.

4.9.16. Askıda Kalma Süresi

Uygulanmamaktadır.

4.10. SERTİFİKA DURUM SERVİSLERİ

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

4.10.1. İşletimsel Özellikler

Kamu SM, sertifikaların iptal kontrolü için SİL ve/veya OCSP hizmeti sağlar. SİL dosyasına sertifika içerisinde yer alan "SİL Dağıtım Noktası" uzantısından erişilebilir. SİL dosyaları aynı zamanda Kamu SM bilgi deposundan yayımlanmaktadır. OCSP yanıtlayıcı adresine sertifika içerisinde yer alan "Yetkili Bilgi Erişimi" uzantısından erişilebilir. OCSP servis adresleri aynı zamanda Bölüm 4.9.9'da belirtilmiştir.

İptal edilen sertifikalar geçerlilik süreleri dolmadan SİL ve OCSP'den kaldırılmaz.

BR gereksinimleri doğrultusunda, Kamu SM sertifikanın özel anahtarının o sertifika için SİL girdisinde belirtilen iptal tarihinden önce tehlikeye girdiğini belirlediğinde SİL girdisindeki iptal tarihini güncelleyebilir.

4.10.2. Servisin Erişilebilirliği

Kamu SM, SİL ve OCSP servislerini 7 gün 24 saat kesintisiz olarak sunmak için gerekli tüm tedbirleri alır. Kamu SM, SİL ve OCSP kapasitesini normal çalışma koşullarında 10 saniye veya daha kısa bir yanıt süresi sağlamaya yetecek kaynaklarla işletir.

4.10.3. İsteğe Bağlı Özellikler

Düzenlenmesine gerek duyulmamıştır.

4.11. SERTİFİKA SAHİPLİĞİNİN SONA ERMESİ

Sertifikanın kullanım süresinin dolması, iptal edilmesi veya Kamu SM'nin sertifika hizmetlerini sonlandırmasıyla sertifika sahipliği sona erer. Kamu SM, sertifikanın iptal edilmesi veya Kamu SM tarafından sertifika hizmetlerinin sonlandırılması durumunda sertifika sahibini ve/veya kurum yetkilisini bilgilendirir. Kullanım süresinin dolması durumunda Kamu SM sertifika sahibini bilgilendirmek zorunda değildir; sertifika sahibi, sertifikasının kullanım süresinin dolduğu zamanı kendisi takip etmekle yükümlüdür.

4.12. ANAHTAR SAKLAMA VE YENİDEN ÜRETME

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

5. YÖNETİM, İŞLEMSEL VE FİZİKSEL KONTROLLER

Kamu SM'nin sertifika yönetim süreçleri aşağıdakileri içerir:

- Fiziksel ve çevresel güvenlik kontrolleri
- Sistem bütünlüğü kontrolleri (kötü amaçlı yazılım tespiti/önlenmesi, yapılandırma yönetimi vs.)
- Ağ güvenliği ve güvenlik duvarı yönetimi (port kısıtlamaları, IP adres filtrelemesi vs.)
- Kullanıcı yönetimi, güvenilir rollerin ayrılığı, personel eğitimleri
- Mantıksal erişim kontrolleri, aktivite loglarının tutulması

Kamu SM, sertifika yönetim süreçlerindeki riskleri değerlendirir. Kamu SM tarafından gerçekleştirilen risk değerlendirmesi, sertifika verilerine veya sertifika yönetim süreçlerine yetkisiz erişim, ifşa, kötüye kullanım, değişiklik veya imha ile sonuçlanabilecek öngörülebilir iç ve dış tehditleri tanımlar. Kamu SM, bu tehditlerin olasılığını ve potansiyel zararını değerlendirir. Bunun yanı sıra, Kamu SM'nin bu tür tehditlere karşı koymak için sahip olduğu politikaların, prosedürlerin, bilgi sistemlerinin ve diğer düzenlemelerin yeterliliği de değerlendirilir.

Risk değerlendirme sonuçlarını dikkate alarak uygun risk tedavi aksiyonlarını ve kontrollerini belirler. İlgili aksiyonların ve kontrollerin uygulanması için gerekli kaynakları sağlar. Tüm risklerle birlikte artık riskler de üst yönetim tarafından onaylanır. Tüm riskler yılda en az bir defa gözden geçirilir.

Kamu SM Bilgi Güvenliği Politikası yönetim tarafından onaylanmıştır. Resmî web sitesinde ilgili tarafların erişimine sunulmuştur.

Sistem konfigürasyonları bilgi güvenliği politikaları ihlalleri tespitine yönelik 3 (üç) aylık periyotlarla örneklem alınarak kontrol edilmektedir.

Kamu SM bilgi varlıklarını tanımlar ve envanterini tutar. Varlıkların gizlilik derecelendirme sınıflarına göre erişim yetkilendirmesini ve muhafazasını yapmaktadır.

5.1. FİZİKSEL GÜVENLİK KONTROLLERİ

Kamu SM, sertifika üretim ve yönetim süreçlerinde kullanılan sistemler için fiziksel ve çevresel güvenlik politikaları uygular.

Kamu SM sisteminin çalıştığı cihazların bulunduğu binalar ve odalar, giriş ve çıkışların kontrol edildiği, yetkisiz kişilerin girişini engelleyen güvenlik önlemleri ile donatılmıştır. Bu alanlar dahili ve harici kötü niyetli etkinliklerden korunur. Güvenli alanlara tüm erişimin kaydı tutulur.

Kamu SM sertifika makamlarına ait özel anahtarlar normal operasyonların gerçekleştiği alandan fiziksel olarak ayrılmıştır. Bu alana erişim için en az 2 (iki) yetkili personelin aynı anda hazır bulunması gerekir.

5.1.1. Tesis Yeri ve İnşaatı

Kamu SM operasyonları Gebze ve Ankara'daki tesislerde yürütülmektedir. Kamu SM sisteminin çalıştığı binanın bulunduğu Gebze tesisi, yerleşim merkezinden uzak, yangın, su baskını, deprem, yıldırım ve hava kirliliğinden en az etkilenecek, giriş ve çıkışların kontrol edildiği bir bölgedir. Alanlara ve binalara erişim, fiziki güvenlik, video izleme ve kimlik doğrulama olmak üzere çoklu güvenlik ile korunmaktadır. Ankara tesisi farklı seviyelerde fiziksel kontrolü bulunan bir alandır.

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. Yazılım ve donanım modülleriyle arşivler yetkisiz değişiklik, ikame ve imha durumlarını önlemek için görevler ayrılığına uygun olarak sınıflandırılmıştır. Yetkisiz personel ve kayıtsız ziyaretçiler bu hassas alanlara giremez.

5.1.2. Fiziksel Erişim

Kamu SM yazılım ve donanım sistemleri ile 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 kartlı geçiş sistemleri ve biyometrik kontroller yapan gelişmiş erişim kontrol cihazlarıyla yapılmaktadır. Güvenli alanlarda yetkisiz kişilerin çalışması gereken durumlarda en az bir yetkili personel eşlik eder. 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 sistemler kullanılarak gerekli 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. Özel anahtar içeren kriptografik cihazlar, akıllı kartlar ve diğer cihazlar endüstrideki en iyi uygulamalara göre imha edilir ve sıfırlanır. Diğer atıklar standart atık imha prosedürüne uygun olarak imha 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. PROSEDÜREL KONTROLLER

5.2.1. Güvenilir Roller

Kamu SM'de çalışan personelin rolleri ETSI EN 319 401 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 uygulamalarının yürütülmesinden 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/iptal başvurusunun alınması, başvuru evraklarının ve kurum kimliğinin doğrulanmasından sorumlu personeldir.

Sertifika Üretim Sorumlusu: Alan adı sahipliğinin ve sertifika istek dosyasının doğrulanmasından sorumlu, sertifika üretimini gerçekleştiren personeldir.

Doğrulama Sorumlusu: CA/B Forum Baseline Requirements kapsamında Sİ/SUE dokümanında belirtilen bilgi doğrulama görevlerini yerine getirmekten sorumlu personeldir. Kamu SM işleyişinde Sertifika Kayıt Sorumlusu ve Sertifika Üretim Sorumlusu, Doğrulama Sorumlusu olarak görev almaktadır.

5.2.2. Her İşlem İçin Gereken Kişi Sayısı

Kamu SM, CA sertifikalarının üretilmesi ve iptal edilmesi için birden fazla yetkili personelin aynı anda hazır bulunmasını sağlar.

Kamu SM, CA özel anahtarlarının yedeklenmesi, saklanması ve kurtarılması için fiziksel olarak güvenli bir ortamda birden fazla yetkili personelin aynı anda hazır bulunmasını sağlar.

5.2.3. Her Bir Rol için 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.

Kullanıcı hesapları yetkilendirme ve yönetiminde Kamu SM Erişim Yönetimi Politikası temel alınmaktadır.

5.2.4. Görevlerin Ayrılmasını Gerektiren Roller

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

görevler ayrılığı vardır.

5.3. PERSONEL GÜVENLİK KONTROLLERİ

5.3.1. Kişisel Geçmiş, Deneyim ve Nitelik Gerekleri

Herhangi bir kişi sertifika yönetim sürecinde görevlendirilmeden önce, Kamu SM söz konusu kişinin kimliğini ve güvenilirliğini doğrular. Kamu SM, sunduğu hizmetler için işin gerekliliklerine uygun olarak gerekli uzmanlık, bilgi, deneyim ve niteliklere sahip personel istihdam eder.

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. Adli sicil kayıtları incelenir. Güvenlik soruşturması biten personel işe başlatılır. Bilgi Güvenliği Farkındalık eğitimleri almadan sistemlere erişim verilmez.

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.

Kamu SM yılda en az bir defa olmak üzere çalışanlara bilgi güvenliği politikaları hakkında siber güvenlik ve sosyal mühendislik saldırılarına karşı bilgi güvenliği farkındalığı oluşturmak amacıyla eğitim vermektedir. Bunun yanı sıra Doğrulama Sorumlusu olarak çalışan personele sertifika yönetim süreçlerindeki görevleri kapsamında eğitimler verilir.

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 bilgi güvenliği politikaları ihlali ve ihlalin boyutuna göre hukuki soruşturma ve disiplin süreci başlatılır.

5.3.7. Anlaşmalı Personel Gereksinimleri

Güvenilir rollerdeki personeller bağımsız yüklenici veya anlaşmalı personel olamaz. Sertifika üretiminde herhangi bir Yetkilendirilmiş Üçüncü Taraf personeli yer almamaktadır.

5.3.8. Sağlanan Dokümantasyon

Kamu SM, personeline iş sorumluluklarıyla ilgili teknik ve operasyonel dokümanları sağlar.

5.4. DENETİM KAYITLARI

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. Kamu SM, gerekli görüldüğü takdirde bu kayıtları nitelikli denetçilere sunar. Elektronik kayıtların tutulduğu sunucunun saati günde en az bir kez UTC ile senkronize edilir.

5.4.1. Kaydedilen İşlemler

Kamu SM sisteminde aşağıdaki olayların kayıtları tutulur:

- Kamu SM sertifika ve anahtarlarının yaşam döngüsü işlemleri
  - Anahtar üretimi, yedekleme, imha
  - Sertifika istekleri, üretimi ve iptali
  - Kriptografik modül yaşam döngüsü işlemleri
  - SİL yayımlanması ve OCSP cevaplarının imzalanması
  - Yeni sertifika profili oluşturulması ve mevcut profillerin ortadan kaldırılması
- SSL sertifikası yaşam döngüsü yönetimi işlemleri
  - Sertifika istekleri, üretimi ve iptali

- Sİ/SUE ve CA/B Forum Baseline Requirements dokümanları kapsamında yapılan tüm doğrulama işlemleri
- Geçerli ve geçersiz tüm sertifika istekleri
- SİL yayımlanması
- OCSP cevaplarının imzalanması
- Başvuru sırasında elektronik veya kağıt ortamda alınan form veya belgeler

- Güvenlikle ilgili diğer işlemler
  - Sistemin başlatılması ve kapatılması
  - 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
  - Sertifika sistemine yazılım yüklenmesi, güncellenmesi ve kaldırılması
  - Sistemin çökmesi, donanım hataları ve diğer bozukluklar
  - Güvenlik cihaz/yazılım işlemleri (Güvenlik Duvarları, IPS, HIDS, Router vb.)
  - Kamu SM'ye ziyaretçi giriş ve çıkışı

Kayıtlarda olay açıklaması, olay tarihi-saati ve kaydı oluşturan çalışanın bilgileri bulunur.

5.4.2. Kaydın İncelenme Sıklığı

Sistemin işleyişiyle ilgili tutulan kayıtlar belirli aralıklarla 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. Kaydın Saklanma Süresi

Kamu SM, sertifika ve anahtarlarının yaşam döngüsü işlemlerine ilişkin olay kayıtlarını, Kamu SM özel anahtarının imhası veya CA sertifikasının süresi dolması/iptal edilmesinden sonra en az iki yıl süreyle saklamaya devam eder.

SSL sertifikası yaşam döngüsü yönetimi işlemlerine ilişkin olay kayıtları, SSL sertifikasının süresinin dolmasından sonra en az iki yıl süreyle saklanmaya devam eder.

Herhangi bir güvenlik olayı kaydı, olay gerçekleştikten sonra en az iki yıl süreyle saklanmaya devam eder.

Kamu SM, bu kayıtları yasalar ve/veya ETSI standartları gereğince daha uzun süre saklayabilir.

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 saklanması gereken yasal süre içerisinde silinmesine, değiştirilmesine veya imha edilmesine izin verilmez, bunun için gerekli güvenlik önlemleri alınır.
- 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 çevrimiçi yedeği alınmaktadır. Yedekleme ihtiyacını gidermek üzere teyp kütüphanesi ve yedekleme işlemlerini otomatikleştirmek için yedekleme yönetim yazılımı mevcuttur. Kritik kayıtlar coğrafi olarak ayrı bir şehirde bulunan güvenli felaket kurtarma merkezlerine yedeklenmektedir.

5.4.6. Kayıtların Toplanması

Kayıtlar uygulama katmanında, ağ katmanında ve işletim sistemi düzeyinde 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.

Zafiyetlerin değerlendirilmesiyle ilgili detaylar Kamu SM Teknik Açıklık Yönetim Politikasında belirtilmektedir. Kamu SM bu politikaya uygun şekilde periyodik olarak zafiyet taraması ve sızma testi yapar. Kayıt altına alınan zafiyetler risk değerlendirme süreçlerine göre işlenir.

5.5. KAYIT ARŞİVLEME

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 ile bunların doğrulandığına ilişkin kayıtlar
- Sertifika üretimi ve iptal başvuruları sırasında elektronik veya kağıt ortamda alınan formlar
- Üretilen tüm sertifikalar
- Geçerlilik süresi dolan tüm Kamu SM kök ve alt kök sertifikaları
- Yayımlanan tüm sertifika iptal durum kayıtları
- Sertifika İlkeleri ve Sertifika Uygulama Esasları dokümanı
- Sertifika yönetim prosedürleri
- Sertifika Sahibi Taahhütnameleri
- Sertifikasyon süreçlerinde kullanılan sistemlerin NTP senkronizasyon logları

Kamu SM, sertifika sistemleri, sertifika yönetim sistemleri ve kök sertifika makamı sistemlerinin güvenliğine ilişkin belgeleri arşivler.

5.5.2. Arşivlerin Tutulma Süresi

Bölüm 5.5.1'de belirtilen arşivlenen bilgi ve belgeler, kayıt oluşturma zamanından itibaren en az 2 (iki) yıl süreyle veya yasalar ve/veya ETSI standartları uyarınca saklanmaları gereken süre boyunca (hangisi daha uzunsa) saklanır.

5.5.3. Arşivlerin Korunması

Arşivlenen bilgi ve belgeler izinsiz izlenmeyi, değiştirilmeyi ve silinmeyi engelleyecek şekilde elektronik ve fiziksel olarak güvenli ortamlarda tutulur. Arşivler yetkisiz çalışanların erişimine kapalıdır. Arşivlerin tutulduğu ortam Bölüm 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 İş Sürekliliği Politikası gereğince yedeklenir.

5.5.5. Kayıtların Zaman Damgası Gereksinimleri

Kamu SM gerekli gördüğü kayıtlara zaman damgası ekler. Zaman damgası yönteminden bağımsız olarak, tüm kayıtlarda olayın gerçekleştiği zamanı gösteren veriler bulunur.

5.5.6. Arşivlerin Toplanması

Arşivler elektronik veya kağıt ortamda ilgili Kamu SM prosedürlerine 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 DEĞİŞİMİ

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

- 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 https://kamusm.bilgem.tubitak.gov.tr internet adresi üzerinden duyurur.
- Yenilenen Kamu SM sertifikaları, Kök Programları ve/veya BR tarafından izin verilen süre içerisinde CCADB platformuna bildirilir.

5.7. GÜVENİLİRLİĞİN YİTİRİLMESİ VE ARIZA DURUMLARINDA YAPILACAKLAR

Bilgi sistemleri altyapısı olası güvenlik ihlaline karşı izlenmekte ve ihlal olayları raporlanmaktadır. Kritik güvenlik açığı tespit edildikten sonra en geç 48 saat içerisinde ele alınmaktadır. Kayıt fonksiyonunun başlatılması/durdurulması işlemleri ve ihtiyaç duyulan ağ hizmetlerinin durumu izlenmektedir.

5.7.1. Güvenilirliğin Yitirilmesi Durumunun Düzeltilmesi

Güvenilirliğin yitirilmesi durumlarında (olay veya güvenlik zayıflığı vb.), sertifika yönetim sisteminin en kısa zamanda yeniden güvenilir olarak çalışmaya başlaması ve zararlarının en aza indirgenmesi için Kamu SM'nin ilgili prosedürlerinde belirlenen süreçler işletilir. Varsa durumdan etkilenen taraflar 24 saat içerisinde haberdar edilir.

Kamu SM bünyesinde olası bir kriz, felaket veya güvenlik ihlali durumlarının gerçekleşmesi halinde operasyonları kesintiye uğratabilecek olaylara müdahale ve yönetim çerçevesi çizmek amacıyla İş Sürekliliği Planları hazırlanmıştır. İş Sürekliliği Planlarının test edilmesi, gözden geçirilmesi ve güncellenmesi yılda en az bir defa gerçekleştirilir.

5.7.2. Donanım, Yazılım veya Veri Bozulması Durumunda İzlenecek Prosedürler

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 olay yönetim süreci başlatılır.

İş sürekliliğini sağlamak için sistemde kullanılacak aktif cihazlar, sunucular ve depolama alan ağı bileşenleri yedekli yapıda çalışmaktadır ve kritik süreçler için felaket kurtarma merkezi oluşturulmuştur. Depolama ünitesi fiziksel olarak farklı 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 Durumunda İzlenecek Prosedürler

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

- Kamu SM kendisine ait sertifikanın iptal edildiğini, iptal sebebi ile birlikte en hızlı şekilde https://kamusm.bilgem.tubitak.gov.tr internet adresi üzerinden duyurur ve ilgili kurumları yazıyla bilgilendirir.
- İptal edilen Kamu SM sertifikaları, Kök Programları ve/veya BR tarafından izin verilen süre içerisinde CCADB platformuna bildirilir.
- 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 yeni 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 Planlarında tanımlar.

Kamu SM başka bir şehirde felaket kurtarma merkezine sahiptir. Kamu SM Yedekleme Yönetim Politikasına uygun olarak önemli veri ve uygulamaların yedeklerini almakta ve gerekli durumlarda yedekten geri dönme işlemlerini uygulamaktadır. 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 Planlarını periyodik olarak gözden geçirir ve test eder. Kamu SM arıza durumlarının tekrarlanmaması için gerekli önlemleri alır.

5.8. SERTİFİKA HİZMETLERİNİN SONLANDIRILMASI

Kamu SM sertifika hizmetlerinin başka bir ESHS'ye devretmeden sonlandırılması durumunda Kamu SM, Sertifika Hizmetleri Sonlandırma Planı çerçevesinde aşağıdaki işlemleri yerine getirir:

- Sertifika hizmetlerine son vereceği tarihten en az 3 (üç) ay önce durumu sertifika hizmeti verdiği kurumlara ve bağlı olduğu üst mercilere 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 Bölüm 5.5.1'de belirtilen süre boyunca korur.

Kamu SM hizmetlerinin başka bir ESHS'ye devredilmesi durumunda devir işlemi Kamu SM Sertifika Hizmetleri Sonlandırma Planı çerçevesinde gerçekleştirilir. Plan kapsamında ESHS özel anahtarları, kayıtlar, loglar ve kritik dokümanlar belirlenen ESHS'ye gerekli güvenlik önlemleri alınarak standartlara uygun şekilde devredilir.

6. TEKNİK GÜVENLİK KONTROLLERİ

Kamu SM'nin kendi anahtar çiftleri ve erişim verilerini ürettiği, tüm sertifika yönetim işlemlerini gerçekleştirdiği sistemler ETSI EN 319 401, ETSI EN 319 411-1 ve CA/B Forum Baseline Requirements gereklerini sağlar.

6.1. ANAHTAR ÇİFTİ ÜRETİMİ VE KURULUMU

6.1.1. Anahtar Çifti Üretimi

Kök ve alt kök makamlara ait anahtar çiftleri, yetkisi olmayan personelin giremeyeceği güvenli odada, ağ ortamına kapalı sistemlerde, güvenli anahtar üretimi için gereken testlerden geçmiş, FIPS PUB 140-2 Seviye 3 veya EAL4+ standartlarını sağlayan güvenli yazılım ve/veya donanım kullanılarak güvenilir rollerdeki birden fazla eğitimli personel tarafından 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 EN 319 411-1 ve BR dokümanlarının gereklilikleri yerine getirilir.

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

SSL sertifikaları için anahtar çifti üretimi sertifika talep eden tarafça gerçekleştirilir. Kamu SM son kullanıcı için anahtar çifti üretmez ve gönderilen CSR dosyası için aşağıdakilerden birinin ortaya çıkması durumunda sertifika isteklerini reddeder:

- Anahtar çiftinin Bölüm 6.1.5 veya Bölüm 6.1.6'da belirtilen gereksinimleri karşılamaması,
- Özel anahtarın üretiminde kullanılan yöntemin hatalı/zayıf olduğuna dair kanıt elde edilmesi,
- Özel anahtarın ele geçirilmesine sebep olacak bir metot ortaya çıktığına dair kanıt bulunması,
- Daha önce aynı anahtarın ele geçirildiğinden haberdar olunması,
- Anahtarın kolaylıkla ele geçirilebileceğine dair kanıt bulunması (Debian zayıf anahtar gibi).

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, sertifika başvuru sürecinde 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.

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 en az 2048 bittir ve 8'e bölünebilirdir. ECC anahtar boyu en az 256 bittir; yalnızca NIST P-256 ve NIST P-384 eğrilerinin kullanımına izin verilmektedir. Burada belirtilenler haricinde algoritma veya anahtar boyu kullanımına izin verilmemektedir.

6.1.6. Anahtar Üretim Parametreleri ve Kalitesinin Kontrolü

Kamu SM, CA/B 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/veya "Genişletilmiş Anahtar Kullanımı" uzantısı içerisinde belirtilir.

Kamu SM kök anahtarı, alt kök sertifikası ve SİL imzalamak için kullanılır. Kamu SM SSL sertifikalarının imzalanmasında kullanılan sertifika zinciri Ek-A'da detaylı olarak bulunmaktadır. OCSP cevaplarının imzalanmasında alt kök ve kök tarafından yetkilendirilmiş OCSP sertifikası kullanılır.

6.2. ÖZEL ANAHTARIN KORUNMASI

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 belirtilen güvenlik standartlarından en az birisini sağlar: FIPS PUB 140-2'ye göre Seviye 3 (veya üzeri) veya ISO/IEC 15408'e göre EAL4 (veya üzeri).
- Kullanım süresi dolan ve/veya arızalanan kriptografik modüller güvenli bölge dışına çıkarılamaz ve bilgi varlıkları imha prosedürü gereğince imha edilir.

6.2.2. Özel Anahtara Birden Fazla Kişi Kontrolünde Erişim

Kamu SM'ye ait özel anahtarın bulunduğu odaya erişim, güvenilir rollerde yer alan 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

Uygulanmamaktadır.

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 özel anahtarları arşivlemez.

6.2.6. Özel Anahtarın Kriptografik Modüle/Modülden Taşınması

Taşıma işlemi, güvenilir yöntemlerle şifreli olarak ve birden fazla yetkili personelin denetiminde yerine getirilir. Taşıma işlemi esnasında yetkisiz personel ya da organizasyon tarafından özel anahtarın güvenliğine dair bir zafiyet oluşması durumunda özel anahtar kullanılarak üretilmiş tüm sertifikalar iptal edilir.

6.2.7. Özel Anahtarın Kriptografik Modülde Saklanması

Kamu SM'ye ait özel anahtarlar, yetkisiz kişilerin erişimine kapalı, FIPS PUB 140-2 Seviye 3 veya EAL4+ 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. Kamu SM anahtarları donanım güvenlik modülü üreticisi tarafından sağlanan talimatlara ve belgelere uygun olarak aktifleştirilir.

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 ÇİFTİ YÖNETİMİYLE İLGİLİ DİĞER KONULAR

6.3.1. Açık Anahtarın Arşivlenmesi

Kamu SM ve son kullanıcı açık anahtarları sertifikaların içinde yer alır ve sertifikalar Bölüm 5.5'de belirtilen şekilde arşivlenmektedir. Sertifika arşivleri yetkisiz kişiler tarafından müdahale edilmeye ve silinmeye karşı gerekli tedbirlerin alındığı bir ortamda tutulmaktadır.

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. SSL sertifikalarının kullanım süresi 398 günü aşamaz. SSL sertifikalarının süresi, Kamu SM alt kök sertifikasının kullanım ömrünü geçemez.

6.4. ERİŞİM VERİLERİ

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 PUB 140-2 Seviye 3 veya EAL4+ 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. BİLGİSAYAR GÜVENLİĞİ DENETİMLERİ

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. Sertifika üretim süreçlerinde sistemlere girişlerde çok faktörlü doğrulamalar yapılır. Her kurulan yazılımın yedek kopyası yaratılır ve sistemin güvenliği konusunda bütün iyileştirme eylemleri gecikmesiz uygulanır. Güvenlik yamaları değerlendirilip daha büyük bir riske sebebiyet vermesi durumunda yüklenmez ve risk süreç takip sistemi üzerinde kayıt altına alınır. Ağ bileşenleri ve konfigürasyonları dönemsel olarak Ağ Güvenliği Prosedürüne göre kontrol edilir.

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 kayıt tutma faaliyetleri gerçekleştirilir.

6.5.2. Bilgisayar Sisteminin Sağladığı Güvenlik Seviyesi

Düzenlenmesine gerek duyulmamıştır.

6.6. YAŞAM DÖNGÜSÜ TEKNİK KONTROLLERİ

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 GÜVENLİĞİ KONTROLLERİ

Son teknolojik gelişmeler göz önünde bulundurularak gerekli ağ güvenliği kontrolleri yapılır. Sertifikasyon işlemlerinde ağlar arası gereksinim duyulmayan protokoller güvenlik duvarları ile engellenmiştir. 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 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. Farklı güvenilir sistemlerle iletişim ihtiyacı olması durumunda, diğer iletişim kanallarından mantıksal olarak farklı olan güvenilir iletişim kanalları kurulur.

Yüksek güvenlik gerektiren işlemlerin yapıldığı sistemler (kök ve alt kök sunucuları gibi) için farklı ağ segmentleri oluşturulmuştur. Kök sunucuları kapalı halde tutulmaktadır. Bu sunucular, yalnızca Kamu SM'nin sistem, ağ ve erişim prosedürlerinde tanımlı gerekli durumlarda açılmakta ve işlemler tamamlandığında tekrar kapatılmaktadır. Canlı ortam servis ve sistemleri, geliştirme ve test ortamlarından ayrılmıştır. Güvenli ve yüksek güvenli bölgelere erişimler erişim kontrol protokolüne göre belirlenir. Yüksek güvenlik gerektiren sistemlerde kullanılan donanımlar farklı yerlerde tekrar tekrar kullanılmaz, imha edilirler.

Bilgi işlem yöneticileri, uygulama geliştiricileri gibi farklı çalışan gruplarına ait farklı amaca hizmet eden ağlar da birbirinden ayrılmıştır. Sistemlerdeki ayrıcalıklı erişim hesaplarına yetkiler güvenlik ekibince kontrollü olarak verilir ve kayıtlar üzerinden izlenir. Farklı bölgelere olan iletişim ve erişim engellendiği gibi gerekli olmayan bağlantı ve hizmetler de ağ güvenliği açısından devre dışı bırakılır.

Güvenlik politikası yönetim uygulamaları farklı amaçlarda kullanılmaz. Kök ve alt kök üzerinde bulunan gereksiz hesaplar, uygulamalar, hizmetler, port ve protokoller Kamu SM Sıkılaştırma Prosedürüne göre

kaldırılır ya da devre dışı bırakılır. Ağ ve sistem güvenliğine dair tüm işlemler siber olaylara müdahale ekibi tarafından izlenir ve gerektiğinde olay müdahale süreçleri doğrultusunda aksiyon alınır. Kamu SM çevrimiçi açık anahtar altyapısı hizmetlerinin devamlılığı için Kamu SM ana merkez ve felaket kurtarma merkezinin dış ağ bağlantı hizmetlerini yedekli olarak kurgulamıştır.

Sistemler üzerinde periyodik olarak zafiyet taramaları ve yılda en az bir kez penetrasyon testi yapılır. Penetrasyon testini yapan kişi veya kurum; test metot ve araçlarını, testleri yapan kişilerin yetkinliklerini içeren raporlar hazırlar. Bu raporlar Kamu SM tarafından saklanır. Sistemlerin belirlenen kural setlerine uygunluğu düzenli olarak gözden geçirilir.

6.8. ZAMAN DAMGASI

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. SERTİFİKA PROFİLLERİ

Bu bölümde Kamu SM tarafından oluşturulan kök, alt kök ve SSL sertifikalarının 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.

BR'a uygun olarak ön sertifikalar doğrudan alt kök makamı tarafından yayımlanır.

Sertifika seri numaraları, kriptografik sistemlerde kullanılmak üzere tasarlanmış bir rastgele sayı üreteci tarafından oluşturulmuş en az 64 bit çıktı içeren sıfırdan büyük 2^{159}'dan küçük bir sayıdır. RFC 5280'e bir istisna olarak, bir SSL ön sertifikası ile ilişkili asıl SSL sertifikasının seri numaraları aynıdır.

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

7.1.1. Sürüm Numarası

Kamu SM, X.509 v3 ile uyumlu olarak sertifika yayımlar.

7.1.2. Sertifika Alanları ve Uzantıları

Kamu SM tarafından üretilen sertifikalar IETF RFC 5280 uyarınca zorunlu alanların yanı sıra X.509 v3 sertifika uzantılarını da içerir.

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

7.1.3. Algoritma Nesne Tanımlayıcıları

Kamu SM, BR Bölüm 7.1.3 ile uyumlu imza algoritmaları ve kodlaması kullanır.

Kamu SM tarafından oluşturulan tüm sertifikaların, SİL'lerin ve OCSP cevaplarının imzalanmasında "RSA with SHA-256" algoritması (OID = {1 2 840 113549 1 1 11}) kullanılır.

7.1.4. İsim Biçimleri

Kamu SM, RFC 5280 ve BR Bölüm 7.1.4 ile uyumlu isim biçimlerine sahip sertifikalar yayımlar.

SSL sertifikalarının *Subject* alanında yer alan öznitelikler sırasıyla *countryName*, *stateOrProvinceName*, *organizationName* ve *commonName*'dir. Her bir özniteliğin içeriği Bölüm 3.1.5'te belirtilmiştir. Kamu SM tarafından oluşturulan kök, alt kök ve SSL sertifikalarının isim biçimleri EK-A'da bulunmaktadır. Kamu SM, IP adreslerine veya iç sunucu adreslerine sertifika vermemektedir.

7.1.5. İsim Kısıtları

Kamu SM, ".tr" ccTLD ile biten alan adına sahip kamu kurum ve kuruluşlarına OV SSL sertifikası hizmeti vermektedir. Bunun dışındaki ccTLD'ler için SSL sertifikası verilmemektedir.

7.1.6. Sertifika İlkeleri Nesne Tanımlayıcısı

Kamu SM tarafından üretilen SSL sertifikalarının "Sertifika İlkeleri" uzantısında CA/B Forum OV SSL OID (2.23.140.1.2.2) ve Kamu SM OV SSL OID (2.16.792.1.2.1.1.5.7.1.3) kullanılmaktadır.

Kamu SM tarafından oluşturulan sertifikalarda kullanılan 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 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 PROFİLİ

Kamu SM, IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" dokümanına ve CA/B Forum Baseline Requirements dokümanında belirtilen profile uygun olarak SİL oluşturur.

Kamu SM tarafından yayımlanan SİL'lerde temel olarak yayımcı bilgileri, SİL numarası, SİL'in yayımlanma tarihi, bir sonraki SİL'in yayımlanacağı tarih ve iptal edilen sertifikaların seri numaraları ile iptal zamanları yer alır.

7.2.1. Sürüm Numarası

Kamu SM'nin ürettiği SİL'ler RFC 5280 uyarınca versiyon 2 formatına uygundur.

7.2.2. SİL ve SİL Kayıt Uzantıları

Kamu SM tarafından üretilen SİL'lerde 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

*Kamu SM tarafından SSL sertifikalarının iptalinde kullanılan sebep kodları öncelik sırasına göre aşağıda listelenmiştir:

1. RFC 5280 CRLReason #1: keyCompromise
2. RFC 5280 CRLReason #9: privilegeWithdrawn
3. RFC 5280 CRLReason #5: cessationOfOperation
4. RFC 5280 CRLReason #3: affiliationChanged
5. RFC 5280 CRLReason #4: superseded

Sertifika sahibi, SSL İptal Başvuru Formunda belirtilen iptal sebeplerinden birini seçerek iptal talebinde bulunmalıdır. Birden fazla iptal sebebinin geçerli olması durumunda yüksek önceliğe sahip olan iptal sebebi seçilmelidir. Kamu SM, SSL sertifikalarının aşağıda belirtilen sebeplerden biri nedeniyle iptal edilmesi durumunda, SİL dosyasında sertifikaya karşılık gelen girdiye "CRLReason/ReasonCode" niteliği eklemektedir. Kullanımına izin verilen iptal sebepleri ve SİL sebep kodlarının hangi durumlarda kullanılacağı aşağıda açıklanmıştır:

- **Sertifika Özel Anahtarının Kaybolması/Çalınması** (keyCompromise): Sertifikada yer alan açık anahtara karşılık gelen özel anahtarın kaybedilmesi, silinmesi ya da yetkisiz kişilerce ele geçirildiğinin anlaşılması durumunda seçilecek iptal sebebidir.
- **Alan Adı Sahipliğinin/Kullanımının Sona Ermesi** (cessationOfOperation): Sertifikanın geçerlilik süresi sona ermeden önce sertifikalandırılan alan adına ait sahipliğin sona ermesi ya da ilgili alan adını içeren web sitesinin artık kullanılmaması durumunda seçilmelidir.
- **Sertifika İçeriğinde Yer Alan Bilgilerin Değişmesi** (affiliationChanged): Sertifika başvurusu sırasında verilen ve sertifika içeriğine yazılan bilgilerde (Kurum adı, il vb.) değişiklik olması durumunda seçilmelidir.
- **Sertifikanın Hatalı Üretilmesi** (superseded): Üretilen sertifikadaki geçerlilik tarihi, yayımcı ve sertifika sahibi bilgileri vb. alanlarda yer alan bilgilerde ya da sertifika yapısında hata bulunduğunun fark edilmesi durumunda seçilecek iptal sebebidir.
- **Yeni Sertifika Talebi** (superseded): Sertifika sahibinin mevcut sertifikasının yerine yeni bir sertifika talep etmesi durumunda mevcut sertifikasının iptal edilmesi için kullanılmalıdır.
- **Diğer** (RFC 5280 CRLReason #0: unspecified): Yalnızca yukarıda belirtilen iptal sebeplerinden herhangi birinin kullanılabilir olmadığı durumda seçilmelidir.

"*privilegeWithdrawn*" iptal kodu, sertifika sahibinin sertifika talebinde yanıltıcı bilgi sağlaması veya Sİ/SUE ve SSL Başvuru Formu ve Taahhütnamesi kapsamındaki önemli yükümlülüklerini yerine getirmemesi gibi durumlarda kullanılmaktadır. Bu iptal sebebinin oluşma durumu kullanıcı tarafından değil Kamu SM tarafından belirleneceğinden sertifika sahibine bir iptal sebebi olarak sunulmamaktadır.

Bu iptal sebebi nedeniyle sertifika iptali gerçekleştirildiğinde SİL dosyasında sertifikaya karşılık gelen girdiye "*CRLReason/ReasonCode*" niteliği eklenmektedir.

"*Diğer*" iptal sebebi, belirtilen iptal sebeplerinden birinin uygulanabilir olmadığı durumlar için kullanıcıya varsayılan seçenek olarak sunulmaktadır. Sertifika sahibinin "*Diğer*" iptal sebebini seçmesi durumunda SİL dosyasına ilgili sertifika için "*CRLReason/ReasonCode*" niteliği eklenmemektedir.

Kamu SM, SİL girdisi mevcutta "*ReasonCode*" niteliği içermeyen veya "*keyCompromise*" olmayan "*ReasonCode*" niteliğine sahip bir sertifika için özel anahtar güvenliğinin ihlal edildiğine dair bir kanıt elde ettiğinde, SİL girdisini "*keyCompromise*" olacak şekilde güncelleyecektir. Ayrıca, sertifikanın özel anahtarının, o sertifikaya karşılık gelen SİL girdisinde belirtilen iptal tarihinden önce ele geçirildiğini belirlediğinde, SİL girdisindeki iptal tarihini güncelleyecektir.

Kamu SM'ye ait alt kök sertifikaların iptal edilmesi durumunda SİL dosyasında sertifikaya karşılık gelen girdiye uygun "*CRLReason*/*ReasonCode*" niteliği eklenmektedir.

7.3. OCSP PROFİLİ

Kamu SM, OCSP desteğini IETF RFC 6960: "Internet X.509 Public Key Infrastructure Online Certificate Status Protocol - OCSP" dokümanına uygun olarak sunar. Kamu SM tarafından üretilen OCSP Yanıtlayıcı Sertifikaları CA/B Forum Baseline Requirements dokümanında belirtilen profile uygun olarak oluşturulur.

İptal olmuş alt kök için üretilen OCSP cevaplarında *revocationReason* alanı bulunur. İptal sebebi olarak belirtilen *CRLReason,* SİL'ler için Bölüm 7.2.2'de tanımlanan geçerli bir değer içerir.

7.3.1. Sürüm Numarası

Kamu SM, RFC 6960'a uygun olarak versiyon 1 OCSP cevaplarını destekler.

7.3.2. OCSP Uzantıları

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

OCSP cevabının *singleExtensions* alanında *reasonCode* SİL girdisi uzantısı bulunmaz.

8. UYGUNLUK DENETİMLERİ VE DİĞER DEĞERLENDİRMELER

Bu Sİ/SUE dokümanındaki politika ve prosedürler, ETSI EN 319 411-1 ve CA/B Forum the BRs dokümanlarının son sürümleri ile Bölüm 1'de listelenen diğer programlar dahil olmak üzere genel kabul görmüş endüstri standartlarının gereksinimlerine uyacak şekilde tasarlanmıştır.

8.1. UYGUNLUK DENETİMİNİN SIKLIĞI

Uygunluk denetimleri, ETSI EN 319 411-1 standardı ve CA/B Forum Baseline Requirements kapsamında yetkili bir denetçi kurum tarafından yıllık olarak iki denetim periyodu arasında boşluk kalmayacak şekilde yapılmaktadır. Denetim periyodu bir yılı aşamaz. Bu denetimlerin kapsamı OV SSL ile sınırlıdır.

Bilgi güvenliği denetimleri, ISO 27001 kapsamında yapılan BGYS denetimleri ve güvenilir personel tarafından yapılan iç denetimlerden oluşur.

8.2. DENETÇİNİN NİTELİKLERİ

Denetim otoritesi, ETSI EN 319 403 standardında belirtilen nitelikleri sağlayan ISO 17065 kapsamında akreditasyonu bulunan denetçi kurumlar arasından seçilir. Ek olarak, nitelikli denetçiler Kök Programları ve BR tarafından belirtilen kriterleri sağlamalıdır.

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. DENETÇİNİN DENETLENEN TARAFLA OLAN İLİŞKİSİ

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

8.4. DENETİMİN KAPSAMI

Kamu SM, ETSI EN 319 401'e normatif referanslar içeren ETSI EN 319 411-1 standardının güncel sürümü uyarınca yıllık olarak denetimden geçer.

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 dokümanlara uygun işletimi,
- Personel yetkinlikleri,
- Görevler ayrılığı prensiplerine uygunluklar,
- Sİ/SUE, ISO 27001, ETSI EN 319 401, ETSI EN 319 411-1 ve CA/B Forum Baseline Requirements'e uygunluk denetlenir.

8.5. EKSİKLİĞİN TESPİTİ DURUMUNDA YAPILACAKLAR

Denetim sırasında Kamu SM'nin, Sİ/SUE dokümanının veya ilgili standartların 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.

8.6. SONUCUN BİLDİRİLMESİ

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

Denetim raporu denetim periyodunun bitiminden sonra en geç 3 (üç) ay içerisinde Kamu SM web sitesinden veya denetçi firmanın web sitesinden yayımlanır.

8.7. İÇ DENETİM

Kamu SM, SSL sertifikalarının CP/CPS ve BR ile uygunluğunu son iç denetimden bu yana verdiği sertifikaların en az yüzde üçünü kapsayacak şekilde rastgele seçilen örnekler üzerinden en az üç ayda bir SSL iç denetimleriyle kontrol eder.

9. DİĞER İŞLER VE HUKUKSAL MESELELER

9.1. ÜCRETLENDİRME

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, ürettiği sertifikalar için iptal ücreti talep etmez.

Kamu SM, SİL veya OCSP aracılığıyla sertifikanın geçerlilik durumunu kontrol etmek için herhangi bir 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 ücret talep etmez.

9.1.5. İade Ücreti

Sertifika sahibi, Bölüm 4.4.1'de belirtilen süre içerisinde sertifikasını ilk teslim aldığında yaptığı kontrollerde sertifikasını kullanamadığını tespit ederse ve sorunun Kamu SM'den kaynaklanan bir hata sebebiyle ortaya çıktığı anlaşılırsa talebi halinde sertifika sahibinin sertifika için ödediği ücret iade edilir.

9.2. FİNANSAL SORUMLULUK

Kamu SM'nin, kanundan doğan yükümlülüklerini yerine getirmemesi sonucu doğacak zararların karşılanması amacıyla yaptırmakla yükümlü olduğu Sertifika Mali Sorumluluk Sigortası ve Kamu SM bünyesinde ayrılan mali kaynak kapsamında sertifika alan kamu kurumları teminat altındadır.

9.3. TİCARİ BİLGİNİN KORUNMASI

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.

Özel anahtarlar, özel anahtara veya ESHS sistemlerine erişmek için kullanılan veriler, iş sürekliliği ve felaket kurtarma planları denetim kayıtları ve Kamu SM'nin hizmete özel prosedür/politika dokümanları gizli olarak kabul edilir ve ifşaya karşı makul düzeyde korunur.

9.3.2. Gizlilik Kapsamında Olmayan Bilgileri

Kamu SM tarafından http://depo.kamusm.gov.tr/ilke adresinden yayımlanan her türlü doküman 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. KİŞİSEL BİLGİNİN GİZLİLİĞİ

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. Kamu SM, 6698 sayılı Kişisel Verilerin Korunması Kanunu'na uygun olarak ilgili taraflara bilgilendirme yapmaktadır.

9.4.2. Gizli 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. Gizli Olarak Tanımlanmayan Bilgiler

Kamu SM tarafından 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.

Kamu SM, Kişisel Verilerin Korunması Kanunu kapsamında kurumsal web sayfası üzerinden bilgilendirme yapmaktadır.

9.4.5. Gizli Bilginin Kullanımına İzin Verilmesi

Kamu SM sertifika sahibinin rızasını aldıktan sonra veya yürürlükteki yasalar gereğince gizli bilgileri üçüncü taraflarla paylaşabilir.

9.4.6. Yetkili Mercilerin 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. TELİF HAKLARI

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

9.6. BEYAN VE TAAHHÜTLER

Kamu SM, sertifika sahipleri ve üçüncü kişiler 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/SUE dokümanını 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,
- Başvuru sahibi kurumun kimlik doğrulamasını Sİ/SUE'de belirtilen prosedürler çerçevesinde doğrulamak,
- Kurum yetkilisinin sertifika talep eden kurum adına yetkili olduğunu Sİ/SUE'de belirtilen prosedürler çerçevesinde doğrulamak,
- Başvuru sahibinin sertifikada listelenen alan adı/adlarını kullanım hakkına veya kontrolüne sahip olduğunu Sİ/SUE dokümanında belirtilen prosedürler çerçevesinde doğrulamak,
- Sertifikaların içeriğindeki bilgilerin doğruluğunu sağlamak,
- Gerekli başvuru şartlarını sağlamayan başvuru sahiplerine sertifika vermemek,

- Sertifika başvurularını değerlendirerek, başvurunun sonucu hakkında başvuru sahiplerini bilgilendirmek,
- Sertifika yenileme başvurularını Sİ/SUE'de belirtilen şekilde kabul etmek,
- Sertifika iptal başvurularını Sİ/SUE'de belirtilen prosedürler çerçevesinde kabul etmek ve Sİ/SUE'de belirtilen herhangi bir nedenin ortaya çıkması durumunda sertifikayı iptal etmek,
- Sİ/SUE dokümanı ile SSL Başvuru Formu ve Taahhütnamesine 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 7 gün 24 saat sağlamak için her türlü tedbiri almak,
- Sertifika üretim, yönetim ve iptali ile ilgili yapılan tüm işlemlerin kaydını tutmak,
- Tüm kağıt ve elektronik kayıtları Sİ/SUE'de belirtilen süreler boyunca güvenli olarak saklamak.

9.6.2. Kayıt Birimi Beyan ve Taahhütleri

Kayıt birimlerinin sorumlulukları şunlardır:

- Sertifika başvurularının alınması,
- Sertifika başvuru sahibinin kimlik bilgilerinin Sİ/SUE'de belirtilen yöntemlerle gerekli belgelere dayanarak tespiti,
- Sertifika sahibinden gerekli belgelerin ve bilgilerin alınması,
- Sertifika istek dosyasının kontrol edilmesi,
- Doğrulanan sertifika isteklerinin Kamu SM'nin ilgili birimlerine iletilmesi,
- Üretilen SSL sertifikalarının sahiplerine iletilmesi,
- Sertifika iptal başvurularının alınması,
- Doğrulanan sertifika iptal başvurularının Kamu SM'nin ilgili birimlerine iletilmesi,
- İptal edilen sertifikalar hakkında sahiplerinin bilgilendirilmesi.

9.6.3. Sertifika Sahibi Beyan ve Taahhütleri

Kamu SM, SSL Başvuru Formu ve Taahhütnamesinin bir parçası olarak, başvuru sahibinin bu bölümdeki beyan ve taahhütleri kabul etmesini zorunlu kılar.

Başvuru sahibinin sertifika talebinde bulunurken SSL Başvuru Formu ve Taahhütnamesini kabul etmesi gerekir. Taahhütname, burada belirtilenlere ek beyan ve taahhütler içerebilir.

Sertifika/başvuru sahibinin yükümlülükleri şunlardır:

- Sertifika başvuru, iptal ve diğer işlemleri Sİ/SUE'de belirtildiği şekilde, detayları Kamu SM sertifika yönetim prosedürlerinde anlatılan usule uygun biçimde yerine getirmek,
- Sertifika başvurusu ve iptal işlemleri sırasında ve sertifika yönetim süreçleri kapsamında Kamu SM tarafından talep edildiği diğer durumlarda doğru bilgi beyan etmek,
- Verilen sertifikadaki bilgilerin doğruluğunu kontrol etmek,
- Özel anahtarın güvenliğini ve gizliliğini sağlamak, uygun şekilde korumak için gerekli önlemleri almak,

- Özel anahtarın fiili veya şüpheli bir şekilde kötüye kullanılması veya gizliliğinin yitirilmesi durumunda sertifikanın iptal edilmesi için Kamu SM'ye en kısa zamanda başvurmak,
- Sertifikanın içeriğinde bulunan bilgilerin yanlış veya hatalı olduğunun fark edilmesi veya değişmesi durumunda derhal sertifikanın iptal edilmesi için Kamu SM'ye başvurmak ve sertifika kullanımına derhal son vermek,
- Özel anahtarın gizliliğinin yitirilmesi durumunda sertifika kullanımına derhal son vermek,
- İptal olmuş veya geçerlilik süresi dolmuş sertifika ile işlem yapmamak,
- Kamu SM'nin sertifikanın kötüye kullanımı veya anahtarın ele geçirilmesiyle ilgili talimatlarına makul süre içerisinde yanıt vermek,
- Verilen sertifikayı, yalnızca sertifika içerisinde belirtilen alan adlarında kullanmak,
- Sertifikayı yürürlükteki tüm yasalara uygun olarak, SSL Başvuru Formu ve Taahhütnamesinde ve Sİ/SUE'de belirtilen şartlar dahilinde kullanmak,
- Başvuru sahibinin SSL Başvuru Formu ve Taahhütnamesinde belirtilen koşulları ihlal etmesi veya Sİ/SUE veya BR tarafından sertifikanın iptalinin gerekmesi durumunda Kamu SM'nin sertifikayı derhal iptal etme hakkına sahip olduğunu bilmek ve kabul etmek.

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, sertifikalara güvenerek işlem yapmadan önce sertifikanın aşağıda belirtilen geçerlilik kontrollerini yapmakla yükümlüdür:

- Sertifikaları kullanmak için gerekli teknik yeterliliğe sahip olmak,
- ESHS ve son kullanıcı sertifikalarının geçerliliğini doğrulamak ve SİL veya OCSP kullanarak iptal kontrollerini gerçekleştirmek,
- Sertifikanın tanımlanan veriliş amacına uygun olarak kullanıldığını doğrulamak,
- Sertifikanın kullanımına ilişkin olarak sertifika içerisinde veya Sİ/SUE'de belirtilen her türlü sınırlamayı dikkate almak,
- Sertifikanın kullanım süresinin dolup dolmadığını kontrol etmek.

Sertifikaya yetkisiz olarak güvenilmesinin riski ilgili tarafa aittir.

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 Başvuru Formu ve Taahhütnamesinde belirtildiği şekilde sona erer.

9.8. SORUMLULUKLA İLGİLİ SINIRLAMALAR

Kamu SM, sertifikaları CA/B Forum Temel Gereksinimlerine ve bu Sİ/SUE dokümanına uygun olarak ürettiği ve yönettiği ölçüde, söz konusu sertifikanın kullanılması veya bu sertifikaya güvenilerek işlem yapılması sonucu uğranılan herhangi bir zarardan dolayı sertifika sahibine veya herhangi bir üçüncü tarafa karşı sorumlu olmayacaktır.

Kamu SM'nin tüm sorumluluğu fiili ve yasal olarak kanıtlanabilir zararlarla sınırlıdır.

Kamu SM ve sertifika sahiplerinin sorumlulukları ile ilgili sınırlamalar SSL Başvuru Formu ve Taahhütnamesinde belirtilir.

9.9. TAZMİNAT HALLERİ

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

9.10. SÜRE VE FESİH

9.10.1. Süre

Bu Sİ/SUE dokümanı, Kamu SM web sitesinde/bilgi deposunda yayımlandığında yürürlüğe girer ve daha yeni bir sürüm yayımlanana kadar yürürlükte kalır.

9.10.2. Fesih

Bu Sİ/SUE dokümanı, daha yeni bir sürüm yayımlanana kadar yürürlükte kalır.

9.10.3. Fesihin Etkileri

Bu Sİ/SUE dokümanı feshedilse dahi sertifika sahipleri söz konusu sertifikalarının geçerlilik süreleri dolana kadar buradaki hükümlere bağlı kalmaya devam eder.

SSL Başvuru Formu ve Taahhütnamesinin kullanımının sona ermesiyle hizmeti alan kurumun, Sİ/SUE dokümanında belirtilen şartları sağlamakla ilgili yükümlülükleri ortadan kalkar.

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

9.11. SİSTEM BİLEŞENLERİ İLE HABERLEŞME VE KİŞİSEL BİLGİLENDİRME

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

9.12. DEĞİŞİKLİK HALLERİ

9.12.1. Değişiklik Prosedürü

Kamu SM tarafından hazırlanan bu Sİ/SUE dokümanı yıllık olarak gözden geçirilir. İhtiyaç olması halinde daha sık gözden geçirilebilir. Bu dokümanlarda yapılabilecek değişiklikler ekleme ve değiştirme şeklinde olabileceği gibi, Kamu SM dokümanların tamamen yenilenmesine de karar verebilir. Sİ/SUE dokümanında yapılan değişiklikler uygun numaralandırma ile doküman içerisinde belirtilir. Dokümandaki değişiklikler Sİ/SUE'nin güncellenmiş sürümünün Kamu SM Bilgi Deposunda yayınlanmasıyla yapılır.

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. Sİ/SUE'nin geçerlilik tarihi doküman içerisinde belirtilir. Yenilenen dokümanlar makul bir süre içerisinde bilgi deposundan yayımlanır.

9.12.3. Nesne Tanımlama Numarasının Değişmesini Gerektiren Durumlar

Düzenlenmesine gerek duyulmamıştır.

9.13. ANLAŞMAZLIK HALLERİ

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

9.14. UYGULANACAK HUKUK

Bu Sİ/SUE dokümanı, Türkiye Cumhuriyeti'nin yürürlükteki tüm uygulanabilir yasa ve yönetmeliklerine tabidir. Sİ/SUE'nin uygulanmasında ve yorumlanmasında Türkiye Cumhuriyeti Hukuku geçerlidir.

9.15. UYGULANABİLİR YASALARLA UYUM

Kamu SM, sertifika sahibi ve ilgili tüm taraflar Türkiye Cumhuriyeti'nde yürürlükte olan tüm uygulanabilir yasa ve yönetmeliklere uymayı kabul eder. Sİ/SUE dokümanında geçen hükümlerin daha sonra yürürlüğe girecek ilgili mevzuata aykırı bulunması halinde dokümanda gerekli değişiklikler yapılarak uygun hale getirilir.

9.16. ÇEŞİTLİ HÜKÜMLER

9.16.1. Tüm Sözleşmeler

Kamu SM ürün ve hizmetlerini kullanan her bir tarafın, ürün veya hizmete ilişkin şartları tanımlayan bir sözleşme yapmasını gerektirir.

9.16.2. Atama

Düzenlenmesine gerek duyulmamıştır.

9.16.3. Bölünebilirlik

Bu Sİ/SUE'nin herhangi bir hükmünün geçersiz veya uygulanamaz olduğu tespit edilirse, Sİ/SUE'nin geri kalanı geçerli ve uygulanabilir olmaya devam eder.

BR ile Türkiye'deki bir yasa veya yönetmelik arasında bir ihtilaf olması durumunda, Kamu SM CA/Browser Forum'u derhal bilgilendirecek ve BR Bölüm 9.16.3'te tanımlanan prosedürleri izleyecektir.

9.16.4. İcra (Avukatlık Ücretleri ve Haklardan Feragat)

Düzenlenmesine gerek duyulmamıştır.

9.16.5. Mücbir Sebepler

Kamu SM, yürürlükteki yasaların izin verdiği ölçüde bu Sİ/SUE kapsamındaki bir yükümlülüğün yerine getirilmesinde kendi makul kontrolü dışındaki bir olaydan kaynaklanan gecikme veya başarısızlıklardan sorumlu değildir.

9.17. DİĞER HÜKÜMLER

Düzenlenmesine gerek duyulmamıştır.

10. EK-A SERTİFİKA PROFİLLERİ

10.1. KAMU SM SSL KÖK SERTİFİKASI

Alan	Değer
Sürüm	V3
Seri Numarası	01
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	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	Kritik=Hayır; 65 3f c7 8a 86 c6 3c dd 3c 54 5c 35 f8 3a ed 52 0c 47 57 c8
Anahtar Kullanımı	**Kritik=Evet**; Sertifika İmzalama, SİL İmzalama
Temel Kısıtlamalar	**Kritik=Evet**; Konu Türü=CA; Yol Uzunluğu Kısıtlaması=Yok

10.2. KAMU SM SSL ALT KÖK SERTİFİKASI

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, SİL İmzalama
Temel Kısıtlar	**Kritik=Evet**; Konu Türü=CA; Yol Uzunluğu Kısıtlaması=0
Sertifika İlkeleri	Kritik=Hayır; [1] Sertifika İlkesi: İlke Tanımlayıcısı=All issuance policies [1,1] İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimliği=SUE 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	Kritik=Hayır; [1] SİL Dağıtım Noktası Dağıtım Noktası Adı: Tam Ad: URL=http://depo.kamusm.gov.tr/ssl/SSLKOKSIL.S1.crl
Yetkili Bilgi Erişimi	Kritik=Hayır; [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. OV SSL SERTİFİKA ŞABLONU

Alan	Değer
Sürüm	V3
Seri Numarası	En az 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	Sertifika üretim zamanı
Geçerlilik Sonu	Sertifika geçerlilik sonu
Konu	C = TR ST = Başvuru sahibinin bulunduğu il O = Başvuru sahibi kurum adı CN = Web sitesi DNS adı
Açık anahtar	RSA/ECC
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 İmza (RSA ve ECC için), Anahtar Şifreleme (Yalnızca RSA için)
Sertifika İlkeleri	Kritik=Hayır; [1] Sertifika İlkesi: İlke Tanımlayıcısı=2.23.140.1.2.2 [2] Sertifika İlkesi: İlke Tanımlayıcısı=2.16.792.1.2.1.1.5.7.1.3
Gelişmiş Anahtar Kullanımı	Kritik=Hayır; 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	Kritik=Hayır; [1] SİL Dağıtım Noktası Dağıtım Noktası Adı: Tam Ad: URL=http://depo.kamusm.gov.tr/ssl/SSLSIL.S1.crl
Yetkili Bilgi Erişimi	Kritik=Hayır; [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	Kritik=Hayır; DNS Name=<alan adı 1> DNS Name=<alan adı 2> ... DNS Name=<alan adı n>
İmzalı Sertifika Zaman Damgası Listesi	Kritik=Hayır; RFC 6962'de belirtildiği gibi OCTET STRING olarak kodlanmış *SignedCertificateTimestampList* değerini içerir.