# Kamu SM
# SERTİFİKA UYGULAMA ESASLARI
# (NİTELİKLİ ELEKTRONİK SERTİFİKA İÇİNDİR)

| Doküman Kodu | Yayın Numarası | Yayın Tarihi |
|---|---|---|
| **YONG-001-007** | **07** | **30.12.2010** |

## *DEĞİŞİKLİK KAYITLARI*

| Yayın No | Yayın Nedeni | Yayın Tarihi |
|---|---|---|
| 01 | İlk yayın | 28.03.2005 |
| 02 | RFC 3647 tam uyumluluğu için yeniden düzenleme yapıldı. | 06.06.2005 |
| 03 | Sİ ve SUE yayın adreslerinin ve tarihlerinin değiştirilmesi | 15.11.2005 |
| 04 | Sertifika yönetim süreçlerinde değişiklik yapılması<br>Kurum logosunda değişiklik yapılması<br>Nitelikli Elektronik Sertifika Taahhütnamesi'nin yönetim süreçlerine eklenmesi | 13.02.2007 |
| 05 | Planlı gözden geçirme sonrası küçük değişiklikler yapıldı. | 07.05.2008 |
| 06 | BTK denetimi sonrası, kapsamlı bir güncelleme yapıldı. | 05.10.2009 |
| 07 | Sertifikaların askıya alınması ve kullanıma açılması ile ilgili hususlar tekrar düzenlendi. | 30.12.2010 |

# İÇİNDEKİLER

## 1. Giriş

Bu doküman, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu'na (TÜBİTAK) bağlı Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM) tarafından oluşturulan Kamu Sertifikasyon Merkezi'nin (Kamu SM) nitelikli elektronik sertifika (NES) hizmeti verirken uyguladığı esasları tanımlayan Sertifika Uygulama Esasları (SUE) dokümanıdır.

Kamu SM, 15 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza Kanunu, Telekomünikasyon Kurumu'nun yayımladığı Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik, Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de tanımlandığı şekliyle Elektronik Sertifika Hizmet Sağlayıcısı (ESHS) işlevlerini yerine getirir.

Kamu SM açık anahtarlı altyapı mimarisi içinde, en üst seviyede bir Kök Sertifika Hizmet Sağlayıcısı (Kök SHS) ile buna bağlı olarak çalışan iki ayrı Sertifika Hizmet Sağlayıcısı bulunur. Sözü geçen Sertifika Hizmet Sağlayıcılar, Kamu Elektronik Sertifika Hizmet Sağlayıcısı (Kamu ESHS) ve Cihaz Sertifikası Hizmet Sağlayıcısı'dır. Kök SHS, sertifika sahipleri için sertifika üretmeyip, yürüttükleri görevler açısından özel niteliği haiz kamu kurum ve kuruluşları ile dileyen gerçek ve tüzel kişilerin kuracakları Elektronik Sertifika Hizmet Sağlayıcılarına kök sertifika, köprü veya çapraz sertifika hizmeti verir. Kamu ESHS, Kök SHS'nin imzasını taşıyan Elektronik Sertifika Hizmet Sağlayıcısı (ESHS) sertifikasına sahiptir. Kamu ESHS, Başbakanlığın 2004/21 sayılı Kamu Sertifikasyon Merkezi Oluşturulması başlıklı genelgesi uyarınca kamu kurum ve kuruluşlarının elektronik sertifika ihtiyaçlarının tek merkezden sağlanması amacıyla öncelikli olarak kamu çalışanlarına nitelikli elektronik sertifika verir. Nitelikli elektronik sertifikalar ile bağlantılı imza oluşturma verileri, elektronik imza mevzuatında belirtildiği şekilde güvenli elektronik imza oluşturmak amacıyla kullanılırlar. Kamu çalışanları nitelikli elektronik sertifikalarını ve ilgili imza oluşturma verilerini kamu kurum ve kuruluşlarındaki veya kendi özel işlerindeki güvenli elektronik imza uygulamalarında kullanırlar. Cihaz Sertifikası Hizmet Sağlayıcısı ise cihazlara elektronik sertifika temini amacıyla hizmet verir. Cihazlara verilen sertifikalar 5070 sayılı Elektronik İmza Kanunu'nda sözü geçen nitelikli elektronik sertifika kapsamında değerlendirilmezler.

Kamu SM, Sertifika İlkeleri (Sİ) dokümanında belirtilen ilkelere uygun olarak hazırlanan bu SUE dokümanında tanımlanan esaslar uyarınca çalışır. SUE dokümanı, nitelikli elektronik sertifikaların yönetimi ve kayıt işlemleri sırasında yapılan işlerin hangi ortamlarda ve nasıl yürütüldüğünü Sİ dokümanına bağlı olarak detaylandırarak anlatır.

Kamu SM'den sertifika talebinde bulunanlar bu dokümanda belirtilen esaslar çerçevesinde sertifikayı kullanmayı kabul etmiş sayılır. Nitelikli sertifika talebinde bulunanlar bununla ilgili olarak, Nitelikli Elektronik Sertifika Sözleşmesi veya Nitelikli Elektronik Sertifika Sahibi Taahhütnamesi'ni imzalar.

### 1.1. Genel Bakış

SUE dokümanı, Kamu SM içinde yer alan sistem bileşenlerinin rollerini, sorumluluklarını ve ilişkilerini tanımlar; sertifika yönetim ve kayıt işlemlerinin gerçekleştirilme şeklini anlatır. Sertifika yönetimi, sertifika sahipleri için anahtar çifti ve sertifika üretmek, sertifikaları yayımlamak, yenilemek, askıya almak, iptal etmek, sertifika

iptal bilgisini yayımlamak, sertifika işlemleri ile ilgili kişileri başvuru ve sertifikanın durumu hakkında bilgilendirmek, gerekli kayıtları tutmak ve kayıt işlemlerini gerçekleştirmek gibi işlerden oluşur. Kayıt işlemleri sertifika verilecek kişilerin başvurularını, kimlik bilgileri ve ilgili resmi belgeleri toplama, kimlik doğrulama, onaylama, iptal, yenileme isteklerini alma, değerlendirme, onaylanan sertifika başvuru ve iptal istekleri doğrultusunda gerekli işlemleri başlatmayı içerir.

SUE dokümanı, "Internet Açık Anahtar Altyapısı Sertifika İlkeleri ve Sertifika Uygulama Esasları Çerçeve Planı" [IETF - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 3647)] referans alınarak hazırlanmış olup, doküman içeriğinde belirtilen bir kısım alt başlıkların altındaki "düzenlenmesine gerek duyulmamıştır" ibaresi, bu aşamada ihtiyaç duyulmadığından düzenleme yapılmadığını ifade etmektedir.

### 1.2. Doküman Adı ve Tanımı

**Doküman Adı:** Kamu SM
Sertifika Uygulama Esasları
(Nitelikli Elektronik Sertifika içindir)

**Doküman Sürüm Numarası:** 07

**Yayın Tarihi:** 30.12.2010

### 1.3. Sistem Bileşenleri

#### 1.3.1. Elektronik Sertifika Hizmet Sağlayıcısı

Kamu SM, Kök Sertifika Hizmet Sağlayıcısı olarak kök sertifika hizmeti, ve aynı zamanda Kamu Elektronik Sertifika Hizmet Sağlayıcısı olarak da kamu kurum ve kuruluşlarına Nitelikli Elektronik Sertifika hizmeti vermektedir.

**Kök Sertifika Hizmet Sağlayıcısı**

Kök SHS, Kamu SM içinde en yetkili imza derecesine sahiptir ve sertifikası kendi imza oluşturma verisi ile imzalanmıştır.

Kamu SM güvenlik gerekleri dolayısıyla özel statüye sahip kamu kuruluşlarına (Türk Silahlı Kuvvetleri, Dışişleri Bakanlığı, vb.) ait ESHS'ler, ülke içinde hizmet veren ulusal ESHS'ler ve ülke dışında kurulmuş olan diğer ESHS'lerle ortak çalışırlığı sağlayabilmek için kök, köprü ve çapraz sertifika hizmetleri verir. Üretilen çapraz sertifikalar Kök SHS'nin imzasını taşır. Kök SHS tarafından sertifika hizmeti veren kurumlara verilen sertifikalar için başvuru, üretim, dağıtım, yenileme ve iptal etme ile ilgili süreçler içindeki işlemler bu dokümanın içeriğinde bulunmaz. Kök SHS sertifika başvuru ve yönetim işlemleri Kamu SM Kök, Köprü ve Çapraz Sertifikasyon Yönetimi dokümanında anlatılmaktadır.

Kök SHS imza oluşturma verisinin bulunduğu sistem çevrim dışı çalışır. İmza oluşturma verisi, en üst düzeyde fiziksel ve elektronik güvenlik sağlanarak korunur.

**Kamu Elektronik Sertifika Hizmet Sağlayıcısı**

Kamu ESHS'nin sertifikası Kök SHS tarafından imzalanmıştır. Kişilere dağıtılan nitelikli elektronik sertifikalar Kamu ESHS'nin elektronik imzasını taşır.

### 1.3.2. Kayıt Birimleri

Düzenlenmesine gerek duyulmamıştır.

### 1.3.3. Sertifika Sahipleri

Kamu SM tarafından dağıtılan sertifikanın üzerinde adları bulunan ve sertifikalarını Kamu SM sertifika ilke ve uygulama esaslarına uygun olarak kullanmakla yükümlü olan gerçek kişilerdir.

### 1.3.4. Üçüncü Kişiler

Kamu SM tarafından oluşturulan sertifikaların içindeki kimlik bilgileri ve imza doğrulama verisi arasındaki bağın doğruluğuna güvenerek sertifikaları kabul eden ve işlem yapan kişilerdir.

Üçüncü kişiler sertifikaları kullanmadan önce gerekli gördüğü geçerlilik kontrollerini yapar.

### 1.3.5. Diğer Bileşenler

Düzenlenmesine gerek duyulmamıştır.

## 1.4. Sertifika Kullanımı

### 1.4.1. Uygun Olan Sertifika Kullanımı

Kamu SM'nin kişiler adına ürettiği nitelikli elektronik sertifikalar güvenli elektronik imza uygulamalarında kullanılır. Nitelikli elektronik sertifika sahibi kamu çalışanı, ilgili imza oluşturma verisini kamu kurum ve kuruluşlarının elektronik ortamlarda yürütecekleri iş ve işlemlerinde veya kendi özel işlerinde güvenli elektronik imza oluşturmak amacıyla kullanır. İmza oluşturma verisi kullanılarak oluşturulan güvenli elektronik imzanın, elle atılan imza ile aynı hukuki sonucu doğurabilmesi için, imza oluşturma verisinin güvenli elektronik imza oluşturma aracı içinde saklanması, güvenli elektronik imzanın elektronik imza mevzuatında belirtildiği gibi güvenilir yöntemlerle, güvenli yazılım veya donanım araçları kullanılarak oluşturulması gerekmektedir.

Nitelikli elektronik sertifika içeriğindeki imza doğrulama verisi güvenli elektronik imzayı doğrulamak için kullanılır.

### 1.4.2. Sertifika Kullanımının Sınırları

Nitelikli elektronik sertifika ve ilgili imza oluşturma verisi, güvenli elektronik imza oluşturma ve doğrulama dışında kullanılamaz. Nitelikli elektronik sertifika sahibi kişi, kanunların resmi şekle veya özel bir merasime tabi tuttuğu hukuki işlemler ile teminat sözleşmelerini güvenli elektronik imza ile gerçekleştiremez. Nitelikli elektronik sertifikaların ve ilgili imza oluşturma verilerinin tanımlı maddi sınırları üzerinde değerde işlem yapmak, elektronik imzalı e-posta göndermek, açık ağlar üzerinde kimlik doğrulaması yapmak, iletilen mesajların bütünlüğünü ve gizliliğini sağlamak gibi amaçlarla kullanımından doğan zararlardan Kamu SM sorumlu tutulamaz.

Kamu SM, dağıttığı sertifikaların hangi uygulamalarda ne amaçlar doğrultusunda kullanıldığının kontrolünü yapmakla yükümlü değildir.

### 1.5. Uygulama Esaslarının Yönetimi

#### 1.5.1. Doküman Yönetimi

SUE dokümanı Kamu SM tarafından yazılmıştır. Kamu SM, gerekli gördüğü durumlarda SUE dokümanında değişiklik yapabilir.

#### 1.5.2. İletişim Bilgileri

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

**Adres** : TÜBİTAK BİLGEM, PK. 74, 41470 Gebze-KOCAELİ

**Tel** : (262) 648 18 18

**Faks** : (262) 648 18 00

**E Posta** : bilgi@kamusm.gov.tr

**URL** : http://www.kamusm.gov.tr

Kamu SM, SUE dokümanını herkesin erişimine açık bulunan aşağıdaki internet adresinden yayımlar:

http://www.kamusm.gov.tr/BilgiDeposu/

#### 1.5.3. Sertifika Uygulama Esaslarının İlkelere Uygunluğunu Belirleyen Kişi

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

#### 1.5.4. Sertifika Uygulama Esasları Onay Prosedürleri

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

### 1.6. Tanımlar ve Kısaltmalar

#### 1.6.1. Tanımlar

**Anahtar çifti:** Elektronik imza oluşturmak amacıyla kullanılan özel anahtar ve ilgili açık anahtar. İmza oluşturma ve doğrulama verileri.

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

**Çevrim içi sertifika durum protokolü :** Üçüncü kişilerin sertifika iptal listesine alternatif olarak sertifika geçerlilik kontrol talebini yapıp, sertifikanın iptal durumunu öğrenmelerine imkan tanıyan standart iletişim kuralı.

**Elektronik sertifika:** İmza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kayıt.

**Güvenli elektronik imza:** Münhasıran imza sahibine bağlı olan, sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan, nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan, imzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan elektronik imza. Bu dokümanda bahsi geçen elektronik imza ibaresi güvenli elektronik imzayı ifade etmek amacıyla kullanılmıştır.

**Güvenli elektronik imza oluşturma aracı:** Sertifika sahibine ait imza oluşturma verisi ve sertifikanın içinde bulunduğu taşınabilir, akıllı kart ya da benzeri güvenli cihaz.

**Güvenli elektronik imza oluşturma aracı erişim verisi:** Sertifika sahibine ait imza oluşturma verisine erişimin kontrolünü sağlayan PIN ve PUK bilgisidir

**İmza doğrulama verisi:** Elektronik imzayı doğrulamak için kullanılan şifreler, kriptografik açık anahtarlar gibi veriler.

**İmza oluşturma verisi:** İmza sahibine ait olan, imza sahibi tarafından elektronik imza oluşturma amacıyla kullanılan ve bir eşi daha olmayan şifreler, kriptografik gizli anahtarlar gibi veriler.

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

**Kamu Elektronik Sertifika Hizmet Sağlayıcısı:** Kamu Sertifikasyon Merkezi içinde oluşturulmuş, Kök Sertifika Hizmet Sağlayıcısı'nın imzasını taşıyan sertifikaya sahip olan ve son kullanıcıların sertifikalarını oluşturup imzalamakla yetkili kılınmış Elektronik Sertifika Hizmet Sağlayıcısı.

**Kamu Sertifikasyon Merkezi:** Türkiye Bilimsel ve Teknolojik Araştırma Kurumu'na bağlı Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü Müdürlüğü bünyesinde, elektronik sertifika hizmeti sağlamak üzere oluşturulan birim.

**Kimlik Paylaşım Sistemi**: İçişleri Bakanlığı Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü ile yapılan güvenli bağlantı ile tüm T.C. vatandaşlarına ait nüfus bilgilerinin paylaşıldığı sistem.

**Kurum Yetkilisi:** Kamu kurumları ile yapılan sözleşmelerde belirlenen ve NES ile ilgili süreçlerde kurumu temsile yetkili kişidir.

**Kök Sertifika Hizmet Sağlayıcısı:** Kamu Sertifikasyon Merkezi içinde oluşturulmuş, en yetkili imza derecesi verilmiş ve sertifikasını kendisi imzalamış olan Sertifika Hizmet Sağlayıcısı.

**Son Kullanıcı:** Kamu ESHS sisteminde kimlik doğrulaması yapılmış ve sertifika almak üzere tanımlanmış kişiler. Sertifika sahibi olan kişiler, aynı zamanda Kamu ESHS sistemi son kullanıcılarıdır.

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

**Nitelikli elektronik sertifika:** 5070 sayılı Elektronik İmza Kanunu'nun 9'uncu maddesinde sayılan nitelikleri haiz elektronik sertifika.

**Sertifika iptal listesi:** İptal olmuş sertifika bilgilerinin içinde yer aldığı ESHS'nin imzasını taşıyan elektronik dosya.

**Sertifika sahibi:** Kamu ESHS'den güvenli elektronik imza oluşturmak amacıyla sertifika alan gerçek kişi.

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

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

### 1.6.2. Kısaltmalar

**BS (British Standards)**: İngiliz Standartları

**BTK:** Bilgi Teknolojileri ve İletişim Kurumu

**CEN (Comité Européen de Normalisation):** Avrupa Standardizasyon Komitesi

**CWA (CEN Workshop Agreement):** CEN Çalıştay Kararı

**ÇİSDUP (OCSP):** Çevrim İçi Sertifika Durum Protokolü [Online Certificate Status Protocol]

**DSA (Digital Signature Algorithm):** Sayısal İmza Algoritması

**DSA Eliptik Eğrisi (DSA Elliptical Curve):** Sayısal İmza Algoritması Eliptik Eğrisi

**EAL (Evaluation Assurance Level):** Değerlendirme Garanti Düzeyi

**ESHS:** Elektronik Sertifika Hizmet Sağlayıcısı

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

**ETSI TS (ETSI Technical Specification):** ETSI Teknik Özellikleri

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

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

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

**ITU (International Telecommunication Union):** Uluslararası Telekomünikasyon Birliği

**KPS**: Kimlik Paylaşım Sistemi

**Kamu SM:** Kamu Sertifikasyon Merkezi

**LDAP (Lightweight Directory Access Protocol):** Dizin Erişim Protokolü

**PKI (Public Key Infrastructure):** Açık Anahtarlı Altyapılar

**RIPEMD (RACE Integrity Primitives Evaluation Message Digest):** RACE Bütünlük Asli Mesaj Değerlendirme Özeti

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

**SHA (Secure Hash Algorithm):** Güvenli Özet Algoritması

**Sİ:** Sertifika İlkeleri

**SİL:** Sertifika İptal Listesi

**SUE:** Sertifika Uygulama Esasları

## 2. Yayımlama ve Bilgi Deposu

Bilgi deposu, Kamu SM'nin ürettiği sertifikaları, iptal durum kayıtlarını, Sİ ve SUE gibi ilgili dokümanları sertifika sahiplerinin ve üçüncü kişilerin ulaşabileceği şekilde kesintisiz, güvenli ve ücretsiz olarak yayımladığı ortamdır.

Kamu SM'nin bilgi deposuna internet üzerinden erişilir. İnternet üzerinden Kamu SM hakkında bilgiler, sertifika yönetimiyle ilgili dokümanlar, teknik bilgilendirme dokümanları, başvuru formları ve duyurular yayımlanır.

### 2.1. Bilgi Depoları

Kamu SM, bilgi deposu olarak internet üzerinden hizmet veren servisleri kullanmaktadır. Bilgi depolarına erişim adresleri ve erişilebilen bilgiler aşağıda verilmektedir.

http://www.kamusm.gov.tr/BilgiDeposu internet adresi üzerinden Nitelikli Elektronik Sertifika Sözleşmesi, Taahhütnamesi, Kamu SM Taahhütnamesi, SUE ve Sİ dokümanları, Kamu SM'ye ait sertifikalar ve SİL'lere erişilmektedir.

ldap://dizin.kamusm.gov.tr/ adresinden erişilebilen LDAP dizin sunucusu üzerinden sertifikalara ve SİL'lere erişim sağlanır.

### 2.2. Sertifika Hizmeti ile İlgili Bilgilerin Yayımlanması

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

- Kamu SM'ye ait Kök SHS ve Kamu ESHS sertifikaları,
- Sertifika sahibi kişilerle yapılan sözleşmelerde aksi belirtilmediği sürece sertifika sahiplerine ait nitelikli elektronik sertifikalar,
- Kamu SM'ye ait Kök SHS sertifikasının özet değeri ile özet değerinin hesaplanmasında kullanılan özetleme algoritmasının hangisi olduğu bilgisi,
- Kamu SM Sİ ve SUE dokümanları,
- Taahhütnameler,
- Sözleşmeler,
- Formlar,
- Sertifika iptal durum kayıtları.

### 2.3. Yayın Sıklığı ve Zamanı

Nitelikli elektronik sertifikalar üretildiği hafta içinde yayımlanır.

Taahhütnameler, Sertifika Sözleşmeleri, nitelikli elektronik sertifika yönetim prosedürleri, SUE ve Sİ dokümanları içeriğinin değişmesi üzerine güncellenir. Güncellenen dokümanlar, güncelleme yapılmasını müteakip derhal yayımlanır.

Kamu SM'ye ait sertifikalar yenilenmesini müteakip derhal yayımlanır.

Sertifika iptal durum kayıtlarının yayımlanma sıklığı bu dokümanda Bölüm 4.9.7 ve 4.9.9'da belirtilmektedir.

### 2.4. Erişim Kontrolleri

Kamu SM bilgi deposuna bilgi edinme amaçlı erişim herkese açıktır.

Bilgi deposunun güncellenmesi, yetkisi olan Kamu SM çalışanı kişiler 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 doğruluğu ve güncelliğini sağlamak,
- Bilgi deposunu sürekli olarak katılımcıların erişimine açık tutmak,
- Bilgi deposunun kesintisiz olarak erişilebilirliğini sağlamak için gerekli önlemleri almak,
- Bilgi deposuna erişimi ücretsiz sağlamak.

## 3. Kimlik Belirleme ve Doğrulama

Nitelikli elektronik sertifikalarla ilgili işlemler yapılmadan önce, işlemi talep etmeye yetkisi olan kişi veya kurumun öncelikle kimlik tanımlama veya doğrulaması yapılır. Bu bölümde nitelikli elektronik sertifika yönetim prosedürleri içinde uygulanan kimlik tanımlama ve doğrulama yöntemleri ile nitelikli elektronik sertifikanın içinde yazılan kimlik bilgileri anlatılmıştır.

### 3.1. İsimlendirme

#### 3.1.1. İsim Alanı Tipleri

Nitelikli elektronik sertifikalarda Kamu SM ve sertifika sahibine ait kimlik bilgilerinin belirtildiği DN [Distinguished Name (Ayırt edici isim)] alanı içinde "ITU X.500" biçiminin desteklediği isim tipleri kullanılır.

#### 3.1.2. Kimlik Bilgilerinin Teşhise Elverişli Olması

Nitelikli elektronik sertifika içeriğindeki isim alanına yazılan bilgiler kişiyi tanımlayan ve kişinin kimliğinin tespit edilmesini sağlayan niteliktedir. Nitelikli elektronik sertifika içeriğine konulacak bilgiler; kişiyi teşhis edebilecek kimlik bilgilerinden oluşur.

#### 3.1.3. Sertifika Sahibinin Takma İsim veya Lakap Kullanması

Sertifika sahibinin nitelikli elektronik sertifikasının içeriğinde takma isim veya lakap kullanılmasına izin verilmez.

#### 3.1.4. Farklı İsim Alanı Tiplerinin Yorumlanması

Nitelikli elektronik sertifikalar içinde ITU X.500 biçimi dışında isim alanı tipi kullanılmaz.

#### 3.1.5. Kimlik Bilgilerinin Tekilliği

Dağıtılan nitelikli elektronik sertifikaların içeriğindeki kimlik bilgileri her kişi için ayırt edici niteliktedir. Aynı kişiye ait nitelikli elektronik sertifikaların içeriğindeki kimlik bilgilerinin aynı olmasına izin verilmektedir. Ancak farklı kişilere ait nitelikli elektronik sertifikaların içeriğindeki kimlik bilgilerinin aynı olması engellenmektedir. Bunun sağlanabilmesi için nitelikli elektronik sertifikaların isim alanı içinde benzersiz bir sayı olduğu kabul edilen, sertifika sahibinin T.C. kimlik numarası yer alır. Yabancı uyruklu sertifika sahipleri için isim alanı içinde pasaport numarası yer alır.

#### 3.1.6. Markanın Tanınması, Doğrulanması ve Rolü

Düzenlenmesine gerek duyulmamıştır.

### 3.2. İlk Kimlik Belirleme

Kamu SM nitelikli elektronik sertifika hizmetlerinden faydalanmak için ilk defa başvuruda bulunulduğunda, ilgili kişi ve kurumun kimliklerinin doğrulanabilmesi için aşağıda tanımlanan yöntemler uygulanır.

#### 3.2.1. İmza Oluşturma Verisine Sahip Olmanın Kanıtlanması

Sertifika sahibine ait imza oluşturma ve doğrulama verileri, kişiler adına Kamu SM tarafından üretilerek sahibine güvenli elektronik imza oluşturma aracı içinde ulaştırılır. İmza

oluşturma verisine sahiplik güvenli elektronik imza oluşturma aracının sertifika sahibi tarafından şahsen teslim alınması yoluyla kanıtlanır.

### 3.2.2. Kurumsal Kimliğin Belirlenmesi

Çalışanları adına nitelikli elektronik sertifika başvurusunda bulunan kurumlar, Kamu SM tarafından istenen kurum bilgilerini kurumu temsile yetkili kişilerin imzaladığı ve kurumun onayını taşıyan resmi yazıyla Kamu SM'ye bildirir. Kamu SM resmi yazıya istinaden kurum kimliğini belirler.

### 3.2.3. Kişisel Kimliğin Belirlenmesi

Nitelikli elektronik sertifika başvurusunda bulunan kurumlar, nitelikli elektronik sertifika almak istediği çalışanlarına ait bilgileri, kurumun onayını taşıyan resmi yazıyla yada kurum yetkilisinin elektronik olarak imzaladığı form ile Kamu SM'ye bildirir. Resmi yazının ekinde nitelikli elektronik sertifika alınacak kişilerin listesini Kamu SM'ye iletir. Kişilere ait kimlik bilgileri Kimlik Paylaşım Sistemi ile kurumsal başvuru belgesine dayanılarak belirlenir.

### 3.2.4. Doğrulanmayan Sertifika Sahibi Bilgileri

Sertifika sahibi veya kurum tarafından başvuru sırasında ve daha sonra değişiklik sebebiyle beyan edilen aşağıdaki erişim bilgilerinin doğruluğu Kamu SM tarafından kontrol edilmez.

- Telefon numaraları
- Faks numaraları
- Güvenli elektronik imza oluşturma aracı tesliminde kullanılacak adres bilgisi
- Sertifika sahibinin elektronik posta adresi

Bu bilgilerin doğruluğu sertifika sahibinin veya kurumun beyanı üzerine kabul edilir.

Kurum ve sertifika sahibi bu bilgileri Kamu SM'ye doğru beyan etmekle yükümlüdür. Bu bilgilerin Kamu SM'ye yanlış verilmesinden dolayı doğabilecek zararlardan, sertifika yönetim sürecinde meydana gelebilecek gecikme veya aksaklıklardan Kamu SM sorumlu tutulamaz.

### 3.2.5. Yetkinin Doğrulanması

Düzenlenmesine gerek duyulmamıştır.

### 3.2.6. Uyum Kriterleri

Düzenlenmesine gerek duyulmamıştır.

## 3.3. Sertifika Yenileme İsteğinde Kimlik Doğrulama

### 3.3.1. Olağan Sertifika Yenileme İsteğinde Kimlik Doğrulama

Geçerli bir sertifikası olan sertifika sahipleri, sertifikanın kullanım süresi dolmadan önce ve sertifikanın içeriğinde herhangi bir değişiklik olmaması durumunda, Kamu SM'ye olağan sertifika yenileme talebinde bulunabilirler.

Sertifika yenileme isteği, geçerli sertifikanın kullanım süresi dolmadan önce; internetten doldurulan formun ıslak imzalı yada elektronik imzalı kopyasının Kamu SM'ye

iletilmesi ile yapılır. Sertifika yenileme isteği yerine getirilmeden önce, talebi yapan kişinin kimlik doğrulaması, Kamu SM sisteminde kayıtlı bilgiler ve KPS kullanılarak yapılır.

Kimlik doğrulaması için sertifika sahibinden ilk sertifika başvurusu sırasında istenen belgeler yeniden istenmez.

### 3.3.2. İptal Sonrası Yeni Sertifika Talebinde Kimlik Doğrulama

Nitelikli elektronik sertifikanın içeriğindeki bilgilerin değişmesi, kullanım süresinin dolması ve iptal sonrası yeni nitelikli elektronik sertifika isteğinde bulunulması durumunda, yeniden nitelikli elektronik sertifika almak isteyen sertifika sahibi sertifika talebinde bulunur. Yeni sertifika talebinin, sertifika sahibinin bağlı olduğu kurum tarafından da kabul edilmesi durumunda süreç başlatılır.

Sertifika sahibinin çalıştığı kurum, yeni sertifika başvurusunu onayladığını kabul eden yazı ile Kamu SM'ye bildirir. Kurumun kimlik doğrulaması gelen resmi yazıya dayanılarak yapılır.

## 3.4. Sertifika İptal İsteğinde Kimlik Doğrulama

Nitelikli elektronik sertifika sahibi internet üzerinden işlem yaparak, çağrı merkezini arayarak veya Kamu SM'ye kağıt üzerinde ıslak imzalı form veya yazı göndererek nitelikli elektronik sertifikasının iptal edilmesini isteyebilir.

İnternet üzerinden ve çağrı merkezinden iptal isteklerinin kabul edilebilmesi için sertifika sahibine ait parola veya kişisel bilgiler kullanılarak kimlik doğrulaması yapılır. Bunun için sertifika sahibinin iptal başvurusunda bulunduğu sırada bildirdiği güvenlik sözcüğü ve diğer kişisel bilgileri, Kamu SM sisteminde kayıtlı bulunan bilgilerle kıyaslanarak doğruluğu kontrol edilir. Kağıt üzerinde ıslak imzalı form veya yazı ile yapılan iptal başvurularında kimlik doğrulaması ıslak imzanın doğruluğunun kontrolü ile yapılır.

## 4. İşlemsel Gerekler

Bu bölümde sertifika yönetim süreçlerinde yapılan işlemler anlatılmaktadır. Süreçlerle ilgili ayrıntılar Kamu SM'nin internet sitesinde belirtilmektedir. Sertifika yönetimi aşağıdaki süreçlerden oluşmaktadır:

- Sertifika başvurusu
- Sertifika yenileme
- Sertifika askıya alma ve askıdan çıkarma
- Sertifika iptal etme

Süreçler sertifika sahipleri, kurumlar ve Kamu SM arasında gerçekleştirilen işlemlerden oluşmaktadır.

### 4.1. Sertifika Başvurusu

#### 4.1.1. Sertifika Başvurusunu Kimlerin Yapabildiği

Nitelikli elektronik sertifika başvurusu, kurum veya kuruluşlar tarafından Kamu SM'ye kurumsal olarak yapılır. Kurum çalışanı kurumun talebi olmadan bireysel olarak nitelikli elektronik sertifika başvurusunda bulunamaz.

Kurum, başvuru sırasında nitelikli elektronik sertifika almak istediği çalışanlarının temel başvuru bilgilerini (T.C. kimlik no, ad, soyad, kurumsal e-posta adresi, kurum birimi ve sertifika üretim nedeni), Kamu SM'ye bildirir. Kurum, çalışanının haberi olmadan çalışanı adına sertifika başvurusunda bulunamaz. Kurum çalışanının durumdan haberdar olması ve nitelikli elektronik sertifika almayı kendisinin talep etmesi gerekir. Bu talep, kurum çalışanı tarafından doldurulup imzalanan;

- Basılı formlar için ıslak imzalı
- Elektronik formlar için e-imzalı

sertifika başvuru formunun Kamu SM'ye iletilmesi ile yapılır.

#### 4.1.2. Kayıt İşlemleri ve Sorumluluklar

Nitelikli elektronik sertifika başvurusu, sertifika sahipleri adına sertifika sahiplerinin bağlı bulunduğu kamu kurum veya kuruluşu tarafından Kamu SM'ye yapılır. Kurum, Kamu SM'den alacağı sertifika hizmetlerinin şartlarını belirleyen Nitelikli Elektronik Sertifika Temini Sözleşmesini TÜBİTAK BİLGEM ile karşılıklı imzalar.

Kurum nitelikli elektronik sertifika almak istediği personelinin listesini, personelin kimliklerinin belirlenmesi için istenen bilgilerle birlikte Kamu SM'ye gönderir.. Başvurunun işleme alınabilmesi için nitelikli elektronik sertifika alacak olan çalışanlar, kişisel bilgileri ile adres, telefon numarası gibi erişim bilgilerinin bulunduğu nitelikli elektronik sertifika başvuru formunu doldurup ıslak imza ile imzalarlar. Başvuru formları kurum tarafından, kurumun yetkilendirdiği kişi tarafından, Kamu SM'ye iletilir. Bilgi ve belgelerin gizliliğinin sağlanması için belgelerin kapalı zarf içinde Kamu SM'ye iletilmesi gerekmektedir. Belgelerin Kamu SM'nin eline geçene kadarki zaman içerisinde gizliliğinin sağlanmasından kurum sorumludur.

Kurum ve nitelikli elektronik sertifika alacak olan kurum çalışanı başvuru sırasında Kamu SM'ye doğru bilgi beyan etmekle sorumludur. Kamu SM, nitelikli elektronik sertifika içinde yer alacak bilgilerin doğruluğunu kontrol eder ve kendisine beyan edilen bilgilerin gizliliğini sağlamak için gerekli tedbirleri alır.

Sertifika başvurusunda bulunan kişi başvuru sırasında, nitelikli elektronik sertifikasının herkesin erişimine açık dizin sunuculardan yayımlanıp yayımlanmayacağı konusundaki talebini ve nitelikli elektronik sertifikanın kullanımıyla ilgili maddi sınıra ilişkin bilgilendirmeyi Kamu SM'ye yapar. Nitelikli elektronik sertifika başvurusunun nasıl yapılacağı ile ilgili ayrıntılar Kamu SM'nin internet sitesinde yayımlanmaktadır.

Kamu SM nitelikli elektronik sertifika verilecek kişilerin kimlik belirlemelerini yaptıktan sonra başvuruları değerlendirmeye alır ve uygun görülen başvuruları işleme koyar.

### 4.2. Sertifika Başvurusunun İşlenmesi

#### 4.2.1. Kimlik Tanımlama ve Doğrulama İşlevlerinin Yerine Getirilmesi

Başvuru sırasında kurumdan gelen belgelerin Kamu SM tarafından incelenmesi sonucunda kimlik tanımlama ve doğrulama işlevleri yerine getirilir. Nitelikli elektronik sertifika başvurusunda bulunan kurumlar aşağıdaki bilgi ve belgeleri Kamu SM'ye gönderir:

- Nitelikli elektronik sertifika alacak çalışanların, T.C. kimlik no (yabancı uyruklular için pasaport no), ad, soyad, kurumsal e-posta adresi, kurum birimi ve sertifika üretim nedeni bilgisinin bulunduğu liste,
- Nitelikli elektronik sertifika alacak çalışanların ıslak imzasını taşıyan nitelikli elektronik sertifika başvuru formları,
- Yabancı uyruklular için noter onaylı pasaport sureti,

Kurumdan gönderilen belgeler üzerinde kimlik tanımlama işlemleri için aşağıdaki kontroller yapılır:

- Kurum'dan gelen yazının ve formların imzalı ve onaylı olup olmadığına bakılır.
- Kurum tarafından gönderilen nitelikli elektronik sertifika alacak çalışanlar listesindeki T.C. kimlik no (yabancı uyruklular için pasaport no), ad, soyad, kurumsal e-posta adresi, kurum birimi ve sertifika üretim nedeni bilgisinin tamlığına ve doğruluğuna bakılır.
- NES'te kullanılacak bilgilerin doğruluğu, KPS kullanılarak yapılır.
- Yabancı uyruklu nitelikli elektronik başvuru sahiplerinin noter onaylı pasaport suretlerine bakılır.

Bilgi ve belgeler hatasız ve tam ise kimlik tanımlama ve doğrulama işlevi tamamlanır. Belgelerde gözle görülen tahrifat, hata, eksik onay ya da eksik bilgi olması veya bilgilerin yanlışlığının tespit edilmesi durumunda kimlik tanımlama ve doğrulama yapılamaz. Bu durumda; Kamu SM, ilgili kurum yetkilisine hataları bildirir ve gerekli görülen bilgi ve belgeleri tekrar talep eder.

#### 4.2.2. Sertifika Başvurusunun Kabul veya Reddi

Bölüm 4.2.1'deki kontrollerin yapılması sonucunda, nitelikli elektronik sertifika başvurusu sırasında beyan edilen belgelerde tahrifat, hata, eksik onay, eksik bilgi veya yanlış bilgi olması durumlarında başvuru geri çevrilir. Başvurusu kabul edilmeyenlerle ilgili bilgilendirme, kurumun yetkili kıldığı kişiye ve/veya başvuru sahibi kişiye yapılır. Yazılı bilgilendirme, kuruma resmi yazı gönderme veya kurum yetkilisine ve/veya başvuru sahibine e-posta gönderme yoluyla yapılır. Sözlü bilgilendirme kurum yetkilisine ve/veya başvuru sahibine telefon açılarak yapılır. Sözlü bildirimler kayıt altına alınır. Kurum ve başvuru

sahibine ait e-posta ve telefon bilgileri başvuru sırasında beyan edilen bilgilerdir. Gereken düzeltmeler yapılıp eksiklikler tamamladıktan sonra başvuru tekrarlanabilir.

Başvurusu kabul edilenler Kamu SM sisteminde tanımlanır ve nitelikli elektronik sertifika üretim süreci başlatılır.

#### 4.2.3. Sertifika Başvurusunun İşlenme Zamanı

Başvuru ile ilgili geçerli tüm belgelerin Kamu SM'nin eline geçmesinin ardından en fazla 1 (bir) ay içinde sertifika başvurusu işleme alınır ve sonuçlandırılır.

### 4.3. Sertifikanın Oluşturulması

#### 4.3.1. Sertifika Oluşturulmasında ESHS'nin İşlevleri

Sertifika başvurusu tamamlanarak, sistemde tanımlanan kişiler adına anahtar çifti ile güvenli elektronik imza oluşturma aracı erişim verisi Kamu SM tarafından üretilir. Anahtar çiftleri ve erişim verilerinin üretilmesi, güvenli elektronik imza oluşturma aracının ilklendirilmesi gibi işlemler nitelikli elektronik sertifika üretim aşamasında gerçekleştirilir.

Nitelikli elektronik sertifika, imza doğrulama verisi ve sistemde onayı verilmiş kimlik bilgilerinin Kamu ESHS'ye ait imza oluşturma verisi ile imzalanması suretiyle üretilir. Nitelikli elektronik sertifikalar ETSI TS 101 862, ITU-T X.509 v.3 standartlarına ve Kanunun 9'uncu maddesinde belirtilen niteliklere uygun olarak üretilir. İmza oluşturma verisi ve nitelikli elektronik sertifika güvenli elektronik imza oluşturma aracına yüklenir. İmza oluşturma verisi, güvenli elektronik imza oluşturma aracı içinde şifreli saklanır ve kopyası sistemde tutulmaz. Güvenli elektronik imza oluşturma aracı erişim verisi oluşturularak kapalı parola zarfına basılır yada sistemde şifreli olarak tutulur. Güvenli elektronik imza oluşturma aracı erişim verisinin nasıl teslim edileceği başvuru sırasında tanımlanır. Güvenli elektronik imza oluşturma aracı erişim verisi sertifika sahiplerine öncelikli olarak web servislerinden teslim edilir. Web servislerinin kullanılamadığı durumda parola zarfı ile teslimat gerçekleştirilir.

Kapalı parola zarfına basılan güvenli elektronik imza oluşturma aracı erişim verisi sistemden silinir. Kapalı parola zarfına basılan erişim verisi, NES teslim edildikten sonra, ikinci bir gönderim ile sertifika sahibine teslim edilir.

Web üzerinden erişimi sağlanan güvenli elektronik imza oluşturma aracı erişim verisi sertifika sahibi insiyatifinde sistemden silinebilir. Güncellenen veri Kamu SM sistemi ile senkronize edilmez.

Sertifika üretim süreci tamamlandıktan ve güvenli elektronik imza oluşturma aracına yazıldıktan sonra; bilgilendirme amaçlı belgeler ile birlikte zarflanır. Kurumla yapılan sözleşmeye göre başka donanımlar da eklenebilir. Zarf kurye ile sertifika sahibine iletilir ve resmi kimlik belgesi ve imza karşılığı teslim eder. İmzalanan sertifika teslim fişi Kamu SM'ye geri getirilir.

Sertifika teslim fişi barkod bilgisi okutularak, sertifikanın teslim edildiği Kamu SM kayıtlarına işlenir. Kapalı parola zarfı ile erişim verisi teslim edilecek ise; ikinci adımda parola zarfı gönderilir. Parola zarfı da resmi kimlik ve imza karşılığı sertifika sahibine teslim edilir. İmzalanan parola teslim fişi Kamu SM'ye geri getirilir. Parola teslim fişi barkodu okutularak sisteme kayıt edilir ve teslimat tamamlanır.

Kamu SM, kurum ile yapılan sözleşmelerde belirtilmiş ise, kurum personeline ait, içerisinde imza oluşturma verisi ve sertifika olan güvenli elektronik imza oluşturma araçlarını

ve güvenli elektronik imza oluşturma aracı erişim verilerini toplu olarak kurum yetkilisine imza karşılığında teslim edebilir.

Kamu SM'nin yükümlülüklerinin belirtildiği Kamu SM Taahhütnamesi http://www.kamusm.gov.tr/BilgiDeposu adresinden yayınlanır.

#### 4.3.2. Sertifika Oluşturulması ile İlgili Sertifika Sahibinin Bilgilendirilmesi

Sertifika sahibi kendisine gönderilen güvenli elektronik imza oluşturma aracını teslim aldığında, nitelikli elektronik sertifikasının oluşturulduğu konusunda bilgilendirilmiş olur.

### 4.4. Sertifikanın Kabulü

#### 4.4.1. Sertifikanın Kabul Koşulu

Kamu SM, nitelikli elektronik sertifikaları içeren güvenli elektronik imza oluşturma aracını kurye vasıtası ile sahibine ulaştırır. Sertifika sahibi kullanmaya başlamadan önce sertifikasının içeriğini kontrol eder ve doğrular.. Sertifikanın kendisine ait olmaması ya da sertifika içerisindeki bilgilerde hata olması durumunda, 5 iş günü içerisinde iade sebebini belirterek güvenli elektronik imza oluşturma aracını Kamu SM'ye iade eder. 5 iş günü içerisinde iade edilmemesi durumunda sertifika kabul edilmiş sayılır.

.

#### 4.4.2. Sertifikanın ESHS Tarafından Yayımlanması

Kamu SM, ürettiği sertifikaları, sertifika sahibinin onayını almak kaydıyla, herkesin erişimine açık dizin yada web servisi üzerinden yayımlar.

Sertifika sahibi başvuru sırasında nitelikli elektronik sertifikasının üçüncü kişilerin ulaşabileceği ortamlardan yayımlanmaması için Kamu SM'ye bildirimde bulunabilir. Kamu SM, sertifika sahibinin bu talebi doğrultusunda nitelikli elektronik sertifikayı yayımlamaz. Ancak nitelikli elektronik sertifikanın yayımlanmaması durumunda, üçüncü kişilerin sertifika sahibinin elektronik imzasını doğrulaması için gerekli olan imza doğrulama verisine erişim engellenmiş olur. Elektronik imzasının doğrulanabilmesi için, sertifika sahibinin elektronik imzasıyla birlikte nitelikli elektronik sertifikasını da doğrulama yapan tarafa göndermesi gerekir.

#### 4.4.3. Sertifikanın Oluşturulmasının Diğer Taraflara Duyurulması

Sertifikanın oluşturulması, internetten erişimi sağlanan raporlar ya da e-posta yolu ile kurum yetkilisine bildirilir.

### 4.5. Sertifikanın ve İmza Oluşturma Verisinin Kullanımı

#### 4.5.1. Sertifika Sahibinin Sertifika ve İmza Oluşturma Verisini Kullanımı

Nitelikli elektronik sertifika sahibi, imza oluşturma verisini elektronik imza mevzuatında belirtildiği şekilde güvenli elektronik imza uygulamalarında kullanır. Güvenli elektronik imza oluşturma verisinin, güvenli elektronik imza oluşturma aracı içinde bulunması zorunludur. Güvenli elektronik imza oluşturma aracının Bölüm 6.2.1'de belirtilen güvenlik standartlarını sağlaması gerekmektedir.

Nitelikli elektronik sertifikalarla ilgili imza oluşturma verilerinin güvenli elektronik imza oluşturma amacı dışında kullanımlarından doğan zararlardan Kamu SM sorumlu tutulamaz.

İptal olmuş veya geçerlilik süresi dolmuş nitelikli elektronik sertifikalara ait imza oluşturma verileri ile işlem yapılamaz.

#### 4.5.2. Üçüncü Kişilerin Sertifika ve İmza Doğrulama Verisini Kullanımı

Sertifika sahibine ait nitelikli elektronik sertifikaların içinde yer alan imza doğrulama verileri, üçüncü kişilerce elektronik imzalı verilerin imzasının doğrulanması amacıyla kullanılır. İmza doğrulama verilerinin üçüncü kişilerce, güvenli elektronik imza doğrulama dışında kullanılması sonucu oluşabilecek zararlardan üçüncü kişiler sorumludur.

### 4.6. Sertifika Süresinin Uzatılması

Sertifika süresinin uzatılması, kullanım süresi dolan sertifikalarda, sertifikada yer alan bilgiler değişmeden aynı anahtar çifti kullanılarak sertifikanın yeni bir son kullanım tarihi ile tekrar üretilmesini tanımlamaktadır. Kamu SM bu işlemi gerçekleştirmez..

### 4.7. Sertifika Yenileme

Kamu SM, sertifika yenileme işlemini, yeni anahtar çifti üretmek ve yeni bir başvuru olarak ele almak sureti ile yerine getirir.

#### 4.7.1. Sertifikanın Yenileme Koşulları

Sertifika yenileme işlemi:

- Güvenli elektronik imza oluşturma aracının kayıp edilmesi,veya çalınması durumunda,
- Güvenli elektronik imza oluşturma aracının arızalanması durumunda,
- Güvenli elektronik imza oluşturma aracı erişim verisin kayıp edilmesi, çalınması, veya unutulması durumunda,
- Elektronik sertifikanın iptal edilmesi ve yenisinin talep edilmesi durumunda,
- Elektronik sertifikanın geçerlilik süresinin sona ermesi durumunda,
- Elektronik sertifikada bilgi değişikliği gerekmesi durumunda,

yapılmaktadır.

#### 4.7.2. Sertifika Yenileme Başvurusunu Kimlerin Yapabildiği

Bölüm 4.1.1'de tanımlanmaktadır.

#### 4.7.3. Sertifika Yenileme Başvurusunun İşlenmesi

Bölüm 4.2'de tanımlanmaktadır.

#### 4.7.4. Sertifika Yenileme ile İlgili Sertifika Sahibinin Bilgilendirilmesi

Bölüm 4.3.2'de tanımlanmaktadır.

#### 4.7.5. Sertifika Yenileme Sonrası Kabul Koşulu

Bölüm 4.4.1'de tanımlanmaktadır.

#### 4.7.6. Sertifika Yenileme Sonrası Sertifikanın Yayımlanması

Bölüm 4.4.2'de tanımlanmaktadır.

#### 4.7.7. Sertifika Yenilemenin Diğer Taraflara Duyurulması

Bölüm 4.4.3'de tanımlanmaktadır.

### 4.8. Sertifikada Bilgi Değişikliği

Sertifikada bilgi değişikliği, sertifikada yer alan bilgilerin, anahtar çifti hariç, değişmesi olarak tanımlanmaktadır.

Sertifikada yer alan bilgilerde; Ad, Soyad, T.C Kimlik No, Para Limiti Değeri, değişiklik olması, sertifikada bilgi değişikliği gerektirmektedir. Kamu SM, sertifikada bigi değişikliği gerçekleştirmez. Bilgi değişikliği gerekli olduğu durumlarda, sertifika anahtar yenileme ile sertifika yeniden üretir.

### 4.9. Sertifikanın İptali ve Askıya Alınması

#### 4.9.1. Sertifikanın İptal Edildiği Durumlar

Sertifikanın, kullanım süresi dolmadan geçerliliğini yitirdiği durumlarda, sertifika iptal edilir. İptal edilen sertifika ile bir daha işlem yapılmaz. Sertifika, aşağıda belirtilen;

- Sertifika sahibinin talebi,
- Sertifika içeriğindeki bilgilerin sahteliğinin veya yanlışlığının ortaya çıkması veya bilgilerin değişmesi,
- Sertifika sahibinin fiil ehliyetinin sınırlandığının, iflasının veya gaipliğinin ya da ölümünün öğrenilmesi,
- Sertifika sahibinin kurum ile ilişiğinin kesilmesinin bildirilmesi,
- İmza oluşturma verisinin güvenliğinin kaybedildiğinden şüphelenilmesi,
- İmza oluşturma verisinin içinde bulunduğu güvenli elektronik imza oluşturma aracının kaybolması, çalınması veya bozulması,
- Güvenli elektronik imza oluşturma aracı erişim verisinin unutulması veya kayıp edilmesi,
- Sertifikanın Nitelikli Elektronik Sertifika Sahibi Taahhütnamesi, Kurum ile imzalanan Nitelikli Elektronik Sertifika Temini Sözleşmesi, Sİ veya SUE dokümanında belirtilen şartlara aykırı kullanımının tespit edilmesi,
- Kamu SM'nin nitelikli elektronik sertifikayı imzalamak için kullandığı imza oluşturma verisinin bütünlüğünün bozulması veya gizliliğinin ortadan kalkması,
- Kamu SM'nin işleyişine son verilmesi ve verilen nitelikli elektronik sertifikaların yönetim işlemlerinin başka bir ESHS tarafından devamlılığının sağlanamaması,

durumlarında iptal edilir..

#### 4.9.2. Sertifika İptal Başvurusunu Kimler Yapabilir

Sertifika iptal başvurusu aşağıda tanımlanan kişiler tarafından yapılabilir;

- Sertifika sahibinin kendisi,
- Karşılıklı imzalanan sözleşmelerde, kurumu temsile yetkili kişiler,
- Kamu SM, madde 4.9.1'de tanımlanan tüm durumlarda iptal yetkisine sahiptir.

#### 4.9.3. Sertifika İptal Başvurusunun İşlenmesi

Nitelikli elektronik sertifika iptal başvurusu, sertifika sahibi tarafından telefonla çağrı merkezinden, internet sitesi üzerinden veya yazılı olarak Kamu SM'ye yapılır. İptal başvurusu

alındığında öncelikle başvuruyu yapan sertifika sahibinin kimlik belirlemesi ve doğrulaması yapılır. Kimlik doğrulaması yapılamayan iptal başvuruları işleme alınmaz.

İnternet üzerinden yapılan iptal başvurusunda, sertifika sahibi https://nesbireysel.kamusm.gov.tr internet adresi üzerinden, Kamu SM sisteminde kayıtlı bulunan erişim parolasını girerek iptal talebinde bulunur. İnternet üzerinden kimlik doğrulama işleminin yapılmasıyla, nitelikli elektronik sertifika Kamu SM sisteminde otomatik olarak iptal edilir.

Çağrı merkezi aracılığıyla yapılan iptal başvurularında, sertifika sahibi Kamu SM çağrı merkezini arar. Çağrı merkezi üzerinden kimlik doğrulama işleminin yapılmasıyla nitelikli elektronik sertifika çağrı merkezinde çalışan sertifika işletmeni tarafından iptal edilir.

Yazılı olarak yapılan taleplerde sertifika sahibi, imzasını taşıyan iptal başvuru formunu Kamu SM'ye iletir. Form üzerindeki bilgiler ve sertifika sahibine ait imza kontrol edilerek kimlik doğrulaması yapılır. Kimlik doğrulamasının yapılmasının ardından nitelikli elektronik sertifika Kamu SM sertifika işletmeni tarafından iptal edilir.

Başvuruların nasıl yapılacağı Kamu SM'nin http://www.kamusm.gov.tr web adresinde ayrıntılı olarak anlatılır. Kamu SM internet sitesi üzerinden iptal işleminin gerçekleştirilebilmesi için gerekli hizmetleri kesintisiz olarak sunar.

Nitelikli elektronik sertifika iptal başvurusu sırasında iptal sebebi Kamu SM'ye bildirilir. Geçmişe yönelik olarak nitelikli elektronik sertifika iptal edilmez.

Nitelikli elektronik sertifika iptal edildikten sonra, Kamu SM sertifika sahibini ve gerekirse bağlı bulunduğu kurum tarafından yetkilendirilen kişiyi nitelikli elektronik sertifikanın iptal edildiğine dair bilgilendirir.

Kamu SM iptal bilgilerini en kısa zamanda işler ve kamuya duyurur. Kamuya duyurulan iptal durum kayıtları en azından nitelikli elektronik sertifikanın seri numarası ile Kamu SM'nin elektronik imzasını taşır. Kamu SM, iptal durum kayıtlarını SİL yayımlamak ve ÇİSDUP Yanıtlayıcı'da nitelikli elektronik sertifikanın durumunu iptal konumuna getirmek suretiyle duyurur.

SİL dosyası, Kamu SM'ye ait imza oluşturma verisi ile imzalanır. İptal edilen nitelikli elektronik sertifikalar geçerlilik süresinin sonuna kadar SİL içinde tutulur. Geçerlilik süresi dolduktan sonra nitelikli elektronik sertifika SİL içinden çıkarılır. ÇİSDUP Yanıtlayıcı'da geçerlilik süresi dolan iptal edilmiş nitelikli elektronik sertifikaların durumu iptal edilmiş konumda görünmeye devam eder.

Nitelikli elektronik sertifika iptal edildikten sonra yeniden nitelikli elektronik sertifika talebinde bulunulabilir.

### 4.9.4. İptal İsteği Ertelenme Süresi

Böyle bir süre öngörülmemiştir.

### 4.9.5. İptal İsteğinin İşlenme Süresi

Kamu SM, kendisine gelen geçerli iptal başvurularını derhal işleme alır ve nitelikli elektronik sertifikayı iptal eder. İptal edilen nitelikli elektronik sertifika bilgisini bir sonraki SİL içinde yayımlar, ÇİSDUP Yanıtlayıcı'dan derhal duyurur. Sertifika iptal talebinin Kamu SM sistemi içinde işlenmesinin ardından bir sonraki SİL'in yayımlanma süresi. Bölüm 4.9.7'de belirtilmiştir.

### 4.9.6. Üçüncü Kişilerin Sertifika İptal Durumunu Kontrol Gerekliliği

Kamu SM, iptal durum kayıtlarını ücretsiz olarak kamuya açar. Sertifika iptal durum kayıtlarına, sorgulama yapacak kişinin kimlik doğrulamasına gerek kalmadan dileyen herkes tarafından erişilebilir. Kamu SM, iptal durum kayıtlarına erişimin sürekliliğini sağlar.

Üçüncü kişiler nitelikli elektronik sertifikalara dayanarak işlem yapmadan önce nitelikli elektronik sertifikaların geçerliliğini SİL ya da ÇİSDUP yöntemlerinden birini kullanarak kontrol etmekle yükümlüdür.

Üçüncü kişiler nitelikli elektronik sertifika geçerlilik kontrolünü yaptığı SİL dosyasının veya ÇİSDUP Yanıtlayıcı'dan aldığı iptal durum kaydının Kamu SM'ye ait imza oluşturma verisiyle imzalandığını kontrol eder. Üçüncü kişilerin yapması gereken geçerlilik kontrolleri Bölüm 9.6.4'te belirtilmiştir.

### 4.9.7. Sertifika İptal Listesi Yayımlama Sıklığı

Sertifika sahiplerine ait iptal bilgisinin bulunduğu SİL'lerin geçerlilik süresi 36 (otuzaltı) saattir. Ancak bu sürenin dolması beklenmeden SİL yayım zamanından sonra her 10 (on) dakikada bir SİL tekrar yayımlanır. Gün içinde yeni bir nitelikli elektronik sertifika iptali olmasa dahi SİL 10 (on) dakika da bir güncellenir. Eski SİL dosyaları geçerlilik süresinin sonuna kadar geçerliliğini korur.

Kamu SM'ye ait sertifikaların iptal bilgilerinin duyurulduğu SİL dosyası 3 (üç) ayda bir yenilenir. Sertifikanın iptali durumunda SİL dosyası derhal yenilenir.

### 4.9.8. Sertifika İptal Listesi Yayımlama Gecikme Süresi

Sertifika İptal Listesi, belirtilen yayımlama zamanından en geç 5 (beş) dakika sonra yayımlanır.

### 4.9.9. Çevrim İçi Sertifika İptal Durum Kaydı Desteği

Kamu SM, nitelikli elektronik sertifikaların iptal durum bilgisini ÇİSDUP üzerinden yayımlar. ÇİSDUP'dan yayımlanan iptal durum kaydı Kamu SM'ye ait olduğu duyurulan imza oluşturma verisiyle imzalanır.

ÇİSDUP desteği olan uygulamalar nitelikli elektronik sertifikanın geçerlilik durum kontrolünü ESHS Erişim Bilgisi sertifika uzantısında yer alan adres üzerinden gerçekleştirir.

### 4.9.10. Çevrim İçi Sertifika İptal Durum Kaydı Kontrol Gereksinimi

Kamu SM, sertifika iptal bilgisinin sisteme daha az yük getirecek biçimde yayımlanmasını sağladığı için, SİL yanında çevrim içi sertifika iptal durum kaydı desteğini de vermektedir.

SİL dosyası, iptal edilen her nitelikli elektronik sertifika için iptal bilgisinin eklenmesiyle gittikçe büyüyen bir dosya niteliğindedir. Güncel iptal durum kaydına her ihtiyaç duyulduğunda dosyanın Kamu SM bilgi deposundan indirilmesi gerekir. Gittikçe büyüyen SİL dosyasının sisteme getireceği yüke karşılık, ÇİSDUP ilgili nitelikli elektronik sertifikanın iptal olup olmadığı bilgisinin talep eden tarafa soru cevap yöntemiyle iletilmesine olanak tanımaktadır.Bu nedenle, üçüncü tarafların teknolojik altyapıları el verdiği ölçüde ÇİSDUP kullanmaları gerekir.

### 4.9.11. Diğer Sertifika Durum Bildirim Yöntemleri

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

### 4.9.12. İmza oluşturma Verisinin Güvenliğini Yitirmesi Durumu

Sertifika sahibine ait imza oluşturma verisinin güvenliğini yitirmesi durumunda nitelikli elektronik sertifika iptal edilir. Nitelikli elektronik sertifikanın iptal edilmesi dışında herhangi bir husus uygulanmamaktadır.

### 4.9.13. Sertifikanın Askıya Alındığı Durumlar

Nitelikli elektronik sertifikanın geçici bir süre için iptal durumunda olup sürenin sonunda yeniden kullanılabilir olmasını sağlamak amacıyla askıya alma işlemi tanımlanmıştır.

Sertifika sahibi, aşağıda belirtilenlere benzer sebeplerden dolayı nitelikli elektronik sertifikasını askıya almak isteyebilir:

- Sertifika sahibinin bir süreliğine görev başında olmaması ve nitelikli elektronik sertifikasını kullanım dışı bırakmak istemesi,
- Nitelikli elektronik sertifikanın iptal sebebinin ortaya çıktığından şüphelendiği halde, yanlışlıkla iptalini engellemek amacıyla, nitelikli elektronik sertifikayı önce askıya almak istemesi.

### 4.9.14. Sertifika Askıya Alma Başvurusunu Kimlerin Yapabildiği

Nitelikli elektronik sertifika askıya alma başvurusu sadece sertifika sahibi tarafından yapılır.

### 4.9.15. Sertifika Askıya Alma Başvurusunun İşlenmesi

Nitelikli elektronik sertifika askı başvurusu, sertifika sahibi tarafından telefonla çağrı merkezinden veya yazılı olarak Kamu SM'ye yapılır. Askı başvurusu alındığında öncelikle başvuruyu yapan sertifika sahibinin kimlik belirlemesi ve doğrulaması yapılır. Kimlik doğrulaması yapılamayan askı başvuruları işleme alınmaz.

Askıya alınan nitelikli elektronik sertifika için, SİL'de tanımlı geçici olarak iptal edildiğini belirten ifade kullanılır, ÇİSDUP Yanıtlayıcı'da sertifika durum bilgisi iptal konumuna getirilir. Kamu SM, nitelikli elektronik sertifika askıya alındıktan sonra, gerekli gördüğü durumlarda sertifika sahibini ve bağlı bulunduğu kurum tarafından yetkilendirilen kişiyi sertifikanın askıya alındığına dair bilgilendirir.

Kamu SM'ye ait Kök SHS ve Kamu ESHS sertifikaları askıya alınmaz.

### 4.9.16. Askıda Kalma Süresi

Böyle bir süre öngörülmemiştir.

## 4.10. Sertifika Durum Servisleri

Üçüncü kişiler, Kamu SM sertifika iptal durum kayıtlarına SİL ve ÇİSDUP servisleri aracılığıyla aşağıda belirtilen şekilde ulaşır.

### 4.10.1. İşletimsel Özellikleri

Üçüncü kişiler, sertifika iptal durum kayıtlarına Kamu SM'ye ait SİL dosyalarından erişebilirler. Kamu SM'ye ait SİL dosyalarına erişim bilgileri 2. Bölüm'de verilmiştir.

Üçüncü kişiler, iptal durum kaydını her kontrol etmek istediklerinde güncel SİL dosyasını Kamu SM bilgi deposundan kendi sistemlerine kopyalar ve gerekli kontrolleri yaparlar.

ÇİSDUP İstemci desteği olan üçüncü kişiler, sertifika iptal durumunu ÇİSDUP Yanıtlayıcı'dan öğrenebilirler. ÇİSDUP Yanıtlayıcı erişim adresi 2. Bölümde verilmiştir. Üçüncü kişiler nitelikli elektronik sertifika veya sertifikaların geçerlilik durumunu her kontrol etmek istediklerinde, ÇİSDUP Yanıtlayıcı üzerinden sorgulama yaparlar.

### 4.10.2. Servisin Erişilebilirliği

SİL ve ÇİSDUP servislerinin verildiği sistemlere erişimin kesintisiz olarak sağlanabilmesi için gereken tüm tedbirler Kamu SM tarafından alınır. Ancak buna rağmen erişimin bir süreliğine kesilmiş olması durumunda üçüncü kişiler, problem giderilinceye kadar sertifika iptal durum kaydını kontrol etmeleri gereken işlemlerini durdurur. Üçüncü kişilerin iptal durum kaydını, erişimin kesilmesi sebebiyle kontrol etmeden yaptıkları işlemlerden doğan zararlardan Kamu SM sorumlu tutulamaz.

### 4.10.3. İsteğe Bağlı Özellikler

Düzenlenmesine gerek duyulmamıştır.

## 4.11. Sertifika Sahipliğinin Sona Ermesi

Nitelikli elektronik sertifikanın kullanım süresinin dolması, iptal edilmesi ve Kamu SM'nin sertifika hizmetlerini sonlandırmasıyla sertifika sahipliği sona erer. Kamu SM nitelikli elektronik sertifikanın iptal edilmesi ve Kamu SM tarafından sertifika hizmetlerinin sonlandırılması durumunda sertifika sahibini ve varsa sözleşmelerde belirtilen kişileri bilgilendirir. Kullanım süresinin dolması durumunda Kamu SM sertifika sahibini bilgilendirmez; sertifika sahibi nitelikli elektronik sertifikasının kullanım süresinin dolduğu zamanı kendisi takip etmekle yükümlüdür.

## 4.12. Anahtar Yeniden Üretme

Sertifika sahiplerine ait anahtarların yeniden üretilmesi veya yedeklenmesi işlemi uygulanmamaktadır.

## 5. Yönetim, İşlemsel ve Fiziksel Kontroller

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

### 5.1. Fiziksel Güvenlik Denetimleri

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

#### 5.1.1. Tesis Yeri ve İnşaatı

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

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

Kamu SM'nin kurulduğu yer ve binada güç birimleri, haberleşme birimleri, havalandırıcılar, yangın söndürücüler mevcut olup, deprem, su ve afetlere karşı gerekli tedbirler alınmıştır.

#### 5.1.2. Fiziksel Erişim

Kamu SM yazılım ve donanım modülleri 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 gelişmiş erişim kontrol cihazlarıyla yapılmaktadır. Yetkisi olmayan kişiler sistemin kurulu olduğu odalara giriş yapamamaktadır. Yetkisiz kişilerin donanım bakımı veya bunun gibi sıra dışı bir amaçla sistemin kurulu olduğu odalara girişleri özel erişim talimatları uyarınca düzenlenir.

#### 5.1.3. Güç Kaynağı ve Havalandırma

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

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

Bina gerekli havalandırma sistemi 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 işlevlerinin yerine getirildiği ortamlarda yangını önleyici ve olası yangınlarda zararı en aza indirecek önlemler alınmıştır.

### 5.1.6. Saklama ve Yedekleme Ortamlarının Korunması

Kullanılan veri saklama ortamları (disk, CD, kağıt vs.) bozulmaya, yıpranmaya karşı fiziksel ve elektronik olarak korunur.

### 5.1.7. Atıkların Yok Edilmesi

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

### 5.1.8. Farklı Mekanlarda Yedekleme

Kamu SM, 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.

## 5.2. Prosedürsel Kontroller

### 5.2.1. Güvenilir Roller

Kamu SM'de çalışan personelin rolleri aşağıda belirtildiği şekilde sınıflandırılmıştır:

**Kamu SM Yöneticisi:** Kamu SM iç işleyişinin yürütülmesini, Kamu SM'nin yasal yükümlülüklerinin yerine getirilmesini, talimat ve politikaların uygun olarak kullanılmasını, gerekli gördüğü durumlarda değişiklik ve düzenlemelerin yapılmasını sağlar.

**Kamu SM Teknik Sorumlusu:** Kamu SM birimleri arasında teknik uyumun gerçekleşmesini sağlar. Teknik faaliyetleri gözden geçirir. Bilgi sistemlerinin güvenliğini ve performansını izler.

**Güvenlik Yöneticisi:** Kamu SM güvenlik yöntemleri ve politikalarının uygulanmasını takip eder. Zaman içinde sistemin güvenlik ihtiyaçlarını belirler ve bu ihtiyaçların giderilmesini koordine eder.

**Güvenlik İşletmeni:** İşletmen sınır güvenliği ile ilgili varlıkların işlerliğinden sorumludur. Güvenlik duvarları, saldırı tespit sistemi, kayıt sistemi ve antivirüs sistemi idamesini sağlar.

**Sistem Yöneticisi:** Güvenlik bileşenleri hariç bütün sistemin işletiminden sorumludur. Sistemde zaman içerisinde yapılması gereken değişiklikleri koordine eder.

**Sistem İşletmeni:** Bütün sunucuların işletim sistemi ve donanım idamesinden sorumludur. Bileşenlerle ilgili gerekli güncellemeleri yapar.

**Veri Sistemleri Yöneticisi:** Dizin ve veritabanı yığınlarının (cluster) yönetimini yapar. Veritabanı yönetim faliyetlerini gerçekleştirir.

**Sertifika Üretim Ekip Lideri:** Sertifikanın üretiminin planlanması, gerçekleştirilmesi ve sertifikaların teslimatı ile ilgili tüm çalışmaları yapar, sertifika üretim işletmenlerini koordine eder.

**Sertifika Üretim İşletmeni:** Nitelikli elektronik sertifika yaşam döngüsü işlemlerini Nitelikli Elektronik Sertifika Yönetim Prosedürleri'nde belirtildiği şekilde yapar. Sertifika yaşam döngüsü süreçleri kapsamında gelen ve giden evrakı kontrol eder ve arşivler.

**Denetçi:** Yönetim tarafından TÜBİTAK BİLGEM içinde uygunluk denetimleri yapan birimlerden veya Kamu SM bünyesinde çalışan personel arasından görevlendirilen bir kişi olan denetçi, sistem denetim profilinin kurulması, denetimlerin yönetimi ve gözden geçirilmesi ile sistemin teknik ve idari işleyişinin kontrolü ve raporlarının hazırlanmasından sorumludur.

#### 5.2.2. Her İşlem İçin Gereken Kişi Sayısı

Kamu SM, Kök SHS ve Kamu ESHS ye ait sertifika üretilmesi ve iptal edimesi için birden fazla kişinin aynı anda hazır bulunmasını sağlar.

Kamu SM, Kök SHS ve Kamu ESHS ye ait imza oluşturma verilerinin başka bir kriptografik modül içersine yedeklenmesi için birden fazla kişinin aynı anda hazır bulunmasını sağlar.

Nitelikli Elektronik Sertifika üretimi iki kişinin konrolünde gerçekleştirilir.

#### 5.2.3. Kimlik Doğrulama ve Yetkilendirme

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

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

#### 5.2.4. Görevlerin Ayrılmasını Gerektiren Roller

Tanımlanan roller içinde sertifika işletmenleri dışındakiler için bir kişi birden fazla rolden sorumlu olabilir.

### 5.3. Personel Güvenlik Kontrolleri

#### 5.3.1. Kişisel Geçmiş, Deneyim ve Nitelik Gerekleri

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

#### 5.3.2. Geçmiş Araştırması

Çalışanların Kamu SM'nin işletilmesinde güvenlik ihtiyaçlarının gerektirdiği güvenilirliğe sahip olması gerekmektedir. Personelin güvenilirliği geçmişine yönelik yapılan

araştırmalar ile belirlenir. İşe alınmadan önce geçmişe yönelik yapılan araştırmalarda personelin herhangi bir sebepten dolayı hüküm giyip giymemiş olduğu araştırılır.

#### 5.3.3. Eğitim Gerekleri

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

#### 5.3.4. Sürekli Eğitim Gerekleri ve Sıklığı

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

#### 5.3.5. Görev Değişim Sıklığı ve Sırası

Düzenlenmesine gerek duyulmamıştır.

#### 5.3.6. Yetkisiz Eylemlerin Cezalandırılması

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

#### 5.3.7. Anlaşmalı Personel Gereksinimleri

Kamu SM verdiği hizmetler için dış kaynak kullanmak durumunda kaldığında, bu hizmeti sağlayacak firma personeli ile ilgili güvenlik kontrollerini firma ile yaptığı sözleşme ile belirler

#### 5.3.8. Sağlanan Dokümantasyon

Çalışanlara işleriyle ve süreçlerle ilgili gerekli kılavuz ve destek dokümanları sağlanır.

### 5.4. Denetim Kayıtları

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

#### 5.4.1. Kaydedilen İşlemler

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

- Kamu SM anahtarlarının yaşam döngüsü yönetimi işlemleri
  - Anahtar üretimi
  - Anahtar yedekleme
  - Anahtar dağıtımı
  - Anahtar saklama
  - Anahtar arşivleme
  - Anahtar yok etme

- Kriptografik modül yaşam döngüsü işlemleri

- Nitelikli elektronik sertifika üretim, yenileme, askıya alma ve iptal başvuruları
  - Başvuru sahibi tarafından sunulan belgelerin neler olduğu bilgisi
  - Başvuru sırasında alınan kimlik tanımlamaya yarayan belgeler
  - Başvuru sırasında elektronik veya kağıt ortamda alınan form veya belgeler
  - Kağıt belgelerin kopyalarının nerede saklandığı bilgisi
  - Geçerli ve geçersiz alınan tüm başvuru bilgileri
- Nitelikli elektronik sertifika yaşam döngüsü yönetimi işlemleri
  - Nitelikli elektronik sertifika başvurusunun işlenmesi
  - Nitelikli elektronik sertifika sahibi için anahtar çifti üretimi
  - Nitelikli elektronik sertifika üretimi
  - Nitelikli elektronik sertifika sahibine ait güvenli elektronik imza oluşturma aracı ile ilgili yapılan işlemler
  - Güvenli elektronik imza oluşturma aracı dağıtımı
  - Nitelikli elektronik sertifika yenileme
  - Nitelikli elektronik sertifika askıya alma
  - Nitelikli elektronik sertifika askıdan çıkarma
  - Nitelikli elektronik sertifika iptal etme
  - Nitelikli elektronik sertifika yayımlanması
  - SİL yayımlanması
  - ÇİSDUP Yanıtlayıcı'dan duyurulan iptal durum kayıtları
- Güvenlikle ilgili diğer işlemler
  - Sisteme başarılı veya başarısız tüm erişim denemeleri
  - Çalışanlar tarafından gerçekleştirilen güvenlik sistemi işlemleri
  - Güvenli tutulması gereken hassas dosyaların okunması, yazılması ve değiştirilmesi
  - Güvenlik profili değişiklikleri
  - Sistemin çökmesi, donanım hataları ve diğer bozukluklar
  - Güvenlik duvarı (firewall) ve yönlendirici (router) işlemleri
  - Kamu SM'ye ziyaretçi giriş ve çıkışı

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

### 5.4.2. Kayıtların İncelenme Sıklığı

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

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

### 5.4.3. Kayıtların Saklanma Süresi

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

### 5.4.4. Kayıtların Korunması

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

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

### 5.4.5. Kayıtların Yedeklenmesi

Sistemin kritikliği göz önüne alındığında her gün düzenli olarak, sistemin yoğun olarak kullanılmadığı bir saatte gerekli görülen kayıtların çevrim içi yedeği alınmaktadır. Yedekleme ihtiyacını gidermek üzere teyp kütüphanesi ve yedekleme işlemlerini otomatikleştirmek için yedekleme yönetim yazılımı mevcuttur.

### 5.4.6. Kayıtların Toplanması

Kayıtlar uygulama katmanında, ağ katmanında ve işletim seviyesi düzeyinde otomatik olarak toplanır. Kamu SM çalışanları da sertifika işlemleri ile ilgili bilgi girişi yaptıklarında kayıt hazırlar.

### 5.4.7. Kayda Sebebiyet Veren Tarafın Bilgilendirilmesi

Kayıt oluşmasına sebep olan işlemi başlatan Kamu SM sertifika yönetim sistemi 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.

## 5.5. Kayıt Arşivleme

### 5.5.1. Arşivlenen Kayıt Bilgileri

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

- Sertifika sahibi veya bağlı bulunduğu kurum tarafından, başvuru sırasında verilen tüm bilgi ve belgeler
- Nitelikli elektronik sertifika yenileme, askıya alma, askıdaki sertifikayı kullanıma açma ve iptal başvuruları sırasında elektronik veya kağıt ortamda alınan formlar
- Nitelikli elektronik sertifika işlemleriyle ilgili yapılan önemli yazışmalar
- Üretilen tüm nitelikli elektronik sertifikalar
- Geçerlilik süresi dolan tüm Kamu SM Kök SHS ve Kamu ESHS sertifikaları
- Yayımlanan tüm sertifika iptal durum kayıtları
- Sertifika İlkeleri dokümanı
- Sertifika Uygulama Esasları dokümanı
- Zaman Damgası İlkeleri
- Zaman Damgası Uygulama Esasları
- Nitelikli elektronik sertifika yönetim prosedürleri
- Kurumlarla yapılan NES Temini Sözleşmeleri
- Nitelikli Elektronik Sertifika Sahibi Taahhütnameleri
- Kamu SM Taahhütnameleri
- Sertifika sahipleri ile yapılan Sertifika Sözleşmeleri

### 5.5.2. Arşivlerin Tutulma Süresi

Arşivlenen bilgiler ve belgeler Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik uyarınca en az 20 (yirmi) yıl boyunca saklanır.

### 5.5.3. Arşivlerin Korunması

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

### 5.5.4. Arşivlerin Yedeklenmesi

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

### 5.5.5. Kayıtların Zaman Damgası Gereksinimleri

Kamu SM gerekli gördüğü kayıtlara zaman damgası ekler.

### 5.5.6. Arşivlerin Toplanması

Arşivler elektronik veya kağıt ortamda toplanır.

### 5.5.7. Arşiv Bilgilerinin Elde Edilme ve Doğrulanma Metodu

Arşiv bilgileri yetkili personelden edinilir. Yasal gereksinimlerin ortaya çıkması ya da BTK tarafından denetim amacıyla talep edilmesi durumunda yetkili personel eşliğinde arşiv bilgileri elde edilebilir.

### 5.6. Anahtar Değişimi

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

- Sertifika kullanım süresinin dolmasından en geç 6 (altı) ay önce işlemler başlatılır. Eski anahtarlarla sertifika verilmesi durdurulur.
- Kamu SM'nin eski imza oluşturma verisiyle imzalanmış nitelikli elektronik sertifikaların doğrulanabilmesi için, eski Kamu SM sertifikası yayımlanmaya devam eder.
- SİL dosyası aynı Kamu SM imza oluşturma verisiyle imzalanıyorsa, Kamu SM'nin eski imza oluşturma verisiyle oluşturulmuş nitelikli elektronik sertifikaların kullanım tarihleri dolana kadar, Kamu SM SİL'leri eski imza oluşturma verisiyle imzalamaya devam eder. Yeni üretilen nitelikli elektronik sertifikalar için oluşturulan SİL dosyası yeni Kamu SM imza oluşturma verisiyle imzalanır.
- Kamu SM anahtarlarının yenilendiği bilgisini http://www.kamusm.gov.tr internet adresi üzerinden duyurur ve sertifika hizmeti verdiği kurumları bilgilendirir.

### 5.7. Güvenliğin Yitirilmesi ve Arıza Durumlarında Yapılacaklar

#### 5.7.1. Güvenilirliğin Yitirilmesi Durumunun Düzeltilmesi

Güvenilirliğin yitirilmesi durumlarında, sertifika yönetim sisteminin en kısa zamanda yeniden güvenli olarak çalışmaya başlaması, durumdan etkilenen tarafların haberdar edilmesi, zararlarının en aza indirgenmesi için belirlenen süreçler işletilir.

#### 5.7.2. Donanım, Yazılım veya Veri Bozulması

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

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

#### 5.7.3. İmza Oluşturma Verisinin Gizliliğinin Kaybedilmesi

Kamu SM'nin nitelikli elektronik sertifika imzalamada kullandığı imza oluşturma verisinin gizliğinin kaybedildiğinden şüphelenilmesi ya da bunun öğrenilmesi durumunda ilgili sertifika en kısa zamanda iptal edilir ve aşağıdaki işlemler yerine getirilir:

- Kamu SM kendisine ait sertifikanın iptal edildiğini, iptal sebebi ile birlikte en hızlı şekilde http://www.kamusm.gov.tr internet adresi üzerinden duyurur ve ilgili kurumları yazıyla bilgilendirir.
- Kamu SM, nitelikli elektronik sertifika sahiplerinin durumdan ne şekilde etkileneceğini belirten açıklamayı yapar, eski gizli anahtarıyla oluşturulan nitelikli elektronik sertifikalara güvenilmemesi için ilgili taraflara ihtarda bulunur.

- Kamu SM, kendisine ait sertifikanın iptal edildiği bilgisini yayımladığı SİL dosyasında belirtir.
- Kamu SM, tarafından üretilen nitelikli elektronik sertifikaların gerekli görünen bir kısmı veya hepsi iptal edilir. İptal bilgisi sertifika sahipleri ile ilgili kurumlara en kısa zamanda bildirilir.
- Kamu SM nitelikli elektronik sertifika isteklerine yanıt vermeyi durdurur.
- İlgili taraflar Kamu SM'nin durumuyla ilgili sürekli bilgilendirilir.
- Kamu SM imza oluşturma verisinin yok edilmesi sürecini işletir.
- Kamu SM, yeni bir anahtar çifti ve sertifika üreterek yeni sertifikayı taraflara bildirir.
- Kamu SM anahtar çiftinin yenilenmesiyle, iptal edilen nitelikli elektronik sertifikaların sertifika sahibinden gelen talep doğrultusunda sertifika yenileme süreci başlatılır.

### 5.7.4. Arıza Sonrası Yeniden Çalışırlık

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

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

## 5.8. Sertifika Hizmetlerinin Sonlandırılması

Kamu SM, işleyişine Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik'te belirtilen şekilde son verebilir. Bu durumda Kamu SM aşağıdaki işlemleri yerine getirir:

- Sertifika hizmetlerine son vereceği tarihten 3 (üç) ay öncesine kadar durumu sertifika hizmeti verdiği bütün kurumlara yazı ile, sertifika sahiplerine 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 nitelikli elektronik sertifikaları iptal eder, iptal bilgisini SİL ve ÇİSDUP aracılığıyla üçüncü kişilere duyurur. İptal ettiği nitelikli elektronik sertifikaların bilgisini kurumlara yazılı olarak, sertifika sahiplerine e-posta ile duyurur.
- İptal ettiği nitelikli elektronik sertifikaların kullanım süreleri dolana kadar en son ürettiği SİL dosyasını yayımlamaya devam eder.
- SİL dosyasını imzalamada kullandığı imza oluşturma verisine karşılık gelen sertifikasını, SİL dosyasının geçerlilik süresi boyunca yayımlamaya devam eder.
- Nitelikli elektronik sertifikaları imzalamak için kullandığı imza oluşturma verisini imha eder.
- İlgili tüm kayıtları ve arşivleri uygun bir şekilde 20 (yirmi) yıl boyunca korur.

## 6. Teknik Güvenlik Kontrolleri

Kamu SM'nin kendisi ve sertifika sahipleri adına, anahtar çiftleri ve erişim verilerini ürettiği, sertifika yönetim işlemlerini gerçekleştirdiği sistemler CWA 14167-1, ETSI TS 101 456 ve TS ISO/IEC 27001 veya ISO/IEC 27001 gereklerini sağlar.

### 6.1. Anahtar Çifti Üretimi ve Kurulumu

### 6.1.1. Anahtar Çifti Üretimi

#### 6.1.1.1. Kök SHS, Kamu ESHS, ÇİSDUP Yayınlayıcı Anahtar Çifti Üretimi

Kamu SM bünyesinde aşağıdaki imza oluşturma ve doğrulama verileri oluşturulur..

- Kök SHS'ye ait imza oluşturma ve doğrulama verisi
- Kamu ESHS'ye ait imza oluşturma ve doğrulama verisi
- ÇİSDUP yayınlayıcıya ait imza oluşturma ve doğrulama verisi
- NES sahiplerine ait imza oluşturma ve doğrulama verileri

Kök SHS, Kamu ESHS ve ÇİSDUP yanıtlayıcı'ya ait anahtar çiftleri, yetkisi olmayan personelin giremeyeceği gizli odada, birden fazla eğitimli personelin gözetiminde, ağ ortamına kapalı sistemlerde, güvenli anahtar üretimi için gereken testlerden geçmiş, güvenli yazılım kullanılarak üretilir. Üretilen imza oluşturma verisi güvenli kriptografik modül içinde saklanır. Modül güvenli odadan dışarıya çıkarılmaz. Yapılan bütün işlemler kayıt altına alınır ve işlemi gerçekleştiren personeller tarafından onaylanır.

İmza oluşturma verisinin saklandığı kriptografik modül Bölüm 6.2.1'de belirtilen standartlara uyar.

#### 6.1.1.2. Sertifika Sahibi Anahtar Çiftinin Üretimi

Sertifika sahibinin anahtar çiftleri Kamu SM tarafından yetkisi olmayan personelin giremediği odalarda, güvenli yazılım kullanılarak üretilir ve şifrelenerek güvenli elektronik imza oluşturma aracı içinde saklanır.

Anahtar çiftleri güvenli anahtar üretimi için gereken testlerden geçmiş, güvenilir programlar kullanılarak üretilir. Anahtar çifti üretmek için güvenilirliği dünyaca kabul görmüş algoritmalar kullanılır. Anahtar çiftleri RSA, DSA, DSA Eliptik Eğrisi elektronik imza algoritmaları ile kullanılmak üzere üretilirler.

Sertifika sahibine ait imza oluşturma verisinin yedeği alınmaz, bir kopyası hiçbir şekilde sistemde tutulmaz. Güvenli elektronik imza oluşturma aracı sertifika sahibine teslim edilene kadar yetkisiz kişilerin erişemediği güvenli ve kilitli odalarda saklanır.

Sertifika sahibine ait imza oluşturma verisinin saklandığı güvenli elektronik imza oluşturma aracı Bölüm 6.2.1'de belirtilen güvenlik standartlarına uyar.

### 6.1.2. Sertifika Sahibine İmza Oluşturma Verisinin Ulaştırılması

Sertifika sahiplerine ait anahtar çiftlerinin Kamu SM tarafından oluşturulmasına müteakip, imza oluşturma verisi, sertifika ile birlikte güvenli elektronik imza oluşturma aracına yüklenir. Güvenli elektronik imza oluşturma aracı imza karşılığı ve resmi kimlik kontrolü yapılarak sahibine teslim edilir.

Güvenli elektronik imza oluşturma aracı erişim verisi ise iki farklı yöntem ile teslim edilir;

- Kapalı parola zarfı: Sertifika teslim fişi Kamu SM'ye ulaştıktan sonra, güvenli elektronik imza oluşturma aracı erişim verisi parola zarfına yazılarak kapatılır. Bu işlem operatörün bu verileri göremeyeceği şekilde gerçekleşir. Kapalı parola zarfı sertifika sahibine iletilir ve kimlik kontrolü ve imza karşılığı teslim edilir.
- Web üzerinden: Web üzerinden teslim edilen veriler için güvenli bağlantı protokolleri (https) kullanılmaktadır. Sertifika sahibinin kimlik kontrol için,T.C. kimlik no, başvuru formunu doldururken tanımladığı güvenlik sözcüğü ve mobil telefona gönderilen SMS onay mesajı kullanılmaktadır. Bu şekilde gerçekleştirilen kimlik doğrulaması sonrasında sertifika sahibi güvenli elektronik imza oluşturma aracı erişim verisine erişir.

Kamu SM, kurum ile yapılan sözleşmelerde belirtilmiş ise, kurum personeline ait, içerisinde imza oluşturma verisi ve sertifika olan güvenli elektronik imza oluşturma araçlarını ve güvenli elektronik imza oluşturma aracı erişim verilerini toplu olarak kurum yetkilisine imza karşılığında teslim eder. Kamu SM'nin yükümlülüklerinin belirtildiği Kamu SM Taahhütnamesi http://www.kamusm.gov.tr/BilgiDeposu adresinden yayınlanır.

### 6.1.3. Elektronik Sertifika Hizmet Sağlayıcısı'na İmza Doğrulama Verisinin Ulaştırılması

Sertifika sahiplerine ait nitelikli elektronik sertifikalarla ilgili anahtar çiftleri Kamu SM tarafından üretildiği için imza doğrulama verisinin Kamu SM'ye ulaştırılması söz konusu değildir.

### 6.1.4. Elektronik Sertifika Hizmet Sağlayıcısı Sertifikalarına Erişim Sağlanması

Kamu SM'ye ait Kök SHS ve Kamu ESHS sertifikaları internet ortamında tarafların erişimine hazır bulundurulur. Sertifikanın yayımlandığı ortamın izinsiz değiştirmeye ve silinmeye karşı güvenliği sağlanır.

Kamu SM'ye ait sertifikalar internet üzerinden yayımlanır.

Kök SHS ve Kamu ESHS sertifikasının özet değeri ve özet algoritması http://www.kamusm.gov.tr web adresi üzerinden yayımlanır ve Kamu SM'nin faaliyete geçmesini müteakip 7 (yedi) gün içinde ulusal yayın yapan en yüksek trajlı 3 (üç) gazetede ilan vermek suretiyle kamuoyuna duyurulur.

### 6.1.5. Anahtar Uzunlukları

Kamu SM Kök SHS'ye ait, RSA açık anahtar algoritması imza oluşturma anahtar çiftinin boyu en az 2048-bittir.

Sertifika sahiplerine ait nitelikli elektronik sertifikaları imzalayan Kamu ESHS'ye ait, RSA açık anahtar algoritması imza oluşturma anahtar çiftinin boyu en az 2048-bittir.

ÇİSDUP Yanıtlayıcı'dan duyurulan iptal durum kayıtlarını imzalamak için kullanılan RSA imza oluşturma anahtar çiftlerinin boyu en az 2048-bittir.

Kamu SM tarafından üretilen nitelikli elektronik sertifika sahiplerine ait, RSA imza oluşturma anahtar çiftlerinin boyu en az 2048-bittir.

### 6.1.6. Anahtar Üretim Parametreleri ve Kalitesinin Kontrolü

Kamu SM tarafından anahtar üretiminde kullanılan algoritmaların güvenliği ispatlanmış ve dünyaca kabul görmüştür. Algoritmaların gerçekleştiriminde kullanılan yöntemler gerekli güvenlik kriterlerini sağlar. Anahtarları üreten programlar gerekli güvenlik testlerinden geçirilirler.

### 6.1.7. Anahtar Kullanım Amaçları

Kök SHS'ye ait imza oluşturma verisi, kendi sertifikasını, Kamu ESHS'ye ait sertifikayı ve yürüttükleri görevler açısından özel niteliği haiz Türk Silahlı Kuvvetleri, Emniyet Genel Müdürlüğü, MİT Müsteşarlığı, Jandarma Genel Komutanlığı, Sahil Güvenlik Komutanlığı, Dışişleri Bakanlığı ve Telekomünikasyon Kurumu bünyesinde kurulabilecek olan ESHS lerin sertifikalarını imzalamak amacıyla kullanılır.

Kamu ESHS'ye ait imza oluşturma verisi, Kamu ESHS tarafından oluşturulan nitelikli elektronik sertifikaların ve yayınlanan SİL dosyalarının imzalanması amacıyla kullanılır.

ÇİSDUP yayınlayıcıya ait imza oluşturma verisi, ÇİSDUP yanıtlayıcıdan duyurulan iptal durum kayıtlarının imzalanması amacıyla kullanılır.

NES sahiplerine ait imza oluşturma verileri Elektronik İmza Kanunu'nda tanımlı güvenli elektronik imzayı üretmek kullanılırlar. Sertifika sahibi, güvenli elektronik imza oluşturma aracı içinde bulunan imza oluşturma verisini imza oluşturma dışında kullanmaz. Üçüncü kişiler, nitelikli elektronik sertifikalar içindeki imza doğrulama verilerini, sertifika sahibi tarafından oluşturulmuş elektronik imzanın doğruluğunu kontrol etmek için kullanır. Anahtar çiftlerinin güvenli elektronik imza oluşturma ve doğrulama dışında kullanımlarından doğan sorumluluk sertifika sahibine ve üçüncü kişilere aittir; Kamu SM bu durumda sertifika sahibinin veya üçüncü kişilerin gördükleri zarardan sorumlu tutulamaz.

## 6.2. İmza Oluşturma Verisinin Korunması

### 6.2.1. Kriptografik Modül Standartları

Kamu SM'ye ait imza oluşturma verisi güvenli yazılım kullanılarak üretilir, güvenli kriptografik modül içinde saklanır ve geçerli olduğu süre boyunca bu modül dışına çıkmaz.

Kriptografik modül aşağıda belirlenen güvenlik işlevlerine sahiptir:

- İmza oluşturma verisinin geçerlilik süresi boyunca gizlilik ve bütünlüğünü sağlar.
- Modüle erişimde kimlik belirleme ve doğrulama işlevlerini yerine getirir.
- Erişim yetkisi birden fazla kişinin kontrolünde olacak şekilde tanımlanabilir.
- Sistem kullanıcısına tanımlanan roller doğrultusunda, verdiği hizmetlere erişimi sınırlar.
- Düzgün çalıştığı test edilebilir, test sırasında hata oluştuğunda güvenli duruma geçer.
- Modüle izinsiz erişim ve kullanım ile tahrifata yol açabilecek her türlü fiziksel önlem alınmıştır.
- Yetkisiz erişime teşebbüs edilmesi durumunda, modül içindeki veriyi siler.
- İmza oluşturma verisinin yedeğinin güvenli biçimde alınmasına olanak verir.

- Sertifika sahibinin imza oluşturma verisinin içinde bulunduğu güvenli elektronik imza oluşturma aracı, imza oluşturma verisinin aracın dışına çıkmasını engelleyen ve araca erişimi parola ile sağlayan teknik özelliklere sahiptir.

Kriptografik modül ve sertifika sahibinin güvenli elektronik imza oluşturma aracı Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de belirtilen aşağıdaki güvenlik standartlarından en azından birisini sağlar:

- FIPS PUB 140-1 veya FIPS PUB 140-2'ye göre seviye 3 veya üzeri,
- CWA 14169 standardına uygun ve TS ISO/IEC 15408 (-l,-2,-3)'e veya ISO/IEC 15408 (-1,-2,-3)'e göre en az EAL4+.

### 6.2.2. İmza Oluşturma Verisine Birden Fazla Kişi Kontrolünde Erişim

Kamu SM'ye ait imza oluşturma verisinin bulunduğu odaya erişim 2 (iki) çalışan tarafından sağlanmaktadır.

### 6.2.3. İmza Oluşturma Verisinin Yeniden Elde Edilmesi

Düzenlenmesine gerek duyulmamıştır.

### 6.2.4. İmza Oluşturma Verisinin Yedeklenmesi

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

Sertifika sahiplerine ait imza oluşturma verileri Kamu SM tarafından yedeklenmez.

### 6.2.5. İmza Oluşturma Verisinin Arşivlenmesi

Kamu SM'ye ve sertifika sahiplerine ait imza oluşturma verileri arşivlenmez. Kullanım süreleri sonunda geri dönüşsüz şekilde silinir.

### 6.2.6. İmza Oluşturma Verisinin Kriptografik Modüle Yüklenmesi

Kamu SM'ye ait imza oluşturma verisi üretildikten hemen sonra kriptografik modüle yüklenir. İşlem, güvenilir yöntemlerle ve birden fazla yetkili personelin denetiminde yerine getirilir.

Sertifika sahiplerine ait imza oluşturma verileri, sadece yetkili personelin giriş izninin bulunduğu odalarda güvenli elektronik imza oluşturma aracına, şifrelenerek yüklenir. İmza oluşturma verisi güvenli elektronik imza oluşturma aracına yüklendikten sonra kopyası sistemden silinir.

### 6.2.7. İmza Oluşturma Verisinin Kriptografik Modülde Saklanması

Kamu SM'ye ait imza oluşturma verileri, yetkisiz kişilerin erişimine kapalı, fiziksel ve elektronik olarak güvenli kriptografik donanım cihazı içinde tutulur. İmza oluşturma verisinin yedekleme amacı haricinde cihaz dışına çıkması engellenmiştir. İmza oluşturma verisi kriptografik modül içinde güvenli algoritma ve yöntemlerle şifreli olarak saklanır.

Sertifika sahibine ait imza oluşturma verisi sertifika sahibinin güvenli elektronik imza oluşturma aracı içinde saklanır, başka bir ortamda bulunmaz. Kamu SM sertifika sahiplerine ait imza oluşturma verilerini kendi sistemi içinde saklamaz.

### 6.2.8. İmza Oluşturma Verisine Erişim

Kamu SM'nin imza oluşturma verisine erişim birden fazla yetkili çalışanın ortak denetimi altındadır. İmza oluşturma verisinin bulunduğu odaya giriş için, tanımlanan yetkililerin aynı anda hazır bulunması ve elektronik olarak kimliklerinin ve yetkilerinin doğrulanması gerekir. Yeterli sayıda yetkili personelin hazır bulunmadığı ve kimliklerinin doğrulanamadığı durumlarda imza oluşturma verisinin bulunduğu odaya erişim sağlanamaz.

İmza oluşturma verisi kriptografik modül içinde şifreli durumdayken erişime kapalıdır. Erişime açılması için erişimi sağlayan verinin modüle sunulması gerekir. İmza oluşturma verisinin erişime açılması ve kullanılır duruma getirilmesi birden fazla yetkili çalışanın ortak denetimi altındadır.

Sertifika sahibine ait imza oluşturma verisi güvenli elektronik imza oluşturma aracı içinde sertifika sahibinin erişim verisi ile korunmuş olarak saklanır. Erişim denetimi erişim denetim verisi ile sağlanır.

### 6.2.9. İmza Oluşturma Verisine Erişimin Kesilmesi

Kamu SM'nin imza oluşturma verisi imzalama için kullanıldıktan sonra oturum kapandığında veriye erişim otomatik olarak kesilir ve bir dahaki kullanımına kadar şifrelenerek erişime kapalı tutulur. Erişimin yeniden sağlanabilmesi için Bölüm 6.2.8'de belirtilen yöntemin yeniden işletilmesi gerekir.

Sertifika sahibinin kullandığı güvenli donanım araçları, imza oluşturma verisini kullanan oturumun kapanmasından sonra veriye erişimi kesecek biçimde çalışır. Erişimin yeniden sağlanabilmesi için sertifika sahibinin erişim verisini yeniden girmesi gerekir. Erişim verisinin ard arda 3 (üç) defa yanlış girilmesi durumunda güvenli elektronik imza oluşturma aracı kilitlenir ve araca erişim sağlanamaz.

### 6.2.10. İmza Oluşturma Verisinin Yok Edilmesi

Kamu SM'ye ait imza oluşturma verileri kullanım süresinin dolmasının ardından, aslı ve bütün yedekleri bulundukları ortamlardan uygun yöntemlerle geri dönüşsüz şekilde silinir. Kamu SM'ye ait imza oluşturma verisinin silinmesi işlemi için Bölüm 6.2.8'de belirtilen şekilde yeterli sayıda yetkili personelin hazır bulunması gerekir.

Sertifika sahiplerine ait imza oluşturma verileri kullanım süresinin sonunda veya sertifikanın iptal edilmesinden sonra sahibi tarafından güvenli elektronik imza oluşturma aracı üzerinden silinmelidir. Bu işlemin yapılmasından sertifika sahibi sorumludur.

### 6.2.11. Kriptografik Modülün Değerlendirilmesi

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

## 6.3. Anahtar Çifti Yönetimiyle İlgili Diğer Konular

### 6.3.1. İmza Doğrulama Verisinin Arşivlenmesi

Kamu SM'ye ve sertifika sahibine ait imza doğrulama verileri sertifikalar içinde tutulur ve nitelikli elektronik sertifikalar kullanım sürelerinin dolmasından itibaren 20 (yirmi)

yıl boyunca arşivlenir. Nitelikli elektronik sertifikaların arşivleri yetkisiz kişilerce tahrifatına ve silinmesine karşı gerekli önlemlerin alındığı ortamlarda tutulur.

### 6.3.2. İmza Oluşturma ve Doğrulama Verilerinin Kullanım Süreleri

İmza oluşturma verisinin kullanım süresi, nitelikli elektronik sertifikanın içeriğinde belirtilen nitelikli elektronik sertifika kullanım süresi kadardır. Nitelikli elektronik sertifikanın kullanım süresinin dolmasıyla ya da nitelikli elektronik sertifikanın iptal edilmesiyle imza oluşturma verisinin kullanımı sona erer. Ancak, kullanım süresi dolsa bile nitelikli elektronik sertifikalar içindeki imza doğrulama verileri geçmişe yönelik imzaların doğrulanabilmesi için kullanılır.

Kamu SM'ye ve sertifika sahibine ait anahtar çiftlerinin kullanım süresi, anahtar uzunlukları ve kullanılan imza algoritmasına göre belirlenir. Kamu SM'ye ait 2048 ve 4096 bitlik RSA anahtar çiftleri en fazla 10 (on) yıl için kullanılır. Sertifika sahiplerine ait 2048 bitlik RSA anahtar çiftleri en fazla 3 (üç) yıl için kullanılır.

Üretilen nitelikli elektronik sertifikaların son kullanma tarihi kendisine nitelikli elektronik sertifika veren Kamu SM'ye ait SHS sertifikasının son kullanma tarihini aşamaz.

## 6.4. Erişim Denetim Verileri

Kamu SM çalışanlarının erişim denetim verileri erişim parolalarını, güvenli donanım araçları içindeki erişim denetimi sağlayan diğer verileri, biyometrik verileri içerir.

Sertifika sahibine ait iki farklı erişim denetim verisi tanımlanmıştır. Bunlar, güvenli elektronik imza oluşturma aracı erişim verisi ile internet ve çağrı merkezi üzerinden erişerek askıdaki nitelikli elektronik sertifikaları kullanıma açma ve iptal etme işlemlerinin yapılabilmesi için kullanılan güvenlik sözcüğüdür.

### 6.4.1. Erişim Denetim Verilerinin Oluşturulması

Kamu SM sistemi içinde kullanılan erişim denetim verileri ile sertifika sahibine ait erişim parolaları yetkisiz kişilerin erişimine kapalı, fiziksel ve elektronik olarak güvenli ortamlarda, sistem tarafından yeterli uzunlukta, tahmin edilemez nitelikte ve rasgele üretilir.

Kamu SM tarafından sertifika sahibi adına oluşturulan erişim parolaları da yukarıdaki paragrafta belirtilen güvenlik şartlarını sağlar.

### 6.4.2. Erişim Denetim Verilerinin Korunması

Kamu SM sistemi içinde kullanılan erişim denetim verileri yalnızca yetkili çalışanlar tarafından bilinir.

Sertifika sahibine ait erişim parolaları sertifika sahibine güvenli yöntemlerle ulaştırılır.

Erişim parolaları ilk kullanımda sertifika sahibi tarafından değiştirilir. Parolayı yetkisiz kişilerin erişimine karşı korumak sertifika sahibinin yükümlülüğü altındadır.

### 6.4.3. Erişim Denetim Verileri İle İlgili Diğer Konular

Erişim denetimi verilerinin sahibine ulaştırılması güvenli yollarla yapılır. Sertifika sahibine ait erişim parolaları, kapalı zarf içinde, resmi kimlik kontrolü yapılarak imza karşılığı ya da iki kademeli kimlik doğrulama ile erişilen web sayfası üzerinden sahibine teslim edilir.

### 6.5. Bilgisayar Güvenliği Denetimleri

#### 6.5.1. Bilgisayar Güvenliği İle İlgili Teknik Gerekler

Kamu SM sistemi içinde 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. Kritik işlemlerin yapıldığı bilgisayarlar ağ ortamı dışında tutulur. Bilgilerinin tahrifata, silinmeye ve kaçağa karşı korunması ve işletimin sürekliliğinin sağlanması için gerekli güvenlik sağlanır. Her kurulan yazılımın yedek kopyası yaratılır ve sistemin güvenliği konusunda bütün iyileştirme eylemleri gecikmesiz uygulanır.

#### 6.5.2. Bilgisayar Sisteminin Sağladığı Güvenlik Seviyesi

Düzenlenmesine gerek duyulmamıştır.

### 6.6. Yaşam Döngüsü Teknik Denetimleri

#### 6.6.1. Sistem Geliştirme Denetimleri

Sistem geliştirilirken genel anlamda yapılan denetimler 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 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 TS ISO/IEC 27001 gereklerini sağlar.

#### 6.6.2. Güvenlik Yönetimi Denetimleri

Sistem içinde kurulu olan yazılım ve donanım ürünleri ile ağ ortamının işleyişinin planlanan şekilde güvenli olarak sürdürüldüğünü göstermek için iki (2) yılda en az bir defa güvenlik yönetimi denetimi yapılır. Kamu SM içinde güvenliğe uygun olmayan hareketler ve yetkilendirmeler denetleme sonucunda açıklanır ve düzeltici önlemler alınır.

#### 6.6.3. Yaşam Döngüsü Güvenlik Denetimleri

Düzenlenmesine gerek duyulmamıştır.

### 6.7. Ağ Güvenliği Denetimleri

Son teknolojik gelişmeler göz önünde bulundurularak gerekli ağ güvenliği denetimleri yapılır. Sistem, dış açık ağa bağlantısında güvenlik duvarlarını 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 sunucuları mevcuttur.

Sunucular üzerine ağ ve sistem yönetimi ajanları kurulmuştur. Yönetim yazılımı bu ajanlardan disk, hafıza, işlemci kullanımı gibi 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 yazılımı çektiği bilgileri merkezi bir veri tabanında saklar. Böylece herhangi bir anda verilerin sorgulanmasına ve geçmişe dönük rapor üretilmesine imkan tanınır.

Yüksek güvenlik gerektiren işlemlerin yapıldığı sistemler için farklı ağlar kurulmuştur. Kritik işlemlerin yapıldığı sistemler ağa bağlı değildir.

### 6.8. Zaman Damgası

Kamu SM sistemi içinde kullanılan zaman damgası gerekli kesinlik ve bütünlük şartlarını sağlar. Kamu SM sistemi içinde kullanılan zaman damgası Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de belirtilen şartlara uyar.

Zaman damgasıyla ilgili ayrıntılı bilgi Zaman Damgası İlkeleri ve Zaman Damgası Uygulama Esasları'nda bulunur.

## 7. Sertifika ve Sertifika İptal Listesi Biçimleri

### 7.1. Sertifika Biçimi

Bu bölümde Kamu SM tarafından dağıtılan nitelikli elektronik sertifikaların içeriği ile ilgili bilgilendirme yapılmaktadır.

#### 7.1.1. Sürüm Numarası

Kamu SM "ITU-T X.509 V.3" sertifika standardını destekler.

#### 7.1.2. Sertifika Uzantıları

Kamu SM tarafından dağıtılan nitelikli elektronik sertifikalar X.509 V.3 formatında tanımlanan sertifikanın seri numarası, geçerlilik tarihi, ilgili imza doğrulama verisi, sertifika sahibine ve sertifikayı yayımlayan Kamu SM'ye ait isim bilgileri ve Kamu SM'nin elektronik imzası gibi zorunlu alanların yanı sıra X.509 V.3 sertifika uzantılarını içerir. Nitelikli elektronik sertifikanın içeriğinde bulunan sertifika uzantıları sertifikanın kullanılacağı uygulamanın gereklerine bağlı olarak belirlenir.

Aşağıdaki tabloda Kamu SM tarafından üretilen nitelikli elektronik sertifikada asgari düzeyde bulunması gereken uzantılar tanımlanmıştır.

| Sertifika Uzantısı | Kritik Uzantı | Açıklama |
|---|---|---|
| Temel Kısıtlar[1] | HAYIR | Sertifikanın son kullanıcı sertifikası olduğu, ESHS sertifikası amacıyla kullanılamayacağı belirtilir. |
| ESHS Anahtar Tanımlayıcı[2] | HAYIR | Kamu SM'ye ait Kamu ESHS açık anahtarının SHA-1 özet çıktısından oluşur. |
| Sertifika Anahtar Tanımlayıcı[3] | HAYIR | Sertifikanın içeriğindeki "subjectPublicKey" alanının "BIT STRING" olarak değerinin SHA-1 özet çıktısından oluşur. |
| Anahtar Kullanım[4] | EVET | Anahtarların sadece elektronik imza amaçlı kullanıldığının ifade edilmesi için "nonRepudiation" [inkar edilemezlik] alanı ve "digitalSignature" [sayısal imza] alanı seçilmiştir. |
| SİL Yayımlama Adresi[5] | HAYIR | http://www.kamusm.gov.tr/BilgiDeposu/<br><br>ldap://dizin.kamusm.gov.tr/ |

[1] BasicConstraints
[2] AuthorityKeyIdentifier
[3] SubjectKeyIdentifier
[4] KeyUsage
[5] CRLDistributionPoints

| | | |
|---|---|---|
| ESHS Erişim Bilgisi[6] | HAYIR | http://www.kamusm.gov.tr/BilgiDeposu/<br><br>ldap://dizin.kamusm.gov.tr/<br><br>http://ocsp. kamusm.gov.tr/ |
| Sertifika İlkeleri[7] | HAYIR | Kamu SM Sİ dokümanına ait nesne tanımlama numarası (2.16.792.1.2.1.1.5.7.1.1) ile SUE dokümanının bulunduğu http://www.kamusm.gov.tr/BilgiDeposu/Kamu SM_NES_SUE internet adresini ve TK tarafından oluşturulan nitelikli elektronik sertifika ibaresine ait metni içerir. |
| Nitelikli Elektronik Sertifika İbaresi[8] | EVET | ETSI 101 862'ye göre, id-etsi-qcs-QcCompliance= 0.4.0.1862.1.1 nesne tanımlama numarasını ve varsa sertifikanın kullanımına ilişkin maddi sınır bilgisini içerir.<br><br>Telekomünikasyon Kurumu tarafından belirlenen nitelikli elektronik sertifika ibaresi ile bu ibareye ait nesne tanımlama numarası bilgisini içerir. |

Uzantılardan bazıları kritik olarak tanımlanmıştır. Kritik olarak belirtilen uzantıların sertifikayı kullanan uygulama tarafından tanımlanamaması durumunda sertifika kullanılamaz.

Kamu SM tarafından kişilere verilen nitelikli elektronik sertifikaların kullanımına ilişkin, varsa maddi sınırlamalar ile ilgili bilgilendirme ETSI 101 862'ye göre "Nitelikli Elektronik Sertifika İbaresi Uzantısı" içinde yapılır.

Sertifikanın nitelikli olduğu "Nitelikli Elektronik Sertifika İbaresi Uzantısı" içerisindeki ETSI ve Telekomünikasyon Kurumu'na ait nitelikli elektronik sertifika ibareleri ile belirtilir.

Telekomünikasyon Kurumu tarafından belirlenen ibare "Nitelikli Elektronik Sertifika İbaresi Uzantısı" içinde yer alan "İbare Bilgisi[9]" alanının içine yazılır. Bu ibareye ait nesne tanımlama numarası ise "İbare Numarası[10]" alanı içinde yer alır. Bu ibare ve ibareye ait nesne tanımlama numarası aşağıda belirtilmiştir.

**"Bu sertifika 5070 sayılı Elektronik İmza Kanununa göre nitelikli elektronik sertifikadır."**

Nesne tanımlama numarası: 2.16.792.1.61.0.1.5070.1.1

{joint-iso-itu-t(2) ülke(16) tr(792) tk(61.0.1) nes-profili(5070) nes-ibaresi (1) nes-uygunlugu (1)}

### 7.1.3. Algoritma ve Nesne Tanımlayıcılar

Kamu SM, kişilere verdiği nitelikli elektronik sertifikaları imzalamak için SHA-1 özet algoritması ile RSA açık anahtarlı imzalama algoritmasını kullanır.

[6] AuthorithyInformationAccess
[7] CertificatePolicies
[8] QcStatement
[9] StatementInfo
[10] StatementId

Sertifika sahiplerine ait anahtar çiftleri RSA algoritması anahtar çiftleridir.

Kullanılan algoritmaların nesne tanımlama numaraları X.509 sertifikaları içinde belirtilir.

### 7.1.4. İsim Alanı Biçimleri

Kamu SM tarafından üretilen nitelikli elektronik sertifikalardaki isim alanı "ITU X.500 Distinguished Name [Ayırt edici isim]" biçimine uygundur.

### 7.1.5. İsim Kısıtları

Üretilen nitelikli elektronik sertifikalardaki isim bilgileri kişiyi tekil olarak tanımlamayı sağlayacak niteliktedir ve resmi kimlik belgelerinde geçen ad ve soyad bilgisinden oluşur.

Kamu SM tarafından farklı kişiler için üretilen nitelikli elektronik sertifikaların isim alanları aynı olamaz. İsim alanlarının benzersizliğinin sağlanması için T.C. Kimlik Numarası DN alanı içinde yer alır. Yabancı uyruklu nitelikli elektronik sertifika sahiplerinin isim alanlarının benzersizliğinin sağlanması için, pasaport numarası DN alanı içinde yer alır.

Aşağıdaki tabloda nitelikli elektronik sertifika içinde yer alan isim alanları ve bu alanlar içine yazılacak bilgiler belirtilmiştir.

| Alan Adı | Nitelikli Elektronik Sertifika İçeriği |
|---|---|
| **CN**[11] | Sertifika sahibinin adı soyadı |
| **Serial**[12] | T.C. kimlik numarası / Pasaport numarası |
| **C**[13] | TR |

### 7.1.6. Sertifika İlkeleri Nesne Tanımlama Numarası

Bağlı olunan Kamu SM Sİ dokümanına ait nesne tanımlama numarası:

2.16.792.1.2.1.1.5.7.1.1

Kamu SM (Nitelikli Elektronik Sertifika) Sertifika İlkeleri { joint-iso-itu-t(2) ülke(16) tr(792) TÜBİTAK(1.2.1.1) UEKAE(5) Kamu SM(7) Kamu SM-sertifika-ilkeleri(1) Kamu SM-nes-ilke-1 (1) }

### 7.1.7. İlke Kısıtları Uzantısının Kullanımı

Düzenlenmesine gerek duyulmamıştır.

### 7.1.8. İlke Niteleyiciler

"Sertifika İlkeleri Uzantısı" nitelikli elektronik sertifikaların üretim ve yönetim işlemlerinde uyulan ilke ve esasların Kamu SM Sİ ve Kamu SM SUE olduğuna işaret eder. Nitelikli elektronik sertifikaların üretim ve yönetiminde takip edilen kurallara işaret eden Sİ dokümanına ait nesne tanımlama numarası [Certificate Policy Object Identifier(s)] Kamu SM tarafından üretilen nitelikli elektronik sertifikanın "Sertifika İlkeleri Uzantısı[14]"nın içinde yer

[11] CN: Common Name [Genel isim]
[12] Serial: Serial Number [Seri Numarası]
[13] C: Country [Ülke]
[14] Certificate Policies

alır. "Sertifika İlkeleri Uzantısı"nın içinde "İlke Niteleyici[15]" olarak belirtilen alana Kamu SM SUE dokümanının bulunduğu internet adresi yazılır.

Üçüncü kişiler "Sertifika İlkeleri Uzantısı"nı kontrol ettiğinde Sİ ve SUE'de belirtilen ilke ve uygulama esasları çerçevesinde nitelikli elektronik sertifikaları kullanarak işlem yapar.

Kamu SM tarafından kişilere verilen elektronik sertifikaların nitelikli olduğunu belirten ibare "Sertifika İlkeleri Uzantısı" içindeki "Kullanıcı Bildirim Alanı[16]"nda tanımlanır. Kamu SM tarafından tanımlanan nitelikli elektronik sertifika ibaresi Kamu SM Sİ dokümanında verilmiştir.

#### 7.1.9. Kritik Belirtilmiş Olan İlke Belirleyici Uzantılarının İşlenmesi

Düzenlenmesine gerek duyulmamıştır.

### 7.2. Sertifika İptal Listesi Biçimi

#### 7.2.1. Sürüm Numarası

Kamu SM'nin ürettiği SİL'ler "ITU X.509 V.2" SİL formatına uygundur.

#### 7.2.2. Sertifika İptal Listesi Uzantıları

Üretilen SİL'ler "ITU X.509" SİL formatına uygun olarak aşağıdaki bilgileri içerir:

- SİL'i oluşturan Kamu SM'ye ait isim bilgileri
- SİL imzalamak için kullanılan algoritmalara ait nesne tanımlama numarası (Kamu SM yayımladığı SİL'i imzalamak için SHA-1 özet algoritması ile RSA açık anahtarlı imzalama algoritmasını kullanır.)
- SİL'in yayımlanma tarihi
- SİL numarası
- Bir sonraki SİL yayımlanma tarihi
- İptal edilen nitelikli elektronik sertifikalarla ilgili aşağıdaki bilgiler:
    - Sertifikanın seri numarası
    - Sertifikanın iptal tarihi
    - Sertifikanın neden iptal edildiği bilgisi
- Kamu SM tarafından oluşturulan elektronik imza
- SİL imzasını doğrulamak için kullanılan Kamu SM'ye ait sertifikanın "ESHS Anahtar Tanımlayıcı" numarası

### 7.3. Çevrim İçi Sertifika Durum Protokolü Biçimi

#### 7.3.1. Sürüm Numarası

Çevrim İçi Sertifika Durum Protokolü RFC 2560 V.1'i destekler.

#### 7.3.2. ÇİSDUP Uzantıları

ÇİSDUP sorguları aşağıdaki bilgileri içermelidir.

- Protokol versiyonu

[15] Policy Identifier
[16] User Notice

- Hedef sertifika belirteci (kullanılan özetleme algoritması, sertifikayı veren ESHS'nin DN özeti, sertifikayı veren ESHS'nin imza doğrulama verisi özeti, sertifika seri numarası,)

ÇİSDUP cevapları aşağıdaki bilgileri içermektedir.

- Versiyon bilgisi
- Cevaplayıcının adı
- Her bir sertifika için cevap bilgisi (sertifika belirteci (sertifika seri numarası), sertifika durumu, cevap geçerlilik süresi)
- Kullanılan İmza algoritması nın OID si.
- ÇİSDUP yanıtlayıcı imzası

Bütün geçerli ÇİSDUP cevapları ÇİSDUP yanıtlayıcı tarafından imzalanır. Geçersiz ÇİSDUP sorguları için dönen hata mesajları imzalanmaz.

Çevrim İçi Sertifika Durum Protokolü RFC 2560'da tarif edilen "ÇİSDUP" formatını destekler. ÇİSDUP Yanıtlayıcı'dan alınan cevaplar aşağıdaki şekilde değerlendirilir:

*Good [iyi]:* Sertifika geçerli konumdadır.

*Bad [kötü]:* Sertifika askıdadır, iptal edilmiştir ya da henüz kullanıma açılmamıştır.

*Unknown [bilinmiyor]:* Sorgusu yapılan sertifika hakkında herhangi bir bilgi bulunmamaktadır.

RFC 2560'da belirtilen uzantılar ÇİSDUP cevap formatında kullanılmamaktadır.

## 8. Uygunluk Denetimleri

Kamu SM, mevzuat gereği Bilgi Teknolojileri Kurumu tarafından incelenir/denetlenir.

Kamu SM, ek olarak ISO/IEC 27001 bilgi güvenliği yönetim standardına uygun olarak hizmet verir ve standart gereği düzenli olarak iç ve dış denetimlere tabi tutulur.

Kamu SM iç işleyişini denetlemek için, ayrıca iç denetimler gerçekleştirilir.

### 8.1. Uygunluk Denetiminin Sıklığı

Kamu SM iki yılda en az bir defa Kurum tarafından denetlenir.

Kamu SM, ISO/IEC 27001 bilgi güvenliği yönetim sistemi standardı gereğince yılda bir defa uygunluk denetimi geçirir. Her üç yılda bir sertifika yenilenir.

İç denetim, iki yılda bir defa olmak üzere gerçekleştirilir. Gerekli hallerde denetim sayısı arttırılabilir.

### 8.2. Denetçinin Nitelikleri

Kamu SM faaliyetlerinin denetimi, kanunla yetkilendirilmiş olan Kurum tarafından gerçekleştilir.

ISO/IEC 27001 BGYS'nin denetimi bağımsız ve akredite edilmiş kuruluşlarca gerçekleştirilir.

İç denetim, Kamu SM SUE'sine hakim, sertifika süreçlerini bilen ve denetim konusunda tecrübeli Kamu SM personeli tarafından gerçekleştirilir.

### 8.3. Denetçinin Denetlenen Tarafla Olan İlişkisi

Kurum, kanun gereği tüm ESHS'leri denetlemekle yetkili kılınmış düzenleyici kurumdur.

Kamu SM'nin ISO/IEC 27001 BGYS denetimi, bağımsız ve akredite edilmiş kuruluşlarca gerçekleştirilir.

İç denetim, Kamu SM SUE'sine hakim, sertifika süreçlerini bilen ve denetim konusunda tecrübeli Kamu SM personeli tarafından gerçekleştirilir.

### 8.4. Denetimin Kapsamı

Kamu SM'nin denetim kapsamı Kurum tarafından belirlenir.

BGYS standardına uygun denetim kapsamı bağımsız kurum denetçisi tarafından belirlenir.

İç denetim kapsamı denetimi gerçekleştirecek Kamu SM personeli tarafından belirlenir.

### 8.5. Yetersizliğin Tespiti Durumunda Yapılacaklar

Kurum tarafından gerçekleştirilen denetimlerde ortaya çıkan eksiklikler, Kamu SM tarafından planlı çalışma ile giderililir. Eksiklikler Kamu SM'nin işleyişini etkileyecek kadar büyük ise, ilgili mevzuata göre yaptırım ve cezalar uygulanır.

ISO/IEC 27001 standardına göre gerçekleştirilen denetimlerde ortaya çıkan eksiklikler, Kamu SM tarafından planlı çalışma ile giderilir. Eksiklikler, BGYS'sinin temel işleyişini

etkileyecek kadar büyük ise, Kamu SM, ISO/IEC 27001 uygunluk belgesi eksikler giderilinceye kadar askıya alınır.

İç denetimlerde ortaya çıkan eksiklikler, Kamu SM ilgili personeli tarafından giderilir. Tüm denetimlerden elde edilen bulgular Düzeltici Önleyici Faaliyetler açılarak takip edilir.

### 8.6. Sonucun Bildirilmesi

Denetim sonucu, Kurum ve ISO/IEC 27001 denetçilerinin hazırladığı resmi raporlar ile Kamu SM'ye bildirilir.

İç denetim sonuçu, Kamu SM üst yönetimine raporlanır.

## 9. Diğer İşler ve Hukuksal Meseleler

### 9.1. Ücretlendirme

#### 9.1.1. Sertifika Oluşturma ve Yenileme Ücreti

Kamu SM tarafından üretilen, yenilenen ve güncellenen nitelikli elektronik sertifikalar için kurumlardan veya sertifika sahiplerinden ücret alınır. Ücretin miktarı ve ödeme şekli Kamu SM tarafından gönderilen teklif mektuplarında veya kurumlarla yapılan sözleşmelerde bildirilir.

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

#### 9.1.2. Sertifika Erişim Ücreti

Kamu SM, kendisine ve sertifika sahiplerine ait nitelikli elektronik sertifikaları ücretsiz olarak yayımlar.

#### 9.1.3. İptal Durum Kaydına Erişim Ücreti

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

#### 9.1.4. Diğer Servis Ücretleri

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

Kamu SM imza oluşturma verisinin saklandığı güvenli elektronik imza oluşturma aracı teminini kendi imkanlarıyla sertifika sahibine sağlayabilir. Nitelikli elektronik sertifikalar ve güvenli donanım araçları için ödenecek bedelin miktarı ile ilgili bilgilendirme Kamu SM tarafından gönderilen teklif mektuplarında veya kurumlarla yapılan sözleşmelerde yapılır. Ödemenin usulüne uygun biçimde yapılmaması durumunda nitelikli elektronik sertifika üretimi yapılmaz.

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

#### 9.1.5. İade Ücreti

Sertrifika sahibi nitelikli elektronik sertifikasını ilk teslim aldığında yaptığı kontrol neticesinde, sertifikasını kullanamadığını tespit ederse ve sorunun Kamu SM'den kaynaklanan bir hata sebebiyle ortaya çıktığı anlaşılırsa, talebi halinde sertifika sahibinin nitelikli elektronik sertifika için ödenen ücreti iade edilir. Güvenli elektronik imza oluşturma aracı erişim verisinin kaybolması, unutulması, aracın yanlış erişim verisi girilmesi dolayısıyla kilitlenmesi, sertifika sahibinin yanlış kullanımından dolayı aracın kullanılamaz duruma gelmesi, sertifikanın iptali ve benzeri durumlarda ücret iadesi yapılmaz..

### 9.2. Finansal Sorumluluk

#### 9.2.1. Sigorta Kapsamı

Kamu SM, Bölüm 9.2.3'de belirtilen sertifika sahibi mali sorumluluk sigortası dışında, kendi sorumluluklarını karşılamak amacıyla sigortalanmamıştır.

#### 9.2.2. Diğer Varlıklar

Düzenlenmesine gerek duyulmamıştır.

#### 9.2.3. Sertifika Mali Sorumluluk Sigortası

Kamu SM, yükümlülüklerini yerine getirmemesi sonucu doğan zararların karşılanması amacıyla, dağıttığı nitelikli elektronik sertifikaları 15 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza Kanunu gereğince mali sorumluluk sigortası ile sigortalar.

### 9.3. Ticari Bilginin Korunması

#### 9.3.1. Gizli Bilginin Kapsamı

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

#### 9.3.2. Gizlilik Kapsamında Olmayan Bilgiler

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

#### 9.3.3. Gizli Bilginin Korunma Sorumluluğu

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

### 9.4. Kişisel Bilginin Gizliliği

#### 9.4.1. Gizlilik Planı

Düzenlenmesine gerek duyulmamıştır.

#### 9.4.2. Gizli Olarak Tanımlanan Bilgiler

Kişisel bilgi, sertifika sahibinin, başvuru sırasında kimlik tanımlama ve doğrulama ile sertifika yönetim prosedürleri içinde kullanılmak üzere Kamu SM'ye beyan ettiği doğum tarihi, doğum yeri gibi nüfus bilgileri ile adres ve telefon numarası gibi erişim bilgilerini kapsar. Kamu SM veya sertifika sahibi tarafından atanan parolalar, numara, sembol gibi diğer tanımlayıcıyı bilgiler de kişisel bilgi kapsamına girer.

#### 9.4.3. Gizli Olarak Tanımlanmayan Bilgiler

Nitelikli elektronik sertifikanın içeriğinde bulunan bilgiler aksi taraflar arası sözleşmelerde belirtilmediği sürece gizli değildir.

#### 9.4.4. Gizli Bilginin Korunma Sorumluluğu

Kamu SM sertifika talep eden kişiden, elektronik sertifika vermek için gerekli bilgiler hariç bilgi talep etmez. Kamu SM elde ettiği kişisel 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 kişisel bilgilerine erişirler.

#### 9.4.5. Gizli Bilginin Kullanımına İzin Verilmesi

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

#### 9.4.6. Yetkili Merciilerin Kararına Uygun Olarak Bilginin Açıklanması

Kamu SM sertifika sahiplerine ait gizli kişisel bilgiler, mahkeme kararı olması durumunda açıklanabilir.

#### 9.4.7. Diğer Başlıklar

Düzenlenmesine gerek duyulmamıştır.

### 9.5. Telif Hakları

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

### 9.6. Temsil Hakkı ve Yükümlülükler

Kamu SM verdiği sertifika hizmetlerinde sistem bileşenleri olan Kamu SM, sertifika sahipleri ve üçüncü kişiler 15 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza Kanunu, 2004/21 sayılı Başbakanlık Genelgesi, Telekomünikasyon Kurumu'nun yayımladığı Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik, Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de belirtilen şekilde üzerlerine düşen yükümlülükleri sağlarlar.

Kamu SM, sertifika sahipleri, sertifika sahiplerinin bağlı bulunduğu kamu kurum veya kuruluşları ile üçüncü kişiler yasa ve yönetmeliklerde belirtilmediği halde, Nitelikli Elektronik Sertifika Sahibi Taahhütnamesi, Kamu SM Taahhütnamesi ve NES Temini Sözleşmesi'nde sözü geçen yükümlülükleri yerine getirirler.

Kamu SM'nin ESHS olarak işleyişinin güvenli olabilmesi için, sistem bileşenlerinin yerine getirmesi gereken yükümlülükler aşağıda belirtilmiştir.

#### 9.6.1. Elektronik Sertifika Hizmet Sağlayıcısı Yükümlülükleri

ESHS olarak Kamu SM'nin yükümlülükleri şunlardır:

- Hizmetin gerektirdiği nitelikte personel istihdam etmek,
- Belirlediği ilke ve esaslara uygun olarak sertifika işlemlerini yürütmek,
- Sİ ve SUE dokümanlarını herkesin erişimine açık bilgi deposundan yayımlamak,
- Kök SHS ve Kamu ESHS için anahtar çifti üretmek ve bu anahtar çiftleri için sertifikalar oluşturmak,
- Kök SHS ve Kamu ESHS sertifikalarını son kullanıcıların erişebileceği ortamlarda yayımlamak,

- Nitelikli elektronik sertifika verdiği kişilerin kimliğini resmi belgelere göre güvenilir bir biçimde tespit etmek,
- Kurumlardan gelen nitelikli elektronik sertifika başvurularını usulüne uygun biçimde kabul etmek ve başvuruda bulunan kişilerin belgeleri ile başvuru formlarını gerekli kontrollerden geçirmek,
- Nitelikli elektronik sertifikanın içeriğindeki bilgilerin doğruluğunu beyan edilen belgelere dayanarak sağlamak,
- Gerekli başvuru şartlarını sağlamayan başvuru sahiplerine nitelikli elektronik sertifika vermemek,
- Nitelikli elektronik sertifika başvurularını değerlendirerek, başvurunun sonucu hakkında ilgili kişileri bilgilendirmek,
- Nitelikli elektronik sertifika başvurusu kabul edilmiş kişiler için anahtar çifti ve nitelikli elektronik sertifika üretmek,
- Sertifika sahibine ait imza oluşturma verisini oluşturduktan sonra imza oluşturma verisini ve üretiminde kullanılan gizli değişkenleri kendi sisteminden silmek, imza oluşturma verisinin kopyasını hiçbir şekilde tutmamak,
- Sertifika sahibine imza oluşturma aracı temin etmesi durumunda, bu aracın güvenli elektronik imza oluşturma aracı olmasını sağlamak,
- Üretilen nitelikli elektronik sertifikalar ile imza oluşturma verilerini Sİ ve SUE'de belirtilen şekilde güvenli olarak sertifika sahiplerine teslim etmek,
- Sertifika sahiplerinin nitelikli elektronik sertifikalarını aksi taraflar arası sözleşmelerde belirtilmedikçe son kullanıcıların erişebileceği ortamlarda yayımlamak,
- Nitelikli elektronik sertifikaların kullanım şartlarını belirleyen sertifika profillerini oluşturmak,
- Nitelikli elektronik sertifika başvurularını Sİ ve SUE'de belirtilen şekilde kabul etmek ve değerlendirerek gerekli işlemlerini yapmak,
- Nitelikli elektronik sertifika askıya alma başvurularını Sİ ve SUE'de belirtilen şekilde kabul etmek ve değerlendirerek gerekli askıya alma işlemlerini yapmak,
- Nitelikli elektronik sertifika askıdan çıkarma işlemlerini Sİ ve SUE'de belirtilen şekilde yapmak,
- Nitelikli elektronik sertifika iptal başvurularını Sİ ve SUE'de belirtilen şekilde kabul etmek ve değerlendirerek gerekli iptal işlemlerini zamanında yapmak,
- Yayımlanan Sİ ve SUE dokümanları ile Nitelikli Elektronik Sertifika Sahibi Taahhütnamesi'ne uygun olmayan nitelikli elektronik sertifika kullanımlarının tespit edilmesi durumunda ilgili nitelikli elektronik sertifikayı iptal etmek,
- İptal edilmiş nitelikli elektronik sertifika bilgilerini sertifika iptal listelerinde yayımlamak veya ÇİSDUP Yanıtlayıcı aracılığıyla duyurmak,
- Nitelikli elektronik sertifikaların ve iptal durum kayıtlarının bütünlüğünü ve erişilebilirliğini sağlamak için her türlü tedbiri almak,

- Sertifika sahiplerine ait elektronik veya kağıt ortamda tutulan bilgilerin gizliliğinin korunması için gerekli önlemleri almak, bu bilgileri üçüncü kişilere mahkeme kararı olmaksızın vermemek,
- Nitelikli elektronik sertifika üretim, yönetim ve iptali ile ilgili yapılan tüm işlemlerin kaydını tutmak,
- İşleyiş sırasında kullanılan tüm kağıt ve elektronik kayıtları ilgili Sİ ve SUE'de belirtilen süreler boyunca güvenli olarak saklamak,
- Kök SHS sertifikasının özet değerini Kamu SM'ye ait internet ortamından yayımlamak, ulusal yayın yapan en yüksek trajlı 3 (üç) gazetede ilan vermek suretiyle kamuoyuna duyurmak ve gazete ilanlarının bir örneğini Telekomünikasyon Kurumu'na iletmek.

### 9.6.2. Kayıt Birimi Yükümlülükleri

Düzenlenmesine gerek duyulmamıştır.

### 9.6.3. Sertifika Sahibinin Yükümlülükleri

Sertifika sahibinin yükümlülükleri şunlardır:

- Nitelikli elektronik sertifika başvuru, askıya alma, iptal ve diğer işlemleri ilgili Sİ ve SUE'de belirtildiği şekilde, detayları Kamu SM nitelikli elektronik sertifika yönetim prosedürlerinde anlatılan usule uygun biçimde yerine getirmek,
- Nitelikli elektronik sertifika başvurusu, yenileme ve iptal işlemleri sırasında doğru bilgi beyan etmek,
- Adına düzenlenen, imza oluşturma verisini içeren güvenli elektronik imza oluşturma aracı ve kapalı parola zarfını şahsen teslim almak,
- Adına düzenlenen nitelikli elektronik sertifika yayımlandığında nitelikli elektronik sertifikadaki bilgilerin doğruluğunu kontrol etmek,
- SUE Bölüm 6.2.1'de belirtilen standartlara uygun güvenli elektronik imza oluşturma aracı kullanmak,
- İmza oluşturma verisinin güvenliğini sağlamak, kendisine ait imza oluşturma verisinin içinde bulunduğu güvenli elektronik imza oluşturma aracının ve imza oluşturma verisi erişim verisinin gizliliğini korumak, bunları başkasına kullandırmamak ve bu konuda gerekli tedbirleri almak,
- İnternet veya çağrı merkezi üzerinden sertifika işlemlerini yapabilmesi için kullandığı parolalarının gizliliğini ve güvenliğini sağlamak,
- İmza oluşturma verisinin içinde bulunduğu güvenli elektronik imza oluşturma aracının kaybolması, çalınması veya imza oluşturma verisinin gizliliğinin yitirildiğinden şüphelenmesi durumunda nitelikli elektronik sertifikanın iptal edilmesi için Kamu SM'ye en kısa zamanda başvurmak,
- Güvenli elektronik imza oluşturma aracı erişim verisini ve sertifika işlemlerinde kullandığı diğer parolaları her ay düzenli olarak değiştirmek,
- Nitelikli elektronik sertifikanın içeriğinde bulunan bilgilerin değişmesi durumunda derhal sertifikanın iptal edilmesi için Kamu SM'ye başvurmak,

- Nitelikli elektronik sertifika başvurusu sırasında ve sertifikanın geçerlilik süresi boyunca beyan ettiği bilgilerde meydana gelen değişiklikleri derhal Kamu SM'ye bildirmek,
- İptal olmuş, kullanıma açılmamış, askıya alınmış veya geçerlilik süresi dolmuş nitelikli elektronik sertifika ile işlem yapmamak,
- İmza oluşturma verisini SHS sertifikası imzalamak amacıyla kullanmamak,
- Kendisine verilen nitelikli elektronik sertifikayı Sİ ve SUE dokümanlarında belirtildiği biçimde, Nitelikli Elektronik Sertifika Sözleşmesi'nde, Nitelikli Elektronik Sertifika Sahibi Taahhütnamesi'nde belirtilen şartlar dahilinde kullanmak.
- İmza oluşturma verisini, nitelikli elektronik sertifika içerisinde belirtilen maddi sınırları aşan finansal işlemlerde kullanmamak.

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

### 9.6.4. Üçüncü Kişilerin Yükümlülükleri

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

- Nitelikli elektronik sertifikaların, tanımlanan veriliş amacına uygun olarak kullanıldığını doğrulamak,
- Nitelikli elektronik sertifikanın kullanım süresinin dolup dolmadığını kontrol etmek,
- Nitelikli elektronik sertifikanın geçerliliğini SİL veya ÇİSDUP Yanıtlayıcı aracılığıyla kontrol etmek,
- SİL veya ÇİSDUP Yanıtlayıcı'dan aldığı iptal durum kaydının bütünlüğünü Kamu SM'nin ilgili nitelikli elektronik sertifikalarının içinde mevcut olan imza doğrulama verilerini kullanarak doğrulamak,
- Nitelikli elektronik sertifikanın doğruluğunu Kamu ESHS sertifikasının içinde mevcut olan imza doğrulama verisini kullanarak doğrulamak,
- Kamu ESHS sertifikasının doğruluğunu Kök SHS sertifikasının içinde mevcut olan imza doğrulama verisini kullanarak doğrulamak,
- Kök SHS sertifikasının doğruluğunu sertifika özet değerini kontrol etmek suretiyle doğrulamak,
- Sertifika sahibinin nitelikli elektronik sertifikasının içindeki imza doğrulama verisine karşılık gelen imza oluşturma verisine sahip olduğunu doğrulamak.
- Finansal işlemlerde sertifika içerisinde bulunan maddi sınır bilgisini kontrol etmek.

### 9.6.5. Diğer Bileşenlerin Yükümlülükleri

Düzenlenmesine gerek duyulmamıştır.

## 9.7. Yükümlülüklerden Feragat

Kamu SM ile sertifika sahipleri veya sertifika sahiplerinin bağlı bulunduğu kamu kurum veya kuruluşları arasındaki yükümlülük, Nitelikli Elektronik Sertifika Sözleşmesi, Nitelikli

Elektronik Sertifika Sahibi Taahhütnamesi, Kamu SM Taahhütnamesi ve kurumla imzalanan NES Temini Sözleşmesi'nde belirtildiği şekilde sona erer.

### 9.8. Sorumlulukla İlgili Sınırlamalar

Kamu SM ve sertifika hizmeti alan tarafların sorumlulukları 15 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza Kanunu, 2004/21 sayılı Başbakanlık Genelgesi, Telekomünikasyon Kurumu'nun yayımladığı Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik, Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de belirtilen şartlar ile sınırlıdır.

Kamu SM ve sertifika hizmetlerini alan tarafların sorumlulukları ilgili sınırlamalar Nitelikli Elektronik Sertifika Sözleşmesi, Nitelikli Elektronik Sertifika Sahibi Taahhütnamesi ve kurumla imzalanan NES Temini Sözleşmesi'nde de belirlenebilir. Ayrıca sertifika mali sorumluluk sigortası genel şartları ile diğer düzenlemeler dikkate alınır.

### 9.9. Tazminat Halleri

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

### 9.10. Anlaşma Süresi ve Anlaşmanın Sona Ermesi

Sertifika sahipleri Nitelikli Elektronik Sertifika Sözleşmesi, Nitelikli Elektronik Sertifika Sahibi Taahhütnamesi'ne uygun olarak Kamu SM ile işbirliği içinde çalışır. Kamu SM'den nitelikli elektronik sertifika hizmeti alan kamu kurumları NES Temini Sözleşmesi'ne uygun olarak Kamu SM ile işbirliği içinde çalışır.

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

Kamu SM sertifika hizmeti verdiği süre boyunca Sİ, SUE dokümanları, sertifika yönetim prosedürleri, sertifika sahibine ilettiği Kamu SM Taahhütnamesi ve kurum ile imzaladığı NES Temini Sözleşmesi'ndeki şartları yerine getirir.

#### 9.10.1. Anlaşma Süresi

Sertifika sahibinin imzaladığı Nitelikli Elektronik Sertifika Sözleşmesi veya Nitelikli Elektronik Sertifika Sahibi Taahhütnamesi'nin süresi nitelikli elektronik sertifikanın geçerlilik süresi kadardır. Ancak, sertifikanın iptal edilmesi durumunda Nitelikli Elektronik Sertifika Sözleşmesi veya taahhütnamenin süresi de sona erer. Aynı şekilde Kamu SM Taahhütnamesi de sertifika sahibinin nitelikli elektronik sertifikasının geçerlilik süresince geçerlidir.

Kurumla imzalanan NES Temini Sözleşmesi'nin geçerlilik süresi sözleşme içerisinde belirtilir.

#### 9.10.2. Anlaşmanın Sona Ermesi

Kamu SM ile kurum arasında imzalanan NES Temini Sözleşmesi aşağıdaki durumlarda sonlandırılabilir:

- Taraflardan birisinin sözleşmeye uygun olarak, sözleşmenin sonlandırılması için talepte bulunması
- Sözleşmenin süresinin sona ermesi

- Her iki tarafın da ortak karar alarak sözleşmeyi bitirmesi
- Taraflardan birisinin sözleşmeye aykırı davranması: Taraflardan biri sözleşme kapsamında üzerine düşen yükümlülükleri yerine getirmez ise diğer taraf sözleşmeye aykırı davranan tarafa bu yükümlülüğü yerine getirmesi için 5 (beş) günlük süre verir. Bu sürenin sonunda da sözleşmeye aykırılık ortadan kaldırılamaz veya doğacak zarar, ziyan talepleri saklı kalmak kaydıyla yükümlülük yerine getirilmez ise sözleşme tek taraflı olarak fesh edilebilir.
- Bölüm 5.7.3'te belirtilen güvenlik açığının ortaya çıkması sebebiyle Kamu SM sertifika sahiplerine ait nitelikli elektronik sertifikaları iptal ederek NES Temini Sözleşmesini sonlandırabilir.
- Kamu SM Bölüm 5.8'de belirtildiği biçimde sertifika hizmetlerini sonlandırırsa, sertifika sahiplerine ait nitelikli elektronik sertifikaları iptal ederek NES Temini Sözleşmesini sonlandırabilir.

Kamu SM Taahhütnamesi ve Nitelikli Elektronik Sertifika Sahibi Taahhütnamesi veya Nitelikli Elektronik Sertifika Sözleşmesi aşağıdaki durumlarda sonlandırılabilir:

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

### 9.10.3. Anlaşmanın Sona Ermesinin Etkileri

NES Temini Sözleşmesi'nin sona ermesiyle hizmeti alan kurumun, sözleşme ile Sİ ve SUE dokümanlarında belirtilen şartları sağlamakla ilgili yükümlülükleri ortadan kalkar. Kamu SM kurumdan sertifika başvurularını almayı durdurur. Ancak daha önceden yapılmış başvurular ile ilgili işlemler, anlaşmanın sona erme sebebine bağlı olarak kurumun talep etmesi durumunda devam eder.

Nitelikli Elektronik Sertifika Sözleşmesi veya Nitelikli Elektronik Sertifika Sahibi Taahhütnamesi'nin sona ermesiyle sertifika sahibinin, taahhütname ile Sİ ve SUE dokümanlarında belirtilen şartları sağlamakla ilgili yükümlülükleri ortadan kalkar. Nitelikli Elektronik Sertifika Sözleşmesi veya Nitelikli Elektronik Sertifika Sahibi Taahhütnamesi'nin sona erme sebebi, sertifika sahibinin taahhütnameden, Sİ veya SUE dokümanlarından kaynaklanan yükümlülüklerini yerine getirmemesinden dolayı, Kamu SM'nin sertifikayı iptal etmesi ise, bu durumda sertifika sahibinin 6 (altı) ay içinde yapacağı ikinci bir nitelikli elektronik sertifika talebi kabul edilmeyecektir. Sertifika sahibinin taahhütnameye uygun hareket etmemesinden dolayı uğrayacağı zararlardan Kamu SM sorumlu tutulamaz.

Sözleşme ve taahhütnameler sona erse bile Kamu SM, dağıttığı nitelikli elektronik sertifikalarla ilgili, elektronik imza mevzuatında belirtilen yükümlülüklerini yerine getirmeye devam eder. Kamu SM, dağıttığı nitelikli elektronik sertifikalara, iptal durum kayıtlarına

taraflarca erişimin sağlanması, Bölüm 5.4 ve 5.5'de belirtilen kayıtların ve arşivlerin saklanması ile ilgili hizmetleri sürdürür.

### 9.11. Sistem Bileşenleri İle Haberleşme ve Kişisel Bilgilendirme

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

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

Sertifika yönetim işlemleri sırasında sertifika sahibi veya kurumlarla yapılan haberleşmenin hangi durumlarda, ne şekilde yapılacağı Kamu SM'nin nitelikli elektronik sertifika yönetim prosedürlerinde detaylı olarak belirtilir.

### 9.12. Değişiklik Halleri

#### 9.12.1. Değişiklik Metodları

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

#### 9.12.2. Bilgilendirme Mekanizması ve Sıklığı

SUE dokümanında yapılan değişiklikler dokümanın yenilenerek Kamu SM bilgi deposu üzerinden erişime açılması ile duyurulur. Yenilenen doküman en fazla 1 (bir) hafta sonra bilgi deposundan yayımlanır ve yayımlandığı tarihte yürürlüğe girer. SUE'de yapılan değişiklikler 7 (yedi) gün içinde Telekomünikasyon Kurumu'na bildirilir.

#### 9.12.3. Nesne Tanımlama Numarasının Değişmesini Gerektiren Durumlar

Düzenlenmesine gerek duyulmamıştır.

### 9.13. Anlaşmazlık Halleri

Taraflar arasında çıkan tüm anlaşmazlıkların sulhen çözümü esastır. İhtilafların çözümünde 5070 sayılı Elektronik İmza Kanunu, Telekomünikasyon Kurumu'nun yayımladığı Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik, Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ, karşılıklı imzalanan sözleşmeler, taahhütnameler, Kamu SM Sertifika İlkeleri ve Kamu SM Sertifika Uygulama Esasları dokümanlarına başvurulur. İhtilafların sulhen çözümünün mümkün olmaması halinde, ihtilafların çözümünde görevli ve yetkili mahkeme Türkiye Cumhuriyeti Gebze Mahkemeleridir.

### 9.14. Uygulanacak Hukuk

SUE dokümanındaki hükümler 15 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza Kanunu'na uygun olarak yazılmıştır.

### 9.15. Uygulanabilir Yasalarla Uyum

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

### 9.16. Diğer Hükümler

Düzenlenmesine gerek duyulmamıştır.