TASNİF DIŞI

TÜBİTAK BİLGEM
KAMU SERTİFİKASYON MERKEZİ

KURUMSAL ŞİFRELEME SERTİFİKA UYGULAMA ESASLARI

Doküman Kodu
YON.05.02

Revizyon No
01

Revizyon Tarihi
18.01.2021

TASNİF DIŞI

REVİZYON GEÇMİŞİ		
Revizyon No	**Revizyon Nedeni**	**Revizyon Tarihi**
00	İlk Çıkış.	15.01.2021
01	Doküman formatı güncellenmiştir.	18.01.2021

İÇİNDEKİLER

TABLOLAR

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) Türkiye Cumhuriyeti Devleti'ne bağlı kamu kurum ve kuruluşlara Kurumsal Şifreleme Sertifikası sağlayıcılığı konusundaki faaliyetlerini nasıl yürüttüğünü anlatmak amacıyla yazmış olduğu 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. 2017/21 sayılı Başbakanlık Genelgesi ile Kurumsal Şifreleme Sertifikalarının üretilmesi için TÜBİTAK bünyesindeki Kamu Sertifikasyon Merkezi (Kamu SM) yetkilendirilmiştir. Kamu SM; 2019/DK-BTD/160 Sayılı Bilgi Teknolojileri ve İletişim Kurulu Kararı ile yayımlanan Kurumsal Şifreleme ve Elektronik Mühür Sertifikalarına İlişkin Usul ve Esaslar'da belirtilen tanıma uygun olarak Kurumsal Şifreleme Sertifikası hizmeti sağlamaktadır.

Kamu SM, Sertifika İlkeleri (Sİ) dokümanında belirtilen ilkelere uygun olarak hazırlanan bu SUE dokümanında tanımlanan esaslar uyarınca çalışır. SUE dokümanı, Kurumsal Şifreleme Sertifikalarının yönetimi ve kayıt işlemleri sırasında yapılan işlerin hangi ortamlarda ve nasıl yürütüldüğünü Sİ dokümanına bağlı olarak detaylandırarak anlatır. Bu SUE dokümanı, sertifika başvurularının alınması, sertifika üretimi ve yönetimi, sertifika yenileme ve sertifika iptal işlemleriyle ilgili hizmetlerin, idari, teknik ve yasal gerekliliklere uygun olarak yürütülmesiyle ilgili esasları ortaya koyar; Kamu SM'nin, sertifika sahibinin ve üçüncü kişilerin uygulama sorumluluklarını belirler.

Kamu SM'den Kurumsal Şifreleme Sertifikası talebinde bulunan tüzel kişiler bu dokümanda belirtilen esaslar çerçevesinde sertifikayı kullanmayı kabul etmiş sayılır. Kurumsal Şifreleme Sertifikası talebinde bulunan kurumlar bununla ilgili olarak Kamu SM ile imzaladıkları sözleşme veya başvuru formu ve taahhütnamelerde SUE dokümanına atıfta bulunurlar. Kurumsal Şifreleme Sertifikası sahibi kurumlar ilgili sözleşme veya başvuru formu ve taahhütnamesini imzalayarak SUE dokümanında belirtilen esasları kabul ederler.

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, askıdan indirmek, 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 kurumların başvurularını, kurum bilgileri ve ilgili resmi belgeleri toplama, kurum kimliği doğrulama, onaylama, iptal, yenileme isteklerini alma, değerlendirme, onaylanan sertifika başvuru ve iptal istekleri doğrultusunda gerekli işlemleri başlatmayı içerir.

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

Doküman Sürüm Numarası: 01

Yayın Tarihi: 18.01.2021

Nesne Tanımlama Numarası: 2.16.792.1.2.1.1.5.7.1.11

Bu doküman, Kamu SM'nin Kurumsal Şifreleme Sertifikası hizmeti verirken uyguladığı esasları tanımlayan SUE dokümanıdır ve kamu kurum ve kuruluşlarına verilen Kurumsal Şifreleme Sertifikalarını kapsar. SUE dokümanı http://depo.kamusm.gov.tr/ilke/ adresinde kamuya açık olarak kesintisiz yayımlanmaktadır.

1.3. Sistem Bileşenleri

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

1.3.1. Elektronik Sertifika Hizmet Sağlayıcısı

Temel görevi sertifika ve iptal durum kayıtlarını üretip kendisine ait imza oluşturma verisiyle imzalamak olan ESHS'ler, sertifika başvurusunda bulunan kurumların kayıt ve kimlik doğrulama işlemleri ile Kurumsal Şifreleme Sertifikası üretim, dağıtım, yenileme, askı, iptal etme ve iptal olmuş sertifika bilgilerini tüm taraflara duyurma süreçlerini mevzuatta belirtilen şartlara uygun olarak yerine getirmekle yükümlüdür.

Kamu SM, Kurumsal Şifreleme Sertifika Hizmet Sağlayıcısı (Kurumsal Şifreleme SHS) olarak kamu kurum ve kuruluşlarına Kurumsal Şifreleme Sertifikası hizmeti sağlamaktadır.

1.3.2. Kayıt Birimleri

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

1.3.3. Sertifika Sahipleri

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

1.3.4. Üçüncü Kişiler

Kamu SM tarafından oluşturulan sertifikaların içindeki kurum bilgileri ve açık anahtar arasındaki bağın doğruluğuna güvenerek sertifikaları kabul eden ve işlem yapan kişilerdir/kurumlardır.

Üçüncü kişiler sertifikaları kullanmadan önce gerekli gördüğü geçerlilik kontrollerini yapar.

1.3.5. Diğer Bileşenler

1.3.5.1. Kurum

Kamu SM'den Kurumsal Şifreleme Sertifikası talep eden, DETSİS'te bilgileri bulunan ve Kurumsal Şifreleme Sertifikası almaya yetkisi olan tüzel kişiliktir. Kurum sözleşme veya başvuru formu ve taahhütnamesine uygun olarak sertifika başvuru, üretim ve dağıtım süreçlerinde bu dokümanda adı geçen yerlerdeki işlemleri yapmaktan sorumludur.

1.3.5.2. Kurumsal Şifreleme Sertifikası Asıl ve Yedek Sorumlusu

Sertifika başvurusunda bulunan kurum tarafından yetkilendirilen ve Kurumsal Şifreleme Sertifikası başvurusu sırasında kurumların bilgilerini Kamu SM'ye ileten, sertifika yönetim süreçlerinde Kamu SM ile iletişim içinde olan kişi/kişilerdir. Kurumsal Şifreleme Sertifikası Asıl ve Yedek Sorumlusu Kamu SM tarafından kendisine imzalatılan taahhütnamedeki şartları yerine getirmekten sorumludur.

Kurumsal Şifreleme Sertifikası Asıl ve Yedek Sorumlusu, Kurumsal Şifreleme Sertifikasını kullanmaya yetkili olmak zorunda değildir. Kurumsal Şifreleme Sertifikasını kullanmaya yetkili kişi/kişilerin belirlenmesi kurum inisiyatifindedir.

1.4. Sertifika Kullanımı

1.4.1. Uygun Olan Sertifika Kullanımı

2017/21 sayılı Başbakanlık Genelgesi ile elektronik ortamda iletilen resmi yazıların şifreli şekilde gönderilebilmesine imkan sağlanmıştır. Kurumsal Şifreleme Sertifikası, kamu kurum ve kuruluşları arasında elektronik ortamdaki belge paylaşımında şifreleme yapmak amacıyla e-Yazışma Teknik Rehberi'ne uygun olarak kullanılmalıdır.

Kamu kurum ve kuruluşları adına üretilen Kurumsal Şifreleme Sertifikalarında bulunan açık anahtar, gönderici kurumların şifreli paket oluşturabilmesi; sertifika sahibi kurumun himayesinde bulunan özel anahtar ise kendisine gönderilen şifreli paketlerin açılabilmesi amacıyla kullanılır. Kurumsal Şifreleme Sertifikaları elektronik imzalama için kullanılmaz.

1.4.2. Sertifika Kullanımının Sınırları

Kurumsal Şifreleme Sertifikası Bölüm 1.4.1'de belirtilen amaçlar dışında kullanılamaz. Belirtilen kapsam dışında kullanımdan doğan zararlardan Kamu SM sorumlu tutulamaz.

Kamu SM, ürettiği 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 : Kamu Sertifikasyon Merkezi, TÜBİTAK Yerleşkesi, 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://depo.kamusm.gov.tr/ilke/
- http://www.kamusm.gov.tr/BilgiDeposu/KSM_SIFRELEME_SUE/KSM_SIFRELEME_SUE.pdf

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

Açık Anahtar: İlgili özel anahtarın sahibinin herkes ile paylaşılabildiği, özel anahtarı ile oluşturduğu dijital imzaların doğrulanmasında ve/veya kendisine şifreli mesaj iletilmesinde kullanılan anahtar çiftinin gizli olmayan bileşeni.

Akıllı Kart veya HSM Erişim Verisi: Sertifika sahibine ait Özel Anahtara erişimin kontrolünü sağlayan PIN ve PUK bilgisi.

Akıllı Kart: Sertifika ve sertifika ile ilişkili özel anahtarın içinde bulunduğu güvenli donanım.

Anahtar Çifti: Özel anahtar ve onunla ilişkili olan açık anahtar.

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

ÇİSDUP (Çevrim İçi Sertifika Durum Protokolü): Üçüncü kişilerin sertifika iptal listesine alternatif olarak sertifika geçerlilik kontrol talebini yapıp, sertifikanın iptal durumunu öğrenmelerine imkan tanıyan standart iletişim kuralı.

DETSİS (Devlet Teşkilatı Merkezi Kayıt Sistemi): Türkiye Cumhuriyeti Devlet yapısındaki tüm kurum ve kuruluşların ve alt birimlerin tekil ve değişmez nitelikte numaralar ile elektronik ortamda kodlanarak tanımlandığı sistem.

EYP (e-Yazışma Projesi): Kamu kurum ve kuruluşları arasındaki resmi yazışmaların elektronik ortamda yürütülmesini amaçlayan proje.

HSM (Hardware Security Module): Sertifikanın kriptografik anahtarlarının içinde bulunduğu harici aygıt; donanımsal güvenlik modülü.

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 özel 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 SM (Kamu Sertifikasyon Merkezi): Türkiye Bilimsel ve Teknolojik Araştırma Kurumu'na (TÜBİTAK) bağlı Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM) bünyesinde, elektronik sertifika hizmeti sağlamak üzere oluşturulan birim.

KAYSİS (Elektronik Kamu Bilgi Yönetim Sistemi): Kamu kurum ve kuruluşlarının teşkilat yapısının tanımlanmasından, sunulan hizmetlere; hizmetlerde kullanılan belgelerden, kurumların iletişim ve yönetici bilgilerine kadar kamu yönetiminde yer alan unsurların mevzuat dayanaklarıyla birlikte tespit edilerek elektronik ortamda tanımlandığı, geliştirilen Dijital Türkiye (e-Devlet) uygulamalarının birbirine tek merkezden entegre edilmesini sağlayacak bilgi yönetim sistem.

KEP (Kayıtlı Elektronik Posta): E-postanın gönderim ve alımına dair kanıtların oluşturulup saklandığı e-posta iletim hizmeti.

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

Kurum Doküman Doğrulama Sistemi: Elektronik ortamda hazırlanan belgelerin doğrulanması işleminde kullanılacak kuruma ait sistem veya e-Devlet belge doğrulama sistemidir.

Kurum HSM Cihaz Sorumlusu: Kamu SM ile kurum arasında HSM cihazına anahtar çifti ve sertifika yükleme ile ilgili süreci yürütecek kişidir.

Kurum: TÜBİTAK BİLGEM Kamu Sertifikasyon Merkezi'nden Kurumsal Şifreleme Sertifikası talep eden, DETSİS'te bilgileri bulunan ve Kurumsal Şifreleme Sertifikası almaya yetkisi olan tüzel kişilik.

Kurumsal Şifreleme SHS (Kurumsal Şifreleme 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.

Kurumsal Şifreleme Sertifikası Asıl Sorumlusu: Kamu kurumlarının başvuru formu ve taahhütname ile Kamu SM'ye bildirdiği ve Kurumsal Şifreleme Sertifikası ile ilgili süreçlerde kurumu temsile asıl yetkili kişi.

Kurumsal Şifreleme Sertifikası Yedek Sorumlusu: Kamu kurumlarının başvuru formu ve taahhütname ile Kamu SM'ye bildirdiği ve Kurumsal Şifreleme Sertifikası ile ilgili süreçlerde asıl yetkilinin bulunmaması durumunda kurumu temsile yetkili kişi.

Kurumsal Şifreleme Sertifikası: Elektronik ortamdaki belge paylaşımında şifreleme yapmak amacıyla kullanılan açık anahtarı içeren elektronik sertifika.

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

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

SİL (Sertifika İptal Listesi): İptal olmuş sertifika bilgilerinin içinde yer aldığı, ESHS'nin imzasını taşıyan elektronik dosya.

Sertifika Sahibi: Kurumsal Şifreleme Sertifikası başvurusunda bulunan ve sertifikayı kullanma yetkisine sahip tüzel kişi.

Sertifika Süresi: Üretim anında sertifikanın içine yazılan, sertifikanın geçerlilik başlangıç ve bitiş tarihleri arasında kalan süre.

Sİ ve SUE (Sertifika İlkeleri ve Uygulama Esasları): Kamu SM resmi web sitesi Bilgi Deposu menüsü altındaki İlke ve Uygulama Esasları'nda Elektronik Sertifika Hizmet Sağlayıcısı'nın (ESHS) işleyişi ile ilgili genel kuralları ve bu kuralların nasıl uygulanacağını detaylı olarak anlatan belgeler.

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

BGYS: Bilgi Güvenliği Yönetim Sistemi

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)

EAL (Evaluation Assurance Level): Değerlendirme Garanti Düzeyi

ECDSA (Elliptical Curve Digital Signature Algorithm): Eliptik Eğrisi Sayısal İmza Algoritması

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 Organization for Standardization/International Electrotechnical Commission): Uluslararası Standardizasyon Teşkilatı/Uluslararası Elektroteknik Komisyonu

ITU (International Telecommunication Union): Uluslararası Telekomünikasyon Birliği

Kamu SM: Kamu Sertifikasyon Merkezi

PKI (Public Key Infrastructure): Açık Anahtar Altyapısı

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 Yükümlülükleri

Bilgi deposu, Kamu SM'nin ürettiği sertifikaları, iptal durum kayıtlarını, Sİ ve SUE gibi ilgili dokümanları sertifika sahibi kurumların 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 internet adresi üzerinden yayımlanan Bilgi Deposu'nda sertifika sahibi kurumlara imzalatılan başvuru formu ve taahhütnameler, Kamu SM Taahhütnamesi, Sİ ve SUE dokümanları, sertifika hizmetleri ile ilgili yönergeler, Kamu SM'ye ait sertifikalar ve SİL'lere erişilmektedir.

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 güncel Kök SHS ve Kurumsal Şifreleme SHS sertifikaları
- Kamu SM'ye ait geçmişte oluşturulmuş Kök SHS ve Kurumsal Şifreleme SHS sertifikaları
- Kamu SM'ye ait Kök SHS sertifikalarının özet değerleri ile özet değerinin hesaplanmasında kullanılan özetleme algoritmasının hangisi olduğu bilgisi
- Kamu SM Sİ ve SUE dokümanları
- Taahhütnameler
- Yönergeler
- Formlar
- Sertifika iptal durum kayıtları

2.3. Yayım Sıklığı ve Zamanı

Taahhütnameler, yönergeler, formlar, Sİ ve SUE dokümanları içeriğinin değişmesi üzerine güncellenir. Güncellenen dokümanlar, güncelleme yapılmasını 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 personeli tarafından yapılmaktadır. Kamu SM, bilgi deposu ile ilgili olarak aşağıdaki yükümlülükleri yerine getirir:

- Bilgi deposunda tutulan bilgilerin izinsiz silinmeye ve değiştirilmeye karşı bütünlüğünü korumak
- Bilgi deposunda tutulan bilgilerin 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

Kurumsal Şifreleme Sertifikası ile ilgili işlemler yapılmadan önce, işlemi talep etmeye yetkisi olan kurumun kimlik tanımlama veya doğrulaması yapılır. Bu bölümde Kurumsal Şifreleme Sertifikası yönetim prosedürleri içinde uygulanan kurum kimlik tanımlama ve doğrulama yöntemleri ile Kurumsal Şifreleme Sertifikası içinde yazılan kurum bilgileri anlatılmıştır.

3.1. İsimlendirme

3.1.1. İsim Alanı Tipleri

Kurumsal Şifreleme Sertifikalarında Kamu SM ve sertifika sahibi kurumlara ait bilgilerin 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

Kurumsal Şifreleme Sertifikaları içeriğindeki isim alanına yazılan bilgiler kurumu tanımlayan ve kurumun kimliğinin tespit edilmesini sağlayan niteliktedir.

3.1.3. Sertifika Sahibinin Takma İsim veya Lakap Kullanması

Kurumsal Şifreleme Sertifikası içeriğinde takma isim veya lakap kullanılmasına izin verilmez.

3.1.4. Farklı İsim Alanı Tiplerinin Yorumlanması

Kurumsal Şifreleme Sertifikası içinde ITU X.500 biçimi dışında isim alanı tipi kullanılmaz.

3.1.5. Kimlik Bilgilerinin Tekilliği

Kurumsal Şifreleme Sertifikası içeriğindeki kurum bilgileri, DETSİS'te yer alan bilgilerdir ve her kurum için ayırt edici niteliktedir. Aynı kuruma ait Kurumsal Şifreleme Sertifikaları içeriğindeki kurum bilgilerinin aynı olmasına izin verilmektedir. Ancak farklı kurumlara ait Kurumsal Şifreleme Sertifikaları içeriğindeki kurum bilgilerinin aynı olması engellenmektedir. Bunun sağlanabilmesi için Kurumsal Şifreleme Sertifikalarının isim alanı içinde benzersiz bir sayı olduğu kabul edilen sertifika sahibi kuruma ait DETSİS numarası da yer alır.

3.1.6. Markanın Tanınması, Doğrulanması ve Rolü

Düzenlenmesine gerek duyulmamıştır.

3.2. İlk Kimlik Belirleme

Kamu SM Kurumsal Şifreleme Sertifikası hizmetlerinden faydalanmak için ilk defa başvuruda bulunulduğunda, ilgili kurumun doğrulanabilmesi için aşağıda tanımlanan yöntemler uygulanır.

3.2.1. Özel Anahtar Sahipliğinin Kanıtlanması

Sertifika sahibine ait açık ve özel anahtar, kurumun talebi üzerine Kamu SM tarafından üretilerek Güvenli Donanım Modülü (HSM)'ne veya akıllı karta yüklenir ve Kurumsal Şifreleme Sertifikası Asıl veya Yedek Sorumlusuna teslim edilir. Asıl veya Yedek Sorumlu tarafından Kurumsal Şifreleme Sertifikasının

teslim alındığı teyit edilir. Ek olarak, HSM'ye yüklenmesi talep edilen sertifikalar için Kurum HSM Cihaz Sorumlusu tarafından imzalanan teslim tutanağı ile teyit işlemi yapılır.

3.2.2. Kurumsal Kimliğin Belirlenmesi

Kurumsal Şifreleme Sertifikası başvurusunda bulunan kurumlar, Kamu SM tarafından istenen kurum bilgilerini, kurumu temsile yetkili kişilerin imzaladığı ve kurumun onayını taşıyan resmi yazı ile Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhütnamesi ile Kamu SM'ye bildirir. Kamu SM, başvuru formunda yer alan bilgilere istinaden kurum kimliğini belirler. Kurumların sertifika alma yetkisi DETSİS aracılığıyla kontrol edilir. Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhütnamesinde sertifika işlemlerini kurum adına yürütecek Kurumsal Şifreleme Sertifikası Sorumluları da belirlenerek Kamu SM'ye iletilir.

3.2.3. Kişisel Kimliğin Belirlenmesi

Kurumsal Şifreleme Sertifikası, kurum adına üretildiğinden yalnızca kurumsal başvuru kabul edilmektedir. Başvuru formu ve taahhütnamelerde yer alan kişisel bilgilerin doğruluğu kurumun sorumluluğundadır.

3.2.4. Doğrulanmayan Sertifika Sahibi Bilgileri

Sertifika sahibi kurum ve sertifika sorumluları tarafından başvuru sırasında ve daha sonra değişiklik sebebiyle beyan edilen aşağıdaki erişim bilgileri ve diğer bilgilerin doğruluğu Kamu SM tarafından kontrol edilmez:

- Telefon numaraları
- Kurumsal Şifreleme Sertifikası tesliminde kullanılacak adres bilgisi
- Elektronik posta adresleri
- Kurumsal Şifreleme Sertifikası Asıl ve Yedek Sorumlusunun unvanı veya görevi ile ilgili bilgiler
- Kurumsal Şifreleme Sertifikası Asıl ve Yedek Sorumlusunun çalıştığı kurum ile ilgili bilgiler
- Kurumsal Şifreleme Sertifikası Asıl ve Yedek Sorumlusunun çalıştığı birim ile ilgili bilgiler

Bu bilgilerin doğruluğu kurumun beyanı üzerine kabul edilir.

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

3.2.5. Yetkinin Doğrulanması

Sertifika içeriğine sertifika sahibi kurumun yetkisi ile ilgili bilgiler yazılmamaktadır.

3.2.6. Uyum Kriterleri

Düzenlenmesine gerek duyulmamıştır.

3.3. Sertifika Yenileme İsteğinde Kimlik Doğrulama

Bölüm 3.2'de anlatıldığı şekilde uygulanır.

3.3.1. Olağan Sertifika Yenileme İsteğinde Kimlik Doğrulama

Bölüm 3.2'de anlatıldığı şekilde uygulanır.

3.3.2. İptal Sonrası Yeni Sertifika Talebinde Kimlik Doğrulama

Bölüm 3.2'de anlatıldığı şekilde uygulanır.

3.4. Sertifika İptal İsteğinde Kimlik Doğrulama

Sertifika sahibi kurumun yetkilendirdiği sertifika sorumluları Kamu SM resmi web sitesinde yer alan Online İşlemlere kimlik doğrulamasıyla giriş yaparak iptal işlemini gerçekleştirebilir. Online İşlemler adresine ulaşılamaması durumunda Kamu SM'ye sertifika iptal başvuru formu resmi yazısı ile birlikte gönderilerek iptal işlemi gerçekleştirilebilir. Kurumsal Şifreleme Sertifikası İptal Başvuru Formu ile yapılan iptal başvurularında kurumdan gelen evraklar doğrulanır ve sertifika sorumlusu bilgileri kontrol edilir. Üst yazıda yer alan belge doğrulama kodu ile Kurum Doküman Doğrulama Sistemi üzerinden kurum doğrulaması gerçekleştirir. Kurumsal Şifreleme Sertifikası İptal Başvuru Formunun ıslak imzalı olması durumunda, Kurumsal Şifreleme Sertifikası Sorumlusu telefon ile aranarak iptal talebi teyit edilir.

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 indirme
- Sertifika iptal etme

Süreçler sertifika sahibi kurumlar ile kurum tarafından yetkilendirilen sertifika sorumluları ve Kamu SM arasında gerçekleştirilen işlemlerden oluşmaktadır.

4.1. Sertifika Başvurusu

4.1.1. Sertifika Başvurusunu Kimlerin Yapabildiği

DETSİS'te bilgileri bulunan ve DETSİS tarafından Kurumsal Şifreleme Sertifikası alma yetkisi olduğu belirtilen kamu kurum ve kuruluşları Kurumsal Şifreleme Sertifikası başvurusunda bulunabilirler.

Başvuru süreci, kamu kurumunun resmi yazısı ekinde Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhütnamesi ile HSM kullanılacaksa HSM Cihazına Anahtar ve Sertifika Yükleme Bilgi Formu ve Taahhütnamesini Kamu SM'ye göndermesiyle başlar. Belgelerin iletim yöntemi Kamu SM resmi internet sitesinden yayımlanır. Kurumun sertifika başvuru işlemleri, kurum tarafından yetkilendirilmiş sertifika sorumluları tarafından yürütülür.

4.1.2. Kayıt İşlemleri ve Sorumluluklar

Kurumsal Şifreleme Sertifikası başvurusu, kamu kurum veya kuruluşu tarafından Kamu SM'ye yapılır. Kurumun Kamu SM'den alacağı sertifika hizmetlerinin şartları TÜBİTAK BİLGEM ile karşılıklı imzalanan sözleşmeler ve/veya kurumun imzaladığı Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhütnamesi, Kamu SM'nin internet üzerinden yayımladığı ilgili yönergeler, Sİ ve SUE dokümanları doğrultusunda belirlenir.

Kurum, Kamu SM web sitesinde yayımlanan Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhütnamesini doldurur. Ardından üst yazısıyla birlikte Kurumsal Şifreleme Sertifikası Başvuru Formu

ve Taahhütnamesi eki de imzaya dahil olacak şekilde EYP dosyası oluşturarak e-posta veya KEP üzerinden Kamu SM'ye iletir. Kurum, Kurumsal Şifreleme Sertifikasını HSM içerisinde kullanmayı tercih ederse HSM Cihazına Anahtar ve Sertifika Yükleme Bilgi Formu ve Taahhütnamesi dosyasını da EYP formatı imzalı eklerine dahil etmelidir. EYP dosyası, başvuru formunda yetkili olarak belirtilen sertifika sorumlularından birine ait kurumsal e-posta veya KEP adresi üzerinden iletilmelidir. Bunun mümkün olmadığı durumlarda başvuru evrakları Kamu SM ile görüşülerek alınan onaya istinaden harici depolama aygıtı ile gönderilebilir.

Cumhurbaşkanlığı tarafından 10.06.2020 tarihli ve 2646 sayılı Resmî Gazetede yayımlanan "Resmî Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik" in, 4. Maddesi gereğince; kamu kurum ve kuruluşlarınca resmi yazışmalar, elektronik ortamda e-Yazışma Teknik Rehberi'ne uygun olarak hazırlanan ve güvenli elektronik imza ile imzalanan belgelerle yapılır. Bu kapsamda, zorunlu haller veya olağanüstü durumlar dışında EYP dosyası ile başvuru dışında başvurular kabul edilmeyecektir. Zorunlu hallerde veya olağanüstü durumlarda resmi yazışmalar, KEP veya kurumsal e-posta yoluyla iletilen ilgili başvuru formu ve taahhütnamelerin doğrulanmasının ardından ıslak imzalı ve mühürlü olacak şekilde üst yazısıyla birlikte Kamu SM'ye posta yoluyla iletilir. Kurumsal Şifreleme Sertifikası başvurusunun nasıl yapılacağı ile ilgili ayrıntılar Kamu SM'nin internet sitesinde yayımlanmaktadır.

Kurum başvuru sırasında Kamu SM'ye doğru bilgi beyan etmekle sorumludur. Kurum, Kamu SM'ye göndermiş olduğu bilgilerin doğruluğunu takip etmekle ve bu bilgilerde değişiklik olması halinde belirlenmiş araç ve yöntemler ile Kamu SM'yi bilgilendirmekle yükümlüdür. Kamu SM, Kurumsal Şifreleme Sertifikası içinde yer alacak bilgilerin doğruluğunu kontrol eder ve kendisine beyan edilen bilgilerin gizliliğini sağlamak için gerekli tedbirleri alır.

Kamu SM, sertifika verilecek kurumların kimlik tanımlama ve doğrulama işlemlerini yaptıktan sonra başvurularını değerlendirir ve uygun görülen başvuruları onaylayarak işleme alır.

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 kurum kimlik tanımlama ve doğrulama işlevleri yerine getirilir. Kurumsal Şifreleme Sertifikası başvurusunda bulunan kurumların Kamu SM'ye gönderdiği bilgi ve belgeler aşağıda sıralanmıştır:

- Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhütnamesi
- Kurum tarafından yazılan resmi yazı
- HSM kullanılacaksa HSM Cihazına Anahtar ve Sertifika Yükleme Bilgi Formu ve Taahhütnamesi

Kurumdan gönderilen belgelerin doğrulanması için aşağıdaki kontroller yapılır:

- Kurum tarafından gönderilen EYP dosyası kontrol edilerek üst yazı ve eklerinin e-imza doğrulaması yapılır.
- EYP dosyası içerisinde üst yazıda yer alan belge doğrulama kodu ile Kurum Doküman Doğrulama Sistemi üzerinden kurum doğrulaması gerçekleştirilir.
- Başvuru evraklarında yer alan kurum DETSİS numarası, DETSİS üzerinden sağlanan servis aracılığıyla kontrol edilerek kurumun Kurumsal Şifreleme Sertifikası almaya yetkili olup olmadığı sorgulanır.

- Kurum tarafından gönderilen Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhütnamesinde yer alan kurumun adı, vergi kimlik numarası, yetkilendirilen Kurumsal Şifreleme Sertifikası Asıl ve Yedek Sorumlusunun T.C. kimlik numarası, ad, soyad, kurumsal e-posta adresi, kurum birimi ve sertifika üretim nedeni bilgilerinde eksiklik olup olmadığı kontrol edilir.
- Belgelerin elektronik ortamdan iletimi mümkün olmadığı durumda kurumdan evrak asılları talep edilir. Evrak asılları ulaşan kurumların başvurularını doğrulamak için, KEP ile gönderilen evraklar ile evrakların asılları karşılaştırılarak birbirinin aynı olduğu doğrulanır. KEP kullanmayan kurum başvurularını doğrulayabilmek için kuruma iki seçenek sunulur; resmi olarak sahibi oldukları web sitelerinin belirlenen dosya yoluna elektronik ortamda ilettikleri başvuru evraklarının özet değeri eklenmeli veya başvuru formunda kurum onayını veren üst düzey yetkili ses kaydı alabilen telefon ile aranarak doğrulama onayı alınmalıdır.

Bilgi ve belgeler hatasız ve tam ise kurum kimlik tanımlama ve doğrulama işlemi tamamlanır. Belgelerde gözle görülen tahrifat, hata, eksik sayfa, eksik onay/paraf ya da eksik bilgi olması veya bilgilerin yanlışlığının tespit edilmesi durumunda kurum kimlik tanımlaması ve doğrulaması yapılamaz. Başvuru evraklarının, tanımlanan yöntemler dışında bir yöntemle iletilmesi veya evraklarda hata/eksiklik bulunması durumunda kurum, e-posta ile bilgilendirilir.

4.2.2. Sertifika Başvurusunun Kabul veya Reddi

Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından 29.05.2019 tarihli ve 2019/DK-BTD/160 sayılı Kurul Kararı ile "Kamu Kurum ve Kuruluşları Arasında Elektronik Ortamdaki Belge Paylaşımında Kullanılan Kurumsal Şifreleme ve Elektronik Mühür Sertifikalarına ilişkin Usul ve Esaslar" yayımlanmıştır. İlgili Karar ikinci bölüm, 5'inci maddesinin ikinci fıkrasının (a) bendine dayanarak, Kamu SM, DETSİS'te bilgileri bulunmayan veya Kurumsal Şifreleme Sertifikası almaya yetkisi olmayan tarafların başvurusunu reddeder.

Buna ek olarak, Bölüm 4.2.1'deki kontrollerin yapılması sonucunda, başvuru sırasında beyan edilen belgelerde tahrifat, hata, eksik onay, eksik veya yanlış bilgi olması durumlarında başvuru geri çevrilir. Başvurusu kabul edilmeyen kurumlarla ilgili yazılı bilgilendirme, Kurumsal Şifreleme Sertifikası Sorumlularının başvuru sırasında beyan ettikleri e-posta adresleri aracılığı ile yapılır ve gerekli görülen bilgi ve belgeler tekrar talep edilir. Gereken düzeltmeler yapılıp eksiklikler tamamladıktan sonra başvuru tekrarlanabilir.

Başvurusu kabul edilen kurumlar, Kamu SM sisteminde tanımlanır ve sertifika üretim süreci başlatılır.

4.2.3. Sertifika Başvurusunun İşlenme Zamanı

Başvuru evraklarının eksiksiz bir şekilde Kamu SM'ye ulaşması ve doğrulanması ardından en fazla 15 (on beş) iş günü içerisinde sertifika başvurusu işleme alınır ve sonuçlandırılır.

4.3. Sertifikanın Oluşturulması

4.3.1. Sertifika Oluşturulmasında ESHS'nin İşlevleri

Bölüm 4.2.2'de yer alan esaslar uyarınca kabul edilen sertifika başvuruları Kamu SM tarafından işlenir. Kurum, işlem kapasitesini göz önünde bulundurarak başvuru sırasında sertifikanın yükleneceği donanım olarak akıllı kart ya da HSM tercih eder.

Kurumsal Şifreleme Sertifikası, kayıp veya arıza gibi durumlarda kurumun işlemlerinde aksaklık yaşanmaması amacıyla biri yedek olmak üzere 2 adet üretilir.

4.3.2. Sertifika Oluşturulması ile İlgili Sertifika Sahibinin Bilgilendirilmesi

Akıllı karta yüklenen sertifika, sertifika sorumlusuna teslim edildiğinde Kurumsal Şifreleme Sertifikasının oluşturulduğu konusunda bilgilendirilmiş olur.

HSM cihazına sertifika yükleme işlemi, Kurum HSM Cihaz Sorumlusu gözetiminde gerçekleştirilir. İşlem sonrasında teslim tutanağı imzalanır ve Kurumsal Şifreleme Sertifikasının oluşturulduğu konusunda bilgilendirilmiş olur.

4.4. Sertifikanın Kabulü

4.4.1. Sertifikanın Kabul Koşulu

Akıllı karta basılan Kurumsal Şifreleme Sertifikası anlaşmalı kurye ile kurum adresine gönderilir ve Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhütnamesinde belirtilen Asıl Sorumluya teslim edilir. Teslimat, gerekli hallerde Asıl Sorumlunun bilgi vermesi durumunda Yedek Sorumluya yapılabilecektir. Sertifika sorumlusu kendisine teslim edilen zarf içerisinde sertifika bulunmuyorsa zarfı teslim almadan iade eder.

Kurumsal Şifreleme Sertifikasının HSM'ye yüklenmesi talebi durumunda kuruma yerinde ve uzaktan olmak üzere iki farklı yükleme seçeneği sunulmaktadır. Yerinde yükleme, kurum tarafından belirtilen zorunlu hallerde Kamu SM personelinin kurum yerleşkesine gidip HSM cihazına anahtar üretimi ve sertifika yükleme işlemlerini yerinde gerçekleştirdiği süreçlerdir. Uzaktan yükleme, Kamu SM ve kurum arasında yapılan güvenli uzak bağlantı sonrası Kamu SM personelinin HSM cihazına anahtar üretimi ve sertifika yükleme işlemlerini uzaktan gerçekleştirdiği süreçlerdir. Her iki süreç de HSM Cihazına Anahtar ve Sertifika Yükleme Bilgi Formu ve Taahhütnamesinde belirtilen Kurum HSM Cihaz Sorumlusu gözetiminde gerçekleştirilmektedir.

Asıl veya Yedek Sorumlu, sertifikanın içeriğini kontrol eder, herhangi bir eksiklik veya hata olması durumunda 5 (beş) iş günü içerisinde Kamu SM'yi bilgilendirir, aksi halde sertifikayı kabul etmiş sayılır.

4.4.2. Sertifikanın ESHS Tarafından Yayımlanması

Kamu SM tarafından üretilen ve kurum tarafından teslim alındıktan sonra askıdan indirilen Kurumsal Şifreleme Sertifikası, DETSİS'e yüklenmektedir.

4.4.3. Sertifikanın Oluşturulmasının Diğer Taraflara Duyurulması

Kamu SM tarafından üretilen ve kurum tarafından teslim alındıktan sonra askıdan indirilen Kurumsal Şifreleme Sertifikası, DETSİS'e yüklenmektedir.

4.5. Sertifikanın ve Özel Anahtarın Kullanımı

4.5.1. Sertifika Sahibinin Sertifika ve Özel Anahtar Kullanımı

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

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

4.5.2. Üçüncü Kişilerin Sertifika ve Açık Anahtarı Kullanımı

Sertifika sahibine ait Kurumsal Şifreleme Sertifikasının içinde yer alan açık anahtar, üçüncü kişilerce EYP 2.0 kapsamında verilerin şifreli iletimi amacıyla kullanılır. Açık anahtarın veya sertifikanın, belirtilen amaç 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 suretiyle yerine getirir. Sertifika yenileme işlemleri Bölüm 4.1'de anlatılan ilk sertifika başvuru işlemleri ile aynıdır.

4.7.1. Sertifikanın Yenileme Koşulları

Sertifika yenileme işlemi aşağıdaki durumlarda yapılmaktadır:

- Kurumsal Şifreleme Sertifikasının kaybedilmesi veya çalınması
- Kurumsal Şifreleme Sertifikasının arızalanması
- Akıllı karta veya HSM'ye erişim verisinin kaybedilmesi, çalınması veya unutulması
- Kurumsal Şifreleme Sertifikasının iptal edilmesi ve yenisinin talep edilmesi
- Kurumsal Şifreleme Sertifikasının geçerlilik süresinin sona ermesi veya geçerlilik süresinin sonuna yaklaşılması
- Kurumsal Şifreleme Sertifikasında bilgi değişikliği gerekmesi

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'te tanımlanmaktadır.

4.8. Sertifikada Bilgi Değişikliği

Sertifikada bilgi değişikliği, anahtar çifti hariç sertifikada yer alan bilgilerin değişmesi olarak tanımlanmaktadır. Sertifika içeriğinde kurum KAYSİS unvanı ve DETSİS numarası yer alır. Sertifika içeriğinde yer alan bilgilerde değişiklik olması, sertifikanın yenilenmesini gerektirmektedir. Bilgi değişikliğinin gerekli olduğu durumlarda, kurum Bölüm 4.7'de belirtilen sertifika yenileme sürecini işletmelidir.

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 sertifikayla bir daha işlem yapılamaz. Sertifika, aşağıda belirtilen durumlarda iptal edilir:

- Sertifika sahibi kurumun talebi
- Sertifika içeriğindeki bilgilerin sahteliğinin veya yanlışlığının ortaya çıkması veya bilgilerin değişmesi
- Sertifika sahibi kurumun kapanması
- Sertifika sahibi kurumun KAYSİS unvanının değişmesi
- Sertifika sahibi kurumun DETSİS numarasının değişmesi
- Özel anahtarın güvenliğinin kaybedildiğinden şüphelenilmesi
- Özel anahtarın içinde bulunduğu aracın kaybolması, çalınması veya bozulması
- Akıllı kart veya HSM erişim verisinin unutulması veya kaybedilmesi
- Sertifikanın Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhütnamesi, kurum ile imzalanan sözleşmeler veya SUE dokümanında belirtilen şartlara aykırı kullanımının tespit edilmesi
- Kamu SM'ye evrakları gönderen sertifika sorumlularının kurumun onayını almadığının tespit edilmesi veya ilgili kurum tarafından söz konusu durumun Kamu SM'ye bildirilmesi
- Kamu SM'nin Kurumsal Şifreleme Sertifikasını imzalamak için kullandığı imza oluşturma verisinin bütünlüğünün bozulması veya gizliliğinin ortadan kalkması
- Kamu SM'nin işleyişine son verilmesi ve verilen Kurumsal Şifreleme Sertifikalarının yönetim işlemlerinin başka bir ESHS tarafından devamlılığının sağlanamaması

4.9.2. Sertifika İptal Başvurusunu Kimler Yapabilir

Sertifika iptal başvurusu, sertifika sahibi kurum veya sertifika sahibi kurum tarafından yetkilendirilmiş Kurumsal Şifreleme Sertifikası Asıl veya Yedek Sorumlusu tarafından yapılabilir. Kamu SM, Bölüm 4.9.1'de tanımlanan tüm durumlarda iptal yetkisine sahiptir.

4.9.3. Sertifika İptal Başvurusunun İşlenmesi

Kurumsal Şifreleme Sertifikası iptal işlemi, kurum tarafından yetkilendirilen Kurumsal Şifreleme Sertifikası Asıl veya Yedek Sorumlusu tarafından Kamu SM resmi internet sitesinde yer alan Online İşlemler menüsü aracılığı ile yapılır.

Kamu SM Online İşlemler üzerinden yapılan iptal başvurusunda, Kurumsal Şifreleme Sertifikası Asıl veya Yedek Sorumlusu sisteme kimlik doğrulamasıyla giriş yaparak iptal talebinde bulunur. İlgili talebin ardından, Kurumsal Şifreleme Sertifikası Kamu SM sisteminde otomatik olarak iptal edilir.

İptal işlemlerinin Kamu SM Online İşlemler üzerinden yapılamadığı durumda Kurumsal Şifreleme Sertifikası İptal Başvuru Formu, Kurumsal Şifreleme Sertifikası Sorumlusu tarafından doldurularak iletilmelidir. Kurumsal Şifreleme Sertifikası Sorumlusunda veya sorumluya ait bilgilerde değişiklik olması durumunda Kurumsal Şifreleme Sertifika Sorumlusu Bilgi Güncelleme Formu da eksiksiz bir şekilde doldurulmalıdır. Formlar üst yazısıyla birlikte sorumluya ait kurumsal e-posta üzerinden Kamu SM'ye gönderilir. Formun ıslak imzalı ve mühürlü halinin üst yazısıyla birlikte mutlaka Kamu SM'nin Gebze adresine posta yoluyla acil olarak iletilmesi gerekmektedir. Kurumdan e-posta ile gelen evraklarda yer alan bilgiler kontrol edilerek üst yazıda yer alan belge doğrulama kodu ile Kurum Doküman Doğrulama Sistemi üzerinden kurum doğrulaması gerçekleştirilir. İptal sürecinin başlatılmasının ardından evrak asılları Kamu SM'ye ulaşana kadar kurum yazışmalarında yaşanabilecek aksaklıkların en aza indirgenmesi amacıyla Kurumsal Şifreleme Sertifikası Sorumlusu telefon ile aranarak iptal talebi teyit edilir ve iptali talep edilen sertifika askıya alınarak varsa yedek sertifika devreye alınır. Evrak asıllarının ulaşmasının ardından Kamu SM'ye e-posta üzerinden gönderilen evraklar ile asılları karşılaştırılır ve askıya alınan sertifika iptal edilir.

Kurumsal Şifreleme Sertifikası iptal edildikten sonra, Kamu SM sertifika sahibi kurumu ve gerekirse sertifika sorumlularını iptal işlemine dair bilgilendirir. Kurumsal Şifreleme Sertifikaları geçmişe yönelik olarak iptal edilmez.

İptal süreci, Kamu SM resmi web sitesinde ayrıntılı olarak anlatılmaktadır. Kamu SM, internet sitesi üzerinden iptal işleminin gerçekleştirilebilmesi için gerekli hizmetleri kesintisiz olarak sunar.

Kamu SM iptal bilgilerini en kısa zamanda işler ve kamuya duyurur. Kamuya duyurulan iptal durum kayıtları en azından Kurumsal Şifreleme Sertifikasının seri numarası ile Kamu SM'nin elektronik imzasını taşır. Kamu SM, iptal durum kayıtlarını SİL yayımlamak ve ÇİSDUP Yanıtlayıcı'da Kurumsal Şifreleme Sertifikasının durumunu iptal konumuna getirmek suretiyle duyurur. İptal edilen sertifika bilgisi Kamu SM tarafından DETSİS'ten kaldırılır.

SİL dosyası, Kamu SM'ye ait imza oluşturma verisi ile imzalanır. İptal edilen Kurumsal Şifreleme Sertifikaları geçerlilik süresinin sonuna kadar SİL içinde tutulur. Geçerlilik süresi dolduktan sonra Kurumsal Şifreleme Sertifikası SİL içinden çıkarılır. ÇİSDUP Yanıtlayıcı'da geçerlilik süresi dolan iptal edilmiş Kurumsal Şifreleme Sertifikalarının durumu iptal edilmiş olarak görünmeye devam eder.

Kurum, Kurumsal Şifreleme Sertifikası iptal edildikten sonra yeniden Kurumsal Şifreleme Sertifikası 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 Kurumsal Şifreleme Sertifikasını en geç 24 saat içerisinde iptal eder. İptal edilen Kurumsal Şifreleme Sertifikası 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 Kurumsal Şifreleme Sertifikasına dayanarak işlem yapmadan önce Kurumsal Şifreleme Sertifikasının geçerliliğini SİL ya da ÇİSDUP yöntemlerinden birini kullanarak kontrol etmekle yükümlüdür.

Üçüncü kişiler Kurumsal Şifreleme Sertifikası 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 (otuz altı) saattir. Ancak bu sürenin dolması beklenmeden her 4 (dört) saatte bir SİL tekrar yayımlanır. Gün içinde yeni bir Kurumsal Şifreleme Sertifikası iptali olmasa dahi SİL 4 (dört) saatte bir güncellenir. Eski SİL dosyaları geçerlilik süresinin sonuna kadar geçerliliğini korur.

Kamu SM'ye ait sertifikaların iptal bilgilerinin duyurulduğu SİL dosyası, en geç 12 (on iki) ayda bir yenilenir. Kamu SM'ye ait bu sertifikalardan birinin 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 Hizmeti

Kamu SM, Kurumsal Şifreleme Sertifikalarının iptal durum bilgisini ÇİSDUP üzerinden yayımlar. ÇİSDUP Yanıtlayıcı'dan yayımlanan iptal durum kaydı Kamu SM'ye ait olduğu duyurulan imza oluşturma verisiyle imzalanır.

ÇİSDUP desteği olan uygulamalar Kurumsal Şifreleme Sertifikalarının geçerlilik durum kontrolünü ESHS Erişim Bilgisi isimli sertifika uzantısında (Authority Information Access) 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 Kurumsal Şifreleme Sertifikası 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 Kurumsal Şifreleme Sertifikasının 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. Özel Anahtarın Güvenliğini Yitirmesi Durumu

Sertifika sahibi kuruma ait özel anahtarın güvenliğini yitirmesi durumunda Kurumsal Şifreleme Sertifikası iptal edilir. Kurum Şifreleme Sertifikasının iptal edilmesi dışında herhangi bir işlem uygulanmamaktadır.

4.9.13. Sertifikanın Askıya Alındığı Durumlar

Kurumsal Şifreleme Sertifikası, üretim veya kullanım aşamasında geçici iptal durumunu sağlamak amacıyla askıya alınabilir.

Kurumsal Şifreleme Sertifikaları biri yedek olmak üzere 2 adet üretilir ve askı durumunda kuruma gönderilir. Kullanılacak sertifika, kurumun sertifika sorumlusu tarafından Kamu SM Online İşlemler üzerinden askıdan indirilir. Aynı anda sertifikalardan sadece biri aktif olabilir. Aktif olan sertifika askıya alınmadan ya da iptal edilmeden yedek sertifika askıdan indirilemez.

Sertifika sahibi kurum veya kurumun yetkilendirdiği Asıl veya Yedek Sertifika Sorumlusu, aşağıda belirtilenlere benzer sebeplerden dolayı Kurumsal Şifreleme Sertifikasını askıya alabilir:

- Sertifika sahibi kurumun Kurumsal Şifreleme Sertifikasını kullanım dışı bırakmak istemesi
- Kurumsal Şifreleme Sertifikasının iptal sebebinin ortaya çıktığından şüphelenildiği durumlarda, yanlışlıkla iptalini engellemek amacıyla, Kurumsal Şifreleme Sertifikasının önce askıya alınmak istenmesi
- Aktif kullanılan geçerli sertifikanın kayıp/çalıntı/arıza durumunda yedek sertifikanın kullanıma açılabilmesi

4.9.14. Sertifika Askıya Alma Başvurusunu Kimlerin Yapabildiği

Kurumsal Şifreleme Sertifikasının askıya alma başvurusu, sadece sertifika sahibi kurum veya kurumun yetkilendirdiği Kurumsal Şifreleme Sertifikası Asıl veya Yedek Sorumlusu tarafından yapılır.

4.9.15. Sertifika Askıya Alma Başvurusunun İşlenmesi

Kurumsal Şifreleme Sertifikası askı başvurusu, Kamu SM web sitesinde yer alan Online İşlemler menüsünden veya Online İşlemlerin Kamu SM kaynaklı erişilemez olması durumunda sertifika sorumluları tarafından telefonla Kamu SM'ye bildirilerek yapılır. Askı başvurusu alındığında öncelikle başvuruyu yapan sertifika sahibi kurumun ve yetkililerinin kimlik belirlemesi ve doğrulaması yapılır. Kimlik doğrulaması yapılamayan askı başvuruları işleme alınmaz.

Askıya alınan Kurumsal Şifreleme Sertifikası için, SİL'de geçici olarak iptal edildiğini belirten sebep kodu kullanılır, ÇİSDUP Yanıtlayıcı'da sertifika durum bilgisi iptal konumuna getirilir. Kamu SM, Kurumsal Şifreleme Sertifikası askıya alındıktan sonra, gerekli gördüğü durumlarda sertifika sahibi kurumu ve bağlı bulunduğu kurum tarafından yetkilendirilen sorumluları sertifikanın askıya alındığına dair bilgilendirir.

Sertifika sorumluları, Kamu SM Online İşlemler üzerinden kuruma ait sertifikayı askıdan indirebilir. Askıya alınan sertifika en az bir defa SİL'e girmeden askıdan indirilemez.

Kuruma ait Kurumsal Şifreleme Sertifikalarından aynı anda sadece biri aktif olabilir. Aktif olan sertifika askıya alınmadan ya da iptal edilmeden yedek sertifika askıdan indirilemez.

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

4.9.16. Askıda Kalma Süresi

Sertifikalar askıda üretilir, ilk üretim sonrasında askıdan indirmeyle ilgili bir süre kısıtı bulunmamakla birlikte kurum tarafından askıya alınan sertifikalar en az 12 (on iki) saat süresince askıdan indirilemez.

4.10. Sertifika Durum Servisleri

Üçüncü kişiler, Kamu SM sertifika iptal durum kayıtlarına SİL ve ÇİSDUP servisleri aracılığıyla 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 Bölüm 7.1.2 Tablo 1'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 Bölüm 7.1.2 Tablo 1'de verilmiştir. Üçüncü kişiler, Kurumsal Şifreleme Sertifikalarının 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

Kurumsal Şifreleme Sertifikasının kullanım süresinin dolması, iptal edilmesi ve Kamu SM'nin sertifika hizmetlerini sonlandırmasıyla sertifika sahipliği sona erer. Kamu SM, Kurumsal Şifreleme Sertifikasının iptal edilmesi ve Kamu SM tarafından sertifika hizmetlerinin sonlandırılması durumunda sertifika sahibi kurumu ve Kurumsal Şifreleme Sertifikası Asıl ve/veya Yedek Sorumlularını bilgilendirir. Kamu SM, Kurumsal Şifreleme Sertifikalarının süresi dolmadan en az 15 (on beş) gün önce sertifika sahibi kurumu bilgilendirir.

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. Güvenli alanlara erişimlerin kaydı tutulmaktadır.

5.1.1. Tesis Yeri ve İnşaatı

Kamu SM operasyonları Gebze ve Ankara'daki tesislerde yürütülmektedir. Kamu SM sisteminin çalıştığı binanın bulunduğu Gebze tesisi, yerleşim merkezinden uzak, yangın, su baskını, deprem, yıldırım ve hava kirliliğinden en az etkilenecek, giriş ve çıkışların kontrol edildiği bir bölgedir. Alanlara ve binalara

erişim, tek kişinin girişine veya çıkışına izin veren HI-SEC kilitleme kapıları dahil olmak üzere fiziki güvenlik, video izleme ve kimlik doğrulama olmak üzere çoklu güvenlik ile korunmaktadır. Ankara tesisi farklı seviyelerde fiziksel kontrolü bulunan bir alandır. Yetkisiz personel ve kayıtsız ziyaretçiler bu hassas alanlara giremez.

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 üniteleri, yedekli iklimlendirme üniteleri, havalandırıcılar, yangın söndürücü sistemler 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. Güvenli alanlarda tek kişi çalışma yapamaz, en az biri yetkili olmak üzere 2 (iki) kişi ile çalışma yapılır. 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 sürekliliğin sağlanması için kullanılmaktadır:

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

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

5.1.4. Su Baskınları

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

5.1.5. Yangın Önleme ve Korunma

Kamu SM 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. Buna ek olarak gerekli görülen ortamların yerinde yedeği alındığı gibi gerekli güvenlik kriterlerini sağlayan ayrı bir lokasyonda da yedekler alınmaktadır.

5.1.7. Atıkların Yok Edilmesi

Hassas bilgilerin bulunduğu ve artık kullanılmayan elektronik veya kağıt ortamda tutulan bilgiler/cihazlar imha prosedürüne uygun bir şekilde geri dönüşümsüz olarak imha edilir.

5.1.8. Farklı Mekanlarda Yedekleme

Kamu SM, farklı mekanda yedekleme işi için konum olarak tamamen ayrı, uzak bir felaket kurtarma merkezine sahiptir. Yedek sistemin bulunduğu mekan, asıl sistemin sağladığı tüm güvenlik ve işlevsellik şartlarını sağlar.

Kamu SM, sisteminin sürekliliğini sağlayabilmek amacıyla gerekli gördüğü bileşenleri, farklı bir fiziksel mekanda güvenli kasalarda saklar.

5.2. Prosedürsel Kontroller

5.2.1. Güvenilir Roller

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

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

Güvenlik Personeli: Kamu SM güvenlik politikalarının uygulanmasından sorumludur.

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

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

Sistem Denetçisi: Sertifika hizmetleriyle ilgili iş ve işlemlerin denetlenmesinden sorumludur.

Sertifika Kayıt Sorumlusu: Sertifika üretim/iptal başvurusunun alınması, başvuru evraklarının ve kurum kimliğinin doğrulanmasından sorumlu personeldir.

Sertifika Üretim Sorumlusu: Sertifika üretimini gerçekleştiren personeldir.

5.2.2. Her İşlem İçin Gereken Kişi Sayısı

Kamu SM, Kök SHS ve Kurumsal Şifreleme SHS'ye ait sertifika üretilmesi ve iptal edilmesi için birden fazla kişinin aynı anda hazır bulunmasını sağlar.

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

Kurumsal Şifreleme Sertifikalarının üretimi iki kişinin kontrolünde 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.

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

5.2.4. Görevlerin Ayrılmasını Gerektiren Roller

Aşağıda verilen roller arasında görevler ayrılığı vardır:

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

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. Adli sicil kayıtları incelenir. Güvenlik soruşturması biten personel işe başlatılır. İşe başlayan personelin bilgi güvenliği farkındalık eğitimleri tamamlanmadan, sistemlere erişimine izin verilmez.

5.3.3. Eğitim Gerekleri

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

Kamu SM, çalışanlarına yılda en az bir defa, siber güvenlik ve sosyal mühendislik saldırılarına karşı farkındalık oluşturmak amacıyla, bilgi güvenliği eğitimi vermektedir.

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

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 Kamu SM süreçleriyle ilgili gerekli kılavuz ve destek dokümanlar ve bilgi güvenliği politikaları kapsamındaki ilgili dokümanlar 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
- 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
- Sertifika yaşam döngüsü yönetimi işlemleri
    - Sertifika başvurusunun işlenmesi
    - Sertifika üretimi
    - Sertifika yenileme

- Sertifika iptal etme
- SİL yayımlanması

- Güvenlikle ilgili diğer işlemler
  - Sisteme başarılı veya başarısız tüm erişim denemeleri
  - Çalışanlar tarafından gerçekleştirilen güvenlik sistemi işlemleri
  - Güvenli tutulması gereken hassas dosyaların okunması, yazılması ve değiştirilmesi
  - Güvenlik profili değişiklikleri
  - Sistemin çökmesi, donanım hataları ve diğer bozukluklar
  - Güvenlik cihaz/yazılım işlemleri (Güvenlik Duvarları, IPS, HIDS, Router vb.)
  - Kamu SM'ye ziyaretçi giriş ve çıkışı

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

5.4.2. Kayıtların İncelenme Sıklığı

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

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

5.4.3. Kayıtların Saklanma Süresi

Kayıtlar incelenmelerinden sonra, en az 2 (iki) ay sistemde tutulur. Ardından arşivlenir. Talep edilmesi halinde kayıtlar yetkili denetçilere sunulur.

5.4.4. Kayıtların Korunması

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

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

5.4.5. Kayıtların Yedeklenmesi

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

5.4.6. Kayıtların Toplanması

Kayıtlar uygulama katmanında, ağ katmanında ve işletim seviyesi düzeyinde otomatik olarak toplanır.

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 sertifika başvurusu ve sertifika yaşam döngüsüyle ilgili, elektronik olarak ya da kağıt üzerinde tutulan aşağıdaki belgeler arşivlenir:

- Sertifika sahibi kurum tarafından, başvuru sırasında verilen tüm bilgi ve belgeler
- Sertifika üretimi, yenileme, askıya alma, askıdaki sertifikayı kullanıma açma ve iptal başvuruları sırasında elektronik veya kağıt ortamda alınan formlar
- Sertifika işlemleriyle ilgili yapılan önemli yazışmalar
- Üretilen tüm sertifikalar
- Geçerlilik süresi dolan tüm Kamu SM kök ve alt kök sertifikaları
- Yayımlanan tüm sertifika iptal durum kayıtları
- Sertifika İlkeleri dokümanı
- Sertifika Uygulama Esasları dokümanı
- Sertifika yönetim prosedürleri
- Sertifika Sahibi Taahhütnameleri
- Sertifikasyon süreçlerinde kullanılan sistemlerin NTP senkronizasyon loglar

5.5.2. Arşivlerin Tutulma Süresi

Arşivlenen bilgiler ve belgeler 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 Bölüm 5.5.2'de belirtilen süre boyunca arşivlerin zarar görmesini engelleyecek şekilde seçilir.

5.5.4. Arşivlerin Yedeklenmesi

Kritik bilgi içeren elektronik arşivler Kamu SM 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.

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:

- Kök sertifikası kullanım süresinin dolmasından en geç 3 (üç) yıl önce; alt kök sertifikası kullanım süresinin dolmasından en geç 1 (bir) yıl önce işlemler başlatılır. Eski anahtarlarla sertifika verilmesi durdurulur.
- Kamu SM'nin eski imza oluşturma verisiyle imzalanmış sertifikaların doğrulanabilmesi için, eski Kamu SM sertifikası yayımlanmaya devam eder.
- SİL dosyaları aynı Kamu SM imza oluşturma verisiyle imzalanıyorsa, Kamu SM'nin eski imza oluşturma verisiyle oluşturulmuş sertifikaların kullanım tarihleri dolana kadar, Kamu SM SİL'leri eski imza oluşturma verisiyle imzalanmaya devam eder. Yeni üretilen sertifikalar için oluşturulan yeni SİL dosyası yeni Kamu SM imza oluşturma verisiyle imzalanır.
- Kamu SM, anahtarlarının yenilendiği bilgisini Kamu SM resmi web sitesi 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 ve kritik süreçler için felaket kurtarma merkezi oluşturulmuştur. 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 Kurumsal Şifreleme Sertifikalarını 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 Kamu SM resmi web sitesi üzerinden duyurur ve ilgili kurumları yazıyla bilgilendirir.

- Kamu SM, Kurumsal Şifreleme Sertifikası sahiplerinin durumdan ne şekilde etkileneceğini belirten açıklamayı yapar, eski özel anahtarıyla oluşturulan Kurumsal Şifreleme Sertifikalarına güvenilmemesi için ilgili taraflara ihtarda bulunur.
- Kamu SM, kendisine ait sertifikanın iptal edildiği bilgisini yayımladığı SİL dosyasında belirtir.
- Kamu SM tarafından üretilen Kurumsal Şifreleme Sertifikalarının gerekli görülen bir kısmı veya hepsi iptal edilir. İptal bilgisi sertifika sahipleri ile ilgili kurumlara en kısa zamanda bildirilir.
- Kamu SM Kurumsal Şifreleme Sertifikası 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 Kurumsal Şifreleme Sertifikalarının 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 iş sürekliliği planlarında tanımlar.

Kamu SM başka bir şehirde felaket kurtarma merkezine sahiptir. Kamu SM yedeklilik yönetim politikasına uygun olarak önemli veri ve uygulamaların yedeklerini almakta ve gerekli durumlarda yedekten geri dönme işlemlerini uygulamaktadır. İş sürekliliğinin devamı için Kamu SM merkez ofiste saklanan verilerin yedekleri felaket kurtarma merkezinde de saklanmaktadır.

Kamu SM, arıza sonrası yeniden çalışırlığı sağlayacak Kamu SM iş sürekliliği planlarını periyodik olarak gözden geçirir ve test eder. Kamu SM arıza durumlarının tekrarlanmaması için gerekli önlemleri alır.

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, sertifika sahiplerine ise 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.
- Ürettiği Kurumsal Şifreleme Sertifikalarını iptal eder, iptal bilgisini SİL ve ÇİSDUP aracılığıyla üçüncü kişilere duyurur. İptal ettiği Kurumsal Şifreleme Sertifikalarının bilgisini kurumlara yazılı olarak, sertifika sahiplerine e-posta ile duyurur.
- İptal ettiği Kurumsal Şifreleme Sertifikalarının 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.
- Kurumsal Şifreleme Sertifikalarını 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, Kurumsal Şifreleme SHS, ÇİSDUP Yayımlayıcı Anahtar Çifti Üretimi

Kamu SM bünyesinde aşağıdaki anahtar çiftleri oluşturulur:

- Kök SHS'ye ait imza oluşturma ve doğrulama verisi
- Kurumsal Şifreleme SHS'ye ait imza oluşturma ve doğrulama verisi
- ÇİSDUP Yayımlayıcı'ya ait imza oluşturma ve doğrulama verisi
- Kurumsal Şifreleme Sertifikası sahiplerine ait anahtar çifti

Kök SHS, Kurumsal Şifreleme SHS ve ÇİSDUP Yanıtlayıcı'ya ait anahtar çiftleri, yetkisi olmayan personelin giremeyeceği güvenli odada, birden fazla eğitimli personelin gözetiminde, ağ ortamına kapalı sistemlerde, güvenli anahtar üretimi için gereken testlerden geçmiş, FIPS-140-2 seviye 3 veya EAL4+ standartlarını sağlayan güvenli yazılım ve/veya donanım kullanılarak üretilir. Üretilen özel anahtar güvenli kriptografik modül içinde saklanır. Modül güvenli odadan dışarıya çıkarılmaz. Yapılan bütün işlemler kayıt altına alınır ve işlemi gerçekleştiren personel tarafından onaylanır.

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

6.1.1.2. Sertifika Sahibi Anahtar Çiftinin Üretimi

Kurumsal Şifreleme Sertifikası akıllı karta yüklenecekse, sertifika sahibinin anahtar çiftleri Kamu SM tarafından yetkisi olmayan personelin giremediği odalarda, güvenli yazılım ve/veya donanım kullanılarak üretilir.

Kurumsal Şifreleme Sertifikası HSM'ye yüklenecekse, Kurum HSM Cihaz Sorumlusu gözetiminde Kamu SM yetkili personeli tarafından, HSM yerli ve millî ise HSM içerisinde, değilse HSM dışında güvenli yazılım ve/veya donanım kullanılarak üretilir.

Anahtar çiftleri güvenli anahtar üretimi için gereken testlerden geçmiş, güvenilir programlar kullanılarak üretilir. Anahtar çifti üretmek için güvenilirliği dünyaca kabul görmüş algoritmalar kullanılır.

Sertifika sahibine ait özel anahtarın yedeği alınmaz, bir kopyası hiçbir şekilde sistemde tutulmaz. Sertifika sahibine ait özel anahtarın saklandığı akıllı kart veya HSM Bölüm 6.2.1'de belirtilen güvenlik standartlarına uyar.

6.1.2. Sertifika Sahibine Özel Anahtarın Ulaştırılması

Sertifika sahiplerine ait anahtar çiftlerinin Kamu SM tarafından oluşturulmasına müteakip, özel anahtar, sertifikayla birlikte akıllı kart veya HSM'ye yüklenir. Akıllı kart, imza karşılığı ve resmi kimlik kontrolü yapılarak sahibine teslim edilir. HSM'ye özel anahtar ve sertifika yükleme işlemi, Kurum HSM Cihaz Sorumlusu gözetiminde gerçekleştirilir ve işlem sonrası Teslim Tutanağı doldurularak kurum tarafından imzalanır.

Akıllı karta erişim verisi web üzerinden teslim edilir. Web üzerinden teslim edilen veriler için güvenli bağlantı protokolleri (HTTPS) kullanılmaktadır. Asıl veya Yedek Sertifika Sorumlusunun kimlik kontrolü

için, T.C. kimlik numarası ve mobil telefona gönderilen SMS onay mesajı kullanılmaktadır. Bu şekilde gerçekleştirilen kimlik doğrulaması sonrasında sertifika sahibi akıllı kart erişim verisine erişir. HSM'ye erişim verisinden Kamu SM sorumlu değildir, kurum inisiyatifindedir.

Kamu SM'nin yükümlülüklerinin belirtildiği Kamu SM Taahhütnamesi, Kamu SM resmi web sitesi Bilgi Deposu sayfası üzerinden yayımlanır.

6.1.3. Elektronik Sertifika Hizmet Sağlayıcısı'na Açık Anahtarın Ulaştırılması

Kurumsal Şifreleme Sertifikası HSM'ye yüklenecekse, PKCS#10 formatında sertifika imzalama isteği, Kamu SM yetkili personeli tarafından kurumsal e-posta aracılığıyla Kamu SM'ye ulaştırılır.

Kurumsal Şifreleme Sertifikası akıllı karta yüklenecekse, Kurumsal Şifreleme Sertifikaları anahtar çiftleri Kamu SM tarafından üretildiği için açık anahtarın Kamu SM'ye ulaştırılması söz konusu değildir.

6.1.4. Elektronik Sertifika Hizmet Sağlayıcısı Sertifikalarına Erişim Sağlanması

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

Kök SHS ve Kurumsal Şifreleme SHS sertifikaları, sertifikaların özet değeri ve özet algoritması Kamu SM resmi web sitesi Bilgi Deposu sayfası üzerinden yayımlanır.

6.1.5. Anahtar Uzunlukları

Kamu SM Kök SHS'ye ait ECDSA anahtar boyu en az 384-bittir.

Kurumlara ait Kurumsal Şifreleme Sertifikalarını imzalayan Kurumsal Şifreleme SHS'ye ait ECDSA anahtar boyu en az 384-bittir.

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

Kamu SM tarafından üretilen Kurumsal Şifreleme Sertifikaları, RSA anahtar 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

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

Kamu SM kök anahtarı, alt kök sertifikasını ve SİL'i imzalamak için kullanılır. Kamu SM Kurumsal Şifreleme Sertifikalarının imzalanmasında kullanılan sertifika zinciri Ek-A'da detaylı olarak bulunmaktadır. ÇİSDUP yanıtlarının imzalanmasında alt kök ve kök tarafından yetkilendirilmiş ÇİSDUP sertifikası kullanılır.

6.2. Özel Anahtarın Korunması

6.2.1. Kriptografik Modül Standartları

Kamu SM'ye ait imza oluşturma verisi güvenli yazılım ve/veya donanım 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 özel anahtarının içinde bulunduğu akıllı kart veya HSM cihazı, özel anahtarın donanım dışına çıkmasını engelleyen ve donanıma erişimi parola ile sağlayan teknik özelliklere sahiptir.
- Kriptografik modül ve sertifika sahibine ait akıllı kart veya HSM cihazı, 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. Özel Anahtara Birden Fazla Kişi Kontrolünde Erişim

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

6.2.3. Özel Anahtarın Yeniden Elde Edilmesi

Düzenlenmesine gerek duyulmamıştır.

6.2.4. Özel Anahtarın 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 özel anahtarlar Kamu SM tarafından yedeklenmez.

6.2.5. Özel Anahtarın Arşivlenmesi

Kamu SM'ye ve sertifika sahiplerine ait özel anahtarlar arşivlenmez. Kullanım süreleri sonunda geri dönüşsüz şekilde silinir.

6.2.6. Özel Anahtarın 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 özel anahtarlar, sadece yetkili personelin kontrolünde akıllı kart veya HSM cihazına şifrelenerek yüklenir. Özel anahtar, akıllı kart veya HSM cihazına yüklendikten sonra kopyası sistemden silinir.

6.2.7. Özel Anahtarın 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 sahibinin özel anahtarı, kendisine ait akıllı kart veya HSM cihazı içinde saklanır, başka bir ortamda bulunmaz. Kamu SM, sertifika sahiplerine ait özel anahtarları kendi sistemi içinde saklamaz.

6.2.8. Özel Anahtara 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 özel anahtar, akıllı kart veya HSM cihazı içinde sertifika sahibinin erişim verisi ile korunmuş olarak saklanır. Erişim denetimi erişim denetim verisi ile sağlanır.

6.2.9. Özel Anahtara 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, özel anahtarı kullanan oturumun kapanmasından sonra veriye erişimi kesecek biçimde çalışır. Erişimin yeniden sağlanabilmesi için sertifika sahibinin erişim verisini yeniden girmesi gerekir. Erişim verisinin art arda 3 (üç) defa yanlış girilmesi durumunda güvenli donanım aracı kilitlenir ve araca erişim sağlanamaz.

6.2.10. Özel Anahtarın 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 özel anahtarların kullanım süresinin sonunda veya sertifikanın iptal edilmesinden sonra sahibi tarafından akıllı kart veya HSM cihazı 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. Açık Anahtarın Arşivlenmesi

Kamu SM'ye ve sertifika sahibine ait açık anahtarlar, sertifikalar içinde tutulur ve Kurumsal Şifreleme Sertifikaları kullanım sürelerinin dolmasından itibaren 20 (yirmi) yıl boyunca arşivlenir. Kurumsal Şifreleme Sertifikalarının arşivleri yetkisiz kişilerce tahrifatına ve silinmesine karşı gerekli önlemlerin alındığı ortamlarda tutulur.

6.3.2. Özel ve Açık Anahtarların Kullanım Süreleri

Özel anahtarın kullanım süresi, Kurumsal Şifreleme Sertifikasının içeriğinde belirtilen kullanım süresi kadardır. Kurumsal Şifreleme Sertifikasının kullanım süresinin dolmasıyla ya da Kurumsal Şifreleme Sertifikasının iptal edilmesiyle özel anahtarın kullanımı sona erer.

Kamu SM'ye ve sertifika sahibine ait anahtar çiftlerinin kullanım süresi, anahtar uzunlukları ve kullanılan algoritmaya göre belirlenir. Kamu SM'ye ait 384 bitlik ECDSA anahtar çiftleri en fazla 10 (on) yıl için kullanılır. Sertifika sahiplerine ait 2048 bitlik RSA anahtar çiftleri en fazla 1 (bir) yıl için kullanılır.

Üretilen Kurumsal Şifreleme Sertifikalarının son kullanma tarihi, Kurumsal Şifreleme 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 sahibi kuruma ait iki farklı erişim denetim verisi tanımlanmıştır. Bunlar, akıllı karta erişim verisi ile sertifika işlemlerinin yapıldığı internet şubesine erişim verileridir.

6.4.1. Erişim Denetim Verilerinin Oluşturulması

Kamu SM sistemi içinde kullanılan erişim denetim verileri ile sertifika sahibi kuruma 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 kurum 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 sahibi kuruma ait erişim parolaları sertifika sahibi kuruma 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 ile İlgili Diğer Konular

Erişim denetimi verilerinin sahibine ulaştırılması güvenli yollarla yapılır. Sertifika sahibine ait erişim parolaları, iki kademeli kimlik doğrulama ile erişilen web sayfası üzerinden sahibine teslim edilir.

6.5. Bilgisayar Güvenliği Denetimleri

6.5.1. Bilgisayar Güvenliği ile 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, bunlar sürekli güncel tutulmaktadır. Kritik işlemlerin yapıldığı bilgisayarlar ağ ortamı dışında tutulur. Bilgilerin 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. Güvenlik yamaları değerlendirilip daha büyük bir riske sebebiyet vermesi durumunda yüklenmez ve risk süreç takip sistemi üzerinde kayıt altına alınır. Ağ bileşenleri ve konfigürasyonları dönemsel olarak ağ güvenliği prosedürü yönergesine göre kontrol edilir.

6.5.2. Bilgisayar Sisteminin Sağladığı Güvenlik Seviyesi

Düzenlenmesine gerek duyulmamıştır.

6.6. Yaşam Döngüsü Teknik Kontrolleri

6.6.1. Sistem Geliştirme Kontrolleri

Sistem geliştirilirken 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 işler TS ISO/IEC 27001 gereklerini sağlar.
- Geliştirme faaliyetleri sırasında geliştirme, test ve canlı sistemler ayrılır. Canlıya alınma işlemi onay mekanizmalarından sonra gerçekleştirilir.
- Sistem bileşenlerine dair periyodik risk değerlendirmeleri yapılır ve yönetime sunulur.
- Sistemlerde gerçekleştirilen değişiklikler kayıt altına alınır ve izlenir.
- Uzaktan erişim dahil üçüncü tarafların sistemlere erişimine izin verilmez.

6.6.2. Güvenlik Yönetimi Kontrolleri

Sistem içinde kurulu olan yazılım ve donanım ürünleri ile ağ ortamının işleyişinin planlanan şekilde güvenli olarak sürdürüldüğünü göstermek için 2 (iki) 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. Güvenlik kontrolleri için temel dayanak ISO 27001'in güncel sürümüdür.

6.6.3. Yaşam Döngüsü Güvenlik Denetimleri

Düzenlenmesine gerek duyulmamıştır.

6.7. Ağ Güvenliği Denetimleri

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

Sunucular üzerine ağ ve sistem yönetimi ve güvenliği ajanları kurulmuştur. Yönetim yazılımı bu ajanlardan disk, hafıza, işlemci kullanımı, dosya bütünlüğü, güvenlik kayıtları, harici depolama üniteleri takibi vb. bilgileri çeker ve bu bilgileri gerçek zamanlı görüntüler. Sunucuların çalışması için önem arz eden kaynaklar için eşik değerler belirlenir ve bu eşik değerlerin aşılması durumunda sistem yöneticisi otomatik olarak uyarılır. Ağ ve sistem yönetimi ve güvenliği altyapısı çektiği bilgileri merkezi bir veri tabanında saklar. Böylece herhangi bir anda verilerin sorgulanmasına ve geçmişe dönük rapor üretilmesine imkan tanınır. Farklı güvenilir sistemlerle iletişim ihtiyacı olması durumunda, diğer iletişim kanallarından mantıksal olarak farklı olan güvenilir iletişim kanalları kurulur.

Yüksek güvenlik gerektiren işlemlerin yapıldığı sistemler (kök ve alt kök sunucuları gibi) için farklı ağ segmentleri oluşturulmuştur. Kritik işlemlerin yapıldığı sistemler ağa bağlı değildir. Canlı ortam servis ve sistemleri, geliştirme ve test ortamlarından ayrılmıştır. Güvenli ve yüksek güvenli bölgelere erişimler erişim kontrol protokolüne göre belirlenir. Yüksek güvenlik gerektiren sistemlerde kullanılan donanımlar farklı yerlerde tekrar tekrar kullanılmaz, imha edilirler.

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

Güvenlik politikası yönetim uygulamaları farklı amaçlarda kullanılmaz. Kök ve alt kök üzerinde bulunan gereksiz hesaplar, uygulamalar, hizmetler, port ve protokoller sıkılaştırma prosedürlerine göre kaldırılır ya da devre dışı bırakılır. Ağ ve sistem güvenliğine dair tüm işlemler siber olaylara müdahale ekibi tarafından izlenir ve gerektiğinde olay müdahale süreçleri doğrultusunda aksiyon alınır. Kamu SM çevrim içi açık anahtar altyapısı hizmetlerinin devamlılığı için Kamu SM ana merkez ve felaket kurtarma merkezinin dış ağ bağlantı hizmetlerini yedekli olarak kurgulamıştır.

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

6.8. Zaman 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 Esaslarında bulunur.

7. Sertifika ve Sertifika İptal Listesi Biçimleri

7.1. Sertifika Biçimi

Bu bölümde Kamu SM tarafından dağıtılan Kurumsal Şifreleme Sertifikalarının 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 Kurumsal Şifreleme Sertifikaları X.509 V.3 formatında tanımlanan sertifikanın seri numarası, geçerlilik tarihi, ilgili açık anahtar, sertifika sahibi kurumun adı ve DETSİS numarası, 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. Kurumsal Şifreleme Sertifikasının içeriğinde bulunan sertifika uzantıları sertifikanın kullanılacağı uygulamanın gereklerine bağlı olarak belirlenir.

Tablo 1'de Kamu SM tarafından üretilen Kurumsal Şifreleme Sertifikalarında asgari düzeyde bulunması gereken uzantılar tanımlanmıştır.

Tablo 1 Kurumsal Şifreleme Sertifika Uzantıları

Sertifika Uzantısı	Kritik Uzantı	Açıklama
Temel Kısıtlar[1]	HAYIR	Sertifikanın son kullanıcı sertifikası olduğu, ESHS sertifikası amacıyla kullanılamayacağı belirtilir.
Yetkili Anahtar Tanımlayıcısı[2]	HAYIR	Kamu SM'ye ait Kurumsal Şifreleme SHS açık anahtarının SHA-1 özet çıktısından oluşur.

[1] BasicConstraints

[2] AuthorityKeyIdentifier

Sertifika Anahtar Tanımlayıcı[3]	HAYIR	Sertifikanın içeriğindeki "subjectPublicKey" alanının "BIT STRING" olarak değerinin SHA-1 özet çıktısından oluşur.
Anahtar Kullanımı[4]	EVET	Anahtarların sadece şifreleme amaçlı kullanıldığının ifade edilmesi için "keyEncipherment" [anahtar şifreleme] alanı seçilmiştir.
SİL Dağıtım Noktaları[5]	HAYIR	http://depo.kamusm.gov.tr/ksifreleme/ksifreleme.v1.crl
Yetkili Bilgi Erişimi[6]	HAYIR	http://depo.kamusm.gov.tr/ksifreleme/ksifreleme.v1.crt http://ksifrelemeocspv1.kamusm.gov.tr/
Sertifika İlkeleri[7]	HAYIR	Kamu SM Sİ dokümanına ait nesne tanımlama numarası (2.16.792.1.2.1.1.5.7.1.11) ile SUE dokümanının bulunduğu http://depo.kamusm.gov.tr/ilke internet adresini ve BTK tarafından oluşturulan Kurumsal Şifreleme Sertifikası ibaresine ait metni içerir.
Genişletilmiş Anahtar Kullanımı[8]	HAYIR	Kurumsal Şifreleme Sertifikası nesne tanımlama numarasını (2.16.792.1.2.1.1.5.7.51.1) içerir.

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

7.1.3. Algoritma ve Nesne Tanımlayıcılar

Kamu SM, kurumlara verdiği Kurumsal Şifreleme Sertifikalarını imzalamak için SHA-384 özet algoritması ile ECDSA açık anahtarlı imzalama algoritmasını kullanır.

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 Kurumsal Şifreleme Sertifikalarındaki isim alanı "ITU X.500 Distinguished Name [Ayırt edici İsim]" biçimine uygundur.

---

[3] SubjectKeyIdentifier

[4] KeyUsage

[5] CRLDistributionPoints

[6] AuthorithyInformationAccess

[7] CertificatePolicies

[8] ExtendedKeyUsage

7.1.5. İsim Kısıtları

Bölüm 3.1'de belirtilmiştir.

Tablo 2'de Kurumsal Şifreleme Sertifikası içinde yer alan isim alanları ve bu alanlar içine yazılacak bilgiler belirtilmiştir.

Tablo 2 Kurumsal Şifreleme Sertifika İsim Alanı Bilgileri

Alan Adı	Kurumsal Şifreleme Sertifika İçeriği
CN[9]	Kurum DETSİS adı
Serial[10]	Kurum DETSİS numarası
C[11]	TR

7.1.6. Sertifika İlkeleri Nesne Tanımlama Numarası

Bağlı olunan Kamu SM Sİ dokümanına ait nesne tanımlama numarası: 2.16.792.1.2.1.1.5.7.1.11

7.1.7. İlke Kısıtları Uzantısının Kullanımı

Düzenlenmesine gerek duyulmamıştır.

7.1.8. İlke Niteleyiciler

"Sertifika İlkeleri Uzantısı" Kurumsal Şifreleme Sertifikalarının üretim ve yönetim işlemlerinde uyulan ilke ve esasların Kamu SM Sİ ve Kamu SM SUE olduğuna işaret eder. Kurumsal Şifreleme Sertifikalarının üretim ve yönetiminde takip edilen kurallara işaret eden Sİ dokümanına ait nesne tanımlama numarası [Certificate Policy Object Identifier(s)] Kamu SM tarafından üretilen Kurumsal Şifreleme Sertifikasının "Sertifika İlkeleri Uzantısı[12]"nın içinde yer alır. "Sertifika İlkeleri Uzantısı"nın içinde "İlke Niteleyici[13]" 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 Kurumsal Şifreleme Sertifikalarını kullanarak işlem yapar.

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.

---

[9] CN: Common Name [Genel isim]

[10] Serial: Serial Number [Seri Numarası]

[11] C: Country [Ülke]

[12] Certificate Policies

[13] Policy Identifier

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-384 özet algoritması ile ECDSA açık anahtarlı imzalama algoritmasını kullanır.)
- SİL'in yayımlanma tarihi
- SİL numarası
- Bir sonraki SİL yayımlanma tarihi
- İptal edilen Kurumsal Şifreleme Sertifikaları ile 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 "Yetkili Anahtar Tanımlayıcı" numarası

7.3. Çevrim İçi Sertifika Durum Protokolü Biçimi

7.3.1. Sürüm Numarası

Çevrim İçi Sertifika Durum Protokolü RFC 6960 V.1'i destekler.

7.3.2. ÇİSDUP Uzantıları

ÇİSDUP sorguları aşağıdaki bilgileri içermelidir:

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

ÇİSDUP yanıtları aşağıdaki bilgileri içermektedir:

- Versiyon bilgisi
- Yanıtlayıcının adı
- Her bir sertifika için cevap bilgisi (sertifika belirteci (sertifika seri numarası), sertifika durumu, cevap geçerlilik süresi)
- Kullanılan imza algoritmasının nesne tanımlama numarası
- 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 6960'ta 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 6960'ta belirtilen uzantılar ÇİSDUP cevap formatında kullanılmamaktadır.

8. Uygunluk Denetimleri

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

8.1. Uygunluk Denetiminin Sıklığı

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, yılda bir defa gerçekleştirilir.

8.2. Denetçinin Nitelikleri

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

İç denetim, Kamu SM sertifika süreçlerini bilen ve denetim konusunda tecrübeli Kamu SM personeli tarafından gerçekleştirilir.

8.3. Denetçinin Denetlenen Tarafla Olan İlişkisi

Dış denetçiler, herhangi bir çıkar çatışması olmaması ve bağımsızlığın zedelenmemesi için Kamu SM'den bağımsız kişilerden oluşur. İç denetim için seçilen denetçiler ise denetlenecek birimden seçilmez.

8.4. Denetimin Kapsamı

Kamu SM iç denetimlerinde, Sİ ve SUE dokümanına uygunluk denetlenir. İç denetim kapsamı denetimi gerçekleştirecek Kamu SM personeli tarafından belirlenir.

ISO/IEC 27001 BGYS denetiminin kapsamı BGYS standardına uygun şekilde bağımsız kurum denetçisi tarafından belirlenir.

8.5. Yetersizliğin Tespiti Durumunda Yapılacaklar

ISO/IEC 27001 standardına göre gerçekleştirilen denetimlerde ortaya çıkan eksiklikler, Kamu SM tarafından planlı çalışma ile giderilir. Eksiklikler, BGYS'nin 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 Uygunsuzluk veya Düzeltici/İyileştirici Faaliyetler açılarak takip edilir.

8.6. Sonucun Bildirilmesi

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

İç denetim sonucu, 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 Kurumsal Şifreleme Sertifikası için kurumlardan ücret alınır. Ücretin miktarı ve ödeme şekli a Kamu SM web sitesinde bildirilir.

Kamu SM'nin imza oluşturma verisinin çalınması, kaybolması, gizliliğinin veya güvenilirliğinin ortadan kalkması, sertifika ilkelerinin değişmesi ya da Kurumsal Şifreleme Sertifikasının hatalı üretilmesi gibi sertifika sahibi kurumun kusurunun bulunmadığı durumların sonucunda Kurumsal Şifreleme Sertifikalarının Kamu SM tarafından iptal edilmesi ve güncellenmesi halinde, hiçbir ücret talep edilmez.

9.1.2. Sertifika Erişim Ücreti

Kamu SM, kendisine ait sertifikaları resmi web sitesinde ücretsiz olarak yayımlar. Kamu SM tarafından üretilen Kurumsal Şifreleme Sertifikaları DETSİS'e yüklenir.

9.1.3. İptal Durum Kaydına Erişim Ücreti

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

9.1.4. Diğer Servis Ücretleri

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

Kamu SM, kuruma ait özel anahtar ve sertifikanın saklandığı akıllı kartın teminini kendi imkanlarıyla sağlayabilir. Kurumsal Şifreleme Sertifikaları ve güvenli donanım araçları için ödenecek bedelin miktarı ile ilgili bilgilendirme Kamu SM tarafından gönderilen teklif mektuplarında veya Kamu SM web sitesinde bildirilir. Ödemenin usulüne uygun biçimde yapılmaması durumunda Kurumsal Şifreleme Sertifikası üretimi yapılmayabilir.

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

9.1.5. İade Ücreti

Ön ödemeli olarak talepte bulunulan sertifikanın/sertifikaların üretimi tamamlanmamışsa kurumun talebi doğrultusunda yatırılan miktar kadar ücret iadesi yapılır. Üretilen sertifikalar için ücret iadesi söz konusu değildir.

9.2. Finansal Sorumluluk

9.2.1. Sigorta Kapsamı

Kamu SM, Bölüm 9.2.3'te 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, ürettiği Kurumsal Şifreleme 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 resmi web sitesi bilgi deposu üzerinden yayımlanan doküman ve sertifikalar içerisinde yer alan bilgiler gizli olarak değerlendirilmez.

9.3.3. Gizli Bilginin Korunma Sorumluluğu

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

9.4. Kişisel Bilginin Gizliliği

9.4.1. Gizlilik Planı

Kamu SM verdiği hizmetlerde sertifika sahiplerinin ve diğer paydaşların kişisel verilerinin gizliliğini 2017/21 Sayılı Başbakanlık Genelgesi, Bilgi Teknolojileri ve İletişim Kurulu Kamu Kurum ve Kuruluşları Arasında Elektronik Ortamdaki Belge Paylaşımında Kullanılan Kurumsal Şifreleme ve Elektronik Mühür Sertifikalarına İlişkin Usul ve Esaslar'da ve 6698 sayılı kanunlar kapsamındaki mer'i mevzuata uygun olarak sağlar.

9.4.2. Gizli Olarak Tanımlanan Bilgiler

Kişisel bilgi, sertifika sahibi kurumun ve yetkilendirdiği Kurumsal Şifreleme Sertifikası Asıl ve Yedek Sorumlusu ile Kurum HSM Cihaz Sorumlusunun, başvuru sırasında kimlik tanımlama ve doğrulama ile sertifika yönetim prosedürleri içinde kullanılmak üzere Kamu SM'ye beyan ettiği bilgiler ile adres ve telefon numarası gibi erişim bilgilerini kapsar. Kamu SM veya sertifika sahibi kurum tarafından atanan parolalar, numara, sembol gibi diğer tanımlayıcıyı bilgiler de kişisel bilgi kapsamına girer.

9.4.3. Gizli Olarak Tanımlanmayan Bilgiler

Kurumsal Şifreleme Sertifikası içeriğinde bulunan bilgiler, aksi taraflar arası sözleşmelerde belirtilmediği sürece gizli değildir.

9.4.4. Gizli Bilginin Korunma Sorumluluğu

Kamu SM, sertifika talep eden kurumdan Kurumsal Şifreleme Sertifikası 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 sahibi kurumun 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 sahibi kurumun bilgilerine erişirler.

9.4.5. Gizli Bilginin Kullanımına İzin Verilmesi

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

9.4.6. Yetkili Mercilerin Kararına Uygun Olarak Bilginin Açıklanması

Kamu SM tarafından sertifika sorumlularına 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 Kurumsal Şifreleme Sertifikaları 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 tarafından verilen sertifika hizmetlerinde sistem bileşenleri olarak tanımlanan Kamu SM, sertifika sahipleri ve üçüncü kişiler 2017/21 Sayılı Başbakanlık Genelgesi, Bilgi Teknolojileri ve İletişim Kurulu Kararı ile yayımlanan Kamu Kurum ve Kuruluşları Arasında Elektronik Ortamdaki Belge Paylaşımında Kullanılan Kurumsal Şifreleme ve Elektronik Mühür Sertifikalarına İlişkin Usul ve Esaslarda belirtilen şekilde üzerlerine düşen yükümlülükleri sağlar.

Kamu SM, sertifika sahibi kamu kurum veya kuruluşları ile üçüncü kişiler yasa ve yönetmeliklerde belirtilmediği halde imzalanmış olan Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhütnamesi yükümlülüklerini de 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 aşağıda belirtilmiştir:

- 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 Kurumsal Şifreleme SHS için anahtar çifti üretmek ve bu anahtar çiftleri için sertifikalar oluşturmak
- Kök SHS ve Kurumsal Şifreleme SHS sertifikalarını son kullanıcıların erişebileceği ortamlarda yayımlamak
- Kurumsal Şifreleme Sertifikası verdiği kurumların kimliğini DETSİS üzerinden güvenilir bir biçimde doğrulamak

- Kurumlardan gelen Kurumsal Şifreleme Sertifikası başvurularını usulüne uygun biçimde kabul etmek ve başvuruda bulunan kurumların belgeleri ile başvuru formlarını gerekli kontrollerden geçirmek
- Kurumsal Şifreleme Sertifikasının içeriğindeki bilgilerin doğruluğunu beyan edilen belgelere dayanarak sağlamak
- Gerekli başvuru şartlarını sağlamayan başvuru sahiplerine Kurumsal Şifreleme Sertifikası vermemek
- Kurumsal Şifreleme Sertifikası başvurularını değerlendirerek, başvurunun sonucu hakkında kurumları ya da kurumların yetkilendirdikleri sorumlu kişileri bilgilendirmek
- Kurumsal Şifreleme Sertifikası başvurusu kabul edilmiş kurumlar için anahtar çifti ve Kurumsal Şifreleme Sertifikası üretmek
- Sertifika sahibi kuruma ait özel anahtarı oluşturduktan sonra özel anahtar ve üretiminde kullanılan gizli değişkenleri kendi sisteminden silmek, özel anahtarın kopyasını hiçbir şekilde tutmamak
- Sertifika sahibine akıllı kart temin etmesi durumunda, bu aracın güvenli olmasını sağlamak
- Üretilen Kurumsal Şifreleme Sertifikaları özel anahtarlarını Sİ ve SUE'de belirtilen şekilde güvenli olarak sertifika sahiplerine teslim etmek
- Sertifika sahiplerinin Kurumsal Şifreleme Sertifikalarını DETSİS'e yüklemek
- Kurumsal Şifreleme Sertifikalarının kullanım şartlarını belirleyen sertifika profillerini oluşturmak
- Kurumsal Şifreleme Sertifika başvurularını Sİ ve SUE'de belirtilen şekilde kabul etmek ve değerlendirerek gerekli işlemlerini yapmak
- Kurumsal Şifreleme Sertifikası askıya alma başvurularını Sİ ve SUE'de belirtilen şekilde kabul etmek ve değerlendirerek gerekli askıya alma işlemlerini yapmak
- Kurumsal Şifreleme Sertifikası askıdan indirme işlemlerini Sİ ve SUE'de belirtilen şekilde yapmak
- Kurumsal Şifreleme Sertifikası iptal başvurularını Sİ ve SUE'de belirtilen şekilde kabul etmek ve değerlendirerek gerekli iptal işlemlerini zamanında yapmak
- Yayımlanan Sİ ve SUE dokümanları ile Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhütnamesine uygun olmayan Kurumsal Şifreleme Sertifikası kullanımlarının tespit edilmesi durumunda ilgili Kurumsal Şifreleme Sertifikasını iptal etmek
- İptal edilmiş Kurumsal Şifreleme Sertifikası bilgilerini sertifika iptal listelerinde yayımlamak veya ÇİSDUP Yanıtlayıcı aracılığıyla duyurmak
- Kurumsal Şifreleme Sertifikalarının 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
- Kurumsal Şifreleme Sertifikası 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

9.6.2. Kayıt Birimi Yükümlülükleri

Kayıt birimlerinin yükümlülükleri Bölüm 9.6.1'de belirtilen ESHS yükümlülükleri ile aynıdır.

9.6.3. Sertifika Sahibinin Yükümlülükleri

Sertifika sahibinin yükümlülükleri aşağıda belirtilmiştir:

- Kurumsal Şifreleme Sertifikası başvuru, askıya alma, iptal ve diğer işlemleri, ilgili Sİ ve SUE'de belirtildiği şekilde, detayları Kamu SM Kurumsal Şifreleme Sertifikası yönetim prosedürlerinde anlatılan usule uygun biçimde yerine getirmek
- Kurumsal Şifreleme Sertifikası başvurusu, yenileme ve iptal işlemleri sırasında doğru bilgi beyan etmek
- Kurum adına düzenlenen Kurumsal Şifreleme Sertifikası üretildiğinde sertifikadaki bilgilerin doğruluğunu kontrol etmek
- SUE Bölüm 6.2.1'de belirtilen standartlara uygun akıllı kart veya HSM kullanmak
- Özel anahtarın güvenliğini sağlamak, kendisine ait özel anahtarın içinde bulunduğu akıllı kart veya HSM'in ve 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
- Özel anahtarın içinde bulunduğu akıllı kart veya HSM'in kaybolması, çalınması veya özel anahtarın gizliliğinin yitirildiğinden şüphelenmesi durumunda Kurumsal Şifreleme Sertifikasının iptal edilmesi için Kamu SM'ye en kısa zamanda başvurmak
- Akıllı kart veya HSM erişim verisini ve sertifika işlemlerinde kullandığı diğer parolaları düzenli olarak değiştirmek
- Kurumsal Şifreleme Sertifikası içeriğinde bulunan bilgilerin değişmesi durumunda derhal sertifikanın iptal edilmesi için Kamu SM'ye başvurmak
- Kurumsal Şifreleme Sertifikası 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 Kurumsal Şifreleme Sertifikası ile işlem yapmamak
- Özel anahtarını imzalama amacıyla kullanmamak

Sertifika sahibi kurum, Kamu SM Kurumsal Şifreleme Sertifikası Sİ ve SUE dokümanlarında belirtilen şartları okuduğunu, başvuru süreci ve sertifika geçerliliği boyunca Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhütnamesi, ilgili mevzuatlar ile Sİ ve SUE dokümanında belirtilen şartlara uygun olarak hareket edeceğini kabul ve taahhüt eder. Yükümlülüklerin ihlali nedeniyle üçüncü kişilerin/kurumun zarara uğraması halinde TÜBİTAK BİLGEM'in ödemek zorunda olduğu tazminatlarla ilgili sertifika sahibine rücu hakkı saklıdır.

9.6.4. Üçüncü Kişilerin Yükümlülükleri

Üçüncü kişiler, Kurumsal Şifreleme Sertifikasıyla işlem yapmadan önce sertifikanın aşağıda belirtilen geçerlilik kontrollerini yapmakla yükümlüdür:

- Kurumsal Şifreleme Sertifikasının tanımlanan veriliş amacına uygun olarak kullanıldığını doğrulamak
- Kurumsal Şifreleme Sertifikasının kullanım süresinin dolup dolmadığını kontrol etmek

- Kurumsal Şifreleme Sertifikasının geçerliliğini SİL veya ÇİSDUP Yanıtlayıcı aracılığıyla kontrol etmek
- SİL veya ÇİSDUP Yanıtlayıcı'dan aldığı iptal durum kaydının bütünlüğünü Kamu SM'nin ilgili sertifikası içinde mevcut olan imza doğrulama verisini kullanarak doğrulamak
- Kurumsal Şifreleme Sertifikasının doğruluğunu Kurumsal Şifreleme SHS sertifikasının içinde mevcut olan imza doğrulama verisini kullanarak doğrulamak
- Kurumsal Şifreleme SHS 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 Kurumsal Şifreleme Sertifikasının içindeki açık anahtarına karşılık gelen özel anahtara sahip olduğunu doğrulamak

9.6.5. Diğer Bileşenlerin Yükümlülükleri

9.6.5.1. Kurumun Yükümlülükleri

Kamu SM'ye sertifika başvurusunda bulunan kurumun yükümlülükleri aşağıda belirtilmiştir:

- Sertifika yönetim süreçlerinde Kamu SM ile iletişim içinde olacak biri asıl biri yedek olmak üzere iki tane kurum sertifika sorumlusu görevlendirmek ve Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhütnamesi ile kurum sertifika sorumlularının bilgilerini Kamu SM'ye bildirmek
- Kurum sertifika sorumlusunun görevi sonlandırıldığında bunu Kamu SM'ye resmi yazı ve Kurumsal Şifreleme Sertifikası Yetkili Güncelleme Formu ile bildirmek
- Yeni görevlendirdiği kurum sertifika sorumlularının bilgilerini Kamu SM'ye resmi yazı ve Kurumsal Şifreleme Sertifikası Yetkili Güncelleme Formu ile bildirmek
- Sertifika yönetim süreçleri ile ilgili varsa Kamu SM ile imzalanan sözleşmeye uymak
- Sertifika yönetim süreçleri ile ilgili Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhütnamesindeki yükümlülükleri yerine getirmek
- Kamu SM'nin internet sitesi üzerinden yayımladığı Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhütnamesini doldurarak sertifika başvurusu sırasında resmi yazı ile Kamu SM'ye iletmek

9.6.5.2. Kurum Sertifika Sorumlularının Yükümlülükleri

Kurum adına Kurumsal Şifreleme Sertifikası başvurusunda bulunan Kurumsal Şifreleme Sertifikası Asıl ve Yedek Sorumlusunun yükümlülükleri aşağıda belirtilmiştir:

- Sertifika alınacak kuruma ait bilgileri tam ve doğru bir şekilde Kamu SM'ye iletmek
- Sertifika yönetim süreçleri ile ilgili işleri Kamu SM ile koordineli bir şekilde yürütmek
- Kamu SM'nin kendisine imzalattığı taahhütnamedeki yükümlülükleri yerine getirmek

Kurumsal Şifreleme Sertifikası Asıl ve Yedek Sorumlusunun sertifika teslimatları ile ilgili yükümlülükleri Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhütnamesinde belirtilmiştir.

9.7. Yükümlülüklerden Feragat

Kamu SM ile sertifika sahipleri olan kamu kurum veya kuruluşları arasındaki yükümlülük, Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhütnamesi ve varsa imzalanan sözleşmelerde belirtildiği şekilde sona erer.

9.8. Sorumlulukla İlgili Sınırlamalar

Kamu SM ve sertifika hizmeti alan tarafların sorumlulukları 2017/21 Sayılı Başbakanlık Genelgesi, Bilgi Teknolojileri ve İletişim Kurulu Kararı ile yayımlanan Kamu Kurum ve Kuruluşları Arasında Elektronik Ortamdaki Belge Paylaşımında Kullanılan Kurumsal Şifreleme ve Elektronik Mühür Sertifikalarına İlişkin Usul ve Esaslar'da belirtilen şartlar ile sınırlıdır.

Kamu SM ve sertifika hizmetlerini alan tarafların sorumlulukları ile ilgili sınırlamalar Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhütnamesi ve varsa imzalanan sözleşmelerde belirlenir. 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 sahibi kurum, Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhütnamesi ve varsa imzalanan sözleşmelere uygun olarak Kamu SM ile iş birliği içinde çalışır.

Sertifika sahibi kurumlar 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 ve SUE dokümanları, sertifika yönetim prosedürleri, sertifika sahibine ilettiği Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhütnamesi ve varsa kurum ile imzaladığı sözleşmelerdeki şartları yerine getirir.

9.10.1. Anlaşma Süresi

Sertifika sahibi kurumun imzaladığı Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhütnamesinin veya imzalanan sözleşmenin süresi sertifikanın geçerlilik süresi veya taahhütname veya sözleşmede belirtilmişse hizmetin alınma süresi kadardır. Ancak, sertifikanın iptal edilmesi durumunda sözleşme veya taahhütnamenin süresi de sona erer. Kurumla imzalanan sözleşmenin geçerlilik süresi sözleşme içerisinde belirtilir.

9.10.2. Anlaşmanın Sona Ermesi

Kamu SM ile kurum arasında varsa imzalanan sözleşme 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 20 (yirmi) 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 feshedilebilir.
- Bölüm 5.7.3'te belirtilen güvenlik açığının ortaya çıkması sebebiyle Kamu SM sertifika sahiplerine ait Kurumsal Şifreleme Sertifikalarını iptal ederek sözleşmeyi sonlandırabilir.

- Kamu SM Bölüm 5.8'de belirtildiği biçimde sertifika hizmetlerini sonlandırırsa, sertifika sahiplerine ait Kurumsal Şifreleme Sertifikalarını iptal ederek sözleşmeyi sonlandırabilir.

Kamu SM Taahhütnamesi ve Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhütnamesi veya imzalanan sözleşme aşağıdaki durumlarda sonlandırılabilir:

- Sertifika sahibi kurumun sertifikasını iptal etmesi
- Sertifikanın kullanım süresinin sona ermesi
- Sertifika sahibi kurumun imzalanan sözleşme veya Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhütnamesine aykırı davranması durumunda Kamu SM'nin sertifika sahibi kuruma ait sertifikayı iptal etmesi
- Bölüm 5.7.3'te belirtilen güvenlik açığının ortaya çıkması sebebiyle Kamu SM'nin sertifika sahibi kuruma ait sertifikayı iptal etmesi
- Kamu SM Bölüm 5.8'de belirtildiği biçimde sertifika hizmetlerini sonlandırırsa, Kamu SM'nin sertifika sahibi kuruma ait sertifikayı iptal etmesi

9.10.3. Anlaşmanın Sona Ermesinin Etkileri

Kurumla imzalanan sözleşmenin 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.

İmzalanan sözleşme veya Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhütnamesinin sona ermesiyle sertifika sahibinin, taahhütname ile Sİ ve SUE dokümanlarında belirtilen şartları sağlamakla ilgili yükümlülükleri ortadan kalkar. Sertifika sahibi kurumun Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhütnamesinden, Sİ ve SUE dokümanlarından kaynaklanan yükümlülüklerini yerine getirmemesi durumunda, Kamu SM sertifikayı iptal eder. Sertifika sahibi kurumun taahhütnameye uygun hareket etmemesinden dolayı uğrayacağı zararlardan Kamu SM sorumlu tutulamaz.

Sözleşme ve taahhütnameler sona erse bile Kamu SM, ürettiği Kurumsal Şifreleme Sertifikaları ile ilgili mevzuatta belirtilen yükümlülükleri yerine getirmeye devam eder. Kamu SM, ürettiği Kurumsal Şifreleme Sertifikalarının iptal durum kayıtlarına taraflarca erişimin sağlanması, Bölüm 5.4 ve 5.5'te belirtilen kayıtların ve arşivlerin saklanması ile ilgili hizmetleri sürdürür.

9.11. Sistem Bileşenleri ile Haberleşme ve Kişisel Bilgilendirme

Kamu SM, Kurumsal Şifreleme Sertifikaları başvuru, iptal ve yenileme taleplerinin sonuçları hakkında sertifika sahibi kurumu bilgilendirir. Bilgilendirmeler telefon veya kurumsal e-posta aracılığıyla sağlanır. Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhütnamesinde belirtilen sertifika sorumlusunun kurumsal e-posta adresine, değişmesi halinde yeni bildirdiği kurumsal e-posta adresine yapılan bilgilendirmeler resmi bildirim olarak kabul edilir.

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

Sertifika yönetim işlemleri sırasında sertifika sorumluları veya kurumlarla yapılan haberleşmenin hangi durumlarda, ne şekilde yapılacağı Kamu SM'nin Kurumsal Şifreleme Sertifikası yönetim prosedürlerinde detaylı olarak belirtilir.

9.12. Değişiklik Halleri

9.12.1. Değişiklik Metotları

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 SUE dokümanının 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.

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 2017/21 Sayılı Başbakanlık Genelgesi, Bilgi Teknolojileri ve İletişim Kurulu Kararıyla yayımlanan Kamu Kurum ve Kuruluşları Arasında Elektronik Ortamdaki Belge Paylaşımında Kullanılan Kurumsal Şifreleme ve Elektronik Mühür Sertifikalarına İlişkin Usul ve Esaslara başvurulur. İhtilafların sulhen çözümünün mümkün olmaması halinde, ihtilafların çözümünde görevli ve yetkili mahkeme Türkiye Cumhuriyeti Gebze Mahkemeleri'dir.

9.14. Uygulanacak Hukuk

SUE dokümanındaki hükümler, 2017/21 Sayılı Başbakanlık Genelgesi, Bilgi Teknolojileri ve İletişim Kurulu kararıyla yayımlanan Kamu Kurum ve Kuruluşları Arasında Elektronik Ortamdaki Belge Paylaşımında Kullanılan Kurumsal Şifreleme ve Elektronik Mühür Sertifikalarına İlişkin Usul ve Esaslara 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.

10. EK-A SERTİFİKA PROFİLLERİ

10.1. KAMU SM KURUMSAL ŞİFRELEME KÖK SERTİFİKASI

Alan	Değer
Sürüm	V3
Seri Numarası	00ed1db82e01d6
İmza Algoritması	SHA-384 ile ECDSA { 1 2 840 10045 4 3 3}
Sertifikayı Veren	CN = Kamu SM Kök Sertifika Hizmet Sağlayıcısı - Sürüm 6 OU = BİLGEM O = Türkiye Bilimsel ve Teknolojik Araştırma Kurumu - TÜBİTAK L = Gebze - Kocaeli C = TR
Geçerlilik Başlangıcı	9 Ağustos 2019 Cuma 19:25:08
Geçerlilik Sonu	6 Ağustos 2029 Pazartesi 19:25:08
Konu	CN = Kamu SM Kök Sertifika Hizmet Sağlayıcısı - Sürüm 6 OU = BİLGEM O = Türkiye Bilimsel ve Teknolojik Araştırma Kurumu - TÜBİTAK L = Gebze - Kocaeli C = TR
Açık anahtar	384 bit ECC { 1 2 840 10045 2 1 } ECDSA_P384 { 1 3 132 0 34 }
Uzantılar	**Değer**
Konu Anahtarı Tanımlayıcısı	Kritik=Hayır; Anahtar Kimliği= 30 cb d6 81 10 23 2c 9f 44 32 0f e0 ba 7b f1 89 c2 c0 39 da
Anahtar Kullanımı	**Kritik=Evet**; Sertifika İmzalama, Çevrimdışı SİL İmzalama, SİL İmzalama
Temel Kısıtlamalar	**Kritik=Evet**; Konu Türü=CA; Yol Uzunluğu Kısıtlaması=Yok

10.2. KAMU SM KURUMSAL ŞİFRELEME ALT KÖK SERTİFİKASI

Alan	Değer
Sürüm	V3
Seri Numarası	00f4dfbe9d0289
İmza Algoritması	SHA-384 ile ECDSA {1 2 840 10045 4 3 3}
Sertifikayı Veren	CN = Kamu SM Kök Sertifika Hizmet Sağlayıcısı - Sürüm 6 OU = BİLGEM O = Türkiye Bilimsel ve Teknolojik Araştırma Kurumu - TÜBİTAK L = Gebze - Kocaeli C = TR
Geçerlilik Başlangıcı	20 Kasım 2020 Cuma 15:56:15
Geçerlilik Sonu	6 Ağustos 2029 Pazartesi 19:25:08
Konu	CN = Kurumsal Şifreleme Sertifika Hizmet Sağlayıcısı - Sürüm 1 OU = Kamu Sertifikasyon Merkezi O = TÜBİTAK - BİLGEM L = Gebze - Kocaeli C = TR
Açık anahtar	384 bit ECC {1 2 840 10045 2 1} ECDSA_P384 {1 3 132 0 34}
Uzantılar	**Değer**
Yetkili Anahtarı Tanımlayıcısı	Kritik=Hayır; Anahtar Kimliği= 30 cb d6 81 10 23 2c 9f 44 32 0f e0 ba 7b f1 89 c2 c0 39 da
Konu Anahtarı Tanımlayıcısı	Kritik=Hayır; Anahtar Kimliği= ab 71 39 0b 21 74 35 cb 23 40 79 a7 3f d1 2c 21 73 94 a0 ab
Anahtar Kullanımı	**Kritik=Evet**; Sertifika İmzalama, Çevrimdışı SİL İmzalama, SİL İmzalama
Temel Kısıtlar	**Kritik=Evet**; Konu Türü=CA; Yol Uzunluğu Kısıtlaması=0

Sertifika İlkeleri	[1]Sertifika İlkesi: İlke Tanımlayıcısı=2.16.792.1.2.1.1.5.7.1.11 [1,1]İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimliği=CPS Niteleyici= http://depo.kamusm.gov.tr/ilke [1,2]İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimliği=Kullanıcı Uyarısı Niteleyici= Uyarı Metni=Bu sertifika ile ilgili sertifika ilke ve uygulama esaslarını okumak için belirtilen web sitesini ziyaret ediniz.
SİL Dağıtım Noktaları	[1]SİL Dağıtım Noktası Dağıtım Noktası Adı: Tam Ad: URL=http://depo.kamusm.gov.tr/nes/kokshs.v6.crl
Yetkili Bilgi Erişimi	[1]Yetkili Bilgi Erişimi Erişim Yöntemi=Sertifika Yetkilisi Yayımcısı (1.3.6.1.5.5.7.48.2) Diğer Ad: URL=http://depo.kamusm.gov.tr/nes/kokshs.v6.crt

10.3. SON KULLANICI KURUMSAL ŞİFRELEME SERTİFİKA ŞABLONU

Alan	Değer
Sürüm	V3
Seri Numarası	64 bit rastsal sayı içeren tam sayı
İmza Algoritması	SHA-384 ile ECDSA {1 2 840 10045 4 3 3}
Sertifikayı Veren	CN = Kurumsal Şifreleme Sertifika Hizmet Sağlayıcısı - Sürüm 1 OU = Kamu Sertifikasyon Merkezi O = TÜBİTAK - BİLGEM L = Gebze - Kocaeli C = TR
Geçerlilik Başlangıcı	Sertifika geçerlilik başlangıcı
Geçerlilik Sonu	Sertifika geçerlilik sonu

Konu	CN = Kurum DETSİS adı Serial = Kurum DETSİS numarası C = TR
Açık anahtar	2048 bit RSA {1 2 840 113549 1 1 1}
Uzantılar	**Değer**
Yetkili Anahtarı Tanımlayıcısı	Kritik=Hayır; Anahtar Kimliği= ab 71 39 0b 21 74 35 cb 23 40 79 a7 3f d1 2c 21 73 94 a0 ab
Konu Anahtarı Tanımlayıcısı	Kritik=Hayır; Anahtar Kimliği= Sertifikanın içeriğindeki "subjectPublicKey" alanının "BIT STRING" olarak değerinin SHA-1 özet çıktısından oluşur.
Anahtar Kullanımı	**Kritik=Evet**; Anahtar Şifreleme
Temel Kısıtlar	Kritik=Hayır; Konu Türü=Son Varlık; Yol Uzunluğu Kısıtlaması=Yok
Sertifika İlkeleri	[1]Sertifika İlkesi: İlke Tanımlayıcısı=2.16.792.1.2.1.1.5.7.1.11 [1,1]İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimliği=CPS Niteleyici= http://depo.kamusm.gov.tr/ilke [1,2]İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimliği=Kullanıcı Uyarısı Niteleyici= Uyarı Metni=Bu sertifika, 2017/21 sayılı Başbakanlık Genelgesi kapsamında belirtilen kurumsal şifreleme sertifikasıdır.
Genişletilmiş Anahtar Kullanımı	Kurumsal Şifreleme Sertifikası (2.16.792.1.2.1.1.5.7.51.1)
SİL Dağıtım Noktaları	[1]SİL Dağıtım Noktası Dağıtım Noktası Adı: Tam Ad: URL=http://depo.kamusm.gov.tr/ksifreleme/ksifreleme.v1.crl

Yetkili Bilgi Erişimi	[1]Yetkili Bilgi Erişimi Erişim Yöntemi=Sertifika Yetkilisi Yayımcısı (1.3.6.1.5.5.7.48.2) Diğer Ad: URL=http://depo.kamusm.gov.tr/ksifreleme/ksifreleme.v1.crt [2]Yetkili Bilgi Erişimi Erişim Yöntemi=Çevrimiçi Sertifika Durum Protokolü (1.3.6.1.5.5.7.48.1) Diğer Ad: URL=http://ksifrelemeocspv1.kamusm.gov.tr/