TASNİF DIŞI

TÜBİTAK BİLGEM
KAMU SERTİFİKASYON MERKEZİ

ELEKTRONİK MALİ MÜHÜR SERTİFİKA İLKELERİ

Doküman Kodu
POL.01.06

Revizyon No
01

Revizyon Tarihi
28.10.2022

TASNİF DIŞI

ELEKTRONİK MALİ MÜHÜR SERTİFİKA İLKELERİ

REVİZYON GEÇMİŞİ		
Revizyon No	**Revizyon Nedeni**	**Revizyon Tarihi**
00	İlk yayın (YONG-001-011 kodu ve "Kamu SM Elektronik Mali Mühür Sertifika İlkeleri ve Sertifika Uygulama Esasları" ismi ile kabul edilmiştir.)	01.02.2010
01	Aynı doküman içerisinde yer alan; Kamu SM Elektronik Mali Mühür Sertifika İlkeleri ve Sertifika Uygulama Esasları iki ayrı doküman olacak şekilde düzenlenerek kodu ve şablonu güncellenmiştir. Doküman genelinde düzenlemeler yapılarak, web sitesi adresleri yeni altkök sertifikasına göre düzenlenmiştir.	28.10.2022

İÇİNDEKİLER

1. Giriş

Bu doküman, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu'na (TÜBİTAK) bağlı Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM) tarafından oluşturulan Kamu Sertifikasyon Merkezi'nin (Kamu SM) Türkiye Cumhuriyeti Devleti bünyesinde ticaret yapan kurum/kuruluş/tüzel/gerçek kişilere Elektronik Mali Mühür Sertifikası sağlayıcılığı konusundaki işlevleri sırasında uyulması gereken kuralları ve çalışma ilkelerini tanımlayan Sertifika İlkeleri (Sİ) dokümanıdır.

19 Ekim 2019 tarihli 509 Sıra No'lu Vergi Usul Kanunu Genel Tebliği ile TÜBİTAK bünyesindeki Kamu Sertifikasyon Merkezi (Kamu SM) belirtilen tanıma uygun olarak Elektronik Mali Mühür Sertifikası hizmeti sağlamaktadır.

Kamu SM Sİ dokümanı Elektronik Mali Mühür Sertifikası hizmeti verilirken ESHS'nin kendisine özel işlevsel ortamından bağımsız olarak sertifikaların başvuru, üretim, dağıtım, yenileme, iptal etme ile ilgili süreçler içindeki işlemlerinin hangi genel ilkeler doğrultusunda gerçekleştirildiğini, Açık Anahtar Altyapısı'nı (Public Key Infrastructure-PKI) oluşturan ve kullanan tüm bileşenlere uygulanan yönetim kurallarını tanımlayan üst düzey bir dokümandır.

Kamu SM, Sİ'de tanımlanan gerekleri nasıl karşıladığını anlatan Sertifika Uygulama Esasları (SUE) dokümanını hazırlar ve SUE dokümanına bağlı kalarak çalışır. Sİ dokümanı sertifika yönetim işlemleri ile ilgili olarak "ne" yapılacağını tanımlarken, SUE dokümanı bunun "nasıl" yapılacağını tanımlar.

1.1. Genel Bakış

Bu doküman, Elektronik Mali Mühür Sertifikalarının üretim ve yönetim ilkelerinin, sertifika yönetimi ile ilgili tüm kural ve usullerin en üst düzeyde tanımlandığı bir dokümandır. Kamu SM'den sertifika talebinde bulunan kullanıcılar bu dokümanda belirtilen şartları kabul etmiş sayılırlar.

Kamu SM açık anahtar altyapısı mimarisi içinde, en üst seviyede bir Kurumsal Kök Sertifika Hizmet Sağlayıcısı (Kurumsal Kök SHS) ile buna bağlı olarak çalışan Mali Mühür Elektronik Sertifika Hizmet Sağlayıcısı (Mali Mühür ESHS) bulunur.

Kurumsal Kök SHS son kullanıcılar için sertifika üretmeyip, yürüttükleri görevler açısından özel niteliği haiz kamu kurum ve kuruluşları ile dileyen gerçek ve tüzel kişilerin kuracakları Elektronik Sertifika Hizmet Sağlayıcıları'na kök, köprü veya çapraz sertifika hizmeti verir.

Mali Mühür ESHS ve Kamu SM'den kök sertifika hizmeti alan kamu kuruluşları veya özel kuruluşlar, Kurumsal Kök SHS'nin elektronik imzasını taşıyan sertifikaya sahiptir.

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

1.2. Doküman Adı ve Tanımı

Doküman Adı: Kamu SM Elektronik Mali Mühür Sertifika İlkeleri

Doküman Sürüm Numarası: 01

Yayın Tarihi: 28.10.2022

Nesne Tanımlama Numarası: 2.16.792.1.2.1.1.5.7.4.1

1.3. Sistem Bileşenleri

Kamu SM açık anahtar altyapısını oluşturan sistem bileşenleri aşağıda tanımlanmıştır.

1.3.1. Elektronik Sertifika Hizmet Sağlayıcı

Temel görevi sertifika ve iptal durum kayıtlarını üretip kendisine ait özel anahtarıyla imzalamak olan ESHS'ler, sertifika başvurusunda bulunanların kayıt ve kimlik doğrulama işlemleri ile Elektronik Mali Mühür Sertifikası askı, iptal etme ve iptal olmuş sertifika bilgilerini tüm taraflara duyurma süreçlerini mevzuatta belirtilen şartlara uygun olarak yerine getirmekle yükümlüdür.

Kamu SM, Mali Mühür Elektronik Sertifika Hizmet Sağlayıcısı (Mali Mühür ESHS) olarak gerçek, tüzel kişiler ile kurum, kuruluş ve işletmelere Elektronik Mali Mühür Sertifikası hizmeti sağlamaktadır.

1.3.2. Kayıt Birimleri

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

1.3.3. Sertifika Sahipleri

Sertifika sahipleri, elektronik sertifikanın içeriğinde adı bulunan ve sertifikasını Kamu SM sertifika ilkelerine ve uygulama esaslarına uygun olarak kullanmakla yükümlü olan gerçek kişilerdir.

1.3.4. Üçüncü Kişiler

Üçüncü kişiler, sertifikaların içindeki kimlik ve açık anahtar arasındaki bağın doğruluğuna güvenerek sertifikaları kabul eden ve işlem yapan kişilerdir.

1.3.5. Diğer Bileşenler

1.3.5.1. Kurum

Kamu SM'den Mali Mühür Sertifikası talep eden, Gelir İdaresi Başkanlığı'nda kaydı bulunan Mali Mühür Sertifikası almaya yetkisi olan gerçek, tüzel kişiler ile kurum, kuruluş ve işletmelerdir.

1.3.5.2. Elektronik Mali Mühür Sertifikası Sorumlusu

Sertifika başvurusunda bulunan kurum/kuruluş/tüzel kişi tarafından yetkilendirilen ve Elektronik Mali Mühür Sertifikası başvurusu sırasında gerekli bilgileri Kamu SM'ye ileten, sertifika yönetim süreçlerinde Kamu SM ile iletişim içinde olan kişi/kişilerdir.

1.4. Sertifika Kullanımı

1.4.1. Uygun Olan Sertifika Kullanımı

Elektronik Mali Mühür Sertifikası, kurum/kuruluş/tüzel kişi/ gerçek kişiler tarafından elektronik belge olarak oluşturulacak fatura ve diğer yasal belgelerin bütünlüğünün, kaynağının ve içeriğinin garanti altına alınması, elektronik ortamda muhataplarına iletilmesi ve elektronik ortamda saklanması sırasında güvenliğinin ve gizliliğinin sağlanması amacıyla 509 Sıra No'lu Vergi Usul Kanunu Genel Tebliği'ne uygun olarak kullanılmalıdır.

1.4.2. Sertifika Kullanımının Sınırları

Elektronik Mali Mühür Sertifikası Bölüm 1.4.1'de belirtilen amaçlar dışında kullanılamaz. Belirtilen kapsam dışında kullanımdan doğan zararlardan Kamu SM sorumlu tutulamaz.

1.5. İlkelerin Yönetimi

1.5.1. Doküman Yönetimi

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

1.5.2. İletişim Bilgileri

Bu Sİ 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 : https://kamusm.bilgem.tubitak.gov.tr

Kamu SM, Sİ dokümanını herkesin erişimine açık bulunan aşağıdaki internet adreslerinden yayımlar:

- http://depo.kamusm.gov.tr/ilke/
- https://kamusm.bilgem.tubitak.gov.tr/depo/ilke_ve_uygulama_esaslari/guncel_ilke_ve_uygulama_esaslari.jsp

1.5.3. Sertifika Uygulama Esaslarının İlkelere Uygunluğunu Belirleyen Kişi

Bu Sİ dokümanına uygun olarak yazılmış olan SUE dokümanlarının uygunluğu, Kamu SM yönetimi ve yönetim tarafından yetki verilen kişiler tarafından belirlenir.

1.5.4. Sertifika Uygulama Esasları Onay Prosedürleri

Bu Sİ dokümanına uygun olarak oluşturulan 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 web sunucular, 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.

Elektronik Sertifika Hizmet Sağlayıcısı: Elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişiler.

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

Elektronik Mali Mühür Sertifikası Sorumlusu: Kurum/Kuruluş/Tüzel Kişilerin başvuru sırasında başvuru formu ile Kamu SM'ye bildirdiği ve Elektronik Mali Mühür Sertifikası ile ilgili süreçlerde kurumu temsil eden yetkili kişi.

Elektronik Sertifika(lar): Sertifika sahibinin, elektronik mali mühür doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kayıttır (MÜS, GÜS ve Güvenli Mali Sertifika).

Güvenlik Hizmetleri Sertifikası (GÜS): Sertifika sahibinin Vergi Kimlik Numarası/TCKN ve unvan bilgilerini içeren, e-fatura ve ilgili mevzuatla izin verilen diğer belgeleri şifreleyen şifreleme sertifikası.

Mali Mühür Sertifikası (MÜS): Sertifika sahibinin Vergi Kimlik Numarası/TCKN ve unvan bilgilerini içeren, e-fatura ve ilgili mevzuatla izin verilen diğer belgeleri mühürleyen imzalama sertifikası.

Güvenli Mali Sertifika: İşletici Kuruluş bu sertifikaya bağlı bir alt sertifika olarak; sistemini çalıştırdığı her bir uç nokta (web veya değil) güvenli mali uygulama yazılımı için, hizmet verilen mükellefe ait vergi kimlik numarası ile eşlenik, belirli süreli tekil bir sertifika üretir.

Elektronik Mali Mühür Sertifikası: Elektronik belge olarak oluşturulacak fatura ve diğer yasal belgelerin bütünlüğünün, kaynağının ve içeriğinin garanti altına alınması için kullanılacak elektronik sertifikadır. Kurum/Kuruluş/Tüzel/Gerçek Kişilerin GİB ile elektronik ortamdaki belge ve bilgi paylaşımında kimliklerini güvenli bir şekilde tanımlamak ve doğrulamak amacıyla kullanılan elektronik sertifikadır.

Gelir İdaresi Başkanlığı (GİB): Devlet gelirleri politikasını uygulayan, vergiler ile diğer gelirleri tahsil eden, mükelleflerin vergiye uyumunu kolaylaştıran Türkiye Cumhuriyeti Hazine ve Maliye Bakanlığına bağlı bir devlet kurumudur.

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

Elektronik Mali Mühür Oluşturma Aracı: Kurum/Kuruluş/Tüzel/Gerçek Kişilere ait imza oluşturma verisi ve sertifikanın içinde bulunduğu akıllı kart ya da benzeri taşınabilir güvenli cihaz.

Elektronik Mali Mühür Oluşturma Aracı Erişim Verisi: Kurum/Kuruluş/Tüzel/Gerçek Kişilere ait imza oluşturma verisine erişimin kontrolünü sağlayan PIN ve PUK bilgisi.

Elektronik Mali Mühür Oluşturma Aracı Okuyucusu: Elektronik mali mühür oluşturma aracının içerisindeki bilgilere erişimi sağlayan donanım aracıdır (akıllı kart okuyucusu vb).

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.

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

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

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

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

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

DSA (Digital Signature Algorithm): Sayısal İmza Algoritması

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

EAL (Evaluation Assurance Level): Değerlendirme Garanti Düzeyi

EC: Eliptik Eğri 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

GİA: Güvenli İletişim Anahtarı

GİB: Gelir İdaresi Başkanlığı

GÜS: Güvenlik Hizmetleri Sertifikası

HSM: Donanımsal Güvenlik Modülü (Hardware Security Module)

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

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

ITU (International Telecommunication Union): Uluslararası Telekomünikasyon Birliği

Kamu SM: Kamu Sertifikasyon Merkezi

LDAP (Lightweight Directory Access Protocol): Dizin Erişim Protokolü

MERSİS: Merkezi Sicil Kayıt Sistemi

MM ESHS: Mali Mühür Elektronik Sertifika Hizmet Sağlayıcısı

MÜS: Mali Mühür Sertifikası

PKI (Public Key Infrastructure): Açık Anahtarlı Altyapılar

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

2.1. Bilgi Depoları

ESHS, sistem bileşenleri ile paylaştığı bilgileri bilgi depoları üzerinden yayımlar. Bilgi deposu, Kamu SM'nin ürettiği sertifikaları, iptal durum kayıtlarını, Sİ ve SUE gibi ilgili dokümanları sertifika sahiplerinin ve üçüncü kişilerin ulaşabileceği şekilde kesintisiz, güvenli ve ücretsiz olarak yayımladığı ortamdır.

https://kamusm.bilgem.tubitak.gov.tr internet adresi üzerinden yayımlanan Bilgi Deposu'nda sertifika sahiplerine imzalatılan başvuru formu ve taahhütnameler, 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 Alt kök SHS Sertifikaları
- Kamu SM'ye ait geçmişte oluşturulmuş Kök SHS ve Alt kök 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
- Kullanıcı test setifikaları

2.3. Yayım Sıklığı ve Zamanı

ESHS'nin kendisine ait sertifikalar, ESHS'nin hizmet süresi boyunca kesintisiz olarak yayımlanır. ESHS'nin kendisine ait sertifikaların güncellenmesi durumunda, yenilenen sertifikalar güncelleme yapılmasını müteakip derhal yayımlanır.

Sİ/SUE dokümanları ve sertifika yönetim işlemleri ile ilgili bilgilendirmenin yapıldığı dokümanlar güncellendikten sonra en kısa zamanda yayımlanır.

İptal durum kayıtlarının yayımlanma sıklığı, SUE Bölüm 4.9.7 ve 4.9.9'da anlatıldığı şekilde uygulanır.

2.4. Erişim Kontrolleri

ESHS bilgi deposuna erişim herkese açıktır.

ESHS, bilgi deposunun kesintisiz olarak erişilebilirliğini sağlamak için gerekli önlemleri almak, bilgi deposunda tutulan bilgilerin doğruluğunu ve güncelliğini sağlamakla yükümlüdür.

3. Kimlik Belirleme ve Doğrulama

Elektronik Mali Mühür Sertifikası kurum kimlik tanımlama ve doğrulama yöntemleri ile Elektronik Mali Mühür Sertifikası içinde yazılan kurum bilgileri bu bölümde anlatılmıştır.

3.1. İsimlendirme

3.1.1. İsim Alanı Tipleri

Elektronik Mali Mühür Sertifikalarında Kamu SM ve sertifika sahiplerine ait isim/unvan bilgilerinin belirtildiği DN [Distinguished Name (Ayırt edici isim)] alanı içinde "ITU X.500" biçiminin desteklediği isim tipleri kullanılır.

3.1.2. Kimlik Bilgilerinin Teşhise Elverişli Olması

Sertifikalar üzerinde yer alan kimlik bilgileri kurum/kuruluş/tüzel/gerçek kişileri tanımlayacak niteliktedir.

3.1.3. Sertifika Sahibinin Takma İsim veya Lakap Kullanması

Sertifika içeriğinde takma isim veya lakap kullanılmasına izin verilmez.

3.1.4. Farklı İsim Alanı Tiplerinin Yorumlanması

Sertifikalar içinde ITU X.500 biçimi dışında isim alanı tipi kullanılmaz.

3.1.5. Kimlik Bilgilerinin Tekilliği

Kamu SM tarafından oluşturulan sertifikaların içeriğindeki kimlik bilgileri kurum/kuruluş/tüzel/gerçek kişiler için ayırt edici niteliktedir. Elektronik Mali Mühür Sertifikalarının isim alanı içinde benzersiz bir sayı olduğu kabul edilen sertifika sahibi kuruma ait Vergi Kimlik Numarası (VKN) numarası da yer alır.

3.1.6. Markanın Tanınması, Doğrulanması ve Rolü

Düzenlenmesine gerek duyulmamıştır.

3.2. İlk Kimlik Belirleme

Kamu SM Elektronik Mali Mühür Sertifika hizmetlerinden faydalanmak için ilk defa başvuruda bulunulduğunda ilgili kurum/kuruluş/tüzel/gerçek kişilerin doğrulanabilmesi için aşağıda tanımlanan yöntemler uygulanır.

3.2.1. Özel Anahtar Sahipliğinin Kanıtlanması

Sertifika sahibine ait açık ve özel anahtar, kurum/kuruluş/tüzel/gerçek kişi talebi üzerine Kamu SM tarafından üretilerek Güvenli Donanım Modülü (HSM)'ne veya akıllı karta yüklenir ve kurye vasıtasıyla teslim edilir. Sertifika sorumlusu tarafından Elektronik Mali Mühür Sertifikasının teslim alındığı teyit edilir. Ek olarak, HSM'ye yüklenmesi talep edilen sertifikalar için teslim tutanağı ile teyit işlemi yapılır.

3.2.2. Kurumsal Kimliğin Belirlenmesi

Elektronik Mali Mühür Sertifikası başvurusunda bulunan kurum/kuruluş/tüzel kişiler, talep edilen bilgileri Kamu SM tarafından sunulan başvuru yöntemleriyle Kamu SM'ye bildirir. Kamu SM, kurum/kuruluş/tüzel kişi tarafından iletilen bilgilere istinaden kurum kimliğini belirler. Kurumların vergi kimlik numaraları portal başvurusu sırasında MERSİS üzerinden kontrol edilir.

3.2.3. Kişisel Kimliğin Belirlenmesi

Elektronik Mali Mühür Sertifikası başvurusunda bulunan gerçek kişiler, talep edilen bilgileri Kamu SM tarafından sunulan başvuru yöntemleriyle Kamu SM'ye bildirir. Kamu SM, gerçek kişi tarafından iletilen bilgileri Kimlik Paylaşım Sistemi üzerinden doğrulayarak kişinin kimliğini belirler.

3.2.4. Doğrulanmayan Sertifika Sahibi Bilgileri

Portal üzerinden bildirilen ve GİB tarafından bildirilen kurum imza yetkilisine ait kişisel bilgilerin doğruluğu sertifika sahibi sorumluluğundadır. Herhangi bir ek doğrulama yapılmaz.

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 belirtildiği gibi yapılır.

3.3.1. Olağan Sertifika Yenileme İsteğinde Kimlik Doğrulama

Bölüm 3.2'de belirtildiği gibi yapılır.

3.3.2. İptal Sonrası Yeni Sertifika Talebinde Kimlik Doğrulama

Bölüm 3.2'de belirtildiği gibi yapılır.

3.4. Sertifika İptal İsteğinde Kimlik Doğrulama

Sertifika sahibi kurum/kuruluş/tüzel/gerçek kişiler Kamu SM resmi web sitesinde yer alan Online İşlemlere kimlik doğrulamasıyla giriş yaparak iptal işlemini gerçekleştirebilir. Online İşlemler adresine erişilememesi durumunda bilgi@kamusm.gov.tr adresine mail atarak iptal talebinde bulunabilir. Mail üzerinden gelen iptal taleplerinde kimlik doğrulaması, sertifika sorumlusunun iletişim bilgileri kullanılarak irtibata geçilmesi yolu ile yapılır.

4. Sertifika Yaşam Döngüsü İşlevsel Gereklilikleri

Bu bölümde, sertifika yaşam döngüsü içinde sertifika yönetimiyle ilgili gerçekleştirilen işlemler ile sertifika sahipleri, Kamu SM ve üçüncü kişilerin bu işlemlerdeki rol ve sorumlulukları anlatılmıştır.

4.1. Sertifika Başvurusu

4.1.1. Sertifika Başvurusunu Kimlerin Yapabildiği

GİB tarafından Elektronik Mali Mühür Sertifikası alma yetkisi olduğu belirtilen kurum/kuruluş/tüzel/gerçek kişiler Elektronik Mali Mühür Sertifikası başvurusunda bulunabilirler.

4.1.2. Kayıt İşlemleri ve Sorumluluklar

Elektronik Mali Mühür Sertifikası başvurusu, kurum/kuruluş/tüzel/gerçek kişiler tarafından Kamu SM'ye yapılır. Kurum/kuruluş/tüzel/gerçek kişilerin Kamu SM'den alacağı sertifika hizmetlerinin şartları Kamu SM'nin internet üzerinden yayımladığı ilgili yönergeler, Sİ ve SUE dokümanları doğrultusunda belirlenir.

Kurum/kuruluş/tüzel/gerçek kişiler başvuru sırasında Kamu SM'ye doğru bilgi beyan etmekle sorumludur. Başvuru sahibi, 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, Elektronik Mali Mühür Sertifikası içinde yer alacak bilgileri kontrol eder ve kendisine beyan edilen bilgilerin gizliliğini sağlamak için gerekli tedbirleri alır.

Kayıt işlemleri ve sorumluluklar ile ilgili detaylı bilgi SUE Bölüm 4.1.2'de yer almaktadır.

4.2. Sertifika Başvurusunun İşlenmesi

4.2.1. Kimlik Tanımlama ve Doğrulama İşlevlerinin Yerine Getirilmesi

Başvuru sırasında kurum/kuruluş/tüzel/gerçek kişilerden veya GİB'den gelen belgelerin Kamu SM tarafından incelenmesi sonucunda kimlik tanımlama ve doğrulama işlevleri yerine getirilir.

4.2.2. Sertifika Başvurusunun Kabul veya Reddi

Kamu SM, MERSİS sorgusundan geçen ya da GİB üzerinden liste ile gelen kurum/kuruluş/tüzel/gerçek kişilerin başvurusunu kabul eder, MERSİS sorgusundan geçemeyen tarafların başvurusunu reddeder.

4.2.3. Sertifika Başvurusunun İşlenme Zamanı

Başvuru ve ödeme işlemlerinin tamamlanmasının ardından sertifika başvurusu işleme alınır ve sonuçlandırılır.

4.3. Sertifikanın Oluşturulması

4.3.1. Sertifika Oluşturulmasında ESHS'nin İşlevleri

Kamu SM tarafından değerlendirilen ve uygun bulunan sertifika başvuruları için sertifika üretim aşamasına geçilir. Bu işlemin nasıl yapılacağı SUE'de anlatılır.

4.3.2. Sertifika Oluşturulması ile İlgili Sertifika Sahibinin Bilgilendirilmesi

Sertifikla akıllı karta yüklenmeden hemen önce sertifika sorumlusuna sertifikanın üretim aşamasında olduğuna dair bilgilendirme gönderilir.

HSM cihazına sertifika yükleme işlemi, sertifika sorumlusu gözetiminde gerçekleştirilir. İşlem sonrasında teslim tutanağı imzalanır ve Elektronik Mali Mühür Sertifikasının oluşturulduğu konusunda bilgilendirilmiş olur.

4.4. Sertifikanın Kabulü

4.4.1. Sertifikanın Kabul Koşulu

Elektronik Mali Mühür Sertifikası akıllı kart veya HSM cihazı içerisinde kullanılabilmektedir. Sertifikanın kullanılacağı cihaz seçimine göre SUE Bölüm 4.4.1'de belirtilen kabul koşulu uygulanmaktadır.

4.4.2. Sertifikanın ESHS Tarafından Yayımlanması

Elektronik Mali Mühür Sertifikaları, Kamu SM tarafından yayımlanmaz.

4.4.3. Sertifikanın Oluşturulmasının Diğer Taraflara Duyurulması

Sertifika oluşturulması ile ilgili bilgiler oluşturulan rapor sistemi üzerinden GİB'e iletilir.

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.

4.5.2. Üçüncü Kişilerin Sertifika ve Açık Anahtarı Kullanımı

Sertifikaların içinde yer alan elektronik mali mühür imza doğrulama verileri, üçüncü taraflarca doğrulama amacıyla kullanılır. Üçüncü taraflar, güvenecekleri sertifikanın ve sertifikayı oluşturan ESHS'nin sertifikasının geçerliliğini kontrol etmekle, sertifika "Anahtar kullanım" alanında belirtilen amaçlar doğrultusunda kullanıldığını doğrulamakla ve bu SUE'de belirtilen kullanım koşullarına uymakla yükümlüdürler.

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.

4.7.1. Sertifika Yenileme Koşulları

Sertifika yenileme işlemi SUE Bölüm 4.7.1'de belirtilen durumlarda yapılmaktadır.

4.7.2. Sertifika Yenileme Başvurusunu Kimlerin Yapabildiği

Bölüm 4.1.1'de tanımlanmaktadır.

4.7.3. Sertifika Yenileme Başvurusunun İşlenmesi

Bölüm 4.2'de tanımlanmaktadır.

4.7.4. Sertifika Yenileme ile İlgili Sertifika Sahibinin Bilgilendirilmesi

Bölüm 4.3.2'de tanımlanmaktadır.

4.7.5. Sertifika Yenileme Sonrası Kabul Koşulu

Bölüm 4.4.1'de tanımlanmaktadır.

4.7.6. Sertifika Yenileme Sonrası Sertifikanın Yayımlanması

Bölüm 4.4.2'de tanımlanmaktadır.

4.7.7. Sertifika Yenilemenin Diğer Taraflara Duyurulması

Bölüm 4.4.3'de tanımlanmaktadır.

4.8. Sertifikada Bilgi Değişikliği

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

Kamu SM, sertifikada bilgi değişikliği gerçekleştirmez. Sertifikada bilgi değişikliği gerekli ise anahtar yenileme ile yeni bir sertifika üretilir.

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. Sertifikanın iptalini gerektiren durumlar SUE Bölüm 4.9.1'de verilmiştir.

4.9.2. Sertifika İptal Başvurusunu Kimler Yapabilir

Sertifika iptal başvurusu, sertifika sahibi kurum/kuruluş/tüzel/gerçek kişi veya sertifika sahibi kurum/kuruluş/tüzel kişi tarafından yetkilendirilmiş Elektronik Mali Mühür Sertifika Sorumlusu veya GİB tarafından yapılabilir.

4.9.3. Sertifika İptal Başvurusunun İşlenmesi

SUE Bölüm 4.9.3'te belirtildiği şekilde işletilir.

4.9.4. İptal İsteği Ertelenme Süresi

Böyle bir süre öngörülmemiştir.

4.9.5. İptal İsteğinin İşlenme Süresi

Geçerli bir sertifika iptal talebi geldikten sonra Kamu SM, sertifika iptal talebini derhal işleme alır.

4.9.6. Üçüncü Kişilerin Sertifika İptal Durumunu Kontrol Gerekliliği

Kamu SM, iptal durum kayıtlarını ücretsiz olarak kamuya açar. Sertifika iptal durum kayıtlarına, dileyen herkes kimlik doğrulaması yapılmaksızın erişebilir. Kamu SM, iptal durum kayıtlarına erişimin sürekliliğini sağlar. Üçüncü kişilerin yapması gereken geçerlilik kontrolleri SUE 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 Elektronik Mali Mühür Sertifikası iptali olmasa dahi SİL 4 (dört) saatte bir güncellenir. Eski SİL dosyaları geçerlilik süresinin sonuna kadar geçerliliğini korur.

Kamu SM sertifikaları için yayımlanan 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 üretildiğini andan itibaren mümkün olan en kısa sürede yayımlanır.

4.9.9. Çevrim İçi Sertifika İptal Durum Kaydı Hizmeti

Kamu SM, ÇİSDUP (Çevrim İçi Sertifika Durum Protokolü) hizmeti sağlar. ÇİSDUP Yanıtlayıcı'dan yayımlanan iptal durum kaydı Kamu SM'ye ait olduğu duyurulan imza oluşturma verisiyle imzalanır.

4.9.10. Çevrim İçi Sertifika İptal Durum Kaydı Kontrol Gereksinimi

Çevrim içi sertifika iptal durum kayıtları, iptal bilgisinin daha hızlı ve sisteme daha az yük getirecek biçimde duyurulmasını sağlayabilir. Bu nedenle, üçüncü tarafların teknolojik altyapıları el verdiği ölçüde ÇİSDUP kullanmaları önerilir.

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 sahibine ait özel anahtarın güvenliğini yitirmesi durumunda sertifikanın iptali sağlanır. Sertifika iptali dışında herhangi bir işlem uygulanmamaktadır.

4.9.13. Sertifikanın Askıya Alındığı Durumlar

Elektronik Mali Mühür Sertifikası, üretim veya kullanım aşamasında geçici iptal durumunu sağlamak amacıyla askıya alınabilir. Sertifikanın askıya alındığı durumlar SUE Bölüm 4.9.13'te verilmiştir.

4.9.14. Sertifika Askıya Alma Başvurusunu Kimlerin Yapabildiği

Askıya alma başvurusu sertifika sahibi tarafından yapılabilir.

4.9.15. Sertifika Askıya Alma Başvurusunun İşlenmesi

Elektronik Mali Mühür Sertifikası askı başvurusu, Kamu SM web sitesinde yer alan Online İşlemler menüsünden yapılır. Askıya alma başvurusunun işlenme yöntemi, SUE Bölüm 4.9.3'de belirtilen iptal başvurusu işlenme yöntemleri ile aynı biçimde ve SUE Bölüm 4.9.15'de belirtiği şekilde yapılabilir.

4.9.16. Askıda Kalma Süresi

Askıya alınan sertifikalar, en az bir kere SİL dosyasına girmeden askıdan indirilemez.

4.10. Sertifika Durum Servisleri

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

4.10.1. İşletimsel Özellikleri

SİL dosyası Kamu SM'ye ait bilgi deposunda güncel haliyle tutulur. SİL dosyasına erişmek isteyen üçüncü kişiler, SUE'de belirtilen erişim adreslerini kullanarak dosyayı kendi sistemlerine yüklerler. Güncel SİL dosyasına erişmek isteyen üçüncü kişilerin, her sertifika iptal durum kaydını öğrenmek istediklerinde, SİL dosyasını Kamu SM bilgi deposundan kendi sistemlerine indirerek, gerekli kontrolleri yapmaları önerilir.

ÇİSDUP servisinden sertifika iptal durumunun öğrenilebilmesi için, ilgili sertifika veya sertifikaları tanımlayan bilgiler ÇİSDUP İstemci tarafından Kamu SM ÇİSDUP Yanıtlayıcı'ya gönderilir. ÇİSDUP Yanıtlayıcı, sertifika veya sertifikaların iptal olup olmadığını anlık olarak istemciye bildirir.

4.10.2. Servisin Erişilebilirliği

SİL ve ÇİSDUP servislerinin verildiği sistemlere erişim, Kamu SM tarafından kesintisiz olarak sağlanır. Kamu SM bu konuda gereken tüm tedbirleri alır, oluşan teknik problemleri en kısa zamanda giderir. Ancak, buna rağmen erişimin bir süreliğine kesilmiş olması durumunda üçüncü kişilerin, problem giderilinceye kadar sertifika iptal durum kaydını kontrol etmeleri gereken işlemlerini durdurması önerilir. Üçüncü kişilerin, erişimin kesilmesi sebebiyle iptal durum kaydını 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

Sertifika sahipliği; sertifikanın kullanım süresinin sona ermesi, sertifikanın iptal edilmesi, Kamu SM'nin sertifika hizmetlerini sonlandırması ile sona erer.

4.12. Anahtar Yeniden Üretme

Sertifika sahiplerine ait anahtarların yeniden üretilmesi veya yedeklenmesi işlemi uygulanmaz.

5. Yönetim, İşlemsel ve Fiziksel Kontroller

Bu bölümde, Kamu SM tarafından sertifika hizmeti verilirken yerine getirilmesi gereken teknik olmayan kontroller anlatılmıştır.

5.1. Fiziksel Güvenlik Denetimleri

Kamu SM'ye ait sistemlerin kurulu olduğu cihazlara yetkisiz kişilerce erişim engellenir; hırsızlık, kaybolma gibi tehlikelere karşı gerekli önlemler alınır. Bunun için, sistemin kurulu olduğu binalar belirli güvenlik ihtiyaçlarını karşılar.

5.1.1. Tesis Yeri ve İnşaatı

Kamu SM'ye ait yazılım ve donanım modüllerinin bulunduğu binalar, konum olarak güvenli yerlere inşa edilir. Bina, yüksek güvenlik gerektiren işlerin gerçekleştirilmesine imkan verecek ölçüde dışarıdan gelebilecek saldırılara karşı korumalıdır. Bina içinde, yazılım ve donanım modüllerinin yerleştirilmesi için kilitli ve giriş kontrollü odalar bulunur.

5.1.2. Fiziksel Erişim

Binaya giriş, güvenlik görevlileri ve gerekli güvenlik donanımının sağladığı fiziksel kontrollerle yapılır. Kamu SM işlemlerinin gerçekleştirildiği yazılım ve donanım modülleri ile her türlü elektronik veya kağıt ortamda tutulan bilgilerin bulunduğu odalara, yetkisiz kişilerin erişiminin engellenmesi için gerekli önlemler alınır.

5.1.3. Güç Kaynağı ve Havalandırma

Kamu SM işlemlerinin sürekliliği için sistem, kesintisiz güç kaynağı ile beslenir.

Bina gerekli havalandırma sistemi ile donatılır.

5.1.4. Su Baskınları

Kamu SM'ye ait yazılım ve donanım modüllerinin bulunduğu ortamlarda, su baskınlarından en az zarar görecek şekilde tedbirler alınır.

5.1.5. Yangın Önleme ve Korunma

Kamu SM'ye ait yazılım ve donanım modüllerinin bulunduğu ortamlarda, yangını önleyen ve yangından korunmayı sağlayan tedbirler alınır.

5.1.6. Saklama ve Yedekleme Ortamlarının Korunması

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

5.1.7. Atıkların Yok Edilmesi

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

5.1.8. Farklı Mekanlarda Yedekleme

Kamu SM, sisteminin sürekliliğini sağlayabilmek amacıyla gerekli gördüğü bileşenleri, farklı bir fiziksel mekanda güvenli kasalarda saklar. Yedek sistemin bulunduğu mekan, asıl sistemin sağladığı tüm güvenlik ve işlevsellik şartlarını sağlar.

5.2. Prosedürsel Kontroller

5.2.1. Güvenilir Roller

Sertifika ve bilgi sistemleri süreçlerinde kritik görevler üstlenen roller SUE dokümanında detaylandırılır.

5.2.2. Her İşlem İçin Gereken Kişi Sayısı

Kamu SM, işlemin gereklerine bağlı olarak, bir işlemin gerçekleştirilebilmesi için birden fazla kişinin aynı anda hazır bulunmasını tanımlayabilir.

5.2.3. Kimlik Doğrulama ve Yetkilendirme

Kamu SM çalışanlarının, sisteme erişimi ve işlemleri sırasında kimlikleri ve erişim yetkileri doğrulanır.

5.2.4. Görevlerin Ayrılmasını Gerektiren Roller

Kamu SM içinde, aynı kişinin birden fazla görevde bulunmasını engelleyecek sınırlamalar getirilebilir.

5.3. Personel Güvenlik Kontrolleri

5.3.1. Kişisel Geçmiş, Deneyim ve Nitelik Gerekleri

Kamu SM bilgi güvenliği, elektronik imza teknolojileri ve veri tabanı yönetimi alanlarında yeteri kadar teknik personel istihdam eder. Teknik personel, konusunda yeterli mesleki deneyime sahip ya da ilgili alanlarda eğitim almış kişilerdir.

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, gerekli öğrenim şartlarını sağlayan kişilerden seçilir ve Kamu SM işleyişinde yaptığı işle ilgili görev ve sorumluluklarının anlatıldığı eğitimden geçirilir. Tüm personele, Kamu SM tarafından uygulanan güvenlik ilkelerinin ve bu dokümanda belirtilen sertifika yönetimiyle ilgili ilkelerin neler olduğunun anlatıldığı temel farkındalık eğitimi verilir.

5.3.4. Sürekli Eğitim Gerekleri ve Sıklığı

Kamu SM sisteminin işleyişinde yapılan her değişiklik personele, verilen eğitimlerle bildirilir. Yeni personelin işe başlamasında eğitimler tekrarlanır.

5.3.5. Görev Değişim Sıklığı ve Sırası

Düzenlenmesine gerek duyulmamıştır.

5.3.6. Yetkisiz Eylemlerin Cezalandırılması

Kamu SM personelinin mevzuata aykırı işlem yapması halinde ilgili mevzuat gereğince işlem yapılır.

5.3.7. Anlaşmalı Personel Gereksinimleri

Kamu SM, kendi personeli olmayıp anlaşmalı olarak çalıştırdığı kişilerin gerekli güvenirliği sağlaması için gereken kontrolleri yapar.

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 ve denetimi yapılmak istenen işlerin kayıtları tutulur. Denetimler sırasında gerekli görüldüğü takdirde bu kayıtlar görevliler tarafından incelenir.

5.4.1. Kaydedilen İşlemler

Sistem güvenliğiyle ilgili işlemler ile sertifika yaşam döngüsü içinde gerçekleştirilen işlemler için, en azından aşağıdaki kayıtlar tutulmalıdır:

- Sertifika başvurusu ve başvuru onay kayıtları
- Sertifika yenileme başvurusu ve başvuru onay kayıtları
- Sertifika askıya alma ve iptal başvurusu ile başvuru onay kayıtları
- Sertifika üretim kayıtları
- Sertifika iptal kayıtları
- Sertifika askıya alma ve askıdan indirme kayıtları
- SİL üretim kayıtları
- Tutulan tüm kayıtların zamanı
- Süreçlerin işleyişi sırasında yapılan işlemler
- İşlemi yapan personelin kimlik bilgisi
- SUE dokümanında belirtilen diğer işlemler

5.4.2. Kayıtların İncelenme Sıklığı

Tutulan kayıtlar, belirli zaman aralıklarıyla incelenir. İncelemeler, güvenlik açıklarını uygun sürede yakalayabilecek sıklıkta yapılır.

5.4.3. Kayıtların Saklanma Süresi

Kayıtlar, sistemin veri depolama kapasitesine göre, sistemde erişilebilir olarak tutulur. Ancak, yasalar gereğince daha uzun süre saklanması gereken kayıtlar arşivlenir. Arşivlenen kayıtlar ile ilgili bilgilendirme Bölüm 5.5'te yapılmıştır.

5.4.4. Kayıtların Korunması

Kayıtlar, izinsiz izlenmeyi, değiştirmeyi ve silinmeyi engelleyecek şekilde elektronik ve fiziksel olarak güvenli tutulur.

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. Kritik kayıtlar ayrı bir şehirde bulunan güvenli felaket kurtarma merkezlerine yedeklenmektedir.

5.4.6. Kayıtların Toplanması

Kayıtlar, elektronik olarak veya kağıt ortamda toplanır. Elektronik olarak toplanan kayıtlar, Kamu SM sisteminde tutulur; kağıt üzerindeki kayıtlar ise, ilgili Kamu SM çalışanı tarafından dosyalanır.

5.4.7. Kayda Sebebiyet Veren Tarafın Bilgilendirilmesi

Sistemde elektronik olarak yapılan sertifika başvurusunu onaylama, sertifikanın üretimi veya iptali gibi kritik işlemlerde kayda sebep olan taraf, kayıt hakkında bilgilendirilir.

5.4.8. Saldırıya Açıklığın Değerlendirilmesi

Denetim kayıtlarının tahrifata, silinmeye ve kaçağa karşı korunması ve izinsiz erişimin engellenmesi için, kayıtlarının bulunduğu sistemler üzerinde elektronik ve fiziksel olarak gerekli güvenlik tedbirleri alınır.

5.5. Kayıt Arşivleme

Elektronik ya da kağıt üzerinde tutulan kayıtlar ESHS tarafından arşivlenir.

5.5.1. Arşivlenen Kayıt Bilgileri

SUE Bölüm 5.4.1'de belirtilen kayıtlara ek olarak SUE Bölüm 5.5.1'de belirtilen sertifika başvurusu ve sertifika yaşam döngüsüyle ilgili elektronik ortamda ya da kağıt üzerinde tutulan belgeler arşivlenir.

5.5.2. Arşivlerin Tutulma Süresi

Arşivlenen bilgiler ve belgeler, Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik'te belirtilen süre boyunca saklanır.

5.5.3. Arşivlerin Korunması

Arşivlenen bilgi ve belgeler, izinsiz izlenmeyi, değiştirmeyi ve silinmeyi engelleyecek şekilde elektronik ve fiziksel olarak güvenli tutulur. Elektronik olarak tutulan arşivlerin, üzerinde kayıtlı bulunduğu elektronik ortamın bozulmasını önlemek için gerekli önlemler alınır. Kağıt üzerinde tutulan arşivler, her türlü yıpranma ve hasar görmeye karşı korunaklı ortamlarda tutulur.

5.5.4. Arşivlerin Yedeklenmesi

Kamu SM, ihtiyaç duyduğu durumlarda içeriğindeki bilginin güvenliğini bozmayacak şekilde arşivlerin yedeklerini alabilir. Yedeği alınan arşivler, orijinalleri ile aynı derecede güvenlik şartlarının sağlandığı ortamlarda tutulur.

5.5.5. Kayıtların Zaman Damgası Gereksinimleri

Kamu SM gerekli gördüğü kayıtlara zaman damgası ekleyebilir.

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. Aynı bilgiye ait birden fazla arşiv olması durumunda, arşivler kıyaslanarak doğruluğu kontrol edilir.

5.6. Anahtar Değişimi

Kamu SM'ye ait anahtarların ve sertifikaların, güvenlik sebeplerinden dolayı değiştirilmesi gerekebilir. Bu durumda eski anahtarlar, geçerlilik süresinin sonuna kadar kullanılabilir durumda saklanır. Kamu SM'nin Özel Anahtarın değişiminden itibaren, yeni üretilecek olan sertifikalar yeni özel anahtarıyla imzalanır. Ancak, eskiden üretilmiş olan sertifikaların doğrulanabilmesi için, eski açık anahtarının içinde bulunduğu Kamu SM'ye ait eski sertifikaların erişilebilirliğinin sağlanması gerekir.

5.7. Güvenliğin Yitirilmesi ve Arıza Durumlarında Yapılacaklar

5.7.1. Güvenilirliğin Yitirilmesi Durumunun Düzeltilmesi

Kamu SM, güvenliği tehlikeye düşürebilecek olayları en aza indiren ve herhangi bir felaket anında güvenliği en kısa zamanda yeniden sağlayan önlemleri alır.

5.7.2. Donanım, Yazılım veya Veri Bozulması

Kamu SM, hizmeti kesintiye uğratan yazılım veya donanım arızalarında, iptal durum kaydını yayımladığı servislere öncelik vermek şartıyla en kısa zamanda gerekli düzeltmeleri yaparak sistemi yeniden işler hale getirir. Kamu SM'ye ait kayıtların yitirilmesi halinde yedekleme sistemleri aracılığıyla, Kamu SM sistemi tekrar işler hale getirilir. Eğer tam olarak işler hale getirilemez veya kayıtların bazıları yeniden elde edilemez ise, bu durumdan etkilenebilecek olan bütün sertifika sahipleri ve kuruluşlar derhal bilgilendirilir. Gerekirse bazı sertifikalar iptal edilip, sertifika sahiplerine yeni sertifika üretilir.

5.7.3. Özel Anahtarın Gizliliğinin Kaybedilmesi

Kullanıcı sertifikalarını imzalayan Kamu SM, özel anahtarın çalınması, bozulması, erişilememesi gibi durumlarda, kendisine ait sertifikasını iptal eder. Bu durumu, iptal sebebi ile birlikte en hızlı şekilde internet üzerinden duyurur ve ilgili tarafları bilgilendirir. Duyurunun yapılacağı internet adresi SUE dokümanında belirtilir. Kamu SM, sertifikasının iptal sebebine bağlı olarak sertifika sahiplerinin durumdan ne şekilde etkileneceğini belirten açıklamayı da yapar. Kamu SM kendi sertifikasını, özel anahtarın güvenliği veya gizliliğinin tehlikeye düşmesi durumunda iptal etmişse, ilgili taraflara eski sertifikalara güvenilmemesi konusunda ihtarda bulunur.

Kamu SM için, yeni anahtar çiftleri oluşturularak yeni bir sertifika üretilir. Üretilen yeni sertifika, mevzuta uygun olarak ilgili taraflara iletilir. Eski özel anahtar ile imzalanan son kullanıcı sertifikaları iptal edilir ve en kısa sürede yenilenen ESHS özel anahtar kullanılarak yeniden sertifikalar üretilir ve dağıtılır.

Sertifika sahibine ait güvenli elektronik imza oluşturma aracının ve özel anahtarın güvenliğinden şüphe edildiğinde, sertifika askıya alma/iptal işlemleri yapılır.

5.7.4. Arıza Sonrası Yeniden Çalışırlık

Kamu SM, arıza sonrası çalışırlığın sağlanması için gerekli planları yapar ve önlemleri alır.

5.8. Sertifika Hizmetlerinin Sonlandırılması

Kamu SM Hizmetleri Sonlandırma Planı dokümanında tanımlanmıştır.

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. Elektronik Sertifika Hizmet Sağlayıcısı Anahtar Çiftinin Üretimi

Kamu SM'ye ait, sertifika imzalama amaçlı kullanılan 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 SUE Bölüm 6.2.1'de belirtilen standartlara uyar.

6.1.1.2. Sertifika Sahibi Anahtar Çiftinin Üretimi

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

Elektronik Mali Mühür Sertifikası HSM'ye yüklenecekse, sertifika sorumlusu gözetiminde Kamu SM yetkili personeli tarafından HSM içerisinde güvenli yazılım ve/veya donanım kullanılarak üretilir.

Sertifika sahibine ait özel anahtarın yedeği alınmaz, bir kopyası hiçbir şekilde sistemde tutulmaz. Sertifika sahibine ait özel anahtarın saklandığı akıllı kart veya HSM SUE 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, sertifika sorumlusu gözetiminde gerçekleştirilir ve işlem sonrası Teslim Tutanağı doldurularak kurum tarafından imzalanır.

6.1.3. Elektronik Sertifika Hizmet Sağlayıcısı'na Açık Anahtarın Ulaştırılması

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

Elektronik Mali Mühür Sertifikası akıllı karta yüklenecekse, Elektronik Mali Mühür 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 Kurumsal Kök SHS ve Mali Mühür ESHS sertifikaları internet ortamında tarafların erişimine hazır bulundurulur. Sertifikanın yayımlandığı ortamın izinsiz değiştirmeye ve silinmeye karşı güvenliği sağlanır.

6.1.5. Anahtar Uzunlukları

Kamu SM'ye ait kök ve alt köklerin RSA açık anahtar algoritması imza oluşturma anahtar çiftinin boyu en az 2048 bittir.

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

Kamu SM tarafından üretilen Elektronik Mali Mühür Sertifikaları, RSA imza oluşturma anahtar çiftlerinin boyu en az 2048 bittir.

6.1.6. Anahtar Üretim Parametreleri ve Kalitesinin Kontrolü

Anahtarların üretiminde, kriptografik açıdan gerekli güvenlik şartlarını sağlayan algoritma ve parametreler kullanılır. Anahtar üretme yöntemlerinin gerekli güvenlik şartlarını sağladığı, kriptografik testlerle ispatlanır.

6.1.7. Anahtar Kullanım Amaçları

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

Kamu SM kök anahtarı, alt kök sertifikasını ve SİL'i imzalamak için kullanılır. Kamu SM Elektronik Mali Mühür Sertifikalarının imzalanmasında kullanılan sertifika zinciri SUE dokümanında 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 modülün sahip olduğu güvenlik işlevleri SUE Bölüm 6.2.1'de açıklanmaktadır.

6.2.2. Özel Anahtara Birden Fazla Kişi Kontrolünde Erişim

Kamu SM'ye ait imza oluşturma verisinin bulunduğu odaya erişim aynı anda 2 (iki) yetkili personel 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 verileri, yetkisiz kişilerin erişimine kapalı, fiziksel ve elektronik olarak güvenli kriptografik donanım cihazı içinde yedeklenir. Özel anahtarın yedeklenmesi işlemi, birden fazla yetkili personelin ortak denetimi altında gerçekleştirilir.

Sertifika sahiplerine ait imza oluşturma verileri Kamu SM tarafından yedeklenmez.

6.2.5. Özel Anahtarın Arşivlenmesi

Kamu SM'ye ve sertifika sahiplerine ait imza oluşturma verileri arşivlenmez. Kamu SM'ye ait imza oluşturma verileri 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 personelin ortak denetimi altındadır. İmza oluşturma verisinin bulunduğu odaya giriş için, tanımlanan yetkililerin aynı anda hazır bulunması ve elektronik olarak kimliklerinin ve yetkilerinin doğrulanması gerekir.

İmza oluşturma verisi kriptografik modül içinde şifreli durumdayken erişime kapalıdır. Erişime açılması için erişimi sağlayan verinin modüle sunulması gerekir.

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 SUE 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 verilerinin aslı ve bütün yedekleri kullanım süresinin dolmasının ardından, bulunduğu sistemden uygun yöntemlerle geri dönüşsüz şekilde silinir. Özel anahtarın silinmesi, birden fazla yetkili personelin ortak denetimi altındadır.

Sertifika sahiplerine ait imza oluşturma verileri sadece sahibinde bulunduğundan yok edilmesi sahibinin sorumluluğundadır.

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 imza doğrulama verilerinin içinde bulunduğu sertifikalar yasa ve ilgili yönetmelikte belirtilen süre boyunca arşivlenir. Arşivde bulunduğu süre boyunca, sertifikaların veri bütünlüğünün sağlanması için gereken her türlü önlem alınır.

6.3.2. Özel ve Açık Anahtarların Kullanım Süreleri

Özel anahtarın kullanım süresi, Elektronik Mali Mühür Sertifikasının içeriğinde belirtilen kullanım süresi kadardır. Üretilen Elektronik Mali Mühür Sertifikalarının son kullanma tarihi, Mali Mühür ESHS Sertifikasının son kullanma tarihini aşamaz.

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

6.4. Erişim Denetim Verileri

Kamu SM çalışanlarının erişim denetim verileri erişim parolalarını, güvenli donanım araçları içindeki erişim denetimi sağlayan diğer verileri, biyometrik verileri içerir. Sertifika sahibine ait iki farklı erişim denetim verisi tanımlanmıştır. Bunlar, 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 sahibine ait erişim parolaları yetkisiz kişilerin erişimine kapalı, fiziksel ve elektronik olarak güvenli ortamlarda tahmin edilemez nitelikte ve rasgele üretilir.

6.4.2. Erişim Denetim Verilerinin Korunması

Kamu SM sistemi içinde kullanılan erişim denetim verileri yalnızca yetkili çalışanlar tarafından bilinir. Sertifika sahibine ait erişim parolaları sertifika sahibine güvenli yöntemlerle ulaştırılır. Erişim parolaları ilk kullanımda sertifika sahibi tarafından değiştirilir. Parolayı yetkisiz kişilerin erişimine karşı korumak sertifika sahibinin yükümlülüğü altındadır.

6.4.3. Erişim Denetim Verileri İle İlgili Diğer Konular

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

6.5. Bilgisayar Güvenliği Denetimleri

6.5.1. Bilgisayar Güvenliği İle İlgili Teknik Gerekler

Kamu SM sistemi içinde, son teknolojik gelişmeler göz önünde bulundurularak bilgisayar güvenliği sağlanır.

6.5.2. Bilgisayar Sisteminin Sağladığı Güvenlik Seviyesi

Düzenlenmesine gerek duyulmamıştır.

6.6. Yaşam Döngüsü Teknik Kontrolleri

6.6.1. Sistem Geliştirme Kontrolleri

Sistemin geliştirilmesi sırasında ortam ve personel güvenliği, kurulan yazılım ve donanım ürünlerinin güvenliği en güncel yöntemler göz önünde bulundurularak sağlanır.

6.6.2. Güvenlik Yönetimi Kontrolleri

Sistem içindeki yazılım ve donanım ürünleri ile ağ ortamının belirlenen güvenlik şartlarını sağlayıp sağlamadığı, test cihazları ve test prosedürleri kullanılarak kontrol edilir. 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

Kamu SM sisteminde son teknolojik gelişmeler göz önünde bulundurularak gerekli ağ güvenliği denetimleri yapılır. Ağ güvenliği denetimlerine ilişkin detaylar SUE Bölüm 6.7'de açıklanmaktadır.

6.8. Zaman Damgası

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

7. Sertifika ve Sertifika İptal Listesi Biçimleri

7.1. Sertifika Biçimi

Bu bölümde Kamu SM tarafından dağıtılan Elektronik Mali Mühür 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 Elektronik Mali Mühür Sertifikaları X.509 V.3 formatında tanımlanan sertifikanın seri numarası, geçerlilik tarihi, ilgili açık anahtar, sertifika sahibine ve sertifikayı yayımlayan Kamu SM'ye ait isim bilgileri ve Kamu SM'nin elektronik imzası gibi zorunlu alanların yanı sıra X.509 V.3 sertifika uzantılarını içerir.

Elektronik Mali Mühür Sertifikasının içeriğinde bulunan sertifika uzantıları sertifikanın kullanılacağı uygulamanın gereklerine bağlı olarak belirlenir. Kamu SM tarafından üretilen Elektronik Mali Mühür Sertifikalarında asgari düzeyde bulunması gereken uzantılar SUE Bölüm 7.1.2'de tanımlanmıştır.

7.1.3. Algoritma ve Nesne Tanımlayıcılar

Kamu SM, Elektronik Mali Mühür Sertifikalarını imzalamak için SHA-256 özet algoritması ile RSA 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

Üretilen sertifikalardaki isim alanı, "ITU X.500 Distinguished Name (Ayırt edici isim)" biçimine uygundur.

7.1.5. İsim Kısıtları

SUE Bölüm 7.1.5'te belirtilmektedir

7.1.6. Sertifika İlkeleri Nesne Tanımlama Numarası

Bağlı olunan Kamu SM Sİ dokümanına ait nesne tanımlama numarası: 2.16.792.1.2.1.1.5.7.4.1

7.1.7. İlke Kısıtları Uzantısının Kullanımı

Düzenlenmesine gerek duyulmamıştır.

7.1.8. İlke Niteleyiciler

"Sertifika İlkeleri" uzantısı Elektronik Mali Mühür Sertifikalarının üretim ve yönetim işlemlerinde uyulan ilke ve esasların Kamu SM Sİ ve Kamu SM SUE olduğuna işaret eder. Elektronik Mali Mühür Sertifikalarının üretim ve yönetiminde takip edilen kurallara işaret eden Sİ dokümanına ait nesne tanımlama numarası [Certificate Policy Object Identifier(s)] Kamu SM tarafından üretilen Elektronik Mali Mühür Sertifikasının "Sertifika İlkeleri" uzantısının içinde yer alır. "Sertifika İlkeleri" uzantısının

içinde "İlke Niteleyici " olarak belirtilen alana Kamu SM SUE dokümanının bulunduğu internet adresi yazılır.

Üçüncü kişiler "Sertifika İlkeleri" uzantısını kontrol ettiğinde Sİ ve SUE'de belirtilen ilke ve uygulama esasları çerçevesinde Elektronik Mali Mühür 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.

7.2.2. Sertifika İptal Listesi Uzantıları

Üretilen SİL'ler "ITU X.509 V.2" SİL formatına uygun olarak SUE Bölüm 7.2.2'de belirtilen bilgileri içerir.

7.3. Çevrim İçi Sertifika Durum Protokolü Biçimi

7.3.1. Sürüm Numarası

Çevrim İçi Sertifika Durum Protokolü RFC 6960'ta belirtilen versiyonları destekler.

7.3.2. ÇİSDUP Uzantıları

Çevrim İçi Sertifika Durum Protokolü RFC 6960'ta tarif edilen "ÇİSDUP" formatını destekler.

8. Uygunluk Denetimleri

Kamu SM, ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS) standardına uygun olarak hizmet verir ve standart gereği düzenli olarak iç ve dış denetimlere tabi tutulur.

8.1. Uygunluk Denetiminin Sıklığı

ISO/IEC 27001 BGYS standardı gereğince yılda bir defa uygunluk denetimi gerçekleştirilir. Her üç (3) yılda bir sertifika yenilenir.

İç denetim, yılda en az bir (1) defa gerçekleştirilir. Gerekli hallerde denetim sayısı arttırılabilir.

8.2. Denetçinin Nitelikleri

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

İç denetim, Sİ dokümanının gereklerini iyi anlayan ve uygunluk denetimi konusunda tecrübeli ESHS 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 Elektronik Mali Mühür Sertifikası için ücret alınır. Ücretin miktarı ve ödeme şekli Kamu SM web sitesinde bildirilir.

Kamu SM'nin imza oluşturma verisinin çalınması, kaybolması, gizliliğinin veya güvenilirliğinin ortadan kalkması, sertifika ilkelerinin değişmesi ya da Elektronik Mali Mühür Sertifikasının hatalı üretilmesi gibi sertifika sahibi kurumun kusurunun bulunmadığı durumların sonucunda Elektronik Mali Mühür 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.

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, 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/kişinin 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

Düzenlenmesine gerek duyulmamıştır.

9.2.2. Diğer Varlıklar

Düzenlenmesine gerek duyulmamıştır.

9.2.3. Sertifika Mali Sorumluluk Sigortası

Kamu SM tarafından oluşturulan Elektronik Mali Mühür Sertifikası'nın sertifika sorumlusu ve üçüncü taraflar tarafından kullanımı ile ilgili doğabilecek risklerden sertifika sorumlusu ve üçüncü taraflar sorumludur.

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 değerlendirilmezler.

9.3.3. Gizli Bilginin Korunma Sorumluluğu

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

9.4. Kişisel Bilginin Gizliliği

9.4.1. Gizlilik Planı

Kamu SM verdiği hizmetlerde sertifika sahiplerinin ve diğer paydaşların kişisel verilerinin gizliliğini 5070 ve 6698 sayılı kanunlar kapsamındaki mer'i mevzuata uygun olarak sağlar.

9.4.2. Gizli Olarak Tanımlanan Bilgiler

Sertifika başvurusu sırasında ve sonrasında kimlik tanımlama ve doğrulama ile sertifika yönetim işlemleri içinde kullanılmak üzere toplanan, ancak sertifikanın içinde yer almayan sertifika sahiplerine ait bilgiler, kişisel gizli bilgi kapsamına girer.

9.4.3. Gizli Olarak Tanımlanmayan Bilgiler

Sertifika içeriğinde bulanan bilgiler, aksi taraflar arası sözleşmelerde belirtilmediği sürece gizli bilgi kapsamında değerlendirilmez.

9.4.4. Gizli Bilginin Korunma Sorumluluğu

Kamu SM, sertifika talep eden kurumdan Elektronik Mali Mühür 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.

Kamu SM Kişisel Verilerin Korunması Kanunu kapsamında https://bilgem.tubitak.gov.tr/tr/icerik/kvkk-aydinlatma-metni kurumsal web sayfasından bilgilendirme yapmaktadır.

9.4.5. Gizli Bilginin Kullanımına İzin Verilmesi

Kamu SM, sertifika talep eden kişinin onayı ve yazılı rızası olması durumunda, kişisel verileri üçüncü kişilere verebilir.

9.4.6. Yetkili Mercilerin Kararına Uygun Olarak Bilginin Açıklanması

Sertifika sahiplerine ait gizli kişisel bilgiler mahkeme kararı olması durumunda açıklanabilir.

9.4.7. Diğer Başlıklar

Düzenlenmesine gerek duyulmamıştır.

9.5. Telif Hakları

Bu Sİ dokümanına bağlı olarak geliştirilen tüm bilgilerin fikri mülkiyet hakları Kamu SM'ye aittir.

9.6. Temsil Hakkı ve Yükümlülükler

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

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

9.6.1. Elektronik Sertifika Hizmet Sağlayıcısı Yükümlülükleri

Kamu SM'nin ESHS olarak işleyişinin güvenli olabilmesi için, sistem bileşenlerinin yerine getirmesi gereken yükümlülükler SUE Bölüm 9.6.1'de açıklanmaktadır.

9.6.2. Kayıt Birimi Yükümlülükleri

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

9.6.3. Sertifika Sahibinin Yükümlülükleri

Sertifika sahibinin yükümlülükleri SUE Bölüm 9.6.3'te açıklanmaktadır.

Sertifika sahibi kurum, Kamu SM Elektronik Mali Mühür Sertifikası Sİ ve SUE dokümanlarında belirtilen şartları okuduğunu, başvuru süreci ve sertifika geçerliliği boyunca Elektronik Mali Mühür 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, Elektronik Mali Mühür Sertifikasıyla işlem yapmadan önce SUE Bölüm 9.6.4'te belirtilen sertifika geçerlilik kontrollerini yapmakla yükümlüdür.

9.6.5. Diğer Bileşenlerin Yükümlülükleri

Diğer bileşenlerin yükümlülükleri SUE dokümanında anlatılmaktadır.

9.7. Yükümlülüklerden Feragat

Düzenlenmesine gerek duyulmamıştır.

9.8. Sorumlulukla İlgili Sınırlamalar

Kamu SM ve sertifika hizmetlerini alan tarafların sorumlulukları ile ilgili sınırlamalar Elektronik Mali Mühür Sertifika İlkeleri ve Uygulama Esasları ve varsa imzalanan sözleşmelerde belirlenir.

9.9. Tazminat Halleri

Kamu SM ve sertifika hizmeti alan taraflar arasında yasa ve yönetmelikte belirtilen 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

9.10.1. Anlaşma Süresi

Düzenlenmesine gerek duyulmamıştır.

9.10.2. Anlaşmanın Sona Ermesi

Düzenlenmesine gerek duyulmamıştır.

9.10.3. Anlaşmanın Sona Ermesinin Etkileri

Düzenlenmesine gerek duyulmamıştır.

9.11. Sistem Bileşenleri İle Haberleşme ve Kişisel Bilgilendirme

Kamu SM, Elektronik Mali Mühür Sertifikaları başvuru, iptal ve yenileme taleplerinin sonuçları hakkında sertifika sahibi kurumu bilgilendirir. Bilgilendirmeler telefon veya kurumsal e-posta aracılığıyla sağlanır. Sertifika yönetimiyle ilgili kritik görülen işlemlerle ilgili bilgilendirmeler resmi yazıyla yapılır.

9.12. Değişiklik Halleri

9.12.1. Değişiklik Metotları

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

9.12.2. Bilgilendirme Mekanizması ve Sıklığı

Sİ 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 Maliye Bakanlığı'nın yayınladığı 19/10/2019 tarih 509 sıra numaralı Vergi Usul Kanunu Genel Tebliğ'ine ve ilgili ESHS'ye ait Sertifika Uygulama Esasları dokümanlarına başvurulur. İhtilafların sulhen çözümünün mümkün olmaması halinde, ihtilafların çözümünde görevli ve yetkili mahkeme Türkiye Cumhuriyeti Gebze Mahkemeleri'dir.

9.14. Uygulanacak Hukuk

Sİ dokümanındaki hükümler, Maliye Bakanlığı'nın yayınladığı 19/10/2019 tarih 509 sıra numaralı Vergi Usul Kanunu Genel Tebliğ'e uygun olarak yazılmıştır.

9.15. Uygulanabilir Yasalarla Uyum

Sİ 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.