TASNİF DIŞI

TÜBİTAK BİLGEM
KAMU SERTİFİKASYON MERKEZİ

ELEKTRONİK MÜHÜR SERTİFİKA İLKELERİ

Doküman Kodu
POL.05.01

Revizyon No
03

Revizyon Tarihi
07.01.2022

TASNİF DIŞI

REVİZYON GEÇMİŞİ		
Revizyon No	**Revizyon Nedeni**	**Revizyon Tarihi**
00	İlk yayın	15.01.2021
01	Doküman formatı güncellenmiştir.	18.01.2021
02	Yenileme süreci güncellenmiştir.	29.11.2021
03	Elektronik mühür ve kurumsal şifreleme sertifikaları başvuru formlarının birleştirilmesi doğrultusunda “Elektronik Mühür Sertifikası Başvuru Formu ve Taahhütnamesi” dokümanının adı “Elektronik Mühür/Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhütnamesi” olarak değiştirilmiştir.	07.01.2022

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'ne bağlı kamu kurum ve kuruluşlara Elektronik Mühür Sertifikası sağlayıcılığı konusundaki işlevleri sırasında uyulması gereken kuralları ve çalışma ilkelerini tanımlayan Sertifika İlkeleri (Sİ) 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 Elektronik Mühür 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 Elektronik Mühür Sertifikası hizmeti sağlamaktadır.

Kamu SM Sİ dokümanı Elektronik 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 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 kurumlar bu dokümanda belirtilen şartları kabul etmiş sayılırlar.

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

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.

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

Sİ 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: Elektronik Mühür Sertifika İlkeleri

Doküman Sürüm Numarası: 03

Yayın Tarihi: 07.01.2022

Nesne Tanımlama Numarası: 2.16.792.1.2.1.1.5.7.1.10

1.3. Sistem Bileşenleri

Kamu SM açık anahtar altyapısını oluşturan sistem bileşenleri aşağıda tanımlanmıştır.

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 bulunanların kayıt ve kimlik doğrulama işlemleri ile Elektronik Mühür Sertifikası dağıtım, yenileme, askı, iptal etme ve iptal olmuş sertifika bilgilerini tüm taraflara duyurma süreçlerini mevzuatta belirtilen şartlara uygun olarak yerine getirmekle yükümlüdür.

Kamu SM, Elektronik Mühür Sertifika Hizmet Sağlayıcısı (Elektronik Mühür SHS) olarak kamu kurum ve kuruluşlarına Elektronik 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

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.

1.3.5. Diğer Bileşenler

1.3.5.1. Kurum

Kamu SM'den Elektronik Mühür Sertifikası talep eden, DETSİS'te bilgileri bulunan ve Elektronik Mühür Sertifikası almaya yetkisi olan tüzel kişiliktir.

1.3.5.2. Elektronik Mühür Sertifikası Asıl ve Yedek Sorumlusu

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

1.4. Sertifika Kullanımı

1.4.1. Uygun Olan Sertifika Kullanımı

Elektronik mühür sertifikası, kamu kurum ve kuruluşları arasında elektronik ortamdaki belge paylaşımında yazışma yapan tarafların kurumsal kimliklerini güvenli bir şekilde tanımlamak ve doğrulamak amacıyla e-Yazışma Teknik Rehberi'ne uygun olarak kullanılmalıdır.

1.4.2. Sertifika Kullanımının Sınırları

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

1.5. Uygulama Esaslarının 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 adresinden 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 uygunluğu, Kamu SM tarafından onaylanır.

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.

Elektronik Mühür SHS (Elektronik Mühür 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.

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

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

Elektronik Mühür Sertifikası: Kamu kurum ve kuruluşları arasında elektronik ortamdaki belge paylaşımında yazışma yapan tarafların kurumsal kimliklerini güvenli bir şekilde tanımlamak ve doğrulamak amacıyla kullanılan elektronik sertifika.

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.

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 Elektronik Mühür Sertifikası talep eden, DETSİS'te bilgileri bulunan ve Elektronik Mühür Sertifikası almaya yetkisi olan tüzel kişilik.

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: Elektronik Mühür 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

2.1. Bilgi Depoları

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.

https://kamusm.bilgem.tubitak.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 Elektronik Mühür SHS sertifikaları
- Kamu SM'ye ait geçmişte oluşturulmuş Kök SHS ve Elektronik Mühür 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 ilgili SUE dokümanında 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 deposunun kesintisiz olarak erişilebilirliğini sağlamak için gerekli önlemleri almak, bilgi deposunda tutulan bilgilerin doğruluğunu ve güncelliğini sağlamakla yükümlüdür.

3. Kimlik Belirleme ve Doğrulama

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

3.1. İsimlendirme

3.1.1. İsim Alanı Tipleri

Elektronik Mühür 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

Elektronik Mühür 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

Elektronik Mühür Sertifikası içeriğinde takma isim veya lakap kullanılmasına izin verilmez.

3.1.4. Farklı İsim Alanı Tiplerinin Yorumlanması

Elektronik Mühür Sertifikası içinde ITU X.500 biçimi dışında isim alanı tipi kullanılmaz.

3.1.5. Kimlik Bilgilerinin Tekilliği

Elektronik Mühür Sertifikası içeriğindeki kurum bilgileri, DETSİS'te yer alan bilgilerdir ve her kurum için ayırt edici niteliktedir. Elektronik Mühür 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 Elektronik Mühür 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 Elektronik Mühür Sertifikası Asıl veya Yedek Sorumlusuna teslim edilir. Asıl veya Yedek Sorumlu tarafından Elektronik Mühür 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

Elektronik Mühür Sertifikası başvurusunda bulunan kurumlar, Kamu SM tarafından istenen kurum bilgilerini, kurumu temsile yetkili kişilerin imzaladığı ve kurumun onayını taşıyan resmi yazı ile Elektronik Mühür/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 sorgusu aracılığıyla kontrol edilir.

3.2.3. Kişisel Kimliğin Belirlenmesi

Elektronik Mühür Sertifikası, kurum adına verildiğinden yalnızca kurumsal başvuru kabul edilmektedir.

3.2.4. Doğrulanmayan Sertifika Sahibi Bilgileri

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

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

SUE Bölüm 3.2'de anlatıldığı şekilde uygulanır.

3.3.1. Olağan Sertifika Yenileme İsteğinde Kimlik Doğrulama

SUE Bölüm 3.2'de anlatıldığı şekilde uygulanır.

3.3.2. İptal Sonrası Yeni Sertifika Talebinde Kimlik Doğrulama

SUE 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 Elektronik Mühür/Kurumsal Şifreleme Sertifikası İptal Başvuru Formu resmi yazısıyla birlikte gönderilerek iptal işlemi gerçekleştirilebilir. Kurum kimlik doğrulaması ve iptal işleminin teyidi SUE Bölüm 3.4'te anlatıldığı şekilde gerçekleştirilir.

4. İşlemsel Gerekler

Bu bölümde sertifika yönetim süreçlerinde yapılan işlemler anlatılmaktadır. Süreçlerle ilgili ayrıntılar Kamu SM'nin internet sitesinde belirtilmektedir.

4.1. Sertifika Başvurusu

4.1.1. Sertifika Başvurusunu Kimlerin Yapabildiği

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

4.1.2. Kayıt İşlemleri ve Sorumluluklar

Elektronik Mühür 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 Elektronik Mühür/Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhütnamesi, Kamu SM'nin internet üzerinden yayımladığı ilgili yönergeler, Sİ ve SUE dokümanları doğrultusunda belirlenir.

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, Elektronik Mühür Sertifikası içinde yer alacak bilgilerin doğruluğunu 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 kurumdan gelen belgelerin Kamu SM tarafından incelenmesi sonucunda kurum kimlik tanımlama ve doğrulama işlevleri yerine getirilir. Kurumdan gönderilen belgelerin doğrulanması için yapılan işlemler SUE Bölüm 4.2.1'de yer almaktadır.

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, 7'inci maddesinin ikinci fıkrasının (a) bendine dayanarak, Kamu SM, DETSİS'te bilgileri bulunmayan veya Elektronik Mühür Sertifikası almaya yetkisi olmayan tarafların başvurusunu reddeder.

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

SUE 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.

Elektronik Mühür 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 Elektronik Mühür Sertifikasının oluşturulduğu konusunda bilgilendirilmiş olur.

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

4.4. Sertifikanın Kabulü

4.4.1. Sertifikanın Kabul Koşulu

Elektronik 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 Mühür Sertifikaları, Kamu SM tarafından yayımlanmaz.

4.4.3. Sertifikanın Oluşturulmasının Diğer Taraflara Duyurulması

Elektronik Mühür Sertifikaları, Kamu SM tarafından yayımlanmaz.

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

Sertifika sahibine ait Elektronik Mühür Sertifikasının içinde yer alan açık anahtar, üçüncü kişilerce EYP 2.0 kapsamında elektronik mührün doğrulanması 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 SUE Bölüm 4.7'de anlatıldığı şekilde gerçekleştirilir.

4.7.1. Sertifikanın Yenileme Koşulları

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

4.7.2. Sertifika Yenileme Başvurusunu Kimlerin Yapabildiği

SUE Bölüm 4.7.2'de tanımlanmaktadır.

4.7.3. Sertifika Yenileme Başvurusunun İşlenmesi

SUE Bölüm 4.7.3'te tanımlanmaktadır.

4.7.4. Sertifika Yenileme ile İlgili Sertifika Sahibinin Bilgilendirilmesi

SUE Bölüm 4.7.4'te tanımlanmaktadır.

4.7.5. Sertifika Yenileme Sonrası Kabul Koşulu

SUE Bölüm 4.7.5'te tanımlanmaktadır.

4.7.6. Sertifika Yenileme Sonrası Sertifikanın Yayımlanması

SUE Bölüm 4.7.6'da tanımlanmaktadır.

4.7.7. Sertifika Yenilemenin Diğer Taraflara Duyurulması

SUE Bölüm 4.7.7'de tanımlanmaktadır.

4.8. Sertifikada Bilgi Değişikliği

Sertifika içeriğinde yer alan bilgilerde değişiklik olması, sertifikanın yenilenmesini gerektirmektedir. Bilgi değişikliğinin gerekli olduğu durumlarda, kurum SUE 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. 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 veya sertifika sahibi kurum tarafından yetkilendirilmiş Elektronik Mühür Sertifikası Asıl veya Yedek Sorumlusu tarafından yapılabilir. Kamu SM, SUE Bölüm 4.9.1'de tanımlanan tüm durumlarda iptal yetkisine sahiptir.

4.9.3. Sertifika İptal Başvurusunun İşlenmesi

Elektronik Mühür Sertifikası iptal işlemi, kurum tarafından yetkilendirilen Elektronik Mühür Sertifikası Asıl veya Yedek Sorumlusu tarafından Kamu SM resmi internet sitesinde yer alan Online İşlemler menüsü aracılığı ile yapılır. İptal işlemlerinin Kamu SM Online İşlemler üzerinden yapılamadığı durumda süreç 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

Kamu SM, kendisine gelen geçerli iptal başvurularını derhal işleme alır ve Elektronik Mühür Sertifikasını en geç 24 saat içerisinde iptal eder. İptal edilen Elektronik Mühür 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 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 Mühür 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, Elektronik Mühür Sertifikalarının iptal durum bilgisini ÇİSDUP üzerinden yayımlar. 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

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. 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 Elektronik Mühür Sertifikası iptal edilir. Elektronik Mühür Sertifikasının iptal edilmesi dışında herhangi bir işlem uygulanmamaktadır.

4.9.13. Sertifikanın Askıya Alındığı Durumlar

Elektronik 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

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

4.9.15. Sertifika Askıya Alma Başvurusunun İşlenmesi

Elektronik Mühür 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. Askıya alma başvurusunun işlenmesi ile ilgili detaylar SUE Bölüm 4.9.15'te verilmiştir.

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

4.9.16. Askıda Kalma Süresi

İlk 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. 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. Üçüncü kişiler, Elektronik Mühür 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

Elektronik Mühür Sertifikasının kullanım süresinin dolması, iptal edilmesi ve Kamu SM'nin sertifika hizmetlerini sonlandırmasıyla sertifika sahipliği sona erer. Kullanım süresinin dolması durumunda Kamu SM sertifika sahibini bilgilendirmek zorunda değildir; sertifika sahibi sertifikanın kullanım süresinin dolduğu zamanı kendisi takip etmekle yükümlüdür.

4.12. Anahtar Yeniden Üretme

Sertifika sahiplerine ait anahtarların yeniden üretilmesi veya yedeklenmesi işlemi uygulanmamaktadır.

5. Yönetim, İşlemsel ve Fiziksel Kontroller

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

5.1. Fiziksel Güvenlik Denetimleri

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

5.1.1. Tesis Yeri ve İnşaatı

Kamu SM operasyonları Gebze ve Ankara'daki tesislerde yürütülmektedir. Bina, yüksek güvenlik gerektiren işlerin yapılmasına imkan sağlayan yapıdadır. 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. Bina içinde, yazılım ve donanım modüllerinin yerleştirilmesi için kilitli ve giriş kontrollü odalar bulunur.

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.

5.1.3. Güç Kaynağı ve Havalandırma

Kamu SM işlevlerinin yerine getirilmesi ve sürekliliğin sağlanması için sistem, kesintisiz güç kaynağı ile beslenir. Bina gerekli havalandırma sistemi ile donatılır.

5.1.4. Su Baskınları

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

5.1.5. Yangın Önleme ve Korunma

Kamu SM işlevlerinin yerine getirildiği ortamlarda yangını önleyici ve olası yangınlarda zararı en aza indirecek önlemler alınmıştır.

5.1.6. Saklama ve Yedekleme Ortamlarının Korunması

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

5.1.7. Atıkların Yok Edilmesi

Hassas bilgilerin bulunduğu ve 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.

5.2. Prosedürel Kontroller

5.2.1. Güvenilir Roller

Güvenilir roller, SUE Bölüm 5.2.1'de detaylandırılır.

5.2.2. Her İşlem İçin Gereken Kişi Sayısı

Kamu SM, Kök SHS ve Elektronik Mühür SHS'ye ait sertifika üretilmesi, iptal edilmesi, imza oluşturma verilerinin başka bir kriptografik modül içerisine yedeklenmesi için birden fazla kişinin aynı anda hazır bulunmasını sağlar. Elektronik Mühür 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.

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

Çalışanlar sistemin işleyiş ve güvenlik gereklerini sağlayabilecek nitelikte, bilgili ve deneyimli kişilerden seçilir.

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 erişim izni 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 en az yılda 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, SUE Bölüm 5.4.1'de belirtilen elektronik veya kağıt ortamda yapılan işlerin kayıtları tutulur.

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.

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 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 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 SUE 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

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 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 SUE 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 değişimine ilişkin detaylar SUE Bölüm 5.6'da açıklanmaktadır.

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.

5.7.3. İmza Oluşturma Verisinin Gizliliğinin Kaybedilmesi

Kamu SM'nin Elektronik Mühür Sertifikalarını imzalamada kullandığı imza oluşturma verisinin gizliğinin kaybedildiğinden şüphelenilmesi ya da bunun öğrenilmesi durumunda ilgili sertifika en kısa zamanda iptal edilir ve SUE Bölüm 5.7.3'te belirtilen işlemler yerine getirilir.

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 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'nin yerine getirmesi gereken işlemler SUE Bölüm 5.8'de açıklanmaktadır.

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, Elektronik Mühür SHS, ÇİSDUP Yayımlayıcı Anahtar Çifti Üretimi

Kök SHS, Elektronik Mühür 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 SUE Bölüm 6.2.1'de belirtilen standartlara uyar.

6.1.1.2. Sertifika Sahibi Anahtar Çiftinin Üretimi

Elektronik 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 Mühür 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.

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, Kurum HSM Cihaz Sorumlusu gözetiminde gerçekleştirilir ve işlem sonrası Teslim Tutanağı doldurularak kurum tarafından imzalanır.

6.1.3. Elektronik Sertifika Hizmet Sağlayıcısı'na Açık Anahtarın Ulaştırılması

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

6.1.5. Anahtar Uzunlukları

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

Kurumlara ait Elektronik Mühür Sertifikalarını imzalayan Elektronik Mühür 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 Elektronik Mühür 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" uzantısı içerisinde belirtilir.

Kamu SM kök anahtarı, alt kök sertifikasını ve SİL'i imzalamak için kullanılır. Kamu SM Elektronik 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) 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. 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.

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 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 SUE 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 Elektronik Mühür Sertifikaları kullanım sürelerinin dolmasından itibaren 20 (yirmi) yıl boyunca arşivlenir. Elektronik

Mühür 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, Elektronik Mühür Sertifikasının içeriğinde belirtilen kullanım süresi kadardır. Üretilen Elektronik Mühür Sertifikalarının son kullanma tarihi, Elektronik Mühür SHS Sertifikasının son kullanma tarihini aşamaz.

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.

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.

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, son teknolojik gelişmeler göz önünde bulundurularak bilgisayar güvenliği sağlanır. Bilgisayar güvenliğiyle ilgili teknik gerekler SUE Bölüm 6.5.1'de açıklanmaktadır.

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 SUE Bölüm 6.6.1'de açıklanmaktadır.

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 Esaslarında bulunur.

7. Sertifika ve Sertifika İptal Listesi Biçimleri

7.1. Sertifika Biçimi

Bu bölümde Kamu SM tarafından dağıtılan Elektronik 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 Mühür 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. Elektronik Mühür Sertifikasının içeriğinde bulunan sertifika uzantıları sertifikanın kullanılacağı uygulamanın gereklerine bağlı olarak belirlenir.

Kamu SM tarafından üretilen Elektronik Mühür Sertifikalarında asgari düzeyde bulunması gereken uzantılar SUE Bölüm 7.1.2'de tanımlanmıştır.

7.1.3. Algoritma ve Nesne Tanımlayıcılar

Kamu SM, kurumlara verdiği Elektronik Mühür 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 Elektronik Mühür Sertifikalarındaki isim alanı "ITU X.500 Distinguished Name [Ayırt edici İsim]" 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: 2.16.792.1.2.1.1.5.7.1.10

7.1.7. İlke Kısıtları Uzantısının Kullanımı

Düzenlenmesine gerek duyulmamıştır.

7.1.8. İlke Niteleyiciler

"Sertifika İlkeleri Uzantısı" Elektronik Mühür Sertifikalarının üretim ve yönetim işlemlerinde uyulan ilke ve esasların Kamu SM Sİ ve Kamu SM SUE olduğuna işaret eder. Elektronik 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 Mühür Sertifikasının "Sertifika İlkeleri Uzantısı[1]"nın içinde yer alır. "Sertifika İlkeleri Uzantısı"nın içinde "İlke Niteleyici[2]" 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 Elektronik 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" 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 V.1'i destekler.

7.3.2. ÇİSDUP Uzantıları

ÇİSDUP sorguları SUE Bölüm 7.3.2'de belirtilen bilgileri içerir.

[1] Certificate Policies

[2] Policy Identifier

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 Elektronik Mühür Sertifikası için kurumlardan 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 Mühür Sertifikasının hatalı üretilmesi gibi sertifika sahibi kurumun kusurunun bulunmadığı durumların sonucunda Elektronik 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 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, SUE 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 Elektronik Mühür 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 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 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 Elektronik Mühür 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.

9.4.3. Gizli Olarak Tanımlanmayan Bilgiler

Elektronik Mühür 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 Elektronik 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.

9.4.5. Gizli Bilginin Kullanımına İzin Verilmesi

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

9.4.6. Yetkili Mercilerin Kararına Uygun Olarak Bilginin Açıklanması

Kamu SM 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 Elektronik Mühür 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 Elektronik Mühür/Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhütname yükümlülüklerini de yerine getirirler.

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

9.6.5. Diğer Bileşenlerin Yükümlülükleri

9.6.5.1. Kurumun Yükümlülükleri

Kamu SM'ye sertifika başvurusunda bulunan kurumun yükümlülükleri SUE Bölüm 9.6.5.1'de belirtilmektedir.

9.6.5.2. Kurum Sertifika Sorumlularının Yükümlülükleri

Kurum adına Elektronik Mühür Sertifikası başvurusunda bulunan Elektronik Mühür Sertifikası Asıl ve Yedek Sorumlusunun yükümlülükleri SUE Bölüm 9.6.5.2'de belirtilmektedir.

9.7. Yükümlülüklerden Feragat

Kamu SM ile sertifika sahipleri olan kamu kurum veya kuruluşları arasındaki yükümlülük, Elektronik Mühür/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.

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, Elektronik Mühür/Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhütnamesi ve varsa imzalanan sözleşmelere uygun olarak Kamu SM ile iş birliği içinde çalışır; süreçleri yerine getirirken gerekli desteği ve koordinasyonu Sİ ve SUE dokümanlarında belirtilen şartlar altında sağlar.

9.10.1. Anlaşma Süresi

Sertifika sahibi kurumun imzaladığı Elektronik Mühür/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 SUE Bölüm 9.10.2'de belirtilen durumlarda sonlandırılabilir.

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.

9.11. Sistem Bileşenleri ile Haberleşme ve Kişisel Bilgilendirme

Kamu SM, Elektronik 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 Sİ dokümanının 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 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

Sİ 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

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.