T.C.
EMNİYET GENEL MÜDÜRLÜĞÜ
SERTİFİKA UYGULAMA ESASLARI (SUE)
(Nitelikli Elektronik Sertifika İçindir)

SÜRÜM :03
TARİH :12.10.2012

1. GİRİŞ

Türk Polis Teşkilatı, rütbeleri Polis Memurluğundan başlayıp Emniyet Genel Müdürlüğüne kadar uzanan, tüm il ve ilçelerde örgütlenmiş, kırsalda görevini askeri polis olan jandarmaya bırakmış, kentte ise görevi kendisi yöneten iç güvenlikten sorumlu devlet teşkilatıdır. 10 Nisan 1845 tarihinde temeli atılmıştır.

Merkez teşkilatı bünyesinde Ana Komuta Kontrol, Strateji Geliştirme, Arşiv, Asayiş, Bilgi İşlem, Dış İlişkiler, Eğitim, Güvenlik, Haberleşme, Havacılık, İdari ve Mali işler, İkmal-Bakım, İnşaat-Emlak, Interpol, İstihbarat, Kaçakçılık ve Organize Suçlarla Mücadele, Koruma, Kriminal, Özel Harekât, Personel, Sağlık İşleri, Sivil Savunma, Sosyal Hizmetler, Teftiş Kurulu, Terörle Mücadele Harekât, Trafik Eğitim ve Araştırma, Trafik ve Denetleme, Yabancılar Hudut İltica Daireleri vardır. Taşra teşkilatını ise, il emniyet müdürlükleri ve ilçe Emniyet Amirlikleri oluşturur. Genel müdürlük, üst kurum ve yönetim bakımından İçişleri Bakanlığı'na bağlıdır.

Kurumun yapılanması iki şekilde olmuştur. Birincisi Merkez Teşkilatı ve ikincisi ise Taşra Teşkilatı'dır. Merkez Teşkilatı, Daire Başkanlıkları şeklinde yapılanmıştır. Taşra Teşkilatı ise 81 ilde İl Emniyet Müdürlükleri olarak faaliyet yürütmektedir. Merkez Teşkilatı'ndaki daire başkanlıklarının bazıları direkt olarak emniyet genel müdürüne bağlı olmak ile birlikte diğerleri ise 5 adet emniyet genel müdür yardımcısına bağlı olarak hizmet vermektedir. Taşra teşkilatında ise illerin başında il emniyet müdürü bulunmakta ve ildeki bütün birimler il emniyet müdürüne bağlı olmaktadır.

Türkiye Cumhuriyeti sınırları içerisinde, belediye teşkilatlanması tamamlanmış olan il, ilçe ve beldelerde güvenlik, Emniyet Genel Müdürlüğü tarafından sağlanmakta; daha küçük birimlerin ve yapılaşmaya açılmamış alanların güvenliği ise Jandarma Genel Komutanlığı tarafından sağlanmaktadır. Emniyet Genel Müdürlüğü Merkez ve 81 ilde teşkilatlanmış olup konularına göre uzmanlaşmış alt birimlere ayrılmıştır.

T.C. Emniyet Genel Müdürlüğü (EGM) Sertifika Uygulama Esasları (SUE) dokumanı, 15 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza Kanunu, 2004/21 sayılı Başbakanlık Genelgesi, Bilgi Teknolojileri ve İletişim Kurumu'nun yayımladığı Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik, Elektronik İmza İle İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'e uygun olarak hazırlanmıştır.

EGM'nin nitelikli elektronik sertifika hizmeti alanındaki faaliyetlerini nasıl yürüttüğü, 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) Sertifika İlkeleri (Sİ) dokümanında belirlenen ilkeler doğrultusunda tanımlanmıştır.

SUE dokümanı, elektronik sertifika hizmet sağlayıcısı (ESHS) olarak nitelikli elektronik sertifikalar için, başvuru, üretim, yenileme ve iptal işlemleriyle ilgili hizmetlerin, idari, teknik ve yasal gerekliliklere uygun olarak yürütülmesiyle ilgili esasları ortaya koyar.

1.1. Genel Bakış

SUE dokümanı, EGM'nin verdiği nitelikli elektronik sertifika hizmetini kapsar. Bu bağlamda, Kamu SM Sİ dokümanı ilkelerine uygun olarak sertifika başvuru taleplerinin alınması, bu başvuruların işlenmesi ve üretilmesi, askıya alma ve iptal taleplerinin alınması ve gerçekleştirilmesi ve sertifika durum bilgilerinin yayınlanması, yenileme taleplerinin alınması ve gerçekleştirilmesi gibi işlemlerin nasıl yapılacağını gösterir.

Bu işlemler, SUE dokümanında yer alan uygulama esaslarına göre hazırlanan ve ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi uyarınca dokümante edilen prosedür ve talimatlar ile kılavuzlar aracılığıyla yürütür.

SUE dokümanı, "Internet Açık Anahtar Altyapısı Sertifika İlkeleri ve Sertifika Uygulama Esasları Çerçeve Planı" (IETF RFC 3647 Internet X.509 PublicKeyInfrastructureCertificatePolicyandCertificationPractices Framework) rehber kitapçığına uygun olarak hazırlanmıştır.

1.2. Doküman Adı ve Tanımı

Bu SUE dokümanının açık adı "T.C. Emniyet Genel Müdürlüğü Sertifika Uygulama Esasları (SUE) (Nitelikli Elektronik Sertifika İçindir)"dir. Dokümanın sürüm numarası "02" ve tarihi "10.10.2012"dir ve kapak sayfasında yer almaktadır.

SUE dokümanı, Kamu SM Sİ'de belirlenen ve nesne tanımlayıcı numarası (OID) aşağıda verilen nitelikli elektronik sertifika ilkelerinin uygulama esaslarını kapsar:

- KAMU SM Nitelikli Elektronik Sertifika İlkeleri (2.16.792.1.2.1.1.5.7.1.1): Kanun, yönetmelik ve tebliğ uyarınca, bireylerin elle atılan imzaya eşdeğer güvenli elektronik imza kullanımına olanak veren nitelikli elektronik sertifikaları kapsar.

SUE dokümanı "http://www.egmsm.gov.tr" web adresinde kamuya açık olarak yayımlanmaktadır.

1.3. Sistem Bileşenleri

1.3.1. Elektronik Sertifika Hizmet Sağlayıcısı

Elektronik sertifika hizmet sağlayıcısı olarak EGM personeline nitelikli elektronik sertifika hizmeti vermektedir. Bu kapsamda, EGM ESHS'nin sertifikası, Kamu SM, Kök SHS tarafından imzalanmıştır. EGM personeline dağıtılan nitelikli elektronik sertifikalar ise EGM ESHS'nin imzasını taşır.

EGM ESHS, sertifika başvuru işlemlerini ve bu işlemlerin ayrılmaz bir parçası olan kimlik doğrulama işlemleri ile üretim, dağıtım, yayımlama, yenileme, askı ve iptal işlemlerini yapmaktadır.

1.3.2. Kayıt Birimleri

Düzenleme dışıdır.

1.3.3. Sertifika Sahipleri

Sertifika sahipleri, kimliği doğrulanan ve buna bağlı olarak adlarına sertifika üretilen EGM personeli gerçek kişilerdir.

Sertifika sahibinin sorumluluğu ve sertifika kullanımından doğan sonuçlar, ilgili mevzuatla ve sertifika sahibi taahhütnamesiyle belirlenir.

1.3.4. Üçüncü Kişiler

Üçüncü kişiler, EGM tarafından verilmiş olan sertifikalara bağlı imza oluşturma verileriyle imzalanmış belgeleri alan, ilgili sertifikalara güvenen taraflardır.

EGM tarafından verilmiş sertifikaların kullanımına bağlı üçüncü kişilere karşı EGM'nin sorumluluğunun sınırları işbu dokümanda belirtilmiştir.

1.3.5. Diğer Bileşenler

Düzenleme dışıdır.

1.4. Sertifika Kullanımı

1.4.1. Uygun Olan Sertifika Kullanımı

EGM alt kök sertifikası sadece kullanım amacı doğrultusunda sertifika imzalamak için kullanılır.

EGM personeli adına üretilen nitelikli elektronik sertifikalar, ilgili mevzuat uyarınca elle atılan imzayla aynı hukuki sonucu doğuran güvenli elektronik imza oluşturmak amacıyla kullanılır. Güvenli elektronik imzanın hukuki sonuçlarını doğurabilmesi için imza oluşturma verisinin güvenli elektronik imza aracının içinde bulunması ve güvenli yazılım veya donanım araçları kullanılarak güvenilir yöntemlerle oluşturulması gerekmektedir.

1.4.2. Sertifika Kullanım Sınırları

Nitelikli elektronik sertifikaya ait imza oluşturma ve doğrulama verileri, güvenli imza oluşturma ve oluşturulan güvenli elektronik imzanın doğrulanması dışında başka amaçla kullanılamaz.

Mevzuatta da belirtildiği gibi, kanunun resmi şekle veya özel merasime bağladığı işlemlerde ve teminat sözleşmelerinde ve diğer kısıtlar dışında nitelikli elektronik sertifika kullanılamaz.

1.5. Sertifika Uygulama Esasları Yönetimi

1.5.1. Doküman Yönetimi

İşbu SUE dokümanının tüm hakları ve sorumluluğu EGM'ye aittir.

1.5.2. İletişim Bilgileri

SUE dokümanıyla ilgili iletişim bilgileri aşağıdadır:

T.C. Emniyet Genel Müdürlüğü
Adres : Ayrancı Mahallesi Dikmen Cad. No:11 Çankaya ANKARA
Telefon : 312 462 0 462
Faks : 312 462 67 62
Çağrı Merkezi : 312 462 67 59
E-posta : egmsm@egm.gov.tr
Web : http://www.egmsm.gov.tr

1.5.3. SUE'nin İlkelere Uygunluğunu Belirleyen Kişi

EGM, SUE dokümanının Kamu SM Sİ dokümanına uygunluğunu EGM tarafından yetkilendirilen kişiler belirler.

1.5.4. SUE Onay Prosedürü

SUE dokümanı, KAMU SM Sİ dokümanına uygun olarak hazırlanmıştır. SUE dokümanı EGM tarafından onaylanır.

1.6. Kısaltmalar ve Tanımlar

1.6.1. Tanımlar

Açık Anahtar: Bir çift anahtarlı şifreleme algoritmasında diğer kişilerin de bilgisine açık olan kriptografik anahtar; Kanun'da imza doğrulama verisi olarak isimlendirilmiştir.

Açık Anahtarlı Altyapı (PKI): Matematiksel bağlantısı bulunan kriptografik anahtar çiftlerine dayalı ve sertifika tabanlı bir kriptografik sistemin kurulması ve işletilmesini sağlayan mimari yapı, teknikler, uygulamalar ve düzenlemeler bütünüdür.

Aktivasyon: İmza oluşturma verisi erişim şifresinin, kullanıcıya şifre zarfıyla gönderilmesi yerine, kendisi tarafından belirlenmesine imkân sağlayan güvenli yöntem. Buna göre kullanıcı, TÜRKTRUST tarafından sağlanan yazılımı kullanır. Akıllı kartı bilgisayara takılıyken, bu yazılım içinden "aktivasyon kodu" talebinde bulunur ve "aktivasyon kodu" başvurusu sırasında verdiği cep telefonuna veya e-posta adresine gönderilir. Kullanıcı, aynı yazılımı ve "aktivasyon kodunu" kullanarak imza oluşturma verisi erişim şifresini belirler.

Alt Kök Sertifikası: ESHS'nin PKI hiyerarşisi uyarınca sertifika üretim merkezi tarafından oluşturulmuş, ESHS kök sertifikasının imzasını taşıyan ve son kullanıcı sertifikalarını imzalama amaçlı kullanılan sertifikadır.

Anahtar: İmza oluşturma verisi veya imza doğrulama verisinden herhangi biri.

Anahtar Yenileme: İmza doğrulama verisi ve geçerlilik süresi dışında, bir sertifika içinde yer alan tüm bilgi alanlarının aynı şekilde kullanılmasıyla yeni bir sertifikanın üretilmesidir.

Arşiv: ESHS'nin saklamakla yükümlü olduğu bilgi, belge ve elektronik verilerdir.

Ayırt Edici İsim Alanı (Distinguished Name [DN] Field): Ayırt edici isim alanı, sertifika sahibinin veya sertifikayı veren kuruluşun kimlik bilgilerini içeren bilgi alanıdır. Bu alan içinde CN, O, OU, T, L, C ve SERIALNUMBER gibi farklı alt alanlar sertifika tipine göre uygun içerikle yer alabilir.

Çevrim İçi Sertifika Durum Protokolü (ÇİSDUP): Sertifikaların geçerlilik durumunun kamuya duyurulması için oluşturulmuş, sertifika durum bilgisinin çevrim içi yöntemlerle anında ve kesintisiz alınmasını sağlayan standart protokol.

Denetim: ESHS'nin her türlü faaliyet ve işleyişinin ilgili mevzuat hükümlerine ve standartlara uygunluğunun incelenerek; muhtemel hata, noksanlık, usulsüzlük ve/veya suiistimallerin tespit edilmesi ve ilgili mevzuatta veya standartlarda öngörülen yaptırımların uygulanması amacıyla yapılan çalışmalar bütünüdür.

Dizin: Geçerli sertifikaları içinde bulunduran elektronik depodur.

Elektronik İmza: Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veridir.

Elektronik Sertifika: Açık anahtarlı alt yapıda, açık anahtar ile anahtar sahibinin kimliğini, elektronik sertifika hizmet sağlayıcısının gizli anahtarını kullanarak birbirine bağladığı elektronik kayıttır. Metin içinde "elektronik" sözcüğü yer almaksızın da "sertifika" aynı anlamda kullanılmıştır.

Elektronik Sertifika Hizmet Sağlayıcısı: Elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişilerdir. Metin içinde, "elektronik" sözcüğü yer almaksızın da "sertifika hizmet sağlayıcısı" aynı anlamda kullanılmıştır.

Elektronik Veri: Elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıtlardır.

Erişim Şifresi: Güvenli elektronik imza oluşturma araçlarına erişim için kullanılan parola, biyometrik değer gibi verilerdir.

Gizli Anahtar: PKI yapısında, bir çift anahtarlı şifreleme algoritmasında sadece anahtar sahibinin bilgisinde olan kriptografik anahtar; Kanun'da imza oluşturma verisi olarak isimlendirilmiştir.

Güvenli Elektronik İmza: Kanunun 4 üncü maddesinde sayılan niteliklere sahip, Kanunun hariç tuttuğu işlemler dışında elle atılan imzayla aynı hukuki sonucu doğuran elektronik imzadır.

Güvenli Elektronik İmza Doğrulama Aracı: Kanunun 7 nci maddesinde sayılan niteliklere sahip imza doğrulama aracıdır.

Güvenli Elektronik İmza Oluşturma Aracı: Kanunun 6 ncı maddesinde sayılan niteliklere sahip imza oluşturma aracıdır.

İmza Doğrulama Aracı: Elektronik imzayı doğrulamak amacıyla imza doğrulama verisini kullanan yazılım veya donanım aracıdır.

İmza Doğrulama Verisi: Elektronik imzayı doğrulamak için kullanılan şifreler, kriptografik açık anahtarlar gibi verilerdir.

İmza Oluşturma Aracı: Elektronik imza oluşturmak üzere, imza oluşturma verisini kullanan yazılım veya donanım aracıdır.

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

İmza Sahibi: Elektronik imza oluşturmak amacıyla bir imza oluşturma aracını kullanan gerçek kişidir.

İnceleme: Kuruma yapılan bildirimin gerekli şartları sağlayıp sağlamadığını tespit etmek amacıyla yapılan çalışmalardır.

İptal Durum Kaydı: Kullanım süresi dolmamış sertifikaların iptal bilgisinin yer aldığı, iptal zamanının tam olarak tespit edilmesine imkân veren ve üçüncü kişilerin hızlı ve güvenli bir biçimde ulaşabileceği kayıttır.

Kanun: 15 Ocak 2004 tarihli ve 5070 sayılı Elektronik İmza Kanunu'dur.

Kök Sertifika: ESHS kurumsal kimlik bilgilerini ESHS imza doğrulama verisine bağlayan, sertifika üretim merkezi tarafından üretilmiş olan ve kendi imzasını taşıyan, ESHS'nin ürettiği tüm sertifikaların doğrulanabilmesi için ESHS tarafından yayımlanan sertifikadır.

Kurum: Bilgi Teknolojileri ve İletişim Kurumu'dur.

Nitelikli Elektronik Sertifika (NES): Kanunun 9 uncu maddesinde sayılan niteliklere sahip elektronik sertifikadır.

Özetleme Algoritması: İmzalanacak elektronik verilerin sabit uzunlukta bir özetinin çıkarılmasında kullanılan algoritmadır.

Özne: Sertifikanın CN alanında yer alan kişi veya sunucu adıdır.

Sertifika: Bkz. "Elektronik Sertifika"

Sertifika İlkeleri: ESHS'nin işleyişi ile ilgili genel kuralları içeren belgedir.

Sertifika İptal Listesi: İptal edilmiş sertifikaların kamuya duyurulması amacıyla ESHS tarafından oluşturulan, imzalanan ve yayımlanan elektronik dosyadır.

Sertifika Mali Sorumluluk Sigortası: ESHS'nin, Kanundan doğan yükümlülüklerini yerine getirmemesi sonucu doğacak zararların karşılanması amacıyla yaptırmakla yükümlü olduğu sigortadır.

Sertifika Sahibi: Adına, sertifika hizmetlerinin koşullarına ilişkin ESHS ile sertifika sahibi taahhütnamesi veya sözleşmesi imzalanan kişidir.

Sertifika Uygulama Esasları: Sertifika ilkelerinde yer alan hususların nasıl uygulanacağını detaylı olarak anlatan belgedir.

Sertifika Üretim Merkezi: ESHS yapısında yer alan, onaylı sertifika talepler doğrultusunda sertifika üretimi yapan, sertifika iptal işlemlerini gerçekleştirilen, sertifika kayıtları ile sertifika iptal durum kayıtlarını yaratan, işleten ve yayımlayan birimdir.

Sertifika Yenileme: İmza doğrulama verisi de dâhil olmak üzere, geçerlilik süresi dışında bir sertifika içinde yer alan tüm bilgi alanlarının aynı şekilde kullanılmasıyla yeni bir sertifikanın üretilmesidir. Sertifika yenileme için, sertifikanın geçerli olması zorunludur.

Tebliğ: Bilgi Teknolojileri ve İletişim Kurumu tarafından yayımlanan Elektronik İmzaya İlişkin Süreçler ile Teknik Kriterlere İlişkin Tebliğ'dir.

Yönetmelik: Bilgi Teknolojileri ve İletişim Kurumu tarafından yayımlanan Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmeliktir.

Zaman Damgası: Bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı ve/veya kaydedildiği zamanın tespit edilmesi amacıyla, elektronik sertifika hizmet sağlayıcısı tarafından elektronik imzayla doğrulanan kayıttır.

Zaman Damgası İlkeleri: Zaman damgası ve hizmetleri ile ilgili genel kuralları içeren belgedir.

Zaman Damgası Uygulama Esasları: Zaman damgası ilkelerinde yer alan hususların nasıl uygulanacağını detaylı olarak anlatan belgedir.

1.6.2. Kısaltmalar

ÇİSDUP: Çevrim İçi Sertifika Durum Protokolü (OCSP – Online CertificateStatus Protocol)

DN : Distinguished Name – Ayırt Edici İsim

ESHS : Elektronik Sertifika Hizmet Sağlayıcısı

ETSI : European Telecommunication Standards Institute – Avrupa Telekomünikasyon Standartları Enstitüsü

FKM : Felaket Kurtarma Merkezi

IETF : Internet Engineering Task Force – İnternet Mühendisliği Görev Grubu

KPS : Kimlik Paylaşım Sistemi

NES : Nitelikli Elektronik Sertifika

OID : Object Identifier – Nesne Tanımlayıcı Numarası

PKI : Public Key Infrastructure – Açık Anahtarlı Altyapı

RFC : IETF tarafından yayımlanan, kılavuz niteliğinde yorum talebi dokümanları

SERİM : Sertifika İrtibat Masası

SHM : Sertifika Hizmetleri Merkezi

Sİ : Sertifika İlkeleri

SİL : Sertifika İptal Listesi

SUE : Sertifika Uygulama Esasları

TCKN : T.C. Kimlik Numarası

TSE : Türk Standartları Enstitüsü

2. YAYIMLAMA VE BİLGİ DEPOSU YÜKÜMLÜLÜKLERİ

EGM, ESHS olarak nitelikli elektronik sertifika hizmetleriyle ilgili doküman ve kayıtları hazırlamak ve saklamakla yükümlüdür. Bu doküman ve kayıtların bazıları, ESHS yükümlülükleri gereğince kamuya açık şekilde yayımlanır.

2.1. Bilgi Depoları

EGM, sertifika sahipleri ve üçüncü tarafların ulaşabileceği şekilde SUE ve iptal listeleri, ilgili doküman ve bilgileri web üzerinden kamuya açık şekilde bilgi deposunda sürekli olarak yayımlar.

2.2. Sertifika Hizmeti ile İlgili Bilgilerinin Yayımlanması

EGM nitelikli elektronik sertifika ve zaman damgası hizmetlerine ilişkin alt kök sertifikaları herkesin erişimine açık olarak bilgi deposunda yayımlanır. Güncel iptal durum kayıtları, hem ÇİSDUP desteğiyle hem de SİL'ler aracılığıyla erişime açık tutulur.

EGM tarafından üretilen sertifikalar, ancak sertifika sahibinin yazılı rızası olması kaydıyla herkesin erişimine açık tutulur.

Ayrıca taahhütname, müşteri kılavuzu benzeri dokümanlar da yine aynı şekilde yayımlanır.

Bu bölümde sözü geçen bilgilere erişim, http://www.egmsm.gov.tr adresli web sitesinden kamuya açık olarak sağlanır.

2.3. Yayımın Sıklığı ve Zamanı

Yukarıda bahsi geçen dokümanların yeni sürümleri çıktıkça, eski sürümlerle birlikte bilgi deposunda yayımlanır. Sertifika ve çevrim içi sertifika durum sorgulama kayıtları sürekli yayımlanır. SİL, 12 (on iki) saatte bir olmak üzere günde 2 (iki) kez ve 24 (yirmidört) saatlik geçerlilik süresiyle yayımlanır.

2.4. Erişim Kontrolleri

EGM, bilgi deposu herkesin erişimine açıktır. Bu nedenle, hem yayımlanan bilgilerin gerçekliğini hem de yayımlamanın kesintisiz şekilde devam etmesini sağlamak üzere, ilgili web adres için gerekli her türlü güvenlik önlemini alır.

3. KİMLİK BELİRLEME VE DOĞRULAMA

EGM, nitelikli elektronik sertifikada ilk başvuru sırasında personelinin kimlik doğrulamasını yasal ve teknik gereklilikler uyarınca resmi kaynaklara dayandırarak yapar.

Bu kimlik doğrulamasına dayanarak daha sonra yenileme, askıya alma ve iptal taleplerini değerlendirir.

3.1. İsimlendirme

3.1.1. İsim Alanı Tipleri

Nitelikli elektronik sertifikalarda X.500 ayırt edici isimleri kullanılır.

3.1.2. Kimlik Bilgilerinin Teşhise Elverişli Olması

Üretilen nitelikli elektronik sertifikaların isim alanlarında, ESHS tarafından doğrulanmış sertifika sahiplerinin kimlik belgeleri ve güncel nüfus kayıtlarından doğrulanan isimler bulunur.

Alt kök sertifikaların isim alanında ise Kamu SM tarafından belirlenen kurum adı ve ilgili kök bilgisi açık olarak yer alır.

3.1.3. Sertifika Sahiplerinin Takma İsim veya Lakap Kullanması

Takma isim ve lakap içeren sertifika üretilmez.

3.1.4. Farklı İsim Alanı Tiplerinin Yorumlanması

Nitelikli elektronik sertifikalarda yer alan isimler X.500 ayırt edici isim biçimine uygun olarak değerlendirilir.

3.1.5. Kimlik Bilgilerinin Tekliği

Nitelikli elektronik sertifikalarda, ayırt edici isim alanında yer alan bilgilerle sertifika sahiplerinin benzersiz biçimde belirlenmesine olanak tanır.

Seri numarası (SERIALNUMBER) alanında, Türkiye Cumhuriyeti vatandaşı olan sertifika sahibinin benzersiz kimlik numarası yer alır.

3.1.6. Markaların Tanınması, Doğrulanması ve Rolü

Düzenleme dışıdır.

3.2. İlk Kimlik Belirleme

Nitelikli elektronik sertifika başvuru sahiplerinin ilk kimlik belirleme işlemleri için aşağıdaki yöntemler uygulanır.

3.2.1. İmza Oluşturma Verisine Sahip Olmanın Kanıtlanması

Sertifika sahibinin nitelikli elektronik sertifika talebi üzerine EGM tarafından üretilir. Güvenli elektronik imza oluşturma aracı sertifika sahibine yetkililerce şahsen teslim edilir. Böylelikle gizli anahtara sahip olduğu kanıtlanır.

3.2.2. Kurumsal Kimliğin Belirlenmesi

Düzenleme dışıdır.

3.2.3. Kişisel Kimliğin Belirlenmesi

Sertifika başvuru sahibi personelin kimlik doğrulama işlemi, yasal düzenlemelerde belirlendiği şekilde, bağlı bulunduğu Şube Müdürü tarafından, yüz yüze kimlik doğrulaması yapılarak tamamlanır.

Başvuru sahiplerinin kimlik bilgileri ise Kimlik Paylaşım Sistemi ve kimlik belgesine dayanılarak belirlenmiş olur.

3.2.4. Doğrulanmayan Sertifika Sahibi Bilgileri

Başvuru sahibinin telefon, adres gibi iletişim bilgileri ve e-posta adres bilgisi ESHS tarafından doğrulanmayan bilgilerdir. Başvuru sahibinin belgelerde bulunan beyanı kabul edilir.

3.2.5. Yetkinin Doğrulanması

Düzenleme dışıdır.

3.2.6. Uyum Kriteri

Düzenleme dışıdır.

3.3. Sertifika Yenileme İsteğinde Kimlik Doğrulama

3.3.1. Olağan Sertifika Yenileme İsteğinde Kimlik Doğrulama

Sertifika sahibi sertifika yenileme talebini, mevcut nitelikli elektronik sertifikanın geçerlilik süresi içinde, internet üzerinden geçerli sertifikasını kullanarak başlatır. Talep sahibi işlem sırasında aldığı nitelikli elektronik sertifika sahibi taahhütnamesini diğer belgelerle birlikte yetkililere teslim eder.

Yenileme talebinde bulunan kişinin kimlik doğrulaması, hem sistemdeki bilgileri ve KPS üzerinden, hem de Şube Müdürü'nün onayıyla yapılır.

Başvuru sahibinin telefon, adres gibi iletişim bilgileri ve e-posta adres bilgisi ESHS tarafından doğrulanmayan bilgilerdir. Başvuru sahibinin belgelerde bulunan beyanı kabul edilir. Bu bilgiler yenileme işlemi sırasında başvuru sahibinin beyanına dayanılarak değiştirilebilir.

3.3.2. İptal Sonrası Yeni Sertifika Talebinde Kimlik Doğrulama

Sertifika içinde yer alan bilgilerde herhangi bir değişiklik olması, kullanım süresinin dolması ya da çalıntı, kayıp gibi nedenlerle iptal sonrasında yeniden sertifika almak isteyen sertifika sahibinin kimlik doğrulaması ilk başvuru işlemlerinde olduğu gibi bağlı bulunduğu Şube Müdürü tarafından başvuru belgeleri onaylanarak yapılır.

3.4. Sertifika İptal İsteğinde Kimlik Doğrulama

Sertifika sahibi internet veya çağrı merkezi üzerinden ya da Şube Müdürleri ise kendisine bağlı personeli için ıslak imzalı beyan yazısıyla iptal talebine bulunabilir.

İnternet ve çağrı merkezi üzerinden iptal işlemi için kimlik doğrulama adımları sertifika sahibine verilen parola ve kişisel bilgilerle yapılır. Şube Müdürü tarafından gönderilen ıslak imzalı iptal taleplerinde ise ilgili yazının onayı kontrol edilir.

4. İŞLEMSEL GEREKLER

SUE dokümanının bu bölümünde nitelikli elektronik sertifikaların yaşam döngüsü içinde sertifika yönetimiyle ilgili işlemler anlatılmaktadır. Bu işlemler sırasında sertifika sahipleri, ESHS ve üçüncü tarafların sorumlulukları da belirlenmiştir.

4.1. Sertifika Başvurusu

4.1.1. Sertifika Başvurusunu Kimlerin Yapabildiği

EGM personeli bağlı bulunduğu Şube Müdürünün, Şube Müdürü veya daha üst bir amir pozisyonunda olması halinde ise üst amirin onayıyla bireysel olarak nitelikli elektronik sertifika başvurusunda bulunabilir. Başvuru sahibi tarafından doldurulup imzalanan nitelikli elektronik sertifika sahibi taahhütnamesi bağlı bulunduğu Şube Müdürü tarafından onaylanarak yetkililerce üretim merkezine ulaştırılır.

EGM personeli Şube Müdürünün ya da bir üst amir kimlik doğrulama işlemi olmadan nitelikli elektronik sertifika başvurusu yapamayacağı gibi EGM'de personelin haberi olmadan adına başvuru işlemlerini başlatamaz.

4.1.2. Kayıt İşlemleri ve Sorumluluklar

Nitelikli elektronik sertifika başvuru sahibi, başvuru işlemlerini ilgili web sitesinden başlatır. Başvuru işlemleri tamamlamadan önce nitelikli elektronik sertifika sahibi taahhütnamesinin çıktısını alır ve imzalar. Başvuru sahibi bu nitelikli elektronik sertifika sahibi taahhütnamesi üzerinde bulunan bilgilerin doğruluğundan sorumludur.

Nitelikli elektronik sertifika başvuru sahibinin, nitelikli elektronik sertifika sahibi taahhütnamesi ve kimlik belgesinden oluşan evraklarını bağlı bulunduğu Şube Müdürüne şahsen onaylatması sonucunda yüz yüze kimlik doğrulama işlemi tamamlanmış olur. Bu evraklar elden veya kurye aracılığıyla Sertifika İrtibat Masasına (SERİM) iletilir. Evrakları alan SERİM Görevlisi başvuru evraklarını kontrol eder ve herhangi bir eksiklik olmaması durumunda Sertifika Hizmetleri Merkezine (SHM) bilgi ve belgelerin gizliliği sağlamak amacıyla kapalı zarfta gönderir.

SHM Görevlisi kimlik belgesi ve KPS üzerinden kimlik doğrulamalarını tamamladıktan sonra başvuruyu değerlendirmeye alır.

4.2. Sertifika Başvurusunun İşlenmesi

4.2.1. Kimlik Tanımlama ve Doğrulama İşlevlerinin Yerine Getirilmesi

Nitelikli elektronik sertifika başvuru sahibinin yüz yüze kimlik doğrulama işlemi bağlı bulunduğu Şube Müdürü tarafından yapılır. SERİM Görevlisi, kimlik doğrulama işlemi sonrasında, başvuru sahibi tarafından elden verilen veya kurye aracılığıyla gönderilen belgelerin tam ve doğru olduğunu kontrol eder. Eksiklik ya da hata olması halinde sistemde ilgili kaydı düşer ve başvuru sahibine bilgi verir.

SERİM Görevlisi tam olan başvuru belgelerini, SHM'ye gönderir. SHM Görevlisi başvuruyu onaylamadan önce ilgili Şube Müdürü onayının olup olmadığını kontrol eder. Sonrasında başvuru sahibinin kimlik tanımlama ve doğrulama işlemlerinin ikinci adımı olarak kimlik belgesi ve KPS üzerinden bilgileri doğrular.

SHM Görevlisi başvuru belgeleri üzerinde herhangi bir tahrifat, hata, eksiklik veya yanlışlıkla karşılaşması halinde başvuru işleme alınmaz. Bu durumda sistemde ilgili kaydı düşer ve SERİM Görevlisine bilgi verir.

4.2.2. Sertifika Başvurusunun Kabul veya Reddi

Kimlik tanımlama ve doğrulama işlemlerinde anlatılan kontroller sonrasında başvuru bilgi ve belgelerinde herhangi bir tahrifat, eksiklik, hata veya yanlışlık bulunması hallerinde başvuru reddedilir. Reddedilen başvurular SERİM Görevlisi aracılığıyla veya doğrudan başvuru sahibine e-posta ya da telefonla bildirilir. Eksikliğin tamamlanması ya da hatanın düzeltilmesinin ardından başvuru tekrar değerlendirmeye alınır.

Kimlik tanımlama ve doğrulama işlemleri tamamlanan başvurular ise sistemde işlenerek üretim süreci başlatılır.

4.2.3. Sertifika Başvurusunun İşlenme Zamanı

Nitelikli elektronik sertifika başvuruları, belgelerde herhangi bir eksiklik olmaması ve kimlik belirleme ve doğrulama adımlarının tamamlanmasının ardından en çok 10 (on) iş günü içinde işlenir.

4.3. Sertifika Oluşturulması

4.3.1. Sertifika Oluşturulmasında ESHS'nin İşlevleri

Nitelikli elektronik sertifika başvuru sahibi, kimlik doğrulama işlemi tamamlandıktan sonra başvuru belgelerini SERİM Görevlisine teslim ederken kabul işlemi gerçekleşiyorsa sistem üzerinde anahtar çifti üretimi tamamlanır, akıllı karta yüklenir ve sertifika başvuru sahibine teslim edilir.

SHM'ye gelen başvurular için gerekli doğrulama adımları tamamlandıktan sonra üretim işlemi yapılır. Sertifika sahibine e-postayla üretim bilgisi gönderilir. Sertifika sahibi daha önce anahtar çifti üretilmiş ve kendisine teslim edilen akıllı kartını kullanarak sertifika yükleme ve aktivasyon işlemlerini yapar.

Üretim öncesinde akıllı kartta sertifika bulunmaması ve kartın aktivasyon işlemlerinin yapılmaması nedeniyle güvenlik sağlanmış olur.

4.3.2. Sertifika Oluşturulmasıyla ile İlgili Sertifika Sahibinin Bilgilendirilmesi

Sertifika üretimi tamamlandıktan sonra, sertifika sahibine e-posta ile üretimin yapıldığı bilgisi gönderilir.

4.4. Sertifikanın Kabulü

4.4.1. Sertifikanın Kabul Koşulu

Nitelikli elektronik sertifika sahipleri, sertifikayı yüklemeden veya kullanmadan önce sertifika içeriğindeki bilgileri gözden geçirmek ve doğrulamakla, doğru olmayan veya başvuruyla tutarsız bilgiler olması durumunda ESHS'yi bilgilendirmek ve sertifikanın iptalini talep etmekle yükümlüdür.

Sertifikanın doğru olmaması ya da bilgilerinde hata olması gibi durumlarda, sertifika sahibinin üretimden sonra 10 (on) iş günü içinde itiraz etmesi gerekir. Bu ve benzeri nedenlerle nitelikli elektronik sertifika sahibinden herhangi bir itiraz gelmezse sertifika kabul edilmiş sayılır.

4.4.2. Sertifikanın ESHS Tarafından Yayımlanması

EGMSM tarafından sunulacak elektronik sertifika hizmeti, yalnızca EGM personelini kapsayan kurumsal bir hizmettir. Bu nedenle EGM bu sertifikaları kamuya açık bir dizinde yayımlamaz.

4.4.3. Sertifikanın Oluşturulmasının Diğer Taraflara Duyurulması

Düzenleme dışıdır.

4.5. Sertifikanın ve İmza Oluşturma Verisinin Kullanımı

4.5.1. Sertifika Sahibinin Sertifika ve İmza Oluşturma Verisini Kullanımı

Nitelikli elektronik sertifika sahibi sertifikasını ve imza oluşturma verisini Kanun, Yönetmelik ve diğer düzenlemeler ile KAMU SM Sİ ve EGM SUE dokümanları ve ilgili sertifika sahibi taahhütnamesinde yer alan koşullar ve belirlenmiş sınırlar içinde kullanılabilir.

Nitelikli elektronik sertifikalarda imza oluşturma verilerinin güvenli elektronik imza oluşturma amacı dışında kullanımından doğan zararlardan ESHS sorumlu tutulamaz. Ayrıca iptal olmuş veya geçerlilik süresi dolmuş sertifikalara ait imza oluşturma verilerini kullanarak yasal geçerliliği olan işlem yapılamaz.

4.5.2. Üçüncü Kişilerin Sertifika ve İmza Doğrulama Verisini Kullanımı

Üçüncü kişiler, güvenecekleri sertifikaların geçerliliğini kontrol etmekle ve sertifikaları Kanun, Yönetmelik ve diğer düzenlemeler ile KAMU SM Sİ ve bu EGM SUE dokümanlarında belirlenmiş kullanım amaçları dâhilinde kullanmakla yükümlüdürler.

4.6. Sertifika Süresinin Uzatılması

Sertifika süresinin uzatılması, sertifika içeriğinde açık anahtar dâhil aynı bilgiler yer almak kaydıyla, sertifika geçerlilik süresinin uzatıldığı yeni bir sertifika üretilmesiyle yapılır. Bu işlem ESHS tarafından gerçekleştirilmez.

4.7. Sertifika Yenileme

Nitelikli elektronik sertifikalarda yenileme işlemi yeni bir başvuru alınarak ve yeni bir anahtar çiftiüreterek gerçekleştirilir.

4.7.1. Sertifika Yenileme Koşulları

Nitelikli elektronik sertifikanın; çalınması, kaybolması, sertifikanın ve anahtar çiftinin yüklü bulunduğu akıllı kartın bozulması, sertifikanın iptal edilmesi, geçerlilik süresinin dolması veya sertifika sahibine ait sertifika içinde bulunan bilgilerde herhangi bir değişiklik olması sonucunda yenileme işlemi yapılır.

4.7.2. Sertifika Yenileme Başvurusunu Kimlerin Yapabildiği

Bölüm 4.1.1'de yer alan esaslar uygulanır.

4.7.3. Sertifika Yenileme Başvurusunun İşlenmesi

Bölüm 4.2'de yer alan esaslar uygulanır.

4.7.4. Sertifika Yenileme ile İlgili Sertifika Sahibinin Bilgilendirilmesi

Bölüm 4.3.2'de yer alan esaslar uygulanır.

4.7.5. Sertifika Yenileme Sonrası Kabul Koşulu

Bölüm 4.4.1'de yer alan esaslar uygulanır.

4.7.6. Sertifika Yenileme Sonrası Sertifikanın Yayımlanması

Bölüm 4.4.2'de yer alan esaslar uygulanır.

4.7.7. Sertifika Yenilemenin Diğer Taraflara Duyurulması

Düzenleme dışıdır.

4.8. Sertifika Bilgi Değişikliği

Sertifika bilgi değişikliği nitelikli elektronik sertifikalarda anahtar çifti hariç sertifikada yer alan bilgilerin değişmesidir. EGM sertifika bilgi değişikliği gerçekleştirmez, bilgi değişikliğinin gerektiği durumlarda yeni bir başvuruyla yeniden sertifika üretilir.

4.9. Sertifika İptali ve Askıya Alınması

4.9.1. Sertifikanın İptal Edildiği Durumlar

Sertifikanın kullanım süresi içinde geçerliliğini kaybetmesi durumunda sertifika iptal edilir. Aşağıda yer alan koşullar sertifikanın iptalini gerektirir:

- Sertifika sahibinin talebi,
- Sertifika başvurusunda veya sertifikada yer alan bilgilerin sahteliğinin veya yanlışlığının ortaya çıkması,
- Sertifika içeriğinde yer alan özne veya sertifika sahibi bilgilerinde bir değişiklik olması,
- Sertifika sahibinin fiil ehliyetinin sınırlandığının veya gaipliğinin veya ölümünün öğrenilmesi,
- Gizli anahtarın kaybedilmesi, çalınması, ortaya çıkma şüphesinin veya üçüncü kişilerin erişimi ve kullanımı tehlikesinin oluşması,
- Gizli anahtara erişim şifresinin ortaya çıkması veya benzer bir nedenle sertifika sahibinin gizli anahtar üzerindeki kontrolünü kaybetmesi,
- Gizli anahtarın içinde bulunduğu yazılım veya donanım aracının kaybolması, bozulması veya güvenilirliğini kaybetmesi,
- EGM'nin sertifikanın KAMU SM Sİ ve EGM SUE dokümanları ile EGM sertifika sahibi taahhütnamesi veya anlaşması hükümlerine aykırı olarak kullanıldığına ilişkin bir bildirim alması veya böyle olduğunun anlaşılması,

- EGM'nin Kanun'a dayalı sertifika verme hakkının ortadan kalkması ve nitelikli elektronik sertifikaların yönetim işlemlerinin başka bir ESHS tarafından devamlılığının sağlanamaması,
- EGM'nin kök veya alt kök sertifikalarına ait gizli anahtarların çıkma şüphesinin oluşması veya açığa çıkması.

4.9.2. Sertifika İptal Başvurusunu Kimler Yapabilir

Sertifika sahibi ve iptal nedenine bağlı olarak EGM yetkilileri nitelikli elektronik sertifika iptal talebinde bulunabilir.

4.9.3. Sertifika İptal Başvurusunun İşlenmesi

Sertifika sahibi ESHS'ye nitelikli elektronik sertifika iptal talebini, yazılı, telefonla çağrı merkezi üzerinden veya web sitesi aracılığıyla olmak üzere farklı yollarla yapabilir. İptal başvurusu hangi yolla yapılmış olursa olsun ESHS tarafından gerçekleştirilmeden önce kimlik doğrulama işlemi yapılır. Kimlik doğrulama işleminin gerçekleştirilemediği durumlarda sertifika iptal edilmez.

Çağrı merkezine gelen iptal taleplerinde, çağrı merkezi operatörü kimlik doğrulama işlemini yaparak sertifika iptalini gerçekleştirir. Bu hizmet 7gün 24 saat esasına göre verilmektedir.

Benzer bir şekilde sertifika sahibi nitelikli elektronik sertifikası için, kamuya açık şekilde duyurulan www.egmsm.gov.tr web adresi üzerinden parolasıyla bağlanarak iptal talebinde bulunabilir. Kimlik doğrulama aşamasını da geçtikten sonra sertifika iptal nedeni girilerek online iptal işlemi tamamlanır. Bu hizmette 7 gün 24 saat esasına göre verilmektedir.

Ayrıca sertifika sahibinin işten ayrılması, vefat vb. durumlarda bağlı bulunduğu Şube Müdürü tarafından resmi yazıyla da sertifika iptal işlemleri başlatılır. SHM'ye ulaşan resmi yazının onayı kontrol edildikten sonra iptal işlemi gerçekleştirilir.

EGM SHM'ye ait bir güvenlik sorunu oluşması, mevcut sertifikalarla ilgili ihbar alınması ya da ESHS'nin iç işleyişinde oluşan bir hatanın fark edilmesi durumlarından birinin gerçekleşmesi halinde, EGM sertifika iptalini başlatabilir. Gereken durumlarda, yeni sertifika üretim işlemleri iptal işleminden sonra hemen yapılır.

İşlem sonrası iptal durumu sertifika sahibine e-posta ile bildirilir.

İptal edilmiş bir sertifikanın yeniden kullanılabilir hale gelmesi veya geçmişe yönelik iptal işlemi yapılması mümkün değildir.

İptal işlemi talep ulaştıktan sonra en kısa sürede tamamlanır ve kamuya ÇİSDUP ve SİL üzerinden duyurulur. Bu kayıtlarda güncelleme ÇİSDUP hizmetinde anlık, SİL hizmetinde ise bir sonraki yayımlamada tamamlanır.

4.9.4. İptal İsteğinin Ertelenme Süresi

Böyle bir süre öngörülmemiştir.

4.9.5. İptal İsteğinin İşlenme Süresi

Çağrı merkezi ve web sitesi üzerinden 7 gün 24 saat esasına göre verilen bu hizmetlerde iptal talepleri, kimlik doğrulama işleminin tamamlanmasının ardından anında sonuçlandırılır. Yazıyla kağıt ortamında alınan sertifika iptal talepleri mesai saatleri içinde derhal değerlendirmeye alınır ve gerekli işlemler ivedilikle tamamlanır. İptal edilen nitelikli elektronik sertifika bilgisi bir sonraki SİL listesinde, ÇİSDUP üzerinden ise derhal duyurulur.

4.9.6. Üçüncü Kişilerin Sertifika İptal Durumunu Kontrol Gerekliliği

Üçüncü kişiler, kendilerine gönderilen bir elektronik imzaya güvenmeden önce, ilgili sertifikayı doğrulamakla yükümlüdür. Sertifika durumunun doğrulanması için, EGM tarafından ücretsiz, kamuya açık ve kesintisiz şekilde yayımlanan güncel SİL ya da ÇİSDUP servisi kullanılmalıdır.

Üçüncü kişiler nitelikli elektronik sertifika geçerlilik kontrolü yaptığı SİL dosyasının veya ÇİSDUP Yanıtlayıcıdan aldığı iptal durum kaydının EGM'ye ait imza oluşturma verisiyle imzalandığını kontrol eder.

4.9.7. Sertifika İptal Listesi (SİL) Yayımlama Sıklığı

EGM nitelikli elektronik sertifikalar için sertifika durumlarında hiçbir değişiklik olmasa bile, günde en az bir kez yeni bir SİL yayımlar. SİL, 12 (on iki) saatte bir olmak üzere günde 2 (iki) kez ve 24 (yirmi dört) saatlik geçerlilik süresiyle yayımlanır.

Alt kök sertifikalarına ait SİL'ler, bir alt kök sertifika iptali durumunda veya sertifika iptali olmasa bile yılda en az bir kez yayımlanır.

4.9.8. Sertifika İptal Listesi Yayımlama Gecikme Süresi

SİL'ler üretildikleri andan itibaren en geç 5 (beş) dakika içinde yayımlanır.

4.9.9. Çevrim İçi Sertifika İptal Durum Kaydı Desteği (ÇİSDUP)

EGM, nitelikli elektronik sertifikaların iptal durum bilgisi için SİL'in yanı sıra kesintisiz çevrim içi sertifika durum protokolü ÇİSDUP desteği verir. ÇİSDUP üzerinden yayımlanan iptal durum kayıtları EGM'ye ait olduğu duyurulan imza oluşturma verisiyle imzalanır.

4.9.10. Çevrim İçi Sertifika İptal Durum Kaydı Kontrol Gereksinimi

Üçüncü kişilerin sertifika durum sorgusu yaparken, eğer teknik imkânları yeterliyse ÇİSDUP'u tercih etmeleri, SİL'i ikinci alternatif olarak seçmeleri gerekir.

4.9.11. Diğer Sertifika Durum Bildirim Yöntemleri

EGM, ÇİSDUP ve SİL dışında iptal durumu yayımlama yöntemi kullanmaz.

4.9.12. İmza Oluşturma Verisinin Güvenliğini Yitirilmesi Durumu

Nitelikli elektronik sertifikalar için, imza oluşturma verisinin güvenliğini yitirmesi durumunda EGM tarafından sertifikalar iptal edilir. İptal işlemi dışında başka herhangi bir işlem öngörülmemiştir.

4.9.13. Sertifika Askıya Alındığı Durumlar

Askıya alma işlemi sertifikanın geçici süre, iptal edilen bir sertifika gibi hukuksal olarak geçerli bir işlem oluşturamaz hale getirilmesidir.

EGM sertifika sahibinin isteğiyle veya bir sertifika iptal talebinin kaynağının doğrulanamadığı durumlarda doğrulama işlemi sonuçlanıncaya kadar, iptal işlemi yapmak yerine ilgili sertifikayı askıya alır.

ESHS'ye ait sertifikalar askıya alınmaz.

4.9.14. Sertifika Askıya Alma Başvurusunu Kimlerin Yapabildiği

Bölüm 4.9.2'de yer alan esaslar uygulanır.

4.9.15. Sertifika Askıya Alma Başvurusunun İşlenmesi

Bölüm 4.9.3'de yer alan esaslar uygulanır.

4.9.16. Askıda Kalma Süresi

EGM'nin, bir sertifika iptal talebinin kaynağının doğrulanamadığı durumlarda askıya aldığı sertifikalar, doğrulama işlemi sonuçlanıncaya veya süre sınırı aşılana kadar askıda bırakılır. Sertifika sahipleri tarafından iptali gerektiren bir durumun olup olmadığından emin olunamadığında askıya alınan sertifikalar, sertifika sahibinden iptal gerekliliği onaylandığında iptal edilir.

Her iki durumda da, askıya alma süresi 30 (otuz) günü aşamaz. Bu sürenin sonunda hala askıda bulunan sertifikalar, güvenlik nedeniyle otomatik olarak iptal edilir.

Sertifikaların askıda bulunduğu süre içinde, iptali gerektiren bir durumun olmadığı anlaşılırsa, sertifika askıdan çıkarılarak tekrar geçerli duruma alınabilir.

4.10. Sertifika Durum Servisleri

Üçüncü kişiler sertifika iptal durum kayıtlarına SİL ve ÇİSDUP üzerinden ulaşır.

4.10.1. İşletimsel Özellikleri

SİL'ler, 12 (oniki) saatte bir olmak üzere günde 2 (iki) kez ve 24 (yirmidört) saatlik geçerlilik süresiyle, sertifika durumlarında hiçbir değişiklik olmasa bile yayımlanır. Kamuya açık şekilde bilgi deposunda yayımlanan SİL dosyalarında bir sonraki güncelleme tarihi belirtilir.

ÇİSDUP sorgusunda ise, gerçek zamanlı sertifika durum (geçerli, askıda, iptal, süresi dolmuş/bilinmiyor) bilgisi alınabilir.

4.10.2. Servisin Erişilebilirliği

EGM, SİL ve ÇİSDUP hizmetlerini kesintisiz olarak 7 gün 24 saat ilkesine göre verir.EGM kesintisiz hizmet verebilmek için yedek sistemlerle gereken tüm tedbirleri alır. Bu önlemlere rağmen herhangi bir kesintinin oluşması halinde üçüncü tarafların işlemlerini durdurması önerilir ve iptal durum kaydı kontrol edilmeden kabul edilen işlemlerden doğan zararlardan EGM sorumlu tutulamaz.

4.10.3. İsteğe Bağlı Özellikler

Düzenleme dışıdır.

4.11. Sertifika Sahipliğinin Sona Ermesi

Nitelikli elektronik sertifikanın geçerlilik süresinin dolması, iptal edilmesi veya EGM'nin sertifika hizmetlerini sonlandırması sırasında başka bir ESHS tarafından devamlılığının sağlanamaması durumlarında gerçekleşir. EGM sertifika sahibinin talebi veya ESHS faaliyetinin sona ermesinden dolayı yapılan iptallerde sertifika sahibini bilgilendirir.

4.12. Anahtar Yeniden Üretme

Nitelikli elektronik sertifika sahiplerine ait anahtarların yeniden üretilmesi ya da yedeklenmesi işlemi uygulanmamaktadır.

5. YÖNETİM, İŞLEMSEL VE FİZİKSEL KONTROLLER

Bu bölümde EGM'nin nitelikli elektronik sertifika hizmetlerini yürütürken uygulamak zorunda olduğu teknik olmayan güvenlik kontrolleri yer almaktadır.

5.1. Fiziksel Güvenlik Denetimleri

EGM, ESHS faaliyetlerini çerçevesinde kullandığı cihaz ve alanlar için dış tehditlere karşı korunaklı, yetkisiz erişimi engelleyecek güvenli bir alan oluşturulmuştur.

5.1.1. Tesis Yeri ve İnşaatı

EGM, ESHS faaliyetlerini sürdürdüğü alanlarda kurumun kendi özelliklerinden kaynaklanan yüksek güvenlik önlemlerine sahiptir.

5.1.2. Fiziksel Erişim

EGM, ESHS faaliyetlerini yürüttüğü alanlarda fiziksel erişimi denetim altında tutar ve sürekli olarak kontrol eder.

Tesise dışarıdan kontrolsüz giriş ve çıkış önlenmiştir. Bina dışarıdan gelebilecek saldırılara karşı da korumalıdır. ESHS donanım ve modüllerinin bulunduğu alanlar ve arşiv kartlı geçiş kontrol sistemi ve bazı yerlerde biyometrik kontrollerle yetkisiz erişime karşı korunaklı hale getirilmiştir. Ayrıca ek güvenlik önlemi olarak kritik bölge ve geçişler sürekli kameralarla izlenir ve kamera çekim kayıtları güvenlik gereklilikleri nedeniyle saklanır. Bu sistemlerle giriş çıkışlar kontrol ve kayıt altına alınmıştır.

5.1.3. Güç Kaynağı ve Havalandırma

EGM, ESHS faaliyetlerindeki kesintisizlik prensibi gereğince tüm donanım ve teçhizat için güç kaynakları oluşturmuştur. Kesinti sırasında devreye girecek güç kaynakları ve jeneratörlerin bakımları düzenli olarak yapılmaktadır.

Binanın kapasitesine uygun olarak havalandırma sağlanmaktadır.

5.1.4. Su Baskınları

Binanın su baskınına karşı gerekli yalıtımı yapılarak koruma önlemleri alınmıştır.

5.1.5. Yangın Önleme ve Korunma

ESHS faaliyetlerinin sürdürüldüğü alanlar için yangın önleyici önlemler alınmıştır. Binada sigara içme yasağı uygulanmakta, yıldırım etkisine bağlı paratoner kurulumu yapılmış ve elektrik sistemleri için önlemler alınmıştır.

5.1.6. Saklama ve Yedekleme Ortamlarının Korunması

EGM, ESHS faaliyetleri kapsamında tüm kayıtların yedeklerini uygun ortamlarda tutar ve korur.

5.1.7. Atıkların Yok Edilmesi

Temel sertifika hizmetlerine bağlı, elektronik veya kâğıt ortamda saklanan tüm bilgi ve belgeler, saklanmaları gerekmiyorsa tamamen imha edilerek atılır.

5.1.8. Farklı Mekanlarda Yedekleme

EGM, ESHS faaliyetleri kapsamında iş sürekliliğini sağlayabilmek amacıyla, herhangi bir problem anında sistemlerini yeniden işletebilmek için elektronik işlem kayıtlarının yedeklerini tesis dışında güvenli şekilde saklar.

5.2. Prosedürsel Kontroller

5.2.1. Güvenilir Roller

EGM, ESHS faaliyetleri kapsamında görev alan personelin organizasyonunun sağlanması amacıyla, tüm sertifika iş süreçlerinin yürütülmesinde görev alacak güvenilir roller belirlenmiştir.

- **EGM SHM Yöneticisi:** EGM sertifika hizmetlerinin yürütülmesinden idari açıdan sorumlu yöneticilerdir.

- **EGM SHM Teknik Sorumlusu:** EGM sertifika hizmetlerinin yürütülmesinden teknik açıdan sorumlu yöneticilerdir.
- **Güvenlik Yöneticisi:** Güvenlik politikaları ve uygulamalarının yönetimi ve yürütülmesinden sorumlu yöneticilerdir.
- **Güvenlik İşletmeni:** Dışarıdan gelecek ataklara karşı güvenlik duvarları, saldırı tespit sistemi, kayıt sistemi ve antivirüs sistemlerinin yöneticilerin verdiği talimatlar doğrultusunda oluşturulmasından ve sürekliliğinin sağlanmasından sorumlu çalışanlardır.
- **Sistem Yöneticisi:** Güvenlik bileşenleri hariç sertifika hizmetlerine ilişkin sistemlerin kurulumu, konfigürasyonu ve devamlılığının sağlanması ve aynı zamanda sistem yedekleme ve geri yükleme işlemleri için yetkilendirilmiş yöneticilerdir.
- **Sistem İşletmeni:** Nitelikli elektronik sertifika hizmetlerine ilişkin bütün sunucuların işletim sistemi ve donanım idamesinden ve güncellemesinden sorumlu çalışanlardır.
- **Veri Sistemleri Yöneticisi:** Dizin ve veri tabanı yığınlarının yönetimini yapar. Veri tabanı yönetim faaliyetlerini gerçekleştirir.
- **Sertifika Üretim Ekip Lideri:** Nitelikli elektronik sertifika hizmetlerinde üretimin planlanması, gerçekleştirilmesi ve sertifika sahibine ulaştırılmasıyla ilgili tüm çalışmaları yapar.
- **SHM Üretim Yetkilileri:** Nitelikli elektronik sertifika yaşam döngüsü içinde üretim işlemlerinden sorumlu ve prosedürler uyarınca gerçekleştiren çalışanlardır.
- **SERİM ve SHM Görevlileri:** Evrak kontrolü, sertifika başvuru kaydı, askıya alma ve iptal gibi rutin sertifika hizmetlerinden sorumlu çalışanlardır.
- **Denetçi:** Nitelikli elektronik sertifika hizmetlerine ilişkin sistem denetim profilinin kurulması, denetim yönetimi ve gözden geçirilmesiyle ilgili sistem teknik ve idari işleyişinin kontrolü ve raporların hazırlanmasından sorumlu çalışanlardır.

5.2.2. Her İşlem İçin Gereken Kişi Sayısı

EGM sertifika üretim işlemleri, en az iki yetkilinin hazır bulunmasıyla sonuçlandırılabilmektedir.

Yukarıda belirtilen rutin sertifika üretim adımları dışında, alt kök sertifikalarıyla ilgili her türlü üretim, yenileme, iptal ve yedekleme işleminde en az iki yetkilinin hazır bulunmasıyla yapılabilmektedir.

5.2.3. Kimlik Doğrulama ve Yetkilendirme

EGM, ESHS faaliyeti kapsamında çalışan personelinin ilgili alanlara ve sistemlere erişiminde kimlik doğrulamasını çeşitli yöntemlerle mutlaka yapar. Böylelikle her alan veya sistem için yetkilendirilmiş personel yetkisi çerçevesinde erişim sağlamış olur. Kimlik doğrulama işlemeleri genel olarak nitelikli elektronik sertifika kullanımı, akıllı kart sistemleri, biyometrik veri kullanımı, şifre veya parola kullanımı vb. yöntemler şeklinde tanımlanmıştır.

5.2.4. Görevlerin Ayrılmasını Gerektiren Roller

Nitelikli elektronik sertifika yaşam döngüsü içinde bir birini takip eden işler birbirinden farklı kişiler tarafından yapılır. Böylelikle bir kişinin işin tamamını yapması engellenmiş olur.

Özellikle, “Güvenlik İşletmeni” veya “Güvenlik Yöneticisi” veya “Sertifika Üretim Ekip Lideri” veya “Sertifika Üretim İşletmeni” olarak yetkilendirilmiş bir kişi, “Denetçi” olarak yetkilendirilemez. “Sistem Yöneticisi” olarak yetkilendirilmiş bir kişiyse, “Güvenlik İşletmeni” veya “Güvenlik Yöneticisi” veya “Denetçi” olarak yetkilendirilemez.

5.3. Personel Güvenlik Kontrolleri

5.3.1. Kişisel Geçmiş, Deneyim ve Nitelik Gerekleri

EGM, ESHS faaliyetlerinde çalışan personeli, sertifika süreçlerinin işleyişini sağlayabilecek nitelikte, göreve uygun eğitim düzeyine sahip, konusunda bilgili ve eğitimli, benzer çalışma alanlarında deneyimli ve güvenlik kontrollerinden geçmiştir.

5.3.2. Geçmiş Araştırması

EGM kurum niteliği nedeniyle, çalışan personeline ait geçmiş araştırmalarını tereddütsüz yapmakta ve personelin işe teknik ve idari açıdan uygunluğundan emin olmaktadır.

5.3.3. Eğitim Gerekleri

EGM, ESHS faaliyetleri kapsamında her kademede çalışacak personelini, göreve başlamadan önce sorumlulukları kapsamında eğitimden geçirir. Eğitim süresince personel, genel olarak bilgi güvenliği ve ESHS faaliyetleri açısından bilgilendirilirken, ayrıca her personel görevine özel şekilde eğitilir.

5.3.4. Sürekli Eğitim Gerekleri ve Sıklığı

Mevcut personel periyodik ve ESHS faaliyetleri kapsamında yapılan değişiklikler ve iyileştirmelerle ilgili olarak, eğitimlerle bilgilendirilir. Ayrıca göreve yeni başlayan personel için mutlaka eğitim düzenlenir.

5.3.5. Görev Değişim Sıklığı ve Sırası

Düzenlenmesine gerek duyulmamıştır.

5.3.6. Yetkisiz Eylemlerin Cezalandırılması

EGM, personelinin teşebbüs edeceği yetkisiz işlemler için mevzuat uyarınca işlem yapar.

5.3.7. Anlaşmalı Personel Gereksinimleri

EGM verdiği hizmetlerde herhangi bir dış kaynak kullanımında bulunmadığı için düzenleme gereği duyulmamıştır.

5.3.8. Sağlanan Dokümantasyon

EGM personeline, Sİ ve SUE dokümanları gibi kamuya açık dokümanlar sağladığı gibi, göreve özel talimat veya kılavuz düzeyinde de dokümanlar sağlar.

5.4. Denetim Kayıtları

Sertifika yaşam döngüsü içinde yürütülen tüm sertifika hizmetlerine ait kayıtlar EGM tarafından tutulur. Gerektiğinde denetimler sırasında incelenebilecek bu kayıtlar elektronik ortamda veya kağıt üzerinde bulunur.

5.4.1. Kaydedilen İşlemler

EGM tarafından tutulan kayıtlar arasında sertifika başvuru ve başvuru onay kayıtları; üretilen, yenilenen, askıya alınan ve iptal edilen sertifikalarla ilgili her türlü sertifika sahibi talebinin kayıtları; üretilip yayımlanan sertifikalar ile SİL'ler hakkındaki kayıtlar; güvenilir rollere sahip çalışanların işlem kayıtları; çalışanların birimlerine giriş ve çıkış kayıtları ile sistem modüllerine erişim kayıtları; doküman takibiyle ilgili kayıtlar; yazılım ve donanım kurulum, güncelleme ve onarım kayıtları sayılabilir.

5.4.2. Kayıtları İncelenme Sıklığı

EGM ESHS faaliyeti kapsamındaki kayıtları sürekli olarak tutar ve periyodik olarak bu kayıtlar incelenir.

5.4.3. Kayıtların Saklanma Süresi

Kayıtlar incelendikten sonra en az 2 (iki) ay sistemde tutulur ve daha sonra arşivlenir.

5.4.4. Kayıtların Korunması

Kayıtlar izlenmeyi, silinmeyi, tahrif edilmeyi, değiştirilmeyi engelleyecek şekilde fiziksel ve elektronik güvenlik önlemleriyle korunur, sadece yetkili kişilerin erişimine açık tutulur.

5.4.5. Kayıtların Yedeklenmesi

Yedekleme prosedürleri uyarınca, kayıtların periyodik olarak tesis içi ve tesis dışı yedekleri alınır.

5.4.6. Kayıtların Toplanması

Elektronik kayıtlar ESHS yönetim yazılımı tarafında, kağıt kayıtlar ise ilgili personel tarafından dosyalanarak tutulur.

5.4.7. Kayda Sebebiyet Veren Tarafın Bilgilendirilmesi

Rutin işlemlerin dışında kalan denetim kayıtlarının oluştuğu durumlarda, olayı yaratan kişi sistem tarafından bilgilendirilir.

5.4.8. Saldırıya Açıklığın Değerlendirilmesi

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

5.5. Kayıt Arşivleme

5.5.1. Arşivlenen Kayıt Bilgileri

EGM, ESHS faaliyetleri kapsamında, Madde 5.4'te belirtilen tüm denetim kayıtları, sertifika süreçlerine yönelik başvuru, talep ve talimatlar, kağıt üzerinde alınan tüm destekleyici belgeler ile sertifika sahibi taahhütnamesi, üretilen tüm sertifikalar ve SİL'ler, Sİ ve SUE dokümanlarının tüm sürümleri, uygulama prosedürlerinin, talimatların ve formların bütünü, geçerlilik süresinin sona ermesinden itibaren ESHS sertifikaları, sertifika yönetimine ilişkin tüm işlemlere, bu işlemlerin yapıldığı zamana ve işlemleri yapan kişiye veya kişilere ait bilgileri içeren kayıtlar, EGM "Doküman ve Kayıt Kontrol Prosedürü" uyarınca arşivlenir. Arşivlerin büyük bir kısmı elektronik ortamda tutulurken, kağıt üzerindeki formlar, belgeler, sertifika sahibi dosyaları gibi kayıtlar da kağıt ortamında arşivlenir.

5.5.2. Arşivlerin Tutulma Süresi

NES'lerle ilgili kağıt, elektronik ve her türlü kayıtlardan oluşan arşivler, yasal düzenlemeler uyarınca en az 20 (yirmi) yıl süreyle saklanır.

5.5.3. Arşivlerin Korunması

Arşivler fiziksel ve elektronik güvenlik önlemleriyle korunur, sadece yetkili kişilerin erişimine açık tutulur.

5.5.4. Arşivlerin Yedeklenmesi

Yedekleme prosedürleri uyarınca, elektronik ortamdaki arşivlerin yedekleri tutulur. Kağıt ortamdaki arşivlerin ise yedekleri alınmaz.

5.5.5. Kayıtların Zaman Damgası Gereksinimleri

EGM, ESHS faaliyetleri kapsamında gerekli gördüğü kayıtlara zaman damgası ekleyebilir.

5.5.6. Arşivlerin Toplanması

Arşiv kayıtları, "Doküman ve Kayıt Kontrol Prosedürü" uyarınca derlenir.

5.5.7. Arşiv Bilgilerinin Elde Edilme ve Doğrulanma Metodu

EGM ESHS faaliyetleri kapsamında bulunan arşiv bilgilerine, ilgili düzenlemeler ve yasal süreçlerin bir gereği olarak kontrollü erişim sağlanır.

5.6. Anahtar Değişimi

EGM'ye ait alt kök sertifikalar ve bunlara bağlı anahtarlar iki nedenden yenilenebilir. Bunlar; geçerlilik süresinin dolması veya güvenlik gerekliliklerdir.

Alt kök sertifikaların süresi sonuna yaklaşıldığında, üretilecek son kullanıcı sertifikalarının geçerlilik süresi, bağlı bulunduğu alt kök sertifikanın son kullanma tarihini geçmeyecek biçimde verilir. Bu nedenle, alt kök sertifika anahtar çiftinin geçerlilik süresinin bitmesine, en uzun süreli sertifikanın geçerlilik süresi kadar kalmasından 1 (bir) yıl önce Kamu SM ile iletişime geçilir ve ilgili prosedürler uyarınca alt kök sertifikanın üretim işlemleri yapılır.

Eski anahtarlar geçerlilik süresinin sonuna kadar kullanılabilir durumda saklanır. Bu anahtar çiftinden üretilen sertifikaların doğrulanabilmesi için EGM eski sertifikasını da yayımlamaya devam eder. SİL dosyası aynı imza oluşturma verisiyle imzalanıyorsa bu anahtar çiftinden verilen son kullanıcı sertifikalarının geçerlilik süreleri dolana kadar EGM SİL'lerini eski imza oluşturma verisiyle imzalamaya devam eder.

Güvenlik gereklilikleri nedeniyle anahtar değişimine gidilmesi halinde ise yeni alt kök sertifika Kamu SM'den talep edilir. Bu sertifika sağlanana kadar son kullanıcı sertifikası üretimi durdurulur.

5.7. Güvenliğin Yitirilmesi ve Arıza Durumunda Yapılacaklar

5.7.1. Güvenilirliğin Yitirilmesi Durumunun Düzeltilmesi

EGM güvenilirliğin yitirilmesi durumunda iş sürekliliği yönetimi ve planı uyarınca en kısa sürede duruma müdahale eder.

5.7.2. Donanım, Yazılım veya Veri Bozulması

EGM, ESHS faaliyetleri kapsamında donanım veya yazılım arızalarında öncelikle tesisteki hasarlı donanım yeniden işler hale getirilir. Daha sonra, kaybolan kayıtlar yedekleme sistemleri aracılığıyla yeniden oluşturulur ve sertifika hizmetleri tekrar etkin hale getirilir. Eğer tam olarak işler hale getirilemez veya kayıtların bazıları yeniden elde edilemez ise, bu durumdan etkilenebilecek olan bütün sertifika sahipleri ile üçüncü kişiler ivedilikle bilgilendirilir. Gerekli durumlarda bazı sertifikalar iptal edilip yeni sertifika üretimine geçilir.

5.7.3. İmza Oluşturma Verisinin Gizliliğinin Kaybedilmesi

EGM imza oluşturma verilerinin gizliliğini kaybetmesi durumunda, iş sürekliliği planları uyarınca, ilgili sertifikalar iptal edilir ve Madde 5.6 uyarınca yeni imza oluşturma verisi oluşturularak devreye alınır. EGM'ye ait sertifikanın iptal edildiğine dair http://www.egmsm.gov.tr adresinden duyuru yapılır ve ilgili kurum ve birimler yazıyla bilgilendirilir.İptal edilen sertifikaların yerine prosedürler gereği yeni sertifikalar üretilir ve bu durumdan etkilenebilecek olan bütün sertifika sahipleri ile üçüncü kişiler ivedilikle bilgilendirilir.

5.7.4. Arıza Sonrası Yeniden Çalışırlık

EGM, ESHS faaliyetleri kapsamında merkezi dışında felaket kurtarma merkezi (FKM) tesis etmiştir. Afet sonrasında iş sürekliliğini temin etmek üzere merkezinde bulunan veriler yedeklenir. Özellikle, bir ihtiyacın ortaya çıkması durumunda FKM aracılığıyla OCSP veya CRL gibi gerçek zamanlı web hizmetleri en fazla 2 (iki) saatlik sürede hazır hale getirilebilir.

5.8. Sertifika Hizmetlerinin Sonlandırılması

EGM, ESHS faaliyetlerinin son bulması halinde, Kanun ve Yönetmelik gereği bu durumu en az 3 (üç) ay önce Kuruma bildirir ve kamuoyuna duyurur. ESHS işletmenin durdurulması prosedürü uyarınca, mevcut sertifikalarla ilgili tüm bilgi, belge ve kayıtları, Kanun gereği bir ay içinde başka bir ESHS'ye devreder. Kurum, uygun görmesi halinde, bir ayı geçmemek üzere ek süre verebilir. Eğer devir işlemi belirtilen süreler içinde tamamlanamazsa, EGM ilgili sertifikaları iptal eder ve tüm ilgili tarafları genel duyuru ve sertifika sahiplerine doğrudan e-posta aracılığıyla haberdar eder.Bu durumda, EGM son SİL kaydını oluşturduktan sonra kendi imza oluşturma verisi ile yedeklerini imha eder.

6. TEKNİK GÜVENLİK KONTROLLERİ

EGM'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

EGM, alt kök sertifikalarına ait anahtar çiftleri, üst düzey bir yöneticinin ve TÜBİTAK BİLGEM Yetkilileri'nin talebi ve EGM SH Yetkililerinin kabulü halinde Kamu SM Yetkililerinin gözetiminde, en az iki yetkilinin bir araya gelmesiyle, sadece görevli personelin girebileceği erişim yetkisi sınırlanmış alanlarda, alt kök sertifika üretim prosedürü uyarınca üretilir ve uygun biçimde yedeklenir. İmza oluşturma verisi yetkisiz erişime karşı fiziksel ve teknik güvenlik önlemleriyle korunur. İki yetkilinin hazır bulunmasıyla ilgili kontroller, şifre kontrolleri ve biyometrik yöntemlerle sağlanır. Sistem, sadece her iki yetkilinin de, şifrelerini ve biyometrik verilerini kullanarak sırayla sisteme giriş yapmasıyla çalışır hale gelir.

Alt kök sertifikaların anahtar çifti üretiminde en az EAL4+ veya FIPS 140-2 Düzey 3 güvenlik düzeyinde kriptografik güvenlik donanım modülü kullanılır. Anahtar çiftlerinin uzunluğu ve kullanılacak algoritmalar güncel mevzuat ve standartlarla uyumlu olacak şekilde belirlenir. Aynı şekilde üretilen anahtar çiftinin ömrü güncel mevzuat, standartlar ve anahtarların kriptografik güvenlik süresiyle sınırlandırılmıştır.

6.1.1.2. Sertifika Sahibi Anahtar Çiftinin Üretimi

Sertifika sahibi için üretilecek anahtar çiftleri en az iki yetkilinin bir araya gelmesiyle, sadece görevli personelin girebileceği erişim yetkisi sınırlanmış alanlarda, özel ve güvenli bir yazılım kullanılarak üretilir ve şifrelenerek güvenli imza oluşturma aracının içinde saklanır.

Anahtar üretiminde kullanılan algoritmalar ve anahtar uzunlukları Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de belirtilen şekilde seçilir.

EGM'de herhangi bir sertifika sahibine ait imza oluşturma verisinin yedeği alınmaz, kopyalanmaz ya da veri tabanında tutulmaz. İmza oluşturma verisinin yüklü bulunduğu güvenli imza oluşturma aracı sertifika sahibine teslim edilene kadar yetkisiz erişime karşı korunur.

6.1.2. Sertifika Sahibine İmza Oluşturma Verisinin Ulaştırılması

EGM, sertifika sahibi için oluşturduğu ve güvenli elektronik imza oluşturma aracının içinde bulunan imza oluşturma ve doğrulama verilerini, sertifika sahibine kimlik kontrollü ve imza karşılığında teslim eder.

Sertifika üretimi sonrasında sertifika sahibi ilgili web sitesi üzerinden kendi için tanımlanan özel alana giriş yaparak güvenli elektronik imza oluşturma aracına nitelikli elektronik sertifikasını yükler.

Güvenli elektronik imza oluşturma aracına erişim verisi, sertifika sahibi tarafından sertifika üretimi sonrasında aktivasyon işlemi ile tanımlanır.

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

Anahtar çiftleri ESHS tarafından üretildiği için imza doğrulama verisinin sertifika sahibi tarafından ESHS ye ulaştırılmasına gerek yoktur.

6.1.4. EGM İmza Doğrulama Verilerinin Üçüncü Kişilere Ulaştırılması

EGM alt kök sertifikasını üçüncü kişilerin erişebileceği şekilde http://www.egmsm.gov.tr adresinde yayımlar. Bu sertifikalara ait SHA-1 özeti Türkiye'de yayınlanan en yüksek tirajlı 3 (üç) gazetede yayımlanır. Böylelikle, EGM'ye ait imza doğrulama verileri üçüncü kişilerce kullanılabilir.

6.1.5. Anahtar Uzunlukları

EGM alt kök sertifikası, son kullanıcı sertifikaları ve iptal durum kayıtlarını imzalamak için kullanılan RSA anahtar çiftlerinin boyu Tebliğ'le belirlenen minimum anahtar uzunluklarına uygun olarak 2048 bittir.

6.1.6. Anahtar Üretim Parametreleri ve Kalitesinin Kontrolü

Anahtar çifti uygun güvenlik düzeyine sahip donanım güvenlik modüllerinde, Tebliğ'de belirlenen parametrelere uygun olarak üretilir.

6.1.7. Anahtar Kullanım Amaçları

EGM ESHS hizmetleri kapsamında üretilen son kullanıcı anahtarları, kimlik doğrulama ve elektronik imza amaçlı kullanılır.

EGM alt kök sertifikalarına ait anahtarlar, sertifika ve SİL imzalamak için kullanılır.

Anahtarların kullanım amacı, X.509 v3 sertifikaların anahtar kullanım alanlarında belirtilir.

6.2. İmza Oluşturma Verisinin Korunması

6.2.1. Kriptografik Modül Standartları

EGM anahtar çifti üretimi ile sertifika ve SİL imzalama işlemleri, Tebliğ'le belirlenen standartlarla uyumlu, güvenli kriptografik donanım modüllerinde gerçekleştirilir.Cihazların tüm kullanım ömürleri boyunca, cihazlar işlevsellikleriyle ilgili sürekli kontrol altında tutulur ve herhangi bir güvenlik ihlali durumu bilgi güvenliği ihlal olayı prosedürü uyarınca yönetilir.

NES sahiplerinin imza oluşturma verileri, Tebliğ'le belirlenen standartlarda güvenlik düzeyine sahip akıllı kartlara, akıllı çubuklara ve benzeri güvenli elektronik imza oluşturma araçlarına yüklenir. Güvenli elektronik imza oluşturma araçlarındaki imza oluşturma verilerinin dışarıya çıkarılması, değiştirilmesi veya kopyalanması engellenmiştir.

6.2.2. İmza Oluşturma Verisine Birden Fazla Kişi Kontrolünde Erişim

Fiziksel ve teknik erişim kontrollerinin yanı sıra, EGM'ye ait imza oluşturma verilerinin kullanımı, ilgili modüle aynı anda iki ayrı yetkilinin bağlanması ve sistem tarafından onaylanmasıyla mümkündür.

NES imza oluşturma verileri sadece sertifika sahiplerinin kendi sorumluluğu altındaki, şifre kontrollü güvenli elektronik imza oluşturma araçlarında saklanır. Aracın şifresi bilinmediği sürece imza oluşturma verisi kullanılamaz. Şifre güvenliği araç donanımı tarafından sağlanır.

6.2.3. İmza Oluşturma Verisinin Yeniden Elde Edilmesi

Düzenleme dışıdır.

6.2.4. İmza Oluşturma Verisinin Yedeklenmesi

Üretilen son kullanıcı sertifikalarına bağlı imza oluşturma verileri yedeklenmez, bu verilerin kopyası alınmaz.

Herhangi bir afet durumu veya sorun anında hizmetlerin kesintiye uğramaması amacıyla, alt kök sertifikasına bağlı imza oluşturma verisi,alt kök sertifikaları anahtar üretim prosedürü uyarınca yedeklenir ve fiziksel ve teknik güvenlik kontrolleri altında saklanır.

Alt kök sertifikalarına bağlı gizli anahtarlar, EAL4+ veya FIPS 140-2 Düzey 3 sertifikalı güvenli donanımlarda (token) yedeklenir. Herhangi bir yeniden kullanım ihtiyacında, bu donanımlar gizli anahtarların ilgili donanım güvenlik modüllerine geri yüklenmesi için, yetkili kişiler tarafından gerekli erişim bilgileri girilerek kullanılır.

6.2.5. İmza Oluşturma Verisinin Arşivlenmesi

EGM veya sertifika sahiplerine ait imza oluşturma verileri arşivlenmez.

6.2.6. İmza Oluşturma Verisinin Kriptografik Modüle Yüklenmesi

ESHS alt kök sertifikalarına ait imza oluşturma verileri güvenli kriptografik donanım modüllerinde üretilir. Bu veriler yedekleme amacıyla kullanılan güvenli modüllere transferi dışında hiçbir biçimde modül dışına çıkarılamaz. Yedekleme işlemi, kriptografik donanım modülü üzerinde şifreli bir biçimde gerçekleştirilir.

Anahtar çifti uygun güvenlik düzeyine sahip güvenli kriptografik donanım modüllerinde üretilir ve NES sahiplerinin güvenli elektronik imza oluşturma araçlarına güvenli yollarla taşınır.

6.2.7. İmza Oluşturma Verisinin Kriptografik Modülde Saklanması

Alt kök sertifikalarına bağlı imza oluşturma verileri, üretildikleri ve Tebliğ'de tanımlı güvenlik düzeyine sahip kriptografik donanım modüllerinde saklanır.

Sertifika sahiplerinin imza oluşturma verileri, üretildikleri Tebliğ'de tanımlı güvenlik düzeyine sahip güvenli elektronik imza oluşturma araçlarında saklanır. Güvenli elektronik imza oluşturma araçlarındaki imza oluşturma verisinin dışarıya çıkarılması, değiştirilmesi veya kopyalanması engellenmiştir.

6.2.8. İmza Oluşturma Verisine Erişim

Alt kök sertifikasına bağlı imza oluşturma verileri, içinde bulundukları donanım güvenlik modülü üzerinde, iki yetkilinin hazır bulunmasıyla aktive edilir.

Nitelikli elektronik sertifikalara bağlı imza oluşturma verileri, güvenli elektronik imza oluşturma aracı üzerinde şifre girişiyle aktive edilir.

6.2.9. İmza Oluşturma Verisine Erişimin Kesilmesi

Alt kök sertifikasına bağlı imza oluşturma verileri, içinde bulundukları donanım güvenlik modülü üzerinde sadece belirli bir süreyle ve işlem bazlı aktive edilir; işlem tamamlandıktan ya da işlem süresi bittikten sonra deaktive olur. İmza oluşturma verisinin yeniden kullanılabilmesi için, yetkililerin tekrar sisteme tanıtılarak imza oluşturma verisinin aktive edilmesi gerekir.

Nitelikli elektronik sertifikalara bağlı imza oluşturma verileri güvenli elektronik imza oluşturma aracı üzerinde şifre girişiyle belirli bir süre için aktive edilir ve işlem süresi sonunda de aktive olur. Ayrıca, sertifika sahibi kendi isteğiyle de imza oluşturma verisini deaktive edebilir. İmza oluşturma verisinin yeniden kullanılabilmesi için, sertifika sahibinin güvenli elektronik imza oluşturma aracı şifresini tekrar girmesi gerekir.

6.2.10. İmza Oluşturma Verisinin Yok Edilmesi

Alt kök sertifikalarına bağlı imza oluşturma verileri, sertifika geçerlilik süreleri sonunda, içinde bulundukları donanım güvenlik modüllerinin sıfırlama özelliği kullanılarak sadece yetkili kişiler tarafından yok edilir. Bu işlem için en az iki kişinin aynı anda hazır bulunması gerekir.

Nitelikli elektronik sertifikalara bağlı olan ve güvenli elektronik imza oluşturma aracı içinde saklanan imza oluşturma verileri, sertifika sahibinin imza oluşturma verilerinisilinmesiyle veya donanımın imha etmesiyle yok edilebilir.

6.2.11. Kriptografik Modülün Değerlendirilmesi

Alt kök sertifikalarına bağlı imza oluşturma verileri, Tebliğ'de tanımlı güvenlik düzeyine sahip kriptografik donanım modüllerinde üretilir ve saklanır.

Nitelikli elektronik sertifika sahiplerinin imza oluşturma verileri de, Tebliğ'de tanımlı güvenlik düzeyine sahip güvenli elektronik imza oluşturma araçlarında saklanır.

6.3. Anahtar Çifti Yönetimiyle İlgili Diğer Konular

6.3.1. İmza Doğrulama Verisinin Arşivlenmesi

Alt kök sertifikalarına bağlı imza doğrulama verileri, ESHS tarafından 20 yıl süreyle saklanır.

6.3.2. İmza Oluşturma ve Doğrulama Verilerinin Kullanım Süreleri

EGM tarafından üretilen nitelikli elektronik sertifikaların geçerlilik süreleri 3 (üç) yıldır.

Alt kök sertifikaların geçerlilik süreleri ise 10 (on) yılı aşmaz. Bu sürenin sonunda sertifikalar yenilenirken mutlaka anahtar çiftleri de yenilenir.

6.4. Erişim Denetim Verileri

6.4.1. Erişim Denetim Verilerinin Oluşturulması

EGMalt kök sertifikasına ait anahtarların üretimi ve bu anahtarlara ait erişim şifrelerinin oluşturulması, Kök Sertifika Üretim Prosedürü'ndeaçıklanan törene göre yapılır. Alt kök sertifikasının gizli anahtarlarının bulunduğu kriptografik modüllere erişim ve anahtarların kullanılması erişim şifrelerine sahip iki yetkilinin aynı anda bulunmasıyla mümkündür.

Erişim şifreleri, rastgele belirlenmiş en az 8 (sekiz) alfa nümerik değerden oluşur. Sisteme erişim bu şifrelerin yanında yetkililerin biyometrik doğrulama yapmalarını da gerektirir. Erişim şifrelerinin oluşturulması, kurulumu ve kullanılması logları (keyedhash ile) veri tabanında tutulur.

Sertifika sahiplerinin imza oluşturma verilerine ait erişim şifreleri aktivasyon yöntemiyle kendilerine belirttirilir.

Aktivasyon yönteminde, benzer biçimde sertifika üretim aşamasında rastgele en az 6 (altı) rakamdan oluşan bir erişim şifresi üretilir. Aynı işlem sırasında sertifika ve sertifikanın yazıldığı karta bağlı alfa nümerik 6 (altı) karakterden oluşan aktivasyon kodu da üretilir ve şifrelenerek veri tabanına kaydedilir.

Aktivasyon kodunun üretilme yöntemi, sertifika ve akıllı kart ile bir araya geldiğinde erişim şifresini yeniden oluşturulacak biçimde tasarlanmıştır. Böylece, kartı kendisine ulaşan ve aktivasyon kodu talep eden bir sertifika sahibi, başvuru sırasında bildirdiği cep telefonuna veya e-posta adresine gönderilen aktivasyon kodunu kullanarak kendi erişim şifresini belirler.

6.4.2. Erişim Denetim Verilerinin Korunması

Alt kök sertifikasına ait gizli anahtarları kullanan yetkili kişiler, erişim şifrelerini en geç 6 (altı) ayda bir değiştirirler. Yetkili kişiler, erişim şifrelerinin gizliliğinden ve korunmasından sorumludur.

Sertifika sahipleri gizli anahtarlarına ait erişim şifrelerini uygun şekilde belirlemek ve korumaktan sorumludur.

6.4.3. Erişim Denetim Verileri İle İlgili Diğer Konular

Aktivasyon yönteminde erişim şifresi elektronik veya fiziksel hiçbir biçimde taşınmaz. Aktivasyon kodu veri tabanında şifrelenmiş halde tutulur ve herhangi bir kullanıcının erişimine kapalıdır. Aktivasyon kodunun veri tabanından deşifre edilerek çıkması ancak sertifika sahibinin kartını bilgisayarına takması ve aktivasyon talep etmesiyle mümkündür. Bu durumda bile sertifika sahibinin bilgisayarıyla sunucu arasında şifreli haberleşme yapılır.

6.5. Bilgisayar Güvenliği Denetimleri

6.5.1. Bilgisayar Güvenliği İle İlgili Teknik Gerekler

EGM, ESHS faaliyetleri kapsamında bilgi sistemlerine erişim ve bu sistemlerin işletilmesi için aşağıda yer alan güvenlik kontrolleri uygulanmaktadır:

- Bilgisayar sistemlerinde güvenilir ve sertifikalı donanım ve yazılım ürünleri kullanılmaktadır.
- Bilgisayar sistemleri yetkisiz erişime ve güvenlik açıklarına karşı korunmuştur. Penetrasyon ve istemsiz erişim kontrolleri kurulmuş ve ilgili testlerle kontrollerin güncelliği ve sürekliliği sağlanmıştır.
- Bilgisayar sistemleri, virüslere, kötü niyetli ve yetkisiz yazılımlara karşı korunmaktadır.
- Bilgisayar sistemleri ağ güvenliği saldırılarına karşı korunmaktadır.
- Bilgisayar sistemlerine erişim hakları ve kimlik doğrulama, personele verilen şifrelerle sağlanmaktadır.
- Bilgisayarlara erişim hakları, yetkili personele tanımlanan rollerle sınırlanmıştır.
- Özellikle, sertifika kaydı, üretimi, askıya alma, iptali gibi sertifika hizmetlerine özgü tüm işlemler veri tabanında kaydedilir. Veri tabanına yetkisiz erişimi ve istenmeden yapılan değişiklikleri önlemek için kimlik doğrulamanın farklı erişim seviyelerinde çeşitli fiziksel ve elektronik önlemler alınır.Veri tabanı seviyesindeki mantıksal tutarlılık, aksi halde geri dönüşü olmayan sonuçlar doğurabilecek iptal durumu değişikliklerini önlemek için ilave bir güvenlik katmanı oluşturur.
- Bilgisayar sistemini oluşturan birimler arasındaki veri iletişimi güvenli olarak yapılmaktadır.
- İşlem kayıtları sürekli olarak tutulduğu için bilgisayar sistemlerinde oluşabilecek sorunlar kısa zamanda ve doğru biçimde belirlenebilmektedir.
- Değişikliklere karşı korunmuş güvenilir sistemler ve ürünler kullanır. Bu bağlamda, Bilgi Teknolojileri ve İletişim Kurumu'nun sürekli denetimi altında,CWA14167-1 standardının önerileri kesin olarak uygulanır.

6.5.2. Bilgisayar Sisteminin Sağladığı Güvenlik Seviyesi

Düzenleme dışıdır.

6.6. Yaşam Döngüsü Teknik Denetimleri

6.6.1. Sistem Geliştirme Denetimleri

Sistem geliştirme kontrolleri, geliştirme tesisi güvenliği (tesis güvenlik belgeleri aracılığıyla), geliştirme ortamı güvenliği, geliştirme personeli güvenliği, ürün bakımı sırasında konfigürasyon yönetimi güvenliği için uygulanır.

6.6.2. Güvenlik Yönetimi Denetimleri

İşlevsel sistemler ve ESHS içinde kullanılan bilgisayar ağının güvenliğinin sağlanması için uygun araçlar kullanılmakta ve güvenlik prosedürleri işletilmektedir.

EGM, ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemleri standardı sertifikası sahibidir.

6.6.3. Yaşam Döngüsü Güvenlik Denetimleri

Düzenleme dışıdır.

6.7. Ağ Güvenliği Denetimleri

Alt kök sertifikasının imza oluşturma verisi, ağ güvenliği sağlanmış ortamlarda kullanılmaktadır. Bu sistemler fiziksel ve teknik olarak korunurlar.

EGM, ESHS faaliyetleri kapsamında uygun ağ güvenliği yöntemleriyle korunmaktadır. Güvenlik duvarları, anahtarlama cihazları ve yönlendiriciler gibi tüm ağ elemanları, doğru ve güvenli bir biçimde ağ konfigürasyonu prosedürleri uyarınca kurulmuştur. Bu ağ elemanlarının güvenlik kontrolleri prosedürler uyarınca sürekli olarak yapılmaktadır.

6.8. Zaman Damgası

EGM'nin, ESHS faaliyetleri kapsamında, ilgili işlemlere ait elektronik kayıtlar,zaman damgası hizmetlerinde kullanılan zaman kaynağı ile senkronize edilmiş zaman bilgisini içerir.Kayıt bütünlüğü anahtarlanmış özet yöntemi kullanılarak korunur ve arşivleme aşamasında zaman damgası kullanılır.

7. SERTİFİKA VE SERTİFİKA İPTAL LİSTESİ (SİL) BİÇİMLERİ

7.1. Sertifika Biçimi

EGM sertifikaları genel olarak "ISO/IEC 9594-8/ ITU-T Recommendation X.509: "Information Technology- Open SystemsInterconnection- The Directory: Public –keyandattributecertificateframeworks" ile "IETF RFC 5280: "Internet X.509 PublicKeyInfrastructureCertificateandCertificateRevocationList (CRL) Profile" dokümanlarına uygundur.Ayrıca,EGM tarafından oluşturulan nitelikli elektronik sertifikalar Bilgi Teknolojileri ve Telekomünikasyon Kurumu tarafından yayımlanan "Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri – Nisan 2007" dokümanına uygundur.

EGMsertifikalarındatemel olarak aşağıdaki alanlar bulunur:

Alan Adı	Açıklama
Seri No	(Aynı sertifika veren için) Eşsiz numara
İmza Algoritması	Nesne tanımlayıcı numarası (Bkz. 7.1.3)
Sertifikayı Veren	Bkz. 7.1.4
Geçerlilik Başlangıcı	RFC 5280'e göre kodlanmış UTC zamanı
Geçerlilik Sonu	RFC 5280'e göre kodlanmış UTC zamanı
Özne	Bkz. 7.1.4
Açık Anahtar	RFC 5280'e göre kodlanmış anahtar değeri
İmza	RFC 5280'e göre kodlanmış imza değeri

EGM nitelikli elektronik sertifikalarında Kanun gereği, "Bu sertifika 5070 sayılı Elektronik İmza Kanununa göre nitelikli elektronik sertifikadır." ibaresi zorunlu olarak yer alır.

7.1.1. Sürüm Numarası

EGM tarafından oluşturulan alt kök sertifikalar ile son kullanıcı sertifikaları, "IETF RFC 5280 Internet X.509 PublicKeyInfrastructureCertificateandCertificateRevocationList (CRL) Profile" dokümanı uyarınca X.509 v3 sürümünü destekler.

7.1.2. Sertifika Uzantıları

Nitelikli elektronik sertifikalar, "IETF RFC 3039 Internet X.509 PublicKeyInfrastructureQualifiedCertificates Profile" ve "Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri – Nisan 2007" dokümanları uyarınca tanımlanan nitelikli elektronik sertifika uzantılarını içerir.EGMtarafından oluşturulan nitelikli elektronik sertifikalar içerisinde aşağıdaki sertifika uzantıları bulunur:

Uzantı Adı	Kritik İşaretli	Açıklama
AuthorityKeyIdentifier (Yetkili Anahtarı Tanımlayıcısı)	Hayır	Sertifikayı yayımlayan ESHS sertifikasının açık anahtar özet değeri.
SubjectKeyIdentifer (Özne Anahtarı Tanımlayıcısı)	Hayır	Sertifikada yer alan açık anahtarın özet değeri.
KeyUsage (Anahtar Kullanımı)	Evet	Digitalsignature (elektronik imza) ve non-repudiation (inkar edilemezlik) alanları bulunmaktadır.
CertificatePolicies (Sertifika İlkeleri)	Hayır	• İlke Tanımlayıcı Numarası (PolicyIdentifier) olarak 2.16.792.1.2.1.1.5.7.1.1 değeri • Sertifika Uygulama Esasları adresi (PolicyQualifierInfo – CPS) olarak http://www.egmsm.gov.tr/sue değeri

		• Kullanıcı Uyarısı (PolicyQualifierInfo – User Notice) olarak "Bu sertifika 5070 sayılı Elektronik İmza Kanununa göre nitelikli elektronik sertifikadır." ibaresi Kullanılmaktadır.
Basic Constraints (Temel Kısıtlar)	Hayır	ESHS (CA) değeri "false" olarak işaretlenmektedir.
SubjectAlternative Name (Özne Alternatif Adı)	Hayır	Opsiyonel olarak sertifika sahibinin elektronik posta adresi kullanılabilmektedir.
QualifiedCertificateStatements (Nitelikli Sertifika İbareleri)	Hayır	• ETSI TS 101 862 uyumunu belirten nesne tanımlayıcısı (0.4.0.1862.1.1) • Bilgi Teknolojileri ve İletişim Kurumu uyumunu belirten nesne tanımlayıcısı (2.16.792.1.61.0.1.5070.1.1) • Opsiyonel olarak Para Limiti İbaresi Kullanılmaktadır.
CRL Distribution Points (SİL Dağıtım Noktaları)	Hayır	Sertifikayı yayımlayan ESHS sertifikası tarafından imzalanmış olan SİL (CRL) dosyasının HTTP URL adresi.
Authority Information Access (ESHS Bilgi Erişimi)	Hayır	Sertifikayı yayımlayan ESHS sertifikasına ve OCSP servisine erişim adresleri.

7.1.3. Algoritma ve Nesne Tanımlayıcılar

EGM, ESHS faaliyetleri kapsamında son kullanıcı sertifikalarını imzalamak için SHA-1 özet algoritmasıyla RSA açık anahtarlı imzalama algoritmasını kullanır.

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

7.1.4. İsim Alanı Biçimleri

EGM tarafından üretilen sertifikalarda "ITU X.500 Distinguished Name [Ayırt edici isim]" biçiminde ayırt edilebilir isimler kullanılır.

7.1.5. İsim Kısıtları

EGM tarafından üretilen sertifikalarda anonim veya takma adlar kullanılmaz. Nitelikli elektronik sertifikalardaki isimlerde ayırt edici özellik olarak T.C. kimlik numarası kullanılır.

7.1.6. Sertifika İlkeleri Nesne Tanımlama Numarası

EGM, tarafından üretilen nitelikli elektronik sertifikaların "sertifika ilkeleri" uzantısında,2.16.792.1.2.1.1.5.7.1.1 sertifika ilkeleri nesne tanımlayıcı numarası (OID) kullanılır.

7.1.7. İlke Kısıtları Uzantısının Kullanımı

Düzenleme dışıdır.

7.1.8. İlke Niteleyiciler

EGM tarafından üretilen nitelikli elektronik sertifikaların "sertifika ilkeleri" uzantısında, ilke niteleyicisi olarak SUE dokümanına erişim bilgisi URL olarak verilmiştir.

7.1.9. Kritik Belirtilmiş Olan İlke Belirleyici Uzantılarının İşlenmesi

Düzenleme dışıdır.

7.2. Sertifika İptal Listesi Biçimi

EGM tarafından yayımlanan SİL'lerde temel olarak, EGM elektronik imzasıyla birlikte yayımlayıcı bilgileri, SİL'in yayımlanma tarihi, bir sonraki SİL'in yayımlanma tarihi ve iptal edilen sertifikaların seri numarası ile iptal tarih ve zamanı yer alır.EGMtarafından yayımlanan SİL'ler Bilgi Teknolojileri ve Telekomünikasyon Kurumu tarafından yayımlanan "Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri – Nisan 2007" dokümanına uygundur.

7.2.1. Sürüm Numarası

EGM tarafından oluşturulan SİL'ler, "IETF RFC 5280 Internet X.509 PublicKeyInfrastructureCertificateandCertificateRevocationList (CRL) Profile" dokümanı uyarınca X.509 v2 sürümünü destekler.

7.2.2. Sertifika İptal Listesi Uzantıları

EGM tarafından yayımlanan SİL'lerde, RFC 5280 tarafından tanımlanan uzantılar kullanılır.

7.3. Çevrim İçi Sertifika Durum Protokolü Biçimi

EGM gerçek zamanlı bir sertifika durum sorgusu olan OCSP desteğini kesintisiz olarak sağlar. Bu hizmetle, uygun sertifika durum sorguları alındığında, sorguda talep edilen sertifikaların durumu ve protokol gereği gereken diğer ek bilgiler sorgu cevabı olarak talep sahibine döndürülür.EGM tarafından verilen OCSP cevap mesajları, Bilgi Teknolojileri ve Telekomünikasyon Kurumu tarafından yayımlanan "Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri – Nisan 2007" dokümanına uygundur.

7.3.1. Sürüm Numarası

EGM tarafından verilen OCSP hizmeti, "IETF RFC 2560 Internet X.509 PublicKeyInfrastructureOnlineCertificateStatus Protocol - OCSP" dokümanı uyarınca v1 protokol sürümünü destekler.

7.3.2. ÇİSDUP Uzantıları

EGM tarafından verilen OCSP hizmeti içeriğinde, RFC 2560 tarafından tanımlanan uzantılar kullanılabilir. Ancak, temel OCSP bilgileri dışındaki tüm uzantıların kullanılması zorunlu değildir.

8. UYGUNLUK DENETİMLERİ

EGM, ESHS faaliyetleri kapsamında, e-imza mevzuatı gereğince Bilgi Teknolojileri ve İletişim Kurumu tarafından incelenir.

Aynı zamanda bu faaliyetler kapsamında ISO/IEC 27001Bilgi Güvenliği Yönetim Sistemi sertifikası uyarınca periyodik olarak uygunluk denetimine tabi tutulur.

ESHS hizmetlerinin verilişi ve işletmeye dair güvenlik koşulları bir iç denetim planı uyarınca kontrol altında tutulur.

8.1. Uygunluk Denetiminin Sıklığı

Bilgi Teknolojileri ve İletişim Kurumu, EGM ESHS faaliyetleri kapsamında gerekli gördüğü durumlarda re 'seninceleme yapar.

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi sertifikası uyarınca, her yıl takipdenetiminden veher üç yılda bir de belge yenileme denetiminden geçilir.

İç denetim, plan gereği yılda en az bir defa, gerek görülmesi durumunda daha fazla sayıda tekrar edilir.

8.2. Denetçinin Nitelikleri

Bilgi Teknolojileri ve İletişim Kurumu, Kanunla belirlenmiş düzenleyici ve denetçi kurumdur.

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi sertifikasyonu, yetkilendirilmiş bir denetçi tarafından gerçekleştirilir.

İç denetim, EGM bünyesindeki görevli personel tarafından yürütülür.

8.3. Denetçinin Denetlenen Tarafla Olan İlişkisi

Denetçi kuruluş olan Kurum, Kanun gereği Türkiye'de NES ile ilgili faaliyet gösteren tüm ESHS'leri denetlemekle yetkili kılınmış düzenleyici kuruluştur.

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi sertifikasyonu bağımsız ve yetkili bir denetçi tarafından gerçekleştirilir.

İç denetim, EGM bünyesindeki görevli personel tarafından yapılır.

8.4. Denetimin Kapsamı

Kurum'un denetimi veya incelemesi, Kanunla kendisine verilen yetki çerçevesinde, ESHS'nin elektronik sertifika hizmetlerine dair tüm süreçleri, bu hizmetlerin yerine getirilmesi sırasında kullanılan teknik altyapı ve hizmetlerin verildiği tesisleri kapsar.

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi sertifikasyonu, "Kurumun kurumsal donanım, yazılım, iletişim, nitelikli elektronik sertifika ve güvenlik gibi bilişim sistemlerinin alımı, kurulumu, geliştirilmesi, işletimi, yönetimi ile bilginin gizliliği, bütünlüğü ve sürekliliğinin sağlanması hizmetinin verilmesidir" kapsamındadır.

İç denetimde de, yasal denetim altına giren tüm konular kapsanır.

8.5. Yetersizliğin Tespiti Durumunda Yapılacaklar

Yönetmelik gereği Kurum tarafından yapılan denetimler sırasında ortaya çıkan eksiklikler, ESHS tarafından planlı çalışma ile giderilir.ESHS'ninfaaliyet ve işleyişini olumsuz yönde etkileyebilecek derecede önemli konuların belirlenmesi durumunda, ilgili mevzuatta öngörülen yaptırım ve cezalar uygulanır.

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi denetimleri sırasında saptanan eksiklikler planlı çalışmalarla giderilir.

İç denetimlerde belirlenen aksaklıklar hakkında düzeltici ve önleyici faaliyetler yürütülür ve giderilir.

8.6. Sonucun Bildirilmesi

Kurum ve ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi denetim sonuçlarıresmi yollarla ESHS'ye bildirilir. İç denetim sonuçları ise, iç denetim sonuç raporlarında yer alır ve ilgili yetkililerin değerlendirmesine sunulur.

9. DİĞER İŞLER VE HUKUKSAL MESELELER

9.1. Ücretlendirme

9.1.1. Sertifika Oluşturma ve Yenileme Ücreti

EGM, ESHS faaliyetlerini teşkilatıyla sınırlı tutmuştur. Bu yapı içerisinde nitelikli elektronik sertifika üretim ve yenileme işlemleri için herhangi bir ücret talep edilmemektedir.

9.1.2. Sertifika Erişim Ücreti

EGM tarafından üretilen sertifikalar, sertifika sahibinin yazılı rızası olması kaydıyla herkesin erişimine açık tutulur.

Sertifika erişim hizmetleri için ücret talep edilmez.

9.1.3. İptal Durum Kaydına Erişim Ücreti

Kanun gereği, NES iptal veya durum bilgisi erişim hizmetleri için ücret talep edilmez.

9.1.4. Diğer Servis Ücretleri

EGM Bilgi deposunda yayımladığı bilgi ve dokümanlara erişim için ücret talep etmez.

9.1.5. İade Ücreti

Düzenleme dışıdır.

9.2. Finansal Sorumluluk

9.2.1. Sigorta Kapsamı

EGM, ESHS faaliyetleri kapsamında Bölüm 9.2.3'de açılanan "Sertifika Mali Sorumluluk Sigortası" yaptırmıştır. Bu sigortanın kapsamı ilgili yönetmelikte belirtilmiştir.

9.2.2. Diğer Varlıklar

Düzenleme dışıdır.

9.2.3. Sertifika Mali Sorumluluk Sigortası

EGM, ESHS faaliyetleri kapsamında Kanundan doğan yükümlülüklerini yerine getirmemesi sonucu doğacak zararların karşılanması amacıyla, NES'lerisertifikasahiplerine teslim etmeden önce sertifika malî sorumluluk sigortası yaptırmıştır.

9.3. Ticari Bilginin Korunması

9.3.1. Gizli Bilginin Kapsamı

ESHS'nin kurum niteliği ve ESHS faaliyetlerinin kendi teşkilatında bulunan görevli kamu personeliyle sınırlı olması nedeniyle her türlü bilgi, belge, donanım, yazılım, işlem kaydı, kısıtlı bölgelere erişim şifreleri vb. gizli bilgi kapsamındadır.

9.3.2. Gizlilik Kapsamı Olmayan Bilgiler

EGM'nin ESHS faaliyetleri kapsamında Kanun ve uygulamalar gereği kamuya açık olması gereken bilgi ve belgeleri gizlilik kapsamı dışında tutulur.

9.3.3. Gizli Bilginin Korunma Sorumluluğu

EGM'nin tüm personeli gizli bilgilerin korunması konusunda sorumluluk sahibidir.

9.4. Kişisel Bilginin Gizliliği

9.4.1. Gizlilik Planı

Düzenleme dışıdır.

9.4.2. Gizli Olarak Tanımlanan Bilgiler

EGM'nin, ESHS faaliyetleri kapsamında sertifika başvuru sahiplerinden aldığı kimlik bilgileri, iletişim bilgileri, sertifika sahibi tarafından belirlenen parolalar gibi bilgiler, kişisel gizli bilgi olarak değerlendirilir.

9.4.3. Gizli Olarak Tanımlanmayan Bilgiler

Sertifika sahiplerine ait sertifikaların içeriğinde yer alan bilgiler, aksi sertifika sahibi tarafından talep edilmedikçe kişisel gizli bilgi olarak sayılmaz.

9.4.4. Gizli Bilginin Korunma Sorumluluğu

EGM'nin, ESHS faaliyetleri kapsamında sertifika başvuru sahiplerinden aldığı kimlik bilgileri, iletişim bilgileri, sertifika sahibi tarafından belirlenen parolalar gibi bilgilerin korunma sorumluluğu tüm ESHS personeline aittir. Yetkisiz erişim ve sertifika sahibinin izni olmadan üçüncü taraflarla herhangi bir bilgi paylaşımı hiçbir personel tarafından gerçekleştirilmez.

9.4.5. Gizli Bilginin Kullanma İzin Verilmesi

EGM, ESHS faaliyetleri kapsamında sertifika sahiplerine ait gizli kişisel bilgileri, sertifika sahibinin yazılı rızası olması durumunda, üçüncü kişilere verebilir.

9.4.6. Yetkili Merciilerin Kararına Uygun Olarak Bilginin Açıklanması

Hukuki veya idari süreçler gereği ihtiyaç duyulan sertifika sahibinin özel bilgileri, sadece talep sahibi resmi makama veya sertifika sahibinin kendisine verilir.

9.4.7. Diğer Başlıklar

Düzenleme dışıdır.

9.5. Telif Hakları

EGM tarafından üretilen tüm sertifikaların, SİL'lerin, tüm iç ve dış dokümanların fikri mülkiyet hakları EGM'yeaittir.

9.6. Temsil Hakkı ve Yükümlülükler

ESHS, sertifika sahipleri ve üçüncü kişiler; 5070 sayılı Elektronik İmza Kanunu ve bu kanuna bağlı yönetmelik, teknik tebliğ, taahhütname, SUE vb. düzenlemelerle oluşturulan yükümlülükleri yerine getirmek zorundadırlar.

9.6.1. Elektronik Sertifika Hizmet Sağlayıcısı Yükümlülükleri

EGM, ESHS faaliyetleri kapsamında, Kanun Madde 10 ve Yönetmelik Madde 14'te yer alan ESHS yükümlülüklerini yerine getirir. Bu yükümlülüklerle bağlı olarak üretilen sertifikaların içeriğinin doğruluğunu, kimlik doğrulama işleminin tam ve doğru şekilde yapıldığını, üretilen sertifikaların doğru şekilde sertifika sahibine teslim edildiğini, yayımlanan sertifika durum bildirimlerinin güncelliğini ve doğruluğunu; SUE'de yer alan tüm uygulama gereklilikleri ve yükümlülüklerini yerine getireceğini garanti eder.

9.6.2. Kayıt Birimleri Yükümlülükleri

Düzenleme dışıdır.

9.6.3. Sertifika Sahibi Yükümlülükleri

Sertifika sahipleri, Yönetmelik Madde 15'te yer alan yükümlülüklerle birlikte, sertifika sahibi taahhütnamesinde yer alan koşulları da yerine getireceğini garanti eder.

9.6.4. Üçüncü Kişilerin Yükümlülükleri

Üçüncü kişiler, elektronik imzaların geçerliliğini doğrulamaktan kendileri sorumludur.

9.6.5. Diğer Bileşenlerin Yükümlülükleri

Düzenleme dışıdır.

9.7. Yükümlülüklerden Feragat

Sertifika sahibi taahhütnamesinde belirtilen bir yöntem varsa bu şekilde sona erer.

9.8. Sorumluluklarla İlgili Sınırlamalar

ESHS, sertifika sahipleri ve üçüncü kişiler; 5070 sayılı Elektronik İmza Kanunu ve bu kanuna bağlı yönetmelik, teknik tebliğ, taahhütname, SUE vb. düzenlemelerle oluşturulan yükümlülükleri yerine getirmek zorundadırlar.

Ayrıca sertifikalar, parasal işlemlerde maddi işlem sınırları dahilinde sigortalıdır. Sertifikalar ve bu sertifikaların kullanımıyla ilgili sorumluluk sınırları, sertifika sahibi taahhütnamesinde açıkça belirtilmiştir.

9.9. Tazminat Halleri

EGM ve sertifika hizmeti alan taraflar arasında Kanun ve bağlı bulunan yönetmelikte belirtilen yükümlülüklerin yerine getirilmemesinden kaynaklanan zararlarda, zarara neden olan taraf tazminle yükümlüdür. Bu durumlarda ESHS kusursuzluğunu ispat ettiği takdirde tazminat ödeme yükümlülüğü doğmaz.

9.10. Anlaşma Süresi ve Anlaşmanın Sona Ermesi

9.10.1. Anlaşma Süresi

Sertifika sahibi tarafından imzalanan Nitelikli Elektronik Sertifika Sahibi Taahhütnamesi 'nin süresi nitelikli elektronik sertifikanın geçerlilik süresiyle sınırlıdır. Sertifikanın iptal edilmesi durumunda taahhütnamenin süresi de sona erer.

9.10.2. Anlaşmanın Sona Ermesi

Nitelikli elektronik sertifikanın süresinin dolması, sertifikanın herhangi bir nedenden dolayı sertifika sahibi veya ESHS tarafından iptal edilmesi, sertifika sahibinin taahhütnameye aykırı davranması veya ESHS'nin faaliyetinin sona ermesi gibi durumlarda anlaşma sona erer.

9.10.3. Anlaşmanın Sona Ermesinin Etkileri

Nitelikli elektronik sertifikanın süresinin dolması, sertifikanın herhangi bir nedenden dolayı sertifika sahibi veya ESHS tarafından iptal edilmesi gibi durumlarda sertifika sahibinin Kamu SM Sİ ve EGM SUE dokümanlarında belirtilen yükümlülükleri ortadan kalkar. Sertifika sahibinin taahhütnameye aykırı davranmasından dolayı doğan zararlardan ESHS sorumlu tutulamaz.

Nitelikli elektronik sertifikaların süresinin dolması ya da başka bir nedenden dolayı iptal edilmesi halinde, EGM'nin kanundan kaynaklanan, sertifikalarla ilgili iptal durumu kayıtlarının tutulması ve bu kayıtlara erişim, kayıtların ve arşivlerin saklanması gibi yükümlülükleri devam eder.

9.11. Sistem Bileşenleriyle Haberleşme ve Kişisel Bilgilendirme

EGM, sertifika sahiplerine yapacağı bilgilendirmelerini telefon veya e-posta yoluyla yapabilir. Kritik görülen bilgilendirmeler de ise resmi yazı kanalı kullanılır.

9.12. Değişiklik Halleri

9.12.1. Değişiklik Metotları

Bu SUE dokümanı EGM tarafından hazırlanmıştır. EGM, ESHS faaliyetleri kapsamında yapacağı değişikliklerle ilgili SUE dokümanını, yeni bir sürümle hazırlar ve yayımlar. SUE dokümanındaki değişiklik belli bölümleri kapsayabileceği gibi tamamen de yapılabilir.

Kamu SM Sİ dokümanında gerçekleşecek değişiklikler, EGM SUE dokümanına yansıtılır.

9.12.2. Bilgilendirme Mekanizması ve Sıklığı

EGM, nitelikli elektronik sertifika hizmetleri kapsamında yaptığı değişiklikleri, yeni sürüm SUE dokümanını web sitesi üzerinden bilgi deposunda kamuya açık şekilde yayımlayarak duyurur.

SUE dokümanı yenilenmesinden en fazla 1 (bir) hafta içinde bilgi deposunda yayımlanır ve yayımlandığı an itibariyle yürürlüğe girer. Ayrıca yeni SUE dokümanı yayınlanmasından sonra1 (bir) hafta içinde Bilgi Teknolojileri ve İletişim Kurumu'na bildirilir.

9.12.3. Nesne Tanımlama Numarasının Değişmesini Gerektiren Durumlar

Düzenleme dışıdır.

9.13. Anlaşmazlık Halleri

Anlaşmazlık hallerinde, 5070 sayılı Elektronik İmza Kanunu ve bağlı yönetmelik, tebliğ ve EGM SUE dokümanı, prosedürler ve taahhütnameler uyarınca sorunun çözümlenmesine çalışılır. Sorunun sulh en çözülememesi halinde ise anlaşmazlıkların çözümü için Ankara Mahkemeleri yetkilidir.

9.14. Uygulanacak Hukuk

EGM SUE dokümanındaki hükümler 5070 sayılı Elektronik İmza Kanunu'na uygun olarak düzenlenir.

9.15. Uygulanabilir Yasalara Uyum

EGM ESHS faaliyetlerini 5070 sayılı Elektronik İmza Kanunu ve Bilgi Teknolojileri ve İletişim Kurumu tarafından yayımlanmış Yönetmelik ve Tebliğler ile diğer ilgili düzenlemeler uyarınca yürütür. Mevzuat değişiklikleri sonucunda SUE dokümanının mevzuata uyumlu hale getirilmesi esastır.

9.16. Diğer Hükümler

Düzenleme dışıdır.