KAMU SM SERTİFİKA İLKELERİ (NİTELİKLİ ELEKTRONİK SERTİFİKA İÇİNDİR)

Doküman Kodu	Yayın Numarası	Yayın Tarihi
POLT-001-013	**09**	**28.08.2013**

KAMU SM SERTİFİKA İLKELERİ (NES)

DEĞİŞİKLİK KAYITLARI

Yayın No	Yayın Nedeni	Yayın Tarihi
01	İlk yayın	28.03.2005
02	RFC 3647 tam uyumluluğu için yeniden düzenleme	06.06.2005
03	Sertifika yönetim süreçlerinde değişiklik yapılması Kurum logosunda değişikliği yapılması Nitelikli Elektronik Sertifika Taahhütnamesi'nin yönetim süreçlerine eklenmesi	13.02.2007
04	Planlı gözden geçirme sonrası küçük değişiklikler yapıldı	07.05.2008
05	BTK denetimi sonrası, kapsamlı bir güncelleme yapılmıştır.	05.10.2009
06	Sertifikaların askıya alınması ve kullanıma açılması ile ilgili hususlar tekrar düzenlendi.	30.12.2010
07	Kayıtçı hizmeti eklendi. Sistem bileşenleri ve anahtar üretiminin kullanıcı tarafında yapılması ile ilgili eklemeler yapıldı.	02.11.2012
08	Şablon düzeltildi.	11.12.2012
09	Kayıtçı hizmeti politikalardan kaldırıldı.	28.08.2013

KAMU SM SERTİFİKA İLKELERİ (NES)

İÇİNDEKİLER

ŞEKİLLER

TABLOLAR

KAMU SM SERTİFİKA İLKELERİ (NES)

1. Giriş

Bu doküman, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu'na (TÜBİTAK) bağlı Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM) tarafından oluşturulan Kamu Sertifikasyon Merkezi'nin (Kamu SM) nitelikli elektronik sertifika üreten Elektronik Sertifika Hizmet Sağlayıcısı (ESHS) 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 kapsamında ve Başbakanlığın 2004/21 sayılı "Kamu Sertifikasyon Merkezi Oluşturulması" başlıklı genelgesi uyarınca kamu kurum ve kuruluşlarının elektronik sertifika ihtiyaçlarının tek merkezden sağlanması amacıyla kurulmuştur. Kamu SM, kamu çalışanlarına kurum içi ve kurumlar arası işlemlerde kullanmak üzere nitelikli elektronik sertifika üretip, nitelikli elektronik sertifikaların yaşam döngüsü içinde gerekli iptal ve yenileme gibi işlemlerini yerine getirir. Kamu çalışanları Kamu SM tarafından kendilerine verilen nitelikli elektronik sertifikaları bireysel işlemlerinde de kullanabilirler.

Kamu SM Sİ dokümanı nitelikli elektronik sertifika 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. Bu doküman, 15 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza Kanunu, 2004/21 sayılı Başbakanlık Genelgesi, Telekomünikasyon Kurumu'nun yayımladığı Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik, Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ esas alınarak hazırlanmıştır.

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, nitelikli elektronik sertifikaların üretim ve yönetim ilkelerinin, sertifika yönetimi ile ilgili tüm kural ve usullerin en üst düzeyde tanımlandığı bir dokümandır. Kamu SM'den sertifika talebinde bulunan kullanıcılar bu dokümanda belirtilen şartları kabul etmiş sayılırlar.

Kamu SM açık anahtarlı altyapı mimarisi içinde, en üst seviyede bir Kök Sertifika Hizmet Sağlayıcısı (Kök SHS) ile buna bağlı olarak çalışan iki ayrı Sertifika Hizmet Sağlayıcısı bulunur. Sözü

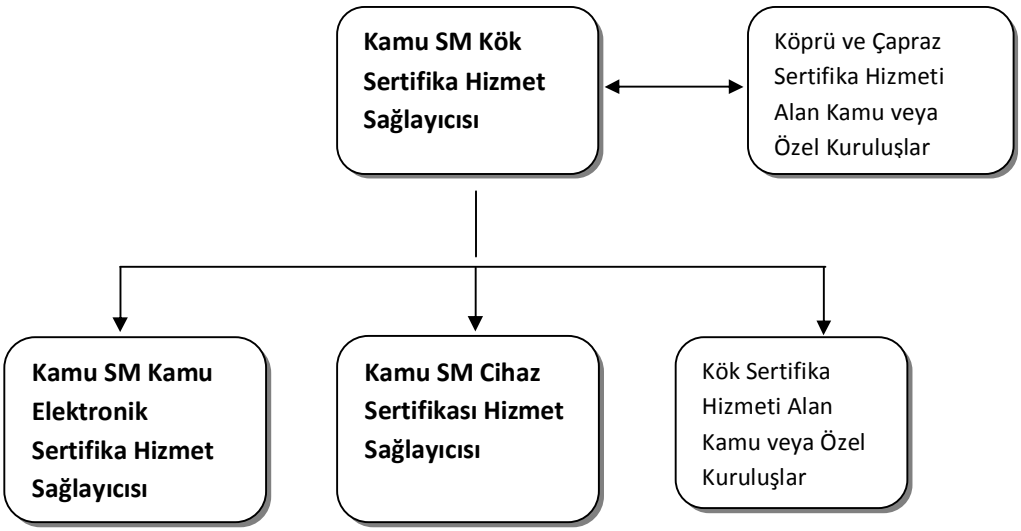
geçen Sertifika Hizmet Sağlayıcılar, Kamu Elektronik Sertifika Hizmet Sağlayıcısı (Kamu ESHS) ve Cihaz Sertifikası Hizmet Sağlayıcısı'dır.

Kök SHS 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.

Kamu ESHS, Cihaz SHS ve Kamu SM'den kök sertifika hizmeti alan kamu kuruluşları veya özel kuruluşlar, Kök SHS'nin elektronik imzasını taşıyan sertifikaya sahiptir. Kamu SM açık anahtarlı altyapı mimarisi Şekil 1-1'de verilmiştir.

Kamu ESHS gerçek kişilere Nitelikli Elektronik Sertifika (NES) temini amacıyla hizmet verir. Cihaz Sertifikası Hizmet Sağlayıcısı cihazlara elektronik sertifika temin etmek amacıyla hizmet verir. Cihazlara verilen sertifikalar 5070 sayılı Elektronik İmza Kanunu'nda sözü geçen nitelikli elektronik sertifika kapsamında değerlendirilmezler.

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



Şekil 1 Kamu SM açık anahtarlı altyapı mimarisi

1.2. Doküman Adı ve Tanımı

Doküman Adı: Kamu SM Sertifika İlkeleri (Nitelikli Elektronik Sertifika içindir)

Doküman Sürüm Numarası: 09

Yayın Tarihi: 28.08.2013

Nesne Tanımlama Numarası: 2.16.792.1.2.1.1.5.7.1.1

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

1.3. Sistem Bileşenleri

Kamu SM açık anahtar altyapısını oluşturan sistem bileşenleri aşağıda tanımlanmıştır.

1.3.1. Elektronik Sertifika Hizmet Sağlayıcısı

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. Kamu SM, BTK tarafından yetkilendirilmiş bir elektronik sertifika hizmet sağlayıcısıdır. Kamu SM bünyesinde kurulan sertifika hizmet sağlayıcıları ve Kamu SM'den hizmet alan diğer ESHS'ler Kamu SM açık anahtar alt yapısını oluşturan sistem bileşenleridir. Bu bileşenler aşağıda belirtilmiştir.

Kök Sertifika Hizmet Sağlayıcısı (Kök SHS)

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

Kamu SM güvenlik gerekleri dolayısıyla özel statüye sahip kamu kuruluşlarına (Türk Silahlı Kuvvetleri, Dışişleri Bakanlığı, vb.) ait ESHS'ler, ülke içinde hizmet veren ulusal ESHS'ler ve ülke dışında kurulmuş olan diğer ESHS'lerle ortak çalışırlığı sağlayabilmek için kök, köprü ve çapraz sertifika hizmetleri verir. Üretilen kök, köprü ve çapraz sertifikalar Kök SHS'nin imzasını taşır.

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

Kamu Elektronik Sertifika Hizmet Sağlayıcısı (Kamu ESHS)

Kamu ESHS, kamu çalışanı gerçek kişilere nitelikli elektronik sertifika üretmekle yetkilidir. Kamu ESHS'nin sertifikası Kök SHS tarafından imzalanmıştır. Kişiler adına üretilen nitelikli elektronik

sertifikalar Kamu ESHS'nin elektronik imzasını taşır. Kamu ESHS tarafından verilen nitelikli elektronik sertifikalar 5070 sayılı elektronik imza kanunu kapsamında verilir. Kamu ESHS, elektronik imza kanunu kapsamına girmeyen nitelikli olmayan sertifikalar da verebilir.

Cihaz Sertifikası Hizmet Sağlayıcısı (Cihaz SHS)

Cihaz SHS, gerçek kişilere değil cihazlara elektronik sertifika üretir. Cihaz SHS'nin sertifikası Kök SHS tarafından imzalanmıştır. Yurt içi veya yurt dışında kurulmuş olan kamu veya özel kuruluşlara ait cihazlara verilen sertifikalar Cihaz SHS'nin imzasını taşır. Cihaz SHS tarafından verilen sertifikalar 5070 sayılı elektronik imza kanunu kapsamında değildir.

Kök Sertifika Hizmeti Alan Kuruluşlar

Kamu SM'den kök sertifika hizmeti alan yurt içinde veya yurt dışında kurulmuş kamu veya özel kuruluşlara verilen alt kök sertifikalar Kök SHS tarafından imzalanmıştır. Kök sertifika hizmeti alan kuruluşlara verilen sertifikalar için başvuru, üretim, dağıtım, yenileme ve iptal etme ile ilgili süreçler içindeki işlemler bu dokümanın içeriğinde bulunmaz. Kamu SM'den kök sertifika hizmeti almak isteyen ESHS'ler konuyla ilgili olarak başvuru işlemlerini Kamu SM tarafından belirlenen şartlar doğrultusunda yerine getirirler. Üretilen kök sertifikaların üretim, dağıtım, iptal ve yenilenmeleri ile ilgili yönetim işlemleri de yine Kamu SM'nin belirlediği şartlara göre yerine getirilir. Kök sertifikasyon hizmeti alan ESHS'ler kullanıcılara verdikleri sertifika hizmetiyle ilgili süreçleri bu Sİ dokümanında belirtilen sertifika ilkelerine bağlı kalarak yerine getirirler.

Köprü veya Çapraz Sertifika Hizmeti Alan Kuruluşlar

Kamu SM'den köprü veya çapraz sertifika hizmeti alan yurt içinde veya yurt dışında kurulmuş kamu veya özel kuruluşlara verilen köprü veya çapraz sertifikalar Kök SHS tarafından imzalanmıştır. Köprü veya çapraz sertifika hizmeti alan tarafların başvuru işlemleri ile üretilen köprü ve çapraz sertifikaların yönetimi ile ile ilgili süreçler bu dokümanın içeriğinde bulunmaz. Kamu SM ile hizmeti alan taraf arasında karşılıklı güvenin temin edilmesi için gereken şartlar imzalanan sözleşmelerde belirtilir.

1.3.2. Kayıt Birimleri

Kayıt birimleri, son kullanıcıların sertifika başvuru kayıt işlemlerini ve sertifika teslimatlarını yapmakla yetkili birimlerdir. ESHS kendi bünyesi ve fiziksel ortamı içinde kayıt birimleri bulundurduğu gibi kayıt birimi hizmetini kendi fiziksel ortamından uzakta bir ortamda da kurabilir.

1.3.3. Sertifika Sahipleri

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

1.3.4. Üçüncü Kişiler

Üçüncü kişiler, sertifikaların içindeki kimlik ve imza doğrulama verisi arasındaki bağın doğruluğuna güvenerek sertifikaları kabul eden ve işlem yapan kişilerdir.

1.3.5. Diğer Bileşenler

Yukarıda yazılanlar dışındaki bileşenlerdir. Diğer bileşenler gerekirse bu Sİ dokümanına uygun oluşturulan SUE dokümanında detaylandırılır.

1.4. Sertifika Kullanımı

1.4.1. Uygun Olan Sertifika Kullanımı

Üretilen nitelikli elektronik sertifikalara ait imza oluşturma verileri, elektronik imzaya ilişkin mevzuatta tanımı yapıldığı şekilde sertifika sahibi tarafından, güvenli elektronik imza oluşturma aracıyla birlikte, güvenli elektronik imza oluşturmak amacıyla kullanılır. Güvenli elektronik imza, elle atılan imza ile aynı hukuki sonucu doğurur.

Nitelikli elektronik sertifika içeriğindeki imza doğrulama verisi, oluşturulan güvenli elektronik imzanın doğrulanması için kullanılır.

1.4.2. Sertifika Kullanımının Sınırları

Nitelikli elektronik sertifikaya ait imza oluşturma verisi, güvenli elektronik imza oluşturmak dışında başka amaçlar için kullanılmaz. Nitelikli elektronik sertifika içeriğindeki imza doğrulama verisi, oluşturulan güvenli elektronik imzanın doğrulanması dışında başka amaçlar için kullanılmaz.

Kanunların resmi şekle veya özel bir merasime tabi tuttuğu hukuki işlemler ile teminat sözleşmeleri, güvenli elektronik imza ile gerçekleştirilemez.

ESHS, dağıttığı sertifikaların hangi uygulamalarda ne amaçlar doğrultusunda kullanıldığını denetlemekle yükümlü değildir.

1.5. İlkelerin Yönetimi

1.5.1. Doküman Yönetimi

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

1.5.2. İletişim Bilgileri

Bu Sİ dokümanının uygulanması ve ilgili yönetim ilkeleri hakkındaki sorular, TÜBİTAK BİLGEM'in aşağıdaki erişim noktalarına yönlendirilebilir:

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

Tel. : 444 5 576

Faks : (262) 648 18 00

E Posta : bilgi@kamusm.gov.tr

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

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

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

1.5.3. Sertifika Uygulama Esaslarının İlkelere Uygunluğunu Belirleyen Kişi

Bu 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

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

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

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

Elektronik sertifika: İmza sahibinin, imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kayıt. Bu dokümanda bahsi geçen elektronik sertifika ve sertifika kelimeleri, nitelikli elektronik sertifikayı ifade etmek amacıyla kullanılmıştır.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1.6.2. Kısaltmalar

BGYS: Bilgi Güvenliği Yönetim Sistemi

BS (British Standards): İngiliz Standartları

BTK: Bilgi Teknolojileri ve İletişim Kurumu

CEN (Comité Européen de Normalisation): Avrupa Standardizasyon Komitesi

CWA (CEN Workshop Agreement): CEN Çalıştay Kararı

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

EAL (Evaluation Assurance Level): Değerlendirme Garanti Düzeyi

ESHS: Elektronik Sertifika Hizmet Sağlayıcısı

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

ETSI TS (ETSI Technical Specification): ETSI Teknik Özellikleri

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

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

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

ITU (International Telecommunication Union): Uluslararası Telekomünikasyon Birliği

KPS: Kimlik Paylaşım Sistemi

Kamu SM: Kamu Sertifikasyon Merkezi

LDAP (Lightweight Directory Access Protocol): Dizin Erişim Protokolü

PKI (Public Key Infrastructure): Açık Anahtarlı Altyapılar

Sİ: Sertifika İlkeleri

SİL: Sertifika İptal Listesi

SUE: Sertifika Uygulama Esasları

2. Yayımlama ve Bilgi Deposu Yükümlülükleri

2.1. Bilgi Depoları

ESHS, sistem bileşenleri ile paylaştığı bilgileri bilgi depoları üzerinden yayımlar. Bilgi deposu olarak web sunucular veya dizin sunucuları kullanılır. Bilgi depolarına erişim internet üzerinden sağlanır.

2.2. Sertifika Hizmeti ile İlgili Bilgilerin Yayımlanması

ESHS, kendisine ait sertifikaları, iptal durum kayıtlarını, Sİ ve SUE dokümanlarını bilgi deposundan ücretsiz olarak erişime açık tutar; bilgi deposunun kesintisiz olarak erişilebilirliğini sağlamak için gerekli önlemleri alır; bilgi deposunda tutulan bilgilerin doğruluğunu ve güncelliğini sağlar. ESHS, sertifika sahibinin izni olmadan sertifikayı üçüncü kişilerin ulaşabileceği ortamlarda bulunduramaz. ESHS, kendi sertifikasına ait sertifika özet değeri ile özet değerini hesaplamada hangi özetleme algoritmasını kullandığı bilgisini internet sitesi üzerinden yayımlar.

2.3. Yayın Sıklığı ve Zamanı

ESHS'nin kendisine ait sertifikalar, ESHS'nin hizmet süresi boyunca kesintisiz olarak yayımlanır. ESHS'nin kendisine ait sertifikaların güncellenmesi durumunda, yenilenen sertifikalar en kısa zamanda yayımlanır.

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

İptal durum kayıtlarının yayımlanma sıklığı, ilgili SUE dokümanında belirtilir. NES iptal durum kayıtlarının yayımlanma sıklığı 1 (bir) günden fazla olamaz.

2.4. Erişim Kontrolleri

ESHS bilgi deposuna erişim herkese açıktır.

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

3. Kimlik Belirleme ve Doğrulama

Sertifika başvurusu sırasında, sertifika içeriğinde adı bulunan kişilerinkimliklerinin belirlenmesi, daha sonra gerçekleştirilen yenileme, askıya alma ve iptal taleplerinin yerine getirilebilmesi için kimlik doğrulaması yapılması gerekir. Sertifika işlemlerinde gerekli olan, kimliklerinin belirlenmesi ve doğrulanması, bu bölümde anlatılan ilkelere uygun olarak gerçekleştirilir.

3.1. İsimlendirme

3.1.1. İsim Alanı Tipleri

Üretilen sertifikalarda kimlik bilgilerinin yazıldığı isim alanı "ITU X.500 Distinguished Name (Ayırt edici isim)" biçimine uygundur.

3.1.2. Kimlik Bilgilerinin Teşhise Elverişli Olması

Sertifika içeriğindeki kimlik bilgilerinin, anlamlı ve kişiyi tanımlayıcı nitelikte olması gerekmektedir. İsim alanlarının içinde sertifika sahibinin teşhis edilebileceği, kimlik bilgisi bulunur.

3.1.3. Sertifika Sahibinin Takma İsim veya Lakap Kullanması

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

3.1.4. Farklı İsim Alanı Tiplerinin Yorumlanması

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

3.1.5. Kimlik Bilgilerinin Tekilliği

ESHS'nin ürettiği, farklı kişilere ait sertifikalarda aynı kimlik bilgilerinin kullanılması engellenir. Sertifika içeriğinde, sertifika sahibini tekil biçimde ifade edecek şekilde yeterli kimlik bilgisi kullanılır. Sertifikaların isim alanlarında, hangi bilgilerin benzersiz kimlik bilgisi oluşturma amacıyla kullanılacağı SUE dokümanında belirtilir.

3.1.6. Markanın Tanınması, Doğrulanması ve Rolü

Düzenlenmesine gerek duyulmamıştır.

3.2. İlk Kimlik Belirleme

Kişi veya kuruluşların kimliklerinin ilk sertifika başvurusu sırasında belirlenmesi için aşağıdaki yöntemler uygulanır.

3.2.1. İmza Oluşturma Verisine Sahip Olmanın Kanıtlanması

Sertifika sahibine ait imza oluşturma ve doğrulama verileri, ESHS tarafından üretilerek sertifika sahibine ulaştırılır. İmza oluşturma ve doğrulama verileri aynı anda sahibine teslim edildiğinden sertifika sahibinin imza oluşturma verisine sahip olduğu kabul edilir. Ancak gerekli görüldüğü durumlarda imza oluşturma ve doğrulama verileri sertifika sahibi olan tarafça da üretilebilir. İmza oluşturma verisinin sertifika sahibinde olduğunun kanıtlanması için kriptografik yöntemlerden faydalanılır.

3.2.2. Kurumsal Kimliğin Belirlenmesi

ESHS, sertifika başvurusunda bulunan kurumların kurum bilgilerini, resmi ve onaylı belgelere dayanarak belirler. Kamu kurum veya kuruluşlarının kimliklerinin belirlenmesi için resmi yazı ile yapılan bilgilendirmeler yeterlidir.

3.2.3. Kişisel Kimliğin Belirlenmesi

Nitelikli elektronik sertifika başvurusunda bulunan kurumlar, nitelikli elektronik sertifika almak istediği çalışanlarına ait bilgileri ESHS'ye bildirir. Kişilere ait kimlik bilgileri, Kimlik Paylaşım Sistemi ve kurumsal başvuru belgesine dayanılarak belirlenir.

3.2.4. Doğrulanmayan Sertifika Sahibi Bilgileri

Sertifika sahibine ve kurumlara ait adres, faks numarası, telefon numarası ve elektronik posta gibi erişim bilgileri ile varsa SUE dokümanında işaret edilen diğer bilgiler ESHS tarafından doğrulanmayan bilgilerdir. Bu bilgilerle ilgili olarak sertifika sahibinin ve kurumun beyanı doğru kabul edilir.

3.2.5. Yetkinin Doğrulanması

Sertifika sahibinin yetkisi ile ilgili bilgiler sertifika içeriğine yazılacaksa resmi belgelere dayanılarak yetki tespit edilir.

3.2.6. Uyum Kriterleri

Düzenlenmesine gerek duyulmamıştır.

3.3. Sertifika Yenileme İsteğinde Kimlik Doğrulama

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

3.3.1. Olağan Sertifika Yenileme İsteğinde Kimlik Doğrulama

Olağan sertifika yenileme isteği, geçerli sertifikanın kullanım süresi dolmadan önce ve sertifika içeriğinde herhangi bir değişiklik olmaması durumunda yapılır. Sertifika yenileme isteği yerine getirilmeden önce, talebi yapan kişinin kimlik doğrulaması, ESHS sisteminde kayıtlı bilgiler ve KPS kullanılarak yapılır.

Sertifika yenileme başvurusu formunda, ilk kimlik belirlemesi sırasında verilen ve sertifikanın içeriğinde bulunan bilgilerin geçerliliğinin devam ettiği belirtilir. Sertifika sahibinden kimlik belirlemesi için ilk başvuru sırasında istenen belgeler gerekli görülmedikçe tekrar istenmez. Kimlik doğrulaması elektronik olarak gönderilen imzalı formun imzasının geçerli bulunmasıyla ve formdaki bilgilerin ESHS sisteminde kayıtlı bilgiler ile kıyaslanarak kontrol edilmesiyle yapılır.

3.3.2. İptal Sonrası Yeni Sertifika Talebinde Kimlik Doğrulama

İptal sonrası yenileme başvuruları, ilk sertifika başvurusunda olduğu gibi yapılır. Kimlik doğrulaması için, ilk kimlik belirlemesi işlemlerinde istenen bilgiler yeniden gözden geçirilir ve güncellenen bilgiler varsa gerekli görülen belgelerin yeniden ESHS'ye gönderilmesi istenir. Kimlik doğrulaması, ilk başvuru sırasında beyan edilen belgelerle birlikte yeni gönderilen belgelerin incelenmesiyle yapılır.

3.4. Sertifika İptal İsteğinde Kimlik Doğrulama

ESHS'nin kullanım süresi dolmamış sertifikaları kullanımdan kaldırması işlemi, "sertifika iptali" olarak adlandırılır. İptal istekleri, internet üzerinden veya telefonla işlem yaparak ya da ESHS'ye ıslak imzalı yazı göndererek yapılır. İnternet üzerinden ve telefonla işlem yaparak iptal taleplerinin gerçekleştirilmesi için, güvenlik sözcüğü veya kişisel bilgiler kullanılarak kimlik doğrulaması yapılır. Resmi yazı ile yapılan iptal isteklerinde, yazı üzerindeki ıslak imza kontrol edilerek kimlik doğrulaması yapılır. Elektronik ortamdan yapılan iptal isteklerinde elektronik belge üzerindeki elektronik imza doğrulanarak kimlik doğrulaması yapılır.

4. İşlemsel Gerekler

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

4.1. Sertifika Başvurusu

4.1.1. Sertifika Başvurusunu Kimlerin Yapabildiği

Sertifika başvurusu, kamu kurumları tarafından ESHS'ye kurumsal olarak yapılır. Kamu çalışanları bağlı bulundukları kurumdan bağımsız olarak bireysel başvuruda bulunamazlar. Kamu kurumu ve ESHS arasında yapılan resmi yazışmalar veya imzalanan sözleşmeler sonrasında, kurum çalışanları bireysel başvuruda bulunabilir.

4.1.2. Kayıt İşlemleri ve Sorumluluklar

Sertifika başvurusu ESHS'ye yapılır. Kayıt süreçleri ile ilgili detaylar SUE dokümanında anlatılır.

Sertifika başvurusu sırasında, başvuru sahibinin kimliği tanımlanır ve doğrulanır. Bunun için kurum veya kuruluş, sertifika talebinde bulunduğu kişilerin çalışanları olduğunu ispatlayan bilgi ve belgeleri ESHS'ye gönderir. Kurumsal başvuru sahibi, adına başvuruda bulunduğu kişilerin sertifika taleplerini resmi yazı ile; ıslak imzalı yada elektronik imzalı olarak belgelendirir.

Sertifika başvurusunda bulunan çalışanlar, başvuru sırasında veya sertifikalarını teslim aldıklarında sertifika kullanımıyla ilgili sorumluluklarının belirtildiği sertifika sözleşmesini veya taahhütnamesini imzalarlar.

Başvuru sahibi kurum ve çalışanları, ESHS'nin tanımladığı, detayları SUE dokümanında yer alan başvuru şartlarını yerine getirmekten sorumludur. ESHS, sertifika içinde yer alacak bilgilerin doğruluğunun sağlanmasından sorumludur.

4.2. Sertifika Başvurusunun İşlenmesi

4.2.1. Kimlik Tanımlama ve Doğrulama İşlevlerinin Yerine Getirilmesi

Başvuru sırasında ESHS'ye gönderilen belgeler incelenerek, işleme alınır. Belgelerin hatalı olması, eksik veya yanlışlığının tespit edilmesi durumunda, kimlik tanımlama ve doğrulama yapılamaz.

4.2.2. Sertifika Başvurusunun Kabul veya Reddi

Başvuru sırasında alınan belgelerin incelenmesi sonucunda, başvuru kabul edilir veya geri çevrilir. Başvurunun kabul edilmesi veya geri çevrilmesi ile ilgili kriterler, SUE dokümanında yer alır. Geri çevrilen başvurular, reddediliş sebepleriyle birlikte kuruma bildirilir. Bilgilendirme süreci, elektronik ortam üzerinden veya yazı ile yapılabilir. Geçerli bulunan başvurular için sertifika üretim süreci başlatılır.

Sertifika başvurusunda bulunulmuş olması, sertifika üretimini zorunlu kılmaz. Usulüne uygun yapılmayan başvurular geri çevrilir ve sertifika üretimi yapılmaz.

4.2.3. Sertifika Başvurusunun İşlenme Zamanı

Başvuru ile ilgili geçerli tüm belgelerin ESHS'nin eline geçmesinin ardından en fazla 15 (onbeş) iş günü içinde sertifika başvurusu işleme alınır ve sonuçlandırılır.

4.3. Sertifikanın Oluşturulması

4.3.1. Sertifika Oluşturulmasında ESHS'nin İşlevleri

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

4.3.2. Sertifika Oluşturulması ile İlgili Sertifika Sahibinin Bilgilendirilmesi

Anahtar çiftlerinin ESHS tarafından üretilmesine müteakip sertifika, sahibine imza oluşturma verisiyle birlikte güvenli elektronik imza oluşturma aracı içinde teslim edilir. Sertifika sahibi kendisine gönderilen güvenli elektronik imza oluşturma aracını teslim aldığında, sertifikasının oluşturulduğu konusunda bilgilendirilmiş olur.

4.4. Sertifikanın Kabulü

4.4.1. Sertifikanın Kabul Koşulu

Sertifika sahibi, kullanmaya başlamadan önce, sertifikasının içeriğini kontrol eder ve doğrular. Sertifikanın son kullanıcıya ait olmaması, sertifika içerisindeki bilgilerde hata olması ya da donanım sorunlarının olması durumunda; son kullanıcı sertifikayı, iade sebebini belirterek ESHS'ye iade eder.

4.4.2. Sertifikanın ESHS Tarafından Yayımlanması

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

4.4.3. Sertifikanın Oluşturulmasının Diğer Taraflara Duyurulması

Sertifikanın oluşturulması, kurumun talep etmesi durumunda, ESHS tarafından, internetten erişimi sağlanan raporlar ya da e-posta ile kuruma bildirilir.

4.5. Sertifikanın ve İmza Oluşturma Verisinin Kullanımı

4.5.1. Sertifika Sahibinin Sertifika ve İmza Oluşturma Verisini Kullanımı

Sertifika sahipleri, ilgili imza oluşturma verilerini elektronik imza mevzuatında belirtildiği şekilde güvenli elektronik imza oluşturmak amacıyla kullanırlar. Sertifikalarla ilgili imza oluşturma verileri, güvenli elektronik imza oluşturma amacı dışında kullanılmaz. İmza oluşturma verisinin güvenli elektronik imza oluşturma dışında kullanılması sonucu oluşabilecek zararlardan sertifika sahibi sorumludur.

Sertifika sahibi, geçerlilik süresi dolmuş veya iptal olmuş sertifikalara ait imza oluşturma verilerini kullanarak yasal geçerliliği olan işlem yapamaz.

4.5.2. Üçüncü Kişilerin Sertifika ve İmza Doğrulama Verisini Kullanımı

Üçüncü kişiler, oluşturulmuş güvenli elektronik imzayı doğrulama işlemini, sertifika içeriğinde bulunan imza doğrulama verisini kullanarak yapar. Sertifika içeriğindeki imza doğrulama verileri, üçüncü kişilerce imza doğrulaması dışında kullanılmaz.

İmza doğrulama verisinin veya sertifikanın, güvenli elektronik imza doğrulaması 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. ESHS bu işlemi gerçekleştirmez.

4.7. Sertifika Yenileme

ESHS, sertifika yenileme işlemini, yeni anahtar çifti üretmek sureti ile yerine getirir.

4.7.1. Sertifika Yenileme Koşulları

Sertifika yenileme işlemi:

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

yapılmaktadır.

4.7.2. Sertifika Yenileme Başvurusunu Kimlerin Yapabildiği

Bölüm 4.1.1'de tanımlanmaktadır.

4.7.3. Sertifika Yenileme Başvurusunun İşlenmesi

Bölüm 4.2'de tanımlanmaktadır.

4.7.4. Sertifika Yenileme ile İlgili Sertifika Sahibinin Bilgilendirilmesi

Bölüm 4.3.2'de tanımlanmaktadır.

4.7.5. Sertifika Yenileme Sonrası Kabul Koşulu

Bölüm 4.4.1'de tanımlanmaktadır.

4.7.6. Sertifika Yenileme Sonrası Sertifikanın Yayımlanması

Bölüm 4.4.2'de tanımlanmaktadır.

4.7.7. Sertifika Yenilemenin Diğer Taraflara Duyurulması

Bölüm 4.4.3'de tanımlanmaktadır.

4.8. Sertifikada Bilgi Değişikliği

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

Sertifikada yer alan bilgilerde değişiklik olması, sertifikanın değiştirilmesini gerektirir. ESHS, sertifikada bilgi değişikliği gerçekleştirmez. Sertifikada bilgi değişikliği gerekli ise sertifika anahtar yenileme ile yeni bir sertifika üretilir.

4.9. Sertifikanın İptali ve Askıya Alınması

4.9.1. Sertifikanın İptal Edildiği Durumlar

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

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

- durumlarında iptal edilir.

4.9.2. Sertifika İptal Başvurusunu Kimler Yapabilir

Sertifika iptal başvurusu aşağıda tanımlanan kişiler tarafından yapılabilir;

- Sertifika sahibinin kendisi,
- Kurum,
- Kamu SM, madde 4.9.1'de tanımlanan tüm durumlarda iptal yetkisine sahiptir.

4.9.3. Sertifika İptal Başvurusunun İşlenmesi

Bireysel sertifika iptal başvurusu internet üzerinden veya telefonla yapılabilir.

Kurumun iptal başvurularını ne şekilde yapacağı SUE dokümanında anlatılır.

Kamu SM tarafından gerçekleştirilen iptaller sonrası, sertifika sahibi ve bağlı bulunduğu kurum bilgilendirilir.

Geçerli iptal başvurusunun alınmasından sonra sertifika derhal iptal edilir.

4.9.4. İptal İsteği Ertelenme Süresi

Böyle bir süre öngörülmemiştir.

4.9.5. İptal İsteğinin İşlenme Süresi

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

4.9.6. Üçüncü Kişilerin Sertifika İptal Durumunu Kontrol Gerekliliği

Üçüncü kişilerin, sertifika sahiplerine ait sertifikaları işleme almadan önce, geçerlilik durumlarını ESHS'nin işaret ettiği internet ortamından edinebilecekleri SİL dosyasından veya tanımlanan diğer yöntemler aracılığıyla kontrol edip öğrenme sorumluluğu vardır.

Kamu SM, sertifikaların iptal edildiği zamanın tam olarak tespit edilmesini sağlayan, üçüncü kişilerin herhangi bir kimlik doğrulamasına gerek olmaksızın kesintisiz ve ücretsiz olarak ulaşabileceği şekilde iptal durum kaydını yayımlar. İptal edilen sertifika bilgisi, iptal durum kayıtlarında yer alır. Kayıtların bir sonraki güncelleme zamanı, söz konusu kayıtlarda açıkça gösterilir.

Sertifika iptal durum kaydının duyurulması için yaygın olarak kullanılan yöntem, "Sertifika İptal Listesi (SİL)" yayımlamaktır. İptal edilen sertifikalar, sertifikanın geçerlilik süresinin sonuna kadar

SİL içinde tutulur. Sertifikanın iptal durum kaydına erişim, internet üzerinden çevrim içi yöntemlerle de sağlanabilir. SİL veya çevrim içi iptal durum kaydına erişimin sağlanacağı internet adresleri SUE dokümanında belirtilir.

4.9.7. Sertifika İptal Listesi Yayımlama Sıklığı

NES için sertifika iptal listeleri internet ortamından, iptal bilgisini yeterli güncellikte sunacak şekilde, en geç 1 (bir) günlük periyodik aralıklarla yayımlanır. Bir sonraki SİL yayımlama tarihi, duyurulan zamandan daha önce olabilir.

ESHS sertifikaları için SİL yayımlanma sıklığı 1 (bir) yıldan fazla olamaz.

SİL yenileme aralığı ESHS tarafından, sertifikaların kullanım amacının kritikliği doğrultusunda tespit edilir ve SUE'de belirtilir.

4.9.8. Sertifika İptal Listesi Yayımlama Gecikme Süresi

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

4.9.9. Çevrim İçi Sertifika İptal Durum Kaydı Desteği

ESHS, SİL yanında ÇİSDUP (Çevrim İçi Sertifika Durum Protokolü) desteğini sağlar.

4.9.10. Çevrim İçi Sertifika İptal Durum Kaydı Kontrol Gereksinimi

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

4.9.11. Diğer Sertifika Durum Bildirim Yöntemleri

ESHS, bu dokümanda belirtilmeyen ancak yaygınlıkla kullanılmaya başlanan diğer sertifika iptal durum kaydı bildirim yöntemlerini de destekleyebilir. Bu yöntemlerin neler olduğunu SUE dokümanında açıklar. Kullanılan yöntemler iptal durum kaydının bütünlüğünü ve ESHS tarafından yayımlandığını doğrulayacak şekilde tanımlanmış olmalıdır.

4.9.12. İmza oluşturma Verisinin Güvenliğini Yitirmesi Durumu

Sertifika sahibine ait imza oluşturma verisinin güvenliğini yitirmesi durumunun, sertifikanın iptal nedeni olması dışında herhangi bir husus öngörülmemiştir.

4.9.13. Sertifikanın Askıya Alındığı Durumlar

Askıya alma işlemi, sertifikanın geçici süre iptal edilmesi amacıyla tanımlanmıştır. Askıya alınmış bir sertifika iptal olmuş muamelesi görür. Ancak askıdan çıkartıldığında, yeniden geçerli bir sertifika olarak kullanılır.

Sertifikanın geçici olarak kullanım dışı olmasının istendiği durumlarda, sertifika sahibinin isteği doğrultusunda sertifika askıya alınır.

ESHS'lere ait sertifikalar askıya alınmaz.

4.9.14. Sertifika Askıya Alma Başvurusunu Kimlerin Yapabildiği

Askıya alma başvurusu sertifika sahibi tarafından yapılır.

4.9.15. Sertifika Askıya Alma Başvurusunun İşlenmesi

Askıya alma başvurusunun işlenme yöntemi, Bölüm 4.9.3'de belirtilen iptal başvurusu işlenme yöntemleri ile aynı biçimde yapılabilir.

4.9.16. Askıda Kalma Süresi

Böyle bir süre öngörülmemiştir.

4.10. Sertifika Durum Servisleri

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

4.10.1. İşletimsel Özellikleri

SİL dosyası ESHS'ye ait bilgi deposunda güncel haliyle tutulur. SİL dosyasına erişmek isteyen üçüncü kişiler, SUE'de belirtilen erişim adreslerini kullanarak dosyayı kendi sistemlerine yüklerler. Bir sonraki SİL dosyasının yayımlanma tarihi bir öncekinde belirtilir. SİL dosyası, yeni bir iptal olması durumunda güncelleme tarihinin dolması beklenmeden yeniden yayımlanabilir. Güncel SİL dosyasına erişmek isteyen üçüncü kişilerin, her sertifika iptal durum kaydını öğrenmek istediklerinde, SİL dosyasını ESHS bilgi deposundan kendi sistemlerine indirerek, gerekli kontrolleri yapmaları önerilir.

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

4.10.2. Servisin Erişilebilirliği

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

4.10.3. İsteğe Bağlı Özellikler

Düzenlenmesine gerek duyulmamıştır.

4.11. Sertifika Sahipliğinin Sona Ermesi

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

4.12. Anahtar Yeniden Üretme

Sertifika sahiplerine ait anahtarların yeniden üretilmesi veya yedeklenmesi işlemi uygulanmaz.

5. Yönetim, İşlemsel ve Fiziksel Kontroller

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

5.1. Fiziksel Güvenlik Denetimleri

ESHS sisteminin kurulu olduğu cihazlara, yetkisiz kişilerce erişim engellenir; hırsızlık, kaybolma gibi tehlikelere karşı gerekli önlemler alınır. Bunun için, sistemin kurulu olduğu binalar belirli güvenlik ihtiyaçlarını karşılar.

5.1.1. Tesis Yeri ve İnşaatı

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

5.1.2. Fiziksel Erişim

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

5.1.3. Güç Kaynağı ve Havalandırma

ESHS işlemlerinin sürekliliği için sistem, kesintisiz güç kaynağı ile beslenir.

Bina gerekli havalandırma sistemi ile donatılır.

5.1.4. Su Baskınları

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

5.1.5. Yangın Önleme ve Korunma

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

5.1.6. Saklama ve Yedekleme Ortamlarının Korunması

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

5.1.7. Atıkların Yok Edilmesi

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

5.1.8. Farklı Mekanlarda Yedekleme

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

5.2. Prosedürsel Kontroller

5.2.1. Güvenilir Roller

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

5.2.2. Her İşlem İçin Gereken Kişi Sayısı

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

5.2.3. Kimlik Doğrulama ve Yetkilendirme

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

5.2.4. Görevlerin Ayrılmasını Gerektiren Roller

ESHS içinde, aynı kişininin birden fazla görevde bulunmasını engelleyecek sınırlamalar getirilebilir.

5.3. Personel Güvenlik Kontrolleri

5.3.1. Kişisel Geçmiş, Deneyim ve Nitelik Gerekleri

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

5.3.2. Geçmiş Araştırması

ESHS'nin istihdam ettirdiği personel, taksirli suçlar hariç olmak üzere, affa uğramış olsalar bile ağır hapis veya 6 (altı) aydan fazla hapis ya da basit veya nitelikli zimmet, irtikap, rüşvet, hırsızlık, dolandırıcılık, sahtekarlık, inancı kötüye kullanma, dolanlı iflas gibi yüz kızartıcı suçlar ile istimal ve istihlak kaçakçılığı dışında kalan kaçakçılık suçları, resmi ihale ve alım satımlara fesat karıştırma, kara para aklama veya devlet sırlarını açığa vurma, vergi kaçakçılığı ya da iştirak veya bilişim alanındaki suçlar nedeniyle hüküm giymemiş kişilerden oluşur. Bu şartların sağlanması için personeli işe almadan önce ESHS gerekli güvenlik soruşturmasını yapar.

5.3.3. Eğitim Gerekleri

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

5.3.4. Sürekli Eğitim Gerekleri ve Sıklığı

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

5.3.5. Görev Değişim Sıklığı ve Sırası

Düzenlenmesine gerek duyulmamıştır.

5.3.6. Yetkisiz Eylemlerin Cezalandırılması

ESHS personelinin mevzuata aykırı işlem yapması halinde ilgili mevzuat gereğince işlem yapılır.

5.3.7. Anlaşmalı Personel Gereksinimleri

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

5.3.8. Sağlanan Dokümantasyon

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

5.4. Denetim Kayıtları

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

5.4.1. Kaydedilen İşlemler

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

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

5.4.2. Kayıtların İncelenme Sıklığı

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

5.4.3. Kayıtların Saklanma Süresi

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

5.4.4. Kayıtların Korunması

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

5.4.5. Kayıtların Yedeklenmesi

Sistemin işleyişi ile ilgili elektronik kayıtlar, en azından her gün, sistemin yoğun olarak kullanılmadığı bir saatte yedeklenir. Sistem, geri kazanım işlevini yerine getirebilecek kapasitede olmalıdır. Herhangi bir arıza durumunda sistemin son durumuna dönebilmek için, alınan en son kayıt yedekleri sisteme yüklenir.

5.4.6. Kayıtların Toplanması

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

5.4.7. Kayda Sebebiyet Veren Tarafın Bilgilendirilmesi

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

5.4.8. Saldırıya Açıklığın Değerlendirilmesi

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

5.5. Kayıt Arşivleme

Elektronik ya da kağıt üzerinde tutulan kayıtlar ESHS tarafından arşivlenir.

5.5.1. Arşivlenen Kayıt Bilgileri

Elektronik veya kağıt ortamda arşivlenmesi gereken kayıtlar şunlardır:

- Bölüm 5.4.1'de belirtilen, elektronik olarak kaydı yapılan tüm işlemler
- Üretilen tüm sertifikalar
- Yayımlanan tüm Sertifika İptal Listeleri
- Sertifika İlkeleri dokümanı
- Sertifika Uygulama Esasları dokümanı
- Zaman Damgası İlkeleri
- Zaman Damgası Uygulama Esasları
- Sertifika taahhütnameleri
- Sözleşmeler
- Sertifika sahibinin sertifika başvurusu sırasında beyan ettiği kimlik bilgileri ve verdiği tüm belgeler
- Sertifika sahibinin çalıştığı kurum veya kuruluş tarafından beyan edilen bilgi ve belgeler
- İptal, askıya alma ve sertifika başvuru formları
- Verilen hizmetler sırasında yapılan önemli yazışmalar, alınan ve gönderilen fakslar

5.5.2. Arşivlerin Tutulma Süresi

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

5.5.3. Arşivlerin Korunması

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

5.5.4. Arşivlerin Yedeklenmesi

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

5.5.5. Kayıtların Zaman Damgası Gereksinimleri

ESHS gerekli gördüğü kayıtlara zaman damgası ekleyebilir.

5.5.6. Arşivlerin Toplanması

Arşivler elektronik veya kağıt ortamda toplanır.

5.5.7. Arşiv Bilgilerinin Elde Edilme ve Doğrulanma Metodu

Arşiv bilgileri, yetkili personelden edinilir. Aynı bilgiye ait birden fazla arşiv olması durumunda, arşivler kıyaslanarak doğruluğu kontrol edilir.

5.6. Anahtar Değişimi

ESHS'ye ait anahtarların ve sertifikaların, güvenlik sebeplerinden dolayı değiştirilmesi gerekebilir. Bu durumda eski anahtarlar, geçerlilik süresinin sonuna kadar kullanılabilir durumda saklanır. ESHS'nin imza oluşturma verisinin değişiminden itibaren, yeni üretilecek olan sertifikalar yeni imza oluşturma verisiyle imzalanır. Ancak, eskiden üretilmiş olan sertifikaların doğrulanabilmesi için, eski imza doğrulama verisinin içinde bulunduğu ESHS'ye ait eski sertifikaların erişilebilirliğinin sağlanması gerekir.

5.7. Güvenliğin Yitirilmesi ve Arıza Durumlarında Yapılacaklar

5.7.1. Güvenilirliğin Yitirilmesi Durumunun Düzeltilmesi

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

5.7.2. Donanım, Yazılım veya Veri Bozulması

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

5.7.3. İmza Oluşturma Verisinin Gizliliğinin Kaybedilmesi

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

ESHS için, yeni anahtar çiftleri oluşturularak yeni bir sertifika üretilir. Üretilen yeni sertifika, güvenilir yollardan ilgili taraflara iletilir. Eski imza oluşturma verisi ile imzalanan son kullanıcı sertifikaları iptal edilir ve en kısa sürede yenilenen ESHS imza oluşturma verisi kullanılarak yeniden sertifikalar üretilir ve dağıtılır.

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

5.7.4. Arıza Sonrası Yeniden Çalışırlık

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

5.8. Sertifika Hizmetlerinin Sonlandırılması

ESHS'nin işleyişine, Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik'te belirtilen şekilde son verilebilir. Bu durumda yapılacaklar ilgili SUE'de tanımlanmıştır. ESHS sertifika hizmetlerine son verecek olursa, bu durumu 3 (üç) ay öncesinden tüm sistem bileşenlerine duyurur. ESHS sistemi ile ilgili tüm kayıtlar ve arşivler, uygun bir şekilde yönetmeliğe uygun süre boyunca korunur; kamuya açık bilgilere erişim, sistemin işlerliğine son verilmesinden sonra yönetmelikte belirtilen süre kadar devam eder. En son yayımlanan, güncel SİL'ler, sistemin kapanmasından sonra en az 1 (bir) yıl süreyle erişime açık tutulur.

6. Teknik Güvenlik Kontrolleri

ESHS'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

ESHS'ye ait, sertifika imzalama amaçlı kullanılan anahtar çiftleri, yetkisi olmayan personelin giremeyeceği gizli odada, yazılım veya donanım aracı içinde üretilirler. Anahtar üretiminde kullanılan algoritmalar ve anahtar uzunlukları, Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de belirtilen şekilde seçilir. Anahtar çiftlerinden imza oluşturma verisi, güvenli kriptografik donanım aracı içinde saklanır ve bu ortamdan yedekleme amacı dışında dışarıya çıkarılmaz. Üretilen anahtar çiftinin gerekli güvenlik şartlarını sağlaması için uygun üretim ve test yöntemleri kullanılır.

6.1.1.2. Sertifika Sahibi Anahtar Çiftinin Üretimi

Anahtar çiftleri, ESHS tarafından yetkisi olmayan personelin giremeyeceği gizli odada, yazılım veya donanım aracı içinde üretilirler. Anahtar üretiminde kullanılan algoritmalar ve anahtar uzunlukları Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de belirtilen şekilde seçilir. Anahtar çiftinin gerekli güvenlik şartlarını sağlaması için uygun üretim ve test yöntemleri kullanılır. Sertifika sahibine ait imza oluşturma verisi güvenli elektronik imza oluşturma aracı içinde saklanır, kopyası veya anahtar çifti üretiminde kullanılan gizli değişkenler hiçbir şekilde sistemde tutulmaz. Güvenli elektronik imza oluşturma aracı sertifika sahibine teslim edilene kadar yetkisiz kişilerin erişemediği güvenli ve kilitli odalarda saklanır.

6.1.2. Sertifika Sahibine İmza Oluşturma Verisinin Ulaştırılması

Üretilen imza oluşturma verisi şifrelenerek, ilgili sertifika ile birlikte, güvenli elektronik imza oluşturma aracı içinde, sertifika sahibine kimlik kontrolü ve imza karşılığında teslim edilir.

Güvenli elektronik imza oluşturma aracı erişim verisi ise aşağıdaki yöntemlerle sertifika sahibine teslim edilir;

- Kapalı parola zarfı içinde imza karşılığı ve kimlik kontrolü yapılarak,

- Web üzerinden, güvenli bağlantı ve güçlü kimlik doğrulama gerçekleştirilerek.

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. Elektronik Sertifika Hizmet Sağlayıcısı Sertifikalarına Erişim Sağlanması

ESHS'ye ait sertifikalar, internet ortamında ilgili tarafların erişimine hazır bulundurulur. Ayrıca, ESHS kendi sertifikasına ait sertifika özet değeri ile özetleme algoritmasını internet sitesi üzerinden yayımlar ve faaliyete geçmesini müteakip 7 (yedi) gün içinde ulusal yayın yapan en yüksek trajlı 3 (üç) gazetede ilan vermek suretiyle kamuoyuna duyurur. Üçüncü kişiler, sertifika özet değerini, yayımlanan özet değeriyle kıyaslayarak sertifikanın güvenilirliğine karar verirler.

6.1.5. Anahtar Uzunlukları

ESHS'nin, nitelikli elektronik sertifikaları ve iptal durum kayıtlarını imzalamak amacıyla kullandığı anahtar çiftlerinin uzunluğu en az 5 (beş) yıl boyunca güvenliği sağlayacak şekilde belirlenir.

Sertifika sahibine ait anahtar çiftlerinin uzunluğu en az 3 (üç) yıl boyunca güvenliği sağlayacak şekilde belirlenir.

Belirlenen anahtar uzunlukları Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'e uygundur.

6.1.6. Anahtar Üretim Parametreleri ve Kalitesinin Kontrolü

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

6.1.7. Anahtar Kullanım Amaçları

Üretilen sertifikalar ve ilgili imza oluşturma verileri Elektronik İmza Kanunu'nda tanımlı güvenli elektronik imzayı üretmek ve doğrulamak amacıyla kullanılırlar.

ESHS'ye ait anahtar çiftleri sertifika imzalama, SİL imzalama, sertifika iptal durum kaydı imzalama ve ESHS'nin işleyişinde gerekli olduğu durumlarda elektronik imza, kimlik doğrulama, mesaj bütünlüğünün ve gizliliğinin sağlanması amacıyla kullanılırlar.

6.2. İmza Oluşturma Verisinin Korunması

6.2.1. Kriptografik Modül Standartları

ESHS'ye ait, sertifika imzalama amaçlı kullanılan imza oluşturma verisinin üretildiği veya saklandığı kriptografik modül ile sertifika sahibine ait güvenli elektronik imza oluşturma aracı, Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de belirtilen güvenlik standartlarını sağlar.

Kriptografik modül ve güvenli elektronik imza oluşturma aracı, üzerinde kayıtlı olan elektronik imza oluşturma verilerinin araç dışına hiçbir biçimde çıkarılamamasını ve gizli kalmasını sağlar; üzerinde kayıtlı olan elektronik imza oluşturma verilerinin, üçüncü kişilerce elde edilememesini, kullanılamamasını ve elektronik imzanın sahteciliğe karşı korunmasını sağlayacak teknik özelliklere sahiptir.

6.2.2. İmza Oluşturma Verisine Birden Fazla Kişi Kontrolünde Erişim

ESHS'ye ait imza oluşturma verisine erişim birden fazla kişinin kontrolünde sağlanır.

6.2.3. İmza Oluşturma Verisinin Yeniden Elde Edilmesi

Düzenlenmesine gerek duyulmamıştır.

6.2.4. İmza Oluşturma Verisinin Yedeklenmesi

ESHS'ye ait, sertifika imzalama amaçlı kullanılan imza oluşturma verileri, yetkisiz kişilerin erişimine kapalı, fiziksel ve elektronik olarak güvenli kriptografik donanım cihazı içinde yedeklenir. İmza oluşturma verisinin yedeklenmesi işlemi, birden fazla yetkili çalışanın ortak denetimi altındadır.

Sertifika sahiplerine ait imza oluşturma verileri yedeklenmez.

6.2.5. İmza Oluşturma Verisinin Arşivlenmesi

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

6.2.6. İmza Oluşturma Verisinin Kriptografik Modüle Yüklenmesi

ESHS'ye ait, sertifika imzalama amaçlı kullanılan imza oluşturma verileri, güvenlik gereklerine uygun biçimde kriptografik modül dışında üretilebilir. Ancak, imza oluşturma verisinin kriptografik

modül içinde saklanması zorunludur. Kriptografik modül dışında üretilen imza oluşturma verisi, yetkili birden fazla personelin denetiminde modüle yüklenir.

Sertifika sahibinin imza oluşturma verisinin, sertifika sahibine ait güvenli elektronik imza oluşturma aracı dışında üretilmesi durumunda, imza oluşturma verisi güvenli elektronik imza oluşturma aracı içine yetkili personelden başkasının giremediği güvenli odalarda ve şifreli olarak yüklenir. İmza oluşturma verisinin güvenli elektronik imza oluşturma aracı içinde üretilmesi durumunda, aracın Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de belirtilen güvenlik standartlarına uygunluğu sağlanır.

6.2.7. İmza Oluşturma Verisinin Kriptografik Modülde Saklanması

ESHS'ye ait sertifika imzalamak amaçlı kullanılan imza oluşturma verileri yetkisiz kişilerin erişimine kapalı, fiziksel ve elektronik olarak güvenli kriptografik modül içinde şifreli olarak tutulur. İmza oluşturma verisinin kriptografik modül dışına çıkması engellenir.

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

6.2.8. İmza Oluşturma Verisine Erişim

ESHS'ye ait, sertifika imzalama amaçlı kullanılan imza oluşturma verisi güvenli algoritma ve yöntemlerle şifreli olarak güvenli kriptografik modül içinde saklanır. İmza oluşturma verisinin erişime açılması ve kullanılır duruma getirilmesi, yetkili birden fazla çalışanın ortak denetimi altındadır.

Sertifika sahibine ait güvenli elektronik imza oluşturma aracı içindeki imza oluşturma verisine erişim, sadece sertifika sahibinin bildiği parola veya diğer kriptografik yöntemler ile sağlanır.

6.2.9. İmza Oluşturma Verisine Erişimin Kesilmesi

İmza oluşturma verisi imzalama için kullanıldıktan sonra, 6.2.7'de tanımlanan şekilde erişime yeniden açılıncaya kadar erişime kapalı tutulur.

6.2.10. İmza Oluşturma Verisinin Yok Edilmesi

ESHS'ye ait imza oluşturma verilerinin aslı ve bütün yedekleri kullanım süresinin dolmasının ardından, bulunduğu sistemden uygun yöntemlerle geri dönüşsüz şekilde silinir. İmza oluşturma verisinin silinmesi, birden fazla yetkili çalışanın ortak denetimi altındadır.

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

6.2.11. Kriptografik Modülün Değerlendirilmesi

ESHS, bölüm 6.2.1 de belirtilen standartlara uygun kriptografik modül kullanır.

6.3. Anahtar Çifti Yönetimiyle İlgili Diğer Konular

6.3.1. İmza Doğrulama Verisinin Arşivlenmesi

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

6.3.2. İmza Oluşturma ve Doğrulama Verilerinin Kullanım Süreleri

İmza oluşturma ve doğrulama verilerinin kullanım süreleri, kullanım amaçlarına göre birbirlerinden farklı olabilir. İmza doğrulama verisinin kullanım süresi içinde bulunduğu sertifikanın geçerlilik süresidir.

Kullanıcı sertifikalarını imzalamak için kullanılan ESHS'ye ait imza oluşturma verisinin kullanım süresi ilgili mevzuatta tanımlanan süreden fazla olamaz.

İptal durum kayıtlarını imzalamak için kullanılan ESHS'ye ait imza oluşturma verilerinin kullanım süresi, sertifikanın kullanım süresi kadardır.

Sertifika sahiplerine ait imza oluşturma verilerinin kullanım süresi sertifikanın kullanım süresi ile aynıdır. Kullanıcılara ait sertifikaların son kullanma tarihi, sertifikayı imzalayan ESHS'ye ait sertifikanın son kullanma tarihinden fazla olamaz.

6.4. Erişim Denetim Verileri

Erişim denetim verileri ESHS çalışanlarının erişim parolalarını, güvenli donanım araçları içindeki erişim denetimi sağlayan diğer verileri ve sertifika sahiplerinin güvenli donanım araçlarına erişim parolalarını içerir.

6.4.1. Erişim Denetim Verilerinin Oluşturulması

ESHS sistemi içinde kullanılan erişim denetim verileri ile sertifika sahibine ait erişim parolaları yetkisiz kişilerin erişime kapalı, fiziksel ve elektronik olarak güvenli ortamlarda tahmin edilemez rastsallıkta üretilir.

6.4.2. Erişim Denetim Verilerinin Korunması

ESHS sistemi içinde kullanılan erişim denetim verileri yalnızca yetkili çalışanlar tarafından bilinir, diğer veriler ve bunları içeren güvenli donanım araçları yetkisiz erişime karşı güvenli saklanır.

Güvenli elektronik imza oluşturma aracı erişim verisi ESHS'de bulunduğu süre zarfında, güvenli bir ortamda şifreli olarak saklanır.

6.4.3. Erişim Denetim Verileri İle İlgili Diğer Konular

Erişim denetimi verilerinin sahibine ulaştırılması güvenli yollarla yapılır. Sertifika sahibine ait erişim parolaları kapalı zarf içinde, kimlik kontrolü yapılarak imza karşılığı ya da güvenli çevrim içi yöntemlerle sahibine teslim edilir.

6.5. Bilgisayar Güvenliği Denetimleri

6.5.1. Bilgisayar Güvenliği İle İlgili Teknik Gerekler

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

6.5.2. Bilgisayar Sisteminin Sağladığı Güvenlik Seviyesi

Düzenlenmesine gerek duyulmamıştır.

6.6. Yaşam Döngüsü Teknik Denetimleri

6.6.1. Sistem Geliştirme Denetimleri

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

6.6.2. Güvenlik Yönetimi Denetimleri

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

6.6.3. Yaşam Döngüsü Güvenlik Denetimleri

Düzenlenmesine gerek duyulmamıştır.

6.7. Ağ Güvenliği Denetimleri

ESHS sisteminde son teknolojik gelişmeler göz önünde bulunarak gerekli ağ güvenliği denetimleri yapılır.

6.8. Zaman Damgası

ESHS sistemi içinde kullanılan zaman damgası Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de belirtilen şartlara uyar.

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

7. Sertifika ve Sertifika İptal Listesi Biçimleri

7.1. Sertifika Biçimi

7.1.1. Sürüm Numarası

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

7.1.2. Sertifika Uzantıları

ESHS ve son kullanıcı sertifikaları içinde, ITU-T X.509 V.3 tarafından desteklenen bütün uzantılar kullanılabilir. Nitelikli elektronik sertifika profilleri oluşturulurken ETSI TS 101 862'de belirtilen yöntemler kullanılır. Kamu SM tarafından belirlenen ilkelere uygun sertifika üretim ve yönetimi yapıldığının belirtildiği uzantılarla ilgili açıklamalar aşağıda anlatılmıştır.

7.1.2.1. Anahtar Kullanım Alanları Uzantısı

ESHS tarafından üretilen nitelikli elektronik sertifikaların anahtar kullanım alanı uzantısında "inkar edilemezlik" tanımının tek başına veya "sayısal imza" tanımıyla birlikte kullanılması gerekir. Anahtar kullanımı ile ilgili diğer tanımlar sertifika içeriğinde bulunmaz.

Üretilen nitelikli elektronik sertifikalar içeriğinde tanımlanabilecek anahtar kullanım alanları kombinasyonları aşağıdaki tabloda verilmiştir:

Tablo 1 NES Anahtar Kullanım Alanları

Sertifikanın Tipi	İnkar Edilemezlik[1]	Sayısal İmza[2]	Anahtar Şifreleme[3] veya Anahtar Anlaşması[4]
Nitelikli elektronik sertifika	√		-
Nitelikli elektronik sertifika	√	√	-

ESHS'ye ait sertifikaların içindeki anahtar kullanım alanı uzantısında, "sertifika imzalama[5]" ve "SİL imzalama[6]" tanımları kullanılır.

7.1.2.2. Nitelikli Sertifika İbaresi Uzantısı

ESHS tarafından üretilen nitelikli elektronik sertifikalarda "Nitelikli Sertifika İbaresi"[7] uzantısının bulunması zorunludur. Nitelikli olmayan sertifikalarda bu uzantı bulunmaz. "Nitelikli Sertifika İbaresi" uzantısının kullanımı ETSI TS 101 862'ye uygun olarak yapılır. Bu uzantı içerisinde aşağıdaki "ibare tanımlayıcılar"[8] mevcuttur:

[1] Non-Repudiation

[2] DigitalSignature

[3] KeyEncipherment

[4] KeyAgreement

[5] KeyCertSign

[6] CRLSign

[7] QcStatements

[8] StatementID

- Nitelikli Elektronik Sertifika'nın ETSI'ye uygunluğunun gösterilmesi amacıyla ETSI tarafından tanımlanan aşağıdaki "ibare tanımlayıcı" uzantının içinde bulunur.

  Nesne Tanımlama Numarası: 0.4.0.1862.1.1

  { itu-t(0) identified-organization(4) etsi(0) id-qc-profile(1862) id-etsi-qcs(1) id-etsi-qcs-QcCompliance(1) }

- Nitelikli Elektronik Sertifika'nın 5070 sayılı Elektronik İmza Kanunu'na uygunluğunun gösterilmesi amacıyla BTK tarafından tanımlanan aşağıdaki "ibare tanımlayıcı" ve ibarenin kendisi metin olarak uzantının içinde bulunur. Bu ibare ve ibareye ait nesne tanımlama numarası aşağıda belirtilmiştir:

  Nesne Tanımlama Numarası: 2.16.792.1.61.0.1.5070.1.1

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

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

Sertifikanın kullanımına ilişkin, varsa maddi sınırlamalar ile ilgili bilgilendirme de "Nitelikli Sertifika İbaresi Uzantısı" içinde ETSI TS 101 862'de belirtilen biçimde yapılır. Bu amaçla aşağıdaki "ibare tanımlayıcı" kullanılır:

- Nesne Tanımlama Numarası: 0.4.0.1862.1.2

{ itu-t(0) identified-organization(4) etsi(0) id-qc-profile(1862) id-etsi-qcs(1) id-etsi-qcs-QcLimitValue(1) }

7.1.3. Algoritma ve Nesne Tanımlayıcılar

Kullanılan algoritmaların nesne tanımlayıcıları üretilen sertifikaların içeriğinde belirtilir.

7.1.4. İsim Alanı Biçimleri

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

7.1.5. İsim Kısıtları

ESHS'nin ürettiği sertifikaların içinde kişiyi tekil olarak tanımlamayı sağlayacak nitelikte isim bilgileri kullanılır. Sertifika sahibinin ad ve soyadı bilgisi ile gerekiyorsa çalıştığı şirket veya kurumun bilgisi resmi kayıtlarda geçen isimlerden oluşmak zorundadır.

Kamu SM'ye ait ESHS sertifikalarında tanımlanan isim alanları ve bu isim alanlarına yazılan bilgiler aşağıdaki tabloda belirtilmiştir. Sürüm X ibaresi rakam olarak 1 den başlar ve yeni Kök SHS ve Kamu ESHS sertifikası üretildiğinde rakam olarak bir sonraki değeri alır.

Tablo 2 Sertifika İsim Alanları

Alan Adı[9]	**Kök SHS Sertifikası**	**Kamu ESHS Sertifikası**
CN	TÜBİTAK UEKAE Kök Sertifika Hizmet Sağlayıcısı [Sürüm X]	Kamu Elektronik Sertifika Hizmet Sağlayıcısı [Sürüm X]
O	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu-TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu-TÜBİTAK
OU	Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü-UEKAE	Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü-UEKAE
OU	Kamu Sertifikasyon Merkezi	Kamu Sertifikasyon Merkezi
L	Gebze-Kocaeli	Gebze-Kocaeli
C	TR	TR

7.1.6. Sertifika İlkeleri Nesne Tanımlama Numarası

Bu Sİ dokümanına ait nesne tanımlama numarası bu dokümanın 1.2. Bölüm'ünde verilmiştir.

7.1.7. İlke Kısıtları Uzantısının Kullanımı

Düzenlenmesine gerek duyulmamıştır.

[9] CN: Common Name [Genel isim], O: Organization [Organizasyon adı], OU: Organization Unit [Organizasyon birimi], L: Locality [Şehir], C: Country [Ülke]

7.1.8. İlke Niteleyiciler

ESHS'lere ait elektronik sertifikaların Kamu SM Sİ dokümanına uygunluğu "Sertifika İlkeleri Uzantısı" içine Sİ dokümanına ait nesne tanımlama numarasının yazılmasıyla belirtilir. "Sertifika İlkeleri Uzantısı[10]" içindeki "İlke Niteleyici[11]" olarak belirtilen alana ESHS'ye ait SUE dokümanının erişilebileceği internet adresi tanımlanır.

ESHS'ler Kamu SM tarafından belirlenen ilke ve esasların yanında başka kurumlar tarafından belirlenen ilke ve esaslara da uygun olarak çalışabilir. Bu durumda ESHS veya son kullanıcı sertifikalarının içinde Kamu SM Sİ nesne tanımlama numarasının yanında başka Sİ dokümanlarına referans veren nesne tanımlama numaraları da bulunur.

Kullanıcı sertifikalarının "Sertifika İlkeleri Uzantısı" içine Sİ dokümanına ait nesne tanımlama numarası, "İlke Niteleyici" olarak belirtilen alana, Kamu SM'nin belirlediği ilkelere uygun olarak yazılmış SUE dokümanının bulunduğu internet adresi yazılır. Kamu SM tarafından tanımlanan nitelikli sertifika ibaresi "Kullanıcı Bildirim[12]" alanına yazılır. Kamu SM tarafından tanımlanan nitelikli sertifika ibaresi aşağıda verilmiştir:

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

7.1.9. Kritik Belirtilmiş Olan İlke Belirleyici Uzantılarının İşlenmesi

Düzenlenmesine gerek duyulmamıştır.

7.2. Sertifika İptal Listesi Biçimi

7.2.1. Sürüm Numarası

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

7.2.2. Sertifika İptal Listesi Uzantıları

SİL uzantıları ile ilgili detay SUE dokümanında yer almaktadır.

---

[10] Certificate Policies

[11] Policy Identifier

[12] User Notice

7.3. Çevrim İçi Sertifika Durum Protokolü Biçimi

7.3.1. Sürüm Numarası

Çevrim İçi Sertifika Durum Protokolü RFC 2560'da belirtilen versiyonları destekler.

7.3.2. ÇİSDUP Uzantıları

Çevrim İçi Sertifika Durum Protokolü RFC 2560'da tarif edilen "ÇİSDUP" formatını destekler.

8. Uygunluk Denetimleri

Bu bölümde, Kamu SM Sİ dokümanına bağlı olarak çalıştığını beyan eden ESHS'lerin denetlenmesi ile ilgili hususları kapsamaktadır.

ESHS, mevzuat gereği BTK tarafından incelenir/denetlenir.

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

ESHS iç işleyişini denetlemek için, ayrıca iç denetimler gerçekleştirilir.

8.1. Uygunluk Denetiminin Sıklığı

Bu Sİ dokümanına uygun çalışan ESHS'ler, iki yılda en az bir defa BTK tarafından denetlenir.

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

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

8.2. Denetçinin Nitelikleri

ESHS faaliyetlerinin denetimi, kanunla yetkilendirilmiş olan BTK tarafından gerçekleştilir.

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

İç denetim, Sİ dokümanının gereklerini iyi anlayan ve uygunluk denetimi konusunda tecrübeli ESHS personeli tarafından gerçekleştirilir.

8.3. Denetçinin Denetlenen Tarafla Olan İlişkisi

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

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

İç denetim, Sİ dokümanının gereklerini iyi anlayan ve uygunluk denetimi konusunda tecrübeli ESHS personeli tarafından gerçekleştirilir.

8.4. Denetimin Kapsamı

ESHS'lerin denetim kapsamı BTK tarafından belirlenir.

BGYS standardına uygun denetim kapsamı bağımsız kurum denetçisi tarafından belirlenir.

İç denetim kapsamı denetimi gerçekleştirecek ESHS personeli tarafından belirlenir.

8.5. Yetersizliğin Tespiti Durumunda Yapılacaklar

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

ISO/IEC 27001 standardına göre gerçekleştirilen denetimlerde ortaya çıkan eksiklikler, ESHS tarafından planlı çalışma ile giderilir. Eksiklikler, BGYS'sinin temel işleyişini etkileyecek kadar büyük ise, ISO/IEC 27001 uygunluk belgesi eksikler giderilinceye kadar askıya alınır.

İç denetimlerde ortaya çıkan eksiklikler, ESHS ilgili personeli tarafından giderilir.

8.6. Sonucun Bildirilmesi

BTK ve ISO/IEC 27001 denetçilerinin hazırladığı resmi raporlar ile ESHS'ye bildirilir.

İç denetim sonuçu, ESHS üst yönetimine raporlanır.

9. Diğer İşler ve Hukuksal Meseleler

9.1. Ücretlendirme

9.1.1. Sertifika Oluşturma ve Yenileme Ücreti

ESHS tarafından üretilen, güncellenen ve yenilenen her sertifika için ücret alınır. Ödenecek bedelin miktarı ile ilgili bilgilendirmenin ne şekilde yapıldığı SUE dokümanında belirtilir.

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

9.1.2. Sertifika Erişim Ücreti

ESHS, kendisine ve sertifika sahiplerine ait sertifikaları ücretsiz olarak erişime açar.

9.1.3. İptal Durum Kaydına Erişim Ücreti

ESHS, iptal durum kaydını duyurmak için sertifika sahibinden veya üçüncü kişilerden ücret talep etmez.

9.1.4. Diğer Servis Ücretleri

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

9.1.5. İade Ücreti

Sertifika sahibi sertifikasını ilk teslim aldığında yaptığı kontrol neticesinde, sertifikasını kullanamadığını tespit ederse ve sorunun ESHS'den kaynaklanan bir hata sebebiyle ortaya çıktığı anlaşılırsa, talebi halinde sertifika sahibinin sertifika için ödenen ücreti iade edilir.

9.2. Finansal Sorumluluk

9.2.1. Sigorta Kapsamı

ESHS kendi sorumluluklarını karşılamak amacıyla sigorta yaptırabilir.

9.2.2. Diğer Varlıklar

Düzenlenmesine gerek duyulmamıştır.

9.2.3. Sertifika Mali Sorumluluk Sigortası

ESHS'nin dağıttığı nitelikli elektronik sertifikalar, 15 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza Kanunu gereğince mali sorumluluk sigortası ile sigortalanır.

9.3. Ticari Bilginin Korunması

9.3.1. Gizli Bilginin Kapsamı

Paylaşılan iş planları, satış bilgileri, ticari sırlar ve yapılan gizli anlaşmalarda verilen bilgiler, ticari bilgi olarak değerlendirilir.

9.3.2. Gizlilik Kapsamında Olmayan Bilgiler

ESHS'nin kendi güvenliğini sarsmayacak şekilde, yönetimsel ve teknik bilgi ile güvenlik stratejisini gerçekleştirme yolu gizlilik kapsamında olmayan bilgilerdir.

9.3.3. Gizli Bilginin Korunma Sorumluluğu

Sertifika hizmeti verilirken ESHS ve ilgili kuruluşların karşılıklı paylaştığı ticari bilgiler üçüncü taraflara açılmaz.

9.4. Kişisel Bilginin Gizliliği

9.4.1. Gizlilik Planı

Düzenlenmesine gerek duyulmamıştır.

9.4.2. Gizli Olarak Tanımlanan Bilgiler

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

9.4.3. Gizli Olarak Tanımlanmayan Bilgiler

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

9.4.4. Gizli Bilginin Korunma Sorumluluğu

ESHS, 5070 sayılı Elektronik İmza Kanunu uyarınca kişilere ait gizli bilgilerin korunması için aşağıda belirtilen şartları yerine getirir:

- Elektronik sertifika talep eden kişiden, elektronik sertifika vermek için gerekli bilgiler haricinde bilgi talep edemez ve bu bilgileri kişinin rızası dışında elde edemez,
- Elektronik sertifika sahibinin izni olmaksızın sertifikayı üçüncü kişilerin ulaşabileceği ortamlarda bulunduramaz,
- Elektronik sertifika talep eden kişinin yazılı rızası olmaksızın üçüncü kişilerin kişisel verileri elde etmesini engeller. Bu bilgileri sertifika sahibinin onayı olmaksızın üçüncü kişilere iletemez ve başka amaçlarla kullanamaz.

9.4.5. Gizli Bilginin Kullanımına İzin Verilmesi

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

9.4.6. Yetkili Merciilerin Kararına Uygun Olarak Bilginin Açıklanması

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

9.4.7. Diğer Başlıklar

Düzenlenmesine gerek duyulmamıştır.

9.5. Telif Hakları

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

9.6. Temsil Hakkı ve Yükümlülükler

ESHS'nin verdiği sertifika hizmetlerinde sistem bileşenleri olan ESHS'ler, sertifika sahipleri ve üçüncü kişiler 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 belirtilen şekilde üzerlerine düşen yükümlülükleri sağlarlar. ESHS'ler, sertifika sahipleri ve üçüncü kişiler yasa ve yönetmeliklerde belirtilmediği halde, karşılıklı imzaladıkları sözleşmelerde, taahhütnamelerde, Sİ,

SUE, Zaman Damgası İlkeleri ve Zaman Damgası Uygulama Esasları dokümanlarında sözü geçen yükümlülükleri de yerine getirirler.

9.6.1. Elektronik Sertifika Hizmet Sağlayıcısı Yükümlülükleri

Elektronik imzaya ilişkin mevzuata uygun olarak elektronik sertifikaları üretmek, sertifika verdiği kişilerin kimliğini resmi belgelere göre güvenilir bir biçimde tespit etmek, yenileme, askıya alma ve iptal gibi sertifika işlemlerinin gerçekleştirilmesini sağlamak, iptal olmuş sertifika bilgilerini zamanında ve doğru olarak duyurmak, sertifikanın veya sertifika işlemleriyle ilgili başvuruların durumu hakkında ilgili kişileri bilgilendirmekle yükümlüdür.

9.6.2. Kayıt Birimi Yükümlülükleri

Düzenlenmesine gerek duyulmamıştır.

9.6.3. Sertifika Sahibinin Yükümlülükleri

Sertifika sahibi başvuru, yenileme, askıya alma ve iptal işlemlerini Kamu SM sertifika ilkelerinde belirtilen yöntemlere uygun olarak tanımlanmış usule göre yerine getirmek, sertifikasını ve ilgili imza oluşturma verisini, varsa taraflar arası sözleşme veya taahhütnameler ile Sİ ve SUE dokümanlarında belirtildiği şekilde kullanmak, imza oluşturma verisinin içinde bulunduğu güvenli elektronik imza oluşturma aracının kayıp ve üçüncü kişilerin yetkisiz kullanımı durumlarına karşı Bölüm 6.1, 6.2 ve 6.4'de belirtilen şekillerde gereken önlemleri almak, imza oluşturma verisinin güvenliğinin yitirildiğinden şüphelendiği durumlarda sertifikasını iptal ettirmek, sertifika başvurusu sırasında doğru bilgi beyan etmekle yükümlüdür.

Bölüm 1.4'te belirtilen sertifika kullanım amaçları dışındaki kullanımlarda kendisinin ve üçüncü kişilerin görebileceği zararlar, kendisine ait imza oluşturma verisi kullanılarak yapılan işlemler, elektronik imza oluşturma verisini kullandığı sırada sertifikasının geçerli (kullanım süresinin dolmamış olması ve iptal edilmemiş/askıya alınmamış olması) durumda olması sertifika sahibinin yükümlülükleri arasındadır.

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

9.6.4. Üçüncü Kişilerin Yükümlülükleri

Üçüncü kişiler, sertifikaları kullanmadan önce gerekli geçerlilik kontrollerini yapmakla yükümlüdür. Üçüncü kişiler, sertifikanın geçerlilik kontrolünü yapıp yapmamaya veya geçerlilik

kontrolünü ne şekilde yapacaklarına kendileri karar verirler. Sertifikaları uygun geçerlilik denetimlerini yapmadan kullandığı takdirde doğabilecek zararlardan sorumludur.

ESHS'nin yayımladığı SUE dokümanı üçüncü kişilerin yapması gereken sertifika geçerlilik kontrollerinin neler olması gerektiğini belirtir.

9.6.5. Diğer Bileşenlerin Yükümlülükleri

Diğer bileşenlerin yükümlülükleri SUE dokümanında anlatılmaktadır.

9.7. Yükümlülüklerden Feragat

ESHS ile sertifika sahipleri ve kurumlar arasındaki yükümlülük karşılıklı imzalanan sözleşmelerde veya taahhütnamelerde belirtildiği şekilde sona erer.

9.8. Sorumlulukla İlgili Sınırlamalar

ESHS ve sertifika hizmeti alan tarafların sorumlulukları 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 belirtilen şartlar ile sınırlıdır.

9.9. Tazminat Halleri

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

9.10. Anlaşma Süresi ve Anlaşmanın Sona Ermesi

9.10.1. Anlaşma Süresi

Sertifika hizmetlerinin gerçekleştirilmesinde ESHS ile sertifika sahipleri ve ilgili kuruluşlar karşılıklı imzaladıkları sözleşmeler veya taahhütnameler süresince işbirliği içinde çalışır; süreçleri yerine getirirken gerekli desteği ve koordinasyonu Sİ ve SUE dokümanlarında belirtilen şartlar altında sağlar.

9.10.2. Anlaşmanın Sona Ermesi

ESHS ile sertifika hizmetlerini alan taraflar arasında imzalanan sözleşmeler veya taahhütnameler, sözleşme veya taahhütnameye uygun olarak yapılan taleple sonlandırılabilir. Anlaşmanın sonlandırıldığı durumlar SUE dokümanında anlatılır.

9.10.3. Anlaşmanın Sona Ermesinin Etkileri

ESHS ile sertifika hizmetlerini alan taraflar arasında imzalanan sözleşme veya taahhütnamenin sona ermesi ile sertifika hizmeti alan tarafların Sİ ve SUE dokümanları ile ilgili yükümlülükleri sona erer. Ancak ESHS, dağıttığı nitelikli elektronik sertifikalarla ilgili, elektronik imza mevzuatında belirtilen yükümlülüklerini yerine getirmeye devam eder.

9.11. Sistem Bileşenleri İle Haberleşme ve Kişisel Bilgilendirme

Sertifika yönetim prosedürleri içindeki kritik her işlem sonrasında ESHS sertifika sahibini bilgilendirir. ESHS ile sertifika sahipleri arasındaki haberleşmeler posta yoluyla, telefonla veya elektronik ortam üzerinden yapılır.

9.12. Değişiklik Halleri

9.12.1. Değişiklik Metodları

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

9.12.2. Bilgilendirme Mekanizması ve Sıklığı

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

9.12.3. Nesne Tanımlama Numarasının Değişmesini Gerektiren Durumlar

Kamu SM'nin, Sİ dokümanında belirlediği ilkelerde yaptığı değişiklikler, sertifika kullanım amaç ve hedeflerini temel anlamda değiştirmediği sürece yeni Sİ dokümanı için yeni bir nesne tanımlama numarası almasına gerek yoktur. Kamu SM eski kullandığı nesne tanımlama numarasını

yeni Sİ dokümanı için de kullanabilir. Ancak, sertifika ilkelerinde yaptığı değişiklikler sertifikanın kullanım amacını değiştiriyorsa Kamu SM'nin yeni belirlediği Sİ dokümanı için yeni bir nesne tanımlama numarası alması zorunludur.

9.13. Anlaşmazlık Halleri

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

9.14. Uygulanacak Hukuk

Sİ dokümanındaki hükümler 15 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza Kanunu'na 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.