SERTİFİKA UYGULAMA ESASLARI (SUE)

(Nitelikli Elektronik Sertifikalar içindir)

SÜRÜM : 10

TARİH : 02.06.2016

1. GİRİŞ

TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. (kitapçıkta bundan sonra kısaca "TÜRKTRUST" olarak anılacaktır), 23 Ocak 2004 tarih ve 25355 sayılı Resmi Gazete'de yayımlanmış ve 23 Temmuz 2004 tarihinde yürürlüğe girmiş olan 15 Ocak 2004 tarihli ve 5070 sayılı "Elektronik İmza Kanunu (kitapçıkta bundan sonra kısaca "Kanun" olarak anılacaktır)" ve Kanun gereği Bilgi Teknolojileri ve İletişim Kurumu tarafından yayımlanmış olan Yönetmelik ve Tebliğ uyarınca, elektronik sertifika hizmet sağlayıcılığı alanında faaliyet göstermektedir.

Sertifika Uygulama Esasları (SUE) (Nitelikli Elektronik Sertifikalar içindir) olarak adlandırılan bu kitapçık, TÜRKTRUST'ın sertifika hizmet sağlayıcılığı alanındaki nitelikli elektronik sertifika faaliyetlerini nasıl yürüttüğünü göstermek amacıyla, Bilgi Teknolojileri ve İletişim Kurumu'nun kanun kapsamında yayımlamış olduğu "Elektronik İmzaya İlişkin Süreçler ve Teknik Kriterlere İlişkin Tebliğ"in 7. Maddesi uyarınca "IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" rehber kitapçığına uygun olarak TÜRKTRUST tarafından hazırlanmıştır.

SUE dokümanı, nitelikli elektronik sertifika başvurularının alınması, üretimi ve yönetimi, yenileme ve iptal işlemleriyle ilgili hizmetlerin, idari, teknik ve yasal gerekliliklere uygun olarak yürütülmesiyle ilgili esasları ortaya koyar; elektronik sertifika hizmet sağlayıcısı (ESHS) olarak TÜRKTRUST'ın, sertifika sahibinin ve üçüncü kişilerin uygulama sorumluluklarını belirler.

1.1. Genel Bakış

SUE dokümanı, TÜRKTRUST'ın verdiği nitelikli elektronik sertifika hizmetlerini kapsar. SUE'de yer alan uygulama esasları, TÜRKTRUST'ın tüm müşteri hizmetleri, kayıt merkezleri ve sertifika üretim merkezleri uygulamalarını kapsar.

TÜRKTRUST sertifika hizmet sağlayıcısı, ilgili Sertifika İlkeleri (Sİ) kitapçığı hükümlerine bağlı bir uygulama kitapçığı olan bu SUE uyarınca işletme faaliyetlerini yürütür.

TÜRKTRUST, elektronik sertifika hizmetlerini, SUE dokümanında yer alan uygulama esaslarına göre hazırlanan ve ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi ile TS EN ISO 9001 Kalite Yönetim Sistemi uyarınca dokümante edilen prosedür ve talimatlar ile müşteri kılavuzları aracılığıyla yürütür.

Sertifika İlkeleri (Sİ) ve Sertifika Uygulama Esasları (SUE) kitapçıkları mevzuat ve standartlar çerçevesinde en az yılda bir kere Yönetim Gözden Geçirme Toplantısında değerlendirilir. Bu değerlendirmeler ya da yıl içinde ortaya çıkabilecek gereklilikler doğrultusunda bu kitapçıklar güncellenir.

1.2. Kitapçık Adı ve Tanımlama

Bu SUE dokümanının açık adı "TÜRKTRUST Sertifika Uygulama Esasları (SUE) (Nitelikli Elektronik Sertifikalar içindir) "dır. Kitapçığın sürüm numarası ve tarihi kapak sayfasında yer almaktadır.

TÜRKTRUST SUE dokümanı, TÜRKTRUST Sİ dokümanında tanımlanan sertifika ilkeleri uyarınca TÜRKTRUST'ın sertifika hizmetleri ile ilgili faaliyetlerini nasıl yürüttüğünü açıklar. SUE dokümanı, Sİ'de belirlenen ve nesne tanımlayıcı numarası (OID) aşağıda verilen sertifika ilkelerinin uygulama esaslarını kapsar:

- TÜRKTRUST NES İlkeleri (2.16.792.3.0.3.1.1.1): Kanun, yönetmelik ve tebliğ uyarınca, bireylerin elle atılan imzaya eşdeğer güvenli elektronik imza kullanımına olanak veren nitelikli elektronik sertifikaları kapsar. Mobil imza kullanım amaçlı nitelikli elektronik sertifikalar da aynı ilkelere bağlıdır.

SUE dokümanı "http://www.turktrust.com.tr" web adresinde kamuya açık olarak yayımlanmaktadır.

1.3. Taraflar

Bu uygulama esasları kitapçığında hak ve yükümlülükleri tanımlanan TÜRKTRUST sertifika hizmetleriyle ilgili taraflar, sertifika hizmetlerini veren ESHS birimleri ve hizmeti alan müşteri ve kullanıcılar olarak tanımlanır.

1.3.1. Sertifika Üretim Merkezleri

Sertifika üretim merkezleri, ESHS'lerin nitelikli elektronik sertifika üretim, dağıtım ve yayımlamasından sorumlu birimleridir. TÜRKTRUST sertifika üretim merkezleri bir hiyerarşi içinde çalışır. Ana sertifika üretim merkezi TÜRKTRUST'ın kök sertifikasına sahiptir. Bu merkez tarafından üretilmiş alt kök sertifikalara sahip olan diğer sertifika üretim merkezleri tarafından son kullanıcı sertifikaları üretilir.

TÜRKTRUST ile Türkiye Barolar Birliği (TBB) arasında yapılan anlaşma gereği TBB, avukatlardan veya Türk Yargısında görev yapan hakim, savcı ve benzeri her türlü görevliden oluşan kapalı bir kullanıcı kitlesine yönelik olarak, TÜRKTRUST Sİ ve SUE dokümanları uyarınca ve hizmet sözleşmesi çerçevesinde, TÜRKTRUST kök sertifikasına bağlı TBB NES alt kökü aracılığıyla, NES üretim ve dağıtım faaliyetleri yürütmektedir.

1.3.2. Sertifika Kayıt Merkezleri

Sertifika kayıt merkezleri, ESHS'lerin nitelikli elektronik sertifika başvuru, yenileme ve iptal gibi doğrudan son kullanıcılara yönelik hizmetlerini yürüten birimleridir. Bu birimler, prosedürler uyarınca müşteri kayıtlarını oluşturur, gerekli kimlik tanımlama ve doğrulama süreçlerini yürütür, ilgili sertifika taleplerini sertifika üretim merkezlerine yönlendirir.

Kayıt merkezleriyle ilgili işlemler, TÜRKTRUST satış temsilcilerinden gelen sertifika başvuruları doğrultusunda TÜRKTRUST merkezinde yer alan kayıt birimlerince yürütüldüğü gibi, doğrudan TÜRKTRUST'a bağlı kayıt merkezleri tarafından da yürütülür. Her iki durumda da, sertifika talepleri TÜRKTRUST sertifika üretim merkezine iletilir ve sertifika üretimi gerçekleştirilir.

1.3.3. Sertifika Sahipleri

Sertifika sahipleri, kimlik veya unvanları doğrulanan ve buna bağlı olarak adlarına sertifika üretilen kişilerdir.

Kimlik veya unvan doğrulaması, ilgili mevzuat ve standartlara göre yapılır. Sertifika sahibinin sorumluluğu ve sertifika kullanımından doğan sonuçlar, ilgili mevzuatla ve sertifika sahibi taahhütnamesiyle belirlenir.

1.3.4. Üçüncü Kişiler

Üçüncü kişiler, TÜRKTRUST sertifika hizmetleri kapsamında, TÜRKTRUST tarafından verilmiş olan nitelikli elektronik sertifikalara bağlı imza oluşturma verileriyle imzalanmış belgeleri alan, ilgili sertifikalara güvenen taraflardır.

TÜRKTRUST tarafından verilmiş sertifikaların kullanımına bağlı üçüncü kişilere karşı TÜRKTRUST'ın sorumluluğunun sınırları işbu kitapçıkta belirtilmiştir.

1.3.5. Diğer Katılımcılar

TÜRKTRUST nitelikli elektronik sertifika hizmetleri kapsamında nitelikli elektronik sertifika üretimi, bilgi deposu yayımlama ve benzeri sertifika hizmetlerinin tümü TÜRKTRUST tarafından verilir.

TÜRKTRUST, nitelikli elektronik sertifika hizmetlerini verirken işbirliği yaptığı ve hizmet aldığı tüm kişi ve kuruluşlardan oluşan diğer katılımcıların verecekleri hizmeti güvenilir ve doğru biçimde vereceklerini iş süreçleri ve müşterilerle ilgili gizli veya özel bilgileri açığa çıkarmayacaklarını garanti etmelerini sağlamak amacıyla sözleşmeler imzalar.

1.4. Sertifika Kullanımı

1.4.1. Geçerli Sertifika Kullanım Şekilleri

TÜRKTRUST kök ve alt kök sertifikaları sadece kullanım amaçları doğrultusunda sertifika imzalamak için kullanılır.

TÜRKTRUST NES, ilgili mevzuat uyarınca elle atılan imzayla aynı hukuki sonucu doğuran güvenli elektronik imza oluşturmak amacıyla kullanılır. E-devlet, e-ticaret ve benzeri uygulamalarda belge ve form imzalamak, elektronik ortamdaki her türlü sözleşme ve kontrat gibi ticari veya resmi belgeleri imzalamak, e-posta mesaj metinlerini imzalamak, web üzerindeki işlem talimatlarını imzalamak, kimlik tanımlama ve doğrulama gerektiren ağ ortamlarında kimliği ispat etmek geçerli sertifika kullanım şekilleridir.

1.4.2. Yasaklanmış Sertifika Kullanım Şekilleri

TÜRKTRUST NES, mevzuatta belirlenen şartlar dışında kullanılamaz.

1.5. Sertifika İlkeleri Yönetimi

TÜRKTRUST sertifika ilkelerini oluşturan otorite olarak, işbu SUE dokümanının bağlı bulunduğu Sİ dokümanının yönetimi ve kayıt altına alınmasından sorumludur.

1.5.1. SUE Dokümanından Sorumlu Organizasyon

İşbu SUE dokümanının tüm hakları ve sorumluluğu TÜRKTRUST'a aittir.

1.5.2. İletişim Noktası

SUE dokümanıyla ilgili iletişim bilgileri aşağıdadır:

TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş.
Adres : Hollanda Caddesi 696.Sokak No:7 Yıldız, Çankaya 06550 ANKARA
Telefon : (90-312) 439 10 00
Faks : (90-312) 439 10 01
Çağrı Merkezi : 0 850 222 444 6
E-posta : sertifika@turktrust.com.tr
Web : http://www.turktrust.com.tr

1.5.3. SUE'nin İlkelere Uygunluğunu Belirleyen Yetkili

TÜRKTRUST SUE dokümanının TÜRKTRUST Sİ dokümanına uygunluğu TÜRKTRUST üst yönetimi tarafından belirlenir.

1.5.4. SUE Onaylama Prosedürleri

SUE dokümanı TÜRKTRUST Yönetim Kurulu tarafından onaylanır. Gerekli onayı alan SUE, ESHS faaliyetlerini düzenlemek ve işletmek için kullanılır.

TÜRKTRUST üst yönetimi, bu SUE dokümanında belirtilen gerekliliklerin karşılanması için oluşturulan sertifika uygulama esaslarının, uygun bir biçimde yürütülmesini sağlamaktan sorumludur.

1.6. Kısaltmalar ve Tanımlar

1.6.1. Kısaltmalar

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

NES : Nitelikli Elektronik Sertifika

OID : Object Identifier – Nesne Tanımlayıcı Numarası

OCSP : On-line Certificate Status Protokol – Çevrim İçi Sertifika Durum Protokolü

PKI : Public Key Infrastructure – Açık Anahtarlı Altyapı

RFC : IETF tarafından yayımlanan, kılavuz niteliğinde yorum talebi dokümanları

Sİ : Sertifika İlkeleri

SİL : Sertifika İptal Listesi

SUE : Sertifika Uygulama Esasları

TCKN : T.C. Kimlik Numarası

TSE : Türk Standartları Enstitüsü

1.6.2. 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 bir yöntemdir. Bu yöntemde 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 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 Çifti: Aynı anda üretilen ve güvenli elektronik imza oluşturma aracına yüklenen imza oluşturma verisi ile imza doğrulama verisidir.

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): 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 (Online Certificate Status Protokol OCSP): Sertifikaların geçerlilik durumunun kamuya duyurulması için oluşturulmuş, sertifika durum bilgisinin çevrim içi yöntemlerle anında ve kesintisiz alınmasını sağlayan standart protokoldür.

Denetim: ESHS'nin her türlü faaliyet ve işleyişinin ilgili mevzuat hükümlerine ve standartlara uygunluğunun incelenerek; muhtemel hata, noksanlık, usulsüzlük veya suistimallerin 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 (ESHS): 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.Maddesinde sayılan niteliklere sahip imza doğrulama aracıdır.

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

Hat Kullanıcısı: Mobil iletişim cihazı hat sahibi tarafından kullanılıyorsa hat sahibinin kendisidir; mobil iletişim cihazı hat sahibinin bilgisi ve onayı ile başka bir kişi tarafından kullanılıyorsa, mobil imza hizmetini de kapsayan mobil operatör hizmetlerinin kullanıcısı olan kişidir.

Hat Sahibi: Mobil operatörün kurmuş olduğu GSM sisteminde verilen hizmetlerden yararlanmak üzere, kendi isteğiyle ve abonelik sözleşmesinde belirtilen hükümler çerçevesinde mobil operatör şebekesine kaydını yaptırmak için bizzat veya vekili ya da yetkilisi aracılığıyla başvurarak abonelik sözleşmesini imzalayan ve hükümlerine uymayı taahhüt eden gerçek veya tüzel kişidir.

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.

Kurumsal Başvuru: Bir tüzel kişiliğin çalışanları, müşterileri, üyeleri veya hissedarları adına yaptığı nitelikli elektronik sertifika başvurusudur.

Mobil İmza: Mobil iletişim cihazlarıyla, ilgili ağ ve hizmet altyapısı kullanılarak nitelikli elektronik sertifika sahibi tarafından oluşturulan güvenli elektronik imzadır.

Mobil İmza Hizmeti: Kanun ve ilgili mevzuat koşullarına uyan ve kullanıcılar tarafından mobil iletişim cihazları aracılığıyla çeşitli servislerde kullanılacak imzaya ilişkin verilen hizmettir.

Mobil Operatör: Mobil imza kullanıcısı nitelikli elektronik sertifika sahiplerine GSM altyapısı üzerinden işlem yapma imkânı sağlayan ve mobil imza kullanım amaçlı nitelikli elektronik sertifikalar için kurumsal başvuru sahibi olan operatördür.

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 imzalanan kişidir.

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

Sertifika Kayıt Merkezi: ESHS yapısında yer alan, nitelikli elektronik sertifika başvuruları ile sertifika yenileme başvurularını alan, ilgili kimlik tanımlama ve doğrulama süreçlerini yürüten, sertifika taleplerini onaylayarak sertifika üretim merkezine yönelten, ESHS faaliyetleri kapsamında müşteri ilişkilerini yöneten alt birimlere sahip olan birimdir.

Sertifika Üretim Merkezi: ESHS yapısında yer alan, onaylı sertifika talepler doğrultusunda nitelikli elektronik 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, sertifika içinde yer alan tüm bilgi alanlarının aynı şekilde kullanılmasıyla yeni bir sertifikanın üretilmesidir. Sertifika yenileme için, sertifikanın geçerli olması zorunludur.

SIM Kart: Hat sahiplerinin mobil operatörden temin edeceği, çeşitli özel uygulamaları barındıran, mobil iletişim cihazlarıyla entegre çalışan ve mobil imza hizmetinde kullanılabilen SIM karttır.

Tebliğ: Bilgi Teknolojileri ve İletişim Kurumu tarafından yayımlanan Elektronik İmza İle İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'dir.

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

Zaman Damgası: Bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı 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.

2. YAYIN VE BİLGİ DEPOSU SORUMLULUKLARI

TÜRKTRUST, elektronik sertifika hizmet sağlayıcılığı kapsamında sertifika hizmetleriyle ilgili gereken doküman ve kayıtları hazırlamak ve saklamakla yükümlüdür. Bu doküman ve kayıtların bazıları, sertifika hizmetlerinin etkin bir şekilde müşterilere ulaştırılabilmesi ve sertifika kullanımının güvenilirliğinin ve sürekliliğinin sağlanması amacıyla kamuya açık olarak yayımlanır.

2.1. Bilgi Deposu

TÜRKTRUST, bilgi deposunda tutulan tüm bilgilerin doğruluğunu ve güncelliğini sağlar. TÜRKTRUST, bilgi deposunu işletmek ve ilgili doküman ile kayıtları yayımlamak için üçüncü bir güvenilir kişi ya da kuruluş kullanmaz.

2.2. Sertifika Bilgilerinin Yayımlanması

TÜRKTRUST bilgi deposunda, ESHS iç işleyişine ait özel kurumsal prosedür ve talimatlar ile ticari gizli bilgiler dışında kalan, sertifika hizmetlerinin yürütülmesine ilişkin bilgiler herkesin erişimine açık tutulur. Nitelikli elektronik sertifika kapsamında ESHS'nin temel çalışma ilkelerini içeren Sİ dokümanı, bu ilkelerin nasıl uygulandığını gösteren SUE dokümanı, sertifika sahibi ve ESHS sertifika hizmetleri taahhütnameleri, sertifika süreçleriyle ilgili müşteri kılavuzları, herkesin erişimine açık olarak bilgi deposunda yer alır. Ayrıca, TÜRKTRUST elektronik sertifika ve zaman damgası hizmetlerine ilişkin tüm kök ve alt kök sertifikaları herkesin erişimine açık olarak dizin sunucularda ve bilgi deposunda yayımlanır. Güncel iptal durum kayıtları, hem OCSP desteğiyle hem de SİL'ler aracılığıyla erişime açık tutulur.

TÜRKTRUST tarafından üretilen sertifikalar, ancak sertifika sahibinin yazılı rızasıyla herkesin erişimine açık tutulur.

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

2.3. Yayımın Zamanı veya Sıklığı

Madde 2.2'de bahsedilen dokümanların yeni sürümleri çıktıkça, eski sürümlerle birlikte bilgi deposunda yayımlanır. TÜRKTRUST kök ve alt kök sertifikaları ve çevrim içi sertifika durum sorgulama kayıtları (OCSP) sürekli yayımlanır. SİL, 12 (oniki) saatte bir olmak üzere günde 2 (iki) kez ve 24 (yirmidört) saatlik geçerlilik süresiyle yayımlanır. SİL geçerlilik süresi konusunda tek istisna kök ve alt kök sertifikaların geçerlilik sürelerinin dolması sırasında yaşanır. SİL içinde bulunan bir sonraki güncelleme tarihinin, kök veya alt kök sertifika geçerlilik bitiş tarihini aşması halinde, SİL içinde bulunan bu değer kök veya alt kök geçerlilik bitiş tarihi olarak yazılır.

TÜRKTRUST, OCSP ve SİL yayımlama hizmetlerinin cevap verme süresinin 10 (on) saniyenin altında kalması sağlar.

2.4. Bilgi Deposuna Erişim Kontrolleri

Bilgi deposu herkesin erişimine açıktır. TÜRKTRUST bu amaçla, yayımlanan bilgilerin gerçekliğini sağlamak üzere, http://www.turktrust.com.tr adresi için gerekli her türlü güvenlik önlemini alır.

3. KİMLİĞİN DOĞRULANMASI

TÜRKTRUST, ilk kez sertifika başvurusunda bulunan, sertifikasını yenilemek isteyen veya yeni bir sertifika edinmek isteyen kişilerin kimliklerini yasal ve teknik gereklilikler uyarınca gerekli tüm bilgilere ve resmi kaynaklara dayandırarak doğrular.

3.1. İsimlendirme

3.1.1. İsim Tipleri

TÜRKTRUST'ın ürettiği tüm sertifikalarda X.500 ayırt edici isimleri kullanılır.

3.1.2. İsimlerin Anlamlı Olması Gerekliliği

Üretilen sertifikalardaki isimler belirsizlikten uzak ve anlamlıdır.

Nitelikli elektronik sertifikaların isim alanlarında, sertifika sahiplerinin TÜRKTRUST tarafından talep edilen kimlik belgelerinden ve güncel nüfus kayıtlarından doğrulanan isimler bulunur. Kök ve alt kök sertifikaların isim alanlarında, TÜRKTRUST'ın ticari unvanı ve ilgili kök bilgisi açık olarak yer alır.

3.1.3. Sertifika Sahiplerinin Anonimliği ve Takma Ad Kullanılabilirliği

TÜRKTRUST, anonim veya takma ad içeren sertifika üretmez.

3.1.4. İsim Biçimlerinin Değerlendirilmesi

Sertifikalarda yer alan isimler X.500 ayırt edici isim biçimine uygun olarak değerlendirilir.

3.1.5. İsimlerin Benzersizliği

TÜRKTRUST tarafından verilen sertifikalar, ayırt edici isim alanında yer alan bilgilerle sertifika sahiplerinin eşsiz biçimde belirlenmesine olanak tanır.

TÜRKTRUST NES ayırt edici isim alanı altında yer alan seri numarası (SERIALNUMBER) alanında, Türkiye Cumhuriyeti vatandaşları ve Türkiye'de yerleşik yabancı uyruklular için sertifika sahibinin benzersiz TCKN'si, diğer yabancı uyruklular için uluslararası ülke kodu (ISO 3166-1 alpha-3) ve pasaport numarası yer alır.

3.1.6. Ticari Markaların Tanınması, Doğrulanması ve Rolü

Uygulama dışıdır.

3.2. İlk Kimlik Doğrulama

3.2.1. Gizli Anahtara Sahip Olunduğunun Kanıtlanma Yöntemi

Uygulama dışıdır.

3.2.2. Tüzel Kişiliğin Doğrulanması

Bir sertifikada tüzel kişiliğin isminin veya unvanının yer alması halinde, sertifika sahibinin bulunduğu ülkedeki yasal belgelere bağlı olarak ve TÜRKTRUST prosedürlerinde belirlenen şekilde tüzel kişilik doğrulanır.

3.2.3. Gerçek Kişinin Kimliğinin Doğrulanması

NES başvurusunda bulunan kişilerin sertifikada yer alacak bilgileri, yasal düzenlemelerle belirlenen şekilde ve resmi belgelere dayandırılarak doğrulanır. Kişinin ilk NES başvurusu alınırken, mevzuat gereğince yüz yüze kimlik doğrulaması yapılır.

İkinci ve daha sonraki başvurularda,

- Geçerli son sertifikanın kullanım süresi sonundan itibaren 6 (altı) aydan daha uzun bir süre geçmiş olması veya
- Geçerli son sertifikanın "DN" alanındaki TCKN veya isimde değişiklik olması

durumunda yüz yüze kimlik doğrulaması yapılır. İkinci veya daha sonraki başvurularda kimlik doğrulamasına ihtiyaç olmayan hallerde, telefon, faks veya e-posta gibi yollarla TÜRKTRUST prosedürlerine göre doğrulama yapılır.

NES başvurularında kimliğin doğrulanabilmesi için, nüfus cüzdanı, sürücü belgesi veya pasaport gibi resmi kimlik belgelerinden birinin aslı görülerek fotokopisi alınır. Suretin aslına uygunluğu TÜRKTRUST tarafından teyit edilir. Sertifika içeriğinde mesleki unvanın da yer alacak olması halinde, mevzuata göre düzenlenmiş resmi belgelerin ibraz edilmesi zorunludur.

3.2.4. Doğrulama Yapılmaksızın Sertifikada Yer Alabilen Bilgiler

NES başvurularında e-posta adresi sertifika başvuru sahibinin beyanıyla alınır ve doğrulama yapılmaksızın sertifika içeriğinde yer alır.

Sertifikalarda bulunabilen "S" ve "OU" gibi ayırt edici isim alanında yer alan diğer bilgilerde de sertifika başvuru sahibinin beyanına göre doğru kabul edilir.

3.2.5. Yetkinin Doğrulanması

NES içeriğinde bir tüzel kişiliğin isminin yer alması söz konusu ise sertifika başvuru sahibinin bu tüzel kişiliğe ait resmi belgeleri (Ticaret Sicil Gazetesi vb.) ibraz etmesi zorunludur.

3.2.6. Karşılıklı Çalışma Kriterleri

TÜRKTRUST, başka bir ESHS ile karşılıklı çalışma amacıyla çapraz veya tek yönlü sertifikasyon yapmaz.

3.3. Anahtar Yenileme Taleplerinin Doğrulanması

3.3.1. Rutin Anahtar Yenileme için Kimlik Doğrulama

Anahtar çiftinin güvenli kullanım süresinin sonunda, yeni anahtar çifti üretimi, kullanıcının yeni bir NES başvurusunda bulunmasıyla gerçekleştirilir. Yeni sertifika başvurusu, sertifikanın kullanım süresi içinde, elektronik ortamda ve mevcut sertifikaya bağlı imza oluşturma verisiyle imzalanarak yapılabilir.

Yeni sertifika içinde yer alacak bir bilgide değişiklik gerekmesi durumunda, bu değişikliğin resmi belgeye dayandırılması zorunludur. Sertifikada yer almayan diğer kullanıcı bilgilerindeki değişiklikler ise NES sahibinin yazılı veya elektronik beyanıyla kabul edilir.

Rutin anahtar yenileme işlemleri sırasında başvuru sahibinin başvuru bilgileriyle ilgili herhangi bir tereddüt doğması halinde telefonla doğrulama yapılır. Bu doğrulamayı yapan TÜRKTRUST yetkililerince sözkonusu şüphenin giderilememesi durumunda ise yüz yüze kimlik doğrulaması yapılır.

Geçerli bir NES sahibi için anahtar yenileme talebi, sertifikasının süre sonundan en erken 30 (otuz) gün önce yapılabilir. Yapılmış bir talep en fazla 30 (otuz) gün süreyle geçerliliğini korur.

Sertifika sahibinin ilk başvurusundan yenileme başvurusuna kadar geçen sürede TÜRKTRUST sertifika hizmetlerinin sağlanmasına ilişkin kayıt ve şartlarda değişiklik olmuş ise bu değişiklikler uygun biçimde sertifika sahibine bildirilir.

3.3.2. İptal Sonrası Anahtar Yenileme için Kimlik Doğrulama

Aşağıda sayılan iptal nedenleri dışında iptal sonrası anahtar yenilemesi sırasındaki kimlik doğrulaması Madde 3.3.1'de açıklandığı şekilde yapılır:

- Sertifika içeriğinde yer alan bilgilerdeki eksik, kusur veya hataya bağlı iptaller.
- Sertifika başvurusuyla birlikte alınan yetki belgesi, adres ve benzeri belgelerde eksikliğe, kusura veya hataya veya bu belgelerin geçerliliğini yitirmiş olmasına bağlı iptaller.
- Sertifika sahibinin faaliyetinin devam etmemesi veya yasal varlığının ortadan kalkması veya bunlara ilişkin kuvvetli şüpheye bağlı iptaller.

Burada sayılan haller için anahtar yenileme yapılmaz ve ilk kez başvuru yapılıyormuş gibi sertifika başvuru prosedürleri uygulanır.

3.4. İptal Talebi için Kimlik Doğrulama

TÜRKTRUST, NES iptal taleplerini aşağıda açıklandığı gibi güvenilir yollarla alır ve kimlik doğrulaması yapar:

- Sertifika sahibi, başvuru sırasında belirlenmiş kendisine özel bilgileri doğrulayarak TÜRKTRUST web sayfasından, sesli yanıt sisteminden veya kendisine sağlanmış diğer TÜRKTRUST yazılımlarıyla sertifikasını askıya alır veya iptal eder.
- Sertifika sahibi iptal talebini, TÜRKTRUST'a faksla iletebilir. Bu durumda, sertifika derhal askıya alınır. Yazılı iptal talebinin aslının ulaşmasıyla veya 30 (otuz) günlük askı süresinin dolmasıyla birlikte sertifika iptal edilir. Askı süresi içinde sertifika sahibi iptal nedeninin ortadan kalktığını yazılı olarak tebliğ ederse, sertifika askıdan çıkarılır.

4. SERTİFİKA YAŞAM DÖNGÜSÜ İŞLEVSEL GEREKLİLİKLERİ

TÜRKTRUST, sertifikalarını bu SUE dokümanında yer alan uygulama esasları uyarınca üretir ve yaşam döngüsünü yönetir.

4.1. Sertifika Başvurusu

4.1.1. Kimler Sertifika Başvurusunda Bulunabilir?

Herhangi bir yasal engeli olmayan her gerçek kişi NES başvurusunda bulunabilir.

TÜRKTRUST, bir sertifika başvurusu sırasında sunulacak tüm gerekli bilgileri 20 (yirmi) yıllık bir süre boyunca saklama ve arşivleme hakkı olduğunu beyan eder.

4.1.2. Sertifika Başvuru, Kayıt Süreci ve Sorumluluklar

Sertifika başvuru kaydı, aşağıda açıklandığı gibi iki ana adımdan oluşur:

- Kayıt: Sertifika başvurusu dayanak belgelerine göre doğrulanır ve eksiksiz ve doğru biçimde kaydedilir.
- Anahtar üretimi: Açık ve gizli anahtar çifti TÜRKTRUST tarafından üretilir.

TÜRKTRUST NES başvurusu farklı yöntemlerle gerçekleştirilebilir.

TÜRKTRUST NES başvuruları TÜRKTRUST'ın web sitesinden yapılan çevrimiçi başvuruyla başlatılabilir.

TÜRKTRUST'ın ofisi bulunan yerlerde, başvuru sahibi TÜRKTRUST ofisine şahsen giderek başvuru yapabileceği gibi kendi bulunduğu yerde başvurusu alınmak üzere ücret karşılığında TÜRKTRUST yetkilisinin gelmesini talep edebilir. Bu şekilde yapılan eksprEs-İmza başvurularında sertifika sahibinin başvuru belgeleri elden alınır, kimlik doğrulaması yapılır ve akıllı kartı da elden teslim edilir.

TÜRKTRUST'ın doğrudan hizmet vermediği yerlerde başvuru sahibinin TÜRKTRUST'ın web sitesinden başvurusunu başlatması ve noterde yüz yüze kimlik tespiti yaptırması zorunludur. Başvuru sahibi istenilen kimlik doğrulama belgelerini ve noter onaylı sertifika sahibi taahhütnamesini TÜRKTRUST'a iletir. E-imza paketi sadece NES başvuru sahibine teslim edilmek üzere kurye aracılığıyla gönderilir.

Mobil imza kullanım amaçlı NES başvuruları, kurumsal başvuru sahibi olan mobil operatör tarafından hat kullanıcıları adına, gerekli bilgi ve belgeler hat kullanıcılarından alınarak, mobil imza hizmet altyapısı kullanılarak yapılır.

4.2. Sertifika Başvurusunun İşlenmesi

4.2.1. Kimlik Doğrulama İşlemlerinin Yerine Getirilmesi

NES başvurusu sırasında, başvuru sahibinin kimliği yasal düzenlemeler uyarınca resmi belgelere dayandırılarak doğrulanır. İlk başvuru sırasında kimlik doğrulama işlemi TÜRKTRUST veya noter tarafından yüz yüze yapılır, sonraki başvurularda bu şart aranmayabilir. Bu işlemler sırasında TÜRKTRUST çağrı merkezi başvuru sahibiyle iletişim kurarak başvurusunu doğrular ve başvuru prosedürleri hakkında bilgi verir.

Mobil imza kullanım amaçlı NES başvuruları, mobil operatörü tarafından sağlanan kanallar üzerinden ön kayıt işlemi başlatılır. Ardından, mobil operatörün sağladığı kayıt merkezleri üzerinden hat sahibinin ve/veya hat kullanıcısının başvuru bilgi ve belgeleri alınır. Bu işlemler sırasında, mobil operatörün çağrı merkezi hat sahibiyle ve/veya hat kullanıcısıyla iletişim kurarak başvuru prosedürünü tamamlanmasını sağlar.

4.2.2. Sertifika Başvurularının Kabulü veya Reddedilmesi

Aşağıdaki koşulların yerine gelmesi halinde bir sertifika başvurusu kabul edilir:

- Bölüm 3.2'de açıklanan esaslar ve TÜRKTRUST başvuru prosedürlerine göre gerekli belgelerin eksiksiz olarak tamamlanmış olması.
- TÜRKTRUST çağrı merkezinin başvuru sahibiyle iletişime geçerek başvuruyu doğrulamış olması.
- Ödemenin yapılmış olması.

TÜRKTRUST, aşağıdaki hallerin herhangi birinin oluşması halinde sertifika başvurusunu reddeder:

- Bölüm 3.2'de açıklanan esaslar ve TÜRKTRUST başvuru prosedürlerine göre gerekli belgelerin tamamlanmaması.
- TÜRKTRUST çağrı merkezinin başvuru sahibiyle iletişime geçememesi veya başvuruyu doğrulayamaması.
- Bilgi ve belgelerin doğrulanmasına ilişkin sorgulamalara başvuru sahibinin zamanında veya tatminkâr yanıt vermemesi.
- Ödemenin yapılmamış olması.

4.2.3. Sertifika Başvurularının İşlenme Süresi

TÜRKTRUST'a ulaşan NES başvurularının işlenme süresi en fazla 5 (beş) iş günüdür. TÜRKTRUST "eksprEs-İmza" başvuruları, en fazla 1 (bir) iş günü içinde işlenir.

Bu madde altında sertifika başvurusunun işlenmesine ilişkin verilen süre, sertifika başvurularının Bölüm 3.2'de yer alan esaslar ve TÜRKTRUST prosedürlerine göre eksiksiz ve doğru olması halinde geçerlidir.

İşlenmiş bir sertifika başvurusunun, Bölüm 4.2.2'de yer alan esaslar uyarınca kabul edilmesinden sonra üretimi en geç 1 (bir) iş günü içinde yapılır.

4.3. Sertifika Üretimi

4.3.1. Sertifika Üretimi Sırasındaki ESHS Faaliyetleri

Bölüm 4.2.2'de yer alan esaslar uyarınca kabul edilen sertifika başvuruları TÜRKTRUST sertifika üretim merkezlerinde işlenir ve sertifikalar üretilir.

4.3.2. Sertifika Üretimiyle İlgili Sertifika Sahibinin Bilgilendirilmesi

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

4.4. Sertifikanın Kabulü

4.4.1. Kabulün Şekli

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

eksprEs-İmza üretimi sonrası ilgili sertifika kayıt merkezi aracılığıyla teslim edilecek olan e-imza paketi 1 (bir) ay içinde sertifika başvuru sahibi tarafından teslim alınmazsa, sertifika kabul edilmemiş sayılır, iptal edilir ve ücret iadesi yapılmaz. Benzer şekilde standart NES üretimi sonrası kurye ile gönderilen e-imza paketinin 1 (bir) ay boyunca sertifika başvuru

sahibi tarafından teslim alınmaması durumunda da yine sertifika kabul edilmemiş sayılır, iptal edilir ve ücret iadesi yapılmaz.

4.4.2. ESHS Tarafından Sertifikanın Yayımlanması

Nitelikli elektronik sertifika, sertifika sahibinin yazılı rızası olması kaydıyla web üzerinde veya dizin sunucularda yayımlanır.

4.4.3. Diğer Katılımcıların Sertifika Üretimiyle İlgili Bilgilendirilmesi

Uygulama dışıdır.

4.5. Anahtar Çifti ve Sertifika Kullanımı

4.5.1. Sertifika Sahibi İmza Oluşturma Verisi ve Sertifika Kullanımı

Sertifika sahibi, sertifikasını ve sertifikaya ait gizli anahtarı, Kanun, Yönetmelik ve diğer düzenlemeler ile Sİ ve SUE kitapçıklarında ve ilgili sertifika sahibi taahhütnamesinde yer alan koşullar ve belirlenmiş sınırlar içinde kullanılabilir.

Sertifika sahibi, sertifikasına karşılık gelen gizli anahtarı diğer kişilerin erişimine karşı korumak ve kendisine mevzuat ile Sİ ve SUE kitapçıklarında ve ilgili sertifika sahibi taahhütnamesinde tanınan yetki ve sınırlar içinde kullanmakla yükümlüdür.

NES için imza oluşturma verisi erişim şifresi, aktivasyon işlemiyle sertifika sahibi tarafından TÜRKTRUST'ın sağlamış olduğu yazılım aracılığıyla belirlenir.

NES sahibi,

- Adına düzenlenen güvenli elektronik imza oluşturma aracını şahsen teslim almalıdır.
- Aktivasyonla belirlenen erişim şifreleri için cep telefonunun veya e-posta adresinin diğer kişilerce kullanımına izin vermemelidir.
- Aktivasyonla belirlenen erişim şifreleri ve güvenli elektronik imza oluşturma aracının diğer kişilerce kullanımına izin vermemelidir.
- İmza oluşturma verisinin ve/veya imza oluşturma aracının, kayıp, açığa çıkma, değişime uğrama ve diğer kişilerce kullanımı durumlarında veya bu durumların oluşmasına neden olabilecek şartların ortaya çıkması halinde sertifikanın iptalini sağlamak üzere derhal ESHS'ye bilgi vermelidir.

4.5.2. Üçüncü Kişilerin İmza Doğrulama Verisi ve Sertifika Kullanımı

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

Sertifikanın geçerliliğinin kontrolü makul ve güvenli koşullar altında yapılmalıdır. Aksi yönde bir durumun oluştuğuna dair bir tereddüt olması halinde, üçüncü kişiler gerekli tedbirleri alır. Bu bağlamda üçüncü kişiler sertifikaya güvenmeden önce;

- Sertifikanın kullanım amacına uygun kullanıldığını; özel olarak bir hatanın yaralanma, ölüm veya çevresel zarara yol açabildiği nükleer tesis, hava trafik kontrol, uçak navigasyon veya silah kontrol gibi sistemlerde kullanılmadığını,
- Sertifika içeriğinde yer alan "anahtar kullanımı" alanının kullanım durumuyla uyumlu olduğunu,

- Sertifikanın dayandığı kök ve alt kök sertifikalarının geçerli olduğunu, sertifikanın askıya alınmadığını, iptal edilmediğini veya süresinin dolmadığını ve sertifikayı veren ESHS'yi tanıdığını,

kontrol etmekle yükümlüdür.

Bu işlemler sırasında, mevzuat ve standartlarca belirlenmiş güvenli yazılım ve donanım araçlarının kullanılması üçüncü kişilerin sorumluluğundadır.

Sertifikaya güvenmeden önce üçüncü kişilerin imza doğrulama verisi ve sertifika kullanımında burada sayılan şartları yerine getirmemelerinden TÜRKTRUST sorumlu tutulamaz.

4.6. Sertifika Yenileme

Sertifika yenileme, sertifika içeriğinde açık anahtar dâhil aynı bilgiler yer almak kaydıyla, sertifika geçerlilik süresinin uzatıldığı yeni bir sertifika üretilmesiyle yapılır.

Sertifika yenilemenin yapılabilmesi için, sertifikanın gizli anahtarının açığa çıkmamış olması zorunludur.

NES'de geçerlilik süresi dolan sertifikalara dayanılarak sertifika yenileme başvurusu yapılamaz. Anahtarların kriptografik güvenliği bakımından, aynı içerikle bir sertifikanın toplam geçerlilik süresi 3 (üç) yıldan fazla olamaz.

4.6.1. Sertifika Yenilemeyi Gerektiren Durumlar

Sertifikanın kullanım süresinin dolmasına belirli bir süre kalmış olması ve sertifika içeriğindeki bilgilerde bir değişiklik olmaması durumunda, sertifika sahibinin talebi üzerine sertifika yenilenir.

Geçerlilik süresi içinde yenileme başvurusunun yapılmış olması kaydıyla, süresi dolmuş sertifika da yenilenebilir. Bu yenileme işlemi en geç 30 (otuz) gün içinde yapılır, aksi takdirde sertifika başvurusu reddedilir.

4.6.2. Yenileme Talebinde Bulunabilecek Kişiler

Sertifika sahibi tarafından yenileme talebinde bulunulabilir.

4.6.3. Sertifika Yenileme Talebinin İşlenmesi

Gizli anahtarın açığa çıkmış olması veya yenileme süresiyle birlikte anahtarların kriptografik güvenliğinin tehlikeye düşecek olması veya yenileme talebinin 30 (otuz) günlük geçerlilik süresini doldurması hallerinde sertifika yenileme talebi reddedilir.

NES için sertifika yenileme süresi her durumda 1 (bir) yıldır. Geçerlilik süresi içinde NES sahibi, sertifika yenileme başvurusunu sadece İnternet üzerinden, TÜRKTRUST uygulaması aracılığıyla ve elektronik imzasıyla yapabilir. Bu işlemle sertifika sahibi sertifika yenileme talebini imzaladığı gibi, sertifikaya bağlı imza oluşturma verisine sahip olduğunu da göstermiş olur. Yenileme talebinin kabulü aşağıdaki şartların tamamının sağlanmasına bağlıdır:

- Sertifika başvuru sahibinden önceki başvuru sırasında verilen bilgilerin hala geçerli olduğunu açıkça gösteren yazılı bir taahhüt alınır. Böyle bir yazılı bir taahhüdün olmaması veya sertifika içeriğinde bilgi değişikliği olduğuna dair bir bilgi alınması durumunda, Bölüm 4.7'de yer alan esaslar uygulanır.
- Yenilenecek sertifikayla birlikte toplam anahtar süresi 3 (üç) yılı aşamaz.
- Öznenin gizli anahtarının ortaya çıkmasına ilişkin bir belirti bulunması durumunda, anahtar yenileme işlemi gerekir.

- Ödemenin yapılmış olması.

4.6.4. Yenilenmiş Sertifikayla İlgili Sertifika Sahibine Bildirim Yapılması

Bölüm 4.3.2'de yer alan esaslar uygulanır.

4.6.5. Yenilenen Sertifikanın Kabulü

Bölüm 4.4.1'de yer alan esaslar uygulanır.

4.6.6. ESHS Tarafından Yenilenen Sertifikanın Yayımlanması

Bölüm 4.4.2'de yer alan esaslar uygulanır.

4.6.7. Diğer Katılımcıların Yeni Sertifika Üretimiyle İlgili Bilgilendirilmesi

Uygulama dışıdır.

4.7. Anahtar Yenileme

4.7.1. Anahtar Yenilemeyi Gerektiren Durumlar

NES için geçerlilik süresinin ilk 3 (üç) ayı içinde sertifika sahibinin kartından sertifikanın silinmiş olması, kartın kaybolması veya kartın bir biçimde çalışamaz olması durumunda, yeniden belge istenmeksizin anahtar yenilemeyle yeni bir sertifika üretilir. Sertifika sahibinin ilk başvuruda sağlamış olduğu hiçbir bilginin değişmemiş olması ön koşuldur. Gerekli görülen hallerde bilgilerin değişmemiş olduğu kontrol edilir.

4.7.2. Anahtar Yenileme Talebinde Bulunabilecek Kişiler

NES için sertifika sahibi gerçek kişidir.

4.7.3. Anahtar Yenileme Talebinin İşlenmesi

NES'te herhangi bir bilgide değişiklik olduğuna dair bir belirti veya şüphe olması durumunda, ilgili bilgi ve destekleyici belgeler yeniden alınır.

4.7.4. Yeni Sertifikayla İlgili Sertifika Sahibine Bildirim Yapılması

Bölüm 4.3.2'de yer alan esaslar uygulanır.

4.7.5. Anahtarı Yenilenen Sertifikanın Kabulü

Bölüm 4.4.1'de yer alan esaslar uygulanır.

4.7.6. ESHS Tarafından Anahtarı Yenilenen Sertifikanın Yayımlanması

Bölüm 4.4.2'de yer alan esaslar uygulanır.

4.7.7. Diğer Katılımcıların Yeni Sertifika Üretimiyle İlgili Bilgilendirilmesi

Uygulama dışıdır.

4.8. Sertifika Değişikliği

4.8.1. Sertifika Değişikliğini Gerektiren Durumlar

TÜRKTRUST tarafından üretilmiş olan sertifikaların içeriğindeki bilgilerde bir değişiklik olması durumunda, sertifika iptal edilir ve yeni bilgilerle birlikte yeni bir sertifika başvurusunda bulunulur.

Yeni sertifika başvurusu Bölüm 4.1'de belirtilen esaslar uyarınca yürütülür.

4.8.2. Sertifika Değişiklik Talebinde Bulunabilecek Kişiler

Bölüm 4.1.1'de yer alan esaslar uygulanır.

4.8.3. Sertifika Değişiklik Talebinin İşlenmesi

Bölüm 3.2'de yer alan esaslar uygulanır.

4.8.4. Yeni Sertifikayla İlgili Sertifika Sahibine Bildirim Yapılması

Bölüm 4.3.2'de yer alan esaslar uygulanır.

4.8.5. Değişiklik Yapılmış Sertifikanın Kabul Şekli

Bölüm 4.4.1'de yer alan esaslar uygulanır.

4.8.6. ESHS Tarafından Değişiklik Yapılmış Sertifikanın Yayımlanması

Bölüm 4.4.2'de yer alan esaslar uygulanır.

4.8.7. Diğer Katılımcılarının Yeni Sertifika Üretimiyle İlgili Bilgilendirilmesi

Uygulama dışıdır.

4.9. Sertifika İptali ve Askıya Alma

4.9.1. Sertifika İptalini Gerektiren Durumlar

4.9.1.1. Son Kullanıcı Sertifikaları

Sertifikanın kullanım süresi içinde geçerliliğini kaybetmesi durumunda sertifika iptal edilir. NES için iptal işlemi talebin ulaşmasının ardından derhal gerçekleştirilir. Aşağıda yer alan koşullar sertifikanın iptalini gerektirir:

- Sertifika sahibinin veya temsile yetkili kişinin talebi,
- Sertifika başvurusunda veya sertifikada yer alan bilgilerin sahteliğinin veya yanlışlığının ortaya çıkması; TÜRKTRUST bu şartın oluştuğuna dair makul kanıta dayalı kanaat oluşturabileceği gibi aynı şart sertifika sahibi veya temsili yetkili kişinin bildirimiyle de oluşabilir,
- eksprEs-İmza üretimi sonrası ilgili sertifika kayıt merkezi ofis veya şube aracılığıyla teslim edilecek olan e-imza paketinin 1 (bir) ay içinde sertifika başvuru sahibi tarafından teslim alınmaması veya standart NES üretimi sonrası kurye ile gönderilen e-imza paketinin 1 (bir) ay boyunca sertifika başvuru sahibi tarafından teslim alınmaması,
- Sertifika içeriğinde yer alan özne veya sertifika sahibi bilgilerinde bir değişiklik olması,
- Sertifika sahibinin fiil ehliyetinin sınırlandığının, iflâsının veya gaipliğinin veya ölümünün öğrenilmesi,
- Sertifikanın amacı dışında kullanıldığına dair bir kanıtın elde edilmesi,
- 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,

- TÜRKTRUST'ın, sertifikanın Sİ ve SUE rehber kitapçıkları ile TÜRKTRUST sertifika sahibi taahhütnamesi hükümlerine aykırı olarak kullanıldığına ilişkin bir bildirim alması veya böyle olduğunun anlaşılması,
- Mobil imza kullanım amaçlı NES sahiplerinin, kullanmakta oldukları GSM hatlarına dair aboneliğin son bulması,
- TÜRKTRUST'ın tamamen kendi takdiri sonucu, sertifikanın verilişi sırasında işbu SUE rehber kitapçıklarının uygulama esaslarına ilişkin bir uygunsuzluk tespit etmesi,
- TÜRKTRUST'ın Kanun'a dayalı sertifika verme hakkının ortadan kalkması,
- TÜRKTRUST kök veya alt kök sertifikalarına ait gizli anahtarların açığa çıkma şüphesinin oluşması veya açığa çıkması,
- TÜRKTRUST'ın sertifika hizmetleri vermeyi durdurması ve başka bir ESHS ile anlaşmaması.

4.9.1.2. TÜRKTRUST Alt Kök Sertifikaları

Alt kök sertifikanın kullanım süresi içinde geçerliliğini kaybetmesi durumunda en geç 7 (yedi) gün içinde iptal edilir. Aşağıda yer alan koşullar alt kök sertifikasının iptalini gerektirir:

- Üretimde kullanılan alt kök sertifikasına ait gizli anahtarların açığa çıkma şüphesinin oluşması veya açığa çıkması,
- Alt kök sertifikasının amacı dışında kullanıldığının ortaya çıkması,
- Alt kök sertifikanın TÜRKTRUST Sİ ve SUE rehber kitapçıkları gerekliliklerine uygun olarak üretilmediğinin ortaya çıkması,
- Alt kök sertifikanın içinde yer alan bilgilerin hatalı veya yanıltıcı olduğunun ortaya çıkması,
- TÜRKTRUST'ın herhangi bir nedenle faaliyetlerine son vermesi ve iptal desteğini sağlamak amacıyla herhangi başka bir ESHS ile anlaşmaması,
- TÜRKTRUST'ın sertifika verme yetkisinin süresinin dolması, sona ermesi veya iptal edilmesi (SİL ve OCSP hizmetleri için gerekli düzenlemeler sağlanmışsa),
- TÜRKTRUST Sİ ve SUE rehber kitapçıkları uyarınca sertifika iptali gerekiyorsa.

4.9.1.3. Alt ESHS Sertifikaları

Alt ESHS sertifikasının kullanım süresi içinde geçerliliğini kaybetmesi durumunda en geç 7 (yedi) gün içinde iptal edilir. Aşağıda yer alan koşullar alt kök sertifikasının iptalini gerektirir:

- Alt kök sertifika kullanıcısı olan ESHS'nin yazılı iptal talebi,
- Alt kök sertifika kullanıcısı olan ESHS'nin, sertifika talebinin geçersiz olduğu bilgisini TÜRKTRUST'a bildirmesi,
- Alt kök sertifika kullanıcısı olan ESHS'nin sertifika üretimde kullandığı gizli anahtarların açığa çıkma şüphesinin oluşması veya açığa çıkması,
- Alt kök sertifikasının amacı dışında kullanıldığının ortaya çıkması,
- Alt kök sertifikanın TÜRKTRUST Sİ ve SUE rehber kitapçıkları gerekliliklerine uygun olarak üretilmediğinin ortaya çıkması,

- Alt kök sertifikanın içinde yer alan bilgilerin belirsiz veya yanıltıcı olduğunun ortaya çıkması,
- Alt kök sertifika kullanıcısı olan ESHS'nin veya TÜRKTRUST'ın herhangi bir nedenle faaliyetlerine son vermesi ve başka bir ESHS ile anlaşmaması,
- Alt kök sertifika kullanıcısı olan ESHS'nin veya TÜRKTRUST'ın sertifika verme yetkisinin sona ermesi veya iptal edilmesi (SİL ve OCSP hizmetleri için gerekli düzenlemeler sağlanmışsa),
- TÜRKTRUST Sİ ve SUE rehber kitapçıkları uyarınca sertifika iptali gerekiyorsa.

4.9.2. Sertifika İptal Talebinde Bulunabilecek Kişiler

Aşağıda belirtilen kişiler sertifika iptal talebinde bulunabilir:

- Sertifika sahibi ile sertifikada kurum bilgisinin yer alması halinde ilgili kurumu temsile yetkili kişi,
- Güvenli elektronik imza oluşturma aracının sahibi,
- Mobil imza kullanım amaçlı NES için mobil operatör,
- TBB alt kök sertifikası altında kalan sertifikalar için TBB yetkilileri,
- TÜRKTRUST yetkilileri.

4.9.3. Sertifika İptal Talebi Prosedürleri

NES iptal talepleri, sertifika sahibinden

- 7 gün 24 saat ilkesine göre TÜRKTRUST web sitesi üzerinden,
- 7 gün 24 saat ilkesine göre, tüm müşterilere duyurulan ve açıkça ilan edilen telefon numarası üzerinden sesli çağrı sistemi aracılığıyla,
- Mesai saatleri içinde yazıyla (faks ya da posta aracılığıyla gelen imzalı yazılar)

olmak üzere farklı yollarla alınabilir.

Sertifika sahibi, web üzerinden iptal başvurusunu tercih ederse, TÜRKTRUST web sitesine interaktif parolasıyla bağlanarak iptal edilecek sertifikayı seçer. İkincil kimlik doğrulama aşamasını da geçtikten sonra sertifika iptal nedeni girilerek online iptal işlemi 7 gün 24 saat ilkesine göre tamamlanır.

NES sahibi, telefonla iptal başvurusunu tercih ederse, ilan edilen telefon numarası üzerinden sesli çağrı sistemine ulaşır. Sistem üzerinde T.C. Kimlik Numarası ve istenilen diğer bilgileri girerek doğrulama adımlarını tamamlar. Seri numarasını bildirdiği sertifikasının askı veya iptal işlemini 7 gün 24 saat ilkesine göre tamamlar.

Ayrıca, NES sahibi, tercih etmesi durumunda sertifika iptal talebini elle atılan imzayla hazırlayacağı bir sertifika iptal talep yazısıyla da TÜRKTRUST'a bildirebilir. Yazının aslı TÜRKTRUST yetkililerine ulaştığında yazıdaki imza doğrulanarak sertifika iptal edilir. İptal talep yazısı faksla alınmışsa, yazı aslı gelene kadar sertifika askıya alınır.

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

Mobil imza kullanım amaçlı NES iptali için, sertifika sahibi mobil operatör çağrı merkezine ulaşarak iptal talebini bildirir. Kullanıcının kimliği ilgili kontrol adımlarıyla doğrulandıktan sonra, mobil operatör çağrı merkezi yetkilisi iptal talebini sisteme girer. Mobil imza hizmet altyapısı aracılığıyla iptal talebi TÜRKTRUST tarafından alınır ve iptal işlemi

sonuçlandırılır. İşlem sonrası iptal durumu yine mobil imza hizmet altyapısı aracılığıyla sertifika sahibine bildirilir.

İçeriğinde kurum bilgisi de yer alan NES iptal talepleri, sertifika sahiplerinin yanı sıra onaylı iptal başvuruları ile ilgili kurumu temsile yetkili kişilerden de alınabilir. Yetkililerinden gelen yazılı sertifika iptal talebi doğrulandıktan sonra iptal işlemi tamamlanır. İşlem sonrası iptal durumu yetkili ile sertifika sahibine e-posta ile bildirilir.

Mobil imza kullanım amaçlı NES'lerin mobil operatör tarafından iptal edilmesinin gerektiği durumlarda, iptal talebi mobil imza hizmet altyapısı aracılığıyla TÜRKTRUST'a iletilir.

TÜRKTRUST'a ait bir güvenlik sorunu oluşması, mevcut sertifikalarla ilgili ihbar alınması ya da TÜRKTRUST'ın iç işleyişinde oluşan bir hatanın fark edilmesi durumlarından birinin gerçekleşmesi halinde, TÜRKTRUST sertifika iptalini başlatabilir. TÜRKTRUST kaynaklı tüm sertifika iptal işlemlerinde, sonuç ilgili sertifika kullanıcılarına e-posta yoluyla duyurulur. Gereken durumlarda, yeni sertifika üretim işlemleri ücretsiz olarak, iptal işleminden sonra hemen başlatılır.

İptal edilmiş bir sertifikanın yeniden kullanılabilir hale gelmesi için bir prosedür olmadığı gibi, iptal edilmiş bir sertifikanın yeniden kullanılabilir hale getirilmesi için sunulan bir araç da yoktur. İptal işlemi, veritabanında farklı güncellemelere yol açar; OCSP hizmetinde anlık güncelleme ve bir sonraki SİL'in güncellemesi. İptal edilmiş bir sertifika, geçerlilik süresinin sonuna kadar SİL'de yayımlanmaya devam eder.

TÜRKTRUST'a ait kök ve alt kök sertifikaların iptal edilmesi durumunda, mümkün olan en kısa sürede durum tüm ilgili taraflara elektronik ortamda ivedilikle duyurulur. İptal edilen kök veya alt kök sertifikanın imzasını taşıyan son kullanıcı sertifikaları da iptal edilir ve kullanıcılar e-postayla bilgilendirilir.

4.9.4. Sertifika İptal Talebi Gecikme Periyodu

Sertifika iptal talebi teknik ve ticari imkânların elverdiği en kısa süre içinde işleme alınır.

4.9.5. TÜRKTRUST'ın Sertifika İptal Talebini İşleme Süresi

TÜRKTRUST, kendisine web ve sesli çağrı sistemi üzerinden kesintisiz olarak ulaşan tüm sertifika iptal taleplerini, talebin uygun bulunması ve kimlik doğrulamanın çevrim içi olarak tamamlanmasının ardından anında sonuçlandırır. Yazıyla kâğıt ortamında alınan sertifika iptal talepleri ise mesai saatleri içinde derhal değerlendirmeye alınır ve gerekli işlemler ivedilikle tamamlanır.

Mobil imza kullanım amaçlı NES iptal talepleri, kurumsal başvuru sahibi olan mobil operatör tarafından gerekli doğrulamaların yapılmasının ardından mobil imza hizmet altyapısı aracılığıyla TÜRKTRUST'a iletilir ve anında sonuçlandırılır.

4.9.6. Üçüncü kişilerin İptal Kontrol Gerekliliği

Üçüncü kişiler, kendilerine gönderilen bir elektronik imzaya güvenmeden önce, ilgili sertifikayı doğrulamakla yükümlüdür. Sertifika durumunun doğrulanması için TÜRKTRUST tarafından yayımlanan güncel SİL ya da çevrim içi sertifika durum sorgulama servisi olan OCSP kullanılmalıdır. TÜRKTRUST üçüncü kişilere, Kanun'a göre oluşturulan güvenli elektronik imzalı doğrulamada güvenli elektronik imza doğrulama araçlarını kullanmalarını tavsiye eder.

4.9.7. Sertifika İptal Listesi (SİL) Yayımlama Sıklığı

TÜRKTRUST son kullanıcı sertifikaları için, sertifika durumlarında hiçbir değişiklik olmasa bile, günde en az bir kez yeni bir SİL yayımlar.

TÜRKTRUST 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. SİL'lerin En Geç Yayımlanma Zamanı

SİL'ler üretildikleri andan itibaren en geç 10 (on) dakika içinde yayımlanır.

4.9.9. Çevrim İçi Sertifika İptal/Durum Kontrol İmkânı (OCSP)

TÜRKTRUST, kesintisiz çevrim içi sertifika durum protokolü OCSP desteği verir. SİL'lere göre daha güvenilir ve gerçek zamanlı bir sertifika durum sorgusu olan OCSP hizmetiyle, müşteri tarafındaki uygun yazılımlar aracılığıyla çevrimiçi olarak sertifika durum sorgusu yapılabilir. Bu sorguyla, belirli bir zamanda bir sertifikanın durumu (geçerli, iptal, bilinmiyor) hakkında bilgi edinmek mümkündür.

TÜRKTRUST OCSP hizmeti kapsamında, sorgu yapan sistemlere verilen cevaplar, OCSP cevabı imzalama amacıyla üretilmiş olan OCSP hizmet sertifikaları kullanılarak imzalanır. Ayrıca durumu sorgulanan ve TÜRKTRUST tarafından üretilmiş herhangi bir sertifika için oluşturulan cevap, bu sertifikayı imzalamış olan kök veya alt kök sertifika tarafından imzalanmış bir OCSP hizmet sertifikası kullanılarak imzalanır.

4.9.10. Çevrim İçi Sertifika İptal/Durum Kontrol Gereklilikleri

Üçüncü kişilerin sertifika durum sorgusu yaparken, eğer teknik imkânları yeterliyse OCSP'yi tercih etmeleri, SİL'i ikinci alternatif olarak seçmeleri önerilir.

4.9.11. Diğer İptal Durumu Yayımlama Çeşitlerinin Varlığı

TÜRKTRUST, OCSP ve SİL dışında iptal durumu yayımlama yöntemi kullanmaz.

4.9.12. Anahtar Güvenliğinin Yitirilmesine İlişkin Özel Gereklilikler

TÜRKTRUST'a ait bir güvenlik sorunu oluşması durumunda, durumdan etkilenen son kullanıcı sertifikaları TÜRKTRUST tarafından iptal edilir. TÜRKTRUST'a ait kök veya alt kök sertifikaların iptal edilmesi gerekirse, bu sertifikaların imzasını taşıyan son kullanıcı sertifikaları da iptal edilir ve kullanıcılar e-postayla bilgilendirilir.

Güvenlik sorunu ve sonuçları, TÜRKTRUST tarafından ivedilikle kamuya açık bir şekilde web sitesi üzerinden ve gerekli durumlarda basın ve yayın organları aracılığıyla sertifika sahiplerine ve üçüncü kişilere duyurulur.

TÜRKTRUST'a ait bir güvenlik sorununun duyurulması durumunda, sertifika sahiplerinin sertifikalarını kullanmaya devam etmelerine izin verilmez.

TÜRKTRUST kaynaklı tüm sertifika iptal işlemlerinde, iptal sonrası yeni sertifika üretim işlemlerinin ivedilikle başlatılmasından TÜRKTRUST sorumludur.

4.9.13. Sertifika Askıya Alma Gerektiren Durumlar

TÜRKTRUST, NES iptal talebinin kaynağının doğrulanamadığı durumlarda doğrulama işlemi sonuçlanıncaya kadar veya son kullanıcı tarafından iptali gerektiren bir durumun olup olmadığından emin olunamadığı zamanlarda gelen talep üzerine, iptal işlemi yapmak yerine ilgili sertifikaları askıya alır.

4.9.14. Sertifika Askıya Alma Talebinde Bulunabilecek Kişiler

Bölüm 4.9.2'de yer alan esaslar uygulanır.

4.9.15. Sertifika Askıya Alma Talebi Prosedürü

Aşağıdaki istisnai haller saklı kalmak kaydıyla Bölüm 4.9.3'de yer alan esaslar uygulanır.

TÜRKTRUST'a ait bir güvenlik sorunu oluşması ya da mevcut sertifikalarla ilgili ihbar alınması durumunda NES'ler için iptal gerekliliği kesinleşene kadar TÜRKTRUST ilgili sertifikaları askıya alabilir. TÜRKTRUST tarafından başlatılan askı süreci, kayıt merkezi ya da sertifika üretim merkezi kaynaklı olabilir. TÜRKTRUST kaynaklı tüm sertifika askıya alma işlemlerinde, sonuç ilgili sertifika kullanıcılarına e-posta yoluyla duyurulur.

TÜRKTRUST'a ait kök ve alt kök sertifikaları için askıya alma işlemi uygulanmaz.

4.9.16. Sertifikanın Askıda Kalma Süresinin Sınırları

TÜRKTRUST, NES iptal talep kaynağının doğrulanamadığı durumlarda askıya aldığı sertifikaları, 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.

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

4.10. Sertifika Durum Servisleri

TÜRKTRUST tarafından üretilmiş olan sertifikalar, sertifika sahibinin yazılı rızası olması kaydıyla, tüm sertifika sahiplerinin ve üçüncü kişilerin erişimine açık olarak web veya LDAP dizin sunucusu üzerinden yayımlanır.

Sertifika durum sorgulaması ise iki ayrı yöntemle yapılır: Sertifika İptal Listesi (SİL-CRL) ve Çevrimiçi Sertifika Durum Protokolü (OCSP).

4.10.1. İşlevsel Özellikler

TÜRKTRUST 12 (oniki) saatte bir olmak üzere günde 2 (iki) kez ve 24 (yirmidört) saatlik geçerlilik süresiyle, sertifika durumlarında hiçbir değişiklik olmasa bile yeni bir SİL yayımlar.

SİL geçerlilik süresi konusunda tek istisna kök ve alt kök sertifikaların geçerlilik sürelerinin dolması sırasında yaşanır. SİL içinde bulunan bir sonraki güncelleme tarihinin, kök veya alt kök sertifika geçerlilik bitiş tarihini aşması halinde SİL içinde bulunan bu değer kök veya alt kök geçerlilik bitiş tarihi olarak yazılır.

TÜRKTRUST, çevrim içi sertifika durum protokolü OCSP desteği verir. Bu sorguyla, gerçek zamanlı sertifika durum (geçerli, iptal, bilinmiyor) bilgisi alınabilir.

4.10.2. Hizmetin Sürekliliği

TÜRKTRUST, Madde 4.10.1'de belirtilen koşullarda SİL ve OCSP hizmetini, kesintisiz olarak 7 gün 24 saat ilkesine göre verir. OCSP hizmetinin kesintiye uğramasını engellemek için TÜRKTRUST yedek sistemler kullanır.

TÜRKTRUST merkezinde sunulan sertifika hizmetleri, erişilebilirlik ve yeniden devreye alma amaçları uyarınca her zaman yeterli düzeyde bir altyapı ile idame ettirilir. Hizmetlerde kesintiye yol açan ve TÜRKTRUST'ın kontrolünün ötesinde bir durum ortaya çıktığında,

TÜRKTRUST İş Sürekliliği Prosedüründe tanımlanan Kriz Yönetim Ekibinin kararıyla TÜRKTRUST FKM, en geç 2 saat içinde devreye alınır.

4.10.3. İsteğe Bağlı Özellikler

Uygulama dışıdır.

4.11. Sertifika Sahipliğinin Sona Ermesi

Sertifika sahipliğinin sona ermesi, sertifikanın süresinin dolması ya da iptal edilmesiyle gerçekleşir.

4.12. İmza Oluşturma Verisi Saklama ve Yeniden Oluşturma

TÜRKTRUST, imza oluşturma verisinin kendisi tarafından oluşturulması halinde, bu veriyi hiçbir biçimde saklamaz veya yeniden oluşturmaz; yeniden oluşturulabileceği bilgileri elinde tutmaz.

4.12.1. Anahtar Saklama ve Yeniden Oluşturma İlke ve Esasları

Uygulama dışıdır.

4.12.2. Oturum Anahtarı Zarflama ve Yeniden Oluşturma İlke ve Esasları

Uygulama dışıdır.

5. TESİS, YÖNETİM VE İŞLETMEYLE İLGİLİ KONTROLLER

SUE dokümanının bu kısmında, TÜRKTRUST'ın sertifika hizmetlerini yürütürken tesis ve işletme güvenliğini sağlamaya yönelik olarak uyguladığı, teknik olmayan çeşitli güvenlik kontrolleri yer almaktadır.

5.1. Fiziksel Kontroller

5.1.1. Tesis Yeri ve İnşaatı

TÜRKTRUST merkezi, dış tehditlere karşı korunaklı ve güvenli bir alanda kurulmuş, tesis içinde yüksek güvenlikli bölgeler ve çeşitli güvenlik alanları oluşturulmuştur.

5.1.2. Fiziksel Erişim

TÜRKTRUST merkezindeki alanlara fiziksel erişim sürekli kontrol altında tutulmaktadır.

Tesisin çevresi, dışarıdan kontrolsüz giriş çıkışın engellenmesi için korunaklı bir şekilde çevrilmiştir. Merkezin dışarıyla bağlantılı tüm giriş çıkış noktalarında güvenlik görevlileri bulunur. Güvenli alanlara fiziksel erişim kartlı geçiş kontrol sistemleri aracılığıyla yapılır. Yetkisiz kişilerin belirli bölgelere girişi yasaklanmıştır. Temel sertifika üretim işlemlerinin gerçekleştirildiği yüksek güvenlikli bölgeler daima yetkisiz girişe kapalı tutulur. Giriş çıkışlar kayıt altına alınır. Ek güvenlik önlemi olarak kritik bölge ve geçişler sürekli kameralarla izlenir ve kamera çekim kayıtları güvenlik gereklilikleri nedeniyle saklanır.

Türkiye Barolar Birliği'nde bulunan NES üretim merkezinin fiziksel erişimi de sürekli kontrol altında tutulmaktadır. Tesisin çevresi korunaklı bir şekilde çevrilmiş ve giriş çıkış 7 gün 24 saat ilkesine göre güvenlik görevlileriyle korunmaktadır. NES üretim merkezinde bulunan kartlı geçiş sistemiyle yetkisiz erişim engellenmektedir.

5.1.3. Güç Kaynakları ve Havalandırma

TÜRKTRUST merkezinde kullanılan tüm donanım ve teçhizat için kesintisiz çalışacak güç kaynakları oluşturulmuştur. Sistemler güç kesintilerine karşı, anında devreye girecek kesintisiz güç kaynakları ve jeneratörlerle desteklenir. Yedek güç ünitelerinin düzenli olarak bakımı yapılır ve ihtiyaca göre kapasiteleri geliştirilir.

Özellikle bilgisayar donanımlarının yoğun bulunduğu bölgelerde, bu bölgelerin dışında kalan alanlarda ise ihtiyaca göre yeterli havalandırma kesintisiz olarak sağlanır. Bina içinde belirli noktalarda optimum iklim koşullarının sağlanması için uygun ısıtma ve soğutma sistemleri kullanılarak sıcaklık ve nem kontrol altında tutulur.

5.1.4. Su Baskınları

TÜRKTRUST merkezi, inşaat önlemleriyle doğal afetlere dayalı sel ve su baskınlarına karşı korunmuştur. Binanın dış cephe ve zemin kaplamaları su geçirmez niteliktedir. Taban suyunun binaya sızmasını önlemek için gerekli yalıtım oluşturulmuştur.

Binanın su ve kanalizasyon tesisatında oluşabilecek arızalara bağlı iç su baskınlarının önlenmesi için, tesisat uygun biçimde yapılmış, su kanallarının binada kontrollü biçimde ana tesisat yollarından geçirilmesiyle, su akışı kontrol altına alınmıştır. Kritik donanım ve teçhizatın bulunduğu bölüm ve alanlarda su ve kanalizasyon yolunun bulunmaması sağlanmıştır.

Alınan bütün inşaat önlemlerine rağmen oluşabilecek olası su baskınlarını mevcut sisteme zarar vermeden bertaraf edebilmek için, yeterli düzeyde uyarı ve su tahliye sistemleri kurulmuştur.

5.1.5. Yangın Önleme ve Yangından Korunma

TÜRKTRUST binasında yıldırım etkisine bağlı yangın çıkmaması için uygun nitelikte paratoner sistemi kurulmuştur. Elektrik kontaklarına bağlı yangınları önlemek için elektrik altyapısı kaliteli ve uygun malzeme ile hazırlanmış, güç sistemlerinde yeterli oranlarda elektrik sigortaları kullanılmıştır. Binanın sınırlı ve belirli, mutfak ve benzeri bazı bölgeleri dışında açık ateş kullanılmamakta, binadasigara içme yasağı uygulanmaktadır.

Olası yangın durumlarını büyümeden fark edip önleyebilmek için tesisin uygun noktalarına duman ve ısı algılayıcıları yerleştirilmiştir. Bir alarm anında otomatik olarak devreye giren yerleşik yangın söndürme sistemi mevcuttur. Yerleşik sistemde, binanın bölgelerine göre farklı fiziksel ve kimyasal nitelikteki yangın söndürme malzemeleri kullanılmaktadır. Bunun dışında, yine uygun kimyasal ve fiziksel niteliklere sahip yangın söndürme üniteleri binanın gerekli yerlerine konuşlandırılmış olup, personel kritik malzeme ve bölgeler için yangına müdahale etme konusunda eğitilerek bilgilendirilmiştir.

5.1.6. Saklama Ortamları

TÜRKTRUST faaliyetleri sırasında oluşturulan tüm kayıtların yedekleri uygun saklama ortamlarında tutulur. Bu yedekler, bina içinde su ve yangın korumalı bir alanda, fiziksel ve elektromanyetik güvenlik önlemleri alınmış, erişim güvenliği sağlanmış ve sadece prosedürel kontroller uygulanarak erişilebilecek şekilde saklanır.

5.1.7. Atıkların Atılması

Temel sertifika hizmetlerine bağlı, elektronik veya kâğıt ortamda saklanan tüm bilgi ve belgeler, saklanmaları gerekmiyorsa ilgili prosedürler uyarınca tamamen imha edilerek atılır. Kriptografik modüller atılmaları gerektiğinde üretici firmaya ait teknik dokümanlar doğrultusunda sıfırlanır ve fiziksel olarak imha edilir.

Binanın ve TÜRKTRUST birimlerinin diğer tüm atıkları uygun biçimde tesis dışına çıkarılır.

5.1.8. Tesis Dışı Yedekleme

TÜRKTRUST, sertifika hizmetleri iş sürekliliğini sağlayabilmek amacıyla, mevcut tesis ve binada oluşabilecek herhangi bir afet durumunda sistemlerini yeniden işletilebilir duruma getirebilmek için elektronik işlem kayıtlarının yedeklerini FKM'de ve tesis dışında güvenli kasalarda saklar.

5.2. Prosedürel Kontroller

5.2.1. Güvenilir Roller

TÜRKTRUST elektronik sertifika hizmetlerinde görev alan personelin organizasyonunun sağlanması amacıyla, tüm sertifika iş süreçlerinin yürütülmesinde görev alacak güvenilir roller belirlenmiştir.

- **Üst Düzey Yöneticiler:** TÜRKTRUST sertifika hizmetlerinin yürütülmesinden teknik ve idari açıdan sorumlu üst düzey yöneticilerdir.
- **Müşteri Hizmetleri Sorumluları:** Müşteri hizmetleri, evrak kontrolü, sertifika başvuru kaydı, üretim, nitelikli elektronik sertifikaları askıya alma ve iptal gibi rutin sertifika hizmetlerinden sorumlu çalışanlardır.
- **Güvenlik Yetkilileri:** Güvenlik politikaları ve uygulamalarının yönetimi ve yürütülmesinden sorumlu çalışanlardır.

- **Sistem Yöneticileri:** Sertifika hizmetlerine ilişkin sistemlerin kurulumu, konfigürasyonu ve devamlılığının sağlanması ve aynı zamanda sistem yedekleme ve geri yükleme işlemleri için yetkilendirilmiş çalışanlardır.
- **Sistem Denetçileri:** Sertifika hizmetlerine ilişkin arşivlerin ve denetim kayıtlarının izlenmesi için yetkilendirilmiş çalışanlardır.
- **Güvenlik Görevlileri:** Tüm TÜRKTRUST tesislerinin fiziksel güvenliğini sağlamaktan sorumlu çalışanlardır.

5.2.2. Her Görev İçin Gereken En Az Kişi Sayısı

TÜRKTRUST'ta sertifika süreçleri dâhilindeki kritik işlemlerin yapılabilmesi için çok kişi kontrollü bir sistem kurulmuştur. TÜRKTRUST kök ve alt kök sertifikalarıyla ilgili her türlü üretim, yenileme, iptal, imha ve yedekleme işlemi, TÜRKTRUST kök, alt kök ve son kullanıcı sertifikalarının anahtar çiftlerinin üretimi en az iki yetkilinin hazır bulunması ve onaylı görev talimatının ilgili yetkililere verilmiş olmasıyla yapılabilmektedir.

5.2.3. Her Görev için Kimlik Doğrulama

TÜRKTRUST içinde güvenilir rollere atanan çalışanlar, öncelikle atanmış yetkileriyle birlikte güvenlik sistemine tanıtılır. Böylelikle her kritik işlem öncesi bu rollerdeki kişilerin kimlik doğrulaması yapılır. Doğrulama tamamlandıktan sonra işleme izin verilir ve işlem tamamlandıktan sonra kaydedilir.

5.2.4. Görevlerin Ayrılmasını Gerektiren Roller

Sertifika süreçleri işletilirken, aynı sertifikayla yapılan ardışık işlemlerin tümü farklı işlem noktalarında farklı kişiler tarafından yapılır. Görevlerin dağıtımı farklı rollere atanarak süreç içinde aynı kişinin işin bütününü ya da büyük bir kısmını yapması engellenmiştir. Yapılan her işlem, rol bazlı olarak ayrıntılı yer ve zaman bilgisi içerecek şekilde kayıt altına alınmaktadır.

Özellikle, "Güvenlik Yetkilisi" veya "Müşteri Hizmetleri Sorumlusu" olarak yetkilendirilmiş bir kişi, "Sistem Denetçisi" olarak yetkilendirilemez. "Sistem Yöneticisi" olarak yetkilendirilmiş bir kişiyse, "Güvenlik Yetkilisi" veya "Sistem Denetçisi" olarak yetkilendirilemez.

5.3. Personel Kontrolleri

5.3.1. Nitelik, Deneyim ve Güvenlik Gereklilikleri

TÜRKTRUST'ta çalışan personel, sertifika süreçlerinin işleyişini doğru ve güvenilir bir şekilde yürütebilecek nitelikte, göreve uygun eğitim düzeyine sahip (lise, üniversite, yüksek lisans vb.), konusunda bilgili ve eğitimli, benzer çalışma alanlarında deneyimlidir ve tüm güvenlik kontrollerinden geçmiştir.

5.3.2. Kişisel Geçmiş Kontrol Gereklilikleri

TÜRKTRUST'ta çalışan personelin özgeçmişi ve referansları ayrıntılı bir şekilde değerlendirilmekte, işe teknik ve idari açıdan uygunluğundan emin olunmaktadır. Uygun nitelikte olduğu belirlenen kişiler için adli sicil belgesi istenir ve gerekiyorsa güvenlik soruşturması yapılır.

5.3.3. Eğitim Gereklilikleri

TÜRKTRUST personeli göreve başlamadan önce sorumlulukları kapsamında eğitimden geçirilir. Eğitim süresince, çalışanlar temel sertifika iş süreçleri; müşteri hizmetleri, kayıt merkezleri ve sertifika üretim merkezi işleyişiyle ilgili prosedürler ve talimatlar; bilgi güvenliği

ilkeleri ve mevcut bilgi güvenliği yönetim sistemi; kullanılacak yazılım ve donanım birimleri hakkında ayrıntılı olarak bilgilendirilir.

Kayıt merkezlerindeki çalışanlar da görevlerinin gerektirdiği ölçüde eğitime tabi tutulurlar.

5.3.4. Tekrar Eğitimi Sıklığı ve Gereklilikleri

Çalışanlara yönelik eğitim, göreve başlanırken verilen ilk eğitimin ardından periyodik olarak ve diğer gerekli görülen durumlarda tekrarlanır. Sürekli olarak yürütülen ölçme ve değerlendirme çalışmalarının sonuçları ışığında ilgili personelin eğitim ihtiyacı belirlenir ve periyodik eğitimlerin yanı sıra verimin artırılmasına yönelik ek eğitim seansları da düzenlenebilir. Verilen eğitimlerin konuları ve kapsamı, gelişen teknoloji ve yenilenen yazılım ve donanım birimlerine uygun olarak sürekli güncellenir ve yenilenir.

5.3.5. İş Rotasyonu Sıklığı ve Sırası

TÜRKTRUST'a bağlı güvenlik görevlileri ve operatörler kendi çalışma alanları içindeki alt görevler üzerinde rotasyona tabi tutulurlar. Kalıcı bir görevlendirme değişikliği olmadığı sürece, farklı çalışma alanları arasında rutin rotasyon yapılmaz.

5.3.6. Yetkisiz İşlemler için Yaptırımlar

TÜRKTRUST personelinin teşebbüs edeceği yetkisiz işlemler için, TÜRKTRUST insan kaynakları yönergesi uyarınca gerekli disiplin cezaları uygulanır. Eğer bu yetkisiz işlem sonucunda TÜRKTRUST ya da TÜRKTRUST müşterileri zarar görürse, bu zararın ilgili çalışandan tazmini yoluna gidilir.

TÜRKTRUST yetkisiz işlem yapanlar hakkında, Kanun, Yönetmelik ve Tebliğ gereğince işlem yapılmasını temin etmek üzere, adli mercilere başvuruda bulunur.

5.3.7. Bağımsız Alt Yüklenici Gereklilikleri

Sertifika süreçleri dâhilinde alt yükleniciler aracılığıyla yürütülen işlemler için, TÜRKTRUST ile alt yüklenici firma arasında bir hizmet sözleşmesi imzalanır. Bu hizmet sözleşmesi TÜRKTRUST'ın gerektirdiği güvenlik koşullarını ve hizmet esaslarını ortaya koyar.

5.3.8. Personele Sağlanan Dokümantasyon

TÜRKTRUST personeline, Sİ ve SUE dokümanları, sertifika süreçleriyle ilgili kurumsal prosedürler ve güvenlik prosedürleri ile talimatları, çalışanların rollerine göre düzenlenmiş görev tanımları, kullanılan yazılım ve donanıma ait kullanım kılavuzları sağlanır.

5.4. Denetim Kayıtları Alma Prosedürleri

5.4.1. Kaydedilen Olay Tipleri

Sertifika yaşam döngüsü içinde yürütülen tüm sertifika hizmetlerine ait kayıtlar TÜRKTRUST tarafından tutulur. Bu kayıtların arasında sertifika başvuru kayıtları; üretilen, yenilenen, askıya alınan ve iptal edilen sertifikalarla ilgili her türlü müşteri talebinin kayıtları; üretilip yayımlanan sertifikalar ile SİL'ler hakkındaki kayıtlar; TÜRKTRUST birimlerindeki güvenilir rollere sahip çalışanların işlem kayıtları; çalışanların TÜRKTRUST birimlerine giriş ve çıkış kayıtları ile sistem modüllerine erişim kayıtları; doküman takibiyle ilgili kayıtlar; yazılım ve donanım kurulum, güncelleme ve onarım kayıtları sayılabilir.

İşlem kayıtları tutulurken işlemin tanımı, işlemi yapan kişi, işlemin tarih ve zaman bilgisi ve işlemin sonucu kaydedilir. Kayıtların tam zamanı, zaman damgası hizmetlerinde kullanılan zaman kaynağı ile senkronize edilmiş ilgili sunuculardan alınır.

5.4.2. Kayıtları İşleme Sıklığı

Denetim kayıtları sürekli olarak tutulur ve periyodik olarak bu kayıtların yedekleri alınarak arşivlenir.

5.4.3. Denetim Kayıtlarının Saklanma Süresi

TÜRKTRUST işleyişine ait denetim kayıtları, aktif kullanım süresince sistemde tutulur. Bu sürenin sonunda yasal düzenlemeler uyarınca saklanmak üzere arşivlenir.

5.4.4. Denetim Kayıtlarının Korunması

Denetim kayıtları fiziksel ve elektronik güvenlik önlemleriyle korunur, sadece yetkili kişilerin erişimine açık tutulur. Denetim kayıtlarının veri bütünlüğü anahtarlanmış özet yöntemiyle sağlanmaktadır.

5.4.5. Denetim Kayıtlarının Yedeklenme Prosedürleri

İlgili prosedürler uyarınca, kayıtların periyodik olarak yedekleri alınır.

5.4.6. Denetim Bilgisi Toplama Sistemi (İç ve Dış)

Denetim kayıtları, ESHS iş süreçlerinin yürütülmesinde kullanılan ESHS yönetim yazılımı tarafından tutulur.

5.4.7. Olayı Yaratan Kişiyi Bilgilendirme

Rutin işlemlerin dışında kalan denetim kayıtlarının oluştuğu durumlarda, olayı yaratan kişi sistem tarafından uyarılır. Olayın çeşidine ve önemine göre, sistem üzerinde olayı yaratan kişinin yönetiminden sorumlu üst yetki seviyesindeki kişi veya kişiler de bilgilendirilebilir.

5.4.8. Zarar Görebilirlik Değerlendirmesi

Denetim kayıtları sistem üzerinde raporlanır. Bu raporların analiz edilmesiyle sistemdeki güvenlik açıkları ve sertifika süreçlerindeki hata noktaları belirlenerek önlem alınmaktadır.

5.5. Kayıtların Arşivlenmesi

5.5.1. Arşivlenen Kayıt Tipleri

TÜRKTRUST işleyişi uyarınca, 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, müşterilerle yapılan tüm yazışmalar, üretilen tüm sertifikalar ve SİL'ler, Sİ ve SUE kitapçıklarının tüm sürümleri, uygulama prosedürlerinin, talimatların ve formların bütünü, TÜRKTRUST arşiv prosedürleri uyarınca arşivlenir. Arşivlerin büyük bir kısmı elektronik ortamda tutulurken, kağıt üzerindeki yazışmalar, formlar, belgeler, müşteri dosyaları, şirket belgeleri gibi kayıtlar da kağıt ortamında arşivlenir.

5.5.2. Arşivlerin Saklanma Süresi

NES'lerle ilgili TÜRKTRUST işleyişine ait 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.

Elektronik arşivlerin yetkili olmayan kişiler tarafından görülmesi, değiştirilmesi veya silinmesi önlenmiştir. Kağıt üzerindeki arşivler ise sadece yetkili kişilerin girme izni bulunan özel birimlerde tutulurlar.

5.5.4. Arşivlerin Yedeklenme Prosedürleri

İlgili prosedürler uyarınca, elektronik ortamdaki arşivlerin yedekleri tutulur. Kağıt ortamdaki arşivlerin ise yedekleri alınmaz.

5.5.5. Kayıtların Zaman Damgası Altına Alınması Gereklilikleri

TÜRKTRUST elektronik arşiv kayıtları zaman bilgisiyle birlikte saklanır.

5.5.6. Arşiv Toplama Sistemi

Arşiv kayıtları, TÜRKTRUST arşiv yönetim sistemi kullanılarak, ilgili prosedürler uyarınca derlenir.

5.5.7. Arşiv Bilgisinin Edinilmesi ve Doğrulanması Prosedürleri

TÜRKTRUST arşiv bilgilerine, Kurum talebi veya yasal süreçlerin bir gereği olarak kontrollü erişim sağlanır.

5.6. Anahtar Değişimi

TÜRKTRUST'a bağlı sertifika üretim merkezlerinin yeni kök ve alt kök sertifikalarının üretim işlemleri, TÜRKTRUST merkezi tarafından yönetilir.

Kök sertifikaların süresi sonuna yaklaşıldığında, üretilecek son kullanıcı sertifikalarının geçerlilik süresi, bağlı bulunduğu kök sertifikaların her hangi birinin son kullanma tarihini geçmeyecek biçimde verilir.

5.7. Güvenliğin Yitirilmesi ve Felaket Kurtarma

5.7.1. Güvenlik Kaybına Neden Olabilecek Olaylar

TÜRKTRUST işleyişini engelleyecek nitelikte olayların ya da güvenlik sorunlarının oluşması durumunda, TÜRKTRUST bilgi güvenliği ihlal olayı ve iş sürekliliği yönetimi prosedürleri ve iş sürekliliği planları uyarınca duruma müdahale edilir. TÜRKTRUST personeli tarafından fark edilerek raporlanan ihlal olayları ve güvenlik açıklarına müdahale ve sorun giderme yöntemleri bahsi geçen dokümanlarda açıkça ifade edilmiştir.

TÜRKTRUST sertifika sahiplerinin ve üçüncü kişilerin, sertifikalarının kullanımı sırasında karışılacakları güvenlik sorunlarını bildirebilmelerini temin etmek üzere TÜRKTRUST web sitesinde Sertifika Güvenlik Sorunu Bildirim Formu bulunmaktadır. Buraya yapılan güvenlik açığı bildirimleri TÜRKTRUST tarafından değerlendirilir ve gerekli görülen hallerde en kısa süre içinde geri dönüş yapılır.

5.7.2. Bilgisayar Kaynakları, Yazılım ve/veya Verilerin Bozulmuş Olması

Bilgisayar kaynaklarının zarar görmesi, yazılım birimlerinde veya işleyişe dair verilerde bozulma oluşması durumunda, 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 Verilerinin Güvenliğinin Yitirilmesi

TÜRKTRUST imza oluşturma verilerinin güvenliğinin ve güvenilirliğinin yitirilmesi durumunda, TÜRKTRUST iş sürekliliği planları uyarınca, ilgili sertifikalar iptal edilir ve Madde 5.6 uyarınca yeni imza oluşturma verisi oluşturularak devreye alınır. 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. İş Sürekliliği Yetenekleri ve Felaket Kurtarma

TÜRKTRUST, merkezi dışında felaket kurtarma merkezi (FKM) tesis etmiştir. Afet sonrasında iş sürekliliğini temin etmek üzere TÜRKTRUST merkezinde bulunan veriler yedeklenir. Özellikle, bir ihtiyacın ortaya çıkması durumunda FKM aracılığıyla OCSP veya SİL gibi gerçek zamanlı web hizmetleri en fazla 2 saatlik sürede hazır hale getirilebilir. Benzer şekilde, askıya alma, iptal ve benzeri diğer zorunlu sertifika hizmetleri, veri kaybına veya iş kesintisine yol açmadan 7 gün 24 saat esasına göre FKM'de hizmet vermek üzere çalıştırılabilir. Bu işleyişin devamlılığını sağlamak üzere, ilgili prosedürler uyarınca tatbikatlar düzenlenir. TÜRKTRUST işleyişini engelleyecek nitelikte olayların ya da güvenlik sorunlarının oluşması durumunda, TÜRKTRUST iş sürekliliği prosedürü ve planı uyarınca duruma müdahale edilir.

5.8. TÜRKTRUST'ın Faaliyetinin Son Bulması

TÜRKTRUST'ın faaliyetlerinin son bulması halinde, Kanun ve Yönetmelik gereği bu durumu en az 3 (üç) ay önce Kuruma bildirir ve kamuoyuna duyurur. TÜRKTRUST, işletmenin durdurulması prosedürü uyarınca, mevcut sertifikalarla ilgili tüm bilgi, belge ve kayıtları, Kanun gereği 1 (bir) ay içinde başka bir ESHS'ye devreder. Kurum, uygun görmesi halinde, 1 (bir) ayı geçmemek üzere ek süre verebilir. Eğer devir işlemi belirtilen süreler içinde tamamlanamazsa, TÜRKTRUST ilgili sertifikaları iptal eder ve tüm ilgili tarafları genel duyuru ve sertifika sahiplerine doğrudan e-posta aracılığıyla haberdar eder. Bu durumda, TÜRKTRUST son SİL kaydını oluşturduktan sonra kendi imza oluşturma verisi ile yedeklerini imha eder.

6. TEKNİK GÜVENLİK KONTROLLERİ

SUE dokümanının bu kısmında, TÜRKTRUST'ın sertifika hizmetleriyle ilgili iş süreçlerinde kullanılan gizli anahtarlarının ve erişim verilerinin yönetimi ile teknik altyapıya ve sertifika hizmetlerinin işleyişine yönelik güvenlik kontrolleri yer almaktadır.

6.1. Anahtar Çifti Üretimi ve Kurulumu

6.1.1. Anahtar Çifti Üretimi

TÜRKTRUST kök ve alt kök sertifikalarına ait anahtar çiftleri, sadece yetkili kişilerin kontrolünde, 2 (iki) yetkilinin hazır bulunmasıyla, Bölüm 5.1.2'de belirtildiği gibi teknik ve idari güvenlik önlemleri alınmış ortamlarda, TÜRKTRUST kök sertifika üretim, yayımlama ve imha prosedürü uyarınca üretilir ve uygun biçimde yedeklenir. İmza oluşturma verisi yetkisiz erişime karşı fiziksel ve teknik güvenlik önlemleriyle korunur. 2 (iki) 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.

TÜRKTRUST kök ve alt kök sertifikaları 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 yapılır. Aynı şekilde üretilen anahtar çiftinin ömrü güncel mevzuat, standartlar ve anahtarların kriptografik güvenlik süresiyle sınırlandırılmıştır. Bir kök veya alt kök sertifikasının geçerlilik süresi sonundan yeterince makul bir süre önce yeni bir anahtar çifti ve sertifika üretilerek hizmetin kesintisiz bir biçimde devam etmesi sağlanır.

TÜRKTRUST donanım güvenlik modülleri, fiziksel ve elektronik her türlü müdahaleye karşı koruma altında tutulur ve çalıştırılır. Modüllerde bulunan verinin güvenli yedekleri ilgili prosedürlere göre alınır ve saklanır. Böylece fiziksel ve ekonomik ömrünü tamamlamış bir modülün içindeki anahtarlar Bölüm 6.2.10'da belirtildiği gibi yok edilir ve yeni modüllerde kullanılmak üzere gerekli yedekler başka ortamlarda saklanır.

TBB NES alt kök sertifikaları anahtar çiftlerinin üretimi ise TÜRKTRUST merkezinde diğer alt kök üretimleriyle aynı prosedür uyarınca gerçekleştirilir. TBB alt kök üretiminde kullanılan donanım güvenlik modülü, TÜRKTRUST'ın diğer kök ve alt kök sertifika anahtarlarını tutan donanım güvenlik modülleriyle aynı güvenlik düzeyinde bulunur.

NES sahiplerinin imza oluşturma ve doğrulama verileri TÜRKTRUST tarafından üretilir. Bu üretim işlemi için TÜRKTRUST sertifika üretim merkezinde uygun güvenlik düzeyine sahip donanım güvenlik modüllerinde işlem gerçekleştirilir. Müşterilere ait imza oluşturma verileri hiçbir koşulda TÜRKTRUST'ta saklanmaz ve kopyası alınmaz.

6.1.2. İmza Oluşturma Verisinin Sertifika Sahibine Ulaştırılması

NES için anahtar çifti, en az 2 (iki) yetkilinin sisteme aynı anda şifreleri ve biyometrik verileriyle bağlanıp onay vermeleriyle TÜRKTRUST merkezinde üretilir. Bu üretim işlemi sırasında oluşturulan anahtar çifti için erişim şifreleri sistem tarafından rastgele belirlenir ve güvenli imza oluşturma aracına yazılır. Anahtar çiftinin yüklü bulunduğu güvenli elektronik imza oluşturma aracı sertifika kayıt merkezlerine gönderilir. İmza oluşturma verisi güvenli elektronik imza oluşturma aracının içinde kurye ile kimlik kontrolü ve imza karşılığında teslim edilmek üzere sertifika sahibine gönderilebileceği gibi TÜRKTRUST veya TBB Yetkilileri tarafından yine kimlik kontrollü ve imza karşılığında sertifika sahibine teslim edilir. Güvenli

elektronik imza oluşturma aracının erişim şifresi ise aktivasyon uygulamasıyla sertifika sahibi tarafından belirlenir.

Mobil imza kullanım amaçlı NES başvurularında, anahtar çifti hat kullanıcısının SIM kartında üretilir ve imza doğrulama verisi sertifika üretimi için mobil imza hizmet altyapısı üzerinden TÜRKTRUST'a ulaştırılır.

Mobil imza kullanım amaçlı NES'de imza oluşturma verisi hat kullanıcısının SIM kartında üretilir. Sadece mobil imza kullanımı için imza oluşturma verisine erişimi sağlayan mobil imza PIN kodu, SIM kart yazılımı aracılığıyla kullanıcı tarafından belirlenir.

6.1.3. İmza Doğrulama Verisinin ESHS'ye Ulaştırılması

Mobil imza kullanım amaçlı NES başvurularında, hat kullanıcısı tarafından SIM kartı üzerinde üretilen imza doğrulama verisi sertifika üretimi için mobil imza hizmet altyapısı üzerinden TÜRKTRUST'a ulaştırılır.

6.1.4. TÜRKTRUST İmza Doğrulama Verilerinin Üçüncü Kişilere Ulaştırılması

TÜRKTRUST kök ve alt kök sertifikaları üçüncü kişilerin erişebileceği şekilde http://www.turktrust.com.tr adresinden, kök sertifikalara ait parmak izi ise Türkiye'de yayınlanan en yüksek tirajlı 3 (üç) gazetede yayımlanır. Böylelikle, TÜRKTRUST'a ait imza doğrulama verileri üçüncü kişilerce kullanılabilir.

6.1.5. Anahtar Uzunlukları

TÜRKTRUST sertifikaları, Tebliğ'le belirlenen minimum anahtar uzunluklarına uygundur.

TÜRKTRUST sertifika üretim merkezlerinin kök ve alt kök sertifikaları üretilirken 2048 bit RSA anahtar çiftleri kullanılır.

TÜRKTRUST tarafından üretilen tüm son kullanıcı sertifikaları için 2048 bit RSA anahtar çifti kullanılır.

TÜRKTRUST tarafından üretilen nitelikli elektronik sertifikada kullanılan özetleme algoritması hakkında bilgi, Bölüm 7.1.3'te verilmiştir.

6.1.6. Anahtar Üretimi ve Kalite Kontrolü

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

6.1.7. Anahtar Kullanım Amaçları

TÜRKTRUST sertifika hizmetleri kapsamında üretilen son kullanıcı anahtarları, kimlik doğrulama ve elektronik imza amaçlı kullanılır.

TÜRKTRUST sertifika üretim merkezlerinin kök ve alt kök sertifikalarına ait anahtarlar, sertifika ve SİL imzalamak için kullanılır.

TÜRKTRUST OCSP hizmet sertifikalarına ait anahtarlar, OCSP sunucularına gelen sorgulara karşılık üretilen OCSP cevaplarını imzalamak için kullanılır.

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

6.2. İmza Oluşturma Verisinin Korunması ve Kriptografik Modül Mühendislik Kontrolleri

6.2.1. Kriptografik Modül Standartları ve Kontroller

TÜRKTRUST'ta anahtar çifti üretimi ile sertifika ve SİL imzalama işlemleri, Tebliğ'le belirlenen standartlarla uyumlu, güvenli kriptografik donanım modüllerinde gerçekleştirilir. Satın alma sonrası donanım güvenlik modülünün ilk kullanımından önce, sevkiyat ve depolama sırasında cihazların zarar görmediğinden emin olmak için kontroller uygulanır. Cihazların kabulü sırasında fabrika paketlemesi ve güvenlik mühürleri kontrol edilir ve cihazlar fiziksel ve teknik bakımdan güvenliği sağlanmış alanlarda saklanır ve kullanılır. 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.

TÜRKTRUST tarafından üretilen NES anahtar çifti, 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 Verisinin Çok Kullanıcılı Kontrolü

TÜRKTRUST'a bağlı sertifika üretim merkezlerinin kök ve alt kök imza oluşturma verilerine erişim, yetkili kişiler dışında yasaklanmıştır. Fiziksel ve teknik erişim kontrollerinin yanı sıra, bu imza oluşturma verilerinin kullanımı, ilgili modüle aynı anda iki ayrı yetkilinin bağlanması ve sistem tarafından onaylanmasıyla mümkündür. Sistem, hiçbir yetkilinin tek başına TÜRKTRUST imza oluşturma verilerini kullanabilmesine izin vermez.

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 Saklanması

TÜRKTRUST kök ve alt kök imza oluşturma verilerinin saklanması fiziksel ve teknik erişim kontrolleriyle sağlanmaktadır. Ayrıca bu imza oluşturma verilerinin kullanımı, ilgili modüle aynı anda iki ayrı yetkilinin bağlanması ve sistem tarafından onaylanmasıyla mümkündür.

TÜRKTRUST tarafından üretilen son kullanıcı sertifikalarına bağlı imza oluşturma verileri TÜRKTRUST tarafından kesinlikle saklanmaz, bu verilerin bir kopyası alınmaz.

6.2.4. İmza Oluşturma Verisinin Yedeklenmesi

TÜRKTRUST tarafından üretilen son kullanıcı sertifikalarına bağlı imza oluşturma verileri yedeklenmez, bu verilerin kopyası alınmaz.

Herhangi bir afet durumu veya sorun anında hizmetlerin kesintiye uğramaması amacıyla, TÜRKTRUST sertifika üretim merkezlerinin kök ve alt kök sertifikalarına bağlı imza oluşturma verileri, TÜRKTRUST kök sertifikaları anahtar üretim, yayımlama ve imha prosedürü uyarınca yedeklenir ve fiziksel ve teknik güvenlik kontrolleri altında saklanır.

TÜRKTRUST kök ve alt kök sertifikalarına bağlı gizli anahtarlar, EAL4+ veya FIPS 140-2 Düzey 3 sertifikalı güvenli donanımlarda (token) yedeklenir. Bu donanımlar, tesis dışındaki güvenli kasalarda saklanır. Herhangi bir nedenle yeniden kullanım ihtiyacında, bu donanımlar gizli anahtarların ilgili donanım güvenlik modüllerine geri yüklenmesi için, yetkili kişiler tarafından gerekli erişim bilgileri girilerek kullanılır. Gizli anahtarların bu yedekleme ve

yeniden kullanım işlemleri, iki yetkili personelin aynı anda hazır bulunmasıyla, Bölüm 5.2.2'de belirtildiği gibi, teknik ve idari güvenliği sağlanmış alanlarda yürütülür.

6.2.5. İmza Oluşturma Verisinin Arşivlenmesi

Uygulama dışıdır.

6.2.6. İmza Oluşturma Verisinin Kriptografik Modül Transferi

ESHS kök ve 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 üretimi TÜRKTRUST'ta uygun güvenlik düzeyine sahip güvenli kriptografik donanım modüllerinde gerçekleştirilir ve NES sahiplerinin güvenli elektronik imza oluşturma araçlarına güvenli yollarla taşınır.

6.2.7. İmza Oluşturma Verisinin Kriptografik Modülde Saklanması

TÜRKTRUST sertifika üretim merkezlerinin kök ve alt kök sertifikalarına bağlı imza oluşturma verileri, üretildikleri ve Tebliğ'de tanımlı güvenlik düzeyine sahip kriptografik donanım modüllerinde saklanır.

NES sahiplerinin imza oluşturma verileri 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. Gizli Anahtarın Aktive Edilme Yöntemi

TÜRKTRUST sertifika üretim merkezlerinin kök ve alt kök sertifikalarına bağlı imza oluşturma verileri, içinde bulundukları donanım güvenlik modülü üzerinde, iki yetkilinin hazır bulunmasıyla aktive edilir.

NES'e bağlı imza oluşturma verileri, güvenli elektronik imza oluşturma aracı üzerinde şifre girişiyle aktive edilir. Sertifika sahibi aktivasyon verisinin diğer kişilerce izinsiz kullanımını, verinin çalınmasını veya kaybolmasını önlemek üzere gerekli tedbirleri almaktan sorumludur.

6.2.9. Gizli Anahtarın Deaktive Edilme Yöntemi

TÜRKTRUST sertifika üretim merkezlerinin kök ve alt kök sertifikalarına 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.

NES'e bağlı imza oluşturma verileri güvenli elektronik imza oluşturma aracı üzerinde şifre girişiyle belirli bir süre için aktive edilir ve işlem süresi sonunda deaktive 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. Gizli Anahtarı Yok Etme Metodu

TÜRKTRUST sertifika üretim merkezlerinin kök ve alt kök sertifikalarına bağlı imza oluşturma verilerinin tüm kopyaları, sertifika geçerlilik süreleri sonunda, içinde bulundukları donanım güvenlik modüllerinin anahtar silme özelliği kullanılarak sadece yetkili kişiler

tarafından yok edilir ve yapılan işlemler prosedürler uyarınca kayıt altına alınır. Bu işlem için en az 2 (iki) kişinin aynı anda hazır bulunması gerekir.

NES'e bağlı olan ve güvenli elektronik imza oluşturma aracı içinde saklanan imza oluşturma verileri, imza oluşturma verilerinin silinmesiyle veya donanımın imha edilmesiyle yok edilebilir.

6.2.11. Kriptografik Modül Değerlendirmesi

TÜRKTRUST sertifika üretim merkezlerinin kök ve alt kök sertifikalarına bağlı imza oluşturma verileri, Tebliğ'de tanımlı güvenlik düzeyine sahip kriptografik donanım modüllerinde üretilir ve saklanır.

NES 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 Verilerinin Arşivlenmesi

TÜRKTRUST sertifika üretim merkezlerinin kök ve alt kök sertifikalarına bağlı imza doğrulama verileri, ESHS tarafından 20 yıl süreyle saklanır.

6.3.2. Sertifikanın İşlevsel Süreleri ve Anahtar Çifti Kullanım Süreleri

TÜRKTRUST tarafından üretilen NES'lerin geçerlilik süreleri 1 (bir), 2 (iki) veya 3 (üç) yıldır. Anahtarların kriptografik güvenliği bakımından, aynı içerikle bir sertifikanın toplam geçerlilik süresi 3 (üç) yıldan fazla olamaz.

TÜRKTRUST'a ait kök ve alt kök sertifikaların geçerlilik süreleri 10 (on) yılı aşmaz. Bu sürenin sonunda sertifikalar yenilenirken mutlaka anahtar çiftleri de yenilenir.

6.4. Erişim Şifreleri

6.4.1. Erişim Şifrelerinin Oluşturulması ve Kurulumu

Erişim şifresi, gizli anahtar yönetiminde kullanılan parola, şifre, PIN ya da benzeri özel verilere karşılık gelir.

TÜRKTRUST alt kök ve kök sertifikalarına ait anahtarların üretimi ve bu anahtarlara ait erişim şifrelerinin oluşturulması, Kök ve Alt Kök Sertifika Üretim Yayımlama ve İmha Prosedürü'nde açıklanan törene göre yapılır. Bölüm 6.2.2'de açıklandığı gibi kök ve alt kök sertifikaların gizli anahtarlarının bulunduğu kriptografik modüllere erişim ve anahtarların kullanılması erişim şifrelerine sahip 2 (iki) yetkilinin aynı anda bulunmasıyla mümkündür. Erişim şifreleri, BR'a uyumlu olarak 12 (oniki) alfa numerik değerden oluşur. Sisteme erişim bu şifrelerin yanında yetkililerin biometrik doğrulama yapmalarını da gerektirir. Erişim şifrelerinin oluşturulması, kurulumu ve kullanılması logları (keyed hash ile) veritabanında tutulur.

NES'e ait gizli anahtar güvenlik şartları ve mevzuata uygun olarak akıllı kart içindeki bir devreye güvenli şekilde yerleştirilir. NES'in gizli anahtarı sadece sertifika sahibi tarafından oluşturulan PIN şifresi aracılığıyla kullanılır. NES sahibine gönderilmeden önce rastgele 6 (altı) haneli PIN oluşturulur ve akıllı kart içinde gizli anahtarın bulunduğu güvenli alana yerleştirilir. Akıllı kartı ulaşan sertifika sahibi, TÜRKTRUST akıllı kart yönetim yazılımı aracılığıyla aktivasyon kodunu talep ederek yeni PIN şifresini belirler. TÜRKTRUST akıllı kart yönetim yazılımı tarafından sertifika sahibinin cep telefonuna SMS yoluyla gönderilen aktivasyon kodu aracılığıyla sertifika sahibi PIN şifresini belirler. Sertifika sahibi NES aktivasyon işlemlerinde kullanılan cep telefonu numarasını, sertifika başvuru işlemleri sırasında TÜRKTRUST'a verir.

TÜRKTRUST NES sertifika sahipleri için erişim şifrelerini oluştururken aşağıdaki güvenlik kurallara uyulmasını kuvvetle tavsiye eder:

- En az 6 (altı) karakter kullanılması,
- Bir karakterin fazla sayıda tekrar etmemesi,
- Doğum günü gibi tahmin edilmesini kolaylaştıran verilerin kullanılmaması.

TÜRKTRUST, sertifika sahiplerine en geç 6 (altı) ayda bir erişim şifrelerini değiştirmelerini ve öncekilerden farklı yeni bir şifre belirlemelerini önerir.

6.4.2. Erişim Şifrelerinin Korunması

TÜRKTRUST kök ve alt kök sertifikalarına ait gizli anahtarları kullanan yetkili kişiler, erişim şifrelerini en geç 90 (doksan) günde bir değiştirirler. Yetkili kişiler, erişim şifrelerinin gizliliğinden ve korunmasından sorumludur.

TÜRKTRUST sertifika sahipleri gizli anahtarlarına ait erişim şifrelerini yukarıda belirtilen tavsiyelere uygun şekilde belirlemek ve korumaktan sorumludur.

6.4.3. Erişim Şifreleriyle İlgili Diğer Konular

NES aktivasyon yönteminde erişim şifresi elektronik veya fiziksel hiçbir biçimde taşınmaz. NES aktivasyon kodu TÜRKTRUST veritabanında şifrelenmiş halde tutulur ve herhangi bir kullanıcının erişimine kapalıdır. NES aktivasyon kodunun veritabanından deşifre edilerek çıkması ancak sertifika sahibinin kartını bilgisayarına takması ve TÜRKTRUST yazılımı içinden aktivasyon talep etmesiyle mümkündür. Bu durumda bile sertifika sahibinin bilgisayarıyla TÜRKTRUST sunucusu arasında şifreli haberleşme yapılır. Böylece sertifika sahibine teslim edilmek üzere gönderilen kartın erişim şifresi güvenliği, kartın yaşam döngüsü içinde herhangi bir andan daha az değildir.

6.5. Bilgisayar Güvenlik Kontrolleri

6.5.1. Bilgisayar Güvenliği Teknik Gereklilikleri

TÜRKTRUST tarafından yürütülen sertifika iş süreçleri kapsamında, tüm 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, TÜRKTRUST personeline 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. Veritabanına yetkisiz erişimi ve istenmeden yapılan değişiklikleri önlemek için kimlik doğrulamanın farklı erişim seviyelerinde çeşitli fiziksel ve elektronik önlemler alınır. Veritabanı 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.
- TÜRKTRUST, değişikliklere karşı korunmuş güvenilir sistemler ve ürünler kullanır. Bu bağlamda, Bilgi Teknolojileri ve İletişim Kurumu'nun sürekli denetimi altında, CWA 14167-1 standardının önerileri kesin olarak uygulanır.

6.5.2. Bilgisayar Güvenliğinin Derecelendirilmesi

Uygulama dışıdır.

6.6. Yaşam Döngüsü Teknik Kontrolleri

6.6.1. Sistem Geliştirme Kontrolleri

Sistem geliştirme kontrolleri, geliştirme tesisi güvenliği (tesis güvenlik belgeleri aracılığıyla), geliştirme ortamı güvenliği, geliştirme personeli güvenliği, ürün bakımı sırasında konfigürasyon yönetimi güvenliği ve yazılım geliştirme metodolojisi (ISO/IEC 27001 ve ISO 9001 belgeleri aracılığıyla) için uygulanır. Bu konular ve değişim yönetimi hakkındaki ayrıntılar, Tasarım Kontrolü Prosedürü ile Bilgi Sistemleri Edinim, Geliştirme ve Bakım Prosedüründe dokümante edilmiştir.

6.6.2. Güvenlik Yönetimi Kontrolleri

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

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

6.6.3. Yaşam Döngüsü Güvenlik Kontrolleri

Uygulama dışıdır.

6.7. Ağ Güvenlik Kontrolleri

TÜRKTRUST sertifika üretim merkezlerinin kök ve alt kök sertifikalarının imza oluşturma verileri, ağ güvenliği sağlanmış ortamlarda kullanılmaktadır. Bu sistemler fiziksel ve teknik olarak korunurlar.

TÜRKTRUST içindeki diğer tüm sistemler de 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.

TÜRKTRUST sertifika kayıt merkezleri, sertifika işlemlerine ilişkin kayıtları güvenli ağ bağlantısıyla, internet üzerinden TÜRKTRUST'a iletir.

6.8. Zaman Damgası

TÜRKTRUST tarafından sertifika hizmetlerinin yürütülmesi sırasında 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, SERTİFİKA İPTAL LİSTESİ (SİL) VE OCSP PROFİLLERİ

SUE dokümanının bu kısmında, TÜRKTRUST tarafından üretilen sertifikalar ile SİL'lerin profilleri ve verilen OCSP hizmetinin yapısı yer almaktadır.

7.1. Sertifika Profili

TÜRKTRUST sertifikaları genel olarak "ISO/IEC 9594-8/ ITU-T Recommendation X.509: "Information Technology- Open Systems Interconnection- The Directory: Public –key and attribute certificate frameworks" ile "IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" dokümanlarına uygundur. Ayrıca, TÜRKTRUST tarafından oluşturulan NES'ler Bilgi Teknolojileri ve İletişim Kurumu tarafından yayımlanan "Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri" dokümanına uygundur.

TÜRKTRUST sertifikalarında temel 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

TÜRKTRUST NES "Sertifika İlkeleri" alanı içinde Kanun gereği, "Bu sertifika, 5070 sayılı Elektronik İmza Kanununa göre nitelikli elektronik sertifikadır." ibaresi zorunlu olarak yer alır.

7.1.1. Sürüm Numaraları

TÜRKTRUST tarafından oluşturulan kök ve alt kök sertifikalar ile son kullanıcı sertifikaları, "IETF RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" dokümanı uyarınca X.509 v3 sürümünü destekler.

7.1.2. Sertifika Uzantıları

NES'ler, "IETF RFC 3039 Internet X.509 Public Key Infrastructure Qualified Certificates Profile" ve "Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri" dokümanları uyarınca tanımlanan nitelikli elektronik sertifika uzantılarını içerir.

TÜRKTRUST tarafından oluşturulan NES'ler içerisinde aşağıdaki sertifika uzantıları bulunur:

Uzantı Adı	Kritik İşaretli	Açıklama
Authority Key Identifier (Yetkili Anahtarı Tanımlayıcısı)	Hayır	Sertifikayı yayımlayan TÜRKTRUST ESHS sertifikasının açık anahtar özet değeri.
Subject Key Identifer	Hayır	Sertifikada yer alan açık anahtarın özet

(Özne Anahtarı Tanımlayıcısı)		değeri.
Key Usage (Anahtar Kullanımı)	Evet	Digital signature (elektronik imza) ve non-repudiation (inkar edilemezlik) alanları bulunmaktadır.
Certificate Policies (Sertifika İlkeleri)	Hayır	• İlke Tanımlayıcı Numarası (Policy Identifier) olarak 2.16.792.3.0.3.1.1.1 değeri • Sertifika Uygulama Esasları adresi (Policy Qualifier Info – CPS) olarak http://www.turktrust.com.tr/sue değeri • Kullanıcı Uyarısı (Policy Qualifier Info – 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.
Subject Alternative Name (Özne Alternatif Adı)	Hayır	Opsiyonel olarak sertifika sahibinin elektronik posta adresi kullanılabilmektedir.
Qualified Certificate Statements (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 TÜRKTRUST ESHS sertifikası tarafından imzalanmış olan SİL (CRL) dosyasının HTTP URL adresi.
Authority Information Access (ESHS Bilgi Erişimi)	Hayır	Sertifikayı yayımlayan TÜRKTRUST ESHS sertifikasına ve TÜRKTRUST OCSP servisine erişim adresleri.

TÜRKTRUST tarafından oluşturulan ve NES sertifikalarının dâhil olduğu hiyerarşilerde kullanılan OCSP hizmet sertifikalarında aşağıdaki uzantılar bulunur:

Uzantı Adı	Kritik İşaretli	Açıklama
Authority Key Identifier (Yetkili Anahtarı Tanımlayıcısı)	Hayır	Sertifikayı yayımlayan ESHS sertifikasının açık anahtar özet değeri.
Subject Key Identifer (Özne Anahtarı Tanımlayıcısı)	Hayır	Sertifikada yer alan açık anahtarın özet değeri.
Basic Constraints (Temel Kısıtlar)	Hayır	ESHS (CA) değeri "false" olarak işaretlenmektedir.
Extended Key Usage (Genişletilmiş Anahtar Kullanımı)	Hayır	OCSP signing (OCSP imzalama) değeri bulunmaktadır.
CRL Distribution Points (SİL Dağıtım Noktaları)	Hayır	Sertifikayı yayımlayan TÜRKTRUST ESHS sertifikası tarafından imzalanmış olan SİL (CRL) dosyasının URL adresi.
Authority Information Access (ESHS Bilgi Erişimi)	Hayır	Sertifikayı yayımlayan TÜRKTRUST ESHS sertifikasına ve TÜRKTRUST OCSP servisine erişim adresleri.

7.1.3. Algoritma Nesne Tanımlayıcıları

TÜRKTRUST tarafından oluşturulan tüm sertifikaların imzalanmasında aşağıdaki algoritmalardan biri kullanılır.

Algoritma Adı	Nesne Tanımlayıcı Numarası
SHA-256 ile RSA	1.2.840.113549.1.1.11
SHA-384 ile RSA	1.2.840.113549.1.1.12
SHA-512 ile RSA	1.2.840.113549.1.1.13

NES için ilgili algoritmalar yasal düzenlemelerin gerektirdiği şekilde kullanılmaktadır.

7.1.4. İsim Biçimleri

TÜRKTRUST tarafından üretilen sertifikalarda X.500 biçiminde ayırt edilebilir isimler kullanılır.

"Sertifikayı Veren" olarak TÜRKTRUST, "O=TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş." açık unvanıyla yazılır. Ayrıca NES'lerde bu alan altında "OU= Dayanak: T.C. 5070 sayılı Elektronik İmza Kanunu" ibaresi yer alır.

NES'lerde "Sertifika Sahibi" alt alanlarında aşağıdaki değerler bulunur:

"SERIAL NUMBER"	T.C. vatandaşı gerçek kişiler (NES) için eşsiz TCKN numarası, yabancı kişiler için, yabancı kimlik numarası ya da uluslararası ülke kodu ile birlikte pasaport numarası.
"CN"	Kişinin açık ve tam ismi.
"C"	"TR" değeri.
"L"	Opsiyonel olarak kişinin yaşadığı şehir.
"O"	Opsiyonel olarak kişinin çalıştığı kurum.
"OU"	Opsiyonel olarak kişinin kurumunda bağlı olduğu birim.
"T"	Opsiyonel olarak kişinin mesleki unvanı.

7.1.5. İsim Kısıtları

TÜRKTRUST tarafından üretilen sertifikalarda anonim veya takma adlar kullanılmaz. TÜRKTRUST nitelikli elektronik sertifikalarındaki isimlerde ayırt edici özellik olarak T.C. kimlik numarası veya pasaport numarası kullanılır.

7.1.6. Sertifika İlkeleri Nesne Tanımlayıcısı

TÜRKTRUST tarafından üretilen sertifikaların "sertifika ilkeleri" uzantısında bu SUE dokümanı Madde 1.2'de belirtilen ilgili sertifika ilkeleri nesne tanımlayıcı numarası (OID) kullanılır.

7.1.7. İlke Kısıtları Uzantısının Kullanımı

TÜRKTRUST alt kök sertifikalarında ihtiyaca göre ilke kısıtları uzantısı kullanabilir.

7.1.8. İlke Niteleyicilerinin Yazımı

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

7.1.9. Kritik Sertifika İlkeleri Uzantısının İşlenme Semantiği

Uygulama dışıdır.

7.2. SİL Profili

TÜRKTRUST tarafından yayımlanan SİL'lerde temel olarak, TÜRKTRUST 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. TÜRKTRUST tarafından yayımlanan SİL'ler Bilgi Teknolojileri ve İletişim Kurumu tarafından yayımlanan "Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri" dokümanına uygundur.

7.2.1. Sürüm Numarası

TÜRKTRUST tarafından oluşturulan SİL'ler, "IETF RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" dokümanı uyarınca X.509 v2 sürümünü destekler.

7.2.2. SİL ve SİL Giriş Uzantıları

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

7.3. OCSP Profili

TÜRKTRUST 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. TÜRKTRUST tarafından verilen OCSP cevap mesajları, Bilgi Teknolojileri ve İletişim Kurumu tarafından yayımlanan "Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri" dokümanına uygundur.

7.3.1. Sürüm Numarası

TÜRKTRUST tarafından verilen OCSP hizmeti, "IETF RFC 6960 Internet X.509 Public Key Infrastructure Online Certificate Status Protocol - OCSP" dokümanı uyarınca v1 protokol sürümünü destekler.

7.3.2. OCSP Uzantıları

TÜRKTRUST tarafından verilen OCSP hizmeti içeriğinde, RFC 6960 tarafından tanımlanan uzantılar kullanılabilir. Ancak, temel OCSP bilgileri dışındaki tüm uzantıların kullanılması zorunlu değildir.

8. UYGUNLUK DENETİMİ VE DİĞER DEĞERLENDİRMELER

TÜRKTRUST, ilgili elektronik imza mevzuatı gereğince Bilgi Teknolojileri ve İletişim Kurumu tarafından denetlenir.

Ayrıca, tüm ESHS süreçleri, bilgi güvenliği yönetim sisteminin sürekliliği açısından ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi ve TS EN ISO 9001 Kalite Yönetim Sistemi sertifikaları uyarınca periyodik olarak uygunluk denetimine tabi tutulur.

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

TÜRKTRUST, ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemine göre risk değerlendirmelerini gerçekleştirir. Bunun sonucunda, iş riskleri değerlendirilir ve gerekli güvenlik koşulları ve işletim prosedürleri belirlenir. Risk analizi düzenli olarak gözden geçirilir ve gerektiğinde güncelleme yapılır.

8.1. Denetim Sıklığı ve Durumları

Bilgi Teknolojileri ve İletişim Kurumu, düzenleyici ve denetleyici Kurum olarak gerekli gördüğü durumlarda re'sen denetim yapar. Denetleme sırasında, denetleme yapmaya yetkili görevliler tarafından her türlü defter, belge ve kayıtların verilmesi, yönetim yerleri, binalar ve eklentilerine girme, yazılı ve sözlü bilgi alma, örnek alma ve işlem ve hesapları denetleme isteminin elektronik sertifika hizmet sağlayıcıları ve ilgililer tarafından yerine getirilmesi zorunludur.

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi ve TS EN ISO 9001 Kalite Yönetim Sistemi sertifikaları uyarınca, her yıl takip denetiminden ve her üç yılda bir de belge yenileme denetiminden geçilir.

İç denetim, plan gereği her üç ayda bir ESHS süreçleri, yılda iki defa ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi ve TS EN ISO 9001 Kalite Yönetim Sistemi süreçleri üzerinden yapılır.

8.2. Denetçinin Kimliği ve Özellikleri

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

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi ve TS EN ISO 9001 Kalite Yönetim Sistemi sertifikasyonları, yetkilendirilmiş denetçi tarafından gerçekleştirilir.

TÜRKTRUST'ın kurumsal iç denetimi, TÜRKTRUST yetkili personeli tarafından yapılır. İç denetim, TÜRKTRUST bünyesindeki Bilgi Güvenliği Yönetim Sistemi Sorumlusu ve Kalite Yönetim Sistemi Sorumlusu tarafından yürütülür.

8.3. Denetçinin ESHS'yle İlişkisi

Denetçi kuruluş olan Bilgi Teknolojileri ve İletişim Kurumu, Kanun gereği Türkiye'de NES ile ilgili faaliyet gösteren tüm ESHS'leri denetlemekle yetkili kılınmış düzenleyici kuruluştur.

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi ve TS EN ISO 9001 Kalite Yönetim Sistemi sertifikasyonları bağımsız ve yetkili denetçi tarafından gerçekleştirilir.

TÜRKTRUST'ın kurumsal iç denetimi, TÜRKTRUST yetkili personeli tarafından yapılır.

8.4. Denetimde Kapsanan Başlıklar

Bilgi Teknolojileri ve İletişim Kurumu'nun denetimi Kanun'la kendisine verilen yetki çerçevesinde, TÜRKTRUST'ın 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 ve TS EN ISO 9001 Kalite Yönetim Sistemi sertifikasyonları, TÜRKTRUST elektronik sertifika ve zaman damgası hizmetleri kapsamındadır.

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

8.5. Eksiklik Durumunda Yapılacaklar

Yönetmelik gereği Bilgi Teknolojileri ve İletişim Kurumu tarafından yapılan denetimler sırasında, TÜRKTRUST'ın faaliyet ve işleyişini olumsuz yönde etkileyebilecek derecede önemli konuların belirlenmesi durumunda, ilgili mevzuatta öngörülen yaptırım ve cezalar uygulanır.

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi ve TS EN ISO 9001 Kalite Yönetim Sistemi denetimleri sırasında saptanan eksikliklerin majör nitelikte olması sertifikanın geri alınmasına neden olabilir. Minör eksikler, bir sonraki denetim dönemine kadar TÜRKTRUST tarafından giderilir.

TÜRKTRUST tarafından yapılan iç denetimlerde belirlenen aksaklıklar hakkında düzeltici faaliyetler yürütülür.

8.6. Sonuçların Bildirilmesi

Kanun gereği Bilgi Teknolojileri ve İletişim Kurumu tarafından yapılan denetimin sonuçları gerek duyulduğu takdirde resmi yollarla TÜRKTRUST'a iletilir. Kurum'un bir geri bildirimde bulunmaması, olumsuz bir değerlendirmenin olmadığı anlamını taşır.

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi ve TS EN ISO 9001 Kalite Yönetim Sistemi denetim sonuçları, denetçi tarafından resmi olarak TÜRKTRUST'a bildirilir.

İç denetim sonuçları ise, iç denetim sonuç raporlarında yer alır ve ilgili yetkililerin değerlendirmesine sunulur.

9. DİĞER İŞ KONULARI VE YASAL KONULAR

SUE dokümanının bu kısmında, TÜRKTRUST'ın ticari ve yasal uygulamaları ile sertifika süreçleri uyarınca yerine getirilmesi gereken hizmet koşulları yer almaktadır.

9.1. Ücretler

9.1.1. Sertifika Üretim ve Yenileme Ücretleri

TÜRKTRUST tarafından üretilen nitelikli elektronik sertifikalar, geçerlilik sürelerine göre ve içeriklerinde yer alan maddi işlem sınırı ölçüsünde, sertifika üretim maliyetleri ve piyasa koşulları uyarınca fiyatlandırılır. Artan maddi işlem sınırı, artan sertifika mali sorumluluk sigortası primleri üzerinden sertifika fiyatlarına yansıtılır.

Güncel sertifika fiyat bilgileri, TÜRKTRUST web sitesi ve uygun görülen diğer iletişim kanalları üzerinden müşterilere duyurulur.

9.1.2. Sertifika Erişim Ücretleri

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

Sertifika erişim hizmetleri için ücret talep edilmez.

9.1.3. İptal veya Durum Bilgisi Erişim Ücretleri

TÜRKTRUST tarafından üretilen sertifikalara ait iptal veya durum bilgisi, SİL'ler ve OCSP hizmeti aracılığıyla üçüncü kişilerin erişimine açık tutulur.

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

9.1.4. Diğer Hizmetlerin Ücretleri

TÜRKTRUST, kamuya açık olarak yayımladığı Sİ, SUE, sertifika sahibi ve sertifika hizmetleri taahhütnameleri gibi kitapçık ve belgeler için ücret talep etmez.

Bunların dışında kalan ve katma değerli olarak üretilerek müşterilere sunulan diğer ürün ve hizmetler için uygulanacak ücretler, web sitesi ve uygun görülen diğer iletişim kanalları üzerinden müşterilere duyurulur.

9.1.5. Bedel İadesi

TÜRKTRUST, NES hizmetlerinde bedel iadesi yapmaz. Ancak, TÜRKTRUST'tan kaynaklanan nedenlerle, sertifika içeriğinde başvurudan farklı verilerin bulunması durumunda, her hangi bir ücret talep edilmeden yeni bir sertifika verilir veya talep edilmesi durumunda bedel iadesi yapılır.

9.2. Finansal Sorumluluk

TÜRKTRUST, Kanun'dan doğan yükümlülüklerini yerine getirmemesi sonucu doğacak zararların karşılanması amacıyla sertifika mali sorumluluk sigortası yaptırmakla yükümlüdür. Sigortaya ilişkin koşullar 26 Ağustos 2004 tarih ve 25565 sayılı Resmi Gazetede yayımlanmış olan "Sertifika Mali Sorumluluk Sigortası Yönetmeliği" ve ilgili tebliğlerde yer almaktadır.

9.2.1. Sigorta Kapsamı

"Sertifika Mali Sorumluluk Sigortası Yönetmeliği" Madde 6 uyarınca, zorunlu sertifika mali sorumluluk sigortası, ESHS'nin güvenli ürün ve sistemleri kullanma, hizmeti güvenilir bir biçimde yürütme ve sertifikaların taklit ve tahrif edilmesini önlemekle ilgili yükümlülüklerini

yerine getirmemesi dolayısıyla zarar görecek olanlara karşı doğacak hukuki sorumlulukların teminat altına alınmasını kapsar.

9.2.2. Diğer Varlıklar

Uygulama dışıdır.

9.2.3. Son Kullanıcılar için Sigorta veya Garanti Kapsamı

TÜRKTRUST, Kanundan doğan yükümlülüklerini yerine getirmemesi sonucu doğacak zararların karşılanması amacıyla, NES'leri sertifika sahiplerine teslim etmeden önce sertifika malî sorumluluk sigortası yaptırmakla yükümlüdür.

9.3. İş Bilgisinin Gizliliği

9.3.1. Gizli Bilginin Kapsamı

TÜRKTRUST'ın elektronik sertifika hizmet sağlayıcılığı işlevleriyle ilgili her türlü ticari gizli bilgi ve belge, TÜRKTRUST sertifika üretim merkezlerinin kök ve alt kök sertifikalarının imza oluşturma verileri, kullanılan yazılım ve donanım bilgileri, işlem kayıtları, denetim raporları, tesis içi bölge ve cihazlara ait erişim şifreleri, tesis planı ve iç tasarımı, acil eylem planları, iş planları, satış bilgileri, işbirliği sözleşmeleri, iş ortaklığı yapılan kuruluşlara ait gizlilik dereceli bilgiler, gizli bilgi kapsamına girer.

9.3.2. Gizlilik Kapsamı Dışındaki Bilgi

TÜRKTRUST'ın ticari gizliliği olmayan, Kanun ve uygulamalar gereği kamuya açık olması gereken bilgi ve belgeleri gizlilik kapsamı dışında tutulur. Üretilen sertifikalar, SİL'ler, sertifika hizmetleriyle ilgili müşteri kılavuzları, Sİ dokümanı, SUE dokümanı, sertifika sahibi ve sertifika hizmetleri taahhütnameleri içeriğindeki bilgiler gizlilik kapsamına girmez.

9.3.3. Gizli Bilginin Korunması Sorumluluğu

TÜRKTRUST çalışanlarının tamamı gizli bilgilerin korunması konusunda sorumluluk sahibidir. Güvenlik politikaları gereği hiçbir gizli bilgiye, yetkilisi dışındaki çalışanların ya da üçüncü kişilerin erişimine izin verilmez. Bilgi güvenliğinin sağlanmasıyla ilgili tüm prosedürler çalışanlar tarafından eksiksiz uygulanır ve bu prosedürlerin uygulanması TÜRKTRUST iç denetimine tabidir.

9.4. Kişisel Bilgilerin Gizliliği/Özelliği

9.4.1. Gizlilik Planı

TÜRKTRUST, verdiği sertifika hizmetleri kapsamında, sertifika başvuru sahiplerine, sertifika sahibi müşterilerine ya da diğer katılımcılara ait kişisel bilgilerin gizliliğini korur.

9.4.2. Özel Olarak Değerlendirilecek Bilgi

TÜRKTRUST tarafından sertifika hizmetlerinin verilmesi sırasında ihtiyaç duyulan ve sertifika başvuru sahiplerinden alınmış olan kimlik doğrulama bilgi ve belgeleri ile TÜRKTRUST tarafından sertifika hizmetlerinin yürütülmesi için kullanılacak olup sertifika içeriğinde yer almayan nüfus bilgileri, iletişim bilgileri gibi müşteri bilgileri, özel bilgi olarak değerlendirilir.

9.4.3. Özel Sayılmayacak Bilgi

TÜRKTRUST müşterisi olan nitelikli elektronik sertifika sahiplerine ait sertifikaların içeriğinde yer alan ve sertifikalarla birlikte üçüncü kişilere duyurulan bilgiler, aksi sertifika sahibi tarafından talep edilmedikçe özel bilgi sayılmaz.

9.4.4. Özel Bilgiyi Koruma Sorumluluğu

TÜRKTRUST çalışanlarının tamamı başvuru sahiplerine ve müşterilere ait özel bilgilerin korunması konusunda sorumluluk sahibidir. Hiçbir özel bilgiye, yetkilisi dışındaki çalışanların ya da üçüncü kişilerin erişimine izin verilmez.

9.4.5. Özel Bilgiyi Kullanma Bildirimi ve Onayı

TÜRKTRUST, işbu dokümanda ve nitelikli elektronik sertifika sahibi taahhütnamesinde düzenlenmiş amaçlar için sertifikayı veya sertifika başvurusunda sağlanmış bilgi içeriğini kullanabilir.

9.4.6. Yargısal ve İdari Süreçlere Uygun Olarak Bilginin Açıklanması

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

9.4.7. Bilginin Açıklandığı Diğer Durumlar

Uygulama dışıdır.

9.5. Fikri Mülkiyet Hakları

TÜRKTRUST tarafından üretilen sertifikalar, SİL'ler, sertifika hizmetleriyle ilgili müşteri kılavuzları, Sİ ve SUE kitapçıkları, sertifika sahibi ve sertifika hizmetleri taahhütnameleri, sertifika hizmetlerinin yürütülmesiyle ilgili her türlü iç ve dış doküman, veritabanları, web siteleri ile sertifika hizmetlerine bağlı olarak geliştirilen tüm ürünlerin fikri mülkiyet hakları TÜRKTRUST'a aittir.

Sertifika sahipleri, sertifika içeriğinde yer alan ve kendilerine ait her türlü ayırt edici isim ve markanın mülkiyet haklarına sahiptir.

9.6. Sorumluluklar

9.6.1. ESHS Beyan ve Garantileri

TÜRKTRUST'a bağlı sertifika üretim merkezleri, üretilen nitelikli elektronik sertifikaların içeriğinin doğru olduğunu, kimlik doğrulama adımlarının doğru ve güvenilir biçimde yürütüldüğünü, doğru sertifikanın doğru başvuru sahibi adına üretildiğini ve doğru kişiye teslim edildiğini, yayımlanan sertifika durum bilgilerinin güncelliğini ve doğruluğunu; Sİ ve SUE'de yer alan tüm uygulama gereklilikleri ve yükümlülüklerini yerine getireceğini garanti eder. Bu işlemlerin doğru şekilde yapılması için her süreçle ilgili iş prosedür ve talimatları detaylı şekilde belirler.

TÜRKTRUST'a bağlı sertifika üretim merkezleri, NES verebilmek için, Kanun Madde 10 ve Yönetmelik Madde 14'te yer alan ESHS yükümlülüklerini yerine getirir.

9.6.2. Kayıt Merkezi Sorumlulukları

TÜRKTRUST'a bağlı kayıt merkezleri, kendilerine başvuran gerçek veya tüzel kişilerin sertifika tiplerine göre işbu SUE dokümanında belirtilen kimlik doğrulama adımlarının doğru ve güvenilir biçimde yürütüldüğünü, kayıtların doğru biçimde tutulduğunu, ESHS merkezine gönderilen sertifika üretim, yenileme ve iptal taleplerinin doğru ve eksiksiz olduğunu garanti eder.

9.6.3. Sertifika Sahibi Sorumlulukları

Nitelikli elektronik sertifika sahipleri, sertifika başvurusu ile yenileme ve iptal talepleri sırasında TÜRKTRUST'a güncel ve doğru bilgi ve belgeler sunmayı, sertifikalarını Sİ ve SUE

kitapçıklarında yer alan koşullar uyarınca kullanmayı, sertifika sahibi taahhütnamesinde yer alan tüm yükümlülüklerini yerine getireceğini garanti eder.

NES sahipleri, nitelikli elektronik sertifika sahibi taahhütnamesinde yer alan koşullarla birlikte, Yönetmelik Madde 15'te yer alan yükümlülükleri de yerine getirmek zorundadır.

9.6.4. Üçüncü Kişilerin Sorumlulukları

Nitelikli elektronik sertifika sahipleri ile üçüncü kişiler, TÜRKTRUST NES'lerine dayanılarak oluşturulmuş elektronik imzaların geçerliliğini doğrulamaktan kendileri sorumludur.

9.6.5. Diğer Katılımcıların Sorumlulukları

TÜRKTRUST'ın sertifika hizmetlerini verirken işbirliği yaptığı ve hizmet aldığı tüm kişi ve kuruluşlardan oluşan diğer katılımcılar, verecekleri hizmeti güvenilir ve doğru biçimde vereceklerini ve TÜRKTRUST iş süreçleri ve müşterileriyle ilgili gizli veya özel bilgileri açığa çıkarmayacaklarını garanti eder. TÜRKTRUST ile hizmet aldığı kuruluşlar arasında bu garantilerin açıkça belirtildiği hizmet sözleşmeleri imzalanır.

9.7. Sorumlulukların Geçersiz Olduğu Durumlar

Uygulama dışıdır.

9.8. Sorumluluk Sınırları

TÜRKTRUST tarafından verilen nitelikli elektronik sertifikalar, parasal işlemlerde maddi işlem sınırları dahilinde sigortalıdır. Sertifikalar ve bu sertifikaların kullanımıyla ilgili sorumluluk sınırları, nitelikli elektronik sertifika sahibi taahhütnamesinde açıkça belirtilmiştir.

NES'ler için zorunlu sertifika mali sorumluluk sigortası, 10.000 TL tutarında olay başına teminat limitini ve 1.000.000 TL tutarında yıllık azami teminat limitini kapsar.

9.9. Tazminatlar

TÜRKTRUST, bu Sİ ve SUE'de yer alan ilke ve esaslar gereği yükümlülüklerini yerine getiremez ve bu durumdan üçüncü kişiler zarar görürse ilgili zarar, TÜRKTRUST tarafından tazmin edilir.

Nitelikli elektronik sertifika hizmetleri uyarınca, Kanun Madde 13 gereği, TÜRKTRUST Kanun ve Yönetmelik hükümlerinin ihlali suretiyle üçüncü kişilere vereceği zararları tazminle yükümlüdür. Bu durumlarda TÜRKTRUST kusursuzluğunu ispat ettiği takdirde tazminat ödeme yükümlülüğü doğmaz.

Nitelikli elektronik sertifika sahipleri, nitelikli elektronik sertifika sahibi taahhütnamesi hükümleri gereği yükümlülüklerini yerine getirmez ve bu durumdan TÜRKTRUST veya üçüncü kişiler zarar görürse, ilgili zararın sertifika sahibi tarafından tazmin edilmesi gerekir.

9.10. SUE dokümanının Geçerliliği

9.10.1. SUE dokümanının Geçerlilik Dönemi

SUE dokümanının bu sürümü, yeni bir sürüm çıkarılana kadar geçerlidir.

9.10.2. SUE dokümanının Geçerliliğinin Sona Ermesi

TÜRKTRUST faaliyetlerinde ve sertifika hizmetlerinde oluşabilecek değişikliklere ve düzenlemelere bağlı olarak, SUE dokümanının mevcut sürümünün içeriğinin değişmesini gerektiren herhangi bir durum ortaya çıktığında, kitapçık kısmen ya da tamamen geçersiz

duruma düşebilir. Bu durumda, ilgili değişikliklerin yansıtıldığı yeni bir SUE dokümanı sürümü TÜRKTRUST tarafından hazırlanır ve yayımlanır.

9.10.3. Geçerliliğin Sona Ermesinin Etkileri ve İşlerliğin Sürdürülmesi

Mevcut SUE sürümünün geçerliliğinin sona ermesi durumunda, TÜRKTRUST faaliyetlerinin ve sertifika hizmetlerinin kesintiye uğramaması için gerekli önlemler alınır. Yeni SUE sürümü, eski SUE sürümünün geçerliliği sona ermeden hazırlanır ve değişim hizmet kesintisi olmadan gerçekleştirilir.

Değişiklikler gereği TÜRKTRUST tarafından üretilen nitelikli elektronik sertifikalarda herhangi bir değişiklik yapılması gerekirse, sertifika sahipleriyle ve üçüncü kişilerle bu durum paylaşılır ve gerekli işlemler hızlıca tamamlanır. Yeni sürüm gereği değişen uygulamalar TÜRKTRUST tarafından hemen devreye alınır.

9.11. Taraflara Özel Duyurular ve İletişim

TÜRKTRUST tarafından sertifika sahiplerine yapılacak olan kişisel duyurular için e-posta kullanılır. Gerekli görülen durumlarda ise yazı ile duyurular gönderilebilir.

TÜRKTRUST'ın üçüncü kişilere yapacağı duyurular web üzerinden ya da basın yayın organları aracılığıyla yayımlanır.

9.12. Değişiklikler

TÜRKTRUST faaliyetlerinde ve sertifika hizmetlerinde oluşabilecek değişikliklere ve düzenlemelere bağlı olarak, SUE dokümanının mevcut sürümünün içeriğinin değişmesini gerektiren herhangi bir durum ortaya çıktığında, ilgili değişikliklerin yansıtıldığı yeni bir SUE dokümanı sürümü TÜRKTRUST tarafından hazırlanır ve TÜRKTRUST Yönetim Kurulu'nun onayının ardından yayımlanır.

SUE dokümanında, önceden üretilmiş olan nitelikli elektronik sertifikaların kullanımını ve kabul edilirliğini etkilemeyecek olan küçük değişiklikler olabileceği gibi, sertifika kullanımına doğrudan etki edebilecek önemli değişiklikler de olabilir. Her iki durumda TÜRKTRUST uygulamaları farklı olacaktır.

9.12.1. Değişiklik Prosedürü

TÜRKTRUST faaliyetlerinde ve sertifika hizmetlerinde oluşabilecek değişikliklere ve düzenlemelere bağlı olarak, SUE dokümanının mevcut sürümünün içeriğinin değişmesini gerektiren herhangi bir durum ortaya çıktığında, ilgili değişikliklerin yansıtıldığı yeni bir SUE dokümanı sürümü TÜRKTRUST tarafından hazırlanır ve yayımlanır.

SUE dokümanı ve ilgili uygulamalar, yönetim gözden geçirme toplantılarında yıllık olarak gözden geçirilir.

Sİ'de oluşan değişiklikler, SUE'deki ilgili uygulamalara da yansıtılır. Dolayısıyla yeni bir Sİ sürümü, yeni bir SUE sürümünü de gerektirir. TÜRKTRUST tarafından üretilen yeni sertifikaların "sertifika ilkeleri" uzantısında URL olarak verilen SUE dokümanına erişim bilgisi aynı kalır, ama bu adresin işaret ettiği SUE dokümanı yeni sürümdür.

Küçük değişiklikler olması durumunda, önceden verilmiş olan sertifikalar da yeni Sİ ve SUE'ye uygun olarak kullanılmaya devam eder. Ancak önemli değişiklikler nedeniyle yeni bir Sİ sürümü çıkarılmışsa, önceden üretilmiş sertifikaların, değişiklik yapılan sertifika ilkelerine bağlı olanları, yeni Sİ'ye uyumlu olarak kullanılamayabilir.

9.12.2. Duyuru Mekanizması ve Süresi

TÜRKTRUST faaliyetleri ve sertifika hizmetlerindeki uygulama değişiklikleri ile mevcut Sİ ve SUE kitapçıklarında değişiklik oluşması durumunda, çıkarılan güncel Sİ ve SUE sürümleri hakkında nitelikli elektronik sertifika sahipleri ile üçüncü kişiler ivedilikle bilgilendirilir.

Özellikle önemli değişikliklerde, sertifikanın kullanılabilirliği ve kabul edilirliği bazı uygulamalarda etkilenebileceğinden, TÜRKTRUST nitelikli elektronik sertifika sahipleri ile üçüncü kişileri bilgilendirebilmek için tüm makul imkânları kullanır. Değişiklik TÜRKTRUST web sitesinde yayımlanır, sertifika sahiplerine e-posta aracılığıyla bildirilir, gerektiğinde basın ve yayın organları aracılığıyla tüm üçüncü kişilerin durumdan haberdar olması sağlanır.

Küçük değişikliklerde ise web sitesi aracılığıyla durum ilan edilir.

Yeni Sİ ve SUE sürümleri, eski sürümlerle birlikte TÜRKTRUST bilgi deposunda, ayrıntılı sürüm bilgisi içerecek şekilde yayımlanır ve ilgili tarafların erişimine açık tutulur.

9.12.3. Nesne Tanımlayıcı Numaralarının Değişmesini Gerektiren Durumlar

Nitelikli elektronik sertifika kullanımını ve kabul edilirliğini doğrudan etkileyebilecek olan, kullanılan kimlik doğrulama adımlarını önemli ölçüde etkileyen veya sertifika hizmetlerinde sertifikanın güvenlik düzeyine etki edebilecek biçimde gerçekleşen önemli değişiklikler, Sİ dokümanında tanımlanan ilgili sertifika ilkelerinin nesne tanımlayıcı numaralarının da değişmesini gerektirebilir. Bu durumda, yeni üretilen sertifikalarda, uygulanacak olan yeni sertifika ilkelerinin nesne tanımlayıcı numaraları yer alır.

9.13. Anlaşmazlıkların Çözümü

TÜRKTRUST, sertifika sahipleri ve üçüncü kişiler arasında çıkabilecek anlaşmazlıklarda öncelikle, Sİ ve SUE kitapçıklarında belirlenmiş ilke ve uygulama esasları ile prosedürler, taahhütnameler ve sözleşmeler uyarınca sorunun çözümlenmesine çalışılır.

Nitelikli elektronik sertifikalarla ilgili işlemler TÜRKTRUST tarafından Kanun ve Yönetmelikler ile bunlara bağlı Tebliğler uyarınca yürütülür.

Taraflar arasındaki anlaşmazlıklar sulhen çözüme kavuşmadığı takdirde, anlaşmazlıkların çözümü için Ankara Mahkemeleri yetkilidir.

9.14. Yasal Düzenleme

Türkiye'de, elle atılan imza ile aynı hukuki sonucu doğuran güvenli elektronik imzanın kullanımı, 5070 sayılı "Elektronik İmza Kanunu" ve Bilgi Teknolojileri ve İletişim Kurumu tarafından yayımlanmış Yönetmelik ve Tebliğler uyarınca düzenlenir. Kurum ESHS'lerin Kanun uyarınca işleyişinin düzenlenmesi ve denetlenmesinden sorumludur.

9.15. İlgili Yasalara Uygunluk

TÜRKTRUST, NES hizmetlerini 5070 sayılı "Elektronik İmza Kanunu" ve Bilgi Teknolojileri ve İletişim Kurumu tarafından yayımlanmış Yönetmelik ve Tebliğler ile diğer ilgili düzenlemeler uyarınca yürütür.

9.16. Çeşitli Hükümler

9.16.1. Bütün Anlaşma

Uygulama dışıdır.

9.16.2. Görevlendirme

Uygulama dışıdır.

9.16.3. Kitapçık Kısımlarının Ayrılabilirliği

Sİ ve SUE kitapçıklarının diğer bölümlerinin geçerliliğini etkilemeyen herhangi bir bölümü geçerliliğini kaybettiğinde, TÜRKTRUST tarafından ilgili değişikliklerin yansıtıldığı yeni sürümler çıkarılana kadar, kitapçığın etkilenmemiş diğer bölümleri geçerliliğini korur ve uygulanır.

9.16.4. Yasal Haklardan Vazgeçme

Uygulama dışıdır.

9.16.5. Mücbir Sebepler

TÜRKTRUST'ın elektronik sertifika hizmet sağlayıcılığıyla ilgili faaliyetlerini yerine getirmesini engelleyecek ve normal koşullar altında kontrol edilebilir olmayan durumlar mücbir sebep olarak adlandırılır. Bu durumlar devam ettiği sürece, TÜRKTRUST faaliyetleri aksaklığa veya kesintiye uğrayabilir. Doğal afetler, savaşlar, terör, telekomünikasyon, İnternet ve benzeri diğer altyapılarda oluşabilecek aksaklıklar mücbir sebep kabul edilir.

9.17. Diğer Hükümler

Uygulama dışıdır.

EK – 1

TÜRKTRUST

NİTELİKLİ ELEKTRONİK SERTİFİKA SAHİBİ TAAHHÜTNAMESİ

1. Bu taahhütnamede geçen;
   a) "Sertifika" deyimi; 5070 sayılı Elektronik İmza Kanununun 9. maddesinde tanımlanan nitelikli elektronik sertifikayı,
   b) "Sertifika sahibi" deyimi; 5070 sayılı Elektronik İmza Kanununun 3. maddesinde tanımlanan sertifika sahibi gerçek kişiyi,
   c) "TÜRKTRUST" deyimi; TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş.'yi,
   d) "TÜRKTRUST düzenlemeleri" deyimi; nitelikli elektronik sertifikalar için TÜRKTRUST web sitesinde ilan edilen Sertifika İlkelerini, Sertifika Uygulama Esasları dokümanlarını ve müşteri kılavuzlarını,
   e) "Mevzuat" deyimi; 5070 sayılı Elektronik İmza Kanununu, Bilgi Teknolojileri ve İletişim Kurumu tarafından yayımlanan "Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik", "Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ" ile "Sertifika Mali Sorumluluk Sigortası Yönetmeliği"ni,
   f) "İmza oluşturma aracı" deyimi, 5070 sayılı Elektronik İmza Kanununun 6. maddesinde tanımlanan güvenli elektronik imza oluşturma aracını

   ifade eder.

2. Sertifika sahibi,
   a) Güvenli elektronik imzanın elle atılan imza ile eşdeğer olduğunu bilir ve kabul eder.
   b) İlgili Mevzuatı ve TÜRKTRUST düzenlemelerini okuduğunu kabul eder.
   c) Sertifika başvurusu sırasında ve sertifikanın geçerlilik süresi boyunca, TÜRKTRUST'a bildirdiği tüm kişisel bilgilerin tam ve doğru olduğunu beyan ve taahhüt eder.
   d) Sertifikayı iptal etmek istediğinde, TÜRKTRUST'a bu bildirimi mümkün olan en kısa sürede yapacağını kabul eder.
   e) Eğer imza oluşturma aracı TÜRKTRUST tarafından sağlanmış ise, adına düzenlenen akıllı kart, akıllı çubuk ve benzeri elektronik imza oluşturma aracını ve bu araca ait erişim şifreleri zarfını şahsen teslim alacaktır.
   f) İmza oluşturma aracını ve erişim şifrelerini, diğer kişilerin her türlü erişimine karşı koruyacak, hiçbir durumda diğer kişilere kullandırmayacak, fiziki zarara veya kaybetmeye karşı koruyacaktır.
   g) Sertifika başvurusu sırasında veya sertifikanın geçerlilik süresi boyunca, sertifika içeriğinde yer alacak veya almış olan bilgiler dışında, kişisel bilgilerinde meydana gelen değişiklikleri TÜRKTRUST'a mümkün olan en kısa sürede bildirecektir.
   h) Sertifikasının iptalini temin etmek üzere, sertifika başvurusu sırasında veya sertifikanın geçerlilik süresi boyunca, sertifika içeriğinde yer alacak veya almış olan kişisel bilgilerde meydana gelen değişiklikleri, mümkün olan en kısa sürede TÜRKTRUST'a bildirecektir.
   i) İmza oluşturma aracının veya erişim şifrelerinin diğer kişilerce kullanılma tehlikesinin ve/veya bu tehlikenin oluşmasına neden olabilecek şartların ortaya çıkması halinde, iptalini temin etmek üzere derhal TÜRKTRUST'a bilgi verecektir.
   j) Tarafınca oluşturulan elektronik imzaların doğrulanmasına imkan tanımak üzere, sertifikasının üçüncü taraflara ilanına rıza ..... (SERTİFİKA SAHİBİ el yazısıyla ***gösterir*** veya ***göstermez*** yazacaktır).

3. Genel Şartlar
   a) Nitelikli elektronik sertifikanın süresi, sertifika sahibinin tercihine göre, sertifikanın üretim tarihinden itibaren **1 (bir)**, **2 (iki)** veya **3 (üç)** yıldır.
   b) TÜRKTRUST, Mevzuat ve TÜRKTRUST düzenlemeleri uyarınca hizmet verir.
   c) TÜRKTRUST, sertifika sahibinin talebi veya Mevzuatın gerektirdiği haller uyarınca sertifikayı iptal edebilecektir.
   d) Sertifika başvurusu sırasında sertifika sahibinin beyan ettiği kişisel bilgilerde bir eksiğin veya hatalı bilginin olduğunun ortaya çıkması durumunda, TÜRKTRUST'ın sertifika başvurusunu reddetme, sertifika verilmiş ise sertifikayı askıya alma veya iptal etme hakkı saklıdır.
   e) Sertifika sahibi, sertifikasının yenilenmesi talebini ancak sertifika süresinin sona ermesinden önce yapabilecektir.
   f) TÜRKTRUST'ın, düzenlemelerinde, Mevzuat ve teknik gereklilikler uyarınca değişiklik yapma hakkı saklıdır.

4. Bu taahhütname, imza tarihinde yürürlüğe girer.

SERTİFİKA SAHİBİ (el yazısıyla, eksiksiz doldurulacaktır.)

T.C. Kimlik No	:
Adı Soyadı	:
Tarih	:
İmza	:

EK – 2

TÜRKTRUST NİTELİKLİ ELEKTRONİK SERTİFİKA HİZMETLERİ TAAHHÜTNAMESİ

1. Bu taahhütnamede geçen;

a) "Sertifika" deyimi; 5070 sayılı Elektronik İmza Kanununun 9. maddesinde tanımlanan nitelikli elektronik sertifikayı,
b) "Sertifika sahibi" deyimi; 5070 sayılı Elektronik İmza Kanununun 3. maddesinde tanımlanan sertifika sahibi gerçek kişiyi,
c) "TÜRKTRUST" deyimi; TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş.'yi,
d) "TÜRKTRUST düzenlemeleri" deyimi; nitelikli elektronik sertifikalar için TÜRKTRUST web sitesinde ilan edilen Sertifika İlkelerini, Sertifika Uygulama Esasları dokümanlarını ve müşteri kılavuzlarını,
e) "Mevzuat" deyimi; 5070 sayılı Elektronik İmza Kanununu, Bilgi Teknolojileri ve İletişim Kurumu tarafından yayımlanan "Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik", "Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ" ile "Sertifika Mali Sorumluluk Sigortası Yönetmeliği"ni,
f) "İmza oluşturma aracı" deyimi, 5070 sayılı Elektronik İmza Kanununun 6. maddesinde tanımlanan güvenli elektronik imza oluşturma aracını

ifade eder.

2. TÜRKTRUST,

a) Sertifika hizmetlerinde, mevzuatla belirlenen güvenli ürün ve sistemleri kullandığını, hizmeti güvenilir biçimde yürüttüğünü ve sertifikaların taklit ve tahrif edilmesini önlemekle ilgili her türlü tedbiri aldığını,
b) İmza oluşturma verisinin TÜRKTRUST tarafından veya sertifika talep eden kişi tarafından TÜRKTRUST'a ait yerlerde üretilmesi durumunda, bu işlemin gizliliğini sağladığını veya TÜRKTRUST'ın sağladığı araçlarla üretilmesi durumunda, bu işleyişin güvenliğini sağladığını; bu hallerde üretilen imza oluşturma verisinin bir kopyasını almadığını veya saklamadığını,
c) TÜRKTRUST düzenlemelerinin güncel sürümlerini sürekli ve kesintisiz bir biçimde web sitesinden yayımladığını,
d) İmza oluşturma aracını sağlaması durumunda, bu aracın Mevzuatla uyumlu olduğunu,
e) İmza oluşturma aracının tüm bileşenlerinin 2 (iki) yıl süreyle aracın imalatından kaynaklanacak kusurlara karşı garanti kapsamında olduğunu,
f) Sertifika sahibine elden teslim etmiş olduğu nitelikli elektronik sertifika için, geçerlilik süresi içinde sertifika iptal ve sertifika durum hizmetleri ile dizin hizmetlerini Mevzuatın öngördüğü biçimde erişime açık kanallar üzerinden kesintisiz bir biçimde verdiğini,
g) Kendisine web üzerinden kesintisiz olarak haftada 7 gün 24 saat ulaşan tüm sertifika iptal taleplerini, talebin uygun bulunması ve kimlik doğrulamanın çevrim içi olarak tamamlanmasının ardından anında sonuçlandırmayı; Çağrı Merkezi üzerinden telefonla gelen veya yazıyla kağıt ortamında alınan sertifika iptal taleplerini ise, mesai saatleri içinde derhal değerlendirmeye almayı ve gerekli işlemleri ivedilikle tamamlamayı,
h) Sertifikanın, sertifikada yer alan maddi sınır için, Mevzuatla belirlenen şartlarda mali sorumluluk sigortası kapsamında olduğunu,
i) Sertifika hizmetlerine ilişkin tüm kayıtları Mevzuatla belirlenen süreyle sakladığını,

kabul, beyan ve taahhüt eder.

3. TÜRKTRUST'ın, düzenlemelerinde, Mevzuat ve teknik gereklilikler uyarınca değişiklik yapma hakkı saklıdır.

4. Bu taahhütname, TÜRKTRUST'ın, müşterisi konumunda bulunan sertifika sahibine karşı yükümlülüklerini saymaktadır[1]. Taahhütname, sertifika sahibinin TÜRKTRUST'tan temin etmiş olduğu nitelikli elektronik sertifikanın geçerlilik süresi başlangıcından itibaren yürürlüğe girer.

TÜRKTRUST A.Ş.

İşbu taahhütnamenin bir örneğine www.turktrust.com.tr adresli TÜRKTRUST web sitesinden erişilebilir.