SERTİFİKA UYGULAMA ESASLARI (SUE)

(DV SSL, OV SSL, NİMS ve benzeri elektronik sertifikalar)

SÜRÜM : 12

TARİH : 29.03.2017

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)" gereği Bilgi Teknolojileri ve İletişim Kurumu tarafından yayımlanmış olan Yönetmelik ve Tebliğ ile uluslararası standartlar uyarınca, elektronik sertifika hizmet sağlayıcılığı alanında faaliyet göstermektedir.

Sertifika Uygulama Esasları (SUE) olarak adlandırılan bu kitapçık, TÜRKTRUST'ın nitelikli elektronik sertifika hariç olmak üzere diğer elektronik sertifika hizmet sağlayıcılığı alanındaki faaliyetlerini nasıl yürüttüğünü göstermek amacıyla, "IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" rehber kitapçığına uygun olarak TÜRKTRUST tarafından hazırlanmıştır.

SSL (Secure Socket Layer) Sertifikası hizmeti için TÜRKTRUST, "ETSI TS 102 042 Electronic Signatures Infrastructure (ESI); Policy Requirements for Certification Authorities Issuing Public Key Certificates" standardının güncel sürümüne uyar. TÜRKTRUST ayrıca, SSL sertifikaları için, ETSI TS 102 042 standardında referans verilen ve http://www.cabforum.org adresinde yayımlanan "CA/Browser Forum Baseline Requirements (BR) for the Issuance and Management of Publicly-Trusted Certificates" dokümanına uyum sağlar. Sertifika Uygulama Esasları (SUE) kitapçığı ile bu dokümanlar arasında herhangi bir uyuşmazlık olması durumunda ilgili dokümanlardaki gereklilikler geçerli olacaktır. İlgili dokümanlara uyum, ETSI TS 102 042 standardında yer alan "Publicly-Trusted Certificate Policy - Baseline Requirements – BR Gerekliliklerini Kapsayan Kamuoyunca Güvenilen Sertifika İlkesi"ni (PTC-BR) kapsamaktadır.

SUE dokümanı, sertifika başvurularının alınması, sertifika üretimi ve yönetimi, sertifika yenileme ve sertifika 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 sertifikalar hariç diğer 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 ETSI TS 102 042 Electronic Signatures Infrastructure (ESI); Policy Requirements for Certification Authorities Issuing Public Key Certificates standardı, ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi ile 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) (DV SSL, OV SSL, NİMS ve benzeri elektronik sertifikalar)"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 numaraları (OID) aşağıda verilen sertifika ilkelerinin uygulama esaslarını kapsar:

- TÜRKTRUST OV SSL Sertifikası İlkeleri (2.16.792.3.0.3.1.1.2): Sunuculara yönelik OV SSL sertifikalarını kapsar. OV SSL Sertifikaları, ETSI TS 102 042 standardında tanımlanan "Normalized Certificate Policy – Standartlaştırılmış Sertifika İlkeleri" uyarınca üretilir ve idame ettirilir.
- TÜRKTRUST NİMS İlkeleri (2.16.792.3.0.3.1.1.4): Nesne imzalama işlemlerine yönelik sertifikaları kapsar. NİMS Sertifikaları, ETSI TS 102 042 standardında tanımlanan "Normalized Certificate Policy – Standartlaştırılmış Sertifika İlkeleri" uyarınca üretilir ve idame ettirilir.
- TÜRKTRUST DV SSL Sertifikası İlkeleri (2.16.792.3.0.3.1.1.6): Sunuculara yönelik DV SSL sertifikalarını kapsar. DV SSL Sertifikaları, ETSI TS 102 042 standardında tanımlanan "Normalized Certificate Policy – Standartlaştırılmış Sertifika İlkeleri" uyarınca üretilir ve idame ettirilir.

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 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 olan alt kök sertifikalara sahip olan diğer sertifika üretim merkezleri tarafından son kullanıcı sertifikaları üretilir.

1.3.2. Sertifika Kayıt Merkezleri

Sertifika kayıt merkezi, ESHS'lerin sertifika başvuru, yenileme ve iptal gibi doğrudan son kullanıcılara yönelik hizmetlerini yürüten birimdir. Bu birim, prosedürler uyarınca müşteri kayıtlarını oluşturur, gerekli kimlik tanımlama ve doğrulama süreçlerini yürütür, ilgili sertifika taleplerini sertifika üretim merkezine yönlendirir.

Kayıt merkeziyle ilgili işlemler, TÜRKTRUST satış temsilcilerinden gelen sertifika başvuruları doğrultusunda TÜRKTRUST merkezinde yer alan kayıt birimince yürütülür. 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 elektronik sertifikalara bağlı imza oluşturma verileriyle imzalanmış belgeleri alan, ilgili sertifikalara güvenen taraflardır.

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

1.3.5. Diğer Katılımcılar

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

TÜRKTRUST, 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.

Sunucu sertifikaları (DV veyaOV), sertifika sahipleri tarafından sadece sertifikada yer alan sunucu için ve SSL işleminde kullanılır.

NİMS, sertifikada yer alan kişi tarafından veya onun uhdesinde geliştirilen yazılım kodu için kullanılır.

1.4.2. Yasaklanmış Sertifika Kullanım Şekilleri

TÜRKTRUST sertifikalarının, sertifika sahiplerinin uhdesi dışında kullanılması yasaktır. Sertifikalar, işbu SUE dokümanında belirtilen amaçlar ve sınırlar 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

TÜRKTRUST'ın bu SUE dokümanı, TÜRKTRUST Sİ dokümanına uygun olarak hazırlanmıştır. 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.

TÜRKTRUST OV SSL sertifikaları için, ETSI TS 102 042 standardında referans verilen ve http://www.cabforum.org adresinde yayımlanan "CA/Browser Forum Baseline Requirements (BR) for the Issuance and Management of Publicly-Trusted Certificates" dokümanına uyum sağlar. Bu rehber doküman ve işbu SUE dokümanı arasında bir tutarsızlık olması durumunda belirtilen rehber doküman esas alınır.

1.6. Kısaltmalar ve Tanımlar

1.6.1. Kısaltmalar

BR : CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates – CA/Browser Forum Temel Gereklilikler dokümanı

CSR : Certificate Signing Request – Sertifika İmzalama Talebi

DN : Distinguished Name – Ayırt Edici İsim

DNS : Domain Name System – Alan Adı Sistemi

DV : Domain Validation – Alan Adı Doğrulamalı ı

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

NİMS : Nesne İmzalama Sertifikası

OID : Object Identifier – Nesne Tanımlayıcı Numarası

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

OV : Organization Validation – Kurumsal Doğrulamalı

PKI : Public Key Infrastructure – Açık Anahtarlı Altyapı

PTC-BR: Publicly-Trusted Certificate - Baseline Requirements – BR gerekliliklerini kapsayan ve kamuoyunca güvenilen sertifikalar

RFC : IETF tarafından yayımlanan, kılavuz niteliğinde yorum talebi dokümanları

SAN : Subject Alternative Name – Özne Alternatif Adı

Sİ : Sertifika İlkeleri

SİL : Sertifika İptal Listesi

SSL : Secure Sockets Layer

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; 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.

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

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

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

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

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

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

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

Dizin: Geçerli sertifikaları içinde bulunduran elektronik depodur.

DV SSL: ETSI TS 102 042 standardında tanımlanan "Domain Validation Certificate Policy – Alan Adı Doğrulamalı Sertifika İlkeleri" uyarınca üretilen ve idame edilen SSL sertifikasıdır.

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

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

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

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

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

İmzalı Sertifika Talebi (CSR): Talep sahibi tarafından üretilen ve sahip olduğu gizli anahtarla imzaladığı sertifika talebidir. Genellikle PKCS#10 formatında üretilir.

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.

Kamuoyunca Güvenilen Sertifika: Karşılık gelen kök sertifikanın, güvenilir bir referans noktası olarak yaygın kullanılan yazılım uygulamalarında dağıtılması uyarınca güvenilen sertifikadır (Publicly-Trusted Certificate – PTC)

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.

Nesne İmzalama Sertifikası (NİMS): Bilgisayarda çalıştırılabilen bir yazılım kodunun kaynak sahibini doğrulayan sertifikadır.

OV SSL: ETSI TS 102 042 standardında tanımlanan "Organization Validation Certificate Policy – Kurumsal Doğrulamalı Sertifika İlkeleri" uyarınca üretilen ve idame edilen SSL sertifikasıdır.

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, 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 talepleri doğrultusunda sertifika üretimi yapan, sertifika iptal işlemlerini gerçekleştirilen, sertifika kayıtları ile sertifika iptal durum kayıtlarını yaratan, işleten ve yayımlayan birimdir.

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

SSL (Secure Sockets Layer): İnternet haberleşmesinde veri gizliliğinin sağlanması, veriyi sunan sunucu kaynağının doğrulanması ve opsiyonel olarak veriyi alan istemcinin doğrulanması amacıyla geliştirilmiş güvenlik protokolüdür.

SSL Sertifikası: Veriyi sunan sunucu kaynağının kimliğini doğrulayan sertifikadır.

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

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 ve 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. 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 veya anlaşmaları, 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.

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.

Sertifika ve çevrim içi sertifika durum sorgulama kayıtları sürekli yayımlanır. Son kullanıcı sertifika durumlarında hiçbir değişiklik olmasa bile SİL, 12 (oniki) saatte bir olmak üzere günde 2 (iki) kez ve 24 (yirmidört) saatlik geçerlilik süresiyle yayımlanır. Herhangi bir son kullanıcı sertifikasının iptal edilmesi halinde 10 (on) dakika içinde yeni bir SİL üretilir.

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 elektronik sertifika başvurusunda bulunan veya yeni bir sertifika edinmek isteyen kişilerin kimliklerini veya adına sertifika alınacak olan web, elektronik posta ve benzeri sunucuların elektronik adres bilgilerini, 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.

Sunucu sertifikalarında, TÜRKTRUST tarafından doğrulanmış sunucu ismi, NİMS'de resmi belgelere göre doğrulanmış gerçek veya tüzel kişi adı kullanılır. 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 elektronik sertifikalar, ayırt edici isim alanında yer alan bilgilerle sertifika sahiplerinin eşsiz biçimde belirlenmesine olanak tanır. Ayırt edici isim alanında benzersizliği sağlayan bilgiler burada açıklanmıştır.

3.1.5.1. DV SSL veOV SSL (Türkiye'de yerleşik ticari kişiler)

TÜRKTRUST sunucu sertifikalarında sertifika sahibinin eşsiz biçimde ayırt edilmesi amacıyla ayırt edici isim alanı aşağıda açıklandığı biçimde belirlenir.

TÜRKTRUST DV SSL sertifikalarında sadece alan adı doğrulaması yapılmakta, herhangi bir kurumsal doğrulama yapılmamaktadır. DV SSL sertifikalarının doğrulama seviyesi nedeniyle sertifika içeriğinde tüzel kişiliğe ait herhangi bir bilgi yer almaz, sadece alan adı bulunur.

Türkiye'de yerleşik sermaye şirketleri için DN alanı:

- "CN" alanında DNS'te sertifika sahibi tüzel kişi adına kayıtlı sunucu adı;
    - DV SSL ve OV SSL wildcard sertifikalarında bu alana "*.<alan adı>" yazılır. Bu alan "*.com" veya "*.com.tr" gibi ayırt edici olmayan adlar içermez.
    - DV SSL veya OV SSL sertifikalarında bu alana, IP adresi veya iç sunucu adı yazılmaz.
- "O" alanında, sertifika sahibi tüzel kişinin Türkiye Ticaret Sicili'nde kayıtlı açık ticari unvanı veya ticaret unvanının anlaşılır şekilde kısaltılmış biçimi.
- "OU" alanında organizasyon birimi ya da marka adının bulunması halinde, Türk Standartları Enstitüsü'nde kayıtlı marka adı.

- "L" alanında, sertifika sahibi tüzel kişinin Türkiye Ticaret Sicili'nde kayıtlı açık ticari adresinde yer alan il.
- "C" alanında, başvuru sahibi tüzel kişinin ticari faaliyetinin bulunduğu ülkenin ISO 3166-1 Alpha-2 standardında yer alan ülke kodu (TR).
- "SAN" alanında, CN alanında bulunan DNS'te sertifika sahibi tüzel kişi adına kayıtlı sunucu adı. Sunucu sertifikalarında her bir alan adının sertifika başvuru sahibi tüzel kişiye ait veya kontrolü altında olduğunun doğrulanması koşuluyla birden fazla alan adı da yazılabilir. CN alanı için geçerli olan tüm kısıtlar SAN alanı için de geçerlidir.

Türkiye'deki kamu kurumları için DN alanı:

- "CN" alanında DNS'te sertifika sahibi kamu kurumu veya kuruluşu adına kayıtlı sunucu adı.
    - DV SSL ve OV SSL wildcard sertifikalarında bu alana "*.<alan adı>" yazılır. Bu alan "*.com" veya "*.com.tr" gibi ayırt edici olmayan adlar içermez.
    - DV SSL veya OV SSL sertifikalarında bu alana, IP adresi veya iç sunucu adı yazılmaz.
- "O" alanında, sertifika sahibi kamu kurumu veya kuruluşunun teşkilat kanununda veya diğer mevzuatta yer alan açık unvanı veya anlaşılır şekilde kısaltılmış biçimi.
- "OU" alanında organizasyon birimi ya da marka adının bulunması halinde, Türk Standartları Enstitüsü'nde kayıtlı marka adı.
- "L" alanında, sertifika sahibi kamu kurumu veya kuruluşun bulunduğu il.
- "C" alanında, başvuru sahibi kamu kurum ve kuruluşunun bulunduğu ülkenin ISO 3166-1 Alpha-2 standardında yer alan ülke kodu (TR).
- "SAN" alanında, CN alanında bulunan DNS'te sertifika sahibi kamu kurum veya kuruluşu adına kayıtlı sunucu adı. Sunucu sertifikalarında her bir alan adının sertifika başvuru sahibi tüzel kişiye ait veya kontrolü altında olduğunun doğrulanması koşuluyla birden fazla alan adı da yazılabilir. CN alanı için geçerli olan tüm kısıtlar SAN alanı için de geçerlidir.

Türkiye'de yerleşik dernek, vakıf, oda veya birlikler için DN alanı:

- "CN" alanında DNS'te sertifika sahibi dernek, vakıf, oda veya birliğin adına kayıtlı sunucu adı
    - DV SSL ve OV SSL wildcard sertifikalarında bu alana "*.<alan adı>" yazılır. Bu alan "*.com" veya "*.com.tr" gibi ayırt edici olmayan adlar içermez.
    - DV SSL veya OV SSL sertifikalarında bu alana, IP adresi veya iç sunucu adı yazılmaz.
- "O" alanında, sertifika sahibinin resmi makamlar nezdinde tutulan kayıtlara göre yer alan açık unvanı veya anlaşılır şekilde kısaltılmış biçimi.
- "OU" alanında organizasyon birimi ya da marka adının bulunması halinde, Türk Standartları Enstitüsü'nde kayıtlı marka adı.

- "L" alanında, sertifika sahibi dernek, vakıf, oda veya birliğin bulunduğu il.
- "C" alanında, başvuru sahibi dernek, vakıf, oda veya birliğin bulunduğu ülkenin ISO 3166-1 Alpha-2 standardında yer alan ülke kodu (TR).
- "SAN" alanında, CN alanında bulunan DNS'te sertifika sahibi dernek, vakıf, oda veya birliğin adına kayıtlı sunucu adı. Sunucu sertifikalarında her bir alan adının sertifika başvuru sahibi tüzel kişiye ait veya kontrolü altında olduğunun doğrulanması koşuluyla birden fazla alan adı da yazılabilir. CN alanı için geçerli olan tüm kısıtlar SAN alanı için de geçerlidir.

Türkiye'de yerleşik şahıs şirketi veya adi ortaklıklar için DN alanı:

- "CN" alanında DNS'te sertifika sahibi şahıs şirketi veya adi ortaklık adına kayıtlı sunucu adı
  - DV SSL ve OV SSL wildcard sertifikalarında bu alana "*.<alan adı>" yazılır. Bu alan "*.com" veya "*.com.tr" gibi ayırt edici olmayan adlar içermez.
  - DV SSL veya OV SSL sertifikalarında bu alana, IP adresi veya iç sunucu adı yazılmaz.
- "O" alanında, sertifika sahibinin güncel vergi tahakkuk belgelerindeki açık unvanı veya anlaşılır şekilde kısaltılmış biçimi.
- "OU" alanında organizasyon birimi ya da marka adının bulunması halinde, Türk Standartları Enstitüsü'nde kayıtlı marka adı.
- "L" alanında, sertifika sahibi tüzel kişinin Türkiye Ticaret Sicili'nde kayıtlı olduğu il.
- "C" alanında, başvuru sahibi tüzel kişinin merkezinin bulunduğu ülkenin ISO 3166-1 Alpha-2 standardında yer alan ülke kodu (TR).
- "SAN" alanında, CN alanında bulunan DNS'te sertifika sahibi şahıs şirketi veya adi ortaklık adına kayıtlı sunucu adı. Sunucu sertifikalarında her bir alan adının sertifika başvuru sahibi tüzel kişiye ait veya kontrolü altında olduğunun doğrulanması koşuluyla birden fazla alan adı da yazılabilir. CN alanı için geçerli olan tüm kısıtlar SAN alanı için de geçerlidir.

3.1.5.2. DV SSL ve OV SSL (Türkiye'de yerleşik olmayan ticari kişiler)

Sunucu sertifikalarında, ayırt edici isim alanında Türkiye'de yerleşik olan kişiler için aranan şartlar, ilgili yerel mevzuata göre muadil resmi dayanak belgeleri istenerek uygulanır.

3.1.5.3. NİMS

TÜRKTRUST NİMS sertifikaları için ayırt edici isim alanı aşağıdaki şekilde oluşturulur:

- "CN" alanında sertifika sahibi kişinin bulunduğu ülkedeki mevzuata göre belgelendirilebilen açık unvanı.

3.1.6. Ticari Markaların Tanınması, Doğrulanması ve Rolü

Sertifika sahipleri, sertifika başvurularında ticari marka isimlerinin doğru biçimde yer almasından sorumludur. Bu bağlamda, sertifika sahipleri diğer kişilere ait fikri mülkiyet veya isim haklarının her türlü ihlalinden sorumlu olurlar.

TÜRKTRUST, OV SSL sertifika başvurularında yer alan ticari marka isimlerini kontrol eder. Alan adında ".tr" ülke kodu olduğunda, nic.tr doğrulaması yapılır. Bu durumda marka

tescil doğrulamasına gerek kalmaz. Alan adında Türkiye dışında ülke kodu bulunan başvurular için ilgili ülke mevzuatına göre hareket edilir.

Ülke koduna sahip olmayan OV SSL sertifika başvuruları ile NİMS başvurularında ise başvurunun yurt içinden yapılması durumunda marka tescil belgesi, yurt dışından yapılması halinde ise o ülke kanunları kapsamında marka tescil belgesine denk olan belgenin gönderilmesini ister.

Bununla birlikte TÜRKTRUST, sertifika başvurusunda ticari marka isimlerinin kullanımına ilişkin bir ihlali tespit ederse başvuruyu reddetme veya sertifikayı iptal etme hakkını saklı tutar.

3.2. İlk Kimlik Doğrulama

3.2.1. Gizli Anahtara Sahip Olunduğunun Kanıtlanma Yöntemi

Sertifika başvuru sahipleri, gizli anahtara sahipliklerini PKCS#10 veya eş değeri bir dosyayı TÜRKTRUST'a ibraz ederek gösterirler. Gizli anahtarın TÜRKTRUST tarafından sertifika başvuru sahibi adına üretildiği durumlarda bu şart aranmaz.

3.2.2. Tüzel Kişiliğin Doğrulanması

Bir sertifikada bir tüzel kişiliğin isminin veya unvanının yer alması halinde, sertifika sahibinin bulunduğu ülkedeki yasal belgelere bağlı olarak doğrulanır. Burada yapılan doğrulama işlemi TÜRKTRUST prosedürlerinde belirlendiği gibi yürütülür. Sertifika türüne göre aşağıdaki doğrulama yöntemleri uygulanır.

3.2.2.1. DV SSL, OV SSL ve NİMS

DV SSL sertifikaları için tüzel kişilik doğrulaması yapılmaz.

OV SSL ve NİMS için sertifikada yer alacak tüzel kişiliğin ismi veya unvanı, sertifika sahibinin bulunduğu ülkedeki yasal belgelere bağlı olarak doğrulanır. Burada yapılan doğrulama işlemi TÜRKTRUST prosedürlerinde belirlendiği gibi yürütülür.

OV SSL ve NİMS başvurularında, başvuruların yurt içinden ya da yurt dışından gelmesine göre farklı kontrol adımları uygulanır. Bu ayrımın belirlenmesinde başvuru sahibi olan tüzel kişinin ikametgâh adresi esas alınır. Başvuru sahibinin yasal varlığının ve kimlik bilgilerinin, alan adının, kurum/firma temsilcisinin ve başvurunun varlığının, CSR bilgilerinin ve benzeri diğer bilgilerin doğrulanması gerekir. Bu doğrulama işlemi, yetkili kişinin e-posta adresine gönderilen eşsiz kullanıcı adı ve erişim kodu ile sağlanır.

3.2.3. Doğrulama Yapılmaksızın Sertifikada Yer Alabilen Bilgiler

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

3.2.4. Yetkinin Doğrulanması

OV SSL sertifika başvuruları ile sertifika sahibinin tüzel kişilik olduğu NİMS başvurularında, başvuruda bulunan kurum veya firma temsilcisi ile başvurunun varlığı, TÜRKTRUST prosedürlerinde belirtildiği üzere bağımsız bir kaynak aracılığıyla doğrulanır.

3.2.5. 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

Sunucu sertifikaları ve NİMS için sertifika ve anahtar yenileme yapılmaz.

3.3.2. İptal Sonrası Anahtar Yenileme için Kimlik Doğrulama

Sunucu sertifikaları ve NİMS için anahtar yenileme yapılmaz ve ilk kez başvuru yapılıyormuş gibi sertifika başvuru prosedürleri uygulanır.

3.4. İptal Talebi için Kimlik Doğrulama

TÜRKTRUST sunucu sertifikaları ve NIMS için iptal taleplerini aşağıda açıklandığı gibi güvenilir yollarla alır ve kimlik doğrulaması yapar:

- Sertifika sahibi, iptal talebini TÜRKTRUST'a kurum yetkilisi imzalı faksla bildirir. Bu faksın ulaşmasının ardından kurum yetkilisine telefonla ulaşılarak iptal talebi doğrulanır ve sertifika iptal edilir.
- Sertifika sahibi, web üzerinden iptal başvurusunu tercih ederse, sunucu sorumlusu veya kurum/firma temsilcisi sertifika tipi, sertifika seri numarası gibi sertifika bilgilerini girerek web sitesinde interaktif işlemler alanına bağlanır. İkincil kimlik doğrulama aşamasını da geçildikten sonra sertifika iptal nedeni girer. Sistem üzerinden çevrim içi iptal işlemi 7 gün 24 saat ilkesine göre tamamlanır. İşlem sonrası iptal durumu yetkiliye e-postayla bildirilir.

4. SERTİFİKA YAŞAM DÖNGÜSÜ İŞLEVSEL GEREKLİLİKLERİ

TÜRKTRUST, sertifikalarını bu SUE dokümanında yer alan uygulama esasları uyarınca üretir ve yaşam döngüsünü yönetir. İzleyen bölümde, farklı sertifika çeşitleri için uygulanan esaslar açıklanmıştır.

4.1. Sertifika Başvurusu

4.1.1. Kimler Sertifika Başvurusunda Bulunabilir?

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

Sunucu sertifikaları ve NİMS için özel hukuk tüzel kişileri ile kamu kurum ve kuruluşları dâhil olmak üzere her tüzel kişi sertifika 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 başvurusunun dayanak belgelerine göre doğrulanması ve eksiksiz ve doğru biçimde kaydedilmesi.
- Anahtar üretimi: Açık ve gizli anahtar çifti sertifika başvuru sahibi veya TÜRKTRUST tarafından üretilir. Anahtar çiftinin sertifika başvuru sahibi tarafından üretilmesi durumunda, açık anahtarın belirlenen prosedür ve standartlara göre TÜRKTRUST'a elektronik ortamda gönderilmesi gerekir. Bu durumda TÜRKTRUST, sertifika başvuru sahibinin açık anahtara karşılık gelen gizli anahtara sahip olduğunu gösteren bu elektronik kaydı doğrular.

4.2. Sertifika Başvurusunun İşlenmesi

4.2.1. Kimlik Doğrulama İşlemlerinin Yerine Getirilmesi

Sunucu sertifikası ve NİMS için başvurular Bölüm 3.2'de açıklanan esaslar ve buna bağlı TÜRKTRUST prosedürleri uyarınca yürütülür.

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 form ve belgelerin eksiksiz olarak tamamlanmış 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 form ve belgelerin tamamlanmaması.
- Bilgi ve belgelerin doğrulanmasına ilişkin sorgulamalara başvuru sahibinin zamanında veya tatminkâr yanıt vermemesi.
- OV SSL ve NİMS için, başvuru sahibi sermaye şirketi, şahıs şirketi veya adi ortaklık ise firmanın ticaret sicil kaydı olmaması, eğer başvuru sahibi resmi bir kurum ise kurumun herhangi bir resmi kaydı olmaması.
- OV SSL ve NİMS için, başvuru kaydından sonra CSR dosyasının en geç 30 (otuz) gün içinde TÜRKTRUST'a ulaşmaması.

- Sunucu sertifikası veya NİMS için yapılan bir başvuruda sertifika üretilmesinin, TÜRKTRUST'ın itibarını zedeleyebileceğine ilişkin kuvvetli bir kanaatinin oluşması.
- Sunucu sertifikası veya NİMS için, kamu kurumlarından gelen başvurular hariç olmak üzere, ödemenin yapılmamış olması.

Sunucu sertifikası başvuruları sırasında CA/Browser Forum BR dokümanında tanımlanan "Certification Authority Authorization (CAA)" kayıtları TÜRKTRUST tarafından kontrol edilmemekte ve bu kayıtlar uyarınca herhangi bir işlem yapılmamaktadır.

4.2.3. Sertifika Başvurularının İşlenme Süresi

Sunucu sertifikası ve NİMS başvuruları TÜRKTRUST'a ulaştıktan sonraki en geç 5 (beş) 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 elektronik sertifika başvuruları TÜRKTRUST sertifika üretim merkezlerinde işlenir ve elektronik sertifikalar üretilir.

OV SSL sertifikaları ile NİMS üretimleri, üretimden sorumlu güvenilir rolde bulunan iki yetkilinin aynı anda sisteme bağlanması ve üretim onayını vermesiyle gerçekleştirilir.

4.3.2. Sertifika Üretimiyle İlgili Sertifika Sahibinin Bilgilendirilmesi

Elektronik 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, tüm sertifika tipleri için elektronik 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.

4.4.2. ESHS Tarafından Sertifikanın Yayımlanması

Sertifikalar, sertifika sahiplerinin yazılı rızası olması kaydıyla web üzerinde veya dizin sunucularda yayımlanır.

TÜRKTRUST üçüncü tarafların sertifikalarını test edebilmeleri için üretmiş olduğu DV SSL ve OV SSL sertifikalarını imzalayan her alt kök sertifikası için iki adet test sertifikası üretir ve bunlardan birini iptal ederek bir test web sitesi üzerinden yayımlar.

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, tabi olunan standartlar 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.

4.5.2. Üçüncü Kişilerin İmza Doğrulama Verisi ve Sertifika Kullanımı

Üçüncü kişiler, güvenecekleri sertifikaların geçerliliğini kontrol etmekle ve sertifikaları tabi olunan standartlar 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, 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

Sunucu sertifikası ve NİMS için sertifika yenileme yapılmaz ve ilk kez başvuru yapılıyormuş gibi sertifika başvuru prosedürleri uygulanır. Bu başvuru sonucunda yeni bir anahtar çiftine sahip yeni bir sertifika üretilir.

4.7. Anahtar Yenileme

Sunucu sertifikası ve NİMS için anahtar yenileme yapılmaz ve ilk kez başvuru yapılıyormuş gibi sertifika başvuru prosedürleri uygulanır. Bu başvuru sonucunda yeni bir anahtar çiftine sahip yeni bir sertifika üretilir.

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. Sunucu sertifikası ve NİMS için iptal işlemi, talebin ulaşmasının ardından en geç 24 (yirmi dört) saat içinde gerçekleştirilir. Sunucu sertifikası ve NİMS için askıya alma işlemi uygulanmaz. 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,
- Sertifika içeriğinde yer alan özne veya sertifika sahibi bilgilerinde bir değişiklik olması,
- Sertifika sahibinin fiil ehliyetinin sınırlandığının, iflâsının veya gaipliğinin veya ölümünün öğrenilmesi,
- OV SSL sertifikaları için, sertifika sahibi tüzel kişinin yasal varlığının veya faaliyetinin devamının ortadan kalktığına dair TÜRKTRUST'a bir bildirimde bulunulması veya böyle olduğunun anlaşılması,
- Sertifikanın amacı dışında kullanıldığına dair bir kanıtın elde edilmesi halinde,
- Bir Wildcard sertifikasının sahtecilikle yanlış yönlendirebilecek bir tam nitelikli alt alan adını doğruladığının anlaşılması halinde,
- Sunucu sertifikasının oltalama, sahtecilik, zararlı yazılım dağıtma gibi suç unsuru oluşturan eylemlerde kullanıldığının tespit edilmesi halinde,

- 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,
- Sunucu sertifikaları için, bir mahkemenin veya bir yetkilinin sertifika sahibinin alan adı sahipliğini veya kullanma yetkisini ortadan kaldırdığına dair TÜRKTRUST'a bir bildirimde bulunulması veya bunun TÜRKTRUST tarafından anlaşılması,
- TÜRKTRUST'ın tamamen kendi takdiri sonucu, sertifikanın verilişi sırasında işbu SUE rehber kitapçıklarının uygulama esaslarına ilişkin bir uygunsuzluk tespit etmesi,
- Sunucu sertifikaları için, TÜRKTRUST'ın sertifika verme hakkının ortadan kalkması,
- TÜRKTRUST kök veya alt kök sertifikalarına ait gizli anahtarların açığa çıkma şüphesinin oluşması veya açığa çıkması,
- Sunucu sertifikalarının üretiminde kullanılan anahtar uzunluğunun veya kriptografik algoritmaların uygunluğunun ortadan kalkması,
- 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 ve BR 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,
- TÜRKTRUST'ın, sunucu sertifikalarının üretiminde kullanılan anahtar uzunluğunun veya kriptografik algoritmaların uygunluğunun ortadan kalkması.

4.9.2. Sertifika İptal Talebinde Bulunabilecek Kişiler

Aşağıda belirtilen kişiler sertifika iptal talebinde bulunabilir:

- NİMS için, sertifika sahibi ile sertifikada kurum bilgisinin yer alması halinde ilgili kurumu temsile yetkili kişi,
- DV SSL için sertifika sahibi tüzel kişiliğin sisteme kayıtlı sunucu sorumlusu veya temsile yetkili kişileri,
- OV SSL ve NİMS için sertifika sahibi tüzel kişiliği temsile yetkili kişi,
- TÜRKTRUST yetkilileri.

4.9.3. Sertifika İptal Talebi Prosedürleri

Sunucu sertifikası ve NİMS için sertifika iptal talepleri sertifika sahibi tüzel kişiliği temsile yetkili kişi imzasıyla yazılı olarak veya 7 gün 24 saat ilkesine göre TÜRKTRUST web sitesi üzerinden alınır.

Sunucu sertifikası ve NİMS için gelen yazılı sertifika iptal talebi doğrulandıktan sonra iptal işlemi tamamlanır. İşlem sonrası iptal durumu yetkiliye veya kurum/firma temsilcisine e-postayla bildirilir.

Sunucu sertifikası ve NİMS için sertifika sahibi, web üzerinden iptal başvurusunu tercih ederse, sunucu sorumlusu veya kurum/firma temsilcisi sertifika tipi, sertifika seri numarası gibi sertifika bilgilerini girerek web sitesinde interaktif işlemler alanına bağlanır. İkincil kimlik doğrulama aşaması da geçildikten sonra sertifika iptal nedeni girilerek çevrim içi iptal işlemi 7 gün 24 saat ilkesine göre tamamlanır. İşlem sonrası iptal durumu yetkiliye veya kurum/firma temsilcisine e-postayla bildirilir.

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, veri tabanında OCSP ve SİL hizmetlerinde anlık güncellemeye yol açar.

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 sitesi 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 sonuçlandırır. Yazıyla kâğıt ortamında alınan sertifika iptal talepleri ise mesai saatleri içinde derhal değerlendirmeye alınır ve gerekli işlemler en geç 24 (yirmi dört) saat içinde gerçekleştirilir.

4.9.6. Üçüncü kişilerin İptal Kontrol Gerekliliği

Üçüncü kişiler, kendilerine gönderilen bir elektronik sertifikaya 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.

4.9.7. Sertifika İptal Listesi (SİL) Yayımlama Sıklığı

TÜRKTRUST, herhangi bir son kullanıcı sertifikasının iptal edilmesi halinde OCSP ve SİL servislerinin tutarlı olması amacıyla 10 (on) dakika içinde yeni bir SİL üretir. Ayrıca 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 imzalanırlar. 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

Sunucu sertifikası ve NİMS için askıya alma işlemi uygulanmaz. İkincil doğrulama adımları tamamlanarak sertifika iptal edilir.

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

4.9.14. Sertifika Askıya Alma Talebinde Bulunabilecek Kişiler

Uygulama dışıdır.

4.9.15. Sertifika Askıya Alma Talebi Prosedürü

Uygulama dışıdır.

4.9.16. Sertifikanın Askıda Kalma Süresinin Sınırları

Uygulama dışıdır.

4.10. Sertifika Durum Servisleri

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

4.10.1. İşlevsel Özellikler

TÜRKTRUST sertifika ve çevrim içi sertifika durum sorgulama kayıtları sürekli yayımlar. Son kullanıcı sertifika durumlarında hiçbir değişiklik olmasa bile SİL, 12 (oniki) saatte bir olmak üzere günde 2 (iki) kez ve 24 (yirmidört) saatlik geçerlilik süresiyle yayımlar. Herhangi bir son kullanıcı sertifikasının iptal edilmesi halinde OCSP ve SİL servislerinin tutarlı olması amacıyla 10 (on) dakika içinde yeni bir SİL üretir. 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 haftada 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, TUÜRKTRUST FKM, olayın ardından en geç 2 saat içinde sertifika hizmetlerinin yönetimini devreye alır.

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. Ayrıca bakım ve destek faaliyetleri, toplantılar ve benzeri nedenlerle binada bulunan ziyaretçiler bina içinde yalnız bırakılmaz, yetkili bir TÜRKTRUST personeli tarafından refakat edilir.

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 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, binanın belirlenmiş bazı alanları dışında kalan tüm alanlarda sigara 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 ya fiziksel olarak imha edilir ya da üretici firma talimatları doğrultusunda sıfırlanır.

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 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.
- **Kayıt ve 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.

Güvenilir rollerde görev alacak personelin ataması TÜRKTRUST üst yönetimi tarafından ilgili prosedürlere göre yapılır.

Üst yönetim, üst düzey yöneticiler ve güvenilir rollerdeki tüm personel, TÜRKTRUST'ın sağladığı hizmetlerdeki güveni ve tarafsızlığı zedeleyecek veya çıkar çatışmasına neden olabilecek herhangi bir ticari veya finansal faaliyette bulunmaz.

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. Kriptografik modül kullanımı gerektiren sertifika ve SİL üretimi işlemleri, en az iki yetkilinin hazır bulunmasıyla sonuçlandırılabilmektedir.

Yukarıda belirtilen rutin sertifika üretim adımları dışında, TÜRKTRUST kök ve alt kök sertifikalarıyla ilgili her türlü üretim, yenileme, iptal, imha ve yedekleme işlemi 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 "Kayıt ve Müşteri Hizmetleri Yetkilisi" 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 deneyimli ve 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, 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 tesis içi ve tesis dışı yedekleri alınır.

5.4.6. Denetim Bilgisi Toplama Sistemi (İç ve Dış)

Denetim kayıtları, ESHS iş süreçlerinin yürütülmesinde kullanılan ESHS yönetim yazılımı tarafından tutulur. Denetim kayıtlarının oluşturulması yazılımın çalıştırılmasıyla başlar ve sadece yazılımın kapatılmasıyla sona erer.

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

Sunucu sertifikaları ve NİMS'lere ilişkin arşivler TÜRKTRUST tarafından 20 (yirmi) yıl süreyle korunur.

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, 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 afet yönetim prosedürleri ve 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, başvuru kaydı, askıya alma, iptal ve benzeri diğer sertifika hizmetleri, veri kaybına veya iş kesintisine yol açmadan 7x24 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.

Ayrıca yıllık olarak yapılan kapasite planlamaları ilgili teknik personel tarafından gerçekleştirilir ve üst yönetime sunulur. Bu kapasite planlaması çerçevesinde ESHS faaliyetlerinde değişen talepler hizmet kesintisine uğramadan karşılanır. Diğer taraftan bu kapasite talepleri, üst yönetim ve ilgili birim amirleri tarafından izlenir. Bütçeleme faaliyetlerinde ve finansal yönetimde gelecekteki kapasite ihtiyaç tahminleri, uygun işleme gücünü ve depolamayı elverişli kılmak üzere yapılır.

5.8. TÜRKTRUST'ın Faaliyetinin Son Bulması

TÜRKTRUST'ın faaliyetlerinin son bulması halinde, Kanun ve Yönetmelik gereği bu durumu en az 3 ay önce Kuruma bildirir ve kamuoyuna duyurur. TÜRKTRUST, işletmenin durdurulması prosedürü uyarınca, mevcut sertifikalarla ilgili tüm bilgi, belge ve kayıtları, Kanun gereği bir ay içinde başka bir ESHS'ye devreder. Kurum, uygun görmesi halinde, bir ayı geçmemek üzere ek süre verebilir. Eğer devir işlemi belirtilen süreler içinde tamamlanamazsa, 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.

Sunucu sertifikası ve NİMS sahipleri de yukarıda kamuoyuna yapılan duyuruyla ve e-postayla faaliyetin son bulmasından haberdar olmuş olurlar. Bu kapsamda geçerlilik süresi içinde olan sertifikaların, bunlara ilişkin TÜRKTRUST yükümlülüklerinin ve geçerli sertifikaların durum bilgilerinin yayımlanmasının devam edilmesine ilişkin hususlar yapılacak devirde düzenlenir.

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, 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. İki yetkilinin hazır bulunmasıyla ilgili kontroller, şifre kontrolleri ve biyometrik yöntemlerle sağlanır. Sistem, sadece her iki yetkilinin de, şifrelerini ve biyometrik verilerini kullanarak sırayla sisteme giriş yapmasıyla çalışır hale gelir.

TÜRKTRUST DV SSL ve OV SSL kök ve alt kök sertifikalarına ait anahtar çiftlerinin üretimleri sırasında ETSI TS 102 042 ve Baseline Requirements dokümanlarının gereklilikleri yerine getirilir. Bu gerekliliklerin belirttiği şekilde kök sertifikalara ait anahtar çiftlerinin üretimi, nitelikli bir denetçinin sürece şahitlik etmesiyle ve/veya tüm sürecin kamera kaydına alınmasıyla gerçekleşir.

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.

Sunucu sertifikaları için başvuruda bulunan sunucu sorumluları veya kurum/firma temsilcileri ve NİMS başvurunda bulunan teknik yöneticiler, güvenli bir şekilde anahtar üretiminin yürütülmesinden sorumludur.

6.1.2. İmza Oluşturma Verisinin Sertifika Sahibine Ulaştırılması

Sunucu sertifikası ve NİMS başvurusunda bulunacak sertifika başvuru sahibi, sertifika başvurusu sırasında anahtar üretiminin güvenli yapılmasından sorumludur.

Sunucu sertifikası ve NİMS başvurusu sırasında alınan ve doğrulanan bilgiler kullanılarak üretim sonrası sertifika sahibine sertifika üretim bilgisi e-postayla bildirilir. Sertifika sahibinin başvuru sırasında CSR dosyasını göndermek için kullandığı alandan sertifika yükleme işlemi yapması sağlanır.

6.1.3. İmza Doğrulama Verisinin ESHS'ye Ulaştırılması

Anahtar üretiminin sertifika başvuru sahibi tarafından gerçekleştirildiği durumlarda, sertifika talebinin gizli anahtarla imzalanmış olması şarttır. Talep bilgisine üçüncü kişilerin

erişimini engellemek için, talebin güvenli elektronik haberleşme yoluyla TÜRKTRUST'a gönderilmesi sağlanır.

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 adresinde yayımlanır. Kök sertifikalara ait parmak izi 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 sertifika üretim merkezlerinin kök ve alt kök sertifikaları üretilirken 2048 bit RSA anahtar çiftleri kullanılır. Ayrıca üretilen tüm son kullanıcı sertifikaları için de 2048 bit RSA anahtar çifti kullanılır.

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

6.1.6. Anahtar Üretimi ve Kalite Kontrolü

Kök ve alt kök sertifikalara ait anahtar çifti uygun güvenlik düzeyine sahip donanım güvenlik modüllerinde, mevzuat veya standartlarda belirlenen parametrelere uygun olarak üretilir.

Anahtar üretiminin müşteri tarafında yapıldığı DV SSL, OV SSL, ve NİMS son kullanıcı sertifikalarında, imza oluşturma verisinin uygun araçlarda ve uygun nitelikte üretiminden müşteri sorumludur. Ancak bu durumda TÜRKTRUST, müşteri tarafından gönderilen CSR dosyasının geçerliliğini, dosyanın imzasının yanında, kullanılan anahtar uzunluğuna ve diğer parametrelere göre doğrular. CSR dosyalarının bilinen zayıf anahtarlardan biriyle oluşturulup oluşturulmadığı otomatik olarak kontrol edilir ve zayıf anahtar bulunması halinde başvuru reddedilir. Ayrıca başvuru sırasında verilen ve sisteme kaydedilen sertifika içerik bilgileri ile müşterinin gönderdiği CSR içinde bulunan bilgiler karşılaştırılır ve bir tutarsızlık olması halinde CSR reddedilir.

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, uluslararası 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.

6.2.2. İmza Oluşturma Verisinin Çok Kullanıcılı Kontrolü

TÜRKTRUST'a bağlı sertifika üretim merkezlerinin kök ve alt kök sertifikalarına 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.

6.2.3. İmza Oluşturma Verisinin Saklanması

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 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 üretiminin müşteri tarafında olduğu durumlarda, imza oluşturma verisinin kontrolü ve olası transferi sırasında güvenliğinin sağlanması müşterinin sorumluluğundadır.

6.2.7. İmza Oluşturma Verisinin Kriptografik Modülde Saklanması

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

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.

Sunucu sertifikaları ve NİMS için gizli anahtarın aktivasyonu sertifika sahibine ait yazılım veya donanım üzerinde yapılır.

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.

Sunucu sertifikaları ve NİMS için gizli anahtarın deaktive edilmesi sertifika sahibine ait yazılım veya donanım üzerinde yapılır.

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 iki kişinin aynı anda hazır bulunması gerekir.

Sunucu sertifikaları ve NİMS son kullanıcı sertifikalarına ait gizli anahtarların sertifika iptali ya da sertifika süresinin dolmasından sonra yok edilmesiyle ilgili bir koşul yoktur. Ancak, sertifika sahibinin gizli anahtarını yok etmesi tavsiye edilir.

6.2.11. Kriptografik Modül Değerlendirmesi

TÜRKTRUST sertifika üretim merkezlerinin kök ve alt kök sertifikalarına bağlı imza oluşturma verileri, kriptografik donanım modüllerinde üretilir ve 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 DV SSL ve OV SSL sertifikaları ile NİMS'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 sunucu sertifikası ve NİMS kök ve alt kök sertifikaların geçerlilik süreleri 30 (otuz) 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 iki yetkilinin aynı anda bulunmasıyla mümkündür. Erişim şifreleri, BR'a uyumlu olarak 12 (on iki) 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) veri tabanında tutulur.

Sunucu sertifikası ve NİMS sahipleri sertifikalarına ait anahtarlara erişim şifrelerini güvenli biçimde oluşturmaktan ve korumaktan sorumludur.

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

Uygulama dışıdır.

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. Veri tabanına yetkisiz erişimi ve istenmeden yapılan değişiklikleri önlemek için kimlik doğrulamanın farklı erişim seviyelerinde çeşitli fiziksel ve elektronik önlemler alınır. Veri tabanı seviyesindeki mantıksal

tutarlılık, aksi halde geri dönüşü olmayan sonuçlar doğurabilecek iptal durumu değişikliklerini önlemek için ilave bir güvenlik katmanı oluşturur.

- Bilgisayar sistemini oluşturan birimler arasındaki veri iletişimi güvenli olarak yapılmaktadır.
- İşlem kayıtları sürekli olarak tutulduğu için bilgisayar sistemlerinde oluşabilecek sorunlar kısa zamanda ve doğru biçimde belirlenebilmektedir.
- 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 ve 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. İlgili prosedürler uyarınca, bu ağ elemanları sürekli izlenmekte, iç veya dış noktalardan gelebilecek saldırılar ve yetkisiz erişimler tespit edilmekte ve diğer güvenlik kontrolleri aracılığıyla da saldırılar engellenmektedir. Ayrıca düzenli olarak yapılan zayıflık ve penetrasyon testleri sonucu bulunan zayıflıkların ve açıklıkların belli planlar çerçevesinde giderilmesi de sağlanmaktadır.

TÜRKTRUST ağına dışarıdan yapılabilecek her türlü erişim şifrelenmiş kanallar üzerinden sağlanmakta ve sadece sunulan hizmetlere erişime izin verilmektedir. Hassas bilgilerin bulunduğu sistemlere erişim ise sadece TÜRKTRUST merkezindeki yetkili ağlar üzerinden yapılabilmektedir.

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

TÜRKTRUST ağ güvenliği ile ilgili işlemlerini ETSI TS 102 042, Baseline Requirements ve Network and Certificate System Security Requirements dokümalarının gereksinimlerini yerine getirerek, İletişim ve İşletim Yönetimi Prosedürüne göre yürütür. Bu gereksinimler genel olarak aşağıdaki şekilde sıralanabilir;

- TÜRKTRUST ESHS sistemine doğrudan erişim yetkisi olan personelinin kullanıcı hesaplarının yönetimi, denetimi ve erişim haklarının düzenlenmesi veya kaldırılmasıyla ilgili yönetimini etkin bir şekilde düzenler.
- Sistemlere doğrudan erişimi bulunan güvenilir roldeki personelin (Sistem ve Ağ Yöneticisi gibi) yetki değişikliği olması durumunda, bu personelin yetki alanı içindeki tüm hesaplara ait şifreler değişir.
- Tüm kullanıcı hesapları periyodik olarak kontrol edilir ve işlemeyen hesapları kapatılır.
- Personelin işten ayrılması halinde sistem üzerindeki bütün hesapları kapatılır.
- Sistem ve Ağ Yöneticisi yapacağı değerlendirme sonrasında ağ güvenliği yazılım bileşenleri için yamanın veya güncellenmenin uygulanması, bekletilmesi veya hiç uygulanmaması yönünde karar verir.
- ESHS sistemleri için prosedürde belirlenen sayıda hatalı şifre girişi yapılması halinde kullanıcı hesabı kilitlenir.
- Sistem Denetçisi tarafından periyodik olarak sistem logları gözden geçirilir ve herhangi bir problem tespit edilmesi halinde derhal yönetime raporlanır.
- ESHS sistemleri en geç 3 (üç) ayda bir zayıflık testine ve en azından yılda 1 (bir) kez penetrasyon testine tabi tutulur. Bu testlerin sonuçları değerlendirilerek sistem üzerinde düzenlemeler yapılır.

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.

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

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

TÜRKTRUST tarafından oluşturulan DV SSL 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.
Key Usage (Anahtar Kullanımı)	Evet	Signing (imzalama), key encipherment (anahtar şifreleme), data encipherment (veri şifreleme) ve key agreement (anahtar anlaşması) alanları bulunmakta ve uzantı kritik olarak işaretlenmektedir.
Certificate Policies (Sertifika İlkeleri)	Hayır	• İlke Tanımlayıcı Numarası (Policy Identifier) olarak TÜRKTRUST DV

		SSL OID değeri: 2.16.792.3.0.3.1.1.6 • Sertifika Uygulama Esasları adresi (Policy Qualifier Info – CPS) olarak http://www.turktrust.com.tr/sue değeri Kullanılmaktadır.
Basic Constraints (Temel Kısıtlar)	Hayır	ESHS (CA) değeri "false" olarak işaretlenmektedir.
Subject Alternative Name (Özne Alternatif Adı)	Hayır	Özne sunucuya ait alternatif isimler kullanılabilmektedir.
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.
Extended Key Usage (Genişletilmiş Anahtar Kullanımı)	Hayır	Server authentication (sunucu doğrulama) ve client authentication (istemci doğrulama) değerleri bulunmaktadır.

TÜRKTRUST tarafından oluşturulan OV SSL 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.
Key Usage (Anahtar Kullanımı)	Evet	Signing (imzalama), key encipherment (anahtar şifreleme), data encipherment (veri şifreleme) ve key agreement (anahtar anlaşması) alanları bulunmakta ve uzantı kritik olarak işaretlenmektedir.
Certificate Policies (Sertifika İlkeleri)	Hayır	• İlke Tanımlayıcı Numarası (Policy Identifier) olarak TÜRKTRUST OV SSL OID değeri: 2.16.792.3.0.3.1.1.2

		• Sertifika Uygulama Esasları adresi (Policy Qualifier Info – CPS) olarak http://www.turktrust.com.tr/sue değeri Kullanılmaktadır.
Basic Constraints (Temel Kısıtlar)	Hayır	ESHS (CA) değeri "false" olarak işaretlenmektedir.
Subject Alternative Name (Özne Alternatif Adı)	Hayır	Özne sunucuya ait alternatif isimler kullanılabilmektedir.
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.
Extended Key Usage (Genişletilmiş Anahtar Kullanımı)	Hayır	Server authentication (sunucu doğrulama) ve client authentication (istemci doğrulama) değerleri bulunmaktadır.

TÜRKTRUST tarafından oluşturulan NİMS 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.
Key Usage (Anahtar Kullanımı)	Evet	Signing (imzalama), non-repudiation (inkar edilemezlik) alanları bulunmakta ve uzantı kritik olarak işaretlenmektedir.
Certificate Policies (Sertifika İlkeleri)	Hayır	• İlke Tanımlayıcı Numarası (Policy Identifier) olarak TÜRKTRUST NIMS OID değeri: 2.16.792.3.0.3.1.1.4 • Sertifika Uygulama Esasları adresi (Policy Qualifier Info – CPS) olarak http://www.turktrust.com.tr/sue değeri Kullanılmaktadır.

Basic Constraints (Temel Kısıtlar)	Hayır	ESHS (CA) değeri "false" olarak işaretlenmektedir.
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.
Extended Key Usage (Genişletilmiş Anahtar Kullanımı)	Hayır	Code signing (kod imzalama) ve commercial software publishing (ticari yazılım yayımlama) değerleri bulunmaktadır.

TÜRKTRUST tarafından oluşturulan ve sunucu sertifikaları ile NIMS sertifikalarının dahil 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.
Key Usage (Anahtar Kullanımı)	Hayır	Signing (imzalama) alanı bulunmaktadır.
Basic Constraints (Temel Kısıtlar)	Hayır	ESHS (CA) değeri "false" olarak işaretlenmektedir.
Extended Key Usage (Genişletilmiş Anahtar Kullanımı)	Hayır	OCSP signing (OCSP imzalama) değeri bulunmaktadır.
OCSP No Check	Hayır	OCSP hizmet sertifikasının kendi geçerlilik kontrolünün yapılmasına gerek olmadığını belirten uzantı.

7.1.3. Algoritma Nesne Tanımlayıcıları

TÜRKTRUST tarafından oluşturulan tüm sertifikaların imzalanmasında aşağıdaki algoritmalardan biri kullanılır.

Algoritma Adı	Nesne Tanımlayıcı Numarası
SHA-1 ile RSA	1.2.840.113549.1.1.5
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

Sunucu sertifikaları ve NIMS son kullanıcı sertifikalarının tamamı SHA-256 algoritmasıyla üretilmektedir. Bu sertifikaların üretiminde kullanılan kök sertifikalar halen SHA-1 veya SHA-256 olmakla birlikte, yeni üretilen tüm kök ve alt kök sertifikalarda SHA-256 kullanılmakta, SHA-1 ile yeni kök ve alt kök üretimi yapılmamaktadır.

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.

DV SSL sertifikalarında "Sertifika Sahibi" alt alanlarında aşağıdaki değerler bulunur:

"CN"	İşbu SUE dokümanının 3.1.5.2 ve 3.1.5.3 bölümlerinde açıklanan değerler.
"OU"	"Domain Validated (DV) – WindSSL (R)" ifadesi.

OV SSL sertifikalarında "Sertifika Sahibi" alt alanlarında aşağıdaki değerler bulunur:

"CN"	İşbu SUE dokümanının 3.1.5.2 ve 3.1.5.3 bölümlerinde açıklanan değerler.
"C"	Sertifika sahibinin ülke kodu.
"S"	Opsiyonel olarak sertifika sahibinin semt, il veya eyalet adı.
"L"	Sertifika sahibinin kayıtlı olduğu şehir.
"O"	İşbu SUE dokümanının 3.1.5.2 ve 3.1.5.3 bölümlerinde açıklanan değerler.
"OU"	Opsiyonel olarak sertifika sahibinin kurumsal birimi.

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

"CN"	Sertifika sahibi kişinin bulunduğu ülkedeki mevzuata göre belgelendirilebilen açık unvanı.
"C"	"TR" değeri.
"S"	Opsiyonel olarak sertifika sahibinin semt, il veya eyalet adı.
"L"	Sertifika sahibinin kayıtlı olduğu şehir.
"O"	Opsiyonel olarak sertifika sahibi tüzel kişinin bulunduğu ülkedeki mevzuata göre belgelendirilebilen açık unvanı.
"OU"	Opsiyonel olarak sertifika sahibinin kurumsal birimi.

7.1.5. İsim Kısıtları

TÜRKTRUST tarafından üretilen sertifikalarda anonim veya takma adlar kullanılmaz.

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.

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.

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, gerektiğinde RFC 6960 tarafından tanımlanan uzantılar kullanılabilir. Ancak, temel OCSP bilgileri dışındaki tüm uzantıların kullanılması zorunlu değildir.

8. UYGUNLUK DENETİMİ VE DİĞER DEĞERLENDİRMELER

TÜRKTRUST, ETSI TS 102 042 standardı kapsamında da yetkili bir denetçi kurum tarafından OV SSL denetime tabi tutulur.

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, ETSI TS 102 042 standardı ve 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

ETSI TS 102 042 denetim standardı kapsamında OV SSL hizmet süreçleri her yıl uygunluk denetimine tabi tutulur ve her üç yılda bir bu sertifikasyon yenilenir.

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

ETSI 102 042 denetimi, aşağıdaki hususlara sahip olan yetkin bir denetçi tarafından gerçekleştirilir:

- Açık anahtarlı altyapı (PKI) teknolojisi, bilgi güvenliği araçları ve teknikleri, bilgi teknolojileri ve güvenliği denetimi ve üçüncü parti bağımsız raporlamaları alanında yetkinliğine sahip olmalıdır.
- Denetçi, European Cooperation for Accreditation gibi resmi bir akreditasyon kuruluşu tarafından ISO/IEC 17021'e uyumlu olduğuna dair akredite edilmiş olmalıdır.
- Denetçi ayrıca, CEN Workshop Agreement (CWA) 14172-2 standardının 3.4 maddesi uyarınca da akredite edilmiş olmalıdır.

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

ETSI TS 102 042 denetimi, bağımsız ve yetkili bir denetçi tarafından yapılır.

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

ETSI TS 102 042 denetimi, OV SSL hizmetlerine ilişkin tüm süreçleri, bu hizmetlerin yerine getirilmesi sırasında kullanılan teknik altyapı ve hizmetlerin verildiği tesisleri içermektedir.

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, ETSI TS 102 042, ISO/IEC 27001 ve TS EN ISO 9001 kapsamında yer alan tüm konular ele alınır.

8.5. Eksiklik Durumunda Yapılacaklar

OV SSL süreçlerinin ETSI TS 102 042 standardına uyumu kapsamında gerçekleştirilen denetimlerde ortaya çıkan minör eksiklikler için TÜRKTRUST, düzeltici ve önleyici faaliyetleri belirler ve gerekli işlemleri yerine getirir. Eksiklerin majör nitelikte olması, geçerli olan yetkilendirme belgesinin geri alınmasına neden olur.

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 olur. Minör eksikler, bir sonraki denetim dönemine kadar TÜRKTRUST tarafından giderilir.

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

8.6. Sonuçların Bildirilmesi

Bağımsız denetim firması tarafından ETSI TS 102 042 uyarınca gerçekleştirilen OV SSL süreçleri denetim sonuçları resmi olarak TÜRKTRUST'a bildirilir.

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 sunucu sertifikaları ile NİMS, sertifika çeşidine, kullanım süresine ve özelliklerine bağlı olarak fiyatlandırılır. Ayrıca, sunucu sertifikası fiyatlandırmasında artan maddi işlem sınırı ve genel sorumluluk sigortası primleri de dikkate alınır.

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.

TÜRKTRUST'ın sunucu sertifikaları ile NİMS için verdiği iptal veya durum bilgisi erişim hizmetleri ücretsizdir.

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, sunucu sertifikası ve NİMS hizmetlerinde 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, sunucu sertifikası hizmetleri için ETSI TS 102 042 standardı uyarınca ticari genel sorumluluk sigortası yaptırmakla yükümlüdür.

9.2.1. Sigorta Kapsamı

Sunucu sertifikaları, aşağıda özellikleri belirtilen ticari genel sorumluluk sigortası kapsamındadır.

"Ticari Genel Sorumluluk Sigortası (Commercial General Liability Insurance)", sunucu sertifikasıyla ilgili hizmetlere doğrudan veya dolaylı bağlı olarak oluşabilecek her türlü zarara 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, sunucu sertifikaları için ETSI TS 102 042 standardı uyarınca ticari genel sorumluluk sigortasını yaptırmakla yükümlüdür.

9.3. İş Bilgisinin Gizliliği

9.3.1. Gizli Bilginin Kapsamı

TÜRKTRUST'ın 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, standartlar 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 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 SUE dokümanında ve sertifika sahibi taahhütnamesinde düzenlenmiş amaçlar için sertifikayı, mührü 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 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, veri tabanları, 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 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.

DV SSL ve OV SSL sertifikaları bağlamında, TÜRKTRUST aşağıdakileri garanti eder:

- ***Yasal Varlık:*** TÜRKTRUST, OV SSL sertifikasının üretildiği tarihte, OV SSL sertifikası içinde belirtilen Özne'nin yasal olarak var olduğunu ve geçerli bir organizasyon ya da varlık olduğunu doğrular. Bu doğrulama ülkenin nitelikli resmi bilgi kaynağı aracılığıyla yapılır. Türkiye için bu kaynak Ticaret Sicil Gazetesi, Resmi Gazete veya bağlı bulunduğu sicil kaydıdır.
- ***Kimlik:*** TÜRKTRUST, OV SSL sertifikasının üretildiği tarihte, OV SSL sertifikası içinde belirtilen Özne'nin yasal adının, resmi devlet kayıtlarındaki isimle uyuştuğunu teyit eder. Bu doğrulama, yasal varlığın doğrulanmasında kullanılan nitelikli resmi bilgi kaynağı kullanılarak yapılır.
- ***Alan Adı Kullanma Hakkı:*** TÜRKTRUST, sunucu sertifikasının üretildiği tarihte, sunucu sertifikası içinde belirtilen Özne'nin ve tüm alternatif özne adlarının, varlığını, münhasıran başvuru sahibi tarafından kullanma hakkına sahip olduğunu veya kontrolü altında olduğunu doğrular. OV SSL başvurularında bu doğrulama alan adı

üzerinde özel bir web sayfasının tanımlanması veya özel bir e-posta adresiyle iletişim kurulması yöntemlerinden biriyle yapılır. DV SSL sertifikalarında ise bu doğrulama adımı özel bir e-posta adresiyle iletişim kurulması yöntemiyle yapılır. Bu doğrulama OV SSL başvurularında ulusal ya da uluslararası alan adı kayıt kuruluşunun bilgileri kullanılarak da yapılabilir. Alan adının kullanım hakkının başka bir tüzel kişiliğe ait olması durumunda ise alan adı kontrolünün yetkilendirme veya anlaşmaya dayanılarak verildiğinin doğrulamasıyla tamamlanır.

- ***OV SSL Sertifikası için Yetkilendirme:*** TÜRKTRUST, OV SSL sertifikası içinde belirtilen Özne'nin, OV SSL sertifikasının üretimini yetkilendirdiğini doğrular. Bu yetki doğrulaması, resmi yetki belgesi üzerinden veya bağımsız bir kaynak aracılığıyla bulunan bilgilerin doğrulanması yöntemleriyle yapılır. Bağımsız bir kaynak aracılığıyla bulunan bilgiler telefonla doğrulanabildiği gibi gerekirse yüz yüze kimlik doğrulaması da yapılabilir.
- ***Bilginin Doğruluğu:*** TÜRKTRUST, sunucu sertifikasının üretildiği tarihte, sunucu sertifikası içinde yer alan diğer tüm bilgilerin doğru olduğunu teyit etmek için aşağıdaki adımları uygular.
    - ***Alan Adı (CN):*** Özel bir web sayfasının tanımlanması veya özel bir e-posta adresiyle iletişim kurulması yöntemlerinden biriyle yapılır. Ulusal ya da uluslararası alan adı kayıt kuruluşu bilgileri kullanılarak da alan adı doğrulaması yapılabilir. Alan adının kullanım hakkının başka bir tüzel kişiliğe ait olması durumunda ise alan adı kontrolünün yetkilendirme veya anlaşmaya dayanılarak verildiğinin doğrulamasıyla tamamlanır.
    - ***Şirket/Kurum Adı (O):*** Sertifika sahibinin resmi devlet kayıtlarındaki açık unvanıyla karşılaştırılarak doğrulanır.
    - ***Kurumsal Birim (OU):*** Bu alan opsiyoneldir. Organizasyon birimi başvuru formu üzerinden ve yetkili imzasıyla doğrulanır. Bu alanda marka adının bulunması halinde ya da şirket/kurum adının anlamlı kısaltması, adresi veya ili içeriyorsa resmi kayıtlar kullanılarak doğrulanır.
    - ***İl (L):*** Sertifika sahibinin resmi kayıtlardaki açık ticari adresinde yer alan il bilgisiyle karşılaştırılarak doğrulanır.
    - ***Semt (S):*** Bu alan opsiyoneldir ve herhangi bir bilgi bulunması halinde sertifika sahibinin resmi kayıtlardaki açık ticari adresinde yer alan semt, il veya eyalet bilgisiyle karşılaştırılarak doğrulanır.
    - ***Ülke Kodu (C):*** başvuru sahibinin faaliyette bulunduğu ülkenin ISO 3166-1 Alpha-2 standardında yer alan ülke koduyla karşılaştırılarak doğrulanır.
    - ***Özne Alternatif Adı (SAN):*** Alan adının doğrulanması sırasında kullanılan yöntemler geçerlidir. Sertifikada SAN alanında yer alacak her bir alan adı için bu doğrulama yapılır.
- ***Yanıltıcı Bilgi Olmaması:*** TÜRKTRUST, sunucu sertifikasının üretildiği tarihte, sunucu sertifikası içinde yer alan bilgilerde herhangi bir yanıltıcı bilgi bulunmaması için yukarıda açıklanan doğrulama adımlarını prosedür ve talimatlarında detaylı şekilde uygular.
- ***Taahhütname:*** Sunucu sertifikasında belirtilen Özne, TÜRKTRUST ile SUE'nin gerekliliklerini sağlayan, yasal olarak geçerli ve bağlayıcı bir taahhütname imzalamıştır veya başvuru sahibinin temsilcisi ilgili şartları onaylamış ve kabul etmiştir.

- ***Durum:*** TÜRKTRUST bu SUE dokümanının gerekliliklerini sağlar ve sunucu sertifikalarının durumuyla ilgili geçerli ya da iptal şeklinde güncel bilgileri içeren bir Bilgi Deposunu 24 x 7 olarak online erişime açık biçimde idame ettirecektir.
- ***İptal:*** TÜRKTRUST bu SUE dokümanının gerekliliklerini sağlar ve CA-Browser Forum kılavuzunda belirtilen iptal nedenleri gereği sunucu sertifikasının iptalini gerçekleştirir.

TÜRKTRUST, SSL sertifika sahiplerine sertifika başvurusu sırasında SSL Sertifika Sahibi Taahhütnamesini imzalatarak sertifika kullanımında uyulması gereken yükümlülükleri bildirir. TÜRKTRUST'a bağlı sertifika kayıt merkezi ve sertifika üretim merkezi, sunucu sertifikası ve NİMS hizmetlerini yürütebilmek için ETSI TS 102 042 standardında ve BR'da belirtilen yükümlülükleri yerine getirir.

TÜRKTRUST, Sertifika İlkeleri ve Sertifika Uygulama Esasları dokümanlarının yanı sıra SSL Sertifika Sahibi ve TÜRKTRUST SSL Sertifika Hizmetleri Taahhütnamelerini de www.turktrust.com.tr adresinde Bilgi Deposu alanından 7 gün 24 saat ilkesine uygun olarak yayımlar.

9.6.2. Kayıt Merkezi Sorumlulukları

TÜRKTRUST'a bağlı kayıt merkezi, kendisine 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

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.

9.6.4. Üçüncü Kişilerin Sorumlulukları

Sunucu sertifikası ve NİMS sahipleri ile üçüncü kişiler, TÜRKTRUST tarafından oluşturulmuş sertifikaların kabulü sırasında ve bu sertifikalara güvenirken sertifikaların içeriğini doğrulamaktan 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 elektronik sertifikalar, parasal işlemlerde maddi işlem sınırları dahilinde sigortalıdır. Sertifikalar ve bu sertifikaların kullanımıyla ilgili sorumluluk sınırları, sertifika sahibi taahhütnamesinde açıkça belirtilmiştir.

Sunucu sertifikaları ve NİMS'lerde genel sorumluluk sigortası 1.000.000 USD tutarında olay başına teminat limitini ve 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. TÜRKTRUST bu durum karşısında kusursuzluğunu ispat ettiği takdirde tazminat ödeme yükümlülüğü doğmaz.

Sertifika sahipleri, 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 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 veya SMS 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 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 sertifika sahipleri ile üçüncü kişiler ivedilikle bilgilendirilir.

Özellikle önemli değişikliklerde, sertifikanın kullanılabilirliği ve kabul edilirliği bazı uygulamalarda etkilenebileceğinden, TÜRKTRUST sertifika sahipleri ile üçüncü kişileri bilgilendirebilmek için tüm makul imkânları kullanır. Değişiklik TÜRKTRUST web sitesinde yayımlanır, sertifika sahiplerine e-posta veya SMS 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

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.

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

9.14. Yasal Düzenleme

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

9.15. İlgili Yasalara Uygunluk

TÜRKTRUST, nitelikli elektronik sertifika 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.