EİMZATR
NİTELİKLİ ELEKTRONİK SERTİFİKA İLKELERİ
(NESİ)

Sürüm 3.0

23.07.2026

Prof. Dr. Ahmet Taner Kışlalı Mah. 2778. Sokak No:3 Çayyolu / Ankara
+90 (312) 242 01 11 | bilgi@e-imzatr.com.tr | www.e-imzatr.com.tr

İÇİNDEKİLER

1. GİRİŞ

EİMZATR Bilgi Güvenliği Hizmetleri A.Ş (kısaca "E-İMZATR" 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 (kısaca "Kanun" olarak anılacaktır)" ve Bilgi Teknolojileri ve İletişim Kurumu tarafından yayımlanmış olan ikincil mevzuat uyarınca, elektronik sertifika hizmet sağlayıcılığı alanında faaliyet göstermektedir.

Nitelikli Elektronik Sertifika İlkeleri (Kısaca "NESİ") olarak isimlendirilen bu doküman 5070 sayılı Elektronik İmza Kanunu , Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik (Kısaca "Yönetmelik" olarak anılacaktır) ile Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ (Kısaca "Tebliğ" olarak anılacaktır) uyarınca "E-İMZATR"nin "ESHS" sıfatıyla yürüttüğü faaliyetler sırasında yerine getirdiği teknik ve hukuki gereklilikleri, "ESHS"nin faaliyetlerini, teknik ve organizasyonel altyapısını, "ESHS"nin sunduğu hizmetlere ilişkin süreçlerde belirli roller üstlenen tarafların sorumluluklarını açıklamak ve kamuoyuna duyurmak üzere hazırlanmıştır. "NESİ" belgesi, hangi elektronik sertifika hizmetlerinin "E-İMZATR" tarafından sunulduğunu belirlerken, "NESUE" bu hizmetlerin "E-İMZATR" tarafından nasıl gerçekleştirildiğini tanımlar.

1.1. Genel Bakış

5070 sayılı Elektronik İmza Kanunu uyarınca güvenli elektronik imza, Kanunda belirtilen koşulları sağlaması hâlinde elle atılan imza ile aynı hukuki sonucu doğurur. Nitelikli Elektronik Sertifika (NES), güvenli elektronik imzanın oluşturulması ve doğrulanmasında kullanılan temel unsurlardan biridir.

EİMZATR Bilgi Güvenliği Hizmetleri A.Ş., 5070 sayılı Elektronik İmza Kanunu ve ilgili mevzuat kapsamında Bilgi Teknolojileri ve İletişim Kurumuna gerekli bildirimde bulunarak **Elektronik Sertifika Hizmet Sağlayıcısı (ESHS)** olarak faaliyet göstermektedir. EİMZATR, elektronik sertifika hizmetlerini yürürlükteki elektronik imza ve kimlik doğrulama mevzuatına uygun olarak yürütür.

Bu doküman, EİMZATR tarafından sunulan Nitelikli Elektronik Sertifika hizmetlerine ilişkin temel ilke, kural, sorumluluk ve güvenlik gerekliliklerini belirleyen **Nitelikli Elektronik Sertifika İlkelerini (NESİ)** açıklamaktadır. **NESUE** ise NESİ'de belirlenen ilke ve kuralların EİMZATR tarafından nasıl uygulandığını düzenler.

1.2. Kitapçık Adı ve Tanımlama

Doküman Adı: EİMZATR Nitelikli Elektronik Sertifika İlkeleri (NESİ)

Doküman sürümü: 3.0

Hazırlanma tarihi: 03.08.2026

Nesne tanımlayıcı (OID): 2.16.792.3.0.10.10.1.1

1.3. Taraflar

Bu ilke kitapçığında hak ve yükümlülükleri tanımlanan EİMZATR sertifika hizmetleriyle ilgili taraflar, sertifika hizmetlerini veren ESHS birimleri ve hizmeti alan müşteri ve sertifika sahipleri olarak tanımlanır.

1.3.1. Sertifika Üretim Merkezleri

Sertifika üretim merkezleri, ESHS'lerin sertifika üretim, dağıtım ve talep edildiği taktirde sertifikanın yayımlamasından sorumlu birimleridir. Ana sertifika üretim merkezi E-İMZATR'nin kök

sertifikasına sahiptir. Bu merkez tarafından üretilmiş alt kök sertifikalara sahip olan diğer sertifika üretim merkezleri tarafından son kullanıcı sertifikaları üretilir.

1.3.2. Sertifika Kayıt Merkezleri

"E-İMZATR" tarafından belirlenen kayıt birimleri (Kısaca "KB" olarak anılacaktır) "E-İMZATR" adına son kullanıcı kimlik kontrolü, sertifika oluşturma istekleri ve yenileme yetkilerine sahip gerçek veya tüzel kişilerdir.

"KB" ler ile yapılan anlaşmanın detaylarına göre değişmekle birlikte aşağıdaki yetkilere sahiptir:

- "NESİ" ve "NESUE" ye uygun olarak sertifika üretim istekleri oluşturma
- Başvuru sürecindeki tüm belgeleri talep etmek ve doğruluğunu kontrol etmek
- "NESİ" ve "NESUE" ye uygun olarak sertifika iptal isteklerini almak
- "E-İMZATR" ile arasında yapılan sözleşme, "NESİ" ve "NESUE"ye uygun hareket etme

1.3.3. Sertifika Sahipleri

NES sahibi, adına Nitelikli Elektronik Sertifika düzenlenen gerçek kişidir. Kurumsal bilgi içeren NES başvurularında da başvuru, sertifika sahibi olacak gerçek kişi tarafından yapılır. Gerekli hâllerde kişinin ilgili tüzel kişiyle ilişkisi, görevi veya yetkisi EİMZATR tarafından uygun belgeler üzerinden doğrulanır. Sertifikada kurum, görev veya yetki bilgisinin bulunması, sertifika sahibinin gerçek kişi olma niteliğini değiştirmez.

1.3.4. Üçüncü Kişiler

Üçüncü kişiler, "EİMZATR" tarafından oluşturulan "NES"ler kullanılarak imzalanmış verileri imzalayan kişinin kimliğini tespit eden; "NES"lerin, "EİMZATR" kök ve alt kök sertifikalarının, "EİMZATR" zaman damgalarının geçerlilik kontrollerini yerine getirerek veya "NES" doğrulama aracı

kullanmak suretiyle doğrulama işlemini gerçekleştiren ve "NES" ile imzalanmış verilere güvenerek iş ve işlemlerde bulunan taraflardır. "NES" sahipleri yukarıda bahsedilen doğrulama süreçlerini kendileri yerine getirmeleri durumunda üçüncü kişi olarak hareket etmektedirler.

1.3.5. Diğer Katılımcılar

Yukarıda yazılanlar dışındaki bileşenlerdir. Diğer bileşenler bu NESİ dokümanına uygun oluşturulan NESUE dokümanında detaylandırılır.

1.4. Sertifika Kullanımı

1.4.1. Geçerli Sertifika Kullanım Şekilleri

EİMZATR tarafından üretilen NES ve bu sertifikaya bağlı imza oluşturma verisi, sertifika sahibinin güvenli elektronik imza oluşturması amacıyla kullanılır. İmza oluşturma verisi yalnızca sertifika sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı üzerinde ve sertifika sahibinin kontrolünde kullanılmalıdır.

NES içeriğinde bulunan imza doğrulama verisi; oluşturulan güvenli elektronik imzanın, imza sahibinin kimliğinin, imzalanmış verinin bütünlüğünün ve sertifikanın geçerlilik durumunun doğrulanması amacıyla kullanılır. Güvenli elektronik imza, 5070 sayılı Kanunda belirtilen koşullar altında elle atılan imza ile aynı hukuki sonucu doğurur.

1.4.2. Sertifika Kullanımının Sınırları

E-İMZATR" Tarafından oluşturulan "NES"ler "NESİ"de belirtilen amaçlar dışında kullanımı yasaktır. Elektronik İmza Kanunu'nun 5. maddesi hükmü uyarınca "Kanunların resmî şekle veya özel bir merasime tabi tuttuğu hukukî işlemler ile teminat sözleşmeleri" "NES" kullanılarak yapılamaz. Bu nedenle bahsi geçen işlemlerin "NES" yapılması ve bu işlemlere ilişkin "NES" oluşturma ve doğrulama süreçlerinde "NES"lerin kullanılması yasaktır.

1.5. Sertifika İlkeleri Yönetimi

NESİ dokümanı, EİMZATR tarafından yazılmış olup gerekli gördüğü durumlarda NESİ dokümanında değişiklik yapabilir.

1.5.1. NESİ Dokümanından Sorumlu Organizasyon

İşbu NESİ dokümanının tüm hakları ve sorumluluğu EİMZATR'ye aittir.

1.5.2. İletişim Noktası

NESİ kitapçığı ile ilgili bilgiler aşağıdaki gibidir.

EİMZATR BİLGİ GÜVENLİĞİ HİZMETLERİ A.Ş

Adres:Prof Dr. Ahmet Taner KIŞLALI Mah. 2778. Sok No: 3 Çayyolu / ANKARA

Tel: +90 312 242 01 11

Fax: +90 312 242 00 42

E-posta: bilgi@e-imzatr.com.tr

Web: www.e-imzatr.com.tr

1.5.3. NESİ'nin İlkelere Uygunluğunu Belirleyen Yetkili

"NESİ" dokümanının uygunlu ve uygulanabilirliği "EİMZATR üst yönetimi tarafından belirlenir.

1.5.4. NESİ Onaylama Prosedürleri

"NESİ" dokümanının uygunluğu ve uygulanabilirliği "EİMZATR üst yönetimi tarafından takip edilir, güncellenmesi için gerekli yönlendirmeler yapılır ve onaylanır. Gerekli onayı alan NESİ, ESHS faaliyetlerine ilişkin ilke ve kuralları düzenlemek için kullanılır.

1.6. Kısaltmalar ve Tanımlar

1.6.1. Kısaltmalar

Kısaltma	Açılımı
BTK	Bilgi Teknolojileri ve İletişim Kurumu
EİMZATR	EİMZATR Bilgi Güvenliği Hizmetleri A.Ş.
ESHS	Elektronik Sertifika Hizmet Sağlayıcısı
NES	Nitelikli Elektronik Sertifika
NESİ	Nitelikli Elektronik Sertifika İlkeleri
NESUE	Nitelikli Elektronik Sertifika Uygulama Esasları
KB	Kayıt Birimi
PKI	Public Key Infrastructure – Açık Anahtarlı Altyapı
HSM	Hardware Security Module – Donanımsal Güvenlik Modülü
FKM	Felaket Kurtarma Merkezi
OCSP	Online Certificate Status Protocol – Çevrim İçi Sertifika Durum Protokolü
CRL	Certificate Revocation List – Sertifika İptal Listesi
OID	Object Identifier – Nesne Tanımlayıcı Numarası

DN	Distinguished Name – Ayırt Edici İsim
CN	Common Name – Yaygın İsim
O	Organisation – Kurum Adı
OU	Organizational Unit – Kurumsal Birim
C	Country – Ülke
L	Locality – Yerleşim Yeri
ETSI	European Telecommunications Standards Institute – Avrupa Telekomünikasyon Standartları Enstitüsü
IETF	Internet Engineering Task Force – İnternet Mühendisliği Görev Grubu
RFC	Request for Comments – IETF tarafından yayımlanan teknik dokümanlar
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission – Uluslararası Standardizasyon Teşkilatı / Uluslararası Elektroteknik Komisyonu
TSE	Türk Standartları Enstitüsü
EKDS	Elektronik Kimlik Doğrulama Sistemi
KEC	Kart Erişim Cihazı
KDB	Kimlik Doğrulama Bildirimi
KDHS	Kimlik Doğrulama Hizmet Sağlayıcısı
TEKB	Temaslı İletişim Kabiliyetini Haiz Elektronik Kimlik Belgesi
YAKB	Yakın Alan İletişimi Kabiliyetini Haiz Elektronik Kimlik Belgesi
TCKN	Türkiye Cumhuriyeti Kimlik Numarası
KVKK	6698 sayılı Kişisel Verilerin Korunması Kanunu

1.6.2. Tanımlar

Terim	Tanım
Elektronik İmza	Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veridir.
Güvenli Elektronik İmza	5070 sayılı Elektronik İmza Kanununda belirtilen şartları sağlayan; münhasıran imza sahibine bağlı, yalnızca imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracıyla oluşturulan, Nitelikli Elektronik Sertifikaya dayanan ve imzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan elektronik imzadır.
Elektronik Sertifika	İmza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kayıttır.
Nitelikli Elektronik Sertifika (NES)	5070 sayılı Elektronik İmza Kanununda nitelikli elektronik sertifika için öngörülen zorunlu bilgileri ve nitelikleri taşıyan elektronik sertifikadır.
Elektronik Sertifika Hizmet Sağlayıcısı (ESHS)	Elektronik sertifika, zaman damgası ve elektronik imza ile ilgili hizmetleri 5070 sayılı Elektronik İmza Kanunu ve ilgili mevzuat uyarınca sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişileridir.

Terim	Tanım
Sertifika Sahibi	Adına Nitelikli Elektronik Sertifika düzenlenen gerçek kişidir.
Kurumsal Bilgi İçeren NES	Sertifika sahibinin gerçek kişi olma niteliğini değiştirmeksizin, NES içerisinde ilgili tüzel kişiye, göreve, unvana veya yetkiye ilişkin doğrulanmış bilgilerin yer aldığı sertifikadır.
Kurumsal Başvuru	Yönetmelikte tanımlanan şekilde, bir tüzel kişinin çalışanları, müşterileri, üyeleri veya hissedarları adına yaptığı NES başvurusudur. Bu başvuru türüne ilişkin hükümler, EİMZATR tarafından ilgili hizmetin sunulduğu ölçüde uygulanır.
Kurumsal Başvuru Sahibi	Yönetmelikte tanımlanan kurumsal başvuruyu EİMZATR'ye ileten ve başvuru kapsamındaki kişiler adına ilgili mevzuatta öngörülen yükümlülükleri yerine getiren tüzel kişidir.
Kayıt Birimi (KB)	EİMZATR adına başvuru alma, kimlik doğrulama ile gerekli bilgi ve belge kontrollerini yürütme ve yetkisi kapsamındaki sertifika yönetim taleplerini EİMZATR'ye iletme görevlerini yerine getiren yetkilendirilmiş birimdir.
Üçüncü Kişi	NES'e veya bu NES'e dayanılarak oluşturulan güvenli elektronik imzaya güvenerek işlem yapan ve gerekli sertifika ve imza doğrulama kontrollerini gerçekleştiren gerçek veya tüzel kişidir.
İmza Oluşturma Verisi	İmza sahibine ait olan ve elektronik imza oluşturmak amacıyla kullanılan benzersiz veridir. Kriptografik uygulamalarda özel anahtarı ifade eder.
İmza Doğrulama Verisi	Elektronik imzanın doğrulanması amacıyla kullanılan ve imza oluşturma verisiyle matematiksel olarak ilişkili veridir. Kriptografik uygulamalarda açık anahtarı ifade eder.
Güvenli Elektronik İmza Oluşturma Aracı	5070 sayılı Elektronik İmza Kanunu ve ilgili teknik düzenlemelerde belirlenen güvenlik koşullarını sağlayan, imza oluşturma verisinin güvenli biçimde oluşturulmasını, korunmasını ve kullanılmasını sağlayan yazılım veya donanımdır.
Sertifika İptal Listesi (SİL/CRL)	İptal edilen sertifikalara ilişkin durum bilgilerinin ESHS tarafından elektronik olarak imzalanarak yayımlandığı sertifika iptal listesidir.
Çevrim İçi Sertifika Durum Protokolü (OCSP)	Bir elektronik sertifikanın güncel geçerlilik durumunun çevrim içi olarak sorgulanmasını sağlayan protokoldür.
Sertifika İptali	Bir NES'in geçerlilik süresi sona ermeden önce sertifika statüsünün geri döndürülemez biçimde iptal durumuna geçirilmesidir.
Sertifika Askıya Alma	Bir NES'in kullanımının ve geçerlilik durumunun, iptal kararı verilmeden önce geçici olarak durdurulmasıdır. EİMZATR tarafından uygulanan askıya alma süresi ve bu sürenin sonunda uygulanacak işlemler Bölüm 4.9'da düzenlenmiştir.
Zaman Damgası	Bir elektronik verinin üretildiği, değiştirildiği, gönderildiği, alındığı ve/veya kaydedildiği zamanın tespit edilmesi amacıyla ESHS tarafından elektronik imzayla doğrulanan kayıttır.
Güven Merkezi	EİMZATR'nin ESHS faaliyetleri kapsamındaki kritik sertifika yönetimi, kriptografik işlemler ve güven hizmetlerinin fiziksel ve mantıksal güvenlik kontrolleri altında

Terim	Tanım
	yürütüldüğü altyapı ve güvenli alanlardır.
Güvenli Personel	ESHS faaliyetleri kapsamında kritik görevleri yerine getirmek üzere gerekli güvenilirlik, yetkinlik ve yetkilendirme koşullarını sağlayan personeldir.
Donanımsal Güvenlik Modülü (HSM)	ESHS'ye ait kritik kriptografik anahtarların güvenli biçimde oluşturulması, korunması ve kullanılması amacıyla kullanılan donanımsal güvenlik modülüdür.
Felaket Kurtarma Merkezi (FKM)	Olağanüstü durumlarda ESHS hizmetlerinin sürekliliğini ve geri kazanımını sağlamak amacıyla kullanılan alternatif sistem ve altyapı merkezidir.
Bilgi Deposu	NESİ, NESUE, kök ve alt kök sertifikalar, sertifika durum bilgileri ile mevzuat gereği kamuya açık tutulması gereken diğer bilgi ve belgelerin yayımlandığı erişim ortamıdır.
Nitelikli Elektronik Sertifika İlkeleri (NESİ)	EİMZATR'nin NES hizmetlerine ilişkin temel ilke, kural, sorumluluk ve güvenlik gerekliliklerini açıklayan dokümandır.
Nitelikli Elektronik Sertifika Uygulama Esasları (NESUE)	NESİ'de belirlenen ilke ve kuralların EİMZATR tarafından nasıl uygulandığını açıklayan dokümandır.

Kimlik Doğrulama Yönetmeliği Elektronik Haberleşme Sektöründe Başvuru Sahibinin Kimliğinin Doğrulanma Süreci Hakkında Yönetmeliğidir.

2. YAYIN VE BİLGİ DEPOSU SORUMLULUKLARI

2.1. Bilgi Deposu

EİMZATR, bilgi deposunda tutulan tüm bilgilerin doğruluğunu ve güncelliğini sağlar. Bilgi depolarına erişim internet üzerinden sağlanır.

2.2. Sertifika Bilgilerinin Yayımlanması

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

2.3. Yayımın Zamanı veya Sıklığı

EİMZATR tarafından yayımlanması gereken sertifika ve sertifika durum bilgileri, ilgili işlemlerin gerçekleşmesini takiben güncellenir ve yayımlanır. SİL yayımlama sıklığı ve geçerlilik süreleri Bölüm 4.9.7'de belirtilmiştir. Sertifika durum bilgileri OCSP hizmeti üzerinden de erişilebilir tutulur.

2.4. Bilgi Deposuna Erişim Kontrolleri

EİMZATR tarafından kamuya açık olarak yayımlanması öngörülen sertifika ilkeleri, sertifika uygulama esasları, kök ve alt kök sertifikalar, sertifika iptal listeleri ve sertifika durum bilgileri, ilgili tarafların erişimine sunulur.

Kamuya açık bilgi deposuna erişim için gerekli teknik ve güvenlik kontrolleri EİMZATR tarafından uygulanır. Bu kontroller, yayımlanan bilgilerin yetkisiz şekilde değiştirilmesini, silinmesini, bozulmasını veya amacı dışında kullanılmasını önlemek amacıyla gerçekleştirilir.

"ESHS" kullanıcıların özel bilgilerini istekleri dışında paylaşmaz. "NES" ve "NESİ" de belirtildiği şekilde sertfikalar ve sertifika durum bilgileri üçüncü kişilerle paylaşılacaktır. Yanlış ve yetkisiz kullanımı önlemek için gerekli önlemler "ESHS" tarafından alınır.

3. KİMLİĞİN DOĞRULANMASI

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

3.1. İsimlendirme

Bu bölümde sertifika içerisindeki isimlendirmelerle ilgili bilgiler açıklanır.

3.1.1. İsim Tipleri

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

3.1.2. İsimlerin Anlamlı Olması Gerekliliği

"NES" lerde kullanılacak isimler ve bilgiler başvuru sırasında verilen resmi belgelere dayandırılarak hazırlanır. İsimlendirme bir yanlışlık ya da standartlara uygunsuzluk tespit edilirse "NES" başvurusu iptal edilir.

3.1.3. Sertifika Sahiplerinin Anonimliği ve Takma Ad Kullanılabilirliği

"NES"lerde sadece gerçek isimlerin kullanılmasına izin verilir. "NES" sahibinin isminin gizlenmesi kanunen yasaktır.

3.1.4. İsim Biçimlerinin Değerlendirilmesi

"EİMZATR" tarafından oluşturulan tüm "NES"lerin "DN" alanı içerisinde ITU X.500 standartları tarafından belirlenen isimlendirme kuralları uygulanır.

3.1.5. İsimlerin Benzersizliği

"EİMZATR" "NES"lerde bulunan bilgilerin benzersiz olmasını sağlamakla yükümlüdür.

3.1.5.1.NES

NES'lerde kullanılan isimler, kendi aralarında benzersizdir.

3.1.6. Ticari Markaların Tanınması, Doğrulanması ve Rolü

"NES" başvuru sahiplerinin, bireysel veya kurumsal başvurularda başkalarının fikri mülkiyet haklarını ihlal eden isimler kullanmaları yasaktır.

3.2. İlk Kimlik Doğrulama

3.2.1. Gizli Anahtara Sahip Olunduğunun Kanıtlanma Yöntemi

EİMZATR işleyişinde son kullanıcıya ait imza oluşturma ve imza doğrulama verileri, EİMZATR'ın kontrolündeki güvenli sertifika üretim süreci kapsamında oluşturulduğundan, başvuru sahibinden gizli anahtara sahip olduğunu ayrıca kanıtlaması istenmez.

3.2.2. Tüzel Kişiliğin Doğrulanması

Sertifikada yer alacak tüzel kişiliğin ismi veya unvanı, sertifika sahibinin bulunduğu ülkedeki yasal belgelere bağlı olarak doğrulanır.

3.2.3. Gerçek Kişinin Kimliğinin Doğrulanması

Başvuru sahibinin kimliği, yürürlükteki mevzuatın kabul ettiği doğrulama yöntemlerinden biri kullanılarak teyit edilir. Başvurunun yapıldığı kanalın ve kimlik belgesinin özelliğine göre kimlik doğrulama işlemi aşağıdaki yöntemlerden biriyle gerçekleştirilebilir:

- E-Devlet Kapısı üzerinden kimlik doğrulama ve başvuru onayı alınması,
- Yakın Alan İletişimi Kabiliyetini Haiz Elektronik Kimlik Belgesinin (YAKB) okunması ve bu işlemin yapay zekâ destekli veya yetkili personel tarafından yürütülen görüntülü doğrulamayla tamamlanması,
- Temaslı İletişim Kabiliyetini Haiz Elektronik Kimlik Belgesinin (TEKB) kullanılması ve şifre ya da parmak izi özeti aracılığıyla kimliğin doğrulanması,
- Yüz yüze yapılan başvurularda resmî kimlik belgesinin kontrol edilmesi ve ilgili başvuru işlemine özgü video kaydının oluşturulması,
- Yabancı başvuru sahiplerinin kimlik bilgilerinin Göç İdaresi Başkanlığı tarafından sunulan sistem ve doğrulama yöntemleri üzerinden teyit edilmesi.

EİMZATR, uygulanacak kimlik doğrulama yöntemini başvuru türüne, başvuru sahibinin statüsüne, kullanılan kimlik belgesine ve ilgili mevzuat hükümlerine göre belirler.

3.2.4. Doğrulama Yapılmaksızın Sertifikada Yer Alabilen Bilgiler

NES içerisinde yer alacak bilgiler, yürürlükteki mevzuat ve ilgili sertifika profilleri doğrultusunda belirlenir. Doğrulanması gereken kimlik, kurum, görev, unvan veya yetki bilgileri uygun ve güvenilir kaynaklar üzerinden doğrulanır. Mevzuat veya sertifika profili kapsamında doğrulama zorunluluğu bulunmayan bilgiler, niteliğine göre başvuru sahibinin beyanına dayanılarak sertifikada yer alabilir.

3.2.5. Yetkinin Doğrulanması

NES içeriğinde bir tüzel kişiliğin isminin yer alması söz konusu ise sertifika başvuru sahibinin bu tüzel kişiliği temsil ve ilzama yetkili olduğunu gösterir resmi belgeleri ibraz etmesi zorunludur.

3.2.6. Karşılıklı Çalışma Kriterleri

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

3.3. Sertifika Yenileme İsteğinde Kimlik Doğrulama

Sertifikanın güvenli kullanım süresinin sonunda, yeni anahtar çifti üretimi, kullanıcının yeni bir NES başvurusunda bulunmasıyla gerçekleştirilir. Yeni sertifika başvurusu, sertifikanın kullanım süresi içinde, elektronik ortamda ve mevcut sertifikaya bağlı imza oluşturma verisiyle imzalanarak yapılabilir. Yeni sertifika içinde yer alacak bir bilgide değişiklik gerekmesi durumunda, bu değişikliğin resmi belgeye dayandırılması zorunludur. Sertifikada yer almayan diğer kullanıcı bilgilerindeki değişiklikler ise NES sahibinin yazılı veya elektronik beyanıyla kabul edilir.

Rutin anahtar yenileme işlemleri sırasında başvuru sahibinin başvurusu sertifikanın kullanım süresi içinde, elektronik ortamda ve mevcut sertifikaya bağlı imza oluşturma verisiyle imzalanarak yapılabileceği gibi 3.2.3 maddesi yöntemleri uygulanarak süreç tamamlanır.

3.4. İptal Talebi için Kimlik Doğrulama

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

- Sertifika sahibi başvuru sırasında belirttiği kendisine özel bilgileri kullanarak Online İşlemler bölümünde iptal/askı işlemini gerçekleştirebilir.
- Sertifika sahibi EİMZATR ofislerine gelerek dilekçe ile başvurabilir iptal/askı işlemini gerçekleştirebilir.
- Çağrı merkezi üzerinden kimlik doğrulaması gerçekleştirerek iptal/askı işlemini sağlayabilir.

4. SERTİFİKA YAŞAM DÖNGÜSÜ İŞLEVSEL GEREKLİLİKLERİ

EİMZATR, sertifikalarını bu NESİ dokümanında yer alan ilke ve kurallar uyarınca üretir ve yaşam döngüsünü yönetir.

4.1. Sertifika Başvurusu

4.1.1. Kimler Sertifika Başvurusunda Bulunabilir?

Herhangi bir yasal engeli olmayan her gerçek kişi NES başvurusunda bulunabilir. Belirtilen kimlik doğrulama prosedürlerini yerine getirebilen gerçek kişiler ve yetki belgesine sahip tüzel kişi temsilcileri “NES” başvurusunda bulunabilirler.

4.1.2. Sertifika Başvuru, Kayıt Süreci ve Sorumluluklar

NES başvuruları, EİMZATR internet sitesi, EİMZATR’a bağlı kayıt birimleri veya EİMZATR tarafından kullanıma sunulan ve yürürlükteki mevzuata uygun diğer başvuru kanalları üzerinden başlatılabilir.

Başvuru sırasında başvuru sahibinin kimlik ve iletişim bilgileri, talep edilen sertifikaya ilişkin bilgiler, teslimat tercihi ve gerekli olması hâlinde kurumsal yetki bilgileri alınır. Her başvuru için tekil bir başvuru kaydı oluşturulur ve başvuru sürecinde gerçekleştirilen işlemler bu kayıtla ilişkilendirilir.

Başvuru sahibi, başvuru kapsamında sunduğu bilgi ve belgelerin eksiksiz ve doğru olmasından, gerekli onay ve taahhütleri vermekten ve başvuru sonuçlanmadan önce bilgilerinde meydana gelen değişiklikleri EİMZATR’a bildirmekten sorumludur.

EİMZATR, başvuruya ilişkin bilgi ve belgeleri, kimlik doğrulama sonuçlarını, başvuru sahibinin onaylarını ve işlem kayıtlarını bütünlüğü korunacak ve başvuruyla ilişkilendirilebilecek şekilde kayıt altına alır.

Başvuru sahibinin kimliğinin doğrulanması, başvurunun değerlendirilmesi, kabul veya reddedilmesi ve sertifika üretim sürecine aktarılması bu NESİ’nin ilgili bölümlerinde belirtilen esaslara göre gerçekleştirilir.

4.2. Sertifika Başvurusunun İşlenmesi

4.2.1. Kimlik Doğrulama İşlemlerinin Yerine Getirilmesi

Başvuru sahibinin kimliği, başvuru türü, başvuru kanalı, vatandaşlık durumu ve kullanılan kimlik belgesine göre, bu NESİ’nin 3.2’nci bölümünde belirtilen ve yürürlükteki mevzuatın izin verdiği yöntemlerden biri kullanılarak doğrulanır.

4.2.2. Sertifika Başvurularının Kabulü veya Reddedilmesi

Başvurunun kabul edilebilmesi için gerekli bilgi ve belgelerin eksiksiz olması, başvuru sahibinin kimliğinin ve varsa yetkisinin doğrulanması, gerekli onay ve taahhütlerin tamamlanması ve ücret koşullarının karşılanması gerekir.

Eksik, tutarsız, doğrulanamayan veya gerçeğe aykırı bilgi içeren; kimlik doğrulaması tamamlanamayan ya da gerekli koşulları karşılamayan başvurular reddedilir veya eksikliklerin giderilmesi amacıyla başvuru sahibine iade edilir. Başvuru hakkında verilen karar kayıt altına alınır ve başvuru sahibine bildirilir.

4.2.3. Sertifika Başvurularının İşlenme Süresi

Başvurular; gerekli bilgi ve belgelerin tamamlanması, kimlik doğrulama işleminin sonuçlanması ve ücret koşullarının karşılanmasının ardından işleme alınır. Başvurunun işlenme süresi; başvuru yöntemi, yapılması gereken kontroller ve teslimat tercihine göre değişebilir. Eksik veya ek inceleme gerektiren başvurularda işlem süresi, eksikliğin giderilmesinden sonra başlar.

Sertifikanın üretilmesi veya aktifleştirilmesinde uygulanacak yasal bekleme süresine ilişkin esaslar NESİ'nin 4.3.1'inci maddesinde düzenlenmiştir.

4.3. NES Üretimi

4.3.1. NES Üretimi Sırasındaki ESHS Faaliyetleri

Bu NESİ'nin 4.2.2'nci maddesine göre kabul edilen başvurular, EİMZATR'ın yetkilendirilmiş sertifika üretim sistemlerinde; yürürlükteki mevzuat, NESİ, NESUE ve ilgili güvenlik prosedürlerine uygun olarak işlenir.

Başvuru kaydı ile sertifika sahibinin kimlik bilgileri ve sertifikada yer alacak bilgiler kontrol edilerek eşleştirilir. İmza oluşturma ve imza doğrulama verileri ile NES, mevzuata uygun güvenli araçlar, algoritmalar ve teknik standartlar kullanılarak oluşturulur.

Başvuru işlemlerinin elektronik ortamda eksiksiz olarak tamamlanmasının ardından, başvuru sahibinin Türkiye Cumhuriyeti Kimlik Numarasına veya Yabancı Kimlik Numarasına tanımlı mobil numaralarına, adına NES başvurusu yapıldığına ilişkin bilgilendirme mesajı gönderilir.

İspatlanabilir nitelikte zorunlu hâller dışında NES, söz konusu bilgilendirmenin yapılmasından itibaren en az üç saat geçmeden oluşturulmaz veya aktifleştirilmez. EİMZATR, bu yükümlülüğü sertifikanın aktifleştirilmesi aşamasında uygular.

EİMZATR'ın olağan işleyişinde sertifika, yasal bekleme süresi korunarak takip eden gün saat 00.00 itibarıyla kullanıma açılır. Kullanıma açılacağı tarih ve saat, başvuru sırasında sertifika sahibine bildirilir.

Başvuru sahibinin sertifikaya yasal kurul kararı bekleme süresi dolmadan ihtiyaç duyduğu ispatlanabilir zorunlu hâllerde; zorunluluğun nedeni, sertifikanın kullanılacağı işlem veya yer ve talebin gerekçesi başvuru sahibi tarafından beyan edilerek imzalı belge ile kayıt altına alınır. Talebin EİMZATR tarafından uygun bulunması hâlinde üç saatlik bekleme süresi uygulanmadan sertifika aktifleştirilebilir.

4.3.2. NES Üretimiyle İlgili Sertifika Sahibinin Bilgilendirilmesi

Sertifika üretimi tamamlandıktan sonra, sertifika sahibi sertifikanın durumunu online işlemlerden görüntüleyebilir.

4.4. NES'in Kabulü

4.4.1. Kabulün Şekli

Sertifika sahibi, EİMZATR tarafından adına oluşturulan Nitelikli Elektronik Sertifikayı (NES) kullanmaya başlamadan önce sertifika içerisinde yer alan bilgileri kontrol eder.

Sertifika sahibinin, NES içerisinde yer alan bilgilerin başvuru sırasında beyan ettiği bilgilerle uyumlu olduğunu kontrol etmesi esastır.

Sertifika sahibinin;

- NES'in kendisine ait olmadığını,

- Sertifika içerisinde yer alan bilgilerde hata veya eksiklik bulunduğunu,
- Sertifika bilgilerinin başvuru sırasında beyan edilen bilgilerle uyuşmadığını veya
- NES'in kullanımını etkileyen bir uygunsuzluk bulunduğunu

tespit etmesi halinde EİMZATR'yi gecikmeksizin bilgilendirmesi gerekir.

Herhangi bir uygunsuzluk bildiriminde bulunulmaksızın NES'in kullanılmaya başlanması, sertifika sahibinin NES'i kabul ettiği anlamına gelir.

Bildirilen uygunsuzluğun doğrulanması halinde gerekli iptal, yeniden üretim veya diğer işlemler ilgili mevzuat ile EİMZATR sertifika ilke ve uygulama esasları doğrultusunda gerçekleştirilir.

4.4.2. ESHS Tarafından Sertifikanın Yayımlanması

EİMZATR, sertifika sahibinin onayını almak kaydıyla Nitelikli Elektronik Sertifikayı (NES) kamuya açık dizinde yayımlar. Sertifika sahibinin onayının bulunmaması halinde NES kamuya açık dizinde yayımlanmaz. EİMZATR, kamuya açık dizin hizmetinin sürekliliğini sağlar.

4.4.3. Diğer Katılımcıların Sertifika Üretimiyle İlgili Bilgilendirilmesi

EİMZATR tarafından NES üretimi sonrasında, sertifika sahibi dışında herhangi bir katılımcıya ayrıca sertifika üretim bildirimi yapılmaz.

4.5. NES Kullanımı

4.5.1. Sertifika Sahibi İmza Oluşturma Verisi ve "NES" Kullanımı

NES sahibi, imza oluşturma verisini ve Nitelikli Elektronik Sertifikasını (NES); 5070 sayılı Elektronik İmza Kanunu, ilgili Yönetmelik ve Tebliğ, EİMZATR NESİ ve NESUE dokümanları, sertifika sahibi ile yapılan sözleşme ve/veya taahhütname ile NES içerisinde belirtilen sınırlamalarına uygun olarak kullanır.

NES sahibi, imza oluşturma verisini yalnızca elektronik imza oluşturma amacıyla kullanmak; imza oluşturma verisinin ve bu veriye erişimde kullanılan PIN, parola ve benzeri erişim verilerinin gizliliğini ve güvenliğini sağlamakla yükümlüdür.

NES sahibi;

- İmza oluşturma verisini ve güvenli elektronik imza oluşturma aracını üçüncü kişilere kullandıramaz,
- İmza oluşturma aracına ait PIN, parola ve benzeri erişim verilerini üçüncü kişilerle paylaşamaz,
- İmza oluşturma aracının ve erişim verilerinin yetkisiz kişilerin kullanımına karşı korunması için gerekli tedbirleri alır,
- Güvenli elektronik imza oluşturma aracı kullanır,
- NES'i, sertifikada belirtilmiş olan sınırlamalarına uygun şekilde kullanır.

İmza oluşturma aracının veya erişim verisinin kaybolması, çalınması, yetkisiz kişilerce kullanılması veya kullanılabileceğinden şüphe edilmesi ya da imza oluşturma verisinin gizliliği veya güvenilirliğinin tehlikeye girdiğinin değerlendirilmesi halinde NES sahibi, EİMZATR'yi derhal bilgilendirir ve gerekli iptal işlemlerinin başlatılmasını sağlar.

4.5.2. Üçüncü Kişilerin İmza Doğrulama Verisi ve "NES" Kullanımı

EİMZATR tarafından düzenlenen Nitelikli Elektronik Sertifikaya (NES) ve bu sertifikaya dayanılarak oluşturulan güvenli elektronik imzaya güvenerek işlem yapacak üçüncü kişiler, işlem öncesinde gerekli sertifika ve imza doğrulama kontrollerini gerçekleştirmekle yükümlüdür.

Üçüncü kişiler;

- Kullanılan sertifikanın Nitelikli Elektronik Sertifika niteliğinde olup olmadığını,

- NES'in geçerlilik süresini ve iptal durumunu,
- Sertifikanın güvenilir bir sertifika zincirine dayanıp dayanmadığını,
- NES içerisinde kullanım amacına veya maddi kapsama ilişkin herhangi bir sınırlama bulunup bulunmadığını,
- Elektronik imzanın doğrulama sonucunun geçerli olup olmadığını

kontrol eder.

NES'in geçerlilik ve iptal durumu, EİMZATR tarafından sunulan SİL ve/veya OCSP hizmetleri kullanılarak ya da ilgili mevzuata uygun güvenli elektronik imza doğrulama araçları aracılığıyla kontrol edilebilir.

Üçüncü kişiler, NES'in kullanımına veya maddi kapsamına ilişkin sınırlamaların bulunması halinde gerçekleştirecekleri işlemin bu sınırlamalara uygunluğunu değerlendirmekle yükümlüdür.

Sertifikanın geçerliliğinin veya elektronik imzanın doğruluğunun doğrulanamaması, sertifikanın iptal edilmiş veya geçerlilik süresinin sona ermiş olması ya da sertifika üzerindeki kullanım sınırlamalarının gerçekleştirilecek işlemle uyumlu olmaması halinde üçüncü kişiler NES'e ve bu NES kullanılarak oluşturulan elektronik imzaya dayanarak işlem yapmamalıdır.

Üçüncü kişilerin, mevzuat ile EİMZATR NESİ ve NESUE dokümanlarında belirtilen doğrulama ve kontrol yükümlülüklerini yerine getirmemelerinden kaynaklanan sonuçlardan EİMZATR sorumlu tutulamaz.

4.6. NES Yenileme

Nitelikli Elektronik Sertifika (NES) yenileme işlemi, sertifika sahibinin talebi üzerine ve mevcut NES'in geçerlilik süresi sona ermeden gerçekleştirilir.

Yenileme kapsamında mevcut sertifikanın geçerlilik süresi değiştirilmez; yenileme talebinin uygun bulunması halinde yürürlükteki mevzuat ile EİMZATR NESİ ve NESUE hükümleri doğrultusunda yeni bir NES oluşturulur.

Yenileme sırasında sertifika sahibine ait bilgilerin güncelliği kontrol edilir. NES içerisinde kurumsal bilgi bulunması halinde, bu bilginin ve sertifika sahibinin ilgili tüzel kişiyle olan yetki veya ilişkisinin geçerliliği gerekli belgeler üzerinden doğrulanır.

Sertifika bilgilerinde değişiklik bulunması veya yeniden kimlik ya da yetki doğrulaması gerektiren bir durumun ortaya çıkması halinde ilgili başvuru ve doğrulama süreçleri uygulanır. Geçerlilik süresi sona ermiş NES için yeni NES başvuru süreci işletilir.

4.6.1. NES Yenilemeyi Gerektiren Durumlar

Nitelikli Elektronik Sertifika (NES), geçerlilik süresinin sona ermesinden önce sertifika sahibinin veya sertifika sahibinin onayı alınmak kaydıyla kurumsal başvuru sahibinin talebi üzerine yenilenebilir.

NES yenileme işlemi aşağıdaki durumlarda gerçekleştirilebilir:

- NES'in geçerlilik süresinin sona ermesinin yaklaşması ve sertifika sahibinin sertifikayı kullanmaya devam etmek istemesi,
- EİMZATR tarafından yapılan kontroller sonucunda sertifika sahibine ait bilgilerin geçerliliğinin doğrulanması ve yenilemeye engel bir durumun bulunmaması,
- EİMZATR'nin imza oluşturma verisinin çalınması, kaybolması, gizliliğinin veya güvenilirliğinin ortadan kalkması, sertifika ilkelerinin değişmesi veya benzeri nedenlerle mevcut NES'in EİMZATR tarafından iptal edilerek yenilenmesinin gerekmesi.

NES'in geçerlilik süresinin sona ermiş olması halinde yenileme işlemi yapılmaz; bu durumda yeni NES başvuru ve üretim süreci işletilir.

Sertifika sahibine ait imza oluşturma aracının veya erişim verisinin kaybolması, çalınması, yetkisiz kişilerin eline geçtiğinin veya güvenilirliğinin tehlikeye girdiğinin düşünülmesi halinde durum yenileme işlemi olarak değerlendirilmez. Mevcut NES için iptal süreci başlatılır ve gerekli olması halinde yeni NES üretimine ilişkin süreç uygulanır.

4.6.2. Yenileme Talebinde Bulunabilecek Kişiler

Nitelikli Elektronik Sertifikanın yenilenmesine ilişkin talep sertifika sahibi tarafından yapılır. Kurumsal bilgi içeren NES'lerde gerekli kurumsal yetki ve ilişki doğrulamaları EİMZATR tarafından gerçekleştirilir.

4.6.3. NES Yenileme Talebinin İşlenmesi

NES yenileme talepleri EİMZATR tarafından, yürürlükteki mevzuat ile NESİ ve NESUE'de belirlenen esaslar doğrultusunda değerlendirilir.

Yenileme talebinin alınmasının ardından;

- Yenileme talebinde bulunan kişinin talepte bulunmaya yetkili olup olmadığı,
- Yenilenecek NES'in geçerlilik durumu,
- Sertifika sahibine ait kimlik ve sertifika bilgilerinin güncelliği,
- Yenileme en fazla 3 yıl olabilir,
- Yenilemeye engel bir iptal, güvenlik olayı veya başka bir durumun bulunup bulunmadığı

kontrol edilir.

Sertifika sahibine ait bilgilerin değişmiş olması veya bilgilerin yeniden doğrulanmasını gerektiren bir durumun bulunması halinde gerekli kimlik doğrulama ve başvuru işlemleri gerçekleştirilir.

Yenileme talebinin ve gerekli kontrollerin uygun bulunması halinde yeni NES'in oluşturulmasına ilişkin işlemler başlatılır.

Mevcut NES'in geçerlilik süresinin sona ermiş olması, sertifikanın iptal edilmiş olması veya yenileme koşullarının sağlanmaması halinde yenileme talebi bu kapsamda işleme alınmaz; gerekli olması halinde yeni NES başvuru süreci uygulanır.

4.6.4. Yenilenmiş Sertifikayla İlgili Sertifika Sahibine Bildirim Yapılması

Sertifika üretimi tamamlandıktan sonra, sertifika ESHS durum bilgilendirmesi yapmakla yükümlüdür.

4.6.5. Yenilenen NES Kabulü

Sertifika sahibi, EİMZATR tarafından adına oluşturulan Nitelikli Elektronik Sertifikayı (NES) kullanmaya başlamadan önce sertifika içerisinde yer alan bilgileri kontrol eder.

Sertifika sahibinin, NES içerisinde yer alan bilgilerin başvuru sırasında beyan ettiği bilgilerle uyumlu olduğunu kontrol etmesi esastır.

Sertifika sahibinin;

- NES'in kendisine ait olmadığını,
- Sertifika içerisinde yer alan bilgilerde hata veya eksiklik bulunduğunu,
- Sertifika bilgilerinin başvuru sırasında beyan edilen bilgilerle uyuşmadığını veya
- NES'in kullanımını etkileyen bir uygunsuzluk bulunduğunu

tespit etmesi halinde EİMZATR'yi gecikmeksizin bilgilendirmesi gerekir.

Herhangi bir uygunsuzluk bildiriminde bulunulmaksızın NES'in kullanılmaya başlanması, sertifika sahibinin NES'i kabul ettiği anlamına gelir.

Bildirilen uygunsuzluğun doğrulanması halinde gerekli iptal, yeniden üretim veya diğer işlemler ilgili mevzuat ile EİMZATR sertifika ilke ve uygulama esasları doğrultusunda gerçekleştirilir.

4.6.6. ESHS Tarafından Yenilenen Sertifikanın Yayımlanması

“ESHS” üretilen sertifikaları "NES" sahibinin izni ile en kısa süre içerisinde veri depolarında yayınlamak zorundadır.

4.6.7. Diğer Katılımcıların Yeni Sertifika Üretimiyle İlgili Bilgilendirilmesi

EİMZATR tarafından NES üretimi sonrasında, sertifika sahibi dışında herhangi bir katılımcıya ayrıca sertifika üretim bildirimi yapılmaz.

4.7. Anahtar Yenileme

4.7.1. Anahtar Yenilemeyi Gerektiren Durumlar

Sertifika sahibine ait mevcut anahtar çiftinin kullanılmaya devam edilmesinin mümkün veya güvenli olmadığı durumlarda yeni bir anahtar çifti oluşturularak yeni NES düzenlenir.

Anahtar yenileme işlemi özellikle;

- Güvenli elektronik imza oluşturma aracının kaybolması veya çalınması,
- Güvenli elektronik imza oluşturma aracının arızalanması veya kullanılamaz hale gelmesi ve mevcut imza oluşturma verisine güvenli biçimde erişilememesi,
- İmza oluşturma verisinin gizliliğinin veya güvenilirliğinin tehlikeye girdiğinin tespit edilmesi ya da bundan şüphe edilmesi,
- Mevcut anahtar çiftinin kullanılmaya devam edilmesinin güvenlik gerekleri veya uygulanması gereken kriptografik kriterler nedeniyle uygun olmaması

hallerinde gerçekleştirilir.

Mevcut imza oluşturma verisinin kaybolması, çalınması, yetkisiz kişilerin erişimine maruz kalması veya güvenilirliğinin tehlikeye girmesi halinde mevcut NES için gerekli iptal işlemleri gerçekleştirilir. Gerekli kimlik doğrulama ve başvuru kontrollerinin tamamlanmasının ardından yeni anahtar çifti oluşturularak yeni NES üretilebilir.

4.7.2. Anahtar Yenileme Talebinde Bulunabilecek Kişiler

Anahtar yenileme talebi sertifika sahibi tarafından yapılır. Gerekli kimlik ve yetki doğrulama işlemleri ilgili NESİ ve NESUE hükümlerine göre gerçekleştirilir.

4.7.3. Anahtar Yenileme Talebinin İşlenmesi

Anahtar yenileme talebi EİMZATR tarafından değerlendirilir. Talepte bulunan kişinin yetkisi, mevcut NES’in durumu ve anahtar yenilemeyi gerektiren koşullar kontrol edilir.

Gerekli doğrulama işlemlerinin tamamlanmasının ardından mevcut NES için gerekiyorsa iptal işlemi gerçekleştirilir ve yeni anahtar çifti oluşturularak yeni NES üretim süreci başlatılır.

4.7.4. Yeni Sertifikayla İlgili Sertifika Sahibine Bildirim Yapılması

4.3.2 uygulanır.

4.7.5. Anahtarı Yenilenen Sertifikanın Kabulü

4.4.1 uygulanır.

4.7.6. ESHS Tarafından Anahtarı Yenilenen Sertifikanın Yayınlanması

4.4.2 uygulanır.

4.7.7. Diğer Katılımcıların Sertifika Üretimiyle İlgili Bilgilendirilmesi

EİMZATR tarafından NES üretimi sonrasında, sertifika sahibi dışında herhangi bir katılımcıya ayrıca sertifika üretim bildirimi yapılmaz.

4.8. Sertifika Değişikliği

4.8.1. Sertifika Değişikliğini Gerektiren Durumlar

NES içerisinde yer alan ve sertifika sahibine ilişkin bilgilerin değişmesi veya bu bilgilerde hata bulunduğunun tespit edilmesi halinde sertifika değişikliği süreci uygulanır.

Sertifika değişikliği özellikle;

- Sertifika sahibinin ad veya soyad bilgilerinin değişmesi,
- NES içerisinde yer alan kimlik veya diğer sertifika bilgilerinde hata tespit edilmesi,
- Sertifikada yer alan kurum, unvan veya benzeri bilgilerin değişmesi ve bu bilgilerin sertifika profilinde bulunması,
- Sertifika içeriğinin güncel veya doğrulanmış bilgilerle uyumlu olmadığının tespit edilmesi

hallerinde gerçekleştirilebilir.

Mevcut NES üzerinde sonradan değişiklik yapılmaz. Değişiklik gerektiren durumlarda mevcut NES gerekli hallerde iptal edilir ve sertifika sahibine ait güncel bilgilerin doğrulanmasının ardından yeni NES oluşturulmasına ilişkin süreç işletilir.

4.8.2. Sertifika Değişiklik Talebinde Bulunabilecek Kişiler

Sertifika değişiklik talebinde bulunabilecek kişiler bakımından Bölüm 4.1.1'de belirtilen esaslar uygulanır.

4.8.3. Sertifika Değişiklik Talebinin İşlenmesi

Sertifika değişiklik talebinin işlenmesi bakımından Bölüm 3.2'de belirtilen esaslar uygulanır.

4.8.4. Yeni Sertifikayla İlgili Sertifika Sahibine Bildirim Yapılması

Yeni sertifikanın üretildiğine ilişkin bildirim, Bölüm 4.3.2'de belirtilen esaslar uygulanır.

4.8.5. Değişiklik Yapılmış Sertifikanın Kabul Şekli

Değişiklik talebi sonucunda oluşturulan yeni sertifikanın kabulü, Bölüm 4.4.1'de belirtilen esaslar uygulanır.

4.8.6. ESHS Tarafından Değişiklik Yapılmış Sertifikanın Yayımlanması

Değişiklik talebi sonucunda oluşturulan yeni sertifikanın yayımlanmasına ilişkin işlemler, Bölüm 4.4.2'de belirtilen esaslar uygulanır.

4.8.7. Diğer Katılımcılarının Yeni Sertifika Üretimiyle İlgili Bilgilendirilmesi

EİMZATR tarafından NES üretimi sonrasında, sertifika sahibi dışında herhangi bir katılımcıya ayrıca sertifika üretim bildirimi yapılmaz.

4.9. Sertifika İptali ve Askıya Alma

4.9.1. Sertifika İptalini Gerektiren Durumlar

Nitelikli Elektronik Sertifika (NES), aşağıdaki durumlarda iptal edilir:

- Sertifika sahibinin veya sözleşme ile iptal talebinde bulunma yetkisi verilen kişinin geçerli iptal talebinde bulunması,

- EİMZATR tarafından, yürürlükteki mevzuat, NESİ veya NESUE hükümleri uyarınca sertifikanın iptalini gerektiren bir durumun tespit edilmesi,
- NES içerisinde yer alan bilgilerin yanlış veya gerçeğe aykırı olduğunun tespit edilmesi ya da sertifikanın geçerliliğini etkileyen bilgilerin değişmesi,
- NES içerisinde kurum, görev veya yetki bilgisinin bulunması hâlinde, bu bilginin dayanağını oluşturan yetki veya ilişkinin sona ermesi ya da değişmesi,
- Sertifika sahibine ait imza oluşturma verisinin veya güvenli elektronik imza oluşturma aracının kaybolması, çalınması, yetkisiz kişilerin erişimine maruz kalması, güvenilirliğinin tehlikeye girmesi veya güvenli kullanımının mümkün olmaması,
- EİMZATR'ye ait sertifika imzalama verisinin çalınması, kaybolması, gizliliğinin veya güvenilirliğinin ortadan kalkması ya da sertifika ilkelerinde ilgili NES'in iptalini gerektiren bir değişiklik meydana gelmesi,
- Sertifika sahibinin ölümü veya NES'in kullanılmasını ya da geçerliliğinin sürdürülmesini hukuken mümkün kılmayan bir durumun ortaya çıkması,
- Yürürlükteki mevzuat, NESİ, NESUE veya sertifika hizmetine ilişkin sözleşme hükümleri uyarınca NES'in iptal edilmesini gerektiren diğer durumların ortaya çıkması.

Geçerli iptal talebinin alınması veya iptali gerektiren durumun EİMZATR tarafından tespit edilmesi hâlinde NES derhal iptal edilir. İptal edilen NES geçmişe yönelik olarak iptal edilemez.

4.9.2. Sertifika İptal Talebinde Bulunabilecek Kişiler

"NES"ler aşağıda belirtilen kişiler tarafından iptal edilebilir "NES" sahibi

Yetkisi bulunması halinde kurumsal başvuru sahipleri

Yetkisi bulunması halinde üçüncü kişiler

"EİMZATR"

Yetkileri doğrultusunda kamu kurumları ve yargı makamları

4.9.3. Sertifika İptal Talebi Prosedürleri

NES iptal talepleri; sertifika sahibi, EİMZATR veya sözleşme ile iptal talebinde bulunma yetkisi verilen kişiler tarafından gerçekleştirilebilir.

İptal talepleri EİMZATR Çağrı Merkezi, yetkili başvuru/kayıt birimleri, yazılı başvuru ile talep edebilir veya EİMZATR Online İşlemler üzerinden kendisi yapabilir.

EİMZATR, iptal taleplerini telefon aracılığıyla kesintisiz olarak alınabilmesini sağlar.

İptal talebinde bulunan kişinin kimliği ve iptal talebinde bulunma yetkisi, kullanılan başvuru kanalına uygun doğrulama yöntemleriyle kontrol edilir.

İptal talebinin doğrulanmasının ardından ilgili NES derhal iptal edilir ve sertifika sahibi iptal işleminin gerçekleştiği konusunda bilgilendirilir.

İptal işleminin sonucu; işlemin gerçekleştirildiği kanala göre çağrı merkezi aracılığıyla, elektronik ortamda gösterilen işlem sonucu veya EİMZATR tarafından kullanılan diğer uygun iletişim yöntemleriyle bildirilir.

4.9.4. Sertifika İptal Talebi Gecikme Periyodu

Sertifika iptal talepleri işleme alındıktan sonra gecikme yaşanmaz ve yayınlanacak ilk "SİL"de yer alır.

4.9.5. EİMZATR'nin Sertifika İptal Talebini İşleme Süresi

Sertifika iptal talepleri onaylanması için hemen işleme alınır yayınlanacak ilk "SİL"de yer alır.

4.9.6. Üçüncü Kişilerin İptal Kontrol Gerekliliği

Üçüncü kişiler, güvenli elektronik imzaya veya bu imzanın dayandığı NES'e güvenmeden önce sertifikanın geçerlilik ve iptal durumunu kontrol etmekle yükümlüdür.

Sertifikanın geçerlilik ve iptal durumu, EİMZATR tarafından yayımlanan güncel Sertifika İptal Listesi (SİL), OCSP hizmeti veya ilgili mevzuata uygun güvenli elektronik imza doğrulama araçları kullanılarak kontrol edilir.

Sertifikanın iptal edilmiş olması, geçerlilik süresinin sona ermiş olması veya geçerlilik durumunun güvenilir şekilde doğrulanamaması halinde üçüncü kişiler söz konusu NES'e dayanarak işlem yapmamalıdır.

4.9.7. Sertifika İptal Listesi (SİL) Yayımlama Sıklığı

EİMZATR tarafından son kullanıcı NES'lerine ilişkin Sertifika İptal Listeleri (SİL), 5 dakikada bir yeniden oluşturularak yayımlanır. Yayımlanan SİL'lerin geçerlilik süresi 24 saattir.

EİMZATR alt kök sertifikalarına ilişkin Sertifika İptal Listeleri ise en az yılda bir kez yayımlanır. Alt kök sertifikalarından herhangi birinin iptal edilmesini gerektiren bir durumun ortaya çıkması halinde, belirlenen periyot beklenmeksizin güncel SİL yayımlanır.

4.9.8. SİL'lerin En Geç Yayımlanma Zamanı

"SİL"ler otomatik süreçler dahilinde oluşturulmalarının ardından hemen yayımlanır.

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

"EİMZATR" gerçek zamanlı sertifika iptal durumu kontrolü sağlayan OCSP hizmetini 7/24 ulaşılabilecek şekilde sağlar.

4.9.10. Çevrim İçi Sertifika İptal/Durum Kontrol Gereklilikleri

Üçüncü kişiler elektronik imzaya güvenerek bir iş veya işlem yapmadan önce "NES"in geçerlilik durumunu kontrol etmek zorundadırlar. Üçüncü kişiler "NES"in geçerlilik durumu kontrollerini "SİL" veya "OCSP" aracılığıyla kontrol etmelidirler.

4.9.11. Diğer İptal Durumu Yayımlama Çeşitlerinin Varlığı

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

4.9.12. Anahtar Güvenliğinin Yitirilmesine İlişkin Özel Gereklilikler

EİMZATR'ye ait bir güvenlik sorunu oluşması durumunda, durumdan etkilenen son kullanıcı sertifikaları EİMZATR tarafından iptal edilir EİMZATR ait kök veya alt kök sertifikalarının iptal edilmesi gerekirse, bu sertifikaların imzasını taşıyan son kullanıcı sertifikaları da iptal edilir ve kullanıcılar bilgilendirilir. Güvenlik sorunu ve sonuçları, EİMZATR tarafından ivedilikle kamuya açık bir şekilde web sitesi üzerinden ve gerekli durumlarda basın ve yayın organları aracılığıyla sertifika sahiplerine ve üçüncü kişilere duyurulur. EİMZATR'a ait bir güvenlik sorununun duyurulması durumunda, sertifika sahiplerinin sertifikalarını kullanmaya devam etmelerine izin verilmez. EİMZATR kaynaklı tüm sertifika iptal işlemlerinde, iptal sonrası yeni sertifika üretim işlemlerinin ivedilikle başlatılmasından EİMZATR sorumludur.

4.9.13. Sertifika Askıya Alma Gerektiren Durumlar

NES, sertifika sahibinin talebi üzerine veya EİMZATR tarafından sertifikanın güvenli kullanımını etkileyebilecek bir durumun tespit edilmesi hâlinde, durum açıklığa kavuşturuluncaya kadar geçici olarak askıya alınabilir.

4.9.14. Sertifika Askıya Alma Talebinde Bulunabilecek Kişiler

NES'in askıya alınması sertifika sahibi tarafından talep edilebilir. EİMZATR, gerekli gördüğü durumlarda yetkili personeli aracılığıyla NES'i askıya alabilir.

4.9.15. Sertifika Askıya Alma Talebi Prosedürü

Askıya alma ve askıdan çıkarma işlemleri, talepte bulunan kişinin kimliği ve yetkisi doğrulandıktan sonra EİMZATR tarafından gerçekleştirilir. EİMZATR tarafından başlatılan askıya alma işlemlerinde, askıya alma nedeninin ortadan kalktığının doğrulanması hâlinde NES askıdan çıkarılabilir.

4.9.16. Sertifikanın Askıda Kalma Süresinin Sınırları

NES en fazla 30 (otuz) gün süreyle askıda tutulabilir. Askıya alma nedeninin ortadan kalkması ve gerekli doğrulamaların tamamlanması hâlinde NES bu süre içerisinde askıdan çıkarılabilir.

Askıya alındığı tarihten itibaren 30 gün içerisinde askıdan çıkarılmayan NES, 30 günlük sürenin sonunda otomatik olarak iptal edilir.

4.10. Sertifika Durum Servisleri

EİMZATR tarafından oluşturulan Nitelikli Elektronik Sertifikaların geçerlilik ve iptal durumları, Sertifika İptal Listesi (SİL/CRL) ve Çevrim İçi Sertifika Durum Protokolü (OCSP) hizmetleri aracılığıyla sorgulanabilir.

4.10.1. İşlevsel Özellikler

EİMZATR 5 dkda 1 ve 24 (yirmidört) saatlik geçerlilik süresiyle, sertifika durumlarında hiçbir değişiklik olmasa bile yeni bir SİL yayımlar. EİMZATR, çevrim içi sertifika durum protokolü OCSP desteği verir. Bu sorguyla, gerçek zamanlı sertifika durum (geçerli, askıda, iptal, süresi dolmuş/bilinmiyor) bilgisi alınabilir.

4.10.2. Hizmetin Sürekliliği

EİMZATR, Bölüm 4.10.1 kapsamında sunulan Sertifika İptal Listesi (SİL) ve Çevrim İçi Sertifika Durum Protokolü (OCSP) hizmetlerini 7 gün 24 saat kesintisiz olarak sunar.

Sistem arızası, hizmet kesintisi, afet veya EİMZATR'nin kontrolü dışında gerçekleşen diğer olağanüstü durumlarda, sertifika durum hizmetlerinin sürekliliğinin sağlanması amacıyla iş sürekliliği ve felaket kurtarma süreçleri işletilir.

SİL ve OCSP hizmetlerinin kesintiye uğraması halinde hizmetlerin en geç 3 saat içerisinde yeniden erişilebilir hale getirilmesi hedeflenir.

İş sürekliliğinin sağlanması amacıyla gerekli durumlarda EİMZATR Felaket Kurtarma Merkezi (FKM) devreye alınır.

4.10.3. İsteğe Bağlı Özellikler

İlgili değildir.

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

EİMZATR, 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

İlgili değildir.

4.12.2. Oturum Anahtarı Zarflama ve Yeniden Oluşturma İlke ve Esasları

İlgili değildir.

5. TESİS, YÖNETİM VE İŞLETMEYLE İLGİLİ KONTROLLER

5.1. Fiziksel Kontroller

5.1.1. Tesis Yeri ve İnşaatı

EİMZATR 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

ESHS hizmetlerinin yürütüldüğü, kritik yazılım ve donanım bileşenlerinin bulunduğu alanlar ile elektronik ve fiziksel ortamda tutulan bilgi ve kayıtların bulunduğu bölümlere erişim yetkilendirme esasına göre sınırlandırılır.

Yetkisiz kişilerin bu alanlara erişimini engellemek amacıyla uygun fiziksel güvenlik kontrolleri uygulanır. Yetkili personelin erişimleri kayıt altına alınır; ziyaretçi ve üçüncü kişilerin erişimleri kontrollü ve yetkili personel gözetiminde gerçekleştirilir.

Fiziksel erişim yetkileri görev ve sorumluluklar doğrultusunda verilir, gerekli durumlarda gözden geçirilir ve yetkinin sona ermesi halinde kaldırılır.

5.1.3. Güç Kaynakları ve Havalandırma

ESHS hizmetlerinin sürekliliğinin sağlanması amacıyla kritik bilgi sistemleri kesintisiz güç kaynakları ile desteklenir. Sistemlerin bulunduğu alanlarda, donanımların güvenli çalışma koşullarının korunması amacıyla uygun sıcaklık ve çevresel koşullar iklimlendirme sistemleri ile sağlanır.

5.1.4. Su Baskınları

ESHS hizmetlerinin yürütüldüğü kritik alanlarda, sel, su baskını ve su sızıntısından kaynaklanabilecek risklere karşı gerekli fiziksel ve çevresel tedbirler alınır.

Kritik bilgi sistemlerinin bulunduğu alanlarda su sızıntısı ve su baskını risklerinin erken tespitine yönelik su algılama sensörleri kullanılır. Kritik sistem ve altyapı bileşenleri, su kaynaklı riskler dikkate alınarak konumlandırılır ve korunur.

5.1.5. Yangın Önleme ve Yangından Korunma

EİMZATR merkezinde, yangın ihbar sistemleri ile olası yangın durumlarına anında müdahale edilmesini sağlayacak söndürme sistemleri kurulmuştur.

5.1.6. Saklama Ortamları

EİMZATR faaliyetleri sırasında oluşturulan tüm kayıtların yedekleri uygun saklama ortamlarında tutulur.

5.1.7. Atıkların Atılması

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

5.1.8. Tesis Dışı Yedekleme

ESHS, sisteminin sürekliliğini sağlayabilmek amacıyla gerekli gördüğü bileşenleri, farklı bir fiziksel mekanda güvenli elektronik saklama ortamlarında muhafaza eder. Yedek sistemin bulunduğu mekan, asıl sistemin sağladığı tüm güvenlik ve işlevsellik şartlarını sağlar.

5.2. Prosedürel Kontroller

5.2.1. Güvenilir Roller

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

5.2.2. Her Görev İçin Gereken En Az Kişi Sayısı

EİMZATR bünyesinde güvenilir roller ve bu rollere ait yetkiler, görevlerin ayrılığı ve en az yetki prensipleri doğrultusunda belirlenir. Personelin sistem ve kaynaklara erişim yetkileri, görev ve sorumluluklarını yerine getirebilecekleri ölçüde sınırlandırılır.

Tek bir kişinin kontrolünde gerçekleştirilmesi güvenlik riski oluşturabilecek kritik kriptografik işlemlerde ikili kontrol uygulanır.

Özellikle EİMZATR'ye ait sertifika imzalama anahtarlarının oluşturulması ile bu anahtarların yedeklenmesi, saklanması ve geri yüklenmesine ilişkin işlemler en az iki güvenilir kişinin kontrolünde gerçekleştirilir.

Diğer işlemlerde görev alması gereken asgari kişi sayısı; işlemin niteliği, görev ayrılığı gereksinimleri, erişim yetkileri ve yapılan risk değerlendirmeleri doğrultusunda belirlenir.

5.2.3. Her Görev için Kimlik Doğrulama

Güvenilir rollere atanan personelin kimliği, kritik ESHS sistemlerine erişim öncesinde doğrulanır. Erişimler, kişilerin görev ve yetkileri ile sınırlandırılır ve gerçekleştirilen kritik işlemler ilgili kullanıcı ile ilişkilendirilerek kayıt altına alınır.

5.2.4. Görevlerin Ayrılmasını Gerektiren Roller

Sertifika yönetim süreçlerinde birbiriyle bağdaşmayan ve tek bir kişinin kontrolünde gerçekleştirilmesi güvenlik riski oluşturabilecek görevler, görevlerin ayrılığı ilkesi doğrultusunda farklı rollere atanır. Kritik işlemlerde gerekli yetkilendirme ve kontrol mekanizmaları uygulanarak aynı kişinin birbirini denetlemesi gereken işlemleri tek başına gerçekleştirmesi önlenir.

5.3. Personel Kontrolleri

5.3.1. Nitelik, Deneyim ve Güvenlik Gereklilikleri

"EİMZATR" Personel işe alımları ikiye ayrılmıştır. "Güvenli Personel" istihdamı, Genel personel istihdamı. "Güvenli Personel" "NES" üretimi hazırlanması gibi kritik görevlerde bulunmaktadır. "Güvenli Personel" istihdamı sırasında kişilerin adli sicil kayıtları ve sosyal yaşantılarındaki yerleri de dahil olmak üzere sıkı güvenlik kontrollerinden geçtikten sonra mesleki yeterlilik ve deneyim konularında ibraz edeceği belgelerle birlikte "Güven Merkezi" yöneticileri tarafından mülakata alınır. Personel adayları tüm bu denetimlerden geçtikten sonra uygun bulunursa istihdam edilir.

5.3.2. Kişisel Geçmiş Kontrol Gereklilikleri

Bakınız 5.3.1.

5.3.3. Eğitim Gereklilikleri

"EİMZATR" personelleri göreve başlamadan önce ESHS hizmetleri, sertifika yaşam zinciri hizmetleri, mesleki sorumluluklar, temel açık anahtar alt yapısı çerçevesi, "EİMZATR" güvenlik prosedürleri ve sertifika politikaları konularında gerekli hukuki ve teknik eğitimden geçirilirler.

5.3.4. Tekrar Eğitimi Sıklığı ve Gereklilikleri

"EİMZATR" Düzenli olarak eğitim içeriklerini kontrol eder ve güncelleme, değişiklik ya da uygun görülmesi halinde tazeleme eğitimleri düzenler.

5.3.5. İş Rotasyonu Sıklığı ve Sırası

İlgili değildir.

5.3.6. Yetkisiz İşlemler için Yaptırımlar

"EİMZATR" personelin ya da işbirlikçilerin güvenlik prosedürlerinin dışında işlem yapması veya "EİMZATR" ve kullanıcılarının bilgilerini tehlikeye sokacak, zarara uğratacak eylemlerde bulunmasını önlemek için gerekli mantıksal iş ayrımı ve gizlilik sözleşmeleriyle güvence altına almıştır. Yetkisiz eylemler veya süreç ihlali fiilleri Elektronik İmza Kanunu, Türk Ceza Kanunu veya ilgili diğer kanunlarda

belirtilen suç tanımlarına dahil olması durumunda bu eylemleri gerçekleştirenler hakkında gerekli yasal işlemler yapılır.

5.3.7. Bağımsız Alt Yüklenici Gereklilikleri

"EİMZATR", "ESHS" faaliyetlerini yürütmek için bağımsız yükleniciler ile hizmet sözleşmeleri akdedebilir Hizmet sözleşmeleri "EİMZATR"nın güvenlik ve işleyiş süreçlerine uyumlu olacak şekilde düzenlenir.

5.3.8. Personele Sağlanan Dokümantasyon

"EİMZATR" tüm personeline "NESUE", "NESİ" belgelerini ve görevleriyle ilgili özel nitelikli yazılım ve donanım kullanım kılavuzlarını verir.

5.4. Denetim Kayıtları Alma Prosedürleri

5.4.1. Kaydedilen Olay Tipleri

EİMZATR, ESHS faaliyetlerinin güvenliğinin, izlenebilirliğinin ve gerektiğinde doğrulanabilirliğinin sağlanması amacıyla, sertifika yönetimi ve bilgi sistemlerine ilişkin önemli olayları denetim kaydı olarak tutar.

Denetim kayıtları, gerçekleştirilen işlemin ve işlemi gerçekleştiren kişi veya sistemin gerektiğinde tespit edilmesine imkân sağlayacak şekilde oluşturulur.

5.4.2. Kayıtları İşleme Sıklığı

Kayıt tutma işlemi sürekli gerçekleşir. Kayıtlar ayda bir kere denetlenir. "EİMZATR" gerekli görmesi durumunda kayıt denetleme işleminin periyodunu değiştirebilir.

5.4.3. Denetim Kayıtlarının Saklanma Süresi

Denetim kayıtları işlendikten sonra veri depolama kapasitesine göre erişilebilir şekilde sistemde tutulur. İlgili mevzuata göre saklanması gereken bilgi ve belgeler ise 20 yıl boyunca saklanır.

5.4.4. Denetim Kayıtlarının Korunması

Elektronik ve kağıt ortamındaki denetim kaydı dosyalarına, yetkisiz kişilerin izlemesine, değişiklikler yapmasına, silmesine veya başka herhangi bir şekilde erişmesine karşı fiziksel ve mantıksal erişim kontrolleri kullanılır ve bu yolla denetim kaydı dosyaları korunur.

5.4.5. Denetim Kayıtlarının Yedeklenme Prosedürleri

İlgili prosedürler uyarınca, kayıtların periyodik olarak yedekleri alınır.

5.4.6. Denetim Bilgisi Toplama Sistemi (İç ve Dış)

Başvuru safhasında, ağ ve işletim sistemi seviyesinde, elektronik ortamda gerçekleşen işlemlerin denetim verileri otomatik olarak oluşturulur ve kaydedilir. Manuel olarak yapılan işlemlere ilişkin denetim verileri "EİMZATR" personelince manuel olarak kaydedilir.

5.4.7. Olayı Yaratan Kişiyi Bilgilendirme

Denetim bilgisi toplama sistemi bir olay kaydettiği zaman, olaya sebep olan birey, kurum veya görevliye ihbarda bulunmaya gerek yoktur. Ancak olayın niteliğine ve önem derecesine göre sistem ilgiliye ihbarda bulunabilir.

5.4.8. Zarar Görebilirlik Değerlendirmesi

Denetim kayıtlarının rutin olarak gözden geçirilmesi sonucunda sistemdeki ve süreçlerdeki güvenlik açıkları tespit edilerek gerekli olan önlemler alınır.

5.5. Kayıtların Arşivlenmesi

5.5.1. Arşivlenen Kayıt Tipleri

EİMZATR, ESHS faaliyetleri kapsamında oluşturulan ve sertifika yaşam döngüsünün, gerçekleştirilen işlemlerin ve mevzuata uyumun doğrulanması açısından gerekli olan kayıtları arşivler.

Bu kapsamda; sertifika başvuru ve kimlik doğrulama kayıtları, sertifika üretim, yenileme, değişiklik ve iptal işlemlerine ilişkin kayıtlar, denetim kayıtları, sertifika sahibiyle yapılan sözleşme ve ilgili belgeler, üretilen sertifikalar ve Sertifika İptal Listeleri (SİL) ile EİMZATR NESİ ve NESUE dokümanlarının ilgili sürümleri arşivlenir.

Kayıtlar, niteliğine uygun olarak elektronik ve/veya fiziksel ortamda muhafaza edilir.

5.5.2. Arşivlerin Saklanma Süresi

"Yönetmelik" ve ilgili mevzuat hükümleri doğrultusunda 5.4.1'de belirtilen kayıtlar en az 20 yıl süreyle saklanır.

5.5.3. Arşivlerin Korunması

Elektronik olarak arşivlenmiş veriler, uygun fiziksel ve mantıksal erişim kontrolleri kullanılarak, yetkisiz izleme, değiştirme, silme veya başka herhangi bir şekilde erişime karşı korunur. Manuel olarak girilen kâğıt ortamındaki bilgiler ise sadece yetkililerin erişebildiği fiziksel korumalı alanlarda saklanır.

5.5.4. Arşivlerin Yedeklenme Prosedürleri

"EİMZATR" gerekli gördüğü bilgi ve belgelerin yedeklerini, orijinalleriyle aynı güvenlik seviyesinde olmak şartıyla "Güven Merkezi" içinde ve/veya dışında tutabilir.

5.5.5. Kayıtların Zaman Damgası Altına Alınması Gereklilikleri

ESHS faaliyetleri kapsamında oluşturulan ve merkezi kayıt yönetim sisteminde arşivlenen denetim kayıtlarının bütünlüğü ve zaman bilgisinin doğrulanabilirliği, kriptografik bütünlük kontrolleri ve zaman damgası mekanizmaları kullanılarak güvence altına alınır. Kayıtların oluşturulmasında kullanılan sistem zamanları güvenilir zaman kaynakları ile senkronize edilir.

5.5.6. Arşiv Toplama Sistemi

Arşiv kayıtları, "E-İMZATR" yönetim sistemleri ve arşiv yönetim süreçleri kullanılarak elektronik ortamda veya yetkili personelin sorumluluğunda manuel olarak, ilgili prosedürlere uygun şekilde toplanır ve derlenir.

5.5.7. Arşiv Bilgisinin Edinilmesi ve Doğrulanması Prosedürleri

"NESUE", "NESİ" dokümanları ile son kullanıcı sözleşme örnekleri EİMZATR'ın resmî internet sitesindeki bilgi bankası alanında yayınlanmaktadır (https://e-imzatr.com.tr/tr/bilgi-bankasi/sozlesmeler). Gizli belgelere ise sadece "güvenli personel" ve Bilgi Teknolojileri ve İletişim Kurumu yetkilileri erişebilecektir. "NES" başvuruları ve "NES" sahiplerinin kimlik bilgilerine ise sadece kendisiyle ilgisi olmak şart ve koşuluyla kurumsal başvuru yetkilileri, "güvenli personel", kayıt işlemlerinden sorumlu yetkililer ve Bilgi Teknolojileri ve İletişim Kurumu yetkilileri erişebilecektir. Arşivde bulunan belgeler saklanma süresi boyunca okunabilir bir formatta tutulacaktır.

5.6. Anahtar Değişimi

"EİMZATR" "ESHS" imza oluşturma ve doğrulama verilerinin geçerlilik süreleri, ilgili mevzuatta belirtildiği üzere, en fazla 10 yıl olacaktır. Gerekli görülen durumlarda güvenlik sebebiyle ve "ESHS" imza oluşturma verisinin geçerlilik süresinin dolmasından önce "ESHS" imza oluşturma verisi yenilenir. Bu durumda eski anahtarlar (imza oluşturma ve doğrulama verileri) geçerlilik süresinin sonuna kadar kullanılabilir durumda saklanır. "ESHS"nin imza oluşturma verisinin değişiminden itibaren yeni oluşturulacak olan "NES"ler yeni imza oluşturma verisiyle imzalanır. Ancak eskiden oluşturulmuş olan "NES"lerin doğrulanabilmesi için eski imza doğrulama verisinin içinde bulunduğu eski "EİMZATR" "ESHS" kök sertifikası ve alt kök sertifikasının erişilebilirliği sağlanır. "EİMZATR" tebliğ ve yönetmelikler aksini belirtmediği takdirde 7 yılda bir anahtar değişimi gerçekleştirir.

5.7. Güvenliğin Yitirilmesi ve Felaket Kurtarma

5.7.1. Güvenlik Kaybına Neden Olabilecek Olaylar

“E-İMZATR” ESHS faaliyetlerinin güvenilirliğini veya sürekliliğini etkileyebilecek bir olay ya da güvenlik ihlali meydana gelmesi durumunda, bilgi güvenliği ihlal yönetimi ve iş sürekliliği prosedürleri kapsamında gerekli müdahaleler gerçekleştirilir.

Bu kapsamda, sistem güvenliğinin ve hizmet sürekliliğinin sağlanması amacıyla gerekli teknik ve idari önlemler alınır. Durumdan etkilenebilecek sertifika sahipleri ve ilgili kurumlar, gerekli görülmesi halinde uygun iletişim kanalları kullanılarak bilgilendirilir.

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

“Güven Merkezi”nde bulunan donanım, yazılım ve gerekli verilerin zarar görmesi veya kullanılamaz hale gelmesi durumunda, öncelikle yedek donanım ve yazılım sistemleri devreye alınır.

“İş Sürekliliği Yönetimi ve Felaketten Kurtarma Prosedürü” kapsamında, kaybolan veya zarar gören veriler yedekleme sistemlerinden geri yüklenir ve gerekli durumlarda yeniden oluşturulur.

Kurtarma işlemlerinin tamamlanamaması veya sertifika yönetim süreçlerinde geri döndürülemez bir durum oluşması halinde, etkilenebilecek sertifikalar ilgili prosedürlere uygun olarak iptal edilir. Bu durumdan etkilenen sertifika sahipleri ve ilgili taraflar, “E-İMZATR” tarafından ivedilikle bilgilendirilir.

5.7.3. İmza Oluşturma Verilerinin Güvenliğinin Yitirilmesi

“E-İMZATR” imza oluşturma verilerinin güvenliğinin veya güvenilirliğinin tehlikeye girmesi durumunda, “E-İMZATR” afet yönetimi prosedürleri ve iş sürekliliği planları kapsamında gerekli işlemleri gerçekleştirir.

Bu kapsamda, ilgili sertifikalar iptal edilir ve Madde 5.6 uyarınca yeni imza oluşturma verisi oluşturularak devreye alınır. İptal edilen sertifikaların yerine, ilgili prosedürlere uygun olarak yeni sertifikalar oluşturulur.

Gerçekleşen durumdan etkilenebilecek sertifika sahipleri ve üçüncü taraflar, “E-İMZATR” tarafından uygun iletişim kanalları kullanılarak ivedilikle bilgilendirilir.

5.7.4. İş Sürekliliği Yetenekleri ve Felaket Kurtarma

“EİMZATR” merkezi dışında felaket kurtarma merkezi (FKM) tesis etmiştir. Afet sonrasında iş sürekliliğini temin etmek üzere “EİMZATR” merkezinde bulunan veriler yedeklenir. “EİMZATR” işleyişini engelleyecek nitelikte olayların ya da güvenlik sorunlarının oluşması durumunda, “EİMZATR” iş sürekliliği prosedürü ve planı uyarınca duruma müdahale edilir.

5.7.5. EİMZATR’nin Faaliyetinin Son Bulması

“EİMZATR”'nin faaliyetlerinin son bulması halinde, Kanun ve Yönetmelik gereği bu durumu en az 3 ay önce Kuruma bildirir ve kamuoyuna duyurur. “EİMZATR”, 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, “EİMZATR” ilgili sertifikaları iptal eder ve tüm ilgili tarafları bu durumdan haberdar eder. Bu durumda, “EİMZATR” son SİL kaydını oluşturduktan sonra kendi imza oluşturma verisi ile yedeklerini imha eder.

6. TEKNİK GÜVENLİK KONTROLLERİ

6.1. Anahtar Çifti Üretimi ve Kurulumu

6.1.1. Anahtar Çifti Üretimi

“E-İMZATR” kök ve alt kök sertifikalarına ait imza oluşturma ve doğrulama verileri, güvenliği ve gerekli kriptografik dayanıklılığı sağlayan güvenilir sistemler kullanılarak, yetkilendirilmiş birden fazla “Güvenli Personel” ve ilgili görevlilerin katılımıyla oluşturulur.

“E-İMZATR” kök sertifikasına ait anahtar çiftlerinin oluşturulmasında kullanılan kriptografik donanım modülleri, FIPS 140-2 Seviye 3 güvenlik gerekliliklerini karşılar. Anahtar oluşturma işlemleri, “Tebliğ”de belirtilen algoritma ve standartlara uygun olarak gerçekleştirilir ve gerçekleştirilen işlemler kayıt altına alınarak denetim ve izleme amacıyla saklanır.

İmza oluşturma verileri, “E-İMZATR” güvenli elektronik imza oluşturma araçlarında oluşturulur ve yedekleme amacı dışında cihaz dışına çıkarılamaz. İmza oluşturma verilerinin yetkisiz erişime karşı korunması amacıyla gerekli fiziksel ve teknik güvenlik önlemleri uygulanır.

İmza oluşturma verilerinin yedeklenmesi, yetkili personel tarafından güvenli yöntemlerle gerçekleştirilir ve güvenli ortamlarda saklanır. Anahtar çiftlerinin kullanım süreleri, yürürlükteki mevzuat ve güvenlik standartlarına uygun olarak belirlenir. Sertifika geçerlilik süresi sona ermeden önce gerekli görülmesi halinde yeni anahtar çifti ve sertifika oluşturularak hizmet sürekliliği sağlanır.

6.1.2. İmza Oluşturma Verisinin Sertifika Sahibine Ulaştırılması

İmza oluşturma verileri, “NES” sahiplerine güvenli elektronik imza oluşturma aracı içerisinde, gerekli güvenlik önlemleri alınarak teslim edilir.

“E-İMZATR” tarafından hazırlanan güvenli elektronik imza oluşturma araçları, sertifika sahibine yetkili kayıt noktaları aracılığıyla elden veya güvenli kargo hizmetleri kullanılarak ulaştırılabilir. Teslim işlemi sırasında sertifika sahibinin kimlik doğrulaması yapılır ve teslim bilgileri kayıt altına alınır.

6.1.3. İmza Doğrulama Verisinin ESHS'ye Ulaştırılması

İmza doğrulama verileri güvenli aktarım protokolleri kullanılarak “EİMZATR” veri tabanına kaydedilir.

6.1.4. EİMZATR İmza Doğrulama Verilerinin Üçüncü Kişilere Ulaştırılması

“E-İMZATR” kök ve alt kök sertifikaları, üçüncü kişilerin erişimine açık olacak şekilde “E-İMZATR” tarafından yayımlanan resmî internet adresi üzerinden yayımlanır.

Bu sayede, “E-İMZATR” tarafından oluşturulan güven zincirine ait imza doğrulama verileri, ilgili taraflar tarafından sertifika doğrulama işlemlerinde kullanılabilir.

6.1.5. Anahtar Uzunlukları

“E-İMZATR” tarafından oluşturulan sertifikalarda kullanılan anahtar uzunlukları, “Tebliğ”de belirtilen asgari güvenlik gerekliliklerine uygundur.

“E-İMZATR” kök ve alt kök sertifikalarına ait imza oluşturma ve doğrulama verileri, güvenlik gerekliliklerine uygun anahtar uzunlukları kullanılarak oluşturulur. Bu kapsamda kök ve alt kök sertifikalarda kullanılan anahtar çiftleri, yürürlükteki mevzuat ve güvenlik politikalarında belirtilen kriptografik gereklilikleri karşılar.

“E-İMZATR” tarafından üretilen NES’lerde kullanılan imza oluşturma ve doğrulama verileri en az 2048 bit RSA anahtar uzunluğuna ve 384 bit ve üstü ECDSA teknik standartları seviyesine sahip algoritmalara dayanır.

Sertifikalarda kullanılan özetleme algoritmaları ve kriptografik algoritmalara ilişkin bilgiler, ilgili NESİ dokümanında belirtilen teknik gerekliliklere uygun olarak uygulanır.

6.1.6. Anahtar Üretimi ve Kalite Kontrolü

“E-İMZATR” tarafından NES’lere ait anahtar çiftleri, “Tebliğ”de belirtilen güvenlik gerekliliklerine uygun olarak “Güven Merkezi” içerisinde bulunan güvenli kriptografik donanım modülleri üzerinde oluşturulur.

6.1.7. Anahtar Kullanım Amaçları

“E-İMZATR” tarafından üretilen NES’lere ait imza oluşturma ve doğrulama verileri yalnızca güvenli elektronik imza oluşturma ve doğrulama amaçlarıyla kullanılır.

“E-İMZATR” kök ve alt kök sertifikalarına ait imza oluşturma ve doğrulama verileri; NES imzalama, SİL imzalama, ÇSDP (OCSP) hizmetlerine ait sertifikaların imzalanması ve ilgili güven altyapısı kapsamında kullanılan sertifikaların imzalanması amaçlarıyla kullanılabilir.

“E-İMZATR” tarafından kullanılan ÇSDP (OCSP) hizmet sertifikalarına ait anahtarlar, OCSP cevaplarının imzalanması amacıyla kullanılır. Zaman damgası hizmetlerinde kullanılan sertifikalara ait anahtarlar ise ilgili zaman damgası hizmetlerinin güvenli şekilde yürütülmesi amacıyla kullanılır.

6.2. İmza Oluşturma Verisinin Korunması ve Kriptografik Modül Mühendislik Kontrolleri

6.2.1. Kriptografik Modül Standartları ve Kontroller

"EİMZATR'ye ait anahtar çifti üretimi ile sertifika ve SİL imzalama işlemleri, Tebliğ’le belirlenen standartlarla uyumlu, güvenli kriptografik donanım modüllerinde gerçekleştirilir. Satın alma sonrası donanım güvenlik modülünün ilk kullanımından önce, sevkiyat ve depolama sırasında cihazların zarar görmediğinden emin olmak için kontroller uygulanır. Cihazların kabulü sırasında fabrika paketlemesi ve güvenlik mühürleri kontrol edilir ve cihazlar fiziksel ve teknik bakımdan güvenliği sağlanmış alanlarda saklanır ve kullanılır. Cihazların tüm kullanım ömürleri boyunca, cihazlar işlevsellikleriyle ilgili sürekli kontrol altında tutulur ve herhangi bir güvenlik ihlali durumu bilgi güvenliği ihlal olayı prosedürü uyarınca yönetilir. NES sahiplerinin imza oluşturma verileri "EİMZATR" tarafında üretildiğinde, Tebliğ’le belirlenen standartlarda güvenlik düzeyine sahip akıllı kartlara, akıllı çubuklara ve benzeri güvenli elektronik imza oluşturma araçlarına yüklenir. Güvenli elektronik imza oluşturma araçlarındaki imza oluşturma verilerinin dışarıya çıkarılması, değiştirilmesi veya kopyalanması engellenmiştir. Sertifika başvuru sahibinin kendi tarafında anahtar üretimi yapması durumunda, yine Tebliğ’de tanımlı güvenlik düzeyine sahip bir araç kullanılmalıdır.

6.2.2. İmza Oluşturma Verisinin Çok Kullanıcılı Kontrolü

“E-İMZATR” kök ve alt kök sertifikalarına ait imza oluşturma verilerine erişim yalnızca yetkilendirilmiş “Güvenli Personel” tarafından gerçekleştirilebilir. Yetkisiz kişilerin bu verilere fiziksel veya teknik olarak erişimi engellenir.

“ESHS” imza oluşturma verilerinin kullanımı, gerekli kimlik doğrulama ve güvenlik prosedürlerinin yerine getirilmesi ile mümkün olur. Kritik imza oluşturma verilerine erişim ve kullanım işlemleri, birden fazla yetkili “Güvenli Personel”in katılımı ve onayı ile gerçekleştirilir; hiçbir yetkili personelin tek başına bu verileri kullanmasına izin verilmez.

NES sahiplerine ait imza oluşturma verileri, yalnızca sertifika sahibinin kontrolündeki güvenli elektronik imza oluşturma araçlarında saklanır. Bu veriler, ilgili aracın erişim şifresi/PIN bilgisi ile korunur ve şifre doğrulanmadan kullanılamaz. İmza oluşturma verilerinin güvenliği, güvenli elektronik imza oluşturma aracının teknik güvenlik mekanizmaları ile sağlanır.

6.2.3. İmza Oluşturma Verisinin Saklanması

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

6.2.4. İmza Oluşturma Verisinin Yedeklenmesi

"EİMZATR" "NES" sahiplerine ait imza oluşturma verilerinin yedeklerini almaz. "EİMZATR" "ESHS" imza oluşturma ve doğrulama verilerini yedekleme işlemi birden çok yetkili "Güvenli Personel" ile anahtar töreni sırasında kriptografik kartlara yüklenerek farklı lokasyonlardaki kasalarda saklanır.

6.2.5. İmza Oluşturma Verisinin Arşivlenmesi

"EİMZATR" "ESHS" kök sertifikalarına ait imza oluşturma verileri arşivlenmez, imza doğrulama verileri ve kök sertifikalar ise ileride çıkması muhtemel uyuşmazlıklarda kullanılmak üzere 20 yıl süreyle saklanır. "EİMZATR", "NES" sahiplerinin imza oluşturma verilerini arşivlemez.

6.2.6. İmza Oluşturma Verisinin Kriptografik Modül Transferi

"EİMZATR", "ESHS" kök sertifikalarının imza oluşturma ve doğrulama verilerini, "ESHS"ye ait olan güvenli elektronik imza oluşturma aracı içerisinde (kriptografik modül) oluşturur. "ESHS" imza oluşturma verisi yedekleme amacı dışında kesinlikle "ESHS" güvenli elektronik imza oluşturma aracından çıkarılamaz. Yedekleme amacıyla imza oluşturma verisinin başka bir kriptografik modüle transferi gerekli teknik ve fiziksel güvenlik önlemleri altında sadece birden çok yetkili "Güvenli Personel" tarafından gerçekleştirilebilir. "NES" sahiplerine ait imza oluşturma verileri güvenli elektronik imza oluşturma araçlarında oluşturulur ve oluşturuldukları güvenli elektronik imza oluşturma aracı dışarısına kesinlikle çıkarılamaz.

6.2.7. İmza Oluşturma Verisinin Kriptografik Modülde Saklanması

6.2.6 da anlatılmıştır.

6.2.8. Gizli Anahtarın Aktive Edilme Yöntemi

"EİMZATR" "ESHS" kök sertifikaları imza oluşturma verilerinin aktivasyonu gerekli teknik ve fiziksel güvenlik önlemleri altında sadece birden çok yetkili "Güvenli Personel" tarafından gerçekleştirilebilir. "NES" sahiplerine ait imza oluşturma verisinin aktivasyonu güvenli elektronik imza oluşturma aracına erişim verisinin girilmesiyle sağlanır.

6.2.9. Gizli Anahtarın Deaktive Edilme Yöntemi

"ESHS" imza oluşturma verilerinin pasif hale getirilmesi işlemi cihazlar aktif durumdayken en az iki yetkili "Güvenilir Personel" tarafından gerçekleştirilir.

6.2.10. Gizli Anahtarı Yok Etme Metodu

"E-İMZATR" tarafından kullanılan kök ve alt kök sertifikalarına ait imza oluşturma verileri ile diğer kritik kriptografik veriler, yaşam döngülerinin sona ermesinin ardından güvenli imha prosedürleri doğrultusunda yetkili güvenli personel tarafından imha edilir.

İmha işlemleri sırasında kriptografik donanım modüllerinin güvenli anahtar silme özelliklerinden yararlanılır ve gerçekleştirilen tüm işlemler kayıt altına alınır. Kritik imha işlemleri, gerekli durumlarda en az iki yetkili personelin kontrolü ve katılımı ile gerçekleştirilir.

NES sahiplerine ait imza oluşturma verileri, güvenli elektronik imza oluşturma aracından silinerek veya ilgili donanımın güvenli şekilde imha edilmesiyle kullanılamaz hale getirilir.

6.2.11. Kriptografik Modül Değerlendirmesi

"E-İMZATR" tarafından kullanılan güvenli elektronik imza oluşturma araçları ile NES sahiplerine sağlanan güvenli elektronik imza oluşturma araçları, "Tebliğ"de belirtilen güvenlik gerekliliklerine ve standartlara uygundur.

"E-İMZATR" kök ve alt kök sertifikalarına ait imza oluşturma verileri, "Tebliğ"de tanımlanan güvenlik seviyesine sahip güvenli kriptografik donanım modüllerinde oluşturulur ve saklanır. NES sahiplerine ait imza oluşturma verileri ise, güvenli elektronik imza oluşturma araçları içerisinde güvenli şekilde muhafaza edilir.

6.3. Anahtar Çifti Yönetimiyle İlgili Diğer Konular

6.3.1. İmza Doğrulama Verilerinin Arşivlenmesi

"E-İMZATR" tarafından oluşturulan kök ve alt kök sertifikaları, son kullanıcı NES'leri ve bunlara ilişkin imza doğrulama verileri, yürürlükteki mevzuat ve arşivleme yükümlülükleri doğrultusunda en az 20 (yirmi) yıl süreyle güvenli şekilde saklanır.

6.3.2. Sertifikanın İşlevsel Süreleri ve Anahtar Çifti Kullanım Süreleri

"E-İMZATR" tarafından üretilen NES'lerin geçerlilik süreleri, başvuru sahibinin tercihine ve yürürlükteki hizmet koşullarına bağlı olarak sözleşmelerinde belirtilir. Aynı anahtar çifti ile kullanılan bir NES'in geçerlilik süresi, yürürlükteki mevzuat ve güvenlik gereklilikleri dikkate alınarak belirlenir.

"E-İMZATR" kök ve alt kök sertifikalarının geçerlilik süreleri 10 (on) yılı aşmaz. Bu sertifikaların yenilenmesi sırasında gerekli durumlarda yeni anahtar çiftleri oluşturularak güvenli anahtar yönetimi ilkelerine uygun şekilde işlem gerçekleştirilir.

NES'in geçerlilik süresinin sona ermesi, geçerlilik süresi içerisinde oluşturulmuş güvenli elektronik imzaların doğrulanmasını engellemez. İmza doğrulama verileri, ilgili mevzuat ve teknik standartlar çerçevesinde kullanılmaya devam edebilir.

6.4. Erişim Şifreleri

6.4.1. Erişim Şifrelerinin Oluşturulması ve Kurulumu

Erişim şifresi; gizli anahtarların kullanımında yararlanılan parola, PIN veya benzeri gizli doğrulama verilerini ifade eder.
"E-İMZATR" kök ve alt kök sertifikalarına ait imza oluşturma verileri, güvenli kriptografik donanımlarda saklanır ve yalnızca en az iki yetkili güvenli personelin kriptografik kimlik doğrulaması ile birlikte kullanılabilir.

NES sahiplerine ait erişim verileri, sertifika üretimi sırasında güvenli yöntemlerle oluşturulur ve güvenli şekilde korunur. Aktivasyon işlemi sırasında NES sahibi, PIN kodunu kendisi belirler. Kullanıcı tarafından belirlenen PIN kodu "E-İMZATR" tarafından saklanmaz ve hiçbir şekilde üçüncü kişilerle paylaşılmaz.

6.4.2. Erişim Şifrelerinin Korunması

Erişim verilerinin NES sahiplerine ve güvenli personele teslim edilmesinden sonra, bu verilerin gizliliğinin ve güvenliğinin korunmasına ilişkin sorumluluk ilgili kişilere aittir. NES sahipleri, kendilerine tahsis edilen erişim şifrelerini ve güvenli elektronik imza oluşturma aracına ait erişim bilgilerini yetkisiz kişilere açıklamamak, güvenli şekilde muhafaza etmek ve bilgi güvenliği kurallarına uygun olarak kullanmakla yükümlüdür.

6.4.3. Erişim Şifreleriyle İlgili Diğer Konular

"E-İMZATR" tarafından sunulan NES aktivasyon yönteminde, güvenli elektronik imza oluşturma aracına ilişkin erişim şifresi elektronik veya fiziksel hiçbir ortamda açık şekilde saklanmaz ya da iletilmez. NES aktivasyon kodu, "E-İMZATR" sistemlerinde güvenli kriptografik yöntemlerle korunur ve yalnızca yetkili süreçler tarafından erişilebilir şekilde muhafaza edilir.

NES aktivasyon işlemi, yalnızca sertifika sahibinin güvenli elektronik imza oluşturma aracını kullanarak aktivasyon talebinde bulunması halinde gerçekleştirilir. Aktivasyon sürecinde sertifika sahibi ile "E-İMZATR" sistemleri arasındaki veri iletişimi güvenli ve şifreli haberleşme kanalları üzerinden sağlanır

6.5. Bilgisayar Güvenlik Kontrolleri

6.5.1. Bilgisayar Güvenliği Teknik Gereklilikleri

"EİMZATR" 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, "EİMZATR" 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.

6.5.2. Bilgisayar Güvenliğinin Derecelendirilmesi

İlgili değildir.

6.6. Yaşam Döngüsü Teknik Kontrolleri

6.6.1. Sistem Geliştirme Kontrolleri

"E-İMZATR" sertifika yaşam döngüsüne ilişkin sistem geliştirme kontrollerini, kalite yönetim sistemi prosedürleri ile TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi kapsamında belirlenen kontroller doğrultusunda yürütür.

Sistem geliştirme faaliyetlerinde geliştirme tesisi güvenliği, geliştirme ortamının güvenliği, geliştirme personelinin yetkilendirilmesi, ürün bakım süreçlerinde konfigürasyon yönetimi ve yazılım geliştirme metodolojisine ilişkin güvenlik kontrolleri uygulanır. Geliştirme ve bakım süreçlerinde tespit edilen riskler uygun risk azaltma yöntemleriyle yönetilir.

Sistem geliştirme, değişiklik yönetimi ve konfigürasyon yönetimine ilişkin usul ve esaslar ilgili politika ve prosedürlerde dokümante edilir ve kontrollü şekilde uygulanır.

6.6.2. Güvenlik Yönetimi Kontrolleri

"E-İMZATR" işlevsel sistemlerinin ve bilgi işlem altyapısının güvenliğinin sağlanması amacıyla uygun teknik ve idari güvenlik kontrollerini uygular ve bilgi güvenliği prosedürlerini işletir. Bilgisayar ağı, yetkisiz erişimlere ve güvenlik tehditlerine karşı gerekli koruma mekanizmaları ile güvence altına alınır.

"E-İMZATR", TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi standardı doğrultusunda faaliyetlerini yürütür ve bu kapsamda düzenli denetimler gerçekleştirir. Sistemlerde değişiklik yapılması gerektiğinde öncelikle ihtiyaç belirlenir, ilgili değişiklik talebi yazılı olarak yönetime iletilir ve gerekli onayların alınmasının ardından değişiklik kayıt altına alınarak kontrollü şekilde uygulanır.

6.6.3. Yaşam Döngüsü Güvenlik Kontrolleri

İlgili değildir.

6.7. Ağ Güvenlik Kontrolleri

"E-İMZATR" bilgi sistemlerinde kullanılan güvenlik duvarları, ağ anahtarları, yönlendiriciler ve diğer ağ bileşenleri, güvenli ağ yapılandırma prosedürlerine uygun olarak kurulup işletilir ve düzenli olarak güvenlik kontrollerine tabi tutulur.

Kayıt Birimleri (KB) ile Güven Merkezi arasındaki veri iletişimi güvenli iletişim kanalları üzerinden gerçekleştirilir. Bu bağlantılar saldırılara karşı gerekli güvenlik önlemleri ile korunur ve kullanılan

sistemler “ESHS” hizmetleri dışında kalan yetkisiz sorgu ve erişim taleplerini reddedecek şekilde yapılandırılır.

6.8. Zaman Damgası

“E-İMZATR” tarafından sertifika hizmetlerinin yürütülmesi sırasında gerçekleştirilen işlemlere ilişkin elektronik kayıtlar, zaman damgası hizmetlerinde kullanılan güvenilir zaman kaynağı ile senkronize edilmiş zaman bilgisi içerir. Kayıtların bütünlüğü uygun kriptografik yöntemlerle korunur ve arşivleme işlemlerinde zaman damgası kullanılır.

Zaman Damgası hizmetine ilişkin bağlantılar için gerekli bilgi güvenliği önlemleri uygulanır. Bu kapsamda kullanılan sistem ve ekipmanlar, “ESHS” hizmetleri dışında gelen yetkisiz sorgu ve erişim taleplerini reddedecek şekilde yapılandırılır.

7. SERTİFİKA, SERTİFİKA İPTAL LİSTESİ (SİL) VE ÇSDP(OCSP) PROFİLLERİ

7.1. Sertifika Profili

7.1.1. Sürüm Numaraları

EİMZATR tarafından oluşturulan kök ve alt kök sertifikalar ile son kullanıcı Nitelikli Elektronik Sertifikaları (NES), yürürlükteki elektronik imza mevzuatı, ilgili BTK sertifika profilleri ve RFC 5280 hükümlerine uygun olarak X.509 v3 formatında oluşturulur.

7.1.2. Sertifika Uzantıları

EİMZATR tarafından oluşturulan Nitelikli Elektronik Sertifikalarda yer alan alan ve uzantılar; yürürlükteki elektronik imza mevzuatı, Bilgi Teknolojileri ve İletişim Kurumu tarafından yayımlanan Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri ile RFC 5280'de belirtilen esaslara uygun olarak oluşturulur.

7.1.3. Algoritma Nesne Tanımlayıcıları

EİMZATR tarafından oluşturulan sertifikalarda kullanılan kriptografik algoritmalar ve bunlara ilişkin nesne tanımlayıcıları (OID), yürürlükteki elektronik imza mevzuatı ve ilgili teknik standartlara uygun olarak belirlenir ve üretilen sertifikaların içeriğinde belirtilir.

7.1.4. İsim Biçimleri

“E-İMZATR” tarafından üretilen NES’lerde yer alan ayırt edilebilir isim (Distinguished Name) bilgileri X.500 standardına uygun biçimde oluşturulur.

7.1.5. İsim Kısıtları

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

7.1.6. Sertifika İlkeleri Nesne Tanımlayıcısı

“EİMZATR" tarafından üretilen sertifikaların “sertifika ilkeleri” uzantısında, sertifikanın çeşidine göre bu NESİ dokümanı Madde 1.2.’de belirtilen ilgili sertifika ilkeleri nesne tanımlayıcı numarası (OID) kullanılır.

7.1.7. İlke Kısıtları Uzantısının Kullanımı

“EİMZATR" alt kök sertifikalarında ihtiyaca göre ilke kısıtları uzantısı kullanabilir.

7.1.8. İlke Niteleyicilerinin Yazımı

“E-İMZATR” tarafından üretilen sertifikaların “sertifika ilkeleri” uzantısında, ilke niteleyicisi olarak NESUE dokümanına erişim sağlayan URL bilgisi yer alır.

7.1.9. Kritik Sertifika İlkeleri Uzantısının İşlenme Semantiği

İlgili değildir.

7.2. SİL Profili

“E-İMZATR” tarafından yayımlanan SİL’lerde temel olarak; “E-İMZATR” elektronik imzası ile birlikte yayımlayıcı bilgileri, SİL’in yayımlanma tarihi, bir sonraki SİL’in yayımlanma tarihi, iptal edilen sertifikaların seri numaraları ile iptal tarih ve zaman bilgileri yer alır.

“E-İMZATR” tarafından yayımlanan SİL’ler, Bilgi Teknolojileri ve İletişim Kurumu tarafından yayımlanan “Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri” dokümanına uygundur.

7.2.1. Sürüm Numarası

“E-İMZATR” 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

“EİMZATR” tarafından yayımlanan SİL’lerde, RFC 5280 tarafından tanımlanan uzantılar kullanılır.

7.3. OCSP Profili

““E-İMZATR” gerçek zamanlı bir sertifika durum sorgulama hizmeti olan ÇSDP (OCSP) desteğini kesintisiz olarak sağlar.

Bu hizmet kapsamında, uygun sertifika durum sorgularının alınması halinde, sorguda talep edilen sertifikaların güncel durum bilgileri ve protokol kapsamında sağlanması gereken diğer bilgiler, sorgu cevabı olarak talep sahibine iletilir.

“E-İMZATR” tarafından sunulan ÇSDP (OCSP) hizmetine ilişkin cevap mesajları, Bilgi Teknolojileri ve İletişim Kurumu tarafından yayımlanan “Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri” dokümanında belirtilen gerekliliklere uygundur.

7.3.1. Sürüm Numarası

“E-İMZATR” tarafından sunulan ÇSDP (OCSP) hizmeti, “IETF RFC 6960 Internet X.509 Public Key Infrastructure Online Certificate Status Protocol - OCSP” dokümanı uyarınca OCSP v1 protokol sürümünü destekler.

7.3.2. OCSP Uzantıları

“E-İMZATR” tarafından sunulan OCSP hizmeti kapsamında, RFC 6960 standardında tanımlanan OCSP uzantıları kullanılabilir. Ancak, temel OCSP yanıt bilgileri dışında kalan tüm uzantıların kullanılması zorunlu değildir.

8. UYGUNLUK DENETİMİ VE DİĞER DEĞERLENDİRMELER

8.1. Denetim Sıklığı ve Durumları

Bilgi Teknolojileri ve İletişim Kurumu, düzenleyici ve denetleyici kurum olarak Kanun kapsamında gerekli gördüğü durumlarda “E-İMZATR”nin elektronik sertifika hizmet sağlayıcılığı faaliyetlerine ilişkin denetimler gerçekleştirebilir.

Denetimler sırasında, Kurum tarafından yetkilendirilen görevlilerin talep ettiği bilgi, belge, kayıt ve dokümanların sunulması; gerekli görülen durumlarda hizmetlerin yürütüldüğü alanlara, sistemlere ve

ilgili altyapılara erişim sağlanması; yazılı ve sözlü bilgi verilmesi ile inceleme ve değerlendirme faaliyetlerinin yürütülmesi "E-İMZATR" tarafından sağlanır.

TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi kapsamında gerçekleştirilen uygunluk denetimleri, ilgili belgelendirme kurallarına uygun olarak yürütülür. Uygulanması halinde ilgili yönetim sistemi denetimleri kapsamında takip denetimleri ve belge yenileme denetimleri gerçekleştirilir.

"E-İMZATR" tarafından gerçekleştirilen iç denetimler, belirlenen denetim planları doğrultusunda bilgi güvenliği, elektronik sertifika hizmetleri, "NESİ", "NESUE" ve ilgili süreçlerin uygunluğunu değerlendirmek amacıyla düzenli olarak yürütülür.

8.2. Denetçinin Kimliği ve Özellikleri

Bilgi Teknolojileri ve İletişim Kurumu, 5070 sayılı Elektronik İmza Kanunu kapsamında elektronik sertifika hizmet sağlayıcılığı faaliyetleri üzerinde düzenleme ve denetim yetkisine sahip kurumdur.

"E-İMZATR"nin bilgi güvenliği denetim aşamaları, yetkilendirilmiş ve bağımsız denetçiler tarafından gerçekleştirilir.

"E-İMZATR"nin kurumsal iç denetimleri, yetkilendirilmiş "E-İMZATR" personeli tarafından gerçekleştirilir. İç denetim faaliyetleri; Bilgi Güvenliği Yönetim Sistemi, "NESİ", "NESUE" ve ilgili politika/prosedürler kapsamında değerlendirilir.

İç denetim sonuçları ilgili sorumlular tarafından incelenir ve gerekli görülen durumlarda düzeltici faaliyetler başlatılır.

8.3. Denetçinin ESHS'yle İlişkisi

Bilgi Teknolojileri ve İletişim Kurumu, 5070 sayılı Elektronik İmza Kanunu kapsamında Türkiye'de elektronik sertifika hizmet sağlayıcılığı faaliyetinde bulunan ESHS'leri denetlemeye yetkili düzenleyici kurumdur. "E-İMZATR"nin elektronik sertifika hizmetlerine ilişkin mevzuat, "NESİ" ve "NESUE" hükümlerine uygunluğu kapsamında gerçekleştirilen dış denetimler, yetkili ve bağımsız denetçiler tarafından yürütülür.

TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi ve uygulanabilir diğer yönetim sistemi denetimleri, tarafsız ve bağımsız değerlendirme sağlayacak şekilde yetkili denetçiler tarafından gerçekleştirilir. Denetçiler ve denetimi gerçekleştiren kuruluşlar ile "E-İMZATR" arasında denetimin tarafsızlığını etkileyebilecek mali, hukuki veya benzeri bir ilişki bulunmaması esastır.

"E-İMZATR"nin kurumsal iç denetimleri, yetkilendirilmiş "E-İMZATR" güvenli personeli tarafından gerçekleştirilir. İç denetim faaliyetlerinde mevzuat, "NESİ", "NESUE" ve ilgili güvenlik politikalarına uygunluk değerlendirilir.

8.4. Denetimde Kapsanan Başlıklar

Bilgi Teknolojileri ve İletişim Kurumu tarafından yapılan denetimlerde "NESİ" de belirtilen özelliklere uygun hizmet verildiğinin kontrolü gerçekleştirilir.

TS ISO/IEC 27001 sertifikasına ilişkin denetimlerde "EİMZATR" "Güven Merkezi" operasyonları ve "ESHS" işleyişine ilişkin süreçler denetlenir.

8.5. Eksiklik Durumunda Yapılacaklar

Yönetmelik gereği Bilgi Teknolojileri ve İletişim Kurumu tarafından gerçekleştirilen denetimler sırasında, "E-İMZATR"nin elektronik sertifika hizmet sağlayıcılığı faaliyetlerini ve işleyişini olumsuz yönde etkileyebilecek nitelikte önemli hususların tespit edilmesi halinde, ilgili mevzuatta öngörülen yaptırım ve cezalar uygulanır.

Denetimlerde tespit edilen küçük veya minör nitelikteki eksiklikler, belirlenen süreler içerisinde "E-İMZATR" tarafından giderilir.

"E-İMZATR" tarafından gerçekleştirilen iç denetimlerde belirlenen uygunsuzluklar için düzeltici ve önleyici faaliyetler yürütülür, sonuçlar ilgili yetkililer tarafından değerlendirilir.

8.6. Sonuçların Bildirilmesi

"E-İMZATR"nin elektronik sertifika hizmet sağlayıcılığı faaliyetleri kapsamında gerçekleştirilen denetimler, 5070 sayılı Elektronik İmza Kanunu, ilgili mevzuat hükümleri ve uygulanabilir standartlar doğrultusunda yürütülür.

Bilgi Teknolojileri ve İletişim Kurumu tarafından gerçekleştirilen denetimlerin sonuçları, gerekli görülmesi halinde resmî yollarla "E-İMZATR"ye bildirilir. Kurum tarafından ayrıca bir geri bildirimde bulunulmaması, olumsuz bir değerlendirmenin bulunmadığı şeklinde yorumlanmaz.

"E-İMZATR" tarafından uygulanan bilgi güvenliği süreçlerine ilişkin denetim sonuçları ilgili denetim raporlarında kayıt altına alınır ve yetkili kişilerin değerlendirmesine sunulur.

İç denetim sonuçları, iç denetim raporları aracılığıyla kayıt altına alınır ve gerekli iyileştirme faaliyetlerinin yürütülmesi amacıyla ilgili yetkililer tarafından değerlendirilir.

Denetimler sonucunda alınan kararlar ve gerekli görülen durumlar, "E-İMZATR" tarafından ilgili taraflara uygun iletişim kanalları aracılığıyla bildirilir.

9. DİĞER İŞ KONULARI VE YASAL KONULAR

9.1. Ücretler

9.1.1. Sertifika Üretim ve Yenileme Ücretleri

"E-İMZATR" tarafından sunulan "NES" hizmetlerine ilişkin oluşturma, yenileme ve diğer sertifika hizmet ücretleri; sertifikanın geçerlilik süresi, hizmet kapsamı, sertifika hizmetlerinin yürütülmesi için oluşan maliyetler, piyasa koşulları ve ilgili diğer kriterler dikkate alınarak belirlenir.

Güncel "NES" oluşturma, yenileme ve diğer sertifika hizmetlerine ilişkin ücret bilgileri, "E-İMZATR" internet sitesi ve uygun görülen diğer iletişim kanalları aracılığıyla kullanıcıların bilgisine sunulur.

9.1.2. Sertifika Erişim Ücretleri

"EİMZATR" "NES" erişim hizmetleri için ücret talep etmez.

9.1.3. İptal veya Durum Bilgisi Erişim Ücretleri

"EİMZATR" "NES"lerine ilişkin iptal ve durum bilgileri "SİL"ler ve "ÇSDP" aracılığıyla ilgililere duyurulur. "EİMZATR" "SİL"ler ve "ÇSDP" erişim için herhangi bir ücret talep etmez.

9.1.4. Diğer Hizmetlerin Ücretleri

"E-İMZATR" tarafından kamuya açık olarak yayımlanan "NESİ", "NESUE", kullanıcı sözleşmeleri, sertifika hizmetleri kapsamında yayımlanan bilgilendirme dokümanları ve benzeri belgeler için ücret talep etmez.

Bunların dışında kalan ve katma değerli olarak sunulan ürün ve hizmetlere ilişkin ücretlendirme bilgileri, "E-İMZATR" internet sitesi ve uygun görülen diğer iletişim kanalları aracılığıyla kullanıcıların bilgisine sunulur.

9.1.5. Bedel İadesi

Ön ödemeli olarak talepte bulunulan NES'in üretimi tamamlanmamış olması hâlinde, başvuru sahibinin talebi doğrultusunda tahsil edilen ücret iade edilir. Üretimi tamamlanmış NES'ler için, yürürlükteki mevzuattan doğan haklar saklı kalmak kaydıyla ücret iadesi yapılmaz.

EİMZATR kaynaklı nedenlerle sertifika içeriğinin başvuru bilgilerinden farklı oluşturulması hâlinde, sertifika sahibinin talebi doğrultusunda NES ek ücret alınmaksızın yeniden oluşturulur veya tahsil edilen ücret iade edilir.

9.2. Finansal Sorumluluk

9.2.1. Sigorta Kapsamı

"Sertifika Mali Sorumluluk Sigortası Yönetmeliği" Madde 6 uyarınca, zorunlu sertifika mali sorumluluk sigortası, ESHS'nin güvenli ürün ve sistemleri kullanma, hizmeti güvenilir bir biçimde yürütme ve sertifikaların taklit ve tahrif edilmesini önlemekle ilgili yükümlülüklerini yerine getirmemesi dolayısıyla zarar görecek olanlara karşı doğacak hukuki sorumlulukların teminat altına alınmasını kapsar.

9.2.2. Diğer Varlıklar

İlgili değildir.

9.2.3. Son Kullanıcılar için Sigorta veya Garanti Kapsamı

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

9.3. İş Bilgisinin Gizliliği

9.3.1. Gizli Bilginin Kapsamı

"E-İMZATR"nin elektronik sertifika hizmet sağlayıcılığı faaliyetleri kapsamında; teknik, operasyonel ve ticari faaliyetlere ilişkin gizli bilgi ve belgeler, "ESHS" operasyonlarına ait bilgi güvenliği kapsamında koruma altındadır.

"E-İMZATR"nin ticari faaliyetlerine ilişkin her türlü gizli bilgi ve belge, "E-İMZATR" kök ve alt kök sertifikalarına ait imza oluşturma verileri, işlem kayıtları, denetim ve değerlendirme kayıtları, "NES" sahiplerine ait mevzuat kapsamında kişisel veri olarak değerlendirilen bilgiler, "Güven Merkezi" ile ilgili gizli bilgiler, donanım ve yazılımlara ilişkin teknik güvenlik bilgileri gizli bilgi kapsamındadır.

Ayrıca; tesis güvenliği kapsamında erişim bilgileri, fiziksel alanlara ilişkin plan ve düzenlemeler, acil durum ve iş sürekliliği planları, erişim yetkileri ile "E-İMZATR"nin iş ortakları ve hizmet aldığı kuruluşlara ait gizlilik dereceli bilgiler de gizli bilgi olarak değerlendirilir.

9.3.2. Gizlilik Kapsamı Dışındaki Bilgi

"NESUE", "NESİ", kullanıcı sözleşmeleri, bilgi deposunda bulunan bilgiler, "NES" sahibinin rızası doğrultusunda kamuya açık bir dizinde "EİMZATR" tarafından yayımlanan "NES"ler, "EİMZATR" kök ve alt kök sertifikaları, "SİL"ler gizli bilgi kapsamında sayılmazlar..

9.3.3. Gizli Bilginin Korunması Sorumluluğu

"E-İMZATR" çalışanlarının tamamı, "NES" hizmetlerinin yürütülmesi kapsamında elde edilen gizli bilgilerin, kişisel verilerin ve özel nitelikli kişisel verilerin korunmasından sorumludur.

"E-İMZATR", bilgi güvenliği politikaları ve prosedürleri doğrultusunda, gizli bilgilere yalnızca görev ve yetkileri kapsamında ihtiyaç duyan yetkili personelin erişebilmesini sağlar. Yetkisi bulunmayan çalışanların veya üçüncü kişilerin gizli bilgilere erişimine izin verilmez.

"E-İMZATR" bünyesinde uygulanan bilgi güvenliği prosedürleri çalışanlar tarafından eksiksiz şekilde uygulanır ve bu uygulamalar gerekli görülen durumlarda iç denetim süreçleri kapsamında kontrol edilir.

5070 sayılı Elektronik İmza Kanunu'nun 12'nci maddesi kapsamında "ESHS";

"NES" talep eden kişiden, elektronik sertifika verilmesi için gerekli olan bilgiler dışında bilgi talep edemez ve bu bilgileri kişinin rızası dışında elde edemez,

"NES" sahibinin izni olmaksızın sertifikayı üçüncü kişilerin erişimine açık ortamlarda bulunduramaz,

“NES” sahibinin açık onayı olmaksızın kişisel verilerin üçüncü kişiler tarafından elde edilmesini engeller, bu bilgileri üçüncü kişilere aktaramaz ve farklı amaçlarla kullanamaz.

9.4. Kişisel Bilgilerin Gizliliği/Özelliği

9.4.1. Gizlilik Planı

“E-İMZATR”, sunduğu “NES” hizmetleri kapsamında; “NES” başvuru sahiplerine, kurumsal başvuru sahiplerine ve ilgili diğer taraflara ait kişisel verilerin ve özel nitelikli kişisel verilerin gizliliğini sağlar.

“E-İMZATR”, kişisel verilerin korunmasına ilişkin yükümlülüklerini 6698 sayılı Kişisel Verilerin Korunması Kanunu, ilgili mevzuat hükümleri, “NESİ”, “NESUE”, kullanıcı sözleşmeleri ve ilgili prosedürler doğrultusunda yerine getirir. Kişisel verilerin yetkisiz erişim, kullanım veya açıklamaya karşı korunması için gerekli teknik ve idari tedbirleri alır.

9.4.2. Özel Olarak Değerlendirilecek Bilgi

“NES” sahibinden “NES” başvurusu sırasında alınan ve “NES” içeriğinde ve “SİL”lerde yer almayan bilgiler özel bilgilerdir.

9.4.3. Özel Sayılmayacak Bilgi

“NES” ve “SİL” içerisinde yer alan ve “E-İMZATR” tarafından üçüncü kişilerin erişimine açık şekilde yayımlanan bilgiler, aksi “NES” sahibi tarafından talep edilmedikçe veya ilgili mevzuat hükümleri gereğince sınırlandırılmadıkça özel bilgi olarak kabul edilmez.

“E-İMZATR”, yayımlanan “NES” bilgileri ile sertifika durum bilgilerinin yalnızca belirlenen amaç ve kapsam dahilinde erişilebilir olmasını sağlar. “NES” sahibine ait yayımlanan bilgilerin kapsamı, “NESİ”, “NESUE”, kullanıcı sözleşmeleri ve yürürlükteki mevzuat hükümleri doğrultusunda belirlenir.

9.4.4. Özel Bilgiyi Koruma Sorumluluğu

“EİMZATR” “NESİ” de belirtilen bilgilerin korunması konusunda sorumluluk sahibidir. Yetkili olmayan personel özel bilgilere erişememektedir.

9.4.5. Özel Bilgiyi Kullanma Bildirimi ve Onayı

“E-İMZATR”, “NES” hizmetlerinin sunulması kapsamında; kullanıcılar tarafından başvuru sırasında sağlanan bilgileri, “NES” üretimi, yenilenmesi, iptali, askıya alınması, yayımlanması ve sertifika yönetim süreçlerinin yürütülmesi amacıyla, “NESİ”, “NESUE”, kullanıcı sözleşmeleri ve ilgili mevzuat hükümleri doğrultusunda kullanabilir.

“E-İMZATR”, sertifika hizmetlerinin güvenli ve etkin şekilde yürütülmesi, kullanıcı taleplerinin karşılanması, hizmet kalitesinin geliştirilmesi ve yasal yükümlülüklerin yerine getirilmesi amacıyla gerekli kişisel verileri ilgili mevzuata uygun olarak işleyebilir.

“E-İMZATR”, kullanıcıların açık rızası ve ilgili mevzuat hükümleri doğrultusunda; yeni hizmetleri, uygulamaları, ürünleri ve kampanyaları hakkında kişisel iletişim bilgileri üzerinden bilgilendirme yapabilir.

9.4.6. Yargısal ve İdari Süreçlere Uygun Olarak Bilginin Açıklanması

Hukuki veya idari süreçler kapsamında ihtiyaç duyulan “NES” sahibine ait özel nitelikli veya kişisel bilgiler, yalnızca ilgili mevzuat kapsamında yetkili resmî makamlara veya “NES” sahibinin kendisine verilir.

6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında, “NES” sahipleri kişisel verileriyle ilgili bilgi alma, düzeltme, silme, yok etme ve Kanun’un 11’inci maddesinde belirtilen diğer haklarını kullanmak amacıyla “E-İMZATR”ye başvurabilirler.

Kişisel veri sahipleri tarafından yapılan başvurular, ilgili mevzuatta belirtilen usul ve esaslar çerçevesinde değerlendirilir ve yasal süre içerisinde “E-İMZATR” tarafından yazılı olarak veya elektronik ortamda cevaplandırılır.

9.4.7. Bilginin Açıklandığı Diğer Durumlar

Uygulama dışıdır.

9.5. Fikri Mülkiyet Hakları

“EİMZATR” tarafından yayımlanan tüm “NESİ”, “NESUE”, Kullanıcı sözleşmeleri, “EİMZATR” tarafından www.EİMZATR.com.tr adresinde yayımlanan her türlü metin ve marka değeri içeren belge, görsel ve işitsel içeriğin fikri ve mülkiyet hakları “EİMZATR” ye aittir.

9.6. Sorumluluklar

9.6.1. ESHS Beyan ve Garantileri

EİMZATR; Nitelikli Elektronik Sertifika hizmetlerini, yürürlükteki mevzuat, NESİ, NESUE ve ilgili politika ve prosedürlere uygun olarak yürütür.

Bu kapsamda; başvuru ve kimlik doğrulama işlemlerinin doğru ve güvenilir biçimde gerçekleştirilmesini, sertifikaların doğrulanmış başvuru bilgilerine uygun olarak doğru sertifika sahibi adına oluşturulmasını ve teslim edilmesini, sertifika yaşam döngüsü işlemlerinin güvenli ve izlenebilir biçimde yürütülmesini, sertifika durum bilgilerinin güncel, doğru ve erişilebilir tutulmasını ve kritik sertifika hizmetlerinin yalnızca yetkilendirilmiş kişiler ve güvenli sistemler aracılığıyla gerçekleştirilmesini sağlar.

EİMZATR, 5070 sayılı Elektronik İmza Kanunu ve elektronik imzaya ilişkin yürürlükteki diğer mevzuat kapsamında Elektronik Sertifika Hizmet Sağlayıcısına yüklenen yükümlülükleri yerine getirir.

9.6.2. Kayıt Merkezi Sorumlulukları

“KB”ler, başvuru sahiplerinin kimlik kontrolü ve doğrulama işlemlerini, “NESİ”, “NESUE” ve ilgili prosedürlerde belirtilen esaslara uygun, doğru ve güvenilir şekilde gerçekleştirmekle yükümlüdür. “KB”ler tarafından gerçekleştirilen kimlik doğrulama işlemlerine ilişkin kayıtların doğru, eksiksiz ve güvenilir biçimde tutulmasını sağlamak; sertifika üretim, yenileme ve iptal taleplerini gerekli kontrolleri gerçekleştirerek doğru ve eksiksiz bir şekilde “E-İMZATR”ye iletmek KB’lerin sorumluluğundadır.

“KB”ler, kullanıcıların ilk kayıt işlemlerini gerçekleştirmek, sertifika başvurularını almak, yenileme ve iptal taleplerini değerlendirmek ve bu talepleri “E-İMZATR” süreçlerine uygun olarak iletmekle görevlidir.

Bu yükümlülüklere aykırı hareket eden “KB”ler hakkında “E-İMZATR” tarafından inceleme başlatılabilir ve gerekli görülmesi hâlinde sözleşmesel, idari veya yasal süreçler uygulanabilir.

9.6.3. Sertifika Sahibi Sorumlulukları

“NES” sahipleri ve kurumsal başvuru sahipleri: “NES” sahibi, kullanımdan önce “NES”in geçerlilik durumunu kontrol etmekle, geçerliliği sona ermiş, askıda bulunan veya iptal edilmiş “NES”i kullanmamakla, “NES”i sadece güvenli elektronik imza oluşturma ve doğrulama süreçlerinde kullanmakla, “NES”i kullanım ve maddi kapsama ilişkin sınırlar dahilinde kullanmakla, “NES”i kullandığı ortamların gizliliğini ve güvenliğini sağlamakla, “NES”i imzalamış olduğu kullanıcı sözleşmesine, “NESUE”ye, “NESİ”ye uygun olarak ve hukuka uygun amaçlarla kullanmakla, başvuru süreçlerinde “KB” yetkililerine, “Kurumsal Başvuru Sahibi”ne ve “EİMZATR” personeline doğru, geçerli ve yeterli bilgi ve belgeleri sağlamakla yükümlüdür. “NES” sahiplerinin, yukarıda belirtilen yükümlülüklerini yerine getirmedikleri takdirde bu yükümlülüklerini yerine getirmemeleri sebebiyle doğan veya doğmuş olacak “EİMZATR”nin,üçüncü kişilerin, kurumsal başvuru sahiplerinin ve ilgili diğer tarafların zararlarını tazmin sorumlulukları vardır.

9.6.4. Üçüncü Kişilerin Sorumlulukları

Üçüncü kişiler “NES”le ilişkili olarak oluşturulmuş bir güvenli elektronik imzaya güvenerek herhangi bir iş veya işlem yapmadan önce güvenli elektronik imzayı doğrulamakla ve “NES”in geçerliliğini kontrol

etmekle yükümlüdürler. Üçüncü taraflar bu sorumluluklarını “Güvenli Elektronik İmza Doğrulama Aracı” kullanarak yerine getirebilirler. Üçünci kişiler aynı zamanda “Yönetmelik”in 16. Maddesinde belirtilen yükümlülüklere uymakla mükelleflerdir. Üçüncü kişilerin, yukarıda belirtilen yükümlülüklerine yerine getirmedikleri takdirde bu yükümlülüklerini yerine getirmemeleri sebebiyle doğmuş ve doğacak “EİMZATR”nin, “NES” sahiplerinin, kurumsal başvuru sahiplerinin ve ilgili diğer tarafların zararlarını tazmin sorumlulukları vardır..

9.6.5. Diğer Katılımcıların Sorumlulukları

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

9.7. Sorumlulukların Geçersiz Olduğu Durumlar

Uygulama dışıdır.

9.8. Sorumluluk Sınırları

Sorumluluklar ve Sınırlamalar: “ESHS” kullanıcı bilgilerinin kötüye kullanımı, ihmal v.b amaçlarla kullanımını önlemek için gerekli önlemleri alır, “ESHS” bu belgede bildirilenler dışında gerçekleştirilen kullanım, kötüye kullanım durumlarında sorumluluk kabul etmez. Kullanımı gerçekleştiren kişilerden zarar tazmin sorumluluğu vardır. “ESHS” bilgisi ve kontrolü dışında kullanıcıların uğrayacağı zararlardan sorumlu değildir.

9.9. Tazminatlar

“NES” sahiplerinin kullanıcı sözleşmeleri uyarınca yükümlülüklerini yerine getirmedikleri durumlarda, “EİMZATR”nin, kurumsal başvuru sahiplerinin veya üçüncü kişilerin zarar görmesi halinde, “NES” sahipleri bu zararları tazminle mükelleftir. Kurumsal başvuru sahiplerinin Kurumsal Başvuru Sözleşmesi uyarınca yükümlülüklerini yerine getirmedikleri durumlarda, “EİMZATR”nin, “NES” sahiplerinin veya üçüncü kişilerin zarar görmesi halinde, “NES” sahipleri bu zararları tazminle mükelleftir.

“EİMZATR” “Kanun” ve ilgili mevzuattan kaynaklanan yükümlülüklerini yerine getirmediği takdirde, “NES” sahiplerinin ve üçüncü kişilerin bu durumdan kaynaklanan zararlarını tazminle mükelleftir.

9.10. NESİ dokümanının Geçerliliği

9.10.1. NESİ dokümanının Geçerlilik Dönemi

“NESİ” ve “NESİ” de yapılan değişiklikler www.e-imzatr.com.tr adresinde yayımlanmasından itibaren yürürlüğe girer.

9.10.2. NESİ dokümanının Geçerliliğinin Sona Ermesi

“EİMZATR” faaliyetlerinde ve sertifika hizmetlerinde oluşabilecek değişikliklere ve düzenlemelere bağlı olarak, NESİ 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 NESİ dokümanı sürümü “EİMZATR” tarafından hazırlanır ve yayımlanır.

9.10.3. Geçerliliğin Sona Ermesinin Etkileri ve İşlerliğin Sürdürülmesi

E-İMZATR NESİ dokümanında, NESİ sürüm değişiklikleri sonucunda eski sürüm hükümlerinin sona ermesi ve yeni NESİ hükümlerinin ilgili taraflar açısından uygulanabilir hâle gelmesine ilişkin esaslar düzenlenmiştir. Bununla birlikte, sürüm geçiş sürecinin kesintisiz yürütülmesi, yeni NESİ sürümünün önceki sürümün geçerlilik süresi sona ermeden hazırlanması, gerekli bilgilendirmelerin sertifika sahipleri ve üçüncü kişilere yapılması ve yeni uygulamaların devreye alınmasına ilişkin operasyonel süreçler mevcut düzenlemede ayrıca belirtilmemiştir.

E-İMZATR tarafından gerçekleştirilecek NESİ değişikliklerinde; hizmet sürekliliğinin sağlanması, sertifika sahipleri ve üçüncü kişilerin zamanında bilgilendirilmesi, sertifika hizmetlerinde oluşabilecek etkilerin değerlendirilmesi ve gerekli teknik/operasyonel geçiş işlemlerinin planlı şekilde yürütülmesi amacıyla ilgili süreçlerin NESİ veya ilgili prosedür dokümanlarında tanımlanması uygun olacaktır.

Bu kapsamda, mevcut NESİ hükmü yeni sürümün bağlayıcılığını düzenlemekle birlikte, sürüm geçiş yönetimine ilişkin operasyonel kontrollerin ayrıca belirtilmesiyle daha kapsamlı ve uygulanabilir bir çerçeve oluşturulacaktır.

9.11. Taraflara Özel Duyurular ve İletişim

“EİMZATR”tarafından sertifika sahiplerine yapılacak olan kişisel duyurular için sertifika sahiplerinin uygun olan iletişim bilgileri kullanılır.

“EİMZATR”’nin üçüncü kişilere yapacağı duyurular web üzerinden ya da basın yayın organları aracılığıyla yayımlanır.

9.12. Değişiklikler

“EİMZATR” faaliyetlerinde ve sertifika hizmetlerinde oluşabilecek değişikliklere ve düzenlemelere bağlı olarak, NESİ dokümanının mevcut sürümünün içeriğinin değişmesini gerektiren herhangi bir durum ortaya çıktığında, ilgili değişikliklerin yansıtıldığı yeni bir NESİ dokümanı sürümü “EİMZATR” tarafından hazırlanır ve “EİMZATR” Yönetim Kurulu’nun onayının ardından yayımlanır. NESİ 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 “EİMZATR” uygulamaları farklı olacaktır.

9.12.1. Değişiklik Prosedürü

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

NESİ ve NESUE dokümanında yer alan ilgili ilkeler ve uygulamalar, yönetim gözden geçirme toplantılarında yıllık olarak gözden geçirilir. NESİ’de oluşan değişiklikler, NESUE’deki ilgili uygulamalara da yansıtılır. Dolayısıyla yeni bir NESİ sürümü, yeni bir NESUE sürümünü de gerektirir. “EİMZATR” tarafından üretilen yeni sertifikaların “sertifika ilkeleri” uzantısında URL olarak verilen NESUE dokümanına erişim bilgisi aynı kalır, ama bu adresin işaret ettiği NESUE dokümanı yeni sürümdür. Küçük değişiklikler olması durumunda, önceden verilmiş olan sertifikalar da yeni NESİ ve NESUE’ye uygun olarak kullanılmaya devam eder. Ancak önemli değişiklikler nedeniyle yeni bir NESİ sürümü çıkarılmışsa, önceden üretilmiş sertifikaların, değişiklik yapılan sertifika ilkelerine bağlı olanları, yeni NESİ’ye uyumlu olarak kullanılamayabilir.

9.12.2. Duyuru Mekanizması ve Süresi

“EİMZATR” faaliyetleri ve sertifika hizmetlerindeki uygulama değişiklikleri ile mevcut NESİ ve NESUE kitapçıklarında değişiklik oluşması durumunda, çıkarılan güncel NESİ ve NESUE sürümleri hakkında sertifika sahipleri ile üçüncü kişiler ivedilikle bilgilendirilir. Özellikle önemli değişikliklerde, sertifikanın kullanılabilirliği ve kabul edilirliği bazı uygulamalarda etkilenebileceğinden, “EİMZATR” sertifika sahipleri ile üçüncü kişileri bilgilendirebilmek için tüm makul imkanları kullanır. Yeni NESİ ve NESUE sürümleri, eski sürümlerle birlikte “EİMZATR” bilgi deposunda, ayrıntılı sürüm bilgisi içerecek şekilde yayımlanır ve ilgili tarafların erişimine açık tutulur.

9.12.3. Nesne Tanımlayıcı Numaralarının Değişmesini Gerektiren Durumlar

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, NESİ 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

"EİMZATR", sertifika sahipleri ve üçüncü kişiler arasında çıkabilecek anlaşmazlıklarda öncelikle, NESİ ve NESUE kitapçıklarında belirlenmiş ilke ve uygulama esasları ile prosedürler, taahhütnameler ve sözleşmeler uyarınca sorunun çözümlenmesine çalışılır. Nitelikli elektronik sertifikalarla ilgili işlemler "EİMZATR" tarafından Kanun ve Yönetmelikler ile bunlara bağlı Tebliğler uyarınca yürütülür. Taraflar arasındaki anlaşmazlıklar sulhen çözüme kavuşmadığı takdirde, anlaşmazlıkların çözümü için Ankara Mahkemeleri yetkilidir.

9.14. Yasal Düzenleme

Türkiye'de, elle atılan imza ile aynı hukuki sonucu doğuran güvenli elektronik imzanın kullanımı, 5070 sayılı "Elektronik İmza Kanunu" ve Bilgi Teknolojileri ve İletişim Kurumu tarafından yayımlanmış

Yönetmelik ve Tebliğler uyarınca düzenlenir. Kurum ESHS'lerin Kanun uyarınca işleyişinin düzenlenmesi ve denetlenmesinden sorumludur.

9.15. İlgili Yasalara Uygunluk

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

9.16. Çeşitli Hükümler

9.16.1. Bütün Anlaşma

İlgili değildir.

9.16.2. Görevlendirme

İlgili değildir.

9.16.3. Kitapçık Kısımlarının Ayrılabilirliği

NESİ ve NESUE kitapçıklarının diğer bölümlerinin geçerliliğini etkilemeyen herhangi bir bölümü geçerliliğini kaybettiğinde, "EİMZATR" tarafından ilgili değişikliklerin yansıtıldığı yeni sürümler çıkarılana kadar, kitapçığın etkilenmemiş diğer bölümleri geçerliliğini korur ve uygulanır.

9.16.4. Yasal Haklardan Vazgeçme

İlgili değildir.

9.16.5. Mücbir Sebepler

"EİMZATR"'nin 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, "EİMZATR" 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

İlgili değildir.