EİMZATR

NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

(NESUE)

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. tarafından yürütülen Nitelikli Elektronik Sertifika hizmetleri, 5070 sayılı Elektronik İmza Kanunu, ilgili ikincil düzenlemeler, EİMZATR NESİ ve bilgi güvenliği yönetim sistemi kapsamında işletilir. Bu NESUE, NESİ de belirlenen ilke ve yükümlülüklerin EİMZATR süreçlerinde nasıl yerine getirildiğini açıklar.

Uygulama esasları; başvurunun alınması, kimlik doğrulama, sertifika üretimi ve aktivasyonu, teslimat, yenileme/değişiklik, askıya alma ve iptal, sertifika durum servisleri, kayıtların saklanması, teknik güvenlik kontrolleri ve iş sürekliliği süreçlerini kapsar.

1.1. Genel Bakış

EİMZATR NES hizmetleri, başvuru sahibinin kimliğinin ve sertifikaya yazılacak bilgilerin doğrulanmasıyla başlar; güvenli anahtar ve sertifika üretimi, aktivasyon, güvenli elektronik imza oluşturma aracının teslimi ve sertifika yaşam döngüsü yönetimi ile devam eder.

Her işlem, başvuru veya sertifika kaydıyla ilişkilendirilebilir şekilde yürütülür. Kritik işlemlerde yetkilendirme, görevlerin ayrılığı ve gerekli hâllerde ikili kontrol uygulanır.

1.2. Kitapçık Adı ve Tanımlama

Doküman Adı: EİMZATR Nitelikli Elektronik Sertifika Uygulama Esasları (NESUE)

Doküman Sürümü: 3.0

İlgili Sertifika İlkeleri OID: 2.16.792.3.0.10.10.1.1

1.3. Taraflar

NESUE kapsamındaki taraflar; EİMZATR Güven Merkezi ve sertifika üretim bileşenleri, kayıt birimleri, sertifika sahibi gerçek kişiler, kurumsal bilgi içeren NES başvurularında ilgili tüzel kişiler, üçüncü kişiler ve EİMZATR adına hizmet sağlayan yetkilendirilmiş tedarikçi/alt yüklenicilerden oluşur.

1.3.1. Sertifika Üretim Merkezleri

Kök ve alt kök sertifika altyapısı ile son kullanıcı NES üretim sistemleri yetkili kişiler tarafında işletilir. Sertifika üretim talebi, başvuru sistemi üzerinde kimlik ve başvuru kontrolleri tamamlanmış kayıtlar için oluşturulur. Üretim sistemlerine erişim yalnızca görev tanımına göre yetkilendirilmiş güvenli personel ve servis hesapları ile sınırlandırılır.

1.3.2. Sertifika Kayıt Merkezleri

Kayıt birimleri, EİMZATR tarafından yetkilendirilmiş kullanıcı hesapları üzerinden başvuru ve yönetim sistemlerine erişir. Başvurunun alınması, kimlik doğrulama adımlarının tamamlanması, gerekli bilgi ve belgelerin kontrolü, eksik/hatalı başvuruların iadesi ve yetkileri kapsamındaki iptal/askı taleplerinin alınması işlemleri merkezî sistem üzerinden yürütülür.

Kayıt birimlerinin yetkileri sözleşme, görev tanımı ve rol bazlı erişim profilleriyle sınırlandırılır. Kayıt birimi personelinin gerçekleştirdiği işlemler kullanıcı kimliği ve zaman bilgisiyle kaydedilir; yetki sona erdiğinde ilgili kullanıcı erişimleri kapatılır.

1.3.3. Sertifika Sahipleri

NES başvurusu ve sertifika sahibine ilişkin işlemler gerçek kişi üzerinden yürütülür. Kurumsal bilgi içeren NES başvurularında kişinin ilgili tüzel kişiyle ilişkisi, görevi veya yetkisi; başvurunun niteliğine göre resmî kayıt, imza sirküleri, kurum yazısı veya doğrulanabilir diğer belgeler üzerinden kontrol edilir ve başvuru kaydıyla ilişkilendirilir.

1.3.4. Üçüncü Kişiler

Üçüncü kişiler sertifikaya veya güvenli elektronik imzaya dayanarak işlem yapmadan önce sertifika zincirini, sertifika geçerlilik süresini, kullanım kısıtlarını ve iptal/askı durumunu SİL, OCSP veya mevzuata uygun

doğrulama araçları üzerinden kontrol eder. EİMZATR, bu kontroller için gerekli kök/alt kök sertifikaları ve durum servislerini kamuya açık erişimde tutar.

1.3.5. Diğer Katılımcılar

Kargo, haberleşme, sistem bakım/destek, barındırma, güvenlik ve benzeri destek hizmeti sağlayan taraflar; yalnızca sözleşmeyle belirlenmiş görevleri ve yetkileri kapsamında sürece dâhil edilir. Bu tarafların erişimleri gerekli olduğu süre ve kapsamla sınırlandırılır; gizlilik, bilgi güvenliği ve kayıt yükümlülükleri sözleşmelerle düzenlenir.

1.4. Sertifika Kullanımı

1.4.1. Geçerli Sertifika Kullanım Şekilleri

Sertifika sahibine teslim edilen güvenli elektronik imza oluşturma aracı, sertifika sahibinin belirlediği veya güvenli biçimde aktive ettiği erişim bilgileriyle kullanılır. İmza oluşturma verisi cihaz dışına çıkarılmaz ve sertifika sahibinin kontrolü dışında kullanılamaz. İmza doğrulama işlemleri sertifika içindeki açık anahtar, sertifika zinciri ve güncel durum bilgileri kullanılarak gerçekleştirilir.

1.4.2. Sertifika Kullanımının Sınırları

Başvuru ve bilgilendirme ekranlarında, kullanıcı sözleşmesinde/taahhütnamede ve yayımlanan NESİ/NESUE belgelerinde sertifikanın kullanım sınırları mevzuatla belirlenir.

1.5. Sertifika İlkeleri Yönetimi

NESİ ve NESUE, EİMZATR doküman yönetim süreci kapsamında sürüm kontrollü olarak yönetilir. Mevzuat, teknik standart, süreç, altyapı veya organizasyon değişikliği olduğunda etki değerlendirmesi yapılır; gerekli revizyon hazırlanır, kontrol edilir, yetkili yönetim organının onayından sonra yürürlüğe alınır ve kamuya açık sürüm bilgi deposunda yayımlanır.

1.5.1. NESUE Dokümanından Sorumlu Organizasyon

NESİ/NESUE doküman setinin sahipliği EİMZATR'ye aittir. Dokümanın koordinasyonu, mevzuat ve süreç sahiplerinden alınan girdilerle yürütülür; bilgi güvenliği, operasyon, sistem/ağ ve gerektiğinde hukuk/uyum birimlerinin görüşleri revizyon sürecine dâhil edilir.

1.5.2. İletişim Noktası

NESİ/NESUE hakkında bilgi talepleri EİMZATR'nin yayımlanmış kurumsal iletişim kanalları üzerinden alınır. Gelen talepler ilgili birime yönlendirilir ve talebin niteliğine göre kayıt altına alınarak cevaplandırılır.

EİMZATR BİLGİ GÜVENLİĞİ HİZMETLERİ A.Ş.

Prof. Dr. Ahmet Taner Kışlalı Mah. 2778. Sokak No:3 Çayyolu / Ankara

Tel: +90 312 242 01 11

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

Web: www.e-imzatr.com.tr

1.5.3. NESUE'nin NESİ'ye Uygunluğunu Belirleyen Yetkili

NESUE'nin NESİ, yürürlükteki mevzuat ve EİMZATR'nin fiilî işleyişiyle uyumluluğu ilgili süreç sahipleri tarafından kontrol edilir; nihai uygunluk ve yürürlüğe alma kararı yetkili yönetim organı tarafından verilir.

1.5.4. NESUE Onaylama Prosedürleri

1. Revizyon ihtiyacı veya yeni sürüm gereksinimi doküman sorumlusu tarafından kayıt altına alınır.

2. İlgili bölüm, süreç sahibi ve teknik/uyum sorumluları tarafından gözden geçirilir.

3. Değişikliğin mevcut sertifikalara, kullanıcı süreçlerine, teknik profillere ve yayımlanan bilgilere etkisi değerlendirilir.

4. Onaylanan metne sürüm ve tarih bilgisi verilir; önceki sürüm arşivlenir.

5. Güncel sürüm bilgi deposunda yayımlanır ve gerekli taraflara duyurulur.

1.6. Kısaltmalar ve Tanımlar

1.6.1. Kısaltmalar

Kısaltma	Açılım
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
KDY	Elektronik Haberleşme Sektöründe Başvuru Sahibinin Kimliğinin Doğrulanma Süreci Hakkında Yönetmelik
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
IETF	Internet Engineering Task Force
RFC	Request for Comments
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
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
SIEM	Security Information and Event Management – Güvenlik Bilgisi ve Olay Yönetimi
NTP	Network Time Protocol – Ağ Zaman Protokolü

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 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 ilgili mevzuat uyarınca sağlayan hizmet sağlayıcıdır.
Kimlik Doğrulama Yönetmeliği (KDY)	Elektronik haberleşme sektöründe başvuru sahibinin kimliğinin doğrulanmasına ilişkin usul ve esasları düzenleyen Elektronik Haberleşme Sektöründe Başvuru Sahibinin Kimliğinin Doğrulanma Süreci Hakkında Yönetmeliktir. NES başvurularında kapsam dâhilindeki kimlik doğrulama ve işlem belgesi süreçleri ilgili hükümler doğrultusunda yürütülür.
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 ilgili yükümlülükleri yerine getiren tüzel kişidir.
Kayıt Birimi (KB)	EİMZATR adına başvuru alma, kimlik doğrulama ile gerekli bilgi/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/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	İlgili mevzuat ve teknik düzenlemelerde belirlenen güvenlik koşullarını sağlayan, imza oluşturma verisinin güvenli biçimde oluşturulması, korunması 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.
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 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.

2. YAYIN VE BİLGİ DEPOSU SORUMLULUKLARI

2.1. Bilgi Deposu

Kamuya açık belgeler EİMZATR'nin kurumsal internet sitesi üzerindeki bilgi deposu/bilgi bankası alanında yayımlanır. Yayımlama yetkisi sınırlı sayıdaki yetkili kullanıcıya verilir; yeni veya revize edilmiş belge, onay süreci tamamlandıktan sonra yayın ortamına aktarılır. Yayınlanan dosyanın sürüm, tarih ve erişim adresi kontrol edilir.

2.2. Sertifika Bilgilerinin Yayımlanması

NESİ, NESUE, kullanıcı sözleşmesi/taahhütnameler, müşteri kılavuzları, EİMZATR kök ve alt kök sertifikaları, SİL erişim bilgileri ve OCSP hizmet bilgileri kamuya açık alanda yayımlanır. Ticari sır, güvenlik yapılandırması, özel anahtar bilgisi, iç prosedür ve kişisel veri niteliğindeki içerikler kamuya açık alana aktarılmaz.

2.3. Yayımın Zamanı veya Sıklığı

Doküman ve sertifika bilgileri onaylanan değişikliklerin yürürlüğe girmesiyle güncellenir. Son kullanıcı SİL'leri otomatik görevlerle 5 dakikada bir üretilir ve yayımlanır; yayımlanan listenin geçerlilik süresi 24 saattir. Sertifika durum değişiklikleri OCSP altyapısına işlem sonucunda yansıtılır. Alt kök sertifikalara ilişkin SİL üretimi NESİ'de belirlenen periyot ve olay koşullarına göre yürütülür.

2.4. Bilgi Deposuna Erişim Kontrolleri

Kamuya açık bilgi deposuna okuma erişimi kimlik doğrulama gerektirmeden sağlanır; içerik ekleme/değiştirme/ yetkileri rol bazlı olarak sınırlandırılır. Yönetim erişimleri güvenli yönetim kanalları üzerinden gerçekleştirilir. Yayın sunucuları ve içerik değişiklikleri güvenlik izleme ve kayıt mekanizmalarıyla takip edilir.

3. KİMLİĞİN DOĞRULANMASI

Kimlik doğrulama işlemleri başvuru kanalı, başvuru sahibinin vatandaşlık/statü durumu, kullanılan kimlik belgesi ve yürürlükteki KDY hükümleri dikkate alınarak gerçekleştirilir. Kimlik doğrulama sonucu başvuru kaydıyla ilişkilendirilir; başarısız veya tamamlanmamış doğrulama sonucu bulunan başvurular sertifika üretimine aktarılmaz.

3.1. İsimlendirme

Sertifika alanları, doğrulanmış başvuru verilerinden sertifika üretim sistemine kontrollü olarak aktarılır. Alan eşleştirmeleri sertifika profiline göre tanımlanmıştır; kullanıcı tarafından serbest metin girilebilen alanlar gerekli doğrulamalardan geçmeden sertifika içeriğine taşınmaz.

3.1.1. İsim Tipleri

Sertifika üretim sistemi, ayırt edici isim (DN) alanlarını X.500 isimlendirme yapısına uygun olarak oluşturur. CN, O, OU, C, L ve ilgili kimlik tanımlayıcıları, sertifika profili ve başvuru verilerine göre otomatik/kurallı biçimde eşleştirilir.

3.1.2. İsimlerin Anlamlı Olması Gerekliliği

Ad, soyad ve sertifikaya yazılacak diğer kimlik bilgileri doğrulanan resmî kayıtlardaki biçimi esas alınarak kullanılır. Uyuşmazlık tespitinde kayıt birimi başvuruyu üretime sevk etmez; düzeltme veya yeniden doğrulama ister. Düzeltme işlemleri kullanıcı ve zaman bilgisiyle kaydedilir.

3.1.3. Sertifika Sahiplerinin Anonimliği ve Takma Ad Kullanılabilirliği

NES başvuru ekranlarında takma ad veya anonim isim seçeneği sunulmaz. Sertifika sahibinin kimlik bilgileri doğrulanmış gerçek kişi bilgileri üzerinden işlenir.

3.1.4. İsim Biçimlerinin Değerlendirilmesi

DN alanlarının karakter seti, alan uzunluğu ve format kontrolleri sertifika üretim sistemi üzerinde teknik profil kurallarıyla doğrulanır. Profil dışı veya zorunlu alanı eksik kayıt üretime alınmaz.

3.1.5. İsimlerin Benzersizliği

Sertifikalar yalnız isim alanı ile değil, sertifika seri numarası ve sertifika sahibine ilişkin benzersiz kimlik tanımlayıcıları ile ayırt edilir. Üretim sistemi her NES için benzersiz sertifika seri numarası oluşturur; aynı sertifika kaydının mükerrer üretimini engelleyen kontroller uygulanır.

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’nin standart son kullanıcı üretim sürecinde anahtar çifti güvenli üretim ve kişiselleştirme sürecinde oluşturulduğundan başvuru sahibinden ayrıca özel anahtara sahiplik kanıtı istenmez. Üretim sistemi, oluşturulan açık anahtarın ilgili başvuru ve güvenli elektronik imza oluşturma aracı ile eşleştirilmesini sağlar.

3.2.2. Tüzel Kişiliğin Doğrulanması

Kurumsal bilgi içeren NES talebinde kurum unvanı ve başvuru sahibiyle kurum arasındaki ilişki, başvurunun türüne göre ticaret sicili/kurumsal kayıtlar, imza sirküleri, kurum yazısı, görev/yetki belgesi veya doğrulanabilir diğer belgeler üzerinden kontrol edilir. Kontrol sonucu ve kullanılan belge türü başvuru kaydıyla ilişkilendirilir; belge kopyası veya elektronik kayıt, veri minimizasyonu ve saklama kuralları dikkate alınarak muhafaza edilir.

3.2.3. Gerçek Kişinin Kimliğinin Doğrulanması

EİMZATR’da gerçek kişi kimlik doğrulaması, başvuru kanalında aktif olarak sunulan ve yürürlükteki mevzuata uygun kimlik doğrulama yöntemleri kullanılarak gerçekleştirilir. Uygulanacak yöntem başvuru sahibinin statüsüne, kullanılan kimlik veya pasaport ve başvuru kanalına göre sistem tarafından veya yetkili personelce seçilir.

EİMZATR’ın elektronik başvuru akışında e-Devlet Kapısı üzerinden kimlik doğrulama ve başvuru onayı alınabilir. Desteklenen elektronik kimlik veya pasaport, belgenin teknik kabiliyetine uygun okuyucu/yakın

alan iletişimi yöntemiyle doğrulanır. Yabancı başvuru sahiplerinde Göç İdaresi Başkanlığı tarafından sunulan sistemlerde desteklenen belge doğrulama veya yüz doğrulama yöntemleri kullanılabilir.

Kimlik doğrulama sonucu başvuru kaydına aktarılır ve başvuru formundaki kimlik bilgileriyle karşılaştırılır. Doğrulama başarısızsa veya bilgiler arasında uyuşmazlık varsa başvuru sertifika üretimine aktarılmaz; gerekli düzeltme veya yeniden doğrulama işlemi tamamlanır.

Kimlik Doğrulama Yönetmeliği kapsamındaki işlemlerde, başvuru ve doğrulama verilerinden işlem belgesi oluşturulur ve başvuru sahibinin gerekli onayı alınır. İşlem belgesi, EİMZATR adına yetkilendirilmiş Nitelikli Elektronik Sertifika kullanılarak PAdES-LTV formatında imzalanır ve zaman damgası ile güvence altına alınır; belge ilgili başvuru kaydıyla ilişkilendirilerek saklanır ve başvuru sahibine sunulur.

3.2.4. Doğrulama Yapılmaksızın Sertifikada Yer Alabilen Bilgiler

Sertifika profilinde mevzuat veya ilgili sertifika profili kapsamında ayrıca doğrulanması zorunlu olmayan bir alan bulunması hâlinde, bu bilgi başvuru sahibinin beyanı üzerinden alınabilir.

Beyan edilen bilginin kimlik tespitini, kurum/görev/unvan/yetki bilgisini veya sertifikanın kullanımını etkileyen bir niteliğe sahip olduğu değerlendirilirse uygun ve güvenilir kaynak üzerinden doğrulama yapılmadan sertifikaya aktarılmaz. Sertifika üretim ekranları ve operasyon kontrolleri bu ayrım gözetilerek uygulanır.

3.2.5. Yetkinin Doğrulanması

Sertifikada kurum, görev, unvan veya yetki bilgisi yer alacaksa, sertifika sahibinin ilgili tüzel kişiyle ilişkisi ve sertifikaya yazılacak bilginin doğruluğu niteliğine uygun, doğrulanabilir belge veya resmî kayıt üzerinden kontrol edilir.

Sertifikaya temsil ve ilzam yetkisine ilişkin bir bilgi yazılması talep ediliyorsa bu yetkiyi gösteren resmî belgeler ayrıca doğrulanır. Yalnızca kurumla çalışma/görev ilişkisini gösteren bilgiler için kurum yazısı veya eşdeğer doğrulanabilir belge kullanılabilir. Doğrulanamayan bilgi sertifikaya yazılmaz.

3.2.6. Karşılıklı Çalışma Kriterleri

EİMZATR, başka bir ESHS ile çapraz veya tek yönlü sertifikasyon işletmediğinden bu kapsama ilişkin teknik güven ilişkisi kurulmaz. Üçüncü taraf doğrulamalarında EİMZATR'nin yayımladığı kök/alt kök sertifika zinciri esas alınır.

3.3. Sertifika Yenileme İsteğinde Kimlik Doğrulama

Yenileme talebi mevcut NES geçerliyken elektronik imza ile alınabiliyorsa, talep mevcut sertifikaya bağlı imza oluşturma verisi kullanılarak imzalanır ve imza geçerliliği doğrulanır. Bu yöntemin kullanılamadığı veya sertifika/kimlik bilgilerinde değişiklik bulunduğu durumlarda 3.2.3'teki kimlik doğrulama yöntemlerinden uygun olanı yeniden uygulanır.

Kurumsal bilgi içeren NES'lerde kurum ilişkisi ve yetki/görev bilgisi yenileme sırasında yeniden kontrol edilir. Güncelliği doğrulanamayan bilgi yeni sertifikaya taşınmaz; gerekli belge tamamlanana kadar talep bekletilir veya reddedilir.

3.4. İptal Talebi için Kimlik Doğrulama

İptal ve askıya alma talepleri Online İşlemler, çağrı merkezi, kayıt birimi/ofis üzerinden yazılı başvuru veya EİMZATR tarafından kabul edilen güvenli elektronik kanallar aracılığıyla alınır. Talep kanalına göre kimlik doğrulama yapılır; başarılı doğrulama olmadan sertifika statüsü değiştirilmez.

1. Online İşlemler kanalında kullanıcıya özel doğrulama bilgileri ve ilgili güvenlik adımları uygulanır.

2. Çağrı merkezi kanalında arayan kişinin kimliği, kayıtlı başvuru/sertifika bilgileri üzerinden doğrulanır ve çağrı kaydı/talep kaydı oluşturulur.

3. Fiziksel başvuruda kimlik ve talep belgesi kontrol edilir; talep yetkili personel tarafından sisteme işlenir.

4. Doğrulanan talep sertifika seri numarasıyla eşleştirilir; iptal veya askı işlemi yetkili kullanıcı tarafından gerçekleştirilir ve sonuç kayıt altına alınır.

4. SERTİFİKA YAŞAM DÖNGÜSÜ İŞLEVSEL GEREKLİLİKLERİ

4.1. Sertifika Başvurusu

4.1.1. Kimler Sertifika Başvurusunda Bulunabilir?

Başvuru, sertifika sahibi olacak gerçek kişi adına açılır. Kurumsal bilgi içeren NES talebinde de sertifika sahibi gerçek kişidir; kurumla ilişki/yetki bilgisi ayrıca doğrulanır. Yönetmelikteki kurumsal başvuru modeli EİMZATR tarafından sunulan hizmet kapsamındaysa, ilgili tüzel kişinin yetkili hesabı üzerinden toplu/kurumsal başvuru akışı işletilir ve her sertifika için ayrı gerçek kişi kaydı oluşturulur.

4.1.2. Sertifika Başvuru, Kayıt Süreci ve Sorumluluklar

Başvurular EİMZATR internet sitesi, kayıt birimleri/şubeler veya EİMZATR tarafından mevzuata uygun olarak kullanıma alınan diğer kanallar üzerinden başlatılır. Her başvuruya tekil başvuru numarası atanır.

1. Başvuru sahibinin kimlik ve iletişim bilgileri alınır; talep edilen NES süresi/türü ve teslimat yöntemi seçilir.

2. Varsa kurumsal bilgi ve bu bilginin dayanağı olan belge/ilişki bilgisi başvuruya eklenir.

3. Kimlik doğrulama süreci 3. bölümdeki yöntemle tamamlanır ve sonuç başvuruya bağlanır.

4. Başvuru sahibinin gerekli onayları, sözleşme/taahhütleri ve KDY kapsamındaki işlem belgesi tamamlanır.

5. Ücret koşulları ve başvuru bütünlüğü kontrol edilir.

6. Başvuru yetkili operasyon personelinin kontrolüne alınır; kabul edilen kayıt üretim kuyruğuna aktarılır, eksik/hatalı kayıt gerekçesiyle iade veya reddedilir.

Kayıt/kanıt: Başvuru numarası, başvuru kanalı, başvuru sahibinin onayları, kimlik doğrulama sonucu, varsa kurumsal belge, ödeme/ürün bilgisi ve tüm durum değişiklikleri sistemde tarihçe/denetim kaydıyla tutulur.

4.2. Sertifika Başvurusunun İşlenmesi

4.2.1. Kimlik Doğrulama İşlemlerinin Yerine Getirilmesi

Başvuru ekranı ve yönetim paneli, kimlik doğrulama sonucunu tamamlanmış olarak almadan üretim onayına izin vermeyecek şekilde işletilir. Yetkili personel doğrulama sonucunu ve sertifikaya yazılacak bilgileri başvuru kaydı üzerinden kontrol eder.

4.2.2. Sertifika Başvurularının Kabulü veya Reddedilmesi

Yetkili operasyon personeli başvuruyu; kimlik doğrulama, zorunlu alanlar, onay/taahhüt, ödeme, kurumsal bilgi/yetki ve teknik üretim uygunluğu yönlerinden kontrol eder. Uygun başvurunun durumu “onay/üretime hazır” seviyesine getirilir. Eksik veya doğrulanamayan başvuru, gerekçe kodu/açıklama ile başvuru sahibine iade edilir ya da reddedilir.

4.2.3. Sertifika Başvurularının İşlenme Süresi

İşlem süresi; kimlik doğrulama ve başvuru belgelerinin tamamlanmasından sonra başlar. Eksiklik nedeniyle kullanıcıya iade edilen kayıtlarda süre, eksikliklerin tamamlanması ve yeniden kontrole alınmasıyla devam eder. KDY kapsamında uygulanması gereken bilgilendirme ve bekleme süresi üretim/aktivasyon takvimine dâhil edilir.

4.3. NES Üretimi

4.3.1. NES Üretimi Sırasındaki ESHS Faaliyetleri

Üretime hazır başvuru sertifika üretim sistemine kontrollü olarak aktarılır. Üretim sistemi, başvuru kaydındaki kimlik bilgileri ile sertifika profili alanlarını eşleştirir; güvenli elektronik imza oluşturma aracı için gerekli anahtar çifti güvenli üretim ortamında oluşturulur ve NES ilgili alt kök sertifika tarafından imzalanır.

Başvuru işlemleri tamamlandığında, başvuru sahibinin TCKN/YKN’sine tanımlı mobil numaraya başvuru bilgilendirmesi gönderilir. İspatlanabilir zorunlu hâller dışında sertifika, bu bilgilendirmeden itibaren en az üç saat geçmeden aktifleştirilmez. EİMZATR’ın olağan akışında sertifika, bekleme süresi korunarak takip eden

gün 00.00 itibarıyla kullanıma açılır. Erken aktivasyon talebi yalnız belgelendirilmiş zorunluluk ve yetkili değerlendirmesiyle işleme alınır.

Kayıt/kanıt: SMS/bilgilendirme zamanı, aktivasyon zamanı, sertifika seri numarası, başvuru-seri numarası eşleşmesi ve üretim sistemine ait denetim kayıtları saklanır.

4.3.2. NES Üretimiyle İlgili Sertifika Sahibinin Bilgilendirilmesi

Sertifikanın üretim/aktivasyon durumu, başvuru sırasında kayıtlı iletişim kanallarından uygun olanı üzerinden kullanıcıya bildirilir. Teslimat yöntemi kargo ise gönderi bilgisi ayrıca kullanıcıya iletilir; şube tesliminde teslim işlemi şube kaydıyla tamamlanır.

4.4. NES'in Kabulü

4.4.1. Kabulün Şekli

Sertifika sahibi, güvenli elektronik imza oluşturma aracını kullanmadan önce sertifika görüntüleme/doğrulama aracı veya kendisine sunulan sertifika bilgileri üzerinden ad-soyad, kimlik/kurum bilgisi ve geçerlilik süresi gibi alanları kontrol eder. Hata bildirimi alınırsa kullanım durdurulur; olay kaydı açılır ve doğrulama sonucuna göre iptal/yeniden üretim süreci işletilir.

Kullanıcının herhangi bir uygunsuzluk bildirmeden sertifikayı kullanmaya başlaması kabul olarak değerlendirilir. Teslim kaydı ile sertifika kabulü birbirinden ayrıdır; kargo veya şube teslim kaydı fiziksel cihazın teslim edildiğini kanıtlar.

4.4.2. ESHS Tarafından Sertifikanın Yayımlanması

NES'in kamuya açık dizinde yayımlanması, yalnızca sertifika sahibinin bu işleme ilişkin açık onayının bulunduğu ve ilgili dizin hizmetinin aktif olarak sunulduğu durumda gerçekleştirilir. Yayım tercihi başvuru/sertifika kaydıyla ilişkilendirilir.

Onay bulunmayan NES kamuya açık dizine aktarılmaz. Dizin yayımından bağımsız olarak sertifikanın geçerlilik ve iptal durumu SİL ve OCSP hizmetleri üzerinden erişilebilir tutulur.

4.4.3. Diğer Katılımcıların Sertifika Üretimiyle İlgili Bilgilendirilmesi

Sertifika üretimi sonucunda üçüncü kişilere otomatik bireysel bildirim yapılmaz. Üçüncü kişiler gerekli durum bilgisine SİL/OCSP ve yayımlanan güven zinciri bilgileri üzerinden erişir.

4.5. NES Kullanımı

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

Güvenli elektronik imza oluşturma aracı teslim/aktivasyon sonrasında sertifika sahibinin kontrolüne bırakılır. PIN/parola ve benzeri erişim verileri EİMZATR personeliyle paylaşılmaz; kullanıcının belirlediği PIN EİMZATR tarafından açık olarak saklanmaz. Kayıp, çalıntı, yetkisiz erişim veya güvenilirlik şüphesi bildirimleri çağrı merkezi/Online İşlemler/kayıt birimi kanallarından alınır ve iptal/askı süreci başlatılır.

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

EİMZATR, üçüncü kişilerin doğrulama yapabilmesi için kök ve alt kök sertifikalarını, güncel SİL'leri ve OCSP hizmetini erişilebilir tutar. Doğrulama aracı sertifika zincirini, imza bütünlüğünü, geçerlilik zamanını ve iptal durumunu teknik profil kurallarına göre kontrol eder.

4.6. NES Yenileme

Yenileme, mevcut sertifikanın süresinin uzatılması olarak değil; yenileme talebinin uygun bulunması üzerine yeni sertifika oluşturulması şeklinde işletilir. Mevcut sertifika süresi sona ermeden talep alınır ve sertifika sahibinin güncel bilgileri kontrol edilir.

4.6.1. NES Yenilemeyi Gerektiren Durumlar

Yenileme talebi, sertifika sahibi hizmete devam etmek istediğinde veya EİMZATR kaynaklı teknik/güvenlik sebepleriyle yeni sertifika düzenlenmesi gerektiğinde başlatılır. Kayıp/çalıntı veya özel anahtar güvenliği şüphesinde önce mevcut sertifika iptal edilir; bu olay rutin yenileme olarak değerlendirilmez.

4.6.2. Yenileme Talebinde Bulunabilecek Kişiler

Standart yenileme talebi sertifika sahibi tarafından yapılır. Kurumsal bilgi içeren NES'te ilgili kurum bilgisi ve ilişki/yetki belgeleri yeniden kontrol edilir. Yönetmelikteki kurumsal başvuru hizmeti kullanılıyorsa ilgili tüzel kişinin talebi, sertifika sahibinin gerekli onayı ve yetki kontrolleriyle işleme alınır.

4.6.3. NES Yenileme Talebinin İşlenmesi

1. Talep mevcut NES ile imzalı elektronik işlem veya yeniden kimlik doğrulama yoluyla alınır.

2. Mevcut NES'in geçerlilik/iptal durumu kontrol edilir.

3. Kimlik ve sertifika bilgilerinin güncelliği; varsa kurumsal ilişki/yetki bilgisi doğrulanır.

4. Yenilemeye engel güvenlik olayı veya açık iptal durumu bulunmadığı doğrulanır.

5. Uygun talep için yeni anahtar/sertifika üretim süreci başlatılır; süresi dolmuş NES için yeni başvuru akışı uygulanır.

4.6.4. Yenilenmiş Sertifikayla İlgili Sertifika Sahibine Bildirim Yapılması

Yeni NES üretim/aktivasyon sonucu, kayıtlı iletişim kanalı ve/veya Online İşlemler üzerinden sertifika sahibine bildirilir. Yeni sertifikanın seri numarası ve teslim/aktivasyon bilgisi ilgili yenileme kaydıyla ilişkilendirilir.

4.6.5. Yenilenen NES Kabulü

Yenilenen NES, 4.4.1'deki kabul kontrollerine tabi tutulur. Sertifika sahibi yeni sertifikayı kullanmadan önce sertifika içeriğini kontrol eder; uyuşmazlık halinde işlem kaydı açılarak sertifikanın kullanımına izin verilmez.

4.6.6. ESHS Tarafından Yenilenen Sertifikanın Yayımlanması

Kamuya açık dizin yayım tercihi bulunan ve dizin hizmeti kullanılan sertifikalarda, yeni sertifika ilgili onay kaydı doğrultusunda dizine aktarılır. Eski sertifikanın durum bilgisi SİL/OCSP üzerinden güncel statüsüyle yayımlanır.

4.6.7. Diğer Katılımcıların Yeni Sertifika Üretimiyle İlgili Bilgilendirilmesi

Üçüncü kişilere bireysel bildirim yapılmaz; yeni sertifika ve eski sertifikanın durum bilgisi, uygulanabilir olduğu ölçüde dizin/SİL/OCSP ve güven zinciri servisleri üzerinden doğrulanabilir.

4.7. Anahtar Yenileme

4.7.1. Anahtar Yenilemeyi Gerektiren Durumlar

Güvenli elektronik imza oluşturma aracının kaybolması, çalınması, arızalanması; özel anahtarın güvenilirliğinin şüpheli hâle gelmesi veya yürürlükteki kriptografik kriterlerin mevcut anahtarın kullanılmasına izin vermemesi durumunda yeni anahtar çifti oluşturulur. Güvenlik şüphesi bulunan mevcut sertifika iptal sürecine alınır.

4.7.2. Anahtar Yenileme Talebinde Bulunabilecek Kişiler

Anahtar yenileme talebi sertifika sahibi tarafından doğrulanmış kanal üzerinden iletilir. Kurumsal bilgi bulunan sertifikalarda gerekli kurumsal ilişki/yetki kontrolleri de yenilenir.

4.7.3. Anahtar Yenileme Talebinin İşlenmesi

Talebin nedeni ve mevcut sertifikanın durumu kontrol edilir. Kayıp/çalıntı veya yetkisiz erişim şüphesinde mevcut sertifika derhal iptal edilir. Kimlik doğrulama ve başvuru kontrolleri tamamlandıktan sonra yeni güvenli elektronik imza oluşturma aracı/anahtar çifti kişiselleştirilir ve yeni NES üretilir.

4.7.4. Yeni Sertifikayla İlgili Sertifika Sahibine Bildirim Yapılması

4.3.2'deki üretim bildirimi süreci uygulanır.

4.7.5. Anahtarı Yenilenen Sertifikanın Kabulü

4.4.1'deki kabul kontrolü uygulanır.

4.7.6. ESHS Tarafından Anahtarı Yenilenen Sertifikanın Yayınlanması

4.4.2'deki yayım tercihi ve dizin işlemleri uygulanır; önceki sertifikanın iptal durumu SİL/OCSP'ye yansıtılır.

4.7.7. Diğer Katılımcıların Sertifika Üretimiyle İlgili Bilgilendirilmesi

Üçüncü kişilere ayrıca üretim bildirimi yapılmaz. Güncel durum bilgisi sertifika durum servislerinden doğrulanır.

4.8. Sertifika Değişikliği

4.8.1. Sertifika Değişikliğini Gerektiren Durumlar

Ad/soyad, kurum, unvan, görev veya sertifikada yer alan diğer doğrulanmış bilgilerin değişmesi ya da sertifika içeriğinde hata tespit edilmesi halinde mevcut sertifika üzerinde değişiklik yapılmaz. Yeni bilgiler doğrulandıktan sonra gerektiğinde mevcut NES iptal edilir ve yeni NES oluşturulur.

4.8.2. Sertifika Değişiklik Talebinde Bulunabilecek Kişiler

Talep sertifika sahibi tarafından; kurumsal bilgi içeren kayıtlarda ise ilgili kurum ilişki/yetki kanıtlarıyla birlikte alınır. Yetkisiz üçüncü kişilerden gelen değişiklik talepleri işleme alınmaz.

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 üretim/aktivasyon bilgisi 4.3.2'ye göre sertifika sahibine iletilir.

4.8.5. Değişiklik Yapılmış Sertifikanın Kabul Şekli

Yeni sertifika 4.4.1'e göre kontrol ve kabul edilir.

4.8.6. ESHS Tarafından Değişiklik Yapılmış Sertifikanın Yayımlanması

Yeni sertifikanın dizin yayımı varsa 4.4.2'deki açık onay ve yayın akışı uygulanır; eski sertifika durumu SİL/OCSP üzerinden güncellenir.

4.8.7. Diğer Katılımcılarının Yeni Sertifika Üretimiyle İlgili Bilgilendirilmesi

Üçüncü kişilere bireysel bildirim yapılmaz; doğrulama güncel sertifika durum servisleri üzerinden gerçekleştirilir.

4.9. Sertifika İptali ve Askıya Alma

4.9.1. Sertifika İptalini Gerektiren Durumlar

İptal nedeni sertifika sahibi talebi, yetkili kişi talebi, sertifika bilgilerinin geçersiz hâle gelmesi, kurum ilişkisinin/yetkinin sona ermesi, güvenli elektronik imza oluşturma aracının veya imza oluşturma verisinin güvenliğinin kaybı, EİMZATR kaynaklı güvenlik olayı, sertifika sahibinin ölümü veya mevzuat/sözleşme kapsamında iptali gerektiren diğer bir durum olabilir. Olay/talep alındığında ilgili sertifika seri numarası doğrulanır ve iptal yetkisine sahip kullanıcı tarafından işlem gerçekleştirilir.

4.9.2. Sertifika İptal Talebinde Bulunabilecek Kişiler

İptal talebi sertifika sahibi, EİMZATR veya sözleşme/mevzuat kapsamında iptal talebinde bulunma yetkisi bulunan kişi/kurum tarafından iletilebilir. Talebin kaynağına göre kimlik ve yetki kontrolü yapılır; kamu/yargı makamlarından gelen talepler resmî yazı ve yetki doğrulamasıyla işleme alınır.

4.9.3. Sertifika İptal Talebi Prosedürleri

1. Talep çağrı merkezi, Online İşlemler, kayıt birimi/ofis, yazılı başvuru veya kabul edilen güvenli elektronik kanal üzerinden alınır.

2. Talep sahibinin kimliği ve iptal yetkisi doğrulanır.

3. İlgili NES seri numarası, sertifika sahibi ve mevcut statü kontrol edilir.

4. Geçerli talep için sertifika statüsü derhal iptal olarak değiştirilir; işlem geri alınamaz.

5. İptal sonucu OCSP servisinde güncellenir ve ilk yayımlanacak SİL'e dâhil edilir.

6. İşlem sonucu talebin alındığı kanala uygun biçimde sertifika sahibine bildirilir ve kayıt altına alınır.

4.9.4. Sertifika İptal Talebi Gecikme Periyodu

Kimlik ve yetki doğrulaması tamamlanmış geçerli iptal talebinde ayrıca bekleme periyodu uygulanmaz. İşlem derhal sertifika yönetim sistemine yansıtılır.

4.9.5. EİMZATR'nin Sertifika İptal Talebini İşleme Süresi

Geçerli iptal talebi alındığında yetkili işlem gecikmeksizin gerçekleştirilir. OCSP statüsü işlem sonucunda güncellenir; SİL kaydı otomatik yayın periyodunda ilk listeye alınır.

4.9.6. Üçüncü Kişilerin İptal Kontrol Gerekliliği

EİMZATR, üçüncü kişilerin güncel statüye ulaşabilmesi için SİL ve OCSP servislerini sunar. Doğrulama yapan taraf, imzaya güvenmeden önce bu servislerden veya uygun doğrulama aracından güncel sertifika durumunu kontrol eder.

4.9.7. Sertifika İptal Listesi (SİL) Yayımlama Sıklığı

Son kullanıcı NES SİL'i zamanlanmış otomatik görevle her beş dakikada bir yeniden oluşturulur, EİMZATR'nin ilgili imzalama anahtarıyla imzalanır ve yayın noktasına aktarılır. SİL'in thisUpdate/nextUpdate alanları teknik profile uygun üretilir ve yayımlanan SİL 24 saatlik geçerlilik bilgisi taşır. Alt kök SİL'leri NESİ'de belirlenen periyot ve olay koşullarına göre oluşturulur.

4.9.8. SİL'lerin En Geç Yayımlanma Zamanı

SİL üretim görevi tamamlandığında dosya otomatik olarak yayın dizinine aktarılır. Yayın başarısızlığı izleme sistemleri üzerinden olay olarak değerlendirilir; yetkili teknik personel tarafından tekrar yayın ve kök neden incelemesi yapılır.

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

OCSP hizmeti, internet üzerinden erişilebilir servis uç noktaları aracılığıyla 7/24 çalıştırılır. Gelen uygun OCSP isteği sertifika veri kaynağındaki güncel duruma göre değerlendirilir ve yanıt ilgili OCSP imzalama anahtarıyla imzalanarak istemciye iletilir.

4.9.10. Çevrim İçi Sertifika İptal/Durum Kontrol Gereklilikleri

OCSP altyapısının erişilebilirliği ve yanıt üretimi sistem izleme araçlarıyla takip edilir. Yanıtların imza doğrulanabilirliği, zaman bilgisi ve sertifika durum veri kaynağıyla tutarlılığı periyodik/olay bazlı kontrollerle doğrulanır.

4.9.11. Diğer İptal Durumu Yayımlama Çeşitlerinin Varlığı

EİMZATR sertifika durumunu SİL ve OCSP üzerinden yayımlar. Bunların dışında ayrı bir sertifika durum yayın mekanizması kullanılmıyorsa ek uygulama yapılmaz.

4.9.12. Anahtar Güvenliğinin Yitirilmesine İlişkin Özel Gereklilikler

EİMZATR'ye ait sertifika imzalama verisinin güvenliğinin şüpheli hâle gelmesi durumunda bilgi güvenliği olay yönetimi, anahtar güvenliği ve iş sürekliliği prosedürleri eş zamanlı devreye alınır. Etkilenen sertifika zinciri ve son kullanıcı sertifikaları belirlenir; risk değerlendirmesine göre iptal/yeni anahtar üretimi/yeni sertifika üretimi gerçekleştirilir. Gerekli duyurular web sitesi ve uygun iletişim kanalları üzerinden yapılır.

4.9.13. Sertifika Askıya Alma Gerektiren Durumlar

Geçici şüphe veya sertifika sahibinin talebi gibi durumlarda, iptal kararı verilmeden önce NES askıya alınabilir. Askı işlemi sertifika statü kayıtlarında gerçekleştirilir ve durum bilgisi SİL/OCSP altyapısına yansıtılır.

4.9.14. Sertifika Askıya Alma Talebinde Bulunabilecek Kişiler

Askı talebi sertifika sahibinden doğrulanmış kanal üzerinden alınabilir. EİMZATR yetkili personeli, güvenli kullanımın risk altında olduğunu tespit ettiğinde kayıtlı gerekçe ile resen askı işlemi gerçekleştirebilir.

4.9.15. Sertifika Askıya Alma Talebi Prosedürü

1. Talep/olay kaydı açılır ve ilgili NES seri numarası belirlenir.

2. Sertifika sahibinden gelen taleplerde kimlik doğrulama yapılır.

3. Yetkili kullanıcı sertifika statüsünü askıda olarak değiştirir; işlem zamanı ve gerekçesi kaydedilir.

4. Askı nedeni ortadan kalktığında kimlik/yetki ve gerekçe kontrol edilerek askıdan çıkarma işlemi yapılabilir.

5. Askı/askıdan çıkarma sonucu sertifika durum servislerine yansıtılır.

4.9.16. Sertifikanın Askıda Kalma Süresinin Sınırları

Askıya alınan NES için sistemde askı başlangıç zamanı tutulur. Sertifika en fazla 30 gün askıda kalır. Bu süre içinde askıdan çıkarma işlemi yapılmamış NES, 30 günlük sürenin sonunda sistemsel kural uyarınca otomatik olarak iptal edilir; sonuç denetim kaydına ve sertifika durum servislerine yansıtılır.

4.10. Sertifika Durum Servisleri

SİL ve OCSP servisleri ayrı fakat aynı sertifika durum kayıtlarını esas alan bileşenler olarak işletilir. Sertifika üretim, askı, askıdan çıkarma ve iptal işlemlerinin güncel duruma doğru yansıyıp yansımadığı izleme ve operasyon kontrolleriyle takip edilir.

4.10.1. İşlevsel Özellikler

Son kullanıcı SİL'i her beş dakikada bir ve 24 saatlik geçerlilik bilgisiyle yayımlanır. OCSP servisi sertifika için geçerli/askıda/iptal veya teknik profile uygun diğer durum yanıtlarını çevrim içi sağlar. Yanıt ve SİL verisi sertifika yönetim sistemindeki durumla tutarlı tutulur.

4.10.2. Hizmetin Sürekliliği

SİL ve OCSP altyapısı 7/24 hizmet verecek şekilde izlenir. Servis kesintisi, erişim hatası veya veri üretim problemi tespit edildiğinde olay yönetimi süreci başlatılır; birincil sistemlerin geri getirilmesi veya gerekli hâllerde FKM bileşenlerinin devreye alınması sağlanır. NESİ'de belirlenen en geç dört saatlik yeniden erişilebilirlik hedefi iş sürekliliği planlarında dikkate alınır.

4.10.3. İsteğe Bağlı Özellikler

NESİ kapsamında ayrıca tanımlanmış isteğe bağlı sertifika durum servisi bulunmadığından ek uygulama yapılmaz.

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

Son kullanıcıya ait imza oluşturma verisi güvenli elektronik imza oluşturma aracı üzerinde oluşturulur/saklanır ve EİMZATR tarafından kopyalanmaz, merkezi olarak saklanmaz veya yeniden oluşturulabilir biçimde tutulmaz.

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

Güven Merkezi ve sistem odaları, yetkisiz fiziksel erişimi sınırlandıran kontrollü alanlar içinde işletilir. Kritik sistemler, çevresel tehditler ve altyapı kesintileri dikkate alınarak konumlandırılır; fiziksel güvenlik, enerji, iklimlendirme, yangın ve su riski kontrolleri bütüncül olarak uygulanır.

5.1.2. Fiziksel Erişim

Kritik alanlara erişim yalnız görev gereği yetkili personele tanımlanır. Personel girişleri kartlı geçiş/erişim sistemi üzerinden kayıt altına alınır. Ziyaretçiler yetkili personel refakatinde bulunur; ziyaret kaydı tutulur. İşten ayrılma/görev değişikliği hâlinde fiziksel erişim yetkileri kaldırılır.

5.1.3. Güç Kaynakları ve Havalandırma

Kritik bilgi sistemleri kesintisiz güç kaynaklarıyla desteklenir. Sistem odalarında cihazların güvenli çalışma sıcaklığını sağlayan iklimlendirme altyapısı kullanılır. Enerji/iklimlendirme arızaları izlenir ve bakım kayıtları saklanır.

5.1.4. Su Baskınları

Sistem odalarında su sızıntısı ve su baskını riskini erken tespit etmek amacıyla su algılama sensörleri kullanılır. Sensör uyarıları ve fiziksel kontroller bakım/olay yönetimi süreçlerine dâhil edilir; kritik cihazlar su kaynaklı riskler dikkate alınarak konumlandırılır.

5.1.5. Yangın Önleme ve Yangından Korunma

Kritik alanlarda yangın algılama/alarm sistemleri ve bilgi teknolojisi ekipmanlarına uygun otomatik söndürme altyapısı kullanılır. Sistemlerin periyodik bakım ve kontrolleri yetkili hizmet sağlayıcılarca gerçekleştirilir ve kayıt altına alınır.

5.1.6. Saklama Ortamları

Elektronik kayıt ve yedekler yetkilendirilmiş sunucu/depolama sistemlerinde tutulur. Fiziksel belge saklanması gereken durumlarda erişimi sınırlandırılmış arşiv alanları kullanılır. Saklama ortamlarının erişim ve çevresel kontrolleri bilgi sınıflandırmasına uygun belirlenir.

5.1.7. Atıkların Atılması

Kişisel, gizli veya güvenlik açısından hassas veri içeren kâğıt ve elektronik ortamlar yeniden kullanıma verilmeden önce geri döndürülemeyecek yöntemlerle imha edilir. Elektronik ortamlar güvenli silme/fiziksel imha prosedürlerine, kâğıt belgeler kontrollü parçalama/imha süreçlerine tabi tutulur; gerekli imha kayıtları saklanır.

5.1.8. Tesis Dışı Yedekleme

İş sürekliliği için gerekli sistem ve verilerin yedekleri Genel Merkez dışındaki FKM veya güvenli elektronik depolama altyapısında tutulur. Yedekler erişim kontrolü, bütünlük kontrolü ve geri yükleme testleriyle doğrulanır. Yedeklerin taşınması fiziksel medya ile değil, kontrollü ve güvenli elektronik aktarım/depolama yöntemleriyle yürütülür.

5.2. Prosedürel Kontroller

5.2.1. Güvenilir Roller

Sertifika üretimi, CA/HSM yönetimi, sistem/ağ yönetimi, kayıt yönetimi, arşiv, denetim ve güvenlik operasyonlarında görev alan güvenilir roller görev tanımları ve erişim yetki matrisleriyle belirlenir. Rol atamaları yönetim onayıyla gerçekleştirilir; erişimler kişisel hesaplarla ilişkilendirilir.

5.2.2. Her Görev İçin Gereken En Az Kişi Sayısı

Rutin operasyonlarda görev için gerekli asgari kişi sayısı risk ve görev ayrılığı esasına göre belirlenir. CA anahtar oluşturma, kritik anahtar yedekleme/geri yükleme ve benzeri yüksek riskli kriptografik işlemler en az iki yetkili güvenli personelin katılımı ve kontrolüyle yürütülür. Arşiv ve diğer operasyonel görevlerde ikili kontrol yalnız ilgili risk/prosedür gerektiriyorsa uygulanır.

5.2.3. Her Görev için Kimlik Doğrulama

Kritik sistemlere erişim kişisel kullanıcı hesabı, güçlü kimlik doğrulama ve rol bazlı yetki kontrolüyle sağlanır. Servis hesapları yalnız ilgili hizmet için kullanılır; yetki ve parola/anahtar yönetimi kontrollü olarak yapılır. Kritik işlemlerin hangi kullanıcı veya servis hesabı tarafından gerçekleştirildiği loglanır.

5.2.4. Görevlerin Ayrılmasını Gerektiren Roller

Talep açma/onay, sistem yönetimi/güvenlik denetimi, CA anahtar yönetimi ve kritik değişikliklerin uygulanması gibi birbirini denetlemesi gereken görevler mümkün olduğunca farklı rollere dağıtılır. Bir kullanıcının kendi işlemini tek başına onaylamasına yol açabilecek yetki birleşimleri periyodik erişim gözden geçirmelerinde kontrol edilir.

5.3. Personel Kontrolleri

5.3.1. Nitelik, Deneyim ve Güvenlik Gereklilikleri

Güvenli personel ve genel personel rolleri, görevin kritikliği dikkate alınarak ayrılır. Kritik göreve atanacak personelin kimliği, adli sicil ve mevzuatın izin verdiği geçmiş kontrolleri, mesleki yeterliliği, deneyimi ve güvenilirliği değerlendirilir. Atama öncesinde gizlilik ve bilgi güvenliği yükümlülükleri personele bildirilir.

5.3.2. Kişisel Geçmiş Kontrol Gereklilikleri

Kritik görevlere atamada geçerli mevzuat ve şirket insan kaynakları/güvenlik prosedürleri çerçevesinde gerekli geçmiş kontrolleri yapılır. Kontrol sonucu yalnız yetkili personelin erişebileceği personel dosyasında muhafaza edilir.

5.3.3. Eğitim Gereklilikleri

Personel göreve başlamadan önce elektronik imza mevzuatı, NESİ/NESUE, sertifika yaşam döngüsü, bilgi güvenliği, kişisel veri güvenliği, olay yönetimi ve görevine özgü teknik sistemler hakkında eğitim alır. Kritik sistem erişimi, görev için gerekli eğitim/yetkinlik tamamlandıktan sonra verilir.

5.3.4. Tekrar Eğitimi Sıklığı ve Gereklilikleri

Mevzuat, sistem veya süreç değişikliği; denetim bulgusu; güvenlik olayı veya eğitim ihtiyacı ortaya çıktığında tazeleme eğitimi planlanır. Eğitim katılımı ve içeriği kayıt altına alınır.

5.3.5. İş Rotasyonu Sıklığı ve Sırası

Zorunlu bir iş rotasyonu periyodu uygulanmıyorsa görev değişiklikleri organizasyon ihtiyacı ve risk değerlendirmesine göre yapılır. Görev değişikliğinde eski yetkiler kaldırılır, yeni yetkiler onaylı rol profiline göre tanımlanır.

5.3.6. Yetkisiz İşlemler için Yaptırımlar

Yetki dışı işlem, güvenlik prosedürü ihlali veya gizlilik ihlali tespitinde bilgi güvenliği olay yönetimi ve insan kaynakları/disiplin süreçleri işletilir. Gerektiğinde erişim derhal askıya alınır; olay kayıtları korunur ve hukuki/idari bildirim yükümlülükleri değerlendirilir.

5.3.7. Bağımsız Alt Yüklenici Gereklilikleri

Alt yükleniciler işe başlamadan önce hizmet kapsamı, bilgiye erişim ihtiyacı, güvenlik şartları, gizlilik yükümlülükleri, olay bildirim süresi ve hizmet sonlandırma/erişim kapatma koşulları sözleşmede tanımlanır. Uzaktan veya yerinde erişimler süreli ve yetkili personel gözetiminde yürütülür; kritik değişiklikler şirket personelinin onayıyla uygulanır.

5.3.8. Personele Sağlanan Dokümantasyon

Personel, göreviyle ilgili güncel NESİ/NESUE, politika, prosedür, talimat ve teknik kullanım kılavuzlarına kontrollü doküman sistemi üzerinden erişir. Eski/iptal edilmiş dokümanların yanlışlıkla kullanılmasını önlemek için sürüm yönetimi uygulanır.

5.4. Denetim Kayıtları Alma Prosedürleri

5.4.1. Kaydedilen Olay Tipleri

Sertifika başvurusu, kimlik doğrulama, başvuru kabul/red, üretim, aktivasyon, teslimat, yenileme, değişiklik, askıya alma, askıdan çıkarma, iptal, SİL/OCSP işlemleri ile kritik sistem/ağ/uygulama yönetim faaliyetleri denetim kapsamına alınır. Mümkün olan sistemlerde kullanıcı, işlem, tarih-saat, kaynak IP/cihaz, işlem sonucu ve değişen veriler kayıt altına alınır.

Merkezi toplama: Sistem ve güvenlik logları merkezi log/SIEM platformu olan Logsign'a aktarılır. Kaynakların log gönderim durumu izlenir; kritik kaynaklarda log akışının kesilmesi olay olarak değerlendirilir.

5.4.2. Kayıtları İşleme Sıklığı

Log üretimi ve merkezi toplama süreklidir. Kayıtların planlı gözden geçirmesi aylık kontrol kapsamında yapılır; güvenlik olayı, sistem kesintisi, şüpheli işlem veya denetim ihtiyacında ilgili kayıtlar periyot beklenmeden incelenir.

5.4.3. Denetim Kayıtlarının Saklanma Süresi

Operasyonel çevrim içi logların erişilebilir saklama süresi sistem kapasitesi ve kayıt yönetimi politikasına göre belirlenir. Mevzuat kapsamında uzun süre saklanması gereken sertifika yaşam döngüsü ve denetim kanıtları arşiv ortamına alınarak en az 20 yıl muhafaza edilir.

5.4.4. Denetim Kayıtlarının Korunması

Log sistemine erişim rol bazlı sınırlandırılır; kayıtların yetkisiz değiştirilmesini veya silinmesini önleyen erişim, bütünlük ve yedekleme kontrolleri uygulanır. Kaynak sistem saatleri güvenilir zaman kaynağıyla senkronize edilir. Log dışa aktarımları/raporları yetkili kullanıcılar tarafından alınır ve gerektiğinde bütünlük kanıtlarıyla birlikte arşivlenir.

5.4.5. Denetim Kayıtlarının Yedeklenme Prosedürleri

Merkezi log platformu ve kritik kaynakların yedekleri kurumsal yedekleme prosedürü kapsamında alınır. Yedeklerin başarısı izlenir; geri yükleme kabiliyeti planlı testlerle doğrulanır.

5.4.6. Denetim Bilgisi Toplama Sistemi (İç ve Dış)

ESHS faaliyetlerinde üretilen uygulama, veritabanı, işletim sistemi, ağ ve güvenlik cihazı logları merkezi log/SIEM platformu olan Logsign'a aktarılır. Log kaynağı, olay zamanı, olay türü, kullanıcı/sistem bilgisi ve ilgili teknik alanlar kaynak sistemin üretebildiği ölçüde merkezi kayıtta tutulur.

Kaynakların log gönderim durumu izlenir; kritik bir kaynağın log akışının kesilmesi veya olağan dışı log davranışı bilgi güvenliği olayı kapsamında değerlendirilir. Sistemsel log üretmeyen kritik manuel işlemler için işlem formu, tutanak veya uygulama içi denetim kaydı oluşturulur.

Kayıt/kanıt: merkezi log kayıtları, kaynak tanımı, log akış durumu, ilgili olay/inceleme kayıtları ve manuel işlem kanıtları.

5.4.7. Olayı Yaratan Kişiyi Bilgilendirme

Denetim kaydı üretildiğine dair kullanıcıya işlem bazında ayrıca bildirim yapılmaz. Güvenlik olayı veya uyum ihlali tespitinde ilgili kişinin bilgilendirilmesi, olay yönetimi ve insan kaynakları/hukuk süreçlerine göre gerçekleştirilir.

5.4.8. Zarar Görebilirlik Değerlendirmesi

Log incelemeleri, zafiyet taramaları, güvenlik testleri ve olay analizlerinde tespit edilen zayıflıklar risk/olay kaydına alınır. Düzeltici faaliyet, sorumlu ve hedef tarih belirlenir; uygulama sonrasında etkinlik doğrulaması yapılır.

5.5. Kayıtların Arşivlenmesi

5.5.1. Arşivlenen Kayıt Tipleri

Başvuru ve kimlik doğrulama kayıtları, KDY işlem belgeleri, sözleşme/taahhütler, sertifika üretim/yenileme/değişiklik/iptal/askı kayıtları, teslimat kanıtları, üretilen sertifikalar, SİL'ler, kritik denetim kayıtları ile NESİ/NESUE sürümleri arşivlenir. Elektronik kanıtlar ilgili başvuru/sertifika numarası üzerinden bulunabilir olacak şekilde indekslenir.

5.5.2. Arşivlerin Saklanma Süresi

Mevzuat kapsamında saklanması gereken ESHS kayıtları en az 20 yıl tutulur. Saklama süresi dolmadan kayıt silme/imha işlemi yapılmaz; hukuki ihtilaf, denetim veya yasal saklama gereksinimi varsa imha süreci durdurulur.

5.5.3. Arşivlerin Korunması

Elektronik arşiv erişimi yetkili rollerle sınırlandırılır; arşiv sorumlusu kayıtların erişilebilirliğini ve okunabilirliğini takip eder. Fiziksel belgeler erişimi kontrollü arşiv alanında saklanır. Arşiv kaydının değiştirilmesi/silinmesi yetkisiz kullanıcılar için engellenir ve erişim işlemleri loglanır.

5.5.4. Arşivlerin Yedeklenme Prosedürleri

Elektronik arşiv verileri kurumsal yedekleme altyapısıyla yedeklenir; yedek kopyalar Genel Merkez dışında FKM/güvenli elektronik depolama ortamında tutulabilir. Yedekler erişim ve bütünlük kontrolleriyle korunur; geri dönüş testleri planlı olarak gerçekleştirilir.

5.5.5. Kayıtların Zaman Damgası Altına Alınması Gereklilikleri

Kayıtların tarih-saat bilgisi güvenilir zaman kaynaklarıyla senkronize edilmiş sistemlerden üretilir. Merkezi log yönetiminde kayıt bütünlüğünü ve zaman bilgisinin doğrulanabilirliğini destekleyen kriptografik bütünlük ve imzalama/damgalama kontrolleri uygulanır.

Mevzuat veya ilgili işlem akışının güvenilir zaman kanıtı gerektirdiği kayıt ve belgelerde ayrıca zaman damgası mekanizması kullanılır. Kullanılan mekanizmaya ilişkin doğrulama verileri ilgili kayıt veya belgeyle birlikte muhafaza edilir.

5.5.6. Arşiv Toplama Sistemi

Elektronik kayıtlar kaynak sistemlerden arşiv ortamına kontrollü iş akışı veya yedekleme/aktarım süreçleriyle alınır. Fiziksel kayıtlar arşiv sorumlusuna teslim kaydıyla devredilir. Kayıt sınıfı, saklama süresi, erişim yetkisi ve ilgili başvuru/sertifika referansı arşiv indeksinde tutulur.

5.5.7. Arşiv Bilgisinin Edinilmesi ve Doğrulanması Prosedürleri

Arşivden kayıt talebi yalnız yetkili kişi/birim tarafından açılır. İstenen kayıt, başvuru numarası, sertifika seri numarası, kişi/kurum bilgisi veya tarih aralığı üzerinden bulunur. Çıkarılan elektronik kayıtların bütünlük ve okunabilirlik kontrolü yapılır; dışarı verilen kopya/rapor teslimi kayıt altına alınır.

5.6. Anahtar Değişimi

EİMZATR CA anahtarlarının yaşam döngüsü, sertifika geçerlilik süreleri, kriptografik güvenlik seviyesi ve yürürlükteki teknik kriterler dikkate alınarak yönetilir. Yeni CA anahtarı gerektiğinde anahtar töreni planlanır; yetkili güvenli personel katılımıyla HSM üzerinde yeni anahtar çifti oluşturulur, gerekli sertifikalar üretilir ve

güven zinciri kontrollü olarak devreye alınır. Eski doğrulama anahtarları geçmiş sertifikaların doğrulanabilmesi için erişilebilir ve arşivlenmiş olarak tutulur.

5.7. Güvenliğin Yitirilmesi ve Felaket Kurtarma

5.7.1. Güvenlik Kaybına Neden Olabilecek Olaylar

Yetkisiz erişim, kötü amaçlı yazılım, veri bütünlüğü kaybı, CA anahtarı güvenliği şüphesi, fiziksel güvenlik olayı, enerji/iletişim kesintisi, kritik sistem arızası ve benzeri durumlar bilgi güvenliği olayı olarak değerlendirilir. Olay tespitinde olay kaydı açılır, etki ve kapsam belirlenir, deliller korunur ve gerekli izolasyon/kurtarma işlemleri başlatılır.

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

Bozulma veya kayıp tespitinde etkilenen sistem servis dışı bırakılabilir; yedek sunucu/servis bileşeni devreye alınır. Veriler doğrulanmış yedeklerden geri yüklenir, servis fonksiyonları ve veri bütünlüğü test edilir. Geri dönüş mümkün değilse sertifika yaşam döngüsüne etkisi değerlendirilir ve gerekli sertifika iptal/yeniden üretim işlemleri uygulanır.

5.7.3. İmza Oluşturma Verilerinin Güvenliğinin Yitirilmesi

CA imza oluşturma verisinin gizliliği veya güvenilirliği kaybolduğunda ilgili anahtar kullanımı durdurulur. Etkilenen sertifika zinciri belirlenir, iptal ve yeni anahtar oluşturma süreçleri yetkili güvenli personel tarafından yürütülür; gerekli sertifika sahipleri ve üçüncü kişiler uygun kanallarla bilgilendirilir.

5.7.4. İş Sürekliliği Yetenekleri ve Felaket Kurtarma

Birincil merkezde hizmet verilememesi hâlinde iş sürekliliği planı devreye alınır. Kritik servisler önceliklendirilir; FKM'de hazır tutulan sistemler, yedekler ve güvenli bağlantılar kullanılarak servisler geri kazanılır. Sertifika durum servisleri, sertifika üretim/başvuru bileşenleri ve destek sistemleri için geri kazanım sırası iş sürekliliği planlarında tanımlanır. Geri dönüş sonrası veri bütünlüğü ve servis testleri tamamlanmadan normal işletime geçilmez.

5.7.5. EİMZATR'nin Faaliyetinin Son Bulması

EİMZATR faaliyetinin sonlandırılması kararı hâlinde, mevzuatta öngörülen süre ve usullere göre BTK bildirimi, kullanıcı/kamuoyu bilgilendirmesi ve hizmetlerin kontrollü sonlandırılmasına ilişkin plan devreye alınır. Mevzuatın öngördüğü tarihten itibaren yeni NES başvurusu ve yeni sertifika üretimi durdurulur.

Mevcut sertifika ve arşiv kayıtlarının devri gerekiyorsa aktarım kapsamı, teslim yöntemi, bütünlük kontrolleri ve sorumlular belirlenerek kontrollü devir gerçekleştirilir. Devredilemeyen veya kullanımının sürdürülmesi mümkün olmayan sertifikalar mevzuat kapsamında iptal edilir ve sertifika durum hizmetlerinin devamına ilişkin yükümlülükler yerine getirilir.

Arşiv ve kayıtlar mevzuatta öngörülen süre boyunca korunur. EİMZATR'ye ait kritik imza oluşturma verilerinin imhası, artık kullanılmalarını gerektiren yükümlülüklerin sona ermesinden sonra yetkili güvenli personel tarafından kontrollü ve kayıtlı biçimde gerçekleştirilir.

6. TEKNİK GÜVENLİK KONTROLLERİ

6.1. Anahtar Çifti Üretimi ve Kurulumu

6.1.1. Anahtar Çifti Üretimi

Kök ve alt kök CA anahtar çiftleri, yetkilendirilmiş güvenli personelin katıldığı kontrollü anahtar töreni kapsamında, güvenli kriptografik donanım modülü üzerinde oluşturulur. Tören öncesinde kullanılacak HSM, yetki bileşenleri, prosedür ve katılımcılar kontrol edilir; işlem adımları kayıt/tutanakla belgelenir.

HSM ve anahtar üretim yöntemi yürürlükteki Tebliğ ve ilgili teknik kriterlerde öngörülen güvenlik seviyesini karşılar. CA imza oluşturma verisi yedekleme amacı dışında güvenli modül dışına açık biçimde çıkarılmaz.

6.1.2. İmza Oluşturma Verisinin Sertifika Sahibine Ulaştırılması

Son kullanıcı anahtarı güvenli elektronik imza oluşturma aracı içinde tutulur. Şube tesliminde cihaz sertifika sahibine yüz yüze teslim edilir ve teslim kaydı oluşturulur. Kargo tesliminde cihaz, gönderi takip bilgisiyle güvenli kargo sürecine verilir; kargo teslim sonucu/teslim alan bilgisi başvuru kaydıyla ilişkilendirilir. Teslim öncesinde/teslim sırasında uygulanması gereken kimlik doğrulama kontrolleri ilgili kanal prosedürüne göre yapılır.

6.1.3. İmza Doğrulama Verisinin ESHS'ye Ulaştırılması

Anahtar üretimi sırasında oluşan açık anahtar, güvenli üretim sürecinde ilgili başvuru kaydıyla eşleştirilerek sertifika üretim sistemine aktarılır. Aktarım yetkili sistem bileşenleri arasında güvenli iletişim kanalı üzerinden gerçekleştirilir; veri bütünlüğü teknik kontrollerle doğrulanır.

6.1.4. EİMZATR İmza Doğrulama Verilerinin Üçüncü Kişilere Ulaştırılması

EİMZATR kök ve alt kök sertifikaları kamuya açık bilgi deposunda indirmeye sunulur. Yayınlanan sertifika dosyalarının doğru sürüm ve güven zincirine ait olduğu yayın öncesi kontrol edilir; önceki/geçerli sertifikaların arşiv erişimi korunur.

6.1.5. Anahtar Uzunlukları

Anahtar uzunlukları, algoritmalar ve diğer kriptografik parametreler sertifika üretim profilleri ve güvenlik yapılandırmalarında merkezi olarak tanımlanır. Kullanılan değerlerin yürürlükteki Tebliğ, BTK profilleri ve ilgili teknik standartlarda belirtilen asgari güvenlik gerekliliklerini karşılaması sağlanır.

Yeni sertifika profili, algoritma veya anahtar parametresi devreye alınmadan önce teknik ve mevzuatsal uygunluk kontrol edilir; değişiklik kontrollü değişiklik yönetimi süreciyle uygulanır. Böylece kriptografik parametrelerin güncelliği, dokümanda sabit teknik değerlere bağımlı kalmadan yönetilir.

6.1.6. Anahtar Üretimi ve Kalite Kontrolü

Son kullanıcı anahtarları, EİMZATR'nin güvenli üretim sürecinde güvenli elektronik imza oluşturma aracında/uygun güvenli kriptografik bileşende oluşturulur. Üretimden sonra açık anahtar formatı, sertifika profili ve cihaz-sertifika eşleşmesi teknik kontrollerden geçirilir. Hatalı üretim tespitinde ilgili cihaz/anahtar kullanıma verilmez ve kayıt altına alınır.

6.1.7. Anahtar Kullanım Amaçları

Son kullanıcı imza oluşturma verisi yalnız güvenli elektronik imza oluşturmak için kullanılır. CA imza anahtarları sertifika/SİL ve güven altyapısı kapsamındaki yetkili imzalama işlemleriyle sınırlandırılır; OCSP ve zaman damgası hizmetlerine ait anahtarlar kendi hizmet amaçları dışında kullanılmaz. HSM üzerindeki anahtar kullanım yetkileri bu ayrımı destekleyecek biçimde yapılandırılır.

6.2. İmza Oluşturma Verisinin Korunması ve Kriptografik Modül Mühendislik Kontrolleri

6.2.1. Kriptografik Modül Standartları ve Kontroller

HSM cihazları teslim alındığında fiziksel bütünlük, paket/mühür ve cihaz kimlik bilgileri kontrol edilir; ilk kurulum yetkili güvenli personel tarafından kontrollü alanda yapılır. HSM yönetim erişimleri çoklu yetkilendirme ve rol ayrılığıyla sınırlandırılır. Cihazlar kullanım ömrü boyunca sağlık/güvenlik durumu açısından izlenir; arıza veya güvenlik olayı bilgi güvenliği olay sürecinde ele alınır.

6.2.2. İmza Oluşturma Verisinin Çok Kullanıcılı Kontrolü

CA özel anahtarına erişim tek bir kişinin tek başına gerçekleştiremeyeceği biçimde yetki bileşenlerine ayrılır. Kritik anahtar kullanım/backup/restore işlemleri en az iki yetkili güvenli personelin birlikte katılımıyla yapılır. Son kullanıcı anahtarları ise yalnız sertifika sahibinin PIN/parola ile kontrol ettiği güvenli cihaz üzerinde kullanılabilir.

6.2.3. İmza Oluşturma Verisinin Saklanması

Son kullanıcıya ait özel anahtarın sunucu, veritabanı veya EİMZATR arşivinde kopyası tutulmaz. CA özel anahtarları yalnız onaylı HSM/kriptografik güvenli modül ve prosedürde tanımlı güvenli yedek bileşenlerinde korunur.

6.2.4. İmza Oluşturma Verisinin Yedeklenmesi

Son kullanıcı anahtarları yedeklenmez. CA anahtar yedekleri, anahtar töreni veya onaylı anahtar yönetimi prosedürü kapsamında çoklu yetkilendirme ile oluşturulur; yedekler şifreli/korumalı kriptografik taşıyıcıda farklı güvenli lokasyonlarda muhafaza edilir. Yedek erişimi ve geri yükleme işlemleri kayıt altına alınır.

6.2.5. İmza Oluşturma Verisinin Arşivlenmesi

Son kullanıcı özel anahtarları arşivlenmez. Süresi sona eren CA anahtarları aktif imzalama için kullanılmayacak şekilde yönetilir; doğrulama için gerekli CA sertifikaları ve açık anahtar bilgileri mevzuatın öngördüğü saklama süresince arşivlenir.

6.2.6. İmza Oluşturma Verisinin Kriptografik Modül Transferi

CA özel anahtarı yalnız yedekleme/geri yükleme gibi onaylı işlemlerde, HSM'nin güvenli anahtar taşıma mekanizmasıyla ve çoklu yetkili personel kontrolünde başka onaylı kriptografik modüle aktarılabilir. Açık/şifresiz özel anahtar aktarımına izin verilmez. Son kullanıcı anahtarları üretildikleri güvenli elektronik imza oluşturma aracı dışına çıkarılmaz.

6.2.7. İmza Oluşturma Verisinin Kriptografik Modülde Saklanması

CA anahtarları HSM içerisinde erişim politikaları, kimlik doğrulama ve yetki bölüşümüyle korunur. Anahtar nesnelerinin dışa aktarılabilirlik özellikleri prosedür ve cihaz güvenlik politikasına göre sınırlandırılır.

6.2.8. Gizli Anahtarın Aktive Edilme Yöntemi

CA özel anahtarının aktivasyonu, gerekli sayıda güvenli personelin HSM kimlik doğrulama/anahtar bileşenlerini kullanmasıyla gerçekleştirilir. Son kullanıcı özel anahtarı, sertifika sahibinin güvenli cihaz üzerinde PIN/parola ile başarılı kimlik doğrulaması sonrasında kullanılabilir.

6.2.9. Gizli Anahtarın Deaktive Edilme Yöntemi

CA anahtarı oturum sonlandırma, HSM güvenli kapatma veya anahtarın kullanım dışı bırakılması prosedürüyle deaktive edilir. Kritik deaktive etme işlemleri yetkili personel kontrolünde kaydedilir. Son kullanıcı anahtarı cihaz oturumu kapatıldığında/PIN doğrulaması sona erdiğinde kullanılamaz hâle gelir.

6.2.10. Gizli Anahtarı Yok Etme Metodu

CA anahtarının yaşam döngüsü sonunda, tüm onaylı HSM ve yedek kopyalarda güvenli silme/imha işlemi yapılır. İmha kararı ve işlemi yetkili güvenli personel tarafından yürütülür; kritik imhada görev ayrılığı uygulanır ve tutanak oluşturulur. Son kullanıcı özel anahtarının imhası cihazın güvenli silme fonksiyonu veya cihazın güvenli fiziksel imhası yoluyla gerçekleştirilir.

6.2.11. Kriptografik Modül Değerlendirmesi

Kullanılan HSM ve son kullanıcı güvenli elektronik imza oluşturma araçlarının, devreye alındıkları tarihte yürürlükteki teknik kriter ve güvenlik sertifikasyon şartlarını karşıladığı tedarikçi/ürün belgeleriyle doğrulanır. Ürün sertifikaları ve teknik değerlendirme kayıtları ilgili varlık kayıtlarıyla ilişkilendirilir.

6.3. Anahtar Çifti Yönetimiyle İlgili Diğer Konular

6.3.1. İmza Doğrulama Verilerinin Arşivlenmesi

Kök/alt kök sertifikalar, son kullanıcı NES'leri ve doğrulama için gerekli açık anahtar bilgileri arşivleme politikasına alınır. Sertifika dosyaları, geçerlilik dönemleri, seri numarası ve zincir bilgileri üzerinden bulunabilir durumda en az mevzuatta öngörülen süre boyunca saklanır.

6.3.2. Sertifikanın İşlevsel Süreleri ve Anahtar Çifti Kullanım Süreleri

Son kullanıcı NES geçerlilik süresi başvuru sırasında seçilen ürün/hizmet koşullarına göre üretim sistemine aktarılır ve sertifikadaki NotBefore/NotAfter alanları bu bilgiyle oluşturulur. CA sertifika ve anahtar kullanım süreleri güvenlik, teknik kriter ve sertifika zinciri planına göre yönetilir. Süresi dolan anahtar yeni imza üretiminde kullanılmaz; geçmiş imzaların doğrulanabilmesi için açık doğrulama verileri erişilebilir tutulur.

6.4. Erişim Şifreleri

6.4.1. Erişim Şifrelerinin Oluşturulması ve Kurulumu

CA/HSM erişim kimlikleri güvenli personel bazında ve çoklu kontrol gereksinimini destekleyecek biçimde tanımlanır. Son kullanıcı güvenli cihazı için PIN, aktivasyon sürecinde sertifika sahibi tarafından belirlenir veya kullanıcıya güvenli aktivasyon yöntemi sunulur; kullanıcı tarafından belirlenen PIN EİMZATR tarafından açık olarak saklanmaz.

6.4.2. Erişim Şifrelerinin Korunması

Personel erişim parolaları ve kriptografik kimlik doğrulama bileşenleri kişiye özeldir; paylaşılması yasaktır. Parola politikaları, başarısız giriş, kilitleme ve yetki iptali kontrolleri sistem yeteneklerine göre uygulanır. Son kullanıcı PIN/parola güvenliği kullanıcı sorumluluğunda olup kayıp/şüphe durumunda sertifika güvenliği prosedürü devreye alınır.

6.4.3. Erişim Şifreleriyle İlgili Diğer Konular

Aktivasyon kodları ve geçici erişim bilgileri güvenli kanallarla iletilir veya sistem üzerinde kriptografik olarak korunur; açık metin olarak kalıcı saklanmaz. Aktivasyon sırasında istemci ile EİMZATR sistemleri arasındaki haberleşme şifreli kanal üzerinden gerçekleştirilir.

6.5. Bilgisayar Güvenlik Kontrolleri

6.5.1. Bilgisayar Güvenliği Teknik Gereklilikleri

Sertifika hizmetlerinde kullanılan sunucu, uygulama, veritabanı ve yönetim sistemleri; kimlik doğrulama, rol bazlı yetkilendirme, kötü amaçlı yazılım koruması, güvenlik duvarı/ağ segmentasyonu, yama ve zafiyet yönetimi, loglama, yedekleme ve güvenli yapılandırma kontrolleriyle korunur. Sertifika başvuru, üretim, askı ve iptal gibi kritik işlemler uygulama/veritabanı denetim kayıtlarıyla izlenebilir tutulur.

Yönetim erişimleri kişisel hesaplarla yapılır. Üretim ortamı değişiklikleri değişiklik talebi, test/etki değerlendirmesi, onay ve uygulama kaydı ile gerçekleştirilir. Tedarikçi uzaktan erişimi gerektiğinde süreli ve yetkili EİMZATR personeli gözetiminde açılır; işlem bitiminde erişim sonlandırılır.

6.5.2. Bilgisayar Güvenliğinin Derecelendirilmesi

İlgili değildir.

6.6. Yaşam Döngüsü Teknik Kontrolleri

6.6.1. Sistem Geliştirme Kontrolleri

Sertifika yaşam döngüsü sistemlerindeki yazılım geliştirme ve bakım işlemleri kontrollü değişiklik yönetimi kapsamında yürütülür. Geliştirme/test ve üretim ortamları görev ve erişim açısından ayrıştırılır. Kod değişiklikleri yetkili geliştirici tarafından hazırlanır, test edilir; üretime geçiş EİMZATR'nin onaylı değişiklik süreci ve yetkili personeli üzerinden gerçekleştirilir. Değişen dosyalar/sürüm, test sonucu, yedek/geri dönüş planı ve uygulayan/onaylayan bilgileri kayıt altına alınır.

6.6.2. Güvenlik Yönetimi Kontrolleri

Bilgi varlıkları risk değerlendirmesine tabi tutulur; güvenlik açıkları, yapılandırma değişiklikleri ve tedarikçi erişimleri ilgili BGYS prosedürleriyle yönetilir. Kritik değişikliklerden önce yedek ve geri dönüş yöntemi doğrulanır; uygulama sonrasında servis ve log kontrolleri yapılarak değişiklik kapatılır.

6.6.3. Yaşam Döngüsü Güvenlik Kontrolleri

İlgili değildir.

6.7. Ağ Güvenlik Kontrolleri

Güven Merkezi, kullanıcı/kurumsal ağlar, yönetim ağları ve dış servis bağlantıları uygun ağ segmentleri ve güvenlik duvarı kurallarıyla ayrılır. İnternete açık servisler yalnız gerekli port/protokoller üzerinden

yayımlanır. Kayıt birimi bağlantıları ve uzaktan yönetim erişimleri şifreli, kimlik doğrulamalı güvenli kanallar üzerinden sağlanır. Ağ ve güvenlik cihazı logları merkezi log platformuna gönderilir.

6.8. Zaman Damgası

Sertifika hizmetlerinde kullanılan sunucular güvenilir zaman kaynaklarıyla senkronize edilir. KDY işlem belgeleri ve zaman kanıtı gerektiren diğer elektronik belgelerde EİMZATR zaman damgası hizmeti veya mevzuata uygun güvenilir zaman damgası mekanizması kullanılır. Zaman damgası isteği/yanıtı ile ilgili uygulama kaydı, işlem belgesiyle ilişkilendirilerek saklanır.

Zaman damgası hizmeti internet/ağ güvenliği kontrolleri altında işletilir; servis erişimi, sertifika/anahtar kullanımı ve sistem sağlığı izlenir. Yetkisiz istek ve yönetim erişimleri güvenlik duvarı ve uygulama kontrolleriyle sınırlandırılır.

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

7.1. Sertifika Profili

Sertifika profilleri üretim sisteminde kontrollü teknik şablonlar olarak tanımlanır. Profil değişiklikleri teknik kriter ve BTK profil dokümanlarıyla karşılaştırılır; test ortamında doğrulandıktan ve değişiklik onayı alındıktan sonra üretime alınır.

7.1.1. Sürüm Numaraları

Kök, alt kök ve son kullanıcı NES üretim şablonları X.509 v3 formatında yapılandırılır. Üretilen sertifika örnekleri dağıtımdan önce teknik doğrulama araçlarıyla sürüm ve alan yapısı açısından kontrol edilir.

7.1.2. Sertifika Uzantıları

Zorunlu/isteğe bağlı sertifika alan ve uzantıları BTK NES/SİL/OCSP profilleri ve RFC 5280 esas alınarak şablonda tanımlanır. Kritik uzantı işaretleri, keyUsage, certificatePolicies, basicConstraints, CRL dağıtım noktaları, AIA/OCSP ve diğer uygulanabilir alanlar profil testlerinde doğrulanır.

7.1.3. Algoritma Nesne Tanımlayıcıları

Üretim sistemi ve HSM üzerinde etkin algoritmalar, anahtar parametreleri, özet algoritmaları ve ilgili OID değerleri kontrollü teknik profil/yapılandırmada tanımlanır. Sertifika oluşturulduğunda seçilen algoritma ve OID değerleri X.509 kodlamasına otomatik olarak yazılır. Mevzuat/teknik kriter değişikliğinde yeni profil test edilip değişiklik yönetimiyle devreye alınır.

7.1.4. İsim Biçimleri

DN alanları başvuru verilerinden belirlenmiş eşleştirme kurallarıyla oluşturulur. Karakter kodlama, alan sırası ve zorunlu alanlar X.500/RFC 5280 ve BTK profil kurallarına göre sistemsel şablonda uygulanır.

7.1.5. İsim Kısıtları

Takma ad/anonim ad girişi desteklenmez. Kimlik tanımlayıcı alanlar doğrulanan başvuru verisinden alınır; kullanıcı tarafından değiştirilemez. Üretim öncesi alan doğrulaması uygulanır.

7.1.6. Sertifika İlkeleri Nesne Tanımlayıcısı

Sertifika ilkeleri OID değeri ilgili sertifika profilinde sabit bir yapılandırma parametresi olarak tutulur. Profil değişikliği gerektiren önemli politika değişikliklerinde OID etkisi 9.12.3 kapsamında değerlendirilir ve yeni OID kullanımı onaylı değişiklikle devreye alınır.

7.1.7. İlke Kısıtları Uzantısının Kullanımı

Alt kök sertifika profilinde policyConstraints veya ilgili kısıtlama uzantısı kullanılacaksa, ihtiyaç teknik tasarım ve sertifika zinciri planında belirlenir; üretim öncesi test sertifikasında doğrulanır.

7.1.8. İlke Niteleyicilerinin Yazımı

CertificatePolicies uzantısında NESUE'ye erişim sağlayan CPS/uygulama esasları adresi teknik profil üzerinden tanımlanır. URL değişikliği gerektiğinde yayın adresinin sürekliliği ve eski sertifikaların doğrulanabilirliği dikkate alınır.

7.1.9. Kritik Sertifika İlkeleri Uzantısının İşlenme Semantiği

NESİ'de bu alt madde için özel uygulama tanımlanmadığından, kritik uzantıların işlenmesi RFC 5280 ve ilgili BTK profilinde belirtilen genel kurallara göre gerçekleştirilir.

7.2. SİL Profili

SİL üretim şablonu yayımlayıcı, thisUpdate, nextUpdate, CRL numarası, iptal edilen sertifika seri numaraları, iptal zamanı ve uygulanabilir diğer uzantıları içerecek şekilde yapılandırılır. SİL üretimi yetkili CA/SİL imzalama anahtarıyla otomatik gerçekleştirilir.

7.2.1. Sürüm Numarası

SİL üretim sistemi X.509 v2 CRL formatını kullanacak şekilde yapılandırılır; üretilen liste RFC 5280 ve BTK profil kontrollerinden geçirilir.

7.2.2. SİL ve SİL Giriş Uzantıları

SİL ve SİL giriş uzantıları teknik profile göre otomatik oluşturulur. Yeni bir uzantı kullanılmadan önce istemci uyumluluğu, BTK profili ve RFC 5280 şartları test edilir.

7.3. OCSP Profili

OCSP servisi sertifika durum veri kaynağına kontrollü erişir ve gelen uygun istekleri gerçek zamanlı değerlendirir. Yanıtlar OCSP hizmet sertifikası/anahtarıyla imzalanır; servis yalnız gerekli ağ portları üzerinden yayımlanır ve erişilebilirliği izlenir.

7.3.1. Sürüm Numarası

OCSP yanıt servisi RFC 6960 ile tanımlanan OCSP v1 protokolünü destekleyecek şekilde yapılandırılır. Uyum, servis testleri ve örnek istek/yanıt kontrolleriyle doğrulanır.

7.3.2. OCSP Uzantıları

Temel OCSP yanıt alanları zorunlu profile göre oluşturulur. İsteğe bağlı uzantılar yalnız ihtiyaç ve uyumluluk doğrulaması sonrasında etkinleştirilir; bilinmeyen/uygunsuz istekler servis güvenlik politikası ve protokol kuralları çerçevesinde reddedilir veya uygun hata yanıtı üretilir.

8. UYGUNLUK DENETİMİ VE DİĞER DEĞERLENDİRMELER

8.1. Denetim Sıklığı ve Durumları

BTK veya diğer yetkili makamların denetim talepleri resmî kayıtla karşılanır. İç denetimler ve BGYS denetimleri onaylı denetim planlarında belirlenen periyotlarda yürütülür; önemli değişiklik, güvenlik olayı veya önceki bulgunun takibi gerektiğinde plan dışı inceleme yapılabilir. Denetim öncesinde kapsam, sorumlu kişiler ve istenecek kanıtlar belirlenir.

8.2. Denetçinin Kimliği ve Özellikleri

Dış denetimlerde yetkili makam veya bağımsız denetim kuruluşunun görevlendirdiği denetçilerle çalışılır. İç denetçiler değerlendirdikleri faaliyetin doğrudan uygulayıcısı olmayacak şekilde mümkün olan görev ayrılığı gözetilerek atanır; gerekli yetkinlik ve gizlilik şartları sağlanır.

8.3. Denetçinin ESHS'yle İlişkisi

Bağımsızlık gerektiren dış denetimlerde çıkar çatışması yaratabilecek ilişkiler değerlendirilir. İç denetimlerde denetçinin kendi yaptığı işlemi denetlememesi ve bulguların süreç sahibinden bağımsız biçimde raporlanması esas alınır.

8.4. Denetimde Kapsanan Başlıklar

Denetim kapsamına mevzuat uyumu, NESİ/NESUE uygulaması, kimlik doğrulama, sertifika yaşam döngüsü, CA/HSM anahtar yönetimi, SİL/OCSP, loglama ve arşiv, fiziksel güvenlik, personel/tedarikçi kontrolleri, iş sürekliliği, ağ/sistem güvenliği ve doküman/değişiklik yönetimi dâhil edilir. Denetimde örnek kayıtlar sistem üzerinden gösterilir ve gerektiğinde rapor/kanıt kopyaları hazırlanır.

8.5. Eksiklik Durumunda Yapılacaklar

Bulgu tespit edildiğinde bulgunun kaynağı, etki alanı ve risk seviyesi değerlendirilir. Düzeltici faaliyet kaydı açılır; sorumlu, hedef tarih ve yapılacak işlem tanımlanır. Uygulama tamamlandığında kanıt eklenir ve etkinlik kontrolü yapılarak bulgu kapatılır. Resmî makam tarafından verilen süre ve talimatlar öncelikli olarak takip edilir.

8.6. Sonuçların Bildirilmesi

Denetim raporları yetkili yönetim ve ilgili süreç sahiplerine iletilir. Yönetim kararları, düzeltici faaliyetler ve kapanış kanıtları doküman/kayıt yönetimi kapsamında saklanır. Sertifika sahiplerini veya üçüncü kişileri etkileyen önemli bir bulgu/olay varsa gerekli bilgilendirme uygun iletişim kanallarıyla yapılır.

9. DİĞER İŞ KONULARI VE YASAL KONULAR

9.1. Ücretler

9.1.1. Sertifika Üretim ve Yenileme Ücretleri

Ürün, geçerlilik süresi ve hizmet kanalına göre ücretler yetkili ticari/mali birimlerce belirlenir ve satış/başvuru sistemindeki ürün tanımlarına işlenir. Güncel ücretler internet sitesi ve satış kanallarında yayımlanır. Fiyat değişiklikleri onaylı değişiklik kaydıyla sisteme aktarılır; eski başvuru/ödemelerin hangi fiyatla işleneceği ilgili satış kuralına göre belirlenir.

9.1.2. Sertifika Erişim Ücretleri

Kamuya açık sertifika/güven zinciri erişimi için ayrı bir erişim ücreti uygulanmaz. Erişim altyapısı web bilgi deposu ve sertifika durum servisleri üzerinden sağlanır.

9.1.3. İptal veya Durum Bilgisi Erişim Ücretleri

SİL ve OCSP servislerine erişim için kullanıcıdan ücret alınmaz. Servis uç noktaları kamuya açık olarak yayımlanır ve erişim sürekliliği teknik izleme kapsamındadır.

9.1.4. Diğer Hizmetlerin Ücretleri

NESİ, NESUE, sözleşme/taahhüt örnekleri ve kamuya açık bilgilendirme belgeleri ücretsiz yayımlanır. NES dışında katma değerli ürün/hizmet bulunması hâlinde bedel ve koşullar ilgili satış kanallarında ayrıca gösterilir.

9.1.5. Bedel İadesi

İade talebi alındığında öncelikle başvuru numarası üzerinden sertifikanın üretilip üretilmediği kontrol edilir. Üretimi tamamlanmamış ön ödemeli başvuruda talep uygun bulunursa ödeme kaydı mali birime aktarılır ve tahsil edilen tutar ilgili ödeme/iade prosedürüne göre kullanıcıya iade edilir.

Üretilmiş NES için genel olarak iade yapılmaz; mevzuattan doğan haklar saklıdır. EİMZATR kaynaklı nedenle sertifika içeriğinin başvuru bilgileriyle uyumsuz olduğu doğrulanırsa olay ve hata kaydı oluşturulur; sertifika sahibinin talebine göre ek ücret alınmadan yeni NES üretilir veya tahsil edilen tutarın iade süreci başlatılır.

9.2. Finansal Sorumluluk

9.2.1. Sigorta Kapsamı

Zorunlu sertifika mali sorumluluk sigortası poliçesinin geçerlilik süresi ve teminat bilgileri sorumlu birim tarafından takip edilir. Yenileme işlemleri poliçe süresi sona ermeden başlatılır; poliçe ve ilgili belgeler arşivlenir. Zarar bildirimi alınırsa olay/başvuru kaydı oluşturularak sigorta ve hukuk süreçlerine yönlendirilir.

9.2.2. Diğer Varlıklar

NESİ'de ayrıca bir uygulama tanımlanmadığından bu başlık altında ek operasyonel süreç bulunmamaktadır.

9.2.3. Son Kullanıcılar için Sigorta veya Garanti Kapsamı

NES hizmetlerinin yürütüldüğü dönemlerde zorunlu mali sorumluluk sigortasının geçerli olması sağlanır. Sertifika hizmetinden kaynaklandığı iddia edilen zarar talepleri kayıt altına alınır; olayın nedeni, sorumluluk ve sigorta kapsamı ilgili kayıt ve teknik kanıtlarla değerlendirilir.

9.3. İş Bilgisinin Gizliliği

9.3.1. Gizli Bilginin Kapsamı

CA özel anahtar bilgileri, HSM erişim bileşenleri, sistem güvenlik yapılandırmaları, zafiyet/denetim kayıtları, kişisel veriler, ticari bilgiler, tesis güvenliği ve iş sürekliliği ayrıntıları gizli bilgi olarak sınıflandırılır. Bu bilgiye erişim yalnız görev ihtiyacı bulunan yetkili personelle sınırlandırılır.

9.3.2. Gizlilik Kapsamı Dışındaki Bilgi

Kamuya açık NESİ/NESUE, kök/alt kök sertifikalar, SİL, OCSP erişim bilgileri, yayımlanması onaylanmış kılavuzlar ve sertifika sahibinin onayıyla kamuya açık dizine alınan bilgiler gizli bilgi sınıfında tutulmaz. Yayın öncesinde iç/gizli bilgi içermediği kontrol edilir.

9.3.3. Gizli Bilginin Korunması Sorumluluğu

Personel ve tedarikçiler gizlilik yükümlülüğü altındadır. Elektronik gizli bilgiler erişim yetkilendirmesi, şifreleme, loglama ve yedekleme kontrolleriyle; fiziksel belgeler kontrollü arşiv/alanlarla korunur. Yetkisiz açıklama veya erişim şüphesinde olay yönetimi ve gerekiyorsa KVKK/diğer bildirim süreçleri başlatılır.

9.4. Kişisel Bilgilerin Gizliliği/Özelliği

9.4.1. Gizlilik Planı

NES başvuru ve yaşam döngüsü süreçlerinde kişisel veriler yalnız hizmetin yürütülmesi ve yasal yükümlülüklerin yerine getirilmesi için gerekli kapsamda işlenir. Veri işleme envanteri, aydınlatma metinleri, saklama/imha kuralları ve erişim yetkileri KVKK yönetim sürecine göre güncel tutulur.

9.4.2. Özel Olarak Değerlendirilecek Bilgi

Sertifika içeriğinde/SİL'de kamuya açık olmayan başvuru belgeleri, iletişim bilgileri, kimlik doğrulama kayıtları, işlem belgeleri, video/görüntü kayıtları ve benzeri kişisel veriler özel/gizli bilgi olarak erişim kontrolüne tabi tutulur.

9.4.3. Özel Sayılmayacak Bilgi

Mevzuat ve sertifika sahibinin onayı doğrultusunda yayımlanan sertifika/dizin bilgileri ile kök/alt kök sertifikalar ve SİL/OCSP durum bilgileri kamuya açık veri olarak yönetilir. Yayın kapsamı, gerekli olandan fazla kişisel veri içermeyecek şekilde sınırlandırılır.

9.4.4. Özel Bilgiyi Koruma Sorumluluğu

Kişisel verilere erişim görev bazlıdır. Operasyon, teknik destek, arşiv ve yönetim rollerine yalnız iş gereği ihtiyaç duydukları veri alanları için yetki verilir. Yetki değişiklikleri kayıt altına alınır; erişim logları merkezi sistemlerde tutulur.

9.4.5. Özel Bilgiyi Kullanma Bildirimi ve Onayı

Başvuru sırasında aydınlatma ve gerekli onay metinleri kullanıcıya gösterilir; onay gerektiren işlemler ayrı ve ispatlanabilir kayıtla alınır. Pazarlama/tanıtım iletişimi için gereken izinler NES hizmetinin zorunlu onaylarından ayrıştırılır. Onay kaydı tarih-saat ve başvuru referansıyla saklanır.

9.4.6. Yargısal ve İdari Süreçlere Uygun Olarak Bilginin Açıklanması

Yetkili resmî makamdan gelen veri talebi, talepte bulunan makamın yetkisi, talebin kapsamı ve hukuki dayanağı kontrol edilerek ilgili birime yönlendirilir. Yalnız talep için gerekli bilgi paylaşılır; teslim edilen bilgi ve teslim tarihi kayıt altına alınır. Veri sahibinin KVKK başvuruları kimlik doğrulama sonrasında yasal sürelerde cevaplandırılır.

9.4.7. Bilginin Açıklandığı Diğer Durumlar

İlgili değildir.

9.5. Fikri Mülkiyet Hakları

EİMZATR'ye ait NESİ/NESUE, kılavuz, metin, marka ve diğer yayın içerikleri kurumsal yayın süreciyle yönetilir. Dış kaynak içerik/standart kullanımlarında lisans ve atıf koşulları gözetilir. Yetkisiz değişiklik veya EİMZATR adına sahte yayın tespitinde ilgili güvenlik/hukuk süreci başlatılır.

9.6. Sorumluluklar

9.6.1. ESHS Beyan ve Garantileri

EİMZATR, NES hizmetlerinin doğrulanmış başvuru bilgileri üzerinden, doğru sertifika sahibi adına ve yetkilendirilmiş güvenli sistemler aracılığıyla yürütülmesi için başvuru, kimlik doğrulama, üretim, teslimat, durum servisleri, loglama ve arşiv kontrollerini uygular.

Bu kontrollerin gerçekleştirildiğine ilişkin işlem ve sistem kayıtları, ilgili başvuru veya sertifika kaydıyla ilişkilendirilerek saklanır. Mevzuat kapsamında ESHS'ye yüklenen yükümlülüklerin uygulanması ilgili süreç sahipleri ve yetkilendirilmiş personel tarafından takip edilir.

9.6.2. Kayıt Merkezi Sorumlulukları

Kayıt birimi personeli, kendisine tanımlanan yetki kapsamında başvuru alma, kimlik ve belge kontrolü ile sertifika yönetim taleplerini EİMZATR tarafından belirlenen ekran, prosedür ve iş akışları üzerinden yürütür.

Eksik, doğrulanamayan veya tutarsız başvurular gerekçesi belirtilerek ilerletilmez. Kayıt biriminde gerçekleştirilen işlemler kullanıcı hesabı ve işlem zamanı ile ilişkilendirilerek kayıt altına alınır; erişim ve işlem yetkileri görev değişikliği veya yetkinin sona ermesi hâlinde güncellenir/kaldırılır.

9.6.3. Sertifika Sahibi Sorumlulukları

Sertifika sahibinin doğru ve güncel bilgi sağlama, sertifika içeriğini kontrol etme, güvenli elektronik imza oluşturma aracını ve PIN/parola gibi erişim verilerini koruma, NES'i kullanım koşullarına uygun kullanma ve güvenliğin tehlikeye girdiği durumları gecikmeksizin EİMZATR'ye bildirme yükümlülükleri sözleşme/taahhütname ve kullanıcı bilgilendirmelerinde açıklanır.

Kayıp, çalınma, yetkisiz kullanım şüphesi veya sertifika bilgilerinde hata/değişiklik bildirimi alınması hâlinde ilgili sertifika yönetim süreci başlatılır ve yapılan işlem kayıt altına alınır.

9.6.4. Üçüncü Kişilerin Sorumlulukları

Üçüncü kişilerin bir NES'e veya bu NES'e dayanılarak oluşturulan elektronik imzaya güvenmeden önce sertifikanın geçerlilik durumunu, güven zincirini, iptal/askı bilgisini, varsa kullanım sınırlamalarını ve elektronik imzanın doğrulama sonucunu kontrol edebilmesi için gerekli kök/alt kök sertifikaları, SİL ve OCSP erişim bilgileri yayımlanır.

Doğrulama hizmetlerinin kullanılmasına ilişkin teknik bilgiler, kamuya açık EİMZATR dokümanları ve bilgi deposu üzerinden erişilebilir tutulur.

9.6.5. Diğer Katılımcıların Sorumlulukları

EİMZATR'nin hizmet aldığı tedarikçi ve iş ortaklarının güvenlik, gizlilik, erişim, olay bildirimi, hizmet seviyesi ve mevzuata uyum yükümlülükleri ilgili sözleşme ve güvenlik şartlarında tanımlanır.

ESHS hizmetlerini etkileyen kritik tedarikçi faaliyetleri risk değerlendirmesine dâhil edilir; gerekli durumlarda erişimler sınırlandırılır, faaliyetler izlenir ve hizmet/uygunluk performansı gözden geçirilir.

9.7. Sorumlulukların Geçersiz Olduğu Durumlar

NESİ'de bu madde için özel bir istisna mekanizması tanımlanmamıştır. Sorumluluk değerlendirmeleri yürürlükteki mevzuat ve taraflar arasındaki sözleşmeler çerçevesinde yapılır.

9.8. Sorumluluk Sınırları

Zarar veya hizmet ihtilafı bildirimi alındığında olayın EİMZATR kontrol alanında olup olmadığı teknik kayıtlar, işlem geçmişi ve sözleşme/mevzuat hükümleri üzerinden değerlendirilir. EİMZATR'nin kanundan doğan sorumluluklarını ortadan kaldıracak bir uygulama yapılmaz; kullanıcı veya üçüncü kişinin kendi yükümlülüğüne aykırı davranışının etkisi olay bazında değerlendirilir.

9.9. Tazminatlar

Tazminat talebi kayıt altına alınır; başvuru/sertifika işlem kayıtları, teknik loglar, sözleşme ve olay kanıtları toplanır. Talebin hangi tarafın yükümlülüğünün ihlalinden kaynaklandığı hukuk/uyum ve ilgili süreç sahiplerince değerlendirilir. Sigorta kapsamına giren durumlarda sigorta bildirim süreci de işletilir.

9.10. NESUE Dokümanının Geçerliliği

9.10.1. NESUE Dokümanının Geçerlilik Dönemi

NESUE 3.0, yetkili yönetim organı tarafından onaylanarak bilgi deposunda yayımlandığı tarihte yürürlüğe girer. Yürürlükteki sürüm doküman yönetim sisteminde "geçerli" olarak işaretlenir; önceki sürümler arşiv statüsüne alınır.

9.10.2. NESUE Dokümanının Geçerliliğinin Sona Ermesi

Yeni sürüm onaylanıp yayımlandığında önceki NESUE sürümünün aktif uygulama statüsü sona erer. Önceki sürüme göre yürütülmüş işlemlerin kanıtları ve o tarihte geçerli olan doküman sürümü arşivde korunur.

9.10.3. Geçerliliğin Sona Ermesinin Etkileri ve İşlerliğin Sürdürülmesi

Yeni NESUE sürümünün yürürlüğe alınmasında etkilenen süreçler, sistemler ve uygulama adımları değişiklik yönetimi kapsamında belirlenir. Yeni sürümün mevcut sertifikalar üzerindeki etkisi değerlendirilir ve gerekli teknik/operasyonel geçiş faaliyetleri planlanır.

Önceki sürüm kapsamında oluşturulmuş sertifika ve kayıtların doğrulanabilirliği korunur. Sertifika sahibi veya üçüncü kişileri etkileyen önemli değişikliklerde gerekli duyuru ve bilgilendirmeler yapılır; geçiş hizmet sürekliliğini bozmayacak şekilde kontrollü olarak yürütülür.

9.11. Taraflara Özel Duyurular ve İletişim

Sertifika sahibine özel bildirimler, başvuruda doğrulanmış telefon/e-posta/Online İşlemler kanallarından uygun olanı kullanılarak yapılır. Genel servis, güvenlik, sertifika ilkesi veya güven zinciri duyuruları EİMZATR internet sitesinde; olayın önemine göre ek iletişim kanallarında yayımlanır. Kritik bildirimlerin gönderim/yayın kayıtları saklanır.

9.12. Değişiklikler

NESİ/NESUE, mevzuat, teknik standart, altyapı, organizasyon veya hizmet modelindeki değişiklikler doküman değişiklik süreciyle yönetilir. Değişiklik sınıfı, etki alanı, test/onay ihtiyacı, sertifika OID/profile etkisi ve duyuru ihtiyacı değerlendirilir.

9.12.1. Değişiklik Prosedürü

1. Değişiklik ihtiyacı kayıt altına alınır ve gerekçesi belirtilir.

2. Etkilenen NESİ/NESUE maddeleri, süreçler, sistemler ve kullanıcı grupları belirlenir.

3. Teknik/uyum/hukuk ve süreç sahibi değerlendirmeleri tamamlanır.

4. Gerekli test ve geçiş planı hazırlanır; yönetim onayı alınır.

5. Yeni sürüm yayımlanır, eski sürüm arşivlenir ve ilgili sistem/prosedür değişiklikleri kontrollü olarak devreye alınır.

6. Uygulama sonrası doğrulama yapılarak değişiklik kaydı kapatılır.

9.12.2. Duyuru Mekanizması ve Süresi

Değişikliğin sertifika sahibinin kullanımını, üçüncü kişilerin doğrulamasını veya güvenlik seviyesini etkilediği durumlarda duyuru hazırlanır. Güncel NESİ/NESUE bilgi deposunda yayımlanır; gerekli hâllerde kullanıcı iletişim bilgileri üzerinden ek bildirim yapılır. Eski sürümler sürüm bilgisiyle erişilebilir/arşivlenmiş olarak tutulur.

9.12.3. Nesne Tanımlayıcı Numaralarının Değişmesini Gerektiren Durumlar

Kimlik doğrulama güven seviyesi, sertifika kullanım amacı veya güvenlik politikasını esaslı şekilde değiştiren revizyonlarda sertifika ilkeleri OID etkisi teknik/uyum değerlendirmesine alınır. Yeni OID gerekiyorsa sertifika profilinde yeni değer tanımlanır, test edilir ve yalnız değişikliğin yürürlük tarihinden sonra üretilen ilgili sertifikalarda kullanılır.

9.13. Anlaşmazlıkların Çözümü

Şikâyet/itiraz EİMZATR iletişim kanallarından alınır ve kayıt numarası oluşturulur. İlgili başvuru, sertifika, teslimat, kimlik doğrulama, çağrı, log ve arşiv kayıtları toplanarak süreç sahibi ve gerektiğinde hukuk/uyum tarafından incelenir. Sonuç kullanıcıya uygun kanaldan bildirilir; çözülemeyen uyuşmazlıklarda yürürlükteki sözleşme ve mevzuat hükümleri uygulanır.

9.14. Yasal Düzenleme

EİMZATR, elektronik imza mevzuatını ve hizmete uygulanabilir diğer düzenlemeleri mevzuat takip süreciyle izler. Yeni veya değişen düzenleme tespit edildiğinde ilgili süreç sahibi, NESİ/NESUE ve sistem/prosedürlere etkisini değerlendirir; gerekli aksiyonlar değişiklik yönetimi kapsamında uygulanır.

9.15. İlgili Yasalara Uygunluk

Uyum gereklilikleri mevzuat envanteri, risk değerlendirmeleri, iç denetimler ve yönetim gözden geçirmeleri aracılığıyla takip edilir. Uygunsuzluk tespitinde düzeltici faaliyet açılır; mevzuatta bildirim gerektiren olaylar yetkili kurumlara tanımlı yöntem ve sürelerde bildirilir.

9.16. Çeşitli Hükümler

9.16.1. Bütün Anlaşma

İlgili değildir.

9.16.2. Görevlendirme

İlgili değildir.

9.16.3. Kitapçık Kısımlarının Ayrılabilirliği

Bir hükmün uygulanamaz hâle gelmesi diğer hükümleri kendiliğinden geçersiz kılmaz. Etkilenen madde için revizyon kaydı açılır; yeni sürüm yayımlanana kadar uygulanabilir diğer hükümler ve yürürlükteki mevzuat esas alınır.

9.16.4. Yasal Haklardan Vazgeçme

İlgili değildir.

9.16.5. Mücbir Sebepler

Mücbir sebep veya EİMZATR kontrolü dışındaki olağanüstü olaylarda iş sürekliliği/kriz yönetimi süreci işletilir. Öncelik can güvenliği, kritik sertifika durum servislerinin sürekliliği, veri/anahtar bütünlüğünün korunması ve etkilenen tarafların bilgilendirilmesidir. Olay ve alınan kararlar kayıt altına alınır.

9.17. Diğer Hükümler

İlgili değildir.