NİTELİKLİ ELEKTRONİK SERTİFİKA İLKELERİ

E-İMZA BİLGİ GÜVENLİĞİ HİZMETLERİ A.Ş.
PROF.DR.AHMET TANER KIŞLALI MAH.
2778.SOK. NO:3 ÇAYYOLU/ANKARA
TÜRKİYE

Tel : 90 312 242 0 111
Fax: 90 312 242 0 042

www.e-imzatr.com
bilgi@e-imzatr.com

1. GİRİŞ
1.1. Genel Bakış
1.2. Kitapçık Adı ve Tanımlama
1.3. Taraflar
1.3.1. Sertifika Üretim Merkezleri
1.3.2. Sertifika Kayıt Merkezleri
1.3.3. Kullanıcılar
1.3.4. Üçüncü Kişiler
1.3.5. Diğer Katılımcılar
1.4. Sertifika Kullanımı
1.4.1. Geçerli Sertifika Kullanım Şekilleri
1.4.2. Yasaklanmış Sertifika Kullanım Şekilleri
1.5. Sertifika İlkeleri Yönetimi
1.5.1. NESİ Dokümanından Sorumlu Organizasyon
1.5.2. İletişim Noktası
1.5.3. NESİ'nin İlkelere Uygunluğunu Belirleyen Yetkili
1.5.4. NESİ Onaylama Prosedürleri
1.6. Kısaltmalar ve Tanımlar
1.6.1. Kısaltmalar
1.6.2. Tanımlar
2. YAYIN VE BİLGİ DEPOSU SORUMLULUKLARI
2.1. Bilgi Deposu
2.2. Sertifika Bilgilerinin Yayımlanması
2.3. Yayımın Zamanı veya Sıklığı
2.4. Bilgi Deposuna Erişim Kontrolleri
3. KİMLİĞİN DOĞRULANMASI
3.1. İsimlendirme
3.1.1. İsim Tipleri
3.1.2. İsimlerin Anlamlı Olması Gerekliliği
3.1.3. Sertifika Sahiplerinin Anonimliği ve Takma Ad Kullanılabilirliği
3.1.4. İsim Biçimlerinin Değerlendirilmesi
3.1.5. İsimlerin Benzersizliği
3.1.6. Ticari Markaların Tanınması, Doğrulanması ve Rolü
3.2. İlk Kimlik Doğrulama
3.2.1. Gizli Anahtara Sahip Olunduğunun Kanıtlanma Yöntemi
3.2.2. Tüzel Kişiliğin Doğrulanması
3.2.3. Gerçek Kişinin Kimliğinin Doğrulanması
3.2.4. Doğrulama Yapılmaksızın Sertifikada Yer Alabilen Bilgiler
3.2.5. Yetkinin Doğrulanması
3.2.6. Karşılıklı Çalışma Kriterleri
3.3. Anahtar Yenileme Taleplerinin Doğrulanması
3.3.1. Rutin Anahtar Yenileme için Kimlik Doğrulama
3.3.2. İptal Sonrası Anahtar Yenileme için Kimlik Doğrulama
3.4. İptal Talebi için Kimlik Doğrulama
4. SERTİFİKA YAŞAM DÖNGÜSÜ İŞLEVSEL GEREKLİLİKLERİ
4.1. Sertifika Başvurusu
4.1.1. Kimler Sertifika Başvurusunda Bulunabilir?
4.1.2. Sertifika Başvuru, Kayıt Süreci ve Sorumluluklar
4.2. Sertifika Başvurusunun İşlenmesi
4.2.1. Kimlik Doğrulama İşlemlerinin Yerine Getirilmesi

4.2.2. Sertifika Başvurularının Kabulü veya Reddedilmesi
4.2.3. Sertifika Başvurularının İşlenme Süresi
4.3. "NES Üretimi
4.3.1. "NES Üretimi Sırasındaki ESHS Faaliyetleri
4.3.2. NES Üretimiyle İlgili Sertifika Sahibinin Bilgilendirilmesi
4.4. "NES"in Kabulü
4.4.1. Kabulün Şekli
4.4.2. ESHS Tarafından Sertifikanın Yayımlanması
4.4.3. Diğer Katılımcıların Sertifika Üretimiyle İlgili Bilgilendirilmesi
4.5. Anahtar Çifti ve "NES" Kullanımı
4.5.1. Sertifika Sahibi İmza Oluşturma Verisi ve "NES" Kullanımı
4.5.2. Üçüncü Kişilerin İmza Doğrulama Verisi ve "NES" Kullanımı
4.6. NES Yenileme
4.6.1. NES Yenilemeyi Gerektiren Durumlar
4.6.2. Yenileme Talebinde Bulunabilecek Kişiler
4.6.3. NES Yenileme Talebinin İşlenmesi
4.6.4. Yenilenmiş Sertifikayla İlgili Sertifika Sahibine Bildirim Yapılması
4.6.5. Yenilenen NES Kabulü
4.6.6. ESHS Tarafından Yenilenen Sertifikanın Yayımlanması
4.6.7. Diğer Katılımcıların Yeni Sertifika Üretimiyle İlgili Bilgilendirilmesi
4.7. Anahtar Yenileme
4.7.1. Anahtar Yenilemeyi Gerektiren Durumlar
4.7.2. Anahtar Yenileme Talebinde Bulunabilecek Kişiler
4.7.3. Anahtar Yenileme Talebinin İşlenmesi
4.7.4. Yeni Sertifikayla İlgili Sertifika Sahibine Bildirim Yapılması
4.7.5. Anahtarı Yenilenen Sertifikanın Kabulü
4.7.6. ESHS Tarafından Anahtarı Yenilenen Sertifikanın Yayınlanması
4.7.7. Diğer Katılımcıların Sertifika Üretimiyle İlgili Bilgilendirilmesi
4.8. Sertifika Değişikliği
4.8.1. Sertifika Değişikliğini Gerektiren Durumlar
4.8.2. Sertifika Değişiklik Talebinde Bulunabilecek Kişiler
4.8.3. Sertifika Değişiklik Talebinin İşlenmesi
4.8.4. Yeni Sertifikayla İlgili Sertifika Sahibine Bildirim Yapılması
4.8.5. Değişiklik Yapılmış Sertifikanın Kabul Şekli
4.8.6. ESHS Tarafından Değişiklik Yapılmış Sertifikanın Yayımlanması
4.8.7. Diğer Katılımcılarının Yeni Sertifika Üretimiyle İlgili Bilgilendirilmesi
4.9. Sertifika İptali ve Askıya Alma
4.9.1. Sertifika İptalini Gerektiren Durumlar
4.9.2. Sertifika İptal Talebinde Bulunabilecek Kişiler
4.9.3. Sertifika İptal Talebi Prosedürleri
4.9.4. Sertifika İptal Talebi Gecikme Periyodu
4.9.5. e-imzaTR'nin Sertifika İptal Talebini İşleme Süresi
4.9.6. Üçüncü Kişilerin İptal Kontrol Gerekliliği
4.9.7. Sertifika İptal Listesi (SİL) Yayımlama Sıklığı
4.9.8. SİL'lerin En Geç Yayımlanma Zamanı
4.9.9. Çevrim İçi Sertifika İptal/Durum Kontrol İmkânı (OCSP)
4.9.10. Çevrim İçi Sertifika İptal/Durum Kontrol Gereklilikleri
4.9.11. Diğer İptal Durumu Yayımlama Çeşitlerinin Varlığı
4.9.12. Anahtar Güvenliğinin Yitirilmesine İlişkin Özel Gereklilikler
4.9.13. Sertifika Askıya Alma Gerektiren Durumlar
4.9.14. Sertifika Askıya Alma Talebinde Bulunabilecek Kişiler
4.9.15. Sertifika Askıya Alma Talebi Prosedürü
4.9.16. Sertifikanın Askıda Kalma Süresinin Sınırları
4.10. Sertifika Durum Servisleri
4.10.1. İşlevsel Özellikler

4.10.2. Hizmetin Sürekliliği
4.10.3. İsteğe Bağlı Özellikler
4.11. Sertifika Sahipliğinin Sona Ermesi
4.12. İmza Oluşturma Verisi Saklama ve Yeniden Oluşturma
4.12.1. Anahtar Saklama ve Yeniden Oluşturma İlke ve Esasları
4.12.2. Oturum Anahtarı Zarflama ve Yeniden Oluşturma İlke ve Esasları
5. TESİS, YÖNETİM VE İŞLETMEYLE İLGİLİ KONTROLLER
5.1. Fiziksel Kontroller
5.1.1. Tesis Yeri ve İnşaatı
5.1.2. Fiziksel Erişim
5.1.3. Güç Kaynakları ve Havalandırma
5.1.4. Su Baskınları
5.1.5. Yangın Önleme ve Yangından Korunma
5.1.6. Sakalma Ortamları
5.1.7. Atıkların Atılması
5.1.8. Tesis Dışı Yedekleme
5.2. Prosedürel Kontroller
5.2.1. Güvenilir Roller
5.2.2. Her Görev İçin Gereken En Az Kişi Sayısı
5.2.3. Her Görev için Kimlik Doğrulama
5.2.4. Görevlerin Ayrılmasını Gerektiren Roller
5.3. Personel Kontrolleri
5.3.1. Nitelik, Deneyim ve Güvenlik Gereklilikleri
5.3.2. Kişisel Geçmiş Kontrol Gereklilikleri
5.3.3. Eğitim Gereklilikleri
5.3.4. Tekrar Eğitimi Sıklığı ve Gereklilikleri
5.3.5. İş Rotasyonu Sıklığı ve Sırası
5.3.6. Yetkisiz İşlemler için Yaptırımlar
5.3.7. Bağımsız Alt Yüklenici Gereklilikleri
5.3.8. Personele Sağlanan Dokümantasyon
5.4. Denetim Kayıtları Alma Prosedürleri
5.4.1. Kaydedilen Olay Tipleri
5.4.2. Kayıtları İşleme Sıklığı
5.4.3. Denetim Kayıtlarının Saklanma Süresi
5.4.4. Denetim Kayıtlarının Korunması
5.4.5. Denetim Kayıtlarının Yedeklenme Prosedürleri
5.4.6. Denetim Bilgisi Toplama Sistemi (İç ve Dış)
5.4.7. Olayı Yaratan Kişiyi Bilgilendirme
5.4.8. Zarar Görebilirlik Değerlendirmesi
5.5. Kayıtların Arşivlenmesi
5.5.1. Arşivlenen Kayıt Tipleri
5.5.2. Arşivlerin Saklanma Süresi
5.5.3. Arşivlerin Korunması
5.5.4. Arşivlerin Yedeklenme Prosedürleri
5.5.5. Kayıtların Zaman Damgası Altına Alınması Gereklilikleri
5.5.6. Arşiv Toplama Sistemi
5.5.7. Arşiv Bilgisinin Edinilmesi ve Doğrulanması Prosedürleri
5.6. Anahtar Değişimi
5.7. Güvenliğin Yitirilmesi ve Felaket Kurtarma
5.7.1. Güvenlik Kaybına Neden Olabilecek Olaylar
5.7.2. Bilgisayar Kaynakları, Yazılım ve/veya Verilerin Bozulmuş Olması
5.7.3. İmza Oluşturma Verilerinin Güvenliğinin Yitirilmesi
5.7.4. İş Sürekliliği Yetenekleri ve Felaket Kurtarma
5.7.5. e-imzaTR'nin Faaliyetinin Son Bulması
6. TEKNİK GÜVENLİK KONTROLLERİ

6.1. Anahtar Çifti Üretimi ve Kurulumu
6.1.1. Anahtar Çifti Üretimi
6.1.2. İmza Oluşturma Verisinin Sertifika Sahibine Ulaştırılması
6.1.3. İmza Doğrulama Verisinin ESHS'ye Ulaştırılması
6.1.4. e-imzaTR İmza Doğrulama Verilerinin Üçüncü Kişilere Ulaştırılması
6.1.5. Anahtar Uzunlukları
6.1.6. Anahtar Üretimi ve Kalite Kontrolü
6.1.7. Anahtar Kullanım Amaçları
6.2. İmza Oluşturma Verisinin Korunması ve Kriptografik Modül Mühendislik Kontrolleri
6.2.1. Kriptografik Modül Standartları ve Kontroller
6.2.2. İmza Oluşturma Verisinin Çok Kullanıcılı Kontrolü
6.2.3. İmza Oluşturma Verisinin Saklanması
6.2.4. İmza Oluşturma Verisinin Yedeklenmesi
6.2.5. İmza Oluşturma Verisinin Arşivlenmesi
6.2.6. İmza Oluşturma Verisinin Kriptografik Modül Transferi
6.2.7. İmza Oluşturma Verisinin Kriptografik Modülde Saklanması
6.2.8. Gizli Anahtarın Aktive Edilme Yöntemi
6.2.9. Gizli Anahtarın Deaktive Edilme Yöntemi
6.2.10. Gizli Anahtarı Yok Etme Metodu
6.2.11. Kriptografik Modül Değerlendirmesi
6.3. Anahtar Çifti Yönetimiyle İlgili Diğer Konular
6.3.1. İmza Doğrulama Verilerinin Arşivlenmesi
6.3.2. Sertifikanın İşlevsel Süreleri ve Anahtar Çifti Kullanım Süreleri
6.4. Erişim Şifreleri
6.4.1. Erişim Şifrelerinin Oluşturulması ve Kurulumu
6.4.2. Erişim Şifrelerinin Korunması
6.4.3. Erişim Şifreleriyle İlgili Diğer Konular
6.5. Bilgisayar Güvenlik Kontrolleri
6.5.1. Bilgisayar Güvenliği Teknik Gereklilikleri
6.5.2. Bilgisayar Güvenliğinin Derecelendirilmesi
6.6. Yaşam Döngüsü Teknik Kontrolleri
6.6.1. Sistem Geliştirme Kontrolleri
6.6.2. Güvenlik Yönetimi Kontrolleri
6.6.3. Yaşam Döngüsü Güvenlik Kontrolleri
6.7. Ağ Güvenlik Kontrolleri
6.8. Zaman Damgası
7. SERTİFİKA, SERTİFİKA İPTAL LİSTESİ (SİL) VE ÇSDP(OCSP) PROFİLLERİ
7.1. Sertifika Profili
7.1.1. Sürüm Numaraları
7.1.2. Sertifika Uzantıları
7.1.3. Algoritma Nesne Tanımlayıcıları
7.1.4. İsim Biçimleri
7.1.5. İsim Kısıtları
7.1.6. Sertifika İlkeleri Nesne Tanımlayıcısı
7.1.7. İlke Kısıtları Uzantısının Kullanımı
7.1.8. İlke Niteleyicilerinin Yazımı
7.1.9. Kritik Sertifika İlkeleri Uzamtısının İşlenme Semantiği
7.2. SİL Profili
7.2.1. Sürüm Numarası
7.2.2. SİL ve SİL Giriş Uzantıları
7.3. ÇSDP(OCSP) Profili
7.3.1. Sürüm Numarası
7.3.2. ÇSDP(OCSP) Uzantıları
8. UYGUNLUK DENETİMİ VE DİĞER DEĞERLENDİRMELER

8.1. Denetim Sıklığı ve Durumları
8.2. Denetçinin Kimliği ve Özellikleri
8.3. Denetçinin ESHS'yle İlişkisi
8.4. Denetimde Kapsanan Başlıklar
8.5. Eksiklik Durumunda Yapılacaklar
8.6. Sonuçların Bildirilmesi
9. DİĞER İŞ KONULARI VE YASAL KONULAR
9.1. Ücretler
9.1.1. Sertifika Üretim ve Yenileme Ücretleri
9.1.2. Sertifika Erişim Ücretleri
9.1.3. İptal veya Durum Bilgisi Erişim Ücretleri
9.1.4. Diğer Hizmetlerin Ücretleri
9.1.5. Bedel İadesi
9.2. Finansal Sorumluluk
9.2.1. Sigorta Kapsamı
9.2.2. Diğer Varlıklar
9.2.3. Son Kullanıcılar için Sigorta veya Garanti Kapsamı
9.3. İş Bilgisinin Gizliliği
9.3.1. Gizli Bilginin Kapsamı
9.3.2. Gizlilik Kapsamı Dışındaki Bilgi
9.3.3. Gizli Bilginin Korunması Sorumluluğu
9.4. Kişisel Bilgilerin Gizliliği/Özelliği
9.4.1. Gizlilik Planı
9.4.2. Özel Olarak Değerlendirilecek Bilgi
9.4.3. Özel Sayılmayacak Bilgi
9.4.4. Özel Bilgiyi Koruma Sorumluluğu
9.4.5. Özel Bilgiyi Kullanma Bildirimi ve Onayı
9.4.6. Yargısal ve İdari Süreçlere Uygun Olarak Bilginin Açıklanması
9.4.7. Bilginin Açıklandığı Diğer Durumlar
9.5. Fikri Mülkiyet Hakları
9.6. Sorumluluklar
9.6.1. ESHS Beyan ve Garantileri
9.6.2. Kayıt Merkezi Sorumlulukları
9.6.3. Sertifika Sahibi Sorumlulukları
9.6.4. Üçüncü Kişilerin Sorumlulukları
9.6.5. Diğer Katılımcıların Sorumlulukları
9.7. Sorumlulukların Geçersiz Olduğu Durumlar
9.8. Sorumluluk Sınırları
9.9. Tazminatlar
9.10. NESİ dokümanının Geçerliliği
9.10.1. NESİ dokümanının Geçerlilik Dönemi
9.10.2. NESİ dokümanının Geçerliliğinin Sona Ermesi
9.10.3. Geçerliliğin Sona Ermesinin Etkileri ve İşlerliğin Sürdürülmesi
9.11. Taraflara Özel Duyurular ve İletişim
9.12. Değişiklikler
9.12.1. Değişiklik Prosedürü
9.12.2. Duyuru Mekanizması ve Süresi
9.12.3. Nesne Tanımlayıcı Numaralarının Değişmesini Gerektiren Durumlar
9.13. Anlaşmazlıkların Çözümü
9.14. Yasal Düzenleme
9.15. İlgili Yasalara Uygunluk
9.16. Çeşitli Hükümler
9.16.1. Bütün Anlaşma

9.16.2. Görevlendirme
9.16.3. Kitapçık Kısımlarının Ayrılabilirliği
9.16.4. Yasal Haklardan Vazgeçme
9.16.5. Mücbir Sebepler
9.17. Diğer Hükümler

1. GİRİŞ

E-İMZA Bilgi Güvenliği Hizmetleri A.Ş (kısaca "e-imzaTR" olarak anılcaktır), 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-imzaTR"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-imzaTR" tarafından sunulduğunu belirlerken, "NESUE" bu hizmetlerin "e-imzaTR" tarafından nasıl gerçekleştirildiğini tanımlar.

Bu doküman "Tebliğ"de belirtilen ETSI TS 101 456, CWA 14167-1, IETF RFC 3647 standartlarına uygun olarak hazırlanmıştır.

1.1. Genel Bakış

5070 sayılı Elektronik İmza Kanunu'nun 5. maddesine göre güvenli elektronik imza, elle atılan imza ile aynı hukuki sonucu doğurur. "Kanun"un 4. maddesine göre güvenli elektronik imza; sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulabilir ve yalnızca nitelikli elektronik sertifika (Kısaca "NES")'ya dayanarak imza sahibinin kimliği tespit edilebilir. Güvenli elektronik imza oluşturma sürecindeki gerekli bileşenlerden biri olan "NES", yalnızca 5070 Sayılı Elektronik İmza Kanunu ve ilgili mevzuat hükümlerinde tanımlanmış olan "Elektronik Sertifika Hizmet Sağlayıcı"lar tarafından oluşturulabilir. Elektronik Sertifika Hizmet Sağlayıcı'lar "Kanun"un 8. Maddesi hükmü uyarınca Bilgi Teknolojileri ve İletişim Kurumu'na bildirimde bulunarak; ilgili mevzuat hükümleri uyarınca bildirimde bulunduğu koşulları yerine getirdiği Bilgi Teknolojileri ve İletişim Kurumu'nca uygun görülerek faaaliyete geçebilirler. Elektronik Sertifika Hizmet Sağlayıcı'lar elektronik sertifika, zaman damgası ve elektronik imzayla ilgili hizmetleri sunan gerçek veya tüzel kişilerdir.

E-İMZA BİLGİ GÜVENLİĞİ HİZMETLERİ A.Ş "Kanun" ve ilgili mevzuattaki gereklilikleri yerine getirerek Bilgi Teknolojileri ve İletişim Kurumu'na usulü dairesinde bildirimde bulunmuş ve bildirimde belirttiği koşulları sağladığı "Bilgi Teknolojileri ve İletişim Kurumu tarafından uygun görülerek faaliyete geçmesi hususunda yetki verilmiş bir "Elektronik Sertifika Hizmet Sağlayıcısı"dır..

Bu döküman "e-imzaTR" Nitelikli Elektronik Sertifika İlkeleri'ni açıklamaktadır.

1.2. Kitapçık Adı ve Tanımlama

1.3. Taraflar

1.3.1. Sertifika Üretim Merkezleri

Sertifika üretim merkezleri, ESHS'lerin sertifika üretim, dağıtım ve yayımlamasından sorumlu birimleridir.

1.3.2. Sertifika Kayıt Merkezleri

"e-imzaTR" tarafından belirlenen kayıt birimleri (Kısaca "KB" olarak anılacaktır) "e-imzaTR" adına son kullanıcı kimlik kontrolü, sertifika oluşturma istekleri, sertifika iptal etme 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 istekleri
- "e-imzaTR" ile arasında yapılan sözleşme, "NESİ" ve "NESUE"ye uygun hareket etme

1.3.3. Kullanıcılar

Kullanıcılar; adına sertifika oluşturulan gerçek yada tüzel kişilerdir. 5070 sayılı Elektronik İmza Kanunu'na göre "NES"ler sadece gerçek kişiler adına "ESHS"ler tarafından oluşturulabilirler.

1.3.4. Üçüncü Kişiler

Üçüncü kişiler, "e-imzaTR" tarafından oluşturulan "NES"ler kullanılarak imzalanmış verileri imzalayan kişinin kimliğini tespit eden; "NES"lerin, "e-imzaTR" kök ve alt kök sertifikalarının, "e-imzaTR" 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 kişilerdir. "NES" sahipleri yukarıda bahsedilen doğrulama süreçlerini kendileri yerine getirmeleri durumunda üçüncü kişi olarak hareket etmektedirler

1.3.5. Diğer Katılımcılar

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

1.4. Sertifika Kullanımı

1.4.1. Geçerli Sertifika Kullanım Şekilleri

Kullanıcı "NES"i kullanmaya başlayarak getirdiği tüm hukuki sorumlulukları kabul etmiş olur.

- "e-imzaTR" kök ve alt kök sertifikaları sadece "NES" imzalanması, "SİL" imzalanması, "ÇSDP" ve zaman damgası sertifikalarının imzalanması ile bahsi geçen sertifikaların ve verilerin doğrulanması süreçlerinde kullanılabilir

- “e-imzaTR” tarafından oluşturulan“ NES”ler sadece güvenli elektronik imza oluşturma ve doğrulama süreçleri içerisinde, “NES”in içinde yer alan kullanıma ve maddi kapsama ilişkin sınırlamalar dahilinde ve “NES Kullanıcı Sözleşmesi” hükümlerine uygun olarak kullanılabilirler.

1.4.2. Yasaklanmış Sertifika Kullanım Şekilleri

“e-imzaTR” 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” dokümanının yayınlanmasından, değiştirilmesinden, yenilenmesinden ve bu dokümana ilişkin diğer tüm işlemlerden “e-imzaTR” tarafından yetkilendirilmiş “NESİ” yönetim ekibi sorumludur.

1.5.1. NESİ Dokümanından Sorumlu Organizasyon

"NESİ" tüm hakları ve sorumluluğu "e-imzaTR"ye aittir. "NESİ" dökümanının güncelleme, kontrol ve yayınlama işlemlerinden e-imzatr yönetimi sorumludur. Kitapçığın yeni versiyonu yayınlandığında eski versiyonu geçersiz sayılır.

1.5.2. İletişim Noktası

E-İMZA BİLGİ GÜVENLİĞİ HİZMETLERİ A.Ş
Prof Dr. Ahmet Taner KIŞLALI Mah. 2778. Sok No: 3
Çayyolu / ANKARA

Tel : +90 312 242 0 111
Fax: +90 312 242 0 042
E-posta: bilgi@e-imzatr.com
Web: www.e-imzatr.com

1.5.3. NESİ’nin İlkelere Uygunluğunu Belirleyen Yetkili

"NESİ" dökümanının uygunlu ve uygulanabilirliği "e-imzaTR üstyönetimi tarafından belirlenir.

1.5.4. NESİ Onaylama Prosedürleri

"NESİ" dökümanının uygunlu ve uygulanabilirliği "e-imzaTR 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

“BTK”	Bilgi Teknolojileri ve İletişim Kurumu
"CEN"	Comité Européen de Normalisation - Avrupa Standardizasyon

	Komitesi
"CRL"	Certificate Revocation List (Bkn "SİL")
"CSR"	Certificate Signing Request – Sertifika İmzalama Talebi
"CWA"	CEN Workshop Agreement- CEN Çalıştay Kararı
"ÇSDP"	Çevrimiçi Sertifika Durum Protokolü (OCSP - Online Certificate Status Protokol)
"DN"	Distinguished Name – Ayırt Edici İsim
"DNS"	Domain Name System – Alan Adı Sistemi
"EAL"	Evaluation Assurance Level - Değerlendirme Garanti Düzeyi
"ESHS"	Elektronik Sertifika Hizmet Sağlayıcı
"ETSI TS"	ETSI Technical Specifications - ETSI Teknik Özellikleri
"ETSI"	European Telecommunication Standartization Institute - Avrupa Telekomünikasyon Standartları Enstitüsü
"e-imzaTR"	E-İMZA Bilgi Güvenliği Hizmetleri A.Ş
"FKM"	Felaket Kurtarma Merkezi
"IETF RFC"	Internet Engineering Task Force Request for Comments - İnternet Mühendisliği Görev Grubu Yorum Talebi
"IETF"	Internet Engineering Task Force - İnternet Mühendisliği Görev Grubu
"ISO/IEC"	International Organisation for Standardisation / International Electrotechnical Commitee - Uluslararası Standardizasyon Teşkilatı / Uluslararası Elektroteknik Komitesi.
"KB"	Kayıt Birimi
"NES"	Nitelikli Elektronik Sertifika
"OCSP"	Online Certificate Status Protokol (Bkn "ÇSDP")
"OID"	Object Identifier - Nesne betimleyicisi.
"PKI"	**"PKI"**Public-Key Infrastructure
"Sİ"	Sertifika İlkeleri
"SİL"	Sertifika İptal Listesi (CRL - Certificate Revocation List)
"SSL"	Secure Sockets Layer
"TC"	Türkiye Cumhuriyeti
"TCKN"	Türkiye Cumhuriyeti Kimlik Numarası
"TSE"	Türk Standartları Enstitüsü

1.6.2. Tanımlar

"Aktivasyon"	"NES"sahipleri için, İmza oluşturma verisi erişim şifresinin, kendisi tarafından belirlenmesine imkân

	sağlayan interaktif güvenli yöntem.
"Açık Anahtar Altyapısı" ("AAA")	Matematiksel bağlantısı bulunan kriptografik anahtar çiftlerine dayalı ve sertifika tabanlı bir kriptografik sistemin kurulması ve işletilmesini sağlayan mimari yapı, teknikler, uygulamalar ve düzenlemeler bütünü.
"Açık Anahtar"	"AAA" yapısında, Çift anahtarlı şifreleme algoritmasında üçüncü kişilere de açık olan kriptografik anahtar.("Kanun"da imza doğrulama verisi olarak isimlendirilmiştir.)
"Alt Kök Sertifikası"	"ESHS"nin "AAA"hiyerarşisi içerisinde "Güven Merkezi"tarafından oluşturulmuş, "ESHS"kök sertifikasının imzasını taşıyan ve son kullanıcı sertifikalarını imzalama amaçlı kullanılan sertifika.
"Anahtar"	İmza oluşturma veya imza doğrulama verilerinden herbiri.
"Arşiv"	"ESHS"nin saklamakla yükümlü olduğu her türlü bilgi, belge, evrak ve elektronik veri.
"Başvuru Yöntemleri"	"ESHS"ile Başvuru Sahibi"arasında başvurunun yapılması, sertifika sahibinin kimliğinin tespiti, gerekli evrakların hazırlanması, sertifika ücretlerinin ödenmesi, evrakların saklanması, sertifikaların yayınlanması ve sertifika sahibi'ne iletilmesi, sertifika iptal, yenileme ve askı taleplerinin iletimindeki usuller gibi hususların belirlendiği teknik ve idari süreçlerden oluşan yöntemler. Bu yöntemlere www.e-imzatr.comadresinden ulaşılabilir.
"Çevrim İçi Sertifika Durum Protokolü"("ÇSDP")	Sertifikaların geçerlilik durumunun üçüncü kişilere duyurulması için sertifika durum bilgisinin çevrim içi olarak kesintisiz alınmasını sağlayan standart protokol.
"Dizin"	Geçerli sertifikaları yayınlamak amacıyla içinde bulunduran elektronik depo.
"Elektronik İmza Kanunu"	23 Ocak 2004 tarih 25355 sayılı Resmi Gazete'de yayımlanan 5070 Sayılı Kanun.
"Elektronik İmza"	Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri.
"Elektronik Sertifika Hizmet Sağlayıcısı"	Elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişiler.
"Elektronik Veri"	Elektronik, optik veya benzeri yollarla elektronik ortamda üretilen, taşınan veya saklanan kayıtlar.
"Erişim Şifresi"	Güvenli elektronik imza oluşturma araçlarına erişim için kullanılan parola.
"Gizli Anahtar"	"AAA"yapısında, Çift anahtarlı şifreleme algoritmasında sadece anahtar sahibinin uktesinde olan kriptografik

	anahtar.(Kanun'da imza oluşturma verisi olarak isimlendirilmiştir.)
"Güven Merkezi"	"ESHS"yapısında yer alan, Kayıt Birim'lerinden gelen sertifika talepler doğrultusunda başvuru onay ve sertifika üretimi yapan, sertifika iptal işlemlerini gerçekleştirilen, sertifika kayıtları ile sertifika iptal durum kayıtlarını yaratan, işleten ve yayımlayan birim.
"Güvenli Elektronik İmza Doğrulama Aracı"	Kanunun 7 nci maddesinde sayılan niteliklere sahip: a) İmzanın doğrulanması için kullanılan verileri, değiştirmeksizin doğrulama yapan kişiye gösteren, b) İmza doğrulama işlemini güvenilir ve kesin bir biçimde çalıştıran ve doğrulama sonuçlarını değiştirmeksizin doğrulama yapan kişiye gösteren, c) Gerektiğinde, imzalanmış verinin güvenilir bir biçimde gösterilmesini sağlayan, d) İmzanın doğrulanması için kullanılan elektronik sertifikanın doğruluğunu ve geçerliliğini güvenilir bir biçimde tespit ederek sonuçlarını değiştirmeksizin doğrulama yapan kişiye gösteren, e) İmza sahibinin kimliğini değiştirmeksizin doğrulama yapan kişiye gösteren, f) İmzanın doğrulanması ile ilgili şartlara etki edecek değişikliklerin tespit edilebilmesini sağlayan ve CWA 14171 standardına uygun imza doğrulama araçları.
"Güvenli Elektronik İmza Oluşturma Aracı"	Kanunun 6 ncı maddesinde sayılan niteliklere sahip: a) Ürettiği elektronik imza oluşturma verilerinin kendi aralarında bir eşi daha bulunmamasını, b) Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin araç dışına hiçbir biçimde çıkarılamamasını ve gizliliğini, c) Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin, üçüncü kişilerce elde edilememesini, kullanılamamasını ve elektronik imzanın sahteciliğe karşı korunmasını, d) İmzalanacak verinin imza sahibi dışında değiştirilememesini ve bu verinin imza sahibi tarafından imzanın oluşturulmasından önce görülebilmesini sağlayan ve ISO/IEC 15408 (-1,-2,-3)'e göre en az EAL4+ seviyesinde olan araçlar.
"Güvenli Elektronik İmza"	Güvenli elektronik imza; a) Münhasıran imza sahibine bağlı olan, b) Sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan, c) Nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan, d) İmzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan, e) Kanunun 4 üncü maddesinde sayılan niteliklere sahip, Kanunun hariç tuttuğu işlemler dışında elle atılan

	imzayla aynı hukuki sonucu doğuran elektronik imzadır.
"İmza Doğrulama Aracı"	Elektronik imzayı doğrulamak amacıyla imza doğrulama verisini kullanan yazılım veya donanım aracı.
"İmza Doğrulama Verisi"	Elektronik imzayı doğrulamak için kullanılan şifreler, kriptografik açık anahtarlar gibi veriler.
"İmza Oluşturma Aracı"	Elektronik imza oluşturmak üzere, imza oluşturma verisini kullanan yazılım veya donanım aracı.
"İmza Oluşturma Verisi"	İmza sahibine ait, imza sahibi tarafından elektronik imza oluşturma amacıyla kullanılan ve eşi daha olmayan şifreler, kriptografik gizli anahtarlar gibi veriler.
"İmza Sahibi"	Elektronik imza oluşturmak amacıyla bir imza oluşturma aracını kullanan "NES"sahibi gerçek kişi.
"İptal Durum Kaydı"	Geçerlilik süresi dolmamış sertifikaların iptal bilgisinin yer aldığı, iptal zamanının tam olarak tespit edilmesine imkan veren ve üçüncü kişilerin hızlı ve güvenli bir biçimde ulaşabileceği kayıt.
"Kanun"	15 Ocak 2004 tarihli ve 5070 sayılı Elektronik İmza Kanunu.
"Kayıt Birimi"	"e-imzaTR"ye bağlı olarak faaliyette bulunan, Sertifika Sahipleri ile "Kurumsal Başvuru Sahipleri"nin sertifika başvurularını alan, ilgili kimlik tanımlama ve doğrulama süreçlerini yürüten, sertifika taleplerini onaylayarak "Güven Merkezi"ne yönelten, "ESHS" faaliyetleri kapsamında müşteri ilişkilerini yöneten alt birimlere sahip "e-imzaTR"nin yetkili birimleri ve onların personelleri.
"Kimlik Bilgileri"	"Sertifika Kullanıcısı"nın Adı-Soyadı, Türkiye Cumhuriyeti Kimlik Numarası veya Pasaport Numarası, doğum yeri, doğum tarihi ve uyruğu.
"Kök Sertifika"	"ESHS"kurumsal kimlik bilgilerini "ESHS"imza doğrulama verisine bağlayan, "Güven Merkezi" tarafından üretilen ve kendi imzasını taşıyan, "ESHS"nin ürettiği diğer tüm sertifikaların doğrulanabilmesi için "ESHS"tarafından yayımlanan sertifika.
"Kurum"	Bilgi Teknolojileri ve İletişim Kurumu.
"Kurumsal Başvuru Sahibi"	"ESHS"ile Kurumsal Başvuru Sözleşmesi akdetmiş olan ve bu sözleşme hükümleri ve "Yönetmeliğin"3. ve 9. maddeleri uyarınca çalışanları veya müşterileri veya üyeleri veya hissedarları adına nitelikli elektronik sertifika başvurusunda bulunan tüzel kişilik .
"Kurumsal Başvuru Yetkilisi"	"Sertifika Kullanıcısı"adına "NES"düzenlenmesi için "ESHS"ye bildirilecek olan bilgileri "Yönetmeliğin"Mad. 9/1.de belirtilen belgelere dayanarak tespit eden ve "Kurumsal Başvuru Sözleşmesi"içerisinde kendisiyle ilgili belirtilen işlemleri "Kurumsal Başvuru Sahibi"adı ve hesabına yerine getiren "Kurumsal Başvuru Sahibi"nin çalışanı.

"Kurumsal Başvuru"	Bir tüzel kişiliğin çalışanları veya müşterileri veya üyeleri veya hissedarları adına yaptığı nitelikli elektronik sertifika başvurusu.
"Mali Sorumluluk Sigortası"	"ESHS"nin, "Kanun"dan veya uygulamalardan doğan yükümlülüklerini yerine getirmemesi sonucu doğacak zararların karşılanması amacıyla yaptırmakla yükümlü olduğu sigorta.
"Nitelikli Elektronik Sertifika("NES")	5070 Sayılı Kanunun 9. Maddesinde içerik olarak; "Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ"in 5. Maddesinde ise teknik bakımdan özellikleri belirtilen elektronik sertifika.
"Özetleme Algoritması"	İmzalanacak elektronik verilerin sabit uzunlukta bir özetinin çıkarılmasında kullanılan algoritma.
"Özne"	Sertifikanın CN alanında yer alan kişi veya sunucu adı.
"Sertifika İlkeleri"	Sertifikaların belli bir topluluk ve/veya genel güvenlik gereklilikleri olan uygulamalar bakımından kabul edilebilirliğini belirten kurallar bütününe ve ESHS'nin işleyişi ile ilgili genel kuralları içeren belgeye "Sertifika İlkeleri"denir. "Sertifika İlkeleri", Elektronik Sertifika Hizmet Sağlayıcıları tarafından umuma açıklanan yönelik bir belgedir. "ESHS"tarafından yayınlanan "Sİ"ye, "Sertifika Kullanıcı"ları uymak zorundadır. "Sİ"ye, duruma göre zaman zaman yapılabilecek değişiklikler de dahil olmak üzere, güncel ve önceki sürümlerine "ESHS"nin web sitesinden erişilebilir.
"Sertifika İmzalama Talebi" ("CSR")	Talep sahibi tarafından üretilen ve sahip olduğu gizli anahtarla imzaladığı sertifika talebi.
"Sertifika İptal Listesi"	İptal edilmiş sertifikaların üçüçü kişilere duyurulması amacıyla "ESHS"tarafından yayımlanan elektronik dosya.
"Sertifika Kullanıcısı"- "Sertifika Sahibi"	Adına "ESHS"tarafından sertifika düzenlenen gerçek veya tüzel kişilik. Bu doküman içerisinde geçen "Sertifika Sahibi"kavram "Sertifika Kullanıcısı"ile eş anlamlı olarak kullanılmaktadır.
"Sertifika Uygulama Esasları"	"Sertifika Sahipleri"başta olmak üzere "Sİ"içerisinde tanımlanan herbir tarafın "Sİ"içinde tanımlı operasyonları gerçekleştirmek için uymak zorunda olduğu gerekliliklerin tespit edildiği, uygulamaların ve prosedürlerin açıklandığı, belli süreçler içerisinde güncellenen ve "ESHS"tarafından umuma yapılan bir açıklamadır. "SUE"ye, duruma göre zaman zaman yapılabilecek değişiklikler de dahil olmak üzere, "ESHS"nin web sitesinden erişilebilir.
"Tebliğ"	6 Ocak 2005 tarih 25692 sayılı Resmi Gazete'de Bilgi Teknolojileri ve İletişim Kurumu tarafından yayımlanan "Elektronik

	İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ"
"Yönetmelik"	6 Ocak 2005 tarih 25692 sayılı Resmi Gazete'de Bilgi Teknolojileri ve İletişim Kurumu tarafından yayımlanan "Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik".

2. YAYIN VE BİLGİ DEPOSU SORUMLULUKLARI

2.1. Bilgi Deposu

"e-imzaTR" Veri depoları "SİL", "ÇSDP" ve ilgili tüm dökümanlar 7/24 ulaşılabilecek şekilde erişime açık bulundurulur

2.2. Sertifika Bilgilerinin Yayımlanması

"e-imzaTR" veri deposundan aşağıdaki bilgiler yayınlanır.

- "NES" başvuru dökümanları
- Kurumsal başvuru sözleşmeleri
- "NES" kullanıcı sözleşmeleri
- "NES" ile ilgili yayınlar ve bilgilendirme dökümanları
- "NESİ" ve "NESUE"
- "e-imzaTR" "SİL"
- "e-imzaTR" Kök Sertifikası
- "e-imzaTR" Alt Kök Sertifikası
- "e-imzaTR" Zaman Damgası Sertifikası
- "e-imzaTR" "ÇSDP" Sertifikası

2.3. Yayımın Zamanı veya Sıklığı

"ESHS" sertifika bilgileri değişiklik yapıldığı an yayınlanır. "SİL" bilgileri değişiklikten sonra yayınlanır. "ÇSDP" iptal işlemi sonrasında bilgileri hemen erişerek hizmetini sürdürür.

Üretilen tüm "NES" ve "SİL" ler manuel müdaheleye gerek olmaksınız 24 saatte bir otomatik olarak yayınlanır. "SİL"de değişiklik olması durumunda 2 dakika içerisinde yeni sil yayınlanır.

2.4. Bilgi Deposuna Erişim Kontrolleri

Veri depolarına yapılacak tüm erişimler sözleşmede belirtildiği üzere gerçekleştirilir.

Halka açık olarak sunulan tüm bilgiler gizlilik önemi taşımaz ancak sertifikalara ulaşmak için gereken erişim kontrolleri bir katma değer hizmeti taşıyabileceğinden bazı durumlarda erişim maliyeti söz konusu olabilir.

"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

3.1. İsimlendirme

Bu bölümde sertifika içerisindeki isimlendirmelerle ilgili bilgiler açıklanır.

3.1.1. İsim Tipleri

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

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

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

3.1.5. İsimlerin Benzersizliği

"e-imzaTR" "NES"lerde bulunan bilgilerin benzersiz olmasını sağlamakla yükümlüdür. Şirketler için vergi numarası, T.C vatandaşları için kimlik numarası, kullanılarak "NES" lerin benzersizliği sağlanır.

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

"e-imzaTR" "ESHS" işleyişi içerisinde imza oluşturma ve doğrulama verileri sadece "ESHS" tarafından oluşturulmaktadır. Bu sebeple "NES"in ve güvenli "NES" oluşturma aracının "NES" sahibine imza karşılığı teslim edilmesi halinde, "NES" sahibinin imza oluşturma verisine sahip olduğu kabul edilir.

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

NES başvurusunda bulunan kişilerin sertifikada yer alacak bilgileri, yasal düzenlemelerle belirlendiği şekilde ve resmi belgelere dayandırılarak doğrulanır. NES başvuruları alınırken, mevzuat gereği kişinin birinci başvurusu sırasında yüz yüze kimlik doğrulaması yapılır.

3.2.4. Doğrulama Yapılmaksızın Sertifikada Yer Alabilen Bilgiler

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

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

3.2.5. Yetkinin Doğrulanması

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

3.2.6. Karşılıklı Çalışma Kriterleri

e-imzaTR başka bir ESHS ile karşılıklı çalışma amacıyla çapraz veya tek yönlü sertifikasyon yapmaz.

3.3. Anahtar Yenileme Taleplerinin Doğrulanması

3.3.1. Rutin Anahtar Yenileme için Kimlik Doğrulama

Anahtar çiftinin güvenli kullanım süresinin sonunda, yeni anahtar çifti üretimi, kullanıcının yeni bir NES başvurusunda bulunmasıyla gerçekleştirilir. Yeni sertifika başvurusu, sertifikanın kullanım süresi içinde, elektronik ortamda ve mevcut sertifikaya bağlı imza oluşturma verisiyle imzalanarak yapılabilir. Bu durumda eğer anahtar çifti sertifika sahibi tarafından üretiliyorsa sertifika talebiyle birlikte imza doğrulama verisi de ESHS'ye gönderilir. Yeni sertifika içinde yer alacak bir bilgide değişiklik gerekmesi durumunda, bu değişikliğin resmi belgeye dayandırılması zorunludur. Sertifikada yer almayan diğer kullanıcı bilgilerindeki değişiklikler de NES sahibinin yazılı veya elektronik beyanıyla kabul edilir. Anahtar yenilemesinde, NES sahibinin yeniden yüz yüze kimlik tespiti yapması aranmaz. Ancak, telefon veya faks ile yapılan kimlik doğrulamasında bir tereddüt olması halinde yüz yüze kimlik tespiti istenir.

3.3.2. İptal Sonrası Anahtar Yenileme için Kimlik Doğrulama

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

- Sertifika içeriğinde yer alan bilgilerdeki eksik, kusur veya hataya bağlı iptaller.

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

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

3.4. İptal Talebi için Kimlik Doğrulama

e-imzaTR NES iptal taleplerini aşağıda açıklandığı gibi güvenilir yollarla alır ve kimlik doğrulaması yapar:

- Sertifika sahibi başvuru sırasında belirttiği kendisine özel bilgileri kullanarak e-imzaTR bireysel kullanıcı servislerinde iptal işlemini gerçekleştirebilir
- Sertifika sahibi e-imzaTR ofislerine gelerek dilekçe ile başvurabilir
- Çağrı merkezi üzerinden kimlik doğrulaması gerçekleştirerek

4. SERTİFİKA YAŞAM DÖNGÜSÜ İŞLEVSEL GEREKLİLİKLERİ

4.1. Sertifika Başvurusu

4.1.1. Kimler Sertifika 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” sahibi olmak isteyenler şahsen “KB” ye giderek başvuru yapabilirler. Başvuru sırasında “KB” yetkilisine geçerli bir kimlik belgesi beyan ederek kimlik doğrulama işlemini gerçekleştirir. Gerekli sözleşmeler ve belgeler doldurulup başvuru sahibi tarafından imzalandıktan sonra “KB” yetkilisine teslim eder. Belgeler “KB” yetkilisi tarafından onaylandıktan sonra üretim safhasına geçilir.
- "NES" Sahibi olmak isteyenler www.e-imzatr.com üzerinden başvuru formunu doldurarak ödeme işlemini gerçekleştirir. e-imzaTR taahhüt namesini noter aracılığıyla kimlik doğrulamasını gerçekleştirir ve "e-imzaTR" ye posta yoluyla gönderir

4.2. Sertifika Başvurusunun İşlenmesi

4.2.1. Kimlik Doğrulama İşlemlerinin Yerine Getirilmesi

“KB” Yetkilileri “NESİ” 3.2 de belirtildiği şekilde doğrulanır.

4.2.2. Sertifika Başvurularının Kabulü veya Reddedilmesi

“KB” yetilileri yapılan başvuruların kontrolünden ve “e-imzaTR” tarafından yayınlanan “NES” ve “NESİ”ye uygunluğunun kontrolünden, uygunsuzluk durumlarında reddedilmesinden sorumludur.

4.2.3. Sertifika Başvurularının İşlenme Süresi

Başvuru süreci tamamlandıktan sonra “e-imzaTR” 10 iş günü içerisinden üretimi gerçekleştirip ilgili yollarla kullanıcıya postalamakla sorumludur.

4.3. "NES" Üretimi

4.3.1. "NES" Üretimi Sırasındaki ESHS Faaliyetleri

Başvurular “KB” tarafından onaylandıktan sonra “ESHS” tarafından “TEBLİĞ” de belirtilen "NES" oluşturma araçları kullanılarak ilgili algoritma ve standartlar içerisinde imza oluşturma ve doğrulama verilerini oluşturarak başvuru sahibine imza karşılığında teslim eder.

4.3.2. "NES" Üretimiyle İlgili Sertifika Sahibinin Bilgilendirilmesi

“ESHS” “NES” üretiminin hangi durumda olduğu kullanıcıya bildirmekle yükümlüdür.

4.4. "NES"in Kabulü

4.4.1. Kabulün Şekli

“NES” “ESHS” tarafından imzalandıktan ve Veri Depolarında yayınlandıktan sonra “ESHS” tarafından kabulü yapılmış olur. Üretimi yapılan “NES” imza karşılığında kullanıcıya teslim edildiğinde kullanıcı tarafından kabul edilmiş sayılır. Kullanıcı “NES” teslim aldıktan sonra paketini açarak eksiklik olup olmadığını kontrol etmekle yükümlüdür. Eksik teslimat durumunda “KB”ye ivedilikle başvurmalıdır. Eksiksiz teslim alınan “NES” kullaınıcı tarafından kurulum yönergeleri uygulanarak kurulduktan sonra sertifika içerisindeki bilgiler başvuru sırasında vermiş olduğu bilgilerden farklı olduğunu tespit etmesi durumunda “e-imzaTR” çağrı merkezini arayarak iptal ettirmesi gerekmektedir. “e-imzaTR” iptal işlemini gerçekleştirdikten sonra yeni oluşturacağı“NES”i “NESİ”de belirtilen kurallar çevresinde kullanıcı ya teslim eder.

4.4.2. ESHS Tarafından Sertifikanın Yayımlanması

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

4.4.3. Diğer Katılımcıların Sertifika Üretimiyle İlgili Bilgilendirilmesi

Diğer ilgililere yapılacak bildirimler “e-imzaTR” web sayfasından duyurulur.

4.5. Anahtar Çifti ve "NES" Kullanımı

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

“NES” sahipleri imza oluşturma verilerini ve “NES”lerini, “NESUE”, “NESİ, “Kanun”, “Yönetmelik”, “Tebliğ” ve imzalamış oldukları kullanıcı sözleşmeleri ile belirlenen yükümlükleri doğrultusunda kullanmak zorundadırlar.”NES” sahibi imza oluşturma versinin güvenliğini ve gizliliğini sağlamakla yükümlüdür. İmza oluşturma versinin gizliliği ve doğruluğundan şüphe ettiği durumlarda ivedilikle “e-imzaTR” ye belirtmelidir.

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

“NES”e güvenerek iş ve işlem yapacak olan üçüncü kişiler öncelikle “NES”in kontrolünü yapmalıdırlar.Üçüncü kişiler “NES”i kullanan üçüncü şahıslar “NES” kullanılarak yapılan işlemin “Kanun”da yasaklanan hukuki işlemlerden biri olmadığını ve yapılan işlemin “NES”in içerisinde yer alan maddi kapsama veya kullanıma ilişkin sınırlamalara aykırı olmadığını tespit etmekle yükümlüdür. Üçüncü kişiler “NES” kontrolünün ve doğrulama prosedürlerinin başarısız olması durumunda “NES”e dayanarak işlem yapmamalıdır.

4.6. "NES" Yenileme

“NES” yenileme sertifika bilgileri korunarak farklı bir anahtar çifti ile tekrar oluşturulmasıdır. "e-imzaTR" yeni anahtar çifti oluşturma yöntemini kullanmaz. Başvuru yeni yapılmış kabul edilerek yeni "NES" oluşturma süreci baştan başlatılır.

4.6.1. "NES" Yenilemeyi Gerektiren Durumlar

Sertifika süresinin dolmasına belirli bir süre kalmış olması ya da sertifika son kullanım tarihinin geçmiş olması. Kayıp, çalınma, v.b. sebepler

4.6.2. Yenileme Talebinde Bulunabilecek Kişiler

Sertifika sahibi ya da sertifika sahibini temsile yetkili kişiler tarafından yenileme talebinde bulunulabilir.

4.6.3. "NES" Yenileme Talebinin İşlenmesi

Sertifika sahibi "NES"in kullanım süresi sona ermeden önce elektronik imzalı olarak yenileme talebinde bulunmuş ise kimlik kontrolü yapılmış sayılarak yenileme talebi işleme alınır. "NES"in süresi dolmuş ise Madde 4.1.2 de belirtilen adımlar uygulanır.

4.6.4. Yenilenmiş Sertifikayla İlgili Sertifika Sahibine Bildirim Yapılması

“ESHS” “NES” üretiminin hangi durumda olduğu kullanıcıya bildirmekle yükümlüdür.

4.6.5. Yenilenen "NES"in Kabulü

“NES” “ESHS” tarafından imzalandıktan ve Veri Depolarında yayınlandıktan sonra “ESHS” tarafından kabulü yapılmış olur. Üretimi yapılan “NES” imza karşılığında kullanıcıya teslim edildiğinde kullanıcı tarafından kabul edilmiş sayılır. Kullanıcı “NES” teslim aldıktan sonra paketini açarak eksiklik olup olmadığını kontrol etmekle yükümlüdür. Eksik teslimat durumunda “KB”ye ivedilikle başvurmalıdır. Eksiksiz teslim alınan “NES” kullanıcı tarafından kurulum yönergeleri uygulanarak kurulduktan sonra sertifika içerisindeki bilgiler yenileme başvurusu sırasında vermiş olduğu bilgilerden farklı olduğunu tespit etmesi durumunda “e-imzaTR” çağrı merkezini arayarak iptal ettirmesi gerekmektedir. “e-imzaTR” iptal işlemini gerçekleştirdikten sonra yeni oluşturacağı“NES”i “NESİ”de belirtilen kurallar çevresinde kullanıcı ya teslim eder.

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

Diğer ilgililere yapılacak bildirimler "e-imzaTR" web sayfasından duyurulur.

4.7. Anahtar Yenileme

4.7.1. Anahtar Yenilemeyi Gerektiren Durumlar

İlgili değildir.

4.7.2. Anahtar Yenileme Talebinde Bulunabilecek Kişiler

İlgili değildir.

4.7.3. Anahtar Yenileme Talebinin İşlenmesi

İlgili değildir.

4.7.4. Yeni Sertifikayla İlgili Sertifika Sahibine Bildirim Yapılması

İlgili değildir.

4.7.5. Anahtarı Yenilenen Sertifikanın Kabulü

İlgili değildir.

4.7.6. ESHS Tarafından Anahtarı Yenilenen Sertifikanın Yayınlanması

İlgili değildir.

4.7.7. Diğer Katılımcıların Sertifika Üretimiyle İlgili Bilgilendirilmesi

İlgili değildir.

4.8. Sertifika Değişikliği

4.8.1. Sertifika Değişikliğini Gerektiren Durumlar

e-imzaTR tarafından üretilmiş olan sertifikaların içeriğindeki bilgilerde bir değişiklik olması durumunda, sertifika iptal edilir ve yeni bilgilerle birlikte yeni bir sertifika başvurusunda bulunulur. Yeni sertifika başvurusu Bölüm 4.1'de belirtilen ilkeler uyarınca yürütülür.

4.8.2. Sertifika Değişiklik Talebinde Bulunabilecek Kişiler

Bölüm 4.1.1'de yer alan ilkeler uyarınca yürütülür.

4.8.3. Sertifika Değişiklik Talebinin İşlenmesi

Bölüm 3.2'de yer alan ilkeler uyarınca yürütülür.

4.8.4. Yeni Sertifikayla İlgili Sertifika Sahibine Bildirim Yapılması

Bölüm 4.3.2'de yer alan ilkeler uyarınca yürütülür.

4.8.5. Değişiklik Yapılmış Sertifikanın Kabul Şekli

Bölüm 4.4.1'de yer alan ilkeler uyarınca yürütülür.

4.8.6. ESHS Tarafından Değişiklik Yapılmış Sertifikanın Yayımlanması

Bölüm 4.4.2'de yer alan ilkeler uyarınca yürütülür.

4.8.7. Diğer Katılımcılarının Yeni Sertifika Üretimiyle İlgili Bilgilendirilmesi

Uygulama dışıdır.

4.9. Sertifika İptali ve Askıya Alma

4.9.1. Sertifika İptalini Gerektiren Durumlar

"NES" ler aşağıda belirtilen durumlarda iptal edilir;

- "NES" sahibinin yazılı talebi
- "NES" sahibinin çağrı merkezi üzerinden iptal talebinde bulunması
- "NES" sahibinin elektronik imzalı olarak göndereceği e-posta yoluyla iptal isteminde bulunması
- "Sertifika Kullanıcısı"nın "ESHS" veya "Kurumsal Başvuru Sahibi" aleyhine "NES"i kullanarak suç teşkil eden bir fiili icra etmesi
- "NES" içerisinde yer alan bilgilerin sertifikanın geçerli olduğu süre içerisinde herhangi bir zamanda gerçeğe aykırı olduğunun "ESHS" veya "Kurumsal Başvuru Sahibi" tarafından anlaşılması
- "NES"lerin "Sertifika Kullanıcısı" tarafından hukuka veya "NES" içerisinde yer alan kullanım veya maddi kapsama aykırı amaçlarla kullanıldığının "ESHS" veya "Kurumsal Başvuru Sahibi" tarafından tespiti
- "Sertifika Kullanıcısı"nın imza oluşturma verisinin üçüncü kişilerin eline geçtiğinin, ifşa edildiğinin veya tehlike altında olduğunun "ESHS", "NES" sahibi veya "Kurumsal Başvuru Sahibi" tarafından tespiti
- "Sertifika Kullanıcısı"nın "NES" kullanarak icra ettiği kasti bir fiili neticesinde "ESHS"nin veya "Kurumsal Başvuru Sahibi"nin zarara uğraması
- "Sertifika Kullanıcısı Sözleşmesi"nin "Sertifika Kullanıcısı" tarafından tek taraflı olarak fesh edildiğinin "ESHS"ye yazılı olarak bildirilmesi veya "Sertifika Kullanıcısı Sözleşmesi"nin herhalde taraflardan biri tarafından tek taraflı olarak feshedilmesi
- Gerekli olan durumlarda "Kurumsal Başvuru Sahibi" ile "Sertifika Kullanıcısı" arasında "Kurumsal Başvuru"da bulunmaya esas teşkil eden hukuki ilişkinin sona ermesi
- "ESHS"nin, "NES" sahibinin veya "Kurumsal Başvuru Sahibi"nin "Sertifika Kullanıcısı"na ait olan güvenli elektronik imza oluşturma aracının veya erişim verisinin çalınması, kaybolması, işlerliğini kaybetmesi yolunda bilgiye sahip olması veya "Sertifika Kullanıcısı"na ait olan güvenli elektronik imza oluşturma aracının veya erişim verisinin gizliliği ve güvenliği hakkında şüpheye düşmesi
- "NES" sahibinin fiil ehliyetinin sınırlandırıldığının, iflasının, gaipliğinin veya ölümünün öğrenilmesi
- "e-imzaTR"nın "ESHS" olarak hizmet vermeyi durdurması

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
- “e-imzaTR”
- Yetkileri doğrultusunda kamu kurumları ve yargı makamları

4.9.3. Sertifika İptal Talebi Prosedürleri

NES sahibi, yetkili kurumsal başvuru sahibi veya yetkili üçüncü kişiler, elektronik imzalı olarak gönderilen e-posta yoluyla, “KB”ler veya “e-imzaTR” Çağrı Merkezi aracılığıyla ve yazılı talimat ile sertifika iptal talebinde bulunabilirler. Ayrıca "e-imzaTR" websitesi üzerinden bireysel kullanıcı arayüzünü kullanarak iptal edebilirler. Sertifika iptal talebi, iptal talebinde bulunan kimsenin iptal yetkisinin tanımlanmasından ve onaylanmasından sonra derhal gerçekleştirilir. Yetkinin tanımlanmasında ise kişisel bilgiler ve ilgili gizli bilgiler kullanılır. Yazılı talimatlarda talimat üzerindeki imza ile sertifika başvuru formundaki imza karşılaştırılır. İptal durumu, iptal işlemi sonrası iptal talebinde bulunan kimseye telefonla veya e-posta ile 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. e-imzaTR’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, kendilerine gönderilen bir elektronik imzaya güvenmeden önce, ilgili sertifikayı doğrulamakla yükümlüdür. Sertifika durumunun doğrulanması için e-imzaTR tarafından yayımlanan güncel SİL ya da çevrim içi sertifika durum sorgulama servisi olan ÇSDP kullanılmalıdır. “e-imzaTR” üçüncü kişilere, Kanun’a göre oluşturulan güvenli elektronik imzalı doğrulamada güvenli elektronik imza doğrulama araçlarını kullanmalarını tavsiye eder.

4.9.7. Sertifika İptal Listesi (SİL) Yayımlama Sıklığı

“NES”lere ait “SİL”ler her 24 saatte bir 24 saat geçerli olacak şekilde, “e-imzaTR” alt kök sertifikalarına ait “SİL”ler 6 ayda bir yayınlanır.

4.9.8. SİL’lerin En Geç Yayımlanma Zamanı

“SİL”ler otomatik süreçler dahilinde oluşturulmalarının ardından hemen yayınlanır.

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

“e-imzaTR” gerçek zamanlı sertifika iptal durumu kontrolü sağlayan “ÇSDP” 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 "ÇSDP" aracılığıyla kontrol etmelidirler.

4.9.11. Diğer İptal Durumu Yayımlama Çeşitlerinin Varlığı

e-imzaTR, OCSP ve SİL dışında iptal durumu yayımlama yöntemi kullanmaz.

4.9.12. Anahtar Güvenliğinin Yitirilmesine İlişkin Özel Gereklilikler

e-imzaTR'ye ait bir güvenlik sorunu oluşması durumunda, durumdan etkilenen son kullanıcı sertifikaları e-imzaTR tarafından iptal edilir e-imzaTR 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, e-imzaTR tarafından ivedilikle kamuya açık bir şekilde web sitesi üzerinden ve gerekli durumlarda basın ve yayın organları aracılığıyla sertifika sahiplerine ve üçüncü kişilere duyurulur. e-imzaTR'a ait bir güvenlik sorununun duyurulması durumunda, sertifika sahiplerinin sertifikalarını kullanmaya devam etmelerine izin verilmez. e-imzaTR kaynaklı tüm sertifika iptal işlemlerinde, iptal sonrası yeni sertifika üretim işlemlerinin ivedilikle başlatılmasından e-imzaTR sorumludur.

4.9.13. Sertifika Askıya Alma Gerektiren Durumlar

"e-imzaTR" "NES" lerin askıya alma işlemi gerçekleştirmemekte olup, gerekli durumlarda "NES" ler iptal edilir.

4.9.14. Sertifika Askıya Alma Talebinde Bulunabilecek Kişiler

Bakınız 4.9.13

4.9.15. Sertifika Askıya Alma Talebi Prosedürü

Bakınız 4.9.13

4.9.16. Sertifikanın Askıda Kalma Süresinin Sınırları

Bakınız 4.9.13

4.10. Sertifika Durum Servisleri

e-imzaTR tarafından üretilmiş olan sertifikalar, sertifika sahibinin yazılı rızası olması kaydıyla, tüm sertifika sahiplerinin ve üçüncü kişilerin erişimine açık olarak web veya dizin sunucusu üzerinden yayımlanır.
Sertifika durum sorgulaması ise iki ayrı yöntemle yapılır: Sertifika İptal Listesi (SİLCRL)
ve Çevrimiçi Sertifika Durum Protokolü (ÇSDP).

4.10.1. İşlevsel Özellikler

e-imzaTR 12 (oniki) saatte bir olmak üzere günde 2 (iki) kez ve 24 (yirmidört) saatlik geçerlilik süresiyle, sertifika durumlarında hiçbir değişiklik olmasa bile yeni bir SİL yayımlar. Sistem 5 dakikada bir kendini yenileyerek herhangi bir değişiklik durumunda yeni SİL Yayınlar. e-imzaTR, 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

e-imzaTR , Madde 4.10.1.'de belirtilen koşullarda SİL ve OCSP hizmetini, kesintisiz olarak haftada 7 gün 24 saat ilkesine göre verir e-imzaTR merkezinde sunulan sertifika hizmetleri, erişilebilirlik ve yeniden devreye alma amaçları uyarınca her zaman yeterli düzeyde bir altyapı ile idame ettirilir. Hizmetlerde kesintiye yol açan ve e-imzaTR 'ın kontrolünün ötesinde bir durum ortaya çıktığında, e-imzaTR FKM, olayın ardından en geç 1 saat içinde sertifika hizmetlerinin yönetimini devreye alır.

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

e-imzaTR, 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

"Güven Merkezi" operasyonel gizliliği sağlayabilmek ve verilerin güvenliğini sağlayabilmek için gerekli tüm tedbirleri almıştır.

"Güven Merkezi" aşağıdaki fiziksel kontrolleri içerir.

- Yapı korkuluklarla çevrilmiştir.
- Korkuluklar 2.5 metre yüksekliğindedir.
- Girişler güvenlik görevlisinin kontrolü altındadır.
- Farklı güvenlik seviyelerinde farklı alanlardan oluşur.

5.1.2. Fiziksel Erişim

"e-imzaTR" "Güven Merkezi"ine giriş birden çok güvenlik kontrolüne tabi tutularak sağlanır. "Güven Merkezi"ine erişim için öncelikle yapıya erişim sağlanır. Yapıya erişim sağlandıktan sonra ikinci bir kontrolle "Güven

Merkezi"ine erişim sağlanır. "Güven Merkezi" erişimleri biyometrik kontrolde dahil olmak üzere 3 ayrı parametreli giriş sistemi ile kontrol edilir. Güvenilir ekipmanların bulunduğu silindirik turnike aracılığı ile her seferde bir kişi girecek şekilde gerçekleştirilebilir. Bölgeye girişler kayıt altına alınır ve 7/24 güvenlik kameraları ile izlenir.

5.1.3. Güç Kaynakları ve Havalandırma

"e-imzaTR" "Güven Merkezi" %99.9 süreklilikle hizmet verecek şekilde tasarlanmıştır. Güvenli ekipmanların bulunduğu alanlar alçak/yüksek gerilime karşı özel ekipmanlarla korunmaktadır. Enerji kesintilerinde otomatik olarak devreye giren jeneratör sistemiyle enerji devamlılığı sağlanır. "Güven Merkezi" da bulunan ekipmanların iklim şartlarından etkilenmemesi için klima sistemiyle sürekli ısı ve nem kontrolü yapılarak uygun ısıda tutulur.

5.1.4. Su Baskınları

Su baskınına maruz kalma bilgi işlem donanımlarında önemli hasara yol açabilir ve dolayısıyla "Güven Merkezi" tarafından sunulan hizmeti etkileyebilir. Su baskından kaynaklanabilecek hasarları önlemek için aşağıdaki önlemler alınmış.

- Yapı inşa aşamasındayken özel su geçirmez ekipmanlarla inşa edilmiştir.
- Su baskını durumlarında yetkili personele bilgi vermek için yapının çeşitli bölgelerinde su dedektörleri bulunmaktadır.

5.1.5. Yangın Önleme ve Yangından Korunma

Su ile söndürme sistemi bilgi işlem donanımlarında kalıcı hasara neden olabileceği için sunulan hizmeti etkileyebilir. Bu sebeple aşağıdaki yangın önleme sistemleri kullanılmaktadır..

- Yapı içerisinde sigara içilmesi yasaklanmıştır.
- Yangın uyarı ekipmanları yapı içerisinde çeşitli yerlerde konumlandırılmıştır.
- Yangın uyarı ekipmanları enerji kesintilerinden etkilenmez.
- "e-imzaTR" personeli yangın sırasında yapılacaklarla ilgili eğitim almıştır.
- "Güven Merkezi" bilgi işlem donanımlarına arar vermeyecek FM200 gazlı yangın söndürme sistemi ile donatılmıştır.

5.1.6. Saklama Ortamları

Veri depolama için aşağıdaki araçlar kullanılabilir.

- Kağıt, DVD, USB Bellekler, Harici Harddiskler.

Veri depolama araçlarına aşağıdaki kontroller uygulanır;

- Gizlilik arzeden tüm veriler özel dizayn edilmiş arşiv odasında saklanır.
- Arşiv odasına erişim biyometrik giriş kontrolleri uygulanarak iki katmanlı giriş kontrolüyle sağlanır.
- Zorunlu durumlarda medyalar dışarı şifreli şekilde çıkarılabilir.
- Veri depolama araçları arşiv odalarında kilitli bölümlerde saklanır.
- Tokenlar Güvenli bölgede saklanır.

5.1.7. Atıkların Atılması

Aşağıdaki atık kontrol politikaları uygulanır:

- Atıklar çevreye zarar vermeyecek şekilde imha edilir.
- Atıklar haftada en az bir kez bertaraf edilir.
- Gizlilik seviyesindeki atıkların dışarı sızması önlenir.

5.1.8. Tesis Dışı Yedekleme

"e-imzaTR" olası teknik arızalara ve/veya afetlere karşı, "Güven Merkezi" içinde ve dışında rutin olarak elektronik kayıtların yedeklerini alır ve saklar.

5.2. Prosedürel Kontroller

5.2.1. Güvenilir Roller

Güvenilir rollere sahip bir kişi görevinin düzgün yapılmaması halinde güvenlik sorunlarına neden olabilir. Bu rollerde görev alacak kişiler seçilirken görevlerini tam anlamıyla yerine getirebilecek ve oluşacak sorunlarda doğru karar verecek kişiler olmalıdır. Bu roller "Güven Merkezi"nin devamlılığı için temel oluşturmaktadır. Güvenilir roller aşağıdaki gibidir:

- Güven Merkezi Yöneticisi
- Kayıt Memuru
- Güvenlik Memuru
- Sistem Operatörleri
- Sistem Yöneticileri
- Sistem Denetçileri

5.2.2. Her Görev İçin Gereken En Az Kişi Sayısı

Roller oluşturulurken kişilerine kötü niyetli olabileceği düşünülerek gerekli görev ayrımları oluşturulmuştur. Her bir kullanıcının sisteme erişim yetkisi sorumluluklarını yerine getirebilecekleri şekilde sınırlandırılmıştır. Kriptogafik araçlara, güvenli bölgelere ve arşive erişim birden çok kullanıcının birlikte erişimiyle sağlanır. Kişisel hataların önüne geçebilmek için önemli rollerdeki işlemler en az iki kişi ile gerçekleştirilir.

İkili kontrol sistemleri aşağıdakiler için uygulanır::

- Sertifika ve Kök sertifikaların bulunduğu sistemlere erişim
- Arşive erişim

5.2.3. Her Görev için Kimlik Doğrulama

"Güvenli personel" olarak seçilen kimseler gerekli kimlik ve biyolojik bilgileri alınarak kendilerine atanan yetkiler doğrultusunda güvenlik sistemine kaydedilir. Kritik operasyonel işlemler öncesinde, işlemle ilgili yetki kontrolü ve görevli tanımlaması yapılır; yetki kontrolü ve tanımlamanın başarılı olması halinde işleme izin verilir ve kayıt altına alınır.

5.2.4. Görevlerin Ayrılmasını Gerektiren Roller

Bazı “NES” sertifika yaşam zinciri işlemleri, “ESHS” anahtar yönetimi işlemleri ve bunlara ilişkin kontroller birden çok “güvenli personel”in katılımıyla ve sorumlulukların ayrıştırılması prensibiyle gerçekleştirilir. Sorumlulukların ayrıştırılması prensibi ile bir işlemin tümünün veya büyük bir kısmının tek bir kişi tarafından yapılması engellenmiştir.
Yönetim; sorumlulukların atanması ve görevlerin ayrılığını sağlarken, aşağıdaki hususları göz önünde bulundurur:

a) Dolandırıcılığı önlemek için, gizlilik gerektiren faaliyetler, örneğin satın alma siparişinin verilmesi ve malların alındığının doğruluğunun kanıtlanması faaliyetleri, ayrılır;
b) Eğer gizliliğin ihlal edilmesi tehlikesi varsa, faaliyetten sorumlu personel sayısı artırılır;
c) Sistem erişim kontrollerinin yönetilmesi sorumluluğu, güvenlik kontrollerinin zayıflamasına sebep olabilecek diğer sorumluluklardan ayrılır;
d) Sistem kullanıcı erişim hakları üzerinde yapılacak tüm yaratma, değişiklik, kaldırma istekleri, Güven Merkezi Yöneticisi onayladıktan sonra gerçekleştirilir ve bu istekler, alınan ve uygulanan kararlar belgelenir. Belgeler ileride olabilecek bir kontrol için en az 1 yıl saklanır;
e) Sistem erişim hakları, Sistem Yöneticisi tarafından düzenli aralıklarla gözden geçirilir ve ihtiyaç duyulmadığında kaldırılır. Paylaşılan şifrelerin kontrolü ve yönetimi için sorumluluklar atanır;
f) Yüksek risk taşıyan görevlerde, ek kontroller uygulanır;
Yönetimsel prosedürlerin uygulanması denetlenir.

5.3. Personel Kontrolleri

5.3.1. Nitelik, Deneyim ve Güvenlik Gereklilikleri

“e-imzaTR” 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

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

5.3.4. Tekrar Eğitimi Sıklığı ve Gereklilikleri

“e-imzaTR” Düzenli olarak eğitim içeriklerini kontrol eder ve güncelleme, değişiklik yada uygun görülmesi halinde tazeleme eğitimleri düzenler.

5.3.5. İş Rotasyonu Sıklığı ve Sırası

İlgili değildir.

5.3.6. Yetkisiz İşlemler için Yaptırımlar

"e-imzaTR" personelin ya da işbirlikçilerin güvenlik prosedürlerinin dışında işlem yapması veya "e-imzaTR" 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

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

5.3.8. Personele Sağlanan Dokümantasyon

"e-imzaTR" 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

"e-imzaTR"nın "ESHS" işleyişine ve organizasyonel fonksiyonlarına ilişkin aşağıdaki kayıtlar elektronik ve/veya kağıt ortamında olayın tanımı, gerçekleşme tarihi, olayla ilgili kişilere ilişkin bilgiler de dahil olmak üzere tutulur.

- Sistemlerin kapatılması/açılması;
- "NES" uygulamalarının kapatılması/açılması;
- "ESHS" anahtar (veri) yaratma, yedekleme, saklama, kurtarma, arşivleme ve imha etme.;
- "NES" profilleri yada uygulamalarının değiştirilmesi;
- "NES" üretim politikalarında yapılan değişiklikler;
- Başarılı veya başarısız sisteme erişim girişimleri.;
- "NES" üretimi ve iptal edilmesi;
- Sistem arızaları, donanım arızaları ve diğer anormallikler
- Fiziksel erişim kayıtları;
- Sistem ayarlarında yapılan değişiklikler ve bakımlar;
- "e-imzaTR personel değişiklikleri;
- Tutarsızlık ve uzlaşma raporları;
- "NESİ" ve "NESUE" tüm versiyonları;
- Geçerli ve geçerlilik süresi geçmiş anlaşmalar
- Bireysel ve kurumsal "NES" başvuruları, başvurularda kullanılan bilgi ve belgeler.
- Bireysel ve kurumsal başvuru sözleşmeleri, ilgili diğer sözleşme ve belgeler.
- "NES"lerin oluşturulması, iptali, askıya alınması ve yenilenmesiyle ilgili eylem ve bilgiler (eylemlerin zamanı ve eylemleri yapan yetkililer de dahil olmak üzere).
- Müşteriler ve iş ortaklarıyla yapılan sözleşmeler, önemli yazışmalar.
- Geçerlilik süresi sona eren "NES"ler.
- Geçerlilik süresinin sona ermesinden itibaren "ESHS" kök ve alt kök sertifikası.
- İptal, askıya alma, askıdan kaldırma ile ilgili talep ve talebin doğrulanması eylemleri ve ilgili iletişim bilgileri, "SİL"ler.

Kayıtlar; doğru ve tam olarak sıralanması, saklanması, korunması ve çoğaltılması şartıyla elektronik veya basılı kopya halinde tutulabilir.

5.4.2. Kayıtları İşleme Sıklığı

Kayıt tutma işlemi sürekli gerçekleşir. Kayıtlar ayda bir kere denetlenir. "e-imzaTR" 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

Denetim kayıtları günlük ve haftalık arşivleme süreçleri doğrultusunda periyodik olarak yedeklenir.

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 "e-imzaTR" 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

Bakınız 5.4.1

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

"e-imzaTR" 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

NES'ler, SİL'ler, diğer iptal veri tabanı girdileri ve "e-imzaTR" tarafından gerekli görülen diğer bilgi ve belgeler tarih bilgisi içerir ; kullanılan tarih bilgisi zamanı UTC ile senkronize edilir.

5.5.6. Arşiv Toplama Sistemi

Arşivler "e-imzaTR" yönetim sistemleri kullanılarak elektronik ortamda veya yetkili kişilerin sorumluluğunda manuel olarak toplanır.

5.5.7. Arşiv Bilgisinin Edinilmesi ve Doğrulanması Prosedürleri

"NESUE", "NESİ" dokümanları ile son kullanıcı sözleşme örnekleri web sitesinin ilgili bölümünde yayınlanmaktadır (http://www.e-imzatr.com/bilgi-bankasi). 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

"e-imzaTR" "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 "e-imzaTR" "ESHS" kök sertifikası ve alt kök sertifikasının erişilebilirliği sağlanır. "e-imzaTR" 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-imzaTR" "ESHS" işlemlerinin güvenilirliğini ya da sürekliliğini tehlikeye atacak bir durum geliştiğinde ilgili prosedürler doğrultusunda sistemin güvenliğini ve sürekliliğini sağlayarak gerekli durumlarda ilgili kullanıcı ve kurumlara bilgilendirme yapar.

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

"Güven Merkezi"nde bulunan donanım, yazılım ve gerekli verilerin bozulması halinde öncelikle yedek donanım ve yazılım faaliyete geçirilir. "İş Sürekliliği Yönetimi ve Felaketten Kurtarma Prosedürü" doğrultusunda kaybolan verilerin yedekleri işleme konulur ve/veya yeniden oluşturulur. Kurtarılamayan veriler sebebiyle sertifika yönetim süreçlerinde geri dönülemez arızalar meydana gelmesi halinde, arızadan etkilenen sertifikalar derhal iptal edilir ve ilgili taraflara bilgi verilir.

5.7.3. İmza Oluşturma Verilerinin Güvenliğinin Yitirilmesi

"e-imzaTR" imza oluşturma verilerinin güvenliğinin ve güvenilirliğinin yitirilmesi durumunda, "e-imzaTR" afet yönetim prosedürleri ve iş sürekliliği planları uyarınca, ilgili sertifikalar iptal edilir ve Madde 5.6 uyarınca yeni imza oluşturma verisi oluşturularak devreye alınır. İptal edilen sertifikaların yerine prosedürler gereği yeni sertifikalar üretilir ve bu durumdan etkilenebilecek olan bütün sertifika sahipleri ile üçüncü kişiler ivedilikle bilgilendirilir.

5.7.4. İş Sürekliliği Yetenekleri ve Felaket Kurtarma

"e-imzaTR" merkezi dışında felaket kurtarma merkezi (FKM) tesis etmiştir. Afet sonrasında iş sürekliliğini temin etmek üzere "e-imzaTR" merkezinde bulunan veriler yedeklenir.

"e-imzaTR" işleyişini engelleyecek nitelikte olayların ya da güvenlik sorunlarının oluşması durumunda, "e-imzaTR" iş sürekliliği prosedürü ve planı uyarınca duruma müdahale edilir.

5.7.5. e-imzaTR'nin Faaliyetinin Son Bulması

"e-imzaTR"'nin faaliyetlerinin son bulması halinde, Kanun ve Yönetmelik gereği bu durumu en az 3 ay önce Kuruma bildirir ve kamuoyuna duyurur. "e-imzaTR" , 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, "e-imzaTR" ilgili sertifikaları iptal eder ve tüm ilgili tarafları bu durumdan haberdar eder. Bu durumda, "e-imzaTR" 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

"ESHS" imza oluşturma ve doğrulama verileri oluşturma işlemi, oluşturulan veriler için güvenliği ve gerekli şifreleme gücünü temin eden güvenilir sistemler kullanılarak, önceden seçilmiş birden fazla eğitimli "güvenli personel" ve ilgili görevliler tarafından yerine getirilir. "e-imzaTR" kök sertifikası için, imza oluşturma ve doğrulama verileri oluşturmada kullanılan şifreleme modülleri FIPS 140-2 Seviye 3 şartlarını karşılar. "e-imzaTR" kök sertifikasının imza oluşturma ve doğrulama verileri "Tebliğ"de belirtilen algoritmalara ve standartlara uygun olarak oluşturulur; anahtar oluşturma işlemi sırasında yapılan faaliyetler kaydedilir, tarih atılarak imzalanır. Bu kayıtlar denetim ve izleme amacıyla saklanır. İmza oluşturma verisi "ESHS"nin güvenli elektronik imza oluşturma aracında oluşturulur ve buradan yedekleme amacı dışında çıkarılamaz. İmza oluşturma verisinin güvenli olarak saklanması için gerekli fiziksel ve teknik güvenlik önlemleri alınır.

6.1.2. İmza Oluşturma Verisinin Sertifika Sahibine Ulaştırılması

İmza oluşturma verileri “NES” sahiplerine “NES” ile birlikte güvenli elektronik imza oluşturma aracı içerisinde imza karşılığında yada kargo ile iletilir.

6.1.3. İmza Doğrulama Verisinin ESHS'ye Ulaştırılması

İmza doğrulama verileri güvenli aktarım protokolleri kullanılarak “e-imzaTR” veri tabanına kaydedilir.

6.1.4. e-imzaTR İmza Doğrulama Verilerinin Üçüncü Kişilere Ulaştırılması

“e-imzaTR” “ESHS” sertifikaları (kök ve alt kök sertifikalar) http://www.e-imzatr.com adresinde yayınlanmaktadır. Bu sertifikalara ait SHA-1 özeti Türkiye’de yayımlanan en yüksek tirajlı üç ulusal gazetede kamuoyuna duyurulur. Ayrıca “e-imzaTR” imza doğrulama verisi ve “e-imzaTR” kök sertifikası, “e-imzaTR” tarafından sağlanabilecek olan güvenli elektronik imza doğrulama aracında yüklü olarak bu aracın sahiplerinin kullanımına sunulabilecektir.

6.1.5. Anahtar Uzunlukları

“e-imzaTR” “ESHS” imza oluşturma ve doğrulama verileri, 2048 bit RSA büyüklüğündedir. “NES”ler ise en az 2048 bit RSA büyüklüğünde imza oluşturma ve doğrulama verileri kullanılarak yaratılır

6.1.6. Anahtar Üretimi ve Kalite Kontrolü

“e-imzaTR” “NES” anahtarlarını tebliğin belirttiği standarlara uygun olarak “Güven Merkezi”nde oluşturur.

6.1.7. Anahtar Kullanım Amaçları

“NES” imza oluşturma ve doğrulama verileri sadece elektronik imza oluşturma ve doğrulama amacıyla kullanılır. “e-imzaTR” kök sertifikası imza oluşturma ve doğrulama verileri ise “NES” imzalama, “SİL” imzalama, “ÇSDP” sertifikası imzalama, zaman damgası sertifikası imzalama, sertifika iptal durum kaydı imzalama amaçlarıyla kullanılabilirler. Anahtarların kullanım amaçları, sertifikaların anahtar kullanım alanlarında belirtilir.

6.2. İmza Oluşturma Verisinin Korunması ve Kriptografik Modülü Mühendislik Kontrolleri

6.2.1. Kriptografik Modül Standartları ve Kontroller

"e-imzaTR'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 "e-imzaTR" 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-imzaTR" "ESHS" imza oluşturma ve doğrulama verilerine erişim ancak birden çok yetkili "Güvenli Personel"in gerekli güvenlik ve tanımlama prosedürlerini yerine getirmesi halinde gerçekleşmektedir.

6.2.3. İmza Oluşturma Verisinin Saklanması

"e-imzaTR" "NES" sahiplerine ait imza oluşturma verilerinin kopyalarını saklamaz.

6.2.4. İmza Oluşturma Verisinin Yedeklenmesi

"e-imzaTR" "NES" sahiplerine ait imza oluşturma verilerinin yedeklerini almaz. "e-imzaTR" "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

"e-imzaTR" "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. "e-imzaTR", "NES" sahiplerinin imza oluşturma verilerini arşivlemez.

6.2.6. İmza Oluşturma Verisinin Kriptografik Modül Transferi

"e-imzaTR", "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

Bkz. "NESİ" 6.2.6

6.2.8. Gizli Anahtarın Aktive Edilme Yöntemi

"e-imzaTR" "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-imzaTR" ye ait imza oluşturma ve doğrulama verileri yaşam ömürleri doldurduktan sonra kayıt altına alınarak yetkili personel tarafından imha edilebilir.

6.2.11. Kriptografik Modül Değerlendirmesi

"e-imzaTR" "ESHS" güvenli elektronik imza oluşturma araçları ve "NES" sahiplerine sağlanan güvenli elektronik imza oluşturma araçları "Tebliğ"de belirtilen standartlara uygundur.

6.3. Anahtar Çifti Yönetimiyle İlgili Diğer Konular

6.3.1. İmza Doğrulama Verilerinin Arşivlenmesi

"e-imzaTR" "ESHS" kök sertifikaları, "NES"ler ve bunlara bağlı imza doğrulama verileri en az 20 yıl boyunca saklanır.

6.3.2. Sertifikanın İşlevsel Süreleri ve Anahtar Çifti Kullanım Süreleri

"e-imzaTR" kök sertifikalarının geçerlilik süreleri 10 yılı aşmaz. "NES" kullanıcılarının sertifika süreleri sözleşmelerinde belirtildiği süre kadardır ancak imza doğrulama verileri sertifika geçerlilik süresinden sonra kullanılmaya devam edilebilir.

6.4. Erişim Şifreleri

6.4.1. Erişim Şifrelerinin Oluşturulması ve Kurulumu

"ESHS" imza oluşturma ve doğrulama verileri kriptografik verilerde saklanır ve en az iki yetkili "Güvenilir Personel" tarafından kriptografik akıllı kartlar ve şifreler aracılığıyla aktive edilebilir.

Kullanıcıların pin kodları kurulum esnasında sistem tarafından rastgele oluşturulur ve şifreli bir şekilde saklanır. Aktivasyon işlemi sırasından kullanıcı pin kodunu değiştirir ve bu kod "e-imzaTR tarafından saklanmaz.

6.4.2. Erişim Şifrelerinin Korunması

Erişim verilerinin "NES" sahiplerine ve "Güvenli Personel"e iletilmesinden sonra, verilerin gizliliğinin ve güvenliliğinin korunmasıyla ilgili sorumluluk "NES" sahiplerine ve "Güvenli Personel"e aittir

6.4.3. Erişim Şifreleriyle İlgili Diğer Konular

İlgili değildir.

6.5. Bilgisayar Güvenlik Kontrolleri

6.5.1. Bilgisayar Güvenliği Teknik Gereklilikleri

"e-imzaTR" 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, "e-imzaTR" 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-imzaTR" sertifika yaşam zinciri sistem geliştirme kontrolleri "e-imzaTR" kalite yönetimi prosedürleri ve TS ISO/IEC 27001 denetimleri sonucunda ortaya çıkan risk azaltma metodları uyarınca gerçekleştirilir.

6.6.2. Güvenlik Yönetimi Kontrolleri

TS ISO/IEC 27001 standardına uyumlu şekilde denetimler gerçekleştirilir. Değişiklik yapılması gerektiğinde öncelikle ihtiyaç belirlenir. Belirlenen ihtiyaç yazılı şekilde yöneticilere iletilir. Yöneticilerden onay geldiğinde yapılacak değişiklik kayıt altına alınarak gerçekleştirilir.

6.6.3. Yaşam Döngüsü Güvenlik Kontrolleri

İlgili değildir.

6.7. Ağ Güvenlik Kontrolleri

"KB" ve "Güven Merkezi" arasındaki bağlantılar da saldırılara karşı gerekli güvenlik önlemleri alınmıştır. Kullanılan ekipmanlar "ESHS" hizmetleri dışında gelecek tüm sorgu ve istekleri reddeder.

6.8. Zaman Damgası

Zaman Damgası ile ilgili bağlantılar da saldırılara karşı gerekli güvenlik önlemleri alınmıştır. Kullanılan ekipmanlar "ESHS" hizmetleri dışında gelecek tüm sorgu ve istekleri reddeder.

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

7.1. Sertifika Profili

7.1.1. Sürüm Numaraları

"NES"ler X.509 v3 standartlarına uygun olarak hazırlanır.

7.1.2. Sertifika Uzantıları

"e-imzaTR" tarafından oluşturulan "NES"ler ve "SİL"ler en yaygın kullanılan uygulamalarla çalışabilecek şekilde RFC 3280, X.509 v3 standardına uygun olarak hazırlanmıştır.

7.1.3. Algoritma Nesne Tanımlayıcıları

"e-imzaTR" sertifikaları aşağıdaki algoritmayı kullanarak imzalar.
sha256WithRSAEncryption algorithm (1.2.840.113549.1.1.11).

Algoritma tanımlayıcısı rsaEncryption olacaktır.
(OID: = 1.2.840.113549.1.1.1).

7.1.4. İsim Biçimleri

"NES" içerisindeki bilgi alanları X.500 standardına göre hazırlanacaktır.

7.1.5. İsim Kısıtları

"e-imzaTR" tarafından üretilen sertifikalarda anonim veya takma adlar kullanılmaz.
"e-imzaTR" nitelikli elektronik sertifikalarındaki isimlerde ayırt edici özellik olarak T.C. kimlik numarası kullanılır.

7.1.6. Sertifika İlkeleri Nesne Tanımlayıcısı

"e-imzaTR" 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

"e-imzaTR" alt kök sertifikalarında ihtiyaca göre ilke kısıtları uzantısı kullanabilir.

7.1.8. İlke Niteleyicilerinin Yazımı

"e-imzaTR" tarafından üretilen sertifikaların "sertifika ilkeleri" uzantısında, ilke niteleyicisi olarak NESUE dokümanına erişim bilgisi URL olarak verilmiştir.

7.1.9. Kritik Sertifika İlkeleri Uzantısının İşlenme Semantiği

İlgili değildir.

7.2. SİL Profili

"e-imzaTR" tarafından yayımlanan SİL'lerde temel olarak"e-imzaTR" elektronik imzasıyla birlikte yayımlayıcı bilgileri, SİL'in yayımlanma tarihi, bir sonraki SİL'in yayımlanma tarihi ve iptal edilen sertifikaların seri numarası ile iptal tarih ve zamanı yer alır. "e-imzaTR" tarafından yayımlanan SİL'ler Bilgi Teknolojileri ve Telekomünikasyon

Kurumu tarafından yayımlanan "Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri" dokümanına uygundur.

7.2.1. Sürüm Numarası

"e-imzaTR" ITU X.509 v2 standartlarında "SİL"ler üretir.

7.2.2. SİL ve SİL Giriş Uzantıları

"e-imzaTR" tarafından yayımlanan SİL'lerde, RFC 5280 tarafından tanımlanan uzantılar kullanılır.

7.3. ÇSDP(OCSP) Profili

"e-imzaTR" gerçek zamanlı bir sertifika durum sorgusu olan ÇSDP(OCSP) desteğini kesintisiz olarak sağlar. Bu hizmetle, uygun sertifika durum sorguları alındığında, sorguda talep edilen sertifikaların durumu ve protokol gereği gereken diğer ek bilgiler sorgu cevabı olarak talep sahibine döndürülür. "e-imzaTR" tarafından verilen ÇSDP(OCSP) cevap mesajları, Bilgi Teknolojileri ve Telekomünikasyon Kurumu tarafından yayımlanan "Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri" dokümanına uygundur.

7.3.1. Sürüm Numarası

"e-imzaTR" tarafından verilen ÇSDP(OCSP) hizmeti, "IETF RFC 2560 Internet X.509 Public Key Infrastructure Online Certificate Status Protocol - OCSP" dokümanı uyarınca v1 protokol sürümünü destekler.

7.3.2. OCSP Uzantıları

"e-imzaTR" tarafından verilen OCSP hizmeti içeriğinde, RFC 2560 tarafından tanımlanan uzantılar kullanılır. Ancak, temel OCSP bilgileri dışındaki tüm uzantıların kullanılması zorunlu değildir.

8. UYGUNLUK DENETİMİ VE DİĞER DEĞERLENDİRMELER

8.1. Denetim Sıklığı ve Durumları

Bilgi Teknolojileri ve İletişim Kurumu tarafından yapılan denetimlerin sıklığı, Kurum yetkililerinin inisiyatifinde olmakla beraber, en az iki yılda bir yapılacaktır.

TS ISO/IEC 27001 sertifikasına bağlı uyumluluk denetimleri her yıl yapılacaktır.

8.2. Denetçinin Kimliği ve Özellikleri

Bilgi Teknolojileri ve İletişim Kurumu Yeşilırmak Sokak No:16 06430
Demirtepe/Ankara
Tel: 0 312 294 72 00
Fax: 0 312 294 71 45

8.3. Denetçinin ESHS'yle İlişkisi

Tarafsız ve bağımsız bir değerlendirme sağlamak için denetçiler ve denetleme yapan kurumla mali, hukuki ve başka bir ilişki içerisinde bulunulmaz.

"e-imzaTR" iç denetimleri yetkili "e-imzaTR" "Güvenli personel" tarafından yapılacaktır.

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 "e-imzaTR" "Güven Merkezi" operasyonları ve "ESHS" işleyişine ilişkin süreçler denetlenir.

8.5. Eksiklik Durumunda Yapılacaklar

Yönetmelik gereği Kurum tarafından yapılan denetimler sırasında, "e-imzaTR"'nin faaliyet ve işleyişini olumsuz yönde etkileyebilecek derecede önemli konuların belirlenmesi durumunda, ilgili mevzuatta öngörülen yaptırım ve cezalar uygulanır.

8.6. Sonuçların Bildirilmesi

Denetlemelerde alınan kararlar ve ilgili durumlar "e-imzaTR" tarafından uygun görüldüğü şekilde taraflara bildirilebilir.

9. DİĞER İŞ KONULARI VE YASAL KONULAR

9.1. Ücretler

9.1.1. Sertifika Üretim ve Yenileme Ücretleri

Sertifika oluşturma ve yenileme ücretleri www.e-imzatr.com adresinden güncel bir şekilde öğrenilebilecektir.

9.1.2. Sertifika Erişim Ücretleri

"e-imzaTR" "NES" erişim hizmetleri için ücret talep etmez.

9.1.3. İptal veya Durum Bilgisi Erişim Ücretleri

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

9.1.4. Diğer Hizmetlerin Ücretleri

"e-imzaTR" kamuya açık yayınladığı belgeler için ücret talep etmez. Diğer hizmetlerle ilgili fiyat bilgisi www.e-imzatr.com adresinde belirtilmiştir.

9.1.5. Bedel İadesi

"e-imzaTR" ye yapılan "NES" başvurularında ücret peşin olarak tehsil edilir. Yapılan incelemeler sonucu "e-imzaTR" başvuru yapan kişi/kurum için "NES" oluşturulmasında bir sakınca tespit eder ise 5(beş) işgünü içerisinde ücreti iade eder. Yapılan başvuru sonunda eksik evrak olduğu tespit edilirse "e-imzaTR" başvuru sahibi kişi/kurumu bilgilendirir. Bilgilendirme sonucu eksik evraklar belirtilen süreler içerisinde tamamlanmazsa "e-imzaTR" tarafından yapılan harcalamalar mahsup edilerek kalan tutar başvuru sahibine iade edilir. Sertifika Kullanıcısı" "NES Paketi"ni teslim aldıktan sonra paket içerisinde yer alan ekipmanların eksiksiz ve çalışır durumda olduğunu ivedilikle kontrol

edecektir. “Sertifika Kullanıcısı”nın, “NES Paketi” içerisinde almış olduğu ekipmanların eksik ve ayıplı olduğunu tespit etmesi durumunda 7 (yedi) işgünü içerisinde "ESHS"yi çağrı merkezinden arayarak haberdar edecektir.Eksik yada ayıplı ürün bildirimlerinde "ESHS" bu çağrıyı aldıktan sonra ivedilikle herhangi bir masraf talep etmeden gerekli olan değişiklik işlemlerini yapacaktır.”e-imzaTR” kullanıcı hatalarından kaynaklanacak sorunlardan sorumlu olmadığı gibi bu durumlarla ilgili problemlerin çözümü için "ESHS"nin “Sertifika Kullanıcısı”na veya “Kurumsal Başvuru Sahibi”ne ayrıca ücret tahakkuk ettirme hakkı saklıdır. “Sertifika Kullanıcısı”nın sertifikasını iptal ettirmesi, erişim verisini veya güvenli elektronik imza aracını kaybetmesi halinde kendisine yeniden “NES” veya “NES”le birlikte güvenli elektronik imza aracı sağlanacak olursa, bunların ücreti tahakkuk edilir. “NES”in geçerlilik süresinin bitiminden önce “Sertifika Kullanıcısı” “NES” iptal eder veya iptal ettikten sonra yeni “NES” başvurusunda bulunursa, “NES”in iptal edildiği andan geçerlilik süresinin sonuna kadar olan kısmın ücreti mahsup veya geri iade edilmez. "e-imzaTR" Sertifika oluşturma verilerinin açığa çıkması ya da "e-imzaTR" den kaynaklı sorunlar sebebiyle son kullanıcı sertifikalarının güvenliği tehlikeye düşer ise "e-imzaTR" son kullanıcı sertifikalarını ücret talep etmeden yeniler.

9.2. Finansal Sorumluluk

9.2.1. Sigorta Kapsamı

Ulusal veya uluslararası düzeyde nitelikli elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan sigortalının elektronik imza kanunundan doğan yükümlülüklerini yerine getirmemesi sonucu oluşan, nitelikli elektronik sertifika sahibi kişi veya kuruluşların ve üçüncü şahısların uğrayacağı zararlara ilişkin sorumluluklar

9.2.2. Diğer Varlıklar

İlgili değildir.

9.2.3. Son Kullanıcılar için Sigorta veya Garanti Kapsamı

"e-imzaTR" kullanıcıları son kullanıcıların hatalarından kaynaklanmayan durumlarda olay başına 10.000 TL garanti kapsamına alınmaktadır

9.3. İş Bilgisinin Gizliliği

9.3.1. Gizli Bilginin Kapsamı

“ESHS”nin teknik ve operasyonel anlamda işlemlerine ilişkin bilgi güvenliği kapsamında gizli sayılan tüm bilgi ve belgeler, “ESHS”nin ticari faaliyetlerine ilişkin her türlü gizli bilgi ve belge, “ESHS” kök ve alt kök sertifikaları imza oluşturma verileri, işlem kayıtları, “NES” sahiplerinin “Kanun” kapsamında “kişisel veri” sayılan bilgileri, denetim ve değerlendirme kayıtları, “Güven Merkezi” ile ilgili her türlü gizli bilgi ve belge, donanım ve yazılımla ilgili teknik güvenlik bilgileri gizli bilgi kapsamındadır.

9.3.2. Gizlilik Kapsamı Dışındaki Bilgi

“NESUE”, “NESİ”, kullanıcı sözleşmeleri, bilgi deposunda bulunan bilgiler, “NES” sahibinin rızası doğrultusunda kamuya açık bir dizinde “e-imzaTR” tarafından yayınlanan “NES”ler, “e-imzaTR” kök ve alt kök sertifikaları, “SİL”ler gizli bilgi kapsamında sayılmazlar..

9.3.3. Gizli Bilginin Korunması Sorumluluğu

Elektronik İmza Kanunu’nun 12. maddesine göre “ESHS”;

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

9.4. Kişisel Bilgilerin Gizliliği/Özelliği

9.4.1. Gizlilik Planı

“e-imzaTR” “Kanun” kapsamındaki yükümlülükleri doğrultusunda “NES” sahiplerinin kişisel bilgilerini korur.

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”te ve “SİL”lerde herkesin erişimine açık bir şekilde yayınlanan bilgiler özel sayılmayan bilgilerdir.

9.4.4. Özel Bilgiyi Koruma Sorumluluğu

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

9.4.5. Özel Bilgiyi Kullanma Bildirimi ve Onayı

“e-imzaTR” kullanıcıların izinleri dahilinde yeni kampanya ve uygulamaları hakkında kişisel bilgiler doğrultusunda bilgilendirme yapabilir..

9.4.6. Yargısal ve İdari Süreçlere Uygun Olarak Bilginin Açıklanması

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

9.4.7. Bilginin Açıklandığı Diğer Durumlar

Uygulama dışıdır.

9.5. Fikri Mülkiyet Hakları

“e-imzaTR” tarafından yayınlanan tüm “NESİ”, “NESUE”, Kullanıcı sözleşmeleri, “e-imzaTR” tarafından www.e-imzatr.com adresinde yayınlanan her türlü metin ve marka değeri içeren belge, görsel ve işitsel içeriğin fikri ve mülkiyet hakları “e-imzaTR” ye aittir.

9.6. Sorumluluklar

9.6.1. ESHS Beyan ve Garantileri

"ESHS" aşağıdaki şartları kabul ve garanti eder:

- Operasyonel altyapı ve belgelendirme hizmetlerini sağlamak;
- "ÇSDP" ve veri depose hizmetleri vermek ve ilgili "NESİ" ve "NESUE" yi hazırlamak;
- "ESHS" imza oluşturma ve doğrulama verilerini sadece sertifika ve "SİL" leri imzalamak için kullanmak;
- Yürürlükteki Anlaşma ve Operasyonel Politikalar ve Prosedürler uyarınca doğrulama ve tanımlama prosedürlerini gerçekleştirmek;
- "NESİ" ve "NESUE" yönetmelikleri doğrultusunda sertifika oluşturma, iptal etme, yayınlama ve sertifika yönetim hizmetlerini sağlamak;
- "Güvenli personel"lerin sadece belirtilen amaçlar doğrultusunda işlem yaptığını kontrol etmek.

9.6.2. Kayıt Merkezi Sorumlulukları

"KB"ler kullanıcıların kimlik kontrolünü yaparak sisteme ilk kayıtlarını gerçekleştirmek, iptal ve yenileme taleplerini almak, aldıkları talepleri doğru ve eksiksiz bir biçimde "e-imzaTR"ye iletmekle görevlidirler.Bu yükümlülüklere aykırı bir şekilde hareket eden "KB" ler hakkında "e-imzaTR" inceleme başlatabilir gerekli gördüğü durumlarda yasal yaptırımlara tabi tutabilir.

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 "e-imzaTR" 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 "e-imzaTR"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 "e-imzaTR"nin, "NES" sahiplerinin, kurumsal başvuru sahiplerinin ve ilgili diğer tarafların zararlarını tazmin sorumlulukları vardır..

9.6.5. Diğer Katılımcıların Sorumlulukları

"e-imzaTR"'nin sertifika hizmetlerini verirken işbirliği yaptığı ve hizmet aldığı tüm kişi ve kuruluşlardan oluşan diğer katılımcılar, verecekleri hizmeti güvenilir ve doğru biçimde vereceklerini ve "e-imzaTR" iş süreçleri ve müşterileriyle ilgili gizli veya özel bilgileri açığa çıkarmayacaklarını garanti eder. "e-imzaTR" 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, "e-imzaTR"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, "e-imzaTR"nin, "NES" sahiplerinin veya üçüncü kişilerin zarar görmesi halinde, "NES" sahipleri bu zararları tazminle mükelleftir.
- "e-imzaTR" "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 ve "NESİ"nin yeni versiyonları www.e-imzatr.com adresinde yayınlanmasında itibaren yürürlüğe girer.

9.10.2. NESİ dokümanının Geçerliliğinin Sona Ermesi

"e-imzaTR" 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 "e-imzaTR" tarafından hazırlanır ve yayımlanır.

9.10.3. Geçerliliğin Sona Ermesinin Etkileri ve İşlerliğin Sürdürülmesi

"NESİ"nin geçerliliğinin sona ermesinden itibaren ilgili taraflar geçerliliği sona eren "NESİ"nin hükümleri ile bağlı değildir; "NESİ"nin geçerliliğinin sona ermesinden sonra yürürlüğe giren yeni "NESİ"nin hükümleri ilgili tüm taraflar için geçerli olacaktır.

9.11. Taraflara Özel Duyurular ve İletişim

"e-imzaTR"tarafından sertifika sahiplerine yapılacak olan kişisel duyurular için sertifika sahiplerinin uygun olan iletişim bilgileri kullanılır.

"e-imzaTR"'nin üçüncü kişilere yapacağı duyurular web üzerinden ya da basın yayın organları aracılığıyla yayımlanır.

9.12. Değişiklikler

"e-imzaTR" 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 "e-imzaTR" tarafından hazırlanır ve "e-imzaTR" 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 "e-imzaTR" uygulamaları farklı olacaktır.

9.12.1. Değişiklik Prosedürü

"e-imzaTR" 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 "e-imzaTR" 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. "e-imzaTR" 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

"e-imzaTR" 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, "e-imzaTR" sertifika sahipleri ile üçüncü kişileri bilgilendirebilmek için tüm makul imkanları kullanır.

Yeni NESİ ve NESUE sürümleri, eski sürümlerle birlikte "e-imzaTR" 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

"e-imzaTR", 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 "e-imzaTR" 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

"e-imzaTR", 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, "e-imzaTR" 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

"e-imzaTR"'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, "e-imzaTR" 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.