ARK|İMZA

NİTELİKLİ ELEKTRONİK SERTİFİKA İLKELERİ

Sürüm: 1.0

Yayın Tarihi: 02.03.2023

ArkSigner Yazılım ve Donanım San. Tic. A.Ş.

Üniversiteler Mah. 1606 Cad. Bilkent Cyberpark Cyberplaza A-Blok Kat:6 No:603

Tel: +90 312 484 79 33 e-Posta: destek@arkimza.com

İçindekiler Tablosu

1. GİRİŞ

ArkSigner Yazılım ve Donanım San. Tic. A.Ş. (kısaca "ArkSigner" olarak anılacaktır.), 23 Ocak 2004 tarih ve 25355 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiş olan 15 Ocak 2004 tarihli ve 5070 sayılı "Elektronik İmza Kanunu (kısaca "Kanun" olarak anılacaktır)" ve Bilgi Teknolojileri ve İletişim Kurumu (kısaca "BTK" olarak anılacaktır) tarafından yayımlanmış olan ikincil mevzuat uyarınca, elektronik sertifika hizmet sağlayıcılığı alanında faaliyet göstermektedir.

Nitelikli Elektronik Sertifika İlkeleri (kısaca "NESİ" olarak anılacaktır) olarak isimlendirilen bu doküman, Kanun, 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 ETSI TS 101 456, CWA 14167-1, IETF RFC 3647 standartlarına uygun şekilde ArkSigner'ın Elektronik Sertifika Hizmet Sağlayıcı (ESHS) olarak işleyişiyle ilgili genel kuralları içerir.

Bu kapsamda NESİ dokümanı, nitelikli elektronik sertifika başvurularının alınması, oluşturulması, yayımlanması, yenilenmesi ve iptal edilmesi gibi sertifikasyon süreciyle ilgili tüm idari, teknik ve yasal gereklilikler ile ESHS olarak ArkSigner'ın, sertifika sahibinin ve üçüncü kişilerin uygulama sorumluluklarını belirler.

1.1 Genel Bakış

NESİ dokümanı, ArkSigner tarafından verilen nitelikli sertifika hizmetlerini kapsar. NESİ dokümanında yer alan hususların nasıl uygulanacağını detaylı olarak anlatan doküman ise Nitelikli Elektronik Sertifika Uygulama Esasları (kısaca NESUE olarak anılacaktır)'dır.

ArkSigner sertifika hizmet sağlayıcısı, bu Nitelikli Elektronik Sertifika İlkeleri (NESİ) kitapçığı hükümlerine bağlı bir uygulama kitapçığı olan Nitelikli Elektronik Sertifika Uygulama Esasları (NESUE) uyarınca işletme faaliyetlerini yürütür ve kamuoyunun ve ilgili tarafların bilgisine sunar.

NESİ ve NESUE kitapçıkları mevzuat ve standartlar çerçevesinde en az yılda bir kere Yönetim Gözden Geçirme Toplantısı'nda değerlendirilir. Bu değerlendirmeler ya da yıl içinde ortaya çıkabilecek gereklilikler doğrultusunda bu kitapçıklar güncellenir.

1.2 Kitapçık Adı ve Tanımlama

Bu NESİ dokümanının açık adı ArkSigner Nitelikli Elektronik Sertifika İlkeleri (NESİ)'dir. Kitapçık sürüm numarası ve tarihi kapak sayfasında yer almaktadır.

ArkSigner NESİ dokümanı, kapsadığı sertifika ilkeleri Türk Standartları Enstitüsü'nden (TSE) alınan "2.16.792.3.0.061" benzersiz kurumsal nesne tanımlayıcı numarasını (OID) almıştır. ArkSigner, NESİ kitapçığında yer alan aşağıdaki sertifika tipleri için, ArkSigner kurumsal nesne tanımlayıcı numarasına bağlı aşağıdaki nitelikli elektronik sertifika ilkeleri nesne tanımlayıcı numarasını atamıştır.

NESİ dokümanı, http://www.arkimza.com web adresinde kamuya açık olarak yayımlanmaktadır.

"ArkSigner" Nitelikli Elektronik Sertifika İlkeleri:

5070 sayılı Kanun ile ilgili yönetmelik ve tebliğ uyarınca, bireylerin elle atılan imzaya eşdeğer güvenli elektronik imza kullanımına olanak veren nitelikli elektronik sertifikaları kapsar.

Nesne Belirteci : 2.16.792.3.0.061

1.3 Taraflar

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

1.3.1 Sertifika Üretim Merkezleri

Sertifika üretim merkezleri, ESHS'lerin nitelikli elektronik sertifika üretim, dağıtım ve yayımlamasından sorumlu birimleridir. Ana sertifika üretim merkezi ArkSigner'ın kök sertifikasına sahiptir. Son kullanıcı sertifikaları da burada üretilir.

1.3.2 Sertifika Kayıt Merkezleri

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

Kayıt merkeziyle ilgili işlemler, ArkSigner uygulamasından gelen sertifika başvuruları doğrultusunda ArkSigner merkezinde yer alan müşteri hizmetleri birimlerince yürütülür. Sertifika talepleri ArkSigner sertifika üretim merkezine iletilir ve sertifika üretimi gerçekleştirilir.

1.3.3 Sertifika Sahipleri

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

Kimlik ve/veya unvan doğrulaması, başvuru yapılan sertifika türüne göre ilgili mevzuat ve standartlara göre yapılır.

Sertifika sahibinin sorumluluğu ve sertifika kullanımından doğan sonuçlar, başvuru yapılan sertifika türüne göre ilgili mevzuatla ve sertifika sahibi tarafından imzalanan ya da onaylanan taahhütname veya sözleşmeyle belirlenir.

Kanunu'na göre "NES"ler sadece gerçek kişiler adına "ESHS"ler tarafından oluşturulabilirler.

1.3.4 Üçüncü Kişiler

Üçüncü kişiler, ArkSigner sertifika hizmetleri kapsamında, ArkSigner tarafından verilmiş olan nitelikli elektronik sertifikalara bağlı imza oluşturma verileriyle imzalanmış belgeleri alan, ilgili sertifikalara güvenen taraflardır. ArkSigner tarafından verilmiş sertifikaların kullanımına bağlı üçüncü kişilere karşı ArkSigner'ın sorumluluğunun sınırları işbu kitapçıkta belirtilmiştir.

1.3.5 Diğer Katılımcılar

ArkSigner'ın, sertifika hizmetlerini gerçekleştirirken iş birliği yaptığı ve hizmet aldığı tüm gerçek/tüzel kişiler ve kuruluşlar diğer katılımcıları oluşturur.

ArkSigner, 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 Sertifikaların Kullanım Şekilleri

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

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

1.4.2 Yasaklanmış Sertifika Kullanım Şekilleri

ArkSigner NES, mevzuatta belirlenen şartlar dışında kullanılamaz.

1.5 Sertifika İlkeleri Yönetimi

Sertifika ilkelerini oluşturan otorite olarak ArkSigner, "NESİ" dokümanının yönetiminden sorumludur.

1.5.1 NESİ Dokümanından Sorumlu Organizasyon

NESİ dokümanının tüm hakları ve sorumluluğu ArkSigner' a aittir.

1.5.2 İletişim Noktası

ArkSigner Yazılım ve Donanım San. Tic. A.Ş.

Adres **:** Üniversiteler Mah. 1606 Cad. Cyberpark A Blok, No:603 Çankaya/ANKARA

Telefon **:** +90 312 484 7933

Faks **:** +90 312 484 7933

E-posta **:** *info@arkimza.com*

Web **:** *www.arkimza.com*

1.5.3 NESİ'nin İlkelere Uygunluğunu Belirleyen Yetkili

NESİ dokümanının uygunluğu ve uygulanabilirliği ArkSigner üst yönetimi tarafından belirlenir.

1.5.4 NESİ Onaylama Prosedürleri

"NESİ" dokümanı ve "ESHS" isleyişine yönelik ilkelerin denetim çalışmaları düzenli olarak sürdürülür. Denetim çıktıları doğrultusunda ve/veya işleyiş süreçlerinde değişikliğe gidilmesi durumunda "NESİ" üzerinde değişiklik veya yenileme yapılır. "NESİ" üzerindeki değişiklikler veya yeni sürümler üst yönetiminin onayına sunulur.

1.6 Kısaltmalar ve Tanımlar

1.6.1 Kısaltmalar

BR	Baseline Requirement – Temel Gereksinimler
BTK	Bilgi Teknolojileri ve İletişim Kurumu
C	City - Şehir
CN	Common Name – Yaygın İsim
CRL	Certificate Revocation List- Sertifika İptal Listesi
CWA	Cen Workshop Agreement - Cen Çalıştay Sözleşmesi
DN	Distinguished Name - Ayırt Edici İsim

EAL	Evaluation Assurance Level - Değerlendirme Güvence Seviyesi
ECDSA	Elliptic Curve Digital Signature Algorithm - Eliptik Eğri Dijital İmza Algoritması
ESHS	Elektronik Sertifika Hizmet Sağlayıcısı
ETSI	European Telecommunication Standards Institute - Avrupa Telekomünikasyon Standartları Enstitüsü
FIPS	Federal Information Processing Standard - Federal Bilgi İşleme Standardı
FKM	Felaket Kurtarma Merkezi
IETF	Internet Engineering Task Force - İnternet Mühendisliği Görev Grubu
ISO	International Organization for Standardization - Uluslararası Standartlar Organizasyonu
L	Location - Lokasyon
NES	Nitelikli Elektronik Sertifika
NESİ	Nitelikli Elektronik Sertifika İlkeleri
NESUE	Nitelikli Elektronik Sertifika Uygulama Esasları
O	Organization - Kurum Adı
OCSP	On-line Certificate Status Protocol - Çevrim İçi Sertifika Durum Protokolü
OID	Object Identifier - Nesne Tanımlayıcı Numarası
OU	Organizational Unit - Kurumsal Birim
PIN	Personal Identification Number
PKI	Public Key Infrastructure - Açık Anahtar Altyapısı
RFC	IETF tarafından yayımlanan, kılavuz niteliğinde yorum talebi dokümanları
RSA	Ron Rivest, Adi Shamir ve Leonard Adleman tarafından güvenilirliği çok büyük tam sayılarla işlem yapmanın zorluğuna dayanan bir şifreleme tekniği
SHA	Secure Hash Algorithm
SİL	Sertifika İptal Listesi
SMS	Short Message Service – Kısa Mesaj Servisi
TCKK	Türkiye Cumhuriyeti Kimlik Kartı
TCKN	T.C. Kimlik Numarası
TSE	Türk Standartları Enstitüsü
URL	Uniform Resource Locator - Tekdüzen Kaynak Bulucu
UTC	Universal Time Coordinate - Eşgüdümlü Evrensel Zaman

1.6.2 Tanımlar

Açık Anahtar: Bir çift anahtarlı şifreleme algoritmasında diğer kişilerin de bilgisine açık olan kriptografik anahtar; Kanun'da imza doğrulama verisi olarak isimlendirilmiştir.

Açık Anahtarlı Altyapı (PKI): Matematiksel bağlantısı bulunan kriptografik anahtar çiftlerine dayalı ve sertifika tabanlı bir kriptografik sistemin kurulması ve işletilmesini sağlayan mimari yapı, teknikler, uygulamalar ve düzenlemeler bütünüdür.

Aktivasyon: İmza oluşturma verisi erişim şifresinin, kullanıcıya şifre zarfıyla gönderilmesi yerine, kendisi tarafından belirlenmesine imkân sağlayan güvenli bir yöntemdir. Bu yöntemde kullanıcı, ArkSigner tarafından sağlanan yazılımı kullanır. Akıllı kartı bilgisayara takılıyken, bu yazılım içinden "aktivasyon kodu" talebinde bulunur ve "aktivasyon kodu" başvurusu sırasında verdiği cep telefonuna gönderilir. Kullanıcı, aynı yazılımı ve "aktivasyon kodunu" kullanarak imza oluşturma verisi erişim şifresini belirler.

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

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

Anahtar Çifti: Aynı anda üretilen ve güvenli elektronik imza oluşturma aracına yüklenen imza oluşturma verisi ile imza doğrulama verisidir.

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

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

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

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

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

Dizin: Geçerli sertifikaları içinde bulunduran elektronik depodur.

Elektronik İmza: Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veridir.

Elektronik Sertifika: Açık anahtarlı alt yapıda, açık anahtar ile anahtar sahibinin kimliğini, elektronik sertifika hizmet sağlayıcısının gizli anahtarını kullanarak birbirine bağladığı elektronik kayıttır.

Elektronik Sertifika Hizmet Sağlayıcısı: Elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişilerdir.

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

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

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

Güvenli Elektronik İmza: Kanunun 4 üncü maddesinde sayılan niteliklere sahip:

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,

Elektronik imzadır.

Güvenli Elektronik İmza Doğrulama Aracı: Kanunun 7. 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,

İmza doğrulama aracıdır.

Güvenli Elektronik İmza Oluşturma Aracı: Kanunun 6. 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 imza oluşturma araçlarıdır.

İmza Doğrulama Aracı: Elektronik imzayı doğrulamak amacıyla imza doğrulama verisini kullanan yazılım veya donanım aracıdır.

İmza Doğrulama Verisi: Elektronik imzayı doğrulamak için kullanılan şifreler, kriptografik açık anahtarlar gibi verilerdir.

İmza Oluşturma Aracı: Elektronik imza oluşturmak üzere, imza oluşturma verisini kullanan yazılım veya donanım aracıdır.

İmza Oluşturma Verisi: İmza sahibine ait olan, imza sahibi tarafından elektronik imza oluşturma amacıyla kullanılan ve bir eşi daha olmayan şifreler, kriptografik gizli anahtarlar gibi verilerdir.

İmza Sahibi: Elektronik imza oluşturmak amacıyla bir imza oluşturma aracını kullanan gerçek kişidir.

İnceleme: Kuruma yapılan bildirimin gerekli şartları sağlayıp sağlamadığını tespit etmek amacıyla yapılan çalışmalardır.

İptal Durum Kaydı: Kullanım süresi dolmamış sertifikaların iptal bilgisinin yer aldığı, iptal zamanının tam olarak tespit edilmesine imkân veren ve üçüncü kişilerin hızlı ve güvenli bir biçimde ulaşabileceği kayıttır.

Kanun: 15 Ocak 2004 tarihli ve 5070 sayılı Elektronik İmza Kanunu'dur.

Kart Erişim Cihazı (KEC): Vatandaşın kimliğini doğrulama işlevi için kullanılan terminaldir.

KEC Standardı: Elektronik kimlik kartları için güvenli kart erişim cihazları ile ilgili TSE tarafından belirlenen TS 13582, TS 13583, TS 13584 ve TS 13585 standartlardır.

Kimlik Doğrulama Yönetmeliği: 26/6/2021 tarihli ve 31523 sayılı Resmî Gazete'de yayımlanan Elektronik Haberleşme Sektöründe Başvuru Sahibinin Kimliğinin Doğrulanma Süreci Hakkında Yönetmeliğidir.

Kök Sertifika: ESHS kurumsal kimlik bilgilerini ESHS imza doğrulama verisine bağlayan, sertifika üretim merkezi tarafından üretilmiş olan ve kendi imzasını taşıyan, ESHS'nin ürettiği tüm sertifikaların doğrulanabilmesi için ESHS tarafından yayımlanan sertifikadır.

Kurum: Bilgi Teknolojileri ve İletişim Kurumu'dur.

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

Nitelikli Elektronik Sertifika (NES): Kanunun 9 uncu maddesinde sayılan niteliklere sahip:

a) Sertifikanın "nitelikli elektronik sertifika" olduğuna dair bir ibarenin,

b) Sertifika hizmet sağlayıcısının kimlik bilgileri ve kurulduğu ülke adının,

c) İmza sahibinin teşhis edilebileceği kimlik bilgilerinin,

d) Elektronik imza oluşturma verisine karşılık gelen imza doğrulama verisinin,

e) Sertifikanın geçerlilik süresinin başlangıç ve bitiş tarihlerinin,

f) Sertifikanın seri numarasının,

g) Sertifika sahibi diğer bir kişi adına hareket ediyorsa bu yetkisine ilişkin bilginin,

h) Sertifika sahibi talep ederse meslekî veya diğer kişisel bilgilerinin,

ı) Varsa sertifikanın kullanım şartları ve kullanılacağı işlemlerdeki maddî sınırlamalara ilişkin bilgilerin,

j) Sertifika hizmet sağlayıcısının sertifikada yer alan bilgileri doğrulayan güvenli elektronik imzasının,

bulunması zorunlu olan elektronik sertifikadır.

Özetleme Algoritması: İmzalanacak elektronik verilerin sabit uzunlukta bir özetinin çıkarılmasında kullanılan algoritmadır.

Özne: Sertifikanın CN alanında yer alan kişi veya sunucu adıdır.

Sertifika: Bkz. "Elektronik Sertifika"

Sertifika İlkeleri: ESHS'nin işleyişi ile ilgili genel kuralları içeren belgedir.

Sertifika İptal Listesi (SİL): İptal edilmiş sertifikaların kamuya duyurulması amacıyla ESHS tarafından oluşturulan, imzalanan ve yayımlanan elektronik dosyadır.

Sertifika Mali Sorumluluk Sigortası: ESHS'nin, Kanundan doğan yükümlülüklerini yerine getirmemesi sonucu doğacak zararların karşılanması amacıyla yaptırmakla yükümlü olduğu sigortadır.

Sertifika Sahibi: Adına, sertifika hizmetlerinin koşullarına ilişkin ESHS ile sertifika sahibi taahhütnamesi ya da sözleşmesi imzalanan ya da onaylanan kişidir.

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

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

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

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

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

Zaman Damgası İlkeleri: Zaman damgası ve hizmetleri ile ilgili genel kuralları içeren belgedir.

Zaman Damgası Uygulama Esasları: Zaman damgası ilkelerinde yer alan hususların nasıl uygulanacağını detaylı olarak anlatan belgedir.

2 YAYIN VE BİLGİ DEPOSU SORUMLULUKLARI

ArkSigner, elektronik sertifika hizmet sağlayıcılığı kapsamında sertifika hizmetleriyle ilgili gereken doküman ve kayıtların etkin bir şekilde müşterilere ulaştırılabilmesi ve sertifika kullanımının güvenilirliğinin ve sürekliliğinin sağlanması amacıyla kamuya açık olarak yayımlanır.

2.1 Bilgi Deposu

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

2.2 Sertifika Bilgilerinin Yayımlanması

ArkSigner bilgi deposunda, ESHS iç işleyişine ait özel kurumsal prosedür ve talimatlar ile ticari gizli bilgiler dışında kalan, sertifika hizmetlerinin yürütülmesine ilişkin bilgiler herkesin erişimine açık tutulur. Nitelikli elektronik sertifika kapsamında ESHS'nin temel çalışma ilkelerini içeren NESİ dokümanı, bu ilkelerin nasıl uygulandığını gösteren NESUE dokümanı, sertifika sahibi ve ESHS sertifika

hizmetleri taahhütnameleri, sertifika süreçleriyle ilgili müşteri kılavuzları, herkesin erişimine açık olarak bilgi deposunda yer alır. Ayrıca, ArkSigner elektronik sertifika ve zaman damgası hizmetlerine ilişkin tüm kök ve alt kök sertifikaları herkesin erişimine açık olarak dizin sunucularda ve bilgi deposunda yayımlanır. ArkSigner tarafından üretilen sertifikalar, sertifika sahibinin yazılı rızası olmadan herkesin erişimine açık tutulmaz. Güncel iptal durum kayıtları hem OCSP desteğiyle hem de SİL'ler aracılığıyla erişime açık tutulur.

2.3 Yayımın Zamanı veya Sıklığı

Sertifika ve çevrim içi sertifika durum sorgulama kayıtları sürekli yayımlanır. Son kullanıcı sertifika durumlarında hiçbir değişiklik olmasa bile SİL, 12 (oniki) saatlik zaman aralığını geçmeyecek şekilde günde en az 2 (iki) kez ve 24 (yirmidört) saatlik geçerlilik süresiyle yayımlanır. Herhangi bir son kullanıcı sertifikasının iptal edilmesi halinde 5 (beş) dakika içinde yeni bir SİL üretilir. SİL geçerlilik süresi konusunda tek istisna kök ve alt kök sertifikaların geçerlilik sürelerinin dolması sırasında yaşanır. SİL içinde bulunan bir sonraki güncelleme tarihinin, kök veya alt kök sertifika geçerlilik bitiş tarihini aşması halinde SİL içinde bulunan bu değer kök veya alt kök geçerlilik bitiş tarihi olarak yazılır. ArkSigner, OCSP ve SİL yayımlama hizmetlerinin cevap verme süresinin 10 (on) saniyenin altında kalması sağlar.

2.4 Bilgi Deposuna Erişim Kontrolleri

Bilgi deposu herkesin erişimine açıktır. ArkSigner bu amaçla, yayımlanan bilgilerin gerçekliğini sağlamak üzere, https://www.arkimza.com adresi için gerekli her türlü güvenlik önlemini alır.

3 KİMLİĞİN DOĞRULANMASI

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

3.1 İsimlendirme

3.1.1 İsim Tipleri

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

3.1.2 İsimlerin Anlamlı Olması Gerekliliği

"NES" lerde kullanılacak isimler ve bilgiler başvuru sırasında verilen resmi belgelere dayandırılarak hazırlanır. İsimlendirmede bir belirsizlik tespit edilirse NES başvurusu iptal edilir.

3.1.3 Sertifika Sahiplerinin Anonimliği ve Takma Ad Kullanılabilirliği

"NES" sahibinin isminin gizlenmesi kanunen yasaktır. Bu sebeple anonim ve takma ad içeren sertifika üretilmez. Gerçek isimli sertifika üretilir.

3.1.4 İsim Biçimlerinin Değerlendirilmesi

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

3.1.5 İsimlerin Benzersizliği

ArkSigner tarafından verilen sertifikalar, ayırt edici isim alanında yer alan bilgilerle sertifika sahiplerinin eşsiz biçimde belirlenmesine olanak tanır. ArkSigner 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 Olduğunun Kanıtlanma Yöntemi

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

3.2.2 Tüzel Kişiliğin Doğrulanması

5070 sayılı Elektronik İmza Kanunu'na göre NES'ler sadece gerçek kişilere verilebilir. Bu nedenle tüzel kişilerin sertifika sahibi olarak kimliğinin doğrulanması söz konusu değildir.

Kurumsal Başvuru olarak nitelendirilen sertifikada tüzel kişiliğin isminin veya unvanının yer alması şekilde bir başvurunun kabul edilebilmesi için sertifika sahibinin bulunduğu ülke mevzuatı uyarınca gerekli belgelerin (ticari sicil kaydı, faaliyet belgesi, imza sirküleri, yetki belgesi vb.) sunulması ile kimlik doğrulama yapılır. Sunulan belgeler ile birlikte ilgili mevzuat, ArkSigner NESUE, NESİ ve sair düzenlemeler ile belirlenen prosedürlere uygun olacak şekilde doğrulama yapılır.

3.2.3 Gerçek Kişinin Kimliğinin Doğrulanması

NES başvurusunda bulunan kişilerin sertifikada yer alacak bilgileri, yasal düzenlemelerle belirlenen şekilde ve resmî belgelere dayandırılarak doğrulanır. NES başvurusu alınırken Kimlik Doğrulama Yönetmeliği'nin 5. maddesinin 2. fıkrasının (b), (c) ve (ç) bentlerinde düzenlenen yöntemlerden tercih edileni kullanılarak kişinin kimliği doğrulanır. Buna göre, kişinin tercihine göre kimlik doğrulama iki şekilde gerçekleştirilir:

- Yapay zekâ veya yetkili ile görüntülü görüşme ile kimlik doğrulama
- Yüz yüze yapılan işlemlerde kimlik doğrulama

Seçilen yönteme göre Kimlik Doğrulama Yönetmeliği'nin 7. maddesi ya da 8. maddesinde tariflenen usul ve esaslar uyarınca kimlik doğrulama yapılır.

İkinci veya daha sonraki başvurularda kimlik doğrulamasına ihtiyaç olmayan hallerde, telefon, faks veya e-posta gibi yollarla ArkSigner prosedürlerine göre doğrulama yapılır.

3.2.4 Doğrulama Yapılmaksızın Sertifikada Yer Alabilen Bilgiler

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

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

3.2.5 Yetkinin Doğrulanması

NES içeriğinde bir tüzel kişiliğin isminin yer alması söz konusu ise sertifika başvuru sahibinin temsil ve ilzama yetkili olduğu bu tüzel kişiliğe ait resmî belgeleri ibraz etmesi zorunludur.

3.2.6 Karşılıklı Çalışma Kriterleri

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

3.3 Anahtar Yenileme Taleplerinin Doğrulanması

3.3.1 Rutin Anahtarlar Yenileme için Kimlik Doğrulama

Anahtar çiftinin güvenli kullanım süresinin sonunda, yeni anahtar çifti üretimi, kullanıcının yeni bir NES başvurusunda bulunmasıyla gerçekleştirilir.

Yeni sertifika başvurusu, sertifikanın kullanım süresi içinde, elektronik ortamda ve mevcut sertifikaya bağlı imza oluşturma verisiyle imzalanarak yapılabilir. Yeni sertifika içinde yer alacak bir bilgide değişiklik gerekmesi durumunda, bu değişikliğin resmî belgeye dayandırılması zorunludur. Sertifikada yer almayan diğer kullanıcı bilgilerindeki değişiklikler ise NES sahibinin yazılı veya elektronik beyanıyla kabul edilir.

Rutin anahtar yenileme işlemleri sırasında başvuru sahibinin başvuru bilgileriyle ilgili herhangi bir tereddüt doğması halinde telefonla doğrulama yapılır. Bu doğrulamayı yapan yetkililerce söz konusu şüphenin giderilememesi durumunda ise Madde 3.2 ile düzenlenen usullerden biri ile kimlik doğrulanır.

Geçerli bir NES sahibi için anahtar yenileme talebi, sertifikasının süre sonundan en erken 30 (otuz) gün önce yapılabilir. Yapılmış bir talep en fazla 30 (otuz) gün süreyle geçerliliğini korur. Sertifika sahibinin ilk başvurusundan yenileme başvurusuna kadar geçen sürede ArkSigner sertifika hizmetlerinin sağlanmasına ilişkin kayıt ve şartlarda değişiklik olmuş ise bu değişiklikler uygun biçimde sertifika sahibine bildirilir.

3.3.2 İptal Sonrası Anahtar Yenileme için Kimlik Doğrulama

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

- 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.

3.4 İptal Talebi için Kimlik Doğrulama

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

- Sertifika sahibi ArkSigner uygulaması üzerinden veya müşteri temsilcisiyle görüşerek kimlik doğrulaması yapıldıktan sonra iptal işlemini gerçekleştirebilir.
- Sertifika sahibi ArkSigner ofisine gelerek dilekçe ile başvurabilir.

4 SERTİFİKA YAŞAMSAL DÖNGÜSÜ İŞLEVSEL GEREKLİLİKLERİ

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

4.1 Sertifika Başvurusu

4.1.1 Kimler Sertifika Başvurusunda Bulunabilir?

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

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

4.1.2 Sertifika Başvurusu, Kayıt Süreci ve Sorumluluklar

NES başvurusu farklı yöntemlerle gerçekleştirilebilir.

Kişilerin Arksigner yetkili ofisine gelerek müşteri temsilcileri aracılığıyla ve KEC ile kimlik doğrulama yapılması ile NES başvurusu yapılabilir. Ödeme alındıktan sonra NES taahhütnamesinin başvuru sahibince onaylanması ya da imzalanması ile akıllı kart elden teslim edilir.

Kişiler, ArkSigner NES satımında yetkili olduğu ArkSigner uygulamasında ilan edilen satış mağazalarından token satın alabilir. Bu durumda, satın alınan token cihazı ile ArkSigner uygulaması üzerinden de başvuru ve kimlik doğrulama yapılabilmektedir. Başvuru sahibinin kimlik belgesi ile uygulama üzerinden Madde 3.2 ile tariflenen yöntemlerden tercih edileni ile kimlik doğrulaması yapılır. Sonraki adımda müşteri temsilcisine bağlanılır. Başvuru sahibi ArkSigner ofisinin bulunduğu ilde ise, müşteri temsilcisi tarafından uygulama yardımı ile kişiye ait TCKK ve PIN ile kimlik doğrulaması yapılır. Ödeme alındıktan sonra NES taahhütnamesinin başvuru sahibince onaylanması ya da imzalanması ile akıllı kart elden teslim edilir.

Sertifika başvuru kaydı gerek ArkSigner uygulaması üzerinden uzaktan gerek ise ArkSigner yetkili ofislerine bizzat gidilmesi ile ArkSigner uygulaması üzerinden yapılacak kimlik doğrulaması ile yapabilir. Ödeme alındıktan sonra NES taahhütnamesinin başvuru sahibince onaylanması ya da imzalanması ile akıllı kart elden teslim edilir.

Bu kayıtlar doğrultusunda anahtar üretimi ArkSigner tarafından gerçekleştirilir.

4.2 Sertifika Başvurusunun İşlenmesi

4.2.1 Kimlik Doğrulama İşlemlerinin Yerine Getirilmesi

NES başvurusu sırasında, başvuru sahibinin kimliği yasal düzenlemeler uyarınca resmî belgelere dayandırılarak doğrulanır. Kimlik doğrulama işlemi ArkSigner uygulaması ile Kimlik Paylaşım Sistemi üzerinden yapılır.

4.2.2 Sertifika Başvurularının Kabulü veya Reddedilmesi

Aşağıdaki koşulların yerine gelmesi halinde bir sertifika başvurusu kabul edilir:

- Kimlik doğrulamanın yapılması ve başvuru için gerekli belgelerin eksiksiz olarak tamamlanmış olması.
- Başvuru sahibinin ARKSİGNER uygulaması üzerinden başvuruyu tamamlamış olması.
- Ödemenin yapılmış olması.

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

- Kimlik doğrulamanın yapılamaması ve başvuru için gerekli belgelerin tamamlanmaması.
- Başvuru sahibinin ARKSİGNER uygulaması üzerinden başvuruyu tamamlayamamış olması.
- Ödemenin yapılmamış olması.

4.2.3 Sertifika Başvurularının İşleme Süresi

Başvuru sahibinin evraklarının eksiksiz olması durumunda ArkSigner'a ulaşan NES başvurularının işlenme süresi en fazla 5 (beş) iş günüdür.

Başvuru sahibinin ArkSigner ofisine gelerek başvuru yapması durumunda akıllı kart hemen üretilip teslim edilir.

Bu madde altında sertifika başvurusunun işlenmesine ilişkin verilen süre, sertifika başvurularının

Madde 3.2'de yer alan esaslar ve sair ArkSigner prosedürlerine göre eksiksiz ve doğru olması halinde geçerlidir.

4.3 Sertifika Üretimi

4.3.1 Sertifika Üretimi Sırasındaki ESHS Faaliyetleri

Bölüm 4.2.2'de yer alan esaslar uyarınca kabul edilen sertifika başvuruları ArkSigner tarafından işlenerek Tebliğ'in 8. maddesinde yer alan "Güvenli Elektronik İmza Oluşturma ve Doğrulama Araçlarına" uygun olarak üretilir ve teslim edilir.

4.3.2 Sertifika Üretimiyle İlgili Sertifika Sahibinin Bilgilendirilmesi

Sertifika üretildikten sonra sertifika sahibine ArkSigner prosedürlerine uygun iletişim kanalıyla üretimin yapıldığı bilgisi verilir.

4.4 Sertifikanın Kabulü

4.4.1 Kabulün Şekli

Sertifika ArkSigner tarafından imzalandıktan ve Bilgi Depolarında yayınlandıktan sonra ArkSigner tarafından kabulü yapılmış olur. Üretimi yapılan sertifika kullanıcıya teslim edildiğinde kullanıcı tarafından kabul edilmiş sayılır.

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

4.4.2 ESHS Tarafından Sertifikanın Yayımlanması

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

4.4.3 Diğer Katılımcıların Sertifika Üretimiyle İlgili Bilgilendirilmesi

Uygulama dışıdır.

4.5 Anahtar Çifti ve Sertifika Kullanımı

4.5.1 Sertifika Sahibi İmza Oluşturma Verisi ve Sertifika Kullanımı

Sertifika sahibi, sertifikasını ve sertifikaya ait gizli anahtarı, Kanun, Yönetmelik ve diğer düzenlemeler ile NESİ ve NESUE kitapçıklarında ve ilgili nitelikli elektronik sertifika başvuru ve taahhütnamesinde yer alan koşullar ve belirlenmiş sınırlar içinde kullanılabilir.

NES için imza oluşturma verisi erişim şifresi, aktivasyon işlemiyle sertifika sahibi tarafından ArkSigner uygulamaları aracılığıyla belirlenir.

NES sahibi,

- Adına düzenlenen güvenli elektronik imza oluşturma aracını şahsen veya uygulama üzerinden beyan ettiği kişi tarafından teslim alınmalıdır.

- Aktivasyonla belirlenen erişim şifreleri için cep telefonunun veya e-posta adresinin diğer kişilerce kullanımına izin vermemelidir.

- Aktivasyonla belirlenen erişim şifreleri ve güvenli elektronik imza oluşturma aracının diğer kişilerce kullanımına izin vermemelidir.

- İmza oluşturma verisinin ve/veya imza oluşturma aracının, kayıp, açığa çıkma, değişime uğrama ve diğer kişilerce kullanımı durumlarında veya bu durumların oluşmasına neden olabilecek şartların ortaya

çıkması halinde sertifikanın iptalini sağlamak üzere derhal ArkSigner'a bilgi vermelidir.

4.5.2 Üçüncü Kişilerin İmza Doğrulama Verisi ve Sertifika Kullanımı

Üçüncü kişiler, güvenecekleri sertifikaların geçerliliğini kontrol etmekle ve sertifikaları Kanun, Yönetmelik ve diğer düzenlemeler ile NESİ ve NESUE kitapçıklarında belirlenmiş kullanım amaçları ile maddi kapsamı dâhilinde kullanmakla yükümlüdürler.

Sertifikanın geçerliliğinin kontrolü makul ve güvenli koşullar altında yapılmalıdır. Aksi yönde bir durumun oluştuğuna dair bir tereddüt olması halinde, üçüncü kişiler gerekli tedbirleri almakla sorumludur.

4.6 Sertifika Yenileme

Sertifika yenileme, sertifika içeriğinde açık anahtar dâhil aynı bilgiler yer almak kaydıyla, sertifika geçerlilik süresinin uzatılmasıdır. ArkSigner yeni anahtar çifti oluşturma yöntemini kullanarak başvuru yeni yapılmış kabul ederek yeni sertifika oluşturma süreci baştan başlatılır.

4.6.1 Sertifika Yenilemeyi Gerektiren Durumlar

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

4.6.2 Yenileme Talebinde Bulunabilecek Kişiler

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

4.6.3 Sertifika Yenileme Talebinin İşlenmesi

Geçerlilik süresi içinde NES sahibi, sertifika yenileme başvurusunu ArkSigner uygulaması aracılığıyla elektronik imzasıyla yapabilir. Bu işlemle kimlik kontrolü yapılmış sayılarak yenileme talebi işleme alınır. Sertifikanın süresi dolmuş ise Madde 4.1.2 de belirtilen adımlar uygulanır.

4.6.4 Yenilenmiş Sertifikayla İlgili Sertifika Sahibine Bildirim Yapılması

Bölüm 4.3.2'de yer alan ilkeler uyarınca yürütülür.

4.6.5 Yenilenen Sertifikanın Kabulü

Bölüm 4.4.1'de yer alan ilkeler uyarınca yürütülür.

4.6.6 ESHS Tarafından Yenilenen Sertifikanın Yayımlanması

Bölüm 4.4.2'de yer alan ilkeler uyarınca yürütülür.

4.6.7 Diğer Katılımcıların Yeni Sertifika Üretimiyle İlgili Bilgilendirilmesi

Uygulama dışıdır.

4.7 Anahtar Yenileme

4.7.1 Anahtar Yenilemeyi Gerektiren Durumlar

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

4.7.2 Anahtar Yenileme Talebinde Bulunabilecek Kişiler

NES için sertifika sahibi ve/veya kurumu temsile yetkili gerçek kişidir.

4.7.3 Anahtar Yenileme Talebinin İşlenmesi

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

4.7.4 Yeni Sertifikayla İlgili Sertifika Sahibine Bildirim Yapılması

Bölüm 4.3.2'de yer alan ilkeler uyarınca yürütülür.

4.7.5 Anahtarı Yenilenen Sertifikanın Kabulü

Bölüm 4.4.1'de yer alan ilkeler uyarınca yürütülür.

4.7.6 ESHS Tarafından Anahtarı Yenilenen Sertifikanın Yayımlanması

Bölüm 4.4.2'de yer alan ilkeler uyarınca yürütülür.

4.7.7 Diğer Katılımcıların Yeni Sertifika Üretimiyle İlgili Bilgilendirilmesi

Uygulama dışıdır.

4.8 Sertifika Değişikliği

4.8.1 Sertifika Değişikliğini Gerektiren Durumlar

ArkSigner 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 Katılımcıların Yeni Sertifika Üretimiyle İlgili Bilgilendirilmesi

Bölüm 4.4.3'de yer alan ilkeler uyarınca yürütülür.

4.9 Sertifika İptali ve Askıya Alınması

4.9.1 Sertifika İptalini Gerektiren Durumlar

4.9.1.1 Son Kullanıcı Sertifikaları

Sertifikanın kullanım süresi içinde geçerliliğini kaybetmesi durumunda sertifika iptal edilir. NES için iptal işlemi talebin ulaşmasının ardından derhal gerçekleştirilir.

Aşağıda yer alan koşullar sertifikanın iptalini gerektirir:

- Sertifika sahibinin veya temsile yetkili kişinin talebi,

- Sertifika başvurusunda veya sertifikada yer alan bilgilerin sahteliğinin veya yanlışlığının ortaya çıkması; ArkSigner bu şartın oluştuğuna dair makul kanıta dayalı kanaat oluşturabileceği gibi aynı şart sertifika sahibi veya temsili yetkili kişinin bildirimiyle de oluşabilir.

- Sertifika içeriğinde yer alan özne veya sertifika sahibi bilgilerinde bir değişiklik olması,
- Sertifika sahibinin fiil ehliyetinin sınırlandığının, iflâsının veya gaipliğinin veya ölümünün öğrenilmesi,
- Sertifikanın amacı dışında kullanıldığına dair bir kanıtın elde edilmesi,
- Gizli anahtarın kaybedilmesi, çalınması, ortaya çıkma şüphesinin veya üçüncü kişilerin erişimi ve kullanımı tehlikesinin oluşması,
- Gizli anahtara erişim şifresinin ortaya çıkması veya benzer bir nedenle sertifika sahibinin gizli anahtar üzerindeki kontrolünü kaybetmesi,
- Gizli anahtarın içinde bulunduğu yazılım veya donanım aracının kaybolması, bozulması veya güvenilirliğini kaybetmesi,
- ArkSigner'ın, sertifikanın NESİ ve NESUE rehber kitapçıkları ile ArkSigner sertifika sahibi taahhütnamesi hükümlerine aykırı olarak kullanıldığına ilişkin bir bildirim alması veya böyle olduğunun anlaşılması,
- ArkSigner'ın tamamen kendi takdiri sonucu, sertifikanın verilişi sırasında işbu NESİ rehber kitapçıklarının uygulama esaslarına ilişkin bir uygunsuzluk tespit etmesi.
- ArkSigner'ın Kanun'a dayalı sertifika verme hakkının ortadan kalkması.
- ArkSigner kök veya alt kök sertifikalarına ait gizli anahtarların açığa çıkma şüphesinin oluşması veya açığa çıkması.
- ArkSigner'ın sertifika hizmetleri vermeyi durdurması ve başka bir ESHS ile anlaşmaması.

4.9.1.2 ArkSigner Alt Kök Sertifikaları

Alt kök sertifikanın kullanım süresi içinde geçerliliğini kaybetmesi durumunda en geç 7 (yedi) gün içinde iptal edilir.

Aşağıda yer alan koşullar alt kök sertifikasının iptalini gerektirir:

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

4.9.1.3 Alt ESHS Sertifikaları

Uygulama dışıdır.

4.9.2 Sertifika İptal Talebinde Bulunabilecek Kişiler

Aşağıda belirtilen kişiler sertifika iptal talebinde bulunabilir:

- Sertifika sahibi ile sertifikada kurum bilgisinin yer alması halinde ilgili kurumu temsile yetkili kişi,
- Güvenli elektronik imza oluşturma aracının sahibi,
- ArkSigner yetkilileri.

4.9.3 Sertifika İptal Talebi Prosedürleri

NES iptal talepleri, sertifika sahibinden;

- 7 gün 24 saat ilkesine göre ArkSigner uygulamaları üzerinden,
- 09.00-18.00 saatleri ve 18:00'den sonra ArkSigner uygulaması üzerinden randevu oluşturarak, tüm müşterilere duyurulan ve açıkça ilan edilen telefon numarası üzerinden sesli çağrı sistemi aracılığıyla,
- Mesai saatleri içinde yazıyla (posta aracılığıyla gelen imzalı yazılar)

olmak üzere farklı yollarla alınabilir.

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

İçeriğinde kurum bilgisi de yer alan NES iptal talepleri, sertifika sahiplerinin yanı sıra onaylı iptal başvuruları ile ilgili kurumu temsile yetkili kişilerden de alınabilir. İşlem sonrası iptal durumu yetkili ile sertifika sahibine e-posta/sms ile bildirilir.

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

İptal edilmiş bir sertifikanın yeniden kullanılabilir hale gelmesi için bir prosedür olmadığı gibi, iptal edilmiş bir sertifikanın yeniden kullanılabilir hale getirilmesi için sunulan bir araç da yoktur. İptal işlemi, veri tabanında OCSP ve SİL hizmetlerinde anlık güncellemeye yol açar.

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

4.9.4 Sertifika İptal Talebi Gecikme Periyodu

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

4.9.5 ArkSigner'ın Sertifika İptal Talebini İşleme Süresi

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

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 ArkSigner tarafından yayımlanan

güncel SİL ya da çevrim içi sertifika durum sorgulama servisi olan OCSP kullanılmalıdır. ArkSigner 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

ArkSigner, herhangi bir son kullanıcı sertifikasının iptal edilmesi halinde OCSP ve SİL servislerinin tutarlı olması amacıyla 5 (beş) dakika içinde yeni bir SİL üretir. Ayrıca sertifika durumlarında hiçbir değişiklik olmasa bile, günde en az iki kez yeni bir SİL yayımlar. ArkSigner alt kök sertifikalarına ait SİL'ler, bir alt kök sertifika iptali durumunda veya sertifika iptali olmasa bile yılda en az bir kez yayımlanır.

4.9.8 SİL'lerin En Geç Yayımlanma Zamanı

SİL'ler üretildikleri andan itibaren en geç 5 (beş) dakika içinde yayımlanır.

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

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

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

4.9.10 Çevirim İçi Sertifika İptal/Durum Kontrol Gereklilikleri

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

4.9.11 Diğer İptal Durumu Yayımlama Çeşitlerinin Varlığı

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

4.9.12 Anahtar Güvenliğinin Yitirilmesine İlişkin Özel Gereklilikler

ArkSigner'a ait bir güvenlik sorunu oluşması durumunda, durumdan etkilenen son kullanıcı sertifikaları ArkSigner tarafından iptal edilir. ArkSigner'a 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, ArkSigner tarafından ivedilikle kamuya açık bir şekilde web sitesi üzerinden ve gerekli durumlarda basın ve yayın organları aracılığıyla sertifika sahiplerine ve üçüncü kişilere duyurulur.

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

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

4.9.13 Sertifika Askıya Alma Gerektiren Durumlar

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

Nitelikli elektronik imza sertifikasının sertifika sahibine ulaştıktan sonra aktivasyon işlemi yapılıncaya

kadar geçen süre içerisinde de sertifikalar askıda kalır.

4.9.14 Sertifika Askıya Alma Talebinde Bulunabilecek Kişiler

Bölüm 4.9.2'de yer alan ilkeler uyarınca yürütülür.

4.9.15 Sertifika Askıya Alma Talebi Prosedürü

Aşağıdaki istisnai haller saklı kalmak kaydıyla Bölüm 4.9.3'de yer alan ilkeler uyarınca yürütülür.

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

4.9.16 Sertifikanın Askıda Kalma Süresinin Sınırları

ArkSigner, NES iptal talep kaynağının doğrulanamadığı durumlarda askıya aldığı sertifikaları, doğrulama işlemi sonuçlanıncaya veya süre sınırı aşılana kadar askıda bırakılır. Sertifika sahipleri tarafından iptali gerektiren bir durumun olup olmadığından emin olunamadığında askıya alınan sertifikalar, sertifika sahibinden iptal gerekliliği onaylandığında iptal edilir.

Her iki durumda da, askıya alma süresi 30 (otuz) günü aşamaz. Bu sürenin sonunda hala askıda bulunan sertifikalar, güvenlik nedeniyle otomatik olarak iptal edilir.

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

4.10 Sertifika Durum Servisleri

ArkSigner tarafından üretilmiş olan sertifikalar yayımlanmaz.

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

4.10.1 İşlevsel Özellikler

ArkSigner sertifika ve çevrim içi sertifika durum sorgulama kayıtları sürekli yayımlar. Son kullanıcı sertifika durumlarında hiçbir değişiklik olmasa bile SİL, 12 (on iki) saatlik zaman aralığını geçmeyecek şekilde günde en az 2 (iki) kez ve 24 (yirmi dört) saatlik geçerlilik süresiyle yayımlar. Herhangi bir son kullanıcı sertifikasının iptal edilmesi halinde OCSP ve SİL servislerinin tutarlı olması amacıyla 5 (beş) dakika içinde yeni bir SİL üretir.

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

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

4.10.2 Hizmetin Sürekliliği

ArkSigner, Madde 4.10.1'de belirtilen koşullarda SİL ve OCSP hizmetini, kesintisiz olarak 7 gün 24 saat ilkesine göre verir.

ArkSigner 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

ArkSigner'ın kontrolünün ötesinde bir durum ortaya çıktığında ArkSigner İş Sürekliliği Prosedürü'ne göre gerekli işlemler yapılır.

4.10.3 İsteğe Bağlı Özellikler

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

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

4.12.1 Anahtar Saklama ve Yeniden Oluşturma İlke ve Esasları

Uygulama dışıdır.

4.12.2 Oturum Anahtarı Zarflama ve Yeniden Oluşturma İlke ve Esasları

Uygulama dışıdır.

5 TESİS, YÖNETİM VE İŞLETMEYLE İLGİLİ KONTROLLER

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

5.1 Fiziksel Kontroller

5.1.1 Tesis Yeri ve İnşaatı

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

5.1.2 Fiziksel Erişim

ArkSigner merkezinde bulunan NES Üretim Merkezindeki alanlara fiziksel erişim sürekli kontrol altında tutulmaktadır.

5.1.3 Güç Kaynakları ve Havalandırma

ArkSigner merkezinde kullanılan tüm donanım ve teçhizat için kesintisiz çalışacak güç kaynakları oluşturulmuştur. Özellikle bilgisayar donanımlarının yoğun bulunduğu bölgelerde, bu bölgelerin dışında kalan alanlarda ise ihtiyaca göre yeterli havalandırma kesintisiz olarak sağlanır.

5.1.4 Su Baskınları

ArkSigner merkezi, sel ve su baskınlarına karşı korunmuştur.

5.1.5 Yangın Önleme ve Yangından Korunma

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

5.1.6 Saklama Ortamları

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

5.1.7 Atıkların Atılması

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

fiziksel olarak imha edilir. Binanın ve ArkSigner birimlerinin diğer tüm atıkları uygun biçimde tesis dışına çıkarılır.

5.1.8 Tesis Dışı Yedekleme

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

5.2 Prosedürel Kontroller

5.2.1 Güvenilir Roller

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

- **Üst Düzey Yöneticiler:** ArkSigner sertifika hizmetlerinin yürütülmesinden teknik ve idari açıdan sorumlu üst düzey yöneticilerdir.

- **Müşteri Hizmetleri Sorumluları:** Müşteri hizmetleri, evrak kontrolü, sertifika başvuru kaydı, üretim, nitelikli elektronik sertifikaları askıya alma ve iptal gibi rutin sertifika hizmetlerinden sorumlu çalışanlardır.

- **Güvenlik Yetkilileri:** Güvenlik politikaları ve uygulamalarının yönetimi ve yürütülmesinden sorumlu çalışanlardır.

- **Sistem Yöneticileri:** Sertifika hizmetlerine ilişkin sistemlerin kurulumu, konfigürasyonu ve devamlılığının sağlanması ve aynı zamanda sistem yedekleme ve geri yükleme işlemleri için yetkilendirilmiş çalışanlardır.

- **Sistem Denetçileri:** Sertifika hizmetlerine ilişkin arşivlerin ve denetim kayıtlarının izlenmesi için yetkilendirilmiş çalışanlardır.

5.2.2 Her Görev İçin Gereken En Az Kişi Sayısı

ArkSigner'da sertifika süreçleri dâhilindeki kritik işlemlerin yapılabilmesi için çok kişi kontrollü bir sistem kurulmuştur.

ArkSigner kök ve alt kök sertifikalarıyla ilgili her türlü üretim, yenileme, iptal, imha ve yedekleme işlemi, ArkSigner kök, SİL ve son kullanıcı sertifikalarının anahtar çiftlerinin üretimi en az iki yetkilinin hazır bulunması ve onaylı görev talimatının ilgili yetkililere verilmiş olmasıyla yapılabilir.

5.2.3 Her Görev İçin Kimlik Doğrulama

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

5.2.4 Görevlerin Ayrılmasını Gerektiren Roller

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

5.3 Personel Kontrolleri

5.3.1 Nitelik, Deneyim ve Güvenlik Gereklilikleri

ArkSigner'da çalışan personel, sertifika süreçlerinin işleyişini doğru ve güvenilir bir şekilde

yürütebilecek nitelikte, göreve uygun eğitim düzeyine sahip (lise, üniversite, yüksek lisans vb.), konusunda bilgili ve eğitimli, benzer çalışma alanlarında deneyimlidir ve tüm güvenlik kontrollerinden geçmiştir.

5.3.2 Kişisel Geçmiş Kontrol Gereklilikleri

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

5.3.3 Eğitim Gereklilikleri

ArkSigner personeli göreve başlamadan önce sorumlulukları kapsamında eğitimden geçirilir. Eğitim süresince, çalışanlar temel sertifika iş süreçleri; müşteri hizmetleri, sertifika üretim merkezi işleyişiyle ilgili prosedürler ve talimatlar, bilgi güvenliği yönetim sistemi, kullanılacak yazılım ve donanım birimleri hakkında ayrıntılı olarak bilgilendirilir. Kayıt merkezlerindeki çalışanlar da görevlerinin gerektirdiği ölçüde eğitime tabi tutulurlar.

5.3.4 Tekrar Eğitim Sıklığı ve Gereklilikleri

Çalışanlara yönelik eğitim, göreve başlanırken verilen ilk eğitimin ardından periyodik olarak ve diğer gerekli görülen durumlarda tekrarlanır.

5.3.5 İş Rotasyonu Sıklığı ve Sırası

Kalıcı bir görevlendirme değişikliği olmadığı sürece, farklı çalışma alanları arasında rutin rotasyon yapılmaz.

5.3.6 Yetkisiz İşlemler için Yaptırımlar

ArkSigner personelinin teşebbüs edeceği yetkisiz işlemler için, ArkSigner insan kaynakları prosedürü uyarınca gerekli disiplin cezaları uygulanır. Eğer bu yetkisiz işlem sonucunda ArkSigner ya da ArkSigner müşterileri zarar görürse, bu zararın ilgili çalışandan tazmini yoluna gidilir. ArkSigner yetkisiz işlem yapanlar hakkında, Kanun, Yönetmelik ve Tebliğ gereğince işlem yapılmasını temin etmek üzere, adli mercilere başvuruda bulunur.

5.3.7 Bağımsız Alt Yüklenici Gereklilikleri

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

5.3.8 Personele Sağlanan Dokümantasyon

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

5.4 Denetim Kayıtları Alma Prosedürleri

5.4.1 Kaydedilen Olay Tipleri

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

kaydedilir.

5.4.2 Kayıtları İşleme Sıklığı

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

5.4.3 Denetim Kayıtlarının Saklanma Süresi

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

5.4.4 Denetim Kayıtlarının Korunması

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

5.4.5 Denetim Kayıtlarının Yedeklenme Prosedürleri

İlgili prosedürler uyarınca, kayıtların periyodik olarak yedekleri alınır.

5.4.6 Denetim Bilgisi (İç ve Dış) Toplama Sistemi

Denetim kayıtları, ArkSigner uygulamaları tarafından tutulur.

5.4.7 Olayı Yaratan Kişiyi Bilgilendirme

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

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

ArkSigner işleyişi uyarınca, Madde 5.4'te belirtilen tüm denetim kayıtları, sertifika süreçlerine yönelik başvuru, talep ve talimatlar, kağıt üzerinde alınan tüm destekleyici belgeler ile sertifika sahibi taahhütnamesi, müşterilerle yapılan tüm yazışmalar, üretilen tüm sertifikalar ve SİL'ler, NESİ ve NESUE kitapçıklarının tüm sürümleri, uygulama prosedürlerinin, talimatların ve formların bütünü arşivlenir. Arşivlerin büyük bir kısmı elektronik ortamda tutulurken, kâğıt üzerindeki yazışmalar, formlar, belgeler, müşteri dosyaları, şirket belgeleri gibi kayıtlar da kâğıt ortamında arşivlenir.

5.5.2 Arşivlerin Saklama Süresi

NES'lerle ilgili ArkSigner işleyişine ait arşivler, yasal düzenlemeler uyarınca en az 20 (yirmi) yıl süreyle saklanır.

5.5.3 Arşivlerin Korunması

Arşivler fiziksel ve elektronik güvenlik önlemleriyle korunur, sadece yetkili kişilerin erişimine açık tutulur.

5.5.4 Arşivlerin Yedeklenme Prosedürleri

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

5.5.5 Kayıtların Zaman Damgası Altına Alınması Gereklilikleri

ArkSigner elektronik arşiv kayıtları zaman bilgisiyle birlikte saklanır.

5.5.6 Arşiv Toplama Sistemi

Arşiv kayıtları, ArkSigner uygulamaları kullanılarak veya manuel olarak tutulur.

5.5.7 Arşiv Bilgisinin Edinilmesi ve Doğrulanması Prosedürleri

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

5.6 Anahtar Değişimi

ArkSigner kök ve alt kök sertifikalarının anahtar yenileme işlemleri ArkSigner sertifika merkezi tarafından yönetilir.

5.7 Güvenliğin Yitirilmesi ve Felaket Kurtarma

5.7.1 Güvenlik Kaybına Neden Olabilecek Olaylar

ArkSigner işleyişini engelleyecek nitelikte olayların ya da güvenlik sorunlarının oluşması durumunda, ArkSigner ihlal olayı yönetimi prosedürü ve iş sürekliliği prosedürü uyarınca duruma müdahale edilir.

5.7.2 Bilgisayar Kaynakları, Yazılım ve/veya Verilerin Bozulmuş Olması

Bilgisayar kaynaklarının zarar görmesi, yazılım birimlerinde veya işleyişe dair verilerde bozulma oluşması durumunda, öncelikle tesisteki hasarlı donanım yeniden işler hale getirilir. Daha sonra, kaybolan kayıtlar yedekleme sistemleri aracılığıyla yeniden oluşturulur ve sertifika hizmetleri tekrar etkin hale getirilir. Eğer tam olarak işler hale getirilemez veya kayıtların bazıları yeniden elde edilemez ise, bu durumdan etkilenebilecek olan bütün sertifika sahipleri ile üçüncü kişiler ivedilikle bilgilendirilir. Gerekli durumlarda bazı sertifikalar iptal edilip yeni sertifika üretimine geçilir.

5.7.3 İmza Oluşturma Verilerinin Güvenliğinin Yitirilmesi

ArkSigner imza oluşturma verilerinin güvenliğinin ve güvenilirliğinin yitirilmesi durumunda, 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

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

ArkSigner işleyişini engelleyecek nitelikte olayların ya da güvenlik sorunlarının oluşması durumunda, ArkSigner iş sürekliliği prosedürü uyarınca duruma müdahale edilir.

5.8 ArkSigner'ın Faaliyetinin Son Bulması

ArkSigner'ın faaliyetlerinin son bulması halinde, Kanun ve Yönetmelik gereği bu durumu en az 3 (üç) ay önce Kuruma bildirir ve kamuoyuna duyurur.

ArkSigner, mevcut sertifikalarla ilgili tüm bilgi, belge ve kayıtları, Kanun gereği 1 (bir) ay içinde başka bir ESHS'ye devreder. Kurum, uygun görmesi halinde, 1 (bir) ayı geçmemek üzere ek süre verebilir. Eğer devir işlemi belirtilen süreler içinde tamamlanamazsa, ArkSigner ilgili sertifikaları iptal eder ve tüm ilgili tarafları bu durumdan haberdar eder. Bu durumda, ArkSigner son SİL kaydını oluşturduktan sonra kendi imza oluşturma verisi ile yedeklerini imha eder.

6 TEKNİK GÜVENLİK KONTROLLERİ

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

6.1 Anahtar Çifti Üretimi ve Kurulumu

6.1.1 Anahtar Çifti üretimi

ArkSigner kök ve alt kök sertifikalarına ait anahtar çiftleri, sadece yetkili kişilerin kontrolünde, iki yetkilinin hazır bulunmasıyla, Bölüm 5.2.2'de belirtildiği gibi teknik ve idari güvenlik önlemleri alınmış ortamlarda üretilir ve uygun biçimde yedeklenir. İmza oluşturma verisi yetkisiz erişime karşı fiziksel ve teknik güvenlik önlemleriyle korunur. ArkSigner kök ve alt kök sertifikaları anahtar çifti üretiminde en az EAL4+ veya FIPS 140-2 Düzey 3 güvenlik düzeyinde kriptografik güvenlik donanım modülü kullanılır. Anahtar çiftlerinin uzunluğu ve kullanılacak algoritmalar güncel mevzuat ve standartlarla uyumlu olacak şekilde yapılır. Aynı şekilde üretilen anahtar çiftinin ömrü güncel mevzuat, standartlar ve anahtarların kriptografik güvenlik süresiyle sınırlandırılmıştır. Bir kök veya alt kök sertifikasının geçerlilik süresi sonundan yeterince makul bir süre önce yeni bir anahtar çifti ve sertifika üretilerek hizmetin kesintisiz bir biçimde devam etmesi sağlanır. ArkSigner donanım güvenlik modülleri, fiziksel ve elektronik her türlü müdahaleye karşı koruma altında tutulur ve çalıştırılır. Modüllerde bulunan verinin güvenli yedekleri alınır ve saklanır. Böylece fiziksel ve ekonomik ömrünü tamamlamış bir modülün içindeki anahtarlar Bölüm 6.2.10'da belirtildiği gibi yok edilir ve yeni modüllerde kullanılmak üzere gerekli yedekler başka ortamlarda saklanır. NES sahiplerinin imza oluşturma ve doğrulama verileri ArkSigner tarafından üretilir. Bu üretim işlemi için ArkSigner sertifika üretim merkezinde uygun güvenlik düzeyine sahip donanım güvenlik modüllerinde işlem gerçekleştirilir. Müşterilere ait imza oluşturma verileri hiçbir koşulda ArkSigner'da saklanmaz ve kopyası alınmaz.

6.1.2 İmza Oluşturma Verisinin Sertifika Sahibine Ulaştırılması

NES için anahtar çifti, en az 2 (iki) yetkilinin sisteme aynı anda şifreleri ve biyometrik verileriyle bağlanıp onay vermeleriyle ArkSigner merkezinde üretilir. Bu üretim işlemi sırasında oluşturulan anahtar çifti için erişim şifreleri rastgele sistem tarafından belirlenir.

Kişiler, ArkSigner NES satımında yetkili olduğu ArkSigner uygulamasında ilan edilen satış mağazalarından veya ArkSigner Yetkili ofisinden güvenli elektronik imza oluşturma aracını temin eder. Kimlik doğrulamanın yasal ve teknik gerekliliklere uygun olarak tamamlanmasından sonra imza oluşturma verisi güvenli elektronik imza oluşturma aracının içine yazılır. Güvenli elektronik imza oluşturma aracının erişim şifresi ise aktivasyon uygulamasıyla sertifika sahibi tarafından belirlenir.

6.1.3 İmza Doğrulama Verisinin ESHS'ye Ulaştırılması

İmza doğrulama verileri güvenli aktarım protokolleri kullanılarak ArkSigner veri tabanına kaydedilir.

6.1.4 ArkSigner İmza Doğrulama Verilerinin Üçüncü Kişilere Ulaştırılması

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

6.1.5 Anahtar Uzunlukları

ArkSigner sertifikaları, Tebliğ ile belirlenen minimum anahtar uzunluklarına uygundur. ArkSigner sertifika üretim merkezinin kök ve alt kök sertifikaları üretilirken 2048 bit ve üstü RSA veya 384 bit ve üstü ECDSA anahtar çiftleri kullanılır. ArkSigner tarafından üretilen tüm son kullanıcı sertifikaları için 2048 bit ve üstü RSA veya 384 bit ve üstü ECDSA anahtar çifti kullanılır. ArkSigner tarafından üretilen nitelikli elektronik sertifikalarda kullanılan özetleme algoritmaları hakkında bilgi, Bölüm 7.1.3'te verilmiştir.

6.1.6 Anahtar Üretimi ve Kalite Kontrolü

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

6.1.7 Anahtar Kullanım Amaçları

ArkSigner sertifika hizmetleri kapsamında üretilen son kullanıcı anahtarları, kimlik doğrulama ve elektronik imza amaçlı kullanılır. ArkSigner sertifika üretim merkezlerinin kök ve alt kök sertifikalarına ait anahtarlar, sertifika ve SİL imzalamak için kullanılır. ArkSigner OCSP hizmet sertifikalarına ait anahtarlar, OCSP sunucularına gelen sorgulara karşılık üretilen OCSP cevaplarını imzalamak için kullanılır. Anahtarların kullanım amacı, X.509 v3 sertifikaların anahtar kullanım alanlarında belirtilir.

6.2 İmza Oluşturma Verisinin Korunması ve Kriptografik Modül Mühendislik Kontrolleri

6.2.1 Kriptografik Modül Standartları ve Kontroller

ArkSigner'da anahtar çifti üretimi ile sertifika ve SİL imzalama işlemleri, Tebliğ ile 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. ArkSigner tarafından üretilen NES anahtar çifti, Tebliğ ile belirlenen standartlarda güvenlik düzeyine sahip akıllı kartlara, akıllı çubuklara ve benzeri güvenli elektronik imza oluşturma araçlarına yüklenir. Güvenli elektronik imza oluşturma araçlarındaki imza oluşturma verilerinin dışarıya çıkarılması, değiştirilmesi veya kopyalanması engellenmiştir.

6.2.2 İmza Oluşturma Verisinin Çok Kullanıcılı Kontrolü

ArkSigner sertifika üretim merkezinin kök ve alt kök imza oluşturma verilerine erişim, yetkili kişiler dışında yasaklanmıştır. Fiziksel ve teknik erişim kontrollerinin yanı sıra, bu imza oluşturma verilerinin kullanımı, ilgili modüle aynı anda iki ayrı yetkilinin bağlanması ve sistem tarafından onaylanmasıyla mümkündür. Sistem, hiçbir yetkilinin tek başına ArkSigner imza oluşturma verilerini kullanabilmesine izin vermez. NES imza oluşturma verileri sadece sertifika sahiplerinin kendi sorumluluğu altındaki, şifre kontrollü güvenli elektronik imza oluşturma araçlarında saklanır. Aracın şifresi bilinmediği sürece imza oluşturma verisi kullanılamaz. Şifre güvenliği araç donanımı tarafından sağlanır.

6.2.3 İmza Oluşturma Verisinin Saklanması

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

6.2.4 İmza Oluşturma Verisinin Yedeklenmesi

ArkSigner tarafından üretilen son kullanıcı sertifikalarına bağlı imza oluşturma verileri yedeklenmez, bu verilerin kopyası alınmaz. Herhangi bir afet durumu veya sorun anında hizmetlerin kesintiye uğramaması amacıyla, ArkSigner sertifika üretim merkezinin kök ve alt kök sertifikalarına bağlı imza oluşturma verileri yedeklenir ve fiziksel ve teknik güvenlik kontrolleri altında saklanır.

6.2.5 İmza Oluşturma Verisinin Arşivlenmesi

Uygulama dışıdır.

6.2.6 İmza Oluşturma Verisinin Kriptografik Modül Transferi

ESHS kök ve alt kök sertifikalarına ait imza oluşturma verileri güvenli kriptografik donanım modüllerinde üretilir. Bu veriler yedekleme amacıyla kullanılan güvenli modüllere transferi dışında

hiçbir biçimde modül dışına çıkarılamaz. Yedekleme işlemi, kriptografik donanım modülü üzerinde şifreli bir biçimde gerçekleştirilir. Anahtar üretimi ArkSigner'da uygun güvenlik düzeyine sahip güvenli kriptografik donanım modüllerinde gerçekleştirilir ve NES sahiplerinin güvenli elektronik imza oluşturma araçlarına güvenli yollarla taşınır.

6.2.7 İmza Oluşturma Verisinin Kriptografik Modülde Saklanması

ArkSigner sertifika üretim merkezinin kök ve alt kök sertifikalarına bağlı imza oluşturma verileri, üretildikleri ve Tebliğ'de tanımlı güvenlik düzeyine sahip kriptografik donanım modüllerinde saklanır. NES sahiplerinin imza oluşturma verileri Tebliğ'de tanımlı güvenlik düzeyine sahip güvenli elektronik imza oluşturma araçlarında saklanır. Güvenli elektronik imza oluşturma araçlarındaki imza oluşturma verisinin dışarıya çıkarılması, değiştirilmesi veya kopyalanması engellenmiştir.

6.2.8 Gizli Anahtarın Aktive Edilme Yöntemi

ArkSigner sertifika üretim merkezinin kök ve alt kök sertifikalarına bağlı imza oluşturma verileri, içinde bulundukları donanım güvenlik modülü üzerinde, iki yetkilinin hazır bulunmasıyla aktive edilir. NES'e bağlı imza oluşturma verileri, güvenli elektronik imza oluşturma aracı üzerinde şifre girişiyle aktive edilir. Sertifika sahibi aktivasyon verisinin diğer kişilerce izinsiz kullanımını, verinin çalınmasını veya kaybolmasını önlemek üzere gerekli tedbirleri almaktan sorumludur.

6.2.9 Gizli Anahtarın Deaktive Edilme Yöntemi

ArkSigner sertifika üretim merkezinin kök ve alt kök sertifikalarına bağlı imza oluşturma verileri, içinde bulundukları donanım güvenlik modülü üzerinde sadece belirli bir süreyle ve işlem bazlı aktive edilir, işlem tamamlandıktan ya da işlem süresi bittikten sonra deaktive olur. İmza oluşturma verisinin yeniden kullanılabilmesi için, yetkililerin tekrar sisteme tanıtılarak imza oluşturma verisinin aktive edilmesi gerekir. NES'e bağlı imza oluşturma verileri güvenli elektronik imza oluşturma aracı üzerinde şifre girişiyle belirli bir süre için aktive edilir ve işlem süresi sonunda deaktive olur. Ayrıca, sertifika sahibi kendi isteğiyle de imza oluşturma verisini deaktive edebilir. İmza oluşturma verisinin yeniden kullanılabilmesi için, sertifika sahibinin güvenli elektronik imza oluşturma aracı şifresini tekrar girmesi gerekir.

6.2.10 Gizli Anahtarı Yok Etme Metodu

ArkSigner sertifika üretim merkezinin kök ve alt kök sertifikalarına bağlı imza oluşturma verilerinin tüm kopyaları, sertifika geçerlilik süreleri sonunda, içinde bulundukları donanım güvenlik modüllerinin anahtar silme özelliği kullanılarak sadece yetkili kişiler tarafından yok edilir ve yapılan işlemler prosedürler uyarınca kayıt altına alınır. Bu işlem için en az iki kişinin aynı anda hazır bulunması gerekir.

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

6.2.11 Kriptografik Modül Değerlendirmesi

ArkSigner sertifika üretim merkezinin kök ve alt kök sertifikalarına bağlı imza oluşturma verileri, Tebliğ'de tanımlı güvenlik düzeyine sahip kriptografik donanım modüllerinde üretilir ve saklanır. NES sahiplerinin imza oluşturma verileri Tebliğ'de tanımlı güvenlik düzeyine sahip güvenli elektronik imza oluşturma araçlarında saklanır.

6.3 Anahtar Çifti Yönetimiyle İlgili Diğer Konular

6.3.1 İmza Doğrulama Verilerinin Arşivlenmesi

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

6.3.2 Sertifikanın İşlevsel Süreleri ve Anahtar Çifti Kullanım Süreleri

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

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

6.4 Erişim Şifreleri

6.4.1 Erişim Şifrelerinin Oluşturulması ve Kurulumu

Erişim şifresi, gizli anahtar yönetiminde kullanılan parola, şifre, PIN ya da benzeri özel verilere karşılık gelir. ArkSigner alt kök ve kök sertifikalarına ait anahtarların üretimi ve bu anahtarlara ait erişim şifrelerinin oluşturulması Bölüm 6.2.2'de açıklandığı gibi iki yetkilinin aynı anda bulunmasıyla mümkündür.

NES imza oluşturma verilerine ait erişim şifreleri sertifika sahipleri tarafından aktivasyon yöntemi ile belirlenir. Aktivasyon yönteminde, sertifika üretim aşamasında bir erişim şifresi üretilir. Aynı işlem sırasında sertifika ve sertifikanın yazıldığı karta bağlı aktivasyon kodu da üretilir ve şifrelenerek veri tabanına kaydedilir.

Aktivasyon kodunun üretilme yöntemi, sertifika ve akıllı kart ile bir araya geldiğinde erişim şifresini yeniden oluşturacak biçimde tasarlanmıştır. NES'in gizli anahtarı sadece sertifika sahibi tarafından oluşturulan PIN şifresi aracılığıyla kullanılır.

6.4.2 Erişim Şifrelerinin Korunması

ArkSigner kök ve alt kök sertifikalarına ait gizli anahtarları kullanan yetkili kişiler, erişim şifrelerini belirli periyotlarda değiştirirler. Yetkili kişiler, erişim şifrelerinin gizliliğinden ve korunmasından sorumludur.

6.4.3 Erişim Şifreleriyle İlgili Diğer Konular

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

6.5 Bilgisayar Güvenlik Kontrolleri

6.5.1 Bilgisayar Güvenliği Teknik Gereklilikleri

ArkSigner 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, ArkSigner 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.

- ArkSigner, değişikliklere karşı korunmuş güvenilir sistemler ve ürünler kullanır. Bu bağlamda, Bilgi Teknolojileri ve İletişim Kurumu'nun sürekli denetimi altında, CWA 14167-1 standardının önerileri kesin olarak uygulanır.

6.5.2 Bilgisayar Güvenliğinin Derecelendirilmesi

Uygulama dışıdır.

6.6 Yaşam Döngüsü Teknik Kontrolleri

6.6.1 Sistem Geliştirme Kontrolleri

Sistem geliştirme kontrolleri, kalite yönetimi prosedürleri ve ISO/IEC 27001 denetimleri sonucunda ortaya çıkan risk azaltma metotları uyarınca gerçekleştirilir.

6.6.2 Güvenlik Yöntemi Kontrolleri

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

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

6.6.3 Yaşam Döngüsü Güvenlik Kontrolleri

Uygulama dışıdır.

6.7 Ağ Güvenlik Kontrolleri

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

ArkSigner içindeki diğer tüm sistemler de uygun ağ güvenliği yöntemleriyle korunmaktadır.

6.8 Zaman Damgası

ArkSigner tarafından sertifika hizmetlerinin yürütülmesi sırasında ilgili işlemlere ait elektronik kayıtlar, zaman damgası hizmetlerinde kullanılan zaman kaynağı ile senkronize edilmiş zaman bilgisini içerir. Kayıt bütünlüğü anahtarlanmış özet yöntemi kullanılarak korunur ve arşivleme aşamasında zaman damgası kullanılır.

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

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

7.1 Sertifika Profili

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

ArkSigner sertifikalarında temel olarak aşağıdaki alanlar bulunur:

Alan Adı	Açıklama
Seri No	(Aynı sertifika veren için) Eşsiz numara
İmza Algoritması	Nesne tanımlayıcı numarası (Bkz. 7.1.3)
Sertifikayı Veren	Bkz. 7.1.4
Geçerlilik Başlangıcı	RFC 5280'e göre kodlanmış UTC zamanı
Geçerlilik Sonu	RFC 5280'e göre kodlanmış UTC zamanı
Özne	Bkz. 7.1.4
Açık Anahtar	RFC 5280'e göre kodlanmış anahtar değeri
İmza	RFC 5280'e göre kodlanmış imza değeri

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

7.1.1 Sürüm Numaraları

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

7.1.2 Sertifika Uzantıları

ArkSigner, RFC 3280 - X.509 v3 standardı uyarınca tanımlanmış olan tüm sertifika uzantılarını destekler. Sertifikanın çeşidine göre, yetkili anahtar tanımlayıcısı (authority key identifier), özne anahtar tanımlayıcısı (subject key identifier), anahtar kullanımı (key usage), sertifika ilkeleri (certificate policies), temel kısıtlar (basic constraints), özne alternatif adı (subject alternative name), SİL dağıtım noktaları (CRL distribution points), genişletilmiş anahtar kullanımı (extended key usage) uzantıları uygun biçimde ayarlanır. NES'ler, "IETF RFC 3039 Internet X.509 Public Key Infrastructure Qualified Certificates Profile" ve "Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri" dokümanları uyarınca tanımlanan nitelikli elektronik sertifika uzantılarını içerir.

7.1.3 Algoritma Nesne Tanımlayıcıları

ArkSigner tarafından oluşturulan tüm sertifikaların imzalanmasında aşağıdaki algoritmalardan biri kullanılır.

Algoritma Adı	Nesne Tanımlayıcı Numarası
SHA 256 ile RSA	1.2.840.113549.1.1.11
SHA 384 ile RSA	1.2.840.113549.1.1.12
SHA 512 ile RSA	1.2.840.113549.1.1.13
SHA 256 ile ECDSA	1.2.840.10045.4.3.2
SHA 384 ile ECDSA	1.2.840.10045.4.3.3
SHA 512 ile ECDSA	1.2.840.10045.4.3.4

NES için ilgili algoritmalar yasal düzenlemelerin gerektirdiği şekilde kullanılmaktadır.

7.1.4 İsim Biçimleri

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

7.1.5 İsim Kısıtları

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

7.1.6 Sertifika İlkeleri Nesne Tanımlayıcısı

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

7.1.7 İlke Kısıtları Uzantısının Kullanımı

ArkSigner alt kök sertifikalarında ihtiyaca göre ilke kısıtları uzantısı kullanabilir.

7.1.8 İlke Niteleyicilerinin Yazımı

ArkSigner 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

Uygulama dışıdır.

7.2 SİL Profili

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

7.2.1 Sürüm Numarası

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

7.2.2 SİL ve SİL Giriş Uzantıları

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

7.3 OCSP Profili

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

7.3.1 Sürüm Numarası

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

7.3.2 OSCP Uzantıları

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

8 UYGUNLUK DENETİMİ VE DİĞER DEĞERLENDİRMELER

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

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

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

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

8.1 Denetim Sıklığı ve Durumları

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

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

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

8.2 Denetçinin Kimliği ve Özellikleri

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

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

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

8.3 Denetçinin ESHS'yle İlişkisi

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

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

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

8.4 Denetimde Kapsanan Başlıklar

Bilgi Teknolojileri ve İletişim Kurumu'nun denetimi Kanunla kendisine verilen yetki çerçevesinde, ArkSigner'ın elektronik sertifika hizmetlerine dair tüm süreçleri, bu hizmetlerin yerine getirilmesi sırasında kullanılan teknik altyapı ve hizmetlerin verildiği tesisleri kapsar.

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi ve TS EN ISO 9001 Kalite Yönetim Sistemi sertifikasyonları, ESHS faaliyetleri ile Yazılım Geliştirme ve Bakım süreçleri altında ArkSigner elektronik sertifika ve zaman damgası hizmetleri kapsamındadır.

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

8.5 Eksiklik Durumunda Yapılacaklar

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

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

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

8.6 Sonuçların Bildirilmesi

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

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

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

9 DİĞER İŞ KONULARI VE YASAL KONULAR

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

9.1 Ücretler

9.1.1 Sertifika Üretim ve Yenileme Ücretleri

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

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

9.1.2 Sertifika Erişim Ücretleri

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

Sertifika erişim hizmetleri için ücret talep edilmez.

9.1.3 İptal veya Durum Bilgisi Erişim Ücretleri

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

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

9.1.4 Diğer Hizmetlerin Ücretleri

ArkSigner, kamuya açık olarak yayımladığı belgeler için ücret talep etmez.

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

9.1.5 Bedel İadesi

ArkSigner, NES hizmetlerinde bedel iadesi yapmaz. Ancak, ArkSigner'dan kaynaklanan nedenlerle, sertifika içeriğinde başvurudan farklı verilerin bulunması durumunda, herhangi bir ücret talep edilmeden yeni bir sertifika verilir veya talep edilmesi durumunda bedel iadesi yapılır.

9.2 Finansal Sorumluluk

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

9.2.1 Sigorta Kapsamı

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

9.2.2 Diğer Varlıklar

Uygulama dışıdır.

9.2.3 Son Kullanıcılar için Sigorta veya Garanti Kapsamı

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

9.3 İş Bilgisinin Gizliliği

9.3.1 Gizli Bilginin Kapsamı

ArkSigner'ın elektronik sertifika hizmet sağlayıcılığı işlevleriyle ilgili her türlü ticari gizli bilgi ve belge, teknik ve operasyonel anlamda işlemlerine ilişkin bilgi güvenliği kapsamında gizli sayılan tüm bilgi ve belgeler, ArkSigner sertifika üretim merkezinin kök ve alt kök sertifikalarının imza oluşturma verileri, kullanılan yazılım ve donanım bilgileri, işlem kayıtları, erişim şifreleri, "NES" sahiplerinin "Kanun" kapsamında "kişisel veri" sayılan bilgileri, denetim ve değerlendirme kayıtları, tesis planı ve iç tasarımı, acil eylem planları, iş planları, satış bilgileri, işbirliği sözleşmeleri, iş ortaklığı yapılan kuruluşlara ait gizlilik dereceli bilgiler, gizli bilgi kapsamına girer.

9.3.2 Gizlilik Kapsamı Dışındaki Bilgi

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

9.3.3 Gizli Bilginin Korunması Sorumluluğu

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

9.4 Kişisel Bilgilerin Gizliliği/Özelliği

9.4.1 Gizlilik Planı

ArkSigner, verdiği sertifika hizmetleri kapsamında, personeline, sertifika başvuru sahiplerine, sertifika sahibi müşterilerine ya da diğer katılımcılara ait kişisel verilerin veya özel nitelikli kişisel verilerin gizliliğini sağlar ve kişiye özel olma durumunu 6698 sayılı Kişisel Verilerin Korunması Kanunu uyarınca korur.

9.4.2 Özel Olarak Değerlendirilecek Bilgi

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

9.4.3 Özel Sayılmayacak Bilgi

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

9.4.4 Özel Bilgiyi Koruma Sorumluluğu

ArkSigner çalışanlarının tamamı, başvuru sahiplerine ve müşterilere ait kişisel veya özel nitelikli kişisel verilerin korunması konusunda sorumluluk sahibidir. Hiçbir veriye, yetkilisi dışındaki çalışanların ya da üçüncü kişilerin erişimine izin verilmez.

9.4.5 Özel Bilgiyi Kullanma Bildirimi ve Onayı

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

9.4.6 Yargısal ve İdari Süreçlere Uygun Olarak Bilginin Açıklanması

Hukuki süreçler gereği, ihtiyaç duyulan nitelikli elektronik sertifika sahibinin özel bilgileri, sadece talep sahibi resmi makama veya sertifika sahibinin kendisine verilir. Ayrıca, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 11. maddesi uyarınca kişiler yazılı olarak ArkSigner'a başvurarak kişisel verileriyle ilgili bilgi ve işlemleri talep edebilirler. Yasal düzenleme çerçevesinde başvuru sahibine 30 (otuz) gün içinde e-posta veya yazılı olarak ArkSigner tarafından bilgi verilir.

9.4.7 Bilginin Açıklandığı Diğer Durumlar

Uygulama dışıdır.

9.5 Fikri Mülkiyet Hakları

ArkSigner tarafından üretilen sertifikalar, SİL'ler, sertifika hizmetleriyle ilgili kullanıcı sözleşmeleri, NESİ ve NESUE kitapçıkları, sertifika hizmetlerinin yürütülmesiyle ilgili her türlü iç ve dış doküman, veri tabanları, web siteleri ile sertifika hizmetlerine bağlı olarak geliştirilen tüm ürünlerin fikri mülkiyet hakları ArkSigner'a aittir.

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

9.6 Sorumluluklar

9.6.1 ESHS Beyan ve Garantileri

ArkSigner'a bağlı sertifika üretim merkezleri, üretilen nitelikli elektronik sertifikaların içeriğinin doğru olduğunu, kimlik doğrulama adımlarının doğru ve güvenilir biçimde yürütüldüğünü, doğru sertifikanın doğru başvuru sahibi adına üretildiğini ve doğru kişiye teslim edildiğini, yayımlanan sertifika durum bilgilerinin güncelliğini ve doğruluğunu; NESİ ve NESUE'de yer alan tüm uygulama gereklilikleri ve yükümlülüklerini yerine getireceğini garanti eder.

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

9.6.2 Kayıt Merkezi Sorumlulukları

ArkSigner kayıt merkezi sorumluları, kendilerine başvuran gerçek veya tüzel kişilerin sertifika tiplerine göre işbu NESİ dokümanında belirtilen kimlik doğrulama adımlarının doğru ve güvenilir biçimde yürütüldüğünü, kayıtların doğru biçimde tutulduğunu, ESHS merkezine gönderilen sertifika üretim, yenileme ve iptal taleplerinin doğru ve eksiksiz olduğunu garanti eder.

9.6.3 Sertifika Sahibi Sorumlulukları

Nitelikli elektronik sertifika sahipleri, sertifika başvurusu ile yenileme ve iptal talepleri sırasında ArkSigner'a güncel ve doğru bilgi ve belgeler sunmayı, sertifikalarını NESİ ve NESUE kitapçıklarında yer

alan koşullar uyarınca kullanmayı, nitelikli elektronik sertifika başvuru ve taahhütnamesinde yer alan tüm yükümlülüklerini yerine getireceğini garanti eder.

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

9.6.4 Üçüncü Kişilerin Sorumlulukları

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

9.6.5 Diğer Katılımcıların Sorumlulukları

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

9.7 Sorumlulukların Geçersiz Olduğu Durumlar

Uygulama dışıdır.

9.8 Sorumluluk Sınırları

ArkSigner tarafından verilen nitelikli elektronik sertifikalar, parasal işlemlerde maddi işlem sınırları dahilinde sigortalıdır. Sertifikalar ve bu sertifikaların kullanımıyla ilgili sorumluluk sınırları, nitelikli elektronik sertifika başvuru ve taahhütnamesinde açıkça belirtilmiştir. NES'ler için zorunlu sertifika mali sorumluluk sigortası, 10.000 TL tutarında olay başına teminat limitini ve 1.000.000 TL tutarında yıllık azami teminat limitini kapsar.

9.9 Tazminatlar

ArkSigner, bu NESİ ve NESUE'de yer alan ilke ve esaslar gereği yükümlülüklerini yerine getiremez ve bu durumdan üçüncü kişiler zarar görürse ilgili zarar, ArkSigner tarafından tazmin edilir.

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

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

9.10 NESİ Dokümanının Geçerliliği

9.10.1 NESİ Dokümanının Geçerlilik Dönemi

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

9.10.2 NESİ dokümanının Geçerliliğinin Sona Ermesi

ArkSigner 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 ArkSigner tarafından hazırlanır ve yayımlanır.

9.10.3 Geçerliliğin Sona Ermesinin Etkileri ve İşlerliğin Sürdürülmesi

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

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

9.11 Taraflara Özel Duyurular ve İletişim

ArkSigner tarafından sertifika sahiplerine yapılacak olan kişisel duyurular için sertifika sahiplerinin uygun olan iletişim bilgileri kullanılır.

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

9.12 Değişiklikler

ArkSigner 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 ArkSigner tarafından hazırlanır ve ArkSigner Yönetim Kurulu'nun onayının ardından yayımlanır.

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

9.12.1 Değişiklik Prosedürü

ArkSigner 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 ArkSigner 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. ArkSigner 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

ArkSigner 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, ArkSigner sertifika sahipleri ile üçüncü kişileri bilgilendirebilmek için tüm makul imkanları kullanır.

Küçük değişikliklerde ise web sitesi aracılığıyla durum ilan edilir.

Yeni NESİ ve NESUE sürümleri, eski sürümlerle birlikte ArkSigner bilgi deposunda, ayrıntılı sürüm bilgisi içerecek şekilde yayımlanır ve ilgili tarafların erişimine açık tutulur.

9.12.3 Nesne Tanımlayıcı Numaralarının Değişmesini Gerektiren Durumlar

Nitelikli elektronik sertifika kullanımını ve kabul edilirliğini doğrudan etkileyebilecek olan, kullanılan kimlik doğrulama adımlarını önemli ölçüde etkileyen veya sertifika hizmetlerinde sertifikanın güvenlik düzeyine etki edebilecek biçimde gerçekleşen önemli değişiklikler, 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

ArkSigner, 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 ArkSigner 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

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

9.16 Çeşitli Hükümler

9.16.1 Bütün Anlaşma

Uygulama dışıdır.

9.16.2 Görevlendirme

Uygulama dışıdır.

9.16.3 Kitapçık Kısımlarının Ayrılabilirliği

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

9.16.4 Yasal Haklardan Vazgeçme

Uygulama dışıdır.

9.16.5 Mücbir Sebepler

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

9.17 Diğer Hükümler

Uygulama dışıdır.