AYYILDIZ

İMZA BİLGİ GÜVENLİĞİ A.Ş

Sürüm-1

Nitelikli Elektronik Sertifika Uygulama Esasları

(NESUE)

3 Haziran 2021

OID:2.16.792.3.0.60.1.2.1

www.ayyildizimza.com.tr

İçindekiler

1. GİRİŞ

AYYILDIZ İMZA BİLGİ GÜVENLİĞİ VE TEKNOLOJİLERİ A.Ş (bundan sonra "AYYILDIZİMZA" olarak anılacaktır). 25355 Sayılı ve 23 Temmuz 2004 tarihli Resmî gazete yayımlanarak yürürlüğe girmiş olan 15 Ocak 2004 tarih ve 5070 Sayılı "Elektronik İmza Kanunu (bundan sonra "Kanun" olarak anılacaktır) ve Bilgi Teknolojileri ve İletişim Kurumu tarafından yayımlanmış olan ikincil mevzuat uyarınca, elektronik hizmet sağlayıcılığı (Bundan sonra "ESHS" olarak anılacaktır) alanında faaliyet göstermektedir.

Bu Doküman, Kanun kapsamından yayınlanmış olan "Elektronik İmza ile İlgili Süreçlerde ve Teknik Kriterlerde İlişkin Tebliğ" uyarınca AYYILDIZİMZA 'nın Nitelikli Elektronik Sertifika hizmetini yürütürken uyguladığı esasları içeren Sertifika Uygulama Esasları Dokümanıdır. (Bundan sonra NESUE olarak anılacaktır).

Bu Doküman (NESUE), nitelikli elektronik sertifika başvurularının alınması, üretimi ve yönetimi, sertifika yenileme, sertifika iptal edilmesi ve ilgili işlemlerde idari, teknik ve yasal gereklilikleri yerine getirmesi sırasında uygulanan esasları açıklayarak, AYYILDIZİMZA 'nın, sertifika sahibinin ve üçüncü kişilerin uygulama sorumluluklarını belirtir.

1.1. Genel Bakış

Bu doküman (NESUE), AYYILDIZİMZA 'nın Nitelikli Elektronik Sertifika Uygulama Esaslarını açıklamaktadır. Bu esaslar, AYYILDIZİMZA 'nın müşteri hizmetleri, kayıt birimleri ve üretim merkezleri gibi tüm ünitelerindeki yönetim sürecinin Nitelikli Elektronik Sertifika İlkeleri (Bundan sonra NESİ olarak anılacaktır) dokümanın da belirtilen ilkelerin "***nasıl***" uygulandığıdır.

Bu doküman (NESUE) da yer alan uygulama esasları Kanun kapsamında yayınlanmış olan "Elektronik İmza ile İlgili Süreçlerde ve Teknik Kriterlerde İlişkin Tebliğ" in 7. Maddesinde işaret edilen IETF RFC 3647'ye uygun olarak hazırlanmıştır.

1.2. Kitapçık Adı ve Tanımlama

Bu doküman, AYYILDIZİMZA Nitelikli Elektronik Sertifika Uygulama Esaslarını kapsamaktadır. Kitapçık sürüm bilgileri ve yayımlanma tarihi kapakta yer almaktadır.

AYYILDIZİMZA, bu NESUE dokümanı gereğince elektronik sertifika faaliyetlerine yönelik ilkeleri tanımlayan kuruluş olarak, Türk Standartları Enstitüsü 'nden (TSE) "2.16.792.3.0.60" kurumsal nesne tanımlayıcı tepe OID numarasını almıştır. AYYILDIZİMZA tepe OID numarasına bağlı olarak

- Nitelikli Elektronik Sertifika Uygulama Esasları: 2.16.792.3.0.60.1.2.1 numarasını atayarak TSE 'ye bildirmiştir.

NESUE dokümanı http://ayyildizimza.com.tr/bilgidepo adresinde herkesin erişimine açık olarak yayımlanmaktadır.

1.3. Taraflar

NESUE de yer alan taraflar, AYYILDIZİMZA' nın ESHS olarak üzerinden hizmet sağladığı birimler ve bu hizmeti alan müşteri, sertifika sahipleri ve kullanıcılarını kapsar.

1.3.1. Elektronik sertifika Hizmet Sağlayıcı

AYYILDIZİMZA, NESİ de ilke ve kurallarını duyurduğu Nitelikli Elektronik Sertifika Hizmetini sağlayıcısıdır. "Kanun" da belirtilen yükümlülüklerini yerine getirir.

- Sertifika başvurusunun alınması,
- Sertifika üretiminin yapılması,
- Sertifika yenilenmesinin yapılması,
- Sertifika askı-iptal sürecinin yönetilmesi,
- Kesintisiz olarak SİL (Sertifika İptal Listesi) hizmetinin verilmesi,
- Kesintisiz olarak ÇİSDUP (Çevrim İçi Durum Protokolü) hizmetinin verilmesi,
- Kesintisiz olarak Sertifika Deposu hizmetinin verilmesi,
- Ve İlgili Açık Anahtar Altyapısı Operasyonlarını yürütür.

1.3.2. Sertifika Kayıt Birimleri

AYYILDIZİMZA bünyesinde bulunan Sertifika Kayıt Birimleri, nitelikli elektronik sertifika başvuru taleplerini alma ve sertifika teslimatlarını yapmakla yetkilidir. Bu birimler, müşteri kayıtlarını oluşturur, gerekli kimlik tanıma ve doğrulama süreçlerini yürütür.

ESHS kendi bünyesi ve fiziksel ortamı içinde kayıt birimleri bulundurduğu gibi kayıt birimi hizmetini kendi fiziksel ortamından uzakta da kurabilir.

1.3.3. Sertifika Sahipleri

Sertifika sahipleri adına nitelikli elektronik sertifika üretilen ve sertifikasını AYYILDIZİMZA NESİ ve NESUE'ye uygun olarak kullanmakla yükümlü olan gerçek kişilerdir.

Bu doğrulamalar ilgili mevzuat ve standarda uygun olarak yapılır.

1.3.4. Üçüncü Kişiler

Üçüncü kişiler, sertifikaların içindeki kimlik ve imza doğrulama verisi arasındaki bağın doğruluğuna güvenerek sertifikaları kabul eden ve işlem yapan taraflardır.

1.3.5. Diğer Katılımcılar

Diğer Katılımcılar, AYYILDIZİMZA 'nın faaliyet sürecinde iş birliği yaptığı ve hizmet aldığı tüm gerçek ve tüzel kişileri kapsar. Bu katılımcılar, verecekleri hizmeti güvenilir ve doğru biçimde olduğunu, ayrıca bu süreçlerde yer alan müşteriler ile ilgili özel ve gizli bilgilerin korunmasını garanti altına almak için "NESUE" e göre hazırlanmış sözleşmeler imzalar.

1.4. Sertifika Kullanımı

1.4.1. Geçerli Sertifika Kullanım Şekilleri

AYYILDIZİMZA Kök ve Alt Kök sertifikaları yalnızca;

- NES (Nitelikli Elektronik Sertifika) sertifikalar,
- SİL (Sertifika İptal Listesi),
- ÇİSDUP (Çevrimiçi Durum Protokolü) sertifikaları,
- Zaman Damgası sertifikası,
- Sertifika zincirindeki diğer sertifikalardır.

İmzalanması ve Doğrulanması için kullanılır. AYYILDIZİMZA Kök Sertifikası, kendi imza oluşturma verisi ile imzalanmış en üst düzey sertifikadır. Çevrim dışı olarak tutulur, sadece Alt Kök sertifikaları veya kendi SİL listesini imzalamak için çevrim içi yapılır. İşlem tamamlandıktan sonra derhal tekrar çevrim dışına çekilir.

AYYILDIZİMZA Nitelikli Elektronik Alt Kök sertifikası da AYYILDIZİMZA kök sertifikası tarafından imzalanmıştır. Nitelikli Elektronik Sertifika başvurusu kabul edilen gerçek kişilerin sertifikalarını imzalamak için kullanılır.

AYYILDIZİMZA tarafından üretilen Nitelikli Elektronik İmza oluşturma verileri, elektronik imzaya ilişkin mevzuatta tanımı yapıldığı şekilde sertifika sahibi tarafından, güvenli elektronik imza oluşturma aracıyla birlikte, güvenli elektronik imza oluşturmak için kullanılır. Oluşturulan bu imza "Kanun" a göre ıslak imzanın karşılığıdır.

Nitelikli Elektronik Sertifika içerisinde yer alan doğrulama verileri, üretilen güvenli elektronik imzayı doğrulamak için kullanılır.

1.4.2. Yasaklanmış Sertifika Kullanım Şekilleri

AYYILDIZİMZA Kök ve Alt Kök sertifikaları 1.4.1 de detayları belirtilen amaçları dışında kullanılamaz. AYYILDIZİMZA tarafından üretilen Nitelikli Elektronik Sertifikalar mevzuatta belirlenen şartlar dışında kullanılamaz.

1.5. Sertifika Uygulama Esasları Yönetimi

İş bu, NESUE dokümanı yönetiminden AYYILDIZİMZA sorumludur.

1.5.1. NESUE Dokümanından Sorumlu Organizasyon

Bu dokümanın değiştirilmesi, yayınlanması ve uygunluğundan **AYYILDIZİMZA Bilgi Güvenliği Kurulu** sorumludur.

1.5.2. İletişim Noktası

NESUE dokümanı ile ilgili İletişim bilgileri aşağıda yer almaktadır.

AYYILDIZ İMZA BİLGİ GÜVENLİĞİ VE TEKNOLOJİLERİ A.Ş

Adres:	Göktürk Merkez, Menekşe Sok. No:18, 34077 Eyüpsultan/İSTANBUL
Telefon:	(0212) 322 43 33
Faks:	(0212) 322 43 33
Çağrı Merkezi:	(0212) 322 43 33
E-Posta:	bilgi@ayyildizimza.com.tr
Web:	www.ayyildizimza.com.tr

1.5.3. NESUE'nin İlkelere Uygunluğunu Belirleyen Yetkili

İşbu, NESUE dokümanının uygunluğu ve uygulanabilirliği **AYYILDIZİMZA Bilgi Güvenliği Kurulu** tarafından belirlenir.

1.5.4. NESUE Onaylama Prosedürleri

NESİ ve NESUE Dokümanı AYYILDIZİMZA Bilgi Güvenliği Kurulu tarafından düzenli olarak takip edilerek uygunluğu ve uygulanabilirliği kontrol edilir. AYYILDIZİMZA Sertifika İlkeleri Yönetim Ekibi, bağımsız denetim kuruluşlarının denetim sonuçlarını değerlendirerek, NESİ ve NESUE 'nin uygunluğunu

kontrol etmek ile sorumludur. Herhangi bir değişiklik yapıldığında, bu değişikliğin yeni bir OID 'ye gerek duyup duymadığına karar verir.

1.6. Kısaltmalar ve Tanımlar

1.6.1. Kısaltmalar

BTK:	Bilgi Teknolojileri ve İletişim Kurumu
BGYS:	Bilgi Güvenliği Yönetim Sistemi
ESHS:	Elektronik Sertifika Hizmet Sağlayıcısı
ÇİSDUP	Çevrim İçi Sertifika Durum Protokolü
OCSP	Online Certificate Status Protocol (Bkz. "ÇİSDUP")
EAL:	Evaluation Assurance Level-Değerlendirme Garanti Düzeyi
CEN:	Comité Européen de Normalisation-Avrupa Standardizasyon Komitesi
CRL:	Certificate Revocation List (Bkz. "SİL")
CSR:	Certificate Signing Request – Sertifika İmzalama Talebi
FIPS PUB:	Federal Information Processing Standards Publications-Federal Bilgi İşleme Standartları Yayınları
ISO/IEC:	International Organisation for Standardisation / International Electrotechnical Commitee- Uluslararası Standardizasyon Teşkilatı / Uluslararası Elektroteknik Komitesi
ITU:	International Telecommunication Union-Uluslararası Telekomünikasyon Birliği
KEP:	Kayıtlı Elektronik Posta
KPS:	Kimlik Paylaşım Sistemi
PKI:	Public Key Infrastructure(Bkz. AAA)
AAA:	Açık Anahtar Altyapısı
Sİ:	Sertifika İlkeleri
SİL:	Sertifika İptal Listesi
CWA:	CEN Workshop Agreement- CEN Çalıştay Kararı
FKM:	Felaket Kurtarma Merkezi
KB:	Kayıt Birimi

IETF:	Internet Engineering Task Force-İnternet Mühendisliği Görev Grubu
DN:	Distinguished Name – Ayırt Edici İsim
NES:	Nitelikli Elektronik Sertifika
NESİ:	Nitelikli Elektronik Sertifika İlkeleri
SUE:	Sertifika Uygulama Esasları
NESUE:	Nitelikli Elektronik Sertifika Uygulama Esasları
CN:	Common Name-Sertifika Sahibi Adı ve Soyadı
L:	Location
C:	Country
O:	Organisation – Kurum Adı
OID:	Object Identifier – Nesne Tanımlayıcı Numarası
OU:	Organizational Unit – Kurumsal Birim
RFC:	IETF tarafından yayımlanan, kılavuz niteliğinde yorum talebi dokümanları
TCKN:	T.C. Kimlik Numarası
TSE:	Türk Standartları Enstitüsü

1.6.2. Tanımlar

Açık Anahtar:	AAA mimarisinde, birbirleri ile asimetrik anahtarlara anahtar çifti denir. Bu anahtar çiftinde diğer kişilerin de bilgisine açık olan kriptografik anahtar açık anahtardır. Kanun da imza doğrulama verisi olarak isimlendirilmiştir.
Açık Anahtar Altyapı:	Asimetrik anahtar çiftlerini kullanarak, kimlik doğrulama, inkâr edilemezlik, mesaj bütünlüğü ve gizlilik gibi hizmetleri simetrik kriptografi ile anahtar dağıtımı ve sayısal imza özellikleri asimetrik kriptografi'nin kullandığı yöntemler ile sunan alt yapı sistemidir.
Aktivasyon:	NES sahiplerinin gerekli doğrulama adımlarını geçerek imza oluşturma verisine, erişim şifresini sadece kendisinin belirlemesini sağlayarak sertifikasını kullanıma hazır hale getirdiği online işlemdir.
Alt Kök Sertifikası:	ESHS'nin AAA mimarisine uygun olarak, sertifika zincirinde son kullanıcı sertifikalarını imzalayacak olan ve kendisi de ESHS'nin kök sertifikası tarafından imzalanan sertifikadır.
Kök Sertifika:	ESHS 'nin AAA mimarisinde uygun olarak kendini ve sertifika zincirindeki bir alt kademesinde yer alan sertifikaları imzalayan, ESHS Kurumsal kimlik bilgilerini, ESHS imza doğrulama verisine bağlayan, sertifika zincirindeki tüm sertifikaların doğrulanabilmesi için geçerliliğinin şart olduğu sertifika zincirinin en tepesindeki sertifikadır.
Anahtar:	İmza oluşturma veya imza doğrulama verilerinden her biri.
Kurumsal Başvuru:	Bir tüzel kişiliğin çalışanları, müşterileri veya üyeleri ya da hissedarları adına yaptığı nitelikli elektronik sertifika başvurusudur.
Mali Sorumluluk Sigortası:	ESHS'nin, kanundan doğan yükümlülüklerini yerine getirmemesi sonucu doğacak zararların karşılanması amacıyla yaptırmakla yükümlü olduğu sigortadır.

Özne:	Sertifikanın CN alanında yer alan kişinin adı ve soyadıdır.
Özetleme Algoritması:	Güncel Kanun ve yönetmeliklerde uygun olarak verilerin sabit uzunlukta sayısal bir parmak izi değerini çıkartmak için kullanılan algoritmadır.
Anahtar Çifti:	Aynı anda üretilen ve birbirleri ile asimetrik kriptografik yapıda olan imza oluşturma verisi ile imza doğrulama verisidir.
Arşiv:	ESHS'nin saklamakla yükümlü olduğu bilgi, evrak, belge, dosya ve ilgili elektronik verilerdir.
Ayırt Edici İsim Alanı:	Sertifika sahibinin veya sertifikayı veren kuruluşun kimlik bilgilerini İçeren ve içerisin de CN, O, OU, T, L, C ve SERIALNUMBER gibi sertifika tipine göre uygun bilgi ve içerikle doldurulan alandır.
Çevrim İçi Durum Protokolü:	Elektronik Sertifikaların geçerlilik durumunu çevrim içi bir şekilde anlık olarak sorgulanabilmesini sağlayan protokoldür.
Elektronik İmza:	Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama ile inkâr edilemezlik amacıyla kullanılan elektronik veridir.
Elektronik İmza Kanunu:	23 Ocak 2004 tarih 25355 sayılı Resmî Gazete de yayımlanan 5070 Sayılı Kanundur.
Elektronik Sertifika Hizmet Sağlayıcısı:	Elektronik Sertifika, zaman damgası ve elektronik imzalar ile ilgili hizmetleri sağlayan kamu kurum ve kuruluşlar ile gerçek ve özel hukuk tüzel kişilerdir.
Elektronik Veri:	Elektronik, optik veya benzeri yollarla elektronik ortamda üretilen, taşınan veya saklanan kayıtlar.
Erişim Şifresi:	Güvenli elektronik imza oluşturma araçlarına erişim için kullanılan şifredir.

Gizli Anahtar:	AAA yapısında, Çift anahtarlı şifreleme algoritmasında sadece anahtar sahibinin erişebildiği kripto grafik anahtardır (Kanun'da imza oluşturma verisi olarak isimlendirilmiştir).
Güven Merkezi:	ESHS bünyesinde kayıt birimlerinden gelen sertifika başvurularının onaylayan, sertifika üretimini yapan, sertifika iptal durumlarını gerçekleştiren ve sertifika durum bilgilerini yayınlanmasını sağlayan birimdir.
Sertifika İlkeleri:	ESHS 'nin Faaliyet sürecindeki genel kuralları ve ilkeleri içeren belgedir.
Sertifika İptal Listesi:	ESHS 'nin İptal Edilen Sertifikaları periyodik olarak yayınlığı ve duyurduğu listedir.
Sertifika Sahibi:	ESHS tarafından kimlik tespiti yapılarak, adına sertifika düzenlenen gerçek kişidir.
Sertifika Uygulama Esasları:	NESİ de belirtilen ilke ve kuraların nasıl olacağını açıklayan belgedir.
Sertifika Kayıt Birimi:	ESHS bünyesinde bulunan, nitelikli elektronik sertifika hizmet sürecindeki sertifika başvurusu alma, kimlik tespiti yapma-doğrulama ve teslimat süreçlerini gerçekleştiren birimdir.
Sertifika Yenileme:	Sertifika geçerlilik süresi bitmeden, sertifika içindeki bilgiler aynı kalacak şekilde yeni sertifika bitiş tarihi ile tekrar üretiminin yapılıp süresinin uzatılmasıdır. Sertifika Yenilme başvurusu süresi bitmemiş olan sertifika ile imzalanarak kişinin kendisi tarafından elektronik ortamda yapılır.
Güvenli Elektronik İmza Doğrulama 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 ve ISO/IEC 15408 (-1,-2,-3)'e göre en az EAL4+ seviyesinde olan araçlarıdır.
Güvenli Elektronik İmza:	Güvenli elektronik imza; a) Münhasıran imza sahibine bağlı olan, b) Sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan, c) Nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan, d) İmzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan, e) Kanunun 4.üncü maddesinde sayılan niteliklere sahip, Kanunun hariç tuttuğu işlemler dışında elle atılan imzayla aynı hukuki sonucu doğuran elektronik imzadır.
İmza Doğrulama Aracı:	Elektronik imzayı doğrulamak amacıyla imza doğrulama verisini kullanan yazılım veya donanım aracıdır.
İmza Doğrulama Verisi:	Bkz. Açık Anahtar
İmza Oluşturma Aracı:	Elektronik imza oluşturmak üzere, imza oluşturma verisini kullanan yazılım veya donanım aracı.
İmza Oluşturma Verisi:	Bkz. Gizli Anahtar

İmza Sahibi:	Elektronik imza oluşturmak amacıyla bir imza oluşturma aracını kullanan NES sahibi gerçek kişi.
İptal Durum Kaydı:	Geçerlilik süresi dolmamış sertifikaların iptal bilgisinin yer aldığı, iptal zamanının tam olarak tespit edilmesine imkân veren ve üçüncü kişilerin hızlı ve güvenli bir biçimde ulaşabileceği kayıttır.
Kanun:	15 Ocak 2004 tarihli ve 5070 sayılı Elektronik İmza Kanunu
Kurum:	Bilgi Teknolojileri ve İletişim Kurumu.
Kurumsal Başvuru Sahibi:	ESHS ile Kurumsal Başvuru Sözleşmesi akdetmiş olan ve bu sözleşme hükümleri ve "Yönetmeliğin" 3. ve 9. maddeleri uyarınca çalışanları veya müşterileri ya da üyeleri veya hissedarları adına nitelikli elektronik sertifika başvurusunda bulunan tüzel kişiliktir.
Kurumsal Başvuru Yetkilisi:	Sertifika Kullanıcısı adına NES düzenlenmesi için ESHS'ye bildirilecek olan bilgileri, Yönetmeliğin Mad. 9/1.de belirtilen belgelere dayanarak tespit eden ve "Kurumsal Başvuru Sözleşmesi" içerisinde kendisiyle ilgili belirtilen işlemleri "Kurumsal Başvuru Sahibi" adı ve hesabına yerine getiren "Kurumsal Başvuru Sahibi"nin çalışanıdır.
Sertifika İmzalama Talebi (CSR):	Sertifikayı talep eden kişi tarafından üretilen ve sahip olduğu imza oluşturma verisi kullanarak imzalanan sertifika istek talebidir.
Sertifika Kullanıcısı:	Bkz. Sertifika Sahibi
Sertifika Uygulama Esaslar:	ESHS'nin elektronik sertifika yönetim sürecindeki ilke ve kurallarının "Nasıl?" uygulandığını sertifika İlkelerine (NESİ) bağlı kalarak detaylandırıp açıklayan ve gerekli durumlarda güncellenen kamuoyuna yaptığı duyurudur. Sertifika Uygulama esasları dokümanına tüm değişikleri ile beraber ESHS 'in web sitesinden erişilebilir.

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

2. YAYIN VE BİLGİ DEPOSU SORUMLULUKLARI

2.1. Bilgi Deposu

AYYILDIZİMZA, http://www.ayyildizimza.com.tr adresinde çevrim içi olarak kesintisiz şekilde sunduğu Bilgi Deposunda Kök Sertifika, Alt Kök sertifikaları, NESİ ve NESUE dokümanları, Sertifika İptal Listeleri (SİL) ve benzeri tüm bilgilerin doğruluğunu ve güncelliğini sağlar. Bu hizmeti sağlamak için üçüncü bir güvenilir kişi ya da kuruluş kullanmaz.

2.2. Sertifika Hizmeti ve İlgili Bilgilerinin Yayınlanması

AYYILDIZİMZA bilgi deposun da ESHS, iç yönetimindeki süreçlerde kullanılan şirkete özel belgeler dışında kalan, Nitelikli Elektronik Sertifika hizmetlerinin yönetim sürecinde yer alan bilgi ve belgeler herkesin erişimine açık halde tutulur.

- AYYILDIZİMZA Kök ve Alt Kök sertifikaları ve sürüm geçmişleri,
- Güncel SİL dosyaları,
- Zaman Damgası Sertifikaları ve sürüm geçmişleri,
- ÇiSDUP Sertifikaları ve sürüm geçmişleri,
- NESİ ve NESUE Dokümanları ve sürüm geçmişleri,

- İlgili Kanun ve Yönetmelikler,
- NES Başvuru Dokümanları,
- Taahhütnameler,
- Sözleşmeler,
- Kılavuzlar,
- Kullanıcı yardım doküman ve materyalleridir.

Yukarıdaki bilgiler, herkesin erişimine açık olarak dizin sunucularda ve bilgi deposunda yayınlanır.

2.3. Yayımlanma Zamanı ve Sıklığı

- NESUE ve NESİ dokümanları güncellediği zaman AYYILDIZİMZA Sertifika İlkeleri Yönetim ekibi tarafından onaylandıktan sonra eski sürümleri ile beraber yayımlanır.
- Sertifika hizmet sürecindeki taahhütnameler, sözleşme ve kılavuzlar güncellendiği zaman yayımlanır.
- Kök, Alt Kök, Zaman Damgası ve ÇİSDUP sertifikalarda değişiklik olduğu anda eski sürümleri ile beraber yayımlanır.
- Son kullanıcıya ait bir elektronik sertifikanın durum bilgisi değiştikten en geç 5 dakika sonra otomatik olarak SİL listesi üretilir ve yayımlanır. SİL geçerlilik süresi 24 saattir. Eğer son kullanıcıya ait sertifikalar da bir durum güncellemesi olmaz ise SİL 8 saatlik zaman dilimleri içinde otomatik olarak tekrar üretilerek yayımlanır.
- Alt Kök sertifikaları yayımlandıktan sonra, en kısa zamanda SİL yayımlanır.
- Alt kök sertifikalarına ait SİL, yılda bir defa olmak üzere veya ilgili Alt Kök Sertifikası iptal edilmesi durumunda derhal yayımlanır.
- SİL içinde yer alan bir sertifika süresi dolmuş ise yeni yayımlanacak SİL içinden çıkartılır ve yayım bilgisi silinir.
- Son kullanıcıya ait bir sertifika, son kullanıcı izni alınarak ortak dizin listesinde yayınlanır.

2.4. Bilgi Deposuna Erişim Kontrolleri

AYYILDIZİMZA, bilgi deposunu ilgili herkesin erişimine açık tutar. Ayrıca kesintisiz olarak erişilebilirliğini ve güvenliğini sağlamak için gerekli tüm önlemleri alır. Bilgi deposundaki verilerin kontrolü AYYILDIZİMZA Bilgi Güvenliği Kurulu tarafından yönetilir. Bilgi Deposundaki verilerin güncellenmesi, yetkilendirilmiş AYYILDIZİMZA personelleri tarafından gerçekleştirilir.

3. KİMLİĞİN DOĞRULANMASI

AYYILDIZİMZA, aşağıda belirtilen işlemleri yasal ve teknik gereklilikleri gözeterek sertifika sahibinin eğer sertifika içinde kurum bilgisi var ise ilgili kurumun kimlik tespitini, resmi evrak ve dokümanlara dayandırarak gerçekleştirir.

- Yeni sertifika başvurusunun alınması,
- Mevcut sertifikanın yenilenmesi,
- Sertifikanın Askıya Alınması,
- Sertifikanın Askıdan İndirilmesi,
- Sertifikanın İptal Edilmesi,

Bu taleplerin nasıl uygulanacağı bu bölümde açıklanmıştır.

3.1. İsimlendirme

3.1.1. İsim Tipleri

Üretilen sertifikalar da kimlik bilgilerinin yazıldığı isim alanı "ITU X.500 Distinguished Name (Ayırt edici isim)" kuralına uygun olarak kullanılır.

3.1.2. İsimlerin Anlamlı Olması Gerekliliği

Üretilen sertifikalardaki isimler belirsizlikten uzak ve anlamlıdır.

3.1.3. Sertifika Sahiplerinin Anonimliği ve Takma Ad Kullanılabilirliği

AYYILDIZİMZA, ürettiği nitelikli elektronik imza sertifikasında sadece gerçek isim kullanımına izin verir. İçerisinde anonim ve takma ad olan bir sertifika üretemez.

3.1.4. Farklı İsim Biçimlerinin Değerlendirilmesi

Üretilen sertifikalarda ITU X.500 standartları gereğince ayırt edici biçimine uygun olarak isimlendirme kullanılır.

3.1.5. İsimlerin Benzersizliği

AYYILDIZİMZA, ürettiği her sertifikadaki ayırt edici isim alanında yer alan bilgileri, sertifikanın benzersiz şekilde oluşmasını sağlayacak şekilde tanımlar. Böylelikle üretilen sertifikalar tekil yapıda ve kendi aralarında eşi yoktur.

Türkiye Cumhuriyeti vatandaşları için TCKN bilgisi, Türkiye'de yerleşik yabancı uyruklular için ise Ülke Kodu (ISO 3166-1 alpha-3) ve pasaport numarası bilgisi, ayırt edici isim alanında seri numarası (SERIALNUMBER) olarak kullanılarak sertifika benzersizliği sağlanır.

3.1.6. Ticari Markaların Tanınması, Doğrulanması ve Rolü

AYYILDIZİMZA, sertifika başvuru sürecinde, başkalarının fikir ve mülkiyet hakkını ihlal eden bilgiler yer alamaz.

3.2. İlk Kimlik Doğrulama

3.2.1. İmza Oluşturma Verisine Sahip Olunduğunun Kanıtlanma Yöntemi

AYYILDIZİMZA sertifika yönetim sürecinde, imza oluşturma ve doğrulama verisi sadece ESHS tarafından üretilir. İçinde imza oluşturma verisi ve imza doğrulama verisi bulunan güvenli elektronik imza oluşturma aracı kişinin kendisine teslim edilir. Böylelikle kişi, imza oluşturma verisine sahip olduğunu kabul eder.

3.2.2. Tüzel Kişiliğin Doğrulanması

Kanuna göre Nitelikli Elektronik Sertifika sadece gerçek kişiler adına üretilir. Eğer üretilen sertifikaların içerisinde bir tüzel kişiliğin isminin veya unvanının bulunması durumunda, resmî belgeler ve kaynaklara dayanarak ilgili tüzel kişilik doğrulanır. İmza sahibinin, Kurumsal Başvuru olarak nitelendirilen bu şekilde bir başvurusunun kabul edilebilmesi için ticari sicil kaydı, faaliyet belgesi, imza sirküleri, yetki belgesi gibi evraklar istenir ve doğrulanır.

3.2.3. Gerçek Kişinin Doğrulanması

AYYILDIZİMZA, üreteceği NES içerisinde yer alacak bilgiler, ancak sertifika başvuru sahibinin beyan ettiği bilgilerin ilgili yasal yönetmeliklere uygun olarak resmî belge ve kaynaklara dayandırarak doğrulaması ile gerçekleştirir. İlk imza üretiminde kişinin yüz yüze kimlik tespiti yapılması zorunludur. Yüz yüze kimlik doğrulamasında;

- Nüfus Cüzdanı,
- Pasaport,
- Ehliyet,
- Noter Onaylı Vekalet (elektronik imza kullanıma ilişkin ibareler geçmesi gerekir).

Gibi resmî belgelerin ibraz edilmesi şarttır. Eğer Başvuru sahibi, sertifika içerisine mesleki unvanın da yazılmasını isterse diploma aslı veya noter onaylı örneği, mezuniyet belgesi ibraz etmek zorundadır.

İkinci ve daha sonraki başvurularda ise sertifikanın ayırt edici isim alanında bulunan "CN", "SERIALNUMBER" bilgilerinde bir değişiklik olmaması halinde yüz yüze kimlik doğrulamasına ihtiyaç duyulmaz. Bu durum, ancak başvuru sahibinin AYYILDIZİMZA tarafından üretilmiş geçerli son sertifikasının bitiş tarihinden itibaren 3(üç) ayı aşmamak koşulu ile uygulanır. Koşulu sağlayan başvuruların doğrulama işlemi cep telefonu, faks veya e-posta yolu ile AYYILDIZİMZA prosedürlerine uygun olarak gerçekleştirilir. Yapılan doğrulama sonucunda bir şüphe oluşması halinde yüz yüze kimlik tespiti uygulanır. Eğer kullanıcı, geçerli bir elektronik imzaya sahip ise kimlik tespiti elektronik imzalı başvurunun doğrulanması ile de gerçekleştirebilir.

3.2.4. Doğrulama Yapılmaksızın Sertifikada Yer Alabilen Bilgiler

NES içerisinde yer alabilen e-posta adresi, başvuru sahibinin beyanıyla alınır ve doğrulama yapılmaksızın üretilen sertifika bilgilerinde yer alır.

Sertifika ayırt edicisi isim alanında bulunan "OU", "S", "L" bilgileri de aynı şekilde başvuru sahibinin beyanı doğru kabul edilerek, AYYILDIZİMZA tarafından ek bir doğrulama ihtiyacı olmadan sertifika içerisine konulur.

3.2.5. Yetkinin Doğrulanması

Sertifika içerisinde, eğer tüzel bir kişiliğin ismi veya unvanı bulunuyorsa, bu bilgi ancak resmî belge ve kaynaklara dayandırılarak doğrulama işlemi ile gerçekleştirilir. Sertifika başvuru sahibi, ilgili tüzel kişilik tarafından yetkilendirilmiş olduğunu imza sirküleri ile ibraz etmek zorundadır.

3.2.6. Karışlıklı Çalışma Kriterleri

Uygulama dışıdır. Düzenlenmesine gerek duyulmamıştır.

3.3. Anahtar Yenileme işlemi İşleminde Kimlik Doğrulama

3.3.1. Olağan Anahtar Yenileme İşlemlerinde Kimlik Doğrulama

Bu Doküman (NESUE) de bölüm 3.2 de yer alan esaslar uygulanır.

3.3.2. İptal Edilen Sertifika Sonrası Anahtar Yenileme işlemlerinde Kimlik Doğrulama

İptal edilmiş NES kimlik doğrulama süreçlerinde kullanılamaz. İptal sonrası süreçte, kullanıcı ilk kez sertifika başvuru yapıyormuş gibi kimlik doğrulamasını bölüm 3.2 ye göre tekrar yapar.

3.4. Sertifika İptal Talebi için Kimlik Doğrulama

ESHS, sertifika sahibinin talebi doğrultusunda veya İşbu NESUE ve ilgili NESİ de belirtilen şartların gerçekleşmesi durumda kendisi de iptal edebilir. İptal talepleri, sertifika sahibi veya kurumsal bir sertifika ise ilgili tüzel kişilik tarafından da aşağıdaki belirtilen güvenli yöntemler ile oluşturulur ve AYYILDIZİMZA tarafından doğrulanır.

- İptal talebi, çağrı merkezi veya çevrim içi olarak web sitesi üzerinden kabul edilir. Sertifika sahibinin başvurusunda vermiş olduğu bilgiler ile doğrulaması gerçekleştirilir.
- Sertifika sahibi AYYILDIZİMZA kayıt birimlerine dilekçe ile başvurarak iptal talebi oluşturabilir.

4. SERTİFİKA YAŞAM DÖNGÜSÜ İŞLEVSEL GEREKLİLİKLERİ

AYYILDIZİMZA, nitelikli elektronik sertifikalarını bu NESUE dokumanda yer alan uygulama esaslarına uyarak üretimini yapar ve sertifika yaşam döngüsünü yönetir.

4.1. Sertifika Başvurusu

4.1. Kimler Sertifika Başvurusunda bulunabilir?

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

Sertifikanın içinde kurum bilgisi yer alacak ise (Kurumsal İmza) bu başvuru ancak sertifika sahibi olan gerçek kişinin ilgili kurum yetki belgelerini resmî belge ve kaynaklara dayandırarak ibraz etmesi ile mümkündür.

4.1.2. Sertifika Başvurusu, Kayıt Süreci ve Sorumluluklar

AYYILDIZİMZA, NES başvuru talebini çeşitli yöntemler ile kabul edebilir. Kullanıcı sertifika başvurusunda bulunmak için kayıt birimlerine bizzat gidebilir. Kullanıcı ister ise sertifika başvuru sürecini

AYYILDIZİMZA web sitesi üzerinden "başvuru formunu" doldurarak çevrim içi olarak da başlatabilir. Başvuru ve kayıt süreçleri aşağıdaki adımlar ile gerçekleşir.

Kayıt birimi üzerinden;

- Başvuru sahibi, kayıt birimine giderek Nitelikli Elektronik Sertifika başvuru formunu doldurur ve NES taahhütnamesi ile birlikte imzalar.
- Başvuru sahibi, sertifika içinde yer alacak bilgilerin doğruluğunu resmi evrak ve belgelere dayandırarak kayıt birimi huzurunda kanıtlamak zorundadır.
- Kayıt birimi, sertifika başvuru sahibinin Kimlik Kart, Ehliyet veya Pasaport belgelerini ibraz etmesini ister. Eğer kurumsal bir başvuru yapılacak ise ilgili tüzel kişiliğe ait imza sirküler ininde ibraz edilmesi zorunludur.
- Kayıt birimi, resmi evrak ve belgeler aracılığı ile doğrulamasını yaptığı kişinin sertifika başvurusunu AYYILDIZİMZA sistemi üzerinden oluşturur. Bu işlemi, kayıt birimi kendi elektronik imzasıyla sisteme giriş yaparak gerçekleştirir ve tüm işlemler AYYILDIZİMZA tarafından kayıt altına alınır.

Çevrimiçi olarak web sitesi üzerinden;

- Başvuru sahibi, çevrimiçi olarak AYYILDIZİMZA web sitesi üzerinden sertifika başvuru formunu doldurarak başvuru işlemini başlatır.
- Başvuru sahibi, Noter üzerinden kimlik tespitini yaptırarak, NES taahhütnamesi ve başvuru sürecindeki gerekli resmi evrakların bir suretlerini Noter onaylı olarak AYYILDIZİMZA 'ya kargo ile gönderir.

Başvuru sahibi, bu bölümde detayları açıklanan başvuru şartlarını yerinde getirmekle, ESHS ise sertifika içerisinde yer alan bilgilerin başvuru sürecinde doğruluğu sağlamakla sorumludur.

4.2. Sertifika Başvurusunun İşlenmesi

4.2.1. Kimlik Doğrulama işlemlerinin Yerine Getirilmesi

AYYILDIZİMZA sertifika başvuru sürecinde, bu doküman (NESUE) bölüm 3.2 de açıklanan uygulama esaslarına göre kimlik doğrulama işlemini yapar.

4.2.2. Sertifika Başvurusunun Kabulü ve Reddedilmesi

AYYILDIZİMZA, sertifika başvuru sürecinde beyan edilen belgelerin incelenmesi sonucunda başvuruyu kabul veya reddeder.

Başvuru aşağıdaki koşular yerine getirilmesi durumunda kabul edilir;

- Bölüm 3.2 de belirtilen esaslara göre gerekli belgelerin AYYILDIZİMZA prosedürlerine göre noksansız olarak tamamlanması,
- Ödemenin yapılmış olması,

Başvuru aşağıdaki koşullar gerçekleşmesi durumunda reddedilir;

- Bölüm 3.2 de belirtilen esaslara göre gerekli belgelerin AYYILDIZİMZA prosedürlerine göre eksik bulunması,
- Başvuru sürecindeki gerekli belgelerin doğrulaması sırasında yapılan sorgulamalar da başvuru sahibinin şüpheli veya tatminkâr yanıt vermemesi,
- Ödemenin yapılmamış olması,

Onaylanan başvurular için üretim süreci başlatılır. Ret edilen başvuruların ret edilme nedeni başvuru sahibine bildirilir.

4.2.3. Sertifika Başvurularının İşlenme Süresi

NES başvuruları, ilgili geçerli belgelerin AYYILDIZİMZA 'ya ulaşmasının ardından en fazla 5(beş) iş günü içerisinde işleme alınır.

Bu madde içerisinde belirtilen işleme alınma süresi, sertifika başvurularının bu doküman (NESUE) 3.2 de yer alan ilkelerin sorunsuz bir şekilde doğrulanarak gerçekleşmesi halinde geçerlidir.

4.3. Sertifika Üretimi

4.3.1. Sertifika Üretimi Sırasındaki ESHS Faaliyetleri

AYYILDIZİMZA tarafından bölüm 4.2.2 de açıklanan esaslara göre doğrulanan ve kabul edilen sertifika başvuruları, onay sürecinin ardından sertifika üretim sürecine geçilir. Sertifika üretim sürecinde şu adımlar uygulanır;

- Kayıt birimleri tarafından doğrulanan başvurular, AYYILDIZİMZA sertifika onay ekibi tarafından ikinci defa kontrol yapılarak onay işlemi verilir.
- Sertifika yönetim ekibi tarafından başvurusu onaylanan NES, ESHS tarafından kanun ve yönetmeliklerde belirtilen ilgili algoritma ve standartlara göre üretimi yapılır.

4.3.2. Sertifika Üretimiyle İlgili Sertifika Sahibinin Bilgilendirilmesi

Sertifika başvurusu onaylandıktan sonra, üretimi yapılan sertifikanın üretiminin gerçekleşmiş olduğu bilgisi e-posta veya SMS yolu ile sertifika sahibine iletilir.

4.4. Sertifikanın Kabulü

4.4.1. Sertifikanın Kabulünün Biçimi

AYYILDIZİMZA tarafından üretilen NES sertifika sahibine teslim edilir. Sertifika sahibi kullanmaya başlamadan önce sertifikasını kontrol eder ve doğrular. Kontrol sonucunda aşağıda yer alan durumlarda;

- Sertifikanın kendisine ait olmaması,
- Teslim alınan sertifika bilgilerinde eksik ya da hata olması,
- Teslim alınan imzalama aracında donanımsal sorun bulunması,

ESHS'yi bilgilendirmek ile yükümlüdür aksi durumda sertifika kabul edilmiş sayılır. AYYILDIZİMZA, kabulü gerçekleşmeyen sertifikaları derhal iptal eder.

Kargo ile gönderilen veya kayıt birimlerin den teslim edilecek NES, 1(Bir) ay içerisinde teslim alınmak zorundadır. Aksi durumda sertifika kabul edilmemiş sayılır ve iptal edilir. Bu durumda ücret iadesi yapılmaz.

4.4.2. ESHS Tarafından Sertifikanın Yayımlanması

AYYILDIZİMZA, sertifika sahibinin yazılı izni bulunmak şartı ile ürettiği NES 'i kamuya açık bir ortak dizinde yayınlar.

4.4.3. Diğer Katılımcıların Sertifika Üretimiyle İlgili Bilgilendirilmesi

Uygulama dışıdır. Düzenlenmesine gerek duyulmamıştır.

4.5. Anahtar Çifti ve Sertifika Kullanımı

4.5.1. Sertifika Sahibinin İmza oluşturma Verisi ve Sertifika Kullanımı

Sertifika sahibi, üretilen sertifika ve imza oluşturma verisini, ancak yasal düzenlemeler ve sertifika başvurusunda imzalamış olduğu NES taahhütnamesinin sınırları içerisinde, güvenli elektronik imza oluşturmak için kullanabilir.

Güvenli elektronik imza verisi ancak güvenli elektronik imza aracında bulunur. Güvenli elektronik imza aracı ise bölüm 6.2.1 de yer verilen güvenlik standartlarını taşımak zorundadır.

İmza oluşturma verisinin başkalarının erişimine karşı korumak ve gizliliğini sağlamak sertifika sahibinin sorumluluğundadır. Sertifika ve imza oluşturma verisinin güvenli elektronik imza oluşturma gayesi dışında kullanılmasında oluşabilecek her türlü zarardan sertifika sahibi yükümlüdür.

Sertifika sahibi, geçerlilik süresi dolmuş veya iptal edilmiş sertifika ya ait imza oluşturma verisi ile geçerli bir güvenli elektronik imza oluşturamaz.

4.5.2. Üçüncü Kişilerin İmza Doğrulama Verisi ve Sertifika Kullanımı

Üçüncü kişiler, oluşturulmuş güvenli elektronik imzayı, sertifika ve sertifikaya bağlı imza doğrulama verisi kullanarak doğrulama işlemini gerçekleştirir ve güvenir. Üçüncü Kişiler, doğrulama işlemi sırasında;

- Sertifika ve Sertifika zincirinin geçerlilik kontrolünü,
- Sertifika içerisinde yer alan "Anahtar Kullanımı" alanının kullanım durumu ile uyumluluğunu,
- Sertifikanın yasal çerçeveler tarafından belirtilen amaçlar doğrultusunda kullanılıp kullanılmadığı kontrolünü yapmakla yükümlüdürler.

Sertifikanın ve imza doğrulama verisi ile hatalı doğrulama yapılması durumunda oluşabilecek zararlardan üçüncü kişiler sorumludur.

4.6. Sertifika Yenileme

Sertifika yenileme, sertifika içindeki imza doğrulama verisi ve sertifika içerisindeki bilgilerin aynı kalmak şartı ile süresinin uzatılması işlemidir. AYYILDIZİMZA ancak yeni anahtar çifti üreterek yenileme işlemini gerçekleştirir.

4.6.1. Sertifika Yenilemeyi Gerektiren Durumlar

Sertifika süresinin bitiş tarihinin yaklaşması ve sertifikanın içinde yer alan bilgilerden herhangi bir değişiklik gerçekleşmeyecek olması koşulu ile sertifika sahibi yenilenme talebinde bulunabilir.

4.6.2. Yenileme Başvurusunda Bulunacak Kişiler

Sertifika sahibi tarafından yenileme başvurusu yapılabilir.

4.6.3. Sertifika Yenilenme Başvurusunun İşlenmesi

Sertifika yenileme başvuruları, AYYILDIZİMZA web sitesi veya uygulaması üzerinden geçerli bir nitelikli elektronik sertifika ile geçekleştirilir ve en fazla 5(beş) iş günü içinde değerlendirilerek işleme alınır. Kişinin yenileme yapacağı sertifika bilgilerinde herhangi bir değişiklik kuşkusu oluşmuş ise AYYILDIZİMZA, bölüm 3.2 de belirtilen esasları uygular.

Sertifika yenileme sürecinde;

- Kullanıcı, geçerli elektronik imzası ile imzaladığı yenileme sözleşmesi doğrulanır ve kimlik tespiti yapılmış sayılır.
- Kullanıcı mevcut sertifikasının geçerlilik süresi bitmiş veya iptal edilmiş ise bölüm 4.1.2 de belirtilen esaslar uygulanır.

4.6.4. Yenilenmiş Sertifikayla İlgili Sertifika Sahibine Bildirim Yapılması

Bu doküman (NESUE) de yer alan 4.3.2 esaslar uygulanarak yürütülür.

4.6.5. Yenilenen Sertifikanın Kabulü

Bu doküman (NESUE) de yer alan 4.4.1 esaslar uygulanarak yürütülür.

4.6.6. ESHS Tarafından Yenilenen Sertifikanın Yayımlanması

Bu doküman (NESUE) de yer alan 4.4.2 esaslar uygulanarak yürütülür.

4.6.7. Diğer Katılımcıların Yeni Sertifika Üretimiyle İlgili Bilgilendirilmesi

Uygulama dışıdır. Düzenlenmesine gerek duyulmamıştır.

4.7. Anahtar Yenileme

4.7.1. Anahtar Yenilemeyi Gerektiren Durumlar

AYYILDIZİMZA, sertifika geçerlilik süresinin ilk 2 (iki) ayı süresi zarfında sertifika sahibinin kartından sertifikanın silinmiş olması, güvenli elektronik imza oluşturma aracının kaybolması, çalınması veya bozulması durumunda anahtar çiftini yenileyerek yeni bir sertifika üretir.

AYYILDIZİMZA, NES yenileme işlemlerini yeniden anahtarlama yöntemini kullanarak gerçekleştirir.

4.7.2. Anahtar Yenileme Talebine Bulunabilecek Kişiler

AYYILDIZİMZA, ürettiği sertifikalarda anahtar yenileme talebini sadece sertifika sahibinden kabul eder.

4.7.3. Anahtar Yenileme Talebinin İşlenmesi

Bölüm 4.7.1 de yer alan anahtar yenilemeyi gerektiren durumların gerçeklemesi halinde, eski sertifika AYYILDIZİMZA tarafından iptal edilir. Yeniden anahtarlama yapılarak yeni bir sertifika üretilir. Bu işlem için tekrardan ek belge istenmez fakat sertifikadaki bilgilerin değişmezliği şarttır. Eğer bu durumdan kuşku duyulursa bilgilerin değişmediğinin kanıtlanması için gerekli evrak ve belgelerin ibrazı sertifika sahibinden yeniden istenir.

4.7.4. Yeni Sertifikayla İlgili Sertifika Bildirim Yapılması

Bu Doküman (NESUE) de 4.3.2 yer alan esaslar uygulanır.

4.7.5. Anahtar Yenilemesi Yapılan Sertifikanın Kabulü

Bu Doküman (NESUE) de 4.4.1 yer alan esaslar uygulanır.

4.7.6. ESHS Tarafından Anahtarı Yenilenen Sertifikanın Yayımlanması

Bu Doküman (NESUE) de 4.4.2 yer alan ilkeler uygulanır.

4.7.7. Diğer Katılımcıların yeni Sertifika Üretimiyle İlgili Bilgilendirilmesi

Uygulama dışıdır. Düzenlenmesine gerek duyulmamıştır.

4.8. Sertifika Değişikliği

4.8.1. Sertifika Değişikliğini Gerektiren Durumlar

Üretilen NES içinde yer alan bilgi değiştirilemez. Sertifika sahibi böyle bir talepte bulunuyorsa elektronik sertifika başvurusu yeniden yapmalıdır. Yeni sertifika başvuru süreci bu doküman (NESİ) 4.4.1'deki ilkeler doğrultusunda gerçekleştirilir. Sertifika değişimi sırasında eksi sertifika iptal edilerek kullanımı sonlandırılır.

4.8.2. Sertifika Değişiklik Talebinde Bulunacak Kişiler

Bu Doküman (NESUE) de 4.1.1'de yer alan ilkeler uygulanır.

4.8.3. Sertifika Değişiklik Talebinin İşlenmesi

Bu Doküman (NESUE) de 3.2' de yer alan ilkeler uygulanır.

4.8.4. Yeni Sertifikayla İlgili Sertifika Sahibine Bildirim Yapılması

Bu Doküman (NESUE) de 4.3.2' de yer alan ilkeler uygulanır.

4.8.5. Değişiklik Yapılmış Sertifikanın Kabul Şekli

Bu Doküman (NESUE) de 4.4.1' de yer alan ilkeler uygulanır.

4.8.6. ESHS Tarafından Değişiklik Yapılmış Sertifikanın Yayımlanması

Bu Doküman (NESUE) de 4.4.2' de yer alan ilkeler uygulanır.

4.8.7. Diğer Katılımcıların Yeni Sertifika Üretimiyle İlgili Bilgilendirilmesi

Uygulama dışıdır. Düzenlenmesine gerek duyulmamıştır.

4.9. Sertifika İptali ve Askıya Alma

4.9.1. Sertifika İptalini Gerektiren Durumlar

Sertifikanın geçerlilik süresi dolmadan kullanımının sonlandırılması "Sertifika İptali" olarak nitelendirilir. İptal edilen bir sertifikaya ait imza oluşturma verisi ile bir daha asla güvenli elektronik imza oluşturulamaz. Aşağıda meydana gelen durumların gerçekleşmesi sertifika iptalini gerektirir;

- Sertifika sahibinin talep etmesi,
- Sertifika başvurusundaki bilgilerin sahteliğinin ve yanlışlığını ortaya çıkması. AYYILDIZİMZA, bu hususa dayalı iptali, ilgili delillere dayanarak bizzat kendisi tek taraflı olarak yapabileceği gibi, başvuru sahibinin ya da yetkili kişinin bu konuda beyanı ile de gerçekleştirebilir.
- Sertifika içerisinde yer alan bilgilerde bir değişiklik olması,
- Sertifika sahibinin fiil ehliyetinin sınırlandığının ya da ölümünün öğrenilmesi,
- İmza oluşturma verisinin güvenliliğinin kaybedildiğinden kuşku duyulması,
- Kurumsal bir sertifika ise ilgili tüzel kişiliğin faaliyetini durdurması,
- Kurumsal bir sertifika ise, Tüzel kişilik ile sertifika sahibi arasındaki hukuki ilişkinin sonlandırılmış olması,
- Güvenli elektronik imza aracının kaybedilmesi veya çalınması,
- Güvenli elektronik imza erişim verisinin kaybedilmesi veya çalınması,
- Elektronik Sertifikanın, AYYILDIZİMZA sertifika sahibi taahhütnamesi, NESİ ve NESUE de belirtilen şartlara aykırı olarak kullanıldığının tespit edilmesi,
- İmza oluşturma verisinin gizliliğinin ortadan kalkması,

- Kayıt birimleri tarafından elden teslim edilecek veya posta yolu ile gönderilen NES 'in 1(bir) ay içinde başvuru sahibi tarafından teslim alınmaması,
- AYYILDIZİMZA tek taraflı olarak, NESİ ve NESUE dokümanında yer alan ilke ve uygulama esaslarına aykırı bir durumu tespit etmesi,
- AYYILDIZİMZA Kök veya Alt Kök sertifikasının imza oluşturma verisinin gizliliğinin ortadan kalkması,
- AYYILDIZİMZA faaliyetini durdurması ve başka bir ESHS tarafından devamlılığının sağlanamamasıdır.

4.9.2. Kimler Sertifika İptal Başvurusunda Bulunabilir?

NES iptali için aşağıdaki kişiler iptal talebinde bulunabilir;

- Sertifika sahibi,
- İçerisinde kurum bilgisi bulunan bir "Kurumsal Sertifika" ise ilgili kurumun yetkilendirdiği gerçek kişi,
- Sertifika sahibinin kendisinin temsiline resmi olarak yetki verdiği kişiler,
- Gerekli durumda, AYYILDIZİMZA yetkilisi.

4.9.3. Sertifika İptal Talebi Prosedürleri

AYYILDIZİMZA sertifika iptal hizmeti taleplerini,

- Web sitesi (https://ayyildizimza.com.tr) üzerinden,
- Web sitesinde yayımlanan İptal Hattı üzerinden,
- Faks ya da eposta aracılığı ile gelen imzalı yazılar ile
- Mesai saatleri içinde kayıt birimlerine sertifika sahibinin ya da resmi olarak yetki verdiği kişilerin müracaatı gibi yöntemleri ile kabul eder.

İptal başvurusu doğrulandıktan sonra sertifika derhal iptal edilir. Sertifika iptali sonrasında, sertifika sahibine SMS ve e-posta bilgilendirilmesi yapılarak sertifikasının durumu bildirilir.

AYYILDIZİMZA 'ya ait bir güvenlik sorunu oluşması, mevcut sertifikalar ile ilgili ihbarın alınması veya iç işleyişinde oluşan bir hatanın fark edilmesi durumlarının herhangi birinin gerçekleşmesi halinde, AYYILDIZİMZA sertifika iptal sürecini tek taraflı olarak da başlatabilir.

İptal edilmiş bir sertifika tekrar kullanılamaz. AYYILDIZİMZA iptal işleminin gerçekleşmesi sonucunda anlık olarak ÇİSDUP servisini en geç 5(beş) dakika içinde de SİL listesini günceller.

4.9.4. Sertifika İptal Talebi Gecikme Periyodu

Sertifika iptal taleplerinde gecikme yaşanmaz, talep ilk geldiğinde sertifika öncelikle derhal askıya alınır. Gerekli doğrulamalar yapıldıktan sonra mümkün olan en kısa sürede işleme alınır ve derhal iptal edilir. İptal işlemi gerçekleşir gerçekleşmez bu iptal bilgisinin yer aldığı yeni SİL en geç 5(beş) dakika içinde üretilir ve yayımlanır. ÇİSDUP servisine ise iptal bilgisini anında yansır.

4.9.5. Sertifika İptal Talebinin İşlenme Süresi

AYYILDIZİMZA, gelen sertifika iptal talebinin doğrulamasını yaptıktan sonra derhal işleme alır ve sertifikayı iptal eder. İptal işleminin gerçekleşmesinin en geç 5(beş) dakika içinde yeni SİL üretilir ve yayınlanır. ÇİSDUP servisine iptal bilgisi anında yansır.

4.9.6. Üçüncü Kişilerin İptal Kontrol Gerekliliği

Üçüncü kişiler, kendi süreçlerinde işlem yapmak istedikleri elektronik imzaya güvenmeden önce sertifikanın geçerlilik durumunu kontrol etmek ile yükümlüdürler. Sertifikanın geçerlilik durumunu SİL listesi veya ÇİSDUP servisi kullanarak yapmalıdır.

Gerekli doğrulama yapılmadan işleme alınan elektronik imzalardan doğan hiçbir zarardan AYYILDIZİMZA sorumlu değildir.

4.9.7. Sertifika İptal Listesi (SİL) Yayımlama Sıklığı

AYYILDIZİMZA, herhangi bir kullanıcının sertifika iptal edilme işleminin gerçekleşmesinin en geç 5(beş) dakika içinde günceller ve yayımlar.

AYYILDIZİMZA, düzenli olarak her 4 saate bir 24 saat geçerli olmak üzere SİL üretir ve yayımlar.

4.9.8. SİL Listelerinin En Geç Yayımlanma Zamanı

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

4.9.9. Çevrim İçi Sertifika Durum Protokolü Servisinin (ÇİSDUP) erişilebilirliği

AYYILDIZİMZA, ürettiğini nitelikli elektronik sertifikaların anlık olarak geçerlilik durumlarının kontrol edilebileceği Çevrim İçi Durum Protokolü hizmetini (ÇİSDUP) 7/24 kesintisiz olarak sağlar ve erişime açık tutar.

4.9.10. Çevrim İçi Sertifika Durum Protokolü Servisinin (ÇİSDUP) Kontrol Gereklilikleri

ÇİSDUP, sertifikaların geçerlilik durumlarının çevrim içi olarak en sağlıklı ve hızlı kontrol edilme imkânı sağlar. İptal edilen her sertifika anlık olarak ÇİSDUP 'a yansıtılır. Dolayısı ile üçüncü kişilerin teknolojik alt yapısı müsaade ettiği ölçüde ÇİSDUP servisini kullanmaları gerekir.

4.9.11. Diğer İptal ve Durum Yayımlama Çeşitlerinin Varlığı

AYYILDIZİMZA, ÇİSDUP ve SİL haricinde iptal durumu yayımlama yöntemi kullanmaz.

4.9.12. Anahtar Güvenliğinin Yitirilmesine İlişkin Özel Gereklilikler

AYYILDIZİMZA, Kök ve Alt Kök sertifikalarının iptalini gerektirecek bir durum oluşması halinde Kök, Alt Kök ve bu alt kökten üretilen tüm sertifikaları iptal edilerek sertifika sahiplerine ve üçüncü kişilere duyurur.

AYYILDIZİMZA, kullanıcıların sertifikalarına ait imza oluşturma verisinin, güvenliğinin ortadan kalkması durumunda kullanıcı sertifikasını iptal eder ve sertifika sahibini bilgilendirir.

AYYILDIZİMZA, kendisinden kaynaklı tüm iptal işlemlerinde, iptal sonrası yeni sertifika üretimlerinin en hızlı şekilde başlatılmasından sorumludur.

4.9.13. Sertifika Askıya Almayı Gerektiren Durumlar

Sertifikanın geçici bir süreliğine kullanımdan kaldırılmasına askıya alma işlemi denir. SİL ve ÇİSDUP üzerinden iptal edilmiş bir sertifika gibi iptal bilgisi yayımlanır. Askıya alma işleminin, sertifika iptal işleminden tek farkı, askından geri alınarak sertifikanın kullanıma tekrar açılabilmesidir.

AYYILDIZİMZA, sertifikanın geçici olarak iptal edilmesi istendiği durumlarda sertifika sahibinin talebi üzerine sertifikayı askıya alma işlemini gerçekleştirir.

Sertifikanın iptali ancak onay ve kimlik doğrulama sürecinin tamamlanması ile mümkündür. İptal başvurusunun yapıldığı andan itibaren gerekli kontroller sağlanana kadar ki süre zarfında sertifika askıya alınır.

AYYILDIZİMZA Kök ve Alt Kök sertifikaları askıya alınmaz.

4.9.14 Sertifika Askıya Alma Talebinde Bulunabilecek Kişiler

Bu Doküman (NESUE) de 4.9.2' de yer alan esaslar uygulanır.

4.9.15. Sertifika Askıya Alma Prosedürü

Aşağıdaki durumlar haricinde, Bu Doküman (NESUE) de 4.9.2' de yer alan esaslar uygulanır.

AYYILDIZİMZA'ya ait bir güvenlik sorunu oluşması ya da mevcut sertifikalarla ilgili bir ihbar alınması durumunda NES'ler için iptal gerekliliği kesinleşene kadar AYYILDIZİMZA ilgili tüm sertifikaları aksıya alabilir. Bu tür askıya alma işlemlerinde, sonuç ilgili sertifika kullanıcılarına duyurulur.

4.9.16. Sertifikanın Askıda Kalma Süresinin Sınırları

AYYILDIZİMZA, sertifika iptal talebi kaynağını doğrulanamadığı durumlarda aksıya aldığı sertifikaları, doğrulama işlemi tamamlanıncaya kadar askıda bırakabilir. Sertifika sahipleri tarafından iptali gerektiren bir durumun olup olunamadığına karar verilememesinden dolayı askıya alınan sertifikalar ise sertifika sahibinin iptal gerekliliği onaylandığı zaman iptal edilir.

Sertifika, askıda bulunduğu süre içinde, iptali gerektiren bir durumun olmadığı anlaşılırsa, sertifika askından çıkartılıp tekrar aktif hale getirilebilir.

Tüm durumlarda sertifika askı süresi 30(otuz) takvim gününü geçemez. Bu süre zarfında askından inmeyen sertifikalar AYYILDIZİMZA tarafından otomatik olarak iptal edilir.

4.10. Sertifika Durum Servisleri

AYYILDIZİMZA, ürettiği sertifikaların geçerlilik durumlarını ÇİSDUP ve SİL olmak üzere iki farklı hizmette sunar.

4.10.1. İşlevsel Özellikler

AYYILDIZİMZA, çevrim içi durum protokolü (ÇİSDUP) hizmetini sürekli olarak güncel tutar. Sertifikaların geçerlilik durumları anlık olarak ÇİSDUP üzerinden alınabilir. İstemci tarafından gönderilen ÇİSDUP istekleri, AYYILDIZİMZA ÇİSDUP yanıtlayıcı tarafından imzalanır. İptal Bilgisi olarak sertifikanın durumu "Geçerli", "Bilinmiyor", "İptal" şeklinde ÇİSDUP cevabının içerisine yer almaktadır.

SİL hizmeti, son kullanıcıların herhangi birine ait sertifikada bir durum güncellemesi olmasının arkasından 5(beş) dakika içinde yeniden oluşturulur ve yayınlanır. Oluşturulan her SİL 24(yirmi dört) saat geçerlilik süresine sahiptir.

AYYILDIZİMZA, SİL hizmetini son kullanıcı sertifika değişikliğinden bağımsız olarak her 4(dört) saatte bir 24 saat geçerli olmak üzere otomatik olarak yeninden oluşturur.

4.10.2. Hizmetin Sürekliliği

AYYILDIZİMZA, bu doküman (NESUE) 4.10.1 de belirtilen SİL ve ÇİSDUP hizmetini 7 gün 24 saat ilkesine göre verir.

4.10.3. İsteğe Bağlı Özellikler

Uygulama dışıdır. Düzenlenmesine gerek duyulmamıştır.

4.11. Sertifika Sahipliğinin Sona Ermesi

Sertifika sahipliğinin sona ermesi, sertifikanın geçerlilik süresinin bitmesi ile ya da sertifikanın iptal edilerek kullanımdan kaldırılması ile gerçekleştirilir.

4.12. İmza Oluşturma Verisi Saklama ve Yeniden Oluşturma

AYYILDIZİMZA, sertifikaya ait imza oluşturma verisini hiçbir zaman saklamaz ve yeniden oluşturmaz; yeniden oluşturabileceği bilgileri elinde tutmaz.

4.12.1. Anahtar Saklama ve Yeniden Oluşturma İlke ve Esasları

Düzenlenmesine gerek duyulmamıştır.

4.12.2. Oturum Anahtarı Zarflama ve Yeniden Oluşturma İlke ve Esasları

Düzenlenmesine gerek duyulmamıştır.

5. TESİS, YÖNETİM VE İŞLETMEYLE İLGİLİ KONTROLLER

AYYILDIZİMZA, sertifika hizmet sürecini, oluşabilecek iç ve dış tehditleri durduran, saptayan ve bu tehditlere karşı tedbir alan bir **Güven Merkezi** içinde yürütür.

Bu bölümde, AYYILDIZİMZA 'nın Güven Merkezi içinde tesis, yönetim ve işleyiş ile ilgili uyguladığı teknik olmayan; fiziksel, prosedürel ve personel kontrolleri yer almaktadır.

5.1. Fiziksel Kontroller

5.1.1. Tesis Yeri ve İnşaatı

Güven merkezi, fiziksel dış tehditlere karşı her türlü koruma ve güvenlik tedbirleri alınarak, bina içinde Güvenlikli ve Yüksek Güvenlikli bölgeler oluşturulmuştur.

5.1.2. Fiziksel Erişim

Güven Merkezi içindeki güvenlik bölgelerine, fiziksel erişim sürekli kontrol altında tutulur. Yüksek Güvenlikli Bölgelere erişmek için, bir önceki güvenlikli bölgesinden geçilmek zorunludur. ESHS işlemlerinin gerçekleştirildiği yazılım ve donanım modülleri ile her türlü elektronik veya kâğıt ortamdaki bilgilerin bulunduğu bu bölgelere, yetkisiz kişilerin erişiminin engellenmesi için gerekli önlemler alınmıştır.

- Güvenlikli Bölgelere erişim sadece güvenilir personeller tarafından olur ve kendilerine özel olarak tahsis edilen güvenlik kartları ile gerçekleştirilir.
- Yüksek Güvenlikli Bölgelere erişim ise güvenlik kartları ile beraber biyometrik doğrulamanın da yapıldığı iki faktörlü kimlik doğrulaması ile sağlanır.
- Güvenlik Bölgelerindeki tüm haraketlilik kayıt altındadır.
- Güvenilir Personel özelliğine sahip olmayan bir kişi, ancak yanlarında güvenilir personel bulunması ve giriş sebebinin tutanak altına alınması ile mümkündür.

5.1.3. Güç Kaynakları ve Havalandırma

AYYILDIZİMZA, ESHS hizmetini kesintisiz olarak vermek için kullandığı donanımları güç kaynakları ile beslemiştir. Sistemin sürekliliğini sağlamak için sıcaklık-nem değerleri her zaman kontrol altında tutularak gerekli iklimlendirme ve havalandırma yapılmıştır.

5.1.4. Su Baskınları

AYYILDIZİMZA, yazılım, donanım ve fiziksel arşivlerinin bulunduğu yüksek güvenlikli bölgeler sel ve su baskınlarına karşı koruma ile korumuştur.

5.1.5. Yangın Önleme ve Yangından Korunma

AYYILDIZİMZA, yazılım, donanım ve fiziksel arşivlerinin bulunduğu yüksek güvenlikli bölgelerin de yangını önlemek ve yangından korunmak için gerekli tüm önlemleri almıştır.

5.1.6. Saklama Ortamları

AYYILDIZİMZA, faaliyeti sırasında oluşturduğu tüm kayıtları yedekli ve uygun saklama ortamlarında tutar.

5.1.7. Atıkların Atılması

AYYILDIZİMZA, içinde hassas bilgilerin yer aldığı kullanılmayan elektronik veya kâğıt ortamdaki tüm bilgileri geri dönüşümsüz olarak yok eder.

5.1.8. Tesis Dışı Yedekleme

AYYILDIZİMZA, ESHS faaliyetinin sürekliliğini sağlamak için olası bir felaket senaryosunda, sistemini tekrar işler duruma getirerek gerekli gördüğü tüm bileşenleri tesis dışında yüksek güvenlik ortamda saklar.

5.2. Prosedürel Kontroller

5.2.1. Güvenilir Roller

AYYILDIZİMZA, sertifika hizmet faaliyeti sürecindeki görev alan güvenilir roller aşağıda açıklanmıştır.

Bilgi Güvenliği Kurulu Başkanı ve üyeleri: AYYILDIZİMZA, Elektronik Sertifika Hizmet Sağlayıcı Faaliyetleri süresince bilgi güvenliği sağlamak ve faaliyet sürecinin tüm adımlarında bilgi güvenliğini gözetmek, önlemler almak, denetlemek, tartışmak ve karar verip uygulamaya koymak için şirket içinde Bilgi Güvenliği Kurulunu kurmuştur. Kurula Bilgi Güvenli Kurulu Başkanı, başkanlık eder ve alınan kararları onaylar.

Güven Merkezi Yöneticisi: AYYILDIZİMZA, ESHS faaliyetlerini içinde güvenlikli ve yüksek güvenlikli bölgelerin bulunduğu, bir Güven Merkezi içinde yürütür. Güven Merkezinin, Bilgi Güvenliği Politika ve Prosedürlere uygun olarak işletilmesinden Güven Merkezi Yöneticisi sorumludur. Bilgi Güvenliği Kurulu Başkanına (Genel Müdür) bağlıdır.

BGYS Yönetim Temsilcisi (İç denetçi): AYYILDIZİMZA, Varlık listelerinin güncelliğini takip etmek, BGYS risklerinin belirlenmesi ve değerlendirilmesi konusunda gerekli çalışmaları yürütür. Uygulanabilirlik bildirgesini hazırlamak ve güncelliğini takip etmek, tespit edilen riskler karşısında seçilen kontrollerin etkinliğini takip etmekle sorumludur. Bilgi Güvenliği Kurulu başkanına bağlıdır.

Kayıt Birimi Personeli: Sertifika Başvurularının kabul edilmesi, doğrulanması, onaylanması, fiziksel arşivlerin saklanması ve düzenlemesi, sertifika askı / iptal taleplerinin kabul edilip onay/ret yapılmasından sorumludur. Güven Merkezi Yöneticisine bağlıdır.

Ağ ve Sistem Yöneticisi: AYYILDIZİMZA Sistem alt yapısını, ağını kurmak, güncel tutmak ve Bilgi Güvenliği Politika ve Prosedürler doğrusunda işletmekle sorumludur. Güven Merkezi yöneticisine bağlıdır.

Ağ ve Sistem Uzmanı: Ağ ve Sistem Yöneticisine bağlı olarak sistem alt yapısı ve ağ sisteminde operatörlük yapmakla sorumludur.

Sistem Denetçisi: AYYILDIZİMZA sistem alt yapısının Bilgi Güvenliği politika ve prosedürlere uygun olarak işletilmesi için denetler. İç Denetim Komitesi üyesidir ve Bilgi Güvenliği Kurulu Başkanına bağlıdır.

5.2.2. Her Görev için Gereken En Az Kişi Sayısı

AYYILDIZİMZA, sertifika süreçlerinde bulunan kritik işlem ve görevler an az iki kişi ile birlikte gerçekleştirilir. Yüksek güvenlikli tüm bölgelere erişim aynı şekilde en az iki kişinin hazır bulunması ile mümkündür.

5.2.3. Her Görev için Kimlik Doğrulama

AYYILDIZİMZA, güvenilir rollere atamış olduğu personellerin gerekli kimlik ve biyometrik bilgilerini alarak güvenlik sistemine kayıt eder. Böylelikle her kritik işlem öncesi bu rollerdeki kişilerin doğrulaması yapılarak atanmış olduğu görevi gerçekleştirmesine izin verilir. Yüksek güvenlikli bölgelere giriş ve çıkış işlemleri ancak parmak izi ve personele atanmış güvenlik geçiş kartı doğrulması ile mümkündür.

5.2.4. Görevlerin Ayrılmasını Gerektiren Roller

AYYILDIZİMZA, sertifika hizmet sürecindeki operasyonların da aynı personelin işin bütününü ya da büyük bir kısmını yapmasına izin vermez. Denetleme görevindeki roller ile işletme görevindeki roller kesinlikle aynı kişiye verilemez. İşlem kayıtlarında mutlaka rol bilgisi yer alır.

5.3. Personel Kontrolleri

5.3.1. Nitelik, Deneyim ve Güvenlik Gereklilikleri

AYYILDIZİMZA, sertifika hizmet faaliyetini sürdürürken bünyesinde istihdam edeceği personeli, daha önce benzer çalışma alanlarında deneyim kazanmış, alanlarında nitelikli ve sürecin güvenilir şekilde yürütülebilmesi için gerekli kontrolleri sağlamış adaylar arasından seçer.

5.3.2. Kişisel Geçmiş Kontrol Gereklilikleri

AYYILDIZİMZA, bünyesinde istihdam edecek personellerin özgeçmişini ayrıntılı bir şekilde değerlendirir. Bu değerlendirmeler sonucunda uygun görülen kişilerden güvenlik geçmişini öğrenmek amacı ile ayrıca adli sicil kayıt belgesi ister ve gerekirse güvenlik soruşturması yapar.

5.3.3. Eğitim Gereklilikleri

AYYILDIZİMZA, istihdam ettiği personelleri göreve başlamadan önce, sertifika yaşam zincirinin tüm halkalarının, Bu Doküman (NESİ) ve NESUE açıklanan ilkelere uygun olarak yürütülmesi için gerekli hukuki ve teknik eğitimden geçirir.

Eğitim süreci sonunda ilgili personel tekrar değerlendirmeye alınır ve uygun görülmez ise işbaşı yaptırılmaz.

5.3.4. Tekrar Eğitim Sıklığı ve Gerekliliği

AYYILDIZİMZA, sertifika ilkelerinin eksiksiz bir şekilde tüm süreçte uygulanması için personellerini işe başlamadan önce eğitimden geçirir. Bu eğitim, sonrasında periyodik olarak gerekli görülen durumlarda tekrarlanır.

5.3.5. İş Rotasyonu Sıklığı ve Sırası

Uygulama dışıdır. Düzenlenmesine gerek duyulmamıştır.

5.3.6. Yetkisiz İşlemler için Yaptırımlar

AYYILDIZİMZA, personelinin ya da işbirlikçilerinin güvenlik ve işleyiş prosedürlerine aykırı bir ihlali tespit etmesi durumunda gerekli disiplin cezalarını uygular. Tespit edilen bu ihlaller sonucunda AYYILDIZİMZA ya da müşterileri zarar görmüş ise bu zararı ilgili kişilerden tanzim ettirebilir. Yetkisiz eylemler veya süreç ihlali fiilleri Elektronik İmza Kanunu, Türk Ceza Kanunu veya ilgili diğer kanunlarda

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

5.3.7. Bağımsız Alt Yüklenici Gereklilikleri

AYYILDIZİMZA, sertifika hizmetlerini yürütürken bağımsız yükleniciler ile sözleşme imzalayabilir. Bu sözleşmeler, AYYILDIZİMZA güvenlik koşulları ve hizmet esaslarına uygun olarak yapılır.

5.3.8. Personele Sağlanan Dokümantasyon

AYYILDIZİMZA, Bu Doküman (NESUE) ve NESİ de belirtilen ilkelerinin ve uygulanışının, sertifika hizmet sürecinde personelleri tarafından eksiksiz olarak yürütülmesi için gerekli kılavuz ve destek dokümanlarını bilgi güvenliği yönetim sistemi doğrultusunda hazırlayarak sağlar.

5.4. Denetim Kayıt Altına Alma Prosedürleri

5.4.1. Kaydedilen Olay Tipleri

AYYILDIZİMZA, sertifika yaşam döngüsü içinde gerçekleştirdiği ve denetimini yapmak istediği işlemleri kayıt altına alır. Bu Kayıtlar;

- Sertifika başvuru kayıtları,
- Sertifika başvuru onay kayıtları,
- Sertifika üretim işlemi kayıtları,
- Sertifika askıya alma, aksıdan indirme başvurusu onay kayıtları,
- Sertifika iptal başvurusu onay kayıtları,
- Sertifika askıya alma ve aksından indirerek yeniden aktif etme işlem kayıtları,
- Sertifika iptal işlem kayıtları,
- Güvenlikli bölgelere giriş-çıkış kayıtları,
- NESİ ve NESUE değişiklikleri sonucu oluşan tüm versiyonlar,
- İşlemi yapan personelin kimlik bilgisi, işlemin tarih ve zaman bilgisi,
- SİL ile ilgili kayıtlar,

- ESHS Kök ve Alt Kök sertifikalarına ilişkin kayıtlar,
- ÇİSDUP cevap imzalayıcı sertifika ile ilgili kayıtlar,
- Sistem arıza kayıtları,
- Sistem donanım ve yazılım güncelleme kayıtlarıdır.

AYYILDIZİMZA, gerekli gördüğü durumda sertifika yaşam döngüsüne etki eden yukarıdaki olay tiplerine ilave kayıtlar tutabilir.

5.4.2. Kayıt İşleme Sıklığı

Tutulan kayıtlar, işlemin oluşmasına eş zamanlı olarak sürekli olarak gerçekleşir. Kayıtlar düzgün zaman aralıkları ile incelenir. Bu incelemeler, güvenlik açıklarını uygun sürede yakalayacak sıklıkta düzenlenmiştir.

5.4.3. Denetim Kayıtlarının Saklanma Süresi

Tutulan kayıtlar, sistemin veri depolama kapasitesine göre sistemde erişilebilir halde tutulur. Yasa gereğince daha uzun süre saklanması gereken kayıtlara arşivleme işlemi uygulanır. Arşivleme işlemi Bu Doküman (NESUE) 5.5 de belirtilen ilkelere göre gerçekleştirilir.

5.4.4. Denetim Kayıtlarının Korunması

Tutulan kayıtlar, izinsiz izlenmeyi, değiştirmeyi ve silinmeyi engelleyecek şekilde elektronik ve fiziksel olarak güvenli şekilde korunur.

5.4.5. Denetim Kayıtlarının Yedeklenme Prosedürleri

Tutulan kayıtlar, ilgili prosedürlerine göre periyodik olarak yedekleri alınır.

5.4.6. Denetim Bilgisi Toplama Sistemi (İç ve Dış)

Tutulan kayıtlar, elektronik olarak veya kâğıt ortamda toplanır. Elektronik olarak toplanan kayıtlar, ESHS sisteminde tutulur. Kâğıt üzerindeki kayıtlar ise ilgili ESHS çalışanı tarafından dosyalanır ve yüksek güvenlikli bölgede yer alan arşiv odasına kaldırılır.

5.4.7. Olayı Yaratan Kişiyi Bilgilendirme

AYYILDIZİMZA, olay yaratan kişiye olayın nitelik, önem ve derecesine göre bilgilendirme yapar. Oluşan tüm olayların, ilgili kişiye bilgilendirmesi yapılmaz. AYYILDIZİMZA gerekli gördüğü durumlarda ise ilgili kişi ile beraber üst yetki seviyesinde bulunan kişi ya da kişilere de bilgilendirme yapabilir.

5.4.8. Zarar Görebilirlik Değerlendirmesi

Tutulan kayıtlar, sertifika yaşam döngüsünün güvenli bir şekilde gerçekleşebilmesi için hayati öneme sahiptir. AYYILDIZİMZA, oluşan bu kayıtların oluşturduğu raporları sürekli olarak izler ve kontrol altında tutar. Oluşan raporlar incelenerek değerlendirilir, eğer sertifika hizmet sürecinin güvenliğini tehdit edecek bir bulgu tespit ederse gerekli tüm güvenlik tedbirlerini alır.

5.5. Kayıtların Arşivlenmesi

5.5.1. Arşivlenen Kayıt Tipleri

Bu Doküman (NESUEİ) de 5.4.1'de yer alan tüm kayıt tiplerine ilave olarak;

- Üretilen tüm sertifikalar,
- Yayımlanmış tüm sertifika iptal listeleri,
- Sözleşmeler,
- Elektronik imza başvurusu sırasındaki beyan edilen tüm resmî belge ve kaynaklar,
- Taahhütnameler,
- İptal, Askı, Askıdan indirme ve tüm sertifika başvuru formaları,
- Kurumsal imza için beyan edilen tüm belge ve resmi kaynaklar,

- Yayımlanan tüm Sertifika İlkeleri dokümanı versiyonları (NESİ),
- Yayımlanan tümü Sertifika Uygulama Esasları Dokümanı versiyonları (NESUE),
- Müşteri ile ilgili yapılan tüm yazışmalar ve müşteri dosyalarıdır.

5.5.2. Arşivlerin Saklanma Süresi

AYYILDIZİMZA, arşivlediği bilgi ve belgeleri Kanun da belirtilen yasal düzenlemelerdeki belirtilen süre ile en az (20) yıl boyunca saklar.

5.5.3. Arşivlerin Korunması

AYYILDIZİMZA, arşivlerini fiziksel ve elektronik güvenlik önlemleriyle korur, arşivlerin tutulduğu yüksek güvenlikli bölgelere sadece yetkili kişilerin erişimine izin verir.

5.5.4. Arşivlerin Yedeklenme Prosedürleri

AYYILDIZİMZA, gerekli gördüğü elektronik arşivlerinin yedeğini ilgili prosedürler doğrultusunda alır ve yedekler. Kâğıt ortamındaki arşivlerin ise yedekleri alınmaz.

5.5.5. Kayıtların Zaman Damgası Altına Alınması Gereklilikleri

AYYILDIZİMZA, sertifika yaşam döngüsünde yer alan işlemlerin elektronik arşivleri zaman bilgisini içerecek şekilde saklar. Bu zaman bilgisi UTC ile senkron zaman sunucusundan alınmıştır.

5.5.6. Arşiv Toplama Sistemi

Elektronik arşivler sistem üzerinden, kâğıt arşivleri ise yetkili personeller tarafından manuel olarak toplanır.

5.5.7. Arşiv Bilgisinin Edinilmesi ve Doğrulanması Prosedürleri

AYYILDIZİMZA, Kamuya açık arşiv dokümanları;

- Kök ve Alt Kök sertifikalar,
- SİL listeleri,
- Sİ ve SUE Dokümanları,
- Sertifika başvuru formları,
- Son kullanıcı sözleşmesi örnekleri

Web sitesinin ilgili bölümlerinde erişime sunulur.

Gizli belgeler ise ilgili prosedürler doğrultusunda sadece yetkili personeller ve Bilgi Teknolojileri Kurumunun yetkililerinin erişimine sunulur. Sertifika başvuru sahipleri, bizzat kendisi ya da resmi olarak yetkilendirdiği kişi başvuruda bulunarak, arşivlenen özel bilgilerine erişim talebinde bulunabilir.

5.6. Anahtar Değişimi

AYYILDIZİMZA, Kök ve Alt Kök sertifikalarının geçerlilik süresi Kanun' a göre 10(on) yıldır. ESHS gerekli gördüğü güvenlik durumların da veya kök sertifikalarının süresi bitmeden belirli bir süre önce Sertifika ve ona bağlı imza oluşturma verisini yeniden oluşturabilir. Bu durumda, Eski Kök ve Alt kök sertifikalar geçerlilik süresinin sonunda kadar, mevcut son kullanıcı sertifikalarının üçüncü kişiler tarafından sertifika zincirinin doğruluğunu sağlamak amacı ile erişime açık tutulur.

Üretilen sertifikalar, yeni yayımlanan Kök ve Alt kökten gerçekleştirilir.

Kök anahtar üretim işlemleri birden fazla güvenilir personel ve bağımsız gözlemcilerin şahitliğinde anahtar üretim seremonisi olarak yapılır. Tüm adımları yazılı ve görsel kayıt altına alınır.

5. 7. Güvenliğin Yitirilmesi ve Felaket Kurtarma

5.7.1. Güvenlik Kaybına Neden Olabilecek Olaylar

AYYILDIZİMZA, faaliyetinin güvenilirliğini etkileyecek nitelikte, olayların meydana gelmesi durumunda, İş Sürekliliği Yönetimi ve Felaketten Kurtarma Prosedürleri doğrultusunda oluşturduğu planlar ile olaya en kısa sürede müdahale ederek sistemin en hızlı şekilde tekrar güvenli hizmeti

verebilmesi için gerekli önlemleri alır. Süreçten etkilenen kullanıcı veya kullanıcılara gerekli bilgilendirmeleri yapar.

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

AYYILDIZİMZA merkezinde bulunan donanım, yazılım ve verilerde bir bozulma meydana gelmesi durumda, İş Sürekliliği Yönetimi ve Felaketten Kurtarma Prosedürleri doğrultusunda oluşturduğu planlar ile olaya hemen müdahale eder. Bozulmuş veya artık ulaşılamayan verilerin derhal yedekleri işleme alınır. Eğer kurtarılamayan veriler bulunuyor ise sertifika doğrulama sürecinde oluşabilecek hatalara karşı sertifika sahipleri ve üçüncü kişiler ivedilikle bilgilendirilir.

Donanım ve yazılım sistemlerinin, meydana gelebilecek bozulma veya arızalara karşı AYYILDIZİMZA hizmetinin kesintiye uğramaması için felaket senaryosu olarak hazır tuttuğu yedek sistemleri derhal devreye alır ve hizmetinin sürekliliğini sağlar.

5.7.3. İmza Oluşturma Verilerinin Güvenliğinin Yitirilmesi

AYYILDIZİMZA, imza oluşturma verilerinin güvenliğini yitirmesi halinde İş Sürekliliği Yönetimi ve Felaketten Kurtarma Prosedürleri doğrultusunda ilgili sertifikaları derhal iptal eder. Aynı şekilde İptal edilmiş olan bu imza oluşturma verisinin daha önce imzaladığı mevcut tüm sertifikaları da iptal eder. Bu Doküman (NESUE) 5.6 kısım da bulunan ilkeleri uygulayarak yeni bir sertifika ve ona ait imza oluşturma verisi üretir. İptal edilmiş ve yeni üretilen tüm sertifikalar oluşturulan bu yeni imza oluşturma verisi ile imzalanır. Böyle bir durumda ilgili sertifika sahiplerine ve üçüncü kişilere gerekli bilgilendirmeleri yapar.

5.7.4. İş Sürekliliği Yetenekleri ve Felaket Kurtarma

AYYILDIZİMZA, merkezi dışında Felaket Kurtarma Merkezi (FKM) tesis etmiştir. Meydana gelebilecek bir afet sonrası hizmet sürekliliğini sağlamak için gerekli tüm verileri yedekler.

AYYILDIZİMZA, işleyişini engelleyecek nitelikte olayların ya da güvenlik sorunlarının oluşması durumunda, İş Sürekliliği Yönetimi ve Felaketten Kurtarma Prosedürleri doğrultusunda oluşturulan planlar ile derhal müdahale eder.

5.8. AYYILDIZİMZA Faaliyetinin Son Bulması

AYYILDIZİMZA, ESHS faaliyetinin son bulması halinde, Kanun ve Yönetmelik gereği en az 3(üç) ay önce Kuruma bildirim yapar ve kamuoyuna duyurur.

AYYILDIZİMZA, işletmenin durdurulması prosedürü uyarınca mevcut kullanıcı sertifikalar ile ilgili tüm bilgi, belge ve kayıtları, Kanun gereği 1(bir) ay içinde başka bir ESHS' ye devreder. Kurum uygun görmemesi halinde 1(bir) ayı geçmemek üzere ek süre verilir. Eğer verilen bu sürede de işlem tamamlanmaz ise, ilgili tüm sertifikaları iptal eder ve bu durumdan tüm sertifika sahipleri ve üçüncü kişileri haberdar eder. Bu durumda, AYYILDIZİMZA son SİL listesini imzalayıp yayınlandıktan sonra imza oluşturma verisi ile yedeklerini imha eder.

6. TEKNİK GÜVENLİK KONTROLLERİ

6.1. Anahtar Çifti Üretimi ve Kurulumu

6.1.1. Anahtar Çifti Üretimi

6.1.1.1 Elektronik Sertifika Hizmet Sağlayıcı Anahtar Çifti Üretimi

AYYILDIZİMZA Alt Kök sertifikalarına ait anahtar çiftleri, AYYILDIZİMZA merkezinde bulunan yüksek güvenlikli bölgeler içinde, Güvenilir Rollere atanmış az iki kişi ve gerekli yetkililer tarafından, FIPS-140-2 Seviye 3 veya EAL4+ özelliklerine sahip Güvenli Donanım Modülleri üzerinde güncel mevzuat ve standartlara uygun algoritmalar ve anahtar uzunlukları kullanılarak üretilir. Anahtar oluşturma işleminin tüm süreci kayıt ve tutanak altına alınır.

AYYILDIZİMZA Kök sertifikası anahtar çifti, Alt Kök anahtar çifti üretim prosedürüne ek olarak ancak aşağıdaki şartları yerine getirilmesi koşulu ile üretilir.

- Kök Sertifikası anahtar çifti üretimi birden fazla güvenilir personel, kurum imza yetkilisi, avukat ve bağımsız gözlemcilerin şahitliğinde anahtar üretim seremonisi yapılarak üretilir.
- Seremoninin tüm adımları yazılı ve görsel kayıt ile tutanak altına alınır.
- Seremoninin delilleri şahitler huzurunda paketlenir ve imzalanır.
- Kök Sertifikası anahtar çifti üretiminde kullanılacak güvenli donanım modülleri seremoni sırasında fabrika ayalarına çekilir ve en baştan yeniden yapılandırılır.

Anahtar çiftleri AYYILDIZİMZA Kök ve Alt Kök Sertifikalarına ait imza oluşturma ve doğrulama verileridir. İmza oluşturma verisi bulunduğu Güvenli Donanım Modülünden ancak aynı standartları destekleyen başka bir Güvenli Donanım Modülüne yedekleme amacı ile çıkartılabilir. Sürecin tüm adımları anahtar çiftlerinin güvenlik şartlarını sağlayacak şekilde yürütülür ve kontrol edilir.

6.1.1.2. Sertifika Sahibi Anahtar Çifti Üretimi

Sertifika sahiplerine ait anahtar çiftleri, AYYILDIZİMZA tarafından güncel mevzuat ve standartlara uygun algoritmalar ve anahtar uzunlukları kullanılarak Güvenli İmza Oluşturma Aracı üzerinde üretilir. Sertifika sahibine ait imza oluşturma verileri asla AYYILDIZİMZA tarafından saklanmaz ve kopyalanmaz. Sürecin tüm adımları anahtar çiftlerinin güvenlik şartlarını sağlayacak şekilde yürütülür ve kontrol edilir.

6.1.2. İmza Oluşturma Verisinin Sertifika Sahibine Ulaştırılması

Üretilen imza oluşturma verisi, güvenli imza oluşturma aracı içerisinde sertifika sahibine kargo veya kurye ile gönderilir. Sertifika sahibi ya da resmi olarak yetki vermiş olduğu gerçek kişi kayıt birimlerine gelerek de imza oluşturma verisini imza karşılığı teslim alabilir.

Güvenli elektronik imza oluşturma aracı erişim verisi, sertifika sahibinin başvuru sırasında beyan ettiği cep telefonuna gönderilidir.

6.1.3. İmza Doğrulama Verisinin ESHS 'ye Ulaştırılması

Anahtar çiftleri ESHS tarafından üretildiği için imza doğrulama verisinin ESHS'ye ulaştırılmasına gerek yoktur.

6.1.4. AYYILDIZİMZA İmza Doğrulama Verilerinin Üçüncü Kişilere Ulaştırılması

AYYILDIZİMZA Kök ve Alt Kök sertifikalarına ait imza doğrulama verileri ve sertifika özet değerli AYYILDIZİMZA web sitesi üzerindeki sertifika deposunda kesintisiz olarak üçüncü kişilerin erişime açık halde tutulur.

6.1.5. Anahtar Uzunlukları

Anahtar çiftleri oluşturulurken kullanılan anahtar uzunlukları Elektronik İmza ve İlgili Süreçlere ve Teknik Kriterlere ilişkin Tebliğ'e uygundur.

6.1.6. Anahtar Üretimi ve Kalite Kontrolü

Anahtar çiftleri "Tebliğ"e uygun olarak, kriptografik açıdan gerekli güvenlik şartlarını sağlayan algoritma ve parametreler ile Güvenli Donanım Modülleri üzerinde üretilir. Sürecin tüm adımlarının güvenlik şartlarını eksiksiz olarak sağladığı kontrol edilir.

6.1.7. Anahtar Kullanım Amaçları

AYYILDIZİMZA Kök ve Alt Kök Sertifikalarına ait anahtar çiftleri, SİL listesi, Zaman Damgası Sertifikası, ÇiSDUP Sertifikası ve sertifika zincirindeki diğer sertifikaları imzalamak için,

AYYILDIZİMZA ÇiSDUP Sertifikaları ait anahtar çiftleri, Çevirim İçi Sertifika Durum yanıtlarını imzalamak için,

AYYILDIZİMZA son kullanıcı sertifikalarına ait anahtar çiftleri ise kimlik doğrulama ve güvenli elektronik imza oluşturmak için kullanılır.

Anahtar kullanım amaçları, ilgili sertifikaların anahtar kullanım amacı alanı içerisinde tanımlanır.

6.2. İmza Oluşturma Verisinin Korunması ve Kriptografik Modül Mühendislik Kontrolleri

6.2.1. Kriptografik Modül Standartları ve Kontroller

AYYILDIZİMZA Kök ve Alt Kök sertifikalarına ait imza oluşturma verileri, "Tebliğ" e uygun olarak gerekli standartları taşıyan Güvenli Donanım Modülleri üzerinde üretilir.

Son kullanıcı sertifikalarına ait imza oluşturma verileri ise "Tebliğ"e uygun olarak Güvenli Donanım Modüllerinde ya da aynı standartları taşıyan Güvenli Elektronik İmza Oluşturma araçları üzerinde üretilir.

İmza oluşturma verilerinin oluşturduğu ve saklandığı bu donanımlar; FIPS-140-2 Seviye 3 veya EAL4+ standartlarını sağlar. Üzerinde barındırdıkları imza oluşturma verilerinin hiçbir koşulda dışarı çıkmasına izin vermez, üçüncü kişilerce elde edilememesini ve sahteciliğe karşı korunma sağlayacak teknik özelliklere sahiptir.

6.2.2. İmza Oluşturma Verisinin Çok Kullanıcılı Kontrolü

AYYILDIZİMZA Kök ve Alt Kök sertifikalarına ait imza oluşturma verisine erişim, yetkili en az iki güvenilir personelin kontrolünde sağlanır.

Son kullanıcı sertifikalarına ait imza oluşturma verisine erişim, sadece sertifika sahiplerinin kendi sorumluluğu altındaki "Erişim Verisi" ile sağlanır. Güvenli Elektronik İmza Aracı Erişim Verisi bilinmediği sürece İmza Oluşturma verisi kullanılamaz.

6.2.3. İmza Oluşturma Verisinin Saklanması

Uygulama dışıdır. Düzenlenmesine gerek duyulmamıştır.

6.2.4. İmza Oluşturma Verisinin Yedeklenmesi

AYYILDIZİMZA Kök ve Alt Kök sertifikalarına ait imza oluşturma verileri, AYYILDIZİMZA merkezindeki yüksek güvenlikli bölgeler de ve Güvenli Donanım Modülleri üzerinde yedeklenir.

Son kullanıcı sertifikalarına ait İmza Oluşturma Verisi AYYILDIZİMZA tarafından kesinlikle yedeklenmez.

6.2.5. İmza Oluşturma Verisinin Arşivlenmesi

Uygulama dışıdır. Düzenlenmesine gerek duyulmamıştır.

6.2.6. İmza Oluşturma Verisinin Kriptografik Modül Transferi

AYYILDIZİMZA Kök ve Alt Kök sertifikalarına ait imza oluşturma verileri Güvenli Donanım Modülleri üzerinde üretilir. İmza Oluşturma verileri kesinlikle dışarda üretilmez. AYYILDIZİMZA Kök ve Alt Kök sertifikalarına ait bu veriler sadece yedeklenmek amacı ile başka bir Güvenli Donanım Modülüne, transfer edilmek üzere mevcut modülünden çıkartılabilir. Yedekleme işlemi Yüksek Güvenlikli Bölgelerde, birden fazla yetkili kişinin kontrolünde yapılır.

Son kullanıcı sertifikalarına ait imza oluşturma verileri, Güvenli elektronik imza oluşturma araçları üzerinde üretilir, taşınır ve hiçbir koşulda dışarı çıkartılamaz.

6.2.7. İmza Oluşturma Verisinin Kriptografik Modülde Saklanması

AYYILDIZİMZA Kök ve Alt Kök sertifikalarına ait imza oluşturma verisi, AYYILDIZİMZA merkezindeki yüksek güvenlikli bölgelerde Güvenli Donanım Modüllerinde saklanır. Bölüm 6.2.6 haricinde dışarıya çıkartılamaz.

Son kullanıcı sertifikalarına ait imza oluşturma verileri, "Tebliğ" de tanımlı güvenlik standartlarına uygun Güvenli Elektronik İmza Oluşturma Araçlarında Saklanır. Güvenli Elektronik İmza Oluşturma aracından imza oluşturma verisi dışarıya çıkartılamaz.

6.2.8. İmza Oluşturma Verisinin Aktif Edilme Yöntemi

AYYILDIZİMZA Kök ve Alt Kök sertifikalarına ait imza oluşturma verileri, Güvenilir Donanım Modülleri üzerinde en az yetkili iki kişinin kontrolünde aktif edilir.

Son kullanıcı sertifikalarına ait imza oluşturma verileri, sertifika sahibinin Güvenli Elektronik İmza Aracı Erişim verisi ile aktif edilir. "Erişim Verisi" kaybolmasını önlemek ve gerekli tedbirleri almak sertifika sahibinin sorumluluğu altındadır.

6.2.9. İmza Oluşturma Verisinin Pasif Edilme Yöntemi

AYYILDIZİMZA Kök ve Alt Kök sertifikalarına ait imza oluşturma verileri en az yetkili iki kişinin kontrolünde pasif edilir.

6.2.10. İmza Oluşturma Verisinin Yok Edilmesi

AYYILDIZİMZA Kök ve Alt Kök sertifikalarına ait imza oluşturma verileri ve yedekleri, sertifika bitiş tarihinden sonra üzerinde bulunduğu Güvenli Donanım Modüllerinden cihazların anahtar silmek için tanımladığı prosedürler kullanarak geri dönülemez şekilde silinir. İmza Oluşturma Verisinin silinmesi birden fazla yetkili kişinin kontrolünde yapılır.

Son kullanıcı sertifikalarına ait imza oluşturma verileri, Sertifika Sahibinin kendisi tarafından Güvenli Elektronik İmza Oluşturma Aracı üzerinden silinmesi ya da cihazın imha edilmesi ile yok edilir.

6.2.11. Kriptografik Modülün Değerlendirilmesi

AYYILDIZİMZA Kök ve Alt Kök sertifikalarına ait imza oluşturma verileri, "Tebliğ" e uygun olarak gerekli standartları taşıyan Güvenli Donanım Modülleri üzerinde üretilir.

Son kullanıcı sertifikalarına ait imza oluşturma verileri ise "Tebliğ"e uygun olarak Güvenli Donanım Modüllerinde ya da aynı standartları taşıyan Güvenli Elektronik İmza Oluşturma araçları üzerinde üretilir.

6.3. Anahtar Çifti Yöntemi ile İlgili Diğer Konular

6.3.1. İmza Doğrulama Verilerinin Arşivlenmesi

AYYILDIZİMZA Kök ve Alt Kök sertifikalarına ait imza doğrulama verileri yasal düzenlemeler ve ilgili yönetmeliklerde belirtilen süre boyunca arşivlenir. Bu süreçte verilerin bütünlüğünün bozulmaması için gerekli tüm önlemler alınır.

6.3.2. Sertifikanın İşlevsel Süreleri ve Anahtar Çifti Kullanım Süreleri

AYYILDIZİMZA Kök ve Alt Kök sertifikalarının imza oluşturma verisinin süresi, yasal düzenlemeler ve ilgili yönetmeliklerde belirlenen süreyi geçemez ve sertifikanın bitiş tarihi ile sınırlıdır.

Sertifika sahiplerine ait imza oluşturma verisinin süresi ilgili sertifikanın bitiş tarihine kadardır.

Sertifika zincirindeki herhangi bir sertifikanın süresi, kendisini imzalayan bir üst sertifikanın bitiş süresinden fazla olamaz.

Sertifika sahiplerinin anahtar çifti kullanım süresi 3(üç) yılı geçemez. AYYILDIZİMZA yenileme işlemlerinde var olan anahtar çiftini kriptografik ömür güvenliği nedeniyle kullanmaz ve yeniden üretir.

6.4. Erişim Şifreleri

6.4.1. Erişim Şifrelerinin Oluşturulması ve Kurulumu

AYYILDIZİMZA, merkezindeki yüksek güvenlikli bölgelerde bulunan Güvenli Donanım Modüllerinin erişim şifreleri, yetkili kişilerin katılımı ile yapılan Anahtar Seremonisi sırasında oluşturulur ve tutanak altına alınır.

Son kullanıcı sertifikalarına ait erişim şifreleri, aktivasyon işlemi sırasında sertifika sahipleri tarafından belirlenir. Kullanıcılar üretim işlemi tamamlandıktan sonra başvuru sırasında beyan edilen cep telefonlarına aktivasyon kodu gönderilir. Sertifika sahibi bu aktivasyon kodu ile AYYILDIZİMZA aktivasyon uygulaması üzerinden şifre tanımlama işlemini gerçekleştirir.

6.4.2. Erişim Şifrelerinin Korunması

AYYILDIZİMZA merkezindeki Güvenli Donanım Modüllerinin erişim şifresi yalnızca yetkili kişiler tarafından bilinir. Yetkili kişiler erişim şifrelerinin gizliliğinden ve korunmasından sorumludur.

Son kullanıcılara ait Güvenli Elektronik İmza Oluşturma Aracı erişim verisinin korunması, sertifika sahiplerinin sorumluluğu altındadır.

6.4.3. Erişim Şifreleriyle ilgili Diğer Konular

Uygulama dışıdır. Düzenlenmesine gerek duyulmamıştır.

6.5. Bilgisayar Güvenlik Kontrolleri

6.5.1. Bilgisayar Güvenliği Teknik Gereklilikleri

AYYILDIZİMZA, sertifika yönetim sürecinde bünyesinde kullanılan donanım ve yazılımlar, bilgi güvenliği gereksinimleri doğrultusunda en son teknolojik gelişmeler göz önünde bulundurularak gerekli tüm güvenlik unsuları uygulanarak kontrol edilir ve işletilir.

6.5.2. Bilgisayar Güvenliğinin Derecelendirilmesi

Uygulama dışıdır. Düzenlenmesine gerek duyulmamıştır.

6.6. Yaşam Döngüsü ve Teknik Kontrolleri

6.6.1. Sistem Geliştirme Kontrolleri

AYYILDIZİMZA, sertifika yaşam döngüsünü yürütürken kullandığı sistemlerin geliştirme kontrollerini, ISO/IEC 27001, ISO 9001 denetimleri sonucu ortaya çıkan bulguları göz önüne alarak ve AYYILDIZİMZA güvenlik prosedürlerinin uygulanması ile sağlar.

6.6.2. Güvenlik Yönetimi Denetimleri

Sertifika yaşam döngüsünü yürütürken periyodik olarak ISO/IEC 27001 standartları uygun olarak denetimler gerçekleştirilir.

6.6.3. Yaşam Döngüsü Güvenlik Kontrolleri

Uygulama dışıdır. Düzenlenmesine gerek duyulmamıştır.

6.7. Ağ Güvenlik Kontrolleri

AYYILDIZİMZA sistemleri içine alan ağ yapısı, en son teknolojik gelişmeler göz önünde bulundurularak gerekli tüm ağ güvenliği denetimlerinden periyodik olarak geçirilir.

6.8. Zaman Damgası

AYYILDIZİMZA Sertifika hizmetleri verirken kullanılan her türlü cihaz ve yazılım, zaman bilgisini, zaman damgası hizmetlerinde kullanılan zaman kaynağı ile eşleştirir.

Zaman damgası ile ilgili ayrıntılı bilgi, Zaman Damgası İlkeleri ve Zaman Damgası Uygulama Esasların da açıklanmıştır.

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

Bu bölümde AYYILDIZİMZA tarafından üretilen nitelikli elektronik sertifikaların ve bu sertifikaların geçerliliğini kontrol etmek için kullanılan SİL ve ÇİSDUP servisinin profilleri anlatılmaktadır.

7.1. Sertifika Profili

AYYILDIZİMZA tarafından üretilen NES sertifikaları,

- ITU-T X.509 The Directory: Public-key and attribute certificate frameworks,
- "IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile",
- Bilgi Teknolojileri ve İletişim Kurumu "Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri"

Uygun olarak üretilmektedir.

7.1.1. Sürüm Numarası

AYYILDIZİMZA tarafından üretilen NES sertifikaları, "IETF RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" dokümanına uygun olarak X.509 v3 sürümüne uygun olarak üretilir.

7.1.2. Sertifika Uzantıları

AYYILDIZİMZA tarafından üretilen NES'ler, "IETF RFC 3739 Internet X.509 Public Key Infrastructure Qualified Certificates Profile" ve "Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri" dokümanlarında tanımlanan nitelikli sertifika uzantılarını içermektedir. AYYILDIZİMZA NES sertifika uzantıları aşağıdaki tabloda yer almaktadır.

Uzantı Adı	Kritik Uzantı	Açıklama
BasicConstraints (Temel Kısıtlar)	Hayır	Sertifikanın son kullanıcı (End Entity) sertifikası olduğunu ve başka bir sertifikayı imzalamak amacı ile kullanılamayacağını belirtir.
Subject Alternative Name (Alternatif özne adı)	Hayır	İsteğe bağlı olarak sertifika sahibinin, mail adresi yer alır.
Qualified Certificate Statements (Nitelikli Sertifika İbareleri)	Evet	ETSI 101 862'ye göre, id-etsi-qcs-QcCompliance= 0.4.0.1862.1.1 nesne tanımlama numarasını ve varsa sertifikanın kullanımına ilişkin maddi sınır bilgisini içerir. BTK tarafından belirlenen nitelikli elektronik sertifika ibaresi ile bu ibareye ait nesne tanımlama numarası *2.16.792.1.61.0.1.5070.1.1* bilgisini içerir.
CRL Distribution Points (SİL Dağıtım Noktaları)	Hayır	AYYILDIZİMZA nitelikli alt kök sertifikası tarafından imzalanmış olan SİL (CRL) dosyasının HTTP URL adresi.
Authority Information Access (ESHS Bilgi Erişimi)	Hayır	AYYILDIZİMZA ÇİSDUP(Ocsp) servis adres bilgisi ve kök sertifika erişim URL adresleri içerir
Key Usage (Anahtar Kullanımı)	Evet	Digital signature (elektronik imza) ve non-repudiation (inkâr edilemezlik) kullanım anahtarları bulunmaktadır.

CertificatePolicies (Sertifika İlkeleri)	Hayır	AYYILDIZİMZA NESİ dokümanına ait nesne tanımlama numarası (2.16.792.3.0.60.1.1.1) ile NESUE dokümanının bulunduğu http://ayyildizimza.com.tr/bilgidepo internet adresini ve BTK tarafından oluşturulan NES ibaresine ait metni içerir.
SubjectKeyIdentifier (Sertifika Anahtar Tanımlayıcı)	Hayır	Sertifikanın içeriğindeki "subjectPublicKey" parmak izi değeri
AuthorityKeyIdentifier **(**ESHS Anahtar Tanımlayıcı**)**	Hayır	AYYILDIZİMZA nitelikli alt kök sertifikasını açık anahtar parmak izi değeri

7.1.3. Algoritma Nesne Tanımlayıcıları

AYYILDIZİMZA tarafından oluşturulan, tüm sertifikalar aşağıdaki algoritmalardan biri ile imzalanmaktadır. Sertifika içinde aşağıdaki nesne tanımlayıcıları ile belirtilmektedir.

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

7.1.4. İsim Biçimleri

AYYILDIZİMZA tarafından üretilen tüm sertifikalarda X500 standardına uygun olarak ayırt edici isimler kullanılır.

Ayırt Edici İsim	Açıklama	
SERIALNUMBER	Sertifika sahibinin TC Kimlik Numarası, yabancılar için ise Ülke Kodu ve PasaportNo	Zorunlu
CN	Sertifika sahibinin Açık ve Tam ismi	Zorunlu
O	Kurumsal Sertifika ise Organizasyon (Şirket Unvanı) bilgisi	Opsiyonel
OU	Şirket içindeki organizasyon birimi	Opsiyonel
T	Kişinin Meslek Unvanı	Opsiyonel
L	Kişinin Yaşadığı Şehir	Opsiyonel
C	"TR"	Sabit

7.1.5. İsim Kısıtları

AYYILDIZİMZA son kullanıcı nitelikli elektronik sertifikalarında anonim veya takma adlar kullanılmaz. Türkiye Cumhuriyeti Vatandaşları için T.C. Kimlik Numarası ve yabancı kişiler için, uluslararası ülke kodu ve pasaport numarası, ayırt edici alan olarak kullanılmaktadır.

7.1.6. Sertifika İlkeleri Nesne Tanımlayıcısı

Sertifika ilkeleri nesne tanımlayıcı numarası, bu doküman (NESİ) bölüm 1.2'de verilmiştir.

7.1.7. İlke Kısıtları Uzantısının Kullanımı

AYYILDIZİMZA, alt kök sertifikalarında ilke kısıtlaması uzantısı kullanabilir.

7.1.8. İlke Niteleyicilerin Yazımı

AYYILDIZİMZA tarafından üretilen sertifikaların "sertifika ilkeleri uzantısı" içinde, ilke niteleyicisi olarak NESUE dokümanı internet adresi ve nesne tanımlayıcı numarası olarak da bölüm 1.2'deki NESİ nesne tanımlayıcı numarası yer almaktadır. Ayrıca QC Statement-Statement ID alanında "Bu sertifika, 5070 sayılı Elektronik İmza Kanunu'na göre nitelikli elektronik sertifikadır" ibaresi yer almaktadır.

7.1.9. Kritik Sertifika İlkeleri Uzantısının İşlenme Semantiği

Uygulama dışıdır. Düzenlenmesine gerek duyulmamıştır.

7.2. SİL Profili

AYYILDIZİMZA tarafından yayımlanan SİL'ler "IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" ve BTK tarafından yayımlanan "Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri" dokümanına uygundur.

7.2.1. Sürüm Numarası

AYYILDIZİMZA tarafından üretilen tüm SİL'ler ITU X.509 v2 sürümünü desteklemektedir.

7.2.2. SİL ve SİL Giriş Uzantıları

AYYILDIZİMZA tarafından yayımlanan SİL'lerde, "IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" ve BTK tarafından yayımlanan "Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri" dokümanlarında tanımlanan uzantılar kullanılmaktadır.

7.3. ÇİSDUP(OCSP) Profili

AYYILDIZİMZA tarafından yayımlanan son kullanıcı sertifikalarının anlık durumunu öğrenmek için, ÇİSDUP servisleri 7/24 kesintisiz olarak sunulmaktadır. AYYILDIZİMZA tarafından verilen ÇİSDUP servisleri "IETF RFC 6960 Internet X.509 Public Key Infrastructure Online Certificate Status Protocol -

OCSP" ve BTK tarafından yayımlanan "Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri" dokümanlarına uygun olarak verilmektedir.

7.3.1. Sürüm Numarası

AYYILDIZİMZA ÇİSDUP(OCSP) hizmeti "IETF RFC 6960" dokümanına uygun olarak v1 protokol sürümünü desteklemektedir.

7.3.2. ÇİSDUP uzantıları

AYYILDIZİMZA ÇİSDUP hizmeti, IETF RFC 6960 ve BTK tarafından yayımlanan "Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri" dokümanında belirtilen uzantıları desteklemektedir. BTK dokümanı içindeki zorunlu ve tavsiye edilen uzantılar dışında, tümünün kullanımı zorunlu değildir.

8. UYGUNLUK DENETİMİ VE DİĞER DEĞERLENDİRMELER

AYYILDIZİMZA, ilgili elektronik imza kanunu gereğince BTK tarafından denetlenir. BTK, AYYILDIZİMZA'nın mevzuat ve standartlara uygunluğunu, NESİ ve NESUE'ye uygun üretim ve dağıtım süreçlerinin uygulanıp uygulanmadığını denetlemektedir.

AYYILDIZİMZA, ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi kurallarına uygunluğu bağımsız ve akredite olmuş yetkili kuruluşlar tarafından yapılmaktadır. Denetim kapsamı ISO/IEC 27001 maddelerinin hepsini kapsamaktadır.

Kendi iç işleyişini kontrol etmek ve iyileştirmek için, ayrıca iç denetimler gerçekleştirmektedir. İç denetimlerin içeriği, AYYILDIZİMZA'nın uyması gereken mevzuat ve standartlara bağlı olarak, kendi personeli tarafından belirlenmektedir.

8.1. Denetim Sıklığı ve Durumları

BTK (Bilgi Teknolojileri Kurumu), denetleyici ve düzenleyici kurumdur. Gerekli gördüğü zamanda denetleme yetkisine sahip olmak ile birlikte en az 2 yılda bir denetim gerçekleştirir.

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi uygunluk denetimleri her yıl bağımsız denetçiler tarafından yapılmaktadır.

İç denetimler AYYILDIZİMZA iç denetim komitesi tarafından, ISO/IEC 27001 Bilgi Güvenliği Yönetim sistemi süreçleri gereğince, en az yılda 2 defa yapılmaktadır. İç denetim komitesi gerek görüldüğü durumlarda, bu periyottan bağımsız olarak da denetimlerini sıklaştırabilir.

8.2. Denetçinin Kimliği ve Özellikleri

BTK tarafından yapılan denetimler, BTK tarafından görevlendirilmiş yetkili personel tarafından gerçekleştirilir.

ISO/IEC 27001 BGYS denetimleri bağımsız ve akredite olmuş kuruluşlar ve onların yetkilendirdiği elemanlarıdır.

İç denetim, NESİ ve NESUE dokümanı gereklerini, uyulması gereken mevzuat ve standartları iyi anlayan, uygunluk denetimi konusunda tecrübeli AYYILDIZİMZA iç denetim komitesi personelleri tarafından gerçekleştirilir.

8.3. Denetçinin ESHS ile İlişkisi

BTK, Kanun ile yetkili kılınmış denetçi ve düzenleyici kuruluştur. BTK denetçileri kendi personeli veya yetkilendirdiği diğer kişilerden oluşmaktadır. AYYILDIZİMZA ile herhangi bir ticari veya yasal bağları yoktur.

ISO/IEC 27001 denetçileri, bağımsız ve yetkili denetçi kuruluşlar ve onların yetkilendirilmiş çalışanlarıdır. Bağımsız denetçilerin AYYILDIZİMZA ile herhangi bir ticari veya yasal bağları yoktur.

İç denetçiler, AYYILDIZİMZA kendi personelinden oluşmaktadır.

8.4. Denetimde Kapsanan Başlıklar

BTK, AYYILDIZİMZA'nın elektronik sertifika hizmetlerine ait tüm süreçlerini ve bu hizmetleri yerine getirirken kullandığı tüm yapının NESi ve NESUE'ye uygunluğunu denetler.

ISO/IEC 27001 denetçileri, AYYILDIZİMZA'nın işleyişinin ISO/IEC 27001 uygunluğunu denetler.

İç denetçiler, yasal denetime giren tüm konuları kapsamaktadır.

8.5. Eksiklik Durumunda Yapılacaklar

BTK tarafından yapılan denetimlerde herhangi bir uygunsuzluk bulunması durumda, ilgili mevzuatta öngörülen yaptırım ve cezalar uygulanır.

ISO/IEC 27001 BGYS denetimleri sırasında majör seviyede eksiklik bulunması ve eksiklik sayısı, sertifikanın geri alınmasına sebep olabilir. Minör seviyede ki eksiklikler, bir sonraki denetimde ilk denetlenecek maddeler arasında yer almak şartı ile, daha sonra giderilebilir.

İç denetimlerde bulunan eksiklikler için en kısa sürede düzeltici ve önleyici faaliyetler yürütülür.

8.6. Sonuçların Bildirilmesi

BTK tarafından yapılan denetim sonuçları, gerek duyulduğu takdirde resmi yollar ile iletilmektedir. BTK tarafından herhangi bir bildirimde bulunulmamış olması, denetim sonuçlarının olumsuz olmadığı anlamını taşımaktadır.

ISO/IEC 27001 denetim sonuçları denetçi firma tarafından resmi olarak, AYYILDIZİMZA'ya bildirilmektedir. AYYILDIZİMZA denetim sonuçlarını kendi web sayfasında,

İç denetim sonuçları, denetleme sonrası iç denetim sonuç raporu olarak hazırlanır ve üst yönetime sunulur.

9. DİĞER İŞ KONULARI ve YASAL KONULAR

9.1. Ücretler

9.1.1. Sertifika Üretim ve Yenileme Ücretleri

Sertifika üretimi ve yenileme için ücret alınmaktadır. Güncel sertifika ücretlerine AYYILDIZİMZA web sayfası https://ayyildizimza.com.tr üzerinden yayınlanmaktadır.

ESHS'nin imza oluşturma verisinin çalınması, kaybolması, gizliliğinin veya güvenilirliğinin ortadan kalkması ya da sertifika ilkelerinin değişmesi gibi sertifika sahibinin kusurunun bulunmadığı durumların sonucunda nitelikli elektronik sertifikaların ESHS tarafından iptal edilmesi ve yenilenmesi halinde, yenileme işlemleri için hiçbir ücret talep edilemez.

9.1.2. Sertifika Erişim Ücretleri

Son kullanıcı sertifikası, son kullanıcının yazılı izni ile aktif dizinde yayınlanır ve herhangi bir ücret talep edilmez.

9.1.3. İptal ve Durum Bilgisi Erişim Ücretleri

Sertifika iptal veya durum bilgisi erişimi için, yasal düzenlemelere göre ücret talep edilmez.

9.1.4. Diğer Hizmetlerin Ücretleri

AYYILDIZİMZA kamuya açık yayınladığı belgelerden ücret talep edilmez. Diğer hizmetleri içeren fiyat bilgisi ihttps://ayyildizimza.com.tr yayımlanmaktadır.

9.1.5. Bedel İadesi

AYYILDIZİMZA, sertifika ücretlerinde bedel iadesi yapmaz. Ancak AYYILDIZİMZA dan kaynaklanan nedenler ile sertifika içindeki bilgiler, başvurudaki kullanıcı bilgileri ile aynı değilse herhangi bir ücret talep edilmeden yeni bir sertifika verilir veya talep edilmesi halinde ücret iadesi yapılır. AYYILDIZİMZA hizmet bedelini peşin olarak tahsil eder ve ancak aşağıdaki şartlar gerçekleşmesi halinde ücret iadesi yapılır.

- AYYILDIZİMZA tarafından yapılan incelemeler sonucunda başvurunun ret edilmesi.
- Teknik destek birimi tarafından Aktivasyon /Kurulum işlemleri sırasında Güvenli Elektronik İmza oluşturma aracının bozuk / arıza tespiti,
- Sertifika sahibi tarafından teslim alınan ürünlere ayıplı bir durum söz konusu ise sertifika sahibi 14 gün içerisinde AYYILDIZİMZA'ya bildirmekte yükümlüdür. Durumun tespitine müteakip başvuru sahibine ücret iadesi yapılır.

AYYILDIZİMZA, güvenli elektronik imza aracının, kullanıcı hataları sebebi ile (ezilme, kırılma, kaybetme, darp edilmesi vb.) işlevsiz hale gelmesi durumunda bedel iadesi yapmaz.

9.2. Finansal Sorumluluk

9.2.1. Sigorta Kapsamı

AYYILDIZİMZA, kanundan doğan sorumlulukları yerine getirmemesi sonucu, doğacak zararların karşılanması amacıyla nitelikli elektronik sertifika sahibine teslim edilmeden önce "Sertifika mali sorumluluk sigortası" yaptırmak zorundadır.

Sertifika mali sorumluluk sigortası, elektronik sertifika hizmet sağlayıcısının 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. Düzenlenmesine gerek duyulmamıştır.

9.2.3. Son Kullanıcılar İçin Sigorta veya Diğer Garantilerin Kapsamı

Bu doküman (NESİ) bölüm 9.2.1 yer alan ilkeler uygulanır.

9.3. İş Bilgisinin Gizliliği

9.3.1. Gizli Bilginin Kapsamı

AYYILDIZİMZA ESHS faaliyet sürecinde aşağıda yer alan bilgiler gizli bilgi kapsamındadır;

- AYYILDIZİMZA kök ve alt kök imza oluşturma verisi,
- NES sahiplerinin, kanun kapsamında kişisel veri olarak sayılan bilgileri, operasyonel kayıtlar,
- BGYS kapsamında gizli sayılan tüm bilgi ve belgeler,
- AYYILDIZİMZA'nın ticari faaliyetlerine ait her türlü gizli bilgi ve belgeler,
- Yüksek güvenlikli bölgeler içinde bulunduğu tesisin planları,
- Yüksek güvenlikli bölgeler içindeki network ve sistemlerin fiziksel ve mantıksal yapı şemaları,
- Yüksek güvenlikli bölge de çalışan her türlü yazılım ve donanım ile ilgili her türlü teknik bilgilerdir.

9.3.2. Gizlilik Kapsamı Dışındaki Bilgi

NES sahibinin ortak dizinde yayınlanmasına izin verdiği sertifikalar, SİL'ler, NESİ dokümanı, NESUE dokümanı, kullanıcı sözleşmeleri içeriğindeki bilgiler gizlilik kapsamına girmez.

9.3.3. Gizli Bilginin Korunması Sorumluluğu

BGYS politikaları gereği, her bilgiye yetkilisi dışında erişim verilmemekte ve üçüncü kişiler ile paylaşılmaz. Bilgi güvenliğinin sağlanması ile ilgili tüm prosedürler personel tarafından eksiksiz uygulanır.

9.4. Kişisel Bilgilerin Gizliliği

9.4.1. Gizlilik Planı

AYYILDIZİMZA, 6698 sayılı Kişisel Verilerin Korunması Kanunu uyarınca, çalışanlarının, sertifika başvuru sahiplerinin, sertifika sahibi müşterilerinin kişisel verilerinin gizliliğini sağlar ve korur.

9.4.2. Özel Olarak Değerlendirilecek Bilgi

Sertifika hizmetlerinin verilmesi için, sertifika başvuru sahibinden alınan her türlü bilgi ve belge, sertifika hizmetlerinin yürütülmesi için kullanılacak olup, sertifika içeriğinde ve SİL'de yer almayan her türlü bilgi özel bilgi olarak sayılır.

9.4.3. Özel Sayılmayacak Bilgi

NES ve SİL herkesin erişimine açık bir şekilde yayınlana her türlü bilgi özel sayılmayan bilgilerdir.

9.4.4. Özel Bilgiyi Koruma Sorumluluğu

AYYILDIZİMZA, tüm çalışanları ile birlikte, sertifika hizmetlerini yürütmek için başvuru sahiplerinden ve müşterilerinden topladığı kişisel verilerden sorumludur. Hiçbir veriye yetkilisi dışında ve üçüncü kişilerin erişimine izin verilmez.

9.4.5. Özel Bilgiyi Kullanma Bildirimi ve Onayı

AYYILDIZİMZA sertifika hizmetlerini yürütmek için kişisel verileri gerektiğinde kullanır. Ayrıca müşterilerine daha iyi hizmet vermek için kullanıcıların izni dahilinde yeni kampanya ve uygulamaları duyurmak amaçlı kullanabilir.

9.4.6. Yargısal ve İdari Süreçlere Uygun Olarak Bilginin Açıklanması

Sertifika sahibinin özel bilgileri, sadece talep eden resmi makama veya sertifika sahibinin kendisine verilir.

6698 sayılı Kişisel Verilerin Korunması Kanunu 11. Maddesi uyarınca, kişiler yazılı olarak AYYILDIZİMZA'ya başvurup kişisel verileri ile ilgili bilgi ve işlemleri takip edebilirler. Yasal düzenleme gereği, 30 gün içinde e-posta veya yazılı olarak AYYILDIZİMZA tarafından bilgi verilir.

9.4.7. Bilginin Açıklandığı Diğer Durumlar

Uygulama dışıdır. Düzenlenmesine gerek duyulmamıştır.

9.5. Fikri Mülkiyet Hakları

AYYILDIZİMZA tarafından bilgi deposunda yayınlanan NESİ, NESUE ve son kullanıcı sözleşmeleri, https://ayyildizimza .com.tr adresinde yayınlanan her türlü görsel ve işitsel bilginin fikri ve mülkiyet hakları AYYILDIZİMZA'ya aittir.

9.6. Sorumluluklar

9.6.1. ESHS Beyan ve Garantileri

AYYILDIZİMZA, NESİ ve NESUE de yer alan tüm maddelerin gerekliliklerini yerine getireceğini, sürekli güncel ve doğru sertifika durum bilgisi sağlayacağını, kimlik doğrulama işleminin güvenilir bir şekilde yürütüldüğünü, kişisel verilerin resmi makamlar veya kişisel veri sahibi istemediği sürece, üçüncü kişilerin erişimine kapalı olacağını, sertifika içindeki bilgileri ve doğru kişiye üretildiğini ve teslim edildiğini garanti eder.

9.6.2. Kayıt Kayıt birimleri Sorumlulukları

AYYILDIZİMZA sertifika kayıt birimleri, başvuru sahibi tüzel veya bireysel kişilerin bilgilerinin doğruluğunu NESİ ve NESUE dokümanına uygun ve doğru bir şekilde tespit ettiklerini, yeni sertifika üretimi, sertifika yenileme ve iptal taleplerinin doğru ve eksiksiz olduğunu garanti eder.

9.6.3. Sertifika Sahibi Sorumlulukları

Sertifika sahibi son kullanıcılar, sertifika başvurusu, yenileme ve iptal işlemleri sırasında güncel ve doğru bilgi verdiklerini, sertifikalarını NESİ ve NESUE'ye uygun bir şekilde kullanacaklarını garanti eder.

9.6.4. Üçüncü Kişilerin Sorumlulukları

Sertifikanın "Nitelikli Elektronik Sertifika" olup olmadığını kontrol etmekle, nitelikli elektronik sertifikanın iptal ve geçerlilik durumunu kontrol ederek güvenli elektronik imza doğrulaması yapmakla nitelikli elektronik sertifikanın kullanımına yönelik herhangi bir kısıtlamanın olup olmadığını kontrol etmekle yükümlüdür.

9.6.5. Diğer Katılımcıların Sorumlulukları

AYYILDIZİMZA sertifika hizmetlerini yürütürken, hizmet aldığı ve iş birliği yaptığı kişi ve kuruluşlar, diğer katılımcılar olarak adlandırılmaktadır. Diğer katılımcılar ile hizmet ve gizlilik sözleşmeleri yaparak, sertifika sahiplerinin kişisel verilerini açığa çıkarmayacağını ve alınan servisin doğru ve güvenilir olduğunu garanti altına alır.

9.7. Sorumlulukların Geçersiz Olduğu Durumlar

Uygulama dışıdır. Düzenlenmesine gerek duyulmamıştır.

9.8. Sorumluluk Sınırları

ESHS ve Nitelikli Elektronik Sertifika sahibinin sorumlulukları, 5070 sayılı Elektronik İmza Kanunu, Telekomünikasyon Kurumu'nun yayımladığı Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik, Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de belirtilen şartlar ile sınırlıdır.

9.9. Tazminatlar

AYYILDIZİMZA, yasa ve yönetmelikte belirtilen yükümlülükleri ile birlikte NESİ ve NESUE de yayımlandığı ilke ve esasları yerine getiremez ve bu durumdan üçüncü kişiler zarar görürse, ilgili zarar AYYILDIZİMZA Kanun'un 13. Madde gereği tarafından tazmin edilir.

Eğer, Sertifika sahipleri başvuru sırasında imzaladığı NES Taahhütnamesi şartlarını yerine getiremez ve bu durumdan AYYILDIZİMZA ve üçüncü kişiler zarar görürse, bu zararın taziminden sertifika sahibi yükümlüdür.

Kurumsal NES sahipleri, kurumsal başvuru sözleşmesi yükümlülüklerini ihlal etmesi halinde AYYILDIZİMZA ve üçüncü kişilere karşı oluşabilecek zararın tanziminden sorumludur.

9.10. NESUE Dokümanın Geçerliliği

9.10.1. NESUE Dokümanın Geçerlilik Dönemi

NESUE dokümanının bu sürümü, AYYILDIZ imza web sitesinde (https://ayylidizimza.com.tr) yeni bir versiyon yayımlanana kadar geçerlidir.

9.10.2. NESUE Dokümanının Geçerliliğinin Sona Ermesi

Kanun ve yönetmeliklerde yapılacak değişiklikler veya AYYILDIZİMZA faaliyet ve sertifika hizmetlerinde oluşabilecek değişiklikler sebebi ile NESUE dokümanı değişiklik gerektirebilir. Bu durumda hizmet kesintisi olmadan yeni bir sürüm hazırlanır ve web sayfasında yayımlanır.

9.10.3. Geçerliliğin Sona Ermesinin Etkileri ve İşlerliğin Sürdürülmesi

AYYILDIZİMZA herhangi bir hizmet kesintisi olmaması için, NESUE dokümanı geçerliliği sona ermeden yeni bir sürüm hazırlar ve https://ayyildizimza.com.tr adresinde yayımlar. Geçerliliği sona eren NESİ dokümanının maddeleri bağlayıcı değildir.

9.11. Taraflara Özel Duyurular ve İletişim

AYYILDIZİMZA tarafından sertifika sahiplerine yapılacak duyurular için başvuru sırasında beyan ettiği iletişim kanalları kullanılır.

AYYILDIZİMZA üçüncü kişilere duyurularını ise web sitesi ya da basın yayın organları üzerinden yayımlanır.

9.12. Değişiklikler

AYYILDIZİMZA ESHS faaliyet sürecinde iş akışlarında bir değişiklik olması durumunda mevcut NESİ dokümanının değişiklik ve düzenlenmesine gerek olup olmadığını şirket içinde Bilgi Güvenliği Kurulu tarafından görüşülür. NESİ dokümanının güncellenmesine karar verilirken bu değişikliğin mevcut hali hazırda kullanılmada olan sertifikaların geçerliliğini etkilememesini kontrol altında tutar fakat bu değişiklikler mevcut sertifikaların kullanımına doğrudan da etki edebilir. Böyle bir durumda AYYILDIZİMZA gerekli aksiyon planı yaparak kullanıcılarını bilgilendirir.

9.12.1. Değişiklik Prosedürü

AYYILDIZİMZA ESHS faaliyetleri sürecinde, değişikliklere bağlı olarak gerek görmesi durumunda yeni bir NESİ dokümanı oluşturur ve yayımlar.

NESİ ve NESUE dokümanlarında meydana gelebilecek değişikliklerden Bilgi Güvenliği Kurulu sorumludur. Yönetim gözden geçirme toplantılarında da bu değişiklikler gündeme alınarak ve her yıl incelenir.

NESİ de yer alan ilkeler de oluşan değişiklikler, NESUE de bulunan uygulama esaslarına yansıtılır. AYYILDIZİMZA ürettiği NES içerisine, sertifika ilkeleri uzantısında bulunan URL adresini değiştirmez ve her zaman en son versiyon NESUE'ye referans eder.

NESİ ve NESUE yeniden hazırlanması gerektiren durum, daha önce üretilmiş sertifikaları etkilemeyecek ise yeni NESİ ve NESUE'ye uygun olarak bu sertifikalar kullanılmaya devam edilebilir. Şayet güncelleme gerektiren durum mevcut sertifikaların geçerliliğini etkileyecek ise mevcut müşteriler bilgilendirilir ve gerekli planlama yapılır.

9.12.1. Duyuru Mekanizması ve Süresi

AYYILDIZİMZA faaliyetleri sürecinde iş akışlarındaki değişiklikleri ile mevcut NESİ ve NESUE kitapçıklarında değişiklik oluşması durumunda, çıkarılan güncel NESİ ve NESUE sürümleri hakkında sertifika sahipleri ve üçüncü kişiler derhal bilgilendirilir.

Kritik öneme sahip değişikliklerde, sertifikanın kullanılabilirliği ve kabul edilirliği bazı uygulamalarda etkilenebileceğinden, AYYILDIZİMZA sertifika sahipleri ile üçüncü kişileri bilgilendirebilmek için tüm makul imkanları kullanır.

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

9.12.3. Nesne Tanımlayıcı Numaralarının Değişmesini Gerektiren Durumlar

Sertifika kullanımını ve kabul edilirliğini direkt olarak etkileyebilecek olan, kullanılan kimlik doğrulama adımlarını önemli ölçüde etkileyen veya sertifika hizmetlerinde sertifikanın güvenlik düzeyine etki edebilecek biçimde gerçekleşen önemli değişiklikler, NESUE dokümanında tanımlanan ilgili sertifika uygulama esaslarının nesne tanımlayıcı numaralarının da değişmesini gerektirebilir. Böyle bir durumda, yeni üretilen sertifikalarda, uygulanacak olan yeni sertifika uygulama esaslarının nesne tanımlayıcı numaraları yer alır.

9.13. Anlaşmazlıkların Çözümü

AYYILDIZİMZA, 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 AYYILDIZİMZA tarafından Kanun ve Yönetmelikler ile bunlara bağlı Tebliğler uyarınca yürütülür.

Taraflar arasındaki anlaşmazlıklar karşılıklı çözüme kavuşmadığı takdirde, anlaşmazlıkların çözümü için İstanbul 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. İlgi Yasalar Uygunluk

AYYILDIZİMZA, 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. Düzenlenmesine gerek duyulmamıştır.

9.16.2. Görevlendirme

Uygulama dışıdır. Düzenlenmesine gerek duyulmamıştır.

9.16.3. Kitapçık Kısımlarının Ayrılabilirliği

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

9.16.4. Yasal Haklardan Vazgeçme

Uygulama dışıdır. Düzenlenmesine gerek duyulmamıştır.

9.16.5. Mücbir Sebepler

AYYILDIZİMZA'nın 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, AYYILDIZİMZA faaliyetleri aksaklığa veya kesintiye uğrayabilir. Pandemi (Salgın, doğal afetler, savaşlar, terör, telekomünikasyon, İnternet vb.) diğer altyapılarda oluşabilecek aksaklıklar mücbir sebep kabul edilir.

9.16.5. Diğer Hükümler

Uygulama dışıdır. Düzenlenmesine gerek duyulmamıştır.