AYYILDIZ

İMZA BİLGİ GÜVENLİĞİ A.Ş

Sürüm-1

Zaman Damgası Sertifika İlkeleri

(Zİ)

3 Haziran 2021

OID:2.16.792.3.0.60.2.1.1

www.ayyildizimza.com.tr

İçindekiler

KAPAK
1. GİRİŞ 5
1.1. Genel Bakış 5
1.2. Kitapçık Adı ve Tanımlama 6
1.3. Taraflar 6
1.3.1. Elektronik sertifika Hizmet Sağlayıcı 6
1.3.2. Zaman Damgası Sahipleri 6
1.3.3. Üçüncü Kişiler 7
1.3.4. Diğer Katılımcılar 7
1.4. Zaman Damgası İlkelerinin Yönetimi 7
1.4.1. Zİ Dokümanından sorumlu Organizasyon 7
1.4.2. İletişim Noktası 7
1.4.3. Zİ'nin İlkelere Uygunluğunun Belirlenmesi 8
1.4.3. Zİ Onaylama Prosedürleri 8
1.5. Kısaltmalar ve Tanımlar 8
1.5.1. Kısaltmalar 8
1.5.2. Tanımlar 10
2. YAYIN VE BİLGİ DEPOSU SORUMLULUKLARI 15
2.1. Bilgi Deposu 15
2.2. Zaman Hizmeti ve İlgili Bilgilerinin Yayımlanması 15
2.3. Yayımlanma Zamanı ve Sıklığı 16
2.4. Bilgi Deposuna Erişim Kontrolleri 16
3. ZAMAN DAMGASI İŞLEVSEL GEREKLİLİKLERİ 16
3.1. Zaman Damgası 16
3.1.1. UTC ile Zaman Birliği Sağlanması 16
3.2. Zaman Damgası Başvurusu 17
3.2.1. Kimler Zaman Damgası Başvurusunda Bulunabilir? 17
3.2.2. Zaman Damgası Başvuru Kayıtları 17
3.2.3. Zaman Damgası Başvurularının Doğrulanması 17

3.3. Zaman Damgası Üretimi 17
3.3.1. Zaman Damgası İsteği Gönderimi 17
3.3.2. Zaman Damgası İsteğinin İşlenmesi ve Üretim 17
3.3.3. Zaman Damgasının Gönderilmesi 18
4. TESİS, YÖNETİM VE İŞLETMEYLE İLGİLİ KONTROLLER 18
4.1. Fiziksel Kontroller 18
4.1.1. Tesis Yeri ve İnşaatı 18
4.1.2. Fiziksel Erişim 18
4.1.3. Güç Kaynakları ve Havalandırma 19
4.1.4. Su Baskınları 19
4.1.5. Yangın Önleme ve Yangından Korunma 19
4.1.6. Saklama Ortamları 19
4.1.7. Atıkların Atılması 19
4.1.8. Tesis Dışı Yedekleme 20
4.2. Prosedürel Kontroller 20
4.2.1. Güvenilir Roller 20
4.2.2. Her Görev için Gereken En Az Kişi Sayısı 20
4.2.3. Her Görev için Kimlik Doğrulama 20
4.2.4. Görevlerin Ayrılmasını Gerektiren Roller 20
4.3. Personel Kontrolleri 21
4.3.1. Nitelik, Deneyim ve Güvenlik Gereklilikleri 21
4.3.2. Kişisel Geçmiş Kontrol Gereklilikleri 21
4.3.3. Eğitim Gereklilikleri 21
4.3.4. Tekrar Eğitim Sıklığı ve Gerekliliği 21
4.3.5. İş Rotasyonu Sıklığı ve Sırası 21
4.3.6. Yetkisiz İşlemler için Yaptırımlar 22
4.3.7. Bağımsız Alt Yüklenici Gereklilikleri 22
4.3.8. Personele Sağlanan Dokümantasyon 22
4.4. Denetim Kayıt Altına Alma Prosedürleri 22
4.4.1. Kaydedilen Olay Tipleri 22

4.4.2. Kayıt İşleme Sıklığı 23
4.4.3. Denetim Kayıtlarının Saklanma Süresi 23
4.4.4. Denetim Kayıtlarının Korunması 23
4.4.5. Denetim Kayıtlarının Yedeklenme Prosedürleri 23
4.4.6. Denetim Bilgisi Toplama Sistemi (İç ve Dış) 24
4.4.7. Olayı Yaratan Kişiyi Bilgilendirme 24
4.4.8. Zarar Görebilirlik Değerlendirmesi 24
4.5. Kayıtların Arşivlenmesi 24
4.5.1. Arşivlenen Kayıt Tipleri 24
4.5.2. Arşivlerin Saklanma Süresi 25
4.5.3. Arşivlerin Korunması 25
4.5.4. Arşivlerin Yedeklenme Prosedürleri 25
4.5.5. Kayıtların Zaman Damgası Altına Alınması Gereklilikleri 25
4.5.6. Arşiv Toplama Sistemi 25
4.6. Güvenliğin Yitirilmesi ve Felaket Kurtarma 25
4.6.1. Güvenlik Kaybına Neden Olabilecek Olaylar 25
4.6.2. Bilgisayar Kaynakları, Yazılım ve /veya Verilerin Bozulmuş Olması 26
4.6.3. İmza Oluşturma Verilerinin Güvenliğinin Yitirilmesi 26
4.6.4. İş Sürekliliği Yetenekleri ve Felaket Kurtarma 26
4.7. AYYILDIZİMZA Faaliyetinin Son Bulması 27
5. TEKNİK GÜVENLİK KONTROLLERİ 27
5.1. Anahtar Çifti Üretimi ve Kurulumu 27
5.1.1. Anahtar Çifti Üretimi 27
5.1.2. AYYILDIZİMZA İmza Doğrulama Verilerinin Üçüncü Kişilere Ulaştırılması 27
5.1.5. Anahtar Uzunlukları 27
5.1.6. Anahtar Üretimi ve Kalite Kontrolü 28
5.1.7. Anahtar Kullanım Amaçları 28
5.2. İmza Oluşturma Verisinin Korunması ve Kriptografik Modül Mühendislik Kontrolleri 28
5.2.1. Kriptografik Modül Standartları ve Kontroller 28
5.2.2. İmza Oluşturma Verisinin Çok Kullanıcılı Kontrolü 28

5.2.3. İmza Oluşturma Verisinin Saklanması 29
5.2.4. İmza Oluşturma Verisinin Yedeklenmesi 29
5.2.5. İmza Oluşturma Verisinin Arşivlenmesi 29
5.2.6. İmza Oluşturma Verisinin Kriptografik Modül Transferi 29
5.2.7. İmza Oluşturma Verisinin Kriptografik Modülde Saklanması 29
5.2.8. İmza Oluşturma Verisinin Aktif Edilme Yöntemi 30
5.2.9. İmza Oluşturma Verisinin Pasif Edilme Yöntemi 30
5.2.10. İmza Oluşturma Verisinin Yok Edilmesi 30
5.2.11. Kriptografik Modülün Değerlendirilmesi 30
5.3. Anahtar Çifti Yöntemi ile İlgili Diğer Konular 31
5.3.1. İmza Doğrulama Verilerinin Arşivlenmesi 31
5.3.2. İşlevsel Süreleri ve Anahtar Çifti Kullanım Süreleri 31
5.4. Erişim Denetim Verileri 31
5.5. Bilgisayar Güvenlik Kontrolleri 31
5.6. Yaşam Döngüsü Güvenlik Denetimleri 31
5.7. Ağ Güvenliği Denetimleri 32
6. UYGUNLUK DENETİMLERİ 32
7. DİĞER İŞLER VE HUKUKSAL KONULAR 32
7.1. Ücretlendirme 32

1. GİRİŞ

AYYILDIZ İMZA BİLGİ GÜVENLİĞİ VE TEKNOLOJİLERİ A.Ş. (bundan sonra "AYYILDIZİMZA" olarak anılacaktır). 25355 Sayılı ve 23 Temmuz 2004 tarihli Resmî gazete yayınlanarak 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, Zaman Damgası İlkeleri (bundan sonra "Zİ" olarak anılacaktır), AYYILDIZİMZA'nın ESHS olarak hizmet Zaman damgası hizmeti süreçlerinde uyması gereken ilke ve kuralları belirlemek amacıyla "Elektronik İmza ile İlgili Süreçlerde ve Teknik Kriterlere İlişkin Tebliğ" 'in10. Maddesine uygun olarak hazırlanmıştır.

Bu Doküman (Zİ), zaman damgası hizmeti sağlanırken hangi ilkeler doğrultusunda gerçekleştiğini ortaya koyar. ESHS olarak AYYILDIZİMZA'nın, sertifika sahibinin ve üçüncü kişilerin uygulama sorumluluklarını belirtir.

1.1. Genel Bakış

Bu doküman (Zİ), AYYILDIZİMZA'nın Zaman Damgası ilkelerini açıklamaktadır. Bu ilkeler, AYILDIZİMZA'nın zaman damgası başvurularını alması, zaman damgasının üretimi, istek sahibine zaman damgasının gönderilmesi gibi süreçleri yönetirken uyguladığı ilke ve kurallarıdır.

Zİ, AYYILDIZİMZA'nın Zaman Damgası Hizmeti yönetim sürecindeki ilke ve kuralların "***ne***" olduğunu açıklarken, hazırlamış olduğu Zaman Damgası Uygulama Esasları dokümanını (bundan sonra "ZUE" olarak anılacaktır) ile de Zİ'ye bağlı kalarak bu yöntem, ilke ve kuralların "***nasıl***" gerçekleştiğini açıklar.

1.2. Kitapçık Adı ve Tanımlama

Bu doküman, AYYILDIZİMZA Zaman Damgası İlkelerini kapsamaktadır. Kitapçık sürüm bilgileri ve yayımlanma tarihi kapakta yer almaktadır.

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

- Zaman Damgası İlkeleri: 2.16.792.3.0.60.1.1.1 numarasını atayarak TSE 'ye bildirmiştir.

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

1.3. Taraflar

Zİ de yer alan taraflar, AYILDIZİMZA'nın ESHS olarak üzerinden zaman damgası hizmet sağladığı birimler ve bu hizmeti alan müşteri, sertifika sahipleri ve kullanıcıları kapsar.

1.3.1. Elektronik sertifika Hizmet Sağlayıcı

AYYILDIZİMZA, Bu Doküman (Zİ) ilke ve kurallarını duyurduğu Nitelikli Elektronik Sertifika Hizmeti sağlayıcısıdır. Kanun da belirtilen yükümlülüklerini yerine getirir.

- Zaman Damgası başvurusunun alınması,
- Zaman Damgası Hizmetinin verilmesi,
- Zaman Damgası hizmetinin iptali operasyonlarını yürütür.

1.3.2. Zaman Damgası Sahipleri

Zaman Damgası sahipleri, zaman damgası başvurusunda bulunan, satın aldığı zaman damgası hizmetini kullanan kişidir.

1.3.3. Üçüncü Kişiler

Üçüncü kişiler, oluşturulmuş zaman damgası verilerini doğrulayarak işlem yapan gerçek veya tüzel kişilerdir.

1.3.4. Diğer Katılımcılar

Diğer Katılımcılar, AYYILDIZİMZA'nın zaman damgası hizmet faaliyetleri sürecinde iş birliği yaptığı ve hizmet aldığı tüm gerçek ve tüzel kişileri kapsar. Bu katılımcılar, verecekleri hizmetin güvenilir ve doğru biçimde olduğunu, ayrıca bu süreçlerde yer alan müşteriler ile ilgili özel ve gizli bilgilerin korunmasını garanti altına almak için hazırlanmış sözleşmeleri imzalar.

1.4. Zaman Damgası İlkelerinin Yönetimi

İş bu, Zİ dokümanı yönetiminden AYYILDIZİMZA sorumludur.

1.4.1. Zİ Dokümanından sorumlu Organizasyon

İş bu, Zİ dokümanın değiştirilmesi, yayınlanması ve uygunluğundan **AYYILDIZİMZA Bilgi Güvenliği Kurulu** sorumludur.

1.4.2. İletişim Noktası

AYYILDIZ İMZA BİLGİ GÜVENLİĞİ VE TEKNOLOJİLERİ A.Ş.

Adres:	Göktürk Merkez, Menekşe Sk. 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

1.4.3. Zİ'nin İlkelere Uygunluğunun Belirlenmesi

İş bu, Zİ dokümanının uygunluğu ve uygulanabilirliği Bilgi Güvenliği Kurulu başkanının önderliğinde **AYYILDIZİMZA Bilgi Güvenliği Kurulu** tarafından belirlenir.

1.4.3. Zİ Onaylama Prosedürleri

Zİ ve ZUE Dokümanı bilgi güvenliği kurulu tarafından düzeli olarak takip edilerek uygunluğu ve uygulanabilirliği kontrol edilir. AYYILDIZİMZA bilgi güvenliği kurulu bağımsız denetim kuruluşlarının denetim sonuçlarını değerlendirerek, Zİ ve ZUE'nin uygunluğunu kontrol etmek ile sorumludur. Herhangi bir değişiklik yapıldığında, bu değişikliğin yeni bir OID 'ye gerek duyup duyulmadığına karar verir.

1.5. Kısaltmalar ve Tanımlar

1.5.1. Kısaltmalar

BTK:	Bilgi Teknolojileri ve İletişim Kurumu
BGYS:	Bilgi Güvenliği Yönetim Sistemi
ESHS:	Elektronik Sertifika Hizmet Sağlayıcısı
Zİ:	Zaman Damgası İlkeleri
ZUE:	Zaman Damgası Uygulama Esasları
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 - Açık Anahtar Alt Yapısı
AAA:	Açık Anahtar Altyapısı
NESİ:	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
NESUE:	Nitelikli Elektronik Sertifika Uygulama Esasları
CN:	Common Name-Sertifika Sahibi Adı Soyadı
C:	Country
L:	Location
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

1.5.2. 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'nın kullandığı yöntemler ile sunan alt yapı sistemidir.
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 veya müşterileri veya üyeleri veya 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 yönetmelikler de 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 içeren ve içinde 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 sorgulanabilmesinin sağlayan protokoldür.
Elektronik İmza:	Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama ve 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 imzalarla 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 başvurularını 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 araçları.
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 veya 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 Madde 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" 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 Esasları:	ESHS'nin elektronik sertifika yönetim sürecindeki ilke ve kurallarının "Nasıl" uygulandığını sertifika İlkelerine (NESİ) bağlı kalarak detaylandırıp açıklayan ve gerekli durumlarda güncelleyip kamuoyuna yaptığı duyurudur. Sertifika Uygulama esasları dokümanına tüm değişikleri ile beraber ESHS'nin 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 Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmeliktir".
Zaman Damgası İlkeleri:	Zaman damgası hizmetleri ile ilgili ilke ve kuralları içeren belgedir.
Zaman Damgası Uygulama Esasları:	Zaman damgası hizmetleri ile ilgili ilke ve kuralların hangi esaslara göre uygulandığını açıklayan belgedir.

2. YAYIN VE BİLGİ DEPOSU SORUMLULUKLARI

2.1. Bilgi Deposu

AYYILDIZİMZA çevrimiçi olarak kesintisiz şekilde sunduğu Bilgi deposunda zaman damgası ve kök sertifikası Zİ ve ZUE 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. Zaman Hizmeti ve İlgili Bilgilerinin Yayımlanması

AYYILDIZİMZA bilgi deposunda, ESHS iç yönetimindeki süreçlerde kullanılan özel belgeler dışında kalan, Zaman Damgası hizmetinin yönetim sürecinde yer alan bilgi ve belgeler herkesin erişimine açık halde tutulur.

- Zaman Damgası Kök sertifikası ve sürüm geçmişleri,
- Zaman Damgası Sertifikaları ve sürüm geçmişleri,

- Zaman Damgası başvuru dokümanları,
- Güncel SİL dosyaları,
- Zİ VE ZUE Dokümanları ve sürüm geçmişleri.

2.3. Yayımlanma Zamanı ve Sıklığı

Bölüm 2.2 de yer alan dokümanlar yeni sürümleri AYYILDIZİMZA Bilgi Güvenliği Kurulu tarafından onaylandıktan sonra yayımlanır.

2.4. Bilgi Deposuna Erişim Kontrolleri

AYYILDIZİMZA bilgi deposunu ilgili herkesin erişimine açık tutar. Ayrıca kesintisiz olarak erişilebilirliğini ve güvenliğini sağlamak için gerekli önlemleri alır.

3. ZAMAN DAMGASI İŞLEVSEL GEREKLİLİKLERİ

AYYILDIZİMZA, Zaman damgası hizmetlerini bu Zİ doküman da yer alan ilke ve kurallara uyarak üretimini yapar ve yönetir.

3.1. Zaman Damgası

AYYILDIZİMZA Zaman damgası hizmeti RFC 3161'de tanımlı zaman damgası protokolünü destekler. AYYILDIZİMZA verdiği zaman damgalarını imzalamak için BTK'nın yayımlamış olduğu Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de belirtilen algoritmaları kullanır.

3.1.1. UTC ile Zaman Birliği Sağlanması

AYYILDIZİMZA, zaman bilgisini güvenilir ve yedekli (Atomik ve/veya GPS) kaynaklardan temin eder.

3.2. Zaman Damgası Başvurusu

3.2.1. Kimler Zaman Damgası Başvurusunda Bulunabilir?

Elektronik verilerinin varlığını kesin ve doğru bir zaman bilgisiyle kanıtlamak isteyen tüm gerçek ve tüzel kişiler, AYYILDIZİMZA zaman damgası hizmeti başvurusunda bulunabilir.

3.2.2. Zaman Damgası Başvuru Kayıtları

Zaman damgası başvuruları, AYYILDIZİMZA web sitesi üzerinden, ya da kayıt birimleri aracılığı ile yapılabilir.

3.2.3. Zaman Damgası Başvurularının Doğrulanması

AYYILDIZİMZA Zaman damgası başvurularını, üretime geçmeden önce Zİ ve ZUE ye uygunluğunu kontrol eder. Gerekli gördüğü durumda ret etme hakkına sahiptir.

3.3. Zaman Damgası Üretimi

Zaman damgası başvurusu onaylandıktan sonra başvuru sahibine zaman damgası hizmetini kullanacağı, Kullanıcı ID ve Şifre bilgisi gönderilir ve siparişte bulunduğu kontör adedi hesabına yüklenir.

3.3.1. Zaman Damgası İsteği Gönderimi

Kullanıcı, ID ve Şifre bilgisini içeren isteği AYYILDIZİMZA hizmet adresine RFC 3161 standardına uygun olarak gönderir.

İstek gönderimi için kullanıcı AYYILDIZİMZA'dan yardımcı kütüphaneler talep edebilir.

3.3.2. Zaman Damgası İsteğinin İşlenmesi ve Üretim

Zaman Damgası isteği sırasıyla aşağıdaki adımlar ile işlenir.

- Gelen istek, standartlara uygun olup olmadığının kontörlü yapılır.
- Kullanıcı ID ve şifre doğrulanır.
- Kontör miktarı kontrol edilir ve kullanım sonucu azaltılır.
- Zaman Damgası oluşturulur.

3.3.3. Zaman Damgasının Gönderilmesi

AYYILDIZİMZA, oluşturduğu zaman damgasını RFC 3161'de tanımlı zaman damgası protokolü yoluyla istemciye gönderir.

4. TESİS, YÖNETİM VE İŞLETMEYLE İLGİLİ KONTROLLER

AYYILDIZİMZA, zaman damgası 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.

4.1. Fiziksel Kontroller

4.1.1. Tesis Yeri ve İnşaatı

AYYILDIZİMZA, zaman damgası 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.

4.1.2. Fiziksel Erişim

Güven Merkezi içindeki güvenlik bölgelerine, fiziksel erişim sürekli kontrol altında tutulur. Yüksek Güvenlikli Bölgelere erişmek için, bir önceki güvenlik bölgesinden geçmek zorunludur. ESHS

işlemlerinin gerçekleştirildiği yazılım ve donanım modülleri ile her türlü elektronik veya kâğıt ortamındaki bilgilerin bulunduğu bu bölgelere, yetkisiz kişilerin erişiminin engellenmesi için gerekli önlemler alınmıştır.

4.1.3. Güç Kaynakları ve Havalandırma

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

4.1.4. Su Baskınları

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

4.1.5. Yangın Önleme ve Yangından Korunma

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

4.1.6. Saklama Ortamları

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

4.1.7. Atıkların Atılması

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

4.1.8. Tesis Dışı Yedekleme

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

4.2. Prosedürel Kontroller

4.2.1. Güvenilir Roller

AYYILDIZİMZA, zaman damgası hizmet faaliyeti sürecindeki görev alan personelinin rolleri ZUE dokümanın da detaylı olarak açıklanmıştır.

4.2.2. Her Görev için Gereken En Az Kişi Sayısı

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

4.2.3. 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.

4.2.4. Görevlerin Ayrılmasını Gerektiren Roller

AYYILDIZİMZA, zaman damgası hizmet sürecindeki operasyonlarında, 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.

4.3. Personel Kontrolleri

4.3.1. Nitelik, Deneyim ve Güvenlik Gereklilikleri

AYYILDIZİMZA, zaman damgası 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.

4.3.2. Kişisel Geçmiş Kontrol Gereklilikleri

AYYILDIZİMZA bünyesinde, istihdam edeceği 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.

4.3.3. Eğitim Gereklilikleri

AYYILDIZİMZA, istihdam ettiği personelleri göreve başlamadan önce, sertifika yaşam zincirinin tüm halkalarının, bu doküman (Zİ) ve ZUE açıklanan ilkelere uygun olarak yürütülmesi için gerekli eğitimden geçirir.

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

4.3.4. Tekrar Eğitim Sıklığı ve Gerekliliği

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

4.3.5. İş Rotasyonu Sıklığı ve Sırası

Uygulama dışıdır. Düzenlenmesine gerek duyulmamıştır.

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

4.3.7. Bağımsız Alt Yüklenici Gereklilikleri

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

4.3.8. Personele Sağlanan Dokümantasyon

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

4.4. Denetim Kayıt Altına Alma Prosedürleri

4.4.1. Kaydedilen Olay Tipleri

AYYILDIZİMZA, zaman damgası hizmet döngüsü içinde gerçekleştirdiği ve denetimini yapmak istediği işlemleri kayıt altına alır.

Bu Kayıtlar;

- Zaman damgası başvuru kayıtları,
- Zaman Damgası istek ve cevap kayıt bilgileri,
- Güvenlikli bölgelere giriş-çıkış kayıtları,
- Zİ ve ZUE değişiklikleri sonucu oluşan tüm versiyonlar,

- İşlemi yapan personelin kimlik bilgisi, işlemin tarih ve zaman bilgisi,
- SİL ile ilgili kayıtlar,
- Sistem arıza kayıtları,
- Sistem donanım ve yazılım güncelleme kayıtlarıdır.

4.4.2. Kayıt İşleme Sıklığı

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

4.4.3. 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 (Zİ) 4.5 belirtilen ilkelere göre gerçekleştirilir.

4.4.4. Denetim Kayıtlarının Korunması

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

4.4.5. Denetim Kayıtlarının Yedeklenme Prosedürleri

Tutulan kayıtlar, ilgili prosedürlerine göre periyodik olarak yedekleri alınır.

4.4.6. Denetim Bilgisi Toplama Sistemi (İç ve Dış)

Tutulan kayıtları, 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.

4.4.7. 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.

4.4.8. Zarar Görebilirlik Değerlendirmesi

Tutulan kayıtlar, zaman damgası hizmetinin 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 tedbirleri alır.

4.5. Kayıtların Arşivlenmesi

4.5.1. Arşivlenen Kayıt Tipleri

Bu Doküman (Zİ) da 4.4.1' de yer alan tüm kayıt tiplerine ilave olarak;

- Sözleşmeler,
- Taahhütnameler,
- Yayımlanan tüm Zaman Damgası İlkeleri dokümanı versiyonları (Zİ),
- Yayımlanan tümü Zaman Damgası Uygulama Esasları Dokümanı versiyonları (ZUE),
- Müşteri ile ilgili yapılan tüm yazışmalar ve müşteri dosyalarıdır.

4.5.2. Arşivlerin Saklanma Süresi

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

4.5.3. Arşivlerin Korunması

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

4.5.4. Arşivlerin Yedeklenme Prosedürleri

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

4.5.5. Kayıtların Zaman Damgası Altına Alınması Gereklilikleri

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

4.5.6. Arşiv Toplama Sistemi

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

4.6. Güvenliğin Yitirilmesi ve Felaket Kurtarma

4.6.1. 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 sitemin en hızlı şekilde tekrar güvenli hizmeti

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

4.6.2. 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 ivedilikler bilgilendirilir.

Donanım ve yazılım sisteminin 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.

4.6.3. İmza Oluşturma Verilerinin Güvenliğinin Yitirilmesi

AYYILDIZİMZA, imza oluşturma verilerinin güvenliğinin ve güvenilirliğinin yitirilmesi durumunda, AYYILDIZİMZA iş sürekliliği yönetimi prosedürleri ve iş sürekliliği planları uyarınca yeni imza oluşturma verisi oluşturularak devreye alınır.

4.6.4. 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.

4.7. 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, faaliyetinin durdurulması prosedürü uyarınca, zaman damgası hizmetlerini başka bir ESHS'ye devredebilir.

5. TEKNİK GÜVENLİK KONTROLLERİ

5.1. Anahtar Çifti Üretimi ve Kurulumu

5.1.1. Anahtar Çifti Üretimi

AYYILDIZİMZA Zaman Damgası 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.

5.1.2. AYYILDIZİMZA İmza Doğrulama Verilerinin Üçüncü Kişilere Ulaştırılması

AYYILDIZİMZA Zaman Damgası 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.

5.1.5. Anahtar Uzunlukları

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

5.1.6. 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.

5.1.7. Anahtar Kullanım Amaçları

AYYILDIZİMZA zaman damgası oluşturma verisi zaman damgası oluşturmak amacıyla, ilgili imza doğrulama verisi ise zaman damgasının doğruluğunu denetleme amacıyla kullanılır.

5.2. İmza Oluşturma Verisinin Korunması ve Kriptografik Modül Mühendislik Kontrolleri

5.2.1. Kriptografik Modül Standartları ve Kontroller

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

5.2.2. İmza Oluşturma Verisinin Çok Kullanıcılı Kontrolü

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

5.2.3. İmza Oluşturma Verisinin Saklanması

AYYILDIZİMZA Zaman damgası hizmetine ait imza oluşturma verileri yetkisiz kişilerin erişimine kapalı, fiziksel ve elektronik olarak güvenli kriptografik modül içinde şifreli olarak tutulur. İmza oluşturma verisinin kriptografik modül dışına çıkması engellenir.

5.2.4. İmza Oluşturma Verisinin Yedeklenmesi

AYYILDIZİMZA Zaman Damgası Kök ve Alt Kök sertifikalarına ait imza oluşturma verileri, AYYILDIZİMZA merkezindeki yüksek güvenlikli bölgelerde ve Güvenli Donanım Modülleri üzerinde yedeklenir.

5.2.5. İmza Oluşturma Verisinin Arşivlenmesi

AYYILDIZİMZA zaman damgası hizmetine ait imza oluşturma verileri arşivlenmez. Kullanım süreleri sonunda geri dönüşümsüz şekilde silinir.

5.2.6. İmza Oluşturma Verisinin Kriptografik Modül Transferi

AYYILDIZİMZA Zaman Damgası Kök ve Alt Kök sertifikalarına ait imza oluşturma verileri Güvenli Donanın Modülleri üzerinde üretilir. İmza Oluşturma verileri kesinlikle dışarda üretilmez. AYYILDIZİMZA Zaman Damgası 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 Bölgeler de birden fazla yetkili kişinin kontrolünde yapılır.

5.2.7. İmza Oluşturma Verisinin Kriptografik Modülde Saklanması

AYYILDIZİMZA Zaman Damgası Kök ve Alt Kök sertifikalarına ait imza oluşturma verisi, AYYILDIZİMZA merkezindeki yüksek güvenlikli bölgelerde Güvenli Donanım Modüllerinde saklanır. Bölüm 5.2.6 haricinde dışarıya çıkartılamaz.

5.2.8. İmza Oluşturma Verisinin Aktif Edilme Yöntemi

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

5.2.9. İmza Oluşturma Verisinin Pasif Edilme Yöntemi

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

5.2.10. İmza Oluşturma Verisinin Yok Edilmesi

AYYILDIZİMZA Zaman Damgası 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.

5.2.11. Kriptografik Modülün Değerlendirmesi

AYYILDIZİMZA Zaman Damgası 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.

5.3. Anahtar Çifti Yöntemi ile İlgili Diğer Konular

5.3.1. İmza Doğrulama Verilerinin Arşivlenmesi

AYYILDIZİMZA Zaman Damgası 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.

5.3.2. İşlevsel Süreleri ve Anahtar Çifti Kullanım Süreleri

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

5.4. Erişim Denetim Verileri

Zaman damgası hizmeti ile ilgili erişim denetim verileri Nitelikli Elektronik Sertifika İlkeleri (NESİ) dokümanın da tanımlanan erişim denetim verileri güvenlik şartlarını sağlar. .

5.5. Bilgisayar Güvenlik Kontrolleri

Zaman damgası hizmetine ait bilgisayar sistemlerine Nitelikli Elektronik Sertifika İlkeleri (NESİ) ve Uygulama Esasları (NESUE) dokümanlarında belirtilen güvenlik denetimleri uygulanır.

5.6. Yaşam Döngüsü Güvenlik Denetimleri

Zaman damgası hizmeti ile ilgili sistemlere, yaşam döngüsü boyunca, Nitelikli Elektronik Sertifika İlkeleri (NESİ) ve Uygulama Esasları (NESUE) dokümanlarında belirtilen güvenlik denetimleri uygulanır.

5.7. Ağ Güvenliği Denetimleri

Zaman damgası hizmeti sistemine Nitelikli Elektronik Sertifika İlkeleri (NESİ) ve Uygulama Esasları (NESUE) dokümanlarında belirtilen ağ güvenliği denetimleri uygulanır.

6. UYGUNLUK DENETİMLERİ

Zaman damgası hizmeti sistemine Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de ve Nitelikli Elektronik Sertifika İlkeleri (NESİ) dokümanında belirtilen uygunluk denetimleri uygulanır.

7. DİĞER İŞLER VE HUKUKSAL KONULAR

Nitelikli Elektronik Sertifika Uygulama Esaslarında (NESUE) belirtildiği gibidir.

7.1. Ücretlendirme

AYYILDIZİMZA ürettiği her zaman damgası için zaman damgası istemcisinden ücret talep eder. Zaman Damgası başvurusunda belirtilen sayıda zaman damgası kontör olarak hesaba eklenir. Zaman damgası ücretlendirilmesi ile ilgili ayrıntılar AYYILDIZİMZA web sitesinde detaylı olarak yer almaktadır.