ARK|İMZA

ArkSigner

ZAMAN DAMGASI İLKELERİ

(ZDİ)

Sürüm: 1.0

Yayın Tarihi: 01.08.2021

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

Üniversiteler Mah. 1606 Cad. Bilkent Cyberpark Cyberplaza A-Blok Kat:6

No:603 Tel: +90 312 484 79 33 e-Posta: destek@arkimza.com

İçindekiler

1 Giriş

Bu doküman, ArkSigner Yazılım ve Donanım Ticaret A.Ş. bünyesinde yer alan zaman damgası hizmetinin işleyişi sırasında uyulması gereken kuralları ve çalışma ilkelerini tanımlayan Zaman Damgası İlkeleri (ZDİ) dokümanıdır. Elektronik sertifika hizmet sağlayıcılığı kapsamında zaman damgasına yönelik faaliyetler sırasında uyulması gereken ilke ve kuralları belirlemek amacıyla, Bilgi Teknolojileri ve İletişim Kurumu'nun kanun kapsamında yayımlamış olduğu "Elektronik İmzaya İlişkin Süreçler ile Teknik Kriterlere İlişkin Tebliğ"in 10. Maddesi uyarınca hazırlanmıştır.

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

2 Kapsam

Bu dokümanın kapsamında, ArkSigner'ın sunduğu zaman damgası hizmetlerine özgü teknik ve hukuki nitelikleri, faaliyetleri, altyapısı, ilgili tarafları ve bu tarafların hak ve yükümlülüklerin açıklanması ve kamuoyuna duyurulması yer almaktadır.

3 Taraflar

3.1 Zaman Damgası Üretim Merkezi

Zaman damgası üretim merkezi, ArkSigner'ın zaman damgası üretim ve dağıtımından sorumlu birimidir.

3.2 Zaman Damgası Sahibi

Zaman damgası sahipleri, zaman damgası talep eden ve başvuru yapan, üretilen zaman damgasının iletildiği kişi, kurum ve/veya kuruluşlardır.

3.3 Üçüncü Taraflar

Üçüncü taraflar ArkSigner tarafından verilmiş olan zaman damgalarını alan ve ilgili zaman damgalarını doğrulayan taraflardır.

4 Zaman Damgası İlkeleri Yönetimi

4.1 Doküman Değişim Yönetimi

ZDİ dokümanı ArkSigner tarafından yazılmıştır. ArkSigner gerekli gördüğü durumlarda ZDİ dokümanında değişiklik yapabilir.

4.2 İletişim Bilgileri

Bu ZDİ dokümanı ve ilgili iletişim bilgileri aşağıdadır:

ArkSigner Yazılım ve Donanım San. Tic. A.Ş.
Adres : Üniversiteler Mah. 1606 Cad. Cyberpark A Blok, No:603 Çankaya/ANKARA

Telefon : +90 312 484 7933

Faks : +90 312 484 7933

E-posta : info@arkimza.com

Web : www.arkimza.com

4.3 Yayın ve Duyuru Politikaları

ArkSigner, ZDİ dokümanını herkesin erişimine açık bulunan aşağıdaki internet adreslerinden yayımlar:

www.arkimza.com

4.4 ZDİ'nin İlkelere Uygunluğunun Belirlenmesi

ArkSigner ZDİ kitapçığının uygunluğu ve uygulanabilirliği, ArkSigner yönetimi tarafından belirlenir.

4.5 ZDİ Onaylama Prosedürleri

ZDİ kitapçığı ArkSigner Yönetim Kurulu tarafından onaylanır. Gerekli onayı alan ZDİ, ArkSigner'ın zaman damgası faaliyetlerine ilişkin ilke ve kuralları düzenlemek için kullanılır.

5 Kısaltmalar ve Tanımlar

5.1 Kısaltmalar

ESHS: Elektronik Sertifika Hizmet Sağlayıcısı

5.2 Kısaltmalar

BTK: Bilgi Teknolojileri ve İletişim Kurumu

CWA: Communications Workers of America

ÇİSDuP: Çevrim İçi Sertifika Durum Protokolü

EAL: Evaluation Assurance Level

ECDSA: Elliptic Curve Digital Signature Algorithm

ESHS: Elektronik Sertifika Hizmet Sağlayıcısı

ETSI: European Telecommunications Standard Institute

FIPS: Federal Information Processing Standards

GPS: Global Positioning System

IEC: International Electrotechnical Commission

IETF: Internet Engineering Task Force – İnternet Mühendisliği Görev Grubu

ISO: International Organization for Standardization

ISO: International Organization for Standardization

OCSP: Online Certificate Status Protocol

OID: Object Identifier – Nesne Tanımlayıcı Numarası

PIN: Personal Identification Number

PKI: Public Key Infrastructure – Açık Anahtarlı Altyapı

RFC: IETF tarafından yayımlanan, kılavuz niteliğinde yorum talebi dokümanları

RSA: Ron **R**ivest, Adi **S**hamir ve Leonard **A**dleman tarafından güvenilirliği çok büyük tam sayılarla işlem yapmanın zorluğuna dayanan bir şifreleme tekniğidir

SHA: Secure Hash Algorithm

TSE: Türk Standartları Enstitüsü

URL: Uniform Resource Locator

UTC: Universal Time Coordinate

ZDH: Zaman Damgası Hizmeti

ZDİ: Zaman Damgası İlkeleri

ZDUE: Zaman Damgası Uygulama Esasları

5.3 Tanımlar

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

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

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

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

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

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

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

Dizin: Geçerli sertifikaları içinde bulunduran elektronik depodur.

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

Elektronik Sertifika: İmza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kayıttır.

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

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

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

Güvenli Elektronik İmza: Kanunun 4. maddesinde sayılan niteliklere sahip, Kanunun hariç tuttuğu işlemler dışında elle atılan imzayla aynı hukuki sonucu doğuran elektronik imzadır.

Güvenli Elektronik İmza Doğrulama Aracı: Kanunun 7. maddesinde sayılan niteliklere sahip imza doğrulama aracıdır.

Güvenli Elektronik İmza Oluşturma Aracı: Kanunun 6.maddesinde sayılan niteliklere sahip imza oluşturma aracıdır.

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

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

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

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

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

İnceleme: Kuruma yapılan bildirimin gerekli şartları sağlayıp sağlamadığını tespit etmek amacıyla yapılan çalışmalar bütününü,

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

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

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

Kurum: Bilgi Teknolojileri ve İletişim Kurumu'dur.

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

Nitelikli Elektronik Sertifika: Kanunun 9 uncu maddesinde sayılan niteliklere sahip elektronik sertifikadır.

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

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

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

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

Sertifika Özet Değeri: Sertifikanın, özetleme algoritması ile elde edilen çıktısıdır.

Sertifika Uygulama Esasları: Sertifika ilkelerinde yer alan hususların nasıl uygulanacağını detaylı olarak anlatan belgeyi,

Sertifika Kayıt Merkezi: ESHS yapısında yer alan, sertifika başvuruları ile sertifika yenileme başvurularını alan, ilgili kimlik doğrulama süreçlerini yürüten, sertifika taleplerini onaylayarak sertifika üretim merkezine yönelten, ESHS faaliyetleri kapsamında müşteri ilişkilerini yöneten alt birimlere sahip olan birimdir.

Sertifika Üretim Merkezi: ESHS yapısında yer alan, onaylı sertifika talepleri doğrultusunda sertifika üretimi yapan, sertifika iptal işlemlerini gerçekleştirilen, sertifika kayıtları ile sertifika iptal durum kayıtlarını yaratan, işleten ve yayımlayan birimdir.

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

Tebliğ: Elektronik İmzaya İlişkin Süreçler ile Teknik Kriterlere İlişkin Tebliğ'dir.

Yönetmelik: Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik'tir.

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

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

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

Zaman Damgası Hizmeti (ZDH): Zaman damgası oluşturan hizmet servisi.

6 Zaman Damgası Hizmetlerine Yönelik Yayınlar

ArkSigner, ESHS kapsamında zaman damgası hizmetleriyle ilgili gereken doküman ve kayıtları hazırlamak ve saklamakla yükümlüdür. Bu doküman ve kayıtların bazıları, zaman damgası hizmetlerinin etkin bir şekilde müşterilere ulaştırılabilmesi ve zaman damgası kullanımının güvenilirliğinin ve sürekliliğinin sağlanması amacıyla kamuya açık olarak yayımlanır.

6.1 Zaman Damgası Hizmetleri Bilgi Deposu

ArkSigner, bilgi deposunda tutulan tüm bilgilerin güncel ve doğru olmasını sağlar. Bilgi deposunu işletmek, ilgili doküman ve kayıtları yayımlamak için üçüncü bir güvenilir taraf kullanmaz.

6.2 Zaman Damgası Hizmetleri Bilgisinin Yayımlanması

ArkSigner bilgi deposunda, zaman damgası hizmetlerine ait özel kurumsal prosedür ve talimatlar ile ticari gizli bilgiler dışında zaman damgası hizmetlerinin yürütülmesine ilişkin bilgiler, herkesin erişimine açık tutulur. ArkSigner'ın zaman damgası hizmetlerine yönelik ilkelerini içeren ZDİ kitapçığı, bu ilkelerin nasıl uygulandığını gösteren ZDUE, zaman damgası iş süreçleriyle ilgili uygulama prosedürleri bilgi deposunda yer alır.

ArkSigner elektronik sertifika ve zaman damgası hizmetlerine ilişkin tüm kök ve alt kök sertifikaları herkesin erişimine açık olarak ESHS'ye özgü sunucularda yayımlanır.

6.3 Yayımın Zamanı veya Sıklığı

İlgili dokümanların yeni sürümleri çıktıkça, eski sürümlerle birlikte bilgi deposunda yayımlanır.

6.4 Bilgi Deposuna Erişim Kontrolleri

Bilgi deposu herkesin erişimine açıktır. ArkSigner, yayımlanan bilgilerin gerçekliği ve güvenliği için gerekli tüm önlemleri alır.

7 Yükümlülükler ve Sorumluluklar

7.1 Yükümlülükler

7.1.1 ESHS Yükümlülükleri

ArkSigner, güvenilir zaman kaynağı kullanmakla yükümlüdür. ArkSigner Zaman damgası hizmetleri, CWA 14171-1, ETSI TS 101 456 ve ETSI TS 102 203 standartlarına uygun bir şekilde yürütülmektedir. Verilen hizmetler olağandışı durumlar haricinde 7 gün /24 saat hizmete verecek şekilde yürütülür.

ArkSigner, zaman damgası ilke ve esaslarına tam olarak uygunluğu sağlamak, bu dokümanlara göre zaman damgası üretmek ve bunların taklit ve tahrif edilmesini önlemekle ilgili her türlü tedbiri almakla yükümlüdür.

Aynı zamanda ArkSigner, zaman damgası üretme işlemlerini zaman damgası uygulama esasları dokümanı doğrultusunda yapmakla yükümlüdür.

7.1.2 Kullanıcı yükümlülükleri

Zaman damgalı bir veri yaratan kullanıcı, ESHS Zaman Damgası Hizmet Sağlayıcının elektronik imzasını doğrulamalı ve ESHS Zaman Damgası Hizmet Sağlayıcının sertifikasının iptal durumunu kontrol etmelidir.

7.1.3 Üçüncü Kişilerin Yükümlülükleri

Zaman damgalı bir veri alan üçüncü kişiler, ESHS Zaman Damgası Hizmet Sağlayıcının elektronik imzasını doğrulamalı ve ESHS Zaman Damgası Hizmet Sağlayıcının sertifikasının iptal durumunu kontrol etmelidir.

7.2 Sorumluluklar

7.2.1 ESHS Sorumlulukları

ArkSigner, zaman damgası hizmetiyle ilgili olarak, 15 Ocak 2004 tarih ve 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 şartları yerine getirmekten sorumludur.

7.2.2 Kullanıcı Sorumlulukları

Zaman damgalı bir veri yaratan kullanıcı zaman damgalarını uygun geçerlilik denetimlerini yapmadan kullandığı takdirde doğabilecek zararlardan sorumludur.

7.2.3 Üçüncü Kişi Sorumlulukları

Zaman damgalı bir veri alan üçüncü kişiler, ESHS Zaman Damgası Hizmet Sağlayıcının elektronik imzasını doğrulamalı ve ESHS Zaman Damgası Hizmet Sağlayıcının sertifikasının iptal durumunu kontrol etmelidir.

8 Zaman Damgası İşlevsel Gereklilikleri

8.1 Zaman Damgası

Zaman Damgası, elektronik bir verinin, üretildiği, değiştirildiği, gönderildiği, alındığı veya kaydedildiği zamanın tespit edilmesi amacıyla, hizmet sağlayıcısı tarafından elektronik imzayla doğrulanan kayıtların resmi olarak kanıtlanmasıdır. ArkSigner, zaman damgasının güvenli şekilde oluşturulmasını ve doğru zamanı içermesini sağlayacak tedbirler alır. Zaman damgası hizmeti RFC 3161'de tanımlı zaman damgası protokolünü destekler ve zaman damgası içindeki zaman bilgisi UTC ile uyumludur. ArkSigner, zaman bilgisinin senkronizasyonunu, GPS uydularından senkronize olan bir zaman sunucusuyla sağlamaktadır.

8.2 Zaman Damgası Başvurusu

Zaman damgası başvuruları, başvuru sahipleri tarafından elektronik ortamda ve belirlenen protokoller üzerinden yapılır. Başvuru sahiplerinin bilgileri ve zaman damgası verilecek olan elektronik verilere ait kayıtlar ArkSigner tarafından düzenli olarak tutulur. ArkSigner, zaman damgası hizmetinden faydalanmak isteyen başvuru sahiplerinin başvuru taleplerini alır. Başvuru sonrasında başvuru sahiplerine, zaman damgası isteği sırasında kullanacakları hesap bilgileri ulaştırılır. Zaman damgası müşterileri, zaman damgası başvurusu sırasında belirtilen kontörleri bitene kadar ArkSigner'dan zaman damgası alırlar.

8.3 Zaman Damgası İsteme

İstemci, ZDH tarafından sağlanan yazılımı kullanarak kendisine verilen kullanıcı adı ve parola ile RFC 3161 de tanımlı olan zaman damgası protokolü yoluyla zaman damgası isteğinde bulunur.

8.4 Zaman Damgası Başvurularının Doğrulanması

ArkSigner, zaman damgası başvurularını teknik olarak doğrular. Zaman damgası başvuruları ZDUE hükümlerine ve ilgili prosedürlere uygunsa kabul edilir. Başvuruların doğrulanamaması durumunda ArkSigner başvuruyu reddetme hakkını saklı tutar.

8.5 Zaman Damgası İsteğinin İşlenmesi

ZDH tarafından, istemciden gelen zaman damgası isteğinin uygunluk denetimleri yapılır.

Bu denetimler kapsamında:

1. Kullanıcı adı ve parolanın doğruluğu kontrol edilir.
2. İstemcinin zaman damgası alabilmek için yeterli kontörünün olup olmadığına bakılır.
3. Anlaşma şartlarının koyduğu diğer kısıtlamalar kontrol edilir.

Denetimler, isteğin anlaşma şartları içinde olup olmadığını anlama amaçlıdır. İstek anlaşma şartlarına uygunsa, zaman damgası üretilir.

8.6 Zaman Damgasının Gönderilmesi

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

İstemci, ZDH tarafından sağlanan yazılımı kullanarak zaman damgasını alır.

Gönderilen her zaman damgası anlaşma koşulları uyarınca ücretlendirilir.

8.7 Zaman Damgası Hizmet Protokolü

ArkSigner, talep üzerine, http veya https protokolü üzerinden oluşturulmuş zaman damgası verisini zaman damgası başvuru sahiplerine çevrim içi gönderir.

9 Yönetim Tesis ve İşletme Kontrolleri

9.1 Fiziksel Kontroller

- ArkSigner, olası dış tehditlere karşı korunaklı ve güvenli bir alanda kurulmuştur.
- Kurulan alanda yüksek güvenlikli bölgeler ve çeşitli güvenlik alanları oluşturulmuştur.
- Güvenlikli alanlara fiziksel erişim 7/24 kontrol altında tutulmaktadır.
- Kullanılan tüm donanım ve teçhizat için kesintisiz çalışacak güç kaynakları oluşturulmuştur.
- Ortam sel ve su baskınlarına karşı korunmaktadır.
- Yangın ihbar sistemleri ile olası yangın durumlarına anında müdahale edilmesini sağlayacak söndürme sistemleri kurulmuştur.
- ArkSigner faaliyetleri sırasında oluşturulan tüm kayıtların yedekleri uygun saklama ortamlarında tutulmaktadır.
- Temel zaman damgası hizmetlerine bağlı, elektronik veya kâğıt ortamda saklanan tüm bilgi ve belgeler, saklanmaları gerekmiyorsa ilgili prosedürler uyarınca tamamen imha edilerek atılır.
- Kriptografik modüller atılmaları gerektiğinde ya fiziksel olarak imha edilir ya da üretici firma talimatları doğrultusunda sıfırlanır.
- ArkSigner, sertifika hizmetleri iş sürekliliğini sağlayabilmek amacıyla, mevcut tesis ve binada oluşabilecek herhangi bir afet durumunda sistemlerini yeniden işletilebilir duruma getirebilmek için elektronik işlem kayıtlarının yedeklerini tesis dışında güvenli kasalarda saklar.

9.2 Prosedürel Kontroller

ArkSigner zaman damgası hizmetlerinde görev alan personelin organizasyonun sağlanması amacıyla, tüm zaman damgası iş süreçlerinin yürütülmesinde görev alacak güvenilir roller belirlenmiştir.

- **Üst Düzey Yöneticiler:** Sertifika hizmetlerinin yürütülmesinden teknik ve idari açıdan sorumlu üst düzey yöneticilerdir.
- **Güvenlik Yetkilileri:** Güvenlik politikaları ve uygulamalarının yönetimi ve yürütülmesinden sorumlu çalışanlardır.
- **Sistem Yöneticileri:** Sertifika hizmetlerine ilişkin sistemlerin kurulumu, konfigürasyonu ve devamlılığının sağlanması ve aynı zamanda sistem yedekleme ve geri yükleme işlemleri için yetkilendirilmiş çalışanlardır.
- **Sistem Denetçileri:** Sertifika hizmetlerine ilişkin arşivlerin ve denetim kayıtlarının izlenmesi için yetkilendirilmiş çalışanlardır.
- **Güvenlik Görevlileri:** Tüm ArkSigner tesislerinin fiziksel güvenliğini sağlamaktan sorumlu çalışanlardır.

ArkSigner'da zaman damgası süreçleri dâhilindeki kritik işlemlerin yapılabilmesi için çok kişi kontrollü bir sistem kurulmuştur. Kriptografik modül kullanımı gerektiren ve rutin akışın dışında kalan kritik

işlemler, en az iki yetkilinin hazır bulunmasıyla sonuçlandırılabilmektedir. ArkSigner zaman damgası kök sertifikasıyla ilgili her türlü üretim, yenileme ve iptal işlemi en az iki yetkilinin hazır bulunmasıyla idari ve teknik onaylı görev talimatının ilgili yetkililere verilmiş olmasıyla yapılabilmektedir.

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

9.3 Personel Kontrolleri

ArkSigner'da çalışan personel, zaman damgası süreçlerinin işleyişini doğru ve güvenilir bir şekilde yürütebilecek nitelikte, göreve uygun eğitim düzeyine sahip (lise, üniversite, yüksek lisans vb.), konusunda bilgili ve eğitimli, benzer çalışma alanlarında deneyimli ve güvenlik kontrollerinden geçmiştir. Personelin özgeçmişi ve referansları ayrıntılı bir şekilde değerlendirilmekte, işe teknik ve idari açıdan uygunluğundan emin olunmaktadır. Uygun nitelikte olduğu belirlenen kişiler için adli sicil belgesi istenir ve gerekiyorsa güvenlik soruşturması yapılır.

ArkSigner personeli göreve başlamadan önce sorumlulukları kapsamında eğitimden geçirilir. Eğitim süresince, çalışanlar temel zaman damgası iş süreçleri işlevsel prosedürler ve talimatlar bilgi güvenliği ilkeleri ve mevcut bilgi güvenliği yönetim sistemi; kullanılacak yazılım ve donanım birimleri hakkında ayrıntılı olarak bilgilendirilir. Çalışanlara yönelik eğitim, göreve başlanırken verilen ilk eğitimin ardından periyodik olarak ve diğer gerekli görülen durumlarda tekrarlanır. Sürekli olarak yürütülen ölçme ve değerlendirme çalışmalarının sonuçları ışığında ilgili personelin eğitim ihtiyacı belirlenir ve periyodik eğitimlerin yanı sıra verimin artırılmasına yönelik ek eğitim seansları da düzenlenebilir. Verilen eğitimlerin konuları ve kapsamı, gelişen teknoloji ve yenilenen yazılım ve donanım birimlerine uygun olarak sürekli güncellenir ve yenilenir.

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

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

ArkSigner personeline, ZDİ ve ZDUE kitapçıkları, zaman damgası süreçleriyle ilgili uygulama ve güvenlik prosedürleri ile talimatları, çalışanların rollerine göre düzenlenmiş iş tanımları, kullanılan yazılım ve donanım birimlerinin kullanım kılavuzları sağlanır.

9.4 Denetim Kayıtları Alma Prosedürleri

Zaman damgası hizmetlerine ait tüm kayıtlar ArkSigner tarafından tutulur.

Bu kayıtlar:

- Zaman damgası başvuru kayıtları,
- Üretilen zaman damgaları hakkındaki kayıtlar,
- ArkSigner zaman damgası işlemlerine dâhil olan tüm yönetici ve operatörlerin işlem kayıtları,
- Çalışanların ArkSigner birimlerine giriş ve çıkış kayıtları,
- Sistem modüllerine erişim kayıtları,
- Doküman takibiyle ilgili kayıtlar,
- Yazılım ve donanım kurulum, güncelleme ve onarım kayıtları

İşlem kayıtları tutulurken temel olarak işlemin tanımı, işlemi yapan kişi, işlemin tarih ve zaman bilgisi kaydedilir.

Denetim kayıtları sürekli olarak tutulur ve periyodik olarak bu kayıtların yedekleri alınarak arşivlenir. İşleyişe ait denetim kayıtları, aktif tutulma süresince sistemde tutulur. Bu sürenin sonunda yasal düzenlemeler uyarınca saklanmak üzere arşivlenir. Denetim kayıtları fiziksel ve elektronik güvenlik önlemleriyle korunur, sadece yetkili kişilerin erişimine açık tutulur. Denetim kayıtlarının veri bütünlüğü anahtarlanmış özet yöntemiyle sağlanmaktadır. İlgili prosedürler uyarınca, kayıtların periyodik olarak tesis içi ve tesis dışı yedekleri alınır.

Denetim kayıtları, ESHS iş süreçlerinin yürütülmesinde kullanılan ESHS yönetim yazılımı tarafından tutulur. Rutin işlemlerin dışında kalan denetim kayıtlarının oluştuğu durumlarda, olayı yaratan kişi sistem tarafından uyarılır. Olayın çeşidine ve önemine göre, sistem üzerinde olayı yaratan kişinin yönetiminden sorumlu üst yetki seviyesindeki kişi veya kişiler de bilgilendirilebilir.

Denetim kayıtları sistem üzerinde raporlanır. Bu raporların analiz edilmesiyle sistemdeki güvenlik açıkları ve zaman damgası süreçlerindeki hata noktaları belirlenerek önlem alınmaktadır.

9.5 Kayıtların Arşivlenmesi

ArkSigner'a ait tüm denetim kayıtları, müşterilerle yapılan tüm yazışmalar, ZDİ ve ZDUE kitapçıklarının tüm sürümleri, uygulama prosedürlerinin, talimatların ve formların bütünü, ArkSigner arşiv prosedürleri uyarınca arşivlenir. Arşivlerin büyük bir kısmı elektronik ortamda tutulurken, kâğıt üzerindeki yazışmalar, formlar ve belgeler de kâğıt ortamında arşivlenir. Zaman damgası hizmetlerine ait arşivler, yasal düzenlemeler uyarınca en az 20 yıl süreyle saklanır. Arşivler fiziksel ve elektronik güvenlik önlemleriyle korunur, sadece yetkili kişilerin erişimine açık tutulur. Elektronik arşivlerin yetkili olmayan kişiler tarafından görülmesi, değiştirilmesi veya silinmesi önlenmiştir. Kâğıt üzerindeki arşivler ise sadece yetkili kişilerin girme izni bulunan özel birimlerde tutulurlar. İlgili prosedürler uyarınca, elektronik ortamdaki arşivlerin yedekleri tutulur. Kâğıt ortamdaki arşivlerin ise yedekleri alınmaz.

ArkSigner tarafından saklanan tüm elektronik arşiv kayıtları elektronik olarak imzalı ve zaman damgalıdır. Arşiv kayıtları, ArkSigner arşiv yönetim sistemi kullanılarak ilgili prosedürler uyarınca derlenir.

9.6 Güvenliğin Yitirilmesi ve Afet Durumlarında Yapılacaklar

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

Bilgisayar kaynaklarının zarar görmesi, yazılım birimlerinde veya işleyişe dair verilerde bozulma oluşması durumunda, öncelikle tesisteki hasarlı donanım yeniden işler hale getirilir. Daha sonra, kaybolan kayıtlar yedekleme sistemleri aracılığıyla yeniden oluşturulur ve zaman damgası hizmetleri tekrar etkin hale getirilir. Eğer tam olarak işler hale getirilemez veya kayıtların bazıları yeniden elde edilemez ise, bu durumdan etkilenebilecek olan bütün zaman damgası kullanıcıları ile üçüncü kişiler ivedilikle bilgilendirilir.

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

9.7 ArkSigner'ın Faaliyetlerinin Son Bulması

ArkSigner, zaman damgası hizmetlerine son vermesi durumunda, Kanun ve Yönetmelik gereği bu durumu en az 3 ay önce Kuruma bildirir ve kamuoyuna duyurur. ArkSigner, faaliyetinin durdurulması prosedürü uyarınca, zaman damgası hizmetlerini başka bir ESHS'ye devredebilir.

10 Teknik Güvenlik Kontrolleri

10.1 ESHS Anahtar Çifti Yönetimi

10.1.1 Anahtar Çifti Üretimi ve Korunması

ArkSigner zaman damgası kök ve alt kök sertifikalarına ait anahtar çiftleri, sadece yetkili kişilerin kontrolünde, iki yetkilinin hazır bulunmasıyla, teknik ve idari güvenlik önlemleri alınmış ortamlarda, ArkSigner zaman damgası kök ve alt kök sertifika üretim, yayımlama ve imha prosedürü uyarınca üretilir ve uygun biçimde yedeklenir. İmza oluşturma verisi yetkisiz erişime karşı fiziksel ve teknik güvenlik önlemleriyle korunur.

ArkSigner kök ve alt kök sertifikaları anahtar çifti üretiminde en az EAL4+ veya FIPS 140-2 Düzey 3 güvenlik düzeyinde kriptografik güvenlik donanım modülü kullanılır. Anahtar çiftlerinin uzunluğu ve kullanılacak algoritmalar güncel mevzuat ve standartlarla uyumlu olacak şekilde yapılır. Aynı şekilde üretilen anahtar çiftinin ömrü güncel mevzuat, standartlar ve anahtarların kriptografik güvenlik süresiyle sınırlandırılmıştır. Bir kök veya alt kök sertifikasının geçerlilik süresi sonundan yeterince makul bir süre önce yeni bir anahtar çifti ve sertifika üretilerek hizmetin kesintisiz bir biçimde devam etmesi sağlanır.

ArkSigner donanım güvenlik modülleri, fiziksel ve elektronik her türlü müdahaleye karşı koruma altında tutulur ve çalıştırılır. Modüllerde bulunan verinin güvenli yedekleri ilgili prosedürlere göre alınır ve saklanır. Böylece fiziksel ve ekonomik ömrünü tamamlamış bir modülün içindeki anahtarlar yok edilir ve yeni modüllerde kullanılmak üzere gerekli yedekler başka ortamlarda saklanır.

10.1.2 İmza Doğrulama Verilerinin Üçüncü Taraflara Ulaştırılması

ArkSigner zaman damgası kök ve alt kök sertifikaları üçüncü tarafların erişebileceği şekilde yayımlanır. Böylelikle, ArkSigner'a ait imza doğrulama verileri üçüncü taraflarca kullanılabilir.

10.1.3 Anahtar Uzunlukları

ArkSigner sertifikaları, Tebliğ'le belirlenen minimum anahtar uzunluklarına uygundur. ArkSigner sertifika üretim merkezlerinin kök ve alt kök sertifikaları üretilirken elliptic curve 256 veya 384 bit anahtar çiftleri kullanılır.

10.1.4 Anahtar Üretimi ve Kalite Kontrolü

Anahtar üretiminin ArkSigner merkezinde veya bağlı kayıt merkezlerinde olması durumunda, anahtar çifti uygun güvenlik düzeyine sahip donanım güvenlik modüllerinde, Tebliğ'de belirlenen parametrelere uygun olarak üretilir. Anahtar üretiminin müşteri tarafında olduğu durumlarda, imza oluşturma verisinin uygun araçlarda ve nitelikte üretiminden müşteri sorumludur.

10.1.5 Anahtar Değişimi

ArkSigner zaman damgası kök ve alt kök sertifikalarının anahtar yenileme işlemleri, ArkSigner merkezi tarafından yönetilir.

10.1.6 Kriptografik Modül Standartları ve Kontroller

ArkSigner'da anahtar çifti üretimi ve zaman damgası işlemleri, Tebliğ'le belirlenen standartlarla uyumlu, güvenli kriptografik donanım modüllerinde gerçekleştirilir. Satın alma sonrası donanım güvenlik modülünün ilk kullanımından önce, sevkiyat ve depolama sırasında cihazların zarar

görmediğinden emin olmak için kontroller uygulanır. Cihazların kabulü sırasında fabrika paketlemesi ve güvenlik mühürleri kontrol edilir ve cihazlar fiziksel ve teknik bakımdan güvenliği sağlanmış alanlarda saklanır ve kullanılır. Cihazların tüm kullanım ömürleri boyunca, cihazlar işlevsellikleriyle ilgili sürekli kontrol altında tutulur ve herhangi bir güvenlik ihlali durumu bilgi güvenliği ihlal olayı prosedürü uyarınca yönetilir.

ArkSigner'a bağlı sertifika üretim merkezlerinin kök ve alt kök sertifikalarına erişim, yetkili kişiler dışında yasaklanmıştır. Fiziksel ve teknik erişim kontrollerinin yanı sıra, bu imza oluşturma verilerinin kullanımı, ilgili modüle aynı anda iki ayrı yetkilinin bağlanması ve sistem tarafından onaylanmasıyla mümkündür. Sistem, hiçbir yetkilinin tek başına ArkSigner imza oluşturma verilerini kullanabilmesine izin vermez.

10.1.7 İmza Oluşturma Verisinin Yedeklenmesi

Herhangi bir felaket durumu veya sorun anında hizmetlerin kesintiye uğramaması amacıyla, ArkSigner zaman damgası kök ve alt kök sertifikalarına bağlı imza oluşturma verileri, ArkSigner kök sertifikaları anahtar üretim prosedürü uyarınca yedeklenir ve fiziksel ve teknik güvenlik kontrolleri altında saklanır. Bu işlem için kök ve alt kök sertifikalara bağlı imza oluşturma verilerinin yedeklenmesi prosedürü uygulanır.

10.1.8 İmza Oluşturma Verisinin Kriptografik Modül Transferi

ESHS kök ve alt kök sertifikalarına ait imza oluşturma verileri güvenli kriptografik donanım modüllerinde üretilir. Bu veriler yedekleme amacıyla kullanılan güvenli modüllere transferi dışında hiçbir biçimde modül dışına çıkarılamaz. Yedekleme işlemi, kriptografik donanım modülü üzerinde şifreli bir biçimde gerçekleştirilir.

10.1.9 İmza Oluşturma Verisinin Kriptografik Modülde Saklanması

ArkSigner sertifika üretim merkezlerinin zaman damgası kök ve alt kök sertifikalarına bağlı imza oluşturma verileri, üretildikleri ve Tebliğ'de tanımlı güvenlik düzeyine sahip kriptografik donanım modüllerinde saklanır.

10.1.10 İmza Oluşturma Verisinin Aktive Edilme Yöntemi

ArkSigner sertifika üretim merkezlerinin zaman damgası kök ve alt kök sertifikalarına bağlı imza oluşturma verileri, içinde bulundukları donanım güvenlik modülü üzerinde, iki yetkilinin hazır bulunmasıyla aktive edilir.

10.1.11 İmza Oluşturma Verisinin Deaktive Edilme Yöntemi

ArkSigner sertifika üretim merkezlerinin zaman damgası kök ve alt kök sertifikalarına bağlı imza oluşturma verileri, içinde bulundukları donanım güvenlik modülü üzerinde sadece belirli bir süreyle ve işlem bazlı aktive edilir; işlem tamamlandıktan ya da süre bittikten sonra deaktive olur. İmza oluşturma verisinin yeniden kullanılabilmesi için, yetkililerin tekrar sisteme tanıtılarak imza oluşturma verisinin aktive edilmesi gerekir.

10.1.12 İmza Oluşturma Verisi Yok Etme Metodu

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

10.1.13 Kriptografik Modül Değerlendirmesi

ArkSigner sertifika üretim merkezlerinin zaman damgası kök ve alt kök sertifikalarına bağlı imza oluşturma verileri, Tebliğ'de tanımlı güvenlik düzeyine sahip kriptografik donanım modüllerinde üretilir ve saklanır.

10.1.14 İmza Doğrulama Verilerinin Arşivlenmesi

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

10.1.15 Sertifikanın İşlevsel Süreleri ve Anahtar Çifti Kullanım Süreleri

ArkSigner sertifika üretim merkezlerinin zaman damgası kök ve alt kök sertifikalarının geçerlilik süreleri 10 yılı aşmaz. Bu sürenin sonunda sertifikalar yenilenirken mutlaka anahtar yenileme yapılır.

10.2 Erişim Şifreleri

10.2.1 Erişim Şifrelerinin Oluşturulması ve Kurulumu

ArkSigner zaman damgası kök ve alt kök sertifikalarının imza oluşturma verilerine ya da bu verilerin bulunduğu kriptografik modüllere erişim, iki ayrı yetkilinin hazır bulunmasıyla ve erişim şifreleriyle gerçekleşir. Erişim şifresi, gizli anahtar yönetiminde kullanılan parola, şifre, PIN ya da benzeri özel verilere karşılık gelir.

ArkSigner alt kök ve kök sertifikalarına ait anahtarların üretimi ve bu anahtarlara ait erişim şifrelerinin oluşturulması, Kök ve Alt Kök Sertifika Üretim Yayımlama ve İmha Prosedürü'nde açıklanan törene göre yapılır. Kök ve alt kök sertifikaların gizli anahtarlarının bulunduğu kriptografik modüllere erişim ve anahtarların kullanılması erişim şifrelerine sahip iki yetkilinin aynı anda bulunmasıyla mümkündür.

10.2.2 Erişim Şifrelerinin Korunması

ArkSigner kök ve alt kök sertifikalarına ait gizli anahtarları kullanan yetkili kişiler, erişim şifrelerini en geç 90 (doksan) günde bir değiştirirler. Yetkili kişiler, erişim şifrelerinin gizliliğinden ve korunmasından sorumludur.

10.3 Bilgisayar Güvenlik Kontrolleri

ArkSigner tarafından yürütülen zaman damgası iş süreçleri kapsamında, tüm bilgi sistemlerine erişim ve bu sistemlerin işletilmesi için aşağıda yer alan güvenlik kontrolleri uygulanmaktadır:

- Bilgisayar sistemlerinde güvenilir ve sertifikalı donanım ve yazılım ürünleri kullanılmaktadır.
- Bilgisayar sistemleri yetkisiz erişime ve güvenlik açıklarına karşı korunmuştur. Penetrasyon ve istemsiz erişim kontrolleri kurulmuş ve ilgili testlerle kontrollerin güncelliği ve sürekliliği sağlanmıştır.
- Bilgisayar sistemleri, virüslere, kötü niyetli ve yetkisiz yazılımlara karşı korunmaktadır.
- Bilgisayar sistemleri ağ güvenliği saldırılarına karşı korunmuştur.
- Bilgisayar sistemlerine erişim hakları ve kimlik doğrulama, ArkSigner personeline verilen şifrelerle sağlanmaktadır.
- Bilgisayarlara erişim hakları, yetkili personele tanımlanan rollerle sınırlanmıştır.
- Bilgisayar sistemini oluşturan birimler arasındaki veri iletişimi güvenli olarak yapılmaktadır.
- İşlem kayıtları sürekli olarak tutulduğu için bilgisayar sistemlerinde oluşabilecek sorunlar kısa zamanda ve doğru biçimde belirlenebilmektedir.
- ArkSigner, değişikliklere karşı korunmuş güvenilir sistemler ve ürünler kullanır. Bu bağlamda, Bilgi Teknolojileri ve İletişim Kurumu'nun sürekli denetimi altında, CWA 14167-1 standardının önerileri kesin olarak uygulanır.

10.4 Ağ Güvenlik Kontrolleri

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

ArkSigner içindeki diğer tüm sistemler de uygun ağ güvenliği yöntemleriyle korunmaktadır. Güvenlik duvarları, anahtarlama cihazları ve yönlendiriciler gibi tüm ağ elemanları, doğru ve güvenli bir biçimde ağ konfigürasyonu prosedürleri uyarınca kurulmuştur. Bu ağ elemanlarının güvenlik kontrolleri prosedürler uyarınca sürekli olarak yapılmaktadır. Ayrıca ArkSigner, ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemleri standardı sertifikası sahibidir.

11 Zaman Damgası Profilleri

11.1 Başvurularda Algoritma Nesne Tanımlayıcıları

ArkSigner, SHA2-256, SHA2-384 ve SHA2-512 özet algoritmaları kullanılarak oluşturulmuş özet verileri için zaman damgası hizmetleri verir. Bu algoritmalar dışında kalan algoritmalarla üretilmiş veriler için gönderilen başvurular reddedilir.

11.2 Zaman Damgasında Algoritma Nesne Tanımlayıcıları

ArkSigner tarafından üretilen zaman damgalarında özetleme algoritması olarak SHA2-256,384,512 elektronik imza için ise RSA veya ECDSA kullanılır.

12 Uygunluk Denetimi ve Diğer Değerlendirmeler

ArkSigner, ilgili mevzuat gereğince Bilgi Teknolojileri ve İletişim Kurumu tarafından denetlenir. Ayrıca, tüm ESHS süreçleri, bilgi güvenliği yönetim sisteminin sürekliliği açısından ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi ve TS EN ISO 9001 Kalite Yönetim Sistemi sertifikaları uyarınca periyodik olarak uygunluk denetimine tabi tutulur. ESHS hizmetlerinin verilişi ve işletmeye dair güvenlik koşulları bir iç denetim planı uyarınca kontrol altında tutulur.

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

12.1 Denetim Sıklığı ve Durumları

Bilgi Teknolojileri ve İletişim Kurumu, düzenleyici ve denetleyici Kurum olarak gerekli gördüğü durumlarda re'sen ve iki yılda en az bir defa resen denetim yapar. Denetleme sırasında, denetleme yapmaya yetkili görevliler tarafından her türlü defter, belge ve kayıtların verilmesi, yönetim yerleri, binalar ve eklentilerine girme, yazılı ve sözlü bilgi alma, örnek alma ve işlem ve hesapları denetleme isteminin elektronik sertifika hizmet sağlayıcıları ve ilgililer tarafından yerine getirilmesi zorunludur. ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi sertifikası uyarınca, her yıl takip denetiminden ve her üç yılda bir de belge yenileme denetiminden geçilir. İç denetim, plan gereği yılda en az bir defa, gerek görülmesi durumunda daha fazla sayıda tekrar edilir.

12.2 Denetçinin Kimliği ve Özellikleri

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

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi sertifikasyonu, yetkilendirilmiş bir denetçi tarafından gerçekleştirilir. ArkSigner'ın kurumsal iç denetimi, ArkSigner yetkili personeli tarafından yapılır. İç denetim, ArkSigner bünyesindeki Bilgi Güvenliği Yönetim Sistemi Sorumlusu ve Kalite Yönetim Sistemi Sorumlusu tarafından yürütülür.

12.3 Denetçinin ESHS'yle İlişkisi

Denetçi kuruluş olan Kurum, Kanun gereği Türkiye'de nitelikli elektronik sertifikalar ve zaman damgasıyla ilgili faaliyet gösteren tüm ESHS'leri denetlemekle yetkili kılınmış düzenleyici kuruluştur. ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi sertifikasyonu bağımsız ve yetkili bir denetçi tarafından gerçekleştirilir. ArkSigner'ın kurumsal iç denetimi, ArkSigner yetkili personeli tarafından yapılır

12.4 Denetimde Kapsanan Başlıklar

Kurum'un denetimi Kanunla kendisine verilen yetki çerçevesinde, ArkSigner'ın elektronik sertifika ve zaman damgası hizmetlerine dair tüm süreçleri, bu hizmetlerin yerine getirilmesi sırasında kullanılan teknik altyapı ve hizmetlerin verildiği tesisleri kapsar. ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi sertifikasyonu, ArkSigner elektronik sertifika ve zaman damgası hizmetleri kapsamındadır. İç denetimde de, yasal denetim altına giren tüm konular kapsanır.

12.5 Eksiklik Durumunda Yapılacaklar

Yönetmelik gereği Kurum tarafından yapılan denetimler sırasında, ArkSigner'ın faaliyet ve işleyişini olumsuz yönde etkileyebilecek derecede önemli konuların belirlenmesi durumunda, ilgili mevzuatta öngörülen yaptırım ve cezalar uygulanır. ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi denetimleri sırasında saptanan eksikliklerin majör nitelikte olması sertifikanın geri alınmasına neden olur. Minör eksikler, bir sonraki denetim dönemine kadar ArkSigner tarafından giderilir. ArkSigner tarafından yapılan iç denetimlerde belirlenen aksaklıklar hakkında düzeltici ve önleyici faaliyetler yürütülür.

12.6 Sonuçların Bildirilmesi

Kanun gereği Kurum tarafından yapılan denetimin sonuçları gerek duyulduğu takdirde resmi yollarla ArkSigner'a iletilir. Kurum'un bir geri bildirimde bulunmaması, olumsuz bir değerlendirmenin olmadığı anlamını taşır. ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi denetim sonuçları, denetçi tarafından resmi olarak ArkSigner'a bildirilir. İç denetim sonuçları ise, iç denetim sonuç raporunda yer alır ve ilgili yetkililerin değerlendirmesine sunulur.

13 Diğer İş Konuları ve Yasal Konular

13.1 Ücretler

13.1.1 Zaman Damgası Hizmet Ücretleri

ArkSigner tarafından verilen zaman damgası hizmetlerinin güncel fiyat bilgileri, ArkSigner web sitesi ve uygun görülen diğer iletişim kanalları üzerinden müşterilere duyurulur.

13.1.2 Diğer Hizmetlerin Ücretleri

ArkSigner, kamuya açık olarak yayımladığı ZDİ, ZDUE gibi kitapçık ve belgeler için ücret talep etmez. Bunların dışında kalan ve katma değerli olarak üretilerek müşterilere sunulan diğer ürün ve hizmetler için uygulanacak ücretler, web sitesi ve uygun görülen diğer iletişim kanalları üzerinden müşterilere duyurulur.

13.1.3 Bedel İadesi

ArkSigner, zaman damgası hizmetleriyle ilgili olarak bedel iadesi yapmaz. Ancak, ArkSigner'dan kaynaklanan nedenlerle, zaman damgası içeriğinde sorun bulunması durumunda, herhangi bir ücret talep edilmeden başka bir zaman damgası verilir.

13.2 Finansal Sorumluluk

ArkSigner, Kanun'dan doğan yükümlülüklerini yerine getirmemesi sonucu doğacak zararların karşılanması amacıyla sertifika mali sorumluluk sigortası yaptırmakla yükümlüdür. Sigortaya ilişkin koşullar 26 Ağustos 2004 tarih ve 25565 sayılı Resmi Gazetede yayımlanmış olan "Sertifika Mali

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

13.3 İş Bilgisinin Gizliliği

13.3.1 Gizli Bilginin Kapsamı

ArkSigner'ın zaman damgası hizmetlerine yönelik ESHS işlevleriyle ilgili her türlü ticari gizli bilgi ve belge, ArkSigner zaman damgası kök ve alt kök sertifikalarının imza oluşturma verileri, kullanılan yazılım ve donanım bilgileri, işlem kayıtları, denetim raporları, tesis içi bölge ve cihazlara ait erişim şifreleri, tesis planı ve iç tasarımı, acil eylem planları, iş planları, satış bilgileri, işbirliği sözleşmeleri, iş ortaklığı yapılan kuruluşlara ait gizlilik dereceli bilgiler gizli bilgi kapsamına girer.

13.3.2 Gizlilik Kapsamı Dışındaki Bilgi

ArkSigner'ın ticari gizliliği olmayan, Kanun ve uygulamalar gereği kamuya açık olması gereken bilgi ve belgeleri gizlilik kapsamı dışında tutulur. Zaman damgası hizmetleriyle ilgili müşteri prosedürleri, ZDİ kitapçığı, ZDUE kitapçığının içeriğindeki bilgiler gizlilik kapsamına girmez.

13.3.3 Gizli Bilginin Korunması Sorumluluğu

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

13.4 Kişisel Bilgilerin Gizliliği/Özelliği

13.4.1 Gizlilik Planı

ArkSigner, verdiği zaman damgası hizmetleri kapsamında, zaman damgası başvuru sahiplerine ya da diğer taraflara ait kişisel verilerin veya özel nitelikli kişisel verilerin gizliliğini sağlar ve kişiye özel olma durumunu 6698 sayılı Kişisel Verilerin Korunması Kanunu uyarınca korur.

13.4.2 Özel Olarak Değerlendirilecek Bilgi

ArkSigner tarafından zaman damgası hizmetlerinin verilmesi sırasında ihtiyaç duyulan ve zaman damgası başvuru sahiplerinden alınmış olan müşteri bilgileri, özel bilgi olarak değerlendirilir.

13.4.3 Özel Bilgiyi Koruma Sorumluluğu

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

13.4.4 Yargısal ve İdari Süreçlere Uygun Olarak Bilginin Açıklanması

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

13.5 Fikri Mülkiyet Hakları

ArkSigner tarafından üretilen zaman damgası hizmetleriyle ilgili müşteri prosedürleri, ZDİ ve ZDUE kitapçıkları, zaman damgası hizmetlerinin yürütülmesiyle ilgili her türlü iç ve dış doküman, veri

tabanları, web siteleri ile zaman damgası hizmetlerine bağlı olarak geliştirilen tüm ürünlerin fikri mülkiyet hakları ArkSigner'a aittir. Zaman damgası başvuru sahipleri, zaman damgası içeriğinde yer alan ve kendilerine ait elektronik verilerinin mülkiyet haklarına sahiptir.

13.6 Tarafların sorumlulukları

ArkSigner, yasal mevzuat ile ZDİ ve ZDUE kitapçıklarında belirlenen ilke ve esaslara göre zaman damgası hizmetlerini kesintisiz bir biçimde verir. Zaman damgası sahipleri ve üçüncü taraflar, zaman damgasını doğrulamaktan kendileri sorumludur.

13.7 Tazminatlar

ArkSigner, bu ZDİ ve ZDUE'de yer alan ilke ve esaslar gereği yükümlülüklerini yerine getiremez ve bu durumdan üçüncü kişilerin zarar gördüğü hukuken belirlenirse, yasal mevzuat uyarınca ilgili zarar ArkSigner tarafından tazmin edilir. ArkSigner kusursuzluğunu ispat ettiği takdirde tazminat ödeme yükümlülüğü doğmaz.

13.8 ZDİ Kitapçığının Geçerliliği

13.8.1 ZDİ Kitapçığının Geçerlilik Dönemi

ZDİ kitapçığının bu sürümü, yeni bir sürüm çıkarılana kadar geçerlidir.

13.8.2 ZDİ Kitapçığının Geçerliliğinin Sona Ermesi

ArkSigner faaliyetlerinde ve zaman damgası hizmetlerinde oluşabilecek değişikliklere ve düzenlemelere bağlı olarak, ZDİ kitapçığının mevcut sürümünün içeriğinin değişmesini gerektiren herhangi bir durum ortaya çıktığında, kitapçık kısmen ya da tamamen geçersiz duruma düşebilir. Bu durumda, ilgili değişikliklerin yansıtıldığı yeni bir ZDİ kitapçığı sürümü ArkSigner tarafından hazırlanır ve yayımlanır.

13.8.3 Geçerliliğin Sona Ermesinin Etkileri ve İşlerliğin Sürdürülmesi

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

13.9 Taraflara Özel Duyurular ve İletişim

ArkSigner tarafından zaman damgası kullanıcılarına yapılacak olan duyurular için zaman damgası kullanıcılarının uygun olan iletişim bilgileri kullanılır. ArkSigner'ın üçüncü taraflara yapacağı duyurular web üzerinden ya da basın yayın organları aracılığıyla yayımlanır.

13.10 Değişiklikler

13.10.1 Değişiklik Prosedürü

ArkSigner faaliyetlerinde ve zaman damgası hizmetlerinde oluşabilecek değişikliklere ve düzenlemelere bağlı olarak, ZDİ kitapçığının mevcut sürümünün içeriğinin değişmesini gerektiren herhangi bir durum ortaya çıktığında, ilgili değişikliklerin yansıtıldığı yeni bir ZDİ kitapçığı sürümü ArkSigner tarafından hazırlanır ve ArkSigner Yönetim Kurulu'nun onayının ardından yayımlanır. ZDİ ve ZDUE dokümanında yer alan ilkeler ve uygulamalar, yönetim gözden geçirme toplantılarında yıllık olarak gözden geçirilir. ZDİ'de oluşan değişiklikler, ZDUE'deki ilgili uygulamalara da yansıtılır. Dolayısıyla yeni bir ZDİ sürümü, yeni bir ZDUE sürümünü de gerektirir. ArkSigner tarafından üretilen yeni zaman damgaları "zaman damgası ilkeleri" uzantısında URL olarak verilen SUE dokümanına erişim bilgisi aynı kalır, ama bu adresin işaret ettiği ZDUE dokümanı yeni sürümdür.

13.10.2 Duyuru Mekanizması ve Süresi

ArkSigner faaliyetleri ve zaman damgası hizmetlerindeki uygulama değişiklikleri ile mevcut ZDİ ve ZDUE kitapçıklarında değişiklik oluşması durumunda, çıkarılan güncel ZDİ ve ZDUE sürümleri hakkında zaman damgası sahipleri ve üçüncü taraflar ivedilikle bilgilendirilir. Özellikle önemli değişikliklerde, zaman damgasının kullanılabilirliği ve kabul edilirliği bazı uygulamalarda etkilenebileceğinden, ArkSigner zaman damgası sahiplerini ve üçüncü tarafları bilgilendirebilmek için tüm makul imkânları kullanır. Yeni ZDİ ve ZDUE sürümleri, eski sürümlerle birlikte ArkSigner bilgi deposunda, ayrıntılı sürüm bilgisi içerecek şekilde yayımlanır ve ilgili tarafların erişimine açık tutulur.

13.10.3 Nesne Tanımlayıcı Numaralarının Değişmesini Gerektiren Durumlar

Zaman damgası içeriğindeki bilgi alanlarında veya ArkSigner'ın zaman damgası hizmetlerinde uyguladığı güvenlik kriterlerinde güvenlik düzeyine etki edecek değişiklikler olması durumunda, ZDİ kitapçığında tanımlanan zaman damgası ilkelerinin nesne tanımlayıcı numarası değiştirilir.

13.11 Anlaşmazlıkların Çözümü

ArkSigner, zaman damgası sahipleri ve üçüncü taraflar arasında çıkabilecek anlaşmazlıklarda, öncelikle ZDİ ve ZDUE kitapçıklarında belirlenmiş ilke ve uygulama esasları ile prosedürler ve sözleşmeler uyarınca sorunun çözümlenmesine çalışılır. Zaman damgası hizmetleriyle ilgili işlemler ArkSigner tarafından Kanun ve Yönetmelikler ile bunlara bağlı Tebliğler uyarınca yürütülür. Taraflar arasındaki anlaşmazlıklar sulhen çözüme kavuşmadığı takdirde ,anlaşmazlıkların çözümü için Ankara Mahkemeleri yetkilidir.

13.12 Yasal Düzenleme

Türkiye'de zaman damgası hizmetleri, 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 de sorumludur.

13.13 İlgili Yasalara Uygunluk

ArkSigner, zaman damgası hizmetlerini 5070 sayılı "Elektronik İmza Kanunu" ve Bilgi Teknolojileri ve İletişim Kurumu tarafından yayımlanmış Yönetmelik ve Tebliğler uyarınca yürütür.

13.14 Kitapçık Kısımlarının Ayrılabilirliği

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

13.15 Mücbir Sebepler

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