

**e-imza KIBRIS  
Zaman Damgası  
Uygulama Esasları**

**Denizler Bilişim Hizmetleri Limited**

**Sürüm 1.0**

**Yürürlük Tarihi: 1.06.2016**

**OID**

**2.16.792.3.0.011.1.3.2**

**36/B, Mimar Mehmet Vahip Caddesi, Dumlupınar Mahallesi, Lefkoşa / KKTC.**

Tel : +90 (392) 225 5260

Fax : +90 (392) 2255276

Web Adresi : <http://www.e-imzakibris.com>

---

## **e-imza KIBRIS Zaman Damgası Uygulama Esasları**

© 2016 Denizler Bilişim Hizmetleri Limited. Her hakkı saklıdır.

### **Açıklamalar ve Uyarılar**

Bu dokümanda kullanılan markalar Denizler Bilişim Hizmetleri Limited, Moso Technologies Limited veya ilgili tarafların mülkiyetindedir.

Yukarıda belirtilen haklar saklı kalmak kaydıyla ve aşağıda özel olarak aksine izin verilen durumlar hariç olmak üzere, bu yayının hiçbir parçası, önceden Denizler Bilişim'in izni alınmadan herhangi bir formda veya herhangi bir araçla (elektronik, mekanik, fotokopi, kayıt veya başka araçlar) çoğaltılamaz, aktarılamaz ya da bir veri okuma sistemine kaydedilemez veya işlenemez.

Bununla birlikte, (i) yukarıdaki telif hakkı uyarısının ve giriş paragraflarının her bir nüshanın başında açıkça gösterilmesi ve (ii) bu dokümanın, Denizler Bilişim'e atıf yapılarak, bir bütün halinde ve hatasız kopyalanması şartıyla, bu eserin ücreti ödenmeden çoğaltılmasına ve dağıtılmasına izin verilebilir. Bununla birlikte çoğaltma ve dağıtım izni herhangi bir kişiye münhasıran verilmez.

e-imza KIBRIS Zaman Damgası Uygulama Esasları (ZDUE); 93/2007 Sayılı Elektronik İmza Yasası ve ilgili mevzuat uyarınca ve ETSI TS 101 456, ETSI TS 102 023, CWA 14167-1, IETF RFC 3647 standartlarına uygun olarak hazırlanmıştır. İşbu ZDUE ile ilgili yorum ve uyuşmazlıklar öncelikle Denizler Bilişim ile uyuşmazlığın karşı tarafı veya dokümanla ilgili olan kişi arasında akdedilen işbu ZDUE'ye atıfta bulunan sözleşme veya taahhütname ile yorumlamaya konu olan olayın meydana geldiği ve uyuşmazlıkların ortaya çıktığı zaman yürürlükte olan ZDUE'nin hükümleri çerçevesinde değerlendirilecektir. İşbu ZDUE'de geçen terimler, değerlendirmeler ve açıklamalar 93/2007 Sayılı Elektronik İmza Yasası'nın kapsamındadır. İşbu ZDUE ile ilgili uyuşmazlıklarda ve yorumlamalarda 93/2007 Sayılı Elektronik İmza Yasası hükümleri ve bu kanunla ilgili mevzuat geçerli olacaktır.

İşbu ZDUE içerisinde [www.e-izmakibris.com](http://www.e-izmakibris.com) web sitesinden erişilebileceği veya e-izmakibris.com uzantılı elektronik posta adresinden bildirimde bulunulabileceği belirtilen

iletiřim adresi, bilgi, belge ve dokümanlara <http://www.e-imzakibris.com> sitesinden ulařılabilecektir.

İřbu e-imza KIBRIS Zaman Damgası Uygulama Esasları ile ilgili çoğaltılma izinleri (ve yanı sıra e-imza KIBRIS'dan kopyalarının temini) için talepler "Denizler Biliřim Hizmetleri Limited'in, **36/B, Mimar Mehmet Vahip Caddesi, Lefkořa/KKTC** Adresine ,Uygulama ve Geliřtirme Bölümü Dikkatine yapılmalıdır. Tel: +90 (392) 225 5260 Faks: +90 (392) 225 5276 Elektronik Posta: [info@e-imzakibris.com](mailto:info@e-imzakibris.com)

### **Teřekkür**

Denizler Biliřim Hizmetleri Limited, dokümanın yazılmasında ve incelenmesinde görev alan teknoloji, hukuk ve politika gibi çeřitli alanlarda uzman olan çok sayıda kiřiye, özellikle Cüneyt ÇERKEZ, Vehbi AKTÜN ve Nofel BAYLAROV'a, iř ortakları MOSO Technologies Limited ve Elektronik Bilgi Güvenliđi A.ř.'e katkılarından dolayı sonsuz teřekkür eder.

## İÇİNDEKİLER

Giriş.....	6
1. Kapsam.....	6
2. Referanslar .....	7
3. Kısaltmalar .....	8
4. Genel Hükümler .....	12
4.1. Zaman Damgası Hizmetleri.....	12
4.2. ESHS (Zaman Damgası Hizmet Sağlayıcısı).....	12
4.3. Kullanıcılar.....	12
4.4. Zaman Damgası İlkeleri (ZDİ) ve Zaman Damgası Uygulama Esasları (ZDUE) ...	13
4.4.1. Amaç .....	13
4.4.2. Özgüllük Seviyesi .....	13
4.4.3. Yaklaşım.....	13
5. Zaman Damgası Uygulama Esasları .....	13
5.1. Genel .....	13
5.2. Tanımlama.....	13
5.3. Kullanıcı Grubu ve Uygulanabilirlik.....	14
5.4. Uyumluluk.....	14
6. Yükümlülükler ve Sorumluluklar.....	14
6.1. ESHS Yükümlülükleri.....	14
6.1.1. Genel .....	14
6.1.2. Kullanıcılara Karşı ESHS Yükümlülükleri .....	14
6.2. Kullanıcı Yükümlülükleri .....	15
6.3. Üçüncü Kişilerin Yükümlülükleri .....	15
6.4. Sorumluluklar.....	15
7. ESHS Hizmetlerinin Gereksinimleri .....	15
7.1. Uygulama Esasları ve İlkeleri .....	15
7.1.1. ESHS Uygulama Esasları.....	15
7.1.2. ESHS İlkeleri.....	15
7.2. Anahtar Yönetimi Yaşam Döngüsü .....	15
7.2.1. Zaman Damgası Ünitesi Kapalı Anahtar Koruması.....	15
7.2.2. Zaman Damgası Ünitesi Özel Anahtar Koruması.....	16
7.2.2.1 Şifreleme Modülü Standartları ve Kontrolleri .....	16
7.2.2.2 İmza Oluşturma Verisi (n* m) Birden Fazla Kişi Kontrolü.....	16
7.2.2.3 İmza Oluşturma Verisinin Saklanması.....	16
7.2.2.4 İmza Oluşturma Verisi Yedekleme .....	16
7.2.2.5 İmza Oluşturma Verisi Arşivleme.....	17
7.2.2.6 İmza Oluşturma Verisinin Aktif Hale Getirilmesinin Metodu.....	17
7.2.2.7 İmza Oluşturma Verisinin Aktif Durumdan Çıkarılmasının Metodu .....	17
7.2.3. Zaman Damgası Ünitesi Açık Anahtar Dağıtımı .....	17
7.2.4. Zaman Damgası Ünitesi Anahtarının Yeniden Anahtarlanması .....	17
7.2.5. Zaman Damgası Ünitesi Anahtar Yaşam Döngüsünün Sonlandırılması .....	17
7.2.6. Zaman Damgası Hizmetinde Kullanılan Şifreleme Modüllerinin Yaşam Döngüsü Yönetimi .....	17
7.3. Zaman Damgası Hizmeti.....	18
7.3.1. Zaman Damgası.....	18

7.3.2.	UTC ile Saat Senkronizasyonu .....	19
7.4.	ESHS Zaman Damgası Sağlayıcı Yönetimi ve Operasyonları .....	19
7.4.1.	Güvenlik Yönetimi .....	19
7.4.1.1	Güvenli Roller .....	19
7.4.1.2	Her Bir Görev için Gereken Kişi Sayısı .....	20
7.4.1.3	Her Bir Görev için Tanımlama ve Kimlik Kontrolü .....	21
7.4.1.4	Sorumlulukların Ayrılmasını Gerektiren Roller .....	21
7.4.2.	Risk Değerlendirmesi .....	21
7.4.3.	Personel Güvenliği .....	21
7.4.3.1	Mesleki Bilgi, Nitelikler, Deneyim ve Resmi Makam İzinlerinin Şartları ..	21
7.4.3.2	Mesleki Bilgi Kontrol Prosedürleri .....	22
7.4.3.3	Eğitim Şartları .....	22
7.4.3.4	Eğitim Sıklığı ve Şartları .....	22
7.4.3.5	Yetkisiz Eylemlere Karşı Yaptırımlar .....	22
7.4.3.6	Bağımsız Yüklenici İsterleri .....	23
7.4.3.7	Personele Verilen Dokümanlar .....	23
7.4.4.	Fiziksel ve Çevresel Güvenlik .....	23
7.4.4.1	Güven Merkezi Konumu ve İnşası .....	23
7.4.4.2	Fiziksel Erişim .....	23
7.4.4.3	Elektrik ve Klima Koşulları .....	24
7.4.4.4	Suya Karşı Korunma .....	24
7.4.4.5	Yangın Önlemleri ve Korunması .....	24
7.4.4.6	Veri Araçları Saklanması .....	24
7.4.4.7	Atık Kontrolü .....	24
7.4.4.8	Arka Plan Yedeklemesi .....	25
7.4.5.	Operasyon Yönetimi .....	25
7.4.6.	Sistem Erişimi Yönetimi .....	25
7.4.7.	Güvenilir Ortam .....	25
7.4.8.	ESHS Zaman Damgası İmza Oluşturma Verisinin Açığa Çıkması .....	25
7.4.9.	ESHS Zaman Damgası Hizmet Sağlayıcısı İptali .....	26
7.4.10.	Yasal Gerekliliklere Uyumluluk .....	26
7.4.11.	ESHS Zaman Damgası Sağlayıcı Faaliyet Günlüğü .....	26
7.5.	Organizasyonel Plan .....	26

## Giriş

93/2007 sayılı Elektronik İmza Yasası ile “Elektronik Sertifika Hizmet Sağlayıcısı – (ESHS)”ların tanımları yapılmış, hak ve yükümlülükleri belirtilmiştir. Yasaya göre ülke içerisinde ESHS olarak görev yapacak kişi ve kurumlar Bilgi Teknolojileri ve Haberleşme Kurumu’na bildirimde bulunarak Yasa ve ilgili mevzuattaki gereksinimleri yerine getirmek zorundadırlar. Yasaya göre nitelikli elektronik sertifikaları sağlama yetkisi münhasıran ESHS'lere verilmiştir.

Denizler Bilişim, e-imza KIBRIS markası ile, Yasa ve ilgili mevzuattaki gereksinimleri yerine getirerek Bilgi Teknolojileri ve Haberleşme Kurumu’na bildirimde bulunmuş ve gerekli yetkiye sahip bir “**Elektronik Sertifika Hizmet Sağlayıcısı (ESHS)**”dır.

Bu doküman e-imza KIBRIS Zaman Damgası Uygulama Esasları’dır (ZDUE). ZDUE, 93/2007 Sayılı Elektronik İmza Yasası ve ilgili mevzuat hükümlerine uygun olarak hazırlanmıştır. ZDUE aynı zamanda Bilgi Teknolojileri ve Haberleşme Kurumu tarafından<sup>1</sup> yayımlanan, Elektronik İmza Yasasının Uygulanmasına İlişkin Usul ve Esaslar Tüzüğü ve Elektronik İmzaya İlişkin Süreçler ile Teknik Kriterlere İlişkin Yönetmelik’te atıfta bulunulan Avrupa Telekomünikasyon Standartları Enstitüsü (ETSI), Avrupa Standardizasyon Komitesi (CEN), İnternet Mühendisliği Görev Grubu’nun (IETF) nitelikli elektronik sertifika ilkeleri ve zaman damgası ilkeleri ile ilgili standartları ETSI TS 101 456, ETSI TS 102 023, CWA 14167-1, IETF RFC 3647 standartlarına uyumlu olacak şekilde hazırlanmıştır. ZDUE Yönetmelik’te belirtildiği üzere ETSI TS 102 023 uyumlu olacak şekilde hazırlanmıştır. ZDUE kapsamında verilen hizmetlerde ETSI TS 101 456, CWA 14167–1 ve ETSI TS 101 861 standartlarına uyulur.

## 1. Kapsam

Bu doküman, e-imza KIBRIS’in sunduğu zaman damgası hizmetlerine özgü teknik ve hukuki nitelikleri, faaliyetlerini, altyapısını, ilgili tarafları ve bu tarafların hak ve yükümlülüklerini açıklamak ve kamuoyuna duyurmak üzere hazırlanmıştır.

---

<sup>1</sup> Elektronik İmza Yasasının uygulanmasına ilişkin ikincil düzenleme yapma yetkisi Elektronik İmza Yasasının 20. maddesi ile Bilgi Teknolojileri ve Haberleşme Kurumu’na verilmiştir.

## 2. Referanslar

e-imza KIBRIS Nitelikli Elektronik Sertifika Uygulama Esasları (NESUE)

e-imza KIBRIS Genel Kullanıma İlişkin Nitelikli Elektronik Sertifika İlkeleri (GKNESİ)

e-imza KIBRIS Mobil Kullanıma İlişkin Nitelikli Elektronik Sertifika İlkeleri (MKNESİ)

e-imza KIBRIS Zaman Damgası İlkeleri (ZDİ)

ETSI TS 102 023

ETSI TS 101 861

ETSI TS 101 456

CWA 14167-1

RFC 3161

RFC 3628

### 3. Kısaltmalar

<b><u>KAVRAM/KISALTMA</u></b>	<b><u>AÇIKLAMA/TANIM</u></b>
<b>Başvuru Yöntemleri</b>	ESHS ile NES başvurusunda bulunan kişi arasında başvurunun yapılması, sertifika sahibinin kimliğinin tespiti, gerekli evrakların hazırlanması, sertifika ücretlerinin ödenmesi, evrakların saklanması, nitelikli elektronik sertifikaların yayınlanması ve sertifika sahibi'ne iletilmesi, sertifika iptal, yenileme ve askı taleplerinin iletimindeki usuller gibi hususların belirlendiği teknik ve idari süreçlerden oluşan yöntemler. Bu yöntemlere ESHS'nin Web adresinden ulaşılabilir.
<b>CEN</b>	Comité Européen de Normalisation - Avrupa Standardizasyon Komitesi
<b>CWA</b>	CEN Workshop Agreement- CEN Çalıştay Kararı
<b>ÇSDP</b>	Çevrimiçi Sertifika Durum Protokolü
<b>EAL</b>	Evaluation Assurance Level - Değerlendirme Garanti Düzeyi
<b>e-imza KIBRIS</b>	Denizler Bilişim Hizmetleri Limited ve Moso Technologies Limited şirketlerinin ortak girişiminin marka adıdır
<b>Elektronik İmza Yasası</b>	11 Aralık 2007 tarih 219 sayılı Resmi Gazete'de yayımlanan 93/2007 Sayılı Yasa.
<b>ESHS</b>	Elektronik Sertifika Hizmet Sağlayıcı
<b>Erişim Verisi</b>	Güvenli elektronik imza oluşturma araçlarına erişim için kullanılan parola, biyometrik değer gibi verileri.
<b>ETSI</b>	European Telecommunication Standardization Institute- Avrupa Telekomünikasyon Standartları Enstitüsü
<b>ETSI TS</b>	ETSI Technical Specifications - ETSI Teknik Özellikleri
<b>GKNESİ</b>	Genel Kullanıma İlişkin Nitelikli Elektronik Sertifika İlkeleri
<b>Güvenli Elektronik İmza</b>	Güvenli elektronik imza; Münhasıran imza sahibine bağlı olan, Sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan, Nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan, İmzalanmış elektronik veride sonradan herhangi bir değişiklik yapıp yapılmadığının tespitini sağlayan, Elle atılmış imza ile aynı hukuki sonuçları doğuran Elektronik imzadır.



<p><b>Güvenli Elektronik İmza Doğrulama Aracı</b></p>	<p>Güvenli elektronik imza doğrulama araçları;  İmzanın doğrulanması için kullanılan verileri, değiştirmeksizin doğrulama yapan kişiye gösteren,  İmza doğrulama işlemini güvenilir ve kesin bir biçimde çalıştıran ve doğrulama sonuçlarını değiştirmeksizin doğrulama yapan kişiye gösteren,  Gerektiğinde, imzalanmış verinin güvenilir bir biçimde gösterilmesini sağlayan,  İmzanın doğrulanması için kullanılan elektronik sertifikanın doğruluğunu ve geçerliliğini güvenilir bir biçimde tespit ederek sonuçlarını değiştirmeksizin doğrulama yapan kişiye gösteren,  İmza sahibinin kimliğini değiştirmeksizin doğrulama yapan kişiye gösteren,  İmzanın doğrulanması ile ilgili şartlara etki edecek değişikliklerin tespit edilebilmesini sağlayan ve CWA 14171 standardına uygun imza doğrulama araçlarıdır.</p>
<p><b>Güvenli Elektronik İmza Oluşturma Aracı</b></p>	<p>Güvenli elektronik imza oluşturma araçları;  Ürettiği elektronik imza oluşturma verilerinin kendi aralarında bir eşi daha bulunmamasını,  Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin araç dışına hiçbir biçimde çıkarılmamasını ve gizliliğini,  Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin, üçüncü kişilerce elde edilememesini, kullanılmamasını ve elektronik imzanın sahteciliğe karşı korunmasını,  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 araçlardır.</p>
<p><b>Güvenli Personel</b></p>	<p>NES yaşam zinciri ve güvenli elektronik imza oluşturma aracı yönetim kontrolleri, anahtar yönetimi kontrolleri, ESHS sertifika yönetim sistemleri ve veri bankaları kontrolleri faaliyetlerini gerçekleştiren, gerekli erişim ve kontrol yetkisine sahip Denizler Bilişim veya Denizler Bilişim yetkilisi personeli (Bkz. NESUE 5.2.1)</p>
<p><b>IETF RFC</b></p>	<p>Internet Engineering Task Force Request for Comments - İnternet Mühendisliği Görev Grubu Yorum Talebi</p>

<b>ISO/IEC</b>	International Organisation for Standardisation / International Electrotechnical Committee - Uluslararası Standardizasyon Teşkilatı / Uluslararası Elektroteknik Komitesi.
<b>Yasa</b>	11 Aralık 2007 tarih 219 sayılı Resmi Gazete'de yayımlanan 93/2007 Sayılı Yasa.
<b>Kayıt Makamı (KM)</b>	ESHS'ye bağlı olarak faaliyette bulunan, NES başvurusunda bulunan kişiler ile Kurumsal Başvuru Sahipleri'nin NES başvurularını alan ESHS'nin yetkili birimi.
<b>Kimlik Bilgileri</b>	NES Sahibinin Adı-Soyadı, Kuzey Kıbrıs Türk Cumhuriyeti Kimlik Numarası, doğum yeri, doğum tarihi ve uyuşu.
<b>Kurumsal Başvuru Sahibi</b>	Bir tüzel kişiliğin çalışanları veya müşterileri veya üyeleri veya hissedarları adına yaptığı nitelikli elektronik sertifika başvurusunu ESHS ile Kurumsal Başvuru Sözleşmesi akdetmiş olan ve bu sözleşme hükümleri ve Tüzüğü'nün 9. maddesi uyarınca çalışanları veya müşterileri veya üyeleri veya hissedarları adına nitelikli elektronik sertifika başvurusunda bulunan tüzel kişilik.
<b>MKNESİ</b>	Mobil Kullanıma İlişkin Nitelikli Elektronik Sertifika İlkeleri
<b>Mobil İmza</b>	Mobil terminaller ve GSM ağı kullanılarak yaratılan Güvenli Elektronik İmza
<b>Mobil Operatör</b>	Mobil operatör, elektronik imza uygulamasında aktif operasyonlarda bulunan sujelere; kendi altyapısı üzerinden iş ve işlemlerde bulunma imkanı sağlamaktadır.
<b>NES</b>	Nitelikli Elektronik Sertifika
<b>NESUE</b>	Nitelikli Elektronik Sertifika Uygulama Esasları
<b>NES Sahibi</b>	Adına ESHS tarafından NES düzenlenen gerçek kişi.
<b>Nitelikli Elektronik Sertifika</b>	93/2007 Sayılı Yasanın 10. Maddesinde içerik olarak; Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin 'in Yönetmeliğın 6. Maddesinde ise teknik bakımdan özellikleri belirtilen elektronik sertifika.
<b>OID</b>	Object Identifier - Nesne belirteci.
<b>Sertifika İlkesi (Sİ)</b>	Sertifikaların belli bir topluluk ve/veya genel güvenlik gereklilikleri olan uygulamalar bakımından kabul edilebilirliğini belirten kurallar bütününe Sertifika İlkeleri denilmektedir. Sertifika İlkeleri, Elektronik Sertifika Hizmet Sağlayıcıları tarafından umuma açıklanan yukarıda belirtilen amaçları karşılamaya yönelik bir belgedir. ESHS tarafından yayınlanan Sİ'ye, Sİ içerisinde belirtilen tüm katılımcılar

	uymak zorundadır. Sİ, duruma göre zaman zaman yapılabilecek değişiklikleri de dahil olmak üzere, ESHS'nin web sitesinden erişilebilir. İşbu doküman içerisinde geçen Nitelikli Elektronik Sertifika İlkeleri tamlaması Sertifika İlkesi tamlaması ile eş anlamlı olarak kullanılmıştır.
<b>SİL</b>	Sertifika İptal Listesi.
<b>SSCD</b>	Secure Signature Creation Device – Güvenli İmza Oluşturma Aracı
<b>Sertifika Uygulama Esasları</b>	NES Sahip'leri başta olmak üzere Sİ içerisinde tanımlanan her bir tarafın Sİ içinde tanımlı operasyonları gerçekleştirmek için uymak zorunda olduğu gerekliliklerin tespit edildiği, uygulamaların ve prosedürlerin açıklandığı, belli süreçler içerisinde güncellenen ve ESHS tarafından umuma yapılan bir açıklamadır. Sertifika Uygulama Esasları, duruma göre zaman zaman yapılabilecek değişiklikleri de dahil olmak üzere, ESHS'nin web sitesinden erişilebilir. İşbu doküman içerisinde geçen Nitelikli Elektronik Sertifika Uygulama Esasları” tamlaması Sertifika Uygulama Esasları tamlaması ile eş anlamlı olarak kullanılmaktadır.
<b>Yönetmelik</b>	25 Aralık 2008 tarih 223 sayılı Resmi Gazete’de yayımlanan Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Yönetmelik.
<b>KKTC</b>	Kuzey Kıbrıs Türk Cumhuriyeti
<b>Üçüncü Kişiler</b>	Denizler Bilişim tarafından düzenlenmiş NES’lerle bağlı güvenli elektronik imza oluşturma verisi ile yaratılmış güvenli elektronik imzalara dayanarak menfi ve müspet açıdan iş ve işlemlerde bulunan gerçek ve tüzel kişiler.
<b>Tüzük</b>	21 Ekim 2008 tarih 760 sayılı Resmi Gazete’de yayımlanan Elektronik İmza Yasasının Uygulanmasına İlişkin Usul ve Esaslar Tüzüğü.
<b>ZDUE</b>	Zaman Damgası Uygulama Esasları
<b>ZDİ</b>	Zaman Damgası İlkeleri

## 4. Genel Hükümler

### 4.1. Zaman Damgası Hizmetleri

Zaman Damgası, 93/2007 sayılı Elektronik İmza Yasası'nda tanımlandığı üzere "elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı ve / veya kaydedildiği zamanın tespit edilmesi amacıyla, elektronik sertifika hizmet sağlayıcısı tarafından elektronik imzayla doğrulanan kayıt"tır.

e-imza KIBRIS zaman damgası hizmetleri ile ilgili olarak Zaman Damgası Hizmet Sağlayıcısı olarak hizmet verir. Zaman damgası hizmetleri şu iki temel bileşenden oluşmaktadır:

- Zaman damgası çıkaran teknik bileşen
- Zaman damgası çıkarılmasını yöneten, izleyen ve kontrol eden sistem lojistiği.

### 4.2. ESHS (Zaman Damgası Hizmet Sağlayıcısı)

93/2007 sayılı Elektronik İmza Yasası kapsamında zaman damgası yayınlayan ve zaman damgası yönetimi ve operasyonları ile ilgili hizmet veren bir ESHS'dir. Denizler Bilişim zaman damgası hizmetlerinin sunulmasında dış kaynak kullanımı yöntemini kullanabilir; bu durumda dış kaynak hizmet sağlayıcısı faaliyet gösterdiği kapsamda, mevzuat ile Denizler Bilişim'e tanımlanan yükümlülükleri Denizler Bilişim ile olan sözleşme ilişkisi doğrultusunda yerine getirmektedir.

### 4.3. Kullanıcılar

#### Zaman Damgası Sahibi

Zaman damgası sahibi, zaman damgası hizmet sağlayıcısına başvurarak zaman damgası isteminde bulunan, bu istem sonucunda kendisine zaman damgası üretilen gerçek veya tüzel kişidir.

#### Üçüncü Kişiler

Üçüncü kişiler, zaman damgalı bir veriye veya elektronik imzaya güvenerek işlem yapan gerçek veya tüzel kişilerdir.

## **4.4. Zaman Damgası İlkeleri (ZDİ) ve Zaman Damgası Uygulama Esasları (ZDUE)**

### **4.4.1. Amaç**

ZDUE, Denizler Bilişim'in ESHS olarak sağladığı zaman damgası hizmetlerinin gerektirdiği ve Denizler Bilişim'in yerine getirdiği hukuki ve teknik nitelikleri, organizasyonel yapıyı ve hizmetlerin sağlanmasında ilgili tarafların hak ve yükümlülüklerini belirtmek amacıyla yayınlanmıştır.

ZDİ, Denizler Bilişim'in *hangi* zaman damgası hizmetlerini sunduğunu belirtirken, ZDUE söz konusu hizmetlerin Denizler Bilişim tarafından *nasıl* gerçekleştirildiğini tanımlar.

### **4.4.2. Özgüllük Seviyesi**

ZDUE zaman damgası çıkarılması ve yöneltmesinde geçerli olacak kuralların sadece genel olanlarını tanımlamaktadır. Sistemin detaylı tanımı, genelde kamuya açık olmayan ek dokümanlarda verilir. Kamuya açık olmayan dokümanlarla birlikte raporlar, ekipman değerlendirme ve dahili kontrol sonuçları, dokümantasyon dizisini meydana getirir ve sadece yetkili personel ile Bilgi Teknolojileri ve Haberleşme Kurumu'nun kontrolüne açıktır

### **4.4.3. Yaklaşım**

ZDUE, "NESUE" ve yukarıda belirtilen ek dokümanlar ile birlikte "e-imza KIBRIS" ESHS Zaman Damgası Sağlayıcısı'nın tüm işleyiş ve yönetim süreçlerini tanımlar.

## **5. Zaman Damgası Uygulama Esasları**

### **5.1. Genel**

ZDUE, e-imza KIBRIS tarafından sağlanan zaman damgası hizmetlerini kapsayan genel kuralları ortaya koyar. Bu doküman bu sürecin katılımcılarını tanımlar, sorumluluklarını, haklarını ve uygulanabilirlik aralığını belirtir. Bu dokümanın ilgili yerlerinde geniş açıklamalarla ilgili olarak NESUE'ye atıfta bulunulmuştur.

### **5.2. Tanımlama**

**Zaman Damgası Uygulama Esasları için Belirteç**

e-imza KIBRIS Zaman Damgası Uygulama Esasları Sürüm 1.0

**Nesne Belirteci** : 2.16.792.3.0.011.1.3.2

### **Zaman Damgası İlkeleri için Belirteç**

e-imza KIBRIS Zaman Damgası İlkeleri Sürüm 1.0

**Nesne Belirteci** : 2.16.792.3.0.011.1.3.1

## **5.3. Kullanıcı Grubu ve Uygulanabilirlik**

ZDUE, e-imza KIBRIS Zaman Damgası Hizmet Sağlayıcısı tarafından çıkarılan zaman damgalarını kapsar; bahsedilen zaman damgalarının kamuya açık veya sınırlı/kapalı bir ortamda sağlanmış olması ZDUE'nin kullanılabilirliği açısından fark yaratmaz

## **5.4. Uyumluluk**

ZDUE, Yönetmelik'te belirtilen ETSI TS 102 023 standardına uygun olarak hazırlanmıştır. e-imza KIBRIS zaman damgası hizmetlerinde CWA 14167-1 ve ETSI TS 101 861 standartlarına uyar

## **6. Yükümlülükler ve Sorumluluklar**

### **6.1. ESHS Yükümlülükleri**

#### **6.1.1. Genel**

e-imza KIBRIS zaman damgası hizmetlerini yerine getirirken işbu ZDUE ve elektronik imza mevzuatı ile belirlenen gereksinimleri yerine getirir.

#### **6.1.2. Kullanıcılara Karşı ESHS Yükümlülükleri**

e-imza KIBRIS, zaman damgası hizmetlerini CWA 14171-1, ETSI TS 101 456 ve ETSI TS 102 203 standartlarına uyararak ve olağandışı durumlar haricinde 7/24 hizmete verecek şekilde yürütür.

## **6.2. 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.

## **6.3. 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.

## **6.4. Sorumluluklar**

Denizler Bilişim ve diğer ilgili taraflar, ZDUE ve elektronik imza mevzuatı ile belirlenen yükümlülüklerini yerine getirmedikleri takdirde, yükümlülüklerini yerine getirmemelerinden ortaya çıkan diğer tarafların zararlarını tazminle sorumludurlar.

## **7. ESHS Hizmetlerinin Gereksinimleri**

### **7.1. Uygulama Esasları ve İlkeleri**

#### **7.1.1. ESHS Uygulama Esasları**

Bkz. ZDUE 4.4

#### **7.1.2. ESHS İlkeleri**

Bkz. ZDUE 4.4

### **7.2. Anahtar Yönetimi Yaşam Döngüsü**

#### **7.2.1. Zaman Damgası Ünitesi Kapalı Anahtar Koruması**

Zaman Damgası Hizmet Sağlayıcısı sertifikası imza oluşturma ve doğrulama verileri yaratma işlemi, yaratılan veriler için güvenliği ve gerekli şifreleme gücünü temin eden güvenilir

sistemler kullanılarak, önceden seçilmiş birden fazla güvenli personel tarafından yerine getirilir. Zaman Damgası Hizmet Sağlayıcısı sertifikasının, imza oluşturma ve doğrulama verilerini yaratmada kullanılan şifreleme modüllerinin bileşenleri FIPS 140-2 Seviye 3 şartlarını karşılar.

Denizler Bilişim iş gereklilikleri doğrultusunda birden fazla Zaman Damgası Hizmet Sağlayıcısı sertifikası üretebilecek, bunları ve ilgili sistemleri birbirlerinden farklı lokasyonlarda barındırabilecektir. İşbu dokümanda Zaman Damgası Hizmet Sağlayıcısı sertifikası ile ilgili olarak belirlenen kurallar tüm Zaman Damgası Hizmet Sağlayıcısı sertifikaları için uygulanacaktır.

## **7.2.2. Zaman Damgası Ünitesi Özel Anahtar Koruması**

### **7.2.2.1 Şifreleme Modülü Standartları ve Kontrolleri**

e-imza KIBRIS, Zaman Damgası Hizmet Sağlayıcısı sertifikası imza oluşturma ve doğrulama verilerini yaratma işlemleri için FIPS 140-2 Seviye 3 onaylı bileşenlere sahip donanım şifreleme modülleri kullanır.

### **7.2.2.2 İmza Oluşturma Verisi (n\* m) Birden Fazla Kişi Kontrolü**

e-imza KIBRIS Zaman Damgası Hizmet Sağlayıcısı sertifikasının imza oluşturma verilerinin kullanılmasını gerektiren işlemler en az iki güvenli personelin katılımıyla ve gerekli tanımlama ve güvenlik kontrollerinin yerine getirilmesiyle gerçekleştirilir.

### **7.2.2.3 İmza Oluşturma Verisinin Saklanması**

e-imza KIBRIS, Zaman Damgası Hizmet Sağlayıcısı sertifikasının imza oluşturma verisini, resmi makamların erişimi amacıyla dahi olsa herhangi bir üçüncü şahsa vermez.

### **7.2.2.4 İmza Oluşturma Verisi Yedekleme**

e-imza KIBRIS, rutin ve felaketten kurtarma amaçlarıyla e-imza KIBRIS, rutin ve felaketten kurtarma amaçlarıyla Zaman Damgası Hizmet Sağlayıcısı sertifikasının imza oluşturma verilerinin yedek kopyalarını oluşturur. Bu veriler, Güven Merkezi dışındaki güvenli bir lokasyonda saklanır.



### **7.2.2.5 İmza Oluşturma Verisi Arşivleme**

e-imza KIBRIS Zaman Damgası Hizmet Sağlayıcısı sertifikasının imza oluşturma ve doğrulama verileri arşivlenmez.

### **7.2.2.6 İmza Oluşturma Verisinin Aktif Hale Getirilmesinin Metodu**

e-imza KIBRIS Zaman Damgası Hizmet Sağlayıcısı sertifikasının imza oluşturma verilerinin aktivasyonu, her zaman damgası talebinde gerçekleşir.

### **7.2.2.7 İmza Oluşturma Verisinin Aktif Durumdan Çıkarılmasının Metodu**

e-imza KIBRIS Zaman Damgası Hizmet Sağlayıcısı sertifikasının imza oluşturma verisi, imzalama için kullanıldıktan sonra veriye erişim otomatik olarak kesilir.

### **7.2.3. Zaman Damgası Ünitesi Açık Anahtar Dağıtımı**

e-imza KIBRIS, Zaman Damgası Hizmet Sağlayıcısı sertifikasının imza doğrulama verilerini de içeren Zaman Damgası Hizmet Sağlayıcısı sertifikası <http://www.e-izakibris.com/databank/principles> adresinden indirilebilir.

### **7.2.4. Zaman Damgası Ünitesi Anahtarının Yeniden Anahtarlanması**

e-imza KIBRIS, Zaman Damgası Hizmet Sağlayıcısı sertifikasının imza oluşturma verisinin geçerlilik süresi, seçilen algoritma ve anahtar uzunluğunun kabul edilmiş olan geçerlilik süresinden uzun olamaz.

### **7.2.5. Zaman Damgası Ünitesi Anahtar Yaşam Döngüsünün Sonlandırılması**

e-imza KIBRIS, Zaman Damgası Hizmet Sağlayıcısı sertifikasının imza oluşturma verileri geçerlilik sürelerinin sona ermesinden itibaren veya güvenlik problemleri sebebiyle gerekli teknik ve fiziksel güvenlik önlemleri altında sadece birden çok yetkili güvenli personel tarafından yok edilebilir.

### **7.2.6. Zaman Damgası Hizmetinde Kullanılan Şifreleme Modüllerinin Yaşam Döngüsü Yönetimi**

e-imza KIBRIS, Zaman Damgası Hizmet Sağlayıcısı sertifikasının imza oluşturma ve doğrulama verileri, verilerin kullanılacağı donanım şifreleme modüllerinde yaratır. Denizler Bilişim, ayrıca, rutin ve felaketten kurtarma amaçlarıyla bu Zaman Damgası Hizmet Sağlayıcısı sertifikasının imza oluşturma ve doğrulama verilerinin kopyalarını yaratır. Zaman

Damgası Hizmet Sağlayıcısı sertifikasının imza oluşturma ve doğrulama verilerinin başka bir medyaya yedeklenmesi durumunda bu imza oluşturma ve doğrulama verileri şifrelenmiş formda aktarılır.

### **7.3. Zaman Damgası Hizmeti**

#### **7.3.1. Zaman Damgası**

e-imza KIBRIS ESHS Zaman Damgası Hizmet Sağlayıcı tarafından çıkarılan her zaman damgası özel bir tanımlayıcı içerir. e-imza KIBRIS ESHS Zaman Damgası Hizmet Sağlayıcısı tarafından çıkarılan her zaman damgası gerçek UTC zaman değerine kadar geriye doğru izlenebilecek tarih ve zaman değeri içermektedir. Temel saat GPS uydu alıcısı ve atomik saati ile sunulmaktadır. e-imza KIBRIS ESHS Zaman Damgası Hizmet Sağlayıcısı, uydu saatinin arızalanması durumunda ikincil saatlere sahiptir. Zaman damgasında kullanılan zamanın doğruluğu ZDUE 7.3.2'de açıklanmıştır. Bu bilgiyi zaman damgası belirteç içinde sunmak mecburi değildir.

e-imza KIBRIS önceden takvime bağlanmış ve ayrı dokümanlarda belirtilmiş ekipman ve sistem bakımıyla ilgili teknik çalışmada zamanları dışında zaman damgası hizmetlerine sürekli erişimi garanti eder. Zaman damgası içine yerleştirilen UTC zamanı  $\pm 100$  ms doğruluk oranı sunar. Servis birçok eş zamanlı bağlantı arasında doğruluk ve kesinlik sunar ve doğruluk oranı  $\pm 30$  s olacak şekilde değiştirilebilir

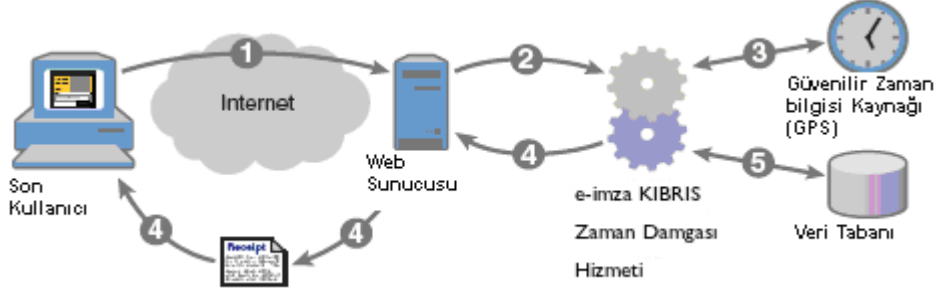
Ana saatin bozulması ya da kalibrasyona ihtiyaç duyması halinde, e-imza KIBRIS ESHS Zaman Damgası Hizmet Sağlayıcısı zamanı ikincil saatten öğrenir.

Zaman damgası, zaman damgası talebi (TSQ) yapan öznelerin verdiği veriye göre çıkarılır. Yanıttaki (TSR) belirteçleri, TSQ belirteçte sunulan veriyi içerir. Zaman damgası tanımlayıcı, ETSI 102 023 standardının 7.3.1 h başlığında belirtilen "Zaman Damgası Tanımlayıcı" gerekliliklerine uyar.

e-imza KIBRIS ESHS Zaman Damgası Sağlayıcısı zaman damgası hizmeti şu esaslarla çalışır:

- Elektronik bir zaman damgası yaratılması, güvenilir bir kaynaktan zamanın alınması ve bu zaman bilgisinin zaman damgasıyla ilişkilendirilecek verinin parmak izi bilgisiyle birleştirilmesiyle gerçekleşir

- Zaman damgası için, e-imza KIBRIS ESHS Zaman Damgası Hizmet Sağlayıcısı'nın elektronik imzasıyla imzalanmasıyla "Elektronik Makbuz" elde edilir,
- "Elektronik Makbuz" talep eden tarafa iletilir,
- "Elektronik Makbuz" ve ilgili bilgi saklanır.



### 7.3.2. UTC ile Saat Senkronizasyonu

e-imza KIBRIS önceden takvime bağlanmış ve ayrı dokümanlarda belirtilmiş ekipman ve sistem bakımıyla ilgili teknik çalışmada zamanları dışında zaman damgası hizmetlerine sürekli erişimi garanti eder. Zaman damgası içine yerleştirilen UTC zamanı  $\pm 100$  ms doğruluk oranı sunar. Servis birçok eş zamanlı bağlantı arasında doğruluk ve kesinlik sunar ve doğruluk oranı  $\pm 30$  s olacak şekilde değiştirilebilir.

## 7.4. ESHS Zaman Damgası Sağlayıcı Yönetimi ve Operasyonları

### 7.4.1. Güvenlik Yönetimi

#### 7.4.1.1 Güvenli Roller

NES yaşam zinciri, zaman damgası hizmetleri ve güvenli elektronik imza oluşturma aracı yönetim kontrolleri, anahtar yönetimi kontrolleri, ESHS sertifika yönetim sistemleri ve veri bankaları kontrolleri, gerekli erişim ve kontrol yetkisine sahip güvenli personel tarafından yürütülür. Güvenli personel, faaliyet alanlarına göre; elektronik imza teknolojisi, bilgi güvenliği ve risk yönetimi konularında yeterli bilgi ve tecrübe seviyesine sahip kişilerden seçilir. Güvenli personel tanımları aşağıdaki şekildedir;

- Güven Merkezi ve Güvenlik Yöneticisi: Güvenlik sisteminin tüm politika ve prensiplerinin belirlenmesi, uygulanması, onaylanması görev, yetki ve sorumluluğuna sahip güvenli personel
- Sistem Denetçisi: ESHS güvenli sistemlerinin denetim kayıtlarına ve arşivlerine erişme ve devamlılığını sağlama görev ve yetkisine sahip güvenli personel
- Güven Merkezi Sistem Yöneticisi: NES başvuruları yönetimi, NES oluşturulması, güvenli elektronik imza oluşturma araçları yönetimi, sertifika iptal yönetimi için kullanılan ESHS güvenli sistemlerini kurma, konfigüre etme ve bakımını yapma görev ve yetkisine sahip güvenli personel
- Güven Merkezi İşletim Sistemi ve Veritabanı Yöneticisi: Güven Merkezi'nde koşan yazılımların üzerinde koştuğu işletim sisteminin ve veritabanlarının konfigüre edilmesi, yönetilmesi; bunların tuttukları kayıtların ve arşivlerin işletilmesi görev ve yetkisine sahip güvenli personel
- Güven Merkezi Ağ Yöneticisi: Güven Merkezi ağ yapısının yönetilmesi, kullanıcı ihlallerinin tespiti ve raporlanması görev ve sorumluluğuna sahip personel
- Kayıt Makamı (RA) Sistem İşletmenleri: NES'lerin oluşturulması, iptali, askıya alınması konularında onaylama görev ve yetkisine sahip güvenli personel.
- Güven Merkezi Sistem İşletmenleri: ESHS güvenli sistemlerini günlük bazda kullanma, sistem yedeklemesi ve kurtarma fonksiyonlarını kullanma görev ve yetkisine sahip güvenli personel

Güvenli personel, "Personel Prosedürü" doğrultusunda NESUE 5.3'deki kriterleri yerine getiren kimseler arasından; Güven Merkezi ve Güvenlik Yöneticisi veya Denizler Bilişim Direktörü tarafından seçilir ve görevlendirilir.

#### **7.4.1.2 Her Bir Görev için Gereken Kişi Sayısı**

Denizler Bilişim, görevlerin sorumluluklara göre ayrılmasını sağlamak için sıkı kontrol prosedürleri uygular. ESHS şifreleme donanımına (kriptografik imzalama ünitesi veya CSU) ve ilgili anahtar malzemesine erişim gibi en hassas görevler birden fazla güvenilen şahıs gerektirir.

Bu dahili kontrol prosedürleri, cihaza fiziksel veya mantıksal erişime sahip olmak için en az iki güvenilen personelin gerekli olmasını sağlayacak şekilde tasarlanmıştır. ESHS şifreleme donanımına erişim, ilk alındığı ve kontrolden geçirildiği andan son mantıksal ve/veya fiziksel imhaya kadar donanımın ömrü boyunca daima birden fazla güvenilen şahısla sağlanır. Bir modül, işlem kodlarıyla devreye alındığında, cihaza hem fiziksel, hem de mantıksal erişim üzerinde ikili kontrol sağlamak için süreklilik arz eden erişim kontrolleri uygulanır.

#### **7.4.1.3 Her Bir Görev için Tanımlama ve Kimlik Kontrolü**

Güvenli personel, yetkileri doğrultusunda gerçekleştirecekleri faaliyetleri için tanımlama kontrollerine tabi tutulurlar. Tanımlama kontrolleri için güvenli personelin kimlik ve biyolojik bilgileri alınarak güvenlik sistemine kaydedilir.

#### **7.4.1.4 Sorumlulukların Ayrılmasını Gerektiren Roller**

Bazı NES sertifika yaşam zinciri işlemleri, ESHS anahtar yönetimi işlemleri, Zaman Damgası Hizmet Sağlayıcısı sertifikası anahtar yönetimi işlemleri ve bunlara ilişkin kontroller birden çok güvenli personelin katılımıyla ve sorumlulukların ayrıştırılması prensibiyle gerçekleştirilir.

#### **7.4.2. Risk Değerlendirmesi**

Bkz. ZDUE 7.4.4.1

#### **7.4.3. Personel Güvenliği**

##### **7.4.3.1 Mesleki Bilgi, Nitelikler, Deneyim ve Resmi Makam İzinlerinin Şartları**

Güvenli personel olmak isteyen kişiler, görev sorumluluklarını gerektiği gibi ve tatmin edici şekilde yerine getirmesi için gereken mesleki bilgi, nitelik ve deneyimlerini kanıtlayan belgeleri sunmalıdır.

Denizler Bilişim'in, kurucu ortakları, tüzel kişiliği temsile yetkili yöneticileri ve istihdam ettiği veya ettirdiği personeli; taksirli suçlar hariç olmak üzere, affa uğramış olsalar bile ağır hapis veya altı (6) aydan fazla hapis yahut basit veya nitelikli zimmet, irtikap, rüşvet, hırsızlık, dolandırıcılık, sahtekarlık, inancı kötüye kullanma, dolanlı iflas gibi yüz kızartıcı suçlar ile istimal ve istihlak kaçakçılığı dışında kalan kaçakçılık suçları, resmi ihale ve alım satımlara fesat karıştırma, kara para aklama veya devlet sırlarını açığa vurma, vergi kaçakçılığı ya da iştirak veya bilişim alanındaki suçlar nedeniyle hüküm giymemiş olacaktır.

İşe kabul edilen personel ile karşılıklı gizlilik ve işe alım anlaşmaları imzalanır, ve herhangi bir resmi ya da özel kuruluşa karşı hizmet yükümlülüğü bulunmaması gerekmektedir.

#### **7.4.3.2 Mesleki Bilgi Kontrol Prosedürleri**

Personel bir güvenilen konumda çalışmaya başlamadan önce, Denizler Bilişim, aşağıdakileri içeren mesleki bilgi kontrolleri yapar:

- Önceki işinin doğrulanması
- Mesleki referansın kontrolü
- Adli sicil soruşturması
- Vergi ve vatandaşlık numarası

Bir mesleki bilgi kontrolünde ortaya çıkan ve güvenilen şahıs adaylarının reddedilmesine yol açan ya da mevcut bir güvenilen şahsa karşı belirli bir hareket tarzının uygulanması için zemin oluşturduğu düşünülebilecek faktörler genel olarak aşağıda sıralanmaktadır:

- Aday veya güvenilen şahsın hatalı veya yanıltıcı beyanlarda bulunması.
- Büyük ölçüde olumsuz veya güvenilir olmayan kişisel referanslar.

Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Tüzüğü'nün 19. maddesinde belirtilen suçlardan hüküm giymiş olma.

#### **7.4.3.3 Eğitim Şartları**

Güvenli personel mesleki sorumluluklar, güvenlik prosedürleri ve politikaları konularında gerekli hukuki ve teknik eğitimden geçirilirler. Güvenli personel eğitim programları periyodik olarak gözden geçirilir ve gerekli görüldüğünde güncellenir.

#### **7.4.3.4 Eğitim Sıklığı ve Şartları**

Denizler Bilişim, personeline, iş sorumluluklarını gerektiği gibi ve tatmin edici düzeyde yerine getirmesi ve gerekli uzmanlık seviyesini muhafaza etmesini sağlamak için gereken ölçüde ve sıklıkta bilgi güncelleme eğitimi verir. Periyodik güvenlik bilinci eğitimi devamlı olarak verilmektedir.

#### **7.4.3.5 Yetkisiz Eylemlere Karşı Yaptırımlar**

Yetkisiz eylemler veya Denizler Bilişim politikalarının ve prosedürlerinin başka şekillerde ihlali durumunda gereken disiplin önlemleri alınır. Yetkisiz eylemler veya prosedür ihlali fiilleri

Elektronik İmza Yasası, ilgili diğer yasalarda belirtilen suç tanımlarına dahil olması durumunda bu eylemleri gerçekleştirenler hakkında gerekli yasal işlemler yapılır.

#### **7.4.3.6 Bağımsız Yüklenici İsterleri**

Denizler Bilişim gerekli durumlarda, ESHS faaliyetleri veya diğer faaliyetleri için bağımsız yükleniciler veya danışmanlar kullanılabilir. Bilgi güvenliği kapsamına giren konularda faaliyet gösteren yükleniciler, mevzuat ile Denizler Bilişim'e tanımlanan yükümlülükleri Denizler Bilişim ile olan sözleşme ilişkisi doğrultusunda yerine getirmektedir. Yüklenicilerin çalışanları veya danışmanlar, eşdeğer konumdaki Denizler Bilişim personeliyle aynı mesleki koşullara ve güvenlik koşullarına tâbi tutulur.

#### **7.4.3.7 Personele Verilen Dokümanlar**

Denizler Bilişim personeli ve yüklenici personeline, faaliyetleri doğrultusunda öğrenmeleri gereken gizli bilgiler dışında, yetkileri doğrultusunda kullandıkları donanım ve yazılıma ilişkin dokümanları, Denizler Bilişim ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi dokümanları (yüklenici personeli eğer varsa yüklenicinin bilgi güvenliği yönetim sistemi dokümanlarına sahip olacaklardır), NESUE, sertifika ilkeleri (GKNESİ), ZDUE ve ZDİ belgeleri verilir.

### **7.4.4. Fiziksel ve Çevresel Güvenlik**

#### **7.4.4.1 Güven Merkezi Konumu ve İnşası**

Bütün e-imza KIBRIS ESHS operasyonları, gizli veya açık müdahaleleri durduracak, önleyecek ve tespit edecek şekilde tasarlanmış, fiziksel olarak korunan bir Güven Merkezi içinde yürütülür.

Denizler Bilişim ile yaptığı özel sözleşme ile kendi bünyesinde sistem kurulan kurumsal başvuru sahipleri, kayıt makamları ve diğer üçüncü partiler kendi bünyelerinde yürütecekleri operasyonlarla ilgili güvenli tesislerinin, kendileri ile yapılan sözleşmede belirtilen güvenlik şartlarını karşılamasını sağlamalıdır.

#### **7.4.4.2 Fiziksel Erişim**

e-imza KIBRIS ESHS sistemleri ve Güven Merkezi, "Fiziksel ve Çevresel Güvenlik Prosedürü" doğrultusunda çeşitli fiziksel güvenlik seviyeleriyle korunur. Yüksek bir seviyeye sahip bir alana veya sisteme erişim yapılmadan önce alçak seviyelere erişilmelidir.

Her katmana erişim fiziksel erişim kontrolleri aracılığı ile gerçekleşir. Her katmana erişim sadece güvenli personele ait olan güvenlik kartlarıyla gerçekleşir. Tüm fiziksel erişim hareketleri otomatik olarak kaydedilir ve video ile de görüntüsel kayıt altına alınır. İleri katmanlara erişim biometrik tanımlamanın da kullanıldığı iki faktörlü doğrulama kontrolüyle gerçekleşir. Güvenli personel özelliğine sahip olmayan personelin veya ziyaretçilerin refakatsiz olarak güvenli alanlara girmesine izin verilmemektedir. İmza oluşturma verisi cihazlarına ve yan ürünlerine erişim yetkilerin ayrımı kurallarının gereğince yerine getirilir.

#### **7.4.4.3 Elektrik ve Klima Koşulları**

e-imza KIBRIS'ın güvenli tesisleri aşağıdaki sistemlere ait ana ve yedek sistemlerle donatılmıştır:

- Elektrik gücüne sürekli ve kesintisiz erişim sağlamak için elektrik sistemleri.
- Sıcaklığı ve nispi nemi kontrol etmek için ısıtma/havalandırma/klima sistemleri.

#### **7.4.4.4 Suya Karşı Korunma**

Güven Merkezi, su baskınları ve sele karşı gerekli yalıtım sistemleri ve su dedektörleri ile korunmakta ve izlenmektedir.

#### **7.4.4.5 Yangın Önlemleri ve Korunması**

Güven Merkezi, yangınları veya hasara yol açan diğer alev veya duman vakalarını önlemek ve söndürmek için yangın alarmları, ısı dedektörleri ve yangın söndürme sistemleri ile donatılmıştır.

#### **7.4.4.6 Veri Araçları Saklanması**

Üretimde kullanılan yazılım ve veriler ile denetim, arşiv veya yedekleme bilgilerini içeren bütün araçlar Denizler Bilişim tesislerinde veya erişimi yetkili kişilerle sınırlandırılarak ve araçları kazayla hasara (örneğin, su, yangın ve elektromanyetik) karşı koruyacak şekilde tasarlanarak, uygun fiziksel ve mantıksal erişim kontrollerine sahip Güven Merkezi dışındaki güvenli depolama tesislerinde muhafaza edilir.

#### **7.4.4.7 Atık Kontrolü**

Denizler Bilişim ESHS işleyişi uyarınca kayıtları tutulan tüm organizasyonel bilgiler, süreleri geldiğinde imha edilirler. Elektronik kayıtların yetkili olmayan kişiler tarafından görülmesi, değiştirilmesi ve/veya silinmesi önlenmiştir. Kağıt üzerinde bulunan kayıtlar ise sadece yetkili



kişilerin girme izni bulunan özel birimlerde tutulurlar. Yedekleme prosedürü uyarınca tüm kayıtlar yedeklenir. Kağıt ya da elektronik ortamda saklanan tüm bilgi ve belgeler saklanmaları gerekmiyorsa “Kayıt İmha Prosedürü”ne göre imha edilir. Kriptografik modüller atılmaları gerektiğinde ya fiziksel olarak imha edilir ya da üretici firma talimatları doğrultusunda sıfırlanır.

#### **7.4.4.8 Arka Plan Yedeklemesi**

e-imza KIBRIS, kritik sistem verilerini, denetim kaydı verilerini ve diğer gizli bilgileri “İş Sürekliliği ve Felaketten Kurtarma Planı” çerçevesinde rutin olarak yedekler.

#### **7.4.5. Operasyon Yönetimi**

e-imza KIBRIS zaman damgası hizmetleri operasyonlarını ETSI TS 101 861, ETSI TS 102 023 ve CWA 14167-1 standartlarına uygun olarak yürütür.

#### **7.4.6. Sistem Erişimi Yönetimi**

Denizler Bilişim güvenli personelinin erişim verileri, parolaları ve biyometrik verileri içerir. Güvenli personelin parolaları kendileri tarafından yaratılır ve değiştirilebilir niteliğe sahiptir. Biyometrik veriler ise yetkili güvenli personel eşliğinde sisteme kaydedilir.

Erişim verilerinin güvenli personele iletilmesinden veya kendileri tarafından yaratılmasından sonra, verilerin gizliliğinin ve güvenliliğinin korunmasıyla ilgili sorumluluk NES sahiplerine ve güvenli personele aittir. Güvenli personele iletilmeyen erişim verileri kasalarda ve farklı lokasyonlardaki fiziksel güvenliğe sahip alanlarda saklanırlar

#### **7.4.7. Güvenilir Ortam**

Bkz. ZDUE 7.4.4.1

#### **7.4.8. ESHS Zaman Damgası İmza Oluşturma Verisinin Açığa Çıkması**

e-imza KIBRIS Zaman Damgası Hizmet Sağlayıcısı sertifikasına ait imza oluşturma verilerinin gizliliğinin ve güvenilirliğinin şüphe altında olması halinde e-imza KIBRIS Zaman Damgası Hizmet Sağlayıcısı sertifikası iptal edilir. e-imza KIBRIS Zaman Damgası Hizmet Sağlayıcısı sertifikasının iptal edilmesi durumu [www.e-izmakibris.com](http://www.e-izmakibris.com) web sitesinden kamuoyuna ve ilgililere duyurulur.

#### **7.4.9. ESHS Zaman Damgası Hizmet Sağlayıcısı İptali**

e-imza KIBRIS'ın ESHS faaliyetlerini durdurması gerektiği durumlarda, ESHS operasyonları durdurulmadan önce son kullanıcıları, kurumsal başvuru sahiplerini, üçüncü kişileri ve diğer ilgili kuruluşları bundan haberdar etmek için ticari açıdan gerekli her türlü çabayı gösterir. Operasyonun durdurulması kararının verilmesinden sonra e-imza KIBRIS ESHS işleyişinde kendisine yardımcı olan bağlı kişi ve kuruluşlarla (Kayıt Makamları, araç sağlayıcılar, v.s. ) olan sözleşmelerini sonlandırır.

Elektronik İmza Yasası'nın Uygulanmasına İlişkin Usul ve Esaslar Tüzüğü'nün 22 ve 23. maddelerine göre Denizler Bilişim'in faaliyetlerine kendisi veya Bilgi Teknolojileri ve Haberleşme Kurumu tarafından son vermesi halinde sorumluluk ve yükümlülükleri NESUE 5.8.1 ve NESUE 5.8.2'de açıklanmaktadır.

#### **7.4.10. Yasal Gerekliliklere Uyumluluk**

İşbu ZDUE 93/2007 sayılı Elektronik İmza Yasası, Elektronik İmza Uygulanmasına İlişkin Usul ve Esaslar Tüzüğü, Zorunlu Sertifika Mali Sorumluluk Sigortası ve Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Yönetmelik'te referans gösterilen uluslararası standartlara uygun olarak hazırlanmıştır.

#### **7.4.11. ESHS Zaman Damgası Sağlayıcı Faaliyet Günlüğü**

e-imza KIBRIS zaman damgası hizmetleri sistemi zaman damgalarının yayınlanmasıyla ilgili her türlü olayı kayıt altına alır.

### **7.5. Organizasyonel Plan**

e-imza KIBRIS, zaman damgası hizmetlerini ESHS yetkisi ve görevi altında yürütür.