E-GÜVEN

ZAMAN DAMGASI UYGULAMA ESASLARI

Açıklamalar ve Uyarılar

Bu dokümanda kullanılan markalar Elektronik Bilgi Güvenliği A.Ş 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 Elektronik Bilgi Güvenliği A.Ş.'nin 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, Elektronik Bilgi Güvenliği A.Ş.'ye 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-Güven Zaman Damgası Uygulama Esasları (ZDUE); 5070 Sayılı Elektronik İmza Kanunu 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 E-Güven 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 5070 Sayılı Elektronik İmza Kanunu'nun kapsamındadır. İşbu ZDUE ile ilgili uyuşmazlıklarda ve yorumlamalarda 5070 Sayılı Elektronik İmza Kanunu hükümleri ve bu kanunla ilgili mevzuat geçerli olacaktır.

İşbu ZDUE içerisinde Elektronik Bilgi Güvenliği A.Ş. web sitesinden erişilebileceği veya e-guven.com uzantılı elektronik posta adresinden bildirimde bulunulabileceği belirtilen iletişim adresi, bilgi, belge ve dokümanlara http://www.e-guven.com sitesinden ulaşılabilecektir.

İşbu E-Güven Zaman Damgası Uygulama Esasları ile ilgili çoğaltılma izinleri (ve yanı sıra E-Güven'den kopyalarının temini) için talepler "Elektronik Bilgi Güvenliği A.Ş.'nin,

Değirmen Sokak Nida Kule İş Merkezi No:18 Kat:5 34742 Kozyatağı - İSTANBUL

Adresine, Uygulama ve Geliştirme Bölümü Dikkatine yapılmalıdır. Tel: +90 216 360 46 05 Faks: +90 216 360 33 56 Elektronik Posta: info@e-guven.com

Teşekkür

Elektronik Bilgi Güvenliği A.Ş., dokümanın incelenmesinde görev alan ve hukuk, politika ve teknoloji gibi çok çeşitli alanlarda uzman olan çok sayıda kişiye katkılarından dolayı teşekkür eder.

İÇİNDEKİLER

Giriş

5070 sayılı Elektronik İmza Kanunu ile "Elektronik Sertifika Hizmet Sağlayıcı – (ESHS)"ların tanımları yapılmış, hak ve yükümlülükleri belirtilmiştir. Kanuna göre ülke içerisinde ESHS olarak görev yapacak kişi ve kurumlar Bilgi Teknolojileri ve İletişim Kurumu'na bildirimde bulunarak Kanun ve ilgili mevzuattaki gereksinimleri yerine getirmek zorundadırlar. Kanuna göre nitelikli elektronik sertifikaları sağlama yetkisi münhasıran ESHS'lere verilmiştir.

E-Güven, Kanun ve ilgili mevzuattaki gereksinimleri yerine getirerek Bilgi Teknolojileri ve İletişim Kurumu'na bildirimde bulunmuş ve gerekli yetkiye sahip bir "Elektronik Sertifika Hizmet Sağlayıcısı (ESHS)"dır.

Bu doküman E-Güven Zaman Damgası Uygulama Esasları'dır (ZDUE). ZDUE, 5070 Sayılı Elektronik İmza Kanunu ve ilgili mevzuat hükümlerine uygun olarak hazırlanmıştır. ZDUE aynı zamanda Bilgi Teknolojileri ve İletişim Kurumu tarafından[1] yayımlanan, Elektronik İmza Kanunun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik ve Elektronik İmzaya İlişkin Süreçler ile Teknik Kriterlere İlişkin Tebliğ'de 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 Tebliğ'de 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-Güven'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.

2. Referanslar

E-Güven Nitelikli Elektronik Sertifika Uygulama Esasları (NESUE)
E-Güven Genel Kullanıma İlişkin Nitelikli Elektronik Sertifika İlkeleri (GKNESİ)
E-Güven Mobil Kullanıma İlişkin Nitelikli Elektronik Sertifika İlkeleri (MKNESİ)
E-Güven Zaman Damgası İlkeleri (ZDİ)
ETSI TS 102 023
ETSI TS 101 861
ETSI TS 101 456
CWA 14167–1
RFC 3161
RFC 3628

[1] Elektronik İmza Kanununun uygulanmasına ilişkin ikincil düzenleme yapma yetkisi Elektronik İmza Kanunun 20. maddesi ile Bilgi Teknolojileri ve İletişim Kurumu'na verilmiştir.

3. Kısaltmalar

KAVRAM/KISALTMA	AÇIKLAMA/TANIM
Başvuru Yöntemleri	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.
CEN	Comité Européen de Normalisation - Avrupa Standardizasyon Komitesi
CWA	CEN Workshop Agreement- CEN Çalıştay Kararı
ÇSDP	Çevrimiçi Sertifika Durum Protokolü
EAL	Evaluation Assurance Level - Değerlendirme Garanti Düzeyi
Elektronik İmza Kanunu	23 Ocak 2004 tarih 25355 sayılı Resmi Gazete'de yayımlanan 5070 Sayılı Kanun.
ESHS	Elektronik Sertifika Hizmet Sağlayıcı
Erişim Verisi	Güvenli elektronik imza oluşturma araçlarına erişim için kullanılan parola, biyometrik değer gibi verileri.
ETSI	European Telecommunication Standartization Institute- Avrupa Telekomünikasyon Standartları Enstitüsü
ETSI TS	ETSI Technical Specifications - ETSI Teknik Özellikleri
GKNESİ	Genel Kullanıma İlişkin Nitelikli Elektronik Sertifika İlkeleri
Güvenli Elektronik İmza	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 yapılıp yapılmadığının tespitini sağlayan, Elle atılmış imza ile aynı hukuki sonuçları doğuran Elektronik imzadır.
Güvenli Elektronik İmza Doğrulama Aracı	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.
Güvenli Elektronik İmza Oluşturma Aracı	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 çıkarılamamasını ve gizliliğini, Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin, üçüncü kişilerce elde edilememesini, kullanılamamasını 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.
Güvenli Personel	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 E-Güven veya E-Güven yetkilisi personeli (Bkz. NESUE 5.2.1)
IETF RFC	Internet Engineering Task Force Request for Comments - İnternet Mühendisliği Görev Grubu Yorum Talebi
ISO/IEC	International Organisation for Standardisation / International Electrotechnical Commitee - Uluslararası Standardizasyon Teşkilatı / Uluslararası Elektroteknik Komitesi.
Kanun	23 Ocak 2004 tarih 25355 sayılı Resmi Gazete'de yayımlanan 5070 Sayılı Elektronik İmza Kanunu
Kayıt Makamı (KM)	ESHS'ye bağlı olarak faaliyette bulunan, NES başvurusunda bulunan kişiler ile Kurumsal Başvuru Sahipleri'nin NES başvurularını alan ESHS'nin yetkili birimi.
Kimlik Bilgileri	NES Sahibinin Adı-Soyadı, Türkiye Cumhuriyeti Kimlik Numarası, doğum yeri, doğum tarihi ve uyruğu.
Kurumsal Başvuru Sahibi	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 Yönetmeliğin 3. ve 9. maddeleri uyarınca çalışanları veya müşterileri veya üyeleri veya hissedarları adına nitelikli elektronik sertifika başvurusunda bulunan tüzel kişilik.
MKNESİ	Mobil Kullanıma İlişkin Nitelikli Elektronik Sertifika İlkeleri
Mobil İmza	Mobil terminaller ve GSM ağı kullanılarak yaratılan Güvenli Elektronik İmza

Mobil Operatör	Mobil operatör, elektronik imza uygulamasında aktif operasyonlarda bulunan sujelere; kendi altyapısı üzerinden iş ve işlemlerde bulunma imkanı sağlamaktadır.
NES	Nitelikli Elektronik Sertifika
NESUE	Nitelikli Elektronik Sertifika Uygulama Esasları
NES Sahibi	Adına ESHS tarafından NES düzenlenen gerçek kişi.
Nitelikli Elektronik Sertifika	5070 Sayılı Kanunun 9. Maddesinde içerik olarak; Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'in 5. Maddesinde ise teknik bakımdan özellikleri belirtilen elektronik sertifika.
OID	Object Identifier - Nesne belirteci.
Sertifika İlkesi (Sİ)	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.
SİL	Sertifika İptal Listesi.
SSCD	Secure Signature Creation Device – Güvenli İmza Oluşturma Aracı
Sertifika Uygulama Esasları	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 içersinde 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.
Tebliğ	6 Ocak 2005 tarih 25692 sayılı Resmi Gazete'de yayımlanan Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ
TC	Türkiye Cumhuriyeti
Üçüncü Kişiler	E-Güven 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.
Yönetmelik	6 Ocak 2005 tarih 25692 sayılı Resmi Gazete'de yayımlanan Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik.
ZDUE	Zaman Damgası Uygulama Esasları
ZDİ	Zaman Damgası İlkeleri

4. Genel Hükümler

4.1. Zaman Damgası Hizmetleri

Zaman Damgası, 5070 sayılı Elektronik İmza Kanunu'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-Güven 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)

E-Güven 5070 sayılı Elektronik İmza Kanunu kapsamında zaman damgası yayınlayan ve zaman damgası yönetimi ve operasyonları ile ilgili hizmet veren bir ESHS'dir.

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

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

4.4.2. Özgüllük Seviyesi

ZDUE zaman damgası çıkarılması ve yöneltilmesinde 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 İletişim Kurumu'nun kontrolüne açıktır

4.4.3. Yaklaşım

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

5. Zaman Damgası Uygulama Esasları

5.1. Genel

ZDUE, E-Güven 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-Güven Zaman Damgası Uygulama Esasları Sürüm 1.0

Nesne Belirteci : 2.16.792.3.0.1.1.3.1

Zaman Damgası İlkeleri için Belirteç

E-Güven Zaman Damgası İlkeleri Sürüm 1.0

Nesne Belirteci : 2.16.792.3.0.1.1.3.2

5.3. Kullanıcı Grubu ve Uygulanabilirlik

ZDUE, E-Güven 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, Tebliğ'de belirtilen ETSI TS 102 023 standardına uygun olarak hazırlanmıştır. E-Güven 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-Güven zaman damgası hizmetlerini yerine getirirken işbu ZDUE ve elektronik imza mevzuatı ile belirlenen gereksinimleri yerine getirir.

6.1.2. Kullanıcılara Karşı ESHS Yükümlülükleri

E-Güven, zaman damgası hizmetlerini CWA 14171-1, ETSI TS 101 456 ve ETSI TS 102 203 standartlarına uyarak 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

E-Güven 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.

7.2.2. Zaman Damgası Ünitesi Özel Anahtar Koruması

7.2.2.1. Şifreleme Modülü Standartları ve Kontrolleri

E-Güven, 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-Güven 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-Güven, 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-Güven, rutin ve felaketten kurtarma amaçlarıyla E-Güven, 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-Güven Zaman Damgası Hizmet Sağlayıcısı sertifikasının imza oluşturma ve doğrulama verileri arşivlenmez.

7.2.2.6. İmza Oluşturma Verisinin Aktif Hale Getirilmesinin Metodu

E-Güven 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-Güven 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-Güven, Zaman Damgası Hizmet Sağlayıcısı sertifikasının imza doğrulama verilerini de içeren Zaman Damgası Hizmet Sağlayıcısı sertifikası https://www.e-guven.com/bilgi-bankasi adresinden indirilebilir.

7.2.4. Zaman Damgası Ünitesi Anahtarının Yeniden Anahtarlanması

E-Güven, 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-Güven, 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-Güven, Zaman Damgası Hizmet Sağlayıcısı sertifikasının imza oluşturma ve doğrulama verileri, verilerin kullanılacağı donanım şifreleme modüllerinde yaratır. E-Güven, 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-Güven ESHS Zaman Damgası Hizmet Sağlayıcı tarafından çıkarılan her zaman damgası özel bir tanımlayıcı içerir. E-Güven ESHS Zaman Damgası Hizmet Sağlayıcı 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-Güven ESHS Zaman Damgası Hizmet Sağlayıcı, 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-Güven önceden takvime bağlanmış ve ayrı dokümanlarda belirtilmiş ekipman ve sistem bakımıyla ilgili teknik çalışmama zamanları dışında zaman damgası hizmetlerine sürekli erişimi garanti eder. Zaman damgası içine yerleştirilen UTC zamanı ±100 ms doğruluk oranı sunar. Servis birçok eş zamanlı bağlantı arasında doğruluk ve kesinlik sunar ve doğruluk oranı ±30 s olacak şekilde değiştirilebilir

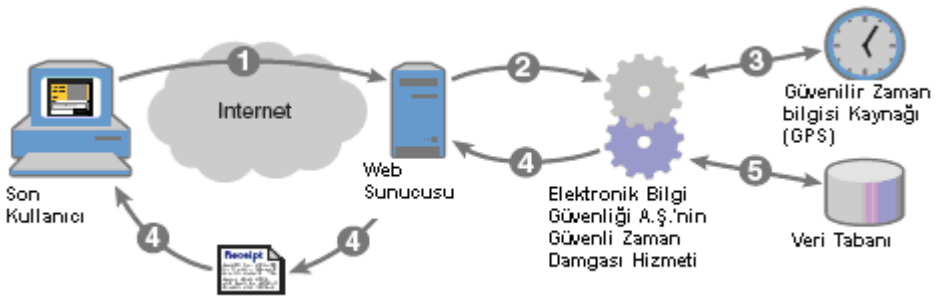
Ana saatin bozulması ya da kalibrasyona ihtiyaç duyması halinde, E-Güven ESHS Zaman Damgası Hizmet Sağlayıcı zamanı ikincil saatten öğrenir.

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-Güven ESHS Zaman Damgası Sağlayıcı 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-Güven ESHS Zaman Damgası Hizmet Sağlayıcı'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-Güven önceden takvime bağlanmış ve ayrı dokümanlarda belirtilmiş ekipman ve sistem bakımıyla ilgili teknik çalışmama zamanları dışında zaman damgası hizmetlerine sürekli erişimi garanti eder. Zaman damgası içine yerleştirilen UTC zamanı ±100 ms doğruluk oranı sunar. Servis birçok eş zamanlı bağlantı arasında doğruluk ve kesinlik sunar ve doğruluk oranı ±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 E-Güven Genel Müdürü tarafından seçilir ve görevlendirilir.

7.4.1.2. Her Bir Görev için Gereken Kişi Sayısı

E-Güven, 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. Sorumlukların 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.

E-Güven'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, personelin T.C. vatandaşı olması veya T.C 'de ikamet ve çalışma izni almış olması, 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, E-Güven, 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 Hakkında Yönetmeliğin 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

E-Güven, 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 E-Güven politikalarının ve prosedürlerinin başka şekillerde ihlali durumunda gereken disiplin önlemleri alınır. Yetkisiz eylemler veya prosedür ihlali fiilleri Elektronik İmza Kanunu, Türk Ceza Kanunu veya ilgili diğer kanunlarda belirtilen suç tanımlarına dahil olması durumunda bu eylemleri gerçekleştirenler hakkında gerekli yasal işlemler yapılır.

7.4.3.6. Bağımsız Yüklenici İsterleri

E-Güven gerekli durumlarda, ESHS faaliyetleri veya diğer faaliyetleri için bağımsız yükleniciler veya danışmanlar kullanılabilir. Bilgi güvenliği kapsamına giren konularda faaliyet gösteren yükleniciler, yüklenicilerin çalışanları veya danışmanlar, eşdeğer konumdaki E-Güven personeliyle aynı mesleki koşullara ve güvenlik koşullarına tâbi tutulur.

7.4.3.7. Personele Verilen Dokümanlar

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

7.4.4. Fiziksel ve Çevresel Güvenlik

7.4.4.1. Güven Merkezi Konumu ve İnşası

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

E-Güven ile yaptığı özel sözleşme ile kendi bünyesinde sistem kurulan kurumsal başvuru sahipleri ve kayıt makamları kendi bünyelerinde yürütecekleri operasyonlarla ilgili güvenli tesislerinin, kendileri ile yapılan sözleşmede belirtilen güvenlik şartlarını karşılamasını sağlamalıdır.

7.4.4.2. Fiziksel Erişim

E-Güven 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 biyometrik 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-Güven'in 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 E-Güven 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

E-Güven 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 "Varlık Yönetimi 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-Güven, kritik sistem verilerini, denetim kaydı verilerini ve diğer gizli bilgileri "İş Sürekliliği Planı" çerçevesinde rutin olarak yedekler.

7.4.5. Operasyon Yönetimi

E-Güven 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

E-Güven 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-Güven Zaman Damgası Hizmet Sağlayıcısı sertifikasına ait imza oluşturma verilerinin gizliliğinin ve güvenilirliğinin şüphe altında olması halinde E-Güven Zaman Damgası Hizmet Sağlayıcısı sertifikası iptal edilir. E-Güven Zaman Damgası Hizmet Sağlayıcısı sertifikasının iptal edilmesi durumu E-Güven web sitesinden kamuoyuna ve ilgililere duyurulur.

7.4.9. ESHS Zaman Damgası Hizmet Sağlayıcısı İptali

E-Güven'in 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-Güven ESHS işleyişinde kendisine yardımcı olan bağlı kişi ve kuruluşlarla (Kayıt Makamları, araç sağlayıcılar, v.s.) olan sözleşmelerini sonlardır.

Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmeliğin 29 ve 30. maddelerine göre E-Güven'in faaliyetlerine kendisi veya Bilgi Teknolojileri ve İletişim 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 5070 sayılı Elektronik İmza Kanunu, Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik, Zorunlu Sertifika Mali Sorumluluk Sigortası Yönetmeliği ve Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ ve Tebliğ'de referans gösterilen uluslararası standartlara uygun olarak hazırlanmıştır.

7.4.11. ESHS Zaman Damgası Sağlayıcı Faaliyet Günlüğü

E-Güven zaman damgası hizmetleri sistemi zaman damgalarının yayınlanmasıyla ilgili her türlü olayı kayıt altına alır.

7.5. Organizasyonel Plan

E-Güven, zaman damgası hizmetlerini ESHS yetkisi ve görevi altında yürütür.

REVİZYON DURUMU		
Revizyon Tarihi	**Revizyon No**	**Açıklama**