EBG Bilişim Teknolojileri ve Hizmetleri A.Ş

ZAMAN DAMGASI iLKELERİ

(ZDİ)

Sürüm 1.0

Yürürlük Tarihi: Haziran, 2006

OID
2.16.792.3.0.4.1.1.3

EBG Bilişim Teknolojileri ve Hizmetleri A.Ş
Tel: 0-312-472 21 13
www.e-tugra.com

EBG Bilişim Teknolojileri ve Hizmetleri A.Ş **Zaman Damgası ilkeleri**

Açıklamalar ve Uyarılar

İÇİNDEKİLER

Giriş

EBG Bilişim Teknolojileri ve Hizmetleri A.Ş. (Kısaca “e-Tuğra”) Türk Ticaret Kanunu hükümlerine uyarınca kurularak faaliyetlerini sürdüren bir anonim şirkettir. “e-Tuğra”, 5070 sayılı Elektronik İmza Kanunu’nun 8. Maddesi hükmü uyarınca, Telekominikasyon Kurumu’na usulü dairesinde bildirimde bulunarak ve kanuni gereklilikleri yerine getirerek Elektronik Sertifika Hizmet Sağlayıcı (Kısaca “ESHS”) sıfatıyla “elektronik imza”, “elektronik sertifika” ve “zaman damgası” ile ilgili hizmetleri sunma hak ve yetkisini elde etmiştir.

Zaman Damgası İlkeleri (kısaca “ZDİ”) olarak isimlendirilen bu doküman 5070 sayılı Elektronik İmza Kanunu (kısaca “Kanun”), Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik (kısaca “Yönetmelik”) ile Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ (kısaca “Tebliğ”) uyarınca “e-Tuğra”nın “ESHS” sıfatıyla sunduğu zaman damgası hizmetlerine ilişkin yürüttüğü faaliyetler sırasında yerine getirdiği teknik ve hukuki gereklilikleri, “ESHS”nin zaman damgasına ilişkin faaliyetlerini, teknik ve organizasyonel altyapısını, “ESHS”nin zaman damgası hizmetlerine ilişkin süreçlerde belirli rolller üstlenen tarafların sorumluluklarını açıklamak ve kamuoyuna duyurmak üzere hazırlanmıştır. “ZDİ” dokümanı “ZDUE” dokümanında ayrıntılı olarak “nasıl” yapıldığı belirtilen “ESHS”nin zaman damgasına ilişkin süreçlerinin “ne”ler olduğunu belirler.

Bu doküman “Tebliğ”de belirtildiği üzere ETSI TS 102 023 uyumlu olacak şekilde hazırlanmıştır. Dokümanın hazırlanmasında “e-Tuğra” “ZDUE”, “e-Tuğra” “SUE”, RFC 3161, RFC 3628 dokümanları referans alınmıştır. “e-Tuğra” zaman damgası hizmetlerinin yürütümünde ETSI TS 101 456, CWA 14167–1 ve ETSI TS 101 861 standartlarına uyar.

1. Kapsam

“ZDİ” dokümanı, “e-Tuğra”nın “ESHS” sıfatıyla sunduğu zaman damgası hizmetlerine ilişkin yürüttüğü faaliyetler sırasında yerine getirdiği teknik ve hukuki gereklilikleri,

“ESHS”nin zaman damgasına ilişkin faaliyetlerini, teknik ve organizasyonel altyapısını, “ESHS”nin zaman damgası hizmetlerine ilişkin süreçlerde belirli rollller üstlenen tarafların sorumluluklarını açıklamak ve kamuoyuna duyurmak üzere hazırlanmıştır. “ZDİ” dokümanı “ZDUE” dokümanında ayrıntılı olarak “nasıl” yapıldığı belirtilen “ESHS”nin zaman damgasına ilişkin süreçlerinin “ne”ler olduğunu belirler.

2. Referanslar

ETSI TS 102 023

ETSI TS 101 861

ETSI TS 101 456

CWA 14167–1

RFC 3161

RFC 3628

e-Tuğra Sertifika Uygulama Esasları (“SUE”)

e-Tuğra Sertifika İlkeleri (“Sİ”)

e-Tuğra Zaman Damgası Uygulama Esasları (“ZDUE”)

3. Tanımlamalar ve Kısaltmalar

3.1. Tanımlar

KAVRAM/KISALTMA	AÇIKLAMA/TANIM
“Elektronik İmza Kanunu”	23 Ocak 2004 tarih 25355 sayılı Resmi Gazete’de yayımlanan 5070 Sayılı Kanun.

"Güvenli Elektronik İmza"	Güvenli elektronik imza; a) Münhasıran imza sahibine bağlı olan, b) Sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan, c) Nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan, d) İmzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan, elektronik imzadır.
"Güvenli Elektronik İmza Doğrulama Aracı"	Güvenli elektronik imza doğrulama araçları; a) İmzanın doğrulanması için kullanılan verileri, değiştirmeksizin doğrulama yapan kişiye gösteren, b) İmza doğrulama işlemini güvenilir ve kesin bir biçimde çalıştıran ve doğrulama sonuçlarını değiştirmeksizin doğrulama yapan kişiye gösteren, c) Gerektiğinde, imzalanmış verinin güvenilir bir biçimde gösterilmesini sağlayan, d) İmzanın doğrulanması için kullanılan elektronik sertifikanın doğruluğunu ve geçerliliğini güvenilir bir biçimde tespit ederek, sonuçlarını değiştirmeksizin doğrulama yapan kişiye gösteren, e) İmza sahibinin kimliğini değiştirmeksizin doğrulama yapan kişiye gösteren, f) 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; a) Ürettiği elektronik imza oluşturma verilerinin kendi aralarında bir eşi daha bulunmamasını, b) Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin araç dışına hiçbir biçimde çıkarılamamasını ve gizliliğini, c) Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin, üçüncü kişilerce elde edilememesini, kullanılamamasını ve elektronik imzanın sahteciliğe karşı korunmasını, d) İmzalanacak verinin imza sahibi dışında değiştirilememesini ve bu verinin imza sahibi tarafından imzanın oluşturulmasından önce görülebilmesini, Sağlayan ve ISO/IEC 15408 (-1,-2,-3)'e göre en az EAL4+ seviyesinde olan araçlardır.
"Güvenli e-imza	En az nitelikli elektronik sertifika ve güvenli elektronik imza

Paketi”	oluşturma aracından oluşan "ESHS" tarafından “Sertifika Kullanıcıları”na sağlanan hizmet ve ekipmanlar bütünü. “Güvenli e-imza Paketi”nin fiyatları ile içerdiği ekipmanlar ve hizmetlere ilişkin detaylı açıklama www.e-tugra.com web adresinden erişilebilir durumdadır.
“Kayıt Birimi”	"ESHS"ye bağlı olarak faaliyette bulunan “Sertifika Kullanıcıları” ile “Kurumsal Başvuru Sahipleri”nin “NES” başvurularını alan "ESHS"nin yetkili birimi. “Kayıt Birim”leri "ESHS"nin www.e-tugra.com web adresinden açıklanan yerleşik yapılar olabileceği gibi, “"ESHS"nin bu konuda yetkilendirdiği gerçek kişiler de olabilir. "ESHS"nin bu konuda yetkilendirdiği gerçek kişiler için "ESHS", fotoğraflı bir “Kayıt Birimi Yetki Belgesi” tanzim eder.
“Kimlik Bilgileri”	“Sertifika Kullanıcısı”nın; adı, soyadı, Türkiye Cumhuriyeti kimlik numarası, doğum yeri, doğum tarihi ve uyruğu.
“Kurumsal Başvuru”	Bir tüzel kişiliğin çalışanları/müşterileri/üyeleri veya hissedarları adına yaptığı nitelikli elektronik sertifika başvurusu.
“Kurumsal Başvuru Sahibi”	"ESHS" ile Kurumsal Başvuru Sözleşmesi akdetmiş olan ve bu sözleşme hükümleri ve “Yönetmelik”in 3. ve 9. maddeleri uyarınca çalışanları/müşterileri/üyeleri veya hissedarları adına nitelikli elektronik sertifika başvurusunda bulunan tüzel kişilik.
“Kurumsal Başvuru Yetkilisi”	**“**Sertifika Kullanıcısı” adına "NES" düzenlenmesi için "ESHS"ye bildirilecek olan bilgileri “Yönetmelik”in Mad. 9/1.de belirtilen belgelere dayanarak tespit eden ve “Kurumsal Başvuru Sözleşmesi” içerisinde kendisiyle ilgili belirtilen işlemleri “Kurumsal Başvuru Sahibi” adı ve hesabına yerine getiren “Kurumsal Başvuru Sahibi”nin çalışanı.
“NES” Başvuru Sahibi	“ESHS”ye bireysel veya kurumsal başvuruda bulunan kişi.
“Nitelikli Elektronik	5070 Sayılı Kanunun 9. Maddesinde içerik olarak; “Elektronik

Sertifika"	İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ"in 5. Maddesinde ise teknik bakımdan özellikleri belirtilen elektronik sertifika.
"Sertifika İlkesi"	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"ye, duruma göre zaman zaman yapılabilecek değişiklikleri de dahil olmak üzere, "ESHS"nin web sitesinden (www.e-tugra.com) erişilebilir.
"Sertifika Kullanıcısı"	Adına "ESHS" tarafından "NES" düzenlenen gerçek kişi. Bu doküman içersinde geçen "Sertifika Sahibi" ve "NES" Sahibi" kavramları "Sertifika Kullanıcısı" ile eş anlamlı olarak kullanılmaktadır.
"Sertifika Uygulama Esasları"	"Sertifika Kullanıcı"ları 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. "SUE"ye, duruma göre zaman zaman yapılabilecek değişiklikleri de dahil olmak üzere, "ESHS"nin web sitesinden (www.e-tugra.com) erişilebilir.
"Zaman Damgası"	Elektronik verinin; üretildiği, değiştirildiği, gönderildiği, alındığı ve/veya kaydedildiği zamanın tespit edilmesi amacıyla, elektronik sertifika hizmet sağlayıcısı tarafından elektronik imzayla doğrulanan kayıt.

3.2. Kısaltmalar

"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
"e-Tuğra"	EBG Bilişim Teknolojileri ve Hizmetleri A.Ş.
"ESHS"	Elektronik Sertifika Hizmet Sağlayıcı
"ETSI"	European Telecommunication Standartization Institute- Avrupa Telekomünikasyon Standartları Enstitüsü
"ETSI TS"	ETSI Technical Specifications - ETSI Teknik Özellikleri
"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.
"NES"	Nitelikli Elektronik Sertifika
"OID"	Object Identifier - Nesne betimleyicisi.
"Sİ"	Sertifika İlkesi
"SİL"	Sertifika İptal Listesi
"SSCD"	Secure Signature Creation Device – Güvenli İmza Oluşturma Aracı
"SUE"	Sertifika Uygulama Esasları
"TC"	Türkiye Cumhuriyeti
"ZDİ"	Zaman Damgası İlkeleri
"ZDUE"	Zaman Damgası Uygulama Esasları
"Tebliğ"	6 Ocak 2005 tarih 25692 sayılı Resmi Gazete'de yayımlanan "Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ".

“Yönetmelik”	6 Ocak 2005 tarih 25692 sayılı Resmi Gazete’de yayımlanan “Elektronik İmza Kanununun Uygulanmasına İlişkin Usül ve Esaslar Hakkında Yönetmelik”.

4. Genel Hükümler

4.1. Zaman Damgası Hizmetleri

Zaman Damgası, “Kanun”da 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.

Zaman damgası hizmetleri, gereksinimlerinin sınıflandırılması amacıyla belli bir ayrım yapılarak tanımlanır:

- Zaman Damgası Aracı

Bu servis zaman damgalarının oluşturulmasını sağlayan bileşenleri içerir.

- Zaman Damgası Yönetimi

Bu servis zaman damgası aracı servisinin operasyonlarının izlenmesi, denetlenmesi ve yönetilmesine ilişkin bileşenleri içerir.

4.2. “ESHS” (Zaman Damgası Hizmet Sağlayıcısı)

“e-Tuğra”, “ESHS” işleyişi içerisinde zaman damgası hizmet sağlayıcısı olarak faaliyet gösterir. Zaman damgası hizmeti “e-Tuğra” zaman damgası sertifikasıyla imzalanmış zaman damgaları ile verilir. “e-Tuğra” zaman damgası hizmetlerinin “ZDUE”ye uygunluğunu denetler.

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" dokümanı "e-Tuğra"nın "ESHS" işleyişi içerisinde zaman damgası hizmetlerine ilişkin olarak yerine getirdiği teknik ve hukuki isterleri, faaliyetleri, teknik ve organizasyonel altyapısını, zaman damgası hizmetlerinde tarafların sorumluluklarını açıklamak ve kamuoyuna duyurmak üzere hazırlanmıştır.

"ZDİ" belgesi, *hangi* zaman damgası hizmetlerinin "e-Tuğra" tarafından sunulduğunu belirlerken, "ZDUE" bu hizmetlerin "e-Tuğra" tarafından *nasıl* gerçekleştirildiğini tanımlar. "ZDUE" ve "ZDİ" dokümanları www.e-tugra.com adresinden kamuoyunun bilgi ve erişimine açık tutulur.

4.4.2. Özgüllük Seviyesi

"ZDUE" ve "ZDİ" dokümanlarında kamuoyuna açıklanmasında sakınca görülmeyen zaman damgası hizmetlerinin tanımlamaları ve açıklamaları yer almaktadır. Zaman damgası hizmetlerinin detaylı tanımları kamuya açık olmayan ve "e-Tuğra" tarafından gizli olarak kabul edilen dokümanlarda bulunmaktadır.

4.4.3. Yaklaşım

“e-Tuğra” zaman damgası hizmetleri; “ZDUE”, “ZDİ” “NESUE” ve ilgili diğer dokümanlarla tanımlanmıştır. “ZDUE” ve “ZDİ” “e-Tuğra” yetkili personeli tarafından hazırlanmış ve kamuoyunun bilgisine sunulmuştur.

5. Zaman Damgası Uygulama Esasları

5.1. Genel

“ZDUE”, “e-Tuğra” zaman damgası hizmetlerinde “ZDİ”nin belirlediği ilkeler çerçevesinde, “e-Tuğra”nin temel zaman damgası işleyiş süreçlerini ve altyapısını, tarafların hak ve yükümlülüklerini ve uygulanabilirlik alanını belirler.

5.2. Tanımlama

Zaman Damgası Uygulama Esasları için Belirteç

“e-Tuğra” Zaman Damgası Uygulama Esasları Sürüm 1.0
Nesne Belirteci : 2.16.792.3.0.4.1.1.4

Zaman Damgası İlkeleri için Belirteç

“e-Tuğra” Zaman Damgası İlkeleri Sürüm 1.0
Nesne Belirteci : 2.16.792.3.0.4.1.1.3

5.3. Kullanıcı Grubu ve Uygulanabilirlik

“e-Tuğra” zaman damgası hizmetleri, herhangi bir elektronik verinin; üretildiği, değiştirildiği, gönderildiği, alındığı ve/veya kaydedildiği zamanın tespit edilmesi amacıyla kullanılır. Bu kullanımlara örnek olarak; herhangi bir elektronik veriye bağlı güvenli elektronik imzaların uzun dönemli bir çevrimde doğrulanmasını sağlamak, güvenli elektronik imzalara eklenerek imzanın oluşturulduğu zamanını belirlemek, elektronik verilerin arşivlendiği ve bu verilere hangi zamanlarda erişildiğini belirlemek veya elektronik ortamda gerçekleşen herhangi bir hukuki işlemin gerçekleşme

zamanını tespit etmek gibi uygulamalar gösterilebilir. Zaman damgası hizmetlerinden, “e-Tuğra”nın web sitesinden yayınlanan zaman damgası hizmet bedellerini ödeyen ve “ZDUE” ve ilgili mevzuat hükümlerine uymayı kabul eden gerçek ve tüzel kişiler yararlanabilir.

5.4. Uyumluluk

Bu doküman “Tebliğ”de belirtildiği üzere ETSI TS 102 023 uyumlu olacak şekilde hazırlanmıştır. Dokümanın hazırlanmasında “e-Tuğra”, “SUE”, RFC 3161, RFC 3628 dokümanları referans alınmıştır. “e-Tuğra” zaman damgası hizmetlerinin yürütümünde CWA 14167-1, ETSI TS 101 456 ve ETSI TS 101 861 standartlarına uyar.

6. Yükümlülükler ve Sorumluluklar

6.1. “ESHS” Yükümlülükleri

6.1.1. Genel

“e-Tuğra” zaman damgası hizmetlerini yürütürken “ZDİ” 7. bölüm altında belirtilen hususları yerine getirmekle yükümlüdür. “e-Tuğra” zaman damgası hizmetleri, “e-Tuğra”nın yapacağı anlaşmalar doğrultusunda üçüncü kişiler tarafından dış kaynaklı olarak sunulabilir. Bu durumda “e-Tuğra”, zaman damgası hizmetlerinin “ZDİ”ye ve ilgili mevzuat hükümlerine uyumluluğunu sağlar ve garanti eder.

6.1.2. Kullanıcılara Karşı “ESHS” Yükümlülükleri

“e-Tuğra”, zaman damgası hizmetlerini - öngörülemeyen teknik aksaklıklar, sistem kontrolleri ve “e-Tuğra”nın kontrolü dışında ortaya çıkan durumlar dışarıda bırakılarak - haftada 7 gün 24 saat hizmet verecek şekilde sunulmasını sağlayacaktır. “e-Tuğra”, zaman damgası hizmetlerini CWA 14171-1, ETSI TS 101 456 ve ETSI TS 102 203 standartları doğrultusunda yürütür.

6.2. Kullanıcı Yükümlülükleri

Zaman damgası hizmetleri kullanıcısı, oluşturulan zaman damgasının geçerliliğini kontrol etmekle yükümlüdür. Kullanıcı zaman damgasının geçerliliğini kontrol ederken zaman damgası üzerindeki elektronik imzayı doğrulamalı ve “e-Tuğra” zaman damgası sertifikasının geçerliliğini “SİL” veya “ÇSDP” servisini kullanarak kontrol etmelidir. Kullanıcılar zaman damgasının geçerliliğini güvenli elektronik imza doğrulama aracı kullanarak da kontrol edebilirler.

6.3. Üçüncü Tarafların Yükümlülükleri

Zaman damgalı bir veriye veya imzaya güvenerek işlem yapacak üçüncü kişiler zaman damgasının geçerliliğini kontrol etmekle yükümlüdür. Üçüncü kişiler zaman damgasının geçerliliğini kontrol ederken zaman damgası üzerindeki imzayı doğrulamalı ve “e-Tuğra” zaman damgası sertifikasının geçerliliğini “SİL” veya “ÇSDP” servisini kullanarak kontrol etmelidir. Üçüncü kişiler ayrıca, zaman damgasında kullanılan hash fonksiyonunun ve zaman damgası sertifikasına ait imza oluşturma verisinin boyutunun ve kullanılan algoritmanın zaman damgasının oluşturulduğu tarihte güvenli olup olmadığını kontrol etmekle de yükümlüdürler. Üçüncü kişiler zaman damgasının geçerliliğini güvenli elektronik imza doğrulama aracı kullanarak da kontrol edebilirler.

6.4. Sorumluluklar

“e-Tuğra”, zaman damgası kullanıcıları ve üçüncü kişiler “ZDİ” ve ilgili mevzuat 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. “ZDİ” 4.4

7.1.2. “ESHS” İlkeleri

Bkz. “ZDİ” 4.4

7.2. Anahtar Yönetimi Yaşam Döngüsü

7.2.1. Zaman Damgası Ünitesi Kapalı Anahtar Koruması

“e-Tuğra” zaman damgası sertifikası imza oluşturma ve doğrulama verileri (anahtarlar) oluşturma işlemi, oluşturulan veriler için güvenliği ve gerekli şifreleme gücünü temin eden güvenilir sistemler kullanılarak, önceden seçilmiş birden fazla eğitimli “güvenli personel” tarafından yerine getirilir. “e-Tuğra” zaman damgası sertifikası için, imza oluşturma ve doğrulama verileri oluşturmada kullanılan şifreleme modülleri FIPS 140-1 Seviye 3 şartlarını karşılar. “e-Tuğra” zaman damgası sertifikası imza oluşturma ve doğrulama verileri “Tebliğ”de belirtilen algoritma ve parametrelere uygun olarak oluşturulur. Anahtar oluşturma işlemi sırasında yapılan faaliyetler kaydedilir, tarih atılarak imzalanır. Bu kayıtlar denetim ve izleme amacıyla saklanır. “e-Tuğra” zaman damgası sertifikasıyla ilişkili İmza oluşturma verisi “ESHS”ye ait güvenli elektronik imza oluşturma aracında oluşturulur ve buradan yedekleme amacı dışında çıkarılamaz. İmza oluşturma verisinin güvenli olarak saklanması için gerekli fiziksel ve teknik güvenlik önlemleri alınır.

“e-Tuğra” zaman damgası sertifikası imza oluşturma ve doğrulama verileri Türkiye Cumhuriyeti sınırları içerisinde oluşturulur ve imza oluşturma verisi hiçbir şekilde bu sınırlar dışına çıkarılamaz. “e-Tuğra” zaman damgası sertifikasıyla ilişkili imza oluşturma ve doğrulama verilerinin geçerlilik süresi 10 yılı aşamaz.

7.2.2. Zaman Damgası Ünitesi Özel Anahtar Koruması

7.2.2.1 Şifreleme Modülü Standartları ve Kontrolleri

“e-Tuğra” zaman damgası sertifikasıyla ilişkili imza oluşturma ve doğrulama verilerini oluşturma ve imza oluşturma verisi saklama işlemleri için EAL4+ seviyede güvenlik düzeyini karşılayan donanım şifreleme modülleri kullanılır.

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

“e-Tuğra” zaman damgası sertifikasıyla ilişkili imza oluşturma ve doğrulama verilerine erişim, ancak birden çok yetkili “güvenli personel”in gerekli güvenlik ve tanımlama süreçlerini yerine getirmesi halinde gerçekleşmektedir.

7.2.2.3 İmza Oluşturma Verisinin Saklanması

“e-Tuğra” zaman damgası sertifikasıyla ilişkili imza oluşturma verisi, resmi makamların erişimi amacıyla dahi olsa herhangi bir üçüncü şahsa verilemez.

7.2.2.4 İmza Oluşturma Verisi Yedekleme

“e-Tuğra”, rutin ve felaketten kurtarma amaçlarıyla zaman damgası sertifikası imza oluşturma verilerinin yedek kopyalarını oluşturur. Bu veriler, donanım şifreleme modüllerinde ve ilgili anahtar saklama cihazlarında gerekli teknik ve fiziksel güvenlik önlemleri alınarak şifrelenmiş formda saklanır.

7.2.2.5 İmza Oluşturma Verisi Arşivleme

“e-Tuğra” zaman damgası sertifikasına ait imza oluşturma verileri arşivlenmez. İmza doğrulama verileri ve kök sertifikalar ise ileride çıkması muhtemel uyuşmazlıklarda kullanılmak üzere 20 yıl süreyle saklanır.

7.2.2.6 İmza Oluşturma Verisinin Aktif Hale Getirilmesinin Metodu

“e-Tuğra” zaman damgası sertifikası imza oluşturma verilerinin aktivasyonu gerekli teknik ve fiziksel güvenlik önlemleri altında sadece birden çok yetkili “güvenli personel” tarafından gerçekleştirilebilir.

7.2.2.7 İmza Oluşturma Verisinin Aktif Durumdan Çıkarılmasının Metodu

“e-Tuğra” zaman damgası sertifikası imza oluşturma verileri sadece kullanım sırasında aktif halde tutulur. Kullanım tamamlandıktan sonra aktif durumdan çıkarılır. “ESHS”ye ait güvenli elektronik imza oluşturma aracı okuyucudan çıkartıldığında, imza oluşturma verisi aktif durumdan çıkar.

7.2.3. Zaman Damgası Ünitesi Açık Anahtar Dağıtımı

“e-Tuğra” zaman damgası sertifikası http://www.e-tugra.com adresinde yayınlanmaktadır. Ayrıca “e-Tuğra” zaman damgası sertifikası ve bu sertifikaya bağlı imza doğrulama verisi, güvenli elektronik imza doğrulama aracında yüklü olarak gelebilir veya güvenli elektronik imza doğrulama aracı sahibi, güvenli elektronik imza doğrulama aracını kullanarak “e-Tuğra” zaman damgası sertifikası ve bu sertifikaya bağlı imza doğrulama verisini güvenli elektronik imza doğrulama aracına indirebilecektir.

7.2.4. Zaman Damgası Ünitesi Anahtarının Yeniden Anahtarlanması

“e-Tuğra” zaman damgası sertifikası 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-Tuğra” zaman damgası sertifikası 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-Tuğra”, zaman damgası sertifikası imza oluşturma ve doğrulama verilerini, “ESHS”ye ait güvenli elektronik imza oluşturma aracında (kriptografik modül) oluşturur. Zaman damgası sertifikası imza oluşturma verisi yedekleme amacı dışında kesinlikle “ESHS”ye ait olan güvenli elektronik imza oluşturma aracından çıkarılamaz. Yedekleme amacıyla imza oluşturma verisinin başka bir kriptografik modüle transferi gerekli teknik ve fiziksel güvenlik önlemleri altında sadece birden çok yetkili “güvenli personel” tarafından gerçekleştirilebilir.

7.3. Zaman Damgası Hizmeti

7.3.1. Zaman Damgası

“e-Tuğra” zaman damgası sağlayıcı, zaman damgası yayınlanması için gerekli güvenlik kriterlerini yerine getirir. “e-Tuğra” zaman damgası sağlayıcı tarafından yayınlanan zaman damgaları eşsiz tanımlayıcılar ve “e-Tuğra” “ZDİ”ye ilişkin tanımlayıcı içerirler. “e-Tuğra” zaman damgası sağlayıcı tarafından yayınlanan zaman damgaları gerçek UTC zaman damgası değerine kadar geriye doğru izlenebilecek tarih ve zaman değeri içermektedir; zaman damgalarında kullanılan saat değeri GPS uydu alıcısı ile sunulmaktadır. “e-Tuğra” zaman damgası sağlayıcı, uydu alıcısının arızalanması durumunda ikincil saate başvurur. “e-Tuğra” zaman damgası sağlayıcı tarafından yayınlanan zaman damgaları sadece zaman damgası sertifikası imza oluşturma verisi ile imzalanır. “e-Tuğra” zaman damgası sağlayıcı tarafından yayınlanan zaman damgaları “e-Tuğra”ya ve “e-Tuğra” zaman damgası sağlayıcıya ilişkin tanımlayıcılar içerirler.

Zaman damgası kullanıcıya aşağıdaki şekilde verilir;

Kullanıcı RFC 3161 uyumlu bir zaman damgası istemcisi ile http://tsa.e-tugra.com/signserver/tsa adresine veya internetten www.e-tugra.com adresindeki web ara yüzünden zaman damgası almak için başvurur. Bu başvuru zaman damgalanacak belgenin özet bilgisi zaman damgası sunucusuna iletilerek yapılır.

Zaman damgası sunucusu kendisine gelen özet bilgisine istinaden bir zaman damgası "token"ı üretir ve bunu istemciye gönderir. "Token" bilgisi veri tabanında saklanır.

7.3.2. UTC ile Saat Senkronizasyonu

"e-Tuğra" zaman damgası sağlayıcı tarafından yayınlanan zaman damgaları gerçek UTC zaman damgası değerine kadar geriye doğru izlenebilecek tarih ve zaman değeri içermektedir; zaman damgalarında kullanılan saat değeri GPS uydu alıcısı ile sunulmaktadır. Zaman damgası içine yerleştirilen UTC zamanı ±100 ms doğruluk oranı sunar. "e-Tuğra" zaman damgası sağlayıcının işleyişinde ve sağlayıcıya erişimde "ZDUE" 7.4 altında belirtilen güvenlik kontrolleri kullanılır. Bu güvenlik kontrolleri sayesinde saatin kalibrasyonunun bozulması ya da saatin fiziksel zarar görmesi engellenmiş olur. Zaman sunucusunun, uyduyla ve diğer kaynaklarla senkronizasyonunu kaybettiği durumlarda 14 gün süreyle dahili saatinden hassasiyetini koruma özelliği bulunmaktadır.

7.4. "ESHS" Zaman Damgası Sağlayıcı Yönetimi ve Operasyonları

7.4.1. Güvenlik Yönetimi

7.4.1.1 Güvenli Roller

"e-Tuğra" zaman damgası sertifikası yaşam zinciri ve güvenli elektronik imza oluşturma aracı yönetim kontrolleri, anahtar yönetimi kontrolleri, "e-Tuğra" yönetim sistemleri ve veri bankaları kontrolleri, gerekli erişim ve kontrol yetkisine sahip "güvenli personel" tarafından yürütülür. "Güvenli personel" elektronik imza teknolojisi, bilgi güvenliği ve risk yönetimi konularında yeterli bilgi ve tecrübe seviyesine sahip kişilerden seçilir. "Güvenli personel" tanımları aşağıdaki şekildedir;

- Güvenlik Yöneticileri: Güvenlik sistemininin tüm politika ve prensiplerinin belirlenmesi, uygulanması, onaylanması görev, yetki ve sorumluluğuna sahip "güvenli personel"

- Sertifika Makamı (CA) Yöneticileri: Güvenlik uygulamalarının yönetimine ilişkin tüm sorumluluğa sahip "güvenli personel"

- Kayıt Makamı (RA) Yöneticileri: "NES"lerin oluşturulması, iptali, askıya alınması konularında onaylama görev ve yetkisine sahip "güvenli personel"

- Sistem Yöneticileri : "NES" başvuruları yönetimi, "NES" oluşturulması, güvenli elektronik imza oluşturma araçları yönetimi, sertifika iptal yönetimi için kullanılan "e-Tuğra" "ESHS" güvenli sistemlerini kurma, konfigüre etme ve bakımını yapma görev ve yetkisine sahip "güvenli personel"

- Sistem Operatörleri : "e-Tuğra" "ESHS" güvenli sistemlerini günlük bazda kullanma, sistem yedeklemesi ve kurtarma fonksiyonlarını kullanma görev ve yetkisine sahip "güvenli personel"

- Sistem Denetçileri : "e-Tuğra" "ESHS" güvenli sistemlerinin denetim kayıtlarına ve arşivlerine erişme ve devamlılığını sağlama görev ve yetkisine sahip "güvenli personel"

"Güvenli personel" "ZDİ" 7.4.3'deki kriterleri yerine getiren kimseler arasından ve güvenlik açısından tam yetkili bir yönetici tarafından seçilir ve görevlendirilir.

7.4.1.2 Her Bir Görev için Gereken Kişi Sayısı

"e-Tuğra" kritik operasyonel süreçleri genel olarak birden fazla "güvenli personel"in katılımıyla gerçekleştirilmektedir. Kritik operasyonel süreçler, kriptografik araç kullanımı gerektiren yüksek güvenlik gereksinimli uygulamalardır.

“e-Tuğra” zaman damgası sertifikasına ilişkin oluşturma, yenileme ve iptal işlemleri, en az ikisi yönetici seviyesinde “güvenli personel” olmak üzere, gerekli nitelik ve yetkilere sahip birden çok kişinin katılımıyla gerçekleştirilir.

7.4.1.3 Her Bir Görev için Tanımlama ve Kimlik Kontrolü

“Güvenli personel” olarak seçilen kimseler gerekli kimlik ve biyolojik bilgileri alınarak kendilerine atanan yetkiler doğrultusunda güvenlik sistemine kaydedilir. Kritik operasyonel işlemler öncesinde, işlemle ilgili yetki kontrolü ve görevli tanımlaması yapılır; yetki kontrolü ve tanımlamanın başarılı olması halinde işleme izin verilir ve işlem kayıt altına alınır.

7.4.1.4 Sorumlukların Ayrılmasını Gerektiren Roller

“ESHS” kök sertifikaları ve zaman damgası sertifikası anahtar yönetimi işlemleri ve bunlara ilişkin kontroller birden çok “güvenli personel”in katılımıyla ve sorumlulukların ayrıştırılması prensibiyle gerçekleştirilir. Sorumlulukların ayrıştırılması prensibi ile bir işlemin tümünün veya büyük bir kısmının tek bir kişi tarafından yapılması engellenmiştir.

7.4.2. Risk Değerlendirmesi

Bkz. “ZDİ” 7.4.4.1

7.4.3. Personel Güvenliği

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

“e-Tuğra” istihdam politikası, “e-Tuğra” “ESHS“ gereksinimleri göz özünde bulundurularak oluşturulmuştur. İstihdam politikası “genel personel istihdamı” ve “güvenli personel istihdamı” olarak ikiye ayrılmaktadır. “e-Tuğra” genel personeli, “Güven Merkezi” operasyonlarında görev almayan, pazarlama, organizasyon yönetimi ve belirli idari işler gibi bir takım ticari operasyonları yerine getirmek amacıyla seçilmiş personelden oluşur.

“e-Tuğra” genel personel işe alımı, üst düzeyde bir yönetici tarafından personel adayının gerekli niteliklere sahip olduğuna ve sır saklama yükümlülüğünü taşıyabileceğine kanaat getirildikten sonra gerçekleştirilir.

“Güvenli personel” işe alımı ise personel adayının, görev sorumluluklarını gerektiği gibi ve tatmin edici şekilde yerine getirmesi için gereken mesleki bilgi, nitelik ve deneyimini kanıtlayan belgeleri sunmasından ve personel adayının üst düzeyde bir yönetici tarafından, konuyla ilgili yeterliliğine kanaat getirilmesinden sonra gerçekleştirilir. “Güvenli personel” için mesleki bilgi kontrolleri en az 5 yılda bir tekrarlanır.

“e-Tuğra”’nin, 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.

7.4.3.2 Mesleki Bilgi Kontrol Prosedürleri

“e-Tuğra” genel personeli ve “güvenli personel”i hakkında işe alımdan önce, referansların değerlendirilmesi, önceki işin kontrolü, eğitim bilgilerinin ve niteliklerinin doğrulanması, adli sicil kontrolünü de içeren bir dizi güvenlik ve tanımlama kontrolleri yapılır.

7.4.3.3 Eğitim Şartları

“e-Tuğra” personeli göreve başlamadan önce “ESHS” hizmetleri, sertifika yaşam zinciri hizmetleri, mesleki sorumluluklar, temel açık anahtar alt yapısı süreçleri, “e-Tuğra” güvenlik süreçleri ve sertifika politikaları konularında gerekli hukuki ve teknik eğitimden geçirilirler. “e-Tuğra” eğitim programları periyodik olarak gözden geçirilir ve gerekli görüldüğünde güncellenir.

7.4.3.4 Eğitim Sıklığı ve Şartları

“e-Tuğra” personeline belirli aralıklarla ve güncellenmiş içeriklerle eğitim verilir. Kurum içerisinde yapılan performans analizleri doğrultusunda eğitim sıklığı ve içeriği değiştirilebilir. “e-Tuğra” operasyonlarında veya kullanılan yazılım ve donanımlarda değişiklik veya güncelleme olduğunda ve gerekli görüldüğü takdirde eğitimler düzenlenebilir.

7.4.3.5 Yetkisiz Eylemlere Karşı Yaptırımlar

“e-Tuğra” güvenlik ve işleyiş politikalarının personel tarafından ihlali halinde “e-Tuğra” tarafından personel hakkında gerekli disiplin önlemleri alınır ve personel ile yapılan gizlilik sözleşmelerindeki cezai şartlar yürürlüğe konulur. Söz konusu ihlaller sebebiyle “e-Tuğra” veya hizmet sağladığı kimseler herhangi bir şekilde zarar görürse, “e-Tuğra” sorumlu personele zararı tazmin ettirebilir.

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-Tuğra”, “ESHS” faaliyetlerini yürütmek için bağımsız yükleniciler ile hizmet sözleşmeleri akdedebilir. Hizmet sözleşmeleri “e-Tuğra”nin güvenlik ve işleyiş süreçlerine uyumlu olacak şekilde düzenlenir.

7.4.3.7 Personele Verilen Dokümanlar

“e-Tuğra” tüm personeline “SUE”, “Sİ”, “ZDUE”, “ZDİ” belgelerini ve görevleriyle ilgili özel nitelikli yazılım ve donanım kullanım kılavuzlarını verir.

7.4.4. Fiziksel ve Çevresel Güvenlik

7.4.4.1 Güven Merkezi” Konumu ve İnşası

“e-Tuğra”, “NES” yaşam zinciri operasyonları, anahtar yönetimi ve zaman damgası hizmetleri de dahil olmak üzere temel “ESHS” operasyonlarının tümünü gizli veya

açık müdahaleleri durduracak, önleyecek ve tespit edecek şekilde tasarlanmış, fiziksel olarak korunan bir “Güven Merkezi” içinde yürütür.

7.4.4.2 Fiziksel Erişim

“e-Tuğra” “Güven Merkezi”ne fiziksel erişim, birden çok güvenlik seviyesiyle korunan güvenlik sisteminden geçilmesiyle mümkündür. Güvenlik sistemi seviyeleri “dış alana erişim” ve “’Güven Merkezi’ne erişim” olarak ikiye ayrılmaktadır; “’Güven Merkezi’ne erişim”in sağlanması dış alana erişimin tamamlanmasıyla mümkün olmaktadır.

Dış alana erişim seviyelerinde, güvenlik görevlileri, kimlik kontrolü, ve ziyaretçi kayıtları gibi güvenlik yöntemleri kullanılır. Sertifika yaşam zinciri hizmetleri ve anahtar yönetimi operasyonlarının yapıldığı “Güven Merkezi”ne erişim ise çok daha güvenli yöntemlerin kullanılmasıyla gerçekleştirilir. “Güven Merkezi”ne erişim sadece “güvenli personel”in erişebildiği biometrik tanımlama yöntemi ile gerçekleştirilmekte, ayrıca tüm giriş ve çıkışlar kayıt altına alınmaktadır. “Güven Merkezi” devamlı olarak kameralar aracılığıyla izlenmekte ve kamera kayıtları saklanmaktadır.

7.4.4.3 Elektrik ve Klima Koşulları

“Güven Merkezi” ve “e-Tuğra”nın temel “ESHS” operasyonlarında kullanılan donanımlar, 7/24 operasyonlarına devam edebilmeleri için kesintisiz güç kaynakları ile, sıcaklığı ve nispi nemi kontrol etmek için ise ısıtma/havalandırma/klima sistemleri ile donatılmıştır.

7.4.4.4 Suya Karşı Korunma

“e-Tuğra” “Güven Merkezi” su baskınları ve sele karşı binanın üst katında inşaa edilmiş ve gerekli yalıtım sistemleri ile takviye edilmiştir. Herhangi bir su baskını durumunda zeminde bulunan 1 mm su seviyesine hassas su dedektörleri sistemin alarma geçmesini sağlar.

7.4.4.5 Yangın Önlemleri ve Korunması

“e-Tuğra”, yangınları veya hasara yol açan diğer alev veya duman vakalarını önlemek ve söndürmek için gerekli tüm makul önlemleri almıştır. “Güven Merkezi”

yangın alarmları ile takviye edilmiştir, ayrıca tüm binada yangın söndürme cihazları bulunmaktadır ve tüm personel yangın söndürme konusunda eğitim almıştır.

7.4.4.6 Veri Araçları Saklanması

Üretimde kullanılan yazılım ve veriler ile denetim, arşiv veya yedekleme bilgilerini içeren bütün araçlar “Güven Merkezi”nde 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”nin dışında depolama tesislerinde muhafaza edilir.

7.4.4.7 Atık Kontrolü

Sertifika yaşam zinciri hizmetlerinde ve “e-Tuğra”nın diğer “ESHS” operasyonlarında kullanılan ve geçerliliğini ve/veya gerekliliğini yitiren tüm dokümanlar, ilgili süreçler doğrultusunda imha edilir. “e-Tuğra”nın kendisine ait güvenli elektronik imzalama araçları ve ilgili diğer kriptografik donanım fiziksel olarak imha edilir veya üretici firmanın talimatları doğrultusunda sıfırlanır, diğer tüm atıklar ise normal süreçlerle bina dışına çıkarılır.

7.4.4.8 Harici Alan Yedeklemesi

“e-Tuğra” olası teknik arızalara ve/veya afetlere karşı, sertifika yönetim süreçleri iş sürekliliğini sağlamak amacıyla “İş Sürekliliği ve Felaketten Kurtarma Planı” doğrultusunda “Güven Merkezi” içinde ve dışında rutin olarak elektronik kayıtların yedeklerini alır ve saklar.

7.4.5. Operasyon Yönetimi

“e-Tuğra” 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-Tuğra” “ESHS” işleyişi içerisinde yürütülen operasyonlarda tüm iş ve işlemler bilgi güvenliği gereksinimleri doğrultusunda gerçekleştirilmektedir. “e-Tuğra” bilgi güvenliği gereksinimleri, güvenli ve lisanslı yazılım ve donanımların kullanılması, ağ içerisinde

saldırı tespit sistemlerinin bulunması, bilgi ve zilyetlik bazlı tanımlama yöntemleri ile erişim ve işlem kontrolü, “güvenli personel” arasında münhasır yetki ve görev dağılımı, gerekli tüm işlemlerin ve kayıtların yedeklenmesi ve saklanması yöntemleri ile sağlanır.

Güvenli personel, sisteme erişimde aktivasyon verilerini kullanır. Aktivasyon verileri “e-Tuğra” tarafından yaratılır ve “güvenli personel”e kapalı zarf içerisinde imza karşılığında teslim edilir. Aktivasyon verileri sahipleri kendi kontrolleri ile istedikleri zaman aktivasyon verilerinde değişiklik yapabilirler.

7.4.7. Güvenilir Ortam

Bkz. “ZDİ” 7.4.4.1

7.4.8. “ESHS” Zaman Damgası İmza Oluşturma Verisinin Açığa Çıkması

“e-Tuğra” zaman damgası sertifikasına ait imza oluşturma verilerinin gizliliğinin ve güvenilirliğinin şüphe altında olması halinde “e-Tuğra” zaman damgası sertifikası iptal edilir. “e-Tuğra” zaman damgası sertifikasının iptal edilmesi durumu “e-Tuğra” web sitesinden (www.e-tugra.com) kamuoyuna ve ilgililere duyurulur.

7.4.9. “ESHS” Zaman Damgası Hizmet Sağlayıcısı İptali

“e-Tuğra” “ESHS” faaliyetlerini durdurması gerektiği durumlarda, “ESHS” operasyonları durdurulmadan önce “NES” sahipleri, üçüncü kişileri ve diğer ilgili kuruluşları bundan haberdar etmek için ticari açıdan gerekli her türlü çabayı gösterir.

“ESHS”nin faaliyetlerine kendisi veya Telekomünikasyon Kurumu tarafından son verilmesi halinde ortaya çıkacak olan durum, “ESHS”nin yükümlülük ve sorumlukları ile birlikte “Yönetmelik”in 29 ve 30. maddelerinde açıklanmaktadır.

7.4.10. Yasal Gerekliliklere Uyumluluk

Bu doküman “Tebliğ”de belirtildiği üzere ETSI TS 102 023 uyumlu olacak şekilde hazırlanmıştır. Dokümanın hazırlanmasında “e-Tuğra” “ZDİ”, “e-Tuğra” “SUE”, RFC

3161, RFC 3628 dokümanları referans alınmıştır. “e-Tuğra” zaman damgası hizmetlerinin yürütümünde CWA 14167-1, ETSI TS 101 456 ve ETSI TS 101 861 standartlarına uyar.

7.4.11. ESHS Zaman Damgası Sağlayıcı Faaliyet Günlüğü

“e-Tuğra” zaman damgası hizmetleri sistemi zaman damgalarının yayınlanmasıyla ilgili her türlü olayı kayıt altına alır.

7.5. Organizasyonel Plan

“e-Tuğra”, zaman damgası hizmetlerini “ESHS” yetkisi ve görevi altında yürütür.