e-imzaTR

ZAMAN DAMGASI UYGULAMA ESASLARI

E-İMZA BİLGİ GÜVENLİĞİ HİZMETLERİ A.Ş.
PROF.DR.AHMET TANER KIŞLALI MAH.
2778.SOK. NO:3 ÇAYYOLU/ANKARA
TÜRKİYE

Tel : 90 312 242 0 111
Fax: 90 312 242 0 042

www.e-imzatr.com
bilgi@e-imzatr.com

İçindekiler

1 Önsöz

E-İMZA Bilgi Güvenliği Hizmetleri A.Ş (kısaca "e-imzaTR" olarak anılcaktır), 23 Ocak 2004 tarih ve 25355 sayılı Resmi Gazete'de yayımlanmış ve 23 Temmuz 2004 tarihinde yürürlüğe girmiş olan 15 Ocak 2004 tarihli ve 5070 sayılı "Elektronik İmza Kanunu (kısaca "Kanun" olarak anılacaktır)" ve Bilgi Teknolojileri ve İletişim Kurumu tarafından yayımlanmış olan ikincil mevzuat uyarınca, elektronik sertifika hizmet sağlayıcılığı alanında faaliyet göstermektedir.

Zaman Damgası Uygulama Esasları (Kısaca "ZDUE") olarak isimlendirilen bu doküman 5070 sayılı Elektronik İmza Kanunu , Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik (Kısaca "Yönetmelik" olarak anılacaktır) ile Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ (Kısaca "Tebliğ" olarak anılacaktır) uyarınca "e-imzaTR"nin "ESHS" sıfatıyla yürüttüğü faaliyetler sırasında yerine getirdiği teknik ve hukuki gereklilikleri, "ESHS"nin faaliyetlerini, teknik ve organizasyonel altyapısını, "ESHS"nin sunduğu hizmetlere ilişkin süreçlerde belirli roller üstlenen tarafların sorumluluklarını açıklamak ve kamuoyuna duyurmak üzere hazırlanmıştır. "ZDUE" belgesi, hangi elektronik sertifika hizmetlerinin "e-imzaTR" tarafından sunulduğunu belirlerken, "ZDUE" bu hizmetlerin "e-imzaTR" tarafından nasıl gerçekleştirildiğini tanımlar.

Bu doküman "Tebliğ"de belirtilen ETSI TS 101 456, CWA 14167-1, IETF RFC 3647 standartlarına uygun olarak hazırlanmıştır.

1.1 Genel Bakış

5070 sayılı Elektronik İmza Kanunu'nun 5. maddesine göre güvenli elektronik imza, elle atılan imza ile aynı hukuki sonucu doğurur. "Kanun"un 4. maddesine göre güvenli elektronik imza; sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulabilir ve yalnızca nitelikli elektronik sertifika (Kısaca "NES")'ya dayanarak imza sahibinin kimliği tespit edilebilir. Güvenli elektronik imza oluşturma sürecindeki gerekli bileşenlerden biri olan "NES", yalnızca 5070 Sayılı Elektronik İmza Kanunu ve ilgili mevzuat hükümlerinde tanımlanmış olan "Elektronik Sertifika Hizmet Sağlayıcı"lar tarafından oluşturulabilir. Elektronik Sertifika Hizmet Sağlayıcı'lar "Kanun"un 8. Maddesi hükmü

uyarınca Bilgi Teknolojileri ve İletişim Kurumu'na bildirimde bulunarak; ilgili mevzuat hükümleri uyarınca bildirimde bulunduğu koşulları yerine getirdiği Bilgi Teknolojileri ve İletişim Kurumu'nca uygun görülerek faaaliyete geçebilirler. Elektronik Sertifika Hizmet Sağlayıcı'lar elektronik sertifika, zaman damgası ve elektronik imzayla ilgili hizmetleri sunan gerçek veya tüzel kişilerdir.

E-İMZA BİLGİ GÜVENLİĞİ HİZMETLERİ A.Ş "Kanun" ve ilgili mevzuattaki gereklilikleri yerine getirerek Bilgi Teknolojileri ve İletişim Kurumu'na usulü dairesinde bildirimde bulunmuş ve bildirimde belirttiği koşulları sağladığı "Bilgi Teknolojileri ve İletişim Kurumu tarafından uygun görülerek faaliyete geçmesi hususunda yetki verilmiş bir "Elektronik Sertifika Hizmet Sağlayıcısı"dır..

Bu döküman "e-imzaTR" Nitelikli Elektronik Sertifika İlkeleri'ni açıklamaktadır.

1.1.1 ZDİ ve ZDUE

"ZDİ" belgesi, hangi ZAMAN DAMGASI hizmetlerinin "e-imzaTR" tarafından sunulduğunu belirlerken,.

"ZDUE" bu hizmetlerin "e-imzaTR" tarafından nasıl gerçekleştirildiğini tanımlar.

1.1.2 Kapsam

Bu belge, "ESHS" tarafından yürütülen uygulamaların ve prosedürlerin sınırlarını belirtir.

1.2 Döküman Adı ve Tanımlamalar

Döküman Adı: e-imzaTR Zaman Damgası Uygulama Esasları v.1.0
Döküman versiyonu : versiyon 1.0
Hazırlanma tarihi: 20- Ekim, 2013
Nesne belirteci: 2.16.792.3.0.10.20.2.1

1.3 Kısaltmalar

"BTK"	Bilgi Teknolojileri ve İletişim Kurumu
"CEN"	Comité Européen de Normalisation - Avrupa Standardizasyon Komitesi
"CRL"	Certificate Revocation List (Bkn "SİL")
"CSR"	Certificate Signing Request – Sertifika İmzalama Talebi
"CWA"	CEN Workshop Agreement- CEN Çalıştay Kararı
"ÇSDP"	Çevrimiçi Sertifika Durum Protokolü (OCSP - Online Certificate Status Protokol)
"DN"	Distinguished Name – Ayırt Edici İsim
"DNS"	Domain Name System – Alan Adı Sistemi
"EAL"	Evaluation Assurance Level - Değerlendirme Garanti Düzeyi
"ESHS"	Elektronik Sertifika Hizmet Sağlayıcı

"ETSI TS"	ETSI Technical Specifications - ETSI Teknik Özellikleri
"ETSI"	European Telecommunication Standartization Institute - Avrupa Telekomünikasyon Standartları Enstitüsü
“e-imzaTR”	E-İMZA Bilgi Güvenliği Hizmetleri A.Ş
"FKM"	Felaket Kurtarma Merkezi
"IETF RFC"	Internet Engineering Task Force Request for Comments - İnternet Mühendisliği Görev Grubu Yorum Talebi
"IETF"	Internet Engineering Task Force - İnternet Mühendisliği Görev Grubu
"ISO/IEC"	International Organisation for Standardisation / International Electrotechnical Commitee - Uluslararası Standardizasyon Teşkilatı / Uluslararası Elektroteknik Komitesi.
"KB"	Kayıt Birimi
"NES"	Nitelikli Elektronik Sertifika
"OCSP"	Online Certificate Status Protokol (Bkn "ÇSDP")
"OID"	Object Identifier - Nesne betimleyicisi.
"PKI"	**"PKI"**Public-Key Infrastructure
"Sİ"	Sertifika İlkeleri
"SİL"	Sertifika İptal Listesi (CRL - Certificate Revocation List)
"SSL"	Secure Sockets Layer
"TC"	Türkiye Cumhuriyeti
"TCKN"	Türkiye Cumhuriyeti Kimlik Numarası
"TSE"	Türk Standartları Enstitüsü

1.4 Tanımlamalar

"Aktivasyon"	"NES"sahipleri için, İmza oluşturma verisi erişim şifresinin, kendisi tarafından belirlenmesine imkân sağlayan interaktif güvenli yöntem.
"Açık Anahtar Altyapısı" ("AAA")	Matematiksel bağlantısı bulunan kriptografik anahtar çiftlerine dayalı ve sertifika tabanlı bir kriptografik sistemin kurulması ve işletilmesini sağlayan mimari yapı, teknikler, uygulamalar ve düzenlemeler bütünü.
"Açık Anahtar"	“AAA” yapısında, Çift anahtarlı şifreleme algoritmasında üçüncü kişilere de açık olan kriptografik anahtar.("Kanun"da imza doğrulama verisi olarak isimlendirilmiştir.)
"Alt Kök Sertifikası"	"ESHS"nin "AAA"hiyerarşisi içerisinde "Güven Merkezi"tarafından oluşturulmuş, "ESHS"kök sertifikasının imzasını taşıyan ve son kullanıcı sertifikalarını imzalama amaçlı kullanılan

	sertifika.
"Anahtar"	İmza oluşturma veya imza doğrulama verilerinden herbiri.
"Arşiv"	"ESHS"nin saklamakla yükümlü olduğu her türlü bilgi, belge, evrak ve elektronik veri.
"Başvuru Yöntemleri"	"ESHS"ile Başvuru Sahibi"arasında başvurunun yapılması, sertifika sahibinin kimliğinin tespiti, gerekli evrakların hazırlanması, sertifika ücretlerinin ödenmesi, evrakların saklanması, 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 www.e-imzatr.comadresinden ulaşılabilir.
"Çevrim İçi Sertifika Durum Protokolü"("ÇSDP")	Sertifikaların geçerlilik durumunun üçüncü kişilere duyurulması için sertifika durum bilgisinin çevrim içi olarak kesintisiz alınmasını sağlayan standart protokol.
"Dizin"	Geçerli sertifikaları yayınlamak amacıyla içinde bulunduran elektronik depo.
"Elektronik İmza Kanunu"	23 Ocak 2004 tarih 25355 sayılı Resmi Gazete'de yayımlanan 5070 Sayılı Kanun.
"Elektronik İmza"	Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri.
"Elektronik Sertifika Hizmet Sağlayıcısı"	Elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişiler.
"Elektronik Veri"	Elektronik, optik veya benzeri yollarla elektronik ortamda üretilen, taşınan veya saklanan kayıtlar.
"Erişim Şifresi"	Güvenli elektronik imza oluşturma araçlarına erişim için kullanılan parola.
"Gizli Anahtar"	"AAA"yapısında, Çift anahtarlı şifreleme algoritmasında sadece anahtar sahibinin uktesinde olan kriptografik anahtar.(Kanun'da imza oluşturma verisi olarak isimlendirilmiştir.)
"Güven Merkezi"	"ESHS"yapısında yer alan, Kayıt Birim'lerinden gelen sertifika talepler doğrultusunda başvuru onay ve sertifika üretimi yapan, sertifika iptal işlemlerini gerçekleştirilen, sertifika kayıtları ile sertifika iptal durum kayıtlarını yaratan, işleten ve yayımlayan birim.
"Güvenli Elektronik İmza Doğrulama Aracı"	Kanunun 7 nci maddesinde sayılan niteliklere sahip: 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 araçları.
"Güvenli Elektronik İmza Oluşturma Aracı"	Kanunun 6 ncı maddesinde sayılan niteliklere sahip: a) Ürettiği elektronik imza oluşturma verilerinin kendi aralarında bir eşi daha bulunmamasını, b) Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin araç dışına hiçbir biçimde çıkarılamamasını ve gizliliğini, c) Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin, üçüncü kişilerce elde edilememesini, kullanılamamasını ve elektronik imzanın sahteciliğe karşı korunmasını, d) İmzalanacak verinin imza sahibi dışında değiştirilememesini ve bu verinin imza sahibi tarafından imzanın oluşturulmasından önce görülebilmesini sağlayan ve ISO/IEC 15408 (-1,-2,-3)'e göre en az EAL4+ seviyesinde olan araçlar.
"Güvenli Elektronik İmza"	Güvenli elektronik imza; a) Münhasıran imza sahibine bağlı olan, b) Sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan, c) Nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan, d) İmzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan, e) Kanunun 4 üncü maddesinde sayılan niteliklere sahip, Kanunun hariç tuttuğu işlemler dışında elle atılan imzayla aynı hukuki sonucu doğuran elektronik imzadır.
"İmza Doğrulama Aracı"	Elektronik imzayı doğrulamak amacıyla imza doğrulama verisini kullanan yazılım veya donanım aracı.
"İmza Doğrulama Verisi"	Elektronik imzayı doğrulamak için kullanılan şifreler, kriptografik açık anahtarlar gibi veriler.
"İmza Oluşturma Aracı"	Elektronik imza oluşturmak üzere, imza oluşturma verisini kullanan yazılım veya donanım aracı.
"İmza Oluşturma Verisi"	İmza sahibine ait, imza sahibi tarafından elektronik imza oluşturma amacıyla kullanılan ve eşi daha olmayan şifreler, kriptografik gizli anahtarlar gibi veriler.

"İmza Sahibi"	Elektronik imza oluşturmak amacıyla bir imza oluşturma aracını kullanan "NES"sahibi gerçek kişi.
"İptal Durum Kaydı"	Geçerlilik süresi dolmamış sertifikaların iptal bilgisinin yer aldığı, iptal zamanının tam olarak tespit edilmesine imkan veren ve üçüncü kişilerin hızlı ve güvenli bir biçimde ulaşabileceği kayıt.
"Kanun"	15 Ocak 2004 tarihli ve 5070 sayılı Elektronik İmza Kanunu.
"Kayıt Birimi"	"e-imzaTR"ye bağlı olarak faaliyette bulunan, Sertifika Sahipleri ile "Kurumsal Başvuru Sahipleri"nin sertifika başvurularını alan, ilgili kimlik tanımlama ve doğrulama süreçlerini yürüten, sertifika taleplerini onaylayarak "Güven Merkezi"ne yönelten, "ESHS" faaliyetleri kapsamında müşteri ilişkilerini yöneten alt birimlere sahip "e-imzaTR"nin yetkili birimleri ve onların personelleri.
"Kimlik Bilgileri"	"Sertifika Kullanıcısı"nın Adı-Soyadı, Türkiye Cumhuriyeti Kimlik Numarası veya Pasaport Numarası, doğum yeri, doğum tarihi ve uyruğu.
"Kök Sertifika"	"ESHS"kurumsal kimlik bilgilerini "ESHS"imza doğrulama verisine bağlayan, "Güven Merkezi" tarafından üretilen ve kendi imzasını taşıyan, "ESHS"nin ürettiği diğer tüm sertifikaların doğrulanabilmesi için "ESHS"tarafından yayımlanan sertifika.
"Kurum"	Bilgi Teknolojileri ve İletişim Kurumu.
"Kurumsal Başvuru Sahibi"	"ESHS"ile Kurumsal Başvuru Sözleşmesi akdetmiş olan ve bu sözleşme hükümleri ve "Yönetmeliğin"3. ve 9. maddeleri uyarınca çalışanları veya müşterileri veya üyeleri veya hissedarları adına nitelikli elektronik sertifika başvurusunda bulunan tüzel kişilik .
"Kurumsal Başvuru Yetkilisi"	"Sertifika Kullanıcısı"adına "NES"düzenlenmesi için "ESHS"ye bildirilecek olan bilgileri "Yönetmeliğin"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.
"Kurumsal Başvuru"	Bir tüzel kişiliğin çalışanları veya müşterileri veya üyeleri veya hissedarları adına yaptığı nitelikli elektronik sertifika başvurusu.
"Mali Sorumluluk Sigortası"	"ESHS"nin, "Kanun"dan veya uygulamalardan doğan yükümlülüklerini yerine getirmemesi sonucu doğacak zararların karşılanması amacıyla yaptırmakla yükümlü olduğu sigorta.
"Nitelikli Elektronik Sertifika"("NES")	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.
"Özetleme Algoritması"	İmzalanacak elektronik verilerin sabit uzunlukta bir özetinin çıkarılmasında kullanılan algoritma.
"Özne"	Sertifikanın CN alanında yer alan kişi veya sunucu adı.
"Sertifika İlkeleri"	Sertifikaların belli bir topluluk ve/veya genel güvenlik gereklilikleri olan uygulamalar bakımından kabul edilebilirliğini belirten kurallar bütününe ve ESHS'nin işleyişi ile ilgili genel kuralları içeren belgeye "Sertifika İlkeleri"denir. "Sertifika İlkeleri", Elektronik Sertifika Hizmet Sağlayıcıları tarafından umuma açıklanan yönelik bir belgedir. "ESHS"tarafından yayınlanan "Sİ"ye, "Sertifika Kullanıcı"ları uymak zorundadır. "Sİ"ye, duruma göre zaman zaman yapılabilecek değişiklikler de dahil olmak üzere, güncel ve önceki sürümlerine "ESHS"nin web sitesinden erişilebilir.
"Sertifika İmzalama Talebi" ("CSR")	Talep sahibi tarafından üretilen ve sahip olduğu gizli anahtarla imzaladığı sertifika talebi.
"Sertifika İptal Listesi"	İptal edilmiş sertifikaların üçüçü kişilere duyurulması amacıyla "ESHS"tarafından yayımlanan elektronik dosya.
"Sertifika Kullanıcısı"- "Sertifika Sahibi"	Adına "ESHS"tarafından sertifika düzenlenen gerçek veya tüzel kişilik. Bu doküman içerisinde geçen "Sertifika Sahibi"kavram "Sertifika Kullanıcısı"ile eş anlamlı olarak kullanılmaktadır.
"Sertifika Uygulama Esasları"	"Sertifika Sahipleri"başta olmak üzere "Sİ"içerisinde tanımlanan herbir 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. "SUE"ye, duruma göre zaman zaman yapılabilecek değişiklikler de dahil olmak üzere, "ESHS"nin web sitesinden erişilebilir.
"Tebliğ"	6 Ocak 2005 tarih 25692 sayılı Resmi Gazete'de Bilgi Teknolojileri ve İletişim Kurumu tarafından yayımlanan "Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ"
"Yönetmelik"	6 Ocak 2005 tarih 25692 sayılı Resmi Gazete'de Bilgi Teknolojileri ve İletişim Kurumu tarafından yayımlanan "Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında

	Yönetmelik".
"Zaman Damgası"	Elektronik verinin; üretildiği, değiştirildiği, gönderildiği, alındığı ve/veya kaydedildiği zamanın tespit edilmesi amacıyla, elektronik sertifika hizmet sağlayıcısı tarafından elektronik imzayla doğrulanan kayıt.
"ZDİ"	Zaman Damgası İlkeleri
"ZDUE"	Zaman Damgası Uygulama Esasları

1.4.1 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.
.

1.4.2 "ESHS" (Zaman Damgası Hizmet Sağlayıcısı)

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

1.5 Kullanıcılar

1.5.1 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.

1.5.2 Üçüncü Kişiler

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

2 Veri Deoplama ve Yayınlama Sorumlulukları

2.1 Veri Depoları

“e-imzaTR” Veri depoları “SİL”, “ÇİSDUP” ve ilgili tüm dökümanlar 7/24 ulaşılabilecek şekilde erişime açık bulundurulur

2.2 Yayınlama Sıklığı ve Periyodu

Bu "ZDİ" de yapılacak major değişiklikler 3 gün içerisinde halka açık şekilde yayınlanır.

2.2.1 Veri Depoları Erişim Kontrolü

Tüm Zaman DAmgası İlkeleri www.e-imzatr.com adresi üzerinden halka açık şekilde yayınlanır..

3 Genel Hükümler

3.1 Zaman Damgası Hizmetleri ve "ESHS" Sorumlulukları

- "ESHS" Zaman damgası hizmeti sunar.
- "ZDİ" ve ZDUE de belirtildği şekilde hizmet verilir.
- "ESHS" hizmetin güvenliğini sağlar
- Zaman bilgisini Uydu lardan alarak en doğru zamanı kullanıcılarına sunar,
- "ESHS" %99.9 ulaşılabilir bir hizmet sunar

3.2 Kullanıcı Yükümlülükleri

Tüm Kullanıcılar:

- "ZDİ" ve "ZDUE" de belirtilenler çerçevesinde Zaman Damgası kullanmalıdır.
- Zaman Damgası üzerindeki imzayı doğrulamalı" e-imzaTR" den geldiğini kontrol etmelidir.
- Zaman damgasının geçerliliğini kontrol etmelidir.

3.3 Üçüncü Tarafların Yükümlülükleri

Zaman damgalı bir veriye veya imzaya güvenerek işlem yapacak üçüncü kişiler :

- Zaman damgasının geçerliliğini kontrol etmekle,
- Zaman Damgası üzerindeki imzanın "e-imzaTR" ait olup olmadığını kontrol etmekle,
- Zaman Damgası sertifika geçerliliğini "SİL" ve "ÇİSDUP" servislerini kullanarak doğrulamakla, yükümlüdürler.

4 "ESHS" Hizmetlerinin Gereksinimleri

"ESHS" vermiş olduğu tüm zaman damgası hİzmetlerini RFC 3161 standardında belirtildiği şekilde gerçekleştirir:

- Kullanıcı ve üçüncü şahıslara güvenilir bir hizmet sunar
- "ZDİ" de belirtildiği şekilde hizmet sunar

- Zaman damgasına ait anahtar oluşturma ve doğrulama verileri FIPS 140-1 Seviye 3 standardında Kriptografik koruma modüllerinde saklanır.
- 5070 sayılı elektronik imza kanununda belirtildiği şekilde hizmet sunulur.

4.1 Nesne Belirteci

Oluşturulan tüm zaman damgaları "ZDİ" ye uygun olarak oluşturulur ve aşağıdaki Nesne Belirteci numarasını içerir.
"ZDİ" Nesne Belirteci (OID) : 2.16.792.3.0.10.20.1.1

"ZDUE" Nesne Belirteci (OID) : 2.16.792.3.0.10.20.2.1

4.2 Zaman Damgası

Zaman damgasının güvenli ve doğru zamanı içererek oluşturulması için gerekli tüm güvenlik kontrollerini yerine getirir. Zaman damgası aşağıda belirtilen bilgileri içerir:

- "e-imzaTR" ye ilişkin tanımlayıcı
- "ZDİ" ye ilişkin tanımlayıcı
- Tarih ve Zaman bilgisi
- Eşsiz bir seri numarası,
- Nesne belirteci
- "ESHS" tarafından imzalanmış zaman damgası verisi.

4.3 Zaman Damgası Anahtarları Yaşam Döngüsü ve Yönetimi

"ESHS" Zaman Damgası anahtar oluşturma işlemi önceden belirlenmiş birden fazla "Güvenilir Personel" tarafından "tebliğ" de belirtilen standartlar dahilinde gerçekleştirilir. Kullanım ömürlerini dolduran anahtarlar imha edilirler.

4.3 Zaman Senkronizasyonu

"e-imzaTR" zaman damgası sunucuları Zaman bilgisini Uydularda bulunan atomik saatlerin yaymış olduğu foton patlamalarından alır. Aynı anda en az 5 atomik saatten zaman bilgisi alarak en doğru zamanı tespit eder ve kullanıcı işlemlerinde kullanır. Uydu bağlantısını kaybetmesi halinde kendi içerisinden bulunan yüksek hassasiyetli kristal saatinden işmeleri devam ettirir.

5 Tesis Yönetimi ve Operasyonel Kontroller

5.1 Fiziksel Erişim

“e-imzaTR” “Güven Merkezi”ine giriş birden çok güvenlik kontrolüne tabi tutularak sağlanır. “Güven Merkezi”ine erişim için öncelikle yapıya erişim sağlanır. Yapıya erişim sağlandıktan sonra ikinci bir kontrolle “Güven Merkezi”ine erişim sağlanır. “Güven Merkezi” erişimleri biyometrik kontrolde dahil olmak üzere 3 ayrı parametreli giriş sistemi ile kontrol edilir. Güvenilir ekipmanların bulunduğu silindirik turnike aracığılı ile her seferde bir kişi girecek şekilde gerçekleştirilebilir. Acil durumlar haricinde tek kişi girişe izin verilmemektedir. Bölgeye girişler kayıt altına alınır ve 7/24 güvenlik kameraları ile izlenir.

5.1.1 Enerji ve İklimlendirme Koşulları

“e-imzaTR” “Güven Merkezi” %99.9 süreklilikle hizmet verecek şekilde tasarlanmıştır. Güvenli ekipmanların bulunduğu alanlar alçak/yüksek gerilime karşı özel ekipmanlarla korunmaktadır. Enerji kesintilerinde otomatik olarak devreye giren jeneratör sistemiyle enerji devamlılığı sağlanır. “Güven Merkezi” da bulunan ekipmanların iklim şartlarından etkilenmemesi için klima sistemiyle sürekli ısı ve nem kontrolü yapılarak uygun ısıda tutulur.

5.1.2 Su Baskını Koruması

Su baskınına maruz kalma bilgi işlem donanımlarında önemli hasara yol açabilir ve dolayısıyla “Güven Merkezi” tarafından sunulan hizmeti etkileyebilir. Su baskından kaynaklanabilecek hasarları önlemek için aşağıdaki önlemler alınmış.

- Yapı inşaa aşamasındayken özel su gerçirmez ekipmanlarla inşaa edilmiştir.
- Su baskını durumlarında yetkili personele bilgi vermek için yapının çeşitli bölgelerinde su dedektörleri bulunmaktadır.

5.1.3 Yangın Önlemleri ve Korunması

Su ile söndürme sistemi bilgi işlem donanımlarında kalıcı hasara neden olabileceği için sunulan hizmeti etkileyebilir. Bu sebeple aşağıdaki yangın önleme sistemleri kullanılmaktadır..

- Yapı içerisinde sigara içilmesi yasaklanmıştır.
- Yangın uyarı ekipmanları yapı içerisinde çeşitli yerlerde konumlandırılmıştır.
- Yangın uyarı ekipmanları enerji kesintilerinden etkilenmez.
- “e-imzaTR” personeli yangın sırasında yapılacaklarla ilgili eğitim almıştır.
- “Güven Merkezi” bilgi işlem donanımlarına arar vermeyecek FM200 gazlı yangın söndürme sistemi ile donatılmıştır.

5.1.4 Veri Depolama Araçlarının Saklanması

Veri depolama için aşağıdaki araçlar kullanılabilirr.

- Kağıt, DVD, USB Bellekler, Harici Harddiskler.

Veri depolama araçlarına aşağıdaki kontroller uygulanır;

- Gizlilik arzeden tüm veriler özel dizayn edilmiş arşiv odasında saklanır.
- Arşiv odasına erişim biyometrik giriş kontrolleri uygulanarak iki katmanlı giriş kontrolüyle sağlanır.
- Zorunlu durumlarda medyalar dışarı şifreli şekilde çıkarılabilir.
- Veri depolama araçları arşiv odalarında kilitli bölümlerde saklanır.
- Tokenlar Güvenli bölgede saklanır.

5.1.5 Atık Kontrolü

Aşağıdaki atık kontrol politikaları uygulanır:

- Atıklar çevreye zarar vermeyecek şekilde imha edilir.
- Atıklar haftada en az bir kez bertaraf edilir.
- Gizlilik seviyesindeki atıkların dışarı sızması önlenir.

5.1.6 Harici Alan Yedeklemesi

"e-imzaTR" olası teknik arızalara ve/veya afetlere karşı, "Güven Merkezi" içinde ve dışında rutin olarak elektronik kayıtların yedeklerini alır ve saklar.

5.2 Prosedür Kontrolleri

5.2.1 Güvenli Roller

Güvenilir rollere sahip bir kişi görevinin düzgün yapılmaması halinde güvenlik sorunlarına neden olabilir. Bu rollerde görev alacak kişiler seçilirken görevlerini tam anlamıyla yerine getirebilecek ve oluşacak sorunlarda doğru karar verecek kişiler olmalıdır. Bu roller "Trust Center"ın devamlılığı için temel oluşturmaktadır. Güvenilir roller aşağıdaki gibidir:

- Güven Merkezi Yöneticisi
- Kayıt Memuru
- Güvenlik Memuru
- Sistem Operatörleri
- Sistem Denetçileri

5.2.2 Her Bir Görev İçin Gereken Kişi Sayısı

Roller oluşturulurken kişilerine kötü niyetli olabileceği düşünülerek gerekli görev ayrımları oluşturulmuştur. Her bir kullanıcının sisteme erişim yetkisi sorumluluklarını yerine getirebilecekleri şekilde sınırlandırılmıştır. Kriptogafik araçlara, güvenli bölgelere ve arşive erişim birden çok kullanıcının birlikte erişimiyle sağlanır. Kişisel hataların önüne geçebilmek için önemli rollerdeki işlemler en az iki kişi ile gerçekleştirilir.

İkili kontrol sistemleri aşağıdakiler için uygulanır::

- Sertifika ve Kök sertifikaların bulunduğu sistemlere erişim,
- Bu sistemlerde yapılacak herhangi bir değişiklik,
- Sistemlerin kapatılıp açılması.

5.2.3 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 kayıt altına alınır.

5.2.4 Görevlerin Ayrılmasını Gerektiren Roller

Bazı “NES” sertifika yaşam zinciri işlemleri, “ESHS” 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.
Yönetim; sorumlulukların atanması ve görevlerin ayrılığını sağlarken, aşağıdaki hususları göz önünde bulundurur:

a) Dolandırıcılığı önlemek için, gizlilik gerektiren faaliyetler, örneğin satın alma siparişinin verilmesi ve malların alındığının doğruluğunun kanıtlanması faaliyetleri, ayrılır;
b) Eğer gizliliğin ihlal edilmesi tehlikesi varsa, faaliyetten sorumlu personel sayısı artırılır;
c) Sistem erişim kontrollerinin yönetilmesi sorumluluğu, güvenlik kontrollerinin zayıflamasına sebep olabilecek diğer sorumluluklardan ayrılır;
d) Sistem kullanıcı erişim hakları üzerinde yapılacak tüm yaratma, değişiklik, kaldırma istekleri, Güven Merkezi Yöneticisi onayladıktan sonra gerçekleştirilir ve bu istekler, alınan ve uygulanan kararlar belgelenir. Belgeler ileride olabilecek bir kontrol için en az 1 yıl saklanır;
e) Sistem erişim hakları, Sistem Yöneticisi tarafından düzenli aralıklarla gözden geçirilir ve ihtiyaç duyulmadığında kaldırılır. Paylaşılan şifrelerin kontrolü ve yönetimi için sorumluluklar atanır;
f) Yüksek risk taşıyan görevlerde, ek kontroller uygulanır;
Yönetimsel prosedürlerin uygulanması denetlenir.

5.3 Personel Kontrolleri

5.3.1 Mesleki Bilgi, Nitelikler, Deneyim ve Adli Sicil Gereksinimleri

“e-imzaTR” Personel işe alımları ikiye ayrılmıştır. “Güvenli Personel” istihdamı, Genel personel istihdamı. “Güvenli Personel” “NES” üretimi hazırlanması gibi kritik görevlerde bulumaktadır. “Güvenli Personel” istihdamı sırasında kişilerin adli sicil kayıtları ve sosyal yaşantılarındaki yerleride dahil olmak üzere sıkı güvenlik kontrollerinden geçtikten sonra mesleki yeterlilik ve deneyim konularında ibraz edeceği belgelerle birlikte “Güven Merkezi” yöneticileri tarafından mülakata alınır. Personel adayları tüm bu denetimlerden geçtikten sonra uygun bulunursa istihdam edilir.

5.3.2 Mesleki Bilgi Kontrol Prosedürleri

Bakınız 5.3.1.

5.3.3 Eğitim Şartları

“e-imzaTR” personelleri göreve başlamadan önce ESHS hizmetleri, sertifika yaşam zinciri hizmetleri, mesleki sorumluluklar, temel açık anahtar alt yapısı çerçevesi, “e-imzaTR”

güvenlik prosedürleri ve sertifika politikaları konularında gerekli hukuki ve teknik eğitimden geçirilirler.

5.3.4 Eğitim Sıklığı

"e-imzaTR" Düzenli olarak eğitim içeriklerini kontrol eder ve güncelleme, değişiklik yada uygun görülmesi halinde tazeleme eğitimleri düzenler.

5.3.5 İş Rotasyon Sıklığı ve Sırası

İlgili eğildir.

5.3.6 Yetkisiz Eylemlere Karşı Yaptırımlar

"e-imzaTR" personelin ya da işbirlikçilerin güvenlik prosedürlerinin dışında işlem yapması veya "e-imzaTR" ve kullanıcılarının bilgilerini tehlikeye sokacak, zarara uğratacak eylemlerde bulunmasını önlemek için gerekli mantıksal iş ayrımı ve gizlilik sözleşmeleriyle güvence altına almıştır. Yetkisiz eylemler veya süreç 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.

5.3.7 Bağımsız Yüklenici Gereksinimleri

"e-imzaTR", "ESHS" faaliyetlerini yürütmek için bağımsız yükleniciler ile hizmet sözleşmeleri akdedebilir. Hizmet sözleşmeleri "e-imzaTR"nın güvenlik ve işleyiş süreçlerine uyumlu olacak şekilde düzenlenir.

5.3.8 Personele Verilen Dökümanlar

"e-imzaTR" tüm personeline "NESUE", "NESİ" belgelerini ve görevleriyle ilgili özel nitelikli yazılım ve donanım kullanım kılavuzlarını verir.

5.4 Denetim Kayıt Prosedürleri

5.4.1 Kaydedilen Olay Tipleri

"e-imzaTR"nın "ESHS" işleyişine ve organizasyonel fonksiyonlarına ilişkin aşağıdaki kayıtlar elektronik ve/veya kağıt ortamında - olayın tanımı, gerçekleşme tarihi, olayla ilgili kişilere ilişkin bilgiler de dahil olmak üzere - tutulur.

- Sistemlerin kapatılması/açılması;
- "NES" uygulamalarının kapatılması/açılması;
- "ESHS" anahtar (veri) yaratma, yedekleme, saklama, kurtarma, arşivleme ve imha etme;
- "NES" profilleri yada uygulamalarının değiştirilmesi;
- "NES" üretim politikalarında yapılan değişiklikler;

- Başarılı veya başarısız sisteme erişim girişimleri.;
- "NES" üretimi ve iptal edilmesi;
- Sistem arızaları, donanım arızaları ve diğer anormallikler
- Fiziksel erişim kayıtları;
- Sistem ayarlarında yapılan değişiklikler ve bakımlar;
- "e-imzaTR personel değişiklikleri;
- Tutarsızlık ve uzlaşma raporları;
- "NESİ" ve "NESUE" tüm versiyonları;
- Geçerli ve geçerlilik süresi geçmiş anlaşmalar
- Bireysel ve kurumsal "NES" başvuruları, başvurularda kullanılan bilgi ve belgeler.
- Bireysel ve kurumsal başvuru sözleşmeleri, ilgili diğer sözleşme ve belgeler.
- "NES"lerin oluşturulması, iptali, askıya alınması ve yenilenmesiyle ilgili eylem ve bilgiler (eylemlerin zamanı ve eylemleri yapan yetkililer de dahil olmak üzere).
- Müşteriler ve iş ortaklarıyla yapılan sözleşmeler, önemli yazışmalar.
- Geçerlilik süresi sona eren "NES"ler.
- Geçerlilik süresinin sona ermesinden itibaren "ESHS" kök ve alt kök sertifikası.
- İptal, askıya alma, askıdan kaldırma ile ilgili talep ve talebin doğrulanması eylemleri ve ilgili iletişim bilgileri, "SİL"ler.

Kayıtlar; doğru ve tam olarak sıralanması, saklanması, korunması ve çoğaltılması şartıyla elektronik veya basılı kopya halinde tutulabilir.

5.4.2 Kayıtların İşleme Sıklığı

Kayıt tutma işlemi sürekli gerçekleşir. Kayıtlar ayda bir kere denetlenir. "e-imzaTR" gerekli görmesi durumunda kayıt denetleme işleminin periyodunu değiştirebilir.

5.4.3 Denetim Kayıtlarının Saklama Süresi

Denetim kayıtları işlendikten sonra veri depolama kapasitesine göre erişilebilir şekilde sistemde tutulur. İlgili mevzuata göre saklanması gereken bilgi ve belgeler ise 20 yıl boyunca saklanır.

5.4.4 Denetim Kayıtlarının Korunması

Elektronik ve kağıt ortamındaki denetim kaydı dosyalarına, yetkisiz kişilerin izlemesine, değişiklikler yapmasına, silmesine veya başka herhangi bir şekilde erişmesine karşı fiziksel ve mantıksal erişim kontrolleri kullanılır ve bu yolla denetim kaydı dosyaları korunur.

5.4.5 Denetim Kayıtlarını Yedekleme Prosedürleri

Denetim kayıtları günlük ve haftalık arşivleme süreçleri doğrultusunda periyodik olarak yedeklenir.

5.4.6 Denetim Verilerini Toplama Sistemi

Başvuru safhasında, ağ ve işletim sistemi seviyesinde, elektronik ortamda gerçekleşen işlemlerin denetim verileri otomatik olarak oluşturulur ve kaydedilir. Manuel olarak yapılan işlemlere ilişkin denetim verileri "e-imzaTR" personelince manuel olarak kaydedilir.

5.4.7 Olaya Sebep Olan Kişilere Bilgilendirme Yapılması

Denetim bilgisi toplama sistemi bir olay kaydettiği zaman, olaya sebep olan birey, kurum veya görevliye ihbarda bulunmaya gerek yoktur. Ancak olayın niteliğine ve önem derecesine göre sistem ilgiliye ihbarda bulunabilir.

5.4.8 Güvenlik Açıkları Değerlendirmesi

Denetim kayıtlarının rutin olarak gözden geçirilmesi sonucunda sistemdeki ve süreçlerdeki güvenlik açıkları tespit edilerek gerekli olan önlemler alınır..

5.5 Anahtar Değişimi

"e-imzaTR" "ESHS" zaman damgası oluşturma ve doğrulama verilerinin geçerlilik süreleri, ilgili mevzuatta belirtildiği üzere, en fazla 10 yıl olacaktır. Gerekli görülen durumlarda güvenlik sebebiyle ve "ESHS" zaman damgası oluşturma verisinin geçerlilik süresinin dolmasından önce "ESHS" zaman damgası oluşturma verisi yenilenir. Bu durumda eski anahtarlar (zaman damgası oluşturma ve doğrulama verileri) geçerlilik süresinin sonuna kadar kullanılabilir durumda saklanır. "ESHS"nin zaman damgası oluşturma verisinin değişiminden itibaren yeni oluşturulacak olan "Zaman Damgaları yeni zaman damgası oluşturma verisiyle imzalanır. Ancak eskiden oluşturulmuş olan zaman damgalarının doğrulanabilmesi için eski zaman damgası doğrulama verisinin içinde bulunduğu eski "e-imzaTR" "ESHS" kök sertifikası ve alt kök sertifikasının erişilebilirliği sağlanır..

.

5.6 Tehlike ve Felaketten Kurtarma

"e-imzaTR" "ESHS" işlemlerinin güvenilirliğini ya da sürekliliğini tehlikeye atacak bir durum geliştiğinde ilgili prosedürler doğrultusunda sistemin güvenliğini ve sürekliliğini sağlayarak gerekli durumlarda ilgili kullanıcı ve kurumlara bilgilendirme yapar. "Zaman Damgası" sunucusunun bir yedeği "Felaket Kurtarma Merkezi"nde bulunmaktadır. Arıza durumunda kullanıcılar aktif bekleyen "FKM" sistemine yönlendirilerek kesintisiz bir şekilde hizmet alması sağlanır.

6 TEKNİK GÜVENLİK KONTROLLERİ

6.1 imza Verilerini Oluşturma ve Kurma

6.1.1 İmza Oluşturma Verilerini Yaratma

"ESHS" "Zaman Damgası" oluşturma ve doğrulama verileri oluşturma işlemi, oluşturulan veriler için güvenliği ve gerekli şifreleme gücünü temin eden güvenilir sistemler kullanılarak, önceden seçilmiş birden fazla eğitimli "güvenli personel" ve ilgili görevliler tarafından yerine getirilir. "e-imzaTR" kök sertifikası için, "Zaman

Damgası" oluşturma ve doğrulama verileri oluşturmada kullanılan şifreleme modülleri FIPS 140-2 Seviye 3 şartlarını karşılar. “e-imzaTR” kök sertifikasının "Zaman Damgası" oluşturma ve doğrulama verileri “Tebliğ”de belirtilen algoritmalara ve standartlara uygun olarak oluşturulur; anahtar oluşturma işlemi sırasında yapılan faaliyetler kaydedilir, tarih atılarak imzalanır. Bu kayıtlar denetim ve izleme amacıyla saklanır. "Zaman Damgası" oluşturma verisi “ESHS”nin güvenli elektronik imza oluşturma aracında oluşturulur ve buradan yedekleme amacı dışında çıkarılamaz. "Zaman Damgası" oluşturma verisinin güvenli olarak saklanması için gerekli fiziksel ve teknik güvenlik önlemleri alınır.

6.1.2 İmza Oluşturma ve Doğrulama Verilerinin Büyüklüğü

“e-imzaTR” “ESHS” Zaman Damgası oluşturma ve doğrulama verileri, 2048 bit RSA büyüklüğündedir. "Zaman Damgası" SHA-256 özet algoritması kullanılarak imzalanır.

6.2 Anahtarların Korunması ve Şifreleme Modulü Sistem Kontrolleri

All TSAs are required to take all appropriate and adequate steps in accordance with the requirements of this CP to protect and prevent the loss, damage, disclosure, modification or unauthorized use their private keys.

6.2.1 şifreleme Modülü Standartları ve Kontrolleri

Şifrele modülü uygulamaları FIPS 140-2 “Security Requirements for Cryptographic Modules” standardına uygun olarak gerçekleştirilir.

6.2.2 İmza Oluşturma Verisine Birden Fazla Kişiyle Erişim Sağlanması

“e-imzaTR” “ESHS” imza oluşturma ve doğrulama verilerine erişim ancak birden çok yetkili “Güvenli Personel”in gerekli güvenlik ve tanımlama prosedürlerini yerine getirmesi halinde gerçekleşmektedir.

6.2.3 İmza Oluşturma Verisinin Saklanması

“e-imzaTR” “NES” sahiplerine ait "Zaman Damgası" oluşturma verilerinin kopyalarını saklamaz.

6.2.4 İmza Oluşturma Verisi Yedekleme

“e-imzaTR” “ESHS” imza oluşturma ve doğrulama verilerini yedekleme işlemi birden çok yetkili “Güvenli Personel” ile anahtar töreni sırasında kriptografik kartlara yüklenerek farklı lokasyonlardaki kasalarda saklanır.

6.2.5 İmza Oluşturma Verisi Arşivleme

“e-imzaTR” “ESHS” kök sertifikalarına ait "Zaman Damgası" oluşturma verileri arşivlenmez, "Zaman Damgası" doğrulama verileri ve kök sertifikalar ise ileride çıkması muhtemel uyuşmazlıklarda kullanılmak üzere 20 yıl süreyle saklanır

6.2.6 İmza Oluşturma Verisinin Şifreleme Modülüne/Modülünden Transferi

“e-imzaTR”, “ESHS” kök sertifikalarının "Zaman Damgası" oluşturma ve doğrulama verilerini, “ESHS”ye ait olan güvenli elektronik imza oluşturma aracı içerisinde (kriptografik modül) oluşturur. “ESHS” "Zaman Damgası" oluşturma verisi yedekleme amacı dışında kesinlikle “ESHS” güvenli elektronik imza oluşturma aracından çıkarılamaz. Yedekleme amacıyla "Zaman Damgası" oluşturma verisinin başka bir

kriptografik modüle transferi gerekli teknik ve fiziksel güvenlik önlemleri altında sadece birden çok yetkili “Güvenli Personel” tarafından gerçekleştirilebilir.

6.2.7 Anahtarın Şifreleme Modülünde Saklanması
Bkz. "ZDİ" 6.2.6

6.2.8 İmza Oluşturma Verisinin Aktif Hale Getirilmesinin Metodu
“e-imzaTR” “ESHS” kök sertifikaları "Zaman Damgası" oluşturma verilerinin aktivasyonu gerekli teknik ve fiziksel güvenlik önlemleri altında sadece birden çok yetkili “Güvenli Personel” tarafından gerçekleştirilebilir.

6.2.9 İmza Oluşturma Verisinin Pasif Hale Getirilmesinin Metodu

“ESHS” "Zaman Damgası" oluşturma verilerinin pasif hale getirilmesi işlemi cihazlar pasif durumdayken en az iki yetkili “Güvenilir Personel” tarafından gerçekleştirilir.

6.2.10 İmza Oluşturma Verisinin İmha Edilmesi Metodu

“e-imzaTR” ye ait imza oluşturma ve doğrulama verileri yaşam ömürleri doldurduktan sonra kayıt altına alınarak yetkili personel tarafından imha edilebilir.

6.2.11 Şifreleme Modülü Operasyonel Limitleri
“e-imzaTR” “ESHS” "Zaman Damgası" oluşturma araçları “Tebliğ”de belirtilen standartlara uygundur.

6.3 Anahtar Çifti Yönetimi Diğer Yönleri

6.3.1 İmza oluşturma Verisinin Saklanması
“e-imzaTR” “ESHS” kök sertifikaları, “NES”ler ve bunlara bağlı imza doğrulama verileri en az 20 yıl boyunca saklanır.

6.3.2 Sertifikanın Operasyonel Periyodu ve Anahtar Çifti Kullanım Periyodu
“e-imzaTR” kök sertifikalarının geçerlilik süreleri 10 yılı aşmaz. “NES” kullanıcılarının sertifika süreleri sözleşmelerinde belirtildiği süre kadardır ancak imza doğrulama verileri sertifika geçerlilik süresinden sonra kullanılmaya devam edilebilir.

6.4 Erişim Verileri

6.4.1 Erişim Verilerinin Yaratılması ve Kurulması
“ESHS” "Zaman Damgası" oluşturma ve doğrulama verileri kriptografik verilerde saklanır ve en az iki yetkili “Güvenilir Personel” tarafından kriptografik akıllı kartlar ve şifreler aracılığıyla aktive edilebilir.

6.4.2 Erişim Verilerinin korunması

bkz "ZDİ" 6.2

6.4.3 Erişim Verileriyle İlgili Diğer Durumlar

İlgili değildir.

6.5 Bilgisayar Güvenlik Kontrolleri

6.5.1 Erişim Kontrolü

Erişim kontrolü politikalarında detaylı olarak belirtilmekle birlikte "e-imzaTR" ihtiyaç duyulan her alanda mantıksal ve fiziksel olarak erişim kontrolü prosedürlerini sıklaştırabilir ve güvenlik seviyesini yükseltebilir. "ESHS" imza oluşturma ve doğrulama verileriyle ilgili işlemlerin hepsi en az 2 yetkili " Güvenilir Personel" tarafından gerçekleştirilir ve kayıt altına alınır.

6.5.2 İşletim Sistemleri

Sadece lisanslı ve tutarlı çalıştığı onaylanmış işletim sistemleri kullanılır.

6.6 Yaşam Zinciri Teknik Kontrolleri

6.6.1 Sistem Geliştirme Kontrolleri

"e-imzaTR" sertifika yaşam zinciri sistem geliştirme kontrolleri "e-imzaTR" kalite yönetimi prosedürleri ve TS ISO/IEC 27001 denetimleri sonucunda ortaya çıkan risk azaltma metodları uyarınca gerçekleştirilir.

6.6.2 Güvenlik Yönetim Kontrolleri

TS ISO/IEC 27001 standardına uyumlu şekilde denetimler gerçekleştirilir. Değişiklik yapılması gerektiğinde öncelikle ihtiyaç belirlenir. Belirlenen ihtiyaç yazılı şekilde yöneticilere iletilir. Yöneticilerden onay geldiğinde yapılacak değişiklik kayıt altına alınarak gerçekleştirilir.

6.6.3 Yaşam Zinciri Güvenlik Kontrolleri

İlgili değildir..

7 REFERANSLAR

e-imzaTR NESİ http://www.e-imzatr.com/e-imzatr-nessi
e-imzaTR NESUE http://www.e-imzatr.com/e-imzatr-nessue