T.C.

EMNİYET GENEL MÜDÜRLÜĞÜ

ZAMAN DAMGASI UYGULAMA ESASLARI

SÜRÜM :01

TARİH:05.07.2012

1. GİRİŞ

Türk Polis Teşkilatı, rütbeleri Polis Memurluğundan başlayıp Emniyet Genel Müdürlüğüne kadar uzanan, tüm il ve ilçelerde örgütlenmiş, kırsalda görevini askeri polis olan jandarmaya bırakmış, kentte ise görevi kendisi yöneten iç güvenlikten sorumlu devlet teşkilatıdır. 10 Nisan 1845 tarihinde temeli atılmıştır.

Merkez teşkilatı bünyesinde Ana Komuta Kontrol, Strateji Geliştirme, Arşiv, Asayiş, Bilgi İşlem, Dış İlişkiler, Eğitim, Güvenlik, Haberleşme, Havacılık, İdari ve Mali işler, İkmal-Bakım, İnşaat-Emlak, Interpol, İstihbarat, Kaçakçılık ve Organize Suçlarla Mücadele, Koruma, Kriminal, Özel Harekât, Personel, Sağlık İşleri, Sivil Savunma, Sosyal Hizmetler, Teftiş Kurulu, Terörle Mücadele Harekât, Trafik Eğitim ve Araştırma, Trafik ve Denetleme, Yabancılar Hudut İltica Daireleri vardır. Taşra teşkilatını ise, il emniyet müdürlükleri ve ilçe Emniyet Amirlikleri oluşturur. Genel müdürlük, üst kurum ve yönetim bakımından İçişleri Bakanlığı'na bağlıdır.

Kurumun yapılanması iki şekilde olmuştur. Birincisi Merkez Teşkilatı ve ikincisi ise Taşra Teşkilatı'dır. Merkez Teşkilatı, Daire Başkanlıkları şeklinde yapılanmıştır. Taşra Teşkilatı ise 81 ilde İl Emniyet Müdürlükleri olarak faaliyet yürütmektedir. Merkez Teşkilatı'ndaki daire başkanlıklarının bazıları direkt olarak emniyet genel müdürüne bağlı olmak ile birlikte diğerleri ise 5 adet emniyet genel müdür yardımcısına bağlı olarak hizmet vermektedir. Taşra teşkilatında ise illerin başında il emniyet müdürü bulunmakta ve ildeki bütün birimler il emniyet müdürüne bağlı olmaktadır.

Türkiye Cumhuriyeti sınırları içerisinde, belediye teşkilatlanması tamamlanmış olan il, ilçe ve beldelerde güvenlik, Emniyet Genel Müdürlüğü tarafından sağlanmakta; daha küçük birimlerin ve yapılaşmaya açılmamış alanların güvenliği ise Jandarma Genel Komutanlığı tarafından sağlanmaktadır. Emniyet Genel Müdürlüğü Merkez ve 81 ilde teşkilatlanmış olup konularına göre uzmanlaşmış alt birimlere ayrılmıştır.

T.C. Emniyet Genel Müdürlüğü (EGM) Zaman Damgası Uygulama Esasları (ZDUE) dokumanı, 15 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza Kanunu, 2004/21 sayılı Başbakanlık Genelgesi, Bilgi Teknolojileri ve İletişim Kurumu'nun yayımladığı Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik, Elektronik İmza İle İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'e uygun olarak hazırlanmıştır.

ZDUE kitapçığı, zaman damgası başvurularının alınması, zaman damgası üretimi ve talep sahibine zaman damgasının gönderilmesi gibi temel zaman damgası hizmet ve işlemleriyle ilgili idari, teknik ve yasal gerekliliklere nasıl uyulduğunu ortaya koyar; elektronik sertifika hizmet sağlayıcısı (ESHS) olarak EGM' nin ve diğer tarafların uygulama sorumluluklarını belirler.

1.1. Genel Bakış

ZDUE kitapçığı, tüm zaman damgası hizmetlerini kapsar.

EGM, zaman damgası alanındaki faaliyetlerini nasıl yürüttüğü, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu'na (TÜBİTAK) bağlı Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM) tarafından oluşturulan, Kamu Sertifikasyon Merkezi'nin (Kamu SM) Zaman Damgası İlkeleri (ZDİ) dokümanında belirlenen ilkeler doğrultusunda tanımlanmıştır.

1.2. Doküman Tanımı

Bu ZDUE dokümanının açık adı "T.C. Emniyet Genel Müdürlüğü Zaman Damgası Uygulama Esasları (ZDUE)"dır. Dokümanın sürüm numarası ve tarihi kapak sayfasında yer almaktadır.

ZDUE dokümanı "http://www.egmsm.gov.tr" web adresinde kamuya açık olarak yayımlanmaktadır.

1.3. Sistem Bileşenleri

1.3.1. Zaman Damgası Hizmeti

Zaman Damgası üreten son kullanıcılar tarafından güvenilen sistem bileşeni zaman damgası bileşeni olarak adlandırılır.

1.3.2. Son Kullanıcılar

Zaman damgası sahipleri, kendilerinden zaman damgası başvuruları alınan ve talep edilen zaman damgası üretilerek yine kendilerine gönderilen kişilerdir.

1.3.3. Üçüncü Taraflar

Üçüncü taraflar, EGM zaman damgası hizmetleri kapsamında, EGM tarafından verilmiş olan zaman damgalarını alan ve ilgili zaman damgalarını doğrulayan taraflardır.

1.4. Uygulama Esaslarının Yönetimi

1.4.1. Doküman Değişim Yönetimi

Bu ZDUE kitapçığının tüm hakları ve sorumluluğu EGM' ye aittir.

1.4.2. İletişim Bilgileri

ZDUE dokümanıyla ilgili iletişim bilgileri aşağıdadır:

T.C. Emniyet Genel Müdürlüğü
Adres : Ayrancı Mahallesi Dikmen Cad. No:11 Çankaya ANKARA
Telefon : 312 462 0 462
Faks : 312 462 67 62
Çağrı Merkezi : 312 462 67 59
E-posta : egmsm@egm.gov.tr
Web : http://www.egmsm.gov.tr

1.4.3. Yayın ve Duyuru Politikaları

ZDUE dokümanı ve duyurular "http://www.egmsm.gov.tr" web adresinde kamuya açık olarak yayımlanmaktadır.

1.4.4. Zaman Damgası Uygulama Esasları Onay Prosedürleri

ZDUE dokümanının, ZDİ dokümanına uygunluğu EGM tarafından onaylanır.

1.5. Kısaltmalar ve Tanımlar

1.5.1. Kısaltmalar

A.A.A. : Açık Anahtarlı Altyapılar - PKI

ESHS : Elektronik Sertifika Hizmet Sağlayıcısı

IETF : Internet Engineering Task Force – İnternet Mühendisliği Görev Grubu

OID : Object Identifier – Nesne Tanımlayıcı Numarası

PKI : Public Key Infrastructure – Açık Anahtarlı Altyapı

RFC : IETF tarafından yayımlanan, kılavuz niteliğinde yorum talebi dokümanları

ZDİ : Zaman Damgası İlkeleri

ZDUE : Zaman Damgası Uygulama Esasları

TSE : Türk Standartları Enstitüsü

1.5.2. Tanımlar

Açık Anahtar: bkz. İmza Doğrulama Verisi.

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

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

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

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

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

Çevrim İçi Sertifika Durum Protokolü (ÇİSDUP): Sertifikaların geçerlilik durumunun kamuya duyurulması için oluşturulmuş, sertifika durum bilgisinin çevrim içi yöntemlerle anında ve kesintisiz alınmasını sağlayan standart protokol.

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

Dizin: Geçerli sertifikaları içinde bulunduran elektronik depodur.

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

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

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

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

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

Gizli Anahtar: bkz. İmza Oluşturma Verisi.

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

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

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

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

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

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

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

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

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

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

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

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

Kurum: Bilgi Teknolojileri ve İletişim Kurumu'dur.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2. GENEL HÜKÜMLER VE ZAMAN DAMGASI HİZMETLERİNE YÖNELİK YAYINLAR

Zaman Damgası Hizmetiyle ilgili genel hükümler KSM ZDİ dokümanında düzenlenmiştir. EGM bu yükümlülük ve sorunluluklara uyumlu şekilde hizmet verir.

EGM, elektronik sertifika hizmet sağlayıcılığı kapsamında zaman damgası hizmetleriyle ilgili gereken doküman ve kayıtları hazırlamak ve saklamakla yükümlüdür. Bu doküman ve kayıtların bazıları, zaman damgası hizmetlerinin etkin bir şekilde talep sahiplerine ulaştırılabilmesi ve zaman damgası kullanımının güvenilirliğinin ve sürekliliğinin sağlanması amacıyla kamuya açık olarak yayımlanır.

2.1. Zaman Damgası Hizmetleri Bilgi Deposu

EGM, bilgi deposunda tutulan tüm bilgilerin doğruluğunu ve güncelliğini sağlar.

2.2. Zaman Damgası Hizmetleri Bilgisinin Yayımlanması

EGM bilgi deposunda, zaman damgası hizmetlerine ait özel kurumsal prosedür ve talimatlar gizli bilgiler dışında kalan, zaman damgası hizmetlerinin yürütülmesine ilişkin bilgiler, herkesin erişimine açık tutulur. EGM' nin zaman damgası hizmetlerine yönelik ilkelerin nasıl uygulandığını gösteren ZDUE, zaman damgası iş süreçleriyle ilgili uygulama prosedürleri bilgi deposunda yer alır.

Bu bölümde sözü geçen bilgilere erişim, http://www.egmsm.gov.tr adresinden yapılır.

2.3. Yayımın Zamanı veya Sıklığı

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

2.4. Bilgi Deposuna Erişim Kontrolleri

Bilgi deposu kesintisiz olarak herkesin erişimine açıktır. Bu amaçla, yayımlanan bilgilerin gerçekliğini sağlamak üzere, http://www.egmsm.gov.tr adresi için gerekli her türlü güvenlik önlemi alınır.

3. İŞLEMSEL GEREKLER

3.1. Zaman Damgası

Zaman Damgası Hizmeti RFC 3161'de tanımlı zaman damgası protokolünü destekler.

3.1.1. Zaman Damgası Andacı

EGM zaman damgası andaçlarının güvenli şekilde oluşturulmasını ve doğru zamanı içermesini sağlayacak tedbirler alır. Zaman damgası andacı damgalanan verinin özet değerini içerir ve bu özet değer zaman damgası istemcisi tarafından zaman damgası hizmetlerine ulaştırılır.

Zaman damgası andacı yalnızca zaman damgası imzala amacıyla yaratılmış imza oluşturma verisi kullanılarak imzalanır. Zaman damgası içindeki zaman bilgisi UTC ile uyumludur.

3.1.2. UTC ile Zaman Birliğinin Sağlanması

EGM, zaman bilgisinin senkronizasyonunu, GPS uydularından senkronize olan bir zaman sunucusuyla sağlamaktadır. UTC (evrensel zaman değeri) ile EGM zaman bilgisi senkronizasyon farkı, saniyenin milyonda biri düzeyindedir. Hizmetin doğru ve kesintisiz olarak sağlanabilmesi için EGM gereken tüm önlemleri alır.

3.2. Zaman Damgası Başvurusu

EGM daire başkanlıkları adına yetkilendirilecek personel belirlenen prosedürler çerçevesinde zaman damgası talep edebilir. Talep içeriğinde istenen zaman damgası sayısının (kontörünün) belirtilmesi gerekmektedir.

3.3. Zaman Damgası İsteme

Zaman damgası başvuruları, ilgili personel tarafından elektronik ortamda ve belirlenen protokoller üzerinden yapılır. Zaman damgası istenmesi sırasında istemci kimliğini doğrular. Kimlik doğrulama işleminde kullanıcı adı ve parola kullanılır.

3.4. Zaman Damgası İsteğinin İşlenmesi

Zaman damgası isteğinin işlenebilmesi için kullanıcı kimliğinin doğrulanması ve kullanılabilecek kontör olup olmadığının kontrol edilmesi gerekmektedir.

Bu iki koşulun doğrulanması halinde zaman damgası üretimi yapılır. Başvuruda kimlik doğrulamasının yapılmaması ya da yeterli kontör bulunmaması halinde ise başvuru reddedilir.

3.5. Zaman Damgasının Gönderilmesi

Zaman damgası talebi yukarıda belirtilen yöntemlerle üretildikten sonra RFC 3161'de tanımlı zaman damgası protokolü aracılığıyla istemciye gönderilir.

İstemci ilgili yazılımı kullanarak zaman damgasını alır.

3.6. Zaman Damgasının Uzun Süreli Geçerliliği

Zaman damgası imzalamak için kullanılan imzalama anahtar çiftinin kullanım süresinin dolmasından sonra da geçerliliğini koruyabilmesi gerekmektedir. Geçerlilik durumları süreleri sonra da yayımlanmaya devam eder.

4. YÖNETİM, İŞLEMSEL VE FİZİKSEL KONTROLLER

EGM' nin zaman damgası hizmetlerini yürütürken tesis ve işletme güvenliğini sağlamaya yönelik olarak uyguladığı, teknik olmayan çeşitli güvenlik kontrolleri yer almaktadır. Fiziksel güvenlik kontrolleri, prosedürel kontroller ve personel güvenlik kontrolleri EGM Sertifika Uygulama Esaslarında belirtilen şartları sağlar.

4.1. Denetim Kayıtları

4.1.1. Kaydedilen İşlemler

Zaman damgası hizmetlerine ait tüm kayıtlar EGM tarafından tutulur. Bu kayıtların arasında zaman damgası başvuru kayıtları; üretilen zaman damgaları hakkındaki kayıtlar; zaman damgası işlemlerine dahil olan tüm yönetici ve operatörlerin işlem kayıtları; çalışanların EGM ESHS birimlerine giriş ve çıkış kayıtları ile sistem modüllerine erişim kayıtları; doküman takibiyle ilgili kayıtlar; yazılım ve donanım kurulum, güncelleme ve onarım kayıtları sayılabilir.

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

4.1.2. Kayıtların İncelenme Sıklığı

Denetim kayıtları sürekli olarak tutulur ve güvenlik açıklarının yakalanabilmesi için uygun aralıklarla incelenir.

4.1.3. Kayıtların Saklanma Süresi

Kayıtlar hukuksal anlaşmazlıklara çözüm oluşturmak amacıyla, anahtar çiftinin kullanım süresinin dolmasından sonra da arşivlenerek saklanır.

4.1.4. Kayıtların Korunması

Kayıtlar, fiziksel ve elektronik güvenlik önlemleriyle korunur, sadece yetkili kişilerin erişimine açık tutulur. EGM kayıtların bütünlüğünü ve gizliliğini korur.

4.1.5. Kayıtların Yedeklenmesi

Yedekleme prosedürleri uyarınca, kayıtların periyodik olarak tesis içi ve tesis dışı yedekleri alınır.

4.1.6. Kayıtların Toplanması

Kayıtlar elektronik veya kağıt ortamda toplanır.

4.2. Kayıtların Arşivlenmesi

Tutulan kayıtlar EGM Sertifika Uygulama Esaslarına uygun şekilde arşivlenir.

5. TEKNİK GÜVENLİK KONTROLLERİ

EGM zaman damgası hizmetleriyle ilgili iş süreçlerinde kullanılan imza oluşturma verilerinin ve erişim verilerinin yönetimi ile teknik altyapıya ve zaman damgası hizmetlerinin işleyişine yönelik güvenlik kontrollerini Sertifika Uygulama Esasları dokümanı temel alınarak belirlenmiştir.

5.1. Zaman Damgası Hizmeti Anahtar Çifti Üretimi ve Kurulumu

5.1.1. Zaman Damgası Hizmeti Anahtar Çifti Üretimi

Zaman damgası alt kök sertifikasına ait anahtar çiftleri, sadece yetkili kişilerin kontrolünde, teknik ve idari güvenlik önlemleri alınmış ortamlarda üretilir. İmza oluşturma verisi yetkisiz erişime karşı fiziksel ve teknik güvenlik önlemleriyle korunur.

5.1.2. Zaman Damgası Hizmeti Sertifikalarına Erişim Sağlanması

Zaman damgası alt kök sertifikası üçüncü tarafların erişebileceği şekilde yayımlanır. Böylelikle, imza doğrulama verileri üçüncü taraflarca kullanılabilir.

5.1.3. Zaman Damgası Hizmeti Anahtar Uzunlukları

Zaman damgası alt kök sertifikasında, Tebliğ'le belirlendiği gibi en az 2048 bit RSA anahtar çiftleri kullanılır.

5.1.4. Zaman Damgası Hizmeti Anahtar Kullanım Amaçları

Zaman damgası imza oluşturma verisi, güvenilir zaman damgası oluşturmak amacıyla, ilgili imza doğrulama verisi ise zaman damgasının doğrulunu denetlemek amacıyla kullanılır.

5.2. Zaman Damgası Hizmeti İmza Oluşturma Verisinin Korunması

5.2.1. Kriptografik Modül Standartları

Anahtar çifti üretimi ve zaman damgası işlemleri, Tebliğ'le belirlenen standartlarla uyumlu, güvenli kriptografik donanım modüllerinde gerçekleştirilir.

5.2.2. Zaman Damgası Hizmeti İmza Oluşturma Verisine Erişim Denetimi

İmza oluşturma verisine erişim güvenli alanlarda birden çok personelin aynı anda bulunmasıyla sağlanabilir. Bu personellerin elektronik olarak kimlik ve yetki kontrolleri yapılır.

5.2.3. Zaman Damgası Hizmeti İmza Oluşturma Verisinin Saklanması

Zaman damgası alt kök sertifikasına bağlı imza oluşturma verisi, üretildikleri ve Tebliğ'de tanımlı güvenlik düzeyine sahip kriptografik donanım modüllerinde saklanır.

5.2.4. Zaman Damgası Hizmeti İmza Oluşturma Verisinin Yedeklenmesi

Zaman damgası alt kök sertifikasına bağlı imza oluşturma verisinin kontrollü olarak yedeği alınır ve fiziksel ve teknik güvenlik kontrolleri altında saklanır. Bu işlem birden çok yetkili personelin aynı anda bulunmasıyla yapılabilir.

5.2.5. Zaman Damgası Hizmeti İmza Oluşturma Verisinin Arşivlenmesi

Zaman damgası alt kök sertifikasına bağlı imza doğrulama verileri, ESHS tarafından 20 yıl süreyle saklanır.

5.2.6. Zaman Damgası Hizmeti İmza Oluşturma Verisinin Kriptografik Modüle Yüklenmesi

İmza oluşturma verisi güvenlik gereklerine uygun biçimde kriptografik modül dışında üretilebilir, ancak imza oluşturma verisinin kriptografik modül içinde saklanması zorunludur. Modül dışında üretim sonrası kriptografik modüle yükleme işlemi sırasında yine birden çok yetkilinin bulunması gerekir.

5.2.7. Zaman Damgası Hizmeti İmza Oluşturma Verisine Erişim

Zaman damgası alt kök sertifikasına bağlı imza oluşturma verisi, içinde bulundukları donanım güvenlik modülü üzerinde, iki yetkilinin hazır bulunmasıyla aktive edilir.

5.2.8. Zaman Damgası Hizmeti İmza Oluşturma Verisine Erişimin Kesilmesi

Zaman damgası alt kök sertifikasına bağlı imza oluşturma verisi, içinde bulundukları donanım güvenlik modülü üzerinde sadece belirli bir süreyle ve işlem bazlı aktive edilir; işlem tamamlandıktan ya da süre bittikten sonra deaktive olur.

İmza oluşturma verisinin yeniden kullanılabilmesi için, yetkililerin tekrar sisteme tanıtılarak imza oluşturma verisinin aktive edilmesi gerekir.

5.2.9. İmza Oluşturma Verisi Yok Etme Metodu

Zaman damgası alt kök sertifikasına bağlı imza oluşturma verisi, içinde bulunduğu donanım güvenlik modüllerinin sıfırlama özelliği kullanılarak sadece yetkili kişiler tarafından yok edilebilir. Bu işlem için en az iki kişinin aynı anda hazır bulunması gerekir.

5.3. Zaman Damgası Hizmeti Anahtar Çiftiyle İlgili Diğer Konular

5.3.1. Zaman Damgası Hizmeti İmza Doğrulama Verisinin Arşivlenmesi

Zaman damgası alt kök sertifikasının imza doğrulama verisinin içinde bulunduğu sertifikalar yasa ve ilgili yönetmeliklerin belirttiği süreler uyarınca arşivlenir. Veri bütünlüğünün sağlanması için her türlü önlem alınır.

5.3.2. Zaman Damgası Hizmeti İmza Oluşturma ve Doğrulama Verilerinin Kullanım Süreleri

Zaman damgası alt kök sertifikasının geçerlilik süreleri 10 yılı aşmaz. Bu sürenin sonunda sertifikalar yenilenirken mutlaka anahtar yenileme yapılır.

5.3.3. Zaman Damgası Hizmeti İmza Oluşturma ve Doğrulama Verilerinin Yenilenmesi

Zaman damgası imzalama anahtar çiftinin kullanım süresi dolmadan yenileriyle değiştirilmesi için gereken önlemler alınır ve süresi dolan anahtar çifti tekrar kullanılamaması için silinir.

5.4. Erişim Denetim Verileri

Zaman damgası hizmetiyle ilgili erişim denetim verileri, KSM Sertifika İlkeleri dokümanına uygun şekilde güvenlik şartlarını sağlar.

5.5. Bilgisayar Güvenliği Denetimleri

EGM Sertifika Uygulama Esasları dokümanında belirlenen bilgisayar güvenliği denetimleri zaman damgası hizmetinde de uygulanmaktadır.

5.6. Yaşam Döngüsü Güvenlik Denetimleri

Zaman damgasıyla ilgili yaşam döngüsünde, EGM Sertifika Uygulama Esasları dokümanında yer alan güvenlik denetimleri uygulanır.

5.7. Ağ Güvenlik Kontrolleri

Zaman damgasıyla ilgili ağ güvenliğinde, EGM Sertifika Uygulama Esasları dokümanında yer alan güvenlik denetimleri uygulanır.

6. UYGUNLUK DENETİMLERİ

Zaman damgasıyla ilgili uygunluk denetimleri, EGM Sertifika Uygulama Esasları dokümanında yer alan şekliyle uygulanır.

7. DİĞER İŞLER VE HUKUKSAL MESELELER

Zaman damgasıyla ilgili bu konular, EGM Sertifika Uygulama Esasları dokümanında yer alan şekliyle uygulanır.