TÜBİTAK BİLGEM
KAMU SERTİFİKASYON MERKEZİ

ZAMAN DAMGASI UYGULAMA ESASLARI

Doküman Kodu	Yayın Numarası	Yayın Tarihi
YONG-001-008	**01**	**20.10.2015**

ZAMAN DAMGASI UYGULAMA ESASLARI

DEĞİŞİKLİK KAYITLARI

Yayın No	Yayın Nedeni	Yayın Tarihi
00	İlk Çıkış.	12.08.2005
01	Tanımlar kısmında ve doküman genelinde gramer düzenlemeleri yapıldı.	20.10.2015

ZAMAN DAMGASI UYGULAMA ESASLARI

İÇİNDEKİLER

ZAMAN DAMGASI UYGULAMA ESASLARI

1 Giriş

Bu doküman, TÜRKİYE BİLİMSEL ve TEKNOLOJİK ARAŞTIRMA KURUMUNA'na (TÜBİTAK) bağlı BİLİŞİM ve BİLGİ GÜVENLİĞİ İLERİ TEKNOLOJİLERİ ARAŞTIRMA MERKEZİ (BİLGEM) Başkanlığı bünyesinde yer alan Kamu Sertifikasyon Merkezi'nin (Kamu SM) zaman damgası hizmetinin işleyişi sırasında uyguladığı esasları tanımlayan Zaman Damgası Uygulama Esasları (ZDUE) dokümanıdır.

KAMU SM, 15 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza Kanunu, 2004/21 sayılı Başbakanlık Genelgesi, Telekomünikasyon Kurumu'nun yayımladığı Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik, Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de tanımlandığı şekliyle Elektronik Sertifika Hizmet Sağlayıcısı (ESHS) işlevlerini yerine getirir. KAMU SM yapısı içinde kullanıcılara güvenilir zaman kaynağı olarak hizmet veren Zaman Damgası Hizmeti (ZDH) mevcuttur.

Bu doküman 15 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza Kanunu, Telekomünikasyon Kurumu'nun yayımladığı Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik, Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ esas alınarak hazırlanmıştır.

1.1 Genel Bakış

Elektronik imzalı veriye eklenen zaman damgası elektronik imzanın belirli bir tarihten önce oluşturulduğunu ispatlayarak *inkar edilmezlik* özelliğini güçlendirir.

Zaman damgası, ZDH'nin imzasını içerir ve böylece zaman bilgisinin bütünlüğü korunur. Zaman damgası, tarih ve zaman bilgisi, damgalanacak verinin özeti ve bunların ZDH tarafından oluşturulmuş imzasını içerir.

KAMU SM bünyesindeki zaman damgası hizmetleri bu dokümanda tanımlanan uygulama esasları uyarınca çalışır. Bu ZDUE dokümanı ZDİ dokümanında belirtilen ilkelere uygun olarak hazırlanmıştır Bu doküman ZDH'nin ve sistem bileşenlerinin tanımlı çalışma ilkeleri doğrultusunda işleyişlerini nasıl yürüttüklerini anlatır.

Zaman damgası hizmeti verilirken, ZDİ dokümanı "ne" yapılacağını tanımlarken, ZDUE dokümanı bunun "nasıl" yapılacağını tanımlar.

Bu ZDUE dokümanı, "Zaman Damgası Otoriteleri İçin Politika Gerekleri" [RFC 3628], "Uzun Süreli Elektronik İmzalar için İmza Biçimi" [RFC 5126], "X.509 Açık Anahtar Altyapısı Zaman Damgası Protokolü" [RFC 3161], "Elektronik İmzalar ve Elektronik İmza Altyapıları: Zaman Damgası Otoriteleri için Politika Gerekleri" [ETSI

TS 102 023], Kamu Sertifikasyon Merkezi Sertifika İlkeleri ve Kamu Sertifikasyon Merkezi Sertifika Uygulama Esasları dokümanları referans alınarak hazırlanmıştır.

Bu ZDUE dokümanı ZDİ dokümanında belirtilen ilkelere uygun olarak hazırlanmıştır.

1.2 Doküman Tanımı

Doküman Adı: Zaman Damgası Uygulama Esasları

Doküman Sürüm Numarası: 1

Yayın Tarihi: 20 Ekim 2015

1.3 Sistem Bileşenleri

1.3.1 Zaman Damgası Hizmeti

Zaman damgası üreten, kullanıcılar tarafından zaman bilgisi kaynağı olarak güvenilen sistem bileşeni *zaman damgası hizmeti* olarak isimlendirilir.

Zaman damgası hizmeti tekil bir şekilde isimlendirilmelidir.

KAMU SM zaman damgası oluşturma sorumluluklarını taşır ve yükümlülüklerini yerine getirir.

Bu dokümanda anlatılan zaman damgası hizmeti *Kamu Sertifikasyon Merkezi Zaman Damgası Hizmeti* olarak isimlendirilmiştir.

1.3.2 Son Kullanıcılar

Zaman Damgası İstemcisi

ZDH'ye bağlanarak herhangi bir veri için zaman damgası isteminde bulunan sistem bileşenidir. . Zaman damgası istemcisi gerçek bir kişi olabileceği gibi tüzel kişi de olabilir.

Üçüncü Kişiler

ZDH tarafından yaratılmış bir zaman damgasının doğruluğuna güvenerek işlem yapan gerçek veya tüzel kişilerdir.

1.4 Uygulama Esaslarının Yönetimi

1.4.1 Doküman Değişim Yönetimi

ZDUE dokümanı KAMU SM tarafından yazılmıştır. KAMU SM gerekli gördüğü durumlarda ZDUE dokümanında değişiklik yapabilir.

1.4.2 İletişim Bilgileri

Bu ZDUE dokümanının uygulanması ve ilgili yönetim politikaları hakkındaki sorular TÜBİTAK BİLGEM Kamu SM'nin aşağıdaki erişim noktalarına yönlendirilebilir:

Adres: Kamu Sertifikasyon Merkezi TÜBİTAK Yerleşkesi, PK. 74, 41470 Gebze-KOCAELİ

Tel: (262) 648 18 18

Çağrı Merkezi: 444 5 576

Faks: (262) 648 18 00

E Posta: bilgi@kamusm.gov.tr

URL: http://www.kamusm.gov.tr

1.4.3 Yayın ve Duyuru Politikaları

KAMU SM, ZDUE dokümanını herkesin erişimine açık bulunan aşağıdaki internet adreslerinden yayımlar:

- http://www.kamusm.gov.tr/BilgiDeposu/KSM_ZDUE
- http://depo.kamusm.gov.tr/ilke/KSM_ZDUE

1.4.4 Zaman Damgası Uygulama Esasları Onay Prosedürleri

Bu ZDUE dokümanının ZDİ dokümanına uygunluğu, KAMU SM tarafından onaylanır.

1.5 Tanımlar ve Kısaltmalar

1.5.1 Tanımlar

Kamu Sertifikasyon Merkezi Sertifika İlkeleri dokümanında bulunan tanımlara ek olarak,

Koordine edilmiş evrensel zaman (Coordinated Universal Time (UTC)): ITU-R Recommendation TF.460-5'ye göre tanımlanmış saniye düzeyinde belirlilik sağlayan zaman birimi.

Zaman damgası: Bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı ve/veya kaydedildiği zamanın tespit edilmesi amacıyla, ESHS tarafından elektronik imzayla doğrulanan kayıt.

Zaman damgası hizmeti: Zaman damgası oluşturan hizmet servisi.

Zaman damgası ilkeleri: Zaman damgası hizmetinin oluşturduğu zaman damgasının kullanılabilirliğini tanımlayan, zaman damgası isteğinde bulunma, zaman damgası oluşturma ve zaman damgası doğrulama işlemleri sırasında uyulması gereken çalışma ilkelerini anlatan doküman.

Zaman damgası uygulama esasları: Zaman damgası hizmetinin zaman damgası oluştururken uyguladığı çalışma yöntemlerini anlatan doküman.

1.5.2 Kısaltmalar

Kamu Sertifikasyon Merkezi Sertifika İlkeleri dokümanında bulunan kısaltmalara ek olarak,

UTC: Koordine edilmiş evrensel zaman (Coordinated Universal Time)

ZDH: Zaman damgası hizmeti

ZDİ: Zaman Damgası İlkeleri

ZDUE: Zaman Damgası Uygulama Esasları

2 Genel Hükümler

2.1 Yükümlülükler

2.1.1 KAMU SM'nin Yükümlülükleri

ZDİ dokümanında anlatılanlara ek olarak,

- Zaman damgası içine güvenilir zaman bilgisi eklemekle,
- Her zaman damgası içine tekil bir tanımlayıcı sayı eklemekle,
- Zaman damgası istemcisinden uygun bir zaman damgası isteği aldığında zaman damgası üretmekle,
- Zaman damgası içine ilgili zaman damgası politikasının tanımlayıcı ismini eklemekle,
- Damgalanacak verinin özet değeri için zaman damgası üretmekle,
- Zaman damgası istemcisinden damgalanacak verinin kendisini istememekle,
- Özet değeri uzunluğunun tanımlı özet algoritmasının özet uzunluğuyla aynı olup olmadığını denetlemekle,
- Zaman damgası içine zaman damgası isteyen istek sahibinin kimliğiyle ilgili bilgiler eklememekle,
- Zaman damgası oluştururken yalnızca zaman damgası oluşturma amacıyla üretilmiş anahtarlar kullanmakla,
- Zaman damgası imza doğrulama verisini içeren sertifikaya sertifikanın kullanım amacını eklemekle yükümlüdür.

2.1.2 Zaman Damgası İstemcisi Yükümlülükleri

ZDİ dokümanında anlatılanlara ek olarak zaman damgasının doğruluğunu denetlerken

- Zaman damgasının istediği veri için üretilip üretilmediğini,
- Zaman damgası üzerindeki imzanın doğruluğunu,

- ZDH'nin sertifikasının geçerliliğini,

denetlemekle yükümlüdür.

2.1.3 Üçüncü Kişi Yükümlülükleri

Üçüncü kişiler bir zaman damgasının geçerliliğini doğrularken aşağıdaki denetimleri yapmakla yükümlüdür:

- ZDH'nin zaman damgası üzerindeki imzasının geçerli olduğunun denetimi,
- ZDH'nin imza oluşturma verisinin geçerliliğinin denetimi,
- Kullanıcı sözleşmesi, ilkeler ve uygulama esasları dokümanlarında tanımlı zaman damgası kullanımı üzerindeki kısıtlamaların denetimi.

2.2 Sorumluluklar

2.2.1 KAMU SM'nin Sorumlulukları

KAMU SM zaman damgası hizmetiyle ilgili olarak, 15 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza Kanunu, Telekomünikasyon Kurumu'nun yayımladığı Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik, Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de belirtilen şartları yerine getirmekten sorumludur.

2.2.2 Zaman Damgası İstemcisi Sorumlulukları

Zaman damgası istemcisi zaman damgalarını uygun geçerlilik denetimlerini yapmadan kullandığı takdirde doğabilecek zararlardan sorumludur.

Kamu SM tarafından istemciye verilen hesap bilgilerinin gizliliği istemcinin kendi sorumluluğundadır.

İstemcinin talebi üzerine, hesap bilgilerinde yapılacak değişikliklerden doğabilecek zararlardan istemci sorumludur.

2.2.3 Üçüncü Kişi Sorumlulukları

Üçüncü kişiler zaman damgalarını uygun geçerlilik denetimlerini yapmadan kullandığı takdirde doğabilecek zararlardan sorumludur.

3 İşlemsel Gerekler

Zaman damgası yönetimi aşağıdaki süreçlerden oluşmaktadır:

- Zaman damgası anlaşmasının yapılması
- Zaman damgası isteme
- Zaman damgası isteğinin işlenmesi
- Zaman damgasının gönderilmesi

3.1 Zaman Damgası

ZDH RFC 3161'de tanımlı zaman damgası protokolünü destekler.

ZDH verdiği zaman damgalarını imzalamak için BTK'nın yayınlamış olduğu tebliğ gereği 16 Eylül 2014 tarihinden itibaren SHA-256 özet algoritması ile RSA açık anahtarlı imzalama algoritmasını kullanır. Bu algoritmalar Kamu Sertifikasyon Merkezi Sertifika Uygulama Esasları'nda belirtilen ESHS'lerin kullandığı algoritmalardır.

KAMU SM zaman damgasının güvenli şekilde oluşturulmasını ve doğru zamanı içermesini sağlayacak tedbirleri alır.

Zaman damgası, damgalanan verinin özet değerini içerir. Özet değeri zaman damgası istemcisi tarafından ZDH'ye ulaştırılır.

ZDH zaman damgası eklenecek verinin kendisini istemciden talep etmez.

Zaman damgası yalnızca zaman damgası imzalama amacıyla yaratılmış bir imza oluşturma verisi kullanılarak imzalanır. Zaman damgası imzalama verisi başka işlemler için kullanılmaz.

Zaman damgası Kamu Sertifikasyon Merkezi Zaman Damgası İlkeleri tanımlayıcı numarasını içerir.

Her zaman damgasında zaman damgasına özel, tanımlayıcı bir numara bulunur.

Zaman damgası içindeki zaman bilgisi UTC ile uyumludur.

ZDH'nin kullandığı zaman değerleri UTC zamanına bu ZDUE dokümanında tanımlanan kesinlik derecesinde uyumludur.

Zaman damgası ZDH'nin kurulduğu ülke bilgisini içerir.

Zaman damgası ZDH tanımlama bilgisini (ismini) içerir.

3.1.1 UTC ile Zaman Birliği Sağlanması

ZDH, zaman bilgisini güvenilir ve yedekli (Atomik ve/veya GPS) kaynaklardan temin eder.

ZDH'nin zamanı UTC zamanına 1 (bir) saniyeyi aşmayacak kesinlikte uyar. ZDH bu kesinliği sağlayacak şekilde düzenli olarak denetimler ve ayarlamalar yapar.

ZDH saatinin izinsiz değiştirilmesini engellemek için her türlü tedbiri alır.

ZDH saatinin UTC zamanından belirtilen kesinlik düzeyinden fazla sapması durumunun uygun zamanda fark edilmesi, alarm üretilmesi ve düzeltilmesi için gerekli tedbirleri alır. Herhangi bir uygunsuzluk durumunda ilgili bileşenler bilgilendirilir.

3.2 Zaman Damgası Başvurusu

KAMU SM zaman damgası hizmetinden faydalanmak isteyen başvuru sahiplerinin başvurusunu alır. Başvuru sonrasında başvuru sahiplerine, zaman damgası isteği sırasında kullanacakları hesap bilgileri ulaştırılır.

Başvuru sahipleri zaman damgası başvurusu sırasında belirtilen kontörleri bitene kadar Kamu SM'den zaman damgası alırlar.

3.3 Zaman Damgası İsteme

İstemci, ZDH tarafından sağlanan yazılımı kullanarak kendisine verilen kullanıcı adı ve parola ile RFC 3161 de tanımlı olan zaman damgası protokolü yoluyla zaman damgası isteğinde bulunur.

3.4 Zaman Damgası İsteğinin İşlenmesi

ZDH tarafından, istemciden gelen zaman damgası isteğinin uygunluk denetimleri yapılır.

Bu denetimler kapsamında:

- Kullanıcı adı ve parolanın doğruluğu kontrol edilir.
- İstemcinin zaman damgası alabilmek için yeterli kontörünün olup olmadığına bakılır.
- Anlaşma şartlarının koyduğu diğer kısıtlamalar kontrol edilir.

Denetimler, isteğin anlaşma şartları içinde olup olmadığını anlama amaçlıdır. İstek anlaşma şartlarına uygunsa, zaman damgası üretilir.

3.5 Zaman Damgasının Gönderilmesi

ZDH, , oluşturduğu zaman damgasını RFC 3161'de tanımlı zaman damgası protokolü yoluyla istemciye gönderir.

İstemci, ZDH tarafından sağlanan yazılımı kullanarak zaman damgasını alır.

Gönderilen her zaman damgası anlaşma koşulları uyarınca ücretlendirilir.

4 Yönetim, İşlemsel ve Fiziksel Kontroller

KAMU SM zaman damgası hizmetinin verildiği servisler, Kamu Sertifikasyon Merkezi Sertifika Uygulama Esasları'nda belirtilen güvenlik, yönetimsel, işlemsel ve fiziksel şartlarını sağlar. Fiziksel güvenlik kontrolleri, prosedürsel kontroller, personel güvenlik kontrolleri Kamu Sertifikasyon Merkezi Uygulama Esasları'nda belirtilen ESHS ile aynıdır.

4.1 Denetim Kayıtları

KAMU SM zaman damgası hizmetinin işleyişi sırasında gerçekleştirilen ve denetimi yapılmak istenen işlerin kayıtlarını tutar. KAMU SM zaman damgası hizmetinin işleyişi ile ilgili her türlü gerekli bilgiyi Kamu Sertifikasyon Merkezi Zaman Damgası Uygulama Esasları'nda belirtilen süre boyunca saklar. Bu kayıtların temel amacı olası anlaşmazlıklar durumunda hukuksal delil oluşturmaktır.

Kayıtlarda kayıt zamanı ve kaydın oluşmasına sebep olan varlığın ismi bulunur.

4.1.1 Kaydedilen İşlemler

Şu işlemler kaydedilir:

- Zaman ayarlamaları
- ZDH saatinin sıradan ayarlamaları
- ZDH saatinin sıra dışı ayarlamaları
- Zaman ayarının kaybolmasıyla ilgili uyarılar, alarmlar
- ZDH sertifikalarının yaşam döngüsüyle ilgili işlemler
- Sertifika başvurusu
- Sertifikanın kullanıma alınması
- Sertifika yenileme
- Sertifika güncelleme
- Sertifika iptal başvurusu
- ZDH anahtarlarının yaşam döngüsüyle ilgili işlemler
    - Anahtar üretimi
    - Anahtar yedekleme
    - Anahtar dağıtımı
    - Anahtar saklama
    - Anahtar arşivleme
    - Anahtar yok etme
- Kriptografik modül yaşam döngüsü işlemleri
- Güvenlikle ilgili diğer işlemler
- Sisteme erişim denemeleri (başarılı-başarısız)

- Çalışanlar tarafından gerçekleştirilen güvenlik sistemi işlemleri
- Güvenli tutulması gereken hassas dosyaların okunması, yazılması ve değiştirilmesi
- Güvenlik profili değişiklikleri
- Sistemin çökmesi, donanım hataları ve diğer bozukluklar
- Güvenlik duvarı (firewall) ve yönlendirici (router) işlemleri
- KAMU SM'ye ziyaretçi giriş ve çıkışı

Bunların dışında zaman damgası ile ilgili olarak şunların kayıtları tutulur:

- Zaman Damgası İstemci Anlaşmaları
- Oluşturulan ve gönderilen zaman damgaları
- Sisteme tanımlı kullanıcılardan gelen başarısız zaman damgası istekleri

Sisteme tanımlı olmayan varlıklardan gelen başarısız zaman damgası istekleri kaydedilmez.

4.1.2 Kayıtların İncelenme Sıklığı

Tutulan kayıtlar düzgün zaman aralıklarıyla incelenir. İncelemeler güvenlik açıklarını uygun sürede yakalayabilecek sıklıkta yapılır. Denetimler sırasında gerekli görüldüğü takdirde bu kayıtlar görevliler tarafından incelenir. Kayıtlar, hukuksal anlaşmazlıklara çözüm oluşturmak amacıyla gerekli görüldüğünde yetkili makamlarca incelenir.

4.1.3 Kayıtların Saklanma Süresi

Kayıtlar izinsiz izlemeyi, değiştirmeyi ve silmeyi engelleyecek şekilde elektronik ve fiziksel olarak güvenli bir şekilde ve mevzuat gereği 20 yıl süreyle saklanır. KAMU SM zaman damgası hizmeti ile ilgili işlemlerin kayıtlarının bütünlüğünü ve gizliliğini korur. Zaman damgası sistemi kullanıcıları hakkındaki özel bilgiler gizliliği sağlanarak korunur.

Elektronik olarak saklanan ve sistemin işleyişi açısından kritik olan kayıtlar işlemi yapan personel tarafından elektronik imza ile imzalanarak saklanır. Böylece kritik kayıtlarda oluşabilecek her değişiklik sistem tarafından fark edilir.

Kritik bilgiler gerektiğinde şifreli olarak saklanır.

Yetkisi olmayan kişiler elektronik kayıtların bulunduğu ortamlara erişemezler.

Kağıt üzerindeki kayıtlar sadece yetkililerin girme izni bulunan kilitli odalarda bulunur.

4.1.4 Kayıtların Korunması

Kayıtlar izinsiz izlenmeyi, değiştirmeyi ve silinmeyi engelleyecek şekilde elektronik ve fiziksel olarak güvenli tutulur. KAMU SM zaman damgası hizmeti ile ilgili işlemlerin kayıtlarının bütünlüğünü ve gizliliğini korur. Zaman damgası sistemi kullanıcıları hakkındaki özel bilgiler gizliliği sağlanarak korunur.

4.1.5 Kayıtların Yedeklenmesi

Sistemin işleyişi ile ilgili elektronik kayıtlar en azından her gün, sistemin yoğun olarak kullanılmadığı bir saatte yedeklenir. Herhangi bir arıza durumunda sistemin son durumuna dönebilmek için alınan en son kayıt yedekleri sisteme yüklenir.

4.1.6 Kayıtların Toplanması

Kayıtlar elektronik olarak veya kağıt ortamda toplanır.

4.2 Kayıt Arşivleme

Tutulan kayıtlar Kamu Sertifikasyon Merkezi Sertifika Uygulama Esasları'nda belirtilen şekilde arşivlenir.

5 Teknik Güvenlik Kontrolleri

Zaman damgası hizmeti veren sisteme uygulanan teknik güvenlik kontrolleri Kamu Sertifikasyon Merkezi Sertifika İlkeleri dokümanında belirtilen güvenlik şartlarını sağlar ve Kamu Sertifikasyon Merkezi Sertifika Uygulama Esasları dokümanı temel alınarak oluşturulmuştur.

5.1 ZDH Anahtar Çifti Üretimi ve Kurulumu

ZDH'ye ait imzalama anahtar çifti Kamu Sertifikasyon Merkezi Sertifika İlkeleri dokümanında belirtilen güvenlik şartlarını sağlayacak şekilde ve Kamu Sertifikasyon Merkezi Sertifika Uygulama Esasları dokümanı temel alınarak oluşturulur.

5.1.1 ZDH Anahtar Çifti Üretimi

ZDH'ye ait anahtar çiftleri (imza oluşturma ve doğrulama verileri) oluşturulurken aşağıdaki şartlara uyulur:

- Anahtar çiftleri yetkisi olmayan personelin giremeyeceği gizli odada oluşturulur.
- Anahtar çiftleri ağ ortamına kapalı ortamlarda, yasayla belirlenmiş güvenlik seviyelerini sağlayan yazılım veya donanım aracı içinde üretilir.
- Anahtar çiftlerinden imza oluşturma verisi güvenli kriptografik donanım aracı içinde saklanır ve bu ortamdan yedekleme amacı dışında dışarıya çıkarılmaz.
- Üretilen anahtar çiftinin gerekli güvenlik şartlarını sağlaması için uygun üretim ve test yöntemleri kullanılır.
- Üretilen anahtar çifti yasayla belirlenen ve KAMU SM'nin kullandığı en kısa anahtar boylarına ve algoritma şartlarına uyar.

5.1.2 ZDH Sertifikalarına Erişim Sağlanması

ZDH'ye ait sertifikalar internet ortamında ilgili tarafların erişimine hazır bulundurulur. Ayrıca, sertifikaların özet değeri ve özet algoritması internet üzerinden yayımlanır. Üçüncü kişilar sertifika özet değerini yayımlanan özet değeriyle kıyaslayarak sertifikanın güvenilirliğine karar verirler.

5.1.3 ZDH Anahtar Uzunlukları

Belirlenen anahtar uzunluğu Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de belirtilen şartları sağlar.

ZDH'nin zaman damgası oluşturmak için kullandığı RSA imza oluşturma anahtarının boyu 2048-bittir.

5.1.4 ZDH Anahtar Kullanım Amaçları

ZDH imza oluşturma verisi zaman damgası oluşturmak amacıyla, ilgili imza doğrulama verisi ise zaman damgasının doğruluğunu denetleme amacıyla kullanılır.

5.2 ZDH İmza Oluşturma Verisinin Korunması

5.2.1 Kriptografik Modül Standartları

ZDH'ye ait imza oluşturma verisinin üretildiği veya saklandığı kriptografik modül Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de belirtilen güvenlik standartlarını sağlar.

Kriptografik modül aşağıda belirlenen güvenlik işlevlerine sahiptir:

- Modüle erişim yetkisi birden fazla kişinin kontrolünde olacak şekilde tanımlanabilir.
- Modüle izinsiz erişim ve kullanım ile tahrifata yol açabilecek her türlü tehlikeye karşı fiziksel önlem alınmıştır.
- Modüle yetkisiz erişime teşebbüs edilmesi durumunda içerideki veri silinir.

5.2.2 ZDH İmza Oluşturma Verisine Erişim Denetimi

ZDH'nin imza oluşturma verisine erişim birden fazla yetkili çalışanın ortak denetimi altındadır. İmza oluşturma verisi işlemleri için yeterli sayıda yetkili personelin hazır bulunması ve elektronik olarak kimliklerinin ve yetkilerinin doğrulanması gerekir.

5.2.3 ZDH İmza Oluşturma Verisinin Saklanması

ZDH'ye ait imza oluşturma verileri yetkisiz kişilerin erişimine kapalı, fiziksel ve elektronik olarak güvenli kriptografik modül içinde şifreli olarak tutulur. İmza oluşturma verisinin kriptografik modül dışına çıkması engellenir.

5.2.4 ZDH İmza Oluşturma Verisinin Yedeklenmesi

ZDH'ye ait imza oluşturma verileri yetkisiz kişilerin erişimine kapalı, fiziksel ve elektronik olarak güvenli kriptografik donanım cihazı içinde yedeklenir. İmza oluşturma verisinin yedeklenmesi işlemi birden fazla yetkili çalışanın ortak denetimi altındadır.

5.2.5 ZDH İmza Oluşturma Verisinin Arşivlenmesi

ZDH'ye ait imza oluşturma verileri arşivlenmez. Kullanım süreleri sonunda geri dönüşsüz şekilde silinir.

5.2.6 ZDH 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. Kriptografik modül dışında üretilen imza oluşturma verisi yetkili birden fazla personelin denetiminde modüle yüklenir.

5.2.7 ZDH İmza Oluşturma Verisine Erişim

ZDH'ye ait imza oluşturma verisi güvenli algoritma ve yöntemlerle şifreli olarak güvenli kriptografik modül içinde saklanır. İmza oluşturma verisinin erişime açılması ve kullanılır duruma getirilmesi yetkili birden fazla çalışanın ortak denetimi altındadır.

5.2.8 ZDH İmza Oluşturma Verisine Erişimin Kesilmesi

ZDH'ye ait imza oluşturma verisi imzalama için kullanıldıktan sonra erişime yeniden açılıncaya kadar erişime kapalı tutulur.

5.2.9 ZDH İmza Oluşturma Verisinin Yok Edilmesi

ZDH'ye ait imza oluşturma verisi kullanım süresinin dolmasının ardından, bulunduğu sistemden uygun yöntemlerle geri dönüşsüz şekilde silinir. İmza oluşturma verisinin silinmesi birden fazla yetkili çalışanın ortak denetimi altındadır.

5.3 ZDH Anahtar Çifti Yönetimiyle İlgili Diğer Konular

5.3.1 ZDH İmza Doğrulama Verisinin Arşivlenmesi

ZDH'ye ait imza doğrulama verilerinin içinde bulunduğu sertifikalar yasa ve ilgili yönetmelikte belirtilen süre boyunca arşivlenir. Arşivde bulunduğu süre boyunca sertifikaların bütünlüğünün sağlanması için gereken her türlü önlem alınır.

5.3.2 ZDH İmza Oluşturma ve Doğrulama Verilerinin Kullanım Süreleri

ZDH'ye ait imza oluşturma ve doğrulama anahtar çiftinin kullanım süresi ilgili yönetmelikte belirtilen sürelere uyar ve KAMU SM tarafından gerekli güvenliği sağlayacak şekilde seçilir.

5.3.3 ZDH İmza Oluşturma ve Doğrulama Verilerinin Yenilenmesi

ZDH'nin sertifikasının kullanım süresi anahtar çiftinin güvenli kullanım süresinden uzun olamaz.

ZDH zaman damgası imzalama anahtar çiftini kullanım süresi dolmadan yenileriyle değiştirecek önlemleri alır.

ZDH kullanım süresi dolduğunda zaman damgası imzalamak için kullanılan imza oluşturma verilerinin geri dönüşsüz şekilde silindiğinden emin olur.

5.4 Erişim Denetim Verileri

Zaman damgası hizmeti ile ilgili erişim denetim verileri Kamu Sertifikasyon Merkezi Sertifika İlkeleri dokümanında tanımlanan erişim denetim verileri güvenlik şartlarını sağlar.

5.5 Bilgisayar Güvenliği Denetimleri

Zaman damgası hizmetine ait bilgisayar sistemlerine Kamu Sertifikasyon Merkezi Sertifika İlkeleri ve Uygulama Esasları dokümanlarında belirtilen güvenlik denetimleri uygulanır.

5.6 Yaşam Döngüsü Güvenlik Denetimleri

Zaman damgası hizmeti ile ilgili sistemlere, yaşam döngüsü boyunca, Kamu Sertifikasyon Merkezi Sertifika İlkeleri ve Uygulama Esasları dokümanlarında belirtilen güvenlik denetimleri uygulanır.

5.7 Ağ Güvenliği Denetimleri

Zaman damgası hizmeti sistemine Kamu Sertifikasyon Merkezi Sertifika İlkeleri ve Uygulama Esasları dokümanlarında belirtilen ağ güvenliği denetimleri uygulanır.

6 Uygunluk Denetimleri

Zaman damgası hizmeti sistemine Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de ve Kamu Sertifikasyon Merkezi Sertifika İlkeleri dokümanında belirtilen uygunluk denetimleri uygulanır.

7 Diğer İşler ve Hukuksal Meseleler

Kamu Sertifikasyon Merkezi Sertifika Uygulama Esasları'nda belirtildiği gibidir.

7.1 Ücretlendirme

KAMU SM ürettiği her zaman damgası için zaman damgası istemcisinden ücret talep eder. Ücret bilgisi ve ücretin ödenme şekli zaman damgası istemcisinin başvuru sırasında kabul etmesi gereken Zaman Damgası İstemci Anlaşması'nda tanımlanır.

Zaman Damgası İstemci Anlaşması ile istemciye anlaşmada belirtilen sayıda zaman damgası alma hakkı (kontör) tanınır. Bu hizmet için zaman kısıtlaması uygulanabilir. Anlaşmada kuruma tanınan kontör için talep edilen ücret belirtilir. Kuruma gönderilen her zaman damgası için kontör düşürülerek ücretlendirme yapılır. Zaman damgasının ücretlendirilmesi ile ilgili ayrıntılar kurumla yapılan sözleşmelerde belirtilir.

8 Referanslar

[RFC 5126] Electronic Signature Formats for Long Term Electronic Signatures, "Uzun Süreli Elektronik İmzalar için İmza Biçimi"

[RFC 3161] Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), "X.509 Açık Anahtar Altyapısı Zaman Damgası Protokolü"

[RFC 3628] Policy Requirements for Time-Stamping Authorities (TSAs), "Zaman Damgası Otoriteleri İçin Politika Gerekleri"

[ETSI TS 102 023] Electronic Signatures and Infrastructures (ESI); Policy Requirements for Time-Stamping Authorities, "Zaman Damgası Otoriteleri İçin Politika Gerekleri".

[ETSI TS 101 861] Time Stamping Profile, "Zaman Damgası Profili".