

TASNİF DIŐI



**TÜBİTAK BİLGEM
KAMU SERTİFİKASYON MERKEZİ**

ZAMAN DAMGASI UYGULAMA ESASLARI

Doküman Kodu

YON.01.02

Revizyon No

04

Revizyon Tarihi

11.12.2024

TASNİF DIŐI

REVİZYON GEÇMİŐİ		
Revizyon No	Revizyon Nedeni	Revizyon Tarihi
00	İlk Çıkış.	12.08.2005
01	Tanımlar kısmında ve doküman genelinde gramer düzenlemeleri yapıldı.	20.10.2015
02	Doküman genelinde düzenleme yapıldı, ücretlendirme kısmı güncellendi. Doküman kodu ve şablonu değıştirildi. Dokümanın eski revizyonları Doküman Yönetim Sistemi'nde YONG-001-008 kodu ile yer almaktadır.	21.06.2018
03	Genel kontrol yapıldı. 1.4.2. İletişim Bilgileri, 1.5.1. Tanımlar, 1.5.2. Kısaltmalar, 3.2. Zaman Damgası Başvurusu, 3.3. Zaman Damgası İsteme ve 3.5. Zaman Damgasının Gönderilmesi alanlarında güncellemeler yapılmıştır.	06.10.2022
04	Doküman genelinde düzenleme yapıldı. Güvenilir roller düzenlendi. Görevlerin ayrılmasını gerektiren roller, kaydedilen işlemler güncellendi.	11.12.2024

İÇİNDEKİLER

1. GİRİŞ.....	6
1.1. Genel Bakış	6
1.2. Doküman Tanımı.....	7
1.3. Sistem Bileşenleri.....	7
1.3.1. Zaman Damgası Hizmeti	7
1.3.2. Son Kullanıcılar	7
1.4. Uygulama Esaslarının Yönetimi.....	7
1.4.1. Doküman Değişim Yönetimi	7
1.4.2. İletişim Bilgileri	8
1.4.3. Yayın ve Duyuru Politikaları	8
1.4.4. Zaman Damgası Uygulama Esasları Onay Prosedürleri	8
1.5. Tanımlar ve Kısaltmalar	8
1.5.1. Tanımlar	8
1.5.2. Kısaltmalar	9
2. GENEL HÜKÜMLER	10
2.1. Yükümlülükler.....	10
2.1.1. Kamu SM'nin Yükümlülükleri	10
2.1.2. Zaman Damgası İstemcisi Yükümlülükleri	10
2.1.3. Üçüncü Kişi Yükümlülükleri	10
2.2. Sorumluluklar	11
2.2.1. Kamu SM'nin Sorumlulukları	11
2.2.2. Zaman Damgası İstemcisi Sorumlulukları	11
2.2.3. Üçüncü Kişi Sorumlulukları.....	11
3. İŞLEMSEL GEREKLER	11
3.1. Zaman Damgası.....	11
3.1.1. UTC ile Zaman Birliği Sağlanması	12
3.2. Zaman Damgası Başvurusu	12
3.3. Zaman Damgası İsteme	13
3.4. Zaman Damgası İsteğinin İşlenmesi	13
3.5. Zaman Damgasının Gönderilmesi	13
4. YÖNETİM, İŞLEMSEL VE FİZİKSEL KONTROLLER.....	13
4.1. Fiziksel Güvenlik Denetimleri.....	13
4.1.1. Tesis Yeri ve İnşaatı.....	13
4.1.2. Fiziksel Erişim	14
4.1.3. Güç Kaynağı ve Havalandırma	14
4.1.4. Su Baskınları.....	14
4.1.5. Yangın Önleme ve Korunma	14
4.1.6. Saklama ve Yedekleme Ortamlarının Korunması	14
4.1.7. Atıkların Yok Edilmesi	15
4.1.8. Farklı Mekanlarda Yedekleme	15
4.2. Prosedürel Kontroller	15
4.2.1. Güvenilir Roller	15

ZAMAN DAMGASI UYGULAMA ESASLARI

4.2.2.	Her İşlem İçin Gereken Kişi Sayısı.....	15
4.2.3.	Kimlik Doğrulama ve Yetkilendirme.....	16
4.2.4.	Görevlerin Ayrılmasını Gerektiren Roller	16
4.3.	Personel Güvenlik Kontrolleri	16
4.3.1.	Kişisel Geçmiş, Deneyim ve Nitelik Gerekleri	16
4.3.2.	Geçmiş Araştırması	16
4.3.3.	Eğitim Gerekleri	16
4.3.4.	Sürekli Eğitim Gerekleri ve Sıklığı	17
4.3.5.	Görev Değişim Sıklığı ve Sırası	17
4.3.6.	Yetkisiz Eylemlerin Cezalandırılması	17
4.3.7.	Anlaşmalı Personel Gereksinimleri	17
4.3.8.	Sağlanan Dokümantasyon	17
4.4.	Denetim Kayıtları	17
4.4.1.	Kaydedilen İşlemler	17
4.4.2.	Kayıtların İncelenme Sıklığı	18
4.4.3.	Kayıtların Saklanma Süresi	18
4.4.4.	Kayıtların Korunması	19
4.4.5.	Kayıtların Yedeklenmesi	19
4.4.6.	Kayıtların Toplanması	19
4.5.	Kayıt Arşivleme	19
4.5.1.	Arşivlenen Kayıt Bilgileri	19
4.5.2.	Arşivlerin Tutulma Süresi	20
4.5.3.	Arşivlerin Korunması	20
4.5.4.	Arşivlerin Yedeklenmesi	20
4.5.5.	Kayıtların Zaman Damgası Gereksinimleri	20
4.5.6.	Arşivlerin Toplanması	20
4.5.7.	Arşiv Bilgilerinin Elde Edilme ve Doğrulanma Metodu.....	20
5.	TEKNİK GÜVENLİK KONTROLLERİ	20
5.1.	ZDH Anahtar Çifti Üretimi ve Kurulumu	20
5.1.1.	ZDH Anahtar Çifti Üretimi	20
5.1.2.	ZDH Sertifikalarına Erişim Sağlanması	21
5.1.3.	ZDH Anahtar Uzunlukları	21
5.1.4.	ZDH Anahtar Kullanım Amaçları.....	21
5.2.	ZDH İmza Oluşturma Verisinin Korunması	21
5.2.1.	Kriptografik Modül Standartları	21
5.2.2.	ZDH İmza Oluşturma Verisine Erişim Denetimi	22
5.2.3.	ZDH İmza Oluşturma Verisinin Saklanması	22
5.2.4.	ZDH İmza Oluşturma Verisinin Yedeklenmesi	22
5.2.5.	ZDH İmza Oluşturma Verisinin Arşivlenmesi	22
5.2.6.	ZDH İmza Oluşturma Verisinin Kriptografik Modüle Yüklenmesi	22
5.2.7.	ZDH İmza Oluşturma Verisine Erişim	22
5.2.8.	ZDH İmza Oluşturma Verisine Erişimin Kesilmesi	22
5.2.9.	ZDH İmza Oluşturma Verisinin Yok Edilmesi	23
5.3.	ZDH Anahtar Çifti Yönetimiyle İlgili Diğer Konular	23
5.3.1.	ZDH İmza Doğrulama Verisinin Arşivlenmesi	23

ZAMAN DAMGASI UYGULAMA ESASLARI

5.3.2.	ZDH İmza Oluřturma ve Doğrulama Verilerinin Kullanım Süreleri	23
5.3.3.	ZDH İmza Oluřturma ve Doğrulama Verilerinin Yenilenmesi	23
5.4.	Eriřim Denetim Verileri	23
5.4.1.	Eriřim Denetim Verilerinin Oluřturulması	23
5.4.2.	Eriřim Denetim Verilerinin Korunması.....	24
5.4.3.	Eriřim Denetim Verileri İle İlgili Diğer Konular	24
5.5.	Bilgisayar Güvenlięi Denetimleri	24
5.5.1.	Bilgisayar Güvenlięi İle İlgili Teknik Gerekler	24
5.5.2.	Bilgisayar Sisteminin Sağladığı Güvenlik Seviyesi.....	24
5.6.	Yařam Döngüsü Teknik Denetimleri.....	24
5.6.1.	Sistem Geliřtirme Denetimleri	24
5.6.2.	Güvenlik Yönetimi Denetimleri	25
5.6.3.	Yařam Döngüsü Güvenlik Denetimleri.....	25
5.7.	Aę Güvenlięi Denetimleri.....	25
6.	UYGUNLUK DENETİMLERİ.....	25
6.1.	Uygunluk Denetiminin Sıklığı	26
6.2.	Denetçinin Nitelikleri	26
6.3.	Denetçinin Denetlenen Tarafla Olan İliřkisi	26
6.4.	Denetimin Kapsamı	26
6.5.	Yetersizlięin Tespiti Durumunda Yapılacaklar	26
6.6.	Sonucun Bildirilmesi.....	27
7.	DİĞER İŐLER VE HUKUKSAL MESELELER	27
7.1.	Ücretlendirme.....	27
7.1.1.	Zaman Damgası Ücretlendirme	27
7.1.2.	Sertifika Eriřim Ücreti	27
7.1.3.	İptal Durum Kaydına Eriřim Ücreti.....	27
7.1.4.	Dięer Servis Ücretleri	27
7.1.5.	İade Ücreti.....	27
8.	REFERANSLAR	28

1. Giriő

Bu doküman, Türkiye Bilimsel ve Teknolojik Arařtırma Kurumu'na (TÜBİTAK) baėlı Biliőim ve Bilgi Güvenliėi İleri Teknolojiler Arařtırma Merkezi (BİLGEM) Başkanlıėı bünyesinde yer alan Kamu Sertifikasyon Merkezi'nin (Kamu SM) zaman damgası hizmetinin iőleyiőı sırasında uyguladıėı 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 yayımladıėı Elektronik İmza Kanunu'nun Uygulanmasına İliőkin Usul ve Esaslar Hakkında Yönetmelik, Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İliőkin Tebliė'de tanımlandıėı őekliyle Elektronik Sertifika Hizmet Sağlayıcısı (ESHS) iőlevlerini yerine getirir. Kamu SM yapısı içinde kullanıcılara güvenilir zaman kaynaėı olarak hizmet veren Zaman Damgası Hizmeti (ZDH) mevcuttur.

Bu doküman 15 Ocak 2004 tarih ve 5070 Sayılı Elektronik İmza Kanunu, Telekomünikasyon Kurumu'nun yayımladıėı Elektronik İmza Kanunu'nun Uygulanmasına İliőkin Usul ve Esaslar Hakkında Yönetmelik, Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İliőkin Tebliė esas alınarak hazırlanmıőtır.

1.1. Genel Bakıő

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

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

Kamu SM bünyesindeki zaman damgası hizmetleri bu dokümanda tanımlanan uygulama esasları uyarınca çalıőır. Bu ZDUE dokümanı ZDİ dokümanında belirtilen ilkelere uygun olarak hazırlanmıőtır. Bu doküman ZDH'nin ve sistem bileőenlerinin tanımlı çalıőma ilkeleri doėrultusunda iőleyiőlerini nasıl yürüttüklerini anlatır.

Zaman damgası hizmeti verilirken, Zaman Damgası İlkeleri (ZDİ) dokümanı "ne" yapılacaėını tanımlarken, Zaman Damgası Uygulama Esasları (ZDUE) dokümanı bunun "nasıl" yapılacaėını 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" [IETF - Internet X.509 Public Key Infrastructure Time-Stamp Protocol (RFC 3161)], "Elektronik İmzalar ve Elektronik İmza Altyapıları: Zaman Damgası Otoriteleri için Politika Gerekleri" [ETSI TS 102 023], Nitelikli Elektronik Sertifika İlkeleri ve Nitelikli Elektronik Sertifika Uygulama Esasları dokümanları referans alınarak hazırlanmıőtır.

Bu ZDUE dokümanı ZDİ dokümanında belirtilen ilkelere uygun olarak hazırlanmıőtır.

1.2. Doküman Tanımı

Doküman Adı: Zaman Damgası Uygulama Esasları

Doküman Sürüm Numarası: 4

Yayın Tarihi: 11.12.2024

Nesne Tanımlama Numarası: 2.16.792.1.2.1.1.5.7.3.1

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 yükümlölüklerini yerine getirir.

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

1.3.2. Son Kullanıcılar

1.3.2.1. Zaman Damgası İstemcisi

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

1.3.2.2. 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 Değışim Yönetimi

ZDUE dokümanı Kamu SM tarafından yazılmıştır. Kamu SM gerekli gördüğü durumlarda ZDUE dokümanında değışiklik yapabilir.

1.4.2. İletişim Bilgileri

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

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

Tel : (262) 648 18 18

Faks : (262) 648 18 00

E-Posta : bilgi@kamusm.gov.tr

Web : <https://kamusm.bilgem.tubitak.gov.tr>

1.4.3. Yayın ve Duyuru Politikaları

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

- https://kamusm.bilgem.tubitak.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

Anahtar Çifti: Özel anahtar ve onunla ilişkili olan açık anahtar çifti.

Bilgi Deposu: Sertifikaların, sertifika iptal durum kayıtlarının ve diğer sertifika işlemleri ile ilgili bilgilerin yayımlandığı web sunucular, izin sunucular gibi veri saklama ortamları.

Eş Güdümlü Evrensel Zaman (Coordinated Universal Time (UTC)): ITU-R Recommendation TF.460-5'ye göre tanımlanmış saniye düzeyinde belirlilik sağlayan zaman birimi.

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

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 kayıt.

ZAMAN DAMGASI UYGULAMA ESASLARI

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 veriler.

Kamu Sertifikasyon Merkezi (Kamu SM): Türkiye Bilimsel ve Teknolojik Araştırma Kurumu'na (TÜBİTAK) bağlı Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM) bünyesinde, elektronik sertifika hizmeti sağlamak üzere oluşturulan birim.

Üçüncü Kişiler: Sertifikalara güvenerek işlem yapan gerçek veya tüzel kişiler.

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 İlkeleri: 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.

Zaman Damgası Yetkilisi: Kurumsal başvurularda kurumu temsil eden kişi.

1.5.2. Kısaltmalar

BGYS: Bilgi Güvenliği Yönetim Sistemi

BTK: Bilgi Teknolojileri ve İletişim Kurumu

CWA (CEN Workshop Agreement): CEN Çalıştay Kararı

ESHS: Elektronik Sertifika Hizmet Sağlayıcısı

ETSI (European Telecommunications Standards Institute): Avrupa Telekomünikasyon Standartları Enstitüsü

ETSI TS (ETSI Technical Specification): 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 Commission): Uluslararası Standardizasyon Teşkilatı / Uluslararası Elektroteknik Komisyonu

ITU (International Telecommunication Union): Uluslararası Telekomünikasyon Birliği

Kamu SM: Kamu Sertifikasyon Merkezi

UTC (Coordinated Universal Time): Eş Güdümlü Evrensel Zaman

ZDH: Zaman Damgası Hizmeti

ZDİ: Zaman Damgası İlkeleri

ZDUE: Zaman Damgası Uygulama Esasları

2. Genel Hükümler

2.1. Yükümlölükler

2.1.1. Kamu SM'nin Yükümlölükleri

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 isteęi 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 uzunluęunun tanımlı özet algoritmasının özet uzunluęuyla aynı olup olmadığını denetlemekle,
- Zaman damgası içine zaman damgası isteyen istek sahibinin kimlięiyle 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 Yükümlölükleri

ZDİ dokümanında anlatılanlara ek olarak zaman damgasının doğruluęunu denetlerken

- Zaman damgasının istedięi veri için üretilip üretilmedięini,
- Zaman damgası üzerindeki imzanın doğruluęunu,
- ZDH'nin sertifikasının geçerlilięini,

denetlemekle yükümlüdür.

2.1.3.Üçüncü Kiři Yükümlölükleri

Üçüncü kişiler bir zaman damgasının geçerlilięini doğrularken aőağıdaki denetimleri yapmakla yükümlüdür:

ZAMAN DAMGASI UYGULAMA ESASLARI

- 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.

ZAMAN DAMGASI UYGULAMA ESASLARI

ZDH verdiđi zaman damgalarını imzalamak için BTK'nın yayımlamış olduđu Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de belirtilen algoritmaları kullanır.

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 kurulduđu ülke bilgisini içerir.

Zaman damgası ZDH tanımlama bilgisini (ismini) içerir.

3.1.1. UTC ile Zaman Birliđi 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 kesinliđi sağlayacak şekilde düzenli olarak denetimler ve ayarlamalar yapar.

ZDH saatinin izinsiz deđiştirilmesini 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 başvurusu, bireysel ya da kurumsal olarak <https://zdportal.kamusm.gov.tr/> adresinden alınır. Başvuru işlemlerinin tamamlanması sonrasında başvuru sahiplerine, zaman damgası isteđi sırasında kullanacakları hesap bilgileri ulaştırılır. Kurumsal başvurularda kurumu temsil eden Zaman Damgası Yetkilisi, bireysel başvurularda ise başvuru sahibinin kendisi zaman damgası hesabı üzerinde kontör talep etme, hesabı bir başkasına devretme gibi yetkilere sahip olur.

Başvuru sahipleri, zaman damgası hesaplarındaki kontör bitene kadar Kamu SM'den zaman damgası alabilirler.

3.3. Zaman Damgası İsteme

İstemci, ZDH tarafından 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:

1. Kullanıcı adı ve parolanın doğruluğı kontrol edilir.
2. İstemcinin zaman damgası alabilmek için yeterli kontörünün olup olmadığına bakılır.
3. Anlaşma şartlarının koyduğu diğer kısıtlamalar kontrol edilir.

Denetimler, isteğın 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.

Gönderilen her zaman damgası anlaşma koşulları uyarınca ücretlendirilir.

4. Yönetim, İşlemsel ve Fiziksel Kontroller

Bu bölümde Kamu SM tarafından yerine getirilmesi gereken teknik olmayan güvenlik kontrolleri anlatılmıştır.

4.1. Fiziksel Güvenlik Denetimleri

Kamu SM sisteminin çalıştığı cihazların bulunduğu binalar ve odalar, giriş ve çıkışların kontrol edildiğı, yetkisiz kişilerin girişini engelleyen güvenlik önlemleri ile donatılmıştır. Güvenli alanlara erişimlerin kaydı tutulmaktadır.

4.1.1. Tesis Yeri ve İnşaatı

Kamu SM operasyonları Gebze ve Ankara'daki tesislerde yürütölmektedir. Kamu SM sisteminin çalıştığı binanın bulunduğu Gebze tesisi, yerleşim merkezinden uzak, yangın, su baskını, deprem, yıldırım ve hava kirliliğinden en az etkilenecek, giriş ve çıkışların kontrol edildiğı bir bölgedir. Alanlara ve binalara erişim, fiziki güvenlik, video izleme ve kimlik doğrulama olmak üzere çoklu güvenlik ile korunmaktadır. Ankara tesisi farklı seviyelerde fiziksel kontrolü bulunan bir alandır. Bina, yüksek güvenlik gerektiren işlerin yapılmasına imkân sağlayan yapıdadır. Bina, esnek (çelik yapı) ve sert (çelik çatıyla desteklenmiş beton yapı veya desteklenmiş beton yapı) yapı şartlarını sağlamaktadır.

Kamu SM'nin kurulduđu yer ve binada güç birimleri, haberleşme üniteleri, yedekli iklimlendirme üniteleri, havalandırıcılar, yangın söndürücü sistemler mevcut olup, deprem, su ve afetlere karşı gerekli tedbirler alınmıştır. Yetkisiz personel ve kayıtsız ziyaretçiler bu hassas alanlara giremez.

4.1.2.Fiziksel Erişim

Kamu SM yazılım ve donanım modülleri ile arşivlere erişim denetim altındadır. Binaya girişler güvenlik görevlilerinin kontrolü altında, gelişmiş erişim kontrol cihazlarıyla sağlanmaktadır.

Bina içinde Kamu SM sistemine ait yazılım ve donanım araçlarının bulunduğu, elektronik veya kağıt ortamdaki bilgilerin tutulduğu, sistemin işletildiği ve yönetildiği odalara erişim gelişmiş erişim kontrol cihazlarıyla yapılmaktadır. Yetkisi olmayan kişiler sistemin kurulu olduğu odalara giriş yapamamaktadır. Yetkisiz kişilerin donanım bakımı veya bunun gibi sıra dışı bir amaçla sistemin kurulu olduğu odalara girişleri özel erişim talimatları uyarınca düzenlenir.

4.1.3.Güç Kaynağı ve Havalandırma

Aşağıdaki güç kaynakları Kamu SM işlevlerinin yerine getirilmesi ve sürekliliğin sağlanması için kullanılmaktadır:

- Güç alma ve devşirme (transformatör) birimleri
- Dağıtım paneli
- Trafo
- UPS
- Kuru akü
- Acil jeneratör

Bina gerekli havalandırma sistemi ile donatılmıştır.

4.1.4.Su Baskınları

Kamu SM işlevlerinin yerine getirildiği ortamlarda su baskınlarından en az zarar görecekt şekilde önlemler alınmıştır.

4.1.5.Yangın Önleme ve Korunma

Kamu SM işlevlerinin yerine getirildiği ortamlarda yangını önleyici ve olası yangınlarda zararı en aza indirecek önlemler alınmıştır.

4.1.6.Saklama ve Yedekleme Ortamlarının Korunması

Kullanılan veri saklama ortamları (disk, CD, kağıt vs.) bozulmaya, yıpranmaya karşı fiziksel ve elektronik olarak korunur.

4.1.7. Atıkların Yok Edilmesi

Hassas bilgilerin bulunduđu ve artık kullanılmayan elektronik veya kâğıt ortamda tutulan bilgiler/cihazlar imha prosedürüne uygun bir şekilde geri dönüşümsüz olarak imha edilir.

4.1.8. Farklı Mekanlarda Yedekleme

Kamu SM, farklı mekânda yedekleme işi için konum olarak tamamen ayrı, uzak bir felaket kurtarma merkezine sahiptir. Yedek sistemin bulunduğu mekân, asıl sistemin sağladığı tüm güvenlik ve işlevsellik şartlarını sağlar.

Kamu SM, sisteminin sürekliliğini sağlayabilmek amacıyla gerekli gördüğü bileşenleri, farklı bir fiziksel mekânda güvenli kasalarda saklar.

4.2. Prosedürel Kontroller

4.2.1. Güvenilir Roller

Kamu SM’de çalışan personelin rolleri aşağıda belirtildiği şekilde sınıflandırılmıştır:

Kamu SM Yönetimi: Kamu SM’nin stratejik hedeflerinin gerçekleştirilmesi için gerekli tüm idari ve teknik faaliyetlerin yönetilmesinden sorumludur.

Güvenlik Personeli: Kamu SM güvenlik politikalarının uygulanmasından sorumludur.

Sistem Yöneticileri: Zaman Damgası hizmetlerinin yürütülmesi için bilgi teknolojileri altyapısının yönetilmesinden sorumludur.

Sistem Operatörleri: Tüm sistem bileşenlerinin işletiminden, yedeklenmesinden ve kurtarma faaliyetlerinin yürütülmesinden sorumludur.

Sistem Denetçisi: Zaman Damgası hizmetleriyle ilgili arşiv ve denetim kayıtlarının denetlenmesinden sorumludur.

Zaman Damgası Yöneticisi: Zaman damgası hizmetinin yürütülmesi için bilgi ve teknoloji altyapısının yönetilmesinden sorumludur.

Zaman Damgası Kayıtçısı: Zaman damgası hesaplarıyla ilgili operasyonel süreçlerin yürütülmesinden sorumludur.

4.2.2. Her İşlem İçin Gereken Kişi Sayısı

Kamu SM, Kök SHS’ye ait sertifika üretilmesi, iptal edilmesi ve özel anahtarların başka bir kriptografik modül içerisine yedeklenmesi için birden fazla yetkili personelin aynı anda hazır bulunmasını sağlar.

4.2.3. Kimlik Doğrulama ve Yetkilendirme

Kamu SM işleyişinin her adımında, işlemleri yerine getirecek kişilerin kimlik tanımlaması ve doğrulaması yapılır. Böylece her sistem birimine sadece yetkili kişilerin erişimi sağlanır. Sistemdeki bazı birimlere erişim, farklı derecelerdeki yetkilendirme tanımlamalarıyla yapılır. Bu birimlere erişimin sağlanabilmesi için kimlik doğrulaması yapıldıktan sonra yetkilendirme tanımlamalarında verilen yetkiler çerçevesinde sistemde işlem yapılabilir.

Kamu SM sistemi içinde kimlik doğrulama; güvenli donanım araçları, parolalar ve biyometrik veri kullanılarak güncel kriptografik yöntemlerle yapılır.

4.2.4. Görevlerin Ayrılmasını Gerektiren Roller

- Sistem Denetçisi ile diğer roller arasında,
- Sistem Yöneticisi ile Güvenlik Personeli ve Sistem Denetçisi arasında,
- Zaman Damgası Kayıtçısı ile Zaman Damgası Yöneticisi arasında, görevler ayrılığı vardır.

4.3. Personel Güvenlik Kontrolleri

4.3.1. Kişisel Geçmiş, Deneyim ve Nitelik Gereklere

Çalışanlar sistemin işleyiş ve güvenlik gereklerini sağlayabilecek nitelikte, bilgili ve deneyimli kişilerden seçilir. Kamu SM'nin istihdam ettirdiği personel sistem güvenliği, veri tabanı yönetimi, elektronik imza teknolojileri ve uygulamaları, sertifika yönetimi ile ilgili konularda bilgi ve deneyimi olan nitelikli kişilerden oluşur.

4.3.2. Geçmiş Araştırması

Çalışanların Kamu SM'nin işletilmesinde güvenlik ihtiyaçlarının gerektirdiği güvenilirliğe sahip olması gerekmektedir. Personelin güvenilirliği geçmişine yönelik yapılan araştırmalar ile belirlenir. İşe alınmadan önce geçmişe yönelik yapılan araştırmalarda personelin herhangi bir sebepten dolayı hüküm giyip giymemiş olduğu araştırılır. Adli sicil kayıtları incelenir. Güvenlik soruşturması biten personel işe başlatılır. İşe başlayan personelin bilgi güvenliği farkındalık eğitimleri tamamlanmadan, sistemlere erişimine izin verilmez.

4.3.3. Eğitim Gereklere

Çalışanlar, Kamu SM'deki işlerine aktif olarak başlamadan önce gerekli eğitimden geçirilirler. Çalışanlara verilen eğitimde Kamu SM'de uygulanan güvenlik ilkeleri, sistemin teknik ve idari işleyişi, işleriyle ilgili süreçler, süreç içindeki görev ve sorumluluklar anlatılır.

4.3.4.Sürekli Eğitim Gereklere ve Sıklığı

Kamu SM sisteminde yapılan değişikliklerin bildirilmesi amacıyla personele verilen eğitimler gerekli görüldükçe tekrarlanır. Yeni göreve başlayanlar için eğitimler tekrarlanır.

Kamu SM, çalışanlarına yılda en az bir defa, siber güvenlik ve sosyal mühendislik saldırılarına karşı farkındalık oluşturmak amacıyla, bilgi güvenliği eğitimi vermektedir.

4.3.5.Görev Değişim Sıklığı ve Sırası

Düzenlenmesine gerek duyulmamıştır.

4.3.6.Yetkisiz Eylemlerin Cezalandırılması

Kamu SM personelinin tamamen veya kısmen sahte elektronik sertifika oluşturması, geçerli olarak oluşturulan elektronik sertifikaları taklit veya tahrif etmesi, yetkisi olmadan elektronik sertifika oluşturması veya bu elektronik sertifikaları bilerek kullanması halinde ve diğer yetkisiz eylemlerde ilgili mevzuat gereğince bilgi güvenliği politikaları ihlali ve ihlalin boyutuna göre hukuki soruşturma ve disiplin süreci başlatılır.

4.3.7.Anlaşmalı Personel Gereksinimleri

Kamu SM verdiği hizmetler için dış kaynak kullanmak durumunda kaldığında, bu hizmeti sağlayacak firma personeli ile ilgili güvenlik kontrollerini, firma ile yaptığı sözleşme ile belirler.

4.3.8.Sağlanan Dokümantasyon

Çalışanlara işleriyle ve Kamu SM süreçleriyle ilgili gerekli kılavuz ve destek dokümanlar ve bilgi güvenliği politikaları kapsamındaki ilgili dokümanlar sağlanır.

4.4. 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.

4.4.1. Kaydedilen İşlemler

Şu işlemler kaydedilir:

- ZDH sertifikalarının yaşam döngüsüyle ilgili işlemler

ZAMAN DAMGASI UYGULAMA ESASLARI

- Sertifikanın kullanıma alınması
- 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

Bunların dışında zaman damgası ile ilgili olarak aşağıdaki kayıtlar 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.

4.4.2. Kayıtların İncelenme Sıklığı

Tutulan kayıtlar belirli 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.

4.4.3. Kayıtların Saklanma Süresi

Kayıtlar izinsiz erişimi, 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.

4.4.4. Kayıtların Korunması

Kamu SM'ye ait kayıtların elektronik ve fiziksel olarak güvenlik altında tutulması için aşağıdaki önlemler alınmıştır:

- Yetkisi olmayan kişiler elektronik kayıtların bulunduğu ortamlara erişemezler.
- Kağıt üzerindeki kayıtlar sadece yetkililerin girme izni bulunan kilitli odalarda bulunur.
- Kayıtlar izinsiz erişimi, değiştirmeyi ve silinmeyi engelleyecek şekilde elektronik ve fiziksel olarak güvenli tutulur.
- Kritik bilgiler gerektiğinde şifreli olarak saklanır.
- Kamu SM zaman damgası hizmeti ile ilgili işlemlerin kayıtlarının bütünlüğünü ve gizliliğini korur.
- Zaman damgası sistemi kullanıcıları hakkındaki özel bilgiler gizliliği sağlanarak korunur.

4.4.5. Kayıtların Yedeklenmesi

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

4.4.6. Kayıtların Toplanması

Kayıtlar elektronik olarak veya kağıt ortamda toplanır.

4.5. Kayıt Arşivleme

4.5.1. Arşivlenen Kayıt Bilgileri

Bölüm 4.4.1'de belirtilen kayıtlara ek olarak, elektronik ortamda ya da kağıt üzerinde tutulan aşağıdaki belgeler arşivlenir:

- Zaman damgası hesabı ile ilgili yapılan önemli yazışmalar
- Geçerlilik süresi dolan tüm Kamu SM Kök SHS ve zaman damgası sertifikaları
- Yayımlanan tüm sertifika iptal durum kayıtları
- Zaman Damgası İlkeleri
- Zaman Damgası Uygulama Esasları
- Zaman Damgası Bilgi Güncelleme Formu
- Zaman Damgası Talep Formu

4.5.2.Arşivlerin Tutulma Süresi

Arşivlenen bilgiler ve belgeler Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik uyarınca en az 20 (yirmi) yıl boyunca saklanır.

4.5.3.Arşivlerin Korunması

Arşivlenen bilgi ve belgeler, izinsiz erişimi, değiştirmeyi ve silinmeyi engelleyecek şekilde elektronik ve fiziksel olarak güvenli tutulur. Arşivler yetkisiz çalışanların erişimine kapalıdır. Arşivlerin tutulduğu ortam 4.5.2'de belirtilen süre boyunca arşivlerin zarar görmesini engelleyecek şekilde seçilir.

4.5.4.Arşivlerin Yedeklenmesi

Kritik bilgi içeren elektronik arşivler Kamu SM iş sürekliliği politikası gereğince yedeklenir.

4.5.5.Kayıtların Zaman Damgası Gereksinimleri

Kamu SM gerekli gördüğü kayıtlara zaman damgası ekler.

4.5.6.Arşivlerin Toplanması

Arşivler elektronik veya kağıt ortamda toplanır.

4.5.7.Arşiv Bilgilerinin Elde Edilme ve Doğrulanma Metodu

Arşiv bilgileri yetkili personelden edinilir. Yasal gereksinimlerin ortaya çıkması ya da BTK tarafından denetim amacıyla talep edilmesi durumunda yetkili personel eşliğinde arşiv bilgileri elde edilebilir.

5. Teknik Güvenlik Kontrolleri

Kamu SM'nin kendisi ve sertifika sahipleri adına, anahtar çiftleri ve erişim verilerini ürettiği, sertifika yönetim işlemlerini gerçekleştirdiği sistemler CWA 14167-1, ETSI TS 101 456 ve ISO/IEC 27001 gereklerini sağlar.

5.1. ZDH Anahtar Çifti Üretimi ve Kurulumu

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 güvenli odada oluşturulur.

ZAMAN DAMGASI UYGULAMA ESASLARI

- 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.

5.1.3. ZDH Anahtar Uzunlukları

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

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 Oluőturma Verisine Eriőim Denetimi

ZDH'nin imza oluőturma verisine eriőim birden fazla yetkili alıőanın ortak denetimi altındadır. İmza oluőturma verisi iőlemleri iin yeterli sayıda yetkili personelin hazır bulunması ve elektronik olarak kimliklerinin ve yetkilerinin doėrulanması gerekir.

5.2.3. ZDH İmza Oluőturma Verisinin Saklanması

ZDH'ye ait imza oluőturma verileri yetkisiz kiőilerin eriőimine kapalı, fiziksel ve elektronik olarak güvenli kriptografik modöl iinde őifreli olarak tutulur. İmza oluőturma verisinin kriptografik modöl dıőına ıkması engellenir.

5.2.4. ZDH İmza Oluőturma Verisinin Yedeklenmesi

ZDH'ye ait imza oluőturma verileri yetkisiz kiőilerin eriőimine kapalı, fiziksel ve elektronik olarak güvenli kriptografik donanım cihazı iinde yedeklenir. İmza oluőturma verisinin yedeklenmesi iőlemi birden fazla yetkili alıőanın ortak denetimi altındadır.

5.2.5. ZDH İmza Oluőturma Verisinin Arőivlenmesi

ZDH'ye ait imza oluőturma verileri arőivlenmez. Kullanım sūreleri sonunda geri dōnūősūő şekilde silinir.

5.2.6. ZDH İmza Oluőturma Verisinin Kriptografik Modölle Yūklenmesi

İmza oluőturma verisi güvenlik gereklerine uygun biimde kriptografik modöl dıőında ūretilir. Ancak imza oluőturma verisinin kriptografik modöl iinde saklanması zorunludur. Kriptografik modöl dıőında ūretilen imza oluőturma verisi yetkili birden fazla personelin denetiminde modölle yūklenir.

5.2.7. ZDH İmza Oluőturma Verisine Eriőim

ZDH'ye ait imza oluőturma verisi güvenli algoritma ve yōntemlerle őifreli olarak güvenli kriptografik modöl iinde saklanır. İmza oluőturma verisinin eriőime aılması ve kullanılır duruma getirilmesi yetkili birden fazla alıőanın ortak denetimi altındadır.

5.2.8. ZDH İmza Oluőturma Verisine Eriőimin Kesilmesi

ZDH'ye ait imza oluőturma verisi imzalama iin kullanıldıktan sonra eriőime yeniden aılıncaya kadar eriőime kapalı tutulur.

5.2.9. ZDH İmza Oluřturma Verisinin Yok Edilmesi

ZDH'ye ait imza oluřturma verisi kullanım süresinin dolmasının ardından, bulunduđu sistemden uygun yöntemlerle geri dönüşsüz şekilde silinir. İmza oluřturma 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 bulunduđu sertifikalar yasa ve ilgili yönetmelikte belirtilen süre boyunca arşivlenir. Arşivde bulunduđu süre boyunca sertifikaların bütünlüğünün sağlanması için gereken her türlü önlem alınır.

5.3.2. ZDH İmza Oluřturma ve Doğrulama Verilerinin Kullanım Süreleri

ZDH'ye ait imza oluřturma ve doğrulama anahtar çiftinin kullanım süresi ilgili yönetmelikte belirtilen sürelerle uyar ve Kamu SM tarafından gerekli güvenliği sağlayacak şekilde seçilir.

5.3.3. ZDH İmza Oluřturma 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 değiřtirmek için önlemleri alır.

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

5.4. Eriřim Denetim Verileri

Kamu SM çalışanlarının eriřim denetim verileri eriřim parolalarını, güvenli donanım araçları içindeki eriřim denetimi sağlayan diğer verileri, biyometrik verileri içerir.

5.4.1. Eriřim Denetim Verilerinin Oluřturulması

Kamu SM sistemi içinde kullanılan eriřim denetim verileri yetkisiz kiřilerin eriřimine kapalı, fiziksel ve elektronik olarak güvenli ortamlarda, sistem tarafından yeterli uzunlukta, tahmin edilemez nitelikte ve rasgele üretilir.

5.4.2.Eriřim Denetim Verilerinin Korunması

Zaman damgası istemcisine ait eriřim parolasını yetkisiz kiřilerin eriřimine karřı korumak istemcinin yükümlülüğü altındadır.

5.4.3.Eriřim Denetim Verileri İle İlgili Diğer Konular

Zaman damgası istemcisine ait eriřim parolası zaman damgası hesabı başvurusu sırasında kullanıcı tarafından oluşturulur.

5.5. Bilgisayar Güvenliğı Denetimleri

5.5.1.Bilgisayar Güvenliğı İle İlgili Teknik Gerekler

Kamu SM sistemi içinde kötü niyetli yazılımlara karřı gereken önlemler alınır. Sistemde ağı ve sunucu bazlı sensörler içeren saldırı tespit sistemi bulunmaktadır. Bütün sunucular üzerinde merkezden yönetilebilen virüs tespit ve temizleme ajanları kurulmuřtur. Kritik işlemlerin yapıldığı bilgisayarlar ağı ortamı dışında tutulur. Bilgilerin tahrifata, silinmeye ve kaçağı karřı korunması ve işlemin sürekliliğinin sağlanması için gerekli güvenlik sağlanır. Her kurulan yazılımın yedek kopyası yaratılır ve sistemin güvenliğı konusunda bütün iyileřtirme eylemleri gecikmesiz uygulanır.

5.5.2.Bilgisayar Sisteminin Sağladığı Güvenlik Seviyesi

Düzenlenmesine gerek duyulmamıřtır.

5.6. Yařam Döngüsü Teknik Denetimleri

5.6.1.Sistem Geliřtirme Denetimleri

Sistem geliřtirilirken genel anlamda yapılan denetimler ařağıda verilmiřtir:

- Yeterli düzeyde kalite ve güvenlik tedbirleri alınır.
- Belirlenen güvenlik kriterlerine uygun personel çalıştırılır.
- Her kurulan yazılımın yedek kopyası yaratılır.
- Sertifika işlemlerinin sürekliliğini sağlamak için sistem bilgilerini tutan bileřenlerin yedekleri oluşturulur.
- Sistemin açık ağı bağlantısında gerekli güvenlik önlemleri alınır.
- Kurulum sırasında dışarıdan gelen yazılımlar kullanılmadan önce virüs ve resmi olmayan yazılımların sisteme girmesi engellenir. Bu konuda tüm güvenlik gerekleri yerine getirilir, bütün iyileřtirme eylemleri gecikmesiz uygulanır.

ZAMAN DAMGASI UYGULAMA ESASLARI

- Anormal sistem koşullarını yakalamak için ilk dönemlerde sistem durumları yakından gözlemlenir.
- Geliştirilmekte olan sisteme erişim kimlik, parola gibi tanıtıcı bilgilerin doğrulanmasıyla yapılır.
- Sistemin geliştirilmesi sırasında yapılan denetimler TS ISO/IEC 27001 gereklerini sağlar.

5.6.2. Güvenlik Yönetimi Denetimleri

Sistem içinde kurulu olan yazılım ve donanım ürünleri ile ağ ortamının işleyişinin planlanan şekilde güvenli olarak sürdürüldüğünü göstermek için iki (2) yılda en az bir defa güvenlik yönetimi denetimi yapılır. Kamu SM içinde güvenliğe uygun olmayan hareketler ve yetkilendirmeler denetleme sonucunda açıklanır ve düzeltici önlemler alınır.

5.6.3. Yaşam Döngüsü Güvenlik Denetimleri

Düzenlenmesine gerek duyulmamıştır.

5.7. Ağ Güvenliği Denetimleri

Son teknolojik gelişmeler göz önünde bulundurularak gerekli ağ güvenliği denetimleri yapılır. Sistem, dışa açık ağa bağlantısında güvenlik duvarlarını kullanır. Sistemdeki sunucu ve aktif cihazların durum ve performanslarını izlemek, geçmişe yönelik performans raporları çıkarmak ve geleceğe yönelik performans eğilimlerini saptamak amacı ile ağ ve sistem yönetimi sunucuları mevcuttur.

Sunucular üzerine ağ ve sistem yönetimi ajanları kurulmuştur. Yönetim yazılımı bu ajanlardan disk, hafıza, işlemci kullanımı gibi bilgileri çeker ve bu bilgileri gerçek zamanlı görüntüler. Sunucuların çalışması için önem arz eden kaynaklar için eşik değerler belirlenir ve bu eşik değerlerin aşılması durumunda sistem yöneticisi otomatik olarak uyarılır. Ağ ve sistem yönetimi yazılımı çektiği bilgileri merkezi bir veri tabanında saklar. Böylece herhangi bir anda verilerin sorgulanmasına ve geçmişe dönük rapor üretilmesine imkan tanınır.

Yüksek güvenlik gerektiren işlemlerin yapıldığı sistemler için farklı ağlar kurulmuştur. Kritik işlemlerin yapıldığı sistemler ağa bağlı değildir.

6. Uygunluk Denetimleri

Kamu SM, mevzuat gereği BTK tarafından incelenir/denetlenir.

Kamu SM, ek olarak ISO/IEC 27001 bilgi güvenliği yönetim sistemi standardına uygun olarak hizmet verir ve standart gereği düzenli olarak iç ve dış denetimlere tabi tutulur.

Kamu SM iç işleyişini denetlemek için, ayrıca iç denetimler gerçekleştirilir.

6.1. Uygunluk Denetiminin Sıklığı

BTK gerekli gördüğü durumlarda re'sen denetim yapabilir.

Kamu SM, ISO/IEC 27001 bilgi güvenliği yönetim sistemi standardı gereğince yılda bir defa uygunluk denetimi geçirir. Her üç yılda bir sertifika yenilenir.

İç denetim, yılda en az 1 (bir) defa olmak üzere gerçekleştirilir.

6.2. Denetçinin Nitelikleri

Kamu SM faaliyetlerinin denetimi, kanunla yetkilendirilmiş olan BTK tarafından gerçekleştirilir.

ISO/IEC 27001 BGYS'nin denetimi bağımsız ve akredite edilmiş kuruluşlarca gerçekleştirilir.

İç denetim, Kamu SM ZDUE'sine hakim, sertifika süreçlerini bilen ve denetim konusunda tecrübeli Kamu SM personeli tarafından gerçekleştirilir.

6.3. Denetçinin Denetlenen Tarafla Olan İlişkisi

BTK, kanun gereği tüm ESHS'leri denetlemekle yetkili kılınmış düzenleyici kurumdur.

Kamu SM'nin ISO/IEC 27001 BGYS denetimi, bağımsız ve akredite edilmiş kuruluşlarca gerçekleştirilir.

İç denetim için seçilen denetçiler denetlenecek birimden seçilmez.

6.4. Denetimin Kapsamı

Kamu SM'nin denetim kapsamı BTK tarafından belirlenir.

BGYS standardına uygun denetim kapsamı bağımsız kurum denetçisi tarafından belirlenir.

İç denetim kapsamı denetimi gerçekleştirecek Kamu SM personeli tarafından belirlenir.

6.5. Yetersizliğin Tespiti Durumunda Yapılacaklar

BTK tarafından gerçekleştirilen denetimlerde ortaya çıkan eksiklikler, Kamu SM tarafından planlı çalışma ile giderilir. Eksiklikler Kamu SM'nin işleyişini etkileyecek kadar büyük ise, ilgili mevzuata göre yaptırım ve cezalar uygulanır.

ISO/IEC 27001 standardına göre gerçekleştirilen denetimlerde ortaya çıkan eksiklikler, Kamu SM tarafından planlı çalışma ile giderilir. Eksiklikler, BGYS'nin temel işleyişini etkileyecek kadar büyük ise, Kamu SM, ISO/IEC 27001 uygunluk belgesi eksikler giderilinceye kadar askıya alınır.

İç denetimlerde ortaya çıkan eksiklikler, Kamu SM ilgili personeli tarafından giderilir. Tüm denetimlerden elde edilen bulgular Uygunsuzluk veya Düzeltici/İyileştirici Faaliyetler açılarak takip edilir.

6.6. Sonucun Bildirilmesi

Denetim sonucu, BTK ve ISO/IEC 27001 denetçilerinin hazırladığı resmi raporlar ile Kamu SM'ye bildirilir.

İç denetim sonucu, Kamu SM üst yönetimine raporlanır.

7. Diğer İşler ve Hukuksal Meseleler

7.1. Ücretlendirme

7.1.1.Zaman Damgası Ücretlendirme

Kamu SM, zaman damgası başvurusunda talep edilen sayıda zaman damgası içeren kontör paketini hesaba ekler. Yüklenen her zaman damgası kontör paketi için başvuru sahibinden ücret talep edilir. Bu hizmet için zaman kısıtlaması uygulanabilir. Kuruma gönderilen her zaman damgası için bir kontör düşürülür. Zaman damgası ücretlendirilmesi ile ilgili ayrıntılar Kamu SM web sitesinde belirtilir.

7.1.2.Sertifika Erişim Ücreti

ESHS, kendisine ve zaman damgası makamlarına ait sertifikaları resmî web sitesinde ücretsiz olarak yayımlar .

7.1.3.İptal Durum Kaydına Erişim Ücreti

ESHS, sertifika iptal durum kaydını duyurmak için ücret talep etmez.

7.1.4.Diğer Servis Ücretleri

ESHS, bilgi deposundan yayımladığı bilgi ve dokümanlara erişim için ücret talep etmez.

7.1.5.İade Ücreti

İade talepleri Kamu SM tarafından siparişin durumuna göre değerlendirilerek işletilir.

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 için Politika Gereklere"

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

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