ZAMAN DAMGASI UYGULAMA ESASLARI (ZDUE)

SÜRÜM : 02

TARİH : 28.08.2013

© 2005 - 2013 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. Tüm hakları saklıdır.

© 2005 - 2013 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. Tüm hakları saklıdır.

© 2005 - 2013 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. Tüm hakları saklıdır.

© 2005 - 2013 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. Tüm hakları saklıdır.

© 2005 - 2013 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. Tüm hakları saklıdır.

1. GİRİŞ

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

Zaman Damgası Uygulama Esasları (ZDUE) olarak adlandırılan bu kitapçık, TÜRKTRUST'ın elektronik sertifika hizmet sağlayıcılığı kapsamındaki zaman damgası alanındaki faaliyetlerini nasıl yürüttüğünü göstermek amacıyla, Bilgi Teknolojileri ve İletişim Kurumu'nun kanun kapsamında yayımlamış olduğu "Elektronik İmzaya İlişkin Süreçler ile Teknik Kriterlere İlişkin Tebliğ"in 10. Maddesi uyarınca 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 TÜRKTRUST'ın ve diğer tarafların uygulama sorumluluklarını belirler.

1.1. Genel Bakış

ZDUE kitapçığı, TÜRKTRUST'ın verdiği tüm zaman damgası hizmetlerini kapsar.

TÜRKTRUST, ilgili Zaman Damgası İlkeleri (ZDİ) kitapçığı hükümlerine bağlı bir uygulama kitapçığı olan bu ZDUE kitapçığında yer alan uygulama esaslarına göre hazırlanan ve ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi ile ISO 9001 Kalite Yönetim Sistemi uyarınca dokümante edilen prosedür ve talimatları aracılığıyla yürütür.

Zaman Damgası İlkeleri (ZDİ) ve Zaman Damgası Uygulama Esasları (ZDUE) kitapçıkları mevzuat ve standartlar çerçevesinde en az yılda bir kere Yönetim Gözden Geçirme Toplantısında değerlendirilir. Bu değerlendirmeler sonucunda ya da yıl içinde ortaya çıkabilecek gereklilikler doğrultusunda bu kitapçıklar güncellenir.

1.2. Kitapçık Adı ve Tanımlama

Bu ZDUE kitapçığının açık adı "TÜRKTRUST Zaman Damgası Uygulama Esasları (ZDUE)"dır. Kitapçığın sürüm numarası ve tarihi kapak sayfasında yer almaktadır.

TÜRKTRUST ZDUE kitapçığı, TÜRKTRUST ZDİ kitapçığında tanımlanan zaman damgası ilkeleri uyarınca TÜRKTRUST'ın zaman damgası hizmetleri ile ilgili faaliyetlerini nasıl yürüttüğünü açıklar. ZDUE kitapçığı, nesne tanımlayıcı numarası (OID) "2.16.792.3.0.3.2.1" olarak belirlenen TÜRKTRUST Zaman Damgası İlkeleri'nde belirtilen ve ETSI TS 102 023 kitapçığında tanımlanan zaman damgası ilkelerinin uygulama esaslarını kapsar.

ZDUE kitapçığı "http://www.turktrust.com.tr" web adresinde kamuya açık olarak yayımlanmaktadır.

© 2005 - 2013 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. Tüm hakları saklıdır.

1.3. Taraflar

Bu uygulama esasları kitapçığında hak ve yükümlülükleri tanımlanan TÜRKTRUST zaman damgası hizmetleriyle ilgili taraflar, zaman damgası hizmetlerini veren ESHS birimleri ve hizmeti alan müşteri ve kullanıcılar olarak tanımlanır.

1.3.1. Zaman Damgası Üretim Merkezi

Zaman damgası üretim merkezi, TÜRKTRUST'ın zaman damgası üretim ve dağıtımından sorumlu birimidir.

1.3.2. Zaman Damgası Sahibi

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, TÜRKTRUST zaman damgası hizmetleri kapsamında, TÜRKTRUST tarafından verilmiş olan zaman damgalarını alan ve ilgili zaman damgalarını doğrulayan taraflardır.

1.3.4. Diğer Taraflar

TÜRKTRUST sertifika hizmetleri kapsamında zaman damgası üretimi, bilgi deposu yayımlama ve benzeri zaman damgası hizmetlerinin tümü TÜRKTRUST tarafından verilir.

TÜRKTRUST'ın zaman damgası hizmetlerini verirken işbirliği yaptığı ve dışarıdan hizmet aldığı tüm kuruluşlar, verecekleri hizmeti güvenilir ve doğru biçimde vereceklerini ve TÜRKTRUST iş süreçleri ve müşterileriyle ilgili gizli veya özel bilgileri açığa çıkarmayacaklarını garanti eder. TÜRKTRUST ile hizmet aldığı kuruluşlar arasında bu garantilerin açıkça belirtildiği hizmet sözleşmeleri imzalanır.

1.4. Zaman Damgası İlkeleri Yönetimi

TÜRKTRUST, zaman damgası ilkelerini oluşturan otorite olarak, bu ZDUE kitapçığının bağlı bulunduğu ZDİ kitapçığının yönetimi ve kayıt altına alınmasından sorumludur.

1.4.1. ZDUE Kitapçığından Sorumlu Organizasyon

Bu ZDUE kitapçığının tüm hakları ve sorumluluğu TÜRKTRUST'a aittir.

1.4.2. İletişim Noktası

ZDUE kitapçığıyla ilgili iletişim bilgileri aşağıdadır:

TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş.
Adres : Hollanda Caddesi 696.Sokak No:7 Yıldız, Çankaya 06550 ANKARA
Telefon : (90-312) 439 10 00
Faks : (90-312) 439 10 01
Çağrı Merkezi : 0850 222 444 6
E-posta : sertifika@turktrust.com.tr
Web : http://www.turktrust.com.tr

1.4.3. ZDUE'nin İlkelere Uygunluğunun Belirlenmesi

TÜRKTRUST ZDUE kitapçığının TÜRKTRUST ZDİ kitapçığına uygunluğu ve uygulanabilirliği TÜRKTRUST üst yönetimi tarafından belirlenir.

© 2005 - 2013 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. Tüm hakları saklıdır.

1.4.4. ZDUE Onaylama Prosedürleri

TÜRKTRUST'ın bu ZDUE kitapçığı, TÜRKTRUST ZDİ kitapçığına uygun olarak hazırlanmıştır. ZDUE kitapçığı TÜRKTRUST Yönetim Kurulu tarafından onaylanır. Gerekli onayı alan ZDUE, TÜRKTRUST zaman damgası faaliyetlerini düzenlemek ve işletmek için kullanılır.

TÜRKTRUST üst yönetimi, bu ZDUE kitapçığında belirtilen gerekliliklerin karşılanması için oluşturulan zaman damgası uygulama esaslarının, uygun bir biçimde yürütülmesini sağlamaktan sorumludur.

1.5. Kısaltmalar ve Tanımlar

1.5.1. Kısaltmalar

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 (OCSP): 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 suistimallerin tespit edilmesi ve ilgili mevzuatta öngörülen yaptırımların uygulanması amacıyla yapılan çalışmalar bütünüdür.

© 2005 - 2013 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. Tüm hakları saklıdır.

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.

© 2005 - 2013 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. Tüm hakları saklıdır.

Kurum: Bilgi Teknolojileri ve İletişimKurumu'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.

© 2005 - 2013 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. Tüm hakları saklıdır.

2. ZAMAN DAMGASI HİZMETLERİNE YÖNELİK YAYINLAR

TÜRKTRUST, 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 müşterilere ulaştırılabilmesi ve zaman damgası kullanımının güvenilirliğinin ve sürekliliğinin sağlanması amacıyla kamuya açık olarak yayımlanır.

2.1. Zaman Damgası Hizmetleri Bilgi Deposu

TÜRKTRUST, bilgi deposunda tutulan tüm bilgilerin doğruluğunu ve güncelliğini sağlar. TÜRKTRUST, bilgi deposunu işletmek ve ilgili doküman ve kayıtları yayımlamak için üçüncü bir güvenilir taraf kullanmaz.

2.2. Zaman Damgası Hizmetleri Bilgisinin Yayımlanması

TÜRKTRUST bilgi deposunda, zaman damgası hizmetlerine ait özel kurumsal prosedür ve talimatlar ile ticari gizli bilgiler dışında kalan, zaman damgası hizmetlerinin yürütülmesine ilişkin bilgiler, herkesin erişimine açık tutulur. TÜRKTRUST'ın zaman damgası hizmetlerine yönelik ilkelerini içeren ZDİ kitapçığı, bu ilkelerin nasıl uygulandığını gösteren ZDUE kitapçığı bilgi deposunda yer alır. Ayrıca, TÜRKTRUST elektronik sertifika ve zaman damgası hizmetlerine ilişkin tüm kök ve alt kök sertifikaları herkesin erişimine açık olarak dizin sunucularda yayımlanır.

Bu bölümde sözü geçen bilgilere erişim, http://www.turktrust.com.tr adresinden yapılır.

2.3. Yayımın Zamanı veya Sıklığı

Madde 2.2'de bahsedilen dokümanların yeni sürümleri çıktıkça, eski sürümlerle birlikte bilgi deposunda yayımlanır.

2.4. Bilgi Deposuna Erişim Kontrolleri

Bilgi deposu herkesin erişimine açıktır. TÜRKTRUST bu amaçla, yayımlanan bilgilerin gerçekliğini sağlamak üzere, http://www.turktrust.com.tr adresi için gerekli her türlü güvenlik önlemini alır.

© 2005 - 2013 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. Tüm hakları saklıdır.

3. ZAMAN DAMGASI İŞLEVSEL GEREKLİLİKLERİ

TÜRKTRUST zaman damgası hizmetleri, bu ZDUE kitapçığında yer alan uygulama esasları uyarınca yürütülür.

3.1. Zaman Damgası Başvurusu

3.1.1. Kimler Zaman Damgası Başvurusunda Bulunabilir?

Elektronik ortamda yer alan belirli elektronik verilerinin varlığını kesin ve doğru bir zaman bilgisiyle kanıtlamak isteyen tüm gerçek ve tüzel kişiler, TÜRKTRUST'a zaman damgası başvurusunda bulunabilir.

3.1.2. Zaman Damgası Başvuru Kayıtları

Zaman damgası başvuruları, başvuru sahipleri tarafından elektronik ortamda ve belirlenen protokoller üzerinden yapılır. Başvuru sahiplerinin bilgileri ve zaman damgası verilecek olan elektronik verilere ait kayıtlar TÜRKTRUST tarafından düzenli olarak tutulur.

3.2. Zaman Damgası Üretimi

3.2.1. Zaman Damgası Başvurularının Doğrulanması

TÜRKTRUST, zaman damgası başvurularını teknik olarak doğrular. Zaman damgası başvuruları ZDUE hükümlerine ve ilgili prosedürlere uygunsa kabul edilir. Başvuruların doğrulanamaması durumunda TÜRKTRUST başvuruyu reddetme hakkını saklı tutar.

3.2.2. Zaman Damgası Üretimi

Zaman damgası başvuru sahibi, zaman damgası talebini gerçek zamanda, ETSI TS 101 861 dokümanında belirlenen biçimde TÜRKTRUST'a iletir. TÜRKTRUST, adı geçen dokümanda belirlenen biçimde zaman damgasını oluşturarak, talep sahibine Madde 3.3'te belirlenen yolla cevap verir.

3.2.3. Zaman Bilgisinin Senkronizasyonu

TÜRKTRUST, zaman bilgisinin senkronizasyonunu, GPS uydularından senkronize olan bir zaman sunucusuyla sağlamaktadır. UTC (evrensel zaman değeri) ile TÜRKTRUST zaman bilgisi senkronizasyon farkı, saniyenin milyonda biri düzeyindedir.

3.3. Zaman Damgası Hizmet Protokolü – HTTP Protokolü

TÜRKTRUST, talep üzerine, http protokolü üzerinden oluşturulmuş zaman damgası verisini zaman damgası başvuru sahiplerine çevrim içi gönderir.

© 2005 - 2013 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. Tüm hakları saklıdır.

4. TESİS, YÖNETİM VE İŞLETMEYLE İLGİLİ KONTROLLER

ZDUE kitapçığının bu kısmında, TÜRKTRUST'ın zaman damgası hizmetlerini yürütürken tesis ve işletme güvenliğini sağlamaya yönelik olarak uyguladığı, teknik olmayan çeşitli güvenlik kontrolleri yer almaktadır.

4.1. Fiziksel Kontroller

4.1.1. Tesis Yeri ve İnşaatı

TÜRKTRUST merkezi, dış tehditlere karşı korunaklı ve güvenli bir alanda kurulmuş, tesis içinde yüksek güvenlikli bölgeler ve çeşitli güvenlik alanları oluşturulmuştur.

4.1.2. Fiziksel Erişim

TÜRKTRUST merkezindeki alanlara fiziksel erişim sürekli kontrol altında tutulmaktadır.

Tesisin çevresi, dışarıdan kontrolsüz giriş çıkışın engellenmesi için korunaklı bir şekilde çevrilmiştir. Merkezin dışarıyla bağlantılı tüm giriş çıkış noktalarında güvenlik görevlileri bulunur. Güvenli alanlara fiziksel erişim kartlı geçiş kontrol sistemleri aracılığıyla yapılır. Yetkisiz kişilerin belirli bölgelere girişi yasaklanmıştır. Zaman damgası hizmetlerinin gerçekleştirildiği yüksek güvenlikli bölgeler daima yetkisiz girişe kapalı tutulur. Giriş çıkışlar kayıt altına alınır. Ek güvenlik önlemi olarak kritik bölge ve geçişler sürekli kameralarla izlenir ve kamera çekim kayıtları güvenlik gereklilikleri nedeniyle saklanır.

4.1.3. Güç Kaynakları ve Havalandırma

TÜRKTRUST merkezinde kullanılan tüm donanım ve teçhizat için kesintisiz çalışacak güç kaynakları oluşturulmuştur. Sistemler güç kesintilerine karşı, anında devreye girecek kesintisiz güç kaynakları ve jeneratörlerle desteklenir. Yedek güç ünitelerinin düzenli olarak bakımı yapılır ve ihtiyaca göre kapasiteleri geliştirilir.

Özellikle bilgisayar donanımlarının yoğun bulunduğu bölgelerde, bu bölgelerin dışında kalan alanlarda ise ihtiyaca göre yeterli havalandırma kesintisiz olarak sağlanır. Bina içinde belirli noktalarda optimum iklim koşullarının sağlanması için uygun ısıtma ve soğutma sistemleri kullanılarak sıcaklık ve nem kontrol altında tutulur.

4.1.4. Su Baskınları

TÜRKTRUST merkezi, inşaat önlemleriyle doğal afetlere dayalı sel ve su baskınlarına karşı korunmuştur. Binanın dış cephe ve zemin kaplamaları su geçirmez niteliktedir. Taban suyunun binaya sızmasını önlemek için gerekli yalıtım oluşturulmuştur.

Binanın su ve kanalizasyon tesisatında oluşabilecek arızalara bağlı iç su baskınlarının önlenmesi için, tesisat uygun biçimde yapılmış, su kanallarının binada kontrollü biçimde ana tesisat yollarından geçirilmesiyle, su akışı kontrol altına alınmıştır. Kritik donanım ve teçhizatın bulunduğu bölüm ve alanlarda su ve kanalizasyon yolunun bulunmaması sağlanmıştır.

Alınan bütün inşaat önlemlerine rağmen oluşabilecek olası su baskınlarını mevcut sisteme zarar vermeden bertaraf edebilmek için, yeterli düzeyde su tahliye sistemleri kurulmuştur.

4.1.5. Yangın Önleme ve Yangından Korunma

TÜRKTRUST binasında yıldırım etkisine bağlı yangın çıkmaması için uygun nitelikte paratoner sistemi kurulmuştur. Elektrik kontaklarına bağlı yangınları önlemek için elektrik

© 2005 - 2013 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. Tüm hakları saklıdır.

altyapısı kaliteli ve uygun malzeme ile hazırlanmış, güç sistemlerinde yeterli oranlarda elektrik sigortaları kullanılmıştır. Binanın sınırlı ve belirli, mutfak ve benzeri bazı bölgeleri dışında açık ateş kullanılmamakta, binanın belirlenmiş bazı alanları dışında kalan tüm alanlarda sigara içme yasağı uygulanmaktadır.

Olası yangın durumlarını büyümeden fark edip önleyebilmek için tesisin uygun noktalarına duman ve ısı algılayıcıları yerleştirilmiştir. Bir alarm anında otomatik olarak devreye giren yerleşik yangın söndürme sistemi mevcuttur. Yerleşik sistemde, binanın bölgelerine göre farklı fiziksel ve kimyasal nitelikteki yangın söndürme malzemeleri kullanılmaktadır. Bunun dışında, yine uygun kimyasal ve fiziksel niteliklere sahip yangın söndürme üniteleri binanın gerekli yerlerine konuşlandırılmış olup, personel kritik malzeme ve bölgeler için yangına müdahale etme konusunda eğitilerek bilgilendirilmiştir.

4.1.6. Saklama Ortamları

TÜRKTRUST faaliyetleri sırasında oluşturulan tüm kayıtların yedekleri uygun saklama ortamlarında tutulur. Bu yedekler, bina içinde su ve yangın korumalı bir alanda, fiziksel ve elektromanyetik güvenlik önlemleri alınmış, erişim güvenliği sağlanmış ve sadece prosedürel kontroller uygulanarak erişilebilecek şekilde saklanır.

4.1.7. Atıkların Atılması

Temel zaman damgası hizmetlerine bağlı, elektronik veya kağıt ortamda saklanan tüm bilgi ve belgeler, saklanmaları gerekmiyorsa ilgili prosedürler uyarınca tamamen imha edilerek atılır. Kriptografik modüller atılmaları gerektiğinde ya fiziksel olarak imha edilir ya da üretici firma talimatları doğrultusunda sıfırlanır.

Binanın ve TÜRKTRUST birimlerinin diğer tüm atıkları uygun biçimde tesis dışına çıkarılır.

4.1.8. Tesis Dışı Yedekleme

TÜRKTRUST, sertifika hizmetleri iş sürekliliğini sağlayabilmek amacıyla, mevcut tesis ve binada oluşabilecek herhangi bir afet durumunda sistemlerini yeniden işletilebilir duruma getirebilmek için elektronik işlem kayıtlarının yedeklerini tesis dışında güvenli kasalarda saklar.

4.2. Prosedürel Kontroller

4.2.1. Güvenilir Roller

TÜRKTRUST zaman damgası hizmetlerinde görev alan personelin organizasyonun sağlanması amacıyla,, tüm zaman damgası iş süreçlerinin yürütülmesinde görev alacak güvenilir roller belirlenmiştir.

- **Üst Düzey Yöneticiler:** TÜRKTRUST sertifika hizmetlerinin yürütülmesinden teknik ve idari açıdan sorumlu üst düzey yöneticilerdir.
- **Güvenlik Yetkilileri:** Güvenlik politikaları ve uygulamalarının yönetimi ve yürütülmesinden sorumlu çalışanlardır.
- **Sistem Yöneticileri:** Sertifika hizmetlerine ilişkin sistemlerin kurulumu, konfigürasyonu ve devamlılığının sağlanması ve aynı zamanda sistem yedekleme ve geri yükleme işlemleri için yetkilendirilmiş çalışanlardır.
- **Sistem Denetçileri:** Sertifika hizmetlerine ilişkin arşivlerin ve denetim kayıtlarının izlenmesi için yetkilendirilmiş çalışanlardır.

© 2005 - 2013 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. Tüm hakları saklıdır.

- **Güvenlik Görevlileri:** Tüm TÜRKTRUST tesislerinin fiziksel güvenliğini sağlamaktan sorumlu çalışanlardır.

4.2.2. Her Görev İçin Gereken En Az Kişi Sayısı

TÜRKTRUST'ta zaman damgası süreçleri dahilindeki kritik işlemlerin yapılabilmesi için çok kişi kontrollü bir sistem kurulmuştur. Kriptografik modül kullanımı gerektiren ve rutin akışın dışında kalan kritik işlemler, en az iki yetkilinin hazır bulunmasıyla sonuçlandırılabilmektedir.

TÜRKTRUST zaman damgası kök sertifikasıyla ilgili her türlü üretim, yenileme, iptal ve yedekleme işlemi en az iki yetkilinin hazır bulunmasıyla idari ve teknik onaylı görev talimatının ilgili yetkililere verilmiş olmasıyla yapılabilmektedir.

4.2.3. Her Görev için Kimlik Doğrulama

TÜRKTRUST içinde güvenilir rollere atanan çalışanlar, öncelikle atanmış yetkileriyle birlikte güvenlik sistemine tanıtılır. Böylelikle her kritik işlem öncesi bu rollerdeki kişilerin kimlik doğrulaması yapılır. Doğrulama tamamlandıktan sonra işleme izin verilir ve işlem tamamlandıktan sonra kaydedilir.

4.2.4. Görevlerin Ayrılmasını Gerektiren Roller

Zaman damgası süreçleri işletilirken yapılan her işlem, rol bazlı olarak ayrıntılı yer ve zaman bilgisi içerecek şekilde kayıt altına alınmaktadır.

Özellikle, "Güvenlik Yetkilisi" veya "Kayıt ve Müşteri Hizmetleri Yetkilisi" olarak yetkilendirilmiş bir kişi, "Sistem Denetçisi" olarak yetkilendirilemez. "Sistem Yöneticisi" olarak yetkilendirilmiş bir kişiyse, "Güvenlik Yetkilisi" veya "Sistem Denetçisi" olarak yetkilendirilemez.

4.3. Personel Kontrolleri

4.3.1. Nitelik, Deneyim ve Güvenlik Gereklilikleri

TÜRKTRUST'ta çalışan personel, zaman damgası süreçlerinin işleyişini doğru ve güvenilir bir şekilde yürütebilecek nitelikte, göreve uygun eğitim düzeyine sahip (lise, üniversite, yüksek lisans vb.), konusunda bilgili ve eğitimli, benzer çalışma alanlarında deneyimli ve güvenlik kontrollerinden geçmiştir.

4.3.2. Kişisel Geçmiş Kontrol Gereklilikleri

TÜRKTRUST'ta çalışan personelin özgeçmişi ve referansları ayrıntılı bir şekilde değerlendirilmekte, işe teknik ve idari açıdan uygunluğundan emin olunmaktadır. Uygun nitelikte olduğu belirlenen kişiler için adli sicil belgesi istenir ve gerekiyorsa güvenlik soruşturması yapılır.

4.3.3. Eğitim Gereklilikleri

TÜRKTRUST personeli göreve başlamadan önce sorumlulukları kapsamında eğitimden geçirilir. Eğitim süresince, çalışanlar temel zaman damgası iş süreçleri; işlevsel prosedürler ve talimatlar; bilgi güvenliği ilkeleri ve mevcut bilgi güvenliği yönetim sistemi; kullanılacak yazılım ve donanım birimleri hakkında ayrıntılı olarak bilgilendirilir.

4.3.4. Tekrar Eğitimi Sıklığı ve Gereklilikleri

Çalışanlara yönelik eğitim, göreve başlanırken verilen ilk eğitimin ardından periyodik olarak ve diğer gerekli görülen durumlarda tekrarlanır. Sürekli olarak yürütülen ölçme ve

© 2005 - 2013 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. Tüm hakları saklıdır.

değerlendirme çalışmalarının sonuçları ışığında ilgili personelin eğitim ihtiyacı belirlenir ve periyodik eğitimlerin yanı sıra verimin artırılmasına yönelik ek eğitim seansları da düzenlenebilir. Verilen eğitimlerin konuları ve kapsamı, gelişen teknoloji ve yenilenen yazılım ve donanım birimlerine uygun olarak sürekli güncellenir ve yenilenir.

4.3.5. Yetkisiz İşlemler için Yaptırımlar

TÜRKTRUST personelinin teşebbüs edeceği yetkisiz işlemler için, TÜRKTRUST insan kaynakları yönergesi uyarınca gerekli disiplin cezaları uygulanır. Eğer bu yetkisiz işlem sonucunda TÜRKTRUST ya da TÜRKTRUST müşterileri zarar görürse, bu zararın ilgili çalışandan tazmini yoluna gidilir.

TÜRKTRUST yetkisiz işlem yapanlar hakkında, Kanun, Yönetmelik ve Tebliğ gereğince işlem yapılmasını temin etmek üzere, adli mercilere başvuruda bulunur.

4.3.6. Bağımsız Alt Yüklenici Gereklilikleri

Zaman damgası süreçleri dahilinde alt yükleniciler aracılığıyla yürütülen işlemler için, TÜRKTRUST ile alt yüklenici firma arasında bir hizmet sözleşmesi imzalanır. Bu hizmet sözleşmesi TÜRKTRUST'ın gerektirdiği güvenlik koşullarını ve hizmet esaslarını ortaya koyar.

4.3.7. Personele Sağlanan Dokümantasyon

TÜRKTRUST personeline, ZDİ ve ZDUE kitapçıkları, zaman damgası süreçleriyle ilgili uygulama ve güvenlik prosedürler ile talimatları, çalışanların rollerine göre düzenlenmiş iş tanımları, kullanılan yazılım ve donanım birimlerinin kullanım kılavuzları sağlanır.

4.4. Denetim Kayıtları Alma Prosedürleri

4.4.1. Kaydedilen Olay Tipleri

Zaman damgası hizmetlerine ait tüm kayıtlar TÜRKTRUST tarafından tutulur. Bu kayıtların arasında zaman damgası başvuru kayıtları; üretilen zaman damgaları hakkındaki kayıtlar; TÜRKTRUST zaman damgası işlemlerine dahil olan tüm yönetici ve operatörlerin işlem kayıtları; çalışanların TÜRKTRUST 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.

4.4.2. Kayıtları İşleme Sıklığı

Denetim kayıtları sürekli olarak tutulur ve periyodik olarak bu kayıtların yedekleri alınarak arşivlenir.

4.4.3. Denetim Kayıtlarının Saklanma Süresi

TÜRKTRUST işleyişine ait denetim kayıtları, aktif tutulma süresince sistemde tutulur. Bu sürenin sonunda yasal düzenlemeler uyarınca saklanmak üzere arşivlenir.

4.4.4. Denetim Kayıtlarının Korunması

Denetim kayıtları fiziksel ve elektronik güvenlik önlemleriyle korunur, sadece yetkili kişilerin erişimine açık tutulur. Denetim kayıtlarının veri bütünlüğü anahtarlanmış özet yöntemiyle sağlanmaktadır.

© 2005 - 2013 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. Tüm hakları saklıdır.

4.4.5. Denetim Kayıtlarının Yedeklenme Prosedürleri

İlgili prosedürler uyarınca, kayıtların periyodik olarak tesis içi ve tesis dışı yedekleri alınır.

4.4.6. Denetim Bilgisi Toplama Sistemi (İç ve Dış)

Denetim kayıtları, ESHS iş süreçlerinin yürütülmesinde kullanılan ESHS yönetim yazılımı tarafından tutulur.

4.4.7. Olayı Yaratan Kişiyi Bilgilendirme

Rutin işlemlerin dışında kalan denetim kayıtlarının oluştuğu durumlarda, olayı yaratan kişi sistem tarafından uyarılır. Olayın çeşidine ve önemine göre, sistem üzerinde olayı yaratan kişinin yönetiminden sorumlu üst yetki seviyesindeki kişi veya kişiler de bilgilendirilebilir.

4.4.8. Zarar Görebilirlik Değerlendirmesi

Denetim kayıtları sistem üzerinde raporlanır. Bu raporların analiz edilmesiyle sistemdeki güvenlik açıkları ve zaman damgası süreçlerindeki hata noktaları belirlenerek önlem alınmaktadır.

4.5. Kayıtların Arşivlenmesi

4.5.1. Arşivlenen Kayıt Tipleri

TÜRKTRUST işleyişi uyarınca, Madde 5.4.'te belirtilen tüm denetim kayıtları, müşterilerle yapılan tüm yazışmalar, ZDİ ve ZDUE kitapçıklarının tüm sürümleri, uygulama prosedürlerinin, talimatların ve formların bütünü, TÜRKTRUST arşiv prosedürleri uyarınca arşivlenir. Arşivlerin büyük bir kısmı elektronik ortamda tutulurken, kağıt üzerindeki yazışmalar, formlar ve belgeler de kağıt ortamında arşivlenir.

4.5.2. Arşivlerin Saklanma Süresi

TÜRKTRUST zaman damgası hizmetlerine ait arşivler, yasal düzenlemeler uyarınca en az 20 yıl süreyle saklanır.

4.5.3. Arşivlerin Korunması

Arşivler fiziksel ve elektronik güvenlik önlemleriyle korunur, sadece yetkili kişilerin erişimine açık tutulur.

Elektronik arşivlerin yetkili olmayan kişiler tarafından görülmesi, değiştirilmesi veya silinmesi önlenmiştir. Kağıt üzerindeki arşivler ise sadece yetkili kişilerin girme izni bulunan özel birimlerde tutulurlar.

4.5.4. Arşivlerin Yedeklenme Prosedürleri

İlgili prosedürler uyarınca, elektronik ortamdaki arşivlerin yedekleri tutulur. Kağıt ortamdaki arşivlerin ise yedekleri alınmaz.

4.5.5. Kayıtların Zaman Damgası Altına Alınması Gereklilikleri

TÜRKTRUST tarafından saklanan tüm elektronik arşiv kayıtları elektronik olarak imzalı ve zaman damgalıdır.

4.5.6. Arşiv Toplama Sistemi

Arşiv kayıtları, TÜRKTRUST arşiv yönetim sistemi kullanılarak ilgili prosedürler uyarınca derlenir.

© 2005 - 2013 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. Tüm hakları saklıdır.

4.6. Güvenliğin Yitirilmesi ve Felaket Kurtarma

4.6.1. Güvenlik Kaybına Neden Olabilecek Olaylar

TÜRKTRUST işleyişini engelleyecek nitelikte olayların ya da güvenlik sorunlarının oluşması durumunda, TÜRKTRUST bilgi güvenliği ihlal olayı, iş sürekliliği yönetimi prosedürleri ve iş sürekliliği planları uyarınca duruma müdahale edilir. TÜRKTRUST personeli tarafından fark edilerek raporlanan ihlal olayları ve güvenlik açıklarına müdahale ve sorun giderme yöntemleri bahsi geçen dokümanlarda açıkça ifade edilmiştir.

4.6.2. Bilgisayar Kaynakları, Yazılım ve/veya Verilerin Bozulmuş Olması

Bilgisayar kaynaklarının zarar görmesi, yazılım birimlerinde veya işleyişe dair verilerde bozulma oluşması durumunda, öncelikle tesisteki hasarlı donanım yeniden işler hale getirilir. Daha sonra, kaybolan kayıtlar yedekleme sistemleri aracılığıyla yeniden oluşturulur ve zaman damgası hizmetleri tekrar etkin hale getirilir. Eğer tam olarak işler hale getirilemez veya kayıtların bazıları yeniden elde edilemez ise, bu durumdan etkilenebilecek olan bütün zaman damgası kullanıcıları ile üçüncü kişiler ivedilikle bilgilendirilir.

4.6.3. İmza Oluşturma Verilerinin Güvenliğinin Yitirilmesi

TÜRKTRUST imza oluşturma verilerinin güvenliğinin ve güvenilirliğinin yitirilmesi durumunda, TÜRKTRUST iş sürekliliği yönetimi prosedürleri ve iş sürekliliği planları uyarınca yeni imza oluşturma verisi oluşturularak devreye alınır.

4.6.4. İş Sürekliliği Yetenekleri ve Felaket Kurtarma

TÜRKTRUST merkezi dışında felaket kurtarma merkezi (FKM) tesis etmiştir. Afet sonrasında iş sürekliliğini temin etmek üzere TÜRKTRUST merkezinde bulunan veriler yedeklenir. Özellikle, bir ihtiyacın ortaya çıkması durumunda FKM aracılığıyla OCSP veya SİL gibi gerçek zamanlı web hizmetleri ile zaman damgası hizmetleri en fazla 2 saatlik sürede hazır hale getirilebilir.

TÜRKTRUST işleyişini engelleyecek nitelikte olayların ya da güvenlik sorunlarının oluşması durumunda, TÜRKTRUST iş sürekliliği yönetimi prosedürleri ve iş sürekliliği planları uyarınca duruma müdahale edilir.

4.7. TÜRKTRUST'ın Faaliyetlerinin Son Bulması

TÜRKTRUST, zaman damgası hizmetlerine son vermesi durumunda, Kanun ve Yönetmelik gereği bu durumu en az 3 ay önce Kuruma bildirir ve kamuoyuna duyurur. TÜRKTRUST, faaliyetinin durdurulması prosedürü uyarınca, zaman damgası hizmetlerini başka bir ESHS'ye devredebilir.

© 2005 - 2013 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. Tüm hakları saklıdır.

5. TEKNİK GÜVENLİK KONTROLLERİ

ZDUE kitapçığının bu kısmında, TÜRKTRUST'ın zaman damgası hizmetleriyle ilgili iş süreçlerinde kullanılan imza oluşturma verilerinin ve erişim verilerinin yönetimi ile teknik altyapıya ve zaman damgası hizmetlerinin işleyişine yönelik güvenlik kontrolleri yer almaktadır.

5.1. ESHS Anahtar Çifti Yönetimi

5.1.1. Anahtar Çifti Üretimi ve Korunması

TÜRKTRUST zaman damgası kök ve alt kök sertifikalarına ait anahtar çiftleri, sadece yetkili kişilerin kontrolünde, iki yetkilinin hazır bulunmasıyla, teknik ve idari güvenlik önlemleri alınmış ortamlarda, TÜRKTRUST zaman damgası kök ve alt kök sertifika üretim, yayımlama ve imha prosedürü uyarınca üretilir ve uygun biçimde yedeklenir. İmza oluşturma verisi yetkisiz erişime karşı fiziksel ve teknik güvenlik önlemleriyle korunur.

TÜRKTRUST kök ve alt kök sertifikaları anahtar çifti üretiminde en az EAL4+ veya FIPS 140-2 Düzey 3 güvenlik düzeyinde kriptografik güvenlik donanım modülü kullanılır. Anahtar çiftlerinin uzunluğu ve kullanılacak algoritmalar güncel mevzuat ve standartlarla uyumlu olacak şekilde yapılır. Aynı şekilde üretilen anahtar çiftinin ömrü güncel mevzuat, standartlar ve anahtarların kriptografik güvenlik süresiyle sınırlandırılmıştır. Bir kök veya alt kök sertifikasının geçerlilik süresi sonundan yeterince makul bir süre önce yeni bir anahtar çifti ve sertifika üretilerek hizmetin kesintisiz bir biçimde devam etmesi sağlanır.

TÜRKTRUST donanım güvenlik modülleri, fiziksel ve elektronik her türlü müdahaleye karşı koruma altında tutulur ve çalıştırılır. Modüllerde bulunan verinin güvenli yedekleri ilgili prosedürlere göre alınır ve saklanır. Böylece fiziksel ve ekonomik ömrünü tamamlamış bir modülün içindeki anahtarlar Bölüm 5.1.11'de belirtildiği gibi yok edilir ve yeni modüllerde kullanılmak üzere gerekli yedekler başka ortamlarda saklanır.

5.1.2. TÜRKTRUST İmza Doğrulama Verilerinin Üçüncü Taraflara Ulaştırılması

TÜRKTRUST zaman damgası kök ve alt kök sertifikaları üçüncü tarafların erişebileceği şekilde yayımlanır. Böylelikle, TÜRKTRUST'a ait imza doğrulama verileri üçüncü taraflarca kullanılabilir.

5.1.3. Anahtar Uzunlukları

TÜRKTRUST sertifikaları, Tebliğ'le belirlenen minimum anahtar uzunluklarına uygundur. TÜRKTRUST sertifika üretim merkezlerinin kök ve alt kök sertifikaları üretilirken 2048 bit RSA anahtar çiftleri kullanılır.

5.1.4. Anahtar Üretimi ve Kalite Kontrolü

Anahtar üretiminin TÜRKTRUST merkezinde veya bağlı kayıt merkezlerinde olması durumunda, anahtar çifti uygun güvenlik düzeyine sahip donanım güvenlik modüllerinde, Tebliğ'de belirlenen parametrelere uygun olarak üretilir.

Anahtar üretiminin müşteri tarafında olduğu durumlarda, imza oluşturma verisinin uygun araçlarda ve nitelikte üretiminden müşteri sorumludur.

© 2005 - 2013 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. Tüm hakları saklıdır.

5.1.5. Anahtar Değişimi

TÜRKTRUST zaman damgası kök ve alt kök sertifikalarının anahtar yenileme işlemleri, TÜRKTRUST merkezi tarafından yönetilir.

5.1.6. Kriptografik Modül Standartları ve Kontroller

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

Satınalma sonrası donanım güvenlik modülünün ilk kullanımından önce, sevkiyat ve depolama sırasında cihazların zarar görmediğinden emin olmak için kontroller uygulanır. Cihazların kabulü sırasında fabrika paketlemesi ve güvenlik mühürleri kontrol edilir ve cihazlar fiziksel ve teknik bakımdan güvenliği sağlanmış alanlarda saklanır ve kullanılır. Cihazların tüm kullanım ömürleri boyunca, cihazlar işlevsellikleriyle ilgili sürekli kontrol altında tutulur ve herhangi bir güvenlik ihlali durumu bilgi güvenliği ihlal olayı prosedürü uyarınca yönetilir.

TÜRKTRUST'a bağlı sertifika üretim merkezlerinin kök ve alt kök sertifikalarına erişim, yetkili kişiler dışında yasaklanmıştır. Fiziksel ve teknik erişim kontrollerinin yanı sıra, bu imza oluşturma verilerinin kullanımı, ilgili modüle aynı anda iki ayrı yetkilinin bağlanması ve sistem tarafından onaylanmasıyla mümkündür. Sistem, hiçbir yetkilinin tek başına TÜRKTRUST imza oluşturma verilerini kullanabilmesine izin vermez.

5.1.7. İmza Oluşturma Verisinin Yedeklenmesi

Herhangi bir felaket durumu veya sorun anında hizmetlerin kesintiye uğramaması amacıyla, TÜRKTRUST zaman damgası kök ve alt kök sertifikalarına bağlı imza oluşturma verileri, TÜRKTRUST kök ve alt kök üretim, dağıtım, yayımlama ve imha prosedürü uyarınca yedeklenir ve fiziksel ve teknik güvenlik kontrolleri altında saklanır. Bu işlem için kök ve alt kök sertifikalara bağlı imza oluşturma verilerinin yedeklenmesi prosedürü uygulanır.

5.1.8. İmza Oluşturma Verisinin Kriptografik Modül Transferi

ESHS kök ve alt kök sertifikalarına ait imza oluşturma verileri güvenli kriptografik donanım modüllerinde üretilir. Bu veriler yedekleme amacıyla kullanılan güvenli modüllere transferi dışında hiçbir biçimde modül dışına çıkarılamaz. Yedekleme işlemi, kriptografik donanım modülü üzerinde şifreli bir biçimde gerçekleştirilir.

5.1.9. İmza Oluşturma Verisinin Kriptografik Modülde Saklanması

TÜRKTRUST sertifika üretim merkezlerinin zaman damgası kök ve alt kök sertifikalarına bağlı imza oluşturma verileri, üretildikleri ve Tebliğ'de tanımlı güvenlik düzeyine sahip kriptografik donanım modüllerinde saklanır.

5.1.10. İmza Oluşturma Verisinin Aktive Edilme Yöntemi

TÜRKTRUST sertifika üretim merkezlerinin zaman damgası kök ve alt kök sertifikalarına bağlı imza oluşturma verileri, içinde bulundukları donanım güvenlik modülü üzerinde, iki yetkilinin hazır bulunmasıyla aktive edilir.

5.1.11. İmza Oluşturma Verisinin Deaktive Edilme Yöntemi

TÜRKTRUST sertifika üretim merkezlerinin zaman damgası kök ve alt kök sertifikalarına bağlı imza oluşturma verileri, 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.

© 2005 - 2013 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. Tüm hakları saklıdır.

5.1.12. İmza Oluşturma Verisi Yok Etme Metodu

TÜRKTRUST sertifika üretim merkezlerinin zaman damgası kök ve alt kök sertifikalarına bağlı imza oluşturma verilerinin tüm kopyaları, sertifika geçerlilik süreleri sonunda, içinde bulundukları donanım güvenlik modüllerinin anahtar silme özelliği kullanılarak sadece yetkili kişiler tarafından yok edilir ve yapılan işlemler prosedürler uyarınca kayıt altına alınır. Bu işlem için en az iki kişinin aynı anda hazır bulunması gerekir.

5.1.13. Kriptografik Modül Değerlendirmesi

TÜRKTRUST sertifika üretim merkezlerinin zaman damgası kök ve alt kök sertifikalarına bağlı imza oluşturma verileri, Tebliğ'de tanımlı güvenlik düzeyine sahip kriptografik donanım modüllerinde üretilir ve saklanır.

5.1.14. İmza Doğrulama Verilerinin Arşivlenmesi

TÜRKTRUST sertifika üretim merkezlerinin zaman damgası kök ve alt kök sertifikalarına bağlı imza doğrulama verileri, ESHS tarafından 20 yıl süreyle saklanır.

5.1.15. Sertifikanın İşlevsel Süreleri ve Anahtar Çifti Kullanım Süreleri

TÜRKTRUST sertifika üretim merkezlerinin zaman damgası kök ve alt kök sertifikalarının geçerlilik süreleri 10 yılı aşmaz. Bu sürenin sonunda sertifikalar yenilenirken mutlaka anahtar yenileme yapılır.

5.2. Erişim Şifreleri

5.2.1. Erişim Şifrelerinin Oluşturulması ve Kurulumu

Erişim şifresi, gizli anahtar yönetiminde kullanılan parola, şifre, PIN ya da benzeri özel verilere karşılık gelir.

TÜRKTRUST alt kök ve kök sertifikalarına ait anahtarların üretimi ve bu anahtarlara ait erişim şifrelerinin oluşturulması, Kök ve Alt Kök Sertifika Üretim Yayımlama ve İmha Prosedürü'nde açıklanan törene göre yapılır. Bölüm 5.1.6'da açıklandığı gibi kök ve alt kök sertifikaların gizli anahtarlarının bulunduğu kriptografik modüllere erişim ve anahtarların kullanılması erişim şifrelerine sahip iki yetkilinin aynı anda bulunmasıyla mümkündür.

5.2.2. Erişim Şifrelerinin Korunması

TÜRKTRUST kök ve alt kök sertifikalarına ait gizli anahtarları kullanan yetkili kişiler, erişim şifrelerini en geç 90 (doksan) günde bir değiştirirler. Yetkili kişiler, erişim şifrelerinin gizliliğinden ve korunmasından sorumludur.

5.3. Bilgisayar Güvenlik Kontrolleri

TÜRKTRUST tarafından yürütülen zaman damgası iş süreçleri kapsamında, tüm bilgi sistemlerine erişim ve bu sistemlerin işletilmesi için aşağıda yer alan güvenlik kontrolleri uygulanmaktadır:

- Bilgisayar sistemlerinde güvenilir ve sertifikalı donanım ve yazılım ürünleri kullanılmaktadır.
- Bilgisayar sistemleri yetkisiz erişime ve güvenlik açıklarına karşı korunmuştur. Penetrasyon ve istemsiz erişim kontrolleri kurulmuş ve ilgili testlerle kontrollerin güncelliği ve sürekliliği sağlanmıştır.

© 2005 - 2013 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. Tüm hakları saklıdır.

- Bilgisayar sistemleri, virüslere, kötü niyetli ve yetkisiz yazılımlara karşı korunmaktadır.
- Bilgisayar sistemleri ağ güvenliği saldırılarına karşı korunmuştur.
- Bilgisayar sistemlerine erişim hakları ve kimlik doğrulama, TÜRKTRUST personeline verilen şifrelerle sağlanmaktadır.
- Bilgisayarlara erişim hakları, yetkili personele tanımlanan rollerle sınırlanmıştır.
- Bilgisayar sistemini oluşturan birimler arasındaki veri iletişimi güvenli olarak yapılmaktadır.
- İşlem kayıtları sürekli olarak tutulduğu için bilgisayar sistemlerinde oluşabilecek sorunlar kısa zamanda ve doğru biçimde belirlenebilmektedir.
- TÜRKTRUST, değişikliklere karşı korunmuş güvenilir sistemler ve ürünler kullanır. Bu bağlamda, Bilgi Teknolojileri ve İletişim Kurumu'nun sürekli denetimi altında, CWA 14167-1 standardının önerileri kesin olarak uygulanır.

5.4. Yaşam Döngüsü Teknik Kontrolleri

5.4.1. Sistem Geliştirme Kontrolleri

Sistem geliştirme kontrolleri, geliştirme tesisi güvenliği (tesis güvenlik belgeleri aracılığıyla), geliştirme ortamı güvenliği, geliştirme personeli güvenliği, ürün bakımı sırasında konfigürasyon yönetimi güvenliği ve yazılım geliştirme metodolojisi (ISO/IEC 27001 ve ISO 9001 belgeleri aracılığıyla) için uygulanır. Bu konular ve değişim yönetimi hakkındaki ayrıntılar, Bilgi Sistemleri Edinim, Geliştirme ve Bakım Prosedüründe dokümante edilmiştir.

5.4.2. Güvenlik Yönetimi Kontrolleri

İşlevsel sistemler ve TÜRKTRUST içinde kullanılan bilgisayar ağının güvenliğinin sağlanması için uygun araçlar kullanılmakta ve güvenlik prosedürleri işletilmektedir.

TÜRKTRUST, ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemleri standardı sertifikası sahibidir.

5.4.3. Yaşam Döngüsü Güvenlik Kontrolleri

Uygulama dışıdır.

5.5. Ağ Güvenlik Kontrolleri

TÜRKTRUST sertifika üretim merkezlerinin zaman damgası kök ve alt kök sertifikalarının imza oluşturma verileri, ağ güvenliği sağlanmış ortamlarda kullanılmaktadır. Bu sistemler fiziksel ve teknik olarak korunurlar.

TÜRKTRUST içindeki diğer tüm sistemler de uygun ağ güvenliği yöntemleriyle korunmaktadır. Güvenlik duvarları, anahtarlama cihazları ve yönlendiriciler gibi tüm ağ elemanları, doğru ve güvenli bir biçimde ağ konfigürasyonu prosedürleri uyarınca kurulmuştur. Bu ağ elemanlarının güvenlik kontrolleri prosedürler uyarınca sürekli olarak yapılmaktadır. Ayrıca TÜRKTRUST, ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemleri standardı sertifikası sahibidir.

© 2005 - 2013 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. Tüm hakları saklıdır.

6. ZAMAN DAMGASI PROFİLLERİ

TÜRKTRUST zaman damgası hizmetlerine ait zaman damgası başvuru ve cevap profilleri, ETSI TS 101 861 dokümanında belirlenen profillere uygundur. TÜRKTRUST zaman damgalarında, seri numarası, zaman damgası verilen veri, uygulanan ilke nesne tanımlayıcısı ve zaman bilgisi yer alır.

6.1.1. Başvurularda Algoritma Nesne Tanımlayıcıları

TÜRKTRUST, SHA-256, SHA-384, SHA-512 ve WHIRLPOOL özet algoritmaları kullanılarak oluşturulmuş özet verileri için zaman damgası hizmetleri verir. Bu algoritmalar dışında kalan algoritmalarla üretilmiş veriler için gönderilen başvurular reddedilir.

6.1.2. Zaman Damgasında Algoritma Nesne Tanımlayıcıları

TÜRKTRUST tarafından üretilen zaman damgalarında özetleme algoritması olarak SHA256, elektronik imza için RSA kullanılır.

© 2005 - 2013 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. Tüm hakları saklıdır.

7. UYGUNLUK DENETİMİ VE DİĞER DEĞERLENDİRMELER

TÜRKTRUST, ilgili mevzuat gereğince Bilgi Teknolojileri ve İletişim Kurumu tarafından denetlenir.

Ayrıca, tüm ESHS süreçleri, bilgi güvenliği yönetim sisteminin sürekliliği açısından ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi ve TS EN ISO 9001 Kalite Yönetim Sistemi sertifikaları uyarınca periyodik olarak uygunluk denetimine tabi tutulur.

ESHS hizmetlerinin verilişi ve işletmeye dair güvenlik koşulları bir iç denetim planı uyarınca kontrol altında tutulur.

TÜRKTRUST, ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemine göre risk değerlendirmelerini gerçekleştirir. Bunun sonucunda, iş riskleri değerlendirilir ve gerekli güvenlik koşulları ve işletim prosedürleri belirlenir. Risk analizi düzenli olarak gözden geçirilir ve gerektiğinde güncelleme yapılır.

7.1. Denetim Sıklığı ve Durumları

Bilgi Teknolojileri ve İletişim Kurumu, düzenleyici ve denetleyici Kurum olarak gerekli gördüğü durumlarda re'sen ve iki yılda en az bir defa resen denetim yapar. Denetleme sırasında, denetleme yapmaya yetkili görevliler tarafından her türlü defter, belge ve kayıtların verilmesi, yönetim yerleri, binalar ve eklentilerine girme, yazılı ve sözlü bilgi alma, örnek alma ve işlem ve hesapları denetleme isteminin elektronik sertifika hizmet sağlayıcıları ve ilgililer tarafından yerine getirilmesi zorunludur.

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi sertifikası uyarınca, her yıl takip denetiminden ve her üç yılda bir de belge yenileme denetiminden geçilir.

İç denetim, plan gereği yılda en az bir defa, gerek görülmesi durumunda daha fazla sayıda tekrar edilir.

7.2. Denetçinin Kimliği ve Özellikleri

Bilgi Teknolojileri ve İletişim Kurumu, Kanunla belirlenmiş düzenleyici ve denetçi kurumdur.

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi sertifikasyonu yetkilendirilmiş bir denetçi tarafından gerçekleştirilir.

TÜRKTRUST'ın kurumsal iç denetimi, TÜRKTRUST yetkili personeli tarafından yapılır. İç denetim, TÜRKTRUST bünyesindeki Bilgi Güvenliği Yönetim Sistemi Sorumlusu ve Kalite Sistemi Sorumlusu tarafından yürütülür.

7.3. Denetçinin ESHS'yle İlişkisi

Denetçi kuruluş olan Kurum, Kanun gereği Türkiye'de nitelikli elektronik sertifikalar ve zaman damgasıyla ilgili faaliyet gösteren tüm ESHS'leri denetlemekle yetkili kılınmış düzenleyici kuruluştur.

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi sertifikasyonu bağımsız ve yetkili bir denetçi tarafından gerçekleştirilir.

TÜRKTRUST'ın kurumsal denetimi, TÜRKTRUST yetkili personeli tarafından yapılır.

© 2005 - 2013 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. Tüm hakları saklıdır.

7.4. Denetimde Kapsanan Başlıklar

Kurum'un denetimi Kanunla kendisine verilen yetki çerçevesinde, TÜRKTRUST'ın elektronik sertifika ve zaman damgası hizmetlerine dair tüm süreçleri, bu hizmetlerin yerine getirilmesi sırasında kullanılan teknik altyapı ve hizmetlerin verildiği tesisleri kapsar.

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi sertifikasyonu, TÜRKTRUST elektronik sertifika ve zaman damgası hizmetleri kapsamındadır.

İç denetimde de, yasal denetim altına giren tüm konular kapsanır.

7.5. Eksiklik Durumunda Yapılacaklar

Yönetmelik gereği Kurum tarafından yapılan denetimler sırasında, TÜRKTRUST'ın faaliyet ve işleyişini olumsuz yönde etkileyebilecek derecede önemli konuların belirlenmesi durumunda, ilgili mevzuatta öngörülen yaptırım ve cezalar uygulanır.

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi denetimleri sırasında saptanan eksikliklerin majör nitelikte olması sertifikanın geri alınmasına neden olur. Minör eksikler, bir sonraki denetim dönemine kadar TÜRKTRUST tarafından giderilir.

TÜRKTRUST tarafından yapılan iç denetimlerde belirlenen aksaklıklar hakkında düzeltici ve önleyici faaliyetler yürütülür.

7.6. Sonuçların Bildirilmesi

Kanun gereği Kurum tarafından yapılan denetimin sonuçları gerek duyulduğu takdirde resmi yollarla TÜRKTRUST'a iletilir. Kurum'un bir geri bildirimde bulunmaması, olumsuz bir değerlendirmenin olmadığı anlamını taşır.

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi denetim sonuçları, denetçi tarafından resmi olarak TÜRKTRUST'a bildirilir.

İç denetim sonuçları ise, iç denetim sonuç raporunda yer alır ve ilgili yetkililerin değerlendirmesine sunulur.

© 2005 - 2013 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. Tüm hakları saklıdır.

8. DİĞER İŞ KONULARI VE YASAL KONULAR

ZDUE kitapçığının bu kısmında, TÜRKTRUST'ın ticari ve yasal uygulamaları ile zaman damgası faaliyetleri uyarınca yerine getirilmesi gereken hizmet koşulları yer almaktadır.

8.1. Ücretler

8.1.1. Zaman Damgası Hizmet Ücretleri

TÜRKTRUST tarafından verilen zaman damgası hizmetlerinin güncel fiyat bilgileri, TÜRKTRUST web sitesi ve uygun görülen diğer iletişim kanalları üzerinden müşterilere duyurulur.

8.1.2. Diğer Hizmetlerin Ücretleri

TÜRKTRUST, kamuya açık olarak yayımladığı ZDİ, ZDUE gibi kitapçık ve belgeler için ücret talep etmez.

Bunların dışında kalan ve katma değerli olarak üretilerek müşterilere sunulan diğer ürün ve hizmetler için uygulanacak ücretler, web sitesi ve uygun görülen diğer iletişim kanalları üzerinden müşterilere duyurulur.

8.1.3. Bedel İadesi

TÜRKTRUST, zaman damgası hizmetleriyle ilgili olarak bedel iadesi yapmaz. Ancak, TÜRKTRUST'tan kaynaklanan nedenlerle, zaman damgası içeriğinde sorun bulunması durumunda, her hangi bir ücret talep edilmeden başka bir zaman damgası verilir.

8.2. Finansal Sorumluluk

TÜRKTRUST, Kanun'dan doğan yükümlülüklerini yerine getirmemesi sonucu doğacak zararların karşılanması amacıyla sertifika mali sorumluluk sigortası yaptırmakla yükümlüdür. Sigortaya ilişkin koşullar 26 Ağustos 2004 tarih ve 25565 sayılı Resmi Gazetede yayımlanmış olan "Sertifika Mali Sorumluluk Sigortası Yönetmeliği" ve ilgili tebliğlerde yer almaktadır.

"Sertifika Mali Sorumluluk Sigortası Yönetmeliği" Madde 6 uyarınca, sertifika mali sorumluluk sigortası, ESHS'nin güvenli ürün ve sistemleri kullanma, hizmeti güvenilir bir biçimde yürütme ve zaman damgalarının taklit ve tahrif edilmesini önlemekle ilgili yükümlülüklerini yerine getirmemesi dolayısıyla zarar görecek olanlara karşı doğacak hukuki sorumlulukların teminat altına alınmasını kapsar.

8.3. İş Bilgisinin Gizliliği

8.3.1. Gizli Bilginin Kapsamı

TÜRKTRUST'ın zaman damgası hizmetlerine yönelik ESHS işlevleriyle ilgili her türlü ticari gizli bilgi ve belge, TÜRKTRUST zaman damgası kök ve alt kök sertifikalarının imza oluşturma verileri, kullanılan yazılım ve donanım bilgileri, işlem kayıtları, denetim raporları, tesis içi bölge ve cihazlara ait erişim şifreleri, tesis planı ve iç tasarımı, acil eylem planları, iş planları, satış bilgileri, işbirliği sözleşmeleri, iş ortaklığı yapılan kuruluşlara ait gizlilik dereceli bilgiler gizli bilgi kapsamına girer.

8.3.2. Gizlilik Kapsamı Dışındaki Bilgi

TÜRKTRUST'ın ticari gizliliği olmayan, Kanun ve uygulamalar gereği kamuya açık olması gereken bilgi ve belgeleri gizlilik kapsamı dışında tutulur. Zaman damgası hizmetleriyle

© 2005 - 2013 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. Tüm hakları saklıdır.

ilgili müşteri prosedürleri, ZDİ kitapçığı, ZDUE kitapçığının içeriğindeki bilgiler gizlilik kapsamına girmez.

8.3.3. Gizli Bilginin Korunması Sorumluluğu

TÜRKTRUST çalışanlarının tamamı gizli bilgilerin korunması konusunda sorumluluk sahibidir. Güvenlik politikaları gereği hiçbir gizli bilgiye, yetkilisi dışındaki çalışanların ya da üçüncü kişilerin erişimine izin verilmez. Bilgi güvenliğinin sağlanmasıyla ilgili tüm prosedürler çalışanlar tarafından eksiksiz uygulanır ve bu prosedürlerin uygulanması TÜRKTRUST iç denetimine tabidir.

8.4. Kişisel Bilgilerin Gizliliği/Özelliği

8.4.1. Gizlilik Planı

TÜRKTRUST, verdiği zaman damgası hizmetleri kapsamında, zaman damgası başvuru sahiplerine ya da diğer taraflara ait kişisel bilgilerin gizliliğini korur.

8.4.2. Özel Olarak Değerlendirilecek Bilgi

TÜRKTRUST tarafından zaman damgası hizmetlerinin verilmesi sırasında ihtiyaç duyulan ve zaman damgası başvuru sahiplerinden alınmış olan müşteri bilgileri, özel bilgi olarak değerlendirilir.

8.4.3. Özel Bilgiyi Koruma Sorumluluğu

TÜRKTRUST çalışanlarının tamamı başvuru sahiplerine ve müşterilere ait özel bilgilerin korunması konusunda sorumluluk sahibidir. Hiçbir özel bilgiye, yetkilisi dışındaki çalışanların ya da üçüncü kişilerin erişimine izin verilmez.

8.4.4. Yargısal ve İdari Süreçlere Uygun Olarak Bilginin Açıklanması

Hukuki veya idari süreçler gereği ihtiyaç duyulan özel kişisel bilgiler, sadece talep sahibi resmi makama verilir.

8.5. Fikri Mülkiyet Hakları

TÜRKTRUST tarafından üretilen zaman damgası hizmetleriyle ilgili müşteri prosedürleri, ZDİ ve ZDUE kitapçıkları, zaman damgası hizmetlerinin yürütülmesiyle ilgili her türlü iç ve dış doküman, veri tabanları, web siteleri ile zaman damgası hizmetlerine bağlı olarak geliştirilen tüm ürünlerin fikri mülkiyet hakları TÜRKTRUST'a aittir.

Zaman damgası başvuru sahipleri, zaman damgası içeriğinde yer alan ve kendilerine ait elektronik verilerinin mülkiyet haklarına sahiptir.

8.6. Tarafların sorumlulukları

TÜRKTRUST, yasal mevzuat, ZDİ ve bu ZDUE kitapçığında belirlenen ilke ve esaslara göre zaman damgası hizmetlerini kesintisiz bir biçimde verir.

Zaman damgası sahipleri ve üçüncü taraflar, zaman damgasını doğrulamaktan kendileri sorumludur.

8.7. Tazminatlar

TÜRKTRUST, bu ZDİ ve ZDUE'de yer alan ilke ve esaslar gereği yükümlülüklerini yerine getiremez ve bu durumdan üçüncü kişilerin zarar gördüğü hukuken belirlenirse, yasal

© 2005 - 2013 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. Tüm hakları saklıdır.

mevzuat uyarınca ilgili zarar TÜRKTRUST tarafından tazmin edilir. TÜRKTRUST kusursuzluğunu ispat ettiği takdirde tazminat ödeme yükümlülüğü doğmaz.

8.8. ZDUE Kitapçığının Geçerliliği

8.8.1. ZDUE Kitapçığının Geçerlilik Dönemi

ZDUE kitapçığının bu sürümü, yeni bir sürüm çıkarılana kadar geçerlidir.

8.8.2. ZDUE Kitapçığının Geçerliliğinin Sona Ermesi

TÜRKTRUST faaliyetlerinde ve zaman damgası hizmetlerinde oluşabilecek değişikliklere ve düzenlemelere bağlı olarak, ZDUE kitapçığının mevcut sürümünün içeriğinin değişmesini gerektiren herhangi bir durum ortaya çıktığında, kitapçık kısmen ya da tamamen geçersiz duruma düşebilir. Bu durumda, ilgili değişikliklerin yansıtıldığı yeni bir ZDUE kitapçığı sürümü TÜRKTRUST tarafından hazırlanır ve yayımlanır.

8.8.3. Geçerliliğin Sona Ermesinin Etkileri ve İşlerliğin Sürdürülmesi

Mevcut ZDUE sürümünün geçerliliğinin sona ermesi durumunda, TÜRKTRUST faaliyetlerinin ve zaman damgası hizmetlerinin kesintiye uğramaması için gerekli önlemler alınır. Yeni ZDUE sürümü, eski ZDUE sürümünün geçerliliği sona ermeden hazırlanır ve değişim hizmet kesintisi olmadan gerçekleştirilir.

8.9. Taraflara Özel Duyurular ve İletişim

TÜRKTRUST tarafından zaman damgası kullanıcılarına yapılacak olan duyurular için zaman damgası kullanıcılarının uygun olan iletişim bilgileri kullanılır. TÜRKTRUST'ın üçüncü taraflara yapacağı duyurular web üzerinden ya da basın yayın organları aracılığıyla yayımlanır.

8.10. Değişiklikler

8.10.1. Değişiklik Prosedürü

TÜRKTRUST faaliyetlerinde ve zaman damgası hizmetlerinde oluşabilecek değişikliklere ve düzenlemelere bağlı olarak, ZDUE kitapçığının mevcut sürümünün içeriğinin değişmesini gerektiren herhangi bir durum ortaya çıktığında, ilgili değişikliklerin yansıtıldığı yeni bir ZDUE kitapçığı sürümü TÜRKTRUST tarafından hazırlanır ve TÜRKTRUST Yönetim Kurulu'nun onayının ardından yayımlanır. ZDİ ve ZDUE dokümanında yer alan ilkeler ve uygulamalar, yönetim gözden geçirme toplantılarında yıllık olarak gözden geçirilir.

ZDİ'de oluşan değişiklikler, ZDUE'deki ilgili uygulamalara da yansıtılır. Dolayısıyla yeni bir ZDİ sürümü, yeni bir ZDUE sürümünü de gerektirir. TÜRKTRUST tarafından üretilen yeni zaman damgaları "zaman damgası ilkeleri" uzantısında URL olarak verilen SUE dokümanına erişim bilgisi aynı kalır, ama bu adresin işaret ettiği ZDUE dokümanı yeni sürümdür.

8.10.2. Duyuru Mekanizması ve Süresi

TÜRKTRUST faaliyetleri ve zaman damgası hizmetlerindeki uygulama değişiklikleri ile mevcut ZDİ ve ZDUE kitapçıklarında değişiklik oluşması durumunda, çıkarılan güncel ZDİ ve ZDUE sürümleri hakkında zaman damgası sahipleri ve üçüncü taraflar ivedilikle bilgilendirilir.

Özellikle önemli değişikliklerde, zaman damgasının kullanılabilirliği ve kabul edilirliği bazı uygulamalarda etkilenebileceğinden, TÜRKTRUST zaman damgası sahiplerini ve üçüncü tarafları bilgilendirebilmek için tüm makul imkanları kullanır.

© 2005 - 2013 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. Tüm hakları saklıdır.

Yeni ZDİ ve ZDUE sürümleri, eski sürümlerle birlikte TÜRKTRUST bilgi deposunda, ayrıntılı sürüm bilgisi içerecek şekilde yayımlanır ve ilgili tarafların erişimine açık tutulur.

8.10.3. Nesne Tanımlayıcı Numaralarının Değişmesini Gerektiren Durumlar

Zaman damgası içeriğindeki bilgi alanlarında veya TÜRKTRUST'ın zaman damgası hizmetlerinde uyguladığı güvenlik kriterlerinde güvenlik düzeyine etki edecek değişiklikler olması durumunda, ZDİ kitapçığında tanımlanan zaman damgası ilkelerinin nesne tanımlayıcı numarası değiştirilir.

8.11. Anlaşmazlıkların Çözümü

TÜRKTRUST, zaman damgası sahipleri ve üçüncü taraflar arasında çıkabilecek anlaşmazlıklarda, öncelikle ZDİ ve ZDUE kitapçıklarında belirlenmiş ilke ve uygulama esasları ile prosedürler ve sözleşmeler uyarınca sorunun çözümlenmesine çalışılır.

Zaman damgası hizmetleriyle ilgili işlemler TÜRKTRUST tarafından Kanun ve Yönetmelikler ile bunlara bağlı Tebliğler uyarınca yürütülür.

Taraflar arasındaki anlaşmazlıklar sulhen çözüme kavuşmadığı takdirde, anlaşmazlıkların çözümü için Ankara Mahkemeleri yetkilidir.

8.12. Yasal Düzenleme

Türkiye'de zaman damgası hizmetleri, 5070 sayılı "Elektronik İmza Kanunu" ve Bilgi Teknolojileri ve İletişim Kurumu tarafından yayımlanmış Yönetmelik ve Tebliğler uyarınca düzenlenir. Kurum ESHS'lerin Kanun uyarınca işleyişinin düzenlenmesi ve denetlenmesinden de sorumludur.

8.13. İlgili Yasalara Uygunluk

TÜRKTRUST, zaman damgası hizmetlerini 5070 sayılı "Elektronik İmza Kanunu" ve Bilgi Teknolojileri ve İletişim Kurumu tarafından yayımlanmış Yönetmelik ve Tebliğler uyarınca yürütür.

8.14. Kitapçık Kısımlarının Ayrılabilirliği

ZDİ ve ZDUE kitapçıklarının diğer bölümlerinin geçerliliğini etkilemeyen herhangi bir bölümü geçerliliğini kaybettiğinde, TÜRKTRUST tarafından ilgili değişikliklerin yansıtıldığı yeni sürümler çıkarılana kadar, kitapçığın etkilenmemiş diğer bölümleri geçerliliğini korur ve uygulanır.

8.15. Mücbir Sebepler

TÜRKTRUST'ın zaman damgası hizmetlerine yönelik ESHS faaliyetlerini yerine getirmesini engelleyecek ve normal koşullar altında kontrol edilebilir olmayan durumlar mücbir sebep olarak adlandırılır. Bu durumlar devam ettiği sürece, TÜRKTRUST faaliyetleri aksaklığa veya kesintiye uğrayabilir. Doğal afetler, savaşlar, terör, telekomünikasyon, İnternet ve benzeri diğer altyapılarda oluşabilecek aksaklıklar mücbir sebep kabul edilir.

© 2005 - 2013 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. Tüm hakları saklıdır.