

**TASNİF DIŐI**



**TÜBİTAK BİLGEM  
KAMU SERTİFİKASYON MERKEZİ**

**İNTERNET SİTESİ YÜKÜMLÜLÜĞÜNE TABİ ŐİRKETLERİN VEYA  
MTHS'LERİN ALACAKLARI TEKNİK RAPORDA YER ALMASI GEREKEN  
TEKNİK KRİTERLER REHBERİ**

**Doküman Kodu**

REH.05.05

**Revizyon No**

04

**Revizyon Tarihi**

01.06.2018

**TASNİF DIŐI**

REVİZYON GEÇMİŐİ		
Revizyon No	Revizyon Nedeni	Revizyon Tarihi
00	İlk çıkıő.	14.08.2013
01	İnternette yayınlanan ilk sürüm.	08.10.2013
02	Üst bilgi güncellendi.	04.11.2016
03	Elektronik İmza Profili bölümü güncellendi.	14.03.2018
04	Doküman biçimi yeni Őablona aktarılmıőtır. Doküman kodu güncellenmiőtir. Dokümanın eski revizyonları Kamu SM doküman yönetim sisteminde "REH-001-003" kodu ile yer almaktadır.	01.06.2018

## İÇİNDEKİLER

1	<i>Amaç ve Kapsam</i> .....	3
2	<i>Tanımlar ve Kısaltmalar</i> .....	4
3	<i>İzleme Kayıtlarının Tutulması</i> .....	5
4	<i>SSL Kullanımı</i> .....	5
5	<i>Yedekleme ve Felaketten Kurtarma Planları</i> .....	5
6	<i>Elektronik İmza Profili</i> .....	6
7	<i>Güvenli Elektronik İmza Oluşturma Yazılımı</i> .....	6
8	<i>Güvenli Elektronik İmza Doğrulama Yazılımı</i> .....	7
9	<i>Elektronik İmzalı Belgelerin Arşivlenmesi</i> .....	7

## 1 Amaç ve Kapsam

Bu rehber, Gümrük ve Ticaret Bakanlıđı'nın 31 Mayıs 2013 tarihli Resmi Gazete'de yayımlanan "Sermaye Őirketlerinin Aaçacakları İnternet Sitelerine Dair Yönetmelik"te tanımı yapılan Őirket ve MTHS'lerin görevleri çerçevesinde uygulamakla yükümlü olduđu teknik kriterleri tanımlamak amacıyla yazılmıştır.

Bu rehber, Őirket veya MTHS'lerin halka açık bildirimlerin yayımlandığı internet sitesi hizmetini verirken içeriđin gösterilmesi, izleme kayıtlarının tutulması, yedekleme ve felaket kurtarma planlarının uygulanması, bildirimlerin güvenli elektronik imza ile imzalanması, imzalı bildirimlerin e-imzalarının dođrulanması, oluşturulacak e-imzaların profilleri ve internet sitesinden yayımlanan elektronik imzalı bildirimlerin e-imza arşivlemelerinin yapılması için belirlenen teknik kriterleri kapsamaktadır.

Bu doküman;

ETSI TS 101 733: Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CADES)

ETSI TS 101 903: Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)

ETSI TS 102 778: Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles (PAdES)

CWA 14170: Security Requirements for Signature Creation Applications

CWA 14171: Procedures for Electronic Signature Verification Profile standartları referans alınarak hazırlanmıştır.



## 2 Tanımlar ve Kısaltmalar

<b>CWA:</b>	CEN (Comité Européen De Normalisation) Workshop Agreement-CEN Çalıőtay Kararları
<b>ESHS:</b>	Elektronik Sertifika Hizmet Saėlayıcısı
<b>ETSI:</b>	European Telecommunications Standards Institute-Avrupa Telekomünikasyon Standartları Enstitüsü
<b>İnternet Sitesi:</b>	Gümrük ve Ticaret Bakanlığı'nın 31 Mayıs 2013 tarihli Resmi Gazete'de yayımlanan "Sermaye Őirketlerinin Aaçacakları İnternet Sitelerine Dair Yönetmelik"te tanımı yapılan İnternet Sitesi
<b>Kamu SM:</b>	Kamu Sertifikasyon Merkezi
<b>MTHS:</b>	Gümrük ve Ticaret Bakanlığı'nın 31 Mayıs 2013 tarihli Resmi Gazete'de yayımlanan "Sermaye Őirketlerinin Aaçacakları İnternet Sitelerine Dair Yönetmelik"te tanımı yapılan Merkezi Veri Tabanı Hizmet Saėlayıcısı
<b>NES:</b>	Nitelikli Elektronik Sertifika
<b>P4 İmza Profili:</b>	Bilgi Teknolojileri ve İletişim Kurumu tarafından 2/7/2012 tarihli ve 2012/DK-15/299 sayılı Kurul Kararı ile yayımlanan Elektronik İmza Kullanım Profilleri Rehberinde yer alan "Uzun Dönemli ve ÇİSDuP Kontrollü Güvenli Elektronik İmza Politikaları (Profil P4)"
<b>Őirket:</b>	Gümrük ve Ticaret Bakanlığı'nın 31 Mayıs 2013 tarihli Resmi Gazete'de yayımlanan "Sermaye Őirketlerinin Aaçacakları İnternet Sitelerine Dair Yönetmelik"te tanımı yapılan Őirket
<b>XAdES:</b>	XML Advanced Electronic Signature - XML Geliőmiş Elektronik İmza
<b>XML:</b>	Extensible Markup Language - Genişletilebilir İőaretleme Dili
<b>Zaman Damgası:</b>	E-imza mevzuatında tanımlanan Zaman Damgası

### 3 İzleme Kayıtlarının Tutulması

Hem MTHS'ler hem de Őirketler en az aŐağıdaki olaylar için izleme kaydı oluŐturmalıdır:

- Dosya yükleme iŐlemi, dosya ismi, dosya kategorisi, yükleme iŐlemini gerçekteŐiren kullanıcı adı, IP adresi (sadece yükleme internete açık IP adresinden yapıldı ise) ve yükleme zamanı
- Her imzalama iŐlemi sonrasında, dosya kategorisi ve imzalama zamanı, imzalayan sertifikanın "DN" alanı
- Herhangi bir imza sertifikasının deęiŐmesi durumunda, sertifikanın deęiŐtięine dair kayıt, yeni sertifikanın "DN" alanı, sertifika güncelleme iŐlemini yapan kullanıcı adı, yükleyen kullanıcıya ait IP adresi (sadece yükleme internete açık IP üzerinden yapıldı ise) ve sertifika güncelleme zamanı.

İzleme kayıtlarının tarih aralıęı, varsa kullanıcı adı ve IP (interneteye açık IP adresleri için) sorgulanmasını saęlayacak bir ekran ile gerektięinde ilgili kayıtların sorgulanması mümkün olmalıdır.

ArŐivleme amacıyla tutulan izleme kayıtlarında T.C. kimlik numarası saklanmamalıdır.

MTHS tarafından içerik saęlanıyor ise içerik sahibi Őirketin kendine özgü bir hesap üzerinden izleme kayıtlarının IP, kullanıcı adı, tarih kriterlerine göre sorgulanabilmesi MTHS tarafından saęlanmalıdır. İzleme kayıtları arŐiv kayıtları ile beraber 5 yıl boyunca imzalı ve zaman damgalı olarak saklanmalıdır.

### 4 SSL Kullanımı

Bilgi toplumu hizmetleri için öngörölen içerięin Őirket internet sitesinin özgölenmiŐ alanında gösterilmesi sırasında SSL kullanımı zorunlu deęildir.

Diđer taraftan MTHS'lerin Őirketlere sunacaęı hizmetlere (içerik yükleme, yapılan iŐlemlerin raporlanması, doküman imzalama vs.) SSL üzerinden eriŐilmesi zorunludur.

SSL kullanılması durumunda yaygın internet tarayıcıları tarafından tanınmayan ve son kullanıcıya sahte sertifika mesajı uyarısı gösterilmesine neden olan sertifikalar kullanılmamalıdır.

### 5 Yedekleme ve Felaketten Kurtarma Planları

Őirketlerin ve MTHS'lerin Yönetmelięin 11 inci maddesinin birinci fıkrası uyarınca yedekleme ve felaketten kurtarma planları ve prosedürleri bulunmalıdır. Kontroller sırasında ilgili prosedürler ibraz edilmelidir. Ayrıca Yönetmelięin 12 nci maddesinin birinci fıkrası uyarınca 5 yıl boyunca yüklenen dosyaların yedekleri alınmalıdır.

MTHS'ler ya da Őirketler en azından aŐağıda listelenmiŐ kontrolleri yerine getirmelidir:

- ISO IEC 27002:2013 Bölüm 12.3 altında listelenmiŐ olan kontroller
- ISO IEC 27002:2013 Bölüm 12.4.2 altında listelenmiŐ olan kontroller

MTHS üzerinden yüklenen ve arşivlenen dosyalar için ilgili MTHS tarafından hizmet alan Őirkete geçmişe dönük arşive erişim sağlayacak şekilde arayüz sunulmalıdır. Sunulan arayüzde en azından tarih bazlı sorgulama mümkün olmalıdır.

## 6 Elektronik İmza Profili

Őirketler/MTHS'ler tarafından oluşturulacak elektronik imzaların profilleri ile ilgili uyulması gereken teknik kriterler aşağıda verilmiştir:

1. İmzalama formatı P4 İmza Profiline uygun olacaktır.
2. Oluşturulan imzalarda XAdES imza tipi kullanılıyorsa "Enveloped" imza yapısı kullanılmayacaktır.

## 7 Güvenli Elektronik İmza Oluşturma Yazılımı

Uyulması gereken teknik kriterler aşağıda verilmiştir:

1. İnternet üzerinden halka açık bilgileri yayımlayan Őirket/MTHS'nin kendi sisteminde güvenli e-imza oluşturma yazılımının olması zorunludur. Güvenli elektronik imza oluşturma yazılımı E-imza mevzuatında yer alan CWA 14170'deki kriterleri sağlayacaktır.
2. Őirket ve MTHS tarafından oluşturulan tüm imzalarda 5070 sayılı Elektronik İmza Kanunu kapsamındaki NES'ler kullanılacaktır.
3. Őirket yetkilisinin veya onun yetkilendirdiđi kişinin imzasının doğrulanamadıđı belgeler internet sitesi üzerinden yayımlanmayacaktır.
4. MTHS, web üzerinden belge imzalanmasına imkan veren güvenli elektronik imza oluşturma yazılım hizmetini müşteri olan Őirketlere sunmak zorundadır.
5. MTHS üzerinden yayımlanacak içeriklerin güvenli elektronik imzalama işlemi, MTHS imza oluşturma yazılımı üzerinden gerçekleştirilecektir. MTHS'nin sunacađı güvenli elektronik imza oluşturma yazılımı, Őirketin yüklediđi içeriđin, Őirket yetkilisi veya onun yetkilendirdiđi kişiye ait sertifika ile imzalanması işlemi gerçekleştirecektir.
6. MTHS verdiđi hizmette, Őirket tarafından yetkilendirilmiş kişilerin bilgilerini kendi sisteminde tuttuđu kayıtlardan kontrol ederek imzalama işlemine izin verecektir. İmzalama işlemi yetki kontrolleri MTHS imza oluşturma uygulaması tarafından yapılacaktır.
7. Yazılım, imza oluşturmadan önce sertifika geçerlilik kontrollerini yapacaktır. Geçersiz sertifikayla imza oluşturulmasına izin verilmeyecek, sertifika doğrulamada hata oluşması durumunda ilgili hata kullanıcıya gösterilerek kullanıcı bilgilendirilecektir.
8. İmza oluştururken hata olması durumunda doğru ve açıklayıcı hata mesajı kullanıcıya gösterilecektir.
9. Őirket/MTHS e-imzalı bildirim dosyasının internet üzerinden kullanıcının bilgisayarına indirilip kaydedilmesine imkan verecektir.

## 8 Güvenli Elektronik İmza Doğrulama Yazılımı

Uyulması gereken teknik kriterler aŐağıda verilmiŐtir:

1. İnternet üzerinden halka açık bilgileri yayımlayan Őirket/MTHS, yayımladıđı e-imzalı belgelerin imzasının dođrulanmasına imkan veren güvenli elektronik imza dođrulama yazılımı hizmetini vermeye zorunludur. Güvenli elektronik imza dođrulama yazılımı e-imza mevzuatında yer alan CWA 14171'deki kriterleri sađlayacaktır.
2. ÖzgülenmiŐ alanda sunulan e-imzalı dokümanın dođrulanmasına, dokümanın imzasız hali ile ayrıık imzasının veya bütünüŐik imzalı halinin kullanıcının bilgisayarına indirilip kaydedilmesine imkan verilecektir.
3. İmza dođrulama uygulaması; e-imzalı dokümanın sečilmesine, içeriđinin gösterilmesine, imzasının dođrulanmasına, imza dođrulama sonucunun ekrandan anlaşılır bir dilde gösterilmesine, imzalayan kiŐinin adı/soyadı, kurumu, varsa unvanı, sertifikayı veren ESHS bilgileri ve zaman damgası üzerindeki imza zamanı bilgisinin ekrandan gösterilmesine imkan verecektir.

## 9 Elektronik İmzalı Belgelerin ArŐivlenmesi

Elektronik imzalı belgelerin arŐivlenmesi ile ilgili uyulması gereken teknik kriterler aŐağıda verilmiŐtir:

1. E-imzalı olarak halka duyurulan bilgilerin, ilgili mevzuat geređi saklanmak zorunda olduđu süre kadar e-imzaların güvenliđinin sađlanması için e-imza arŐivlemelerinin yapılması zorunludur. Bu amaçla Őirket/MTHS'nin e-imza arŐivleme yapan yazılımları mevcut olmalıdır.
2. E-imzalı belgeler arŐivlenirken ETSI TS 101 733, ETSI TS 101 903 veya ETSI TS 102 778'de tanımlanan arŐiv elektronik imza formatına uygun olarak e-imzaların arŐivlenmesi sađlanacaktır.