



TÜBİTAK BİLGEM

KAMU SERTİFİKASYON MERKEZİ

TASNİF DIŐI

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

Doküman Kodu	Yayın Numarası	Yayın Tarihi
REHB-001-003	02	04.11.2016

TÜBİTAK BİLGEM

Kamu Sertifikasyon Merkezi

P.K. 74, 41470 Gebze / KOCAELİ

Tel: 444 5 576, Faks: (0262) 648 18 00

www.kamusm.gov.tr

Soru, Görüş ve Öneriler için: bilgi@kamusm.gov.tr

Uyarı : Yalnız Kamu SM dosya sunucudan erişilen elektronik kopyalar güncel ve kontrollü olup, elektronik ortamdan alınacak kağıt baskılar KONTROLSÜZ KOPYA'dır

TASNİF DIŐI



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

DEĞİŞİKLİK KAYITLARI

Yayın No	Yayın Nedeni	Yayın Tarihi
00	İlk Çıkış.	14.08.2013
01	İnternette yayınlanan ilk Sürüm.	08.10.2013
02	Üst bilgi güncellendi.	04.11.2016

UYARI: Yalnız Kamu SM doküman yönetim sisteminden erişilen elektronik kopyalar güncel ve kontrollü olup, elektronik ortamdan alınacak kağıt baskılar KONTROLSUZ KOPYA'dır

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

İÇİNDEKİLER

1 AMAÇ.....	4
2 KAPSAM.....	4
3 REFERANSLAR	4
4 KISALTMALAR VE TANIMLAR.....	5
5 İZLEME KAYITLARININ TUTULMASI	6
6 SSL KULLANIMI.....	6
7 YEDEKLEME VE FELAKETTEN KURTARMA PLANLARI.....	7
8 ELEKTRONİK İMZA PROFİLİ	7
9 GÜVENLİ ELEKTRONİK İMZA OLUŐTURMA YAZILIMI.....	8
10 GÜVENLİ ELEKTRONİK İMZA DOĞRULAMA YAZILIMI.....	8
11 ELEKTRONİK İMZALI BELGELERİN ARŐİVLENMESİ	9



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

1 AMAÇ

Bu rehber, Gümrük ve Ticaret Bakanlığı'nın 31 Mayıs 2013 tarihli Resmi Gazete'de yayınlanan "Sermaye Şirketlerinin Açacakları İnternet Sitelerine Dair Yönetmelik" te tanımlanan Şirket ve MTHS'lerin görevleri çerçevesinde uygulamakla yükümlü olduğu teknik kriterleri tanımlamak amacıyla yazılmıştır.

2 KAPSAM

Bu rehber, Şirket veya MTHS'lerin halka açık bildirimlerin yayınlandığı internet sitesi hizmetini verirken içeriğin gösterilmesi, izleme kayıtlarının tutulması, yedekleme ve felaket kurtarma planlarının uygulanması, bildirimlerin güvenli elektronik imza ile imzalanması, imzalı bildirimlerin eimzalarının doğrulanması, oluşturulacak e-imzaların profilleri ve internet sitesinden yayınlanan elektronik imzalı bildirimlerin e-imza arşivlemelerinin yapılması için belirlenen teknik kriterleri kapsamaktadır.

3 REFERANSLAR

1. ETSI TS 101 733: Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAAdES)
2. ETSI TS 101 903: Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)
3. ETSI TS 102 778: Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles (PAdES)
4. CWA 14170: Security Requirements for Signature Creation Applications
5. CWA 14171: Procedures for Electronic Signature Verification

**İNTERNET SİTESİ YÜKÜMLÜLÜĞÜNE TABİ ŞİRKETLERİN
VEYA MTHS'LERİN ALACAKLARI TEKNİK RAPORDA YER
ALMASI GEREKEN TEKNİK KRİTERLER REHBERİ****4 KISALTMALAR VE TANIMLAR**

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

UYARI: Yalnız Kamu SM doküman yönetim sisteminden erişilen elektronik kopyalar güncel ve kontrollü olup, elektronik ortamdan alınacak kağıt baskılar KONTROLSUZ KOPYA'dır

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

5 İZLEME KAYITLARININ TUTULMASI

Hem MTHS'ler hem de Őirket'ler 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 İmza sertifikasının deęiŐmesi durumunda, sertifikanın deęiŐtiđine 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 aralıđı, varsa kullanıcı adı ve IP (interneteye açık IP adresleri için) sorgulanmasını sađlayacak bir ekran ile gerektiđinde ilgili kayıtların sorgulanması mümkün olmalıdır.

ArŐivleme amacıyla tutulan izleme kayıtlarında TC kimlik numarası saklanmamalıdır.

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

6 SSL KULLANIMI

Bilgi toplumu hizmetleri için öngörölen içeriđin Őirket internet sitesinin öđgölenmiŐ alanında gösterilmesi sırasında SSL kullanımı zorunlu deđildir.

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

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

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

7 YEDEKLEME VE FELAKETTEN KURTARMA PLANLARI

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

MTHS'ler ya da şirketler en azından aşağıda listelenmiş kontrolleri yerine getirmelidir:

- ISO IEC 27001:2005 Bölüm A.10.5 doğrultusunda ISO IEC 27002 Bölüm 10.5 altında listelenmiş olan kontroller
- ISO IEC 27001:2005 Bölüm A.10.10 doğrultusunda ISO IEC 27001 Bölüm 10.10.3 altında listelenmiş olan kontroller

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

8 ELEKTRONİK İMZA PROFİLİ

Şirketler/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.
3. Oluşturulan imza doğrudan içeriğin imzalanması anlamına gelen paralel imza yapısında olacaktır.

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

9 GÜVENLİ ELEKTRONİK İMZA OLUŞTURMA YAZILIMI

Uyulması gereken teknik kriterler aşağıda verilmiştir:

1. İnternet üzerinden halka açık bilgileri yayınlayan Şirket/MTHS'nin kendi sisteminde güvenli eimza oluşturma yazılımının olması zorunludur. Güvenli elektronik imza oluşturma yazılımı Eimza mevzuatında yer alan CWA 14170'deki kriterleri sağlayacaktır.
2. Şirket ve MTHS tarafından oluşturulan tüm imzalarda 5070 sayılı Elektronik İmza Kanunu kapsamındaki NES'ler kullanılacaktır.
3. Şirket yetkilisinin veya onun yetkilendirdiği kişinin imzasının doğrulanmadığı belgeler internet sitesi üzerinden yayınlanmayacaktır.
4. MTHS, web üzerinden belge imzalanmasına imkan veren güvenli elektronik imza oluşturma yazılım hizmetini müşterisi olan şirketlere sunmak zorundadır.
5. MTHS üzerinden yayınlanacak içeriklerin güvenli elektronik imzalama işlemi, MTHS imza oluşturma yazılımı üzerinden gerçekleştirilecektir. MTHS'nin sunacağı güvenli elektronik imza oluşturma yazılımı, Şirketin yüklediği içeriğin, Şirket yetkilisi veya onun yetkilendirdiği kişiye ait sertifika ile imzalanması işlemini gerçekleştirecektir.
6. MTHS verdiği hizmette, Şirket tarafından yetkilendirilmiş kişilerin bilgilerini kendi sisteminde tuttuğu kayıtlardan kontrol ederek imzalama işlemine izin verecektir. İmzalama işleminde yetki kontrolleri MTHS imza oluşturma uygulaması tarafından yapılacaktır.
7. Yazılım, imza oluşturmada 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. Şirket/MTHS e-imzalı bildirim dosyasının internet üzerinden kullanıcının bilgisayarına indirilip kaydedilmesine imkan verecektir.

10 GÜVENLİ ELEKTRONİK İMZA DOĞRULAMA YAZILIMI

Uyulması gereken teknik kriterler aşağıda verilmiştir:

1. İnternet üzerinden halka açık bilgileri yayınlayan Şirket/MTHS, yayınladığı e-imzalı belgelerin imzasının doğrulanmasına imkan veren güvenli elektronik imza doğrulama yazılımı hizmetini vermeye zorunludur. Güvenli elektronik imza doğrulama yazılımı e-imza mevzuatında yer alan CWA 14171'deki kriterleri sağlayacaktır.

UYARI: Yalnız Kamu SM doküman yönetim sisteminden erişilen elektronik kopyalar güncel ve kontrollü olup, elektronik ortamdan alınacak kağıt baskılar KONTROLSUZ KOPYA'dır

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

2. Özgülenmiş alanda sunulan e-imzalı dokümanın doğrulanmasına, dokümanın imzasız hali ile ayrılmış halinin veya bütünlük imzalı halinin kullanıcının bilgisayarına indirilip kaydedilmesine imkan verilecektir.
3. İmza doğrulama uygulaması; e-imzalı dokümanın seçilmesine, içeriğinin gösterilmesine, imzasının doğrulanmasına, imza doğrulama sonucunun ekrandan anlaşılır bir dilde gösterilmesine, imzalayan kişinin adı/soyadı, kurumu, varsa unvanı, sertifikayı veren ESHS bilgileri ve zaman damgası üzerindeki imza zamanı bilgisinin ekrandan gösterilmesine imkan verecektir.

11 ELEKTRONİK İMZALI BELGELERİN ARŞİVLENMESİ

Elektronik imzalı belgelerin arşivlenmesi ile ilgili uyulması gereken teknik kriterler aşağıda verilmiştir:

1. E-imzalı olarak halka duyurulan bilgilerin, ilgili mevzuat gereği saklanmak zorunda olduğu süre kadar e-imzaların güvenliğinin sağlanması için e-imza arşivlemelerinin yapılması zorunludur. Bu amaçla Şirket/MTHS'nin e-imza arşivleme yapan yazılımları mevcut olmalıdır.
2. E-imzalı belgeler arşivlenirken ETSI TS 101 733, ETSI TS 101 903 veya ETSI TS 102 778'de tanımlanan arşiv elektronik imza formatına uygun olarak e-imzaların arşivlenmesi sağlanacaktır.