

ELEKTRONİK İMZA İLE İLGİLİ SÜREÇLERE VE TEKNİK KRİTERLERE İLİŞKİN TEBLİĞ

BİRİNCİ BÖLÜM Genel Hükümler

Amaç

Madde 1 — Bu Tebliğin amacı, elektronik imzaya ilişkin süreçleri ve teknik kriterleri detaylı olarak belirlemektir.

Kapsam

Madde 2 — Bu Tebliğ; nitelikli elektronik sertifika başvurusu, sertifikanın oluşturulması, yayımlanması, yenilenmesi, iptali ve arşivleme süreçleri dahil olmak üzere ESHS'nin işleyişine, imza oluşturma ve doğrulama verilerine, sertifika ilkelerine ve sertifika uygulama esaslarına, imza oluşturma ve doğrulama araçlarına, ESHS'nin faaliyetleri için kullandığı sistem, cihaz ile fiziki güvenliğine, personeline, zaman damgasına ve hizmetlerine ilişkin teknik hususları kapsar.

Dayanak

Madde 3 — Bu Tebliğ, Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmeliğin 34 üncü maddesine dayanılarak hazırlanmıştır.

Tanımlar

Madde 4 — Bu Tebliğde geçen;
Yönetmelik: Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmeliği,
BS (British Standards): İngiliz Standartlarını,
CEN (Comité Européen de Normalisation): Avrupa Standardizasyon Komitesini,
CWA (CEN Workshop Agreement): CEN Çalıştay Kararını,
DSA (Digital Signature Algorithm): Sayısal İmza Algoritmasını,
DSA Eliptik Eğrisi (DSA Elliptical Curve): Sayısal İmza Algoritması Eliptik Eğrisini,
EAL (Evaluation Assurance Level): Değerlendirme Garanti Düzeyini,
ETSI (European Telecommunications Standards Institute): Avrupa Telekomünikasyon Standartları Enstitüsünü,
ETSI SR (ETSI Special Report): ETSI Özel Raporunu,
ETSI TS (ETSI Technical Specification): ETSI Teknik Özelliklerini,
FIPS PUB (Federal Information Processing Standards Publications): Federal Bilgi İşleme Standartları Yayınlarını,
IETF RFC (Internet Engineering Task Force Request for Comments): İnternet Mühendisliği Görev Grubu Yorum Talebini,

ISO/IEC (International Organisation for Standardisation / International Electrotechnical Committee): Uluslararası Standardizasyon Teşkilatı / Uluslararası Elektroteknik Komitesini,
ITU (International Telecommunication Union): Uluslararası Telekomünikasyon Birliğini,

RIPEMD (RACE Integrity Primitives Evaluation Message Digest): RACE Bütünlük Asli Mesaj Değerlendirme Özetini,

RSA: Rivest-Shamir-Adleman'ı,

SHA (Secure Hash Algorithm): Güvenli Özet Algoritmasını ifade eder.

Bu Tebliğde yer almayan tanımlar için Kanun ve Yönetmelikte yer alan tanımlar geçerlidir.

İKİNCİ BÖLÜM

Teknik Hususlar

ESHS'nin İşleyişi

Madde 5 — ESHS işleyişinin bütün aşamalarında;

- a) ETSITS 101 456 ve
- b) CWA 14167-1

standartlarına uyar.

Nitelikli elektronik sertifikalar;

- a) ETSITS 101 862 ve
- b) ITU-TRec. X.509V.3'e

uygun olarak oluşturulur.

Algoritmalar ve Parametreler

Madde 6 — (Değişik:RG-21/01/2006-26056)

İmza oluşturma ve doğrulama verileri ile özetleme algoritmaları, ETSI TS 102 176-1 standardına ve aşağıda yer alan şartlara uygun olmalıdır:

- a) İmza sahibinin imza oluşturma ve doğrulama verileri
 - i. RSA için en az 1024 bit veya
 - ii. DSA için en az 1024 bit veya
 - iii. DSA Eliptik Eğrisi için en az 163 bit
- b) ESHS'nin imza oluşturma ve doğrulama verileri
 - i. RSA için en az 2048 bit veya
 - ii. DSA için en az 2048 bit veya
 - iii. DSA Eliptik Eğrisi için en az 256 bit
- c) Özetleme algoritması
 - i. RIPEMD – 160 veya
 - ii. SHA – 1 veya
 - iii. SHA-224 veya
 - iv. SHA-256 veya
 - v. WHIRLPOOL

(Değişik fıkra:RG-22/12/2011-28150) Yukarıda belirtilen algoritmalar ve parametreler 31/12/2012 tarihine kadar geçerlidir.

Sertifika İlkeleri ve Sertifika Uygulama Esasları

Madde 7 — ESHS; sertifika ilkelerini ve sertifika uygulama esaslarını IETF RFC 3647'ye uygun olarak hazırlar.

Güvenli Elektronik İmza Oluşturma ve Doğrulama Araçları

Madde 8 — Güvenli elektronik imza oluşturma araçları CWA 14169 standardına uygun ve TS ISO/IEC 15408 (-1,-2,-3)'e veya ISO/IEC 15408 (-1,-2,-3)'e göre en az EAL4+ seviyesinde olmalıdır.

ESHS, sağlamış olduğu güvenli elektronik imza doğrulama araçları için CWA 14171 standardına uyar ve bunu yazılı olarak taahhüt eder.

Güvenlik Kriterleri

Madde 9 — ESHS, güvenlik kriterlerine ilişkin olarak;

- a) CWA 14167-1,
- b) ETSITS 101 456 ve
- c) TS ISO/IEC 17799 veya ISO/IEC 17799

standartlarına uyar.

Zaman Damgası ve Hizmetleri

Madde 10 — ESHS, zaman damgası ve hizmetlerine ilişkin olarak;

- a) CWA 14167-1 ve
- b) ETSI TS 101 861

standartlarına uyar.

Zaman damgası ilkeleri ve zaman damgası uygulama esasları ETSI TS 102 023'e uygun olarak hazırlanır.

Mobil elektronik imza

MADDE 10/A – (Değişik:RG-26/6/2008-26918)

(1) ESHS'ler, mobil elektronik imza hizmetlerinde dolaşım ile ilgili ETSI TS 102 207 standardına ve nitelikli elektronik sertifika başvurusu, oluşturulması, yayınlanması, yenilenmesi süreçleri ile ilgili olarak ETSI TS 102 204 standardına uyar.

Belgeler

Madde 11 — ESHS;

a) **(Değişik:RG-20/06/2006-26204)** TS ISO/IEC 27001 veya ISO/IEC 27001 standardına uygunluğunu,

b) Güvenli elektronik imza oluşturma araçlarının;

i. **(Değişik:R.G.-26/6/2008-26918)** FIPS PUB 140-2'ye göre seviye 3 veya üzerinde olduğunu veya

ii. CWA 14167-2'de belirtilen kriterlere uygunluğunu veya

iii. CWA 14169 standardına uygun ve TS ISO/IEC 15408 (-1,-2,-3)'e veya ISO/IEC 15408 (-1,-2,-3)'e göre en az EAL4+ seviyesinde olduğunu yetkili kurum veya kuruluşlardan alınan belgelerle belgelendirir.

Geçici hükümler

GEÇİCİ MADDE 1– (Ek:RG-20/06/2006-26204)⁽¹⁾

Bu Tebliğ'in yayımlandığı tarih itibariyle faaliyette bulunan ESHS'ler TS ISO/IEC 27001 veya ISO/IEC 27001 standardına uygunluğunu gösteren belgeleri en geç bir (1) yıl içinde Kuruma sunar.

GEÇİCİ MADDE 2 – (Ek:RG-26/6/2008-26918)

(1) Bu Tebliğ'in yayımlandığı tarihten itibaren faaliyette bulunan ESHS'ler;

a) Güvenli elektronik imza oluşturma araçlarının bu Tebliğin "Belgeler" başlıklı 11 nci maddesinin (b) bendinde belirtilen standartlara uygun olduğunu gösteren belgeleri 31/12/2009 tarihine kadar,

b) Mobil elektronik imza uygulamalarının ETSI TS 102 207 ve ETSI TS 102 204 standartlarına uygunluğunu gösteren taahhütnamelerini 6 (altı) ay içerisinde Kurum'a sunar.

ÜÇÜNCÜ BÖLÜM

Diğer Hükümler

Yürürlük

Madde 12 — Bu Tebliğ yayımı tarihinde yürürlüğe girer.

Yürütme

Madde 13 — Bu Tebliğ hükümlerini Telekomünikasyon Kurulu Başkanı yürütür.

(1) 26/6/2008 tarihli ve 26918 sayılı Resmi Gazete'de yayımlanan Tebliğ değişikliği ile geçici madde numarası geçici madde 1 olarak değiştirilmiştir.