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 — (Değişik fıkra:RG-24/3/2020-31078) Bu Tebliğde geçen;

a) Yönetmelik: Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmeliği,

b) BS (British Standards): İngiliz Standartlarını,

c) CEN (Comité Européen de Normalisation): Avrupa Standardizasyon Komitesini,

ç) CWA (CEN Workshop Agreement): CEN Çalıştay Kararını,

d) DSA (Digital Signature Algorithm): Sayısal İmza Algoritmasını,

e) DSA Eliptik Eğrisi (DSA Elliptical Curve): Sayısal İmza Algoritması Eliptik Eğrisini,

f) EAL (Evaluation Assurance Level): Değerlendirme Garanti Düzeyini,

g) ETSI (European Telecommunications Standards Institute): Avrupa Telekomünikasyon Standartları Enstitüsünü,

ğ) ETSI SR (ETSI Special Report): ETSI Özel Raporunu,

h) ETSI TS (ETSI Technical Specification): ETSI Teknik Özelliklerini,

ı) FIPS PUB (Federal Information Processing Standards Publications): Federal Bilgi İşleme Standartları Yayınlarını,

i) IETF RFC (Internet Engineering Task Force Request for Comments): İnternet Mühendisliği Görev Grubu Yorum Talebini,

j) ISO/IEC (International Organisation for Standardisation/International Electrotechnical Commitee): Uluslararası Standardizasyon Teşkilatı/Uluslararası Elektroteknik Komitesini,

k) ITU (International Telecommunication Union): Uluslararası Telekomünikasyon Birliğini,

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

m) RSA: Rivest-Shamir-Adleman'ı,

n) SHA (Secure Hash Algorithm): Güvenli Özet Algoritmasını,

o) PSS (Probabilistic Signature Scheme): Olasılıklı İmza Şemasını,

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-30/1/2013-28544)

(Değişik cümle:RG-13/7/2017-30123) İmza oluşturma ve doğrulama verileri ile özetleme algoritmalarının, ETSI TS 119 312 standardına ve aşağıda yer alan şartlara uygun olması gerekir.

a) İmza sahibinin imza oluşturma ve doğrulama verileri:

i. RSA için en az 2048 bit veya

ii. DSA için en az 3072 bit veya

iii. DSA Eliptik Eğrisi için en az 256 bit

b) ESHS'nin imza oluşturma ve doğrulama verileri:

i. **(Değişik:RG-24/3/2020-31078)** İmzalamalarda RSA-PSS kullanılmak şartıyla RSA için en az 4096 bit veya

ii. DSA için en az 3072 bit veya

iii. DSA Eliptik Eğrisi için en az 256 bit

c) **(Değişik:RG-24/3/2020-31078)** Özetleme algoritması:

i. SHA2-256 veya

ii. SHA2-384 veya

iii. SHA2-512 veya

iv. SHA3-256 veya

v. SHA3-384 veya

vi. SHA3-512

(Değişik fıkra:RG-28/12/2022-32057) Birinci fıkrada belirtilen algoritmalar ve parametreler **(Değişik ibare:RG-4/10/2025-33037)** 31/12/2027 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 (-l,-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) **(Değişik:RG-30/1/2013-28544)** TS ISO/IEC 27001 veya ISO/IEC 27001 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. **(Değişik:RG-30/1/2013-28544)** CWA 14167-2, CWA 14167-3 veya CWA 14167-4'te belirtilen kriterlere uygunluğunu veya

iii. CWA 14169 standardına uygun ve TS ISO/IEC 15408 (-l,-2,-3)'e veya

ISO/IEC 15408 (-1,-2,-3)'e göre en az EAL4+ seviyesinde olduğunu yetkili kurum veya kuruluşlardan alman 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.

GEÇİCİ MADDE 3 – (Ek:RG-30/1/2013-28544) (Değişik:RG-19/9/2013-28770)

Bu maddenin yürürlüğe girdiği tarihte faaliyette bulunan ESHS'ler 15/9/2014 tarihine kadar 6 ncı maddeye uyum sağlar.

GEÇİCİ MADDE 4 – (Ek:RG-3/10/2014-29138)

15/9/2014 tarihinden önce üretilmiş, 6 ncı maddede yer alan kriterleri karşılamayan ve geçerlilik süresi sona ermemiş olan nitelikli elektronik sertifikalar 31/12/2014 tarihine kadar kullanılabilir.

GEÇİCİ MADDE 5 –(Ek:RG-24/3/2020-31078)

ESHS'ler kendi imza oluşturma ve doğrulama verilerine ilişkin olarak bu maddeyi ihdas eden Tebliğin 2 nci maddesiyle değiştirilen bu Tebliğin 6 ncı maddesinin birinci fıkrasının (b) bendinin (i) alt bendinde belirlenen şarta, bu maddenin yürürlüğe girdiği tarihten itibaren bir yıl içerisinde uyum sağlar. Bu maddenin yürürlüğe girdiği tarihten önce ve bu tarihten itibaren bir yıl içerisinde oluşturulan nitelikli elektronik sertifikalar geçerlilik süresi sona erene kadar kullanılabilir.

ÜÇÜNCÜ BÖLÜM
Diğer Hükümler

Yürürlük

Madde 12 — Bu Tebliğ yayımı tarihinde yürürlüğe girer.

Yürütme

Madde 13 — (Değişik:RG-13/7/2017-30123)

Bu Tebliğ hükümlerini Bilgi Teknolojileri ve İletişim Kurulu Başkanı yürütür.

———————

(1) 26/6/2008 tarihli ve 26918 sayılı Resmi Gazete'de yayımlanan Tebliğ değişikliği ile bu maddenin "GEÇİCİ MADDE" olan numarası "GEÇİCİ MADDE 1" olarak değiştirilmiştir.