Telekomünikasyon Kurumundan:

Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ

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 Commitee): 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 — İmza oluşturma ve doğrulama verileri, aşağıda belirtilen algoritma ve parametrelere uygun olarak oluşturulur;

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 160 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 Özetleme algoritması olarak;

a) RIPEMD-160 veya

b) SHA-1

kullanılır.

Yukarıda belirtilen algoritmalar ve parametreler 31/12/2005 tarihine kadar geçerlidir.

Yukarıda belirtilen algoritmalara ve parametrelere bağlı kalmak şartı ile ETSI SR 002 176 raporunda belirtilen imza oluşturma ve doğrulama verilerinin oluşturulmasında kullanılan algoritma ve parametreler de 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) 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.

Belgeler

Madde 11 — ESHS;

a) BS 7799-2 standardına uygunluğunu,

b) Güvenli elektronik imza oluşturma araçlarının;

i. **FIPS PUB 140-1 veya 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 (-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.

ÜÇÜNCÜ BÖLÜM

Diğer Hükümler

Yürürlük

Madde 12 — Bu Tebliğ yayımı tarihinde yürürlüğe girer.

Yürütme

Madde 13 — Bu Tebliğ hükümlerini Telekomünikasyon Kurulu Başkanı yürütür.