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 fikra: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 fikra:RG-24/3/2020-31078) Birinci fıkrada belirtilen algoritmalar ve parametreler 31/12/2022 tarihine kadar geçerlidir.