TEBLİĞ

Bilgi Teknolojileri ve İletişim Kurumundan:

Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğde Değişiklik Yapılmasına Dair Tebliğ

MADDE 1 – 6/1/2005 tarihli ve 25692 sayılı Resmî Gazete'de yayımlanan Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğin 4 üncü maddesinin birinci fıkrası aşağıdaki şekilde değiştirilmiştir.

"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."

MADDE 2 – Aynı Tebliğin 6 ncı maddesinin birinci fıkrasının (b) bendinin (i) alt bendi, (c) bendi ve aynı maddenin ikinci fıkrası aşağıdaki şekilde değiştirilmiştir.

"i. İmzalamalarda RSA-PSS kullanılmak şartıyla RSA için en az 4096 bit veya"

"c) 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"

"Birinci fıkrada belirtilen algoritmalar ve parametreler 31/12/2022 tarihine kadar geçerlidir."

MADDE 3 – Aynı Tebliğe aşağıdaki geçici madde eklenmiştir.

"**GEÇİCİ MADDE 5 –** 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."

MADDE 4 – Bu Tebliğ yayımı tarihinde yürürlüğe girer.

MADDE 5 – Bu Tebliğ hükümlerini Bilgi Teknolojileri ve İletişim Kurulu Başkanı yürütür.