

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURULU
KARARI

Karar Tarihi : 03.03.2020
Karar No : 2020/DK-BTD/062

Gündem Konusu : Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de Değişiklik Yapılmasına İlişkin Tebliğ

KARAR : Bilgi Teknolojileri Dairesi Başkanlığının hazırladığı takrir ve ekleri incelenmiştir.

Teknoloji ve standartlardaki gelişmelere bağlı olarak; Ek'te yer alan "Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de Değişiklik Yapılmasına İlişkin Tebliğ"nin onaylanarak Resmi Gazete'de yayımlanmak üzere T.C. Cumhurbaşkanlığı İdari İşler Başkanlığı Hukuk ve Mevzuat Genel Müdürlüğü'ne gönderilmesi ve yayımlanma aşamasında ihtiyaç duyulacak şekli değişikliklerin yapılabilmesini teminen icranın yetkilendirilmesi hususuna karar verilmiştir.

Bilgi Teknolojileri ve İletişim Kurumundan:

**ELEKTRONİK İMZA İLE İLGİLİ SÜREÇLERE VE TEKNİK KRİTERLERE İLİŞKİN
TEBLİĞ'DE DEĞİŞİKLİK YAPILMASINA DAİR TEBLİĞ**

MADDE 1 — 06/01/2005 tarihli ve 25692 sayılı Resmî Gazete'de yayımlanan Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'in "Tanımlar" başlıklı 4 ncü maddesinin birinci fıkrasına aşağıdaki bent eklenmiştir.

"PSS (Probabilistic Signature Scheme): Olasılıklı İmza Şeması"

MADDE 2 — Aynı Tebliğ'in "Algoritmalar ve Parametreler" başlıklı 6 ncı maddesinin birinci fıkrasının (b) bendinin (i) alt bendi aşağıdaki şekilde değiştirilmiştir.

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

MADDE 3 — Aynı Tebliğ'in "Algoritmalar ve Parametreler" başlıklı 6 ncı maddesinin birinci fıkrasının (c) bendi aşağıdaki şekilde değiştirilmiştir.

"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"

MADDE 4 — Aynı Tebliğ'in "Algoritmalar ve Parametreler" başlıklı 6 ncı maddesinin ikinci fıkrası aşağıdaki şekilde değiştirilmiştir:

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

MADDE 5 — Aynı Tebliğe aşağıdaki geçici madde eklenmiştir.

"Bu Tebliğ'in yürürlüğe girdiği tarihten itibaren bir yıl içerisinde ESHS'ler kendi imza oluşturma ve doğrulama verilerinin, bu Tebliğ'in 6'ncı maddesinin birinci fıkrasının (b) bendinde belirlenen şartlara uygun olmasını sağlarlar. Bu maddenin yürürlüğe girdiği tarihten önce ve bu tarihten itibaren bir yıl içerisinde oluşturulan nitelikli elektronik sertifikalar geçerlilik süresi sona erene kadar kullanılabilir."

MADDE 6 — Bu Tebliğ yayımı tarihinde yürürlüğe girer.

MADDE 7 — Bu Tebliğ hükümlerini Bilgi Teknolojileri ve İletişim Kurulu Başkanı yürütür.