

**TEBLİĞ**

Bilgi Teknolojileri ve İletişim Kurumundan:

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

**MADDE 1** – 6/1/2005 tarihli ve 25692 sayılı Resmî Gazete’de yayımlanan Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğin 6 ncı maddesi aşağıdaki şekilde değiştirilmiştir.

“**MADDE 6** -İmza oluşturma ve doğrulama verileri ile özetleme algoritmalarının, ETSI TS 102 176-1 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. RSA için en az 2048 bit veya
- ii. DSA için en az 3072 bit veya
- iii. DSA Eliptik Eğrisi için en az 256 bit

c) Özetleme algoritması:

- i. SHA-256 veya
- ii. SHA-384 veya
- iii. SHA-512 veya
- iv. WHIRLPOOL

Birinci fıkrada belirtilen algoritmalar ve parametreler 31/12/2016 tarihine kadar geçerlidir.”

**MADDE 2** – Aynı Tebliğin 9 uncu maddesinin birinci fıkrasının (c) bendi aşağıdaki şekilde değiştirilmiştir.

“c) TS ISO/IEC 27001 veya ISO/IEC 27001”

**MADDE 3** – Aynı Tebliğin 11 inci maddesinin birinci fıkrasının (b) bendinin (ii) alt bendi aşağıdaki şekilde değiştirilmiştir.

“ii. CWA 14167-2, CWA 14167-3 veya CWA 14167-4’te belirtilen kriterlere uygunluğunu veya”

**MADDE 4** – Aynı Tebliğe aşağıdaki geçici 3 üncü madde eklenmiştir.

“**GEÇİCİ MADDE 3** –Bu maddenin yürürlüğe girdiği tarihte faaliyette bulunan ESHS’ler altı ay içinde 6 ncı maddeye uyum sağlar.”

**MADDE 5** – Bu Tebliğ yayımı tarihinde yürürlüğe girer.

**MADDE 6** – Bu Tebliğ hükümlerini Bilgi Teknolojileri ve İletişim Kurulu Başkanı yürütür.