

## Tebliğ

Telekomünikasyon Kurumundan:

EK-2

### Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de 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 Tebliğ'in "Algoritmalar ve Parametreler" başlıklı 6 ncı maddesi aşağıdaki şekilde değiştirilmiştir:

#### "Algoritmalar ve Parametreler

**Madde 6** — İmza oluşturma ve doğrulama verileri ile özetleme algoritmaları, ETSI TS 102 176-1 standardına ve aşağıda yer alan şartlara uygun olmalıdır:

- 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 163 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
- c) Özetleme algoritması
  - i. RIPEMD – 160 veya
  - ii. SHA – 1 veya
  - iii. SHA-224 veya
  - iv. SHA-256 veya
  - v. WHIRLPOOL

Yukarıda belirtilen algoritmalar ve parametreler 31/12/2008 tarihine kadar geçerlidir."

**Madde 2** — Bu Tebliğ yayımı tarihinde yürürlüğe girer.

**Madde 3** — Bu Tebliğ hükümlerini Telekomünikasyon Kurulu Başkanı yürütür.