KUZEY KIBRIS TÜRK CUMHURİYETİ

RESMÎ GAZETE

Sayı : 223	25 Aralık 2008, Perşembe	Sayfa : 757

BİLDİRİ

Resmi Gazete'nin bu sayısı aşağıdaki Ek'leri ihtiva etmektedir.

KKTC Devlet Basımevinde basılmıştır.

ELEKTRONİK İMZA YASASI
(93/2007 Sayılı Yasa)
Madde (20) Altında Yapılan "Elektronik İmza Yasasının Uygulanmasına İlişkin Usul ve Esaslar Tüzüğü" ne bağlı Yönetmelik

Kuzey Kıbrıs Türk Cumhuriyeti Bayındırlık ve Ulaştırma Bakanlığı Telekomünikasyon Üst Kurulu Başkanlığı, 93/2007 sayılı Elektronik İmza Yasası'na bağlı "Elektronik İmza Yasası'nın Uygulanmasına İlişkin Usul ve Esaslar Tüzüğü"nün 27'nci maddesinin kendisine verdiği yetkiyi kullanarak aşağıdaki Yönetmeliği yapar:

Kısa İsim

1. Bu Yönetmelik, "Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Yönetmelik" olarak isimlendirilir.

BİRİNCİ KISIM
Genel Kurallar

Tefsir

2. Bu Yönetmelikte metin başka türlü gerektirmedikçe:
"BS" (British Standards): İngiliz Standartlarını
"CEN" (Comité Européen de Normalisation): Avrupa Standardizasyon Komitesini,
"CWA" (CEN Workshop Agreement): CEN Çalıştay Kararını,
"DSA" (Digital Signature Algorithm): Sayısal İmza Algoritmasını,
"DSA" Eliptik Eğrisi (DSA Elliptical Curve): Sayısal İmza Algoritması Eliptik Eğrisini,
"EAL" (Evaluation Assurance Level): Değerlendirme Garanti Düzeyini,
"ETSI" (European Telecommunications Standards Institute): Avrupa Telekomünikasyon Standartları Enstitüsünü,
"ETSI SR" (ETSI Special Report): ETSI Özel Raporunu,
"ETSI TS" (ETSI Technical Specification): ETSI Teknik Özelliklerini,
"FIPS PUB" (Federal Information Processing Standards Publications): Federal Bilgi İşleme Standartları Yayınlarını,
"IETF RFC" (Internet Engineering Task Force Request for Comments): İnternet Mühendisliği Görev Grubu Yorum Talebini,
"ISO/IEC" (International Organisation for Standardisation / International Electrotechnical Commitee): Uluslararası Standardizasyon Teşkilatı / Uluslararası Elektroteknik Komitesini,
"ITU" (International Telecommunication Union): Uluslararası Telekomünikasyon Birliğini,
"RIPEMD" (RACE Integrity Primitives Evaluation Message Digest): RACE Bütünlük Asli Mesaj Değerlendirme Özetini,
"RSA": Rivest-Shamir-Adleman'ı,
"SHA" (Secure Hash Algorithm): Güvenli Özet Algoritmasını,
"Tüzük" : Elektronik İmza Yasasının Uygulanmasına İlişkin Usul ve Esaslar Tüzüğü'nü anlatır.

93/2007

Bu Yönetmelikte yer almayan tanımlar için Elektronik İmza Yasası'nda ve Tüzükte yer alan tanımlar geçerlidir.

Amaç

3. Bu Yönetmeliğin amacı, elektronik imzaya ilişkin süreçleri ve teknik kriterleri detaylı olarak belirlemektir.

Kapsam

4. Bu Yönetmelik; 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.

İKİNCİ KISIM
Teknik Hususlar

ESHS'nin İşleyişi

5. (1)ESHS işleyişinin bütün aşamalarında,
A) ETSI TS 101 456 ve
B) CWA 14167-1
standartlarına uyar.
(2)Nitelikli Elektronik Sertifikalar;
A)ETSI TS 101 862 ve
B)ITU-TRec. X.509V.3'e
uygun olarak oluşturulur.

Algoritmalar ve Parametreler

6. İmza oluşturma ve doğrulama verileri ile özetleme algoritmaları, ETSI TS 102 176-1 standardına ve aşağıda yeralan şartlara uygun olmalıdır.
(1) İmza sahibinin imza oluşturma ve doğrulama verileri
A) RSA için en az 1024 bit veya
B) DSA için en az 1024 bit veya
C) DSA Eliptik Eğrisi için en az 163 bit
(2) ESHS'nin imza oluşturma ve doğrulama verileri
A) RSA için en az 2048 bit veya
B) DSA için en az 2048 bit veya
C) DSA Eliptik Eğrisi için en az 256 bit
(3) Özetleme Algoritması
A) RIPE MD – 160 veya
B)SHA – 1 veya
C) SHA – 224 veya
D) SHA – 256 veya
E)WHIRLPOOL

Sertifika İlkeleri ve Sertifika Uygulama Esasları

7. ESHS, sertifika ilkelerini ve sertifika uygulama esaslarını IETF RFC 3647'ye uygun olarak hazırlar.

Güvenli Elektronik İmza Oluşturma ve Doğrulama Araçları

8. Güvenli Elektronik İmza oluşturma araçları CWA 14169 standardına uygun ve TS ISO/IEC 15408 (-1,-2,-3)'e veya ISO/IEC 15408 (-1,-2,-3)'e gore en az EAL4+ seviyesinde olmalıdır.
ESHS, sağlamış olduğu güvenli elektronik sertifika doğrulama araçları için CWA 14171 standardına uyar ve bunu taahhüt eder.

Güvenlik Kriterleri

9. ESHS, güvenlik kriterlerine ilişkin olarak;
(1) CWA 14167-1
(2) ETSI TS 101 456 ve
(3) TS ISO/IEC 17799 veya ISO/IEC 17799
standartlarına uyar.

Zaman Damgası ve Hizmetleri

10. ESHS, zaman damgası ve hizmetlerine ilişikn olarak;
(1) CWA 14167-1 ve
(2) ETSI TS 101 861
standartlarına uyar.
Zaman damgası ilkeleri ve zaman damgası uygulama esasları ETSI TS 102 023'e uygun olarak hazırlanır.

Mobil Elektronik İmza

11. ESHS'ler, mobil elektronik imza hizmetlerinde;

(1) dolaşım ile ilgili olarak ETSI TS 102 207 standardına ve

(2) nitelikli elektronik sertifika başvurusu, oluşturulması, yayınlanması ve yenilenmesi süreçleri ile ilgili olarak ETSI TS 102 204 standardına uyar ve bu standartlara uygunluğunu gösteren taahhütnamelerini Kuruma sunar.

Belgeler

12. ESHS;

(1) TS ISO/IEC 27001 veya ISO/IEC 27001 standardına uygunluğunu,

(2) Güvenli elektronik imza oluşturma araçlarının

A) FIPS PUB 140-2'ye göre seviye 3 veya üzerinde olduğunu veya

B) CWA 14167-2'de belirtilen kriterlere uygunluğunu veya

C) CWA 14169 standardına uygun ve TS ISO/IEC 15408 (-1,-2,-3)'e veya ISO/IEC 15408 (-1,-2,-3)'e göre en az EAL4+ seviyesinde olduğunu,

yetkili kurum veya kuruluşlardan alınan belgelerle belgelendirir.

ÜÇÜNCÜ KISIM
Geçici Kurallar

Geçici Madde

"Algoritmalar ve Parametreler" başlıklı 6'ncı maddedeki koşullar 31.12.2009 tarihine kadar geçerlidir.

DÖRDÜNCÜ KISIM
Son Kurallar

Yürütme Yetkisi

13. Bu Yönetmelik, Telekomünikasyon Üst Kurulu Başkanı tarafından yürütülür.

Yürürlüğe Giriş

14. Bu Yönetmelik, Resmi Gazetede yayımlandığı tarihten başlayarak yürürlüğe girer.