ELEKTRONİK İMZADA GÜVENLİK VE STANDARTLAR

TELEKOMÜNİKASYON KURUMU
E - İMZA ÇALIŞMA GRUBU

22 Mart 2005

Güvenlik ve Standartlar

Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ 6 Ocak 2005 tarih ve 25565 sayılı Resmi Gazete'de yayınlanmıştır.

Elektronik İmza Güvenliği

- ESHS Güvenliği
- Algoritma Güvenliği
- İmza Oluşturma/Doğrulama Araçları Güvenliği

ESHS Güvenliği

ESHS;

- Güvenli ürün ve sistemleri kullanmakla
- Hizmeti güvenilir bir biçimde yürütmekle
- Sertifikaların taklit ve tahrif edilmesini önlemekle

ilgili her türlü tedbiri almakla yükümlüdür.

ESHS Güvenliği

- ESHS'nin İşleyişi
- Sertifika İlkeleri ve Sertifika Uygulama Esasları
- Güvenlik Kriterleri
- Zaman Damgası ve Hizmetleri
- Belgeler

ESHS'nin İşleyişi

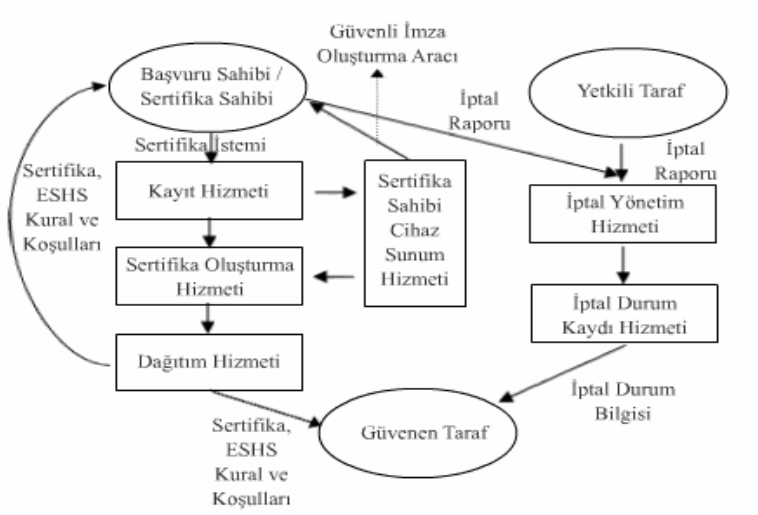
ESHS, işleyişinin bütün aşamalarında;

a) ETSI TS 101 456 ve

b) CWA 14167-1

standartlarına uymakla yükümlüdür.

ETSI TS 101 456



CWA 14167-1

Ana hizmetler:

- Kayıt Hizmeti
- Sertifika Oluşturma Hizmeti
- Dağıtım Hizmeti
- İptal Yönetim Hizmeti
- İptal Durum Hizmeti

Tamamlayıcı hizmetler:

- Sertifika Sahibi Cihaz Sunum Hizmeti
- Zaman Damgası Hizmeti

Sertifika İlkeleri ve Sertifika Uygulama Esasları

TELEKOMÜNİKASYON KURUMU

ESHS, Sertifika İlkeleri (Sİ) ile

Sertifika Uygulama Esasları'nı (SUE)

IETF RFC 3647'ye uygun olarak hazırlar.

RFC 3647 – Sİ ve SUE

TELEKOMÜNİKASYON KURUMU

Sertifika İlkeleri (Sİ):

* Sertifika yönetim kuralları
* Sertifikaya ilişkin sınırlamalar
* ESHS, kullanıcı ve üçüncü kişinin sorumlulukları
* İlgili hukuki düzenlemeler

Sertifika Uygulama Esasları (SUE):

* Sertifika yönetimine ilişkin kurallar ve uygulama süreci
* ESHS'nin işleyişine ilişkin ayrıntılı açıklamalar
* ESHS'nin sorumluluklarını nasıl yerine getireceği

Zaman Damgası için Sİ ve SUE

RFC 3647 – Sİ ve SUE

- Sertifika yayınlama ve depolama
- Kimlik tesbiti ve doğrulama
- Sertifika yaşam döngüsü işletim kuralları
- Tesisler, yönetim ve işletmeye yönelik kontroller
- Teknik güvenlik kontrolleri
- Sertifika, CRL ve OCSP profili
- Uygunluk değerlendirmesi ve raporlaması
- Diğer konular ve hukuki hususlar

ESHS'ye İlişkin Güvenlik Kriterleri

ESHS, güvenlik kriterlerine ilişkin olarak;

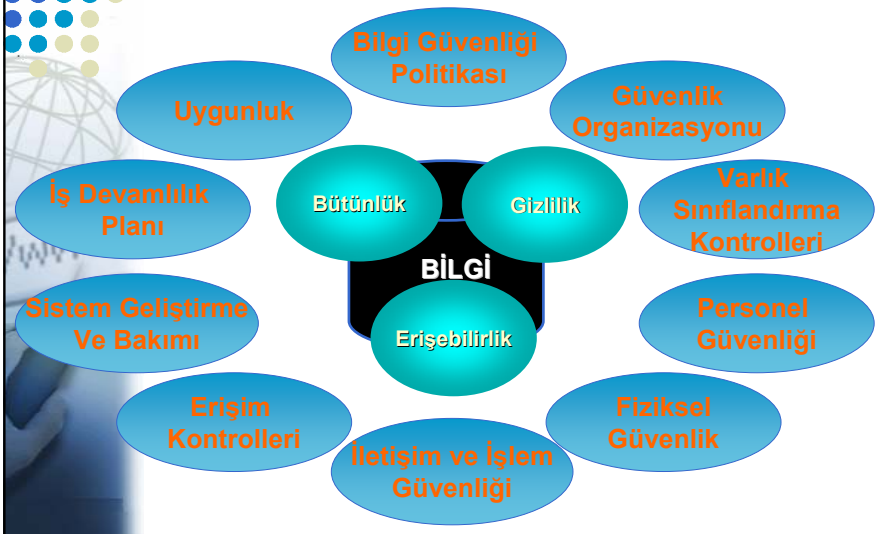
a) CWA 14167-1,

b) ETSI TS 101 456 ve

c) TS ISO/IEC 17799 veya ISO/IEC 17799

standartlarına uyar.

ISO/IEC 17799'un 10 Kontrol Hedefi



Zaman Damgası

ESHS, zaman damgası ve hizmetlerine ilişkin olarak;

a) CWA 14167-1 ve

b) ETSI TS 101 861

standartlarına uyar.

Zaman damgası ilkeleri ve zaman damgası uygulama esasları ETSI TS 102 023'e uygun olarak hazırlanır.

ESHS'den Talep Edilen Belgeler

ESHS;

a) BS 7799-2 standardına uygunluğunu,

b) Güvenli elektronik imza oluşturma araçlarının;

i. FIPS PUB 140-1 veya FIPS PUB 140-2'ye göre seviye 3 veya üzerinde olduğunu veya

ii. CWA 14167-2'de belirtilen kriterlere uygunluğunu veya

iii. 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.

BS 7799-2

BS 7799-2'de ISMS yapısı oluşturulmuştur.

* Varlık tesbiti ve sınıflandırması
* Risk yönetimi ve değerlendirmesi
* Açıklık analizi ve güncelleme
* İç denetim ve kontroller
* Fiziki ve personel güvenliği
* Operasyonel güvenlik
* Bilgi güvenliği politikası
* ...

Elektronik İmza Güvenliği

- ESHS Güvenliği
- Algoritma Güvenliği
- İmza Oluşturma/Doğrulama Araçları Güvenliği

E-imzada Kullanılan Algoritma ve Parametreler

İmza oluşturma ve doğrulama verileri, aşağıda belirtilen algoritma ve parametrelere uygun olarak oluşturulur;

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 160 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**

31.12.2005 tarihine kadar geçerlidir.

Özetleme Algoritması (Hash)

TELEKOMÜNİKASYON KURUMU

Özetleme algoritması (hash) olarak;

a) RIPEMD-160 veya

b) SHA-1

kullanılır.

31.12.2005 tarihine kadar geçerlidir.

Özetleme Algoritması (Hash)

TELEKOMÜNİKASYON KURUMU

* Sabit çıkışlı (RIPEMD-160 bit, SHA-1 128 bit)

* Geri dönüşümsüzdür

* İki farklı mesajın hash değeri birbirinden farklıdır

Elektronik İmza Güvenliği

- ESHS Güvenliği
- Algoritma Güvenliği
- İmza Oluşturma/Doğrulama Araçları Güvenliği

Güvenli İmza Oluşturma/Doğrulama Araçları

Güvenli elektronik imza oluşturma araçları;

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 olmalıdır.

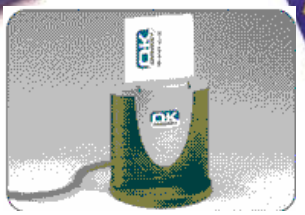
Güvenli elektronik imza doğrulama araçları;

CWA 14171 standardına uygun olmalıdır.

Elektronik İmza Oluşturma Araçları

TELEKOMÜNİKASYON KURUMU

- İmza Oluşturma Verisini tutan yazılım/donanım aracı
- Özellikleri
  - İmza Oluşturma Verisi araç dışına çıkarılamaz.
  - İmzalama işlemi araç üzerinde gerçekleştirilir.
  - Kullanılması zorunludur.
  - Standartları tebliğ ile belirlenmiştir. (EAL 4+)

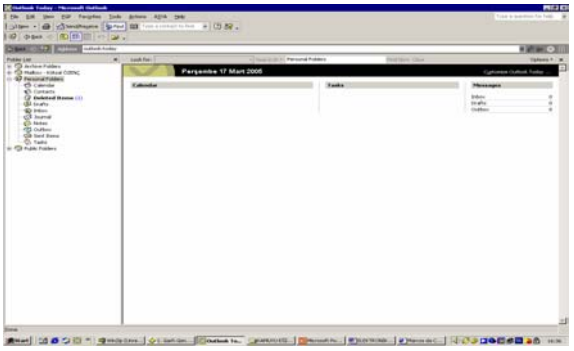


Elektronik İmza Doğrulama Araçları

TELEKOMÜNİKASYON KURUMU

İmza doğrulama işlemini gerçekleştiren yazılım/donanım aracı

- Özellikleri
  - Standartları tebliğ ile belirlenmiştir.
  - Kullanılması zorunludur.



Ortak Kriter (CC)

ORTAK KRİTER: **Bilgi teknolojisi güvenliği değerlendirmeleri için ortaya çıkartılan kriterlerin bütününü temsil eder.**

ISO/IEC 15408-1: Giriş ve Genel Model
ISO/IEC 15408-2: Güvenlik Fonksiyonel Gereksinimleri
ISO/IEC 15408-3: Güvenlik Garanti Gereksinimleri

ORTAK KRİTERİN KULLANIMI:

* **Bir ürünün veya sistemin mevcut güvenlik özelliklerini değerlendirirken**
* **Bu özelliklerinde değişiklik yaparken,**
* **Güvenlik özellikleri olan bir ürünün veya sistemin satın alımında**

Ortak Kriter (CC)

Değerlendirme Garanti Düzeyi
(EAL-Evaluation Assurance Level)

EAL 1: Fonksiyonel Olarak Test Edilmiş (Düşük)

EAL 2: Yapısal Olarak Test Edilmiş (Düşük)

EAL 3: Metodolojik Olarak Test Edilmiş (Orta)

EAL 4: Metodolojik Tasarım, Test ve Kontrol (Orta)

EAL 5: Yarı-Biçimsel Tasarım ve Test (Yüksek)

EAL 6: Yarı-Biçimsel ve Doğrulanmış Tasarım ve Test (Yüksek)

EAL 7: Biçimsel ve Doğrulanmış Tasarım ve Test (Mükemmel)

Nitelikli Elektronik Sertifika

TELEKOMÜNİKASYON KURUMU

Nitelikli elektronik sertifikalar;

a) ETSI TS 101 862 ve

b) ITU-T Rec. X. 509 V.3'e

uygun olarak oluşturulur.

ETSI TS 101 862

TELEKOMÜNİKASYON KURUMU

- **Direktif'in Madde 5'inde belirtildiği üzere nitelikli sertifikalar öneme haiz olduğundan nitelikli sertifikaya dahip ileri e-imzalar hukuki işlemlerde delil olarak sayılmaktadır.**

- **Sertifikanın nitelikli olduğuna dair bir ibarenin bulunması zorunludur.**

% 100 Güvenlik ???

TELEKOMÜNİKASYON KURUMU

Sayısal imza kullanımında dikkat edilecek hususlar

* Sertifikadaki kısıtlamalara uyulması
* Sertifikanın geçerlilik süresi (CRL, OCSP)
* Sertifikanın nitelikli sertifika şartlarını taşıması
* Standartlara uygun cihaz ve yazılım kullanmak
* İmza oluşturma araçlarını başkasına kullandırmamak
* İmza oluşturma aracına erişim şifresini başkasına vermemek/kullandırmamak
* ...

SONUÇ: Kişilerin bilgili ve bilinçli olması