ELEKTRONİK İMZA GÜVENLİĞİ VE GÜVENLİK STANDARTLARI ÇERÇEVESİNDE DÜZENLEYİCİ YAKLAŞIMLAR

Kemal Sacid SARIKAYA

UZMANLIK TEZİ

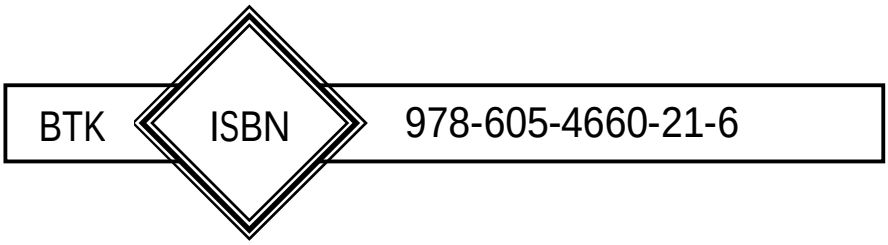
TELEKOMÜNİKASYON KURUMU

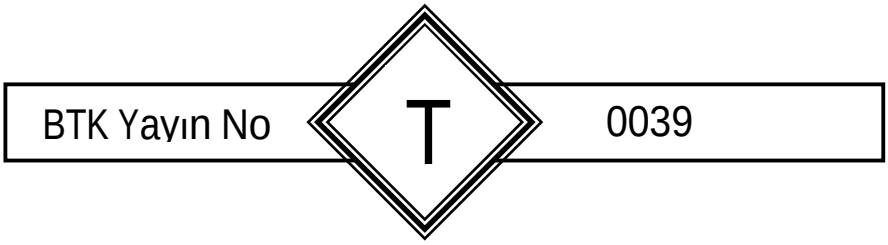
Mart 2005

ANKARA

Bu yayında öne sürülen fikirler eserin yazarına aittir;

Bilgi Teknolojileri ve İletişim Kurumunun görüşlerini yansıtmaz.





Kemal Sacid SARIKAYA tarafından hazırlanan "ELEKTRONİK İMZA GÜVENLİĞİ VE GÜVENLİK STANDARTLARI ÇERÇEVESİNDE DÜZENLEYİCİ YAKLAŞIMLAR" adlı bu tezin Uzmanlık Tezi olarak uygun olduğunu onaylarım.

Doç. Dr. Mustafa ALKAN
Tez Yöneticisi

Bu çalışma, jürimiz tarafından Uzmanlık Tezi olarak kabul edilmiştir.

Başkan : Dr. Murat ATALI

Üye : A. Hicabi ERDİNÇ

Üye : Doç. Dr. Mustafa ALKAN

Üye : Ejder ORUÇ

Üye : Müminhan BİLGİN

Üye : Doç. Dr. Haluk KONURALP

Üye : Yrd. Doç. Dr. Mine ERTURGUT AKKAN

Bu tez, Telekomünikasyon Kurumu tez yazım kurallarına uygundur.

İÇİNDEKİLER

ELEKTRONİK İMZA GÜVENLİĞİ VE GÜVENLİK STANDARTLARI ÇERÇERVESİNDE DÜZENLEYİCİ YAKLAŞIMLAR

(Telekomünikasyon Uzmanlık Tezi)

Kemal Sacid SARIKAYA

TELEKOMÜNİKASYON KURUMU

Mart 2005

ÖZET

Teknolojik gelişmeler, internetin geniş kitlelere ulaşması ve elektronik ortamda güvenli işlem yapabilme ihtiyacı elektronik imzanın ortaya çıkmasına neden olan başlıca unsurlar arasında sayılabilir. Elektronik olarak gerçekleştirilen işlemlere hukuki bir altyapı kazandıran elektronik imzanın güvenliği ve güvenilirliği ele alınması gereken hususlar arasındadır. Bu tez çalışması kapsamında, elektronik imzaya ilişkin temel bilgiler verilerek güvenliği etkileyebilecek faktörlere değinilmiş; ortaya çıkabilecek sorunlar ve güvenlik açıklıklar çerçevesinde, kullanıcıların ve sertifika hizmet sağlayıcılarının karşılaşabilecekleri risk ve tehditler incelenmiştir. Ayrıca, güvenlikle ilgili standartlara ve ülke örneklerine genel bir bakış ile Türkiye'de ve diğer ülkelerde yapılan düzenlemelere ve atılması gerekecek muhtemel adımlara ilişkin değerlendirmelere yer verilmiştir.

Anahtar Kelimeler : Elektronik imza, açık anahtar altyapısı, güvenlik, şifreleme, imzalama algoritması, özetleme algoritması, imza oluşturma aracı, imza doğrulama aracı

Sayfa Adedi : 137

Tez Yöneticisi : Doç. Dr. Mustafa ALKAN

ELECTRONIC SIGNATURE SECURITY AND SECURITY STANDARDS: A REGULATORY APPROACH

(Telecommunications Expert Thesis)

Kemal Sacid SARIKAYA

TELECOMMUNICATIONS AUTHORITY

March 2005

ABSTRACT

Technological developments, spread of internet to large masses, and the need for secure transactions in the electronic environment can be count as the main reasons behind the appearance of electronic signature. Electronic signature, that establishes a legal framework to electronic transactions, has important issues which have to be dealt with, like security and reliability. Under the scope of this thesis study, basic information about electronic signature is given and factors that may affect security are mentioned, risks and threats of users and certificate service providers are analyzed under the framework of potential problems and security gaps. In addition to this, study contains a broad look to security standards, applications in different countries, regulations in Turkey and other countries and an evaluation of necessary steps which are likely to be taken.

Keywords : Electronic signature, public key infrastructure, security, encryption, signature algorithm, hash algorithm, signature creation device, signature verification device

Number of Pages : 137

Advisor : Assoc. Prof. Mustafa ALKAN

TEŞEKKÜR

Çalışmalarıma yaptığı katkılardan, yönlendirmelerinden ve sabrından dolayı tez danışmanım Sayın Doç. Dr. Mustafa ALKAN'a, desteklerini esirgemeyen Sayın Müberra GÜNGÖR'e, yardımlarından dolayı çalışma arkadaşlarıma, bana karşı her zaman anlayışlı olan sevdiklerime ve aileme teşekkürlerimi sunarım.

ÇİZELGELERİN LİSTESİ

ŞEKİLLERİN LİSTESİ

KISALTMALAR

AAA	Açık Anahtar Altyapısı
AB	Avrupa Birliği
AES	Advanced Encryption Standard Gelişmiş Şifreleme Standartı
ANSI	American National Standards Institude Amerika Ulusal Standartlar Enstitüsü
BSI	British Standards Institution İngiliz Standartları Enstitüsü
BT	Bilgi Teknolojisi
CC	Common Criteria Ortak Kriterler
CEN	Comité Européen de Normalisation Avrupa Standardizasyon Komitesi
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria Kanada Güvenilir Bilgisayar Ürünleri Değerlendirme Kriterleri
CWA	CEN Workshop Agreement CEN Çalıştay Kararları
DES	Digital Encryption Standard Sayısal Şifreleme Standardı
DH	Değerlendirme Hedefi
DSA	Digital Signature Algorithm Sayısal İmza Algoritması
DSS	Digital Signature Standard Sayısal İmza Standardı
EAL	Evaluation Assurance Level Değerlendirme Garanti Düzeyi
ECDSA	Elliptic Curve DSA Eliptik Eğri DSA
ESHS	Elektronik Sertifika Hizmet Sağlayıcısı

ETSI	European Telecommunications Standards Institute Avrupa Telekomünikasyon Standartları Enstitüsü
FESA	Forum of European Supervisory Authorities for Electronic Signatures Elektronik İmzalar için Avrupa Denetleme Kurumları Forumu
GEİDA	Güvenli Elektronik İmza Doğrulama Aracı
GEİOA	Güvenli Elektronik İmza Oluşturma Aracı
GİOA	Güvenli İmza Oluşturma Aracı
IDEA	International Data Encryption Algorithm Uluslararası Veri Şifreleme Algoritması
IEEE	Institude of Electrical and Electronics Engineers Elektrik ve Elektronik Mühendisleri Enstitüsü
ISO	International Organisation for Standardisation Uluslararası Standardizasyon Teşkilatı
ITSEC	Information Technology Security Evaluation Criteria Bilgi Teknolojileri Güvenlik Değerlendirme Kriterleri
ITU-T	International Telecommunications Union - Telecommunications Standardization Sector Uluslararası Telekomünikasyon Birliği - Telekomünikasyon Standardizasyon Sektörü
İDV	İmza Doğrulama Verisi
İOA	İmza Oluşturma Aracı
İOU	İmza Oluşturma Uygulaması
İOV	İmza Oluşturma Verisi İmza
İT	İmza Takımı
İV	İmzalanmış Veri
LDAP	Lightweighted Directory Access Protocol Hafifletilmiş Dizin Erişim Protokolü
MD	Message Digest Mesaj Özeti

NIST	National Institude of Standards and Technology Ulusal Standart ve Teknoloji Enstitüsü
OAEP	Optimal Asymmetric Encryption Padding Optimal Asimetrik Şifreleme Doldurması
OBEB	Ortak Bölenlerin En Büyüğü
OK	Ortak Kriterler
PKCS	Public-Key Cryptography Standard Açık Anahtar Şifreleme Standardı
RACE	Research Programme in Advanced Communications for Europe Avrupa için Gelişmiş İletişim Araştırma Programı
RC	Rivest Cipher Rivest Şifresi
RIPEMD	RACE Integrity Primitives Evaluation RACE Bütünlük Asli Değerlendirme Mesaj Özeti
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm Güvenli Özet Algoritması
Sİ	Sertifika İlkeleri
SİL	Sertifika İptal Listesi
SUE	Sertifika Uygulama Esasları
TCSEC	Trusted Computer System Evaluation Criteria Güvenilir Bilgisayar Sistemleri Değerlendirme Kriterleri
TOE	Target of Evaluation Değerlendirme Hedefi
TSE	Türk Standardları Enstitüsü
TÜBİTAK	Türkiye Bilimsel ve Teknik Araştırma Kurumu
TÜRKAK	Türk Akreditasyon Kurumu
UEKAE	Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü

1 GİRİŞ

Elektronik imzanın temelleri 1976 yılında, asimetrik şifrelemenin (açık anahtar şifrelemesi) bulunması ile atılmıştır. Asimetrik şifrelemenin ortaya çıkması ile şifrelemede yeni bir döneme girilmiş ve konu ile ilgili birçok çalışma yapılmıştır. Elektronik imzanın kullanımı, özellikle internetin yaygınlaşması ve uygulama alanlarında ortaya çıkan ihtiyaçlar doğrultusunda 90'lı yıllarda önemli bir artış göstermiştir. Elektronik imza; kimlik doğrulama, bütünlük, inkar edememe gibi hayati önem taşıyan işlevlerin yerine getirilmesini sağlamaktadır. Bunların yanında, kurulan açık anahtar altyapıları (AAA) bünyesinde gizlilik fonksiyonu da kolaylıkla hayata geçirilebilmektedir

Elektronik imza sayesinde elektronik ortamda güvenli işlemler yapabilme imkanı genişlemiş ve bu durum hukuki düzenlemelerle desteklenerek elektronik imzanın ıslak imzaya eşdeğer bir hukuki değer kazanması sağlanmıştır. Konunun düzenlenmesi adına ülkemizde yapılan yasal çalışmalar 1999 yılında başlatılmıştır. Çalışmaların tamamlanması sonrasında, 5070 sayılı Elektronik İmza Kanunu, 23 Ocak 2004 tarih ve 25355 sayılı Resmi Gazete'de yayımlanmış ve 23 Temmuz 2004'te yürürlüğe girmiştir. Bu Kanun kapsamında ikincil düzenlemeleri yapmak üzere Telekomünikasyon Kurumu (Kurum) görevlendirilmiştir. Kurum bünyesinde kurulan Elektronik İmza Çalışma Grubu gerekli çalışmaları tamamlamış ve "Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik" ile "Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ" 6 Ocak 2005 tarih ve 25692 sayılı Resmi Gazete'de yayımlanmıştır.

Bu çalışmada; elektronik ortamda güvenli işlem yapılabilmesini sağlamasının yanında birçok işlevi bulunan elektronik imzanın ne kadar güvenli ve güvenilir olduğunun araştırılması ile konuya ilişkin olarak uyulması gereken standartların ve yapılacak düzenlemelerin irdelenmesi amaçlanmıştır.

Bu amaçlar kapsamında, güvenliği etkileyebilecek risk ve tehditler incelenerek; alınması gereken tedbirlere, kullanılacak sistem, cihaz ve algoritmalara ve uygulanacak standartlara teknik ve düzenleyici bir perspektiften bakılmaya çalışılmıştır. Ayrıca; imza sahibi, elektronik sertifika hizmet sağlayıcı, üçüncü kişi ve düzenleyici kurumun üstüne düşen görevlere ve adı geçen tüm tarafların almaları gereken tedbirlere de yer verilmiştir.

Bu çerçevede, kullanılabilecek standartlar ile Avrupa Birliği (AB) ülkeleri başta olmak üzere çeşitli ülkelerce hayata geçirilmiş düzenleme ve uygulamalar örneklendirilerek konuya ilişkin yaklaşımlar incelenmiştir.

Giriş bölümü sonrasında gelen ikinci bölümde, elektronik imza ve açık anahtar altyapısı ile ilgili temel bilgilere yer verilmiştir.

Üçüncü bölümde, elektronik imza güvenliği ile ilişkili hususlar detaylandırılmış, genel güvenlik yaklaşımı ortaya konulduktan sonra elektronik imza güvenliğinin sağlanmasında önem arz eden bileşenler ile bu bileşenleri etkileyebilecek olası risk ve tehditler anlatılmıştır.

Dördüncü bölümde, özellikle Avrupa Birliği bünyesinde hazırlanmış standartlar ile uluslararası kabul görmüş güvenlik standartları detaylı bir şekilde incelenmiştir.

Beşinci bölüm kapsamında; ülke örneklerine yer verilmiş, bu ülkelerde hayata geçirilen elektronik imza güvenliğine ilişkin düzenlemeler detaylandırılmıştır.

Altıncı bölümde, ülkemizde yer alan düzenlemeler incelenip, elektronik imza güvenliğinin sağlanmasında atılabilecek adımlara ilişkin değerlendirmeler sunulmuştur.

Son bölümde ise elektronik imza güvenliğine ilişkin olarak genel değerlendirmeler yapılmıştır.

2 ELEKTRONİK İMZA ve BİLGİ GÜVENLİĞİ

2.1 Elektronik İmza'ya Genel Bakış

Elektronik imza, başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan, kimlik doğrulama amacıyla kullanılan, inkar edememe ve bütünlüğü sağlayan elektronik veriyi temsil etmektedir. Elektronik imza kavramı; sayısal imza ve sayısallaştırılmış imza gibi alt tanımları ihtiva etse de çoğu kullanımda ve bu tezde de sayısal imzayı işaret etmektedir. Sayısal imza, ileri seviye kriptografik teknikler kullanılarak ve açık anahtar altyapısı üzerinden gerçeklenmektedir. 5070 sayılı Elektronik İmza Kanununda da bu yaklaşıma paralel bir durum söz konusudur.

Günümüzde elektronik ortama aktarılan işlemlerin ve iş akışlarının belirli güvenlik seviyesinde gerçekleştirilebilmesi için elektronik imza büyük önem taşımaktadır. Tanımda da bahsedildiği üzere elektronik imza; inkar edememe, bütünlüğün korunması ve kimlik doğrulama fonksiyonlarının hayata geçirilebilmesini sağlamaktadır. Daha açık bir ifadeyle, birbirini tanımayan iki tarafın elektronik bir ortam üzerinden karşılıklı olarak kimliklerinden şüphe duymadan ve gönderilen/alınan verilerin hiçbir şekilde değişmediğini bilerek haberleşmesi elektronik imza yardımıyla mümkün olmaktadır.

Elektronik imza, finans sektörü başta olmak üzere kamu sektöründe, sağlık sektöründe ve iletişimde sıklıkla kullanılmaya başlanmıştır. Hayata geçirilen uygulamaların başlıca örnekleri:

- Bankacılık işlemleri,
- Sigorta işlemleri,
- e-devlet uygulamaları,
- Her türlü başvuru işlemleri,

- Vergi ödemeleri,
- Elektronik oy verme,
- Sağlık bilgileri ve
- Elektronik ofisler.

olarak sıralanabilir.

2.2 Elektronik İmza Teknik Altyapısı

2.2.1 Şifreleme (Kriptografi)

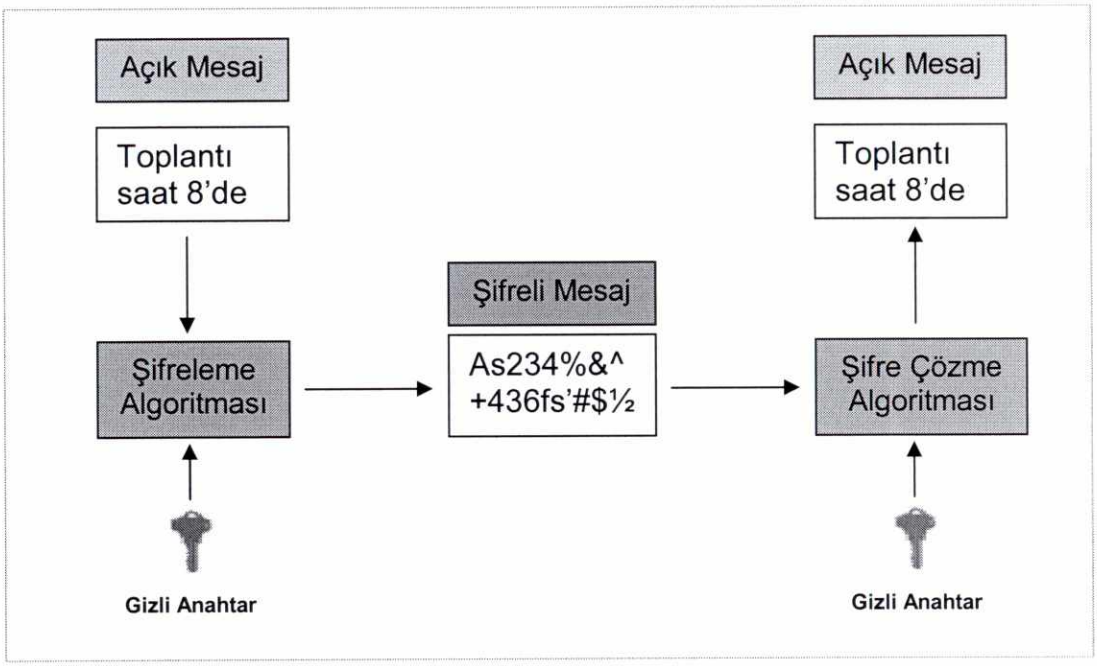
Şifreleme, güvenli olmayan kanallar üzerinden haberleşmede veya verilerin güvenli olmayan ortamlarda saklanmasında kullanılan ve matematiksel fonksiyonlardan oluşan teknikler ve uygulamalar bütünüdür. Kullanılan teknikler ile oluşturulan şifreli veri, farklı bir forma dönüştürülerek anlaşılmaz hale getirilir. Şifrelemede; güvenlik düzeyi, işlevsellik, işlem metotları, performans ve kolay uygulanabilirlik gibi değerlendirme kriterleri önem arz etmektedir. [1]

Şifreleme ve şifre çözmede kullanılan, genelde rastgele bitlerden oluşan veri kümesine anahtar denir. Şifrelemede anahtar seçimi ve uzunluğu güvenlik açısından önemli bir rol oynamaktadır. Ayrıca gizli tutulması gereken bir anahtarın korunması da şifreli verilerin çözülememesi için kritik bir öneme sahiptir.

Yüzyıllardır süregelen gelişmeler ışığında şifreleme teknikleri büyük değişim göstermiştir. Günümüzde modern şifreleme teknikleri, kullanılan anahtarlar temel alınmak üzere simetrik şifreleme ve asimetrik şifreleme olarak iki ana başlıkta incelenebilir.

2.2.1.1 Simetrik Şifreleme

Simetrik şifreleme; şifreleme ve şifre çözme işlemlerinin tek anahtar ile yapıldığı uygulamalardır. Simetrik şifrelemede kullanılan anahtar, şifreleyen ve şifreyi çözen taraflarca gizli tutulmak durumundadır. Bu nedenle simetrik şifreleme, gizli anahtarlı şifreleme olarak da adlandırılmaktadır. (Bkz. Şekil 2.1)



Şekil 2.1 Simetrik Şifreleme

Simetrik şifreleme sistemleri hızlı çalışma ve algoritmaların donanımla kolay gerçeklenebilmesi gibi avantajlara sahiptir. Ancak; anahtar yönetiminin zor olması (Bkz. Çizelge 2.1), gizli anahtarın paylaşılma zorunluluğu, tanınmayan kişilerle haberleşmede oluşabilecek zorluklar ile bütünlük ve kimlik doğrulamanın tam anlamıyla uygulanamaması gibi dezavantajları da beraberinde getirmektedir. [2, 3]

Kullanıcı Sayısı	Anahtar Sayısı
3	3
4	6
10	45
100	4.950
1.000	499.500
10.000	49.995.000
n	n x (n-1) / 2

Çizelge 2.1 Kullanıcı ve Anahtar Sayısı İlişkisi

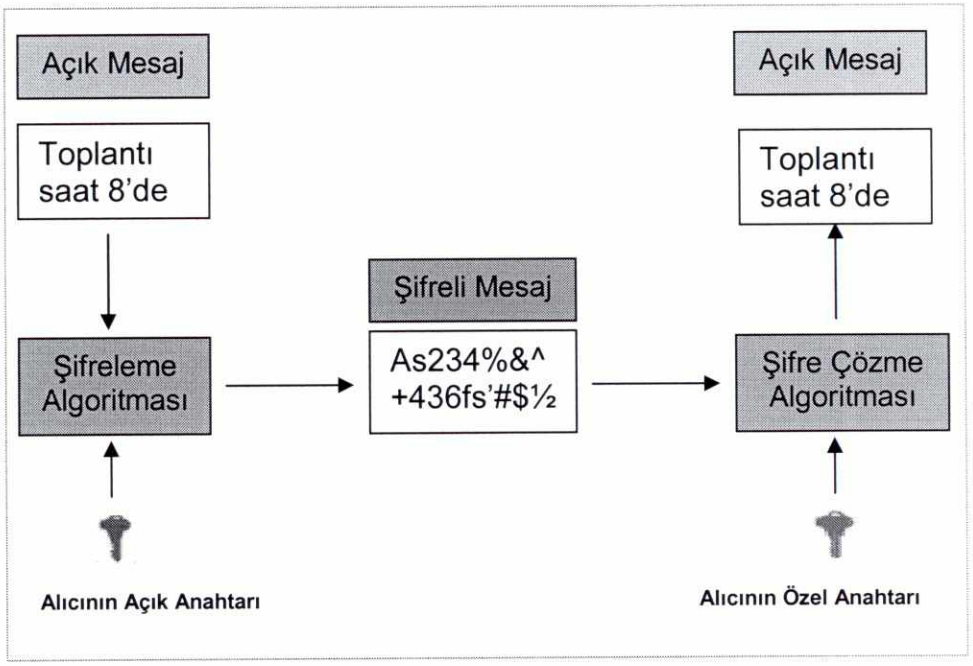
Simetrik şifreleme algoritmalarına örnek olarak DES (Digital Encryption Standard – Sayısal Şifreleme Standardı), AES (Advanced Encryption Standard – Gelişmiş Şifreleme Standardı), RC5 (Rivest Cipher 5 – Rivest Şifresi 5), IDEA (International Data Encryption Algorithm – Uluslararası Veri Şifreleme Algoritması), Blowfish ve CAST verilebilir.

2.2.1.2 Asimetrik Şifreleme

Asimetrik şifreleme, 1970'li yıllarda Whitfield Diffie ve Martin Hellman [4] tarafından ortaya atılmıştır. Bu yöntemde birisi açık birisi de özel olmak üzere matematiksel olarak ilişkili ancak birbirlerinden farklı iki anahtar (anahtar çifti) kullanılmaktadır. Şifreleme işlemi açık anahtarla, şifre çözme işlemi ise özel anahtarla yapılmaktadır. Bu bakımda asimetrik şifreleme, açık anahtar şifrelemesi olarak da adlandırılmaktadır.[5]

Asimetrik şifreleme sistemlerinde özel anahtar gizli tutulur, açık anahtar ise herkesle paylaşılabilir. Örneğin, Ali isimli şahısa gizli bir mesaj göndermek isteyen kişiler Ali'nin açık anahtarıyla mesajı şifreler ve gönderirler. Şifrelenmiş bu mesaj yalnızca açık anahtara karşılık gelen özel anahtara

sahip olan kişi – örnekte Ali – tarafından deşifre edilip okunabilir. (Bkz. Şekil 2.2)



Şekil 2.2 Asimetrik Şifreleme

Açık ve özel anahtar birbiriyle ilişkili oldukları halde açık anahtardan özel anahtara ulaşmak veya tersi bir durum büyük bir işlem gücü gerektirdiğinden dolayı neredeyse imkansızdır.

Asimetrik şifreleme; anahtar yönetiminin kolay olması ve algoritmaların kırılmaya karşı daha dirençli olmaları gibi avantajlara sahiptir. Sisteme dahil olacak her kullanıcı için bir anahtar çifti oluşturmak yeterlidir. Ancak asimetrik şifreleme, simetrik şifrelemeye göre yaklaşık 1500 kat daha yavaş çalışır ve kullanılan anahtarlar bazı uygulamalarda problem oluşturabilecek kadar uzundur. [2]

En çok bilinen asimetrik şifreleme algoritmaları; RSA (Rivest, Shamir, Adleman), Diffie-Helman, ElGamal ve eliptik eğri algoritmaları olarak sıralanabilir.

2.2.2 Özetleme Algoritması

Özetleme algoritmaları, girdi olarak kullanılan herhangi bir uzunluktaki veriyi işleyerek sabit uzunlukta bir özet değeri üreten tek yönlü algoritmalardır. Özetleme algoritmalarının en önemli özellikleri, birbirinden çok az farklı girdiler için dahi tamamen ayrı çıktılar üreterek çakışmaları önleyebilmeleridir. (Bkz. Çizelge 2.2) Özet değerinden girdi verilerine ulaşmak neredeyse imkansızdır. Özet değerleri, veri bütünlüğünün bozulup bozulmadığının kontrolü için kullanılmaktadır. En bilinen özetleme algoritmaları olarak SHA-1 (Secure Hash Algorithm-1 – Güvenli Özet Algoritması-1), RIPEMD-160 (RACE Integrity Primitives Evaluation-160 – RACE Bütünlük Asli Değerlendirme Mesaj Özeti-160) ve MD5 (Message Digest 5 – Mesaj Özeti 5) sayılabilir. [2, 5]

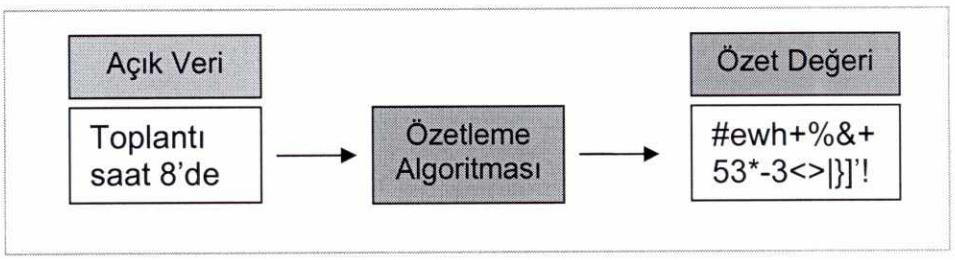
Giriş Metni	Özet Değeri (SHA-1)
Telekomünikasyon Kurumu	53AC528CA6023645A84A2 A8ABA397152C7EC4314
Telekominikasyon Kurumu	D2C3A5EA507DCCD72123 E52A0B677CF8FB675945
Türkiye telekomünikasyon sektöründeki en önemli yapısal değişiklik sektörü düzenleyen temel kanunlarda değişiklik yapan 4502 sayılı Kanundur. Bu Kanunla, Telekomünikasyon Kurumu kurulmuş; politika ve strateji belirleme ile düzenleme ve işletme fonksiyonları birbirinden ayrılmıştır. Politika ve strateji belirleme görevi doğal olarak Ulaştırma Bakanlığında bırakılırken, düzenleyici fonksiyonlar Telekomünikasyon Kurumuna verilmiştir.	5BF166B19B1E688150BB4 6943A97E356E7A2D76F

Çizelge 2.2 Özet Değeri

2.2.3 Elektronik İmzalama ve Doğrulama

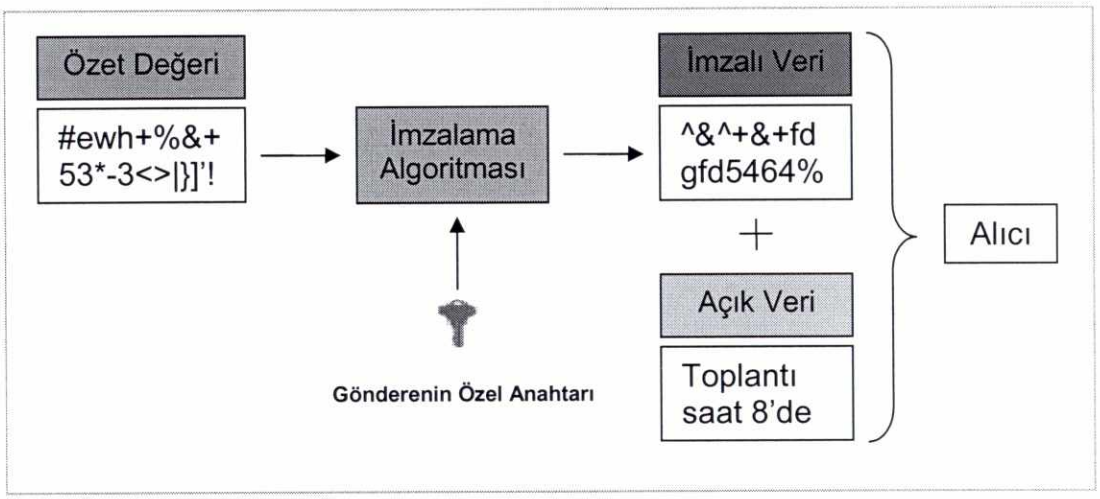
Elektronik imzalama, açık anahtar şifrelemesi tekniği kullanılarak yapılmaktadır. İmzalama ve doğrulama işlemleri adımlar halinde detaylı olarak aşağıda açıklanmıştır. Adım 1 ve Adım 2 imzalama yapan kişi tarafında, Adım 3 ise doğrulama yapan kişi tarafında gerçekleşmektedir.

Adım 1: İmzalanacak veri özetleme algoritmasından geçirilerek sabit uzunlukta olan bir özet değeri elde edilir. Özet değeri hem bütünlük kontrolü için kullanılır hem de gönderilecek verinin büyük olması durumunda imzalama süresini önemli miktarda kısaltır. (Bkz. Şekil 2.3)



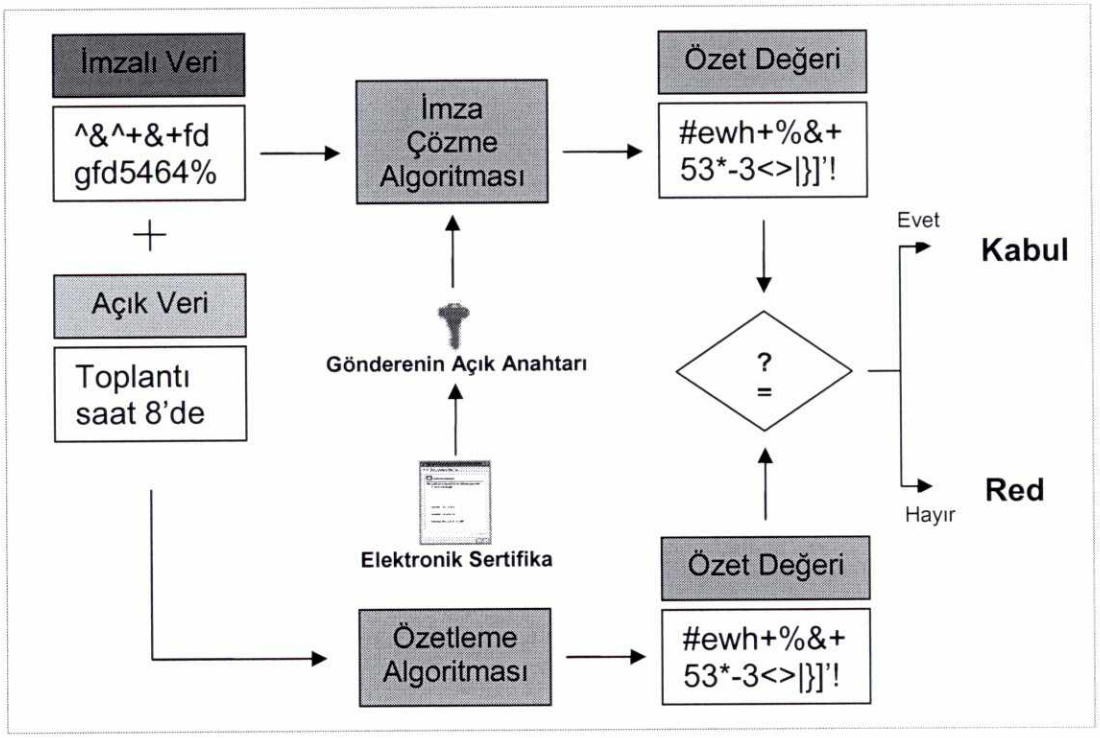
Şekil 2.3 Elektronik İmzalama (Adım 1)

Adım 2: Özet değeri, imzalama yapacak kişinin özel anahtarıyla şifrelenir ve imzalanan verinin orijinali ile birlikte alıcıya gönderilir. (Bkz. Şekil 2.4)



Şekil 2.4 Elektronik İmzalama (Adım 2)

Adım 3: Alıcı, kendisine gelen imzalanmış veriyi gönderen kişinin sertifikasında bulunan açık anahtar ile çözer. Ayrıca imzalanan verinin orijinali özetleme algoritması ile işlenerek özet değeri bulunur ve imzalanan özet değeri ile karşılaştırılır. Bu iki özet değeri arasında yaşanacak bir uyuşmazlık mesajın bütünlüğünün bozulduğunu gösterir. (Bkz. Şekil 2.5) [6]

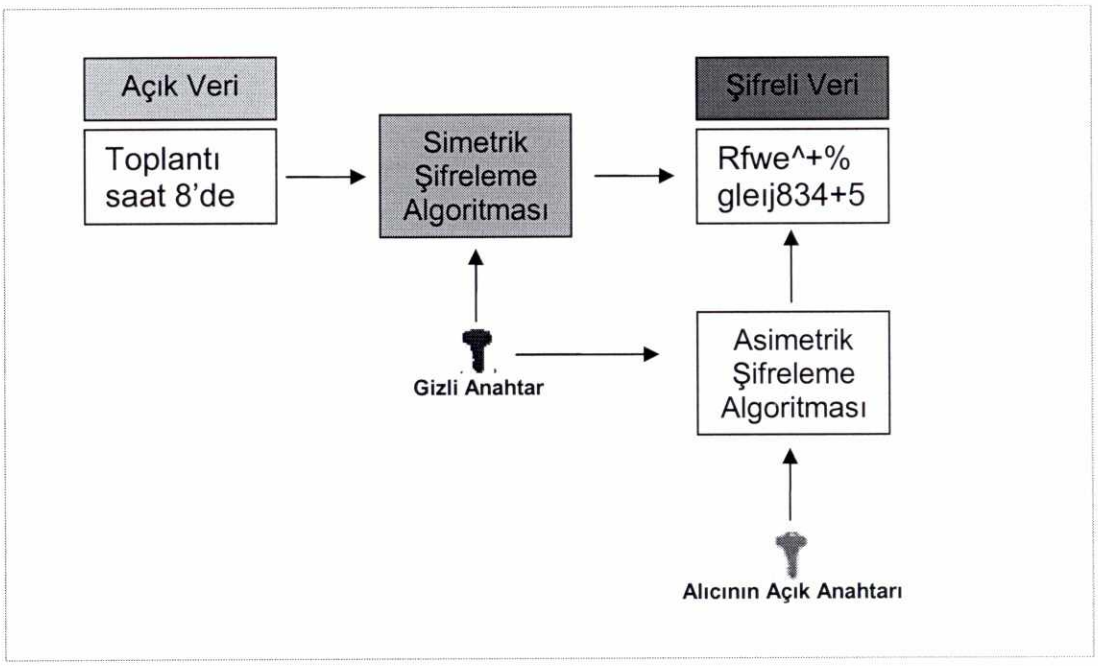


Şekil 2.5 Elektronik İmza Doğrulama (Adım 3)

Genel kanının aksine her kullanıcıya ait bir elektronik imza bulunmamaktadır. İmzalanan veriye göre elde edilen imza değeri değişiklik gösterir; sabit kalan tek unsur ise kullanıcının anahtar çiftidir.

Benzer bir yanılgı da elektronik imzanın gizlilik sağladığı yönündedir. İmzalama işlemi özet değeri üzerinden gerçekleştirilir ve gönderilecek orijinal veri üzerinde herhangi bir değişiklik yapılmaz, yani iletim açık bir şekilde gerçekleştirilir. Verilerin şifrelenerek gizli bir şekilde iletilmek istenmesi durumunda bu veriler simetrik şifreleme kullanılarak gizli hale getirilir. Simetrik şifrelemede ekullanılan gizli anahtar herbir oturum için ayrı ayrı

belirlenir ve alıcı tarafın şifreleme için özel olarak edindiği açık anahtarla şifrelenerek iki taraf arasında paylaşılır. (Bkz. Şekil 2.6) Bu şifreleme yapıldıktan sonra gönderen kişi de dahil olmak üzere şifreleme özel anahtarına sahip olmayan kimse şifreli verinin içeriğini elde etmek için kullanılacak gizli anahtarı elde edemez. Yalnızca alıcı, şifrelemede kullanılan gizli anahtarı şifreleme özel anahtarını kullanarak açabilir. Gizlilik fonksiyonu, açık anahtar altyapısı bünyesinde hayata geçirilebilir.



Şekil 2.6 Şifreleme İşlemi

2.2.4 Açık Anahtar Altyapısı

Açık Anahtar Altyapısı, açık anahtar şifrelemesini destekleyen protokol, hizmet ve standartlardan oluşmaktadır. Literatürde AAA için, açık anahtar sertifikasyonu üzerine kurulmuş güven zinciri [7] veya şifreleme ve elektronik imza hizmetlerinin son kullanıcılara sunumunu sağlayan sistemler şeklinde farklı tanımlamalar da yapılmaktadır. [8]

Günümüzde yapılan birçok çalışmaya rağmen, üzerinde fikir ve uygulama birliğine varılmış açık anahtar altyapı sistemleri bulunmamaktadır. Küresel bir AAA sistemi oluşturulabilmesi yolunda sertifika formatları ve güven mekanizmaları birçok devlet ve standardizasyon kuruluşu tarafından açık ve ölçeklenebilir olarak geliştirilmeye çalışılmaktadır.

Açık anahtar altyapısı; elektronik sertifikaların, açık anahtar şifrelemesinin ve sertifika hizmet sağlayıcıların entegrasyonunu sağlayarak geniş bir güvenlik mimarisi oluşturmaktadır. Tipik bir AAA; bünyesinde yer alan kullanıcılara ve sunucu bilgisayarlara elektronik sertifika verilmesi, sertifikaların yayımlanması, düzenlenmesi, yenilenmesi ve iptal edilmesi ile gerekli teknik desteklerin verilmesi gibi fonksiyonları yerine getirir. [9]

İyi kurulmuş bir AAA; doğru bir şekilde oluşturulmuş güven mekanizması, kolay kullanım, birlikte çalışabilirlik, doğru kimliklendirebilme, ölçeklenebilirlik, esneklik, standartlara uyumluluk gibi özelliklere sahip olmalıdır. [10]

2.2.4.1 AAA İşlevleri

Açık anahtar altyapısı, elektronik imzanın kullanılabilmesini sağlayan temel yapıyı oluşturmaktadır. Elektronik imza ile hayata geçirilen işlevlerin birçoğu AAA tarafından sağlanmaktadır. Bunlar arasında en önemli üç tanesi aşağıda detaylı bir şekilde açıklanmaktadır.

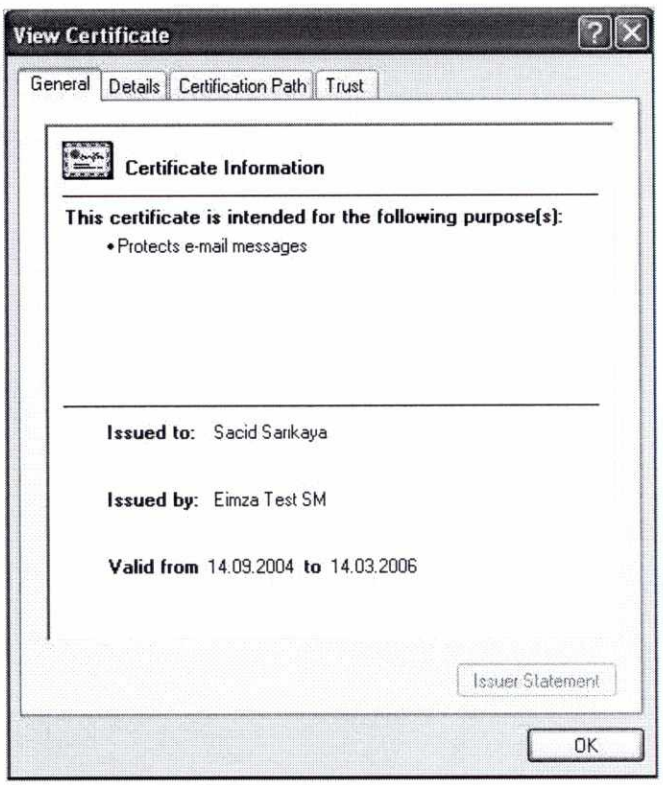
Kimlik Doğrulama: Kimlik doğrulama; bir kullanıcının veya bilgisayarın kendisine ait olduğunu iddia ettiği kimliğin doğrulanması ve onaylanmasıdır. AAA'da kimlik doğrulama işlemleri özel ve açık anahtarla yapılmaktadır. Özel anahtarın gizli tutulması gerektiğinden, yapılan işlemlerin sadece ilgili tarafça gerçekleştirilebileceği kabul edilir. Bunun yanı sıra açık anahtarın ilgili kişiye ait olup olmadığının kontrolü de elektronik sertifikalarla yapılır.

Gizlilik: Gizlilik, iletilen verilerin yetkisiz kişilerden gizlenmesi olarak tanımlanabilir. AAA'da gizlilik; simetrik ve asimetrik şifreleme kullanarak sağlanmaktadır.

Bütünlük: İletilen verilerin doğruluğunun ve eksiksizliğinin sağlanması işlemidir. Gönderilen verinin hedef ve kaynak tarafından karşılıklı olarak özetleme algoritmasından geçirilerek özet değerinin hesaplanması ve çıkan sonuçların karşılaştırılması ile gerçekleştirilir. [11]

2.2.4.2 Açık Anahtar Sertifikası

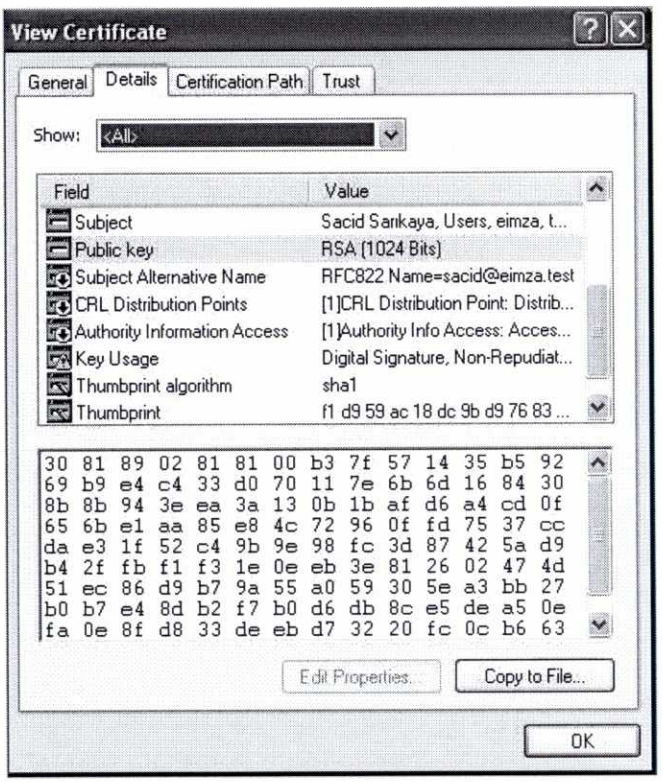
Açık anahtar sertifikası, bir açık anahtarın kime veya neye ait olduğunu gösteren elektronik doküman olup, açık anahtar kullanılarak yapılan işlemlerin doğrulanabilmesini sağlar. (Bkz. Şekil 2.7) [5]



Şekil 2.7 Elektronik Sertifika

Elektronik bir sertifika, temelde en az ait olduğu kişinin ad ve soyadı ile açık anahtarını içermek durumundadır. Fakat genelde; sertifikanın son kullanma tarihi, sertifikayı yayınlayan elektronik sertifika hizmet sağlayıcısının (ESHS) adı, seri numarası, ait olduğu bireyin elektronik posta adresi gibi bilgiler de sertifika içerisinde yer almaktadır. (Bkz. Şekil 2.8) [3]

Sertifikanın ve sertifika içerisinde yer alan bilgilerin doğruluğundan emin olunabilmesi için güven hiyerarşisi kurulmalıdır. Bir başka ifadeyle, yayınlanan sertifikaların güvenilir üçüncü kişiler yani ESHS'ler tarafından elektronik olarak imzalanmış olması gerekir. Bu yapıda hiyerarşinin en üst noktasında bulunan ESHS sertifikasını kendisi imzalar. Bu mekanizma ile herhangi bir kişinin başkası adına sertifika oluşturmasının ve sertifikaların tahrif edilmesinin önüne geçilir.

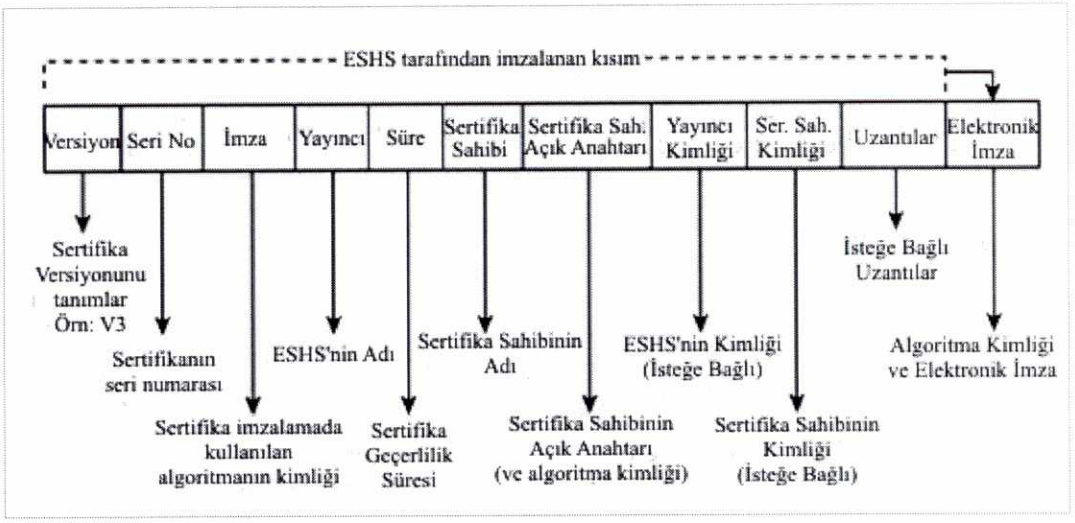


Şekil 2.8 Elektronik Sertifika Detayları

Sertifikalar basit yazılımlardır ve farklı formatlarda oluşturulabilmektedir. PGP (Pretty Good Privacy), SPKI (Simple Public Key Infrastructure – Basit Açık Anahtar Altyapısı) gibi birbirinden farklı yapıda sertifikalar geliştirilmiş olmasına rağmen, halen en yaygın kullanıma sahip olanlar ITU-T'nin (International Telecommunications Union-Telecommunications Standardization Sector – Uluslararası Telekomünikasyon Birliği-Telekomünikasyon Standardizasyon Sektörü) X.509 standardına uygun biçimlendirilmiş sertifikalardır. X.509 sertifikaları :

- Versiyon
- Seri numarası
- İmza Algoritması
- Yayınlayıcı
- Geçerlilik Süresi
- Sertifika Sahibi
- Sertifika Sahibinin Açık Anahtar Bilgisi
- Yayınlayıcının Tekil Kimliği
- Sertifika Sahibinin Tekil Kimliği

gibi standart alanları içermektedir. Bu standart alanların yanı sıra isteğe göre farklı uzantılar da sertifikalara eklenebilmektedir. (Bkz. Şekil 2.9)



Şekil 2.9 X.509 v3 Sertifika Yapısı

2.2.4.3 AAA Bileşenleri

Açık anahtar altyapısı içinde bulunan her bir varlık, AAA bileşeni olarak sayılabilir. Ancak, yapının düzgün bir şekilde işleyebilmesi için gerekli ana unsurlar şunlardır:

Elektronik Sertifika Hizmet Sağlayıcısı: Elektronik sertifikaları imzalayan ve sertifika ile ilgili işlemleri gerçekleştiren güven noktasıdır. ESHS'ler; sertifikaları imzalayarak, sertifika içeriklerinin doğruluğunun güvence altına alınmasını sağlamaktadır. Sertifikaların yayınlanması, yenilenmesi, iptal edilmesi; sertifika ilkelerinin (Sİ) ve sertifika uygulama esaslarının (SUE) yayımlanması gibi işlevlere sahiptir.

Kayıt Kurumu: Elektronik sertifika talebinde bulunanların kimlik kontrollerini yaparak ESHS'ye sertifika oluşturma istemi yapan kurumlardır. AAA altında bulunmaları zorunlu değildir ve bu tür durumlarda görevleri ESHS tarafından yerine getirilir. Kayıt kurumlarının yaygın yerel ofisler şeklinde kurulmasıyla; kolay, iyi ve güvenli hizmet verilmesi amaçlanmaktadır.

Sertifika Deposu: Sertifikaların ve sertifikaların geçerlilik durumunu gösteren iptal durum bilgisinin yayınlanması fonksiyonunu yerine getiren bileşendir. Sertifika deposu olarak genellikle X.500 veya LDAP (Lightweighted Directory Access Protocol – Hafifletilmiş Dizin Erişim Protokolü) dizin sistemleri kullanılsa da sertifikalara web sunucular üzerinden erişilmesi de sağlanabilir. Sertifika depoları genellikle herkes tarafından erişilebilen yapılardır. Ancak bazı AAA sistemlerinde sınırlı/ücretli erişim yapılanması olabilir.

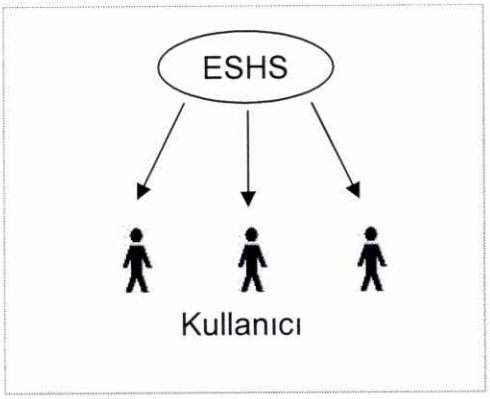
Sertifika Sahibi: Adlarına sertifika düzenlenmiş kullanıcılar veya sistemlerdir. Elektronik sertifika hizmet sağlayıcısına başvuru yapar ve kimliklerini ispat etmek suretiyle sertifika alırlar. Sahip oldukları sertifikalar, sertifika deposunda yayınlanabilir.

Üçüncü Kişi: Sertifikalarla yapılan işlemlere ve atılan elektronik imzaya güvenerek işlem yapan taraflardır. Sertifika depolarına ulaşarak sertifika durumunu kontrol eder. [12, 13, 14]

2.2.4.4 AAA Mimarileri

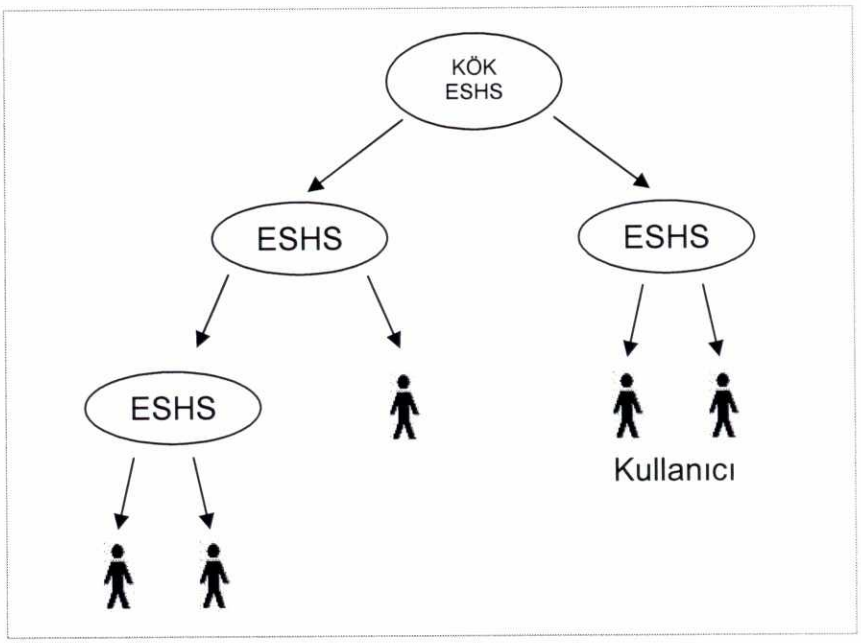
AAA uygulamaları hayata geçirilirken üç çeşit mimari model dikkate alınmaktadır. Bu modeller; elektronik sertifika hizmet sağlayıcılar, kullanıcıların güven duydukları merkez ve sertifika hizmet sağlayıcıların birbirleri arasında kurdukları güven ilişkisi bakımından birbirlerinden farklılık göstermektedir.

Basit Mimari: En temel mimaridir ve yalnızca bir adet ESHS barındırır. Bu ESHS bütün kullanıcıların güven noktasıdır ve sertifika taleplerini karşılar. (Bkz. Şekil 2.10)



Şekil 2.10 Basit Mimari

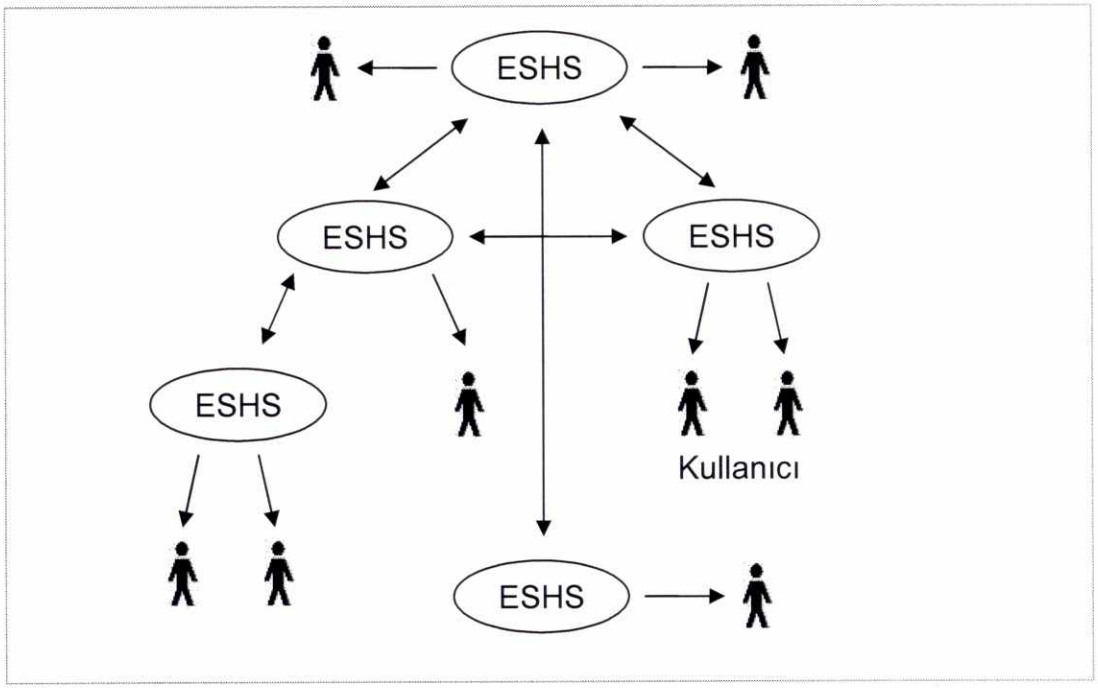
Hiyerarşik Mimari: Bu mimaride tüm ESHS'ler tepe noktada bulunan kök ESHS'ye hiyerarşik olarak bağlıdır. Kök diğer ESHS'leri, ESHS'ler de kullanıcıları ve kendine bağlı diğer ESHS'leri sertifikalandırır. Güven ilişkisi tek yönlüdür ve kök ESHS'nin tamamen güvenli olduğu varsayımına dayanır. (Bkz. Şekil 2.11)



Şekil 2.11 Hiyerarşik Mimari

Ağ Mimarisi: Ağ mimarisinde, güven duyulan birden fazla ESHS vardır ve bu ESHS'ler arasında çapraz sertifikasyon yapılarak güven ağı tesis edilir.

ESHS'lerin birbirleri arasında getirdikleri sınırlamalar sertifikalarda belirtilir. (Bkz. Şekil 2.12)



Şekil 2.12 Ağ Mimarisi

2.2.5 Elektronik Sertifika Hizmet Sağlayıcısı

Literatürde geçen; "Sertifikasyon Kurumu", "Yayınlayıcı Kurum" veya "Sertifika Yayınlayıcı" şeklindeki farklı terimlerin tamamı, 5070 sayılı Elektronik imza Kanununda tanımlanan elektronik sertifika hizmet sağlayıcısı ile aynı kavramı ifade etmektedir. [15]

ESHS'ler, AAA'nın en önemli bileşenlerinden birisidir. Açık anahtarların sertifikalarla ilişkilendirilmesi fikri [16] ortaya atıldıktan sonra güvenilir bir kuruma duyulan ihtiyaç ve kullanılan sertifikaların geçerliliğinin doğrulanması gerekliliği ESHS'lerin önemini artırmıştır.

Birbirini tanıyan kullanıcıların bulunduğu küçük sistemlerde herhangi bir kimlik ispatına veya kontrolüne gerek duyulmazken elektronik imzanın yaygın

kullanılan bir meta haline gelmesi daha önce tanınmayan kişilerle de işlem yapılmasını zorunlu hale gelmiştir. Bu durumda karşılıklı tarafların birbirlerinin kimliklerinden emin olabilmesi için güvenilir bir üçüncü tarafa ihtiyaç duyulmaktadır. Bu güven mekanizmasının merkezinde de ESHS'ler bulunmaktadır. Bu yüzden, güvenilirlik ve kalite güvencesi ESHS seçiminde anahtar rolü oynamaktadır ve bu özelliklerin sağlanması için düzenleme, akreditasyon ve denetleme gibi yaklaşımlar geliştirilmiştir.

2.2.5.1 ESHS'nin Sunduğu Hizmetler

ESHS'ler, elektronik imzanın kullanılmasına yönelik olarak; kayıt, sertifika oluşturma, sertifika dağıtımı, iptal ve iptal durum bilgisi gibi çeşitli hizmetler sunmaktadır:

Kayıt Hizmeti: Sertifika verilen kişilerin kimliklerinin ve sertifika içerisinde yer alacak diğer bilgilerin tam ve doğru bir biçimde tespit edilmesi ile sertifikalarla açık anahtarların eşleştirilmesi ESHS'nin sorumluluğundadır. Ancak ESHS bu görevi kayıt kurumları eliyle de gerçekleştirebilir.

Sertifika Oluşturma: ESHS gerekli bilgileri topladıktan sonra sertifikayı oluşturur ve kendi özel anahtarıyla imzalar.

Sertifika Dağıtımı: Sertifikaların; sahiplerine ve sertifika sahibinin izninin alınması kaydıyla üçüncü kişilere dağıtılmasıdır. Bu hizmet ayrıca; ESHS'nin kural ve koşullarının, yayınlanmış politikalarının ve uygulamaya ilişkin bilgilerinin dağıtımını da kapsamaktadır.

İptal Hizmeti: Sertifika iptallerine ilişkin taleplerin alınmasını, gerekli işlemlerin yapılmasını ve raporlanmasını ihtiva eder. Bu hizmet sonucu ortaya çıkan sonuçlar iptal durum bilgisi hizmeti vasıtasıyla ilgili taraflara sunulmaktadır.

İptal Durum Bilgisi Hizmeti: Üçüncü kişilere, sertifikaların geçerlilik durumlarıyla ilgili bilgi sağlayan hizmettir. İptal durum bilgisi kayıtları gerçek zamanlı veya belirli aralıklarla güncellenen kayıtlar olarak sunulabilir. ESHS, iptal durum bilgisi kayıtlarını imzalayarak yayınlar.

2.2.5.2 Sertifika İlkeleri ve Sertifika Uygulama Esasları

Sertifika ilkeleri, bir ESHS'nin işleyişi ile ilgili taahhütlerini içeren genel kurallar dokümanıdır. Sertifika uygulama esaslarında ise sertifika ilkelerinde yer alan kuralların ne şekilde yerine getirileceği detaylı olarak anlatılır.

Sertifika ilkeleri, sertifika uygulama esaslarından daha basit ve ilgili tüm tarafların erişimine açık dokümanlardır. Doğrulama yapan kişiler tarafından sertifikaların ve sertifikalar içerisinde yer alan bilgilerin yeteri kadar güvenilir veya gerçekleştirilen uygulamalar için uygun olup olmadığını kontrol etmek amacıyla kullanılabilir.[17]

Sertifika uygulama esasları; kural ve koşulların yanı sıra sertifika yönetimi ile ilgili operasyonel yaklaşımları ve yasal hususları da içermektedir. Sertifika uygulama esaslarının, ESHS güvenliğini tehlikeye atabilecek hususlar içeren bölümlerinin kamuya açık olması gerekmez. [18]

2.2.6 Sertifika Sahibi ve Üçüncü Kişi

Sertifika sahibi, adına sertifika düzenlenmiş gerçek kişileri tanımlamaktadır. Sertifika sahibi, başvurusu sırasında ESHS tarafından istenilen bilgileri doğru ve eksiksiz sunmak zorundadır. Bunun yanı sıra sertifikada yer alan bilgilerin değişmesi durumunda bunu ESHS'ye en kısa sürede bildirmelidir. [17]

Sertifika sahibi, özel anahtarını ve özel anahtara erişim şifresini kimseyle paylaşmamalı; özel anahtarının güvenilirliğinden şüphe duyması halinde

sertifikasını iptal ettirmelidir. Sertifika sahibinin yerine getirmesi gereken koşullar sertifika ilkelerinde yer alır. Tüm bunların yanı sıra kanun veya yönetmeliklerle sertifika sahiplerine ek yükümlülükler getirilebilir. [15]

Üçüncü kişi, sertifikada yer alan bilgileri göz önünde bulundurarak elektronik imzayı doğrulayan kişiler olarak tanımlanır. Üçüncü kişinin sertifika içerisinde yer alan bilgilerin muteberliğine ne kadar güveneceği birçok faktöre bağlıdır. Bu faktörler arasında; ESHS'nin sertifika verirken uyguladığı ilkeler, işletme politikaları ve yöntemleri, uygulanan güvenlik kontrolleri ile sertifika sahibinin ve ESHS'nin yükümlülükleri bulunmaktadır. [17]

Üçüncü kişi, bir ESHS tarafından verilmiş sertifikayı kabul etmesi durumunda bu sertifika içerisinde yer alan bilgilerin doğruluğunu da kabul etmiş sayılır. Sertifika, güvenilir bir ESHS tarafından yayınlanmış olsa da doğrulama yapılırken sertifikanın geçerli olup olmadığı sertifika durum bilgisi alınarak kontrol edilmelidir. Ayrıca, sertifikada kullanıma dair kısıtlamalar yer alıyorsa işlemlerin bu kısıtlar çerçevesinde yapıldığından emin olunmalıdır.

2.3 Bilgi ve Bilgi Sistemleri Güvenliği

Bilgi güvenliği, bilgi varlıklarının kasıtlı veya kasıtsız olarak ortaya çıkabilecek yetkisiz erişimlerden, hasarlardan, izinsiz kullanımdan, istenmeyen değişikliklerden veya kaybolma/çalınma gibi durumlardan korunması için kullanılan kavram, teknik ve ölçümlerin tümünü içermektedir. [19] İşleyişi bozabilecek her türlü risk bilgi güvenliği için tehdit oluşturmaktadır. Bu risklerin olabildiğince aşağı çekilmesi sistem ve bilgi güvenliğinin artmasını sağlamaktadır. Ancak alınacak önlemlerin kullanımı zorlaştırmaması, işlevselliği etkilememesi, güvenilir ve maliyet etkin olması gerekmektedir. [20]

Bilgi güvenliği sistemleri için oldukça büyük öneme sahip ve geniş kabul görmüş olan TS ISO/IEC 17799 standardında güvenlik için gereken bileşenler aşağıdaki şekilde sıralanmıştır. [21]

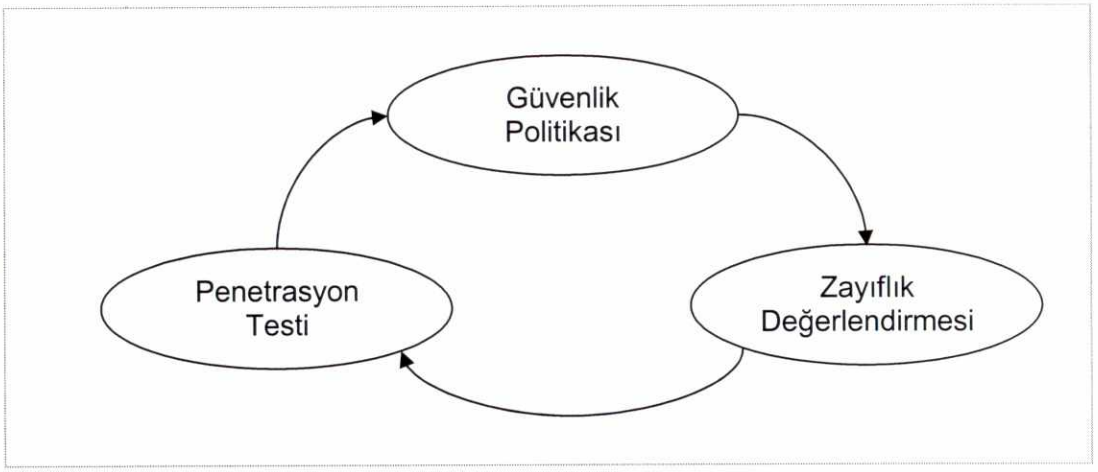
- Güvenlik Politikası
- Organizasyonel Güvenlik
- Varlık Sınıflandırılması ve Kontrolü
- Personel Güvenliği
- Fiziksel Güvenlik ve Çevre Güvenliği
- İletişim ve Operasyon Güvenliği
- Erişim Kontrolü
- Sistem Geliştirme ve Bakım
- İş Sürekliliği Planı
- Uyumluluk

2.3.1 Güvenlik Yaşam Döngüsü

Güvenlik, sürekli bir yaşam döngüsü içerisinde sağlandığında etkili olabilmektedir. Gelişen ve yenilenen teknolojiler ile karşılaşılan tehditler her geçen gün artmakta, risklerin belirlenmesi ve bu riskleri azaltacak önlemlerin alınması süreklilik gerektirmektedir. Bu çerçevede, yaşam döngüsü içerisinde yer alan adımlar:

- zayıflık değerlendirmesi,
- güvenlik politikalarının belirlenmesi ve
- penetrasyon testleri

olarak sıralanabilir. (Bkz. Şekil 2.13)



Şekil 2.13 Güvenlik Yaşam Döngüsü

Zayıflık değerlendirmesi, kurum/kuruluş bünyesinde bulunan varlıkların karşı karşıya kalabileceği risklerin ve halihazırda tespit edilen zayıflıkların ortaya konulmasıdır. Gerekli testler yapıldıktan sonra ortaya çıkan sonuçlar ışığında, güvenlik açıklıkları kullanıldığında çıkabilecek sorunlar ortaya konulur. Bu çıktılar; fiziksel, mantıksal ve verilerden kaynaklanan açıklıkları içerir ve güvenlik politikalarının oluşturulmasında veya güncellenmesinde kullanılır. Zayıflık değerlendirmeleri düzenli aralıklarla tekrarlanmalı ve sistemler günün teknolojik koşulları ışığında yenilenmeli veya değiştirilmelidir. [22]

Bilgi ve bilgi sistemleri güvenliğinin sağlanmasında ikinci adım güvenlik politikalarının oluşturulmasıdır. Güvenlik politikası; ihtiyaç duyulan güvenlik seviyesini belirleyen, bilgi varlıklarını, koruma sorumluluklarını ve kurum/kuruluş taahhütlerini içeren güvenlik çatısını oluşturmaktadır. Bu çatı altında, değerli bilgilerin ne şekilde erişime açılacağını ve korunacağını düzenleyen kural ve uygulamalar bulunmaktadır. [23]

Zayıflık değerlendirmesi sonucunda elde edilen çıktılar değerlendirilip gerekli tedbirler alındıktan sonra penetrasyon testleri yapılmalı ve olası açıklıklar bulunmaya çalışılmalıdır. Gözden kaçan olası güvenlik boşlukları bu testler sonucunda ortaya çıkabilmekte ve güvenliğin artırılması için gerekli sıkılaştırmalar yapılabilmektedir. [22]

2.3.2 Güvenlik Unsurları

Genel çerçevede bakıldığında bilgi güvenliğinin asgari olarak sağlanabilmesi aşağıda belirtilen unsurların yerine getirilmesine bağlıdır. [24, 25]

Gizlilik: Bilginin yetkisiz erişimlere veya kopyalanmasına karşı korunmasıdır. Bilginin bir bütün olarak korunması yanında bu bütünün parçalarının da ele geçirilmesi engellenmelidir. Bu ayrı parçalar tek başına zararsız görünseler bile bütüne ulaşma amacıyla kullanılabilmektedir.

Veri bütünlüğü: Bilginin ve kullanılan programların izin verilmemiş kişiler tarafından değiştirilmesi veya silinmesini kapsamaktadır. Kayıtların, yedeklerin ve dokümanların yanı sıra sahip olunan dosyaların oluşturulma zamanlarına ilişkin bilgilerin korunmasına kadar birçok öğe veri bütünlüğü için önem arz etmektedir.

Erişilebilirlik: Hizmetlerin kullanılamaz veya erişilemez duruma gelmesinin engellenmesidir. Yetkili kullanıcılar sisteme erişmek istediklerinde bu isteğin gerçekleşmemesi; bilginin kaybolması ya da silinmesiyle ortaya çıkacak sonuçların benzerini oluşturmaktadır.

Tutarlılık: Sistemin beklenilen şekilde çalışmasıdır. Kullanılan yazılım ya da donanımın bir yükseltme veya güncelleme sonrasında farklı tepkiler vermesi ve kullanıcıların bundan etkilenmesi tutarlılığın bozulduğunu göstermektedir.

Erişim Kontrolü: Sisteme erişimlerin düzenlenmesi ve kontrol edilmesidir. Sistem içerisinde yer alan her bir varlık için ancak ihtiyaç duyacağı seviyede erişim hakkı verilmeli ve gerekli kontroller yapılmalıdır. Erişim izinleri için politika ve prosedürler de geliştirilebilir.

Denetim Kontrolü: Bilgi sistemleri üzerinde gerçekleştirilen işlemlerin kaydedilmesi ve incelenmesi için ihtiyaç duyulan mekanizmalardır. Şüpheli

erişimlerin, potansiyel tehlikelerin belirlenmesi ve yetkili kullanıcılar tarafından yapılan hataların ortaya çıkarılabilmesi için hangi işlemin, kim tarafından ve ne zaman yapıldığının kayıtları tutulmalıdır.

2.3.3 Risk ve Tehditler

Risk ve tehdit kavramı çoğu zaman birbiriyle karıştırılsa da farklı anlamlar içermektedir. **Risk**, bir bilgi sisteminin karşı karşıya kalabileceği zararları ölçmektedir. **Tehdit** ise olası açıklıkları kullanarak sistemlere zarar veren etkenleri ifade etmektedir. Örneğin bir firma için müşteri listesini kaybetmek bir risk; önemli dosyaların kötü niyetli bir çalışan tarafından silinmesi ise bir tehdit oluşturmaktadır.

Bilgi ve bilgi sistemleri için mutlak bir güvenlikten söz etmek mümkün değildir. Gelişen ve değişen şartlar altında riskler her zaman var olacaktır. Bilgi güvenliğinin sağlanması yönünde yapılan çalışmalarda amaç riski önlemek olmamalıdır. Çünkü karşılaşılabilecek riskleri önlemek teknolojik ve mali açıdan imkansızdır. Ancak risklerin olduğu gibi kabul edilmesi de birçok zarara sebep olabilir. Bu perspektiften bakıldığında, risklerin varlığını kabul etmek fakat bu risklerden kaçınmak için gerekli adımları atarak risk yönetimi de yapmak gerekir. [26]

Etkin bir risk yönetimi için aşağıda sıralanan adımlar gerçekleştirilmelidir. [27]

1. Risk tanımlaması
2. Risk değerlendirmesi
3. Planlama
4. Risk takibi ve yönetimi

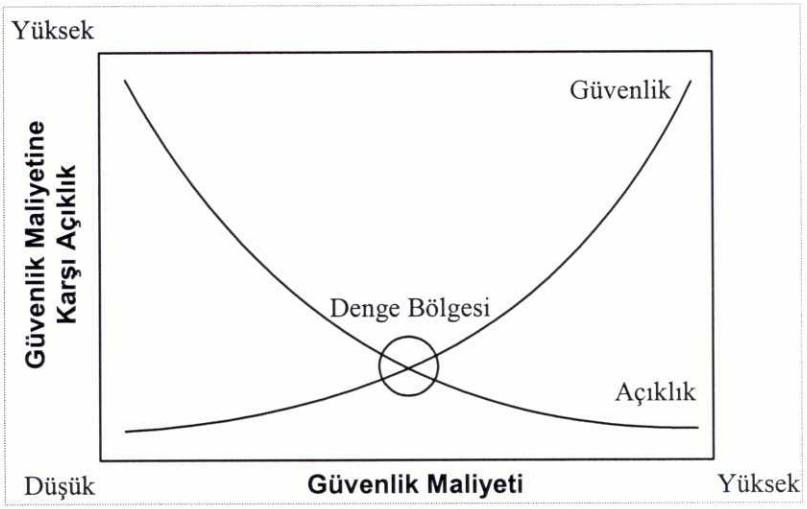
Risklerin tanımlanması sonrasında değişik risklerin gerçekleşme olasılıkları ve bunların verebileceği zararlar dikkate alınarak risk değerlendirmesi yapılır.

Bu değerlendirmede:

Risk = Etki x Olasılık

şeklinde basit bir hesaplama yapılarak riskler değerlerine göre sıralanır. [28] Risk yönetimi sürecinde kabul edilebilir bir risk seviyesi belirlenir ve bu seviyenin altında olan riskler göz önünde bulundurulmaz. Kabul edilebilir risk seviyesi üzerinde bulunan riskler içinse gerekli tedbirler alınır.

Burada göz önünde bulundurulması gereken diğer önemli bir nokta ise maliyettir. Bir risk sonucu herhangi bir zarar doğduğunda oluşacak maliyet ile riski kabul edilebilir seviyeye çekmek için yapılacak harcamaların karşılaştırılması sonrasında riski azaltma maliyeti daha fazla çıkarsa bu maliyetin dengelenmesi gerekmektedir. Belirli bir denge noktası yakalandıktan sonra daha fazla iyileştirme yapılmaz. Çünkü yapılan her sıkılaştırma ek maliyet oluşturacaktır. (Bkz. Şekil 2.14) [29]



Şekil 2.14 Güvenlik Maliyeti – Açıklık Dengesi

Gelişen teknoloji ve değişen güvenlik ihtiyaçları risk değerlendirmesinde farklı sonuçlar ortaya çıkmasına sebep olmaktadır. Bu yüzden gerçekleştirilen bu işlemler belirli aralıklarla tekrarlanmalı ve risk takibi yapılmalıdır.

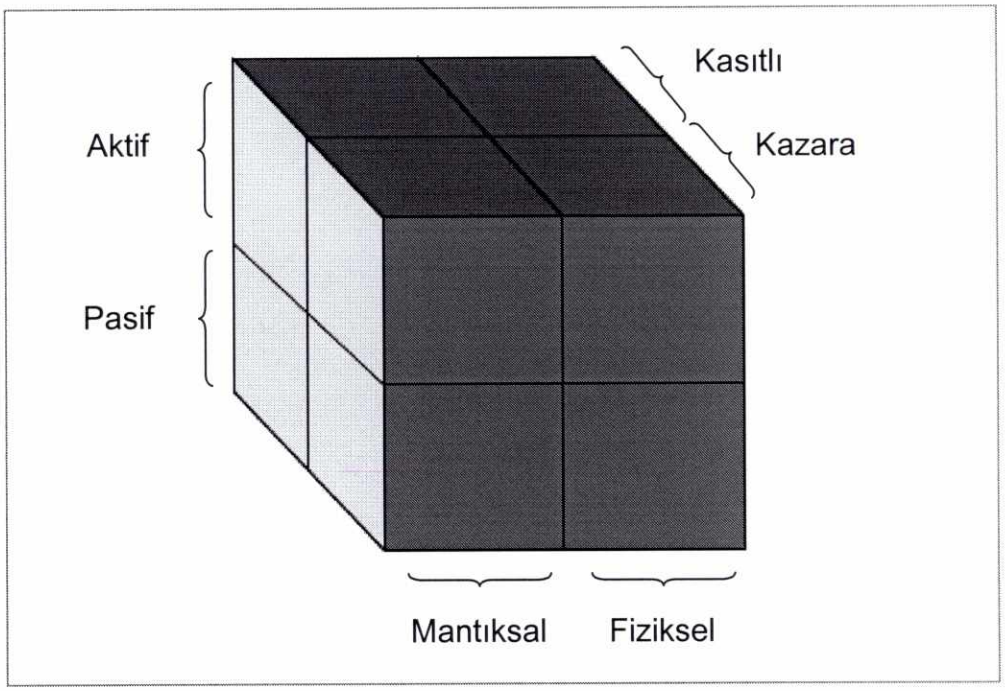
Bilgi sistemleri, çok yüksek maliyetli kayıplara sebep olabilecek farklı tehditlerle karşı karşıyadır. Bu tehditler, sistem erişilebilirliğinden veri bütünlüğüne kadar pek çok güvenlik unsurunu hedef alabilmektedir. Ortaya çıkabilecek tehditlerin iyi bir şekilde bilinmesi ve bunlara yönelik önlemler alınması risk yönetimi sürecinde de büyük önem taşımaktadır.

Tehditler, içeriklerine ve gerçekleşme şekillerine göre aşağıdaki şekilde sınıflandırılabilir:

- Kasıtlı: Kişiler tarafından bilgi sistemlerinde kullanılan açıklıklar kullanılarak gerçekleştirilen saldırılardır. Bilgi sistemlerine izinsiz olarak erişilmesi bu grupta yer alan tehditlerden birisidir.
- Kazara: İstemeden gerçekleşen tehditlerdir. Genellikle bilgi eksikliğinden kaynaklanır. Yetkili bir kullanıcının bilgi eksikliğinden dolayı yanlış işlem yapması örnek olarak verilebilir.
- Mantıksal: Kayıtları, bilgi işlemlerini veya iletimini etkileyen tehdit çeşitleridir. Virüsler ve solucanlar bu gruba dahil edilebilir.
- Fiziksel: Bilgi sistemleri içerisinde yer alan bileşenlerin fiziksel olarak zarar görmesine sebep olan tehditlerdir. Yangın, deprem ve sistemlerin çalınması örnek olarak verilebilir.
- Aktif: Başarıya ulaştıklarında sisteme ve sistemde yer alan verilere zarar veren tehditlerdir. Örneğin web sitesinin yetkisiz kişiler tarafından değiştirilmesi aktif bir tehdittir.
- Pasif: Başarılı olduklarında sisteme hiçbir zarar vermeyen tehditlerdir. Genellikle bilgi veya şifre elde etmede kullanılan saldırılardır. Örneğin kullanıcının bastığı tuşları kaydeden bir program pasif tehditler arasında sayılabilir.

Ortaya çıkabilecek tehditler, yukarıda yer alan sınıflardan bir ya da birkaçına ait olabilir. (Bkz. Şekil 2.15) Örneğin, bilgi işlemde çalışan bir

kişinin ileri bir tarihte çalışması için sisteme yüklediği bir solucan; kasıtlı, mantıksal ve aktif olarak sınıflandırılabilir. [30]



Şekil 2.15 Tehdit Sınıflandırması

3 ELEKTRONİK İMZA GÜVENLİĞİ

3.1 Elektronik İmzada Güvenlik

Elektronik imza güvenliği, kullanılan yazılım ve donanımdan fiziksel korumaya kadar birçok faktöre bağlıdır. Bunun yanında; bir sistemin veya hizmetin güvenliğinin, sahip olduğu bileşenlerden güvenliği en zayıfı seviyesinde olduğu da göz önüne alındığında elektronik imzanın güvenli olarak kullanılabilmesi için elektronik sertifika hizmet sağlayıcıların, kullanıcıların, üçüncü kişilerin ve düzenleyici kurumun çok titiz davranması gerekmektedir.

Elektronik imza güvenliğinde, klasik güvenlik önlemlerinin yanı sıra kullanılan algoritmaların ve anahtarların güvenilir olması da büyük önem taşımaktadır. 5070 sayılı Elektronik İmza Kanununun 5inci maddesinde yer alan "*Güvenli elektronik imza, elle atılan imza ile aynı hukuki sonucu doğurur.*" hükmü uyarınca ilgili tüm taraflar kullanım koşulları ve güvenliğe azami önemi göstermelidir. Çünkü yaşanabilecek olası güvenlik bunalımları hukuki açıdan pek çok yükümlülüğe sebep olabilir.

Elektronik imzanın güvenliğine etki eden en önemli unsurlar aşağıda sıralanmıştır.

1. Özetleme algoritmaları güvenilirliği
2. İmzalama algoritmaları güvenilirliği
3. İmza oluşturma araçları güvenliği
4. İmza doğrulama araçları güvenliği
5. ESHS güvenliği

3.2 Özetleme Algoritmaları ve Güvenilirlikleri

Özetleme algoritmaları, Bölüm 2.2.2'de anlatıldığı üzere farklı uzunluktaki girdiler için sabit uzunlukta ve her bir girdi için farklı sonuçlar üretebilen algoritmalardır. Bu algoritmaların çıktısı olan özet değerleri kullanılarak bütünlük kontrolü yapıldığından dolayı güvenlik açısından önem arz etmektedir.

3.2.1 Özetleme Algoritmalarına Yapılan Saldırılar

Özetleme algoritmalarının güvenliğine yönelik yapılan kriptografik saldırıların birçoğu, rastgele giriş verileri kullanılarak belirlenmiş bir çıktının elde edilmeye çalışılması işlemidir. Bu türde saldırılar hem algoritmaların tek yönlülüğünü hem de çakışma koruması özelliğini tehdit etmektedir.

n bitlik çıktılar üreten bir özetleme algoritması için *y* çıktısını veren girdi verilerine ulaşabilmek için $2^{n/2}$ deneme yapılması beklenir. Bu türde, her bir olasılığın tek tek denendiği saldırılara deneme-yanılma (brute-force) saldırıları denilmektedir. Ancak farklı metotlar kullanılarak bu olasılık değeri yükseltilebilir.

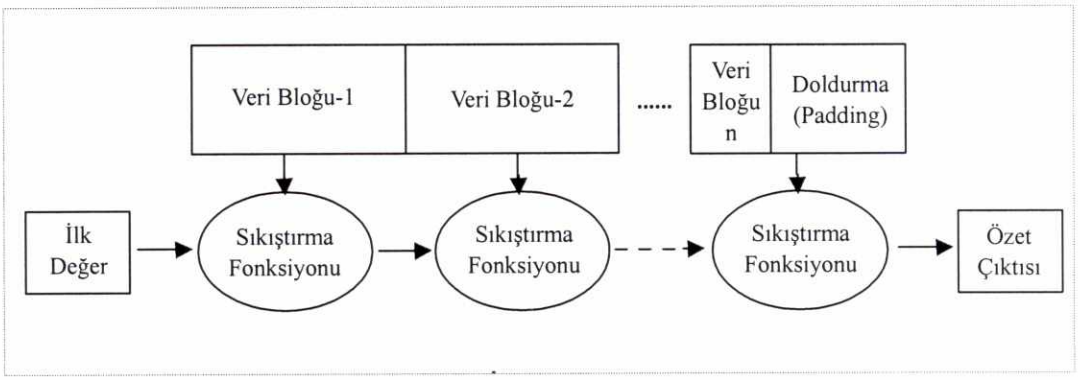
Özetleme algoritmalarına yapılan saldırılardan en yaygın olanı doğum günü (Birthday Attack) saldırılarıdır. Doğum günü saldırıları, doğum günü paradoksunun[1] temelinde yer alan matematiksel yaklaşım kullanılarak gerçekleştirilmektedir. Bu matematiksel yaklaşımda; *h* bir özetleme fonksiyonu ise ve olasılıkları aynı olan *n* adet farklı çıktı üretiyorsa ve *n* yeteri kadar büyük bir sayı ise bu fonksiyon yaklaşık $1{,}2\sqrt{n}$ farklı değişken için

[1] Doğumgünü paradoksu, 23 kişiden oluşan bir toplulukta en az iki kişinin aynı doğumgününe sahip olma olasılığının %50'den biraz fazla olduğunu ifade eder. Bu olasılık 60 veya daha fazla kişiden oluşan bir topluluk için %99'dan fazladır. Paradoks olarak adlandırılması mantıksal bir çelişkiden değil genel kanının matematiksel yaklaşımın tersine olmasındandır. Birçok kişi bu olasılığın %50'den daha az olduğunu düşünmektedir.

çalıştırıldığında $h(x_1) = h(x_2)$ denklemini sağlayan x_1 ve x_2 gibi iki girdi değişkeni bulunması beklenir. [31]

Özetleme algoritmalarının tek yönlülük özelliğini tehdit eden primaj (preimage) saldırılarında ise elde edilen herhangi bir özet değerinden girdi verilerine ulaşılması hedeflenmektedir. [32]

Diğer bir saldırı çeşidi ise sözde çakışmalar (pseudo-collision) üzerinedir. Özetleme algoritmaları uzun girdilerin kısaltılmasında sıkıştırma algoritmaları kullanmaktadır. (Bkz. Şekil 3.1) Zincirleme saldırıları (chaining attacks) olarak da adlandırılan bu saldırılar, sıkıştırma algoritmalarının çıktıları arasında bir çakışma tespit edilmesini amaçlar ve bu sayede özetleme algoritması ile elde edilen sonuçlara ulaşmakta kullanılır. [5]



Şekil 3.1 Sıkıştırma Algoritması

3.2.2 MD4 ve MD5 Özetleme Algoritmaları

MD4 (Message Digest 4 – Mesaj Özeti 4), 1990 yılında Ron Rivest tarafından geliştirilmiş bir özetleme algoritmasıdır. [33], Ancak çeşitli güvenlik gerekçeleri ile fazla kullanılmamış ve kısa süre sonra MD5 özetleme algoritması ortaya çıkarılmıştır. MD5, genel itibarla MD4 ile aynı özelliklere sahiptir ancak dizayn aşamasında yapılan birkaç iyileştirme ile güvenliği sıkılaştırılmıştır.

MD4 ve MD5, 128 bit'lik çıktılar üretir. Büyük dosyaların elektronik olarak imzalanmadan önce sıkıştırılması amacıyla oluşturulmuştur. 32-bit'lik makinalarda hızlı çalışabilir şekilde tasarlanmış bu algoritmalar kolay bir şekilde kodlanabilmektedir. MD4'te iki çıktı arasında çakışma olması olasılığı 2^{20} işlemde bir iken MD5 için 2^{64} işlemde birdir. Ayrıca her iki algoritma için özet değeri üzerinden girdi verisine ulaşmak için 2^{128} işlem yapılması gerektiği öngörülmektedir. (Bkz. Çizelge 3.1) [34, 35]

Güvenilirlik açısından bakıldığında MD4 için çakışma olma olasılığı MD5'ten oldukça yüksektir. Bu bakımdan MD4 güvenilir kabul edilen algoritmalar arasında yer almamaktadır. MD5 algoritması için ise sıkıştırma fonksiyonu çıktılarında sözde çakışmalar olduğu görülmüştür. Bu yüzden her iki algoritma da günümüzde güvenilir kabul edilmemektedir. [1]

Paul van Oorschot ve Mike Wiener tarafından 1994 yılında yayınlanan makalede [36] MD5 algoritmasının 10.000.000$'lık bir yatırımla 24 günde kırılmasını sağlayacak bir yapı tasarlanmıştır. Günümüzde ise aynı tasarımın maliyeti yaklaşık olarak 200.000$ seviyelerine kadar inmiştir. Daha farklı bir ifadeyle, Athlon XP 1700 işlemciye ve 64 Gigabyte'lık sabit diske sahip bir bilgisayar ile doğum günü saldırısı kullanılarak 2 yıl içerisinde çakışma(lar) bulunabileceği öngörülmektedir. [37]

Özetleme Algoritması	**Giriş metni ve Özet Değeri**
	"Telekomünikasyon Kurumu"
MD4	DB6EACBDE8DE3F80787399DBB18CDEB6
MD5	F684AF903A3511757566D75994F4EE3D

Çizelge 3.1 MD4 ve MD5 Özet Çıktısı

3.2.3 SHA Özetleme Algoritması

SHA, ilk olarak 1993 yılında NIST (National Institude of Standards and Technology – Ulusal Standart ve Teknoloji Enstitüsü) tarafından yayınlanan FIPS PUB 180 (Federal Information Processing Standards Publications – Federal Bilgi İşleme Standartları Yayınları) dokümanı ile standart (Secure Hash Standart - SHS) haline getirilmiştir. Daha sonra geliştirilerek, FIPS PUB 180-1 dokümanı ile; DSA (Digital Signature Algorithm – Sayısal İmza Algoritması) ile kullanılmak amacıyla, 2^{64} bitten kısa girdiler için 160 bitlik çıktılar üreten ve MD4'ü temel alan SHA-1 algoritması tanımlanmıştır. SHA-1 algoritmasında girdi olarak kullanılan veriler bitlere çevrilir ve 512 bitlik bloklar halinde sırayla işlenir. [38, 39]

2002 yılında yayınlanan FIPS PUB 180-2 standardı FIPS PUB 180-1'in yerini almış ve SHA-1'in yanı sıra SHA-256, SHA-384 ile SHA-512 algoritmalarını da tanımlamıştır. SHA-256, 2^{64} bitten kısa verileri girdi olarak kullanarak 256 bitlik özet değeri üretirken; SHA-384 ve SHA-512, 2^{128} bit uzunluğunda girdiler kabul etmekte ve sırasıyla 384 ve 512 bitlik çıktılar üretmektedir.

Yukarıda adı geçen algoritmaların uygulamaları iki adımda gerçekleştirilmektedir. Birinci adımda girdi uzunluğunun uygun hale getirilmesi için doldurma (padding) işlemi gerçekleştirilir, bloklar halinde bölünür ve başlangıç değerleri ayarlanır. İkinci adım ise özet değerinin hesaplanması için gerekli işlemleri içermektedir.

Bu dört algoritmanın birbirinden en önemli farkı, girdi değerinin güvenliği için sağlanan ve özet uzunluğu ile doğrudan ilişkili bitlerin sayısının değişiklik göstermesidir. Sözü edilen bu farklılık, değişik uygulamalarda ihtiyaç duyulabilecek farklı parametrelere uygunluk sağlanmasını kolaylaştıracaktır. Örneğin 120 bitlik bir güvenlik isteyen imzalama algoritması için SHA-1 uygun değildir. Bunun yerine SHA-128 algoritmasının kullanılması gerekecektir. [40]

Algoritma	Girdi (Mesaj) Uzunluğu (bit)	Blok Uzunluğu (bit)	Sözcük Uzunluğu (bit)	Özet Uzunluğu (bit)	Güvenlik (bit)
SHA-1	$< 2^{64}$	512	32	160	80
SHA-256	$< 2^{64}$	512	32	256	128
SHA-384	$< 2^{128}$	1024	64	384	192
SHA-512	$< 2^{128}$	1024	64	512	256

Çizelge 3.2 SHA Özellikleri

Çizelge 3.2'de yer alan güvenlik bitleri algoritmaların güvenlik seviyelerini göstermektedir. Bu değerlere göre SHA-1 ile üretilen özet değerlerinin aynı olması olasılığı $1/2^{80}$ iken SHA-256'da $1/2^{128}$, SHA-384'te $1/2^{192}$ ve SHA-512'de $1/2^{256}$ dır.

Güvenlikle ilgili diğer bir husus ise mesaj özeti uzunluklarının artmasıyla deneme-yanılma saldırılarına karşı direncin kuvvetlenmesidir. Güvenli olarak kabul edilmeyen MD5'te sıkıştırma fonksiyonu için kullanılan 16 sözcük uzunluğunda bloklar yerine 80 sözcük uzunluğunda bloklar (SHA-1) kullanılması da güvenliğin artmasını sağlamıştır. (Bkz. Çizelge 3.3) [1]

Özetleme Algoritması	Giriş metni ve Özet Değeri
	"Telekomünikasyon Kurumu"
SHA-1	53AC528CA6023645A84A2A8ABA397152C7EC4314
SHA-256	33819B733BA6924CB469172920AD0702B0AB7AB23773D A958C26B5175A9B59D6
SHA-384	2416E7B135A29BD5AD11A009E73987867521CD2DBB40 C28C5EC5C61705A9D4A3095BB67F316B5D3BC9B3F4C B46B74439
SHA-512	D2596430BBFDCDF388AF7DAC1C528A58E553C6D9BE6 118FFD6844D12C152D1D6B664864100644E2434FBE017 BFB70EC0B2118D3EF834BE938E9A27005B4044FB

Çizelge 3.3 SHA-1, SHA-256, SHA-384, SHA-512 Özet Çıktıları

3.2.4 RIPEMD Özetleme Algoritması

RIPEMD (RACE[1] Integrity Primitives Evaluation Message Digest), bir Avrupa Birliği projesi olan RIPE bünyesinde geliştirilmiş ve MD4 temelli 128 bitlik çıktılar üreten bir özetleme algoritmasıdır. Bu algoritmanın da diğer 128 bitlik çıktılar üreten algoritmalar gibi deneme-yanılma saldırılarına karşı dayanıksız olduğu ispat edilmiştir. [36]

RIPEMD-160, RIPEMD'nin 21 sözcüklük girdiler kullanarak 160 bitlik çıktılar üreten geliştirilmiş bir versiyonudur. (Bkz. Çizelge 3.4) Ortaya çıkarılması aşamasında; RIPEMD, MD4 ve MD5 çatıları göz önünde bulundurulmuştur. RIPEMD'de hesaplama için kullanılan 4 çevrim yerine 5 çevrim barındırmaktadır. Güvenlik bakımından SHA-1 ile aynı özellikleri taşısa da SHA-1'den daha yavaş çalışan bir algoritmadır. [41]

RIPEMD'nin 256 ve 320 bitlik versiyonları ise sırasıyla 128 ve 160 bitlik versiyonların uzantılarıdır ve yalnızca daha uzun girdi değerleri gerektiren fonksiyonlarla kullanılmak amacıyla geliştirilmiştir. Güvenlik ile ilgili hususlar açısından uzantısı oldukları algoritmalarla aralarında fark bulunmamaktadır.

Özetleme Algoritması	Giriş metni ve Özet Değeri
	"Telekomünikasyon Kurumu"
RIPEMD-160	691680570CA7C057C2E9D933A1312E29FB27BFDE

Çizelge 3.4 RIPEMD-160 Özet Değeri

3.3 İmzalama Algoritmaları ve Güvenilirlikleri

İmzalama algoritmaları, girdi verilerini ve imza atacak kişinin özel anahtarını kullanarak asimetrik şifreleme yapan algoritmalardır. Esas olarak asimetrik

[1] Research Programme in Advanced Communications for Europe – Avrupa için Gelişmiş İletişim Araştırma Programı

şifreleme için geliştirilmiş bu algoritmalar, tam eşlemeli olduklarından dolayı şifreleme ve şifre çözme işlemlerinin rolleri karşılıklı olarak değiştirilerek sayısal imzalama için de kullanılmaktadır.

3.3.1 İmzalama Algoritmalarına Yapılan Saldırılar

İmzalama algoritmalarına yapılan saldırılar; orijinal şifresiz verilerin ve şifreli verilerin kullanılmasıyla gerçekleştirilir. Kimi saldırı türlerinde, kullanılan imzalama algoritmasının bilinmesi de gerekmektedir. Algoritmaların güvenilirlikleri bu saldırılara karşı gösterdikleri dirençlere göre belirlenmektedir. Bunun yanı sıra anahtar çiftlerinin üretilmesi aşamasında kullanılan parametreler ve anahtar uzunlukları da güvenlikle ilgili önemli hususlardır.

En temel kriptografik saldırılar, elde edilen birçok şifreli verinin kullanılmasıyla gerçekleştirilen yalnızca şifreli metin (ciphertext-only) saldırılarıdır. Saldırıyı gerçekleştiren kişinin, gizli dinleme (eavesdropping) yaparak elde edilen şifreli verilere ilişkin bilgisi çok azdır. Ayrıca kullanılan şifreleme algoritmasının da bilinmesi gereklidir. Bu yüzden başarıya ulaşma ihtimali oldukça düşüktür. [42]

Bilinen şifresiz metin (known plaintext) saldırılarında hem orijinal şifresiz verilerin hem de bu verilere karşılık gelen şifreli verilerin bilinmesi gerekmektedir. Elde edilen şifreli ve şifresiz veriler karşılaştırılarak şifreleme anahtarına veya şifreli metinlere ulaşılmaya çalışılır. [43]

Seçilmiş şifresiz metin (chosen plaintext) saldırılarında, saldırganın şifrelenecek verileri seçme şansının olduğu kabul edilmektedir. Bu varsayım ütopik görünse de, modern kriptografinin yazılım ve donanımla gerçeklenmesi ve çeşitli uygulamalar tarafından kullanılmasıyla birçok durumda farklı bir şekilde hayata geçirilebilir. Seçilmiş şifresiz metin

saldırıları, toplu (batch) ve uyarlamalı (adaptive) olarak ikiye ayrılmaktadır. Toplu seçilmiş şifresiz metin saldırılarında tüm orijinal veriler şifrelenmeden önce belirlenir. Uyarlamalı seçilmiş şifresiz metin saldırılarında ise etkileşimli sorgularla önceki şifrelemede elde edilen bulgular çerçevesinde şifrelenecek metin seçilir. [44]

Özellikle asimetrik şifreleme algoritmaları üzerinde etkili olan diğer bir saldırı çeşidi ise seçilmiş şifreli metin (chosen ciphertext) saldırılarıdır. Şifreli metinlerin anahtar sahibi tarafından çözülmesi ve çözülen metinlerin saldırgan tarafından elde edilmesi gerekmekte olup, uyarlamalı olarak da gerçekleştirilebilmektedir. [45]

Yukarıda söz edilen saldırıların başarılı olması durumunda ortaya çıkabilecek sonuçlar ise şu şekilde sıralanabilir:

- Tam Kırılma (Total Break): İmza sahibinin özel anahtarının elde edilmesi,
- Evrensel Sahte İmza (Universal Forgery): Tüm mesajları imzalayabilecek etkin bir algoritma oluşturulması,
- Var olan Sahte İmza (Existential Forgery): Yeni bir mesaj – imza çifti oluşturulması[1].

3.3.2 RSA İmzalama Algoritması

Açık anahtar sistemleri fikri ortaya atıldıktan sonra, 1978 yılında R. Rivest, A. Shamir ve L. Adleman [46] tarafından tasarlanmış olan bu algoritma, asimetrik şifrelemenin ve dolayısıyla elektronik imzanın temellerini oluşturan uygulamalardan birisidir. RSA, temel olarak büyük sayıların çarpanlara ayrılması problemi üzerine yapılandırılmıştır.

---

[1] Birçok durumda elde edilen mesaj anlamlı olmadığından ötürü bu saldırılar başarıya ulaşamamaktadır. Ancak bu saldırılar karşısında dirençli olmayan algoritmalarda, imza sahibinin kimliğine tam olarak güvenilemez.

RSA kullanılarak anahtar çifti üretme, imzalama ve imza doğrulama aşamaları ve örnekleri aşağıda verilmiştir. [1, 47]

Anahtar çifti üretme:

1) $Z_n = \{0, 1, 2, 3, \ldots, n - 1\}$ olmak üzere, asal ve birbirinden farklı p ve q sayıları seçilir ve $n = p \cdot q$ hesaplanır,
2) $\Phi = (p - 1) \cdot (q - 1)$ değeri hesaplanır,
3) $1 < e < \Phi$ ve $OBEB^1(\Phi, e) = 1$ olacak şekilde bir e tamsayısı seçilir,
4) $e \cdot d \equiv 1 \pmod{\Phi}$ sağlayacak d değeri hesaplanır.
5) Özel anahtar : (n, d) ve açık anahtar : (n, e)'dir.

İmzalama:

1) M mesaj uzayı ve $m \in M$ olmak üzere bir m mesajı seçilir,
2) $t \in [0, n - 1]$ ve tamsayı olmak üzere $t = R(m)$ hesaplanır,
3) $s \equiv t^d \bmod n$ değeri hesaplanır,
4) s, m mesajının imzalanmış halidir.

İmza doğrulama:

1) İmzalayan kişinin açık anahtarı (n, e) öğrenilir,
2) $t \equiv s^e \bmod n$ hesaplanır,
3) $t \in M_R$ olduğu doğrulanır,
4) $m = R^{-1}(t)$ işleminden m'ye ulaşılır.

RSA imzalama ve imza doğrulama örneği:

Aşağıda yer alan örnek, küçük asal sayılar kullanılarak gerçekleştirilmiştir.

$p = 5$ ve $q = 11$ için $n = p \cdot q = 55$

$\Phi = (p - 1) \cdot (q - 1) = 4 \cdot 10 = 40$

$1 < e < \Phi$ ve $OBEB(\Phi, e) = 1$ olacak şekilde $e = 7$

$e \cdot d \equiv 1 \pmod{\Phi}$ olacak şekilde $7d \equiv 1 \pmod{40} \Rightarrow d = 23$

---

[1] OBEB: Ortak Bölenlerin En Büyüğü

Bu durumda açık anahtar *(55, 7)*, gizli anahtar ise *(55, 23)*
İmzalama: $t = 2$ *için* $s \equiv t^d \bmod n \Rightarrow 2^{23} \bmod 55 \equiv 8$ olur
İmza Doğrulama: $t \equiv s^e \bmod n \Rightarrow 8^7 \bmod 55 \equiv 2$ olarak bulunur.

RSA algoritması üzerine yapılan saldırılardan en önemlisi, elde edilen açık anahtar kullanılarak gizli anahtara ulaşılmaya çalışılmasıdır. Saldırgan, *n* katsayısının çarpanları olan *p* ve *q* değerlerini hesaplamaya çalışır. Eğer bu değerler ve *e* değeri bulunursa özel anahtara ulaşılabilir. Buradaki en zor kısım *n* sayısını çarpanlarına ayırma işlemidir. Ancak *n* değerinin yeterince büyük olmaması veya *p*, *q* çiftinin iyi seçilmemesi durumlarında RSA'nın güvenli olduğu söylenemez. 256 bitlik bir *n* değeri, kişisel bilgisayar kullanılarak birkaç saat içerisinde çarpanlarına ayrılabilir. RSA tarafından gerçekleştirilen RSA Çarpanlara Ayırma Mücadelesi (RSA Factoring Challenge) kapsamında 576 bitlik (155 basamaklı) n sayısı 2003 yılında çarpanlara ayrılmıştır. Farklı uzunluktaki sayıların, bir yıl içerisinde çarpanlarına ayrılabilmesi için gerekli maliyet Çizelge 3.5'te verilmiştir. [48]

Sayı Uzunluğu (Bit)	Bilgisayar[1] Sayısı	Fiziksel Hafıza
430	1	Önemsiz
760	215 000	4 GB
1020	342 000 000	170 GB
1620	$1{,}6 \times 10^{15}$	120 TB

Çizelge 3.5 Çarpanlara Ayırma Maliyeti (1 Yılda)

RSA kullanılarak şifrelenmiş veriler üzerine gerçekleştirilen ilk seçilmiş şifreli metin saldırısı, 1998 yılında Daniel Bleichenbacher [49] tarafından ortaya konulmuştur. Bu saldırı, PKCS[2] #1 v1'de (Public-Key Cryptography Standard – Açık Anahtar Şifreleme Standardı) tanımlanan doldurma (padding)

[1] Pentium 500 MHz işlemciye sahip
[2] RSA Laboratuvarları ile birlikte Apple, Microsoft, DEC, Lotus, Sun ve MIT tarafından geliştirilen standartlardır.

işleminin boşluklarından faydalanılarak, RSA uygulamalarından birisi olan Güvenli Soket Katmanı (Secure Socket Layer) protokolü üzerinde gerçekleştirilmiş ve oturumlarda kullanılan anahtarlar ele geçirilmiştir. Bu olay sonucunda, OAEP (Optimal Asymmetric Encryption Padding – Optimal Asimetrik Şifreleme Doldurması) gibi güvenli doldurma şemaları kullanılması tavsiye edilmiş ve RSA Laboratuarları tarafından PKCS #1'in yeni sürümleri yayımlanmıştır.

Günümüzde kısa süreli kullanılacak RSA imzalama anahtarları için *n* sayısının en az 1024 bit seçilmesi gerekmektedir. Daha uzun süreli uygulamalar için ise 2048 bitlik bir n sayısı seçilmesi doğru olacaktır.

3.3.3 ElGamal İmzalama Algoritması

1985 yılında Taher ElGamal tarafından kesikli logaritma problemini çözmedeki zorluk üzerine, Diffie-Hellman anahtar dağıtım planı (Bkz. Bölüm 3.3.2.1) ile birlikte geliştirilmiş olan imzalama ve asimetrik şifreleme algoritmasıdır. Günümüzde oldukça yaygınlaşmış olan PGP uygulamasında da ElGamal temelli şifreleme kullanılmaktadır. Deterministik olmadığı için bir girdi verisi için birden fazla imza üretilebilir. [50]

ElGamal ile anahtar üretme, imzalama ve imza doğrulama aşamaları ve örnekleri aşağıda yer almaktadır. [50, 1]

Anahtar oluşturma:

1) Yeterince büyük bir *p* asal sayısı seçilir,
2) $\alpha < p$ olmak üzere rastgele bir α tamsayısı seçilir,
3) *x*, rastgele tamsayısı seçilir,
4) $Y = \alpha^x \bmod p$ hesaplanır,
5) Açık anahtar: (α , *p*, *Y*), özel anahtar (*x*)'dir.

İmzalama:

1) $0 \leq m \leq p - 1$ olmak üzere m bir mesaj ise
2) $1 \leq k \leq p - 2$ ve $OBEB(k, p - 1) = 1$ olacak şekilde k sayısı seçilir,
3) $r = \alpha^k \bmod p$ hesaplanır,
4) $s = k^{-1}(m - x.r) \bmod (p-1)$ hesaplanır,
5) m mesajı için imza (r, s) çiftidir.

Doğrulama:

Gönderenin açık anahtarı (α, p, Y) elde edilir,

$1 \leq r \leq p - 1$ olduğu doğrulanır,

$\alpha^m \bmod p = Y^r r^s \bmod p$ ise imza doğrulanmış olur.

ElGamal imzalama ve doğrulama örneği:

Anahtar çifti oluşturma:

$p = 19$ ve $\alpha = 5$ ise

Özel anahtar: x = 4 seçilirse

$Y = \alpha^x \bmod p = 5^4 \bmod 19 = 17$ olur,

Açık anahtar (5, 19, 17)'dir

İmzalama:

m mesaj olmak üzere $m = 12$ alınırsa,

$k = 7$ olarak seçilirse,

$r = 5^7 \bmod 19 = 16$ bulunur,

$s = 4\ (12 - 64) \bmod 18 = 8 \bmod 18 = 8,$

m mesajı için imza (16, 8)'dir.

İmza Doğrulama:

$1 \leq r \leq p - 1 \Rightarrow 1 \leq 16 \leq 18$ doğrulanır,

$\alpha^m \bmod p = 5^{12} \bmod 19 = 11,$

$Y^r r^s \bmod p = 17^{16}\ 16^8 \bmod 19 = 11,$

11 = *11* olduğu için imza doğrudur.

ElGamal algoritması; imzalama ve şifreleme için farklı yapılar sunmaktadır. İmzalama işlemi yalnızca bir üs alma işlemi içerdiği ve bazı hesaplamalar çevrim dışı yapıldığı için oldukça hızlı çalışmaktadır. Ancak doğrulama işlemi 1,875 üs alma işlemi içerdiğinden yavaştır.

Güvenlik karakteristiği olarak Diffie-Hellman anahtar değişimi ile aynı özellikleri taşımaktadır. Olasılıklı bir algoritma olduğu için parametrelerin uygun bir şekilde ve rastgele seçilmesi çok önemlidir. İmzalanmış verilerden anahtara ulaşılma olasılığı *1/p* olduğundan, *p* değerinin büyük seçilmesi güvenliği artırmaktadır. Bunun yanı sıra, imzalamada kullanılan *k* değerinin birden fazla mesaj için aynı seçilmesi durumunda gizli anahtara ulaşmak oldukça kolay olmaktadır. [50]

ElGamal imzalama algoritmasında kullanılan *p* parametresi, RSA'da kullanılan *n* parametresi ile aynı uzunlukta seçildiğinde benzer güvenlik seviyesi sunmaktadır. Ayrıca, güvenli bir elektronik imza için *p* değerinin 1024 bit olması önerilmektedir.

3.3.3.1 Diffie-Hellman Anahtar Değişimi

1976 yılında Whitfield Diffie ve Martin Hellman tarafından yayınlanan makale ile açık anahtarlı altyapıların temeli atılmıştır. Bu makalede, iki kullanıcı arasında güvenli olmayan bir haberleşmenin özel anahtarlar paylaşılmadan nasıl gerçekleşeceği anlatılmaktadır. Diffie-Helman tarafından ortaya konulan bu model, kesikli logaritmaların hesaplanmasındaki zorluklar üzerine kurulmuştur. Anahtar değişim modeli aşağıdaki şekilde çalışmaktadır [4]

1) Bir *p* asal sayısı ve *p*'den küçük olmak üzere rastgele bir α sayısı seçilir. Bu iki sayı açık anahtarı oluşturmaktadır.

2) A kullanıcısı x_A, B kullanıcısı ise x_B şeklinde rastgele bir tamsayı seçer. x_A ve x_B kullanıcıların gizli anahtarıdır.

3) A kullanıcısı $Y_A = \alpha^{x_A} \ mod\ p$ değerini hesaplar ve B'ye gönderir.

4) B kullanıcısı $Y_B = \alpha^{x_B} \ mod\ p$ değerini hesaplar ve A'ya gönderir.

5) Kullanılacak gizli anahtar K_{AB} ise

   a) A kullanıcısı: $K_{AB} = Y_B^{x_A} \ mod\ p = (\alpha^{x_B})^{x_A} \ mod\ p$

   b) B kullanıcısı: $K_{AB} = Y_A^{x_B} \ mod\ p = (\alpha^{x_A})^{x_B} \ mod\ p$

   olarak belirlenir.

3.3.4 DSA İmzalama Algoritması

DSA, 1991 yılında NIST tarafından Elektronik İmza Standardı (DSS – Digital Signature Standard) [51] olarak federal uygulamalarda kullanılmak üzere oluşturulmuştur.

DSA, ElGamal algoritmasının farklı bir versiyonu olup kesikli logaritma problemini temel almaktadır. Diğer algoritmaların aksine, yalnızca elektronik imzalama yapmak için kullanılır. İmzalama işleminde, özetleme algoritması olarak SHA-1 kullanılması gerekmektedir.

DSA ilk versiyonlarında anahtar uzunluğu en fazla 512 bit uzunluğunda olacak şekilde tasarlanmıştır. Ancak 2001 yılında yapılan değişiklikle q değerinin 2^{1023} ile 2^{1024} arasında yani 1024 bit uzunluğunda olmasına karar verilmiştir.

DSA kullanılarak anahtar çifti üretme, imzalama ve imza doğrulama aşamaları ve örnekleri aşağıda verilmiştir.[51, 1]

Anahtar çifti üretme:

1) $2^{1023} < p < 2^{1024}$ olacak şekilde p asal sayısı seçilir
2) $(p - 1)$'in asal böleni ve $2^{159} < q < 2^{160}$ olmak üzere q asal sayısı seçilir
3) $1 < h < p - 1$ ve $h^{(p-1)/q} \bmod p > 1$ olmak üzere h seçilir,
4) $g = h^{(p-1)/q} \bmod p$ hesaplanır.
5) $0 < x < q$ olmak üzere rastgele bir x tamsayısı seçilir,
6) $y = g^x \bmod p$ hesaplanır,
7) açık anahtar (p, q, g, y), özel anahtar (x)'dir.

İmzalama:

1) M mesaj uzayı ve $m \in M$ olmak üzere bir m mesajı seçilir,
2) $m' = SHA\text{-}1\ (m)$ hesaplanır,
3) $r = (g^k \bmod p) \bmod q$ hesaplanır,
4) $0 < k^{-1} < q$ olmak üzere k tamsayısı seçilir.
5) $s = (k^{-1}(m' + x \cdot r)) \bmod q$ hesaplanır,
6) (r, s), m mesajının imzalanmış halidir.

İmza Doğrulama:

1) İmzalayan kişinin açık anahtarı (p, q, g, y) öğrenilir,
2) $0 < r < q$ ve $0 < s < q$ olduğu doğrulanır,
3) $w = s^{-1} \bmod q$ hesaplanır,
4) $u1 = (w \cdot m') \bmod q$ ve $u2 = (r \cdot w) \bmod q$ hesaplanır,
5) $v = ((g^{u1} y^{u2}) \bmod p) \bmod q$ hesaplanır,
6) $v = r$ ise imza doğrulanmış olur.

DSA imzalama ve imza doğrulama örneği:

Anahtar çifti oluşturma:

1) $p = 23$ için $(p-1)/q$ sonucunda asal sayı olacak şekilde $q = 11$
2) $1 < h < 22$ ve $h^2 \bmod 23 > 1$ olacak şekilde $h = 16$ seçilir.
3) $g = 16^2 \bmod 23 = 3$
4) $0 < x\ 23$ olmak üzere rastgele olarak $x = 7$

5) $y = 3^7 \bmod 23 = 2$
6) *Açık anahtar (23, 11, 3, 2), özel anahtar (7)*

İmzalama:

1) $0 < k < 11$ olmak üzere rastgele $k = 5$
2) $m' = SHA\text{-}1(m) = 10$ kabul edersek
3) $r = (3^5 \bmod 23) \bmod 11 = 2$
4) $s = (5^{-1} (10 + 7 . 2)) \bmod 11 = 7$
5) m mesajı için imza :(2, 7)'dir.

İmza Doğrulama:

1) $w = 7^{-1} \bmod 11 = 8$
2) $u1 = (8 . 10) \bmod 11 = 3$
3) $u2 = (2 . 8) \bmod 11 = 5$
4) $v = ((3^3 . 2^5) \bmod 23) \bmod 11 = 2$
5) $v = r = 2$ olduğundan imza doğrulanmış olur.

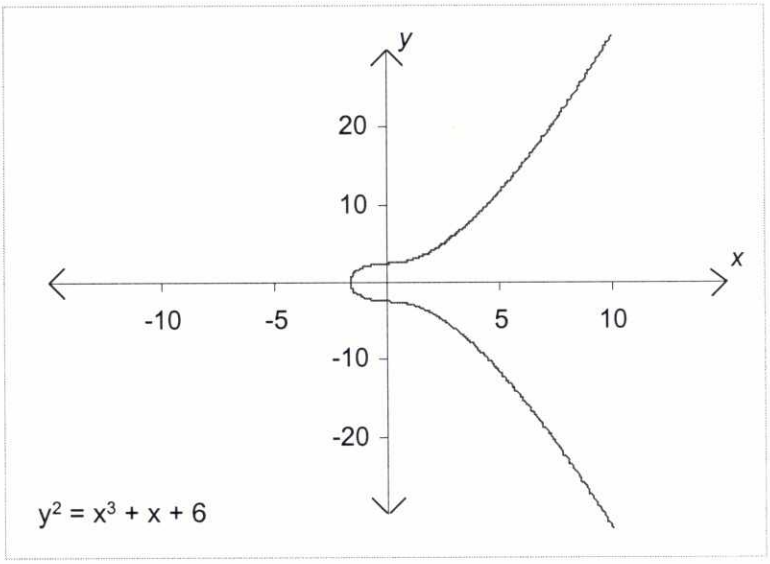
İmzalamada hesaplanan s ve r değerinin 0'dan farklı olması gerekmektedir. Tersi bir durumda s^{-1} hesaplanamayacağından dolayı imza doğrulanamaz. Bu durumun oluşması ihtimali $(½)^{160}$ gibi oldukça küçük bir değer olsa da s ve r'nin sıfırdan farklı olup olmadığı kontrol edilmelidir.

DSA'nın, imza oluşturma performansı oldukça iyidir. Bazı hesaplamaların imzalama öncesinde yapılması dolayısıyla RSA ile karşılaştırıldığında avantajlı durumdadır. Ancak aynı durum imza doğrulama için geçerli değildir. RSA'da, imza doğrulama işlemleri daha çabuk bir şekilde gerçekleştirilebilmektedir. Verilerin bir kez imzalanıp birçok kez doğrulandığı göz önünde bulundurulursa RSA'nın bir adım önde olduğu düşünülebilir. Ancak bu durum ihtiyaçlar ve kullanılacak uygulamalar doğrultusunda değişebilir.

3.3.5 Eliptik Eğri İmzalama Algoritmaları

Eliptik eğriler, 150 yıldır üzerinde çalışılan bir konudur ve yapılan bu çalışmalar sonucunda birçok teori ortaya çıkmıştır. Eliptik eğrilerin kriptografik sistemlere uygulanması, 1985 yılında Neal Koblitz [52] ve Victor Miller [53] tarafından gerçekleştirilmiştir.

Eliptik eğriler, yaygın olarak kullanılan (RSA, DSA gibi) açık anahtar sistemlerinin benzeridir. Ancak bu sistemler için aritmetik işlem grupları kullanılırken, eliptik eğri algoritmalarında yapılan işlemler geometrik olarak tanımlanmıştır. Eliptik eğriler; RSA benzeri olan eliptik eğriler ve kesikli logaritma problemine dayanan eliptik eğriler olarak temelde ikiye ayrılır. Fakat, RSA sistemlerinin güvenliği tamsayıların çarpanlara ayrılması problemine dayandırıldığı için eliptik eğrilerin RSA üzerine uygulanması pratikte güvenliği artırmamaktadır. Kesikli logaritma problemlerinde ise durum tamamen farklıdır. Eliptik eğri sistemlerinin kesikli logaritma kullanılmasıyla farklı bir problem ortaya konulmaktadır ve bu probleme eliptik eğri kesikli matematik problemi denilmektedir. (Bkz. Şekil 3.2) [5]



Şekil 3.2 Eliptik Eğri

Eliptik eğri algoritmalarının en önemli özelliği, RSA ve DSA'nın sağladığı güvenliği daha kısa parametrelerle sağlamasıdır. (Bkz. Çizelge 3.6) Parametreler küçüldükçe yapılan işlemlerin süresi de azalmaktadır. Böylece, imzalama ve imza doğrulama daha hızlı bir şekilde gerçekleştirilmektedir. [54]

Eliptik Eğri Anahtar Uzunluğu (bit)	RSA/DSA Anahtar Uzunluğu (bit)
112	512
160	1024
224	2048
256	3072
384	7680
512	15360

Çizelge 3.6 Anahtar Uzunluğu Karşılaştırması

Eliptik eğri imzalama algoritmaları, kullanıldıkları varyasyonun (RSA, DSA, ElGamal gibi) güvenlik özelliklerini taşımaktadır. Kullanılan anahtar uzunluğu kısa olduğu için en elverişli saldırı yöntemi deneme-yanılma saldırılarıdır. Kullanılan parametrelerin iyi bir şekilde seçilmesi ile yapılabilecek diğer saldırılara karşı korunma sağlanmaktadır.

3.3.5.1 Eliptik Eğri DSA

Eliptik eğri DSA (ECDSA – Elliptic Curve DSA), DSA'nın eliptik eğri kullanılarak meydana getirilmiş bir benzeridir. 1992 yılında hazırlanmış ve 1999 yılında ANSI (American National Standards Institude – Amerika Ulusal Standartlar Enstitüsü) [55] , daha sonra ise IEEE (Institude of Electrical and Electronics Engineers – Elektrik ve Elektronik Mühendisleri Enstitüsü) [56] ve

ISO (International Organisation for Standardisation – Uluslararası Standardizasyon Teşkilatı) [57] tarafından standart olarak kabul edilmiştir.

ECDSA'da kullanılan eliptik eğri algoritmaları ya asal tek sayılar (Z_p) ya da sonlu alanlar ($GF(2^m)$) üzerine uygulanır. Girdi olarak kullanılan veriler, SHA-1 ile özetlendikten sonra 160 bit olarak işlenir. ECDSA'ya ilişkin parametreler ve açıklamaları aşağıda yer almaktadır. [55, 6]

1) q; p veya 2^m için alan uzunluğunu belirtir,
2) $a, b \in Z_p$ veya $a, b \in GF(2^m)$ olmak üzere a ve b sayıları aşağıdaki eliptik eğri eşitliklerini tanımlayacak şekilde seçilmiş parametreleri belirtir,

   Z_p ve $p > 3$ için : $y^2 = x^3 + ax + b$

   $GF(2^m)$ ve $p = 2^m$ için : $y^2 + xy = x^3 + ax^2 + b$
3) $G = (x_G, y_G)$ şeklinde E üzerinde bir G noktasını belirtir.

ECDSA ile anahtar üretme, imzalama ve imza doğrulama aşamaları aşağıda verilmiştir: [6, 55]

Anahtar üretme:

1) $1 \leq d \leq n-1$ olacak şekilde bir d sayısı seçilir,
2) $Q = (x_Q, y_Q) = dP$ olmak üzere Q noktası belirlenir,
3) Açık anahtar: (Q), özel anahtar (d)'dir.

İmzalama:

1) $1 \leq k \leq n-1$ olacak şekilde k sayısı seçilir,
2) $m' = SHA\text{-}1\ (m)$ hesaplanır,
3) $(x_1, y_1) = k.G$ şeklinde eliptik eğri üzerinde nokta hesaplanır,
4) x_1, tamsayı değerine çevrilerek x_1' hesaplanır,
5) $r = x_1' \bmod n$ hesaplanır. $r = 0$ ise birinci adıma dönülür,
6) $s = k^{-1} (m' + d.r) \bmod n$ hesaplanır. $s = 0$ ise birinci adıma dönülür,

7) m mesajı için imza (r, s) çiftidir.

İmza Doğrulama:

1) $1 \leq r \leq n-1$ ve $1 \leq s \leq n-1$ olduğu doğrulanır,
2) $m' = SHA\text{-}1\ (m)$ hesaplanır,
3) $c = s^{-1} \bmod n$ hesaplanır,
4) $u_1 = m'.c \bmod n$ ve $u_2 = r.c \bmod n$ hesaplanır,
5) $(x_1, y_1) = u_1G + u_2Q$ noktası bulunur,
6) x_1, tamsayı değerine çevrilerek x_1' hesaplanır,
7) $v = x_1' \bmod n$ değeri bulunur,
8) $v = r$ ise mesaj doğrulanmış olur.

ECDSA imzalama ve doğrulama örneği:

Eliptik eğri olarak Z_{11} üzerinde E: $y^2 = x^3 + x + 6$ kullanılıyor ise

Anahtar çifti oluşturma:

1) $d = 2$ ve $Q = (7, 9)$ seçilirse
2) Açık anahtar $(7, 9)$, gizli anahtar (2) olarak bulunur.

İmzalama:

1) $k = 5$ ve $G = (8, 3)$ seçilirse,
2) $k.Q = 5.(7, 9) = (10, 2)$ ve $r = x_1 = 20$ olarak bulunur,
3) $k = 5\ (mod\ 13) \Rightarrow k^{-1} = 8$ olur,
4) $m' = 8$ olarak alınırsa, $s = k^{-1}\ (m' + d.r) = 8(8 + 2.10)\ (mod\ 13) = 3$ olur,
5) m mesajı için imza $(10, 3)$'tür.

İmza Doğrulama:

1) $1 \leq 10 \leq 12$ ve $1 \leq 3 \leq 12$ doğrulanır,
2) $c = s^{-1} \bmod n = 3^{-1} \bmod 13 = 9$ olur,
3) $u_1 = m'.c \bmod n = 8.9\ (mod\ 13) = 7$ ve $u_2 = r.c \bmod n = 10.9\ (mod\ 13) = 12$ olarak bulunur,

4) $(x_1, y_1) = u_1G + u_2Q = 7(8, 3) + 12(7, 2) = (3, 5) + (2, 7) = (10, 9)$ olur,

5) $v = 10 = r$ olduğu için mesaj doğrulanır.

3.4 İmza Oluşturma Sistemleri ve Araçları

İmza oluşturma sistemleri; temel olarak iki farklı türde bileşenden oluşmaktadır. Bunlardan ilki, imza oluşturmada kullanılan program ve işletim sistemini içine alan yazılım bileşenleridir. İkincisi ise, programın ve işletim sisteminin üzerinde koşacakları donanım bileşenlerinden oluşmaktadır. Bu donanım bileşenleri, yalnızca imza oluşturma işlemleri için özel olarak üretilmişcihazlar olbileceği gibi kişisel bilgisayar veya avuçiçi bilgisayar gibi farklı işlevler için kullanılan bilgisayarlar da olabilmektedir.

İmza verisi ve imza oluşturma güvenliği, imza oluşturma sisteminin güvenliği ile doğru orantılıdır. Satın alınabilecek herhangi bir bilgisayar ile imza oluşturma sistemi kurulabilir. Ancak imzanın taklit edilememesi, imzalanacak verinin değiştirilememesi ve doğru bir şekilde gösterilmesi gibi güvenlik gereklerinin yerine getirilebilmesi açısından daha güvenilir sistemlerin kullanılması şarttır. [58]

Elektronik imza oluşturma araçları; anahtar çiftini oluşturan, saklayan ve imzalama işlemini gerçekleştiren yazılım veya donanım olarak tanımlanmaktadır. Bu araçlar işlem yapabilme yeteneğine sahiptir ve bunlara kimlik denetim verisi (PIN, biyometrik veriler gibi) ile erişilebilir. Bu araçların güvenli olarak nitelendirilebilmesi için belirli teknik kriterleri ve yasal gerekleri yerine getirmesi beklenir.

5070 sayılı Elektronik İmza Kanununun 6ncı maddesinde güvenli elektronik imza oluşturma araçlarında (GEİOA) bulunması gereken özellikler belirlenmiştir. Bu maddeye göre güvenli elektronik imza oluşturma araçları:

a) Ürettiği elektronik imza oluşturma verilerinin kendi aralarında bir eşi daha bulunmamasını,
b) Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin araç dışına hiçbir biçimde çıkarılamamasını ve gizliliğini,
c) Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin, üçüncü kişilerce elde edilememesini, kullanılamamasını ve elektronik imzanın sahteciliğe karşı korunmasını,
d) İmzalanacak verinin imza sahibi dışında değiştirilememesini ve bu verinin imza sahibi tarafından imzanın oluşturulmasından önce görülebilmesini

sağlamalıdır.

Yukarıda yer alan özelliklerin sağlanabilmesi için, CEN (Comité Européen de Normalisation – Avrupa Standardizasyon Komitesi) tarafından CWA (CEN Workshop Agreement – CEN Çalıştay Kararları) 14169 "Güvenli Elektronik İmza Oluşturma Araçları EAL4+" ve CWA 14170 "İmza Oluşturma Uygulamaları için Güvenlik Gereksinimleri" şeklinde iki farklı standart yayınlanmıştır. Bu standartların ilki Bölüm 4.3.4'de ikincisi ise Bölüm 4.3.5'de detaylı bir şekilde açıklanmaktadır.

Elektronik imza oluşturmada yerine getirilmesi gereken teknik kriterler standartlarla belirlenmiştir. Ancak imza oluşturma sistemlerinin temininde ve kullanımında azami dikkatin gösterilmesi gerekmektedir. Öncelikle, temin edilen araç ve cihazların standartlara uygunluğundan emin olunmalı ve bunlar üzerinde zararlı yazılımlar yüklenmesinin ve bu yazılımların çalıştırılmasının önüne geçmek için gerekli tedbirler alınmalıdır. İmza sahibi; aracının güvenliğini azami seviyede sağlamalı ve çalınmasını veya başka kişiler tarafından kullanılmasını engellemelidir.

3.5 İmza Doğrulama Sistemleri ve Araçları

İmza doğrulama sistemleri; imza doğrulama aracı, imzalanmış veriyi doğru bir biçimde gösteren yazılım ve bu yazılımın üzerinde çalışacağı donanım bileşenlerinden oluşmaktadır. Kullanılan cihazların ve uygulamaların imza doğrulama sistemleri üzerinde güvenlik açısından önemli etkileri bulunmaktadır. Bu yüzden kullanılacak sistemlerin bütünlüğü ve güvenliği önem arz etmektedir.

Elektronik imza doğrulama araçları, elektronik imzanın doğrulanması amacıyla imza doğrulama verisini kullanan yazılım veya donanım olarak tanımlanmaktadır. Bu araçların güvenliği aşağıdaki hususlara dayanmaktadır: [59]

- Aracın güvenli bir şekilde geliştirilmesi,
- Yüklemenin doğru yapılması,
- Aracın yetkisiz girişimleri önleyebilmesi veya bunları tespit edebilmesi.

5070 sayılı Elektronik İmza Kanununun 7. maddesinde güvenli elektronik imza doğrulama araçları (GEİDA):

a) İmzanın doğrulanması için kullanılan verileri, değiştirmeksizin doğrulama yapan kişiye gösteren,
b) İmza doğrulama işlemini güvenilir ve kesin bir biçimde çalıştıran ve doğrulama sonuçlarını değiştirmeksizin doğrulama yapan kişiye gösteren,
c) Gerektiğinde, imzalanmış verinin güvenilir bir biçimde gösterilmesini sağlayan,
d) İmzanın doğrulanması için kullanılan elektronik sertifikanın doğruluğunu ve geçerliliğini güvenilir bir biçimde tespit ederek sonuçlarını değiştirmeksizin doğrulama yapan kişiye gösteren,

e) İmza sahibinin kimliğini değiştirmeksizin doğrulama yapan kişiye gösteren ve
f) İmzanın doğrulanması ile ilgili şartlara etki edecek değişikliklerin tespit edilebilmesini sağlayan

araçlardır.

Kullanıcıların, tercih edecekleri imza doğrulama araçlarında yukarıda yer alan hususların temin edildiğinden emin olması gerekmektedir. Kullanılacak araçların güvenliği hem geliştiren tarafın hem de kullanıcının sorumluluğundadır. Bu yüzden aracı geliştiren tarafın güvenilir olması ve belirli standartları uygulaması tercih sebebi olmalıdır.

Güvenli elektronik imza doğrulama araçlarının sağlaması gereken özellikler CEN tarafından yayınlanan CWA 14171:2004 "Elektronik İmza Doğrulaması için Genel Hususlar" kapsamında tanımlanmaktadır. Bu standart detaylı bir şekilde Bölüm 4.3.5'de incelenmiştir.

3.6 ESHS Güvenliği

Elektronik sertifika hizmet sağlayıcılarının güvenli hizmet verebilmesi sertifika ve imza güvenliği açısından oldukça önemlidir. Genel olarak bakıldığında, bir ESHS'nin kurulduğu yerden kullandığı sistemlere, çalıştırdığı personelden organizasyon yapısına kadar her bir ayrıntının titizlikle gözden geçirilmesi gerekmektedir.

ESHS güvenliğinin ilk aşamasında, organizasyonun güvenlik ölçütlerinin belirlenerek; önemli varlıkların, potansiyel tehditlerin ve genel olarak tüm kaynakların korunması amacıyla güvenlik politikasının tanımlanması bulunmaktadır. Sertifika ilkeleri ve sertifika uygulama esasları ise bu aşamadan sonra oluşturulmalıdır. [60] Güvenlik politikası tanımlamada en

yaygın standartlardan birisi olan TS ISO/IEC 17799, dikkate alınacak hususları da içerecek şekilde Bölüm 4.1.1'de detaylı olarak açıklanmaktadır.

Sertifika ilkeleri ve sertifika uygulama esaslarında ESHS'nin işleyişinde güvenliği sağlamaya ilişkin tüm adımların, kullanılacak cihazların, politika ve prosedürlerin yer alması gerekmektedir. Sertifika uygulama esaslarının hazırlanmasında, sıklıkla kullanılan referans belge niteliğindeki RFC 3647 [17] kapsamında sıralanan:

- Yayınlama ve Saklama Sorumlulukları,
- Tanımlama ve Kimlik Denetimi,
- Sertifika Yaşam Döngüsü Operasyonel Gereksinimleri,
- Yönetimsel, Operasyonel ve Fiziki Kontroller,
- Teknik Güvenlik Kontrolleri

gibi hususların SUE içerisinde yer alması gerekmektedir.

ESHS'nin sunduğu hizmetlere ilişkin olarak kullandığı sistem, cihaz ve yazılımların mutlaka güvenilir olması gerekmektedir. Ayrıca bu bileşenler, gelişen teknoloji ve artan saldırı çeşitliliği karşısında sık sık kontrol edilmeli ve gerekli güncellemeler yapılmalıdır. Güvenilir sistemler için gereklilikler Bölüm 4.3.1'de CWA 14167-1 içerisinde yer almaktadır.

Güvenilir sistemlerin kullanılması, gerekli diğer önlemler alınmadığında tek başına yeterli olmayacaktır. Bunun yanında, yazılım ve donanımların gerekli olmayan özelliklerinin kapatılması veya iptal edilmesi iyi bir seçenek olarak karşımıza çıkmaktadır. Örneğin, kurulan bir güvenlik duvarının ihtiyaç duyulan portlar dışında erişime izin vermemesi gerekir. (Bkz Çizelge 3.7) [61]

	Port Numarası	Hizmet	Kullanım
Zorunlu	829	PKIX	ESHS/Kayıt Kurumu Haberleşmesi
	389	LDAP	LDAP Dizinlerinde Çevrimiçi Sorgulama
	80	HTTP	SİL'lerin genel olarak erişimi
	443	HTTPS	SSL üzerinden SİL erişimi
Tercihli	636	LDAP/S	SSL üzerinden LDAP
	143	IMAP	Elektronik postaların taşınması
	220	IMAP-3	Elektronik postaların taşınması
	585	IMAP/S	SSL üzerinden IMAP

Çizelge 3.7 Güvenlik Duvarı Portları

Bir ESHS'nin güvenilir olabilmesi için korunması gereken en önemli varlıklardan birisi özel anahtardır. Özel anahtarın çalınması, kaybolması veya amaç dışı kullanılmasını önlemek amacıyla her türlü tedbir alınmalı ve özel anahtar hususi olarak üretilen cihazlarda saklanmalıdır. Bu cihazlara ilişkin kriterler, Bölüm 4.3.2'de yer alan CWA 14167-2'de veya muadili bir standartta detaylandırılan koruma profiline uygun olmalıdır. Ayrıca cihazın erişim ve kullanımına ilişkin kurallar TS ISO/IEC 17799 ve ETSI TS 101 456 (Bkz Bölüm 4.2.1) kapsamında belirlenmelidir.

Ayrıca; anahtarın güvenliğinin kaybolması veya olağanüstü durumların ortaya çıkması sonrasında uygulanacak kurtarma planları yapılmalıdır. Anahtar için risk oluşturabilecek olayların tespit edilip raporlanması ve gerekli önlemlerin alınması gerekir. Sel, su baskını, yangın, deprem gibi afetlere karşı hazırlık planları oluşturulması ve fiziksel yerleşimin bu hususlar dikkate alınarak yapılması güvenlik için oldukça ehemmiyetlidir.

İstihdam edilecek personelin yeterli teknik bilgiye ve deneyime sahip olması da önemli hususlar arasında yer almaktadır. Personel istihdamında; iş

deneyimi, diploma ya da klerans belgeleri, eğitim, adli sicil kaydı, referanslar gibi birçok husus göz önünde bulundurulmalıdır.

ESHS, çalışanlarının ve varsa kayıt merkezleri ile alt yüklenicilerinin güvenilirliğinden emin olmalıdır. Bunların seçiminde yasal gereklilikler dikkate alınmalı, söz konusu kişiler için güvenlik soruşturması yaptırılmalı ve bu kişilerle gizlilik anlaşması yapılmalıdır.

4 ELEKTRONİK İMZA GÜVENLİK STANDARTLARI

4.1 Uluslararası Standartlar

Bu bölümde, elektronik imza güvenliğine ilişkin veya dolaylı olarak ilişkili ISO tarafından yayınlanmış standartlara yer verilmiştir. Burada ele alınan standartlar TSE (Türk Standardları Enstitüsü) tarafından Türkçe'ye çevrilerek ulusal standartlarımız arasına katılmıştır.

4.1.1 TS ISO/IEC 17799 Standardı

ISO/IEC 17799 "Bilgi Teknolojisi – Bilgi Güvenliği Yönetimi için Uygulama Prensipleri" ilk olarak 1993 yılında kural rehberi olarak geliştirilmiş, 1993 yılında İngiliz Standartları Enstitüsü (British Standards Institution – BSI) tarafından BS 7799 Bölüm 1 adı altında standartlaştırılmış ve 2000 yılında ISO tarafından uluslararası bir standart olarak kabul edilmiştir. Kasım 2002 tarihinde ise TS ISO/IEC 17799 adı altında TSE tarafından Türk standartları arasına katılmıştır. [62]

TS ISO/IEC 17799; üst seviye, geniş kapsamlı ve kavramsal bir uygulama kılavuzudur. Bu özellikler sayesinde, standardın farklı organizasyonlar ve güvenlik seviyeleri üzerinde uygulanabilmesi imkanı ortaya çıkmaktadır. TS ISO/IEC 17799, genel kanının aksine, teknik bir standart değildir ve herhangi bir ürün veya teknolojiden bağımsızdır. [63]

BSI tarafından geliştirilen BS 7799 Bölüm 2 ise gereksinimler üzerine kurulmuş bir denetim standartıdır. Bilgi güvenliği yönetim sisteminin kurulması, uygulanması, işletilmesi, izlenmesi, gözden geçirilmesi, korunması ve geliştirilmesi için gereken hususları ortaya koymaktadır. Bu kısmın uluslararası bir standart haline getirilmesine yönelik çalışmalar başlatılmış ancak henüz tamamlanmamıştır. Bu yüzden denetim ve belgelendirme yalnızca BSI tarafından yapılmaktadır. [64]

TS ISO/IEC 17799'da bilgi güvenliği kavramı 3 ana kısımda incelenmiştir. Bunlar;

- Gizlilik: Bilgiye sadece yetkili kişiler tarafından erişilebilmesinin sağlanması,
- Bütünlük: Bilginin ve bilgi işleme metotlarının doğruluk ve bütünlüğünün korunması,
- Erişilebilirlik: Yetkili kişilerin gerektiğinde bilgiye ve ilgili varlıklara ulaşabilmesinin sağlanması

olarak sıralanmaktadır.

TS ISO/IEC 17799, bilgi güvenliğinin sağlanmasına yönelik 10 güvenlik kontrolü, bu kontroller altında 36 kontrol nesnesi ve 127 alt kontrol içermektedir. Bu kontroller seçimlidir ve organizasyon yapısı ile güvenlik gereksinimleri paralelinde kullanılmaktadır. [65]

Ana kontroller aşağıdaki 10 başlıkta, diğer kontroller ise bu başlıklar altında verilmektedir. [21]

4.1.1.1 Güvenlik Politikası

Bilgi güvenliğinin sağlanmasında idarenin yönlendirilmesi ve desteğinin sağlanması gerekmektedir. Yönetim, tüm işletme içinde bilgi güvenliğine ilişkin açık bir politika ortaya koymalı, bunun için destek vermeli ve bağlılık göstermeli, bilgi güvenliği politikasını herkese bildirmeli ve sürekliliğini sağlamalıdır.

Bilgi Güvenliği Politikası Belgesi: Güvenlik politikalarının, prensiplerinin, standartlarının ve işletme için öneminin kısa bir açıklamasıdır.

Gözden Geçirme ve Değerlendirme: Politikanın, sürekliliğinin sağlanmasından ve tanımlanmış yöntemlere göre gözden geçirilmesinden sorumlu bir sahibi olmalıdır. Aşağıdaki hususlarla ilgili zamanlanmış, belirli aralıklarda gözden geçirmeler yapılmalıdır:

- Kaydedilmiş güvenlik arızalarının yapısı, sayısı ve etkisi aracılığıyla görüntülenen politikanın etkinliği,
- Denetimlerin iş verimliliği üzerindeki maliyeti ve etkisi,
- Teknolojik değişikliklerin etkisi.

4.1.1.2 Organizasyonel Güvenlik

İşletme içinde bilgi güvenliğinin yönetimini amaçlamaktadır. 3 ana kısımdan oluşmaktadır:

- Bilgi Güvenliği Altyapısı
- Üçüncü Taraf Erişiminin Güvenliği
- Dışarıdan Kaynak Sağlama

Bilgi güvenliği altyapısı: İşletme içindeki bilgi güvenliği ile ilgili yapılacak işlemleri başlatmak, kontrol etmek amacıyla kurulan altyapıdır.

Üçüncü Taraf Erişiminin Güvenliği: Üçüncü taraflarca erişilen işletmeye ait bilgi işleme araçlarının ve bilgi varlıklarının güvenliği sağlanmalıdır. Bunun için gerekli kontrollerin yapılması amaçlanmaktadır.

Dışarıdan Kaynak Sağlama: Bilgi işleme sorumluluğu başka bir işletmenin kaynaklarından sağlanması halinde bilgi güvenliğinin sürdürülmesi gerekmektedir. Bunun için dışarıdan kaynak sağlama sözleşmelerindeki güvenlik gerekleri ortaya konulmuştur.

4.1.1.3 Varlıkların Sınıflandırılması ve Denetimi

İşletmeye ait varlıklar için uygun korumanın sağlanması ve varlıkların sınıflandırılması gerekmektedir. Bu sınıflandırma ve denetim için aşağıdaki hususlar göz önüne alınmalıdır:

- Varlıklar için sorumluluk
- Bilgi sınıflandırması

Varlıklar için Sorumluluk: İşletmeye ait varlıklara uygun korumanın sağlanması için bilgi varlıklarıyla ilgili açıklama yapılmalı, her bir varlık için bir sorumlu belirlenmeli ve varlıkların envanteri çıkarılmalıdır. Bilgi sistemleriyle ilgili varlıklara örnekler aşağıda yer almaktadır:

- Bilgi Varlıkları: Veri tabanları ve veri dosyaları, sistem belgeleri, kullanıcı el kitapları, eğitim malzemeleri, işlemsel ve desteksel yöntemler, süreklilik planları, yedek anlaşmaları, arşivlenmiş bilgi,
- Yazılım Varlıkları: Uygulama yazılımları, sistem yazılımları, geliştirme araçları ve faydaları,
- Fiziksel Varlıklar: Bilgisayar bileşenleri (işlemciler, ekranlar, diz üstü bilgisayarlar, modemler), manyetik ortamlar (kayıt cihazları ve diskler), diğer teknik araçlar (güç kaynakları, havalandırma üniteleri), mobilya, yerleşim düzeni,
- Hizmetler: Bilgi işleme ve haberleşme hizmetleri, genel faydalar; örneğin ısınma, ışıklandırma, elektrik, havalandırma.

Bilgi Sınıflandırması: Bilgi kaynaklarının uygun koruma seviyesine sahip olduklarının garanti edilmesi için sınıflandırma kılavuzlarının oluşturulması, sınıflandırmaya uygun olarak bilgi etiketleme ve bilgi işleme için gerekli süreçlerin tanımlanması gerekmektedir.

4.1.1.4 Personel Güvenliği

Personel güvenliğinin sağlanması ile, personelden kaynaklanan hataların ve uygunsuzlukların önlenebilmesi ve risklerin azaltılması amaçlanmaktadır. Üç ana kontrol içermektedir:

- İş tanımlarındaki ve kaynaklardaki güvenlik
- Kullanıcı eğitimi
- Güvenlik arızalarına ve bozulmalarına cevap verilmesi

İş Tanımlarındaki ve Kaynaklardaki Güvenlik: İnsan hatalarını, hırsızlığı, sahtekarlığı ve araçların yanlış kullanılması risklerini azaltmayı amaçlayan kontrollerdir.

Kullanıcı Eğitimi: Kullanıcıların bilgi güvenliği tehditlerinden ve sorunlarından haberdar oldukları ve normal çalışma seyirleri içinde organizasyonla ilgili güvenlik politikasını desteklemek üzere donatıldıkları garanti edilmelidir. Personele, gerekli bilgi güvenliği eğitimi verilmeli ve bu eğitimler belirli aralıklarla tekrarlanmalıdır.

Güvenlik Arızalarına ve Bozulmalarına Cevap Verilmesi: Güvenlik arızalarından ve bozulmalarından meydana gelen hasarın en aza indirilmesi, bu gibi olayların gözlenmesi ve bunlardan gerekli derslerin çıkarılması amaçlanmaktadır.

4.1.1.5 Fiziki ve Çevresel Güvenlik

Fiziki ve çevresel güvenliği tehdit edecek risklerin en aza indirilmesini sağlamak amacıyla oluşturulmuş denetimdir. Alt başlıklar olarak aşağıda yer alan kontrolleri içermektedir:

- Güvenli bölgeler
- Teçhizat güvenliği
- Genel denetimler

Güvenli Bölgeler: İş alanına ve bilgilerine yetkisiz erişimin ve bunlar üzerinde meydana gelebilecek hasarlar ile müdahalelerin engellenmesi amaçlanmaktadır. Bunun için; fiziki giriş denetimleri yapılmalı ve bürolar, araçlar ve odalar güvenlik altına alınmalıdır. Personel güvenli alanlarda çalışmalı, binanın yan hizmet bileşenlerinin dağıtım ve yükleme alanları ayrılmalıdır.

Teçhizat Güvenliği: Varlıkların kayıplarını, varlıklara gelebilecek hasar veya tehlikelerin önlenmesini ve ticari faaliyetlerin kesintisiz devam ettirilmesini amaçlayan kontrollerdir.

Genel Denetimler: Bilginin ve bilgi işleme araçlarının hırsızlıklara karşı korunmasını ve bu araçların tehlikeye atılmasının önlenmesini amaçlamaktadır. Araçların; yetkisiz kişiler tarafından ifşa edilmesinden, değiştirilmesinden veya çalınmasından korunması ve denetimlerle kayıp ve hasarların en aza indirilmesi gerekmektedir.

4.1.1.6 İletişim ve İşletim Yönetimi

İletişim ve işletim yönetimi yapılarak ortaya çıkabilecek risklerin en aza indirilmesi hedeflenmektedir. Alt kontrolleri ise:

- İşletim prosedürleri ve sorumlulukları
- Sistem planlama ve kabul etme
- Kötü niyetli yazılımlara karşı koruma
- Ortam muhafazası
- Ağ yönetimi

- Bilgi ortamı yönetimi ve güvenlik
- Bilgi ve yazılım değiş tokuşu

olarak sıralanmaktadır.

İşletim Prosedürleri ve Sorumlulukları: Bilgi işlem tesislerinin doğru ve güvenle işletildiğinden emin olunmasını amaçlamaktadır.

Sistem Planlama ve Kabul Etme: Sistem arızalarının en alt seviyeye indirilmesi ile ileriye yönelik hazırlık ve planlamanın yapılması amaçlanmaktadır.

Kötü Niyetli Yazılımlara Karşı Koruma: Bilgi ve yazılım bütünlüğünün korunması amaçlanmaktadır. Bu kapsamda, kötü niyetli yazılımların girişini tespit edecek ve önleyecek tedbirlerin alınması ile gerekli kontrollerin yapılması hedeflenmektedir.

Ortam Muhafazası: Bilgi işlem ve iletişim hizmetlerinin kullanılabilirliğinin ve bütünlüğünün sürdürülmesi ile yedeklerin alınmasını kapsamaktadır.

Ağ Yönetimi: Ağ üzerinde yer alan bilgilerin emniyetinin sağlanması ve bunları destekleyen sistemlerin korunması amaçlanmaktadır. Bunun için, ağ kontrollerin yapılması gerekmektedir.

Bilgi Ortamı Yönetimi ve Güvenlik: İş faaliyetlerinin kesintiye uğratılmasının ve varlıklara zarar verilmesinin önlenmesi hedeflenmektedir. İlgili ortamlar kontrol altında tutulmalı ve fiziksel olarak korunmalıdır.

Bilgi ve Yazılım Değiş Tokuşu: Organizasyonlar arasında akan bilginin yanlış maksatlarla kullanılmasının, değiştirilmesinin ve kaybedilmesinin önlenmesi amaçlanmaktadır.

4.1.1.7 Erişim Denetimi

Bilgiye, bilgi işleme varlıklarına ve yazılımlara erişimin denetlenmesi ve bununla ilgili politikaların oluşturulmasını kapsamaktadır. Aşağıdaki kontrol başlıklarını bünyesinde barındırır:

- Erişimin denetimi için iş gerekleri
- Kullanıcı erişimi yönetimi
- Kullanıcı sorumlulukları
- Ağ erişim denetimi
- İşletim sistemi erişim denetimi
- Uygulama erişimi denetimi
- Sistem erişiminin gözlenmesi ve kullanımı
- Mobil bilgi işlem ve uzaktan çalışma

Erişimin Denetimi için İş Gerekleri: Bilgiye erişimin ve iş süreçlerinin iş ve güvenlik gerekleri kapsamında denetlenmesi amaçlanmaktadır.

Kullanıcı Erişimi Yönetimi: Bilgi sistemlerine yetkisiz girişlerin önlenmesi amacıyla erişim haklarının ayrılması ve kullanıcı yönetimini kapsamaktadır.

Kullanıcı Sorumlulukları: Yetkisiz kullanıcı erişimlerinin engellenmesi ve yetkili kullanıcılar arasında işbirliği yapılması hedeflenmektedir.

Ağ Erişim Denetimi: Ağ üzerinde oluşturulmuş hizmetlerin korunması ile dahili veya harici olarak kurulmuş ağlara erişimin denetlenmesini kapsamaktadır.

İşletim Sistemi Erişim Denetimi: İşletim sistemi düzeyinde yer alan güvenlik araçları ile bilgisayar kaynaklarına yetkisiz erişimin engellenmesi amaçlanmaktadır.

Uygulama Erişimi Denetimi: Uygulama sistemleri içerisinde yer alan bilgilere erişimin kısıtlanması hedeflenmektedir.

Sistem Erişiminin Gözlenmesi ve Kullanımı: Sistemlerin yetkisiz erişimlerden korunması amacıyla gözlenmesi ve bulguların kaydedilmesini amaçlamaktadır.

Mobil Bilgi İşlem ve Uzaktan Çalışma: Mobil bilgi işlem araçları kullanıldığında ve uzaktan erişimlerde bilgi güvenliğinin temin edilmesi amaçlanmaktadır.

4.1.1.8 Sistem Geliştirmesi ve İdamesi

Bilgi işlem sistemlerinde güvenliğin geliştirilmesi ve idame ettirilmesi amacı ile aşağıdaki kontrolleri içermektedir:

- Sistem güvenlik gerekleri
- Uygulama sistemlerinde güvenlik
- Kriptografik kontroller
- Sistem dosyalarının güvenliği
- Geliştirme ve destek süreçlerinde güvenlik

Sistem Güvenlik Gerekleri: Bilgi işlem sistemleri içerisinde güvenliğin sağlanmasının hedeflendiği, güvenlik gerekleri analizinin ve özelleştirilmesinin yapıldığı kontrollerdir.

Uygulama Sistemlerinde Güvenlik: Uygulama sistemlerinde kullanıcı verilerinin kaybedilmesinin, değiştirilmesinin ya da hatalı kullanımların önlenmesi amaçlanmaktadır.

Kriptografik Kontroller: Bilginin gizliliğinin, aslına uygunluğunun ve bütünlüğünün korunması amacıyla uygulanan kontrollerdir.

Sistem Dosyalarının Güvenliği: Bilgi teknolojileri ile ilgili projelerin ve destek hizmetlerinin güvenilir şekilde yürütülmesinin temin edilmesi ile sistem dosyalarına erişimin kontrol altında tutulmasını amaçlamaktadır.

Geliştirme ve Destek Süreçlerinde Güvenlik: Uygulama sistemi yazılımının ve bilgilerinin güvenliğinin sağlanması amaçlanmaktadır.

4.1.1.9 Ticari Süreklilik Yönetimi

İş süreklilik planlarının hazırlanması, uygulanması, test edilmesi ve yeniden değerlendirilmesi gibi ticari süreklilik yönetimi ilkelerinin belirlenmesine ilişkin hususları içeren kontroldür. Ticari faaliyetlerin karşılaşabileceği etkilere karşı gerekli önlemlerin alınması ile başarısızlık ve felaketlerden kaçınılmasını amaçlamaktadır. Alt kontrolleri ise şu şekildedir:

- Ticari süreklilik yönetim süreci
- Ticari süreklilik ve etki çözümlemesi
- Süreklilik planlarının yazılması ve uygulanması
- Ticari süreklilik planlama çerçevesi

4.1.1.10 Uyum

Güvenlik politikalarına ve kanunlara uyumun sağlanması için uygulanan kontrollerdir. Uyum kontrollerine ilişkin olarak ele alınması gereken hususlar aşağıdaki şekilde sıralanabilir:

- Yasal gereksinimlere uyum
- Güvenlik politikası ve teknik uyumun gözden geçirilmesi

- Sistem denetleme hususları

Yasal Gereksinimlere Uyum: Bilgi sistemlerinin şekli, işletilmesi ve kullanılması ile ilgili güvenlik gereksinimlerinin kanunlarla uyumlu olması amaçlanmaktadır.

Güvenlik Politikası ve Teknik Uyumun Gözden Geçirilmesi: Sistemlerin ve organizasyonun güvenlik politikalarının standartlara uygun olması amaçlanmaktadır.

Sistem denetleme hususları: Sistem izleme işlemlerinin etkisinin artırılması amaçlanmaktadır.

4.1.2 TS ISO/IEC 15408 Standardı

TS ISO/IEC 15408 Bilgi Teknolojisi – Güvenlik Teknikleri – Bilgi Teknolojisi Güvenliği için Değerlendirme Kriterleri; Ortak Kriterler (OK) olarak adlandırılan ve bilgi teknolojisi (BT) ürünlerinin güvenlik seviyelerinin değerlendirilebilmesini sağlayan standarttır. Farklı kesimler tarafından geliştirilmiş değerlendirme kriterleri bulunmasına rağmen uluslararası platformda genel kabul görmüş bir standart oluşturulmamasından dolayı bu şekilde ortak bir ölçüt dokümanına ihtiyaç duyulmuştur.

Ortak kriterler projesi 1993 yılında; ABD tarafından kullanılan TCSEC (Trusted Computer System Evaluation Criteria – Güvenilir Bilgisayar Sistemleri Değerlendirme Kriterleri), Avrupa'da kullanılan ITSEC (Information Technology Security Evaluation Criteria – Bilgi Teknolojileri Güvenlik Değerlendirme Kriterleri) ve Kanada tarafından uygulanan CTCPEC (Canadian Trusted Computer Product Evaluation Criteria – Kanada Güvenilir Bilgisayar Ürünleri Değerlendirme Kriterleri) standartlarının bir araya getirilmesi ve geliştirilmesi çalışmalarıyla başlamıştır. 1996 yılında CC

(Common Criteria – Ortak Kriterler) Versiyon 1.0 tamamlanmıştır. Versiyon 1.0, gelen görüşler ve yapılan çalışmalar sonrasında gözden geçirilerek 1998 yılında Versiyon 2.0 olarak yayınlanmıştır. Versiyon 2.0 1999 yılında "Bilgi Teknolojisi – Güvenlik Teknikleri – Bilgi Teknolojisi için Değerlendirme Kriterleri" adı altında 15408 numaralı ISO standardı olarak kabul edilmiştir. Ortak kriterlerin geliştirilmesi çalışmaları halihazırda devam etmektedir ve CC Versiyon 3.0'ın 2005 yılı içerisinde yayınlanması hedeflenmektedir. Ülkemizde ise yetkili kurum olan Türk Standardları Enstitüsü 2002 yılında ISO/IEC 15408'in tercümesini yaparak Türk standardı olarak kabul etmiştir. [66]

ISO/IEC 15408 standardı üç ayrı bölümden oluşmaktadır. Bunlar:

1. ISO/IEC 15408 – 1 Giriş ve Genel Model
2. ISO/IEC 15408 – 2 Güvenlik Fonksiyonel Gereksinimleri
3. ISO/IEC 15408 – 3 Güvenlik Garanti Gereksinimleri

4.1.2.1 Bölüm 1 – Giriş ve Genel Model

Ortak Kriterlerin giriş bölümünü oluşturmaktadır. BT güvenliği değerlendirmesinin genel kavramlarını ve ilkelerini açıklamakta ve genel bir değerlendirme modeli sunmaktadır. Bölüm 1 ayrıca BT güvenlik hedeflerinin ifade edilmesi, BT güvenlik gereksinimlerinin seçilmesi ve tanımlanması ile ürünler/sistemler için yüksek düzeyde belirtimler yazılması için yapılar sunmaktadır. Buna ek olarak, OK'nin üç bölümünün de kullanışlılığı hedef kitlelere göre tarif edilmektedir.

Bölüm 1'de geçen önemli tanımlar ve kavramlar şunlardır:
Değerlendirme Hedefi (Target of Evaluation - TOE): Değerlendirmeye konu olan bir BT ürününü ya da sistemi ve bunlarla ilgili yönetici ve kullanıcı kılavuzlarını ifade eder.

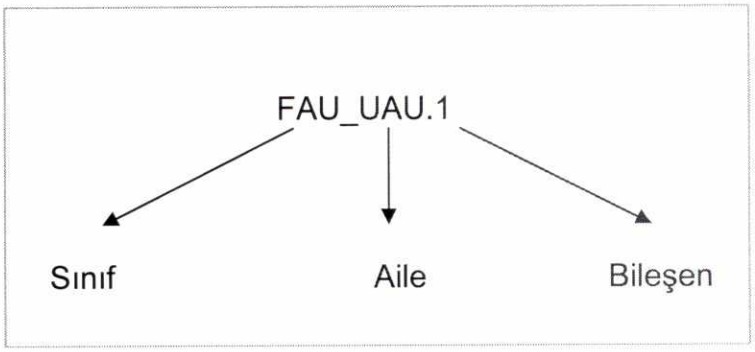
Koruma Profili (Protection Profile - PP): Belli müşteri ihtiyaçlarını karşılayan bir Değerlendirme Hedefi kategorisi için uygulamadan bağımsız güvenlik gerekliliklerini tanımlar.

Güvenlik Hedefi (Security Target - ST): Belirlenmiş bir Değerlendirme Hedefinin değerlendirilmesinde temel alınacak güvenlik gerekliliklerini ve özelliklerini ifade eder. [66]

4.1.2.2 Bölüm 2 – Güvenlik Fonksiyonel Gereksinimleri

Değerlendirme Hedefleri için fonksiyonel gereksinimleri ifade etmenin standart bir yolu olarak bir dizi fonksiyonel bileşeni oluşturmaktadır. Bölüm 2; fonksiyonel bileşenleri, aileleri ve sınıfları katalog halinde sunmaktadır. Güvenlik fonksiyonel gereksinimleri şunlardır: [67]

1. FAU: Güvenlik denetimi
2. FCO: İletişim
3. FCS: Şifreleme desteği
4. FDP: Kullanıcı verilerinin korunması
5. FIA: Tanıma ve kimlik doğrulama
6. FMT: Güvenlik yönetimi
7. FPR: Gizlilik
8. FPT: Güvenlik fonksiyonlarının korunması
9. FRU: Kaynak kullanımı
10. FTA: Değerlendirme hedefi erişimi
11. FTP: Güvenilir yollar/kanallar



Şekil 4.1 Güvenlik Gereksinimleri Organizasyonu

4.1.2.3 Bölüm 3 – Güvenlik Garanti Gereksinimleri

Değerlendirme Hedefleri'nin garanti gereksinimlerini ifade etmek için standart garanti bileşenleri tanımlamakta ve bunları aileleri ve sınıfları ile birlikte katalog halinde sunmaktadır. Ayrıca, koruma profilleri ve güvenlik hedefleri için değerlendirme kriterlerini ve değerlendirme hedefleri için güvenlik seviyelerini belirlemede kullanılmak üzere Değerlendirme Garanti Düzeyleri (Evaluation Assurance Level – EAL) tanımlamaktadır. [68]

Güvenlik garanti gereksinimleri 8 alt başlıkta incelenmiştir:

1. ACM: Konfigürasyon yönetimi
2. ADO: Dağıtım ve işletim
3. ADV: Geliştirme
4. AGD: Kılavuz Dokümanları
5. ALC: Hayat döngüsü desteği
6. ATE: Testler
7. AVA: Açıklık değerlendirmesi
8. AMA: Garantinin sürdürülmesi

Değerlendirme garanti düzeyi olarak da 7 farklı seviye belirlenmiştir. Bu seviyeler aşağıda yer almaktadır:

1. EAL1: Fonksiyonel Olarak Test Edilmiş
2. EAL2 Yapısal Olarak Test Edilmiş
3. EAL3 Metodolojik Olarak Test Edilmiş
4. EAL4 Metodolojik Tasarım, Test ve Kontrol
5. EAL5 Yarı-Biçimsel Tasarım ve Test
6. EAL6 Yarı-Biçimsel ve Doğrulanmış Tasarım ve Test
7. EAL7 Biçimsel ve Doğrulanmış Tasarım ve Test

4.2 ETSI Standartları

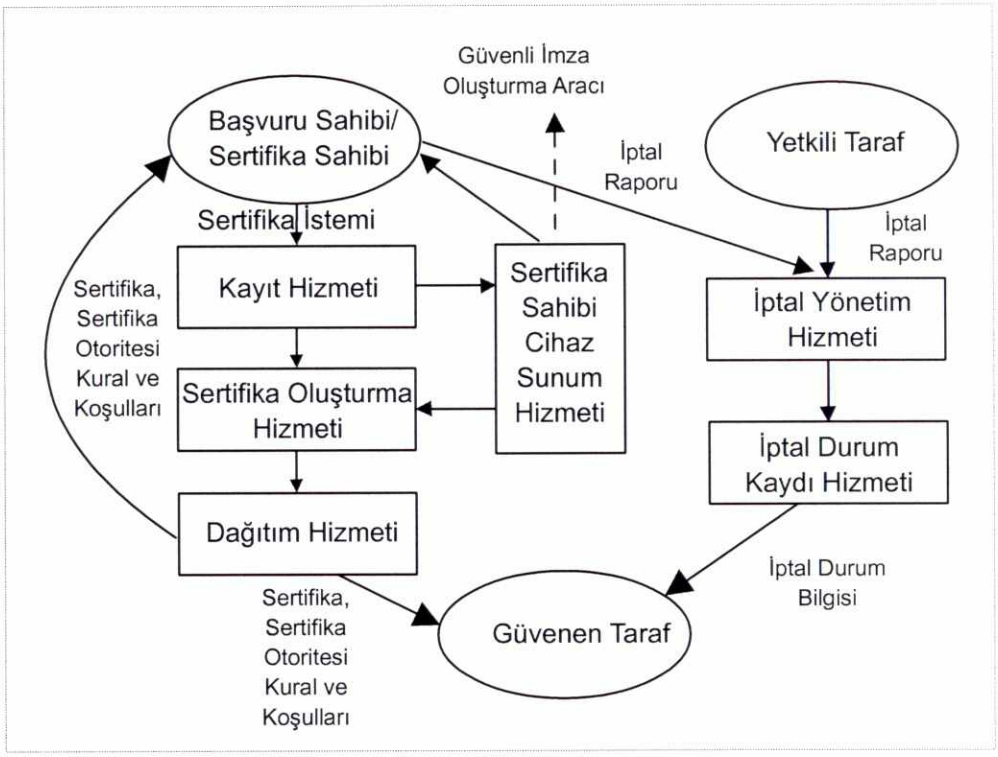
ETSI (European Telecommunications Standards Institude – Avrupa Telekomünikasyon Standartları Enstitüsü), telekomünikasyon standartları hazırlayan bağımsız bir kuruluştur. Özellikle bilgi ve iletişim teknolojilerine ilişkin standartlar düzenlemektedir. Telekomünikasyon Kurumu'nun da aralarında bulunduğu 688 üyeye sahiptir.

4.2.1 TS 101 456 Standardı

ETSI TS 101 456 "Nitelikli Sertifika Yayınlayan Sertifikasyon Otoriteleri için Politika Gerekleri" [18] adlı teknik tanımlama standardı, ETSI Güvenlik Teknik Komitesi tarafından hazırlanmıştır. Bu standart ile sertifika sahipleri, güvenen taraf ve ilgili diğer tarafların gerekli güveni duyabilmeleri için ESHS'lerin işletim ve yönetim uygulamaları çerçevesinde gerekli olan politikalar tanımlanmaktadır.

Elektronik sertifika politikası, bir sertifikanın belirli bir topluluk veya uygulamalar üzerinde uygulanabilirliğini genel güvenlik gerekleri çerçevesinde tanımlayan kurallar kümesi olarak açıklanmaktadır. [69]

ESHS'lerin yerine getirmesi gereken hizmetler arasında; kayıt hizmetleri, sertifika oluşturma, sertifika dağıtımı, sertifika iptal yönetimi, iptal durumu ve gerekli hallerde imza oluşturma aracı sunulması hizmetleri yer almaktadır. (Bkz. Şekil 4.2)



Şekil 4.2 Sertifikasyon Hizmetleri

Politika gerekleri, esas olarak güvenli elektronik imzalama için gerekli olan nitelikli elektronik sertifikaların sunumunu içermektedir. Bu içerik, 99/93/EC sayılı Elektronik İmza Direktifinin [70] Ek I ve Ek II bölümlerinde yer alan nitelikli elektronik sertifika yayınlayan ESHS'ler için güvenlik gerekleri ile Ek III'de tanımlanan güvenli elektronik imza oluşturma araçlarının kullanımıyla ilgili hususları karşılamaktadır. Adı geçen bölümler 5070 sayılı Elektronik İmza Kanunu ile de örtüşmektedir. Bu konu ile ilgili detaylı bilgi Bölüm 6 ve Bölüm 7'de yer almaktadır.

TS 101 456 temel olarak beş alt bölümden oluşmaktadır. Bu temel bölümler kısaca aşağıda yer almaktadır.

4.2.1.1 Genel Kavramlar

Genel kavramlar bölümünde standart içerisinde yer alan temel unsurlarla ilgili tanımlamalar yapılmakta ve bu unsurların doküman içerisinde kullanımları anlatılmaktadır. Bu tanımlamalar:

- Sertifikasyon Otoritesi
- Sertifikasyon Hizmetleri
- Sertifika İlkeleri ve Sertifika Uygulama Esasları
- Sertifika Başvurusu Sahipleri ve Sertifika Sahipleri

olarak sıralanmaktadır.

4.2.1.2 Nitelikli Elektronik Sertifika İlkelerine Giriş

Bu bölümde, elektronik sertifika politikaları tanımlanmış ve bunların standartta hangi şekilde ele alındığı belirtilmiştir. Standart kapsamında iki farklı politika yer almaktadır. Bunlardan ilki "Güvenli elektronik imza oluşturma aracı kullanımını gerektiren ve kamu kullanımına sunulan nitelikli elektronik sertifikalar", ikincisi ise "kamu kullanımına sunulan nitelikli elektronik sertifikalar"dır. Bu bölüm altında yer alan alt başlıklarda adı geçen politikaların tanımı yapılmakta, ilgili kullanıcı grubu ve uygulanabilirlik mercek altına alınarak uygunluk kriterleri belirlenmektedir.

4.2.1.3 Yükümlülük ve Sorumluluklar

Üçüncü bölümde, her iki sertifika politikası için sertifikasyon otoritelerinin ve kullanıcıların yükümlülükleri tanımlanmaktadır. Sertifikasyon otoritelerinin işlevlerini yerine getirirken alt yüklenicilerden aldığı hizmetler de dahil olmak üzere standartta yer alan hususlara, sunduğu hizmetlere ilişkin olarak da sertifika ilkelerine uyması gerektiği belirtilmektedir. Kullanıcılara ise başvuru sırasında doğru bilgilendirme yapması, anahtar çiftini sınırlamalar dahilinde kullanması, özel anahtarına gerekli özeni göstermesi, teknik kriterlere uyması, özel anahtarın güvenliğinden şüpheye düşülmesi veya sertifika içeriğinin değişmesi halinde sertifikasyon otoritesini bilgilendirmesi şeklinde yükümlülükler getirilmektedir.

Üçüncü alt başlık içerisinde, güvenen tarafların sertifikalara güvenerek işlem yapabilmesi için gereken kural ve koşullar sıralanmakta ve ilgili tarafların bu konular hakkında bilgilendirilmesi gerektiği belirtilmektedir. Son bölüm olan sorumluluklarda ise 99/93/EC sayılı AB Direktifinde yer alan sorumluluklar ile ilgili hususlara atıf yapılmaktadır.

4.2.1.4 Sertifika Otoritesi Uygulamaları için Gereklilikler

Bu bölümde, nitelikli elektronik sertifika yayınlayan sertifikasyon otoritelerinin; kayıt işlemlerine, sertifika oluşturma ve dağıtımına, sertifika iptaline, sertifika durum bilgilerine ve genel işleyişe ilişkin olarak sağlaması gereken güvenlik hedefleri ve bu hedeflere ulaşabilmede kullanılacak detaylı kontroller yer almaktadır. Dördüncü bölümde işlenen alt başlıklar aşağıda verilmiştir:

- Sertifika Uygulama Esasları
- Açık Anahtar Altyapısı – Anahtar Yönetimi Yaşam Döngüsü
    - Sertifikasyon otoritesi anahtar üretimi

  - Sertifikasyon otoritesi anahtar depolaması, yedeklemesi ve kurtarması
  - Sertifikasyon otoritesi açık anahtar dağıtımı
  - Anahtarın emanet edilmesi
  - Sertifika otoritesi anahtar kullanımı
  - Sertifika otoritesi anahtarı yaşam döngüsü sonu
  - Sertifika imzalamada kullanılan kriptografik donanımın yaşam döngüsü yönetimi
  - Sertifika otoritesi tarafından sunulan kullanıcı anahtar yönetimi hizmetleri
  - Güvenli elektronik imza oluşturma araçları hazırlanması
- Açık Anahtar Altyapısı – Sertifika Yönetimi Yaşam Döngüsü
  - Sertifika yenilenmesi, anahtar değişimi, ve güncellenmesi
  - Sertifika oluşturma
  - Kural ve koşulların dağıtımı
  - Sertifika dağıtımı
  - Sertifika iptali ve askıya alınması
- Sertifika Otoritesi Yönetimi ve İşleyişi
  - Güvenlik yönetimi
  - Varlık sınıflandırması ve yönetimi
  - Personel güvenliği
  - Fiziki ve çevresel güvenlik
  - İşleyiş yönetimi
  - Sistem erişim yönetimi
  - Güvenli sistem kurulumu ve bakımı
  - İş sürekliliği yönetimi ve acil durumlar
  - Sertifika otoritesi işleyişinin sona ermesi
  - Yasal gereklere uyum
  - Nitelikli sertifikalara ilişkin bilgilerin kaydı
- İşleyiş

4.2.1.5 Diğer Nitelikli Sertifika İlkelerinin Tanımlanması için Çatı

Bu maddede, nitelikli elektronik sertifika sunan sertifika otoritelerinin standart altında yer alan iki sertifika politikası dışında tanımlayacakları politikalar için bir çerçeve ortaya konulmaktadır. Bölüm altında yer alan alt başlıklar ise şu şekildedir:

- Nitelikli elektronik sertifika politikası yönetimi
- Kamuya açık olmayan nitelikli elektronik sertifikaların dışında olduğu hususlar
- İlave gereklilikler
- Uyumluluk

4.2.2 SR 002 176 Raporu

ETSI SR 002 176 "Elektronik İmzalar ve Altyapılar: Güvenli Elektronik İmza için Algoritma ve Parametreler" [71] isimli özel rapor 2003 yılında elektronik imza kullanımında teknik hususlara ilişkin güvenliğin ve birlikte çalışabilirliğin sağlanması amacıyla yayınlanmıştır. Avrupa Birliği tarafından onaylanmış imzalama ve özetleme algoritmaları ve bunlara ilişkin parametreleri içermektedir.

Bu doküman, güvenli elektronik imza oluşturma araçları (CWA 14168 ve CWA 14169) içerisinde yapılacak ve sertifika ilkeleri dokümanında (TS 101 456) referans verilecek imzalama ve doğrulama (CWA 14170 ve CWA 14171) işlemlerine ilişkin olarak kullanılacak algoritma ve parametreler ile diğer teknik bileşenleri ve ilgili alanları kapsamaktadır.
Bu kapsam içerisinde, aşağıda yer alan hususlara değinilmektedir:

- Kriptografik algoritmaların yönetimi
- İmza takımları

- Kriptografik özetleme fonksiyonları
- Doldurma (padding) metotları
- İmzalama algoritmaları ve ilgili anahtar üretme algoritmaları
- Rastgele sayı üretimi

Kriptografik Algoritmaların Yönetimi: Yönetim faaliyetleri olarak, teknik gelişmelerin takip edilmesi ve algoritma ve parametrelerle ilgili güvenliği etkileyecek durumların ortaya çıkması durumunda gerekli tedbirlerin alınması ve önerilen algoritma ve parametrelerin güncellenmesi gerektiği belirtilmektedir.

İmza Takımları: Bu başlık altında, imza takımını (İT) oluşturan bileşenler verilmektedir. Bu bileşenler:

- İmzalama algoritması ve parametreleri
- Anahtar oluşturma algoritması
- Doldurma metodu
- Kriptografik özet fonksiyonu

olarak sıralanmaktadır. Yukarıda sayılan bileşenlerden herhangi birisinin güvenilirliğini kaybetmesi durumunda ilgili imza takımı da güvenilirliğini kaybetmektedir. Ayrıca her bir imza takımının güvenli olarak kullanılabileceği tarih de verilmektedir. İmza takımları ve son kullanma tarihleri Çizelge 4.1'de yer almaktadır.

İT Giriş Dizini	İmza Algoritması	Parametreler	Anahtar Üretme Algoritması	Doldurma Metodu	Özet Fonksiyonu	Tarih
001	RSA	MinModLen=1020	rsagen1	emsa-pkcs1-v1_5	sha1	31.12.2005
002	RSA			emsa-pss	sha1	31.12.2005
003	RSA			emsa-pkcs1-v1_5	ripemd160	31.12.2005
004	RSA			emsa-pss	ripemd160	31.12.2005
005	DSA	pMinLen=1024 qMinLen=160	dsagen1	-	sha1	31.12.2005
006	ECDSA-F_p	qMinLen=160 r_0Min=10^4 MinClass=200	ecgen1	-	sha1	31.12.2005
007	ECDSA-F_{2m}		ecgen2	-	sha1	31.12.2005
008	ECGDSA-F_p		ecgen1	-	sha1	31.12.2005
009	ECGDSA-F_p		ecgen1	-	ripemd160	31.12.2005
010	ECGDSA-F_{2m}		ecgen2	-	sha1	31.12.2005
011	ECGDSA-F_{2m}		ecgen2	-	ripemd160	31.12.2005

Çizelge 4.1 Onaylanmış İmza Takımları

Kriptografik Özet Fonksiyonları: Özet fonksiyonlarının çakışma korumalı olması gerektiği belirtilmiş ve aşağıda yer alan özet fonksiyonları güvenli olarak kabul edilmiştir:

- SHA-1 (Bkz. Bölüm 3.2.2)
- RIPEMD (Bkz. Bölüm 3.2.3)

Doldurma Metotları: Özet değerinin imzalanması işleminde bazı algoritmalar (örneğin RSA) belirli bir blok uzunluğuna ihtiyaç duymaktadır. Bu ihtiyaçların karşılanabilmesi için aşağıda yer alan doldurma metotları önerilmektedir:

- emsa-pkcs1-v1_5 (Bkz. Bölüm 3.3.1)
- emsa-pss (Bkz. Bölüm 3.3.1)

İmzalama ve Anahtar Oluşturma Algoritmaları: Bu kısımda, özet değeri üzerine uygulanacak imzalama algoritmaları ile bu algoritmaların anahtarlarını oluşturmada kullanılacak metotlara yer verilmiştir. Güvenli kabul edilen imza algoritmaları şunlardır:

- RSA (Bkz. Bölüm 3.3.1)
- DSA (Bkz. Bölüm 3.3.3)
- Eliptik eğri DSA (ECDSA) (Bkz. Bölüm 3.3.4)
- Eliptik Eğri Alman DSA (ECGDSA)

Bu algoritmalar için onaylanmış anahtar üretme algoritmaları ise aşağıda verilmiştir:

- rsagen1
- dsagen1
- ecgen1
- ecgen2

Rastgele Sayı Üretimi: Rastgele sayı üretimi, imza oluşturma verisi (özel anahtar) veya bazı parametrelerin oluşturulmasında kullanılmaktadır. Bunların yanında, bazı durumlarda doldurma metotları tarafından da rastgele sayı üretimine ihtiyaç duyulmaktadır. Onaylanmış rastgele sayı üretimi metotları aşağıda verilmiştir:

- trueran
- pseuran
- cr_to_X9.30_x
- cr_to_X9.30_k

4.3 CEN Çalıştay Kararları

CEN, Avrupa Birliği üyesi 28 ülkenin katılımıyla oluşturulan ve ulusal standardizasyon kurumları ile ISO arasında yer alan kuruluştur. CEN tarafından yayınlanan çalıştay kararları (CEN Workshop Agreement - CWA) standart doküman olarak değerlendirilmemektedir. Herkese açık olan bu çalıştay kararları CEN üyesi ulusal standart kurumları için referans belgesi olarak yayınlanmıştır. Ancak elektronik imza ile ilgili düzenlemelerde sıklıkla referans gösterilmektedir. Elektronik imza güvenliği ile ilgili çalıştay kararları alt başlıklarda detaylı bir şekilde açıklanmaktadır.

4.3.1 CWA 14167-1:2003

CWA 14167-1:2003 "Elektronik İmzalar için Güvenilir Sertifika Yönetim Sistemlerine ilişkin Güvenlik Gerekleri – Bölüm 1: Sistem Güvenlik Gerekleri" [72] belgesi, 2003 yılında nitelikli ve nitelikli olmayan elektronik sertifika oluşturan elektronik sertifika hizmet sağlayıcılarının kullandıkları cihaz ve teknolojik bileşenlerin güvenlik gereklerini ortaya koymak için hazırlanmıştır.

Bu çalıştay kararı, özellikle sertifika yönetimi için kullanılan güvenilir sistemlerin üreticilerini ilgilendirmektedir. Ancak, diğer sistemlerin 99/93/EC sayılı Avrupa Birliği Direktifinde yer alan gerekleri karşılanmasında da kullanılabilmektedir.

Doküman içerisinde ESHS'ler tarafından sağlanacak hizmetler iki kısma bölünmüştür. Bunlardan ilki "Ana Hizmetler" olarak adlandırılmıştır ve her ESHS tarafından sunulması zorunlu olan hizmetleri kapsamaktadır. İkincisi ise "Tamamlayıcı Hizmetler" olarak adlandırılmakta olan seçimli hizmetleri içermektedir. Ana hizmetler aşağıda yer alan hizmetleri kapsamaktadır:

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

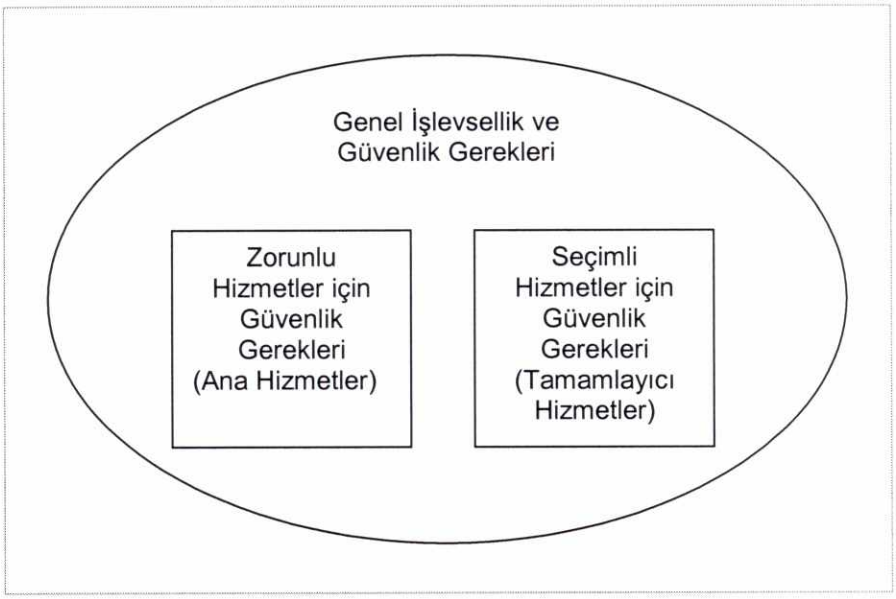
Tamamlayıcı hizmetler ise aşağıda yer almaktadır:

- Sertifika Sahibi Cihaz Sunum Hizmeti
- Zaman Damgası Hizmeti

ESHS'ler sunmak zorunda oldukları veya seçimli olarak tercih ettikleri hizmetler için güvenlik gereklerini karşılamak durumundadır. Bu hizmetlerin sunumunda kullanılacak güvenilir sistemlerin güvenlikleri ile genel işlevsellik ve güvenlik gereklerine ilişkin detaylı açıklamalar bu çalıştay kararı içerisinde yer almaktadır. CWA 14167-1:2003'e ilişkin olarak uygunluk değerlendirmesi için CWA 14172-3 [73] dokümanına başvurulmalıdır.

Özellikle ETSI TS 101 456'ya göre hazırlanmış sertifika ilkelerine uyum, bu çalıştay kararına uygunluğu onaylanmış güvenilir sistemler kullanılarak kolaylıkla gerçekleştirilmektedir.

CWA 14167-1 temel olarak üç alt bölüme ayrılmıştır. Birinci bölümde genel işlevsellik ve güvenliğe, ikinci bölümde ana hizmetlere, üçüncü bölümde ise tamamlayıcı hizmetlere yönelik güvenlik gerekleri tanımlanmaktadır. Bu güvenlik gerekleri arasında kurulmuş ilişki Şekil 4.3'te verilmektedir.



Şekil 4.3 Güvenlik Gerekleri İlişkisi

Genel güvenlik gerekleri içerisinde yer alan alt başlıklar aşağıda yer almaktadır:

- Yönetim
- Sistem ve Çalışma
- Tanımlama ve Kimlik Doğrulama
- Sistem Erişim Kontrolü
- Anahtar Yönetimi
- Hesaplama ve Denetim

- Arşivleme
- Yedekleme ve Kurtarma

4.3.2 CWA 14167-2:2004

CWA 14167-2:2004 "Sertifika Hizmet Sağlayıcıları İmzalama İşlemi için Yedeklemeli Kriptografik Modül – Koruma Profili – CMCSOB PP" [74], CEN tarafından yayınlanan ve ISO 15408 (Ortak Kriterler) (Bkz. Bölüm 4.1.2) standardında yer alan kural ve formatların uygulanması ile kriptografik modüller için hazırlanmış bir koruma profilidir. İlk olarak 2002 yılında yayınlanmıştır. Ancak Ortak Kriterler 2.1'e uygunluk sağlanması için 2004 yılında güncellenmiş ve yedekleme fonksiyonu da eklenmiştir. Yedekleme fonksiyonu bulunmayan koruma profili de CWA 14167-4:2004 [75] olarak varlığını sürdürmektedir.

Değerlendirme hedefi (Target of Evaluation - TOE) olarak adlandırılan kriptografik modüller için koruma profili güvence seviyesi EAL4+ (Artırılmış EAL4) seviyesindedir. Güvence seviyesinin artırılmasında eklenen hususlar şu şekildedir:

- Değerlendirme Hedefi (DH) Güvenlik Fonksiyonlarının Uygulanması (ADV_IMP.2)
- Zayıflık Değerlendirmesi, Gizli Kanal Analizi (AVA_CCA.4)
- Zayıflık Değerlendirmesi, Yüksek Dirençli (AVA_VLA.4)

CWA 14167-2:2004 6 bölümden oluşmaktadır. Bu bölümler aşağıda yer almaktadır:

- Koruma Profili Tanıtımı
- Değerlendirme Hedefi Tanımı
- Değerlendirme Hedefi Güvenlik Çevresi

- Güvenlik Amaçları
- Bilgi Teknolojileri Güvenlik Gerekleri
- Açıklamalar

Koruma Profili Tanıtımı: Giriş olarak hazırlanmış bu bölümde koruma profili ile ilgili genel bilgiler verilmektedir. Ayrıca, koruma profili ile ilgili 99/93/EC sayılı Avrupa Birliği Direktifi Ek II ve ETSI TS 101 456'da yer alan hususlara değinilmektedir.

Değerlendirme Hedefi Tanımı: Değerlendirme hedefi, sertifika hizmet sağlayıcısının imza oluşturma verisinin meydana getirilmesinde ve bu verinin kullanımında işlev gören kriptografik modülleri tanımlamaktadır. Koruma profili kapsamı esas olarak sertifika imzalama işlevi üzerine kurulmuş olsa da iptal durum kayıtlarının oluşturulması veya zaman damgası sunumu gibi imzalama işlemleri üzerine de uygulanabildiği belirtilmektedir. Değerlendirme hedefinin aşağıda yer alan işlevleri de desteklemesi gerekmektedir:

- Kullanıcı kimlik denetimi
- Anahtar oluşturulmasında ve imha edilmesinde erişim kontrolü
- Anahtarların sertifika imzalamada kullanılmasında erişim kontrolü
- DH'de güvenlikle ilgili değişikliklerin denetimi
- DH'nin öz sınaması

Bunların yanı sıra, DH'nin imza oluşturma verisini kendi içerisinde yaratılmasını ve saklanmasını (kriptografik modül dışına çıkarılamamasını) sağlamalı ve imzalanacak veriyi doğru bir şekilde göstermelidir.

Bu bölüm altında yer alan 2 alt başlığın birincisinde DH kullanıcı kategorilerine, ikincisinde ise DH kullanımına ilişkin bilgiler verilmektedir.

DH Güvenlik Çevresi: Bu bölümde, DH'nin kullanımında ilgili olan varlıklar tanımlanmakta ve işlevlere ilişkin kullanıma ilişkin varsayımlarda bulunulmaktadır. Ayrıca bu varlık ve işlevler üzerinde risk oluşturabilecek DH'nin arızalanması, imzanın taklit edilmesi, DH'nin güvensiz kullanımı gibi tehditlere de yer verilmektedir.

Güvenlik Amaçları: Bu bölümde, DH ve DH çevresi için güvenlik amaçları tanımlanmakta ve tarif edilmektedir. Güvenlik amaçları; tanımlanmış tehditlere karşı koymakta ve organizasyonel güvenlik politikaları ve varsayımlarla uyum sağlamaktadır.

Bilgi Teknolojileri Güvenlik Gerekleri: Bu bölümde, DH ve çevresi için güvenlik işlevsel gerekleri ve güvenlik güvence gerekleri verilmektedir. Güvenlik işlevsel gerekleri, Ortak Kriterler Bölüm 2'den alınmıştır. Güvenlik güvence gerekleri ise Ortak Kriterler Bölüm 3'de yer alan güvenlik güvence bileşenlerinden elde edilmiştir. Ayrıca bilgi teknolojileri ile ilgili olmayan hususlar da bu bölüm altında ele alınmaktadır.

Açıklamalar: Bu bölümde bilgi teknolojileri güvenlik amaçlarının politika ve tehditler karşısında yeterli olup olmadığı gösterilmektedir. Her bir politika gereği ve tehdit için ayrı ayrı argümanlar verilmiştir. Ayrıca, tüm gereklerin amaçlar çerçevesinde tam olduğu ve her bir amacın bir veya daha fazla bileşen ile adreslendiği gösterilmektedir. Son olarak da koruma profili gereklerine ilişkin olarak bağlılık analizleri, fonksiyonların dayanıklılıkları ile tutarlılığa ilişkin hususlar ortaya konulmaktadır.

4.3.3 CWA 14169:2004

CWA 14169:2004 "Güvenli İmza Oluşturma Araçları – EAL4+" [76] dokümanında, 99/93/EC sayılı Avrupa Birliği Direktifi Ek III'de tanımlanan güvenli imza oluşturma araçlarına (GİOA) ilişkin güvenlik gerekleri yer

almaktadır. Ortak Kriterlere göre hazırlanmış 3 ayrı koruma profili içermektedir. Bu koruma profilleri:

- Koruma Profili – Güvenli İmza Oluşturma Aracı Tip 1, Versiyon 1.05
- Koruma Profili – Güvenli İmza Oluşturma Aracı Tip 2, Versiyon 1.04
- Koruma Profili – Güvenli İmza Oluşturma Aracı Tip 3, Versiyon 1.05

olarak sıralanmakta ve ilgili çalıştay kararında Ek A, B ve C olarak sunulmaktadır.

Güvenli imza oluşturma araçları koruma profilleri için değerlendirme garanti düzeyi, arttırılmış EAL4 (EAL4+) seviyesindedir. Koruma profiline yapılan eklemeler aşağıdadır:

- Zayıflık Değerlendirmesi: AVA_MSU.3 (Güvensiz durumların analiz ve testi)
- Zayıflık Değerlendirmesi: AVA_VLA.4 (Yüksek dirençli)

CWA 14169:2004 ile güvenli imza oluşturma araçlarının güvenlik gerekleri için olabildiğince teknoloji bağımsız bir yaklaşım sergilenmeye çalışılmıştır. Bu yaklaşımla, hali hazırdaki teknolojiler incelenerek mümkün olduğunda farklı çeşitte cihazın kapsanması amaçlanmıştır. Ancak, uygulamalarda yer alabilecek çeşitliliğe rağmen bu dokümanda ortaya konulan yaklaşım, Şekil 4.4'te verildiği şekliyle imza oluşturma verisi (İOV) işlevselliğini kapsayacak biçimdedir.

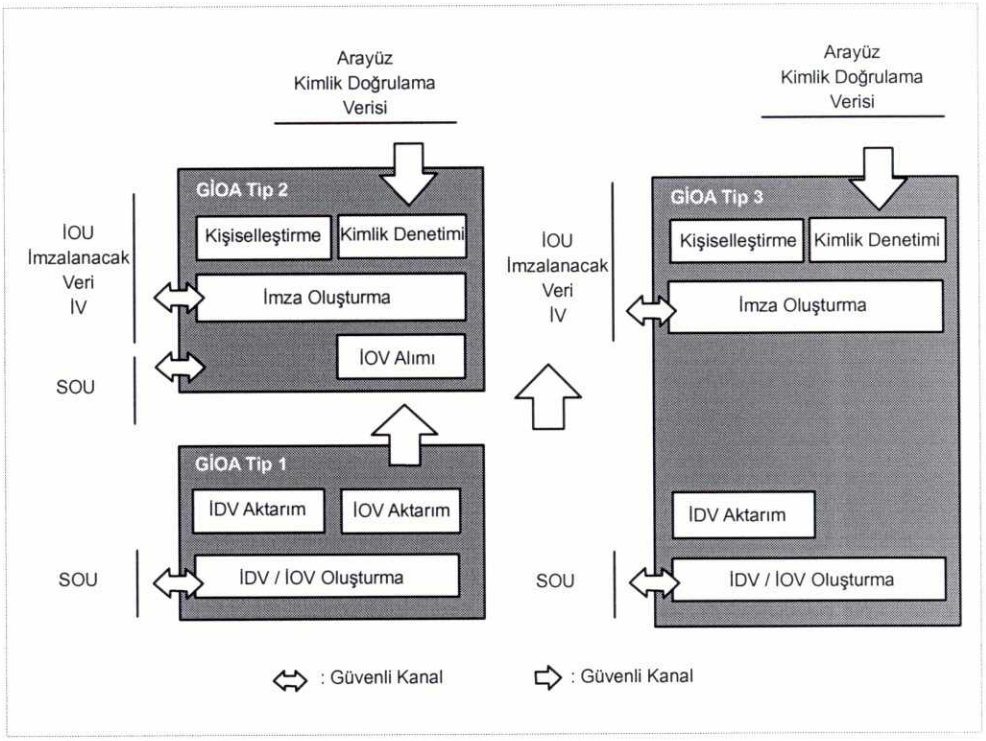
Şekil 4.4 Güvenli İmza Oluşturma Aracı

Güvenli imza oluşturma araçları güvenlik gerekleri, imza oluşturma ve doğrulamada kullanılabilecek algoritma ve parametrelere ilişkin olarak da şartlar içermektedir. Onaylanmış algoritma ve parametreler ile ilgili detaylı açıklamalar ETSI SR 002 076'da (Bkz. Bölüm 4.2.2) verilmektedir.

Koruma profili verilen 3 farklı GİOA yaklaşımı Şekil 4.5'te verilmektedir. Bu şeklin sol tarafında imza oluşturma verisi ve imza doğrulama verisi (İDV) oluşturma bileşenini içeren GİOA Tip 1 ve İOV belleğini ve imza oluşturma bileşenlerini içeren GİOA Tip 2 yer almaktadır. Bu yapıda; GİOA Tip 1 üzerinde oluşturulan bir İOV'nin GİOA Tip 2'ye, imza oluşturma uygulaması (İOU) ile hazırlanan imzalanacak verinin GİOA'ya ve imzalanmış verinin (İV) İOU'ya aktarımında güvenli kanallar kullanılması zorunludur.

Burada yer alan GİOA Tip 2 kullanıcıya tahsis edilmiş olmalı ve kimlik doğrulama verisi ile erişilebilmelidir. GİOA Tip 1 ise farklı kişiler tarafından kullanılabilir.

Şekil 4.5'in sağ tarafında ise İOV aktarımı hariç olmak üzere Tip 1 ve Tip 2'nin kombinasyonundan oluşan GİOA Tip 3 yer almaktadır.



Şekil 4.5 GİOA Tipleri

4.3.4 CWA 14170:2004

CWA 14170:2004 "İmza Oluşturma Uygulamaları için Güvenlik Gerekleri", [77] imza oluşturma araçları (İOA) ile imza oluşturma için kullanılan uygulamalara ilişkin güvenlik gerekleri ile tavsiyeleri içermektedir. Bahse konu imza oluşturma araçları; kendi işlem gücüne sahip, kimlik doğrulaması yapabilen ve kriptografik işlevleri yerine getirebilen fiziksel bir donanım olmalıdır. Aksi belirtilmedikçe İOA kavramı güvenli imza oluşturma araçlarını temsil etmektedir.

Bu doküman kapsamında:

- İmza oluşturma ortamı modeli ve imza oluşturma uygulaması işlevsel modeli,

- İşlevsel model içerisinde yer alan tüm fonksiyonlar üzerinde uygulanacak gerekler,
- İmza oluşturma uygulaması içerisinde tanımlanan tüm işlevler için güvenlik gerekleri

incelenmektedir. Bununla beraber, aşağıda yer alan hususlar kapsam dışında bırakılmıştır:

- İOV oluşturulması ve dağıtımı ile kullanılacak kriptografik algoritmalar,
- Elektronik imza çeşitlerinin ilgili kanunlar çerçevesinde yorumlanması.

CWA 14170:2004 içerisinde yer alan 1-5 arasındaki bölümlerde, güvenlik gereklerinin desteklenmesi için ihtiyaç duyulan tanımlar, modelleme ve teknik hususlara giriş yapılmaktadır. Bu bölümlerde herhangi bir gereklilik tanımlanmamıştır.

Bölüm 6'dan Bölüm 17'ye kadar, imza oluşturma uygulamaları içerisinde yer alan her bir işlevsel bileşen için güvenlik gerekleri açıklamalarla birlikte tanımlanmaktadır. Sözü edilen bölümlerin listesi aşağıda verilmektedir.

- İmza sahibi etkileşim bileşeni
- İmza sahibi kimlik doğrulama bileşeni
- İmzalanacak doküman biçimleyicisi
- Veri özetleme bileşeni
- İOA – İOU iletişimcisi
- İOV – İOU doğrulayıcısı
- İmzalanacak doküman hazırlayıcısı
- İmzalanmış veri hazırlayıcısı
- Giriş/çıkış için harici arayüz

4.3.5 CWA 14171:2004

CWA 14171:2004 "Elektronik İmza Doğrulama için Genel Hususlar" [78] dokümanı, 99/93/EC sayılı AB Direktifi Ek IV kapsamında elektronik imzanın doğrulanması ile ilgili tavsiye edilen işlev ve güvenceler çerçevesinde hazırlanmıştır. İlave olarak, güvenli elektronik imzanın doğrulanmasına ilişkin yöntemlerin yanı sıra imzalama işleminden çok sonra da doğrulamanın yapılabilmesi için gerekli verilerle ilgili hususlar da kapsanmaktadır.

CWA 14171:2004, aşağıda yer alan dört alt bölümden oluşmaktadır:

- Doğrulama Süreci
- İmza Doğrulama Sistemleri
- İmza Doğrulama Sistemleri için Güvenlik Gerekleri
- Arşiv Sistemi

Doğrulama Süreci: Bu bölümde, doğrulama ihtiyacına göre imza çeşitleri ile anlık, kısa süreli ve uzun süreli imzalar olmak üzere imza doğrulama yaşam sürecine ilişkin bilgiler verilmektedir. Ancak anlık olarak kullanılan ve daha sonra ihtiyaç duyulmayan imzalar bu doküman kapsamında yer almamaktadır. Yapılan ilk doğrulamada, sonradan gerçekleştirilecek doğrulamalarda kullanılacak ve doğrulama sonucunda elde edilecek bilgiler ile doğrulamada izlenecek yöntemlere ilişkin kurallar bu bölüm içerisinde işlenmektedir. Bu bölüme ilişkin alt başlıklar aşağıda yer almaktadır:

- İmza yaşam süreci
- Doğrulama bilgi gerekleri
- TS 101 733 [79] ve TS 101 903'de [80] tanımlanan imza biçimleri
- İlk doğrulama girdileri
- İlk doğrulama çıktıları
- Doğrulama süreci kuralları

- Sonradan doğrulama girdileri

İmza Doğrulama Sistemleri: Bu bölümde, imza doğrulama sistemlerine ilişkin bilgiler verilmekte ve bu sistemlerde bulunması gereken özellikler sıralanmaktadır. İmza doğrulama sistemlerinin güvenliğinin; uygulamaların güvenli olarak geliştirilmesine, doğru yüklenmesine ve saldırılardan kaçınabilmesine (en azından saldırıları tespit edebilmesine) bağlı olduğu belirtilmektedir. Ayrıca, sistemlerin güvenli bir şekilde kullanımı yüklemenin doğru yapılmasıyla ve yüklemeden sonra uygulanan güvenlikle ilgili değişikliklerin belirlenmesiyle ilişkili olduğundan bahsedilmektedir. Bu bölüm altında yer alan alt başlıklar aşağıda verilmektedir:

- İlk doğrulama sistemleri
- Sonradan doğrulama sistemleri
- Kişiler tarafından yapılan doğrulama
- Cihaz tarafından yapılan doğrulama
- Üçüncü tarafların doğrulaması

İmza Doğrulama Sistemleri için Güvenlik Gerekleri: Bu bölümde, 99/93/EC sayılı AB Direktifi Ek IV'de yer alan doğrulama işlemi için güvenlik gereklerinin yerine getirilmesi amaçlanmaktadır. Bu gereklerin karşılanması için güvenilir imza doğrulama sistemlerinin, doğrulama işleminin değiştirilmesine ve doğrulama yapan taraflara yanlış bilgi vermesine karşı korumalı olması gerekmektedir. Bu açıdan, teknik koruma seviyesi ve doğrulayan kişiler tarafından uygulanacak risk yönetimi dikkate alınarak üç farklı uygulama seviyesi belirlenmiştir. İlgili güvenlik yöntemlerinin uygulandığı bu modüller aşağıda yer almaktadır:

- Yazılım modülü
- Değişim tespit eden modül
- Değişim önleyen modül

Bu bölüm altında yer alan alt başlıklar ise aşağıda verilmiştir:

- Değişim tespit eden ve değişim önleyen modüller için gerekler
- Yükleme ve doğrulamaya ilişkin varsayımlar
- Gerekler

Arşiv Sistemi: Bu bölümde, arşivlenmiş elektronik imzalar ile bunların geçerliliklerinin sınanması için gerekli olan verilere ilişkin bilgiler verilmektedir. Aynı zamanda arşiv sisteminde bulunması gereken özellikler de sıralanmaktadır.

5 DÜNYA'DA ELEKTRONİK İMZA GÜVENLİĞİ DÜZENLEMELERİ

5.1 Avrupa Birliği

Avrupa Birliği'nin elektronik imzaya ilişkin düzenlemeleri 13 Aralık 1999 tarihinde AB Resmi Gazetesi'nde yayınlanan 99/93/EC sayılı Elektronik İmza Direktifi ile başlamaktadır. Bu direktif ile AB üyesi ülkeler için bir çerçeve ortaya konulmuş ve üye ülkelerin düzenlemelerini 19 Temmuz 2001 tarihine kadar tamamlamaları istenmiştir.

99/93/EC sayılı Direktif, elektronik imza güvenliğine ilişkin hususları ek olarak ortaya koymaktadır. Bunlar:

- Ek-I: Nitelikli Sertifikalar için Gerekler
- Ek-II: Nitelikli Sertifika Yayınlayan Sertifika Hizmet Sağlayıcılar için Gerekler
- Ek-III: Güvenli İmza Oluşturma Araçları için Gerekler
- Ek-IV: Güvenli İmza Doğrulama için Öneriler

olarak sıralanmaktadır.

Ek-I'de yer alan hususlar nitelikli elektronik sertifikalarda bulunması gereken özellikleri tanımlamaktadır. Nitelikli elektronik sertifikalar içerisinde yer alacak alanlar ise şöyle sıralanmaktadır:

a) Sertifikanın nitelikli olduğuna dair ibare,
b) Sertifika hizmet sağlayıcının kimliği ve bulunduğu ülke,
c) İmza sahibinin ismi veya takma adı ile takma ad kullanıldığına dair bilgi,
d) Sertifikanın kullanımı için gerekli olan imza sahibi hakkındaki diğer bilgiler

e) İmza sahibinin imza oluşturma verisine karşılık gelen imza doğrulama verisi,
f) Sertifika geçerlilik süresi,
g) Sertifika seri numarası,
h) Yayınlayan sertifika hizmet sağlayıcının imzası,
i) Varsa sertifikanın kullanımına ilişkin kapsam ve
j) Varsa sertifikanın işlem limiti.

Ek-II'de ise sertifika hizmet sağlayıcılarının güvenilirlikleri ve sundukları hizmetlerin güvenliği için yerine getirmeleri gereken şartlar ortaya konulmaktadır. Bu şartlar aşağıda verilmektedir:

a) Sertifikasyon hizmeti sunumu için gerekli olan güvenilirliği ortaya koymak,
b) Sürekli hazır ve güvenli dizin hizmeti ile güvenli ve anında iptal hizmeti verilmesini sağlamak,
c) Sertifikanın düzenlendiği ya da iptal edildiği tarihin ve zamanın kesin olarak bilinmesine olanak sağlamak,
d) Nitelikli sertifika düzenlenen kişinin kimliğini ve eğer varsa özel atıfların milli mevzuata uygun olarak doğrulanmasını sağlamak,
e) Sunulan hizmetler için gerekli uzmanlık bilgisi, deneyim ve niteliklere sahip olan, özellikle idari seviyede elektronik imza teknolojisinde uzmanlaşmış ve uygun güvenlik prosedürlerini yeterince bilen personel istihdam etmek; kabul edilen standartları ve bu standartlarda yer alan idari prosedürleri uygulamak,
f) Değişikliklere karşı korunan güvenilir sistemler ve ürünler kullanmak ve bunlar tarafından gerçekleştirilen işlemlerin teknik ve şifreleme güvenliğinden emin olmak,
g) Sertifikalarda sahtekarlık yapılmasına karşı gerekli önlemleri almak ve imza oluşturma verilerinin sertifika hizmet sağlayıcısı tarafından üretilmesi durumunda söz konusu işlemin gizliliğini garanti etmek,

h) Direktif'te belirtilen koşullara uygun olarak faaliyetlerin yürütülmesi için yeterli mali kaynağa sahip olmak. Özellikle, meydana gelebilecek hasarlar için örneğin uygun sigorta yollarıyla zarar yükümlülüklerine karşı gerekli mali kaynağı sağlamak,

i) Özellikle hukuki davalarda ispatlayıcı delil olarak kullanılmak üzere, yeterli bir süre boyunca nitelikli sertifikalara ilişkin bilgileri saklamak,

j) Anahtar yönetim hizmeti sunduğu kişilerin elektronik imza oluşturma verilerini kaydetmemek ya da kopyalamamak,

k) Elektronik imza için sertifika talebinde bulunan bir kişiyle sözleşme yapmadan önce, söz konusu kişiye güvenilir bir haberleşme yöntemiyle kullanımdaki sınırlamalar, ihtiyari akreditasyon planı, şikayetler ve anlaşmazlıkların çözümüyle ilgili prosedürler gibi sertifikanın kullanımıyla ilgili olarak koşullar hakkında bilgi vermek. Elektronik olarak gönderilebilecek olan bu bilgiler yazılı ve kolay anlaşılır bir dilde olmalıdır. Bilginin ilgili bölümleri, talep halinde söz konusu sertifikalara dayanarak faaliyette bulunan üçüncü taraflara da gönderilmelidir.

l) Sertifikaların doğrulanabilir bir şekilde saklanmasında güvenilir sistemler kullanmak. Bu sistemler:

   - Sadece yetkili kişilerin sisteme veri girmesine ve değişiklik yapabilmesine izin veren,
   - Doğrulama amaçlı olarak verilerin kontrol edilebilmesini sağlayan,
   - Sertifikaların ancak imza sahibinin onayı alındıktan sonra kamuya açık hale getirilebilmesini sağlayan ve
   - Bu güvenlik koşullarını riske eden her türlü teknik değişiklikten işletmecinin haberinin olmasını sağlayan

özellikte olmalıdır.

Ek-III, gelişmiş elektronik imzanın işlevselliğini temin etmek açısından güvenli elektronik imza oluşturma araçları ile ilgili gerekleri ortaya koymaktadır. Ancak bu gerekler, GİOA'nın üzerinde çalıştığı ortamları kapsamamaktadır. GİOA'da bulunması gereken özellikler aşağıda yer almaktadır:

a) Güvenli imza oluşturma araçları, teknik açıdan ve yöntem açısından asgari olarak:
   - İmza oluşturma verisinin pratikte yalnızca bir defa elde edilen ve gizliliği makul seviyede sağlanan,
   - İmza oluşturma verisinin yeniden elde edilebilmesi ve imzanın mevcut teknolojiler kullanılarak taklit edilmesini önleyen,
   - İmza oluşturma verisinin, imza sahibi dışındakiler tarafından izinsiz kullanımına karşı imza sahibi tarafından korunan

   bir yapıda olması gerekmektedir.
b) Güvenli imza oluşturma aracının, imzalanacak veride herhangi bir değişiklik yapılmasını veya imzalanacak verinin işlemden önce imza sahibine gösterimini engelleyen bir yapıda olmaması gerekmektedir.

Yukarıda detayları verilen her üç Ek'te yer alan hususların uygulanması zorunlu olmasına karşın Ek-IV'de yer alan maddeler yalnızca güvenli imza doğrulamaya ilişkin önerilerden oluşmaktadır. Bu önerilerde güvenli imza doğrulama için:

a) İmza doğrulama için kullanılan verinin, imza doğrulayan tarafa gösterilen verilere uygunluğundan,
b) İmzanın güvenilir bir şekilde doğrulandığından ve doğrulama sonucunun değiştirilmeksizin gösterildiğinden,
c) Gerektiğinde, doğrulama yapan kişiye, imzalanmış verinin içeriğini güvenilir bir şekilde gösterilebildiğinden,
d) İmza doğrulama esnasında sertifikanın doğruluğunun ve geçerliliğinin sınandığından,

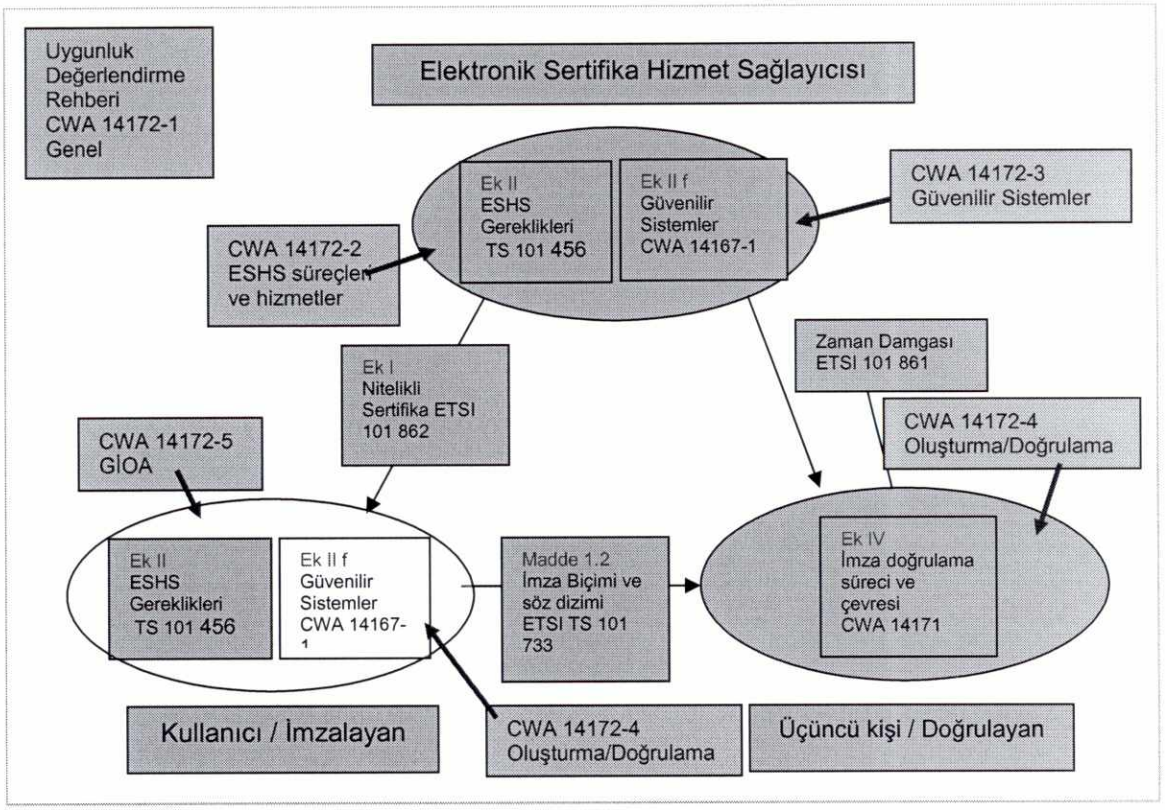
e) Doğrulamanın sonucunun ve imza sahibinin kimliğinin doğru bir biçimde gösterildiğinden,
f) Takma ad kullanımının açık bir şekilde belirtildiğinden,
g) Güvenlikle ilgili değişiklikleri tespit edildiğinden

emin olunmalıdır.

99/93/EC sayılı AB Direktifi'nin 3üncü maddesinin beşinci fıkrası uyarınca, AB Komisyonu Ek-II Madde f ve Ek-III'e ilişkin olarak kabul edilen standartların referans numaralarını 2003/511/EC sayılı Direktif [81] altında 14 Temmuz 2003 tarihli AB Resmi Gazetesi'nde yayınlamıştır. 2003/511/EC'ye göre kabul edilen bu standartlar:

- CWA 14167-1 (Bkz. Bölüm 4.3.1)
- CWA 14167-2 (Bkz. Bölüm 4.3.2)
- CWA 14169 (Bkz. Bölüm 4.3.3)

olarak sıralanmaktadır. Bunun yanı sıra, sertifikasyon hizmetlerine, imzalama/doğrulama işlemlerine, güvenli imza oluşturma araçlarına ve güvenli imza doğrulamaya ilişkin kullanılabilecek standartlar Şekil 5.1'de verilmiştir.



Şekil 5.1 Standart Rehberi

5.1.1 Almanya

Almanya'da elektronik imzaya ilişkin çalışmalar 99/93/EC sayılı AB Direktifi öncesinde, 1997 yılında başlamıştır. Konuya ilişkin olarak 1 Ağustos 1997 tarihinde Sayısal İmza Kanunu, aynı yılın Kasım ayında da Elektronik İmza Yönetmeliği yürürlüğe girmiştir. Ancak; AB Direktifi yayınlandıktan sonra, bu direktife uyum çerçevesinde yeniden hazırlanan Elektronik İmza Kanunu 22 Mayıs 2001'de [82], Yönetmelik ise 22 Kasım 2001'de [83] yürürlüğe girmiştir. [84 85]

Alman İmza Kanunu ve yönetmeliği, 99/93/EC sayılı AB Direktifi çerçevesinde hazırlandığından, güvenlikle ilgili benzer koşulları içermektedir. Bu koşullar; sertifika hizmet sağlayıcılar, güvenli imza oluşturma araçları, güvenli imza doğrulama ve elektronik imza güvenliği çerçevesindedir.

Kanunda, sertifika hizmet sağlayıcıların güvenliğine ilişkin olarak 4üncü maddenin (Genel Gereklilikler) ikinci fıkrası, 5inci maddenin (Nitelikli Sertifikaların Düzenlenmesi) dördüncü ve beşinci fıkraları, 15inci madde (İhtiyari Akreditasyon) ve 17nci maddenin (Elektronik İmza Ürünleri) üçüncü ve dördüncü fıkraları yer almaktadır. Yönetmelik'te ise yukarıda yer alan konulara ilişkin teknik detaylara değinilmiştir. Özellikle sertifika hizmet sağlayıcıların istihdam edecekleri personel, kullanacakları sistem ve cihazlar ile verecekleri hizmetlerin güvenliğine ilişkin detaylı hükümler ilgili yönetmelikte ve ekinde yer almaktadır. ESHS'ye ilişkin güvenlik hususlarının içeriği yönetmeliğin 2nci maddesinde tanımlanmaktadır. Bu kapsamda:

- Gerekli tüm teknik, yapısal ve organizasyonel güvenlik önlemlerinin tanımı ve bunların uygunlukları,
- Elektronik İmza Kanununun 17nci maddenin dördüncü fıkrasının ikinci bendine göre üretici beyanlarına ya da 17nci maddenin dördüncü fıkrasının birinci bendine ya da 15inci maddenin yedinci fıkrasının birinci bendine göre sertifikasyonlara uygun olarak nitelikli elektronik imza için kullanılan ürünlerin bir listesi,
- Kuruluş ve faaliyetler ile sertifikasyon hizmetlerinin organizasyonunun genel durumu,
- Özellikle aciliyet arz eden durumlarda faaliyetleri güvence altına almak ve devam ettirmek için alınan önlem ve tedbirler,
- Personelin güvenilirliğini değerlendirme ve güvence altına almaya ilişkin usul ve esaslar,
- Geriye kalan güvenlik risklerinin ölçülmesi ve değerlendirilmesi

bulunmaktadır. Bunlara ilave olarak, Ek-1'de yayınlanan değerlendirme seviyesi gereklilikleri ile kullanılacak cihaz ve sistemlere ilişkin olarak kriterler getirilmektedir. Ayrıca sertifika hizmet sağlayıcıların kullanacakları sistem ve cihazlara ilişkin olarak AB tarafından kabul edilen ve AB Resmi Gazetesi'nde yayınlanan standartlar (Bkz. Bölüm 5.1) da geçerli sayılmaktadır.

Elektronik imza oluşturma araçlarına yönelik yapılan düzenlemeler ise Kanunun 5inci maddesinin (Nitelikli Sertifikaların Düzenlenmesi) altıncı fıkrası ile 17nci maddenin (Elektronik İmza Ürünleri) birinci ve dördüncü fıkralarında yer almaktadır. Burada getirilen yükümlülükler, AB Direktifi'nde yer alan güvenli imza oluşturma araçları ile ilgili gereklerle paralellik göstermektedir. Ayrıca İmza Yönetmeliği Ek-1'de de güvenli imza oluşturma araçlarına ilişkin teknik kriterler belirlenmiştir. Bu kriterlere uyan cihazlar Resmi Gazete'de ve RegTP'nin internet sayfalarından yayınlanmak suretiyle kullanıcılara duyurulmaktadır.

Elektronik imzalamada kullanılacak algoritma ve parametrelere ilişkin düzenlemeler Yönetmelik Ek-1, 2nci maddede yer almaktadır. Buna göre kullanılacak imzalama ve özetleme algoritmalarına, bunlara ilişkin parametrelere ve geçerlilik sürelerine ilişkin kriterler Resmi Gazete'de yayınlanmak sureti ile kamuoyuna duyurulacaktır. Buna göre, Ocak 2004 tarihinde yayınlanan bildiri [86] ile belirlenen algoritmalara ilişkin teknik kriterler Çizelge 5.1'de verilmiştir.

	2006 Sonu	**2007 Sonu**	**2008 Sonu**	**2009 Sonu**
RSA (n, bit)	-	1024 (minimum) 2048 (önerilen)	1280 (minimum) 2048 (önerilen)	1563 (minimum) 2048 (önerilen)
DSA (p/q, bit)	-	1024/160 (minimum) 2048/160 (önerilen)	1280/160 (minimum) 2048/160 (önerilen)	1563/160 (minimum) 2048/160 (önerilen)
ECDSA - $E(F_p)$ (p/q, bit)	- /160	-	-	192/180
ECDSA - $E(F_{2^m})$ (m/q, bit)	- /160	-	-	191/180

Çizelge 5.1 Almanya'da Kabul Edilen Teknik Kriterler

Ayrıca bu bildiri içerisinde özet fonksiyonları için, kısa dönemli kullanımda SHA-1 ve RIPEMD-160, uzun dönemli kullanımda ise SHA-256, SHA-384 ve SHA-512 güvenli kabul edilmektedir. [86]

5.1.2 Avusturya

Avusturya Elektronik İmza Kanunu [87], 19 Ağustos 1999 tarihinde; Elektronik İmza Yönetmeliği [88] ise 2 Şubat 2000 tarihinde Avusturya Resmi Gazetesi'nde yayınlanarak yürürlüğe girmiştir.

Kanunda, sertifika hizmet sağlayıcıların güvenliği ile ilgili olarak gereken şartlar 6ncı ve 7nci maddelerde; Yönetmelik'te ise 6ncı madde ve 9uncu maddelerde sayılmıştır. Bu maddeler; sertifika hizmet sağlayıcının güvenliğini sağlaması ve bunun gösterilmesi, yeterli sayıda ve bilgi birikimine sahip personel istihdam edilmesi, güvenilir sistemler kullanılması, teknik bileşenlerin ISO 15408 veya ITSEC'e göre değerlendirilmesi, hizmetlerin BS 7799-2 kapsamında değerlendirilebilmesi ve imza oluşturma verisinin korunması gibi hususları içermektedir. Bu değerlendirmeler için yapılan testlerin sonuçları denetim kurumuna sunulmak zorundadır.

Bunların yanı sıra, Kanun Bölüm 4'te ve Yönetmelik 18inci maddede, sertifika hizmet sağlayıcıların denetimi ve ihtiyari akreditasyona ilişkin hükümler bulunmaktadır. Bu hükümler çerçevesinde sertifika hizmet sağlayıcısının sunduğu hizmetlere veya güvenliğine ilişkin değişiklikleri denetleyici kuruma bildirmek zorundadır. Denetleyici kurum ise en az iki yılda bir defa sertifika hizmet sağlayıcıları denetlemeli ve aşağıda yer alan kontrolleri gerçekleştirmelidir:

- Güvenlikle ilgili bilgilerin ve sertifika ilkelerinin kontrolü,
- Güvenli elektronik imzaya ilişkin uygun teknik bileşenlerin ve prosedürlerin kullanımının izlenmesi ve

- Sertifika hizmet sağlayıcıların akredite edilmesi.

İmza oluşturma araçlarına ve yöntemlerine ilişkin kriterler, kanunun 18inci maddesinde ve yönetmeliğin 7nci maddesinde belirlenmiştir. Bu maddelere göre, imza oluşturma işleminde kullanılacak bileşenler ve yöntemlerin; sahteciliğe, çalınmaya ve değiştirilmeye karşı yeterli güveni sağlaması ve yetkili onay kuruluşları tarafından sertifikalandırılması gerekmektedir. ITSEC'e göre yapılan değerlendirmelerde imza oluşturma verisinin üretimi ve saklanması ile güvenli imza oluşturulmasına ilişkin olarak sağlanması gereken güvence seviyesi E3 olarak belirlenmiştir.

Güvenli imza doğrulamaya ilişkin hususlar, kanunun 18inci maddesinin dördüncü fıkrasında açıklanmaktadır. Bu madde uyarınca doğrulama işleminin güvenli olabilmesi için:

- İmzalanan verilerin değiştirilmediğinden,
- İmzanın güvenilir olarak doğrulandığından ve doğrulama sonucunun yanlışsız olarak gösterildiğinden,
- Elektronik imzanın hangi verilere dayandığının doğrulama yapan kişi tarafından tespit edilebildiğinden,
- Elektronik imzanın kime ait olduğunun ve takma ad kullanılıp kullanılmadığının doğrulayan kişi tarafından tespit edilebildiğinden ve
- İmzalanan verinin, güvenlikle ilgili değişikliğe uğraması durumunda bunun tespit edilebildiğinden

emin olunması gerekmektedir. Bunların yanı sıra, yönetmeliğin 9uncu maddesinde, gereken durumlarda güvenli imza doğrulama için sağlanacak güvence seviyesinin E3 olması gerektiği belirtilmiştir.
Güvenli elektronik imzaya ilişkin teknik bileşenlere ve prosedürlere ilişkin parametreler Yönetmelik Ek-1'de yer almaktadır. Buna göre imza oluşturma verileri için anahtar uzunluklarının en az:

- RSA: 1023 bit
- DSA: 1023 bit
- ECDSA çeşitleri: 160 bit

olması gerekmektedir. Ayrıca; Ek-1 ve 3üncü maddenin beşinci fıkrasında, bu anahtarların gerçek rastgele sayılardan oluşması yani yüksek kaliteli rastgele prosedürlerden oluşturulması şartı getirilmektedir. Fakat, yönetmeliğin 5inci maddesinin ikinci fıkrası uyarınca doldurma yöntemlerinde sahte rastlantısal sayılardan yararlanılabilir. Verilen bu kriterler 31.12.2005 tarihine kadar geçerlidir.

Kullanılabilecek özetleme algoritmaları ise yönetmelik Ek 2'de belirlenmiştir. Buna göre:

- SHA-1
- RIPEMD-160

özetleme fonksiyonları, 31.12.2005 tarihine kadar güvenli kabul edilmektedir.

5.1.3 Bulgaristan

Elektronik Belge ve Elektronik İmzaya İlişkin Kanun [89], 2001 yılında kabul edilerek elektronik belgeler ve elektronik imzaya ilişkin düzenlemeler yapılmış, sertifikasyon hizmetlerinin sunulmasına yönelik şartlar ve yöntemler belirlenmiştir. Kanunun yayınlanması sonrası, 8 Şubat 2002 tarihinde üç farklı yönetmelik yürürlüğe girmiştir. Bunlar:

1. Sertifika Hizmet Sağlayıcılarının İşleyişine, Faaliyetin Sona Ermesine İlişkin Şart ve Yöntemler ile Sertifika Hizmetlerinin Sunulması için Gerekliliklere ilişkin Yönetmelik [90],

2. Sertifika Hizmet Sağlayıcıların Kaydına İlişkin Yönetmelik [91] ve
3. Gelişmiş Elektronik İmzalarda Kullanılacak Algoritmalara İlişkin Yönetmelik [92]

olarak sıralanmaktadır.

Sertifika hizmet sağlayıcılarına ilişkin güvenlik gerekleri, Elektronik Belge ve Elektronik İmza Kanunu 21inci maddenin birinci fıkrasında ana hatlarıyla belirlenmiştir. Bu gerekler arasında; teknik ve kriptografik güvenliğin sağlanmasında güvenilir ekipman ve teknolojiler kullanmak, yeterli uzmanlık bilgisine sahip personel istihdam etmek ve sertifikaların taklit edilmesine karşı gerekli önlemleri almak gibi hususlar bulunmaktadır. Sertifika Hizmet Sağlayıcıların İşleyişine, Faaliyetin Sona Ermesine İlişkin Şart ve Yöntemler ile Sertifika Hizmetlerinin Sunulması için Gerekliliklere ilişkin Yönetmelik'te ise yukarıda sayılan hususlar detaylı bir şekilde verilmektedir. Bu yönetmelikte geçen ilgili maddeler aşağıda yer almaktadır:

- 7nci madde ile güvenlikle ilgili standartlar çerçevesinde uluslararası standartlara uygunluk sağlama zorunluluğu getirilmektedir,
- 9uncu maddenin birinci fıkrası ile sertifika hizmet sağlayıcıların imza oluşturma araçlarının fiziksel olarak korunması gerekliliği belirtilmektedir,
- 22nci ve 23üncü maddeler kapsamında istihdam edilecek personele ilişkin şartlar ortaya konulmaktadır,
- 24üncü madde ile tüm sertifika hizmet sağlayıcıların kullandıkları altyapının güvenlik yönetimine ilişkin olarak gerekli tedbirleri alması gerektiği belirtilmektedir,
- 25inci madde altında; teknik ekipman ve teknolojilere ilişkin gereklilikler sayılmakta, kullanılacak sistemlerin ISO 15408'e göre değerlendirilmesi ve bu değerlendirmenin üç yılda bir yenilenmesi gerektiği belirtilmektedir.

- 26ncı madde kapsamında, sertifika hizmet sağlayıcı tarafından kullanılacak güvenli imza oluşturma araçlarının, ISO 15408'e göre en az EAL3 veya diğer değerlendirme kriterlerine göre benzer güvenlik seviyesinde olması zorunluluğu getirilmektedir.
- 28inci maddede, sertifika hizmet sağlayıcılar tarafından kullanılacak teknik ekipmanların işlevlerine ilişkin asgari kriterler verilmektedir,
- 34üncü maddede bilgi teknolojileriyle ilgili olarak genel kabul görmüş standartlara uyum yükümlülüğü getirilmekte ve güvenlik prosedürlerinin kapsamı belirlenmektedir.

Güvenli elektronik imza oluşturma araçlarına ilişkin olarak, Elektronik Belge ve Elektronik İmzalara ilişkin Kanunun 17nci maddesinin birinci fıkrasında gerekli düzenlemeler yapılmıştır. Bu düzenlemeler, 99/93/EC sayılı AB Direktifi çerçevesindeki hususları içermektedir. Ayrıca Sertifika Hizmet Sağlayıcıların İşleyişine, Faaliyetin Sona Ermesine İlişkin Şart ve Yöntemler ile Sertifika Hizmetlerinin Sunulması için Gerekliliklere ilişkin Yönetmelik'te yer alan 29uncu madde ile güvenli imza oluşturma araçlarının ISO 15408'e göre en az EAL3 veya diğer değerlendirme kriterlerine göre benzer güvenlik seviyesinde olma şartı getirilmiştir. Gelişmiş Elektronik İmzalarda Kullanılacak Algoritmalara İlişkin Yönetmeliğin 7nci ve 8inci maddelerinde ise imza oluşturma aracının, işlemciye, işletim sistemine ve özel erişim verisine (PIN veya biyometrik) sahip kartlar olması ve bu gerekliliklerin de ETSI ve CEN tarafından çıkarılan standartlara göre test edilmesi gerektiği belirtilmektedir.

İmza doğrulamaya yönelik düzenlemeler, kanunun 17nci maddesinin ikinci fıkrasında belirlenmektedir. Buna göre imza doğrulamada kullanılacak mekanizmanın; açık anahtar kullanılarak özel anahtarın bu açık anahtara karşılık geldiğinin anlaşılmasını ve özel anahtarın kullanıldığı doğrulanarak, doğrulama sonucunun ilgili kişiye sağlandığını garanti etmesi gerekmektedir.

Elektronik imzalamada kullanılacak algoritma ve parametrelerin belirlenmesi amacıyla çıkarılan Gelişmiş Elektronik İmzalarda Kullanılacak Algoritmalara İlişkin Yönetmelik kapsamında; imzalama ve doğrulama algoritmaları, özet fonksiyonları ve rastgele sayılar ile ilgili düzenlemeler yapılmaktadır. Kullanılacak algoritmalar Ek-1'de, parametreler ise Ek-2'de verilmektedir. Ek-1'e göre kullanılabilecek algoritmalar:

- Özet fonksiyonu için
  - SHA-1
  - RIPEMD-160
- İmzalama için ise
  - RSA
  - DSA
  - ECDSA

olarak belirlenmiştir.

Ek-2'de belirlenen parametreler ise:

- Özet fonksiyonu için en az 128 bit
- RSA ve DSA için en az 1024 bit
- ECDSA için en az 160 bit

şeklindedir. Ayrıca, bu algoritma ve parametrelere ilişkin olarak ETSI SR 002 176 (Bkz. Bölüm 4.2.2) raporuna başvurulabileceği de belirtilmiştir.

5.2 Kanada

Kanada, elektronik imzaya ilişkin kanuni düzenlemesini, 2000 yılında çıkartılan "Kişisel Bilgilerin Korunması ve Elektronik Belgeler Kanunu" [93] ile gerçekleştirmiştir. Kanunun ikinci bölümünde elektronik imzaya ilişkin

tanımlara yer verilmiş ve 48inci madde ile genel düzenlemeler yapılmıştır. Detaylı düzenlemeler Hazine Kurulu'nun tavsiyeleri doğrultusunda gerçekleştirilmektedir.

Bu kapsamda, Hazine Kurulu tarafından elektronik imza güvenliğine ilişkin politika dokümanları ve kılavuz dokümanlar hazırlanmıştır. Ayrıca kullanılacak standartlar da belirlenmiştir. Bu politika dokümanları :

- AAA Yönetimi için Politika
- AAA Sayısal İmza Sertifikası İlkeleri
- AAA Gizlilik Sertifikası İlkeleri
- Elektronik Yetkilendirme ve Kimlik Doğrulama Politikası
- Kanada Şifreleme Politikası
- Güvenlik Politikası

olarak sıralanmaktadır.

Yukarıda sayılan politika dokümanlarında sertifika hizmet sağlayıcıların uyması gereken politikalar ve güvenlik için gerekli görülen tedbirler ile kullanılacak standartlara ilişkin detaylı bilgiler yer almakta ve bu politikalar; Hazine Kurulu, İletişim Güvenliği Kurumu, Politika Yönetim Otoritesi tarafından hazırlanıp geliştirilmektedir. Bu politika dokümanı içerisinde sekiz farklı güvenlik seviyesi için ayrı politikalar tanımlanmaktadır. Bunlardan dört tanesi elektronik imzaya, diğer dört tanesi de şifrelemeye yönelik politikalardır ve basit, temel, orta ve yüksek olmak üzere farklı güvence seviyelerine sahiptir. Bu seviyeler artan güvenlik gereklerine göre düzenlenmiştir. [17]

Yayınlanan kılavuz dokümanlar, AAA'ya ilişkin gereklerin karşılanmasında ve hizmetlerin güvenliğinin yeterli seviyede sağlanmasında yol gösterme amaçlıdır. Elektronik imza güvenliğine yönelik yayınlanan kılavuz dokümanlar:

- Sertifika Otoriteleri Bilgi Teknolojileri Güvenliği Model Kılavuz Dokümanı
- Bilgi Yönetimi – AAA Kılavuzu

olarak sıralanmaktadır.

Güvenliğe ilişkin standartlar akıllı kartları ve bu kartların okunmasını ile kriptografik algoritmaları kapsamaktadır. Hazine Kurulu tarafından hazırlanan akıllı kartlara ilişkin doküman [94] içerisinde; uluslararası kabul görmüş standartlara atıf yapılmakta ve bu kartların mimarisine, desteklemesi gereken özelliklere ve güvenliğine ilişkin hususlar ele alınmaktadır.

İmzalamada kullanılacak algoritmalara ve bunların parametrelerine ilişkin standart, İletişim Güvenliği Kurumu tarafından hazırlanmıştır. Bu kapsamda, kullanılabilecek algoritmalar ve parametreler Çizelge 5.2'de verilmiştir. [95]

Algoritma	Güvenlik Seviyesi	Parametre (Bit)
RSA	Normal	$n \geq 1024$
	Yüksek	$n \geq 2048$
DSA	Normal	$q \geq 1024$
	Yüksek	$q \geq 2048$
ECDSA - $E(F_p)$	Normal	$q \geq 192$
	Yüksek	$q \geq 256$
ECDSA - $E(F_{2^m})$	Normal	$m \geq 163$
	Yüksek	$m \geq 283$

Çizelge 5.2 Kanada'da Kullanılan Algoritma ve Parametreler

Ayrıca, özetleme algoritması olarak SHA-1, SHA-256, SHA – 384 ve SHA-512 kullanılabilmektedir. Ancak, SHA-1 algoritması 2008 yılından itibaren yüksek güvenlik seviyesi gerektiren uygulamalar için uygun olmayacaktır.

6 TÜRKİYE'DE ELEKTRONİK İMZA GÜVENLİĞİ

6.1 Giriş

Ülkemizde elektronik imzaya yönelik çalışmalar, 2001 yılında Dış Ticaret Müsteşarlığı bünyesinde kurulan Hukuk Çalışma Grubu tarafından hazırlanan "Elektronik Veri, Elektronik Sözleşme ve Elektronik İmza Kanunu Tasarısı Taslağı" ile başlamıştır. Bu kanun tasarısının 17.04.2004 tarihinde Başbakanlığa gönderilmesi öncesinde, Adalet Bakanlığı tarafından 14.01.2002 tarihinde ikinci bir çalışma ele alınmıştır. Adalet Bakanlığı'nın hazırladığı "Elektronik İmzanın Düzenlenmesi Hakkında Kanun Tasarısı" ise 10.9.2002 tarihinde Başbakanlığa sunulmuştur. [96] Bu taslak, "Elektronik İmza Kanunu" olarak küçük değişikliklerle 23 Ocak 2004 tarih ve 25355 sayılı Resmi Gazete'de yayımlanmıştır. Bu Kanun ile, kanunun yayımından altı ay sonra yürürlüğe girmesi ve yürürlüğe girmesinden sonra altı ay içinde aşağıda yer alan hususlarda Telekomünikasyon Kurumu'nun gerekli düzenlemeleri yapması hükümleri getirilmektedir:

- Güvenli elektronik imza oluşturma araçları (Madde 6),
- Güvenli elektronik imza doğrulama araçları (Madde 7),
- Elektronik sertifika hizmet sağlayıcısı (Madde 8),
- Elektronik sertifika hizmet sağlayıcısının yükümlülükleri (Madde 10),
- Nitelikli elektronik sertifikaların iptal edilmesi (Madde 11),
- Sertifika mali sorumluluk sigortası (Madde 13),
- Yabancı elektronik sertifikalar (Madde 14).

Kurum, Dış Ticaret Müsteşarlığı bünyesinde gerçekleştirilen çalışmalara katılım göstermiş, Adalet Bakanlığı tarafından hazırlanan kanun tasarısında düzenleyici ve denetleyici kurum olarak görevlendirilmesi üzerine "e-imza Koordinasyon Kurulu" oluşturulmuş ve böylece 2003 yılı başında (henüz Kanun çıkmadan) çalışmalara başlamıştır. Elektronik İmza Kanunu'nun Resmi Gazete'de yayımlanması sonrasında, Kurum bünyesinde oluşturulan

"e-İmza Çalışma Grubu" ile çalışmalara hızla başlanmış ve düzenlemelerin geniş katılımlı ve şeffaf bir şekilde yapılabilmesi amacıyla çeşitli kamu kurum ve kuruluşlardan, sivil toplum örgütlerinden, üniversitelerden ve özel sektörden 200'e yakın kişinin katılımıyla "Ulusal Koordinasyon Kurulu" oluşturulmuştur.

Kurum tarafından yürütülen düzenleme çalışmaları çerçevesinde, "Sertifika Mali Sorumluluk Sigortası Yönetmeliği" 26 Ağustos 2004 tarih ve 25565 sayılı, "Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik" ile "Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ" 6 Ocak 2005 tarih ve 25692 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir.

Telekomünikasyon Kurumu'nun girişimleri ve 10 Haziran 2004 tarihli e-Dönüşüm Türkiye İcra Kurulu kararı sonrasında, 6 Eylül 2004 tarih ve 25575 sayılı Resmi Gazete'de yayımlanan 2004/21 sayılı Başbakanlık Genelgesi ile tüm kamu kurum ve kuruluşlarının sertifika ihtiyacının bir merkezden karşılanması için TÜBİTAK-UEKAE görevlendirilmiştir.

Güvenlik ile ilgili yapılan düzenlemeler; elektronik sertifika hizmet sağlayıcısı, güvenli elektronik imza oluşturma ve doğrulama araçları ile elektronik imzaya ilişkin diğer teknik hususları kapsamaktadır.

6.2 ESHS Güvenliği

ESHS güvenliğine ilişkin olarak, Kanunun 8inci maddesi ikinci fıkrasına göre ESHS:

a) Güvenli ürün ve sistemleri kullanmak,
b) Hizmeti güvenilir bir biçimde yürütmek,

c) Sertifikaların taklit ve tahrif edilmesini önlemekle ilgili her türlü tedbiri almak

zorundadır. Yönetmeliğin 19uncu maddesi uyarınca da ESHS'nin güvenli sistem ve cihazlar kullanması, bu sistem ve cihazlar ile bunların bulunduğu bina veya alanı koruması yükümlülüğü getirilmektedir. Bu kapsamda, ESHS'lerin işleyişine yönelik olarak Tebliğ'in 5inci maddesinde:

- ETSI TS 101 456 (Bkz. Bölüm 4.2.1) ve
- CWA 14167-1 (Bkz. Bölüm 4.3.1)

standartlarına uyma hükmü yer almaktadır. Ayrıca Tebliğ'in güvenlik kriterlerini belirleyen 9uncu maddesi ile yukarıda sayılan standartların yanı sıra TS ISO/IEC 17799 standardına (Bkz. Bölüm 4.1.1) uyma zorunluluğu getirilmiştir. ESHS'ler TS ISO/IEC 17799 uyum çerçevesinde BS-7799-2 sertifikası edinmekle yükümlüdür.

Ayrıca, ESHS'ler Kanunun 10uncu maddesi ve Yönetmeliğin 19uncu maddesi kapsamında hizmetin gerektirdiği nitelikte; bilgi güvenliği, elektronik imza teknolojileri ve veri tabanı yönetimi alanlarında yeteri kadar teknik personel istihdam etmek veya ettirmekle yükümlü kılınmıştır. Teknik personel, konusunda yeterli mesleki deneyime sahip ya da ilgili alanlarda eğitim almış ve güvenilir olmalıdır. ESHS organizasyon şemasında istihdam ettiği veya ettirdiği tüm personelinin görev tanımını ve dağılımını belirlemek zorundadır.

ESHS'lerin denetlenmesi görevi; Kanunun 15inci Maddesi ile Telekomünikasyon Kurumu'na verilmiştir ve denetlemeye ilişkin hususlar Yönetmeliğin 7. Bölümü ile düzenlenmiştir. Bu bölüm altında; ESHS'lerin mevzuata ve teknik hususlara uyumuna yönelik denetiminin, gerekli görülen zamanlarda veya iki yılda bir resen yapılması hükme bağlanmıştır.

6.3 Güvenli Elektronik İmza Oluşturma Aracı

Güvenli elektronik imza oluşturma araçlarında yer alması gereken özellikler Kanunun 6ncı maddesi kapsamında tanımlanmıştır. Buna göre GEİOA'ların

a) Ürettiği elektronik imza oluşturma verilerinin kendi aralarında bir eşi daha bulunmamasını,
b) Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin araç dışına hiçbir biçimde çıkarılamamasını ve gizliliğini,
c) Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin, üçüncü kişilerce elde edilememesini, kullanılamamasını ve elektronik imzanın sahteciliğe karşı korunmasını,
d) İmzalanacak verinin imza sahibi dışında değiştirilememesini ve bu verinin imza sahibi tarafından imzanın oluşturulmasından önce görülebilmesini

sağlaması gerekmektedir. Yukarıda sayılan özellikler çerçevesinde, Tebliğin 8inci maddesinde GEİOA'ları 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 olması zorunluluğu vardır.

ESHS'lerin kullanacakları güvenli elektronik imza oluşturma araçlarına ilişkin kriterler Tebliğin 11inci maddesi ile belirlenmiştir. Buna göre kullanılacak cihazların:

- FIPS PUB 140-1 veya FIPS PUB 140-2'ye göre seviye 3 veya üzerinde olduğunun veya
- CWA 14167-2'de belirtilen kriterlere uygunluğunun veya
- 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 olduğunun

yetkili kurum ve kuruluşlardan alınan belgelerle ispat edilmesi gerekmektedir.

6.4 Güvenli Elektronik İmza Doğrulama Aracı

Elektronik İmza Kanununun 7nci maddesinde güvenli elektronik imza doğrulama araçlarında bulunması gereken özellikler sıralanmaktadır. Bu maddeye göre GEİDA:

a) İmzanın doğrulanması için kullanılan verileri, değiştirmeksizin doğrulama yapan kişiye gösteren,
b) İmza doğrulama işlemini güvenilir ve kesin bir biçimde çalıştıran ve doğrulama sonuçlarını değiştirmeksizin doğrulama yapan kişiye gösteren,
c) Gerektiğinde, imzalanmış verinin güvenilir bir biçimde gösterilmesini sağlayan,
d) İmzanın doğrulanması için kullanılan elektronik sertifikanın doğruluğunu ve geçerliliğini güvenilir bir biçimde tespit ederek sonuçlarını değiştirmeksizin doğrulama yapan kişiye gösteren,
e) İmza sahibinin kimliğini değiştirmeksizin doğrulama yapan kişiye gösteren ve
f) İmzanın doğrulanması ile ilgili şartlara etki edecek değişikliklerin tespit edilebilmesini sağlayan

araçlardır. ESHS'ler kullanıcılara sağlayacakları güvenli elektronik imza doğrulama araçları için CWA 14171 standardına uymak ve bunu yazılı olarak taahhüt etmek zorundadır.

6.5 Algoritma ve Parametreler

Elektronik imzalama ve doğrulama ile özetleme için kullanılacak algoritmalar ve bu algoritmalara ilişkin parametreler Tebliğ'in 6. Maddesi kapsamında belirlenmektedir. Bu madde uyarınca ESHS'nin imza oluşturma ve doğrulama verileri:

- RSA için en az 2048 bit veya
- DSA için en az 2048 bit veya
- DSA Eliptik Eğrisi için en az 256 bit

olmalıdır. Bunun yanında, Yönetmeliğin 18inci maddesi uyarınca ESHS'ye ait imza oluşturma ve doğrulama verilerinin geçerlilik süresi on yılı aşamaz.

İmza sahibinin kullanacakları algoritma ve parametrelerin ise:

- RSA için en az 1024 bit veya
- DSA için en az 1024 bit veya
- DSA Eliptik Eğrisi için en az 160 bit

olması gerekmektedir. Özetleme algoritması olarak da; RIPEMD-160 veya SHA-1 güvenli kabul edilmektedir.

Yukarıda yer alan algoritma ve parametreler 31.12.2005 tarihine kadar geçerlidir. Ayrıca, bu algoritma ve parametrelere bağlı kalmak şartı ile ETSI SR 002 176 raporu da (Bkz. Bölüm 4.2.2) referans olarak alınabilir.

6.6 Düzenleme Yaklaşımı

5070 sayılı Elektronik İmza Kanunu, 99/93/EC sayılı AB Direktifi'ne uyumlu olarak hazırlanmıştır. Bu çerçevede, elektronik imza güvenliğine ilişkin hususlar AB Direktifi ile Almanya ve Avusturya mevzuatına paralellik göstermektedir.

Elektronik imzaya ilişkin düzenlemeler henüz oluşmamış bir pazar üzerinde gerçekleştirildiğinden; pazara girişin engellenmemesi, rekabet ortamının tesis edilmesi ve kullanıcı haklarının korunması oldukça önemlidir. Ancak, sayılan

bu hususların hayata geçirilmesinde hassas dengeler söz konusudur. Sertifikasyon hizmetlerinin sunumu, güven mekanizması üzerine kurulu olduğundan, ESHS olmak isteyen gerçek veya özel hukuk tüzel kişilerin belirli teknik ve hukuki şartları sağlaması gerekmektedir. Bu açıdan bakıldığında, bazı ülkelerde tercih edilen; çok sayıda küçük ESHS'ler yerine az sayıda ve büyük ESHS'lerin piyasada bulunması yaklaşımı göz önünde bulundurulabilir. [97]

Ayrıca, elektronik imzaya ilişkin yapılan düzenlemeler esnek bir yapıda olmalıdır. Bu perspektiften bakıldığında, hem 99/93/EC sayılı AB Direktifi hem de 5070 sayılı Elektronik İmza Kanunu teknoloji nötr bir yaklaşımla genel bir çerçeve ortaya koymaktadır. Halihazırda yürürlükte olan ikincil düzenlemeler, uygulamada ortaya çıkabilecek aksaklıkları giderecek şekilde gözden geçirilmelidir. Büyük bir hızla değişen bilişim teknolojileri ve farklılaşan güvenlik gerekleri sürekli olarak takip edilmeli ve gerekli önlemler alınmalıdır. Bu süreç, elektronik imza teknolojilerinin doğası gereği gayet normal karşılanmalıdır. Örneğin Almanya'da elektronik imzaya ilişkin ilk kanun 1997 tarihinde hazırlanıp 1998'de yürürlüğe girmiş; kazanılan üç senelik tecrübe ve AB Direktifi ilkelerine uyum çerçevesinde 2001 yılında değiştirilmiştir. [98]

Ancak bu yaklaşım, hayata geçirilecek uygulamalar ve faaliyette bulunacak ESHS'ler için belirsizlikler içermemelidir. Düzenlemeler, uyulacak kuralları ve uygulanacak esasları tam olarak belirlemeli; teknolojik gelişmeler paralelinde, pazar şartları göz önünde bulundurularak ve ilgili tarafların fayda sağlayabileceği şekilde gözden geçirilerek gerekli değişiklikler hayata geçirilmelidir.

Avrupa Birliği Direktifi içerisinde yer alıp 5070 sayılı Elektronik İmza Kanununda kapsanmayan en önemli husus akreditasyon mekanizması olarak göze çarpmaktadır. İhtiyari akreditasyon, sertifika hizmet sağlayıcısının talebi üzerine, yetkili kuruluşlar tarafından gerçekleştirilen,

sertifikasyon hizmetlerinin sunumuna ilişkin hak ve yükümlülüklere uyumun detaylı olarak denetlenmesini içermektedir. Akreditasyon kuruluşlarının, bir akreditasyon planı oluşturması ve buna ilişkin işlemleri detaylı bir şekilde ortaya koyması gerekmektedir. Ayrıca, yapılacak denetimler için yeterli sayıda teknik ve idari personel barındırarak akreditasyonun doğru bir biçimde, belirli standartlar çerçevesinde yürütülmesini sağlamalıdır. İhtiyari akreditasyon yaklaşımı, düzenleyici kurumların denetim faaliyetlerinin daha kolay bir şekilde gerçekleştirilebilmesinin yanında güvenliğin ve güvenilirliğin çok önemli olduğu sertifikasyon hizmetlerinin sağlanmasında kullanıcı tercihlerini de etkilemektedir. AB düzenlemeleri kapsamında, akredite edilmiş bir sertifika hizmet sağlayıcısının diğer üye ülkelerde sertifika hizmeti vermesi çok daha kolaydır. Tüm bunların yanında akreditasyon, çapraz sertifikasyon sürecinde önemli avantajlar sağlamaktadır. Ancak, ihtiyari akreditasyon 5070 sayılı kanun kapsamına alınmadığından ötürü, ESHS'lerin denetiminde Kuruma büyük görevler düşmektedir.

Avrupa Birliği üyesi ülkeler, yetkilendirme mekanizmasına yakın bir şekilde işleyen denetleme ve inceleme planları oluşturmuşlardır. Ancak oluşturulan bu planlar henüz çok yeni olduğundan bunlar arasında bir karşılaştırma yapmak oldukça zordur. Çünkü bu planların getirdiği avantaj ve dezavantajlar tam anlamıyla belirlenememiştir. Almanya ve Avusturya gibi bazı ülkelerde katı düzenlemeler uygulanırken; İngiltere ve İrlanda'da daha serbest bir yapı mevcuttur. Ülkemizde uygulanan inceleme ve denetleme prosedürlerinde 99/93/EC sayılı AB Direktifi'nden biraz farklı bir yöntem izlenmiştir. ESHS olmak isteyenler, yapacakları bildirimden iki ay sonra faaliyete geçebilmektedir. Verilen iki aylık sürede Kurum gerekli incelemeleri yaparak herhangi bir uyumsuzluk veya eksiklik olup olmadığını kontrol etmekle yükümlüdür. Hem ESHS'lerin bildirimde bulunmalarını takiben yapılacak incelemeler hem de daha sonra yapılacak denetimler elektronik sertifika pazarının gelişimine ve elektronik imzanın kullanımına doğrudan etki edecektir. ESHS'lerden herhangi birisinde ortaya çıkan ve denetim veya incelemelerde tespit edilemeyen güvenlik açıkları kullanıcıların güvenini

sarsacak ve Kurumun itibar kaybetmesine sebep olacaktır. Bu açıdan bakıldığında, denetime ilişkin her safhanın titizlikle ele alınması gerektiği düşünülmektedir.

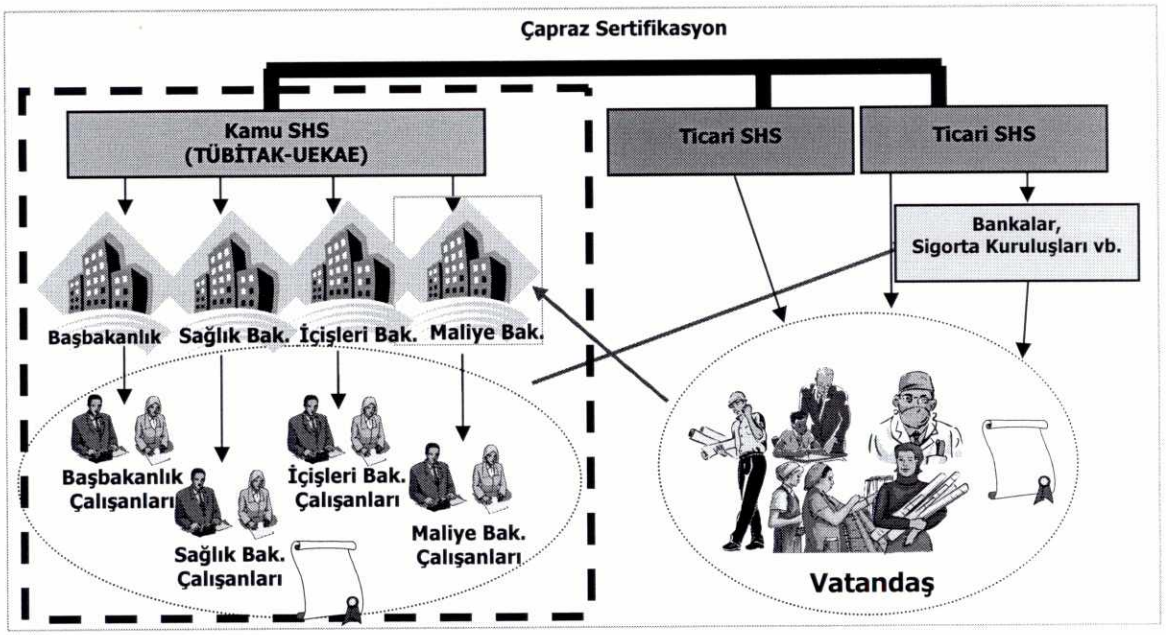
Elektronik imzaya ilişkin olarak verilecek hizmetlerin güvenli bir şekilde sunulabilmesini ve düzenlemelerde yer alan hükümler ile uygulanması zorunlu tutulan standartlara uyulmasını teminen; ESHS'lerin, alması gereken önlemlere ve yapılacak denetimlere ilişkin olarak bilgilendirilmesi ve bilinçlendirilmesi yerinde olacaktır. Tüm bunların yerine getirilebilmesi amacıyla, Bölüm 5.2'de yer alan Kanada örneğinde olduğu üzere Kurum tarafından benzer kılavuzların hazırlanmasında fayda görülmektedir.

5070 sayılı Elektronik İmza Kanununun 21inci maddesi ile kamu kurum ve kuruluşları denetim, cezai hükümler ve ücret düzenlemelerinden muaf tutulmuştur. Bu durum, her bir kamu kurum ve kuruluşunun hemen hiçbir düzenlemeye tabi olmadan ESHS olabilmesine olanak tanımaktadır. Ancak böyle bir yapının; güvenlik, birlikte çalışabilirlik ve standartlaşma ile ilgili olarak birçok problem doğurması kaçınılmaz görünmektedir. Bu tür sorunlarla karşılaşılmasını önlemek amacıyla, Telekomünikasyon Kurumu'nun girişimleri ve 10 Haziran 2004 tarihli e-Dönüşüm Türkiye İcra Kurulu kararı sonrasında, 6 Eylül 2004 tarih ve 2004/21 sayılı Başbakanlık Genelgesi ile tüm kamu kurum ve kuruluşlarının sertifika ihtiyacının bir merkezden karşılanması için TÜBİTAK-UEKAE (Türkiye Bilimsel ve Teknik Araştırma Kurumu – Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü) görevlendirilmiş ve söz konusu yapının gözden geçirilmesi ile uygunluğunun izlenmesi görev ve sorumluluğu Telekomünikasyon Kurumu'na verilmiştir. Bu karar ile:

- Kamu kurum ve kuruluşları tarafından kullanılacak elektronik imza altyapısının daha güvenli olması,
- Bilgi güvenliğinin üst seviyede sağlanması,
- Kurulacak yapının Kurum tarafından gözden geçirilmesi ve izlenmesi,

- Kamu kurum ve kuruluşları arası güven bunalımlarının yaşanmaması,
- Kamu kurum ve kuruluşları arasında birlikte çalışabilirliğin sağlanması,
- Tek elektronik sertifikayla birden çok işlem yapılabilmesi,
- Mükerrer yatırımların önlenmesi,
- Rekabet ortamının korunması

gibi birçok fayda sağlanabilecektir. Hayata geçirilmesi planlanan altyapı Şekil 6.1'de verilmektedir.



Şekil 6.1 Türkiye Elektronik İmza Altyapısı

Kurulması çalışmaları başlamış olan bu yapıda, Telekomünikasyon Kurumu yalnızca düzenleme ve denetleme faaliyetleri gerçekleştirecektir. Kurum, bazı ülkelerde yetkili makamlar tarafından üstlenilen kök sertifika hizmet sağlayıcılığı mekanizmasını hayata geçirmemiştir. Türkiye modelinde yalnızca kamu kurum ve kuruluşları için bir kök sertifika hizmet sağlayıcısı belirlenmiştir ve bu görev TÜBİTAK-UEKAE'ye verilmiştir.

Bazı yaklaşımlarda, Telekomünikasyon Kurumu'nun tüm yapı için kök ESHS olması gerekliliği üzerine fikirler ortaya konulmuştur. Özellikle, güven

zincirinin en üstünde Kurumun yer alması gerektiği ve bu sayede yetkili bir sertifika hizmet sağlayıcısı gibi hareket edebilecek sahtecilerin önüne geçilebileceği vurgulanmıştır. Bu yaklaşımda doğruluk payı olduğu inkar edilemez. Ancak, kök ESHS olma kararının verilmesi öncesinde elde edilecek avantajlar ve ortaya çıkacak dezavantajlar detaylı bir biçimde değerlendirilmeli ve uygulanacak strateji belirlenmelidir. Kuruma bildirimde bulunmuş ve faaliyete geçmiş bir ESHS'nin ismini kullanarak gerçek olmayan sertifikalar üretecek sahtecilerin, Kurumun adını kullanarak sahte sertifika üretmeleri de zor olmayacaktır. Fakat, Kurumun kök ESHS olması durumunda, kök sertifika hizmet sağlayıcısının sertifikasını doğru ve güvenilir bir şekilde elde eden kullanıcıların hangi ESHS'lerin Kuruma bildirimde bulunmuş olduğunu anlamaları kolaylaşacaktır. Kurumun böyle bir yapı oluşturmaya karar vermesi durumunda, gerekli yatırımları yapması, yeterli istihdamı sağlaması ve en önemlisi özel anahtarını son derece sıkı bir şekilde koruması gerekecektir. Çünkü, Kurumun özel anahtarının güvenilirliğinin kaybolması, ülkemizde bulunan tüm ESHS'lerin ve bu ESHS'ler tarafından dağıtılan sertifikaların geçerliliğini yitirmesi anlamına gelmektedir.

Yukarıda yer alan hususların ivedilikle ve doğru bir şekilde gerçekleştirilmesi adına, Kurumun ITU, CEN ve ETSI bünyesinde yapılan elektronik imzaya ilişkin standart ve tavsiye kararı hazırlanması çalışmalarını yakından takip etmesi ve bu çalışmalara katılım sağlaması oldukça önemlidir. Bunun yanısıra, geliştirilen standartların ve diğer dokümanların Türk Standardı haline getirilmesi için TSE ile koordinasyon sağlanmalıdır. Ayrıca, Kurumun da üyesi olduğu FESA (Forum of European Supervisory Authorities for Electronic Signatures – Elektronik İmzalar için Avrupa Denetleme Kurumları Forumu) tarafından yapılan çalışmalar, düzenleyici kurumların karşılaşabilecekleri problemleri doğrudan adreslemesi ve çözüm yöntemlerinin tartışmalar sonucunda ortaya konulması sebebiyle mutlaka takip edilmelidir.

Kullanıcıların, hem elektronik imza kullanımı ile ilgili hem de edinilecek sistem ve cihazlar ile ilgili bilgilendirilmesinde Kurumun da etkin bir rolü olması gerekmektedir. 5070 sayılı Kanun ile getirilen "Güvenli elektronik imza, elle atılan imza ile aynı hukukî sonucu doğurur." hükmü uyarınca, elektronik imza ile yapılan işlemler kullanıcının sorumluluğundadır. Yanlış kullanım veya yönlendirmeler sonucunda, istenmeyen durumlar ortaya çıkabilir. Bu risklerin en aza indirilmesi için kamuoyunun bilgilendirilmesi ve bilinçlendirilmesi gerekmektedir.

Elektronik imza ile ilgili olarak karşılaşılan diğer bir önemli husus olarak kişisel bilgilerin korunmasına ve bilgi güvenliğine ilişkin düzenlemelerdir. Elektronik İmza Kanununun 12nci maddesi kapsamında ele alınan bu hususlar, çıkarılan yönetmelik ve tebliğ ile de detaylı olarak düzenlenmiştir. Tebliğ kapsamında ESHS'lerin edinmesi gereken belgeler arasında bulunan BS 7799-2 sertifikası bilgi güvenliğinin sağlanması için oldukça önemli bir kriter olarak göze çarpmaktadır. Ancak yapılan bu düzenlemelerin, hazırlanma çalışmaları halen devam etmekte olan kişisel bilgilerin korunmasına ilişkin kanun taslağının ivedilikle tamamlanıp yasalaşması ile desteklenmesi uygun olacaktır.

7 SONUÇ

Elektronik imza kullanımı, beklenildiği kadar hızlı olmasa da, gittikçe artmaktadır. Bu sürecin yavaş ilerlemesi birçok faktöre bağlıdır. Bu faktörler arasında standartlaşma, birlikte çalışabilirlik ve güvenlik hususlarında yaşanan sıkıntılar oldukça önemli bir yer tutmaktadır. Bütünlük, inkar edememe ve kimlik doğrulama işlevleri ile elektronik ortamda güvenli işlem yapabilmeyi sağlayan elektronik imzanın güvenilirliği detaylı olarak sorgulanmaktadır. Geliştirilen birçok elektronik imza projesi, neredeyse gün yüzüne çıkamadan kırılmış ve bunların güvensiz olduğu ispatlanmıştır.

Bölüm 3'te detaylı olarak açıklanan elektronik imzaya ilişkin güvenlik kriterleri ve elektronik imzanın güvenilirliğini etkileyen faktörler, üzerinde çalışılmakta olan konular arasındadır. Burada karşımıza çıkan gerçeklerden birisi hiçbir yöntemin mutlak olarak güvenilir olmadığıdır. Zor matematik problemleri üzerine kurulmuş elektronik imza yaklaşımları, yeteri kadar işlem gücüne sahip olunamaması nedeniyle kırılamaz olarak kabul edilmektedir. Ancak, sayılan bu nedenler elektronik imzanın güvensiz olduğu anlamına da gelmemektedir. Bu tez kapsamında belirtilen hususlara ve düzenlemelerde yer alan şartlara ve standartlara uyum ile güvenilirlik problemleri yaşanması olasılığı son derece düşüktür.

Teknolojinin desteklediği bu güvenlik mekanizmasının tek başına yeteri kadar geçerlilik sağlayamaması nedeniyle hukuki düzenlemelere ihtiyaç duyulmuştur. Yapılan düzenlemeler zamanla değiştirilmiş ve geliştirilmiş böylece çok yeni olan bir uygulama alanında adım adım ilerleme sağlanmıştır. Hukuki olarak geçerliliğin sağlanması günlük hayatta birçok yeni imkan doğmasına vesile olmuştur. Bu sayede, 5070 sayılı kanunun 5inci maddesinde yer alan "Kanunların resmi şekle veya özel bir merasime tabi tuttuğu hukuki işlemler ile teminat sözleşmeleri güvenli elektronik imza ile

gerçekleştirilemez." hükmüne uygun olmak şartıyla her türlü işlem güvenli elektronik imza kullanılarak gerçekleştirilebilir.

Kullanılan sistem ve cihazlar, kurulan altyapılar, sertifika sahipleri veya diğer taraflar güvenliğe etki edebilecek risklere maruz kalmaktadır. Bu yüzden, yapılacak yatırımlarda ve düzenlemelerde oldukça titiz davranmak gerekmektedir. Bu aşamada, 5070 sayılı Elektronik İmza Kanunu ile düzenleme ve denetleme görevini üstlenen Telekomünikasyon Kurumu'nun atacağı adımlar ve alacağı tedbirler sektörün geleceğine yön verecektir. Sürekli yaşanan ilerleme ve değişme süreci içerisinde; gelişen teknolojilerin, kriptoanalitik yöntemlerin ve farklı tehditlerin yakından izlenerek gerekli değişikliklerin ivedilikle gerçekleştirilmesi hayati önem taşımaktadır. Elektronik imzanın gelişimi ve bu konuda yapılan düzenlemelerin geçmişi çok uzun olmasa da, diğer ülkelerin yaşadığı problemlerden ve bu ülkelerin deneyimlerinden faydalanmak yararlı olacaktır.

5070 sayılı Elektronik İmza Kanununun 23 Ocak 2004 tarihinde Resmi Gazete'de yayımlanması sonrasında yapılan düzenleme çalışmaları yaklaşık bir yıl sonra tamamlanarak yürürlüğe girmiştir. İkincil düzenlemeler kapsamında yer alan Yönetmelik ve Tebliğ içerisinde güvenlikle ilgili olarak birçok hususa yer verilmiştir. Bu düzenlemeler sonrasında ortaya çıkacak uygulamaların güvenlik gereklerinin karşılanmasında aşağıda yer alan hususlar oldukça önem kazanmaktadır:

- Kanun ve Yönetmelik Kapsamında Getirilen Düzenlemelere Uyulması: Yapılan düzenlemeler çerçevesinde; ESHS'lere, imza sahiplerine ve üçüncü kişilere getirilen yükümlülüklere uyulması sağlanmalıdır. Bu hususların yerine getirilmesi için gerekli önlemler alınmalı ve farkındalılık yaratılmalıdır.

- Tebliğ ile Zorunlu Hale Getirilen Standartların Uygulanması: Tebliğ'de yer alan ve ESHS'lerin işleyişine, kullanılacak sistem ve cihazların

güvenliğine ilişkin standartlara uyulması sağlanmalıdır. Böylece hem güvenlikle ilgili gerekli tedbirler alınmış hem de birlikte çalışabilirlik açısından önemli adımlar atılmış olacaktır.

- ESHS Olmak İsteyenlerin Yapacakları Bildirimlerin Detaylı Olarak İncelenmesi: ESHS olmak isteyenlerin başvurularında istenilen bilgi ve belgeler Yönetmelik ekinde belirlenmiştir. Bu bilgi ve belgelerin detaylı bir biçimde incelenerek uygunsuzluk veya eksiklik tespit edilmesi halinde gerekli prosedür uygulanmalıdır. ESHS'lerin güven mekanizması içerisindeki yerinin önemi ve olası güvenlik açıklıkları veya uygunsuzlukların faaliyet öncesi tespiti büyük önem taşımaktadır. Kurum, bildirimlerin incelenmesi sürecine ilişkin olarak gerekli planları yapmalı ve objektif değerlendirme kriterlerini ortaya koymalıdır.

- Denetimlerin Düzenli ve Sistemli Olarak Yapılması: İnceleme prosedürüne benzer biçimde, denetime ilişkin planlar da oluşturulmalıdır. ESHS'lerin denetimi; çıkarılan yönetmelik uyarınca, Kurumun gerek gördüğü hallerde ve iki yılda bir defa resen yapılmaktadır. Bu hükümden de anlaşılacağı üzere Kurum iki yılda en az bir defa denetleme yapmak zorundadır.

- Rehber ve Açıklayıcı Dokümanlar Hazırlanması: Denetleme, inceleme ve tam olarak anlaşılamayan düzenleme hususlarına ilişkin rehberler ve açıklayıcı dokümanlar hazırlanması sektörün gelişimi için oldukça önemli bir husustur. Konuyla ilgili yetkili tek kurum olan Telekomünikasyon Kurumu gerekli tedbirleri almalıdır.

- Güvenli İmza Oluşturma ve Doğrulama Araçları Pazarının İzlenmesi: Kullanılacak olan elektronik imza oluşturma ve doğrulama araçlarının imza sahiplerine ve üçüncü kişilere sağlanmasında pazarın izlenmesi, özellikle ESHS'ler tarafından sağlanacak araçların teknik kriterlere tam

olarak uyumunun garanti altına alınması ve uygun cihazların ESHS'lerin ve Kurumun internet sayfalarında yayınlanması önem arz etmektedir. Böylece, kullanıcıların yanlış tercihlerden dolayı hukuki veya maddi çerçevede zarara uğramalarının önlenmesi gerekmektedir.

- Teknolojik Gelişmelerin Takip Edilerek Önemli Hususların Düzenlemelere Yansıtılması: 5070 sayılı Elektronik İmza Kanunu herhangi bir teknolojiyi işaret etmemektedir. Ancak yapılan düzenlemeler ve uygulanan standartlar, genel olarak açık anahtar altyapılarını işaret etmektedir. Teknolojik gelişmeler çerçevesinde yaşanacak değişimlere ayak uydurulması, güvenilirliği ispatlanmış ve kabul görmüş teknolojilerin kapsamında düzenlemelerin gözden geçirilmesi elektronik sertifika pazarının gelişimine, uygulamaların artmasına ve kullanımda kolaylıklar sağlanmasına yardımcı olacaktır.

- Standart Çalışmaları Yakından İzlenerek Değişikliklerin Düzenlemeler Kapsamına Alınması: Özellikle Avrupa Birliği bünyesinde gerçekleştirilen çalışmalar, standartlarda yapılan güncellemeler ile düzenleme ve denetleme faaliyetleri incelenerek ülkemiz koşullarına uygun hususların ulusal mevzuata uyarlanması gerekmektedir. Bu hususların gerçekleştirilmesi kapsamında uluslararası toplantılara ve çalışmalara olabildiğince iştirak edilmesi faydalı olacaktır.

- ESHS Hizmetlerinin Güvenliğinin ve Sürekliliğinin Sağlanması: ESHS'ler, sunacakları hizmetin güvenliğinden ve sürekliliğinden sorumludur. Sunulacak hizmetlerin mevzuat ile belirlenen şartlara ve standartlara uygun olması gerekmektedir. Bu şekilde hizmet sunan bir ESHS hem çok fazla problem yaşamayacak hem de güvenilirlikle ilgili herhangi bir sorun ile karşılaşmayacaktır

- Akreditasyon Çerçevesinin Geliştirilmesi: Akreditasyon için gerekli altyapı oluşturularak, ihtiyari akreditasyon mekanizmasının hayata geçirilmesi, sertifika hizmet sağlayıcıların kontrolü ve AB mevzuatı ile uyum çerçevesinde önemli hususlar arasında yer almaktadır. Konuya ilişkin olarak TÜRKAK (Türk Akreditasyon Kurumu) ve TSE ile koordineli bir şekilde çalışılmalıdır.

- Uygulamaların Güvenliğinin Sağlanması: Elektronik imzaya ilişkin altyapıları kullanacak yazılımların; tasarlanması, geliştirilmesi ve güncellenmesi aşamalarında güvenliğin ve güvenilirliğin sağlanması için gerekli tedbirler alınmalı ve oraya çıkabilecek olası açıklıklar süratle kapatılmalıdır.

- Kullanıcıların ve Üçüncü Kişilerin Bilgilendirilmesi ve Bilinçlendirilmesi: İmza sahiplerinin ve imzaya güvenerek işlem yapacak üçüncü kişilerin bilgilendirilmesi güvenlik açısından en az uygulanacak teknik önlemler kadar önemli bir husustur. Konuyla ilgili bilgilendirme toplantıları yapılmalı ve herkesin ulaşabileceği kaynaklar oluşturulmalıdır.

- İmza oluşturma ve doğrulama verilerine ilişkin getirilen kuralların uygulanmasının sağlanması: İmza oluşturma ve doğrulama verilerinin kullanılması, saklanması ve gizliliğine ilişkin gerekli tedbirlerin alınması gerekmektedir. Yapılan düzenlemeler kapsamında, imza oluşturma verisi yalnızca imza sahibinin kontrolünde olmalıdır. Ayrıca bu verilerin kopyalanması veya yedeklenmesi de kanun uyarınca mümkün değildir. Ayrıca, imza oluşturma ve doğrulama verilerinin üretilmesi aşamasında gerekli güvenlik tedbirleri alınmalı ve Tebliğ'de belirtilen algoritma ve parametrelere uygunluk sağlanmalıdır.

- Sahtekarlık ve tahrifata karşı gerekli önlemlerin alınması: ESHS'ler üretecekleri sertifikaların taklit ve tahrif edilmesine ilişkin olarak her

türlü önlemi almakla yükümlüdür. Bunun için tüm işlemlerini güvenli bir şekilde yürütmeli ve kişisel bilgilerin korunmasına azami itina göstermelidir. Tüm bunlara ek olarak, kullanıcıların sahte sertifikalara ve bu sertifikalarla yapılacak işlemlere karşı uyarılması kritik öneme sahiptir.

- İmza oluşturma ve doğrulama için üretilen yazılımların güvenliğinin sağlanmasına ilişkin çalışmalar yapılması: İmza oluşturma ve doğrulama için kullanılacak yazılımlara ilişkin standartlar Tebliğ ile belirlenmiştir. ESHS'lerin veya yazılım geliştiren üçüncü partilerin, sağlayacakları yazılımların güvenli olarak geliştirilmesine azami dikkat göstermeleri gerekmektedir. Bunun yanında, Kurum gerekli tedbirleri alarak yazılımların standartlara uyumlu olup olmadığını kontrol etmeli veya yetkili bir kuruluşa kontrol ettirmelidir.

.

KAYNAKLAR

[1] Menezes A., Van Oorschot P., Vanstone S., 1996, Handbook of Applied Cryptography, CRC Press

[2] TÜBİTAK UEKAE, 2004, Açık Anahtar Altyapısı ve Elektronik İmza Uygulamaları Eğitim Kitapçığı

[3] Adams C., Lloyd S., 2002, Understanding PKI: Concepts, Standards, and Deployment Considerations, Second Edition, Addison Wesley

[4] Diffie, W. and M. Hellman., "New Directions in Cryptography.", IEEE Transactions on Information Theory 22 (1976): 644–654

[5] RSA Security Inc., 2000, Frequently Asked Questions about Today's Cryptography

[6] Rhee Man Y., 2003, Internet Security – Cryptographic principles, algorithms and protocols, Wiley

[7] PC Webopedia Definitions and Links, 2004, PKI

[8] The Open Group, 1999, Architecture for Public-Key Infrastructure (APKI)

[9] Verisign, 2000, Understanding PKI

[10] NIST, 1994, Public Key Infrastructure Study – Final Report

[11] Tulloch Mitch, 2003, Microsoft Encyclopedia of Security, , Microsoft Press

[12] Johner H., Fujiwara S., Yeung A., Stephanou A., Whitmore J., 2000, Deploying a Public Key Infrastructure, IBM

[13] Binder J. C., 2002, Introduction to PKI – Public Key Infrastructure

[14] Lannerstrom S., 2000, Basic Elements of a PKI, Sonera SmartTrust Ltd.

[15] American Bar Association, 1996, Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce

[16] Kohnfelder, L. , 1978, Towards a Practical Public-Key Cryptosystem, MIT S.B. Thesis

[17] Chokhani S., Ford W., Sabett R., Merrill C., Wu S., 2003, RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework

[18] ETSI, 2002, TS 101 456 V1.2.1: Policy requirements for certification authorities issuing qualified certificates

[19] McDaniel, G., 1994, IBM Dictionary of Computing, McGraw-Hill, Inc.

[20] ICC, 2004, Securing Your Bussiness

[21] TSE, 2002, TS ISO/IEC 17799: Bilgi Teknolojisi - Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri

[22] King M., 2002, Security Lifecycle – Managing the Threat, GSEC Practical v1.3

[23] U.S. Congress, 1993, Protecting Privacy in Computerized Medical Information, Office of Technology Assessment, OTA-TCT-576

[24] Garfinkel S., Spafford G., 1996, Practical UNIX and Internet Security, O'REILLY, Second Edition

[25] Department of Human And Health Services, 1998, Security and Electronic Signature Standards; Proposed Rule, Federal Register, Vol. 63, No. 155

[26] Karabacak B., 2004, Risk Yönetimi, TUBİTAK – UEKAE

[27] King R., Govanus G., 2000, MCSE: Windows 2000 Network Security Design Study Guide, Sybex Inc.

[28] Zocco P.A., 2001, 10 Days to Network Security v1.2d, SANS Baltimore

[29] Symantec Corporation, 2001, Symantec Enterprise Security

[30] Bhaskar K., 1993, Computer Security: Threats and Countermeasures, NCC Blackwell Ltd.

[31] Bellare M., Kohno T., 2004, "Hash Function Balance and Its Impact on Birthday Attacks.", EUROCRYPT 2004, pp401–418

[32] Nandi M., 2004, A Class of Secure Double Length Hash Functions, Indian Statistical Institude

[33] Rivest R., 1991, The MD4 Message Digest Algorithm, Advances in Cryptology - CRYPTO '90 Proceedings, Springer-Verlag, pp. 303-311

[34] Rivest R., 1992, RFC 1320: The MD4 Message Digest Algorithm

[35] Rivest R., 1992, RFC 1321: The MD5 Message Digest Algorithm

[36] Oorschot P., Wiener M., 1994, Parallel Collision Search with Applications to Hash Functions and Discrete Logarithms, 2nd ACM

Conference on Computer and Communications Security, ACM Press, , pp. 210-218

[37] Bellare M., Kohno T., 2004, "Hash Function Balance and Its Impact on Birthday Attacks.", EUROCRYPT 2004, pp401–418

[38] NIST, 1995, FIPS PUB 180-1: Specifications for the Secure Hash Standard

[39] Eastlake D., Jones P., 2001, RFC 3174: US Secure Hash Algorithm 1 (SHA1)

[40] NIST, 2002, FIPS PUB 180-2: Secure Hash Standard

[41] Dobbertin H., Bosselaers A., Preneel B., RIPEMD-160: A strengthened version of RIPEMD, Fast Software Encryption, LNCS Vol. 1039, pp. 71-82.

[42] Biryukov A., Kushilevitz E., 1998, From Differential Cryptanalysis to Ciphertext-Only Attacks. Advances in Cryptology, Lecture Notes in Computer Science 1462, Proceedings of CRYPTO'98, pp.72-88

[43] Steffen D. A., 1997, Powercrypt: A Free Crptography Toolkit for Macintosh

[44] Wikipedia, 2005, Chosen plaintext attack

[45] Hare C., 2002, Too Many Secrets, Cryptography 101 Lecture Notes

[46] Rivest R., Shamir A., Adleman L, 1978, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM, Vol. 21, pp. 120-126

[47] Evren G., 2004, RSA Sayısal İmza Oluşturma Algoritması - Yapay Sinir Ağları Uygulaması

[48] RSA Laboratories, 2001, A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths, Bullettin #13

[49] Bleichenbacher D., 1998, Chosen Ciphertext Attacks Against, Protocols Based on the RSA Enryption Standard PKCS #1, Proceedings of CRYPTO'98

[50] ElGamal T., 1985, A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, Advances in Cryptography - CRYPTO'84, Springer-Verlag, pp10 – 18

[51] NIST, 2000, FIPS PUB 186-2: Digital Signature Standard (DSS)

[52] Koblitz N., 1997, Elliptic Curve Cryptosystems, Mathematics of Computation 48, 203-209

[53] Miller V.S., 1986, Use of Elliptic Curves in Cryptography, Advances in Cryptology - Crypto '85, Springer-Verlag, 417-426

[54] Certicom Research, 2000, SEC 1: Elliptic Curve Cryptography Version 1.0, Standards for Efficient Cryptography

[55] American Bankers Association, 1999, ANSI X9.62-1998: Public Key Cryptography for the Financial Services Industry: the Ellipti Curve Digital Signature Algorithm (ECDSA)

[56] Institude of Electrical and Electronics Engineers, 2000, IEEE P363: Standard Specifications for Public-Key Cryptography

[57] ISO, 2002, ISO/IEC 15946-2:2002, Information Technology – Security Techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital Signatures

[58] Kopesky G., 2002, PDA as a Signature Creation Device, Master Thesis

[59] CEN, 2004, CWA 14171:2004 General Guidelines for Electronic Signature Verification

[60] Komar B., Microsoft PKI Team, 2004, Microsoft Windows Server 2003 PKI and Certificate Security, Microsoft Press

[61] Gılbert C., Hodgson K., 2003, Best Practice for PKI Users, EEMA

[62] Infosecure, 2003, BS 7799 / ISO 17799 Bilgi Güvenliği Yönetim Standartı Tanıtımı

[63] Lucent Technologies, 2004, Information Security Management – Understanding ISO 17799

[64] BSI, 2002, BS 7799-2:2002 Information Security Management Systems – Specification with Guidance for Use

[65] Small B., Brykczynski B., 2003, Understanding ISO 17799 Code of Practice for Information Security Management

[66] TSE, 2002, TS ISO/IEC 15408-1 Bilgi Teknolojisi – Güvenlik Teknikleri – Bilgi Teknolojisi (IT) Güvenliği için Değerlendirme Kriterleri – Bölüm 1: Giriş ve Genel Model

[67] TSE, 2002, TS ISO/IEC 15408-2 Bilgi Teknolojisi – Güvenlik Teknikleri – Bilgi Teknolojisi (IT) Güvenliği için Değerlendirme Kriterleri – Bölüm 2: Güvenlik Fonksiyonel Gereksinimleri

[68] TSE, 2002, TS ISO/IEC 15408-3 Bilgi Teknolojisi – Güvenlik Teknikleri – Bilgi Teknolojisi (IT) Güvenliği için Değerlendirme Kriterleri – Bölüm 3: Güvenlik Garanti Gereksinimleri

[69] ITU-T, 2000, X.509: Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks

[70] Official Journal of the European Communities, 2000, Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

[71] ETSI, 2003, SR 002 176 V1.1.1: Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures

[72] CEN, 2003, CWA 14167-1: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements

[73] CEN, 2004, CWA 14172-3: EESSI Conformity Assessment Guidance - Part 3: Trustworthy systems managing certificates for electronic signatures

[74] CEN, 2004, CWA 14167-2: Cryptographic module for CSP signing operations with backup -Protection profile - CMCSOB PP

[75] CEN, 2004, CWA 14167-4: Cryptographic module for CSP signing operations – Protection profile - CMCSO PP

[76] CEN, 2004, CWA 14169: Secure signature-creation devices "EAL 4+"

[77] CEN, 2004, CWA 14170: Security requirements for signature creation applications

[78] CEN, 2004, CWA 14171: General guidelines for electronic signature verification

[79] ETSI, 2002, TS 101 733: Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats

[80] ETSI, 2002, TS 101 903: XML Advanced Electronic Signatures (XAdES)

[81] Official Journal of the European Communities, 2003, Directive3 2003/511/EC, Comission Decision of 14 July 2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council

[82] Law Governing Framework Conditions for Electronic Signatures (Signatures Law – SigG), 2001, Bundesgesetzblatt – BGBl

[83] Federal Law Gazette (Bundesgesetzblatt - BGBl.), 2001, Ordinance on Electronic Signatures p. 3074

[84] Eckl P., The German Signature Act – Evaluation and Practice

[85] Schwemmer J., 2001, Solutions and Problems – (Why) It's a Long Way to Interoperability

[86] RegTP, 2004, Notification in accordance with the Electronic Signatures Act and the Electronic Signature Ordinance

[87] Austrian Signature Law, 1999, Bundesgesetzblatt I Nr. 190/1999

[88] Austrian Signature Order, 2000, SigV pursuant to § 25 of the Signature Law

[89] Electronic Document and Electronic Signature Act, 2001, SG 34/2001

[90] Ordinance on the Activities of Certification-Service-Providers, the Terms and Procedures of Termination thereof, and the Requirements for Provision of Certification Services, 2002, SG No.15

[91] Ordinance on the Procedure for Registration of Certification-Service-Providers, 2002, SG No.15

[92] Ordinance on the Requirements to the Algorithms of Advanced Electronic Signature, 2002, SG No.15

[93] Personal Information Protection and Electronic Documents Act, 2000, c.5

[94] Smart Card and Smart Card Reader Specifications for the Government of Canada Entrust Token, 1999, 2900-1 (DDCEI 3-5-4)

[95] Communications Security Establishment, 2005, Cryptographic Algorithms

[96] İnalöz A., 2003, Telekomünikasyon Regülasyonları Çerçevesinde Elektronik Ticaretin İncelenmesi, Telekomünikasyon Kurumu Uzmanlık Tezi

[97] Signature Directive Consultation, 1998, UK

[98] Ulusal Koordinasyon Kurulu, 2004, Altyapı Çalışma Grubu Raporu

ÖZGEÇMİŞ

1978 yılında Ankara'da doğdu. İlk ve orta öğrenimini Ankara'da tamamladıktan sonra 2001 yılında Hacettepe Üniversitesi Bilgisayar Bilimleri Mühendisliği Bölümünden mezun oldu. 1998-1999 yılları arasında Alarko-Carrier San. Tic. A.Ş.'de Bilgisayar Uzman Yardımcısı olarak yarızamanlı çalıştı. 2001 yılında Telekomünikasyon Kurumu'nda Telekomünikasyon Uzman Yardımcısı olarak çalışmaya başladı. Halen Elektronik İmza Çalışma Grubu bünyesinde görev yapmaktadır.