

T.C.
MARMARA ÜNİVERSİTESİ
TÜRKİYAT ARAŞTIRMALARI ENSTİTÜSÜ
BİLGİ ve BELGE YÖNETİMİ

**ELEKTRONİK İMZALI BELGELERİN
YÖNETİMİ ve ARŞİVLENMESİ**

Yüksek Lisans Tezi

BAHATTİN YALÇINKAYA

İstanbul, 2008

T.C.
MARMARA ÜNİVERSİTESİ
TÜRKİYAT ARAŞTIRMALARI ENSTİTÜSÜ
BİLGİ ve BELGE YÖNETİMİ

**ELEKTRONİK İMZALI BELGELERİN
YÖNETİMİ ve ARŞİVLENMESİ**

Yüksek Lisans Tezi

BAHATTİN YALÇINKAYA

Danışman: PROF. DR. HAMZA KANDUR

İstanbul, 2008



MARMARA ÜNİVERSİTESİ
TÜRKİYAT ARAŞTIRMALARI ENSTİTÜSÜ MÜDÜRLÜĞÜ

Yüksek Lisans öğrencisi Bahattin Yalçinkaya'nın "Elektronik İmzalı Belgelerin Yönetimi ve Arşivlenmesi" konulu tez çalışması jürimiz tarafından Bilgi ve Belge Yönetimi Anabilim Dalı Yüksek Lisans tezi olarak oy birliği / ~~oy çokluğu~~ ile başarılı bulunmuştur.

Tez Danışmanı : Prof.Dr. Hamza Kandur
Üniversitesi Marmara

Üye : Prof.Dr. Ercan Öztemel
Üniversitesi Marmara

Üye : Doç.Dr. Oğuz İcimsoy
Üniversitesi İstanbul

İmza

.....

.....

.....

ONAY

Yukarıdaki jüri kararı Enstitü Yönetim Kurulu' nun / 2008 tarih ve sayılı kararıyla onaylanmıştır.

Prof.Dr. Emel KEFELİ
Müdür
.....

İÇİNDEKİLER

ÖZET	IV
ABSTRACT.....	V
ÖNSÖZ	VI
TABLolar	VII
ŞEKİLLER.....	VIII
KISALTMALAR	IX
1.GİRİŞ.....	1
2. BÖLÜM-BİLGİ ÇAĞI.....	6
2.1. BİLGİ TOPLUMU	8
2.2. BİLGİYE ERİŞİM VE KİŞİSEL BİLGİLERİN KORUNMASI	14
2.3. ELEKTRONİK KAVRAMLAR (E-EKONOMİ, E-DEVLET).....	18
3.BÖLÜM-ELEKTRONİK İMZA.....	24
3.1. ELEKTRONİK İMZA- SAYISAL İMZA KAVRAMLARI	24
3.2. ELEKTRONİK İMZA VE DAYANDIĞI TEMELLER.....	27
3.2.1. Açık Anahtar – Özel Anahtar	30
3.2.2. Özel Anahtarın Güvenliği	31
3.2.3. Elektronik Sertifika	32
3.2.3.1. Kök Sertifika.....	34
3.2.3.2. Sunucu Sertifikası	35
3.2.4. Elektronik Sertifika Hizmet Sağlayıcılar (ESHS)	36
3.2.5. Açık Anahtar Altyapısı (AAA) ve Elektronik İmza Servisleri.....	38
3.2.6. Hash Değeri (Hash Value)	39
3.2.7. Zaman Damgası	41
3.3. ELEKTRONİK İMZA	41
3.3.1. Elektronik İmzalama Nasıl Gerçekleşir	41
3.3.2. Elektronik İmza Nasıl Doğrulandır.....	42
3.3.3. Elektronik İmzalama Prosedürü.....	43
3.3.4. Elektronik İmzanın Fonksiyonu.....	45
3.4. ŞİFRELEME.....	46
3.4.1. Tek Anahtarlı Simetrik Şifreleme	47
3.4.2. Asimetrik (Açık Anahtarlı) Şifreleme	47
4. BÖLÜM-ELEKTRONİK İMZALAMA VE ELEKTRONİK SERTİFİKA	
HİZMET SAĞLAYICILARI	48
4.1. ELEKTRONİK İMZA OLUŞTURMA VE DOĞRULAMA VERİSİ.....	48
4.2. GÜVENLİ ELEKTRONİK İMZA	48
4.3. ELEKTRONİK SERTİFİKA.....	48
4.3.1. İdeal ve Nitelikli Elektronik Sertifikalar	50
4.3.2.Sertifika Başvurusu e-Sertifikanın Oluşturulması	52
4.3.3.Elektronik Sertifikanın yayımlanması ve yenilenmesi	53
4.4. SERTİFİKA MAKAMI	54
4.4.1. Sertifika Makamı	54
4.4.2. Sertifika Makamının Görevleri	55
4.4.3.Kayıt Makamı	56
4.4.4. Elektronik Sertifika Hizmet Sağlayıcısının Faaliyetinin Sona Ermesi	57

4.5. UYGULAMADA ÖZEL SERTİFİKA DOĞRULAMA PROBLEMİNE ALTERNATİF YAKLAŞIM.....	58
4.5.1. Güvenli Resmi Mesajlaşma Altyapısı.....	59
4.5.2. Mesajlaşma Sistemlerinde Karşılaşılan Sorunlar	61
4.5.3. Sertifika Doğrulama Problemi ve Çözüm Önerileri	62
4.5.4. Sertifika Geçerlilik Kontrolündeki Sorunların Giderilmesi.....	64
5. BÖLÜM- ELEKTRONİK BELGE VE E-İMZANIN SAĞLAMIS OLDUĞU GÜVENLİK.....	67
5.1-ELEKTRONİK BELGE	67
5.2-ELEKTRONİK BELGE –ELEKTRONİK İMZA İLİŞKİSİ	68
5.3-E-İMZANIN E-BELGEDEKİ ROLÜ	69
5.4. KÖTÜCÜL VE CASUS YAZILIMLARA KARŞI ELEKTRONİK İMZANIN SAĞLAMIS OLDUĞU KORUNMA DÜZEYİ.....	70
5.4.1.E-imza ve İmza Oluşturma Sürecindeki Genel Güvenlik Ölçütleri	71
5.4.2. Kötücül ve Casus Yazılımlar	75
5.4.3. E-imza Oluşturma sürecinde Kötücül ve Casus Yazılım Saldırıları.....	76
5.5. E-İMZA'DA FORMAT SEÇİMİ	78
5.5.1. Görsellik.....	79
5.5.2. İmzalı veri Paylaşımı	80
5.5.3. Kullanım Kolaylığı ve Hukuka Uygunluk.....	81
5.5.4. Veri boyut ve Standardizasyon	82
5.5.5.PDF İçten İmzalama	84
6.BÖLÜM-E-İMZALI BELGELERİN YÖNETİLMESİ.....	85
6.1. ÇAĞDAŞ YÖNETİM SÜRECİNDE E-İMZA SİSTEMİNİN ROLÜ.....	85
6.2. NASIL BİR E- İMZA SİSTEMİ KURGULANABİLİR: MODELLER VE EVRAK YÖNETİM SÜRECİNDE E-İMZA.....	87
6.2.1. Model 1: Asgari Düzey	89
6.2.2. Model 2: Orta Düzey	90
6.2.3. Model 3: İleri Düzey	93
6.3. KURUMLARARASI ELEKTRONİK BELGE PAYLAŞIM HİZMETİ SPESİFİKASYONU	97
6.3.1. e-Devlet Kapısı Üzerinden Paylaşım Senaryosu	99
6.3.2. Kullanım Senaryoları	100
6.3.3. Başarı Faktörleri	101
6.3.4. Sunulacak Tamamlayıcı Hizmetler.....	101
7. BÖLÜM-GÜVENLİ ELEKTRONİK ARŞİVLEME: STANDARTLAR, YAPILAR VE İŞLEVLER	103
7.1. UZUN DÖNEMLİ İMZA DOĞRULAMADA YAŞANABİLECEK SORUNLAR.....	103
7.2. GÜVENLİ ZAMAN DAMGALI E-İMZA	104
7.3. UZUN DÖNEMLİ ELEKTRONİK İMZA YAPILARI.....	106
7.3.1. İmza verisi (Electronic Signature – ES)	106
7.3.2. Zaman damgalı imza (ES with Timestamp – ES-T).....	106
7.3.3. Tam doğrulama verisi içeren imza (ES with Complete Validation Data – ES-C)	107
7.3.4. Genişletilmiş doğrulama verisi içeren imza (ES with eXtended Validation Data – ES-X).....	108

7.3.5. Arşivlenmiş doğrulama verisi içeren imza (ES with Archive Validation Data – ES-A)	108
7.4. GÜVENLİ E-ARŞİVLEME İŞLEVLERİ	108
7.5. ARŞİV İMZASI	110
8-BÖLÜM-ELEKTRONİK İMZANIN HUKUKİ BOYUTLARI	112
8.1. BÖLÜM-ELEKTRONİK DOKÜMANLARI VEYA MEKTUP'LARIN KANIT OLABİLMESİ İÇİN GEREKSİNİMLER	112
8.2. ELEKTRONİK DOKÜMAN SERVİSLERİ VE OLABİLECEK GÜVENLİK İHLALLERİ	116
8.3.ELEKTRONİK İMZANIN VE İMZALANMIŞ VERİLERİN DELİL NİTELİĞİ	122
8.4.ELEKTRONİK SERTİFİKA HİZMET SAĞLAYICILARI'NIN SERTİFİKA SAHİBİNE KARŞI SORUMLULUĞU	124
8.5. ESHS'NİN ÜÇÜNCÜ KİŞİLERE KARŞI SORUMLULUĞU	125
9.SONUÇ	129
KAYNAKÇA	132
ÖZGEÇMİŞ	146

ÖZET

En genel tanımıyla elektronik imza, elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veridir. Bu tanımda elektronik imzanın en önemli üç unsuru ifade edilmektedir. Buna göre; elektronik imzanın elektronik veriden ayrı olduğu ve ona eklenmesi, ikinci olarak eklendiği veriyle mantıksal bağlantı kurulması, üçüncü olarak, veriye eklenen ve eklendiği veriyle mantıksal bağlantı kurulmasının kimlik doğrulama amacıyla yapılıyor olmasıdır

İnsanların kullanımına sunulan birçok yeni teknolojik altyapının sergilediği kolaylık ve kullanışlılığı gölgeleyebilecek en önemli etkenlerin başında, bilgi ve bilgisayar güvenliği gelmektedir. E-imzanın gerek kişisel ve gerek kurumsal alanda yaygınlaşabilmesi ve var olan geleneksel yapının yerini alabilmesi için yerine getirilmesi gereken en önemli şart, bu teknolojiye olan itimadın toplum içerisinde yaygınlaşması ve bir daha zarar görmeyecek şekilde sağlam bir biçimde yerleşmesidir.

Bu çalışma çerçevesinde kâğıt tasarrufu desteklenerek, kurumların veya şirketlerin e-imzalı belgeleri kullanarak gelişimlerine devam etmelerini sağlamak amacıyla birkaç model üzerinde durulmuştur. Bu modeller uygulamada bulunan birkaç modeldir, şüphesiz farklı yaklaşımlarla geliştirilebilirler.

ABSTRACT

MANAGEMENT AND FILING OF THE ELECTRONIC-SIGNED DOCUMENTS

In its broadest definition, electronic signature refers to an electronic data which is attached or logically connected to an electronic data, and used for identity verification. This description covers three significant components of electronic signature; namely, the electronic signature firstly differs from the electronic data and is attached to it, secondly it has a logical connection with the data to which it is attached, and thirdly it is attached to the data with an aim to verify identity.

The question of security of information and computers is one of the factors overshadowing facilities and efficiencies provided by the modern technology. Settlement of faith on technology within the society is the most important condition in order for enlargement of electronic signature within individual and institutional spaces and its replacement with the conventional structure.

Within the framework of this study, several models are emphasized so as to support paper savings and development of institutions and companies through use of electronic-signed documents. These employed models are few in number but may be improved by different approaches.

ÖNSÖZ

Günümüz teknolojisi neredeyse bütün ihtiyaçlarımızı internetten sağlamamıza olanak sağlayacak seviyeye geldi. Mesafeler kısaldı, zaman paha biçilemez bir mefhum haline geldi. İnternetin sağlamış olduğu bu kolaylıklar hayatımızda bazı şeyler için hızlı kararlar vermemizi sağlarken diğer taraftan internetin güvenilirliği yine tartışma konusu olmaya devam etti. Bu güvenilirliği sağlamak 2000’li yılların başında yeni bir kavramla mümkün bir hale gelmeye başladı. Şüphesiz bunun adı elektronik imzaydı.

Tez aşamasına geçip, konu seçimi için çalışmalar yaparken, işin açık tarafı, bu kadar teknik bir konu seçip, günlerce uğraşacağımı pek tahmin etmiyordum. Özellikle elektronik imzalı belgelerin yönetilmesi ve arşivlenmesi konusunu çalışacağım o zamanlar aklıma geliyor fakat hep bir endişe ve tedirginlikle bu konuya yaklaşıyordum. Fakat Hocamın beni bu konuda cesaretlendirmiş olması bu tezi yazmamdaki temel yapı taşıdır. Böylesine teknik ve zor bir konuyu zamanla sevip her gün yeni bir şeyler öğreneceğimi teze başladıktan hemen sonra fark ettim. Hatta bu tez yazımı esnasında T.C. Başbakanlık Devlet Arşivleri Genel Müdürlüğü’nde görev almaya başladım. Kamuda bu kavramın ve diğer elektronik kavramların ne kadar önemli bir yere sahip olduğunu gördüğümde, tez hocamın beni konuya yönlendirmesinin ne kadar isabetli bir karar olduğunu gördüm.

Beni çalışmamda cesaretlendirip her türlü sorularıma cevap veren, yol gösteren, umutsuzluğa kapıldığım anlarda bana umut veren, bölüm başkanımız Değerli Hocam Prof. Dr. Hamza Kandur’a sonsuz şükranlarımı sunarım. Beni bugünlere getiren bütün öğretmen, hoca ve öğretim görevlilerine de teşekkürü bir borç bilirim. Ayrıca çalışmalarımda maddi manevi desteğini esirgemeyen aileme, kardeşime, Devlet Arşivleri Genel Müdürlüğü Bilgi-İşlem Koordinatörlüğü’ndeki arkadaşlarıma, Dokümantasyon ve Enformasyon Koordinatörlüğündeki arkadaşlarıma da teşekkür ederim.

Ankara, 2008

Bahattin YALÇINKAYA

TABLÖLAR

Tablo 1-Geleneksel Ekonomi ve E-Ekonominin Mukayesesi.....	19
Tablo 2-Güvenlik Tehditleri	74
Tablo 3-E-imzalı Belge Yönetimi Modelleri Arasındaki Farklar Tablosu.....	96
Tablo 4-EBPS kapsamında Sunulacak Tamamlayıcı Hizmetler Tablosu	102

ŞEKİLLER

Şekil 1-Ülkelere göre Toplam ARGE Harcamalarında BT Sektörünün Payı	12
Şekil 2-Türkiye’de, Gelir Gruplarına Göre Evde Bilgisayar Sahipliği	13
Şekil 3- ICT’nin biçimlendirilmesi sürecinde etkin olabilecek bileşenler	23
Şekil 4-Basit Sertifika Örneği	49
Şekil 5-İdeal Sertifika Örneği	51
Şekil 6-Sertifika Yaşam Çevrimi	54
Şekil 7- Mesajlaşma Sistemi Genel Yapısı	60
Şekil 8- A kullanıcı ucundan A’nın Güncel Sertifikası Olmayan B kullanıcı ucuna Direkt mesajlaşma	63
Şekil 9- Sertifika geçerlilik analizi	66
Şekil 10- Standart uzun dönemli Elektronik Kayıt yapısı	68
Şekil 11-Elektronik İmza Oluşturma İşlevsel Modeli	72
Şekil 12-Ana Kötücül Yazılım Türleri	75
Şekil 13: E-imza Oluşturma uygulamasında Truva atı ve casus yazılımlar tarafından hedef alınan arayüzler	77
Şekil 14-İmzalanmış belgenin PDF görünümü	79
Şekil 15-İmzalanmış belgenin XML görünümü	80
Şekil 16-XML ve PDF’te imzalanmış belgelerin kapsadığı boyutlar	83
Şekil 17-PDF belgesinin içten imzalanması	84
Şekil 18-Belge Yönetiminde Model-Gereksinim oranlaması ihtiyaçları	88
Şekil 19-Model 1-Asgari Düzey Genel Yazışmalar	90
Şekil 20-Model 2-Orta Düzey Kurumdışı Yazışmalar	93
Şekil 21-Model 2-Orta Düzey Kurumiçi Yazışmalar	93
Şekil 22-Model 3-İleri Düzey Kurumdışı yazışmalar	94
Şekil 23-Model 3-İleri Düzey Kurumiçi Yazışmalar	95
Şekil 24- Belgelerin Gönderen Kurumdan Alıcı Kuruma İletilmesi	98
Şekil 25-Alınan Belgelerin Zimmet Altına Alınma Bilgilerinin Gönderilmesi	99
Şekil 26- Arşiv imzasının içermesi gereken eklentiler	111
Şekil 27-İnternet üzerinde elektronik posta gönderme-alma işlemi	114

KISALTMALAR

AAA	Açık Anahtar Altyapısı
ABD	Amerika Birleşik Devletleri
ATM	Asynchronous Transfer Mode
BM	Birleşmiş Milletler
CD	Compact Disk
CEN	Comitte European Normalisation
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List
CRLDP	Certificate Revocation List Distirbution Point
DS	Dizin Sistemi
DSA	Digital Signature Algorithm
DVD	Digital Versatile Disk
EBY	Elektronik Belge Yönetimi
EBYS	Elektronik Belge Yönetim Sistemi
EDY	Elektronik Doküman Yönetimi
e-Ekonomi	Elektronik Ekonomi
EFTP	Electronic Federal Tax Payment
EİK	Elektronik İmza Kanunu
e-mail	Elektronik Posta
ES	Electronic Signature
ES-A	Electronic Signature Archive Validation Data
ES-C	Elektronik Signature Complete Validation Data
ESHS	Elektronik Sertifika Hizmet Sağlacısı
ESI	Electronic Signature Formats
ES-T	Electronic Signature Timestamp
ES-X	Electronic Signature eXtended Validation Data

<i>ETKK</i>	Elektronik Ticaret Koordinasyon Kurulu
<i>ETSI</i>	European Telecommunications Standard Institute
<i>EU</i>	European Union
<i>GMAB</i>	Güvenilir Mesaj Aktarım Bildirimi
<i>HSM</i>	Hardware Security Module
<i>ICT</i>	Information & Communications Technology
<i>IETF</i>	Internet Engineering Task Force
<i>IP</i>	Internet Protocol
<i>ISSS</i>	Information Society Standardisation System
<i>ISO</i>	International Standardization Organization
<i>ITU</i>	International Telecommunications Union
<i>İDV</i>	İmza Doğrulama Verisi
<i>İOU</i>	İmza Oluşturma Uygulamaları
<i>İOV</i>	İmza Oluşturma Verisi
<i>JILT</i>	The Journal of Information, Law and Technology
<i>KKDV</i>	Kimlik Kanıtlama Doğrulama Verileri
<i>KM</i>	Kayıt Makamı
<i>md.</i>	Madde
<i>OCSP</i>	Online Certificate Status Protokol
<i>PC</i>	Personel Computer
<i>PDF</i>	Portable Document Format
<i>PEM</i>	Privacy Enhanced Mail
<i>PGP</i>	Pretty Good Privacy
<i>PIN</i>	Personel Identification Number
<i>PKI</i>	Public Key Infrastructure
<i>RDF</i>	Resource Description Framework
<i>RFC</i>	Request for Comments

<i>RKKV</i>	Referans Kimlik Kanıtlama Verileri
<i>RSA</i>	Ron Rivest, Adi Shamir, Len Adleman soyisimleri baş harflerinde türetilmiş algoritma
<i>S/MIME</i>	Secure Multi-Purpose Internet Mail Extensions
<i>SHA</i>	Secure Hash Algorithm
<i>SİL</i>	Sertifika İptal Listesi
<i>SM</i>	Sertifika Makamı
<i>SMTP</i>	Simple Mail Transfer Protocol
<i>SSK</i>	Sosyal Sigortalar Kurumu
<i>SSL</i>	Secure Socket Layer
<i>TBMM</i>	Türkiye Büyük Millet Meclisi
<i>TCP</i>	Transmission Control Protocol
<i>TSP</i>	Time-Stamp Protocol
<i>UEKAE</i>	Elektronik ve Kriptoloji Araştırma Enstitüsü Müdürlüğü
<i>UNCITRAL</i>	United Nations Commission on International Trade Law
<i>vb.</i>	Ve Benzeri
<i>W3C</i>	World Wide Web Consortium
<i>XML</i>	Extensible Markup Language
<i>XSL</i>	Extensible Style Language
<i>ZDHS</i>	Zaman Damgası Hizmet Sağlayıcıları
<i>(t.y.)</i>	Tarih yok
<i>[y. y. : yayl. y.]</i>	Yayın Yeri Yok : Yayınlayan Yok

1.GİRİŞ

XX. yüzyıl sonlarına doğru bilgisayar teknolojisinde yaşanan gelişmeler oldukça hızlı ve insan hayatını direkt etkilemesinden ötürü önemli olmuştur. II. Dünya Savaşı sonrasında dünyada başlayan bilgi üretimi, bilgisayar teknolojisiyle kat kat artmıştır. Bilgiye güvenli ve hızlı erişim, bilgi teknolojilerine bakış açısında radikal olarak adlandırabileceğimiz bir devinime yol açmıştır. Şüphesiz bu gelişmeler demokrasi ve şeffaflık anlayışında etkili olmuştur. Buradan hareketle dünyadaki bütün devletler elektronik devlete geçişi hedeflemişler ve yatırımlarını bu yönde şekillendirmişlerdir.

Bilgi ve iletişim teknolojileri hız ve sınır tanımayan bir olgudur. Tezin temel dayanak noktası da bu sınır tanımayan olguya insanoğlunun nasıl geldiği, hangi duraklarda nasıl şekillendiğidir. Son 20 seneye baktığımızda internet kavramı, bilgi teknoloji kavramının ne denli bir yapıya kavuştuğunu açıklamamızda göstergelerden sadece birisi ve belki de en önemlisidir. Küresel ağ olarak dilimize aktarabileceğimiz bu kavram kilometrelerce mesafeler arasında iletişimi etkin ve hızlı bir şekilde sağlamaktadır. Bu durumda insanoğlu interneti bazı aksiyonlar için kullanmaya başlamış ve bunun sayesinde elektronik ekonomi kavramına kavuşmuştur. Peki bu ağa ne kadar güvenebiliriz. Yaptığımız iş ve işlemlerde nasıl sonuca erişilebilir? Bütün bu kavramları izah edecek bir kavram olan elektronik imza, tıpkı insanoğlunun yaklaşık iki bin yıldır kullandığı imza yerine, elektronik ortamda aynı görevi ifâ edecek olan bu kavramla tanışmasını sağlamıştır.

Elektronik ticaretin gelişmesi ve elektronik imzanın kullanıcılar tarafından benimsenmesi için açık ağ sistemine güven duyulmasının sağlanması gereklidir. Bu güvenin sağlanabilmesi için taraflar arasında iletilen bilgilerin gizliliği, bütünlüğünün korunması, güvenilirliği, tarafların kimliklerinin doğruluğunun güvence altına alınmasına ilişkin hukuki düzenleme yapılması gereklidir. Bu hukuki düzenlemeler dünyada Elektronik İmza Kanunları ya da Dijital İmza Kanunları şeklinde 1998 yılından beri kabul edilmektedir. Hukuki bağlayıcılığı ile insanların zihninde bulanıklığa yol açmayan bu kavram; zaman, işgücü ve tasarrufu desteklemesi açısından da önemli bir kavram olmuş ve bu kavramı insanların gelecekte yoğun olarak kullanacağı daha

şimdiden görülmüştür. İlk başta pek dikkat çekmese de elektronik imza, diğer bileşenlerle ekolojik dengeyi korumak adına insanoğlunun atmış olduğu altın bir adım olarak tarih sayfalarında yerini alacaktır.

Elektronik İmza konusunda Türkiye’de ilk çalışmayı Hazine ve Dış Ticaret Müsteşarlığı yapmış, ikinci çalışma ise Adalet Bakanlığı tarafından gerçekleştirilmiştir. Ülkemizde e-devlete dönüşümün temel dayanak noktasının elektronik imza olduğu kanaati yaygınlaşmış ve 15 Ocak 2004 tarihinde 5070 Sayılı Elektronik İmza Kanunu TBMM tarafından kabul edilmiştir. Bu kanun 23 Ocak 2004 tarihinde 25355 Sayılı Resmi Gazetede yayımlanmıştır.¹ Kanun, konu hakkında yapılacak ikincil mevzuat düzenlemelerini yapma görevini Telekomünikasyon Kurumu’na vermiştir.

Hayatımızda kullandığımız imza gibi, elektronik imza da elektronik ortamda gönderilen bilgi ve belgelerin kime ait olduğunu göstermek için kullanılır. Bu işlemleri gerçekleştirebilmek için elektronik sertifikalara ihtiyaç duyulur. Elektronik Sertifikalar kişilerin ya da kurumların internet ortamında kimliklerini ispatlamalarını sağlayan sayısal bilgi bütünlüğüdür. Bu bütünlük birtakım bileşenlerden oluşur. Bir belgeyi elektronik ortamda imzalamak için elektronik sertifika sahibi olmak gerekir.

Elektronik ticaret ve kamu alanında yürütülecek “e-devlet” olarak adlandırılan projenin alt yapısının temel yapı taşı elektronik imzadır. E-devlet oluşumunda “bilgi güvenliği” vazgeçilmez ve önceliği çok yüksek uygulamasından biridir. Bilgi güvenliğini de en güvenilir şekilde sağlayan elektronik imzadır.

Elektronik İmza, yasal boyutta zemin kazandıktan sonra kişisel veri güvenliği, bilgi güvenliği, elektronik ticaret, elektronik veri ve elektronik belge gibi pek çok kavram üzerinde düzenleme veya çalışma yapılması teşvik edilmiştir.

Bu konulardan birisi olan e-belge konusunda görev Devlet Arşivleri Genel Müdürlüğü’ne verilmiştir. Devlet Arşivleri Genel Müdürlüğü bünyesinde Prof. Dr. Hamza Kandur’un öncülüğünde Elektronik Belge Yönetimi Referans Kriterleri v.1, v.2 şeklinde yayımlanmış, 19 Haziran 2007’de de Türk Standartları Enstitüsünden 13298

¹ 5070 Sayılı, “Elektronik İmza Kanunu”, Kabul Tarihi:15.01.2004, Resmi Gazete Sayısı:25355, Resmi Gazete Tarihi:23.01.2004

sayılı Standard numarası olarak standartlaşmıştır.² Elektronik belge ile ilgili bazı standartların getirilmesi kamudaki belge üretiminde bir refleks oluşturup belli bir düzen sağlayabilecektir. Ayrıca elektronik imza uygulamalarında güvenli ve düzenli bilgi paylaşımını sağlayacak, güvenilebilir arşivlerin elektronik ortamda oluşmasına yol açacaktır.

Bir başka çalışmada Elektronik Belgelerin Paylaşımı konusunda TURKSAT A.Ş. tarafından yürütülmektedir. E-devlet kapısı projesine paralel olarak kamu kurum ve kuruluşlarının birbirleriyle olan muhaberatının bir kapı üzerinden yapılması çalışmaları devam etmektedir.³

Bu tez, üç kısım ve toplam dokuz bölümden oluşmaktadır. I. kısımda genel olarak elektronik imzanın literatüre dayalı bilgisinin yanı sıra bilgi çağının akıl almaz gelişimi de irdelenmeye çalışılmıştır. İkinci bölümde bilgi çağına nasıl ulaştığımızı ve değişimin hızının artık hesaplanabilir olmaktan çıktığı vurgulanmıştır. Bu değişimin, bilgi toplumunu oluşturduğu ve bilgi toplumunun da bilgisayarla genişleyeceği izah edilmeye çalışılmıştır. Hayatımızda giderek genişleyen, e-ortamda bulunan bilgilerin kişisel bilgi güvenliğimizi hangi durumlarda, nasıl ihlal ettiği genel hatlarıyla yine bölümde izah edilmiştir. Elektronik kavramlar (elektronik ekonomi ve e devlet) genel manasıyla bu bölümde irdelenmiştir.

Üçüncü bölümde ise; elektronik imzanın teknik açıklamasını bulmak mümkündür. Elektronik imzanın dayandığı teknik kavramlar, Açık Anahtar Altyapısı, Sertifika, Hash Değeri, Şifreleme, elektronik imzanın nasıl gerçekleştiği ve nasıl doğrulandığı gibi teknik konular bu bölümde literatür bilgisine uygun olarak anlatılmaya çalışılmıştır.

Dördüncü bölüm üçüncü bölümün devamı niteliğinde olup elektronik imzanın fonksiyonel işlemesi için gerekli alt yapının incelenmesine ayrılmıştır. Sertifika Hizmet Sağlayıcılarla ilgili birtakım bilgileri ihtiva eden, bu bölümün sonunda uygulamada olan

² “Elektronik Belge Yönetim Standartları Referans Kriterleri Artık Bir Standart!”, <http://www.devletarsivleri.gov.tr/source.cms4/index.asp?wapp=haberdetaytr&did=E6340703-CEB0-4B0D-A44F-63C8E0F461F8>, (30 Haziran 2008).

³ “Kurumlararası Elektronik Belge Paylaşım Spesifikasyonu”, <http://www.devletarsivleri.gov.tr/source.cms4/index.asp?wapp=anasayfa> (30 Haziran 2008)

özel sertifika doğrulama problemine alternatif bir bakış açısı getirilmeye çalışılmıştır. Ayrıca bu bölüm, birinci kısımda son bölümdür.

İkinci kısımda; Elektronik belge hakkında genel bir bilgilendirmeyi bulmanın yanında teze ismini veren Elektronik İmzalı belgelerin yönetilmesi ve arşivlenmesi ile bilgilerin bulunduğu kısımdır.

Beşinci bölümde elektronik belgenin genel anlamda neyi ifade ettiğini bulunmaktadır. Bu çalışma kapsamında Elektronik Belge Yönetim Sistemine incelenmemiştir. Zira bu kavram son derece geniş bir kavram olmakla beraber ayrı bir tez konusu teşkil etmektedir. Ayrıca beşinci bölümde e-imzanın e-belgedeki rolü, e-imza oluşturmadaki genel güvenlik ölçütlerinin neler olduğu, kötücül ve casus yazılımların bilgisayarlar ve belge üzerinde nasıl etkiler yaptığı, e-imza oluşturma sürecinde kötücül casus yazılımların saldırıları hakkında bilgiler verilmeye çalışılmıştır. Yine bu bölümde elektronik imza uygulamasını hangi formatta oluşturabiliriz sorusuna cevap aranmıştır.

Altıncı bölüm elektronik imzalı belgelerin yönetilmesi üzerinde kurgulanmış bir bölümdür. Öncelikle çağdaş yönetim anlayışında elektronik imzanın ne gibi bir rol üstlendiği aydınlatılmaya çalışılmıştır. Elektronik Belge Yönetiminde oluşturulan belgeler için nasıl bir süreçte yönetileceği konusunda yine bu bölümde bazı modeller öne sürülerek açıklanmaya çalışılmıştır. Modeller kurumsal ihtiyaç ve birikimlere bağlı olarak değişebildiği için birden fazla model oluşturulabileceği görülmüştür fakat bu sınırlandırılarak üç model üzerinde durulmuştur.

Yedinci bölümde; Elektronik İmzalı belgelerin ve elektronik imza arşivlerinin nasıl bir yapıda olduğunu incelemeye çalışılmıştır. Uzun dönemli imza doğrulama problemine karşı yaşanabilecek sorunları yine bu bölümde ele alınmıştır. Yine bu bölümde zaman damgası, güvenli e-arşivleme işlevleri ve arşiv imzası gibi kavramlar hakkında bilgi verilmeye çalışılarak tezin ikinci kısmı sonlandırılmıştır.

Üçüncü kısım tanıtılmadan önce, bu kısma ihtiyaç duyulmasının temel nedeni arşivlerin delil vasfına haiz olmalarıdır. Bu vasıf hukukla arşivler arasında derin bir bağ oluşturmaktadır. Üçüncü kısımda elektronik imzalı belgelerin bağlı bulunduğu

servislerde olabilecek ihlalleri ve elektronik belgelerin veya mektupların delil olabilmeleri için gereksinimlerin neler olduđu incelenmiştir. Yine elektronik sertifika hizmet sağlayıcılarının hukuki sorumluluklarının neler olduğunu bu kısımda izah edilmeye çalışılmıştır.

Sekizinci bölümde elektronik belge veya mektup iletiminde elektronik ortamdaki servis ve protokollerin sağladığı kolaylıkların yanında sahtecilik, aldatma, mesaj başlığının içeriğini deđiştirme, yeniden oluşturma gibi yöntemler kullanılarak farklı kaynaktan, farklı içerikli mesaj gönderilmesi, alıcı ve göndericinin yanıltılması mümkün olabildiğı üzerine durulmuştur. Yine bu bölümde elektronik belge ve mektuplar için olabilecek fiili saldırılara genel bir yaklaşım sergilenmiştir. Elektronik imzanın hukuki boyutlarını, Elektronik İmzanın ve İmzalanmış Verilerin Delil Niteliğini, Elektronik Sertifika Hizmet Sağlayıcılarının Hukuki sorumluluklarını yansıtılmıştır.

Elektronik İmza konusu oldukça geniş ve teknik bir literatüre sahiptir. Tez kapsamında 5070 Sayılı Elektronik İmza Kanunu çerçevesinde yaklaşım gösterilmiştir. Detaylı teknik analizlerden ve literatür bilgilerinden mümkün olduğunca sakınılmıştır.

2. BÖLÜM-BİLGİ ÇAĞI

İnsanın, bilgiyle olan etkileşiminin başlangıç noktası olarak yazıyı kabul ettiğimizde insanoğlunun bugünkü bilgi hazinesini nasıl oluşturduğunu ve ortaya nasıl bir değişim katsayısı çıktığı görülebilmektedir. Günümüzde bilginin etki alanı artık değişimin hızıyla hesaplanabilmektedir.

Taş tabletler üzerine yazı yazmakla başlayan serüven, alfabenin bulunuşu, malzemenin ilkel olarak kopyalama ihtiyacının doğması, matbaanın getirdiği yeni anlayış, iletişimin kavramını yeniden düzenleyen telgrafın icadı ve devasa boyuttaki camdan evlerin* avuç içine sığacak niteliğe kavuşmasında radikal devrim olarak adlandırabileceğimiz transistörün teknolojiyi şekillendirmesi, gibi birtakım duraklara uğradıktan sonra günümüzde de devam etmektedir..⁴

Bu serüvenin detaylarını biraz açmak gerekirse; insanoğlu bir tablete yazı yazmış ve onun değerli olduğu hükmünü ortaya koymuştu. Sonraki dönemlerde genel hatlarıyla papirüse, parşömene ve kâğıda bu değerli hükümler aktarılmaya devam edildi. Hükümler çoğaldıkça, mülkiyet hakkı ve antlaşma kavramlarını beraberinde getirdi. Bu bilgi ve belgeye olan ihtiyaçtan başka bir şey değildi ve her geçen gün ihtiyaçlar artıyor ve yeni arayışlar kaçınılmaz olmaya başlıyordu. İnsan bir taşı veya ağaç dalını eline alarak ilk kez alet olarak kullandığında, çevresiyle arasındaki dengeyi geri dönüşü olmayan bir şekilde değiştirdi. Kullanılan aletlerin sayısı azdı ve yayılıp etki yapmaları uzun süre aldı. Kullanılan aletlerin sayısı arttıkça, etkileri de çoğaldı: aletler çoğaldıkça, değişim hızı da arttı.⁵

* Eski İstanbul evlerinin bazılarında giriş katı ile bahçeyi birleştiren, üstü cam kaplı bir bölme olurdu. Bu alanda çiçek yetiştirilirdi. Bir tür küçük sera olan ve eski İstanbulluların limonluk adını verdiği bu mekâna Avrupa mimarisinde daha sık rastlamak mümkündür. Adına İngilizce “glasshouse”, (camdan ev ya da Sırça Köşk) denir. Bazı bilgisayarıcılar glasshouse deyimini, çoğumuzun varlığını bildiği ama büyük bir olasılıkla tanışmadığı ana bilgisayar sistemleri için kullanmıştır. “Camdan ev” ya da “Sırça Köşk” ana bilgisayar sistemlerinin tarihçesini ve günümüzde bu sistemleri bir kuruluştaki yerini belirtmek açısından uygun bir kavramdır.

⁴ Daniel R Headrick, **Enformasyon Çağı, Akıl ve Devrim Çağında Bilgi Teknolojileri 1700-1850**. Z. Kılıç (çev.), İstanbul: Kitap Yayınevi, 2002, s.18.

⁵ Bill Gates, **Dijital Sinir Sistemiyle Düşünce hızında çalışmak**, Ali Cevat Akkoyunlu (çev.), İstanbul :Doğan Kitap,1999, s.75.

1897 yılında Amerika Birleşik Devletleri Başkanı William McKinley, telefonun icadıyla ilgili olarak insanoğlunun teknolojiye gelebileceği doruk noktasına ulaştığını söylüyor ve insanoğlunun artık bu değişim hızında bir adım bile öteye gidemeyeceğini çok rahatlıkla ilave ediyordu. Ama öyle olmadı, eğer Amerikan başkanı bir 60 yıl daha yaşasa bilgisayarları görüp belki de ne kadar yanıldığını görecekti. Hiç şüphesiz telgrafın icadı bilgi ihtiyacı ve aksiyonları için yeni bir dönemin başlangıcı, iletişimin de çok yeni ve etkin bir kavramıydı.

İnsanların birbirleriyle haberleşme ve iletişim kurma gereksinimi insanın tarihi kadar eski bir kavramdır. Önceleri dumanı, daha sonra posta güvercinlerini derken posta, telgraf, telefon iletişimin etkinliğini arttıran icatlar olarak tarihteki yerlerini aldılar.⁶

1950’li yıllarda bilgisayarlar ancak basit, dört işlemi yapabilen ve devasa boyutlu, apartman görünümlü bir yapıdaydı. 1960’lı ve 1970’li yıllarda bilgisayarlar, günümüz bilgisayarlarından çok geri ve aynı zamanda pahalıydı. Bu bilgisayarların kullanılabilmesi için ileri düzey uzmanlık gerekiyordu. Avrupa’da özellikle İngiltere’de evlerin geçiş bölümlerinde çiçek yetiştirmek için camekânlı bir oda yer alırdı. Zamanın uzmanları, bilgisayarların bulunduğu bu bölümleri İngilizce deyimle “glasshouse” cam ev olarak adlandırıyorlardı. Microsoft’un patronu ve içinde bulunduğumuz çağın sihirbazı olduğunu iddia eden Bill Gates’e göre transistörler yeniçağın başlangıcıydı. Hatta zaman makinesi icat edilse ilk yapmak istediği şeyin transistörün bulunduğu gecede o laboratuara olmak istediğini söylüyordu. 1990’lı yıllarda bilgisayarlar artık şahsi kullanıma başlanmış ve PC ismiyle yani “Personel Computer” yani şahsi bilgisayarlar olarak bekli de hayatımızı çok keskin bir şekilde değiştirerek hayatımıza girmişlerdi. Zamanla hayatımızın bir parçası olmaya başladılar. Gelecekte insanların, işlerinin çoğu için her gün bilgisayar kullanacakları 50’li ve müteakip yıllarda hayal edilemez bir durumdu. Hatta günde sekizer saatlik mesailerinin bu aletlerin başında geçirileceğine, büyük bir ticaret ağı oluşturup bilgi işçileri diye bir çalışma grubunun olacağı hayal bile edilemezdi.

⁶ Elçin Çizmeli (edt.), “Türkiye’de Bilişim Sektörünün Mevcut Durumu”, **Bilgi Toplumuna Doğru, Türkiye Bilişim Şurası**, Ankara: Başbakanlık, 10-12 Mayıs 2002, ODTÜ, s.12.

2.1. BİLGİ TOPLUMU

Bilgi toplumu denilince bilgi kullanımının yüksek olduğu, bilgi düzeyi yüksek, bilginin ekonomik değer taşıdığı toplum akla geliyor. Böyle toplumlarda bilgisayar kullanımı ile bilgi kullanımı ileri düzeydedir. Bilgisayar hayatın her alanına girmiş ve günlük işlerin yapılmasında etkin bir yapıya hâkim olmuştur. Bilgisayarla, bilgi kullanımı içerik anlamı bakımından aynı olmamasına rağmen birbiriyle iç içedir.

Bu topluma baktığımızda bilgisayara dayalı bir teknolojiyi görebiliriz. Bilgi ve teknolojinin getirdiği bu altyapı aynı zamanda toplumun bireylerini derinden etkilemektedir. Bu etkileme başta eğitimlerinden başlayıp düşünce yapılarının analitik olmasına kadar uzanan bir süreçtir.

Bilgi toplumunun en kıymetli varlığı insandır. Bilgiye dayalı emeği pahalı yapan unsur insanın eğitiminin yenileşmesidir. Bilgi işleme altyapısı itibariyle ciddi ve uzun bir eğitim dönemi kapsamaktadır. Sanayi devriminde en önemli hammadde madenler iken günümüzde artık bilgi önem taşımaktadır. Hammadde arayışları toprak altında sürerken bilginin temel kaynağı insandır. İnsanın düşünmesi ile harekete geçen bilgi faktörü toplumların refah seviyesinden, yaşam standartlarına kadar geniş bir alanı etkiler.

Hammaddenin toprak altından bulunup işlenmesi için sınırlar geçip fabrikalara, oradan makineler yoluyla işlenerek tekrar sınırlar geçip pazara sunulması işi maliyet açısından çok pahalı bir durumdu. Günümüzde ise sanal şirketler oluşmaya başlamıştır. Öyle ki eski anlayışa tamamen ters olan bu durum kişinin patronu ve çalışanı olduğu işe gitmesini bile gerektirmektedir. İşçi gücü, iş gücü gibi faktörler organizasyon yapabilme ve yönetime dayalı anlayışlara yerlerini bırakmakta ve kazanılan ekonomik kazanç bile artık elektronik olarak birikime çevrilmektedir.

1980’li yıllardan itibaren sanayide çalışan mavi gömlekliler kabuk değiştirerek bilgi çalışanı olarak adlandırılan bir kesimin doğmasını sağlamıştır.⁷ Mavi gömlekli kesim toplumların büyük diyebileceğimiz bir kısmını oluşturunuyordu.

Bilgi çalışanlarını kabuk değiştirmesi eğitimin seviyelerinin artmasını zorunlu kılıyordu. Eğitim seviyesi artmış bilgi çalışanları sanayide robot, bilgisayar gibi hassas aletleri kullanmalarının yanı sıra hizmet sektöründe karşımıza çıkıyorlardı.

Madenciliğin yerine, karlılığı yüksek yeni üretim sektörleri başta Batı ülkeleri olmak üzere birçok ülkeyi yeni arayışlar içerisine itmiştir. Biyoteknoloji, metalürji, mikro elektrik, telekomünikasyon, bilgisayar yazılımları, nano-teknoloji gibi karlılığı yüksek ve sermayesi bilgi olan kavramların sonraki on yılları hızlı bir şekilde etkileyerek gelişmiştir. Bu sektörlerde ağır çalışmayı gerektiren işçi gücü, ya da kilometrelerce uzak mesafelerden getirilmesi gereken hammaddeye gereksinim yoktur. Günümüz katma değerlerini oluşturan beyin gücüne dayalı insan yapımı sanayilerdir.⁸ Yani hammadde gereksinimi sanayideki kadar çok ve elzem değildir. Bu ekonominin temel kavramı bilgidir.

Teknolojik alt yapının durumuna baktığımızda ise mikro işlemcilerin gelişerek her evde masaların üstünde yerlerini aldığı görülmektedir. Teknoloji her geçen gün kendini hızlı bir şekilde yenilmektedir. Her yıl bilgisayarların veya bilgisayarlara bağlı aletlerin sayısında veya özelliklerinde ciddi artışlar kat edilmektedir.

Bir diğer devrim ise 1990’lı yıllarda yaşanmıştır. Bu devrim bilgisayarları birbirine bağlayan bant genişliklerinin akış hızındaki büyüme izledi. Telefon hattı ile bağlantı, uydu üzerinden haberleşme, fiber optik teknolojileri bu değişime paralel hareketlerde bulunmuşlar ve internet kavramının yaygınlaşması yolunda köklü devinimler oluşturmuşlardır. Artık bilgisayarlar arasında iş ve işlemler mekân ve zaman sınırlaması olmaksızın yapılabilirdi. Bu durum telgrafın icadıyla savaş teknolojilerinin hızlı değişmesine benzetilebilmektedir.

Bilgi toplumunun temel niteliklerini aşağıdaki gibi sıralayabiliriz.

⁷ Peter F. Drucker, Peter M. Senge, **Leading in a time of change**, Jossey-Bass : San Francisco, 2001, s.24.

⁸ Lester C. Thurow, **The age of economic exploration**, San Jose: To Excel, 1999, s.12.

- Sanayi toplumunda maddi sermayenin yerini bilgi toplumunda bilgi ve insan sermayesi,
- Sanayi toplumunda mal ve hizmet üretiminde gelişiminin başlangıcı olan buhar makinesinin yerini bilgi toplumunda bilgisayarlar ,
- Sanayi toplumunda kol gücünün yerini, bilgi toplumunda beyin gücü ,
- Sanayi toplumunda fiziksel ve düşünsel anlamda insan sermayesinin üretime katılımı söz konusu iken, bilgi toplumunda düşünsel anlamda, yükseköğrenim görmüş nitelikli insan sermayesinin üretime katılımı, almaktadır.

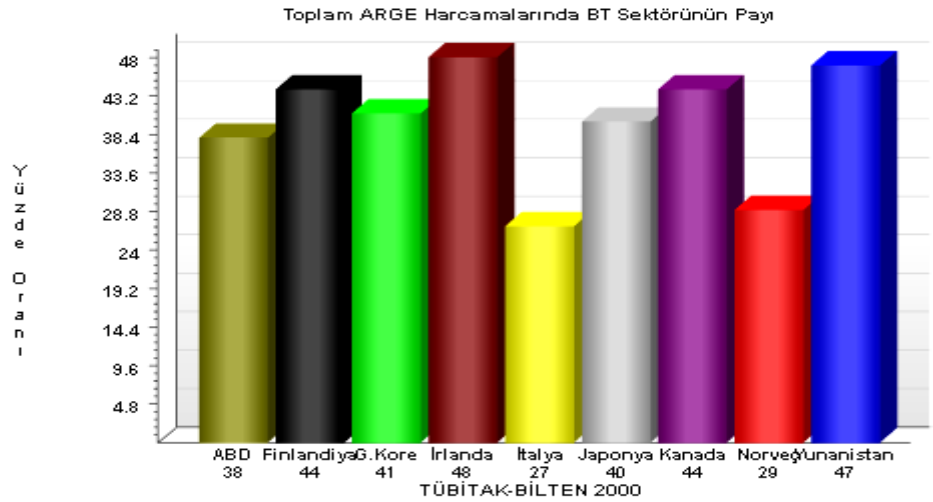
- Sanayi toplumunda sanayi mallarının ve hizmetlerin üretimi yapılmaktadır. Bilgi toplumunda ise bilgi ve teknolojinin üretimi gerçekleşmekte ve bilgi sektörünün ürünü olarak bilgisayar, iletişim ve elektronik araçlar, elektronik haberleşme, robotlar, yeni gelişmiş malzeme teknolojileri gündeme gelmektedir.
- Sanayi toplumundaki fabrikaların yerini bilgi toplumunda bilgi kullanımını içeren bilgi ağları ve veri bankaları (iletişim ağ sistemi) almaktadır. Bilgi, dünyanın her tarafında üretilmekte ve iletişim teknolojisi aracılığıyla anında her tarafa yayılmaktadır.
- Bilgi toplumu işgücünden tasarruf sağlamakta, bu ise kısa dönemde işsizlik, uzun dönemde ise yeni teknolojilerin dünya çapında etkilerini ortaya çıkarmaktadır.
- Sanayi toplumunda; birincil, ikincil ve üçüncül endüstriler tarım, sanayi ve hizmetler, bilgi toplumunda birincil, ikincil ve üçüncül sektörlerin yanı sıra dördüncü sektör olan bilgi sektörü ortaya çıkmaktadır.
- Sanayi toplumundaki özel ve kamu iktisadi kuruluşlardan farklı olarak bilgi toplumunda gönüllü kuruluşların önem kazandığı görülmektedir.

- Sanayi toplumunda başlıca üretim faktörleri emek, tabiat, sermaye, girişimci iken, bilgi toplumunda üretim sürecinde bu üretim faktörlerinin yanı sıra beşinci üretim faktörü teknik "bilgi" ön plana çıkmaktadır.
- Sanayi toplumunda üretilen mal ve hizmetlerin kıtlığı söz konusu iken, bilgi toplumunda bilgi kıt değildir. Bilgi, sürekli artmakta ve artan verimler özelliği içermektedir.
- Sanayi toplumunda üretilen mal ve hizmetlerin bir yerden bir yere taşınmasında uzaklık ve maliyet önemli iken, bilgi toplumunda bilgi otoyolları ile tüketici ile bilgi arasındaki uzaklık önemini kaybetmekte ve maliyetler minimuma inmektedir.
- Sanayi toplumunda temel bilgiyi, fizik, kimya bilimleri, bilgi toplumunda ise; kuantum elektroniği, moleküler biyoloji ve çevresel bilimler gibi yeni araştırma alanlar oluşturmaktadır.
- Sanayi toplumunda politik sistem temsili demokrasi iken, bilgi toplumunda katılımcı demokrasi anlayışının daha belirgin bir önem kazanacağı düşünülmektedir. Bilgi ve iletişim teknolojilerindeki gelişmeler neticesinde adına "Tele-Demokrasi" denilen bir değişimin ileriki yıllarda yaşanacağı tahmin edilmektedir.

Teknoloji ve eğitimin birbirine paralel gelişim gösterdiği toplumlarda internet kullanımı tam manası ile hayatın içine kadar girmiştir. Avrupa'nın en kuzeyinde yer alan ülkelerden biri olan Finlandiya bu konuya örnek olarak gösterilebilir. Finlandiya'da evlerin %60'ında bilgisayar vardır. Finlandiya halkı her türlü devlet işlemlerini, fatura işlemlerini ve günlük hayata dair alış-veriş işlerini, kültürel faaliyetler hakkında bilgilenmelerini, bankacılık işlemlerini internet üzerinden yapmaktadır. Şüphesiz bu alan yapılan yatırım ve verilen önemin büyüklüğünden kaynakladığını söyleyebiliriz. Finlandiya hükümetinin bu durum için ayırdığı bütçe Milli Gelirinin sadece %3'üne tekabül etmektedir. Günümüzde bilgisayarın çok fazla kullanıldığı bu ülkede insanlar

artık iskelet kas sistemini harekete geçirmek ve yürümek için birtakım sporlar bile geliştirmişlerdir.

21. yüzyıl diğer yüzyıllardan farklı bir boyutuyla ön plana çıkmaktadır. İşlem ve dağıtım masraflarını azaltan internet, şirketlerin müşterileriyle ve tedarikçileriyle olan ilişkilerini biçimlendirmektedir. İnternet öncesi dönemde insanlar bir eşyayı ve bir ürünü almak için ilgili mağazalara giderek satıcılarla muhatap olarak alıyorlardı. Şimdi ise durum tamamen değişmiştir. Satın aldığımız ürünü kimden alındığından çok hangi web adresinden alındığını biliyoruz.



Şekil 1-Ülkelere göre Toplam ARGE Harcamalarında BT Sektörünün Payı

Kaynak: Bilgi Toplumuna Doğru, Türkiye Bilişim Şurası, Ankara: Başbakanlık, 10-12 Mayıs 2002, ODTÜ, s.13.

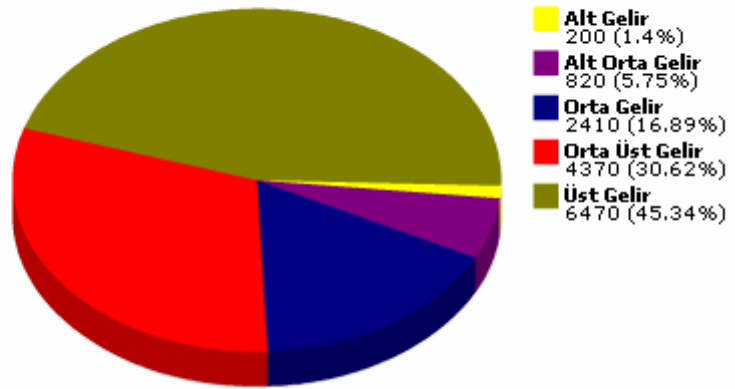
Şekil 1’de toplam Araştırma Geliştirme harcamalarının Bilişim Teknolojilerindeki sektörsel payı gösterilmiştir. En fazla harcamanın İrlanda’da olduğu görülmektedir.

İnternetin getirmiş olduğu yenilikler bilgi çağında, uluslar varlıklarını kanıtlamak için, diğer çağların temel unsurları olan toprak ve işgücü ya da öz sermaye birikimini aşarak, entelektüel varlıklarını ve kültürel değişimlerini, gelişmelerini ön plana çıkarmak durumundadır⁹Özellikle dünyamız son dönemde küresel bir yapıya bürünmüştür. Bu yapının oluşumunda internetin getirmiş olduğu rekabet gücü, bilginin

⁹ Mustafa Gözalan, “Bilgi Yönetimi”,**Bilgi Teknolojilerinin Toplam Kalitede Organizasyon yapısındaki yeri ve Önemi Semineri**, İstanbul: KALDER, 3 Aralık 1996, s.51.

yeniden tanımlanmasına neden olmuştur. Bu da toplumları bilişimin her alanından yeni arayışlara itmiştir. Küreselleşme ile beraber gelen rekabet yenileşme ve farklı arayışlara neden olmuştur. General Electric Genel Direktörü Jack Welch'e göre: "Bugün artık rahatça çalıştığımız hiçbir konu yok. Her alanda ve her bölgede acımasız bir rekabetle karşı karşıyayız. Güvenebileceğimiz tek şey, kendi yeteneğimiz ve rakiplerimize karşı yaratabileceğimiz üstünlüktür."¹⁰

Gelir Gruplarına Göre Evde Bilgisayar Sahipliği /TÜRKİYE



Şekil 2-Türkiye’de, Gelir Gruplarına Göre Evde Bilgisayar Sahipliği

Kaynak: Bilgi Toplumuna Doğru, Türkiye Bilişim Şurası, Ankara: Başbakanlık, 10-12 Mayıs 2002, ODTÜ, s.16.

Şekil 2’de ülkemizde evde bilgisayar sahipliğinin gelir seviyelerine göre oranı incelenmiştir.

Ülkemizde bilgi toplumu olma yolunda son yıllarda ciddi atılımlar atılmış olmasına rağmen gerek evlerdeki bilgisayarlar ve gerekse internet kullanımı son derece yetersizdir. Kamu ve özel sektörde üretilen bilgi ve belgelerin seçimi, toplanması, düzenlenmesi, tanımlanması ve araştırmaya sunulması, kısacası bilgi yönetiminde büyük eksiklikler bulunmaktadır. Bilgi yönetim alanında yetişmiş eğitilmiş insan gücü; bilgi ve belge yöneticisi, kütüphaneci, arşivci, müzeci, bilgisayar mühendisi, çözümleyici, ağ uzmanları gibi meslek dallarında da yeterli bir atılımın yapılmadığı görülüyor.

¹⁰ İbrahim Kavakoğlu, **Değişim ve Yaratıcılık**, İstanbul: Kampus A.Ş. Yayınları, 2000, s.80.

2.2. BİLGİYE ERİŞİM VE KİŞİSEL BİLGİLERİN KORUNMASI

Demokrasi ve şeffaflığın bulunduğu ülkelerin anayasalarında, uluslararası belgelerde ve BM Birleşmiş Milletler Genel Kurulu'nun 10 Aralık 1948 tarih ve 217 A(III) sayılı Kararıyla ilan edilen İnsan Hakları Evrensel Beyannamesinde özel yaşamın gizliliği güvence altına alınmıştır.¹¹ Kişinin izni ve bilgisi olmadan kişi hakkında fiziksel özelliklerini, fikir ve düşüncelerini, vicdan ve inançla ilgili bilgilerini, sağlık, öğrenim, istihdam durumu ile ilgili bilgilerini, fert olarak sürdürdüğü yaşamın mahremiyetini, aile yaşantısını, başkaları ile yapılan haberleşmelerini ifşa etmek, bilgisi dışında bu bilgilere erişmek ya da kullanmak bir ahlak zaafı ve suç unsuru olarak görülmektedir. Aynı zamanda kişinin kendi hakkında verdiği bilginin çarpıtılarak, amaç dışı kullanılması da bu kapsam dâhiline girmektedir.¹²

Bilgi çağında, kişisel bilgilerin yaygın bir şekilde toplanarak işlenmesini kolaylaştırmak ve bunları ilgililerin yararlanmasına sunmak bir zorunluluk haline gelirken, diğer taraftan hakkında bilgi toplanan kişi ve kurumlara ait bilgilerin korunması ve saklanması önemli bir sorun haline gelmiştir. Medeni Kanunun 24. maddesinde kişilik haklarına aykırı bu tür fiil veya faaliyetlere karşı kişiyi koruma vardır.¹³

Fakat son yıllarda kişisel verilerin elektronik bilgi işlem yöntemleri ile derleme, sınıflandırma, saklama işlemlerine tabi tutulması ve istendiğinde istenen biçimde sunabilmesi olanağı ortaya çıkmış ama bunun sonucu olarak özel yaşamla ilgili bu gibi bilgilerin veya teknik deyimi ile kişisel verilerin haksız kullanılması riskini arttırmış, kişinin rızası olmadan başkasına açıklanmasını ve bilginin bulunduğu yerden başka yerlere aktarmayı kolaylaştırmıştır.¹⁴ Hal böyle olunca teknolojinin getirdiği yeniliklere bağlı olarak kişisel verilerin ihlali söz konusu olmuştur.

¹¹ Birleşmiş Milletler, **İnsan Hakları Evrensel Beyannamesi**, 10 Aralık 1948 tarih ve 217 A(III) sayılı Kararıyla ilan edilmiştir. Bakanlar Kurulu Kararı 27 Mayıs 1949 tarih ve 7217 Sayılı Resmi Gazete'de yayınlanmıştır. Madde-12.

¹² 4982 Sayılı, “Bilgi Edinme Hakkı Kanunu”, Kabul Tarihi:09.10.2004, Resmi Gazete Sayısı:25269, Resmi Gazete Tarihi: 24/10/2003.

¹³ İlknur Uluğ, “Sanal Sigortacılık”, **Sosyal Bilimler Araştırma Dergisi**, Yıl:1, Sayı:2, Eylül 2003, s. 230.

¹⁴ Gökçe Üzel (edt.), “Kişisel Verilerin Korunması”, **Bilgi Toplumuna Doğru, Türkiye Bilişim Şurası**, Ankara: Başbakanlık, 10-12 Mayıs 2002, ODTÜ, s.315.

Özel Yaşamın Gizliliğin Korunması Hakkı ile Bilgiye Erişim Özgürlüğü Hakkı birbirine taban tabana zıt kavramlar olarak karşımıza çıkmaktadır. Uygulamada her iki hakkında gereğince güvence altına alınabilmesi ve bu özgürlükleri düzenleyen kurallar konulurken özen gösterilmesi gerekmektedir. Bütün özgürlükler gibi özel yaşamın gizliliği hakkı mutlak olmayıp bazı sınırlamalara tabidir. Diğer bir deyişle diğer bütün özgürlüklerde olduğu gibi kişisel verilerin korunması hakkının kapsamının belirlenmesi ve sınırlarının çizilmesi sırasında bazı ilkelere uyma zorunluluğu vardır. 1990 yılında Birleşmiş Milletler Genel Asamblesi bilgisayarla işlenen kişisel veri dosyaları hakkında yönlendirici ilkeler adını taşıyan belgede bu ilkeleri detaylı olarak incelemiştir.¹⁵ Bu ilkeleri kısaca incelersek;

Yasalara Uygunluk ve dürüstlük: Kişisel veriler kanunlara aykırı yollarla toplanmamalı ve toplanmış bilgiler amaç doğrultusunda kullanılmalıdır.

Doğruluk ve Tutarlılık: Toplanan verileri doğruluğu ve tutarlılığı kontrol edilmeli; bütünlüğü ve güncelliğini sağlamak için saklandığı süre zarfında düzenli olarak kontrole tabi tutulmalıdır.

Haklı ve Belirli Amaçlara Yönelik Olması: Kişisel verilerin hangi amaç uğruna toplanacağı baştan kesin olarak belirlenmeli ve bütün ilgili kişilere açık bir şekilde bildirilmelidir.

İlgili Kişilerin Erişim Hakkı: Kişi kimliğini ispatlamak koşuluyla kendisi hakkında toplanan bilgilerin ne gibi bir işleme tabi tutulduğunu öğrenebilmeli ve bunların bir anlaşılabilir nüshalarını aşırı masraf ve zaman kaybı olmadan elde edebilmelidir.

Ayrımcılıktan Kaçınma: Kişinin kökeni, ırkı, cinsiyeti, dini veya felsefi inançları, cinsel yaşamı ve benzeri gibi konularda bilgiler ancak yasaların izin verdiği haklı ve gerekli durumlarda toplanabilmelidir.

Güvenlik ve Koruma: Kişisel verilerin toplanması, saklanması ve işlenmesi ile görevli bütün kurum ve kişiler, bu verilerin doğal afetler ve kazalar ile insanların

¹⁵ Gökçe Üzel (edt.), s. 317

işleyecekleri hata, kusur ve suçların yaratacağı tehlikelere karşı korunması için her türlü önlemi almalıdırlar.

Denetim ve Yaptırım: Kişisel verilerin korunması ile ilgili düzenlemelerle öngörülen ilke ve kuralların uygulanmasının, önlemlerin alınmasının ve gerekli denetimlerin yapılmasının sorumluluğu tarafsız, yetkin ve adil bir makama verilmelidir.

Uluslararası Veri Aktarımı: Kişisel verilerin saklanmakta olduğu ülkeden başka bir ülkeye aktarılması için her iki ülkenin ulusal mevzuatlarının bu aktarma işlemine izin vermesi yanında bu veriler için, verinin gönderileceği ülkeni bu veri için sağladığı korumanın verinin bulunduğu ülkede sağlanan korumadan daha aşağı düzeyde olmaması da gerekir.¹⁶

Şahsiyet hakkı, kişinin hayatı, vücut tamlığı, sağlığı, şeref ve haysiyeti, ismi, resmi, hürriyeti, özel hayatı ve sırları, kısacası tüm kişisel değerleri üzerinde söz konusu olan mutlak bir haktır.¹⁷ Yukarıda bahsedilen günümüzün hızlı gelişen teknolojisi ve toplum hayatındaki değişimler, her türlü ihlale açık olan kişilik hakkının korunmasının önemini giderek arttırmaktadır.*

Bunun en net görüldüğü yer şüphesiz internettir. İnternet bu bahsedilen ihlalleri artıran ve hızlandıran bir etkiye sahiptir. İnternet sitelerinde yazı ve resim yoluyla kişinin gerek şeref ve haysiyeti ve gerekse de özel hayatı, sırları ihlal edilebilmektedir. Günlük gazeteler gecedan basılıp dünün haberini ya da gündemini aktarıken elektronik ortamda çıkan gazeteler anında her haberi dakikalarla kitlelere ulaştırabilmektedir. Başka amaçlarla oluşturulan web sitelerinde de şahsiyet hakkını ihlal edecek, özellikle reklâm amacıyla resmin yayımlanması ve benzeri yayınların yapıldığı görülmektedir. Bunlara ek olarak elektronik posta yoluyla da şahsi varlıklara yönelik saldırılar gerçekleşebilmektedir. İnternet yoluyla şahsiyet hakkı ihlali çok çeşitli şekillerde gerçekleşebilmektedir.¹⁸ Elektronik posta göndericinin bilgisayarı tarafından

¹⁶ Gökçe Üzel (edt.), s. 319

¹⁷ Yaşar Karayalçın, “Türk Hukukunda Şeref ve Haysiyetin Korunması”, **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, CXIX, n.1-4, 1962, s. 251-253,274.

* “Kişilik hakkının korunması, bir şahsın kişiliğine üçüncü kişiler tarafından yapılabilecek hukuka aykırı tecavüzleri önlemeye, yok etmeye, tanzim etmeye yönelik özel hukuk kurallarının bütünüdür.”

¹⁸. **97/7 Sayılı Tüketicinin Korunmasına Dair AT Yönergesi**, http://www.turkhukuk sitesi.com/makale_168.htm (23 Haziran 2008)

bir mail/server aracılığıyla alıcının mail servisine iletilir. Alıcının genellikle bir elektronik posta alma protokolü vardır.¹⁹ Bu şekilde ulaşan e-posta, alıcının mail sunucusu tarafından yine alıcının mail kutusuna konur. Bunların en başında elektronik posta yoluyla ve web sitesi yoluyla gerçekleştirilenleri görebiliriz. Elektronik ortamda gerçekleşen ihlallere kısaca incelersek;

a)Mail Adresine gönderilen e-postalar: Bir kişi kendi e-mail adresini, göndericiye vermediği halde, kişinin şahsiyetine, şeref ve onuruna, sırlarına ya da özel yaşamına dair elektronik posta gönderilebilir. Benzer şekilde, bir kimse, e-posta adresine gönderilen ve doğrudan şahsiyetine yönelik olmamakla birlikte rahatsız edici haber, reklâmlarla da taciz edebilir. Bu göndericiler kişinin mail adresini ortak forumlardan, bilgi bankalarından elde edebilir. Bu tür gönderilere spamming ya da spam adı verilir.²⁰ Bununla birlikte gönderilen e-postalar sadece reklâm mahiyeti taşımayabilir, bazı durumlarda bozuk dosya formatları ile alıcının bilgisayarına zarar veren virüsler gönderilir. Son olarak başka bir kişinin özel hayatını ilgilendiren fotoğraf, metin ya da ses dosyaları da bu yolla ifşa edilip gerçek veya tüzel kişileri rencide edici dosyalar gönderilebilmektedir.

b)Web Sitesi Yoluyla Gerçekleştirilen ihlaller: Web siteleri yoluyla kişilik hakkı ihlali internette önemli bir yer tutmaktadır. Kişi hakkında herhangi bir yazı, resim veya ses dosyası kişiyi rencide edici, özel yaşamına müdahil bir şekilde kullanılabilir. Bu durum reklâm amacıyla da kullanılsa da aynıdır. Mevzu bahis olan kişinin herhangi bir izni olmaksızın yapılan bu tür eylemler son zamanlar artış göstermiş, hacker olarak tanımlanan kötü niyetli kişiler tarafından bazı eylemler internette vuku bulmuştur. Kişisel hakların internet yoluyla ihlali olarak link ve frame yolu gösterilebilir.* Bu yolla gerçekleşen ihlallerin basın medya yoluyla gerçekleşen ihlallerden temel nitelik olarak pek bir farkı yoktur.

¹⁹ Yargıtay Dergisi ,“İnternet Üzerinde yapılan hukuki işlemler”, c.27, 2001, s. (749-788), 760-761.

²⁰ Atatürk Üniversitesi Hukuk Fakültesi Dergisi, “Tüketicinin Korunması Hakkında Kanunun 16-17 ve Medeni Kanunun 24-25. maddeleri”, c.5., s.1-4.

* Link, ekran üzerinde görüntüsü olan bir web sitesinden diğer web sitesine bağlantıdır. Frame ise başka bir web sitesinin içeriğinin kısmen ekran üzerinde görünmesi ve kalan kısmın asıl site üzerinde bulunmasıdır.

Bu temel ihlallerin dışında bir kişiye ait ismin internette alan ismi olarak tescil ettirilmesiyle gerçekleşen ihlaller gösterilebilir. Bu durumda gerçek kişi sanal ortamda kendi adına alan ismi alamayacaktır.** Bir başka ihlalde bir kimsenin adı, soyadı, yaşı, cinsiyeti, medeni durumu, ailesi, işi, adresi, e-posta adresi, geçirdiği hastalıklar, nitelikleri, hobileri, fobileri ve benzeri bilgileri kişinin şahsi bilgilerini oluşturur. Bu bilgiler kişinin ilgili formu doldurması ile alakalı şirket tarafından arşivlenebilir. Fakat üçüncü bir şahısa ya da başka bir firmaya satılması, sunulması ya da güvenlikten kaynaklanan sebeplerle zikredilen şahıs veya firmalara verilmesi de kişilik haklarının ihlali olarak sayılabilir.

Sonraki bölümlerde gelecek olan sözleşme, antlaşma kavramları ve elektronik olarak gerçekleşen iş ve işlemlerde, yine kişilik haklarına yapılan saldırı ve ihlallere benzer durumlar olabilme ihtimali 2000’li yıllarda yeni bir anlayışın doğmasına neden olmuştur. Zaten bilgisayar sektörünün ileri gelenlerinin kitaplarında ya da demeçlerinde de sık sık belirttiği gibi; bilgisayar teknolojisini insan yaşamının her alanına yerleştirmek ve bilgisayarlı yaşamı insan hayatında etkin ve etkili bir şekilde kullandırmaktır. Microsoft’un patronu ve dijital çağın dahi çocuğu olarak tanımlanan Bill Gates’e göre “Hayat bütün bu değişikliklerden sonra oldukça ilginçleşecek. Bütün bu değişikliklerin on yıl alacağını tahmin ediyorum. O günün dünyası şimdi yaşadığımızdan çok farklı olacak. Microsoft’un bütün hayali bütün bu dijital aletler arasında bağlantı kuracak bir yazılımı tasarlamak ve insanlara Web tarzı yaşama dayalı dijital çözümler üretme fırsatı tanımaktır.”²¹

2.3. ELEKTRONİK KAVRAMLAR (E-EKONOMİ, E-DEVLET)

Bilgi Teknolojilerindeki gelişim 2000’li yılları şekillendiren önemli gelişmeleri gözönüne koymaktadır. Bilgi saklama ve paylaşma bilgi teknolojileri ile kolaylaşmış ve hızlanmıştır. Yazı, ses ve görüntü sayısal biçime dönüştürülerek saklanmakta, işlenip kullanılmaktadır. Bu olanaklardan faydalanan insanlar, şirketleri, şirketler birbirleriyle olan ilişkilerini değiştirmektedir. Kişi ve kuruluşların ilişkilerinin değişmesi ise,

** Ticaret unvanı kişilik hakkı kapsamında yer almadığı için, bir ticaret unvanının alan ismi olarak alınması kişilik hakkını değil, gayri-maddi mallar üzerindeki hakkı ihlal eder. Bu konuda dünyaca ünlü bir içecek firmasını internetin gelişim göstermeye başladığı dönemlerde kendi ismiyle kurulmuş sitesini fahiş bir fiyata satın almak zorunda kalmıştır.

²¹ Gates, 1999, s.78

toplumsal ve ekonomik hayatta bilgi toplumuna ve bilgi tabanlı ekonomiye doğru önemli deęişikliklere yol açmaktadır.

Geleneksel anlamda ekonomide şirketlerin rekabet avantajlarını belirleyen ve stratejilerinin şekillenmesinde etkili olan şartlar e-ekonomi ortamında deęişmiştir. Geleneksel anlamda rekabet kavramı şirketler arasında gerçekleşirken, elektronik ortamda yakın ilişki içinde çalışan ağlar, tedarik ve dağıtım sistemleri arasında rekabeti gündeme getirmiştir.

Tablo 1-Geleneksel Ekonomi ve E-Ekonominin Mukayesesi

	GELENEKSEL EKONOMİ	E-EKONOMİ
Ekonomi Özellikleri		
Pazar	Statik	Dinamik
Faaliyet Alanı	Ulusal	Küresel
Organizasyon	Bürokratik, Hiyerarşik	Çalışma Ağı, girişimci
İşin coğrafi hareket kabiliyeti	Düşük	Yüksek
Bölgelerarası rekabet	Düşük	Yüksek
Endüstri		
Üretim Yöntemi	Kitle üretimi	Esnek Üretim Kabiliyeti
Temel üretim faktörleri	Sermaye, işgören	Yenilik, Bilgi
Kritik teknolojik faktör	Mekanizasyon	Dijitalleşme
Rekabette avantaj kaynağı	Maliyet	Yenilikçilik, kalite, Pazar, maliyet
ARGE faaliyetleri	Orta	Yüksek
İş Gücü		
Hedef	Sürekli İş	Yüksek ücret ve gelir
Beceriler	İşe odaklılık	Geniş kapsamlı beceriler
İşveren-yönetim ilişkileri	Rekabet	Birlikte çalışma
İstihdam Özelliği	Sabit	Risk ve fırsatlarla donatılmış

Kaynak: Kaynak: Bilgi Toplumuna Doğru, Türkiye Bilişim Şurası, Ankara: Başbakanlık, 10-12 Mayıs 2002, ODTÜ, s.16.

Tablo 1’de Geleneksel Ekonomi ile Elektronik ekonomi arasında farkları gösterir tablo bulunmaktadır.

Geleneksel ekonomi şirketleri üretim faaliyetlerine bağlı olarak hammadde ve alan, işgücü eksikliğiyle karşı karşıya kalabilmektedirler. Neticesinde kaynaklar daha fazla harcama gerektirmekte ya da daha düşük kalitede kaynaklara yönelmesine yol

açmaktadır. Ekonomik açıdan ulus devletler, sanayi devriminin ürünüdürler ve bu açıdan işlevlerini tamamlamış bulunmaktadır. Gelecekte belki tamamen bu kavram ortadan kalkmayacaktır ama gücünden çok şeyler kaybedecektir.²²

E-ekonomide yatırımcılar ilk ürünlerini çıkarabilmek için servetler harcarlar. Ancak sonraki seri üretimler çok düşük maliyete yapılır. Microsoft'un ilk Windows 95 disketi 300 milyon dolara mal olmuştur; ancak ikincisinin maliyeti birkaç sent ve kullanım kılavuzunun tekrar basılmasından oluşturmaktadır. Dünyanın evrensel bir köy haline geldiği, Gutenberg Galaksisi'nin yeni baskı tekniğinin yerine, görüntünün egemenliğini ilan ettiği bir ortamda; kitap kültürünün yerini görüntü kültürü almıştır²³

E-ekonominin olanaklarına baktığımızda ürün ve hizmetlerin üretim ve dağıtım maliyetlerini azaltmak olduğunu, internet tabanlı uygulamalarla bilgi paylaşımını daha esnek, hızlı ve ucuz bir şekilde gerçekleştirildiğini görüyoruz. Başka bir olanak iletişimi ve işbirliğini hızlandırmak ve artırmak olduğunu, diğer bir olanak da şeffaflığı ve rekabeti arttırmak olduğunu görüyoruz. Aynı zamanda e- ekonominin yeni şirket modellerini beraberinde getirdiğini ve yeni yönetim şekillerini ortaya çıkardığını da söyleyebiliriz. Müşterilere sunulan hizmetin çeşitliliği ve müşteri ihtiyaçlarının hemen çözüme kavuşturulması da elektronik ekonominin diğer olanakları arasında sayılabilir.

E-ekonomide yapılanmasında devletlerin yeni rolüne baktığımızda bilişim altyapısına, dünya standartlarında eğitim ve öğretime, Bilgi Teknolojisine, devlet hizmetlerinin dönüşümüne yatırım yapmasına gereksinim duyulmaktadır. Elektronik ekonominin yapılanmasında devletin üstleneceği yeni rolün getireceği şartları ve durumları şöyle sıralayabiliriz.

- Hızlı ekonomik büyüme, yüksek verimlilik, fırsatların artırılmasının ve yaşam kalitesinin yükseltilmesini gerektirmektedir.
- Ekonomik gelişmeyi tetikleyen ve sürükleyen en başlıca faktör bilim ve teknolojidir. Kaliteli eğitim ve öğrenim, örgütlülük, yaratıcılık,

²² Alvin Toffler, **Ekonominin Çöküşü**, İstanbul: İnsan Yayınları, 1991, s. 90.

²³ Rıdvan Karluk, **Küreselleşen Dünyada Uluslararası Ekonomik Kuruluşlar ve Entegrasyonlar**, Eskişehir : [y.y.], 1995, s.2.

rekabet gücü ve küresel açık ticaret elektronik ekonominin gelişim sağlaması yolunda önemli duraklardır.

- Kamu yönetimi ihtiyaç duyduğu kamusal destek için etkileşimde olacağı yeni ekonomi ve toplum düzenine uyumlu, hızlı, etkin ve aktif bir yapıda olmalıdır. Gelişmelere yakından ve hızlı bir şekilde takip edebilecek, duyarlı ve esnek olabilecek ve yeniden tanımlanıp yapılandırılacak bir doğrultuda ilerlemelidir.
- Teknoloji ve yaratıcılığın getirdiği kazanımların, artı değerlerin tüm topluma eşit olarak dağılımı sağlanmalıdır.

Elektronik devlet kamuya ait bilgiler ulaşılmasında ve vatandaşlara, işletmelere, kurum çalışanlarına, diğer birim ve kuruluşlara kamu hizmetlerinin sunulmasında teknolojinin ve özellikle de web tabanlı internet uygulamalarının kullanılması olarak tanımlanabilir.²⁴ Devletin elektronik ortama geçişinin sağlayacağı faydalar aşağıdaki gibi sayılabilir.

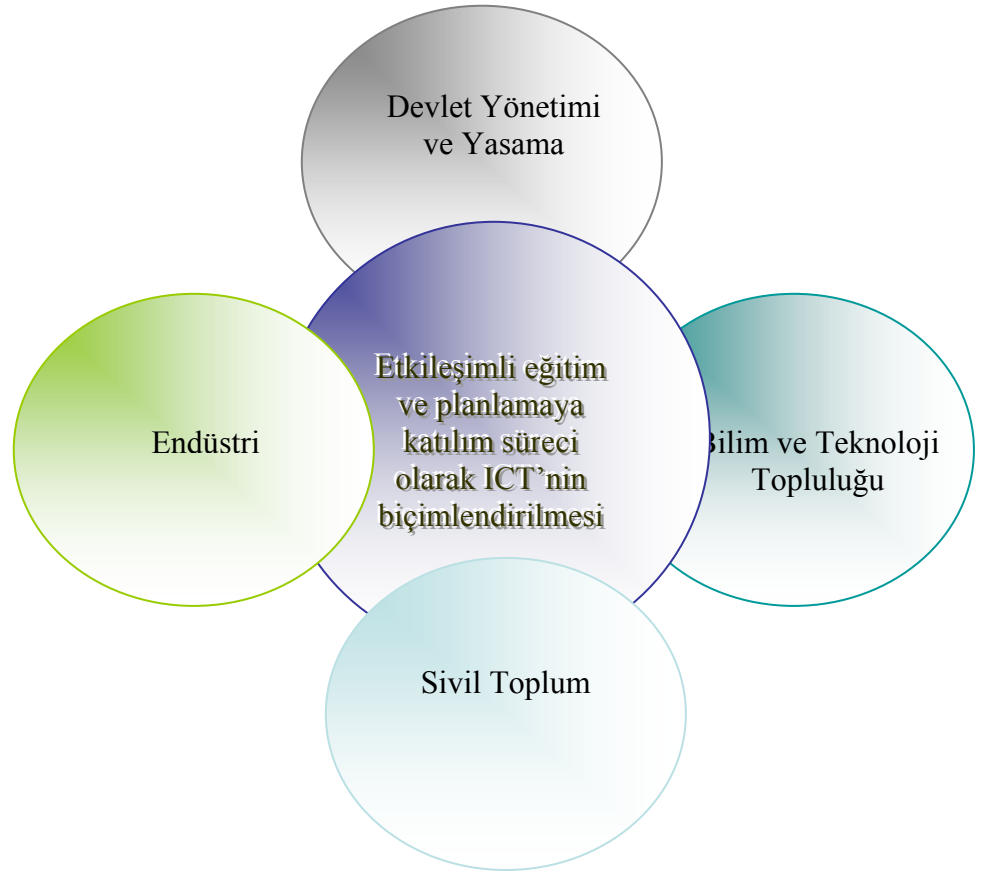
- Her türlü bilgiye erişim olanağının tanınması *
- Kâğıt ortamından kurtularak, bilgilerin hem daha etkin hem de tekrar kullanılabilir ortamlarda saklanması
- Harcamalarda tasarruf ve kontrol hatalarının azalması
- Kamu hizmetlerinin belli bir kalite düzeyinde herkesçe eşit olarak ulaştırabilmesi, evrensel erişim ilkesi
- Haftanın yedi günü, 24 saat hizmet verebilecek mahiyette, işlem süreleri kısa ve verimliliğin fazla olması.

²⁴ Hasan Gül, “Kamu Kuruluşlarında Elektronik Hizmetlerin Yaygınlaştırılması (E-Devlet)”, **Maliye Dergisi**, Sayı :140, 2002,s.15-46.

* Bu noktada her türlü bilgi vatandaşın ya da ilgilinin bilgiye ulaşmasında devlet menfaatleri açısından herhangi bir sınırlama olmamasıdır. Bilgi edinme kanunu çerçevesinde bilgi edinme hakkı söz konusudur. Bilgi edinme kanunuyla herhangi bir netice alamaması durumunda ise Bilgi Edinme Yüksek Kuruluna müracaat ederek yeni bir netice beklenebilir. Ancak devletin, devlet sırrı olarak tanımladığı ya da şahısların bilgiyi görmesinde mahsur, zarar olabileceğini düşünülen ve kanunla muhafaza altına alınan bilgiler bu kapsam dışındadır.

Ayrıca e dönüşüm çerçevesinde kamuda vergi sisteminde vergilerin beyanı, tahsili ve veri çözümleme olanaklarının artarak daha etkin ve adaletli bir vergi toplanması düzenine geçilmesi, çifte vergilendirmelerin önlenmesi gibi pratik çözümler bulunmuştur. Mükellefler Elektronik beyanname ile daha etkin ve hızlı bir şekilde iş ve işlemlerini yapabilmektedir. ABD’de EFTP (Electronic Federal Tax Payment) olarak adlandırılan sistemin varlığıyla, ABD’de federal vergilerin kâğıt esaslı geleneksel vergi ödeme yöntemleri yerine, internet gibi elektronik ortamda ödenmesine izin verilmektedir.²⁵Türkiye’de de tam manası ile olmasa da benzeri uygulamalar mevcuttur. SSK’nın prim ödemeleri internet üzerinden yapılmaktadır. Kamu hizmetlerinin internet aracılığıyla verilmesi toplumunda hazır olması gereken bir dönüşümdür. Bu dönüşüm ülkemizde 2000’li yıllarda ivme kazanmış ve hala dönüşüme devam edilmektedir. Ayrıca devlet, yapacağı Bilgi Teknolojileri yatırımları ve dönüşümleri için tasarruf ederek, bu kaynakları projelere aktarabilecektir. Kamusal enformasyon gereksinimi dikkate alındığında bu hizmetlerin çeşitli olduğunu görülmektedir.

²⁵ Yener Özel, “Vergilerin elektronik ortamda ödenmesinde Amerika Birleşik Devletleri Uygulaması”, **Yaklaşım Dergisi**, Sayı: 107, 2001, s.122-124.



Şekil 3- ICT'nin biçimlendirilmesi sürecinde etkin olabilecek bileşenler

Kaynak: Bilgi Toplumuna Doğru, Türkiye Bilişim Şurası, Ankara: Başbakanlık, 10-12 Mayıs 2002, ODTÜ, s.136.

Şekil 3'te e-ekonomi yapılanması içinde geçerlilik taşıyan temel aktörler sınıflandırılmıştır. Bu temel aktörler: Devlet Yönetimi ve Yasam, Bilim ve Teknoloji topluluğu, Endüstri, Sivil Toplum kuruluşları başlığı altında toplanmaktadır.

3.BÖLÜM-ELEKTRONİK İMZA

İnternet üzerinde yapılan işlemlerde, özellikle elektronik ticaret uygulamalarında, en çok ihtiyaç duyulan şeylerin başında güvenlik gelmektedir. Zaman içinde elektronik ortamda el yazısı ile imza yerine geçebilecek kadar güvenilir bir mekanizma kullanılmak üzere düzenleme arayışlarına gidilmiştir. Böylece internet üzerinden yollanan bilgilerin güvenilirliğinin sağlanması, bilgilerin, güvenli ve değişmeden, aynı zaman hukuki koruma sağlayıcı nitelik kazanarak yerine ulaşması gibi amaçlarla teknik çalışmalara başlanmıştır. Elektronik imza altyapısı, elektronik belgenin şifrelenmesini mümkün kılmakta, değiştirilmesini önlemekte ve ayrıca birden çok kişi ile mesajın şifrelendiği anahtar kelimeyi öğrenmelerine gerek kalmadan, elektronik yoldan haberleşmeyi kolaylaştırmaktır²⁶. Gerçekten de elektronik imza elektronik ortamda ihtiyaç duyulan, özellikle elektronik ticaret için zorunluluk arz eden güvenli bir ortam ihtiyacını karşılamayı amaçlamaktadır. Elektronik imzanın birçok çeşitleri bulunmakta olup bunlardan sayısal imza, düşük maliyeti nedeniyle dünyada en çok kullanılandır²⁷. Sayısal imza, açık anahtar altyapısını kullanarak gerek imzalama gerek şifreleme işlemlerini güvenli bir şekilde yerine getirmektedir. Açık anahtar altyapısı mimarisinde biri imza doğrulama işlevi gerçekleştiren “açık anahtar²⁸”, diğeri imza oluşturmaya yarayan “özel anahtar” olmak üzere iki anahtar kullanılmaktadır. Hangi anahtarın kime ait olduğunu elektronik ortamda kimlik tespiti açısından önem arz etmektedir. Bu görev sertifika otoriteleri tarafından yerine getirilmektedir. Sertifika otoriteleri kişinin açık anahtarı ile kimlik bilgilerini bir araya getirerek adeta elektronik ortamda nüfus kağıdı çıkarırlar. Bu sertifikaları her an ulaşabilecek şekilde tutarlar. Sertifikaların yaşam döngülerini sağlar, gerektiğinde iptal ederek bunlara ilişkin bilgileri de saklarlar.

3.1. ELEKTRONİK İMZA- SAYISAL İMZA KAVRAMLARI

Elektronik imza, her türlü elektronik ses, sembol veya uygulamayı kapsayan ve kullanılan teknolojiden bağımsız bir terim olduğundan bir üst kavram olarak kabul

²⁶ Leyla Keser Berber, “Şekil ve Dijital İmza”, **Elektronikteki Gelişmeler ve Hukuk**, Ankara, 2001, s. 503-556.

²⁷ Mehmet Emin Özgül, “İnternette Hukuki Güvenlik ve Dijital İmza”, [t.y.], <http://inet-tr.org.tr/inetconf8/program/141.html>, (05 Kasım 2007)

²⁸ 5070 Sayılı, “Elektronik İmza Kanunu”, Kabul Tarihi:15.01.2004, Resmi Gazete Sayısı:25355, Resmi Gazete Tarihi:23.01.2004, Madde-3/f.

edilir²⁹. Ancak sayısal imza kavramı yerine kullanıma rastlamak da mümkündür³⁰. Elektronik imza kavramı çok genel bir tanım olup; kişilerin elle atmış olduğu imzaların tarayıcıdan geçirilmiş hali olan sayılaştırılmış imzalar, kişilerin göz retinası, parmak izi ya da ses gibi biyolojik özelliklerinin kaydedilerek kullanıldığı biyometrik yöntemleri içeren elektronik imzaları veya bilginin bütünlüğünü ve tarafların kimliklerinin doğruluğunu sağlayan sayısal imzaları da içermektedir. Elektronik imza, veriyi gönderenin ve alanın kim olduğunun kanıtlanmasına imkân tanır. Dolayısıyla imzalanmış bir belgeyi yollayan kişi onu yolladığını, alıcı da aldığını inkâr edemez. Böylece elektronik imza, elle atılan imzanın elektronik ortamdaki karşılığını oluşturmaktadır. Elektronik imza, kapsamlı bir güvenlik teknolojisinin verilerde değişiklik yapılmasını önleyen veya bu verilerde değişiklik yapılması durumunda bu değişikliğin gerçekleştiğini anlamamızı sağlayan sistemdir. Elektronik imza aynı zamanda Adli Tıp incelemesinin ortaya koyduğu sonuçları da yani verinin orijinini bir başka deyişle elektronik imzalı olarak veriyi kimin oluşturduğunun da tespitine olanak verir³¹. Başka bir tanıma göre elektronik imza, klasik imzaya tanınan işlevleri de kapsayan ve bir veri mesajında bulunan veya ona eklenen ya da mesaj ile mantıksal bağlantısı kurulabilen, bireyin kimliğini tanıtan ve bireyin, mesajın içeriğini onayladığını gösteren elektronik formattaki imzadır³². Elektronik imza; elektronik imza sahibi, nitelikli elektronik sertifika hizmet sağlayıcıları, güvenli elektronik imza doğrulama araçları ve nitelikli elektronik sertifika kavramları ile anlamını bulmaktadır. 13 Aralık 1999 tarihli Avrupa Birliği Direktifinde elektronik imza, doğrulama yöntemi olarak hizmet veren ve başka bir elektronik veriye eklenmiş veya mantıksal olarak ilişkilendirilmiş elektronik biçimdeki veri olarak tanımlanmıştır. 5070 Sayılı Elektronik İmza Kanununda elektronik imza, “*Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri*” şeklinde tarif edilmektedir (m.3/b). Elektronik imza ile sayısal imza aynı şey değildir. Bugün sanal ortamda bağlayıcı işlem yapma olanağını sağlamaya çalışan diğer bir elektronik imza tekniği ise, sayısal imza veya diğer adıyla dijital

²⁹ Mustafa Alkan, “Türkiye Elektronik İmza Kullanımına Hazır Mı?”(Görüşme), **Telekom Dünyası Dergisi**, Şubat 2004, s.8-18.

³⁰ *Sayısal İmza*, www.turkpoint.com/e-yasam/sayisal-imza.asp, (01 Aralık 2006)

³¹ Alkan, “Türkiye Elektronik İmza Kullanımına Hazır Mı?”, s.12.

³² Saadet Arıkan, **Dünyada ve Türkiye’de Elektronik Ticaret Çalışmalarına Hukuki Bir Yaklaşım**, [y.y.]: [yy. y.], Ankara, 1999, s. 151.

imzadır. Sayısal imza teknik olarak bir yazılımdır³³. Sayısal İmza, genel anlamıyla kimliğini ve ekli bilgiye onay verildiğini göstermek niyetiyle bir tarafından (veya onun namına) kullanılan herhangi bir işaret veya kabul edilen herhangi bir güvenlik usulüdür³⁴. Sayısal imza, elektronik imza türlerinden biridir³⁵. Sayısal imza, bir mesajın; imzalayanın açık anahtarına karşılık gelen bir özel anahtar kullanılarak oluşturulup oluşturulmadığı ve başlangıçtaki mesajın dönüşüm esnasında değiştirilip değiştirilmediğinin asimetrik şifreleme sistemi ve başlangıçtaki mesaja sahip olan kişi ve imzalayanın açık anahtarının tam olarak saptanabildiği bir “hash fonksiyonu” kullanılarak dönüştürülmesidir³⁶. Sayısal imza, daha geniş ve genel olan ve umumiyetle bir elektronik ispat yöntemi olarak kullanılan “*elektronik imza*”dan farklıdır. Elektronik imza, bir elektronik posta mesajının “*Kimden*” satırında yer alan bir isim, bazı perakende elektronik sistemlerinde kullanılan el yazısı imzanın sayısallaştırılmış hali veya el ile atılan kağıt tabanlı imzanın bir elektronik türü olabilir. Kıymetli evrak niteliği taşıyan bir belge, kıymetli evrak hukukunun şekil şartlarını karşılayan bir sözleşme türü olduğu gibi, sayısal imza da bir açık şifre altyapısı içinde yerleşik asimetrik şifrelemenin şekle ilişkin şartlarını gerekli kılan bir elektronik ispat metodudur³⁷. Sayısal imzada, kişinin ıslak imzasının elektronik ortama kopyalanması söz konusu değildir. Aksine, elektronik ortamda oluşturulan belgelerin asimetrik anahtarla şifrlenmesi esasına dayanmaktadır³⁸. Sayısal imzanın işlevi elektronik ortamda aslından ayrılması güç olan sahte imzayı önlemek ve orijinal belgelerin olduğu şekilde, herhangi bir tahrip ve tahrife uğramaksızın iletilmesini sağlamaktadır³⁹. Bu nedenle sayısal imza, elektronik ortamın vazgeçilmez unsurlarından birisidir denilebilir. Sayısal imza, kişinin el yazısı ile attığı imzanın sahip olduğu özellikleri elektronik ortamda gerçekleştirmeye çalışan matematiksel formüllere veya şifreleme programına verilen bir isimdir. Bugün için sayısal imza, internette işlem güvenliğini sağlamak için

³³ Zarife Şenocak, “İnternette Kurulan Açık Arttırma ile Satım Sözleşmesi”, **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, C.50, Sayı:3, 2001, s.112.

³⁴ Tarık Mete Çanga, “Elektronik İmza ve Elektronik İmza Yasa Çalışmaları”, www.etkk.gov.tr/hukuk.htm, (7 Kasım 2006).

³⁵ Şenocak, 2001, s. 98.

³⁶ Jane K. Winn, çev. Hayri Bozgeyik, Hüseyin Altay, “Bagajsız Kuryeler: Kıymetli Evrak ve Dijital İmzalar”, “E-Akademi Hukuk”, *Ekonomi ve Siyasal Bilimler Aylık İnternet Dergisi*, Sayı:17, Temmuz, 2003, <http://www.e-akademi.org>, (24 Haziran 2007)

³⁷ Winn, pragraf. 42. <http://www.e-akademi.org>, (24 Haziran 2007)

³⁸ Şenocak, s. 98.

³⁹ Leyla Keser Berber, “İmzalıyorum O Halde Varım- Dijital İmza Hakkındaki Yasal Düzenlemeler, Dijital İmzalı Belgelerin Hukuki Değeri”, **Türkiye Barolar Birliği Dergisi**, Ankara, Sayı: 2, Y.13., 2000, s. 503.

en çok tercih edilen bir elektronik imza çeşididir⁴⁰. Açık anahtar altyapısı, sayısal imzanın oluşturulmasında, kullanılmasında çok önemli rol oynamaktadır. Aşağıda açıklanacağı üzere, imzanın oluşturulmasında ve doğrulanmasında kullanılan açık ve özel anahtarlar ile açık anahtarın kime ait olduğunun belgesi sayılan elektronik sertifika ve bu sertifikaların üretilmesi, yönetilmesini sağlayan elektronik sertifika hizmet sağlayıcıları (ESHS) sayısal imzanın unsurlarını oluşturmaktadır. Elektronik imzalar, uygulamalı matematiğin mesajları anlaşılabilir formlara çeviren bölümü yardımıyla kriptoloji yolu ile oluşturulurlar. Elektronik imzada kullanılan anahtarlar, bir kriptoloji algoritması ile üretilir. Sonucun güvenilir olması için bu sürecin belli standartlarla desteklenmesi gerekir. Avrupa Konseyi ve Avrupa Parlamentosunun 13 Aralık 1999 tarih ve 1999/93/EC sayılı direktifi ile elektronik imza ile ilgili esaslar belirlenmiştir. Ek II – f maddesinde nitelikli sertifika verecek olan sertifika hizmet sağlayıcılarının değişikliklere karşı korunmuş olmaları, destekledikleri işlemlerin teknik ve kriptolojik güvenliği garanti edilen güvenilir sistemler ve ürünler kullanımları şart koşulmuştur⁴¹.

3.2. ELEKTRONİK İMZA VE DAYANDIĞI TEMELLER

En genel tanımıyla elektronik imza, elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veridir. Bu tanımda elektronik imzanın en önemli üç unsuru ifade edilmektedir. Buna göre; elektronik imzanın elektronik veriden ayrı olduğu ve ona eklenmesi, ikinci olarak eklendiği veriyle mantıksal bağlantı kurulması, üçüncü olarak, veriye eklenen ve eklendiği veriyle mantıksal bağlantı kurulmasının kimlik doğrulama amacıyla yapıyor olmasıdır. Burada sözü edilen mantıksal bağlantı, imza anında metnin tamamından oluşturulan ve ileride açıklanacak olan hash değerini ifade etmektedir. Tabi ki bu açıklama günümüzde uygulamada yaygın olarak kullanılan sayısal imzanın işleyişi dikkate alınarak yapılan bir yorumdur. Elektronik imza; genel, belirli bir teknolojiye bağlı olmayan (technology neutral) ve elektronik bir kaydın bütünlüğü ve doğruluğunun ispatı ile kaydın sahibi arasında ilişki kurmak için

⁴⁰ Keser Berber, “Elektronik İmzanın Düzenlenmesi Hakkında Kanun Tasarısı Hükümlerinin Değerlendirilmesi” http://www.hukukcu.com/bilimsel/kitaplar/e_imza_tasari_elistiri.htm, (25 Ekim 2006)

⁴¹ Telekomünikasyon Kurumu, E-İmza Ulusal Koordinasyon Kurulu (UKK) Bilgi Güvenliği ve Standartlar Çalışma Grubu İlerleme Raporu, http://www.tk.gov.tr/eimza/doc/diger/eimza_bgs_taslak_raporuV1.2.pdf, (18 Aralık 2007), s.4-26

kullanılan tüm metotlara verilen genel bir isimdir⁴². İmza, kişinin kimliğini, hüviyetini gösteren, onu belirleyen ve diğer kişilerden ayıran bir işaret⁴³ olarak tanımlandığına göre, elektronik imzanın da, başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik işaret şeklinde tanımlanması mümkündür. Elektronik imza, A.B.D Küresel ve Ulusal Ticarete Elektronik İmza Yasası'nda (Electronic Signatures in Global and National Commerce Act) bir sözleşmeye doğrudan eklenmiş yada mantıksal bağlantı kurulabilen ve kaydı imzalamak niyetini güden kişi tarafından oluşturulmuş veya kullanılmış, her türlü elektronik ses, sembol yada kayıt⁴⁴ olarak tanımlanmaktadır. Elektronik imza, United Nations Commission on International Trade Law (UNCITRAL) Birleşmiş Milletler Uluslar arası Ticaret Yasası Komisyonu tarafından hazırlanan Elektronik İmzalar İçin Yeknesak Kurallar Taslağı'nda *“veri mesajını imzalayanı ve imzalayanın mesajın içeriğindeki bilgiyi kabulünü belirlemek için kullanılabilen, bir veri mesajına ekli veya mantıken onunla ilişkilendirilmiş elektronik şekildeki veri”* şeklinde tanımlanmaktadır⁴⁵. ETKK Hukuk Çalışma Grubu raporlarında elektronik imzanın tanımı şu şekilde yapılmıştır: *“Bir bilginin üçüncü tarafların erişime kapalı bir ortamda, bütünlüğü bozulmadan (bilgiyi ileten tarafın oluşturduğu orijinal haliyle) ve tarafların kimlikleri doğrulanarak iletildiğini elektronik veya benzeri araçlarla garanti eden harf, karakter veya sembollerden oluşmuş bir seti ifade eder”*⁴⁶. Elektronik imza, imza sahibinin adı ya da rolü altında işlem gören reddedilmeyen güvenlik politikası altındaki bazı eylem ve olayların sayısal formdaki kanıtı olarak kabul edilebilir⁴⁷. Bu tanım dört unsur içermektedir. Bunlar:

1. İnkâr edilemezlik,
2. İmza sahibi tarafından tanınan eylemin yada olayın türü,

⁴² Galip H Küçüközyiğit, “Elektronik Ticaret, Elektronik İmza ve Hukuk”, www.ceterisparibus.net/arsiv/g_kucukozyigit2.doc (13 Haziran 2007)

⁴³ Selahattin Sulhi Tekinay, ve Diğerleri, **Borçlar Hukuku Genel Hükümler**, İstanbul: [y.y.], 1993, s. 49.

⁴⁴ Marianne Menna, “From Jamestown to the Silicon Valley Pioneering A Lawless Frontier: The Electronic Signatures in Global and National Commerce Act” <http://www.vjolt.net/vol6/issue2/v6i2-a12-Menna.html> (9 Haziran 2008).

⁴⁵ “Digital Signature Report”, www.un.org.at/uncitral/english/workinggroups/wg_ec/wp-88e.pdf (11 Mart 2007)

⁴⁶ “Elektronik İmza”, <http://www.etkk.gov.tr/hukuk.htm>, (11 Mayıs 2006)

⁴⁷ Ayşe İnalöz, “Telekomünikasyon Regülasyonları Çerçevesinde Elektronik Ticaretin İncelenmesi”, (Yayınlanmamış Uzmanlık Tezi, Ankara, 2003) s. 23.

3. İmza sahibinin rolü

4. Zaman tayini

Her halükarda elektronik imza, elektronik imzayı kullanana kişinin kimliğini belirleme, metnin içeriği ile bağlandığını kabul iradesini ortaya koyma ve imzalanan metnin bütünlüğünü garantileme fonksiyonlarını üstlenir.

Tüm elektronik imzalar, bilgisayar ortamında olduğu sürece mutlaka sayısal olarak ifade edildiği halde, farklı teknolojilerle oluşturulabilir ve değişik şekiller alabilirler. Gönderici tarafından metnin sonuna yazılmış isim, el yazısı ile atılmış imzanın tarayıcıdan geçirilerek elektronik bir belgenin sonuna iliştirilmiş görüntüsü, gizli kod veya şifre, parmak izi ya da retina taraması ile oluşturulan özel bir biyometrik belirleyici şifre, elektronik imza çeşitleri olarak sayılabilir. Teknolojinin gelişmesiyle elektronik imza çeşitlerine yenileri eklenmektedir. Bu türlü tekniklerle elektronik imzalar taklit edilmesi daha güç hale getirilmeye çalışılmaktadır.⁴⁸ Örneğin retina taraması yoluyla oluşturulmuş bir elektronik imzanın taklit edilmesi neredeyse olanaksızdır.⁴⁹ Ancak bu tip bir elektronik imza yüksek maliyet gerektirdiğinden şu an için yaygın ve etkin olarak kullanılmayacağı düşünülmektedir.

Elektronik imzanın başlıca türleri elektronik bir belgeye eklenmiş, sayısallaştırılmış bir el yazısı gizli şifre ATM ve Kredi kartlarında kullanılan PIN kodları, göz retinası, el izi taraması, parmak izi , ses gibi biyometrik tabanlı kimlik belirleyiciler ile açık anahtarlı şifreleme yönetime dayalı sayısal imzalar oluşturur.⁵⁰

Elektronik imza çeşitleri içinde, en çok üzerinde durulan ve kullanımı en kolay, verimli, etkin ve düşük maliyetli olabileceği belirtilen tür açık anahtar şifreleme (Public Key Cryptography) dayanan sayısal imzadır. Elektronik ortamda bilginin orijinalliği bozulmadan tarafların kimliğini de belirleyerek karşı tarafa aktarılmasını garanti eden, harf ve sembollerden oluşmuş bir settir.⁵¹

⁴⁸ Küçüközyiğit, www.ceterisparibus.net/arsiv/g_kucukozyigit2.doc (13 Haziran 2007).

⁴⁹ W. E. Lupton, "The Digital Signature: Your Identity by the Numbers", <http://www.richmond.edu/jolt/v6i2/note2.html> (12 Kasım 2006)

⁵⁰ M. Ford, "Identity Authentication and E-Commerce" *The Journal of Information, Law and Technology (JILT)*, <http://www.elj.warwick.ac.uk/jilt/98-3/ford.html>. (21 Mart 2007)

⁵¹ Mustafa Topaloğlu, "Dijital İmza", *PC-Life*, Şubat, 2001, s.122

Elektronik imza, biyometrik imza ve sayısal imza olmak üzere ikiye ayrılır. Biyometrik imza, kullanıcıların parmak izi veya retina gibi kişiye has özellikler kullanılarak oluşturulan imzadır. Dünyada en çok sayısal imza tercih edilmektedir. Biyometrik yöntemler ise sisteme erişimde kullanılmaktadır. Parmak izine duyarlı mouse'lar buna örnek verilebilir. Elektronik imza özelde sayısal imza, asimetrik şifreleme mantığına dayandığından ⁵² konunun açıklığa kavuşması açısından öncelikle ele alınacaktır.

Elektronik imza ile sağlanmaya çalışılan, internet veya intranet ortamında güvenlidir. Bunun sağlandığını anlamanın yolu, metinlere müdahale edilmesi, değiştirilmeden karşı tarafa ulaştığından emin olunması yani bütünlüğünün sağlanmasıdır. Veri bütünlüğü, verinin izinsiz değiştirilmesi, silinmesinin önlenmesi yanında değişikliğe uğradığının fark edilmesini kapsar.

Öte taraftan imzalı olarak gelen metnin kimden geldiğinin garanti edilmesi gerekir. Ya da tam tersi gönderilen metnin istenilen kişiden başkası tarafından içeriğini görememesini sağlaması gerekir. Aynı şekilde imzanın sonradan inkâr edilmemesini temin etmelidir.

Sayısal imza, birbiriyle haberleşmek isteyen iki taraf arasında veya kapalı bir grup içinde kullanılabilir. Ancak arzu edilen şey, isteyen herkesin diğer bir kimse ile aralarında önceden mevcut bir ilişki olmaksızın spontan olarak haberleşebileceği, herkese açık ağda sayısal imzanın kullanımını yaygınlaştırmaktadır. Ancak bunun için iyi bir organizasyon ve sağlam bir alt yapıya sahip olmak gerekecektir.

3.2.1. Açık Anahtar – Özel Anahtar

Anahtar, şifrelemek veya deşifre etmek için kullanılan sayısal karakter dizisi olarak tanımlanabilir. Açık Anahtar Altyapısında kullanılan asimetrik şifreleme yönteminde, biri açık anahtar ⁵³ diğeri özel anahtar* olmak üzere bir anahtar çifti

⁵² İnalöz, 2003, s. 25.

⁵³ 5070 Sayılı, “Elektronik İmza Kanunu”, Kabul Tarihi:15.01.2004, Resmi Gazete Sayısı:25355, Resmi Gazete Tarihi:23.01.2004, Madde-3/f.

* İngilizcede public key, açık anahtar kelimesinin, private key, özel anahtar kelimesinin karşılığıdır. Açık anahtar ile özel anahtar deyimleri birbirinin karşılığını ifade etmemekle birlikte dilimize yerleşmiş ve Türk bilişim

bulunmaktadır.⁵⁴ Özel anahtar sayısal imzanın oluşturulmasında, açık anahtar ise sayısal imzanın tetkikinde kullanılmaktadır.⁵⁵ Başka bir ifadeyle özel anahtar mesajı şifrelemekte, açık anahtar ise deşifre etmekte kullanılır. Bu yüzden özel anahtar sadece kullanıcıda bulunur ve özenle saklanması gerekir. Başkalarının ona ulaşması şifrenin çözülmesi veya yerine imza atmasıyla eşdeğerdir. Bu durumun aksine açık anahtarın üçüncü kişilerce ulaşılabilir olması, onlar tarafından biliniyor olması gerekmektedir.

Söz konusu anahtar çifti, ya elektronik sertifika hizmet sağlayıcıları tarafından üretilir(5070 Sayılı Elektronik İmza Kanunu 10'uncu maddesinin son fıkrasında "elektronik sertifika hizmet sağlayıcısının üretilen imza oluşturma verisinin bir kopyasını alamayacağını veya bu veriyi saklayamayacağını" hükme bağlamıştır) ⁵⁶ ve sahibine teslim edilir; ya da kişiler tarafından bizzat uygun programlar ⁵⁷ aracılığıyla elde edilir. ⁵⁸ Özel anahtar ile açık anahtar matematiksel olarak birbiriyle bağlantılıdır ⁵⁹ Ancak, bir anahtarı kullanarak diğerine ulaşmak mümkün değildir.⁶⁰

Üçüncü kişilerin mesajı deşifre etmeleri imkansız kabul edilmektedir. Asimetrik şifreleme yönteminde deşifre etme süreci, simetrik şifreleme* yöntemine göre daha uzun sürmektedir. Bunun üstesinden gelmek amacıyla Rivest tarafından hash fonksiyonu ⁶¹ geliştirilmiştir.

3.2.2. Özel Anahtarın Güvenliği

En önemli konulardan biri de şüphesiz özel anahtarın güvenliğinin sağlanmasıdır. Özel anahtar üretildikten sonra ya bilgisayarın diskinde ya da harici bir

sektörü tarafından benimsendiğinden Elektronik İmza Çalışma Komisyonunda açık anahtarla matematiksel bağlantısı bulunan anahtara "kapalı anahtar" yerine "özel anahtar" veya "imza oluşturma verisi" deyimini kabul edilmiştir.

⁵⁴ Calalettin Dönmez, **Regulation of Electronic Signatures and Protection of Private Keys**, Sheffield: University of Sheffield Department of Law, 2002, s. 12.

⁵⁵ Şenocak, 2001, s. 99.

⁵⁶ 5070 Sayılı, "Elektronik İmza Kanunu", Kabul Tarihi:15.01.2004, Resmi Gazete Sayısı:25355, Resmi Gazete Tarihi:23.01.2004, Madde-10.

⁵⁷ Örneğin *PGP-Pretty -good privacy*

⁵⁸ Leyla Keser Berber, "İmzalıyorum O Halde Varım", **Türkiye Barolar Birliği Derigisi**, Sayı:2, 2000, s. 131.

⁵⁹ American Bar Association, **Digital signature guidelines: legal infrastructure for certification authorities and electronic commerce/Information Security Committee, Electronic Commerce and Information Technology**, Chicago: IL, 1996, s.9.

⁶⁰ Ulvi Altınışık, **Elektronik Sözleşmeler**, İstanbul: Seçkin Yayınevi, 2003, s. 82.

* Kriptografik yöntemlerden, hem şifreleme hem de deşifreleme işlemi için aynı anahtarı kullanan kriptosistemlere verilen isimdir.

⁶¹ Hash fonksiyonu bu bölümün 2.2.6. numaralı başlığı altında açıklanmıştır.

depolama biriminde tutulur ve erişilmesini önleyici tedbirler alınır. Ancak, erişilmesi kolay olup ataklara maruz kalacağından disk, disket, CD, DVD gibi elektronik ortamlarda tutulması güvenlik açısından tehlikelidir. Özel anahtarın bulunduğu elektronik medya şifre ile korunsada dahi bu şifrelerin bulunması çok zor değildir. Açık anahtardan yola çıkarak matematiksel yöntemlerle özel anahtarın elde edilmesi imkansız kabul edilmektedir.⁶² Ancak, özel anahtarlar akıllı kartlarda veya bilgisayarlarda tutulmaktadır. Gerekli güvenlik önlemlerinin alınmadığı durumlarda özel anahtara ulaşmak mümkün olabilir. Bu durumda, imza özel anahtarla atıldığından ve inkar edilemeyeceğinden bütün sorumluluk özel anahtar sahibine ait olacaktır.

Özel anahtarın çok iyi korunması gerektiği konusunda kullanıcılar mutlaka bilinçlendirilmeli, suiistimallerin artmasıyla sisteme olan güven baştan zedelenmemelidir. Kurumsal uygulamalarda özel anahtarın sabit veya geçici disk ortamlarında tutulması yerine akıllı kart gibi güvenlik seviyesi yüksek cihazlar özendirilmelidir.

Açık anahtar altyapıları insandan bağımsız olarak düşünülemez. Algoritmalar, protokoller, otoriteler, şifreleme anahtarları gibi unsurların dışında insanlar da bu sistemin bir parçasını teşkil etmektedir.

3.2.3. Elektronik Sertifika

İnternet kullanımı günlük hayatı çok kolaylaştırmıştır. Öyle ki istenilen bilgilere anında ulaşılabilen, haberleşmek istenen kişiye elektronik posta vb. yollarla mesaj gönderip alınabilmektedir. Ancak, bilgisayar kullanarak haberleşilen kişinin, sözleşme yapılan kurumun gerçekten o kişi veya kurum olduğundan ya da yapılan sözleşmenin üçüncü kişilerin eline geçmediğinden nasıl emin olunabilir? Bunun gibi pek çok soru sormak mümkündür.

Elektronik sertifika günlük hayatta kullanılan ehliyet, pasaport gibi kimlik kartlarını elektronik ortamdaki karşılığıdır denilebilir. Elektronik sertifikalar sertifika otoriteleri tarafından düzenlenir.⁶³ Elektronik sertifika, kullanıcı adıyla onun açık

⁶² Altınışık, 2003, s. 82-83.

⁶³ Özgür Deniz Erzincan, "E-imza Deneyimi", **Telekom Dünyası Dergisi**, Temmuz 2004, s.32.

anahtarını içeren ve gizli anahtarının kullanıcıya ait olduğunu doğrulayan elektronik belgedir.⁶⁴ Diğer bir deyişle elektronik sertifika imza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kaydı ifade eder.⁶⁵ Elektronik sertifika, kişilerin veya kuruluşların bilgilerinin elektronik ortamda güvenli bir şekilde iletilmesini sağlamaktadır.

Elektronik sertifika imza sahibinin imza doğrulama verisini yani açık anahtarını ve kimlik bilgilerini birbirine bağlayan elektronik kayıt olarak da tanımlanabilir. Bu tanım Avrupa Birliği Direktifindeki ve mevzuatlardaki sertifika tanımlarına uygundur. Elektronik sertifikalar, imzalama-doğrulama işlemi sırasında imzalayanın kimliğinin güvenilir üçüncü kişi (sertifika hizmet sağlayıcısı) tarafından teyit edilmesi amacıyla kullanılırlar.⁶⁶

Bir kişinin elektronik imzanın geçerliliği, o kişinin açık anahtarını içeren elektronik sertifikanın yetkili bir sertifika otoritesi tarafından verilmiş olması halinde geçerlidir.⁶⁷ Elektronik sertifika, kullanıcı bilgilerini içeren bir verinin sertifika hizmet sağlayıcısı tarafından sayısal olarak imzalanması ile oluşur. Elektronik sertifika belgesinde, kullanıcının adı, soyadı, e-posta adresi gibi bilgilerin yanı sıra, kimlik belgesinin geçerlilik süresi, kullanıcının açık anahtar bilgisi gibi bilgiler de bulunur. Elektronik sertifika, sertifika sahibinin açık anahtarını ve kimlik bilgilerini taşımalı sertifika sağlayıcının özel anahtarı ile onaylamış olmalıdır.⁶⁸ Sertifikanın düzenlendiği tarih ve geçerlilik süresi de önem arz etmektedir.

Elektronik ticaret yapan şirketler ve finans kurumları başta olmak üzere pek çok kurum elektronik sertifika kullanarak internet üzerinden gerçek ve yasal bir şirket olduklarını kanıtlamaktadırlar. Bu şekilde, müşteri kuruma güven duymaktadır.

⁶⁴ Ömer Ergün, “5070 sayılı Elektronik İmza Kanunu ve Dijital İmza”, **Türkiye Noterler Birliği Hukuk Dergisi**, Sayı: 122, 15 Mayıs 2004, s.64.

⁶⁵ İnalöz, 2003, s. 156.

⁶⁶ Telekomünikasyon Kurumu, E-İmza Ulusal Koordinasyon Kurulu (UKK) Bilgi Güvenliği ve Standartlar Çalışma Grubu İlerleme Raporu, http://www.tk.gov.tr/eimza/doc/diger/eimza_bgs_taslak_raporuV1.2.pdf. (18 Aralık 2007), s.12.

⁶⁷ Keser Berber, 2001, s. 23.

⁶⁸ İnalöz, 2003, s. 82.

Elektronik sertifikalar sertifika otoriteleri tarafından hazırlanır. Bir elektronik sertifika almak için, bir sertifika otoritesinin sayfasını ziyaret edip sertifika isteğinde bulunmak gerekir. Bizden gerekli kimlik belirleyici bilgileri sunmamız beklenir.

Elektronik sertifikada bulunması gereken bilgiler Uluslararası Standartlaşma Örgütü (ISO-International Standardization Organization) ve Uluslararası Telekomünikasyon Birliği (ITU-International Telecommunications Union) tarafından tanımlanmış olan X.509* standardına göre belirlenmektedir. Sertifikada yer alan bilgilerin içeriğinin bir kısmı seçime dayalı olmasına rağmen bazıları da zorunlu içeriklerden oluşmaktadır.⁶⁹ Buna göre sürüm numarası zorunlu değildir. Sertifikanın seri numarası, imzalamada kullanılan algoritmanın belirteci, sertifika yayıncısının ismi, sertifikanın geçerlilik süresi, açık anahtar ve özne ismi zorunlu alanlar arasındadır. Özne kısmı gizli anahtarı kontrol eden kısımdır.⁷⁰ Kişisel sertifikalardan başka kök sertifika ve sunucu sertifikaları da bulunmaktadır.

3.2.3.1. Kök Sertifika

Kök sertifika, sertifika hizmet sağlayıcısının kimlik bilgilerini ve açık anahtarını taşıyan elektronik dosyadır.⁷¹ Kök kimliği diğer sertifikalardan ayıran tek özellik, üzerinde kendi imzasını taşıyor olmasıdır.⁷² Kök sertifika, elektronik sertifika hizmet sağlayıcısının sertifikasıdır. Kullanıcılar internet üzerinden kök sertifikayı bilgisayarına yüklerken aynı zamanda bu sertifika sağlayıcının güvenli olduğunu kabul etmiş sayılırlar. Sertifika ile birlikte gelen açık anahtar, sertifika kurumunun kimliğini doğrulamakta kullanılırlar. Zira elektronik sertifikalar sertifika otoritelerinin özel anahtarları ile imzalanırlar. Doğrulama gerçekleştirilerek sertifikanın o hizmet sağlayıcısı tarafından onaylanmış, gerçek bir sertifika olduğu teyit edilmiş olur.

* AAA sistemlerinde yaygın olarak kullanılan sertifika standartlarının başında X.509 standardı gelir. Bu standart IETF tarafından RFC 2459 olarak yayınlanmıştır. "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" adını taşıyan bu standart dâhilinde X.509 Sertifikası V1, V2, V3 sürümleri ve X.509 Sertifika İptal Listesi (SİL) V1, V2 sürümleri tanımlanmıştır.

⁶⁹ İnalöz, 2003, s. 42.

⁷⁰ İnalöz, 2003, s. 43.

⁷¹ Gökçe Üzel (edt.), "Sayısal İmza ve Yasal Düzenleme Yaklaşımları", **Bilgi Toplumuna Doğru, Türkiye Bilişim Şurası**, Ankara: Başbakanlık, 10-12 Mayıs 2002, ODTÜ, s.363.

⁷² Çağlar Çifti, Legal Aspects Of Ict Implementation In Turkish Construction Industry; "Applicability Of Elegal Framework" (**Thesis Submitted To The Graduate School Of Natural And Applied Sciences Of Middle East Technical University**, 2005), s.95-96.

Kök sertifika tanınmış bir otoriteye ait ise pek sorun olmamaktadır. Ancak, tanınmamış bir kök sertifika ile karşılaşıldığında kullanıcıya söz konusu sertifika otoritesine güvenilirlik sorulmaktadır. Bu soruya cevap vermek için özel bir bilgiye sahip olmak gereklidir. Karar vermek kullanıcılar için oldukça zordur. Zira tanınmış kök sertifikalar zaten tarayıcı programlarla birlikte gelmektedir. Görüldüğü gibi kullanıcılar kime ne sebeple güvenmeleri gerektiği konusunda yeterli bilgi sahibi olmamakta ve sadece kendilerinden bekleneni yerine getirmektedirler.⁷³ Sonuç olarak, açık anahtar altyapılarını kullanan sistemlerde “güven” ve “güvenilirlik” bir problem olarak karşımıza çıkmakta, kullanıcılar bir varsayım ile sistemdeki diğer kullanıcılardan emin olabilmekte, kendilerinden beklenenin ötesinde bir güven sorgulamasına girdiklerinde sistemi kullanamaz duruma düşmektedirler.⁷⁴

Bazı sertifika hizmet sağlayıcısı sertifikaları, Netscape ve Internet Explorer gibi popüler olan tarayıcılarda önceden tanımlanmıştır yani kök kimlikler tarayıcıya yüklenmiş durumdadır. Diğer sertifika hizmet sağlayıcılarının da tarayıcıya tanımlanabilmesi için kök kimliklerinin tarayıcıya yüklenmesi gerekmektedir.⁷⁵

Sertifika kullanım süreleri vardır. Bu sürenin sonunda sertifika içerisindeki bilgiler geçersiz hale gelmektedir. Sertifika kullanıcılarının sertifikalarını yenilemelerini sağlayan mekanizma X.509 sertifika iptal listeleridir.⁷⁶

Sertifika otoritesinden sertifika almak amacıyla başvuran bir kullanıcının kimlik bilgilerinin ve diğer tanımlayıcı bilgilerinin doğrulanması, gerçekten iddia ettiği kişi olduğunun onaylanması işlemine sertifikasyon denmektedir.⁷⁷

3.2.3.2. Sunucu Sertifikası

Web sitesinin kimlik bilgilerini ve açık anahtarını taşıyan ve web sitesine bağlanan kullanıcılara sunulan elektronik dosyalara sunucu sertifikaları denilmektedir. Örneğin bir internet tarayıcısı sunucunun göndermiş olduğu sunucu sertifikasını alır.

⁷³ Dinçer Önel, “Açık Anahtar Altyapısı (AAA) Sistemindeki Sertifikasyon Problemleri ve Diğer Güvenlik Sorunları”, [t.y.], Gebze İleri Teknoloji Enstitüsü Mühendislik Fakültesi, Gebze, Kocaeli, <http://www.bilmuh.gyte.edu.tr/-ispinar/BIL571/acik-anahtar.pdf> (03 Şubat 2005), s.4.

⁷⁴ Önel, [t.y.], s.5-6.

⁷⁵ Çifti, 2005, s. 98-99.

⁷⁶ İnalöz, 2003, s. 42

⁷⁷ Önel, [t.y.], s.7.

İçinde web sunucusunun açık anahtarını bulunduran sunucu sertifika tarayıcı, Web sunucusunun kimliğinin doğrulanması, sunucuya gönderilecek olan bilginin SSL (Secure Socket Layer)* teknolojisi kullanılarak şifreli gönderilmesi işlemlerini sağlar.

Gönderilecek olan bilgi, sunucu sertifikasının içindeki açık anahtar ile şifrelenir. Bu şifreli bilgiyi çözecek özel anahtar sadece sunucuda bulunduğundan başka birisinin şifreyi çözmesi mümkün değildir. Böylece şifreli bilginin internet üzerinden gönderiminde güvenlik sağlamış olur.⁷⁸

3.2.4. Elektronik Sertifika Hizmet Sağlayıcılar (ESHS)

Açık Anahtar Altyapısı sisteminde her kullanıcıya sertifika otoritesi tarafından kullanıcıların kimlikleriyle ilişkilendirilmiş sertifikalar dağıtılmaktadır.⁷⁹ En basit anlatımı ile elektronik sertifika, bir açık anahtar ile sahibinin kimliği arasındaki ilişkinin belgesidir. Başka bir söylemle bir açık anahtarın kime ait olduğunu ispatlayan belge hükmündedir. Bir sertifikadaki kişiye ait kimlik bilgilerinden, o sertifikayı onaylayan sertifika otoritesinin imzasına/onayına bakılarak emin olunabilir. Sertifikadaki bilgilerin doğru olduğu varsayılmaktadır. Sertifika otoriteleri “güvenilir” kabul edilmektedir. Güvenilir olduğu kabul edilen sertifika otoritelerinin ürettiği sertifikaların içerdiği bilgilerin sadece doğru varsayılabilmesi bu noktada bir çelişki oluşturmaktadır. Güvenilir sıfatı, varsayımdan daha kuvvetli bir anlam içermelidir. Aslında buradaki sorun “güvenilir” kelimesinin tam kesinlik ifade etmeyen kullanımdan kaynaklanmaktadır.⁸⁰

Elektronik Sertifika Hizmet Sağlayıcıları, açık anahtar sahibinin kimliğini sertifikaya bağlar, yani onaylar, açık anahtarların yayınlanma görevini yüklenir, özel anahtarların güncellenmesi, sertifika bilgilerinin saklanması gibi görevleri üstlenirler ve bu konularda hukuksal sorumluluk altındadırlar.⁸¹ Sertifika hizmet sağlayıcıları, kullanıcıların kimlik bilgilerini doğrulamak üzere, kulacılara üzere, kulacılara

* Secure Socket Layer (SSL), 1995 yılında internet üzerinden güvenli veri alış verişi sağlayabilmek amacıyla Netscape Communications tarafından geliştirilmiştir.

⁷⁸ Çiftçi, 2005, s.100.

⁷⁹ Önel, [t.y.], s.7-8.

⁸⁰ Carl Ellison, Bruce Schneier, “The Risk of PKI: What You’re Not Being Told About Public Key Infrastructure”, **Computer Security Journal**, Vol:16, No:1,2000, s.1-7.

⁸¹ Küçüközyiğit, www.ceterisparibus.net/arsiv/g_kucukozyigit2.doc (13 Haziran 2007).

elektronik sertifika belgesi verirler.⁸² Sertifika içerisindeki bilgilerin bütünlüğü ve doğruluğu sertifika hizmet sağlayıcılar tarafından garanti altına alınmaktadır.⁸³ Sertifika otoritesinin bir görevi de açık anahtar altyapısı içinde bulunan bütün kullanıcılara elektronik sertifikanın dağıtılmasıdır.⁸⁴ Elektronik Sertifika Hizmet Sağlayıcıları, elektronik sertifika vermenin yanı sıra zaman damgası, izin hizmeti, iptal listelerinin tutulmasını da sağlarlar.⁸⁵

Sertifika hizmet sağlayıcılar sayısal imzada “*açık anahtarın*” belirli bir kişiye ait olduğunun güvenli bir şekilde tespiti işlemini yerine getirerek elektronik ortamda adeta kimlik belgesi verirler.

Sertifika hizmet sağlayıcılar ihtiyaca göre sertifikaların dağıtım sorumluluğunu birden fazla alt birime vermek isteyebilir. Dağıtılacak sertifikalar çok fazla olduğunda sertifika hizmet sağlayıcı kurum, kök kurumun altında alt kök kurumlar tanımlayarak hiyerarşik bir sertifika dağıtım modeli oluşturabilir. Kök kurumun altında istenilen seviyede alt kök kurumlar ve bunların sorumlulukları tanımlanabilir. Alt kök sertifika kök sertifika otoritesinin imzasını taşımak zorundadır.⁸⁶

Bir kimse birden çok sertifika otoritesine kayıt yaptırmışsa, sertifika otoriteleri bunun doğruluğunu kontrol etmek için aralarında haberleşirler. Bu durum “*güven zinciri*” adı verilen ilişkinin doğmasına sebep olmaktadır. Dünyadaki farklı ülkelerin “*ana kurum*” olarak adlandırdıkları üst makamları karşılıklı olarak birbirlerini tanır ve yetkilerini tasdik ederlerse, bu durumda artık uluslararası haberleşme gerçekten bir sorun olarak karşımıza çıkmayacaktır. Çünkü bireylerin herhangi bir ülkenin sertifika otoritelerine kayıt yaptırmaları ve bu kurumdan sertifika almaları mümkün hale gelebilecektir.⁸⁷

⁸² İnalöz, 2003, s. 42.

⁸³ Erzincan, 2003, s. 13.

⁸⁴ Erzincan, 2003, s. 14.

⁸⁵ Dönmez, 2002, s. 15; Keser Berber (Şekil), 2001, s. 24; Keser Berber (İmza), 2000, s. 529.

⁸⁶ *Açık anahtarlı Altyapı Belge tasarımları*, 2002, TÜBİTAK, <http://www.tubitak.gov.tr>

⁸⁷ Keser Berber, 2001, s. 530.

3.2.5. Açık Anahtar Altyapısı (AAA) ve Elektronik İmza Servisleri

Açık anahtar altyapısının temeli, 1976 yılında Stanford Üniversitesinden Diffie ve Hellman tarafından ortaya atılan yeni bir şifreleme mantığına dayanmaktadır.⁸⁸ Buna göre karşı tarafa gönderilen mesaj aynı anahtar ile değil, kişiye daha önceden verilmiş özel bir anahtarla açıp okunabilmektedir. Böylelikle mesaj sadece özel anahtara sahip kişi tarafından açılabilir. Verilerin şifrlenmesinde ve şifreli metnin açılmasında aynı şifre kullanımının aksine bu sistemde açık ve özel olmak üzere iki anahtar bulunmaktadır. Bu anahtar çiftleri birbirlerine matematiksel bir bağla bağlıdır.⁸⁹ Ancak birinden diğerini elde etmek imkânsız kabul edilmektedir.

AAA, zaman içinde gelişerek gizlilik yanında, bütünlük, kimlik doğrulama, inkar edememe gibi fonksiyonları da yerine getirir hale gelmiştir.⁹⁰

Sayısal imzanın temelinde açık anahtar altyapısı yer almaktadır. Açık anahtar altyapısı ise simetrik, asimetrik ve özet şifreleme algoritmalarının bir arada bulunduğu kriptografik bir sistemdir.⁹¹

Sertifikasyon yetkilisi, kullanıcı anahtar çiftinin ve sertifikalarının yaratılmasını ve idame edilmesini sağlayacaktır. Sertifikasyon yetkilisi kendi özel anahtarını saklı tutacaktır. X.509 sürüm 3 standardına uygun sertifika yaratabilecek kabiliyette olacak, sistemdeki anahtar yönetimi işlevinden sorumlu olacaktır. Anahtar yönetimi, sistemdeki her gerekli birim için en azından aşağıda belirtilen işlevleri karşılayacaktır:

- I. Anahtar üretimi,
- II. Anahtar dağıtımı,
- III. Anahtar doğrulaması,
- IV. Anahtar iptal edilmesi,

⁸⁸ Önel, [t.y.], s.1; Albert Levi, Mahmut Özcan, “Açık Anahtar Tabanlı Şifreleme Neden Zordur”, <http://people.sabanciuniv.edu/levi/bilisim02.pdf>, (24 Haziran 2005), s.1.

⁸⁹ Andres N. Douzis, **Legislative Approaches Towards Electronic Signatures**, Sheffield: University of Sheffield Department of Law. 2002, s.11.

⁹⁰ Önel, [t.y.], s.3-5.

⁹¹ Erzincan, 2003, s. 13.

V. Anahtar süresinin bitirilmesi,

VI. Anahtar bildirimi,

VII. Anahtar kimlik doğrulaması,

Bir belgeyi elektronik olarak imzalayabilmek için, kullanıcıların, yetkili bir Elektronik Sertifika Hizmet Sağlayıcısından elektronik sertifika almış olmaları gerekmektedir. Kullanıcının bir bilgisayarı ve kendine ait bir yazılım programının mevcut olması gerekir. Kullanıcının ayrıca bilgisayar üzerinden yapacağı işlemlerde kullanacağı bir de şifrenin olması gerekir. Bu şife, ya yazılım programları vasıtasıyla veya akıllı kart olarak da adlandırılan chip kartlar kullanılarak elde edilebilir.

Açık anahtar altyapısı ilk çıktığında bütün güvenlik sorunlarının çözümü olarak gösterilmiştir. Oysa zaman içerisinde bunun böyle olmadığı, güven sorunu ve sertifikasyon problemlerinin bulunduğu tespit edilmiştir.⁹²

Açık anahtar altyapısı sisteminde, açık anahtarla mesajın şifrelenmesi ve sadece özel anahtarla şifreli mesajın açılabilmesi sayesinde gizliliğin büyük bir başarı ile sağlandığı konusunda kimsenin şüphesi bulunmamaktadır.⁹³ Açık anahtar altyapısının, doğru anahtarın edinilmesi, tanınması, dağıtımı ve onaylanması problemlerine yeterli çözümler getirmekte zorlandığı ortaya çıkmıştır. Kimlik doğrulaması düzgün olmayan bir haberleşmenin gizli olabileceğini söyleyebilmekle birlikte güvenli olduğunu iddia etmek mümkün değildir.

3.2.6. Hash Değeri (Hash Value) *

Metnin şifrelenmesi yönteminde çok uzun metinlerin şifrelenmesi zaman aldığından kullanışlı değildir. Bu nedenle metnin tamamı değil; metinden belli bir algoritmayla çıkarılan metnin özeti şifrelenir. Metinden özet çıkarma işini hash fonksiyonu yerine getirir. Bilgisayar terminolojisinde “hash” yazılan bir metnin kısaltılmış şeklini ifade etmektedir.⁹⁴ Hash fonksiyonu elektronik imzanın

⁹² Önel, [t.y.], s.3-5

⁹³ Elison, 2000, s.5-6.

* Bu konuda farklı isimlendirmeler bulunmaktadır. Hash değeri, mesaj özeti, öz değeri bunlardan bazılarıdır. Bu çalışmada hash değeri terimi tercih edilmiştir.

⁹⁴ Keser Berber, 2001, s.524.

hazırlanmasında son derece önemlidir.⁹⁵ Hash fonksiyonu matematiksel bir algoritmadır.⁹⁶ Hash fonksiyonuyla oluşturulan mesaj özeti verilerin parmak izi olarak düşünülebilir.⁹⁷ Bu algoritmalar geneldir ve özel anahtar gerektirmezler.⁹⁸ Hash fonksiyonu sonucu elde edilen değere hash değeri veya mesaj özeti denmektedir.

Hash fonksiyonları genel olup orijinal metinden herkes tekrar hesaplama yaptırabilir. Hash fonksiyonu tek taraflı olarak çalışır.⁹⁹ Bunun anlamı metinden elde edilen mesaj özetinden yola çıkarak metni elde etmek mümkün değildir. Farklı iki belge aynı hash değerini vermesi imkan dahilinde olmakla birlikte, imkansızla yakın kabul edilmektedir.¹⁰⁰

Sayısal imza, bilginin doğruluğunu korumaktadır. Teknik açıdan sayısal imza, imzalanmış belgenin özünü (Hash) içerir. İçerikte yapılacak herhangi bir değişiklik dijital mesaj özetini geçersiz kılacaktır. Çünkü mesaj özeti, metnin karakteristik özelliklerinin tümü dikkate alınarak oluşturulmaktadır. Yapılacak en küçük bir değişiklik mesaj özetinin değişmesine yol açacaktır.¹⁰¹

Burada bilinmesi gereken husus, sayısal imza denilen olgunun metnin içeriğinde değil mesaj özeti üzerinde uygulandığıdır. Metni imzalayan kişinin özel anahtarı ve asimetrik şifreleme sistemi vasıtasıyla mesaj özeti şifrelenir ve bu şekilde şifrelenen mesaj özeti elektronik metne eklenerek muhataba gönderilir.¹⁰² Şifrelenen mesaj özeti metinden ayrı olarak tutulur. Mesaj özetinden bir şekilde metne ulaşmak mümkün değildir.¹⁰³

⁹⁵ Altınışık, s. 83; Özgül, s. 8

⁹⁶ *File Hasher (exe)*, <http://downloads.zdnet.com/abstract.aspx?docid=357921>, (22 Şubat 2008)

⁹⁷ Mario Miccoli, Nadi Günel (çev.), “Teknolojik Açıdan Elektronik Ticaret”, **Noterlik Hukuku Sempozyumu: VII, Elektronikteki Gelişmeler ve Hukuk**, Ankara, 2001, s.83.; İnalöz, 2003, s.31

⁹⁸ Altınışık, 2003, s.83.

⁹⁹ Douzis, 2001, s.12.

¹⁰⁰ A. Michael Froomkin, “The Essential Role of Trusted Third Parties in Electronic Commerce” <http://scholar.google.com.tr/scholar?hl=tr&lr=&q=info:b3aarzFN5AwJ:scholar.google.com/&output=viewport> (07 Aralık 2007) s.49.

¹⁰¹ Mesut Orta, “Türkiye’de elektronik imza uygulaması”, **Konya Barosu Dergisi**, Vol:3, Sayı: 5, Temmuz 2006, s. 63.

¹⁰² Şenocak, 2001, s. 100.

¹⁰³ Faruk Günay Özer, “Sermaye Piyasalarında Elektronik İmzanın Kullanım Alanları”, **Bilgi İşlem Merkezi Yöneticileri Semineri (BİMY)** [y.y.]:[yayl. y.], 8-11 Nisan 2004, Aksu-Antalya, 2004, s. 6.

3.2.7. Zaman Damgası

Elektronik bir belgenin ispat gücünü arttırmak için, belgenin düzenlendiği zamanın şüpheye yer bırakmayacak şekilde tespiti şarttır. Elektronik ortamda bu fonksiyonu, zaman damgası yerine getirmektedir.¹⁰⁴ Zaman damgası, sertifika hizmet sağlayıcıları tarafından, belirli bir elektronik verinin üretildiği, değiştirildiği, gönderildiği, alındığı veya saklandığı zamanı göstermek üzere verilen belgeyi ifade eder.¹⁰⁵ Açık anahtarlı altyapıya sahip bir bilgisayar ağında, kullanıcılar iletişimlerini güvenli hale getirmek için elektronik sertifika kullanabilirler ve bu durumda sistemdeki güvenlik sunucusu sertifika ve zaman damgası hizmeti sağlar.¹⁰⁶

Zaman damgası (time stamp), bilgisayar ağlarında iletilen mesajlara eklenen ve mesajın yazıldığı zamanı güvenli olarak belgeleyen damga olarak tanımlanabilir.¹⁰⁷ Zaman damgası konusunda pek çok standart bulunmaktadır.¹⁰⁸

3.3. ELEKTRONİK İMZA

3.3.1. Elektronik İmzalama Nasıl Gerçekleşir

Elektronik imza, elektronik belgeye eklenmiş bilgidir.¹⁰⁹ Gönderilecek belgeden matematiksel yöntemler yardımıyla ve özgün bir biçimde kısaltmak suretiyle sabit uzunlukta sayısal bir bilgi elde edilir ki buna mesajın özeti veya “hash” adı verilir. Hash metodu ile elde edilen bilgi, geri dönüşümü olmayan bir bilgidir. İkinci adım olarak mesaj özeti gönderen tarafın özel anahtarıyla şifrelenmektedir. Bu kodlanmış olan “hash”, elektronik imza olarak adlandırılmaktadır. Elektronik imza belgeye eklenir ve belgeyle birlikte alıcıya gönderilir. Her mesajın farklı bir özeti vardır. Belgede en ufak değişiklik yapılması halinde şifrelenmiş olan mesaj özeti ile

¹⁰⁴ Leyla Keser Berber, “Elektronik değil dijital İmza Yasası”, **e-Devlet BT Haber**, No:4, Mart 2004, s.18.

¹⁰⁵ Elektronik Ticaret Koordinasyon Kurulu (ETKK) Hukuk Alt Çalışma Grubu, **Elektronik Veri, Elektronik Sözleşme Ve Elektronik İmza Kanunu Tasarısı Taslağı**, 2002, Madde-3, s.1.

¹⁰⁶ UKK e-imza Hukuk Çalışma Grubu Raporu, s. 37.

¹⁰⁷ **Elektronik Ticaret Terimleri Sözlüğü**, “Zaman Damgası”, <http://www.hukukrehberi.net/eticaret/eticsozluk.asp> (26 Aralık 2004)

¹⁰⁸ Telekomünikasyon Kurumu, **Elektronik İmza ile ilgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ**, 6 Ocak 2005, s.4.

¹⁰⁹ Mesut Orta, **Elektronik İmza ve Uygulaması**, İstanbul: Seçkin Kitabevi, 2005, s. 166.

sonradan oluşturulan mesaj özeti arasında fark olacaktır. Fark yoksa imza geçerli bir elektronik imza demektir. Bu şekilde belge içeriğinin değişmediği ispatlanmış olur.

Elektronik imza, mesaj özeti ve gizli anahtara özgüdür. Alıcı mesajı, şifrelenmiş mesaj özetini yollayan kişinin açık anahtarını kullanarak çözer. Bu iki “hash” aynı ise özel anahtarı sadece gönderen bildiği için bu mesajın gönderen kişiye ait olduğu ve mesajın değişmeden geldiği onaylanmış olur. Taraflar böyle bir belgeyi gönderip/almadıklarını ileri süremezler.

3.3.2. Elektronik İmza Nasıl Doğrulandır

Bilgi ağında sadece genel olarak bilgilerin transferi yapılmamakta, bunun ötesinde önemli sözleşmeler, büyük anlaşmalar akdedilmektedir. Hatta tapu sicili gibi kütük kayıtlarının bile gelecekte elektronik olarak yürütülmesi mümkündür. Ancak bunun için, herkese açık olan bu ağ üzerinde yapılacak haberleşmenin güvenilirliğine, güvenliğine ve bağlayıcılığına yönelik olarak acil tedbirler alınması gerektiği vurgulanmaktadır. Sanal ortamda hazırlanan bir mektup veya bir mesaj nasıl bağlayıcı olacaktır? Şüphesiz bunu hazırlayan kişinin imzasıyla mesaj bağlayıcı hale gelir.. Fakat bir belge veya mektup elektronik olarak nasıl imzalanabilir?

Birbirinden kilometrelerce uzakta bulunan kişiler internet üzerinden haberleşmesi, alış veriş yapması veya sözleşme akdetmesi gibi güncel ihtiyaçlar karşısında; kanunlarda yer alan sözleşmelerin şekline ve ispatına ilişkin hükümlerin, bu işlemlerin elektronik yoldan yapılmasına olanak verecek, elektronik iletişimi kolaylaştıracak şekilde yeniden gözden geçirilmesi zorunluluğu doğmuştur. Fakat İnternet üzerinden yapılacak sözleşmelerin geçerli olması ve tarafları bağlaması için gerekli mevzuat düzenlemelerinin yapılması, hukukun elektronik ortamdaki bu işlemlere varlık tanınması gerekmektedir. Elektronik ortamda ıslak imzanın fonksiyonlarını karşılamak için “Elektronik İmza” veya “Sayısal İmza” yöntemleri benimsenmiştir.

Elektronik imza hazırlanışı en karmaşık fakat en güvenilir çözüm yoludur. Elektronik imza, el yazısı ile atılan imzanın sahip olduğu özellikleri, elektronik belgeler bakımından da sağlamaya çalışan bir yöntemdir. Şifreleme yöntemleri sayesinde,

elektronik olarak imzalanan bir belgenin, sadece elektronik imzanın sahibi olan kimse tarafından düzenlendiği tespit edilebilmektedir. Sayısal imzanın başkaları tarafından taklit edilmesi çok güçtür ve ayrıca sayısal imzanın kaynağı da, yani imzanın kimin tarafından atıldığı da şüpheye yer bırakmayacak şekilde ispatlanabilmektedir.

Kısaca özetlenecek olursa; elektronik imza uygulamasında, bugün en çok tercih edilen metot olan, asimetrik şifreleme yönteminde, birbiriyle haberleşmek isteyen her bir tarafın biri gizli, diğeri açık anahtar olmak üzere bir çift anahtarı vardır. Hazırlanan metni sayısal olarak imzalayabilmek için mesajı gönderecek olan kişi, gizli şifresini kullanacaktır. Gönderilecek olan mesaj önce özgün bir biçimde kısaltılarak mesajın yeni bir sürümü elde edilir. Buna hash yöntemi adı verilir. Sonra özel anahtar kullanılarak mesajın bu yeni hash değeri kodlanır. Mesaj iletilirken bir şekilde değişirse, bunun hash'i ilk mesajdan farklı olacaktır. Yani sayısal imza, mesaj ve gizli şifreye özgüdür. Sayısal imza mesaja eklenir ve mesajla birlikte alıcıya gider. Alıcı, bu mesajı aynı şekilde yine özgün bir biçimde kısaltır ve elde ettiği bu yeni hash değeri ile sayısal imzalı hash değerini karşılaştırır. Alıcı imzalı mesajı, mesajı gönderen kişinin açık anahtarını kullanarak deşifre edecektir. Her iki hash değeri de aynı ise, gönderilen ve alınan metnin aynı olduğu, mesajda başkaları tarafından değişiklik yapılmadığı ve gönderilme işlemi sırasında herhangi bir hatanın meydana gelmediği tespit edilmiş olacaktır. Uygulamada, elektronik bir belgeyi oluşturan kişi, daima gizli olan kişisel anahtarıyla bu belgeyi şifreler.¹¹⁰

3.3.3. Elektronik İmzalama Prosedürü

Sayısal olarak şifreleme için, kullanıcıya özel anahtar ve açık anahtar olmak üzere bir anahtar çifti verilmektedir. Bu anahtarlar bilgisayar sistemi tarafından üretilir ve güvenli bir şekilde kullanıcıya ulaştırır.

Elektronik imza kullanımı için, kullanıcı tarafından imzalama anahtar çifti oluşturur. İmzalama açık anahtarı ana bilgisayara gönderilir. Server tarafından sunucuya ait imzalama özel anahtarı ile sertifikalandırıp kullanıcıya geri gönderilir. Anahtarların

¹¹⁰ Christina Spyrelli, "Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach Towards Electronic Authentication", *The Journal of Information, Law and Technology (JILT)*, 16 August 2002, Issue:2, <http://elj.warwick.ac.uk/jilt/02-2/spyrelli.html> (20 Aralık 2007), s.18.

yer aldığı kullanıcı profiline ulaşabilmek için bir parola kullanılır. Kullanıcı kendi özel anahtarını gizli tutmak zorundadır. Şifreleme açık anahtarı ise diğer kullanıcıların ulaşabilecekleri merkezde bir sunucu üzerinde tutulmaktadır. Bu anahtarlar birbirine matematiksel bir ilişkiyle bağlanmıştır fakat anahtarlardan birini kullanarak diğerini elde etmek çok zor hatta imkansızdır.

Anahtarlardan açık olanıyla şifrelenen bir veri ancak bu açık anahtara karşılık gelen özel anahtarla açılabilir.

Kullanıcı bir belgeye elektronik imza altına alıp başka bir kullanıcıya bu belgeyi göndermek istediğinde, öncelikle dizin hizmetlerinden belgeyi göndermek istediği kullanıcının şifreleme açık anahtar sertifikasını elde eder. Belgeden “hash” (SHA-1 Secure Hash Algorithm) algoritması kullanılarak bir özet çıkartılır. Bu özet, gönderenin imzalama özel anahtarı yardımıyla RSA veya DSA (Digital Signature Algorithm) imzalanır ve belgenin sonuna imzalama açık anahtarıyla birlikte eklenir. Ortamda bir kriptolama varsa belge ve özeti simetrik bir anahtarla şifrelenir. Simetrik anahtar, her mesaja bir kez yapılır ve tektir (unique). Alıcının şifreleme açık anahtarı dizinden* bulunup kullanılarak işlem den geçirilir ve mesaj gönderilir. Belgenin hiçbir yere gönderilmeyip saklanacak ise kendi şifreleme açık anahtarını kullanarak simetrik işlem den geçirilir.

Belge ile ilgili kişiye ulaştırıldığında belgeyi alan kullanıcı öncelikle kendi özel anahtarını kullanarak simetrik anahtarı elde eder. Bu simetrik anahtarla belge, özet ve sertifikanın bulunduğu bölümü açar. Elde edilen sertifika ile mesaj özeti açılır. Daha sonra da mesajın özeti tekrar oluşturularak gelen özetle karşılaştırılır. Böylece bu belgenin başkaları tarafından değiştirilmediği, gözetlenmediği, gönderenin ve alanın gerçek kimliği ile belge içeriğinin gönderen tarafından onaylandığı şüpheye yer bırakmayacak şekilde ispatlanmış olmaktadır.

* Dizin hizmetleri elektronik sertifika sağlayıcıları tarafından sunulan bir hizmettir.

3.3.4. Elektronik İmzanın Fonksiyonu

Güvenli elektronik imza, ıslak imzanın sağladığı imzayı kimin attığını tespiti olarak veren kimlik doğrulama, içeriğin değişmediğini garanti eden bütünlük kontrolü, sonradan imzalamadığını ileri sürmeyi engelleyen inkar edememe fonksiyonlarını temin etmektedir. Elektronik imza bunlara ilave olarak erişim kontrolü ve verimlilik de sağlamaktadır. Bu fonksiyonlara daha yakından bakmak gerekirse:

Doğrulama (verification): Belgeyi imzalayan kişinin kimliğinin doğrulanması yoluyla, işleme katılan tarafın kim olduğunun kesin bir şekilde bilinmesi sağlanmaktadır.¹¹¹ Bu özelliğin mantığı, elektronik imzanın sahibinin imzası (gizli anahtarı) üzerinde kontrolü kaybettiğinde taklidini yapmanın mümkün olmamasına dayanmaktadır. Gizli anahtarın başkalarının eline geçmesi, imzanın devredilmesi ile eş anlama gelebilmektedir.

Erişim Kontrolü (access control): Gönderilen bilgilere ve kaynaklara sadece izin verilmiş kişiler tarafından erişilebilmesi ¹¹² garanti edilmektedir. İzin verilmiş bir kişi ise, okuduğu mesajı bir başkasına gönderecek olduğunda kendi imzası ile şifreleyebilecektir. Bu aşamada mesaj içeriğinin değişmesinden kendisi sorumlu olacak, üçüncü kişi de gelen mesajın bir aracı yoluyla geldiğini anlayacak ve gerekiyorsa doğruluğu konusunda teyit alabilecektir.

Bütünlük (integrity): Verinin bütünlüğü korunacaktır ve bu yol ile gönderildiği andan itibaren mesaj içeriğinin hiç değişmemiş olduğu, mesajın hangi amaç ile olursa olsun hiçbir şekilde alıcının gizli anahtarına sahip olmayan biri tarafından açılmayacak olduğu ve göndericinin de mesajı ve açık anahtar altyapısı (PKI), İnternet ve diğer açık ağlar üzerinde gerçekleşen elektronik haberleşme ve işlemlerde çok üst düzeyde bir güvenlik ve güvenilirliği sağlamaktadır.¹¹³

İnkâr Edilememe (non-repudiation): İnkâr edilememe, hukuki bir anlaşmazlık çıktığında, gönderici tarafın mesajdan sorumlu tutulabilmesini

¹¹¹ Spyrelli, 2002, s.12-14.

¹¹² Daniel Greenwood, "Electronic Signatures and Records: Legal, Policy and Technical Considerations", www.state.ma.us/itd/legal/article9.doc, (21 Aralık 2007)

¹¹³ Spyrelli, 2002, s.15.

sağlamaktadır. Karşı tarafın bir mesaja, sözleşmeye ya da ödemeye ilişkin isteği, bu mesajın karşı tarafın tek taraflı iradesiyle reddedilemeyeceğine güvenebilmesi ile yakından ilişkilidir.¹¹⁴ Gönderilen mesajın, gönderen tarafından reddedilememesi ve bu yolla işlemi gerçekleştiren açısından hukuki yükümlülük oluşturması sağlanmaktadır. Bu fonksiyon, elektronik ticaret için hayati öneme sahip uzaktan iletişimi güvenebilmesini sağlayarak, elektronik ticaretin gelişimi olumlu yönde etkileyecektir.

Verimlilik ve Lojistik (efficiency and logistics): Elektronik imza, işlemlere kolaylık, ucuzluk ve hız kazandıracaktır.

3.4. ŞİFRELEME

Şifreleme (Kriptografi), verinin güvenli bir şekilde iletilmesi ve saklanması amacıyla şifreleme ve şifre çözme yöntemleri geliştirilen bilim dalına verilen isimdir. Tarihte ilk şifreleme Cesar tarafından yapılmıştır.¹¹⁵ Şifreleme sayesinde, okunabilir biçimdeki herhangi bir bilgi sadece istediğimiz kişi ve kuruluşların okunabileceği biçime dönüştürülür. İletilen veri ilgilisi tarafından deşifre edilerek okunabilir.¹¹⁶ Şifreleme ve deşifreleme, verinin okunabilir ve kodlanmış formatlara dönüştürülmesini sağlayan bir matematiksel formül veya “algoritma” ile bir anahtar gerekmektedir.¹¹⁷

Bir mesajı şifrelemek veya deşifre etmek için kullanılan anahtar, şifreleme algoritmasının kullanıldığı uzun sayı dizisi anlamına gelen rakamsal bir değerdir. Bu rakamsal değer, elektronik imzayı veya şifreli mesajı üretmek için ham metin ile birleştirilmiştir. Veri ya da mesaja iletim anında üçüncü şahısların eline geçse bile, mesajı deşifre edecek araçlara sahip olmayan kişi veya kurumlar tarafından kesinlikle okunamaz.

¹¹⁴ Thomas Smedinghoff, “Moving with Change”, <http://www.bakernet.com/ecommerce/moveart.doc>, (27 Aralık 2007)

¹¹⁵ Bahattin Yalçınkaya, “Cryptology and Archives an Evalution”, (The Graduation Thesis of Lisence, Marmara Üniversitesi, Fen-Edebiyat Fakültesi, Bilgi ve Belge Yönetimi Bölümü, 2005) s. 13

¹¹⁶ A. Anbar, “Veri Transferi ve iletim güvenliğinin sağlanmasında kullanılan filtreleme yöntemleri ve sayısal imza,” *İş Güç Endüstri Dergisi*, No:6/2, 2004, s. 11.

¹¹⁷ Turhan Yükseliyor, “AAA Sayısal Sertifika Karmaşası”, www.e-imza.gen.tr/index.php?Page=Makaleler&MakaleNo=9 (24 Haziran 2008) s.1-4.

3.4.1. Tek Anahtarlı Simetrik Şifreleme

Tek anahtarlı simetrik şifreleme sistemlerinde, veriyi şifrelemek için kullanılan anahtar ile şifrelenmiş veriyi okuyabilmek için aynı anahtar kullanılmak zorundadır. Karşılıklı şifreli olarak haberleşmek için her iki tarafın birbiriyle simetrik şifreleri paylaşması gerekir.¹¹⁸

3.4.2. Asimetrik (Açık Anahtarlı) Şifreleme

Elektronik imza teknolojisinin temelini oluşturan Asimetrik (Açık Anahtarlı) şifreleme sistemlerinde, açık anahtar ve özel anahtar olmak üzere iki ayrı anahtarın bulunduğu asimetrik bir yöntem kullanılmaktadır. Bu anahtarlar tek yönlü çalışmakta ve birbirlerini tamamlamaktadır. Bu iki anahtar aralarında matematiksel olarak gizli bir bağ olacak şekilde üretilmektedir. Açık anahtar, veriyi şifrelemek için, özel anahtar ise açık anahtar tarafından şifrelenmiş veriyi deşifre etmek için kullanılır. Özel anahtar ait olduğu kişide bulunurken, açık anahtar açık durumdadır.¹¹⁹ Özel anahtarın sahibi dışında kullanılmaması güvenlik açısından son derece önemlidir.

¹¹⁸ Tolga Kılıçlı, “Üniversitelerde Akıllı Kart destekli PKI uygulaması ve E-kimlik”, inet-tr.org.tr/inetconf7/bildiriler/8.doc, (17 Ocak 2008) s.1.

¹¹⁹ Müge Bulut (hızl.), **Dijital İmza Rehberi**, İstanbul: İstanbul Ticaret Odası, 2005, s.10.

4. BÖLÜM-ELEKTRONİK İMZALAMA VE ELEKTRONİK SERTİFİKA HİZMET SAĞLAYICILARI

4.1. ELEKTRONİK İMZA OLUŞTURMA VE DOĞRULAMA VERİSİ

İmza oluşturma ve doğrulama verileri birbirine matematiksel bir bağla bağlıdır. Ancak birinden diğerine ulaşmak çok zor hatta imkânsız kabul edilmektedir. İmza doğrulama, bir matematiksel işlemidir ve imzalamada kullanılan elektronik imza oluşturma verisinin, sertifikaya sahip kişiye ait ve imzalı veride tahrifat yapılmadığını gösterir.

Elektronik imzanın eşsiz bir biçimde oluşmasını sağlayan tek veri imza oluşturma verisidir. Bu veri, imza sahibine aittir ve kişinin imzasıyla kişi arasındaki bağı kurar. Diğer bir deyişle, aynı imza oluşturma verisinin diğer bir kişinin eline geçmesi durumunda, imza sahibinin imzasıyla bağını ispat etmek olanaksızlaşır.

İmza oluşturma verisinin gizliliğinin ve güvenliğinin sağlanması zorunluluğunun aksine, imza doğrulama verisinin sertifikada bulunması, başkaları tarafından ulaşılabilir olması gerekir. Ayrıca elektronik sertifikada kişinin kimlik bilgileriyle imza doğrulama verisi, elektronik bir kayıt ile birbiriyle ilişkilendirilir. Bu şekilde elektronik ortamda kimlik tespitine imkân sağlanmaktadır.

4.2. GÜVENLİ ELEKTRONİK İMZA

Güvenli elektronik imza, gelişmiş elektronik imzanın unsurlarını içermekle birlikte nitelikli elektronik sertifikaya dayanan ve güvenli imza oluşturma araçlar ile oluşturulmuş imzadır. Bu konuda Avrupa Birliği direktiflerine baktığımızda güvenli elektronik imza tanımı yapılmamış, bunun yerine üye ülkelere el yazısı ile imzaya eşdeğer kabul edecekleri ve yargılamada delil olarak kullanılmasını temin edeceklerin imzanın unsurları bakımından güvenli elektronik imza kabul edilmiştir.

4.3. ELEKTRONİK SERTİFİKA

Elektronik sertifika, nüfus cüzdanı, ehliyet belgesi veya diğer sertifikalar gibi kişinin internet üzerinde kimliğini ispatlaması için kullanılan elektronik dosyalardır.

Farklı bir deyişle kimliğin sayısal ispatıdır. Elektronik Sertifikalar çift anahtarlı kriptografi teknolojisine dayanırlar ve kamuya açıktırlar.

Elektronik imzanın sağlayacağı imkanlardan faydalanabilmek için, kamu çalışanları dahil olmak üzere, vatandaşların, Telekomünikasyon Kurumu tarafından yetkilendirilmiş bir elektronik sertifika hizmet sağlayıcılarından elektronik sertifika temin etmeleri gerekmektedir.

Elektronik Sertifikalar kişilere ait olabileceği gibi kurumların ve web sunucuların da elektronik sertifikaları olabilir. Elektronik sertifika sahibinin kişisel bilgilerini ve bu kişisel bilgilere ait açık anahtar bilgisinin belirtilen kişi veya kuruma ait olduğunu temin eder.

Elektronik sertifikaların taklit edilemiyor olmaları gerekmektedir. Bunun sağlanmasının yolu sertifikaların güvenilir kurumlar tarafından dağıtılmasıdır. Sertifika sahibinin kimlik bilgileri ve açık anahtar sertifika hizmet sağlayıcıları tarafından onaylanıp imzalandıktan sonra sertifikaların dağıtımı yapılmalıdır. Burada sertifika hizmet sağlayıcısının imzanın taklit edilemez olması çok büyük bir önem taşımaktadır.

Burada; Sertifikalar ele alacak olursak önce basit sertifika kavramını incelemek gerekmektedir. Aşağıdaki şekil basit bir sertifika örneğini göstermektedir.



Şekil 4-Basit Sertifika Örneği

Asimetrik kriptografide bir kişi için üretilen anahtar çifti, özel ve açık anahtardan oluşur. Bu anahtarlardan açık olanı anahtarın sahibiyle haberleşmek isteyen

herkes tarafından görülebilir ve kullanılabilir. Bu açık anahtarın isteyen kişilerce kullanımını kolaylaştırmak için değişik şekillerde yayınlanması ve isteyenlerin erişimine açılması mümkündür. Bu yayınlama şekline sertifika adını verilmektedir.

Açık anahtar yayınlama biçimlerinden birisi kişisel kartvizitin bu amaçla kullanılması olabilir. Kartvizitleri basit sertifikalar olarak kullanmak mümkündür. Bir toplantı yapıldığını ve Şerafettin Bey'in herkese kartvizitini dağıttığını düşünelim.¹²⁰

- Bu kullanım tarzında aşağıdaki noktalar dikkati çekmektedir.
- Şerafettin Bey kartvizitin arkasındaki açık anahtara denk gelen özel anahtarın kendisinde olduğunu iddia etmektedir.
- Bu kartı alan Burcu Hanım kartta Şerafettin Bey'in ismi yazdığı için karttaki açık anahtarın ona ait olduğunu varsayar.
- Burcu hanım kartı elden alsa bile kartın üzerinde yazan isim ve şirket bilgilerinin doğruluğu şüphelidir:
- Kart üzerindeki bilgilerin güncel olması garanti edilemez.
- Şerafettin Bey 1 ay sonra işinden çıkarsa veya özel anahtarını kaybederse kartviziti anlamsız olacaktır ama bunu kime ve nasıl duyuracaktır?
- Burcu hanım,kriptografik işlemlerde kullanmak için bu açık anahtarı eliyle ve hatasız olarak bilgisayarına girmelidir.

İlk başta oldukça pratik görünen bu yöntem aslında yukarıda bahsedilen sakıncaları taşımaktadır. Bunun için ideal sertifika nitelikli sertifika kavramalarına bakalım.

4.3.1. İdeal ve Nitelikli Elektronik Sertifikalar

Nitelikli Sertifikayı incelemeden önce ideal bir sertifika nasıl olmalıdır ve hangi özellikleri taşımalıdır:

- Elektronik ortamda (örneğin: internette) yayınlanabilmesi ve otomatik olarak işlenebilmesi için tamamen sayısal olmalıdır.

¹²⁰ Ersin Gülaçtı (hızl.),. "Açık Anahtar Altyapısı", <http://www.kamusm.gov.tr/tr/Bilgideposu/Belgeler/teknik/aaa/index.html> (19 Temmuz 2007), s.17.

- Özel anahtarın sahibinin adını, çalıştığı şirketin/kurumun adını ve irtibat kurmak için gerekli bilgileri içermelidir.
- Sertifikanın ne zaman yayınlandığını anlamak kolay olmalıdır.
- Özel anahtarın sahibi tarafından değil güvenilir bir 3. kurum tarafından yaratılmalıdır.
- Güvenilen kurum birçok sertifika yaratacağı için (aynı kullanıcı için bile birden fazla) her bir sertifikanın diğerinden kolayca ayırt edilebilmesi gereklidir.
- Bir sertifikanın gerçek veya sahte olduğu kolayca tespit edilebilmelidir.
- Değiştirmeye karşı korunmuş olmalıdır.
- İçindeki bilgilerin güncel olup olmadığı istendiği anda tespit edilebilmelidir.
- Hangi uygulamalar için kullanılabileceği sertifikanın içinde yazmalıdır.¹²¹

Seri No	3125
Sertifika Sahibi	Şerafettin SÖNMEZ
Şirket/Kurum	T.C. Başbakanlık Devlet Arşivleri Gn.Md.
Yayınlayan	UEKAE
E-posta adresi	ssonmez@basbakanlik.gov.tr
Yayın Tarihi	30.06.2007
Son Kullanım	30.06.2008
Açık Anahtar	05487d24235d2df5as5df1525531 221dfd5f5455487
Yayınlayan Kurumun Sayısal İmzası	dk54578e5sd1f4587f5f4s2fs4f5sf ddf44547wd4545

Şekil 5-İdeal Sertifika Örneği

Nitelikli elektronik sertifikalar ise, kanunlar veya yönetmeliklerle nitelikleri belirlenmiş olan elektronik sertifikaların özelliklerine ek olarak bazı teknik

¹²¹ Gülaçtı, [t.y], s.26

gereksinimleri saęlayan ve sertifika sahibinin kişisel bilgilerini içeren elektronik sertifika türüdür.¹²²

Nitelikli Sertifika (Qualified Certificate), X.509 Sertifikası baz alınarak hazırlanan ve sadece gerçek kişilere verilen bir sertifika çeşididir. Bu sertifika tipi RFC 3739'da tanımlanmıştır. Nitelikli sertifikalar Türkiye'de ve bir çok Avrupa ülkesinde elle atılan ıslak imzaya eşdeğer elektronik imzalar atmak için kullanılır. Bu sertifikaları standart X.509 sertifikasından farklı kılan en önemli özellik üretiminde ve sahibine verilmesinde çok sıkı kimlik doğrulama kuralları uygulanması ve sertifika merkezlerinin işletiminin denetlenmesi olarak sayılabilir.

Nitelikli sertifikalar Türkiye'de, 5070 Sayılı Elektronik İmza Kanununda (Kanun) tarif edilmiştir. Kanunda görevlendirilen Telekomünikasyon Kurumu tarafından hazırlanan Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik (Yönetmelik) ve Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ (Tebliğ) ile Elektronik Sertifika Hizmet Sağlayıcıları (ESHS) ve onların üreteceği nitelikli elektronik sertifikalar konusunda düzenlemeler yapılmıştır.¹²³

4.3.2.Sertifika Başvurusu e-Sertifikanın Oluşturulması

Elektronik sertifika talep üzerine oluşturulur. Bu nedenle öncelikle elektronik sertifika başvurusu gereklidir. ESHS, nitelikli elektronik sertifika başvurusundan sonra sertifikayı oluşturur ve sertifika sahibine teslim eder. Nitelikli elektronik sertifikaların sözleşmeyle belirlenen bir süreleri vardır. Ayrıca sertifikayı veren kurum kullanımı ile ilgili olarak kullanıcıyı aydınlatma ve yol göstermekle mükelleftir.

Başvurular şahsi olabileceği gibi kurumsal başvuru da olabilir. Yönetmelikte kurumsal başvuru, bir tüzel kişiliğin çalışanları veya müşterileri veya üyeleri yahut hissedarları adına yaptığı nitelikli elektronik sertifika başvurusudur denilmektedir.

¹²² Tuğrul Sevim, “Elektronik İmzanın Hukuksal Boyutları Mevcut Durum, Eksiklikler ve Çözüm önerileri”, **II. Türkiye Bilişim Şurası**, Ankara: Başbakanlık, 10-11 Mayıs, 2004. s.341.

¹²³ Gülaçtı, [t.y.], s.44

Elektronik sertifika hizmet sağlayıcı, nitelikli elektronik sertifikayı, elektronik imza sahibine sigorta ettirerek teslim etmekle yükümlüdür.¹²⁴ Bu amaçla Telekomünikasyon Kurumunca hazırlanan, Kanunda öngörülen ikincil mevzuat düzenlemelerinde olan ve Hazine Müsteşarlığı'nın görüşleri alınarak çıkarılan "Sertifika Mali Sorumluluk Sigortası Yönetmeliği" 25565 Sayılı Resmi Gazete'de yayınlanmıştır.

4.3.3. Elektronik Sertifikanın yayımlanması ve yenilenmesi

Elektronik sertifikalar üçüncü kişiler tarafından erişilebilir halde tutulmalıdır. Bunu sağlamak amacıyla ESHS sertifikaları yayımlamak durumundadır. Yukarıda ismi geçen yönetmeliğin 11. Maddesine göre ESHS, sertifika sahibinin onayını almak kaydıyla nitelikli elektronik sertifikayı kamuya açık bir dizinde yayımlamak ve dizin hizmetinin kesintisiz olarak verilmesini sağlamak zorundadır. Açık anahtar altyapısı off-line çalışabilecek bir yapıdadır. Fakat, işlemi gerçekleştirdiğimizde elektronik sertifika geçerli bir sertifika olmayabilir.

Elektronik sertifikalar belli bir süre için verilirler. Bu nedenle, süre sonunda veya süre dolmadan talep halinde yenilenmeleri gerekir. Nitelikli elektronik sertifika, geçerlilik süresinin sona ermesinden önce sertifika sahibinin onayını almak koşuluyla kurumsal başvuru sahibinin talebi doğrultusunda ESHS tarafından yenilebilir.

Sertifikanın yaşam çevrimi aşağıdaki durumlarda sona erer:¹²⁵

Sertifikanın İptali: AAA sistemlerinde özel anahtarların gizli tutulması gerekir. Eğer bir kullanıcının özel anahtarının gizliliği tehlikeye girmişse ya da özel anahtar çalınmışsa, bu kullanıcının sertifikası iptal edilmelidir. Daha sonra bu kullanıcı için yeni bir anahtar çifti üretilerek yeniden sertifikasyon yapılabilir.

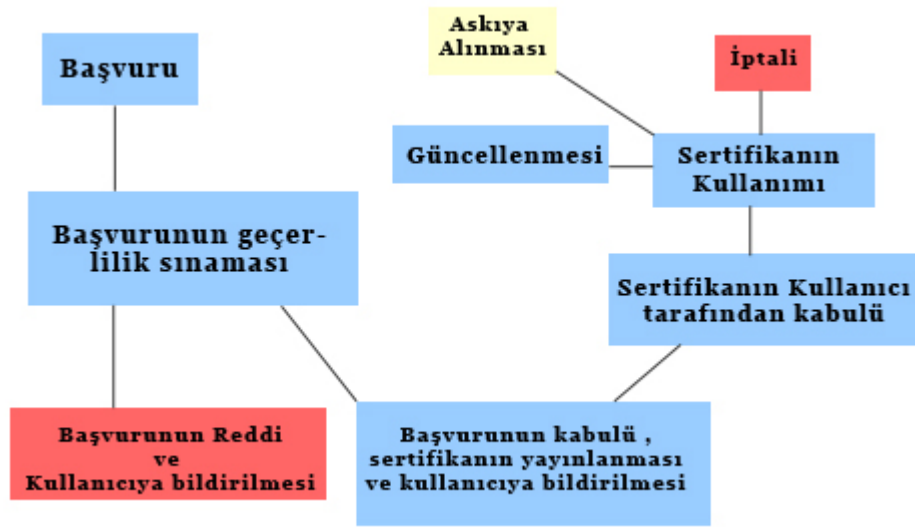
Sertifikanın zaman aşımına uğraması: Her sertifikanın bir geçerlilik süresi vardır. Bu süre aşıldığında sertifika kullanılamaz. Bu durumda sertifikanın güncellenmesi gerekir (yeniden anahtarlandırma). Geçerlilik süresi dolan veya iptal

¹²⁴ 5070 Sayılı, "Elektronik İmza Kanunu", Kabul Tarihi:15.01.2004, Resmi Gazete Sayısı:25355, Resmi Gazete Tarihi:23.01.2004, Madde-13/son fıkra.

¹²⁵ Gülaçtı, [t.y.], s.54.

edilen sertifikalar bir arşivde tutulabilir. Böylece, önceki anahtarlarla şifrelenen mesajlara yeniden erişilebilecektir.

Sertifikanın askıya alınması ve askıdan indirilmesi: Bir sertifikanın kullanımı geçici bir süre için de olsa durdurulabilir. Buna sertifikanın askıya alınması denir. Askıya alınan bir sertifika, askıdan indirilene kadar kullanılamaz.



Şekil 6-Sertifika Yaşam Çevrimi

Kaynak: Gülaçtı, s.38.

4.4. SERTİFİKA MAKAMI

4.4.1. Sertifika Makamı

Sertifika makamı (SM), açık anahtar altyapısında yer alan sertifikaları ve sertifika iptal listelerini üretmekle görevli olan merkezi birime verilen addır. Sertifika makamı, donanım ve yazılım parçalarından ve sistemi işleten kişiler ve kurallardan oluşan bir yapıdır. Bir sertifika makamını diğer sertifika makamlarından ayırt edici özellikleri; adı ve anahtar çiftidir.¹²⁶

Türkiye'de 5070 Sayılı Elektronik İmza Kanununa göre Elektronik Sertifika Hizmet Sağlayıcıları (ESHS) tanımı yapılmıştır. Bir ESHS en az bir Sertifika Makamı işletir. ESHS

¹²⁶ Gülaçtı, [t.y.], s.30.

olarak faaliyet göstermek için gerekli kanuni koşulların neler olduğunu Yasal Mevzuat konu başlığı altında bulunabilir.

4.4.2. Sertifika Makamının Görevleri

Sertifika Makamının görevlerini şu şekilde kısaca sayabiliriz.

- Sertifika yayınlamak
- Sertifika durum bilgilerini güncel tutmak ve sertifika iptal listeleri (SİL) hazırlamak
- Güncel sertifikaları ve SİL'leri isteyen kişilere sunmak
- Süresi dolan ya da iptal edilen sertifikaların arşivini tutmak

Sertifika Makamının yayınladığı sertifikalarla ilgili şunları söyleyebiliriz.

- Bir SM, kullanıcılar ya da diğer SM'ler için sertifika yayınlatabilir.
- SM tarafından yayınlanan sertifika içindeki bilgiler, doğruluğu onaylanmış bilgiler olmalıdır.
- Eğer sertifika başka bir SM için yayınlanmışsa bu diğer SM'nin yayınladığı sertifikalara güvenildiğini gösterir.
- SM her sertifikanın içine kendi ismini yazar ve sertifikayı kullanan kişiler bu ismi ve SM'nin sayısal imzasını kontrol ederek sertifikanın doğruluğunu kontrol eder.

SM'nin birinci görevi özel anahtarını hem kullanım sırasında hem de diğer anlarda gizli tutmaktır. Bunu sağlamak için akıllı kart veya donanımsal güvenlik modülü (HSM:Hardware Security Module) gibi kriptografik modüller kullanılır. Bu modüllerin güvenlik standartları (ör:FIPS 140), NIST ve benzeri kurumlar tarafından yayınlanmıştır.

SM'nin ikinci görevi sertifika yayınlanmadan önce içeriğinin tamamen doğru olduğunu doğrulamaktır. Bu amaçla kullanıcının kimliği, şahsi bilgileri ve yetki seviyeleri tespit edilmelidir.

SM'nin üçüncü görevi yayınladığı tüm sertifikaların ve sertifika iptal listelerinin (SİL) kendi standart profiline uygun olmasını sağlamaktır. Farklı ya da eksik alanları olan sertifikalar yayınlamamalıdır.

SİL içindeki bilgiler (iptal edilen sertifikaların numaraları, iptal tarihleri ve iptal sebepleri) tam ve doğru olmalıdır. Bu SM'nin 4. görevidir.

SM'nin 5. görevi oluşturduğu sertifika ve SİL'lerin isteyen kişilere dağıtımını yapmaktır. Bu dağıtımı internet veya intranet üzerinde yapılabilir. Bu hizmeti verirken erişilebilirliğinin sürekli olması çok önemlidir. Sertifikalar herkese açık olmalıdır ama bu bazen sertifika sahipleri ile ilgili bilgileri açığa çıkarabileceği için sertifika dağıtımı her zaman internette yapılmaz.

SM'nin 6. görevi sertifikaların kullanım süresi dolduktan sonra da arşivlenmesidir. Buna ihtiyaç duyulur çünkü geçmiş bir tarihte aktif olan bir sertifika ile imzalanmış bir dokümanın geçerliliğini kontrol etmek için kullanım süresi dolmuş bile olsa o sertifikaya ihtiyaç vardır. Genellikle sertifikaların neden yaratıldıkları ve neden iptal edildikleri bir veritabanında saklanır ama saklama süresi ebediyen değildir. Bu süre kanunlarla (elektronik imza kanunu vb.) belirlenir.¹²⁷

4.4.3.Kayıt Makamı

Kayıt makamı (KM), sertifika makamı için sertifika başvurularını alır ve sertifika içine yerleştirilecek bilgilerin doğruluğunu kontrol eder. KM, bu bilgilerden bir sertifika isteği oluşturur. Kayıt makamı topladığı bilgileri SM'ye kendi sayısal imzasıyla imzalayarak iletir. Böylece SM sertifika isteğinin güvendiği bir kaynaktan gelip gelmediğini anlayabilir. Bu nedenle kayıt makamı kendi özel anahtarını çok iyi korumalıdır. Bir kayıt makamı birden çok SM için bu hizmeti verebilir.

KM'nin SM ile çalışması genelde iki şekilde olur:

KM sertifika isteği yapmadan önce gerekli bilgileri toplar ve doğruluğunu kontrol eder. Bu genelde KM'ye yapılan şahsi başvurularda kullanılan yoldur. Başvuran

¹²⁷ Gülaçtı, [t.y.], s.32-34

kiři kimlik ya da ehliyet gibi bir belge ile kim olduėunu KM'ye kanıtlar. Bu bilgilerle oluřturulan sertifika isteėi SM'ye iletilir.

Kiři sertifika isteėini elektronik ortamda yapar. rneėin bir e-posta adresinin kendisine ait olduėunu iddia eder ve sertifika ister. SM bu isteėi alır ve istek iindeki bilgileri doėruluėunu kontrol etmesi iin KM'ye gnderir. KM onay verdikten sonra SM sertifika isteėini cevaplar.¹²⁸

4.4.4. Elektronik Sertifika Hizmet Saėlayıcısının Faaliyetinin Sona Ermesi

Faaliyetin sona ermesi, Kurum tarafından faaliyete son verme řeklinde olabileceėi gibi ESHS'nin faaliyetine son vermesi řeklinde olabilir.

Elektronik sertifika hizmet saėlayıcıları, Kurum tarafından gerek grlen hallerde ve iki yılda en az bir kez re'sen denetlenir. Elektronik İmza Kanunun Uygulanmasına İliřkin Usul ve Esaslar Hakkında Ynetmelik, (Md. 22). 06.01.2005 Tarih ve 25692 Sayılı Resmİ Gazetede Yayımlanmıřtır. Kurum, yaptıėı denetim sonucunda, bildirimde belirtilen hususlardan birini veya birkaını kaybettiėini tespit ederse, sz konusu eksikliėi tamamlaması iin bir aya kadar sre verir. Bu sre zarfında ESHS'nin faaliyetini durdurur. Verilen sre sonunda eksikliėin giderilmemiř olması halinde ESHS'nin faaliyetine son verilir.

ESHS'nin faaliyetine son erme nedenlerinden bir diėeri, Elektronik İmza Kanunun 18. Maddesinde belirtilen suların iřlendiėi tarihten geriye doėru  yıl iinde nc kez iřlenmiř olması halidir.

Faaliyetine son verilen veya kendi kendine faaliyetlerini sonlandıran ESHS'ler mevcut kullanıcı bilgilerini, iř ve iřlemlerini yrtmeleri iin bařka bir ESHS'ye devir etmek zorundadırlar. Devir konusunda herhangi bir ESHS ile anlařma saėlanamamıř olması halinde, sertifikaların kime devredileceėini Denetleme Kurumu re'sen belirler. Devredilecek ESHS'nin Kurum tarafından hangi kıstaslara gre belirleneceėi ilgili ynetmelik ve kanunlarda aıklanmamıřtır.

¹²⁸ Glatı, [t.y.], s.31.

Nitelik elektronik sertifikaları devralan ESHS, sertifika yenileme işlemlerini derhal başlatır ve devir kararının kendisine tebliğinden itibaren bir ay içinde tamamlar. Kurumun uygun görmesi halinde, ESHS'ye bir ayı geçmemek üzere ek süre verilebilir.

Faaliyetine son verilen ESHS, nitelikli elektronik sertifikaları devralan ESHS'ye kimlik doğrulamada kullanılan belgeleri, dizini, arşivi ve sertifika yenileme işlemlerinin tamamlanmasından sonra iptal durum kaydını devreder ve kendi imza oluşturma verisi ile yedeklerini imha eder.

4.5. UYGULAMADA ÖZEL SERTİFİKA DOĞRULAMA PROBLEMİNE ALTERNATİF YAKLAŞIM

E-postalar, kişiler ve kurumlar arası bilgi alış verişini elektronik ortamda, bilgisayar aracılığıyla sağlayan ve her geçen gün hayatımıza biraz daha girmektedir. Başlangıçta düz metinleri göndermek amacıyla geliştirilmiş olan e-postalar, teknolojinin kat ettiği yol ve değişim katsayısının parabolik artışı ile ses, görüntü, video, html, doküman ve belgeleri de göndermeyi de mümkün kılmıştır.

Elektronik postalar başlangıçta her türlü bilginin yüksek hızlı ve düşük maliyetli bir şekilde iletimine olanak sağlamışsa da zamanla bir takım sorunları beraberinde getirmiştir. Elektronik haberleşme ortamlarında, bilginin yetkisiz kişilerin eline geçmesi yada ilgili kişi/ kurumun eline ulaşmaması gibi güvenlik problemlerine rastlanmaktadır. Bu durum kurumların ticari kayıplara uğramasına neden olabilmekte, özellikle askeri uygulamalar gibi bilginin gizli ve hızlı iletiminin büyük önem taşıdığı durumlarda çok ciddi sonuçlara neden olabilmektedir.¹²⁹ Askeri ve ticari uygulamada güvenlik ve güvenilirlik yaygın olarak Açık Anahtar Altyapısı ile sağlanmaktadır.

E-posta iletişimde karşılaşılan bir diğer problem ise farklı formatlarda bilgi taşınmasıyla transfer edilen bilginin veri uzunluğunu artmasıdır. Bu durum, düşük bant genişlikli, veri kaybı ve hataları yüksek bağlantısız taşıyıcı katmanı üzerinden yapılan ve “*Taktik Saha*” olarak adlandırılan ortamlarda veri transferini güçleştirmektedir.

¹²⁹ B. Şaşıoğlu, “Güvenli Kurumsal Mesajlaşma Uygulaması”, **Ulusal Elektronik İmza Sempozyumu**, Ankara, 7-8 Aralık, 2006, s.45

4.5.1. Güvenli Resmi Mesajlaşma Altyapısı

Güvenli mesajlaşmanın sağlanabilmesi için yerine getirilmesi gerekli olan başlıca unsurlar; veri kaynağının doğrulanması, gizlilik ve bütünlük, inkar edilememedir. Bu unsurlar doğrulama ve şifreleme yöntemleriyle sağlanmaya çalışılır. Buna ek olarak “S/MIME v3”¹³⁰ standardı kullanılmak suretiyle hazırlanan mesajlarda imzalı alındı notu¹³¹, güvenlik etiketleri, güvenli mesaj listesi gibi ilave güvenlik unsurları tanımlanabilmektedir.¹³²

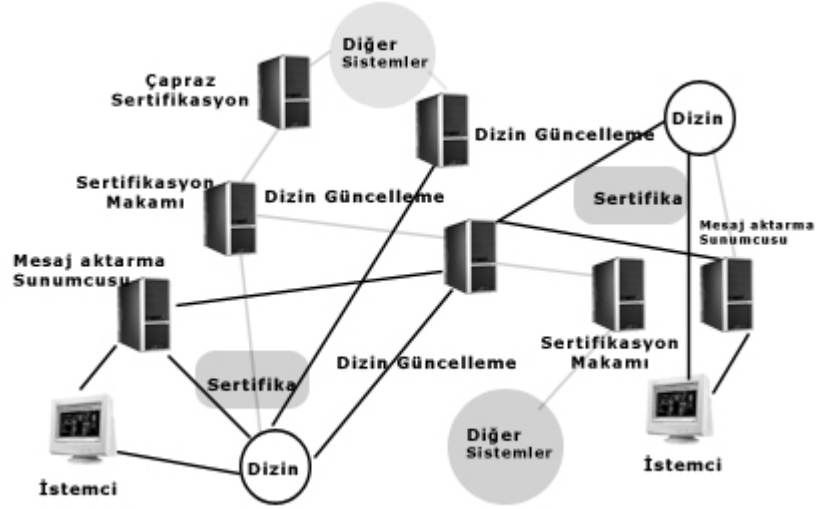
En genel anlamda e-posta iletiminde kullanılmakta olan mesajlaşma alt yapısının temeli, istemci olarak çalışan kullanıcı arayüzü bilgisayarları ile mesajların dağıtımını sağlayan “Mesaj aktarma Sunumcusu”ndan oluşmaktadır. Buna ilave olarak mesajlaşma sistemlerinde kullanıcılara özel bilgilerin tutulduğu “Dizin Sistemleri” ve “Sertifika Makamı”, “Akıllı Kart Okuyucuları”, “Akıllı Kartlar” gibi mesajların uçtan uca güvenliğini ve güvenirliliğini sağlamak amacıyla imzalama ve şifreleme için kullanılan bileşenler yer almaktadır.

Bu bileşenleri değerlendirdiğimizde karşımıza üç önemli altyapı çıkar.

¹³⁰ B. Ramsdell (Ed.), **S/MIME Version 3 Certificate Handling**, [y.y.]: [yayl. y.], 1999, <http://rfc.net/rfc2632.html>, (13 Haziran 2007) s.1-12.

¹³¹ B. Ramsdell (Ed.), **S/MIME Version 3 Messages specification**, [y.y.]: [yayl. y.], Network Working Group, Internet Engineering Task Force (IETF), <http://rfc.net/rfc2633.txt>, (17 Haziran 2007) s.1-32.

¹³² P. Hoffman (Ed.), **Enhanced Security Services for S/MIME**, [y.y.]: [yayl. y.], Network Working Group, Internet Engineering Task Force (IETF), <http://rfc.net/rfc2634.txt>, (17 Haziran 2007) s.42,54,58.



Şekil 7- Mesajlaşma Sistemi Genel Yapısı

Kaynak: European Committee For Standardization, Security requirements for signature creation applications, May 2004, Supersedes CWA 14170:2001, <ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14170-00-2004-May.pdf>, (25 Haziran 2008) s.11.

Dizin Sistemi (DS): Tüm e-posta kullanıcı bilgileri, sertifikalar ve iptal edilen sertifikalara ait SİL (Sertifika İptal Listeleri)¹³³, dizin adı verilen özel amaçlı veri tabanında saklanmaktadır. Dizin Sistemi, gerek “Güvenlik Altyapısı” ile gerekse “İstemci/Sunumcu Altyapısı” ile direk olarak görev yapmaktadır. “Güvenlik Altyapısı” tarafından oluşturulan Kullanıcı Sertifikaları ve iptal edilen sertifikaların listesinin tutulduğu SİL’ler DS’lerde tutulmaktadır. “İstemci/Sunumcu Altyapısı” ise DS’e mesaj göndermek istediği alıcıların e-posta kullanıcı bilgilerine ve geçerli sertifikalarına ulaşmak için bağlanmaktadır. Genelde mimariye göre DS’ler çok sayıda olup her bir dizindeki bilgilerin güncelliğini koruması gerekmektedir. DS’lerin bilgilerinin güncellenmesi özellikle taktik sahada önemli bir sorun olarak karşımıza çıkar.

Güvenlik Altyapısı: Yukarıdaki şekilde mesajlaşma sistemlerinde sıklıkla kullanılan Açık Anahtar Altyapısı gösterilmektedir. Sertifikasyon yöneticisi,

¹³³ R. Housley, W. Polk, W. Ford, D. Solo, **Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation list (CRL) Profile**, <http://www.ietf.org/rfc/rfc3280.txt>, (13 Nisan 2007)

yönetimden sorumludur. Şekilde sertifikanın saklanma mekanizması ve özel anahtarlar gösterilmiştir.

İstemci/Sunucu Altyapısı: Son kullanıcıların bulunduğu istemci makineleriyle e-posta¹³⁴ (SMTP) veya X400¹³⁵ Sunumcuları arasındaki ilişkiyi tanımlamaktadır.

4.5.2. Mesajlaşma Sistemlerinde Karşılaşılan Sorunlar

Taktik sahada bahsi geçen yöntemlerin kullanılmasında şu şekilde sorunlar yaşanmaktadır.¹³⁶

- Yüksek bant genişlikli bağlantılı taşıyıcı ortamlar için geliştirilen güvenli mesajlaşma yöntemleri taktik sahada çoğu zaman performans problemi yaratmaktadır.
- Taktik sahadaki bant genişliği, veri kaybı v.s. gibi ortam özelliklerinden kaynaklanan kısıtlar nedeniyle mesajlaşma kapasitelerinden ve/veya uçtan uca güvenlikten ödün verme durumu ortaya çıkmaktadır.
- Taktik sahada kablosuz bağlantı tiplerinde her türlü saldırı olasıdır. Güvenli haberleşmeyi sağlamak bağlantılı ortamlara göre daha büyük bir sorun olarak karşımıza çıkmaktadır.

Standart protokolleri her seviyede kullanmak sistemlerin birlikte çalışmasını ve esnekliği sağlamakta ancak yukarıda özetlenen sorunlar ortaya çıkmaktadır. Bu sorunların üstesinden gelmek için kablosuz iletişim ortamlarında protokollerin basitleştirilmesi yöntemi benimsenir. Burada ana prensip taşınan verinin mümkün olduğunca azaltılması ve bu şekilde bant genişliğinden tasarruf sağlanmaktadır.¹³⁷ Ayrıca kablolu ortamlarda kullanılan “Ulaşım Katmanı” protokolleri kablosuz ortamlara uygun olmadığından bu katmanda protokol değişikliğine gidilir.

¹³⁴ SMTP Service Extension for Secure SMTP over TSL, (t.y.), <http://www.ietf.org/rfc/>, (25 Haziran 2008)

¹³⁵ Data Communication Networks, (t.y.), <http://ocw.mit.edu/OcwWeb/Electrical-Engineering-and-Computer-Science/6-263JData-Communication-NetworksFall2002/CourseHome/> (13 Haziran 2007)

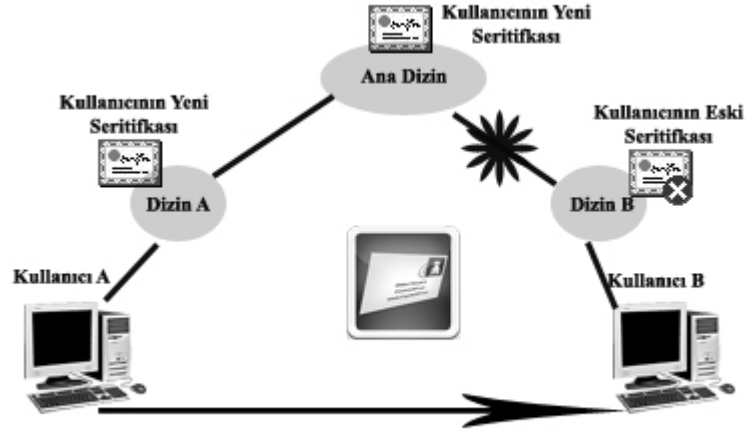
¹³⁶ STANAG, 4406 Annex E: Tactical MMHS Protocol and Profile Solution, Version 2, <http://www.isode.com/solutions/military-messaging.html>, (13 Haziran 2007)

¹³⁷ R. Friend, Transport Layer Security (TLS) Protocol Compression Using Lempel-Ziv-Stac LZS, Network Working Group Request for Comments: 3943, Category: Informational, <http://tools.ietf.org/rfc/rfc3943.txt>, s.2,6,8-9.

4.5.3. Sertifika Doğrulama Problemi ve Çözüm Önerileri

Dizin sistemleri içerisinde bulunan farklı dizinlerin içeriklerinin güncel bilgileri taşıyabilmeleri için belli koşullarda verilerin kopyalanması gerekmektedir. Bu güncelleme işlemi için büyük miktarda veri transferine ihtiyaç duyulmaktadır. Özellikle taktik sahada, ortam koşulları gereği zaman zaman veri transferi kesintiye uğramaktadır. Bu sorunu ele almak için bir senaryo oluşturup dizinde tutulana ve güncellenmesi gereken bir İmzalama Sertifikasının veya SİL'in güncellenmemesi durumudur.

Şekil 7'de belirtilen durumda, B kullanıcısının bağlı olduğu dizinde A kullanıcı ucuna ait imzalama sertifikası güncellenememekte ve bu esnada acil ve gizli bir mesaj A kullanıcısından B kullanıcısına gönderilmek istenmektedir. Bu durumda mesajın direkt olarak (aracı olmaksızın) ya da Güvenilir Mesaj Aktarım Bildirimi (GMAB) aracılığıyla ulaştırılması şeklinde iki çözüm değerlendirilmektedir. Burada GMAB güvenilir makam rolünü üstlenmekte ve kendisine ulaştırılan mesajların alıcılarına mesajları güvenli bir biçimde iletmekle sorumludur. Bu birimin kimliğine her zaman güvenilmesi gerektiği için bazı özel koşullar sağladığı varsayılmaktadır. GMAB kendi imzalama ve şifreleme özel anahtarlarını güvenli bir ortamda saklar, çalınması veya iptal edilmesi gibi durumlar söz konusu değildir. Açık anahtarları ise sahadaki kullanıcı makinelerinde gömülü olarak bulunur ve güvenilen sertifikalar arasında yer alır. GMAB sertifikasının değişmesi gerekiyorsa, yeni açık anahtarların bulunduğu sertifikaların uç kullanıcılara güvenilir yollarla ulaştırılması sağlanır. GMAB'nin güncel dizin sistemine kesintisiz erişimi vardır; imza doğrulama ve şifreleme işlemlerini her zaman güncel sertifika ve SİL'leri ile yaptığı için sahadaki kullanıcılar GMAB'den gelen mesajların gerçekten mesajın göndericisi tarafından gönderildiğini bilir.



Şekil 8- A kullanıcı ucundan A'nın Güncel Sertifikası Olmayan B kullanıcı ucuna Direkt mesajlaşma

Olası senaryo olan; direkt mesajın ulaşmasını inceleyelim:

SİL güncel değildir ve göndericinin sertifikasına erişilebilmektedir. Bu durumda göndericinin imzalama sertifikası dizinden çekilebilmiş ya da göndericinin sertifikası yenilenmiş ve gönderici S/MIME v3 standardında tanımlanan seçenekli olarak bırakılmış olan sertifikanın mesaj içerisinde gönderilebilmesi özelliğini kullanarak yeni sertifikasını mesaj ile birlikte alıcıya ulaşmamıştır. Her iki durumda da alıcı gönderenin sertifikasının zincir kontrolü yapılmalı ve bu sertifikanın SİL'de olup olmadığını kontrol etmelidir. Böyle mesajın gerçekten göndericiden geldiğini ve bütünlüğünün korunduğunu anlayabilecektir.

Göndericinin sertifikasının SİL'de yer alıp almadığını kontrol etmek için dizinden liste çekilmiş fakat listenin güncelliğini kaybettiği görülmüştür. Dizin sistemi imkansızlıklar yüzünden güncelliğini kaybetmiştir. Bu durumda alıcının SİL kontrolünü yapabilmesi için sertifika içerisinde belirtilen Online Certificate Status Protokol (OCSP) veya CRL Distribution Point (CRLDP) adreslerini çevrimiçi kullanması gerekecektir.¹³⁸ Burada belirtilen OCSP, bir sertifikanın iptal edilip edilmediğine dair güncel bilginin çevrimiçi alınabilmesini sağlayan bir protokoldür. İstemci, durumu

¹³⁸ M Myers, R. Ankney, A. Malpani ve Diğerleri, **X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol-OCSP**, <http://www.ietf.org/rfc/rfc2560.txt>, (17 Mayıs 2007).

sorgulamak istediđi sertifikaya ait ayırt edici bir özellik (yayıncı, seri numarası, açık anahtarın özeti gibi) ve diđer eklentilerden oluşan hizmet isteđini OCSP sunucusuna gönderir. Sunucu sertifikayı veren makama ya da istemci tarafından açık anahtarına güvenilen bir OCSP sunucusuna ait olabilir. CRLDP adres noktalarında ise ilgili sertifikayı yayıncı kuruluşun güncel SİL'leri bulunmaktadır.

OCSP kullanılması durumunda alıcının çevrimiçi bir adrese bağlanarak istekte bulunması ve dönen cevabı doğrulayarak işleme devam etmesi gerekmektedir. Dönen cevabın imzalı olması boyutunu artırarak kısıtlı olan bant genişliğinde alınması sorun yaratabilecektir. Ayrıca güvenlik hat safhada olduđu için tekrar saldırılardan korunmak amaçlı büyük bir rasgele sayının üretilip istekle beraber gönderilmesi ve dönen cevapta aynı sayının geri döndürölmesi beklenmektedir. Bu büyük sayı da trafikteki verinin boyutunu arttırabilmektedir.

CRLDP kullanılması durumunda alıcın SİL'in tamamını yereline indirmesi gerekecektir. 10.000 sertifika barındıran bir Sertifika Makamı yayınladıđı SİL'in ortalama olarak 1 MB olduđu düşünölüđünde kısıtlı bant genişliğinde bu verinin de indirilip kullanılması sorun teşkil edebilmektedir.

Sertifika içerisinde OCSP ve CRLDP adreslerinin verilmediđi, bu servislerin çalışmadıđı ya da alıcının bu servislere bağlanma imkânı olmadığı durumlarda (taktik sahada bağlantı kurulmasının sakıncalı olduđu pasif olarak dinleme yapılabildiđi durumlar olabilir) alıcı güncel SİL'e ulaşamayarak sertifikanın güncelliđini kontrol edemeyecek ve mesajın gerçekten göndericisinin tarafından gönderilmediđini anlayamayacaktır.

4.5.4. Sertifika Geçerlilik Kontrolündeki Sorunların Giderilmesi

Bir sertifikanın geçerliliđinin kontrol edilmesi uzun ve kritik bir süreçtir. Bu süreç içerisindeki bir hata geri dönölmez sonuçlara yol açabilir. Örneđin, iptal edilmiş bir sertifika ile atılan bir imza geçerli olmayan bir verinin geçerli sayılması demektir. Sertifika geçerlilik kontrolü, elektronik sertifikayla ilgili her işlem sırasında yapılmalıdır, çünkü sertifika her an iptal edilebilir, süresi dolabilir ya da yerine yeni sertifika üretilebilir. Geçerlilik kontrol süreci içerisinde sadece sertifikanın kendisi

değil, sertifikayı veren Elektronik Sertifika Hizmet Sağlayıcısı (ESHS) sertifikalarının da geçerliliği kontrol edilmelidir. Bir sertifikanın geçerli olabilmesi için:

1. Sertifikanın başlangıç ve bitiş tarihleri arasında olması gerekmektedir.
2. Sertifika güvenilir köklerden üretilmelidir. Eğer en üst kök değil ise , sertifikayı üreten köklerin (ESHS'lerin sertifikalarının) bulunması ve bu kök sertifikaların da geçerliliklerinin ve imzalarının geçerliliği kontrol edilmelidir.
3. Sertifika iptal edilmemiş olmalıdır. Sertifika geçerlilik kontrol süreci de görüntülenmektedir.

Bir sertifikanın üst kökü bulunurken sertifikanın içerisindeki bilgilerden yararlanılır. Her sertifikanın içerisinde Özne Anahtar Tanımlayıcısı(SKI) ve ESHS Anahtar Tanımlayıcısı(AKI) bilgileri vardır. Özne anahtar tanımlayıcısı sertifikanın kendisini, ESHS anahtar tanımlayıcısı da sertifikayı üreten kök sertifikanın özne anahtar tanımlayıcısını gösterir. Bir sertifikanın üst kökünü bulmak için , içerisinde bulunan ESHS anahtar tanımlayıcısı bilgisi ile tüm kök sertifikaların özne anahtar tanımlayıcıları karşılaştırılır. İki değer birbirine eşit olduğunda da sertifikanın kökü bulunmuş olur. Fakat sadece sertifikayı bulmak yeterli değildir, bulunan sertifikanın da geçerliliğinin ve imzasının kontrol edilmesi gerekmektedir.

Sertifikanın iptal durumu ise; sertifikayı üreten ESHS'nin yayınladığı Sertifika İptal Listelerine(SİL) bakarak, ya da ESHS'ye ait OCSP sunucu aracılığıyla olmak üzere iki şekilde öğrenilebilir.

5. BÖLÜM- ELEKTRONİK BELGE VE E-İMZANIN SAĞLAMİŞ OLDUĞU GÜVENLİK

5.1-ELEKTRONİK BELGE

Elektronik belge denildiğinde, en basit ifadesiyle elektronik ortamda sayısal olarak kodlanmış şekilde bulunan elektronik veriler bütünü kastedilmektedir. Bu anlamda karşımıza çıkan elektronik doküman, elektronik belge ve elektronik kayıt gibi kavramlar söz konusudur. Bu kavramlar genel anlamda birbiriyle aynıymış gibi görünse de aslında mesleki terim bakımından aynı şeyleri ifade etmez. Her ne kadar aynı manayı ifade etmese de elektronik ortamda oluşturulan bilgiyi ifade etmek üzere kullanılır.

Belgenin sözlük anlamı “*bir gerçeğe tanıklık eden yazı, fotoğraf, resim, film vb. vesika doküman*”dır.¹³⁹ Belge kavramı günümüze kadar, günlük hayatta kullanıldığı şekliyle çoğu zaman, kağıt üzerinde cisim bulmuş olma unsuruyla bağdaştırılmıştır. Çünkü bu şekliyle kâğıt üzerindeki belgelerin istenildiği anda ibraz edilmesi ve her an gözle algılanabilir şekilde bulunması özelliklerinin getirdiği faydalar ve avantajlar, kağıtta tecessüm etmiş belgelerin şimdiye kadar tercih edilmesini ve yaygın kullanımını sağlamıştır. Bu anlamda elektronik belge kavramı algılama yönünde ilk etapta insanlara ters gelen bir kavram olabilir. Belgelerin herhangi bir yardımcı araç olmaksızın görülebilmesi her zaman algılanabilir olduğu anlamındadır. ¹⁴⁰

Elektronik belge terimi, kâğıda dayalı belgeler karşısında bir sınırlamayı ifade eder ve bununla açıklamanın bulunduğu veri taşıyıcısının nitelemesi anlatılır. Sayfa üzerinde, işaretler ve harflerden oluşan bir yığın taşıyan kâğıt belgeler gibi, elektronik belgeler de çoğunlukla o zamanki işletme sistemi anlamında, bir ya da daha fazla veriler formunda, bilgi yığını içerir.

Kâğıt belgelerin aksine, elektronik belgelerde en önemli sorun, belgenin içeriğinin sonradan değiştirilip değiştirilmediğini hakkındaki kaygı ve endişelerdir. Türk Hukuk sistemi açısından da ilerleyen bölümlerde değineceğimiz bu konu Elektronik

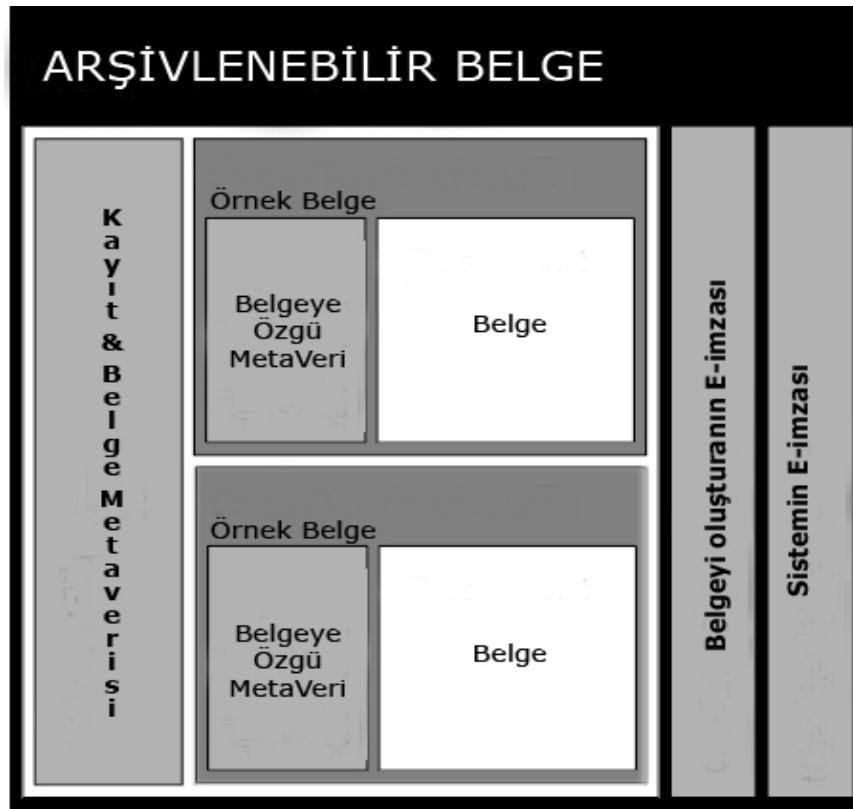
¹³⁹ Türk Dil Kurumu Genel Türkçe Sözlüğü, “Belge”, <http://www.tdk.org.tr/sozluk>, (23 Ağustos 2007)

¹⁴⁰ Billur Yaltı, “E-imza ve E-Belge: Kâğıtsız ve mürekkepsiz Dünyada Hukuk-I”, **Vergi Sorunları Dergisi**, Sayı.151, (Nisan, 2001), s. 131.

Belge Yönetim Sistemi Standartlarıyla aşılacak bir durumdur. Çünkü elektronik belge ve elektronik doküman kavramları birbirlerinden farklı kavramları işaret eder.

5.2-ELEKTRONİK BELGE –ELEKTRONİK İMZA İLİŞKİSİ

Elektronik belgede belirtilen sistem kriterleri, belge kriterleri ve üstveri kriterlerini incelendiğinde elektronik imzanın elektronik belgede fonksiyonel ve etkin bir role sahip olduğunu görülmektedir.



Şekil 10- Standart uzun dönemli Elektronik Kayıt yapısı

Kaynak: Ross Gibbs , Justine Heazlewood (hzl.), **Electronic Records – Problem Solved?: the Victorian Electronic Records Strategy and the future of electronic record keeping in Victoria,** http://www.vala.org.au/vala2000/2000pdf/Gib_Hea.PDF, (30 Haziran 2008)

Şekil 10’da belgenin elektronik ortamda oluşturulurken belgeye özgü metaveri ve belge içeriği ile şekillendiği görülmektedir. Elektronik belgeyi oluşturan E-imzası ve sistemin e-imzası da mevcuttur.

5.3-E-İMZANIN E-BELGEDEKİ ROLÜ

E-imza ve e-belge yönetimi birbirini tamamlayan iki uygulamadır. Belirli program ve stratejilere göre oluşturulmuş e-belge yönetim birimi olmadan başarılı bir e-imza uygulamasını sürdürmek mümkün değildir. Aynı şekilde e-imza olmadan geçerli ve güvenilir bir e-arşiv uygulaması düşünülemez. E-belge yönetiminin geleneksel belge yönetimine göre bir farklılığı da belgelerin yanında e-imza ve e-sertifikaların da arşivlenmesi gerektiğidir. E-imzalı belgelerin arşivlenmesine yönelik olarak önemli yönergeler içeren Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkındaki Yönetmelik'in 14. maddesinde, ESHS'lerin, geçerlilik süresi sona eren nitelikli e-sertifikaları, başvuru sırasında talep edilen bilgi, belge ve elektronik verileri, sertifika ilkelerini ve uygulama esaslarını, zaman damgası ilkelerini ve uygulama esaslarını, nitelikli e-sertifika yönetimine ilişkin tüm işlemleri, işlemlerin yapıldığı zamana ve işlemleri yapan kişiye ait bilgileri içeren kaydı en az yirmi yıl saklaması gerektiği belirtilmiştir. Bu durumda arşivlenen e-sertifikalar, hukuksal zorunluluğunun yanında ESHS'lerin önemini artırırken, gerek kurum gerekse devlet arşivleri yöneticileri için eşsiz bir bilgi kaynağı konumunda olacaktır. Daha önce de bahsedildiği üzere e-sertifikalar sınırlı bir sürede geçerliliklerini korur. Arşivlenecek e-imzalı belgelerin uzun süre geçerliliğini koruyabilmesinde önemli olan, imzanın bir kez geçerli bulunmasından yıllar sonra da geçerliliğinin doğrulanabilmesi ve korunabilmesidir. Bu durum taraflar arasında fiziksel ortamda yapılan bir sözleşmenin geçerli olduğu süre zarfında taraflarca saklanmasına benzetilebilir. E-ortamda yapılan bir anlaşma da geçerli olduğu sürece taraflarca atılan e-imzaların geçerliliğinin korunması gerekecektir. Bu doğrulama e-imzanın belirli bir tarihten önce varolduğunu ispat eden arşiv amaçlı elektronik imzanın bir bileşeni olan zaman damgası fonksiyonu ile saklanabilir. Zaman damgası, bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı zamanın tespit edilmesini sağlayan ve ESHS firma tarafından veriye eklenen elektronik bir mühürdür. E-arşivlemede karşılaşılabilecek önemli sorunlardan biri e-imza oluşturulurken kullanılan kriptografik algoritmaların ve zaman damgasının zamanla zayıflaması ve kırılabilir hale gelmesi olacaktır. Bu zayıflamalara karşı e-belge yönetim

döngüsü sürecinde arşivlenen imzanın geçerliliğini koruyabilmesi için periyodik olarak tekrar güçlendirilmesi gerekecektir.¹⁴¹

5.4. KÖTÜCÜL VE CASUS YAZILIMLARA KARŞI ELEKTRONİK İMZANIN SAĞLAMİŞ OLDUĞU KORUNMA DÜZEYİ

İnsanların kullanımına sunulan birçok yeni teknolojik altyapının sergilediği kolaylık ve kullanışlılığı gölgeleyebilecek en önemli etkenlerin başında, bilgi ve bilgisayar güvenliği gelmektedir. E-imzanın gerek kişisel ve gerek kurumsal alanda yaygınlaşabilmesi ve var olan geleneksel yapının yerini alabilmesi için yerine getirilmesi gereken en önemli şart, bu teknolojiye olan itimadın toplum içerisinde yaygınlaşması ve bir daha zarar görmeyecek şekilde sağlam bir biçimde yerleşmesidir. Günümüzde, artan sayıda ülkede bir belgenin elektronik olarak imzalanmasının yasal sonuçları bulunmaktadır. Ülkemizde de bu durum, Ocak 24 tarihinde kabul edilen E-imza kanuna göre “*Güvenli elektronik imza, elle atılan imza ile aynı hukuki sonucu doğurur*” şeklinde tanımlanmış ve açıkça belirtilmiştir. Bunun için e-imza kullanımında karşılaşılabilecek güvenlik tehdit ve risklerinin belirlenmesi ve bunlara karşı korunma sağlayacak güvenlik alt yapısının oluşturulması ve kullanıcılara sağlanması gerekmektedir. Bu konu hiçbir şekilde göz ardı edilemeyecek kadar çok önemlidir.

Bilgi ve bilgisayar güvenliği, elektronik ortamda verilerin veya bilgilerin saklanması ve taşınması esnasında bilgilerin bütünlüğü bozulmadan, izinsiz erişimlerden korunması için, güvenli bir bilgi işleme zemini oluşturma çabalarının tümüdür. Bunun sağlanması için, uygun güvenlik politikaları belirlenmeli ve uygulanmalıdır.¹⁴²E-imza uygulamalarında, bilgi ve bilgisayar güvenliği bütün etkenleri ve kapsamıyla ele alınması gerekir.

Elektronik imza oluşturulan yazılım ve donanımlar olarak tanımlanan imza oluşturma uygulamalarını (İOU) güvenli hale getirmek için ortaya atılan yaklaşımların çoğu kullanılan şifreleme algoritmaları ve akıllı kart içinde gerçekleştirilen

¹⁴¹ Esin Altın, “Türkiye’de Elektronik İmza ve Elektronik Devlet Uygulamaları:Elektronik Belge Yönetimi Açısından Bir Değerlendirme Denemesi”, **Değişen Dünyada Bilgi Yönetimi Sempozyumu**, [y.y.] :[yayl. y.], 24-26 Ekim 2007, Ankara, s.150-157.

¹⁴² Şeref Sağıroğlu, Gürol Canberk, “Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme”, **Gazi Üniversitesi Politeknik Dergisi**, Cilt.9, Sayı.3, 2006,s.165-174.

hesaplamaların güvenliği üzerine yoğunlaşmaktadır. Tamsayıların çarpanlarına ayrılması, ayrık logaritma ve eliptik eğrilere dayanan yönetmeler ile bu konuda önemli aşamalar kat edilmiş olsa da; imza oluşturma uygulamasının çalıştığı ortam yazılımlar, gerek kullanıcılar tarafından gerekse bizzat bu yazılımları ürene firmalar tarafında göz ardı edilmektedir.¹⁴³ Avrupa Standardları Komisyonu’nun 2004 yılında hazırlamış olduğu rapora göre; normal olarak imza oluşturma uygulaması ile aynı ortamda çalışan, fakat elektronik imza oluşturma sürecine doğrudan dahil olmayan sistemler, uygulama programları, çevre birim ve haberleşme kanalları “güvenilmez” olarak ele alınmalıdır.¹⁴⁴ Bu açıdan bakıldığında elektronik imza oluşturma uygulamalarının karşı karşıya olduğu en büyük güvenlik tehlikelerinin başında kötücül ve casus yazılımlar gelmektedir.

5.4.1.E-imza ve İmza Oluşturma Sürecindeki Genel Güvenlik Ölçütleri

E-imza ile güncel teknolojiler kullanılarak, işlemleri güvenli bir şekilde yapmak; iş verimliliğini arttırmak; iş akışını hızlandırmak; bürokrasiyi azaltmak; dünya ile hızlı bir şekilde bütünleşmek; küresel pazarlara açılmak; kâğıttan elektronik belgeye geçişi sağlamak mümkün olabilecektir.¹⁴⁵

E-imzanın güvenlik unsurlarını hatırlayacak, olursak kimlik kanıtlama, inkar edememe, bütünlük ve gizlilik olduğunu söyleyebiliriz. E-imzada bu unsurların sağlanması için, özetleme fonksiyonları veya açık anahtar altyapısı gibi, günümüz bilgi işlem güç ve kapasitesi ile çözülmesi veya kırılması neredeyse imkânsız olan şifreleme algoritmaları kullanılmaktadır.¹⁴⁶ Bu açıdan e-imza; şifrelenmiş bilgilerin şifresini kırmak veya çözmek için yapılan, kaba kuvvet, sözlük, ortadaki adam, salt şifreli metin, bilinen düz metin, seçilen düz metin veya şifreli metin saldırıları gibi kriptanaliz

¹⁴³ Adrian Spalka, Armin B. Cremers, Hanno Langweg, “Trojan Horse Attacks on Software For Electronic Signature”, **Informatica**, Vol.26, 2002, s. 191-203.

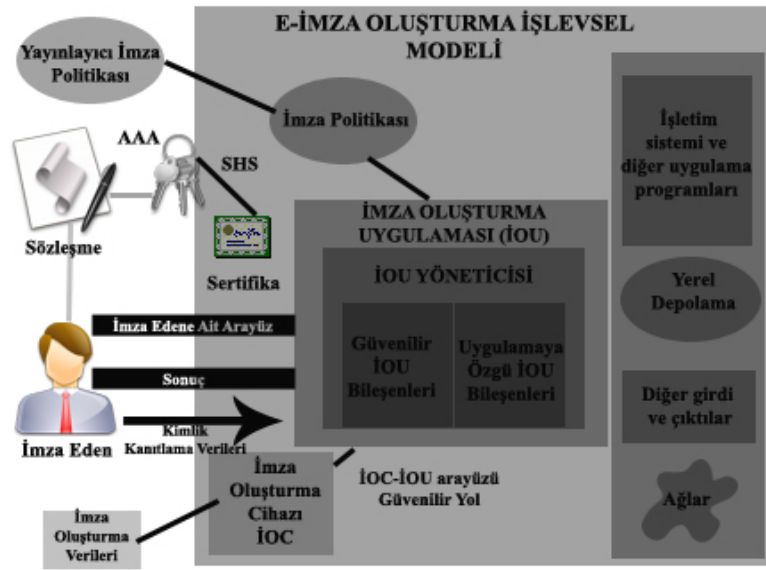
¹⁴⁴ European Committee For Standardization, Security requirements for signature creation applications, May 2004, Supersedes CWA 14170:2001, [ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14170-00-2004-May.pdf](http://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14170-00-2004-May.pdf), (25 Haziran 2008) s.11.

¹⁴⁵ Şeref Sağıroğlu, Mustafa Alkan, “**Her yönüyle E-imza**”, Ankara: Grafiker Yayınları, 2005, s.54.

¹⁴⁶ Şeref Sağıroğlu, Gürol Canberk, “Şifre Bilimi Tarihine Genel Bakış I-II”, **Telekom Dünyası Dergisi**, Haziran 2005, s.36-44.

yöntemlerinin kullanıldığı kriptografik saldırılara karşı son derece etkin bir korunma sağlayabilmektedir.¹⁴⁷

E-imza oluşturma sürecinin ön plana çıkan bu mekanizması dışında çok sayıda bileşen ve etken bulunmaktadır. İmza oluşturma bu bakış açısı ile ele alındığında, bu sürecin tüm öğeleri ile oluşturulduğu modelin, tamamının güvenlik açısından ele alınması gereklidir.



Şekil 11-Elektronik İmza Oluşturma İşlevsel Modeli

Kaynak: Ulusal Elektronik İmza Sempozyumu, Ankara, 7-8 Aralık, 2006.

Bu modelden de görülebileceği gibi imza oluşturma işlevi ile bilgi nesne ve arayüzlerinin hepsi ile ilgili güvenlik hususları söz konusu olabilir. Süreç çok sayıda noktada güvenlik riski ve tehdidi altındadır. Bu noktalardaki korunmasızlık ve zayıflıklardan yararlanan kötücül ve casus yazılımlar, e-imza oluşturma sürecinin güvenliğini tehlikeye sokabilirler.

E-imza oluşturma süreci, güvenlik açısından en geniş çerçevede ele alındığında; çevre etkenleri bakımından iki farklı ortamda, iki farklı güvenlik seviyesine gereksinim duyulmaktadır. Ev ve işyeri gibi ortamlarda e-imza oluşturmada, halka açık

¹⁴⁷ Şeref Sağıroğlu, Gürol Canberk, “Bilgisayar Sistemlerine Yapılan Saldırıları ve Türleri: Bir inceleme”, Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi, Cilt.23, No.1-2, 2007, s.1-12.

ortamlarda e-imza oluşturmada daha fazla düzeyde güvenlik tedbirlerine ihtiyaç duyulacaktır. Dolayısıyla, örneğin ev kullanımı için tasarlanmış bir imza oluşturma sisteminin halka açık ortamlarda kullanılması risklidir.

E-imza oluşturma süreçlerinin güvenlik gereksinimlerini ele alan çeşitli çalışmalar bulunmaktadır. ESIGN Uzman Grubu tarafından, CEN/ISSS için 2001 yılında hazırlanmış olan “Güvenilir İmza Oluşturma Cihazı” raporunda, imza oluşturma sürecinin oluşturan güvenlik ortamı ayrıntıları ile mercek altına alınmıştır.¹⁴⁸ Rapora göre, gizliliği temin edilmiş olan şifre veya özel (gizli) şifre anahtarları gibi, imza edenin bir elektronik imza oluştururken kullandığı benzersiz veri olarak tanımlanan İmza Oluşturma Verileri (IOV)İ dışarı aktarımında bütünlüğü korumuş olan şifre veya genel (açık) şifre anahtarları gibi, bir elektronik imzayı doğrulamak amacıyla kullanılan İmza Doğrulama Verisi (İDV), PIN kodu gibi girdi olarak sağlanan kimlik kanıtlama verisi veya kullanıcının biyometrik karakteristiklerinden türetilen kimlik kanıtlama verisi anlamına gelen ve uç kullanıcı tarafından imza oluşturma işlemi sırasında girilen Kimlik Kanıtlama Doğrulama Verileri (KKDV) ve uç kullanıcının teşhis edilmesi ve kimliğinin kanıtlanması için kullanılan referans PIN kodu ve biyometrik kimlik kanıtlama referansı olarak tanımlanan Referans Kimlik Kanıtlama Verileri (RKKV) e-imza oluşturma işleminin güvenlik ortamının varlıkları olarak kullanıcı veya yönetici ve imza oluşturma sürecini tehdit eden saldırganlar olarak belirlenirse; IOV’nin güvenilir bir biçimde sistemin içerisine aktarıldığı ve sertifika üretme uygulamasının güvenilir biçimde imza edenin adının kimlik kanıtlamasını yaptığı varsayımından hareket edildiğinde, güvenlik tehditleri aşağıdaki şekilde sınıflanmıştır:

Söz konusu raporda e-imza oluşturma sürecinde ulaşılması gereken hedefler şu şekilde belirtilmiştir.

- Süreç sırasında ve sonunda ortaya çıkan emarelerden yararlanılarak bir sonuca ulaşmasını önleyecek veya en azından belirli sınırlar içinde tutacak tasarımın hazırlanması ve uygulanması,

¹⁴⁸ Prepared By: ESIGN Workshop - Expert Group F Prepared For: CEN/ISSS 25 July 2001, “Protection Profile — Secure Signature-Creation Device Type 3 Version: 1.05, EAL 4+”, <http://www.bsi.bund.de/zertifiz/zert/reporte/PP0006b.pdf>, (30 Haziran 2008) s.21-32.

- İklendirme aşaması ile kullanımda olduğu zamanda otaya çıkabilecek kusurların saptanabilmesi ve ihraçtan sonra güvenilir yok etme yöntemlerinin sağlanması,
- İOV ve İDV arasındaki uyuşmanın temin edilmesi,
- İDV'nin aslına uygunluğunun sağlanması,
- Kurcalanmışlığın saptanması,
- Kurcalanmaya karşı direnç gösterilmesi,
- İmza oluşturma cihazları arasındaki İOV'nin güvenli naklinin sağlanması,
- İOV ve İDV'nin sadece yetkili kullanıcılar tarafından başlatılmasının temin edilmesi
- İmza oluşturma verilerinin benzersizliğinin sağlanması

E-imza güvenlik tehlikelerine aşağıdaki tablodan inceleyebiliriz.

Tablo 2-Güvenlik Tehditleri

Güvenlik Tehdidi	Açıklama
Fiziksel Korsanlık	Fiziksel ortamdaki korunmasızlıkların istismarı
İOV ifşası	İmza oluşturma verilerinin depolanması ve kopyalanması
İOV türetilmesi	İmza oluşturma verilerinin türetilmesi
İOV yayınlanması	İmza oluşturma verilerinin yayınlanması
İmza Kalpazanlığı	Elektronik imzanın sahtesinin oluşturulması
İmzanın İnkarı	Geçerli Elektronik imzanın ret ettirilmesi
İDV kalpazanlığı	İmza doğrulama verilerinin sahtesinin oluşturulması

Kaynak:Ersin Gülaçtı, “Elektronik İmza ve Güvenlik”, (Tasnif dışı)

<http://www.kamusal.gov.tr/tr/Kurumsal/Haberler/Bilgi%20Teknolojileri%20Guvencigi%20Eimza.pdf>, (30 Haziran 2008)

Bütün bu amaçlara ulaşabilecek e-imza oluşturma sürecine ait bir güvenlik politikasının hazırlanması ve uygulanabilmesi, çok geniş kapsamda ve titiz bir biçimde yürütülecek araştırma ve çalışmalar istenmektedir. Bahsi geçen tehditleri oluşturacak ve

istenilen saldırı türleri arasında son günlerde gittikçe yaygınlaşan kötücül ve casus yazılımlar gelmektedir.

5.4.2. Kötücül ve Casus Yazılımlar

Bilgisayar teknolojilerinin gelişmesi ile son zamanlarda bilgi ve bilgisayar güvenliği konusunda en ciddi tehditlerin başında kötücül yazılımlar gelmektedir. Kötücül yazılım (malware, İngilizce “malicious software”in kısaltılması) bulaştığı bir bilgisayar sisteminde veya ağ üzerindeki diğer makinelerde zarara yol açmak veya çalışmalarını aksatmak amacıyla hazırlanmış istenmeyen yazılımların genel adıdır.¹⁴⁹ Aslında ana bir tür kötücül yazılım olan fakat bütün kötücül yazılım türleri arasında daha fazla ön plan çıkan birçok kötücül yazılım türünü bir şekilde kapsayan casus yazılım (spyware), kullanıcılara ait önemli bilgilerin ve kullanıcının yaptığı işlemlerin, kullanıcının bilgisi olmadan toplanmasını ve bu bilgilerin kötü niyetli kişilere gönderilmesini sağlayan yazılım olarak tanımlanır.¹⁵⁰ Ana kötücül yazılım türleri aşağıdaki şekilde gösterilmiştir.



Şekil 12-Ana Kötücül Yazılım Türleri

¹⁴⁹ Gürol Canberk, “Klavye Dinleme ve Önleme Sistemleri Analiz, Tasarım ve Geliştirme”,(Yüksek Lisans Tezi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Eylül 2005) s.32-35..

¹⁵⁰Şeref Sağıroğlu, Gürol Canberk, “Kötücül ve Casus Yazılımlar: Kapsamlı bir Araştırma”, Gazi Üniversitesi Müh. Mim. Fak. Dergisi, 2007,Cilt.22, No.1 s.121-136.

Kaynak:Gürol Canberk, Şeref Sağıroğlu. “Kötücül ve Casus Yazılımlar: Kapsamlı bir araştırma”, **Mühendislik Mimarlık Fakültesi Dergisi**. Gazi Üniversitesi, Cilt.22, No:1, Mart 2007. s.121-136.

Bu kötücül yazılımların her biri, çok farklı amaçlar için, çok farklı yöntemler kullanılmaktadır. Ayrıca, bu yazılımlar oldukça yaygın olarak karşılaşılan ve gerek kişisel, gerekse kurumsal çapta önemli maddi ve manevi zararlara sebep olan yapılmıştır.

5.4.3. E-imza Oluşturma sürecinde Kötücül ve Casus Yazılım Saldırıları

Literatürde, sınırlı kapsamda da olsa bazı kötücül yazılım türlerinin e-imza oluşturma sürecine olan olumsuz etkileri ele alınmıştır. Almanya’daki e-imza oluşturma uygulamalarının (İOU) en tehlikeli kötücül yazılım türlerinden biri Truva atları ile nasıl sekteye uğratabileceğini örnekler ile gözler önüne serilmektedir.¹⁵¹

Kötücül ve casus yazılımların elektronik imza oluşturma sürecine olan olumsuz etkilerinin ayrıntılarına geçmeden önce; e-imzanın, hali hazırda oldukça yaygın bazı kötücül yazılımlar hareket alanlarını oldukça kısıtladığı, hatta neredeyse imkânsız hale getirdiğini belirtmek gerekir. E-imzanın, tanımı gereği kimlik kanıtlama, inkâr edememe, bütünlük ve gizlilik güvenlik unsurlarını yerine getirmesinden dolayı; bu noktalardaki korunmazlıkları istismar eden kötücül yazılımlar e-imza kullanıldığında bertaraf edilmektedir. E-imzanın etkisiz hale getirdiği veya caydırdığı kötü yazılımlar türleri şöyledir:

- Mesaj sağanakları (Spam)
- Sazan Avlama (phishing)
- Aldatmaca (hoax)
- Web sahteciliği ve dolandırıcılığı (web scam and fraud)
- E-posta bombardımanı (mail bomber)
- Kitle postacısı (mass mailer)

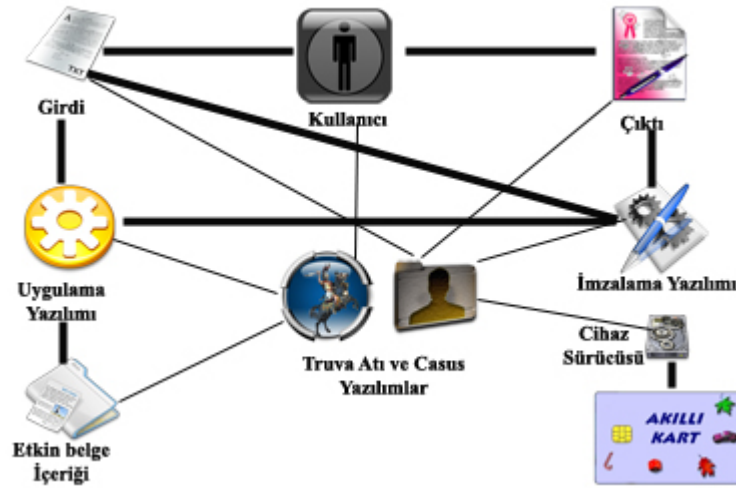
¹⁵¹ Spalka, 2002, s. 195.

- Adres hasatçı (e-mail harvester)
- Web böcekleri (web bugs)

Söz konusu kötücül yazılımların çoğunlukla e-posta aracılığıyla gerçekleştirilen saldırılardır. Bu tür kötü niyetli e-posta iletilerini alan kullanıcıların, iletiyi gönderen kişinin kimliğini kesin bir doğrulukla tespit etmesi mümkün olmadığından çeşitli şekillerde kandırılması ve zarara uğratılması mümkündür.

Kötücül yazılımlar arasında e-imza oluşturma sürecine olumsuz etkileri olan türler ile ilgili açıklamaları aşağıda bulabilirsiniz.

Bilgisayar Virüsleri (Computer Viruses): En tehlikeli ve en eski kötücül yazılı olarak kabul edilen virüslerin e-imza oluşturma süreçlerinde önemli etkileri söz konusudur.¹⁵² İmza oluşturma uygulamasına (İOU) ait .EXE, .DLL gibi çalıştırılabilir modüllerine virüs bulaşması sonucu uygulama hatalı bir şekilde çalışabilir. Özellikle e-posta programlarına bulaşan makro virüsleri gerek PIN numaralarını elde etmek gerekse imzalanan asıl belgede tahrifat yapmak için kullanılabilir.



Şekil 13: E-imza Oluşturma uygulamasında Truva atı ve casus yazılımlar tarafından hedef alınan arayüzler

¹⁵² Gregg Keizer, *Kama Sutra Spoofs Digital Certificates*, <http://www.informationweek.com/news/windows/security/showArticle.jhtml?articleID=177103418>. (21 Mayıs 2008).

Bilgisayar Solucanları (Computer Worms): Solucanlar, yayılmak için başka bir programa veya virüslere olduğu gibi insan etkileşimine ihtiyaç duymayan, kendi kendini çoğaltan bir yapı arz eder.¹⁵³ Solucanlar bulaştığı bilgisayarlardan elde edilen elektronik imzalı e-postaları, başka kişilere göndermek için kullanılır. Şimdiden Windows işletim sisteminin güvenlik sistemini atlatmak için uygulama sayısal sertifikalarını taklit eden bilgisayar solucanları ortaya çıkmıştır.¹⁵⁴ Bu ilerde elektronik imzayı taklit eden bilgisayar solucanlarının da ortaya çıkabileceğinin bir işareti olarak kabul edilir.

Truva Atları (Trojen Horses) ve Casus Yazılımlar (Spyware): Truva Atları meşru yazılım gibi gözükten kötücül yazılımlardır. Casus yazılım, kullanıcılara ait önemli bilgilerin ve kullanıcının yaptığı işlemlerin, kullanıcının bilgisi olmadan toplanmasını ve bu bilgilerin kötü niyetli kişilere gönderilmesini sağlayan yazılım olarak tanımlanır. Bu yazılımlar e-imza oluşturma sürecinde değişik nokta ve arayüzlere saldırılarda bulunabilir. E-posta programı gibi uygulama yazılımları ile imzalama yazılımı arasındaki arayüz, imzalama yazılımı ile akıllı kart arasındaki cihaz sürücülerini ve casus yazılımlar tarafından hedeflenebilir.¹⁵⁵

Bunların dışında, Arka kapılar (backdoor), Klavye dinleme Sistemleri (Keyloggers), Kök kullanıcı takımları (Rootkit), Korunmasızlık Sömürücüleri (Exploit), Uzaktan Yönetim Aracı (Remote Administration tool) ve şifre kırıcılarıdır.

5.5. E-İMZA'DA FORMAT SEÇİMİ

E-imza'nın yaygınlaşmaya başladığı bu günlerde e-imzaya geçmek isteyen kurum ve kuruluşların karşısına çıkacak olan kaçınılmaz soru şu olacaktır: İmzalanacak olan form veya dokümanlar için hangi format tercih edilmelidir? Web üzerinde çalışan bir online formun formatı muhtemelen html, üzerinde jsp, veya .php dir. Doküman yönetim sistemlerinde kullanılan format ise, .doc, .pdf, .tif vb. olabilir. Yukarıdaki sorunun yanıtı ihtiyaçlara ve uygulamaya göre değişebilecektir. Örneğin kullanılmakta olan uygulama yukarıda belirtilen formatları veya düz metin formatını kullanıyorsa ve

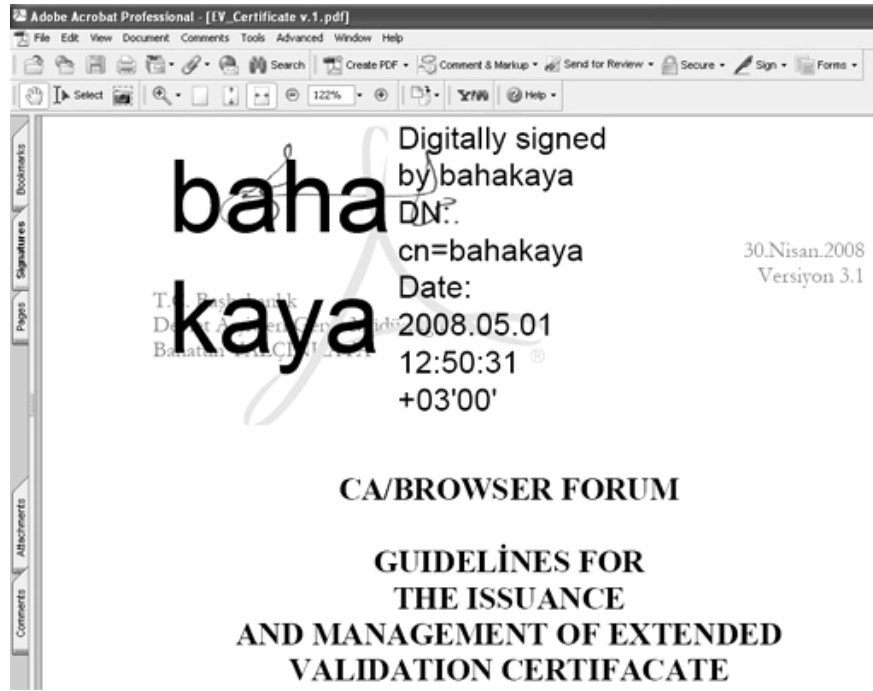
¹⁵³ Spalka, 2002, s.198.

¹⁵⁴ Sağiroğlu, Canberk, 2007, s. 132.

¹⁵⁵ Spalka, 2002, s.201.

kullanıcılara e-imzalı göstermek (görsellik) gibi bir endişe yoksa e-imzaya geçişte bu formatları kullanmaya devam etmek tercih edilebilir. Aksine, e-imza hizmeti müşterilere sunulmak isteniyorsa, bu durumda son kullanıcılara görselliği daha yüksek ve daha anlaşılabilir ve kullanım kolaylığı sağlayacaktır bir format tercih edilebilir. E-imza için güncel olarak 2 temel imzalama formatı kullanılmaktadır:

XML PDF



Şekil 14-İmzalanmış belgenin PDF görünümü

Bu iki formatın da avantaj ve dezavantajları vardır. Bunları konu başlıkları halinde aşağıda inceleyeceğiz.

5.5.1. Görsellik

İngilizce de bir tabir vardır: “*Seeing is believing*” : Görmek inanmaktır. Her ne kadar bu deyiş tartışmaya açık olsa da (bazen görülen yok, görülmeyende var olabilir), insanoğlunun gördüğüne inanmaya eğilimi olduğunu söyleyebiliriz. Bu nedenle de matematik temeline dayanan ve zaten soyut bir kavram olan e-imzaya somut bir görsellik özelliği katmak teknolojinin kullanımı açısından faydalı olacaktır. PDF formatında imzalama denildiğinde aslında, PDF dokümanı açtığınız zaman, e-imzanın dokümanın içinde görsel olarak görülebilmesinden bahsedilmektedir. Aksi taktirde PDF

imzalamanın diğer dosyaların imzalanması arasında bir fark kalmaz. PDF formatında imzalamanın en büyük avantajı, imzanın görsel olarak kullanıcıya gösterilebilmesi ve görselliğin belirli bir çerçeve de isteğe göre özelleştirilebilmesidir. Genel olarak e-imza teknolojisi ile ilgili bilgisi olmayan ortalama kullanıcılar için e-imzayı somutlaştıran bir unsur olarak oldukça faydalıdır. XML formatında ise, doküman kendi başına görsellikten uzak, özellikle imza kısmı ilginç karakterlerden ibarettir. Neyse ki bu durum, XSL formatı ile düzeltilebilmektedir. Yani, bir XML dosyanın görüntüsü diğer bir XSL dosya yoluyla istenen şekilde ayarlanabilmektedir.

```
<?xml version="1.0" encoding="iso-8859-1"?>
<?xml-stylesheet type="text/xsl" href="Belge.xsl"?>
<Veri xmlns:ds="Veri" Id="#SignedData">
  <Belge>
    <BelgeTar>30.08.2007</BelgeTar>
    <BelgeSayi>452645</BelgeSayi>
    <BelgeYazan>Bahattin YALÇINKAYA</BelgeYazan>
  </Belge>
  <ds:Signature>mQGIBDNJc8URBADySyB/T3Kfcq2+Eeluv85xnSx1113Tf0hMTeeHwSN
  XE4aY/Yr
  Fm8kpc41Gxm08xmKeKFT22i+Adm8ukynFnGIdaw4JaCSdlmT7H1SVwQnP0Hw
  2PNOvFYGWw4XFp43ry0bgrQu2/5sF5yDxm1yht8OYj/nyMwUsxUjVtUewCg/+4w
  g1RbT58+iQBCMeIIjRPfp4kD/2quMOz=V8P4Xsj2+OILjVLAmrNrQNmZFlqwrkKJ
  HAGNho0tCYbekATTvKgdBYeNeErxJm8f+hGXLKef/GSeVgEEMrRjL34F8Q6LmqhU
  fEynLhq4T/mo5jh2bC6sUDYrAYPSSVTWIT4DCb9VR4u30AEqliX40V8v5SsDQIZ
  jjb0A/9nbt1h6GjoZ2rvE50d92t1pcotFUZKz2jqkOckzgOYST5ZixKs8nSdec82
  jOMJ2BXHuEx7Tb9Z9TXpmMfRIWlqfoAlR8CE9XhzC021PldSdXrRTBH3/AkstZVv
  0dTGXUVG+vsWxKpq4ltUYjbSXYhkkEkXrBoY02rLzn40Meb3LbQiUGhpbGhwIFlu
  IFpbW11cm1hbm4gPHByekBwZ3AnY29tPokASwQQEQLACwUCM0lzxQQLawECAAof
  </ds:Signature>
</Veri>
```

Şekil 15-İmzalanmış belgenin XML görünümü

5.5.2. İmzalı veri Paylaşımı

E-imza'nın verilerin diğer bir kurum ile paylaşılması söz konusu ise bu durumda, veri paylaşımı için en uygun formatı seçmekte fayda olacaktır. Şüphesiz ki yapılacak seçim e-imzalı verilerin ne kadarının paylaşılacak istendiğine, ne kadarının ise paylaşılacak istenmediğine göre de şekillenecektir. Örneğin e-imzalı bir dosyanın tamamı paylaşılacak isteniyorsa, bu durumda dosya olduğu gibi paylaşımına açılabilir. Eğer e-imzalı dosyanın sadece belirli bir kısmı paylaşılacak isteniyorsa (Örnek: Sadece genel müdürün belge üzerinde imzaladığı belirli bir veri paylaşılacak isteniyor ama diğer verilerin kurumun gizlilik politikasından dolayı veya yaptığı gizlilik anlaşmasından dolayı paylaşılması mümkün gözükmüyor) bu durumda verinin belirli bir kısmını paylaşılmasına izin verecek formatı seçmek daha doğru olacaktır. XML formatındaki bir dosyanın istenilen kısımlarının imzalanması ve değişik kısımlarını değişik kullanıcılara imzalatırılması mümkündür. Bu veri paylaşımında oldukça

esneklik saęlayan bir yntemdir. XML formatının veri paylařımını esas alan bir format olması, aynı esneklięi imzalı XML veriler iin de geerli kılmasına řařırmamak lazım. PDF formatında ise, dosyanın bir kısmını imzalanması veya paylařılması mmkn olmamaktadır. PDF imzalama kullanılıyorsa dosyanın tamamını paylařmak zorunda kalınacaktır.

5.5.3. Kullanım Kolaylıęı ve Hukuka Uygunluk

Kullanım kolaylıęı konusunda PDF'in aık ara nde olduęunu belirtmeliyiz. PDF imzalama iin kullanılacak imzalama aracı, kendi bařına PDF imzalayabilir veya Adobe aralarından birine entegre alıřabilir olacaktır. Her iki durumda da kolay bir imzala arayzne sahip olunacaktır. İmza doęrulamada ise eęer kullanılan ara, Adobe imza formatına uygun imzalama yapıyorsa, bu durumda cretsiz olan “Adobe Reader” ile imza doęrulanabilecektir. Doęrulama tamamen Adobe Reader veya dięer bir PDF Reader tarafından gerekleřtirilir. XML de ise muhtemelen, imzalama ve imza doęrulama iřlemlerini kendiniz gerekleřtirmek durumunda kalırsınız veya bir XML aracı bulunsa dahi, ihtiyalar doęrultusunda zelleřtirmek gerekecektir. XML formatına ait e-imzalama ve imza doęrulama sreci W3C nin XAdes (XML Advanced Electronic Signatures)¹⁵⁶ standardına net olarak tanımlanmıřtır. XAdes standardı ise Avrupa Komisyonu E-imza direktifine uyum saęlamak amacıyla XML İmzalama spesifikasyonu'nun geniřletilmiř halidir. XAdes standardına uyum saęlaması, 5070 sayılı e-imza kanunu ve ilgili ynetmelik ve teblięlere byk lde uyum saęlanması anlamını tařımaktadır. Standart dıřında e-imza uygulamasının yerine getirmesi gereken řartlar da mevcuttur. PDF formatı ise RFC 3778 “The application/pdf Media Type”¹⁵⁷ ile tanımlanmıř uluslararası bir standart olmasına raęmen, E-imzalama ve imza doęrulama ile ilgili uluslararası kabul grmř bir standardı bulunmadıęından dolayı PDF formatında atılan e-imza'nın geerlilięi mevcut pdf imzalama ktphaneleri erevesinde uygulama geliřtiricinin inisiyatifi dahilinde olacaktır.

¹⁵⁶ Juan Carlos Cruellas, Gregor Karlinger, Denis Pinkas, John Ross, *XML Advanced Electronic Signatures (XAdES)*, 2003, <http://www.w3.org/TR/XAdES/> (15 Nisan 2008).

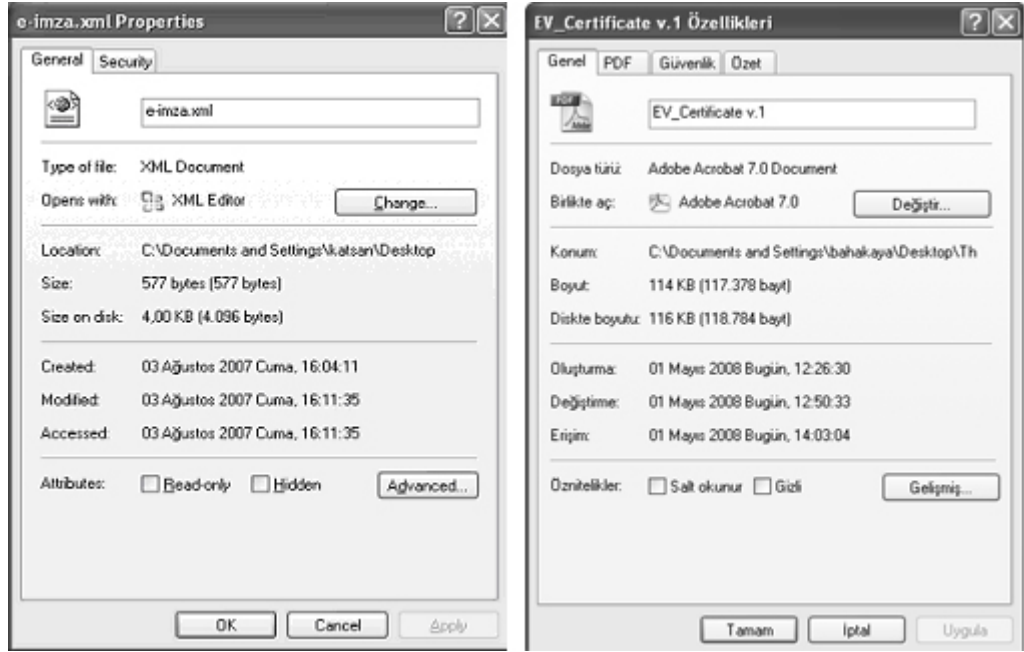
¹⁵⁷ E. Taft, J. Pravetz, S. Zilles, L. Masinter, *RFC 3778 The application/pdf Media Type*, Network Working Group Request for Comments: 3778, <http://www.faqs.org/rfcs/rfc3778.html>, (25 Haziran 2008).

Hukuki açıdan incelediğimiz XAdes standardı esasen uzun dönemli imzaları tanımlar. Uzun dönemli imzaların temel hedefi, imzalı doküman arşivleme ve ileriki bir tarihte yasal zeminde imzayı doğrulayabilmektedir. PDF'in de, ISO tarafından Adobe'un desteği ile yayınlanmış olan, arşivleme standardı (ISO 19005-1) ¹⁵⁸ mevcuttur. Bu standart ile PDF formatı arşivlemeye uygun hale getirilmiş, örneğin PDF içerikte javascript ve çalıştırılabilir dosyaların kullanımı engellenmiştir. Arşivleme noktasından bakıldığında, XML formatının e-imzalı doküman arşivleme konusunda daha etkin bir format olduğu görülmektedir.

5.5.4. Veri boyut ve Standardizasyon

XML formatı, düz metin tabanlı bir format olduğundan dolayı, aynı içerik için, PDF formatına göre daha küçük boyutta olacaktır. Aşağıdaki şekillerde, aynı içerik için bir XML dosya ile PDF dosyanın boyutlarının karşılaştırılması görülmektedir. Aynı veriler için e-imzalı verinin boyutlarının da aynı olması beklenir. Dolayısıyla, boyut farkı tamamen format farkından ileri gelmektedir. Windows sisteminde, örnek imzalı XML formatındaki dosyanın boyutu 577 byte iken, PDF formatındaki imzalı dosyanın boyutu 114 kb olarak görülmektedir.

¹⁵⁸ ISO 19005-1, **Document management – Electronic document file format for long – term preservation – Part 1: Use of PDF 1.4 (PDF/A-1)**, International Organization for Standardization, http://www.iso.org/iso/catalogue_detail?csnumber=38920 (22 Haziran 2007).



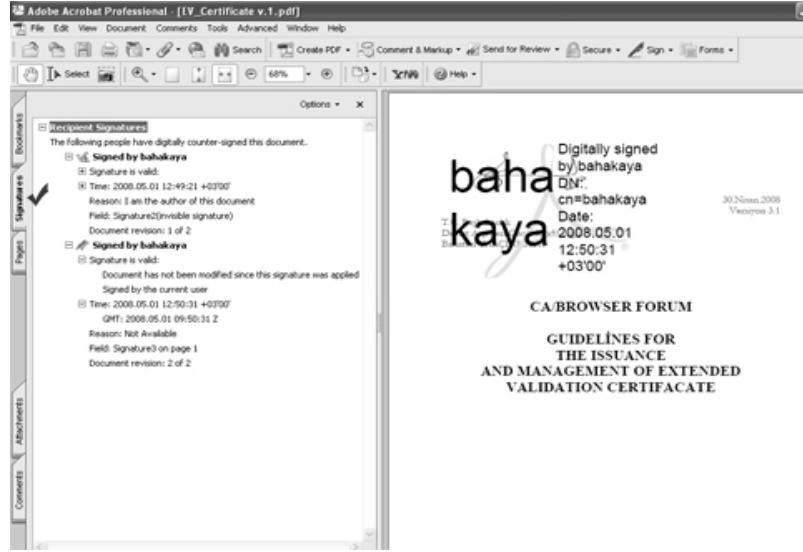
Şekil 16-XML ve PDF’te imzalanmış belgelerin kapsadığı boyutlar

Standartlaşmanın anlamı temelde herkesin aynı dili konuşabilmesidir. E-imza için standartlaşma, herhangi bir kişi veya kurumun imzaladığı belge/dosyanın, diğer bir kişi/kurum tarafından e-imzalı olduğunun anlaşılabilmesi ve işlenebilmesi anlamına gelmektedir. E-imza belirli bir kurum veya kuruluş içinde kullanılıyorsa, standartlaşma problemi bir nebze de olsa çözülmüş kabul edilebilir, şöyle ki: belirli bir standardı uygulamamış (kendi standardınızı uygulamış) veya o standardı yanlış uygulamış olabilirsiniz. Her iki durumda da sadece kurum uygulaması kullanıldığından dolayı, muhtemelen bir problem yaşamazsınız. Standardın uygulanması gerekmediğine veya maliyetinin yüksek olduğuna inanılıyorsa, fakat aynı zamanda diğer bir uygulama ile konuşmak gerekiyorsa, bu durumda, diğer uygulama ile anlaşabilmek için standart uyumu sağlayan bir gateway kullanmak faydalı olacaktır. XML formatının hem kendisi hem de e-imzası ile ilgili olarak oturmuş standartları vardır: “Extensible Markup Language (XML) 1.0 W3C Recommendation 16 August 2006”, RFC 3275 (Extensible Markup Language) XML – Signature Syntax and Processing¹⁵⁹ standartları uluslar arası kabul görmüş ve yaygınlaşmış standartlardır. XML imza’yı gerçeklerken bu standardın kullanılması kaçınılmaz olacaktır. PDF’de kabul görmüş bir uluslar arası standart

¹⁵⁹ Mark Bartel, John Boyer, Barb Fox, Brian LaMacchia, Ed Simon, *XML Signature Syntax and Processing (Second Edition) W3C Proposed Edited Recommendation 26 March 2008*, <http://nelson.w3.org/TR/2008/PER-xmldsig-core-20080326/>, (21 Mart 2008).

olmasına rağmen, e-imza konusunda henüz kabul edilmiş ortak bir standardı yoktur ve PDF imzalama için, “Adobe Systems” ın kendi spesifikasyonu kullanılmaktadır. Standardizasyon açısından XML’in PDF den birkaç adım önde olduğunu söylemek mümkündür.

5.5.5.PDF İçten İmzalama



Şekil 17-PDF belgesinin içten imzalanması

6.BÖLÜM-E-İMZALI BELGELERİN YÖNETİLMESİ

6.1. ÇAĞDAŞ YÖNETİM SÜRECİNDE E-İMZA SİSTEMİNİN ROLÜ

Toplumsal güveni kazanabilen etkin bilgi teknolojilerinden e-dönüşüm sürecinin önemli öğelerinden birisi e-imza sistemidir. E-kurumsal yapıya dönüşüm projesi sürekli gelişim ve paylaşım vizyonudur. Daha dikey bir yönetim sürecine geçiş sağlanabilir. Bu durumda, kurumların temel işleyişinde önemli bir role sahip olan iletişim ve bilgi yönetimi, bilgi güvenliği, birimler ve insanlar arası bir engel olmaktan çıkarak, işleyiş ve iletişim kolaylığı sağlayan bir görünüm içinde olacaktır. Bilişim teknolojilerinin yaşamda kullanımı ile iş ve işlemleri daha hızlı gerçekleyen verimlilik yükseltebilecek, kayıplar en aza indirilebilecektir.¹⁶⁰

Bu yeni olanaklar içeren fırsatları doğru ve bilimsel olarak değerlendiren organizasyonlarda, bireyin kendine yönelimi, kendi eksikliklerinden yola çıkıp, başka sorumlular aramadan kendini düzeltişi önemlidir. Sistem içindeki yerini ve rolünü gözden geçirerek gün yaşamında daha iyi olabilmek için gereken çabayı gösterip eskiyen bilgilerini yenileyişi, bilgi üretimine katkıda bulunuşu kısaca kendini geliştiriş demektir.¹⁶¹ Çağdaş bilimsel ve teknolojik gelişmeler sistem düşüncesiyle ve bütüncül bir bakış açısıyla değerlendirilmelidir. Yapılacak her değişikliğin, sistemin diğer alt sistemleriyle etkileşimi, satranç hamlesi yaklaşımıyla değerlendirilerek olası tüm sonuçları göz önüne almak esastır. Aksi takdirde, sistemin bir noktasında sistemden bağımsız ortaya konan bir iyileştirme ya da değişiklik, sistemin diğer noktalarında sistemin bütününe zarar verecek tarzda olumsuz sonuçları doğurur.¹⁶²

Kurumsal Yönetim ilkeleri, esas itibarıyla, işletmelerin üst kademe yönetim organlarını, işletmelerin faaliyetlerine ilişkin kararları verirken neleri dikkate almaları, bunları nasıl ve hangi mekanizmalar içinde değerlemeleri, kararları nasıl, ne zaman ve kimler açıklamaları ile ilgili kuralların toplamıdır. Bu kavramın temeli, işletmelerin hissedarlarına ve paydaşlarına karşı şeffaf olması, işletmenin gerçek durumunu yansıtması, bunların haklarını koruması, bu konuda etik ilkelere uyması ve sorumlu

¹⁶⁰ Sağiroğlu, Alkan, 2005, s.124.

¹⁶¹ Gönül Budak, **İşletme Yönetimi**, İzmir: Barış Yayınları, 2004, s. 26-29.

¹⁶² Peter M. Senge, **Beşinci Disiplin: öğrenen organizasyon düşüncesi ve uygulaması**, Ayşegül İldeniz – Ahmet Doğukan (çev.), 2. bsk, İstanbul: Yapı Kredi Yayınları, 1993, s.83.

davranması bekleyişine dayanmaktadır. Yani bir anlamda kurumsal yönetim, işletmelerin “iyi sosyal vatandaş” olmasını öngörmektedir.¹⁶³

Uygarlığın evrim sürecinde bilgi toplumuna erişimi, sosyal ekonomik, politik, kültürel ve teknolojik bilimsel sistemlerin bütünselliğidir. Bunun için bilgi toplumuna geçiş sürecinde eğitim, öğrenim, demokrasi, katılım ve dünya görüşünde yenilenen yeni politika ve stratejiler gereksinim vardır.¹⁶⁴ Bu hizmetlerin belirlenip uygulanarak sonuçlanışına değin her evresinde insan kaynaklarının katkı ve katılımlarını içerir. Bu hizmetlerde; bilgi ve bilinç düzeyi daha da arttırılabilir. Çalışma yaşamının sürekliliği içinde sosyal bir faaliyet, insanlığın var oluşundan itibaren başlayan, insan yaşamının en temel işlevlerindendir. Örgütsel gelişim, bilinçli, planlı ve devamlı bir süreçtir.¹⁶⁵

E-ortama güven artışı, bilgi varlıklarının işlenip aktarımında karşılaşılabilecek olası tehdit ve tehlikelerin büyük oranda ortadan kaldırışı ile olanaktır. E-imza konusu oldukça yeni bir konudur. Dikkatli davranılmadığı durumlarda riskler taşıyabilir. Konu doğrudan güvenlikle ilgili olduğu için önemi oldukça yüksektir. Bu nedenle alınacak yazılım, donanım ve hizmetler konusunda çok dikkatli ve bilinçli yaklaşım, yabancı ülke katkısının incelenip güvenirlilik, süreklilik, kurumsallık sorgusunun iyi yapılarak hizmet kalitesinin doğru değerlendirilişi yararlı olacaktır.¹⁶⁶

Yasa ve düzenlemelerle birlikte e-imza fikrinin olgunlaşarak günlük iş yaşamında kullanımı için şüphesiz zamana gereksinim vardır.¹⁶⁷ Yazılan hiçbir maili, gönderilen hiçbir dosyayı, faturayı, herhangi bir belgeyi bundan sonra ne olur ne olmaz diye çıktı alarak raflarda saklamak zorunda olunmayacaktır. E-imzalı verilerin arşivlenmesi de son derece rahat olduğu için, dünyada e-imza ve benzeri teknolojiler sayesinde artık daha çok orman görülebilecektir.¹⁶⁸

¹⁶³ Tamer Koçel, **İşletme Yöneticiliği**, İstanbul: Beta Yayın, 2003, s.468.

¹⁶⁴ H Erkan, “Bilgi Toplumu”, **Bilgi Teknolojileri Kongresi – IV. Akademik Bilişim Şurası**, Ankara, 9-11 Şubat 2006, s. 186- 190.

¹⁶⁵ A. Soysal, “Öğrenen Organizasyon Olabilmek”, **Standart**, Yıl.42, Sayı.504, 2003, s.65-73.

¹⁶⁶ Mehmet Ali Akçayol, H. Erol, “Türkiye’de Elektronik İmza Uygulamalarında Durum Analizi ve Öneriler”, **1.Ulusal E-imza Sempozyumu**, 7-8 Aralık 2006, Ankara, s.182-189.

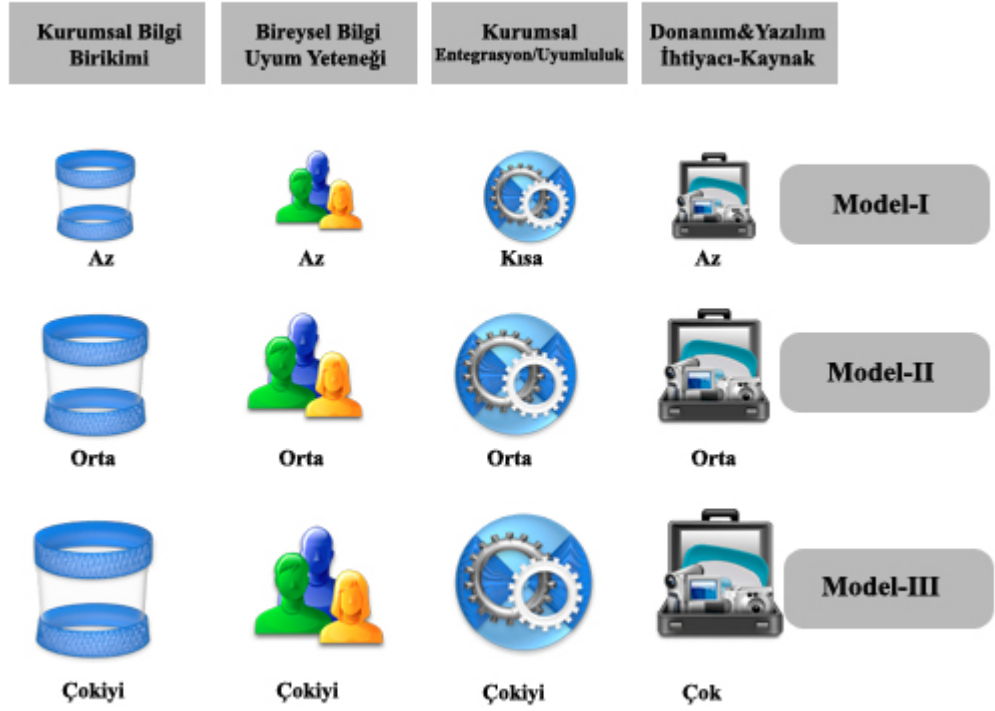
¹⁶⁷ Sezen Yeşil, Mustafa Alkan, Tayfun Acarer, **Yabancı Elektronik Sertifikaların Kullanımı**, <http://www.ueimzas.gazi.edu.tr/pdf/bildiri/58.pdf>, (25 Haziran 2008) s.1-7.

¹⁶⁸ Leyla Keser Berber, E-imza ile ilgili Söyleşi, <http://www.e-imza.gen.tr/index.php?Page=Soylesi&SoylesiNo=20>, (08 Aralık 2007).

Çağdaş yönetim e-imza sistemi kullanımı risklerin ve politikalarının doğru biçimde uygulandığı stratejik yaklaşımla ele alınabilir. E-imza ile birlikte bilgi, belge ve süreç yönetimi uygulamalarında dış sistemlerle kolay bütünleşebilen platform bağımsız ve tüm süreçlerde e-imza altyapısını destekler. Böylece kolaylıkla bilgi, belge ve süreç yönetimi yazılımlarının gelişimi istenilen şeffaflığı sağlar. Kamu ve özel sektör başta olmak üzere, işletmeler, diğer kuruluşlar ve devletlerin sayısal ortamlara yönelim istençleri giderek hızlanabilir. E-arşivleme kurumsal hafızanın yönetiminde en önemli iç organ olarak güvenli içerikle güvenli dağıtım ortamları olacaktır. E-ortamda arşivlenen, yedeklenen belgelerin doğal afet ve kriz durumlarında bilgi kazanımında kağıt tasarrufu, verimlilik artarken, maliyetler azalır. Elektronik Belge yönetim sistemleri, işletmelerin iş süreçlerini hızlandıran, standartlaştıran, gözetilen ve denetlenen sistemler yüksek güvenlik standartları taraflara esneklik ve çabukluk kazandırabilir. Bilişim teknolojilerinin detaylı entegrasyonu e-imza sistemi yönetim sürecinin iç ve dış etkinliğini pozitif yönde etkileyerek değiştirebilir.

6.2. NASIL BİR E- İMZA SİSTEMİ KURGULANABİLİR: MODELLER VE EVRAK YÖNETİM SÜRECİNDE E-İMZA.

Kamu kurum ve kuruluş veya özel sektörde uygun bir model oluşturulup, elektronik imzaya geçilerek hem yatırımların daha sağlıklı yapılması hem de kaynak israfının azaltılması son derece önemlidir. Tez çerçevesinde kâğıt tasarrufu desteklenerek, kurumların veya şirketlerin e-imzalı belgeleri kullanarak gelişimlerine devam etmelerini sağlamak amacıyla birkaç model üzerinde durulmuştur. Bu modeller oluşturulabilecek modellerden sadece birkaç tanesidir. Gerek elektronik gerekse klasik ortamda yapılan yazışmaları incelediğimizde, farklı modellerin de geliştirilebileceği görülmektedir. Fakat çalışma kapsamında aşağıda belirtilen modellerle sınırlı tutulmuştur.



Şekil 18-Belge Yönetiminde Model-Gereksinim oranlaması ihtiyaçları

Aynı zamanda tüm kamuda birden bire genel anlamda elektronik imza kullanılmasını beklemek hata olacaktır. Bir süreç içerisinde hedeflere yönelik çalışarak, bu uygulamaya geçiş daha isabetli olacaktır. Bu da demek oluyor ki, hem elektronik imza hem de ıslak imza beraber kullanılmaya devam edecektir. Tez konusunun elektronik imza olması nedeniyle ıslak imza ile olan prosedür ve modeller üzerine durulmamıştır. Fakat ıslak imzalı belgelerin yönetilmesi ve arşivlenmesi konusu da güvenlik ve güvenilirlik açısından incelenmesinin önemli olduğu açıktır.

Elektronik imzanın sağladığı faydalardan bahsederken en fazla değinmeye değer bulunan noktalardan birisi de getirdiđi ekonomik kazanımlar ve kaynakların faydalı kullanılmasına olanak tanınmasıdır. E-imza modellerini oluştururken en başta gerekli olan sistemin elektronik belge yönetimi sistemine ihtiyaç duymasıdır. EBYs ile ilgili Devlet Arşivleri Genel Müdürlüğü bünyesinde Prof. Dr. Hamza Kandur ve ekibinin bir çalışması mevcuttur. Bu çalışma ülkemizin dünyadaki gelişmeleri takip edebilmesi açısından da çok önemlidir. Elektronik Belge Yönetimi Sisteminin

gereksinimleri ve uygulamaları açısından bu yayın şüphesiz birinci derecede rehber kaynaktır. Tez çerçevesinde çok sıkça bu rehber müracaat edilmiştir.

Elektronik imzanın temel uygulama modellerine bakıldığı zaman; bazı anahtar kavramlar, oluşturulacak sistemin omurgası olacaktır. Bu kavramlardan Kurumsal bilgi birikimi az, bireysel bilgi uyum yeteneği az, kurumsal entegrasyon ve uygulama zamanı kısa vadeli, donanım ve yazılım ihtiyacı düşük maliyetli olanlar için uygulanması doğru olan Model 1'dir. Kurumsal bilgi birikim orta düzeyde, bireysel bilgi uyum yeteneği orta düzeyde, kurumsal entegrasyon ve uygulama zamanı orta vadeli, donanım ve yazılım ihtiyacı orta düzey maliyetli olanlar için uygulanması doğru olan Model 2'dir. Kurumsal bilgi birikimi çok fazla, bireysel bilgi uyum yeteneği çok iyi nitelikte, kurumsal entegrasyon ve uygulama zamanı uzun vadeli, donanım ve yazılım ihtiyacı yüksek maliyetli olanlar için uygulanması doğru olan Model 3'tür.

6.2.1. Model 1: Asgari Düzey

Bu modelde kurumsal olarak tüm belge yönetim sistemi aynen devam etmekte (klasik ıslak imzalı), e-imza ile gelen evrakların kabulü ve kontrolü ile giden evraklarda e-imza işlemi evrak kayıt işleminden sonra yetkili bir kişi tarafından (Evrak yöneticisi, evrak yönetici şefi tarafından) gerçekleştirilebilmektedir. Bu model henüz dijital sinir sistemi (networku) bulunmayan kurumlar için daha uygun bir sistem modelidir. Networku olan fakat elektronik imza sürecine hazır olmayan kurumlar içinde kullanılabilir. Aynı zamanda bu modelde EBYS en gerekli temel ihtiyaç değildir. Bu bağlamda Asgari düzey modeli için asgari sistem ihtiyaçlarını şu şekilde sıralayabiliriz.

- 1 adet Elektronik İmza sertifikası
- 1 adet Elektronik imza oluşturma doğrulama aracı
- 1 adet tarayıcı
- 1 adet yazıcı
- Elektronik posta adresi ve bu adrese internet bağlantısı



Şekil 19-Model 1-Asgari Düzey Genel Yazışmalar

Kaynak: Hamdi Boyacı, “Kamu Kurumları için uygulanabilir E-imza Modelleri”, Özelleştirme İdaresi Başkanlığı, Aralık, 2005.

Model 1’de kurum içi birimler arasında yapılan yazışmalar klasik usulde devam etmektedir. Bir e-imza uygulamasına ihtiyaç duymamaktadır. Kurumsal bilgi birikimi az olduğu için dışa yönelik uygulamalarda kullanılması düşünüldüğü için kurum içinde herhangi bir e-imza süreci bulunmamaktadır.

6.2.2. Model 2: Orta Düzey

Bu model yaklaşımında, belge yönetimine uygun bir sistemin olması gerekmektedir. Elektronik Belge Yönetim Sistemi Kriterlerini inceldiğimizde elektronik imza ile olan entegrasyon sürecini tamamlamış olması başlıca şarttır. Belge hazırlama ve paraf işlemleri gibi yönetsel işlemler EBYS’nin sağladığı yazılım imkânları çerçevesinde gerçekleştirilebilir. E-imza yalnızca evrakı son olarak imzalayan tarafından kullanılır.

Belgenin tanımlanabilirliği, bütünlüğü, onay ve kayıt bilgisi, yapısal özellikleri, üretim sorumluluğu ve mülkiyet hakkı gibi kavramlar da bu bağlamda önemlidir ve burada incelenmesi gerekmektedir.

Belgenin tanımlanabilirliği, üretilen kayıttan belge mi doküman mı olduğu ile alakalıdır. Şayet doküman ise, EBYS içerisinde belgeye dönüşümü tanımlanabilir olması gerekmektedir. “Elektronik belge yönetimi, kurumların gündelik işlerini yerine getirirken oluşturdukları her türlü dokümantasyonun içerisinde kurum aktivitelerinin delili olabilecek belgelerin ayıklanarak bunların içerik, format ve ilişkisel özelliklerini korumak ve bu belgeleri üretimden nihai tasfiyeye kadar olan süreç içerisinde yönetmektir. Bu noktada karşımıza çıkan elektronik doküman yönetim (EDY) ve elektronik belge yönetimi (EBY) kavramları zaman zaman birbirinin yerine kullanılsa da amaçları açısından farklılık gösterirler.”¹⁶⁹ Belgenin tanımlanabilir olması demek; belgenin üreticisinin, yazarının, alıcısının ve belgeye ait tarih bilgilerinin kayıt altına alınmasıyla mümkündür.¹⁷⁰

Belgenin bütünlüğü, üretilen belgenin bütünlüğüyle ilgili bir bozulma olmamalıdır. Sorgulandığı zaman bütünlüğün bozulmadığının gösterilmesi gerekir. Bütünlüğü EBYS Kriterlerine göre incelediğimizde entelektüel içeriğin bozulmaması; belge vasfı kazanmış e-dokümanların içeriğine bir müdahale olmadığını göstermesi ve herhangi bir sistem gereksinimi olmadan belgeye ulaşımın olmasıdır. Bir diğer bütünlük kriteri tanımsal olmasıdır; e-belgelerin üreten, ileten ve alan, kullananlarının tanımlı olduğu, bir bütün içerisinde olduğunu gösterir. Diğer bir bütünlük kriteri de fiziksel bütünlüğünün sağlanmış olmasıdır.¹⁷¹

Belgenin onay ve kayıt bilgisi, EBYS, e-belgenin üreticisi ya da e-belgeyle ilgili kişilerin veya tüzel kişilerin elektronik anlamda onaylayabileceği bir yapıda olmalı ya da onay için gerekli esneklik yapısına ve entegrasyona sahip olmalıdır. “Geleneksel evrak yönetim sistemlerinde bir belgenin ‘resmi’ bir hüviyet kazanabilmesi için o belgenin imza yetkisine sahip kişilerce imzalanmış olması ve belgenin kurumsal evrak kayıt sistemi içerisinde yer alması esastır. Belge ile ifade edilen mal ve hizmet alma ilişkileri, medeni ilişkiler, hak ve alacak ilişkilerinin hukuki geçerliğinin olabilmesi için belgenin ilgili ve yetkili kişilerce imzalanmış ve bir kayıt sistemi içerisinde gösterilmesi

¹⁶⁹ Hamza Kandur, **Elektronik Belge Yönetimi Referans Kriterleri Modeli v.2.0**, 2.Basım, Ankara: T.C. Başbakanlık Devlet Arşivleri Genel Müdürlüğü, 2006, s.12.

¹⁷⁰ Kandur, 2006, s. 52

¹⁷¹ Kandur, 2006, s. 53

esastır.”¹⁷²Bu noktada yasal prosedürler ve uygulamalar önem kazanmıştır ve uygulamada olmazsa olmaz bir şart olarak karşımıza çıkmaktadır. Bir diğer deyişle elektronik işaretlemelere, e-imza, e-mühür, e-onay, zaman damgası, özel elektronik simgelere uyum sağlayabilecek yapıda olmalıdır.¹⁷³

Şüphesiz EBYS ile ilgili olarak rehber niteliğinde olan bu çalışmadan daha fazla yararlandığımı söylemeliyim. Model 2’ye geri döndüğümüzde kurumun belge yönetimi gelen evraklar açısından, EBYS tarafından e-imza doğrulama işlemi Belge Yönetim sürecinde tanımlanmakta ve belge hayat döngüsünü EBYS’nin sağladığı yazılım imkânları çerçevesinde yürütecektir. Model 3’te yazılımın nasıl olacağı ve neleri içerisinde barındırdığı konularına girmeyi hedeflemekteyim.

Model 2 yaklaşımında daha ziyade dijital sinir sistemi (network) ortamı mevcut olan ancak e-imzaya uygulaması tam olarak gerçekleşmemiş olan kurum ve kuruluşlar için uygulanabilir.

Model 2’de asgari düzeyde ihtiyaç duyulan gereksinimleri şöyle sıralayabiliriz.

- Elektronik Belge Yönetim Sistemi yazılımı
- E-imza oluşturma ve doğrulama araçları
- E-imza sertifikası (imza kullanacak kullanıcı sayısı kadar, her biri için ayrı ayrı ve makam tarafından onaylanmış olmalı)
- Elektronik posta adresi ve bu adresle bağlantı kurmak için internet bağlantısı,

Asgari düzeyde olması gerekli sistem ihtiyaçları olarak sıralayabiliriz. Model 2’nin Model 1’den farkı olarak kurumiçi yazışmaların da elektronik olarak yapılmasıdır. Dışarıya gönderilen belgeler veya içeride yapılan yazışmaların güvenlik ve güvenilirliği ile ilgili ileriki bölümlerde daha geniş açıklamalar olacaktır. Aşağıdaki şemada Model 2’nin işleyişini görebiliriz.

¹⁷².Kandur,2006, s. 54.

¹⁷³ Kandur, 2006, s. 54.



Şekil 20-Model 2-Orta Düzey Kurumdışı Yazışmalar

Kaynak: Hamdi Boyacı, “Kamu Kurumları için uygulanabilir E-imza Modelleri”, Özelleştirme İdaresi Başkanlığı, Aralık, 2005.



Şekil 21-Model 2-Orta Düzey Kurumiçi Yazışmalar

Kaynak: Hamdi Boyacı, “Kamu Kurumları için uygulanabilir E-imza Modelleri”, Özelleştirme İdaresi Başkanlığı, Aralık, 2005.

6.2.3. Model 3: İleri Düzey

Bu yaklaşımda, belge yönetimi uygun bir EBYS aracılığı ile sağlanmalıdır. Belge hazırlama ve gönderme EBYS’nin sağladığı yazılım imkânı ile oluşturulmakta ve tüm onay işlemleri (Paraf ve alt imzalama) ile tüm imzalama işlemleri için e-imza

kullanılmaktadır. Kuruma gelen belgeler açısından, EBYS tarafından e-imza doğrulama işlemi belge yönetim sisteminde tamamlanmakta ve evrakın kalan hayat döngüsü içinde havale işlemleri de e-imza ile gerçekleştirilmektedir. Diğer işlemler EBYS'nin sağladığı imkânlar çerçevesinde yürütülmektedir. Bu model yaklaşımda daha ziyade network ortamı mevcut olan ve e-imzalama sürecine tam olarak hazır olan kurumlar için uygulanabilir.

Model 3'de asgari düzeyde ihtiyaç duyulan gereksinimleri şöyle sıralayabiliriz.

- Elektronik Belge Yönetim Sistemi Yazılımı
- E-imza oluşturma ve doğrulama Araçları (entegrasyonu yapılmış)
- E-imza kartı, Sertifikası (Tüm personel için)
- E-posta adresi ve bu adrese ulaşmak için internet bağlantısı



Şekil 22-Model 3-İleri Düzey Kurum dışı yazışmalar

Kaynak: Hamdi Boyacı, “Kamu Kurumları için uygulanabilir E-imza Modelleri”, Özelleştirme İdaresi Başkanlığı, Aralık, 2005.



Şekil 23-Model 3-İleri Düzey Kurumiçi Yazışmalar

Kaynak: Hamdi Boyacı, “Kamu Kurumları için uygulanabilir E-imza Modelleri”, Özelleştirme İdaresi Başkanlığı, Aralık, 2005.

Tablo 3-E-imzalı Belge Yönetimi Modelleri Arasındaki Farklar Tablosu

MODELLER ARASI FARKLAR TABLOSU								
		1. Adım	2.Adım	3.Adım	4.Adım	5.Adım	Sonuç	
Kurumlararası Yazışmalar	E-imzalı Giden Evrak	Model 1	Evrak Hazırlama	Paraflar & İnzalar (İslak)	Evrak Kaydı	Tarama, El. Ort. Akt.	E-İmza İşlemi	Gönderme
		Model 2	Evrak Hazırlama	Paraflar	E-İmza İşlemi	Evrak Kaydı		Gönderme
		Model 3	Evrak Hazırlama	Paraflar (E-imzalı)	İnzalama (E-imza)	Evrak Kaydı		Gönderme
Kurumlararası Yazışmalar	E-imzalı Gelen Evrak	Model 1	Teslim Alma	E-imza Doğrulama	Yazdırma	Evrak Kaydı	Havale İşlenleri	İşlem & Dosyalama
		Model 2	Teslim Alma	E-imza Doğrulama	Evrak Kaydı	Havale İşlenleri		İşlem & Dosyalama
		Model 3	Teslim Alma	E-imza Doğrulama	Evrak Kaydı	Havale İşlenleri (E-imzalı)		İşlem & Dosyalama
Kurum içi Yazışmalar	E-imzalı Giden Evrak	Model 1	Kurum içi Yazışmalar Klasik Usulde Devam Eder.					
		Model 2	Evrak Hazırlama	Paraflar	E-İmza İşlemi	Evrak Kaydı		Gönderme
		Model 3	Evrak Hazırlama	Paraflar (E-imzalı)	İnzalama (E-imza)	Evrak Kaydı		Gönderme
Kurum içi Yazışmalar	E-imzalı Gelen Evrak	Model 1	Kurum içi Yazışmalar Klasik Usulde Devam Eder.					
		Model 2	Teslim Alma	E-imza Doğrulama	Evrak Kaydı	Havale İşlenleri		İşlem & Dosyalama
		Model 3	Teslim Alma	E-imza Doğrulama	Evrak Kaydı	Havale İşlenleri (E-imzalı)		İşlem & Dosyalama

6.3. KURUMLARARASI ELEKTRONİK BELGE PAYLAŞIM HİZMETİ SPESİFİKASYONU

Geçtiğimiz yıllarda pek çok Kamu Kurum ve Kuruluşu, özel işletmeler, yerli ve yabancı yazılımlar ile kendi bünyelerindeki belgelerin elektronik ortamda oluşturulmasını, paylaşılmasını ve saklanmasını gerçekleştirmiştir. Fakat birbirleri ile paylaşım konusunda genele yayılabilecek bir çözüm, ortak standartların bulunmamasından dolayı geliştirilememiştir. Bütün Kamu kurum ve kuruluşlarının güvenle belge alıp verebilecekleri bir kanal olan e-Devlet kapısı projesinde bu eksikliğin giderilmesi amaçlanmış ve çalışmalar bu yönde şekillenmeye başlamıştır.

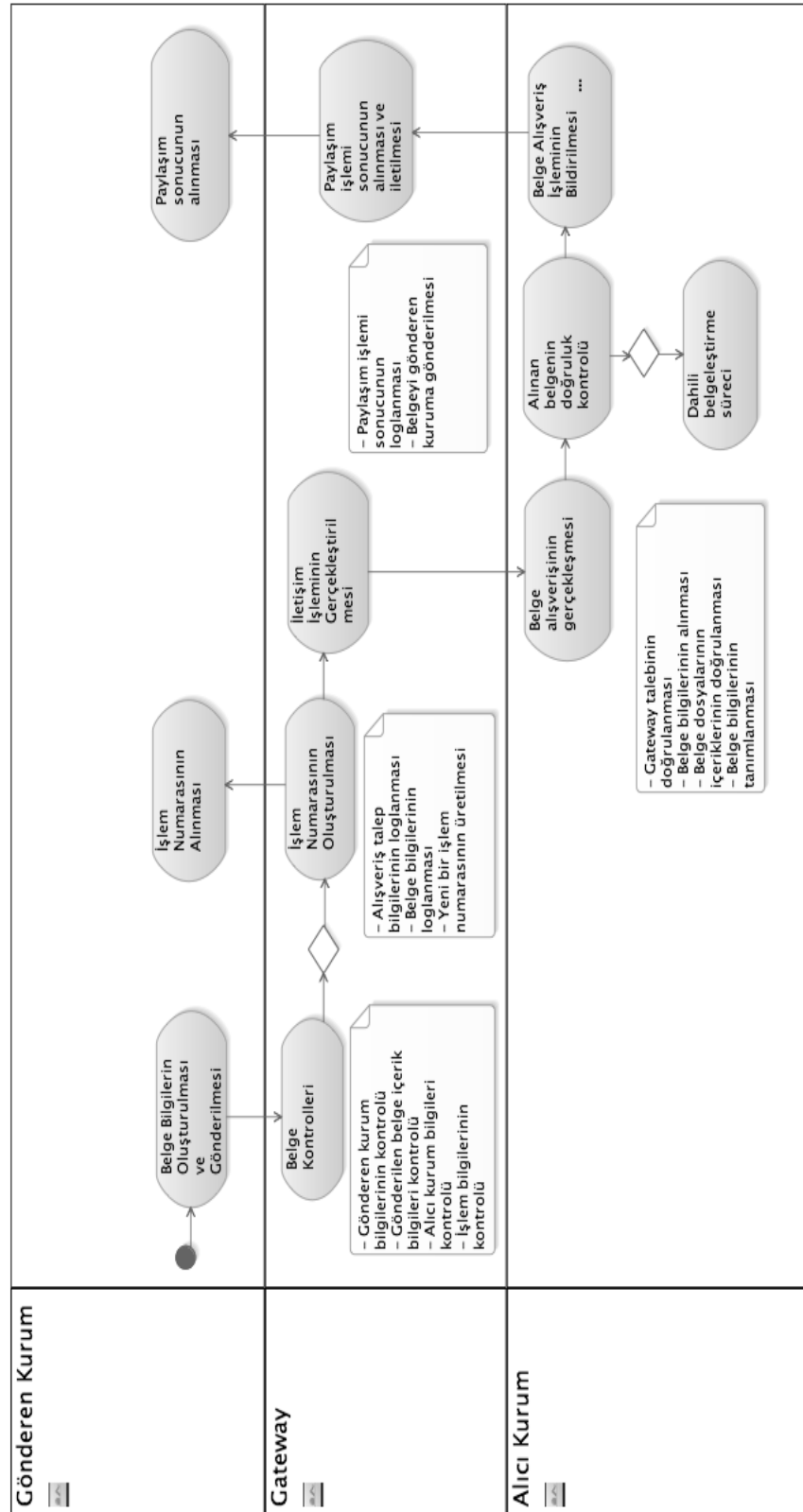
Bu paylaşımda temel olarak iki amaç hedeflenmiş ve bu doğrultuda kurgulanmıştır.

- Belgelerin gönderen kurumlardan alıcı kurumlara iletilmesi
- Gönderilen belgelerin alıcı kurumlar tarafından zimmete alındıkları bilgilerinin gönderen kurumlara iletilmesi

Birinci kurgulanan amaç, gönderen kurum belgelerini bir sonraki metaveri seti ile birlikte e-Devlet Kapısı üzerinden gönderme işlemini başlatır. Alıcı kurumun bilgileri bazında e-Devlet kapısı üzerinden kontroller gerçekleştirir ve alıcı kurumun hizmete sunduğu Web Servisin açık olması ile belge transferi işlemi başlatılır. Gönderen kurumun her bir belge transferi talebi için e-Devlet Kapısı bir hizmet numarası (transaction id) üretir ve bunu gönderen kuruma ve alıcı kuruma bildirir. Bu şekilde gönderilme ve zimmete alınma işlemleri asenkron bir şekilde gerçekleştirilebilir. Belge göndermenin ilk aşaması ise, alıcı kurumun belgeleri aldıktan ve belge bütünlüğünü doğruladıktan sonra göndereceği onay mesajının kapı üzerinden gönderen kuruma iletilmesi ile tamamlanmaktadır.

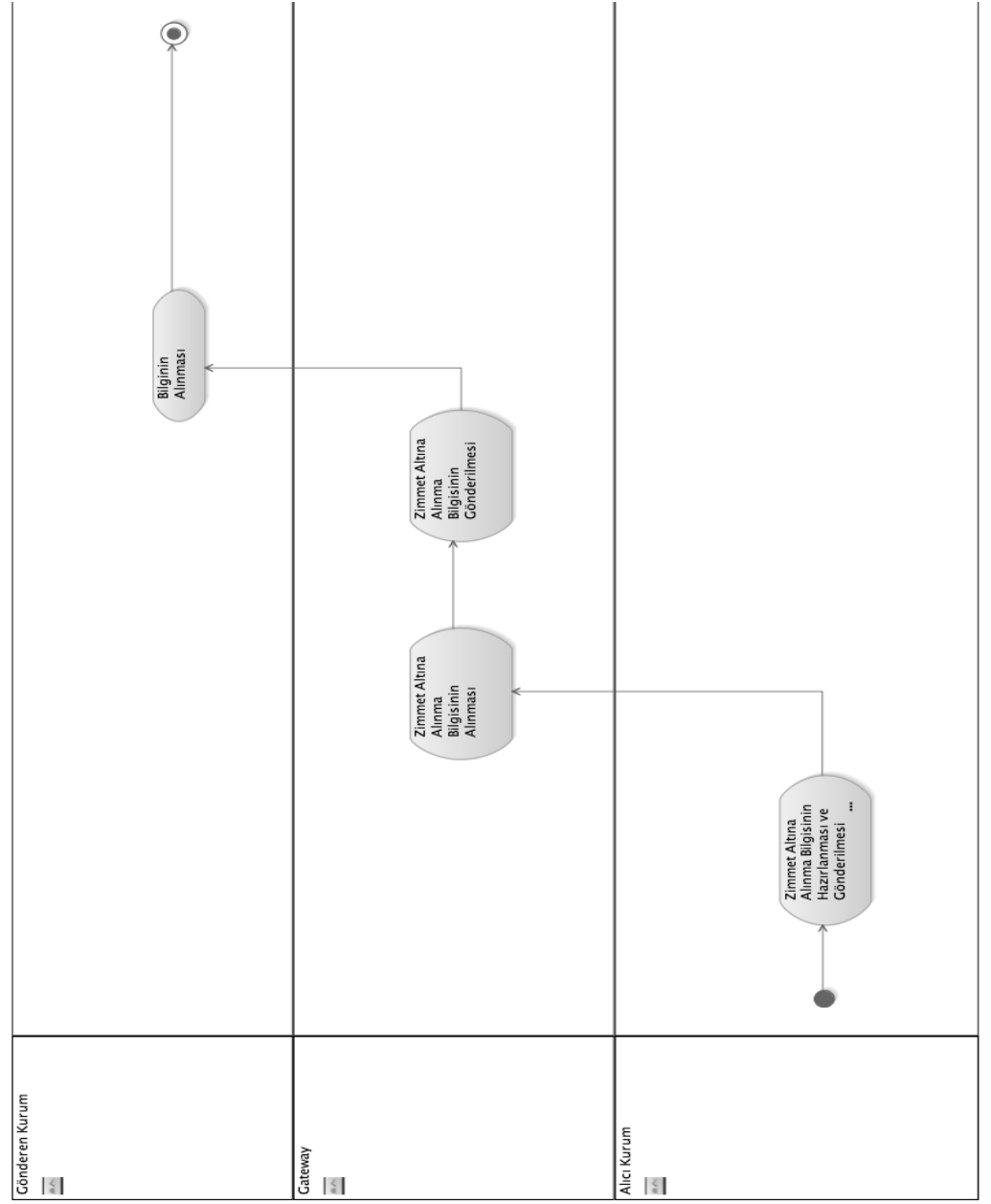
Belge gönderimde kurgulanan ikinci amaç ise, birinci amacı tamamlayıcı bir niteliktedir. Birinci amaçtaki işlemlerde herhangi bir insan müdahalesine gerek yoktur. İkinci amaçta ise alıcı kurum tarafındaki sorumlu kişilerin belgeleri elden teslim almaları ve gelen belgeleri numara vermeleri demektir. Uygun olmayan belgelerin iade edilmesini içerir.¹⁷⁴

¹⁷⁴ Ahmet Kaplan, Mustafa Canlı, Yasin Kahramaner (hızl.), **Kurumlararası Elektronik Belge Paylaşım Hizmeti Spesifikasyonu v.1.**, <http://www.devletarsivleri.gov.tr>. (29 Şubat 2008)



Şekil 24- Belgelerin Gönderen Kurumdan Alıcı Kuruma İletilmesi

Kaynak: Kaplan, Canlı ve Kahramaner, 2008.



Şekil 25-Alınan Belgelerin Zimmet Altına Alınma Bilgilerinin Gönderilmesi

Kaynak: Kaplan, Canlı ve Kahramaner, 2008

6.3.1. e-Devlet Kapısı Üzerinden Paylaşım Senaryosu

e-Devlet Kapısı tarafında çeşitli hizmetlerin verilmesi planlanmaktadır. Bu hizmetlerin tanımlanmasında ise aşağıda belirtilen faktörler göz önünde bulundurulmuştur:

- Sunulacak hizmetler, Java, .Net ve benzeri teknolojiler tarafından erişilebilir olmalıdırlar.
- Hizmetler, belgelerin doğru ve bir bütün olarak güvenilir bir kanaldan aktarılmasını sağlamalıdır.
- Belge metaverilerinin paylaşımı sırasında alıcı ve gönderen kurumlar arasında bilgilerin doğru anlamlandırılmasını sağlayacak standardizasyon sağlanmalıdır.
- Sunulan hizmetler ve bilgiler, ileriki aşamalarda zenginleştirilebilecek türden olmalıdır.¹⁷⁵

6.3.2. Kullanım Senaryoları

Metaveriler tanımlanırken aşağıda belirtilen kullanım senaryolarının gereksinimleri esas alınmıştır:

- Herhangi bir Kamu Kuruluşu, kendi hazırlamış olduğu bir (kurum dışı giden) belgeyi, elektronik ortamda alıcı Kurum ve Kuruluş(-lara) gönderir.
- Gönderilen belge içerisinde birden fazla ek dosya bulunabilir. Bu dosyalar elektronik imza ile imzalanmış olabileceği gibi alıcı ve verici kurumlar arasında mutabık kalınmış bir algoritma / anahtar kombinasyonu ile şifrelenmiş de olabilir.
- Gönderilecek ek dosyalar yine gönderen / alıcı kurumlar tarafından tanımlanan bir teknikle sıkıştırılmış olarak da gönderilebilir.

Yukarıdaki kullanım senaryoları, gereksinimleri karşılanmaya çalışılan genel kullanım senaryosunu betimlemekle beraber, aşağıda belirtilen senaryolar ise bu çalışmanın kapsamı dışında bırakılmıştır:

- Kamu Kurum ve Kuruluşlarına sadece belge paylaşımı platformu sunmak değil, beraberinde de sürekli olarak dosyaları oluşturabilecekleri, üzerinde çalışabilecekleri bir platform sunmak. Bir diğer deyişle, bir Collaboration Platform oluşturmaktansa, bir Communication Channel'in iletişim standartlarını belirlemek.

¹⁷⁵ Kaplan, Canlı ve Kahramaner, 2008, s.[2-3]

- Kamu personelinin bir proje kapsamında başka bir kurumdaki personele iş ataması yapmasını sağlamak.

Tanımlanan standartlar, vatandaşların ya da özel işletmelerin direk olarak belge göndermelerini sağlamayı hedeflememektedir.¹⁷⁶

6.3.3. Başarı Faktörleri

Başarı faktörleri aşağıdaki şekilde sıralanmıştır.

- Tanımlanan metaveriler, kurum dışı giden / gelen belgeler için geçerli olanlar olmalıdır. Taslak ya da bir iç yazışmayı ilgilendirecek bilgi kümelerinden kaçınılmalıdır.
- Metaveriler, hem kurum kuruluşlar için, hem de yazılım tedarikçileri için üretilebilir, yönetilebilir ve anlamlı olmalıdır.
- Devlet Arşivleri tarafından hazırlanmış ve standartlaşmış olan Elektronik Belge Yönetim Standardı, tanımlanan metaveriler için bir baz teşkil etmelidir.
- Metaverilerin tanımlanmasında ve şablonlaştırılmasında şu an öngörülemeyen ileriki dönemlerdeki gereksinimleri barındırabilecek esneklikler tanınmalıdır.

Bununla beraber gereksinim olarak belirtilen metaveriler, direk olarak son kullanıcılar için anlamlı olarak gelmesi de belgelerin sorunsuz bir şekilde paylaşılması, doğru alıcılara hatasız bir şekilde gönderilmesini sağlamak için bir takım ekstra alanları da içermektedir.¹⁷⁷

6.3.4. Sunulacak Tamamlayıcı Hizmetler

Bu proje kapsamında önemli bir hedef, elektronik belgelerin bilgilerinin doğru bir şekilde alışverişinin gerçekleşmesi ve bu belge bilgilerinin mevcut yazılımlarda doğru bir şekilde yorumlanarak belgeleştirilmesidir. Bu nedenle birtakım standart

¹⁷⁶ Kaplan, Canlı ve Kahramaner, 2008, s.[2]

¹⁷⁷ Kaplan, Canlı ve Kahramaner, 2008, s.[1].

bilgiler kapı üzerinden sunulacaktır. Sunulacak bilgi türleri tablosu aşağıda sıralanmıştır.¹⁷⁸

Tablo 4-EBPS kapsamında Sunulacak Tamamlayıcı Hizmetler Tablosu

İçerik Bilgi Kontrolü	Belge Gizlilik Düzeyleri Listesi
Bilgilendirme Hizmeti	Belge Türleri Listesi
İşlem Sonuç Kodları	Dosya Belge Türleri Listesi
Örnek Konu Kodları Hizmeti	Dosya Formatı Listesi
Kamu Kuruluşları Kodları	Sıkıştırma Parametreleri Listesi
Belge Öncelik Düzeyleri Kodları	Şifreleme Parametreleri Listesi
Belge Öncelik Düzeyleri Listesi	Arşiv Dosya Formatları Listesi

Kaynak: Kaplan, Canlı ve Kahramaner, 2008

¹⁷⁸ Kaplan, Canlı ve Kahramaner, 2008, s.[6-7].

7. BÖLÜM-GÜVENLİ ELEKTRONİK ARŞİVLEME: STANDARTLAR, YAPILAR VE İŞLEVLER

Elektronik ortamdaki işlemlere güvenilir zaman bilgisi eklenebilmesini sağlayan zaman damgası, üzerinde zaman bilgisi olması gereken elektronik başvuru, tutanak, sözleşme ve benzeri her türlü elektronik veri üzerinde kullanılabilir ¹⁷⁹ Zaman içerisinde dokümanların bütünlüğü ve kaynağının doğruluğu elektronik imza ile sağlansa bile, imzaların atılmasını sağlayan elektronik sertifikaların ömrü sınırlı olduğundan, geçerlilik kontrolü bakımından yine bir açık doğabilir. Gerçek hayattan örneklemek gerekirse, şirket belgeleri, abonelik sözleşmeleri ve senetler gibi çoğu doküman uzun süre geçerliliğini devam ettirebilir ama onaylayan imzalar gizli anahtarlarının güvenlik sorunları ve idari olarak sertifikalarda yer alan bilgiler sebebiyle kısıtlı ömre sahiptirler. Olası güvenlik sorunları arasında gizli anahtarın tutulduğu aracın çalınması ya da kriptanalizin zaman içerisinde gizli anahtarı açığa çıkarması gibi örnekler sayılabilir. Dolayısıyla, ileri destek olmaksızın, tek başına elektronik imzalar, imzalı dokümanların uzun dönemli tutulması açısından uygun değildirler. İmza doğrulaması yaparken, dokümanın imzalanmış olduğu andaki gizli anahtar güvenliği ve sertifika geçerliliğinden emin olmak (hala “gizli” ve münhasıran sahibine ait) son derece önemli bir noktadır.

Bu problemin üstesinden gelmek için RFC 3161’de¹⁸⁰ belirtilen, “Uzun Dönemli Elektronik İmzalar” kavramı ortaya atılmış ve geleneksel arşiv sistemlerinin yerini elektronik imzalı ve zaman damgalı arşivleme tekniğinin alacağı öne sürülmüştür.

7.1. UZUN DÖNEMLİ İMZA DOĞRULAMADA YAŞANABİLECEK SORUNLAR

Bir elektronik imzanın, oluşturulmasının üzerinden uzun bir süre geçtikten sonra doğrulanabilmesi, problemlili olmaya aday bir konudur. Aradan geçen zaman nedeniyle ortaya çıkabilecek sorunlar şunlardır:

¹⁷⁹ Stuart Haber ve Henry Massias “Time-stamping”, *Encyclopedia of Cryptography and Security*, Springer, 2005, s.12.

¹⁸⁰ C. Adams, P. Cain, D. Pinkas, R. Zuccherato, *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*, August 2001, Request for Comments: 3161, <http://www.ietf.org/rfc/rfc3161.txt>, s.5-26.

1. İmza sahibi sertifikanın imza oluşturulduğu andaki geçerlilik durumunun bilinmemesi: Sertifikalar geçerlilik sürelerini henüz doldurmamışken, geçerlilik durumlarını Elektronik Sertifika Hizmet Sağlayıcısı (ESHS) kurumların yayınladığı iptal listeleri (CRL) veya sağladıkları durum sorgulama protokolü hizmeti (OCSP) aracılığıyla öğrenmek mümkündür. Ancak geçerlilik süresi sona eren sertifikalar, iptal edilmişlerse bile CRL içeriğinden çıkarılırlar. OCSP ise anlık durumu belirten bir protokol olduğu için, OCSP ile herhangi bir sertifikanın geçmişteki bir anda geçerli olup olmadığını sorgulamak mümkün değildir.

2. ESHS kayıtlarından geçmişteki bir iptal listesini elde etmek mümkün olabilir, ancak eski iptal listelerinin çevrimiçi olarak yayınlanması yaygın bir uygulama olmadığı gibi, uzun bir süre geçtikten sonra ESHS'nin faaliyetlerine devam etmiyor olması olasılığı göz ardı edilemez.

3. ESHS gizli anahtarının çalınması: İmza sahibi sertifikayı oluşturmakta kullanılmış olan ESHS gizli anahtarının çalınması, ESHS tarafından üretilmiş geçerli sertifikalar gibi görünen sahte sertifikaların üretilmesine imkan tanıyacaktır. Böyle bir hırsızlık yaşanırsa, doğrulanan bir imzaya güvenmek için hırsızlık anından önce oluşturulmuş geçerli bir sertifika ile atıldığını kanıtlamak gerekecektir.

4. Sertifikada ve imzada kullanılan kriptografik algoritmaların güvenilirliklerini kaybetmiş olması: Sertifikalar ve imzalar oluşturulurken kullanılan özet algoritmaları (örneğin SHA-1) veya şifreleme algoritmaları (örneğin RSA) aradan geçen zamanda kriptografi ve teknoloji alanındaki gelişmeler nedeniyle güvenilirliklerini kaybedebilirler. Böyle bir gelişme, herhangi bir gizli anahtar hırsızlığı olmaksızın sahte sertifika oluşturma veya sahte imza oluşturma imkânlarını kötü niyetli kişilere tanır. Bu nedenle, doğrulanan eski bir imzanın, bu sahteciliğin teknik olarak mümkün olmadığı bir anda oluşturulmuş olduğunu kanıtlamak önem taşıyacaktır.

7.2. GÜVENLİ ZAMAN DAMGALI E-İMZA

Zaman damgası elektronik bir belgenin belirli bir anda varlığının taahhüdüdür. Elektronik verinin korunmasına yönelik e-imza ile beraber delil niteliği taşıması açısından gerekli bir araçtır. Zaman damgası hizmeti, Zaman Damgası Hizmet

Sağlayıcıları (ZDHS) tarafından verilir.¹⁸¹ Güvenli bir elektronik arşivleme için önceki kısımda yazdığımız nedenlerden ötürü zaman damgasının e-imza ile tümleşik şekilde kullanılması gerekir. Elektronik imzalı bir belgenin kullanım süresi zaman damgalama hizmeti ile uzatılabilir.¹⁸²

Genelliği bozmadan, belirli anahtar uzunlukları ile açık metin D dokümanın elektronik imzası δ olan bir elektronik imzalama tekniğini varsayalım.¹⁸³ Gizli anahtar açığa çıkması, hedef uzunluk için sayısal hesaplama gücünün artması ya da algoritmada var olan bir açığın ortaya çıkması gibi herhangi bir sebepten ötürü bir zaman sonra imza geçersiz olabilir. Bu noktada doküman-imza çiftinin güvenilirliği şüphelidir zira orijinal sahibinin dışında başkaları da imzalama yapabilir. Bununla beraber, eğer (D, δ) çifti imza geçerliliğini yitirmeden zaman damgalansaydı, imza hala geçerli olacaktı çünkü imzanın atıldığı anda sadece ve sadece orijinal sahibinin sorumluluğunda olacağı garanti altında olacaktı. Anahtar açığa çıksa dahi, anahtarın açığa çıkış tarihi doküman üzerindeki zaman bilgisi ile çelişeceğinden sorun teşkil etmeyecekti.

Güvenlik açısından bakacak olursak ZDHS'ye sadece özet değer yollandığından gizlilik sağlanmış olunur.¹⁸⁴ Elbette ki hem imzalayan hem doğrulayan taraflar ZDHS'ye güveneceğinden dolayı bütünlük ve kimlik denetimi de vardır. Zaman damgasız elektronik imzalar sertifika iptal olunca geçersiz olacağından, inkar edilemezlik prensibine uymak için mutlaka zamanı da dokümana iliştiirmek gereklidir. Hatta bu prensibi daha da sağlamlaştırmak amacıyla bağlama zaman damgası tasarıları geliştirilmiştir. Zaman damgalı verinin geçici sırasının inkar edilemez biçimde belirlenmesi amacıyla kullanılıp, ZDHS'nin mesuliyetini öne çıkarırlar. Altında yatan nokta, ileride gelecek zaman damgası isteklerinin ve özet değerlerinin bilinemeyeceğidir. Eğer belirli bir zaman damgası önceki zaman damgalarından kısımlar içeriyorsa, aralarında zamana bağımlı bir kısmi sıra kurulur ve güven ile inkar edilemezlik hiyerarşisi bu şekilde sağlanır.

¹⁸¹ Meelis Roos, "Integrating time-stamping and notarization" (Master's Thesis, Tartu University), <http://home.cyber.ee/mroos/thesis/>, s. 11.

¹⁸² Petros Maniatis, Mary Baker, "Enabling the archival storage of signed documents". **FAST '02: Proceedings of the 1st USENIX Conference on File and Storage Technologies**, Monterey, CA ,2002, s.28.

¹⁸³ Adams, Cain, Pinkas, Zuccherato, 2001, s.23-24.

¹⁸⁴ Dave Bayer, Stuart Haber, W. Scott Stornetta, "Improving the efficiency and reliability of digital time-stamping", **Methods in Communication, Security, and Computer Science - Sequences'91**, s.329-334..

7.3. UZUN DÖNEMLİ ELEKTRONİK İMZA YAPILARI

İmzaların uzun dönemli saklanmasıyla yaşanacağı öngörülen sorunlara karşı tedbir alabilmek amacıyla, imzaların gerekli ek verilerle birlikte depolanması bir çözüm önerisi olarak sunulmuştur. İmza veri yapısı standartlarına bağlı olarak bu konuda iki standart geliştirilmiştir: Kriptografik Mesaj Sözdizimi (CMS) yapısındaki imzalar için CMS İleri Elektronik İmzalar (CADES)¹⁸⁵, XML yapısındaki imzalar için XML İleri Elektronik İmzalar (XAdES)¹⁸⁶.

CADES bünyesinde tanımlanan veri yapıları, çekirdekte yer alan imza verisinin üzerine sağlıklı bir arşivleme için gerekli verilerin katmanlar halinde eklenmesini sağlamaktadırlar.¹⁸⁷ Dokümanda tanımlanan yapılar ve olası problemlere karşı tedbirlere nasıl hizmet ettikleri aşağıda özetlenmiştir.¹⁸⁸

7.3.1. İmza verisi (Electronic Signature – ES)

Çekirdekte yer alan imza verisidir. Yapısı CMS standardında, mevcut durumda kullanılmakta olan imza yapısıdır. CADES, imza yapısının zorunlu içeriğine ek olarak, imzanın oluşturulma ilkelerini belirten bir tanımlayıcı numaranın da imzalı veri içinde imzalı özellikler (Signed Attributes) alanında bulunmasını öngörmektedir. Böyle bir numara kullanılmıyorsa, imza oluşturan taraf ilgili alanı boş bırakarak, imza oluşturma ilkelerinin imzalı içerik ve dış veriler tarafından ima edildiğini belirtebilmektedir.

7.3.2. Zaman damgalı imza (ES with Timestamp – ES-T)

Kriptografik imza değerinin zaman damgalanması ve bu damganın bir ek değer olarak imza yapısına yerleştirilmesiyle oluşturulur. Bu zaman damgası imzanın belirtilen zamandan önce oluşturulmuş olduğunu belgeleyerek imzanın uzun dönemli güvenilirliği konusunda önemli bir boşluğu doldurur. Zaman damgası imzaya, imza

¹⁸⁵ D. Pinkas, N. Pope, J. Ross, *CMS Advanced Electronic Signatures (CADES)*, 2008, <http://tools.ietf.org/html/rfc5126>, s.30-34.

¹⁸⁶ Juan Carlos Cruellas, Gregor Karlinger, Denis Pinkas, John Ross, *XML Advanced Electronic Signatures (XAdES)*, 2003, <http://www.w3.org/TR/XAdES/> (15 Nisan 2008).

¹⁸⁷ Stuart Haber , W.Scott Stornetta, “How to time-stamp a digital document”, *Journal of Cryptology*, No.3(2), 1991, s.99-111.

¹⁸⁸ Dave Beckett, **Resource description framework (RDF)**, [y. y.]: [yayl. y.], 1999, <http://www.w3.org/RDF/> (26 Haziran 2008).

oluşturulduktan hemen sonra imza sahibi tarafından eklenebileceği gibi, imzayı doğrulayan başka bir tarafça da eklenebilir. İmza doğrulama ilkeleri açısından imzanın oluşturulma zamanı ile üzerindeki zaman damgasının belirttiği zaman arasındaki fark bir kıstas oluşturabilir. İlkeler, bu farkın belirli bir değerin üzerinde olması halinde imzayı güvenilir kabul etmeyecek şekilde düzenlenebilirler.

7.3.3. Tam doğrulama verisi içeren imza (ES with Complete Validation Data – ES-C)

ES-T verisine ESHS sertifika referanslarının ve geçerlilik durum bilgisi referanslarının eklenmesiyle oluşturulur. ESHS sertifika referansları, imza sahibi sertifikanın bağlı olduğu ESHS kök ve alt kök sertifikalarının referanslarıdır. Sertifika referansları, sertifikaların “imzalayan sertifika adı”, “seri numarası” ve sertifika özeti değerlerinden oluşurlar. Geçerlilik durum bilgisi referansları, imza sahibi sertifika ile bağlı olduğu alt kök sertifikaların geçerliliklerini belgeleyen iptal listelerinin (CRL) veya OCSP sorgusu cevaplarının referanslarıdır. Bu referanslar, iptal listelerinin veya OCSP sorgu cevaplarının özet değerlerinden oluşurlar. İmza yapısına ESHS sertifika referansları ile geçerlilik durum bilgisi referansları eklendiğinde, imza sahibi sertifikanın hangi ESHS sertifikası zincirine bağlı olduğu ve geçerlilik durumunun ESHS’nin hangi bildirimiyle (CRL veya OCSP), ne zaman kontrol edildiği açık olarak ifade edilmiş olur. Bu yapının kullanılması, zaman içerisinde ESHS sertifikaları ve geçerlilik durum kontrolleri hakkında güvenlik tereddütlerinin ortaya çıkması dolayısıyla imzanın güvenilirliğinin sorgulanması durumunda fayda sağlar. İmza yapısı, imza sahibi sertifikanın geçerlilik kontrol verilerine referanslar barındırdığı için bu verilere (ESHs sertifikalarına ve CRL/OCSP verilerine) ulaşarak sertifikanın belirtilen zamandaki geçerliliğini tekrar kontrol etmek mümkün olacaktır. Ancak böyle bir kontrolün yapılabilmesi için ilgili sertifikalar, iptal listeleri ve OCSP sorgusu cevaplarının ulaşılabilir durumda tutulması gerekmektedir.

7.3.4. Genişletilmiş doğrulama verisi içeren imza (ES with eXtended Validation Data – ES-X)

ES-C verisine, referansları verilen ESHS sertifikaları ile iptal listesi ve OSCP sorgusu cevaplarının kendilerinin eklenmesiyle oluşturulur. Böylece doğrulama anında ESHS kök sertifikası dışında hiçbir dış veri kullanılmasına gerek kalmaz. Tüm sertifikalar, iptal listeleri ve OSCP cevapları kök sertifikadan başlayan bir zincirin halkaları olarak doğrulanabilirler.

7.3.5. Arşivlenmiş doğrulama verisi içeren imza (ES with Archive Validation Data – ES-A)

ES-X verisindeki bilgilere zaman damgası vurularak bu zaman damgasının veriye eklenmesiyle oluşturulur. Amacı zaman damgası hizmet sağlayıcısı sertifikaları ve zaman damgalarında kullanılan algoritmaların zaman içinde zayıflamasına karşı tedbir almaktır. ES-A yapısı oluşturulurken vurulan zaman damgasında, imza ve sertifikalardakilere kıyasla daha uzun bir anahtar ve mümkünse daha kuvvetli bir algoritma kullanılmalıdır. Böylece, imza ve sertifikadaki algoritmalar güvenli olma özelliklerini belirli bir süre sonra kaybederseler bile, ES-A yapısındaki zaman damgası içerideki verilerin doğruluğunu daha uzun bir süre boyunca belgeleyebilecektir. ES-A yapıları başka ES-A yapılarının üzerine yeni bir zaman damgası eklenerek de oluşturulabilirler. Bu özellik, ES-A yapılarının üzerine periyodik olarak daha kuvvetli algoritmalarla zaman damgası ekleyerek arşivleme süresini sürekli uzatma imkânını tanır.

7.4. GÜVENLİ E-ARŞİVLEME İŞLEVLERİ

Değişik güvenli elektronik arşivleme yazılım ve donanım ürün ve çözümleri küresel pazarda yer almaktadır.¹⁸⁹ Hukuksal açıdan yeterli olmakla beraber, teknik açıdan kısmi güvenli çözümlerdir. Yerel kanunlara göre, ülkeden ülkeye amaçları, uygulama prensipleri ve güvenlik seviyeleri değişebilir. Yayınlanan tebliğler altyapıyı

¹⁸⁹ Committee on Digital Archiving and the National Archives and Records Administration, “**Building an Electronic Records Archive at the National Archives and Records Administration: Recommendations for a Long-term Strategy**”, National Academies Press: 2005, s.25-36.

belirlemede kıstas oluşturur. Bazı ülkelerde elektronik dokümanların “wormmedia” halinde depolanması güvenli elektronik arşivleme aracı olarak kullanılmaktadır.

Varolan çözümlerin standart olarak içlerinde barındırmaları gereken hizmetler vardır. Son kullanıcı ile olan iletişimde bu işlevler sayesinde etkileşim kurulur. Kısaca özetlemek gerekirse beş başlıkta toplayabiliriz.

1) **Arşivleme:** Tek ya da grup halindeki dokümanların korunumsal vasıflarının yaratılmasını tetikler.

2) **Durum:** Arşivleme işleminin ilerlemesi hakkında bilgi verir.

3) **Doğrulama:** Belli bir dokümanın korunumsal vasıflarını işlemek için doğrulama motorunu tetikler.

4) **İhraç:** Belli bir dokümanın korunumsal vasıflarının ihracı (dosyaya yazılması, diske depolanması) için gereklidir.

5) **Silme:** Arşivlenen dokümanların silinerek arşivden çıkarılması için kullanılır.

Genelliği bozmadan sağlanması gereken şartlar;

1) Arşivlenen dokümanlara uygulanan elektronik imzaların, imzalayan sertifika iptal olsa ya da geçerliliğini yitirse dahi kullanılır olması,

2) Doküman tipinden bağımsız olarak arşivlenen verinin bütünlüğünün herhangi bir zaman dilimi için korunması,

3) Arşivlenen veri ya da dokümana ait tüm değişikliklerin takip edilebilmesi,

4) Arşivlenen verideki bütün önemli alanların (sahibi, yeri, yaratılma zamanı, vb.) herhangi bir zaman çözümlenebilmesi

5) Arşivlenme teknolojisi değişse dahi arşivlenen verinin okunabilir olması,

6) Doğrulamada kullanılacak tamamlayıcı verinin her zaman hazır olması ve üçüncü güvenilir taraflarca kontrolde tutulması;

olarak sıralanabilir.

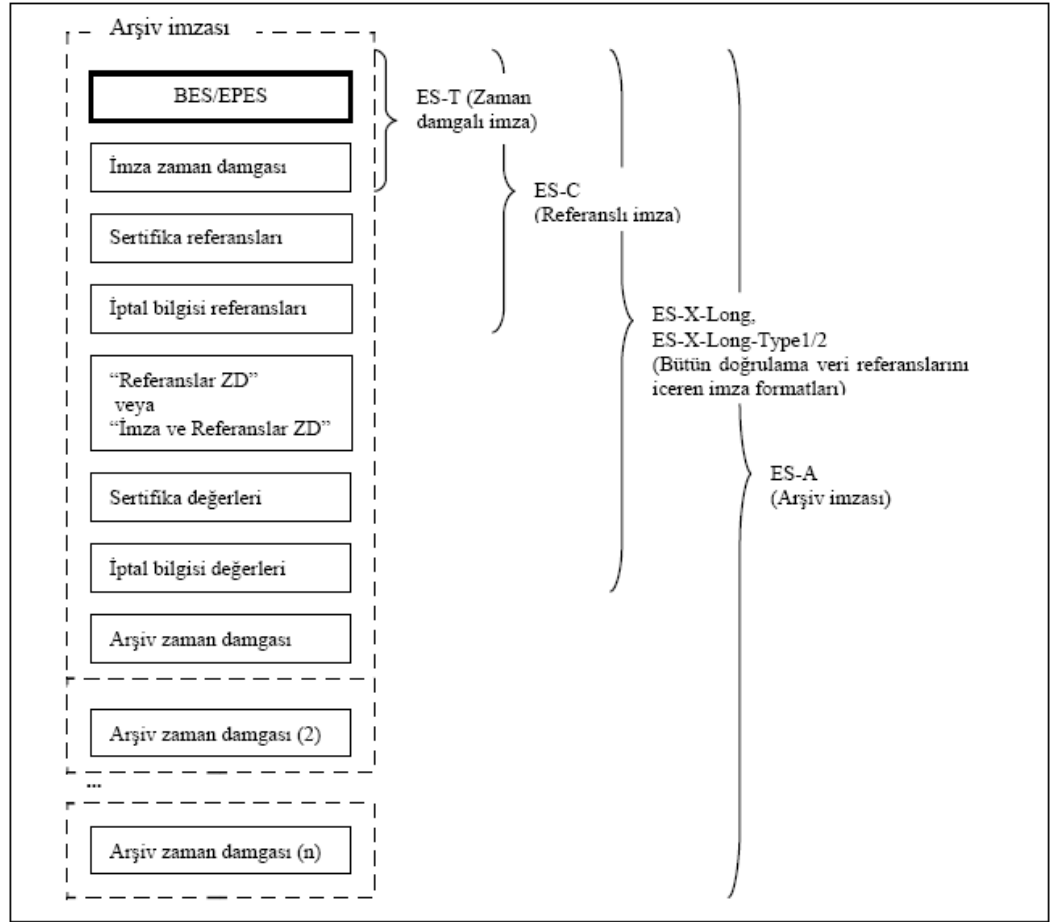
7.5. ARŞİV İMZASI

Elektronik imza oluşturulurken kullanılan kriptografik algoritmalar zamanla zayıflamakta ve kırılabilir hale gelmektedir.¹⁹⁰ Aynı şekilde, imzaya eklenen zaman damgaları da kullanılan algoritmalara bağlı olarak zamanla zayıflamaktadır. İmza oluşturulurken kullanılan sertifikaların ait olduğu üst köklerin de belirli geçerlilik süreleri vardır. Bu zayıflamalardan dolayı, imzanın geçerliliğini koruyabilmesi için periyodik olarak tekrar güçlendirilmesi gerekmektedir. Örneğin; imza oluşturulurken SHA-1 özetleme algoritması kullanılmış ise, belirli bir süre sonra, SHA-1 özetleme algoritması kırılabilir düzeye gelmeden önce daha güçlü bir özetleme algoritması kullanılarak oluşturulmuş olan bir zaman damgası imzaya eklenerek imza güçlendirilmelidir. Hatta eklenen bu zaman damgası; imza değerini de içerek şekilde imzadaki eklentileri, imza zaman damgasını, bütün doğrulama verisi referanslarını, bu referanslara karşılık gelen değerleri, imzayı ve referansları koruyan zaman damgasını veya sadece referansları koruyan zaman damgasını kapsayarak güçlendirmelidir.

ETSI 'de bu ihtiyaca arşivleme işlemi ile çözüm önerisinde bulunmaktadır. Arşivleme işleminde, zayıflayan imzaya imzadaki tüm eklentileri kapsayacak şekilde ve imzadaki zaman damgalarından daha güçlü bir özetleme algoritması kullanılarak bir zaman damgası eklenmektedir. Eklenen bu zaman damgası arşiv zaman damgasıdır . Bu formattaki imza ise ETSI tarafından tanımlanmış olan standartta “Archival Electronic Signature (ES-A)” olarak adlandırılmaktadır. Arşiv imzasının içermesi gereken eklentiler aşağıdaki şekilde gibidir. Arşiv zaman damgası da zaman içinde güçsüzleşebilir. Bu nedenle ETSI imzaya birden fazla arşiv zaman damgası eklenmesine izin vermektedir.¹⁹¹

¹⁹⁰ European Committee For Standardization, Security requirements for signature creation applications, May 2004, Supersedes CWA 14170:2001, <ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14170-00-2004-May.pdf>, (25 Haziran 2008) s.19.

¹⁹¹ ETSI TS 101 733 V1.5.1 (2003-7 12), “Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats”, http://portal.etsi.org/docbox/EC_Files/EC_Files/ts_101733v010400p.pdf, (30 Nisan 2007) s.50.



Şekil 26- Arşiv imzasının içermesi gereken eklentiler

Kaynak: Gonca Hülya Selçuk, "E-Devlet Uygulamaları İçin Elektronik İmza Formatları", www.kamusal.gov.tr/tr/Bilgideposu/Belgeler/Makaleler/EDevletUygulamalariIcinElektronikImzaFormatlari.pdf, (2 Temmuz 2008)

8-BÖLÜM-ELEKTRONİK İMZANIN HUKUKİ BOYUTLARI

8.1. BÖLÜM-ELEKTRONİK DOKÜMANLARI VEYA MEKTUP'LARIN KANIT OLABİLMESİ İÇİN GEREKSİNİMLER

Bilişim sistemlerinin sağladığı, bilgiyi üretme saklama iletme ve erişme servisleri sayesinde günlük hayatımızı kolaylaştıran birçok işlem bu ortamda gerçekleştirilebilmektedir. Bununla birlikte, elektronik ortamda üretilen, saklanan ve iletilen bilgiler aracılığı ile kişi veya kurumlara hakaret, tehdit, dolandırıcılık, sahtecilik, servis durdurma, iletişimi engelleme, gizli ve özel bilgileri ifşa etme vs gibi kötü niyetli eylemler gerçekleştirilebilmektedir. Bu tür eylemleri belirlemek ve önlemek için yine elektronik ortamda koruma önlemleri (Güvenlik duvarları, nüfuz tespit sistemleri, şifreleme kimlik doğrulama, sayılsa imza vs.) alınabilmektedir. Bütün bu önlemlere gerek elektronik ortamın doğası gerekse bilgi iletim ve erişim protokol servislerinin zayıflıklarını nedeniyle sanal ortamdaki suçların önlenmesi mümkün olmamaktadır. Elektronik posta ile gelen ve içeriğinde kurum ve kişiye hakaret bulunduran bir mesaj veya kişisel bilgisayarda da bulunan ve suç teşkil edecek bir eylemin planını açıklayan belge bunlara örnek olarak gösterilebilir.¹⁹² Doğal olarak güvenlik güçleri ihbar veya şikayet üzerine bu mesaj ve belgelere göre ilgili kişileri zanlı olarak değerlendirip haklarında kanuni takibat yapmakta, haklarında dava açabilmektedir.¹⁹³ Ancak bu gibi durumlarda gönderilen e-postanın gerçekten doğru kişiden gönderilip gönderilmediği içeriğinin değişmediğinin veya kişisel bilgisayarda bulunan bir belgenin kim tarafından hazırlanıp oraya kopyalandığının anlaşılması günümüzdeki anlaşmazlık konuları içerisinde önemli bir yer tutmaktadır. Bu gibi durumlarda çoğunlukla müşteki, gelen e-postaya bakarak karşı tarafa hakkında hukuki işlem başlatmakta, bu süreçte ise yargı makamı, Bilirkişi raporuna dayanarak (e-postanın başlık bilgilerinden hareket ederek) mesajı gönderen bilgisayarın IP (Internet Protokol) adresinin tespit edilerek mesaj kaynağının belirlenmesi yolunu seçmekte ve bu bilgiye dayanarak karar verebilmektedir. Bu şekilde verilen karar ise bir üst mahkeme tarafında yanlış bulunarak

¹⁹² Yargıtay 4. Hukuk Dairesi, 20. Asliye Hukuk Mahkemesi, 23 Ağustos 2005, İlgili Karar, http://www.hukuki.net/topic.asp?topic_id=9565, (17 Nisan 2007)

¹⁹³ Yargıtay 4. Ceza Dairesi E. 2004/8763 K. 2005/21445 T. 5.12.2005, “İnternet Yoluyla Hakaret ve Sövme”, <http://www.turkhukusitesi.com/showthread.php?t=7185>, (26 Haziran 2008).

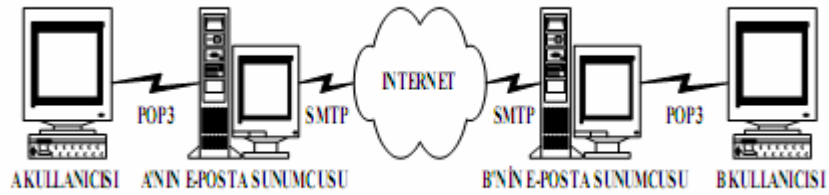
bozulabilmektedir. Bazı durumlarda ise bilirkişi raporları çelişebilmektedir.¹⁹⁴ Elektronik ortamda saklanan ve iletilen bilgilerin güvenilir olması için, verinin gizliliği, bütünlüğü ve kullanılabilirliğinin sağlanması yanında üretici göndericinin kimliğinin doğrulanması, gereklidir. Bu kapsamda elektronik ortamda üretilen, saklanan ve iletilen bilgilerin güvenilir olması için güvenlik özelliklerini sağlayacak şekilde saklanması ve iletilmesi gereklidir. Çünkü elektronik ortamdaki servis ve protokollerin sağladığı kolaylıkları yanında;¹⁹⁵ sahtecilik, aldatma, mesaj başlığını içeriğini değiştirme, yeniden oluşturma gibi yöntemler kullanılarak farklı kaynaktan, farklı içerikli mesaj gönderilecek alıcı ve göndericinin yanıltılması mümkün olabilmektedir. Bu nedenle, gerek, elektronik posta servisleri ile gönderilen mesajlar, gerekse, bilgisayarda saklanan belgeler, eğer gerekli güvenlik önlemleri alınmadan saklanıp gönderilmişler ise, güvensiz bilgi kaynaklarıdır. Dolayısıyla bu tür kaynaklara dayanılarak yapılacak suçlamalarda çok dikkatli davranılması ve kanıtın gerçekten suçlanan kişi tarafından üretildiğinin, bilerek ve isteyerek saklandığı ve gönderildiğinin kanıtlanması gerekmektedir. Bilişim sistemlerinin zayıflıkları nedeniyle mesaj kaynağında aldatma, mesaj içeriğinin değiştirilmesi ve bilgi sistemlerine kişinin izni olmadan suç unsuru teşkil edebilecek belgelerin yerleştirilebilmesinin mümkün olabilmesi yanında, bunu gerçekleştirenlerin tespiti de zor olmaktadır. Bir başka konu, kişilerin tedbirsizliğinden kaynaklanan ihlallerdir ki, bilişim sistemi kullanımının yaygınlaştığı günümüzde, her bireyin uzman olması beklenemeyeceği için tedbirsizliği nedeniyle bilgisayarında suç unsuru içeren belgeler bulunan tarafın suçlanması ise tartışılması gereken bir konudur. Bir bildiride elektronik ortamda saklanan ve iletilen belgelerin mesajların oluşturulması ve iletilmesi sırasında olabilecek güvenlik ihlalleri açıklanarak, gerekli olan önlemler alınmadığı durumda güvenilirlikleri ve özellikle hukuki delil olup olmayacaklarının teknik yönleriyle tartışılması amaçlanmıştır. Önerilen önlemler ile gerek bilirkişi olarak görevlendirilen, gerekse raporlara göre karar veren yargı makamlarının konuyu farklı bir bakış açısı ile daha dikkatli olarak değerlendirmelerinin sağlanması hedeflenmiştir.

¹⁹⁴ Yargıtay 4. Ceza Dairesi E. 2004/8763 K. 2005/21445 T. 5.12.2005, “İnternet Yoluyla Hakaret ve Sövme”, <http://www.turkhukuksitesi.com/showthread.php?t=7185>, (26 Haziran 2008).

¹⁹⁵ Marco de Vivo, Gabriella O.De Vivo, Germinal Iserm, “Internet Security Attacks at the Basic Levels”, *Operating Systems Review, ACM Press*, Vol. 32, No 2, April 1998, s.142.

Elektronik belgeler ağ üzerinde iletilmeden önce belirli araçlar ile oluşturularak saklanırlar veya iletilirler. Saklanan ve iletilen belgelerin bu süreç içerisinde bütünlüğünün sağlanması ve kime ait olduğunun bilinmesi önemlidir. Çünkü oluşturulduktan sonra içeriğinin ve sahibinin değiştirilmesine karşı, önlem alınmayan belgelerin oluşturulduğu hali ile saklandığının ispatı zordur. Ayrıca belgelerin veya mesajların kim tarafından oluşturulduğu önemli olmakla birlikte, bunun ispatı için önlem alınmamış ise yine kime ait olduğunun anlaşılması önemli bir problemdir. Bilgi ve belge iletiminde farklı servisler (Dosya transfer protokolü, mesaj servisleri, e-posta vs.) kullanılmaktadır. Bu bölümde, çok yaygın kullanımı nedeniyle ağırlıklı olarak bilgisayar ağ'ı üzerinde e-posta ile bilgi iletimi ve onun zayıflıkları üzerinde durulmuştur.

İnternet üzerinde e-posta nasıl iletilir: Bilgisayar ağ'ı üzerinde elektronik postalar iletilirken TCP/IP protokolü ve onun alt protokollerinden SMTP (Simple Mail Transfer Protocol) kullanılır. TPC/IP protokolü kullanılarak iletilen mesajlarda, mesaj paketi gönderici ve alıcının IP adreslerini içerir. Bu adresler kullanıcı bilgisayarına sabit veya değişken olarak atanırlar ve bilgisayarları İnternet ortamında tanımlamak için kullanılırlar. Normal koşullarda, kullanıcı bilgisayarı iletmek istediği bir mesajın başlık (header) kısmına kendisinin ve mesaj alıcısının IP numaralarını yazması gerekir. Bu işlem mesaj iletimi ve haberleşme için kullanılan yazımlar ile yapılır.



Şekil 27-İnternet üzerinde elektronik posta gönderme-alma işlemi

Şekil 27’de gösterilen İnternet üzerinde elektronik posta gönderme alma işlemi normal koşullarda aşağıdaki gibi yapılır.

Mesaj göndermek isteyen kullanıcıların kullanacakları E-Posta sunumcular üzerinde hesapları ve bu hesaplar için kullanıcı adı ve şifreleri bulunmaktadır.

A kullanıcısı, B kullanıcısına bir e-posta göndermek istediği zaman kendisinin sunumcusuna smtp protokolü ile mesajı gönderir. Eğer sunumcu ile aynı ağda bulunmayan bir bilgisayar kullanırsa, göndereceği posta değişik düğümler üzerinden sunumcuya iletecektir.

Sunucu-A, B'nin hesabının bulunduğu sunumcu ile bağlantı kurup postayı Internet üzerinden smtp protokolü ile iletilir. Bu aşamada mesaj paketi ağ üzerinde çok çeşitli düğümleri dolaşır.

B kullanıcısı postalarını okumak için POP3 protokolünü kullanarak hesabın olduğu Sunumcu-B'ye bağlanır ve posta kutusuna gelen postaları okur.

E-posta iletimindeki zafiyetler: Gerek TCP/IP gerekse smtp protokolünün güvenlik zayıflıkları nedeniyle, normal koşullarda problemsiz olarak iletilebilen mesaj paketleri kötü niyetli internet kullanıcıları (hacker) tarafından değişikliğe uğratılabilir (içerikleri değiştirilebilir) veya farklı göndericiden gelmiş gibi düzenlenebilir.¹⁹⁶ Elektronik mesajlaşma ve bilgi saklamada ne tür ihlaller yapılabilir?: Elektronik ortamda mesaj iletimi ve saklanması yapılırken aşağıdaki güvenlik ihlalleri gerçekleştirilebilir.¹⁹⁷

Mesaj paketinin gönderici bilgileri farklı yazılabilir. (Bu durumda haberi olmadan bir başkası adına posta gönderilebilir). Mesaj içerikleri değiştirilebilir. (Göndericinin mesajı iletim sırasında değiştirilerek farklı içerikte olabilir).¹⁹⁸

Bilgisayara verilen IP numaralarında sahtecilik yapılarak gönderilen mesajların kendi bilgisayarından gönderildiği gizlenebilir veya başkasının bilgisayarından gönderilmiş gibi gösterilebilir (IP Spoofing). Bir başka ifade ile, Mesaj gruplarından veya dağıtım gruplarından giden mesajlarda mesajın farklı IP numarası ile ve veya farklı, istenilen adres ve IP numarası ile gitmesi sağlanabilir.

¹⁹⁶ Nelson E. Hastings, Paul A. Mclean, "TCP/IP spoofing Fundamentals", **Computers and Communications, 1996, Conference Proceedings of the 1996 IEEE Fifteenth Annual International Phoenix Conference on** Scottsdale, AZ, USA, 27-29 Mar 1996, s.127-129.

¹⁹⁷ Marco de Vivo, Gabriella O.De Vivo, Roberto Koenke ve Germinal Iserm, "Internet Vulnerabilities Related to TCP/IP and T/TCP", **Computer Communication Review**, Vol. 29, No. 1, January 1999, s.81-85.

¹⁹⁸ B. Harris, R. Hunt, "TCP/IP Security Threats and Attack Methods", **Computer Communications**, Vol.22, No.10, 25 June 1999,s. 885-897.

Bir veya birkaç bilgisayarın içinden geçirilerek özel yol açma programları kullanılarak bu mesaj bilgisayarın sahibinin haberi olmadan o bilgisayardan gönderiliyormuş gibi gönderilebilir.

Bilgisayarda saklanan belge izinsiz olarak erişim yapan başkası tarafından değiştirilerek yeniden saklanabilir.

İzinsiz olarak erişim ile suç teşkil eden belgeler kopyalanıp saklanabilir.

Yukarıda açıklanan yanıltma işlemlerini yapabilecek hazır yazılım ve gereçler Internet üzerinden herkes tarafından bulunabilir. Örnek olarak da belirtilen Mendax, spoofit, ipspoof, hunt ve addrees changer programları verilebilir.¹⁹⁹ TCP/IP protokolü ve bilgisayar programlama konusunda biraz bilgisi olanlar bu tür yazılım ve gereçleri kullanarak yukarıda açıklanan yanıltmaları yapabilirler. Bu nedenle yahoogroups gibi mesaj gruplarından gelen mesajları sağlayan ana servis sağlayıcı (bilişim şirketi) ile hukuki ve bilimsel ölçeklerde bizzat yazışmadan hangi IP numaralarının ne zaman o siteye bağlandığı, gerçek sahte adresle mi yolladıkları öğrenilemez. He ne kadar mesaj başlığı içerisinde bulunan IP numaraları gönderici ve alıcının bilgisayarının IP numarasını işaret etse bile bu bilgilerin güvenilirliği düşüktür ve belirleyici kanıt olarak kullanılması yanıltıcı olur. Başka bir ifade ile elektronik posta mesajları ve belgeleri yalın hali ile **“imzasız şekilde posta ile gönderilmiş mektup”** olarak da değerlendirilebilir.

8.2. ELEKTRONİK DOKÜMAN SERVİSLERİ VE OLABİLECEK GÜVENLİK İHLALLERİ

Elektronik ortamda saklanan ve iletilen belge ve mesajların gizliliğinin sağlanması, kaynağın doğrulanması ve içeriğinin değişmediğinin (bütünlüğünün) doğrulanması aşağıdaki amaçlar için hayati öneme sahiptir ve gereklidir.

Eğer belge mesaj içeriği, gizli bilgiler taşıyor ise, söz konusu belge mesaj ilgisiz kişilerin eline geçmesi durumunda bilginin gizliliğinin önemi kalmayacaktır.

¹⁹⁹ Kapil Sharma, *IP Spoofing*, <http://forums.thekeyboardcowboys.org/post.php?action=reply&fid=23&tid=24&repquote=74>, (24 Temmuz 2007).

Gönderilen belge mesaj ile alınan içerikleri farklı olursa yanlış anlaşılmalara nedeniyle belge mesaj'ın içerdiği bilgilere dayanılarak hatalı işlemler yapılabilecektir.

Tarafların belge mesaj konusunda itilafı olduğu durumlarda bilgiyi gönderenin tam olarak saptanmaması durumunda yine hatalı karar verilebilecektir.

Bilgisayarda bulunan ve suç unsuru teşkil eden bir belgenin, bilgisayarın sahibi tarafından mı yoksa başkaları tarafından mı üretilip saklandığını ispat etmek çok güçtür. Dolayısıyla ile bu gibi durumlarda tam olarak doğru karar vermek mümkün olmayabilecektir.

TS ISO/IEC 17799, kurumsal bilgi güvenliği standardında e-posta'ların güvenliği için izlenecek politika aşağıdaki hususları kapsamaktadır.²⁰⁰

Elektronik postalara saldırılar. Örneğin, virüsler, çakışmalar,

Elektronik posta eklerinin korunması,

Şirkete yüklenilmeye çalışan sorumluluğu. Örneğin, Şirketi lekeleyen elektronik posta gönderimi, tacizkar kullanım, yetkisiz satın almalar,

Elektronik mesajların bütünlüğü ve gizliliğini korumak için kriptografik tekniklerin kullanımı (Madde 10.3)

Mahkemeye intikal etmesi durumunda ortaya çıkarılan, saklanan mesajların tutulması.

Kimden geldiği doğrulanamayan istihbarat mesajları için ilave kontrol tedbirleri.

Mesaj gizliliğinin sağlanması için kullanılabilecek yöntem şifrelemedir. Bunun için geliştirilen şifreleme yöntemleri kullanılarak gizlilik sağlanır. Mesaj kaynağının doğrulanması ve inkâr edilmeme özellikle elektronik ticaret ve hukuki işlemlerde çok önemlidir. Eğer bir e-posta ile bir başkasına hakaret veya suçlayıcı ifadeler gönderilmiş ise, bu suçu işleyen tam ve doğru olarak tespit edilmesi, aynı zamanda suçlunun

²⁰⁰ TSE, TS ISO/IEC 17799, **Bilgi Teknolojisi-Bilgi güvenliği Yönetimi için Uygulama Prensibi**, 2005.

suçunu inkar edememesinin sağlanması ve hukuki sürecin işletilmesi önemli olmaktadır. Belge ve mesajı oluşturan kaynağın tam ve doğru olarak saptanması için sayısal imza ve kaynak doğrulamaya dayanan değişik yöntemler geliştirilmiştir. Bu yöntemler arasında PEM, PGP, S/MIME v2 önde gelen kriptografik mesaj güvenlik protokolleridir.²⁰¹ Bunlara ilaveten Eliptik eğri kriptosistem tabanlı güvenli e-posta sistemi de önerilmiştir.²⁰² E-posta kaynağını doğrulamak amacıyla E-posta liste servisleri, e-posta adreslerinin kriptografik takma adı (alias) ve doğrulama için ilave bilgi (doğrulama merkezi ve buraya verilecek alan anahtarı gibi kaynak doğrulama bilgileri) kullanımı yanında, Internet üzerinde seyreden paketleri, dolaşımları esnasında işaretleyerek geriye doğru izlemek suretiyle kaynağına ulaşmak (Traceback) diğer kaynak doğrulama yöntemleridir.²⁰³ Sayısal imzalama yönteminde, belgeyi veya iletilecek e-postayı oluşturan gönderici, belgenin öz bilgisini (hash) hesaplayıp ona kendi kimlik bilgisini ve zamanı ekledikten sonra sadece kendisinin bildiği bir anahtar ile bu bilgiyi şifreler ve belgeye ekleyerek saklar veya birlikte gönderir.²⁰⁴ Alıcı taraf göndericinin diğer anahtarını (açık anahtar) kullanarak imzayı çözer ve mesajın gerçekten gönderen kısmında belirtilen kişi tarafından gönderilip gönderilmediğini anlamış olur. Bu amaç için geliştirilen PGP (Pretty Good Privacy) algoritması güvenli e-posta göndermek için kullanıldığı takdirde, e-postayı gönderenin kimliğini saptamak tam ve doğru olarak yapılabilir.²⁰⁵ Gelen mesajların gelirken geçtiği Internet düğümlerinin izlenerek göndericinin IP numarasının saptanması akademik çalışmalar olarak halen devam etmektedir ve henüz pratik kullanımı yoktur. Bu yöntem daha çok servis etkisizleştirme saldırısının (Denial of Service Attacak) kaynağını belirlemek amacıyla kullanılır. Mesaj içeriğinin değiştirilip değiştirilmediğini ise ayrıca incelenmesi gereken bir konudur.²⁰⁶ Saklanan belgelerin kimin tarafından

²⁰¹ Hal Burch, Bill Cheswick, "Racing Anonymous Packets to Their Approximate Source", **proc. Of 2000 LISA** Vol. XIV, Dec 3-8, 2000, s.313-322.

²⁰² W.Lee, J.Lee, "Design and Implementation of Secure e-mail System Using Elliptic Curve Cryptosystem", **Future Generation Computer Systems Vol.20**, 2004, s. 315,326.

²⁰³ P.C. Van Oorschot, "Message authentication by integrity with public corroboration", **New Security Paradigms Workshop Proceedings of the 2005 workshop on New security paradigms**, Lake Arrowhead, California, s.57-63.

²⁰⁴ M.Kawashima, T. Abe, S.Minamoto, T.Nakagawa, "Cryptographic alias e-mail addresses for privacy enforcement in business outsourcing", **Digital Identity Management 2005, DIM Vol.05**, s.46-53.

²⁰⁵ Albert Levi, M.Ufuk Çağlayan, "Elektronik posta Güvenliği için PGP Kullanımı" <http://people.sabanciuniv.edu/levi/blsm97.pdf>, (26 Haziran 2008), s.3-4.

²⁰⁶ Hassan Aljifri, Macel Smets ve Alexander Pons, "IP Traceback Using Header Compression", **Computers&Security**, Vol 22, No 2, 2003, s.136-151.

oluşturulduğunu anlamak için ise sayısal olarak imzalanması gereklidir. Eğer kendisi kabul etmiyor ise, sayısal olarak imzalanmamış olan bir belgeyi kullanarak kişileri suçlamak tartışılacak bir husustur.²⁰⁷ Ancak sayısal olarak imzalanmış ise, belgenin kim tarafından oluşturulduğunun anlaşılması mümkündür. Eğer oluşturulan belge mesaj sayısal imza yönetimi kullanılarak imzalanmış, ise bu belgenin saklama iletim sırasında değişime uğrayıp uğramadığını anlamak tam olarak mümkündür. Böylece içeriğini ve sahibini inkâr edememe tam olarak sağlanmış olur.²⁰⁸ Açıklanan bu yöntemlerin doğruluğu bilimsel olarak da kanıtlanmıştır. Bu nedenle ancak yukarıda açıklandığı şekilde oluşturulan belge ve e-posta mesajları güvenilirdir ve içeriğinin değişip değişmediğini kolaylıkla kanıtlanabilir.

Günümüzde bilişim sistemleri üzerinde belge bilgi üretme, saklama ve iletmeye çok yangın hale gelmiş bulunmaktadır. Birçok bilgi, bu yol kullanılarak iletilmektedir. Ancak saklanan veya iletilen bilginin varış noktasında, üretenin kimliğinin, doğru kaynaktan geldiğinin, içeriğinin değişmediğinin doğrulanması ve gerekli ise gizliliğinin korunması gereklidir. Güvenlik önlemleri alınmadan iletilmiş olan bir e-posta mesajı alınmış ise onun içeriğine ve üzerinde yazan gönderici bilgilerine (e-posta adresi ve IP numarası) tam olarak güvenmek ve belirleyici kanıt olarak kullanmak yukarıda açıklanan nedenlerden dolayı yanıltıcı olabilecektir. Bu durumda insanlar neden bu kadar çok olarak e-posta servisini kullanmaktadırlar diye düşünülebilir! Eğer, mesajlaşma her iki taraf birbirine güveniyor, e-postalar işe gizli bilgi iletmiyorlar ve gönderilen bilgilerin içeriğinin iletim esnasında değiştirildiği durumda bir kayıp söz konusu değil ise bu servisin kullanılması son derece kolaydır. Ancak önemli içeriğe sahip olan ve içeriğinin değiştirilmesi halinde tarafların menfaatine zarar getirebilecek içerikteki bilgiler kullanılmaksızın e-posta servisi ile gönderilmemelidir. Aksi halde anlaşmazlık durumunda, kaynağın ve bütünlüğünün korunduğunun doğrulanması zordur.

Yukarıda açıklanan nedenlerden dolayı; Eğer bir e-posta mesajı veya elektronik belge, gönderen üreten tarafından sayısal olarak imzalanmamış ise imzasız

²⁰⁷ Abraham Year, Adrian Perrig, Dawn Song, "FIT: Fast Internet Traceback", <http://www.ece.cmu.edu/~adrian/projects/fit.pdf>. (26 Haziran 2008) s.1-12.

²⁰⁸ Hal Burch, Bill Cheswick, "Racing Anonymous Packets to Their Approximate Source", **proc. Of 2000 LISA**, Vol.XIV, Dec 3-8 2000, s 313-322.

bir mektup'tan farklı bir özelliği olmayacağı için (gerek içeriği ve gönderici bilgileri, gerekse taşıdığı IP numarası açısından) suçlayıcı veya yaptırım amaçlı bir kanıt olarak kullanılması yanıltıcı olabilecektir. Çünkü sayısal imza yöntemi ile imzalanmamış olan bir belge veya e-posta mesajının kim tarafından üretilip gönderildiğini ve içeriğinin değiştirilip değiştirilmediğini tam olarak anlamak mümkün olmayacağı için bu gibi belge e-postaların kanıt olarak kullanılması hatalı sonuçlar doğurabilecektir. Bu nedenle elektronik ortamda oluşturulan belgelerin sayısal olarak imzalanmasının hukuki ve teknik yönleri ile kullanıma ilişkin esasları 5070 sayılı kanunla düzenlenmiştir. Elektronik ortamda üretilen, saklanan ve iletilen belgelerin kanıt olarak kullanılması durumunda bu bilgilerin içeriğinin ve üreticisinin değiştirilmemiş olduğunun kanıtlanması gerekir. Oysa açıklanan nedenlerden dolayı eğer gerekli önlem alınmamış ise bu bilgiler başkaları tarafından kolaylıkla değiştirilebilir. Neticede bu tür bilgilere dayanılarak yapılan suçlamalarda, hatalı karar verilmesini önlemek amacıyla anılabilecek teknik önlemler aşağıda belirtilmiştir.

Belge üretme yazılımlarına, üretilen belgenin üreticisinin kimliğini tartışmasız olarak doğrulayacak mekanizmaların eklenmesinin sağlanması (Örneğin Sayısal İmza)

Belgelerin içeriğinin değişip değişmediğinin anlaşılması için yönetim sistemi oluşturulması veya mutlak sayısal olarak imzalanmasının sağlanması. Bilgisayar işletim sisteminin imzasız belgeleri denetleyip ayıklamasının veya farklı klasörlerde saklanmasının sağlanmasıdır.

İnternet veya diğer özel ağlarda iletilen tüm mesajların sayısal olarak imzalanmasının sağlanmasıdır. İmzasız mesajların kaynağının tanınması için yöntemler geliştirilmesi (Örneğin Kaynağa Ulaşma)

Bu konularda bilirkişilik yapan yapacakların bilgi güvenliği ve sanal ortam suçları konusunda eğitimi olmasına dikkat edilmeli ve daha duyarlı davranmaları

Yargı makamlarının bilgi güvenliği ve bilişim suçlarına ilişkin kanıtların özellikleri konusunda bilgilendirilmelerinin sağlanması.

Elektronik ortamlarda üretilip iletilen belgeler ve mesajlar üzerinde kolaylıkla istenmeyen değıştirme yanıltmalar yapılabilmektedir. Dolayısıyla, bu bilgilerin güvenliğinin sağlanması durumunda güvenilir olacaklar hataların azaltılması mümkün olabilecektir.

8.3.ELEKTRONİK İMZANIN VE İMZALANMIŞ VERİLERİN DELİL NİTELİĞİ

Bankacılık alanında 1970'lerden itibaren elektronik sistemlere geçilmesi ile, müşteri tarafından herhangi bir belge doldurmaksızın plastik bir kart kullanarak harekete geçirilen elektronik sistemler aracılığıyla bankacılık işlemleri gerçekleştirilmektedir. Bu sistemler, otomatik vezne makineleri (ATM), satış noktalarından otomatik fon transferi, ev ve ofis bankacılığı adı altında bankacılık faaliyetleri göstermektedir. Elektronik imzanın kullanım alanlarında biri, banka hesapları arasında yapılan elektronik ödeme işlemleridir. Elektronik ödeme işlemlerinin iki çeşidi vardır. İlki, bankanın müşterisinin hesabından, aynı bankada veya başka bankada bulunan bir alıcı hesabına para gönderilmesi; ikincisi ise yabancı bir hesaptan, müşteri hesabına para transferidir. Bu işlemlerdeki veriler, ayrı ayrı gösterilir ve para miktarı, hesap numarası, banka kodu, kullanım amacı gibi havale için gerekli bilgileri içermektedir. Bu veriler kural olarak, uygun muhasebe programlarından veya müşterinin bilgisayarında kullanılan yazılım programınca üretilmektedir. Bu süreç, çoğunlukla otomatik olarak başlar ve biter. Banka hesapları arasında yapılan bu ödemelerde kural olarak yetkililerin imzalarının bulunması gerekir. Ancak işlemler elektronik ortamda yapıldıkları zaman, en azından el yazısı ile imzalamaya eşdeğer hukuken bağlayıcılığı sağlayan bir ikameye ihtiyaç vardır.²⁰⁹

Sermaye Piyasası Kanunu²¹⁰, nun 10. maddesinin sermaye piyasası araçları ve bunlara ilişkin kişisel hakların, Merkezi Kayıt Kuruluşu adlı, özel hukuk tüzel kişiliğini haiz bir kuruluş tarafından bilgisayar ortamında kayden izleneceği, kaydedilen hakların senede bağlanmayacağı öngörülmektedir. Kapalı bilgisayar sistemi içinde tutulacak olan kayıtları, sermaye piyasası araçları üzerindeki hak sahipliğine ilişkin bir uyuşmazlık halinde, gerçek sahipliğini öğrenmek üzere kendisine başvurulacak ve bu durum hukuk önünde doğrudan doğruya delil olarak kabul edilecektir. Bu kayıttan yazıcı aracılığıyla alınan çıktı ise dolaylı bir delildir.

²⁰⁹ Mine Erturgut, "Elektornik İmza Kanunu bakımından E-belge ve E-imza", **Bankacılar Dergisi, Türkiye Bankacılar Birliği**, Sayı:48, Mart, 2004, s.68.

²¹⁰ 4487 Sayılı, "Sermaye Piyasası Kanunu", Kabul Tarihi:15.12.1999, Resmi Gazete Sayısı:24622, Resmi Gazete Tarihi: 26.12.2001, Madde:10.

Mevcut hukuk sistemimizde deliller ikiye kategoride ele alınmaktadır. Bunlar kesin delil ve takdirli delillerdir. Kesin deliller olarak *ikrar*; (“Dava evrakında veya hâkim huzurunda iki taraftan birinin veya vekilinin sebkeden ikrarı muteberdir. Ve mukir olan taraf aleyhine delil teşkil eder. Maddi bir hatadan neşet ettiği sabit olmadıkça ikrardan rücu olunamaz. Sulh müzakeresi esnasında sebkeden ikrar muteber değildir. Mahkeme haricindeki ikrarı teyit edecek delail ve emare mevcut ise hâkim buna binaen hüküm verebilir”²¹¹), *kesin hüküm*; (“Kaziyei muhkeme, ancak mevzuunu teşkil eden husus hakkında muteberdir. Kaziyei muhkeme, mevcuttur denilebilmek için iki tarafın ve müddeabihin ve istinat olunan sebebin müttehit olması lazımdır”²¹²), *senet*; (“Kanunun muayyen bir delil ile ispatını emreylediği hususlar başka suretle ispat olunamaz. İki tarafça muayyen deliller ile ispatı tahriren kabul edilmiş olan veya muhakeme esnasında olveçhile beyinlerinde karar verildiği ikrar olunan maddeler hakkında başka delil kabul olunmaz”²¹³) ve yemindir. Takdiri deliller ise şahit, bilirkişi, keşif ve özel hüküm sebepleridir.²¹⁴

Elektronik imza kanununun özündeki düzenleme elektronik belgenin delil vasfının düzenlenmesine yönelik değil; elektronik imzanın düzenlenmesine yöneliktir. Madde 5’in f bendindeki hüküm güvenli elektronik imzaya elle atılan imza ile aynı hukuki sonuç bağlanmıştır. Uyuşmazlık durumlarında mahkeme öncelikli olarak imza sahibine imzanın kendisine ait olup olmadığını sorması gerekmektedir. Buradaki esas imzanın kişi tarafından ret edilmesine göre düzenlenmiştir. Kişi imzanın kendine ait olmadığını iddia ederse, mahkeme heyeti imza inceleme yoluna başvurur ve ıslak imzada görülen usul ve esaslar aynen muhafaza edilerek tetkikat bilirkişi heyetleri marifetiyle gerçekleştirilir.²¹⁵

Ayrıca elektronik imza kanununda tanımlanan güvenli elektronik imza kavramıyla yalnızca güvenli elektronik imzalar delil vasfı sayılır diye bir şey söylememiz doğru değildir. Şekil olarak elektronik imzalı belgelerin tümü delil olarak

²¹¹ 1086 Sayılı, “Hukuk Usulü Muhakemeleri Kanunu”, Kabul Tarihi:18.06.1927, Resmi Gazete Sayısı:622, Resmi Gazete Tarihi: 02.04.1927, Madde:236.

²¹² 1086 Sayılı, “Hukuk Usulü Muhakemeleri Kanunu”, Madde:237.

²¹³ 1086 Sayılı, “Hukuk Usulü Muhakemeleri Kanunu”, Madde:287.

²¹⁴ Seyithan Deliduman, “İspat sistemimizin mevcut durumu ve elektronik imzanın bu sistemdeki yeri”, *e-Akademi Dergisi* (elektronik), Sayı:2, Nisan 2002, <http://www.e-akademi.org>, (31 Mayıs 2007)

²¹⁵ Haluk Konuralp, “Genel Hatlarıyla Elektronik İmza Kanunu”, <http://www.tbb.org.tr/turkce/konferans.htm> (03 Haziran 2007)

sayılır. Fakat kanunda güvenli elektronik imza dışındaki, imzaların hukuki sonuçlarını düzenleyen maddeler yoktur. Dolaylı olarak güvenli olmayan elektronik imzaya da, güvenli imza kadar olmasa bile, bir ölçüde caiz delil vasfı olarak kabul edilir. Hatta hiç imzalanmamış elektronik veriler dahi delil vasfı olarak mahkeme heyetince dikkate alınır.

Elektronik imzaya tanınan bu değer Medeni Usul hukuku bakımından geçerli olup, Hukuk Usulleri Muhakemeleri Kanununun 295. maddesinden sonra gelmek üzere “*güvenli elektronik imza ile oluşturulan elektronik veriler senet hükmündedir. Bu veriler aksi ispat edilmeye kadar kesin delil sayılırlar*” ifadesi eklenmiştir.²¹⁶ Bu noktada eleştirilebilecek bir nokta mahkeme heyetinin takdir yetkisinin sınırlandırılmasına yönelik olabilir. ABD’de birçok eyalet, elektronik imza imzalanmış belgeleri kesin delil olarak kabul etmekte ve bunların ispat kuvvetini de kesin delil olarak sayılan diğer delillerden daha üstün tutmaktadır.²¹⁷ Buradaki amaç şüphesiz ki elektronik imzanın kullanımının yaygınlaşmasını sağlamaktır.

8.4.ELEKTRONİK SERTİFİKA HİZMET SAĞLAYICILARI’NIN SERTİFİKA SAHİBİNE KARŞI SORUMLULUĞU

Elektronik Sertifika Hizmet sağlayıcısı, elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel ya da hukuksal olarak temsil edilen tüzel kişileridir.

Sertifika hizmet sağlayıcısının sertifika sahibine karşı sorumluluğu konusunda, Elektronik İmza Kanunun 13 Maddesinin 1 fıkrasında “*Elektronik sertifika hizmet sağlayıcısının, elektronik sertifika sahibine karşı sorumluluğu genel hükümlere tâbidir*” hükmü getirilmiştir. Bu hüküm uyarınca akdi sorumluluğun ve sorumsuzluk kayıtları dışında akdi sorumluluktan kurtulma imkanlarının burada geçerli olduğundan kuşku duymamak gerekir.²¹⁸ Zira sorumsuzluk kaydı öngörülerek sertifika sahibine karşı sorumluluktan kurtulmak imkanı tanınmamıştır. Ancak bu durum aynı zamanda

²¹⁶ Konuralp.

²¹⁷ Uluslararası Koordinasyon Kurulu, **Hukuk Çalışma Grubu İlerleme ve Sonuç Raporu**, <http://www.tk.gov.tr/eimza/doc/diger/e-imza%20hukuk%20calisma%20grubu%20raporu.pdf> (04 Haziran 2008).

²¹⁸ Hans Christopher Thomale, “Die haftungsregelung nach §11 SigG”, **Multimedia und Recht.- 7, Bd.** 7,2004, s.80.

nedensellik bağının koptuğu hallerde de sertifika hizmet sağlayıcısı sorumluluğu anlamına gelmez.

Elektronik imza sahibi, EİK’da “*elektronik imza oluşturmak amacıyla bir imza oluşturma aracını kullanan gerçek kişidir*” şeklinde tanımlanmıştır.²¹⁹ İmza sahibi mutlaka bir gerçek kişi olmalıdır. İnternet ortamında güvenli bir biçimde (izin verilen) hukuki işlemleri yapmak isteyen gerçek kişilerin, kendilerine bu imkanı sağlayacak yetkili bir elektronik imza sertifika sağlayıcısı ile bir sözleşme akdetmesi gerekmektedir. Bu sözleşme uyarınca sertifika hizmet sağlayıcısının mesuliyeti, kullanıcıya, biri gizli diğeri açık olmak üzere bir çift anahtar (şifre) tahsis etmek ve bunun yönetimi, gizliliğini sağlama, kamuya açık şifreyi kamuya duyuracak rehberi hazırlamaktır.²²⁰

Elektronik imza kanunu taraflar arasındaki ilişkin hukuki niteliğinin boyutlarıyla ilgili olarak kesin bir belirleme yapılmamıştır. Taraflar irade özgürlüğü çerçevesinde kanuni sınırlamalara riayet etmek suretiyle aralarındaki ilişkiyi serbestçe düzenleyebilir. Sertifika sağlayıcısının yükümlülüğü imzayı imal etme ve bunu içeren veri taşıyıcısını iş sahibine devretmekle sona ermemekte, sertifika içerik hizmetleri sertifikanın geçerliliği süresince veya geri alıncaya kadar devam etmektedir.²²¹ Taraflar arasındaki hukuki ilişkinin akdi niteliği, sözleşmelere ait diğer hüküm ve kuramların da uygulama alanı bulmasına imkan vermektedir. Özellikle kusura karşı sorumluluk, kötüye kullanma, ek faiz ödeme gibi hükümler kanunlarla belirtildiği üzere uygulanabilecektir. Taraflar arasındaki sözleşmenin tüketici sayıldığı takdirde Tüketicinin Korunmasını Hakkındaki Kanun Hükümleri de Borçlar Kanunu’na nazaran özel nitelikli olmaları sebebiyle öncelikle uygulanır.²²²

8.5. ESHS’NİN ÜÇÜNCÜ KİŞİLERE KARŞI SORUMLULUĞU

Elektronik imza Kanuna göre sertifika hizmet sağlayıcısının sorumlu tutulduğu üçüncü kişi kavramı; sertifika sahibi olarak sertifika kuruluşu ile antlaşması

²¹⁹ 5070 Sayılı, “Elektronik İmza Kanunu”, Madde: 3/c.

²²⁰ Mustafa Fadıl Yıldırım, “ESHS Hukuki Sorumlulukları”, **Atatürk Üniversitesi, Erzincan Hukuk Fakültesi Dergisi**, Cilt. II , Sayı.-4, 2004, s.21-25.

²²¹ Alexander Rosnagel, “Erneuerung elektronischer Signaturen:Grundfragen der Archivierung elektronischer Dokumente”, **Computer and Recht**, Bd.19- 2003, s.301.

²²² Yıldırım, 2004,s. 270.

bulunmayan herkes bu kanun çerçevesinde üçün kiři olarak adlandırılır. Üçüncü kişilerin zarar gördüklerini iddia etmeleri durumunda karşı taraf mükelleflerin söz konusu zararın sonucu itibariyle kendilerinin hiçbir kusuru olmadığını ispat etmek durumundadır.²²³ İşin teknik boyutu itibariyle belli bir uzmanlık esas olduğundan ve sertifika hizmet sağlayıcıları olaya daha yakın bir olduklarından oluşan zararın boyutlarıyla açıklanma yükümlülüğünün onlara yüklenmesi yerindedir.

Elektronik imza kanununda, sertifika hizmet sağlayıcılarının üçüncü kişilere karşı sorumlu tutulabilmesi ancak “bu kanun ve bu kanuna dayalı olarak çıkarılan yönetmelik hükümlerine aykırı” davranmak suretiyle zarar verilmesine bağlı tutulmuştur. Üçüncü şahısların görebileceği zararlar teferruatlı olarak açıklanmamıştır(“5070 sayılı Elektronik İmza Kanununda sertifika hizmet sağlayıcılarının yükümlölükleri 10. madde ile düzenlenmiştir. Bunlardan birkaçını belirtme gerekirse; (a) hizmetin gerektirdiği nitelikte personel istihdam etmek, (b) nitelikli sertifika verilen kimliğini resmi belgelere dayalı olarak güvenli bir biçimde tespit etmek, (f) sertifikada bulunan imza doğrulama verisine karşılık gelen imza oluşturma verisini başkasına kullandırmaması konusunda, sertifika sahibini yazılı olarak uyarmak ve bilgilendirmek vb.).²²⁴ Hâlbuki benzeri kanunlarda Örneğin Avusturya Elektronik İmza kanununda bu hallerin neler olabileceği teker teker sayılmıştır.

Bu noktada Elektronik sözleşmelerin Alman hukukunda değerlendirilmesi doktrinine baktığımızda tartışılan bir husus olduğu görölmektedir. Kanun önünde üçüncü kişi sayılan ve haksız fiil esaslarına göre uğradığı zararları tanzim ettirebilme, imkânına sahip olan kişinin sertifika sahibi ile sertifika hizmet sağlayıcı arasındaki antlaşmadan yararlanıp yararlanamayacağı, bir diğer ifadeyle uğradığı zararları sorumluluk esaslarına göre tanzim ettiremeyeceğidir.

Sertifika sahibi ile sertifika kuruluşu arasında yapılan sözleşme hakkında, üçüncü kişiler istedikleri takdirde sertifika içeriğine dair bilgi alabilme yetkisine sahiptir. Verilen bilginin yanlış veya kusurlu olması durumundan kaynaklı bir zarar söz

²²³ **Hukuk Sözlüğü**, “Prima Face”; “Bir şeyi veya bir işi, birisi için yaptı diyebilme; bir şeye dayandırma; yükleme”, http://www.hukuki.net/hukuk_sozlugu.asp?pssearch=isnad, (21 Haziran 2008)

²²⁴ 5070 Sayılı, “Elektronik İmza Kanunu”, Madde:10.

konusu ise burada üçüncü şahıs lehine bir sözleşmenin varlığı kabul edilerek, bu zararların sözleşme hukukuna göre tanzimi mümkündür.²²⁵ Ancak bu noktada bazı hukukçular sertifika hizmet sağlama sözleşmesinde de üçüncü bir kişinin istemesi halinde sağlayıcının, sertifika içeriğini bildirme yükümlülüğü üçüncü kişi lehine sözleşme ilişkisinin kabulünü getirecek bir husus değildir iddiasında bulunmaktadır.²²⁶

Üçüncü şahıs ileride doğacak gerçek bir kişi veya kurulacak tüzel kişi ya da bir kişi topluluğu olabilir. Üçüncü kişinin başka bir kişi tarafından belirlenmesi de mümkündür. Burada aranan tek şart, üçüncü kişinin kendisine taahhüt edilen yükümlülüğün objektif olarak belirlenebilir olmasıdır.²²⁷ Bu noktada belirli bir olayın ifası gerçekleşmesi ile sertifika sağlayıcısının bu kişiye sertifika içeriği ile ilgili olarak bilgi verme yükümlülüğü doğmaktadır. Her ne kadar bu noktada üçüncü kişi lehine sözleşmenin kabulü için bir sorun gözükme de, üçüncü kişilere karşı üstlenilen yükümlülüğün ve alacak hakkı niteliğinde olmaması, ilişkiyi, üçüncü kişi lehine olmaktan çıkaracaktır.

Üçüncü kişinin korunmaya layık bir güvenin bulunmadığı durumlarda, yani imzanın muhatabının durumu biliyor veya durumun gereği olarak bilmesi gereken durumlarda ve sertifika hizmet sağlayıcısının sorumlu tutulmayacağıdır. İmza muhatabının durumu bildiği veya bilmesi gerektiği hususlar kanunumuzda açıkça ifade edilmemiş olmakla birlikte, Medeni Kanunun 2. maddesinde öngörülen dürüstlük kuralından hareketle aynı sonuca varmak gerekir. Bununla birlikte bu hususun Alman Elektronik İmza Kanunu'nda açıkça düzenlendiğini kaynaklara dayanarak söyleyebiliriz.

Nitelikli elektronik sertifikaya haklı olarak güvenip bir hukuki ilişkiye giren taraf, bundan bir zarar gördüğünde, sertifika sahibi ile sertifika sağlayıcı arasındaki sözleşmenin üçüncü kişiyi ve bu arada kendisini koruyucu etkili olduğundan bahisle, uğradığı zararları sözleşme temeline dayalı olarak tanzim ettirme imkanına sahip olup olmadığı konusunda bir fikir birliği bulunmamaktadır.

²²⁵ Yıldırım, 2004, s.272.

²²⁶ Baum, Alman hukukunda üçüncü kişi lehine sözleşme görüşünün doktrinde hakim görüş olması, mahkemelerce benzer olaylarda farklı kararlar verilebilmesi ihtimali, ortaya çıkan koruma boşluğunun özel düzenlemelerle giderilmesi gerektiği düşüncesine sevk etmektedir.

²²⁷ Şener Akyol, **Tam Üçüncü Şahıs Yararına Sözleşme**, İstanbul: Vedat Kitapçılık, 2008, s. 100-101.

Alman doktrinde ayrıca, fikir ayrılıkları ve uygulamada benzer konularda farklı kararlar verilebilme olasılığı üçüncü kişiler bakımından bir koruma boşluğu oluşturduğundan, konunun özel olarak düzenlenmesi gereğine işaret edilmekte ve söz konusu koruma boşluğunun doldurulması istenmektedir. Bu istekler olumlu olarak değerlendirilerek üçüncü şahıslarla ilgili hassasiyetler üzerine gidilmiş ve ilgili maddeler eklenmiştir. Türk Elektronik İmza Kanununda da benzer uygulamalar söz konusudur.

9.SONUÇ

Elektronik imzanın 2000’li yıllardan itibaren hayatımıza girişı bazı farklı sektörlerde kullanım kolaylığı sağlaması açısından çok büyük bir öneme haizdir. E-imzanın kullanım alanlarına baktığımızda bankacılık işlemleri, haberleşme ve belge yönetim sistemlerinin başta geldiğini görmekteyiz. Bu tez kapsamında e-imzanın genel manasıyla tanımı yapılmış, haberleşmede nasıl etkin bir role sahip olduğu irdelenmiştir. Tezin asıl kısmını oluşturan konu ise e-imzanın kullanım alanlarında birisi olan belge yönetim kısmıdır. Belge yönetiminde kullanılan ıslak imza geleneksel bir anlayıştan, daha teknolojik bir anlayışa geçerken beraberinde bazı soru işaretlerini beraberinde getireceği ön görülmüş, bu sorunlara ait çözüm önerileri ele alınmaya çalışılmıştır. Bu yeni anlayışta belge yönetimi modelleri üzerinde durulmuştur. Ayrıca teze ismini veren arşivlenmesi elektronik imzanın başka bir boyutudur. Uzun süreli arşivlemede, belgenin delil vasfını ispatlamak için aradan geçen yıllara rağmen belgenin doğrulanabilir olması gerekmektedir. Tez kapsamında bununla ilgili arşiv imzası kısmını bulmak mümkündür.

Kaynakça kısmına bakıldığında web üzerinden erişilen kaynakların bir hayli fazla olduğu görülmektedir. Bu durum konunun güncel bir konu olması ile açıklanabilir. Dünyada yapılan çalışmalar bir literatür taramasına tabi tutulmuş ve tez kapsamı ile örtüşen kaynaklar ele alınmıştır. Konunun bazı detaylarının henüz ortaya çıkmamış olması nedeniyle yayınlanmamış olan kaynakları da tez kapsamında görmek mümkündür.

Tezde edinilen sonuçları incelediğimizde e-imzanın, e-devlete geçişte geniş ölçekli bir araç olduğu görülmektedir. Bilgi toplumu olma yolunda ilerleyen devletler ar-ge çalışmalarına yatırımları toplam gelirlerinin büyük bir kısmını oluşturmaktadır. Sağlıklı bir bilgi toplumu oluşturma temelinde bilgisayar okur yazarlığını ve dolayısı ile bilgisayar sahipliğini arttırmakla mümkündür. Elektronik ekonomide kavramların geleneksel ekonomiye göre daha hızlı değiştiği görülmekte ve e-ekonomi ülkeler için bir gelişim unsuru olarak kabul edilmektedir.

Tez kapsamında değinilen bir başka konu güvenli resmi mesajlaşma altyapısıdır. Mesajlaşma sistemlerinde karşılaşılan sorunlar irdelenmiş, sertifika doğrulama problemine çözüm önerileri getirilmeye çalışılmıştır. Sertifika geçerlilik

kontrolü ve sorunların giderilmesi, geçerlilik analizleri konunun daha iyi kavranabilmesi açısından ele alınmıştır.

Yine tez kapsamında elektronik belge kavramsal olarak ele alınmıştır. E-belge, e-imza arasındaki ilişki, belgeye eklenen metaverilerde elektronik imzanın fonksiyonları vurgulanmıştır. Bilgisayar sistemlerini, yazılımlarını tehdit eden ve kalıcı zararlar veren kötücül ve casus yazılımlar yine elektronik belge ve güvenliği ile birlikte ele alınmıştır. E-imza oluşturma sürecindeki genel güvenlik ölçütlerine tez kapsamında erişmek mümkündür.

Elektronik imzanın çok geniş bir perspektife sahip olmasından hareketle e-imzada format seçimi incelenmeye uygun bulunan konulardan birisi olmuştur. Farklı platform ve yazılımların e-imzanın kullanımına yönelik sağlamış olduğu avantaj ve dezavantajlar incelenmiştir. Ayrıca kullanılan formatların paylaşımda nasıl bir netice vereceği kullanım kolaylığı ve hukuka uygunluğu konularında da teknik bir yaklaşım sergilenmiştir.

Çağdaş yönetim sürecinde e-imza sisteminin rolü ve sağlamış olduğu yönetim prensipleri ayrıntılara girilmeden izah edilmeye çalışılmıştır. Nasıl bir e-imza modeli oluşturulabilir sorusuna cevap aranmıştır. Bu çalışma kapsamında üç modelle sınırlandırılan elektronik imzalı belgelerin yönetilmesi sadece birkaç tanesiyle sınırlandırılmıştır. Kamuda en yaygın kullanılan ya da kullanılabilecek olan modeller ihtiyaçlar ve olanaklar ele alınarak oluşturulmuştur. Çalışmanın bu kısmının teze ismini verdiği görülmektedir.

Uzun dönemli imza doğrulama ihtiyacı ve yaşanabilecek sorunlar üzerinde durulmuştur. Uzun süre saklanan, arşivlenen e-imzalı belgelere elektronik zaman damgası ve güvenli zaman damgası gibi kavramlar genel sonuçları ile ele alınmıştır. Ayrıca burada uzun dönemli e-imza yapıları ve güvenli e-arşivleme işlevleri, arşiv imzası gibi kavramlara rastlamak da mümkündür.

Teze başlarken konulan hedeflerin birçoğuna ulaşılmıştır. Elektronik imza konusu çok kapsamlı bir konu olduğu için bu konuda veya bu konuyla ilintili başka konularda hazırlanacak tezlerin kapsamı ve sınırları en başında belirgin bir şekilde

belirlenmelidir. Elektronik imza; teknik boyutu ile ya da yönetim, bilişim boyutu ile veyahut hukuki boyutu ile almak mümkündür ve edinilen tecrübelerden her birinin bile kendi içerisinde sınırlandırılması gerekmektedir.

Elektronik Belge Paylaşım Hizmeti Spesifikasyonu, taktik sahada sertifika doğrulama, güvenli veri iletimi gibi konular da ayrıca birer çalışma olabilecek ölçektektir.

KAYNAKÇA

Kitaplar

- Akyol, Şener. **Tam Üçüncü Şahıs Yararına Sözleşme**. İstanbul: Vedat Kitapçılık, 2008.
- Altınışik, Ulvi. **Elektronik Sözleşmeler**. İstanbul: Seçkin Yayınevi, 2003.
- Arıkan, Saadet. **Dünyada ve Türkiye’de Elektronik Ticaret Çalışmalarına Hukuki Bir Yaklaşım**. [y.y.]: [yy. y.], Ankara, 1999.
- Budak, Gönül. **İşletme Yönetimi**. İzmir: Barış Yayınları, 2004.
- Bulut , Müge (hızl.). **Dijital İmza Rehberi**. İstanbul: İstanbul Ticaret Odası, 2005.
- Committee on Digital Archiving and the National Archives and Records Administration. **“Building an Electronic Records Archive at the National Archives and Records Administration: Recommendations for a Long-term Strategy”**. National Academies Press: 2005.
- Dönmez, Calalettin. **Regulation of Electronic Signatures and Protection of Private Keys**. Sheffield: University of Sheffield Department of Law, 2002.
- Drucker, Peter F., Peter M. Senge. **Leading in a time of change**. Jossey-Bass : San Francisco, 2001.
- Gates,Bill. **Dijital Sinir Sistemiyle Düşünce hızında çalışmak**. Ali Cevat Akkoyunlu (çev.). İstanbul :Doğan Kitap,1999.
- Headrick, Daniel R. **Enformasyon Çağı, Akıl ve Devrim Çağında Bilgi Teknolojileri 1700-1850**. Z. Kılıç (çev.). İstanbul: Kitap Yayınevi, 2002.
- Kandur, Hamza. **Elektronik Belge Yönetimi Referans Kriterleri Modeli v.2.0**. 2.Basım. Ankara: T.C. Başbakanlık Devlet Arşivleri Genel Müdürlüğü, 2006.
- Karluk, Rıdvan. **Küreselleşen Dünyada Uluslararası Ekonomik Kuruluşlar ve Entegrasyonlar**. Eskişehir : [yayl.y.], 1995.
- Kavakoğlu, İbrahim. **Değişim ve Yaratıcılık**. İstanbul: Kampus A.Ş. Yayınları, 2000.
- Koçel, Tamer. **İşletme Yöneticiliği**. İstanbul: Beta Yayın, 2003.
- Orta, Mesut. **Elektronik İmza ve Uygulaması**. İstanbul: Seçkin Kitabevi, 2005.
- Sağiroğlu, Şeref, Mustafa Alkan. **“Her yönüyle E-imza”**.Ankara: Grafiker Yayınları, 2005.

Senge, Peter M. **Beşinci Disiplin: öğrenen organizasyon düşüncüsü ve uygulaması.** Ayşegül İldeniz, Ahmet Doğukan (çev.). 2. Baskı. İstanbul: Yapı Kredi Yayınları, 1993.

Tekinay, Selahattin Sulhi, ve diğerleri. **Borçlar Hukuku Genel Hükümler.** İstanbul: [y.y.], 1993.

Thurow, Lester C. **The age of economic exploration.** San Jose: To Excel, 1999.

Makaleler ve Süreli Yayınlar

- Aljifri, Hassan, Macel Smets ve Alexander Pons. "IP Traceback Using Header Compression". **Computers&Security**. Vol 22, No 2, 2003. s.136-151.
- Alkan, Mustafa. "Türkiye Elektronik İmza Kullanımına Hazır Mı?". **Telekom Dünyası Dergisi**. Şubat 2004. s.8-18.
- Anbar ,A. "Veri Transferi ve iletim güvenliğinin sağlanmasında kullanılan filtreleme yöntemleri ve sayısal imza". **İş Güç Endüstri Dergisi**. No:6/2, 2004. s. 11.
- Atatürk Üniversitesi Hukuk Fakültesi Dergisi. "Tüketicinin Korunması Hakkında Kanunun 16-17 ve Medeni Kanunun 24-25. maddeleri". c.5. s.1-4.
- Bayer, Dave, Stuart Haber,W. Scott Stornetta. "Improving the efficiency and reliability of digital time-stamping". **Methods in Communication, Security, and Computer Science – Sequences '91**, s.329-334..
- Boyacı, Hamdi. "Kamu Kurumları için uygulanabilir E-imza Modelleri". **Özelleştirme İdaresi Başkanlığı**, Aralık, 2005.
- Burch, Hal, Bill Cheswick. "Racing Anonymous Packets to Their Approximate Source". **proc. Of 2000 LISA**, Vol.XIV, Dec 3-8 2000. s 313-322.
- Deliduman, Seyithan. "İspat sistemimizin mevcut durumu ve elektronik imzanın bu sistemdeki yeri". **e-Akademi Dergisi (elektronik)**. Sayı:2, Nisan 2002. <http://www.e-akademi.org>, (31 Mayıs 2007)
- Elison , Carl, Bruce Schneier. "The Risk of PKI: What You're Not Being Told About Puplic Key Inrrastructure".**Computer Security Journal**. Vol:16, No:1, 2000. s.1-7.
- Ergün, Ömer. "5070 sayılı Elektronik İmza Kanunu ve Dijital İmza". **Türkiye Noterler Birliği Hukuk Dergisi**. Sayı:122, 15 Mayıs 2004. s.64.
- Erturgut, Mine. "Elektornik İmza Kanunu bakımından E-belge ve E-imza". **Bankacılar Dergisi**. Türkiye Bankacılar Birliği, Sayı:48, Mart, 2004. s.68.
- Erzincan, Özgür Deniz. "E-imza Deneyimi". **Telekom Dünyası Dergisi**. Temmuz 2004. s.32.
- Gül, Hasan. "Kamu Kuruluşlarında Elektronik Hizmetlerin Yaygınlaştırılması (E-Devlet)". **Maliye Dergisi**. Sayı :140, 2002. s.15-46.
- Haber, Stuart, W.Scott Stornetta. "How to time-stamp a digital document". **Journal of Cryptology**. No.3(2), 1991. s.99-111.

- Haris, B., R. Hunt, "TCP/IP Security Threats and Attack Methods". **Computer Communications**. Vol.22, No.10, 25 June 1999. s. 885-897.
- Karayalçın, Yaşar. "Türk Hukukunda Şeref ve Haysiyetin Korunması". **Ankara Üniversitesi Hukuk Fakültesi Dergisi**. CXIX, n.1-4, 1962, s. 251-253,274.
- Kawashima, M., T. Abe, S.Minamoto, T.Nakagawa, "Cryptographic alias e-mail addresses for privacy enforcement in business outsourcing". **Digital Identity Management**. DIM Vol.05, 2005.s.46-53.
- Keser Berber, Leyla. "Elektronik değil dijital İmza Yasası". **e-Devlet BT Haber**, No:4, Mart 2004. s.18.
- Keser Berber, Leyla. "İmzalıyorum O Halde Varım- Dijital İmza Hakkındaki Yasal Düzenlemeler, Dijital İmzalı Belgelerin Hukuki Değeri". **Türkiye Barolar Birliği Dergisi**. Ankara, Sayı: 2, Y.13., 2000. s. 503.
- Keser Berber, Leyla. "İmzalıyorum O Halde Varım". **Türkiye Barolar Birliği Dergisi**. Sayı:2, 2000, s. 131.
- Keser Berber, Leyla. "Şekil ve Dijital İmza". **Elektronikteki Gelişmeler ve Hukuk**. Ankara, 2001. s. 503-556.
- Lee, W., J.Lee. "Design and Implementation of Secure e-mail System Using Elliptic Curve Cryptosystem". **Future Generation Computer Systems**, Vol.20, 2004. s. 315,326.
- Orta, Mesut, " Türkiye’de elektronik imza uygulaması. **Konya Barosu Dergisi**. Vol:3, Sayı: 5, Temmuz 2006. s. 63.
- Özel, Yener "Vergilerin elektronik ortamda ödenmesinde Amerika Birleşik Devletleri Uygulaması". **Yaklaşım Dergisi**. Sayı: 107, 2001. s.122-124.
- Rossnagel, Alexander. "Erneuerung elektronischer Signaturen:Grundfragen der Archivierung elektronischer Dokumente". **Computer and Recht**. Bd.19- 2003, s.301.
- Sağiroğlu, Şeref, Gürol Canberk. "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme". **Gazi Üniversitesi Politeknik Dergisi**. Cilt.9, Sayı.3, 2006.s.165-174.
- Sağiroğlu, Şeref, Gürol Canberk. "Bilgisayar Sistemlerine Yapılan Saldırıları ve Türleri: Bir inceleme". **Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi**. Cilt.23, No.1-2, 2007, s.1-12.
- Sağiroğlu, Şeref, Gürol Canberk. "Kötücül ve Casus Yazılımlar: Kapsamlı bir Araştırma". **Gazi Üniversitesi Müh. Mim. Fak. Dergisi**. Cilt.22, No.1, 2007. s.121-136.

- Sağıroğlu, Şeref, Gürol Canberk. “Şifre Bilimi Tarihine Genel Bakış I-II”. **Telekom Dünyası Dergisi**. Haziran 2005. s.36-44.
- Soysal, A. “Öğrenen Organizasyon Olabilmek”. **Standart**. Yıl.42, Sayı.504, 2003. s.65-73.
- Spalka ,Adrian, Armin B. Cremers, Hanno Langweg. “Trojan Horse Attacks on Software For Electronic Signature”. **Informatica**. Vol.26, 2002. s. 191-203.
- Stuart Haber ve Henry Massias “Time-stamping”, Encyclopedia of Cryptography and Security. Springer,2005, s.12.
- Şenocak, Zarife. “İnternette Kurulan Açık Arttırma ile Satım Sözleşmesi”. **Ankara Üniversitesi Hukuk Fakültesi Dergisi**. C.50, Sayı:3, 2001. s.112.
- Thomale, Hans Cristopher. “Die haftungsregelung nach §11 SigG”. **Multimedia und Recht**.- 7, Bd. 7,2004. s.80.
- Topaloğlu , Mustafa. “Dijital İmza”. **PC-Life**. Şubat, 2001. s.122
- Uluğ, İlknur.“Sanal Sigortacılık”. **Sosyal bilimler Araştırma Dergisi**. Yıl:1, Sayı:2, Eylül 2003. s. 230.
- Vivo , Marco de, Gabriella O.De Vivo, Roberto Koeneke ve Germinal Iserm, “Internet Vulnerabilities Related to TCP/IP and T/TCP”. **Computer Communication Review**, Vol. 29, No. 1, January 1999. s.81-85.
- Vivo, Marco de, Gabriella O.De Vivo, Germinal Iserm. “Internet Security Attacks at the Basic Levels”. **Operating Systems Review**, ACM Press, Vol. 32, No 2, April 1998. s.142.
- Winn, Jane K. çev. Hayri Bozgeyik, Hüseyin Altay. “Bagajsız Kuryeler: Kıymetli Evrak ve Dijital İmzalar, E-Akademi Hukuk”. **Ekonomi ve Siyasal Bilimler Aylık İnternet Dergisi**. Sayı:17, Temmuz, 2003. <http://www.e-akademi.org>. (24 Haziran 2007)
- Yargıtay Dergisi. “İnternet Üzerinde yapılan hukuki işlemler”. c.27, 2001. s. (749-788), 760-761.
- Yatlı, Billur. “E-imza ve E-Belge: Kâğıtsız ve mürekkepsiz Dünyada Hukuk-I”.**Vergi Sorunları Dergisi**. Sayı.151, Nisan, 2001. s. 131.
- Yıldırım, Mustafa Fadıl. “ESHS Hukuki Sorumlulukları”. **Atatürk Üniversitesi, Erzincan Hukuk Fakültesi Dergisi**. Cilt. II , Sayı.-4, 2004, s.21-25.

İnernet Üzerinden erişilen Kaynaklar

“Elektronik Belge Yönetim Standartları Referans Kriterleri Artık Bir Standart!”,
<http://www.devletarsivleri.gov.tr/source.cms4/index.asp?wapp=haberdetaytr&did=E6340703-CEB0-4B0D-A44F-63C8E0F461F8>, (30 Haziran 2008).

Adams, C., P. Cain, D. Pinkas, R. Zuccherato. “Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), August 2001, Request for Comments: 3161”. <http://www.ietf.org/rfc/rfc3161.txt> , s.5-26.

B. Ramsdell (Ed.). “S/MIME Version 3 Certificate Handling”, 1999.
<http://rfc.net/rfc2632.html>, (13 Haziran 2007) s.1-12.

B. Ramsdell (Ed.). “S/MIME Version 3 Messages specification”. Network Working Group, Internet Engineering Task Force (IETF). <http://rfc.net/rfc2633.txt>, (17 Haziran 2007) s.1-32.

Bartel, Mark. John Boyer, Barb Fox, Brian LaMacchia, Ed Simon. “XML Signature Syntax and Processing (Second Edition)”. **W3C Proposed Edited Recommendation 26 March 2008**. <http://nelson.w3.org/TR/2008/PER-xmlsig-core-20080326/>. (21 Mart 2008).

Başçı, Gülen Çelebi. “Sertifika Geçerlilik Kontrolündeki Sorunların Giderilmesi”,
www.tubitak.gov.tr . (02 Temmuz 2008).

Beckett, “Dave. Resource description framework (RDF)”, 1999. <http://www.w3.org/RDF/> (26 Haziran 2008).

Cruellas, Juan Carlos, Gregor Karlinger, Denis Pinkas, John Ross. “XML Advanced Electronic Signatures (XAdES)”, 2003. <http://www.w3.org/TR/XAdES/> (15 Nisan 2008).

Çanga, Tarık Mete. “Elektronik İmza ve Elektronik İmza Yasa Çalışmaları”.
www.etkk.gov.tr/hukuk.htm, (7 Kasım 2006).

Data Communication Networks. <http://ocw.mit.edu/OcwWeb/Electrical-Engineering-and-Computer-Science/6-263JData-Communication-NetworksFall2002/CourseHome/> (13 Haziran 2007)

Elektronik Belge Yönetim Standartları Referans Kriterleri Artık Bir Standart!, <http://www.devletarsivleri.gov.tr/source.cms4/index.asp?wapp=haberdetaytr&did=E6340703-CEB0-4B0D-A44F-63C8E0F461F8>. (30 Haziran 2008).

Elektronik İmza. <http://www.etkk.gov.tr/hukuk.htm>. (11 Mayıs 2006)

Elektronik Ticaret Terimleri Sözlüğü. “Zaman Damgası”. <http://www.hukukrehberi.net/eticaret/eticsozluk.asp> (26 Aralık 2004)

Ersin Gülaçtı (hızl.), “Açık Anahtar Altyapısı”, <http://www.kamusm.gov.tr/tr/Bilgideposu/Belgeler/teknik/aaa/index.html> (19 Temmuz 2007), s.17.

ETSI TS 101 733 V1.5.1 (2003-7 12). “Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats”, http://portal.etsi.org/docbox/EC_Files/EC_Files/ts_101733v010400p.pdf, (30 Nisan 2007) s.50.

European Committee For Standardization, Security requirements for signature creation applications, May 2004. Supersedes CWA 14170:2001. <ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14170-00-2004-May.pdf>, (25 Haziran 2008) s.11.

File Hasher (exe). <http://downloads.zdnet.com/abstract.aspx?docid=357921>. (22 Şubat 2008)

Ford, M. “Identity Authentrication and E-Commerce”. **The Journal of Information, Law and Technology (JILT)**. <http://www.elj.warwick.ac.uk/jilt/98-3/ford.html>. (21 Mart 2007)

Friend, R. “Transport Layer Security (TLS) Protocol Compression Using Lempel-Ziv-Stac LZS, Network Working Group Request for Comments: 3943”. **Category: Informational**. <http://tools.ietf.org/rfc/rfc3943.txt>, s.2,6,8-9.

Froomkin, A. Michael. "The Essential Role of Trusted Third Parties in Electronic Commerce". <http://scholar.google.com.tr/scholar?hl=tr&lr=&q=info:b3aarzFN5AwJ:scholar.google.com/&output=viewport> (07 Aralık 2007) s.49.

Gibbs ,Ross, Justine Heazlewood (hızl.). "Electronic Records – Problem Solved?: the Victorian Electronic Records Strategy and the future of electronic record keeping in Victoria". http://www.vala.org.au/vala2000/2000pdf/Gib_Hea.PDF. (30 Haziran 2008).

Greenwood, Daniel. "Electronic Signatures and Records: Legal, Policy and Technical Considerations". www.state.ma.us/itd/legal/article9.doc. (21 Aralık 2007)

Gülaçtı, Ersin. "Elektronik İmza ve Güvenlik". <http://www.kamusm.gov.tr/tr/Kurumsal/Haberler/Bilgi%20Teknolojileri%20Guvenciligi%20Eimza.pdf>, (30 Haziran 2008)

Housley, R., W. Polk, W. Ford, D. Solo. "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation list (CRL) Profile". <http://www.ieft.org/rfc/rfc3280.txt>, (13 Nisan 2007)

Kaplan, Ahmet, Mustafa Canlı, Yasin Kahramaner (hızl.). "Kurumlararası Elektronik Belge Paylaşım Hizmeti Spesifikasyonu v.1.". <http://www.devletarsivleri.gov.tr>. (29 Şubat 2008)

Keizer, Gregg. "Kama Sutra Spoofs Digital Certificates". <http://www.informationweek.com/news/windows/security/showArticle.jhtml?articleID=177103418>.(21 Mayıs 2008).

Keser Berber, Leyla."Elektronik İmzanın Düzenlenmesi Hakkında Kanun Tasarısı Hükümlerinin Değerlendirilmesi"
http://www.hukukcu.com/bilimsel/kitaplar/e_imza_tasariiestiri.htm, (25 Ekim 2006)

Keser Berber, Leyla. "E-imza ile ilgili Söyleşi". <http://www.e-imza.gen.tr/index.php?Page=Soyleysi&Soyleysi No=20>. (08 Aralık 2007).

- Kılıçlı, Tolga. “Üniversitelerde Akıllı Kart destekli PKI uygulaması ve E-kimlik”. inet-tr.org.tr/ inetconf7/bildiriler/8.doc. (17 Ocak 2008). s.1.
- Konuralp, Haluk. “Genel Hatlarıyla Elektronik İmza Kanunu”. <http://www.tbb.org.tr/turkce/konferans.htm>. (03 Haziran 2007)
- Kurumlararası Elektronik Belge Paylaşım Spesifikasyonu*. <http://www.devletarsivleri.gov.tr/source.cms4/index.asp?wapp=anasayfa>. (30 Haziran 2008)
- Küçüközyiğit, Galip H. “Elektronik Ticaret, Elektronik İmza ve Hukuk”, [www.ceterisparibus.net /arsiv/g/kucukozyigit2.doc](http://www.ceterisparibus.net/arsiv/g/kucukozyigit2.doc) (13 Haziran 2007)
- Levi, Albert, M.Ufuk Çağlayan. “Elektronik posta Güvenliği için PGP Kullanımı”. <http://people.sabanciuniv.edu/levi/blsm97.pdf>. (26 Haziran 2008), s.3-4.
- Levi, Albert, Mahmut Özcan. “Açık Anahtar Tabanlı Şifreleme Neden Zordur”, <http://people.sabanciuniv.edu/levi/bilisim02.pdf> . (24 Haziran 2005), s.1.
- Lupton, W. E., “The Digital Signature: Your Identity by the Numbers”. <http://www.richmond.edu/jolt/v6i2/note2.html> (12 Kasım 2006).
- Menna, Marianne. “From Jamestown to the Silicon Valley Pioneering A Lawless Frontier: The Electronic Signatures in Global and National Commerce Act” <http://www.vjolt.net/vol6/issue2/v6i2-a12-Menna.html> (9 Haziran 2008).
- Myers, M., R.Ankney, A. Malpani ve Diğerleri. “X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol-OCSP”. <http://www.ieft.org/rfc/rfc2560.txt>, (17 Mayıs 2007).
- Önel, Dinçer. “Açık Anahtar Altyapısı (AAA) Sistemindeki Sertifikasyon Problemleri ve Diğer Güvenlik Sorunları”. **Gebze İleri Teknoloji Enstitüsü Mühendislik Fakültesi, Gebze, Kocaeli**. <http://www.bilmuh.gyte.edu.tr/-ispinar/BIL571/acik-anahtar.pdf> (03 Şubat 2005), s.4.
- Özgül, Mehmet Emin. “İnternette Hukuki Güvenlik ve Dijital İmza”. <http://inet-tr.org.tr/inetconf8/program/141.html>. (05 Kasım 2007)

P. Hoffman (Ed.).” Enhanced Security Services for S/MIME”. **Network Working Group, Internet Engineering Task Force (IETF)**. <http://rfc.net/rfc2634.txt>. (17 Haziran 2007). s.42,54,58.

Pinkas, D., N. Pope, J. Ross. “CMS Advanced Electronic Signatures (CADES) 2008”. <http://tools.ietf.org/html/rfc5126>. (12 Haziran 2008) s.30-34.

Prepared By: ESIGN Workshop - Expert Group F Prepared For: CEN/ISSS 25 July 2001. “Protection Profile — Secure Signature-Creation Device Type 3 Version: 1.05, EAL 4+”. <http://www.bsi.bund.de/zertifiz/zert/reporte/PP0006b.pdf>. (30 Haziran 2008) s.21-32.

Sayısal İmza. www.turkpoint.com/e-yasam/sayisal_imza.asp. (01 Aralık 2006).

Sharma, Kapil. “IP Spoofing” <http://forums.thekeyboardcowboys.org/post.php?action=reply&fid=23&tid=24&repquote=74>. (24 Temmuz 2007).

Smedinghoff, Thomas. “Moving with Change”, <http://www.bakernet.com/ecommerce/moveart.doc>. (27 Aralık 2007).

SMTP Service Extension for Secure SMTP over TLS. <http://www.ietf.org/rfc/>, (25 Haziran 2008)

Spyrelli, Christina. “Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach Towards Electronic Authentication”. **The Journal of Information, Law and Technology (JILT)**, Issue:2, 16 August 2002. <http://elj.warwick.ac.uk/jilt/02-2/spyrelli.html> (20 Aralık 2007), s.18.

STANAG, 4406 Annex E: Tactical MMHS Protocol and Profile Solution, Version 2. <http://www.isode.com/solutions/military-messaging.html>. (13 Haziran 2007).

Taft, E., J. Pravetz, S. Zilles, L. Masinter. “RFC 3778 The application/pdf Media Type, Network Working Group Request for Comments: 3778”. <http://www.faqs.org/rfcs/rfc3778.html>, (25 Haziran 2008).

TÜBİTAK, “Açık anahtarlı Altyapı Belge taslakları 2002. <http://www.tubitak.gov.tr> , (17 Haziran 2007)

Uluslararası Koordinasyon Kurulu. Hukuk Çalışma Grubu İlerleme ve Sonuç Raporu. <http://www.tk.gov.tr/eimza/doc/diger/e-imza%20hukuk%20calisma%20grubu%20raporu.pdf> (04 Haziran 2008).

Yargıtay 4. Ceza Dairesi E. 2004/8763 K. 2005/21445 T. 5.12.2005. “İnternet Yoluyla Hakaret ve Sövme”. <http://www.turkhukuksitesi.com/showthread.php?t=7185>, (26 Haziran 2008).

Year, Abraham, Adrian Perrig, Dawn Song. “FIT: Fast Internet Traceback”. <http://www.ece.cmu.edu/~adrian/projects/fit.pdf>. (26 Haziran 2008) s.1-12.

Yeşil, Sezen, Mustafa Alkan, Tayfun Acarer. “Yabancı Elektronik Sertifikaların Kullanımı”.<http://www.ueimzas.gazi.edu.tr/pdf/bildiri/58.pdf>. (25 Haziran 2008) s.1-7.

Yükseliyor, Turhan. “AAA Sayısal Sertifika Karmaşası”. www.e-imza.gen.tr/index.php?Page=Makaleler&MakaleNo=9 (24 Haziran 2008) s.1-4.

Diğer Kaynaklar

Kanun, Yönetmelik ve Tebliğler

Elektronik Ticaret Koordinasyon Kurulu (ETKK) Hukuk Alt Çalışma Grubu. **Elektronik Veri, Elektronik Sözleşme Ve Elektronik İmza Kanunu Tasarısı Taslağı**, 2002.

Telekomünikasyon Kurumu. **Elektronik İmza ile ilgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ**, 6 Ocak 2005.

4487 Sayılı. **Sermaye Piyasası Kanunu**. Kabul Tarihi:15.12.1999, Resmi Gazete Sayısı:24622, Resmi Gazete Tarihi: 26.12.2001.

5070 Sayılı. **Elektronik İmza Kanunu**. Kabul Tarihi:15.01.2004, Resmi Gazete Sayısı:25355, Resmi Gazete Tarihi:23.01.2004.

4982 Sayılı. **Bilgi Edinme Hakkı Kanunu**. Kabul Tarihi:09.10.2004, Resmi Gazete Sayısı:25269, Resmi Gazete Tarihi: 24/10/2003.

1086 Sayılı. **Hukuk Usulü Muhakemeleri Kanunu**. Kabul Tarihi:18.06.1927, Resmi Gazete Sayısı:622, Resmi Gazete Tarihi: 02.04.1927.

Sempozyum, Kongre ve Şuralar

Akçayol Mehmet Ali, H. Erol. “Türkiye’de Elektronik İmza Uygulamalarında Durum Analizi ve Öneriler”. **1.Ulusal E-imza Sempozyumu**. [y.y.]:[yayl. y.], 7-8 Aralık 2006.

Altın, Esin. “Türkiye’de Elektronik İmza ve Elektronik Devlet Uygulamaları: Elektronik Belge Yönetimi Açısından Bir Değerlendirme Denemesi”. **Değişen Dünyada Bilgi Yönetimi Sempozyumu**. [y.y.] :[yayl. y.], 24-26 Ekim, Ankara, 2007,

Çizmeli, Elçin (edt.). “Türkiye’de Bilişim Sektörünün Mevcut Durumu”. **Bilgi Toplumuna Doğru, Türkiye Bilişim Şurası**. Ankara: Başbakanlık, 10-12 Mayıs, ODTÜ, 2002.

Erkan, H. “Bilgi Toplumu”. **Bilgi Teknolojileri Kongresi – IV. Akademik Bilişim Şurası**. [y.y.]:[yayl. y.], 9-11 Şubat Ankara, 2006.

Gözalan, Mustafa. “Bilgi Yönetimi”. **Bilgi Teknolojilerinin Toplam Kalitede Organizasyon yapısındaki yeri ve Önemi Semineri**. İstanbul: KALDER, 3 Aralık 1996.

Hastings, Nelson E., Paul A. Mclean. “TCP/IP spoofing Fundamentals”. **Computers and Communications, 1996, Conference Proceedings of the 1996 IEEE Fifteenth Annual International Phoenix Conference on** Scottsdale. AZ: USA, 27-29 Mar 1996.

- Maniatis, Petros, Mary Baker. “Enabling the archival storage of signed documents”. **FAST '02: Proceedings of the 1st USENIX Conference on File and Storage Technologies**. Monterey, CA , 2002.
- Miccoli Mario. Nadi Günel (çev.).“Teknolojik Açıdan Elektronik Ticaret”. **Noterlik Hukuku Sempozyumu:VII, Elektronikteki Gelişmeler ve Hukuk**. [y.y.]:[yayl. y.], Ankara, 2001.
- Oorschot, P.C. Van. “Message authentication by integrity with puplic corroboration”. **New Security Paradigms Workshop Proceedings of the 2005 workshop on New security paradigms**. Lake Arrowhead: California.
- Özer, Faruk Günay. “Sermaye Piyasalarında Elektronik İmzanın Kullanım Alanları”. **Bilgi İşlem Merkezi Yöneticileri Semineri (BİMY)**. [y.y.]:[yayl. y.], 8-11 Nisan, Aksu-Antalya, 2004.
- Sevim, Tuğrul. “Elektronik İmzanın Hukuksal Boyutları Mevcut Durum, Eksiklikler ve Çözüm önerileri”. **II. Türkiye Bilişim Şurası**. Ankara: Başbakanlık,10-11 Mayıs, 2004.
- Şaşıoğlu, B. “Güvenli Kurumsal Mesajlaşma Uygulaması”, **Ulusal Elektronik İmza Sempozyumu**. Ankara, 7-8 Aralık, 2006.
- Üzel, Gökçe (edt.). “Kişisel Verilerin Korunması”. **Bilgi Toplumuna Doğru, Türkiye Bilişim Şurası**. Ankara: Başbakanlık, 10-12 Mayıs ODTÜ, 2002.
- Üzel, Gökçe (edt.). “Sayısal İmza ve Yasal Düzenleme Yaklaşımları”. **Bilgi Toplumuna Doğru, Türkiye Bilişim Şurası**. Ankara: Başbakanlık, 10-12 ODTÜ Mayıs 2002.

Tezler

- Canberk, Gürol. “Klavye Dinleme ve Önleme Sistemleri Analiz, Tasarım ve Geliştirme”,**Yüksek Lisan Tezi**. Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Eylül 2005.
- Çifti, Çağlar. Legal Aspects Of Ict Implementation In Turkish Construction Industry; “Applicability Of Elegal Framework”, **Thesis Submitted To The Graduate . School Of Natural And Applied Sciences Of Middle East Technical University**, 2005.
- İnalöz, Ayşe. “Telekomünikasyon Regülasyonları Çerçevesinde Elektronik Ticaretin İncelenmesi”, **Yayınlanmamış Uzmanlık Tezi**. Ankara, 2003.
- Roos, Melis. “Integrating time-stamping and notarization”, **Master’s Thesis**. Tartu University. <http://home.cyber.ee/mroos/thesis/> , s. 11.

Yalçinkaya, Bahattin. “Cryptology and Archives an Evalution”, **The Graduation Thesis of Lisence**. Marmara Üniversitesi, Fen-Edebiyat Fakültesi, Bilgi ve Belge Yönetimi Bölümü, 2005.

Raporlar

“Digital Signature Report”. www.un.org.at/uncitral/english/workinggroups/wg_ec/wp-88e.pdf (11 Mart 2007)

Telekomünikasyon Kurumu, “E-İmza Ulusal Koordinasyon Kurulu (UKK)”, **Bilgi Güvenliği ve Standartlar Çalışma Grubu İlerleme Raporu**. http://www.tk.gov.tr/eimza/doc/diger/eimza_bgs_taslak_raporuV1.2.pdf. (18 Aralık 2007).

Sözlükler

Hukuk Sözlüğü. “Prima Face”;
“http://www.hukuki.net/hukuk_sozlugu.asp?psearch=isnad, (21 Haziran 2008)

Türk Dil Kurumu Genel Türkçe Sözlüğü. “Belge”. <http://www.tdk.org.tr/sozluk>, (23 Ağustos 2007)

Standartlar

ISO 19005-1. **Document management – Electronic document file format for long – term preservation – Part 1: Use of PDF 1.4 (PDF/A-1)**. International Organization for Standardization, http://www.iso.org/iso/catalogue_detail?csnumber=38920 (22 Haziran 2007).

TSE, TS ISO/IEC 17799. **Bilgi Teknolojisi-Bilgi güvenliği Yönetimi için Uygulama Prensipleri**, Türk Standartları Enstitüsü, Ankara, 2005.

ÖZGEÇMİŞ

Bahattin Yalçınkaya

24 Ağustos 1980 Gebze'nin Diliskelesi mevkiinde dünyaya geldim. İlköğretimime yine aynı mevkide Diliskelesi İlkokulunda başladım, Bayramoğlu 500 Evler Halide Edip İlkokulundan 1991 yılında mezun oldum. Ortaokul ve liseye Gebze'de devam ettim.2000 yılında Marmara Üniversitesi, Fen-Edebiyat Fakültesi Arşivcilik bölümüne girdim. 2005 yılında mezun oldum. Aynı sene aynı bölümde yüksek lisansa kabul edildim.

Üniversite yıllarımda, gösteri sanatları ile ilgilendim. Yirminin üstünde oyunda rol aldım. Bunun yanı sıra birkaç oyun yazma konusunda tecrübelerim oldu. Yine bu yıllarda MÜ TiyatroM Kulübünde yöneticilik yaptım.

Üniversite stajlarımı biri özel bankada, biri de Galatasaray Lisesi'nde tamamladım. Bir dönem Suna-İnan Kırâç Vakfı, İstanbul Araştırma Merkezi'nde çalıştım. 2006 yılının sonunda T.C. Başbakanlık Devlet Arşivleri Genel Müdürlüğü'nde görev almaya başladım. Halen belirtilen Kurumun Bilgi-İşlem Koordinatörlüğünde görev yapmaktayım.