**TC**
**DİCLE ÜNİVERSİTESİ**
**SOSYAL BİLİMLER ENSTİTÜSÜ**
**MALİYE VE EKONOMİ ANA BİLİM DALI**
**YÜKSEK LİSANS TEZİ**

# BİLGİ GÜVENLİĞİ VE ELEKRONİK İMZA KAVRAMLARI, EKONOMİK BOYUTLARININ İNCELENLEMESİ VE ELEKTRONİK İMZA UYGULAMALARI

**HAZIRLAYAN: İSMAİL ÖZLER**

**DANIŞMAN: PROF. DR. SELİM ERDOĞAN**

**DİYARBAKIR**

**2007**

# ÖZET

Bir savunma projesi olarak ortaya çıkan bilgisayarlar arası iletişim hızla tüm dünyaya yayılmış ve birçok ağın birbirine eklenmesi ile internet adını almıştır. Günümüzde milyonlarca bilgisayar arasında sürekli bir bilgi alışverişi olmaktadır. Bilgisayar ortamında saklanan elektronik verilerin belgelerin güvenliği ile başlayan bilgi güvenliği kavramının, iletişim sistemleri üzerinde hareket eden verilerin uğradığı saldırılar ile bir anda farklı bir boyutu ortaya çıkmıştır.

Bilginin kendisi kadar güvenliğinin de önemi anlaşıldıkça elektronik verilerin, belgelerin korunması adına farklı yöntemler denenmiştir. Bu yöntemler arasında dünyada kabul gören açık anahtar altyapısı, günümüzde en güvenilir ve kullanılabilir yöntem olarak öne çıkmaktadır. Açık anahtar altyapısı birçok ülke gibi Türkiye'de de bilişim sistemleri üzerindeki bilgilerin güvenliği uygulamalarında kullanılmaktadır.

Bilginin güvenliği kadar kime ait olduğu da önemlidir. Elektronik posta ile alınan bir belgenin gerçekten kime ait olduğunu ispatlanamadığı sürece o belge hiçbir değer taşımamaktadır. Kağıt üzerine yazılı metinlerin ve belgelerin en önemli unsurlarından biri olan imza, bilişim sektöründeki hızlı gelişmeler sonucu günümüzde elektronik metinlerde boy göstermektedir. Temel olarak elektronik metinlerin güvenliğinin sağlanması fikri ile ortaya çıkan e-imza, güvenlik kaygıları ile birlikte kimlik bilgisi, zaman bilgisi, inkar edilememezlik ihtiyaçlarına cevap verebilen tek uygulamadır.

Hızlı bir gelişme gösteren elektronik imza dünyada ve Türkiye'de yapılan düzenlemelerle yasal boyut kazanmış, gerek kamu gerek özel sektörde birçok alanda kullanılmaya başlanmıştır. Yapılan çalışmalar elektronik imzanın hukuksal boyutu konusunda bizlere fikir vermektedir. Ancak konunun ekonomik boyutlarının da incelenmesi gerekmektedir. Özellikle finans sektörünün küresel bir boyut kazanması bilişim ağları üzerinde hareket eden bilgilere atılacak olan bir imzanın varlığını gerektirmektedir. Finans sektörü, elektronik ticaret faaliyetleri, e-devlet uygulamaları ve daha birçok alanda kullanılması değerlendirilen e-imza'nın sadece hukuksal boyutu değil ekonomik boyutu ve uygulama alanları bu çalışmaya konu olmuştur.

## ABSTRACT

Communication between computers which was at the beginning a defense Project, has found a worldwide application and evolved into internet with the connection of many networks. Today millions of computers unceasingly communicate with each other. The concept of data security which was necessitated by the need to secure data and documents stored electronically has suddenly found a different dimension with the attacks directed at the data flowing between communication systems.

With the realization that the security of data is as important as the data itself, many different methods have been put under trial in order to project electronic data and documents. Among these methods, globally accepted public key infrastructure is today the foremost in usability and realibity. Public key infrastructure is currently being used for data security applications in Turkey as is the case for many countries.

Origins of informations is as important as the security of data. A document transfered via electronic mail is worthless if its true origins can not be proved. Signature, one of most important element of hard-copy texts and documents can also be found on electronic texts today due to fast developing information technology. E-signature basically necessitated by the idea of protecting electronic texts, is the only application that can hardly satisfy needs such as identity information, time information and undeniability along with security.

Rapidly developing, e-signature has found a legal base with the regulations put in force both in Turkey and the world and beings to be used in many areas both in public and private sectors. Studies provide us information concerning the legal standing of e-signature. However, its economical aspects should also be stutied. Especially the globalization of the finance sector neccessitates the signing of data being transferred by information Networks. This study includes not only the legal aspects, but also, the economical aspects and application areas of e-signature which is being considered for use in finance, e-commerce, e-goverment applications and many other areas.

Sosyal Bilimler Enstitüsü Müdürlüğüne

Bu çalışma jürimiz tarafından

…….

……

……...

Anabilim dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Başkan ……..

Üye ……..

Üye ……..

Üye ……..

Üye ……..

ONAY

Yukarıdaki imzaların adı geçen öğretim üyelerine ait olduğunu onaylarım

# ÖNSÖZ

Bilişim ağları, küresel ekonomilerin temel haberleşme omurgasını oluşturmaktadır. Asya piyasalarındaki bir dalgalanma Avrupa piyasalarını etkileyebilmekte ve yanlış, değiştirilmiş bir bilgi milyonlarca dolar kayıp ya da kazanç sağlamaktadır. Bu açıdan ele alındığında elektronik ortamda iletilen bilgilerin güvenliği, küresel ekonomileri yakından ilgilendirmektedir.

Finans sektörünün dışında internetin kişisel kullanımı yaygınlaştıkça elektronik ticaret uygulamaları hızla kitleler tarafından yoğun bir ilgi ile karşılanmaktadır. 2001 yılında kurulan bir elektronik ticaret uygulaması, 2004 yılında 100.000 kullanıcıya ulaşmış, 2007 yılında ise bu rakam 1.000.000 olmuştur. Baş döndürücü bir hızla yayılan bu alışkanlık beraberinde birçok riski de getirmiştir. Tüm bu değerlendirmeler ışığında gerek ticari ve ekonomik faaliyetler, gerek kamusal uygulamalar gün geçtikçe internet tabanlı düzenlemelerle şekil değiştirmektedir.

Ticaretten finansa, sağlıktan bürokrasiye, ulusal ve uluslar arası birçok uygulamanın yakın bir gelecekte tamamen elektronik ortama taşınacağı değerlendirildiğinde tüm bu faaliyetlerin temel taşlarından biri güvenlik olacaktır. Pasaport bilgileri, banka hesapları, şirketlerin ticari bilgileri, kişisel bilgiler ve burada sayamayacağımız birçok bilgi, veri ve belgenin içerikleri kadar güvenlikleri de önem kazanmaktadır. Son derece önemli bu bilgiler elektronik imza ile korunacaktır, korunmalıdır.

Elektronik imza yasal temeller üzerine oturtularak kullanılmaya başlanmıştır. Elektronik imza için sık sık kullanılan “yakın bir gelecekte” ifadesi artık yerini “günümüzde” ifadesine bırakmıştır.

# İÇİNDEKİLER

BÖLÜM III

E-İMZA'NIN EKONOMİK BOYUTU VE E-TİCARET

BÖLÜM IV

DÜNYADA ve TÜRKİYE'DE ELEKTRONİK İMZA ALTYAPILARI VE UYGULAMALAR

## KISALTMALAR

1. AAA : Açık Anahtar Alt Yapısı
2. AB : Avrupa Birliği
3. AR-GE : Araştırma Geliştirme
4. ATM : Automatic Teller Machine - Otomatik Vezne Makinesi
5. ATS : Alternative Trading Systems–Alternatif Ticaret Sistemlerinin
6. B2B : Business to Business - kurumlar Arası e-Ticaret
7. B2C : Business to Customer – Kurum-Müşteri arası Ticaret
8. BS : Bilgi Sistemleri
9. BTYK : Bilim ve Teknoloji Yüksek Kurulu
10. CD : Compact Disk
11. CIBC : Canadian Imperial Bank of Commerce
12. CMS : Cryptographic Message Syntax–Kriptografik Mesaj Söz Dizimi
13. DCCA : Danimarka Ticaret ve Firma Acenteleri
14. DİR : Dahilde İşleme Rejimi
15. DPT : Devlet Planlama Teşkilatı
16. DSV : Deutscher Sparkassen Verlag
17. DTM : Dış Ticaret Müsteşarlığı
18. EC : European Commision
19. ECA : Dışsal Sertifika Otoritesi
20. ECN : Elektronik İletişim Ağları
21. ECOM : Electronic Commerce Promotion Council of Japan
22. EDI : Elektronik Veri Alışverişi
23. EFT : Elektronik Fon Transferi
24. e-imza : Elektronik imza
25. e-finans : Elektronik finans
26. EİK : Elektronik İmza Kanunu
27. ESHS : Elektronik Sertifika Hizmet Sağlayıcısı
28. e-ticaret : Elektronik ticaret
29. ETKK : Elektronik Ticaret Koordinasyon Kurulu
30. HIPAA : Sağlık Sigortası Taşınabilirlik ve Sorumluluk Kanunu

31. ISO : International Organization for Standardization – Uluslararası Standardizasyon Organizasyonu
32. İGEME : İhracatı Geliştirme Etüd Merkezi
33. İMKB : İstanbul Menkul Kıymetler Borsası
34. İSKİ : İstanbul Su ve Kanalizasyon İdaresi
35. ITU : International Telecommunication Union – Uluslararası Telekominikasyon Birliği
36. KAP : Kamuyu Aydınlatma Platformu
37. KPSS : Kamu Personeli Seçme Sınavı
38. MA3 : Milli Açık Anahtar Altyapısı
39. Md. : Madde
40. MEDAS : Mesaj Dağıtım Sistemi
41. NVİ : Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü
42. OCES : Elektronik Servisler için AÇIK Anahtarları
43. OECD : Organisation for Economic Co-operation and Development-Ekonomik İşbirliği ve Kalkınma Teşkilatı
44. ÖSS : Öğrenci Seçme Sınavı
45. PIN : Personal Identification Number – Kişisel Tanımlama Numarası
46. PKI : Public Key Infrastructure – Açık Anahtar Altyapısı
47. POS : Point of Sales – Satış Noktası
48. RSA : Rivest, Shamir ve Adleman
49. SPK : Sermaye Piyasası Kurulu
50. SSK : Sosyal Sigortalar Kurumu
51. STP : Straight Through Processing
52. TOBB : Türkiye Odalar ve Borsalar Birliği
53. TNB : Türkiye Noterler Birliği
54. TBMM : Türkiye Büyük Millet Meclisi
55. TCDD : Türkiye Cumhuriyeti Devlet Demiryolları
56. TCMB : Türkiye Cumhuriyeti Merkez Bankası
57. TİKA : Türk İşbirliği ve Kalkınma İdaresi Başkanlığı
58. TK : Telekomünikasyon Kurumu
59. TSK : Türk Silahlı Kuvvetleri
60. TSE : Türk Standartları Enstitüsü

61. TUENA : Türkiye Ulusal Enformasyon Altyapı Planı
62. TÜBİTAK : Türkiye Bilimsel ve Teknik Araştırma Kurumu
63. UEKAE : Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü Müdürlüğü
64. UNCTAD : Birleşmiş Milletler Ticaret ve Kalkınma Konferansı
65. UN-CEFACT : Birleşmiş Milletler İdari, Ticari ve Ulaşımla İlgili Uygulama ve Usulleri Kolaylaştırma Merkezi
66. UNCITRAL : Birleşmiş Milletler Uluslararası Ticaret Hukuku Komisyonu
67. VPOS : Virtual Point of Sales – Sanal Satış Noktası
68. WTO : World Trade Organisation - Dünya Ticaret Örgütü
69. WWW : Word Wide Web

# TABLO, ŞEKİL VE EKLER LİSTESİ

**TABLOLAR** **SAYFA NO**



**ŞEKİLLER**



**EKLER**

# GİRİŞ

Bilişim teknolojisi ve internet sosyal ve ekonomik yaşamın vazgeçilmez bir parçası oldukça, haberleşme ve iletişim alışkanlıklarımız sayısal ortama doğru bir yönelme eğilimine girmiştir. Bu eğilimlerin sosyal boyutu toplumlar tarafından kabul görmeye başlamasına rağmen ekonomik eğilimler karşısında toplumsal alışkanlıklar bir direnç duvarı oluşturmaktadır. Bu direnç duvarının en temel yapı taşı güvenlik kavramıdır.

Ekonomik faaliyetlerin birçok unsuru olmakla birlikte bilişim sektörünün bu faaliyetlerde sağlıklı bir ortam olarak kendine yer bulmasında anahtar kelime güvenliktir. Maliyet, verim, kar payı; ticaretin en önemli boyutları olarak düşünülmekte ancak konu elektronik ticaret olduğunda bu faktörlerin başına güvenlik gelmektedir. Temel ihtiyaçlardan biri olan güven duygusunun tam anlamıyla oluşmasından sonra; elektronik ticaret gelişme gösterecek ve toplum tarafından kabul görmeye başlayacaktır. Elektronik ticaret uygulamalarında karşılıklı güven için ortaya atılan fikirlerden dünyada en çok kabul gören kavram ise elektronik imza olarak karşımıza çıkmaktadır.

## A. Çalışmanın amacı

Bu çalışmanın amacı, bilgisayar ağlarına yapılan saldırılar göz önüne alındığında hayati önem taşıyan bilgilerin korunmasına dikkat çekmek, elektronik ticaretin vazgeçilmez bir parçası olan elektronik imza kavramının ekonomik boyutlarını ortaya koymak, dünyada ve Türkiye'de ki uygulamalarını incelenmektir.

## B. Araştırma Soruları

Çalışmada aşağıdaki sorulara cevap aranmıştır.

- Bilgisayar ağları üzerinde iletilen bilgilerin güvenliği neden önemlidir?
- Bilgi güvenliği konusunda dünyada en çok tercih edilen yöntem nedir?
- Elektronik imza nedir, nasıl kullanılır, ekonomik boyutları nelerdir?
- Dünyada ve Türkiye'de elektronik imza uygulamaları nelerdir?

Çalışma dört bölümden oluşmaktadır. Birinci bölümde bilgi güvenliği, açık anahtar altyapısı, konuları incelenmiştir. Bu kapsamda bilgi güvenliği kavramının temelini oluşturan unsurlardan biri olan kriptoloji biliminin tekniklerinden çok uygulamaya yönelik unsurları genel hatları ile anlatılmıştır. Ayrıca elektronik imza uygulamalarında tercih edilen açık anahtar altyapısı incelenmiş ve bir senaryo ile açıklanmıştır.

Çalışmanın ikinci bölümünde Elektronik imza kavramı açıklanmıştır. Dünyada ve Türkiye'de elektronik imzanın oluşumu ve ülkemizde elektronik imza mevzuatı incelenmektedir. Bu bölümde elektronik imzanın temel unsurları, özellikleri hukuki sonuçları 5070 sayılı Elektronik İmza Kanununa değinilmiştir.

Üçüncü bölümde ise bilgi, ürün veya hizmet alışverişinin bilgisayar ağları ile gerçekleştirilmesi sonucu ortaya çıkan elektronik ticari faaliyetler göz önüne alınarak elektronik imzanın ekonomik boyutları incelenmektedir. Küresel ticaret ortamında elektronik ticaretin oluşumu, unsurları, finans piyasalarında elektronik imza örneklerle açıklanmıştır.

Son bölümde ise dünyada ve Türkiye'deki ilk elektronik imza uygulamaları ekonomik ve toplumsal boyutları göz önüne alınarak incelenmektedir. Yine bu bölümde TSK Akıllı Kart sistemi hakkında bilgi verilmiştir.

Genel olarak ana metin içinde bazı kavramlara değinilmiştir ancak EK-A'da elektronik imza mevzuatı çerçevesinde tanımlar açıklamıştır. EK-B' de ise 5070 sayılı Elektronik İmza Kanunu yer almaktadır.

### C. Çalışma Yöntemi

Çalışma esas olarak belge tarama ve uygulama inceleme teknikleri kullanılarak oluşturulmuştur. Ülkemizde bilişim sektörü ve kamu alanında yapılan elektronik imza hazırlıklarını anlayabilmek için çalışma gruplarının raporları incelenmiştir. Ayrıca dünyadaki gelişimi ve uygulamalar WEB siteleri taranarak tespit edilmiştir.

Çalışmanın en büyük sınırlaması, incelenmekte olan temel kavramın en önemli unsurunun güvenlik olması sebebiyle istatistikler ve teknikler hakkında yeterli bilgiye ulaşmakta sıkıntılar ve kısıtlamalar yaşanmıştır. Ayrıca kavram olarak uzun bir geçmişi olmasına rağmen uygulamalar açısından henüz çok yeni bir kavram olması sebebiyle bu konuda yayımlanmış doküman sıkıntısı çekilmiştir.

# BÖLÜM I

# BİLGİ GÜVENLİĞİ VE AÇIK ANAHTAR ALTYAPISI KAVRAMINA GENEL BAKIŞ

## 1.2 Bilişim Güvenliği Kavramı

Geçmişte emek, sermaye ve doğal varlıklar gibi temel üretim faktörlerini yönetmek durumunda olan yöneticiler, günümüzde üretimin temel faktörü durumuna gelen bilgiyi yönetmek durumundadırlar. Bilginin en önemli ekonomik değer haline geldiği bu çağda, etkin bilgi yönetiminin gerekliliği artmıştır. Küçük ya da büyük, bütün kurum ve kuruluşların etkinliğinin bilgi kaynaklarını ne denli kullanabildikleri, yönetebildikleri ve bunlardan ne denli yararlanabildiklerine bağlı olduğu gözlemlenmektedir. Araştırmalar, çalışanların çalışma sürelerinin 1/8'ine varan kısmını evrak almak/göndermek/ aramak/arşivlemek ve akışını kontrol etmek için harcadıklarını göstermektedir. Bu noktadan hareketle, kurumlarda evrak ve bilgi akışının çok ciddi yekünler tutmaması için, hızlı ve daha etkin çözümler üretilmesi gerekmektedir. Bu çözümlerin tümünün de Bilgi ve İletişim Teknolojilerine dayanacağı aşikardır. (Bilişim, 2005 s:4)

Dünyada birçok ülke, yeni yüzyılın baskın yönelimi haline gelen Bilgi ekonomisine geçiş ve bilgi toplumuna dönüşüm için kendilerini hazırlamaktadır. Bu süreçte başarılı bir dönüşüm için tek bir model bulunmamaktadır. Ülkeler bu dönüşüme tarihleri, kültürleri, ulusal öncelikleri, ekonomik statüleri, ekonomik büyüklükleri, coğrafyaları ve nüfusları çerçevesinde farklı biçimlerde cevap vermektedirler. Ancak tüm ülkelerde karşılaşılan ortak bir sorun bulunmaktadır: bu da geçişin risklerinin azaltılıp, ekonomik ve sosyal yararların nasıl artırılabileceği sorusudur. (İİK, 2004)

Riskler analiz edilirken oluşabilecek tehditlerin, saldırıların elektronik anlamda düzenleneceği göz önüne alınmalıdır. Kuzey Kore'de askeri bir e-savunma birliği kurulmuş ve çalışmalar yapmaktadır. Bu da bize, gelecekteki savaşlarda, e-saldırıların yada e-bombaların ne kadar hayati bir öneme sahip olacağı ve ülkelerin savunma doktrininde yer alması gerektiğini göstermektedir. Her geçen gün yeni bir virüs ve/veya saldırı ile karşılaşmaktayız. (Kuran, 2004 s:13)

Bilgi ve iletişim teknolojileri alanındaki gelişmelere paralel olarak yapısı ve fonksiyonları önemli ölçüde değişen ofisler, post-modern yapılarda bilgi işleyen birimler haline dönüşmüştür. Özellikle ofis otomasyonunun gelişmesine paralel olarak gelişen kağıtsız ve dosyasız ofisler yaygınlaşmaya başlamıştır. Devlet'in de verdiği bütün hizmetlerde bu teknolojilerden ve yapılanmalardan yararlanması kaçınılmaz sonuçtur. (Bilişim, 2005 s:4)

Bütün güvenlik önlemleri alınsa dahi, bilgi/belgenin hareketi esnasında riskleri sıfırlamak söz konusu olamayabilir. Güvenlik konusunda yapılan tüm çalışmaların, riskleri makul bir düzeye kadar azaltmak üzerine olduğu düşünülmektedir. (Bilişim, 2005 s:16)

Bilginin kurumlar arasında güvenli bir şekilde iletilmesi ve paylaşılması, işlemlerin elektronik ortamda güvenle yapılabilmesi ve yaygınlaşabilmesi açısından kritik önem taşımaktadır. Kurumların bilgi sistemleri, internet'e bağlı olmanın getirdiği güvenlik risklerine karşı koruma sağlayacak şekilde tasarlanmalı ve yapılandırılmalıdır. Bu sayede vatandaşlar, kamu kurumları ve iş çevreleri arasında güvenli bir etkileşim sağlanmış olacaktır. (Başbakanlık, 2005 s:13)

Kağıt temelli, makine gücü yoğun, sanayi devrimi mekanizmaları ve süreçlerini temel alarak kurgulanan iş dünyasına yönelik hukuksal düzenleme enstrümanları, bilgi ekonomisin yeni iş süreçleri, gayri maddi (intangible) ürün ve hizmetleri kapsama almakta zorlanmaktadır. Bu durum kimi zaman hukuksal yorum sorunu olmasına rağmen kimi zaman da özel düzenleme yapma ihtiyacı ortaya çıkmaktadır. (İİK, 2004)

Genel olarak bilgi güvenliği, "bilgi değerlerini izinsiz erişim, ifşa ve kötüye kullanma, değiştirilme veya zarar ve kayıptan korumak üzere kullanılan işlem ve teknolojilerin toplamıdır." (UNCTAD, 2005 s: 187) şeklinde tanımlanabilir.

### 1.2 Bilgiye Yönelik Saldırılar

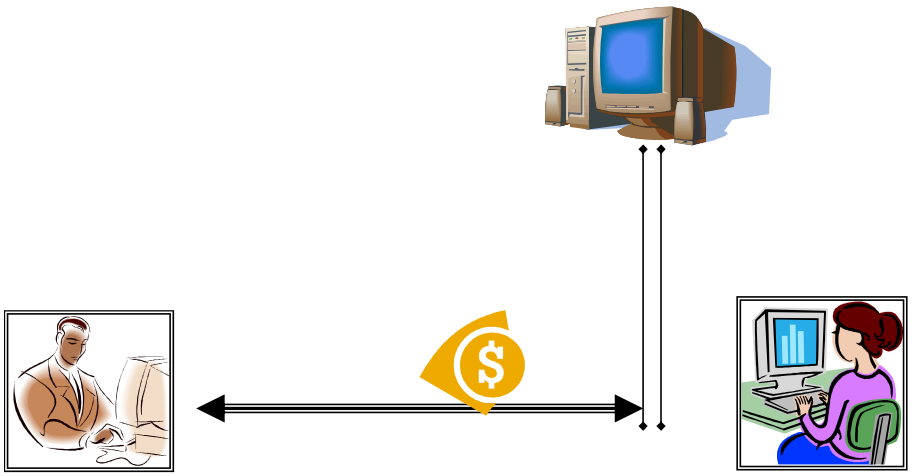
İnternet üzerinden bilgi iletiminde karşılaşılabilecek sorunlar ve saldırılar; Engelleme (Interruption), Dinleme (Interception), Değiştirme (Modification) ve Yeni Mesaj İletme (Fabrication) ana başlıkları altında toplanmaktadır. Engelleme; mesajın gönderilen kişiye ulaşmasının engellenmesi, dinleme; mesajın içeriğinin öğrenilmesi, değiştirme; mesajın içeriğinin değiştirilerek iletilmesi, yeni mesaj

iletme; yeni bir mesaj hazırlayıp başkası adına gönderme olarak kısaca açıklanabilir. (Özer s:5)

**Şekil 1**

Şekil 1.1 de bilgisayar kullanan iki kişi arasındaki veri haberleşmesi görülmektedir. Günlük hayatta birçok alanda kullanılan bu haberleşme yöntemi, alışık olduğumuz ve güvenli olduğunu düşündüğümüz haberleşme/veri iletişimini göstermektedir.

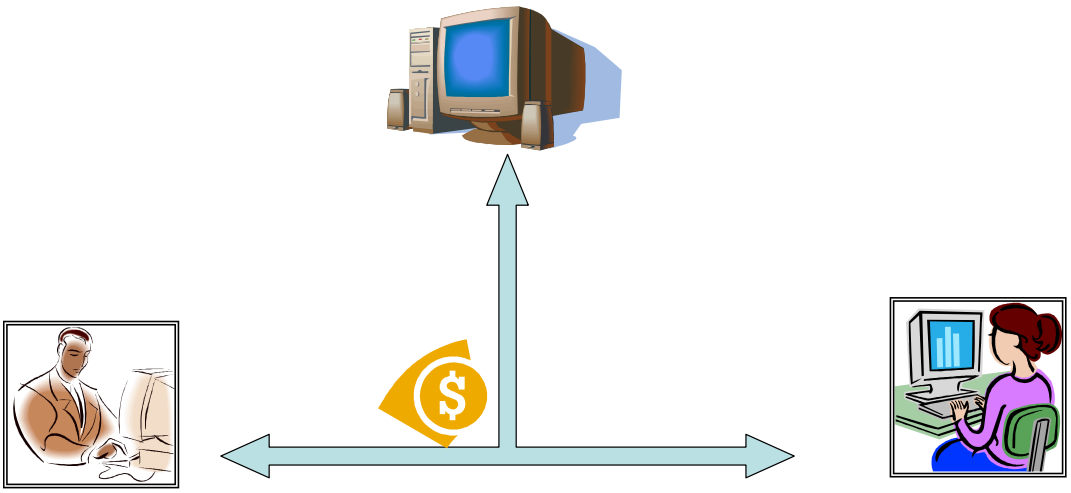
### 1.2.1 Engelleme



**Şekil 2**

Şekil 2 de gönderilen verinin/mesajın başka bir bilgisayar tarafından engellendiği görülmektedir. Aktif bir saldırı türü olan bu eylemde karşılıklı haberleşme kesilir. İletişim saldırgan bilgisayar izin verene kadar ya da başka bir bağlantı üzerinden gerçekleştirilebilir.

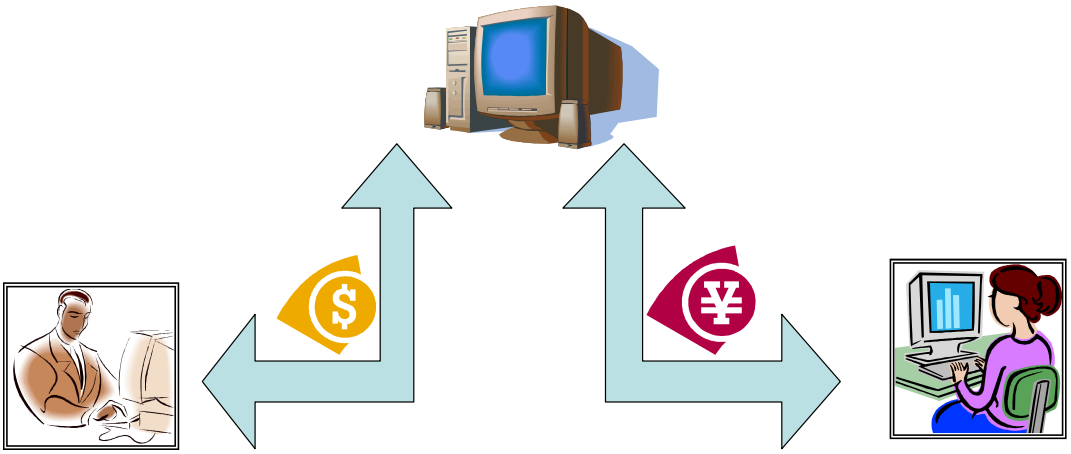
### 1.2.2 Dinleme



**Şekil 3**

Şekil 3 te gönderilen mesajın başka bir bilgisayar tarafından dinlendiği diğer bir deyişle izinsiz olarak gönderilen mesaja eriştiği görülmektedir. Saldırgan bilgisayar mesajı kopyalayabilir. Pasif bir saldırı yöntemidir ve dinlemeden gönderen ve alan bilgisayarların haberi olmaz.

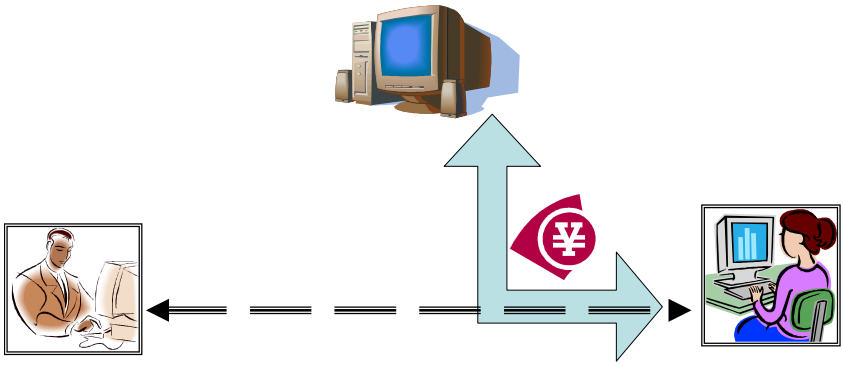
### 1.2.3 Değiştirme



**Şekil 4**

Şekil 4 te gönderilen mesajın saldırgan bilgisayar tarafından alınarak değiştirildiği, yeni mesajın alıcıya iletildiği görülmektedir. En zararla tehlikelerden biridir. Değişikliğin boyutu, içeriği bilinmediği için verebileceği zararlar çok büyük olabilir. Virüs saldırıları yöntemle meydana gelebilir.

### 1.2.4 Yeni Mesaj İletme



**Şekil 5**

Şekil 5 te iki kullanıcı arasında tesis edilen haberleşme pasif olduğunda yada sonlandırıldığında saldırgan gönderen kullanıcıyı taklit ederek alıcıya yeni bir mesaj gönderebilir. Alıcı bilgisayara zarar verebilecek tehlikeli yazılımlar, sahte veriler gönderebilir.

## 1.3 Güvenlik Kriterleri

Bilginin güvenli bir şekilde iletilmesi için kurumların da belli başlı bilgi güvenliği standartlarına uyması ve bilgi paylaşan tüm kurumların bu standartları yakalaması gerekmektedir. Son yıllarda internet kullanımının artmasından dolayı güvenliğin büyük önem kazanmasıyla birlikte bu alandaki standartlaşma çalışmaları da aynı oranda artmaktadır. Bunun sonucunda çok sayıda güvenlik standardı, talimatı ve tavsiyesi ortaya çıkmıştır. (Başbakanlık, 2005 s:13)

Başbakanlık tarafından 2005 yılında yayınlanan "DÖNÜŞÜM TÜRKİYE PROJESİ BİRLİKTE ÇALIŞABİLİRLİK ESASLARI REHBERİ" isimli genelge ile kamu kurum ve kuruluşları tarafından uyulması gereken bilgi güvenliği standartları belirlenmiştir.

Tablo 1: Kullanılacak Standartlar

| **Bileşen** | **Standart/Teknoloji** | **Açıklama** |
|---|---|---|
| Bilgi güvenliği yönetimi için uygulama prensipleri | TS ISO/IEC 17799:2002 | Bilgi güvenliği yönetim sistemlerinde kullanılabilecek karşı önlem önerileridir.<br>Mümkün olan hallerde milli olarak üretilen karşı önlemlerin kullanılmasına azami özen gösterilmelidir.<br>Standart, uluslararası ISO 17799-2:2000 standardının Türkçe çevirisidir. |
| Bilgi güvenliği yönetim sistemleri – Özellikler ve kullanım kılavuzu | TS 17799-2:2005 | Kurumların dokümante edilmiş bir BGYS'yi tüm ticari riskleri bağlamında kurmak, gerçekleştirmek, izlemek, gözden geçirmek, bakımını yapmak ve iyileştirmek için gereksinimleri kapsar. Standart, BS 7799-2:2002 standardının Türkçe çevirisidir. |

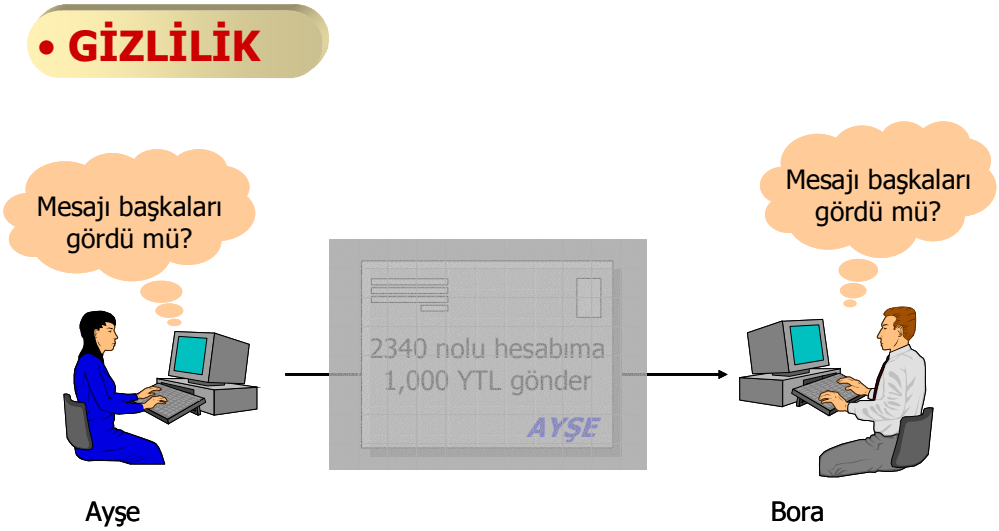
Kaynak**:** Dönüşüm Türkiye Projesi Birlikte Çalışabilirlik Esasları Rehberi

Kurum ve kuruluşları satın alacakları veya geliştirecekleri bilgi teknolojileri sistemlerinde gizlilik dereceli bilgiyi bulundurmaları veya bu sistemleri kullanarak bilgi iletmeleri durumlarında sistemlerinin güvenlik seviyelerini Ortak Kriterler standardına uygun olarak tespit etmeli ve risk analizi sonucunda tespit edilen asgari garanti düzeyini sağlayacak ürün ve/veya sistemleri kullanmalıdırlar. (Başbakanlık, 2005 s:14)

Bilginin güvenli bir şekilde elektronik olarak iki taraf (Örneğin hisse senedi alım emrini veren kişi ile emri alan aracı kuruluş) arasında iletilmesi için iletim kanalından – internet, telefon, faks vb. - bağımsız olarak; **Gizlilik, Bütünlük, Kimlik doğrulama ve Reddedilmezlik** şeklinde sıralan güvenlik kriterlerinin sağlanması gerekmektedir. Söz konusu tanımların bilgi güvenliğindeki anlamları sırasıyla; "iletilen verinin içeriğinin üçüncü kişilerce elde edilememesi", "iletim sırasında verinin kaynaktan çıktığı haliyle korunması", "gönderenin kimliğinin

ispatı" ve "gönderenin daha sonra iletilen verinin kendisi tarafından gönderilmediğini iddia edememesi" olarak açıklanabilir. (Özer s:5)

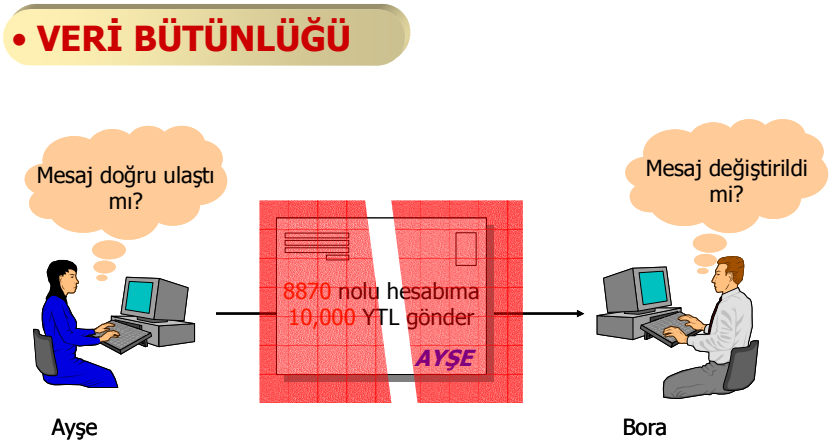
### 1.3.1 Gizlilik




**Şekil 6**

Güvenliğin en önemli unsuru olan gizlilik kavramı Şekil 6 da görülmektedir. Gönderilen mesajın başkaları tarafında görülmesi istenen bir husus değildir. Veri haberleşmesinde gizlilik mesajların şifrelenmesi ile sağlanır. Elektronik veri iletişiminde gönderilen mesajlar başkaları tarafından öğrenilmeyecek şekilde şifrelenerek anlaşılmaz bir hale getirilir. Mesajı alan kullanıcı aynı algoritmayı kullanarak mesajı deşifre eder.

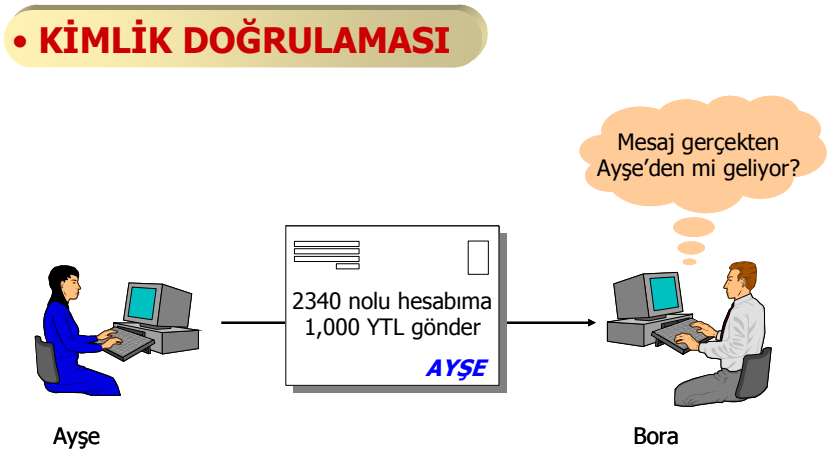
### 1.3.2 Bütünlük




**Şekil 7**

Gönderilen mesajın bütünlüğü Şekil 7 de anlatılmaktadır. Mesajın içeriğinin başka bir kullanıcı tarafından değiştirilip değiştirilmediğini ifade eder. Veri bütünlüğü olarak da tanımlanmaktadır. Şifrelenen bir mesajın başkası tarafından ele geçirilmesi durumunda saldırgan mesajın içeriğini öğrenemediği için değişiklik yapamayacaktır. Değişiklik yapsa dahi yeni mesaj anlamsız olacağı için bütünlüğe zarar verildiği anlaşılacaktır.

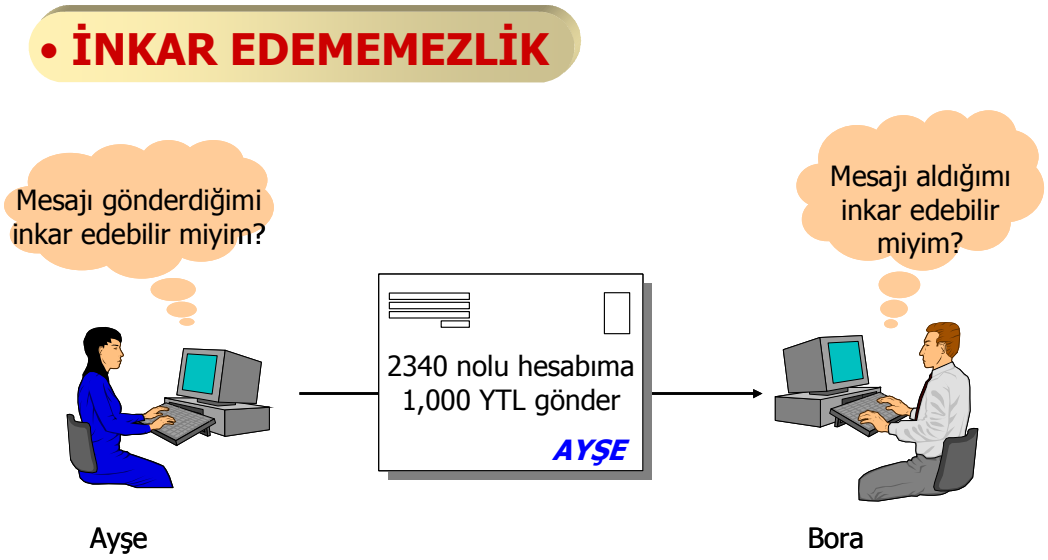
### 1.3.3 Kimlik Doğrulama




**Şekil 8**

Şekil 8 de gönderilen mesajın kimden geldiğinin kanıtlanması gerektiği görülmektedir. Kimlik tanımlama bir sisteme kişinin kimliğinin tanıtılmasından sonra sistem tarafından, kişinin kimliğinin tespit edilmesi işlemidir. Kimlik doğrulaması ihlalini ortadan kaldırmak ve gerekli tedbirleri almak için genellikle özetleme algoritmaları, mesaj özetleri, elektronik imzalar ve sertifikalar kullanılmaktadır. Elektronik ortamda yapılan bu doğrulama işleminin gerçek hayatta yapılan işlemlerden daha güvenli olduğunu burada belirtmekte fayda vardır. (Sağıroğlu ve Alkan, 2005, s:29)

### 1.3.4 Reddedilmezlik (İnkar Edememezlik)




**Şekil 1.9**

Günlük hayatta veri iletişiminde ihtiyaç duyulan hususlardan biri de reddedilmezlik yani inkar edememezliktir. Şekil 1.9 görüldüğü gibi mesajı gönderen ya da alan kullanıcı mesajı aldığını ya da gönderdiğini inkar edebilir. Bunu engellemek için, karşılıklı haberleşmede tarafların birbirinden gelen mesajları aldığını veya gönderdiğini teyit etmesi veya bunu inkar etmemesi gereklidir. Bunu sağlamak için, mesajı gönderen veya alan kişilerin kayıtları güvenilir bir makam tarafından tutulur veya güvenli haberleşmenin yapılabilmesi için uygulanan yaklaşımlar ile inkar edememezlik sağlanmaktadır. (Sağıroğlu ve Alkan, 2005, s:30)

İnternet üzerinden güvenli veri alışverişi için kurulan sistemde yukarıda sayılan bilgi güvenliği ölçütlerinin sağlanması ve böylelikle bahsi geçen sorun ve saldırılara maruz kalındığında bilgiye herhangi bir zarar gelmeden ve başkalarınca ele geçirilmeden karşı tarafa iletildiğinin garanti edilmesi gerekmektedir. (Özer s:5)

Kurumsal ağların dışarıdan veya içeriden gelebilecek saldırılara karşı korunmasında güvenlik duvarları (firewall), anti-virüs yazılımları, zayıflık tarama yazılımları, ağ dinleme ve yönetim yazılımları, saldırı tespit sistemleri (intrusion detection system) ve yedekleme araçları kullanılmaktadır. İnternet gibi açık iletişim ağlarında veri güvenliğinin sağlanmasında ise en güvenilir yöntem açık anahtarlı altyapıdır (kriptografidir). (Sevim, 2004 s:138-139).

### 1.4 Açık anahtar Altyapısı

Şifreleme, elektronik ortamda iletilen bilginin dönüştürülmesi işlemidir. Bu yöntemde bilgi, alıcı dışında başka bir kişi tarafından okunamaması yada değiştirilememesi için kodlanır. Şifreleme ile gönderilen herhangi bir bilginin gizliliği korunmuş ve bütünlüğü bozulmamış olur. (Çak, 2002)

Şifreleme yönteminde güvenliği artırmak amacıyla çeşitli şifreleme algoritmaları kullanılmaktadır. Elektronik imza uygulamalarında kullanılan en yaygın kullanılan yöntem Açık (simetrik olmayan) anahtar algoritmasıdır (altyapısı).

Açık Anahtar Alt Yapısı (AAA) ; 1978 yılında 3 bilim adamı Rivest, Shamir ve Adleman'ın baş harflerinden oluşan RSA matematik algoritmasının onaylanması ile başlar (Yükseliyor, s:1). Geliştirilen ilk asimetrik anahtarlı şifreleme algoritmalarından biridir. Bu teknikte şifreleme ve şifre çözme için farklı kripto anahtarları kullanılır. (Başbakanlık, 2005 s:22)

AAA teknolojisi İkinci Dünya Savaşından başlayarak belli bir bilimsel temel üzerine oturtulmuş, 1970'li yılların başından itibaren çok önemli gelişmelerle birlikte giderek yoğun şekilde ticari uygulamalarda kullanılmaya başlanmış, dünya üzerinde standartları ve küresel ölçekte güvenlik ve işlerlilik alanları oluşturulmuş en güvenilir güvenlik uygulaması olduğu kanıtlanmıştır. Küresel düzeyde birçok yapı bu teknolojiyi kullanmakta ülkelerin bu teknolojiyle ilgili mevcut ve müstakbel yatırımları bulunmaktadır. (TK, 2004d, s:20)

Ülkemizde de gerek devlet gerek özel sektör gerekse de Silahlı Kuvvetler açık anahtarlı alt yapı uygulamalarını kullanmakta bu konuyla ilgili AR-GE yatırımları yapılmakta ve bu uygulamanın etkin olacağı kullanım ve güvenlik alanları oluşturulmaktadır. (TK, 2004d, s:21)

AAA birçok kaynakta **"**Bilgi iletişiminde açık anahtarlı kriptografinin yaygın ve güvenli olarak kullanılabilmesini sağlamaya yarayan ve birbirleriyle eşgüdüm içinde çalışan anahtar üretimi, anahtar yönetimi, onay kurumu, sayısal noterlik, zaman damgası gibi hizmetlerin tümü" şeklinde tanımlanmaktadır.

Günümüzde ağ sistemlerinin çoğu AAA sistemini kullanmaktadır ve bu ağların çoğu kamuya açık ağlar değildir. AAA, pek çok çalışanı olan bir şirkette, şirket çalışanlarının birbirleriyle olan iletişiminin güvenliği, gizli iletilerin sadece yetkili kişiler tarafından görülebilmesi gibi amaçlarına yönelik olarak kullanılabilir.

Böyle bir sistemde şirketin bir sunucusu (server), çalışanlara sertifika dağıtmak görevini üstlenebilir. (Sevim, 2004, s:4)

Ana amacı; sanal dünyada; herhangi bir bilgi taşınırken Gizlilik (Confidentiality), Bilgi Bütünlüğü ( Integrity) , Kimlik Doğrulama ( Authentication) ve Gönderenin İnkar Edememesi ( Non-repudiation) güvenlik özelliklerinin sağlanması olan AAA; bu işlemleri Sayısal İmza ve Sayısal Kripto ile Özel ve Genel anahtar kullanarak gerçekleştirmektedir. Sayısal imza; Kimlik Doğrulama, Bilgi Bütünlüğü ve Gönderenin İnkar Edememesi; Sayısal kripto ise Gizlilik güvenlik fonksiyonlarını sağlamaktadır. (Yükseliyor, s: 1)

Anahtar, şifrelemek veya deşifre etmek için kullanılan sayısal karakterler dizisidir. Simetrik anahtar algoritmasında şifrelemek ve deşifre etmek için aynı anahtar; açık anahtar algoritmasında şifrelemek için açık anahtar, deşifre etmek için ise gizli anahtar kullanılır. (Erdem ve Efiloğlu, s:14)

Açık anahtar algoritması, çok büyük sayılarla yapılan bazı işlemlerin bir yönde kolay aksi yönde ise zor olduğun gerçeğini kullanmaktadır. AAA'da çok büyük asal sayılar üretmenin kolaylığına karşın, büyük sayıların asal bileşenlerinin bulunmasının zor olduğu varsayımı ile hareket edilmektedir. Matematikçilerin tamsayıları asal bileşenlerine ayırmanın hızlı bir yolunu henüz bulamamış olmaları, bu varsayımı destekleyici yöndedir. (Sağıroğlu ve Alkan, 2005, s:43)

Bu altyapı ile gönderilen mesajın bütünlüğünün korunması, gönderenin belirlenmesi, yetkilendirme gibi birçok amaç gerçekleştirilebilir. Anahtarlar ne kadar uzun seçilirse şifrenin kırılması o kadar zor olur. (Başbakanlık, 2005 s:22)

AAA kullanıldığı durumda, açık anahtar genellikle veritabanlarından yayınlanır ve isteyen herkes istediği kişinin elektronik sertifikasını okuyarak açık anahtarını öğrenebilir (Başbakanlık, 2005 s:22).Gizli anahtar ise sadece kullanıcının kendisi tarafından bilinir ve kullanılır(Çak, 2002).

Bir anahtarın diğerinden türetilmesi veya hesaplanması mümkün değildir. Açık anahtarın başkaları tarafından bilinmesinin bir sakıncası yoktur fakat gizli anahtar kesinlikle bir başkası bilmemelidir. Dijital anahtarlar açık-gizli anahtar şifreleme algoritması üzerine kurulmuştur. Bir açık-gizli anahtar çifti bir sayı çiftinden ibarettir. Gizli anahtar sadece sahibi olan kişi ya da kurum tarafından bilinir ve dijital imzayı oluşturmak için kullanılır. Açık anahtar ise dijital imzaların

doğrulanması için kullanılır. Bir dijital imzanın doğrulanması mesajın geldiği kişinin kimliğinin doğrulanması anlamına gelmektedir (Lawrence, 2002, s:63).

Dünya pratiği ve Avrupa Birliği ülkelerine bakıldığı zaman %90 aşan bir oranda elektronik imza uygulamalarında "açık anahtarlı altyapı" (*public key infrastructure*) teknolojisi kullanıldığı ve kanunlaştırılmalarında da bu teknolojiyi temel alan çözümlemeler üretildiği gözlemlenmektedir.

### 1.5 AAA Üzerine Bir Senaryo

AAA algoritmasını anlamak için aşağıdaki senaryo ideal bir örnek teşkil etmektedir.

> *Herkesin özel olarak üretilmiş bir kasası olsun. Bu kasalardan biri kendine ait anahtar ile kilitlendiğinde; bu kasa kilitlenen anahtar dışında dünya üzerinde sadece bir anahtar tarafından açılabilmektedir. Kasayı kilitleyen anahtar; kasayı açamamaktadır. Bu kasalar imal edildiğinde kasayı kilitleyen ve açan anahtar farklı olmalarına rağmen eş olarak üretilmektedir. Aklımıza bu nasıl mümkün olabiliyor sorusunu getiriyor.*
>
> *Kasa ile birlikte üretilen anahtarlardan birini çilingirde birçok defa kopyasını çıkartarak bu kopya anahtarları bana herhangi bir şey gönderecek kişilere dağıtıyorum. Kopya almış olduğum bu anahtarlara Genel Anahtar olarak tanımlıyorum.*
>
> *Herhangi bir kişi bana bir bilgi göndermek istediğinde, yukarıda bahsi geçen özel üretilmiş kasalardan alması, bana göndereceklerini kasaya koyması ve onlara benim vermiş olduğum anahtar ile kasayı kilitlemesi yeterli. Bundan sonra tek yapılması gereken kasayı bana göndermesi. Benim üretilen kasa anahtarlarından bende kalanı olan Özel anahtar ile bana gelen kasayı açabilirim. Böylelikle benden başka birinde bu anahtar bulunmadığından söz konusu kasayı başkaları açamayacaktır. Kasayı açabilmeleri için özel anahtarımı almaları gerekmektedir.*
>
> *Özetlersek, bana göndereceklere vermiş olduğum kopya anahtar benim Genel anahtarım, kendimde kalan ve herhangi birine vermediğim anahtar ise benim Özel Anahtarım dır.*

*Ancak burada bir problem söz konusudur. Bana gönderilen kasayı alıp özel anahtarımla açtığım için, kasa içinde ne varsa bana ait olduğu kesin, kesin olmayan bu kasanın kimin tarafından gönderildiği. Kasa içinde bununla ilgili not da koymuş olsalar, bunun gerçekten doğru bir not bilgisi mi olduğu kesin değil. Çünkü kendilerine Genel Anahtar verdiğim herhangi bir kişi de bu notu yazmış olabilir. Yine de Kasayı gönderen kişinin kimliğini tespit etmenin bir yolu var. Bana gelen kasanın içine girebilen daha küçük bir kasa olsun. Eğer bana büyük kasayı gönderen kişi kendi kimliğini ispatlaması için, küçük kasa içine bazı bilgiler ekleyip küçük kasayı kendi Özel anahtarı ile kilitlemesi ve kilitlenen küçük kasayı; büyük kasanın içine koyması gerekecek. Küçük kasa herkes tarafından açılabilir. Çünkü küçük kasanın açılması için Genel anahtar bana ve diğerlerine bilgi gönderen kullanıcı tarafından verildi. Daha sonra büyük kasayı benim genel anahtarım ile kilitleyip büyük kasa bana geldiğinde, büyük kasayı özel anahtarım ile açıp, kişinin genel anahtarı ile de küçük kasayı açarsam büyük kasanın kimden geldiğini bulmuş olurum.*

*AAA alt yapısını oluşturan yukarıda senaryoda söz konusu edilen Özel ve Genel anahtarlar AAA sisteminin ana bileşenlerini oluşturmaktadır. Yukarıda senaryoda vermiş olduğumuz kasa örneği anahtarların nasıl çalıştığını anlamak açısından ele alınmıştır. Kasa ve anahtarların bilgisayar dünyasında eşleniğine ihtiyaç bulunmaktadır.*

*Bilgisayarlarda kasa olmasa da bunun yerine Sayısal Kriptolama tekniği vardır. Örneğin bir dosyayı sayısal kripto tekniği ile kilitleyip, açmak istediğimizde sayısal kripto tekniğini kullanmak gerekmektedir. Bilişimde de kasa örneğinde olduğu gibi anahtarlar kullanılmakta, herhangi bir bilgisayar dosyası, Genel anahtar ile kriptolandığında; bu dosyayı sadece benim özel anahtarım açabilmektedir. Bu dosyayı kriptolayan kişi dosyanın içine bir metin ekleyip bu metni kendi Özel anahtarı ile kriptolar ise; ben de bu dosyanın kimin tarafından gönderildiğini doğru olarak öğrenmiş olurum. Bilişimde bu durum biraz farklı şekilde yapılmaktadır. Gönderilmek istenen dosyaya özgü bir değer, gönderenin özel anahtarı ile kriptolanarak dosyanın sayısal imzası bulunur. Daha sonra hem ana dosya hemde dosyanın sayısal imzası*

*gönderilecek kişinin Genel anahtarı ile kriptolanır. Kriptolanmış ana dosyayı alan, bunu Özel anahtarı ile açtığında hem dosya aslını hem de sayısal imzasına erişir. Dosyanın Sayısal imzası gönderenin Genel anahtarı ile de-şifre edilebiliyor ise göndereninin kimliği de ispatlanmış olmaktadır.*

*Başkalarının gönderdiklerini açabilmek için; başkalarının Genel anahtarlarına ihtiyaç olduğu bilinmektedir. Her bir kişinin Genel anahtarı üzerinde kime ait olduğunu açıklayan bir etiket olmaz ise açma işlemini yapan kullanıcı; gelen bilgi için hangi anahtarı kullanacağını bulması çok zordur.* (Yükseliyor, s:1-3)

### 1.6 Sayısal Sertifikalar

Uluslararası örnekler incelendiğinde AAA, sayısal imza ve doğrulama amaçlı kullanıldığı görülmüştür. Devlette ise temel amaç olarak kağıt dolaşımını sınırlamak, işlerin elektronik ortamlarda verimli ve süratli bir şekilde yürütülmesi ve vatandaşa sunulan hizmetlerde etkinlik ön plana çıkmıştır. Amaç olarak, kağıtsız ofis, bilgi alma ve gönderme, sağlık işlemleri gibi uygulamalarda doğrulama yönü, elektronik ticaret ve finansal konularda ise sayısal imza yönü ön plana çıkmaktadır. Sunulacak servislere ve yapılacak işe bağlı olarak kurumların iş akış sistemlerinde ve yapılanmalarında önemli oranda değişim gerektirdiği, çok az uygulamanın "tak çalıştır" mantığıyla bağdaşabildiği tespit edilmiştir. Yine incelemeler, hizmette süreklilik için sertifikasyon makamları arasında eşgüdümü sağlayacak ve kök sertifikasyon makamının gerekliliği, sertifikasyon politikaları ile kişisel bilgilerin korunmasını sağlama yöntemleri ve ölçme tekniklerinin ayrılmaz bir bütün olduğunu göstermiştir. (TK, 2004c, s:2)

Sertifika Otoriteleri; bir kişinin veya öznenin Genel anahtarını bir sertifika içinde kime ait olduğunu da gösteren bilgi ile kullanıcılara temin eden bileşenlerdir. Sayısal sertifika, içinde genel anahtar ve kime ait olduğunu gösteren etiket bilgisi, geçerlilik süresi, sertifika üreten merci adının yer aldığı AAA bileşenleridir. Ancak Sertifika Otoriteleri bu bilgileri nasıl temin etmektedir sorusu aklımıza gelebilir. Kullanıcı ve özneler Sertifika Otoritelerine başvurarak; Genel anahtarlarının kopyalamasını ve genel anahtardan sertifika oluşturmasını talep etmektedir. (Yükseliyor, s:3)

# BÖLÜM II

# ELEKTRONİK İMZA

## 2.1 Sayısal-Elektronik İmza

İmza, bir yazının kimin tarafından yazıldığını veya içeriğinin tasdik edildiğini belli etmek amacıyla metnin altına konulan isim veya işarettir. İmza, bir yandan kişinin hüviyetini, diğer yandan da beyanda bulunma iradesini tespit eder. Böylece imzalayanın metni okuyup anladığı ya da belgeyi bizzat hazırlayan kişi olduğu ve bağlanma iradesinin varlığı anlaşılır.(Reed,2003 s:97)

İmza çok eski çağlardan beri değişik şekillerde kullanılmıştır. Örneğin Roma Hukukunda, bir sözleşmenin oluşturulabilmesi için, sözleşme yapan kişilerin mühür yüzüklerini balmumuna basarak metni mühürlemeleri gerekiyordu. Orta çağ boyunca Avrupa'da, belgeler, topraktan yapılmış mühürlerle mühürlenerek doğrulukları/güvenilirlikleri ispat edilmiştir. Daha sonraları, taraflar, el yazısı ile atılmış imzaları, sözleşmenin geçerliliğini ispat vasıtası olarak kullanmaya başlamışlardır.(Everett,1999 s:42)

Elektronik imza (e-imza) ise bir üst kavramdır. Her türlü elektronik ses, sembol veya uygulamayı kapsayan ve kullanılan teknolojiden bağımsız bir terim olduğundan bir üst kavram olarak kabul edilebilir. Ancak "*sayısal imza*" kavramı yerine kullanımına rastlamak da mümkündür.

Sayısal imzanın işlevi, elektronik ortamda aslından ayrılması güç olan sahte imzayı önlemek ve orijinal dokümanların olduğu şekilde, herhangi bir tahrip ve tahrife uğramaksızın iletilmesini sağlamaktır (Berber,2000). Bu nedenle sayısal imza, elektronik ortamın vazgeçilmez unsurlarından birisidir denilebilir.

Sayısal İmza; sanal dünyada kullanıcı ve öznelerin gerçek kimliğini ispat eden, her kullanıldığında farklı bir şekilde oluşan, imzalandığı doküman ve verinin içeriğine göre değişen ve doküman ve veriye eklenen, sözü edilen AAA özel anahtarı ile oluşturulan bir değerdir. (Yükseliyor, s:4)

5070 sayılı Elektronik İmza Kanunu'nda (EİK) ve bu çalışmada "elektronik imza" terimi sayısal imza ile eş anlamlı olarak kullanılmaktadır. 5070 sayılı

EİK'nda yer alan şekliyle e-imza; başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veriyi tanımlar. E-imza; bir bilginin üçüncü tarafların erişimine 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 oluşur.

Başka bir tanıma göre e-imza, ıslak imzanın fonksiyonlarını da 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 imzadır (Arıkan,1999).

E-imza altyapısı, bize, kimlik tespiti, bütünlük kontrolü ve inkâr edilemezlik gibi ıslak imza ile sağlanan fonksiyonların elektronik ortamda temin edilmesi için geliştirilen bir yöntemdir. (Orta)

Parmak izi, retina, yüz ve ses taraması gibi biometrik yöntemlerle oluşturulan veya PIN (Personal Identification Number) verilerek oluşturulan pek çok elektronik imza türü vardır. Ancak sayısal imza, güvenilirliği nedeniyle günümüzde en çok tercih edilen elektronik imza türüdür (ETKK, 1998a: 10).

### 2.2.E-İmza Tekniği

E-imza, "kişinin elle attığı imzanın sahip olduğu özellikleri elektronik ortamda gerçekleştiren matematiksel formüllere ve şifreleme programlarına verilen isimdir" (Berber, 2002). Çift anahtarlı şifreleme yöntemini kullanarak bilginin bozulmamış/ bütün olduğunu ve gönderenin kimliğini ispatlamak için atılan sayısal imza şunlara bağlı olarak oluşturulur: Gönderilen bilginin sayısal içeriği yani bilgisayarda sıfır/bir dizisi halinde gösterimi ve gönderenin gizli anahtarı (TUENA, 1998a: 3).

Bilginin gizliliğini sağlayacak olan şifreleme işlemi ise bilginin sayısal içeriğine ek olarak bilgiyi alacak olan kişinin kamuya açık anahtarını (uzun sayı dizisini) kullanarak yapılır. Sayısal imzanın doğruluğunu kanıtlamak için mesajı alan taraf kendisine gelmiş olan mesajın (ya da bilginin) sayısal içeriğini ve gönderen tarafın açık (ya da kamuya açık) anahtarını kullanır. Şifrelenerek gizlenmiş bir mesajın çözülmesi için ise mesajı alan taraf kendi gizli anahtarını kullanacaktır. Mesaj şifrelenirken alıcının açık anahtarı kullanılmış olduğundan,

alıcıdan başka birisinin bu alıcı için şifrelenmiş mesajı çözebilmesi mümkün değildir (ETKK, 1998b).

E-imza kriptografik bir dönüşüm olarak tanımlanabilir. E-imza, mesajın içeriği ile mesajı imzalayan kişinin asimetrik özel anahtarının beraber kullanılması ile elde edilir.

Açık elektronik ağlardan bilgi yollarken, kimliğini ispat etmek ve gönderdiği bilginin bozulmadan, bütün olarak yerine ulaştığını karşı tarafın denetleyebilmesini sağlamak isteyen her kullanıcı, yolladığı bilgiye sayısal imzasını ekleyecektir. (Öğüt, 2006, s:38)

Sayısal imzanın geçerliliğinin/ doğruluğunun saptanması için, imzayı atanın açık anahtarı gereklidir. Bu nedenle, hangi açık anahtarın hangi kullanıcıya ait olduğunun belgelenmesi, tüm sistemin güvenilirliğini ve güvenliğini belirleyen çok önemli bir etmendir (TUENA, 1998b, s:20).

Elle atılan imzanın değişmeyen biçiminin aksine, elektronik imza verisi değişken bir değerdir. E-imza; imzalanacak olan verinin, imzayı atacak şahsa ait özel anahtar ile birlikte birtakım matematiksel işlemlerden geçirilmesi sonucunda oluşturulan ve imzalanacak veriye eklenen sayısal bir veridir. (Selçuk, s:1)

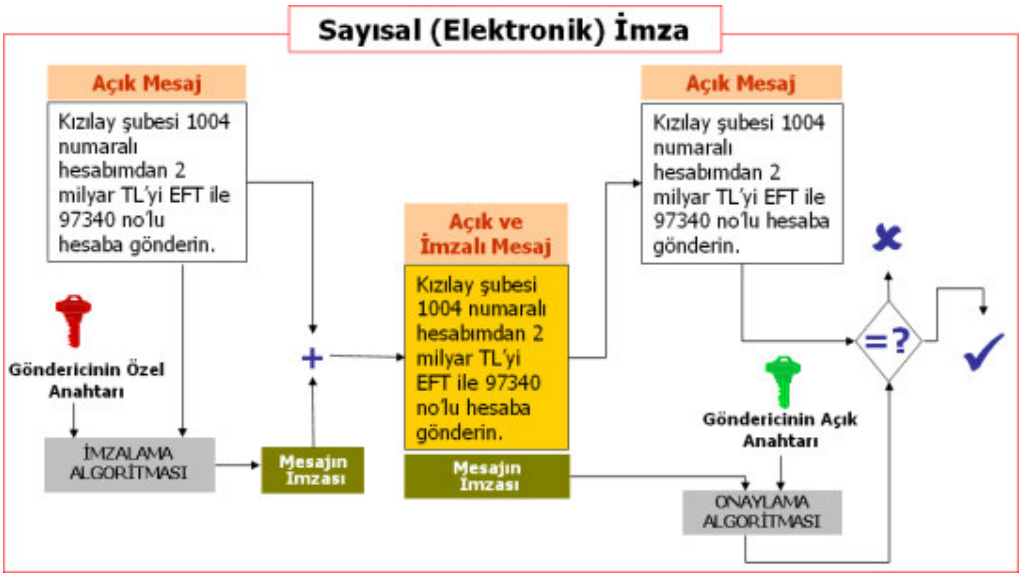
E-imza oluşturma işlemi için tanımlanmış söz dizimi, Kriptografik Mesaj Söz Dizimi (Cryptographic Message Syntax - CMS)'dir. CMS; imza oluşturmanın yanı sıra, özetleme, doğrulama ve isteğe bağlı mesaj içeriğinin şifrelenmesi için de kullanılır. (Selçuk, s:1)

Elektronik imza oluşturulurken kullanılan kriptografik algoritmalar zamanla zayıflamakta ve kırılabilir hale gelmektedir(CWA). 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. (Selçuk, s:5)

### 2.3 Mesaj Özeti

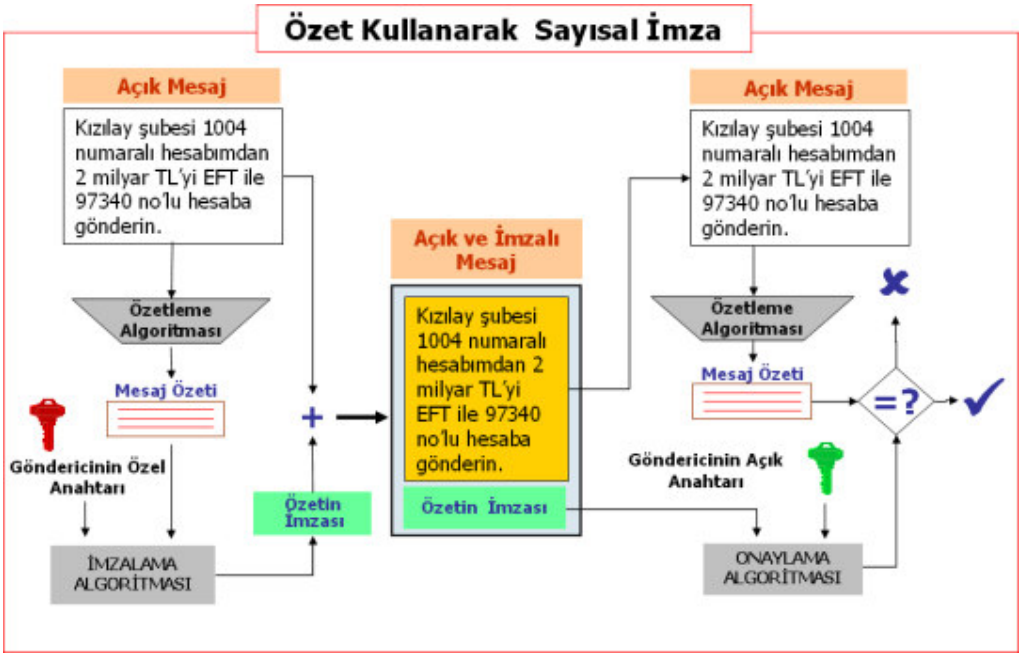
Sayısal imzanın bu şekilde kullanılması bir problemi beraberinde getirir. Bu kullanım şeklinde sayısal imza mesaj uzunluğunu iki katına çıkarır. Bu sorunu

çözmek için özetleme fonksiyonu kullanılarak bir "Mesaj Özeti" çıkarılır. Herhangi bir uzunluktaki veriyi alıp işleyen ve bu veriye özgü olan, sabit uzunlukta bir değer çıkaran algoritmalara mesaj özeti algoritması denir. Bu algoritmaların çıktısı olan değer, mesaj özetidir. En çok bilinen özet algoritmaları MD5 ve SHA ve ailesidir. (TÜBİTAK, 2007)




Şekil 10

Mesaj özeti elde etmek için kullanılan fonksiyonların özellikleri şunlardır: Özet fonksiyonları sabit çıkış uzunluğu üretirler (mesajdan çok kısa). Mesaj hangi uzunlukta olursa olsun MD5 fonksiyonu 128 bit uzunluğunda, SHA-1 fonksiyonu 160 bit uzunluğunda özet değeri üretir. Mesajdaki küçük değişiklikler bile özette büyük değişikliklere yol açabilir. Özet fonksiyonları kriptografik tek yönlü fonksiyonlardır. Bir mesajın özetini elde etmek çok kolaydır, bir özetten asıl mesajı çıkarmak ise çok zordur. Mesaj özeti kullanarak sayısal imzalama aşağıdaki gibi yapılır:




Şekil 11

Başka bir deyişle, teknik açıdan sayısal imza, imzalanmış belgenin özünü (hash) içermektedir. Bilgisayar terminolojisinde öz değeri (hashwert), yazılan bir mesajın kısaltılmış şeklidir. Bu bakımdan içerikte yapılacak herhangi bir değişiklik, sayısal hash'i geçersiz kılacaktır. Hazırladığı mesajı imzalamak isteyen kullanıcı, mesajının hash değerini hesaplayabilmek için bir hash fonksiyonu kullanacaktır. Bu şekilde hash değeri, gizli anahtar ile şifrelenmiş olacaktır. Belgenin hash değeri belli olduğu için, mesajı alan taraf, bu değeri mesajı gönderenin açık şifresi yardımıyla tespit edebilecektir. Alıcı ayrıca, hash fonksiyonunu deşifre edilen mesaja da uygulayarak, her iki değeri birbiriyle karşılaştırabilmektedir (Berber, 2000: 524-525).

### 2.4 Zaman Damgası

Günlük yapılan işlerde, kargaşaya mahal vermemek için yapılan işlemlerden birisi de, işlemlerin çoğunda tarih bilgisi kullanmaktır. Eğer kullanılmaz ise, işlemlerde, haberleşmede, ilişkilerde ve işlerde problemler çıkabilmekte, kişiler zarar görmekte ve kurumlarda kayıplar oluşabilmektedir. (Sağıroğlu ve Alkan, 2005, s:72)

E-imzanın belirli bir tarihten önce var olduğu zaman damgası ile ispat edilebilir; ancak, imzanın geçerli olabilmesi için imzanın atılmış olduğu sertifikanın

da bu tarihte geçerli olduğunun ispatı gerekmektedir. Bu nedenle, imzaya sertifika kontrolü için gerekli imzacı sertifikasının üst kök sertifikalar zinciri ve bu sertifikalara ait iptal bilgisinin kontrol edilebileceği bilgiler de eklenmelidir. Ancak, bu bilgiler imzaya eklendiğinde imzanın boyutu çok büyüyeceğinden bu bilgilere ait özet değerler imzaya eklenerek, bilgilerin imza kontrolü sırasında erişilebilecek başka bir yerde saklanması sağlanmalıdır. (Selçuk, s:3)

### 2.5. E-İmzanın Özellikleri

Yazılı dokümanlarda kullandığınız imzalar gibi, e-imzalar da günümüzde e-posta veya elektronik verilerin yazarlarını/sahiplerini tanılamada kullanılmaktadır. Elektronik imzalar, Elektronik Sertifikalar kullanılarak yaratılır ve doğrulanırlar. Bir bilgiyi imzalamak, güvenli bir alışverişi gerçekleştirmek için kendi özel Elektronik Sertifikanıza ihtiyaç vardır. Günümüzde uluslararası yasama organları e-imzaları ıslak imzalar gibi yasal olarak bağlayıcı ve uluslararası çapta kabul edilebilir kılmak için yasalar çıkarmışlardır.

E-imzanın kullanımın dünya çapında kabul görmesinin ve gittikçe yaygınlaşmasının sebeplerini şöyle sıralayabiliriz;

- E-imza güvenilirdir,
- E-imza taklit edilemez,
- E-imza yeniden kullanılamaz,
- E-imzalı metin değiştirilemez ve
- E-imza inkar edilemez.

E-imzaların sağladığı başlıca önemli işlevleri şöyledir:

- Tanılama,
- Gizlilik,
- Veri bütünlüğü ve
- İnkar-edilememe.

#### 2.5.1. Tanılama

Bir kişinin (veya sunucunun, müşterinin...) kimliğini doğrulamadır. Veriyi imzalayan kişinin yetkinliğini garanti ederek işleme kimin dahil olduğunu yada

mesajın gerçekten kimden geldiğini karşı tarafa gösterir. Ayrıca tanılama işleminin doğru olarak yapılabilmesi için sayısal sertifikayı veren kurumun tarafsız, güvenilir ve dünya çapında tanınıyor olması gerekmektedir.

### 2.5.2. Veri bütünlüğü ve gizlilik

E-imzalar verinin bütünlüğünü koruyarak okuduğunuz mesajın, kazayla veya kötü niyetle size gelene kadar değişmediğini veya değiştirilmediğini garanti eder. Teknik olarak anlatmak gerekirse, sayısal olarak imzalanan dokümanın hash denilen küçük bir özü tutulur. İmzalama işleminin ardından dokümanda yapılacak herhangi bir değişiklik, bu sayısal özü farklı yani geçersiz kılacaktır. Verinin gizliliği, alıcının açık anahtarının mesajı şifrelemede kullanılması sayesinde gerçekleştirilir .

### 2.5.3. İnkar edememe

E-imzanın bir özelliği de, mesajın yazarına (imzalayanına) kimliğini kanıtlama şansı vermesidir. İnkar edilememe ileride bir işleme veya iletişime kimlerin katıldığını kanıtlamanıza imkan vermesidir. Bir dokümanı imzalayan veya o dokümanı alan kişi daha sonra söz konusu işlemleri yapmadığını inkar edemez. Basitçe inkar-edememe, bir kağıt doküman üzerindeki ıslak imzaya yapılan şahitlik gibi, bilginin yadsınamamasıdır.

## 2.6. Elektronik Sertifika Hizmet Sağlayıcısı

Sayısal imza kavramının yasal güvenilirlik kazanabilmesi için, kullanıcıların açık anahtarlarını onaylama yetkisine sahip bir kuruluşa, bir otoriteye gereksinim vardır. Elektronik Sertifika Hizmet Sağlayıcısı (ESHS), herhangi bir kullanıcının kimliğini kontrol ederek, bu kimliğin hangi açık anahtara sahip olduğunu belgeleyebilen ve bu belgeyi ESHS'na ait sayısal imza ile onaylayarak, diğer bütün kullanıcıların bu kullanıcının imzasını tanıyabilmelerini, doğrulayabilmelerini sağlayan bir kuruluştur. Elektronik sertifika, ESHS tarafından hazırlanarak kullanıcılara verilir ve bir kopyası ESHS'nın herkese açık olan erişim bölgesine kaydedilir. ESHS tarafından hazırlanarak kullanıcılara verilen elektronik sertifikalar, sahibinin kimlik bilgilerini, açık anahtarını, belgenin kullanım süresini, seri numarasını, belgeyi veren ESHS'nın adını ve sayısal imzasını taşımalıdır. ESHS, kişilerin açık anahtarlarını ve kimliklerini eşleştiren sertifikaların hazırlanmasında çok titiz davranmak, başvuruda bulunanın kimliğinden kesinlikle emin olacak yöntemler geliştirmek durumundadır.

5070 sayılı EİK ve ilgili ikincil mevzuat gereğince ıslak imza ile aynı hukuksal etkiye sahip e-imza kullanımı yasal bir tabana oturtulmuş ve 2004/21 sayılı Başbakanlık Genelgesi ile kamu kurum ve kuruluşlarının e-imza ile ilgili sertifika ihtiyaç ve işlemlerinin TÜBİTAK-UEKAE bünyesinde kurulmuş olan Kamu Sertifikasyon Merkezi tarafından yürütülmesi kararlaştırılmıştır. Bu düzenleme ışığında hukuksal açıdan geçerliliği olan e-devlet işlemlerinde e-imza kullanma gerekliliği açıktır.

Ayrıca, kamu kurum ve kuruluşları dışındaki kuruluşlar ve gerçek kişiler için nitelikli sertifika hizmeti Telekomünikasyon Kurumu (TK) tarafından yetkilendirilmiş özel sektör sertifika hizmet sağlayıcıları tarafından yürütülecektir. (Başbakanlık, 2005 s:14)

Çift (açık) anahtarlı bir kriptografi sisteminde, kullanıcının gizli-açık anahtar çiftinin oluşturulması ESHS tarafından yapılabileceği gibi, kullanıcı tarafından da yapılabilir. Buradaki önemli nokta, anahtar görevini yapacak sayı dizilerinin, belirli bir kriptografik algoritmanın gerektirdiği kurallara uygun olması ve belirli bir uzunluktan daha kısa seçilmemesidir. Bu sayı dizilerinin uzunluğu, sistemin güvenilirliğini, açık anahtar bilgisiyle gizli anahtarın hesaplanamamasını, ayrı kullanıcılara ayrı anahtarlar verilebilmesini ve sayısal imzanın taklit edilememesini sağlayan önemli bir faktördür. Günümüzde 512 ikil uzunluğunda anahtarlar oldukça güvenli kabul edilmektedir. Çok gizlilik gerektiren uygulamalarda 1024 ikil uzunluğuna kadar çıkılmaktadır (TUENA, 1998a: 11).

ESHS'nın değil de kullanıcının anahtar çiftini oluşturduğu durumda da, kullanıcının ESHS'na başvurarak elektronik sertifikasını alması, ve bu sertifikayı ESHS'nın açık erişim bölgesine kaydettirmesi atacağı sayısal imzanın diğer kullanıcılar tarafından tanınabilmesi için gereklidir. ESHS'nın hazırladığı ve tüm kullanıcılara açık tuttuğu erişim bölgesinin içinde bulunan elektronik sertifika bilgileri, her değişiklikte (yeni bir kullanıcı, süresi dolan elektronik sertifika, gizli anahtarını kaybettiği için elektronik sertifikasını iptal ettirmesi gerekenler vb.) hızlı bir şekilde uyarlanmalıdır. Bu uyarlamanın hızı, sistemin güvenilirliğini ve etkinliğini doğrudan etkileyeceği için oldukça önemlidir (TUENA, 1998a. 12).

### 2.7. 5070 Sayılı Elektronik İmza Kanunu

Avrupa Birliği ile üyelik süreci açısından Türkiye, ulusal programında e-Avrupa'ya paralel "e-Türkiye" girişimini başlatma kararı ile yanıt vermiştir. E-Türkiye girişimi Başbakanlık Müsteşarlığı'nın koordinasyonunda yürütülmeye başlanmıştır. Daha sonra 58. Hükümet tarafından hazırlanan Acil Eylem Planı'nda "e-Dönüşüm Türkiye Projesi"ne yer verilmiş; söz konusu projenin koordinasyonu, izlenmesi, değerlendirilmesi ve yönlendirilmesi ile ilgili olarak Devlet Planlama Teşkilatı (DPT) Müsteşarlığı görevlendirilmiştir. (Başbakanlık, 2003).

Elektronik devlet ve ticaretin en önemli hukuki ve teknik altyapısını oluşturması beklenen EİK'nun ilk taslağı, Dış Ticaret Müsteşarlığı'na (DTM) bağlı Elektronik Ticaret Koordinasyon Kurulu (ETKK) tarafından hazırlanmış ve tartışmaya açılmıştır. 1998 yılında ETKK bünyesinde hukuk, teknik ve finans çalışma grupları oluşturulmuştur. Hukuk Çalışma Grubu tarafından hazırlanmış olan Temmuz 2000 tarihli çalışma sonuç belgesinde, e-imzanın hukuken tanınması için bir kanun taslağının hazırlanmasına değinilmiş ve bu konuda Adalet Bakanlığı'nın çalışmalarının beklenmesine karar verilmiştir. Hukuk Çalışma Grubu Haziran 2001'de tekrar toplanmış; bu toplantıda e-imza ile ilgili kanun taslağını hazırlamak üzere Adalet Bakanlığı, Gümrük Müsteşarlığı, DPT Müsteşarlığı, Merkez Bankası, Telekomünikasyon Kurumu, PTT Genel Müdürlüğü ve DTM temsilcilerinden oluşan Hukuk Alt Çalışma Grubu kurulmuştur. Hukuk Alt Çalışma Grubu çalışmalarına Temmuz 2001'de başlamış ve "Elektronik Veri, Elektronik Sözleşme ve EİK Tasarısı Taslağı"nı hazırlanmıştır. Hazırlanmış olan taslak, Nisan 2002'de Başbakanlığa gönderilmiştir (Çamurdan, 2003, s:52-54).

ETKK Hukuk Grubu'nun çalışmaları devam ederken Adalet Bakanlığı 14 Ocak 2002 tarihli yazısı ile çeşitli kurum ve kuruluşlardan elektronik imzanın düzenlenmesine ilişkin kanun tasarısı taslağının hazırlanması için oluşturulacak komisyona temsilci bildirilmesini talep etmiştir (Çamurdan, 2003, s:52-54).

"E-imzanın Düzenlenmesi Hakkında Kanun Tasarısı" Bakanlar Kurulu tarafından kabul edildikten sonra 9 Haziran 2003 tarihinde Türkiye Büyük Millet Meclisi'ne (TBMM) yasalaşması amacıyla gönderilmiş ve meclis komisyonlarından geçerek Genel Kurul'da 15 Ocak 2004 tarihinde yasalaşmıştır. EİK, 23 Ocak 2004 tarihinde Resmi Gazete'de yayımlanmış ve kanunun 25. maddesi doğrultusunda 23 Temmuz 2004 tarihinde yürürlüğe girmiştir. Kanun metni **EK-B'** dedir.

5070 Sayılı EİK, Avrupa Komisyonu'nun 99/93/EC numaralı direktifi çerçevesinde hazırlanmıştır. Bu nedenle kendisine kaynaklık eden Avrupa Birliği (AB) e-imza direktifinin temel aldığı açık anahtarlı altyapı teknolojisi üzerinde işlevsellik gösteren e-imzayı düzenlemektedir (TK, 2004a: 18-19).

Yasaya kaynaklık eden 99/93/EC Sayılı Direktif elektronik imzalarla ilgili temel hukuksal çerçeveyi ve bu hukuksal çerçevenin en önemli bileşenlerinin statüsünü düzenlemeyi hedeflemektedir. Direktif aynı zamanda Birliğin hukuk siyasetini de açıkça ortaya koymakta ve dünyadaki tüm medeni milletlerin de takip ettiği gibi bu siyasetin sonucu olarak belli bir teknoloji hedef alınmaktadır. Bu teknoloji AAA teknolojisidir. Birlik Direktifin düzenlenmesinden önce kamuoyundan aldığı görüşler ve yaptığı hukuksal risk değerlendirmeleri ile AAA üzerinde geliştirilen uygulamaların hukuksal bir değer kazanması gerekliliğine karar vermiştir. Birlik bununla birlikte diğer teknolojilerin ve bu alt yapı üzerinde geliştirilebilecek diğer uygulamaların da önünü açmak için Direktif'te teknoloji yansızlık (technology neutrality) yaklaşımının bir ifadesi olarak olarak "e- imza"yı çok geniş bir çerçevede tanımlanmıştır. Bu tanım Kanunumuzdaki "e-imza" tanımının aynısıdır. (Beder, 2005)

Kanuna göre e-imza "başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri"dir. Bu tanım AB e-imza direktifinin çevirisi şeklindedir. Çalışmanın ikinci bölümünde açıklandığı gibi elektronik imza bir üst kavramdır. Kanunun e-imza tanımının ikinci kısmı ise bu noktada önem kazanmaktadır, çünkü parmak izi, retina, yüz ve ses taraması gibi biometrik yöntemlerle oluşturulan e-imzalar her ne kadar kimlik doğrulama amacıyla kullanılabiliyor da olsa eklendikleri veriyle "mantıksal bağlantı"ları yoktur. Bu anlamda kanunun ismi her ne kadar "EİK" da olsa kanunla düzenlenen "eklendiği veriyle mantıksal bağ kuran" sayısal imzadır (Tüfekçi, 2003 s:2-3).

5070 Sayılı EİK güvenli bir e-imzanın sahip olması gereken özellikleri ise şöyle sıralamaktadır: "münhasıran imza sahibine bağlı olan, sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan, nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan, imzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan elektronik imza". Bu tanımda yer verilmiş olan

güvenli elektronik imza oluşturma araçlarına ilişkin düzenlemelerin ise ayrıca düzenlenmesine karar verilmiştir. (Öğüt, 2006, s:103)

Ülkemizde gerek devlet gerek özel sektör gerekse de Silahlı Kuvvetler açık anahtar alt yapı uygulamalarını kullanmakta bu konuyla ilgili AR-GE yatırımları yapılmakta ve bu uygulamanın etkin olacağı kullanım ve güvenlik alanları oluşturulmaktadır. (Beder, 2005)

### 2.8. Türkiye'de E-İmzanın Hukuki Altyapısı

E-imzanın kullanımı konusunda halihazırda geçerli bulunan mevzuat şunlardır:

- 5070 Sayılı Elektronik İmza Kanunu **(EK-A)** (23 Ocak 2004)
- Elektronik İmza Kanununun Uygulanmasına İlişkin Usul Ve Esaslar Hakkında Yönetmelik (6 Ocak 2005 R.G. 25692)
- Kamu Sertifikasyon Merkezi Oluşturulması Hakkında Genelge
- Sertifika Mali Sorumluluk Sigortası Yönetmeliği (26 Ağustos 2004 R.G. 25565 )
- Sertifika Mali Sorumluluk Sigortası Tarife ve Talimatı (27.01.2005 R.G.25709)
- Zorunlu Sertifika Mali Sorumluluk Sigortası Genel Şartları (27.01.2005, R.G. 25709)
- Elektronik İmza İle İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ (06 Ocak 2005,ve R.G.25692)
- Elektronik İmza İle İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de Değişiklik Yapılmasına Dair Tebliğ.

#### 2.8.1. Mevcut Mevzuatta E-İmza Kullanımı

Türkiye'de 5070 Sayılı "EİK" dışında da e-imza kullanımına izin veren, aynı zamanda belli kurumlara e-imza kullanım usul ve esaslarını düzenleme yetkisi tanıyan kanunlar bulunmaktadır. Bu kanunlardan en önemlileri Sermaye Piyasası Kanunu, Vergi Usul Kanunu ve Nüfus Kanunu'dur. Henüz yürürlüğe girmiş olmadığı halde içerik açısında önem arz eden ve anılan Kurumların e-Devlet uygulamaları sürecinde açık anahtar altyapısı teknolojisine kayıtsız kalmayacaklarını göstermesi bakımından önem taşıyan, iki adet Kanun Hükmünde

Kararname ve yürürlükte olan bir Yönetmelik mevcuttur.Bunlar sırasıyla; “Sosyal Sigortalar Kurumu Başkanlığının Kurulması ve Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılması Hakkında Kanun Hükmünde Kararname”, “Türkiye İş Kurumunun Kurulması İle Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılması Hakkında Kanun Hükmünde Kararname” ve “İyi Laboratuar Uygulamaları Prensipleri ve Test Laboratuarları’nın Belgelendirilmesine Dair Yönetmelik”tir.

Sermaye Piyasası Kanunu ve Vergi Usul Kanunu elektronik imzanın kullanımına izin vermenin dışında aynı zamanda Sermaye Piyasası Kuruluna (SPK) ve Maliye Bakanlığına elektronik imza kullanımının usul ve esaslarını belirleme yetkisi vermektedir. Nüfus Kanunu’nda ise sadece e-imzanın kullanımına izin verilmekte ve İçişleri Bakanlığına bu yetki tanınmamaktadır. Bahsi geçen Kanunlar tarafından yetki verilen Kurumların “Sertifika Hizmet Sağlayıcıları”nı seçme ve bu Kurumları denetleme hakları da olacaktır. Ancak, gerek “EİK”, gerek “Elektronik Haberleşme Kanunu Tasarısı” e-imzanın kullanımı ve buna ilişkin usul ve esasların belirlenmesi konusunda genel yetkili otorite olarak “TK” belirtilmektedir. Kanunlar arasında uyumsuzluk yaratan bu durumun yorumu ise özellikle Maliye Bakanlığı ve SPK’nun yetki ve görev alanına giren kurumlarla iş yaparken TK yanında bu kurumlarında denetime yetkili olması gibi yetki ve görev karmaşası meydana geldiğinde önemli olacaktır. (Sevim,2004 s:24)

### 2.9. Güvenli E-İmzanın Hukuki Sonuçları

#### 2.9.1. Elle atılmış imza ile aynı hukuki sonuçları doğurması

Kanun'a göre "Güvenli e-imza, elle atılan imza ile aynı hukukî sonucu doğurur". Bu hüküm Direktif Md 5/1'ine uygundur. Direktifteki Md. 5/1'e göre nitelikli sertifikaya dayanan ve güvenli imza oluşturma aracı ile oluşturulan imzaların hukuki etkisi elle atılmış imza ile aynı olmalıdır ayrıca bu imzanın delil niteliği inkar edilmemelidir. (Beder, 2005)

#### 2.9.2. E-İmzanın Delil Niteliği

Kanunun 23. maddesi ile Hukuk Usulü Muhakemeleri Kanunu'nun 295. maddesine eklenmesi kararlaştırılan 295/A maddesinin birinci fıkrasında "güvenli e-imza" ile oluşturulan elektronik veriler senet hükmündedir. Bu veriler aksi ispat edilinceye kadar kesin delil sayılırlar" denilmektedir. Güvenli e-imza ile imzalanmış belgeyi senet ve aksi ispat edilinceye kadar kesin delil kabul edileceğini tespit eden bu madde, hakimin takdir yetkisini kısıtlaması yönünde tenkit edilebilir ise de Birleşik Devletler' de bir çok eyalet elektronik imza ile imzalanmış belgeleri kesin delil olarak kabul etmekte ve bunların ispat kuvvetini de kesin delil olarak sayılan diğer delillerden daha üstün tutmaktadır. (Beder, 2005)

### 2.9.3. E-İmza ile Yapılamayacak Hukuki İşlemler

Kanun'un 5. Maddesinin 2. Fıkrası uyarınca "Kanunların resmî şekle veya özel bir merasime tabi tuttuğu hukukî işlemler ile teminat sözleşmeleri güvenli e-imza ile gerçekleştirilemez". Güvenli e-imzanın uygulama alanın gösterildiği bu maddeye göre noterlerin yapacağı işlemler, noterlerin huzurunda yapılan işlemler, resmi bir makamın katılımını veya tescil zorunluluğu gerektiren işlemler (gayrimenkul, motorlu araç alım satımı v.b.) ile evlenme gibi resmi memur önünde gerçekleştirilmesi zorunlu olan hukuki işlemler güvenli e-imza ile yapılamazlar. Kanun metninde güvenli e-imza ile yapılamayacak hukuki işlemlerin genel bir ifadeyle tanımlanması bazı karışıklıklara sebebiyet verebilecektir. Özellikle doktrinde tartışmalı olan "teminat sözleşmeleri" türleri ile "kanunun özel bir merasime tabi tuttuğu hukuku işlemler" uygulamada tereddüt yaratacak en önemli hususlardır. (Beder, 2005)

# BÖLÜM III

# E-İMZA'NIN EKONOMİK BOYUTU VE E-TİCARET

## 3.1. Küresel Ticaret ve Bilgi Ekonomisi

Özellikle 1980'li yıllarda ekonomide yaşanan önemli değişim ve dalgalanmalar; (enflasyon, uluslararası rekabet, gelişmiş ülkelerde yaşanan verimlilik azalışı, tüketici Küreselleşme ile birlikte dünya çapında büyük bir değişim rüzgarı esmektedir. Değişim rüzgarı aslında iki boyutta esmekte (Kazgan, 1997): Bir yandan teknoloji devriminin haberleşmede yarattığı olağanüstü hızlanma ve alan genişlemesi var; elektroniğin sadece haberleşmede yarattığı devrimle kalmayıp, ekonominin her kesiminde yeni olanaklar ve üretim biçimleri; dünyayı yerleşen deyimiyle "Küresel Köy"e döndürecek kadar küçültmesi, uzaya açılmada yeni boyutlar eklemesi; diğer yandan da serbest piyasa ekonomisi -serbest dış ticaret-serbest sermaye hareketleri. (Akolaş)

Teknolojinin giderek insanların günlük yaşamında etkinlik kazanması, teknolojik bilgilerin -yeni buluş ve yenilikler, AR-GE çabalarının sonuçlarını kapsayan bilgiler birikiminin giderek artmasına, raporların, bilimsel yazıların patentlerin sayılarının hesaplanamayacak ölçülere ulaşmasına yol açmıştır (Dalgıç, 1982). Bu durumda bilgide yaşanan önemli dönüşüm-bilginin anlamında ve kullanımında gelecekte bilginin tamamıyla sayısal olacağını düşündürmektedir. Çünkü sayısal hale gelen bilgi, bir kez depolandığında, kişisel bilgisayar yoluyla erişim izni olan herkes tarafından anında çağrılabilir, karşılaştırılabilir ve yeniden biçimlendirilebilir (Gates, 1999a). Bu yüzden, toplumun her kesiminin verimli ve etkili bilgi kullanımını, iletişimini ve dağıtımını sağlayacak bilişim teknolojisine dayalı ortamları oluşturmaları zorunlu hale gelmiştir. (Akolaş)

Bilginin yaratıcı kullanımı, bilişim teknolojisine hem stratejik önem kazandırmış hem de yönetsel etkinliğin önemli bir dayanağı haline gelmiştir (Düren, 2000). Çünkü yönetsel kararların birçoğu hassas bilişim sistemleri ve bilişim teknolojisi desteği olmaksızın etkin olarak uygulanamamakta ve örgütü rekabetçi bir örgüte dönüştürememektedir (Akın, 2001) .

Bu bağlamda bilişim teknolojisi kavramı incelendiğinde, bu kavram ile; kuruluşlara bilgi sağlamak için kullanılan ve hızla gelişmekte olan araçların (bilgisayar,veri toplama araçları, ağ ve iletişim araçları), uygulamalar ve hizmetlerin tamamının kastedildiği görülmektedir (Güvenen, 1998). Bilişim teknolojisi ile ilgili pek çok değişik tanım yapılabilir. Kimileri bilişim teknolojisini "bilginin bilgisayarlar vasıtasıyla elde edilip, işlenmesi, saklanması ve gerekli yerlere gönderilmesi" (Bennet, 1994) olarak tanımlarken, kimilerine göre de , "bilginin toplanması, işlenmesi, saklanması ve yayımında, mühendislik ve yönetim tekniklerinin kullanıldığı teknolojiler ve bunlarla ilişkili, sosyal, ekonomik ve kültürel yapılanmalar" (Akpınar, 2001) bilişim teknolojisini oluşturmaktadır. En genel şekliyle, "bilişim teknolojisi, bilginin mevcut bilgisayar ve telekomünikasyon teknolojileri ile işlenmesi" (Akdağ ve Diğerleri, 1996) olarak tanımlanmıştır. (Akolaş)

Bilişim teknolojisi kullanımının her alanda önemli sonuçları bulunmaktadır. Bu sonuçlardan biri de; işletmelerde üretim sürecini, üretim ve iş proseslerini değiştirmesi, çalışanları yavaş ve katı kağıt proseslerinden kurtarmasıdır (Gates, 1999b) . Başka bir deyişle, yaratıcı, yenilik getirici ve etkinlik sağlayıcı özellikler ile bilişim teknolojisi üretim ve iş süreçlerine egemen olma eğiliminde olup, bilgisayar destekli tasarım ve üretim teknolojileri, telekomünikasyon ağları, uzman üretim sistemleri, bilgiye dayalı dağıtım organizasyonları, organizasyonlar arası bilgi sistemleri multi-medya ve yönetici bilgi sistemlerini ön plana çıkartmaktadır (Akgeyik, 1998) . Bu bağlamda yeni teknolojik sistemleri kullanan örgütlerin ömürlerinde iyileşme görülerek uzadığı da söylenmektedir (Haşıloğlu, 1999) .

Gerek yerel gerekse uluslararası düzeyde giderek yoğunlaşan bir rekabet ortamında, ülke ekonomisini diğer ülkelerle eşit şanslarla donatmak için, Bilgi ve İletişim Teknolojileri altyapısının güçlendirilmesine de aynı önem verilmek zorundadır. Ulusal bir sözleşme ile garanti altına alınmış hedeflere yönelik olarak, yine ulusal ölçekte işbirlikleri ve ortaklıklarla kurulan, kamu, iş dünyası, sivil toplum kuruluşları ve giderek tüm yurttaşları kapsayacak bir biçimde katılımcı bir bilgi toplumu ağının oluşturulması, bilgi ekonomisine geçişin sürekliliğini sağlayacak, dinamiklerini kalıcı kılacak asıl örgütlenme modeli olarak belirmektedir. Ancak böyle bir ağ yapılanması ile, toplumu gerçek bilgi temelli

dönüşüme uğratacak, değer yaratımını güvence altına alacak bilgi temelli bir ekonomi kurulabilir. (İİK, 2004)

Günümüzde işletme faaliyetlerinde bilişim teknolojisi, stratejik başarı için hayati bir öneme sahiptir. M. Porter'a göre, günümüzün rekabetçi işletmelerinde, bilişim teknolojileri uygulamaları işletmenin yönetilmesi için önemli bir konuma yerleştikleri için, genel işletme stratejisinin bir bölümünü oluşturmaktadır. Bilişim teknolojilerinin, işletmelerin yönetim faaliyetlerindeki değişimde de önemli etkileri olmaktadır. Bilişim teknolojileri, yönetim faaliyetlerindeki bürokratik işlemlerin azalmasında, işletme içi ve dışı iletişimin artmasında, çalışanların denetiminde ve yönetsel kararların etkinliğinin sürdürülmesinde önemli katkılar sağlamaktadır.

Ülkenin bilim ve teknoloji sistemiyle üretim arasında bütünlüğün sağlanamadığı durumlarda, bilim ve teknolojide yeni olan bilgiler ve araştırma yeteneğine sahip insan gücü üretim sistemine taşınamaz; üretim sisteminin değişen beyin gücü ve bilgi gereksinimleri zamanında karşılanamaz ve üniversite-sanayi arasında yaşamsal önemdeki işbirlikleri gerçekleştirilemez. Bunun en canlı örneği Sovyetler Birliği ekonomi sistemi ile Japon ekonomi sisteminin karşılaştırılması sonucunda ortaya çıkmaktadır. Belirli bilim ve teknoloji alanlarında Japonya'nın çok ilerisinde olan Sovyetler Birliği'nde, bilim, teknoloji ile üretim sistemlerinin buluşturulamaması ekonominin çöküşünde çok önemli bir rol oynarken, bilim ve teknoloji sistemi ile üretim sistemi arasındaki etkileşimin önemini ve inovasyondaki sistematik ilişkiyi çok iyi kavrayan Japonya dünyanın başlıca teknolojik güç odaklarından birisi haline gelmiştir. (İİK, 2004)

Bilgi ve İletişim Teknolojilerinde oldukça hızlı yaşanan değişim ve dönüşüm süreci tüm dünya ülkelerinde olduğu gibi ülkemizi de yakından ilgilendirmekte ve etkilemektedir. Bu değişim ve dönüşüm sürecine uygun düzenlemeleri zamanında ve doğru olarak gerçekleştirmek oldukça önem arz etmektedir. (Alkan ve İnalöz, 2003)

Son yirmi yıldır Türk ekonomisi giderek daha rekabetçi ve küresel pazarlara daha açık hale gelmektedir. Bu yapısal dönüşümle birlikte, yeni teknolojilere erişim kolaylaşmakta, ürün ve hizmet üretiminde süreç-yönelimli bir iyileşme göze çarpmakta, maliyetler rasyonalize olmakta ve verimlilik artmaktadır. Ancak aynı küreselleşme dinamiği, rekabet avantajının ve büyüme ivmesinin sürdürülebilir kılınmasını da zorlaştırmaktadır. Türkiye henüz küresel ekonomide geniş yerel

pazarının gücünü, ucuz emek ve uygun coğrafi konum avantajlarını yeterince kullanmaktan uzaktır. (İİK, 2004)

Bilgi Ekonomisine geçmek, küresel rekabet avantajlarımızı güçlendirmek; üretkenliğimizi ve kalite standartlarımızı yükseltmek; milli geliri artırmak ve adil gelir dağılımını sağlamak; sürdürülebilir istihdam kanallarını yaratmak; ulusal eğitim ve öğrenim sistemimizi iyileştirmek, yani sürdürülebilir bir kalkınma ivmesi yaratmak için temel bir koşuldur. (İİK, 2004)

### 3.2. Elektronik Ticaret

İlk çağlardan itibaren insanoğlu ticareti öğrenmiş ve günlük hayatın bir parçası olarak kullanmıştır. İhtiyaçların giderilmesi için, belirlenen nispi bir değer üzerinden mübadele (takas) yapılarak, eldeki mallarla diğer ihtiyaçların karşılanması yoluna gidilmiştir. Yapılan bu ticarette, süt verilerek bal alınmış. Karşılıklı olarak yapılan bu ticarette, insanların güvenini birbirlerini çok iyi tanımaları sağlıyordu. Bu kadar küçük ve güvenin yoğun olduğu bir ortamda ticaret yapmak elbette çok kolaydı. (Kuran, 2004 s:2)

Ticaretin gelişmesine bakıldığında, akidlerin yani yazılı ve sözlü anlaşmaların çok önemli bir yere sahip olduğunu görüyoruz. Bu akidler sayesinde vade kavramı gelişmiş ve iki taraf arasında yapılan anlaşma ve sözüne ve dürüstlüğüne güvenilir bir tanık ile anlaşma yapılarak, ticaretin gelişmesi sağlanmıştı. Bu anlaşmalar uluslararası boyutlarda da kullanılmaya başlandı. Ve hala ticaretin en önemli araçlarından birisidir. Günümüze gelindiği zaman ise, sermaye kuruluşları ve şirketlerin gelecek bir yıl içersinde yapması muhtemel sözleşme, anlaşma ve karlılık oranlarına bakarak yatırım yapılmakta buna karşın ilgili kuruluşların hisse senetleri alınmaktadır. Yani daha gelecekte olacak bir takım gelişmelere göre ticaret yapılmaktadır. (Kuran, 2004 s:2)

Ticaretin gelişmesinde, insanlık olarak epey bir yol kastettiğimiz söylenebilir. Şimdi başka bir devir başladı. Ticaretin "E"-leşmesinden bahsediyoruz. Dijital çağ ile birlikte oluşan bilgi ekonomisi, emek yoğun bir sermayeden bilgi yoğun bir sermaye geçişi sağlayacaktır. (Kuran, 2004 s:2)

Elektronik ticaret (e-ticaret), 20. yüzyılın son döneminde bilgi ve iletişim teknolojilerinde yaşanan hızlı değişim ve gelişmelere paralel bir şekilde ve giderek

artan ölçüde dünya genelinde tartışılan bir kavram olarak karşımıza çıkmaya başlamıştır. (Alkan ve İnalöz, 2003)

E-ticaretin tanımı tam olarak yapılamamaktadır. E-ticaret bazı yorumlara göre; elektronik araçlarla yapılan tüm ticari işlemlerdir. Bazı yorumlara göre de sadece internet üzerinde yapılan işlem ve ödemeleri e-ticaret olarak saymak mümkündür. Uluslararası organizasyonlar da e-ticareti farklı şekilde tanımlamışlardır. Bu tanımlar aşağıda verilmiştir. (Gökçen,2006)

Dünya Ticaret Örgütü'nün (WTO) tanımına göre; E-ticaret, mal ve hizmetlerin üretim, reklam, satış ve dağıtımlarının telekomünikasyon ağları üzerinden yapılmasıdır. (WTO, 1998)

OECD'nin (Organisation for Economic Co-operation and Development) yani Ekonomik İşbirliği ve Kalkınma Teşkilatı'nın tanımına göre; E-ticaret, kurumların ve bireylerin katıldığı ve metin, ses ve görsel imaj gibi sayısallaştırılmış verilerin işlenerek, açık veya kapalı ağlar üzerinden iletilmesine dayanan ticaretle ilgili işlemlerdir. (OECD,1997)

UN-CEFACT (Birleşmiş Milletler İdari, Ticari ve Ulaşımla İlgili Uygulama ve Usulleri Kolaylaştırma Merkezi) ise e-ticareti; İş, yönetim ve tüketim faaliyetlerinin yürütülmesi için, yapılanmış ve yapılanmamış iş bilgilerinin; üreticiler, tüketiciler, kamu kurumları ve diğer organizasyonlar arasında elektronik araçlar (elektronik posta , elektronik bülten panoları vb.) www (word wide web) teknolojisi, akıllı kartlar, elektronik fon transferi, elektronik veri değişimi üzerinde paylaşılmasıdır. (UNICC) şeklinde tanımlamıştır. (Gökçen,2006)

ETKK'nun e-ticaret tanımı; Bireyler ve kurumların, açık ağ ortamında (internet) ya da sınırlı sayıda kullanıcı tarafından ulaşılabilen kapalı ağ ortamlarında (İntranet) yazı, ses ve görüntü şeklindeki sayısal bilgilerin işlenmesi, iletilmesi ve saklanması temeline dayanan ve bir değer yaratmayı amaçlayan ticari işlemlerin tümünü ifade etmektedir. Bu çerçevede, ticari sonuçlar doğuran ya da ticari faaliyetleri destekleyecek eğitim, kamuoyunu bilgilendirme, tanıtım-reklam vb. amaçlar için elektronik ortamlarda yapılan işlemler de e-ticaret kapsamında değerlendirilmektedir. (INET)

Yukarıdaki tanımları dikkate aldığımızda e-ticareti şöyle tanımlayabiliriz; Mal veya hizmetlerin, alış, satış, reklam ve dağıtımla ilgili işlemlerini internet ortamında

yada sınırlı kapalı ağ ortamında (İntranet) dijital olarak satıcı veya alıcıya ulaştırmaktır. (Gökçen,2006)

Gerçekten de internet sayesinde ticari anlamda ülkeler arasındaki sınırlar kalkmıştır. Bilişim teknolojilerindeki inanılmaz gelişimin ardında, aslında bu teknolojilerin ticari faaliyetlerde de kullanılabilmesi düşüncesi yatmaktadır. Bu gelişmeler de gösteriyor ki; öncelikle bu bilişim teknolojilerinin ticari faaliyetlerde kullanılabileceği düşüncesi bilişim teknolojilerinin hızlı bir şekilde gelişmesini sağlamıştır (ATO Danışmanlık Birimi, 2002).

İnternet kullanmanın ucuz olması, şirketlerin kendilerini ulusal ve uluslar arası pazarlarda tanıtmaları için büyük fırsat olmaktadır. Nispeten ufak olan firmalar, çok daha büyük, önceden ulaşmayı hayal bile edemedikleri pazarlara girerek, kendilerini gösterebilirler, pazar paylarını büyük çapta arttırabilirler. Ufak firmalar, internet üzerinde oluşturdukları imaj ile büyük firmalar ile rekabet şansını kazanabilirler (Şahin ve Diktaş, 2002).

### 3.3. Dünyada ve Türkiye'de İnternet Kullanımı

E-ticaret; internetin doğuşu ve telekomünikasyon teknolojilerinin gelişmesi ile ortaya çıkmıştır. Şirketler tarafından yoğun olarak 1996 yılından itibaren kullanılmaya başlanmıştır.

ITU verilerine göre, dünya genelindeki internet kullanıcı sayısı;

2000 yılı sonunda: 385 milyon

2001 yılı sonunda 500 milyon (Artış: % 30)

2002 sonu için: 665 milyon (Artış: % 31)

2005 yılında dünya genelinde internet kullanıcı sayısı: 941.8 milyon (2001 yılı iki katı) olduğu tahmin edilmektedir.

Bu bölümde internetin kullanıcı sayısı açısından ne kadar önemli sayılara ulaştığı tablolar yardımıyla açıklanacaktır. Bunun için dünya ve Türkiye'deki durum ayrı ayrı incelenecektir.

#### 3.3.1. Dünyada internet kullanımı

"Internetworldstats"ın araştırma şirketi ACNielsen'e dayanarak yayımladığı verilere göre, halen dünyada yaşayan 6 milyar 420 milyon insanın yüzde 13,9'u (938

milyon 711 bini) internet kullanıyor. Son 4,5 yılda dünyada internet kullanıcılarının sayısı yüzde 160 arttı. Fakat bu oran Türkiye'nin de içinde bulunduğu Ortadoğu'da yüzde 312, Karayipler ve Latin Amerika'da yüzde 277 ve Afrika'da yüzde 258 olarak gerçekleşti. (www.turk.internet.com, 2005).

İnternetin daha önce de hızlı geliştiği ve bu nedenle pazarın kısmen doyuma ulaştığı Kuzey Amerika'da ise son 4,5 yılda internet kullanıcılarının sayısı sadece yüzde 106,7, Avusturya ve Yeni Zelanda'da yüzde 116 ve Avrupa'da yüzde 161 artabildi. Toplam olarak bakıldığında, nüfusa oranla Kuzey Amerika'da (% 68), sonra Avustralya (% 49.2) ve sonra da Avrupa'da (% 36.8) olduğu görülüyor (www.turk.internet.com, 2005).(Tablo 2)

**Tablo 2.** Dünya İnternet Kullanım İstatistikleri

| **Bölgeler** | Toplam Nüfus (2005Tah.) (Milyon) | Dünya Nüfusunda %'lik Dilimi | İnternet Kullanıcı Sayısı (Milyon) | Büyüme Oranı 2000-2005 | İnternet kullanıcısı Nüfusun % Kaçı | İnternet kullanıcısı Dünyanın % Kaçı |
|---|---|---|---|---|---|---|
| Afrika | 896,721,874 | 14.0 % | 16,174,600 | 258.3% | 1.8 % | 1.7 % |
| Asya | 3,622,994,130 | 56.4 % | 323,756,956 | 183.2% | 8.9 % | 34.5 % |
| Avrupa | 731,018,523 | 11.4 % | 269,036,096 | 161.0% | 36.8 % | 28.7 % |
| Orta Doğu | 260,814,179 | 4.1 % | 21,770,700 | 311.9% | 8.3 % | 2.3 % |
| Kuzey Amerika | 328,387,059 | 5.1 % | 223,392,807 | 106.7% | 68.0 % | 23.8 % |
| Güney Amerika | 546,723,509 | 8.5 % | 68,130,804 | 277.1% | 12.5 % | 7.3 % |
| Okyanusya/Avustralya | 33,443,448 | 0.5 % | 16,448,966 | 115.9% | 49.2 % | 1.8 % |
| **Dünya Toplamı** | 6,420,102,722 | 100.0 | 938,710,929 | 160.0 % | 14.6% | 100.0% |

Kaynak: www.turk.internet.com

Ülkelere bakıldığında ise yaklaşık 203 milyon ile dünyada en fazla internet kullanıcısına sahip ABD'yi 103 milyon internet kullanıcısıyla Çin, 78 milyon internet kullanıcısıyla Japonya ve 47 milyon internet kullanıcısıyla Almanya izliyor

(www.byte.com.tr, 2005). Dünyada internet kullanıcı sayısı en yüksek 25 ülke şöyledir:

**Tablo 3.** Dünyada internet kullanıcısı sayısı bakımından sıralama.

| **Ülke** | Nüfus (Milyon) | İnternet Kullanıcısı (Milyon) | Kullanıcı Sayısının Nüfusa Oranı (%) |
|---|---|---|---|
| 1.ABD | 296,2 | 202,9 | 68,5 |
| 2.Çin | 1.282,2 | 103,0 | 7,9 |
| 3.Japonya | 128,1 | 78,0 | 60,9 |
| 4.Almanya | 82,7 | 47,1 | 57,0 |
| 5.Hindistan | 1.094,9 | 39,2 | 3,6 |
| 6.İngiltere | 59,9 | 35,8 | 59,8 |
| 7.Güney Kore | 49,9 | 31,6 | 63,3 |
| 8.İtalya | 58,6 | 28,6 | 48,8 |
| 9.Fransa | 60,6 | 25,6 | 42,3 |
| 10.Brezilya | 181,8 | 22,3 | 12,3 |
| 11.Rusya | 144,0 | 22,3 | 15,5 |
| 12.Kanada | 32,1 | 20,5 | 63,8 |
| 13.İspanya | 43,4 | 15,6 | 35,8 |
| 14.Endonezya | 219,3 | 15,3 | 7,0 |
| 15.Meksika | 103,9 | 14,9 | 14,3 |
| 16.Tayvan | 22,8 | 13,8 | 60,1 |
| 17.Avustralya | 20,5 | 13,8 | 67,2 |
| 18.Hollanda | 16,3 | 10,8 | 66,2 |

| | | | |
|---|---|---|---|
| 19.Polonya | 38,1 | 10,6 | 27,8 |
| 20.Malezya | 26,5 | 9,5 | 37,9 |
| 21.Tayland | 65,7 | 8,4 | 12,8 |
| 22.Filipinler | 84,2 | 7,8 | 9,3 |
| 23.Arjantin | 37,6 | 7,5 | 20,0 |
| 24.Türkiye | 73,6 | 7,3 | 9,9 |
| 25.İsveç | 9,0 | 6,7 | 73,6 |

Kaynak: tv8 15.08.2005

Türkiye kullanıcı sayısının nüfusa oranı bakımından % 9,9 oranla alt sıralarda yer almaktadır. Özellikle internet erişiminin dünyanın bir çok ülkesi ile karşılaştırıldığında son derece pahalı olması en önemli etken olduğu değerlendirilmektedir.

### 3.3.2 Türkiye'de internet kullanımı

Türkiye'de 2000 yılı sonunda 2 milyon olan internet kullanıcısı sayısı, son 4,5 yılda yüzde 263,5 ile, yüzde 160 olan dünya ortalamasının üzerinde arttı (www.byte.com.tr, 2005).

"InternetWorldStats" yayınlanan ve en son 23 Temmuz 2005'te güncellenen verilere göre Türkiye 7,3 milyon yani % 10'luk internet kullanıcısı sayısı ile dünya sıralamasında 24.sırada. Dünyada internet kullanan sayısının ise 1 milyara yaklaştığı raporlanıyor (www.turk.internet.com, 2005).

Türkiye, bu alanda Tayland, Filipinler ve Arjantin'in ardında kalırken, İsveç, Portekiz, Belçika, İsviçre ve Yunanistan gibi Avrupa ülkeleri yanında Pakistan, Vietnam ve İran gibi kalabalık Asya ülkelerini geride bırakmıştır (www.byte.com.tr, 2005).

İnternetin ilk olarak 1993 yılında girdiği Türkiye'de 2000 yılı sonunda 2 milyon olduğu hesaplanan internet kullanıcısı sayısı, son 4,5 yılda yüzde 263,5 ile, yüzde 160 olan dünya ortalamasının hayli üzerinde artarak 7 milyon 270 bine ulaştı. Buna rağmen Türkiye'de internet kullananların oranı, toplam nüfus dikkate

alındığında, yüzde 13,9 olan dünya ortalamasının altında kalarak yüzde 9,9 olmuştur. (www.byte.com.tr, 2005).

İnternet kullanıcılarının ana dilleri dikkate alındığında ise Türkçe, ilk 10 dil arasına giremedi. İngilizce' nin 296,5 milyon internet kullanıcısı ile başı çektiği listede, 124 milyon ile Çince ikinci, 78 milyon ile Japonca üçüncü, 60 milyon ile İspanyolca dördüncü ve 55 milyon ile Almanca beşincidir. Dünyadaki internet kullanıcıları dikkate alındığında ilk 10'a giren diğer diller ise 38,3 milyon ile Fransızca, 31,6 milyon ile Korece, 28,6 milyon ile İtalyanca ve Portekizce, 14,7 milyon ile de Hollanda'ca olduğu görülmektedir (www.byte.com.tr, 2005).

Devlet İstatistik Enstitüsü "Hane Halkı Bilişim Teknolojileri Kullanımı" başlıklı araştırmasını açıkladı. Nisan-haziran 2005 döneminde, el bilgisayarları kullanılarak yüz yüze görüşme yöntemi ile gerçekleştirilen araştırma için 10,151 hanedeki 27,013 birey ile görüşüldüğü ve bu bireylerin yaşlarının 16-74 arasında olduğu bildiriliyor. Buna göre evlerin % 8,66'sında internet erişimi mevcutken, internete erişen birey sayısı % 19,93. Bilgisayar kullanım oranı ise % 17,65 dir (www.turk.internet.com, 2005).

Araştırma kapsamında, 16-74 yaş grubundaki hane halkı bireylerinin 2005 yılı Nisan-Haziran döneminde bilgisayar kullanımı % 17,65 ve Internet kullanımı % 13,93. Bu oranlar sırasıyla kentsel yerleşim yerlerinde % 23,16 ve % 18,57 iken, kırsal yerleşim alanlarında % 8,28 ve % 6,05. Bir önceki yılın aynı döneminde bilgisayar ve İnternet kullanım oranı % 16,80 ve % 13,25 olarak gerçekleşmiş. Yani 1 yıllık sürede artış oranı bilgisayar kullanımında % 0,85 ve internet kullanımında % 0,68 Özetle son 1 yıl içinde yaklaşık 600.000 yeni kişi bilgisayar kullanmaya ve 500.000 yeni kişi internete erişmeye başlamıştır. (www.turk.internet.com, 2005).

### 3.4. E-Ticaretin Kapsamı

E-ticaret temel olarak iki tip faaliyeti kapsamaktadır “dolaylı e-ticaret” gerçek malların elektronik siparişi, posta hizmetleri veya ticari taşıyıcı kullanarak geleneksel kanallar üzerinden fiziksel olarak teslim edilmesi gerekenler. “Doğrudan e-ticaret” bilgisayar yazılımları, eğlence içerikleri veya küresel ölçekte bilgi hizmetleri gibi fiziksel varlığı olmayan malların hizmetlerin on-line sipariş, ödeme ve teslimini içermektedir (Kartal, 2002)

Kapalı ve açık ağlar kullanılarak yapılabilecek iş ve ticaret aktiviteleri şu şekilde sıralanabilir (Çengel, 2002):

- Mal ve hizmetlerin elektronik alışverişi,
- Üretim planlaması yapma ve üretim zinciri oluşturma,
- Tanıtım, reklam ve bilgilendirme,
- Sipariş verme,
- Anlaşma/sözleşme yapma,
- Elektronik banka işlemleri ve fon transferi,
- Gümrükleme,
- Elektronik ortamda üretim izleme,
- Elektronik ortamda sevkıyat izleme,
- Ortak tasarım geliştirme ve mühendislik,
- Elektronik ortamda kamu alımları,
- Elektronik para ile ilgili işlemler,
- Elektronik hisse alışverişi ve borsa,
- Ticari kayıtların tutulması ve izlenmesi,
- Doğrudan tüketiciye pazarlama,
- Sayısal imza, elektronik noter gibi güvenilir üçüncü taraf işlemleri,
- Sayısal içeriğin anında dağıtımı,
- Anında bilgi oluşturma ve aktarma,
- Elektronik ortamda vergilendirme,
- Fikri, sınai ve ticari mülkiyet haklarının korunması ve transferi.

### 3.5. E-Ticarette Taraflar

Ticari hayatımızda karşılaşılabilecek tarafların hemen hepsi bu sistem içinde de yer almaktadır. Bunlar (Kartal, 2002);

- Alıcılar

- Satıcılar
- Ortaklar
- Üreticiler
- Aracılar
- Bankalar
- Banka dışı finansal kurumlar
- Komisyoncular
- Sigorta şirketleri,
- Nakliye şirketleri,
- Vergi, fon vs. ilişkisinin olduğu resmi kurumlar
- Ticari birlikler
- Sistemin çalışmasını sağlayan bilgi işlem kuruluşları vs.dir.

### 3.6. Finans Piyasaları ve E-Ticaret

Alternatif Ticaret Sistemlerinin (ATS – Alternative Trading Systems) ve Elektronik İletişim Ağlarının (ECN) hızlı bir şekilde büyümesi, teknoloji evriminin ve yatırım toplumunun arada borsa komisyoncusu (broker) olmadan olumlu ve düzenli bir şekilde yatırım yapma istekliliğinin giderek artmasının bir sonucu olarak gösterilebilir. Bu hızlı büyüme sayesinde elektronik ticaretteki fiyat verimliliği ve ulaşılabilirlik; özellikle tezgah-üstü takas olmak üzere alışılagelmiş ticaret metodolojilerinin açık bir şekilde güçsüz kaldığını göstermektedir. (Özer s:3)

Kurumsal yatırımcıların birincil pazar konumunda bulunması, e-ticarette internet kullanımının artması ve komisyonsuz perakende pazarın ortaya çıkması ATS ve ECN‘lerin gelişiminde büyük rol oynamaktadır. Bu yatırım şekillerinin kişisel ve kurumsal yatırımcılar tarafından kullanılması, piyasaları şekillendirmekle kalmayıp aynı zamanda elektronik pazarları evrensel kılan bir hava yaratacaktır. E-ticaret, günümüzde tezgah-üstü takaslarda ve NASDAQ içerisinde geniş bir pay almış durumdadır. Şu aşamada NASDAQ‘daki işlem hacminin %25‘i ECN sistemleri üzerinden gerçekleşmektedir. (Özer s:4)

Üretici firmalarda, e-ticaret pazaryerlerini kullanarak, sıfır stoklu çalışma ve ihtiyaça göre üretme yeteneklerini arttırmaktadır. Bu da iş gücü ve hammadde temini konusunda ciddi indirimler sağlamaktadır. Just-in-Time yani tam zamanında üretimle, %300-400 lere varan, maliyet indirimleri sağlanabilmektedir. (Kuran, 2004 s:18)

Elektronik finans (e-finans) hizmetleri gerek internet üzerinden gerekse diğer uzak iletişim mekanizmalarıyla olsun, geçtiğimiz yıllardan günümüze bir hayli yaygınlaşmıştır. E-finans dağılımındaki ülkeler arası farklılıklara karşın, iletişim altyapısının okunabilirliği ve düzenleyici çatının kalitesi gibi faktörleri içeren birçok ortak noktalar ve önemli yakınlaşmalar mevcuttur. Diğer taraftan yayılma hızları hizmet tiplerine göre değişkenlik göstermektedir. (Özer s:3)

En çok etkilenenler, bilgisayarlı ticaretin bir norm olmaya başladığı komisyon piyasalarıdır. E-finans'a artan bağlılık, menkul kıymet ticaretinde bu alana göçü hızlandırmış ve görünen piyasalardaki finans merkezlerinin konuya eğilimini artırmıştır. Söz konusu kayma büyük bir entegrasyona ve etkileşilimli piyasa hatları oluşumuna sebebiyet vermiştir. Banka hizmetlerinde e-finans yayılımı ülkeler arasında daha fazla değişkenlik göstermiştir. Günümüzde birçok finans kuruluşu, e-finans hizmetleri sunmaktadır. (Özer s:3)

### 3.7. E-Ticaretin Etkileri

Bazı yönetim kuramcılar "Bir şirketin küresel olması için yalnızca uluslararası iş yapması değil; aynı zamanda kaynaklarını dünyanın en büyük rekabet avantajı sunacak herhangi bir yerine taşımasına izin verecek bir şirket kültürüne ve değerler sistemine sahip olması gerekir" derken, küresel olmanın sadece ihracat yapmak, yabancı teknoloji kullanmak, lisans vermek, iş gücü veya malzeme almak değil bunun ötesinde mevcut organizasyonların becerilerini ve düşünce yapılarını da geliştirmeleri gerektiğini ileri sürmüşlerdir. Tüm bunları becerebilen organizasyonlar yaşanan bilimsel ve teknolojik patlama ile, üretim organizasyonunu, dağıtımını dolayısıyla ekonomik alanları ve gelir kaynaklarını etkileyen yeni teknolojiler dönemine geçiş yapacaktır. (Akolaş)

E-ticaret, özü itibariyle ekonomik bir olgu gibi algılansa da sosyal ve kültürel alanlarda da etkiler oluşturmaktadır. E-ticaretin; birey, firmalar ve toplum üzerinde farklı etkiler oluşturduğu görülmektedir. Müşteri beklentilerinin pazarı yeniden

tanımladığı veya yeni pazarlar oluşturduğu koşullara E-ticareti benimseyen firmalar, daha hızlı uyum sağlamakta ve rekabet konusunda avantaj elde etmektedir. Bireylere ise alışveriş, bilgi ve hizmetlere erişim, kamu ile etkileşim konularında fiziki uzaklık ve zaman kısıtlarını ortadan kaldıran yeni yollar sunulmaktadır (Özkan, 2003).

E-ticaret kuşkusuz yenidir, ancak geçerli olan esaslar ve ilkeler bakımından geleneksel ticari yöntemlerle benzerlikler içermekte, zaman zaman aynı yöntemleri kullanmaktadır. Dolayısıyla e-ticaret, her anlamda yeni ve geleneksel ticarete alternatif bir ticari usuller seti değil, iletişim ve bilgi işleme teknolojilerinin gelişimine paralel olarak ortaya çıkan ve ticareti kolaylaştıran bir yeniliktir (İnce, 1999).

### 3.8. Dünyada E-Ticaret

E-ticaret güçlü bir ticaret ortamı olmasına karşın yeni bir ortamdır. Henüz dünyada e-ticaret alt yapısını tam olarak oluşturabilmiş bir ülke bulunmamaktadır. E-ticaret teknolojileri sürekli gelişmektedir ve buna paralel olarak e-ticaretin sorunları da sürekli artmaktadır. E-ticaretin yaygınlaşması yeni hukuki sorunları gündeme getirmiştir . Bu sorunları günümüzde hukukçular yorumlayıp çözümler sunmaktadırlar. (Gökçen,2006)

Uluslararası e-ticaretin gelişimi üçüncü ülkeleri içine alan uluslararası anlaşmaları gerektirmektedir; küresel karşılıklı işlerliğini temin edebilmek için, sertifikasyon hizmetlerinin karşılıklı tanınması hususunda, üçüncü ülkelerle çok taraflı anlaşmalar imzalanması yararlı olabilir. (AP,2000a)

Dünyadaki e-ticaret durumuna bakmadan önce e-ticaretin avantajlarını açıklamak yararlı olacaktır. (Gökçen,2006)

Elektronik Ticaretin İşletmeler Açısından Avantajları:

- Maliyetlerin azalması ve pazarlamanın daha geniş ölçekte yapılması,
- Zamandan tasarruf ve pazarlama süreçlerinin azalması,
- Tüketicilerin satın alma işlemi yaparken satın alma sürecini de kontrol edebilecek yöntemlere kavuşması,
- Bilginin daha zengin ve karşılıklı etkileşime açık olması,

- Bilginin anında ve sürekli ulaşılabilir olması,
- Çıkabilecek sorunlara çok daha hızlı çözümler sunma,
- Pazara girişteki engellerin azalması ve herkese eşit erişim şansı sunulmasıdır

E-ticaretin tüketiciler açısından avantajları ise şu şekilde özetlenebilir:

- Genel ve geniş seçim yapabilme imkanı,
- Hizmet kalitesinin artması,
- Önemli fiyat indirimi,
- İhtiyaçlara çok hızlı yanıt verilmesi,
- Yeni ürünler ve hizmetlerdir.

AB'ne göre bilgi toplumunda elektronik ticaretin gelişmesi, Topluluk içinde ve özellikle de küçük ve orta ölçekli işletmeler için iş imkanlarının artırılması açısından çok önemli fırsatlar sunmaktadır. Bu durum, Avrupa işletmelerinin ekonomik büyümelerini, araştırma geliştirme yatırımlarını kolaylaştıracak ve aynı zamanda herkesin internete erişimine bağlı olarak Avrupa işletmelerinin rekabet gücünü artırabilecektir. (AP,2000a)

1960'lı yıllardan beri özellikle ABD'de Elektronik Veri Alışverişi (EDI) tekniği ile elektronik ticaret yapılmaktaydı. EDI tekniği, işletmelerin bilgisayar sistemleri arasında ticari işlem yapmayı sağlayan, standart dokümanların iletilmesine imkan veren bir tekniktir. Özellikle perakendecilik ve dağıtım sektöründe kullanımı yaygındı. EDI kapalı bir ağ üzerinde gerçekleştirilen bir faaliyetti ve herkese açık değildi. Ayrıca EDI'nin kurulması pahalıdır ve küçük işletmeler için başarılması zordur. İnternetin EDI'ye kıyasla çok ucuz olması, internet üzerinden ticaret yapma fikrini herkes için cazip bir fikir haline getirmektedir (TISK). İnternetin e-ticareti için kullanılması yenidir. E-ticaretin yaygınlaşmaya başlamasının tarihi 1997'dir. Zaten internetin asıl gelişimi ve patlaması ticari kullanımı artamaya başladıktan sonra yaşanmaya başlamıştır. İnternetin ticari ürünleri satmada kullanımı, ilk başta "belki olabilir." türünden ve süslü web sayfalarından oluşan bir takım denemelerden ibaretti. Ancak Amazon (http://www.amazon.com), Dixons (http://www.dixons.co.uk/), Yahoo (http://www.yahoo.com) gibi örneklerin 1-2 yıl içersinde, sadece internetin

üzerinden sattıkları servislerle birer büyük şirket haline gelmeleri, birden bu denemeleri ve hayalleri gerçeğe dönüştürüverdi. İnternet üzerinde dönen ekonomi her geçen gün artmaktadır. Hatta, 1999 yılında Amerikan Ticaret Bakanlığı'nın yaptığı bir araştırmada internet ekonomisinin ( ucuz girdi ve iş gücü, az maliyet vb.. sebebiyle) enflasyon oranının azaltılmasında rol oynadığını saptamıştır. (Gökçen,2006)

ABD Hükümeti, OECD, AB, gibi organizasyon örgütleri , internet üzerinden yapılan elektronik ticaretin globalleşmesi ve sağlıklı bir yapıda gelişmesi konusunda 1990'lı yılların sonlarından beri stratejik toplantılar yapmakta ve ortak eylem planlarını geliştirmeye çalışmaktadırlar. (Gökçen,2006)

Bu çalışmalarda,

- Kullanıcıların ve müşterilerin e-ticarete güvenlerinin artması (kişisel bilgilerin güvenliği, güvenli kredi kartı kullanımı, müşteri haklarının korunması vb),
- Geleneksel ticari faaliyetlerin yapılabilmesi için geliştirilmiş /düzenlenmiş yasa ve kuralların elektronik ticari pazara da hitap eder hale gelmesi,
- E-ticaret için oluşturulan bilgi/işlem altyapısının geliştirilmesi,
- E-ticaretten alınacak verimin artması gibi unsurlar göz önünde tutulmakta ve bu konularda hükümet politikalarına yön verecek kararlar alınmaktadır. (Sırma,2002)

2010 yılına kadar, AB bünyesinde, e-ticaret ile ilgili konularda 20 milyon yeni iş olanağı oluşturulacağı tahmin edilmektedir (EU, 2000) .Bu ve benzeri örnekler ve açıklamalara baktığımızda, globalleşen dünyada e-ticaretin ne kadar önemli olduğunu görmekteyiz. (Gökçen,2006)

Japonya'daki e-ticaretin gelişimi kurumsal düzeyde sağladığı örgütlenme modelleri ile yoğun çalışan, çok sayıda pilot proje yürüten ülkelerin başında gelmektedir. Japonya Uluslararası Ticaret Sanayi Bakanlığı 1995 yılından itibaren bu çalışmalara büyük bir kaynak aktararak, 1995-1997 Kasım ayı arasında toplam 45 projeye 32 milyar Yen harcamıştır.1995'te E-Ticaret Ortamını Geliştirme Komitesi ( Committe on the Improvement for Electronic Commerce),1996 başında

da ECOM (Electronic Commerce Promotion Council of Japan) kurulmuştur. (Ersoy, 1999)

E-ticaretin işlem hacminin ölçülmesi zor bir araştırmadır. Dolayısıyla e-ticaretin hacmi ile ilgili ölçüm sonuçları farklılık göstermekte ve çeşitli kurumlar birbirinden çok farklı tahminlere ulaşmaktadırlar. (Gökçen,2006)

Birçok ülkedeki kamu kesimi de teknolojik gelişmelerden etkilenmektedir. Örneğin, İsveç e-devlet kavramını hayata geçirmiş ve iş akışında büyük bir hızlanma, kağıt maliyetlerinde %40'lara varan kazanç elde etmiştir. Bir vatandaşın evinden internet aracılığı ile vergi ödemesi, tapu kayıtlarına ilişkin bilgileri doldurması mümkün bulunmaktadır. Bu durum birçok gelişmiş ülke için geçerlidir. Öyle ki AB e-Avrupa ve e-Avrupa+ programlarını ortaya koymuş ve üzerinde hassasiyetle durmaktadır. (Özer s:3)

E-ticaretin serbest gelişimine imkan vermek için, yasal çerçeve açık ve sade, öngörülebilir ve uluslararası alandaki kurallarla uyumlu olmalı, böylece Avrupa sanayisinin rekabet yeteneğini olumsuz etkilememeli veya bu sektördeki yenilikleri engellememelidir. (AP,2000)

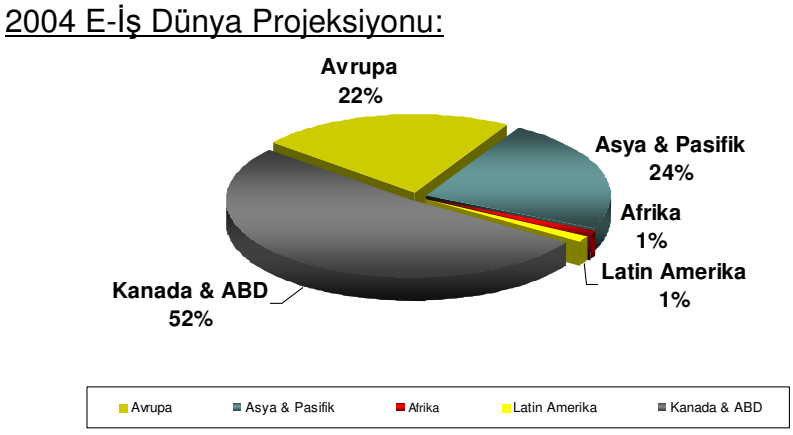
Tüm bu gelişmeler doğal olarak sermaye piyasalarını da yakından etkilemektedir. Bilişim teknolojilerindeki gelişmelerin, sermaye piyasalarını çok daha güvenilir, hızlı, verimli ve entegre bir yapıya kavuşturması kaçınılmazdır.

ABD'de teknolojik açıdan gelişmiş ECN sistemleri ile borsalar arasında işbirliği olanakları yoğun şekilde araştırılmakta ve bazı somut adımların atıldığı görülmektedir. Nasdaq'ın Japonya'da Nasdaq-Japon projesinde, Softbank Corporation gibi İnternetle ilgili alanlarda faaliyet gösteren 60'dan fazla şirkette iştiraki olan ve bilgi teknolojileri konusunda uzmanlaşmış bir firma ile ortak olmayı tercih ettiği görülmektedir. (Özer s:3)

Straight Through Processing (STP) yatırımla ilgili bütün işlemlerin tek bir elden gerçekleştirilmesidir. Bu kapsama takas, saklama, emir, emir eşleştirme gibi tüm konular dahildir. Bir başka deyişle STP, emrin verilişinden gerçekleşmesine kadar tüm ticari aşamaları kapsayan elektronik bir süreçtir. STP süreç döngüsünde işlem eşleşmesi önceden uygulanarak, işlemin gerçekleşmeme riski azaltılmakta ve ortamda bulunan işlem bilgilerinin bütün kullanıcılarca paylaşıldığı bir ortam yaratılmaktadır. STP'nin ana amacı otomatik olmayan işlem kanallarını ve elle

gerçekleştirilen işlemleri ortadan kaldırarak maliyet kazancı sağlayıp, harcamaları azaltmaktır. STP aynı zamanda ön ve arka ofis fonksiyonlarını ve birleşme eğilimini hızlandırarak altyapı ve risk yönetimi harcamalarında ekonomi sağlamaktadır. STP bütün müşteriler ve broker-dealer'lar arasında son işlem süreci için işlem doğrulamasını, işlem gerçekleşmesini ve yatırım hesap bilgilerini içeren bir iletişim kanalıdır. Gene yatırım yöneticileri, broker'lar, dealer'lar ve müşteriler arasında ön ticari işlemler döngüsünde veri transferini gerçekleştirmektedir. Cross-border seviyesinde yer alan bütün ticari detayların ön eşleşmesini yaptığı gibi işlem verisinin tüm kullanıcılara ticari işlemler döngüsü içerisinde anında ulaşımını sağlar.Tüm bu gelişmeler, bu tür mekanizmalara ilişkin yasal altyapının sağlanması ve gerekli düzenlemelerin de yapılmasını gerektirmektedir. Başta ABD olmak üzere birçok ülke düzenleyici otoriteleri bu kapsamda yasal düzenlemeler yapmış bulunmaktadır. (Özer s:4)

Birçok ülke ve çok sayıda organizasyon internet'te yapılan işlemlere ilişkin olarak yapılması gereken düzenlemeler ve gerçekleştirilmesi gerekenlere ilişkin çalışmalar yürütülmektedir. (Gökçen,2006)




**Şekil 12**(Kaynak: ITU,2000)

Rakamsal olarak baktığımızda, ticaretin yeni adı olan e-ticaret pastasından 2004 yılı için ne kadarlık pay alacaklarını gösteren grafiği görüyoruz. 2000 yılında yapılan 2004 projeksiyonunda, Kanada ve ABD'nin %52lik bir pay bundan sonra, Asya ve Avrupa'nın geldiği görülmekte. Her geçen yıl bu paydaki yer, dijitalleşmeye başlayan ülkelerin lehine artacak. (Kuran, 2004 s:4)

2006 yılında gelişmekte olan ülkelerin dünya genelindeki e-ticaretten elde edecekleri payın yaklaşık olarak % 6.7 olacağı ve bu payın % 5.1'lik kısmını Asya-Pasifik bölgesindeki gelişmekte ülkelerin alacağı, diğer gelişmekte olan ülkelerin payının ise %1'in altına düştüğü görülmektedir. Ayrıca gelişmiş ülkelerin % 95.4 olan 2002 yılı payının 2006 yılında % 93.3'e gerileyeceği de gözlemlenen diğer bir husustur. (Alkan ve İnalöz, 2003)

### 3.9. Türkiye'de E- Ticaret

Türkiye'de, özellikle 1999 yılından itibaren internet kullanıcılarında yaşanan artış, Türkiye'deki işletmeleri de internet ortamına girmeye zorlamıştır.Bu sayede işletmeler müşterilerine veya satıcılarına ulaşabilmek için internet kullanarak e-ticaret yapmışlardır. Türkiye'de bankacılık sektörü e-ticaretin gelişiminde sürükleyici bir faktör olmuştur. (Gökçen,2006)

Geniş kapsamlı e-ticaret tanımları esas alındığı takdirde Türkiye'de e-ticaretin ilk uygulaması 1992 yılında Merkez Bankası ile bankalar arasında başlayan Elektronik Fon Transferi (EFT) uygulamasıdır. (Gökçen,2006)

1995 yılında İGEME'nin (İhracatı Geliştirme Etüd Merkezi), UNCTAD (Birleşmiş Milletler Ticaret ve Kalkınma Konferansı) tarafından Ankara'nın ticaret noktası yani gelişmiş ve gelişmekte olan ülkelerin küçük ve orta ölçekli işletmelerinin dünyaya açılabilmelerini sağlamak amacıyla dış ticaret faktörlerini bir araya getirmeyi amaçlayan bir programın seçilmesi Türkiye'de elektronik ticaretin temelleri için önemli bir aşamaydı. Ağustos 1997'de toplanan Bilim ve Teknoloji Yüksek Kurulu (BTYK) aldığı bir kararla elektronik ticaret ağının kurulmasını karara bağlamıştır. Bu çalışma çerçevesinde TÜBİTAK aynı yıl TUENA'yı (Türkiye Ulusal Enformasyon Altyapı Planı) başlatmıştır. Bu proje Türkiye'nin enformasyon altyapısının resmini ortaya koymaktadır ve kamunun konuya yaklaşımının başlangıç noktasını teşkil eder. Daha sonra Bilim ve Teknoloji Yüksek Kurulu Kararı çerçevesinde kamu, özel sektör ve üniversite katılımcıları ile Rekabet Kurumu'nun da temsilci bulundurduğu ETKK (Elektronik Ticaret Koordinasyon Kurulu) oluşturulmuştur (Aydemir, 2004). ETKK 1998'in Mayıs ayında hazırlayıp kamuoyunun ve BTYK'nun bilgisine sunduğu e-ticaretin hukuk ,teknik ve finans boyutlarının incelendiği rapor 4 ana maddeden meydana gelmiştir.Bunlar gerekli teknik ve idari alt yapının kurulması; hukuki alt yapının kurulması; E-ticareti özendirecek politikaların alınması; Ulusal politika ve uygulamaların,uluslar arası

politikalar ve uygulamalarla uyumunun gözetilmesidir (IGEME). ETKK tarafından 1998 yılında hazırlanan rapordaki "Hukuki Altyapının Kurulması" başlığı altında tavsiyelerden biri "*elektronik ödeme sistemlerinde faaliyet gösterecek operatörlerin saptanması, bu operatörler arasında yapılacak sözleşmeler açısından Rekabet Kanunu'ndaki ilkeleri dikkate alan hukuki kuralların saptanması*" şeklinde ifade edilmiştir. (Gökçen,2006)

Elektronik ticaret sayesinde oluşan ekonomik değer, henüz ülke ekonomisinde dolayısıyla dünya ekonomisinde çok az bir paya sahip olmasına rağmen, elektronik ticaret aracılığı ile oluşturulan katma değer ve onu mümkün kılan bilişim, kuşkusuz çok hızlı bir büyüme seyri göstermektedir. Bu büyüme önceki yılda yapılan tahminlerin dahi kestiremediği boyutlara ulaşmış durumdadır. Elektronik ticaret çok büyük bir hızda gelişirken, aynı zamanda, yeni iş yapma biçimlerini mümkün kılmakta ve yeni işletme modelleri oluşturulmaktadır. (Gökçen,2006)

Dünyada elektronik ticaretle yapılan alışverişlerde en çok satılan ürünlerin başında otomobil ve lüks tüketim malları gelirken, Türkiye'de en çok satılan ürünlerin başında kitap ve compact disk (cd) gelmektedir. (Gökçen,2006)

### 3.10. Elektronik Ticarete Konu Olan Kredi Kartlı İşlemler

Kredi kartı ile yapılan elektronik ticaret işlemlerine ait 21 bankadan toplanan veriler konsolide edilerek yayınlanmakta olup, bu veriler 1 Ekim 2004 ile 31 Aralık 2004 arasında gerçekleşen işten-müşteriye (Business to Customer-B2C) işlemlere ait bilgilerden oluşmaktadır. Bu dönem itibariyle banka kredi kartları ile "sanal POS"lar (Virtual Point of Sales – VPOS) üzerinden geçekleştirilen e-ticaret işlem sayısı 3.033.257, işlem tutarı ise 229.562 milyar TL olmuştur. Yurtiçi banka kredi kartları ile yapılan işlem sayısı 2.998.407, işlem tutarı 217.175 milyar TL olurken yurtdışındaki bankalar tarafından çıkarılan kredi kartları ile yapılan işlem adedi 34.850 ve işlem hacmi ise 12.387 milyar TL olarak gerçekleşmiştir.

Türkiye'de çıkarılan kredi kartları ile yapılan işlemlerin adet ve hacim olarak toplam içindeki payı bu dönemde sırasıyla yüzde 94,6 ve yüzde 98,85 olarak gerçekleşmiştir.

Yurtiçi ve yurtdışı bankalar tarafından verilen kredi kartları ile yapılan toplam işlem adedi 3.153.133 ve işlem hacmi 253.524 milyar TL olmuştur. Kredi kartları ile

yapılan işlemlerin e-ticaret işlemleri içerisindeki payı işlem adedinde ve işlem hacminde yüzde 97 gerçekleşmiştir.

Aralık 2003 dönemine göre; Türkiye'deki "sanal POS"lar kullanılarak yurtdışı kredi kartları ile yapılan işlem adedinde yüzde 48 oranında bir artış, işlem hacminde ise yüzde 381 oranında bir artış olmuştur. Aynı döneme göre yurtiçi işlemlerde ise işlem adedi 199 oranında artarken işlem hacmi ise sırasıyla yüzde 199 oranında artmıştır.

Elektronik ticaret verileri dönemsel olarak karşılaştırıldığında; işlem adetleri ve işlem hacmi büyüklüklerindeki artışın devam etmekte olduğu görülmektedir. Aynı şekilde kayıtlı ve aktif işyeri sayısında da önemli bir artış gözlenmektedir.

Elektronik ticaretin gelişmesi ve elektronik imzanın kullanıcılar tarafından benimsenmesi için açık ağ sistemine güven duyulmasının sağlanması gerekir. Bu güvenin sağlanabilmesi, taraflar arasında karşılıklı olarak iletilen bilgilerin gizliliğinin ve bütünlüğünün korunması, tarafların kimliklerinin doğruluğunun güvence altına alınmasına ilişkin hukuki düzenlemelerin yapılması ile mümkün olacaktır. (Gökçen,2006)

### 3.11. E-Ticaret Uygulamalarında E-İmza Kullanımı

E-ticaret uygulamalarının gelişmeye başlamasıyla birlikte, işletmeler organizasyonel yapısını bu alanda da etkinlik sağlayabilecek duruma getirmektedir. Önceleri, sadece işletmelerin ürünleri, adres bilgileri ve sınırlı iletişim amacıyla hazırladıkları web siteleri ve e-iş ortamı, günümüzde her türlü ürün ya da hizmetin pazarlanabildiği e-ticaret yapısına bürünmektedir. Bu bağlamda, bilişim teknolojilerini etkin olarak kullanan işletmelerin e-ticaret faaliyetlerini de başarılı bir şekilde sürdürmesi beklenmektedir. Elektronik ticaretle birlikte ekonomik işlemlerin kolaylaşması ekonominin işleyiş yoğunluğunu artırmaktadır. Gerek işletmeler arasında ve gerekse tüketiciler ile üreticiler arasında etkileşimli (interaktif) ilişkilerin önündeki engellerin büyük ölçüde ortadan kalkması ekonomik ilişkilerin her seviyede yoğunlaşması ile sonuçlanmaktadır. Özellikle finansal işlemler ve yazılım gibi alanlarda işlerin sadece veri transferi ile tamamlanabilmesi coğrafi sınırlamaları ortadan kaldırmıştır. Diğer mal ve hizmet biçimleri için coğrafi sınırlamalar ortadan kalkmasa da, ilişki kurma yöntemlerinin gelişmiş olması ve

ulaştırma hizmetlerinin yaygınlaşması ve ucuzlaması ekonomik ilişkileri her geçen gün daha da artırmaktadır.

Dış ticaret ağları, finans ağları, küresel ekonomik, sosyal ve siyasi karar verme ağları, birbirleriyle senkronize bir bütün oluşturarak, dünyanın ve ulusların kaderini belirleyen tek bir bilgi ağını yaratıyor. Bir ülke, tüm ekonomik ve insani potansiyelleriyle, bu ağın içinde ne kadar değer, yani bilgi yaratır ve bu bilgiyi ağın geri kalanıyla ne kadar eşzamanlı ve uyumlaştırılmış bir biçimde paylaşırsa, o kadar rekabet avantajına sahip oluyor. İş yapmanın küresel kurallarını artık bilginin dolaşım ve paylaşım kabiliyeti belirliyor. (İİK, 2004)

Dünya pazarını sürekli olarak birleştirme eğiliminde olan bankacılık ve sanayi grupları uluslar üstü bazı mekanizma ve kurumları desteklemektedirler. Bu kurumlar aracılığıyla ortak üretim, ticaret standartlarını tüm dünyada yaygın hale getirmektedirler. Ticaret alanında günümüzde standart olan kağıt dış ticaret belgelerinin yerini elektronik imzanın hukuksal geçerlilik kazanması ile elektronik belgelerin alacağı açıkça görülmektedir.

Günümüzde e-ticaretin payı her geçen gün artsa da, e-ticaretle ilgili olarak genel bir güven eksikliği var. Kullanıcılar, kredi kart numaralarını ve kişisel bilgilerini internete vermek istemiyorlar. İşte bu güven sorunu ve güvenli bir alt yapının sağlanması işlevselliğini e-imza sağlıyor. Böylece, sertifika otoritesi tarafından tanınmış bir e-ticaret sitesine kendi dijital imzamızı atarak istediğimiz kadar mal ya da hizmet alımı yapabilecek, ev satın almadan gündelik ihtiyaçların karşılanmasına kadar gönül rahatlığı ile alışveriş yapabileceğiz. (Kuran, 2004 s:7)

Elektronik ticaret uygulamalarında, taraflar arası iletilerde; bilginin gizliliği, bütünlüğü ve tarafların kimliklerinin doğruluğu kurulacak olan teknik ve yasal altyapı ile garanti edilebilmelidir. Bu bağlamda elektronik ticaretin hayata geçirilmesi için en hayati yasal düzenlemenin "EİK" olduğu söylenebilir. (Alkan ve İnalöz, 2003)

E-imzanın kanuni dayanağının olması bu anlamda önemli. Çünkü insanlar, herhangi bir haksızlığa uğradıklarında devletin bu haksızlığı kanunları çerçevesinde gidermesi ve bir çözüm bulmasını istemektedir. (Kuran, 2004 s:7)

15 Ocak 2004 tarihinde kabul edilen ve 23 Ocakta Resmi gazetede yayınlanan 5070 Nolu EİK sayesinde, e-imzanın hukuksal alt yapısı kanuni bir çerçeveyi

kazanmış oldu. Yani, yapılan anlaşmalara attığımız imza nasıl bizi bağlıyorsa, yapacağımız e-anlaşmalara atacağımız e-imzalarda aynı kanuni çerçevede değerlendirilecek. Elektronik sertifikanın niteliklerinden, denetim ve izinsiz kullanıma, sertifika hizmet sağlayıcısının özelliklerinden sahtekarlık ve idari para cezalarına kadar akla gelebilecek bütün noktalar kanunda tanımlandı. Elbette bir takım eksiklikleri olabilir, ama bunlar zamanla aşılacaktır. Burada önemli olan, 1994'lü yıllarda bu yasayı çıkartan ve şu anda yoğun bir şekilde kullanan Amerika'ya, 1999 da bu yasayı çıkaran Singapur'a yetişmemiz ve Dijital bölünmede e-ülkelerin yanında yer almamızdır. (Kuran, 2004 s:7)

Şu anda Sanayi Bakanlığı, www.sanayi.gov.tr adresinde online olarak, garanti belgesi alımından, satış sonrası yeterlilik belgesi alımına kadar bütün başvurular yapılabilmektedir. E-imza uygulaması ile birlikte bu tür belgeler, vatandaşın bakanlığa gelmesine gerek kalmadan online olarak sunulacaktır. (Kuran, 2004 s:10)

Ayrıca, Sanayi Bakanlığına, bağlı bütün esnaf odalarının birleştirildiği, www.esnafonline.com adresinde de online olarak, esnaf işlemleri ve veri girişleri yapılabilmektedir. Esnaf odaları veri girişlerini esnafonline üzerinden yapabilmektedir. E-imza uygulaması ile birlikte, imza gereksinimi duyulan diğer süreçlerde hayata alınacaktır. Bu proje kapsamında 35-40 bin e-imza dağıtılması ve bu e-imzaların sistemle entegre edilmesi planlanmaktadır. (Kuran, 2004 s:10)

Gelecekte, tarihin sayfalarına bakıldığında, toplumsal değişimi ve ticaretin yeni şeklinin ne zaman kayıtlar altına alındığına bakılacak olursa, içinde bulunduğumuz yıl karşımıza çıkacaktır. Bu anlamda, e-imza ile birlikte resmen yeni bir çağa girmiş bulunuyoruz. (Kuran, 2004 s:18)

### 3.12. Elektronik İmzanın Türk Sermaye Piyasalarındaki Diğer Kullanım Alanları

Bilgi ve verinin paylaşıldığı her konunun elektronik imza için bir kullanım alanı olduğunu söylemek yanlış olmaz. Özellikle sermaye piyasaları, gerek bilgi/veri alış-verişinin gerekse bilginin/verinin güvenilirliliğinin üst düzeyde olduğu bir alandır. Bilgi ve veri sermaye piyasalarında birebir mali değer anlamına gelmektedir. Yanlış veya değiştirilmiş bir bilgi sermaye piyasalarında büyük oynamalara (volatilite) neden olabilmekte, bu durum da başta borsada işlem gören

hisse senetleri fiyatlarında gerçek dışı değişimlere sebebiyet verebilmektedir. (Özer s:7)

Sermaye piyasalarında bilgi yatırımcının emrini aracı kuruma vermesi ile başlar, aracı kurumun emri borsaya iletmesi, borsada gerçekleşen emrin borsa sistemlerinde kaydedilmesi, Takas ve saklama kurumlarına (Takasbank, Merkezi Kayıt Kuruluşu) iletilmesi ile devam eder. Aslında bilginin akışı çok daha karmaşık bir yapıda gerçekleşmektedir. Şirketler, aracı kurumlar, yatırım fonları ve diğer kurumlar bilgilerini SPK'na, İstanbul Mekul Kıymetler Borsasına ve Takasbanka iletmektedir. Ayrıca SPK, İstanbul Menkul Kıymetler Borsası, Takasbank, Merkezi Kayıt Kuruluşu arasında çift yönlü sürekli bir bilgi paylaşımı bulunmaktadır.(Özer s:7)

İlk olarak mali tablo bildirimleri ve özel durum açıklamaları ile başlayan Kamuyu Aydınlatma Projesi ileride SPK'na gelen her türlü bilginin elektronik ortamda alınması yönünde genişletilecektir. Aracı Kurumlar, yatırım fonları, yatırım ortaklıkları, bağımsız denetim şirketleri, yabancı yatırım fonları, portföy yönetim şirketleri SPK'ya ilettikleri her türlü bilgiyi Kamuyu Aydınlatma Projesi (KAP) üzerinden iletecek, kayda alma, yetki belgesi, sermaye artırımı gibi başvurular benzer bir sistem üzerinden gerçekleştirilecektir. Aracı kurumlar internet üzerinden emir alımlarında, Aracı Kuruluşlar Birliği aracı kurumlardan bilgi toplanması ve duyurulmasında, Merkezi Kayıt Kuruluşu şirket ve yatırımcılarla bilgi alış verişinde elektronik imzadan faydalanabilecektir. Kurulacak olan KOBİ Borsalarında da elektronik imza teknolojilerinin kullanılması olasılığı oldukça yüksektir. Tüm bu durum sadece sermaye piyasalarına yönelik bir sertifika otoritesine de ihtiyacı ortaya çıkarmaktadır. (Özer s:7)

Görünen odur ki gelecekte sermaye piyasalarının her alanında elektronik imza kullanılacak ve bu kullanıma KAP kapsamında oluşturulan sertifikalar temel teşkil edecektir. (Özer s:8)

# BÖLÜM IV

# DÜNYADA ve TÜRKİYE'DE ELEKTRONİK İMZA ALTYAPILARI VE UYGULAMALAR

## 4.1. E-İmzaya Geçiş

Dünyada 1996 yılında, ülkemizde 2004 yılında hazırlanan mevzuatlarla hukuki altyapısı belirlenmeye başlanan e-imza, halihazırda birçok ülkede yasal olarak uygulanmaya başlamıştır. E-devletin ve yaklaşık 6 trilyon dolar değerindeki elektronik ticaretin altyapısı olan e-imza; internetin hızlı gelişimiyle elektronik ortama aktarılan kamusal ve ticari alandaki birçok uygulamayı güvenilir, etkin, verimli ve tasarruflu hale getirmektedir. E-imza, Birleşmiş Milletler Uluslararası Ticaret Hukuku Komisyonu(UNCITRAL) tarafından, 1996 yılında Elektronik Ticaret Model Yasası'nın ve 2001 yılında Elektronik İmza Model Yasası'nın çıkarılmasıyla, dünya ülkelerince gerekli hukuki düzenlemeler yapılarak uygulamaya geçirilmeye başlanmıştır.(Beder, 2005)

Avrupa Ülkelerinde E-İmzaya Geçiş Tarihleri

**1997 yılı:** İtalya

**1998 yılı:** Almanya

**1999 yılı: Portekiz**, İspanya

**2000 yılı :** Fransa, Danimarka, Lüksemburg, İngiltere, İrlanda, Avusturya, Çek Cumhuriyeti, Estonya, Litvanya, Slovenya

**2001 yılı:** Belçika,İsveç, Macaristan, İzlanda, Norveç

**2002 yılı:** Hollanda,Polonya

**Amerika Kıtasında E-İmzaya Geçiş Tarihleri**

**1999 yılı:** Bermuda,Peru, Kolombiya

**2001 yılı:** Kanada, Arjantin

**Asya ve Diğer Ülkelerin E-İmzaya Geçiş Tarihleri**

**1995 Yılı:** Rusya

**1998 Yılı:** Hindistan

**1999 Yılı:** Singapur

**2000 Yılı:** Japonya, Hong Kong, Filipinler (Beder, 2005)

Avrupa Birliğine uyum süreci Türkiye'de e-imza altyapısının oluşmasına temel teşkil etmiştir. Bu açıdan bakıldığında Avrupa'da e-imza altyapısının oluşum sürecine dikkat etmekte fayda vardır.

### 4.1. 1. Avrupa'da E-İmza Altyapısının Oluşum Süreci

AB Komisyonu, e-imzaların kullanımı için hukukî bir çerçeve kuran bir yönerge teklifi hazırlamıştır. Güvenlik ve sorumluluk ile ilgili asgarî kurallar getiren teklif, hizmetlerin serbest dolaşımı ve esas ülke denetimi şeklindeki Tek Pazar ilkeleri temelinde elektronik imzaların AB çapında hukuken tanınmasını sağlayacaktır. Dolayısıyla teklif, Tek Pazar'ın her yerinde güvenli çevrim-içi işlemler için bir çerçeve yaratacak ve böylece, büyüme, rekabet gücü ve istihdam açısından AB için bundan gelecek olan yararlar ile birlikte, elektronik ticaret hizmetleri alanında yatırım yapılmasını teşvik edecektir. (Özyılmaz ve Evsenal, 2000)

Önerilen yönerge, Ekim 1997'de komisyon tarafından kabul edilmiş olan "Elektronik Haberleşmede Güvenliğin ve Güvenin Sağlanması-Dijital İmzalar ve Şifreleme İçin Bir Avrupa Çerçevesine Doğru" başlıklı tebliğin bir devamıdır. Söz konusu tebliğ, elektronik şebekelerde güvenlik olmayışını, elektronik ticaretin gelişimini engelleyen başlıca engellerden biri olarak belirlemişti. Komisyonun teklifi, Amsterdam'da yapılan AB Konseyi tarafından onaylanan Tek Pazar için Eylem Planı çerçevesinde de öngörülmüştü. (Özyılmaz ve Evsenal,2000)

Birlik, elektronik imzanın kullanılmasını kolaylaştırmak ve hukuken tanınmasına katkıda bulunmak amacıyla 13 Aralık 1999 tarihli ve 99/93/EC sayılı Elektronik İmza Direktifi'ni yayınlamıştır. Direktif; elektronik imza sertifikaları, sertifika hizmet sağlayıcıları ve bunların denetimi ile ilgili esasları belirlemektedir. Bilişim toplumu hizmetlerinin üye ülkeler arasında serbest dolaşımını sağlamak amacıyla hazırlanan 8 Haziran 2000 tarihli 2000/31/EC sayılı Elektronik Ticaret Direktifi ile de elektronik sözleşmeler ve bunların hukuki neticelerine ilişkin önemli hususlar belirlenmiştir. (beder, 2005)

### 4.2. Avrupa'da Elektronik İmza Kullanımı

Avrupa'da e-imzanın en yaygın kullanıldığı alan e-bankacılık olup sınırlı ölçüde de e-devlet uygulamalarıdır.Kişisel e-bankacılık tüm AB üye ülkelerinde birkaç yıldan beri kullanılmaktadır. Geleneksel olarak kişisel e-bankacılık geniş ölçüde token ve bir kerelik(tek kullanımlık) şifreler kullanılarak yapılmaktadır. Ancak sertifika kullanımı tedricen artmaktadır. Birçok e-bankacılık uygulamasında e-imza sisteme giriş amacıyla kullanılmaktaysa da elektronik imza ile yapılan işlemler giderek artmaktadır. Aynı zamanda çok az e-bankacılık uygulamasında akıllı kart kullanılmaktadır. Kurumsal e-bankacılıkta ise (B2B kurumlar arası e-ticaret) ve bankalar arası takas işlemlerinde yüksek güvenlik nedeniyle akıllı kart kullanılmaktadır. (Beder, 2005)

E-devlet, Avrupa'da hızla gelişen bir e-imza uygulaması olma yolundadır. Avusturya, Danimarka, Finlandiya, Almanya, İrlanda, İtalya, İsveç, Estonya, Slovenya, Çek Cumhuriyeti, Polonya, Romanya ve İngiltere gibi ülkeler e-devlet uygulamalarına başlamışlardır. Belçika, Hollanda ve Macaristan ise bu tür uygulamaya başlamayı planlamışlardır. E-devlet uygulamaları sıkça elektronik kimlik kartına dayalıdır. (Beder, 2005)

Avrupa da genel olarak e-imzanın yaygın kullanımının ve pazarda kabul görmesinin önündeki en büyük engel ulusal ve uluslararası düzeyde birlikte kullanılabilirlik (interoperability) konusundaki eksikliktir. Sadece tek bir Sertifika Sağlayıcı alınan ve sadece bir uygulama için kullanımın olması e-imza uygulama adacıklarının oluşmasıyla sonuçlanmaktadır. (Beder, 2005)

Avrupa'da e-imza kullanıcı maliyetleri büyük değişikliler göstermektedir. E-bankacılık uygulamalarında neredeyse bedava olup e-devlet uygulamalarında akıllı karta dayalı olarak yıllık 60 Euro'yu bulmaktadır. (Beder, 2005)

### 4.3. Dünyada E-imza Uygulamaları

#### 4.3.1. Avrupa Birliği İlk E-İmza Uygulamaları

##### 4.3.1.1. Siemens ve SBS Kurumsal PKI Projesi

Dünyanın en büyük kurulu sitelerinden birini oluşturmuş ve işletmektedir. Sertifika Otoritesi, tek merkezden tüm dünyadaki Siemens ve SBS çalışanlarına (2001'den itibaren 190 ülkede, 500 lokasyonda 484.000 kullanıcı) sayısal imzalar ve

şifreleme yoluyla güvenlik çözümü sağlanmıştır. E-posta, dosya ve veri şifreleme, logon, intranet ve ERP erişimi ve iş süreçleri yönetimi alanlarında güvenlik talep eden müşteriye sayısal imzalar, sayısal sertifikalar, sertifika yönetimi, son kullanıcı yazılımları sunulmuştur. Proje kapsamında AAA hizmetleri Akıllı Kartlar ile bütünleşik halde sunulmuştur. Kurum içi ve kurumlar arası güvenli iletişim, iyileştirilmiş ve otomasyonu sağlanmış iş süreçleri, zamandan tasarruf ve yönetilen AAA sayesinde kolay uygulanabilen ve düşük maliyetli çözüm sağlanmıştır. (TK, 2004b)

#### 4.3.1.2. Sanal Şehir Hagen

Sanal Şehir Hagen projesi tüm kamu hizmetlerine sanal ortamda erişim sağlayarak "e-devlet" uygulamalarının temelini oluşturmuştur. İhtiyaçları, erişimde gizlilik ve doğrulama, sayısal imzalar, açık, ileriye dönük ve standart bir çözüm, güvenli ödeme sistemleri ve "e-devlet" ve "çevrim-içi yönetim"de yönetim süreçlerinin düzenlenmesi olan müşteriye yeni teknolojiye geçişte esnek bir yapı, gizliliğin, doğrulamanın şifreli veri transferi ve sayısal imzalarla sağlanması ve Açık Anahtar Altyapısı ile bütünleşik bir çözüm sunulmuştur. Vatandaşın işini kolaylaştıran, "bilişim toplumu" için uygun olan bu çözümle yönetimsel süreçlerin düzenlenmesi ve hızlandırılması, vatandaşa ait bilgilerin gizliliğinin sağlanması, hizmetlere kolay erişim, sayısal imzaların kullanımıyla zaman kazanımı sağlanmıştır. (TK, 2004b)

#### 4.3.1.3. Fransa Maliye Bakanlığı

Fransa Maliye Bakanlığı, 1998 yılında kurumların internet üzerinden vergi beyanını mümkün kılmaya karar verdi. 15 milyon €'dan fazla geliri olan 20,000 firmanın vergi beyanlarını internet üzerinden gerçekleştirmesi zorunluluğu yasalarla getirildi. Bakanlık, kendisi sertifika otoritesi olarak davranmak yerine bu kararını gerçekleştirmek üzere, sertifika dağıtımını yapmayı üçüncü partilere bırakmayı tercih etti. Güvenlik alanında çözümler sunan Verisign'ın bölgedeki iş ortağı Certplus, belli başlı Fransız bankaları ile çalışarak kurumlara sayısal sertifikaların dağıtımı ve kurulumu için gerekli çalışmaları gerçekleştirmiştir. Certplus'ın ilk aşamada dağıttığı 25,000 sertifika aktif bir şekilde kullanılmaktadır. Bu sayı 80,000'lere ulaşmaktadır. Sağlanan çözüm ile hem zaman, hem de maliyet ve insan kaynağından tasarruf sağlanmıştır. (TK, 2004b)

#### 4.3.1.4. Köln Şehri Kartı

Köln Şehir Kartı Projesi, belediye hizmetleri içerisinde bulunan iş süreçlerinin, çalışanlar ve vatandaşlar için güvenli elektronik bir ortama taşınması süreçlerini kapsamaktadır.Vatandaş ve belediye arasındaki elektronik iletişimin sağlanması, yasal olarak kullanılan sayısal imzalar için teknik altyapı ve açık, ileriye dönük ve standart bir çözüm gibi ihtiyaçlara yönelik olarak Açık Anahtar Altyapısı ile akıllı kartların bütünleştirildiği bir çözüm sunulmuştur. Buna bağlı olarak iş süreçleri sayısal imzalar yardımıyla iyileştirilmiş; çoklu uygulamalı kartlarla birlikte çözüm eğitim, kültür ve sağlık alanına da genişletilmiştir. Proje "Bilişim toplumu"na geçişte önemli bir adım olarak görülmüştür. Yönetimsel süreçlerin düzenlenmesi ve hızlandırılması, bilgisayar ağları ve fiziksel erişimde aynı altyapının kullanılması, vatandaşa ait bilgilerin gizliliğinin sağlanması, hizmetlere kolay erişim ve sayısal imzaların kullanımıyla zaman kazanımının sağlanması sağlanan diğer önemli faydalar olarak sıralandırılabilir. (TK, 2004b)

#### 4.3.1.5. Italya İçişleri Bakanlığı Italyan Kimlik (ID) Kart Projesi

İtalyan İçişleri Bakanlığı'nın vatandaşlarının kimlik tanınmalarının geliştirilmesi ve vatandaş ile kamu otoriteleri arasındaki ilişkinin kamu kuruluş binalarının dışına taşınmasını sağlamak amacıyla oluşturduğu çözüm, akıllı kart teknolojisine dayalı yeni bir kimlik kartı üstüne kurulmuştur. Proje kapsamında merkezi PKI yönetimi ile güvenli, belediyelerde online elektronik kimlik kartı dağıtımı prosedürleri ve süreçleri gerçekleştirilmiştir. Proje pilot aşamasında Milano, Parma ve Roma'da bulunan 83 belediye ve 280,000 vatandaşı kapsamıştır. 5 yıl içerisinde İtalyan Hükümeti yaklaşık 40 milyon elektronik kimlik kartı oluşturacaktır. (TK, 2004b)

#### 4.3.1.6. Finlandiya

Finlandiya'da uygulanmakta olan iki akıllı kart projesi bulunmaktadır. Bu projelerden bir tanesi sağlık bilgilerinin takibi, diğeri ise 19 Avrupa ülkesinde geçerli olacak kimlik kartı ve pasaport uygulamaları içindir. Vatandaşların özel sağlık bilgilerine, bankaların ulaşmalarının sakıncaları göz önüne alındığında, bu iki projenin ayrı olarak yürütülmesine karar verilmiştir."Passport Card" adı verilen uygulama, kimlik belirleme sertifikasını, kart sahibinin sayısal imza sertifikasını ve

Nüfus Kayıt Merkezi'nin resmi sertifikalarını içermektedir. Özel bilginin kart üzerinde tutulması bir yonga ile sağlanmakta olup, bu kart bir PIN (Kişisel Kimlik Sayısı) kullanımı sayesinde şifreli olarak korunmaktadır. Öncelikli olarak kimlik ve seyahat belgesi niteliği taşımakta olan bu karta, e-bankacılık, e-sigorta, bölgesel ve kamu yönetimlerince sağlanan diğer hizmetler de dahil edilecektir.

#### 4.3.1.7. Danimarka

Danimarka İstatistik Kuruluşları ve Danimarka Ticaret ve Firma Acentaları (DCCA), faaliyet gösterdikleri alanlarda, Internet ve e-posta tabanlı uygulamalarına ağırlık vermektedirler. Sayısal imza kullanımı neticesinde, işlem verimliliği ve çeşitliliği arttırılmıştır. OCES (Elektronik Servisler için AÇIK Anahtarları), Danimarka'nın Ulusal AAA'sını oluşturmuş olup, bu durum sayısal imzaya geçiş süreci yaşayan özel ve kamu kuruluşlarında önemli ve fark edilebilir bir etki yaratmıştır. (Özeren)

#### 4.3.1.8. Hollanda

Hollanda, Sayısal İmza Yasası'nı, bir yıldan fazla süren bir süreç sonunda, Mayıs 2002'de kanunlaştırmıştır. Hali hazırda, akıllı kartlar üzerinde kullanıcı parmak izi doğrulamasına yönelik bir çalışma olan biyometrik projesi geliştirilmektedir. Bu uygulamaya göre, kullanıcı kimliğinin biyometrik araçlarla doğrulanması sonucunda, kişisel e-postaların ve dokümanların mahremiyeti sağlanacaktır. (Özeren)

#### 4.3.1.9. Almanya DSV

DSV (Deutscher Sparkassen Verlag) Alman bankacılık sisteminin (Sparkassen Finanzgruppe) servis sağlayıcısıdır. Deutscher Sparkassen Verlag (DSV), sunduğu bankacılık alanına yönelik ürün ve hizmetleri ile yaklaşık 600 kuruluşu (tasarruf bankaları, kamu bankaları, kamu sigorta şirketleri, v.b.) ve 18,000 şubeyi içeren Sparkassen-Finanzgruppe (Almanya tasarruf bankaları kurumu) için ana tedarikçi konumundadır. DSV, Finans kuruluşlarına Pazarlama ve medya hizmetleri, debit ve kredi kartları basımı, elektronik ödeme sistemleri ve ATM'ler için terminaller de dahil olmak üzere fonksiyonel bazda ürün ve hizmet sunmaktadır.Önümüzdeki yıllarda basılacak ***20 milyon akıllı kart***a, VeriSign'ın dijital sertifika hizmetlerini kullanarak sertifika eklemeyi ve 600 üye finans kuruluşunun ***e-mail doğrulama*** işlemleri için dijital sertifika altyapısı sunmayı planlamaktadır. Sayısal sertifikalı

akıllı kartlar, kullanıcılarının doğrulanmasında ve kullanıcıların internet üzerinden daha güvenli işlem yapmalarına olanak sağlamaktadır.Buna göre DSV, Verisign'ın yönetilen sayısal sertifika hizmetlerini genel bankacılık hizmetlerini daha güvenilir hale getirmek için kullanmaktadır. (TK, 2004b)

#### 4.3.1.10. Identrus

Nisan 1999'da 8 büyük banka (ABN AMRO Bank, Bank of America, Bankers Trust, Barclays Bank, Chase Manhattan, Citibank, Deutsche Bank ve Hypo Verinsbank) tarafından bir "güven şirketi" olarak kurulan Identrus, şu anda 60'ın üzerinde finansal kuruluşu bünyesine katmış durumdadır. Üye bankalardan ***10 tanesinin Türkiye***'de temsil edilmektedir. (ABN AMRO, BNP Paribas, Citigroup, Credit Lyonnais, Dresdner Bank, HSBC Group, ING Group, J.P.Morgan Chase & Co., Société Générale, West LB) Identrus, Verisign'ın partnerliği ile, üye bankaların, müşterileri olan şirketlere dijital sertifika vermesini sağlayan sistem operatörlüğü görevini yürütmektedir. (TK, 2004b)

Identrus, bankalar, banka müşterilere ve devletler gibi pek çok partiye farklı açılardan avantajlar sunan bir sistemler bütünüdür. Identrus bankalara artan gelir, ilişki yaratma / yönetme daha etkin geleneksel hizmetler ve yeni hizmet sunma olanağı, marka yaratma ve risk yönetimi açılarından faydalar sağlamaktadır. Bu sistemle banka müşterilerine (şirketlere) ise daha düşük işlem maliyetleri, işlemlerin kaydının tutulması, gerçek zamanlı kimlik doğrulama, global pazara erişim şansı, kuralların tüm partilere tutarlı şekilde uygulanması, artan ciro, yeni pazarlar ve daha yüksek müşteri değeri gibi faydalar yaratılmıştır. Devlet açısından ise yeni diplomatik kanalların oluşumu, denetleme gücünün artması gibi pozitif etkileri vardır. İhaleye katılan firmanın kendisinin tanınmaması durumunda bile Identrus tarafından sertifikalanmış bir firmanın kredilitesinin yüksek kabul edilebilir olması, ihalelerde şirket tanınmalarında kolaylık sağlamaktadır. (TK,2004b)

#### 4.3.1.11. İngiltere - Barclays

Barclays, temelde bireysel bankacılık, yatırım bankacılığı ve yatırım yönetimi konularında faaliyet gösteren, İngiltere'deki finansal hizmet sunan en büyük gruplardan biridir. Barclays'in 2003 sonu itibariyle 700,000'in üzerinde kurumsal müşterisi ve internet bankacılığını kullanan 4,5 (285,000'i kurumsal) milyon müşterisi bulunmaktadır. (TK, 2004b)

Barclays, PKI altyapısını kurması ve işletmesi için BT Ignite ile çalışmaya karar vermiş, güvenlik çözümleri sağlayan bu kurum, elektronik ticaretin kullanımı sırasında hem Barclays grubu şirketlerini, hem de müşterilerini korumak üzere güvenli teknoloji çözümlerini (PKI) sağlamıştır. Bu hizmet ile Barclays, müşterileri ile arasında ve aynı zamanda kurum içerisinde, elektronik ortamdaki bilgi alışverişini güvenli hale getirmiştir. Ayrıca kurumsal müşterilerine kendi müşteri ve tedarikçileriyle internet ortamında daha güvenli işlemler gerçekleştirmelerini sağlayacak hizmetler geliştirme fırsatına sahip olmuştur.

### 4.3.2 Asya Ülkeleri

#### 4.3.2.1. Japonya - Suzuken Firması

Suzuken, merkezi Nagoya'da yer alan ve ülke çapında 110.000 eczane ve ilaç kuruluşuna ilaç ve tanı medikal ekipmanı sağlayan bir ilaç toptancısıdır. Suzuken Grubu, Sanwa Kagaku Kenkyusho Co., Ltd. (ilaç şirketi), Nihon Seiyaku Kogyo Co., Ltd. (ilaç üreticisi), Kenzmedico Co.,Ltd. (ekipman üreticisi) ve Lifemedico Co., Ltd. (sağlık alanda faaliyet gösteren reklam şirketi) şirketlerinden oluşmakta olup sağlık hizmetleri alanında toplu bir güce sahiptir.

Suzuken, 2001 yılında ilaç şirketleri yani müşterileri ile olan bilgi alışverişi ve online ürün talepleri için web tabanlı bir satış destek sistemini hizmete sokmuştur. Bu sistemdeki e-posta,ürün talep bilgileri ve diğer değerli bilgilerin güvenli için PKI teknolojisi kurulmuştur. Buna göre bir sertifika otoritesi her kurumdaki her bir satış temsilcisi için sertifika dağıtımını gerçekleştirmiş ve bu sertifikalar sayesinde kimlik doğrulama ve onay işlemleri gerçekleştirilmeye başlanmıştır. Müşterilerin ilk giriş sayfasında kimlikleri onaylandıktan sonra diğer sayfalarda tekrardan güvenlik için bilgi sormaya gereklilik ortadan kalkmış ve böylelikle de sistemin kullanıcılar tarafından kullanımı kolaylaşmıştır.

#### 4.3.2.2. Hong Kong – Hong Kong Post

Hong Kong sertifika otoritesi 2000 yılından itibaren sadece 110,000 e-Cert (sayısal sertifika) satabilmiştir. Kurum sertifika kullanımını artırmak için, akıllı kimlik kart sahiplerine sertifikaları kartlarına yerleştirme olanağını bir yıl için hiç bir ücret almadan gerçekleştirme önerisiyle gitmiştir. Temmuz 2003'ten itibaren Hong Kong kimlik kartı sahipleri, var olan kimlik kartların akıllı kimlik kartları ile değiştireceklerdir. Bu süreç dört yıl sürecektir.

### 4.3.3. Amerika Kıtası Ülkeleri

#### 4.3.3.1. ABD Savunma Bakanlığı Dışsal Sertifika Otoritesi Programı

ABD Savunma Bakanlığı, Bakanlık ile tedarikçiler arasındaki online işlemleri daha güvenli hale getirmek üzere bir sistem kullanmaya karar vermiş ve buna bağlı olarak da Verisign'ı gerekli olan sayısal sertifikaların sağlayıcısı olarak tercih etmiştir.

ECA programı (Dışsal Sertifika Otoritesi), ***Savunma Seyahat Sistemi, Elektronik Doküman Girişi ve Geniş Alan İş Akışı*** olmak üzere üç programı kapsamaktadır. İleriki dönemlerde program, bakanlığın 350.000'den fazla iş ortağını da kapsayan, daha geniş uygulamalar ile daha gelişmiş bir ECA programı haline gelecektir. (TK 2004b)

#### 4.3.3.2. Sağlık Enstitüleri

ABD'de Sağlık Enstitüleri, AAA' ya geçiş uygulamalarında lider kuruluşlar arasında yer almaktadır. Doktorlar, hastaneler ve laboratuarlar, oluşturulan elektronik dağıtım kanalı sayesinde hasta kayıtlarının güvenliğini sağlamaktadırlar. Sağlık Sigortası Taşınabilirlik ve Sorumluluk Kanunu (HIPAA), Amerikan Kongresi tarafından 1996'da yürürlüğe konulmuştur. Bu yasa, AAA sistemlerinin sağlık kurum ve kuruluşlarına yerleştirilmesini şart koşmuştur. Bahse konu kanun, ikinci aşama olarak özel hasta bilgilerinin Internet üzerinden paylaşımının gerçekleştirilmesini hedeflemektedir. Bu sebeple, sağlık kurum ve kuruluşları, AAA uygulamalarının yurt çapında yaygınlaştırılması çalışmalarına hız vermiştir. (Özeren)

Hasta mahremiyetinin sağlanması için gerekli olan güvenlik politikalarının oluşturulması amacıyla, yapılması gereken işlemler ve teknolojiler belirlenmiştir. Böylelikle sağlık kurum ve kuruluşları, yenilenen Internet teknolojileri ile geçmişteki problemlerin üstesinden gelebilecek, maliyetleri düşürebilecek ve verimliliği arttırabilecek bir yapıya geçiş yapabileceklerdir. (Özeren)

#### 4.3.3.3. Kanada Elektronik Tapu ve Kadastro Kayıt Sistemi

Kanada, Elektronik Tapu ve Kadastro Kayıt Sistemi'ni ilk geliştiren ve uygulamaya koyan ülkedir. Devlet ile özel bir kuruluşun gerçekleştirdiği bu sistem, dünyadaki ilk kullanıcı tabanlı ve tamamı elektronik olan ortaklıktır. Buna istinaden,

arsa kayıt dokümanlarının oluşturulması, imzalanması, gönderilmesi ve faturalandırılması elektronik ortamda yapılmaktadır. Bu sistem, Kanada Bilişim Verimlilik ödülü kazanmıştır. (Özeren)

#### 4.3.3.4. Kanada CIBC (Canadian Imperial Bank of Commerce)

CIBC, 9 milyondan fazla bireysel ve kurumsal müşterisi bulunan, Kuzey Amerika'nın lider finansal kuruluşlarından biridir. CIBC, kapsamlı elektronik bankacılık ağı boyunca müşterilerine bankacılık alanında uçtan uca ürün ve hizmetler sunmaktadır ve aynı zamanda Verisign'ın Kanada'daki iş ortağı, işleme merkezi (processing center) olarak da faaliyet göstermektedir. CIBC işleme merkezi, Verisign'ın PKI platformu, güven hizmetleri altyapısını ve işletme hizmetlerini içine almaktadır. CIBC temelde *web sunucu* ve *işletme sertifika* hizmetlerini sunmaktadır. CIBC, Kanada çapında sertifika otorizasyon hizmetlerini sağlamakta ve sertifika işlemlerinin yanı sıra pazarlama, satış, güvenlik, müşteri destek ve operasyon yönetimi gibi hizmetleri de sunmaktadır.

CIBC, imza gerektiren uygulama ve hizmetlerine online olarak ulaşma ve kullanma olanağını müşterilerine sunmayı ve böylelikle de müşteri rahatlığı ve memnuniyetin artırırken uygulama süreç maliyetlerini azaltmayı hedeflemiştir. Normalde bütün CIBC müşterileri VISA kartı, banka hesabı açtırma gibi işlemler için şubeleri ziyaret ederek, yada posta yoluyla başvuru talebini yaparak süreci başlatabiliyorlardı. Bütün başvuruların müşteri tarafından imzalanmış olması gerektiğinde müşterilerin fornu ya direk şubeden almaları yada posta yoluyla alıp imzalayıp tekrar geri göndermeleri gerekiyordu. CIBC bu süreci hızlandırmak ve kolaylaştırmak istedi. 2001'in Şubat ayında CIBC bireysel banka müşterilerine sayısal imza kullanarak uygulamaları imzalama ve bütün bankacılık hizmetlerini online olarak alabilme olanağını tanıyan Kanada'daki ilk banka olmuştur.Daha fazla Kanadalı firmanın ve bireyin elektronik ticaret işlemlerini güvenli bir şekilde gerçekleştirmeleri sağlanmış, banka müşterilerinin memnuniyeti artarken, CIBC de maliyetlerden ve işlemler için harcanan zamandan tasarruf sağlamıştır. (TK,2004b)

### 4.4. Türkiye'de E-İmza Oluşumu ve Uygulamaları

Elektronik İmza Kanun Tasarısı, 15 Ocak 2004 tarihinde TBMM Genel Kurulu'nda görüşülerek kabul edilmiş, Kanun, 23 Ocak 2004 tarih ve 25355 sayılı Resmi Gazete'de yayımlanmıştır. İkincil düzenleme çalışmaları TK'na verildiğinden

Kanunun verdiği 6 aylık zamandan önce ikincil mevzuat çalışmaları tamamlanarak yürürlüğe girmiştir. Mevzuat çalışmalarının ardından elektronik imzanın uygulamaya girmesi için gerekli çalışmalar başlamıştır. (Orta)

2003-2004 yıllarını kapsayan Kısa Dönem Eylem Planı'nın ilk maddesi e-Dönüşüm Türkiye Projesi'nin toplumun tüm kesimlerini kapsayacak, ulusal fayda ve katma değeri arttıracak şekilde gerçekleştirilmesi amacıyla Bilgi Toplumu Stratejisi'nin oluşturulmasıdır (DPT, 2004). Eylem planı Bilgi Toplumu Stratejisi'nin yanı sıra, düzenleyici ve yasal çerçevenin çizildiği hukuki altyapı, hizmetlerin sunulacağı teknik altyapı ve bilgi güvenliği, bilgi toplumunun gerektirdiği insan kaynağı planlamasına ve yetiştirilmesine yönelik eylemlerin yer aldığı eğitim ve insan kaynakları, hizmetlerin elektronik ortamda bürokratik engellere takılmadan kolayca sunulmasını hedefleyen e-devlet, kurumların birlikte çalışabilir entegre hizmetler sunmalarına yönelik olarak standartlar, e-sağlık ve e-ticaret ana başlıklarından oluşmaktadır (DPT, 2004).

E-ticarete ilişkin olarak yürütülen çalışmalar kapsamında, şirket bilgilerinin tutulacağı Şirket Sicil Kayıt Sistemi ile ilgili olarak TOBB tarafından geliştirilmekte olan Ticaret Sicili Arşiv ve Otomasyon Sistemi ile Sanayi ve Ticaret Bakanlığı tarafından hazırlanan Sanayi.NET Bilgi Sistemi arasındaki farklar tespit edilmiş; ticaret sicil memurluklarından toplanacak bilgilerin bakanlık şirket veri tabanına aktarılmasına karar verilmiştir. (DPT, 2005: 21-22).

Elektronik imzanın kamu kurumlarında otomasyonu sağlayacak şekilde yaygınlaştırılması ve özel sektörde elektronik ortamda verilen çeşitli belgelerin e-imza ile yasal geçerliliğinin sağlanması amaçlanmaktadır. Son olarak ise siber alandaki güvenlik tehditlerini takip edecek ve risklerin ortaya çıkması durumunda müdahale edecek bir Bilgisayar Acil Durum Tepki Ekibi'nin kurulması önerilmektedir (DPT, 2006b).

### 4.4.1. Sertifikasyon Merkezleri

Elektronik imza kullanımında en önemli aktörlerin başında elektronik sertifika hizmet sağlayıcıları (ESHS) gelmektedir. Elektronik sertifika hizmet sağlayıcısı olmak için şimdiye kadar biri kamu, üçü özel olmak üzere dört kurum faaliyete geçmek üzere TK'na bildirimde bulunmuş ve lisanslarını almıştır. Dolayısıyla elektronik imza kullanımı için gerekli elektronik sertifikalar bu kurumlardan

sağlanabilmektedir. Diğer taraftan ilk elektronik imza, 18 Temmuz 2005 tarihinde kullanılmıştır.(Orta)

Ulusal güvenlik gerekleri göz önünde bulundurularak, kurumsal sertifika ihtiyacının karşılanması amacıyla oluşturulacak kamu sertifikasyon yapısı içinde kurulacak olan kök sertifika hizmet sağlayıcısı ve Kamu Sertifika Hizmet Sağlayıcısı milli yazılım ürünlerini kullanacaktır. Böylelikle kurumsal sertifikaların tek merkezden sağlanması, kamu sertifikasyon yapısının kurulması sonucu bütün kamunun güveneceği bir Kök ESHS'nin kurulması öngörülmüştür. (Orta)

6 Eylül 2004 tarihinde yayınlanan ve 2004/21 numaralı Kamu Sertifikasyon Merkezi Oluşturulması konulu Başbakanlık Genelgesi ile kamu kurum ve kuruluşlarının elektronik imza kullanımı için yaralanacakları altyapının kurulması ve işletilmesi ile ilgili konulara açıklık getirilmektedir. Genelgeye göre tüm kamu kurum ve kuruluşlarının aynı kurumsal sertifikasyon yapısı altında toplanmasını hedefleyen, sadece kamu kurum ve kuruluşlarına kurumsal sertifikaların oluşturulması ve sertifika yaşam çevriminin yönetilmesini sağlayacak Kamu Sertifikasyon Yapısı'nın kurulması ve işletilmesi görev ve sorumluluğu Türkiye Bilimsel ve Teknik Araştırma Kurumu'na (TÜBİTAK) bağlı Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü Müdürlüğü'ne (UEKAE) verilmiştir. http://www.kamusm.gov.tr/tr/Bilgideposu/Mevzuat/

Yürüttükleri görev açısından özel niteliğe haiz olan Türk Silahlı Kuvvetleri, Emniyet Genel Müdürlüğü, MİT Müsteşarlığı, Jandarma Genel Komutanlığı, Sahil Güvenlik Komutanlığı ve Dışişleri Bakanlığı'nın kamu sertifika sistemlerini kendi bünyelerinde oluşturmalarına izin verilmiş, bu kurumlar dışındaki kamu kurum ve kuruluşlarının sertifika hizmet sağlayıcı olmak üzere kendi bünyelerinde yatırım yapmaları yasaklanmış; bu konuda başlatılmış ve sürdürülmekte olan bütün ihalelerin de iptal edilmesine karar verilmiştir (Başbakanlık, 2005).

Belirtilen istisnalar dışındaki tüm kamu kurum ve kuruluşları, sertifika ihtiyaçlarını karşılamak amacıyla sertifika hizmet sağlayıcısı olmak üzere kendi bünyelerinde hiçbir surette yeni yatırım yapmayacaklar, bu konuda başlatılmış ve sürdürülmekte olan ihale çalışmaları ile henüz sözleşmeye bağlanmamış olan tüm ihaleler derhal iptal edilecektir. Böylece bütün ihalelerin iptal edilmesi, halihazırda kullanılan sistemlerin en kısa sürede bu yapıya uygun hale getirilmesi öngörülmüştür. (Orta)

TÜBİTAK-UEKAE, e- GÜVEN (Elektronik Bilgi Güvenliği A.Ş.), E-TUGRA ve TÜRKTRUST (TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş.), ESHS olmak üzere TK'na başvurmuştur.

Türkiye Bilişim Vakfı tarafından bağımsız bir kurum olarak kurulan e-GÜVEN, TK tarafından Türkiye'nin ilk ESHS olarak yetkilendirilerek 24 Haziran 2005 tarihinde faaliyete geçmiştir. (Büke, 2005).

ESHS, EİK veya bu Kanuna dayanılarak çıkarılan yönetmelik hükümlerinin ihlâli suretiyle üçüncü kişilere verdiği zararları tazminle yükümlüdür. ESHS, kusursuzluğunu ispat ederse tazminat ödemek zorunda değildir (md. 13/2). (Orta)

ESHS, söz konusu yükümlülük ihlâlinin istihdam ettiği kişilerin davranışına dayanması hâlinde de zarardan sorumlu olup, ESHS, bu sorumluluğundan, Borçlar Kanununun 55'inci maddesinde öngörülen türden bir kurtuluş kanıtı getirerek kurtulamaz(Orta).

#### 4.4.1.1 Çapraz Sertifikasyon

Farklı e-imza altyapısına sahip ESHS'lerin vermiş olduğu elektronik sertifikaların birbirini tanıması ve farklı ESHS'lerden elektronik sertifika alan vatandaşların sorunsuz ve rahat bir şekilde güven ilişkisine girip işlemlerini yapabilmesi için bu ESHS'ler arasında, telefon işletmecileri arasında yapılan "arabağlantı" benzeri bir işlem olan, "çapraz sertifikasyon" yapılması gerekmektedir. Aynı e-imza altyapısını kullanan ESHS'lerin böyle bir işlem yapmasına ise gerek bulunmamaktadır. Bu itibarla, kök sertifika hizmetini TÜBİTAK-UEKAE'den alan bir ESHS'nin vereceği elektronik sertifikalar gerek kamusal gerekse özel işlemlerde sorunsuz bir şekilde kullanılabilecekken, bu hizmeti TÜBİTAK-UEKAE'den almayan bir ESHS'nin elektronik sertifikalarının kamusal işlemlerde kullanılabilmesi için "çapraz sertifikasyon" yapılması şart olacaktır. (Beydoğan)

E-devlet ve e-ticaret uygulamalarının artması ve yaygınlaşmasıyla elektronik sertifika ihtiyacı artacak ve önümüzdeki yıllarda pazar hızla büyüyecektir. İlerleyen dönemlerde önemli yapısal sorunların ortaya çıkmaması için pazarın oluşum sürecinde etkin ve sürdürülebilir bir rekabet ortamının tesis edilmesi şarttır. Bu itibarla, TK'nun ve Rekabet Kurumu'nun pazardaki gelişmeleri yakinen takip etmesi ve rekabeti bozması muhtemel gelişmeleri engellemek için özellikle TK'nun ihtiyaç duyulan adımları hızla atması gerekmektedir. (Beydoğan)

#### 4.4.1.2. KAMU SM

Kamu Sertifikasyon Merkezi (Kamu SM®), TÜBİTAK-UEKAE bünyesinde 2005 yılında kurulmuştur. Türkiye'nin ilk ESHS olan Kamu SM®, 5070 sayılı EİK'na uygun olarak kurulmuş ve işletilmektedir.

15 Ocak 2004 tarihli ve 5070 sayılı EİK'na göre, yetkilendirilmiş ESHS'ın vereceği güvenli e-imza, elle atılan imza ile aynı hukuki sonucu doğurmaktadır. Kanuna uygun olarak oluşturulmuş e-imza, bilgisayarda veya elektronik ortamda gerçekleştirilen onay işlemlerine hukuki dayanak kazandırır ve kağıdı ortadan kaldırır. Onay amaçlı irade beyanında bulunmak isteyen kişi, kurumunun elektronik evrak akış sisteminde, web üzerinden sunulan hizmetlerde ya da e-devlet hizmetlerinde e-imza kullanabilir.

Kamu SM®, kişilerin kimlik doğrulamasını sağlayıcı nitelikli sertifikasyon servislerde, elektronik belgelerin, elektronik veri ve donanımların güvenilirlik ve güvenliğini sağlayıcı hizmetlerde uzmanlaşmıştır. Kamu SM® tarafından oluşturulan e-imza, belgeyi imzalayan kişinin kimliğini tanıma amacıyla kullanılmaktadır ayrıca imzalı elektronik verinin/belgenin değiştirilip değiştirilmediğini tanımaya olanak vermektedir.

Kamu SM®, 5070 sayılı kanuna uygun Nitelikli Elektronik Sertifikaları hazırlamak ve bu sertifikaları imza oluşturma verileriyle birlikte Güvenli Elektronik İmza Donanım Araçlarına yükleyerek alıcılarına teslim etmekle yükümlüdür. Kamu SM®, sertifika başvurusunda bulunan kişilerin başvuru bilgilerini toplarken, sertifikaları hazırlarken ve teslim ederken güvenli ürün ve sistemleri kullanmak, hizmeti güvenilir bir biçimde yürütmek, sertifikaların taklit ve tahrif edilmesini önlemekle ilgili her türlü tedbiri almak ile yükümlüdür.

2006 yılında; toplam 64 kamu kurum ve kurulusu ile Nitelikli Elektronik Sertifika talepleri üzerine kurum uygulama analizi gerçekleştirilmiştir. Uygulama analizi olumlu bulunan toplam 36 adet kamu kurum ve kurulusu adına talepleri oranında Nitelikli Elektronik Sertifika üretimi gerçekleştirilmiştir.

#### 4.4.1.3. E- Güven

Elektronik Bilgi Güvenliği A.Ş.; Türkiye'de kurumların ve bireylerin Internet ve ilgili uygulamalardan daha güvenli ve güvenilir şekilde yararlanmalarını sağlayacak Sertifika Otoritesi Hizmetlerini sunmak amacıyla Türkiye Bilişim Vakfı (TBV) önderliğinde, 19 Kasım 2003'te kurulmuştur.

E-Güven, dünyanın bilgi güvenliği alanında lider kuruluşu VeriSign'ın Türkiye'deki ortağı Siemens Business Services ile giriştiği işbirliği sayesinde uluslararası alanda, sektöründeki en ileri ve en geniş teknolojik uygulamaya, güvenlik alt yapısına ve ağına sahiptir.

e-Güven, "Açık Anahtar Altyapısı'nda çalışan anahtarları, kişisel kimliklerle ilişkilendirerek "Sayısal Sertifika" üreten ülkemizin ilk "Sertifika Otoritesi"dir. Oluşturulan iş modeli, Sertifika Otoritesi, Sertifika Otoritesi Servis Sağlayıcısı ve Finans Kurumları olmak üzere üç bileşenden oluşmaktadır.

#### 4.4.1.4. Türktrust

TÜRKTRUST Bilgi, İletişim ve Bilişim Güvenliği Hizmetleri A.Ş., TSK Elele Vakfı'nın bir kuruluşu olarak, 14 Temmuz 2004 tarihinde kurulmuş ve 2 Ağustos 2004 tarihinde 12 Milyon YTL (12 Trilyon TL) sermaye ile ticaret sicilde tescil edilmiştir. TÜRKTRUST, öncelikle 5070 Sayılı EİK kapsamında yetkili ESHS olarak hizmet vermek üzere kurulum çalışmalarını başarıyla tamamlamış ve 18 Temmuz 2005 tarihinde TK'undan resmi törenle yetki belgesini alarak ticari faaliyete başlamıştır. 5070 Sayılı Kanun kapsamında, güvenli e-imza, nitelikli elektronik sertifika ve zaman damgası hizmetlerini vermektedir. TÜRKTRUST, geliştirmiş olduğu bu özel yazılımları ve yazılım bileşenlerini yurt dışına da ihraç edebilmek için çalışmalar yürütmektedir.

#### 4.4.1.5. E-Tuğra

EBG Bilişim Teknolojileri ve Hizmetleri A.Ş., yüzde yüz yerli sermaye ile kurulmuş ve 19 Temmuz 2005 tarihinde Ticaret Siciline tescil edilmiştir. ESHS olarak faaliyet göstermek amacıyla Türk e-İmza Mevzuatının öngördüğü kriterleri ve alt yapı çalışmalarını tamamlamış ve 20 Haziran 2006 tarihinde TK'na müracaat etmiştir. İki aylık inceleme sürecini başarı ile tamamlayan Şirket, 1 Eylül 2006 tarihi itibariyle ESHS olarak faaliyete geçmiştir.

### 4.4.2. Türkiye'de E-imza Uygulamaları

Uygulamalar açısından Türkiye'deki mevcut duruma bakıldığında; kurumsal işlemlerin ve vatandaşa yönelik hizmetlerin elektronik ortama aktarılmakta olduğu, bu anlamda kamu sektöründe birbirinden bağımsız çalışmalar yapıldığı, kurumların bilgi verme amaçlı olarak anakapı oluşturduğu, ancak henüz bu anakapılar üzerinden elektronik işlem yapılması çalışmalarının henüz başlangıç aşamasında olduğu görülmektedir. (Beder, 2005)

E-imzanın Türkiye'deki kamusal uygulamalarının;

- Her türlü başvurular (ÖSS, KPSS, pasaport başvuruları vb.)
- Kurumlar arası işlemler (Emniyet/Nüfus ve Vatandaşlık İşleri)
- Sosyal güvenlik uygulamaları (Emekli Sandığı, SSK, Bağkur)
- Sağlık uygulamaları (Sağlık personeli - hastaneler - eczaneler)
- Vergi ödemeleri
- Elektronik oy verme işlemleri

Ticari uygulamalarının ise;

- İnternet bankacılığı
- Sigortacılık işlemleri
- e-Sipariş ve e-Sözleşmeler alanlarında olması beklenmektedir.

Haziran 2004 tarihinde E-İmza Ulusal Koordinasyon Kurulu Altyapı Çalışma Grubu İlerleme Raporu'nda yer alan ve onbeş adet Kamu kurum ve kuruluşlarına yönelik yapılan bir araştırma sonucunda, Türkiye'de kamu sektörünün e-imza uygulamaları ile ilgili bazı beklentilerine ilişkin sonuçlar saptanmıştır. E-imzanın genel olarak kurum içi ve kurumlar arası kullanımının sistem girişleri şeklinde olacağı belirtilmiştir. Ankete katılan kamu kurum ve kuruluşları ise: Adalet Bakanlığı, Maliye Bakanlığı, Türkiye Noterler Birliği, Denizcilik Müsteşarlığı, Devlet Meteoroloji İşleri Genel Müdürlüğü, Devlet İstatistik Enstitüsü, Dış Ticaret Müsteşarlığı, Emekli Sandığı Genel Müdürlüğü, T.C. Merkez Bankası, Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü, T.C. Devlet Demiryolları, TİKA, TSE, SPK, Gümrük Müsteşarlığı'dır. (Beder, 2005)

Bazı kuruluşlar (DTM, TSE, NVİ, TİKA, TCDD) ise 6–12 ay gibi daha da kısa bir sürede e-imza uygulamalarını kullanıma almayı planladıklarını belirtmişlerdir. Her ne kadar e-imza kullanımı kamuda fazla yaygınlaşmamış olsa da Adalet Bakanlığı, T.C. Merkez Bankası (TCMB), SPK, Türkiye Noterler Birliği (TNB) gibi kurumların iş süreçlerine e-imzayı dahil ettikleri gözlenmiştir. Bu kurumların e-imzayı özellikle kurum içi ve diğer kurumlarla olan işlemlerinde kullandıkları göze çarpmaktadır. Vatandaş ile doğrudan ilişkisi olan ve e-imza kullanmayı planlayan birçok kuruluş da vatandaş ile olan işlemlerinde e-imza altyapısından faydalanacağını belirtmiştir.

Geliştirilecek olan/geliştirilen uygulamalarda ekseriyetle yerli çözüm sağlayıcı firmalarla çalışılması tercih edilmektedir. Her kurum altyapısının kapasitesini kurum içi ve birlikte çalıştığı kişilerle/kurumlarla ilişkilerindeki ihtiyaçlara göre kurmuştur/kurmayı planlamaktadır.

Halihazırda e-imza kullanmayan fakat kullanmayı planlayan kurumların hemen hepsi amaç olarak kurum içi ve kurumlar arası işlemlerin hızlandırılmasını ve elektronik ortamda yapılan işlemlere yasal geçerlilik ve güven unsuru kazandırılmasını göstermiştir. Bununla birlikte e-imza'nın özellikle kamu kuruluşları arasındaki işlemlerde ve kurumların iş ilişkisi içinde bulundukları bankalar, finansal şirketler ve ithalat ihracat şirketleri, medya kuruluşları gibi özel kurumlar ile yapılan elektronik ortamdaki belge ve veri alışverişi için kullanılmasının planlandığı göze çarpmaktadır.

Vatandaşa sunulacak hizmetlere erişimin kolaylaştırılması kısıtlı oranda hedeflenmektedir. Bu alanlarda hemen hepsinde sistem erişimleri/loginleri'nin temel kullanım amacı olarak görüldüğü anlaşılmaktadır. Ayrıca kurum içinde elektronik belge/verilerin imzalanmasının ve kurumlar arasında bunların şifrelenmesine yönelik kullanımın amaçlandığı da göze çarpmaktadır. Vatandaşlara yönelik kullanımda çok yaygın olarak hedeflenen ise belge ve verilerin elektronik ortamda imzalı olarak iletilmesidir.

Yapılan çalışmalarda, halen bir çok kurum ve kuruluş tarafından yeni bir kavram olarak gözlenen e-imza konusunda en can alıcı noktalardan biri olan bilgilendirme konusunun ve akabinde yeni başlaması planlanan projeler için, kurumlar arası veri entegrasyonunun mevcut çalışmanın vazgeçilmez bir parçası

olarak ele alınmasının, çalışmaların verimli ve ileriye yönelik olarak hazırlanmasında dikkate alınması gereken önemli hususlar olduğu düşünülmektedir.

TÜBİTAK BİLTEN tarafından geliştirilmiş *ZEUGMA Sertifika Hizmet Sağlayıcısı Yönetim Yazılımı* aşağıdaki projeler kapsamında ilgili kurumlarda kullanılmaktadır:

SPK ve İstanbul Menkul Kıymetler Borsası (İMKB) KAP, Sosyal Sigortalar Kurumu (SSK) Başkanlığı Sigorta İşleri Genel Müdürlüğü Merkez ve Taşra Teşkilatı Donanım Yaygınlaştırma ve Altyapı Projesi (e-sigorta, e-bildirge). KAP, Türkiye'de elektronik imzanın kullanıldığı ilk resmi uygulamadır. SSK'ya sertifika yönetim Projesi ise, elektronik imzanın yaygın kullanımını amaçlayan Türkiye'deki ilk uygulamadır. (TK 2004b)

#### 4.4.2.1 Sermaye Piyasası Kurulu- Kamuyu Aydınlatma Platformu (KAP)

Sermaye piyasalarında işlem gören halka açık şirketlerin ve tüm aracı kuruluşların mali tablolarının, özel durum açıklamalarının ve diğer bildirimlerinin bilgisayar ağları üzerinden elektronik imza teknolojisi kullanılarak güvenli bir şekilde iletilmesini hedefleyen KAP; SPK ve İMKB ortaklaşa gerçekleştirilmiştir. (Beder, 2005)

KAP kapsamında İMKB'ye kote olan anonim şirketlerin, bağımsız denetim şirketlerinin ve aracı kuruluşların yetkililerine ve SPK-İMKB ilgili uzmanlarına toplam 2.200 akıllı kart ve okuyucu ile elektronik sertifikalar dağıtılacaktır. Gerekli kurulum işlemleri yerinde - şirket merkezlerinde - gerçekleştirilecek ve sistemi kullanacak tüm ilgililere gerekli kullanıcı eğitimleri verilecektir. Ayrıca KAP ile oluşturulacak sistemin 7x24 kesintisiz hizmet vermesinin sağlanması amacıyla gerekli teknolojik alt yapı ve güvenlik önlemleri hem donanım hem de yazılım anlamında alınmaktadır. (Özer s:6)

Kamuyu Aydınlatma Platformu bir e-Devlet uygulamasında olması gereken tüm unsurları (Devlet: SPK, Şirket: KAP şirketleri, Vatandaş: Sermaye Piyasası Yatırımcısı) içermesi sebebiyle, tam bir e-Devlet uygulaması olarak Sermaye Piyasası Kurulunun AB sürecinde attığı önemli bilişim yatırımlarından birisi olarak durmaktadır. Coğrafi olarak tüm Türkiye'ye yayılmış 530'ü aşkın şirketi ve 2500'ü aşkın kullanıcıyı kapsamaktadır. (Beder, 2005)

KAP kapsamında geliştirilen ve şirketlerin kullanımı için hazırlanan uygulama yazılımı aracılığıyla bildirimler doldurulur ve belirli bir hiyerarşide imza yetkisine haiz kişilerce, elektronik imza ile imzalanarak internet üzerinden SPK sistemine gönderilir. Gönderilen bildirimler veri tabanına kaydedilir ve anında kamuoyu ile paylaşılır. Şirket bildirimlerini yazılımlara çevrim dışı olarak kaydedebilir. Belli dönemlerde bağımsız denetim şirketleri de elektronik imzalarını bildirim gönderme sürecindeki sırası ile atarak bildirim gönderme sürecine katılmaktadırlar. (Beder, 2005)

KAP, elektronik imzanın Türkçe elektronik belgelere entegrasyonunun sağlandığı ve Türkiye'de sertifika hizmet sağlayıcılığı konusundaki ilk işletme uygulamasıdır. (Beder, 2005)

Sermaye Piyasası Kurulu, İMKB ve TÜBİTAK-UZAY tarafından ortaklaşa yürütülmekte olan KAP çalışmalarında, sistemin 24.11.2006 tarihi itibariyle internet hatları üzerinden devreye alınması sonrasında, Genel Test Grubu oluşturularak çalışmalara başlanmış ve ilişikte yer alan **"KAP Genel Test Çalışması Esasları"** belirlenmiş ve halen test uygulaması devam etmektedir.

Yukarıda bahsedilen hususlara ve ilgili diğer dokümanlara Sermaye Piyasası Kurulu internet sitesinden (http://www.spk.gov.tr/kap) erişilebilir. (Beder, 2005)

**KAP'ın Sonuçları ve Kazanımları**

Kamuyu Aydınlatma Projesi ile Türkiye'de bir ilk gerçekleştirilerek elektronik imza ve akıllı kartların geniş ölçekte kullanımı sağlanacaktır. Böylelikle Türk Sermaye Piyasalarında bulunan tüm şirket, kurum ve kuruluşlar arası güvenli veri iletişim alt yapısının temelleri atılmış olacaktır. Kanunlar ve mevzuatlar gereği yerine yetirilmesi zorunlu bildirim ve bilgilendirmeler kolaylaşacak, zaman kayıpları büyük ölçüde giderilerek şirketler üzerindeki iş yükleri azalacaktır. Öte yandan sermaye piyasalarında denetim ve gözetim faaliyetlerini yerine getirmekte olan kurum ve kuruluşların doğru veriye zamanında ulaşması sağlanarak verinin bilgiye dönüşüm hızı artırılacaktır. Böylelikle karar verme süreci kısalarak denetim ve gözetim süreci daha da etkinleşecektir. (Özer s:7)

**Güvenilirlik:** Faks veya posta yoluyla gelip yayınlanan bilgilerin elektronik imza ile gönderilmesi suretiyle verilerin güvenilirliği sağlanmaktadır. (Beder, 2005)

**Bilgiye Ulaşma:** Yapılan açıklamaların bekletilmeksizin, sisteme gönderildiği anda kamuya açıklanması suretiyle kullanıcılar eş zamanlı, güvenli ve hızlı bir şekilde bilgiye ulaşmış olacaklardır. Bu durum içeriden öğrenenlerin ticareti (insider trading) uygulamalarını da azaltacaktır. (Beder, 2005)

**Bilgide Etkinlik**: Kullanıcılar bilgiye daha hızlı ulaşmalarının yanında, mali tablo karşılaştırma, mali tablo kalemlerinin karşılaştırılması ve özel durum açıklamalarını konularına göre karşılaştırma olanaklarını kullanarak daha kullanılabilir ve etkin şekilde ulaşmış olacaklardır. Sorgulamalar ve mali analiz için gerekli alt yapı da kurulmuştur. (Beder, 2005)

**Güncellik:** Her bir şirket bazında, ilgili şirket hakkında yatırımcılar için önem taşıyan genel bilgileri içeren "Şirket Genel Bilgi Formu" adı altında bir form oluşturulmuştur. Bu formun büyük bir kısmı şirketler tarafından yapılan özel durum açıklamalarıyla otomatik olarak güncellenmektedir. Bu şekilde hem kullanıcılar ilgili şirket hakkındaki bilgilerin sürekli olarak son şeklini görebilmekte, hem de ilgili şirketler kendi bilgilerini güncellemek için ekstra bir çaba harcamamaktadırlar. (Beder, 2005)

**Tam ve Yeterli Bilgi:** Tasarruf sahipleri, ortaklar ve diğer ilgililerin zamanında bilgilendirilmesini temin etmek suretiyle hazırlanan iligili Tebliğ uyarınca şirketler, Tebliğde yer alan hususlarda kamuya özel durum açıklaması yapmaktadırlar. KAP kapsamında yapılacak her bir özel durum açıklaması için ayrı olmak üzere yaklaşık 250 adet özel durum şablonu oluşturulmuştur. Oluşturulan her bir şablonun her bir hücresi sorgulamaya müsait olarak dizayn edilmiştir.(Beder, 2005)

**Maliyetlerde Azalma:** Mevcut durumda kağıt ortamında SPK ve/veya İMKB'ye gönderilen bilgilerin elektronik ortamda sisteme gönderilmesiyle zaman, kağıt ve işgücü tasarrufu sağlanmış olacaktır. (Şirketler tarafındaki iş gücü hesaba katılmadan, sadece kağıt tasarrufuyla yılda yaklaşık 300 bin YTL'lik bir kazanç sağlanmış olacaktır.) (Beder, 2005)

e-SPK, e-Devlet projeleri arasında KAP çok önemli bir mihenk taşıdır. Çünkü ilerleyen yıllarda kağıt ortamındaki bildirimlerin sadece elektronik olarak yapılmasının yeterli olacağı düşünüldüğünde bu sürecin teknolojik ayağı sermaye piyasalarında KAP ile gerçekleştirmiş olacaktır. (Özer s:7)

#### 4.4.2.2. Dış Ticaret Müsteşarlığı- Dahilde İşleme Rejimi Projesi

Dış Ticaret Müsteşarlığı'nın Dahilde İşleme Rejimi (DİR) projesi, Türkiye çapında 13 İhracatçı Birliği'ne mensup 5000'den fazla firmanın, birlik kullanıcılarının, gümrük kapılarındaki kullanıcıların ve DTM uzmanlarının kullanıcısı olduğu bir sistem olarak hayata geçirilmiştir. Bu proje ile, Dahilde İşleme İzin belgelerinin DTM'ye ulaştırılması ve onaylarının alınması sürecinde yaşanan bürokratik gecikmeler en aza indirilmiştir.

Proje ile, belge başvurusunda bulunacak olan şirket başvurusunu internet aracılığı ile elektronik ortamdan yapabilmekte ve başvuru sonucunu yine elektronik ortamda takip edebilmektedir. Ayrıca şirketin başvurusundan sonra DTM içerisindeki iş akışı da yine elektronik ortamda gerçekleştirilmektedir. Elektronik ortamdaki bu iş akışına katılan şirket ve DTM kullanıcıları, kimliklerini güçlü bir şekilde doğrulayarak sisteme girmek için kendileri için özel olarak kişiselleştirilen akıllı kartlarını kullanmaktadırlar. Ayrıca elektronik işlemlerde bütünlük ve inkâr edememe hizmetlerini vermek amacıyla elektronik imza işlevleri uygulamaya dahil edilmiştir. Bu amaçla TÜBİTAK-BİLTEN tarafından geliştirilen Zeugma AAA yazılımı kullanılmıştır. DTM'nin geliştirdiği bu e-imza uygulaması devreye girmek üzereyken, 6 Eylül 2004 de yayınlanan Başbakanlık Genelgesi ile Elektronik İmza Yasası'nın getirdiği yasal sürece uyum çerçevesinde elektronik imza hizmetlerini kurulacak Kamu Sertifikasyon Yapısı'ndan (KSY) hizmet alma doğrultusunda devam etmektedir. (Beder, 2005)

2004 yılında 4,968 adet dahilde işleme izin belgesi düzenlenmiş olup, belgelerin toplam ihracat taahhüdü 33.7 milyar dolardır. Bir adet dahilde işleme belgesinin düzenlenmesi, revizesi ve kapatma işlemleri için ortalama 450 adet kağıt kullanıldığı dikkate alınırsa, 2004 yılında sadece dahilde işleme izin belgeleri için 2.3 milyon adet civarında kağıt kullanılmıştır, bu da yaklaşık olarak 1.127 ton veya 112 kamyon kağıt demektir.

Proje ile, ihracat genel müdürlüğünce verilen dahilde işleme izin belgelerinin, düzenlenme aşamasından taahhüt hesaplarının kapatılmasına kadar geçen sürecin, hazırlanan web tabanlı program ile ınternet üzerinden yapılması sağlanacaktır. Söz konusu proje ile, ihracatçılar zaman ve mekan kısıtlaması olmaksızın ihracata yönelik yukarıda belirtilen izin belgelerine ilişkin tüm işlemleri bilgisayar üzerinden

anında yapabilecek ve talepleri aynı ortamda Dış Ticaret Müsteşarlığınca değerlendirilerek çok hızlı bir şekilde sonuçlandırılacaktır.

Firmaların güvenli bir şekilde sisteme dahil olarak proje kapsamında işlem yapabilmeleri için elektronik imza sertifikası kullanmaları gerekmektedir. söz konusu e-imza sertifikaları TK tarafından yetkilendirilen özel elektronik imza sağlayıcılarından temin edilebilecektir.

Proje kapsamında firmalarımızın gerçekleştirebileceği işlemlerden bazıları şunlardır;

- Belge müracaatı yapabilme
    - İthalat/ihracat listelerini online/offline hazırlayabilme
    - Hammadde sarfiyat tablolarını online/offline hazırlayabilme
- Mevcut belge bilgileri veya firma bilgileri ile ilgili her türlü revize talebi yapabilme
    - İthalat veya İhracat listelerinde değişiklik talebi,
    - Ek süre talebi,
    - Yan sanayici revizesi,
    - H kodlu belgeler için ülke revizesi
    - Y Kodlu belgeler için faaliyet revizesi
- Kapatma müracaatı yapabilme
    - Yurt içi alım ve satım faturalarını bildirme,
    - Özel fatura ile yapılan satışlarını bildirme,
- Belge kapsamında gerçekleşen ithalat ile ihracatlarını takip edebilme,
- Belge kapsamında gerçekleşen ithalat ile ihracatlarını takip edebilme,
- İptal talebinde bulunabilme**,**
- Evraklarını takip edebilme.

#### 4.4.2.3 TSK Akıllı Kart Projesi

Türkiye'de sayısal imzanın kanunlaştığı göz önüne alındığında elektronik ortamda TSK personelinin yaptığı işlemlerde sayısal imzanın gerekli olacağı

değerlendirilmektedir. Bu nedenle muvazzaf personel için tedarik edilecek kartlarda sayısal imza yeteneği bulunacak ve standartlığın sağlanması için TÜBİTAK tarafından gerçekleştirilmekte olan Milli Açık Anahtar Altyapısını destekleyecek şekilde geliştirilecektir. TSK, yeni teknolojinin sunduğu bu olanağı Cenevre Sözleşmesi'ne uyumlu olarak hayata geçirmiştir. Çoklu işlevlerin tek kartta toplandığı, çağdaş görünümlü ve taklit edilemeyen bu kartların, gerek üzerinde barındırdığı mikro işlemcileri ve gerekse görsel özellikleri bakımından en üst düzeyde güvenliğe sahiptir. TSK personeli tek bir akıllı kartı, 'kimlik kartı, giriş kartı, elektronik cüzdan, elektronik imza ve sağlık kartı' olarak kullanabilecektir.

Genelkurmay Başkanlığı 'Kartların sahip olduğu işlevler ve dağıtılacak kart sayısı bakımından TSK dünya orduları arasında bir ilki başarmış olup dünyadaki diğer akıllı kart projeleri arasında da sayılı büyük projelerdendir. TSK Akıllı Kart Sistemi, tanımlı ve ölçülebilen süreçlere sahip, e-devlet'e geçişin temelini oluşturan birlikte çalışabilirlik esaslarına uygun bir yapıda geliştirilmiştir. Sistemin, yakın bir gelecekte ülke çapında yaygın bir kullanım alanı bulacak e-imza, kimlik ve sağlık kartı gibi uygulamalar için de destek sağlayacağı değerlendirilmektedir. e-cüzdan işlevi sayesinde TSK bünyesindeki nakit para dolaşımının en aza ineceği, verilen hizmetlerin kalitesinin artarak hızlanacağı ve personelin moral seviyesinin yükselmesine katkı sağlayacağı öngörülmektedir.

Akıllı kartlarla birlikte; Elektronik imza kanunu kapsamında, TSK' da sayısal imza taşıma altyapısı oluşturulacaktır. Milli Açık Anahtar Altyapısı (MA3)'na göre üretilen sertifikalar Akıllı Kartta tutulacaktır. Personelin ıslak imzası yerine geçecek sayısal imzası elektronik ortamda kullanılacaktır. TSK çapında yürütülmekte olan diğer projelerde (MEDAS, HvBS, TBS, OMEGA, SBS, vb.) kullanılabilme ortamı sağlanacaktır. Ayrıca mevcut uygulama ile değerlendirildiğinde; Akıllı Kart Projesi kapsamına alınması düşünülen uygulamaların halihazırdaki ve planlanan maliyetleri incelenerek TSK Akıllı Kart Projesinin maliyet-etkinlik analizi yapılmış ve münferit kart uygulamalarının sebep olacağı aşırı maliyetin önlenmesi gerektiği görülmüştür.

Kartın işlemcisinde beyanname ile personelden alınan tüm bilgiler, kartın ön ve arka yüzeyinde bulunan tüm bilgiler, parmak izi bilgisi, personele acil durumlarda müdahale edilmesi amacıyla temel sağlık bilgileri (kritik hastalıklar, alerji bilgileri ortez/ protez vb.) ile sayısal imza ve e-Cüzdan bilgileri yer alacaktır.

#### 4.4.2.4 E-İmzanın Sağlık Alanında Kullanılmasının Getireceği Katkılar

Sağlık hizmetleri, hizmetin verilmesinden verilen hizmetin ödenmesine kadar pek çok aşamayı içeren, sürekliliği olan bir süreçtir. Böyle bir hizmetin entegre ve sürekliliği göz önüne alınarak yerine getirilebilmesi, enformasyonun etkin yönetilmesini gerektirir. İhtiyaç duyulan tüm enformasyon, doğru zamanda, doğru yerde ve doğru kişinin kullanımı için kolaylıkla ulaşılabilir olmalıdır(E-SAGLIK). Böyle bir hizmetin e-imzanın kullanılarak güvenli bir ortamda yapılması aşağıda sıralanan bazı kazanımların elde edilmesini sağlayacaktır.

*-Sağlık sektöründe kullanılan reçete, rapor, fatura, vb belgeleri elektronik ortama taşıyarak kağıt masraflarını azaltacaktır.*

*-Kağıtların bir yerden bir yere taşınmasına gerek bırakmayarak işlem hızını artıracaktır.*

*Yukarıda sözü edilen benzeri nedenlerle toplam maliyeti düşürecektir.*

*-Eczacının kendisine getirilen bir reçeteyi gerçekten bir hekimin yazıp yazmadığını anlaması çok zordur. Elektronik imzanın kullanılması ile reçeteleri sadece yetkilendirilmiş kişilerin yazması söz konusu olacaktır(ETPEOF).*

*-Hekim reçetelerindeki el yazılarının okunaksız olabilmesi nedeni ile ilaç hataları olabilmekte, hastalar bundan zarar görebilmektedir. Reçetelerin ve benzeri belgelerin bilgisayarla yazılması durumunda yanlış anlaşılma sorunu ortadan kalkacaktır(RIEPC).*

*-Ülkemizde zaman zaman yeşil ve kırmızı reçetelerin çalınması sorunu yaşanmaktadır. Reçetelerin elektronik ortama aktarılması ile bu tip sorunların önüne geçilecektir.*

*-Elektronik reçetelemenin kullanımının artması, reçeteleme hatalarını saptayan yazılımların da kullanılmasının artmasına sebep olacak, bu şekilde hastanın güvenliği daha da artacaktır.*

*-Veri bütünlüğünün ve güvenliğinin sağlanması mümkün olacaktır. Hastaya ait bir tıbbi bilginin gönderildikten sonra kasıtlı veya kasıtsız olarak bozulup bozulmadığını tespit etme kolaylaşacaktır.*

*-Reçete, rapor, hekim talimatı gibi hukuki sorumluluk isteyen belgelerin elektronik ortama taşınabilmesi için bu belgenin kimin tarafından oluşturulduğu ve oluşturulduktan sonra değiştirilip değiştirilmediğinin saptanabilmesi gerekir. Bunun gibi satınalma gibi çeşitli bürokratik işlemlerde tarafların hukuki sorumlulukları vardır. Elektronik imza yardımı ile sağlık sektöründeki pek çok belge ve bunlarla ilgili süreçler elektronik ortama taşınabilecektir..*(Beder, 2005)

*-Elektronik imzanın kullanılması, hastane bilgi sistemi ve sağlıkla ilgili diğer yazılımların kullanımını teşvik edecek, sektörel bir maliyet azalması ve kalite artışına dolaylı etkide bulunacaktır (Wang,2001).*

#### 4.4.2.5. Özel Sektör Kuruluşlarında E-İmza Kullanımı

Özel sektör kuruluşlarından gerçekleştirilmiş olan akıllı kart tabanlı AAA projelerinin kuruluş içindeki uygulama alanları ve proje detayları aşağıda sunulmuştur.

##### 4.4.2.5.1 TurkcellMobilİmza

Turkcell, cep telefonları için geliştirilmiş, yasal olarak ıslak imzaya eşdeğer elektronik imza uygulamasını, SIM kart üzerindeki ek güvenlik özellikleriyle beraber kullanıcılarının hizmetine sunuyor. Turkcell, yasal olarak ıslak imzaya eşdeğer yeni servisi Turkcell Mobil imzayı, ilk olarak Internet bankacılığında Akbank, Garanti, Türk Ekonomi Bankası, Türkiye İş Bankası ve Yapı Kredi işbirliğiyle müşterilerine sunuyor.

Turkcell mobil imza ile; kimlikle giderek şahsen yapmak gereken bankacılık, başvuru, kamu uygulamaları gibi işlemleri uzaktan yapabilecek, bu sayede zaman ve emek tasarrufu sağlanacak, internet bankacılığı ve diğer sanal işlemler bilgisayar korsanlarından çekinmeden güvenle yapabilecek, şifre/parola bilgilerini çaldırma riski ortadan kalkacak, farklı uygulama ve banka hesaplarına tek şifre ile erişerek; şifre karıştırma, unutma gibi sorunlar sona erecek, şirketlerin izin, işe alım, satın alma gibi süreçlerini güvenle elektronik ortamdan yapabilecek; tedarikçiler ve iş ortakları sisteme dâhil ederek verimlilik sağlanabilecektir.

Turkcell Mobil İmza, evlilik, tapu gibi kanunen belirli bir şekilde törenle gerçekleştirilmesi şart olan ve üçüncü kişilerin kefaletini gerektiren işlemler dışında, ıslak imza gerektiren tüm özel, kamu ve banka işlemlerinin mobil olarak

yapılabilmesine olanak sağlıyor. E-imza teknolojisini mobil ortama taşıyan Turkcell Mobil imza ile ayrı bir akıllı kart ve kart okuyucu kullanmaya gerek olmadan, imza gerektiren işlemlerin de Internet bankacılığına taşınabiliyor, resmi başvurular uzaktan yapılabiliyor. Turkcell kullanıcıları, ekstra cihaz ve elektronik sertifika yatırımı olmaksızın mevcut telefonlarıyla mobil imzanın sağladığı kolaylık ve ekstra güvenlikten yararlanabilecekler. Turkcell Mobil imza ile kişilerin imza atarken kullanacakları "Nitelikli Elektronik Sertifika"lar E-Güven tarafından sağlanacaktır.

#### 4.4.2.5.2. Denizbank

Kurumsal müşterilere Internet Bankacılığı hizmetini daha güvenli sunmak amacıyla Denizbank bünyesinde bir PKI sistemi tasarlanıp, geliştirilmiştir. Web üzerinden kimlik doğrulama işleminin akıllı kartlarla yapıldığı bu sistemde Gemplus' ın GemSafe 8K kartları ile Todos akıllı kart okuyucuları kullanılmıştır. Microsoft Sertifika Otoritesi yazılımı kurum içerisindeki sertifikaların yaratılması, dağıtımı ve iptal edilmesi işlemlerini gerçekleştirmektedir. (TK 2004b)

#### 4.4.2.5.3. İSKİ

E-imza sahipleri, İSKİ müdürlüklerine gitmeye gerek duymadan, mukavelelerini ıslak imzaya eşdeğer nitelikteki elektronik imza ile onaylayabilecekler. Bu uygulama ilk safhada borçsuz olup ta yenileme işlemi yapmak isteyen müşteriler için başlatılacak. Vatandaşların bu yenilikten faydalanmaları için herhangi bir ulusal ESHS'den alınmış geçerli bir nitelikli elektronik sertifika bulundurmaları yeterli olacak. E-imza, 4 milyon İSKİ abonesine hem kolaylık hem de zamandan ve ulaşım ücretinden tasarruf imkanı sağlayacaktır. (www.E-imza.gen.tr)

#### 4.4.2.5.4. İş Bankası

TÜRKİYE İş Bankası, elektronik imzayı bankacılık işlemlerine uygulayarak nakit kredi kullanma dönemini başlattı. E-imza uygulaması ile banka müşterileri, banka şubesine hiç gitmeden, günün her saatinde kredi başvurusunda bulunup, bir kaç dakika içinde kredi alabilecekler. İstenilen kredi birkaç dakika içinde müşterinin hesabına geçirilecek. Ayrıca isteyenler kredilerini bankamatik kartları olmadan da cep telefonu aracılığıyla bankamatiklerden nakit olarak da çekebilecektir.

E-imza ile kredinin limiti 5 bin YTL, normal banka kredilerinde 70-190 YTL arasında uygulanan kredi masrafı ise e-imzalı nakit kredide 20 YTL olarak

belirlendi. "İnternetten kredi başvurusu yapılabilen, insansız, dijital ve mobil iletişimin iç içe geçtiği ilk bankacılık uygulaması olacak. Bu uygulama ile bankacılık işlemlerine yeni bir boyut getiriyor. Bankacılık işlemlerinde talimat vermekten, kredi işlemlerine kadar pek çok işlemin gerçek anlamda banka şubelerine gitmeden yapılabileceği bir dönem başlıyor. E-imzayı bankacılık sistemine adapte ederek kısa sürede kapsamı genişleyecek yeni bir dönemi başlatmış oluyor.

# SONUÇ

Geçmişte sanayi toplumunu oluşturabilmek amacıyla hareket eden gelişmiş ülkeler, günümüzde sanayi toplumundan bilgi ekonomisine ve bilgi toplumuna ulaşmayı yeni hedef olarak belirlemiştir. Bu hedeflere ise, bilgiyi üretecek beyinler yetiştirmekten ve üretilen bilginin toplumsal ve ekonomik gelişim için kullanılmasını sağlayacak mekanizmaları oluşturmaktan geçmektedir. Gelişmiş ülkelerde bu mekanizmalar, sermaye birikimi, uzun bir süreci öngören kapsamlı ve gerçekçi bilim ve teknoloji politikaları, araştırma ve geliştirme faaliyetlerine olan yatırımlar gibi avantajlarla daha kolaylıkla uygulamaya konulabilmektedir.

Değişen teknolojik süreçle birlikte, karar alma süreçleri hızlanmış ve süreler kısalmıştır. Gerektiği kadar hızlı bir şekilde doğru karar alamayan, vatandaşından devletine, şirketinden kamu kuruluşuna kadar her kesim, ciddi bir tehlike ile karşı karşıya kalacaktır. Bu anlamda, doğru karar alma süreçlerinin hızlandırılması yeni çağda hayatta kalabilmenin en önemli unsuru olacaktır.

İnternetin yaygın kullanımı ile birbirinden bağımsız ağlar, kurumsal uygulamalar her geçen gün birbirine entegre olmakta, bilgi ve iletişim teknolojileri iş yapma alışkanlıklarımızı derinden etkilemektedir. Kişilerin bir kaş saniye içinde, dünyanın herhangi bir yerinden her türlü bilgiye her zaman ulaşabildiği günümüz dünyasında; devletler, kurumlar, işletmeler ve insanlar, iş süreçlerini, ilişki süreçlerini, iletişim süreçlerini ve daha önce var olmayan bilgi süreçlerini yeniden tanımlıyorlar. Meydana gelen bu gelişmeler ışığında, yerel ve global ekonomilerde, yönetimlerde, iş süreçlerinde, sosyal hayatta iletişim ağları üzerinden baş döndürücü bir hızla akmakta olan her türlü bilgi sürekli bir tehdit altındadır. Çünkü bilgiye hükmeden kurumlar kişiler, meydana gelen ve gelecek olan gelişmeleri yakından takip etmekte ve bilgiyi bir katma değer olarak kullanabilmektedir.

Bu açıdan bakıldığında iletişim ağları üzerinde hareket eden bilgilerin korunması, bilginin varlığı kadar önem kazanmaktadır. Geçmişte kağıt üzerindeki bilgilerin korunması, içerinin gizlenmesi ne kadar önemli ise günümüzde de elektronik ortamdaki bilgilerin güvenliği aynı öneme sahiptir. Yüzyıllar boyu hükümdarların, devlet adamlarının, komutanların; bilgiyi korumak adına aldıkları tedbirler, kriptoloji bilimi ile geliştirdikleri teknikler bu gün bilişim teknolojilerinde

de uygulanmaktadır. Tüm bunların sonucu olarak karşımıza çıkan e-imza, ekonomik ve sosyal hayatın vazgeçilmez bir unsuru olacaktır.

E-imza bankacılık, finans, borsa, yurtiçi ve yurtdışı e-iş ve e-ticaret işlemlerinde, sözleşmelerde, ihalelerde, alışverişte, resmi veya özel kurumların iç veya dış yazışmalarında, sosyal güvenlik ve sağlık alanında, vergi ve prim ödemelerinde, ticari, hukuki, bireysel ve kurumsal resmi başvuru işlemlerinde yoğun olarak kullanılacaktır. E-imza kullanılarak, internet bağlantısı olan bir bilgisayarla ya da cep telefonu ile bankaya gitmeden kredi başvurusu yapılabileceğini, alınana kredinin internet bankacılığı ile ödemelerde kullanıldığını düşündüğümüzde, sağlanan zaman tasarrufu insanların günlük hayatını derinden etkileyecektir.

E-imzadan bağımsız düşünülemeyecek bir kavram olan E-ticaret toplumlar tarafından hızla kabul görmekte ve gündelik ihtiyaçların karşılanmasından yatırım alanının tespitine kadar her alanda kullanılmaktadır. Böylece, azalan maliyetler ve kısalan iş süreçleri, toplumun genelinde daha iyi imkanların sunulmasına kaynak aktaracaktır. Kayıt dışı ekonomide, azalan maliyetler sonucunda etkisini giderek kaybedecektir.

Elektronik ticaret, gelişmekte olan ülkelerde makro ve mikro ekonomik dengeler açısından kaynakların daha verimli kullanılmasını sağlayacak fırsatlar sunan bir gelişmedir. Gelişmekte olan ülkelerin bu fırsatları değerlendirmesi, elektronik ticaretin önündeki yasal ve kurumsal engellerin kaldırılmasına ve teşvik edilmesine bağlıdır. ABD başta olmak üzere gelişmiş ülkeler, elektronik ticarette gelişmekte olan ülkelerden bir kaç adım öndedir ve bu üstünlüklerini sürdürme eğilimindedirler. Dolayısıyla gelişmekte olan ülkeleri her konuda olduğu gibi zorlu bir yarış beklemektedir.

Ülkemizin elektronik imza mevzuatı açısından pek çok ülkeden ileri düzenlemelere sahip olduğu değerlendirilmektedir. Ortaya konulan altyapı modeli, uygulamada çıkabilecek sorunları en aza indirmiş, mükerrer yatırımları önlemiş, sertifikasyon açısından kurum ve kuruluşların aynı çatı altında toplanması sağlanmıştır. Ülkelerin elektronik imza konusunda işbirliği yaparak ortak düzenlemeler ya da uluslararası sözleşmeler yapmaları sistemin sağlıklı işleyişi açısından zorunlu görünmektedir. Zira, elektronik imza uygulamaları ülke sınırlarını aşan bir nitelik arz etmektedir.

Elektronik imzanın geniş kitleler tarafından kullanılmasında devlet önemli rol oynamalıdır. Elektronik İmza Kanununun uygulamalarla günlük hayatımıza girmesi ile birlikte devlet hizmetlerinde ve kurumların iş alışkanlıklarında büyük değişimlerin yaşanması kaçınılmaz hale gelecektir. Bu nedenle gelişmelerin zamanında farkına varılarak kamu kurum ve kuruluşları, iş süreçlerini gözden geçirmeli, e-devlet kurumu olmanın gereklerini yerine getirmelidirler.

Elektronik imzanın ülke genelinde kabul görmesi için; kamu ve özel sektörün bilgilendirilmesi gerekmektedir. Şu ana kadar kamu uygulamaları kısıtlı bir kesime hitap etmekte ve ülke genelinde getirileri sınırlı olmaktadır. Özellikle milli eğitim, sağlık ve nüfus uygulamaları hedef seçilerek e-imza uygulamaları geniş kitlelere yaygınlaştırılmalıdır..

Sertifika dağıtımı, iptal ve yenileme işlemlerinin zorluğu, uygulama ve standart problemleri, kullanıcı ve işletme maliyetinin yüksek olması, e-imza sahibi olacak vatandaşların sistemin işleyişi hakkında bilgi sahibi olması gerekliliği gibi konuların sertifika yönetimini ve elektronik imzanın yaygınlaşmasını zorlaştıran unsurlar arasındadır.

Sonuç olarak, elektronik imzanın kullanılmaya başlaması ve yaygınlaşması, kuşkusuz kâğıt ve kalem ikilisinin ortadan kalkması sonucunu doğurmayacaktır. Elektronik imza kullanımı, elektronik ortamda güvenli iletişim ve işlemler için günümüzde vazgeçilmez yöntem olarak görülmekle birlikte isteyen herkes el yazısı ile de işlemlerini yapabileceklerdir. Bir başka değişle fotoğrafa karşın nasıl günümüzde nasıl resim yapılmaya devam ediliyorsa, elektronik haberleşme ve sayısal imzanın yanı sıra kâğıt dokümanlar, el yazıları ve el yazısı ile atılan imza da var olmaya devam edecektir.”

Bilişim yatırımlarına ağırlık verilmesi, bilişim alanında yeterli donanıma sahip insan kaynaklarının oluşturulması gerekiyor. Özellikle kamu kurum ve kuruluşlarında bilgisayar okuryazarlığının teşvik edilmesi gerekmektedir. Bilgisayar okur yazarlığının arttırılması gerekir. Vatandaş ile iletişimin ve etkileşimin güçlendirilmesi gerekir.”

Elektronik imza kullanımının yaygınlaştırılması amacıyla internet üzerinden yapılacak satışlar özendirilmeli, elektronik ortamdan yapılacak sözleşmeler yaşamımıza pek çok kolaylıklar getireceğinden internet üzerinden yapılacak

işlemlere muafiyetler tanınmalıdır. Örneğin verginin elektronik ortamdan yatırılması halinde indirimli olması, elektronik ortamdan yapılacak başvurulara öncelik tanınması gibi. Devlet bu durumda daha az personel istihdam edeceği gibi personelinin performansını takip edebilecek, bina, ulaşım, yakıt gibi giderleri de azalacaktır. Diğer taraftan devlet, elektronik devlete geçmeyi kolaylaştırmak için işlemlerini elektronik ortamdan yapan personelini teşvik etmeli, gerekirse ödüllendirmelidir.

Türkiye'de elektronik imza konusunda yapılan hukuksal düzenlemeler yeterli olmakla birlikte uygulamaya konusunda hazırlanan planlara uyulmaması büyük eksikliktir. Elektronik imzanın kullanılması, kamudaki dönüşümün, yeniden yapılanmanın, verimliliği sağlamanın ve e-devlet olmanın bir gereği olarak görülüp iyi değerlendirilmelidir.

E-imzanın süratle uygulamaya geçebilmesi için önünde bir takım engeller bulunmaktadır. Bu engelleri, Teknolojik, Güvenlik, Mali, Hukuksal ve Sosyal kategorilerde sınıflandırabiliriz. Teknoloji açısından ele aldığımızda, E-imza konusunda firmaların bir takım standartları olmasına karşın, Uluslararası ölçekte tanınmış ve geliştirilmiş yaygın bir standart yok. Bu da zamanla, firmaların ortak bir konsensüs üzerinde anlaşmaları gereğini ortaya koymakta. Ulusal bilgi güvenliği standardımızın oluşması son derece önemlidir. Maalesef bu konuda, her bir kuruluş kendi içerisinde bir takım standartlar belirlemeye çalışıyor. DPT tarafından yapılan e-devlet çalışmasında bu konu geçmesine rağmen, ulusal anlamda bir güvenlik standardı henüz çıkmış değildir. Dünyadaki uygulamalara baktığımızda, e-imza uygulamalarının yasalaştıktan sonra ilerleyebildiğini görmekteyiz. Bu anlamda, e-imzanın ülkemizde de yasalaşması gerekti. 5070 nolu yasa ile e-imzanın hukuksal dayanağı tamamlanmış oldu.

Alınan kararlarda, süratle uygulamaya geçirilebilmelidir. Bu da süreçlerin ve işletmelerin esnekliği kazanması, hantallıktan kurtularak genç ve çevik bir yapıya kavuşmasını gerektirmektedir. Bu esneklik ve çeviklik sadece özel şirketler için değil, hizmet veren bütün kuruluşlar ve devlet içinde geçerlidir.

Sonuç olarak, ülkemizde gerek kamusal alanda gerek özel sektörde işletmelerin, kurumların; müşterilerine ve vatandaşa günün belirli saatlerinde değil 24 saat hizmet verebileceği, personel maliyetlerinin en aza indirilebileceği, mekan ve yer kavramlarının ortadan kalkacağı bilişim ağları üzerinde faaliyet gösteren

elektronik uygulamaların hukuksal olarak geçerli olabilmesi için temel şart olan elektronik imza öncü kuruluşların adımları ile artık adını duyurmuştur. Gelişen teknolojilere karşı toplumların tepkileri, ilgileri, küçülen dünyada tahmin edilenden daha çabuk olmaktadır. 10 yıl gibi kısa bir sürede ülkemizde GSM operatörlerinin 20 milyondan fazla aboneye sahip olduğu düşünülürse, birkaç yıl içinde elektronik imza kullanımının milyonlara ulaşılacağını söylemek yanlış olmaz. Bunun sonucu hem elektronik imza pazarının ciddi bir büyüme kaydedecek, hem de elektronik ortamda yapılan ticari faaliyetlerin ekonomiye olan katkısı ülke kalkınmasında önemli bir rol oynayacaktır.

# KAYNAKLAR


25/8/1997 tarih ve 97/3 sayılı BTYK Kararı. (BTYK,1997)

23 Ocak 2004 tarih ve 25355 sayılı Resmi Gazete

AKDAĞ, Mustafa ve diğerleri, **Fen ve Teknoloji Sözlüğü**, T.Ö.V.Yayınları, Yayın No:14, İzmir,1996, s.110.

AKGEYİK, Tekin, **Stratejik Üretim Yönetimi**, Sistem Yayıncılık, Yayın No:181, 1.Baskı,İstanbul, Ekim 1998, s.27.

AKIN, Bahadır, **"İşletme Süreçlerinin Yeniden Tasarlanması ve...."** http://members.tripod.com/bahadirakin/bildiri.htm,13.05.2001, s.8.

AKOLAŞ, Arzu, **BİLİŞİM SİSTEMLERİ VE BİLİŞİM TEKNOLOJİSİNİN KÜRESELLEŞME OLGUSU VE GİRİŞİMCİLİK ÜZERİNE YANSIMALARI**, http://www.sosyalbil.selcuk.edu.tr/sos_mak/makaleler%5CD.Arzu%20AKOLA%C5%9E%5C29-43+.pdf

AKPINAR, Haldun, **Enformasyon Teknolojisi ve İşletmecilik Öğretimine Etkileri**, http://www.İstanbul.edu.tr/enfor/et.html,13.05.2001,s.6.

ALKAN, Mustafa ve Ayşe İNALÖZ, **Telekomünikasyon Regülasyonları ve Elektronik İmza'nın Elektronik Ticaret Üzerindeki Etkileri** , 2003

AP, (2000a), Bilgi Toplumu Hizmetlerinin Bazı Hukuki Yönleri ve Özellikle İç Pazarda Elektronik Ticaret Konusunda 8 Haziran 2000 tarihli 2000/31/AT sayılı Avrupa Parlamentosu ve Konsey Direktifi **("Elektronik Ticaret Konusunda Direktif")** Topluluk Resmi Gazetesi No: L 178, 17.07.2000 ss.0001-0016

AP, (2000b), Elektronik İmzalar İçin Topluluk Çerçevesi konusunda 13 Aralık 1999 tarihli 1999/93/AT sayılı Avrupa Parlamentosu ve Konsey Direktifi ("**Elektronik İmzalar İçin Topluluk Çerçevesi**") Topluluk Resmi Gazetesi No: L 013, 19.1.2000, s.0012-0020

ARIKAN, Saadet., **Dünyada ve Türkiye'de Elektronik Ticaret Çalışmalarına Hukuki Bir Yaklaşım**, Ankara 1999, s.151.

ATO Danışmanlık Birimi, **ATO YAYIN NO:08**, basım : GRAFİKER Ofset , ANKARA, 2002

AYDEMİR, İbrahim, **Elektronik Ticaret Alandaki Rekabet Sorunları**,Ankara 2004,s. 27

BAŞBAKANLIK, (2003), 27.02.2003 Gün, 2003/12 Sayılı, **e-Dönüşüm Türkiye Projesi Konulu Başbakanlık Genelgesi,** Ankara: Başbakanlık.

BAŞBAKANLIK, (2005) Genelge, 2005/20 - **e-DÖNÜŞÜM TÜRKİYE PROJESİ BİRLİKTE ÇALIŞABİLİRLİK ESASLARI REHBERİ**, 2005

BEDER, Fevki, **Elektronik Belge Yönetim Sistemi ve TCMB Örneği**, Uzmanlık Yeterlilik Tezi, Ankara, Nisan 2005

BENNET, R. , Management, The Manufacturing and Engineering Handbook Series, London 1994, p.263.

BERBER, Keser L., (2002), **"Elektronik İmzanın Düzenlenmesi Hakkında Kanun Tasarısı Hükümlerinin Değerlendirilmesi",** Turk.internet, 25.12.2002,

BERBER Keser, L., (2000), " **'İmzalıyorum O Halde Varım', Dijital İmza, Dijital İmza Hakkındaki Yasal Düzenlemeler, Dijital İmzalı Elektronik Belgelerin Hukuki Değeri**", Türkiye Barolar Birliği Dergisi 2000/2, s.503-556

BEYDOĞAN , T. Ayhan , **Elektronik Sertifika Pazarı ve Rekabet** , Telekomünikasyon Kurumu, Kurul Üyesi

BİLİŞİM, (2005) **3. ÇALIŞMA GRUBU - TBD Kamu-BİB Kamu Bilişim Platformu VII, e-imza, KAMUDA BiLGİ ve BELGE EĞİŞİMİ,** 26-29 Mayıs 2005 , Antalya

**BİLİŞİM Şurası e-Sağlık Çalışma Grubu Raporu**

Büke, M., (2005), **"ESHS Şirketleri Yetki Belgelerini Alıyor",** Turk.internet, 27.06.2005, http://www.turk.internet.com/haber/yaziyaz.php3?yaziid=13073

ÇAK, M., "**Dünyada ve Türkiye'de Elektronik Ticaret ve Vergilendirilmesi**", ITO Yayınları İstanbul, Şubat 2002

CWA , 14171 CEN. Workshop Agreements**:"Procedures for Electronic Signature Verification".**

ÇAMURDAN, Ç., "Elektronik İmza Kanunu Üzerine Bir Değerlendirme", Bilişim Kültürü Dergisi, Haziran 2003, S.86, s.52-54

ÇENGEL, S., **Elektronik Ticaret,** Endüstri Mühendisliği Bölümü, Mühendislik Fakültesi, Kocaeli Üniversitesi, TÜRKİYE. 2002

DTM, WWW.dtm.gov.tr

DALGIÇ, Tevfik, **Bilişim ve Teknoloji**, Ankara İktisadi ve Ticari İlimler Akademisi Yayın No: 203 , Ankara, 1982, s.33-34.

DPT, (2004), **e-Dönüşüm Türkiye Projesi Kısa Dönem Eylem Planı 2003-2004**, http://www.bilgitoplumu.gov.tr

DPT, (2005), **e-Dönüşüm Türkiye Projesi 2003-2004 KDEP Uygulama Sonuçları**

**ve 2005 Eylem Planı**, http://www.bilgitoplumu.gov.tr

DPT, (2006a), **e-Dönüşüm Türkiye Projesi 2005 Eylem Planı Sonuç Raporu**,

http://www.bilgitoplumu.gov.tr

DPT, (2006b), **Bilgi Toplumu Stratejisi Eylem Planı**, http://www.bilgitoplumu.gov.tr

DPT, (2006c), **Bilgi Toplumu Stratejisi**, http://www.bilgitoplumu.gov.tr

DÜREN**,** A. Zeynep, **2000'li Yıllarda Yönetim**, Alfa Yayınevi, Yönetim Dizisi, No:013, 1.Baskı,İstanbul, 2000, s.60.

EC, **The Legal and Market Aspects of Electronic Signature,** Study for the European Commission - DG Information Society

**Electronic Transmission of Prescription Electronic Order Forms** http://www.deadiversion.gov/ecomme/e_ordrs

ERDEM, O. Ayhan ve Özlem EFİLOĞLU, **Bilgi Çağında Elektronik Ticaret,** G.Ü. Teknik Eğitim Fakültesi, Elektronik ve Bilgisayar Eğitimi Bölümü, 06500 Teknikokullar, ANKARA

ERKAN, Ugur, www.hurriyet.com.tr , 2005, ANKARA

ERSOY, Zeynep, **Elektronik Ticaret ve Ticaret Noktaları**, İGEME, Ankara,1999

ETKK, (1998a), **Hukuk Çalışma Grubu Raporu**, http://www.eticaret.gov.tr/raporlar/hukuk.htm

ETKK, (1998b), **Teknik Çalışma Grubu Raporu**, http://www.eticaret.gov.tr/raporlar/teknik.htm

**EU Summit,** Mart 2000, Lizbon, Portekiz

EVERETT, Lupton W. , **The Digital Signature: Your Identity by the Numbers**, 6 RICH. J.L. & TECH.10 (Fall1999) http://www.richmond.edu/jolt/v6i2/note2.html

GATES, Bill, (1999a) **Önümüzdeki Yol**, Çevirenler: Esra Davutoğlu ve Alper Erdal, Arkadaş Yayınları, 2.Baskı, Ankara, Şubat 1999,s.23.

GATES, Bill, (1999b) **Dijital Sinir Sistemiyle Düşünce Hızında Çalışmak**, Çeviren: Ali Cevat Akkoyunlu, Doğan Kitapçılık, 4.Baskı, İstanbul, Nisan 1999, s.53.

GÖKÇEN, Ferhat, İnternet ve Elektronik Ticaret (E-Ticaret) Üzerine, 2006

GÜVENEN, Orhan, **Küreselleşme Sürecinde Bilgi Teknolojileri ve Bilgi Sistemleri Stratejileri**, DPT,Ön Çalışma Raporu, İstanbul, 1998, s.2.

ÖZER, Günay Faruk, **Sermaye Piyasalarında Elektronik İmzanın Kullanım Alanları**

ÖZYILMAZ, Ayşe ve Saliha EVSENAL, **Elektronik İmza**, ACTIVE AGUSTOS-EYLUL 2000

HAŞILOĞLU, Selçuk Burak, **Enformasyon Toplumunda, Elektronik Ticaret ve Stratejileri**, Türkmen Kitabevi, İstanbul,1999, s.23.

İNCE, Murat, El**ektronik Ticaret : Gelişmekte Olan Ülkeler İçin İmkanlar ve Politikalar**, DPT, www.dpt.gov.tr , ANKARA. 1999

İİK, - **22. Çalışma Grubu, Türkiye'de Bilgi Ekonomisine ve Bilgi Toplumuna Geçiş İçin Strateji ve Politikalar,** İzmir İktisat Kongresi, MART 2004

KARTAL, **İnternet Ortamında Pazarlama,** Gazi Kitabevi, ANKARA, 2002,

KAZGAN, Gülten, **Küreselleşme ve Yeni Ekonomik Düzen**, Altın Kitaplar Yayın., 1.Baskı, İstanbul, 1997, s.9-10.

KOBİNET, **E-ticaret Kütüphanesi,** http://www.kobinet.org.tr/hizmetler/e-ticaret

KSM, **Teknik Bilgiler**, Kamu Sertifikasyon Merkezi, http://www.kamusm.gov.tr/net/bilgiler/teknik/tanimlar.jsp#eshs

KURAN, N.Hüseyin, **e-imza: Yeni Bir Çağın Başlangıcı,** e-imza Paneli/ANKARA, 15.07.2004

LAWRENCE, E., Newton, S., CORBİTT, B., BRAITHWAITE, R., Parker, C.," **Technology of Internet Business**", John Wiley & Sons Australia Ltd., 2002

NAPRA, **Recommendations for Implementing Electronic Prescription in Canada**, http://www.napra.ca/pdfs/practice/erxFINAL.pdf

ORTA, Mesut, **Türkiye'de Elektronik İmza Uygulaması**

OECD, **Policy Briefs No. 1-1997.** http://www.oecd.org./publications/polbrief/9701pol.htm

ÖĞÜT, Pelin, **Küreselleşen Dünyada Bilgi Güvenliğine Yönelik Politikalar: Sayısal İmza Teknolojisi ve Türkiye**, Yüksek Lisans Tezi, Ankara – 2006

ÖZBAY, A., Devrim, J., "**7'den 77'ye Yeni Başlayan Herkes İçin e-Ticaret Rehberi"**, Hayat Yayıncılık İstanbul, 2001

ÖZKAN, Y., **Elektronik Ticaret Yazılım Firmalarında Pazarlama Ve Elektronik Ticaret Uygulamaları,** Endüstri Mühendisliği Bölümü, Mühendislik Fakültesi, Kocaeli Üniversitesi, TÜRKİYE. 2003,

REED, Chris, **'What is a Signature?', The Journal of Information, Law and Technology** (JILT).2003/3, http://elj.warwick.ac.uk/jilt/00-3/reed.html/

RHINESMITH, Stephen H. , **Yöneticinin Küreselleşme Rehberi,** Çeviren:Gülden Şen, Sabah Kitapları, .Yayın No: 110, İstanbul , 2000, s.20-21.

SAĞIROĞLU, Şeref ve Mustafa ALKAN, **Her Yönüyle Elektronik İmza, e-İMZA,** Ankara-2005Grafiker Yayınları no:27

SELÇUK, Gonca Hülya, **E-devlet Uygulamaları İçin Elektronik İmza Formatları**, TÜBİTAK – UEKAE Kamu Sertifikasyon Merkezi

SEVİM, Tuğrul, **Elektronik İmzanın Hukuksal Boyutları**, II. TÜRKİYE BİLİŞİM Şurası Hukuk Çalışma Grubu, Mart 2004 İstanbul

SIRMA, İbrahim **"Elektronik Ticaret Stratejileri"** İstanbul Üniversitesi, Aksan Bülteni, (2002)

SOYER, Şule, **Küresel ve Ulusal Ticarette E-İmza**, 17 Ekim 2003

ŞAHİN ve DİKTAŞ, **Elektronik Ticaret**, Endüstri Mühendisliği Bölümü, Mühendislik Fakültesi, Kocaeli Üniversitesi, TÜRKİYE, 2002,

Telekomünikasyon Kurumu, (2004a), **Elektronik İmza Ulusal Koordinasyon Kurulu Hukuk Çalışma Grubu İlerleme ve Sonuç Raporu**, http://www.tk.gov.tr

Telekomikasyon Kurumu, (2004b), **E-İmza Ulusal Koordinasyon Kurulu Altyapı Çalışma Grubu İlerleme Raporu**, http://www.tk.gov.tr

Telekomikasyon Kurumu, (2004c), **E-İmza Ulusal Koordinasyon Kurulu Bilgi Güvenliği ve Standartlar Çalışma Grubu İlerleme Raporu**, http://www.tk.gov.tr

Telekomikasyon Kurumu, (2004d), **Elektronik İmza Ulusal Koordinasyon Kurulu Hukuk Çalışma İlerleme ve Sonuç Raporu**, TEMMUZ 2004 İSTANBUL, http://www.tk.gov.tr

TUENA, (1998a), **Açık İletişim Ağlarında Güvenlik Çalışma Belgesi**, http://www.tuena.tubitak.gov.tr/cbelgeleri.html

TUENA, (1998b), **Elektronik Ticaret Uygulamaları Çalışma Belgesi**, http://www.tuena.tubitak.gov.tr/cbelgeleri.html

TÜBİTAK, DPT, TBD vd., (2004), **Bilgi Toplumuna Doğru,** Türkiye İkinci Bilişim Şurası Sonuç Raporu: Ankara.

TÜBİTAK, UEKAE, (2007), **Açık Anahtar Altyapısı Eğitim Kitabı**, 2007

TÜFEKÇİ, T., (2003a), **"Elektronik İmza Neler Getirecek?",** TBD Bilgi İşlem Merkezi Yöneticileri Semineri, Antalya, 10-13 Nisan 2003, http://www.bilten.metu.edu.tr/Web_2002_v1/common/yayinlar/T_Tufekci_BIMY10_Copy.pdf

UNCTAD, (2005b), **Information Economy Report 2005**, Geneva: UNCTAD.

WTO (1998) **Electronic Commerce and the Role of the WTO**, http://www.wto.org

WANG, H.A. , **Digital signature technology for health care applications**. Southern Medical Journal 2001: 94;281-6

YÜKSELİYOR, Turhan, **AAA Sayısal Sertifika Karmaşası**, www.e-imza.gen.tr/templates/resimler/File/makaleler/AAA_Sayisal_Sertifika_Karmasasi_Turhan_Yukseliyor.doc

http://turk.internet.com/haber/yazigoster.php3?yaziid=13435

http://www.byte.com.tr/haberler/?Gorev=HaberAyrinti&Haber=218

http://www.turk.internet.com/haber/yazigoster.php3yaziid=6212

http://www.igeme.org.tr/tur/atn/etsop.pdf (IGEME)

www.turkpoint.com/e-yasam/sayisal imza.asp (01.12.2003)

http://unicc.org./unece/cefact/intro.htm (UNICC)

http://inet-tr.org.tr/inetconf8/bildiri/71.doc (INET)

http://www.elektronikticaretrehberi.com/e-ticaret_sonuc.php (ETR)

http://www.tisk.org.tr/isveren_sayfa.asp?yazi_id=709&id=42 (TISK)

http://www.eimza.gen.tr

## EK-A

## 5070 SAYILI ELEKTRONİK İMZA KANUNU' NA GÖRE BAZI TANIM VE KAVRAMLAR([1])

**Elektronik Veri**

5070 Sayılı Kanuna göre elektronik veri "Elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıtlar"dır. Elektronik veri tanımı çoğu yabancı mevzuatta ve Direktif'te yapılmamıştır. Sadece İrlanda'da "elektronik veri" tanımı altında Kanunumuzdakine benzer fakat daha geniş (biometrik, fotonik) bir tanım yapılmıştır.

**Elektronik İmza**

Kanuna göre elektronik imza "başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri"dir. Bu tanım Direktif'in çevirisi şeklindedir ve yabancı mevzuatta genel olarak aynı tanım karşımıza çıkmaktadır. Ancak Direktif'te; kanunumuzda "kimlik doğrulama" olarak belirtilen kısım "tanımlama-authentication" olarak belirtilmiştir. Tanımlama, imza sahibinin kimlik bilgilerini değil veriyi tanımlama olarak algılanmalıdır. Buradan çıkarılması gereken sonuç elektronik verinin elektronik imza sayılması için imza sahibinin kimlik bilgilerini taşıması veya bu bilgileri ortaya koyması gerekmemesidir. Ancak bu koşul ve şartları taşıyan ve bir elektronik veriyi tanımlayan ve ona doğrudan veya dolaylı olarak bağlı olan bir diğer elektronik veri elektronik imza sayılacaktır. Kanundaki "kimlik doğrulama" tanımını daha fazla karşılayan "identify" ibaresi Direktif'te gelişmiş elektronik imzanın (advanced electronic signature) gereksinimleri arasında sayılmıştır. Bu sebeplerden ötürü kanunun yorumu yapılırken elektronik imzalarda kimlik bilgilerini doğrulama zorunluluğu aranmamalıdır.

**İmza Sahibi**

Kanunda imza sahibi "Elektronik imza oluşturmak amacıyla bir imza oluşturma aracını kullanan gerçek kişi" olarak tanımlanmıştır. Direktif'te ve yabancı mevzuatta da bu tanımla örtüşen tanımlar mevcuttur. Burada dikkat edilmesi

---

[1] **Keser L. Elektronik İmza Ulusal Koordinasyon Kurulu Hukuk Çalışma Grubu İlerleme Ve Sonuç Raporu, Temmuz 2004, s:23-27**

gereken husus imza sahibinin ancak gerçek kişi olabileceğidir. Ancak yine Kanunun gerekçesinde, sertifikalarda bu hususun açıklıkla belirtilmesi durumunda, tüzel kişiler adına da gerçek kişilerin elektronik imza yaratabilecekleri ve elektronik sertifikaya sahip olabilecekleri belirtilmiştir. Aynı anlama geldiği halde bazı kanunlarda imza sahibi; sertifika sahibi, imza anahtarı sahibi gibi adlarla tanımlanmıştır. Bunlara ek olarak yabancı mevzuatta yapılan tanımlarda imza sahibinin, imzayı kendi veya temsil etmeye yetkili olduğu bir üçüncü kişi veya kurum adına kullanacağı eklenmiştir.

**İmza Oluşturma Verisi**

İmza oluşturma verisinin tanımı Kanun'a göre "İmza sahibine ait olan, imza sahibi tarafından elektronik imza oluşturma amacıyla kullanılan ve bir eşi daha olmayan şifreler, kriptografik gizli anahtarlar gibi veriler" şeklindedir. Tanım Direktif'in çevirisi şeklindedir ve yabancı mevzuatta da aynı biçimde tanımlanmıştır. Bu tanım uygulamada "private key" olarak bilinen özel veya kapalı anahtarı belirtmektedir. İmza oluşturma verisinin tanımı teknoloji bağımsız bir yöntemle yapılmıştır. Ancak konuyla ilgili teknik gereksinimler (anahtar uzunluğu, hash değer, rasgele oluşturma kalitesi -random creation quality- v.b.) yönetmelikle düzenlenmelidir. Uygulamada imza oluşturma verisi hem hizmet sağlayıcı tarafından hem de sertifika sahibi tarafından oluşturulabilmektedir.

**İmza Doğrulama Verisi**

İmza doğrulama verisinin tanımı Kanun'a göre "Elektronik imzayı doğrulamak için kullanılan şifreler, kriptografik açık anahtarlar gibi veriler" şeklindedir. Bu tanım uygulamada "public key" olarak bilinen açık anahtarı belirtmektedir. Tanım Direktif'in çevirisi şeklindedir ve yabancı mevzuatta da aynı şekilde tanımlanmıştır.

**İmza Oluşturma Aracı**

İmza oluşturma aracının tanımı Kanun'a göre "Elektronik imza oluşturmak üzere, imza oluşturma verisini kullanan yazılım veya donanım aracı şeklindedir. Bu tanımda Direktif'in çevirisidir ve yabancı mevzuatta aynı şekilde tanımlanmıştır. Uygulamada imza oluşturma araçları donanım bazlı olarak akıllı (smart) kartlar, USB Token'lar, bilgisayarlar veya veri işleme kapasitesi olan el terminalleri (PDA, cep telefonları, Pocket PC'ler v.b.) ile yazılım bazlı olarak da bilgisayar programları, smartcard'lar, işletim sistemleri veya özel yazılımlar v.b. şeklinde karşımıza çıkabilmektedir.

**İmza Doğrulama Aracı**

İmza doğruluma aracının tanımı Kanun'a göre "Elektronik imzayı doğrulamak amacıyla imza doğrulama verisini kullanan yazılım veya donanım aracı" şeklindedir. Bu tanımda Direktif'in çevirisidir ve yabancı mevzuatta aynı şekilde tanımlanmıştır. İmza oluşturma araçları aynı zamanda imza doğrulama araçları olarak da kullanılacağından dolayı burada istisnai olarak sadece imza doğrulama aracı olarak kullanılacak olan donanım ve/veya yazılım bazlı araçların yönetmelik içinde ayrı standartlara referans gösterilerek tanımlanması gerekebilir. Aksi durumda imza oluşturma araçları için belirlenen standartlar imza doğrulama araçlarını da karşılayacağından dolayı bu noktada suni ayrımlara gidilmeye gerek yoktur.

**Zaman Damgası**

Kanun'a göre zaman damgası "Bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı ve / veya kaydedildiği zamanın tespit edilmesi amacıyla, elektronik sertifika hizmet sağlayıcısı tarafından elektronik imzayla doğrulanan kayıt"tır. Direktif'te zaman damgasının tanımı yapılmamıştır.

Kanunumuzda yönetmelikle düzenlenecek hususlar belirtildiği (md.20)'de zaman damgasını düzenleyen hükme bir atıf olmadığından dolayı zaman damgası müstakilen yönetmelikle ayrıntılı olarak düzenlenemeyecektir. Ancak hizmet sağlayıcıların yükümlülükleri yönetmelikle düzenleneceği için bunlarla birlikte zaman damgası ile ilgili teknik gereksinimler de bu hüküm çerçevesi içersinde ele alınabilir.

**Güvenli Elektronik İmza**

Kanuna göre;

a) Münhasıran imza sahibine bağlı olan,

b) Sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan,

c) Nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan,

d) İmzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığınıntespitini sağlayan, elektronik imzalar güvenli elektronik imzadır." Güvenli elektronik imzaların önemi elle atılmış imza ile aynı hukuki sonucu doğurmalarıdır. Yabancı mevzuatta bu hukuki etkiye sahip elektronik imzalar çeşitli

adlarla (nitelikli, evrensel, elektronik imza v.b.) ve farklı teknik gereksinimlerle tanımlanmıştır. Ancak bütün bu imzaların ortak noktası, nitelikli elektronik sertifikaya dayanarak ve güvenli elektronik imza oluşturma aracıyla oluşturulmuş olmalarıdır.

**Elektronik Sertifika**

Kanun'a göre elektronik sertifika "İmza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kayıt"tır. Bu tanım Direktif'teki ve yabancı mevzuattaki sertifika tanımlarına uygundur. Elektronik sertifikalar; imzalama-doğrulama işlemi sırasında imzalayanın kimliğinin güvenilir üçüncü taraf (elektronik sertifika hizmet sağlayıcısı) tarafından teyit edilmesi amacıyla kullanılırlar.

**Kanunda Yer Almayan, Direktifte Bahsedilen Bazı Tanımlar**

**Elektronik İmza Ürünleri**

Direktifte ve yabancı mevzuatta yer alan bu tanım, sertifika hizmet sağlayıcıları tarafından elektronik imza servisleri için kullanılan veya e-İmza doğrulama veya oluşturma için kullanılan donanım, yazılım ve ilgili bileşenleri belirtmektedir. Buna göre elektronik imza ürünleri Direktif Ek 2/f, 3 ve 4 de yer alan araçlardır. Ek 2/f ve 3'de hizmet sağlayıcıların sertifika hizmeti sırasında kullanacakları araçlar ile imza oluşturma araçlarının gereksinimleri sayılmıştır. Nitelikli sertifika üretmek veya güvenli elektronik imza oluşturmak için burada bahsedilen teknik gereksinimlere uyulması zorunludur. Direktifin 3/5 md.'sine göre Komisyon bu eklerde belirtilen gereksinimlerin yerine geçmek üzere genel olarak tanınmış teknik standartları referans gösterebilir, bu standartları yerine getiren sertifika hizmet sağlayıcıları eklerdeki gereksinimleri yerine getirmiş sayılır. Komisyon bu maddeye dayanarak 13 Temmuz 2003'te aldığı bir kararla bazı standartları referans göstermiştir. Bu standartlara uyan sertifika hizmet sağlayıcıları ve imza oluşturma üreticileri/dağıtıcıları Eklerdeki gereksinimleri yerine getirmiş sayılacaklardır. Komisyon, kararında Avrupa Standardizasyon Komitesinin konuyla ilgili standartlarını referans göstermiştir.

**İhtiyari Akreditasyon**

İhtiyari Akreditasyon, sertifikasyon hizmeti sunulmasıyla ilgili tüm hak ve yükümlülükleri belirleyen, ilgili sertifikasyon hizmeti sunucusunun isteği üzerine bu hak ve yükümlülüklerin geliştirilmesi ve denetimi ile ilgili kamuya da, özel nitelikli kurum tarafından verilen ve sertifikasyon hizmeti sunucusunun bu izinden kaynaklanan haklarını kullanmasına ilgili kararın kendisine ulaşmasına dek engel olan her türlü izindir.

**Elektronik Sertifika Hizmet Sağlayıcısı (ESHS)**

Açık elektronik ağlardan sayısal imzalı bilgi gönderen kişinin imzasının geçerliliğinin/doğruluğunun saptanması için, imzayı atanın açık anahtarı gereklidir. Bu nedenle hangi açık anahtarın hangi kullanıcıya ait olduğunun belgelenmesi çok önemlidir. Bunun için kullanıcıların açık anahtarlarını ve kimlik bilgilerini onaylama yetkisine sahip bir kuruluşa, bir otoriteye gereksinim vardır. Elektronik sertifika hizmet sağlayıcıları kişi ve kurumlara sertifika üreten, dağıtan ve belgelerin yönetimini üstlenen güvenilir kurumlardır.

ESHSlerin kendilerine ait bir veya birden fazla anahtar çiftleri bulunur. Bu anahtar çiftlerinden gizli anahtarın yetkili kişiler dışında kimsenin ulaşamayacağı şekilde güvenli bir ortamda tutulması ve çok iyi korunması gerekmektedir. Açık anahtar ise kullanıcılarda olduğu gibi kök sertifika da denen ESHS sertifikaları içinde bulunur. Her ESHS'nin bir kök sertikası vardır ve ESHS kök sertifikalarını kamuya açarak dizin sunucular (“directory services”) gibi herkesin ulaşabileceği yerlerde tutmalıdır.

**Kişisel Sertifika**

Kişisel sertifikalar sadece kişilere verilen özel bir elektronik sertifikadır. Sertifikalar yaygın olarak X.509 standartına uygun olarak üretilir ve bu standartla uyumlu olan web tarayıcılarına, akıllı kartlara ya da token'lara yüklenebilir.

**Sunucu Sertifikası**

Sunucu sertifikaları, web sitesinin kimlik bilgilerini ve açık anahtarını taşıyan ve web sitesine bağlanan kullanıcılara sunulan elektronik dosyalardır. Sunucu sertifikası, temelde web sunucusunun adresini ve açık anahtarını bulundurur. Sunucu sertifikaları, web sunucunun kimliğinin doğrulanması ve sunucuya gönderilecek olan bilginin SSL teknolojisi kullanılarak şifreli gönderilmesi. Gönderilecek olan bilgi sunucu sertifikasının içindeki açık anahtar ile şifrelenir. Bu şifreli bilgiyi çözecek gizli anahtar sadece sunucuda bulunduğundan

başka birisinin şifreyi çözmesi mümkün değildir. Böylece şifreli bilginin internet üzerinden gönderiminde güvenlik sağlanmış olur.

**Kök Sertifika**

Kök sertifika, ESHS'nin kimlik bilgilerini ve açık anahtarını taşıyan elektronik dosyadır. Kök sertifikasını diğer sertifikalarden ayıran tek özellik, üzerinde kendi imzasını taşıyor olmasıdır. Yayınladıkları diğer sertifikalara güvenilirlik onayının verilebilmesi için kök sertifikanın, kullanıcı tarafında mevcut olmaları gereklidir. Örneğin bir web sunucusunun sertifikasını alan internet tarayıcısı bu kimliğe güvenip güvenmeyeceğine karar verebilmesi için sunucuya sertifikayı veren sertifika hizmet sağlayıcısının kök sertifikasına ihtiyaç duyar. Eğer söz konusu kök sertifika, internet tarayıcısında tanımlı değilse, tarayıcı bu sitenin güvenilir olmadığını kullanıcıya bildirir. Bazı ESHS sertifikaları, Netscape ve Internet explorer gibi popüler olan tarayıcılarda önceden tanımlanmıştır yani kök sertifikalar tarayıcıya yüklenmiş durumdadır. Diğer ESHS kök sertifikalarının da tarayıcıya tanımlanabilmesi için kök sertifikaların tarayıcıya yüklenmesi gerekmektedir.

**Anahtar Anlaşma Protokolü**

Anahtar anlaşma protokolü, tek anahtarlı yapılarda iki tarafın gizli anahtar üzerinde anlaşması gereken durumlarda kullanılır. Bu protokoller ortam güvenli olmasa da, daha önceden üzerinde anlaşılmış anahtara gerek duymaksızın tarafların güvenli bir şekilde gizli anahtar üzerinde anlaşmasını sağlar.

**SSL (Secure Socket Layer)**

SSL teknolojisi TCP/IP protokolü üzerinden çalışan, web sunucusu ve web tarayıcısı arasındaki tüm bilgi akışını koruyan bir güvenlik protokolüdür. Bütün popüler web tarayıcılarda ve web sunuculardа uygulanmaktadır. Bugünün web üzerinden elektronik ticaret ve elektronik iş uygulamalarında önemli bir rolü vardır. SSL protokolü iki taraf arasında güvenli ve gizli iletişimin sağlanmasında elektronik sertifika kullanır. SSL bağlantısı üzerinden gönderilen veriler üçüncü şahıslar tarafından bozguna uğratıldığında, bundan tarafların anında haberi olur.

Bir web sunucusunun kullanıcılarıyla SSL bağlantısı sağlayabilmesi için öncelikle sunucu tarafında bir sunucu sertifikası bulunması gereklidir. SSL ile güvenliği sağlanmış bir siteye bağlanan kullanıcı sitenin URL adresinin "https:" ile başladığını görür. Daha sonra SSL bağlantısı kurulur ve sunucu-tarayıcı arasındaki tüm veriler üçüncü şahısların mesajı okumasını önlemek amacıyla şifrelenir.Bu işlemlerin

amacı kullanıcıya bağlandığı sitenin gerçekten bağlandığını düşündüğü site olduğunun ispatının sağlanmasıdır. Kullanıcı bundan emin olmak için SSL bağlantısı süresince sunucudan gelen her bilgiyi web sayfasının güvenlikle ilgili özelliklerine bakarak kontrol etmelidir. Web sayfalarının güvenlik bilgileri sunucunun sertifikasını kontrol imkanı sağlar. Eğer yabancı veya farklı bir sunucunun sertifikasıyla karşılaşılırsa bağlanılan sunucu bağlanıldığı sanılan sunucu değildir ve iletişimin güvenliği tehdit altındadır.

**Özet Fonksiyonu**

Özet fonksiyonu bir mesajın 16 veya 20 bitlik parmak izini çıkarır. Belli bir mesaj aynı özet algoritması kullanıldığında, aynı mesaj özetini verir. Eğer iyi bir özet fonksiyonu kullanılıyorsa, mesajda yapılan tek bitlik bir değişim bile mesaj özetinin değişmesine sebep olur. Özet fonksiyonu kullanarak, kimlik denetimi amacıyla gizli anahtarla bütün mesajı şifrelemek zorunluluğu ortadan kalkar. Özet fonksiyonları verilen mesajı şifreler, ancak bunun geri dönüşü yoktur, yani eldeki mesaj özeti kullanılarak orijinal mesaj elde edilemez.

**EK - B**

**5070 Sayılı Elektronik İmza Kanunu**

---

*ELEKTRONİK İMZA KANUNU*

**23 Ocak 2004 tarih ve 25355 sayılı Resmi Gazete**

**Kanun No. 5070** **Kabul Tarihi : 15.1.2004**

## BİRİNCİ KISIM

### Amaç, Kapsam ve Tanımlar

**Amaç**

**MADDE 1.-** Bu Kanunun amacı, elektronik imzanın hukukî ve teknik yönleri ile kullanımına ilişkin esasları düzenlemektir.

**Kapsam**

**MADDE 2.-** Bu Kanun, elektronik imzanın hukukî yapısını, elektronik sertifika hizmet sağlayıcılarının faaliyetlerini ve her alanda elektronik imzanın kullanımına ilişkin işlemleri kapsar.

**Tanımlar**

**MADDE 3.-** Bu Kanunda geçen;

a) Elektronik veri: Elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıtları,

b) Elektronik imza: Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veriyi,

c) İmza sahibi: Elektronik imza oluşturmak amacıyla bir imza oluşturma aracını kullanan gerçek kişiyi,

d) İmza oluşturma verisi: İmza sahibine ait olan, imza sahibi tarafından elektronik imza oluşturma amacıyla kullanılan ve bir eşi daha olmayan şifreler, kriptografik gizli anahtarlar gibi verileri,

e) İmza oluşturma aracı: Elektronik imza oluşturmak üzere, imza oluşturma verisini kullanan yazılım veya donanım aracını,

f) İmza doğrulama verisi: Elektronik imzayı doğrulamak için kullanılan şifreler, kriptografik açık anahtarlar gibi verileri,

g) İmza doğrulama aracı: Elektronik imzayı doğrulamak amacıyla imza doğrulama verisini kullanan yazılım veya donanım aracını,

h) Zaman damgası: Bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı ve / veya kaydedildiği zamanın tespit edilmesi amacıyla, elektronik sertifika hizmet sağlayıcısı tarafından elektronik imzayla doğrulanan kaydı,

ı) Elektronik sertifika: İmza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kaydı,

j) Kurum: Telekomünikasyon Kurumunu,

İfade eder.

## İKİNCİ KISIM

## Güvenli Elektronik İmza ve

## Sertifika Hizmetleri

## BİRİNCİ BÖLÜM

## Güvenli Elektronik İmza, Güvenli Elektronik İmza Oluşturma ve Doğrulama Araçları

**Güvenli elektronik imza**

**MADDE 4.-** Güvenli elektronik imza;

a) Münhasıran imza sahibine bağlı olan,

b) Sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan,

c) Nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan,

d) İmzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan,

Elektronik imzadır.

**Güvenli elektronik imzanın hukukî sonucu ve uygulama alanı**

**MADDE 5.-** Güvenli elektronik imza, elle atılan imza ile aynı hukukî sonucu doğurur.

Kanunların resmî şekle veya özel bir merasime tabi tuttuğu hukukî işlemler ile teminat sözleşmeleri güvenli elektronik imza ile gerçekleştirilemez.

**Güvenli elektronik imza oluşturma araçları**

**MADDE 6.-** Güvenli elektronik imza oluşturma araçları;

a) Ürettiği elektronik imza oluşturma verilerinin kendi aralarında bir eşi daha bulunmamasını,

b) Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin araç dışına hiçbir biçimde çıkarılamamasını ve gizliliğini,

c) Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin, üçüncü kişilerce elde edilememesini, kullanılamamasını ve elektronik imzanın sahteciliğe karşı korunmasını,

d) İmzalanacak verinin imza sahibi dışında değiştirilememesini ve bu verinin imza sahibi tarafından imzanın oluşturulmasından önce görülebilmesini,

Sağlayan imza oluşturma araçlarıdır.

**Güvenli elektronik imza doğrulama araçları**

**MADDE 7.-** Güvenli elektronik imza doğrulama araçları;

a) İmzanın doğrulanması için kullanılan verileri, değiştirmeksizin doğrulama yapan kişiye gösteren,

b) İmza doğrulama işlemini güvenilir ve kesin bir biçimde çalıştıran ve doğrulama sonuçlarını değiştirmeksizin doğrulama yapan kişiye gösteren,

c) Gerektiğinde, imzalanmış verinin güvenilir bir biçimde gösterilmesini sağlayan,

d) İmzanın doğrulanması için kullanılan elektronik sertifikanın doğruluğunu ve geçerliliğini güvenilir bir biçimde tespit ederek sonuçlarını değiştirmeksizin doğrulama yapan kişiye gösteren,

e) İmza sahibinin kimliğini değiştirmeksizin doğrulama yapan kişiye gösteren,

f) İmzanın doğrulanması ile ilgili şartlara etki edecek değişikliklerin tespit edilebilmesini sağlayan,

İmza doğrulama araçlarıdır.

## İKİNCİ BÖLÜM

## Elektronik Sertifika Hizmet Sağlayıcısı, Nitelikli Elektronik Sertifika ve Yabancı Elektronik Sertifikalar

**Elektronik sertifika hizmet sağlayıcısı**

**MADDE 8.-** Elektronik sertifika hizmet sağlayıcısı, elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve

kuruluşları ile gerçek veya özel hukuk tüzel kişilerdir. Elektronik sertifika hizmet sağlayıcısı, Kuruma yapacağı bildirimden iki ay sonra faaliyete geçer.

Elektronik sertifika hizmet sağlayıcısı yapacağı bildirimde;

a) Güvenli ürün ve sistemleri kullanmak,

b) Hizmeti güvenilir bir biçimde yürütmek,

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

İle ilgili şartları sağladığını ayrıntılı bir biçimde gösterir.

Kurum, yukarıdaki şartlardan birinin eksikliğini veya yerine getirilmediğini tespit ederse, bu eksikliklerin giderilmesi için, elektronik sertifika hizmet sağlayıcısına bir ayı geçmemek üzere bir süre verir, bu süre içinde elektronik sertifika hizmet sağlayıcısının faaliyetlerini durdurur. Sürenin sonunda eksikliklerin giderilmemesi halinde elektronik sertifika hizmet sağlayıcısının faaliyetine son verir. Kurumun bu kararlarına karşı 19 uncu maddenin ikinci fıkrası hükümleri gereğince itiraz edilebilir.

Elektronik sertifika hizmet sağlayıcılarının faaliyetlerinin devamı sırasında bu maddede gösterilen şartları kaybetmeleri hâlinde de yukarıdaki fıkra hükümleri uygulanır.

Elektronik sertifika hizmet sağlayıcıları, Kurumun belirleyeceği ücret alt ve üst sınırlarına uymak zorundadır.

**Nitelikli elektronik sertifika**

**MADDE 9.-** Nitelikli elektronik sertifikada;

a) Sertifikanın "nitelikli elektronik sertifika" olduğuna dair bir ibarenin,

b) Sertifika hizmet sağlayıcısının kimlik bilgileri ve kurulduğu ülke adının,

c) İmza sahibinin teşhis edilebileceği kimlik bilgilerinin,

d) Elektronik imza oluşturma verisine karşılık gelen imza doğrulama verisinin,

e) Sertifikanın geçerlilik süresinin başlangıç ve bitiş tarihlerinin,

f) Sertifikanın seri numarasının,

g) Sertifika sahibi diğer bir kişi adına hareket ediyorsa bu yetkisine ilişkin bilginin,

h) Sertifika sahibi talep ederse meslekî veya diğer kişisel bilgilerinin,

ı) Varsa sertifikanın kullanım şartları ve kullanılacağı işlemlerdeki maddî sınırlamalara ilişkin bilgilerin,

j) Sertifika hizmet sağlayıcısının sertifikada yer alan bilgileri doğrulayan güvenli elektronik imzasının,

Bulunması zorunludur.

**Elektronik sertifika hizmet sağlayıcısının yükümlülükleri**

**MADDE 10.-** Elektronik sertifika hizmet sağlayıcısı;

a) Hizmetin gerektirdiği nitelikte personel istihdam etmekle,

b) Nitelikli sertifika verdiği kişilerin kimliğini resmî belgelere göre güvenilir bir biçimde tespit etmekle,

c) Sertifika sahibinin diğer bir kişi adına hareket edebilme yetkisi, meslekî veya diğer kişisel bilgilerinin sertifikada bulunması durumunda, bu bilgileri de resmî belgelere dayandırarak güvenilir bir biçimde belirlemekle,

d) İmza oluşturma verisinin sertifika hizmet sağlayıcısı tarafından veya sertifika talep eden kişi tarafından sertifika hizmet sağlayıcısına ait yerlerde üretilmesi durumunda bu işlemin gizliliğini sağlamak veya sertifika hizmet sağlayıcısının sağladığı araçlarla üretilmesi durumunda, bu işleyişin güvenliğini sağlamakla,

e) Sertifikanın kullanımına ilişkin özelliklerin ve uyuşmazlıkların çözüm yolları ile ilgili şartların ve kanunlarda öngörülen sınırlamalar saklı kalmak üzere güvenli

elektronik imzanın elle atılan imza ile eşdeğer olduğu hakkında sertifika talep eden kişiyi sertifikanın tesliminden önce yazılı olarak bilgilendirmekle,

f) Sertifikada bulunan imza doğrulama verisine karşılık gelen imza oluşturma verisini başkasına kullandırmaması konusunda, sertifika sahibini yazılı olarak uyarmak ve bilgilendirmekle,

g)Yaptığı hizmetlere ilişkin tüm kayıtları yönetmelikle belirlenen süreyle saklamakla,

h) Faaliyetine son vereceği tarihten en az üç ay önce durumu Kuruma ve elektronik sertifika sahibine bildirmekle,

Yükümlüdür.

Elektronik sertifika hizmet sağlayıcısı üretilen imza oluşturma verisinin bir kopyasını alamaz veya bu veriyi saklayamaz.

**Nitelikli elektronik sertifikaların iptal edilmesi**

**MADDE 11.-** Elektronik sertifika hizmet sağlayıcısı;

a) Nitelikli elektronik sertifika sahibinin talebi,

b) Sağladığı nitelikli elektronik sertifikaya ilişkin veri tabanında bulunan bilgilerin sahteliğinin veya yanlışlığının ortaya çıkması veya bilgilerin değişmesi,

c) Nitelikli elektronik sertifika sahibinin fiil ehliyetinin sınırlandığının, iflâsının veya gaipliğinin ya da ölümünün öğrenilmesi,

Durumunda vermiş olduğu nitelikli elektronik sertifikaları derhâl iptal eder.

Elektronik sertifika hizmet sağlayıcısı, nitelikli elektronik sertifikaların iptal edildiği zamanın tam olarak tespit edilmesine imkân veren ve üçüncü kişilerin hızlı ve güvenli bir biçimde ulaşabileceği bir kayıt oluşturur.

Elektronik sertifika hizmet sağlayıcısı, faaliyetine son vermesi ve vermiş olduğu nitelikli elektronik sertifikaların başka bir elektronik sertifika hizmet sağlayıcısı

tarafından kullanımının sağlanamaması durumunda vermiş olduğu nitelikli elektronik sertifikaları derhâl iptal eder.

Elektronik sertifika hizmet sağlayıcısının faaliyetine Kurum tarafından son verilmesi halinde Kurum, faaliyetine son verilen elektronik sertifika hizmet sağlayıcısının vermiş olduğu nitelikli elektronik sertifikaların başka bir elektronik sertifika hizmet sağlayıcısına devredilmesine karar verir ve durumu ilgililere duyurur.

Elektronik sertifika hizmet sağlayıcısı geçmişe yönelik olarak nitelikli elektronik sertifika iptal edemez.

**Bilgilerin korunması**

**MADDE 12.-** Elektronik sertifika hizmet sağlayıcısı;

a) Elektronik sertifika talep eden kişiden, elektronik sertifika vermek için gerekli bilgiler hariç bilgi talep edemez ve bu bilgileri kişinin rızası dışında elde edemez,

b) Elektronik sertifika sahibinin izni olmaksızın sertifikayı üçüncü kişilerin ulaşabileceği ortamlarda bulunduramaz,

c) Elektronik sertifika talep eden kişinin yazılı rızası olmaksızın üçüncü kişilerin kişisel verileri elde etmesini engeller. Bu bilgileri sertifika sahibinin onayı olmaksızın üçüncü kişilere iletemez ve başka amaçlarla kullanamaz.

**Hukukî sorumluluk**

**MADDE 13.-** Elektronik sertifika hizmet sağlayıcısının, elektronik sertifika sahibine karşı sorumluluğu genel hükümlere tâbidir.

Elektronik sertifika hizmet sağlayıcısı, bu Kanun veya bu Kanuna dayanılarak çıkarılan yönetmelik hükümlerinin ihlâli suretiyle üçüncü kişilere verdiği zararları tazminle yükümlüdür. Elektronik sertifika hizmet sağlayıcısı kusursuzluğunu ispat ettiği takdirde tazminat ödeme yükümlülüğü doğmaz.

Elektronik sertifika hizmet sağlayıcısı, söz konusu yükümlülük ihlâlinin istihdam ettiği kişilerin davranışına dayanması hâlinde de zarardan sorumlu olup, elektronik sertifika hizmet sağlayıcısı, bu sorumluluğundan, Borçlar Kanununun 55 inci maddesinde öngörülen türden bir kurtuluş kanıtı getirerek kurtulamaz.

Nitelikli elektronik sertifikanın içerdiği kullanım ve maddî kapsamına ilişkin sınırlamalar hariç olmak üzere, elektronik sertifika hizmet sağlayıcısının üçüncü kişilere ve nitelikli elektronik imza sahibine karşı sorumluluğunu ortadan kaldıran veya sınırlandıran her türlü şart geçersizdir.

Elektronik sertifika hizmet sağlayıcısı, bu Kanundan doğan yükümlülüklerini yerine getirmemesi sonucu doğan zararların karşılanması amacıyla sertifika malî sorumluluk sigortası yaptırmak zorundadır. Sigortaya ilişkin usul ve esaslar Hazine Müsteşarlığının görüşü alınarak Kurum tarafından çıkarılacak yönetmelikle belirlenir.

Bu maddede öngörülen sertifika malî sorumluluk sigortası Türkiye'de ilgili branşta çalışmaya yetkili olan sigorta şirketleri tarafından yapılır. Bu sigorta şirketleri sertifika malî sorumluluk sigortasını yapmakla yükümlüdürler. Bu yükümlülüğe uymayan sigorta şirketlerine Hazine Müsteşarlığınca sekizmilyar lira idarî para cezası verilir. Bu para cezasının tahsilinde ve cezaya itiraz usulünde 18 inci madde hükümleri uygulanır.

Elektronik sertifika hizmet sağlayıcısı, nitelikli elektronik sertifikayı elektronik imza sahibine sigorta ettirerek teslim etmekle yükümlüdür.

**Yabancı elektronik sertifikalar**

**MADDE 14.-** Yabancı bir ülkede kurulu bir elektronik sertifika hizmet sağlayıcısı tarafından verilen elektronik sertifikaların hukukî sonuçları milletlerarası anlaşmalarla belirlenir.

Yabancı bir ülkede kurulu bir elektronik sertifika hizmet sağlayıcısı tarafından verilen elektronik sertifikaların, Türkiye'de kurulu bir elektronik sertifika hizmet sağlayıcısı tarafından kabul edilmesi durumunda, bu elektronik sertifikalar nitelikli elektronik sertifika sayılır. Bu elektronik sertifikaların kullanılması sonucunda

doğacak zararlardan, Türkiye'deki elektronik sertifika hizmet sağlayıcısı da sorumludur.

## ÜÇÜNCÜ KISIM

## Denetim ve Ceza Hükümleri

### Denetim

**MADDE 15.-** Elektronik sertifika hizmet sağlayıcılarının bu Kanunun uygulanmasına ilişkin faaliyet ve işlemlerinin denetimi Kurumca yerine getirilir.

Kurum, gerekli gördüğü zamanlarda elektronik sertifika hizmet sağlayıcılarını denetleyebilir. Denetleme sırasında, denetleme yapmaya yetkili görevliler tarafından her türlü defter, belge ve kayıtların verilmesi, yönetim yerleri, binalar ve eklentilerine girme, yazılı ve sözlü bilgi alma, örnek alma ve işlem ve hesapları denetleme isteminin elektronik sertifika hizmet sağlayıcıları ve ilgililer tarafından yerine getirilmesi zorunludur.

### İmza oluşturma verilerinin izinsiz kullanımı

**MADDE 16.-** Elektronik imza oluşturma amacı ile ilgili kişinin rızası dışında; imza oluşturma verisi veya imza oluşturma aracını elde eden, veren, kopyalayan ve bu araçları yeniden oluşturanlar ile izinsiz elde edilen imza oluşturma araçlarını kullanarak izinsiz elektronik imza oluşturanlar bir yıldan üç yıla kadar hapis ve beşyüz milyon liradan aşağı olmamak üzere ağır para cezasıyla cezalandırılırlar.

Yukarıdaki fıkrada işlenen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar artırılır.

Bu maddedeki suçlar nedeniyle oluşan zarar ayrıca tazmin ettirilir.

### Elektronik sertifikalarda sahtekârlık

**MADDE 17.-** Tamamen veya kısmen sahte elektronik sertifika oluşturanlar veya geçerli olarak oluşturulan elektronik sertifikaları taklit veya tahrif edenler ile yetkisi olmadan elektronik sertifika oluşturanlar veya bu elektronik sertifikaları bilerek

kullananlar, fiilleri başka bir suç oluştursa bile ayrıca, iki yıldan beş yıla kadar hapis ve birmilyar liradan aşağı olmamak üzere ağır para cezasıyla cezalandırılırlar.

Yukarıdaki fıkrada işlenen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar artırılır.

Bu maddedeki suçlar nedeniyle oluşan zarar ayrıca tazmin ettirilir.

**İdarî para cezaları**

**MADDE 18.-** Bu Kanunun;

a) 10 uncu maddesindeki yükümlülüklerinden herhangi birini yerine getirmeyen elektronik sertifika hizmet sağlayıcısına onmilyar lira,

b) 11 inci maddesindeki yükümlülüklerden herhangi birini yerine getirmeyen elektronik sertifika hizmet sağlayıcısına sekizmilyar lira,

c) 12 nci maddesi hükümlerine aykırı hareket edenler hakkında onmilyar lira,

d) 13 üncü maddesinin beş ve yedinci fıkralarındaki yükümlülükleri yerine getirmeyen elektronik sertifika hizmet sağlayıcısına sekizmilyar lira,

e) 15 inci maddesi hükmüne aykırı hareket eden elektronik sertifika hizmet sağlayıcısına yirmimilyar lira,

İdarî para cezası Telekomünikasyon Kurulu tarafından verilir. Verilen para cezalarına dair kararlar ilgililere 7201 sayılı Tebligat Kanunu hükümlerine göre tebliğ edilir. Bu cezalara karşı tebliğ tarihinden itibaren en geç yedi gün içinde yetkili idare mahkemesine itiraz edilebilir. İtiraz, verilen cezanın yerine getirilmesini durdurmaz. İtiraz, zaruret görülmeyen hâllerde, evrak üzerinden inceleme yapılarak en kısa sürede sonuçlandırılır. İtiraz üzerine verilen kararlara karşı Bölge İdare Mahkemesine başvurulabilir. Bölge İdare Mahkemesinin verdiği kararlar kesindir. Bu Kanuna göre verilen idarî para cezaları, Kurumun bildirimi üzerine 6183 sayılı Amme Alacaklarının Tahsil Usulü Hakkında Kanun hükümlerine göre Maliye Bakanlığınca tahsil olunur.

**İdarî nitelikteki suçların tekrarı ve kapatma**

**MADDE 19.-** 18 inci maddedeki suçları işleyenlerin bu suçları işledikleri tarihten itibaren geriye doğru üç yıl içinde ikinci kez işlemeleri hâlinde para cezaları iki kat olarak uygulanır, üçüncü kez işlemeleri hâlinde ise Kurum tarafından elektronik sertifika hizmet sağlayıcıları hakkında kapatma cezası verilir.

Kapatma cezası verilmesine ilişkin karar 7201 sayılı Tebligat Kanununa göre ilgililere tebliğ edilir. Bu karara karşı tebliğ tarihinden itibaren en geç yedi gün içinde yetkili idare mahkemesine itiraz edilebilir. İtiraz, yetkili makam tarafından verilen kapatma kararının yerine getirilmesini durdurmaz. İtiraz, zaruret görülmeyen hâllerde, evrak üzerinden inceleme yapılarak en kısa sürede sonuçlandırılır. İtiraz üzerine verilen kararlara karşı Bölge İdare Mahkemesine başvurulabilir. Bölge İdare Mahkemesinin verdiği kararlar kesindir.

## DÖRDÜNCÜ KISIM

## Çeşitli Hükümler

**Yönetmelik**

**MADDE 20.-** Bu Kanunun 6, 7, 8, 10, 11 ve 14 üncü maddelerinin uygulanmasına ilişkin usul ve esaslar, Kanunun yürürlük tarihinden itibaren altı ay içinde ilgili kurum ve kuruluşların görüşleri alınarak Kurum tarafından çıkarılacak yönetmeliklerle düzenlenir.

**Kamu kurum ve kuruluşları hakkında uygulanmayacak hükümler**

**MADDE 21.-** Bu Kanunun 8 inci maddesinin dört ve beşinci fıkraları ile 15 ve 19 uncu maddesi hükümleri, elektronik sertifika hizmet sağlama faaliyeti yerine getiren kamu kurum ve kuruluşları hakkında uygulanmaz.

**MADDE 22.-** 22.4.1926 tarihli ve 818 sayılı Borçlar Kanununun 14 üncü maddesinin birinci fıkrasına aşağıdaki cümle eklenmiştir.

Güvenli elektronik imza elle atılan imza ile aynı ispat gücünü haizdir.

**MADDE 23.-** 18.6.1927 tarihli ve 1086 sayılı Hukuk Usulü Muhakemeleri Kanununa 295 inci maddeden sonra gelmek üzere aşağıdaki 295/A maddesi eklenmiştir.

MADDE 295/A- Usulüne göre güvenli elektronik imza ile oluşturulan elektronik veriler senet hükmündedir. Bu veriler aksi ispat edilinceye kadar kesin delil sayılırlar.

Dava sırasında bir taraf kendisine karşı ileri sürülen ve güvenli elektronik imza ile oluşturulmuş veriyi inkâr ederse, bu Kanunun 308 inci maddesi kıyas yoluyla uygulanır.

**MADDE 24.-** 5.4.1983 tarihli ve 2813 sayılı Telsiz Kanununun 7 nci maddesinin birinci fıkrasına aşağıdaki (m) bendi eklenmiş ve mevcut (m) bendi (n) bendi olarak teselsül ettirilmiştir.

m) Elektronik İmza Kanunu ile verilen görevleri yerine getirmek,

**Yürürlük**

**MADDE 25.-** Bu Kanun yayımı tarihinden altı ay sonra yürürlüğe girer.

**Yürütme**

**MADDE 26.-** Bu Kanun hükümlerini Bakanlar Kurulu yürütür.