TELEKOMÜNİKASYON REGÜLASYONLARI ÇERÇEVESİNDE ELEKTRONİK TİCARETİN İNCELENMESİ

Ayşe İNALÖZ

UZMANLIK TEZİ

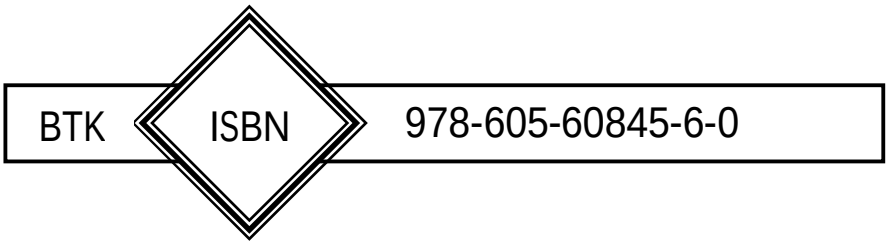
TELEKOMÜNİKASYON KURUMU

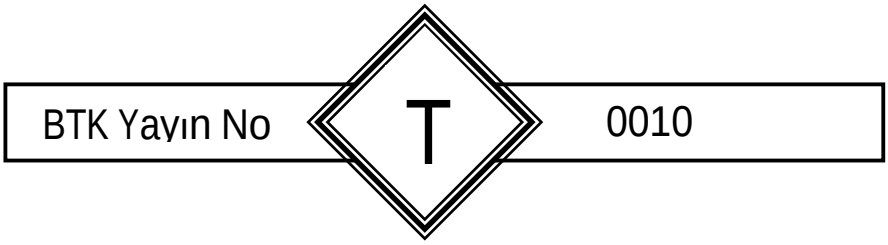
Ağustos 2003

ANKARA

Bu yayında öne sürülen fikirler eserin yazarına aittir;

Bilgi Teknolojileri ve İletişim Kurumunun görüşlerini yansıtmaz.





AYŞE İNALÖZ tarafından hazırlanan **TELEKOMÜNİKASYON REGÜLASYONLARI ÇERÇEVESİNDE ELEKTRONİK TİCARETİN İNCELENMESİ** adlı bu tezin Uzmanlık Tezi olarak uygun olduğunu onaylarım.

Doç. Dr. Mustafa ALKAN
Tez Yöneticisi

Bu çalışma, jürimiz tarafından Uzmanlık Tezi olarak kabul edilmiştir.

Başkan : Hüseyin EDİS

Üye : Prof Dr. Emin ÇARIKÇI

Üye : Prof. Dr. İnan GÜLER

Üye : Doç. Dr. Mustafa ALKAN

Üye : Dr. Mehmet ALTUNER

Üye : Ejder ORUÇ

Üye : Ö. Faruk KOÇAK

Bu tez, Telekomünikasyon Kurumu tez yazım kurallarına uygundur.

İÇİNDEKİLER

TELEKOMÜNİKASYON REGÜLASYONLARI ÇERÇEVESİNDE ELEKTRONİK TİCARETİN İNCELENMESİ

(Uzmanlık Tezi)

AYŞE İNALÖZ

TELEKOMÜNİKASYON KURUMU

Ağustos 2003

ÖZET

Bu tez çalışmasında telekomünikasyon regülasyonları yönünden elektronik ticaret incelenmiştir. Elektronik ticareti kuşatan teknolojik ve piyasa eğilimlerinin içeriği ve tarihçesi, elektronik imza kavramı, sayısal imzanın dayandığı temeller, uluslararası teşebbüsler ve Ülkemizde bu meyanda yürütülmekte olan çalışmalar detaylıca incelenmiştir. Kurumumuzun uygulayacağı uygun modelin çerçevesi çizilerek, sözkonusu modelin oluşturulmasını teminen sayısal imza kanunları vasıtasıyla kök sertifika hizmet sağlayıcısı olarak görevlendirilmiş, elektronik imza konusunda lider konumdaki Almanya, Avusturya, Danimarka, Finlandiya telekomünikasyon regülasyon kurumlarının uyguladıkları modeller örnek olarak seçilmiştir. Sözkonusu ülkelerin yönetmelikleri ve telekomünikasyon regülasyon kurumlarının sorumlulukları incelenmiş, yayınlamış oldukları yönetmeliklerin çevirisi yapılmış ve kurumumuz koordinatörlüğünde yürütülecek olan yönetmelik çalışmalarına model olması açısından iki yönetmelik taslağı hazırlanmıştır. Ayrıca farklı bir örnek olması açısından İngiltere Ticaret ve Endüstri Bakanlığı (Department of Trade and Industry-(DTI) Modeli de incelenmiştir.

Anahtar Kelimeler: Elektronik ticaret, sayısal imza, telekomünikasyon regülasyonu, açık anahtar alt yapısı
Sayfa Adedi : 276
Tez Yöneticisi : Doç. Dr. Mustafa ALKAN

A RESEARCH ON ELECTRONIC COMMERCE IN THE FRAMEWORK OF TELECOMMUNICATIONS REGULATORY ISSUES

(Telecommunications Expert Thesis)

AYŞE İNALÖZ

TELECOMMUNICATIONS AUTHORITY

August 2003

ABSTRACT

In this thesis study electronic commerce was examined with regard to telecommunications regulations. Technological and market trends, history that cover electronic commerce, electronic signature concept, basics of digital signatures, international initiatives and studies that have been executed in our country were investigated in detail. Suitable framework model for our Authority was stated. In order to create this model Danish, Austrian, Finnish and German Telecommunications Regulatory Authorities, authorized by their electronic signature law as the root certification authority, chosen as a sample. Their responsibilities investigated and their ordinances were translated to Turkish. Two ordinance sample was prepared as a model for the ordinance studies that will be coordinated by our authority. In addition to these, British Department of Trade and Industry's Model was examined with regard to be a different model.

Key Words : Electronic Commerce, digital signature, telecommunications regulations, public key infrastructure
Page Number : 276
Adviser : Assoc. Prof. Dr. Mustafa ALKAN, Vice President

TEŞEKKÜR

Tez çalışmam süresince yol göstererek beni destekleyen, değerli katkılarını esirgemeyen kıymetli Tez Danışmanım Sayın Doç. Dr. Mustafa ALKAN'a, Daire Başkanım Sayın Ömer Faruk KOÇAK'a, sağladığı imkanlar dolayısıyla Kurumuma, manevi desteklerini her zaman yanımda hissettiğim saygıdeğer Kurul Başkanımıza ve Kurul Üyelerimize, destek ve yardımlarıyla bana güç veren Uluslararası İlişkiler ve AB ile Koordinasyon Dairesi Başkanlığı ve Telekomünikasyon Kurumundaki arkadaşlarıma, değerli aileme ve dostlarıma içtenlikle teşekkür ederim.

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

SİMGELER VE KISALTMALAR

Kısaltmalar

AB	Avrupa Birliği
APEC	Asian-Pacific Economic Cooperation Asya Pasifik Ekonomik İşbirliği
ARPANET	Advanced Research Projects Agency Network İleri Düzey Araştırma Projeleri Şebekesi
ATM	Automated Teller Machine
APEC	Asian-Pacific Economic Cooperation Asya Pasifik Ekonomik İşbirliği
B2C	Business to Consumer İşletmeler-Tüketiciler arası E-Ticaret
BM	Birleşmiş Milletler
BTYK	Bilim ve Teknoloji Yüksek Kurulu
CA	Certification Authority Sertifika Hizmet Sağlayıcı (SHS)
CEN	European Committee for Standardization Avrupa Standardizasyon Komitesi
CEPT	Conference of European Post and Telecommunications Avrupa Posta ve Telekomünikasyon Konferansı
CWA	CEN Workshop Agreements CEN Çalıştay Anlaşmaları
DARPA	Defense Advanced Research Projects Agency Savunma İleri Düzey Araştırma Projeleri Kurumu
DTI	Department of Trade and Industry İngiltere Ticaret ve Endüstri Bakanlığı
DTM	Dış Ticaret Müsteşarlığı
EESSI	The European Electronic Signature Standardisation Initiative Avrupa Elektronik İmza Standardizasyonu Teşebbüsü
ETKK	Elektronik Ticaret Koordinasyon Kurulu
ETSI	European Telecommunications Standardisation Institude Avrupa Telekomünikasyon Standartları Enstitüsü
FESA	Forum of European Supervisory Authorities for Electronic Signatures Avrupa Elektronik İmzalar Denetleyici Kuruluşlar Forumu
FICORA	Finnish Communications Regulatory Authority Finlandiya Haberleşme Regülasyon Kurumu
FTAA	Free Trade Area of the Americas Amerika Serbest Ticaret Bölgesi
GATS	The General Agreement on Trade in Services Hizmet Ticareti Genel Anlaşması
GATT	General Agreement on Tariffs and Trade Tarifeler ve Ticaret Genel Anlaşması
GSMH	Gayrı Safi Milli Hasıla
HTML	Hypertext mark-up language

ICANN	Internet Corporation for Assigned Names and Numbers İnternet Tahsisli Sayılar ve İsimler Kurumu
ICC	International Chamber of Commerce Uluslararası Ticaret Odası
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force İnternet Mühendisliği Görev Grubu
IMF	International Monetary Fund Uluslararası Para Fonu
IP	Internet Protocol Internet Protokolü
ISDN	Integrated Services Digital Network Tümleşik Hizmetler Sayısal Şebekesi
ISO	International Standardization Organisation Uluslararası Standartlaştırma Organizasyonu
ITU	International Telecommunication Union Uluslararası Telekomünikasyon Birliği
NAFTA	Kuzey Amerika Serbest Ticaret Anlaşması North American Free Trade Agreement
OECD	Organisation for Economic Co-operation and Development Ekonomik İşbirliği ve Kalkınma Teşkilatı
PKI	Public Key Infrastructure Açık Anahtar Altyapısı
PSTN	Public Switched Telecommunications Network Devre Anahtarlamalı Kamu Telekomünikasyon Şebekesi
Reg Tp	Regulatory Authority for Telecommunications and Posts- Almanya Telekomünikasyon ve Posta Regülasyon Kurumu
RTR-GmbH	The Austrian Regulatory Authority for Telecommunications and Broadcasting Avusturya Telekomünikasyon Regülasyon Kurumu
TA	Telecommunications Authority Telekomünikasyon Regülasyon Kurumu
TCP	Transmission Control Protocol Transmisyon Kontrol Protokolü
TRIPS	Fikri Mülkiyet Haklarının Ticaretle İlgili Boyutları The Trade Related Aspects of Intellectual Property Rights
UN-CEFACT	United Nations Centre for Trade Facilitation and Electronic Business Birleşmiş Milletler İdari Ticari ve Ulaşımla İlgili Uygulama ve Usulleri Kolaylaştırma Merkezİ
UNCITRAL	United NationsCommission on International Trade Law Birleşmiş Milletler Uluslararası Ticaret Hukuku Komisyonu
UNCTAD	United Nations Conference on Trade and Development Birleşmiş Milletler Ticaret ve Kalkınma Konferansı
UNDP	United Nations Development Programme Birleşmiş Milletler Kalkınma Programı

UNESCO	United Nations Educational Scientific and Cultural Organisation Birleşmiş Milletler Eğitim Bilim ve Kültürel Kuruluşu
URL	Uniform Resource Locator
VAT	Value-Added Tax Katma Değerli Vergi
WIPO	Dünya Fıkri Mülkiyet Hakları Kuruluşu World Intellectual Property Organisation
WTO	Word Trade Organisation Dünya Ticaret Örgütü
XML	Extensible mark-up language

GİRİŞ

Elektronik 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.

Elektronik Ticaret, bilgi toplumu hizmetlerinin[1] ve malı temsil eden ticari, resmi, taşıma, sigorta ve finans belgelerinin (poliçe, bono, rehin senedi) iletişim şebekesine erişim olanağı veren veya hizmet alanlar tarafından sağlanan bilgileri tutan bir iletişim ağı yoluyla ilgili tarafa (alıcıya) iletilmesi ve ilgili tarafın semeni (mal bedelini) yine aynı elektronik ortamı kullanarak satıcıya ulaştırmasıdır.

"Ticaret" ifadesi kavramsal olarak "mal ve hizmetin satın alınması ve satılması" işlemlerini kapsamaktadır. Telekomünikasyon teknolojilerinin gelişmesiyle bu sürecin elektronik ortamda, internet üzerinden yapılması elektronik ticaret kavramını ortaya çıkarmıştır. Bu sebeple telekomünikasyon imkanlarının artırılması, elektronik ticaretin gelişiminde önemli bir role sahiptir.

Liberalizasyon[2] politikası ve telekomünikasyon hizmetlerinin dünya geneline yaygınlaştırılması işlemi 1990 ların sonlarına doğru hızlanmış olup geleneksel haberleşmeye erişimin, etkinliğin, yenilikçiliğin, geliştirilmesi ve endüstride masrafların azaltılarak ulusal sosyal projelerin geliştirilmesi

---

[1] Ekonomi ile ilgili bir faaliyet alanı oluşturduğu ölçüde, ücret karşılığı olmayan ancak çevrimiçi bilgi sunma esasına dayanan veya ticari iletişimle ilgili olan ya da araştırmacılara verilere erişim ve bu verileri alma olanağı sağlayan hizmetler

[2] Piyasaların Serbestleştirilmesi

temelindeki amaçları hızlandırmıştır. Bu geçiş süreci ülkeden ülkeye değişmekle beraber çoklukla

(i) PTT'nin doğrudan devlet kontrolünden alınarak yürütmeye yönelik ve düzenleyici fonksiyonlarının birbirinden ayrılması,

(ii) telekom operatörlerinin özelleştirilmesi ve sonunda,

(iii) pazarın liberalizasyonu ve liberalizasyonun uygulanması ve denetlenmesi amacıyla telekomünikasyon regülasyon kurumlarının kurulması sıralamasını izlemektedir. Küresel bir olay olan internet ve elektronik ticaretin doğmasıyla telekomünikasyon altyapısı, servisleri, pazar yapısı birdenbire dünya ekonomisi açısından çok önemli bir yere sahip olmuştur.

Bilgi ve iletişim teknolojilerinin giderek artan kullanımı ve internet'in gelişimi, devletlerin ve işletmelerin iç yapılanmalarında, talep edilen iş becerilerinde ve iş örgütlenmelerinde, işletmeler, ticari ortaklıklar, bireyler ve devletler arasındaki ilişkilerde çok ciddi değişikliklere yol açmıştır. Bu teknolojiler, kullanım ve uygulamalarını düzenleyen ve destekleyen ekonominin ve politikaların tamamı üzerinde büyük bir etkiye sahip olmanın yanında, bu ekonomilerin modernizasyonunda etkili olup, istihdam için yeni olanakların yaratılmasında ve yeni küresel ekonomiye dahil olunmasında katkıda bulunmaktadırlar.

Telekomünikasyon regülasyon kurumları elektronik ticaretin kaderini belirleyecek güce sahiptirler. Temel alanlarda alınan kararlar iş imkanlarının şekillenmesinde ve küresel elektronik ticarete katılan ülkelerdeki tüketiciler için özellikle önemli olacaktır. Bu bağlamda bu tezde Telekomünikasyon düzenlemeleri açısıdan elektronik ticaret beş bölümde incelenmiştir.

Bu tez çalışmasının "Elektronik Ticaret ile İlgili Trendler ve Perspektifler" konulu birinci bölümünde elektronik ticareti kuşatan teknolojik ve piyasa eğilimlerinin içeriği ve tarihçesi incelenmiştir.

İkinci bölümünde elektronik imza konusu işlenmiştir. Konuyla ilgili önemli tanımlar yapılmış, elektronik ticaretin hayata geçirilmesi için en önemli unsur olan taraflar arası iletilerde; bilginin gizliliği, bütünlüğü ve tarafların kimliklerinin doğruluğunu sağlayan sayısal imzanın dayandığı temeller, şifrelendirmeye dayalı olmayan güvenik mekanizmaları, şifrelendirmeye dayanan güvenlik mekanizmaları ve açık anahtar altyapısı (PKI) detaylıca açıklanmıştır. Ayrıca sayısal imzanın oluşumu şekil ve grafikler yardımıyla açıklanmaya çalışılmış, bunun yanında uluslararası sayısal imza politikası konuları ve teşebbüsleri incelenmiştir.

Tezin üçüncü bölümünde uluslararası elektronik ticaret politikası konuları ve teşebbüsleri, fonksiyonel kurumların elektronik ticaretle ilgili gerçekleştirmiş oldukları çalışmalar ve faaliyetlere değinilmiş ve Ülkemizde yürütülmekte olan elektronik ticaret çalışmalarının tarihçesi incelenmiş ve son durum hakkında bilgi verilmiştir.

Tezin "Telekomünikasyon Pazarı ile İlgili Regülasyonların Elektronik Ticaret Üzerindeki Etkileri" konulu dördüncü bölümünde telekomünikasyon pazarı ile ilgili;

- Altyapı,
- Evrensel hizmet ,
- Pazar yapısı, rekabet, lisanslandırma ve
- Ekonomik ve ücretlendirici regülasyon

konuları için varolan regülasyon seçenekleri ve bu seçeneklerin elektronik ticaret üzerindeki etkilerinin neler olabileceği araştırılmış ve bunlarla ilgili bazı önerilerde bulunulmuştur.

Tezin "Telekomünikasyon Kurumu'nun Elektronik Ticaret ile İlgili Uygulayacağı Politika Modeli" konulu beşinci bölümünde ise Kurumumuzun elektronik ticaret ile ilgili uygulayacağı politika modelini belirlerken ilk olarak neleri göz önünde bulundurması gerektiği üzerinde durulmuştur.

Kurumumuz için bir model oluşturması için elektronik imza konusunda lider durumunda olan ve kök sertifika hizmet sağlayıcısı olarak faaliyet gösteren Almanya, Avusturya, Finlandiya ve Danimarka telekomünikasyon regülasyon kurumlarının uyguladıkları modeller, yönetmelikleri ve sorumlulukları incelenmiş, yönetmeliklerinin tercümesi yapılmış ve Kurumumuz koordinatörlüğünde yürütülecek olan yönetmelik çalışmalarına model olması açısından "Sertifika Hizmet Sağlayıcıların Telekomünikasyon Kurumu'na Bildirimde Bulunma Yükümlülüğüne Dair Yönetmelik" ve "Nitelikli Elektronik Sertifika Hizmeti Sağlayan Sertifika Hizmet Sağlayıcılarının Güvenilirlik ve Bilgi Güvenliği Yükümlülüklerine Dair Yönetmelik" olmak üzere iki yönetmelik taslağı hazırlanmıştır. Ayrıca farklı bir örnek olması açısından İngiltere Ticaret ve Endüstri Bakanlığı (Department of Trade and Industry-(DTI) Modeli de incelenmiştir.

Sonuç ve öneriler kısmında Kurumumuzun elektronik ticareti ilgilendiren konularda kısa ve uzun vadede neler yapması gerektiğine dair durum tespiti yapılarak gerekli önerilerde bulunulmuştur.

BİRİNCİ BÖLÜM

1. ELEKTRONİK TİCARETLE İLGİLİ TRENDLER VE PERSPEKTİFLER

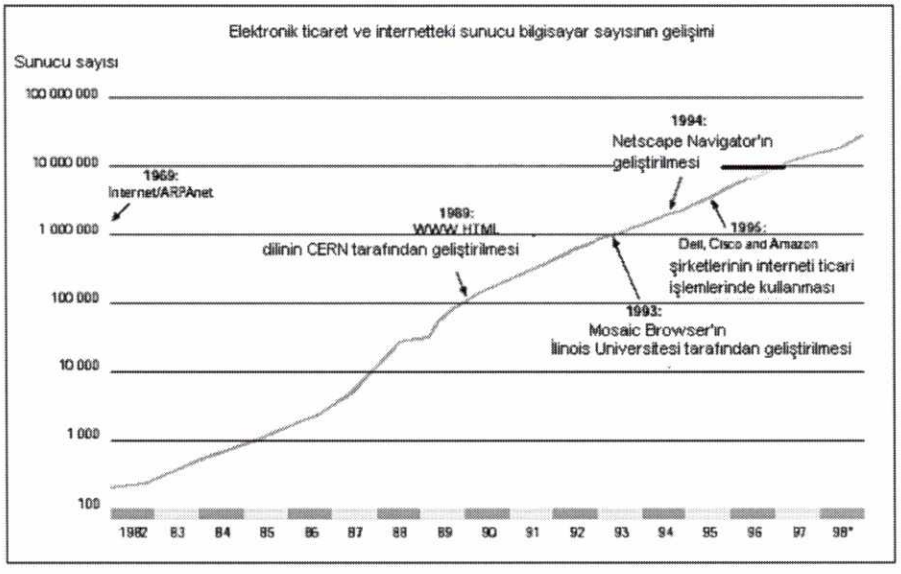
Bu bölümün amacı elektronik ticareti kuşatan teknolojik ve piyasa eğilimlerinin içeriği ve tarihçesi hakkında bilgi vermektir.

1.1 Teknoloji ve Pazar gelişmeleri: Elektronik ticaret nedir?

İnternetin doğuşu ve telekomünikasyon teknolojilerinin gelişmesiyle ortaya çıkan elektronik ticaret (e-ticaret), geleneksel ticareti kolaylaştıran bir yeniliktir [1]. Elektronik ticaret tüm endüstrileri ve uygulamaları, üreticileri ve kullanıcıları, veri alışverişini ve ekonomik faaliyetleri internet olarak adlandırılan küresel bir pazarda bir araya getirmektedir. Elektronik ticaret ödemelerin çevrimiçi yapılması, mal ve servislerin tüketicilere hem internet yoluyla hem de fiziksel olarak ulaştırılması için gerekli teknolojik ve işlemsel kapasitenin sağlanmasını gerektirmektedir. Elektronik ticaret ticari muameleleri kolaylaştırarak etkin hale getirmekte ve masrafları azaltmaktadır. Örneğin "Cisco Systems" şirketi telefon ve faks yoluyla almakta olduğu siparişleri elektronik ortam yoluyla çevrimiçi olarak almaya başladığında yarım milyar dolardan daha fazla tasarruf yapmış ve hata oranını %25'ten %2'ye düşürmüştür [2].

Şekil 1.1'den de görüleceği gibi, internet vasıtasıyla gerçekleştirilen elektronik ticaret şirketler tarafından yoğun olarak 1996 yılından itibaren kullanılmaya başlanmıştır. Bundan önceki yıllarda kapalı ağ ortamı (intranet) olarak adlandırılan şirket içi ağlar ya da şirketlerin kendi aralarında veya belirli müşteriler ile bilgi alışverişi ve ticari ilişkide bulundukları üçüncü taraflara kapalı olan ve elektronik data transferi (Electronic Data Interchange-EDI) yöntemi kullanılarak gerçekleştirilen elektronik ticaret uygulamalarından

bahsetmek mümkündür. Internet üzerinden yapılan elektronik ticaret, EDI'den farklı olarak, yalnız belirli üretici, sağlayıcı, dağıtıcılara yönelik olmayıp, internet erişimi olan her bir kullanıcıya hizmet verilebilmektedir.



Kaynak: Network Wizards [3]

Şekil 1.1 Elektronik ticaret ve internetteki sunucu sayısının gelişimi

Elektronik ticaretin gelişiminin tarihsel boyutuna baktığımızda iki önemli gelişimin belirleyici olduğunu görmekteyiz. Bunlardan birincisi, telekomünikasyon sektöründeki gelişmeler, ikincisi ise piyasaların küreselleşmesi ve liberalizasyonudur [4]. Uluslararası ticaretin ve buna paralel olarak etkin mal ve hizmet taşıma yöntemlerinin gelişmesi, ülkeler arasındaki ekonomik bağımlılığın düzeyini artırmış ve ürünlerle piyasaların küreselleşmesine yol açmıştır. Bilgi toplumuna doğru gidişin temel dinamikleri olan bu gelişmeler, sanayileşmiş ülkelerin bilgi yoğun hizmetlerle yeniden yapılanma sürecini başlatmıştır. Bu sektör, ekonomide tarım ve sanayiden daha hızlı gelişen en güçlü kesim haline gelmiştir. Elektronik ticaret ise, bilgi toplumunun uygulanmasında en önemli alanlardan biridir.

Günümüzde bilginin ve verilerin elektronik olarak değişimi uluslararası ticaretin en önemli bölümlerinden biri haline gelmiştir. Uluslararası ticareti düzenleyen geleneksel kuralların, bu gelişimi karşılayabilecek esneklikte olmadığı ve yeni düzenlemelere gerek duyulduğu kısa sürede kendini ortaya çıkarmıştır. Bu durum, ekonomik yaşamın her yönü için geçerliyken, özellikle haberleşme sektöründe çok acil düzenlemelere gerek duyulmuştur. Günümüzde, 1970'lerin başındaki ulusal düzeyde tek bir kuruluşun sunduğu haberleşme hizmetlerinden, tam liberalizasyonun hedeflendiği, rekabetin teşvik edildiği ve kullanıcı isteklerinin yönlendirdiği rekabetçi bir ortama gelinmiştir. Bilginin haberleşme ağları üzerinden gönderilmesi, alınması ve yönetilmesi, dünyanın her tarafında benzer standartların kullanıldığı, karşılanabilir maliyetlerle, ayrım gözetmeyen, evrensel erişimin sağlandığı bir düzeyin oluşturulmasını gerek kılmaktadır.

Kısaca, bilginin taşınmasındaki ana araçlarından olan telekomünikasyonun, ekonomik faaliyetlerin küreselleşmesinde çok temel bir rol oynadığı söylenebilir.

E-ticaretin gelişim sürecinin, doğal olarak, internetin gelişimine paralel olduğu gözlenmektedir. Çünkü, e-ticaret kavramı genel olarak; herkese açık elektronik ağ üzerinden gerçekleştirilen ticari faaliyetleri ifade etmektedir.

Yeni bir kavram olması dolayısıyla elektronik ticaretin değişik tanımları yapılabilmektedir. Kimilerine göre; elektronik araçlarla yapılan tüm ticari işlemler e-ticaret sayılırken, kimileri de sadece internet gibi açık ağlar üzerinde yapılan işlem ve ödemeleri e-ticaret saymaktadır.

E-ticaret temel olarak telekomünikasyon ve bilgi teknolojilerinin ulusal ve uluslararası ekonomik faaliyetler kapsamındaki uzantısı olarak, doğrudan fiziksel bağlantı kurmaya ya da fiziksel değiş tokuş işlemine gerek kalmadan, tarafların elektronik olarak iletişim kurdukları her türlü ticari iş etkinliği [5] olarak tanımlanabileceği gibi bilgi, ürün ve hizmet satın alma işlemlerinin firmaların internet üzerindeki sitelerinden gerçekleştirilmesi [6]

veya piyasadaki mallar ve hizmetlerin teslimi, satışı, dağıtımı ve üretimini kapsayan işlemleri kolaylaştırmak için bilgisayar ağlarını kullanmak [7] ya da iki veya daha fazla taraf arasında mal ve hizmet değişimini içeren işlemlerin elektronik araçlarla ve tekniklerle yapılması [8] olarak da tanımlanabilmektedir.

Uluslararası organizasyonlar ile bu alanda faaliyet gösteren bazı uluslararası kuruluşların e-ticarete ilişkin tanımlarından bazıları aşağıda belirtilmiştir.

Dünya Ticaret Örgütü'nün (Word Trade Organisation-WTO) tanımına göre; E-ticaret, mal ve hizmetlerin üretim, reklam, satış ve dağıtımlarının telekomünikasyon ağları üzerinden yapılmasıdır [9].

Ekonomik İşbirliği ve Kalkınma Teşkilatı'nın (Organisation for Economic Co-operation and Development-OECD) tanımına göre kurumların ve bireylerin katıldığı ve metin, ses, görsel imaj gibi sayısallaştırılmış verinin işlenerek, açık veya kapalı ağlar üzerinden iletilmesine dayanan ticaretle ilgili işlemlere elektronik ticaret denilmektedir [10] .

Elektronik ticaretin yasal çerçevesinin çizilmesi için önemli çalışmalar yapan BM- Uluslararası Ticaret Hukuku Komisyonu'nun (United Nations Commission on International Trade Law-UNCITRAL) 1996 yılında hazırladığı Model Yasa'ya göre, ticari aktiviteler kapsamında her türlü veri mesajının, elektronik veri değişimi, internet, e-posta gibi gelişmiş yöntemlerin yanında, telekopi ve fax gibi daha az karmaşık yöntemler kullanılarak elektronik ortamda değişimi elektronik ticaret olarak tanımlamıştır [11].

Avustralya'nın hazırladığı bir çalışmada elektronik ticaret, elektronik yöntemler kullanılarak açık veya kapalı ağlar üzerinden ticaret veya ticaretle ilgili her türlü bilginin bilgisayarlar arasında iletilmesi olarak tanımlanmıştır [12].

ABD'nin Washington Eyaleti'nce hazırlanan "Stratejik Bilgi Teknolojisi Planı"nda ise, işle ilgili bilginin iki veya daha çok kuruluşun bilgisayarları arasında elektronik olarak değişimi olarak tanımlanmıştır [9].

Birleşmiş Milletler İdari Ticari ve Ulaşımla İlgili Uygulama ve Usulleri Kolaylaştırma Merkezi'ne (United Nations Centre for Trade Facilitation and Electronic Business, UN-CEFACT) göre e-ticaret; iş, yönetim, ve tüketim faaliyetlerinin yürütülmesi için, yapılanmış (structured) ve yapılanmamış (unstructured) iş bilgilerinin; üreticiler, tüketiciler ve kamu kurumları ve diğer organizasyonlar arasında elektronik araçlar (Elektronik posta ve mesajlar, elektronik bülten panoları), www (word wide web) teknolojisi, akıllı kartlar, elektronik fon transferi, elektronik veri değişimi üzerinde paylaşılmasıdır [14] şeklinde tanımlanmıştır.

Avrupa Komisyonunun 1997 yılında yapmış olduğu tanıma göre; e-ticaret, işletme faaliyetlerinin elektronik olarak yapılmasıdır. Bu faaliyet metin, ses ve video verilerinin elektronik olarak işlenmesi ve aktarımına dayanmaktadır. E-ticaret bu boyutuyla mal hizmet alımı ödemelerinin dijital olarak yapılmasını kapsamaktadır. Bu faaliyetler hem mamulleri (tüketici malları, spesifik ekipmanları) ve hizmetleri (bilgi hizmeti, finansal ve yasal hizmetler) hem de geleneksel faaliyetleri (sağlık, bakım, eğitim) kapsamaktadır [9] .

Elektronik Ticaret Koordinasyon Kurulunun (ETKK), Mayıs 1998 tarihli Hukuk Çalışma Grubu raporunda ise, e-ticaret; bireyler ve kurumların, açık ağ ortamında (İnternet) ya da sınırlı sayıda kullanıcı tarafından ulaşılabilen kapalı ağ ortamlarında (intranet) yazı, ses ve görüntü şeklindeki sayısal bilgilerin işlenmesi, iletilmesi ve saklanması temeline dayanan ve bir değer yaratmayı amaçlayan ticari işlemlerinin 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 [15].

1.1.1 Tarihi Gelişim

Haberleşme şebekelerinin ve bilgisayarların iş dünyası ve tüketiciler tarafından kullanımı ve mali işlemlerle ilgili uygulamalar yaklaşık 20 yıldır yoğunluk kazanmıştır. Tüzel ve mali seviyelerdeki işlemlerde elektronik fon transferi (EFT) metodu kullanılmaktadır. Para taransferi hizmetlerini kendi iç şebekeleri yoluyla gerçekleştirmekte olan bankamatikler 1970'li yılların ortalarından bu yana bankacılık sektöründe kullanılmaktadır.

Tüketiciye yönelimli elektronik ticaret yeni değildir. Buna örnek olarak 1980'lerin ortalarına doğru ABD'de kablolu televizyonun gelişimi ile tüketiciye yönelik ürünlerin pazarlamasının yapıldığı kablolu alışveriş kanallarının sayılarının hızla artması bir örnek olarak verilebilir.

1.1.2 İnternet ve Web

Internet, dünya kapsamında birçok bilgisayar sistemini Transmisyon Kontrol Protokolü/ İnternet Protokolü (Transmission Control Protocol/Internet Protocol-TCP/IP) ile birbirine bağlayan ve gittikçe büyüyen bir iletişim ağıdır. TCP/IP, bilgisayarlar ile veri iletme/alma birimleri arasında organizasyonu sağlayan, böylece bir yerden diğerine veri iletişimini olanaklı kılan pek çok veri iletişim protokolüne verilen genel addır.

İnternet'in ortaya çıkışı Amerikan Federal Hükümeti Savunma Bakanlığı'nın araştırma ve geliştirme kolu olan Savunma İleri Düzey Araştırma Projeleri Kurumu (Defense Advanced Research Projects Agency- DARPA) vasıtasıyla olmuştur. 1969'da çeşitli bilgisayar bilimleri ve askeri araştırma projelerini desteklemek için Savunma Bakanlığı ARPANET (Advanced Research Projects Agency Network) adındaki paket anahtarlamalı ağı oluşturmaya başlamış bu ağ, ABD'deki üniversite ve araştırma kuruluşlarının değişik tipteki bilgisayarlarını da içererek büyümüştür [16].

1973 yılında, ağ için bir protokol seti geliştirmek amacıyla Stanford Üniversitesi'nde bir proje başlatılmıştır. 1978'e kadar transmisyon kontrol protokolünün dört uyarlaması geliştirilip ve denenmiştir. 1980'de bu küme sabitleşmiş ve ARPANET'e bağlı bilgisayarlar arasındaki iletişimi kolaylaştırmıştır. 1983'te tüm ARPANET kullanıcıları TCP/IP olarak bilinen yeni protokole geçiş yapmışlar ve aynı yıl TCP/IP, ARPANET'i de içerecek şekilde Savunma Bakanlığı internetinde kullanılmak üzere standartlaştırılmıştır. ARPANET 1990 Haziranında kullanımdan kaldırılmış ve yerini ABD, Avrupa, Japonya ve Pasifik ülkelerinde ticari ve hükümet işletimindeki omurgalar (backbone) almıştır. ARPANET'in kaldırılmasına rağmen, TCP/IP protokolünün kullanılmasına devam edilip geliştirilmiştir.

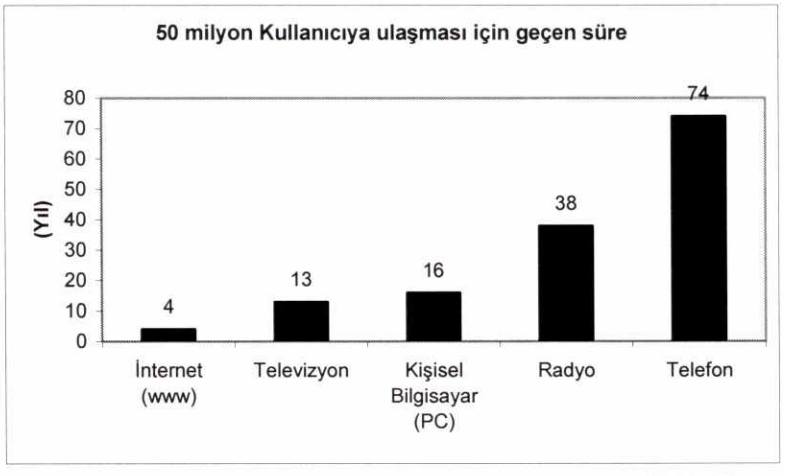
1991 yılında Minnesota Üniversitesi tarafından, Internet kaynaklarına erişimde büyük kolaylık sağlayan GOPHER kullanıma girmiştir. Gopher, internet içinde çeşitli konularda arama yapmayı sağlayan bir sunucu (client) programıdır. Sağladığı en önemli avantaj, internet kaynaklarını menüler halinde sunması ve kullanıcının arzu ettiği kaynak menüden seçilince, bu kaynağın internet adresi bilmeksizin de o kaynağa erişme imkanını sağlamasıdır.

1992 yılında ABD kaynaklı bir şirket olan CERN tarafından, World Wide Web (www) geliştirilmiştir. WWW, hypertext teknolojisini kullanarak Internet kaynaklarına erişimi sağlayan başka bir olanaktır [17].

1994 yılında, Web üzerinde işlem yapmayı sağlayan Mosaic yazılımı piyasaya sürülmüş ve kullanım kolaylığı nedeniyle çok yaygınlaşmıştır. Ayrıca Amazon.com'da ilk kitap satılmış, e-mail yoluyla pazarlama ve reklam keşfedilmiştir.

1995 yılında ise Web üzerinde işlem yapan Netscape yazılımı kullanılır hale gelmiş, Yahoo'da ilk arama yapılmış, e-Bay'da ilk sanal müzayede düzenlenmiştir [18].

İnternet erişimi internete bağlı bilgisayar sayısı (host computers) ya da bu bilgisayarları kullanarak internete bağlanan kişi sayısı vasıtasıyla ölçülebilir. 1990'lara kadar askeri ve akademik çevrelerin kullandığı internet günümüzde küresel olarak yaygınlaşmış ve oldukça ticari bir hale gelmiştir. İnternet diğer haberleşme araçları içerisinde en hızlı şekilde dünya genelinde yayılmış olanıdır. Şekil 1.2 'den de görülebileceği gibi telefonun 50 milyon kullanıcıya ulaşması 70 yıl, radyonun 38 yıl, kişisel bilgisayarların 16 yıl televizyonun 13 yıl almışken internetin sözkonusu kullanıcı sayısına ulaşması sadece 4 yıl almıştır [19].



Kaynak:ITU [19]

Şekil 1.2 Bazı telekomünikasyon hizmetlerinin 50 milyon kullanıcıya ulaşması için geçen süre

ITU[1] verilerine göre dünya genelindeki internet kullanıcı sayısı 2000 yılı sonunda 385 milyon civarında iken 2001 yılı sonunda % 30 artarak 500 milyon civarına yükselmiştir. ITU 2002 sonu için bu sayının 665 milyon civarında olacağını hesaplamıştır. Bu ise bir önceki yıla oranla % 31'lik bir artışa karşılık gelmektedir. Diğer bir ifadeyle dünya nüfusunun % 2.5'luk bir kısmı ya da Rusya Federasyonu'nun nüfusuna eşdeğer olan yaklaşık 150 milyon kişi her yıl internet kullanıcıları arasına katılmaktadır. Çizelge 1.1'de 2001 ve 2002 yılı için dünya genelindeki internet kullanıcı sayısı

[1] Uluslararası Telekomünikasyon Birliği (International Telecommunications Union)

istatistikleri verilmektedir [20]. Çizelge 1.2'de ise 2001 ve 2002 yılları için bölgelere göre internet kullanıcı sayıları ve yıllık değişimleri görülmektedir.

Çizelge 1.1 2001 ve 2002 yılı dünya geneli internet kullanıcı sayısı

Kaynak	2001 (Milyon)	2002 (Milyon)
ITU	500.07	655
Nielsen/NetRatings	498.20	
IDC	497.70	
Nua.com 5	527.57	580.78 (Mayıs)

Kaynak: ITU (2002) [20]

Çizelge 1.2 2000-2001 yılları arası internet kullanıcı sayıları ve yıllık değişimleri

Bölge Adı	2001 (milyon)	2000 (milyon)	Artış	% Değişim
Afrika	6.738	4.601	2.137.000	46.4
Latin Amerika/Karayipler	26.320	19.331	6.989	36.2
Kuzey Amerika	156.323	136.700	19.623	14.4
Asya	157.779	108.231	49.547	45.8
Avrupa	144.410	108.339	36.071	33.3
Okyanusya	8.505	7.635	870	11.4
Diğer Bölgeler	213	205	8	3.9
Tüm Dünya	500.074	384.837	115.237	29.9

Kaynak:ITU (2002) [20]

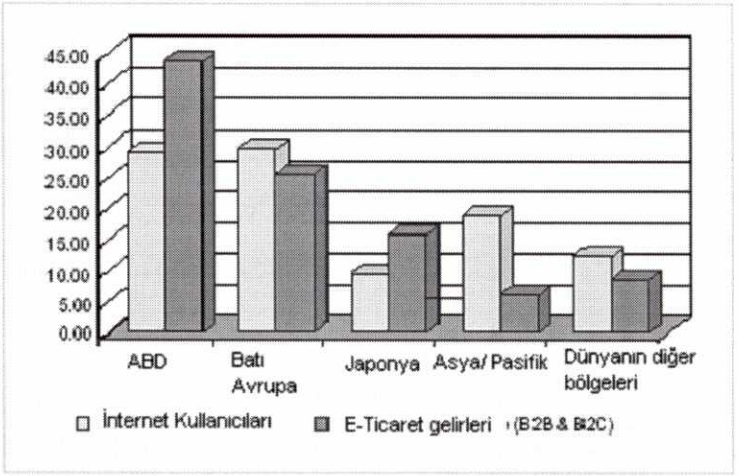
Tarihler incelendiğinde internetin Amerika'da çok hızlı yayıldığı, 1998'in ortalarında bu yayılımın Avrupa'ya geçtiği görülmektedir. Avrupa'nın altyapısı hazır olsa da biraz bekle gör politikası uygulandığı söylenilebilir. Japonya internetle ilgilenmiş ve Amerika'daki internet konusundaki yatırımların hatırı sayılır bir bölümü Japon şirketleri tarafından kendi sermayelerinden kanalize ederek gerçekleştirilmiştir. Şu anda uzak doğu ülkeleri ve ABD bu alandaki çalışmalarıyla başı çekmektedirler [21].

2001 yılında Japonya ve Kore Cumhuriyeti'nin yer aldığı Asya'ya 21 milyon yeni internet kullanıcısı eklenmiştir. Bu ise Kuzey Amerika'daki rakamdan daha yüksek bir rakamdır. ITU'nun yeni istatistiklerine göre ise Çin 56.6 milyon internet kullanıcısı ile dünyanın en büyük ikinci internet kullanıcısına sahip ülkesidir [22].

Diğer bir çalışmada 2005 yılında dünya genelinde 941.8 milyon internet kullanıcısı olacağını göstermektedir. Bu ise 2001 yılı rakamlarının yaklaşık iki katına tekabül etmekte olup en fazla kullanıcı sayısının Batı Avrupa ve Asya/Pasifik'te yoğunlaşacağı tahmin edilmektedir. İnternette görülen bu teşvik edici artışa rağmen gelişmekte olan ülkelerdeki yaygınlık oranı oldukça düşük düzeylerde seyretmektedir [23].

1.1.3 Elektronik Ticaret Aktiviteleri

Dünya geneli incelendiğinde elektronik ticaretin ülkeler arasında farklı oranlarda tercih edildiği görülmektedir. Şekil 1.3'de dünyanın bazı bölgelerindeki internet kullanıcılarının dünya genelindeki payları ve elektronik ticaretten sağlamış oldukları gelirlerin 2002 yılına ait değerleri görülmektedir.



Kaynak: IDC (2002a) [24]

Şekil 1.3 İnternet Kullanıcılarının Dünya Genelindeki Payları ve Elektronik Ticaretten Sağlamış Oldukları Gelirler

Elektronik ticaret geniş anlamda ele alındığında taraflarına göre; işletmeler arasında (Business to Business- B2B), işletme-tüketici arasında (Business to Consumer –B2C) , İşletme-Devlet ve Devlet-İşletme arasında olmak üzere dört kategoride yapıldığı tespit edilmektedir [25]

İşletmeler arasında gerçekleştirilen elektronik ticaret (B2B) elektronik ticaret aktivitelerinin yaklaşık olarak % 95'ini oluşturmaktadır [20]. Çizelge 1.3'te bazı araştırma şirketlerinin hazırlamış olduğu dünya genelinde gerçekleştirilen elektronik ticaret faaliyetlerinden elde edilmiş olan ve 2006 yılına değin elde edilecek olan gelirlerin tahmini miktarları yer almaktadır.

Çizelge 1.3 Dünya geneli E-ticaret Gelirleri ve Tahminleri (Milyar Dolar)

Şirket Adı	**2000**	**2001**	**2002**	**2003**	**2004**	**2005**	**2006**	**Bileşik Büyüme hızı**
Forrester			2.293,50	3.878,80	6.201,10	9.240,60	12.837,30	% 53.81
IDC	354,90	615,30				4.600,00		%66.93
eMarketer	278,19	474,32	823.48	1.408,57	2.367,47			% 70.80

Kaynaklar: eMarketer (2002a), Forrester (2001), IDC (2002a) ve UNCTAD hesaplamaları [20]

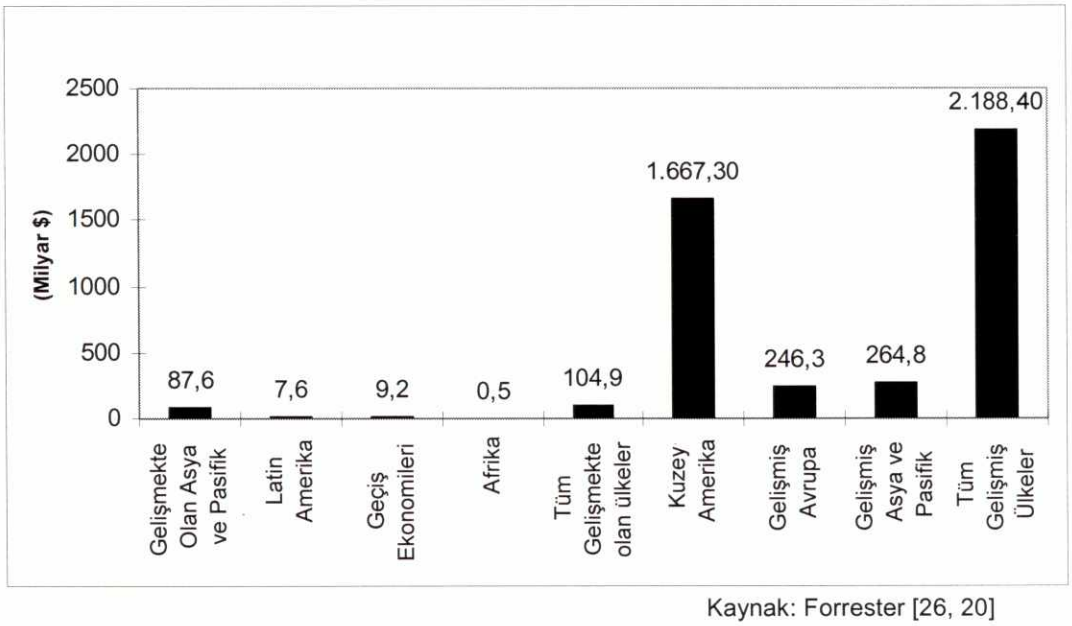
Çizelge 1.3'te yer alan verilerin daha iyi değerlendirilmesini sağlamak için 2001 yılında dünya genelindeki tüm ticari mal ve servislerin ihracatından elde edilen gelir miktarının 7.43 trilyon $ olduğunu [25] vurgulamak yerinde olacaktır. Başka bir ifadeyle 2006 yılında e-ticaret satışlarının hacmi küresel seviyedeki satışların %18'ini oluşturacaktır.

Çizelge 1.4'te ise dünya genelindeki bazı bölgelerde işletmeler arası (B2B) ve işletme-tüketiciler arası (B2C) toplam e-ticaret uygulamalarından elde edilmiş olan ve 2006 yılına değin elde edilecek olan gelirlerin tahmini miktarları yer almaktadır. Çizelge 1.4'teki verilerin daha iyi anlaşılmasını sağlamak için sözkonusu verilerin grafiksel gösterimleri Şekil 1.3, Şekil 1.4, Şekil 1.5 ve Şekil 1.6'da yer almaktadır.

Çizelge 1.4 Bölgesel E-ticaret (B2B ve B2C) Değerleri ve Tahminleri

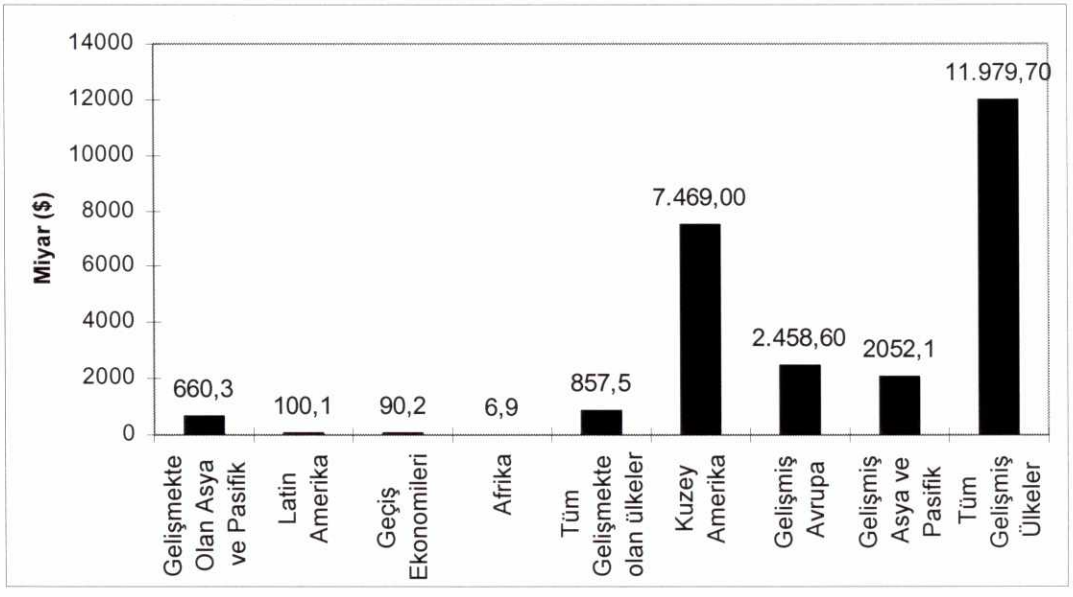
Bölge Adı	2002 (Milyar $)	Dünya genelindeki yüzdesi (%)	2006 (Milyar $)	Dünya genelindeki yüzdesi (%)	2002-2006 arasındaki artış yüzdesi (%)
Gelişmekte olan Asya ve Pasifik	87,6	3,8	660,3	5,1	65,7
Latin Amerika	7,6	0,3	100,1	0,8	90,5
Geçiş Ekonomileri	9,2	0,4	90,2	0,7	77,7
Afrika	0,5	0,0	6,9	0,1	91,1
Tüm gelişmekte olan ülkeler	104,9	4,6	857,5	6,7	69,1
Kuzey Amerika	1.667,3	73,1	7.469,0	58,2	45,3
Gelişmiş Avrupa	246,3	10,7	2.458,6	19,2	77,7
Gelişmiş Asya ve Pasifik	264,8	11,5	2.052.1	16,0	66,8
Tüm Gelişmiş Ülkeler	2.188,4	95,4	11.979,7	93,3	53,0
Dünya Geneli	2.293,5		12.837,3		53,8

Kaynak: Forrester [26, 20]



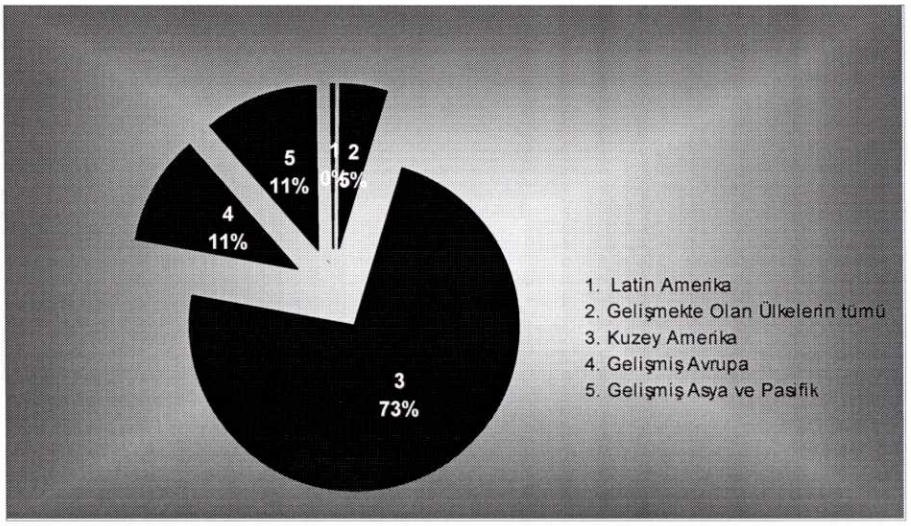
Kaynak: Forrester [26, 20]

Şekil 1.4 2002 Yılı Bölgesel E-Ticaret Gelirleri



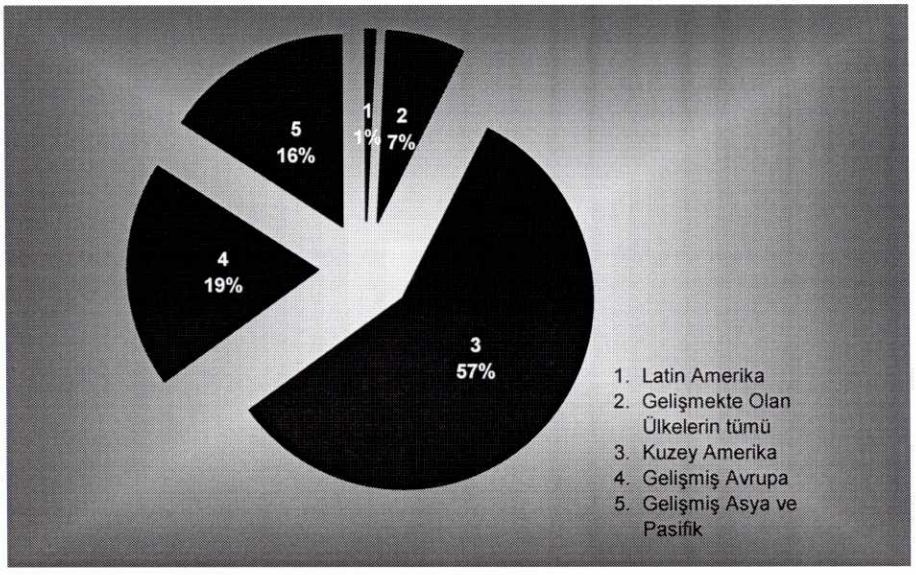
Kaynak: Forrester [26, 20]

Şekil 1.5 2006 Yılı Bölgesel E-Ticaret Gelir Tahminleri



Kaynak: Forrester [26, 20]

Şekil 1.6 Önemli Bölgelerin 2002 Yılında E-Ticaret Gelirlerinden aldığı yüzdelik pay



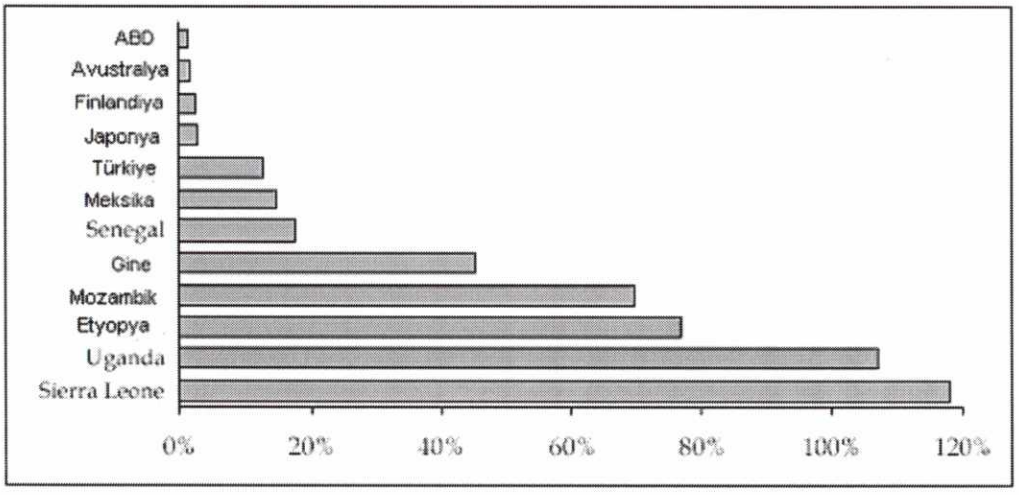
Kaynak: Forrester [26, 20]

Şekil 1.7 Önemli Bölgelerin 2006 Yılı için E-Ticaret Gelirlerinden alması muhtemel yüzdelik pay

Ülkelerin elektronik ticaretten aldıkları pay, şüphesiz bu alana yaptıkları yatırımlarla paralel olarak gelişme göstermektedir. Çizelge 1.4 incelendiğinde 2006 yılında gelişmekte olan ülkelerin dünya genelindeki elektronik ticaretten elde edecekleri payın yaklaşık olarak % 6.7 olacağı görülmektedir. Bu payın % 5.1'lik kısmını Asya-Pasifik bölgesindeki gelişmekte ülkelerin alacağı ve diğer gelişmekte olan ülkelerin payının ise %1'in altına düştüğü tablodan görülmektedir. Ayrıca gelişmiş ülkelerin % 95.4 olan 2002 yılı payının 2006 yılında %93.3'e gerileyeceği de gözlemlenen diğer bir husustur.

Elektronik ticaretin gelişmesi sağlayan hususların başında internete erişim maliyetlerinin ucuz ve web sitesi sayısının fazla olması gelmektedir.

En düşük erişim maliyetlerine sahip ülkeler arasında ABD ön sıralardadır. Bu durum, Şekil 1.8'ten kolaylıkla görülebilir.



Kaynak: ITU, 1999 [19]

Şekil 1.8 Aylık internet bağlantı ücretlerinin GSMH'nın yüzdesi olarak ifadesi

1.2 Gelişmekte olan ülkelerle ilgili hususlar

Gerçek ve potansiyel faydalarına karşın, gelişmekte olan dünyada elektronik ticaretin geniş ölçekli yayılımını engelleyen bazı etkenler bulunmaktadır. Gerçekte gelişmekte olan ülkelerde teknolojilere, altyapı, pazar yapılarına eşit erişim sağlanmadığı takdirde, elektronik ticaretin zengin ve fakir ülkeler arasındaki ayırımları arttıran bir etkisi vardır. Bir bakıma, elektronik ticaretin getirileri tam olarak tanımlanmamış ve anlaşılamamış olsa bile gelişmekte olan ekonomilerin gelişimlerini gelişmekte olan ülkelere nazaran arttırması için şu an için azda olsa bir fırsat bulunmaktadır [26].

İnternetin Amerika'da doğmuş olmasından ve elektronik ticarette başlangıçta gelişmekte olan ülkelerde başlamış olmasından dolayı az gelişmiş ülkeler halihazırda kendilerini bu prosedürden hem endüstriyel hemde politik seviyede dışlanmış hissetmektedirler. Gelişmiş ekonomilerin avantajları açıktır: yerleşmiş bir altyapıları vardır ve teknik altyapıya ve yatırım sermayesine gelişmekte olan ülkelerden daha fazla sahiptirler.

Bununla beraber, OECD ülkelerindeki genel açık piyasa politikaları, düzenlenmemiş ticaret ve müteşebbislerin yer aldığı, tekellerin, ticaret ve rekabette kısıtlamaların sürdüğü gelişmekte olan ülkelere nazaran tercih edilebilirdir [27].

Bu eşitsizlikleri yenmek için az gelişmiş ülkeler aşağıda belirtilen bazı yöntemlere başvurabilirler. Bunlardan bazıları ülke içerisinde bazıları ise uluslararası işbirliği ve yardımlar yoluyla fayda sağlayabilir.

- Günümüzde çoğu gelişmekte olan ülkedeki nüfusun oldukça az bir kesiminin sahip olduğu bilgisayar ekipmanı ve yazılımının elde edilmesini kolaylaştırıcı tedbirlerin alınmasının yanında telekomünikasyon altyapısı servislerine herkesin erişiminin sağlanması

- Pazarın serbestleştirilmesi ve iç ticaret engellerinin azaltılması

- Altyapı sermayesine kısıtlı erişimin arttırılması

- İş yönetimi ve teknoloji ile ilgili eğitim ve öğretimin sağlanması

- Riskleri azaltmak ve yatırım imkanlarını sağlamak amacıyla ekonomik, yasal ve politik kurumlarda istikrar, açıklık ve bütünlüğün sağlanması

Elektronik ticaretin gelişimi yeterli bilgi teknolojisi altyapısının bulunmasına bağlıdır. Gelişmiş ekonomilerde bu kurum oluşturulmuştur. Örneğin OECD, elektronik ticaretteki yasal ve teknik anlamdaki engellerin kaldırılması yönünde kısmen yardımcı olabilmektedir [28] .

1.2.1 Elektronik Ticaretin Faydaları

Elektronik ticaretin gelişmekte olan ekonomilere gelişim ivmesinin artması ve ekonomik transformasyonun gerçekleştirilmesine yönelik sunduğu fırsatlar pek çoktur. Eğer stratejik ve yaratıcı bir şekilde uygulanacak olunursa e-ticaret teknolojileri teorik olarak iç ticarette küçük ve büyük teknolojiler arasında çok seviyeden oluşan bir alan yaratır ve etkin maliyetli[1] (cost effective) ve geniş iç iş olasılıkları sağlar. Gelişmekte olan ekonomiler için muhtemel avantajlar şöyle sıralanabilir [29]:

- Topluluğun geniş kesimlerinin ekonomiyle bütünleşmesine imkan sağladığı için yoksulluğun azaltılması, uzaktan öğretim, doğrudan ticari faaliyetlerle ve tele-sağlık ve elektronik demokrasi gibi uygulamalar vasıtasıyla gelişmenin arttırılmasına imkan sağlaması

- Ulusal ve uluslararası farkındalığın[2] (awareness) arttırılmasının ve yerli ürünlerin ve servislerin dağıtımı yönlerinden pazarlama ve satış masraflarını azaltması

- Ticaret dengesizliklerinin eşitlenmesini sağlayıcı etkisi

- Hükümet ve tüketici faaliyetleri dahil ticaretin çoğu rutin ve gerekli unsurlarını elektronik yolları hızlandırılarak büyük ve küçük işletmeler arasındaki fırsatların eşitlenmesini sağlaması

Kısa ve öz olarak, etkin ve rekabetçi bir pazar; bilgiye erişim ve düşük işlem ve giriş masrafından oluşan iki temel faktörün fonksiyonudur.

---

[1] Maliyet Etkinliği Analizi: En iyi fayda ve maliyet oranının araştırılması, amaca ulaşmanın en düşük maliyetli yönteminin veya belirli maliyet karşılığında en yüksek değer yaratacak yolun bulunması

[2] İthal edilen bir malın bedeli+ulaşım giderleri üretilen malın fiyatına eşitse yerli üretime devam edilebilir (vergiler hariç, sanayi mallarında gümrük vergileri zaten sıfırdır). İçerdeki malın bedeli 100 kabul edilecek olursa; dışarıdaki malın bedeli+taşıma gideri 90 ise %10'luk bir fark var demektir. İthal etmek karlı olur, devam edilebilirdir, ancak %100 aşılırsa yerli üreticinin başka alanlarda üretime geçmesi daha caziptir.

Elektronik ticaret içeriğinde bu iki unsuru da barındırmaktadır. Bu bağlamda küresel ekonomide iş yapmak tüm pazarlarda çok etkili ve kapsamlıdır. Büyük ve gelişmiş ekonomilere nazaran gelişmekte olan ülkeler için sabit pazar dezavantajları oldukça azaltılabilir.

Gelişmekte olan ülkelerdeki hükümetler ve özel sektör bu faydaların avantajlarından yaralanabilmek, gelişmekte olan çevrimiçi servislerin şebeke ağı içinde yer almak, bilgi, pazarlama ve satış imkanları ve için gerekli adımları atmaya başlamışlardır. Küçük ülkelerde bile hükümete ait web siteleri, ulusal yatırımı teşvik eden, turizm, halkla ilişkiler, ulusal ticaret ve organizasyonlara erişimi sağlayan linkler bulunmaktadır.

Kamu sektörünün teşvikinin ötesinde, Amerika ve gelişmekte olan ülkelere kıyasla daha az olmakla birlikte, gelişmekte olan ülkelerdeki çevrimiçi bağımsız perakendeci ve servis sağlayıcı sayısı artmaktadır. Ayrıca, iç ve dış ticarette çevrimiçi iş girişimlerini destekleyici bir çok girişim bulunmaktadır. Bunun en yaygın olanı Ticaret Noktası Programı ve Küresel Ticaret Noktası Şebekesinin Birleşmiş Milletler Ticaret ve Kalkınma Konferansı'dır (United Nations Conference on Trade and Development-UNCTAD).

Ayrıca Uluslararası Telekomünikasyon Birliği (ITU) gelişmekte olan ülkelerdeki tüketici yönelimli elektronik ticaret projelerini destekleyen kendi pilot programını uygulamaya koymuştur. ITU Gelişmekte olan Ülkeler Elektronik Ticaret programı (EC-DC) projesi küçük ölçekli işletmelerin tüketici ürünlerinin satışıyla ilgili web tabanlı pazarlama içi uygulanacak olan pilot projelerin kurulmasına yardımı amaçlamaktadır. Başlangıç projesi küçük kobileri birbirine bağlayan Afrika pazarlama yönteminin geliştirilmesini içermektedir.

İKİNCİ BÖLÜM

2. ELEKTRONİK İMZA

2.1 Elektronik İmza

Elektronik veriler kağıt dokümanlardan farklı olarak kişisel olarak imzalanamazlar. Bunun için elektronik imza adı verilen yeni bir araç gerekmektedir. Elektronik imza pratik terim olarak bir imza değildir ancak elektronik veriyi herhangi bir değişime karşı koruyan bir elektronik mühür olarak kabul edilebilir. Bu bölümde elektronik imza ve sayısal imza kavramı, sayısal imzanın dayanmış olduğu teknik temeller, yasal modeller ve sertifika konuları incelenecektir.

Elektronik 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 oluşmuş bir seti ifade eder. Bu tanımda kullanılan "bilgi" sözcüğü, herhangi bir elektronik ortamda (elektronik, optik veya bunlarla sınırlı olmamak üzere, elektronik data transferi=EDI, elektronik posta, telgraf, teleks veya telekopi de dahil olmak üzere benzer her türlü araçla) yaratılan, iletilen ya da depolanan ve daha sonra yeniden kullanılabilir şekilde geri çağırılabilen her türlü bilgiyi içermektedir [28].

Elektronik imza, imza sahibinin adı ya da rolü altında işlem gören red edilmeyen güvenlik politikası altındaki bazı eylem ve olayların sayısal formdaki kanıtı olarak kabul edilebilir.

Bu tanım dört ana unsuru adreslemektedir [30]:

- inkar edilmeme politikası

- imza sahibi tarafından tanınan eylemin ya da olayın türü

- imza sahibinin rolü

- hepsinin ötesinde bu tanımanın zamanı

1) İnkar edilmeme politikası olmayınca elektronik imza işlem göremez. Bu bağlamda red edilmeme güvenlik politikasını tanımlayan bir arabulucu belirlenmelidir. Daha sonra ise güvenlik politikasıyla uyumlu olarak kullanımına izin verilen mekanizmalar tanımlanmalıdır. Bir sonraki adım elektronik imzanın geçerli olacağı ya da olmayacağı gibi çoğunluğu mekanizmaya bağımlı olan şartların belirlenmesidir.

2) İmza sahibi tarafından kabul edilen eylemler ya da olaylar

Eylemler ve olayların çeşitleri sınırsızdır. Aynı güvenlik politikası altında farklı çeşit olaylar ya da eylemler tanınabilir. Bunlar net olarak tanımlanmalıdır.

3) İmza sahibinin ismi ve/veya rolü bir şirketin elemanı imza sahibi olarak bir anlaşmayı imzaladığında kendi isminden daha fazla önem kazanır. Bir birey bir dokümanı imzaladığı zaman temel konu bu kişinin kolaylıkla tanınabilecek şekilde açık bir şekilde tanınmasıdır.

4) Tanınmanın yapıldığı zaman

İmza zamanının güvenlikli olarak bilinmediği durumda gizli imza anahtarı bilgisi fesh edilmiş ise herhangi bir anlaşmanın çözümü imkansızdır.

Hangi teknolojik yöntemle uygulanırsa uygulansın, elektronik imza, elektronik mesajı gönderen kişinin kimliğini belirleme, göndericinin sözleşme ile bağlanma iradesini ortaya koyma ve imzalanan mesajın bütünlüğünü güvenlik altına alma fonksiyonlarını üstlenir [31].

2.2 Sayısal İmza:

Sayısal imza elektronik imzanın özel bir çeşidi olup, asimetrik şifreleme adı verilen teknik kullanılarak yaratılan bir anahtar çifti (açık ve gizli anahtarlar) ile elektronik ortamda iletilen veriye vurulan bir mühür olarak tanımlanabilir [32].

Sayısal imzanın işlevi; elektronik ortamda aslından ayrılamayan sahte imzayı ve orijinal dokümanların değiştirilmesini önlemektir. Sayısal imzada amaç ise; elle imza atma işlemini elektronik ortamda yapabilmek için zemin yaratmaktır[28].

Elektronik ortamda yaratılan kimlik bilgisi olarak tanımlayabileceğimiz elektronik imza ve sayısal imza terimleri birbirlerinin yerine geçer şekilde kullanılmaktadır [30]. Ancak, elektronik imza her türlü elektronik ses, sembol veya uygulamayı kapsayan ve kullanılan teknolojiden bağımsız bir terim olduğundan bir üst kavram olarak kabul edilebilir.

2.3 Sayısal İmzanın Dayandığı Teknik Temeller

Sayısal imza asimetrik şifreleme tekniğine dayalı olduğundan sayısal imzanın oturduğu teknik temellere güvenlik mekanizmaları kavramından başlayarak değinmek yerinde olacaktır.

2.3.1.Güvenlik Hizmetleri

Güvenlik hizmetlerinde sağlanması gereken dört önemli özellik aşağıda sıralanmıştır [33]:

- Veri Bütünlüğü: Verinin izinsiz ya da yanlışlıkla değişimi, silinmesi, eklenmesinin önlenmesi konularıyla ilgilenmektedir. Veri bütünlüğünün sağlanması için sistem izinsiz veri değişimini belirlemek zorundadır.
- Gizlilik: Hassas verilerinin içeriğinin görüntülenmesinin sadece veriyi görüntülemeye izin verilen şahısların erişimiyle kısıtlanmasıdır.

- Kimlik doğrulama ve onaylama: Mesajın ve mesaj sahibinin iletiminin geçerliliğini sağlamaktadır.

- İnkar edilememezlik: Bireylerin önceden gerçekleştirdikleri eylemleri inkar etmelerini önlemektedir.

Güvenlik mekanizmalarının daha iyi anlaşılmasını sağlamak üzere örnek olarak Ayşe Umut ve Veli seçilmiştir. Ayşe ve Umut güvenlikli bir şekilde haberleşmek isterken Veli'nin Ayşe ve Umut'un kullandığı güvenlik servisine müdahale etmek istediği varsayılmış ve sonraki bölümlerde anlatılacak olan güvenlik mekanizmalarında bu senaryo örneği kullanılmıştır.

2.3.1.1 Şifrelemesiz (Non Cryptografic) Güvenlik Mekanizmaları

Yukarıda belirtilen güvenlik hizmetleri şifreleme (kriptografi) kullanılmadan gerçekleştirmektedir. Şifrelemesiz güvenlik mekanizmaları arasında eşlik bitleri, sayısallaştırılmış imza, kişisel kimlik numaraları (PINs) ve parolalar ve biyometrik yöntemler bulunmaktadır. Çizelge 2.1'de şifrelemesiz güvenlik mekanizmalarının bazı özellikleri verilmektedir.

Çizelge 2.1 Şifrelemesiz (Non Cryptografic) Güvenlik Mekanizmaları

Mekanizma	Veri Bütünlüğü	Güvenilirlik	Kimlik ve kimlik doğrulaması	İnkar edilememezlik
Eşlik Bitleri	Mevcut	Yok	Yok	Yok
Sayısallaştırılmış imza	Mevcut	Yok	Yok	Yok
Kişisel Kimlik Numaraları (PINs) ve Parolalar	Yok	Yok	Mevcut	Yok
Biyometrik Yöntemler	Yok	Yok	Mevcut	Yok

Kaynak NIST [34]

2.3.1.1.1 Eşlik Bitleri

En basit güvenlik mekanizmaları bilgisayarlar ve terminaller gibi cihazlar tarafından iletilen verinin bütünlüğünü sağlamak üzere tasarlanmıştır. Cihazlar telefon hattı gibi gürültülü bir kanaldan haberleşme sağladığında verilerin değiştirilebilme ihtimali bulunur. Bunu önlemek üzere sistemler her veri bayt'ı için eşlik biti adı verilen ekstra bit iletirler. Eğer eşlik bitinin sayısı yanlışsa verinin değiştirilmiş olduğu ortaya çıkar ve bu mekanizma daha çok modem bağlantılarında kullanılır. Eşlik bitleri mesajların boyutunu en az %12.5 arttırması dolayısıyla veri bütünlüğünün korunmasında kullanılan oldukça pahalı bir yöntemdir.

2.3.1.1.2 Sayısallaştırılmış İmza

Kağıt dokümantasyonun kullanıldığı iş dünyasında inkar edilememezliğin kanıt mekanizması elle atılan imzadır. Bu imza imzalayanın kağıt dokümanı yazıp onayladığını ve içeriğinden haberdar olduğu anlamına gelir. Bu yöntem alıcının dokümanı görüntülediğinde imzayı tanıması prensibine dayanmaktadır.

Sayısallaştırılmış imza elle atılmış olan imzanın tarayıcıdan taratılarak kullanılmasıdır. Bir kişi bir elektronik dokümanı imzalamak istediğinde yalnızca imzanın suretini uygun yere yerleştirir. Çok kolay uygulanabilen bir metot olmasına rağmen çok kolay bozulabilecek bir yöntemdir. Ayşe Umut'un imzasını bilir kolaylıkla tanır. Ancak Veli Umut'un sayısallaştırılmış imzasını kesip kopyalayıp bir mesajın içersine yerleştirebilir. Sayısallaştırılmış imza herhangi bir güvenlik hizmetinde kullanılan itimat edilebilir bir metot değildir.

2.3.1.1.3 Kişisel Kimlik Numaraları (PINs) ve Parolalar

Kullanıcılara özel bir sisteme erişim sağlamak istediklerinde özel bir kimlik numarası ya da parola sağlanarak onları onaylamakta kullanılan eski bir yöntemdir.

Bu tip sistemler uygun şekilde idare edildiklerinde etkin olabilirler. Yalnızca parolalara dayalı doğrulama bilgisayar sistemlerinde yeterli korumayı sağlamakta sıklıkla başarısız olmaktadır. Kullanıcıların kendi parolalarını oluşturmaları istendiğinde birçoğu hatırlanması kolay olanları seçtiklerinden dolayı bunların tahmin edilmeleri de kolay olmaktadır. Parolalar karışık karakter kombinasyonları kullanılarak yapıldıysa kullanıcıların çoğu bunu kağıda yazarlar. Bu olayda bir güvenlik sorunu oluşturabilir.

PIN ve parolalar inkar edilememezlik, gizlilik ve veri bütünlüğünü sağlayamazlar. Ayşe parolasını kullanarak Umut'u onaylamak istediğinde Umut'unda parolayı bilmesi gereklidir. Ayşe ve Umut'un ikiside parolayı bildiğinden hangisinin sözkonusu uygulamayı gerçekleştirdiğini belirlemek zordur.

2.3.1.1.4 Biyometrik Yöntemler

Biyometrik onaylama, sistem kullanıcılarının benzersiz fiziksel özelliklerini kullanarak kimliklerini tanımlamaya dayanır. Ortak biyometrik özellikler arasında parmak izi, yazılı imza, ses yapısı, retina taraması ve el geometrisi gelmektedir. Biyometrik onaylama aygıtları, biyometrik özellikleri yakalayıp analiz eden donanımların çok pahalı olması dolayısıyla parolaya dayalı sistemlerden daha yüksek maliyete sahiptir. Ancak biyometrik yollar daha yüksek seviyeli bir güvenlik sağlar.

2.3.1.2 Şifrelemeye (Kriptografi) Dayalı Güvenlik Mekanizmaları

Kriptografi, güvenli veri iletimi ve saklanması amacıyla şifreleme ve şifre çözme yöntemleri geliştiren bilim dalıdır. Şifreleme işlemi, şifre anahtarı ile özgün bilginin, içerik açısından anlamsız bir sayısal veriye dönüştürülmesi olarak düşünülebilir [34].

Kriptografi uygulamalı matematiğin veri iletimi güvenliğinin sağlanmasında kullanılan bir dalı olarak ta tanımlanabilir. Şifrelemede mesajı gönderen taraf korunmasız bir bilgiyi kodlanmış bir metin halinde gönderir.

Alıcı şifrelemeyi;

a) kodlanmış metni çözmede
b) gönderenin kimliğini belirlemede
c) veri bütünlüğünü doğrulamada kullanır.

Şifrelemede kullanılan elektronik iletişimin prensiplerinin anlaşılması açısından aşağıdaki örnek verilebilir:

- Bilgisayara gelen veriler ikili sayılardan oluşmaktadır. Örneğin Ayşe ve Umut "10001110101001110001O1" şeklinde kodlanır.

- Elektronik mesajlar bilgisayarda numarasal olarak temsil edildiklerinden üzerlerinde matematiksel işlemler gerçekleştirmek mümkündür.

- Elektronik mesajlar böylelikle orijinaline eş olan alternatif gösterimlere çevrilirler.

Çoğu durumlarlarda anahtarlar kullanıcı ve alıcı tarafından şifreleme algoritmasına ek girdi olarak kullanır. Veli eğer gizli anahtarı elde ederse Ayşe ve Umut gibi davranabilir. Şifrelemeyle ilgili temel problem kimliği doğrulanmış kullanıcıların gizli anahtarlarını sanal saldırganlara açığa vurmadan elde etmektir.

Şifrelemeye dayalı güvenlik mekanizmalarının içerisinde Simetrik Anahtar Şifrelemesi, Güvenli Karma (Hash) Fonksiyon Şifrelemesi, Asimetrik (Açık Anahtar) Şifrelemesi yer almaktadır. Sözkonusu şifreleme tekniklerinin özellikleri özet halinde Çizelge 2.2'de yer almakta olup tekniklerle ilgili detaylı açıklamalar sonraki bölümlerde sunulmaktadır.

Çizelge 2.2 Şifrelemeye Dayanan Güvenlik Mekanizmaları

Mekanizma		Veri Bütünlüğü	Güvenilirlik	Kimlik ve kimlik doğrulaması	İnkar edilememezlik	Anahtar Dağıtımı
Simetrik Anahtar Şifrelemesi	Şifreleme	Yok	Mevcut	Yok	Yok	Yok
	Mesaj doğrulama kodları	Mevcut	Yok	Mevcut	Yok	Yok
	Anahtar değişimi	Yok	Yok	Yok	Yok	Mevcut
Güvenli Karma Fonksiyonlar	Mesaj Özü	Mevcut	Yok	Yok	Yok	Yok
	HMAC	Mevcut	Yok	Mevcut	Yok	Yok
Asimetrik Şifreleme	Sayısal İmzalar	Evet	Yok	Mevcut	Mevcut	Yok
	Anahtar Değişimi	Yok	Yok	Yok	Yok	Mevcut
	Anahtar Anlaşması	Yok	Yok	Mevcut	Yok	Mevcut

Kaynak NIST [34]

2.3.1.2.1 Simetrik Anahtar Şifrelemesi

Simetrik anahtar şifrelemesi paylaşımlı sır ya da anahtara bağlı olarak çalışmakta ve izole edilmiş çevrelerde iyi çalışmaktadır. Örneğimize dönecek olursak simetrik anahtar şifrelemesi Ayşe ve Umut'un aynı anahtarı paylaştıkları bir algoritma sınıfıdır. Bu algoritmalar birincil olarak gizliliği sağlamada kullanılır ya da veri bütünlüğünün onaylanması ve sınırlı inkar edilememezlik için kullanılır [35].

Simetrik şifrelemeye örnek olarak bankalardaki ATM makineleri verilebilir.

ATM kullanıldığı zaman kişisel kimlik numarası (PIN numarası) girilerek hesaba ulaşılır. Kimlik denetimini banka yapmaktadır. Kişi ve banka PIN numarasını paylaşmakta ve bu sırrın ortaya çıkardığı bilgiye güvenli bir şekilde erişim sağlanmaktadır. Simetrik şifrelemedeki içsel problem bir çeşit ölçeklemedir. Anahtar ya da paylaşılan sır gizli bir şekilde kullanılmalıdır. Genellikle bu çeşit bir güvenli dağıtım haberleşmek istediğiniz farklı insan sayısı oldukça yükseldiği zaman uygun değildir.

2.3.1.2.2 Güvenli Karma (Hash) Fonksiyon Şifrelemesi

Güvenli karma fonksiyon veri dalgasını alır ve tek yönlü bir matematik fonksiyonu kullanarak veriyi uygun boyuta indirger. Bu ise mesajın özü olarak adlandırılır ve verinin parmak izi olarak düşünülebilir. Mesajın özü herhangi bir tarafça aynı veri için tekrar üretilebilir ancak farklı bir verinin aynı mesaj özünü yaratması imkansızdır. Mesaj özü veri bütünlüğünün sağlanmasında kullanılabilir. Ayşe Umut'a bir mesaj ve onun özünü gönderirse Umut veride oluşabilecek değişimlere karşı mesaj özünü tekrar hesaplayarak verinin değişime uğrayıp uğramadığını belirler ancak bu Umut'u sanal bir saldırıdan korumaz. Veli Ayşe'nin mesajını durdurarak yeni bir mesaj ve mesaj özü gönderebilir. Güvenli karma fonksiyon karma tabanlı onaylama kodu (HMAC) kullanılarak yaratılır. Ayşe Umut'a HMAC'lı bir mesaj gönderirse Umut HMAC'ı yeniden hesaplayarak verisini herhangi bir kaynağın yarattığı değişiklere karşı korumuş olur.

2.3.1.2.3 Asimetrik (Açık Anahtar) Şifrelemesi

Diğer bir şifreleme tekniği asimetrik anahtar çifti barındırdığından dolayı açık anahtar şifrelemesi olarak adlandırılmıştır. Sayısal imzanın dayalı olduğu prensip olan asimetrik şifrelemede imzanın doğruluğu kanıtlamada kullanılan farklı bir imza oluşturulmaktadır. Her kullanıcı gizli anahtar ve açık anahtar olarak adlandırılan anahtar çifti adı da verilen iki farklı ancak tamamlayıcı bir anahtar kullanılmaktadır.

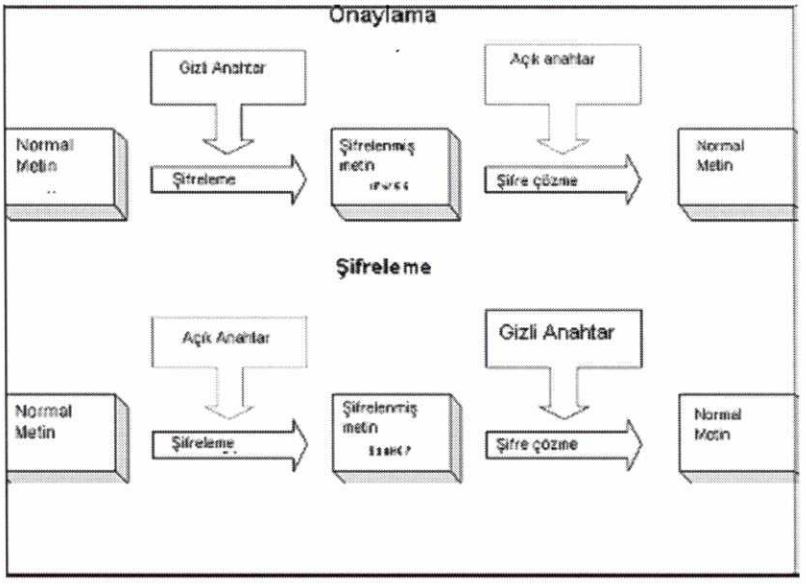
Örneğimize dönecek olursak asimetrik şifreleme Ayşe'nin kendi gizli anahtarının olduğu Umut'un ise Ayşe'nin açık anahtarına sahip olduğu şifrelemedir. Açık ve gizli anahtarlar aynı zamanda üretilirler. Veri bir anahtarla şifrelenirken diğer anahtarla çözümlenir. Yani Ayşe'ye mesaj göndermek isteyen bir şahıs Ayşe'nin açık anahtarını kullanarak mesajını şifreler ve sadece Ayşe bu açık anahtarla eşleşen gizli anahtarını kullanarak şifreyi çözebilir.

Sayısal imzanın gizliliğinin korunması için temel gereklilikler algoritmaların ve sayısal imzanın üretimiyle ilgili parametrelerin gizliliği, anahtar çiftinin benzersizliği ve gizli ve açık anahtarın bir başka yolla üretilememesidir.

Asimetrik algoritmalar geniş mesajları şifrelemede oldukça yavaştırlar. Ancak bu algoritmalar verinin onaylanması, bütünlüğü, inkar edilememezliği ve gizliliğin sağlanmasında kullanılırlar.

Asimetrik algoritmalar sayısal imza, anahtar değişimi, ve anahtar anlaşması için kullanılırlar. Bazı asimetrik algoritmalar (RSA (RSA 78)) şifreleme ve şifre çözmede kullanılabilir. Pratikte simetrik anahtar algoritmasından daha yavaş olduklarından çok fazla boyuttaki veriyi şifrelemede asla kullanılmaz. Ancak bu algoritmalar küçük boyuttaki verileri şifrelemede kullanılırlar. Bu uygulama anahtar değişimi olarak adlandırılır ve bir çok protokolde kullanılır.

Anahtar anlaşmasında ise diğer asimetrik algoritmalar kullanılır (örn. Diffie-Helman [DH 76]). Ayşe ve Umut'un Diffie Hellman anahtarları oluşturduklarını varsayalım. Umut kendi gizli anahtarı ve Ayşe'nin açık anahtarına sahiptir. Ayşe ise kendi gizli anahtarı ve Umut'un açık anahtarına sahiptir. Bir matematiksel algoritma yardımıyla Ayşe ve Umut aynı gizli değeri üretirler. Veli açık anahtarlara sahip olabilir ancak bu gizli değeri hesaplayamaz. Şekil 2.1'den açık anahtar şifrelemesi daha açık bir şekilde anlaşılabilir.



Kaynak:TurSign [37]

Şekil 2.1 Açık Anahtar Şifrelemesi

2.3.2 Açık Anahtar Altyapıları (Public Key Infrastructures (PKIs))

Açık anahtar altyapısı terimi, açık anahtar şifrelemesinden doğmuştur ve bu da sayısal imzanın dayandığı teknolojidir. Açık anahtar şifrelemesini eşsiz kılan sebeplerin başında güvenlik fonksiyonları yer almaktadır [18].

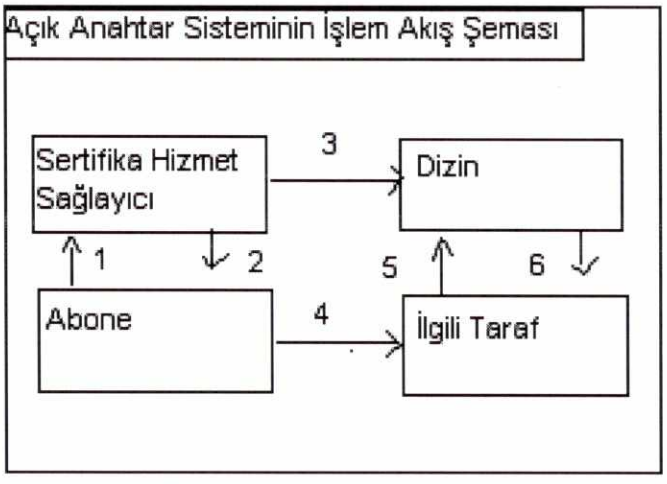
Açık anahtar altyapıları ile eskiden kağıda dayalı olarak gerçekleştirilen ürünlerin gönderilmesi ile ilgili işlemler elektronik yaklaşımlar vasıtasıyla kolaylaştırılıp hızlandırılabilmektedir. Elektronik çözümler veri bütünlüğü ve doğruluğunun sağlanmasına bağlıdır.

Modern güvenlik mimarisinin genel amacı kullanıcılar, kaynaklar, ve parsel sahiplerinin bulunduğu geniş dağılımlı bir çevrede ihtiyaç duyulan bilgileri korumak ve dağıtımını yapmaktır. Tüm bu ihtiyaçların karşılanması amacı açık anahtar altyapısının kullanımını doğurmuştur. Açık anahtar altyapısı kuruluşların kendi haberleşmelerinde şebekeler üzerinden gerçekleştirdikleri işlemlerin güvenliğinin korunmasını temin eden yazılım ve şifreleme tekniklerinin bileşimidir. Açık anahtar altyapısı sayısal sertifikaların, açık

anahtar şifrelemesinin ve sertifika hizmet sağlayıcılarının kuruluş genelindeki güvenlik altyapısında bütünleşmesini sağlar.

Tipik bir kuruluşun açık anahtar altyapısı sertifikaların özel kişi ve servislere dağıtımı, son kullanıcıların yazılıma kayıt yaptırması, sertifika dizinleri ile entegrasyon, sertifikaların idaresi, yenilenmesi ve iptali ile ilgili hizmet ve servisleri ihtiva eder [38].

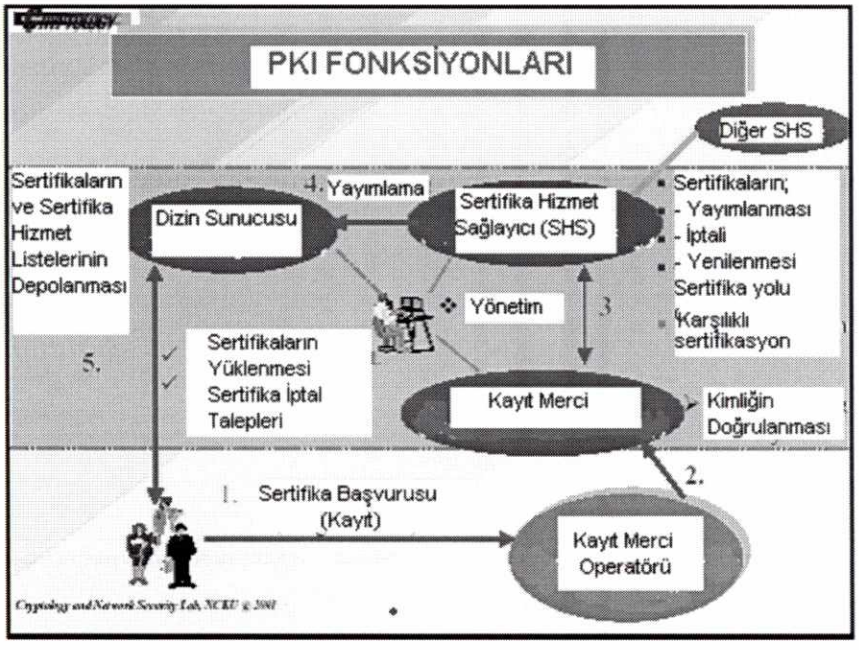
Aşağıda açık anahtar sisteminin işlem akış şemasının grafiksel gösterimi yer almaktadır [32].



Şekil 2.2 Açık Anahtar Akış Şeması

1. Adım: Abone sayısal sertifika için sertifika hizmet sağlayıcısına başvurur.
2. Adım: Sertifika hizmet sağlayıcısı abonenin kimliğini tasdik eder.
3. Adım: Sertifika hizmet sağlayıcısı sertifikanın kaydını bir dizinde toplar
4. Adım: Abone kendi gizli anahtarıyla mesaj sahibinin kimlik doğrulaması, mesajın bütünlüğü ve inkar edilememezliğini sağlayarak mesajı imzalar ve karşı tarafa gönderir.
5. Adım: Karşı taraf mesajı alır. Sayısal imzasını abonenin açık anahtarıyla onaylar ve abonenin sertifikasının geçerliliğini ve durumunu kontrol etmek için veri kütüğüne döner.

6. Adım: Veri kütüğü abonenin sertifikasının durumunun sonucunu karşı tarafa iletir.



Şekil 2.3 Açık Anahtar Altyapısı Fonksiyonları [34]

Açık anahtar altyapısının temellerinin anlaşılması sayısal imza konusunun anlaşılmasında birincil önem teşkil ettiğinden dolayı bir sonraki bölümlerde sırasıyla;

- Açık anahtar altyapısının bileşenleri
- Açık anahtar altyapısı mimarileri
- Açık anahtar altyapısının fiziki mimarisi
- Açık anahtar altyapısı veri tabanları konuları detaylıca incelenmektedir.

3.3.2.1 Açık Anahtar Altyapısı Bileşenleri

Açık anahtar altyapısının fonksiyonel elemanlarını;

- Sertifika hizmet sağlayıcılar,
- Kayıt kurumları,

- Veri kütüğü ve
- Arşiv

oluşturmaktadır [34].

2.3.2.1.1 Sertifika Hizmet Sağlayıcıları

Birbirlerini önceden tanımayan kişiler asimetrik şifreleme tekniklerini kendi sayısal imzalarında kullandıklarında haberleşme işlemi içerisindeki kuruluşları onaylayacak olan güvenilir bir kuruluşa ihtiyaç duyarlar. Sayısal İmza Kanununda bu kuruluş sertifika hizmet sağlayıcısı olarak tanımlanmıştır. Sertifika hizmet sağlayıcılarına kendi sayısal imzaları eklenmiş olan anahtar sertifikaların onaylanması ve bütünlüğünün garanti altına alınması gibi bir garantör rol verilmektedir.

Sertifika hizmet sağlayıcıları açık anahtar altyapısının temel yapıtaşı olup; elektronik ödemeleri yapan ya da gönderen veya diğer temasları gerçekleştiren tarafların kimliklerini onaylayan noter benzeri kuruluşlardır. Onaylama taraflar arasındaki resmi ödeme işlemlerini de içeren çok gerekli bir unsurdur. Sertifika hizmet sağlayıcıları sertifika iptal listelerini de yayınlamak zorundadırlar [39].

Sertifika hizmet sağlayıcının görevi sertifikayı üretim, dağıtım, yenileme, yeni anahtar üretimi, iptal, geçici iptal gibi bir yaşam döngüsü içerisinde yönetmektir. Sertifika hizmet sağlayıcılar sıklıkla abonelerin kayıt yetkilerini kendilerinin bir yan kuruluşu olan kayıt tescil kurumlarına devrederler. Bazı durumlarda sertifika hizmet sağlayıcıları kayıt fonksiyonlarını kendileri gerçekleştirirler. Sertifika hizmet sağlayıcılar ayrıca çevrimiçi durumun korunması mekanizmasını ve iptal listeleri yoluyla sertifika durumlarının yansıtılmasından sorumludurlar. Tipik olarak sertifika hizmet sağlayıcısı sayısal sertifikaları ve sertifika iptal listelerini bir dizin halinde yayınlayarak ilgili taraflar için erişilebilir olmasını sağlarlar.
Bu iş bir başka güvenlik problemini doğurmaktadır. Bir sertifika hizmet sağlayıcısı kendi ürettiği anahtarları onaylar. Teoride bir suçlu bir sertifika

hizmet sağlayıcısı kurarak sertifikalar yaratıp dağıtabilir. Böyle bir durumun önüne geçmek için sayısal imza kanunlarında sertifika hizmet sağlayıcılarına katı güvenlik şartları getirilmeli ve sayısal imzanın geçerliliği ve güvenlikle ilgili altyapı gereksinimlerine yönelik güçleri olan bağımsız bir kuruluşla ilgili hükümleri içermelidir [40].

Sertifika hizmet sağlayıcıları açık anahtar sertifikalarını yayınlar. Bu ise hizmet sağlayıcısının başvuru sahibini geçerli bir pasaport ve diğer geçerli belgeler yoluyla belirlemesini gerektirir.

Sertifika hizmet sağlayıcısı tasdik edilecek olan sayısal imzanın üreticisine kamu telekomünikasyon şebekeleri üzerinden erişilebilir tüm sertifikaların listesine erişimi sağlamalıdır [41].

Bu listeyi kullanan kurum bu sertifika üzerindeki verilerin onaylanmış olduğundan nasıl emin olacaktır? Bu sorunun cevabı sertifika hizmet sağlayıcısının imza anahtarı sahiplerinin verilerini içeren veri sertifikası altına kendi sayısal imzasını ekleyerek belgelendirmesidir [41].

2.3.2.1.2 Kayıt Kurumları

Kayıt Kurumu sertifika hizmet sağlayıcılar için kullanıcıların kayıtlarını tutan güvenilir kuruluşlardır.

2.3.2.1.3 PKI Veri Kütüğü

PKI Veri Kütüğü bir sertifika hizmet sağlayıcısının aktif sayısal sertifikalarını tuttuğu bir veri tabanıdır. Veri kütüğünün temel görevi sayısal olarak imzalanmış mesajlar alan bireyler ile iş çevrelerinin sayısal sertifikaların durumunu teyit etmesini sağlamaktır. Dizin servisleri X.500 standardının şartlarını taşırlar. X.500 standardı kendi içerisinde bir dizi tavsiye kararı ve bazı ISO standartlarına atıflar içerir.

2.3.2.1.4 Arşivler

Arşiv gelecekteki anlaşmazlıkların çözümüne yönelik kullanılan veritabanıdır. Sertifika hizmet sağlayıcısı her bireyin açık anahtarını yayınlar ve sözkonusu bireylerin uygun yeterlilikte olduğunu teyit eder. Tipik bir sayısal sertifika açık anahtar, gizli anahtar sahibi ile ilgili bilgi, sertifikanın geçerli olduğu periyot ve sertifika hizmet sağlayıcısının kendi imzasını içerir. Buna ek olarak sertifikayı imzalayan taraf hakkında ya da açık anahtarın tavsiye edilen kullanımı hakkındaki diğer bilgileri de içerebilir.

2.3.2.1.5 Açık Anahtar Altyapısı Kullanıcıları

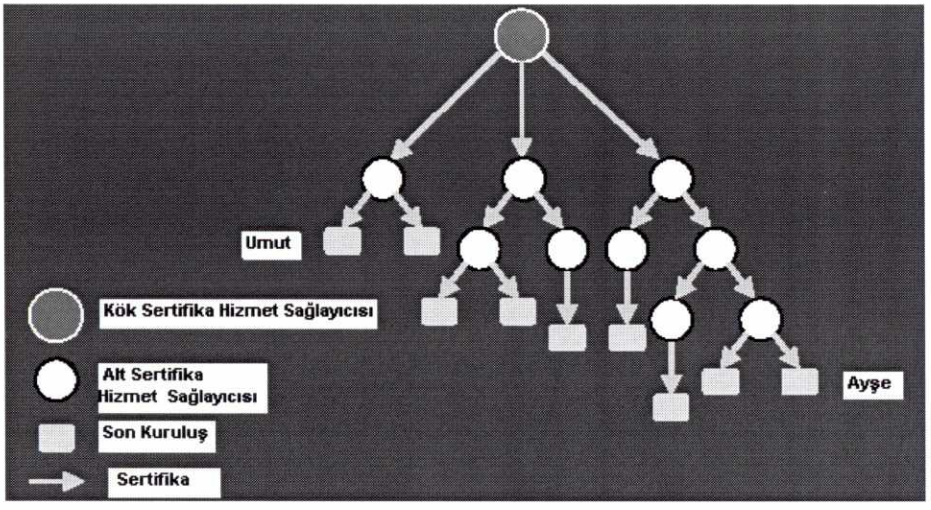
Abone bir birey ya da iş kuruluşu olup sayısal olarak imzalanmış mesajları doğrulayan bir sayısal sertifika almak için sertifika hizmet sağlayıcı ile sözleşme imzalar.

2.3.2.2 Açık Anahtar Altyapısı Mimarileri

2.3.2.2.1 Kuruluş (Şirket) PKI mimarisi

Sertifika sahipleri üyesi oldukları topluluk ve organizasyonlara bağlı olarak farklı sertifika hizmet sağlayıcılarından sertifikalar sağlayabilirler. Tipik bir açık anahtar altyapısı bir çok sertifika hizmet sağlayıcısı ile güvenlikli yollarla bağlıdır. Geleneksel açık anahtar altyapı mimarisi hiyerarşik ve ağ ile bağlantılı (mesh) kuruluş mimarisinden oluşur. Sertifika hizmet sağlayıcılar birbirlerine bir çok yolla bağlanabilirler [34].

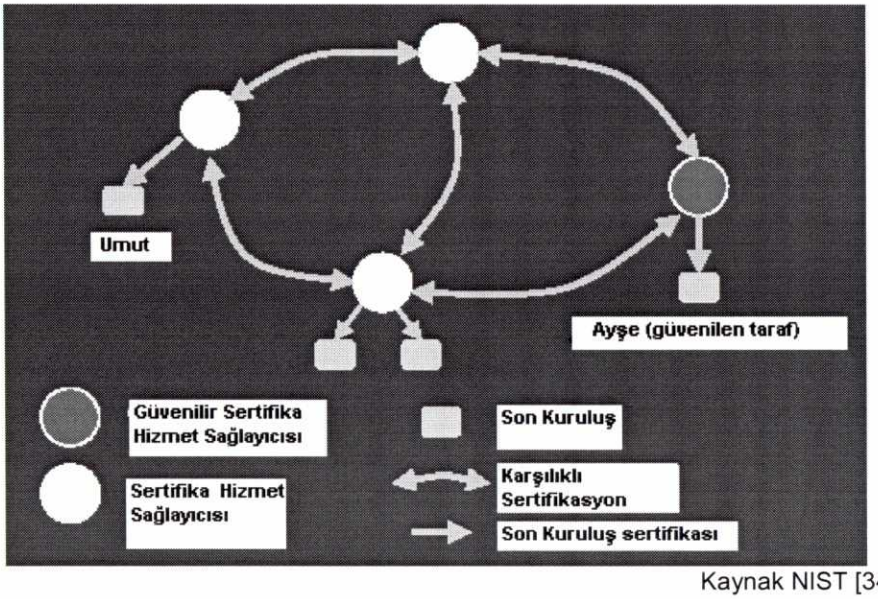
Hiyerarşik Kuruluş Mimarisi: Sözkonusu mimaride kuruluşlar bir kök sertifika hizmet sağlayıcısının altında sıralanırlar. Kök sertifika hizmet sağlayıcısı alt sertifika hizmet sağlayıcıları için sertifika yayınlar. Alt sertifika hizmet sağlayıcılar ise kendi altlarındaki sertifika hizmet sağlayıcılar ya da kullanıcılar için sertifika yayınlayabilirler. Hiyerarşik açık anahtar mimarisinde diğer tarafların hepsi kök sertifika hizmet sağlayıcısının açık anahtarına sahiptirler [34].



Kaynak NIST [34]

Şekil 2.4 Hiyerarşik Kuruluş Mimarisi

Ağ ile bağlantılı (Mesh) Kuruluş Mimarisi: Sözkonusu mimaride bağımsız sertifika hizmet sağlayıcılar birbirlerine karşılıklı olarak sertifika sağlarlar. Sertifika hizmet sağlayıcıları arasında güncel bir güvenlik ağı oluşmuştur. Güvenilir taraf güvenilen sertifika hizmet sağlayıcısından gelen sertifikasyon yolunu onaylayarak sertifikayı onaylamış olur [42].



Kaynak NIST [34]

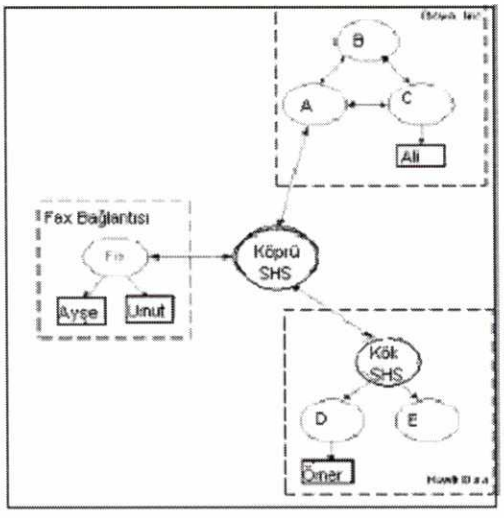
Şekil 2.5 Ağ ile bağlantılı (Mesh) Kuruluş Mimarisi

3.3.2.2.2 Köprü Açık Anahtar Altyapı Mimarisi

Sözkonusu mimari, kuruluş açık anahtar altyapılarını mimariden bağımsız olarak birbirine bağlamak için tasarlanmıştır. Ağ ile bağlantılı sertifika hizmet sağlayıcısının aksine Köprü sertifika hizmet sağlayıcısı hiyerarşi içinde bir güven noktası olarak kullanılma ihtiyacında değildir ve kullanıcılara doğrudan sertifika sağlamaz. Tüm açık anahtar altyapısı kullanıcıları köprü sertifika hizmet sağlayıcıyı aracı olarak kullanırlar.

Köprü sertifika hizmet sağlayıcılar farklı kuruluş sertifika hizmet sağlayıcıları ile eşlerarası ilişkiler kurarlar. Bu ilişkiler farklı açık anahtar altyapılarını birbirlerine bağlayan bir güven köprüsü vazifesini görür.

Güven alanı hiyerarşik planlı olarak kurulmuş ise köprü sertifika hizmet sağlayıcısı kök sertifika hizmet sağlayıcısı ile ilişki kurar. Eğer ağ ile bağlantılı açık anahtar ile kurulmuşsa köprü bu sertifika hizmet sağlayıcılardan yalnız birisiyle ilişki kurar. Her iki durumda da köprü ile güven ilişkisine giren sertifika hizmet sağlayıcısı temel sertifika hizmet sağlayıcısı olarak adlandırılır [43].



Kaynak NIST [34]

Şekil 2.6 Köprü Sertifika Hizmet Sağlayıcı (SHS) ve diğer Kuruluş SHS ları

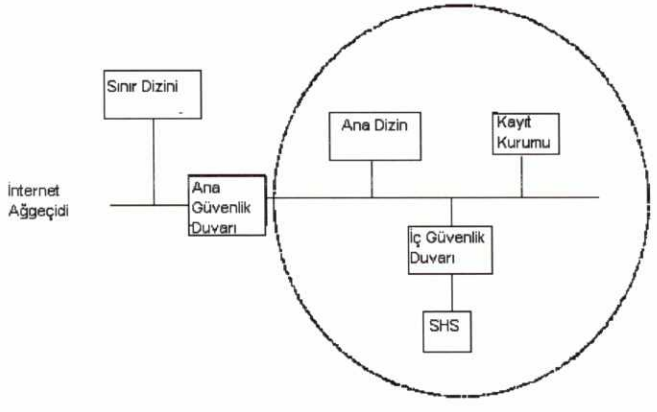
2.3.2.3 Fiziki Mimari

Açık anahtar altyapılarının fiziksel olarak tasarlanmasının bir çok yolu vardır. Ancak ana açık anahtar altyapı bileşenlerinin farklı sistemlerde oluşturulması önerilmektedir. Yani bir sistemde sertifika hizmet sağlayıcısı, bir diğer sistemde kayıt kurumu ve bir başkasında dizin sunucuları oluşturulmalıdır.

Sistemler hassas veriler taşımaları dolayısıyla kuruluşun internet güvenlik duvarının arkasına yerleştirilmelidir. Sertifika hizmet sağlayıcının sistemini tehlikeye atmak açık anahtar altyapı sisteminin tüm uygulamalarını bozabileceğinden sözkonusu sistem oldukça önem taşımaktadır.

Sonuç olarak sertifika hizmet sağlayıcısının kuracağı sistemi ek bir internet güvenlik duvarının ardına yerleştirmesi tavsiye edilir. Kuruluşun internet güvenlik duvarı SHS ve Kayıt kurumunun ve uygun sistemler arasındaki iletişime imkan vermelidir.

Temel dizin sunucusu kuruluşun korunmuş şebekesinin içerisine yerleştirilmiştir ve varolan sertifikaları güncelleyerek ya da yeni sertifikalarla sınır dizinini yeniler. Kuruluş içerisindeki kullanıcılar ana dizin sunucusunu kullanabilirken diğerleri sadece sınır dizinine erişebilirler [44].



Kaynak NIST [34]

Şekil 2.7 Açık Anahtar Altyapısının Fiziki Topolojisi

2.3.2.4 Açık Anahtar Altyapısı Veri Yapıları

İki temel veri yapısı bulunmaktadır. Bunlar açık anahtar sertifikası ve sertifika iptal listeleridir. X.509 açık anahtar sertifikaları esnek ve güçlü bir mekanizmadan oluşur [34].

2.3.2.4.1 X.509 Açık Anahtar Sertifikaları

Sertifika hizmet sağlayıcıları, kullanıcıların kimlik bilgilerini doğrulamak üzere, kullanıcılara elektronik sertifika (kimlik) belgesi verir. Elektronik sertifika, kullanıcı bilgilerini içeren bir verinin sertifika hizmet sağlayıcısı tarafından sayısal olarak imzalanması ile oluşur. Elektronik sertifika belgesinde, kullanıcının adı, soyadı, e-posta adresi gibi bilgilerin yanı sıra, kimlik belgesinin geçerlilik süresi, kullanıcının açık anahtar bilgisi gibi bilgilerde bulunur [44].

X.509 açık anahtar sertifikasında yer alan bilgilerin içeriğinin bir kısmı seçime dayalı olmasına rağmen bazıları da zorunlu içeriklerden oluşmaktadır.

Zorunlu alanlar arasında sertifikanın seri numarası, imzalamada kullanılan algoritmanın belirteci, sertifika yayınlayıcısının ismi, sertifikanın geçerlilik süresi, açık anahtar ve özne ismidir. Özne kısmı gizli anahtarı kontrol eden kısımdır. İsteğe bağlı alan ise versiyon numarası, iki benzersiz tanımlayıcı, ve onların uzantılarıdır. Bu isteğe bağlı alanlar sertifikaların ikinci ve üçüncü versiyonlarında gözükmektedir.

2.3.2.4.2 Sertifika İptal Listeleri (Certification Revocation Lists)

Sertifikaların kullanım süreleri vardır. Bu kullanım süresinin sonuna ulaşıldığında sertifika içerisindeki bilgiler itimat edilmez olmaktadır. Sertifika kullanıcılarının sertifikalarını yenilemelerini sağlayan mekanizma X.509 sertifika iptal listeleridir.

2.3.3 Sayısal İmzanın Üretimi

Sayısal İmzanın üretilmesi için gerekli olan mekanizma karma (hash) fonksiyon olarak adlandırılır. Karma fonksiyon ve imza algoritmaları oldukça karmaşık matematiksel eşitliklerdir. Mesajın özü olarak da tabir edilen karma fonksiyon algoritması orijinal mesajın ikili kodundan 160 bitlik basamak serisine sahip orijinal mesaja eş olarak elde edilir.

İmza algoritması bu mesaj özü üzerinden gerçekleştirilir. Kalan basamak dizileri sayısal imzadır. İmza sahibinin gizli anahtarı imzalama süreci boyunca imza algoritmasına dahil edilir. Bununla ilgili olarak aşağıda oldukça kaba bir örnek sunulmaktadır [38] :

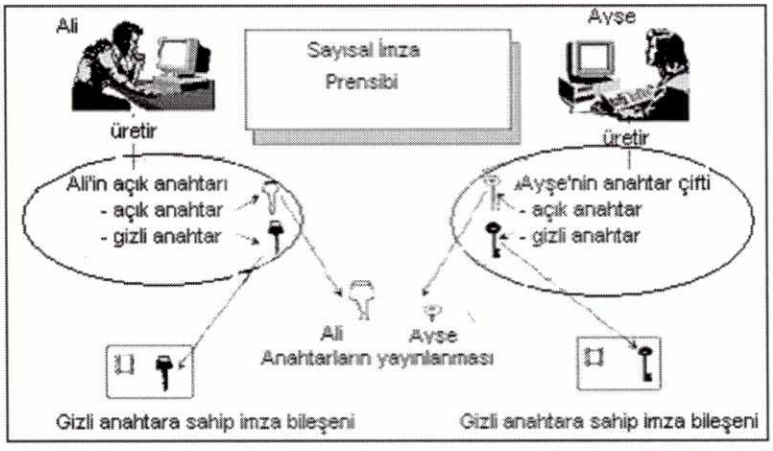
100 Orijinal Mesaj
2 Hash Algoritması
x___
200 Mesaj Özü
2 * İmza Algoritması
x___
800 Sayısal İmza
(*=2=gizli anahtar)

Basitleştirmek amacıyla 100 ikili numarasının orijinal mesajı temsil ettiğini varsayalım Basitliği sağlamak adına hash algoritmasının ikili numaranın 2 ile çarpımı sonucu elde edildiğini düşünelim. Mesajın ikilisine geçişin sonucu mesajın özüdür yada mesajın parmak izidir. Örnekte bu değer 200'dür. Mesaj özü imza sahibinin imza algoritmasından geçirilir. Sayısal imza gizli anahtarın bir bileşenidir. Bu örnekte imza algoritması *'ın 2 katı olarak basitleştirilmiştir. * burada imza sahibinin gizli anahtarıdır. Bu örnek için gizli anahtar(*)=2'dir. Sonuç olarak elde edilen 800 değeri sayısal imzayı ifade etmektedir

Karma fonksiyon mesajın kendisinin sadece imza sahibi tarafından bilinen bir giz ile birleştirilerek dönüşümüdür. Bu yolla imza sahibi ve imzalanan mesaj bağlantılandırılmış olur. İmza sahibinin sayısal imzası imzaladığı her doküman için farklı olacaktır. Bu fonksiyon imzanın üretiminden önce mesajı kendi karma değerine indirgenerek imzalanmasını sağlamaktadır. Mesajın

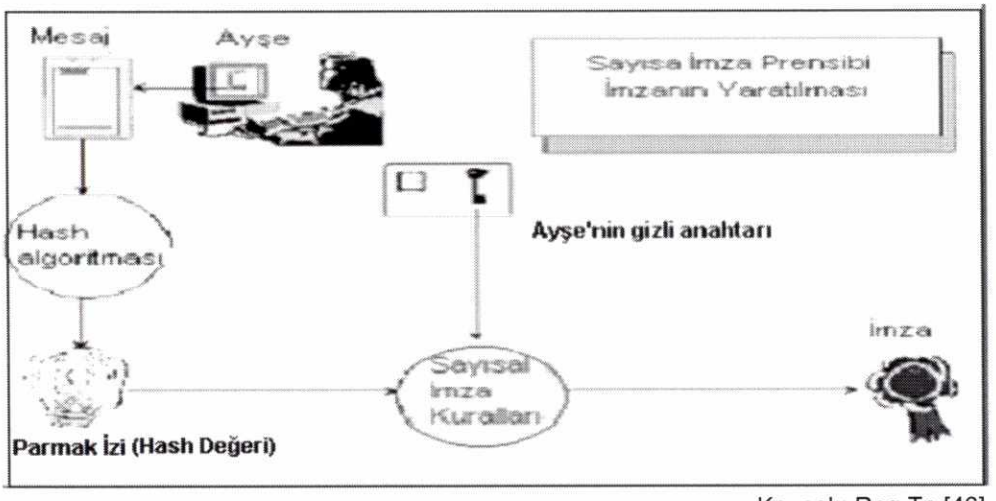
kendisi değil ancak karma değeri imzalanır ve bu sayısal imzayı temsil eder. İmza otomatik olarak mesaja eklenir ve mesaj ve sayısal imza elektronik olarak alıcıya gönderilir. Bu uygulama depolama kapasitesi ve gönderme zamanında tasarruf sağlar. Bu noktada sayısal imzanın güvenliğinin karma fonksiyonunun şifreleme gücüne bağlı olduğu söylenebilir. Karma değeri aynı karma değerine sahip olan farklı mesajların doğurduğu çakışmaya dayanıklı ve tek yönlü olmalıdır.

Eğer çakışmalar oluşursa mesajın karma değerine indirgenmesi, onaylama algoritmasının genel anahtarı orijinal mesajın başka birisiyle değiştirilmesi durumunda güvenlik problemlerine yol açabilir. Diğer bir deyişle karma fonksiyonu sanal olan çakışmaya karşı korumalı olmalıdır. Bu özelliğin ihlali imzalanmış dokümanlar üzerinde tahrifat yapılmasının önünü açabilir [45].



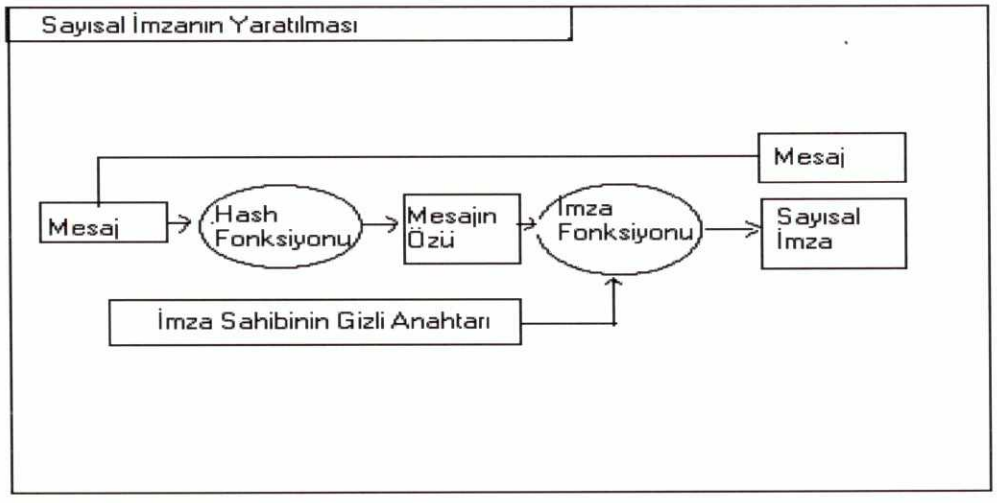
Kaynak: Reg Tp [46]

Şekil 2.8 Anahtarlarların Yayınlanması



Kaynak: Reg Tp [46]

Şekil 2.9 Sayısal İmzanın yaratılması



Kaynak: Digital Signature Trust Company [38]

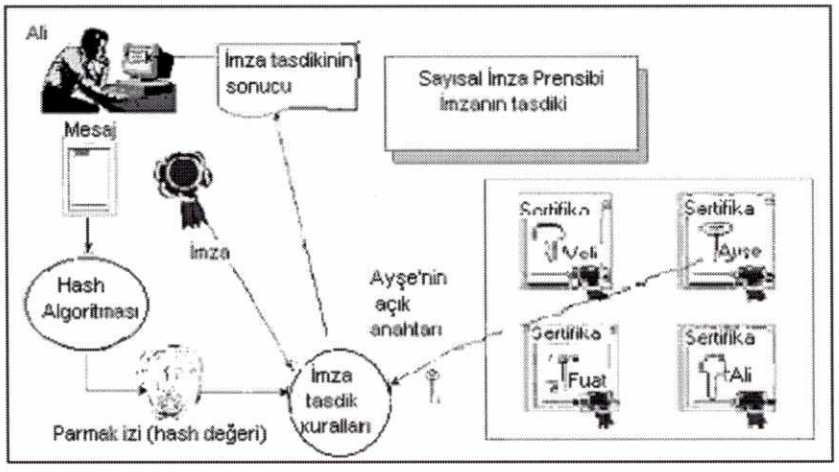
Şekil 2.10 Sayısal İmzanın yaratılması

2.3.4 Sayısal İmzanın Doğrulanması

Mesajın alıcı tarafından doğrulanması karşı sırayı takip eder. Gönderenin eklenmiş olan açık anahtarı kullanılarak imzalanmış olan karma değeri çözümlenir. Bu ise orijinal mesajın karma değerini ortaya çıkarır. Alıcı kendi karma fonksiyonuyla imzanın iliştirildiği mesajın karma değerini belirler. Eğer

bu işlem başarılı olursa imzadan çözümlenen karma değeri ile ikinci karma değeri karşılaştırılır. Eğer sonuç aynı ise imza geçerlidir. Ancak orijinal mesaj gönderim sırasında değişirse karma değeri de değişecektir. Karma değeri orijinal mesaj tarafında belirlendiğinden imzada türetilen karma değeri değişecektir ve alıcı mesajın değiştirilmesinden ya da imzanın tahrifatından dolayı mesajı kabul etmeyecektir [47].

Eğer sayısal imzanın doğrulanması başarıyla gerçekleşirse alıcı mesajın değiştirilmediğini kabul eder (Mesajın bütünlüğü). Ancak mesaja bir imza eklenmiş olsa bile bunun yetkilendirilmiş kişiye ait olup olmadığı bir soru olarak açıkta kalmaktadır.



Kaynak: Reg Tp [46]

Şekil 2.11 Sayısal İmzanın tasdiki

Bir birey için sayısal imza yazılımının satın alınması ya da sunucudan bigisayara yüklenmesi mümkündür. Bir birey anahtar üreterek seçtiği kimliği kullanıp kendi açık anahtarını çevrimiçi dünyada kimliğinin doğruluğu onaylanmaksızın açabilir.

Bu senaryo güvenilir üçüncü taraf olarak bireylere bireylerin kimliğinin ve açık anahtarlarının doğrulanması hizmetini verecek bir kuruluşa duyulan ihtiyacın öneminin altını çizmektedir [47].

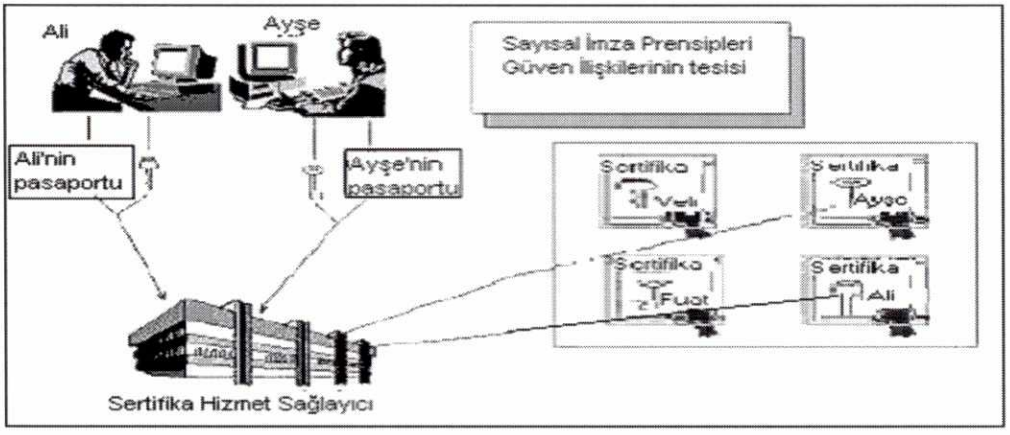
Taraflara güvenlikli elektronik ticaret imkanının sağlanması için gereken teknolojilerle ilgili olarak bir sorunun yanıtlanması gereklidir. Sayısal dünyada bireyin açık anahtarı gerçekte kendisine ait midir? Birey ve bireyin açık anahtarıyla ilgili bilgiyi sağlayan bir sayısal sertifika sorunun yanıtıdır. Bu belge sertifika hizmet sağlayıcısı tarafından sayısal olarak imzalanmaktadır. Sertifika hizmet sağlayıcısı bireyin kimliği ve açık anahtarı arasındaki bağı teyit etmektedir. Sertifika hizmet sağlayıcısı sertifika içerisinde yer alan bilgilerin sertifika üzerindeki kuruluşa ait olduğuna güvence verir. Açık anahtar sertifikası üzerinde sertifika hizmet sağlayıcısı tarafından sağlanan sayısal imza, şifreleme bilgileri, kuruluşun açık anahtarı, ismi ve diğer bilgiler ve son kullanma tarihini içerir. Karşı tarafın sertifikanın sertifika hizmet sağlayıcısı tarafından yayınlandığını anlamak için sertifika hizmet sağlayıcısının sertifika üzerindeki imzasını doğrulamalıdır. Açık anahtarlar pek çok kök sertifika hizmet sağlayıcısı tarafından ilk olarak standart bir web sunucusu yazılımı üzerinden yüklenmişlerdir (Örneğin netscape navigator, Microsoft Internet Explorer).

Bu olay karşı tarafa sertifika hizmet sağlayıcısının açık anahtarını kullanarak sertifikanın güvenilir bir sertifika hizmet sağlayıcısı tarafından yayımlanıp yayımlanmadığının belirlenmesine izin verir.

Güvenli verinin garanti edilmesi için sertifika hizmet sağlayıcısı;

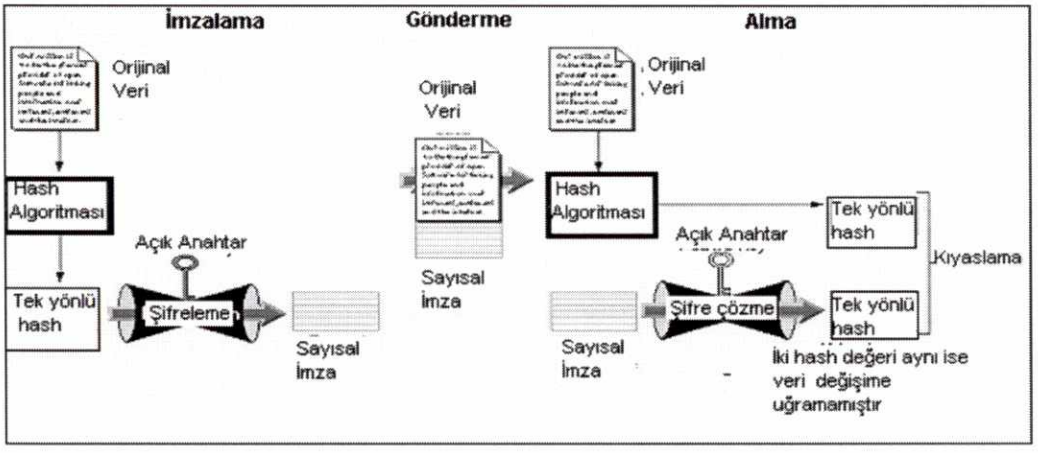
- Sertifikaların içerdiği verilerin değiştirilmemesi için gerekli önlemleri almak,
- Gizli imza anahtarlarının korunması ve yetki dışı kullanıma karşı teknik unsurların korunması için gerekli güvenlik önlemlerini almak,
- Tahrif edilmiş ya da değiştirilmiş sayısal imzaları gizli anahtarların yetki dışı kullanımını ortaya çıkaran mekanizmaları sağlamakla yükümlüdür.

Böylelikle sertifika hizmet sağlayıcısına yetkilendirme ve açık anahtar sertifikalarının bütünlüğünü garanti eden bir fonksiyon yüklenmektedir.



Kaynak: Reg Tp [46]

Şekil 2.12 Güven ilişkilerinin tesisi



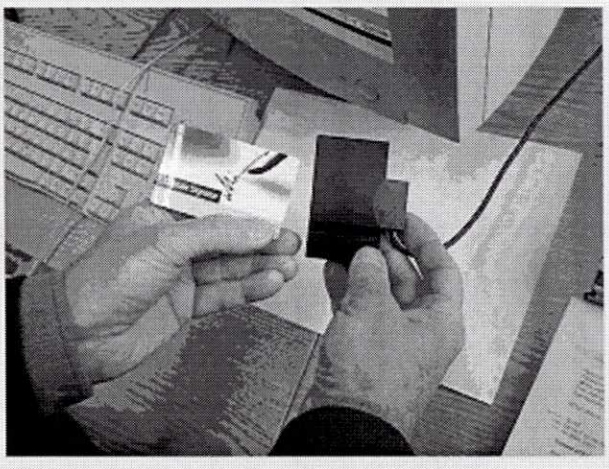
Kaynak: TurSign [37]

Şekil 2.13 Sayısal İmza işlemlerinin bir özeti

Konunun daha iyi anlaşılması için örnek olarak bir sertifika hizmet sağlayıcısına başvurup açık ve gizli anahtarlarınızı oluşturduğunuzu ve sayısal olarak imzalanmış bir e-posta göndermek istediğinizi varsayalım [45].

E-Posta Programınızı çalıştırırsınız

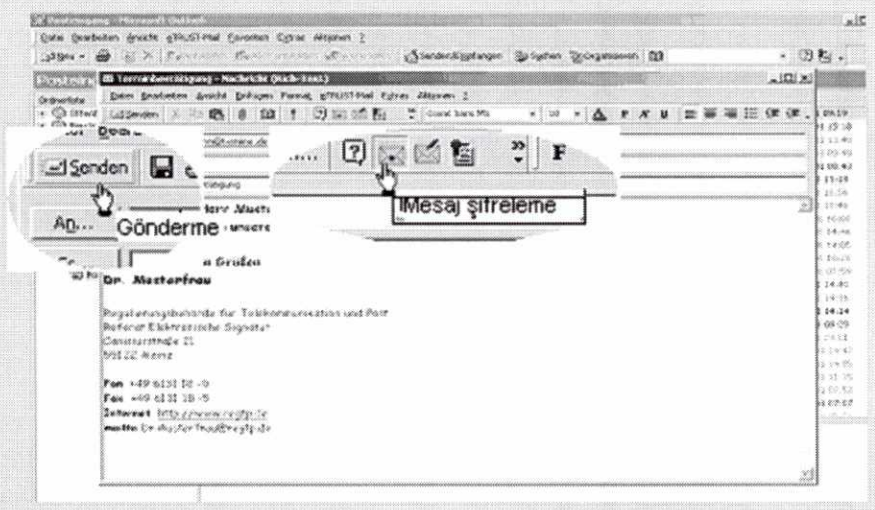
ve Sayısal Kimliğinizi yerleştirirsiniz. Bu bir kart olabileceği gibi güvenli bir siteden yüklediğiniz bir program da olabilir.



E-Posta programınızın menüsünde yer alan "imza" ikonuna tıklarsınız

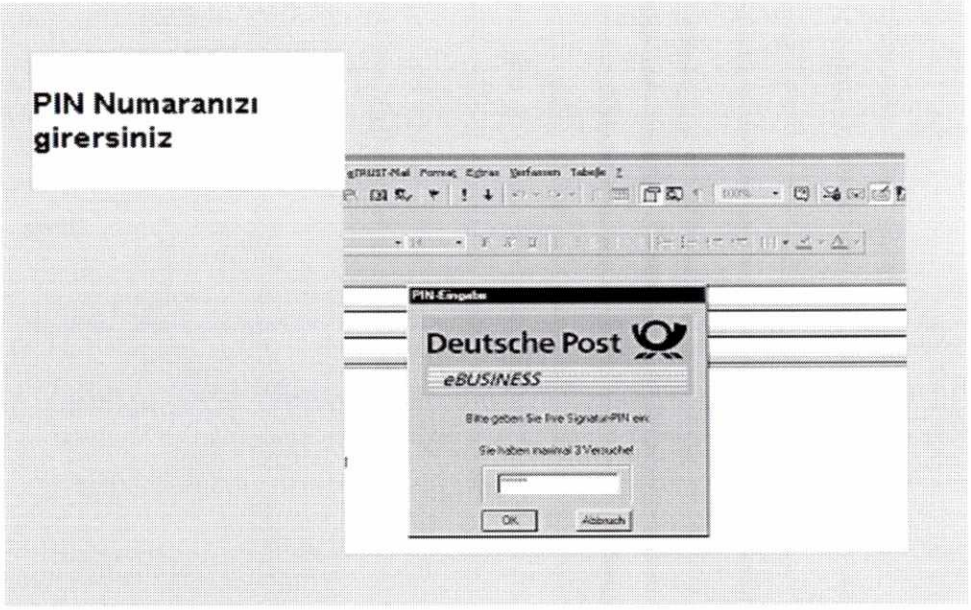
Eğer aynı zamanda mesajınızın şifrelenmesini de istiyorsanız -->

"Mesaj şifreleme" ikonuna tıklarsınız



böylelikle E-postanız gönderilmeye hazır olur

Şimdi ise e-postanızı sayısal olarak imzalamak istediğinizi doğrulamanız gerekir



Şekil 2.14 Bir E-Postanın sayısal olarak imzalanmış şekilde gönderimi [46]

Böylelikle E-Postanız Sayısal olarak imzalanmış ve gönderilmiş olur.

İkinci olarak sayısal olarak imzalanmış bir e-posta aldığınızı ve imzayı doğrulamak istediğinizi varsayalım.

Şekil 2.15 Sayısal olarak imzalanmış bir e-postadaki imzanın doğrulanması [46]

2.3.5 Sayısal İmza ile ilgili kabul edilen Avrupa Standartları

Standardizasyon konusu ile ilgili olarak; Avrupa Komisyonu elektronik ticaret ürünleri ile ilgili standartları kabul etmeye devam etmekte standartların referans numaraları Avrupa Ülkeleri Resmi Gazetesi'nde yayınlanmaktadır. Standardizasyon konusu ile ilgili Avrupa'da gerçekleştirilen çalışmalar;

- Avrupa Telekomünikasyon Standartları Enstitüsü ETSI [48] (European Telecommunications Standards Institude-ETSI) bünyesindeki ETSI Elektronik İmza Çalışma Grubu (ETSI ES Working Group)

- Avrupa Standardizasyon Komitesi CEN [49] (European Commitee for Standardisation/Information Society Standardisation System-CEN/ISSS) bünyesindeki Elektronik İmzalar Çalıştayı (CEN/ISSS Workshop on Electronic Signatures (WS/E-Sign)) ve

- ETSI Elektronik İmza Çalışma Grubu ve CEN Elektronik İmzalar Çalıştayı'nın ortak bir projesi olan Avrupa Elektronik İmza Standardizasyonu Teşebbüsü EESSI (The European Electronic Signature Standardisation Initiative- EESSI)

tarafından gerçekleştirilmektedir.

EESSI bünyesinde yürütülmüş olan çalışmaların 1. ve 2. safhasını 2000-2001 yılları arasındaki dönem oluşturmakta olup bu dönemde çıkarılan standartlar aşağıda yer almaktadır.

Çizelge 2.3 Sayısal İmza ile ilgili kabul edilen 1. ve 2. Safha EESSI Standartları [48]

Standardın Adı	**Yayın Tarihi**	**Konusu**
TS 101 861 v 1.1.1	Eylül 2001	Zaman Damgası Profili
TS 101 862 v 1.2.1	Haziran 2001	Nitelikli Sertifika Profili
TS 101 456 v 1.1.1	Aralık 2000	Nitelikli Sertifika yayınlayan sertifikasyon kurumları için politika şartları
TS 101 862 v 1.1.1	Aralık 2000	Nitelikli Sertifika Profili
TS 101 733 v 1.2.2	Aralık 2000	Elektronik İmza Formatları
ES 201 733 v 1.1.3	Mayıs 2000	Elektronik İmza Formatları

EESSI bünyesinde yürütülmüş olan çalışmaların 3. safhasını 2002-2004 yılları arasındaki dönem oluşturmakta olup bu dönemde yayınlanan standartlar aşağıda yer almaktadır.

Çizelge 2.4 Sayısal İmza ile ilgili kabul edilen 3. Safha EESSI Standartları [48]

Standardın Adı	Yayınlanma Tarihi	Konusu
TR 102 045	Mart 2003	Gelişmiş iş modelinde imza politikası
SR 002 176	Mart 2003	Güvenli elektronik imzalar için kullanılan parametre ve algoritmalar
TR 102 153	Şubat 2003	Sertifika profilleri için ön çalışma
TR 102 046	Şubat 2003	EESSI 2. ve 3. safhası içerisinde ETSI standartlarının muhafazası
TR 102 023	Ocak 2003	Zaman damgası hizmetini sunan kurumlara yönelik politik koşullar
TR 102 044	Aralık 2002	Sertifikasyonun nitelikleri için kimlik şartları
TS 101 733 v 1.4.0	Eylül 2002	Elektronik imza format versiyonları
TR 102 038	Nisan 2002	İmza politikaları için XML formatı
TS 102 023	Nisan 2002	Zaman damgası hizmetini sunan kurumlara yönelik politik koşullar
TS 102 042	Nisan 2002	Açık anahtar sertifikası yayınlayan kurumlara yönelik politika şartları
TS 101 456 v 1.2.1	Nisan 2002	Nitelikli sertifika yayınlayan sertifikasyon kurumlarına yönelik politika şartları
TR 102 030	Nisan 2002	Harmonize olmuş Güven Hizmet Sağlayıcısı durum bilgisi şartı
TR 102 040	Mart 2002	Sertifika Hizmet Sağlayıcıların Uluslararası Harmonizasyonuna İlişkin Politika Şartları
TS 101 861 v1.2.1	Mart 2002	Zaman damgası profili
TR 102 041	Şubat 2002	İmza politikaları raporu
TS 101 903	Şubat 2002	XML İleri Elektronik İmzalar (XAdES)
TS 101 733 v 1.3.1	Şubat 2002	Elektronik imza formatları

CEN çalıştay anlaşmaları vasıtasıyla (CEN Workshop Agreements-CWA) dokümanlarını yayınlamaktadır. Çalışma komitesi aşağıdaki standartları yayınlamıştır.

Çizelge 2.5 Sayısal İmza ile ilgili kabul edilen CEN Standartları [49]

Standardın Adı	**Yayınlanma Tarihi**	**Konusu**
CWA 14365	2003	Elektronik imza kullanım rehberi
CWA 14167-1	Mart 2003	Elektronik imza sertifikalarının düzenlendiği güvenilir sistemler için güvenlik koşulları: 1. Bölüm güvenlik sistemleri (15.07.2003 tarihli Avrupa Birliği Resmi Gazetesinde Komisyon Kararı olarak yayınlanmıştır.)
CWA 14355	2002	Güvenli imza yaratım cihazları uygulama rehberi
CWA 14167-2	Mart 2002	Elektronik imzalar için sertifikaların düzenlendiği güvenilir sistemlere yönelik güvenlik koşulları: 2. Bölüm Sertifika hizmet sağlayıcı imza uygulamaları için şifreleme modülü-Koruma profili (MCSP-PP) (15.07.2003 tarihli Avrupa Birliği Resmi Gazetesinde Komisyon Kararı olarak yayınlanmıştır.)
CWA 14169	Mart 2002	Güvenli imza yaratma cihazları 'EAL 4+' versiyonu, 15.07.2003 tarihli Avrupa Birliği resmi gazetesinde Komisyon Kararı olarak yayınlanmıştır
CWA 14168	2001	Güvenli elektronik imza yaratma cihazları 'EAL 4' versiyonu
CWA 14170	2001	İmza yaratma sistemleri güvenlik şartları
CWA 14171	2001	Elektronik imza doğrulama prosedürleri kılavuzu
CWA 14172-1	2001	EESSI uygunluk belgesi kılavuzu: 1. Bölüm-Genel
CWA 14172-2	2001	EESSI uygunluk belgesi kılavuzu : 2.Bölüm-Sertifika hizmet sağlayıcı hizmetleri ve uygulamaları
CWA 14172-3	2001	EESSI Uygunluk belgesi kılavuzu: 3.Bölüm-Elektronik imzalar için sertifikaları düzenleyen güvenilir sistemler
CWA 14172-4	2001	EESSI Uygunluk belgesi kılavuzu : 4. Bölüm-Elektronik imza doğrulama için imza yaratma uygulamaları ve metotları

CWA 14172-5	2001	EESSI Uygunluk belgesi kılavuzu: 5. Bölüm güvenli imza yaratma cihazları

2.4 Yasal Çerçeve

Elektronik veri insan hatası olmadan ihtiyari olarak teknik bir hata ya da kasıtlı bir hile ile değiştirilebilir. Bazı durumlarda mesajın yaratıcısını belirlemek mümkün olmayabilir. Buradaki temel soru mesaj ve mesajın içeriğinin belirlenmiş kişiye ait olup olmadığıdır. Günümüzdeki geleneksel kağıt mesajlarında otomatik daktilolar, gelişmiş cihazlar yoluyla değiştirilmesi muhtemeldir. Yasal olarak tanınmış sayısal imzalar elektronik mesajlar üzerinde değişiklikler yapılması geleneksel kağıt mesajlarındaki kadar zordur.

Elektronik verilerin;

- Belirlenmiş kişi tarafından imzalanıp imzalanması,
- İmzalandıktan sonra birisi tarafından herhangi bir şekilde değiştirilmemiş olduğunun doğrulanması gerekmektedir.

Sayısal imzanın elle atılan imzada olduğu gibi henüz gizliliği korunamamaktadır. Örneğin veriler istenmeyen üçüncü şahısların eline geçebilmektedir. Bu tip bir bilginin istenmeyen tarafların eline geçmesini önlemek için uygun şifreleme teknikleri kullanılabilir. Ancak bu prosedürler sayısal imza yasasının içerisinde bırakılmamalı ayrı konular olarak ele alınmalıdır.

2.5 E-Devlet Çalışmaları

En yalın biçimiyle; "Devletin vatandaşlara karşı yerine getirmekle yükümlü olduğu görev ve hizmetler ile vatandaşların devlete karşı olan görev ve hizmetlerinin karşılıklı olarak elektronik iletişim ve işlem ortamlarında kesintisiz ve güvenli olarak yürütülmesi" olarak tanımlanabilen e-Devlet'in

hayata geçirilmesi için gerekli olan öncelikli adımlar arasında hukuksal ve teknik altyapının tesisi gelmektedir.

Bu bağlamda, elektronik ortama ve açık ağ sistemine güvenin sağlanması *e-Devlet* oluşumunda vazgeçilmez ve önceliği çok yüksek uygulamalardan biridir. Bu nedenle, taraflar arası iletilerde; bilginin gizliliği, bütünlüğü ve tarafların kimliklerinin doğruluğu kurulacak olan teknik ve yasal altyapı ile garanti edilebilmelidir. e-Devletin hayata geçirilmesi için en hayati yasal düzenlemenin "Elektronik İmza Yasası" olduğu söylenebilir.

Elektronik imza başta elektronik satın alma işlemleri olmak üzere, belge hazırlama, onaylama gibi işlemlerin birçoğunda kullanılacak olduğundan e-Devlet oluşumunun en temel basamaklarından birisidir.

2.6 Elektronik yetkilendirme mevzuatı yaklaşımları

Elektronik imza için kuralcı yaklaşım, iki dizi yaklaşımı, minimalist yaklaşım olmak üzere üç temel yetkilendirme mevzuatı yaklaşımı bulunmaktadır [50].

2.6.1 Kuralcı yaklaşım

Kuralcı yaklaşım altında tahsis edilen sertifika hizmet sağlayıcılarına getirilecek çalışmalarla ve mali zorunluluklarla ilgili uygulamalar, anahtar sağlayıcılarının görevleri ile ilgili kuralları ve elektronik imzaların uyumlu olduğu durumları tanımlamak gibi yasa ve düzenlemeler asimetrik şifrelemeyi yaratılmış olan sayısal imzanın onaylama yolu olarak kabul etmektedir. Güvenlik altyapısının sağlanmasıyla ilgili detaylı regülasyonlar içermektedir. Utah imza kanunu bu yaklaşımın öncülerindendir.

Medeni kanuna sahip olan Almanya, İngiltere ve Arjantin bu yaklaşıma yönelmişlerdir.

2.6.2 İki dizi yaklaşımı

Bazı yargı yetkilileri önceki iki yaklaşımın gerektiği kadar ortak yetkiye sahip olmadığını farkederek yakınsamayı benimseyen ve önceki iki yaklaşımı temsil eden iki dizi yaklaşımını kabul etmişlerdir. Bu yaklaşım açık anahtar altyapılarının (PKI) uygulanması ve öngörülen standartları temsil eden ve yasal amaçlarla kullanılan geçerli elektronik imzayı nelerin oluşturduğuna dair geniş görüşe eşlik eden yasaların formunu oluşturmaktadır.

İki dizi yaklaşımına özellikle Avrupa Birliği ve Singapur'da destek artmaktadır.

2.6.3 Minimalist yaklaşım

Minimalist yaklaşım elektronik imzanın özel bir protokol ya da teknolojiden ziyade genel olarak kullanımına hizmet etmeyi amaçlar. Kanada, Amerika, İngiltere, Avusturalya ve Yeni Zellanda gibi geleneksel yasaya sahip ülkeler minimalist yaklaşıma yönelmişlerdir.

2.7 Uluslararası sayısal imza politikası konuları ve teşebbüsleri

2.7.1 Birleşmiş Milletler

Birleşmiş Milletler Genel Kurulunun 28 Mayıs-14 Haziran 1996 tarihleri arasında NewYork' da yapılan 29. toplantısında Elektronik Ticarete ilişkin Model Kanun ve konuya ilişkin Yasal Rehber'in kabul edilerek "sayısal imza ve sertifika hizmet sağlayıcıları" ile ilgili olarak diğer ülkelerin mevcut düzenlemelerinden de yararlanılmak suretiyle taslak bir metin hazırlanmıştır. Söz konusu taslakta elektronik imza mesaj içeriğine onay verildiğini göstermek niyetiyle mesaja eklenen veya mantıksal olarak mesaja bağlı olan elektronik bilgi olarak tanımlanmış ve güvenli elektronik imzanın standart özellikleri şu şekilde özetlenmiştir;

Teklik: Elektronik imzaların birbirinden farklı olması anlamına gelmektedir. Ya parmak izi, retina taraması gibi biyometrik yöntemlerle ya da

çift anahtar kullanımıyla teklik şartı yerine getirilebilmektedir. Kimlik Tespiti: Elektronik imza sahibinin kimlik tespitinin sağlanması anlamına gelmektedir. Bu tespitin çabuk, nesnel ve otomatik olması özellikleri üzerinde durulmaktadır.

Güvenilirlik: Elektronik imzayı kullanan olarak kimliği tespit edilen kişinin gerçekten mesajı imzalamış olması anlamına gelmektedir. Üçüncü bir güvenilir kişinin (Trusted Third Party), örneğin onay makamının süreç içerisinde üstlendiği görevin önemi ve yararı belirtilmektedir.

Bağlantı; mesajla imza arasında bağlantı olması anlamına gelmektedir mesaj değiştiğinde, elektronik imza geçersiz hale gelmelidir [29].

30 Ocak 2001'de yayınlanan Birleşmiş Milletler UNCITRAL Elektronik İmza Yasa Model Taslağını hazırlamıştır. Sözkonusu taslak ülkelere çıkaracakları elektronik imza yasaları için model vermekte ve e-imzanın temel kurallarının oluşturulmasını hedeflemektedir. Model, çeşitli ülkelerin farklı mevzuatlar geliştirme riskine karşı uyumlaştırma görevi üstlenmiştir. Bu model, Elektronik Ticaret Modeli'nin 7. maddesinde yer alan temel ilkeler üzerine inşa edilmiş ve o modele özel bir alanda ek olmak üzere düzenlenmiştir[51].

Modelde, imza sahibinin sorumlulukları, sertifika servis sağlayıcılarının sorumlulukları, e-imzaya güvenen üçüncü şahısların sorumluluklarına ilişkin hükümler de bulunmaktadır.

Model yasada, yabancı elektronik imzaların ve sertifikaların tanınmasına ilişkin özel bir düzenleme de mevcuttur. Model yasanın 12. maddesine göre, devletler elektronik imzanın hukuki etkisini düzenleme altına alırken, sertifikanın verildiği ve elektronik imzanın yaratıldığı ve kullanıldığı coğrafi yeri, sertifika servis sağlayıcının ve imzacının işyerinin bulunduğu coğrafi yeri dikkate almamalıdır. O ülke dışında verilen sertifikalar ulusal sertifikalarla eşdeğer hukuki etkiye sahip olmalı, ülke dışında yaratılan ve

kullanılan bir elektronik imza ülke içinde yaratılan ve kullanılan bir elektronik imza ile aynı hukuki geçerliliğe sahip olmalıdır.

2.7.2 Avrupa Birliği

AB Konseyi 13 Aralık 1999'da 99/93/EC (Ek-7) elektronik imza direktifini kabul etmiştir. Bu çerçevede, üye ülkelerin yönergeyi ulusal hukuklarına yansıtması için konulan süre 19 Temmuz 2001 olarak belirlenmiştir. Sözkonusu direktif güvenlik ve sorumluluk ile ilgili asgari kurallar getirmekte, hizmetlerin serbest dolaşımı ve esas ülke denetimi şeklindeki tek pazar ilkeleri temelinde elektronik imzaların AB çapında hukuken tanınmasını sağlamayı amaçlamaktadır [52].

Direktif, elektronik imzanın kullanılması ve hukuken tanınması için gereken çerçeveyi oluşturmaktadır. Direktifin 2/1. maddesine göre, elektronik imza, bir elektronik veriye eklenen veya ona mantıksal olarak bağlı olan ve bir tasdik (authentication) yöntemi olarak işlev gören elektronik formattaki veri anlamına gelmektedir. Gelişmiş elektronik imza (advanced electronic signature) ise direktifin 2/2. maddesine göre imzacıya bağlı olan, imzacının kimliği hakkında bilgi verme kapasitesine sahip olan, imzacı tarafından kontrol edilen ve ilgili veriye, veri üzerinde sonradan yapılan bir değişikliğin tespit edilebildiği şekilde bağlanan elektronik imzadır.

Direktifin 5/1. maddesine göre, özel sertifikaya bağlanan ve güvenli-imza-yaratma tekniği ile oluşturulan gelişmiş bir elektronik imza, elektronik bir veriye bağlandığında, tıpkı kağıt üzerine elle atılmış imza gibi hukuki etki yaratmalı ve davalarda delil olarak kabul edilmelidir.

Direktife göre, bu elektronik imzaların tedarik edileceği, imzaları kaydeden ve gelişmiş imzaları geçerli kılan sertifika servis sağlayıcılarının bulunması gerekir fakat bu sistemin mutlaka devlet tarafından yürütülen bir sistem olması gerekmemektedir. Bu servis sağlayıcılarına akreditasyon zorunluluğu getirilmemelidir; sistem gönüllü lisans sistemine

dayanmalıdır. Elbette devlet belirli imza yöntemlerinin onaylanması konusunda rol üstlenmelidir, ancak bu konuda teknoloji tarafsız olmak durumundadır.

Direktif aynı zamanda sertifika servis sağlayıcılarının sorumlulukları ile ilgili düzenleme içermektedir. Bir başka noktası da, üçüncü ülkelerde kurulu sertifika servis sağlayıcılarının verdiği sertifikaların, Topluluk içinde verilenlerle eş değer hukuki etkiye sahip olması gereğini düzenlemesidir (md. 7) [9].

AB üyesi ülkeler arasında [53];

- Almanya, Avusturya, Danimarka, Finlandiya Yunanistan, Hollanda, Macaristan Telekomünikasyon Regülasyon Kurumları,
- Estonya, Çek Cumhuriyeti, İspanya ve İtalya'da ise Bilgi Teknolojisi ve Haberleşme Bakanlıkları,
- Belçika ve Lüksemburg'ta Ekonomi Bakanlığı,
- Fransa ve Slovakya'da Ulusal Güvenlik Bakanlığına bağlı kuruluşlar ve
- İngiltere'de Ticaret ve Endüstri Bakanlığı'nın

99/93/EC direktifinin uygulamaya koyulmasını sağlayan kök sertifika hizmet sağlayıcılığı görevini yürüttüğü görülmektedir.

99/93/EC Direktifini yürürlüğe koymuş olan yukarıda belirtilen Avrupa Birliği ülkelerinin arasında kök sertifika hizmetini sağlama görevi yaklaşık % 68 oranında Telekomünikasyon Regülasyon Kurumlarının ve Bilgi Teknolojisi ve Haberleşme Bakanlıklarının sorumluluğuna verilmiştir.

2.7.3 Amerika Birleşik Devletleri

ABD'de 30 Haziran 2000'de kabul edilen ve 1 Ekim 2000'de yürürlüğe giren Elektronik İmza Yasası ile e-ticarette kullanılan bir çok belgenin hukuken geçerliliği kabul edilmiştir.

Anılan yasa, federe devletler arasında ve uluslararası ticarette kullanılan elektronik imza ve elektronik kayıtları kapsamaktadır. Her federe devletin kendi içindeki ticarette geçerli olan hukuk ise o federe devletin kendi elektronik imza yasası ile düzenlenmektedir. Dolayısıyla, federal yasanın sadece uluslararası ticaret ve federe devletler arasındaki ticaret açısından kural getirmesi, bu konudaki hukuk boşluğunu doldurmaktadır [54].

Anılan yasa, ticari ilişkilerde elektronik imza ve elektronik kayıtların kullanılmasını kabul etmekte ve bu araçlara hukuken meşruluk kazandırmaktadır. Elektronik imza, bir sözleşmeye veya diğer herhangi bir kayda eklenen veya mantıksal olarak sözleşme veya kaydın parçası olan, kişi tarafından o kaydı imzalama iradesi ile uygulanan veya kabul edilen elektronik ses, sembol, veya uygulama olarak tanımlanmaktadır [55].

Sözkonusu yasaya göre, diğer herhangi bir yasa, düzenleme veya diğer bir hukuk kuralı ile bağlı olmaksızın, elektronik formdaki bir imza, sözleşme, veya diğer herhangi bir kaydın hukuki etkisi, geçerliliği ve uygulanabilirliği, sadece elektronik biçimi ileri sürülerek reddedilemez, aynı şekilde, bir sözleşmenin hukuki etkisi, geçerliliği ve uygulanabilirliği, sadece elektronik imza ile oluşturulduğu ve elektronik kayıt kullanıldığı ileri sürülerek reddedilemez .

Ayrıca ABD'de sayısal imza ile ilgili eyaletler bazında yasal düzenlemeler bulunmaktadır. Bunlardan birisi, New York eyaletinin 5 Ağustos 1999 tarihinde kabul ettiği "State Tecnolog Law" dır. Diğerleri ise California ve Pennsylvania'da yürürlüğe giren; Temmuz 1999 tarihli "Uniform Electronic' tir [9].

ÜÇÜNCÜ BÖLÜM

3. ULUSLARARASI ELEKTRONİK TİCARET POLİTİKASI KONULARI VE TEŞEBBÜSLERİ, TÜRKİYE' DE YÜRÜTÜLMEKTE OLAN ELEKTRONİK TİCARET ÇALIŞMALARI

3.1 Elektronik Ticaret ile ilgili izlenmekte olan Uluslararası politika teşebbüsleri

Elektronik ticaretle tüm boyutlarıyla ilgilenen bir kuruluş olmamakla beraber, bazı uluslararası kuruluşlar elektronik ticaretle ilgili zorlukları tanımlamak, çözümler üretmek, özel konularda işbirliği içerisinde çalışmak konusunda dikkate değer çabalar göstermektedir (Çizelge 3.1) [56]. Ulusal hükümetler bu konuya yönelik çalışmalarını varolan uluslararası kuruluşlar vasıtasıyla sürdürmekle beraber hükümetdışı organizasyonlar ve diğer gruplarla birlikte elektronik ticaretin uluslararası boyutlarını inceleyen çalışmalar yapmaktadırlar. Bu çabaların merkezinde teknik işlerliği sağlama hususunda özel sektörün oynamakta olduğu artan rol yer almakta olup özel sektör geleneksel olarak hükümetlere ait olan fonksiyonları da üstlenmektedir.

Elektronik ticaretle ilgili olarak kamu ve özel sektörün yer aldığı çok taraflı çalışmalar; fonksiyonel kuruluşlar, bölgesel ve uluslararası koordinasyon kuruluşları, kar amacı gütmeyen kuruluşların ortakları olan yeni gruplar vasıtasıyla yürütülmektedir [56]:

- WTO, ITU, UNCITRAL ve WIPO gibi uluslararası fonksiyonel kuruluşlar varolan politikaları elektronik dünyaya uyarlamaya çalışmaktadırlar.
- OECD, UNCTAD, Avrupa Birliği, Asya Pasifik Ekonomik İşbirliği (APEC) ve Amerika Serbest Ticaret Bölgesi (FTAA) gibi Bölgesel ve Uluslararası koordinasyon kuruluşları çeşitli elektronik ticaret konularını adreslemektedir.

Çizelge 3.1 E-Ticaret Konularını adresleyen Uluslararası Kuruluşlar

	Yardım	Ticaret	Vergilendirme	Elektronik İmzalar	Mülkiyet Hakları	Standartlar	Güvenlik	Gizlilik	Tüketicinin Korunması	İçerik	Eğitim
WTO			X								
ITU						X	X				
UNCITRAL				X							
UNCTAD											X
UNESCO								X	X		X
Dünya Bankası	X										X
WIPO					X						
OECD			X	X			X	X	X		X
APEC											X
FTAA				X							X
AB				X		X	X	X	X	X	X
ICANN					X	X					
W3C						X		X		X	
IETF						X					

Kaynak: Institude of International Economics [57]

- Hükümetlerin, şirketlerin, ve kar amacı gütmeyen kuruluşların ortakları olan yeni gruplar. Bunlar arasında GBDe, ICANN ve W3C sayılabilir.

Bu grupta yer alan bazı kuruluşların bazıları resmi bir işbirliği olmaksızın düşünce temelindeki ortak payda ve muhtemel yaklaşımlar bakımından paralel ilgilere sahiptirler. Bu ise yasal çerçeve ve güvenli çevre ile ilgili pek çok konu için doğrudur. Gizlilik, kişisel verilerin korunumu gibi diğer konular sosyal değerler ve politika yapıcı hükümet yaklaşımları bakımından ileri farklar getirdiğinden dolayı bu kadar tesadüfi şekilde ele alınmamıştır. Bu bölümde uluslararası elektronik ticaret politikası konuları ve teşebbüsleri detaylı bir şekilde açıklanmaktadır.

3.1.1 Fonksiyonel Kuruluşlar

Uzmanlaşmış kurumların ilk grubu olan fonksiyonel kuruluşlar varolan kurallar ve politikaları elektronik dünyaya uyarlamaya çalışmaktadır. Bunların arasında ITU, UNCITRAL ve WIPO bulunmaktadır. İşçevrelerinin birbirleriyle ve müşterileri arasındaki çoğu yasal ve ticari kod internetten önce

kurulmuştur ve bu iş çerçevelerinin yeni realiteleri kapsayacak şekilde yeniden gözden geçirilmesine ihtiyaç duyulmaktadır. Bu kurumların amaçları ticari kuralları sayısal dünyaya uyarlamak eğer aynı değilse, fiziksel dünyaya yakın bir eşdeğerini bulmaktır. Çoğu alandaki varolan prensipler ve disiplinler canlı kalmaktadır.

Öte yandan, internet ve elektronik ticaretin ekonomik ve sosyal alanda getirdiği yenilikler vergi rejimleri gözönüne alındığında gerilimi arttırıcı bir unsur olarak karşımıza çıkmaktadır. Gerilimin arttıran kuruluşların arasında şüphesiz Dünya Ticaret Örgütü (World Trade Organisation-WTO) gelmektedir.

3.1.1.1 Birleşmiş Milletler Bünyesinde Elektronik Ticaretle İlgilenmekte olan Fonksiyonel Kuruluşlar

3.1.1.1.1 Uluslararası Telekomünikasyon Birliği (ITU)

Hükümetler ve özel sektör arasında küresel telekomünikasyon şebekeleri ve servislerinin koordinasyonunu sağlayan uluslararası bir kuruluş olan Uluslararası Telekomünikasyon Birliği (ITU), küresel bilgi altyapısının mimarisinin standartlarını, kamu anahtarlamalı telefon şebekesi ve internet protokolü şebekelerinin entegrasyonunu da içerecek şekilde yürütmektedir. ITU elektronik ticaret, multimedya terminalleri için haberleşme sistemi, elektronik ticaretle ilgili altyapı ve güvenlikle ilgili standartlarının geliştirilmesi, telekomünikasyon reformu ve regülasyonun elektronik ticaretle ilgili rolü ile ilgili bilincin geliştirilmesi ve gelişmekte olan ülkelerde elektronik ticaret altyapısı ve servislerinin geliştirilmesi hizmetinin verilmesi konuları ile ilgili çalışmaları yürütmektedir [58].

3.1.1.1.2 Birleşmiş Milletler Uluslararası Ticaret Yasası Komisyonu (UNCITRAL)

Elektronik ticaretle ilgili çalışmaları gerçekleştiren uluslararası organizasyonlardan birisi de Birleşmiş Milletler Uluslararası Ticaret Yasası

Komisyonudur (UNCITRAL). UNCITRAL 1996 yılında ülkelere yardımcı olmak amacıyla haberleşmenin ve bilgi depolamanın kağıda dayalı metotlarına alternatiflerin kullanımını sağlayacak yerel kanunları kurmaya yardımcı olmak için elektronik ticaretle ilgili bir model yasa kabul etmiştir. Model yasa ulusal yasalar üzerinde özel bir etkiye sahip olmuş yasal kısıtlamaların azaltılmasını sağlayarak elektronik ticaret için daha güvenli bir ortamın tesisini sağlamıştır. Bir çok ülke ABD dahil 1999'da Milenyum Sayısal Ticaret Yasasını Kongresinden geçirerek UNCITRAL Model Yasası'nın prensiplerini yerel yasalarına dahil etmiştir. Buna ek olarak UNCITRAL'ın elektronik ticaretle ilgilenmekte olan çalışma grubu elektronik imzalar ve sertifikasyon otoriteleriyle ilgili konuları adreslemektedir. Elektronik İmzalar ile ilgili taslak kalıcı kurallar sayısal imzalar ve elektronik imzaların yasal olarak tanınması temelinde elektronik imzaların bir dizi standartlara göre tasarlanmıştır. Taslak kurallar ayrıca sertifikaların yasal olarak tanınmasını sağlayacak olan sertifikasyon otoriteleri tarafından yerine getirilecek standartları ve güvenli sertifikaların küresel seviyede karşılıklı tanınma ihtiyacını adreslemektedir [55].

3.1.1.1.3 Birleşmiş Milletler Ticaret ve Kalkınma Konferansı (UNCTAD)

Ticaret ve kalkınma konularıyla ilgilenen Birleşmiş Milletler'in bir kuruluşu olan Birleşmiş Milletler Ticaret ve Kalkınma Konferansı (UNCTAD) sürdürmekte olduğu çalışmalarını gelişmekte olan ülkelerde elektronik ticaretin faydaları ile ilgili bilinci arttırma çabalarına yöneltmiştir. 1998 ve 1999 yılları arasında düzenlenmiş olan bir dizi "Elektronik Ticaret ve Kalkınma" semineri ve bölgesel toplantısında elektronik ticaretle ilgilenen kuruluşlar, hükümetler ve işçevreleri arasındaki altyapının güçlendirilmesine yönelik işbirliğinin geliştirilmesi amaçlanmıştır. UNCTAD'ın adreslediği faaliyetler arasında gelişmekte olan ülkelerde elektronik ticaretle ilgili bilgilerin yayılması ve elektronik ticaretin getirdiği ekonomik, sosyal ve yasal yaptırımlarla ilgili eğitim faaliyetleri ve analitik çalışmalar bulunmaktadır [59].

3.1.1.1.4 Birleşmiş Milletler Eğitim Bilim ve Kültürel Kuruluşu (UNESCO)

Birleşmiş Milletler Eğitim Bilim ve Kültürel Kuruluşu (UNESCO) siberuzayın toplumsal, ahlaki, yasal yönlerini değerlendiren bir projeyi yürütmektedir. Bu bağlamda bir dizi prensip kabul etmiş ve siberuzay, ahlaki unsurlar, gizlilik ve kripto konularında bazı toplantılar düzenlemiştir. Gündeminde OECD ile ortak çalışmalar, gizliliğin ve şifrelemenin korunması ile ilgili uluslararası yaklaşımlar, internetin yasal olmayan unsurlarından çocukları korumak için gerekli tedbirleri almak ve eğitim teşebbüsleri gibi konular yer almaktadır. UNESCO ayrıca gelişmekte olan ülkelere eğitim ve bilim hizmeti verecek yazılım ve donanım, teknik ve mali yardımlar sağlamaktadır [60].

3.1.1.1.5 Dünya Ticaret Örgütü (WTO)

1995 yılında kurulan Dünya Ticaret Örgütü özellikle haberleşme hizmetleri için piyasaların liberalizasyonu ve yeniden düzenlenmesi konusundaki çalışmaları yürüten bir uluslararası kuruluş olarak öne çıkmıştır. Dünya Ticaret Örgütünün 13 Aralık 1996'da Singapur'da imzalanan Bilgi Teknolojisi Ürünleri Ticareti Bakanlar Deklarasyonu, bilgi teknolojisi ürünlerinde dünya ticaretinin % 80'ini gerçekleştiren Avrupa Birliği ve 13 ülkede gümrük vergilerinin 2000 yılına kadar azaltılmasını bu ülkeler açısından zorunlu hale getirmiştir [61].

15 Şubat 1997 tarihli Dünya Ticaret Örgütü Anlaşması, tüm haberleşme biçimlerini kapsamakta ve haberleşme alt yapısını internet'in gelişimi için önemli bir ölçüt olarak değerlendirmektedir.

Dünya Ticaret Örgütü'nün e-ticareti ilgilendiren Hizmet Sektörlerinde Ticarete İlişkin Genel Anlaşması (The General Agreement on Trade in Services-GATS) ve Fikri Mülkiyet Haklarının Ticaretle İlgili Boyutları (The Trade Related Aspects of Intellectual Property Rights-TRIPS) isimli uluslararası anlaşmaları bulunmaktadır.

WTO elektronik ticaretle ilgili yürüttüğü çalışmalarda yerel ve küresel elektronik ticaret için gerekli olan altyapı konuları ve ticaretle ilgili yönlerle ilgilenmiştir.

Elektronik ticaretle ilgili olarak WTO'nun yapısındaki (GATT ve GATS ve alt komiteleri) ve üyelerinin faaliyetlerindeki süregelen değişiklikler bazı zorluklara sebep olmuştur. Küresel ticaret faaliyetlerini adresleyen bir kuruluş olan WTO ülkelerin elektronik ticaretle ilgili yerel ve sınırlar arası yönlerden yaklaşımlarının paylaşıldığı ideal bir bilgi değişim merkezidir [62].

Elektronik ticaret hızla geliştiğinden 1998 Bakanlar anlaşması internet üzerinden gönderilen ürünler için gümrük işlemleri için geçici morotoryum kabul etmiştir. Ayrıca, elektronik ticaretin ticaretle ilgili yönlerini içeren kapsamlı çalışma programlarına başlamışlardır. Mallar Konseyi, Servisler Konseyi, TRIPS Konseyi, Ticaret ve Kalkınma Komitesi Olarak dört ayrı çalışma grubu Genel Konsey tarafından koordine edilmiştir.

Varolan WTO Kuralları elektronik olarak alınan ve fiziksel olarak dağıtılan ürünlere uygulanabilir görünmektedir. Öte yandan internet üzerinden indirilen ve CD gibi fiziki bir kopyası bulunmayan müzik eserleri için ne söylenebilir? Bu ürünler GATS ve GATT'ın kapsamına girmekte midir? Genel Konseyin çalışma programı elektronik ticaretle ilgili bir takım konuların aydınlatılmasını sağlamıştır. Kasım 1999 Seattle Bakanlıklar Konferansı ticaretle ilgili yeni konuların tartışılmasını sağlayamamış, elektronik ticaretle ilgili konuları çözümsüz bırakmıştır. Konferans sonrasında WTO ülkeleri arasında elektronik ticareti kısıtlayacak olan yeni engeller konulmaması kararı alınmıştır.

Daha geniş olarak WTO elektronik ticaretin gelişimini sağlayacak olan servis sektör altyapısını ve liberalizasyonu adresleyerek yardımcı olmuştur. Tarifeler ve bilgisayarlarla ilgili kısıtlamalar bilgi teknolojileri anlaşması (ITA) altında yer almış ve ürünlerin dağılımı ITA-2 programı ile genişletilmiştir. Temel

telekomünikasyon anlaşması telekomünikasyonun liberalizasyonu ile ilgili taahütler içermektedir. Mali servisler mali servisler anlaşmasında yeralmaktadır. Dağıtım sistemleri, ticaretle ilgili ölçüler (TRIMS) altında ve iletim servisleri GATS 2000 içerisinde incelenmiştir. Elektronik ticaretten ekonomik yarar sağlanması servis sektörleri arasındaki sinerjiye bağlıdır.

Elektronik ticaretin ekonomik ve sosyal önemi ve elektronik ticarete ve onun dayandığı altyapıya küresel erişimin sağlanmasında WTO üyelerinin elektronik ticaretin liberalizasyonunu maksimum seviyede gerçekleştirilmesi temel teşkil etmektedir [63].

3.1.1.1.6 Dünya Fıkri Mülkiyet Hakları Kuruluşu (WIPO)

Birleşmiş Milletler'e bağlı bir kuruluş olan Dünya Fıkri Mülkiyet Hakları Kuruluşu (WIPO) siberuzayda elektronik olarak gönderilen verilerin telif haklarının korunması, ses kayıtlarının çoğaltılmasının etkin korunumu için gerekli müzakereleri düzenleyen bir forumdur.

WIPO edebiyat ve sanatsal çalışmaları koruyan Bern Anlaşması ve sınai mülkiyeti Koruyan Paris Anlaşması aracılığıyla fikri mülkiyet konusunu düzenlemektedir. WIPO Genel Kurulu, bünyesindeki uluslararası bürosunu yeni küresel bilgi altyapısının ve internetin uluslararası fikri mülkiyete etkisini araştırmakla görevlendirmiştir. Bu çalışmada ilk hedef, ticari markalarla internet alan adları (domain names) arasındaki ilişkiyi bulmaktır. WIPO 1996 yılında iki önemli anlaşma daha hazırlamıştır: On-line sayısal materyalleri, veri tabanlarını ve bilgisayar programlarını koruyan Telif Hakları Sözleşmesi ve sayısallaştırılarak çevrimiçi ortama aktarılan müzik eserleri, sanatsal ürünleri ve video eserlerini koruma altına alan İcracı Sanatçı ve Fonogram Yapımcıları Anlaşması. Her iki anlaşma da, çevrimiçi sayısallaştırılmış haberleşmelerin internet üzerinden ticari uygulamalarını kolaylaştırmaktadır. [64].

Varolan anlaşmaların uygulanması WIPO için bir öncelik olmuş ve gelişmekte olan ülkeler için özel çabalar amaçlanmıştır. 1999'da bir dizi bölgesel toplantılar düzenlenmiş böylelikle WIPO'nun sayısal gündemi geliştirilmiştir [65].

3.1.1.1.7 Dünya Bankası (IMF)

Dünya Bankası gelişmekte olan ülkelerin ve ekonomilerinin internet ve bilgi toplumuna geçişi konusuna yoğunlaşmıştır. Dünya Bankası özellikle hükümetlerin bilgi tabanlı faaliyetlerinde özel sektörden gerekli kaynak ve tecrübenin birincil olarak altyapı ve bilgi haberleşmenin kırsal kesimlere sağlanması çabalarını desteklemektedir.

Dünya bankasının Bilgi ve Kalkınma Programı (İnfoDev) elektronik ticaret tarafından sağlanan ekonomik gelişmenin avantajlarını yakalamaları için ülkelere danışmanlık ve kredi sağlamaktadır. Dünya Bankası ülkelere haberleşme ve bilgi şebekelerinin geliştirilmesi, internet kullanımının geliştirilmesi için kapsamlı teknik yardım, eğitim ve fon sağlamaktadır. Elektronik ticaretin geliştirilmesi için düzenlenmiş olan konferans ve fuarlar küresel bağlanabilirlik, pazarın liberalizasyonu, üzerinde yoğunlaşmıştır. Programlar ise ülkelerdeki sayısal teknolojinin tesisindeki temel kuralların tesisini amaçlamaktadır [66].

3.1.2 Bölgesel ve Uluslararası koordinasyon kuruluşları

3.1.2.1 İktisadi İşbirliği ve Kalkınma Teşkilatı (OECD)

OECD, üyesi olan ülkelere karşı herhangi yasal bir yaptırım gücü ve finansman sağlama imkanları olmayan, daha çok güncel konularda küresel politikalar geliştirilmesi amacıyla işbirliğini sağlamakla yükümlü bir kuruluştur. OECD'nin Bilgi, Bilim ve Teknoloji Müdürlüğü'ne ("Directorate for Science, Technology and Industry-DSTI") bağlı, ilgili hükümetlerin temsilcilerinden oluşan Bilgi, Bilgisayar ve Haberleşme Politikası Komitesi ("Information, Computer and Communications Policy Committee-ICCP") bünyesinde

"Küresel Bilgi Altyapısı-Küresel Bilgi Toplumu" konusunda üye ülkeleri yönlendirecek tavsiyeler hazırlanmıştır [4].

OECD bünyesinde 1992'de "Bilgi Sistemlerinin Güvenliği İlkeleri (Guidelines on Security of Information Systems)", 1997 yılında ise tüm üye ülkelerce kabul edilen "Şifreleme Politikası (Cryptography Policy)" hazırlanmıştır. Tüketicilerin korunması konusunda ise yine 1997 yılında "Guidelines on Consumer Redress:Chargebacks" adlı doküman hazırlanmıştır. 1985 yılında tüm üyelerce onaylanan "Sınır Ötesi Veri Akışı Deklarasyonu (Declaration on Transborder Data Flow)", ülkelerin ekonomik bağımlılıkları nedeniyle uluslararası bir boyut kazanan veri akışı konusunda temel bir yaklaşım oluşturmuştur. Bilgisayarlardaki verilerin uluslararası ölçekte serbest dolaşımının gerekli olduğunu kabul eden üye ülkeler, kendi ulusal çıkarlarını gözönünde tutarak, veri, bilgi ve ilgili hizmetlere erişimin desteklenmesi ve buna yönelik haksız engellerin kaldırılması; bilgisayar ve haberleşme hizmetlerine yönelik politika ve düzenlemelerin açıklığını sağlayacak yönde birlikte çalışmaya niyetli olduklarını belirtmişlerdir [4].

OECD, 21. yüzyılın en önemli ekonomik gelişmelerinden biri olarak nitelendirdiği e-ticaretin başka yönleri üzerinde de çalışmalarını sürdürmektedir. OECD E-ticaret alanında uluslararası politika birliği sağlanması amacıyla, G7 Bilgi Toplumu Bakanlar Konferansı (Şubat 1995-Brüksel) ve Küresel Bilgi Ağları Bakanlar Konferansları'na (Temmuz 1997-Bonn) ilaveten 4 adet konferans düzenlemiştir [67].

3.1.2.2 Avrupa Birliği

Avrupa Birliği, e-ticaret konusunda en yoğun çalışmaları yapan kuruluşların başında gelmektedir. Avrupa Komisyonu, Avrupa'nın tamamını içine alacak bir ağın ve bunun bir alt parçası olan iletişim ağının, tek pazar esasına dayalı olarak Topluluğun ekonomik ve sosyal açıdan güçlendirilmesi ve Avrupa ve dünya çapında bir bilgi toplumu oluşturulması açısından önemli olduğunu düşünmektedir. 1980'lerin başından bu yana Avrupa Birliği, Avrupa - Ağı

kapasitesini geliştirmek amacıyla araştırma ve geliştirme ağırlıklı programlar düzenlemekte bu kapsamda elektronik data transmisyonu (EDI) sistemlerine ve belirgin olarak da TEDIS (Trade EDI System) girişimine destek vermektedir. 1994'de Avrupa Komisyonu'nun isteği ve bilişim teknolojileri sektöründen önemli şirketlerin desteği ile Avrupa bilişim altyapısını geliştirmek üzere 10 konuda hedef uygulama çalışmaları başlatılmıştır. Çalışmalardan dördü (KOBİ'ler için Telematik Servisleri, Elektronik Sunum, Avrupa Kamu Yönetimi Ağı ve Şehir Bilgi Ağı) e-ticaretle doğrudan ilişkilidir [68].

Avrupa Komisyonu, e-ticaret konusundaki çalışmaları örgütlemek amacıyla kendi altında açtığı birimler arasında bir görev dağılımı yapmıştır. E-ticarete yönelik AR- GE programlarının büyük bir bölümü 'DGXIII'e kayıtlıdır. Bu programlar, "Avrupa için Güvenli Elektronik Pazar" oluşturulmasına ve bütün e-ticaret çevrimini kapsayan güvenlikli genel modellemeye (secure generic modelling) yöneliktir [69].

Birlik, araştırma, teknoloji ve geliştirme faaliyetlerini düzenleyen 4. Çerçeve Program'da ve 1998-2002 yılları için uygulamaya alınan 5. Çerçeve Programın'da Bilgi Toplumuna geçişin sağlanmasını öncelikli alanlardan birisi olarak belirlemiştir. 2002-2006 yılları için uygulanacak olan 6. Çerçeve Programında da sözkonusu alana özel önem verilmektedir.

AB Komisyonu'nun 1997'de hazırladığı bildirimle e-ticaret planını yayımlamıştır. Bu planın amacı, AB için bir çatı planı oluşturmaktır. Avrupa'da bu konuda oluşan görüşleri derleyip toparlamak ve global bir konsensüs arama ve oluşturmaktır [70]. Birliğin temel hedefinin e-ticaretin Avrupa'da hızla gelişmesini sağlamak olduğu belirtilmiş ve e-ticaretle ilgili çalışmalarda birbirini tamamlayıcı iki hedef belirlenmiştir. Bunlar, e-ticarete güveni oluşturmak ve Tek Pazara tam olarak girilmesini sağlamaktır.

Avrupa Birliği elektronik ticaretle ilgili olarak gizlilik, elektronik imza ve tüketici haklarını içeren geniş bir boyutta ilgilenmekte ve ayrıca araştırma ve teknoloji

programlarına sponsor olmaktadır. Avrupa Birliği 1997 yılında elektronik ticaretin geliştirilmesine yönelik bir dizi önerge kabul etmiştir. Elektronik Ticaret için bir Avrupa İnsiyatifi (A European Initiative in Electronic Commerce [COM[97]0157]) belgesi küresel pazara erişim, yasal ve düzenleyici konular ve uygun iş çerçevesi olmak üzere üç konuyu adreslemektedir. Bu iş çerçevesinin oluşturulmasına yönelik olarak Avrupa Komisyonu Aralık 1999'da eAvrupa [70] İnsiyatifini başlatmıştır. 23-24 Mart 2000 tarihlerinde Lizbon'da yapılan Avrupa Konseyi toplantısında, 15 AB ülkesinin Hükümet ve Devlet Başkanları, Avrupa'nın gelecek onyılda "dünyadaki en rekabetçi ve dinamik bilgi tabanlı ekonomisi" haline gelmesi hedefini koymuşlardır. Bu hedef, Avrupa'nın bir an önce bilgi tabanlı ekonominin, özellikle de internetin sağladığı fırsatlardan sonuna dek yararlanması gerekliliğini ortaya çıkarmıştır. Bu gerekliliğe yanıt olarak, 19-20 Haziran 2000 tarihinde Feira'da eAvrupa Eylem Planı kabul edilmiştir [71].

Bu plan ile; ekonomik, parasal ve siyasal bir birlik olan Avrupa'nın aynı zamanda "Bilgi Toplumu Birliği" olması hedeflenmektedir. Gerek Avrupa Birliği'nin içindeki bölgesel dengesizlikleri gidermek, gerek Amerika'nın yeni ekonomiyle hızlı bir büyüme gerçekleştirmesi, Uzak Doğu ülkelerinin - özellikle Singapur ve Malezya'nın- teknoloji yatırımlarını ön plana çıkarması ve buna bağlı olarak rekabet avantajı kazanmaları, gerekse; Avrupa Birliği'nin rakiplerinden biri olan Japonya'dan teknoloji ve rekabet alanlarında geri kalmak istememeleri ve yapılan araştırmalarda Avrupalıların interneti pek fazla kullanmadıklarına ilişkin sonuçları; Avrupa Birliği'ne üye ülkeler arasında bir eAvrupa Eylem Planı hazırlamayı gerekli kılmıştır. eAvrupa Eylem Planının yürürlüğe girme tarihi (2001); üye ülkelerin telekomünikasyon altyapısının tamamlanması ile çakışmaktadır. Avrupa Birliği, bu girişimden hareketle 2010 yılında ABD'den daha ileri bir bilgi toplumu olmayı hedeflemektedir[72].

Özellikle Amerika kadar internetten yararlanamamaları Avrupa Birliği'nde yukarıda belirtildiği gibi bir girişimi gerekli kılmış ve bu amaçla 19-20 Haziran

2000 tarihlerinde eAvrupa Eylem Planı kabul edilmiştir. Plan; daha ucuz, daha hızlı ve daha güvenli bir internet, insanlara ve yeteneklere yatırım ve internet kullanımını teşvik edip arttırmak olmak üzere üç temel hedeften oluşmaktadır[72].

Teması; her yaşta herkesin, her yerden internete ulaşmasını, elektronik ortamda ticaret yapmasını, ve devlet yapısını, okulları elektronik ortama taşımak olan eAvrupa Eylem Planının amacı; Avrupa Birliği'ni e-devletler (elektronik devletler) başlığı çerçevesinde siyasal bir çatı altında toplamaktır. eAvrupa Eylem Planı'nın nihai hedefi ise; başlangıçta da belirtildiği gibi "Avrupa Bilgi Toplumu" oluşturmaktır.

eAvrupa Eylem Planı ile; Avrupa Birliği, sadece siyasi, ekonomik, parasal bir entegrasyon olmaktan öteye; bilgi toplumlarının ortak paydada buluştuğu bir iktisadi sisteme doğru ilerlemiş olacaktır. 2003 yılında tamamlanması öngörülen eAvrupa Eylem Planı, dört (4) ana başlık altında toplanan, ondört (14) hedef içermektedir:

"0. Bilgi toplumunun temel yapı taşlarını oluşturma çalışmalarının hızlandırılması
a) Herkes için uygun fiyatlı iletişim hizmetlerinin sağlanması
b) Bilgi toplumu ile ilgili müktesebata uyum ve uygulama

1. Daha ucuz, daha hızlı, daha güvenli internet
a) Daha ucuz ve daha hızlı internet erişimi
b) Araştırmacılar ve öğrenciler için daha hızlı internet
c) Güvenli ağlar ve akıllı kartlar

2. İnsan kaynağına yatırım
a) Avrupa gençliğinin sayısal çağa hazırlanması
b) Bilgi tabanlı ekonomide iş gücü

c) Bilgi tabanlı ekonomiye herkesin katılımı

3. İnternet kullanımının canlandırılması
a) E-ticaretin hızlandırılması
b) Elektronik devlet: Kamu hizmetlerine elektronik erişim
c) Çevrimiçi sağlık
d) Küresel ağlar için Avrupa sayısal içeriği
e) Akıllı ulaşım sistemleri
f) Çevrimiçi çevre."

eAvrupa Eylem Planı'nda İnternetin daha ucuz ve hızlı olmasıyla herkesin, her yerden internete ulaşması hedeflenmektedir. Özellikle araştırmacılar ve öğrenciler için hızlı internet hedefi, araştırma ağlarının geliştirilmesini sağlamaya yöneliktir. Güvenli ağların sağlanması ise; internetin gelişimi açısından oldukça büyük bir öneme sahiptir. Yapılan araştırmalar, internetin gelişimi önündeki en önemli engelin "güvenlik" olduğunu göstermektedir. Bu noktadan hareketle Avrupa Birliği de güvenlik konusu üzerinde hassasiyetle durmaktadır[73].

Eylem planında üzerinde durulan diğer bir nokta ise; insan kaynağına yatırım yapmanın gerekliliğidir. İnsan kaynağına yatırım çatısı altında, bilgi tabanlı bir ekonomide artık kas gücünün değil; beyin gücünün artı değer yarattığı bilinciyle Avrupa gençlerinin sayısal çağa hazırlanmaları için tüm okulların internete bağlanmaları, 7'den 70'e herkesin internetten yararlanması öngörülmektedir.

Dördüncü hedef olan internet kullanımının özendirilmesi ise; elektronik ticaretin hızlandırılması, e-devlet, çevrimiçi sağlık, küresel ağlar için Avrupa'nın sayısal içeriği ve akıllı ulaşım sistemleri olmak üzere beş alt başlıktan oluşmaktadır. Avrupa Birliği, yeni ekonominin ve internetin getirdiklerinden yeterli ölçüde yararlanmayı amaçlamaktadır.

Örneğin; "Avrupa Birliği elektronik ticaret alanında KOBİ'lerin desteklenmesi amacıyla başlattığı "Go Digital" girişimine bilgilendirme kampanyasıyla hız kazandırmıştır. Go Digital girişimi AB kapsamındaki çeşitli fonları kullanarak KOBİ'lerin işlerini elektronik dünyaya taşımayı hedeflemektedir. " Aynı zamanda web üzerinden daha fazla Avrupalıya (farklı Avrupa dilleriyle) ulaşmak amacıyla elektronik içerik ("e-content") oluşturmuş ve böylelikle küresel ağlarda Avrupa'ya sayısal içerik kazandırmayı hedeflemektedir. Bunun yanı sıra, internetteki Avrupa Birliği alan adının (.eu) alt alan adlarının (.press.eu, .ngo.eu, .media.eu) oluşturulmasına hız verilmiştir. Küresel araştırma ağlarının yaygınlaştırılması için Géant Projesi başlatılmıştır. Projenin amacı; Avrupa'daki araştırma ağlarını birbirlerine bağlamak ve hızlarını arttırmaktır[73].

Tüm bu on dört hedefi sağlamak amacıyla aktörler Avrupa Parlamentosu, Avrupa Komisyonu, Avrupa Konseyi, Avrupa Yatırım Bankası, üye ülkeler, kamu ve özel sektör, standart organizasyonları ve sosyal taraflar olarak belirlenmiştir.

Tüm bu hedeflerdeki gelişmeleri; Avrupa'nın sayısal olarak nereden nereye geldiğini saptamak amacıyla da elektronik ticaret hacmi, internet üzerinden verilen kamu hizmetlerinin oranı, okulların internete erişim oranı gibi toplam yirmiüç (23) ölçüm kriteri belirlemiştir. Avrupa Birliği üye ülkeleri bu kararı alırken; Birliğe aday ülkeler (Türkiye, Malta ve Güney Kıbrıs Rum Yönetimi) de bu oluşumun bir parçası olabilmek amacıyla 24 Ekim 2000 tarihindeki V. JHLC Toplantısında eAvrupa Eylem Planına benzer bir eylem planı hazırlama kararını almışlardır. 13-14 Mart 2001 tarihinde yapılan VI. JHLC Toplantısında "eAvrupa Benzeri Eylem Planı" diye adlandırılan planın, "eAvrupa+ Eylem Planı" olarak adlandırılmasına karar verilmiştir. eAvrupa+ Eylem Planı, eAvrupa Eylem Planına ek olarak iki maddeyi; - Bilgi toplumunun temel yapı taşlarını

oluşturma çalışmalarının hızlandırılması ve çevre içermektedir.

Tüm Avrupa'da uygulanacak uygun yasal bir çerçeveyi yaratmaktır. Birlik bunun yanında bilginin korunması, veritabanlarının yasal korunması ve uzaktan yapılan sözleşmelerle ilgili direktiflerde e-ticaretin gereksinimlerini gözönünde tutmuştur. Ayrıca değişik politika alanlarındaki tartışmaları canlandırmak için bir dizi danışma ve politika belgeleri yayımlamıştır. Bu alanlar, şifrelenmiş hizmetlerin yasal korunması, telif hakkı ve bağlantılı haklar, endüstriyel mal, ticari haberleşmeler, kamu ihaleleri ve işitme-görme ve bilgi hizmetlerinde küçüklerin ve insan saygınlığının korunmasıdır [4].

E-ticareti düzenleyecek yasal bir çerçevenin ana çizgileri şu şekilde belirlenmiştir:

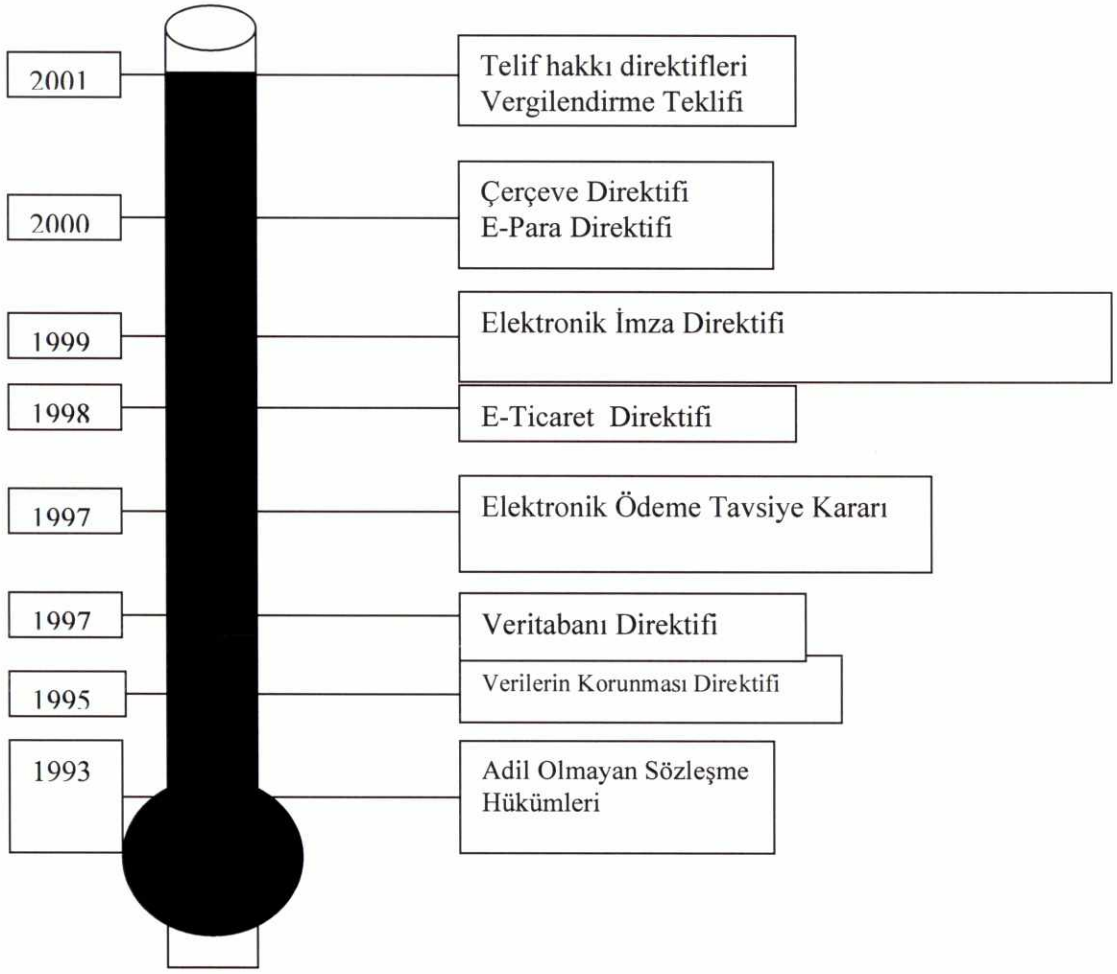
- Düzenlemenin yararı için aşırı düzenleme yapılmamalıdır
- Her düzenleme Tek Pazar özgürlüklerine dayanmalıdır
- Her düzenleme iş hayatının gerçeklerini dikkate almalıdır
- Her düzenleme genel çıkar hedeflerini etkin ve verimli bir biçimde karşılamalıdır.

Avrupa Komisyonu, temiz ve tarafsız bir vergi ortamı yaratmak isteğini beyan etmiştir. Bu itibarla, e-ticaretin gelişebilmesi için vergi sistemlerinde açık, tarafsız ve önceden bilinen bir ortam oluşturmanın ve yasal kesinliği sağlamanın önemi kabul edilmekte ancak bu konuda yapılacak düzenlemelerin, geleneksel ticaretle karşılaştırıldığında ek yükler getirmemesi gerektiği belirtilmektedir. Ayrıca hali hazırda uygulanan KDV üzerinde e-ticaret yüzünden oluşabilecek muhtemel olumsuzlukların mutlaka tespiti ve "bayt vergisi" olarak nitelendirilen verginin kesinlikle kabul edilmemesi görüşlerini de beyan etmişlerdir [74].

Avrupa Komisyonu, e-ticaretin küresel düzeyde gelişimi için, Tek Pazar'da e-ticaretin çeşitli bölümleri için yapılacak düzenlemelerin (şifreleme, sayısal

imza, bilgi güvenliği ve gizliliği, sözleşme yasası, yeni elektronik ödeme araçları gibi) uluslararası işbirliğini içeren düzenleyici bir çerçeve içinde oluşturulması gerektiğini düşünmektedir [4].

Avrupa Birliği'nde e-ticaretle ilgili olan düzenleyici çerçeve aşağıdaki şekille özetlenebilir [74]:



Şekil 3.1 ; e-ticaretle ilgili düzenleyici çerçeve [75]

Çizelge 3.2 e-Ticaretle ilgili düzenleyici çerçeve [70]

İsim	Özet	Resmi Dokümantasyon
Telif Hakları Direktifi 2001/29/EC [76]	İnternetteki telif hakları ile ilgili kuralları telif hakkı sahiplerini korumak için düzenlenmektedir. Sözkonusu direktif telif hakkı sahiplerine internet korsanlığına karşı kendilerini korumaları için digital dosyaların yasadışı olarak yüklenmesini önleme hakkını ve digital dosyaların çoğaltılmasının önlenmesi için şifreleme yönteminin kullanılması imkanını vermektedir.	Komisyonun 22 Mayıs 2001 tarihindeki Telif Hakları ve Bilgi Teknolojileri topluluğu ile ilgili hakların harmonizasyonunun temel yönleri ile ilgili olan Direktifi
388/77/EEC [77], COM (2001) 400 Direktifinde değişiklik yapan Vergilendime Teklifi	Tarafsız ve net bir vergi çevresinin yaratılması ve pazarın bozulmasını önleyecek vergi kurallarının uygulanması için elektronik ticaretin gelişimine imkan verilmesi için yasal kesinliğe sahip vergi sisteminin olması gerektiğini belirterek İdari İşbirliği konusundaki dolaylı vergilendirmenin (VAT) elektronik ticaret için uygun bir vergi türü olduğunu vurgular	İdari işbirliği hususundaki dolaylı vergilendirme (VAT)(ECC) No 218/92'de değişiklik yapan teklif ile elektronik yollarla sağlanan temel servislere uygun olan eklenmiş vergi düzenlemeleri konusundaki 77/388/EEC 'de değişiklik yapan direktif teklifi
E-Para Direktifleri 2000/46/EC [78] 2000/28/EC [79]	Sözkonusu direktifler kısaca e-Paranın geleneksel olmayan kredi kuruluşlarına yani e-para kuruluşlarına tek bir sertifikanın verilmesi, tüketiciyi korumak ve hamillerin güvenini sağlamak, elektronik paranın geleneksel kredi kurumları ve e-para kurumları arasındaki ihtiyatlı bir danışmanlık sağlanarak çözümsüzlüğe engel olmaktır. Sonuç olarak Avrupa Birliği içerisinde e-para ile ilgili olarak yasal çerçevenin harmonizasyonunun sağlanmasıdır.	18 Eylül 2000 Direktifi
Çerçeve Direktifi 2000/31/EC [80]	Bu direktif iç pazarda bilgi topluluğu servislerinin üye ülkeler arasındaki serbest dolaşım foksiyonunun işlemesine katkıda bulunmaktadır. Direktif yukarıda belirtilen amaca ulaşılmasına yönelik iç pazarda bilgi topluluğu servisleri ile ilgili bazı ulusal hükümler, servis sağlayıcıların kurulması, elektronik sözleşmeler, mahkeme dışı üye ülkeler arasındaki işbirliği v.s. sağlanması amacını gütmektedir.	8 Haziran 2000 tarihli elektronik ticaret direktifi
Elektronik İmza Direktifi 99/93/EC [52]	Sözkonusu direktif Avrupa Komisyonu'nun elektronik ticaretin gelişimi için Avrupa işçerçevesinin gelişimine yönelik esnek ve tümleşik yaklaşımlarıyla ilgilidir. Geçmişte sadece elle atılmış olan imzalar geçerliyken bu yasa elektronik ticaretin evsahibi ülkelerin kontrolü ve servislerin serbest dolaşımı iç Pazar prensiplerine göre tanınmasını sağlamaktadır.	13 Aralık 1999 tarihli elektronik ticaret için topluluk işçerçevesi

Elektronik Ticaret Direktifi 98/48/EC [81]	Sözkonusu Direktif , bilgi toplumu hizmetlerinin üye ülkeler arasında serbest dolaşımını sağlamak amacıyla hazırlanmış olup, direktifte elektronik sözleşmeler ve bunların hukuki neticelerine ilişkin de önemli hususlar bulunmaktadır. Direktifin tam adı "Bilgi Toplumu Hizmetlerinin Bazı Yasal Hususları, Özellikle Elektronik Ticaret Hakkında Direktif" şeklindedir. Direktifte esas olarak bilgi toplumu hizmetlerinin serbest dolaşımı amaçlanmakta ve bilgi toplumu hizmet sağlayıcılarının nasıl kurulacağı, sorumlulukları, görevleri, cezalar ve elektronik imkanlarla gerçekleştirilen akitler, ara hizmet sağlayıcılarının sorumlulukları gibi hususlar ele alınmaktadır. Bilgi toplumu hizmetleri elektronik ticaretten çok daha kapsamlıdır ve elektronik ticareti de içermektedir. 98/48 sayılı AB Direktifinden hareketle, bilgi toplumu hizmetlerinin normalde para karşılığında, uzaktan, elektronik yollarla ve alıcının talebi karşılığında verilen hizmetler olarak tanımlandığı söylenebilir.	8 Haziran 2000 tarihli direktif
Elektronik Ödemeler Tavsiye kararı 97/489/EC [82]	Elektronik ödeme kuruluşları tarafından yapılan işlemler konusuyla ilgilidir.	97/489/EC Tavsiye kararının uygulama çalışması
Veritabanı Direktifi 96/9/EC [83]	Sözkonusu direktif tüm formlardaki veritabanlarının yasal olarak korunmasıyla ilgilidir.	96/9/EC Direktifi
Kişisel Verilerin Korunması Direktifi 95/46/EC [84]	Sözkonusu direktif kişisel verilerin serbest olarak dolaşımını garanti altına almak için gerekli kalıcı ve net düzenleyici çerçeveyi kurmaktadır. Kişisel verilerin serbest dolaşımı kişisel verilere bağlı olan mali servisler gibi geniş müşteri tabanına sahip tüm servislerde çok önemlidir. Direktif Tüketicilerin kendi verilerini işlemelerine yönelik geniş haklar vermeyi amaçlayan prensiplere sahiptir.	95/46/EC Direktifi

3.1.2.2 ABD ÖRNEĞİ

Amerika Birleşik Devletleri elektronik ticaret konusunda en etkin ve kapsamlı çalışan, bu konuda dünyaya liderlik yapan ülkelerin başında gelmektedir. İnternet'in Amerika'da doğduğu ve dünyada internet kullanımının en yaygın olduğu ülkelerden biri olduğu düşünüldüğünde, e-ticaret rakamlarının ve teknolojilerinin üst düzeyde olması anlaşılırdır. ABD ekonomisinin son

yıllarda beklentilerin de ötesine geçen bir büyüme yaşamasının arkasındaki temel etkenlerden birinin, internet tarafından belirlenen bilgi teknolojisinde yaşanan gelişmeler ve bilgi tabanlı ekonomiye geçilmiş olması olduğu bizzat ABD yönetimince vurgulanmaktadır [60].

ABD Ticaret Bakanlığı, e-ticaret konusunda çok önemli çalışmalar yapmaktadır. Sadece hükümet ve sadece özel sektör temsilcilerinden oluşan çok sayıda kurum ve kuruluş, politika oluşturmak ve uygulamaya yönelik araç ve standartları belirleme konusunda çalışmaktadır. Eyaletlerde sayısal imza, onay kurumu ve e-ticaretin diğer yönleri ile ilgili yasa çalışmaları sürmektedir [25].

ABD'de elektronik ticaret konusundaki çalışmalara aşağıda verilmiştir.

• Ulusal Bilgi Altyapıları kapsamında (National Information Infastructure-NII) eticaret altyapı programı hazırlanmıştır [8].

• 1995 yılında "Federal Elektronik Ticaret Ekibi" oluşturulmuş, elektronik ticaretin hükümet tarafından kullanılma olanakları değerlendirilmiştir.

• ABD'nin genel yaklaşımı, "Küresel Elektronik Ticaret İçin Bir Çerçeve" dokümanı ile açıklanmıştır.

Öte yandan Mart 1994 yılında Başkan Yardımcısı A.Gore, Buenos Aires'de Dünya İletişim Konferansı'nda yaptığı konuşmada elektronik ticaret alanında güçlüklerin kaldırılmasına değinmiştir. İleri sürdüğüne göre, ABD'de hükümet politikasının iletişim sektöründe dayanması gereken prensipler şunlardır:
(1) Hükümet tarafından kontrol edilen iletişim şirketlerinin özelleştirilmesi yoluyla özel sektör yatırımlarının teşviki,
(2) Monopol niteliği taşıyan telefon piyasalarının rekabetine imkan tanınması, iletişimin adil fiyatlarla yapılmasının güvenceye alınması, piyasaların yabancı yatırımcılara açılması ve antitröst uygulamaların güçlendirilmesi.

(3) Sistemin açık girişe dayandırılması ve böylece küresel bilgi altyapısı kullanıcılarının geniş bir bilgi ve hizmet alanına girebilmesi,
(4) Teknolojik gelişme ile birlikte esnek, rekabetçi, bağımsız bir düzenleme oluşturulması [85].

Bu açıklamada her ülkenin politika yapıcıları, etkin ve güvenli elektronik ticaret sistemlerine güveni oluşturacak, çalışabilir bir altyapı oluşturmaya davet edilmektedir.
Amerikan Hükümeti bu süreçte beş ana ilkeyi içeren bir politika açıklamıştır. Bu ilkeler [4]:

- Özel sektörün öncülük etmesi
- Hükümetin elektronik ticarette aşırı sınırlamalardan kaçınması
- Hükümetin katılması gereken durumlarda amacının, açık, minimalist, sürekli ve basit bir yasal ortam oluşturmak olması
- Hükümetlerin internetin kendine özgü yapısını kabul etmeleri
- İnternet temelli elektronik ticaretin küresel düzeyde kolaylaştırılmasıdır.

3.2 Elektronik Ticaretle İlgili Ticari Yasalar

Elektronik ticaret ve internet işlemlerinin geleneksel ticaretin şekline uzanan bir şekilde verilebilmesini teminen geliştirilmesi için yasal berraklık ve işlemlere uygulanacak olan mekanizmaların yeterliliğine ihtiyaç vardır. Bu olay işlemlerin birden fazla adli yetkiliye ulaşması durumda daha da önem kazanmaktadır. Örneğin en yaygın sözleşme yasası herhangi bir durum için yasalar ve ulusal yargı hakkı tarafından idare edilmekte ve kullanılmakta olan kağıt belgelere ve fiziksel olarak yazılmış olan imzalara dayanmaktadır. Elektronik imzaların ve elektronik dokümantasyonun yorumlanması, kabul edilmesi ve anlaşmaların yürürlüğe konulması ayrıca bu meyandaki ihtilafların çözümlenmesini de içermekte olan konular bir çok ülkede hem iç

yasalarda hemde uluslararası yasada henüz çözüme ulaştırılamamıştır. Varolan yerel sözleşme yasasının elektronik çevreye genel extrapolasyonu bu belirsizlikleri azaltmalıdır. Özellikle uluslararası belgeler durumunda yasal yargı hakkı ve diğer yönler elektronik ticaretin gelişimine yönelik engelleri oluşturabilir.

Bu işlemlerin güvenli ve özel olmasını sağlamak için esasın belirlenmesini sağlamak, makbuz, ve gelen bilginin bütünlüğünün oluşturulmasını sağlamak için bazı yollar olacaktır ve birşeylerin ters gitmesi durumunda gerekli düzenlemelerin yapılması için bazı mekanizmalar olacaktır ve tüm bunlar için koordineli politikalar gerekmektedir. Küresel olarak tanınan resmi onay ve sertifikasyon teknolojileri, mekanizmaları, ve enstitülerinin kullanılması varolan gereksinimleri karşılamada ve elektronik işlemlere olan güvenin tesisinde önemli bir rol oynamaktadır.

Elektronik çevrede ödeme mekanizmalarının bir parçası olarak kimlik ve hakların tesis edilmesi için resmi onaylama kullanılır. (Örneğin akıllı kart ya da şifreleme yoluyla biyometrik tekniklerin paylaşılması). Sertifikasyon mekanizmaları, elektronik çevredeki organizasyonun ve bilginin güvenilirliğini sertifikalar yoluyla sağlayarak sistemler ve taraflar arasındaki işlemlerin belirsizliklerini azaltır. Örneğin güvenilir bir kaynak işlem yaptığı tarafa tanıklık yapabilecek ve bilginin doğrulayabilecektir. Onaylamanın kriptografik tekniklere dayandığı durumlarda sertifikasyon mekanizması genel kriptografik anahtarın bireysel kişilere bir bağlantı olarak kullanılır.

3.2.1 Elektronik Ticaret ile İlgili Uncitral Model Yasası

Birleşmiş Milletler Uluslararası Ticaret Yasası (UNCITRAL) tarafından hazırlanmış olan yasa modeli ulusal kanun koyucular için yasal kısıtlamaların nasıl kaldırılabileceğini ve elektronik ticaret için daha güvenli yasal bir çevrenin nasıl yaratılabileceğini adresleyen kabul edilebilir bir dizi uluslararası kurallar setidir [61]. Model yasa ayrıca e-ticaret kullanıcılarına

bazı yasal kısıtlamaları çözmelerini sağlayarak elektronik ticaretin kullanımının arttırılmasını sağlayacak olan bazı sözleşme çözümlerini sunarak yardımcı olmaktadır. Model yasanın amaçları arasında Elektronik Veri Transferi (EVT) ve elektronik posta gibi haberleşme tekniklerinin kullanımını sağlayarak uluslararası ticaretin etkinliğinde ve ekonominin teşviki için gerekli olan, bilgisayar temelli dokümantasyon ile kağıt temelli dokümantasyona eşit muamelenin sağlanması gelmektedir.

Model yasa veri mesajlarının ayırd edilmemesini, örneğin veri mesajlarını ve kağıt dokümanlar arasında bir ayırım gözetilmemesi gerektiğini somutlaştırmaktadır. Model yasada "yazma"nın sonucu olarak vergi yasasında ya da medeni yasa kapsamında "erişilebilirlik" bilgisayar formundaki verinin okunabilir ve yorumlanabilir olması ve yazılımın bu tip bilgileri okunabilir kılması anlamına gelmektedir.

Model yasada bir "imza"nın amacı kişiyi tanımlamak, imzalama fiiliyle o şahsın kişisel ilgisinin kesinliğini sağlamak, dokümanın içeriğiyle o şahsı ilgili kılmaktır. Bir imza ayrıca imzalanan dokümanın doğası, imzalanan mukaveleyle yükümlülük altına girecek tarafa tanıklık yapmak, ya da şahsın bir metnin yazarlığını onaylama niyeti gibi gibi değişen bir çok fonksiyonu gerçekleştirmektedir. Madde 7 hangi veri mesajlarının yeterli güvenilirliğinin e-ticarete olan güvenle ilgili halihazırda bulunan engeller ortamında "sayısal imza "nın gerekliliklerini icra ederek hangi şartlar altında geçerli olacağını tesis etmektedir. Madde 7 imzanın iki fonksiyonu üzerinde odaklanmaktadır: dokümanın yazarının belirlenmesi ve yazarın sözkonusu dokümanın içeriğini onayladığını doğrulamasıdır [31].

Model Yasa'nın diğer hükümleri "orijinal" ve "el yazısı" data mesajlarının kabul edilebilirliğini ve delil niteliğiyle beraber kontratların oluşumunun ve geçerliğinin korunmasını ve taraflar tarafından tanınmasını adreslemektedir [86].

Uluslararası Ticaret Odası (GUIDEC) 1997 yılında sayısal yollarla gerçekleştirilen küresel elektronik ticaret sisteminin desteklenmesine yönelik olarak uluslararası ticaretin genel kullanımını kabul etmiştir. GUIDEC digital mesajların sertifikasyonu için farklı yasal sistemlerde hali hazırda bulunan yasa ve uygulamalara dayalı olarak gerekli iş çerçevesini tesis eder. Bu iş çerçevesi, işlem yapan tarafların varolan iş uygulamalarına uyumlu bir şekilde, müşteriler, sertifika sağlayıcıları, güvenilir tarafların hakları ve sorumluluklarıyla ilgili risk ve yükümlülükleri tahsis etme amacını gütmektedir. GUIDEC Uncitral Model yasasından çıkarılmıştır. Uncitral ulusal hükümetler ve parlamentoları gözönüne alan hukuki bir çalışma iken GUIDEC metni elektronik ticaretle ilgili olarak uluslararası ticaret perspektifinden harmonize olmuş bir hukuki rejim sunduğundan dolayı özel bir metindir.

3.2.2 OECD'nin Yetkilendirme ve Sertifikasyon ile İlgili Yaklaşımları

OECD ülkeleri ilgilerini elektronik ticarete hizmet eden yasa ve politikalara çevirmiş olup küresel seviyede yetkilendirme ve sertifikasyona yönlenmiş durumdadırlar. 1998'lerin öncesinde OECD kamu ve özel sektördeki ulusal ve uluslararası seviyedeki yasalar, politikalar, teşebbüslerle ilgili bir envanter çalışması yürütmüştür. Bazı ülkeler kağıda dayalı ortamdan sayısal ortama geçerken bu geçişi hızlandırmaya yönelik elektronik ortamdaki kimlikleri tanımlamak ve bilginin doğruluğunu test etmeye yönelik metotları belirlemek ve varolan yasaların yenilenmesinin ya da yeni bir mevzuat gerekip gerekmediği konusunda karar verecek olan sorumlu gruplar oluşturmuşlardır. Uncitral model yasası bir çok ülke tarafından yürürlüğe konulmuştur [87].

Yetkilendirme ve sertifikasyonla ilgili ulusal politika yapmaya yönelik çoğu çabalar sayısal imza teknolojisinin uygulanmasının mümkün kılınmasına odaklanmıştır. Bazı OECD ülkeleri sayısal imzanın yasal olarak tanınması ile ilgili mevzuatı kabul etmiş, bir kısmı sayısal imzanın yürütülmesi ile ilgili gereksinimleri, diğer bir kısmı ise sayısal imzayı sağlayacak sertifika hizmet sağlayıcılarının işletim gereksinimlerini çalışmalarını üstlenmişlerdir. Bu

yaklaşımlar kriptografiye dayanan sayısal imza için, sertifikasyon otoritelerinin yükümlülük kuralları, kurulma ve yetkilendirilme kriterleri, sertifikasyon politikaları, sertifikasyon uygulama bildirileri gibi özel bazı yasal kuralları göstermektedirler [88].

OECD hükümetleri açık anahtarlama kriptolojisine dayanan sayısal imzalar için sertifikasyon otoritelerinin fonksiyonlarını açık şebekeler için desteklemesini zorunlu kılmıştır. Sertifikasyon otoritelerinin hükümete mi bağlı yoksa özel kuruluşlara mı verilmesi gerektiği, eğer özel kuruluşlara verilecekse bu kuruluşların hükümet tarafından lisanslandırılmasının mı yada yetkilendirilmesinin hangi kriterlere göre yapılacağı gerekip gerekmediği gerektiğine dair bir soru her zaman gündemdedir [89].

Bazı OECD ülkeleri bilgi teknolojileri, ürünler ve servisler ve bilgi kullanıcıları olarak elektronik ticaretin teşvik edilmesinde rol oynamaktadırlar. Bazı endüstri girişimleri, küresel elektronik ticaret için onaylama ve sertifikasyon mekanizmalarını yürürlüğe koymuşlardır. Çeşitli ticari yetkilendirme ve sertifikasyon servisleri belirmeye başlamış ve çabaların belirsiz teknolojik, yasal ve kamu politika çevreleri yoluyla yürütüldüğü gözlenmektedir.

Bu alanda birincil politika yapıcıların telekomünikasyon alanında olmadığı ya da telekomünikasyon operatörlerinin sertifikasyon ya da yetkilendirme sağlayan kuruluşlar gözüyle bakılıp bakılmadığı aşikardır. En tarafsız transmisyon sistemleriyle elektronik haberleşme ve işlemlerinin bütünlüğü daha güvenli sağlanabilir.

Telekomünikasyon regülasyonu, kuruluşlar için gelişmenin genel olarak teşviki bağlamında elektronik ticaret için gerekli iş çerçevesinin kurulmasıyla ilgilidir. Pazar yönelimli ekonominin etkin olarak gelişimi oluştuğunda yasa yapıcılar benzer iş kolları telekomünikasyona dayalı iş ilişkilerinde varolan daha evrensel normlarla çok esneklikle ve aciliyetle karşılaşırlar [90].

3.2.2.1 Bilginin Korunması, Gizlilik

Küresel bilgi şebekeleri karmaşık güvenlik problemleri ile yüzyüze gelmektedirler. Hükümetler ve iş çevreleri, hile, suistimal, hırsızlığa hatta elektronik terörizme karşı coğrafi olarak dağılmış güvenli şebekelere ve sayısız erişim noktalarına, ihtiyaç duymaktadırlar. Şebeke kaynakları izinsiz kullanım ve enterferanstan korunurken evrensel bağlanabilirliğin yararlarının arttırılma ihtiyacı küresel veri şebekesi güvenlik çözümleri talebi ihtiyacını arttırmıştır. Elektronik ticaretin kuruluşlar ve müşteriler arasındaki hızlı gelişimi suistimal ve kredi kartlarında dahil olduğu veri ödemelerinin yanlış kullanımı, ürünlerin kalitesine olan güven eksikliği, korkularını doğurmuş olup müşterilerin garantilerinin görülmeyen işlemler için korunmalıdır. Rapor edilmiş olan veri tabanlarının kötü niyetli olarak hacklenmesi olayı iş ve özel haberleşmede internetin ve diğer şebekelerin kullanımını azaltıcı etkileri olmuştur.

1997'de Bilgisayar Güvenliği Enstitüsünce (CSI) yapılan bilgisayar suçları ve güvenliği araştırmasına göre bilgisayar haberleşmesine dayalı suçlar artmaktadır. Araştırmayı yanıtlandırmış olan 563 işletmenin hükümet kurumları, mali kurumlar ve üniversitelerin ¾'ü, güvenlik ihlallerinden dolayı bazı mali kayıplara uğradıklarını yanıtlamışlardır. % 42'si kendi bilgisayar sistemlerinde yetkilendirilmemiş kullanımla karşılaşmış olduklarını belirtmişlerdir. Bu organizasyonların yarısı zararlarını 100 milyon $'dan daha fazla olduğunu belirtmiştir. Virüsler, telekomünikasyon suistimali, mali suistimal, özel bilgilerin hırsızlığı, en çok rastlanılan problemler olarak ifade edilmiştir.

Elektronik ticareti işlemlerin geleneksel formları gibi sağlam olarak gerçekleştirilmesi için halihazırda bazı önlemler alınmaya başlanmıştır. Şifreleme bu yüksek seviyeli şebekeleşmiş çevrede güvenlik için temel bir araçtır. Yüksek güvenilirlikteki şifreleme ucuz olarak yerleştirilmekte olup değerli bilgilerin işlenmesinde bir çok elektronik haberleşme ürünlerinde ve uygulamalarında geniş olarak kabul edilmekte kullanılmaktadır. Bu

uygulamalar arasında dosyaları hırsızlıktan ve yetkilendirilmemiş kullanımdan korumak, güvenli haberleşmeyi önlenmeden korumak, ve güvenli işlemleri sağlamak yer almaktadır. Kriptografi ayrıca bir dosya ya da mesajın değiştirilmeden içeriğinin değiştirilmediği, tarafların belirlenmesi, ya da yasal taahhütleri yapmayı garanti eder.

3.2.2.2 OECD Şifreleme politikası

OECD 1997'de şifreleme politikası direktiflerini hazırlamıştır. Şifreleme politikasının gizliliğin ve verinin bütünlüğünün sağlanmasında etkili bir araç olduğu kabul edilmektedir. Bu faaliyetler arasında kendi vatandaşlarını koruma, ekonomik refahın sağlanması, kamu güvenliğinin korunması, faaliyetlerinin mali gelirlerini arttırma, yasaların icrası ve ulusal güvenliğin korunması sayılabilir. Şifrelemenin yasal, ticari ve bireysel ihtiyaçları ve kullanımları bulunsa da kamu güvenliğine, kanuni icra, iş ve tüketici ilgileri ve gizliliğine yönelik zararlı kanunsuz faaliyetlerde de kullanılabilir.

Kapsamlı müzakerelerden sonra kabul edilen OECD kriptografi politikaları direktiflerini ve kendi 29 üyesinin bu direktifleri yürürlüğe koymaları için gerekli nihai kararı kabul etmiştir. Bu direktifler 8 prensibi teklif etmektedir:

1. Bilgi ve haberleşme sistemlerinin kullanımında güveni tesis etmek için şifreleme metotları emniyetli bir şekilde kullanılmalıdır.

2. Kullanıcılar yürürlükteki yasa bünyesindeki şifreleme metodu seçme hakkına sahiptirler.

3. Şifreleme metotları ihtiyaçlar, bireylerin, iş çevrelerinin ve hükümetlerin sorumlulukları gözönüne alınarak geliştirilmelidirler.
4. Şifreleme metotları için teknik standartlar, kriterler ve protokoller geliştirilmeli ve ulusal ve uluslararası seviyede ilan edilmelidirler.

5. Bireylerin gizliliği, haberleşmenin gizliliği ve kişisel verinin korunması konularına ulusal şifreleme politikaları ve şifreleme metotlarının yürürlüğe konulması temelinde ele alınmalıdır.

6. Ulusal şifreleme politikaları düz metinlere, şifreleme anahtarlarına, ve şifrelenmiş verilere ulaşmayı mümkün kılabilir. Bu politikalar direktiflerde yer alan prensiplere mümkün en geniş anlamda kapsamalıdır.

7. Şifreleme servisleri sunan ya da şifreleme anahtarlarına erişen ya da tutan kurumların yükümlülükleri bir kontrat ya da mevzuat yoluyla açıkça belirlenmelidir.

8. Hükümetler politikalarını koordineli bir şekilde ve işbirliği yoluyla belirlemelidirler. Bu çabaların bir parçası olarak hükümetler şifreleme politikası bağlamında ticarete engellemelerde bulunmaktan kaçınmalı ve bu engelleri kaldırmalıdırlar.

1970'lerin ortalarına doğru şifreleme "açık anahtar" kavramı taraflara önceden paylaşımlı anahtar vasıtasıyla haberleşme yapmaksızın şifrelenmiş verinin değişimini sağlamasından dolayı bir yenilik olarak tanımlanmıştır. Bu dizayn bir gizli anahtarı paylaşmak yerine haberleşen her tarafların her birine matematiksel olarak ilgili olan "açık anahtar" kamu kuruluşuna (hükümet, banka v.s.) açılan kısım ve "özel anahtar" olarak gizli tutulan kısım olmak üzere iki anahtar kullanır.

Mesajların durdurulmasını önlemek "şifreleme" ürünleri sunan ve güvenlik standartları tasarımı yapan kuruluşların ilgisini çekmektedir. Kredi kartı endüstrisinde "Güvenli Elektronik İşlem " ("Secure Electronic Transaction" (SET) standardı bir çözüm olarak üretilmiştir. 1997 yılında kredi kartı veren makamlardan iki tanesi bilgi teknolojisi ve telekomünikasyon sektöründeki bazı firmalarla işbirliği yaparak SET standardını geliştirdiklerini açıklamışlardır. SET internette kredi kartı ile yapılan alışverişlerde ödeme,

yetkilendirme ve para transferiyle ilgili güvenliği geliştirir. Mesajın şifrelenmiş halini şebeke üzerinden gönderildiğinde sayısal imza, kriptografik sertifikalar kredi kartı numaralarının ve işlemlerinin gizli tutulmasını sağlar. Bu işlemin önemli bir rolü anahtarların tutulması ve gönderilmesinde yer alan ve diğerlerinin SET mesajları için şifre çözücüye ihtiyaç duyan 3. taraflar (banka ya da mali kurum) tarafından gerçekleştirilir. Prosedür, ödemelerin değiştirilmelerden korur ve satıcının kimliği ve alıcının kartının geçerliliğini onaylar.

OECD'nin SET gibi direktifleri ve çözümleri hükümetler ve iş çevreleri tarafından geniş bir şekilde kabul görmüştür. Ancak, Amerika ve bazı diğer ülkeler şifreleme ürünlerinin gücünü hükümet onaylı anahtar belgesi ve anahtar kurtarma sistemi kabul edilmemesi durumunda sınırlamışlardır. Bu politika şifreleme ürünleri üreten üreticiler ve kendi küresel şebekeleri için güçlü şifreleme kullanmak isteyen işletmelerin karşısındadır. ABD Clinton yönetimi politikası teröristler ve uyuşturucu kartelleriyle ilgili korkular dolayısıyla kaydedilemeyen yüksek güçteki şifrelemeyi kullanacağını taahhüt etmiştir. Ulusal güvenlik ve yasa uygulama kuruluşları tüm kullanıcılardan gelen kod çözme zorluklarını olmaksızın metin mesajları net biçimde okuyabilmek için şifreleme anahtarlarına erişmeyi talep etmektedirler. Amerika'daki ve diğer ülkelerdeki şebeke operatörleri veri gönderimlerinde güvenliğin sağlanması için güçlü şifrelemeyi kabul etmektedirler.

Telekomünikasyon regülasyonu bakış açısından, bu kaygılar elektronik ticareti destekleyen telekomünikasyon şebekesinin temel kapasitesini ifade etmektedir. Şifrelenmiş ya da şifrelenmemiş çoğu sayısal transmisyonun şebekede gerçekte görünür değilken, çoğu elektronik işlemin yüksek hassasiyete sahip doğası ve yetkilendirme, onaylama fonksiyonları şebekeleri yüksek gizlilikte, güvenlikte servisler sağlamaya zorlamaktadır. Serbestleşmiş telekomünikasyon pazar politikaları kapsamında bu amaç altyapı sağlayıcılarının rekabeti yoluyla gerçekleştirilir. Ancak, regülatörler

düşük kaliteli rekabetçiler, ilkesiz kişiler, gizli işlemlerin engellenmesi yoluyla elektronik ticaretin etkilenmesi gibi muhtemel tehlikelerden haberli olmalıdır.

Eğer gelecekte bir noktada özel ihlaller ya da suistimaller oluşursa şebekeler ve bu şebekelerin regülatörleri kıyaslanacaktır. Elektronik haberleşmenin çevresindeki engellerin kaldırılmasına yönelik herhangi bir düzenleyici bir gerçeği olmasa bile telekom operatörlerinin sistemin bütünlüğüyle ilgili kuşkulara göğüs germek ve bu kuşkuları yenmek için endüstri, ve diğer politik görevlilerle birlikte çalışmak gibi ilgilenmesi gereken bazı özel durumlar olabilir.

3.2.3 Mülkiyet Hakları

Elektronik ticaretin geleceği mülkiyet hakları ile ilgili temel iki konu üzerinde yoğunlaşmaktadır: (1) telif hakları ve ilgili diğer hakların korunması, (2) alan adları ve ticari markaların eşit tahsisi ve korunması. WTO katma değerli, bilgiye dayalı endüstrilere dereceli geçişin ticari ilişkilerinde mülkiyet hakları konusunun önemini arttırdığını vurgulamıştır. Bu tanınma uruguay round'ını mülkiyet hakları ticarete dayalı yönleri ilgili olarak çok katmanlı ticaret sistemlerini mülkiyet haklarının bir bütünü haline getiren bir anlaşma hazırlanmasına (TRIPS) itmiştir.

WTO'nun elektronik ticaret ile ilgili yapmış olduğu bir çalışmaya göre elektronik ticaret mülkiyet hakları konusuyla çok yakından ilgilidir. WTO internet üzerinden gerçekleştirilen ticaret ve diğer haberleşme şebekeleri bilginin lisanslandırılması ve satılmasında yer almakta olup kültürel ürünler ve teknoloji mülkiyet hakları koruyucuları tarafından korunmaktadır. Kitap satışı internet üzerinden yapılan ticaretin en popüler formu durumunda olup ve CD ve kayıtlar gibi diğer ürünlerin satışı da artmaktadır. Çoğu kitaplar, CD'ler ya da filmler internet üzerinden sipariş edilse de hala posta yoluyla gönderilmekte olup internetin ürünlerin tüketicilere gönderilmesinde kullanımı hızla artmaktadır. Şebekelerin kapasitesi arttıkça ve son kullanıcıların

ekipmanları izin verdikçe haberleşme şebekeleri film, kayıtlar, filmler gibi ürünlerin gönderilmesinde bir araç olacaktır.

Elektronik ticaretin ve internetin IPR'ların nasıl yönetileceği ile ilgili önemli etkileri vardır. Bilgi teknolojisi ve haberleşme mülkiyet hakları ile ilgili ulusal, bölgesel ve uluslararası patent ve ticari marka ofislerinin geliştirilmeleri için sıklıkla kullanılmaktadır. Bunun içerisinde daha iyi ve hızlı servisler, mülkiyet haklarını gerçekleştirmek ve bu konularla ilgili bilgilere erişimi hızlı bir şekilde gerçekleştirmek hususu da yer almaktadır. Patent ofisleri dünyanın her bölgesine teknik bilginin neşriyatı hizmetini sunarlar. Ancak, internetin kapasitesi ile ilgili uygulanabilir yasanın belirlenmesinde problemler çıkmıştır. Ayrıca, telif hakları ile korunan ürünlerin dağıtılması çoğunlukla bölgesel lisanslarla hak sahipleri tarafından gerçekleştirilmektedir. Sınırlar arasında ürünlerin gönderilmesinde kullanılan direk posta gibi geleneksel metotlar internet yerini aldıkça değişmektedir. IPR için elektronik gönderme ile ilgili işlemler ulusal ve uluslararası seviyede oldukça ilgi çekmektedirler.

3.2.4 TRIPS Anlaşması ve Elektronik Belgelere Uygulanan WIPO Anlaşması

TRIPS Anlaşması telif ve diğer hakları ilgili konular (yorumcular, ses kayıtları üreticileri, yayıncı kuruluşlar), servis markası dahil ticari markalar, coğrafi belirticiler, endüstriyel modellemeler, entegre devrelerin planı ve test verilerinin ticareti gibi ifşa edilmemiş bilgileri kapsamaktadır. Anlaşma her üyeye sağlanacak olan minimum standardı belirlemektedir. Anlaşma ayrıca mülkiyet haklarının uygulamaları için ulusal prosedürler ve çözümleri sunmaktadır. Sözkonusu anlaşma WTO ülkeleri ve arasındaki ihtilaflara TRIPS anlaşmasının bütünleşmiş ihtilaf çözüm prosedürlerine göre çözüm üretmektedir.

Dünya Fikri Mülkiyet Hakları Kuruluşu (WIPO 1996'da haberleşme hakkı, teknolojik ölçülerde kanunun boşluklarından yararlanma, bilginin yönetimini ve bütünlüğü hakları açısından internet ile ilgili işlerin kullanımı ile ilgili olarak)

telif hakları anlaşması ve performans ve ses (phonogram) anlaşmasını kabul etmiştir. Yazarlar, icracılar ve ses üreticileri, kendi korunmuş ürünlerinin telli ya da telsiz metotlarla yetkili kıldıkları üyelere sağlanmasından hoşlanmaktadırlar. Anlaşmalar hak sahipleri tarafından kullanılan teknolojik ölçüleri etkili korumayı sağlayarak tanımaktadırlar. Elektronik hakların kullanımı bilgisine işlerin ve diğer materyallerin sayısal kopyalarıda eklenebilir.

TRIPS anlaşması ve WIPO telif hakkı anlaşmaları veri ve diğer materyallerin hangi fikri yaratımdan oluştuğuna dair listelerdeki telif hakkı korumasını tanımaktadır. Sayısal teknolojinin telif ve diğer hakları üzerindeki etkisinin korsan ses kayıtları, filmler, yazılım, ve CD-Romlar gibi ürünlerin dağıtımının geniş bir çerçevede tanınması resmi olmayan yollardan kabul edilmiştir. Bu ürünler kaliteden kayıp olmaksızın kopyalanabildiğinden korsanlığa çok yatkındır. TRIPS anlaşması, WTO ülkelerinin uluslararası ticareti fikri mülkiyet hakları ile ilgili ihlalleri birbirleriyle işbirliği yaparak gidermeye yönelik bir takım koruyucu haklar getirmektedir [91].

Bu uluslararası anlaşmalarla önerilen yasal korumalara rağmen, internette ticari markaların kullanımı önemli soruların doğmasını sağlamaktadır. Önemli bir anahtar soru hangi şartlar ve yargı hakkı(ları)nın kayıtlı bir ticari markanın ihlali durumunu oluşturacağıdır. Eğer kullanımın bir ülke içinde bir ihlal yarattığı düşünülüyorsa özellikle transmisyon başka bir ülkeden yapılıyorsa hangi çarelerin uygun olduğu, ticari markaların o bölgeye ait olan kayıtlarının sınırötesi pazar için yeterli olup olmadığı, ve bu gibi soruların için gerekli nihai kararlar etkin ve adaletli bir elektronik ticaretin gerçekleştirilmesinin önemli unsurlarıdır.

3.3 Türkiye' de Elektronik Ticaret ile ilgili konular İzlenen Politikalar

Ülkemizde Elektronik ticaret ile ilgili çalışmalar 1997 yılından itibaren Bilim ve Teknoloji Yüksek Kurulu'nun (BTYK) çalışmalarıyla başlatılmıştır.

Elektronik Ticaret konusu ilk olarak BTYK'nın 25 Ağustos 1997 tarihli toplantısı gündemine alınmıştır. Sözkonusu toplantıda Ülkemizde elektronik ticaretin yaygınlaştırılması amacıyla elektronik Ticaret Koordinasyon Kurulunun Kurulması kararlaştırılmıştır. ETKK'nın çalışmalarının koordinatörlüğünün Dış Ticaret Müsteşarlığı (DTM) tarafından sekreteryasının ise Tübitak tarafından yürütülmesine karar verilmiştir. ETKK'nın üyesi olan kuruluşlar arasında Adalet Bakanlığı, İç İşleri Bakanlığı, Maliye Bakanlığı, Sağlık Bakanlığı, Ulaştırma Bakanlığı, Tarım ve Köy İşleri Bakanlığı, Sanayi ve Ticaret Bakanlığı, Kültür Bakanlığı, Devlet Planlama Teşkilatı, Hazine Müsteşarlığı, Gümrük Müsteşarlığı, Devlet İstatistik Enstitüsü, Merkez Bankası, Rekabet Kurumu, Sermaye Piyasası Kurulu, Milli Prodüktivite Merkezi, Küçük ve Orta Ölçekli Sanayi Geliştirme Bakanlığı, Türkiye Odalar ve Borsalar Birliği, Yapı ve Kredi Bankası, Demirbank, Ziraat Bankası, Emlak Bankası, Vakıflar Bankası, Türk Eximbank, Türkiye Halk Bankası, Esbank, Türkiye İş Bankası, TTGV, Türk Patent Enstitüsü, Türk Telekom, İGEME, BİLTEN, Orta Anadolu İhracatçı Birlikleri Genel Sekreterliği, Dış Ekonomik İlişkiler Kurulu, Uluslararası Nakliyeciler Derneği, Uluslararası Taşıma İşleri Komisyoncuları ve Acentaları Derneği Birliği'nin yer alması kararlaştırılmıştır [92].

Elektronik Ticaret Koordinasyon Kurulu'nun (ETKK) ilk toplantısı, Dış Ticaret Müsteşarlığı başkanlığında 16 şubat 1998 tarihinde yapılmıştır. Böylece, elektronik ticaretin geliştirilmesine ilişkin geniş katılımlı ve düzenli çalışmalar başlatılmıştır.

Anılan toplantıda, çalışmaların verimli bir şekilde sürdürülebilmesi için Teknik, Hukuk ve Finans adı altında, toplantıya katılan kuruluş temsilcileri arasından üç ayrı çalışma grubu oluşturulmuştur. Çalışma gruplarının üç ay içinde bir rapor hazırlamaları kararlaştırılmıştır. ETKK'nın 16 şubat 1998 tarihli toplantısında alınan Karar gereğince Hukuk, Teknik ve Finans çalışma grupları üç aylık raporlarını hazırlayarak 1998 Mayıs ayı içinde, ETKK Değerlerlendirme Komisyonu'na iletmişlerdir. Değerlendirme Komisyonu bu

üç raporun bir özeti olan ETKK Rapor Özeti'ni oluşturarak ETKK'nın onayına sunmuştur. Çalışma gruplarının raporlarıyla birlikte, 26 Mayıs 1998 tarihli ETKK toplantısında son şeklini alan Rapor Özeti BTYK Sekreteryası'na iletilmiştir. ETKK tarafından BTYK'ya sunulan "Özet Rapor"da ülkemizde elektronik ticaretin geliştirilebilmesi için devletin öncelikle aşağıda sıralanan dört ana görevi yerine getirmesinin gerekli olduğu vurgulanmıştır [93] :

. Gerekli teknik ve idari alt yapının kurulmasını sağlamak,

. Hukuki yapıyı oluşturmak,

. Elektronik ticareti özendirecek önlemleri almak,

. Ulusal politika ve uygulamaların uluslararası politikalar ve uygulamalarla uyumunu sağlamak.

BTYK'nın 2 Haziran 1998 tarihli toplantısında, Türkiye'de elektronik ticaretin yaygınlaştırılması ile ilgili düzenlemeler tamamlanıncaya kadar ETKK'nun görevini sürdürmesine ve kendi önerileri doğrultusunda bir eylem planı hazırlayarak uygulamayı izlemesi, sonuçları değerlendirmesi, uygulamada ortaya çıkacak sorunları çözmeye yönelik yeni öneriler geliştirerek bunları ilgili kuruluşların ve BTYK'nun görüşüne sunmaya devam etmesine karar verilmiştir.

İki yıllık bir çalışma sürecinin sonunda yapılan 26.04.2000 tarihli ETKK toplantısında; çalışma gruplarının raporları değerlendirilerek yeniden yapılanmaya gidilmiş, Proje Geliştirme, Hukuk ve Eğitim-Tanıtım Çalışma Gruplarının yeniden belirlenen üyeleri ile toplanmasına karar verilmiştir. Bu çalışmalar sonucunda, Hukuk Çalışma Grubu 01.07.2000 tarihi itibari ile hazırladığı Çalışma Sonuç Belgesi'nde; öncelikle elektronik imzanın hukuken tanınması için bir kanun taslağının hazırlanmasına ve bu konuda Adalet Bakanlığı'nın çalışmalarının beklenmesine karar verilmiştir [94].

3.3.1 DTM Koordinatörlüğü'nde Gerçekleştirilen Çalışmalar:

BTYK tarafından koordinatör olarak görevlendirilen Dış Ticaret Müsteşarlığı daha sonra, Başbakanlığın koordinasyonunda 30.07.2001 tarihli geniş

katılımlı toplantısı ile başlatılan E-Türkiye çalışmaları kapsamında yer alan on üç ayrı çalışma grubu arasındaki "E-ticaret" grubunun koordinasyonu hususunda da görevlendirilmiştir [95].

Dış Ticaret Müsteşarlığı Tablo 5.1 'de belirtilen çalışma grupları ve bu çalışmalara katılan ilgili kuruluşlarla çalışmalarını koordinasyonunu sürdürmeye Başbakanlığın 27 Şubat 2003 tarih ve B.02.PPG.0.12-3120-3416 sayılı genelgesine kadar devam etmiştir. Sözkonusu genelgeyle e-Dönüşüm Türkiye Projesinin koordinasyonu Devlet Planlama Teşkilatı'na (DPT) verilmiştir.

Çizelge 3.3 Dış Ticaret Müsteşarlığı E-ticaret Çalışma Grupları [95]

Grubun Adı	**Koordinatör Kuruluş**	**Üye Kuruluşlar**
1. Güvenli Ağlar ve Akıllı Kartlar-İdari Altyapı	TÜBİTAK-UEKAE	Adalet Bakanlığı, Sanayi ve Ticaret Bakanlığı, TCMB, Telekomünikasyon Kurumu, BDDK, SPK, TÜRKAK, TSE, PTT, Türkiye Bankalar Birliği, Türkiye Noterler Birliği, TÜBİTAK-BİLTEN, TTGV, TOBB, İSO, İhracatçı Birlikleri, TBV, Akıllı Kart Üreticileri (Kobil, PMB, vd), ETKK Hukuk Grubu
2. Kobiler ve Diger İşletmeler	KOSGEB	Sanayi ve Ticaret Bakanlığı, TSE, Türkiye Bankalar Birliği, TOBB, TESK, ATO, İSO, ASO, İGEME, İhracatçı Birlikleri, TÜBİTAK-UEKAE, TÜBİTAK-BİLTEN, TTGV, İTKİB, ALCATEL, KOBILINE, Global Sources, MİLSOFT, Tradanet
3. Tüketici Sorunları	Sanayi ve Ticaret Bakanlığı	Adalet Bakanlığı, İçişleri Bakanlığı, Kültür Bakanlığı, DPT, Rekabet Kurumu, Türk Patent Enstitüsü,TSE, PTT, Türkiye Bankalar Birliği, TOBB, ASO, İSO, TÜBİTAK-UEKAE, TÜBİTAK-BİLTEN, ODTÜ-DNS Yönetimi, İnternet Servis Sağlayıcıları., Tüketici Dernekleri.
4. Dış Ticarette e-Belge	Gümrük Müsteşarlığı - DTM	Maliye Bakanlığı, DTM Serbest Bölgeler Gn. Md.lüğü/İSBİ, TSE, TOBB, Eximbank, TİM,İGEME, Bankalar Birliği, Türkiye Noterler Birliği, Sigorta ve Reasurans Şirketleri Birl., PTT/Uluslararası Posta

		Birl., İhracatçı Birlikleri, TÜBİTAK-UEKAE, UND,Türk Bilişim Vakfı, MİLSOFT.
5. Vergi-Muhasebe	Maliye Bakanlığı	SPK, TÜRMOB
6. Finans ve e-Ödeme Sistemleri	TCMB	Maliye Bakanlığı, Hazine Müsteşarlığı-Sigortacılık ve Banka Kambiyo Gn. Md.lükleri, BDDK, TSE, PTT, Bankalar Birliği, Bankalararası Kart Merkezi.
7. Kamuda e-ticaret ve hizmetler	DPT	Adalet Bakanlığı, Milli Savunma Bakanlığı-STANAC, Maliye Bakanlığı, Sağlık Bakanlığı, Çalışma Bakanlığı, Gümrük Müsteşarlığı, SSK, Emekli Sandığı, Bağkur, DMO, TSE, ATO, TOBB/CALS, Bankalar Birliği, Türkiye Noterler Birliği, Türkiye Belediyeler Birliği, TBD, Üniversiteler.
8. Tarım	Tarım ve Köyişleri Bakanlığı	Maliye Bakanlığı, Sanayi ve Ticaret Bakanlığı, Hazine Müsteşarlığı-KAF Gn. Md.lüğü, TSE, TMO Genel Müdürlüğü,TOBB, Polatlı Ticaret Borsası, TÜBİTAK-UEKAE, TZOB,Yem Sanayicileri Birliği, Makarna Sanayicileri Birliği, FİSKO Birlik, Akdeniz Yaş Meyve Sebze İhracatçıları Birl., Üniversiteler, Sivil Toplum Kuruluşları, Un Sanayicileri Derneği, TARİŞ, MİLSOFT.

3.3.2 DTM Hukuk Çalışma Grubu'nun faaliyetleri:

Dış Ticaret Müsteşarlığı koordinatörlüğü'ndeki Hukuk Çalışma Grubu 29.06.2001 tarihli toplantısında; elektronik imza ile ilgili kanun taslağını hazırlamak üzere Adalet Bakanlığı, Gümrük Müsteşarlığı, Devlet Planlama Teşkilatı Müsteşarlığı, Merkez Bankası, PTT Genel Müdürlüğü ve Dış Ticaret Müsteşarlığı ve Kurumumuz temsilcilerinden oluşan Hukuk Alt Çalışma Grubu kurulmuştur [94].

Hukuk Alt Çalışma Grubu 10.07.2001 tarihinden itibaren çalışmaya başlamış, ülkemizde elektronik veri ve elektronik sözleşme konularında herhangi bir yasal düzenleme bulunmaması nedeniyle, hazırlanacak kanun taslağında bu düzenlemelere de yer verilerek çalışmanın genişletilmesi kararlaştırılmıştır. Bu çalışma sonucunda, uluslararası uygulamalar, AB mevzuatı ve 22.05.2001 tarihinde yürürlüğe giren yeni Alman Elektronik İmza Kanunu göz önünde bulundurularak ve Türk hukuk sisteminin özellikleri

dikkate alınarak "Elektronik Veri, Elektronik Sözleşme ve Elektronik İmza Kanunu Tasarısı Taslağı" hazırlanmıştır. Taslak 01.02.2002 tarihinde ETKK Hukuk Grubu üyelerine gönderilerek görüşleri alınmış, gelen görüşler üzerine Taslağa son şekli verilerek, 17.04.2002 tarihinde Başbakanlığa gönderilmiştir .

ETKK Hukuk Grubunun çalışmaları devam ederken, Adalet Bakanlığı 14.01.2002 tarihli yazısı ile çeşitli kurum ve kuruluşlardan elektronik imzanın düzenlenmesine ilişkin kanun taslağının hazırlanması için oluşturulacak komisyona temsilci bildirilmesini talep etmiş, oluşturulan komisyonun hazırladığı "Elektronik İmzanın Düzenlenmesi Hakkında Kanun Tasarısı" Taslağı 10.09.2002 tarihli yazı ile kurumların görüşüne sunulmuş ve Taslak Başbakanlığa gönderilmiştir.

Seçimler sonrası 59. Hükümetin kurulması üzerine, Adalet Bakanlığı hazırladığı Kanun Tasarısı Taslağını yenileyerek Başbakanlığa tekrar göndermiş, itirazı bulunan Kurumların görüşleri alınıp, Taslağa son şekli verildikten sonra Tasarı imzaya açılmış ve T.B.M.M.'ne sevk edilmiştir [94].

3.3.3 Kurumumuz Faaliyetleri

Kurumumuz ilk olarak Dış Ticaret Müsteşarlığının Güvenli Ağlar ve Akıllı Kartlar- İdari Altyapı grubunun çalışmalarında yer almıştır. Daha sonra Dış Ticaret Müsteşarlığı koordinatörlüğündeki Hukuk Çalışma Grubu 29.06.2001 tarihli toplantısında kurulan Hukuk Alt Çalışma Grubunun çalışmalarında yer almıştır. Adalet Bakanlığı tarafından hazırlanan ve Meclis'e sevkedilen Kanun Tasarısında sorumlu kurum olarak Kurumumuz tanımlanmıştır. Bu bağlamda Kurumumuzun elektronik imza ile ilgili yönetmelikleri bir yıl içerisinde çıkarması gerekmektedir.

e-İmza kanun tasarısı yönetmelik çalışmalarına başlanılmasını teminen Kurumumuz Bilgi Teknolojileri Daire Başkanlığı koordinatörlüğünde, Ulaştırma Bakanlığı, Adalet Bakanlığı, Sanayi ve Ticaret Bakanlığı,

Başbakanlık Dış Ticaret Müsteşarlığı, TÜBİTAK-BİLTEN, TÜBİTAK-UEKAE, Başbakanlık Gümrük Müsteşarlığı, Türkiye Odalar ve Borsalar Birliği (TOBB), Türkiye Bankalar Birliği, Türkiye Noterler Birliği gibi kurum ve kuruluşların da katılımıyla "e-imza Koordinasyon Kurulu" oluşturulmuş ve bu Kurul çalışma yöntemini belirlemek amacıyla ilk toplantısını 31.01.2003 tarihinde yapmıştır. Bu toplantı sonucunda oluşturulan kurulun genişletilmesine karar verilmiş olup bu karar doğrultusunda KOSGEB, Çankaya Üniversitesi, Yıldız Teknik Üniversitesi, Sakarya Üniversitesi, Gazi Üniversitesi, Orta Doğu Teknik Üniversitesi, Hacettepe Üniversitesi, Ankara Üniversitesi, Eximbank, T.C.Merkez Bankası, Tüm İnternet Derneği, Bilişim Derneği, Bilişim Vakfı, gibi kurum ve kuruluş, banka ve üniversitelerin de kurula katılımı için girişimler başlatılmıştır.

DÖRDÜNCÜ BÖLÜM

4. TELEKOMÜNİKASYON PAZARI İLE İLGİLİ REGÜLASYONLARIN ELEKTRONİK TİCARET ÜZERİNE ETKİLERİ

Telekomünikasyon politikasının gelişimi, elektronik ticaretin gelişiminde önemli bir temel oluşturmaktadır.

Bu bölümde telekomünikasyon regülasyon kurumlarının elektronik ticaretle doğrudan ilişkili olduğu konulara değinilecektir. Sözkonusu konuların elektronik ticaretin yapı taşlarını oluşturacak olan telekomünikasyon altyapısı, servisleri, kapasitesi ve maliyetinin kapsamı ve doğası üzerinde dolaylı etkileri bulunmaktadır.

Liberalizasyon ve telekomünikasyonun dünya geneline yaygınlaştırılması işlemi 1990 ların sonlarına doğru hızlanmış olup geleneksel haberleşmeye erişimin, etkinliğin, yenilikçiliğin, geliştirilmesi ve endüstride masrafların azaltılarak ulusal sosyal projelerin geliştirilmesi temelindeki amaçları hızlandırmıştır. OECD ülkeleri içerisinde özellikle telekomünikasyon alanında oldukça iyi neticeler alınması bunun kanıtıdır. Bu geçiş süreci ülkeden ülkeye değişmekle beraber çoklukla (i) PTT'nin doğrudan devlet kontrolünden alınarak yürütmeye yönelik ve düzenleyici fonksiyonlarının birbirinden ayrılması, (ii) telekom operatörlerinin özelleştirilmesinin sonucunda (iii) pazarın serbestleştirilmesinin sağlanması ve serbestleşmenin uygulanması ve denetlenmesi amacıyla telekomünikasyon regülasyon kurumlarının kurulması yollarını izlemektedir.

İnternetin doğuşuyla ortaya çıkan elektronik ticaret telekomünikasyon altyapısı, servisleri ve pazar yapısının dünya ekonomisi açısından çok önemli bir yer teşkil etmesine yol açmıştır. Bu bağlamda telekomünikasyon altyapısı, servisleri ve pazar yapısıyla ilgili politik yönelimler halihazırda başlamıştır ve oluşan yeni ticari çevrede anılan politika konuları tekrar

incelenmeye yada en azından yeniden ele alınmaya ihtiyaç duymaktadır [63]. Bu ise telekomünikasyon regülasyon kurumlarının sorumluluğunda olan bir konudur.

Telekomünikasyon düzenlemeleri, gelişmekte olan dünyada elektronik ticaret fırsatlarının açılımının sağlanmasında büyük öneme haizdir. Dünyanın bir çok bölgesi geçen on yıllık süre içerisinde piyasa yönelimli, etkili, erişilebilir şebeke ve servislerin kurulması amacıyla telekomünikasyon politikalarında ve piyasa yapısında önemli değişimlere sahne olmuştur. Tekellerin kaldırılması, küresel rekabetin başlatılması görevi ve piyasa değişimlerine adaptasyonu kolaylaştırma konularının birincil sorumluluğu yeni kurulmakta olan düzenleyici kurumlara verilmiştir. Elektronik ticaretin ülkelerin kalkınmalarını sağlayan yeni bir güç olarak ortaya çıkması ile, bu amaçlar daha kaçınılmaz olmuştur. Piyasa güçlerini destekleyen düzenleme konuları aşağıdaki gibi sıralanabilir [67]:

- Pazar yapısı regülasyonu, lisanslandırma
- Kaynak tahsisi
- Tarife regülasyonu
- Arabağlantı regülasyonu
- Uyuşmazlıkların çözümlenmesi
- Stratejik planlama ve koordinasyon

Pazar yapısı regülasyonu ve lisanlandırma: Liberalizasyon işlemi (bazen "deregülasyon" olarak da adlandırılır) etkili regülasyon çalışmalarına oldukça bağlıdır. Başlangıçta bu kapsamla ilgili kararların alınması, zamanlama ve pazara yeni giren kuruluşların lisanslandırılmasını da içerecek şekilde pazarın serbestleşmesi ile ilgili kriterleri içermektedir. Pazarın oluşturulması ve oyuncuların sorumlulukları ile ilgili kararlar daha ileri düzeydeki düzenlemeleri ve pazar gelişmelerinin safhasını oluşturacaktır.

Kaynak Tahsisi: Regülasyon kurumları bir bakıma pazarın geliştirilmesi için gerekli olan kaynakların tahsisinin kontrolünü sağlarlar. Bunların arasında her türlü frekans tahsisi, merkezi veri tabanı ve numaralandırma planı tahsisleri, ayrıca evrensel hizmet fonları ya da buna eşdeğer sübvansiyon mekanizmaları gibi mali kaynakların muhtemel tahsisi yer almaktadır.

Tarife regülasyonu: Rekabetçi güçler temel telefon servislerinin sınırlandırılmasında etkili olmadığı durumlarda, regülasyon kurumları baskın operatörlerden tahsil edilmekte olan tarifelerin denetlenmesinden sorumludur. Elektronik ticaretin kapsamında veri transmisyon servislerine etkili bir şekilde erişim sağlanması, kullanıcılar ve servis sağlayıcıların internete ve diğer çevrimiçi kaynaklara erişiminin sağlanması açısından çok önemlidir.

Arabağlantı Regülasyonu: Şebeke servisleri rekabete açıldığında, regülatörün sorumluluğu rekabetçi piyasanın denetlenmesidir. Arabağlantı yeni operatörlerin eşit anlamda rekabet edebilmesi için yeni operatörler etkin operatörün şebekelerine erişim ihtiyacında olduğundan bu görevde en temel unsurdur. Serbest pazar uygulaması servislerin gelişmesinde hayati bir unsur olduğundan elektronik ticaret için gerekli uygulamalar, teknolojiler ve altyapı bu düzenleyici uygulama mekanizması bu alandaki politikanın kritik özelliklerinden birisidir.

Anlaşmazlıkların Çözümlenmesi:

Rekabet, arabağlantı, tarifelerin v.s. düzenlenmesi için kullanılan araçlar ve standartlara ek olarak regülasyon kurumları, servis sağlayıcıların arasında ve servis sağlayıcılarla kullanıcılar arasındaki anlaşmazlıkların çözümünde ve bu konularla ilgili yasa ve düzenlemelerin uygulanmasında sorumluluk üstlenmektedirler. Bu fonksiyon çoğunlukla medyatik görüşmelerin oluştuğu noktalardan birisidir. Etkili bir regülasyon kurumu böyle bir arabuluculuk rolü ile politikalarını uygulatabilir.

Stratejik Planlama ve Koordinasyon:

Telekomünikasyon regülasyon kurumları telekomünikasyon endüstrisindeki eşsiz pozisyonları ve ilgileri sebebiyle modern haberleşmeden doğan ekonomik kalkınmayla ilgili hükümet sektörleri arasındaki müzakerelerde önemli bir rol oynamaktadır.

Telekomünikasyonu düzenleyici politika, bu özel fonksiyonlara ek olarak, ticari yasa, teknik standartlar ve elektronik ticareti ilgilendiren politik kararlardan etkilenmektedir ve etkilemektedir.

Telekomünikasyon Pazarı Regülasyon Konuları:

Ne zaman regülasyon yapılmaması gerektiği yeteneğini içinde barındıran yaratıcı ve koordineli uygulamalar, büyük ve küçük iş çevreleri, tüketiciler ve kamu kuruluşlarının küresel ekonomiden faydalar sağlayabilmelerinde önemli rol oynayabilir [96].

Telekomünikasyon regülasyon kurumları elektronik ticaretin kaderini belirleyecek güce sahiptirler. Bu temel alanlarda alınan kararlar özellikle kısa dönemde alınmış olanlar iş imkanlarının şekillenmesinde ve küresel elektronik ticarete katılan ülkelerdeki tüketiciler için özellikle önemli olacaktır. Ulusal ve uluslararası politikalar elektronik ticaretin dünya ölçeğinde gelişiminin tanımlanmasını yardımcı olacaktır.

Bu bölümde elektronik ticaretin gelişimini doğrudan ilgilendirmekte olan

- Altyapı
- Evrensel hizmet
- Pazar yapısı, rekabet, lisanslandırma
- Ekonomik ve ücretlendirici regülasyon

olmak üzere dört önemli telekomünikasyon regülasyon alanı incelenmektedir.

4.1 Altyapı

Haberleşme ve bilgi teknolojisi altyapısı elektronik ticaretin ortaya çıkışında önemli bir yer teşkil etmektedir. Servis sağlayıcılar, ekipman üreticileri, tüketiciler, işlerini elektronik yollardan yaparak yenilikçi yolları kullanmaktadırlar [86].

Elektronik ticaretin oluşturulması ve geliştirilmesi ile ilgili şebeke altyapısı ve teknolojileri ile ilgili politikalar elektronik ticarete katılım için bir ön gerekliliktir.

Bilgi teknolojisinin altyapısının oluşturulması yine telekomünikasyon düzenleyici kurumlarının sorumluluğu altında yer almaktadır. Bunların içerisinde internet ve e-ticaret servislerinin sağlandığı kamu transmisyon şebekeleri, omurga şebekeleri ve son kullanıcıya erişim bağlantıları ve bu elemanlar arasındaki arabağlantı da yer almaktadır. Bazı durumlarda, regülasyon kurumları çeşitli yazılım ve donanım elemanları üzerinde söz sahibi olabilmektedirler.

Elektronik ticareti destekleyen telekomünikasyon altyapısı temel olarak üç unsurdan oluşur: omurga şebekeler, erişim servisleri, ve son kullanıcı ekipman ve servisleri. Elektronik ticaretin sağlıklı bir şekilde uygulanmasını teminen sayılmış olan üç temel unsur için yatırım, büyüme ve ar-ge imkanlarının sağlanması gerekmektedir. Genel olarak, altyapının geliştirilmesi yönetimi konusu doğrudan düzenleyici kurumların görevi olmasa da pazar iştiraki ile ilgili telekomünikasyon politikaları operatörler için şebeke hizmetlerinin kalitesini arttırmalarını sağlayan teşvikleri etkilmektedir [90].

İnternetin omurgasını oluşturan yüksek hızlı uluslararası veri şebekeleri aslında regüle edilmemiştir. Çoğu ülkede ulusal operatörler yerel internet servis sağlayıcıların ve son kullanıcıların internete bağlanmakta kullandıkları temel ve tek yerel omurgayı kurmuşlardır. Bu tip bir tekelci kontrolün özellikle

yüksek hızlı transmisyon servislerinde sağlanması durumunda, bağlantının zayıflığı ve kısıtlanması riskini haklı çıkarmak çok güçtür.

Omurga altyapısı teknolojisiyle ilgili nazaran ulusal tekel durumundaki operatörler bile düzenleyici bir müdahale olmaksızın yeterli seviyedeki yüksek hızlı veri transmisyon kapasitesi sağlayarak, yerel ve sınır ötesi internet trafiğini destekleyebilirler. Telekomünikasyon pazarının veri transmisyonu rekabetine tamamen açık olmaması durumu telekomünikasyon regülasyon kurumlarının ulusal omurga şebekelerinin genişletilmesi konusuyla ilgilenmeleri için sebep oluşturabilir. Regülasyon Kurumları ayrıca ticari amaçlar için kullanılan internette omurga transmisyon şebekelerinin bağlantı kalitesi, güvenilirlik ve gizliliğini sağlamaya hazır olmalıdırlar.

Altyapı üzerindeki regülasyon etkisinin en etkin olduğu alan şebeke bağlantısı esasına dayanmaktadır. Temel haberleşme altyapısı e-ticaret uygulamaların en az üç boyutta etkilemektedir:

a) Sağlanabilirlik (Kullanılabilirlik): Tüketiciler ve iş çevreleri öncelikle küresel elektronik piyasalara bağlantılı olan telekomünikasyon şebekelerine erişme imkanına sahip olmalıdırlar. E-ticaretin hızla gelişmekte olduğu gelişmiş dünyada bu temel ihtiyaç en fazla adreslenmekte olup gelişmekte olan ülkelerde ise bu imkanı sağlayan evrensel hizmete ulaşmak amacının gerçekleştirilmesini sağlamak oldukça uzak gözükmektedir.

b) Kapasite: Telekomünikasyon erişiminin evrensel olarak sağlandığı gelişmiş olan ekonomilerde bile e-ticaret gibi yeni uygulamalar temel telefon şebekesinin transmisyon kapasitesine, özellikle yerel ağa oldukça bağlıdır. İnternet geliştikçe metin, grafik, ses ve video özellikleri de tümüyle gelişmeye devam edeceğinden dolayı içeriğin kalitesi artacak, ticari kuruluşlar, reklamcılara açık olan çevrimiçi çevre eğlence sektörüne de katkıda bulunacaktır. Ancak yerel ağ hizmetlerinin çoğu düşük hızlı, analog sayısal olmayan multimedya servisleri kullanacak şekilde oluşturulmuştur.

Modem teknolojisi çevirmeli (dial-up) internet kullanıcılarının çevrimiçi uygulamalarında bir sıçrama yaratmışsa da gerçekleştirilenler ve şu anki kamu anahtarlamalı telekomünikasyon şebekesi (PSTN) üzerinden gerçekte yapılabilecek olanlar arasında önemli bir fark vardır.

Gelişmiş şebekelere sahip olan ülkelerde ise yerel ağ yapısının ve servislerinin fiber optik ağlarla, ISDN ya da sayısal ağ taşıyıcı sistemleri ve varolan diğer seçeneklerle yüksek ölçekte geliştirilmesi ile ilgili olarak çeşitli tartışmalar yapılmaktadır. Buna ek olarak kablolu televizyon sistemleri gibi alternatif şebekeler kapasite kısıtlamalarını aşma yolunda önem kazanmaktadır.

c) Kalite ve Esneklik: Ham kapasitenin ötesinde son kullanıcıların ve servis sağlayıcıların bağlantı ihtiyaçları artarak internet kaynaklarına bağlantıda kalite ve esnekliği arttıracak gelişmiş teknoloji ihtiyaçlarına odaklanmaya başlamıştır. Konular sayısal veri tranmisyonuna mobil erişim, ISDN gibi çokkanallı servisler, dinamik band genişliği tahsisi ve yazılım ve transmisyon gerekliliklerinin entegrasyonunu içermektedir. Telefon operatörleri gereksinimlerini adreslemeye başlamışlardır ancak temel kamu anahtarlamalı telefon şebekeleri gelişmiş ticari uygulamalar karşısında yeterli esnekliği sağlayamamaktadır.

Telekomünikasyon regülasyon kurumlarının şebeke altyapısına erişim ile ilgili rolü hem doğrudan hem de dolaylıdır. Uzun vadede telekomünikasyon endüstrisi için uygun teşvikler ve yaptırımlarla yeni, deneysel, potansiyel operatörlerin katılımına imkan sağlayan tüketici yönelimli erişim teknolojileri temin etmek en etkili yoldur.

Aynı zamanda, etkin piyasaya dayalı altyapı gelişiminin çoğu ülkede önemli bir konu olarak kaldığını kabul etmek gerekir. Amerika ya da Avrupa'nın saldırgan serbest piyasa felsefeleri yerel ağın darboğazlarını azaltmıştır. Telekomünikasyon regülasyon kurumları telekomünikasyon pazarının geniş

politikaları kapsamında baskın yerel telefon şebeke operatörlerine uygulanacak pazar yönelimli teşvikleri ve yatırımları arttırıcı seçenekleri gözden geçirmeye hazırlanmalıdırlar.

d) Ekipman ve Servisler: Transmisyon omurgası ve şebeke erişim hizmetlerinin ötesinde bazı ülkelerde özel sektörün yenilikçi bilgi teknolojileri ve telekomünikasyon altyapı politikalarının bir unsuru olarak doğrudan son kullanıcıya servis ve ekipman sağlamada katılımı hususunda genel bir ilgi mevcuttur. Fransa Telekom, kamu sektörü operatörü ve fiili regülatör olarak terminal ekipmanları dahil olmak üzere tüm servis bilgi sistemine geçme kararını açıklamıştır. Telekomünikasyon regülasyon kurumları telefon ekipmanlarının ve diğer ekipmanların tip onay işlemlerinde yer almakta, hatta bazı ülkelerde daha da ileriye giderek örneğin sadece yerel üreticilerin tarafından geliştirilen bazı spesifik modellerin kullanılması zorunluluğunu koymaktadırlar.

Servisler bağlamında regülasyon kurumu spesifik teknolojiler ve uygulamalarını (örneğin GSM, mobil servisler, ISDN) geliştirme ve teşvik etmeye yönelik girişimlerde yer almaktadırlar. Ancak varolan operatörler bunların başlatılmasında yavaş davranabilmekte ya da farklı bir lisans alınmasını zorunlu kılmaktadırlar. Aşağıda tartışılacak olan seçenekler altında bu yaklaşım ancak regülasyon kurumunun girişimleri pazarı başarısızlıklarını tazmin ettiği durumlarda duruma acil müdahale anlamında önerilebilir. Elektronik ticaret için ise yeni tip ekipmanlar ve servislerin pazara çok hızlı girişinin yapılması regülasyon kurumlarının bu gelişmeleri gözden geçirmeleri için bir sebep teşkil etmektedir. ISDN gibi teknolojilerin yavaş bir şekilde geliştiği bazı ülkelerde pazarın bir bütün olarak yeniden yapılandırılmasının bu teknolojiler için yeni tahsisler yapılmasından daha iyi bir yöntem olacağı düşünülmektedir.

4.1.1. Altyapı Regülasyonu ile İlgili Seçenekler

Regülasyona yönelik müdahaleler altyapının yukarıda bahsedilmiş olan boyutlarıyla gelişimi üzerinde etkiye sebep olabilir. Aşağıda elektronik ticaret fırsatlarının gelişimini destekleyici kapsamda çeşitli ülkeler tarafından telekomünikasyon altyapısını geliştirmekte uygulanmakta olan yaklaşım seçenekleri

- Pazarın karar vermesine imkan sağlamak
- Teşvik edici regülasyon (Risk ve ödül)
- Servis ve teknoloji yönetimi (Merkezi kontrol)
- Sınırda regülasyon

olarak sıralanabilir.

Pazarın karar vermesine imkan sağlamak

Regülasyon kurumunun telefon operatörü gibi oldukça karmaşık bir şirketle ilgili kararlar vermesi bazen bazı yanlışlıklara sebep olabilir. Doğal olarak şebeke operatörü hangi teknolojileri kullanacağı, yönetimi, müşteri ihtiyaçları ve maliyeti konusunda daha çok bilgi sahibidir. Regülasyon kurumlarının görevi kuruluş planlarını onaylamak, hangi teknolojilerin çağdışı olduğuna karar vermek olmalıdır.

Bu sebeple altyapının geliştirilmesine yönelik ilk seçenek bu olmalıdır. Telefon operatörleri kendi müşterilerine hizmet etmede serbest bırakılmalıdırlar. Bu güçlü teşviklere sahip olan operatörlerin geniş seçenekli ve en iyi kalitede servis seçeneklerini sunacağı düzenleyici bir müdahalenin olmadığı rekabetçi piyasalar için doğrudur. Müspet geliştirme kararlarının alınma zorunluluğu uygun ve istenilen teknolojiler tatminkar bir biçimde kullanılmadığı zamanlarda ortaya çıkmalıdır. Bu yargılama diğer mukayese edilebilir pazarların incelenmesi ve sağlanabilir seçenekler ve maliyetlerin yer aldığı uzman raporları temeline dayandırılabilir. Diğer seçenekler ise bu tip

durumlar sözkonusu olduğunda regülasyon kurumlarının altyapı geliştirme seçeneklerinin yollarına değinmektedir.

Teşvik edici regülasyon (Risk ve Ödül)

Telekomünikasyon pazarı tümüyle açık olmadığı zaman ya da geçiş dönemindeyken, zorunlu işletmeciler en uygun altyapı ve teknoloji yatırımı için yeterli teşviklere sahip olmayabilirler. Karı arttırmayı amaçlayan tekelci teşvikler tüketici memnuniyetini arttırmayı hedeflemeyebilir. Düzenlenmiş olan servis tarifeleri, operatörün yatırım maliyetlerini karşılamasına izin vermediğinde yeni teknolojiler ve şebeke yenilenmesinde yatırım noksanlığı olarak ortaya çıkar. Öte yandan operatörlerin gelirlerinin maliyetlerini eşit olarak karşılayacak şekilde düzenlendiğinde ise gereğinden fazla yatırım durumu ortaya çıkar. Bu tip bir durum daha etkin olan teknolojilerden sapma ve son kullanıcıya ait ücretlerin artması sonucunu doğurur.

Regülasyon kurumu, operatörlerin müşterilerin ihtiyaçlarını karşılamadığı durumlarda hangi pazarlarlar için hangi teknolojilerin uygun olduğunu bilme yönünden zayıf durumdadır. Ancak rekabetçi pazarı yaratmayı teşvik edici şekilde düzenleyici çevreyi değiştirmek yoluyla bu sağlanabilir. Operatör için teşvik edici regülasyon prensibi, riskleri göğüsleyerek uygun altyapı yatırımlarının ödüllerini toplamaktır. Bunun için gerekli araçlar arasında esnek ücretlendirme ve kazanma standartları, temel olmayan servis tarifelerinin bir çoğunun yeniden düzenlenmesi ve bazen teknolojinin yayılımının sağlanması için özel hedefler yer almaktadır. Operatör ve regülasyon kurumu yeterli talep olduğu zaman oluşan maliyetin karşılanması için mahsurlu yatırım seçeneklerinden fayda sağlanamayacağının farkında olarak operatörün pazar yönelimli kararlar almasında son sorumluluğu vermekte olan kamu politikası konuları ve amaçlarını bir sosyal anlaşma şeklinde müzakere etmelidirler.

Servis ve Teknoloji Yönetimi (Merkezi Kontrol)

Regülasyon kurumları bazı durumlarda kamu ilgisini arttırma sorumluluğu dolayısıyla teknoloji geliştirme fırsatlarında daha doğrudan yer almaya başlamışlardır. Bu yaklaşım açıkça belirtilmiş olan bir teknoloji trendi olduğu zaman oluşur. Sayısal anahtarlama teknolojisine geçişte ya da hücresel mobil servislere ve kablosuz yerel ağlar gibi lisanslandırma, frekans tahsisi ve diğer regülasyon kararları v.b. gerektiren teknolojik gelişmelerde gelişmiş elektronik ticaret uygulamalarına fırsat veren teknolojiler için -örneğin yüksek hızlı bağlantılar- belirlenmiş özel bir teknoloji seçimi (örneğin ISDN, DLC, ADSL, fiber kablo, v.s.) konuları buna örnek olarak verilebilir. Geçmiş yıllarda bu tip seçimler yapılmıştır.

Sınırda Regülasyon:

Teoride altyapının geliştirilmesi seçeneklerinin özel işletmecilerin teşviklerine bağlı olacağı ve her şey hakkında bilgi sahibi olan regülasyon kurumunun belirleyeceği sosyal ve ekonomik açıdan ideal altyapı arasını bölen ince bir çizgi olmalıdır. Daha önceden tartışıldığı gibi pazar yönelimli teşvikler müşterilerin ihtiyaç duymakta oldukları teknolojilerin maliyetlerinin belirlenmesine kadar uzanmalıdır. Bu pazar teşviklerinin serbest bırakılması için operatörlerin kendi ihtiyaçlarını hükümetin yönetiminde etkin olarak belirlemeleri beklenmektedir.

Haberleşme şebekelerinin elektronik ticaretin sonuçlarından kaynaklanan faydaları, talepte bulunmasalar bile altyapının geliştirilmesinin kendileri için iyi olacağına karar verecek olan müşterileri gerekli ödemeleri yapmaları için isteklendirecektir. Bu ise sınırda regülasyona yönelik bir müdahaleyi doğurmaktadır.

Bu durum şebeke erişiminden doğrudan yararlanan müşteri gruplarının ödemeler için eşit kabiliyette olmadığı anlamına gelmektedir. Bu durum ayrıca yatırım ve teknoloji seçimleri için marjinal zaman cetvellerini

gerektirmektedir. Örneğin telefon şirketi kendi erişim şebekelerini belirtilen süre içerisinde bölgelerinin çoğuna sayısal erişimi sağlayacak şekilde yenilemek için bir plan ortaya koyabilir.

Bu planın objektif olarak gözden geçirilmesi için regülasyon kurumunun uzmanları, hız ve gelişim dolayısıyla elektronik ticaret uygulamaları sayesinde beklenmesi muhtemel ekonomik faydaların sağlanacağını belirleyebilirler. Bu belirleme gelişimin hızlandırılmasında teşvikler ya da yaptırımlar için operatörlerle bir anlaşmaya varışın temelini oluşturabilir.

Buradaki temel nokta regülasyon kurumunun marjinal faydaların üzerinde yoğunlaşarak varolan ya da yeni şebeke operatörlerinin bunu gerçekleştirmesi için gerekli en iyi yolu bulmasından geçmektedir. Eğer pazar güçleri gerekli altyapı ve geliştirme için zorlanmakta ise, böyle bir yatırım için bir düzenleme yapmaya gerek yoktur. Eğer kamu yararı tümüyle iş teşvikleriyle uyumlu değilse regülasyon bu devinimi (itmeyi) sağlamalıdır.

4.2 Evrensel Hizmet

Telekomünikasyon sektöründe evrensel hizmetin desteklenmesi teknoloji pazarındaki değişimler ve regülasyon koşullarıyla birlikte yeni bir oluşum sürecine girmektedir. Geleneksel olarak evrensel servis politikasının amacı, telefon haberleşmesinin en fazla kişi ve yere ulaştırılmasıdır.

Geçmişte bu amaçla ilgili olarak telefon servislerindeki devlete ait tekeller kaldırılırken

- Kırsal ve fakir bölgelere hizmet sağlanmasının özel sektör operatörlerine cazip gelmeyeceği ve

- Tekel durumundaki kuruluşların kırsal bölgelerdeki iş ve bilgi servislerinden sağladığı karın arttırılmasına yönelik evrensel servis

fonununu oluşturabilmek için büyük çapraz sübvansiyonlar yapması gerektiği

kabul edilmekteydi.

Gelişmekte olan dünyada evrensel servisin değişen perspektifi, devlet tekellerinin verimsizlik, zayıf yönetim, yetersiz mali kaynak ve diğer sebepler dolayısıyla telefon servislerinin erişime açılması bağlamında yeterli gelişmeyi sağlamada başarısız olduğunu göstermektedir.

Aynı zamanda yenilikçi teknolojiler (kablosuz yerel ağ, akıllı telefon kartları, uydu telefonları) ve pazarın gelişmesi ve genişlemesi müteşebbislerin düşük gelirli kırsal kesime ekonomik olarak uygun telefon hizmetlerini sağlamak hususundaki ilgisini arttırmıştır. Evrensel hizmet politikası geniş pazar liberalizasyon insiyatifleriyle daha uygun ve tamamlayıcı olmaktadır. Çapraz sübvansiyon ile pazar gelişmelerini desteklemek için iç ücretlerin ve kaynakların bozulmasından çok bir fon sağlama mekanizması hedeflenmelidir.

Gelişmekte olan ülkeler için, evrensel hizmetin telefon servisi için sağlanması, ya da evrensel hizmetin haberleşme ve bilgi teknolojileri için sağlanması, telekomünikasyon politikasının en önemli öğesi olmuştur. Elektronik ticaretin gelişmesiyle evrensel hizmet fırsat ve kısıtlamaları için geçerli olan temel geleneksel görüşleri değiştirebilecek olan yeni bir dinamik belirmeye başlamıştır.

Elektronik ticaret telekomünikasyon erişiminin maliyetini dramatik olarak değiştirme potansiyeline sahiptir.

Telekomünikasyon ekonomisindeki hatırlanması güç analitik sorulardan biri telefon servislerinin kırsal nüfusa makroekonomik şartlara bağlı olarak ulusal ve yerel seviyede açılmasının etkisidir.

Elektronik ticaret bu hesaplamayı değiştirecek potansiyele sahiptir. Telekomünikasyon şebekeleri tüketici satın almalarında birincil bir kaynak olmuşken pazarlama, mali belgeler ve çevrimiçi bilgi ve hükümet servisleri ve bu şebekelere bağlanmanın kazandırdığı doğrudan faydalar daha hız ve saydamlık kazanmıştır. Tüketiciler açısından ürünleri elektronik yollardan satın almak mümkün kılındığı takdirde zaman, taşıma, gönderim maliyetleri azalacak bilgi ve seçim imkanlarını artacak ve bu tip ticarete erişim için ödenecek olan ücretlerin ödenmesine yönelik istek artacaktır.

Bu arada, şebeke kullanıcıları için yeni bir kategori gelmektedir: pazarlama ve satışları büyük ölçüde internet tabanına dayanan, tüketicilere ve iş çevrelerine ürün ve servis sunan hizmet sağlayıcılar. Bu hizmet sağlayıcılar için bağlantı kalitesinin sadece kendileri için iyi olması yetmez müşterilerinin de aynı imkanlara sahip olmaları gerekir.

Endüstri dinamiği varolduğu sürece e-ticareti destekleyen sektör telekomünikasyon sektörüne evrensel servisin geliştirilmesi yönünde müdahale edecektir. Ticari sektörlerde "erişim teşviki" olarak adlandırılan bir büyük örnek vardır. Bu bağlamda;

- Hücresel telefon operatörleri bağımsız üreticiler tarafından sağlanılan düşük ücretli telefonları müşterilerine abonelik hükümlerinde sağlarlar.

- Dergi basımcıları okunma oranını arttırmak ve altyapının basımın son kullanıcıya ulaşması için gerekli altyapıyı, son kullanıcıya reklamlara para ödemelerini sağlayarak kurabilirler.

- Ticari televizyon endüstrisi yayıncılığı modelinin tümü, şebeke altyapısının tüketicilerin diğer servis ve ürünlere erişim talebini arttırmaya yönelik olarak tüm kullanıcılara ücretsiz olarak sağlanmasına bir örnek teşkil etmektedir.

Bu yüzden elektronik ticaretin diğer pazarlama ve satış araçları oranında geliştiği söylenebilir.

Aynı zamanda, ticari sağlayıcılara erişime yönelik tüketici talebi şebekenin yenilenmesi ve gelişimi için gerekli gelirleri arttırabilir ve bu tip yatırım teşviklerinin katlanarak artmasını sağlayabilir.

Bu ihtimal temel geleneksel telefon ekonomisi ve evrensel servis politikasıyla o kadar farklılık göstermektedir ki, bizleri bu tip konulardaki öngörülerimizi tekrar gözden geçirmeye itmektedir. Ticaret ve telekomünikasyonun evliliğinin evrensel hizmeti bir gerçeklik olarak gösteren devlet tekelleri ve çapraz sübvansiyonlara dayalı olan ulusal stratejilerin çökmesinde hızlandırıcı bir rolü olabilir mi? Bu sorunun yanıtını bulmak istersek;

Evrensel hizmetin bu yeni modelinde teklif edilen topluluk ve ulusal refah bağlamında en hayati olan "temel" haberleşme hizmeti artık telefon olmayacaktır. Son yıllarda, temel telefon servisleri dünya genelindeki telefon yaygınlık oranı standardı, hatların sayısı ya da yüzdesi ya da kırsal kesimlere en yakın telefon mesafesinin ölçülmü ile tanımlanarak temsil edilmiştir.

Elektronik ticaret, veri haberleşmesinin metin, grafik, ses, veri transmisyonuna dönüştürülmesine bağlıdır. Aslında, ülke evrensel hizmeti tartışmalarının ötesinde, telekomünikasyon endüstrisi, sese dayalı şebeke altyapısından veriye dayalı şebeke altyapısına geçiş problemiyle karşı karşıyadır.

Bilgi tabanlı ekonomiye geçiş faydalarının telefon haberleşmesine nazaran daha kapsamlı ve hızlı olduğu ispatlanabilirse, evrensel hizmet politikaları ve yatırımları kendiliğinden yön değiştirebilir. Bu konuyu çözümlemek için evrensel haberleşmenin az gelişmiş, fakir, kırsal nüfuslar için faydalarının neler olduğu tanımlanmalıdır.

Teknoloji değişirken, yalnızca telefon hizmetinin sağlanmasıyla ihtiyaçların karşılanıp karşılanmadığı, gereken faydaların sağlanıp sağlanmadığının belirlenmesi gerekir.

İdeal bir dünyada, teknoloji temel telefon hizmetlerini geliştirirken bu tip seçimlerin yapılması zorunlu değildir. Bu arada, seçilen yol önemsenmeden yalnızca teknolojinin geliştirilmesi de yeterli değildir. Elektronik ticaret teknolojilerinin az gelirli, kırsal nüfuslara değerli kılmak için, bu kullanıcıların sözkonusu teknolojileri anlayarak kullanmaları gerekmektedir. Bu ise yanlızca bilgisayar uygulamaları, teknik özelliklerin anlaşılmasına yönelik bir eğitimle değil aynı zamanda elektronik ticaretin kişisel, iş ve cemiyet hayatını geliştirici bir çok yönünü ortaya çıkartılmasıyla mümkün olabilir.

Bu yüzden evrensel hizmet politikası, teknolojik gelişmelerin sağlanmasının yanısıra tüketicinin eğitiminin kapsanmasını da zorunlu kılmaktadır. Temel bağlanabilirliğe ve servislerin yakınsaması ve entegrasyonuna ulaşabilmeye yönelik teknik seçenekler ve pazar seçenekleri artmaktadır.

Evrensel hizmet teknolojisinin değişen doğası ihtiyaç duyulan yeni erişim çeşitlerini sunmada teknik ve pazar koşularının genişletilmesini sağlamaktadır. Bir çok ülkenin telekomünikasyon sektöründe uygulanmakta olan destekleyici trend özellikle pazarın açılım politikalarında daha fazla katılım ve yenilikçiliğe izin vermektedir.

Buradaki temel varsayım, teknolojik seçenek için bir talep varsa bunu sağlamaya istekli şirketlerinde olacağıdır. Veri transmisyonu ve kamu internet bağlantısını sağlayan erişim servislerinde bu yeterlilikler geleneksel PSTN sağlayıcılardan ayrı olarak şebeke operatörleri tarafından sağlanabilir.

Şebeke operatörleri;

- Bağımsız veri şebeke sağlayıcıları, karasal telli hatları ya da kablosuz hatları (örneğin VSAT) kullanarak kullanıcıları internet omurga servislerine, bilgi sağlayıcılarına ya da diğer şebekelere bağlayarak uygun pazar yatırımlarının ortaya çıkmasını sağlayabilirler.

- Kablolu televizyon operatörleri, yüksek hızlı internet erişimi ve uygun ekipman kullanarak gerekli özelliklere sahip servisleri sağlayabilirler. Kablolu televizyon sinyallerinin kapasitesi ve kalitesi bu servisleri e-ticaret amaçları için ideal bir aday kılmaktadır.

- Kablosuz servis teknolojileri, sayısal veri erişimi ve gönderimini destekleme kapasitesine sahip olmaktadır. Yeni modem kartları, telsiz şebeke erişiminin hücresel ya da sabit kablosuz şebekelere e-mail, internet ve diğer veri gönderim servislerini dizüstü ya da taşınabilir bilgisayarlardan bağlanabilirliğini mümkün kılar.

Elektrik güç sistemleri gibi kamu şebekeleri, veri transmisyon servisleri birleşerek yenilenmektedirler. Çoğunlukla büyüyen tüketici veri/internet erişimi bu şebekeleri destekleyici bir potansiyel yaratır.

Bu gelişmelerin düzenleyici yaptırımları ile evrensel servis amaçlarına ulaşılması özellikle evrensel servisin genişletilmiş tanımı ile haberleşme şebekeleri yoluyla ekonomik aktivitelerin arttırılması bağlamında bir çok seçeneği ortaya çıkarmaktadır.

Yerel topluluklara ve özel girişimciliğe ait ulusal politikalar, çok uluslu yatırımlar kadar önemli olabilmektedirler.

Sonuç olarak internetin dinamiği, elektronik ticaret ve kamu haberleşmesi, evrensel hizmet amaçlarını gerçekleştirmeye yönelik yerel ve ulusal

teşebbüslerden çok yeni bakış açılarının birleştirilmesine ihtiyaç duymaktadır. Geleneksel evrensel hizmet politikası daha çok ulusal kapsamlı, yerel halkın telekomünikasyon şebekesini karşılayacak kaynakları olmadığı varsayımından hareketle merkezden çapraz sübvansiyon ve kamu politikalarıyla desteklenmektedir.

Şu anda, yerel haberleşmedeki değişimlere ve yeni teknolojiler ve uygulamalarla teşvik edilmiş ekonomik tahminlere şahit olmaktayız. Telekomünikasyon erişim servislerindeki desteğinin artmasıyla yerel seviyedeki yönetimin daha iyi olacağı aşikardır. Tüm servisli telekomünikasyon şebekesinin merkezi olmayan ekonomisinde bu faaliyetlerin tümü karlı olarak ta sağlanabilir.

Bu gözlem temel haberleşme altyapısına erişim ve kullanımın arttırılarak hizmetlerin kamu yararına kullanımı için uygulanabilir.

Aşağıda, yerel girişimciler, taşeronlar, imtiyaz sahipleri ve kamu kurumları yoluyla sağlanabilecek temel servis ve hizmetler listelenmektedir.

- temel telefon şebeke erişimi (kablosuz yerel ağ)
- yerel hizmetlerin kurulması, muhafazası, bakımı, onarımı
- telefon servisleri için ücretlendirme, toplanan paralar
- ödemeli telefonlar, akıllı kartlar, satış ve servis temsilcileri
- e-posta hizmetleri dahil internet erişim hizmetleri,
- Üretici web siteleri dizayn, pazarlama, programlama, sunma
- Bilgisayar ve ekipman satışı, kurma ve muhafazası

Standart telefon hizmeti bu fonksiyonların çoğunu kapsamamaktadır. Ancak elektronik ticareti de içeren veri yönelimli erişim servisleri sağlayıcılara ve müşterilere getirdiği artan karmaşıklık aynı zamanda fırsatı yerel seviyede sunma potansiyelini yaratmaktadır.

Bu sonuç, hizmetlere erişimin artmasıyla bunların kullanımının daha etkin desteklenmesini aynı zamanda haberleşme ve teknoloji alanlarındaki yerel ticaret gelişiminde de bir ivme sağlar.

Elbetteki bu aktivitelerin çoğu piyasaya giriş serbest olsa bile bir anda kazanç getirmeyecektir. Bir çok toplulukta bireylerin yatırımları özellikle büyük projeleri gerçekleştirmek için yeterli kaynak ve tecrübeye sahip değildir.

Bu tip işler hükümet kurumları, üniversiteler, büyük özel sektör kuruluşları gibi ulusal ve bölgesel ortaklıklarla desteklenmeye ihtiyaç duyarlar. Bu destek mali, eğitim, lojistik olabileceği gibi kendi kendini idame edeceği zamana değin ya da tümüyle kalıcı olabilir. Kamu tarafından desteklenen imtiyazlı modeller, örneğin başlangıç, destek ve kaynakların paylaşımı için uygun bir mekanizma olabilir. Diğer durumlarda çekici bir pazar bulan dışarıdaki yatırımcılar yerel yöneticilerle, halk servis merkezlerine bağlı şebekeler yaratmak üzere ortaklık anlaşmaları geliştirebilirler. İhtimaller insanların kendi ihtiyaçlarını karşılamasına yönelik olarak çeşitlidir.

Sonuç olarak;

- Elektronik ticaret bilgi tabanlı ekonomiye geçişin sağlanmasında önemli bir yere sahiptir. Üreticiler geniş pazarlar ararlarken ve tüketiciler haberleşmeden gözle görülür yararlar sağlarken, arz ve talep dengesi değişmektedir.

- Telefon hizmetinin en temel hizmet olması belki de artık tarihe karışacaktır. Veri transmisyonu, elektronik posta, internet ve özellikle ekonomik gelişimi destekleyen diğer yeni servisler evrensel hizmet politikalarında hızla yer alacaktır.

- Temel bağlanabilirlik (connectivity), yakınsama, ve servislerin entegrasyonunu başarmak için gerekli olan piyasa seçenekleri artmaktadır. Pazar teşvikleri tarafından hareketlendirilen yenilikçi

teknolojiler, kırsal, düşük gelirli ve özelleşmiş kullanıcı gruplarının haberleşme ve bağlantı kalitesini artırmaktadır.

- Yerel topluluk ve girişimciliğe ait insiyatifler ulusal politikalar ve çokuluslu yatırımlar kadar önemli olabilmektedir. Yerel işletmeler, hükümetler ve organizasyonların kendi toplulukları için haberleşme hizmetlerini götürmede önder olabilmeleri için bir çok fırsat vardır.

Verilen bu değişen anlayışlar karşısında telekomünikasyon regülasyon kurumları geleneksel evrensel hizmet politika ve amaçlarını bir kez daha gözden geçirmelidirler. Özel sektör ve diğer kamu kuruluşları, sivil toplum örgütleri ile işbirliği vasıtasıyla dünya genelindeki ekonomik ve faydalı haberleşme servislerinin getirilmesine hız katacak olan tecrübeler ve en iyi uygulamalar için çeşitli seçenekler mevcuttur. Bu seçenekler için gerekli anahtar özel yerel yönetimli pazar modeli altındaki geniş teknoloji ve servislere erişimi sağlayacak olan topluluk tabanlı telemerkezlerin oluşumunu teşvik etmektir.

4.2.1 Evrensel Hizmet ile İlgili Regülasyon Seçenekleri

Yukarıda belirtilen tüm seçenekler, tüm topluluğun haberleşme çeşitlerine erişimini arttırıcı bir resim sunmaktadır. Elbette evrensel telekomünikasyon, evrensel elektronik ticareti gereği gibi eşit kılmamıştır. Teknolojinin ticari kullanımı eğitim, sağlık, hükümet servisleri, kültürel ifade gibi sosyal fayda sağlayan uygulamalarla bütünleşmelidir. Bu ek amaçları desteklemekte olan politika ve kaynaklar ekonomik stratejilerle koordine edilerek birleşmiş sistemlerin hızlı ve etkin maliyetli olarak geliştirilmesi sağlanmalıdır. Bu ise telekom sektöründeki regülasyon kurumları ve özel sektör ve hükümete bağlı diğer kuruluşlar ve bölümlerdeki görevliler arasındaki işbirliğini gerektirir.

4.3 Pazar yapısı, Rekabet, Lisanslandırma

Regülasyon kurumlarının belki de en önemli icraatları yeni operatörler için telekomünikasyon servis pazarını rekabete açma, yeni teknoloji ve

servislerin her seviyede genişlemesini sağlayan pazar değişiminin etkilerini ele almaktır.

Elektronik ticaretin temelini teşkil eden pazar yapısı genel olarak geniş, değişken bir endüstriyi kapsamakta ve uluslararası sınırlardan geçen, sayısız aracının katılımıyla üreticilerden servis sağlayıcılara, yazılım sağlayıcılarından bankalara ve nakliyat şirketlerine uzanan geniş bir yapıdan oluşmaktadır. Bu faaliyetlerin çoğu kısıtlanmamış pazarlarda gerçekleştirilmektedir. Elektronik ticaret serbest pazar ekonomistlerinin rehberi olan müşterilerin sayısız rekabetçi üreticilerden adil olarak ürün ve servis kalitesi hakkında bilgi alarak ücretleri kıyaslayabildikleri düşük belge masrafı, zaman ve yatırımın varolduğu ortamın hayata geçirilmesi ile sağlanmaktadır.

Telekomünikasyon altyapısını ve servislerini desteklemeye gelindiğinde, pazar yapısının kısıtlamaları ve regülasyonu istisnadan çok kurallara bağlıdır. WTO yoluyla yürütülmekte olan uluslararası girişimlerde bile telekomünikasyon pazarının dünya geneline açılması amaçlanarak; pazarın hızı, kapsamı ve yapısının yeniden oluşturulması büyük bir oranda ulusal politika yapıcılara, özel yatırımcı ve operatörlere kalmıştır.

Elektronik ticaret altyapı, pazar yapısı kararlarını potansiyel olarak üç seviyede etkileyebilir:

1) Temel telekomünikasyon transmisyon servisleri

2) Katma değerli servis seçenekleri, özellikle internetin rolü

3) Doğrudan kullanıcı servisleri ve diğer servislere ve toptancılara erişim kapısı bağlamında içerik sahipliği ve kontrol

Pazarın açılması lisanslandırma sözleşme şartları, sorumlulukların tanımlanması, yeni girişler gibi bir çok adımı içermektedir. Bir çok durumda, yeni girişler ve eski engellerin kaldırılmasına yönelik için az bir çaba gerekebilir. Regülasyon kurumlarının ilgilenmekte oldukları elektronik ticaretin gelişimini etkileyen rekabet ve lisanslandırma konuları az üç alanda ele alınabilir.

- Telekomünikasyon transmisyon servisleri, data transmisyon servisleri dahil, temel telekomünikasyon servisleri için veri transmisyonu özellikle rekabete girişe hazırlık için gereklidir ve cüzi şeyler regülasyona yönelik cüzi müdahaleler gerektirir. Temel servisleri rekabete açmak karmaşık olabilir ve pazarı bölümlere ayırmayı ve yeni yatırım fırsatları ve yükümlülüklerini içerebilir.

- İnternet erişimi ve katma değerli servisler bazı ülkelerde uygulamaya konulmasına karşın özel herhangi bir lisanslandırma rejimi içerisinde yer almamasının faydalı olabileceği ifade edilmektedir. Regülasyon kurumları güçlü (baskın) telekom operatörlerinin internete girişinde ve katma değerli telekomünikasyon servisi pazarına girerek rekabetçi olmayan birleşmelere yol açabileceğine dikkat etmelidirler.

- Bilgi ve ağ geçidi (gateway) servisleri benzeri şekilde herhangi bir lisans rejimi gerektirmemektedir ancak yine baskın telekom operatörlerinin bu pazarlara hakim olması halinde bir suistimal olasılığı ortaya çıkabilir. Temel telefon servislerinin etkili regülasyona açılması bu tip ilkel pazar hakimiyetini önleyebilen bir önlemdir.

4.3.1 Telekomünikasyon Transmisyon Servisleri Pazar Yapısı

Telekomünikasyon transmisyon servisleri için pazar yapısı ve elektronik ticaretin tümüyle doğrudan bir ilişkisi yoktur. Prensipte gerekli erişim ve omurga hizmetleri tekel içerisinde rekabetçi ve karışık pazar koşullarında sağlanabilir. Ancak yukarıda da tartışıldığı gibi kısıtlayıcı telefon pazarı

prosedürlerinin temel ve gelişmiş haberleşme servislerini kamu erişimine açması amacına zararı dokunduğu büyük çoğunlukça kabul edilmektedir.

Özellikle internet erişim servislerinin artmasından doğan gelire olan talep ve bant genişliğinin arttırılması ihtiyacı yeni oyuncuların pazarın bu bölümünü özel olarak hedeflemesi fırsatlarını arttırmaktadır. Tekelci bir çevrede tüketiciler ve sağlayıcılar ihtiyaçları olan transmisyon servislerini ulusal operatörden sağlayabilirler ve bu operatör hedeflenen yüksek kaliteli ve elektronik ticaretin uygulamalarının gerektirmekte olduğu teknik olarak gelişmiş kapasiteye sahip hizmetleri sunmak için gerekli hazırlıkları yapmamış olabilir. Tekelciler mali kaynak bulma, ücretlendirme seçenekleri, kalkınma öncelikleri, evrensel hizmeti genel olarak engelleyerek elektronik ticaret için çok yararlı servislerin gelişimini yavaşlatacak olan iç yönetim etkinliği, konularında zorluklarla karşılaşabilirler.

Bu perspektiften, temel ve gelişmiş telekomünikasyon servis pazarına giriş politikaları her ülke için kısa vadeli elektronik ticaret politikaları için kritik bir yere sahiptir. Temel sesli telefon servis pazarına girişin bir süre kısıtlandığı yerlerde bile, bazı özelleşmiş veri transmisyon servislerinde rekabet hükümlerine izin verecek olan seçenekler bulunmaktadır.

Temel telekomünikasyon pazarı serbestleştiğinde internet için verilen lisanslar ve benzer veri hizmetleri piyasaya yeni giren girişimcileri cesaretlendirmiş ve yeni pazar yapısı ile ilgili geniş bir başarı yaratmıştır.

4.3.1.1 Regülasyon Seçenekleri: Şebeke Operatörlerinin Lisanslandırılması

Pazar yapısının değişimini sağlayan temel düzenleyici fonksiyon yeni operatörlerin lisanslandırılmasıdır. Telekomünikasyon pazarının rekabete açılması işlemi ve altyapının geliştirilmesi bazı formal lisanslandırma prosedürleri izlenerek başarılabilir. Pazarın en kısıtlandırılmış olan

bölümlerinde bile başvurunun doldurulmasından biraz daha fazla formalite vardır. Başka yerlerde ise şirketler sunacakları haberleşme servisleri için tarifeler, evrensel hizmet katılımı ve teknik standartlar için katı kurallara maruz kalıyor olabilirler.

Regülasyon kurumları veri aktarımı (transmisyonu) ve temel erişim servisleri için, operatörler üzerindeki spesifik yükümlülükler ve kısıtlamalar sonucu bekledikleri faydalarla, bu kontrollerden doğacak olan maliyet ve riskleri iyi dengelemelidirler. Prensip olarak oyuncuların stratejileri ve girişimlerinden çok regülasyon kurumunun hedeflerinden oluşan bir pazar yapısı kurmak gerçek dünya ve kullanıcıların değişen ihtiyaçlarını yanlış bir şekilde birbirine bağlamak olur. Lisanslandırma fonksiyonu kısıtlandırılmış pazarlardan serbest pazara geçişte özellikle yeni servislerin planlamasını yavaşlatacak olan ihtilafları önlemede önemli öncelikler arasında hizmet edebilir.

Lisanslandırma çabaları e-ticaretin pazara girişini veri aktarım servisleri pazarı ya da telekomünikasyon servisleri endüstrisinin kuşatması üzerinde yoğunlaşılarak desteklenebilir

4.3.2. ISP pazarı

İnternet, kamu anahtarlamalı telefon şebekesini özel veri omurga şebekelerine bağlayan katma değerli uygulamaların bir serisi ve elektronik ticaretin yayılmasını sağlayan birincil güç olarak regüle edilmemiş bir çevrede gelişmiştir. Anarşik ve popülist menşeyine rağmen fiili pazar yapısı internete dayalı haberleşmenin bünyesinde olan ikincil erişim, bağlanabilirlik, protokol fonksiyonlarından oluşmuştur.

Bu yapının merkezinde internet servis sağlayıcılar (Internet Service Provider-ISP) en çok tanınan kuruluşlardır. ISP'lerin en temel biçimi ve fonksiyonunun telekomünikasyon operatörü olmamaları olup kendilerine ve müşterilerine doğrudan haberleşme hizmeti sağlamak zorunda değillerdir. ISP'ler bunun yerine elektronik bilginin geri getirilmesi, yedeklenmesi, çevrilmesi ve

gönderilmesi için bilgisayar işlem ve yedekleme hizmetleri –routerlar ve sunucular- sağlarlar. ISP'ler ve son kullanıcılar arasında ve ISP'ler ve internet omurga yönlendiricileri (router) arasındaki bağlantılar genellikle ayrı telekomünikasyon şebeke operatörleri arasında (ayrı ancak bağlı bölümler, Telefon şebekesi ISP'lerinde) olup sözkonusu bağlantılar diğer veri ses servislerindeki internet haberleşmesinde kullanılmayan bağlantılardan farklıdırlar. Bu bağlamda ISP'ler veri işleme ya da kamu şebeke telekomünikasyonuna bağlantı hizmeti konularında diğer diğer katma değerli servislere benzerdirler.

Bu açık farklara rağmen çoğu hükümetler ve regülasyon kurumları ISP'leri ve diğer katma değerli servis sağlayıcıları telekomünikasyon şirketleri olarak bazı lisanslandırma ve regülasyona tabi kılmışlardır. Uç bir örnek olarak ulusal tekelci telefon servis operatörünün ülkedeki tek servis operatörü olarak lisanslandırılması nadir olarak görülmektedir. Daha açık bir örnek olarak regülasyon kurumlarının çoklu ISP lisansları verdiği telefon operatörlerini de içeren ancak bu firmalar için numaraları ile ilgili kısıtlamalar getiren, işletim standartları, ve hükümleri, ücretlendirme ve lisanslandırma gerektiren uygulamaları yürürlüğe koymaktadırlar. Bugüne kadar ülkelerin çok az bir bölümü internetin doğmasını sağlayacak bir model izlemişlerdir.

ISP'lerin sağladığı içerik ve müşterinin korunmasına yönelik politik amaçlar belli seviyedeki regülasyonu haklı kılmaktadır. ISP'lerin pazara girişi ve çalışmaları ile ilgili konulan kısıtlamaların yavaş geliştiği görülmekle beraber, kısıtlanmamış girişlerde ise yüksek ücretler ve internet erişim servislerinde yeniliğin yeterince yapılmadığı görülmektedir. Elbetteki tekel pazar yapısı altındaki telefon servisleri içinde aynı etkiler umulmaktadır. Buradaki fark ISP pazarının rekabetçi, bağımsız bir endüstride başlamış olması ve bağımsız endüstrinin kolaylıkla katılınabilen, rekabetçi, talebin olduğu ve gerekli altyapının sağlandığı durumlarda ISP'lerin internet servisini evrensel servis kapsamında çapraz sübvansiyon olmaksızın sağlayabilecektir. Diğer bir

değişle telekomünikasyon şebeke yapısı kısıtlamalarının temelini oluşturabilecek doğal tekel tartışmaları bile yoktur.

Yukarıda tartışıldığı gibi ISP'lere yerel seviyede başarılı olabilecek işletmeler gözüyle bakılmaktadır. Gerçekte teknik ve müşteri desteğinin birleşmesi ve toptancılara e-ticarete başlangıç için yapılan yerel pazarlama yardımı özel avantajlar sağlayabilecektir. Büyük ulusal operatörler yerel şirketlerle anlaşma yapmadıkları takdirde bu tip topluluk temelli desteği etkin olarak vermeyebilirler. Bu ise bağımsız ya da ulusal ISP'ler için bir pazar olduğunu söylemek olmayıp ISP pazarında kısıtlamalar olmadığında değişik seviyelerde farklı oyuncular olabileceğini göstermektedir.

Özel şirketlerin telefon operatöründen bu servisleri sağladığı yerlerde zorunlu operatörün pazarda aktif bir ISP olmasına izin verilmesi sorgulanması gereken sorular arasındadır. Çok zarar verici olan rekabete aykırı durumlar şu tip koşullarda oluşabilir: tekel durumundaki şebeke sağlayıcısı kendi telekomünikasyon transmisyonunu ve internet servis erişimini tek bir paket halinde toplayarak telefon şirketinin maliyetlerini kolaylıkla arttırabilecek olan transmisyon servislerinin masraflarını ISP'lerden karşılayabilir. Bu tip riskleri en aza indirmek için mali ayırım ve toptan erişim ücretlendirmesi yolllarıyla gerçekleştirilecek olan sıkı bir denetim gerekmektedir. Yeni ve tecrübesiz regülasyon kurumları için bu olay oldukça zorlu bir durumdur.

4.3.2.1 Regülasyon seçenekleri: İnternet Servis Sağlayıcıların Lisanslandırılması

ISP Pazar bölümleri için üç farklı lisanslandırma seçeneği vardır. Bunlar:

1. Yalnızca zorunlu operatöre internet hizmeti sağlama hakkını vermek. Tartışılmış olan sonuçlara göre bu yaklaşım internet servislerinin gelişmesinde en dezavantajlı olanıdır.

2. Zorunlu işletmeciye ve bağımsız ISP'lere internet hizmeti sağlama hakkını vermek. Bu ise zorunlu operatör tarafından toptan erişim ücretlendirilmesinin denetlenmesini ve bireysel internet servislerinin rekabetçi olmayan çapraz sübvansiyondan korunmasını gerektirir. Diğer bir seçenek ise telekom internet servislerinin diğer ISP'lere uygulanmakta olan ücret ve hükümlerin uygulandığı ayrı bir yan kuruluş tarafından sağlanmasıdır.

3. Sadece bağımsız ISP'lere internet hizmeti sağlama hakkını vermek. Bu bağlamda "bağımsızlık" tümüyle tek-başına olan ISP'ler olarak tanımlanabilir ya da zorunlu işlemeciyle bağlantısı bulunmayan ve GSM şirketleri ve diğer kuruluşlar ISPler olarak tanımlanabilir.

Bağımsız ISP'lerle ilgili seçeneklerle bağlantılı olarak regülasyon kurumları şu iki yaklaşımdan birini uygulayabilirler: ISP'lere resmi lisanslandırma zorunlu kılınır ya da piyasaya serbest girişe izin verilir ve pazarın içinde tüm yönleriyle yer alınmasına engel olunur. Telekomünikasyon regülasyon kurumları lisans vermeyi genellikle her türlü telekomünikasyon uygulaması için fiili olarak bir görev olarak algılamaktadır. Böylelikle ISP'ler çoğu ülkede pazar tamamıyla serbest olsa bile lisans alma zorunluluğunda kalmışlardır. Ancak, regülasyon kurumları bu tip zorunlulukları öncelikle lisanslandırma politikasının hangi kamu politikasına hizmet edeceğini ve gerçek anlamda katı kurallarla kısıtlanmamış ISP rekabetini tehlikeye sokabilecek servisin genişlemesi, yenilikçiliği ve etkinliğinin tartılması hususları ile ilgili konuları tekrar gözden geçirme eğilimindedirler.

4.3.3 Bilgi ve Ağ Geçidi (gateway) Servisleri

Elektronik ticaret endüstrisine pazarın katılımının üçüncü seviyesi başlangıç regülasyonu olarak adlandırılan mülkiyet ve çevrimiçi içeriğe yönelik servislerin kontrolü, ticari ve karşılığında yanıt gerektiren "ağ geçidi" servislerinin kontrolü gibi şartlara maruz kalır. İçerik servisleri genel anlamda temel telekomünikasyon şebekeleri üzerinden sağlanan aboneliğe bağlı metin, grafik, ses ve görüntü özellikleri içeren bilgi ve eğlence servisleri

anlamına gelmektedir. Bu servislerin çoğu doğrudan internet üzerinden çeşitli erişim ve ödeme düzenlemeleriyle sunulmaktadır.

Ticari "ağ geçidi" servisleri ayrıca içerikle ilgilidir ancak birincil olarak çevrimiçi işlemlere odaklanmıştır ve bilgi erişimine mani olmaktadır. Bu servislerin çoğunluğu web tabanlıdır ve çevrimiçi üreticileri ve servisleri katalog, reklam, ve gelişmiş yazılım özellikleri yoluyla birbirine bağlayan merkezi bir web sayfasından oluşur. "Ağ geçidi" sağlayıcısı diğer üreticilerle ortaklıklar yoluyla reklam, kataloglar, müşterilere önerilen aboneliklerle gelirler elde edilebilir. Bu ağgeçitleri üreticiler ve çevrimiçi servisler arasındaki işlemleri bir ücret karşılığında gerçekleştirerek bir finans kaynağı olabilirler. Bu tip aktivitelerin her zaman kazançlı olabilmesi için çeşitli modeller bulunmaktadır.

Telekom operatörlerinin elektronik ticaret gibi uygulamalara doğrudan katılmaması için gerçek bir seçenek yoktur. Ancak, regülasyon kurumları telekomünikasyon servislerinin pazar yapısının regülasyonunda telekomünikasyon operatörlerinin katılabilecekleri çevrimiçi işler ile ilgili bazı kısıtlamalarda bulunabilirler. Bu konudaki endişeler baskın olan telefon operatörlerinin temel telekomünikasyon şebekeleri üzerinden elektronik ticaret düzenlemelerinin altını çizen uygulamalarındaki kontrol darboğazından kaynaklanmaktadır. Bu telekom şirketleri aynı zamanda kendi şebekeleri üzerinden parakende iş servisleri sağladığı durumlarda kendi şebekelerinin kontrolünü suistimal ederek pazarın diğer oyuncularına ve müşterilere zarar vermeye başladıklarında riskler başlamaktadır.

Ancak bu risk ISP servislerindeki problemle kıyaslandığında o derece önemli değildir. İnternete dayalı ticari ve bilgi servislerinin genişliği ve çeşitliliği o kadar güçlü görünmektedir ki tekel durumundaki büyük ve saldırgan bir telekomünikasyon şirketi bile rekabeti kolayca azaltamaz. Elektronik ticaretin telekomünikasyon bileşeni ve erişim servislerinin için ücret ayrımı yaratan

(örneğin telekomla ilgili perakende uygulamaların bir fayda sağlayacak şekilde hedeflenmesi) perakende bileşeni arasında bir uzaklık vardır.

Açık bir farklılığı bulunan bir alan istisnasız mali servislerdir. Telekomünikasyon ve mali servis uygulamalarının entegrasyonunun her çeşit suistimal ve elektronik ticaret yoluyla pazarın genişlemesi ve çeşitlendirilmesi amacının tersine gereğinden fazla birleşmenin kontrolü ile ilgili bazı tereddütler vardır. Bir ülkedeki ulusal bankalar, kredi ajansları, komisyoncu firmalar, ve benzerleri telekomünikasyon operatörlerinin lisanslarını kontrol etmenin yollarını arıyorlarsa bu dikkatle gözden geçirilmesi gereken bir teklif olacaktır.

Elektronik ticaret ürünleri ve servis sağlayıcıları için telefon şirketlerinin ikincil ücretlendirici kuruluşlar olarak hizmet vermesi ek bir endişe doğurmaktadır. Telefon şirketi kendi ücretlendirmesi ve ödeme yapılmaması durumda telefon servisini engelleme gözdağı ile tahsilat çabalarını destekleyebileceği özel bir duruma sahiptir. Bilgi çağında bu tip bir gözdağı ölçülen en etkili bir tahsilat mekanizmasıdır. Ancak telefon aboneleri kendilerini hileli faturaları ödemeye mecbur edilmiş hissediyor ve telefon servislerini kaybedebilecekleri korkusuyla da bu düşüncelerini ifade etmekten çekiniyorlarsa bu durum tüketici haklarının suistimali riskini de yaratır. Regülasyon kurumları kendi telefon faturalarının çeşitli tümleşik yönleriyle ilgili müşterilerin ihtilafını bağlantı sağlamama tehdidi olmaksızın çözmeyi kabul edebilirler. Ancak bu haklar bu politikaların etkin olması için net olarak açıklanmalı ve kolayca ikna edici olmalıdır.

Gelişmekte olan ülkelerde rekabet dışı pazar faaliyetleri internet ve elektronik ticaret servislerinin pazara girişinde ve telekomünikasyon pazarının yeniden yapılandırılması esnasında bazı büyük riskler getirebilir. Eğer genel objektif her sektördeki geniş iş imkanlarını görmek ise her ikisini en azından bir geçiş periyodu süresince her sektördeki pazar güçleri birbirini tesis edene kadar ayırmak akıllıca olacaktır.

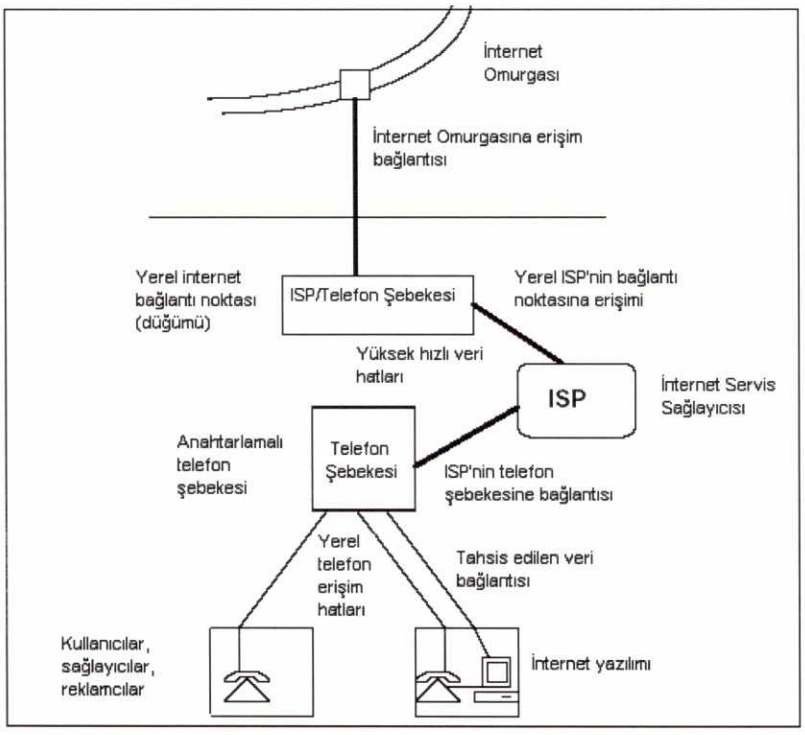
4.4 Ekonomik ve Ücretlendirici Regülasyon

Telekomünikasyon regülasyon kurumları pazarı geliştirirken ve değiştirirken rekabetçi güçlerin etkin olmaması durumunda ekonomik ve ücretlendirici regülasyonun etkileri hatırda tutulmalıdır. Tarife regülasyonu servislerin ücretlendirmesinde maliyete dayalı, pazar yönelimli ve minimum çapraz sübvansiyonlu olmalıdır. Bu özellikle rekabetçi çevrede beliren arabağlantı ücretlendirilmesinde uygulanır. Elektronik ticaret bağlamında, internet ve veri servislerinin gelişimi telekomünikasyon erişimi ve arabağlantı servisleri için etkili ücretlendirmeye güçlüce bağlıdır.

Telekomünikasyon servisleri için son kullanıcılar ya da çeşitli servis sağlayıcıları arasındaki arabağlantı ya da işlemler gibi elektronik ticareti mümkün kılan ilişkilerin çeşitli unsurlarını içeren, mali şartları ve tahsil edilen ücretleri ilgilendiren politik konular elektronik ticaretin özel içeriği bağlamının dışında kalmaktadır. Ancak elektronik ticaretin ulusal ve uluslararası kalkınmada ortaya çıkmış olan önemli rolü düşünüldüğünde bu konuların bir çoğu yeni boyutlar kazanmaktadır.

Telekomünikasyon pazarının daha da serbestleştiği bir ortamda daha çok zorunlu işletmecilerin hakim olduğu pazarın gelişiminin dürüst ve hakça olmasını sağlamak için tarifelerin düzenlenmesi ve arabağlantı kamu sektörünün en temel sorumlulukları arasında sayılabilir. Tetkik etmiş olduğumuz diğer konularla birlikte bu sorumluluk elektronik ticaretin yaygınlaştırılmasını sağlama ve bu servislerden sağlanacak faydaları elde etme seçenekleri arasında en önemlileri arasında yer almaktadır.

Şekil 4.1 diğerlerine oranla farklı ücretlendirilebilecek kuruluşların uçtan uca bağlanabilirliği ile ilgili değişik unsurları göstermektedir. Bu arabağlantı noktaları farklı rekabetçi güçlerin en duyarlı ve pazar gelişmelerini en son ve en fazla etkileyen bağ noktalarıdır.



Kaynak: ITU [62]

Şekil 4.1 İnternet Hizmeti Pazar yapısı

1. İnternet Omurga Arabağlantısı (İnternet omurga operatörüne internet düğüm noktası (node) operatörü tarafından ödenir.)
2. İnternet Omurga erişim bağlantısı (İnternet düğüm noktası operatörü tarafından şebeke operatörüne ödenir.)
3. Yerel İnternet düğüm noktası arabağlantısı (İnternet servis sağlayıcıları tarafından İnternet bağlantı noktası operatörüne ödenir.
4. ISP ve yerel internet düğümü arasındaki bağlantı (ISP tarafından yerel internet bağlantısına ödenir yada kendisi tarafından sağlanır.)
5. Yerel ISP arabağlantı servisleri (Son kullanıcı tarafından ISP'ye ödenir.)
6. ISP ve telefon şebekesi arasındaki erşim bağlantısı (ISP tarafından telefon şebekesi operatörüne ödenir.)
7. Son kullanıcının ISP bağlantısı için telefon şebekesine erişimi ve kullanımı (Son kullanıcı tarafından telefon şebeke operatörüne ödenir.)

8. Son kullanıcı internet yazılımı (ISP'ye ödenir ya da kendileri tarafından sağlanır.)

Bir bilgisayarı diğerine bağlayan sürekli internet şebekesinde bu işlem noktalarından bazıları telekomünikasyon regülasyon kurumlarının görev sahasına girmektedir. Bu bağlantılar yüksek kapasiteden uluslararası veri servislerini internet omurgasına bağlayan (No:2), bazı ülkelerdeki benzer devrelerle (No:4) ulusal omurgaya bağlatı sağlayan, daha düşük kapasitedeki (örn. 2Mbit/s) ISP ve yerel telefon anahtarları arasındaki bağlantılar (No:6), kamu anahtarlamalı şebekeleri üzerinden son kullanıcılar ve ISP'ler arasındaki anahtarlamalı erişime (No:7) uzanan hızlara ulaştıran bağlantılara değin uzanmakta olup temel telefon servisleriyle aynı tarifedeki şekilde ücretlendirilmektedirler.

Sonuç olarak, ISP servislerinin regüle edilmiş telekomünikasyon servisleri tarafından sağlanması durumunda 5 numarada verilen temel bağlantı servisleri de hakça rekabet gözetilerek regüle edilebilir. Kalan işlemler sunucu ve yönlendiricilerin (router) operatöre doğrudan bağlantılı olduğu ya da dolaylı olarak yazılım satıcılarının internet üzerinden kendi kaydetme ve gönderme hizmetleri tarafından sağlanan kapasite ve uygulama başvurusu ödemeleriyle ilgilidir.

Ücretlendirici regülasyonda uygulanacak olan en temel prensip haberleşme servislerinin maliyet temelli olmasıdır. Oldukça basit olarak ücretler hem müşteriler hem de operatörler için kaynakların etkin şekilde kullanılacak olan maliyetleri yansıtmaktadır. Yine burada regülatörün hangi ihtiyaçları gerçekleştirmede doğrudan yer alacağını pazarın ne kadar rekabetçi olacağı belirler.

Bu servisler, ISP'ler ve PSTN ve ISP'ler ve internet omurgası arasındaki çeşitli veri ağı bağlantıları yönünden regülatörün ücretlendirme konusundaki görüşünü ortaya çıkaran rekabetçi bir temelde sağlanabilir. Geniş olarak

halihazırda rekabet tecrübesi olmayan veri hizmetleri pazarı maliyet tabanlı ücretlendirme regülasyonu yoluyla yürümeye odaklanmalıdır. Daha geniş olarak bu veri servisleri pazar rekabetine fazla alışık olmasa da bu konudaki regülasyon maliyet tabanlı ücretlendirmeye dayalı olmalıdır. Bu tip bir ücretlendirmenin faydaları ISP'ler kendi bağlantı ücretlerini kendi abonelerine yansıttığından dolayı son kullanıcının internet erişim servislere ödemekte olduğu ücretlerde doğrudan belirmelidir.

Çoğu ülkede yüksek hızlı veri servisi ücretleri temel telefon servisleri için kaynak olarak kullanılan çapraz sübvansiyona göre oldukça yüksek olarak belirlenmektedir. Ancak haberleşmesinin değişen yüzü elektronik ticaret ve ilgili amaçları için veri bu ücretlerin temel telefon servisi kullanıcı masrafları üzerinde daha doğrudan bir etkisi olmasını sağlamaktadır. Yani veri servisi ücretlerini diğer endüstrilerin toptan üretim masrafları için bir girdi olarak almaktadır. Böylelikle, en azından ISP'lere sağlanan maliyete dayalı veri servisi ücretlerinin makul seviyede sağlanması elektronik ticaretin gelişmesini destekleyen politikalar kapsamı içerisinde yer alır.

Telefon şirketlerinin aynı zamanda ISP servis sağlayıcısı olması durumunda şeffaflık, bu erişim bağlantılarında maliyete dayalı ücretlendirme özellikle çok önemlidir. Daha önceden bahsedildiği gibi telekomünikasyon şirketleri ikili bir rol oynadıkları zaman, kendi servislerinde eşdeğer iç bağlantılarından doğan ek masraflarını rakiplerine sağlayacakları devreleri aşırı fiyatlandıracak projelerle karşılamak yoluyla kendi rakipleri üzerinde adil olmayan ücretlendirme avantajına sahip olabilirler. Veri servislerinin maliyetlerinin uygun bir şekilde belirlenmesi küçük bir iş olmamakla birlikte tümleşik telefon ve ISP servislerinin operasyonel ve ücretlendirici yapısı içerisindeki maliyetleri ayırmak daha bir zordur. Veri servisleri ve ISP servisleri için en etkili çözüm rekabetçi bir pazardır.

4.4.1 Son Kullanıcı Yerel Telefon Hizmeti Ücretlendirmesi

Gerçekçi olarak, çoğu ülkede temel anahtarlamalı telefon erişim servisi şebekesi beklenen gelecek için zorunlu sağlayıcıların hakimiyetinde kalmaktadır. Bu durum temel erişim servislerinde kolaylıkla giderilemeyen fiyat bozulmalarına yol açmaktadır. Bu sebepten dolayı internet kullanımı ve temel yerel telefon servisi ücretlendirmesi önemli bir ihtilaflı konudur. Çoğu ülkede –çok gelişmiş ve telekomünikasyon sektörünün serbestleşmiş olduğu ülkelerde bile- çapraz sübvansiyonların takdimi şiddetlice tartışmalı bir konu olsa da temel servis ücretleri maliyetin altında kalmaktadır. Eğer bu maliyetin altı ücretlerin bir amacı varsa bu, temel telefon servislerinin müşteri grupları arasındaki eşit ücretlendirmenin yanında ödenebilirliğini korumaktır. Bu politikanın geleneksel çevreye yararlarını hesaba katmaksızın yerel şebekenin dial-up (çevirmeli) internet erişiminde kullanımının gelişmesi temel telefon servislerinin maliyetlerini ve ücretlendirmesini değiştirmektedir.

Yerel telefon operatörlerinin çoğu çevirmeli internet bağlantısının kullanımının yüksek olduğu alanlarda trafik talebi modelinin varolan telefon şebeke mimarisiyle uyuşmadığı temel kaygısını gündeme getirmektedirler. Özellikle yerel telefon aramalarında kalış süreleri 3-5 dakika arasında değişirken internet erişimindeki kalış zamanı 30 dakikayı geçmektedir. İnternet kullanımı arttıkça yerel şebekenin taşıma kapasitesinde (hem anahtarlama hem de gönderme hizmetlerinde) aşırı yük oluşacaktır. Bu durum kapasitenin artırılmasına yönelik beklenilmeyen masrafları doğurmaktadır. Ekstra yatırımlar temel yerel servisler için maliyet tarifelerinin altında özellikle dakika ücretlerinin kullanıldığı pazarlarının aksine sabit fiyatlı yerel arama ücretlerinin uygulandığı pazarlarda dengelenemeyecektir.

İnternet kullanımı, temel telekomünikasyon servisleri için ayrıca geleneksel "ödenebilirlik" ve çapraz sübvansiyon politikası görüşlerinin tekrar gözden geçirilmesini zorunlu kılar. Gelişmiş ve gelişmekte olan ülkelerde kişisel bilgisayarlar sayısı ve çevrimiçi internet servislerine abonelik yüksek seviyeli

gelir gruplarına doğru yönelmektedir. Eğer internet kullanıcıları sadece sesi kullanan kullanıcılarla aynı ücreti ödeyerek yerel şebekede uygunsuz bir oranda yüksek kapasiteden istifade ediyorlarsa bu çapraz sübvansiyonun artan miktarının yüksek gelir seviyesindeki telefon müşterilerine akışını destekleyebilir.

Bu endişelerle ilgili olarak regülasyona yönelik bazı yanıtlar bulunmaktadır. Örneğin Amerika'da telefon şirketlerine sunulmuş olan bir yaklaşım, internet kullanımından doğan ekstra maliyetlerin getirdiği sorumlulukları internet servis sağlayıcılarına yüklemek olmuştur. Bu tartışma yerel şebeke maliyetlerinin desteklenmesini sağlayacak olan çapraz sübvansiyon gelirlerini bir kaynak olarak sunan diğer telefon servislerinin dışında olarak ISP servislerini uzun erişimli özel şebekelere eşdeğer görmektedir. Bu seçenek kendi servislerinin ürettiği gelen çevirmeli bağlantı kullanımı miktarı oranında ISP'ler üzerinde bir bağlantı ücretini teklif etmektedir.

Bu teklif maliyete dayalı ücretlendirme formunun bir çeşidi olsa da ISP servis pazarının ve ilgili çevrim içi kullanım ve işlemlerinin etkinliğini azaltmak gibi bazı dezavantajlar taşımaktadır.

Öncelikle, kullanıcılardan gelen trafiği belirleyen bir ücretlendirme kategorisi içermekte ve bununla ilgili bir uygulama uzun mesafeli servislerde operatörler, hücresel mobil ve çağrı sistemlerinde kullanılmaktadır. Böyle bir uygulamayı gerçekte şebeke servisleri sağlamayan ve yerel standart veri servisi abonelerinden ayırdedilemeyen ISP'lere uyarlamak için ek ölçüm ekipmanları ve yönlendirme ve ücretlendirme veri tabanları ISP fonksiyonlarıyla doğrudan ilgisi olmayan ek masraflar gerekmektedir. Böylelikle verimsizlikler diğer çözümsüzlüklerin bir çözümü olarak sunulmuş olmaktadır. Bu problem çoğunlukla kullanım süresine göre ücretlendirme yapmayarak erişim ücretleri dolayısıyla doğan ekstra maliyetler için kendi ücretlendirme sistemlerini değiştirmekte bir sebep bulan ISP'ler ve müşterilerinin ilişkilerine kadar uzanabilir.

Öte yandan, amaç bu sebeplendirmeyle uyuşacak olursa bu yalnızca son kullanıcıların ISP'lere bağlantı sürelerine göre ücretlendirilmeleriyle mümkün olabilir. Ancak yine kullanım ücretlendirmesi eğer uygulama değilse bu yine şebekeye ek maliyetler getirecektir. Ayrıca, uç ve uç dışı kullanım arasındaki ek maliyetler arasında büyük farlar vardır ve kullanım ücreti yalnızca internet kullanımıyla değişen bu uç periyotları arasında uyarlanırsa etkinlik kazancı daha da azalmış olacaktır.

Sonuçta, kullanım tabanlı ücretlendirmeyi spesifik internet kullanımıyla eşleştirmeye çalışmak elektronik ticaretin ilk adımda desteklenmesinin arkasındaki ana ekonomik varsayım anahtarıdır. Kullanım tabanlı ücretlendirme, elektronik ticaretin şebeke genişlemesi hedeflerini kabul ederken, sınırlı kullanımı ve artan şebeke maliyetlerini azaltmayı hedeflemektedir.

İnternet kullanımı üzerindeki sübvansiyon etkilerini daha iyi maliyet temeline dayalı cevap, yeni verimsizlikler yaratmadan sübvansiyonların kendisini mümkün olduğu kadar azaltmak olacaktır. Bu temel servis tarifelerinin ivedilikle tümüyle yeniden dengelenmesi gerektirmeyebilir. Minimum seviyede bu arta kalan sübvansiyonların daha çok uzatılmaması gerektiğini ima etmektedir.

Örneğin, bir çok ülkede çoğu işkolundaki ve konutlardaki sabit telefon kullanıcıları tümüyle gelişmiş şebekelerde internete erişim amacına yönelik ayrı erişim hatları kurmaktadırlar. Bu erişim servislerine uygulanan abonelik tarifeleri sıklıkla aynı yerdeki ilk taşıyıcı hatlara benzerdir. Eğer tek hat kullanıcılarının temel erişim ücretleri maliyetin altında belirlenecek olursa hangi sebeple olursa olsun, aynı yere ikincil bir erişim hattının hangi nedenle sübvanse edilmesi gerektiğini açıklayamayacaktır. İkinci bir erişim hattının ağın ve bu hatların ortalama kullanımının getirdiği ek maliyetlere eşit olarak belirlenmesi ek bir ölçüm, ücretlendirme ve fiyat bozulması olmaksızın gelir gelişimi ile birlikte kullanımında gelişmesini sağlar.

Elektronik ticaret talepleri çerçevesinde değişen şebeke masraflarıyla bağlantılı olarak daha başka ücretlendirme seçenekleri de bulunabilir. Regülasyon kurumlarının amaçları uygulama esnasında yeni maliyetler çıkarmaktan kaçınarak telekomünikasyon endüstrisindeki etkinliğin maliyete yakın ücretlerle sağlanarak arttırma yollarını araştırmak olmalıdır.

BEŞİNCİ BÖLÜM

5. TELEKOMÜNİKASYON KURUMU'NUN ELEKTRONİK TİCARET İLE İLGİLİ UYGULAYACAĞI POLİTİKA MODELİ

Telekomünikasyon düzenlemeleri, gelişmekte olan dünyada elektronik ticaret fırsatlarının açılımının sağlanmasında büyük öneme haiz olup telekomünikasyon politikasının gelişimi, elektronik ticaretin gelişimini birinci derecede etkilemektedir.

Geçen on yıl içerisinde dünya genelinde telekomünikasyon sektöründe tekellerin kaldırılması, küresel rekabetin başlatılması görevinin sorumluluğu telekomünikasyon regülasyon kurumlarına verilmiştir.

Kurumumuz elektronik ticaret ile ilgili uygulayacağı politika modelini belirlerken ilk olarak elektronik ticaretin gelişimini doğrudan ilgilendiren ve aşağıda yer alan dört önemli telekomünikasyon regülasyon alanı ile ilgili, tezin VI. bölümünde detaylıca değinilmiş olan tavsiyeleri gözönünde bulundurmalıdır.

Sözkonusu temel telekomünikasyon regülasyon konuları ve uygulanması gereken politikaların çok kısa bir özeti aşağıda yer almaktadır.

- Altyapı: Regülasyon kurumlarının şebeke altyapısına erişim ile ilgili rolü hem doğrudan hem de dolaylıdır. Uzun vadede telekomünikasyon endüstrisi için uygun teşvikler ve yaptırımlar yoluyla yeni, potansiyel operatörlerin katılımına imkan sağlayan tüketici yönelimli erişim teknolojilerinin temin edilmesi için gerekli önlemler alınmalıdır. Kurum telekomünikasyon pazarının

geniş politikaları kapsamında zorunlu işletmeciye uygulanacak pazar yönelimli teşvikleri ve yatırımları arttırıcı seçenekleri gözden geçirmelidir.

- Evrensel hizmet: Evrensel hizmet politikası geniş pazar liberalizasyon insiyatifleriyle daha uygun ve tamamlayıcı olmalı, çapraz sübvansiyon ile pazar gelişmelerini desteklemek için iç ücretlerin ve kaynakların bozulmasından çok bir fon sağlama mekanizması hedeflenmelidir.

- Pazar yapısı, rekabet, lisanslandırma: Telekomünikasyon transmisyon servisleri için pazar yapısı ve elektronik ticaretin tümüyle doğrudan bir ilişkisi yoktur. Prensipte gerekli erişim ve omurga hizmetleri tekel içerisinde rekabetçi pazar koşullarında sağlanabilir. Pazar yapısının değişimini sağlayan temel düzenleyici fonksiyon yeni operatörlerin lisanslandırılmasıdır. Kısıtlandırılmış pazarlardan serbest pazara geçişte lisanslandırma fonksiyonu özellikle yeni servislerin planlamasını yavaşlatacak olan ihtilafları önlemede önemli öncelikler arasında hizmet edebilir.

- Ekonomik ve ücretlendirici regülasyon; Kurum pazarı geliştirirken ve değiştirirken rekabetçi güçlerin etkin olmaması durumunda ekonomik ve ücretlendirici regülasyonun etkilerini hatırda tutmalıdır. Tarife regülasyonu servislerin ücretlendirmesinde masrafa dayalı, pazar yönelimli ve minimum çapraz sübvansiyonlu olmalıdır.

Kurumun ele alacağı ikinci önemli husus ise elektronik yaşamın gelişebilmesinin ve tarafların birbirlerini sorunsuzca tanıyabilmelerinin en önemli şartı olan elektronik ortama ve açık ağ sistemine güvenin sağlanması olmalıdır.

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 "Elektronik İmza Yasası" olduğu söylenebilir.

Bilindiği üzere Adalet Bakanlığı tarafından hazırlanan ve Meclis'e sevkedilen Kanun Tasarısında sorumlu kurum olarak Kurumumuz tanımlanmıştır. Bu bağlamda Kurumumuzun elektronik imza ile ilgili yönetmelikleri bir yıl içerisinde çıkarması gerekmektedir.

Tezin bu bölümünde Kurumumuz için bir model oluşturması için elektronik imza konusunda lider durumunda olan ve kök sertifika hizmet sağlayıcısı olarak faaliyet gösteren Almanya, Avusturya, Finlandiya ve Danimarka telekomünikasyon regülasyon kurumlarının uyguladıkları modeller, yönetmelikleri ve sorumlulukları incelenmiş ve Kurumumuz koordinatörlüğünde yürütülecek olan yönetmelik çalışmalarına model olması açısından iki yönetmelik taslağı hazırlanmıştır. Ayrıca farklı bir örnek olması açısından İngiltere Ticaret ve Endüstri Bakanlığı (Department of Trade and Industry-(DTI) Modeli de incelenmiştir.

5.1 I. Model: Almanya Telekomünikasyon ve Posta Regülasyon Kurumu Modeli (Regulatory Authority for Telecommunications and Posts-RegTp)

Almanya'nın Telekomünikasyon Düzenleyici Kurumu Reg Tp elektronik imza konusundaki çalışmalarını 1997 yılından bu yana sürdürmektedir. Almanya'nın ilk sayısal imza kanunu 22 Temmuz 1997 yılında yönetmeliği ise 22 Ekim 1997 yılında yayınlamıştır. İkinci sayısal imza kanunu ise 22 Mayıs 2001'de sözkonusu kanunun yönetmeliği ise 22 Kasım 2001 tarihinde yayınlanmıştır. Son çıkan yönetmeliğin çevirisi Kurumumuz koordinasyonunda sürdürülecek olan yönetmelik çalışmalarına model olması açısından Ek-1'de sunulmuştur [98]

Sözkonusu yönetmelik oldukça kapsamlı bir yönetmelik olup başlıca aşağıdaki konuları kapsamaktadır:

Kısım 1 Form, içerik ve bildirimin değişimi
Kısım 2 Güvenlik kapsamının içeriği

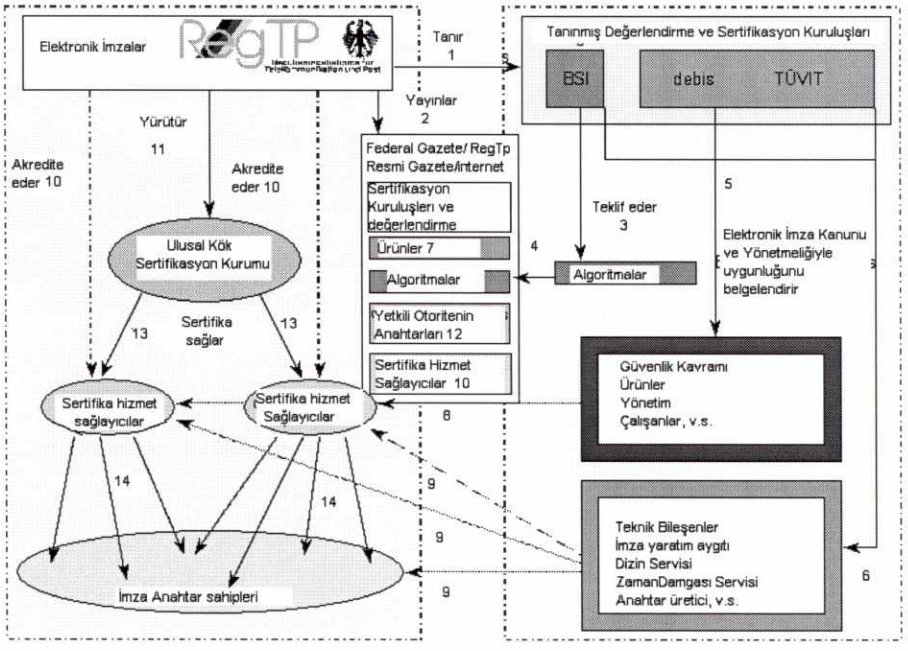
Kısım 3 Kanıtın niteliği ve kimlik doğrulaması
Kısım 4 Sertifika kayıtlarının korunması
Kısım 5 Sertifika hizmet sağlayıcıları tarafından alınacak olan özel güvenlik önlemleri
Kısım 6 Bilgi hükümleri
Kısım 7 Nitelikli sertifikaların iptali
Kısım 8 Dokümantasyonun kapsamı
Kısım 9 Mali hükümlerle ilgili detaylar
Kısım 10 İşlemlerin durdurulması
Kısım 11 İhtiyari akreditasyon
Kısım 12 Harçların toplanma şartı
Kısım 13 Katkıların toplanma şartı
Kısım 14 Nitelikli sertifikaların içeriği ve geçerlilik periyotları
Kısım 15 Nitelikli elektronik imza ürünleriyle ilgili ihtiyaçlar
Kısım 16 Sertifikasyon Kurumlarının tanınması ve işlemlerin değerlendirilmesi ile ilgili prosedürler
Kısım 17 Uzun süreli veri güvenliği için yöntemler ve periyotlar
Kısım 18 Yabancı elektronik imza ve ürünlerinin eşdeğer güvenliğinin belirlenmesi prosedürü
Kısım 19 Yürürlüğe giriş/sona erme

Ek-1 (11(3) ve 15(5) Bölümlerine Ek)
Nitelikli elektronik imza ürünlerinin değerlendirilmesi ile ilgili hükümler
Ek-2 (12. Bölüme Ek)
Harçlar

Reg Tp seçilen diğer ülke örneklerindeki gibi Ulusal Kök sertifikasyon kurumunun teknik muamelelerini gerçekleştirmektedir. Reg Tp kendisinin yetkilendirmiş olduğu BSI, Debis ve TÜVİT kuruluşları ile işbirliği içersinde çalışmaktadır.

BSI kuruluşu Reg Tp'nin açık anahtar altyapısı sistemine uygun algoritmaları hazırlayarak teklif etmekte,
Debis kuruluşu ürünler, yönetim ve çalışanlarla ilgili güvenlik kavramının;
TÜVIT kuruluşu ise imza yaratım aygıtı, dizin servisi, zaman damgası servisi anahtar üretici ile ilgili teknik bileşenlerin Elektronik İmza Kanunu ve Yönetmeliğiyle uygunluğunu belgelendirmektedir.

Reg Tp'nin çalışma mekanizması Şekil 5.1'de yer almaktadır.



Kaynak: Reg Tp [46]

Şekil 5.1 Reg Tp'nin çalışma mekanizması

Reg Tp BSI kuruluşunu tanır. BSI Reg Tp'nin tanıdığı uygun algoritmaları teklif eder. Reg Tp ise bu algoritma standartlarını ve hangi kuruluşları tanıdığını resmi gazetede duyurur.

Debis ürünler, yönetim ve çalışanlarla ilgili güvenlik kavramının, TÜVIT kuruluşu ise imza yaratım aygıtı, dizin servisi, zaman damgası servisi anahtar

üretici ile ilgili teknik bileşenlerin elektronik İmza Kanunu ve Yönetmeliğiyle uygunluğunu belgelendirir. Sözkonusu kuruluşların onayladığı belgelendirmelere sahip olan sertifika hizmet sağlayıcılarını Reg Tp kök sertifika hizmet sağlayıcı olarak akredite eder, sözkonusu hizmet sağlayıcılar için kendi gizli anahtarını taşıyan bir sertifika yayınlayarak onları onaylamış olur. Böylelikle sertifika hizmet sağlayıcıların müşterilerine sağlayacağı elektronik sertifikaların üzerinde kendisinin Reg Tp tarafından akredite edildiğine dair bir ibare bulunur ancak tüm bunlar hep elektronik ortamda yürümektedir.

RegTp'nin görevleri aşağıda sıralanmıştır [98]:

5.1.1 Regülasyon Kurumunun Görevleri

Ülkemiz elektronik imza yasasına örnek olması açısından incelendiğinde Alman elektronik imza yasasının düzenleyici kurum Reg Tp'yi en temel olarak aşağıda belirtilen üç hususta yükümlü kıldığı görülmektedir:

5.1.1.1. Sertifika Hizmet Sağlayıcıların Lisanslandırılması

Güvenilirliğin tespit edilmesi için bazı unsurlar değerlendirilmektedir. Bunların içerisinde çalışanların güvenilir olması, teknik bileşenler ve güvenlik kavramı yer almaktadır.

- Çalışanlar: Çalışanlarının uzmanlığının ve güvenilirliğinin en üst seviyede sağlanması. Başvuru sahibi sertifika hizmet sağlayıcısının yasal temsilcilerinin güvenilir olduğuna emin olunması,

- Teknik Bileşenler: Teknik bileşenlerin halihazırdaki teknik standartlarla ve sayısal imza yasası ve yönetmeliğindeki regülasyon kurumunun yetkilendirilmesi ile ilgili hükümler konusunda gerekli testlerin yapılması,

- Gizlilik kuramı: Gizlilik gereksinimlerine uyumlu olarak önceden alınan tedbirlere yönelik gizlilik kavramının yürürlüğe konması yetkilendirilmiş bir kuruluş tarafından teyit edilmesi, Reg Tp'nin sorumluluğundadır.

5.1.1.2. İmza Anahtar Sertifikalarının Yayınlanması

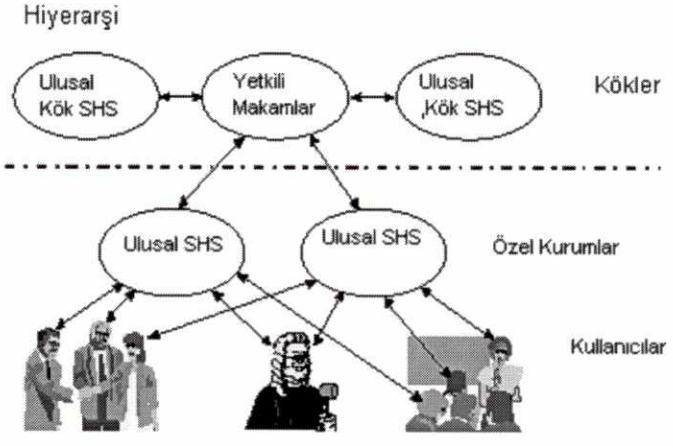
Düzenleyici kurumun Alman elektronik imza yasasında vurgulanan ikinci görevi sertifika hizmet sağlayıcısının imza anahtarlarını sadece anahtar sertifikalarını imzalamada kullanması hususundadır.

Bu ise aşağıdaki hiyerarşiyi doğurur.

1.Yetkili Kuruluş: Sertifika Hizmet sağlayıcısı-kendi açık anahtarının sertifikasını yayınlar:kök sertifika

2.Yetkili Kuruluş ayrıca sertifika hizmet sağlayıcılarının açık anahtar sertifikalarını yayınlar; sertifika hizmet sağlayıcılarının sertifikaları

3.Sertifika Hizmet Sağlayıcısı, kendi müşterilerinin açık anahtar sertifikalarını yayınlar.



Kaynak: Reg Tp[46]

Şekil 5.2 Kuruluşlar arasındaki Hiyerarşi

Diğer bir sorumluluk ise kullanıcı sertifikalarının sayısal imza yasası ve sayısal imza yönetmeliğinin hükümleriyle uyumluluğun denetlenmesidir.

Ayrıca sayısal İmza yönetmeliğinin 8(2) maddesinde düzenleyici kuruluş sayısal imzaların en üst düzeydeki yabancı sertifika hizmet sağlayıcıları tarafından verilmiş olan imza anahtarlarının tanınmasından da sorumludur.

5.1.1.3 Yasa ve Yönetmelik Uyumluluğunun Belirlenmesi

Düzenleyici kurumun diğer bir görevi, ilgili yasal hükümlerin uyumluluğunun belirlenmesidir. Eğer bir kuruluş açık anahtarını yanlışlıkla onayladığını iddia ediyor ve yasanın 4. maddesi altında lisanslandırılmış olduğunu söylüyorsa sertifikasyon faaliyetlerine devam etmesi yasaklanabilir. Düzenleyici kuruma bu tip durumların tanımlanmasında geniş yetkiler verilmiştir.

İnceleme görevleri lisanslandırılan sertifika hizmet sağlayıcısının gereken zamanlarda uygun adımları atıp atmadığını belirlemeyi de içermektedir. Sayısal İmza Yasası ve Yönetmeliğinin uyumluluğunun sağlanması için regülasyon kurumu otorite sertifika hizmet sağlayıcısına uygun olan akla yatkın talimatlar verebilir. Mesela uygun olmayan teknik unsurların kullanımı yasaklanabilir. Gidilecek en son merci olan sertifika hizmet sağlayıcısı lisansı iptal edildiği zaman sertifikasyon faaliyetlerinin gerçekleştirilmesi yasaklanabilir.

Sertifika hizmet sağlayıcılarının her iki yılda bir düzenli olarak düzenleyici kuruma uyumluluk raporu ve teyidinden sonra güvenlikle ilgili değişikliklerin denetlenmesi gerektiği belirtilmiştir.

5.1.1.4 Diğer İdari Görevler

Düzenleyici kurumun idari görevlerinin içerisinde onaylanan özel kuruluşların, liste ve yayınların basımı da yer almaktadır. Düzenleyici kurum diğer kuruluşlar tarafından kapsanmayan onaylama görevlerini de dolaylı olarak yürütür.

5.1.1.4.1. Onaylanmış Kuruluşların Akreditasyonu

Sayısal imza yasasında yetkilendirilmiş kuruluş olarak düzenleyici kurum onaylanmış kuruluşların akreditasyonun da sorumlu tutulmuştur. Bu kuruluşlar sertifika hizmet sağlayıcının ve teknik bileşenlerinin sayısal imza kanunu ve yönetmeliğine uyumluluğunu izlerler.

Bu kuruluş sertifika hizmet sağlayıcısına sayısal imza yasa ve yönetmeliğinin ilgili maddelerinde belirtilen uyumluluk için gerekli gereksinimleri yansıtmalıdır. Bu kuruluşlar idari asistanlar olarak düzenleyici kurumu destekleyecek şekilde çalışırlar.

5.1.1.4.2. Listeler

Sertifika hizmet sağlayıcılarına, kullanıcılara, teknik unsurları üreten üreticilere yardımcı olmak için düzenleyici otorite

- Sayısal imza yönetmeliğinin ilgili maddelerinde sağlanan gizlilik kavramlarını ölçecek olan güvenlik ölçülerinin
- Sayısal İmza yönetmeliğinin ilgili maddelerinde belirtilen teknik unsurlar için güvenlik önlemlerinin listesini tutar.

5.1.1.4.3. Yayınlar

Hedef gruplarla ilgili tüm uygun bilgilerin resmi gazetede yayınlandığından emin olunmalıdır. Yetkilendirilmiş onaylama kuruluşları ve hangi teknik bileşenlerin teyit edildiği sertifika hizmet sağlayıcılarına bildirilir. Ek olarak Düzenleyici Kurum Güvenlik Kurumu tarafından belirlenen uygun şifreleme algoritmalarını ve ilgili parametreleri yıllık olarak gözden geçirir ve yayınlar.

5.1.1.4.4. Özel İdari İşlemler

Alman Telekomünikasyon Yasasının hükümleri sayısal imza ile ilgili idari işlemleri içermemektedir.

Lisanslandırma prosedürü ve sertifika hizmet sağlayıcılarının lisans vermeye uygun olup olmadığı Regülasyon Kurumunun ilk sorumluluk alanıdır.

5.1.1.4.5 Güvenliğin Tesisi

1) Müsaade edilmeyen erişime karşı yüksek teknoloji alanları ve teknik elemanları koruyan altyapının güvenliği

2) Aynı faaliyetlerin paylaşılmasını engelleyecek şekilde uygun organizasyonun yapılarak görev ayrımının sağlanması

3) Özel görevlerin karşılıklı onaylama gibi güvenlik kriterleri

4) Teknik güvenlik aşağıda belirtilen şekilde sağlanabilir:

- Gizli matematiksel fonksiyonlar
- Tek imza anahtarı ve özel imza anahtarının gizliliği
- Hak sahibinin gizli imzasının güvenilirliğinin sağlanması
- Teknik elemanların kullanımı, özel güvenilirlik gereksinimleri ile uyumlu olarak tanımlanan kullanıcı ve çalışma çevresinin kullanımının denetlenmesi

5) Ayrıca sertifika hizmet sağlayıcıları tarafından uygulamaların sayısal imza yasası ve yönetmeliklerine uygun olup olmadığının denetlenmesidir. Hükümlere uyulmaz ise gerekli cezalandırma yapılmalıdır.

6) İmza sahiplerine sayısal imzanın güvenli kullanımı ve korunması hakkında açıklayıcı bilgiler verilmelidir.

Alman e-imza kanununun 15. maddesine göre sertifika hizmet sağlayıcıları başvuru yoluyla yetkili otorite (Reg Tp) tarafından akredite edilebilmektedir. Almanya'nın eski yasasına göre 2001 yılı Mayıs Ayına kadar 10 tane sertifika hizmet sağlayıcısı lisanslandırılmıştır. Lisanslandırılmış sertifika hizmet sağlayıcıların listesi Ek-2'de yer almaktadır. Yeni İmza Kanunundan sonra ise

sertifika hizmet sağlayıcıları akredite edilmeye başlanılmış olup akredite sertifika hizmet sağlayıcılara Reg Tp tarafından bir kalite işareti verilmektedir.

İmza Kanunu Kısım 15 (1) uyarınca akreditasyon başvuruları resmi yazı ile ya da imza yasası gereğince nitelikli elektronik imza eklenen elektronik doküman vasıtasıyla yapılmaktadır. Akreditasyon için yapılan başvurular eğer yönetmeliğin Kısım 1'inde yer alan form ve içerik şartları yerine getirildiyse dikkate alınmaktadır. Güvenlik ürünlerinin oluşumu ve sertifikasyonu sözkonusu yönetmeliğin Ek-1'inin Kısım 1'indeki hükümlere uyumlu olacak şekilde gerçekleştirilmektedir. Sözkonusu Ekte nitelikli elektronik imzalar için ürün değerlendirmesi ile ilgili şartlar yer almaktadır. Anılan Ekte özetle nitelikli sayısal imzanın teknik bileşenlerinin ve güvenli elektronik imza yaratma cihazlarının en azından Avrupa Standardizasyon Komitesi CEN'in çalıştay anlaşmaları vasıtasıyla kabul ettiği CWA 14168 standardında tanımlanan EAL 4 ya da E3 değerlendirme seviyesini; İmza değerlendirme bileşenleri için en az EAL3 ve E2 oluşum seviyesini kapsaması gerektiği, algoritmalar ile ilgili şartlar v.s. teknik konularla ilgili detaylara yer verilmektedir. Ek-2'sinde ise sertifika hizmet sağlayıcıların yapacakları çeşitli başvurulara yönelik kendileri tarafından ödenmesi gereken harç miktarları belirtilmektedir.

13.08.2001 tarihinden bugüne 17 tane sertifika hizmet sağlayıcısı Reg Tp tarafından akredite edilmiştir. Akredite edilen sertifika hizmet sağlayıcıların listesi Ek-3'te yer almaktadır.

Reg Tp ayrıca uygun kabul ettiği şifreleme algoritmalarını Alman Federal Gazetesinde bir tebliğ şeklinde yayınlamaktadır. 11 Mart 2003 tarihli Almanya Federal Gazetesinde yayınlanmış olan tebliğ ile anahtar yaratımı, nitelikli elektronik imza yaratımı ve doğrulaması, imzalanacak olan karma (hash) verisi için uygun kabul edilen algoritmalar ve ilgili parametreler belirlenmiştir.

Sözkonusu tebliğde belirlenen teknik özelliklerle ilgili aşağıdaki özet bilgileri vermek yerinde olabilir.

Uygun Şifreleme Algoritmaları:

Gelecek altı yıl içerisinde (2008 yılı sonuna değin) kullanılacak algoritmalar belirlenmiştir. Kesin bit spesifikasyonları ISO/IEC, NIST ve IEEE'de belirlenmiştir. RSA algoritması için parametre uzunluğu 1280'e çıkarılmıştır.

Uygun Karma (Hash) Fonksiyonlar için :
160 Bit değerindeki
RIPEMD-160([3]),
SHA-1 ([2], [3])
2008'in sonuna kadar kabul edilmiştir.

Uygun imza uygulamaları:

İmza Kanunu Kısım 17(3)'te yer alan sertifikasyon hizmetleri için gerekli teknik bileşenlerle ilgili olarak aşağıda belirtilen algoritmaların uygun olduğu belirtilmiştir.

1. RSA[4]
2. DSA[1], [4]

Eliptik eğrilere dayanan DSA değişkenleri:
- ECDSA [1], [5], [10], [11]
- ECKDSA, ECGDSA[11]
- Nyberg-Rueppel imzaları [19], [22]

Güvenlikle ilgili olarak uygulanacak metotlar:
1. Tamsayılar için faktörizasyon problemi
2. F_p ana alanının çoklu grubunda kesikli logaritma problemi
3. $E(F_p)$ ve $(E(F_2^m)$gruplarında kesikli logaritma problemi olarak belirlenmiştir.

İkinci olarak Reg Tp tarafından yayınlanmış olan sertifikaların listesi mevcuttur. Ayrıca belirlenen teknik bileşenleri onaylamaya yetkili kuruluşların listesi aşağıdaki şekildedir.

Bundesamt für Sicherheit in der Informationstechnik
debis Systemhaus Information Security Services GmbH
TÜV Informationstechnik GmbH
TÜV PRODUCT SERVICE GmbH

Ayrıca onaylanmış olan imza bileşenleri, anahtar üreticiler, fonksiyon kütüphaneleri, kullanıcı bileşenleri, hizmet bileşenler (dizin/zaman damgası), diğer bileşenler v.s. gibi elektronik imza ürünlerin marka ve modelleri Reg Tp tarafından yayınlanmaktadır.

5.2 II. Model: Avusturya Telekomünikasyon Regülasyon Kurumu (The Austrian Regulatory Authority for Telecommunications and Broadcasting (RTR-GmbH)) modeli

Avusturya regülasyon kurumu RTR, bünyesinde oluşturmuş olduğu Telekomünikasyon Kontrol Komitesi vasıtasıyla sayısal imza konularını Almanya örneğinde olduğu gibi Ulusal Kök sertifikasyon kurumu olarak görevlerini yürütmektedir [100] .

Avusturya'nın sayısal imza kanunu 1999 yılında yayınlanmış olup bu kanunla ilgili yönetmelik 2 Şubat 2000 tarihinde yayınlanmıştır.

Sözkonusu yönetmelik [101] her yönden bilhassa teknik açılardan oldukça kapsamlı bir yönetmelik olup sözkonusu yönetmeliğin çevirisi Kurumumuz koordinasyonunda sürdürülecek olan yönetmelik çalışmalarına model olması açısından Ek-4'de sunulmuştur. Sözkonusu yönetmelik başlıca aşağıdaki konuları kapsamaktadır:

5.3 III. Model: Finlandiya Haberleşme Regülasyon Kurumu (Finnish Communications Regulatory Authority-Ficora) Modeli

Finlandiya Haberleşme Regülasyon Kurumu, Ficora, Ulusal Kök sertifikasyon kurumu olarak görevlerini yürütmektedir. Finlandiya'nın elektronik imza yasası 24 Ocak 2003 tarihinde yayınlanmış yasa ile ilgili yönetmeliklerse 29 Ocak 2003 tarihinde yayınlanmışlardır [102].

Finlandiya'nın çıkarmış olduğu yönetmelikler [103,104] Kurumumuz koordinasyonunda sürdürülecek olan yönetmelik çalışmalarına model olması açısından Ek-5'te sunulmuştur. Sözkonusu yönetmelikler başlıca aşağıdaki konuları kapsamaktadır.

1. Sertifika Hizmet Sağlayıcıların FICORA'ya Bildirimde Bulunma Yükümlülüğü ile İlgili Yönetmelik

2. Nitelikli Sertifika Hizmeti Sağlayan Sertifika Hizmet Sağlayıcıları için Güvenilirlik ve Bilgi Güvenliği Yükümlülükleri yönetmeliği'dir.

5.4 IV. Model: Danimarka Ulusal Telekomünikasyon Ajansı (National Telecom Agency) modeli

Danimarka Ulusal Telekomünikasyon Ajansı, NTA, Ulusal Kök sertifikasyon kurumu olarak görevlerini yürütmektedir Danimarka'nın elektronik imza kanunu 29 Mayıs 2000 tarihinde yönetmelikleri ise 5 Ekim 2000 tarihinde yürürlüğe girmiştir[105].

Danimarka'nın çıkarmış olduğu yönetmelikler [106,107] Kurumumuz koordinasyonunda sürdürülecek olan yönetmelik çalışmalarına model olması açısından Ek-6'da sunulmuştur. Sözkonusu yönetmelikler başlıca aşağıdaki konuları kapsamaktadır:

1. Sertifika Hizmet Sağlayıcıları için Güvenlik Şartları Hakkındaki Yönetmelik; Bu yönetmelik

1) Sertifika hizmet sağlayıcıların güvenlik şartları v.s. ile ilgili faaliyetler
2) Nitelikli bir sertifika yayınlanmadan önceki kimlik kontrolü
3) Müşteri anlaşmalarının akdedilmesinde bilgi sunma zorunluluğu
4) Nitelikli sertifikaları ilgilendiren rehber ve iptal listeleri

ile ilgili düzenlemeler yapmaktadır.

2. Bilginin Sertifika Hizmet sağlayıcıları ve sistem denetleyicileri tarafından Ulusal Telekom Ajansına raporlanması hakkındaki yönetmelik;

1) Nitelikli sertifika yayınlayan sertifika hizmet sağlayıcılarının Ulusal Telekom Ajansına sunacağı bildirimin içeriği
2) Nitelikli sertifika yayınlayan sertifika hizmet sağlayıcılarının sistem denetleme performansı

konularına değinmektedir.

5.5 V. Model: İngiltere Ticaret ve Endüstri Bakanlığı (Department of Trade and Industry-(DTI) Modeli

İngiltere'de 99/93/EC direktifinin uygulamaya koyulmasını sağlayan kök sertifika hizmet sağlayıcılığı görevininin sorumluluğu telekomünikasyon regülasyon kurumuna verilmemiş olup bu görevi Ticaret ve Endüstri Bakanlığı (Department of Trade and Industry-(DTI)) [108] yürütmektedir. Ticaret ve Endüstri Bakanlığı Kamuya nitelikli sertifika sağlayan sertifika hizmet sağlayıcıların kamu kaydını tScheme [109] adı verilen bağımsız bir kuruluş ile bağlantılı olarak muhafaza etmektedir. tScheme bağımsız, endüstri yönelimli güvenlik servislerini onaylamakta ve bu kaydı endüstri ile devam etmekte olan temasları adına tutmaktadır.

İngiltere modeli daha detaylıca incelenmek istenirse;

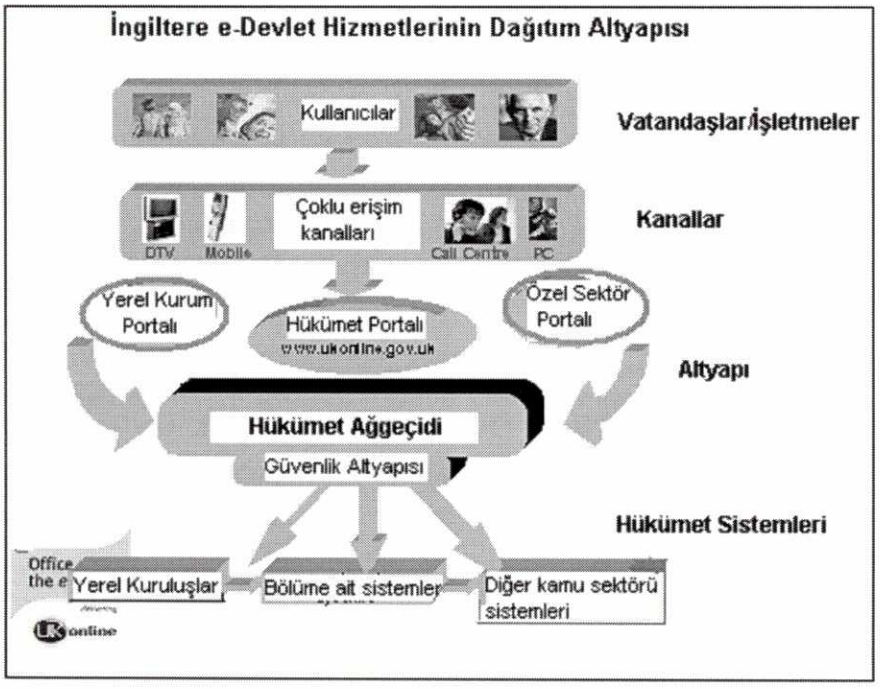
Çevrimiçi İngiltere projesi Ticaret ve Endüstri Bakanlığı vasıtasıyla yürütülmekte ve küçük ve orta ölçekli işletmelere uzman yardımı ve tarafsız tavsiyelerde bulunulmaktadır. Çevrimiçi İngiltere projesi kapsamında İngiltere;

- işletmeler,
- fırsatlar ve
- hükümeti 2005 yılı sonuna kadar çevrimiçi hale getirmeyi amaçlamaktadır.

Bu bağlamda işletmelerin %62'si web sayfasını oluşturmuş, %51'i ticari işlemlerini elektronik yöntemlerle gerçekleştirmiş ve çalışanların %91'i işyerlerinde internete bağlantısına kavuşmuşlardır.

Fırsatların dönüşümü kapsamında sayısal bölünmenin azaltılması amaçlanmaktadır ve bu bağlamda vatandaşlar için düşük maliyetli ya da ücretsiz internet bağlantısı sağlayan çevrimiçi merkezler kurulmaktadır.

Hükümet hizmetlerinin dönüştürülmesi (e-Devlet) kapsamında ise; Sözkonusu hizmetlerin %60'ının çevrimiçi olarak gerçekleştirilmesi sağlanmış ve bazı mükemmel web siteleri, UK online portalı ve hükümet ağgeçidi (gateway) kurulmuştur. Şekil 5.3 İngiltere e-Devlet Hizmetlerinin dağıtım altyapısı görülmektedir.



Kaynak:DTI [107]

Şekil 5.3 İngiltere e-Devlet Hizmetlerinin dağıtım altyapısı

Vatandaşlar, işletmeler, gerçekleştirmekte oldukları işlemlere göre Şekil 5.3'te yer alan hükümet ağgeçidine başvurmaktadırlar. İşlemlerin çeşitlerine göre bazı işlemler sayısal sertifika gerektirmektedir. Kabul edilen sertifikaları veren sertifika hizmet sağlayıcılar bağımsız tScheme kuruluşu tarafından yetkilendirilmektedirler.

5.6. Kurumumuz koordinatörlüğünde yürütülecek olan yönetmelik çalışmaları için model taslağı

5.6.1 I.MODEL

Sertifika Hizmet Sağlayıcıların Telekomünikasyon Kurumu'na Bildirimde Bulunma Yükümlülüğüne Dair Yönetmelik

BİRİNCİ BÖLÜM
Genel Hükümler

Amaç

Madde 1— Bu Yönetmeliğin amacı, kamuya nitelikli sertifika sağlayan sertifika hizmet sağlayıcılarının Telekomünikasyon Kurumu'na bulunmaları zorunlu oldukları bildirimlerle ilgili yükümlülükler hususunda uygulanacak usul ve esasları belirlemektir.

Kapsam

Madde 2 — Bu Yönetmelik; .. sayılı Elektronik İmza Kanunu hükümlerine göre faaliyet gösteren kamuya nitelikli elektronik hizmet sağlayan sertifika hizmet sağlayıcılarının Telekomünikasyon Kurumu'na bulunmaları zorunlu oldukları bildirimlerin usul ve esaslarını kapsar.

Hukuki Dayanak

Madde 3 — Bu Yönetmelik, ... sayılı İmza Kanunu'nun 8 inci ve 10 ncu ve 11 inci maddesi uyarınca hazırlanmıştır.

Tanımlar

Madde 4 — Bu Yönetmelikte geçen;

Kurum: Telekomünikasyon Kurumunu,

Kurul: Telekomünikasyon Kurulunu,

Elektronik Veri: Elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıtları,

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

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

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

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

Nitelikli sertifika: Ek I'de öngörülen şartları yerine getiren ve Ek II'de öngörülen gerekleri yerine getiren bir sertifika hizmet sağlayıcısı tarafından verilen bir sertifikayı,

İmza doğrulama verisi: Elektronik imzayı doğrulamak için kullanılan şifreler, kriptografik açık anahtar gibi verileri,

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

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,

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

Elektronik sertifika hizmet sağlayıcısı: Elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum veya kuruluşları ile özel hukuk gerçek veya tüzel kişileri,

İhtiyari akreditasyon: Sertifikasyon hizmeti sunulmasıyla ilgili tüm hak ve yükümlülükleri belirleyen, ilgili sertifika hizmeti sağlayıcısının isteği üzerine, bu hak ve yükümlülüklerin geliştirilmesi ve denetimi ile ilgili kamu ya da özel nitelikli kurum tarafından verilen ve sertifika hizmet sağlayıcısının bu izinden kaynaklanan haklarını kullanmasına, ilgili kararın kendisine ulaşmasına dek, engel olan her türlü izni,

ifade eder.

İKİNCİ BÖLÜM

Sertifika Hizmet Sağlayıcıların Kurum yapacakları bildirimler

Madde 5 — Sertifika hizmet sağlayıcıların Kuruma yapacağı bildirimler, elektronik imzalarla ilgili nitelikli sertifikaların kamuya sağlanmasına ilişkindir. Bildirimler yazılı olarak yapılacaktır.

Uygulamalara başlama bildirimi 3 ncü Bölümle ilgili bilgileri kapsayacaktır. Sertifika hizmet sağlayıcısı İmza Kanunu'nun 11 inci bölümünde yer alan nitelikli servisler sağlayan uygulamalar sonlandırıldığında Kuruma bilgi sağlama şartlarına uygun olarak daha önceden Kuruma sundukları bilgilerdeki değişiklikler hakkında Kurumu bilgilendirirler.

Sertifika Hizmet sağlayıcısı 5 inci bölümle ilgili faaliyetlere uyumlu olarak ve 6 ncı bölümde listelenen düzenli bilgilere göre kendi faaliyetlerini Kuruma yıllık olarak sunar.

ÜÇÜNCÜ BÖLÜM

İşlemlere Başlama Bildirisi

Madde 6 — Sertifika hizmet sağlayıcısının işlemlere başlamasıyla ilgili bildirisi, kendisinin irtibat bilgisi ve kendisini tanımlayan diğer gerekli bilgiler, sağlanan nitelikli sertifikalarda kullanılan hizmet bilgileri ve nitelikli sertifikaların kullanımı için kurum tarafından konulan şartları içerir. Sertifika hizmet sağlayıcısı ayrıca kendi personeli, hizmet hükümlerinde desteklenen kişiler ve diğer bilgiler, sertifika hizmet sağlayıcısının işlemlerinin güvenilirliği ile ilgili diğer bilgileri sunar.

Mali kaynakların değerlendirilmesinde, sertifika hizmet sağlayıcısı Kuruma sertifikalanmış tüm şirket ve resmi nihai hesaplarını iki yıl öncesi için sunan

bir yıllık plan ve sertifika faaliyetlerine ilişkin bir sonuç ve dengelenmiş bütçe ve izleyen mali periyod için bir operasyonel plan sunar. Yeni faaliyete geçen bir şirket Kuruma ilk mali yılı için dengelenmiş bir bütçe raporunu ve sonucunu, izleyen iki mali periyod için bütçe planları ve ilk periyod için bir operasyonel plan sunar. Buna ek olarak sertifika hizmet sağlayıcısı Kuruma kendisinin mali gücü, operasyonel riskleri, işlemlerinde ortaya çıkabilecek muhtemel güvenlik, kefaletler, garantiler ve düzenlemeler gibi zararların mali sorumluluğunu karşılama yeteneği ilgili diğer bilgileri vermelidir. Bildirim ayrıca şirketin diğer faaliyetleri dolayısıyla sertifikasyon işlemlerinin güvenilirliği ve devamlılığında oluşabilecek muhtemel risklerin değerlendirilmesini de içerir.

Sertifika hizmet sağlayıcısı kurumun bilgi güvenliğinin değerlendirilmesini sağlayan bilgiler sunar. Bu bilgi en azından sağlayıcının güvenlik politikası ve yönetim tarafından kabul edilen ve prensiplerini yazılı bir şekilde, yazılım, anahtar uzunlukları ve algoritmalar gibi sertifikasyon hizmetlerinde kullanılan veri ya da sistem ürünlerinin tanımı, buna ek olarak kuruma, bilgi ve standartlar ve bildirimde bulunan kuruluşlar tarafından verilen muhtemel değerlendirmelerini de sunar.

Sertifika hizmet sağlayıcısı Kurumu uyguladığı prosedürler ve uygulamaları hakkında bilgilendirir. Bu bilgi en azından sertifikasyon politikası ve uygulamalarını içermelidir. Buna ek olarak Sertifika Hizmet Sağlayıcı Kurumu kendisi tarafından verilen nitelikli sertifikaların veri içeriği ve yapısı hakkında bilgilendirir.

DÖRDÜNCÜ BÖLÜM
İşlemlerdeki Değişikliklerin Bildirimi

Madde 7 — Sertifika hizmet sağlayıcısı Kuruma kendi işlemleri ile ilgili temel değişiklikler ve Kuruma sunulan nitelikli sertifikanın içeriği hakkında bildirimde bulunur.

Bunun içerisinde kaydedilen verilerdeki Kurum tarafından korunan kamu kaydı ve kendi mali kaynaklarında ya da bilgi güvenliği ve güvenilirliği ile ilgili ek değişiklikler yer alır.

Sertifika hizmet sağlayıcısı Kurumu ayrıca bilgi güvenliğine ve güvenilirliğine tehlike oluşturacak olay ve kusurlar ve onların onarılması için gerekli tedbirler hakkında da bilgilendirecektir. Bildirimin gerekliliği gözönüne alındığında işlemlerin devamlılığı bağlamında değişikliklerin önemi ve kamu güvenilirliği temel kriter olacaktır.

BEŞİNCİ BÖLÜM

Yıllık Rapor

Madde 8 — Sertifika hizmet sağlayıcısı Kuruma kendi faaliyetleri ve sertifika hizmetleri ile ilgili yıllık bir rapor sunacaktır. Yıllık rapor, işlemlerin yaygınlığı, işlemlerdeki değişikler ve veri bildirimleri, ve güvenlikle ilgili konuları içerir.

Yıllık rapor, en azından tüm şirketin faaliyetlerinin nihai raporunu ve en sertifikalandırılmış resmi nihai hesapları içerir. Sertifika hizmet sağlayıcısı muhtemel sigortalar, kefaletler, garantiler ve zarar ve ziyan yükümlülükleri için olan düzenlemeler hakkındaki temel bilgiler gibi mali durumunun sağlamlığını, operasyonel riskleri ve operasyonlarına ilişkin olarak maruz kalabileceği mali sorumluluklarını karşılama imkanlarının değerlendirilmesi için gerekli olan diğer bilgileri de Kuruma sunacaktır. Beyan ayrıca sertifikasyon operasyonlarının güvenilirliği ve sürekliliğine yönelik olarak şirketin diğer faaliyetlerinin ortaya çıkardığı muhtemel risklerin bir değerlendirmesini de içerecektir.

4 ncü Bölüm uyarınca Kurumun bildirimine sunulmuş işlem değişikliklerine yıllık raporda tekrar değinilmesine ihtiyaç yoktur. Yıllık rapor Kuruma sertifika hizmet sağlayıcının muhasebe periyodunun bitiminden 4 ay içerisinde sunulmalıdır.

ALTINCI BÖLÜM

Diğer Düzenleyici Bilgiler

Madde 9 — Sertifika Hizmet Sağlayıcısının faaliyetleri ile ilgili bir rapor vermesi yasa hükmü ile zorunlu kılındıysa bu rapor bitirilir bitirilmez gecikme olmaksızın Kuruma sunulur.

YEDİNCİ BÖLÜM

İşlemlerin Fesih Duyurusu

Madde 10 — Sertifika hizmet sağlayıcısı nitelikli sertifika sağlamaktan vazgeçerse, fesih duyurusunu Kuruma gecikmeksizin sunar. Duyurudan sertifika hizmet sağlayıcısının nasıl haberdar ettiği ya da bununla ilgili nasıl bilgilendirildiği, örneğin kişilere yardım, imzacılara ve diğer işbirliği ortaklarına fesihin gerekçelerini, ya da imza yasasının 15. bölümüne uygun olarak veriyi güvenlikte tutma zorunluluğuna nasıl dikkat edeceği belli olmalıdır.

SEKİZİNCİ BÖLÜM

Son Hükümler

Yürürlük

Madde 12 — Bu Yönetmelik yayımı tarihinde yürürlüğe girer.

Yürütme

Madde 13 — Bu Yönetmelik hükümlerini Telekomünikasyon Kurulu Başkanı yürütür.

5.6.2 II. MODEL

Nitelikli Elektronik Sertifika Hizmeti Sağlayan Sertifika Hizmet Sağlayıcılarının Güvenilirlik ve Bilgi Güvenliği Yükümlülüklerine Dair Yönetmelik

BİRİNCİ BÖLÜM
Genel Hükümler

Amaç
Madde 1— Bu Yönetmeliğin amacı, nitelikli elektronik sertifika hizmeti sağlayan sertifika hizmet sağlayıcılarının güvenilirlik ve bilgi güvenliği yükümlülükleri hususunda uygulanacak usul ve esasları belirlemektir.

Kapsam
Madde 2 — Bu Yönetmelik; .. sayılı Elektronik İmza Kanunu hükümlerine göre faaliyet gösteren nitelikli elektronik hizmet sağlayan sertifika hizmet sağlayıcılarının güvenilirlik ve bilgi güvenliği yükümlülüklerinde uygulanacak usul ve esasları kapsar. Bu yönetmelik kamuya elektronik imzalara ilişkin nitelikli sertifikalar sağlayan sertifika hizmet sağlayıcılarına uygulanacaktır.

Hukuki Dayanak
Madde 3 — Bu Yönetmelik, ... sayılı İmza Kanunu'nun 8 inci, 10 ncu ve 11 nci maddesi uyarınca hazırlanmıştır.

Tanımlar
Madde 4 — Bu Yönetmelikte geçen;

Kurum: Telekomünikasyon Kurumunu,

Kurul: Telekomünikasyon Kurulunu,

Elektronik Veri: Elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıtları,

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

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

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

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

Nitelikli sertifika: Ek I'de öngörülen şartları yerine getiren ve Ek II'de öngörülen gerekleri yerine getiren bir sertifika hizmeti sağlayıcısı tarafından verilen bir sertifikayı,

İmza doğrulama verisi: Elektronik imzayı doğrulamak için kullanılan şifreler, kriptografik açık anahtar gibi verileri,

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

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,

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

Elektronik sertifika hizmet sağlayıcısı: Elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum veya kuruluşları ile özel hukuk gerçek veya tüzel kişileri,

İhtiyari akreditasyon: , sertifikasyon hizmeti sunulmasıyla ilgili tüm hak ve yükümlülükleri belirleyen, ilgili sertifika hizmeti sağlayıcısının isteği üzerine, bu hak ve yükümlülüklerin geliştirilmesi ve denetimi ile ilgili kamu ya da özel nitelikli kurum tarafından verilen ve sertifika hizmet sağlayıcısının bu izinden kaynaklanan haklarını kullanmasına, ilgili kararın kendisine ulaşmasına dek, engel olan her türlü izni,

ifade eder.

İKİNCİ BÖLÜM

Bilgi Güvenliği ile ilgili Genel Şartlar

Madde 5 — Sertifika hizmet sağlayıcısının diğer konulara ilave olarak bilgi güvenliği düzenlemesini de içeren yazılı olarak ifade edilmiş bir bilgi güvenlik sistemi olacaktır. Bilgi güvenlik yönetim sistemi düzenli olarak güncellenecektir. Sertifika hizmet sağlayıcısının bilgi güvenliğinin amaçları, ilkeleri ve uygulamasına ilişkin yazılı şekilde belirlenmiş ve sertifikasyon operasyonları ile ilgili yönetim ve personelin bağlı olduğu idare tarafından onaylanmış görüşleri olacaktır. Buna ek olarak, sertifika hizmet sağlayıcısının yazılımın kopyasını yedeklemek gibi bireysel uygulamalarla ilgili kendi bilgi güvenliğinin yürürlüğe konması için yazılı detaylı direktifleri olmalıdır. Sertifika hizmet sağlayıcısının bilgi güvenlik uygulamaları bir acil durum planını da içermelidir. Kurum bilgi güvenlik seviyesini düzenli olarak kontrol etmelidir.

Sertifika hizmet sağlayıcısı, kendi diğer prosedürleri yanında sertifika sınırlandırmaları ve imza sahibi ile ilgili yükümlülükler içeren sertifika politikasını halka açık hale getirmelidir. Politika ayrıca sertifikanın güvenilirliğinin değerlendirilmesinde şahıslar tarafından kontrol edilecek sertifikaya dayalı bilgileri de tarif etmelidir. Sertifika hizmet sağlayıcısı ayrıca kendi sertifika faaliyetlerinin içerisinde sertifika politikasının yürürlüğe konması ile ilgili daha detaylı bir tarifi içeren bir sertifika uygulaması düzenlemelidir. Sertifika hizmet sağlayıcısı kendi yazılımı ve donanımını yasadışı erişime karşı korumalıdır. Koruma ayrıca yasadışı çalma ve tahribatları da önlemelidir. Sertifika hizmet sağlayıcının sistemleri farklı erişim haklarını ve korumakta zorunlu olduğu kendi sistemlerinin tümü, kullanıcı adları ve haklarını taşıyan dosyalar ve bu isimlerin saklı tuttuğu hakları destekler.

Sertifika hizmet sağlayıcısı kendi veri, doküman, ekipman servisleri ve yazılımındaki bilgi güvenliğini etkileyen olayları bilgi güvenliğindeki belirlenebilecek öneme göre kontrol eder. Gerekli olduğunda yönetim hatalarıyla ilgili tüm olayların izlenmesi, sistem tanımı, faturalandırma, performans ve bilgi güvenliği sonradan mümkün olacaktır. Sertifika hizmet sağlayıcısı tarafından toplanan müşteri bilgisi yasadışı erişime karşı korunur.

Sertifika Hizmet Sağlayıcısı kendi sistemleri ve kendi bina ve müştemilatı hesabındaki yasadışı kullanıma engel olur. Yabancıların veri ile ilgili değişiklik, bozma, transfer ya da kullanıcı bilgileriyle ilgili bilgi sistemlerinin idaresi, faturalandırma, kaydetme gibi işlemleri yapmalarına izin verilmez.

Sertifika hizmet sağlayıcısı bilgi güvenliğinde minimum risk taşıyan bilgi sistemleri, yazılım ve donanımı kullanır. Şifreleme ve imza ile ilgili anahtarların idaresi ve yaratılması ve onlarla ilgili sertifikalar güvenli ekipmanlarla güvenli bir çerçevede özellikle yetkilendirilmiş kişilerce gerçekleştirilir. Sertifika hizmet sağlayıcısı veri işleme ile en iyi uygulamalarla uyumlu olan kendi veri materyalini ve kendi sertifika uygulamarı için temel olan yazılımın güvenli bir şekilde muhafazasını ve kopyalama yedeklemesini düzenler.

Sertifika hizmet sağlayıcısının yazılım ve ekipmanı sistemlerin kesintisiz kullanımını mümkün olduğu kadar dikkatli bir şekilde garanti eder. Sertifika hizmet sağlayıcısı beklenmedik karışıklıklar, sistemin bozulması, ve faaliyetlerin sınırlaması durumuna karşı yazılım ve ekipmanın seçiminde ve prosedürlerin ayarlanmasında önceden hazırlıklı olur. Faaliyetlerin devamlılığı, sistemlerin yeterli yedeklenmesi ve kopyalanması ile koruma altına alınır. Sertifika hizmet sağlayıcının yazılımı virüsler ve zararlı programlara karşı korunmalıdır. Sertifika hizmet sağlayıcısı dokümanları yazılım ve korunacak verilere göre sınıflandırır.

Bilgi güvenliğinin genel şartlarına ek olarak sertifika hizmet sağlayıcısı güvenilirlik ve kendi sertifika uygulamalarıyla ilgili muhtelif alanlardaki bilgi güvenliği konularını gözetecektir. Muhtelif alanlar ile ilgili şartlar şöyle sıralanır: 3 ncü bölüm içinde geçen kayıt, 4 ncü bölümde geçen nitelikli sertifikaların yaratılması, 5 nci bölümde geçen nitelikli sertifika yaratılmasıyla ilgili bilgilerin dağıtımı, 6 ncı bölümde geçen nitelikli sertifikaların kontrolü ve iptali.

ÜÇÜNCÜ BÖLÜM

Kayıt

Madde 6 — Nitelikli sertifika başvurusunda bulunan bir kişi için kimlik ve diğer muhtemel bilgiler kayıtla bağlantılı olarak başvuru sahibine nitelikli bir sertifika verilmeden önce kontrol edilir.

Başvuru sahibinin kimliği, emniyetli bir usul ve nitelikli sertifikanın bilgi içeriğinin oluşturulmasını teminen gerekli koşulların gerçekleştirilmesi için başvuru sahibinden sağlanan yeterli bilgi ile tasdik edilir. Sertifika hizmet sağlayıcısının anahtar çiftlerini yaratmadığı durumlarda sertifikalandırılacak açık anahtara karşılık gelen başvuru sahibinin gizli anahtarının kendi tasarrufunda olduğu kontrol edilmelidir.

Sertifika hizmet sağlayıcı nitelikli sertifika başvurusu ile bağlantılı olarak başvuru sahibinin bilgilerini bir sertifika dosyasına kaydeder. Bu veri başvuru sahibinin adı ve aynı isimdeki kişileri birbirlerinden ayıracak olan diğer bilgileri içerir. Bu bilgi örnek olarak doğum yeri ve yılı, adresi, diğer bir kimlik kartının numarası olabilir. Buna ek olarak yapılan kimlik tespiti, kimlik tespitinde kullanılan dokümanlar ve nitelikli sertifikanın verilmesi için gerekli diğer veriler bir dosya içerisine kaydedilmelidir.

DÖRDÜNCÜ BÖLÜM

Nitelikli Sertifikaların Yaratılması

Madde 7 — Nitelikli sertifikaların yaratılmasında, sertifika hizmet sağlayıcısı tarafından kullanılan sistemlerin gizliliği ve verilerin bütünlüğünü muhafaza edilmelidir. Bir nitelikli sertifika yalnızca sertifika hizmet sağlayıcısı tarafından konulan zorunluluklara başvuru sahibinin uymasıyla yaratılır.

Nitelikli sertifikalar aşağıdaki hususlara ilgi gösterilerek kanun hükümlerine uyumluluk içerisinde olmalıdır.

1. Nitelikli sertifikanın açık anahtarı başvuru sahibinin gizli anahtarına denk olmalıdır.

2. Nitelikli sertifika, sertifika hizmet sağlayıcısının nitelikli sertifikalar için ürettiği imza anahtarıyla yaratttığı gelişmiş elektronik imzayı ihtiva eder.

3. Nitelikli sertifika, sertifika için benzersiz bir tanıtıcıya sahiptir.

4. Geçerlilik süresi başlangıç ve son kullanma süresi tarihlerinin nitelikli sertifikada belirtilir

5. Algoritmalar ve kullanılan anahtarların uzunluğu genel kabul görüp onaylanan standartlar ve tavsiye kararlarına uyumlu ve güvenli olmalıdır.

Sertifika hizmet sağlayıcısı nitelikli sertifikaların kaydını tutar.

Sertifika hizmet sağlayıcısı nitelikli sertifika yaratmada kullanılan imza anahtarlarının kullanım sürelerinin bitiminden sonra tekrar kullanılmayacağını kabul eder.

BEŞİNCİ BÖLÜM

Yaratılan Nitelikli Sertifika ve İmzaların Teslimi

Madde 8 — Sertifika Hizmet Sağlayıcısı nitelikli sertifikayı imza sahibine teslim eder ve kendisi ve imza sahibi imza sahibinin sertifikayı ilgili olanların dikkatine getireceği hususunda mutabık kalırlar. Sertifika hizmet sağlayıcısı imza sahibiyle mutabık kalırsa nitelikli sertifikaları halka açık bir rehberde yayınlayabilir. Rehber servisleri günde 24 saat kullanılır durumda olmalıdır. Sertifika hizmet sağlayıcısı ayrıca nitelikli sertifikalarla ilgili sertifika politikası ve beyanını hazır tutar.

Sertifika hizmet sağlayıcısı başvuru sahibinin gizli anahtarını ya da 3 ncü taraflar için yaratılmasında kullanılan veriyi kopyalayamaz, kaydedemez ya da veremez.

ALTINCI BÖLÜM

Nitelikli Sertifikaların İptali ve Geçerliliğinin Gözden Geçirilmesi

Madde 9 — Listelerin kopyalanması, nitelikli sertifikaların iptali ile ilgili gelen isteklerin idaresinde kapanış listelerine kayıtla ilgili karar verilir. Nitelikli sertifikaların iptal edilmesinden sonra geri dönüş yoktur. İptalden önce nitelikli sertifika durdurulma durumunda tutulabilir. Bu ise iptal edilme ya da sertifikaların yeniden kullanılmasına imkan sağlar.

Sertifika hizmet sağlayıcı iptal isteklerini tüm istekler eşit ve hassaslıkla kabul eder bir usulde hemen işleme koyar. Kapanış listelerinin güncellemesi gecikmesizin gerçekleştirilir. Sertifika hizmet sağlayıcısı nitelikli sertifikayı yeniden kullanımı ya da iptali için durdurma durumunda tutarak kaydeder. Kapanış listeleri gecikmesizin güncellenir.

Sertifika hizmet sağlayıcısı ve kendisi tarafından kullanılan güvenilir sistemler tarafından verilen tüm nitelikli sertifikalar iptal edilebilmelidir. Sertifika hizmet sağlayıcısı imza sahibini iptal hakkında bilgilendirir.

Nitelikli sertifikaların durumu kapanış listesi üç aylık sürelerde hizmeti yönünden kontrol edilme durumunda olmalıdır. Bu hizmet ya çevrimiçi olmalı ya da düzenli olarak güncellenmelidir.

Sertifika Hizmet sağlayıcısı kapanış listelerinin ya da onun yanıtlarını imzalar. İmzalanmış kapanış listesi yada listenin yanıtları listenin basım tarihini ya da yanıt tarihini içerecektir. Buna ek olarak sertifika hizmet sağlayıcısı nitelikli sertifika kapanış listesi talepleri ve yanıtlarının kontrolü için günlük bilgileri kayıt edebilir.

YEDİNCİ BÖLÜM

Sertifika Hizmet Sağlayıcısının Mali Kaynakları

Madde 10 — Sertifika hizmet sağlayıcısının mali kaynakları kendi sertifika uygulamaları ve bu yönetmelikle uyumlu olarak bilgi güvenliğini ve güvenilirliğini tehlikeye atmaksızın kendi sistemlerinin muhafazasını sağlamaya muktedir olmadır.

Sertifika hizmet sağlayıcısı mali kaynaklarının uygulamaların durması ve zararlardan doğacak sorumlulukları karşılamaya yeterli olduğunu kabul eder. Sertifika hizmet sağlayıcısı zararların sorumluluğunu karşılamak için sigorta, bir banka garantisi ya da ona tekabül eden diğer bir anlaşma yapar.

Sertifika hizmet sağlayıcısı uygulamalar için gerekli mali kaynağı sağlarken sertifika faaliyetleri ve uygulamaların değeri ile ilgili mali riskleri analiz etmelidir. Sertifika hizmet sağlayıcısının sertifikasyondan başka faaliyetleri mevcut ise sertifika hizmet sağlayıcısı kendi sertifikasyon uygulamalarının devamlılığı ve güvenilirliği için doğacak diğer riskleri değerlendirir. Sertifika hizmet sağlayıcı kendi mali kaynaklarının sertifikasyon faaliyetleri ile ilgili muhtemel mali riskler ve zararlardan doğan sorumlulukları kapsamaya yeterli olduğunu kabul eder.

SEKİZİNCİ BÖLÜM

İşlemlere Son verilmesi

Madde 11 — Sertifika hizmet sağlayıcısı işlemlerini yürüten tüm personeli, imza sahiplerini ve diğer paydaşlarını kendi faaliyetlerine son verdiği hususunda bilgilendirir. Sertifika hizmet sağlayıcısı imza sahipleri ve diğer taraflara verilen zararın en az seviyede olduğunu kabul eder.

Sertifika hizmet sağlayıcısı faaliyetlerini durdurmasıyla bağlantılı olarak elektronik imza yasasının 18. bölümünde yeralan verilerin muhafazasından sorumludur.

Faaliyetlerin durdurulmasında, sertifika hizmet sağlayıcısı nitelikli sertifika yaratmada kullanılan imza anahtarlarının yeniden kullanılamayacağını kabul eder.

DOKUZUNCU BÖLÜM

Son Hükümler

Yürürlük
Madde 12 — Bu Yönetmelik yayımı tarihinde yürürlüğe girer.
Yürütme
Madde 13 — Bu Yönetmelik hükümlerini Telekomünikasyon Kurulu Başkanı yürütür.

Ek I

Nitelikli sertifikaların tabi olduğu şartlar

Tüm nitelikli sertifikalar aşağıdaki hususları içerir:

(a) Sertifikanın nitelikli sertifika olarak verildiğine dair bir ibare;

(b) Sertifika hizmet sağlayıcısının ve bulunduğu ülkenin adı;

(c) İmzalayanın ismi ya da bu şekilde tanımlanacak takma adı;

(d) Sertifikanın veriliş amacına bağlı olarak, gerektiğinde imzalayanın özel bir niteliğinin belirtilmesi;

(e) İmzalayanın kontrolü altında, imza yaratımı için gerekli verilere karşılık gelen imza doğrulama verileri;

(f) Sertifikanın geçerlilik süresinin başlangıç ve bitiş tarihine ilişkin bir ibare;

(g) Sertifikanın kimlik kodu;

(h) Nitelikli sertifikayı veren sertifika hizmet sağlayıcısının ileri elektronik imzası;

(i) Gerektiği takdirde, sertifikanın kullanımının kapsamına ilişkin sınırlamalar;

(j) Gerektiği takdirde, sertifikanın kullanılabileceği hukuki işlemlerin değerlerinin sınırları.

EK II

Nitelikli sertifika veren sertifikasyon hizmet sağlayıcıları ile ilgili şartlar

Sertifika hizmet sağlayıcılarının aşağıdaki şartları yerine getirmesi gerekir:

(a) sertifikasyon hizmeti sunmak için yeterli güvenilirlikte olduklarını göstermek;
(b) hızlı ve güvenli bir rehber (başvuru) hizmeti ile güvenli ve çabuk bir iptal hizmetinin işleyişini temin etmek;
(c) sertifikaların verildiği veya iptal edildiği tarih ve saatin kesin olarak belirlenebilmesini temin etmek;
(d) ulusal hukuk çerçevesinde uygun vasıtalarla, nitelikli sertifikanın verildiği kişinin kimliğini ve gerektiğinde, özel niteliklerini doğrulamak;
(e) uzmanlık bilgisine, deneyime ve hizmetlerin sunumunda gerekli niteliklere, özellikle yönetsel seviyede yeterliliğe, elektronik imza teknolojisi konusunda özel bilgilere ve uygun güvenlik prosedürleri alanında deneyime sahip personel çalıştırılması; personelin aynı zamanda kabul edilmiş standartlar çerçevesinde yeterli ve bunları karşılayacak yönetsel prosedürleri de uygulayabilmeleri gereklidir;
(f) değiştirmeye karşı korumalı güvenilir sistem ve ürünlerin kullanımı ile bunlar tarafından desteklenecek işlemin teknik ve kriptografik güvenliğinin temin edilmesi;
(g) sertifikanın taklidine karşı önlemler alınması,ve sertifika hizmet sağlayıcısının imza yaratımını da meydana getirmesi halinde, ilgili verilerin meydana getirilmesi işlemi sırasında gizliliğin temini;
(h) özellikle zararın tazmini sorumluluğunun üstlenilebilmesi için, örneğin uygun bir sigorta sözleşmesi yapma yoluyla, yeterli mali kaynakların bulundurulması,
(i) özellikle yargısal süreçlerde sertifikanın kanıtlanması amacıyla kullanılabilmesini teminen, nitelikli sertifikaya ilişkin tüm kayıtların uygun bir süre boyunca saklanması; bu kayıtların elektronik yollarla yapılması

mümkündür;

(j) Sertifika hizmet sağlayıcısının önemli (esaslı) yönetim hizmeti verdiği kişiyle ilgili verileri kopyalamaması ya da saklamaması;

(k) elektronik imza destekli bir sertifika isteyen kişiyle sözleşmeye dayalı ilişki kurulmadan önce, kalıcı iletişim yollarıyla, sertifika kullanımına ilişkin, kullanımdaki kısıtlamalar da dahil olmak üzere, kesin kural ve koşulların, ihtiyari bir akreditasyon hizmet sisteminin varlığı, şikayet usulleri ve uyuşmazlıkların çözümü prosedürleri konusunda kişiyi bilgilendirmesi. Elektronik yolla da iletilebilecek bu bilgi, yazılı olarak ve kolayca anlaşılabilir bir dille yapılmalıdır. İlgili bilgiler bu sertifikaya dayanan üçüncü kişilere de isteğe bağlı olarak sunulabilmelidir;

(l) Sertifikaları doğrulanabilir bir şekilde saklamak üzere güvenilir sistemler kullanmak ve böylece :

· Sadece yetkili kişilerin verileri alabilmesini ve değiştirebilmesini,

· Bilgilerin doğruluğunun kontrol edilebilmesini,

· Sadece sertifikasyon sahibinin rızasının alındığı durumlarda sertifikaların tekrar kullanılabilir olmasının teminini,

· Bu güvenlik sistemlerini tehlikeye sokabilecek tüm teknik değişikliklerin işletici tarafından fark edilmesinin mümkün olmasını

Sağlamak.

SONUÇ VE ÖNERİLER

Bütün vatandaşlara erişilebilir iletişim hizmeti olanağının sunulması, bilgi toplumunun yaygınlaşması elektronik ortama geçiş sürecini dolayısıyla elektronik ticaretin gelişimini hızlandıracaktır. Bu tür hizmetler; etkin, rekabetçi bir düzenleyici yapıya dayalı olarak faaliyet gösteren, liberalleştirilmiş bir iletişim sektörü temelinde mümkün olabilmektedir.

Elektronik ticarete geçişte;

- Vatandaşların, işletmelerin ve devletin modern iletişim ağlarına ve bu ağlar üzerinden sunulan hizmetlere ulaşabilir olması

- Yeni teknoloji ve rekabeti arttırıcı düzenleyici yapıların, erişim ücretlerini azaltarak yüksek hızlı çokluortam internet erişimini arttırması

- Telekomünikasyon sektörünün liberalizasyonunun hızlandırılması, eksiksiz bir biçimde tamamlanması ve gerekli hizmetlerde yetkilendirmeler yapılması,

- Telekomünikasyon hizmetlerinde evrensel hizmetin hayata geçirilmesine ilişkin uygulama düzenlemelerini başlatmak ve internet erişimine olanak tanıyan, uygun fiyatlı temel telefon hizmetlerinin yaygınlığının sağlanması

elektronik ticaretin gelişimini arttırıcı hususların başında gelmektedirler.

Bilgi toplumunun omurgasının oluşturulması için, altyapının yaygınlaşmasının hızlandırılması gerekmektedir. Bu yaygınlaşma, ülkemizin küresel, bütünleşik bilgi altyapısında kendisine yer bulmasında yardımcı olacak ve küresel pazarlara kaliteli erişim sağlamanın yanında, özellikle bu tür bir altyapıya dayalı ekonomik sektörlerde yatırımları kendine çekecektir.

Yerel erişim hizmetlerinin fiyatlandırılmasında ayrım, 3. nesil gezgin ağlara lisans verilmesi, internet uyumlu sayısal televizyon aglarının devreye girmesi ve Internet Protokolü'nün 6. sürümüne (Ipv6) geçilmesi, rekabetçi hizmet anlayışının çokluortam hizmetlere ulaşılmasını sağladığı görüşü temelinde, teknolojinin yaygınlığını arttıran ek önlemlerdir.

Bu tez çalışmasının;

Birinci bölümünde elektronik ticareti kuşatan teknolojik ve piyasa eğilimlerinin içeriği ve tarihçesi incelenerek konuya bir giriş yapılmış,

İkinci bölümünde yeni bir kavram olarak karşımıza çıkmaya başlayan elektronik imza konusunun dayandığı teknik temellerin daha iyi anlaşılması amaçlanmıştır. Konuyla ilgili önemli tanımlar yapılmış, elektronik ticaretin hayata geçirilmesi için en önemli unsur olan taraflar arası iletilerde; bilginin gizliliği, bütünlüğü ve tarafların kimliklerinin doğruluğunu sağlayan sayısal imzanın dayandığı temeller, şifrelendirmeye dayalı olmayan güvenik mekanizmaları, şifrelendirmeye dayanan güvenlik mekanizmaları ve açık anahtar altyapısı (PKI) detaylıca açıklanmıştır. Ayrıca sayısal imzanın oluşumu şekil ve grafikler yardımıyla açıklanmaya çalışılmış, bunun yanında uluslararası sayısal imza politikası konuları ve teşebbüsleri incelenmiştir.

Tezin üçüncü bölümünde uluslararası elektronik ticaret politikası konuları ve teşebbüsleri, fonksiyonel kurumların elektronik ticaretle ilgili gerçekleştirmiş oldukları çalışmalar ve faaliyetlere değinilmiş ve Ülkemizde yürütülmekte olan elektronik ticaret çalışmalarının tarihçesi incelenmiş ve son durum hakkında bilgi verilmiştir.

Tezin "Telekomünikasyon Pazarı ile İlgili Regülasyonların Elektronik Ticaret Üzerindeki Etkileri" konulu dördüncü bölümünde telekomünikasyon pazarı ile ilgili;

- Altyapı,
- Evrensel hizmet,
- Pazar yapısı, rekabet, lisanslandırma ve
- Ekonomik ve ücretlendirici regülasyon

konuları için varolan regülasyon seçenekleri ve bu seçeneklerin elektronik ticaret üzerindeki etkilerinin neler olabileceği araştırılmış ve bunlarla ilgili bazı önerilerde bulunulmuştur. Sözkonusu regülasyon konuları elektronik ticaretin kaderini belirleyecek güce sahiptir. Kurumumuzun sözkonusu regülasyonları yaparken bilgi tabanlı ekonomiye geçişin temellerini oluşturan bu hususlara dikkat etmesinin özel önem arz ettiği düşünülmektedir.

Elektronik ticaretin yasal temelinin dayanağı olarak, Avrupa Birliğinin ilgili müktesabatının kabulü, pazarın gelişimi için anahtar konumdadır. Bu bağlamda Avrupa Birliği üyesi ülkeleri incelediğimizde; 99/93/EC nolu e-imza direktifinin yürürlüğe konmasını sağlayan kanun ve yönetmelikleri çıkardıklarını, aday ülkelerin de ilgili düzenlemeleri çıkarmaya devam ettiklerini görmekteyiz. Nitekim Ülkemizde de bilindiği üzere Adalet Bakanlığı tarafından hazırlanan ve Meclis'e sevkedilen Elektronik İmza Kanunu Tasarısı da bu amaca yöneliktir. Sözkonusu tasarıda sorumlu kurum olarak Kurumumuz tanımlanmıştır. Bu bağlamda Kurumumuz Elektronik İmza Kanun Tasarısı'nda yer alan aşağıdaki maddelerle ilgili yönetmelikleri bir yıl içerisinde çıkarmakla görevlendirilmiştir.

Madde 6 Güvenli Elektronik İmza Oluşturma Araçları,
Madde 7 Güvenli Elektronik İmza Doğrulama Araçları,
Madde 8 Elektronik Sertifika Hizmet Sağlayıcısı,
Madde 10 Elektronik Sertifika Hizmet Sağlayıcısının Yükümlülükleri

Madde 11 Nitelikli Elektronik Sertifikaların İptal Edilmesi

99/93/EC direktifini yürürlüğe koyan kanun ve yönetmelikler tarafından Telekomünikasyon Regülasyon Kurumları sorumlu kılınan elektronik imza konusunda lider konumdaki Avrupa Birliği ülkeleri bulunmaktadır. Bu ülkeler sözkonusu yönetmelikleri halihazırda yayınlamış olup uygulamaktadırlar. Kurumumuzun koordinatörlüğünde yürütülecek olan bu meyandaki yönetmelik çalışmalarına katkı sağlamak ve bir model oluşturmak amacıyla tezin beşinci bölümünde Almanya, Avusturya, Danimarka ve Finlandiya Telekomünikasyon Regülasyon Kurumlarının uyguladığı modeller, yönetmelikler ve sorumlulukları detaylıca incelenmiş, sözkonusu ülkelerin yayınlamış oldukları yönetmeliklerin çevirisi yapılmış ve Kurumumuz koordinatörlüğünde yürütülecek olan yönetmelik çalışmalarına model olması açısından iki yönetmelik taslağı hazırlanmıştır. Ayrıca farklı bir örnek olması açısından İngiltere Ticaret ve Endüstri Bakanlığı (Department of Trade and Industry-(DTI) Modeli de incelenmiştir.

Model olarak incelenen Almanya, Avusturya, Danimarka ve Finlandiya'da ulusal açık anahtar altyapısını kurma görevi telekomünikasyon regülasyon kurumlarına verilmiştir. Anılan ülkeler ulusal açık anahtar altyapılarını kurarak işletmeye başlamışlardır. Böylelikle akreditasyon ve denetleme tek bir kuruluş tarafından sağlanmakta sertifika hizmet sağlayıcıların sağlaması gereken teknik, idari şartlar, mali yükümlülükler garanti altına alınmaktadır.

Elektronik İmza Yasasında Kurumumuza verilen sorumlulukta aynı türden bir sorumluluktur. Kurumumuzun önce ülkemizin açık anahtar altyapısı sistemini kurması gerekmektedir. Şekil 5.1'den de açıkça görülebileceği gibi kök sertifika hizmet sağlayıcısının bir sertifika hizmet sağlayıcısını akredite etmesi ona kendi yayınladığı elektronik sertifikayı elektronik yolla göndermesi ile mümkündür. Yani her şey elektronik yollarla olmaktadır. Elektronik İmza Kanun Tasarısı'nda da Kurumumuzun kök sertifika hizmet sağlayıcısı olarak

Kurumumuz bünyesinde bu tipten bir ulusal açık anahtar altyapısının kurularak kök sertifikasyon hizmetinin sağlanması için çok temel olarak [92] ;
- 4 ayrı ofis,
- özel güvenlik odası
- takviye edilerek sağlamlaştırılmış kapılar, pencereler,
- izinsiz kişilerin girişinin engellenmesi,
su baskını ve yangın alarm sistemleri, ayrı bir güç kaynağı v.s. gerekmektedir. Bina ve altyapı masrafları bu kısım için yaklaşık olarak 348.000 Euro dolayındadır. Anahtar üreticiden internet sunucusuna sahip anahtar üreticisine kadar olan asıl IT altyapısı güvenlik kavramıyla birlikte 358.000 Euro dolayındadır.

Ancak tüm bunlar güvenlik kavramı sertifikasyonu ya da personel masraflarını içermemektedir. Tüm her şey gözönüne alındığında bu tip bir açık anahtar sisteminin kurulmasının maliyeti 2.6-7.7 milyon Euro civarındadır.

Kurulumu bu tip büyük bir maliyet gerektiren kök sertifikasyon hizmeti sağlayacak olan açık anahtar altyapısının sahibi olan kök sertifika hizmet sağlayıcısının diğer sertifika hizmet sağlayıcılara sunacağı akreditasyonla ilgili hizmetler için talep ettiği harç miktarları Avusturya Telekomünikasyon İdaresinin yönetmeliğinde açıkça belirtilmektedir.

Bunlara bir kaç örnek vermek istenirse Avusturya Telekomünikasyon İdaresi;

Bir sertifika hizmet sağlayıcının, işi için başvurusu nedeni ile kontrolü ve kayıt edilmesi ile ilgili olarak eğer sertifika hizmet sağlayıcı nitelikli bir sertifika hazırlıyor veya güvenli elektronik imza yöntemi uyguluyorsa 6 000 Euro; başka bir güvenlik- ve sertifikalama taslağı başvurusunda güvenlik için önemli değişiklikler varsa 4 000 Euro; başka bir güvenlik- ve sertifikalama

sertifika hizmet sağlayıcısının, yetkilendirme başvurusu nedeni ile tetkiki (SigG – imza kanunu- madde 17) 6 000 Euro; eğer sertifika hizmeti sağlayıcısı nitelikli sertifikalar hazırlıyorsa, mevcut güvenlik- ve sertifikalama taslağında güvenlik için önemli esaslı değişiklikler başvurusu yapan sertifika hizmet sağlayıcısının tetkiki (SigG madde 6 fıkra 5) 4 000 Euro;. bir sertifika hizmet sağlayıcısının düzenli tetkiki (SigG madde 13 fıkra 1) 4 000 Euro; imza kanunu hükümlerini veya önceki esas yönetmeliğin önemsiz ihlalleri tespit edildiğinde sertifika hizmeti sunanın ayrıca tetkiki 6 000 Euro; eğer denetim mercilerine bildirilmedi ise, güvenlik- ve sertifikalama taslağında güvenlik için önemli değişiklikler yapan bir sertifika hizmet sağlayıcısının tetkiki 6 000 Euro; miktarlarını harç olarak belirlemiştir.

Görüldüğü gibi sistemin kurulum masrafları ve istenilen harç miktarları azımsanacak miktarlar değildirler.

Bu bağlamda sözkonusu yönetmeliklerin çıkarılabilmesi için gereken ulusal açık anahtar altyapısının kurulması için ilk olarak Kurumumuz bünyesinde kurulan "e-imza Koordinasyon Kurulu" üyelerinin tavsiyelerinin alınması ve ilgili kuruluşlarla gerekli işbirliğinin sağlanması;

İkinci olarak sözkonusu görevi halihazırda gerçekleştirmekte olan Avrupa Birliği üyesi ülkelerin Telekomünikasyon Regülasyon Kurumlarıyla irtibata geçilmesi, karşılıklı görüş alış verişi, tecrübelerin paylaşımı ve işbirliği imkanlarının araştırılmasının yerinde olacağı düşünülmektedir. Örneğin bu konuda beş yılı aşkın tecrübeye sahip olan aynı zamanda Ülkemiz elektronik imza yasa taslağına örnek olan Almanya'nın elektronik imza yasasının düzenleyici kurumu Reg Tp Kurumumuza yardım sağlamaktan memnun olacaklarını belirterek Kurumumuzu bu konuda karşılıklı görüş alışverişinde bulunmak üzere Almanya'ya davet etmiştir. Aynı şekilde bu konuda ileri tecrübeye sahip bir diğer ülke olan olan Avusturya'da Kurumumuza bu konuda yardım sağlamaktan memnuniyet duyacağını belirtmiş ve Avrupa

Birliği üyesi ve aday ülkelerin elektronik imzalardan sorumlu kuruluşlarının kurmuş olduğu Avrupa Elektronik İmzalar Denetleyici Kuruluşlar Forumu'nun (Forum of European Supervisory Authorities for Electronic Signatures-FESA) çalışmalarına katılmaya kurumumuzu davet etmiştir. Kurumumuz bu daveti olumlu değerlendirerek FESA ile irtibata geçmiştir. Uluslararası Telekomünikasyon Birliği ise Kurumumuz tarafından ulusal açık anahtar altyapısının kurulmasına yönelik bir işbirliği talebinin resmi olarak iletilmesi durumunda bunun değerlendirileceğini bildirmiştir.

Avrupa Birliği ülkeleriyle yapılacak olan işbirliği sayesinde uluslararası standartlara uygun olan açık anahtar altyapısının ülkemizde kurulması temin edilmiş olacaktır. Standartlara uygun olmayan bir sistemin kurulması ulusal açık anahtar altyapısının yayınlayacağı sertifikaların uluslararası boyutta tanınmasını engelleyecektir.

Bu meyanda Kanun tasarısıyla kurumumuza verilmiş olan ulusal açık anahtar altyapısını kurma görevi gerek yurtiçi, gerek yurtdışı gerekli işbirliği sağlanarak gerçekleştirilmelidir. Kanun tasarısında bu görevi gerçekleştirmesi için kurumumuza gerekli kaynak, işgücü, kurum bünyesinde sözkonusu faaliyetleri gerçekleştirecek olan bir birim kurma hakkı verilmemiştir. Ancak sözkonusu faaliyetlerin gerçekleştirilmesini teminen öncelikle ulusal açık anahtar altyapısının kurulması için ihaleye çıkılması, ülkemizde bulunan uzmanların kurumumuz bünyesinde kurulacak olan birimde toplanmasının sağlanması, sorumlu personele bu konuyla ilgili gerekli eğitimleri alma imkanının sağlanmasının yerinde olacağı uygun mütalaa edilmektedir.

Bu bağlamda hazırlanmış olan bu tez çalışmasının telekomünikasyon regülasyonlarının elektronik ticaret üzerindeki etkisinin anlaşılmasının sağlanmasında, yeni bir teknoloji olan sayısal imzanın temellerinin daha iyi anlaşılmasında ve e-imza konusunda Kurumumuza verilecek olan sorumluluklar yerine getirilirken kullanılacak bir kaynak olacağı düşünülmektedir.

KAYNAKLAR

[1] İNCE Murat,1999, Elektronik Ticaret: Gelişme Yolundaki Ülkeler için imkanlar ve politikalar, DPT Raporu, s.2, s 6,

[2] OECD, 1999, 1999b: Voluntary approaches for environmental policy in OECD countries: an assessment, ENV/EPOC/GEEI(98)30/REV1, s.33

[3] SOYDAN Billur Yaltı, Mayıs 2001, E-İmza ve E-Belge: Kağıtsız Mürekkepsiz Dünyada Hukuk-II., Vergi Sorunları, s. 152, 158. 195

[4] ERSOY Zeynep, 1999, Elektronik Ticaret ve Ticaret Noktaları, İGEME, s. 42.

[5] T.C. Ulaştırma Bakanlığı, TUENA, Altyapı Planlaması Sonuçlar Özeti, (Haziran 1998), s. 24.

[6] http://eticaret.garanti.com.tr/dunyada_e_tic.htm

[7] CHARLES E.Mclure, September 1997, Electronic Commerce, State Sales Taxation, ABD Intergovermental Fiscal Relations., National Tax Journal, V. L, N.4,), p. 731

[8] CANGİR Niyazi, Eylül 1998, Elektronik Ticaretin ya da İnternetin Vergilendirilmesi Yaklaşımı s. 53,69

[9] UZUNOĞLU Hakan, 2002, Elektronik Ticaretin Vergilendirilmesinin İncelenmesi ve Değerlendirilmesi , Gazi Üniversitesi Sosyal Bilimler Enstitüsü Maliye Ana Bilim Dalı Master Tezi s. 11, 63, 187

[10] http://www.oecd.org

[11] Tübitak Bilten (Bilgi teknolojileri elektronik araştırma enstitüsü), 2000,Türkiye İçin Elektronik Ticarete Geçiş Durum Değerlendirmesi ve Pilot Uygulama Projesi Raporu, s. 6,8

[12] 86] Public-Key Infrastructure (X.509) (pkix) http://www.ietf.org/html.charters/pkix-charter.html,2003, s.2

[13] http://www.wa.gov

[14] http://unicc.org/unece/cefact/intro.htm

[15] http://www.etkk.gov.tr

[16] Internet society, A brief history of internet, http://www.isoc.org, s.1

[17] WTO,1998, Electronic Commerce and the Role of the WTO, http://www.wto.org, s.1

[18] http:// www.ecommerce.gov

[19] International Telecommunications Union (ITU), 1999, Challenges to the Network: Internet for Development Geneva, s.11

[20] United Nations Conference on Trade and Development (UNCTAD), 2002, E-Commerce and Development report 2002, s. 3-7

[21] Yeni Ekonomi, Mart 2001, NTV MAG Dergisi, Sayı 19, s. 87

[22] www.cnnic.net.cn/develst/rep200201-e.shtml

[23] Computer Sciences Corporation, 2001, CSC's 14th Annual Critical Issues of Information System Managements Survey., s. 6

[24] IDC Research (2002a), 3 January 2002, Western Europe Pulls Ahead of United States. E-newsletter dated 3 January. Available at www.idc.com, s.1, s.2

[25] BOZKURT Veysel, 2000, Elektronik Ticaretin Ekonomik ve Sosyal Boyutu içinde Elektronik Ticaret, s.66

[25] eMarketer Inc, 2001, (2001a) Future Looks Bright As 40.8 Million Users Will be on Line in Latin America by 2004 (www. E-marketer.com), s. 2

[26] Forrester Research Inc. (2001), 26 December 2001,Global Online Trade Will Climb to 18% of Sales. Brief dated 26 December. www.forrester.com/ER/Research/Brief/0,1317,13720,FF.html. s.1

[27] KESER, Aşkın, 2000, Küreselleşen Dünyanın Yeni Gerçeği: Elektronik Ticaret," içinde Elektronik Ticaret, Alfa Yayınları s.2, s.16-17

[28] MANN Catherine, ECKERT Sue E., KNIGHT Sarah Cleeland, 2000, Global Electronic Commerce s.9, s.13, s.144-147

[29] http://www.igeme.org.tr/TUR/etrade/etkk/hukuk/h_altyapi.htm

[30] BLOC Michael, PIGNEUR Yves, SEGEV Arie, 1996, On the Road of Electronic Commerce –A Business Framework, Gaining Competitive Advantage and Some Research Issues, s.2-4

[31] SAX Michael M., 2000, International Law Issues Relating to Electronic Commerce May 1, 2000, Sax Law Office, s. 16, s. 18,

[32] HOUSLEY, R., POLK W.T., 2001, Planning for PKI: Best practices for PKI Deployment, Wiley& Sons, s.5

[33] http://www.turkpoint.com/e-yasam/sayisal_imza.asp

[34] KUHN D. Richard, HU Vincent C., POLK W. Timothy Polk,CHANG Shu-Jen, 26.02.2001, Introduction to Public KeyTechnology and the Federal PKI Infrastructure, NIST National Institude of Standards and Technology, s.3

[35] National Institute of Standards and Technology, January 26 2001, *Certificate Issuing and Management Components Protection profile*, http://csrc.nist.gov/pki/documents/CIMC_PP_final-corrections_20010126.pdf, s. 2, s.8, s.9

[36] ÖZYILMAZ Ayşe, EVSENAL Saliha, Ağustos-Eylül 2000, Elektronik İmza s. 28.

[37] Tursign TK E-İmza Paneli, 02 Eylül 2003, Dijital Sertifikalar ve Dijital İmzalar s.13, s.14

[38] http://www.digsigtrust.com/support/pki_basics.html

[39] BOZKURT Veysel, Ekim 1999, Yöneticilerin Elektronik Ticaretin Geleceğine Dair Görüşleri, Uludağ Üniversitesi İktisadi İdari Bilimler Fakültesi Dergisi, Cilt 17, Sayı:3

[40] LAIH Chi Sung, 2000, The Developing Process and Future Plan of PKI in R.O.C., s.5

[41] DIFFIE W., HELLMAN M.E., 1976, New Directions in Cryptography, IEEE Transactions onInformation Theory, v. IT-22, n. 6, pp. 644-654.

[42] OECD,1998, The role of telecommunications and information Infrastructures in advancing electronic commerce,Background Paper for the OECD Ottawa Ministerial Conference "A BorderlessWorld: Realising the Potential of Global Electronic Commerce, s.2-5

[43] LOPEZ Lourdez, CARRACEDO Justo, 1997, Hierarchical Organisation of Certification Authorities for Secure Environments, EUITT Universitad Politecnica de Madrid, s.8

[44] PKI Forum, November 2002, Basics-A technical perspective s. 1-4

[45] CEN/ISSS Workshop on Electronic Signatures (WS/E-Sign), December 6 2000, Draft CWA "Procedures for electronic signature Verification, s.2, s.4

[46] http://www.regtp.de

[47] Telecom Flash, July 2000, Digital signatures on the move, s.1-2

[48] http://www.ict.etsi.fr/EESSI/EESSI-homepage.htm

[49] http://www.cenorm.be

[50] Danish Bill on Electronic Signatures, 29 March 2000, Bill No. L 229

[51] SMENDING HOFE Thomas - BRO Ruth Hill, 1999, Moving with Change: Electronic Signature Legislation as a Vehicle for Advancing E- commerce., Journal of Computer a Information Law, vol. XVII, no. 3, p. 732-733.

[52] Official Journal of the European Communities, 19.01.2000, Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

[53] http://www.signatur.rtr.at/en/links/index.html

[54] [25] European Commssion, 2002, Europe+ Progress Report

[55] ITU, 1999, Colloquium No.8: Telecommunications regulatory issues for electronic commerce, s. 12, s.16, s.22

[56] MANN Catherine L., ECKERT Sue E., KNIGHT Cleeland, July 2000, Global Electronic Commerce: A policy Primer,s.144

[57] http:www.iee.com

[58] http://www.itu.int

[59] http://www.unctad.org

[60] UNICE Benchmarking Raporu, 2001, Yeni*lenen* Ekonomi, MESS Yayını, No:357, s.13, s.15, s.16

[61] Report of the Electronic Commerce Expert Group to the Attorney General, 31 March 1998, Australia Electronic Commerce: Building the Legal Framework, s. 9, s.12

[62] ITU, 1999, Colloquium No.8: Telecommunications regulatory issues for electronic commerce, s.22, s.29, s.38, s.46

[63] MANN Catherine L, March 2000, Electronic Commerce in Developing Countries' Issues for Domestic Policy and WTO Negotiations, Institude for International Economics, s.2, s.3

[64] James JOHNSON, Marc 1998, Electronic Commerce and the Global Marketplace-Report on International Organizations Activities, http:/www.nii.nist.gov/pubs/ecgm-jj.htm, s.1, s.2

[65] UNCTAD, 2000, Building Confidence Electronic Commerce and Development, s.5-8

[66] http://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm

[67] ITU, 14-16 December 1998, Chairman's Report of the Eighth Regulatory Colloquium Telecommunications Regulatory Issues for Electronic Commerce, s.4, s, 12, s.22

[68] ETKK Teknik Çalışma Grubu Değerlendirme Raporu, Mayıs 1998, s. 4.

[69] A European Initiative in Elektronic Commerce, the Commission of the Europen Communities, http://wwwcordis.lu, s.1

[70] http://www.europa.eu.int/scadplus/leg/en/lvb/l24221.htm

[71] European Commission, 23-24 March 2000, eEurope An Information Society for all Progress report, Lisbon, s.3, s.8

[72] European Commission, 2002, Europe+ Progress Report, s.2, s.5

[73] http://www.cordis.lu/esprit/src/ecomcom3.htr

[74] BOZKURT Veysel, Ekim 1999, Yöneticilerin Elektronik Ticaretin Geleceğine Dair Görüşleri, Uludağ Üniversitesi İktisadi İdari Bilimler Fakültesi Dergisi, Cilt 17, Sayı:3

[75] KIONG Liew Voon, 2000, The Prospect of E-commerce for the Small and Medium Enterprises in Malaysia Thesis report 2000, s.10

[76] Official Journal of the European Communities, 22 May 2001, Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, s.2-4

[77] Official Journal of the European Communities, 07.06.2000, Proposal for a Regulation of the European Parliament and of the Council Amending Regulation (EEC) No 218/92 on Administrative Co-operation in the Field of Indirect Taxation (VAT), s.1-4

[78] Official Journal of the European Communities, 27.10.2000, Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions, s.2-5

[79] Official Journal of the European Communities, 27.10.2000, Directive 2000/28/EC of the European Parliament and of the Council of 18 September 2000 Amending Directive 2000/12/EC Relating to the Taking up and Pursuit of the Business of Credit Institutions, s.2-4

[80] Official Journal of the European Communities, 17.07.2000, Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market (Directive on electronic commerce), s.2-4

[81] Official Journal of the European Communities, 05.08.1998, Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 Amending Directive 98/34/EC Laying Down a Procedure for the Provision of Information in the Field of Technical Standards and Regulations, s.1-4

[82] Commission Recommandation, 30 July 1997, Transactions by Electronic payment instruments and in particular the relationship between issuer and holder (Text with EEA relevance) (97/489/EC), s.1-3

[83] Official Journal of the European Communities, 11 March 1996, Directive of the European Parliament of the Council on the Legal Protection of Databases, s.1-4

[84] Official Journal of the European Communities, 24 October 1995, The Data Protection Directive EU Directive 95/46/EC , s.1-4

[85] İTO, 1998, Bilgi Ekonomisinde Elektronik Ticaret s.142

[86] http://www.bmck.com/ecommerce/uncitral-t.htm

[87] National Institute of Standards and Technology, January 26 2001, Certificate Issuing and Management Components Protection profile, http://csrc.nist.gov/pki/documents/CIMC_PP_final-corrections_20010126.pdf, s. 7-13, s. 15, s. 22, s.18

[88] OECD, April 2002, Policies and institutions for e-commerce readiness: what can developing countries learn, s.2

[89] OECD, 2002, Information Technology Outlook 2002, s.2-9

[90] OECD, 12-13 October 1999, Forum on Electronic Commerce Revised Report on International and Regional Bodies:Activities and Initiatives in Electronic Commerce, s.3-5

[91] http://www.wipo.org/cfdiplaw/en/trips/

[92] CANPOLAT Önder, Mart 2001, E-Ticaret ve Türkiye'deki gelişmeler T.C. Sanayi ve Ticaret Bakanlığı Hukuk Müşavirliği, s.15

[93] OECD, 2001, Policy Brief on e-commerce, s.9

[94] ÇAMURDAN Çiğdem, 26.05.2003, Elektronik İmza Kanunu Üzerine bir Değerlendirme, TBD, s.1

[95] http://www.e-ticaret.gov.tr

[96] CSI Electronic Commerce, 1998, Information Technology& Telecommunications Working Group Recommendations on Electronic Commerce Electronic Commerce Recommendations, http://www.ftc.gov/bcp/icpw/comments/csi.htm, s.9

[97] HIRAMATSU Yuichi, September 2000, Electronic Commerce Trend and Future OKI Technical Review p.183

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

[99] http://www.regtp.de

[100] http://www.signatur.rtr.at/en/index.html

[101] Ausralian Signature Order, 2 February 2000, SigV pursuant to § 25 of the Signature Law

[102] http://www.ficora.fi/englanti/tietoturva/allekirjoitus.htm

[103] Ficora, 29 January 2003, Regulation on certification Authorities' obligation to notify Ficora, issued in Helsinki

[104] Ficora, 29 January 2003, Regulation on the requirements for reliability and information security in the operation of certification authorities providing qualified certificates

[105] http://www.tst.dk/mainpage.asp

[106] Danish Bill on Electronic Signatures, 29 March 2000, Bill No. L 229

[107] Danish Executive Order, 5 October 2000, Reporting of Information to the National Telecom Agency by Certification Authorities and System Auditors, Executive Order No. 922

[108] http://www.dti.gov.uk/

[109] http://www.tscheme.com/

ÖZGEÇMİŞ

1974 yılında Diyarbakır'da doğdu. İlköğrenimini Batman'da orta ve lise öğrenimini İstanbul'da tamamladı. 1997 yılında Hacettepe Üniversitesi Fizik Mühendisliği Bölümünden mezun oldu. 1998 yılında Telsiz Genel Müdürlüğü Standartlar Daire Başkanlığı'nda göreve başladı. Yüksek lisansını Ortadoğu Teknik Üniversitesi Fizik Bölümü'nde Aralık 2001'de tamamladı. Halen Uluslararası İlişkiler ve AB ile Koordinasyon Dairesinde çalışmakta olup iyi derecede İngilizce bilmektedir.