T.C.
İSTANBUL AYDIN ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME ANABİLİM DALI
UZAKTAN EĞİTİM İŞLETME BİLİM DALI

# ELEKTRONİK TİCARET GÜVENLİĞİNE BAKIŞ VE ÖNERİLER

Yüksek Lisans Projesi

**Serdar KUT**

İstanbul, 2011

T.C.
İSTANBUL AYDIN ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME ANABİLİM DALI
UZAKTAN EĞİTİM İŞLETME BİLİM DALI

# ELEKTRONİK TİCARET GÜVENLİĞİNE BAKIŞ VE ÖNERİLER

Yüksek Lisans Projesi

**Serdar KUT**

**Danışman: Yrd.Doç.Dr. A.İhsan ÖZEROĞLU**

İstanbul, 2011

# ÖZET

Son yıllarda internetin yaygınlaşmasına paralel olarak hızla büyüyen ve her geçen gün hayatımıza daha çok giren elektronik ticaretin sağladığı kolaylıklar saymakla bitmez. Ancak internet gibi, tüm dünyaya açık bir ortamda e-ticaret yapmak, bazı güvenlik risklerini de beraberinde getirmektedir.

Bu çalışmada, İnternet üzerinden e-ticaretin daha güvenli bir yapı üzerinden sağlanmasına yönelik bir güvenlik modeli tasarlanmıştır.

**Anahtar Kelimeler:** E-Ticaret, E-Ticaret Güvenliği, E-Ticaret Alternatif Bilgi Güvenliği

## ABSTRACT

E-Commerce, growing rapidly in recent years in parallel with the expansion of the Internet and coming more into our lives every day, provides countless benefits. However, making e-commerce in an open environment like Internet brings some security risks.

In this study, a secure model is designed to provide a more secure structure for e-commerce over Internet.



**Keywords:** E-Commerce, E-Commerce Security, Alternative E-Commerce Data Security

# ÖNSÖZ

Proje çalışmamda bana destek olan saygı değer danışmanım Yrd. Doç. Dr. A.İhsan ÖZEROĞLU'na teşekkürü bir borç bilirim.

Proje hazırlama süreci boyunca bana her an destek olup, güç veren çalışma arkadaşım Zehra TURHAN'a her şey için çok teşekkür ederim.

Bu projede koyu punto ile yazılmış kısımlar kendi yorum, görüş ve önerilerimdir.

Serdar KUT
Nisan 2011
İSTANBUL

# İÇİNDEKİLER

## ŞEKİLLER DİZİNİ

# ELEKTRONİK TİCARET GÜVENLİĞİNE BAKIŞ VE ÖNERİLER

## 1. ELEKTRONİK TİCARETİN TANIMI VE KAPSAMI

**Günümüzde elektronik ortamda gerçekleştirilen işlemlerin başında genellikle "e" harfini görmekteyiz. "Elektronik" ya da İngilizce "Electronic" sözcüğünün baş harfini temsilen kullanılan bu ön ek, son yıllarda sıklıkla karşımıza çıkmaktadır. E-ticaret de bu şekilde karşımıza çıkan kavramlardan bir tanesidir. Genel olarak E-ticaret, pazarlama ve sipariş aktiviteleri de dahil olmak üzere, mal ya da hizmetin alım ve satımının elektronik ortamda yapıldığı bir ticaret türü olarak tanımlanabilir.**

E-ticaret ile ilgili olarak bu alanda faaliyet gösteren bazı organizasyonlarca yapılmış tanımlamalar da aşağıdaki gibidir.

WTO'nun (Dünya Ticaret Örgütü) tanımına göre; E-ticaret, mal ve hizmetlerin üretim, reklam, satış ve dağıtımlarının telekomünikasyon ağları üzerinden yapılmasıdır.[1]

OECD'nin (Ekonomik İşbirliği ve Kalkınma Teşkilatı) tanımına göre; E-ticaret, kurumların ve bireylerin katıldığı ve metin, ses ve görsel imaj gibi sayısallaştırılmış verinin işlenerek, açık veya kapalı ağlar üzerinden iletilmesine dayanan ticaretle ilgili işlemlerdir.[2]

UN-CEFACT (Birleşmiş Milletler İdari, Ticari ve Ulaşımla İlgili Uygulama ve Usulleri Kolaylaştırma Merkezi) ise e-ticareti: "İş, yönetim, ve tüketim faaliyetlerinin yürütülmesi için, yapılanmış (structured) ve yapılanmamış (unstrucred) iş bilgilerinin; üreticiler, tüketiciler ve kamu kurumları ve diğer organizasyonlar arasında elektronik araçlar (Elektronik posta ve mesajlar, elektronik bülten panoları), www (word wideweb)

[1] WTO Special Report 2, Electronic Commerce and the Role of the WTO , (1998), http://www.wto.org/english/res_e/booksp_e/special_study_2_e.pdf

[2] Hakan UZUNOĞLU, Elektronik Ticaretin Vergilendirilmesinin İncelenmesi ve Değerlendirilmesi, (2002), Ankara

teknolojisi, akıllı kartlar, elektronik fon transferi, elektronik veri değişimi üzerinde paylaşılmasıdır." şeklinde tanımlamıştır.[3]

UNCITRAL (BM- Uluslararası Ticaret Hukuku Komisyonu) e-ticareti, ticari aktiviteler kapsamında her türlü veri mesajının, EDI (Electronic Data Interchnge), internet, e-mail gibi yöntemlerin yanında, telekopi ve fax gibi daha az karmaşık veri iletim yöntemleri kullanılarak elektronik ortamda değişimi olarak tanımlanmıştır.[4]

**Elektronik Ticaret, ürün veya hizmet satın alışverişi faaliyetinin haberleşme ağları yardımıyla yapılabilmesini sağlamaktadır. Bununla birlikte, sunulan ürün veya hizmet için talep yaratılmasının, müşteri desteği verilmesinin ve lojistik işlemlerinin takibinin de yine haberleşme ağları yardımıyla yapılması söz konusudur. Elektronik Ticaret, sunulan ürün ve hizmetlere, internetin yaygınlığına bağlı olarak, dünyanın hemen hemen her yerinden hızlı ve kolay erişim imkanı sağlamaktadır.**

**Elektronik iletişim teknolojilerinin gelişimiyle, ticarette kullanımı aslında paralellik göstermektedir. 1980'lerinden bu yana gelişen iletişim teknolojileriyle birlikte ortaya çıkan kolaylıklar, ticarete yansımış ve ticareti kolaylaştırmıştır. Devamında, iletişim teknolojilerinin ticarette kullanımının daha da arttığı yıllarda, internetin de daha yaygın ve daha fazla kullanılan bir ticaret ortamı haline geldiğini ve bu şekilde büyüdüğünü görüyoruz. Özellikle web ve elektronik posta servislerinin sağlanması, internet üzerinde ticaretin gelişmesinde büyük rol oynamıştır. Sunulan bilgi, mal ya da servislerin, konuma bağlı olmaksızın her an erişilebilir olmasını sağlayan web siteleri, ticaret için bulunmaz bir sanal pazarlama yeri olarak yerini almaya başlamıştır. Örnek olarak www.ebay.com, www.amazon.com, www.yahoo.com gibi web sayfaları verdikleri bu servisle çok kısa sürede birer büyük şirket haline gelmişlerdir. Yine elektronik postanın yeni bir iletişim kanalı olarak yaygınlaşmasıyla beraber, elektronik ticarette sipariş**

[3] Oğuz Kara, Elektronik Ticaretin Dış Ticaret İşlemlerinde Uygulanması ve Bilgisayarlı Gümrük Etkinlikleri (BİLGE) Sisteminin Verimliliğinin Değerlendirilmesi, (2002), Kütahya

[4] Hakan UZUNOĞLU, Elektronik Ticaretin Vergilendirilmesinin İncelenmesi ve Değerlendirilmesi, (2002), Ankara

**verme, elektronik fatura, satış öncesi ve sonrası destek gibi alanlarda kullanılmış ve büyük kolaylık sağlamıştır.**

**Elektronik Ticaretin kapsamı, bilgi ve iletişim teknolojilerinin sunduğu servisleri kullanabilmeyle doğru orantılı olarak gelişen bir olgu olarak görülmektedir. Mevcut teknolojik imkanların, yeni e-ticaret fikirleriyle birleştirilmesi sonucunda gelişen bir kapsam söz konusu olduğundan, tarif yapılırken bir sınır çizilmesi mümkün olamamaktadır.** Ancak günümüz teknoloji şartlarında, e-ticaret kapsamındaki uygulamalara göz atacak olursak[5];

- Mal (taşınır, taşınmaz) ve hizmetlerin (bilgi servisleri, danışmanlık,finans, hukuk, sağlık, eğitim, ulaştırma, vb.) elektronik alışverişi,

- Üretim planlaması yapma ve üretim zinciri oluşturma,

- Tanıtım, reklam ve bilgilendirme,

- Sipariş verme,

- Anlaşma yapma,

- Elektronik banka işlemleri ve fon transferi,

- Elektronik konşimento gönderme,

- Gümrükleme,

- Elektronik ortamda üretim izleme,

- Elektronik ortamda sevkiyat izleme,

- Ortak tasarım geliştirme ve mühendislik,

- Elektronik ortamda kamu alımları,

- Elektronik Para ile ilgili işlemler,

[5] Hakan UZUNOĞLU, Elektronik Ticaretin Vergilendirilmesinin İncelenmesi ve Değerlendirilmesi ,(2002), Ankara

- Elektronik hisse alışverişi ve borsa,

- Ticari kayıtların tutulması ve izlenmesi,

- Doğrudan tüketiciye pazarlama,

- Sayısal imza, elektronik noter vb. Güvenilir Üçüncü Taraf (TTP) işlemleri,

- Sayısal içeriğin anında dağıtımı,

- Anında bilgi oluşturma ve aktarma,

- Elektronik ortamda vergilendirme,

- Fikri mülkiyet haklarının transferi.

## 2. E-TİCARET ÇEŞİTLERİ

E-ticaret, gerçekleşme şekline, dayandığı ortama ve katılımcılarına göre çeşitlendirilebilir.[6]

### 2.1. Gerçekleşme Şekline Göre

**Gerçekleşme şekline göre bakıldığında, yapılan ticari alışverişin hangi safhalarının elektronik ortamda gerçekleştirildiğine göre çeşitlendirme yapılabilir.** Bir malın veya hizmetin satışı veya alımı sırasında stok bilgisinin sorgulanması, siparişin verilmesi, ödemesinin yapılması ve tesliminin gerçekleşmesi süreci e-ticaret kapsamında düşünülse de, satılan hizmet ya da malın niteliğine göre bu süreç bazı noktalardan elektronik ortam dışına çıkılmasını zorunlu kılabilir. Bu noktada daha doğru bir çeşitleme yapabilmek için öncelikle malın ya da hizmetin sınıflandırılması gerekmektedir.[7]

Elektronik ticaret yardımıyla elektronik ortamda satılan ya da alınan bir mal veya hizmetler, müşteriye iletim yöntemi noktasında farklılık gösterir.[8] Buna göre, elektronik ortamda satın alınan bazı malların müşteriye teslimi fiziksel olarak gerçekleştirilmesi gerekir. Örneğin elektronik ortamda satın alınan bir dizüstü bilgisayarın, gerekli paketlemeleri yapıldıktan sonra alıcısına teslim edilmesi gerekmektedir. Öte yandan bazı malların dağıtımı için de elektronik ortam kullanılabilir. Bu tür mal ya da hizmetler daha çok sayısal ürünler olarak anılmaktadır.[9] **Örneğin, elektronik ortamda satın alınan bir elektronik kitap, yine elektronik posta ile alıcısına iletilebilir. Benzer şekilde elektronik posta, sesli konferans ve video konferans gibi yöntemler kullanılarak alınan danışmanlık ve destek servisleri elektronik ortamda dağıtımı mümkün olan hizmet/mal kategorisinde düşünülebilir.**

### 2.2. Dayandığı Ortamın Niteliğine Göre

E-ticaretin dayandığı ortamın niteliğine baktığımızda ise açık ve kapalı

[6] Oğuz Kara, Elektronik Ticaretin Dış Ticaret İşlemlerinde Uygulanması ve Bilgisayarlı Gümrük Etkinlikleri (BİLGE) Sisteminin Verimliliğinin Değerlendirilmesi, (2002), Kütahya
[7] Arvind Panagariya, E-Commerce,WTO and Developing Countries, (2000), New York
[8] Arvind Panagariya, E-Commerce,WTO and Developing Countries, (2000), New York
[9] Oğuz Kara, Elektronik Ticaretin Dış Ticaret İşlemlerinde Uygulanması ve Bilgisayarlı Gümrük Etkinlikleri (BİLGE) Sisteminin Verimliliğinin Değerlendirilmesi, (2002), Kütahya

sistemler olmak üzere 2 farklı opsiyon görmekteyiz. [10]

### 2.2.1. Açık Sistem

Açık sistem denildiğinde, ticaret ortamının herkese açık ve erişilebilir olduğu bir yapıdan söz edilmektedir. Örneğin internet, erişim bakımından bir kısıtlama getirmediğinden açık sistemlere örnek olarak verilebilir. [11]

### 2.2.2. Kapalı Sistem

Kapalı sistem ise, erişimin belli kısıtlar dahilinde yapıldığı, her kullanıcıya açık olmayan bir yapı belirtilmektedir.[12] **Kapalı sistemlere örnek olarak iki şirket arasında kiralık devre kullanılarak kurulmuş bir ağ yapısı örnek verilebilir. Yanlızca bu ağa dahil olan şirket kullanıcılarının ağı kullanabilir ve dolayısıyla bu yapı, kapalı sistemler için güzel bir örnektir.**

Elektronik ortamda ticaretin yapılabilmesine olanak sağlayan yapı ise EDI (Electronic Data Interchange)'dir. 1970'li yıllarda geliştirilmeye başlanmış EDI, farklı şirketler arası data haberleşmesi için arayüz sağlamıştır. Son yıllarda internetin yaygınlaşmasıyla birlikte EDI, şirketleri internet üzerinden ticaret yapmasına olanak sağlayan bir yapı olarak gelişmeye devam etmiştir.[13]

## 2.3. Katılımcılarına Göre

Son olarak e-ticaret'in katılımcılarına göre ne şekilde sınıflandırıldığına bakacak olursak 4 farklı tür görmekteyiz. Bunlar işletme-işletme arası, işletme-tüketici arası, işletme-devlet ve tüketici-devlet arası e-ticarettir.[14]

---

[10] Oğuz Kara, Elektronik Ticaretin Dış Ticaret İşlemlerinde Uygulanması ve Bilgisayarlı Gümrük Etkinlikleri (BİLGE) Sisteminin Verimliliğinin Değerlendirilmesi, (2002), Kütahya

[11] Oğuz Kara, Elektronik Ticaretin Dış Ticaret İşlemlerinde Uygulanması ve Bilgisayarlı Gümrük Etkinlikleri (BİLGE) Sisteminin Verimliliğinin Değerlendirilmesi, (2002), Kütahya

[12] Hakan UZUNOĞLU, Elektronik Ticaretin Vergilendirilmesinin İncelenmesi ve Değerlendirilmesi ,(2002), Ankara

[13] Zeynep BEİGH, B2B E-Ticaret İşletme Kavramı ve B2B İşletmelerde Konumlandırma Stratejileri,(2010), İstanbul

[14] Hakan UZUNOĞLU, Elektronik Ticaretin Vergilendirilmesinin İncelenmesi ve Değerlendirilmesi ,(2002), Ankara

### 2.3.1. İşletmeler Arası E-Ticaret

Firmalar arasındaki iş uygulamalarını internet ortamında destekleyen faaliyetlerdir. Bir diğer ifade ile şirketlerin ürün ve/veya hizmetlerin alım-satımına ilişkin iş ve işlemlerinin bir çoğunu internet üzerinde gerçekleştirmeleridir.[15] **Online stok takibi, sipariş verme, ürün yada hizmete ilişkin satış öncesi ve sonrası desteği elektronik ortam üzerinden sağlamak, iş akışına önemli ölçüde katkı sağlayarak maliyetleri düşürmekte ve firmanın karlılığını arttırmaktadır. İşletmeler arası e-ticaret geçmiş yıllarda daha çok kapalı ağlar üzerinden EDI ile yapılmaktaydı. Ancak internetin gelişimi ve yaygınlaşması sonucu açık sisteme geçişler artmıştır.**

### 2.3.2. İşletme Tüketici Arası E-Ticaret

Son tüketiciye yönelik olarak şirketlerin ürün ve hizmetlerinin satışına ilişkin internet ortamında yürüttükleri ticari faaliyetlerdir.[16] İşletmeler pazarlamak istedikleri malın yada hizmeti tanıtan bir web sitesi yada sanal ortam oluşturarak bu işlemi gerçekleştirir. E-ticaretin gelişmeye başladığı yıllarda bu tür ticaret, internetin kullanımının yaygın olmaması, işletmelerin potansiyeli görememesi, son kullanıcının internet üzerinden alışverişe sıcak bakmaması gibi sebeplerden dolayı daha az tercih ediliyordu. Ancak internet kullanımının artmasına ve e-ticaret güvenliğinde belli seviyelere gelinmesine paralel olarak işletme-tüketici arasındaki e-ticaret de hızla artmıştır. BKM'nin yaptığı bir araştırmaya göre ülkemizde e-ticaret'de kullanılan kredi kartı (yerli ve yabancı kartların yurtiçi harcamaları) harcamaları 2005 yılında 1.388,39 milyon TL, 2006 yılında 2.412,8 milyon TL, 2007 yılında 5.537,17 milyon TL, 2008 yılında 9.088,68 milyon TL, 2009 yılında ise 10.273,68 milyon TL'ye ulaşırken 2010 yılı ilk üç çeyrek toplamı şimdiden 12.531,87 milyon TL seviyelerine çıkmıştır.[17] **Buradan da anlaşılacağı gibi işletme-tüketici arasındaki e-ticaret hacmi her geçen yıl hızla artmaktadır.**

[15] Dış Ticaret Müsteşarlığı, İhracatı Geliştirme Etüd Merkezi, B2B e-Ticaret ve e-Pazaryerleri, (2008), Ankara
[16] Dış Ticaret Müsteşarlığı, İhracatı Geliştirme Etüd Merkezi, B2B e-Ticaret ve e-Pazaryerleri, (2008), Ankara
[17] Pelin KABALAK, BKM, Türkiye E-Ticaret Pazarı, (2010)

### 2.3.3. İşletme-Devlet Arası E-Ticaret

İşletme-Devlet arasındaki e-ticaret ise işletmelerin kamu işlemlerini elektronik ortamda gerçekleştirilmesi olarak tanımlanabilir.[18] Örneğin şirketlerin vergilerini elektronik ortam kullanarak ödemeleri buna bir örnek olarak verilebilir. Ayrıca kamu ihalelerinin elektronik ortama taşınması ve başvuruların da yine elektronik ortam üzerinden kabul edilmesi de bu tür ticaretin ilk uygulamalarındandır.[19] **E-devlet kavramının genişlemesiyle birlikte, işletme ile devlet arasındaki ticaret daha aktif şekilde elektronik ortama taşınacaktır. Bu da ticaret işlemlerini kolaylaştırarak işletmelerin devlet ile olan ilişkilerini daha düzenli hale getirecektir.**

### 2.3.4. Tüketici-Devlet Arası E-Ticaret

Tüketici-Devlet arası e-ticaret türünde ise tüketicinin devlet ile olan ilişkilerinin elektronik ortamda yürütülmesi söz konusudur. Örneğin taşıt vergisinin internet üzerinden ödenmesi ya da pasaport/ehliyet başvurularının internet üzerinden yapılması bu kategoride değerlendirilebilir.[20] **Burada tüketicinin elektronik ortamı kullanarak işlemlerini yapması yine e-devletin gelişimiyle paralel olarak artacaktır. Yapılan işlemi ciddi manada kolaylaştırdığı düşünülürse ilişkilerin elektronik ortama geçirilmesi, vergi kaybının önlenmesi, devlet dairelerinde uzun kuyrukların son bulması ve daha dinamik bir yapının sağlanması bakımından oldukça önem arz etmektedir.**

[18] Oğuz Kara, Elektronik Ticaretin Dış Ticaret İşlemlerinde Uygulanması ve Bilgisayarlı Gümrük Etkinlikleri (BİLGE) Sisteminin Verimliliğinin Değerlendirilmesi, (2002), Kütahya

[19] Hakan UZUNOĞLU, Elektronik Ticaretin Vergilendirilmesinin İncelenmesi ve Değerlendirilmesi ,(2002), Ankara

[20] Hakan UZUNOĞLU, Elektronik Ticaretin Vergilendirilmesinin İncelenmesi ve Değerlendirilmesi ,(2002), Ankara

## 3. E-TİCARET'DE KULLANILAN ARAÇLAR

Genel olarak elektronik ticaretin yapılışı sırasında bir çok farklı araç kullanılabilir. **Ticaretin yapıldığı ortamdan, ticareti yapan tarafların konumlarına, kullanılacak aracın yaygınlığından güvenilirliğine kadar bir çok kriter uygun aracı belirlemede önemli rol oynar.** Bu araçlar şu şekilde sıralanabilir: Telefon, faks, televizyon, elektronik ödeme, para transferi ve internet.[21] Ancak günümüzde e-ticaret daha çok internet üzerinden yapılmaktadır. Aynı arayüz ile kitlelere hitap ediyor olması, ses görüntü ve yazılı bilginin interaktif olarak iletilebilmesi, zaman ve mekan sınırının olması internetin en çok kullanılan e-ticaret aracı olmasında önemli rol oynamaktadır. [22]

E-ticaret araçlarını aşağıdaki başlıklar altında inceleyebiliriz:

### 3.1. Klasik Elektronik Ticaret Araçları

**Klasik e-ticaret araçlarına bakıldığında, hemen hemen hepsinin bir kısıtlı olduğunu görüyoruz.** Örneğin telefonla e-ticaret, ses iletiminin sorunsuz sağlanabileceği ancak görselliğin olmadığı bir araç olduğundan kullanımı bir çok mal yada hizmette yeterli olmamaktadır.[23] Yine klasik elektronik ticaret araçlarından olan faksın kullanımında ise kısmi görsellik söz konusudur ancak sesli iletişim mümkün olamamaktadır. Her ne kadar hızlı ve yaygın bir araç olsa da elektronik posta gibi bir rakip karşısında pek fazla kullanılacağı düşünülemez. E-ticarette televizyonun kullanılması da yaygın olması bakımından büyük kitlelere ulaşan bir araç olarak düşünülebilir. Ancak iletişimin tek yönlü olması, sipariş ve ödeme aşamalarında farklı araçların kullanılacağı anlamına gelmekte ve giderek daha az kullanılmaya başlamaktadır.[24]

[21] Okşan KÖMÜRCÜ, Elektronik Ticaret Kavramı, Kapsamı ve Araçları, (2005), http://www.hukuki.net/hukuk/index.php?article=261
[22] WTO Special Report 2, Electronic Commerce and the Role of the WTO , (1998), http://www.wto.org/english/res_e/booksp_e/special_study_2_e.pdf
[23] WTO Special Report 2, Electronic Commerce and the Role of the WTO , (1998), http://www.wto.org/english/res_e/booksp_e/special_study_2_e.pdf
[24] WTO Special Report 2, Electronic Commerce and the Role of the WTO , (1998), http://www.wto.org/english/res_e/booksp_e/special_study_2_e.pdf

## 3.2. İnternet

İnternet genel olarak ağların küresel ağı (global network of networks) olarak tanımlanmaktadır.[25] Tanımdaki "global" kelimesini irdeleyecek olursak; bu ağa bağlı dünya üzerindeki herhangi iki bilgisayarın birbiri ile haberleşmesinin mümkün olduğunu görebiliriz. [26] **Bu teknolojik imkan e-ticaret gözüyle yorumlandığında ise sanal ortamda tüm dünyaya açık bir Pazar yeriniz olabileceği anlamına gelir. Bir diğer önemli nokta ise bu pazara zaman sınır olmadan herhangi bir anda erişilebilinmesidir. Maliyet açısından bakıldığında ise gün geçtikçe daha düşük bedellerle bu sanal Pazar yerini çalışır tutmak mümkündür. Tüm bu avantajlarıyla birlikte hem sesli hem de görsel iletişime olanak tanıması ve her geçen gün daha da yaygınlaşması, interneti günümüzde en çok kullanılan e-ticaret aracı haline getirmiştir. Ancak internetin bir açık sistem olması beraberinde bir takım güvenlik sorunlarını da getirmektedir. İlerleyen bölümde bu güvenlik sorunları için şu an kullanılan yöntemleri inceleyecek ve nasıl geliştirmeler yapılabileceği konusu irdelenecektir.**

## 3.3. İntranet

İntranet, sadece belirli bir kuruluş içindeki bilgisayarları, yerel ağları (LAN; Local Area Network) ve geniş ağları (WAN; Wıde Area Network) birbirine bağlayan, çoğunlukla TCP/IP tabanlı ağlar olarak tanımlanmaktadır.[27] **Yani aslında dış dünyaya kapalı, işletme içi haberleşme ağını ifade eder. Bu açıdan bakıldığında bir şirket içindeki bir kısım ticari faliyetlerin bu haberleşme ağı kullanılarak yapılması bir çok kolaylık sağlar.**

## 3.4. Extranet

Extranet, kapalı bir internet ağını, organizasyonun dışında yer alan ve sistemden bilgi almaları gereken müşterileri ve iş yapılan diğer kişi ve kuruluşları da

[25] Oğuz Kara, Elektronik Ticaretin Dış Ticaret İşlemlerinde Uygulanması ve Bilgisayarlı Gümrük Etkinlikleri (BİLGE) Sisteminin Verimliliğinin Değerlendirilmesi, (2002), Kütahya
[26] WTO Special Report 2, Electronic Commerce and the Role of the WTO , (1998), http://www.wto.org/english/res_e/booksp_e/special_study_2_e.pdf
[27] Oğuz Kara, Elektronik Ticaretin Dış Ticaret İşlemlerinde Uygulanması ve Bilgisayarlı Gümrük Etkinlikleri (BİLGE) Sisteminin Verimliliğinin Değerlendirilmesi, (2002), Kütahya

bağlayacak şekilde tamamlayan sınırlı bir erişim ağıdır.[28] **Genellikle tedarikçi şirketlerin stok kontrolü ve iş tabiki amacıyla kullandıkları bir yapı olarak örneklendirilebilir.**

### 3.5. EDI

EDI e-ticaret yapan öğeler arasında bir arayüz oluşturarak bu işlemlerin en az hatayla ve seri şekilde yapılmasını sağlayan bir yapı olarak karşımıza çıkmaktadır. [29] **Getirdiği büyük kolaylıklar sebebiyle e-ticaretin gelişiminde büyük rol oynamış ve günümüzde de bu katkıyı sürdürmeye devam etmektedir.**

### 3.6. Mobil Sistemler

Mobil sistemler günümüzde e-ticarette çok önemli bir araç olarak karşımıza çıkmaktadır. Mobilite' nin getirdiği konum bağımsızlığı avantajıyla, internete yüksek hızlarla bağlanmak, bu aracın e-ticaret için önemini açıkça göstermektedir.[30] **Son yıllarda ülkemizde de yaygın olarak kullanılmaya başlayan 3G teknolojisi ile internete Megabit seviyelerinde bağlantı mümkün olabilmektedir. Böylece internetteki e-ticaret pazarına hem görsel hem de sesli olarak ulaşılarak e-ticaret yapılabilmektedir.**

[28] Oğuz Kara, Elektronik Ticaretin Dış Ticaret İşlemlerinde Uygulanması ve Bilgisayarlı Gümrük Etkinlikleri (BİLGE) Sisteminin Verimliliğinin Değerlendirilmesi, (2002), Kütahya
[29] Arvind Panagariya, E-Commerce,WTO and Developing Countries, (2000), New York
[30] Oğuz Kara, Elektronik Ticaretin Dış Ticaret İşlemlerinde Uygulanması ve Bilgisayarlı Gümrük Etkinlikleri (BİLGE) Sisteminin Verimliliğinin Değerlendirilmesi, (2002), Kütahya

## 4. E-TİCARET'DE ÖDEME ŞEKİLLERİ

E-ticaretin giderek yaygınlaşmasıyla birlikte kullanılan ödeme şekillerinin de çeşitlendiğini görüyoruz. Ancak temel olarak bakıldığında bu çeşitlenmenin kart tabanlı ve ağ tabanlı olmak üzere iki farklı başlık altında dallandığını görüyoruz.[31]

**Kart tabanlı ödemeler, kredi kartları, sanal kredi kartları ve akıllı kartlar aracılığı ile yapılmaktadır. Kredi kartının tüm dünyada standart bir ödeme altyapısına sahip olması ve kullanıcı kitlesinin genişliği, Internet üzerinden yapılan alışverişlerde en çok kullanılan ödeme yöntemi olmasını sağlamıştır.** Alışveriş sırasında kredi kartı bilgilerinin üçüncü şahıslarca ele geçirilmesinin önlenmesi amacıyla bu bilgilerin şifrelenmesi esasına dayanan SSL ve SET protokolleri kullanılmakta, böylece alışveriş güvenliği kolaylıkla sağlanmaktadır.[32]

Ağ tabanlı ödemeye bakıldığında ise elektronik para ve elektronik çek gibi ödeme araçlarının kullanıldığını görüyoruz. Elektronik para Internet'te kullanılmak üzere geliştirilmiş para birimidir.[33] Elektronik para günlük hayatta kullanılan mağaza çeklerinin Internet ortamındaki karşılığı olarak değerlendirilebilir. Bu sistemden yararlanmak isteyen kişilerin ilk olarak elektronik para hizmeti sunan şirketler tarafından geliştirilen özel yazılımlardan birini bilgisayarlarına yüklemeleri ve o şirketle çalışan bir bankada hesap açtırmaları gereklidir. Bundan sonra elektronik para ile anlaşmalı mağazaların sitelerinden veya kendisi gibi elektronik para yazılımını kullanan diğer taraflar ile sanal alışveriş yapabilirler. Elektronik para yazılımı, istenilen miktarda paranın bir banka hesabından çekilerek, Internet üzerinden yapılacak harcamalarda kullanılmak üzere elektronik ortamda saklanmasını sağlar. Her elektronik paranın normal hayatta olduğu gibi bir seri numarası vardır. Internet üzerinden bir harcama yapıldığında belli seri numaralı elektronik paralar alışveriş yapanın bilgisayarından silinerek alışveriş yapılan bilgisayara geçirilir.[34] Bu şekilde, para akışı aynen günlük hayatta olduğu gibi gerçekleştirilir. Türkiye'de bu sistem henüz uygulamaya geçmemiştir. Dünyada

[31] Hakan UZUNOĞLU, Elektronik Ticaretin Vergilendirilmesinin İncelenmesi ve Değerlendirilmesi ,(2002), Ankara
[32] Hilmi KUŞÇU, E-Ticaret: SSL ve SET, (2010)
[33] Halil Elibol, Burcu Kesici, Çağdaş İşletmecilik Açısından Elektronik Ticaret, (2003)
[34] Hakan UZUNOĞLU, Elektronik Ticaretin Vergilendirilmesinin İncelenmesi ve Değerlendirilmesi ,(2002), Ankara

elektronik para hizmeti veren bazı kuruluşlara örnek olarak CyberCash (www.cybercash.com), DigiCash (www.digicash.com) verilebilir.[35]

Elektronik çek, elektronik ticaret gerçekleştiren sitelerin ödemeleri çek olarak kabul etmelerini ve işleyebilmelerini sağlayan bir ödeme sistemidir. Elektronik çek, ABD'de Financial Services Technology Consortium (www.fstc.org) tarafından SDML, Signed Document Markup Language, adı verilen bir işaretleme dili kullanılarak geliştirilmiştir.[36] Elektronik çek sisteminde, ödemeler kredi kartı olmadan banka hesabı bilgilerinin gerekli olanlarının elektronik ticaret sitesine girilmesi yoluyla yapılır. Kullanıcı bir anlamda ticaret sitesine çek keserek ödeme yapmış olur. Bankadaki sistemler yapılan transferleri her gün temizleyerek bahsedilen hesapta alışverişin tamamlanması için gerekli şartların yeterli olup olmadığını kontrol ederler ve bu durumdan elektronik ticaret sitesini şifreli kanallarla haberdar ederler. Bu işlemler takas merkezi olarak adlandırılan finansal kurumlar tarafından da yürütülebilir. Kullanılması kolay bir sistem olmakla birlikte, daha yaygın kullanımı için gerekli sistemlerin finans sektörü tarafından kabul görmesi gereklidir. Bu hizmet ülkemizde herhangi bir kuruluş tarafından henüz uygulamaya konulmamıştır.[37]

Diğer ödeme araçlarından da kısaca bahsetmek gerekirse:

Escrip: Bağış ödemeleri gibi bazı özel düşük miktarlı ödemeler için kurulmuş bir sistem.[38]
IPIN: Internet harcamalarını ISS faturalarına yansıtan bir sistemdir.[39]
PCPay:Smart Card bazlı bir sistemdir.[40]
ECharge My Phone: Telefon faturası ile entegre edilmiş bir sistemdir. Ülkemizde bağış ve çekiliş uygulamalarında bu ödeme türüne sıkça rastlanmaktadır.[41]

[35] Cihad Demirli, E-Ticaret (İlk Adımlar), (2010)
[36] Halil Elibol, Burcu Kesici, Çağdaş İşletmecilik Açısından Elektronik Ticaret, (2003)
[37] Halil Elibol, Burcu Kesici, Çağdaş İşletmecilik Açısından Elektronik Ticaret, (2003)
[38] Hakan UZUNOĞLU, Elektronik Ticaretin Vergilendirilmesinin İncelenmesi ve Değerlendirilmesi ,(2002), Ankara
[39] Hakan UZUNOĞLU, Elektronik Ticaretin Vergilendirilmesinin İncelenmesi ve Değerlendirilmesi ,(2002), Ankara
[40] Hakan UZUNOĞLU, Elektronik Ticaretin Vergilendirilmesinin İncelenmesi ve Değerlendirilmesi ,(2002), Ankara
[41] Hakan UZUNOĞLU, Elektronik Ticaretin Vergilendirilmesinin İncelenmesi ve Değerlendirilmesi ,(2002), Ankara

First Virtual: Ödemeleri üçüncü bir kuruluşun toplayıp, ilgili taraflara dağıtımını yaptığı bir sistemdir.[42]

**Bu ödeme araçlarından dünyada ve ülkemizde en çok kullanılanı kredi kartıdır. Her ne kadar belirli güvenlik standartları oluşturulmuş olsa da, kredi kartıyla internet üzerinden yapılan ödemeler sırasında bir çok güvenlik problemiyle karşılaşılabilmektedir.**

[42] http://www.e-ticaretmerkezi.net/odemearaclari.php , (2010)

## 5. E-TİCARET'DE GÜVENLİK KRİTERLERİ

Elektronik ticarette alıcı ve satıcı birbirlerini görmez. Bu sebeple karşılıklı olarak güvenin sağlanmasına yönelik ek bir takım önlemler almaya ihtiyaç duyarlar. Öncelikle alıcı ve satıcı taraflar birbirlerinin kimliklerinden emin olmak isterler. Aslında bu ihtiyaç, dijital imza ve dijital sertifikaların geliştirilme nedenidir. Bunlar aracılığıyla iki taraf birbirlerinin kimliğinden emin olabilmektedir.[43] **Türkiye'de dijital sertifikalar ile ilgili yasal altyapı henüz oluşturulmadığı için alıcı tarafında bulunan bireysel kullanıcılar henüz dijital sertifika kullanmaya başlamamışlar, satış yapan siteler de müşterilerine bunu şart koşmamışlardır. Bu nedenle satıcılar alıcıların kimliklerini kontrol edememektedirler. Satıcı bu durumda gerek duyarda, kullanıcı bilgileri için bankadan teyit isteyebilmektedir.**

Elektronik ticarette güvenlik konusunda değerlendirilmesi gereken diğer bir konu da alıcıların elektronik ticaret sitelerinden alışveriş yapmak için vermek durumunda kaldıkları kredi kartı vb. bilgilerin Internet üzerinden iletilirken üçüncü şahısların eline geçmesi riskidir. Bilindiği gibi özellikle telefonla yapılan satışlarda (gazeteye ilan vermek, katalog satışları vb) kredi kartı numarası ve son kullanma tarihi alışveriş için yeterli olmaktadır. [44] **Bu yüzden bu bilgilerin korunması elektronik ticaretin gelişimi için büyük önem taşımaktadır.**

[43] Belgin Behram, Aydan Atalay, Çağrı Tanoğlu, Elif Öztürk, a'dan z'ye Elektronik Ticaret, (2001)
[44] http://www.garantiweb.com/ssl.asp?ID=25&PAGE=2, (2010)

# 6. E-TİCARET'DE KULLANILAN GÜVENLİK ARAÇLARI

Elektronik ticarette kredi kartı bilgilerinin başkalarının eline geçme riski günlük hayattakine göre çok daha azdır. Günlük hayatta ödeme yaparken kredi kartı bir başkasına verilmekte, bu yüzden kredi kartının üzerindeki bilgilerin gizliliği büyük oranda ortadan kalkmaktadır. Sanal alışveriş hizmeti veren firmalar, kredi kartı bilgilerinin güvenliği ve gizliliğini sağlamak için yaygın olarak SSL ve SET gibi güvenlik standartlarını kullanmaktadırlar. [45]

SSL (Secure Sockets Layer), ağ üzerindeki web uygulamalarında güvenli bilgi aktarımının temini için (bilginin doğru kişiye güvenli olarak iletimi), "Netscape" firması tarafından geliştirilmiş bir program katmanıdır. Burada, bilgi iletiminin güvenliği, uygulama programı (web browser, HTTP) ile TCP/IP katmanları arasındaki bir program katmanında sağlanmaktadır. SSL, web sunucularına (Apache vb), bir modül olarak yüklenir ve böylece web sunucuları güvenli erişime uygun hale gelir. SSL, hem istemci (bilgi alan) hem de sunucu (bilgi gönderen) bilgisayarda bir doğrulama (authentication, iki bilgisayarın karşılıklı olarak birbirini tanıması) mekanizması kullanır. Böylece, bilginin doğru bilgisayardan geldiği ve doğru bilgisayara gittiği teyit edilir.[46]

Bilgisayarların birbirlerini "tanıma" işlemi, açık-kapalı anahtar tekniğine (public-private key encryption) dayanan bir kripto sistemi ile sağlanır. Bu sistemde, iki anahtardan oluşan bir anahtar çifti vardır. Bunlardan açık anahtar (public key) herkes tarafından bilinebilen ve gönderilen mesajı "şifrelemede" kullanılan bir dijital anahtardır. (Burada anahtar'dan kasıt, aslında bir şifreleme -kriptolama- algoritmasıdır. Bu algoritma (yani, anahtar) kullanılarak gönderilecek bilgi şifrelenir. Ancak, açık anahtar ile şifrelenen mesaj, sadece bu anahtarın diğer çifti olan "kapalı anahtar" (private key) ile açılabilir. Kapalı anahtar da, sadece sizin bildiğiniz bir anahtar olduğundan, mesaj güvenliği sağlanmış olur.[47] **Yapıyı örneklendirmek gerekirse, birbiri ile güvenli olarak haberleşmek isteyen iki istemci olduğunu varsayalım. Bilgiyi alacak olan istemci, gönderecek olan istemciye kendi açık anahtarını (public key) gönderir, gönderecek olan istemci bu anahtarı kullanarak bilgiyi, alacak**

[45] Hilmi KUŞÇU, E-Ticaret: SSL ve SET, (2010)
[46] http://www.eticarethazirla.com/menu-set , (2010)
[47] Hilmi KUŞÇU, E-Ticaret: SSL ve SET, (2010)

**istemciye iletir. Bu bilgi alacak istemcinin açık anahtarı ile şifrelendiğinden ve yalnızca alacak istemcinin kapalı anahtarı (private key) ile deşifre edilebileceğinden, gönderilen bilginin güvenliği sağlanmış olacaktır. Bu yapıda matematikteki tek yölü fonksiyon çeşitleri kullanılmaktadır.**

SSL, web sunucusunu tanımak için, dijital olarak imzalanan sertifikalar kullanır. Sertifika, aslında, o organizasyon hakkında bazı bilgiler içeren bir veri dosyasıdır. Aynı zamanda da, kuruluşun açık-kapalı anahtar çiftinin "açık" anahtarı da sertifika içinde yer alır. Sunucu sertifikası da, o sunucuyu işleten kuruma ait bilgiler içeren bir sertifikadır. Sertifikalar, "güvenilir" sertifika kuruluşları tarafından dağıtılır (VeriSign gibi).[48] İstemci bilgisayar, SSL destekleyen bir sunucuya bağlandığı anda, (bu, https:// ile başlayan URL satırları ile gerçekleşir) doğrulama işlemi başlar. İstemci, kendi açık anahtarını sunucuya gönderir. Sunucu ise, bu anahtarı kullanarak şifrelediği bir mesajı istemciye geri gönderir. Bir sonraki adımda istemci sadece kendinde olan kapalı (private) anahtarı kullanarak gelen şifreli mesajı çözer ve sunucuya geri gönderir. Mesajı alan sunucu ise, bunu kendisinin gönderdiği orijinal mesaj ile karşılaştırır ve eğer iki mesaj "aynı" ise "doğrulama" işlemi başarıyla tamamlanmıştır ve sunucu bu noktadan itibaren "doğru bilgisayarla/kişiyle" iletişimde olduğunu anlar. Daha sonra sunucu istemciye o an gerçekleşen web oturumunda kullanılacak tüm önemli anahtarları gönderir ve güvenli iletişim başlar.[49]

Anahtarlar üretilirken kullanılan bazı popüler algoritmalar olarak, DES (Data Encryption Standard),3DES, AES, RSA, IDEA verilebilir. [50]

SET (secure Electronic Transaction), elektronik ticarette, internet üzerinde güvenli bilgi aktarımını sağlamak amacıyla aralarında VISA, MasterCard ve IBM'in de olduğu kuruluşlar tarafından geliştirilen bir protokoldür. SET, özellikle on-line (gerçek zamanlı) kredi kartı bilgileri iletimi için geliştirilmiş bir standarttır. SET, kredi kartı ile yapılan online ödemelerde, bilgilerin internet üzerinden aktarımında gizlilik ve güvenlik entegrasyonunu sağlar. SET protokolü sadece müşteri (ürün siparişi veren kredi kartı

[48] Hilmi KUŞÇU, E-Ticaret: SSL ve SET, (2010)
[49] Hilmi KUŞÇU, E-Ticaret: SSL ve SET, (2010)
[50] Hasan ÇIRPAN, E-Ticarette Güvenlik, (2005)

sahibi) ile sanal dükkan (e-dükkan) ve kredi kartı şirketi arasındaki ödeme fazını şifreler. [51]

SET ile, ödeme işlemine taraf olan herkes (müşteri, dükkan sahibi, kredi kartı şirketi), birbirlerini tanırlar (teşhis ederler, authentication) ve bu ispatlanabilir. "Tanıma" işlemi, SSL'dekine benzer bir dijital sertifikasyon sistemi ile yapılır. Yani, ödeme fazına dahil bütün taraflar kendi kimliklerini belirten dijital bir sertifika kullanır.[52]

**SSL ve SET uygulamalarının birlikte kullanılması sonucu mevcut durumun en güvenli mekanizması sağlanabilir. Ancak bu mekanizma bile yüzde yüz güvenlik sağlayamayabilir. Gün geçtikçe ortaya çıkan yeni güvenlik açıkları ve farklı siber saldırı yöntemleri sebebiyle bu mekanizma güçlendirilmeli ve güncel tutulmalıdır.**

[51] Ü. Reha Şendil, E-Ticarette Bilgi Güvenliği Terimleri, (2010)
[52] Oğuz Kara, Elektronik Ticaretin Dış Ticaret İşlemlerinde Uygulanması ve Bilgisayarlı Gümrük Etkinlikleri (BİLGE) Sisteminin Verimliliğinin Değerlendirilmesi, (2002), Kütahya

## 7. TSE'NİN BELİRLEDİĞİ GÜVENLİK STANDARTLARI

Ülkemizde TSE'nin e-ticaret için belirlediği bazı standartlar mevcuttur. TSE, e-ticaret esnasında internet üzerinden aktarılan veriyi, e-ticaret verileri ve hassas e-ticaret verileri olmak üzere ikiye ayırmaktadır.[53] Bunlara bakacak olursak;

E-Ticaret Verileri: E-Ticaretin gerçekleşmesi için/sırasında kullanılan veriler:[54]

- Müşteri Adı
- Müşteri Posta Adresi
- Müşteri Fatura Adresi
- Diğer Bilgiler

Hassas e-Ticaret Verileri: Aşağıdaki veri tipleri hassas olarak değerlendirilmeli ve kurum içinde dahi farklı bölümlere (pazarlama, satış, vb) aktarılmamalı ya da depolanmamalıdır:[55]

- Kredi Kartı Numarası
- Kredi Kartı Şirketi (Kartı üreten banka)
- Kredi Kartı doğrulama numarası (cvc2)
- Kredi Kartı Son Kullanım Tarihi
- Havale Gönderen Hesap Numarası
- Havale Gönderen Banka/Şube Bilgileri
- TC Kimlik No
- Müşteri Parola/Kimlik Doğrulama Bilgileri[56]

Bu kapsamda TSE'ye göre bu verilerin internet üzerinden iletildiği sistem 4 farklı güvenlik kriterini içermektedir.[57] Bunlar:

- Gizlilik

[53] TSE Bilgi İşlem Daire Başkanlığı, e-Dönüşüm Türkiye, E-Ticaret Güvenlik Altyapısı, (2008)
[54] TSE Bilgi İşlem Daire Başkanlığı, e-Dönüşüm Türkiye, E-Ticaret Güvenlik Altyapısı, (2008)
[55] TSE Bilgi İşlem Daire Başkanlığı, e-Dönüşüm Türkiye, E-Ticaret Güvenlik Altyapısı, (2008)
[56] TSE Bilgi İşlem Daire Başkanlığı, e-Dönüşüm Türkiye, E-Ticaret Güvenlik Altyapısı, (2008)
[57] TSE Bilgi İşlem Daire Başkanlığı, e-Dönüşüm Türkiye, E-Ticaret Güvenlik Altyapısı, (2008)

- Bütünlük (integrity)
- Doğruluk/Geçerlilik (authentication)
- İnkar Edememe (non-reputation)

Bu 4 kriterin gerçekleştirilmesinde kullanılan araçlara bakılacak olursa:

## 7.1. Açık Anahtar Yapısı (PKI)

Gönderilen ve alınan verinin değişik şifreleme algoritmaları kullanılarak gönderici tarafından şifrelenmesi ve alıcı tarafından şifrelenmiş verinin, şifresinin açılması temeli üzerine kurulmuş yazılımsal ve yordamsal bütünlük.[58] **Bu yapı günümüzde şifreleme mekanizmalarının temelini oluşturmakta ve bir çok güvenlik uygulamasında sıklıkla karşımıza çıkmaktadır.**

## 7.2. Dijital İmza

Gelen bir mesajın(verinin) gerçekten gönderen kişiden geldiğinin doğrulunu ispatlama(authentication) mekanizması.[59] **Kimlik doğrulama esnasında kullanılabilecek önemli bir elektronik araç olarak olarak karşımıza çıkmaktadır. Ancak kullanımını yaygınlaştırmak için yeni düzenlemeler yapılmasının gerekliliği açıktır.**

## 7.3. Dijital Sertifikalar

Sertifika, açık anahtar sahibinin kimliğini doğrulayan bilgidir. Ehliyet, nüfus cüzdanı gibi sertifika da sahibinin kimliğini ispatlar.

Sertifikalar,

-Sertifika otoritesinin kimliğini

- Sahibinin kimliğini
- Sahibinin public anahtarını
- Sertifikanın kullanımının bitiş zamanını
- Sertifika sunucusunun, bu sertifikayı onaylayan imzasını ve diğer bir takım bilgileri tutar.

[58] TSE Bilgi İşlem Daire Başkanlığı, e-Dönüşüm Türkiye, E-Ticaret Güvenlik Altyapısı, (2008)
[59] TSE Bilgi İşlem Daire Başkanlığı, e-Dönüşüm Türkiye, E-Ticaret Güvenlik Altyapısı, (2008)

Sertifika sayesinde, herhangi bir bilgi alan kişi, bu bilgiyi gönderen kişinin kimliğini, kullandığı sertifikanın geçerli olup olmadığını, sertifikanın güvenilir bir sertifika otoritesi tarafından onaylanıp onaylanmadığını anlayabilir. [60] **Bu uygulama da yine günümüzde güvenlik yapılarında sıklıkla karşımızda çıkmaktadır. Sertifikanın geçerliliğinin bir otorite tarafından doğrulanmasının gerekliliği güvenlik anlamında ek bir fayda sağlamaktadır.**

## 7.4. SSL (Güvenli Giriş Katmanı)

Bu sistemde sunucu (server) bilgisayar ile bilgi alan bilgisayarlar arasında, dijital bir doğrulama amacıyla şifreli bilgiler içeren sertifikalar gönderilir. Bu sayede bilgilerin doğru bilgisayarlar dolayısı ile doğru kişiler/kurumlar arasında gidip gelmesi, kötü niyetli üçüncü şahıs ya da kurumlarca ele geçirilmemesi sağlanır. Gönderilen şifrelerin doğruluğu bu katmanda teyit edildikten sonra güvenli olarak veri değişimi ve aktarımına geçilir.[61] **Bu noktada internet gibi bir açık system üzerinden gönderilen bilginin okunamaması ve değiştirilememesi hedeflenmektedir. Burada önemli olan SSL anahtarının uzunluğuna bağlı olarak güvenliğin yeterli olarak sağlanmasıdır.**

## 7.5. SET

Daha çok B2C pazarında müşteri-firma arasındaki kredi kartlı ödemelerde bilgi güvenliği sağlayan, çalışma prensibi SSL' e benzeyen elektronik güvenlik sistemleri.[62] **Bankadan alıcının kimlik doğrulamasının yapıldığı bir yöntem olarak karşımıza çıkmaktadır.**

## 7.6. Diğer Güvenlik Uygulamaları

- İşletim Sistemi Güvenliği
- Firewall Sistemi
- Saldırı Belirleme Sistemi
- Müşteri Bilgileri Veri tabanı güvenliği
- Web tabanlı dinamik içerik güvenliği
- VPOS(Sanal Ödeme Noktası) güvenliği

[60] TSE Bilgi İşlem Daire Başkanlığı, e-Dönüşüm Türkiye, E-Ticaret Güvenlik Altyapısı, (2008)
[61] TSE Bilgi İşlem Daire Başkanlığı, e-Dönüşüm Türkiye, E-Ticaret Güvenlik Altyapısı, (2008)
[62] TSE Bilgi İşlem Daire Başkanlığı, e-Dönüşüm Türkiye, E-Ticaret Güvenlik Altyapısı, (2008)

- Kart sahibi doğrulama metodu olarak VISA 3-D Secure, MC Secure Payment Application (SPA) ve JCB J-Secure [63]

[63] TSE Bilgi İşlem Daire Başkanlığı, e-Dönüşüm Türkiye, E-Ticaret Güvenlik Altyapısı, (2008)

## 8. TÜRKİYE'DE UYGULANAN GÜVENLİK STANDARTLARI

**E-ticaret'in uygulanması sırasında ülkemizde uygulanan standartlara göz atacak olursak, temel olarak internet üzerinden yapılan e-ticaret uygulamalarında TSE'nin belirlediği standartlara kısmen uyulduğunu görmekteyiz. Örneğin alışverişin ödeme safhasına gelindiğinde, satıcı firmanın web sitesinin SSL bağlantıya geçerek şifrelemeyi devreye aldığını görmekteyiz. Yukarıda da bahsedildiği gibi, bu tür bağlantı yapısına geçilmesiyle beraber, gönderilen ve alınan tüm bilgiler şifrelenmektedir. Ancak burada dikkate alınması gereken konu, şifrelemenin yeterince güçlü algoritmalar kullanarak yapılıp yapılmadığıdır. Bir diğer önemli nokta ise, SSL bağlantıya geçilmesiyle birlikte, alıcının yönlendirildiği yeni sayfanın ne kadar güvenilir olduğudur.**

Ödeme işleminin gerçekleşmesi için TSE'nin hassas bilgiler[64] olarak nitelendirdiği kredi kartı bilgilerinin SSL üzerinden şifrelenerek satıcıya ulaşıyor olması, bu safhada SET güvenlik kriterinin de devreye girdiğini varsayarsak, alıcı ile satıcı arasında güvenli bir alışverişin gerçekleştiği anlamına gelebilir**. Ancak bir diğer önemli nokta, satıcının, alıcının hassas bilgilerini aldıktan sonra, 3. Kurum olan banka ile iletişiminin nasıl olduğudur. Ülkemizde bu işlem için de SSL uygulamalarının sıklıkla kullanıldığını görüyoruz.**

**Dijital sertifikalar ve Açık PKI sistemi, SSL şifrelemesinde kullanılan anahtar yapısını oluşturduğundan, SSL ile şifrelenmiş bir satıcı web sitesinin dijital sertifika ve PKI kullanmama gibi bir durumu söz konusu olamaz. Ancak ülkemizde e-ticaret için kullanılan bazı web sitelerinde, bu dijital sertifikanın bir takım sebeplerden ötürü doğrulanamadığını görebiliyoruz. Bu gibi durumlarda kullanılan tarayıcının özelliklerine göre iletişim devam edebilir ya da sonlandırılabilir.**

**Dijital imza, son yıllarda ülkemizde oldukça yaygın olarak kullanılmaya başlandı. Ancak bu kullanım alanları arasında e-ticaret oldukça**

[64] TSE Bilgi İşlem Daire Başkanlığı, e-Dönüşüm Türkiye, E-Ticaret Güvenlik Altyapısı, (2008)

**az yer almaktadır.** Dijital imza, 5070 sayılı Elektronik İmza Kanunu[65]'na göre hukuki olarak ıslak imza ile aynı değere sahip olduğundan, veri bütünlüğü, kimlik doğrulama ve onaylama ve inkar edilmezlik gibi özelliklere sahiptir. [66] Ülkemizdeki kullanım alanlarına bakacak olursak;

- Kamusal Alandaki Uygulamalar
- Her türlü başvurular (ÖSS, KPSS, LES, pasaport vb)
- Kurumlar arası iletişim (Emniyet Müdürlükleri, Nüfus ve Vatandaşlık İşleri Müdürlükleri vb)
- Sosyal güvenlik uygulamaları
- Sağlık uygulamaları (Sağlık personeli – hastaneler – eczaneler)
- Vergi ödemeleri
- Elektronik oy verme işlemleri
- İnternet bankacılığı
- Sigortacılık işlemleri
- e-Sözleşmeler

Olduğunu görüyoruz.[67]

[65] Elektronik İmza Kanunu(5070), (2005)
[66] Mustafa ALKAN, e-İmza Düzenlemeleri, (2004)
[67] http://www.e-imza.gen.tr/index.php?Page=EImzaNedir&YaziNo=9 , (2010)

## 9. DÜNYADA UYGULANAN GÜVENLİK STANDARTLARI

E-ticaret'de dünyada uygulanan standartlara genel olarak baktığımızda, ISO/IEC 27001[68] dökümanında belirtilen Bilgi Güvenliği Standartları çerçevesinin dikkate alındığını görüyoruz. Bu çerçevede, e-ticarette bilgi güvenliğinin sağlanması için belirlenmiş standart güvenlik kriterlerine bakacak olursak sırasıyla; Güvenlik Politikası, Bilgi Güvenliği Organizasyonu, Varlık Yönetimi, İnsan Kaynakları Güvenliği, Fiziksel ve Çevresel Güvenlik, Haberleşme ve İletişim Güvenliği, Erişim Kontrolü, Bilgi Sistemleri Edinim, Geliştirme ve Bakımı, Bilgi Güvenliği İhlal Olayı Yönetimi, İş Sürekliliği Yönetimi, Yasal Uyum. ISO 27001 standartıyla uyumluluk gösteren e-ticaret firmaları, genel olarak tanımlanan bu gereksinimlere uygunluk sağlayarak standartlaşma yoluna gitmektedirler.[69]

**Daha özel olarak kullanılan teknolojinin çeşidini incelediğimizde, web sitelerinde ülkemizdekine benzer olarak şifreleme için SSL ve SET araçlarının sıklıkla kullanıldığını görüyoruz.**

**Dijital sertifika ve PKI kullanımında, yine ülkemizdekine benzer bir yapı söz konusudur.**

**Dijital imza kullanımına bakıldığında ise dünyadaki kullanımının ülkemize nazaran daha erken tarihlerde yasalaştırılarak yaygınlaştırıldığını görüyoruz.** UNCITRAL (United Nations Commission on International Trade Law-Birleşmiş Milletler Uluslararası Ticaret Hukuku Komisyonu) tarafından ülkelere dijital imzayla ilgili yasa hazırlamaları aşamasında yardımcı olması açısından iki örnek hazırlamıştır. Bunlardan birincisi, 1996 tarihli Model Elektronik Ticaret Yasası, elektronik verilerin ve sözleşmelerin hukuken tanınmasına ilişkin hükümler içermektedir. İkincisi ise, 2001 tarihli Elektronik İmzalara ilişkin standart hükümler, Elektronik İmzalarla ilgili genel esasları belirlemektedir. Bu gelişmelerle birlikte, ülkeler kendi yasalarının oluşturarak yürürlüğe koymuştur.[70]

[68] Hakan Ergin, Bilgi Güvenliği Yönetim Sistemi – Tübitak, (2010)
[69] Fulya Doğantimur, ISO 27001 Standartı Çerçevesinde Kurumsal Bilgi Güvenliği, (2009), Ankara
[70] Mustafa ALKAN ve Köksal ÖZENÇ, E-Ticaretten M-Ticarete Doğru Süreçteki Yeni Yansımalar, (2003)

Dünya kullanımda olan bir diğer uygulama ise e-ticaret sırasında direkt olarak kredi kartı kullanımı yerine ödeme aşamasında farklı bir siteye yönlendirilerek, alıcının burada tanımlı olan para kaynakları (kredi kartı, banka hesabı vb) kullanarak ödemeyi gerçekleştirmesidir. **Böylece kredi kartı bilgilerinin alışveriş yapılan siteyle paylaşılması önlenmiş olur.** Bu uygulamaya örnek olarak PayPal verilebilir.[71] Alıcı PayPal' a abone olarak kredi kartı bilgilerini girer. Güvenlik amacıyla, PayPal tarafından verilen doğrulama kodu kredi kartının ekstresinde görünür ve bu kod tekrar PayPal'a bildirilerek kredi kartının e-ticarette kullanılabilir hale gelmesi sağlanır. **Ayrıca SMS ve e-mail doğrulama, harcama limiti belirleme gibi özellikleri sayesinde e-ticarette yapılan ödemelerde bu tür sitelerin kullanılması, ek bir güvenlik önlemi olarak düşünülebilir.**

[71] https://cms.paypal.com/tr/cgi-bin/?cmd=_render-content&content_ID=ua/UserAgreement_full , (2010)

# 10. MEVCUT E-TİCARET SİSTEMİNİN GÜVENLİK ANALİZİ

## 10.1. Kullanılan Güvenlik Araçlarının İncelenmesi

**E-ticarette ülkemizde kullanılan güvenlik araçlarından en belirgin olanı, alış veriş sırasında hassas bilgilerin iletiminin şifreli olarak yapılmasını sağlayan SSL tekniğinin kullanılmasıdır. SSL'de şifreleme için kullanılacak algoritmanın gücüne göre, şifrelenen bilgilerin ele geçirilme olasılığı da değişkenlik gösterecektir.** Örneğin DES algoritması, günümüzde kırılması çok basit bir şifreleme sunmaktadır. DES ile şifrelenmiş bir SSL bağlantı, üçüncü şahıslar tarafından dinlenmesi kaydıyla rahatça deşifre edilerek, iletilen bilgilere ulaşılabilir.[72]

SSL bağlantılarda kullanılan sertifikanın geçerliliğinin doğru olarak denetlenmesi gerekmektedir.[73] **Bu işlem ise, https: ile sayfaya girildikten sonra, sunucunun gönderdiği sertifikanın, verildiği sertifika otoritesinden web tarayıcı tarafından onaylatılması ile gerçekleşmektedir. Güvenilir sertifika otoritelerinden farklı bir sertifika dağıtıcı tarafından verilmiş bir sertifika söz konusu ise kullanılan web tarayıcının türüne göre bir uyarı görüntülenir yada bağlantı kesilir.**

## 10.2. Olası Tehditlerin Belirlenmesi ve Analiz Edilmesi

**Ülkemizde kullanılan e-ticaret güvenlik kriterlerine baktığımızda birçok tehdit olasılığı görmekteyiz. Özellikle web sitesinin şifreleme güvenliği, satıcı kimliğinin belirlenmesinde ve alıcının kullandığı kaynakların kendisine ait olduğu konusunda önemli soru işaretleri bulunmaktadır.**

SSL kullanılarak hassas bilgilerin korunması oldukça önemli bir güvenlik kriteri olmakla beraber, kullanılan algoritmanın da günümüz standartlarında (3DES, AES) olması gerekir. Ayrıca sertifikanın sağladığı şifrelemenin derecesi de önemlidir. Bazı sertifika otoriteleri 40bit SSL sertifikalar dağıtmaktadırlar.[74] **Fakat günümüz**

[72] http://www.iusmentis.com/technology/encryption/des/ , (2008)
[73] Verisign, Beginer's Guide to SSL Certificates, (2010), http://www.verisign.com/ssl/ssl-information-center/ssl-resources/guide-ssl-beginner.pdf
[74] Kipp E.B. Hickman, The SSL Protocol, (1994)

**standardında en düşük olarak 128bit SSL sertifikalar kullanılmalıdır. Aksi takdirde hassas bilgiler kolayca ele geçirilebilir.**

Yine SSL' de kullanılan sertifikaların, yasal otoriteler tarafından verilmiş olması ve bunun bilgi paylaşımından önce bu otoritelerden teyit edilmesi gerekir.[75] **Yasal olmayan bir otorite tarafından verilmiş olan bir sertifika da şifrelemede kullanılabilir. Ancak, satıcının kimliği doğrulanamadığından ve büyük ihtimalle bağlantı sahte web sitesine doğru olacağından bu bağlantının şifreleniyor olması, hassas bilgilerin güvenli bir şekilde sahte web sitesine gönderilmesi anlamına gelir.**

Bu senaryoya sebep olabilecek başka bir etken ise alıcının bilgisayarındaki DNS (Domain Name Service) sorgularının, sahte DNS sunucularına yönlendirilmesidir.[76] **Böylece alıcı, tarayıcısına web sitesinin adresini yazdığında, DNS sunucu onu sahte web sitesine yönlendirir. Genelde bu sahte web sitesi, gerçeğiyle hemen hemen aynı olarak tasarlanmış olacaktır. Böylece alıcı gerçek siteye girdiğini düşünecek ve alışverişin sonunda kredi kartı bilgilerini girecektir. Sonuçta ise bu bilgiler sahte web sitesine ulaşacak ve çalınmış olacaktır.**

**Bir diğer tehdit ise, çalınmış kredi kartı bilgilerinin alışverişte kullanılmasıdır. Alıcının kimliğinin doğrulanamamasından kaynaklanan bu tehdit, dijital imza, telefon ile teyit gibi doğrulama teknikleriyle önlenebilir. Ancak ülkemizde bu tür doğrulama teknikleri e-ticarette çok nadiren kullanılmaktadır.**

[75] Verisign, Beginer's Guide to SSL Certificates, (2010), http://www.verisign.com/ssl/ssl-information-center/ssl-resources/guide-ssl-beginner.pdf
[76] Tom Olzak, DNS Cache Poisoning: Definition and Prevention, (2006)

# 11. ALTERNATİF GÜVENLİK UYGULAMALARI

**Yukarıda belirtilen olası tehditler, e-ticaret uygulamalarında önemli bir engel olarak göze çarpmaktadır. Mevcut güvenlik standartlarının uygulamada olduğu bir ortamda bu tür tehditlere maruz kalma olasılığı, alternatif güvenlik uygulamalarının gerekli olduğuna bir işaret olarak değerlendirilebilir. Bu anlamda mevcut sistemin güvenlik kriterlerini ve uygulanabilirliğini içeren, aynı zamanda ek olarak bazı uygulamalarla geliştirilmiş yeni bir modelin, e-ticaretteki iş akışını daha güvenli ve sorunsuz hale getirmesi sağlanabilir.**

**Böyle bir modeli oluştururken, asıl amaç e-ticaret güvenliğini arttırmak olsa da, bu modelin uygulanabilir olması ve mevcut sisteme entegrasyonu da önemlidir. Bu noktada güvenlik ve uygulanabilirlik açısından optimumu hedeflemek gerekir. Ne çok sıkı güvenlik kriterleriyle sistemi çalışmaz hale getirmek ne de küçük güvenlik önlemleriyle mevcut tehditlere çözümsüz kalmak doğru olacaktır.**

## 11.1. Öncelikli Tehditlerin Çözümüne İlişkin Model Oluşturulması

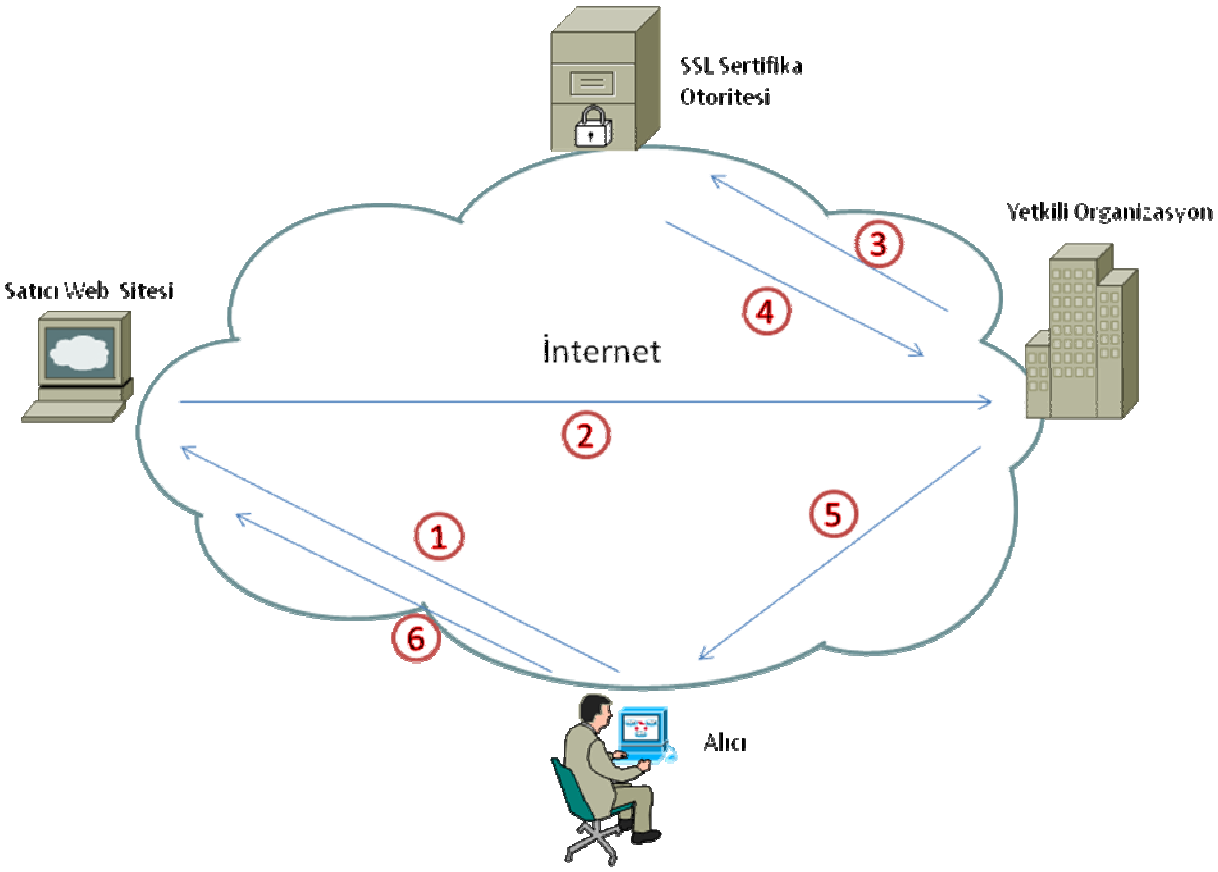
**Günümüz e-ticaret uygulamalarında öncelikli tehditlerin neler olabileceği değerlendirilmişti. Bu açıdan soruna yaklaşılması ve bu tehditleri giderici kriterler ile yeni modelin oluşturulması hedeflenecektir.**

**Öncelikli olarak internet üzerinden yapılan e-ticaret web sayfasının şifreleme özelliklerinin standart hale getirilmesi gerekmektedir. İnternet üzerinden web kullanarak satış yapan tüm e-ticaret firmalarının, önceden belirli bir standart şifreleme ile şifreleme mekanizmalarını oluşturmaları gerekir. Bu standardı belirleyen ve kullanımını zorunlu kılan ve aksi takdirde bazı yaptırım haklarına sahip bir organizasyon olması uygulama açısından önemli bir yapı taşı olacaktır. Ülkemizde bu görevi TSE üstlenebileceği gibi e-ticaret güvenliğini konu edinen farklı bir organizasyon yapısına da gidilebilir.**

**Web üzerinden alış verişte bir diğer tehdit olan SSL sertifikasının doğrulabilir olması da bu standartlara eklenmesi gereken bir kriter olarak karşımıza çıkmaktadır.** Bir anlamda satıcının kimliğinin doğrulanması olan SSL sertifika doğrulama işlemi, şifrelemeye başlanmadan önce sertifikanın verildiği otoriteden sorgulanarak onaylanmasıdır.[77] **Buradaki tehdit, satıcı web sitesinin alıcıya gönderdiği SSL sertifikasının, otorite tarafından doğrulanamamasına rağmen iletişimin devam etmesi olasılığıdır. Bu noktada yapılması gereken, kullanılacak sertifika otoritelerinin açıkça belirlenmesi ve alıcının, satıcı web sitesinin bu otoritelerden alınmış bir sertifikaya sahip olduğunu farklı yollardan doğrulamasını sağlayacak bir yöntem geliştirmektir.**

**Alıcı, satıcı web sitesinden gelen SSL sertifikasının doğruluğunu ilgili otoriteden teyit etmektedir, ancak çözülmesi gereken sorun, doğrulama yapılamasa da işleme devam edilebiliyor olmasıdır. Bu noktada, şifrelemenin başlayacağı anda, ilgili satıcı sitesine ait sertifikasının doğrulamasının yapılmasının ardından alıcıya ulaştırılması bir çözüm olarak düşünülebilir. Burada da yine güvenilir üçüncü bir organizasyona ihtiyaç duyulmaktadır. Ülkemizde bu görevi üstelenebilir bir organizasyon kurulması ya da TSE'nin içinde ayrı bir birim oluşturularak işlemin yapılması sağlanabilir. Bu organizasyon ya da birimin bu noktada yapması gereken, satıcı web sitesiyle alıcı arasında şifreleme başlayacağı zaman, alıcının, satıcı web sitesi tarafından bu organizasyona yönlendirilmesi ve SSL sertifikanın bu organizasyon tarafından alıcıya sağlanmasıdır. Organizasyon bu sertifikayı sağlamadan önce, sertifikanın alındığı otoriteden gerekli doğrulama işlemini, şifreleme standardına ilişkin kontrolleri yapacak ve alıcıya geçerli ve güvenli bir sertifika verecektir. Alıcı da bu sertifikayı aldığında ek bir güvenlik önlemi olarak yeniden otoriteden sorgulayabilir. Böylece alıcı, geçerli bir sertifika ile, kimliği doğrulanmış satıcı web sitesiyle şifreli iletişime geçecektir. Aşağıdaki resimde işlemin nasıl yapılacağı kademeli olarak anlatılmaktadır.**

[77] Oğuz Kara, Elektronik Ticaretin Dış Ticaret İşlemlerinde Uygulanması ve Bilgisayarlı Gümrük Etkinlikleri (BİLGE) Sisteminin Verimliliğinin Değerlendirilmesi, (2002), Kütahya




**Şekil 1. Web Üzerinden Güvenli E-ticaret Adımları**

① **Alıcı alışveriş yapmak istediği satıcı web sitesine girer ve hassas bilgilerin iletileceği şifreli haberleşme aşamasına gelir.**

② **Satıcı web sitesi, SSL sertifikasının doğruluğunu teyit etmesi amacıyla, alıcıyı Yetkili Organizasyona yönlendirir.**

③ **Yetkili organizasyon, satıcı web sitesinin SSL sertifikasının geçerliliğini ve gerçekten bu web sitesine ait olup olmadığını anlamak için SSL sertifika otoritesine bir sorgu yapar.**

④ **SSL Sertifika Otoritesi, gerekli kontrolü yapar ve Yetkili organizasyona sertifikanın geçerli olup olmadığını içeren bir cevap döner.**

⑤ **SSL Sertifika Otoritesinden gelen cevapta sertifikanın geçerli olduğu belirlenmiş ise, Yetkili organizasyon sertifikayı alıcıya iletir.**

⑥ **Alıcı, yetkili organizasyonun verdiği sertifikayı alır ve satıcı web sitesiyle güvenli haberleşmede kullanır. Alıcı, sertifikayı aldıktan sonra SSL sertifika otoritesinden yeninden doğrulatabilir.**

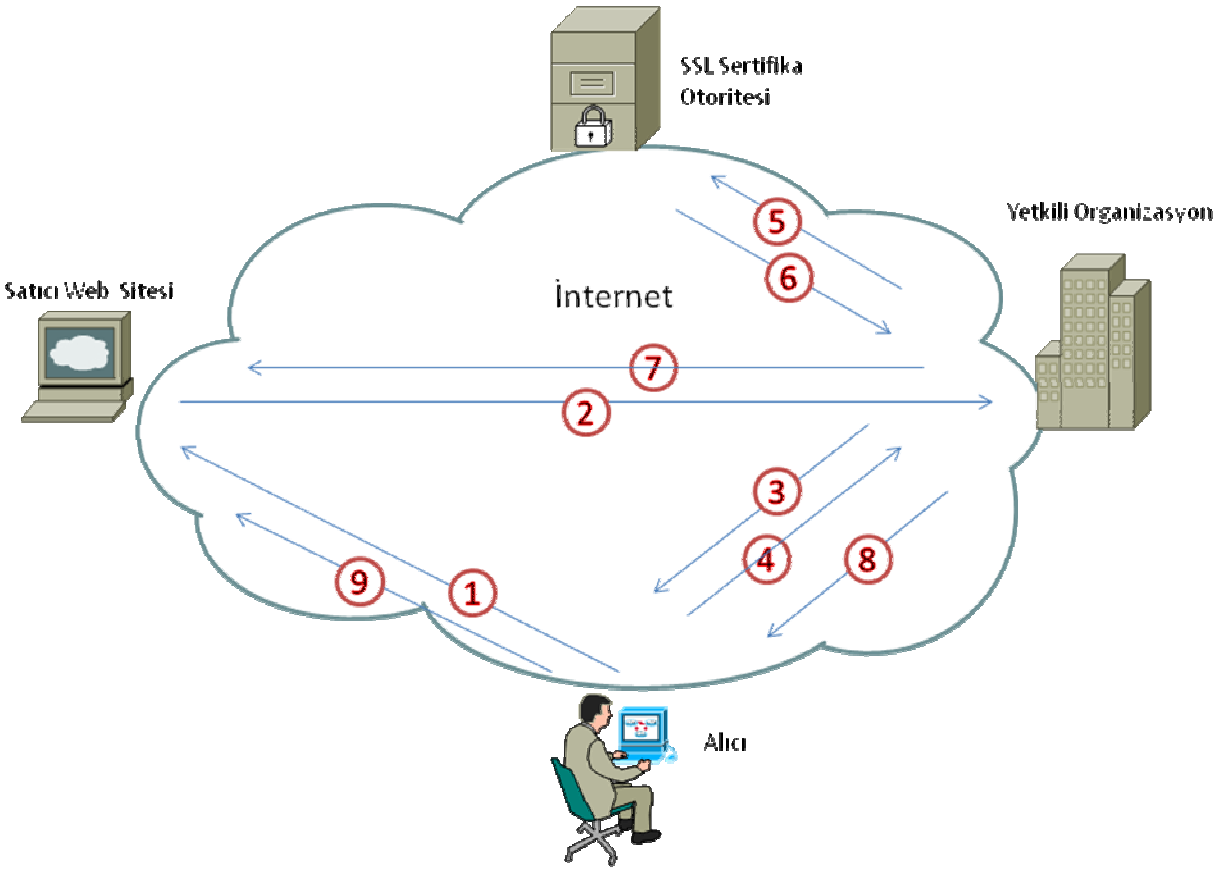
**Burada dikkat edilmesi gereken nokta, satıcı web sitesinin alıcıyı güvenilir organizasyon yerine başka bir sahte siteye yönlendirmesi ihtimalidir. Böyle bir durumda sahte siteye yönlendirilen alıcıya, doğrulanmamış bir sertifika da iletilebilir. Bu da alıcının doğrulanmamış sertifikayı kullanarak alışverişe devam etmesine sebep olabilir. Satıcı web sitesinin, alıcıyı yetkili organizasyonun sitesine yönlendirmesini zorunlu kılacak ek bir işlemin akışa eklenmesi gerekmektedir. Yani satıcı web sitesi, alıcının SSL sertifikasını alarak alışveriş işlemine devam etmesini istiyorsa, alıcıyı mutlaka yetkili organizasyona yönlendirmesini gerektirecek bir sebep olmalıdır.**

**Olası tehdit ve güvensizliklerden bahsederken, alıcının kimliğinin doğrulanamıyor olmasının da önemli bir güvenlik sorunu oluşturabileceğinden bahsedilmişti. Çünkü başka bir şahsın kredi kartı bilgilerine ulaşan bir kullanıcı, bu bilgileri kart kendine aitmiş gibi kullanarak alışveriş yapabilir. Oluşturulan modelde bu probleme uygulanabilecek çözüm, satıcı web sitesinin alıcıyı yetkili siteye yönlendirme zorunluluğu olmasıyla birleştirilerek üretilebilir.**

**Yetkili organizasyon, satıcı web sitesine ait SSL sertifikasını doğrulayıp alıcıya vermeden önce, alıcının kimlik kontrolünü yaparak alıcıyı da doğrulayabilir. Ancak bu doğrulamayı kendi veritabanından yapması daha doğru olacaktır. Çünkü farklı bir otoriteden doğrulaması, yetkili organizasyonun taklit edilmesine olanak sağlayacaktır. Bu doğrulama için farklı yöntemler kullanılabilir. Örneğin kullanıcı bilgilerini, alışverişte kullanılacak kredi kartının verildiği bankaya yönlendirilerek, bankadan**

**alıcının kimlik doğrulamasının yapılması istenebilir. Bu noktada banka kimlik doğrulaması için alıcıya telefon ya da e-posta ile erişebilir. Ancak işlemin bir e-ticaret alışverişi olduğu düşünüldüğünde bu işlemin saniyelerle belirtilen süreler içinde yapılması gerekir. Bu sebeple telefon ile doğrulama kullanışlı bir yöntem olmamakla beraber e-posta kullanımı daha uygun olabilir. Doğrulama için başka bir yöntem ise, yetkili organizasyon tarafından alıcıya önceden verilmiş bir şifre ya da güvenlik sorusu olabilir. Alıcı işlem sırasında bu şifreyi ya da güvenlik kodunu girerek, yetkili organizasyonun kendisini doğrulamasını sağlayabilir. Günümüzde bankaların internet şubelerine girişte de kullanılan tek kullanımlık şifreler de bu amaçla kullanılabilir. Doğrulama işleminin hukuki temellere dayandırılması daha belirleyici ve güvenli olmakla beraber, daha karmaşık bir yapı anlamına gelir. Böyle bir durumda, alıcının bu işlemi elektronik imza ile onaylaması istenebilir. Yetkili organizasyonun tekliği ve taklit edilememesini sağlayabilmek için, elektronik imzada kullanılan sertifikanın da yine yetkili organizasyon tarafından sağlanmış olması gerekir. Aksi takdirde farklı bir otoriteden sorgulama işlemini herhangi bir yapı tarafından yapılabilir olması, yetkili otoritenin taklit edilebilirliğine sebep olacaktır. Elektronik imzanın yetkili organizasyon tarafından etkin kılınarak alıcılara sağlanması her ne kadar oldukça zor bir işlem olsa da, doğrulamanın farklı otoriteler yerine tek yetkili organizasyondan yapılması güvenlik anlamında oldukça önemli bir adım olacaktır. Ülkemizde bu tür bir işlemin yapılması ve bahsi geçen kuruma entegrasyonu için Tübitak' ın mevcut durumda kendi e-ticaret kullanımına özgü sertifika otoritesini kurarak yalnızca yetkili organizasyona servis etmesi gerekir.**

**Bu akışı aşağıdaki resimde inceleyecek olursak:**




**Şekil 2. Web Üzerinden Güvenli E-ticaret Adımları ve Alıcı Doğrulama**

① **Alıcı alışveriş yapmak istediği satıcı web sitesine girer ve hassas bilgilerin iletileceği şifreli haberleşme aşamasına gelir.**

② **Satıcı web sitesi, SSL sertifikasının doğruluğunu teyit etmesi ve alıcının kimliğini belirlemesi amacıyla, alıcıyı Yetkili Organizasyona yönlendirir.**

③ **Yetkili organizasyon, alıcının kimliğini doğrulayabilmek için, önceden verdiği şifreyi ya da elektronik imzayı ister.**

④ **Alıcı, kendisine daha önceden Yetkili organizasyon tarafından sağlanan şifre ya da elektronik imzayı kullanarak kimlik doğrulama cevabını iletir**

⑤ **Yetkili organizasyon, alıcı kimlik doğrulaması başarılı olduktan sonra, satıcı web sitesinin SSL sertifikasının geçerliliğini ve gerçekten bu web sitesine ait olup olmadığını anlamak için SSL sertifika otoritesine bir sorgu yapar. Alıcı kimlik doğrulaması başarısız ise, bu noktada işlemi sonlandırır.**

⑥ **SSL Sertifika Otoritesi, gerekli kontrolü yapar ve Yetkili organizasyona sertifikanın geçerli olup olmadığını içeren bir cevap döner.**

⑦ **SSL Sertifika Otoritesinden gelen cevapta sertifikanın ve alıcı kimliğinin geçerli olduğu belirlenmiş ise Yetkili organizasyon satıcı web sitesine bir onay mesajı döner. Eğer alıcı kimliği geçersiz ise, işlemin güvenli olmadığını bildiren bir mesaj döner.**

⑧ **SSL Sertifika Otoritesinden gelen cevapta sertifikanın geçerli olduğu belirlenmiş ise, Yetkili organizasyon sertifikayı alıcıya iletir. Gelen cevap sertifikanın geçersiz olduğunu belirtiyorsa, yetkili organizasyon alıcıya bu işlemi sonlandırması gerektiği şeklinde bir mesaj döner.**

⑨ **Alıcı, yetkili organizasyonun verdiği sertifikayı alır ve satıcı web sitesiyle güvenli haberleşmede kullanır. Alıcı, sertifikayı aldıktan sonra SSL sertifika otoritesinden yeninden doğrulatabilir.**

**Alıcının kimlik doğrulamasının yalnızca yetkili organizasyon tarafından yapılabiliyor olması, satıcı web sitesinin alıcıyı yetkili organizasyona yönlendirmesini zorunlu kılacaktır. Aksi takdirde alıcı kimlik doğrulaması yapılmadığından alışverişin güvensiz olduğunu bilecek ve işlemi sonlandıracaktır. Doğrulamanın ardından alıcının kimlik bilgileri satıcıyla paylaşılabilir. Satıcı açısından bakıldığında da, alıcının kimlik doğrulamasının yapılması alışverişin güvenilirliği açısından olumlu bir adım olacaktır. Satıcı ürünü kime sattığını kesin olarak bilecek ve daha önemlisi ödemeyi yapan kişinin, ödeme aracının gerçek sahibi olduğundan emin olacaktır.**

**Bu model bir diğer güvenlik tehdidi olarak belirtilen, alıcı bilgisayarındaki DNS sunucularının alıcıyı sahte web sitesine yönlendirmesini tehdidini de engellemiş olacaktır. Çünkü alıcı, sahte web sitesine yönlense bile, sahte web sitesi alıcıyı yetkili organizasyona yönlendirdiğinde, yetkili organizasyon satıcının SSL sertifikasını ilgili otoriteden onaylatamayacağından web sitesinin sahte olduğunu belirleyecek ve alıcının işlemini bu sebeple sonlandıracaktır.**

## 11.2. Alternatif Güvenlik Modelinin Mevcut Sisteme Uygunluğu

**Mevcut yapıya ek bazı önemli iyileştirmelerle beraber oluşturulan yeni modelin, mevcut e-ticaret yapısına entegrasyonu da oldukça önemlidir. Tasarlanan modelde, uygulama aşamasında karşılaşılabilecek sorunlar şu şekilde olacaktır:**

### 11.2.1. Şifreleme Standardının Belirlenmesi

**E-ticaret yapılan web sitelerinde şifreleme standardının belirlenmesi ve uygulanmasını sağlayacak ve bunun denetimini yapacak bir yapının oluşturulması gerekmektedir. Teknik açıdan bakıldığında, bir e-ticaret web sitesinin şifreleme altyapısının değiştirilmesi, başka bir deyişle şifrelemede kullanılan SSL sertifikasının standart güvenlik kriterlerini sağlayacak şekilde değiştirilmesi ve bu yeni sertifikanın sisteme entegre edilmesi zahmetli bir süreç olabilir. En azından bu çalışmanın yapılacağı sürede web sitesinin hizmet veremiyor olması maddi ve manevi kaygılar doğuracaktır. Ancak standardizasyonun tamamlanmasıyla beraber, alıcılara bu güvenlik geliştirmesinin aslında onlara yönelik bir hizmet olarak devreye alındığının bildirilmesi, siteye olan güveni ve sitenin prestijini arttırabilir. Bu noktada standardı belirleyen yetkili organizasyona üyelikle ilgili de bazı lansmanlar yapılabilir. Örneğin satıcı web sitesinde "Bu web sitesi Yetkili Organizasyon'a üyedir." şeklinde bir ifade, alıcıların siteye olan güvenini arttıracaktır.**

### 11.2.2. SSL Sertifikasının Yetkili Organizasyon Tarafından Doğrulanması

**SSL sertifikasının geçersiz olduğu durumlarda alıcının alışverişe devam etme olasılığını ortadan kaldırmak için tasarlanan bu çözümün uygulanması için satıcının web sitesinde hassas bilgilerin iletileceği güvenli iletişime geçilmeden önce alıcının yetkili organizasyona yönlendirilmesi gerekir. Bu işlem teknik açıdan oldukça basit bir değişiklik ile devreye alınabilir. Öte yandan alıcının yetkili organizasyona yönlendirilmesiyle beraber, yetkili organizasyon yönlendirmeyi yapan web sitesinin kimliğini tespit etmeli, diğer bir deyişle sertifikasını alarak bunu sertifikanın verildiği otoriteden doğrulaması gerekir. Bu işlem de teknik olarak oldukça kolay bir işlemdir. Özet olarak, alıcını yapacağı sertifika doğrulama işlemini, yetkili organizasyon yapacaktır. Buradaki en önemli nokta, bu tür alışverişlerin yoğun olarak yapıldığı anlarda, yetkili organizasyondaki sistemin bu yoğunluğu karşılayacak kapasitede olması gerekliliğidir. Bu sistemin kurulumu sırasında, ülkemizdeki e-ticaret verileri incelenerek bir tahmin yapılarak buna uygun yatırımlarla donanım ve yazılım sağlanabilir.**

### 11.2.3. Yetkili Organizasyonun Alıcılara Kimlik Doğrulaması Yapması

**E-ticaretteki alıcının kimliğinin doğrulanamaması problemine çözüm olarak geliştirilen yapıda, bu doğrulamanın yetkili organizasyon tarafından yapılması öngörülmektedir. Yetkili organizasyonun bu doğrulamayı farklı yollardan yapabileceğinden bahsedilmişti. Bunlardan alıcılara tahsis edilecek şifre yada doğrulama kodu uygulaması kullanım olarak oldukça pratik olacaktır. Alıcı bu kodu ya da şifreyi kaybettiğinde belli güvenlik sorularının ardından tekrar ulaşabilecektir. Bu yapının sağlanması, yetkili organizasyonda barındırılacak veritabanı donanım ve uygulamalarını gerektirecektir. Böylesine büyük ve yedekli bir yapının maliyetinin karşılanması aşamasında, satıcıdan belirli aidat ücreti talep edilebilir.**

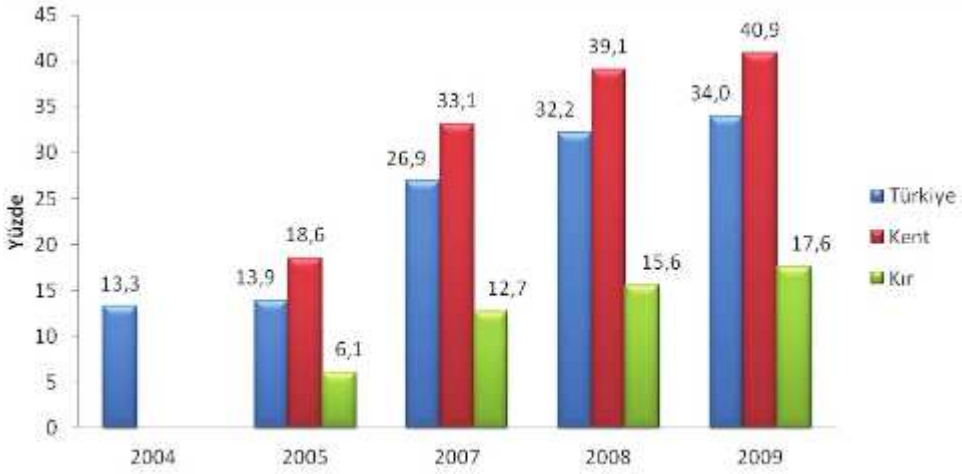
**Yetkili organizasyonun kimlik doğrulamada kullanabileceği bir diğer yöntem ise alıcıya tahsis edilen elektronik imzadır. Elektronik imzada kullanılacak sertifika otoritesinin yetkili organizasyonda bulunması gerekliliği uygulamada bazı güçlüklere sebep olacaktır. Sistemin devreye alınması sırasında ya da sonrasında yaşanabilecek aksaklıklar, web üzerinden e-ticareti durma noktasına getirebilir. Bu sebeple sistemin çok iyi tasarlanması ve tamamen yedekli olarak çalışması gerekmektedir. Yine altyapısal olarak oldukça büyük bir maliyet söz konusu olacaktır. Ancak güvenlik açısından bakıldığında böyle bir uygulamanın, olası tehditler sonucu oluşabilecek maliyetlerden çok daha az olduğu ortadadır.**

**Yeni model ile birlikte, e-ticaret yapmak isteyen web sitelerinin, yetkili organizasyona üye olmaları yasalar ile zorunlu hale getirilebilir. Böyle güvenlik kriterlerinin, faaliyet gösteren tüm yasal e-ticaret web sitelerinde sağlanması garanti altına alınacaktır. Üyeliğin zorunlu olmaması durumunda ise, alıcıların bu konuyla ilgili bilgilendirilmeleri ve yetkili organizasyon tarafından doğrulamalarının yapılmadığı hiçbir alışverişe devam etmemelerinin güvenlik açısından tavsiye edildiği vurgulanabilir.**

# 12. E-TİCARET GÜVENLİĞİNİN GELECEĞİNE YÖNELİK ÖNGÖRÜLER

## 12.1. E-Ticaret'in Mevcut ve Öngörülen Büyüme Oranları

**Elektronik ticaretteki büyüme, internet kullanımının yaygınlığı ile doğru orantılıdır. İnternet kullanımının artması, web üzerinden satış için daha fazla potansiyel alıcı anlamına gelmektedir. Ülkemizdeki elektronik ticaretin büyüme oranını da, internet kullanım oranıyla eşleştirebiliriz.** Devlet Planlama Teşkilatı' nın yaptığı araştırmada 2004-2009 yılları arasında internet kullanımıyla ilgili grafiğe bakacak olursak, Türkiye'de internet kullanımının 5 yıl içinde yaklaşık iki buçuk kat arttığını görmekteyiz.[78]

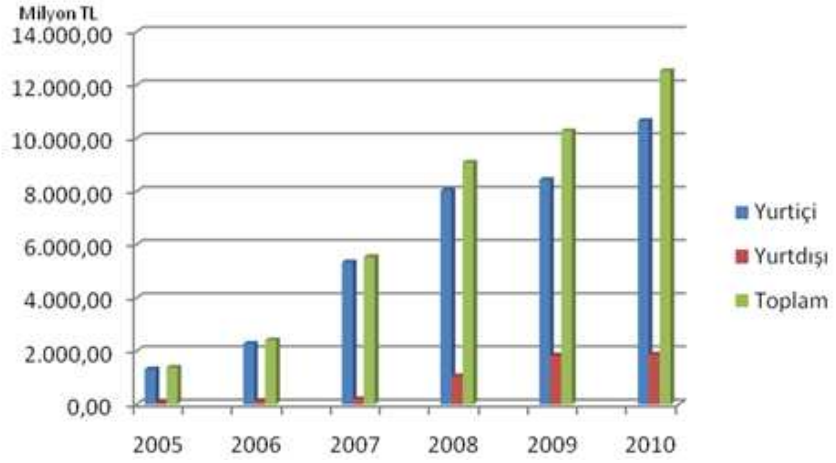



**Grafik 1. 2004-2009 Yılları Arası Türkiye'de İnternet Kullanımı**

Buna paralel olarak, BKM' nin Sanal POS kullanımına ilişkin yaptığı araştırmadaki verilere bakacak olursak:[79]

[78] Devlet Planlama Teşkilatı Müsteşarlığı, Bilgi Toplumu İstatistikleri, (2010)

[79] http://www.bkm.com.tr/istatistik/sanal_pos_ile_yapilan_eticaret_islemleri.asp , (2010)

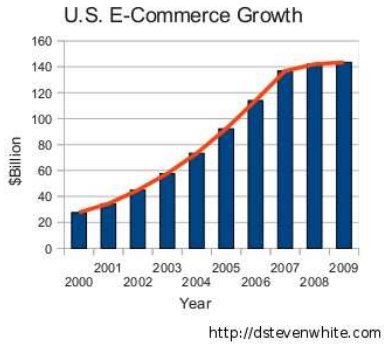



**Grafik 2. 2005-2010 Yılları Arası Sanal POS Kullanımı**

Yukarıdaki grafikte, yerli ve yabancı kredi kartlarının yurt içi sanal pos'larda kullanımıyla oluşan işlem hacmi gösterilmektedir.

**E-ticaretin son 5 yılda ülkemizdeki gelişimini de özetleyen bu grafik, daha önce de bahsedildiği gibi, internet kullanımın artışıyla paralellik göstermektedir. E-ticaretin ilerleyen yıllarda da benzer ivmeyle büyümesi öngörülmektedir.**

E-ticaretin ABD'deki büyüme trendine göz atacak olursak, dstevenwhite.com'um araştırmasına göre ABD'nin e-ticaret hacmini aşağıdaki grafikte görebiliriz:[80]



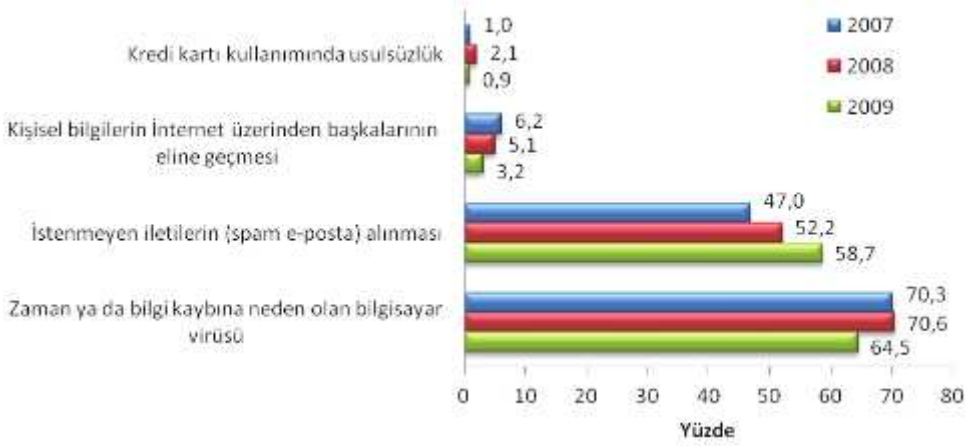

**Grafik 3. 2001-2009 Yılları Arası ABD'deki E-Ticaret Hacmi**

[80] http://dstevenwhite.com/2010/08/20/u-s-e-commerce-growth-2000-2009/ , (2010)

**Grafikten de anlaşılacağı gibi ABD'de elektronik ticaret, son 10 yılda yüksek ivmeli bir büyüme trendi yakalanmıştır. 2008'den itibaren ivmede bir azalma görülse de, öngörüler e-ticaret hacminin ilerleyen yıllarda da artışını sürdüreceği yönündedir.**

## 12.2. Büyümenin Getireceği Güvenlik Endişelerine İlişkin Öngörüler

**Elektronik ticaretin büyüme oranlarına bakıldığında, yakın gelecekte daha fazla ilgi göreceği ve kullanılacağı açıktır. Elektronik ticaretin gelişimi, beraberinde güvenlik sorunlarını da getirmektedir.** Tüik' in yaptığı bir araştırmada, ülkemizdeki internet kullanıcılarının karşılaştığı güvenlik sorunları aşağıdaki grafikte gösterilmektedir.[81]




**Grafik 4. 2007-2009 Yılları Arası İnternet Kullanıcılarının Karşılaştığı Güvenlik Sorunları**

**Buna göre internet kullanıcılarının en fazla karşılaştığı güvenlik problemi virüsler olarak görünmektedir. E-ticarette kullanılan hassas bilgilere ulaşarak bunları kötü niyetli kullanıcılara aktarabilen virüs çeşitleri**

[81] TÜİK, Hanehalkı Bilişim Teknolojileri Kullanım Araştırması, (2010)

**de bulunmaktadır. Bu da e-ticaretin güvenli olarak yapılmasına engel olabilecek alıcı tarafındaki en büyük sorunlardan biridir. Alıcı bu sorunu bilgisayarına yükleyeceği güvenlik yazılımlarıyla en aza düşürmelidir.**

**İstenmeyen iletilerin de (spam e-posta) e-ticarette güvenlik anlamında olmasa da pazarlama anlamında bir sorun teşkil ettiği düşünülebilir. Firmalar reklamlarını, ilgili yada ilgisiz herkese e-posta yoluyla gönderirler. Bu çoğu zaman rahatsızlık verici ve e-ticarete katkısı olmayan bir aksiyondur.**

**Kişisel bilgilerin internet üzerinden başkalarının eline geçmesi ve kredi kartı kullanımında usulsüzlük sorunları da azalma eğilimi göstermiştir. Bu problemler genelde virüsler yada kötü niyetli yazılımlar yardımıyla yapıldığından, güvenlik yazılımlarının yaygın kullanımıyla ters orantılı olarak azalmıştır. Ancak bu güvenlik tehditlerinin de e-ticaret için kısıtlayıcı ve uzaklaştırıcı olduğu kaçınılmazdır.**

**E-ticaret güvenliğine satıcı tarafından bakıldığında ise, mevcut duruma ilişkin analiz yapılmış ve olası problemler belirlenmiştir. Buna göre e-ticaretin gelişimiyle birlikte bu problem ve riskler de daha önemli hale gelecektir. Satıcı tarafındaki risklerin önemli kısmına çözüm sunan model oluşturulmuştur. İlerleyen yıllarda e-ticaret hacminin daha da artacağı göz önüne alındığında, daha güvenli bir elektronik alış veriş için bu güvenlik modelinin uygulanması doğru olacaktır.**

# 13. SONUÇ VE DEĞERLENDİRMELER

**Son yıllarda elektronik dünyasındaki hızlı gelişmelerin ortaya çıkardığı ürünler hayatımıza birçok kolaylık getirmiştir. Elektronik ticaret de özellikle 2000'li yılların başından itibaren yaygınlaşmaya başlamış ve alışveriş kavramına yeni bir ara yüz olmuştur. Özellikle internet kullanımının yaygınlaşmasıyla birlikte elektronik ticaretteki Pazar da hızla büyümüştür. Bugün artık internet üzerinden sipariş verip de alınamayacak bir ürün çeşidi neredeyse kalmamıştır.**

**İnternet üzerinden elektronik ticaretin yaygınlaşması, sağladığı kolaylıkların yanı sıra bazı önemli sorunları da beraberinde getirmiştir. Bu sorunlardan en önemlisi güvenlik tehditleri olarak karşımıza çıkmaktadır. İnternet üzerinden alışverişin yapılabilmesi için, alıcının bazı hassas bilgilerini internet ortamı üzerinden alıcıya ulaştırması kullanılan metoda göre oldukça sakıncalı olabilmektedir. Ayrıca internetteki elektronik ticaret pazarının büyümesi de kötü niyetli kişiler için sahte ya da taklit e-ticaret web siteleri açarak alıcıları dolandırmasına olanak sağlamaktadır. Bir diğer önemli nokta da, internet üzerinden satış yapan satıcının, alıcının kimliğini doğrulayamamasıdır. Bu durumda da kötü niyetli şahıslar ele geçirdikleri başkalarına ait hassas bilgileri kullanarak alışveriş yapabilmektedir.**

**İnternet üzerinden elektronik ticaretin daha da gelişmesine engel olan bu problemlerin çözümlerine yönelik bir güvenlik modeli tasarlanmıştır. Bu modelin uygulanmasıyla birlikte mevcut durumdan daha güvenli bir alış veriş ortamı sağlanmış olacaktır. Modelin uygulanması sırasında karşılaşılabilecek sorunları en aza indirgemeyebilmek için, altyapı çalışmalarının ve yeni modeli geçişin çok iyi planlanması gerekmektedir. Uygulama maliyetleri düşünüldüğünde ise, artı güvenliğin alıcıda sağlayacağı güven ile e-ticaret hacminin artış derecesi göz önünde bulundurulmalıdır.**

**Geçmişten günümüze internet üzerinden elektronik ticaretin gelişimine baktığımızda, bu gelişimin internet kullanım oranlarıyla paralellik**

**göstermekte olduğunu görüyoruz. İnternet kullanımının artması, potansiyel alıcı sayısının artması anlamında gelmektedir. Böylece Pazar büyümekte ve daha çok satıcı bu pazarda bir "elektronik dükkan" oluşturmaktadır. Büyümenin birçok faydasının olmasıyla birlikte beraberinde getireceği güvenlik problemlerini de göz önünde bulundurmak gerekir. Önerilen çözüm modeli, eksiksiz uygulandığı takdirde, yeni alışveriş yöntemleri geliştirilene kadar oldukça güvenli bir metod olarak kullanılabilir.**

## KAYNAKÇA


Arvind Panagariya, E-Commerce,WTO and Developing Countries, (2000), New York

Belgin Behram, Aydan Atalay, Çağrı Tanoğlu, Elif Öztürk, a'dan z'ye Elektronik Ticaret, (2001)

Cihad Demirli, E-Ticaret (İlk Adımlar), (2010)

Devlet Planlama Teşkilatı Müsteşarlığı, Bilgi Toplumu İstatistikleri, (2010)

Dış Ticaret Müsteşarlığı, İhracatı Geliştirme Etüd Merkezi, B2B e-Ticaret ve e-Pazaryerleri, (2008), Ankara

Elektronik İmza Kanunu (5070), (2005)

Fulya Doğantimur, ISO 27001 Standartı Çerçevesinde Kurumsal Bilgi Güvenliği, (2009), Ankara

Hakan Ergin, Bilgi Güvenliği Yönetim Sistemi – Tübitak, (2010)

Hakan UZUNOĞLU, Elektronik Ticaretin Vergilendirilmesinin İncelenmesi ve Değerlendirilmesi, (2002), Ankara

Halil Elibol, Burcu Kesici, Çağdaş İşletmecilik Açısından Elektronik Ticaret, (2003)

Hasan ÇIRPAN, E-Ticarette Güvenlik, (2005)

Hilmi KUŞÇU, E-Ticaret: SSL ve SET, (2010)

http://dstevenwhite.com/2010/08/20/u-s-e-commerce-growth-2000-2009/ , (2010), (erişim tarihi: 18.12.2010)

http://www.bkm.com.tr/istatistik/sanal_pos_ile_yapilan_eticaret_islemleri.asp , (2010), (erişim tarihi: 10.12.2010)

http://www.e-imza.gen.tr/index.php?Page=EImzaNedir&YaziNo=9 , (2010), (erişim tarihi: 22.11.2010)

http://www.eticarethazirla.com/menu-set , (2010), (erişim tarihi: 24.11.2010)

http://www.e-ticaretmerkezi.net/odemearaclari.php , (2010), (erişim tarihi: 03.12.2010)

http://www.garantiweb.com/ssl.asp?ID=25&PAGE=2, (2010), (erişim tarihi: 02.12.2010)

http://www.iusmentis.com/technology/encryption/des/ , (2008), (erişim tarihi: 02.11.2010)

https://cms.paypal.com/tr/cgi-bin/?cmd=_render-content&content_ID=ua/UserAgreement_full , (2010), (erişim tarihi: 07.11.2010)

Kipp E.B. Hickman, The SSL Protocol, (1994)

Mustafa ALKAN ve Köksal ÖZENÇ, E-Ticaretten M-Ticarete Doğru Süreçteki Yeni Yansımalar, (2003)

Mustafa ALKAN, e-İmza Düzenlemeleri, (2004)

Oğuz Kara, Elektronik Ticaretin Dış Ticaret İşlemlerinde Uygulanması ve Bilgisayarlı Gümrük Etkinlikleri (BİLGE) Sisteminin Verimliliğinin Değerlendirilmesi, (2002), Kütahya

Okşan KÖMÜRCÜ, Elektronik Ticaret Kavramı, Kapsamı ve Araçları, (2005), http://www.hukuki.net/hukuk/index.php?article=261

Pelin KABALAK, BKM, Türkiye E-Ticaret Pazarı, (2010)

Tom Olzak, DNS Cache Poisoning: Definition and Prevention, (2006)

TSE Bilgi İşlem Daire Başkanlığı, e-Dönüşüm Türkiye, E-Ticaret Güvenlik Altyapısı, (2008)

TÜİK, Hanehalkı Bilişim Teknolojileri Kullanım Araştırması, (2010)

Ü. Reha Şendil, E-Ticarette Bilgi Güvenliği Terimleri, (2010)

Verisign, Beginer's Guide to SSL Certificates, (2010), http://www.verisign.com/ssl/ssl-information-center/ssl-resources/guide-ssl-beginner.pdf

WTO Special Report 2, Electronic Commerce and the Role of the WTO , (1998), http://www.wto.org/english/res_e/booksp_e/special_study_2_e.pdf

Zeynep BEİGH, B2B E-Ticaret İşletme Kavramı ve B2B İşletmelerde Konumlandırma Stratejileri,(2010), İstanbul