# e-ticaret

Prof. Dr. Eşref Adalı

# İçindekiler

# Şekiller

# 1

# Ticaret

İnsanlar arasında alışverişin ve ticaretin ne zaman başladığına ilişkin çeşitli tahminler yapılmaktadır. Alışverişin 150.000 yıl önce başladığı düşünülmektedir. O dönemlerde insanların bazı değerli taşları aralarında değiş tokuş ettikleri anlaşılmaktadır. O günlerde çakmak taşı ve obsidiyen taşı değerliydi; çünkü ateş yakmak için çakmak taşı, mızrağın ucuna keskin obsidiyen taşı gerekiyordu. Bir kişinin elindeki değerli taşı bir başka kişide bulunan taş ile değiştirmesi için, elinde bulunan taşın gereksiniminden fazla olması; diğer kişide bulunan taşa da gereksinim duyması gerekir. Bu tür alışveriş sonunda iki taraf da sevinir. Bu tür alışverişe mal takası ya da kısaca takas yöntemi adı verilmektedir. Takas usulü ticaretin yakın zamana kadar Anadolu'da sürdürüldüğü bilinmektedir. Örneğin 1950'li yıllarda bir birim dokunmuş bez iki birim ham pamuk ile değiştirilmekteydi.

# 1.1 Ticaretin Gelişimi

Kişiler ve toplumlar arası ticaret zamanla gelişti. Ticaretin gelişim aşamaları şöyle sınıflandırılmaktadır:

## 1.1.1 Sığır Ticareti

MÖ 10.000- MÖ 5.000 döneminde insanlar sığırlarını takas aracı olarak kullanmaya başladılar. Sığırlar yakın zamana kadar insanların en önemli varlıkları sayılmıştır. Sığırlar tarla sürme, yük taşıma, et ve süt sağlama, giyecek üretme gibi önemli işlevleri yerine getirirdi. Sığırların önemini vurgulayan iki bilgiyi hatırlatmakta yarar görüyoruz.

Latince "pecunia" sözcüğü para anlamına gelir ve Latince sığır anlamına gelen "pecus" ile ilgilidir. Osmanlı'da 1831 yılında başlatılan nüfus sayımlarında bir evde yaşayan erkekler ve evin sahip olduğu sığırlar sayılırdı. Sığır sayısı o aileye verilecek arazinin boyutunu belirlerdi. Sığır ticareti takas yöntemi sayılmaz. Çünkü sığırların belli bir değeri vardır.

## 1.1.2 Değerli Malzeme ile Ticaret

MÖ 5.000 - MÖ 1.200 arası dönemde değerli malzemelerin ticarette para gibi kullanıldığı görülmektedir. Bu dönemde deniz kabuklarının değerli malzeme olarak ticarette kullanıldığına ilişkin kanıtlara rastlanmaktadır. Deniz kabukları dayanıklı, hafif, dolayısıyla kolay taşınabilir, kırılması zor, taklit edilmesi ve çoğaltılması zor oldukları için seçilmişlerdir. Çin yazısında "deniz ürünü" için kullanılan şekil para anlamına gelmektedir. Bu dönemde bakır, bronz, altın ve gümüş gibi değerli metaller para gibi kullanılmıştır.

MÖ 19. Yüzyıllarda Asurluların, bugünkü Nevşehir'de ticari koloniler kurduğuna ilişkin izler bulunmaktadır.

## 1.1.3 Para

MÖ 1.200 - MÖ 500: Bugün bildiğimiz para birimine benzeyen ilk madeni paraların, Lidya'nın başkenti Sardeis'te (şimdi Manisa'nın Salihli ilçesi) kullanılmaya başlanmıştır. O zamanlar Sardeis önemli bir ticaret merkeziydi. Mezopotamya ve Anadolu toplumları arasındaki ticarette önemli bir yer tutmaktaydı. İlk madeni paranın Sardeis'te kullanıldığını ünlü tarihçi Heradot'un kitabından şöyle öğreniyoruz: “Onlar ilk altın ve gümüş parayı icat eden ve kullanan insanlardır." İlk **kesilen** madeni paraların üzerinde dönemin tanrıları, kralları veya sporcularının kabartmaları olurdu, Şekil-1-2.

**Şekil-1.1**: Sardeis (Salihli-Manisa)

Paranın bulunması ticarette önemli bir mihenk taşı olarak kabul edilir.

**Şekil-1.2**: Lidya paraları (Vedat Nedim Tör Müzesi - İstanbul)

## 1.1.4 Kraliyet Yolu

MÖ 340: Persler Anadolu toplumları ile ticareti geliştirmek amacıyla MÖ 300 yılında Susa'dan (İran'ın eski başkenti) Sardeis'e kadar uzanan yaklaşık 2.500 Km uzunluğunda **Kraliyet Yolu**nu yaptılar.

## 1.1.5.İpek Yolu

MÖ 40: Kraliyet yolundan yaklaşık 300 yıl sonra Çinliler Uzak Doğu'yu Anadolu'ya bağlamak üzere **İpek Yolu**nu oluşturdular. Amaç Çin ile Hindistan, Pers üzerinden Roma İmparatorluğu ticareti sağlamaktı. İpek yolu, Çinli diplomat Zhang Qian tarafından başlatılmış uzun yıllar Dünyanın en önemli ticaret yolu olmuştur, Şekil-1.3.

Ticaretin gelişmesini sağlamak amacıyla Türkler ticaret yolları üzerine han ve kervansaraylar inşa etmişlerdir. Hanlar yerleşim yerleri içinde, kervansaraylar kırsal kesimde kurulurlardı. Sulh zamanında ticaret kervanlarının konaklaması için hizmet veren han ve kervansaraylar düşman saldırısında çevrede yaşayan insanların sığınakları olurdu, Şekil-1.4. İki kervansaray arasındaki uzaklık genellikle 12 mil olarak belirlenirdi. Bu mesafe bir kervanın gün boyu alabileceği yol olarak hesaplanmaktaydı.

Kraliyet yolu ve İpek yolu yalnızca ticarete hizmet etmekle kalmamış, toplumlar arası etkileşime de neden olmuştur. Bu yollar sayesinde ülkeler arasında kültürel etkileşimler olmuş, bilgiler, düşünceler ve dinler yayılmıştır. İpek ve kağıt bu yol üzerinden batıya taşındı.

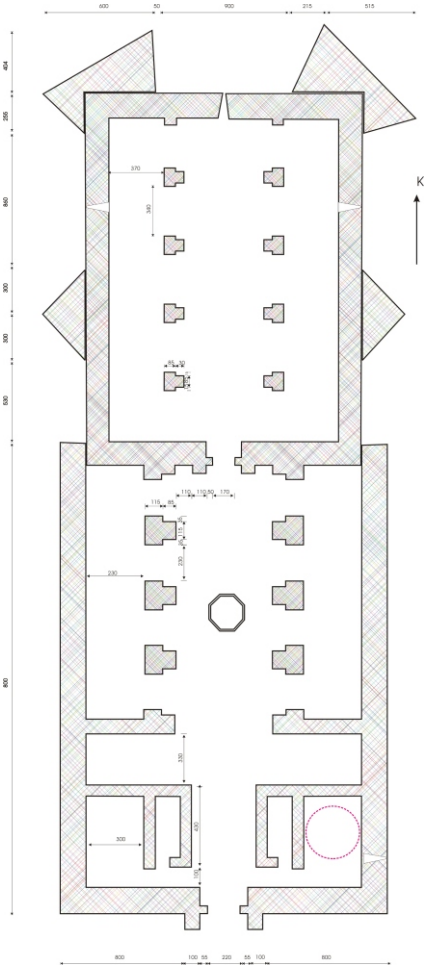

**Şekil-1.3**: İpek Yolu

## 1.1.6 Pazarlar

Zaman içinde kentlerde pazarlar kurulmaya başlamıştır. İnsanlar yiyecek, giyecek, hayvan ve diğer malları pazarlardan sağlayabiliyorlardı. Malını satmak isteyenler de mallarını pazarlara getiriyorlardı. Pazarlar satıcı ve alıcının buluşma yerleri idi. Haftanın belli günlerinde kurulan pazarlar olduğu gibi sürekli çalışan pazarlar da vardı. Belli günlerde kurulan pazarlarda satıcı ve alıcılar bir alanda (genellikle kent merkezinde) toplanırken sürekli çalışanlarda dükkânlar oluşturulmuştur.

Selçuklu ve Osmanlı kentlerinde kurulmuş olan çok sayıda han biçiminde pazarlar günümüzde de ayaktadır. Örneğin Bursa'daki Koza han yaklaşık 600 yıldır çalışan sabit bir pazar yeridir. Özellikle ipek ve ipekli kumaşların pazarlandığı özel bir pazar yeridir, Şekil-1.5.

**Şekil-1.5**: Koza han (Bursa)




**Şekil-1.4**: Ertokuş Kervansarayı (Yeşilköy-Isparta)

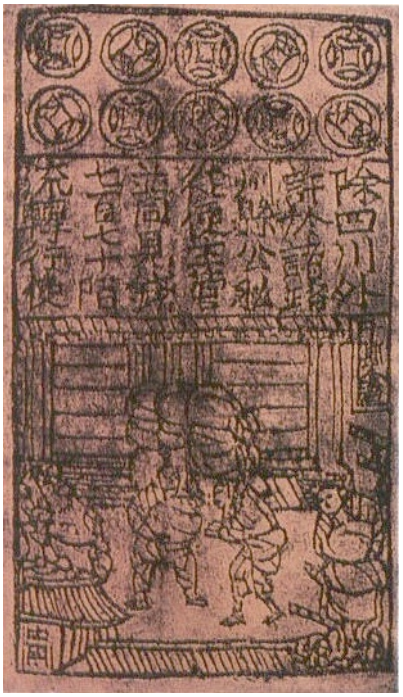
## 1.1.7 Kağıt Para

800: Ticaret için komşu kent veya ülkelere giden tüccarlar malları karşılığında başka mallar, değerli madenler veya madeni para alıyorlardı. Değerli taş ve madeni paralar ağır olduklarından taşınmaları kolay değildi. Değerli maden veya metal para yerine geçecek senetler Çin'de Tang Hanedanlığı döneminde (618–907) kullanılmaya başlanmıştır, Şekil-1.6. Bu paranın kullanımı 1100 yılına kadar sürmüştür.

Avrupa'da kağıt para ilk olarak Leiden (Hollanda) kentinde 1574 yılında basılmıştır. Bu paralarda, önceleri madeni para basmakta kullanılan kalıplar kullanılmıştır. Daha sonra 1660'da Stockholms Banco'nun bastığı kağıt paralar olmuştur.

İlk kağıt paralar, aslında bankaların altın veya gümüş paralara karşılık verdikleri kağıt senetlerdi. Bu yüzden kağıt paralara banknot adı verilmiştir. Bankalar banknotu getirene karşılığında altın veya gümüş para vermeyi taahhüt ederdi.

Kağıt para anlamında olan ancak ipek dokuma olarak üretilmiş banknotlar da üretilmiştir, Şekil-1.7.



**Şekil-6**: Eski Çin kağıt parası

## 1.1.8 Keşifler

XIV. Yüzyılda başlayan keşifler özellikle Amerika kıtasının keşfi İspanyol ve Portekizlilerin gümüş ve altın zengini olmasını sağlamıştır. Ayrıca Avrupalıların İpek yoluna bağımlılığı azaldı; deniz yoluyla Uzak Doğuya erişebilir oldular. Böylece ticarette yeni olanaklar ve yöntemler doğmuş oldu.

Yeni yerlerin keşfi ile Hindistan'dan baharat, pamuk, ipek, çivit, güherçile ve çay deniz yolu ile Avrupa'ya ulaşmaya başladı. Bu dönem bir de köle ticareti başlamıştır. Bu sayede Avrupa ülkeleri, özellikle İngiltere zenginleşmiştir.

Keşifler yeni ticaret kavramlarının ve yöntemlerinin doğmasına, örneğin ticari firmaların, bankaların, nakliyecilerin kurulmasına neden olmuştur.

Bu dönemde kullanılan para gümüş veya altın paradır. Dolayısıyla paranın değeri altınının değeri ile ölçülmektedir. Paranın altın karşılığının olması Avrupa'da Birinci Dünya Savaşı sonrasına kadar devam etmiştir.


**Şekil-1.7**: İpek dokuma banknot (Hiva Müzesi)

## 1.1.9 Kredi Kartı


**Şekil-1.8**: Karton Diners Club kartı

Kredi kartının doğuşunun ilginç bir hikâyesi vardır. Varlıklı iş adamı McNamara'nın 1949'da, cüzdanını unuttuğu için yemek parasını ödeyememesi üzerine düşünüp geliştirdiği Diners Club kartı, kredi kartı uygulamasının başlangıcı sayılır, yıl 1950. Diners Club kartı ilk dönemlerde sadece varlıklı kişilere saygınlık kartı olarak verilmiştir. Hedef, bir ay boyunca yapılan yemek ve konaklama harcamalarının ay sonunda kart işletmecisine ödenmesiydi. Lokanta ve oteller paralarını kart işletmecisinden alıyorlardı. 1980 öncesi kredi kartları ile yapılan ödemeler, karbon kopyalı makbuzlar ile gerçekleştirilmekteydi. Kartların arkasında manyetik şerit yoktu. Bugün yaygın olarak kullanılan kredi kartlarının yaygınlaşması, bilgi teknolojilerindeki gelişmeyle sağlanmıştır. Diners Club kartları karton üzerinde basılmıştır ancak 1959 yılında American Express kredi kartını plastik olarak müşterilerine vermiştir.

## 1.1.10 Elektronik Veri Değişimi

1972'de IBM ve GE ticaret için bir yeni kavramı dünyaya tanıttılar. Value Added Network (VAN) adını verdikleri bu yöntemde firmalar arası belgeler VAN üzerinden aktarılmaya başlanmıştır. VAN firmaları birbirine güvenli biçimde bağlıyor ve aralarında gidip gelen belgeler için noterlik görevi yapıyordu. VAN üzerinden gönderilen belgeler için bir Elektronik Veri Değişimi (Electronic Data Interchange - EDI) ölçünü belirlendi. Bu ölçün daha sonra Birleşmiş Milletler tarafından üstlenildi ve kapsamı genişletildi; sonuç olarak UN/EDIFACT (Electronic Data Interchange for Administration, Commerce and Transport) adını aldı. EDI elektronik ticaretin (e-ticaret) başlangıcı sayılır. Çevrimiçi yöntemiyle yapılan ilk e-ticaret örneğinin, 1994 yılında satılan Sting albümü olduğu bilinmektedir.

## 1.1.11 Sayısal Para (Kripto Para)

Sayısal para ya da diğer adıyla kripto para, koddan oluşturulan sayısal bir para veya şifrelenmiş bir veri dizisi veya bir karmasıdır. Sayısal para birimini belirtecek şekilde kodlanmıştır. Birisi tarafından denetlenmeyen ve bir merkezi olmayan para birimidir. Belirli bir kuruluş veya hükümet tarafından yönetilmez bunun yerine eşler arası Genelağ (internet) protokolü tarafından izlenir. Sayısal paranın izlenmesi için **Öbek Zinciri** (Blockchain) adı verilen bir yapı geliştirilmiştir. Öbek zinciri Sayısal para hareketlerindeki sahteciliği ve para gönderenin, gönderdiği parayı geri çekmesini önlemektedir.

Öbek zinciri yöntemi, günümüzde diğer ticari etkinliklerde de kullanılmaya başlanmıştır. Öbek zinciri üzerinden, bankalar arası para aktarılması, gümrükler arası işlemler yürütülmeye çalışılmaktadır. Bu tür uygulamaların zaman içinde artacağı öngörülmektedir.

## 1.2 Ticaretin Temel Tanımları ve Bileşenleri

Eski zamanlarda ve günümüzde sürdürülen ticaret yöntemlerini anlayabilmek için bazı temel tanımları bilmekte yarar vardır. Bu kısımda bazı temel ticari tanımlar verilmiştir.

**Alışveriş**: Satın alma ve satma işi, alım satım.

**Ticaret (Tecim):** Ticaret, kar amacı ile mal ve hizmetlerin, para ile ifade edilebilen bütün değerlerin alım ve satım işlerinin tamamıdır.

**Tüccar (Tecimen)**: Ticaret yapan, ticaretle uğraşan kimse, tacir.

**Ticarethane (Tecimevi)**: Ticaret yapılan yer

**Esnaf**: Küçük sermaye ve zanaat sahibi

Bu tanımlara baktığımızda alışverişin en temel eylem olduğunu, ticaretin alış veriş sürecinin tüm aşamalarını kapsadığını söyleyebiliriz. Tecim, ticaret sözcüğünün Türkçe karşılığıdır. Bazı Anadolu kentlerinde ticarethane yerine tecimevi sözcüğünün hâlâ kullanıldığına tanık olmaktayız.

Geleneksel ticarettin üç paydaşı vardır. Bunlar üretici, tüketici ve aracılardır. Ticaret üreticinin ürününü tüketiciye ulaştırmayı sağlar ve temel amaç kâr etmektir. Aracıların devreden çıkarılması için değişik yöntemler denenmiş olmasına karşın aracılık günümüzde de sürdürülmektedir. Geleneksel ticaretin üç türü vardır: Perakende, toptan, uluslararası ticaret.

### Perakende Ticaret

Malların küçük miktarlarda satılması perakende satış olarak adlandırılır. Perakende satış, beklendiği gibi malın tüketiciye satılmasıdır. Perakende satış yapana perakendeci denir. Perakendeciler malları üreticiden veya toptan satıcıdan sağlarlar. Perakendecilerin genel olarak küçük işletmeler olduğu düşünülür. Geçmişte bu değerlendirme doğru olabilir ancak günümüzün en büyük e-ticaret firmaları birer perakende satıcıdır. Perakendecinin temel işlevleri şöyle sıralanabilir:

- Malları tüketicilerin ayağına götürme
- Malları uygun ölçeklerde tüketiciye sunma
- Çeşitli malları sunma
- Bilgilendirme ve danışma hizmetleri sunma
- Müşteri şikâyetlerini değerlendirme
- Veresiye satış olanağı sağlama
- Satış öncesi ve sonrası hizmetleri sunma

## Toptan Ticaret

Malların toplu olarak ve büyük miktarda alınıp satıldığı ticarete toptan ticaret ve bu işlevi yerine getirenlere de toptancı denir. Toptancılar üretici ve perakendeci arasında aracılık yapan firmalardır. Bunlar depolama, taşıma ve dağıtım işlevlerini yürütürler; bir anlamda aracı kuruluşlardır. Toptancılar genellikle büyük işletmeler olarak karşımıza çıkarlar. Toptancıların temel işlevleri şöyle sıralanabilir:

- Depolama
- Taşıma
- Pazarlama
- Satın aldıklarını daha küçük miktarda satış

## Uluslararası Ticaret

Ülkeler arası yapılan ticaret biçimidir. Bir ülkede üretilen bir malın diğer bir ülkedeki tüketici veya aracıya satılması eylemidir. Geçmiş dönemlerde yalnızca toptan ticaret biçiminde gerçekleştirilen uluslararası ticaret, günümüzde perakende olarak da yapılmaktadır.

Ticarette görev alan temel paydaşlara, ikinci derece paydaşları ekleyebiliriz. Bu paydaşlar, sırasıyla taşıyıcılar, depolar, dağıtıcılar, reklam ve tanıtıcılar, sigortacılar, satıcılar ve bankalardır.

## Taşıyıcılar

Üretilen ürün ve malların veya ham maddelerin gereksinim duyana ulaştırılması işlevi taşımacılık olarak adlandırılır. Taşıma işini yerine getirenlere taşımacı denir. Bu tanımdan da anlaşılacağı gibi taşınan nesne bir hammadde olabilir, örneğin demir cevheri. Hammadde, bunu işleyecek olan fabrikaya taşınır. Taşınan nesne ürün de olabilir. Bu durumda ürün veya ürünler, üretildikleri veya satıldıkları yerden alıcıya ulaştırılır. Taşımacılık için geçmişte ambar, yakın zamanda lojistik firma deyimi kullanılmaktadır. Taşımacılar her türlü taşıma araçlarını (kara, deniz ve hava) kullanırlar.

## Depolama ve Ambarlama

Ürünün üretilmesi ile tüketilmesi arasında bir zaman varsa ürünün uygun koşullarda saklanması gerekir. Örneğin elma hasadı sonbahar aylarında yapılır ancak tüketimi yıl boyu sürer. Bu nedenle elmaların belli iklim koşullarında saklanması gerekir. Bu amaçla kurulmuş olan depolarda saklanırlar.

## Dağıtım

Ürünlerin tüketicilere ulaştırılması işlevidir. Dağıtım işinin uç paydaşı perakendecidir. Ancak üretici ile perakendeciler arasında dağıtıcı denilen işletmeler de yer alırlar. Dağıtımın doğrudan yapıldığı örnekler de bulunmaktadır.

### Reklam ve Tanıtım

Bir ürünün satılabilmesi için öncelikle o ürünün varlığından tüketicilerin haberi olması gerekir. Ürünlerin tanıtılması ve reklamının yapılması reklam ve tanıtım firmalarının işidir.

### Sigorta

Üretilen ürünlerin depolarda saklanması, taşınması ve pazarlanması sırasında bazı riskler ile karşılaşması olasıdır. Örneğin depodaki ürünlerin çürümesi veya bozulması; taşıma sırasında yaşanabilecek kazalar; pazarlama sırasında olabilecek olumsuzluklar. Bu tür olası risklerden en az zararla kurtulma için ürünler sigortalanır. Sigortalama, bir anlamda riski sigorta şirketine yüklemek paylaşma anlamındadır.

### İletişim

Satıcı ile alıcının bağlantıya geçmesi iletişim olarak adlandırılır. Satıcı ile alıcının yüz yüze iletişime geçmesi, semt pazarında olabileceği gibi mağazada olabilir. Günümüzde telefon ve e-posta ile iletişim yaygın olarak kullanılmaktadır.

### Banka

Üretim yapanlar, üretim yapabilmeleri için gerekli olan hammadde ve diğer kaynakları sağlayabilmek için parasal desteğe gereksinim duyarlar. Tüketiciler de bir ürünü satın alabilmek için paraya ihtiyaçları olabilir. Her iki tarafın parasal gereksinimleri bankalar tarafından karşılanır. Bankalar sağladıkları para karşılığı olarak faiz alırlar.

## 1.3 Ticaretin İşleyişi ve Yöntemleri

Ticarette uygulanan yöntemler doğal olarak yaşanan dönemin olanakları ve koşullarına göre şekillenmektedir. Paranın bilinmediği dönemde yapılan ticaret ile günümüzde uygulanan e-ticaretin yöntemlerinin aynı olması beklenemez. Ancak geçmişten günümüze kadar, ticarette uygulanan yöntemlerin ortak özellikleri de vardır. Bu nedenle eski dönem ve günümüzdeki ticaret yöntemlerini incelemekte yarar vardır.

### 1.3.1 Eski Yöntemler

Eski dönemlerde ticaretin nasıl işlediğini anlayabilmek için kaynakları inceleyebileceğimiz gibi hayal gücümüzü de kullanabiliriz. İpek yolu üzerinden sürdürülen ticaret önemli bir örnek ve kaynaktır. Tarihi ipek yolu bugünkü Şian kentinden başlar ve ilk olarak o dönemlerde Özbekistanın önemli bir kenti olan Kaşgar'a ulaşırdı. Daha sonra yol kuzey ve güney olmak üzere ikiye ayrılırdı. Kuzey yolu Afganistan ovalarından geçerek Hazar Denizi'ne ulaşırdı. Güney yolu Karakurum Dağları'nı aşarak bugünkü İran ve daha sonra Anadolu'ya ulaşırdı. Anadolu'ya ulaşan mallar deniz yolu olarak Akdeniz ve Karadeniz veya karayolu olarak Trakya üzerinden Avrupa ülkelerine gönderilirdi.

## 20 - Ticaret

**Şekil-1.9**: Günümüzdeki Karakurum yolu

Çin'i Pakistan'a bağlayan Karakurum yolu çok yüksek ve sarp dağlar üzerinden geçtiği için bugün bile Dünya'nın en tehlikeli yollarından biri sayılır. Bu yolun orta çağda kervanlar için daha da tehlikeli olduğu açıktır.

İpek yolu üzerinden batıya gönderilen ürünler, ipek, porselen, kağıt, baharat ve değerli taşlar (örneğin yeşim taşı) olarak bilinir. Batıdan doğuya gönderilen ürünler, altın, değerli taş ve camdır. Kaynaklarda baharat olarak adlandırılan ürünler aslında yalnızca baharat değil, ilaç, anestezi, afrodizyak ve parfümdür.

**Şekil-1.10**: İpek yolunun mal taşıyan develeri

İpek yolu üzerindeki ticaret takas yöntemi ile yapılıyordu. Çin'den kalkan bir kervanın Anadolu'ya kadar yol aldığı düşünülemez. Kervan komşu ülkeye kadar ulaşır ve ulaştığı sınır noktasında mallarını komşu ülkenin tüccarları ile takas eder. Çin'in o günkü komşusu Özbekistan olduğu düşünülürse, Çin mallarını, bundan sonra batıya doğru taşıyacak olanlar Özbeklerdir. Özbekler malları Afganlara, Afganlar Perslere ve onlar da Anadolu'da yaşayan uluslara ulaştırırlardı. Dönemin taşıma aracı çift hörgüçlü develerdir. Ancak kervanda çok sayıda hayvan, çok sayıda çoban bulunurdu.

Ortaçağ döneminde İpek yolu hırsız ve haydutlar için uygun bir ortam sağlıyordu. Özellikle dar ve tehlikeli geçitlerin bulunduğu Karakurum bölgesi haydut yuvası idi. Ağırlıklı olarak devlerden oluşan kervanların güvenliğini sağlamak üzere bölge devletleri özel önlemler almıştır. Han İmparatorluğu kervanlara eşlik edecek özel savunma birlikleri oluşturmuş, yol boyunca Çin Seddi'ni inşa etmiştir.

İpek yolunun Anadolu içindeki bölümüne Selçuklu ve Osmanlı'nın 200 kadar kervansaray ve han yaptırdığı kaynaklarda belirtilmektedir. Bu han ve kervansarayların bazıları yıkılmış ya da yok olmuştur. Ancak Turizm ve Kültür Bakanlığı bazılarını yenileyerek turizm amaçlı hizmetler sunabilecek hale getirmiştir. Yenilenen hanların adları aşağıda verilmiştir:

- Sultan Hanı (Aksaray)
- Sarı Han (Nevşehir)
- Şarapsa Han (Antalya)
- Ak Han (Denizli)

- Ağzıkara Han (Aksaray)
- Alara Han (Antalya)
- Silahtar Mustafa Paşa Kervansarayı (Malatya)
- Çardak Han (Denizli)
- Susuz Han (Burdur)
- İncir Han (Burdur)
- Alay Han (Aksaray)

**Şekil-1.11**: Susuz han

Çin'den Anadolu'ya kadar uzanan İpek Yolu'nun uzunluğu yaklaşık 6.000 Km kadardır. İpek yolunun Anadolu'daki kısmının güvenliği Selçuklular ve Osmanlılar tarafından sağlanmıştır. Bu amaçla kervanlara eşlik edecek koruma birlikleri verilmiş; konaklayacakları ve ticaret yapacakları han ve kervansaraylar kurulmuştur. Kervansaray ve hanlardaki yaşam ile ilgili şu öz bilgileri bilmemizde yarar vardır:

Anadolu Selçukluları ve Osmanlılar, ticari kervanları korumayı görev edinmişlerdir. Toprakları içinde malları zarar gören kervan sahibinin zararları giderilmiştir. Devlet kervan sahiplerinden belli oranda vergi alırdı.

Han ve kervansaraylarda konaklayan yolcular din, dil, ırk fark gözetilmeden üç gün kalabilirlerdi. Hasta olan yolcular tedavi edilirdi. Konuklara günde iki öğün yemek çıkarılırdı. Konukların temizlenmesi için handa hamam, ibadet etmeleri için mescit bulunurdu. Kervanın hayvanları ve arabaları için de bakım hizmeti verilirdi. Bu amaçla handa veteriner ve nalbant bulunurdu. Konuklar üç gün boyunca hiçbir ücret ödemeksizin bu hizmetlerden yararlanırlardı. Bu hizmetler, han ya da kervansarayın vakfından elde edilen gelirlerle karşılanırdı.

Kervansaraylarda, konukların yatacağı odalar, yemek yiyeceği yemekhanelerin yanı sıra erzak ambarları, ticari eşya depoları, yolcuların hayvanları için ahırlar, samanlıklar, mescit, kütüphane, konukların yıkanması için hamam, abdest şadırvanı, tedavileri için hastane ve eczane, ayakkabı tamircisi bulunurdu. Fakir yolcular için yeni ayakkabı yapılıp verilirdi.

Han ya da kervansaraylar, ticaret yolları üzerinde, kervanların bir günde erişebileceği aralıklarla inşa edilmeye çalışılmıştır. Bu nedenle, iki han arasındaki uzaklığın bir menzil dolayında olmasına özen gösterilmiştir. (1 menzil = 4 fersah = 12 mil = 22.740 m dir.)

Handa konaklayan yolcuların can ve malları devlet kolluk güçlerince korunurdu. Kervansarayda kalındığı sürece yolcuların can ve malları teminat altına alınırdı.

Kervansaraylar, genellikle iki katlı taş yapılardı. Uzaktan bakıldığında kaleyi andırırlardı. Hanların kale görünümünde ve taştan yapılmalarının nedeni sadece güvenlikti. Han ve kervansarayların dış duvarlarında, güvenlik nedeniyle pencere bulunmazdı. Anadolu Selçukluları ve Osmanlılar zamanında hanlar askeri birlikler tarafından korunurlardı.

Büyük ve korunaklı olan han ve kervansaraylarda akşam olunca ana kapı kapatılırdı. Ana kapı kapatıldıktan sonra handan dışarı çıkış yasaklanırdı. Ancak dışarıdan gelen olursa kapı açılır ve gelen kişi ya da kervan içeri alınırdı. Gün ağardığında, konuklar davul çalınarak uyandırılırdı.

Handa konaklayan yolcular yola koyulmaya hazır olduklarında, kendilerine "*malınız, canınız, elbiseleriniz ve atınız tamam mı?*", diye sorulurdu. Tüm konuklar "*tamam*" dediğinde hanı yaptıran kişi için dua edilir ve ardından kapı açılarak uğurlanırlardı.

Barış zamanında ticaret kervanları ve yolcuların konaklaması amacıyla hizmet veren han ve kervansaraylar, harp zamanında halk için sığınma yerleriydi.

Ticari yaşamı gözetmek amacıyla ''devlet sigorta sistemini" ilk kullanan ve ayrıca gümrük vergilerinde uyguladıkları indirimlerle ticari hayatı özendirmeye çalışan yine Selçuklular olmuştur. Han ve kervansaraylar, bu aktif ortamın önemli görevler yüklenen kuruluşlarıdır.

### 1.3.1.1 İpek Yolundan Öğrenilenler

Tarihi İpek Yolu üzerinde gerçekleştirilen ticaret bize şunları öğretmiştir.

- Ticaret ancak güvenli ortamlarda yapılabilir
- Alışveriş yapan taraflar birbirlerine güvenebilmelidir.
- Alışverişten iki taraf da kazançlı çıkmalıdır.

#### Güvenli Ortam

Güvenli ortam, bölgeyi yöneten devlet veya yapılar tarafından sağlanır. Yöneticiler ülkelerinde ticaretin sürmesini isterler. Çünkü her ülkenin üretim fazlası varsa bunu başkalarına satmak ister ya da tersine gereksinimi olan ürünleri başka ülkelerden sağlamak ister. Böylece ulusuna gelir sağlar ve ulusunun gereksinimlerini karşılar.

Yöneticiler tüccarların güvenliğini sağlamak üzere, öncelikle yolların güvenliğini sağlarlar; kervanlara eşlik edecek güvenlik birlikleri verirler. Kervanların konaklayabilecekleri güvenli mekânlar yaparlar. Bu hizmetlerinin karşılığı olarak alışverişten vergi alırlar.

#### Karşılıklı Güven

Mallarını takas edecek tüccarların birbirine güvenmesi gerekir. Karşılıklı güveni sağlayacak ortam, koşul ve olanaklar genellikle ülkeler tarafından sağlanır. Örneğin han ve kervansarayların görevi, taraflara güvenli ortamı sağlamaktır. Han yöneticisi alışverişe gözetmenlik yapar. Böylece tarafların birbirini kandırması veya soymasının önüne geçilir. Ayrıca han yöneticisi alışverişin değeri üzerinden vergi alır.

#### Karşılıklı kazanç

Ticaretin kâr amaçlı yapıldığını belirtmiştik. Ayrıca bir taraf elindeki üretim veya gereksinim fazlası olan malını satmak ister; buna karşılık gereksinimi olan malı karşı

taraftan sağlamak ister. Bu mantık iki taraf için de geçerlidir. Sağlıklı bir alışverişin sonunda iki taraf da kazançlı çıkmalıdır.

### 1.3.1 Güncel Yöntemler

İpek Yolu üzerinde yapılan ticaretin, o günün koşullarında takas yöntemiyle yapıldığı söylenebilir. Yakın zamanlarda bu ticaret yolunda madeni para ve daha sonra kağıt paranın kullanıldığı bilinmektedir. Günümüzdeki ticaretin yöntemleri farklıdır ancak İpek yolundan öğrenilen üç temel kural hâlâ geçerlidir.

Bugün Çin'deki bir üreticiden mal almak isteyen bir Türk tüccarın aşağıdaki adımları izlemesi gerekir:

#### Ürünü Seçme

Orta çağda, müşteri ayağına gelen ürünü görüp seçebiliyordu. Günümüzde ürünü seçmek için çeşitli yollar bulunmaktadır. Ürünü bir sergide görebilir, tanıtım kitapçığında özellikleri öğrenebilir, üreticinin web sayfasında inceleyebilir veya üreticinin yerine gidip görebilir.

#### Sipariş Verme

Satın almayı düşündüğü ürün için, üreticiden teklif ister. Bu istek üzerine üretici proforma fatura gönderir. Proforma faturada ürünün fiyatı ve satış koşulları yer alır.

#### Dışalım Süreci

Müşteri proforma fatura ile bankasına gider ve istediği ürünün dışalımın yapılması için aracı olunması ister. Anlaşma olduğunda faturada belirtilen parayı bankaya yatırır.

Dışalımlarda izlenen iki ana uygulama vardır: FOB ve CIF

FOB (Free On Board): Bu yöntemde, satıcı malını kendi gümrüğüne teslim ettikten sonra sorumluluğu biter. Ürünün müşterinin ülkesine kadar taşınması ve taşıma ile ilgili masraflar alıcı tarafından ödenir.

CIF (Cost Insurance and Freight): Satıcı malın alıcıya ulaşmasına kadar geçen süre içindeki kayıp ve hasarlarına ilişkin sigorta primini ödemekle yükümlüdür. Ayrıca dışsatım işlerini de satıcının yapması gerekir.

Dışalım biçimine karar verildikten sonra Türkiye'deki banka, Çinli bir banka ile anlaşır. Bu bankaya muhabir banka adı verilir.

#### Malın Denetimi

Satıcının malı gümrüğe teslim edip etmediği ve malın doğru mal olduğunu denetimini muhbir banka yapar; sonucu Türkiye'deki bankaya bildirir. FOB alımlarda, malın gümrüğe teslim edilmesinin ardından satıcıya ödeme yapılır. CIF alımda, ödeme için malın alıcının gümrüğüne kadar gelmesi beklenir.

## Gümrük İşlemleri

Gümrüğe gelen malın gümrükten çekilmesi süreci uzmanlık isteyen bir eylemdir. Bu tür işleri genellikle Gümrük Müşaviri denilen kişi veya kuruluşlar yaparlar.

Yukarıda anlatılan aşamalardan da anlaşılacağı gibi, iki tarafın birbirini kandırmamasını bankalar sağlamaktadır. Malın taşınması sırasında ortaya çıkabilecek sorunlara karşılık mal sigorta ettirilmektedir. Gelen malın, farklı veya ayıplı olması durumunda devreye mahkemeler girmektedir.

Günümüzde, ulusal veya uluslararası alışverişte VAN gibi özel ağlar veya İnternet gibi genel ağlar kullanılmaktadır. Bu tür ticarette satıcı ve alıcılar birbirini tanımamakta, özellikle perakende satışlarda tarafların birbirini kandırması kolay olmaktadır. Genelağ üzerinden gerçekleştirilen e-ticaretin sağladığı olanaklar ve sorunlar ilgili bölümde ayrıntılı biçimde ele alınacaktır.

Günümüze yapılan ticari işlemler aşağıda sıralanmıştır:

**Firma - Müşteri (F-M : B-C)**: Bir firmanın bir ürün veya hizmeti bir bireye satması eylemidir. Örneğin bir bireyin e-ticaret sitesinden ayakkabı satın alması.

**Firma - Firma (F-F : B-B)**: İki firma arasında mal ve hizmet satışı eylemidir. Örneğin bir bilgisayar üreticisinin, ürünlerini bir toptan satıcıya satması.

**Firma - Kamu (F-K : B-A):** Bir firmanın bir kamu kurumuna yaptığı mal ve hizmet satış eylemidir.

**Birey - Birey (B-B : C-C)**: İki birey arasında gerçekleşen mal ve hizmet satışıdır. Örneğin bir birey kalemini diğer bir bireye satabilir.

**Birey - Firma (B-F : C-B)**: Bir bireyin bir firmaya yaptığı mal ve hizmet satış eylemidir.

**Birey - Kamu (B-K : C-A)**: Bir bireyin bir kamu kuruluşuna yaptığı mal ve hizmet satışı eylemidir.

**Kamu - Firma (K-F : A-B)**: Bir kamu kuruluşunun bir firmaya yaptığı mal satışı veya hizmet verme eylemidir.

**Kamu - Birey (K-B : A-C)**: Bir kamu kuruluşunun bireylere yaptığı mal satışı veya hizmet verme eylemidir.

**Doğrudan Birey (D-B : D-C)**: Bir üretici firmanın mal ve hizmetini müşteriye doğrudan satması eylemidir. Bu yöntemde üretici ile müşteri arasında, toptancı, dağıtıcı gibi ara kuruluşlar bulunmaz.

## Kaynaklar ve Önerilen Yayınlar

[1] V. Fryer, *The History of Commerce: From the Silk Road to Modern Ecommerce*, https://www.bigcommerce.com/blog/commerce/

[2] *Trade*, https://www.wkwand.com/en/Trade

[3] B. Uysal, N. H. Tanrısever, O. Düzel, *Avrupa Birliği Temel Terimler Sözlüğü*, 2003

[4] E. Adalı, *Göller Bölgesi*, 2010

# 2

# Elektronik Veri Aktarımı (EDI)

İnsanlar birbirleri ile iletişime geçmek için çeşitli yöntemler kullanmışlardır. XIX YY'da elektrik temelli dizgeler yeni iletişim olanakları sunmaya başlamıştır. Bu alanda geliştirilen ilk dizge telgraf adını alır. Telgraf basit bir elektrik devresidir. Devrede bir elektromıknatıs ve anahtar görevini gören bir maniple bulunur. Maniple devreyi kapattığında elektromıknatıs karşısındaki kolu çeker. Kolun ucundaki kalem yürüyen şerit üzerine değer ve çizmeye başlar. Maniplenin basılı tutulduğu sürece kağıt üzerine çizer. Telgraf dizgesi ile mesaj gönderebileceğini düşünen Samuel Morse, adıyla anılan abeceyi tasarlar ve bu abeceyi kullanan telgraf dizgesini 1935 yılında kurar. Dünyada ilk telgraf hattı 1844 yılında Washington, D.C. ile Baltimore, Maryland arasında kurulur. 1866 yılında ABD ile İslanda arasında Atlantik Okyanusu üzerinden ilk telgraf hattı kurulur. Telgrafın temel yapısı Şekil-2.1'de gösterilmiştir.


**Şekil-2.1:** Telgrafın temel yapısı

**Mors abecesi** uzun ve kısa (çizgi ve nokta) çizgilerden oluşur. Örneğin

T — A ·—

biçiminde yazılır.

Telgraf ağırlıklı olarak kamu ve askeri kuruluşlar tarafından kullanılmıştır. I. Dünya savaşının en önemli iletişim aracı olarak kabul edilir. Telgraf Türkiye'de 10 Eylül 1855'te kullanılmaya başlanmıştır.

İletişimdeki ikinci gelişme A. G. Bell'in telefonu icadıdır, (1876). Firmaların siparişlerini telefon üzerinden üreticiye bildirebilmeleri ticarete zaman kazandırmıştır. Telefon ile sağlanan iletişimin üç kusurundan söz edilebilir: $1^o$ Konuşmanın yanlış anlaşılması, $2^o$ Kimlik belirsizliği, $3^o$ Tarafların aynı anda çalışır olma koşulu.

Özellikle telefon altyapısının zayıf olduğu yerlerde, taraflar birbirini anlamakta zorluk çekerlerdi; bazen yanlış anlarlardı. Bu durum yanlış işlemlere neden olabiliyordu.

Telefon hatlarının bant genişliğinin yetersiz olduğu veya gürültülü hatlar, karşıda konuşan kişinin kimliğini anlamayı güçleştirir. Bu nedenle karşı tarafın kimliğinden şüphe edilir. Bu durum bazı kötü niyetlilerin firmaları kandırmasına neden olabilir.

İki tarafın telefonda konuşabilmeleri için iki tarafın da ayakta olması gerekir. Ülke içi ticarette sorun olmayan bu durum, uluslararası ticarette sorun olabilmektedir. Aralarında 12 saat fark olan iki kentteki firmaların birbiri ile konuşabilmeleri için ortak zaman dilimi ayarlamaları gerekmektedir.

Telefon üzerinden görüşmenin eksiklikleri teleks makinesinin icadı ile giderilmiştir. Teleks makinesi, daktiloya benzetilebilir. Bir daktilonun yazdıkları, uzaktaki bir daktilonun kâğıdı üzerinde görülür. Teleks makinesinin 1926 yılında Almanya'da geliştirildiği ve 1933 yılında hizmete sunulduğu bilinmektedir. Teleks makineleri, telefon altyapısına benzer bir altyapı üzerinden iletişime geçebiliyorlardı. Her teleks makinesinin tekil bir numarası vardı. Teleks makineleri arasındaki iletişim asenkron seri iletişimdi, ikili sayı düzeninde kodlanmış bir abece kullanıyorlardı. Teleks makineleri faks icat edilene dek yani 1990'lara kadar kullanılmıştır. İlk örnekleri dakikada yaklaşık 60 sözcük gönderebiliyordu.

**Şekil-2.2**: Örnek bir teleks makinesi

Faks makinesinin sağladığı faydalar şunlardır:

- Tarafların birbirini kandırması olasılığını kaldırmıştır.
- Zaman sorununu gidermiştir.
- Yadsımayı önlemiştir
- İletişim yazılı olduğu için yanlış anlaşılmaları önlemiştir.

Günümüzde belge iletme amacıyla faks (belge geçer) makineleri kullanılmaktadır. Ancak faks makineleri telefon hatlarını kullandığı için tekil ve yadsınamaz kimlikleri yoktur. Ayrıca belge üzerinde her türlü değişikliği yapmaya olanak sağlar. Bu nedenle yeterli güvenilirliği sağlamazlar. Faks makinelerinin bu güvenlik sorununu çözmek üzere güvenilir faks dizgeleri kurulmuştur.

## 2.1 Katma Değerli Ağ ve Elektronik Veri Aktarımı

Bilgisayarların kullanım sayıları artmaya başlayınca, önceleri büyük firmalar bilgisayar sahibi olmaya başladılar. Bilgisayar sayılarının artması, yeni bir fikrin doğmasına neden oldu. Bu yeni fikir bilgisayarlar arasında iletişimi sağlayacak bir ağın kurulması idi. Hedef, teleks makinesi yerine bilgisayarların birbirine bağlanması ve belgelerin bu ağ üzerinden aktarılması idi. Aslında fikrin asıl önemli özelliği bir bilgisayardaki belgeyi diğer bilgisayara, insan aracılığı olmadan aktarmaktı. Konuyu şöyle açıklayabiliriz:

- Bir taraf diğer tarafa bir sipariş belgesi göndermek istesin. Yapması gereken sipariş belgesini hazırlamak; bunu kağıda dökmek ve karşı tarafa iletmektir. Teleks makinesi kullanarak belgeyi karşı tarafın teleksi üzerinde yazdırabilir.
- Karşı tarafın mektup ya da teleks üzerinden gelen, kağıda yazılı sipariş belgesini okuyup buna yanıt hazırlaması gerekir. Gelen siparişlerin var olup olmadığını depo kayıtlarına bakarak dökecek ve sonucu bir belge olarak hazırlayacaktır. Hazırladığı yanıt belgeyi, sipariş veren tarafa mektup veya teleks üzerinden gönderebilir.
- Birinci taraf gelen yanıta bakarak değerlendirme yapacaktır.
- Konuyu biraz daha kapsamlı kılmak için, birinci tarafın sipariş belgesini birden çok firmaya gönderdiğini düşünelim. Bu durumda çok sayıda üreticiden gelen yanıtları birlikte değerlendirmesi gerekir. Bilgisayarı olduğunu varsayarsak, tüm yanıtları bilgisayarına girecek ve özel bir program aracılığı ile en uygun yanıtı belirlemeye çalışacaktır.

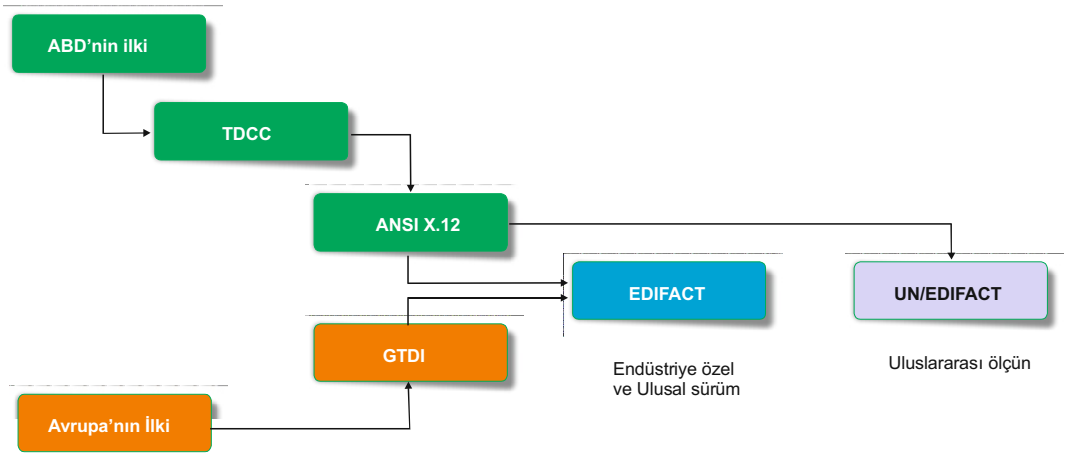
**Katma Değerli Ağ** (KDA veya VAN: Value Added Network) ve Elektronik Veri Aktarma (EVA veya EDI: Electronic Data Interchange) kavramı yukarıda anlatılan senaryoyu değiştirmeyi ve insan katkısını kaldırmayı hedeflemektedir. EVA'nın çalışması şöyle olacaktır:

- Müşteri sipariş belgesini bilgisayarında hazırlayacaktır. Hazırladığı belgeyi KDA üzerinden ürün sağlayıcılara gönderecektir.

- Müşterinin gönderdiği sipariş belgesi doğrudan ürün sağlayıcıların bilgisayarına yüklenecektir. Ürün sağlayıcı, gelen siparişin yanıtını hazırlarken veri tabanındaki bilgilerden yararlanacak ve yanıt belgesini bilgisayarda hazırlayacaktır. Ardından hazırladığı yanıt belgesini KDA üzerinden müşteriye gönderecektir.
- Müşteri çok sayıda ürün sağlayıcıdan gelen yanıtları bilgisayarında bulacaktır ve bu yanıtları değerlendirmek üzere kullandığı özel programı kullanarak en uygun teklifi belirleyecektir.

Yukarıda anlatılan kavramın çalışabilmesi için bazı ölçünlerin belirlenmesi gerekir. İlk ölçün kullanılacak abecedir. İkinci ölçün sipariş ve teklif belgelerinin kalıbının belirlenmesi olacaktır. EVA (EDI) bu nedenle gündeme gelmiştir. EDI kavramını ilk olarak 1960'lı yıllarda Ed Guilbert önermiş ve EDI anlamında ilk belge 1965 yılında Hollanda-Amerikan gemi taşımacılık şirketi tarafından gönderilmiştir. Belge teleks makinesi üzerinden gönderilmiştir. Teleks makinesinin şerit delicisinden çıkan delikli şerit bilgisayara yüklenmiştir. 1968 yılında demiryolu taşımacı şirketler bir araya gelerek Transportation Data Coordinating Committe (TDCC) kurulmuştur. Bu heyetin amacı ölçünlü EDI belgelerini hazırlamaktı.

1973 yılında, bilgisayarlar arası dosya aktarımı için FTP (File Transfer Protocol) yayımlandı. 1975' te TDCC Guilbet'in katkılarıyla ilk EDI ölçününü yayımladı. Aynı yıl KDA ve Telenet kuruldu. 1978'de TDCC adını EDIA (Electronic Data Interchange Association) olarak değiştirdi. 1985 yılında Birleşmiş Milletler UN/EDIFACT (Electronic Data Interchange for Administration, Commerce and Transport) ölçünlerini hazırlayarak ölçünleri uluslararasılaştırdı. EDI ile ilgili gelişmeler Şekil-2.3'te gösterilmiştir.




**Şekil-2.3**: EDIFACT ve UN/EDIFACT'ın oluşumu

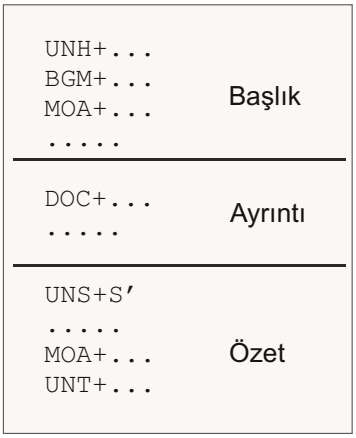
## 2.1.1 EDIFACT

EDIFACT ölçününde her bir belgeye bir ad verilmiştir. Belge adları, belgeyi çağrıştıracak biçimde 6 harf olarak belirlenmiştir. Örneğin

- ORDERS : Purchase Orders : Sipariş belgesi
- CUSDEC : Customs Declaration : Gümrük beyannamesi
- IFTMIN : Instruction Message : Yönerge
- INVOIC : Invoices : Fatura
- PAYORD : Payment Order : Ödeme emri

### 2.1.1.1 Bölüt Yapısı

Bir belge tanımlı alan içine yerleştirilmiş bölütlerden oluşur. Bazı bölütler birden fazla alanda kullanılabilirler. Her alanda kullanılabilecek bölütler EDIFACT kaynaklarında tanımlanmıştır. EDIFACT belgesi sıradüzensel yapıda düzenlenir. Bir belge üç alandan oluşur: 1° Başlık, 2° Ayrıntı ve 3° Özet. Bir belge, *Belge Bölütü* (UNH) ile başlar, *Belge Sonu Bölütü* (UNT) ile biter. Şekil-2.4'te bir EDIFACT belgesinin ana yapısı gösterilmiştir.




**Şekil-2.4**: Bir EDIFACT belge yapısı

Bir bölüt ilgili alanda kullanılıyor ise o alan içinde kullanılır. Bazı bölüt zorunlu (M) veya koşullu (C) olabilir. Zorunlu olan bölüt ilgili alanda en az bir kez yer almalıdır. Koşullu bölüt, gerektiğinde kullanılır. Bölüt çizelgesi, bir bölütün kaç kez kullanıldığını da açıklar. Şekil-2.5'te Ödeme Emri ile ilgili bir örnek verilmiştir.

| Konum | Etiket | Ad | Ger | Yine |
|---|---|---|---|---|
| 0010 | UNH | Belge başlığı | M | 1 |
| 0020 | BGM | Belgenin başlangıcı | M | 1 |
| 0030 | BUS | Ticari işlevi | C | 1 |
| 0040 | DTM | Tarih/zaman/süre | M | 4 |
| 0060 | RFF | Kaynak | M | 1 |
| 0070 | DTM | Tarih/zaman/süre | C | 1 |
| 0080 | FTX | Düz yazı | C | 5 |
| 0090 | PAI | Ödeme yönergesi | C | 1 |
| 0100 | FCA | Mali masraf tahsisi | C | 1 |
| 0120 | MOA | Parasal değer | M | 1 |
| 0130 | CUX | Para birimi | C | 1 |
| 0140 | DTM | Tarih/zaman/süre | C | 2 |
| 0150 | RFF | Kaynak | C | 1 |

**Şekil-2.5**: Bölütler ile ilgili örnekler

### 2.1.1.2 Bölüt Kümeleri

Bölütler kümelenmiş olarak yinelenirler ise bunlara bölüt kümeleri adı verilir. Şekil-2.6'da bölüt kümelerine ilişkin örnek verilmiştir.

Bölüt kümeleri iç içe olabilir. Bu durum bölüt kümelerinin, bir bölüt kümesinin içinde olduğu anlamına gelir.

Şekil-2.7'de iç içe yerleşmiş bölüt kümeleri gösterilmiştir.

7. bölüt kümesinin (CUX, DTM) bölütleri ve 8. bölüt kümesinin (AJT, MOA, RFF) bölütleri, 6. bölüt kümesinin içinde yer almaktadırlar.

| Konum | Etiket | Ad | Ger | Yine |
|---|---|---|---|---|
| 0010 | UNH | Belge başlığı | M | 1 |
| 0020 | BGM | Belgenin başlangıcı | M | 1 |
| 0030 | BUS | Ticari işlevi | C | 1 |
| 0040 | DTM | Tarih/zaman/süre | M | 4 |
| 0050 | | Bölüt kümesi 1 | C | 2 |
| 0060 | RFF | Kaynak | M | 1 |
| 0070 | DTM | Tarih/zaman/süre | C | 1 |
| 0080 | FTX | Düz yazı | C | 5 |
| 0090 | PAI | Ödeme yönergesi | C | 1 |
| 0100 | FCA | Mali masraf tahsisi | C | 1 |
| 0110 | | Bölüt kümesi 2 | C | 2 |
| 0120 | MOA | Parasal değer | M | 1 |
| 0130 | CUX | Para birimi | C | 1 |
| 0140 | DTM | Tarih/zaman/süre | C | 2 |
| 0150 | RFF | Kaynak | C | 1 |

**Şekil-2.6**: Bölüt kümeleri

### 2.1.1.3 Bölütler

Bir bölüt sabit tanımlanmış bir sıradaki mantıksal olarak ilişkili veri ögelerinin dermesidir. Bir bölüt şunları içerir:

- Bölütü tanımlayan üç karakterli harf ve sayılardan oluşan bir kot. Buna bölüt etiketi denir.
- Değişken uzunluklu veri ögeleri. Bunlar basit veya bileşik olabilir.

| Konum | Etiket | Ad | Ger | Yine |
|---|---|---|---|---|
| 0280 | | Bölüt kümesi 6 | C | 9999 |
| 0290 | UNH | Belge başlığı | M | 1 |
| 0310 | DTM | Tarih/zaman/süre | C | 5 |
| 0320 | RFF | Kaynak | C | 5 |
| 0330 | NAD | Ad ve adres | C | 1 |
| 0340 | | Bölüt kümesi 7 | C | 5 |
| 0350 | CUX | Para birimi | M | 1 |
| 0360 | DTM | Tarih/zaman/süre | C | 1 |
| 0370 | | Bölüt kümesi 8 | C | 100 |
| 0380 | AJT | Düzeltme ayrıntısı | M | 1 |
| 0390 | MOA | Para değeri | C | 1 |
| 0400 | RFF | Kaynak | C | 1 |

**Şekil-2.7**: İç içe bölüt kümeleri

Bölütler, bir veri ögesi ayırıcısı (veri ögesi sınırlayıcı) ile ayrılmalıdır. Veri ögesi ayırıcı + and : , and biçiminde olabilir.

Tüm bölütler, BM'nin Ticaret Veri Değişim Rehberi'nde (UNTDID) bulunmaktadır. Bu çizelgelerde bölüt konumu, bölüt etiketi ve bölüt adı yer alır. Bölüt çizelgeleri ayrıca bölütün zorunlu (M) veya koşullu (C) olduğunu ve kaç kez yineleneceğini gösterir.

EDIFACT'ta iki tür bölüt vardır:

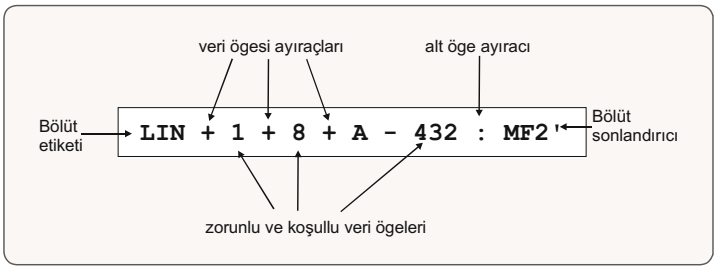
- Hizmet Bölütleri
- Genel Bölütler

Hizmet bölütleri şunlardır:

- Zarflar : `UNB-UNZ, UNG-UNE, UNH-UNT`
- Sınırlayıcı Dizesi Önerisi : `UNA`
- Bölüm Ayırıcı : `UNS`

Genel bölütler şunlardır:

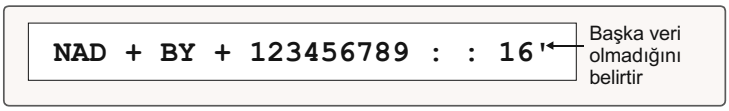
- Belgeleri tanımlamak ve belirlemek için : `DOC`
- Parasal tutarlar için : `MOA`
- Tarihler ve saatler için : `DTM`
- Ad ve adres verileri için : `NAD`



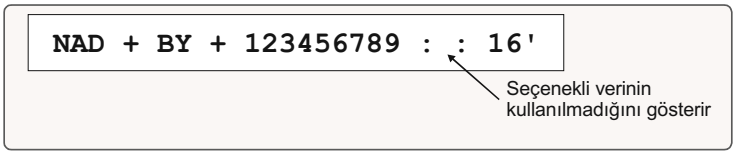

**Şekil-2.8**: Bir bölüt örneği

### 2.1.1.4 Bölüt Sonlandırıcı ve Ayırıcılar

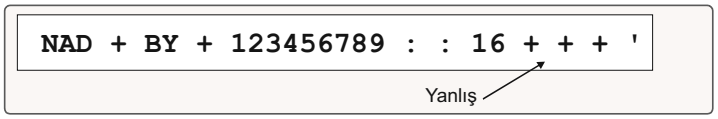
Her bölütün sonu "Veri Bölütü Sonlandırıcı" tarafından belirlenir. EDIFACT'ta ölçünlü veri bölütü sonlandırıcısı " ' " dır.



Seçimli veya koşullu veri ögeleri konumlarına göre hesaba katılmalıdır.




Ancak, veri bölütünün sonunda bulunan, veri içermeyen seçimli veya koşullu veri ögeleri, verileri doğru şekilde konumlandırmak için ek veri ögesi ayracı gerektirmezler.




### 2.1.1.5 Dönüştürme

EDIFACT kullanılmaya başlamadan önce, her işletmenin stok izleme, fatura, ödemeler ile ilgili kendi programları olduğu biliniyordu. Ancak;

- Bir işletmenin bilgisayarındaki program diğer işletmenin programı ile konuşamıyordu. Bir işletmenin bilgisayarında hazırlanan bir belgenin verileri, diğer işletme tarafından alındığında bu işletmenin bilgisayarına yeniden girilmesi gerekiyordu.
- Bir işletmenin bir bölümünde kullanılan programın ürettiği veriler, aynı işletmenin bir başka bölümünde kullanılan program tarafından okunamıyordu.

Dolayısıyla verilerin tekrar girilmesi gerekiyordu. Bu sorunun çözümü, belli belgelerin ürettiği verileri ölçünlü bir kalıba yerleştirmekti. Bu EDI kavramının doğmasına neden olan sorundu. Şekil-2.9'da insan tarafından okunabilen bir sipariş belgesi ve Şekil-2.10'da buna karşılık gelen EDI belgesi gösterilmiştir.

| ADET | BİRİM | No | AÇIKLAMA | FİYAT |
|---|---|---|---|---|
| 3 | KUTU | 5253 | KURŞUN KALEM | 1,25 |
| 5 | TEK | MET4 | KARELİ DEFTER | 8,45 |
| 12 | TEK | 124C | SİLGİ | 2,30 |

**Şekil-2.9**: İnsan tarafından okunabilir sipariş belgesi

```
LIN+1++5253:MF'
IMD+F++:::KURŞUN KALEM'
QTY+21:3:CA'
PRI+CAL+1,25'

LIN+2++MET4:MF'
IMD+F++:::KARELİ DEFTER'
QTY+21:5:EA'
PRI+CAL+8,45'

LIN+3++124C:MF'
IMD+F++:::SİLGİ'
QTY+21:12:EA'
PRI+CAL+2,30'
```

**Şekil-2.10**: Sipariş belgesinin EDIFACT karşılığı

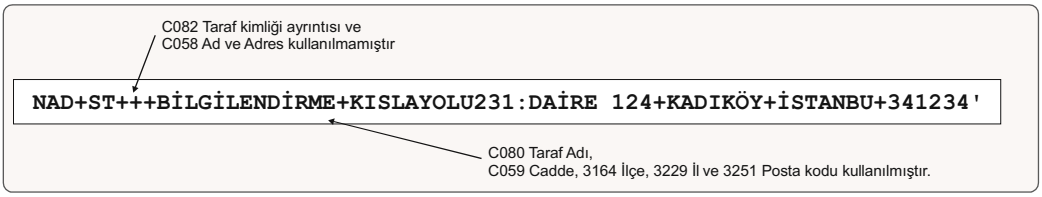
### 2.1.1.6 Basit ve Bileşik Veri Ögeleri

Basit bir veri ögesi bir bilgi içerirken bileşik veri ögesi genellikle niteleyiciler içeren birden fazla bilgi parçası içerir.

EDIFACT'ta, tüm zorunlu veri ögeleri veri içermelidir. Koşullu veri ögeleri iletimin gereksinimlerine bağlı olarak veri içerebilir veya içermez.

Veri ögeleri, bölütteki konumlarına göre hesaba katıldıklarından, eğer seçimli veya koşullu veri ögesi veri içermiyorsa bu veri ögesi, gereken sayıda veri ögesi ayracı kullanılarak, yine de bölütteki konumuna göre hesaba katılmalıdır.

Basit ve bileşik veri ögelerine ilişkin örnek Şekil-2.11'de gösterilmiştir.




**Şekil-2.11**: Basit ve bileşik veri ögeleri için bir örnek

Veri ögesi türlerinin listesi ve bunlar için geçerli olan kurallar aşağıda verilmiştir:

**Sayısal**

Sayısal bir bölüt yalnızca rakamlar, bir ondalık nokta (virgül) ve eksi ise bir eksi işareti içerebilir.

Sayı ondalık sayı olarak verilmişse, noktadan (virgül) önce ve sonra bir rakam içermelidir. Örneğin: 2.0 doğrudur, ancak 2. yanlıştır. 0.50 doğrudur , .50 yanlıştır.

**Abecesel**

Abecesel bir bölüt, boşluk dahil olmak üzere, belirtilen sayıda harf içerir.

Farklı veri ögelerinin de uymaları gereken belirli kurallar vardır. Veri ögesi sözcesi veri ögesi adında genellikle kodları, "kodlanmış (coded)" veya "niteleyici (qualifier)" sözcüklerini kullanarak belirtir.

```
6345   Para birimi,  coded          C  an..3
6343   Para birimi qualifier        C  an..3
```

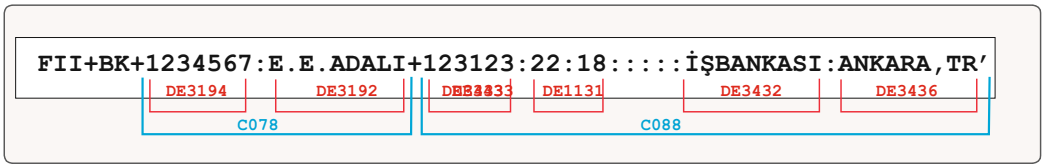
## 2.1.1.7 Bileşik Veri Ögeleri: Niteleyici ve Değer

EDIFACT'ta, bileşik veri ögesi iki veya daha fazla veri parçasından oluşur (bileşenler olarak bilinir). İlk veri ögesi nitelendirilmiş bir değerdir. İkinci veri ögesi niteleyicidir. Bileşik veri ögelerine ilişkin örnekler Şekil-2.12'de verilmiştir.

```
3035     Taraf Niteleyici                 M   an..3

C078     Hesap kimliği                    C
   3194  Hesap sahibinin numarası         C   an..17
   3192  Hesap sahibinin adı              C   an..35
   3192  Hesap sahibinin adı              C   an..35
   6345  Para birim, kodlanmış           C   an..3

C088     Kuruluş kimliği                  C
   3433  Kuruluş adı kimliği              C   an..11
   1131  Kod listesi niteleyicisi         C   an..3
   3055  Kod listesi sorumlusu, kodlanmış C  an..3
   3434  Kuruluş şube numarası            C   an..17
   3131  Kod listesi niteleyicisi         C   an..3
   3055  Kod listesi sorumlusu, kodlanmış C  an..3
   3432  Kuruluş adı                      C   an..70
   3436  Kuruluş şube yeri                C   an..17

3207     Ülke, kodlanmış                  C   an..3
```

**Şekil-2.12**: Bileşik veri ögeleri için örnek

3035 bileşik ögesinin EDIFACT belgesine dönüşmüş biçimi Şekil-2.13'te gösterilmiştir.

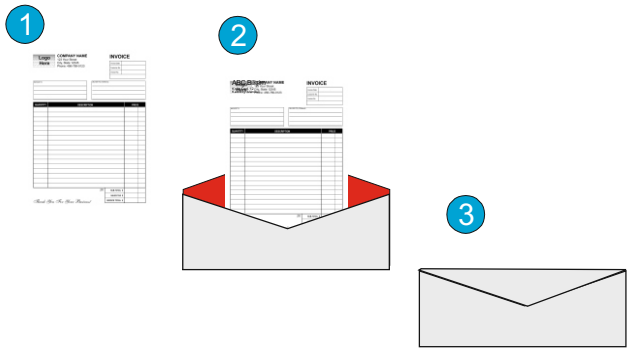



**Şekil-2.13**: 3035 bileşik ögesinin EDIFACT belgesine dönüşmüş biçimi

(C078 ve C088) bileşik veri ögeleri bölüt çizelgesindeki çeşitli koşullu bileşenlerden oluşur. Koşullu olduklarından, tüm veri ögeleri kullanılmaz. Her öge bir alt öge niteleyicisi ":" ile ayrılır.

### 2.1.1.8 Belge Yapısı ve Elektronik Zarflama

Bir belgenin EDIFACT karşılığı hazırlandıktan sonra elektronik olarak zarfa konup gönderilmesi aşamasına geçilir. Süreç Şekil-2.14'te gösterilmiştir. Zarflama sırasında, düzey ve kullanılan karakter sınıfının belirtilmesi gerekir. EDIFACT belgelerinin iletilebileceği iki düzey vardır, bunlar Düzey A ve Düzey B olarak adlandırılmıştır.




**Şekil-2.14**: Bir belgenin zarflanması

**Düzey A (UNA)**: Yalnızca büyük harfler ve yalnızca basılabilen karakterler içerir.

**Düzey B (UNB)**: Büyük ve küçük harfler ile ayraçlar ve yazdırılmayan karakterleri içerir.

UNB iletişim bölütünden önce UNA 9 karakterlik bir dizi gönderir. UNA'nın kullanımı seçimliktir; kullanılmadığında, hazır olan ve Şekil-2.15'te görülen varsayımlar geçerli olur.

| | Düzey A | Düzey B | |
|---|---|---|---|
| Karakter-1 | : | IS1 | alt öge ayracı |
| Karakter-2 | + | IS3 | veri öge ayracı |
| Karakter-3 | ,or, | aynı | ondalık nokta (virgül) belirteci |
| Karakter-4 | ? | kullanılmaz | aralık kullanılmadığında bırakma karakteri |
| Karakter-5 | yedek | yedek | aralık |
| Karakter-6 | ` | IS4 | bölüt sonlandırıcı |

**Şekil-2.15**: UNA için varsayılan değerler

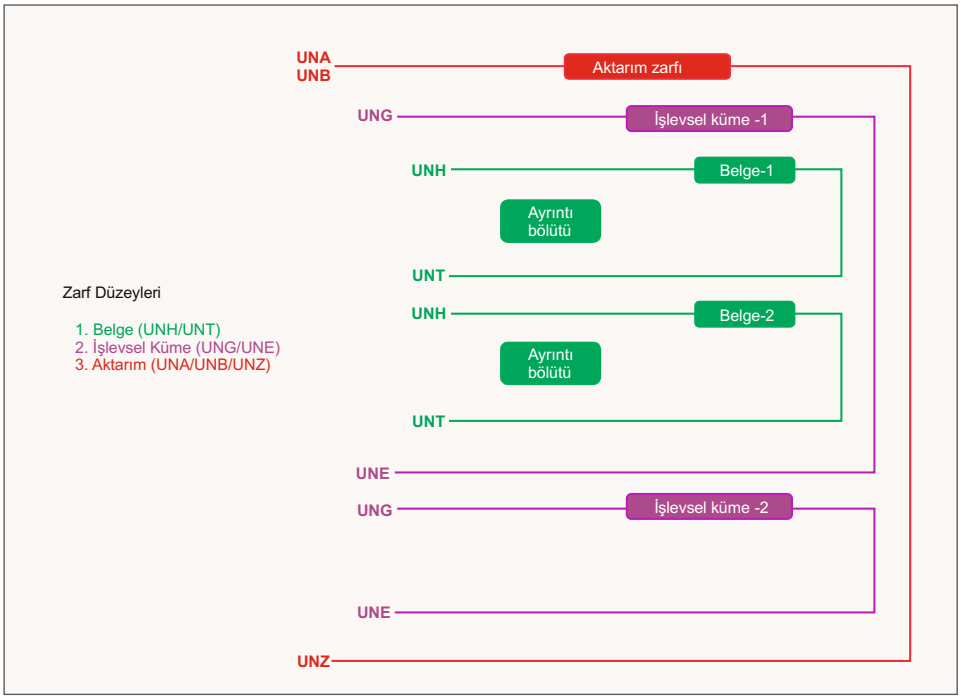
EDIFACT'da gerekli olan iki zarf düzeyi vardır ve bunlar:

- **Aktarma (UNB / UNZ)**: Bir gönderenin posta kutusu adresinden diğer gönderenin posta kutusu adresi
- **Belge (UNH / UNT)**: Belirli bir mesajın zarfı

Ek olarak, isteğe bağlı zarf düzeyi daha vardır:

- **İşlevsel Küme (UNG / UNE)**: İşletmenin alt adresleri belirtmek için kullanılır

EDIFACT elektronik zarflama kalıbı Şekil-2.16'da gösterilmiştir.




**Şekil-2.16**: EDIFACT elektronik zarflama kalıbı

### 2.1.1.9 Belge Zarfı

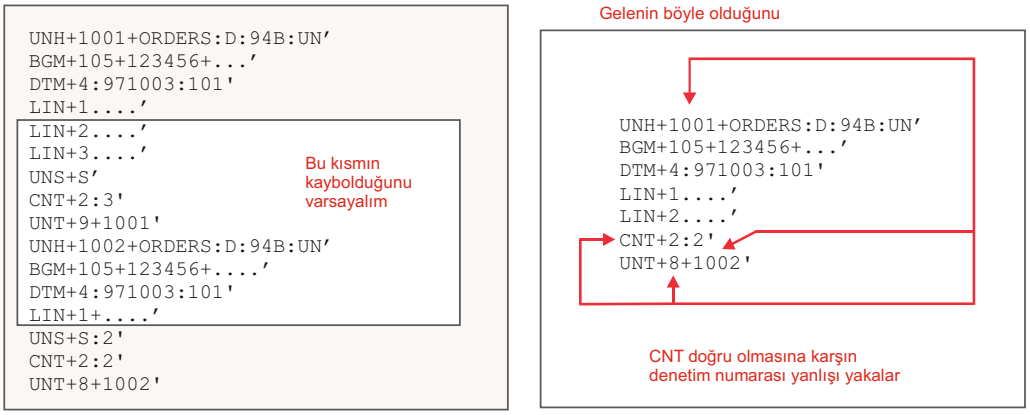
En içte görülen zarf düzeyi her belgeyi zarf içine alır. Başlangıcı UNH ve sonunu UNT bölütleri belirtir. UNH bölütünün dört veri ögesi vardır:

- **Belge Numarası** (M): Gönderenin bilgisayarı tarafından atanır ve denetim amacıyla kullanılır.
- **Belge Tanımlayıcı** (M): Zarflanmakta olan belgeyi tanımlayan altı karakterli mesaj adı (örneğin. PAYEXT, REMADV) ve Sürüm / Yayın verileri.
- **Ortak Erişim Numarası** (C): Birden çok işlemi birbiriyle ilişkilendirir.
- **Aktarımın Durumu** (C): İlgili mesajın sırasıdır.

UNT bölütünün iki veri ögesi vardır:

- **Bir Belgedeki Bölüt** (M): Belgedeki bölüt sayısıdır. UNH ve UNT'yi de içerir.
- **Belge Numarası** (M): Aynı belgede, UNH içinde kullanılan numara ile aynıdır.

UNH ögesindeki denetim yapısının, bir belgenin doğrulanmasında nasıl kullanıldığı Şekil-2.17'de gösterilmiştir.




**Şekil-2.17**: Bir belgenin doğrulanmasında UNH'nın nasıl kullanıldığına örnek

Ortak Erişim Numarası ilgili EDIFACT'ı tanımlamak için kullanılır. Örneğin, bir sipariş işlemi sırasıyla dört belge gerektirebilir. Bu dört belge aşağıdaki sırada olabilir.

- ORDERS : Sipariş
- DESADV : Alındı bilgisi
- INVOIC : Fatura
- REMADV : Havale bilgisi

Bu dört belgenin ortak erişim numarası olması gerekir. Ortak erişim numarasının nasıl kullanıldığı aşağıda gösterilmiştir.

- Sipariş: `UNH+2348+ORDERS:D:94B:UN+10381+1:C'`
- Alındı bilgisi: `UNH+156009+DESADV:D:94B:UN+10381+2'`
- Fatura: `UNH+156078+INVOIC:D:94B:UN+10381+3'`
- Havale bilgisi: `UNH+2451+REMADV:D:94B:UN+10381+4:F'`

### 2.1.1.10 İşlevsel Küme Zarfı

İkinci zarf düzeyi işlev kümeleri barındırır. Başlangıcı UNG ve sonu UNE bölütleri tarafından tanımlanır. Aşağıda işlevsel küme içinde bulunan veri ögelerine ilişkin örnekler verilmiştir.

- İşlevsel Küme (M)
- Belge Tanımlayıcı (M)
- Tarih / Saat Damgası (M): Birden çok işlemi birbiriyle ilişkilendirir.
- Aktarım Durumu (C): İlgili belgeleri sıralar.
- Küme Numarası (M)
- Denetim Kurumu (M)
- Belge Sürümü (M)

- Uygulama Parolası (C)

UNE bölütü şunları içerir:

- Bir Belgedeki Bölüt (M)
- Belge Numarası (M)

### 2.1.1.11 Aktarım Zarfı

Aktarım zarfı belge zarf yapısının en dış düzeyidir. Gönderenden alıcıya aktarılan veriyi belirtir. UNA bölütü aşağıdakileri içerir.

- Ayraç Dizisi Bilgisi
- İçerilen veri ögeleri

UNB bölütü aşağıdakileri içerir:

- Tarih/Zaman Damgası (M)
- Aktarma Denetim Numarası (M)
- Parola ve Uygulamanın Kaynağı (C)
- Sürecin Önceliği (C)
- Onaylandı Gereksinimi Belirteci (C)
- İletişim Anlaşması Kimliği (C)
- Sınama Belirteci (C)

UNZ bölütü aşağıdakileri içerir:

- Aktarma Denetim Numarası (M)
- Belge veya Aktarmadaki Küme Sayısı

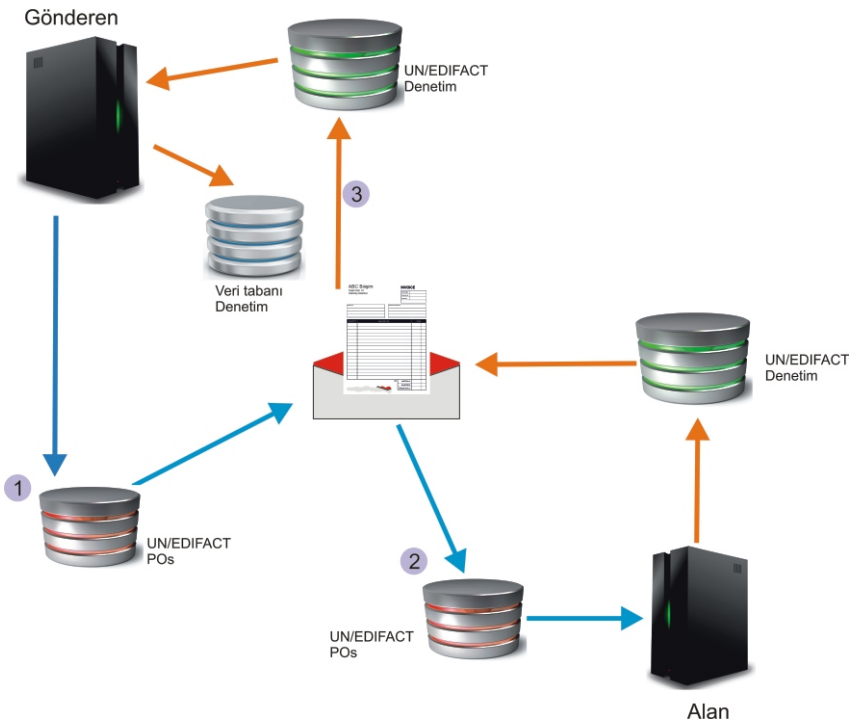
### 2.1.1.12 Denetim Belgesi

Belgeyi alan bilgisayar yazım yanlışlarını ve denetim sayılarını denetlemelidir. Bu denetim sonunda, gönderen tarafa onay belgesi göndermelidir. Bu süreç Şekil-2.18'de gösterilmiştir. Şekil-2.18'deki aşamalar aşağıda açıklanmıştır:

1- Gönderen taraf, dosyayı hazırlarken, denetim ve izleme bilgilerini elektronik zarfın içine ekler.

2- Alıcı tarafın bilgisayarı gelen PO's'ları (PO's: Purchase Order: Satış Siparişleri) aldığında denetim bilgileri gözden geçirir; eğer doğru ise gönderen tarafa onay belgesi gönderir.

3- Gönderen tarafın bilgisayarı Denetim belgesini alır, ardından belgenin durumunu günceller.




**Şekil-2.18**: UN/EDIFACT denetim süreci

# Kaynaklar ve Önerilen Yayınlar

[1] *EDIFACT EDI Document Standard | EDI Basics* ,
https://www.edibasics.com/edi-resources/document-standards/edifact/

[2] *EDIFACT Standards Overview Tutorial,* https://www.gxs.co.uk/wp-content/uploads/tutorial_edifact.pdf

[3] *UNECE / Introducton* , https://unece.org/trade/uncefact/unedfact-part-1-ntroducton

[4] *UNCID - Chapter 1. Introductory Note*,
https://unece.org/trade/uncefact/unedfact/part-2-chapter-1-ntroductory-note

[5] *UN/EDIFACT DRAFT DIRECTORY* , https://unece.org/DAM/trade/untdd/texts/d424_d.htm

# 3

# Ticaret Araçları

Ticaretin temel araçlarından biri para, diğeri ölçmedir. Paranın gelişimi bir önceki bölümde anlatılmıştı. Ticareti yapılan mala parasal bir değer biçebilmek için bu malın ölçülmesi gerekir. Ölçme, ürün veya malın türüne göre değişebilir. Bazıları tartılır, bazılarının boyu, bazılarının yüzeyi ölçülür. Ölçü araçlarının doğruluğu ülke yöneticileri tarafından denetlenir.

Günümüzde özellikle bilişim sistemlerinin gelişmesi ticarete yeni araçların girmesini sağlamıştır. Bu araçların içinde banka ve kredi kartı, kart okuyucular, çizgi yazısı önemli yer tutmaktadır. Bu bölümde sırasıyla;

- Ölçü sistemleri
- Kredi kartları
- Çizgi yazısı ve
- RFID etiket

tanıtılacaktır.

## 3.1 Ölçü Birimleri

En ilkel ticaretin uygulandığı zamanlarda bile değiş tokuşun ölçüldüğü bilinmektedir. Bazı nesneler sayılarak ölçülüyordu, örneğin sığırlar, çakmak taşları, obsidiyen taşları, istiridye kabukları gibi. Bazı ürünler hacim olarak ölçülüyordu, örneğin tahıllar çuval, ambar veya şinik ile ölçülüyordu. Kumaşlar uzunlukları ölçülerek satılırdı. Ağırlık ölçme yöntemlerinin daha sonra kullanılmaya başlandığı düşünülmektedir.

Uluslararası işbirliklerinin az olduğu dönemlerde, her ülke kendine göre ölçme yöntemleri ve ölçünleri oluşturmuştur. Bu yöntemlerden bazıları bilimsel kurallara uygun bazıları değildir. Konuya açıklık getirmek için bazı örnekler verip tartışmak yerinde olabilir.

### Çin Ölçü Sistemi

Ölçü biriminin ilk olarak Sarı İmparatorluk döneminde kullanıldığı *Book of Rites*'de görülmektedir. Ölçü sisteminin insan vücudundan esinlendiği aynı kaynakta belirtilmektedir. Ancak insan vücut ölçülerinin değişken olması nedeniyle Shan Hanedanlığının mezarlarından ölçü birimi oluşturuldu.

Eski Çin uzunluk ölçü birimleri *chi*, *bu* ve *li* dir. Bu birimler arasında oranlar 5 veya 6 kattır. Çizelge-3.1'de bazı örnekler verilmiştir.

**Çizelge-3.1: Tarihi Çin Uzunluk Ölçüleri (sayılar metre karşılığıdır)[2]**

| Hanedan | chi | bu | | li | |
|---|---|---|---|---|---|
| | | =5 chi | =6 chi | =300 bu | =360 bu |
| Shan | 0,1675 | | 1,0050 | 301,50 | |
| Zhou | 0,1990 | | 1,1940 | 358,20 | |
| Qin | 0,2310 | | 1,3860 | 415,80 | |
| Tang | 0,2465 | 1,2325 | | 369,75 | 443,70 |

Çizelge-3.1'den görüldüğü gibi, ölçü biriminin boyu zaman içinde hanedanlığın kararı ile değişebilmektedir. Çinliler onluk sayı düzenini kullanmalarına karşın üç uzunluk birimi arasındaki oran da onluk yapıda değildir.

Uzakdoğu ülkelerinde (Çin, Japonya, Moğolistan ve Türki devletler) geçmişte ve bazılarında günümüzde kullanılan takvim ay ve güneşe bağımlı bir takvimdir. Eski Çin takvimi adı verilen bu takvimde yılda 12 veya 13 ay olabilir. Aylar 29 veya 30 gün çekebilir. Dolayısıyla 12 ay içeren yıl 354 veya 355, 13 ay olan yıl 383 veya 384 gün olabilir.

## Osmanlı Ölçü Sistemi

Osmanlı İmparatorluğu 1875 yılında Metre Anlaşması'nı imza etmeden önce kendisine özgü ölçü sistemleri kullanmıştır. Osmanlı uzunluk, ağırlık ve hacim ölçü birimleri sırasıyla Çizelge-3.2, 3.3 ve 3.4'te gösterilmiştir.

**Çizelge-3.2: Osmanlı Uzunluk Ölçüleri**

| Birimin adı | Eşdeğeri | Metrik karşılığı |
|---|---|---|
| nokta | | 0,219 mm |
| hat | 12 nokta | 2,63 mm |
| parmak | 12 hat | 31,57 mm |
| kerrab veya kirab | | 42,5 mm |
| rubu veya urup | 2 kerrab | 85 mm |
| ayak veya kadem | 12 parmak | 378,87 mm |
| endaze | | 650 mm |
| arşın | | 680 mm |
| zirai arşın | 2 ayak | 757,74 mm |
| kulaç | | 757,74 |
| berid veya menzil | 600 ayak | 227 m |
| eski mil | 5000 ayak | 1.8288 m |
| fersah | 3 eski mil | 5,685 m |
| merhale | 200 berid | 45,48 Km |

**Çizelge-3.3: Osmanlı Ağırlık Ölçüler**

| Birimin adı | Eşdeğeri | Metrik karşılığı |
|---|---|---|
| kırat | | 0,2004 g |
| dirhem | 16 kırat | 3,207 g |
| okka | 400 dirhem | 1,282 Kg |
| miskal | 1,5 dirhem | 42,5 mm |
| batman | 6 okka | 7,697 Kg |
| kantar | | 56,447 Kg |
| çeki | 4 kantar | 225,789 Kg |

**Çizelge-3.4: Osmanlı Hacim Ölçüleri**

| Birimin adı | Eşdeğeri | Metrik karşılığı |
|---|---|---|
| şinik | | 9,25 litre |
| kile | 4 şinik | 37 litre |

Osmanlı ölçü birimleri incelendiğinde göze çarpan sonuçlar şunlardır: İmparatorluğun farklı yörelerinde, daha önce kullanılmış olan ölçü birimlerinin kullanılmaya devam edildiği görülmektedir. Dolayısıyla bazı ölçü birimleri arasında oransal bir ilişki görülmemektedir. Aralarında oransal ilişki olan birimlerin arasındaki ilişki 2, 3, 5 ve 12 olarak görülmektedir. 12'lik sayı düzenini Sümerlerin kullanıldığı, dolayısıyla Orta Doğuda kullanılmasının olağan olduğu değerlendirilmektedir.

Uzunluk ölçü birimi olarak kullanılan arşın, devletin kasasında saklanan ölçün arşın kaynak alınarak çoğaltılırdı. Saklanan arşın sert bir ağaç olan abanozdan yapılırdı. Endaze, ülkede yaşanan enflasyonu örtmek üzere uydurulmuş bir uzunluk ölçüsüdür. İpek kumaşın bir arşını ... akçeye satılırken, ipek kumaşının fiyatını artmış göstermemek üzere arşının boyu kısaltılarak endaze ile ölçülmeye başlanmıştır.

Hacim ölçüsü olarak kullanılan şinik hacmi belli olan bir tencere gibi düşünülebilir. Sıvıların ölçülmesinde sıkıntı yaratmamasına karşın, tahılların ölçülmesine uygun bir araç olduğu söylenemez.

Osmanlı'da yetkililerin, pazarları gezerek kullanılan ölçü araçlarının doğru olup olmadığını denetledikleri bilinmektedir. Ayrıca ölçü birimlerinin ilgili kurum tarafından onaylanıp mühürlendiği de bilinmektedir.

Osmanlılar, İslamiyeti kabul ettikten sonra İslami takvim kullanmaya başlamışlardır. Bu takvimin başlangıç günü 622 yılındaki Hicret olayıdır. İslami takvim, 12 ay içeren ve Ayın hareketlerine göre hesaplanan bir takvimdir. Dünyanın gerçek yılına göre 11 gün kısadır, bilimsel değildir ve ayların başlangıç zamanları kaymaktadır. Bu nedenle 1839 yılında güneş temelli Rumi takvim kullanılmaya başlanmıştır. 1925 yılından sonra Türkiye'de Gregoryan takvim kullanılmaya başlanmıştır.

Osmanlı'da gün 24 saatlik zaman birimi kullanılırdı ve saatin başlangıç anı akşam ezanıydı, yani her akşam ezanı okunduğunda saat 12 olurdu. Günlerin yıl içinde uzayıp kısaldığı bilindiğine göre, saatlerin belli aralıklar ile ayarlanması gerekirdi.

## İngiliz Ölçü Sistemi

İngilizlerin ve eski İngiliz sömürgelerinin hâlâ kullanmaya devam ettikleri İngiliz ölçü sistemine ilişkin bazı örnekler Çizelge-3.5, 3.6 ve 3.7'de verilmiştir.

İngilizler kendilerine özgü ölçü sistemi geliştirmişler ancak bunun bir sistem olarak anılması zordur. Büyüklükler arası oransal ilişkiler çok tutarsızdır.

**Çizelge-3.5: İngiliz Uzunluk Ölçüleri**

| Birimin adı | Eşdeğeri | Metrik karşılığı |
|---|---|---|
| thou (th) | 1/12.000 feet | 0,0254 mm |
| inch (in) | 1/12 feet | 25,4 mm |
| foot | | 304,8 mm |
| yard | 3 feet | 914,4 mm |
| fathom | 6,0761 feet | 1852 mm |
| cable | 100 fathom | 185,2 m |
| nautical mile | 10 cable | 1.852 m |

**Çizelge-3.6: İngiliz Ağırlık Ölçüleri**

| Birimin adı | Eşdeğeri (pound) | Metrik karşılığı |
|---|---|---|
| grain | 1/7000 | 0,064 g |
| drachm | 1/256 | 1,771 g |
| ounce | 1/16 | 28,349 |
| pound | 1 | 453,5 g |
| stone | 14 | 6,350 Kg |
| quarter | 28 | 12,700 Kg |
| ton | 2240 | 1.016 Kg |

**Çizelge-3.7: İngiliz Hacim Ölçüleri (sıvılar için)**

| Birimin adı | Eşdeğeri | Metrik karşılığı |
|---|---|---|
| gill | 1/4 pint | 141,6 ml |
| pint | | 569,6 ml |
| gallon | 1/2 peck | 4,54 l |

## Metrik Sistem

Onluk sayı düzenine uygun olarak 1870 yılında Fransa'da geliştirilmiş ölçü sistemidir. Uluslararası Birimler Sistemi (International System of Unit- SI) olarak kabul edilir. Osmanlı metrik sistemini 1875 yılında imzalayan 17 ülkeden biridir. Cumhuriyet kurulana dek eski ölçü birimleri ve SI birlikte kullanılmış ve 1 Ocak 1933'ten sonra yalnız SI kullanılmaya başlanmıştır.

Türkler, diğer doğu Asya toplulukları gibi onluk sayı düzenini kullanmaya alışık olduklarından metrik sistemi kullanmakta zorlanmamışlardır. İngiltere ve eski sömürgelerinde hâlâ anlaşılması zor ve hata yapmaya açık ölçü sistemleri kullanılmaktadır.

## 3.1.1 Ölçü Birimlerinin Önemi

Daha önce belirtildiği gibi ticareti yapılan mal ve ürünlerin ölçülmesi gerekmektedir. Bir ülkenin kendisine özgü ölçü birimlerini kullanması olağan sayılabilir. İnsanların uzun zamandır kullandığı ölçü birimlerinden vazgeçmesi kolay değildir. Ancak uluslararası kabul gören ölçü birimlerini kullanmak, hem ulusal hem de uluslararası ticaret için önemlidir. Ölçü ve zaman birimlerinin ortak olması veya olmamasının ne tür sorunlara neden olduğu aşağıda madde madde açıklanmıştır:

### Zamanda Uyumsuzluk

İçinde yaşadığımız günün Gregoryan takviminde karşılığını 11 Şubat 2021 olarak varsayalım. Gregoryan takvimi kullanmayan ülkelerde bu günün karşılığını araştırdığımızda Çizelge-3.8'deki sonuçları görürüz:

**Çizelge-3.8: Değişik Takvimler**

| Takvim | Gün | Ay | Yıl |
|---|---|---|---|
| Gregoryan | 11 | Şubat | 2021 |
| Hicri | 28 | Cemaziyelahir | 1442 |
| İran | 23 | Bahman | 1339 |
| Yahudi | 29 | Shevat | 5781 |
| Hint | 22 | Magha | 1942 |

Çizelge-3.8'den görüldüğü gibi, aynı gün için, değişik takvimlerde farklı sonuçlar elde edilmektedir. Haftanın başlangıç günü de toplumdan topluma değişebilmektedir. Gregoryan takviminde, haftanın tatil günü pazar olmasına karşın Hicri takvim kullanan ülkelerde cuma günüdür. Takvimler arası çeviri yapmak kolay bir işlem olarak değerlendirilebilir ancak tatil günündeki farklılık uluslararası ticarette önemli sorunlara neden olmaktadır. Örneğin bir Türk firması Avrupa firmaları ile haftanın beş veya altı günü birlikte çalışabilmektedir. Buna karşın perşembe ve cuma günleri tatil yapan ülkenin firması en çok 3 gün birlikte çalışabilmektedir.

### Birimlerde Uyumsuzluk

Ölçü birimlerindeki uyumsuzluk, günümüzde hesap makineleri ile çözülebilecek bir sorundur. İngiliz ölçü sistemini kullanan ülkelerde, insanlar alışverişlerde bu özel hesap makinelerinden yararlanmaya çalışmaktadırlar. Metrik sistemi ve onluk sayı düzenine alışık olan toplumlarda, birimler arası oranlar onluk düzende olduğu için sorun olmayan durumlar diğer ölçü sistemlerinde sorun olabilmektedir. Konuya açıklık getirmek için aşağıdaki örnekler verilmiştir:

1 litrelik sütün fiyatı 5,00 TL, 1/2 litrelik sütün fiyatı 3,00 TL ise hangisi daha ekonomiktir sorusunun yanıtı metrik sistemi kullananlar için çok kolaydır. Aynı soruyu şöyle

soralım: 1 pint sütün fiyatı 5,00 TL ve bir galon sütün fiyatı 40,00 TL ise hangisi daha ekonomiktir. Bu sorunun yanıtını bulmak için hesap makinesi gerekir.

1 Km içinde kaç metre vardır sorusunu, metrik sistemi öğrenen bir ilkokul öğrencisi yanıtlayabilir. Buna karşın 1 mile içinde kaç yarda vardır sorunun yanıtını vermek için hesap makinesi gerekir.

Özellikle uluslararası ticarette, zaman ve birimlerde uyumun ne kadar önemli olduğunu yukarıdaki örnekler göstermektedir. Bazı ülkeler bunun önemini kavradıkları için SI birimlerine geçmiştir. Türkiye bu konudaki kararını 1925'lerde verip erken davranmıştır. Kanada 1978'lerde bu konuda önemli bir adım atmıştır. ABD 1978'de denemiş ancak başarılı olamamıştır.

## 3.2 Kredi Kartı

XX. Yüzyılın ticaretinde, özellikle bireysel harcamalarda kredi kartı önemli bir rol oynamıştır. Kredi kartı hoş bir olayın sonunda akla gelmiştir. Bir iş adamı olan McNamara 1949 yılında müşterileri ile birlikte New York'ta bir lokantada yemek yerler. Yemek yenip sıra ödemeye geldiğinde, McNamara cüzdanının yanında olmadığını fark eder. Yardımına eşi yetişir ve ödemeyi yaparlar. Bu olay sonrasında McNamara, benzer bir olayın başkalarının da başına gelebileceğini düşünür. Varlıklı insan bile olsanız tanınmadığınız bir yerde zor durumlarda kalınabileceğini düşünür ve bir çözüm arayışına başlar. Bulduğu çözüm, yalnızca varlıklı insanların üye olabilecekleri bir kulüp kurmak ve üyelere bir üyelik kartı vermektir. Kulüp üyeleri lokanta ve otellerde nakit para ile ödeme yapmak yerine bu kartla yapabileceklerdi. Kulüp üyelerinin yaptığı harcamaların karşılığını lokanta ve otellere ödemeyi Diners Club garanti edecektir. Kulüp üyeleri ay içinde yaptıkları harcamaların toplamını kulübe ödeyeceklerdi. Amaç varlıklı insanlara para taşımadan gezme ve eğlenme olanağı sağlamaktır. Bu nedenle karta Diners Club adını verdi.

Diners Club üyeleri varlıklı ve seçkin insanlardan seçiliyordu, dolayısıyla harcamalarının karşılığını kulübe ödemelerinde bir sıkıntı beklenmiyordu. Diners Club üyelerini kabul edecek lokanta ve oteller de seçkin yerler olacaktı. Diners Club müşterilerinin bu yerlerde yapacağı harcamalardan %7 oranında komisyon üyelerden yılda 5 ABD Doları alacaktı. Bu uygulama sayesinde lokanta ve oteller müşterileri sayılarını artırabileceklerdir.

1950 yılının Şubat ayında, McNamara arkadaşları ile birlikte, 1,5 milyon ABD doları sermaye ile Diners Club International'i kurdular. İlk aşamada New York'taki 27 lokantayı ve 200 yakın arkadaşlarını kulübe üye yaparak işe başladılar. 1950 sonunda üye sayıları 20.000, ve 1951 sonunda 42.000'e ulaştı. McNamara 1952 yılında hissesini ortaklarına devretti. 1961 yılı ortalarında ilk plastik kartı dağıtmaya başladığında Diners Club'ın üye sayısı 1,3 milyona ulaşmıştı.

1960 sonlarına doğru Diners Club'a rakip firmalar kurulmaya başlandı. Bank of America Visa'yı Interbank MasterCard'ı kurdular. Bunları zaman içinde başka firmalar da izledi. 1981 yılında Citibank Diners Club'ı satın aldı.

Diners Club kartı bir **borçlanma kartı** olarak adlandırılır. Bu kart ile yapılan tüm harcamaların karşılığı, ödeme zamanı geldiğinde kart sahibi tarafından kartı dağıtan firmaya yapılır. Zamanında yapılmayan ödemeler gecikme faizi ile daha sonra ödenebilir. Üyelerin belli bir harcama sınırları vardır ve bunu aşamazlar.

Visa ve MasterCard kredi kartları, **döner kredi kartı** olarak adlandırılırlar. Bu karta sahip olanlar için harcama sınırı vardır ancak kart sahibi ödeme yaptığı sürece harcama sınırı kadar harcama yapabilir. Bu kartlar ile nakit çekme olanağı da sağlanmış oluyordu.

Günümüzde kredi kartı görünümünde, başka amaçlar için üretilen kartlar da bulunmaktadır. Hava yolu şirketleri müşterilerine mil kazandıran kartlar dağıtmaktadır. Benzer kartları lokantalar, akaryakıt istasyonları müşterilerine vermektedirler. Bu tür kartlara **ödül kredi kartları** adı verilmektedir. Ödül kredi kartlarının amacı, müşterileri kendilerine bağlamaktır diğer bir deyişle müşteri bağlılığını (sadakatini) sağlamaktır.

### 3.2.1 Kredi Kartının Yapısı

1950 yılında kullanılmaya başlayan kredi kartlar, biraz önce söylendiği gibi 1961 yılından sonra plastik olarak üretilmeye başlanmıştır. Bir plastik kart üzerinde bulunan bilgiler Şekil-3.1'de gösterilmiştir. Kredi kartının ön yüzünde;

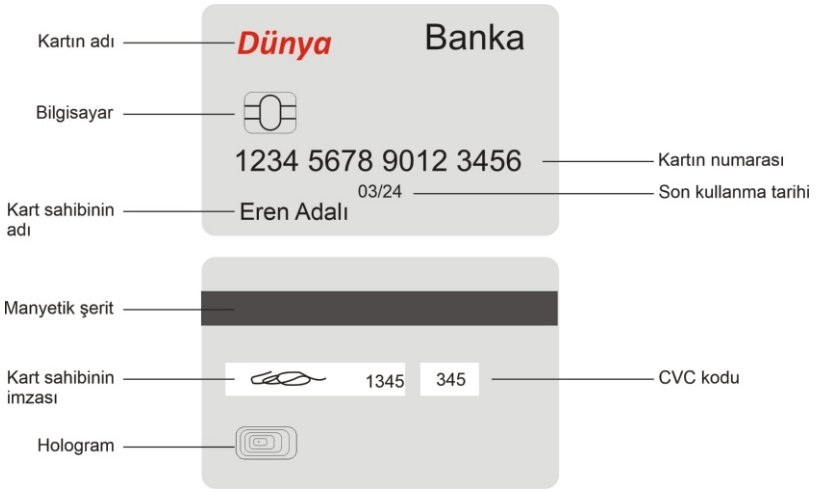
- Kredi kartının adı: Kredi kartına verilmiş olan addır.
- Kartı dağıtan banka: Kartı dağıtan bankanın adıdır.
- Kredi kartının tekil olan numarası: Her karta özgü numaradır.
- Kartın Son kullanım tarihi: Kartın son kullanma zamanını belirtir.
- Kredi kartının sahibinin adı: Kart sahibinin adı.
- Mikrobilgisayar (EMV kartlarda bulunur): Mikrobilgisayar barındıran kartlarda bulunur.

Kartın arka yüzünde;

- Manyetik şerit: Karta ilişkin bilgilerin yazılı olduğu manyetik şerit.
- Kart sahibinin imzası
- Hologram: Taklit edilmeyi önlemek için konur
- CVC kodu

bulunur.

Kredi kartının tekil olan numarasının oluşturulmasında bir algoritma kullanılır. Şekil-3.2'de kartın numarasının yapısı gösterilmiştir.




**Şekil-3.1**: Kredi kartının ön ve arka yüzü

| Kartı üretip dağıtan | | | | | | Kart numarası | | | | | | | | | E |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4 | 4 | 1 | 1 | 0 | 5 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 7 |
| 4x2=8 | 4 | 1x2=2 | 1 | 0x2=0 | 5 | 1x2=2 | 2 | 3x2=6 | 4 | 5x2=10 | 6 | 7x2=14 | 8 | 9x2=18 | 7 |
| 8 | 4 | 2 | 1 | 0 | 5 | 2 | 2 | 6 | 4 | 10-9=1 | 6 | 14-9=5 | 8 | 18-9=9 | 7 |
| 8 | 4 | 2 | 1 | 0 | 5 | 2 | 2 | 6 | 4 | 1 | 6 | 5 | 8 | 9 | 7 |

**Şekil-3.2:** Kredi kartının yapısı

Kredi kartının üzerinde görülen kart numarası 16 basamaklıdır (American Express 12 basamak kullanmaktadır). Kredi kartı numarası şöyle düzenlenir:

- İlk 6 rakam, kartı veren kuruluşu tanımlar. Bu kısmın ilk rakamı, hangi iş kolu olduğunu belirtir; örneğin 4 ve 5 bankacığı belirtir.
- Arkadan gelen 9 basamaklı sayı, müşteriye atanan tekil bir sayıdır.
- Son sayı (E), ilk 15 sayının doğrulama sayısıdır. Eşlik sayısı şöyle hesaplanmaktadır: Tek sayılı sütunlardaki sayılar önce 2 ile çarpılır, sonuçtan 9 çıkarılır ve sonuç en alt satıra yazılır. Çift sayılı sütunlardaki sayılar üzerinde işlem yapılmaz ve en alt satıra taşınır. En alttaki sayıların toplamı 10'a bölündüğünde kalan 0 olacak şekilde E'ye değer atanır. Örneğimiz için E sayısı 7 olarak hesaplanmıştır.

Kredi kartının güvenliğini artırmak üzere, kartın arka yüzüne CVC (Card Verification Code) eklenmiştir (bazı firmalar bu kod için CVV (Card Verification Value) adını kullanırlar). CVC değeri olarak Visa ve MasterCard 3 basamaklı American Express 4 basamaklı sayı kullanmaktadır. CVC

nin değeri, kredi kartının numarası, son kullanma tarihi ve hizmet kodu 32 bitlik bir anahtarla şifrelenerek oluşturulur.

Kartın arka yüzünde bulunan manyetik şerit, kart bilgilerinin bir okuyucu aygıt tarafından okunabilmesi için eklenmiştir. Manyetik kart üzerinde 2 veya 3 kayıt izi bulunur ve bunların üzerinde özetle aşağıdaki bilgiler yer alır:

- Kredi kartı numarası (19 basamağa kadar)
- Kart sahibinin adı (2 den 26 karaktere kadar)
- Son kullanma tarihi
- CVC kodu

EMV türü kartların üzerinde bir mikrobilgisayar bulunur. Bu kart ölçünü üç firma tarafından (Europay, Mastercard ve Visa) oluşturulmuş firmaların baş harfleri ile adlandırılmıştır. Mikrobilgisayarda karta ilişkin bilgiler ve kart sahibinin parolası bulunur. Kart okuyucuya yerleştirildiğinde, kredi kartına ilişkin bilgileri kart okuyucu okur. Ardından okuyucu üzerindeki tuş takımından kullanıcının parolasını girmesi istenir. Kart sahibinin girdiği parolanın doğru olup olmadığını kart üzerindeki bilgisayar söyler.

## 3.2.2 Kredi Kartı ile Ödeme Nasıl Yapılır?

Bir kişi kredi kartına sahip olmak istediğinde, önce hesabı olan banka ile anlaşma yapar. Bu anlaşma sırasında harcama sınırı ve ödeme zamanı belirlenir. Kişinin banka ile yaptığı bu anlaşma kredi kartı firmasına bildirilir. Böylece kişinin kredi kartı geçerlilik kazanır.

Kişi kredi kartını iki türlü kullanabilir: Birinci kullanış biçimi doğrudan alışveriştir. Bir mağazadan yapılan bir alışverişin karşılığını kasada doğrudan ödeme biçimidir. Bu tür ödemelerde kişinin satıcı ile sözleşme yapmasına gerek yoktur. İkinci kullanış biçimi, satıcı ile sözleşme yapılarak yürütülür. Genelağ üzerinden yapılan alışverişler bu türe girer. Kişi satın almak istediği ürünleri kaça ve ne kadar alacağını belirtir. Ardından satıcı ile sözleşme yapılır.

Satıcılar kredi kartı ile yapılan ödemelere ilişkin bilgileri üstlenene gönderir. Üstlenen de bu bilgileri kredi kartı firmasına bildirir. Üstlenicinin görevi, kredi kartının ve sahibinin doğrulanmasıdır.

Kredi kartı ile yapılan alışverişin akışı Şekil-3.3'te gösterilmiştir. Kredi kartı ile alışveriş yapanlarda bir güvenlik kuşkusu vardır. Kredi kartı bilgilerini verdiği satıcı, bu bilgileri kullanarak, kişiyi kandırabilir mi? Bu tür güvenlik sorunlarını çözmek üzere güvenli alışveriş yöntemi geliştirilmiştir.

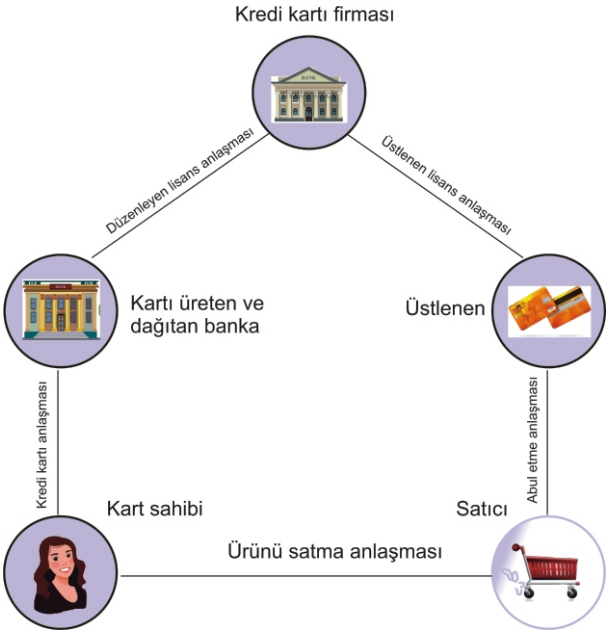
### 3.2.2.1 Güvenli Alışveriş Protokolü (SET)

SET (Secure Electronic Transfer) protokolüne uygun alışveriş için müşteri ve satıcının sayısal yetki belgelerinin olması gerekir. Satıcılar için bu koşul olmazsa olmaz koşuldur. Ancak her

müşteri için bu koşulu sağlamak olanaklı değildir. Bu nedenle, müşterinin kimliği kredi kartı bilgileriyle asıllanmaya çalışılır.

SET protokolünde, bir alışveriş süreci 9 adım olarak tanımlanmıştır:

1. Müşteri, satıcının web sayfasına bağlanır.
2. Müşteri satın almak istedikleri ile ilgili olarak, iki parçadan oluşan sipariş ve ödeme bilgilerini gönderir. Parçalardan birincisi alışveriş ile ilgilidir ve satıcıya gönderilir. İkinci parça kredi kartı bilgisidir ve bu bilgi satıcının müşterisi olduğu bankaya gönderilmek üzere satıcıya gönderilir.
3. Satıcı kredi kartı bilgilerini, bankasına iletir.



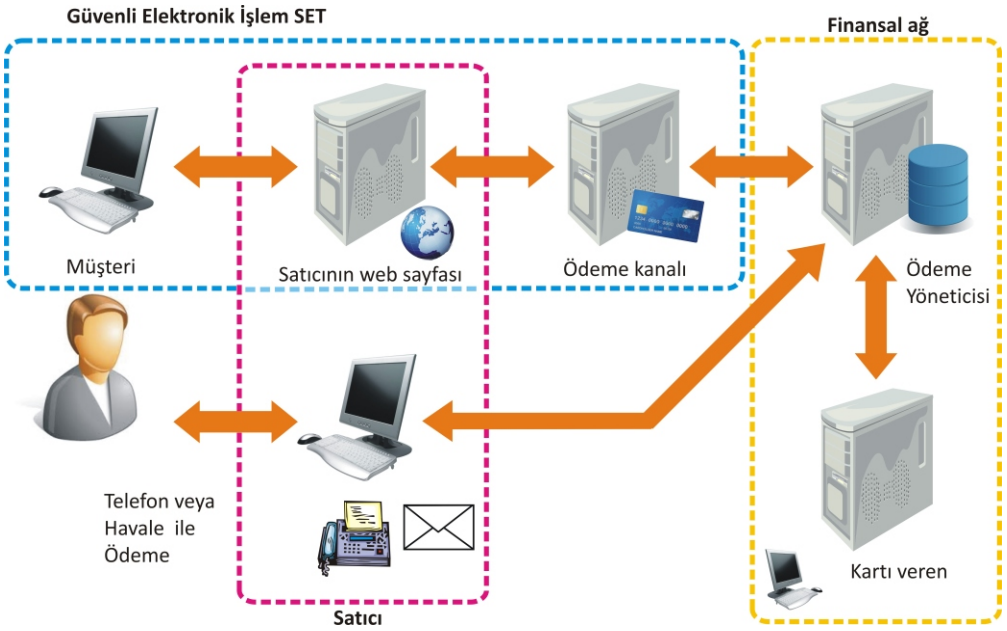

**Şekil-3.3**: Kredi kartı ile ödemenin işleyişi

4. Satıcının bankası, müşterinin kredi kartını, bu kartı veren kuruluşa bağlanarak onay ister.
5. Kredi kartını müşteriye vermiş olan kuruluş, satıcının bankasına onay gönderir.
6. Satıcının bankası, satıcıya onay gönderir.
7. Satıcı siparişi tamamlar ve müşteriye onay bilgisini gönderir.
8. Satıcı bankasından alışveriş ile ilgili işlem kaydını alır.
9. Kredi kartını müşteriye veren kuruluş, müşteriye kredi kartı ödeme belgesini (fiş ya da fatura) gönderir.

SET protokolünün nasıl çalıştığı Şekil-3.4'te gösterilmiştir.

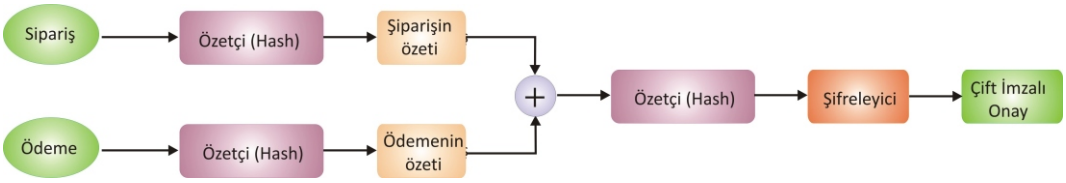
SET protokolünün adımları anlatılırken, ikinci adımda müşterinin sipariş ve ödeme bilgilerini iki parça halinde gönderdiğini söylemiştik. İlk parça alışveriş ile ilgilidir. Bu parçaya Sipariş adını veriyoruz ve bu parça satıcıya gönderiliyor. İkinci parça ödeme ile ilgilidir. Ödeme adını verdiğimiz bu parça kredi kartına ilişkin bilgileri içerir ve satıcının bankasına gönderilir. Satıcının ödeme ile ilgili bilgileri, daha açık bir ifadeyle kredi kartı bilgilerini görmemesi gerekir.

Bir alışverişin tamamlanabilmesi için bu iki parçanın birleştirilmesi gerekir. Şekil-3-5'te Sipariş ve Ödeme bilgilerinin nasıl birleştirildiği gösterilmiştir.




**Şekil-3.4**: SET Protokolü kullanılarak yapılan güvenli alışveriş

Şekil-3.5'ten görüldüğü gibi, ödeme bilgisinin özeti satıcıya gelmektedir. Sipariş ile ilgili bilgiyi satıcı görebilmekte ve bu bilginin özetini çıkarabilmektedir. Her iki özet birleştirilip




**Şekil-3.5**: Sipariş ve Ödeme bilgilerinin birleştirilmesi işlem

şifrelendikten sonra çifte imza onayı ile sonuca ulaşılmaktadır. Böylece alışveriş iki tarafın imzası ile onaylanmış olmaktadır. Bunun sonucu olarak iki tarafın da alışverişi yadsımasının önü kesilmiş olmaktadır. Satıcı, Sipariş, Çift İmza ve Ödemenin Özeti bilgilerini kullanarak bankadan ödemeyi alabilir.

Günümüzde SET protokolü;

- Müşteri kredi kartının Kişisel Kimlik Numarasını (PIN)
- Bilgisayarlı kredi kartlarında, müşteri parolasını
- Eliptik Eğri Şifrelemesini (ECC)

kullanabilmektedir.

### 3.2.3 Kredi Kartı Okuyucular

Kredi kartlarının kullanılmaya yeni başlandığı dönemlerde, lokanta ve marketlerde yapılan ödemelerde, çok yapraklı fiş kullanılırdı. Bugün için çok ilkel olarak değerlendirebileceğimiz bir aygıta önce kredi kart yerleştirilir; kartın üzerine kendinden karbon kopyalı fiş yerleştirilirdi. Son aşamada fişin üzerinden silindir ile geçilirdi. Silindir, kart üzerindeki kabartma yazıların fişlere kopyalanmasını sağlardı. Bu aşamadan sonra, ödenecek miktar rakam ve yazıyla yazılır ve fiş müşteri tarafından imzalanırdı. Fişlerden biri kanıt belge olarak müşteriye verilir; diğeri işletmede tutulur; bir başkası üstleniciye gönderilirdi. Şekil-3.6'da eski dönem kredi kartı fişi üretme aygıtı gösterilmiştir.

**Şekil-3.6**: Eski dönem kredi kartı fişi üretme aygıtı

Bu eski dönem aygıtı bazı ülkelerde hâlâ kullanılmaktadır. Bu türde hazırlanan fişlerin birden çok kopyalandığı, böylece müşterilerin kandırıldığına ilişkin haberler yaygındır.

Günümüzde kredi kartını okumak üzere yetenekli aygıtlar geliştirilmiştir. Yeni okuyucular, kredi kartının arkasındaki manyetik şeritteki bilgileri okuyabildiği gibi EMV kartların mikrobilgisayarı ile iletişime geçebilmektedir. Bu iletişim temaslı ya da temassız olabilmektedir. Şekil-3.7'de yeni nesil kart okuyucu gösterilmiştir.

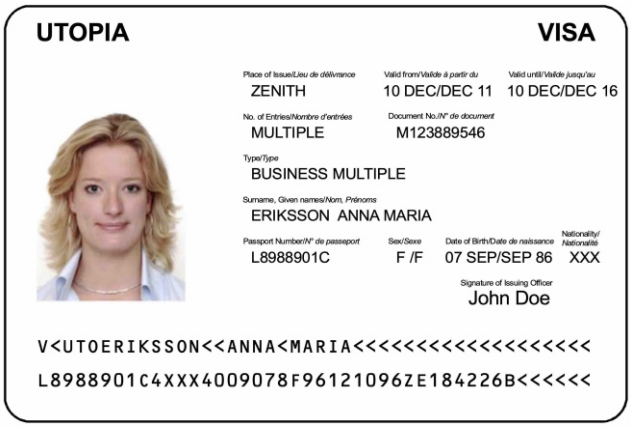

**Şekil-3.7**: Yeni nesil kart okuyucu

## 3.3 Çizgi Yazısı (Barkot)

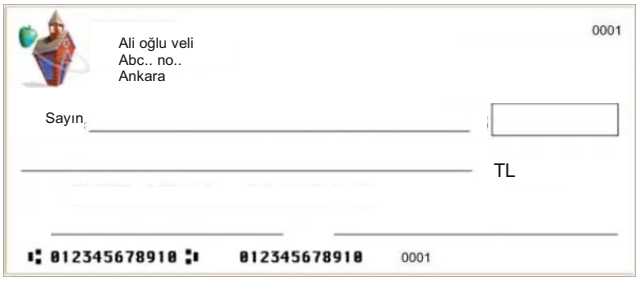
Bir zamanlar yoğun olarak kullanılan mektup dağıtımında, kişilerin elle yazdıkları zarf üstü bilgileri okumak, postane çalışanlarını çok yoruyordu. Bu amaçla yapılan ilk çalışmalar el yazısının okunması üzerine olmuştur. El yazısının okunması zor olunca posta kodu ile çözüm aranmıştır. Posta kodları genellikle sınırlı sayıda harf veya rakamdan oluştuğu için makine tarafından okunması daha kolaydı.

Daktiloda yazılmış metinlerin okunup bilgisayar ortamına aktarılması üzerine yapılan çalışmaların sonunda optik yöntemle okunabilir karakter (OCR- Optical Character Reader) çözümleri üretildi. Daktiloların kullandığı fontlar düzeltilerek OCR türü font biçimine dönüştürüldü.

İnsanın da okuyabildiği, ancak makinenin düşük hata ile okuyabildiği karakterler bugün farklı alanlarda kullanılmaktadır. Şekil-3.8'de makinenin kolayca okuyabileceği karakterler barındıran bir kimlik örneği verilmiştir.




**Şekil-3.8**: Makinenin okuyabildiği karakterler




**Şekil-3.9**: Makinenin okuyabileceği bir çek yaprağı

Makinenin okuyabildiği bir başka yazı biçimi çeklerde kullanılmaktadır. Şekil-3.9'da böyle bir çek örneği gösterilmiştir.

1948 yılında Drexel Teknoloji Enstitüsünde yüksek lisans öğrencisi olan B. Silver, yerel gıda fuarının başkanı ile dekanın konuşmalarına kulak misafiri olur. Başkan, dekandan ürün bilgilerini okuyabilecek bir sistem üzerinde çalışmalarını istiyordu. Silver bu tür bir sistemi geliştirmek üzere arkadaşı N. J. Woodland ile çalışmaya başladılar. İlk çalışmalarında morötesi mürekkep kullandılar. Bu mürekkep kolayca siliniyor ve pahalıydı. Ancak sistemin çalışabileceğini göstermişti.

Bir sonraki aşamada Woodland, Mors abecesinde olduğu gibi karakterlerin dar ve geniş çizgilerle yazılabileceğini düşündü ve düşüncesini uygulamaya çalıştı. Karakterleri düz bir çizgi üzerine

yerleştirmek yerine dart'ın hedef tahtasında olduğu gibi daire üzerine yerleştirdiler. 1952 (başvuru 1949) yılında Woodland ve Silver çalışmalarının patenti için 20 Ekim 1949'da başvurdular patent 1952'de kabul edildi. Bu arada Woodland 1951 yılında IBM'de çalışmaya başladı. IBM patenti satın almak istediyse de patent 1962 yılında Philco'ya satıldı. Philco patenti daha sonra RCA'ya sattı.

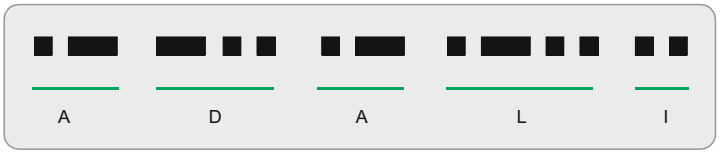
1966 yılında Amerikan ulusal gıda zinciri birliği (NAFC) marketlerin kasalarında kullanılabilecek bir sistem konusunda toplantı düzenledi. Bu toplantıya katılmış olan RCA Woodland'in patentini kullanarak ilk uygulamayı başlattı.

1970 yılının ortalarında NAFC çizgi yazı için bir ölçün belirlenmesini istedi ve bu istek Singer, NCR, Litton, RCA, Pitney-Bowel, IBM ve diğer firmalara iletildi. 1971 ilkbaharında RCA'in çalışmalarını sunduğu toplantıya katılan IBM temsilcisi, hâlâ IBM'de çalışan Woodland'ı hatırladı ve çizgi yazı konusunda bir çalışmayı başlattı. Bu çalışmaların sonunda 1973 yılında UPC çizgi yazı ölçünü IBM tarafından tanıtıldı.

## 3.3.1 Çizgi Kod Abeceleri

Yukarıda anlatılanlardan, çizgi yazının bir tür abece olduğu sonucu çıkarılabilir. Amaç, bir yazının makine, daha doğrusu bilgisayarın kolay okuyabileceği bir abecenin geliştirilmesidir. Geliştirilen abecelerin ortak özelliği, Morse abecesinde olduğu gibi karakterleri dar ve geniş çizgilerle veya dar ve geniş boşluklar ile belirtmek. Morse abecesini hatırlatmak üzere, bu abece de yazılmış kısa bir metin örneği Şekil-3.10 da verilmiştir.

Morse abecesine dikkatle bakıldığında, harflere karşılık oluşturulan nokta ve çizgilerin sayısının değişken olduğu görülür. Çizgi yazı abecelerinde harf ve rakamlar için eşit boyda alan ayrılması ilkesi benimsenmiştir.




**Şekil-3.10**: Morse yazısı için bir örnek

Çizgi yazı için çeşitli abeceler geliştirilmiştir ancak günümüzde yaygın olarak kullanılanlar burada tanıtılacaktır.

### 3.3.1.1 UPC ve EAN

Marketlerde satılan ürünlerin etiketlenmesi amacıyla geliştirilen UPC (Universal Product Code) zaman içinde tüm perakende ürünlerde kullanılır olmuştur. UPC çizgi yazısı yalnızca rakamları yazmaya uygundur. ABD'de kullanılmaya başlayan UPC'nin daha gelişmiş bir biçimi EAN (European Product Code) Avrupa ve Japonya'da kullanılmaktadır. Zaman içinde UPC'nin değişik türleri geliştirilmiştir. Örneğin UPC-A, UPC-B, UPC-C, UPV-D ve UPC-E. Zaman içinde UPC-B ve UPC-C kullanımdan kalkmış, UPC-D EAN 2.0'a dönüşmüştür. Bugün yaygın olarak kullanılan

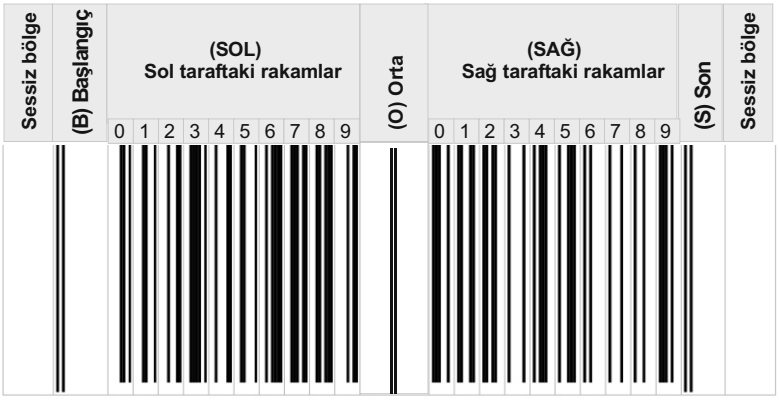
UPC-A dır. UPC-E özellikle küçük paketler için geliştirilmiştir. 12 rakam içeren UPC-A karşın UPC-E 6 rakam içerir. UPC-A nın boyutunu küçültmek için üretici ve ürün kodundaki sıfırlardan vazgeçilmiştir. UPC-A ABD içi kullanım için geliştirildiğinden bir etikette üretici firma ve ürün kodu bulunur. Buna karşın EAN Avrupa ülkeleri için geliştirilmiştir; 13 basamaklıdır ve ülke kodunu da içerir. 13 basamaklı EAN, EAN-13 olarak anılır. 8 basamaktan oluşan EAN-8 de kullanılmaktadır.

UPC-A çizgi yazısının kendisine özgü abecesi (EAN de aynı abeceyi kullanır) ve bir yazım kalıbı vardır. Bunlar aşağıda açıklanacaktır.

## UPC Çizgi Yazısının Abecesi

UPC çizgi yazısının kullanıldığı bir ürün etiketinde 12 basamak sayı bulunur. Her basamak 2 çizgi ve 2 boşluktan oluşur. Çizgi ve boşlukların eni 1, 2, 3 veya 4 **birim** olabilir. Bir basamağın toplam eni 7 birimdir, dolayısıyla bir UPC-A etiketinin ana kısmının eni 7x12=84 birimdir. Etiketin başı, ortası ve sonuna eklenen özel karakterler ile toplam eni 95 birim olur. Şekil-3.11'de UPC etiketinin genel biçimi gösterilmiştir. Şekil-3.11'e dikkatli bakıldığında aynı rakamın sol ve sağ yarıdaki biçiminin farklı olduğu görülür. Sayıların başlangıç ve sonunu belirten B ve S kısımlarının eni 3 basamak eni kadardır ve enleri bir birim olan bir çizgi bir boşluk ve bir çizgiden oluşurlar. Orta için ayrılan alan 5 basamak genişliğindedir; orta kısmında bir birim genişliğinde bir çizgi bir boşluk ve bir çizgiden oluşan **orta çizgi** alır. Başlangıç karakterinden önce ve Son karakterinden sonra 9 basamak genişliğinde sessiz bölgeler yer alır.

UPC-A'nın doğru okunmasını sağlamak üzere eşlik sayısı kullanılmaktadır. Eşlik değeri hesaplanırken, çizgilerin birimleri, yani kaç birim kalınlıkta oldukları hesaba katılır. Sol yarıdaki sayılar ve O bölgesinin orta çizginin soluna eklenecek çizgilerin toplam birim sayısı tek sayıda olacak biçimde düzenlenir.




**Şekil-3.11**: UPC etiketinde rakamların sol ve sağ yarıdaki görünümleri

Sağ taraf için çizgilerin toplam birim sayısı çift olacak şekilde düzenleme yapılır. UPC-A kalıbına uygun yazılmış bir etiketin soldan sağa veya sağdan sola doğru okunabilmesini sağlamak üzere B ve S karakterleri ters sırada

yerleştirilmiştir. Bu düzenleme sayesinde bir UPC-A etiketi baş aşağı geldiğinde de okunabilmektedir.

### UPC Etiketinin Kalıbı

UPC-A 12 rakam içerecek biçimde düzenlenmiştir. Bu rakamlardan birincisi etiketin niteliği, sonuncusu eşlik rakamı için ayrılmıştır, Şekil-3.12. Sayı düzenini belirten basamaktan sonra gelen beş basamaklı sayı üretici firmayı, daha sonraki beş sayı ürün kimliğini tanıtmak için ayrılmıştır. Etiket türünü belirleyen ilk basamak aşağıda açıklandığı biçimde kullanılmaktadır:

**Ölçünlü Etiket**: Bu basamağa 0,1,6,7,8 veya 9 yazılmış olması, etiketin ölçünlü etiket olduğu gösterir. Ölçünlü etikette ilk 5 basamaklı sayı firma, ikinci 5 basamaklı sayı ürün için ayrılmıştır.

**Ağırlık**: Bu basamağa 2 yazılmış ise etiketin marketlerin özel kullanımları için hazırlandığını belirtir. Etiketteki ilk 5 basamaklı sayı ürünü, ikinci 5 basamaklı sayı ürünün ağırlık veya fiyatı için ayrılmıştır.

**İlaç**: Bu basamağa 3 yazılmış ise etiketin ilaç etiketi olduğu anlaşılır. Etiketteki 10 basamaklı sayı ilacı tanımlar.

**Ödül**: Bu basamağa 4 yazılmış ise etiket firmalar tarafından verilen ödülü gösterir.

**İndirim**: Bu basamağa 5 yazılmış ise etiket firma tarafından verilen indirimi gösterir. Etiketteki ilk 5 basamaklı sayı firmayı, ikinci 5 basamaklı sayının ilk üç basamağı ürün ailesini, ardından gelen 2 basamak indirim miktarını belirtmek için ayrılmıştır.


**Şekil-3.12**: UPC-A'nın kalıbı

### Eşlik Sayısının Hesabı

UPC-A okuma yanlışlarını ortaya çıkarabilmek için 12. basamaktaki eşlik sayısından yararlanmaktadır. Eşlik sayısı aşağıdaki formüle göre hesaplanmaktadır:

$3x_1+x_2+3x_3+x_4+3x_5+x_6+3x_7+x_8+3x_9$
$+x_{10}+3x_{11}+x_{12}$ ($x_i$: basamakları göstermektedir.)

$3(x_1+x_3+x_5+x_7x_9x_{11})+(x_2+x_4+x_6+x_8x_{10}+x_{12})$

Bu eşitliğe göre bulunan sonucun sıfır olmasını sağlayacak değer $x_{12}$ ye verilir.

### EAN-13

Daha önce açıklandığı gibi UPC-D EAN-13'e dönüşmüştür. EAN-13 UPC-A ile aynı abeceyi kullanır ve etiket kalıbı çok benzerdir. EAN-13 13 rakam içerir. Son rakamın eşlik için ayrıldığı düşünüldüğünde geriye 12 basamaklı bir sayı kalır. Bu 12 basamak, sırasıyla ülke, firma ve ürün için ayrılmıştır. Şekil-3.13'te örnek bir EAN-13 etiketi gösterilmiştir.


**Şekil-3.13**: Bir EAN-13 etiketi örneği

### EAN Kodunun Dağıtımı

1973 yılında perakende ürünlerin etiketlenmesi için kullanılması kabul edilen UPC-A daha sonra EAN-13 adıyla Avrupa'da 1977 yılında kullanılmaya başlanmıştır. EAN ölçünlerini ve dağıtımını merkezi Brüksel'de bulunan EAN yapmaktadır. EAN 1992 yılında EAN International, 2005'te GS1 adını almıştır. Günümüzde GS1'in 170 ülkede temsilcilikleri vardır. 1988 yılında TOBB EAN'in temsilciliğini almış ve Milli Mal Numaralama Merkezi'ni oluşturmuştur. Bu merkezin adı 2005'te GS1 Türkiye olarak değiştirilmiştir ve niteliği vakıf (GS1 Türkiye Vakfı) olarak değiştirilmiştir

GS1 her ülke için bir kod oluşturmuştur. Türkiye için ayrılan kodlar 868 ve 869'dur. Yerel temsilciler kendi ülkelerindeki firmalar için firma kodu ataması yapmaktadır. Ürün kodları firmalar tarafından üretilmektedir. Ürün kodları ve açıklamaları GS1 yerel temsilcileri tarafından dağıtılmaktadır.

## 3.3.1.2 Code39 (9 da 3)

Code-39 43 karakter içeren bir çizgi yazı abecesidir. Bu abece kapsamında A'dan Z'ye büyük harfler, 0 dan 9 a rakamlar ve -, ., $, /, +, % ve aralık karakterleri bulunur. Ayrıca yazının başını ve sonunu belirtmek için "*" yer alır. Her bir karakter beş çizgi ve 4 boşluktan kurulan 9 ögeden oluşur. Ögelerden üçü geniş ve altısı dardır. Geniş ögeler "1" ve dar ögeler "0" olarak varsayılır. Dar ve geniş ögelerin en oranları çok önemli olmamasına karşın 1/2 veya 1/3 olarak seçilir. Şekil-3.14'te Code-39 abecesi görülmektedir.

Code-39 da yazı "*" karakteriyle başlar, karakterler arasına bir ince boşluk konularak devam edilir ve yazı sonuna "*" karakteri konur. Yazının boyu için bir sınırlandırma yoktur. Code-39' da okumanın doğruluğunu sağlamak üzere eşlik kullanılmamıştır. Ancak istenirse satır sonlarına veya metnin sonuna toplam eşliği yerleştirilebilir. Şekil-3.15'te Code-39 kullanılarak kısa bir örnek gösterilmiştir.

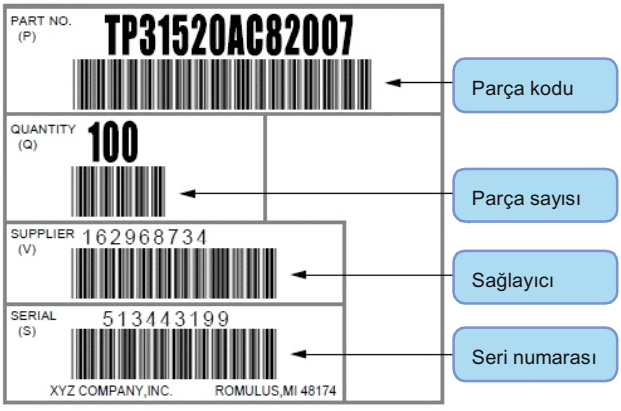
| | | | | | |
|---|---|---|---|---|---|
| 0 | | F | | T | |
| 1 | | G | | U | |
| 2 | | H | | V | |
| 3 | | I | | W | |
| 4 | | J | | X | |
| 5 | | K | | Y | |
| 6 | | L | | Z | |
| 7 | | M | | - | |
| 8 | | N | | . | |
| 9 | | O | | SPACE | |
| A | | P | | $ | |
| B | | Q | | / | |
| C | | R | | + | |
| D | | S | | % | |
| E | | | | * | |

**Şekil-3.14**: Code-39 abecesi

1974 yılında D. Allis ve R. Stevens tarafından geliştirilen Code-39 günümüzde, paketlerde ve mektup zarfları üzerinde kullanılmaktadır. ABD posta idaresi ve askeri kuruluşlar tarafından kullanılmaktadır.


**Şekil-3.15:** Code-39 abecesi ile yazılmış bir yazı örneği

Code-39 AIAG (Automotive Industry Action Group) tarafından, otomobil parçalarının etiketlenmesi amacıyla kullanılmaktadır. AIAG'nin kullandığı etiket kalıbı Şekil-3.16'da gösterilmiştir.




**Şekil-3.16**: AIAG tarafından kullanılan kutu etiketi

### 3.3.1.3 Code-128

Code-128 temel olarak Code-39'a benzemektedir ancak daha yoğundur. Dolayısıyla uzun yazıların yazılması için daha uygundur. A dan Z ye büyük ve küçük harfleri, sayıları ve özel karakterleri içerir. Daha teknik bir açıklama ile Latin-1 kümesinde bulunan tüm karakterleri içerir.

Code-128 de bir karakter üçü boşluk olmak üzere altı ögeden oluşur. Her karakter çizgi ile başlar boşluk ile sonlanır. Bir çizgi ve boşluğun eni 1,2,3 veya 4 birim olabilir. Bu kurallara göre A karakteri 10100011000 olarak yazılır. Bunu çizgi ve boşluk genişlikler cinsinde yazarsak 111323 olarak yazabiliriz.

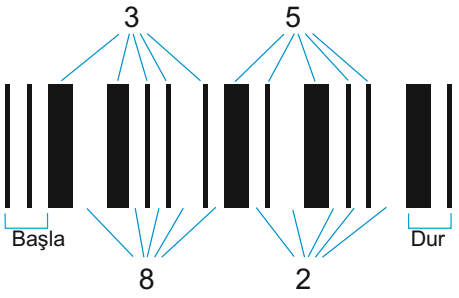

**Şekil-3.17:** Code-128 abecesi ile yazılmış bir yazı örneği

Code-128 de yazı Baş ve Ek karakteriyle başlar, karakterler arasına boşluk yoktur. Yazı sonuna eşlik ve dur karakteri eklenir. Baş karakteri Code-A, Code-B ve Code-C ye göre değişmektedir. Dur karakterinin eni 13 birimdir. Şekil-3.17'de Code-39 kullanılarak kısa bir yazı örneği görülmektedir.

Code-128 ürün dağıtım zincirlerinde paketlerin etiketlenmesinde yaygın olarak kullanılmaktadır.

### 3.3.1.4 ITF (Interleaved Two of Five)

Dağıtım işlerinde kullanılan bir çizgi yazı ölçünüdür, Yalnızca sayılardan oluşur. ITF bir karakter için 5 çizgi ve 5 boşluk kullanır. Bu beş çizgiden ikisi kalındır. Aynı şekilde 5 boşluktan ikisi kalındır. Çizgiler ve boşluklar ile yazılan sayılar iç içe geçmiş durumdadır. Yazının başında Başla ve sonunda Dur karakteri yer alır. ITF'nin temel yapısı Şekil-3.18'de ve abecesi Şekil-3.19'da gösterilmiştir.




**Şekil-3.18**: ITF çizgi yazısının yapısı

| Karakter | Çizgi Karakter | Karakter | Çizgi Karakter |
|---|---|---|---|
| **Başla** | | 5 | |
| 0 | | 6 | |
| 1 | | 7 | |
| 2 | | 8 | |
| 3 | | 9 | |
| 4 | | **Dur** | |

**Şekil-3.19**: ITF abecesi

### 3.3.1.5 Çizgi Kot Okuyucu

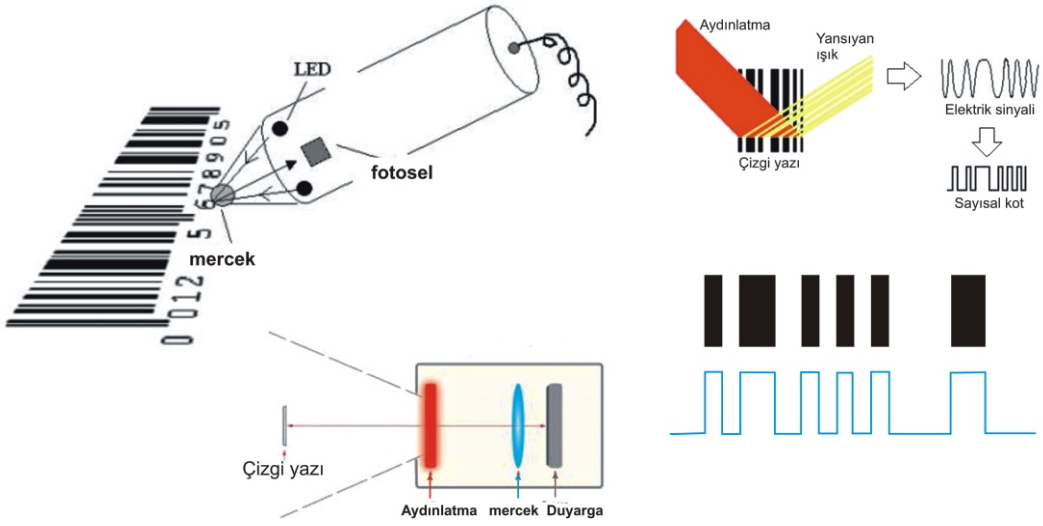
Şu ana kadar tanıtılmış ve tek boyutlu çizgi yazıları okumak için, ilk dönemlerde çizgi yazı kalemleri kullanılmıştır. İnsanın el hızı ile yönlendirilen çizgi yazı kalemleri yavaş kaldıkları için yerlerini daha sonra taramayı kendi yapan aygıtlar kullanılmaya başlanmıştır.

Şekil-3.20'de bazı çizgi yazı okuyucular gösterilmiştir.


**Şekil-3.20**: Değişik tür çizgi yazı okuyucular

Okuyucular, uygulama alanlarına göre, birkaç santimetreden 30 metre uzaklığa kadar okuyabilmektedirler.

Çizgi kod oyucularının nasıl çalıştığı Şekil-3.21'de basit olarak gösterilmiştir.




**Şekil-3.21:** Çizgi yazının okunmasına ilişkin temel yöntem

### 3.3.1.6 Karekot

Bundan önceki bölümlerde tanıtılan çizgi yazılar tek boyutlu olarak nitelendirilir. Karekot iki boyutlu olarak 1994 yılında Denso firması tarafından geliştirilmiştir. Harfler, rakamlar, ikilik değerler ve Japon abecesini içerir. Perakende, duyuru ve reklam işlerinde kullanılır. Şekil-13.22'de örnek bir karekot gösterilmiştir.

**Şekil-3.22**: Karekot

### 3.3.1.6 Çizgi Yazının Yararları

Mahalle bakkalları, dükkânlarındaki tüm ürünlerin fiyatlarını ve müşterilerini tanırlar. Müşteriler ödemeyi doğrudan kendisine yaparlar. Müşterinin ödemesini alırken bir zaman sıkıntısı da yaşamaz. Dükkânlar büyüyüp markete dönüştüğünde artık birden fazla kasa kurulmaya başlandı ve kasada çalışanlar marketin sahibi değildir. Kasiyerlerin ürünlerin fiyatlarını veya kodlarını ezberlemeleri beklenemez. Bu durumda, bir müşterinin ödemesi sırasında, kasiyerin her ürünün fiyatını veya kodunu kasaya girmesi gerekir. Bu bilgi girilirken yanlış yapma olasılığı her zaman vardır. Bu nedenlerle 1948 yılında Drexen Teknoloji Enstitüsünün dekanından ürün bilgilerinin hızlı ve doğru girilmesini sağlayacak bir düzen geliştirilmesi istenmiştir.

Bir ürünün kodu veya fiyatının 10 basamaklı bir sayı olduğunu varsayalım. Yapılan deneyler, deneyimli bir kişinin, yalnızca sayılardan oluşan tuş takımını kullanarak 1 basamaklı bir sayıyı yaklaşık 5-10 saniye arasında girebileceğini göstermiştir. Bir çizgi yazılı etiketin okunması süresi 1 saniyeden kısadır.

Yalnızca sayısal tuşlar kullanılarak yapılan girişlerde yaklaşık 4/10.000 hata yapıldığı, deneyler sonucunda anlaşılmıştır. Bu sonuç, kasiyerlerin girdiği 1000 ürün bilgisinden dördünün yanlış olduğu sonucunu çıkarır. Çizgi yazı okuyucuları hatalı okuma olduğunda kasiyeri uyarır. Buna karşın okuyucuların 1/1.000.000 hata yaptığı görülmüştür.

Yukarıdaki bilgilerden, çizgi yazının hem hız hem de doğruluk sağladığı açıkça görülmektedir. Bu nedenle günümüzde yaygın olarak kullanılmaktadır.

## 3.4 Telsiz Etiketler (RFID)

Ürünleri etiketlemek için çizgi yazının geliştirildiğini ve günümüzde yaygın olarak kullanıldığını önceki kısımlarda anlatılmıştı. Çizgi yazıya rakip olabilecek bir etiket türü RFID etiketlerdir. Bunlar için telsiz etiket diyebiliriz. RFID etiketlerin okunması telsiz iletişimi temeline dayanır. Çok basit bir anlatım ile, okuma alanına giren bir RFID etiket kimlik bilgisini gönderir ve bu bilgi alıcı tarafından okunur. RFID etiketler ürünleri, paketleri, konteynerleri, dorseleri, canlıları etiketlemekten araçları etiketlemeye kadar değişik alanlarda kullanılmaktadır. Bir RFID etiketin okunması için, etiketin okuyucunun alanına girmesi yererlidir. Okuma mesafesi 10 cm - 30 m

arasında değişebilmektedir. Ayrıca etiket okuma alanının içinden 100Km/h hızıyla geçse bile okunabilmektedir. Bu bölümde, ticaret alanında kullanılan RFID etiketler tanıtılacaktır.

Telsiz etiketler, aslında 1970'lerden beri bilinen ve uygulanan teknolojidir. Ancak 1990'lardan sonra boyutları küçüldü ve fiyatları çok düştü. Bu yüzden kullanılabilir oldular.

## 3.4.1 Telsiz Etiketler Nasıl Çalışır?

RFID etiketin temeli bir telsiz vericisi ve anteninden oluşur. Elektronik devre basit bir verici olabileceği gibi vericiye bağlı küçük bir mikrobilgisayar olabilir. Etiket uyarıldığında okuyucu ile etkileşime girer ve kendinden istenen bilgileri okuyucuya gönderir. RFID etiketin temel yapısı Şekil-3.23'te gösterilmiştir. RFID etiketin nasıl okunduğu Şekil-3.24'te çizilmiştir. RFID etiketler genel olarak iki sınıfa ayrılırlar:

- Etkin RFID etiketler
- Edilgen RFID etiketler

### Etkin RFID etiketler

Etkin RFID etiketlerin içinde, enerjisini sağlayan bir kaynak (pil) bulunur. Etiket okuyucunun alanına girdiğinde uyarılır ve uyarana içindeki bilgileri gönderir. İçindeki bilgiler bir kimlik bilgisi olabileceği gibi daha fazla bilgi de olabilir. Etiket alandan çıktığında uyku kipine geçer.

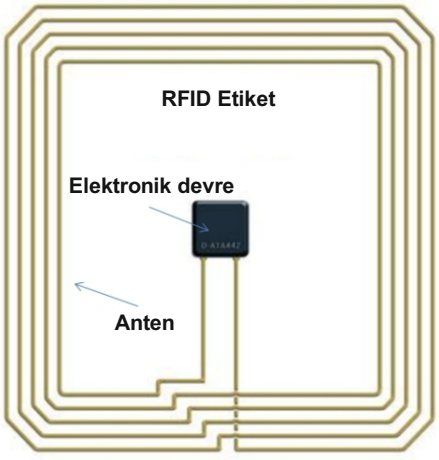
Etkin RFID kimlikler genellikle uzun erimli okumalar için yeğlenir. Örneğin taşıtların veya yüklerinin etiketleri genellikle etkin RFID olarak seçilir. Bu tür uygulamalarda okuyucu ile kimlik arasındaki erim 3 cm den 30 m'ye kadar olabilir. Ayrıca etiket hızlı biçimde okuma alanının içinden geçmektedir.

Etkin RFID'lerin güç kaynaklarının (pil) ömrü yaklaşık 7 yıldır. 7 yıl sonunda güç kaynağının değiştirilmesi gerekir.

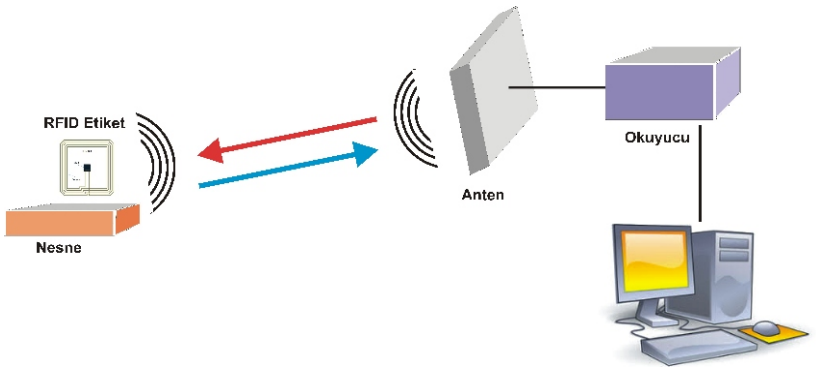
### Edilgen RFID etiketler

Edilgen RFID etiketlerin içinde güç kaynağı yoktur. Okuyucunun gönderdiği elektromanyetik alanın enerjisi ile uyanır ve okuyucuya kimliğini veya içindeki tüm bilgileri gönderir.

Edilgen RFID etiketler daha çok kısa erimli uygulamalar için uygundur.




**Şekil-3.23:** RFID etiketin temel yapısı




**Şekil-3.24**: RFID etiketin okunması ile ilgili yapı

Örneğin kimlik kartları, ürün etiketleri için uygun olurlar. Okuma erimi ortalama 30 cm kadardır. Ancak yakın zamanda hareket halindeki araçlar için de kullanılabilen türleri üretilmektedir.

Edilgen RFID etiketlerde güç kaynağı olmadığı için ömürleri sonsuz kabul edilebilir.

## 3.4.2 Telsiz Etiketlerin Ticarette Kullanılışı

Daha önce açıklandığı gibi RFID etiketler çok farklı alanlarda kullanılmaktadır. Burada yalnızca ticari alanda nasıl kullanıldıklarına değinilecektir. RFID etiketlerinin fiyatları önceleri yüksek olduğu için yalnızca gereken alanlarda kullanılmaktaydı. Zaman içinde fiyatları oldukça ucuzladı. Özellikle edilgen olanların boyutları 1x1cm ve kalınlıkları 0,1 mm'ye inince çekici hâle geldiler. Bugünkü fiyatları 1 TL'nin altındadır. Fiyat karşılaştırması yapıldığında çizgikot etiketlere oranla hâlâ yüksektir ancak sağladığı üstünlükler ileride daha da yaygın olarak kullanılabileceklerini göstermektedir.

Perakende satış yapan yerlerde RFID etiket kullanmanın iki amacı vardır:

1- Müşteri sepetine attığı ürünlerin fiyatını ve toplam ne kadar alışveriş yaptığını anında görebilmeli.

2 - Kasada sıra bekleyip zaman kaybetmemeli.

Şekil-3.26'da ürünleri RFID etiketli olan ve akıllı sepet ile alışveriş yapılan bir marketin nasıl çalıştığı gösterilmiştir.

## 3.4.3 Telsiz Etiketlerin Güvenliği

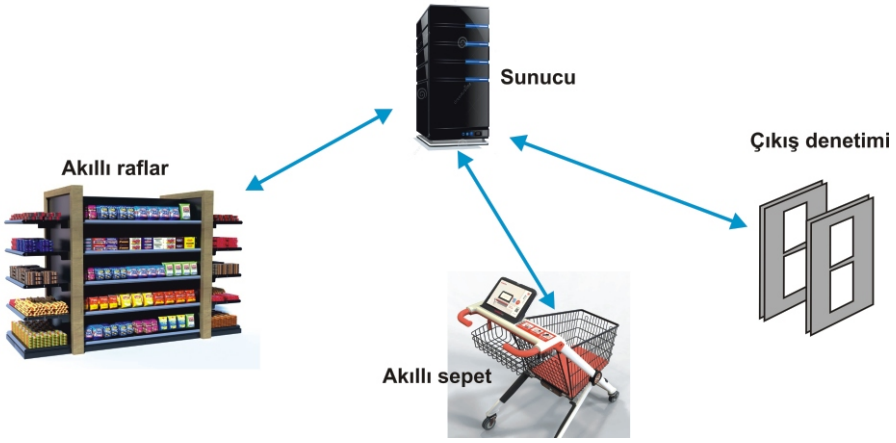
Telsiz etiketlerin güvenlik sorunu olabileceği söylenebilir. Güvenlik sorununu gidermek üzere çalışmalar yapılmış ve yapılmaktadır. İçinde mikrobilgisayar bulunduran etiketler, uyarıldıklarında öncelikle okuyucu ile el sıkışırlar. El sıkışma iki tarafın birbirini tanıması aşamasıdır. Bu aşamada, okuyucu, etiketin kendisi için tanımlı olup olmadığını sınarken, etiket

okuyucunun kendisi tarafından kabul edilen bir okuyucu olup olmadığını sınar. El sıkışma sonucu olumlu ise etiket istenen bilgileri gönderir.

**Şekil-3.25**: RFID'li alışveriş sepeti

## 3.5 RFID Kimlik

Günümüzde kimlikler, içinde RFID temelli telsiz ve buna bağlı bir mikrobilgisayarın bulunduğu kartlar biçiminde üretilmektedir. Çalışma ilkesi RFID etiketi ile aynı olan bu kimlik kartları, etiketten çok fazlasını barındırmaktadır. Güvenlik açısından yakın erimli okuyucular ile iletişime geçmektedir. Bu nedenle yakın erişimli yöntemleri kullanırlar. Ülkemizde temassız kart olarak anılan bu kartlar küçük ödemeler için önerilmektedir.




**Şekil-3.26**: RFID'li market

# Kaynaklar ve Önerilen Yayınlar

[1] Keyence, *Barcode Handbook, https://www.keyence.com/*

# 4

# E-Ticaret

Önceki bölümlerde, ticaretin temel özellikleri ve ticarette kullanılan araçlar tanıtılmıştı. Ayrıca, özellikle toptan ticarette kullanılan EDIFACT ölçünü açıklanmıştı. Bu bölümde Genelağ üzerinden gerçekleştirilen ve ağırlıklı olarak perakende ticareti kapsayan e-ticaret tanıtılacaktır.

Genelağ düşüncesinin temeli 1966 yılında başlatılan DARPA (Defense Advanced Research Projects Agency ) projesine kadar gitmektedir. Bu proje 1970 yılında ARPANET'e (Advanced Research Projects Agency Network)dönüşmüştür. Bu araştırma projesi kapsamında bilgisayarlar arası dosya aktarım protokolü TCP/IP geliştirilmiştir. Bu çalışmalardan esinlenenler 1993 yılında Internet Society'i kurdular. 1996 yılında World Wide Web'in kurulması ile Genelağ doğmuş oldu [1].

Genelağ'ın insanlığa önemli katkıları olmuştur. Bu katkılardan biri de e-ticarettir. Özellikle perakende ticarette önemli bir yol aldığı söylenebilir. Günümüzün sayılı büyük firmalarına baktığımızda karşımıza e-ticaret firmaları çıkmaktadır. Bu firmalar e-ticaret yöntemiyle dünya genelinde satış yapmaktadırlar. E-ticaret etkinlikleri şöyle sınıflandırılmaktadır:

- Firma - Müşteri (F-M)
- Firma - Firma (F-F)
- Firma - Kamu (F-K)
- Birey - Kamu (B-K)
- Birey - Birey (B-B)
- Birey - Firma (B-F)
- Kamu - Birey (K-B)
- Kamu - Firma (K-F)
- Doğrudan - Birey (D-B)

E-ticaret ile birlikte gündeme gelen ve günümüzde yaygın olarak kullanılan bazı uygulamalar aşağıda sıralanmıştır.

- Sözel e-ticaret
- Sayısal cüzdan
- Elektronik bilet
- Çevrimiçi artırma (müzayede)
- Genelağ bankacılığı
- Sanal yardımcı
- Ödeme sistemleri

Genelağ üzerinden sürdürülen ve e-ticaret adını alan bu yeni ticaret modelini farklı açılardan sınıflandırabiliriz. Günümüzdeki e-ticaret uygulamalarını, şöyle de sınıflandırabiliriz:

- Ürün pazarlayanlar
- Hizmet sunanlar
- Aracılık yapanlar

Genelağ'da ürün pazarlayan e-ticaret siteleri incelendiğinde karşımıza aşağıdaki durum çıkmaktadır:

- Kendi ürettiği ürünü kendi pazarlayanlar
- Başkalarının ürettiği ürünler için pazar ortamı sağlayanlar
- Bireyler arası alışverişe ortam sağlayanlar

E-ticaretin hızlı gelişmesinin nedenleri şöyle açıklanabilir:

### Kısa Sürede Başlayabilme

Bir e-ticaret sitesi kurmak için gerekli olan hizmetler ve yazılımlar hazır bulunabilmektedir. Çoğu yazılım araçları şablon olarak sağlanabilmektedir. Bu şablon yazılımlar üzerinde, firmaya özel biçimlendirme yapılarak kısa süre içinde bir e-ticaret sitesi kurulabilmektedir.

### Kesintisiz Açık Olma

E-ticaret işletmeleri günün her anında ve haftanın her günü kesintisiz hizmet verebilmektedir. Bu özellik dünya genelinde satış yapabilme olanağı sağlamaktadır.

### Tutumlu

Geleneksel ticari işletmeler ile karşılaştırıldığında e-ticaret firmalarının masraflar ve giderlerinin daha düşük olduğu söylenebilir. Örneğin, bir bankanın müşterilerine banka şubesinde verdiği bir hizmetin bedeli yaklaşık olarak 20 TL (2,6 ABD Doları) olarak hesaplanırken aynı hizmeti Genelağ üzerinden verdiğinde gideri 1 TL dolayına düşmektedir. Çünkü bina, ısıtma, aydınlatma, çalışan ve güvenlik giderleri azalmaktadır.

### Kolay Büyüyebilme

Çok küçük ölçekte kurulan e-ticaret firmaları zaman içinde kolayca büyüyebilmektedirler. Büyümeleri için gerekli olan yatırım ağırlıklı olarak bilgi sistemleri yatırımıdır. Bilgi sistemlerinin büyütülmesi, binaları büyütmenin yanında çok kolaydır

### Kolaylaştırılmış Ödeme

Satılan ürün ile ilgili ödeme süreci çok kolay ve güvenli biçimde yapılabilmektedir. Ödeme işlemleri gibi, ürünlerin müşteriye ulaştırılması işlemleri de oldukça kolaylaştırılmıştır.

### Hazır Pazarlama Araçları

E-ticaret firmalarının kullanabileceği, ürün tanıtımı, veri analizi, müşteri sadakati gibi yararlı programlar e-ticaret sitesine eklenebilecek biçimde sağlanabilmektedir. Bu tür programlar e-ticaret firmalarının verimini artırmaktadır.

### Kaliteli Müşteri Hizmeti

Bilişim sistemi destekli e-ticaret siteleri müşterilerinin memnuniyetini artırmak üzere önemli hizmetler sunabilmektedir.

Bu bölümde e-ticaret modelleri tanıtılacak ve ticaretin yapılış biçimi ve bilişim yönü ile incelenecektir. E-ticaretin güvenlik, etik, hukuk ve yasal yönleri daha sonraki bölümlerde ele alınacaktır.

## 4.1 E-Ticaret Modelleri

Bu kısımda, bilinen e-ticaret modelleri tanıtılacaktır. E-ticaret modelleri tanıtılırken alışılagelmiş ticaret modelleri ile olan benzerliklerine de değinilecektir. Böylece e-ticaretin sağladığı üstünlükler de ortaya konmuş olacaktır.

### 4.1.1 Kendi Ürününü Pazarlayan

"Kendi ürününü Genelağ üzerinden pazarlamak isteyen bir firma ne yapmalıdır?" sorusunu yanıtlamak için önce e-ticaret öncesi ürünlerini nasıl sattığını bilmekte yarar vardır. Üzerinde irdeleme yapacağımız örneğimizi gömlek üreten ve kendi mağazasında satan bir firma olarak seçelim.

Cadde ya da bir alışveriş merkezinde dükkanı olan ve yalnızca kendi ürettiği gömlekleri pazarlayan firmanın cephesinde bir vitrini olmalıdır. Vitrine koyduğu ürünler, en çok satan ürünler içinden seçilebileceği gibi indirime girmiş ürünler de olabilir. Önemli olan dükkânın önünden geçenlerin dikkatini çekmektir. Vitrindeki ürünlerden biri veya birkaçı bir müşterinin dikkatini çektiğinde, müşteri dükkânın içine girecektir. Dükkan içine giren bir müşteriyi birinin karşılaması, hoş geldiniz, hangi ürüne bakıyordunuz deyip yönlendirmesi müşteriyi memnun edebilir. Karşılayan kişinin yardımıyla, müşteri vitrinde gördüğü ürüne ulaştırılabilir. Bundan sonra müşteri seçtiği ürünün farklı renkteki çeşitlerini inceleyebilir. Beğendiklerini alıp deneme odasında giyip üzerine yakışıp yakışmadığını inceleyebilir. Deneme odasından çıkan müşteri ile bir çalışanın ilgilenmesi müşteriyi memnun edebilir. Hatta müşteriye, beğendiği ürünün yanında, seçtiği ürün ile birlikte kullanabileceği başka ürünler de önerebilir. Müşteri satın almak istediği ürünleri kasaya götürür ve ödemesini yapar. Satın alınan bir ürünün belli süre içinde iade edilebilmesi hakkı yasalarla belirlenmiştir. Bu süre içinde iade edilen ürün için yapılmış olan ödeme geri alınır.

Alışılagelmiş mağaza düzeninde yaşanan bu deneyimi e-ticaret ortamımıza nasıl aktarabileceğimizi adım adım izleyelim.

#### Vitrin

Mağaza vitrini için yaptıklarımızı e-ticaret sayfamızda da yapmalıyız. Bunu yaparken, bilgisayarın grafik yeteneklerinden yararlanılabilir. Örneğin durağan nesneler yerine üç boyutlu canlandırmalardan yararlanılabilir. Gömlekler farkı mankenler üzerinde sunulabilir. Müşterinin bu sunumlara etkileşimli olarak katılması sağlanabilir.

#### Karşılama

Müşteriyi karşılamak amacıyla soru yanıtlama dizgelerinden yararlanılabilir. Robot yardımı ile müşterinin isteği öğrenilmeye çalışılabilir.

#### Müşterinin Niyetini Anlama

Müşterinin niyetinin ne olduğunu anlamak üzere çok sayıda araştırma çalışması yapılmaktadır. Müşterinin hangi ürünleri izlediği, hangi ürünleri izlerken daha çok zaman harcadığı, belli ürünleri birden kez inceleyip incelemediği gibi ölçümler ile müşterinin niyeti anlaşılmaya çalışılmaktadır.

Müşterinin niyeti anlaşılmasından amaç, müşteriye en uygun ürünleri sunmaya çalışmaktır. Böylece müşteri kendisini özel hisseder ve hedeflediği ürüne kısa sürede ulaşır.

### Seçtiği Ürünü Deneme Olanağı Sunmak

Mağazalarda, insanlara giysileri deneme olanağı verilmektedir. benzer bir olanağın e-ticarette sunulması gerekir. Bu konuda önemli çalışmalar bulunmaktadır. Bazı uygulamalarda, müşteri vücut ölçülerini vermektedir. Uygulama kişinin seçtiği ürünü kişinin ölçülerine uyan modele giydirmektedir. Müşteri kendisine benzeyen bir mankeni de seçebilmektedir. Bu tür üç boyutlu grafik çalışmaları oldukça gelişmiştir. Bazılarında, değişik ortamlarda canlandırma yapılabilmektedir. Müşteriye ürünün tüm çeşitleri deneme olanağı vermek oldukça yararlı olur. Böylece müşteri olası tüm çeşitleri üstünde denemiş olabilir.

### Ürün Karşılaştırması

Müşteriye benzer ürünleri sunmak ve müşterinin bunları karşılaştırmasını sağlamak müşteri memnuniyeti için yararlı olabilir. Önerilen ürünleri karşılaştırabileceği bir ortam sunulduğunda, müşteri neden belli bir ürünü yeğlemesi gerektiği sonucuna varır. Tüm ürünlerin üreticisi aynı firma olmasına karşın böyle bir olanağı sunmak müşteri memnuniyetini artırır.

Aynı bölümde, önerilen ürün seçeneklerini daha önce satın almış olanların görüşleri eklenebilir. Bir ürün ile ilgili görüşlerin sayısı müşterinin karar vermesini doğru yönde etkiler.

### Birlikte Alabileceği Ürünleri Sunmak

Müşteri bir ürünü almaya karar verdikten sonra kendisine bir başka ürün daha satılıp satılamayacağı araştırılabilir. Birlikte satış denilen bu yöntemin en ilkel uygulaması, satın almaya karar verdiği ürünleri daha önce satın almış olanların başka hangi ürünleri aldıklarını söylemektir. Bu tür öneriler giysi seçiminde çok yararlı olmayabilir. Çünkü insanlar aynı giysiyi bir başkasının üzerinde görmeyi sevmezler.

Birlikte satılabilecek ürünler, müşteriye önerilirken, müşterinin kendisine özgü önerilerde bulunmak, özel indirimler sağlamak daha çekici olabilir.

### Müşteri Bağlılığı (Sadakati)

Bildiğimiz mağazacılıkta, müşterinin ayağını alıştırmak diye bir deyim vardır. Bunun e-ticaretteki karşılığı müşteri bağlılığı veya sadakati olabilir. Müşteri bağlılığı sağlamak üzere çok sayıda yazılım, bugün hazır olarak sağlanabilmektedir. Bu yazılımlar, müşterinin bireysel bilgileri, alışveriş alışkanlıkları ve alışveriş geçmişine bakarak müşteriyi tanımayı amaçlarlar. Hatta bireyin sosyal medyadaki etkinlik ve bağlantılarını inceleyerek daha ayrıntılı sonuçlara ulaşabilmektedir. Müşteri hakkında toplanan bu

bilgiler kullanılarak, müşteriye çekici gelebilecek ürünler sunulabilmekte, özel indirimler önerilebilmekte, özel günlerinde kutlama mektubu veya hediye gönderilebilmektedir. Amaç müşterinin ayağını firmaya bağlamaktır.

**Ödeme Aşaması**

Ödeme aşaması çok basit olarak kredi kartı veya banka havalesi ile yapılabileceği gibi müşteriye ödeme kolaylıkları da sağlanabilir; örneğin ödeme taksitlendirilebilir, eski bir müşteri ise geçmişte yaptığı alımları ile orantılı indirim sağlanabilir. Müşteri bağlılığını artırmak amacıyla müşterilere ödül kazandıran yöntemler kullanılabilir.

**İade**

Müşteri memnuniyetini sağlamak adına, satın aldığı ürünü belli bir süre içinde iade etmek hakkı verilmesi ticaret yasalarının belirlediği bir kuraldır. Bu kural e-ticaret yapan firmalar için de geçerlidir.

### 4.1.2 Başkasının Ürününü Pazarlayanlar

Günümüzde en yaygın olarak gördüğümüz e-ticaret siteleri, başkalarının ürünlerini pazarlayan sitelerdir. Bu tür pazarlama ortamların esin kaynağı her şeyin satıldığı marketlerdir. Bu nedenle önce, her şeyin satıldığı marketlerin nasıl çalıştığını öğrenmekte yarar vardır.

Her şeyi satmak üzere kurulan marketler önce ürün sınıflarına göre bölmelenirler, örneğin gıda, giysi, spor, alet, araç bölmeleri gibi. Ürünler genellikle raflarda bulunur, dolayısıyla müşteri inceleyebilir. Müşteri satın almak istediği ürünleri sepetine koyar ve kasada ödeme yapar.

Mahalle bakkalı veya küçük marketlerin raflarında bulunan ürünler, market sahibinin peşin ya da vadeli satın aldığı ürünlerdir. Diğer bir anlatımla, markette bulunan ürünlerin karşılığı market sahibi tarafından ödenmiş veya ödenecektir. Buna karşın büyük marketler farklı çalışmaktadırlar. Büyük marketler, üreticilere yer (raf) kiralamaktadır. Yerin market içindeki konumu ve boyutuna göre üretici markete kira ödemektedir. Buna ek olarak kullanacağı depo alanı için de ödeme yapması gerekebilir. Raflara ürünleri yerleştirmek, eksilenlerin yerine yenilerini koymak da üreticinin yükümlülüğündedir. Market işletmecisi, satışlardan elde edilen gelirleri düzenlemek ve ürün sahiplerine belli aralıklar ile ödemek durumundadır. Bu anlatılanlardan, büyük market işletmecilerinin işlerinin genel hatlarıyla, pazar ortamı sunmak ve kasa hizmeti vermek olduğu söylenebilir. Bu değerlendirmelerin sonucu olarak, başkasının ürününü pazarlayan e-ticaret uygulamalarına e-market diyebiliriz ve bundan sonraki kısımlarda bu adla anılacaktır.

E-marketler büyük marketlerin işleyişini örnek almışlardır. İşleyiş biçimleri aşağıda açıklanmıştır:

### Ana Sayfa

E-marketler için mağaza vitrini benzeri bir uygulama yeterli olmayabilir. Bunun yerine ana sayfa kavramından yararlanılabilir. Ana sayfada, e-marketin genel tanıtımı yapılabilir ve buradan diğer bölümlere geçiş yapılması sağlanır.

Ana sayfa üzerinde günün fırsatlarına ve firmaların reklamlarına yer verilebilir.

### Pazarda Yer Verme

E-markette yer almak isteyen ticari kuruluşların, e-marketi işleten firma ile anlaşmaları gerekir. Anlaşma özetle, e-markette ne kadar yer isteneceği, kaç ürün tanıtımının yapılacağı, yer kirası, ödeme koşulları ve ürünün gönderi biçimi ve bedeli konularında olabilir.

### Müşterinin Niyetini Anlama

Müşterinin niyetinin ne olduğunu anlamak e-marketler için de önemli bir araştırma konusudur. Müşterinin aradığı bir ürüne en kısa sürede ulaşması müşteri memnuniyetinin temel ilkesidir. Müşterinin hangi sayfalarda dolaştığı, hangi ürünleri izlediği, hangi ürünleri izlerken daha çok zaman harcadığı, belli ürünleri birden çok kez inceleyip incelemediği gibi ölçümler müşterinin niyeti anlamak için yararlanılan değerlerdir.

### Seçtiği Ürünü İnceleme ve Deneme Olanağı Sunmak

E-marketler çok farklı özellikte ürünlerin satışa sunulduğu yerlerdir. Sattıkları ürünlerin bazıları denenebilir bazıları denenemez. Giysilerin denenmesi için, bir önceki bölümde anlatılan yöntemler burada da kullanılabilir. Giysiler manken üzerine giydirilip müşteriye sunulabilir.

Alet ve aygıt türü ürünleri tanıtmak, nerede ve ne amaçla kullanılabileceklerini müşteriye göstermek üzere video gösterimlerden yararlanılabilir. Gerçek kullanıcıların görüşleri videolar ile gösterilebilir.

Özetle, ürünün niteliğine bağlı olarak müşteriye bilgi sunmak önemlidir. Sunumun gerçekçi olması, canlandırmalar ile desteklenmesi müşteride olumlu etki yapar. Bu tür sunumlar ürün sahipleri tarafından hazırlanır ve üreticinin sunucusunda bulunur. E-market işletmesi, ayrıntı isteyen müşteriyi üreticinin sunucusuna yönlendirir.

### Ürün Karşılaştırması

E-marketlerde satılan ürünlerin çeşitleri çoktur. Bu durum müşterilerin karar vermelerini zorlaştırabilir. Müşterilere yardımcı olmak için, ürünlerin karşılaştırılabileceği bir ortam sunulabilir. Müşteri karşılaştırmak istediği ürünleri bu ortama taşır ve karşılaştırılmasını ister. Karşılaştırma, nitelik ve fiyat olarak yapılıp müşteriye sunulur. Ürün karşılaştırmalarının ayrıntılı ve yansız olması müşteride güven duygusunu artırır.

Ürünlerin karşılaştırıldığı bölüme, bu ürünleri daha önce satın almış olanların görüşleri eklenebilir. Bir ürün ile ilgili müşteri görüşlerinin sayısı, o ürünün değerlendirilmesinde katkı sağlar. Çok az sayıdaki görüş anlamlı olmayabilir.

**Birlikte Alabileceği Ürünleri Sunmak**

Bir ürünü almak üzere sepetine atan müşteri için birlikte satın almayı düşünebileceği ürünler önerilebilir. E-marketlerde satılan ürünler farklı üreticilerin ürünleri olacağından, birlikte satın alınabilecek ürünü öncelikle, sepete atılmış ürünün üreticisinden seçmek gerekir. Daha sonra farklı üreticilerin ürünlerinde öneriler yapılabilir.

**Müşteri Bağlılığı (Sadakati)**

E-market türü ticarette müşterinin bağlılığı e-market açısından değerlendirilir. Çünkü aynı ürünü müşteri başka e-pazarlardan da satın alabilir. Müşterinin bu e-pazarı seçmesi için fiyatın düşük, hizmetin iyi ve teslimatın hızlı olması, dolayısıyla müşteriyi memnun etmesi gerekir. E-marketler müşteri bağlılığını sağlayabilmek için önceki bölümde anlatılan yöntemlere benzer yöntemler kullanabilirler.

**Ödeme Aşaması**

E-marketler üretici adına ödemeyi almaktadır. Dolayısıyla her ürün için farklı bir ödeme yöntemi uygulayabilir. Ödeme kredi kartı veya banka havalesi ile yapılabileceği gibi müşteriye ödeme kolaylıkları da sağlanabilir. Müşteri bağlılığını artırmak amacıyla müşterilere ödül kazandıran yöntemler kullanılabilir. E-marketi işleten kuruluş, satışlardan elde ettiği gelirleri, üreticilere belli aralıklar ile gönderir.

**İade**

Müşteri memnuniyetini sağlamak adına, satın aldığı ürünü belli bir süre içinde iade etmek hakkı verilmesi ticaret yasalarının belirlediği bir kuraldır. Bu kural e-ticaret yapan firmalar için de geçerlidir.

### 4.1.3 Bireyler Arası Alışverişe Ortam Sağlayanlar

Bireyler arası alışverişi Genelağ üzerinden sağlamayı amaçlayan girişimler, başlangıçta bir bireyin sahip olduğu bir nesneyi bir başkasına satabilmesi için kurgulanmıştır. Bu aşamada açık artırma yöntemlerinin kullanıldığı görülmüştür. Daha sonraları bireyler arası alışveriş siteleri pazar yerine dönüşmüştür. Bu pazar yerinde bireyler veya ticari firmalar kendileri için tezgah kurabilmişler ve satış yapabilme olanağı sağlamışlardır. Anlatılanlardan da anlaşılacağı gibi uygulama semt pazarlarının Genelağ üzerindeki uygulamasıdır. Bu yüzden e-pazar yeri veya kısaca e-pazar diye adlandırılmaları doğru olur.

Bireyler arası alışverişte, elindeki bir nesneyi satmak isteyen satıcı e-pazarda nesnenin tanıtımı için yer kiralar; bunun için ödeme yapar. Nesnenin satışta kalacağı süreyi belirtir. Nesneye ilgi duyanlar fiyat teklifinde bulunurlar. Nesnenin satışta kaldığı süre sonunda en yüksek fiyatı

vermiş olan kişi ürünü satın almaya hak kazanır. Ödemeyi e-pazar yöneticisine yapar. E-pazar işletmecisi, ürün sahibine ürünü alıcıya göndermesini söyler ve bekler. Ürünü satın alan taraf ürünü aldığını belirttiğinde e-pazar işletmecisi satıcıya komisyonunu keserek ödemeyi gönderir.

Bireyler arası e-ticareti sağlamak amacıyla kurgulanan e-pazarlar zamanla daha kapsamlı hale gelmiştir. Günümüzde küçük ve büyük işletmeler, perakende ve toptan ürün satışlarını e-pazarlarda yapabilmektedir. Bu nedenle e-pazarlar satıcıların niteliklerine uygun tezgah, dükkan veya mağaza sunmaktadırlar. Sağlanan olanak ile orantılı olarak yer kirası istemektedirler. Bazı e-pazarlar yer kirası almayıp yalnızca satıştan ortalama %15 komisyon almaktadırlar. E-pazarlarda ödeme biçimi, bireyler arası ticaret için oluşturulan biçimiyle devam etmektedir.

Günümüzde, e-marketler ile e-pazarların sundukları olanaklar birbirine yaklaşmıştır. Bazı e-market işletmeleri firmalara e-market içinde firmaya özgü mağaza açma olanağı sunmaya başlamıştır.

### 4.1.4 Hizmet Sunanlar

Genelağ üzerinden kişi, firma ve kamu kuruluşları hizmet sunmaktadırlar. Verdikleri hizmetlerin para ile ilişkisi var ise bunlar e-ticaret sınıfına girmektedir. Örneğin Maliyenin vatandaşlara sunduğu vergi beyannamesi verme, vergi borcu ödeme hizmetleri bu sınıfa girmektedir. Bir kişi veya kuruluşun bedeli karşılığında danışmanlık hizmeti vermesi de aynı sınıfa girer.

Hizmet veren sitelerden beklenen özellikler, doğal olarak ürün pazarlayanlardan farklı olacaktır. Özellikle kamu kurumlarının amacı yalnızca hizmet vermektir. Ana sayfa üzerinde vatandaşları almak istedikleri hizmete yönlendirmek ve müşteri kimliğinin geçerlenmesi ana hedeftir. Müşteri memnuniyeti, müşteri sadakati gibi konular bu tür kuruluşlara uzaktır.

### 4.1.5 E-Bankacılık

Genelağ üzerinden yapılan bankacılık, e-ticaretin en yaygın biçimlerinden biri sayılabilir. E-Bankacılık olarak adlandıracağımız bu uygulama bankalar ve müşteriler için önemli kazançlar sağlamaktadır. E-Bankacılık uygulaması ile bankaların müşteriye verdikleri hizmetin bedeli düşmüştür. Bir önceki kısımda açıklandığı gibi, banka şubesinde sunulan birim hizmetin bedeli yaklaşık 20 TL olarak hesaplanmaktadır. Bu hizmet, çok basit bir para bozdurma, para yatırma veya hesap açma işlemi olabilir. Benzer işlemleri e-banka üzerinden sağlamanın bedeli yaklaşık 1 TL dolayındadır. Bankaların milyonlarca müşterisi olduğu düşünüldüğünde e-bankacılığın bankalar için ne kadar kazançlı olduğu kolayca söylenebilir. E-Bankacılık müşteriler için de kazançlıdır. Müşterinin banka şubesine gitmesine, şubede sıra beklemesine gerek yoktur. Müşteri evinden veya işyerinden bilgisayarı veya cep telefonunu kullanarak her yerden banka

işlemlerini yapabilmektedir. E-bankacılık uygulamaları iki tarafa da önemli kazançlar sağladığı için tutmuş ve yaygınlaşmıştır.

Bankalar hizmet mi yoksa ürün mü satarlar sorusunu bankacılara sorduğumuzda ürün yanıtını alırız. Bankacı gözüyle, bir kredi paketi, kredi kartı ürün olarak değerlendirilmektedir. Bankaları, bir giysi üreten firmadan ayıran önemli farklılıklar vardır. En önemli fark, bankalar insanların güven duydukları kurumlar olmasıdır. Dolayısıyla e-bankacılığın oluşturulmasında ilk önceliği olan konu güvenlik olmalıdır. Günümüzde Türkiye'deki bankaların e-bankacılık hizmetleri dünyanın önde gelen örnekleri arasındadır.

Türkiye'de e-bankacılık 1997 yılında başlamış ve kısa sürede önemli gelişmeler göstermiştir. Günümüzde para vermek dışında akla gelebilecek her türlü bankacılık hizmeti vermektedirler. E-bankacılık Genelağ üzerinden yapılacağından, değişik bir söyleyişle herkese açık bir ortamda yapılacağı için müşterinin bilgilerinin (hesap numarası ve parola) herkes tarafından görülmesi olasıdır. Bu durum bankacılık işlemleri için kabul edilebilir değildir. Türkiye'deki e-bankacılığın gelişmesi süresinde yaşanmış olan güvenlik sorunları, fikir vermesi açısından önemlidir ve gelişmeler zaman sırasıyla anlatılacaktır.

### Açık iletişim

E-bankacılığın ilk yıllarında müşteri ile banka arasındaki iletişimin güvenliği bankalar tarafından sağlanmaya çalışılmıştır. Bu amaçla, bankalar müşterilerine bir program vermek zorunda kalmıştır. Bu program kullanılarak müşteri ile banka arasındaki iletişim şifrelenmeye çalışılmıştır.

Müşterilere verilen program çalıştırıldığında bankanın bilgisayarı ile iletişime geçiyordu. Bu iletişim sırasında asimetrik şifreleme yöntemi kullanılarak müşterinin bilgileri bankaya iletiliyordu. Müşteri kimliği banka tarafından geçerlendikten sonra oturum boyunca kullanılacak simetrik şifrelemenin parolası gönderiliyordu. Bundan sonra müşteri ile banka arasındaki iletişim simetrik şifreleme yöntemiyle gizleniyordu.

### SSL Kullanımı

Ağlar üzerinden yapılan iletişimin güvenilirliği üzerine çalışan Netscape firması Secure Sockets Layer (SSL) adını verdiği güvenlik protokolünü 1994 yılında tanıttı. Ancak yeterli güvenliği sağlayamadığı için ilk sürümü kullanılmadı ancak 3. sürümü 1996 yılında kullanılabilir duruma geldi ve 1999'da güncellendi.

SSL protokolü e-bankacılık için güvenli bir iletişim ortamı sağlıyordu. Bu protokol kullanılarak başlanılan bir web sayfası ile başlanan bilgisayar arasındaki iletişim şifrelenerek gidip geliyordu. Bu olanak bankalar için önemli bir rahatlık sağladı ve artık müşterilerine özel bir program vermek zorunda değillerdi.

### Tuşları Okuma

SSL protokolü ile bankanın sunucusuna bağlanan müşterinin müşteri numarası ve parolası bankaya şifrelenmiş olarak gönderiliyordu ve bu yeter sanıldı. Ancak insanların bankadaki paralarını çalmayı amaçlayan saldırganlar bir yöntem geliştirdiler. Müşterilerin bilgisayarına gönderip yüklenmesini sağladıkları, adına "keylogger" denilen program, müşterinin bankaya bağlanmak istediğini anladığı an müşterinin tuş takımında bastığı her tuşun değerini saldırganın bilgisayarına gönderiyordu. Böylece saldırgan müşterinin hesap numarası ve parolasını açık olarak öğrenebiliyordu. Bu casus programı, bankaların web adreslerini bildiği için müşteri bir bankanın web adresini yazmaya başladığında uyanıyordu.

### Sanal Tuş Takımı

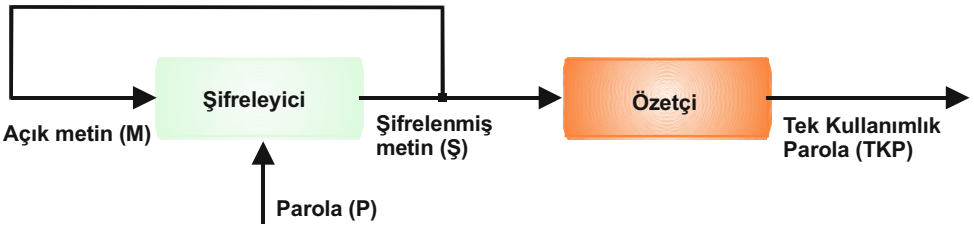
Müşterinin tuş takımının okunduğu anlaşılınca, bankalar ekran üzerinde oluşturulan sanal tuş takımına geçtiler. Sanal tuş takımında tuşların yerleri de ölçünlü değildi. Saldırganlar bunun üzerine "screenshot" adı verilen programı geliştirdiler. Müşteri bankaya bağlanmaya başladığında, bu program çalışmaya başlıyor ve belli aralıklar ile ekranın kopyasını alıp saldırgana gönderiyordu. Böylece e-bankacılıkta bir güvenlik sorunu daha çıkmıştı. Screen shutter programı, müşterinin tuş takımını izliyor ve bir banka adresi yazıldığında ekran kopyalarını çekmeye başlıyordu.

### Tek Kullanımlık Parola (TKP)

Bilgi güvenliği ve şifreleme üzerinde çalışanlar, bir kez kullanılacak parola üzerinde uzun süredir çalışıyorlardı. Adından da anlaşılacağı gibi üretilecek parola bir kez kullanılacak ve kullanıldıktan sonra geçerliliğini yitirecekti. Çok ilkel bir uygulama Şekil-4.1'de gösterilmiştir. Şekilde gösterilen TKP şöyle çalışıyordu: Bankanın bilgisayarı, üzerinde belli sayıda örneğin 20 rastgele sayı bulunan çıktılar üretir. Her sayfaya bir numara verilir. Dolayısıyla her sayfada bulunan rastgele sayılar bilgisayarın veri tabanına kaydedilir. Bir müşteri bankaya gelip bu TKP kağıtlarından aldığında, banka görevlileri verilen kağıdın numarasını (TKP No) bilgisayara girerler. Böylece bilgisayar müşterinin e-bankaya giriş yaparken kullanabileceği parolaları bilmiş olur. Müşteri e-bankaya her bağlandığında sayfadaki bir parolayı kullanır ve kullandığını çizer. Tüm parolalar kullanıldığında bankaya gidip bir yeni TKP kağıdı alır. Çok basit olan bu yapı müşteriye güvenlik sağlar.


**Şekil-4.1**: Kağıt üstü TKP

2005 yıllarında TKP üretici araçlar yapıldı. Bu araçlar her çalıştırıldığında bir yeni parola üretmek üzere geliştirilmiş mikrobilgisayarlardı. Bu yeni TKP'lerin çalışma ilkesi Şekil-4.2'de gösterilmiştir.




**Şekil-4.2**: Tek kullanımlık parolanın ilkesel yapısı

İlkesel yapısı verilen TKP şöyle çalışmaktadır. Şifreleyicinin iki girişi ve bir çıkışı vardır. Açık metin (M), Parola (P) ile şifrelenerek Şifrelenmiş metin (Ş) üretilir. Üretilen metin, bir sonraki adımda M olarak kullanılır. Böylece her adımda farklı bir Ş elde edilir. M ve P nin ilk değerleri bilindiğinde üretilecek Ş değerleri hesaplanabilir. TKP'yi daha güçlü kılmak için Özetçi Ş'ye Hash işlevi uygular. Hash işleminin özelliği bir özetçinin çıkışında üretilen TKP değerinden Ş'yi öğrenme olanağı yoktur. Kağıt TKP'deki gibi bu donanımsal TKP'nin ilk değerlerinin bankanın bilgisayarına girilmesi yeterli olacaktır. Bu arada donanımsal her TKP'nin ilk değerlerinin farklı seçileceğini belirtmekte yarar vardır.

Donanım olarak değişik özellikte TKP aygıtları (çoğunlukla anahtar olarak anılırlar) üretilmiştir. Şekil-4.3'te bazı örnekler gösterilmiştir. Şekilde görülen örneklerden basit olan TKP'nin düğmesine her basıldığında yeni bir parola üretir. İkinci örnek TKP'nin çalışması için kullanıcının bir parola girmesi gerekir. Üçüncü örneğin etkin hale getirilmesi için kredi kartının takılması ve kredi kartının parolasının girilmesi gerekir.


**Şekil-4.3**: Donanımsal TKP örnekleri

Donanım olarak üretilen TKP'ler 2007-2012 arasında yaygın olarak kullanıldı ve e-bankacılığın güvenliğini artırdı. Bu arada donanımda kullanılan algoritmanın aynısını bilgisayarda ve akıllı cep telefonlarında da oluşturarak TKP uygulaması yapılmıştır.

### Onay Kodu

Cep telefonlarının yaygınlaşması, neredeyse herkesin bir cep telefonun olduğu noktaya gelindiğinde yeni bir çözüm oluşturuldu. Bu çözüm, e-bankaya bağlanan müşterinin cep telefonuna bir onay kodu gönderilmesi; gönderilen bu kod e-bankacılık sistemine girilerek işlemlere devam edilmesi biçimindeydi. Güvenliğin en temel ilkesi olan "bilgi ve çözümleyiciyi farklı kanaldan gönderme" ilkesine uygun olan bu yeni yöntem TKP'nin sağladığı güvenliği sağlamış ayrıca donanıma ödeme yapmayı ortadan kaldırmıştır.

Onay kodu kullanma sırasında bir açık görülmüştür. Bu açık kopya SIM kartının elde edilmesidir. İlk dönemlerde ikinci SIM kartı kolayca elde edilebildiği için sorunlar yaşanmış ancak bu yol kısıtlanınca sorun ortadan kaldırılmıştır.

Yukarıda anlatılanlar, 20 yılda e-bankacılığın güvenliğinin artırılması için yapılan çalışmaların özetidir. Günümüzde e-bankacılığın güvenlik düzeyi üst düzeye çıkarılmıştır. E-bankacılık üzerinde yapılabilecek işlemlerden önemli olanlar aşağıda sıralanmıştır:

- Vadeli ve vadesiz (TL veya döviz) hesap açma
- Hesap kapatma
- Hesaba veya kredi kartına havale veya EFT yapma
- Döviz alıp satma
- Otomatik ödeme

Göz önünde bulunan bu hizmetlere ek olarak, müşterilerin güvenliğini sağlamak üzere bazı olanaklar ve kısıtlamalar sağlanmaktadır. Müşteri hangi işlemleri yapabileceğini, zaman aralığını ve para miktarının sınırını belirleyebilmektedir. Bu tür yetki belirleme işlemleri geçmiş dönemlerde yaşanmış olaylardan çıkarılan derslerin sonucudur.

## 4.1.6 Aracılık Yapanlar

Hiçbir üretim yapmayan, başkalarının ürettiklerini de satmayan, yalnızca aracılık eden e-ticaret siteleri de bulunmaktadır. Bu siteler çok basit bir anlatımla telefon santral çalışanı gibi görev yapmaktadırlar. Aracı firmalara verilebilecek en uygun örnekler, çiçek veya yemek firmaları için aracılık yapan sitelerdir.

Aracı siteler, aracılık yaptıkları firmaların ürünlerini web sayfalarında tanıtırlar, fiyatlarını gösterirler. Müşteri sipariş verdiğinde lokanta veya çiçekçiye haber verirler. Yemek veya çiçek bunları üreten tarafından müşteriye ulaştırılır. Ödeme aracı firmaya veya üreticiye yapılabilir. Aracı firma her satıştan bir komisyon alır.

### 4.1.7 E-Artırma

Artırma veya diğer bir deyişle müzayede işleri de günümüzde Genelağ üzerinden yapılabilmektedir. Çalışma ilkeleri eski artırma işlerine çok benzemektedir. Bir artırmaya girebilmek için önce bu siteye üye olmak gerekir. Ardından gireceği artırma için belirlenen pey akçesi yatırması gerekir. Bunun dışında, artırmayı yöneten firmanın belirlediği kurallara uygun olarak artırmaya katılabilir.

## 4.2 E-Ticaret Sitesinin Kurulması

Her gün yeni bir e-ticaret sitesi açılıyor. Bu sitelerden bazıları yaşıyor ve gelişiyor, bazıları ise kapanıyorlar. Bir e-ticaret sitesinin yaşayabilmesi için kuruluş aşamalarını düzgün geçmesi gerekir. Bu aşamaları düzgün geçmesine karşın ilerleme sağlayamayabilir. Ancak bu ön çalışmaları yerine getirmez ise yaşama şansı hiç yoktur. Bir e-ticaret sitesi kurmak için izlenmesi gereken adımlar şunlardır:

- Sitenin amacının belirlenmesi
- İş modelinin belirlenmesi
- Site adına karar verilmesi
- Yasal gereklerin yerine getirilmesi
- Web sitesini geliştirme aracının seçilmesi
- Web sayfasının tasarımı
- Sitenin güvenliği için gerekenlerin belirlenmesi
- Arama motoru seçimi veya geliştirilmesi
- Raporlama araçlarının seçimi
- Müşteri sadakati
- Müşteri memnuniyeti
- Soru yanıtlama sistemi
- Ödeme bağlantılarının yapılması
- Ulaştırıcıların seçimi

Yukarıda sıralanan aşamalar ile ilgili ayrıntılı bilgiler aşağıda verilmiştir:

### 4.2.1 Sitenin Amacı

Ticaretin amacı ürün satarak kazanç elde etmek olduğuna göre e-ticaret sitesi de bu amaçla kurulacaktır. Önceki kısımlarda açıklandığı gibi e-ticaret sitesi kendi ürününü pazarlayabileceği gibi, başkalarının ürünlerini de satabilir. Her iki durumda da sitenin amaçları önce belirlenmelidir. Örneğin amaç giyim, ev eşyaları, kitap kırtasiye, spor ürünleri, sinema tiyatro bileti olabilir. Dünyada satılabilecek ürünlerin çeşitleri oldukça çoktur.

Sitenin hedeflediği müşteri niteliklerinin belirlenmesi de bu aşamada önemlidir. Örneğin gençlere yönelik veya yalnızca kadınlara yönelik site kurulabilir. Hedeflenen pazar da önemlidir. Ülke sınırları içinde kalınabileceği gibi uluslararası ticaret de hedeflenebilir. Önemli olan o andaki boşluğu görmektir. Başka ülkelerde başarıyla uygulanan bir uygulamayı ülke koşullarına uygun olarak uygulamak da para kazanmayı sağlayabilir.

Sitenin amacı belirlenirken dikkat edilmesi gereken önemli bir nokta amaçlanan ticaretin yasal olması gerekir. Sırf para kazanmak için yasal olmayan ürün pazarlamak bu kitabın kapsamı dışındadır.

### 4.2.2 İş Modeli

Önceki bölümlerde e-ticaret bağlamında uygulanabilecek iş modelleri tanıtılmıştı: F-M, F-F, F-K, B-K, B-B, B-F, K-B, K-F, D-B. Kurulacak yeni sitenin bu iş modellerinden birine uygun olarak kurulması gerekir. Daha önce açıklandığı gibi e-ticaret siteleri ürün veya hizmet pazarlamak için kurulabileceği gibi üreticiler ile tüketiciler arasında aracılık yapmak üzere de kurulabilirler. Bir başka bakış açısından değerlendirildiğinde bir e-ticaret sitesi;

- Kendi ürettiği ürünü pazarlayabilir
- Başkalarının ürettiği ürünler için pazar ortamı sağlayabilir
- Bireyler arası alışverişe ortam sağlayabilir.

Yeni e-ticaret sitesi kurma çalışmalarının başlangıç aşamasında bu iş modellerinden birine karar verilmelidir. Belli bir iş modeline uygun olarak kurulan e-ticaret sitesinin zaman içinde kapsamını genişletebileceği veya çeşitlendirilebileceği söylenebilir. Ancak başlangıçtaki kurgulama önemlidir.

### 4.2.3 Site Adı

Başlangıç aşamasında önemsiz gibi görülse de bir e-ticaret sitesinin adının seçimi önemli olmaktadır. Site adı seçiminde dikkat edilmesi gereken noktalar şöyle sıralanabilir:

- Akılda kolay yer etmesi
- Dünya genelinde bilinir olma
- Hedeflenen ticaret alanı ile ilişkili olma
- Abecede ilk sıralarda yer alma
- Olabildiğince kısa olma

Siteye verilecek adın insanların aklında kolay yer etmesi için benimsenen yöntem, Dünya üzerinde bilinen ve çoğu dillerde aynı ad ile anılan nesneleri seçmektir. Örneğin, deniz, nehir, dağ, kıta adlarından birini veya dünya klasiklerinin bilinen kahramanlarının adlarından birini seçmek. Günümüzde başarılı sayılan ve çok büyük boyutlara ulaşmış e-ticaret sitelerinin adları incelendiğinde adlarını bu ölçütlere uygun seçtikleri görülür.

Siteye verilecek adın, hedeflenen iş modeli ile ilişkili olması, insanlarda çağrışım yapması açısından önemlidir. Örneğin, yemek alanında çalışmak isteyen bir sitenin adında "yemek" ve çiçek satmayı hedefleyen sitenin adında "çiçek" adının geçmesi uygun olur. Bir açık artırma sitesi için "artıran var mı" gibi ad verilebilir.

Site adı belirlenirken dikkat edilmesi gereken bir başka nokta, aynı adı alanların olup olmadığını araştırmaktır. Özellikle web sayfaları kurulmaya başlandığında bazı açıkgözler, bazı bilinen adları, ileride satmak üzere aldılar. Bir web sayfası için alan adı almak istendiğinde hiçbir sorgulama yapılmaması açıkgözlere fırsat yaratmıştı. Ancak bazı ülkeler, bu arada Türkiye alan adı alacak olanları sorgulamaya ve denetlemeye başlamıştır. Bu özen dünya genelinde görülmemektedir.

### 4.2.4 Yasal İşlemler

Bir ticari işletme açmak için gerekli olan resmi işlemler e-ticaret siteleri için de gereklidir. Ticaret yasası daha ileride açıklanacaktır. Şu aşamada, başlatılacak olan e-ticaret sitesinin arkasında yasal olarak kurulmuş bir ticari firmanın olması gerektiği söylenebilir. Bunun için firmanın resmi olarak kurulmuş olması, gerekli olan tüm yasal işlemlerin tamamlanması gerekir.

### 4.2.5 Web Sayfasını Geliştirme Aracı

E-ticaret yapacak olan firmaların bilişim sistemleri konusunda uzman olmaları beklenmemektedir. Günümüzde, e-ticaret sitesinin web sayfasını oluşturmak üzere hazır şablon geliştirme araçları sağlanabilmektedir. Bu şablon programlar üzerinde, kurulacak e-ticaret sitesi için uyarlamalar kolayca yapılabilmektedir.

Bünyesinde kuvvetli bir bilişim bölümü bulunan firmalar kendi web sayfalarını tasarlayıp geliştirebilirler. Bu yolu yeğleyenler de bulunmaktadır.

### 4.2.6 Web Sayfasının Tasarımı

Web sayfasının yapısı ve görüntüsü hedeflenen müşteri topluluğunun gelenek, görenek ve kültürüne uygun olmalıdır. Bir ülke için hazırlanmış bir web sayfası diğer bir ülkenin kültürüne uygun olmayabilir. Bu konuda yaşanmış önemli örnekler bilinmektedir. Örneğin, dünya genelinde çok başarılı olan bir e-ticaret sitesi Çin'de başarılı olamamıştır. Bu başarısızlığın nedenleri incelen bir Çinli firma çok başarılı sonuçlar elde etmiştir.

Bir web sayfası tasarımın dikkat edilmesi gereken bir başka konu, sayfanın kullanışlılığıdır. Genelağ'da gördüğümüz ve kullandığımız web sayfaları kullanılabilir niteliktedir ancak bazıları daha kullanışlıdır. Bir web sayfası tasarlanırken kullanışlı olması için bazı ölçütler belirlenir. Örneğin bir müşterinin istediği ürünü bulması için harcaması gereken adım sayısı ve süre belirlenir. Benzer şekilde web sayfası üzerinde arayacağı başka bilgilere ulaşım süresi ve arama adım sayısı belirlenir. Bu ölçütlere göre tasarlanan bir web sayfası tamamlandıktan sonra

kullanışlılık sınamasından geçirilir. Kullanışlılık sınaması için yetkin laboratuvarlardan destek alınabilir.

Bir web sayfasının kullanışlılığını artırmak için, kolay algılanan ekran düzenlemeleri, kullanıcının dikkatini çekecek renklendirmeler ve düğmeler kullanılabilir. Tüm bu çalışmalar yapılırken kullanıcıların genel beğenileri dikkate alınır.

### 4.2.7 Güvenlik Önlemleri

Ticaretin yapılabilmesi ve sürdürülebilmesi için gerek koşullardan birisi güvenli ortamdır. Genelağ'ın ticaret için gerekli olan güvenli ortamı tam olarak sağladığı henüz söylenemez. Çünkü Genelağ hizmete sunulurken, bugünkü yaygınlığa erişebileceği öngörülememiştir. Genelağ'daki iletişim protokolü olarak 1980 yılında ABD Savunma Bakanlığı (DoD) tarafından geliştirilmiş olan TCP/IP protokolü kullanılmaktadır. İki katmandan (Üst Katman (TCP: Transfer Control Protocol ) ve *Alt Katman* (IP: Internet Protocol) ) oluşan bu protokolün zayıflığı zaman içerinde anlaşılmış ve güvenliği artırmak için yeni sürümleri üretilmiştir.

**Üst Katman**

TCP/IP protokolünde iletilecek veri önce paketlere bölünür ve paketler alıcıya gönderilir. Alıcı gelen paketleri birleştirerek asıl veriyi elde eder. Üst katman içinde, Uygulama ve Taşıma katmanları yer alır.

**Uygulama Katmanı:** Farklı bilgisayarlarda bulunan uygulamalar arasındaki iletişimi sağlar.

**Taşıma Katmanı**: İki bilgisayar arasındaki veri akışını sağlar. Bu sunucudan sunucuya taşıma işlemidir

**Alt Katman:**

İletilmek istenen paketleri alıcının adresine iletir. Alt katman içinde Genelağ Katmanı, Ağ Erişim Katmanı ve Fiziksel Katman yer alır.

**Genelağ Katmanı**: Birbirine yönlendiriciler ile bağlanmış ağlar üzerinde, kaynak ve hedef bilgisayarlar arasında verilerin iletilmesini sağlar.

**Ağ Erişim Katmanı:** Bilgisayar ile ağ arasında mantıksal ilişkiyi kuran arabirim olarak değerlendirilir.

**Fiziksel Katman**: İletişim ortamının elektriksel ve fiziksel özelliklerini belirleyen katmandır.

TCP/IP protokolünün güvenliği ilerideki bölümlerde ayrıntılı biçimde ele alınacaktır.

E-ticaret sitelerinin güvenliğini artırmak üzere SSL protokolü kullanılmaktadır. Özellikle parasal işlerin sürdürüldüğü aşamalarda verileri şifreleyerek göndererek güvenliği artırmaktadır.

### 4.2.8 Arama Motoru

Müşteriler e-ticaret sayfalarında genellikle ürün ararlar. Ürünün tam adını veya kodunu bilmeleri beklenmez. Örneğin tek taşlı yüzük araması yapabilir. Eğer sitenin kullandığı arama motoru Türkçe harfleri tanımıyor ise müşterinin karşısına tas, gümüş tas gibi anlamsız nesneler gelebilir. Bu tür örnekler sık sık karşımıza çıkmaktadır. Bunun iki nedeni vardır:

1 - Ürünlere ad verilirken Türkçe harflerin kullanılmaması

2 - Arama motorunun Türkçe desteği olmaması

Her iki durum da müşteri için hoş bir durum değildir. Türklerin kullanacağı bir e-ticaret sitesinde arama motorunun Türkçe desteği olması beklenir.

### 4.2.9 Raporlama Araçları

Ticari etkinliğin başarıya ulaşması için satışların durumunu farklı açılardan inceleyen ve raporlayan araçların kullanılması gerekir. Günümüzde bu amaçla geliştirilmiş Çevrimiçi Analitik İnceleme araçları (OLAP : Online Analytical Processing) bulunmaktadır. Yürütülen ticaretin iş hacmine göre uygun bir OLAP aracı seçilmelidir. Bu raporlama yazılımları, değişik açılardan sonuçları görmeye ve irdelemeye yardımcı olurlar.

Raporlama çalışmaları içine veri madenciliği yöntemleri de eklenebilir. OLAP araçları temel olarak istatistiksel sonuçlar verirler. Buna karşın veri madenciliği yöntemleri nesneler arasındaki ilişkileri incelerler. Veri madenciliği çalışmaları açıklamak için verilen bilindik bir örnek şöyledir: İstatistik yöntemler ile bir mağazada satılan ürünlerin zamana göre satış miktarları çıkarılıp, bunların müşteri bölütleri ile ilişkileri ortaya konabilir. Ancak o mağazaya gelen bir kişinin neyin yanında neyi de aldığı ancak veri madenciliği yöntemleri ile bulunabilir. Bilindik örnek, çocuk bezi alanların çoğu yanında bir de bira aldıklarını göstermiştir.

### 4.2.10 Müşteri Memnuniyeti

Müşterilere bir kez ürün satmaktan daha önemlisi müşterinin ayağını alıştırmaktır. Bir müşterinin mağazaya ayağını alıştırmanın yolu müşteriyi memnun etmektir. Bir müşteri aşağıda açıklanan hizmetler ile memnun edilebilir:

- Kusursuz ürün ile
- Ürün zamanında ulaştırılarak
- Müşteri şikayetleri hızlı yanıtlanılarak
- Ürün iadesinde zorluk çıkarmayarak
- Ödeme kolaylığı sağlayarak
- Müşterileri belli aralıklarla arayarak veya bilgilendirerek
- Özel günlerinde müşterileri arayarak

Müşteri memnuniyeti sağlamak amacıyla yapılan arama ve hatırlatmalarda dikkatli olmak gerekir. Kişilerin özeline girecek davranışlardan kaçınılmalıdır.

### 4.2.11 Soru Yanıtlama

Müşteri memnuniyetini artırmak üzere firmalar çağrı merkezleri kurmuşlardır. Bu merkezleri arayan müşteri, şikayetini bildirebilmekte, istediği ürünün kendisine ne zaman ulaşacağını sorgulayabilmektedir. İnsanlar tarafından verilen bu hizmetlerin yerini, günümüzde bilgisayarlı soru yanıtlama sistemleri almaktadır.

Doğal Dil İşleme teknikleri ile çalışan bu yeni uygulamalar, soruyu anlamaya çalışmakta, ardından verilmesi gereken yanıtı hazırlamaktadır. Doğal olarak yanıtı hazırlarken firmanın veri tabanı, iş akışları ve ulaştırmacılar hakkında bilgilerden yararlanması gerekir.

### 4.2.12 Müşteri Sadakati

Müşterileri firmaya bağlayıcı çalışmalar Müşteri Sadakati olarak adlandırılmaktadır. Bir müşteriyi firmaya bağımlı kılmak için yapılması geren ilk eylem müşteriyi memnun etmektir. Memnun edilmiş bir müşterinin davranışları, alışveriş alışkanlıkları, alışveriş zamanları, özel günleri izlenerek müşteri tanınmaya çalışılmaktadır. Bir müşteri tanındıktan sonra onu firmaya bağımlı kılmak için beğeneceği öneriler sunularak firmaya bağlılığı sağlanabilir.

Müşteri sadakatini sağlamak üzere hazır şablon programlar üretilmektedir. Mevcut programlardan iş koluna uygun olanı seçilip e-ticaret sayfasına eklenebilir.

### 4.2.13 Ödeme Bağlantısı

E-ticaret sayfasından ürün alan müşterinin son yapacağı işlem ödemedir. Ödemeler kredi kartıyla anında veya ürünü teslim alırken yapılabilir veya ödeme banka havalesi biçiminde olabilir. Ödeme hangi yolla yapılırsa yapılsın, e-ticaret sitesinin bir banka ile anlaşması gerekir.

Web sayfası için hazır olan yazılım araçları kullanıldığında bu araçlar ile birlikte banka bağlantısı arabirimleri sağlanmaktadır. Bu bağlantılar temel olarak bir satış terminalinin (POS : Point of Sale) e-ticaret sitesine özgülenmesidir.

### 4.2.14 Ulaştırma

Bir e-ticaret firmasının kendi veya başkasının ürünlerini kendi araçları ile müşterilere ulaştırması oldukça zor bir işlemdir. Bunun yerine, işi bu olan firmalar ile anlaşmak daha çok yeğlenen bir yöntemdir.

Nakliyeci, kargo şirketi veya kurye olarak adlandırılan bu tür işletmeler ile iş birliği anlaşmaları yapılarak ürünlerin müşterilere ulaştırılması sağlanabilir.

Dünya ölçeğinde büyük sayılabilecek e-ticaret firmalarının kendi depoları ve dağıtım araçları olduğu görülmektedir. Ancak bu tür dev firmalar bile uluslararası ulaştırma işini, bu alanda yetkin olan firmalara yaptırmaktadırlar.

# Kaynaklar ve Önerilen Yayınlar

[1] B. M. Leiner, V. G. Cerf, D.D. Clark, R. E. Kahn, L. Kleinrock, D. C. Lynch, J. Postel, L. G. Roberts, S. Wolff, A *Brief Histori of the Internet,* Internetsociety.org

[2] J. Parks, *12 Steps to Building a Successful Ecommerce Site in 12 Months* , https://www.entrepreneur.com/artcle/284175

[3] K. C. Laudon, C. G. Traver, E-commerce 2106, Pearson, 2017

[4] A.Koponen, *E-Commerce Electronic Payments,* http://home.ku.edu.tr/~daksen/mgis410/materials/E-Commerce_Electronic_Payments.pdf

[5] Z. Qin, *Introduction to E-commerce,* Springer, 2009

[6] M. Kütz, *Introduction to E-commerce Combining Business and Information Technology,* Deloitte, 2016

# 5

# E-Ticarette Güvenlik

Genelağ üzerinden gerçekleştirilen e-ticaret doğal olarak Genelağ'ın güvenlik sorunlarıyla karşı karşıyadır. Genelağ'ın geliştirilmesinde temel alınan ARPANET kapalı bir ağdı ve güvenlik konuları buna göre tasarlanmıştı. Buna karşın Genelağ herkese açık bir iletişim ağıdır. Genelağ'ın güvenlik sorunlarını gidermek üzere çalışmalar yapılmış ve yapılmaya devam edilmektedir. Bu bölümde, Genelağ üzerinden gerçekleştirilen e-ticareti ilgilendiren güvenlik sorunları ele alınacaktır.

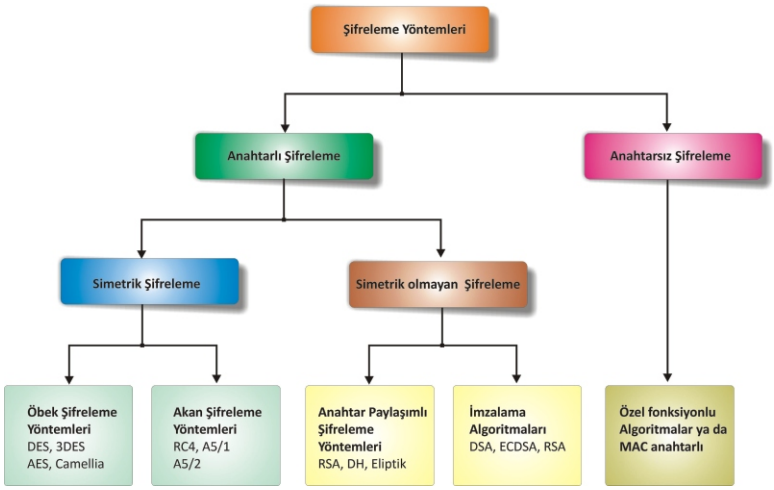
Güvenlik incelemesi iki açıdan yapılacaktır:

- Kimlik doğulama
- İletişim ortamı

Ticaretin temel ilkelerinden biri tarafların birbirine güvenmesidir. Bunun için de birbirlerini tanımaları gerekir. Bu açıdan kimlik doğrulamaya yer verilmiştir. E-ticaretin Genelağ üzerinde yapıldığı düşünüldüğünde bu ortamda kullanılan protokollerin sağladığı güvenliğini bilmek gerekir. Konunun bağlamını sağlamak amacıyla önce şifreleme yöntemleri kısaca tanıtılacaktır.

## 5.1 Elektronik ve Bilgisayar Temelli Şifreleme Yöntemleri

Günümüzde kullanılan şifreleme yöntemleri önceleri elektronik devreler ile gerçekleştirilmiş, daha sonra bilgisayarlı çözümlere geçilmiştir. Bu dönemde gerçekleştirilen şifreleme yöntemleri Şekil-5.1'de gösterilmiştir.

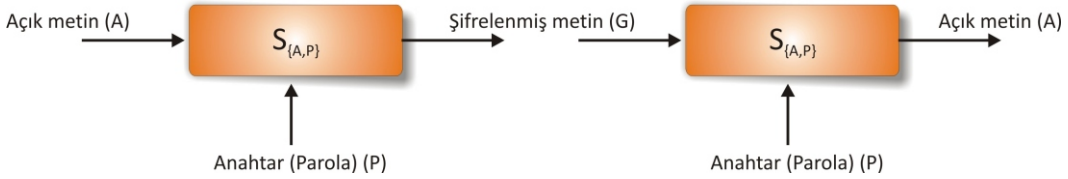



**Şekil-5.1** : Şifreleme yöntemleri

Şekil-5.1'den görüldüğü gibi, şifreleme yöntemleri anahtarlı ve anahtarsız olabilmektedir. Ancak anahtarlı olan çözümlerin ağırlıklı olduğu anlaşılmaktadır. Anahtar kullanan şifreleme yöntemleri kendi içinde iki kümeye ayrılmaktadır: Simetrik ve simetrik olmayan yöntemler. Simetrik şifreleme yöntemlerinin bazıları öbek, bazıları akan şifreleme yöntemini kullanmaktadır. Akan şifreleme yöntemleri, bir anda bir harfi şifrelemek üzere tasarlanırlar. Öbek şifreleme yöntemleri ise n harften oluşan öbekleri şifreleyecek biçimde tasarlanmışlardır. Bu şekilde ana hatları gösterilen şifreleme yöntemleri aşağıda tanıtılmıştır.

### 5.1.1 Simetrik Şifreleme Yöntemleri

Simetrik şifreleme yöntemlerinde açık metni şifrelemek için kullanılan anahtar ile şifrelenmiş metni çözmek için kullanılan anahtar aynıdır. Bu özelliği nedeniyle simetrik şifreleme adını alır. Şekil-5.2'de durum gösterilmiştir. Bu şekilde açık metin A, şifrelenmiş metin G, şifreleme anahtarı P ile ve Şifreleme işlemi $S_{\{A,P\}}$ biçiminde gösterilmiştir. Simetrik şifreleme yönteminde şifreleme ve çözmede kullanılan anahtarın (parola) gönderen ve alıcıda bulunması gerekir. Birbirini bilen gönderen ve alıcı için bu durum sorun oluşturmaz; ancak birbirini bilmeyenler tarafından kullanılması zordur. Bu durum yöntemin eksikliği olarak değerlendirilebilir. Günümüzde kullanılan tüm şifreleme algoritmalarının doğrusal sonuç üretmesi




**Şekil-5.2** : Simetrik şifreleme yönteminde, açık metnin şifrelenmesi ve çözümü

beklenmemektedir. Bir başka deyişle, açık metindeki bir harf için, her zaman aynı karşılığı üretmemesi gerekmektedir.

Simetrik şifreleme algoritmalarının en yaygın kullanılanları arasında DES (Digital Encription Standart) yer almaktadır. DES'in zaman içinde yetersiz kalması nedeniyle üçlü DES (3DES) ve AES (Advaced Encription Standart) geliştirilmiştir. DES'in yetersiz kalma nedeni, günümüzdeki bilgisayarların hızlarının artmasından; dolayısıyla DES ile şifrelenmiş bir metnin kısa sayılacak bir sürede çözülebilir olmasından kaynaklanmaktadır.

### 5.1.1.1 DES, 3DES ve AES

DES'in başlama hikayesi, 1960'lara kadar gitmektedir. Bu yıllarda IBM firmasında başlatılan bir çalışmanın sonucu olarak LUCIFER olarak adlandırılan bir şifreleme algoritması geliştirilmiştir. Bu algoritma 1970'li yılların başlarında ticari amaçla kullanılmaya başlanmıştır. Daha sonraları bu algoritmaya ABD Ulusal Güvenlik Birimi (NSA) katkı sağlamaya başlamıştır. Bu çalışmaların sonucu olarak 1977 yılında, ABD Ulusal Standartlar Ofisi (NBS) algoritmanın son halini, DES adıyla ulusal standart olarak kabul etmiştir.

DES öbek şifreleme yöntemi üzerine kurulmuştur. 64 bitlik öbek veriler üzerinde çalışır. Şifreleme anahtarı 64 bitliktir. Ancak anahtarı oluşturan her sekizlik içinde bir bit eşlik biti (Tek eşlik kullanılıyor) olarak kullanıldığından, anahtar boyu 56 bite inmektedir: (8x7=56). Şifreleme anahtarının boyu, günümüz koşulları için küçük sayılmaktadır. Deneme-yanılma biçiminde yapılan saldırılar ile kısa sayılabilecek bir sürede şifrelenmiş metinler çözülebilmektedir. 2006 yılında yapılan bir denemede, 120 FPGA bilgisayar ile 9 gün içinde çözülebildiği kanıtlanmıştır. DES'in gücünü artırmak amacıyla önce üçlü DES kullanılmış; daha sonra AES (2003) kullanılmaya başlanmıştır. AES'te anahtar boyu 192 ya da 256 bit olabilmektedir. Sözünü ettiğimiz algoritmaların temelini oluşturan DES'in iç yapısı ve çalışma biçimi aşağıda anlatılmıştır. Üçlü DES, DES şifreleme yönteminin art arda 3 kez kullanılmasıyla oluşturulur. Her bir DES için farklı anahtar kullanılabilir.

DES'in temel aldığı yöntem, IBM araştırmacılarından Horst Feistel tarafından geliştirilen Feistel öbek şifreleme yöntemidir. 1970 öncesi geliştirilen bu yöntemin temeli, bitleri karıştırmak

amacıyla turlamaya; doğrusal olmayan değiştirmeye ve YADA işlemlerine dayanır. Günümüzdeki birçok şifreleme algoritması bu yöntemi temel almaktadır.

Daha önce belirtildiği gibi DES 64 bitlik veri bloğu üzerinde çalışabilecek biçimde tasarlanmıştır. Eğer DES'e uygulanan açık metin 64 bitten kısa ise, geri kalan kısım doldurulmaktadır. Çok sayıda permütasyon ve değiştirme işlemi, şifrelenmiş metnin çözümünü zorlaştırmak için düşünülmüştür.

### 5.1.2 Simetrik Olmayan Şifreleme Yöntemleri

Simetrik şifreleme yöntemlerinde, açık metni şifrelemek ve şifrelenmiş bir metni çözmek için aynı anahtarın kullanıldığı açıklanmıştı. Ayrıca, çözümleme sürecinde, şifreleme sırasında izlenen adımlar ters sırada izlenmektedir. Simetrik şifreleme yöntemlerinin temel sıkıntısı, gönderen ve alan tarafın aynı anahtara sahip olma zorunluluğudur. Birbirini tanıyan veya aynı kurumda çalışanlar için büyük bir sorun gibi görülmese de parolaların belli aralıklarla değiştirilmesi kuralı gereği, zaman içinde sıkıntılara neden olabilmektedir. Bu sorunu gidermek üzere, parola değiştirme kuralları belirlenmekte ve çok sayıda parola, taraflara önceden verilmektedir ya da farklı bir kanaldan görüşülerek yeni parola dağıtımı yapılmaktadır. Askeri uygulamalar için hâlâ kullanılabilir bir yöntem olarak değerlendirilmektedir.

Genelağ bankacılığı gibi, çok sayıda müşteri ile bağlantı kurulan sistemlerde, oturum sırasında banka ile müşteri bilgisayarı arasında gidip gelen verilerin gizliliğini sağlamak amacıyla simetrik şifreleme yöntemlerinin kullanılması zordur. Bu nedenle simetrik olmayan şifreleme yöntemleri geliştirilmiştir.

Simetrik olmayan şifreleme yöntemleri üzerindeki ilk çalışmaların 1960'lı yıllarda, İngiliz GCHQ'de (Government Communication Headquarter) çalışan James Ellis'in, Bell Laboratuvarlarının II. Dünya savaşı sırasında yayımladıkları bir ortak yayından esinlenerek başlattığına inanılmaktadır. Ancak Eliss bu düşüncesini gerçekleştirememiştir. 1973'te aynı kurumda çalışmaya başlayan Clifford Cocks ile tanışmış ve birlikte çalışmaya başlamışlardır. Projeye bir yıl sonra Malcolm Williamson katılmasıyla 1975'te simetrik olmayan şifreleme yöntemi ortaya çıkarılmıştır. Çalıştıkları projenin gizlilik içermesinden dolayı çalışmaları bir yayın olarak duyurulmamıştır. Ancak 1997 yılında duyurusu yapılmıştır.

1977 yılında Ron Rivest, Adi Samir ve Len Adleman MIT'de simetrik olmayan şifreleme yöntemini (RSA) geliştirmişler ve 1978'de yayımlamışlardır. Bu üç araştırmacı, Whitfield Diffie ve Martin Hellman tarafından 1976 yılında kuramsal olarak geliştirilmiş ve "New Directions in Cryptography" isimli makalede yayımlanmış olan altyapıyı kullanmışlardır. Diffie-Hellman yöntemi olarak bilinen bu yöntem daha sonra Ralph Markle tarafından bilgisayara uygun olarak geliştirilmiştir. Bu yüzden, yöntemin Diffie-Hellman-Markle adıyla anılmasını, Hellman tarafından 2002 de önerilmiştir.

### 5.1.2.1 RSA Şifreleme Yöntemi

Günümüzde yaygın olarak kullanılan, simetrik olmayan şifreleme yöntemi RSA adıyla bilinmektedir. Bu yöntem ana hatları ile şöyledir:

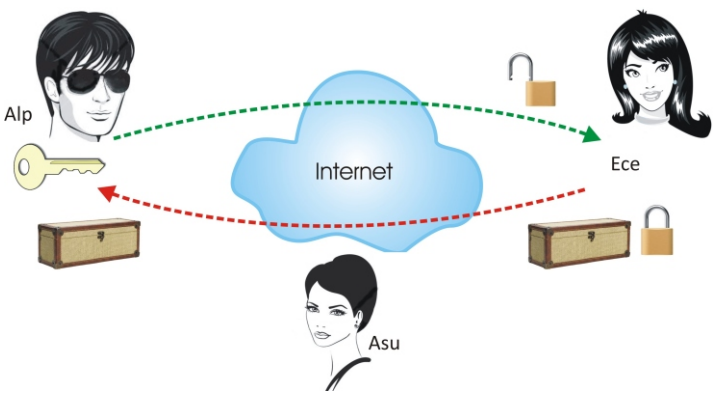
1 - İletişimi başlatacak olan taraf (alıcı olarak da düşünülebilir), karşı tarafa bir açık anahtar gönderir.

2 - Karşı taraf, ileteceği metni bu açık anahtar ile şifreler ve alıcıya gönderir.

3 - Alıcı, gelen gizli metni, kendisinde bulunan özel anahtarı ile açabilir.

Şekil-5.3'te RSA simetrik olmayan şifreleme yönteminin çalışma ilkesi gösterilmiştir.

Şekil-5.3'te görüldüğü gibi, Alp, Ece'ye açık bir kilit göndermektedir. Bu kilit herkes tarafından görülebilmektedir. Bu nedenle *"Açık Anahtar"* olarak adlandırılır. Aslında açık kilit demek daha doğru olurdu; ancak genel adlandırma bu şekildedir. Ece, başkalarının görmesini istemediği mektubunu bu anahtarla kilitleyip Alp'e gönderir. Açık ortamda giden bu mektup açık anahtar ile şifrelenmiş olduğundan başkaları mektubun içeriğini okuyamaz. Ece'den gelen mektubu, ancak Alp kendisinde bulunan *"Özel Anahtar"* ile açıp mektubu okuyabilir.




**Şekil-5.3** RSA simetrik olmayan şifreleme yönteminin çalışma ilkesi

Temel ilkesi yukarıda açıklanan RSA şifreleme yönteminin temel aldığı matematik şöyledir:

p ve d iki asal sayıdır. bu iki sayının çarpımından açık anahtarın n değeri bulunur.

n = p x q hesaplanır. Bunun ardından (n) değeri hesaplanır

(n) = (p-1)(q-1) ; (n) değerinin hesaplanmasının ardından aşağıdaki koşulları sağlayan bir e sayısı bulunur.

1 < e < (n) ; e bir tam sayıdır ve n'in böleni değildir.

Buna göre açık anahtar n ve e den oluşur, özel anahtar (d) ise şöyle hesaplanır:

$$d \quad \frac{2 \quad (n) \quad 1}{e}$$

Konuya açıklık getirmek üzere bir örnek aşağıda verilmiştir:

p = 53 ve q = 59 olarak seçilmiştir. (aslında bu sayıların çok büyük asal sayılar olması gerekir. Basitlik olsun diye bu iki asal sayı seçilmiştir.)

n = p x q = 53 x 59 = 3127

(n) = (p-1)(q-1) = (53-1)(59-1) = 3016

1 < e < (n) koşulunu sağlayan bir tam sayı seçilir.

Bu sayının bu aralıkta olan en büyük asal sayı olması şifrelemenin gücünü artırır. Ancak basit olsun diye e = 3 seçilmiştir.

Dolayısıyla bizim açık anahtarımızın bileşenleri **n = 3127** ve **e = 3** tür ve özel anahtar

$d \quad \frac{2 \quad (n) \quad 1}{e} \quad \frac{2(3016) \quad 1}{3}$ 2011 olarak hesaplanır.

## Şifreleme aşaması

Örnek olarak Ece "A" harfini şifreleyip Alp'e göndermek istesin. Ece, Alp'in göndermiş olduğu **n** ve **e** değerlerini kullanarak, "A" harfini aşağıdaki gibi şifreler: (A harfinin ASCII karşılığı 65 tir)

$C = 65^{e} \bmod n = 65^{3} \bmod 3127 = 274.625 \bmod 3127 = 2.576$

C şifrelenmiş veriyi temsil etmektedir. Aslında 2.576 mod 3127 işlemi sonunda artakalan sayıdır. Ece bu sayıyı Alp'e gönderir.

## Çözüm

Alp kendisine gelen 2.576 sayısını özel anahtarını kullanarak Ece'nin gönderdiği mektubu okur.

Açık metin = $C^{d} \bmod n$ formülüyle hesaplanır.

Açık metin = $2.574^{2011} \bmod 3127 = 65$

Sonuç olarak Alp "A" harfini okur.

Verilen örnek, RSA şifreleme ve çözümleme yönteminin ana hatlarını anlatmak üzere verilmiştir. Anlatımı kolaylaştırmak üzere sayılar küçük tutulmuştur. Gerçek uygulamada kullanılan sayılar çok büyüktür. Örneğin ilk dönemlerinde anahtar boyu 320 bit olan RSA, 2010 yılına gelindiğinde anahtar boyunun 1024 bite çıkarıldığı görülmektedir. Anahtar boyunun büyütülmesi algoritmanın kırılma direncini artırmaktadır ancak işlem süresini uzatmaktadır.

## 5.2 Kimlik Doğrulama

Bir e-ticaret firmasının sunucusuna, çok sayıda kişinin bağlanacağı gerçeği, gündeme kimlik doğrulama konusu getirmiştir. Kimlik sorgulamada akla ilk gelen sorunlar şunlardır:

- Sunucuya bağlanan kişi, gerçekten adı belli olan kişi midir?
- Erişim sırasında belirtilen kullanıcı bilgileri çalıntı olabilir mi?
- Erişilmek istenen sunucu, gerçekten erişilmek istenen sunucu mudur?

Bu kısımda kimlik doğrulaması ile ilgili bilgiler yer alacaktır.

### 5.2.1 http Kimlik Doğrulaması

Bilgi sistemine erişebilmek için kullanıcının, erişmek istediği bilgi sistemine erişim yetkisinin olması gerekir. Bunun için, ilk aşamada, kişi için bir yetki kaydının açılması gerekir. Bu kayıt içinde, kişinin sisteme erişmek istediğinde kullanmak istediği kullanıcı adı ve parolası yer alır. Kullanıcı belirlediği kimlik ve parolası ile sunucu bilgisayar tarafından tanınır ve kendisine erişim yetkisi verilir.

Genelağ'da sunucular ve son kullanıcılar arasında bilgilerin nasıl aktarılacağına ilişkin kurallar ve yöntemleri düzenleyen bir sistem olan Çoklu Metin Aktarımı Protokolü (Hyper Text Transfer Protocol, http) kimlik doğrulama amacıyla iki seçenek sunmaktadır;

1 - Temel kimlik doğrulaması

2 - Özetli kimlik doğrulaması

Bu iki seçeneğin teknik özellikleri “RFC 2617 HTTP Authentication: Basic and Digest Access Authentication“ adıyla yayımlanmıştır. Belgede, erişim için kullanıcı adı ve parolanın kullanılmasına vurgu yapılmaktadır. Önerilen çözüm sadece sunucuya erişme aşaması için önerilmiştir, kullanıcının bilgisayarı ile sunucu arasında gidip gelecek olan verilerin gizliliğini, bütünlüğünü ve yadsınamazlığı hedeflememektedir.

#### 5.2.1.1 Temel Kimlik Doğrulaması

Temel kimlik doğrulama biçimi http’nin tanıtıldığı ilk sunumu 1.0’dan beri kullanılmaktadır. Sunucuya erişim için sadece kullanıcı adı ve parolasını yeterli saymaktadır. Kullanıcı, kullanıcı adı ve parolasını sunucuya gönderdiğinde, sunucu, kullanıcılara ilişkin tablo ya da veri tabanına bakarak, kullanıcı adı ve parolasının eşleşip eşleşmediğini denetler. Uyuşuyorlarsa, kullanıcıya erişim hakkı verir. Sunucu, kullanıcı sayısına göre ya basit bir tablo ya da veri tabanı kullanır. Kullanıcı sayısı çok olduğunda, kullanıcıları kümelere ayırmak, eşleşme işleminin süresini kısaltmak için yararlı olur.

İstemci bilgisayardan, sunucu bilgisayara gönderilen kullanıcı adı ve parolası şifresiz ancak Base64 kodlamasını (Bu kodlama RFC2045’te açıklanmıştır) uygulayarak gitmektedir. Bu kodlama kolayca çözümlenebilmektedir, dolayısıyla, kullanıcı adı ve parolasının başkaları

tarafından görülmesi ve öğrenilmesi olasılığı vardır. Bu nedenle, Temel Kimlik Doğrulama yönteminin sağlam ve güvenilir bir yöntem olduğu söylenemez.

Kimlik doğrulama adımları aşağıda anlatılmıştır:

1 - İstemci, bir web kaynağına erişmek istediğini (***GET Request***) mesajıyla, sunucuya iletir.

2 - Sunucu yanıt olarak "***401 Asıllama İsteği***"ni gönderir. Bu yanıt, kimlik doğrulamanın türünü ve kaynağın sahibi olan erişim alanını belirten "***www-Authenticate***" başlığını içerir.

3 - İstemci, bu kez "***Authentication***" başlığı ile beraber "***http Get***" erişim isteğini sunucuya gönderir. Bu istek mesajı, erişilmek istenen alanın (bundan böyle kale olarak anılacaktır) gerekli gördüğü kullanıcı adı ve parolasını da içerir. Bu anahtar bilgiler, aynı kaleye bir sonraki erişimde de kullanılmak üzere tarayıcının cep belleğinde tutulur.

4- Sunucu, kullanıcıya ilişkin, kendisinde bulunan verileri kullanarak, istemci gibi özet çıkarır. Bu özeti, istemcinin gönderdiği özet ile karşılaştırır. Sonuç olumlu ise "***200 OK***" mesajını istemciye gönderir. Değil ise "***Yetkilendirme Gerekiyor***" (401 Authorization Required) mesajını gönderir.

### 5.2.1.2 Özetli Kimlik Doğrulaması

Temel kimlik doğrulama yönteminin çok yetersiz olan güvenlik özelliğini gidermek üzere "Özetli Kimlik Doğrulaması" biçimi geliştirilmiştir. Bu yöntemde de sunucuya erişmek üzere kullanıcı adı ve parolasının gönderilmesi gerekir. Ancak bu yöntemde parola açık olarak gönderilmez. Parola yerine, parola üzerinde MD5 Hash algoritması uygulanarak özeti çıkarılır ve bu özet sunucuya gönderilir. Bu nedenle yönteme bu ad verilmiştir.

Sunucu, kullanıcılara ilişkin kullanıcı adı ve parolalarının özetini içeren bir tabloyu barındırır. İstemciden istek geldiğinde, kullanıcı adı ve parolasının özetinin uyuşup uyuşmadığını araştırır. Uyuşma var ise kullanıcıya erişim yetkisi verilir.

Özet içeriğinden parolayı elde etme olanağı olmadığından, istemci ile sunucu arasındaki bağlantıyı dinziyen biri kullanıcın parolasını öğrenemez. Özetli kimlik doğrulama yöntemi, kullanıcıların parolalarını gizlemek için yeterli güvenliği sağlıyor kabul edilebilir.

Kimlik doğrulama adımları aşağıda anlatılmıştır:

1 - İstemci, bir web kaynağına erişmek istediğini (***GET Request***) mesajıyla, sunucuya iletir.

2 - Sunucu yanıt olarak "***401 Asıllama İsteği***" ni gönderir. Bu yanıt, kimlik doğrulamanın türünü ve kaynağın sahibi olan erişim alanını belirten "***www-Authenticate***" başlığını içerir.

3 - İstemci, parola ile tek kullanımlık sayıyı, http yöntemini ve URI'yi birleştirir, bunların özetini üretir. Ürettiği özeti sunucuya gönderir. Gönderdiği veri kalıbı aşağıdaki gibidir:

MD5(MD5(<Parola> + ":" + + ":" + MD5(<Yöntem> + ";" + uri)

4 - Sunucu, kullanıcıya ilişkin, kendisinde bulunan verileri kullanarak, istemci gibi özet çıkarır. Bu özeti, istemcinin gönderdiği özet ile karşılaştırır. Sonuç olumlu ise "***200 OK***" mesajını istemciye gönderir. Değil ise "***Yetkilendirme Gerekiyor***" (401 Authorization Required) mesajını gönderir.

Genelağ üzerinden yapılan iletişim, temel olarak bir bilgisayardan diğer bir bilgisayara doğru yapılmaktadır. Ağ üzerinde bir bilgisayarın diğer bir bilgisayarı bulabilmesi için her bilgisayarın bir adresinin olması gerektiği açıktır. Bunun yetmeyeceği de bilindiği için değişik iletişim protokolleri geliştirilmiştir. Bunlar arasında ISO/OSI (International Organization for Standardization/Open Systems Interconnection) ve TCP/IP (Transmission Control Protocol/Internet Protocol) önemli protokollerdir.

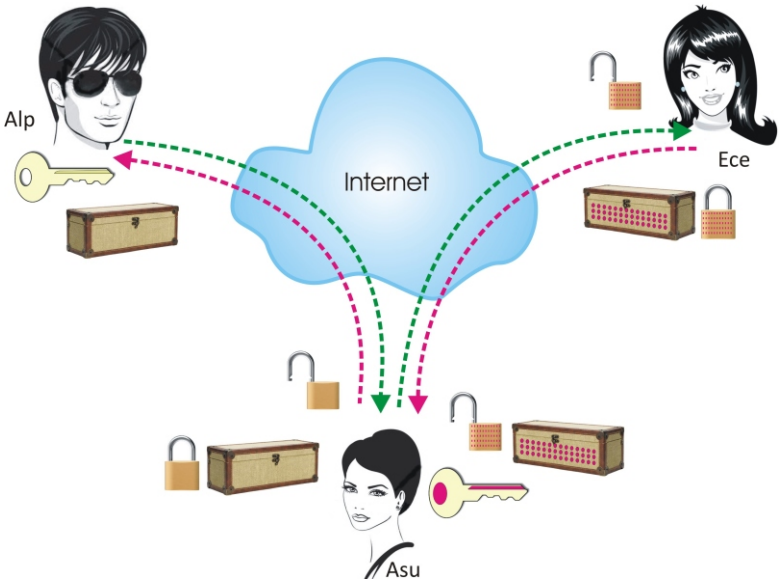
### 5.2.2 Sayısal Yetki Belgesi (Sertifika)

Günümüzde, Genelağ üzerinden farklı amaçlarla işlemler yapılmaktadır. Bu işlemlerin bazıları için güvenlik son derece önemlidir. Örneğin Genelağ bankacılığı yapan ya da Genelağ'dan kredi kartı ile alışveriş yapan birisi için güvenlik son derece önemlidir. Kişiler kandırılmadıklarından ve gerçekten ulaşmak istedikleri kişi ya da kuruluşlarla bağlantı sağladıklarından emin olmak isterler. Bu tür sorunları çözmek üzere geliştirilmiş olan yöntemlerden birisi **Sayısal Yetki Belgesidir (SYB).**

Şekil-5.3'ü hatırlayalım. Alp, Ece ile yazışmak istiyor ancak bu yazışmanın içeriğini Asu'nun öğrenmesini istememektedir. Bunun için Ece'ye açık durumda bir kilit göndermektedir. Ece yazdığı mektubu bir zarfa ya da kutuya koyup, Alp'in gönderdiği asma kilitle kilitlemeyip Alp'e göndermektedir. Alp kendisinde bulunan anahtar ile kutuyu açıp mesajı okuyabilmektedir. Çalışacağı anlaşılan bu senaryo için bir saldırı nasıl olabilir diye düşünelim.

Alp açık kilidi Genelağ ortamında göndermektedir; dolayısıyla Asu da bu kilidi görebilir. Asu'nun, Alp ile Ece'nin iletişim bağlantısının arasına girdiğini de düşünebiliriz. Bu duruma **aradaki adam** adı verilmektedir. Şekil-5.4'te son durum çizilmiştir. Asu'nun aradaki adam rolünü oynadığında ortaya çıkacak durum aşağıda adım adım anlatılmıştır:

- Alp açık kilidini Genelağ üzerinden Ece'ye gönderir. Ancak aradaki Asu bu kilidi alır.
- Asu, Alp'in açık kilidi yerine kendi açık kilidini Ece'ye gönderir.
- Ece Alp'ten açık kilit beklediği için, gelen kilidin Alp'in kilidi olduğunu sanır ve mesajını bu kilitle kilitleyip gönderir.
- Ece'nin gönderdiği kutu Asu'ya ulaşır. Asu Ece'nin gönderdiği kutuyu kendi özel anahtarı ile açar ve mektubu okur.
- Asu, bu arada hazırladığı kandırıcı mektubu kutuya koyar ve Alp'in açık kilidi ile kilitler ve Alp'e gönderir.
- Alp gelen kutuyu, kendi özel anahtarı ile açar ve mektubu okur. Mektubun Ece'den geldiğini düşünür. Mektubun içeriği Alp'i üzer.




**Şekil-5.4** : Simetrik olmayan şifreleme yönteminde aradaki adam sorunu

Bu senaryodan çıkarılacak ders, simetrik olmayan şifreleme yönteminde, alıcıya gelen açık kilidin sahibinin kimliğinin belirsizliğidir. Örnekte olduğu gibi, Ece gelen açık kilidin sahibinin Alp olduğunu sanmakta ancak gelen açık kilit Asu'nundur.

Bunun gibi kandırıcı olayların önüne geçmek üzere SYB yöntemi geliştirilmiştir. Sayısal Yetki Belgesini, Nüfus kağıdı ya da sürücü ehliyetine benzetebiliriz. Şehirlerarası yolda araç kullanırken bir polis kimliğimizi sorduğunda, kendisine adımızı söylememiz yetmez; sürücü ehliyetimizi göstermemiz gerekir. Sürücü ehliyeti yetkili bir kuruluş tarafından verildiği ve onaylı olduğu için polis kimliğimizi doğrulamış olmaktadır. Benzer bir uygulama Genelağ üzerinden gerçekleştirilen işlemler için tasarlanmıştır. Bu yöntemde yetkili bir kuruluşun verdiği **Sayısal Yetki Belgesi (SYB) (Digital Sertificate)** belgesi kullanılır.

Sayısal Yetki Belgesi yetkili ve güvenilir kuruluşlar tarafından verilen kimlik kartı gibi düşünülebilir. Bu belge, belgeyi veren ve kullananın kimliğini tekil olarak tanımlar. Daha önce anlatıldığı gibi birbirini tanımayan kişiler veya bilgisayarlar arasında güvenli iletişimi sağlamak amacıyla simetrik olmayan şifreleme yöntemleri kullanılmaktadır. Günümüzde yaygın olarak kullanılan simetrik olmayan şifreleme yöntemi RSA'dir. SYB, simetrik olmayan şifreleme yöntemindeki açık anahtar görevini görür. Hatırlanacağı gibi, açık anahtar ile şifrelenen bir metin daha sonra bunun tamamlayıcısı olan özel anahtar ile çözülebilmektedir.

Açık anahtarı alan ve bunu kullanarak ticari işlem yapacak olan taraf açık ve gizli anahtarların güvenli biçimde oluşturulduğundan emin olmak ister. Açık anahtarın gerçekten, bağlantı

kurmak istediği kişi ya da kuruluşa ilişkin olduğunu, diğer bir açıdan sahte olmadığını bilmek ister. Bu nedenle, SYB'nin yetkili ve güvenilir bir kuruluş tarafından üretilmesi önemlidir. SYB'yi üreten kuruluşlara, **Setifika Yetkilisi (SY) (Certicate Authority : CA)** adı verilmektedir.

Uluslararası geçerliliği olan SYB için X.509 adı verilen bir ölçün hazırlanmıştır. Bu ölçüne göre bir SYB içeriği Şekil-5.5'teki gibidir.

Şekil-5.5'ten görüldüğü gibi SYB hem kimlik sahibini, hem de bu kimliği veren kuruluşu tanıtmaktadır. Ayrıca, kimliğin geçerlilik zamanını da belirtmektedir. Bu zaman dilimi dışında SYB'nin geçerliliği yoktur; onun için yenilenmesi gerekir.

| |
|---|
| Sürüm |
| Seri Numarası |
| İmzalama Algoritması |
| Veren Kuruluşun Adı |
| Geçerlilik Süresi |
| * Önceki tarihte geçersizdir |
| * Sonraki tarihte geçersizdir |
| Sahibinin Adı |
| Sahibinin Açık Anahtarı |
| * Algoritması |
| * Açık Anahtar |
| Eklemeler |
| İmza |

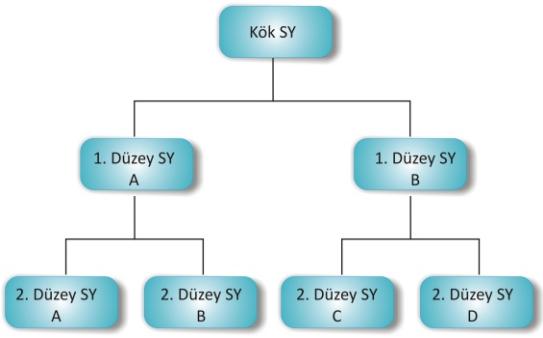
**Şekil-5.5**: X.509'a göre SYB'nin içeriği

Daha önce değinildiği gibi, SYB'yi verecek kuruluşun saygın ve güvenilir olması gerekir. Günümüzde bu tür kuruluşlar vardır ve SYB vermektedirler. Sertifika Yetkilisi (SY) olarak adlandırılan bu kuruluşların en üst düzeyinde Kök SY denilen kuruluş bulunur. Bunun altında, bölge ve ülke SY'leri yer alır; Şekil-5.6.

Sıradüzensel (Hiyerarşik) bir yapıda kurulan sertifika yetkilileri arasındaki onay yapısı vardır ve bu yapı Şekil-5.7'de gösterilmiştir. Şekil-5.7'de SYB nin içeriği biraz basitleştirilmiştir.

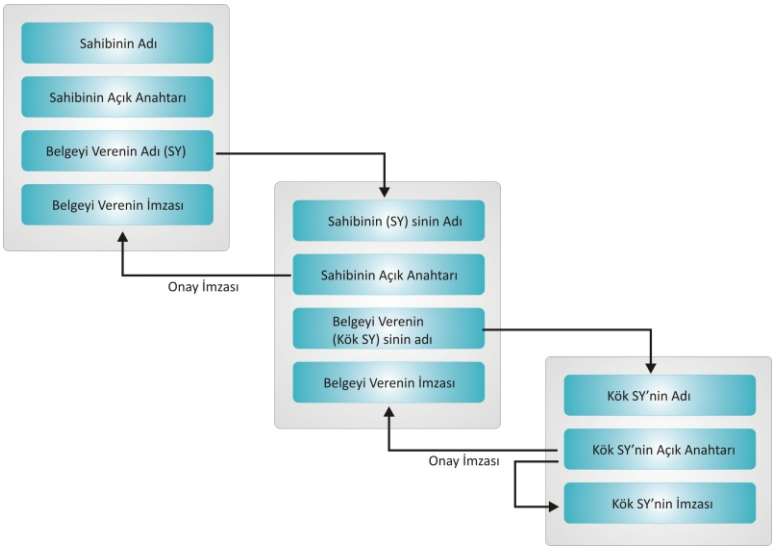
Kuruluş içinde SYB'lerin dağıtımının nasıl yapıldığı Şekil-5.8'de gösterilmiştir.

SYB'sini Genelağ ortamında gönderen birinin, başkaları tarafından kandırılmasını önleyen, kişinin özel anahtarıdır. SYB tek başına bir kişinin kimliğini kanıtlamaz, ancak açık anahtar sayesinde SYB sahibinin kimliğini doğrulamayı sağlar. SYB sahibi, özel anahtarını korumak ve saklamakla yükümlüdür. Özel anahtarın çalınması durumunda, SYB zararlı eylemler için kullanılabilir.

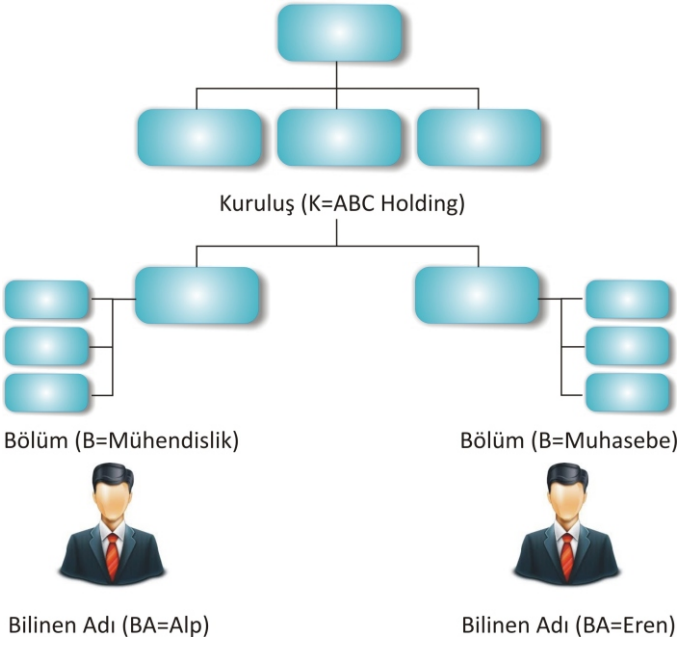



**Şekil-5.6**: SY sıradüzensel yapı

SYB'yi üreten ve dağıtan sertifika yetkili kuruluşlarının görev sorumlulukları son derece önemlidir. Bu kuruluşlar, Dünya genelinde belge dağıtabilecekleri gibi, ülke içinde ya da kurum içinde de SYB üretip dağıtabilirler. Dünya genelinde geçerli olan SYB'yi ülke yetkilisi üzerinden sağlamak olanaklıdır. Ancak bunun




**Şekil-5.7**: SYB üretiminde sıradüzensel yapı




**Şekil-5.8**: SYB'nin ağaç yapısı

kök yetkili kuruluş tarafından onaylanması gerekir. SYB dağıtan kuruluşlar, belge verdikleri her kişinin açık ve gizli anahtarını üst düzey güvenlikli ortamlarda saklamak zorundadır. Kişilerin açık anahtarları, Genelağ üzerinden erişilebilecek bir ortamda tutulur. Bu anahtara gereksinimi olan, buradan iletişim kuracağı kişi veya kuruluşun açık anahtarını edinebilir.

## 5.2.3 Açık Anahtar Altyapısı (AAA)

Genelağ üzerindeki iletişimi güvenli biçimde sağlamak üzere geliştirilmiş altyapıya Açık Anahtar Altyapısı (AAA) (Public Key Infastructures : PKI) adı verilmiştir. Bu yapı ile, bilgi güvenliğinin temel kuralları; gizlilik, bütünlük, asıllama ve inkar edememe kuralları sağlanmaya çalışılmaktadır. Açık anahtarlama altyapısı ile e-postaların daha güvenli gidip gelmesi, e-ticaretin daha güvenli

olması hedeflenmektedir.

Açık anahtar altyapısı, güvenli iletişim için gerekli olan donanım, yazılım, politika, hizmet programları, şifreleme algoritmaları ve protokollerden oluşmaktadır. Bu bileşenler birlikte çalışarak iletişimin güvenliğini sağlamaktadırlar. Açık anahtar altyapısının bileşenleri;

- Simetrik ve simetrik olmayan şifreleme yöntemleri ile verilerin gizliliğini,
- Sayısal yetki belgesiyle, tarafların asıllamasını ve yadsıyamamayı,
- Değişik algoritmalar ile verilerin bütünlüğünü

sağlamaya çalışmaktadır.

Açık anahtar altyapısının çalışma ilkesi sayısal yetki belgesi tanıtılırken izlenen yöntemin aynıdır. Bu altyapının bileşenleri aşağıda tanıtılmıştır:

- Sertifika Yetkilisi
- Kayıt Yetkilisi
- Yetki Belgesi Dolabı

### 5.2.3.1 Sertifika Yetkilisi

Sertifika yetkilisi, kişilere bilişim ortamında kullanılabilecekleri ve kim olduklarını kanıtlayabilecekleri kimlikleri (Sayısal Yetki Belgesi) veren kuruluştur. Bu belgeye Sayısal Sertifika da diyebiliriz. X.509 ölçünü ile içeriği belirlenmiş olan sayısal yetki belgesi, kişinin kimliği ile birlikte onun için hazırlanmış olan açık anahtarı da içerir. Simetrik olmayan şifreleme yönteminden hatırlanacağı gibi, bu yöntemde açık ve özel anahtarlar bir çift olarak hazırlanırlar. Bu anahtarların saklanması sorumluluğu sertifika yetkilisinindir.

Sertifika yetkilisi, görevini yerine getirebilmek üzere gerekli olan donanım ve yazılımlardan oluşan bir ortam hazırlar. Bu ortamın nasıl işleyeceğini belirler ve bunları yönerge haline getirir. Daha sonra, sertifika başvurusunda bulunanları inceler ve uygun olanlara sayısal yetki belgesi verir. Daha önce açıklandığı gibi bu belgeler sürelidir; dolayısıyla süreleri dolduğunda yenilenmeleri gerekir.

Sertifika yetkilisi kuruluşlar güvenilir ve saygın kuruluşlar olmak zorundadırlar. Bu nedenle, nasıl çalışacakları, anahtarları nasıl saklayacakları gibi konuları, açık biçimde tanımlamak ve tanıtmakla yükümlüdürler. Bu kuruluşlar, yerel ve uluslararası denetim örgütleri tarafından denetlenebilirler.

İlgili kısımda anlatıldığı gibi, sayısal yetki belgelerinde, belgeyi üreten sertifika yetkilisinin imzası bulunur. Üretilen sayısal yetki belgesi, bir kuruluş içinde geçerli olacak ise, kuruluş kendisi için bir sertifika yetkilisi tanımlayabilir. Bu birim, söz konusu kuruluş için kök sertifika yetkilisidir. Sayısal yetki belgesinin ulusal düzeyde geçerli olması isteniyor ise bu amaçla ulusal sertifika merkezi ya da merkezleri kurulabilir. Bu merkezler, ülke içinde sayısal yetki belgesi dağıtabilirler. Sayısal yetki belgesinin uluslararası düzeyde geçerli olması isteniyor ise ulusal sertifika merkezlerinin uluslararası yetkiye sahip sertifika merkezlerine bağlanmaları gerekir.

### 5.2.3.2 Kayıt Yetkilisi

Sayısal yetki belgesi istekleri, kayıt yetkilisi tarafından değerlendirilir. Bu değerlendirme sırasında, başvuranın kimlik asıllaması ve verilecek belgenin sınıfı belirlenir. SYB'ler kişi ve kuruluşların gereksinim ve işlevlerine bağlı olarak üç sınıfa ayrılırlar:

**1 - Sınıf SYB** : Kişisel kullanıcılar için tanımlanmış sınıftır. Bu SYB edinenler, genellikle e-postalarının veya mesajlarının gizliliği için SYB'yi kullanırlar.

**2 - Sınıf SYB** : Bu tür SYB genellikle yazılım üreticileri tarafından kullanılır. Yazılım üreticisi firma, dağıtımını yaptığı yazılımın bütünlüğünü korumak üzere bu SYB'yi ekler.

**3 - Sınıf SYB** : Kuruluşlar kendileri için SYB üretirler. Sertifika dağıtımını kendi içlerinde yaparlar. Bunlar, ulusal ya da uluslararası SY'lere bağlanabilir ya da bağlanmazlar.

Bu üç sınıfın görev ve sorumlulukları birbirinden farklı olduğu için kayıt başvurusu yapıldığında farklı bilgilerin kayıt yetkilisine sunulması gerekir. Örneğin,

- 1. Sınıf bir yetki belgesi almak isteyen birey, başvurusunu e-posta yoluyla yapabilir. Sunması gereken belgeler arasında onaylı bir kimlik belgesi ve kullandığı e-posta adresini bildirmesi yeterli olabilir.
- 2. Sınıf bir yetki belgesini ticari kuruluşların istemesi beklendiğinden, bu kuruluşların ticari kayıt belgelerini, kuruluş adına sorumlu ve yetkili kişilerin kimlik belgelerini kayıt yetkilisine sunmaları gerekir. Bu belgeler posta yoluyla gönderilebilir.
- 3. Sınıf yetki belgesi daha üst düzey sorumluluk gerektirdiğinden, kuruluş yetkililerinin kayıt yetkilisi ile yüz yüze görüşmeleri gerekebilir.

Bu üç sınıf başvuru sırasında, başvuranlardan başka bilgiler de istenebilir. Örneğin kullanmak istedikleri anahtar boyu sorulabilir.

Başvuru işlemi tamamlandıktan sonra, başvuru sertifika yetkilisine iletilir. Şekil-5.9'de Sayısal Yetki belgesinin elde edilmesi sırasında izlenmesi gereken adımlar gösterilmiştir.

Şekil-5.9'da izlenen adımlar sırasıyla şöyledir:

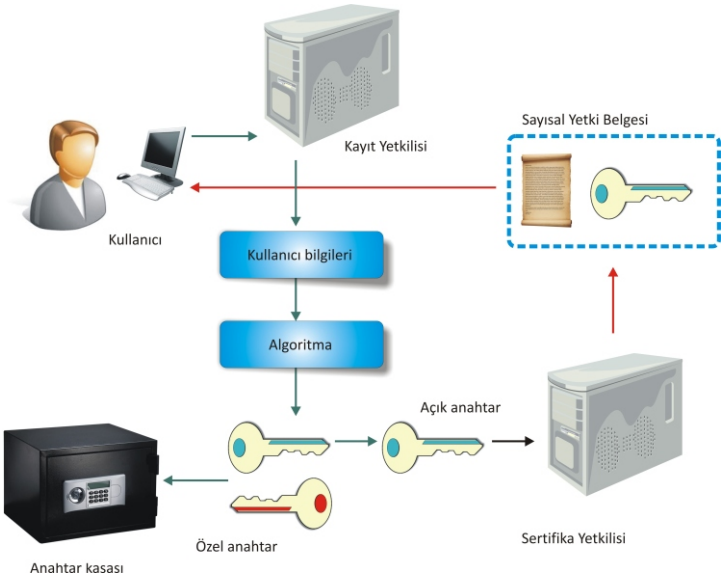
- Başvuruda bulunan, kimlik ve diğer gerekli belgeleri, yukarıda anlatılan biçimde kayıt yetkilisinin bilgi sistemine girer.
- Başvuranın bilgileri kaydedilir ve sınıfı belirlenir.
- Belli bir algoritma kullanılarak başvuru yapan için açık ve özel anahtarlar üretilir.
- Üretilen iki anahtar da anahtar kutusunda saklanır.
- Açık anahtar sertifika yetkilisine gönderilir.
- Sertifika yetkilisi, sayısal yetki belgesini hazırlar ve bununla beraber başvuranın açık anahtarını başvuru sahibine gönderir.

Başvuruda bulunan, birden fazla yetki belgesi isteyebilir. Bu durumda, istediği kadar sayısal yetki belgesi üretilir.

Yerel sertifika yetkilisi olabildiği gibi, yerel kayıt yetkilisi de olabilir.

### 5.2.3.3 Yetki Belgesi Dolabı

Üretilen yetki belgeleri ve açık anahtarlar, Genelağ üzerinden erişilebilir bir yerde tutulmalıdırlar. *Yetki Belgesi Dolabı* diyebileceğimiz bu sanal dolaba LDAP kurallarına uygun olarak erişilebilir.




**Şekil-5.9** : Sayısal Yetki Belgesi başvurusu ve sonlandırılması süreci

İki kişi Genelağ ortamında bağlantı kurduğunda, gönderen durumunda olan taraf açık anahtarını alıcı durumdakine gönderir. Alıcı taraf bu anahtarı kullanarak oturum sırasında kullanacakları simetrik anahtarı üretebilir. Bundan sonraki iletişim bu anahtarla simetrik şifreleme yöntemiyle şifrelenmiş biçimde devam eder.

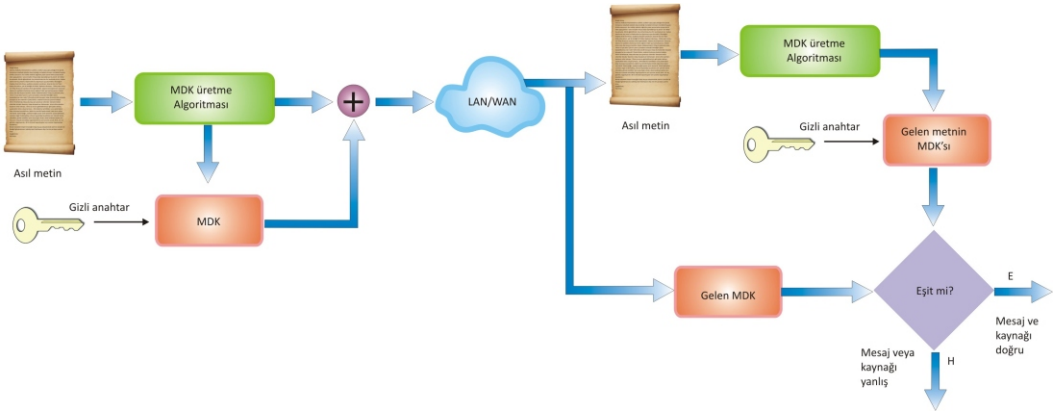
Taraflar, birbirinin kimliğinden emin olmadıkları durumda, taraflar birbirine Sayısal Yetki Belgelerini iletirler. Taraflar bu belgeye bakarak kimlik asıllaması yaparlar.

## 5.2.4 Sayısal İmza

Sayısal imza konusunu anlayabilmek için, önce **Mesaj Doğrulama Kodu** (MDK) (Message Authentication Codes (MAC)) nun anlaşılması gerekir. MDK hem mesajın hem de kaynağının doğrulanmasını sağlamak üzere geliştirilmiş bir yöntemdir. Özet çıkarma yöntemine çok benzer. Tek farkı özet çıkarma işleminde, bir parolanın kullanılmasıdır. Mesajı gönderen taraf bu gizli parolayı, alıcı ile paylaşır. Alıcı taraf mesajı aldığında, gizli parolayı kullanarak MDK'nın sağlanıp sağlanmadığını denetler. Şekil-5.10'da MDK yönteminin nasıl çalıştığı gösterilmiştir.

E-imza yöntemi, mesaj doğrulama yöntemine çok benzemektedir. Ancak, e-imzada gizli anahtar kullanılmamaktadır. Bunun yerine simetrik olmayan şifreleme yöntemine uygun olarak açık ve gizli anahtarlar kullanılmaktadır. Mesajı gönderen taraf, mesajın önce özetini çıkarmaktadır. Ardından bu özeti, gizli anahtarı ile şifrelemektedir. Şifrelenmiş özet bilgi alıcıya gönderilmektedir.

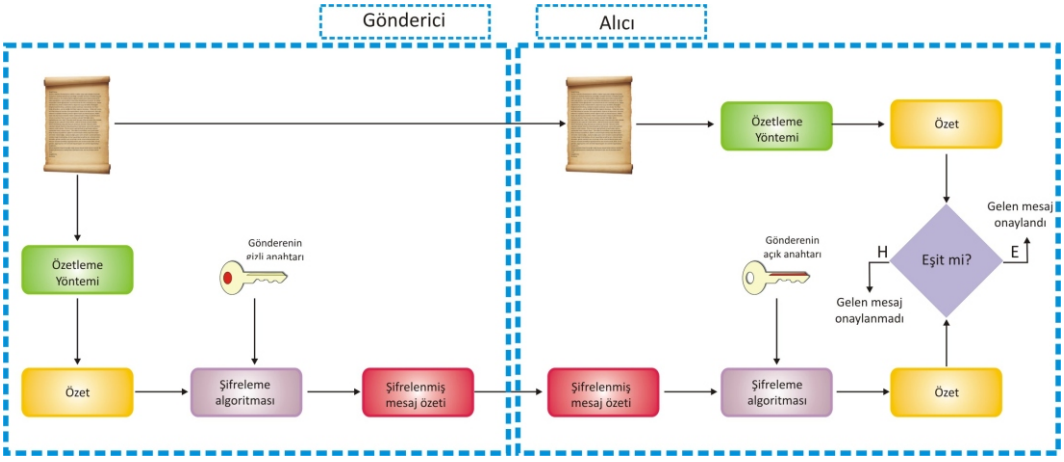
Alıcı taraf, gönderenin açık anahtarını kullanarak özeti açık hale getirmektedir. Buna koşut olarak gelen mesajın özetini oluşturmaktadır. Mesajın özeti ile şifresi çözülmüş özet birbirine




**Şekil-5.10:** Mesaj Doğrulama Kodunun çalışma ilkesi

denk ise gelen mesaj onaylanmakta tersi durumda onaylanmamaktadır. Şekil-5.11'de e-imza yöntemi gösterilmiştir.

Elektronik imza yönteminde, açık ve kapalı anahtarlar, bu konuda yetkili bir kuruluş tarafından dağıtılabilir. Bu durumda, birbirini tanımayan kişiler arasında imza onaylı mesajlaşma olanağı sağlanmış olur.




**Şekil-5.11**: e-imzanın temel çalışma ilkesi

## 5.3 TCP/IP Protokolü

TCP/IP protokolü, bilgisayar ağlarındaki iletişimi kurallara bağlayarak düzenlemek amacıyla ABD Savunma Bakanlığı (DoD) tarafından 1980'li yıllarda geliştirilmiş bir protokoldür. ISO/OSI protokolüne karşıt olarak geliştirildiği değerlendirilmektedir. Önce ARPANET'te, ardından Genelağ'da kullanılmasıyla baskın iletişim protokolü olmuştur. Temel olarak İki katmandan; *Üst Katman* (TCP : Transfer Control Protocol ) ve *Alt Katman* (IP : Internet Protocol) dan oluşur:

**Üst Katman**

Bilgisayarlar arasında iletilecek veri, önce paketlere bölünür ve paketler alıcıya gönderilir. Alıcı, gelen paketleri birleştirerek asıl veriyi elde eder.

**Alt Katman**

İletilmek istenen paketleri, alıcının adresine iletir.

Üst katman içinde, Uygulama ve Taşıma katmanları yer alır.

**Uygulama Katmanı**

Farklı bilgisayarlarda bulunan uygulamalar arasındaki iletişimi sağlar.

**Taşıma Katmanı**

İki bilgisayar arasındaki veri akışını sağlar. Bu sunucudan sunucuya taşıma işlemidir.

Alt katman içinde, Genelağ katmanı, Ağ erişim katmanı ve Fiziksel katman yer alır.

**Genelağ Katmanı**

Birbirine yönlendiriciler ile bağlanmış ağlar üzerinde, kaynak ve hedef bilgisayarlar arasında verilerin iletilmesini sağlar.

**Ağ Erişim Katmanı**

Bilgisayar ile ağ arasında mantıksal ilişkiyi kuran arabirim olarak değerlendirilir.

**Fiziksel Katman**

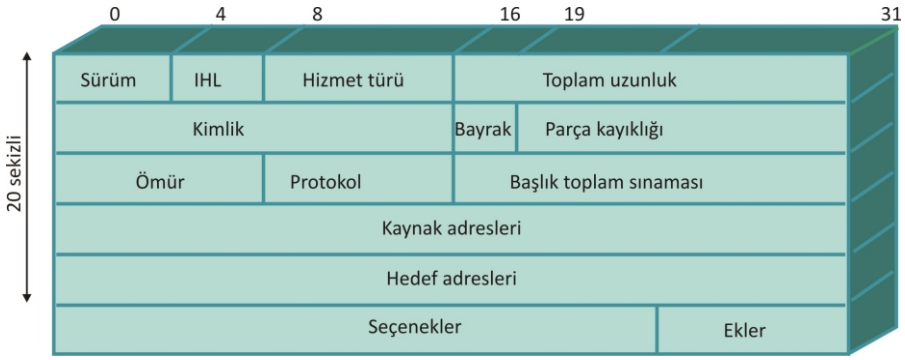
İletişim ortamının elektriksel ve fiziksel özelliklerini belirleyen katmandır.

### 5.3.1 TCP/IP Genelağ Protokolünün Olanakları

Genelağ üzerinde veri iletişimi düzenli biçimde sürdürebilmek amacıyla protokolün sağladığı bazı olanaklar bulunmaktadır. Bu olanaklar, protokolün başlığında yer alırlar. IPv4 protokolünün başlığında yer alan olanaklar Şekil-5.12'de gösterilmiş ve açıklamaları aşağıda verilmiştir:

**Sürüm**

Geçerli olan TCP protokolünün sürüm numarasıdır.




**Şekil-5.12**: IPv4'ün başlığı

### Genelağ Başlık Uzunluğu (IHL)

Başlığın uzunluğunu, sözcüğü birim alarak söyler; örneğin 5 sözcük.

### Hizmet Türü

1988'den sonra bu alanın adı "Farklı Hizmetler" olarak değiştirilmiştir. Hizmet türleri olarak; güvenilirlik, öncelik, gecikme ve veri hacmi olarak belirlenmiştir.

### Toplam Uzunluk

Sekizlik cinsinden *Datagram*'ın (Datagram, içinde kaynak ve hedef bilgisayarın adreslerini içeren veri paketine verilen addır) toplam boyunu söyler.

### Kimlik

Geçerli datagramı tekil olarak belirtmek üzere kullanılan kimlik bilgisidir. Bu değer kaynak, hedef adresi ve kullanıcı protokolü ile belirlenir.

### Bayrak

İki bayrak kullanılmaktadır: Parçalama ya da Birleştirme bayrağı ve Parçalamayı Engelle bayrağı.

### Parça Kayıklığı

Anlık parçanın, datagram'ın hangi parçası olduğunu belirtir. Bir birimi 64 bittir.

### Ömür (TTL)

İleti için biçilen ömrü belirtir. Bu değeri gönderen taraf belirler. Bu değer sıfır olana dek ileti ağda dolaşır. Ömür bittiği halde ileti hedefe ulaşamamış ise, zaman doldu mesajı, iletiyi gönderene bildirilir.

### Protokol

Bir üst düzeydeki protokolü belirtir, örneğin: TCP, UDP, ICMP gibi

### Başlık Toplam Sınaması

Başlık içinde yer alan verilerin doğruluğunu sınamak için kullanılır. Başlıkta yer alan 16 bitlik alanların toplamını sıfırlayacak biçimde hesaplanır.

### Kaynak Adresi

Kaynağın IP adresidir.

### Hedef Adresi

Hedefin IP adresidir.

### Seçenekler

Gönderici tarafından belirlenen ek seçeneklerdir.

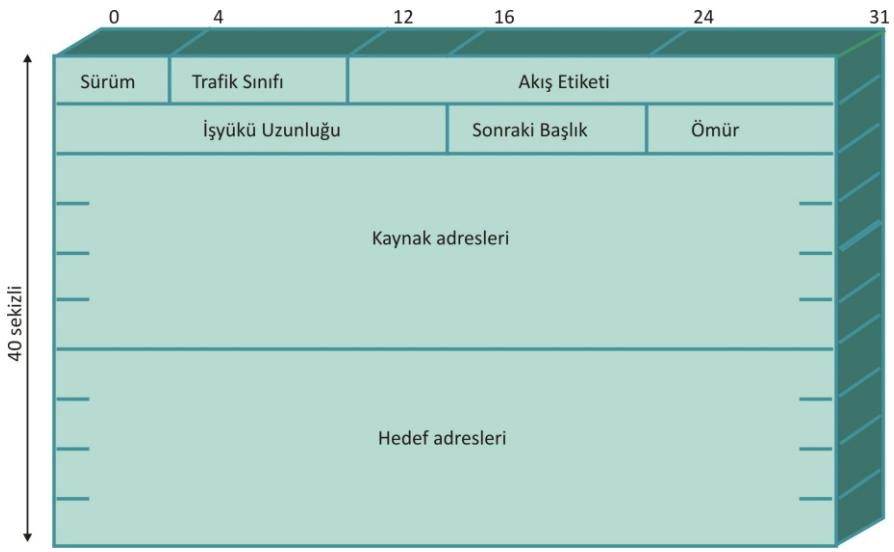
### Ekler

Veri boyu 8 bitin katları biçiminde olmak zorundadır. Eksik bit olursa, ekleme yapılarak düzeltilir.

1981 yılında tasarlanan IP Protokolü (IPv4) bugün artık yetersiz duruma gelmiştir. Bu nedenle IPv6 tasarlanmıştır. IPv6'nın sunduğu olanaklar Şekil-5.13'te gösterilmiştir. Bu olanaklar ile ilgili açıklamalar aşağıda anlatılmıştır:

### Sürüm

Geçerli olan TCP protokolünün sürüm numarasıdır.




**Şekil-5.13**: IPv6'ün başlığı

**Trafik Sınıfı**

8 bitten oluşan bu alanın yüksek anlamlı 6 biti IPv4'te belirtilen Farklı Hizmetleri belirtir. Düşük anlamlı 2 bit kaynağın tıkanıklık denetimi yapılsın ya da yapılmasın denetimi (Explicit Congestion Notification : ECN) için kullanılır.

**Akış Etiketi**

İletinin izleyeceği yönlendiricileri belirmek amacıyla düşünülmüş bir alandır. Günümüzde, paket kandırmasını önlemek amacıyla kullanılmaktadır.

**İşyükü Uzunluğu**

İş yükünün boyunu sekizlik cinsinden belirtir.

**Sonraki Başlık**

Bir sonraki başlığın türünü belirtir.

**Ömür (Hop)**

IPv4'teki TTL alanının karşılığıdır.

**Kaynak Adresi**

Kaynağın IP adresidir; 128 bittir.

**Hedef Adresi**

Hedefin IP adresidir; 128 bittir.

TCP/IP'de iki bilgisayar arasında bağlantı kurma üç aşamada ve el sıkışma biçiminde gerçekleşmektedir. Bu aşamalar sırasıyla aşağıda açıklanmıştır:

1 - Sunucu dinleme durumundadır ve istemcilerden gelecek istekleri bekler.

2 - İstemci sunucudan bağlantı isteğinde bulunur.

3 - Sunucu onay vererek bağlantıyı kurar.

Kurulmuş olan bir bağlantının sonlandırılması için taraflardan birinin FIN bilgisini göndermesi yeterlidir. FIN isteği kabul edildiğinde bağlantı kesilir. Her iki taraf da bağlantıyı sonlandırabilir.

TCP/IP Protokolünde, oturum başlatma ve sonlandırma işlemi Sonlu Durum Makinesi (SDM) gösterimi ile Şekil-5.14'te açıklanmıştır.

## 5.3.2 TCP/IP 4. Sürümün Güvenliği

1980'lerde TCP/IP tasarlandığında, güvenlik konusu çok önemsenmemiştir. Bunun nedeni, belki de uygulanacağı ağın (ARPANET) kapalı bir ağ olarak düşünülmüş olmasıdır. Ancak zaman içinde TCP/IP'nin kullanımının yaygınlaşması, özellikle Genelağ üzerinde kullanılmasıyla güvenlik açıkları görülmeye başlanmıştır. Bu kısımda, TCP/IP'nin ve birlikte kullanılan diğer

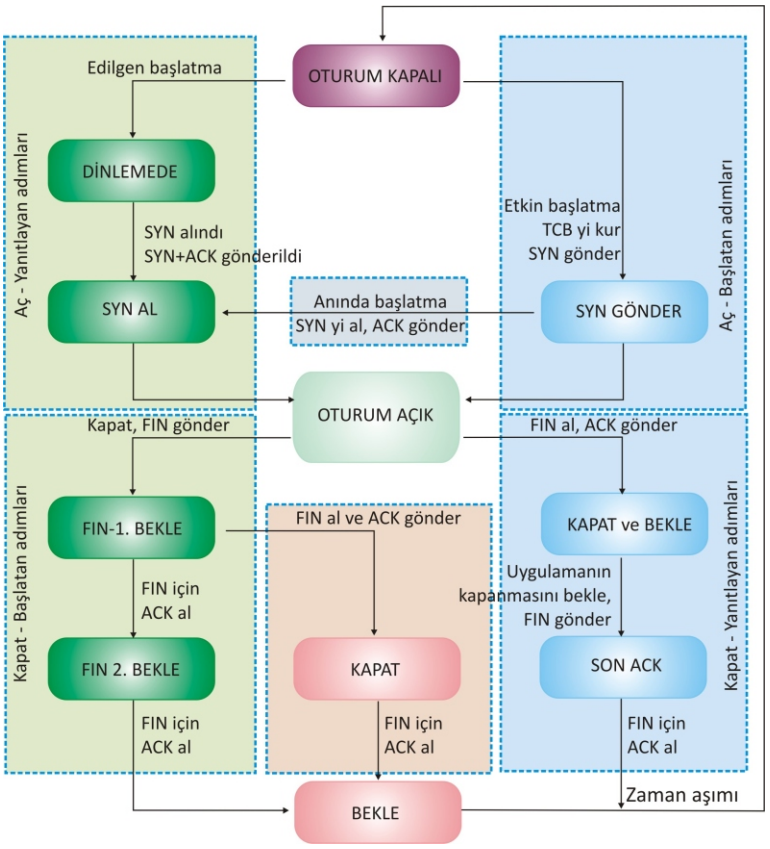
protokollerin güvenlik zayıflıkları ve daha sonra bunlara karşı alınabilecek önlemler anlatılacaktır.

### 5.3.2.1 Saldırılar

Bu kısım TCP/IP v4'te yaşanan saldırılara ayrılmıştır.

#### SYN Saldırıları

Daha önce açıklandığı gibi, TCP/IP protokolünde bilgisayarlar üç aşamada oturum kurarlar. Sunucu dinleme konumundadır ve istemciden istek bekler. İstek SYN olarak gelir. İsteği alan sunucu 75 s kadar bekleme durumunda kalır [11]. Genellikle, sunucular ortalama 5 isteği karşılayacak durumdadır.




**Şekil-5.14**: TCP/IP Protokolünde, oturum başlatma ve sonlandırma işlemi

Sunucuyu meşgul etmeyi hedefleyen saldırganlar, peş peşe bağlantı isteği göndererek, sunucuyu meşgul ederek, hizmet vermesini engelleyebilirler. **SYN kandırması** adı da verilen bu tür saldırılar, TCP/IP protokolünün zayıf yönünden yararlanmaktadır.

#### IP Kandırması

IP kandırması olarak bilinen bu tür saldırılarda, saldırgan kendi IP adresi yerine sahte bir adres kullanılır [12]. Saldırgan, gönderdiği veri paketinin içine sahte bir IP adresi ekleyerek gönderir. Alıcı taraftaki IP katmanı, gelen veri paketinin içindeki adresi gerçek adres olarak değerlendirir.

Günümüzde, IP kandırması yapabilen hazır ve ücretsiz programlar Genelağ üzerinden sağlanabilmektedir. IP kandırması UDP kullanan uygulamalarda kolay kullanılırken, TCP başlık bilgisinde bulunan sıra numarasının kolay tahmin edilememesi nedeniyle http, SMTP ve FTP protokollerinde kullanılması zordur. TCP protokolünde, iki bilgisayar arasında bağlantı kurulması aşaması el sıkışmalı olarak gerçekleşmektedir. Sahte IP ile el sıkışma aşamasını tamamlayabilmek için, TCP'nin başlığında yer alan sıra numarasının (ISN) tahmin edilebilmesi gerekir. İşletim sistemleri sıra numarasını rastgele ürettiklerinden, bu değeri tahmin etmek çok zordur.

IP kandırması türündeki saldırılar genellikle, sunucuların hizmet vermelerini aksatmak amacıyla yapılmaktadır (DDos).

### Sıra Numarasını Tahmin Etme

TCP protokolüne uygun olarak sağlanan bağlantısında kullanılan sıra numarası (Initial Sequence Number : ISN) 32 bit uzunluğundadır; dolayısıyla bu numarayı tahmin etme olasılığı düşüktür. Kaynak bilgisayar tarafından üretilen bu numara belli bir kurala uyularak üretiliyor ise, tahmin etmek kolaylaşır. Unix çekirdeği tarafından üretilen ISN'in belli bir kurala göre hesaplandığı, bu nedenle, bir önceki bağlantıda kullanılan ISN biliniyor ise, bir sonraki ISN numarasının hesaplanabileceği açıklanmıştır [12].

Saldırganlar bu zayıflıktan yararlanmak üzere, çok sayıda ISN'yi denemektedirler.

### Kaynak Yönlendirme

Gönderen taraf, yanıtın hangi yolla hangi IP'ye ulaşması gerektiğini belirlediği bir durumdur [12]. Günümüz yönlendiricileri kaynak yönlendiricisini belirleyebildikleri için bu konu sorun olmaktan çıkmıştır.

### Bağlantıyı Ele Geçirme

Bağlantıyı ele geçirme ya da *Aradaki Adam* olarak adlandırılan bu yöntemde, saldırgan bağlantıda olan iki bilgisayarın arasına girmektedir [13]. Kısım 10.4.2'de anlatılan IP kandırması yöntemi, Unix parolası, Keyberos ve TKP gibi ek güvenlik bilgilerini iki taraf arasında aktaramaz. Ancak bu yöntemde saldırgan, iki bilgisayar arasındaki asıllama işleminin sürmesini sağlar ve bağlantıyı ele geçirir. Aradaki adam yönteminin çalışabilmesi için, aradaki adamın bağlantıdaki iki bilgisayarın iletişim yolu üzerinde bulunması gerekir. Aradaki adam, iki taraftan gelen veri paketleri birbirine aktarır.

Aradaki adam, TCP'nin ayak uyduramama durumundan (desynchronized state) yaralanmaktadır. Gelen veri paketindeki sıra numarası beklenen sıra numarası değil ise iletişimde ayak uyduramıyor kararı verilir. Bu durumda, gelen veri paketi ya ret edilir ya da tampon bellekte tutulur. Bunun nedeni, veri paketlerinin kaybolması veya gecikmesinin önüne geçebilmek amacıyla tasarlanan kayan pencere yöntemiyle etkin bir iletişimin hedeflenmesidir. Bu yüzden, gelen paketin sıra numarası uyuşmuyor

ancak kayan pencerenin içinde ise, bu paket daha sonra gelecek beklentisi ile tampon bellekte saklanır; pencerenin dışında ise ret edilir.

İki bilgisayar iletişimde ayak uydurmama durumuna geldiğinde, gelen paketleri ret etmeye devam ederler. Bu durumda, saldırgan kendi hazırladığı veri paketini doğru sıra numarası ile gönderir. Doğal olarak bu paket ile iletişime eklemeler yaparak isteği biçimde değiştirir.

### Yönlendirme Saldırısı

TCP/IP protokolünde kullanılması kesinlikle gerekli olmayan ancak kullanılan Yönlendirme Bilgisi Protokolü (Routing Information Protocol : RIP) sıkça kullanılmaktadır. RIP, ağ üzerindeki en kısa ya da önerilen yolu tanımlamaktadır. RIP içinde asıllama işlemini barındırmamakta; dolayısıyla doğrulamaya çalışmamaktadır.

Bu açıklardan yararlanan saldırganlar, ileti paketinin geldiği ve gideceği adresleri değiştirebilmektedirler. Böylece saldırganlar, ileti paketlerini ele geçirebilmekte ve içeriğini istediği gibi değiştirebilmektedir.

### ICMP Saldırısı

Alıcı tarafı uyarmak üzere gönderilen mesaj Genelağ Denetim Mesaj Protokolü (Internet Control Message Protocol : ICMP) olarak adlandırılır. Bu mesaj genellikle "*ping atmak*" olarak adlandırılır. Ping atıldıktan sonra, gönderen taraf, karşı tarafın yanıt vermesini bekler. ICMP mesajı içinde asıllama bilgisi yoktur. Bu nedenle hizmet aksatma türü saldırılarda kolaylıkla kullanılmaktadır.

### Alan Adı Hizmeti Saldırısı

Alan Adı Hizmeti (Domain Name Service : DNS) Genelağ ortamında yaygın olarak kullanılmaktadır. İnsanların kolayca belleyebildiği alan adlarını, Genelağ Protokolünün anladığı IP adreslerine dönüştüren işleme DNS ve bu işlemi yapan sunuculara da DNS sunucusu adı verilmektedir. Böylece kullanıcıların web sayfalarına ve sunuculara kolayca erişimi sağlanmaktadır. Genelağ saldırganları, "*Alan Çalma*" adı verilen yöntemle, bir sunucunun ya da web sayfasının IP adresini ele geçirmektedirler. Daha sonra DNS sunucusuna erişerek, DNS'in karşılığı olan IP adresini değiştirirler. Böylece kullanıcıları farklı bir sunucu ya da web sayfasına yönlendirebilirler, [12, 14, 15].

### Tekil Kimliğin Yokluğu

Genelağ'ın kullanılmaya başlandığı ilk dönemlerde, bir bilgisayarı belirtmek için IP adresinin yeterli olmasına karşın zaman içinde yetersiz kalmıştır. Günümüzde, konuma bağlı veya geçici olarak tanımlanan IP adresleri sunucular veya adres dönüştürücüler tarafından değiştirilmektedirler. Dolayısıyla, yere bağlı ya da geçici IP adresine dayalı güvenlik sistemleri saldırılara karşı zayıf kalmaktadır.

### 5.3.2.2 Sorunlar ve Çözüm Önerileri

TCP/IP V4'ün güvenlik açıkları nedeniyle ortaya çıkan sorunların nerelerden kaynaklandığı önceki kısımda anlatılmıştı. Bu sorunlar ile ilgili çok sayıda makale, bildiri ve yazı yayımlanmıştır [12]. Bu kısımda, temel sorunların nasıl çözülebileceği anlatılacaktır.

#### 5.3.2.2.1 Bağlantının Kabulüne ilişkin Sorunlar

SYN saldırısı ile kolayca oluşabilen ve **Hizmeti Aksatma** olarak adlandırdığımız saldırı türü TCP/IP'nin bilinen en önemli zayıflığıdır. Bağlantı temelli TCP/IP protokolünde bir bilgisayarın diğer bir bilgisayara bağlanması süresi ağ üzerinde izlenen yola bağlı olarak değişmektedir. İki bilgisayar aynı kentte olabileceği gibi, dünyanın uzak iki köşesinde de olabilir. Dolayısıyla mesajların gidiş geliş süreleri değişkendir. Bu nedenle, belli bir gecikme süresinin kabul edilmesi gerekmiştir. Sürenin dolması durumunda çok sayıda tamamlanamamış bağlantı mesajı göndererek karşı tarafı hizmet veremez duruma getirilmektedir. TCP/IP protokolü, bağlanmak istenen iki bilgisayar arasındaki uzaklığı göz önüne alarak bağlantı sürecindeki bekleme süresini ayarlayabilir hale getirilmesi bir çözüm olabilir.

Bir başka çözüm, aynı anda hizmet verilebilecek sayısını artırmak olabilir. Bu durumda saldırganların işi biraz daha zorlaşır.

#### 5.3.2.2.2 Asıllama ile ilgili Sorunlar

TCP/IP protokolünün diğer bir zayıflığı paketlerin asıllanması sürecinde yaşanmaktadır. Veri paketini gönderenin kesin olarak belirlenememesi önemli bir asıllama sorununa neden olmaktadır.

Asıllama sorunlarını çözmek üzere;

- Sıra numarasını koruma,
- Güvenlik duvarı kullanma,
- TCP Sargısı,
- Kerberos ve
- Şifrelenmiş ileti

yöntemleri kullanılabilir.

**Sıra Numarasını Koruma**

Sıra numarası üretimine özen gösterilmesi, bu sorunun çözümüne yardımcı olabilir. Bu amaçla, gerçekten rastgele sayı üretebilen üreteçlerin kullanılması önerilebilir. Art arda üretilecek olan sıra numaraları arasında bağlantıların olmamasına dikkat edilebilir.

**Güvenlik Duvarı Kullanma**

Güvenlik duvarları gelen ve giden veri paketlerinin tutarlılığı konusunda başarılı hizmetler sunmaktadırlar. Böylece paketlerin gerçek mi yoksa sahte mi olduğu anlaşılabilmektedir.

**TCP Sargısı**

Bir sisteme peş peşe bağlanmaları denetlemek amacıyla geliştirilen TCP sargısı programı, bilgisayara tekrar bağlanmak isteyenin denetimini yaparak yarar sağlamaktadır [16].

**Kerberos**

Saldırganlardan korunmak için bir çare, uygulama katmanına asıllama bilgisini eklemektir. Buna ek olarak şifrelemek de gerekir.

**Şifrelenmiş İleti**

Her oturumda şifre çözme anahtarının şifrelenmiş olarak gönderilmesi bir çözüm olarak önerilir.

### 5.3.3 TCP/IP 6. Sürümünün Güvenliği

1981 yılında, Genelağ için tasarlanan IPv4'ün özellikle asıllama konusunda yetersiz kaldığı görülmüştür. Bu nedenle yeni bir protokol geliştirmek gerekli olmuştur. 1990 yılında IPv6 tasarlanmıştır. Bu tasarım sırasında, eski sürümün hata ve eksiklikleri giderilmeye çalışılmıştır.

IPv4'te IPv4 Başlığını, Taşıma protokol verisi izler; örneğin TCP, UDP ve ICMP. IPv6'da IPv6'yı Uzatmalı Başlık izler; ardından Taşıma protokol verisi gelir.

IPv6'da IP güvenliği (IPsec) temel bileşendir ve kullanılması zorunludur. IPv6'ya kazandırılan yeni özellikler aşağıda anlatılmıştır.

#### 5.3.3.1 Hizmet Kalitesi

Hizmet kalitesi özelliği, IPv6'nın başlığına Akış Etiketi alanı eklenerek sağlanmıştır. Akış etiketi, belli veri paketlerine öncelik ve ivedilik özelliği kazandırmaktadır. Örneğin iletilen veri paketleri ses ve görüntü içeriyor ise alıcıya bunların eşzamanlı ulaşması bu yöntemle sağlanabilir.

#### 5.3.3.2 Kendiliğinden Kurgulama

IPv6 IP adreslerini durum denetimli ve durum denetimsiz olarak kendiliğinden kurgulayabilme yeteneği vardır. Durum denetimli kurgulamada **Dinamik Sunucu Kurgulama Protokolünü** (Dynamic Host Configuration Protocol (DHCP) kullanır. Bu yöntemde, yeni bağlanan düğümler için sabit tablodan adres ataması yapılır. Durum denetimsiz kurgulama DHCP protokolü kullanmaksızın gerçekleştirilir.

#### 5.3.3.3 Yeni Eklenen Başlıklar

Ipv6'ya aşağıda sıralanan başlıklar eklenmiştir:

**Yönlendirme Başlığı**

Veri paketlerinin belli bir yolu izlemesini sağlar.

### Asıllama Başlığı (Authentication Header : AH)

Asıllama başlığı göndericinin gerçek kimliğini öğrenmesini sağlar. Ayrıca veri bütünlüğünü sağlar.

### Şifreleme Başlığı (Encapsulating Security Payload (ESP) Header)

Şifreleme başlığı mesajın sadece gerçek alıcı tarafından görülebilmesini sağlar.

### Parçalama Başlığı

IPv4'teki parçalama başlığına benzerdir.

### Hedef Seçimli Başlığı

Son hedef düğümüne ilişkin başlık seçeneklerini barındırır.

### Ömür (Hop-by-hop) Başlığı

Yönlendiricilerin gereksinim duyduğu seçeneklerden oluşur.

Güvenliği artırmak amacıyla IPv6'a iki ek başlık eklenmiştir. Bunlardan birincisi Asıllama Başlığı (Authentication Header : AH), diğeri Şifreleme Başlığıdır (Encapsulating Security Payload (ESP) Header). Asıllama başlığı göndericinin gerçek kimliğinin öğrenmesini sağlar. Şifreleme başlığı mesajın sadece gerçek alıcı tarafından görülebilmesini sağlar. Bu iki özelliğin işleyebilmesi için gönderen ve alıcının asıllama ve şifreleme için kullanacakları algoritma ve anahtar konusunda anlaşmış olmalarını gerektirir. Bu anlaşmaya **Güvenlik Birliği** denir ve Güvenlik Değişken Dizini (Security Parameter Index : SPI) olarak adlandırılır. Doğal olarak, SPI anahtar değişimi biçiminde gerçekleşir ve alıcı taraf her gönderici için SPI'yi belirler. Anahtar değişimi için Diffie-Helman anahtar değişim yöntemi kullanılması önerilmektedir, ancak henüz kabul edilmiş değildir.

Asıllama ve şifreleme başlıklarının yapısı sırasıyla Şekil-5.15 ve Şekil-5.16'da gösterilmiştir.


**Şekil-5.15** : Asıllama Başlığı


**Şekil-5.16** : Şifreleme Başlığı

## 5.4 SSL/TSL

Güvenlik ve gizlilik kavramı, elektronik ticarette her zaman önemli ve endişenin kaynağı olmuştur; olmaya da devam etmektedir. Genelağ gibi herkese açık bir ortamda sürdürülen ticarette güvenliğin sağlanması her zaman bu konu ile uğraşan uzmanların ilgi odağı olmuştur. E-ticaret yapanlar da açık ortamda izlenmediklerinden, bilgilerinin çalınmadığından emin olmak isterler.

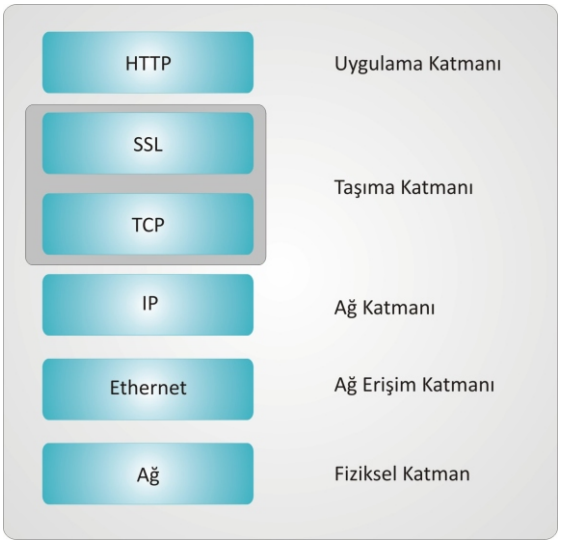
E-Ticareti güvenli kılmak amacıyla, ilk aşamada iletişimin şifrelenerek gizlenmesi amaçlanmıştır. Bu amaçla, Netscape firması Secure Sockets Layer'i (SSL) geliştirilmiştir. İletilen verilerin gizliliği için de RSA firmasının çözümü kullanılmaya başlanmıştır. Çok sayıda kuruluş SSL iletişim protokolünü kullanmaya başlamıştır. Kullanım alanına örnek olarak, her türlü ticari işlemler (F-F (firmalar arası), F-M (firma ile birey arası) ve B-B (bireyler arasında)) ve Genelağ bankacılığı verilebilir.

SSL temel olarak, iletişimin gizliliğini ve bütünlüğünü sağlar. Genelağ üzerinde çalışması hedeflendiğinden TCP/IP üzerinde çalışır. SSL'in TCP/IP'nin neresinde yer aldığı Şekil-5.17'de gösterilmiştir. SSL aşağıdaki protokollerde güvenliği sağlamak amacıyla kullanılmaktadır:

- Web sunucusu ile web tarayıcı arasında iletişimin güvenli biçimde sağlanması için,
- LDAP (Lightweight Directory Access Protocol, Basit Dizin Erişim Protokolü) istemcisi ve LDAP sunucusu arasındaki iletişimin güvenliğini sağlayan LDAP protokolü için,
- İstemci sunucu bağlantısında *Gerektiğinde Sunucu* protokolünün güvenliğini sağlamak için.

SSL, anahtar değişiminde, sunucu asıllaması ve gerektiğinde istemci asıllaması için SYB'yi kullanmaktadır.

TCP/IP ile iki uygulama arasında sağlanan iletişimin gizliliği ve bütünlüğü SSL protokolü tarafından sağlanır. Ayrıca Web'de kullanılan http protokolü güvenlik için SSL'i kullanmaktadır. SSL'in nasıl çalıştığı aşağıda anlatılmıştır:




**Şekil-5.17** : SSL'in TCP/IP'deki yeri

İstemci ve sunucu arasında gidip gelen veriler simetrik şifreleme algoritmaları (örneğin DES veya RC4) ile şifrelenmektedir. Simetrik şifreleme için kullanılacak anahtarlar, bir simetrik olmayan şifreleme algoritması kullanılarak değişilmektedir. Dolayısıyla, bir istemci ile sunucu ilk bağlantıyı kurduklarında simetrik olmayan şifreleme yöntemini (örneğin RSA) kullanırlar. Ardından şifrelemede kullanacakları anahtarı belirlerler. Daha sonra bu anahtarı kullanarak verileri şifrelemekte ve şifrelenmiş verileri çözmektedirler. Simetrik olmayan şifreleme yönteminde sunucu SYB ile açık anahtarını istemciye göndermekte ve istemci bu anahtarı kullanarak yanıtını sunucuya göndermektedir. Bu arada, istemci, sunucunun kimliğini sorgular ve doğrulamaya çalışır. SSL protokolünün 1. ve 2. sürümü sunucunun asıllamasını yapabilirken 3. sürümü hem istemci hem de sunucunun asıllamasını yapabilmektedir.

http temelli bir SSL bağlantısı her zaman istemcinin göndereceği `https://` şeklinde Tekdüze Kaynak Bulucu (Uniform Resource Locator : URL ) ile başlar. SSL oturumunun ilk aşaması el sıkışma süreci ile başlar. Bu süreçte oturum için şifre değişkenleri belirlenir. Sürecin adımları aşağıda açıklanmıştır:

### 1. İstemci "hello" mesajı

İstemci, tercih sırasına uygun olarak yeteneklerini sunucuya açıklamak üzere; kullandığı SSL'in sürüm bilgisini, kullandığı şifreleme programını ve sıkıştırma yöntemini sunucuya bildirir. Bu mesaj rastgele üretilmiş 28 byte veri içerir.

### 2. Sunucu "hello" mesajı

Karşılık olarak sunucu, kullanmak üzere belirlediği şifreleme ve sıkıştırma yöntemini istemciye bildirir. Buna ek olarak oturum kimliği ve rastgele bir sayıyı ekler. İstemcinin tercih ettiği şifreleme yöntemlerinden en az birisinin sunucu tarafında da bulunması gerekir. Genellikle, sunucu en güvenilir şifreleme yöntemini yeğler.

### 3. SYB Gönderme

Sunucu sayısal yetki belgesini istemciye gönderir. Eğer, sunucu 3. sürüm SSL kullanıyor ise, istemciden sayısal yetki belgesini göndermesini ister. Bu istekte bulunurken, hangi

tür SYB'lerini kabul edeceğini de bildirir; örneğin kabul edeceği sertifika yetkilisinin adlarını söyler.

**4. "Hello Tamamlandı"**

Sunucu "hello tamamlandı" mesajını gönderir ve bekleme durumuna geçer.

**5. "hello Kabul Edildi"**

Sunucunun gönderdiği **hello tamamlandı** mesajını alan istemci, diğer bir deyişle web tarayıcısı sunucunun SYB'yi soruşturur. Ayrıca "hello değişkenlerinin kabul edilebilir olup olmadığını sınar. Bu arada, sunucu istemciden SYB istemiş ise bunu sunucuya gönderir. İstemcinin SYB'si yok ise bu durumu sunucuya bildirir. Sunucunun hizmet verebilmesi için istemcinin SYB'si gerekli ise oturum sonlanır; değil ise oturum devam edebilir.

İstemci, SYB'sini sunucuya gönderir ise istemci **Sayısal İmza Sorgulama** mesajını özel anahtarı ile şifreleyerek sunucuya gönderir. Bu mesaj sunucu tarafından sorgulandığında istemcinin sahibi olduğu belgenin doğruluğunu öğrenir.

**6. Anahtar Değişimi**

İstemci kullanmak istediği anahtarı sunucuya gönderir. Anahtar, simetrik anahtarın üretilmesinde kullanılacak bir temel kısım ve 64 bitten oluşan rastgele sayıdan oluşur. Anahtara ek olarak **Mesaj Doğrulama Kodu** (Message Authentication Code : MAC) anahtarını da gönderir. Tüm bu bilgileri, sunucunun açık anahtarı ile şifreleyerek sunucuya gönderir.

**7. Anahtar Üretimi**

İstemci simetrik şifrelemede kullanacağı anahtarı üretir ve **Şifre Değiştirme** (change cipher spec) mesajını sunucunun, yeni anlaşılan şifreleme yöntemi için sunucuya gönderir. Bundan sonra gönderilen istemcinin gönderdiği mesaj, şifrelenmiş ilk mesajdır. Sunucu kendi **Şifre Değiştirme** ve **Sonlandırma** (finished) mesajını gönderir.

Böylece SSL el sıkışma süreci tamamlanmış olur. Bundan sonra istemci ve sunucu arasında simetrik şifreleme yöntemiyle şifrelenmiş veriler gidip gelmeye başlar.

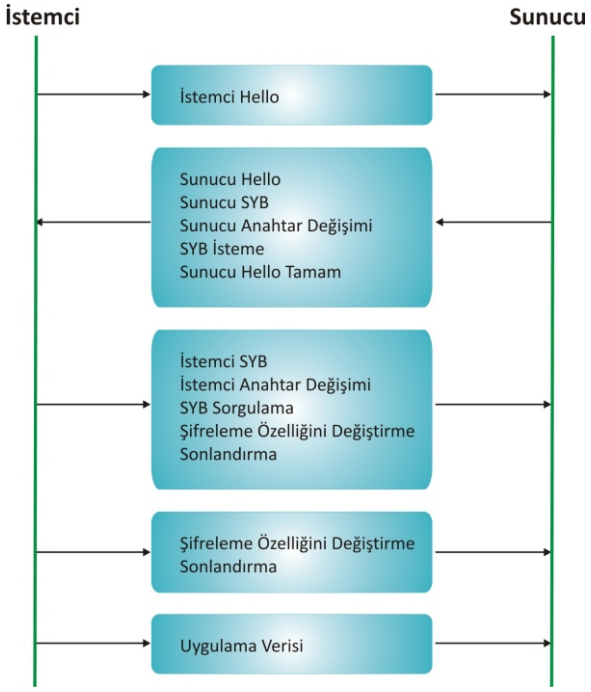
Yukarıda anlatılan adımlar Şekil-5.18'de gösterilmiştir.

## 5.5 İstemci Asıllama

Bir istemcinin, bir sunucuya bağlanması sırasında, sunucu istemcinin kimliğinden emin olmak isteyebilir. Bu durumda istemcinin SYB'sini SSL el sıkışması sırasında isteyebilir. Bu aşamada, sunucu SYB'nin gerçek olup olmadığını da denetler.

## 5.6 Güvenli e-Posta

E-postaların güvenli olması çoğu kişinin isteğidir. Gelen e-postanın, kimliği belli bir kişiden gelip gelmediği önemlidir. Güvenli e-posta için kullanılan **Gizli e-posta** (*Privacy Enhanced Mail: PEM)* veya **Güvenli Genelağ Postası** (*Secure/Multipurpose Internet Mail Extensions* : S/MIME) yöntemleri sayısal imza ve şifreleme ve şifrelenmiş metni çözmek için gerekli olan anahtarların değişimi için SYB kullanılmaktadır.




**Şekil-5.18**: SSL'de el sıkışma süreci

## 5.7 Sanal Özel Ağlar

Sanal özel ağlar, kuruluşların dışarıya kapalı olarak oluşturdukları bilgisayar ağlarıdır. Önceleri kiralık hatlar ile kurulan bu yapı, şimdilerde Genelağ üzerinde de kurulabilmektedir. Bu ağ bir anlamda tünel olarak değerlendirilir. Söz konusu tünele sadece yetkilendirilmiş bilgisayarlar girebilir. Tünelin uçlarında birer güvenlik duvarı bulunur. Tünel içinde gidip gelen veriler, güvenlik duvarı tarafından şifrelenir. Tünel içindeki iletişimde IPsec ölçünü geçerlidir. Tünelden yararlanan taraflar arasındaki anahtar değişimi ve sayısal imza için SYB gerekli olmaktadır.

## 5.8 Güvenli Elektronik Ödemeler

Genelağ üzerinden yapılan ticaretin her gün arttığı bir gerçektir. Bunun giderek daha da artacağı kolayca öngörülebilir. Ancak hem müşteri hem de satıcılar açısından güvenlik endişe ve kuşkusu da sürmektedir. Kredi kartı ile ödemelerin güvenli biçimde yapılması son derece önemli ve endişeli bir süreçtir. Bu amaçla Genelağ üzerinden kredi kartı ile yapılacak ödemeler için, içinde Visa, MasterCard, IBM, Microsoft, Netscape ve VeriSign'nın da bulunduğu 11 teknoloji firması **Güvenli Elektronik Ödeme** (Secure Electronic Transaction : SET) ölçününü 1966'da tasarlamışlardır.

SET protokolünün ana ilkesi, Genelağ üzerinden yapılacak ödemenin, müşteri tarafından satıcıya doğrudan yapılmaması; bunun yerine ödemenin bir aracı kuruluş (ödeme kanalı) üzerinden yapılmasıdır.

Güvenli ödeme sisteminde hem müşteri hem de satıcı için SYB gerekmektedir. SET içinde SYB kullanıldığı için müşteri, satıcı ve banka arasında güvenilir ve gizli bir iletişim sağlanmaktadır. Ödeme işlemi güvenli biçimde kurulmakta, sorunsuz sürdürülmekte ve sahteciliği engellemektedir. Satıcı kredi kartı hakkında bilgi edinemediğinde, kartın çalınmış ya da sahte olduğuna karar verir.

Genelağ üzerinden yapılan ticaret ve ödemelerde, bilgi güvenliğinin dört temel ilkesi geçerlidir: Asıllama, gizlilik, bütünlük ve inkar edilmezlik. Gizliliği sağlamak üzere simetrik ve simetrik olmayan şifreleme yöntemlerinin SSL için de kullanıldığını biliyoruz. Bir web sayfasına bağlanma aşamasında, güvenli ortamı ilk sağlayan SSL'dir. Bu güvenliği, müşteri ve satıcının sayısal yetki belgelerini kullanarak sağlamaktadır. Kısaca, SSL'in müşteri ve satıcı arasında güvenli bir tünel oluşturduğunu söyleyebiliriz. Dolayısıyla, iki taraf dışındakiler, bu tünel içinde gidip gelen verileri göremezler. Sonuç olarak SSL iletişimin gizliliğini sağlamış olur.

Bu anlatılanlardan sonra, SSL'in tümüyle güvenilir bir ortam sağladığı düşünülebilir. Ancak bazı sorunların yaşanma olasılığı hâlâ bulunmaktadır.

- SSL müşteriyi, kulak misafirlerinden korumaktadır; buna karşın sahte satıcılardan koruduğu söylenemez. Bazı satış siteleri sahte veya yanıltıcı site olabilmektedir. Bu tür siteler müşterileri dolandırmak amacıyla kurulurlar. Müşterilerini iki türlü dolandırırlar:
    1- Tanınmış bir satıcının taklidini yaparak ya da
    2- Tümüyle yalancı bir site oluşturarak.
- Birinci yöntemde, tanınmış bir satıcının web sayfasını, müşterinin fark edemeyeceği kadar küçük bir değişiklikle taklit ederler. Dolayısıyla, müşteri bilinen, hatta saygın bir firmadan alışveriş yaptığını düşünür. İkinci yöntemde, satıcı uygun fiyatlarla ürün pazarlıyor gibi görülür. Müşteri seçtiği ürünleri satın alır ve ödemesini yapar. Ancak kendisine sahte bir ürün gönderilir.
- Dolandırıcılardan bazıları müşterilerinden, web sayfalarında belirttikleri fiyattan daha fazlasını tahsil edebilmektedirler. Özellikle, kandırıldığını söylemekten çekineceği tür alışverişte bulunanlar bu tür dolandırıcıların hedefidir.
- Müşterilerin satıcıları dolandırması da olasıdır. Müşteriler, sahte kredi kartı bilgileri kullanarak alışveriş yapabilmektedirler. Özellikle bilgisayarsız kredi kartının kullanıldığı ülkelerde ya da karta ilişkin parolanın sorulmadığı uygulamalarda, müşteriler bir başkasının kredi kartı bilgisini kullanarak alışveriş yapabilmektedirler.
- Bu tür dolandırıcılıkların önüne geçebilmek üzere, *3 boyutlu güvenlik sistemleri* geliştirilmiştir. **Üç boyutlu güvenlik sisteminde**, kredi kartı ile ödeme anında, müşterinin cep telefonuna bir sayı gönderilmekte ve müşterinin bu sayıyı ödeme

ekranındaki alana girmesi istenmektedir. Böylece, kredi kartı ile ödeme yapmak isteyenin gerçek müşteri olup olmadığı kararı verilmektedir.

### 5.8.1 SET Protokolü

Yukarıda anlatılan sorunlara çözüm bulmak amacıyla geliştirilen SET protokolünün temel ilkeleri aşağıda sıralanmıştır:

- Sipariş ve ödeme bilgilerinin gizliliğini sağlamak,
- Ödeme işlemi ve hizmetler ile ilgili verilerin bütünlüğünü sağlamak,
- Müşteri kredi kartı hesabının asıllamasını sağlamak,
- Satıcının asıllamasını sağlamak.

Bu ilkeleri sağlayabilmek amacıyla aşağıda isimleri verilen taraflar üzerinde çalışır:

1 - Kredi kartı sahibi müşteri,

2 - Web sayfası olan satıcı,

3 - Müşteriye kartı veren banka,

4 - Satıcının müşterisi olduğu banka,

5 - Ödeme kanalı,

6 - Sertifika Yetkilisi.

### 5.8.2 SET Protokolü Nasıl Çalışıyor?

İlkesel olarak, SET protokolüne uygun alışveriş için müşteri ve satıcının sayısal yetki belgelerinin olması gerekir. Satıcılar için bu koşul olmazsa olmaz koşuldur. Ancak her müşteri için bu koşulu sağlamak olanaklı değildir. Bu nedenle, müşterinin kimliği kredi kartı bilgileriyle asıllanmaya çalışılır.

SET protokolünde, bir alışveriş süreci 9 adım olarak tanımlanmıştır:

1- Müşteri, satıcının web sayfasına bağlanır.

2 - Müşteri satın almak istedikleri ile ilgili olarak, iki parçadan oluşan sipariş ve ödeme bilgilerini gönderir. Parçalardan birincisi alışveriş ile ilgilidir ve satıcıya gönderilir. İkinci parça kredi kartı bilgisidir ve bu bilgi satıcının müşterisi olduğu bankaya gönderilmek üzere satıcıya gönderilir.

3 - Satıcı kredi kartı bilgilerini, bankasına iletir.

4 - Satıcının bankası, müşterinin kredi kartını, bu kartı veren kuruluşa bağlanarak onay ister.

5 - Kredi kartını müşteriye vermiş olan kuruluş, satıcının bankasına onay gönderir.

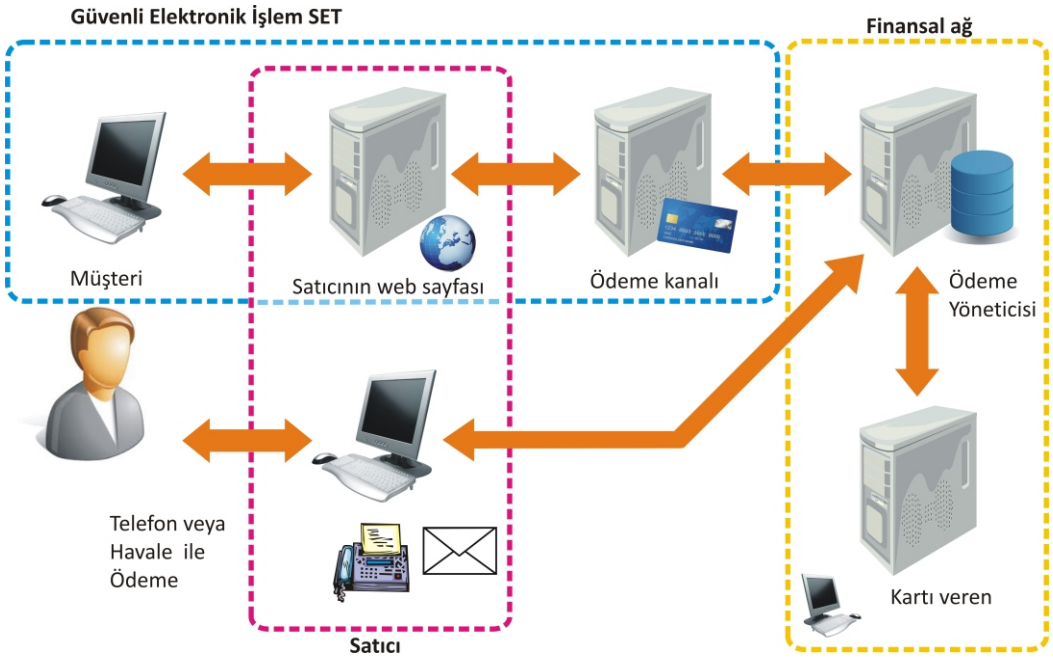
6 - Satıcının bankası, satıcıya onay gönderir.

7 - Satıcı siparişi tamamlar ve müşteriye onay bilgisini gönderir.

8 - Satıcı bankasından alışveriş ile ilgili işlem kaydını alır.

9 - Kredi kartını müşteriye veren kuruluş, müşteriye kredi kartı ödeme belgesini (fiş ya da fatura) gönderir.

SET protokolünün nasıl çalıştığı Şekil-5.19'da gösterilmiştir.

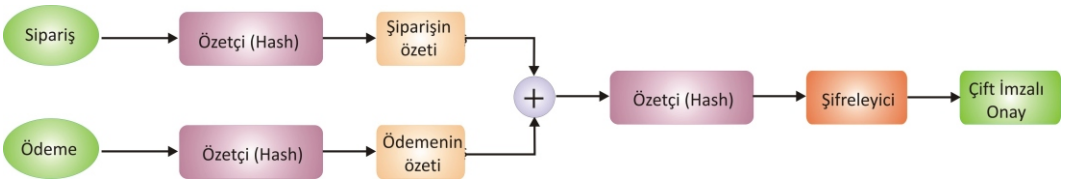



**Şekil-5.19**: SET protokolünün çalışma biçimi

SET protokolünün adımları anlatılırken, ikinci adımda müşterinin sipariş ve ödeme bilgilerini iki parça halinde gönderdiğini söylemiştik. İlk parça alışveriş ile ilgilidir. Bu parçaya Sipariş adını veriyoruz ve bu parça satıcıya gönderiliyor. İkinci Parça ödeme ile ilgilidir. Ödeme adını verdiğimiz bu parça kredi kartına ilişkin bilgileri içerir ve satıcının bankasına gönderilir. Satıcının ödeme ile ilgili bilgileri, daha açık bir ifadeyle kredi kartı bilgilerini görmemesi gerekir.

Bir alışverişin tamamlanabilmesi için bu iki parçanın birleştirilmesi gerekir. Şekil-5.20'da Sipariş ve Ödeme bilgilerinin nasıl birleştirildiği gösterilmiştir.

Şekil-5.20'den görüldüğü gibi, ödeme bilgisinin özeti satıcıya gelmektedir. Sipariş ile ilgili bilgiyi satıcı görebilmekte ve bu bilginin özetini çıkarabilmektedir. Her iki özet birleştirilip şifrelendikten sonra çifte imza onayı ile sonuca ulaşılmaktadır. Böylece alışveriş iki tarafın imzası ile onaylanmış olmaktadır. Bunun sonucu olarak iki tarafın da alışverişi inkâr edebilmesinin önü kesilmiş olmaktadır. Satıcı, Sipariş, Çift İmza ve Ödemenin Özeti bilgilerini kullanarak bankadan ödemeyi alabilir.




**Şekil-5.20**: Sipariş ve Ödeme bilgilerinin birleştirilmesi işlem

Günümüzde SET protokolü;

- Müşteri kredi kartının Kişisel Kimlik Numarasını (PIN)
- Bilgisayarlı kredi kartlarında, müşteri parolasını
- Eliptik Eğri Şifrelemesini (ECC)

kullanabilmektedir.

## 5.9 DNS (Domain Name System)

İnsanların kolayca belleyebildiği alan adlarını, Genelağ Protokolünün anladığı IP adreslerine (IPv4 de 32 bit ve IPv6 de 128 bittir) dönüştüren işleme DNS ve bu işlemi yapan sunuculara da DNS sunucusu adı verilmektedir. Böylece kullanıcıların web sayfalarına ve sunuculara kolayca erişimi sağlanmaktadır. Genelağ saldırganları, "Alan Çalma" adı verilen yöntemle, bir sunucunun ya da web sayfasının IP adresini ele geçirmektedirler. Daha sonra DNS sunucusuna erişerek, DNS'in karşılığı olan IP adresini değiştirirler. Böylece kullanıcıları farklı bir sunucu ya da web sayfasına yönlendirebilirler.

Genelağ'ın tasarlandığı ilk dönemlerde, bu denli kolay olan alan çalma türü saldırılar düşünülememiştir. Ancak zaman içinde bu sorunu çözmek üzere DNSSec geliştirilmiştir.

## 5.10 Güvenlik Duvarı

Güvenlik duvarı, genel anlamıyla, dışarıdan gelebilecek zararlı veya gereksiz veri paketlerinin içeriye geçmesine ve dışarı çıkması istenmeyen veri paketlerinin dışarı çıkmasını engel olan donanım ve yazılımlar olarak tanımlanır.

Bu görevi yapabilmeleri için, güvenlik duvarı, kuruluşun bilgisayar ağı ile Genelağ arasına yerleştirilir. Büyük ölçekli kuruluşlarda, bölüm ağları arasına da yerleştirilir. Böylece bir bölümün diğer bir bölümdeki çalışmaları görmesi engellenir. Örneğin muhasebe bölümü ile ArGe bölümü arasına bir güvenlik duvarının yerleştirilmesi uygun olabilir.

Güvenlik duvarı, genellikle bilgisayar ağları arasına yerleştirilir. Telefon hatları, cep telefonu şebekeleri arasına güvenlik duvarı konulması yüksek maliyetlere neden olur.

Güvenlik duvarı uygulaması ile kuruluş içindeki verilere kuruluş dışından yetkisiz bir kişinin erişmesi istenmez. Benzer şekilde, kuruluş içinden birinin, dışarıdaki her siteye erişmesi istenmeyebilir. Bu tür engellemeler erişilmesi istenmeyen sitelerin adresleri biliniyor ise adres temelli yapılabilir. Benzer şekilde dışarıdan bağlanmak isteyen bilgisayarın IP adresi biliniyor ise engellenebilir.

OSI katmanlı yapısında Ağ ve Taşıma katmanları erişim denetimi için olanak sağlamaktadır. Ağ katmanı bize kaynak ve hedef bilgisayarların IP adreslerini söylemektedir. Taşıma katmanı TCP ve UDP iskele bilgilerini içermektedir. Uygulama katmanı, e-posta adresi, postanın içeriği, web isteklerini, çalışabilir programları, virüs ve zararlı programları, görselleri, kullanıcı adı ve parola gibi uygulamalara ilişkin bilgileri içerir. Dolayısıyla istenmeyen girişler ve çıkışlar için bu katmanlardaki bilgilerden yararlanılarak engelleme olanağı vardır.

Güvenlik duvarları veri paketlerini de engelleyebilmektedirler. OSI Ağ ve Taşıma katmanındaki bilgilere dayanarak, hangi veri paketlerinin duvarı geçebileceği, hangilerinin geçemeyeceğine karar verilebilir.

Bu şekilde verilen kararlara dayalı olarak çalışan güvenlik duvarlarına kural tabanlı güvenlik duvarı adı verilmektedir. Paketlerin süzülmesi için oluşturulan kurallar durağandır ve uygulamada sıkıntı ve rahatsızlıklara neden olabilir ancak, kuruluşun güvenliği açısından gerekli ise bu biçim uygulama gereklidir.

Dinamik olarak çalışan güvenlik duvarları da vardır. Bunlar gelen istek ve yanıtları anlarlar. Örneğin SYN, ACK mesajlarını tanırlar. Paketi engelleme ya da engellememe konusundaki kararı, bu el sıkışma mesajlarına bakarak verinin ilk paketinde karar verirler ve bu karar arkadan gelen paketler için aynen uygulanır.

Kuruluşun güvenlik politikasına ve gereksinimlerine uygun olarak güvenlik duvarının kurulması ve kurgulanması uygun olur. Aşağıda bir örnek kurgulama verilmiştir:

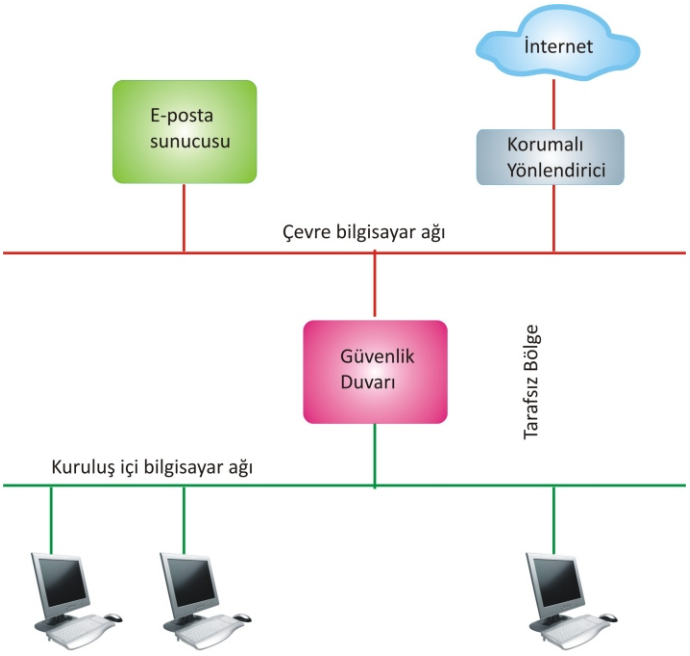
- Genelağ'a çıkışta http, ftp, SSH ve DNS'e izin ver
- Dışarıdan gelen e-postalar için sadece smtp türüne izin ver.
- Posta sunucusundan Genelağ'a çıkışta smtp ve DNS'e izin ver
- Posta sunucusun içeriden erişimde smtp ve pop3'e izin ver
- Yanıt nitelikli paketlere izin ver
- Bunların dışındakileri engelle

Güvenlik duvarının yeri konusunda bir öneri Şekil-5-21'de verilmiştir.

## 5.11 Sızma

Güvenlik duvarları, dışarıdan gelebilecek saldırıların önemli bir kısmını önleyebilecek yetenekte üretilmektedirler. Yukarıda söylendiği gibi bunlar donanım veya yazılım temelli olabilirler.

Güvenlik duvarlarının engelleyemediği saldırı türleri de vardır; örneğin sunuyu meşgul etmek üzere yapılan saldırılar. Ayrıca güvenlik duvarının tüm saldırıları karşılayacak biçimde kurgulanmamış olması da sorunlara neden olmaktadır. Bu tür açıklar nedeniyle kuruluş bilgi sistemine sızmalar olabilmektedir.




**Şekil-5.21**: Güvenlik duvarının yeri konusunda bir öneri

Sızmalara karşı önlemler iki aşamalı olmaktadır; saldırıları algılama ve saldırılara tepki verme. Kuruluş bilgisayar ağına olabilecek sızmaları algılamak üzere, kuruluş sunucularına ve bilgisayar ağına çok sayıda duyarga yerleştirilir. Bunlar aslında birer program parçalarıdır ve kuruluş bilgi sistemine sızmaları algılayıp rapor ederler. Ettikleri raporlar, kuruluşun güvenlik bölümü tarafından değerlendirilir ve verilmesi gereken tepki üretilir.

Duyargalardan toplanan veriler sızmanın türü hakkında bilgi oluşturur. Buna sızmanın örüntüsü veya sızmanın imzası denir. Sızmanın örüntüsü belli olduğunda bu tür sızmalara karşı daha önce hazırlanmış olan tepki eylemi kendiliğinden çalışmaya başlar.

Sızmaların örüntüsünü çıkarabilmek için kural tabanlı yöntemler, sezgisel yöntemler ve makine öğrenmesi yöntemlerinden yararlanılmaktadır.

Sızmalar iki türlü olabilir; Kötü davranışlar ve aykırı davranışlar.

### 5.11.1 Kötü Davranışları Algılama

Kötü kullanımı algılamak için bilgisayar ağındaki trafik ve eylem tutanağı izlenir. Bu izlemeler sırasında şüpheli görülen davranışlar saptanır. Örneğin sunucuya bağlanmak için yapılan

eylemler, bu tür eylemlerin sıklığı, sunucuya meşgul etmek için yapılan SYN kandırması türü saldırılar, yetkisiz birinin veri tabanına erişme eylemi kötü davranışlar olarak sayılır.

Sızma konusunda deneyimi olan ya da çeşitli sızma biçimlerinin örüntüsünü bilen bir bilgi sistemi bu tür sızmaları yakalayabilir. Ayrıca engellemek için gerekli olan tepkiyi verir. Zaman içinde değişik tür sızmaların da olabileceği düşünülmeli ve sızma örüntüsü veri tabanı giderek zenginleştirilmelidir. Zenginleştirme sızma algılama ve önleme sistemini sürekli güncelleyerek gerçekleştirilebilir.

### 5.11.2 Aykırı Davranışları Algılama

Sızma eylemlerini ortaya çıkarmanın bir başka yolu, olağan ve olağan olmayan davranışları ayırt etmektir. Kuruluş bilgisayar ağıdaki iletişim trafiği, programlara erişim sayısı ve sıklığı, veri tabanlarına erişim sayısı ve sıklığı belli süre izlenerek ölçülür. Daha sonra bu olağan davranışın dışına çıkan aykırı davranışların oluşumu izlenir.

Olağan davranışların ve bunun ardından aykırı davranışların çıkarılmasında, günümüzde makine öğrenmesi yöntemlerinden yararlanılmaktadır. Bu yöntemler, insan tarafında kolayca ortaya çıkarılamayacak aykırı davranışları ortaya çıkarmada oldukça başarılı sayılırlar.

### 5.11.3 Ağ Temelli Sızmaları Algılama

Bilgisayar ağındaki trafik sürekli izlenerek, sızmalar yakalanmaya çalışılır. Sızmanın olmadığı olağan bir günde elde edilen trafik bilgileri olağan veri olarak kabul edilip, öğrenen sisteme, eğitim verisi olarak yüklenir. Daha sonra trafik sürekli izlenir ve bu izleme sırasında, trafikte oluşacak hızlanma ya da yavaşlama öğrenen sistem tarafından algılanır.

### 5.11.4 Sunucu Temelli Sızmaları Algılama

Sunucu temelli sızmalar, genellikle eylem tutanağı izlenerek ortaya çıkarılabilir. Bu tür sızmaları ortaya çıkarabilmek amacıyla da öğrenen sistem yöntemlerinden yararlanılabilir. Olağan durumlarda elde edilen eylem tutanağı, öğrenen sisteme eğitim verisi olarak yüklenir. Daha sonra eylem tutanağı sürekli olarak izlenir ve olağan dışı durumlar saptanır.

### 5.11.5 Ballık Yöntemi

Sızmaların özelliklerini ortaya çıkarmanın bir yolu, saldırganları aldatmaktan geçmektedir. Bu yöntemde, kuruluş içinde ballık adı verilen bir bilgisayar oluşturulur. Bu bilgisayar saldırgana, gerçek bilgisayar gibi davranır ve kendisine doğru yöneltir. Saldırgan, bu bilgisayardan veri toplamaya başlar veya başka eylemlerde bulunur. Ballık adı verilen bilgisayar bu sırada saldırganın davranışlarını izler ve bu izleme sonunda saldırganın davranış örüntüsünü çıkarır. Benzer davranışta bulunan saldırganlar için alınacak önlemler hazırlanır. Daha sonra, bu örüntüye uygun davranışlar saptanır ve uygun tepki verilir.

# Kaynaklar ve Okunması Önerilen Yayınlar


[1] *F. Halsall, Data Communications, Computer Networks and Open Systems, Addison-Wesley, 1992*

[2] D. Gollmann, *Computer Security*, John Wilwy&Sons, Ltd, 2005

[3] A. Conklin, G. B. White, C. Cothren, D. Williams, R. L. Davis, *Principles of Computer Security*, Mc Graw Hill, 2004

[4] B. Guttman, E. A. Roback, *Network Security Basics*, www.syngress.com, 2006

[5] S. Bosworth, M.E. Kabay, E. Whyne, *Computer Security Handbook*, John Wiley&Sons, 2009

[6] C. Chambers, J. Ddolske, J. Iyer, *TCP/IP Security, Department of Computer and Information Sci. Ohio State University, Columbus, OH*, http://www.linuxsecurity.com/resource_files/documentation/tcpip-security.html

[7] *IBM Global Secutity Kit : Secure Sockets Layer, Introduction andiKeyman User's Guide*, IBM, 2006, http://www-01.ibm.com/support/docview.wss?uid=pub1sc23651000

[8] D. R. Kuhn, V. C. Hu, W. T. Polk, Shu-Jen Chang, *Introduction to Public Key Technology and the Federal PKI Infrastucture, NIST, 2001*

[9] P. Davies,Secure electronic transactions (SET) in e-commerce ,2006. http://www.pkdavies.co.uk/articles/103-secure-electronic-transactions-set-in-e-commerce.html

[10] *Introduction to Secure Sockets Layer*, Cisco Systems, 2002 http://euro.ecom.cmu.edu/resources/elibrary/epay/SSL.pdf

[11] B. Guha, B. Mukherjee, *Network Security Via Reverse Engineering of TCP Code: Vulnerability Analysis and Proposed Solutions*, Research Projects Agency (ARPA) under Contract No. DOD/DABT63-93-C-0045. 1995

[12] S.M. Bellovin, *Security Problems in the TCP/IP Protocol Suite*, Computer Communication Review, Vol. 19, No. 2, pp. 32-48, April 1989

[13] M. Lin, *An Overview of Session Hijacking at the Network and Application Levels*, GSEC Practical Assignment v1.4c (Option 1), 2005

[14] C. L. Schuba, I. V. Krsul, M. G. Kuhn, *Analysis of a Denial of Service Attack on TCP, http://cs.unc.edu/~fabian/course_papers/schuba.pdf*

[15] T. E. Daniels, E. H. Spafford, *Subliminal Traceroute in TCP/IP, CERIAS Tech Report 2000-10*, https://www.cerias.purdue.edu/assets/pdf/

# 6

# E-Ticaret Etik ve Hukuku

Büyük firmaların 1970'lerden beri bilgisayarlar arası iletişim yoluyla ticaret yaptıkları bilinmektedir. Bu tür ticaret bir özel ağ (VAN: Value Added Network) üzerinden gerçekleştirilmektedir. Genelağ'ın yaygınlaşmasının bir sonucu olarak daha çok bireysel kullanıma yönelik e-ticaret gelişmiştir. Bu yolla yapılan e-ticaret çok hızlı gelişmektedir. İnsanların alışveriş işlemini kolaylaştıran e-ticaret değişik sorunları da beraberinde getirmiştir.

Ticaretin üç temel ilkesi vardır:

- Ticaret güvenli ortam ister.
- Alıcı ve satıcının birbirine güvenmesi gerekir.
- Alan ve satan alışverişten mutlu olmalıdır.

Büyük kuruluşların kapalı bir ağ olan VAN üzerinden gerçekleştirdikleri, EDI belgelerini kullanarak yapılan e-ticarette yeterli güvenlik sağlanmaktadır ve taraflar birbirini çok iyi tanırlar.

Dolayısıyla bu bölümde inceleyeceğimiz uygulama, Genelağ üzerinde süren ve çok sayıda kişiyi ilgilendiren e-ticarettir. Bu bölüm içinde e-ticaret sözcüğü Genelağ'daki e-ticaret anlamında kullanılacak ve e-ticaretin hukuk ve etik sorunları anlatılacaktır.

## 6.1 Tarafların Birbirine Güvenmesi

Önceki bölümlerde Genelağ üzerinden yapılan e-ticareti aşağıdaki gibi sınıflandırmıştık.

- Firma - Müşteri (F-M)
- Firma - Firma (F-F)
- Firma - Kamu (F-K)
- Birey - Kamu (B-K)
- Birey - Birey (B-B)
- Birey - Firma (B-F)
- Kamu - Birey (K-B)
- Kamu - Firma (K-F)
- Doğrudan - Birey (D-B)

Tarafların birbirine güvenmesi konusunun her sınıf için ayrı ayrı değerlendirilmesi uygun olacaktır.

### 6.1.1 Firma ile Müşteri Arası Ticaret

Firma ile müşteri arası ticaret günümüzdeki en yaygın e-ticaret uygulamasıdır. Firma ve bireyin gerçek olamama olasılığı vardır. Bu nedenle sorunlar yaşanmaktadır. Bu ticaret yönteminde satıcı, e-ticaret amaçlı kurulmuş bir firmadır. Alıcı ise çoğunlukla kendisi ya da bir kuruluş adına alım yapan bireydir. İnsanlar için büyük kolaylık sağlayan bu e-ticaret yöntemi aynı zamanda satıcılar için de büyük ticari kazançlar sağlamaktadır. Bu nedenle her geçen gün e-ticaret firmasının sayısı ve buna koşut olarak müşterilerin sayısı artmaktadır. Bu sayıların giderek artacağını söylemek için kâhin olmaya gerek yoktur.

Genelağ üzerinde var olan e-ticaret firmalarının sayısının milyondan fazla olduğu, ancak bunların içinde yıllık ciroları milyar lirayı aşanların sayısının binden az olduğu tahmin edilmektedir. Dünya veya ülke genelinde geçmişi olan ve tanınmış firmalara insanlar güvenebilirler. Ancak geçmişi bilinmeyen ve tanınmayan e-ticaret firmalarından yapılacak alımlarda kandırılma riski her zaman vardır. Çoğu satıcı sattığı ürünü geri almayı kabul etmektedir. Ancak küçük firmaların bu konuda sözlerini tutmayabildiklerine tanık olunmaktadır.

Satıcı firmalara yapılacak ödemeleri güvence altına almak üzere geliştirilmiş güvenlik yöntemleri ve protokoller bir önceki kısımda anlatılmıştı. Kredi kartı ile ödemelerde satıcının Sayısal Yetki Belgesinin olması gerekir. SYB olmayan bir firmadan alışveriş yapılmamalıdır. Bir başka deyişle SYB satıcının kim olduğunun bilinmesi anlamını taşır.

Genellikle az bilinen e-ticaret firmaları ile yaşanan sıkıntılar aşağıda anlatılmıştır:

### Ayıplı Ürün Gönderilmesi

E-ticaret sayfasında beğenilip seçilen ürün müşteriye gönderilmektedir. Ancak gönderilen ürün kullanılmış, bozuk, arızalı ya da tamir edilmiş bir ürün olabilmektedir. Ürün geri gönderildiğinde yenisini gönderen firmalar olabildiği gibi hiç yanıt vermeyenler de olabilmektedir. Özellikle ayıplı ürünü bilerek gönderen firmalardan yeni ve sağlam bir ürün beklemek saflık olur.

### Taklit Ürün Gönderilmesi

Dış görünümü bilinen bir ürüne çok benzer olan bir ürün gönderilmektedir. Taklit ürün gönderenlerin dolandırıcı oldukları kesindir. Dolayısıyla ürünü geri göndermek ve gerçek ürünün gönderilmesini beklemek anlamsızdır.

Bazı Uzakdoğu ülkesi firmaları lisanslı programları (özellikle işletim sistemlerini) ucuz fiyatla satmaktadır. Gelen ürün bilgisayara lisanslı bir ürün gibi kurulabilmektedir. Bu tür programların piyasa fiyatlarının altında nasıl satılabildiği araştırıldığında şu sonuçla karşılaşılmıştır: İşletim sistemi üreten firmalar bilgisayar donanımı üreticisi firmalara bu programların bir aslını vermekte ve çoğaltma hakkı tanımaktadırlar. Her bir çoğaltma için de lisans numarası tanımlamaktadırlar. İşletim sistemi programının kopyasını elde etmek satıcı için kolaydır. Bunun kopyalarını CD veya DVD üzerine hazırlayıp aslı gibi etiketlemektedirler. Donanım üreticilerinden elde ettikleri lisans numaralarını da pakete ekleyip pazarlamaktadırlar.

### Eksik Ürün Gönderilmesi

Bazı ürünler paketler hâlinde satılmakta ve her paketin içinde kaç tane olduğu belirtilmektedir. Dolandırıcı firmalar paketlerin içine ürün sayfasında yazan sayıdan daha az koymaktadırlar.

### Sahte Ürün Gönderilmesi

Disk yerine demir kütle, ilaç yerine toz kireç, kitap yerine, kitabın kapağının geldiğini söyleyen insanları duyuyoruz.

Genelağ üzerinden sürdürülen bankacılık işlemleri kuruluş ve birey arası ticaret sayılabilir. İnsanlar paralarını bankalara güvendikleri için yatırırlar. Genelağ bankacılığında insanların paralarının çalınması bankanın bir eylemi değildir. Müşterinin hesap bilgilerini ve parolasını çalan soyguncuların işidir.

Şu ana kadar hep satıcıların müşterileri kandırabileceği anlatılmıştır. Müşterilerin satıcıları kandırdığı olaylar da görülmektedir. Genellikle kredi kartı ile yapılan ödemelerde kandırmalar olmaktadır. Bir kredi kartının yapısı Şekil-3.2'de tanıtılmıştı. Bu şekle bakıldığı zaman geçerli bir kart olarak görülebilecek bir kredi kartı numarasını oluşturmak olanaklıdır. Bunun için Genelağ'da hazır programlar da bulunmaktadır. Bilgisayarlı kredi kartının kullanılmadığı ve 3 düzeyli güvenliğin uygulanmadığı ülkeler

için geçerli bir kredi kartı numarası üretip bunun ile alışveriş yapılabilmektedir. Satıcı firmaların bu tür kartlar ile alışveriş yapmak isteyenlere karşı özel önlemler alması gerekir.

Sonuç olarak F-M türü e-ticarette satıcının güvenilir olup olmaması çok önemlidir. Geçmişi bilinen ve güven kazanmış e-ticaret firmalarının SYB'leri vardır ve çoğunlukla SET protokolünü kullanırlar. Dolayısıyla bu firmalardan güvenli alışveriş yapılabilir. Adı sanı bilinmeyen firmalardan alışveriş yapmaktan kaçınılmalıdır. Bireysel müşterilerin SYB'lerinin olması gerekmediğinden satıcılar sahte kredi kartlarına karşı önlem almak zorundadırlar.

### 6.1.2 Firmalar Arası Ticaret

Bölümün girişinde açıklandığı gibi VAN üzerinde büyük firmalar arası yapılan ticarette, firmalar birbirini tanımakta ve kullandıkları iletişim ağı kapalı ve güvenlidir. Dolayısıyla etik ve hukuk açısından önemli bir sorun kaynağı değildir.

Genelağ'ın yaygınlaşması ile firmalar arası ticaretin Genelağ üzerinde de gerçekleştirildiği görülmektedir. Genelağ'dan kaynaklanan güvenlik sorunlarını gidermek için firmalar elektronik imza ve Sayısal Yetki Belgesi kullanmayı yeğlemektedirler.

### 6.1.3 Firma ile Kamu Arası Ticaret

VAN ve buna bağlı olarak EDI'nin ortaya çıkmasının kaynağı firmalar ile kamu arasında gerçekleştirilen ticaret gösterilir. 1970'li yıllarda başlatılan bu e-ticaret biçimi kapalı bir ağ üzerinden sürdürüldüğü ve ağa bağlı olanların kimlikleri belli olduğundan önemli bir güvenlik sorunu yaşamamıştır. Günümüzde, firmalar ile kamu kuruluşları arasındaki e-ticaret ağırlıklı olarak VAN üzerinde yapılmaktadır.

Genelağ'ın yaygınlaşması ile kamu kuruluşları Genelağ üzerinden de işlem yapmaya başlamışlardır. Bu yeni uygulamalar genellikle yüksek güvenlik gerektirmeyen alanlarda olmaktadır. Güvenliği artırmak amacıyla sayısal imza ve SYB kullanılmaktadır.

### 6.1.4 Birey ile Kamu Arası Ticaret

Bireyler ile kamu kuruluşları arasında gerçek anlamda bir ticaretin yapıldığını söylemek zordur. Genelağ üzerinden gerçekleştirilen işlemler genellikle vergi sorgulama, beyanname doldurma ve vergi ödeme işlemleri biçiminde olmaktadır. Kamu kuruluşundan elde edilecek bilgileri sorgulama aşamasında elektronik imza kullanılmaktadır. Ödemeler kısmında, bir kişinin, tanımadığı bir kişi için ödeme yapmayacağı görüşüyle buna gerek görülmemektedir.

### 6.1.5 Bireyler Arası Ticaret

E-ticaretin en riskli olan biçimi bireyler arası olan biçimidir. Çünkü iki tarafın da SYB'si yoktur ve olması da beklenmemektedir. Bireyler arasındaki ödemeyi güvence altına almak üzere geliştirilmiş düzenlemeler vardır. Bunlar alıcı ve satıcı arasındaki para aktarımı işini üstlenen kuruluşlardır. Alıcı ve satıcı anlaştıktan sonra alıcı parasını aracıya gönderir. Alıcı ürünü aldığını söylemeden aracı kuruluş satıcıya ödemeyi aktarmaz.

Bireyler arası ticarette de bir önceki kısımda anlatılan sorunlar yaşanabilir:

- Ayıplı ürün gönderilmesi
- Taklit ürün gönderilmesi
- Eksik ürün gönderilmesi

Bireylerin kimlikleri ve adresleri gerçek olmayabilir. Bu nedenle, yukarıda sıralanan sorunların ortaya çıktığı durumlarda, sorun yaratan bireyin bulunması ve hukuki yollara başvurulması oldukça zordur.

## 6.2 Tarafların Kazanması

Bir ticaretin, ticaret sayılabilmesi ve sürdürülebilir olması için alıcı ve satıcının yapılan alışverişten kazançlı çıkması gerekir. Güvenlik sorunu olmadığını bilen bir müşteri güvendiği bir satıcıdan ürün almayı her zaman yeğler. Çünkü:

- Ürünü seçmek için satıcının yerine gitmesi gerekmez. Özellikle, özellikleri bilinen ve ölçünlere uygun olarak üretilmiş ürünleri elle incelemek ve denemek gerekmediğinden e-ticaret sitesinden seçmek yeterlidir. Oturduğu yerden istediği zaman sipariş vermek ve ürünün ayağına kadar getirilmesi müşteriyi mutlu eder.
- Satın aldığı ürünü hiçbir gerekçe belirtmeden değiştirebileceğinin garantisini bilmesi alışveriş kararını daha kolay ve hızlı vermesini sağlar. Geri gönderme yükünün satıcıya ait olması kararını daha da etkiler. Bu kolaylık birden fazla ürün sipariş etmesinin yolunu açar. Gönderilen ürünlerden beğenmediklerini belli süre içinde geri gönderebilir. Böylece ürünleri ve satıcıyı ayağına kadar getirmiş duygusuyla mutlu olur.
- E-ticarette satıcı ürünleri sergilemek üzere geniş alanlara gereksinim duymaz. Hatta ürünleri kendi deposunda saklaması da gerekmeyebilir. Siparişi aldıktan sonra üreticiden isteyebilir. Bu yöntemle işletme giderlerinden çok büyük tasarruf sağlar. Yerinde satış için gerekli olan satış elemanı ve ortamı ısıtma, soğutma ve aydınlatma gibi giderler de olmayacaktır. Giderleri çok azalacak bir kuruluş için e-ticaret yöntemiyle ürün veya hizmet satmak son derece kârlıdır.
- E-ticaret ile dünya geneline ürün ve hizmet satılabilmektedir. Dolayısıyla firmaların ciroları e-ticaret sayesinde artmaktadır. Bu da satıcı için mutluluk vericidir.

## 6.3 E-ticaretteki Etik ve Hukuk Sorunları

Bölümün bu kısmına kadar önce ticaretin ardından e-ticaretin sorunları anlatılmıştır. Bu kısımda söz konusu sorunlar etik ve hukuk açısından değerlendirilecektir.

### 6.3.1 E-ticaretteki Soygunlar

Ticaret ortamının güvenliğini sağlamak kamunun görevidir. Genelağ üzerindeki ticaretin güvenliğini sağlamak da müşterilerin ve satıcıların görevi değildir. İlgili kısımda anlatıldığı gibi e-ticaretin güvenliğini sağlamak üzere epey çalışma yapılmıştır. Müşteriler kimlik ve kredi kartı bilgilerini ve parolalarını çaldırmadıkları sürece sorun olmaması gerekir. Güvenliği kırarak yaşanan olaylar ve değerlendirmeleri şöyledir:

Kullanıcının kimlik bilgileri ve parolasının çalınması, genellikle bankacılık işlemlerinde kullanılan hesap bilgisi ve parolanın çalınması ile gerçekleştirilen soygun türüdür. Soyguncu müşterinin bilgisayarına casus programının yüklenmesini sağlamakta ve bu program sayesinde müşterinin hesap numarası ve parolasını öğrenebilmektedir.

Bu tür soygunların sonunda açılan davalarda konu çok tartışılmıştır. Müşteriler bankanın itibarlı ve güvenilir bir kuruluş olduğunu dolayısıyla soygundan sorumlu olmaları gerektiğini söylemişlerdir. Buna karşın bankalar müşterinin bankaya girişte kullandığı anahtar bilgileri saklaması gerektiğini savunmuşlardır. Aslında iki taraf da haklıdır. Ancak bankaların güvenilir ve sorumlu kuruluş olmaları onları güvenliği artırmak üzere yeni ve etkin çözümler bulmaya itmiştir. Bu çalışmaların sonucu olarak Tek Kullanımlık Parola (TKP), cep telefonuna onay kodu gönderme ve 3 düzeyli güvenlik yöntemleri geliştirilmiştir.

Genelağ bankacılığında bir müşterinin hesap numarasını ve parolasını bir başkasına vererek ortak soygun yapma olasılığı da görülmüştür. Bu tür soygunların nasıl yapıldığı aşağıdaki kısımlarda anlatılacaktır.

#### 6.3.1.1 Genelağ Bankacılığı Soygunları

Genelağ bankacılığı müşteriler ve bankalar için kolaylık ve kazançlı bir uygulamadır. Ancak beraberinde önemli güvenlik sorunlarını da getirmiştir. Ülkemizde bu alanda yaşanmış sorunları zamana bağlı olarak anlatmakta yarar görüyoruz. E-Bankacılıkta, güvenlik sorunları ve güvenliği artırmak amacıyla kullanılan yöntemler;

- Tuş izleme
- Ekran kopyalama
- Tek kullanımlık Parola

Bölüm-4.1.5'te anlatılmıştır.

Genelağ bankacılığı üzerinden yapılan soygunların ilk aşaması müşterinin anahtar bilgilerini ele geçirmek, ikinci aşamada, müşterinin bankadaki parasını izi belli olmayacak bir şekilde bankadan çekmektir. Müşterilere ilişkin anahtar bilgilerinin nasıl elde edilebileceği

Bölüm-4.1.5'te anlatılmıştı. Bundan sonraki kısımda ülkemizde yaşanmış Genelağ bankacılığı soygun örnekleri zamansal sırada anlatılacaktır.

### Kullanıcı Adı ve Parolası ile Genelağ Bankacılığı

Yaşlı bir kişi banka hesabının Genelağ bankası üzerinden çalındığı şikâyeti ile mahkemeye başvurur. Banka müşterinin hesabından ne zaman ve ne kadar para çekildiğini, para çekme işleminin Genelağ bankacılığı üzerinden yapıldığını, bağlanan bilgisayarın IP adresini ve telefon numarasını mahkemeye sunar. İşlem gerçekleştirilirken müşterinin hesap numarası ve parolası doğru girilerek sisteme erişim sağlanmıştır. Banka bu bilgileri mahkemeye vererek kendisinin sorumlu olmadığını belirtmiştir.

Davacı, bankanın bilgisayarına girilerek parasının çalındığını iddia etmiştir.

Hâkim bu iddia üzerine bilirkişi heyetinden bankanın bilgi sistemlerinde inceleme yapmasını istemiştir.

#### İnceleme

- Soygun bankanın bilgisayarına girilerek yapılmamıştır.
- Müşterinin banka hesap numarası ve parolası tuş okuma veya ekran kopyalama yöntemiyle çalınmış olabilir. Bu arada müşterinin bu bilgileri bilinçli biçimde soyguncuya verme olasılığı da unutulmamalıdır.
- Soygun için Genelağ bankacılığına giriş yapan bilgisayarın yeri belirlenmiş ancak belirlenen yerde kimse bulunamamıştır. Çünkü bu inceleme ve araştırmalar aylar almıştır.
- Müşterinin bilgisayarı başvuru sırasında incelenmediğinden, daha sonra bir inceleme yapılması anlamlı bulunmamıştır. Ancak söz konusu bilgisayarın, evdeki çocuklar tarafından Genelağ'da oyun oynamak üzere kullanıldığı anlaşılmıştır.

**Değerlendirme**

- Müşterinin anahtar bilgileri bilgisayarına yüklenen tuş okuma veya ekran kopyalama casus programları ile çalınmış olabilir. Bilgisayarın oyun sitelerine girmek için de kullanılıyor olması bu şüpheyi güçlendirmektedir.
- Müşterinin anahtar bilgilerini dolandırıcıya bilerek verme olasılığı düşük de olsa vardır.
- Bankanın Genelağ bankası kullanıcıları için sağladığı güvenlik düzeyi düşüktür. Saygın ve güvenilir bir kuruluş olması beklenen bankanın, bu tür soygunları önleyecek önlemler alması beklenir.

**Sonuç**

- Müşteri %15 banka %85 oranında suçludur.

## İsme Havale

Geleneksel bankacılıkta bir kişinin adına bankada hesabı olmasa da para gönderilebilmektedir. Soyguncular ilk olarak bu açıktan yararlanmaya çalıştılar. Müşteriye ilişkin anahtar bilgileri elde ettikten sonra bu hesaptaki parayı bir başka kentteki bir kişinin adına havale ettiler. Soyguncu ile iş birliği hâlinde olan bu kişi bankanın havale yapılan şubesine giderek adına gelen havaleyi sadece kimliğini göstererek çekebilmiştir. Bankadaki memur gelen kişinin kimliğinin bir kopyasını alarak işlemi doğru yaptığını sanmıştır. Aslında gösterilen kimlikler genellikle sahtedir. Bu açık hemen fark edilmiş ve bankada hesabı olmayanlara Genelağ bankacılığı ile havale yapılması engellenmiştir.

Soyguncular bunun üzerine sahte kimlikler ile bankalarda hesap açmaya ve bu hesaplara havale yapmaya başlamışlardır. Bankalar buna karşılık olarak yeni hesap açma işlemlerini daha ciddi yapmaya başlamışlar, MERNİS'in sağladığı **Kimlik Paylaşım Sistemin**den **(KPS)** müşteri kimliklerini doğrulamaya çalışmışlardır. Ayrıca yeni açılmış hesaplara belli bir süre Genelağ üzerinden para havalesi yapılmasına izin vermeyerek güvenliği artırmışlardır.

İsme veya hesaba havale yoluyla soygun işine yurt dışındaki soyguncular da katılmıştır. Bu soyguncular, önce parayı Türkiye'deki kişilere aktarmış, ardından bu kişilerden parayı yurt dışındaki hesaba göndermesini istemiştir. Bu sırada, Türkiye'deki kişiyi tehdit ettikleri de gözlenmiştir.

**İnceleme**

- Soygun, müşterinin banka hesap numarası ve parolası tuş okuma veya ekran kopyalama yöntemiyle çalınmıştır.
- Soygun için Genelağ bankacılığına giriş yapan bilgisayarın yurt dışında olduğu anlaşılmıştır.
- Müşterinin bilgisayarı, başvuru sırasında incelenmediğinden, daha sonra bir inceleme yapılması anlamlı bulunmamıştır.

**Değerlendirme**

- Müşterinin anahtar bilgileri, bilgisayarına yüklenen tuş okuma veya ekran kopyalama casus programları ile çalınmıştır.
- Bankanın, Genelağ bankacılığı kullanıcıları için sağladığı güvenlik düzeyi düşüktür. Saygın ve güvenilir bir kuruluş olması beklenen bankanın, bu tür soygunları önleyecek önlemler alması beklenir.
- İsme ya da hesaba yapılan para aktarmalarında güvenlik önlemlerinin artırılması gerekir.

**Sonuç**

- Banka %100 suçludur.

### ATM Kartı

Havale yolunun tıkandığını gören soyguncular yeni arayışlara başlamışlardır. Buldukları çözümlerden biri şöyledir: Bankada hesabı, dolayısıyla ATM kartı olan ancak gelir düzeyi düşük ve genellikle işsiz insanları kandırma yoluna gitmişlerdir. Bu tür kişileri genellikle kahvehanelerde bulup, kolay para kazanma önerisi ile kandırmışlardır. Bu kişilerden banka kartlarını belli bir bedel karşılığında almakta parolasını ve telefon numaralarını da öğrenmektedirler. Kart sahibini telefonla aradıklarında, bankayı aramasını ve cüzdanını kaybettiğini, cüzdanında banka kartının ve bir kâğıt üzerinde de parolasının yazılı olduğunu söylemesinin yeterli olacağını söylerler. Dolayısıyla başının derde girmeyeceğini açıklarlar.

Gerekli anahtar bilgilerini ele geçirdikleri banka hesabındaki paranın tümünü bir banka kartı ile ATM'den çekme olanağı yoktur. ATM'lerden bir gün içinde çekilebilecek para miktarı sınırlı olduğu için farklı bir yol bulmaları gerekmiştir. Bunun için en kolay yol kuyumcudan altın satın almak olarak bulunmuştur. İlk aşamada soyulacak hesaptaki paralar, para karşılığı elde edilen banka kartı sahibinin hesabına aktarılır. Ardından

vakit geçirilmeden bir kuyumcuya gidilir. Bu gidişe evlilik hazırlığı yapan bir çift olarak gidilmesi şüpheleri azaltır. Genç çift kuyumcuya gider. Çalacakları paraya denk gelecek kadar altın ziynet eşyasını ayırırlar. Kuyumcu hesabını yapar. Damat adayı bu kadar parayı cepte taşımasının doğru olmayacağı, dolayısıyla yanında getirmediğini ve ATM'den havale yapacağını söyler. Kuyumcunun banka hesap numarasını öğrenerek dükkândan ayrılır. Gelin adayı kuyumcuda oturmaya devam eder. Damat adayı yakındaki ATM'ye gider ve elindeki banka kartı ile havaleyi yapar. Ardından kuyumcuya geri döner. Kuyumcu banka hesabında havale edilmiş parayı gördüğünden altınları müşterilere teslim eder.

### İnceleme

- Soygun, müşterinin banka hesap numarası ve parolası tuş okuma veya ekran kopyalama yöntemiyle çalınmıştır. Müşterinin hesabındaki paralar, önce ATM kartı, para karşılığı alınan kişinin hesabına, daha sonra kuyumcunun hesabına aktarılmıştır.
- ATM üzerinden, kuyumcuya para aktarımı yapıldıktan kısa bir süre sonra banka kartı sahibi, bankayı arayıp cüzdanını kaybettiğini bildirmiştir. Bu arada, cüzdanında, kart parolasının yazılı olduğu kağıdın bulunduğu bilgisini söylemeyi de unutmamıştır.
- ATM'den para aktarma zamanı ile kart sahibinin bankayı bilgilendirme zamanı arasındaki sürenin kısa olması, dikkat çekicidir ve şüpheyi artırıcı niteliktedir.

### Değerlendirme

- Müşterinin anahtar bilgileri, bilgisayarına yüklenen tuş okuma veya ekran kopyalama casus programları ile çalınmıştır.
- ATM kullanılarak para aktarma işleminde para sınırı yoktur. ATM kartı sahibinin hesabına gelen paranın kısa süre içinde bir kuyumcuya ATM üzerinden aktarılması şüpheli bir işlemdir. Ayrıca, bu işlemden kısa bir süre sonra kart sahibinin bankayı arayarak cüzdanını kaybettiği bilgisini vermesi dikkat çekicidir.
- Kuyumcunun, yapılan ticaretten şüphelenmemesi olağan karşılanabilir.
- ATM kartını para karşılığı veren kişi, kartın kötü amaçla kullanılacağının farkındadır.

### Sonuç

- Soygunu gerçekleştiren kişi ya da kişiler suçludur. ATM kartını bu kişilere satan kişi de suç ortağıdır.

Yukarıda anlatılanlara dikkat edilirse Genelağ bankacılığında yaşananlar savaş oyunlarına benzemektedir. Bir taraf bir silah geliştirir, karşı taraf bu silaha karşı önlem alır. Bunun üzerine ilk taraf daha üstün bir silah geliştirir, karşı taraf buna karşılık yeni bir önlem geliştirir. Bu döngü sürekli olarak devam eder. Genelağ bankacılığında da bankalar bir yöntem geliştirirler, soyguncular bu yöntemin açığını bularak nasıl soygun yapabileceklerini araştırırlar. Bankalar yeni soygun yöntemine karşı yeni güvenlik çözümleri bulurlar. Soyguncular yeni güvenlik yönteminin açığını araştırırlar.

Soyguncuların hedefi bankadaki bir hesaptan paraları iz bırakmadan çalmak olduğuna göre bankaların hangi işlemler için özel güvenlik önlemi almaları gerektiği açıktır. Müşterinin tanımlamadığı ya da onaylamadığı hesaplara para aktarılması kesinlikle engellenmelidir. Bu önlemi gerçekleştirebilmek için müşterilerden para aktarılacak hesapları (Havale ya da EFT) tanımlamaları güvenlik gereği istenmeli ve denetlenmelidir. Bunun için yeni hesap tanımlandığında, müşteri telefonla aranarak sorulmalı ya da cep telefonuna gönderilecek bir kodu onay bilgisi olarak sisteme girmesi istenmelidir. Bu noktada önemle vurgulanması gereken husus, ***müşteri cep numarasının, Genelağ bankacılığı ürün sayfası üzerinden değiştirmesine kesinlikle izin verilmemelidir.*** Müşteriler için Genelağ bankacılığında kullandıkları cep telefonu numaralarını değiştirmek üzere banka şubesine gitmeleri veya ATM üzerinden değişiklik yapmaları veya çağrı merkezini arayarak değişiklik isteğinde bulunmaları yorucu olabilir, ancak güvenlik için gereklidir.

Bankalar saygın ve güvenilir kuruluş olduklarından gerekli güvenlik önlemlerini almakla yükümlüdür. Bunun sonucu olarak olası her türlü soygunda sorumlu duruma düşerler.

### 6.3.1.2 Kredi Kartı Soygunları

Kredi kartının ilk olarak 1950'de kullanılmaya başlanıldığı bilinmektedir. Varlıklı iş adamı McNamara'nın 1949'da cüzdanını unuttuğundan lokantada yemek parasını ödeyememesi üzerine düşünüp geliştirdiği Diners Club kartı, kredi kartı uygulamasının başlangıcı sayılır. Diners Club kartı ilk dönemlerde sadece varlıklı kişilere saygınlık kartı olarak verilmiştir. Hedef bir ay boyunca yapılan yemek ve konaklama harcamalarının ay sonunda kart işletmecisine ödenmesiydi. Lokanta ve oteller paralarını ay sonunda kart işletmecisinden alıyorlardı. Dolayısıyla bugün anladığımız anlamdan biraz farklıydı. 1980 öncesi kredi kartları ile yapılan ödemeler karbon kopyalı makbuzlar ile gerçekleştirilmekteydi. Makbuz kopyalarından biri kart sahibine, biri işletmeye ve biri de bankaya verilmekteydi. Kartların arkasında manyetik şerit yoktu. Bugün yaygın olarak kullanılan kredi kartlarının yaygınlaşması bilgi teknolojilerindeki gelişmelerle sağlanmıştır.

Tıpkı Genelağ'ın başlangıcında olduğu gibi kredi kartının kullanılmaya başlandığı günlerde güvenlik sorunu yaşanacağı öngörülememiştir. İlk dönemlerde sadece varlıklı insanlara verilen kredi kartları artık herkese verilmektedir. Ayrıca ay sonunda borcun kapatılması gerekmemektedir.

Kredi kartının ön yüzünde kartın sahibine ve kartı veren kuruluşa ilişkin bilgiler yer almaktadır; bunlar kartı veren kuruluşun adı, kart sahibinin adı, soyadı, kartın geçerlilik tarihi ve kartı tekil olarak tanımlayan numaradan oluşmaktadır.

Kredi kartının güvenliğini artırmak amacıyla, daha sonra kartın arka yüzünde yazılı olan güvenlik kodu (CVC) eklenmiştir. Güvenlik kodu, kredi kartı numarası ve geçerlilik tarihinden oluşan sayının bir şifreleme algoritması kullanılarak oluşturulduğu bir sayıdır. Yakın zamanda kredi kartının güvenliğini artırmak amacıyla kart içine mikrobilgisayar yerleştirilmiştir. Bu bilgisayar sahibinin bildiği parolanın doğrulamasını yapar, dolayısıyla kartın kişiye ait olduğunu kanıtlar. Bilgisayarlı kartlar EMV kart olarak adlandırılır.

Kredi kartının zayıf olan güvenliği kredi kartı dolandırıcıları için çekim kaynağı olmuştur. Hâlâ bazı ülkelerde kullanılan kopyalı makbuz ve ıslak imza yöntemi güvenlik açısından son derece zayıftır. Kabartmalı kredi kartını kullanarak birden fazla kopya üretilebileceği ve imzanın kolayca taklit edilebileceği düşünülürse artık bu kullanım biçiminden vazgeçilmelidir. EMV ya da akıllı kartlar henüz bütün dünyada kullanılmamaktadır. Kredi kartı numarası güvenlik kodu ve ıslak imzaya güvenilmektedir. Genelağ üzerinden yapılan ticarette ıslak imzanın da kullanılmaması önemli sorunlara neden olmaktadır. Genelağ üzerinden kredi kartı ile yapılan alışverişlerde güvenliği artırmak amacıyla kart sahibinin cep telefonuna onay kodu gönderilerek güvenlik sağlanmaya çalışılmaktadır.

Dünya genelinde yapılan değerlendirmelerde en çok kredi kartı soygunu sırasıyla ABD, Hindistan ve İngiltere'de görülmektedir. Bu ülkelerde gözlenen soygunların sayısının yılda yaklaşık olarak %18 oranında arttığı da rapor edilmektedir. Türkiye'de kredi kartı soygunlarının giderek azaldığı ve azalmanın %70 oranında olduğu görülmektedir. Azalmaya bilgisayarlı kartların kullanılmaya başlanmış olması ve bankaların soygunları sıkı şekilde izlemelerinin neden olduğu söylenebilir.

Kredi kartı ile yapılan soygunların yöntemleri aşağıda sıralanmıştır:

- Fazla kopya çıkarma
- Gerçek kredi kartı bilgisini kullanma
- Kart üzerindeki bilgileri değiştirme

### Fazla Kopya Çıkarma

Karbon kopyalı fiş kullanan ülkelerde görülen bir soygun türüdür. Böyle bir ülkede bir akşam yemeğine gittiğinizi ve yemek sonrası ödemeyi kredi kartı ile yapacağınızı düşünün. Doğal olarak kartınızı garsona vereceksiniz. Garson kartınızı alıp muhasebe bölümüne götürecek ve kopya çıkarma aygıtı ile çıkardığı fişi tabak üzerinde size sunacaktır. Siz fiş üzerine imzanızı atarak ödeme işlemini tamamlamış olacaksınız.

Ülkenizde döndükten sonra kredi kartı döküm bilgileriniz bankadan geldiğinde aynı ya da değişik lokantalarda çok sayıda yemek yediğinizi görüp şaşırabilirsiniz. Bunun nedeni

kartınız kullanılarak çok sayıda fiş üretilmiştir. Her fiş üzerinde imzanız taklit edilerek bankaya gönderilmiştir.

### Gerçek Kredi Kartı Bilgisini Kullanma

Henüz akıllı kredi kartı kullanılmayan ülkelerde sık rastlanan bir soygun türüdür. Kredi kartı ile alışveriş yapılan yerlerde kredi kartının numarası ve güvenlik sayısı (CVC) kopyalanmaktadır. Daha sonra bu bilgiler kullanılarak gerçek ya da sanal Satış Terminali (POS) üzerinden satış yapılmış gibi gösterilmektedir. Bu konuda yaşanmış bir örnek aşağıda anlatılmıştır:

Müzik meraklısı bir kişi belli aralıklarla bir firmadan müzik CD'si almaya başlamıştır. Ödemelerini kredi kartı ile yapmaktadır. Bir süre yurt dışına giden bu müşteri kredi kartı hesap dökümünde CD aldığı yere ilişkin ödeme bilgisi gördüğünde şaşırır ve durumu bankasına iletir. Yapılan incelemede firmanın POS aygıtını kullanarak iki haftada bir aynı miktar satış yaptığı bilgisini girdiği anlaşılmıştır. POS aygıtının ürettiği fişler üzerinde müşterinin imzası olmadığı için firmanın suçu kesinlik kazanmıştır.

Genelağ üzerinden yapılan alışverişlerde gerçek kredi kartlarına ilişkin bilgiler kullanılarak dolandırıcılık yapıldığına tanık olunmaktadır. Örneğin gezi için uçak bileti alanlar izlenmekte ve bu kişiler için yeni uçak biletleri satın alınmaktadır. Bir süre sonra alınan bilet iptal ettirilerek para iadesi istenmektedir.

### Kart Üzerindeki Bilgileri Değiştirme

Kredi kartının manyetik şeridi üstündeki bilgileri değiştirerek yapılan bir soygun yöntemidir. Bu bölümde anlatıldığı gibi kredi kartının ön yüzünde olan bilgiler, POS aygıtları okuyabilsin diye, kartın arka yüzündeki manyetik şeride yazılmıştır. Manyetik şerit üzerindeki bilgileri okuyan ve buraya yeni bilgiler yazabilen aygıtlar, elektronik aygıt satan bazı dükkânlarda satılmaktadır. Kart üzerindeki bilgileri değiştirme yöntemine güzel bir örnek aşağıda anlatılmıştır:

Kendi kredi kartının kullanım sınırı dolmuş bir kişi, kredi kartının parasal üst sınırını yükselttiğini söyleyen bir kişiden kart üst sınırını artırmasını istemiştir. Kartta yapılan değişiklikten sonra bir araç kiralayabilmiştir. Böylece parasal üst sınırın artırılmış olduğuna inanmıştır.

İstanbul'dan Adana'ya doğru nişanlısı ve iki arkadaşı ile birlikte yola çıkan bu kişi kredi kartı ile yolda yakıt almış, bir sorun yaşamamıştır. Daha sonra bir lokantada yemek yemişler ve ödemeyi aynı kartla yapmış, yine bir sorun yaşamamıştır.

Konya'ya vardıklarında bir cep telefonu satıcısından iki cep telefonu satın almış ve bunlardan birini nişanlısına hediye etmiştir. Kredi kartının sorunsuz çalıştığına inanan kişi kısa bir süre sonra başka bir cep telefonu dükkânına gitmiş ve iki tane daha telefon almak istemiştir. Ödemeye sıra gelip kartını satıcıya verdiğinde olay ortaya çıkmıştır.

Satıcı kredi kartını POS aygıtının kart okuyucusuna soktuğunda ekranda "*Bu kredi kartı çalıntıdır. Polise haber verin*" mesajını görmüştür.

Bu yaşanmış örnekten çıkarılacak ders şöyledir:

**İnceleme**

- Kredi kartının kredi üst sınırı ancak kartı veren banka tarafından değiştirilebilir.
- Kredi kartının kredi üst sınırını artırdığını söyleyen kişi aslında, kartın manyetik şeridine kredi kartı bilgilerini bildiği ve kredi üst sınırı yüksek birinin bilgilerini yazmıştır. Örneğimizde bu kişi Münih'te yaşayan bir Alman'dır.

**Değerlendirme**

- Araç kiralama firması kredi kartının ön yüzündeki bilgiler ile POS aygıtının okuduğu bilgileri karşılaştırmayarak önemli bir hata yapmıştır. Ayrıca aracı kiralayandan bir başka kimlik sormamıştır.
- Benzinliklerde kart sahibinin kimliğini araştırma gibi bir alışkanlık olmadığı için yakıt alımında bir sorun ile karşılaşılmamıştır.
- Benzer şekilde lokantalarda da kart sahibinin kimliğini sorgulamak sanki ayıp olur diye yerine getirilmediğinden lokantadaki ödemelerde de bir sorun ile karşılaşılmamıştır.
- İlk cep telefonu satıcısı kimlik denetimi yapmamıştır.
- Birinci telefon alımının ardından kredi kartının manyetik şeridinde kimliği yazılı olan kişi Münih'te kredi kartı ile alışveriş yapmıştır. Kısa bir süre sonra Konya'da aynı kart kullanılmak istendiğinde bankanın sistemi soygunun farkına varmış ve ikinci dükkân sahibini uyarmıştır.

**Sonuç**

- Kart üzerindeki bilgileri değiştirmeyi meslek edinen, bu kartı bir ölçüde bilinçli olarak kullanan kişi suçludur. Araç kiralayıcısı, benzinlik, lokanta ve ilk telefon satıcısı hataları nedeniyle paralarını alamayacaklardır.

- Akılsız kredi kartlarının güvenlik açığı büyüktür.
- Bu kartlar ile yapılan alışverişlerde satıcı mutlaka kartın üzerindeki isim ile kart okuyucunun ürettiği fişteki ismi karşılaştırmalıdır.
- Müşteriden geçerli ve resimli bir kimlik göstermesini istemelidir.

# 6.4 Elektronik Ticaretin Düzenlenmesi Kanunu (6563)

MADDE 1 – (1) Bu Kanun'un amacı, elektronik ticarete ilişkin esas ve usulleri düzenlemektir.

(2) Bu Kanun ticari iletişimi, hizmet sağlayıcı ve aracı hizmet sağlayıcıların sorumluluklarını, elektronik iletişim araçlarıyla yapılan sözleşmeler ile elektronik ticarete ilişkin bilgi verme yükümlülüklerini ve uygulanacak yaptırımları kapsar.

## Tanımlar

MADDE 2 – (1) Bu Kanun'un uygulanmasında;

a) Elektronik ticaret: Fiziki olarak karşı karşıya gelmeksizin elektronik ortamda gerçekleştirilen çevrim içi iktisadi ve ticari her türlü faaliyeti,

b) Ticari iletişim: Alan adları ve elektronik posta adresi dışında, mesleki veya ticari faaliyet kapsamında kazanç sağlamaya yönelik olarak elektronik ticarete ilişkin her türlü iletişimi,

c) Ticari elektronik ileti: Telefon, çağrı merkezleri, faks, otomatik arama makineleri, akıllı ses kaydedici sistemler, elektronik posta, kısa mesaj hizmeti gibi vasıtalar kullanılarak elektronik ortamda gerçekleştirilen ve ticari amaçlarla gönderilen veri, ses ve görüntü içerikli iletileri,

ç) Hizmet sağlayıcı: Elektronik ticaret faaliyetinde bulunan gerçek ya da tüzel kişileri,

d) Aracı hizmet sağlayıcı: Başkalarına ait iktisadi ve ticari faaliyetlerin yapılmasına elektronik ticaret ortamını sağlayan gerçek ve tüzel kişileri,

e) Bakanlık: Gümrük ve Ticaret Bakanlığını,

ifade eder.

## Bilgi verme yükümlülüğü

MADDE 3 – (1) Hizmet sağlayıcı elektronik iletişim araçlarıyla bir sözleşmenin yapılmasından önce;

a) Alıcıların kolayca ulaşabileceği şekilde ve güncel olarak tanıtıcı bilgilerini,

b) Sözleşmenin kurulabilmesi için izlenecek teknik adımlara ilişkin bilgileri,

c) Sözleşme metninin sözleşmenin kurulmasından sonra hizmet sağlayıcı tarafından saklanıp saklanmayacağı ile bu sözleşmeye alıcının daha sonra erişiminin mümkün olup olmayacağı ve bu erişimin ne kadar süreyle sağlanacağına ilişkin bilgileri,

ç) Veri girişindeki hataların açık ve anlaşılır bir şekilde belirlenmesine ve düzeltilmesine ilişkin teknik araçlara ilişkin bilgileri,

d) Uygulanan gizlilik kuralları ve varsa alternatif uyuşmazlık çözüm mekanizmalarına ilişkin bilgileri,

sunar.

(2) Hizmet sağlayıcı varsa mensubu olduğu meslek odası ile meslekle ilgili davranış kurallarını ve bunlara elektronik olarak ne şekilde ulaşılabileceğini belirtir.

(3) Tarafların tüketici olmadığı hâllerde taraflar birinci ve ikinci fıkralardaki düzenlemelerin aksini kararlaştırabilirler.

(4) Hizmet sağlayıcı sözleşme hükümlerinin ve genel işlem şartlarının alıcı tarafından saklanmasına imkân sağlar.

(5) Birinci ve ikinci fıkralar münhasıran elektronik posta yoluyla veya benzeri bireysel iletişim araçlarıyla yapılan sözleşmelere uygulanmaz.

## Sipariş

MADDE 4 – (1) Elektronik iletişim araçlarıyla verilen siparişlerde aşağıdaki esaslar geçerlidir:

a) Hizmet sağlayıcı siparişin onaylanması aşamasında ve ödeme bilgilerinin girilmesinden önce ödeyeceği toplam bedel de dâhil olmak üzere sözleşmenin şartlarının alıcı tarafından açıkça görülmesini sağlar.

b) Hizmet sağlayıcı alıcının siparişini aldığını gecikmeksizin elektronik iletişim araçlarıyla teyit eder.

c) Sipariş ve siparişin alındığının teyidi tarafların söz konusu beyanlara erişiminin mümkün olduğu anda gerçekleşmiş sayılır.

(2) Hizmet sağlayıcı sipariş verilmeden önce alıcıya veri giriş hatalarını belirleyebilmesi ve düzeltebilmesi için uygun, etkili ve erişilebilir teknik araçları sunar.

(3) Tarafların tüketici olmadığı hâllerde taraflar birinci ve ikinci fıkralardaki düzenlemelerin aksini kararlaştırabilirler.

(4) Birinci fıkranın (a) ve (b) bentleri ile ikinci fıkra münhasıran elektronik posta yoluyla veya benzeri bireysel iletişim araçlarıyla yapılan sözleşmelere uygulanmaz.

## Ticari iletişime ilişkin esaslar

MADDE 5 – (1) Ticari iletişimde:

a) Ticari iletişimin ve bu iletişimin adına yapıldığı gerçek ya da tüzel kişinin açıkça belirlenebilir olmasını sağlayan bilgiler sunulmalıdır.

b) İndirim ve hediye gibi promosyonlar ile promosyon amaçlı yarışma veya oyunların bu niteliği açıkça belirlenebilmeli, bunlara katılımın ve bunlardan faydalanmanın şartlarına kolayca ulaşılabilmeli ve bu şartlar açık ve şüpheye yer bırakmayacak şekilde anlaşılır olmalıdır.

### Ticari elektronik ileti gönderme şartı

MADDE 6 – (1) Ticari elektronik iletiler alıcılara ancak önceden onayları alınmak kaydıyla gönderilebilir. Bu onay yazılı olarak veya her türlü elektronik iletişim araçlarıyla alınabilir. Kendisiyle iletişime geçilmesi amacıyla alıcının iletişim bilgilerini vermesi hâlinde temin edilen mal veya hizmetlere ilişkin değişiklik, kullanım ve bakıma yönelik ticari elektronik iletiler için ayrıca onay alınmaz.

(2) Esnaf ve tacirlere önceden onay alınmaksızın ticari elektronik iletiler gönderilebilir.

### Ticari elektronik iletinin içeriği

MADDE 7 – (1) Ticari elektronik iletinin içeriği alıcıdan alınan onaya uygun olmalıdır.

(2) İletide hizmet sağlayıcının tanınmasını sağlayan bilgiler ile haberleşmenin türüne bağlı olarak telefon numarası, faks numarası, kısa mesaj numarası ve elektronik posta adresi gibi erişilebilir durumdaki iletişim bilgileri yer alır.

(3) İletide haberleşmenin türüne bağlı olarak iletinin konusu, amacı ve başkası adına yapılması hâlinde kimin adına yapıldığına ilişkin bilgilere de yer verilir.

### Alıcının ticari elektronik iletiyi reddetme hakkı

MADDE 8 – (1) Alıcılar diledikleri zaman hiçbir gerekçe belirtmeksizin ticari elektronik iletileri almayı reddedebilir.

(2) Hizmet sağlayıcı ret bildiriminin elektronik iletişim araçlarıyla kolay ve ücretsiz olarak iletilmesini sağlamakla ve gönderdiği iletide buna ilişkin gerekli bilgileri sunmakla yükümlüdür.

(3) Talebin ulaşmasını müteakip hizmet sağlayıcı üç iş günü içinde alıcıya elektronik ileti göndermeyi durdurur.

### Aracı hizmet sağlayıcıların yükümlülükleri

MADDE 9 – (1) Aracı hizmet sağlayıcılar hizmet sundukları elektronik ortamı kullanan gerçek ve tüzel kişiler tarafından sağlanan içerikleri kontrol etmek, bu içerik ve içeriğe konu mal veya hizmetle ilgili hukuka aykırı bir faaliyetin ya da durumun söz konusu olup olmadığını araştırmakla yükümlü değildir.

(2) Bu Kanun'un 3, 4, 5, 6, 7 ve 8'inci maddelerinde düzenlenen yükümlülüklerin aracı hizmet sağlayıcılarına uygulanmasına ilişkin usul ve esaslar yönetmelikle belirlenir.

## Kişisel verilerin korunması

MADDE 10 – (1) Hizmet sağlayıcı ve aracı hizmet sağlayıcı:

a) Bu Kanun çerçevesinde yapmış olduğu işlemler nedeniyle elde ettiği kişisel verilerin saklanmasından ve güvenliğinden sorumludur.

b) Kişisel verileri ilgili kişinin onayı olmaksızın üçüncü kişilere iletemez ve başka amaçlarla kullanamaz.

## Bakanlık yetkisi

MADDE 11 – (1) Bakanlık bu Kanun'un uygulanması ve elektronik ticaretin gelişimiyle ilgili her türlü tedbiri almaya ve denetimi yapmaya yetkilidir.

(2) Bakanlıkça görevlendirilen denetim elemanları bu Kanun kapsamında Bakanlık yetkisine giren hususlarla ilgili olarak her türlü bilgi, belge ve defterleri istemeye, bunları incelemeye ve örneklerini almaya, ilgililerden yazılı ve sözlü bilgi almaya yetkili olup ilgililer istenilen bilgi, belge ve defterler ile elektronik kayıtlarını, bunların örneklerini noksansız ve gerçeğe uygun olarak vermek, yazılı ve sözlü bilgi taleplerini karşılamak ve her türlü yardım ve kolaylığı göstermekle yükümlüdür.

## Cezai hükümler

MADDE 12 – (1) Bu Kanun'un;

a) 3'üncü maddesindeki yükümlülüklere, 4'üncü maddesinin birinci fıkrasının (a) bendindeki yükümlülüklere, 6'ncı maddesinin birinci fıkrasına veya 7'nci maddesinin birinci fıkrasına aykırı hareket eden hizmet sağlayıcılara ve aracı hizmet sağlayıcılara bin Türk lirasından beş bin Türk lirasına kadar,

b) 4'üncü maddesinin birinci fıkrasının (b) bendindeki veya aynı maddenin ikinci fıkrasındaki, 5'inci maddesinin birinci fıkrasının (a) bendindeki veya 7'nci maddesinin ikinci ve üçüncü fıkralarındaki yükümlülüklere aykırı hareket eden hizmet sağlayıcılara ve aracı hizmet sağlayıcılara bin Türk lirasından on bin Türk lirasına kadar,

c) 5'inci maddesinin birinci fıkrasının (b) bendindeki, 8'inci maddesinin ikinci ve üçüncü fıkralarındaki yükümlülüklere aykırı hareket eden hizmet sağlayıcılara ve aracı hizmet sağlayıcılara iki bin Türk lirasından on beş bin Türk lirasına kadar,

ç) 11'inci maddesinin ikinci fıkrasına aykırı hareket edenlere iki bin Türk lirasından beş bin Türk lirasına kadar,

idari para cezası verilir.

(2) Bir defada birden fazla kimseye 6'ncı maddenin birinci fıkrasına aykırı olarak ileti gönderilmesi hâlinde birinci fıkranın (a) bendinde öngörülen idari para cezası on katına kadar artırılarak uygulanır.

(3) Bu maddede öngörülen idari para cezalarını verme yetkisi Bakanlığa aittir. Bu yetki merkezde Bakanlığın ilgili genel müdürlüğüne, taşrada ise Bakanlığın il müdürlüklerine devredilebilir.

### Yönetmelikler

MADDE 13 – (1) Bu Kanun'un uygulanmasına ilişkin yönetmelikler Adalet Bakanlığı, Maliye Bakanlığı, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı ve Ekonomi Bakanlığı ile Bilgi Teknolojileri ve İletişim Kurumunun görüşleri alınarak Bakanlık tarafından hazırlanır.

### Değiştirilen mevzuat

MADDE 14 – (1) 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu'nun 50'nci maddesinin beşinci fıkrası aşağıdaki şekilde değiştirilmiş, maddeye aşağıdaki fıkralar eklenmiş ve diğer fıkralar buna göre teselsül ettirilmiştir.

"(5) İşletmeciler tarafından sundukları hizmetlere ilişkin olarak abone ve kullanıcılarla önceden izinleri alınmaksızın otomatik arama makineleri, fakslar, elektronik posta, kısa mesaj gibi elektronik haberleşme vasıtalarının kullanılması suretiyle pazarlama veya cinsel içerik iletimi gibi maksatlarla haberleşme yapılamaz. İşletmeciler sundukları hizmetlere ilişkin olarak abone ve kullanıcılarıyla siyasi propaganda içerikli haberleşme yapamazlar."

"(6) İşletmeciler tarafından abone ve kullanıcıların iletişim bilgilerinin bir mal ya da hizmetin sağlanması sırasında, bu tür haberleşmenin yapılacağına dair bilgilendirilerek ve reddetme imkânı sağlanarak edinilmiş olması hâlinde abone ve kullanıcılarla önceden izin alınmaksızın aynı veya benzer mal ya da hizmetlerle ilgili pazarlama, tanıtım, değişiklik ve bakım hizmetleri için haberleşme yapılabilir.

(7) Abone ve kullanıcılara bu tür haberleşme yapılmasını reddetme ve verdikleri izni geri alma hakkı kolay ve ücretsiz bir şekilde sağlanır."

### Onay alınarak oluşturulan veri tabanları

GEÇİCİ MADDE 1 – (1) Bu Kanun'un yürürlüğe girdiği tarihten önce ticari elektronik ileti gönderilmesi amacıyla onay alınarak oluşturulmuş olan veri tabanları hakkında 6 ncı maddenin birinci fıkrası uygulanmaz.

### Yürürlük

MADDE 15 – (1) Bu Kanun 1/5/2015 tarihinde yürürlüğe girer.

## 6.5 Elektronik İmza Kanunu (5070)

Genelağ üzerinden gerçekleştirilen ticaretin yaygınlaşmasının sonucu olarak Elektronik İmza yasası 12.01.2004'te kabul edilmiştir. Yasanın ana hatları aşağıda sunulmuştur.

### Amaç

MADDE 1.- Bu Kanun'un amacı elektronik imzanın hukuki ve teknik yönleri ile kullanımına ilişkin esasları düzenlemektir.

### Kapsam

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

### Tanımlar

MADDE 3.- Bu Kanun'da geçen;:

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

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

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

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

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

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

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

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

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

ifade eder.

## İKİNCİ KISIM

## Güvenli Elektronik İmza ve Sertifika Hizmetleri

## BİRİNCİ BÖLÜM

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

### Güvenli elektronik imza

MADDE 4.- Güvenli elektronik imza;:

a) Münhasıran imza sahibine bağlı olan,

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

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

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

elektronik imzadır.

### Güvenli elektronik imzanın hukuki sonucu ve uygulama alanı

MADDE 5.- Güvenli elektronik imza, elle atılan imza ile aynı hukuki sonucu doğurur. Kanunların resmî şekle veya özel bir merasime tabi tuttuğu hukuki işlemler ile teminat sözleşmeleri güvenli elektronik imza ile gerçekleştirilemez.

### Güvenli elektronik imza oluşturma araçları

MADDE 6.- Güvenli elektronik imza oluşturma araçları;:

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

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

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

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

sağlayan imza oluşturma araçlarıdır.

### Güvenli elektronik imza doğrulama araçları

MADDE 7.- Güvenli elektronik imza doğrulama araçları;:

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

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

c) Gerektiğinde imzalanmış verinin güvenilir bir biçimde gösterilmesini sağlayan,

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

e) İmza sahibinin kimliğini değiştirmeksizin doğrulama yapan kişiye gösteren,

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

İmza doğrulama araçlarıdır.

## İKİNCİ BÖLÜM

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

### Elektronik sertifika hizmet sağlayıcısı

MADDE 8.- Elektronik sertifika hizmet sağlayıcısı elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişilerdir. Elektronik sertifika hizmet sağlayıcısı Kuruma yapacağı bildirimden iki ay sonra faaliyete geçer.

Elektronik sertifika hizmet sağlayıcısı yapacağı bildirimde;:

a) Güvenli ürün ve sistemleri kullanmak,

b) Hizmeti güvenilir bir biçimde yürütmek,

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

İle ilgili şartları sağladığını ayrıntılı bir biçimde gösterir.

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

Elektronik sertifika hizmet sağlayıcılarının faaliyetlerinin devamı sırasında bu maddede gösterilen şartları kaybetmeleri hâlinde de yukarıdaki fıkra hükümleri uygulanır. Elektronik sertifika hizmet sağlayıcıları Kurumun belirleyeceği ücret alt ve üst sınırlarına uymak zorundadır.

### Nitelikli elektronik sertifika

MADDE 9.- Nitelikli elektronik sertifikada;:

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

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

c) İmza sahibinin teşhis edilebileceği kimlik bilgilerinin,

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

e) Sertifikanın geçerlilik süresinin başlangıç ve bitiş tarihlerinin,

f) Sertifikanın seri numarasının,

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

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

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

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

bulunması zorunludur.

### Elektronik sertifika hizmet sağlayıcısının yükümlülükleri

MADDE 10.- Elektronik sertifika hizmet sağlayıcısı:

a) Hizmetin gerektirdiği nitelikte personel istihdam etmekle,

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

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

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

e) Sertifikanın kullanımına ilişkin özelliklerin ve uyuşmazlıkların çözüm yolları ile ilgili şartların ve kanunlarda öngörülen sınırlamalar saklı kalmak üzere güvenli elektronik imzanın elle atılan imza ile eş değer olduğu hakkında sertifika talep eden kişiyi sertifikanın tesliminden önce yazılı olarak bilgilendirmekle,

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

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

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

yükümlüdür.

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

## Nitelikli elektronik sertifikaların iptal edilmesi

MADDE 11.- Elektronik sertifika hizmet sağlayıcısı;:

a) Nitelikli elektronik sertifika sahibinin talebi,

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

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

durumunda vermiş olduğu nitelikli elektronik sertifikaları derhâl iptal eder.

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

Elektronik sertifika hizmet sağlayıcısı faaliyetine son vermesi ve vermiş olduğu nitelikli elektronik sertifikaların başka bir elektronik sertifika hizmet sağlayıcısı tarafından kullanımının sağlanamaması durumunda vermiş olduğu nitelikli elektronik sertifikaları derhâl iptal eder.

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

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

## Bilgilerin korunması

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

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

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

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

## Hukuki sorumluluk

MADDE 13.- Elektronik sertifika hizmet sağlayıcısının elektronik sertifika sahibine karşı sorumluluğu genel hükümlere tabidir.

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

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

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

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

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

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

## Yabancı elektronik sertifikalar

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

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

## Kaynaklar ve Okunması Önerilen Yayınlar:

[1] H. Acun, *Anadolu Selçuklu Dönemi Kervansarayları*, T.C. Kültür ve Turizm Bakanlığı.

[2] E. Adalı, *Bilgisayar ve Bilgi Güvenliği ve Yönetim*i, İTÜ, 2016

[3]K. C. Laudon, C. G.," *Traver, E-commerce*, Addison Wesley, 2001