İSTANBUL TİCARET ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

DAĞITIM VE ULAŞTIRMA SÜREÇLERİNDE ELEKTRONİK İMZA

Mehmet ÇIKRIKCI

FBE Endüstri Mühendisliği Anabilim Dalından Hazırlanan

YÜKSEK LİSANS TEZİ

Tez Danışmanı: Prof. Dr. Eralp ÖZİL

İSTANBUL,2007

İSTANBUL TİCARET ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

DAĞITIM VE ULAŞTIRMA SÜREÇLERİNDE ELEKTRONİK İMZA

Mehmet ÇIKRIKCI

FBE Endüstri Mühendisliği Anabilim Dalından Hazırlanan

YÜKSEK LİSANS TEZİ

Danışmanı Üye: Prof. Dr. Eralp ÖZİL

İSTANBUL,2007

Hazırlamış olduğum tez özgün bir çalışma olup YÖK ve İTİCU Lisansüstü Yönetmeliklerine uygun olarak hazırlanmıştır. Ayrıca, bu çalışmayı yaparken bilimsel etik kurallarına tamamıyla uyduğumu; yararlandığım tüm kaynakları gösterdiğimi ve hiç bir kaynaktan yaptığım ayrıntılı alıntı olmadığını beyan ederim. Bu tezin ihtiva ettiği tüm hususlar şahsi görüşüm olup; Türk Silahlı Kuvvetlerinin ve İstanbul Ticaret Üniversitesinin resmi görüşlerini yansıtmamaktadır.

Mehmet ÇIKRIKCI

KISALTMA LİSTESİ

SPK	Serbest Piyasalar Kurulu
İMKB	İstanbul Menkul Kıymetler Borsası
KAP	Kamu Aydınlatma Platformu
EİK	Elektronik İmza Kanunu
e-imza	Elektronik İmza
e-devlet	Elektronik Devlet
e-ticaret	Elektronik Ticaret

ŞEKİL LİSTESİ

TABLO LİSTESİ

ÖNSÖZ

Yıllardır gelişmekte olan teknoloji insanları kendisine çekmeyi başarma yolunda büyük yollar kat etmiştir. Teknolojinin kullanımı, bir program ya da basit bir eşyanın kullanımı değil bir hayat tarzının belirlenmesi demek olmuştur. Yine bu kapsamda Maslov'un İhtiyaçlar Hiyerarşisine baktığımızda varolma ya da fiziksel ihtiyaçların arkasını güvenlik takip etmektedir. Bu güvenlik ihtiyacı bütün gerçek dünyada olduğu gibi sanal dünya olan teknolojik ortamda da gereken yerini almıştır. Çünkü kullanıcıları gerçek yaşamda nasıl zarara uğramak istemezlerse teknolojik ortamda da zarara uğramak istemezler. Bunun engellenememesi durumunda ortama girmeyen kullanıcılar yaşam dışına çıkmış olurlar.

Bütün dünyanın kabul ettiği bir sistem tarafından korunmak bir güvendir. Hele işinizde çok büyük miktarlarda mali durumlar dönüyorsa daha da önem kazanmaktadır. İşte bütün bunların çözüm yolu yıllardır filmlere konu olan dijital kart veya elektronik imza yöntemidir. Dağıtım ve ulaştırma süreçlerinde elektronik imza ise kullanıcıya bu güvenlik ihtiyacını sağlamaktadır.

Bu tez kapsamında elektronik imzanın kavramaları, nitelik ve nicelikleri, elektronik belge kavramı, elektronik imzanın Dünya ve Türkiye'deki uygulamaları ve yaşama olan etkileri ele alınmıştır. Bu sayede "Elektronik imza daha etkin nasıl kullanılır" sorusunun cevabına da yaklaşmış olundu. Çünkü elektronik imza kullanıcılara bir çok fayda sağlayan konumda olması nedeniyle çabuk geliştirilen ve sürekli konuma sahip bir sistem durumuna geldi.

Dağıtım ve Ulaştırma Süreçlerinde Elektronik İmza konulu tezimin hazırlanması sürecinde tecrübelerini benden esirgemeyen tez danışmanım Prof. Dr. Eralp ÖZİL'e, yine bilgilerini ve değerli zamanını benimle paylaşan Dr. Alper ÖZPINAR'a, her zaman yanımda olan eşim, ailem ve tüm dostlarıma sonsuz teşekkürlerimi sunarım.

Mehmet ÇIKRIKCI

Kasım 2007

ÖZET

Elektronik imza dünya çapında yaygınlaşan bir sistemdir. Kullanımı kolaylaştıkça yayılacak bir kapasiteye sahiptir. Kullanımı güvenlik ve doğrulama gibi işlemleri tanımlar. Ayrıca zaman olgusunu da taşır. Belgelerin iletimi esnasında kullanıcılara gizli olarak iletişim imkanı verir. Bu kadar öneme sahip bir sistem artık kanunlarla tanımlanmaktadır. 5070 Sayılı Elektronik İmza Kanunu çerçevesine dağıtım ve ulaştırmada elektronik imzanın kullanımı incelenmiştir. Güvenliği ve güvenirliliği, doğrulama sıhhati, zaman olgusu ve gizliliği elektronik imzanın değerini artırmaktadır. Bu konu içerisinde elektronik imza ile ilgili kavramlar ele alınmaktadır. Konunun daha iyi anlaşılması için gerekli kavramlar incelendikten sonra elektronik imzanın etkileri ele alınmaktadır. Daha sonra elektronik imzanın alabileceği tehditler değerledirilmektedir. Ele alınan konular arasında elektronik imzanın gelişimi de yer almaktadır. Ülkemizde ve dünyada elektronik imzanın kullanım alanları incelenmekte ve bu alanların işleyişleri hakkında bilgi verilmektedir. Elektronik imza kavramının yanısıra yine bu tez içerisinde elektronik belgelerin standartları hakkında da bilgi verilmektedir. Elektronik belgelerin taşıdığı nitelikler ve elektronik imzanın nasıl kullanıldığı konusuna da değinilmektedir. Elektronik imzanın nasıl yaygınlaştığı ise bir başka başlıktır. Şu anda kullanımda olan ülkelerin uygulamaları örnek olarak incelenmiştir. En son ise günlük hayat üzerine yaptığı etkiler incelenerek tez tamamlanmıştır.

Anahtar Kelimeler: Elektronik imza, Elektronik belge, Elektronik belgerin güvenlik

ABSTRACT

Digital signature is a system which becomes widespread in world. It has a structure for spreading while easy using. It definites security and verification. And also it carries timing. Users can communicate with high security. These important systems protect with some rules. Ditribution and communication with digital signature studying about Elektronic Signiture Law Number: 5070. Digital Signature has importancy with security, verification, timing information and privacy. Concepts of digital signature discuss under this subject. There is a discussion about threats against digital signature. And also this thesis studying about evolution of digital signature. After these parts digital signature analyzed at home and at world. And also there is some information about standard of electironic documents with digital signature. Some subjects replay like "How is the usage of digital signature?" and "What is qualities about digital signature". And also there is a subject about spreading of digital signature. Then there is a discussion about some digital signature, which is using by some country. At the end thesis is over with focusing on the effect of digital signature.

Keywords: Electronic signature, Electronic document, Security of electronic documents

1 GİRİŞ

İnsanlar, hayatlarında her zaman riskin en az olacağı, olumsuz ihtimallerin minimum seviyede tutulacağı bir ortamda yaşamak için çaba sarf ederler. Eskiden denizlerde korsanlar ticaret yapmak veya seyahat etmek isteyen gemilerin yolunu keserek onları bir şekilde zarara uğratırlardı. Günümüzde ise yine aynı isimle anılan grup daha büyük bir deniz olan dijital dünyada insanları zarara uğratmaya devam etmektedir. Bu büyük denizde yapılan faaliyetlerin güvenlik altına alınarak risklerin minimuma indirilmesi çalışmaları da korsanların faaliyetleri ölçüsünde devam etmektedir. Bu karşılıklı oluşum bir silah – karşı silah anlayışı içinde devam etmektedir.

Yıllardır bilgi ve belge ulaşımındaki güvenlik açısından olan eksiklikler askerler, filolar veya güvenlikli kutular sayesinde kapatılmaya çalışılmaktaydı. Yığınla kağıtlara yazılarak iki taraf arasında karşılıklı imza atılmasıyla varılan ve yukarıdaki gibi ulaşımları sağlanan anlaşmalar güncel ihtiyaçlar nedeniyle artık yerini yavaş yavaş dijital ortamda yapılan anlaşmalara bırakmaya başladı. Çünkü hızla büyüyen dünyanın iki ucu arasındaki mesafe ticari ve iletişimsel anlamda kısalmış; gerçek mesafe olarak ise ulaşım yönünden teknoloji ne kadar gelişse de henüz yeterli kısalığa ulaşamamıştır. Bu durumda iki tarafın da zaman olgusunu kar hesaplamasında aktif bir çarpan olduğunu kabul ettiği için dijital ortamın kullanılması zorunluluğu doğmaktadır. Dijital ortamda yapılan bu bilgi ve belge alışverişlerinin güvenli bir ortamda yapılabilmesi için bir güvenlik filosu oluşturmak gerekmektedir. Bu işlemin ise dijital ortamda faaliyet göstermesi için bir takım güvenlik sistemlerinin kullanılması gerekmektedir. İşte tam burada elektronik imza, güvenlik ihtiyacını belirli oranda karşılayan sistem görevini üstlenmektedir. Bu görev, belge veya bilgilerin bütünlüğünün, gizliliğinin, kaynağının, adresinin, güvenirliliğinin ve güvenliğinin korunması olarak karşımıza çıkmaktadır. Bu görevleri ile "Dağıtım ve Ulaştırma Süreçlerinde Elektronik İmza"nın günümüz koşullarında ne kadar güvenilir olduğu büyük bir soru işareti olarak akıllarda yerini korumaktadır.

2 DAĞITIM VE ULAŞTIRMA SÜREÇLERİNDE ELEKTRONİK İMZA

2.1 Elektronik Veri Tanımı

5070 sayılı Elektronik İmza Kanunu çerçevesinde elektronik veri "Elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıtlar" olarak tanımlanmaktadır. Elektronik verinin tanımı pek çok yabancı devletin elektronik imza ile ilgili kanun veya direktiflerinde yer almamıştır. Sadece İrlanda ve Litvanya'da bu tanıma benzer bir elektronik veri tanımı yapılmış ancak daha kapsamlı olarak ele alınmıştır. (Keser, 2004)

2.2 Elektronik İmza Kavramı

Kanunda elektronik imza "Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri" olarak tanımlanmaktadır. Burada elektronik imzaya bir elektronik verinin iletişimdeki kişilerin kimlik bilgilerini de içeren başka bir elektronik veriye kişiler arasında iletilecek olan bilgilerin kimler arasında iletildiği ve bütünlüğünün bozulmadığının doğrulanması gibi işlevleri üstlendiren bir rol yüklenmektedir. Bu kapsamda değişik tanımları yapılan elektronik imzanın sadece sayısal veya yazısal bir veri olmaktan çıkarılıp farklı formatları da içerdiğinin kabul edilmesi gerekmektedir. Yani aslında elektronik imza, bir kişinin elle atmış olduğu imzanın taranarak gönderilen belgeye eklenmesi veya fotoğraf olarak yapıştırılmasından göz retinası, parmak izi ya da ses gibi biyolojik özelliklerinin kaydedilerek kullanıldığı biyometrik yöntemleri de içeren geniş bir yelpazede ele alınması gereken kavramları da içermektedir.

2.3 Elektronik İmza Sahibi veya Kullanıcısı

Kanunda imza sahibi veya kullanıcısı "Elektronik imza oluşturmak amacıyla bir imza oluşturma aracını kullanan gerçek kişi" olarak tanımlanmıştır. İmza sahibinin gerçek kişi olabileceği gibi sertifikalarda açıklıkla belirtilmesi durumunda, tüzel kişiler adına da gerçek kişiler elektronik imza yaratabilir ve elektronik sertifikaya sahip olabilirler.

2.4 Elektronik İmzanın Oluşturulması

Elektronik imzanın oluşturulması Kanun'da; "İmza sahibine ait olan, imza sahibi tarafından elektronik imza oluşturma amacıyla kullanılan ve bir eşi daha olmayan şifreler, kriptografik gizli anahtarlar gibi veriler" şeklinde tanımlanmıştır. Bu tanım uygulamada "private key" olarak bilinen özel veya kapalı anahtarı belirtmektedir. İmza oluşturma verisi hem hizmet sağlayıcı tarafından hem de sertifika sahibi tarafından oluşturulabilmektedir.

2.5 Elektronik İmzanın Doğrulanması

Elektronik imzanın doğrulanması tanımı Kanun'a göre "Elektronik imzayı doğrulamak için kullanılan şifreler, kriptografik açık anahtarlar gibi veriler" şeklindedir. Bu tanım uygulamada "public key" olarak bilinen açık anahtarı belirtmektedir.

2.6 Elektronik İmza Oluşturma Aracı

Elektronik imza oluşturma aracı Kanun'da; "Elektronik imza oluşturmak üzere, imza oluşturma verisini kullanan yazılım veya donanım aracı" şeklinde yerini almaktadır. Bu araçlarının bazıları akıllı kartlar, USB'ler, bilgisayarlar veya veri işleme kapasitesi olan el terminalleri, bilgisayar programları, işletim sistemleri veya özel yazılımlar şeklinde listelenebilir.

2.7 Elektronik İmza Doğrulama Aracı

İmza doğruluma aracının tanımı Kanun'a göre "Elektronik imzayı doğrulamak amacıyla imza doğrulama verisini kullanan yazılım veya donanım aracı" şeklindedir. İmza oluşturma araçları aynı zamanda imza doğrulama araçları olarak da kullanılacağından dolayı burada istisnai olarak sadece imza doğrulama aracı olarak kullanılacak olan donanım veya yazılım bazlı araçların değerlendirilmesi gerekir.

2.8 Elektronik İmzada Zaman Kavramı

Kanun'a göre elektronik imzanın taşıdığı zaman kavramı "Bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı veya kaydedildiği zamanın tespit edilmesi amacıyla, elektronik sertifika hizmet sağlayıcısı tarafından elektronik imzayla doğrulanan kayıt"tır.

2.9 Elektronik İmzanın Kullanımı

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

Elektronik imzaların sağladığı başlıca önemli işlevleri şöyledir:

- İmzalayanın tanımlanması

- Veri bütünlüğünün kontrol edilmesi

- Gizliliğin korunduğunun teyidi

- İnkar etmenin engellenmesi

2.9.1 İmzalayanın Tanımlanması

Bir belgeyi gönderen veya alan ve altında imzası bulunan kişinin kimliğinin doğrulanmasıdır. Veriyi imzalayan kişinin o imzayı kullanmaya yetkinliğini garanti ederek işleme kimin dahil olduğu ya da mesajın kimden geldiği bilgilerini taşır. Tanımlama işleminin doğru ve güvenilir olarak yapılabilmesi için sayısal sertifika sağlayıcısının tarafsız ve güvenilir olması gerekir.

2.9.2 Veri Bütünlüğünün Kontrol Edilmesi

Sayısal imzalar verinin bütünlüğünü koruyarak okuduğunuz mesajın, kazayla veya kötü niyetle size gelene kadar değişmediğini veya değiştirilmediğini garanti eder. Bu garantinin verile bilmesi için sayısal olarak imzalanan dokümanın hash denilen küçük bir özeti tutulur. Bu özet sayesinde veride yapılan herhangi bir değişiklik iletim anında ortaya çıkar.

2.9.3 Gizliliğin Korunduğunun Teyidi

Verinin gizliliği, alıcının anahtarının mesajın şifresini çözmesi sayesinde gerçekleştirilir. Eğer mesaj şifrelendiyse alıcıda bulunan ve eşsiz olan anahtar olmadan mesajın içeriğinin açılması imkansızdır. Bu sayede elindeki anahtarıyla şifreleme işlemini bitiren ve mesajı gönderen imza sahibinin alıcıyı belirlemesi gizliliğin sağlanması aşamasının birinci adımdır.

2.9.4 İnkar Etmenin Engellenmesi

Sayısal imza aynı zamanda mesajı imzalayanın kimliği hakkında gerekli ve yeterli bilgileri de taşır. İnkar edilememe özelliği, alışverişin devamı esnasında işleme veya iletişime kimlerin katıldığının kanıtlanmasına da imkan verir. Bir dokümanı imzalayan veya o dokümanı alan kişi daha sonra söz konusu işlemleri yapmadığını inkar edemez. Basit olarak inkar edememe bilginin reddedilememesi anlamına gelmektedir.

2.10 Sayısal İmza

Sayısal imza, mesaj özetleme fonksiyonu ve asimetrik şifreleme sistemi yardımıyla bir veri mesajının dönüştürülmesinden teşekkül edilen bir tür elektronik imzadır. Bir diğer tanımıyla sayısal imza veri mesajına eklenen sayısal değerdir. İmzacının gizli şifreleme anahtarına bağlı matematiksel yöntemle elde edilen bu değer yalnızca imzacı tarafından üretilebilmektedir. Bu matematiksel yöntem, bir veri mesajına uygulandığında mesajı dönüştürmekte ve mesajı alan taraf imzacının açık anahtarını bildiğinden, dönüşümün imzacının açık anahtarına karşılık gelen gizli anahtarıyla gerçekleştirilip gerçekleştirilmediği ve dönüşümden sonra orijinal mesajın değişip değişmediği hususunun kusursuz olarak tespit edilmesi imkanını alıcıya yani kullanıcılara sunmaktadır.

Bu sayede alıcı gelen mesajın sahte olup olmadığı, bütünlüğünün bozulup bozulmadığı konusunda güvenilir bir dayanağa sahip olacaktır. Yani sayısal imzanın asıl amacı bir bilgi veya belgenin iletişim esnasında sahteleşip sahteleşmediğini kodlamalar yardımı ile belirleyerek iki tarafında güvenliği açısından yeterli bilgileri barındırmaktır. Bu iletişimin güvenirliliğinin temel dayanağını oluşturmaktadır.

2.11 Elektronik İmzanın Oluşturulmasının Teknik Temelleri

Elektronik imza bu kadar görevi üstlenmesi açısından güvenli bir sisteme oturtulması ve işletiminin yeterli sağlamlıkta bir temele dayandırılması gerekmektedir. Bu gereksinim teknik olarak açık bırakmayacak şekilde ve yeterli güvenirliliği sağlayacak biçimde olması zorunluluğunu doğurmaktadır.

2.11.1 Elektronik İmza Güvenlik Mekanizmaları

Güvenlik hizmetleri elektronik imzanın güvenirliliği çerçevesinde yukarıda listelenmiş olan dört temel hususun sağlanması amacıyla oluşturulmuş mekanizmalardır. Bu dört temel husus;

- İmzalayanın tanımlanması

- Veri bütünlüğünün kontrol edilmesi

- Gizliliğin korunduğunun teyidi

- İnkar etmenin engellenmesi

2.11.2 Şifrelemeye Dayalı Olmayan Güvenlik Sistemleri

Şifrelemeye dayalı olmayan güvenlik sistemleri bir mesajın iletimi esnasında kullanılan basit, aşılabilir, kolayca taklit edilebilir ya da maliyeti açısından uygulanması zor olan sistemlerdir. Bu sistemlerden bazıları;

- Sayısallaştırılmış imzanın kullanımı
- Kişiye özel kullanıcı adları ve parola sistemleri
- Biyometrik verileri kullanarak tanımlama yöntemidir.

Bu güvenlik sistemleri kullanımı açısından fazla güvenilir olmayıp çok yaygın olarak da kullanılmamaktadır.

2.11.2.1 Sayısallaştırılmış İmzanın Kullanımı

Sayısallaştırılmış imza elle atılan imzanın taranarak veya fotoğraflanarak belgeye eklenmesi veya yapıştırılması yolu ile elde edilen bir imza çeşididir. Bu imza yöntemi kolayca taklit edilebileceği gibi içeriğin değiştirilmesine mani olma durumu da mevcut değildir. En az kullanılan yöntemlerden olan sayısallaştırılmış imza iki kişi arasındaki iletişimin doğruluğunu da ispat yetisine sahip değildir. İki tarafın iletişim halinde bulunduğu hatta üçüncü bir kişi tarafından kolayca okunabilir ve değiştirilebilir içeriğe sahip mesaj durumuna gelen belgenin imza sahibi tarafından gönderilmesinin ispatı da mümkün değildir. Böylece sağlanması gereken dört temel ilkenin hiçbirisinin sağlanmadığı ortaya çıkmaktadır.

2.11.2.2 Kişiye Özel Kullanıcı Adları ve Parola Sistemleri

Daha çok basit internet ortamlarında kullanılan ve herkes tarafından güvenirliliğinin olmadığı kabul edilen bir sistemdir. Kullanıcı adı ve parola sistemi, yönetici statüsüne sahip bir tarafça verilen kullanıcı adı ve kullanıcı tarafından değiştirilebilen ancak yönetici tarafından ulaşılabilir özelliğe sahip parolalar yöntemi ile oluşturulur. Bu yöntemde gönderilen mesaj tarafsızlığı ve güvenirliliği belirli olmayan yönetici tarafından değiştirilebileceği gibi yönetici rolünün bir dördüncü kişi tarafından üstlenilmesi veya gerekli bilgilere sahip olunması/çalınması yoluyla da aynı olay gerçekleştirilebilir. Bu yöntem sadece gönderen ve alan arasında sadece kimlik tespitinin yapılmasına yardımcı olmaktadır. Hatta kullanıcı adı bilinen parola yardımı ile kullanılarak üçüncü veya dördüncü tarafça gönderilmemiş olan bir verinin gönderilmesi sağlanabilir. Böylece bu durumda kullanıcı adı yöntemi de yeterli güvenirlilik görevini yerine getirememiş olmaktadır.

2.11.2.3 Biyometrik Verileri Kullanarak Tanımlama Yöntemi

Diğer iki yönteme göre daha güvenli olan biyometrik verileri kullanarak tanımlama yöntemi, imza sahibinin diğer kişilerden farklı fiziksel özelliklerinin kullanılması yoluyla imzanın oluşturulması yöntemini esas almaktadır. En basit akla gelen parmak izinden başlayıp göz retinası taramaya, ses algılamasına, vücut sıcaklığı tanımlamasına kadar varan biyometrik yelpazeyi kapsamakta olan yöntem, taramalar ve tanımlama cihazlarının ekonomik değerleri nedeniyle çok az kullanım alanına sahiptir.(İnalöz,2003)

2.11.3 Şifrelemeye Dayalı Olan Güvenlik Sistemleri

Şifrelemeye dayalı olmayan güvenlik sistemlerinin kullanım kısıtlılığı ve güvenirliliğinin az olması nedeniyle iletişimde daha güvenilir bir sistem bulma çabası artmış ve şifrelemeye dayalı güvenlik sistemleri ortaya çıkmaya başlamıştır. Şifreleme yoluyla mesajların anlamsız birer özetinin veya şifreli bütünün yollanması yolu ile elde edilen yöntemler daha çok kabul görmüş ve yaygınlığı o derece artmıştır. Şifrelemeye dayalı olan güvenlik sistemlerinden bazıları;

- Simetrik şifreli anahtarların kullanımı
- Asimetrik şifreli anahtarların kullanımı

- Özet alma ve şifreleme yöntemi olarak sıralanabilir.

Bu yöntemler ele alınırken şifrelemeyi yapan tarafın güvenirliliğinin her iki tarafça da kabul edilmesi gerekmektedir. Aksi halde güvenilir olmayan bir şifreleme de aslında şifrelemeye dayalı olmayan güvenlik sitemlerinden çok farklı bir içeriğe sahip olamaz. Çünkü yukarıda da bahsedilen dört temel hususun hiçbirisinin sağlanması düşünülemez. Bu temel hususların sağlanmadığı bir iletişim ise güvenilir ve istenilen bir iletişim olamaz. (İnalöz,2003)

2.11.3.1 Simetrik Şifreli Anahtarların Kullanımı

Simetrik anahtar şifrelemesinde iletişim halindeki iki taraf arasında aynı kod algoritmasına sahip sistemlerin bulunması gerekmektedir. Bu sistemler içerisinde algoritmaların yüklü olduğu bir anahtar çifti şeklinde uygulanabilir. Bu sayede imza sahibinin kodladığı mesaj alıcı tarafından bütünlüğü bozulmadan, gizlilik içinde, gönderenin kimliği tanımlanmış ve inkar edilemez bir şekilde alınır. Burada istisna sadece üçüncü tarafın şifreyi ele geçirmesi veya çözmesi yolu ile ulaşmasıdır. Bu durumu şifresiz iletişimle aynı kategoride değerlendirmek gerekmektedir. (İnalöz,2003)

2.11.3.2 Asimetrik Şifreli Anahtarların Kullanımı

Asimetrik şifreli anahtarların kullanımı, birisi açık diğeri gizli iki ayrı anahtarın kullanımı esasına dayanmaktadır. Her kullanıcıda bir adet açık ve bir adet de gizli anahtar bulunmaktadır. Mesajı gönderen kişi, açık anahtar ile göndermek istediği mesajı göndereceği kişinin gizli anahtarına göre şifreler. Bu sırada şifrelenen mesaj artık gizli bir içeriğe sahip, gönderen kişinin kimliğini taşıyan, veri bütünlüğü korunmuş ve zaman bilgisine sahip bir şekilde adresine ulaşacak nitelik kazanmıştır. Bu mesajı ancak alıcının elindeki gizli anahtar çözebilecek şifreye sahiptir. Üçüncü bir kişi açık anahtara sahip olsa bile şifrelenmiş olan mesajın gizli anahtarını elinde bulundurmadığı için mesaja erişim yapamaz. Dolayısı ile daha güvenilir bir yol çizilmiş olur. Bu yöntem diğer yöntemlere göre daha güvenli olmasına rağmen algoritmaların oluşturulması ve gizliliğinin korunması aşamasında bazı durumlar ortaya çıkabilir. Bu yolla elde edilmiş ve kullanılmakta olan elektronik imzanın gizliliğinin korunması için bazı temel maddelerin oluşmasına ihtiyaç vardır. Oluşması gereken maddelerden bazıları;

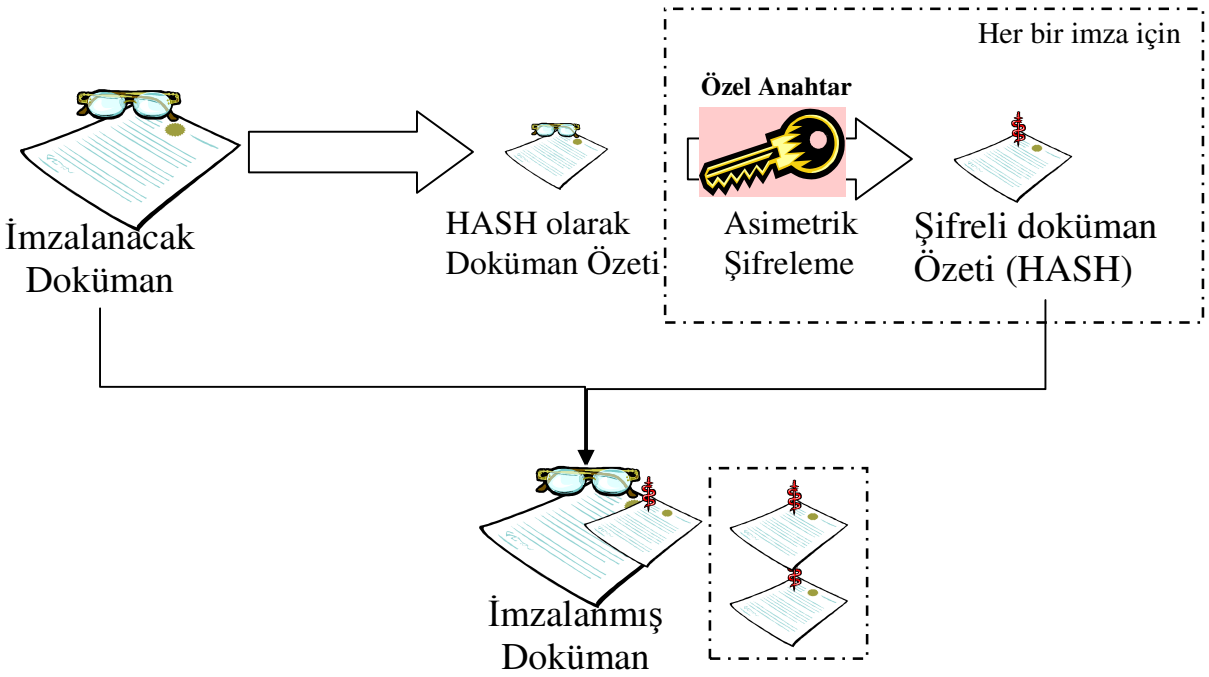
- Algoritmaların ve sayısal imzanın üretimiyle ilgili parametrelerin gizliliğinin korunması

- Anahtar çiftinin benzersizliği ve bilgilerinin gizliliği

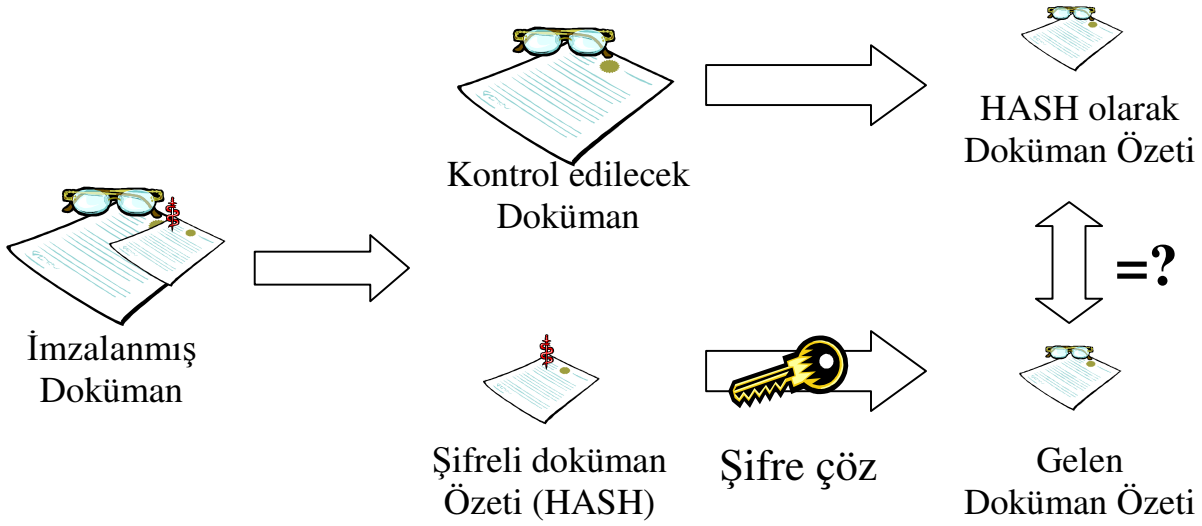
- Gizli ve açık anahtarın bir başka yolla üretilememesidir. (İnalöz,2003)

2.11.3.3 Açık Anahtar Altyapısını Oluşturan Temel Elemanlar

Açık anahtar altyapısı, asimetrik şifreli anahtar sisteminin diğer bir adı olup daha kolay anlaşılması açısından bu isimle de anılmaktadır. Üzerinde bir çok araştırma yapılmış olan bu konu aslında elektronik imzanın temel alt maddelerinden biri olarak da ele alınabilecek kadar öneme sahiptir. Elektronik imzanın temel ilkelerinin tamamını karşılayan bir sistem olan açık anahtar altyapısı bazı temel elemanları barındırmaktadır. (İnalöz,2003)



Şekil 2.1 Elektronik imza şifreleme prosedürü (Orta, 2006)



Şekil 2.2 Elektronik imza doğrulama prosedürü (Orta, 2006)

2.11.3.4 Kayıt Altında Tutma

Açık anahtar altyapısında bulunan kullanıcıların bilgilerine erişim yetki ve imkanını sağlar. Her kullanıcının belli ölçüler dahilinde erişim ve arama yetkisinin tanımlanması için yine üçüncü tarafın görev yaptığı bir temeldir. Bu temelde güncellemeler, iptal listeleri, yedeklemeler ve dağıtım işlemleri bulunur.

2.11.3.5 Yapılan İşlemlerin Doğrulanması

Açık anahtar altyapısının önemli temellerinden birisi de yapılan işlemlerin güvenilirliğinin doğrulanmasıdır. Bu temel altında şifreleme ve şifre çözme, yetkilerin doğrulanması, alıcı/gönderen bilgisi bulunmaktadır.

2.11.3.6 Şifrelemenin Yapılması

Mesajın kripto algoritmaları sayesinde karmaşık bir yapıya kavuşturularak güven ve gizlilik içerisinde ulaşması gereken adrese iletilmesi işleminin yapılması temelini oluşturur.

2.11.3.7 Zaman Kavramının Barındırılması

Zaman kavramının barındırılması işlemi veriye eklenen zamanın doğrulanması, üretilmesi ve kaydedilmesi gibi işlemleri içerir. Bu özellik açık anahtar altyapısının zamana bağımlı işlemlerinde büyük önem taşır.

2.11.3.8 İnkar Etmenin Engellenmesi

İnkar etmenin engellenmesi, verilerin işlenmesi, toplanması, tekrar elde edilmesi ve doğruluğunun onaylanması gibi işlemleri içerir. Bu işlemler bağımsız ve tarafsızlığı kabul edilmiş üçüncü kişi tarafından gerçekleştirilir ve oluşturma, iptal etme, karışıkların çözümü ve onaylama gibi işlemlerden bünyesinde barındırır.

2.11.3.9 Anahtar Yönetimi

Anahtar yönetimi anahtarlar ile yapılan bütün işlemlerin gerçekleştiği temeldir. Anahtarların üretilmesi, dağıtılması, gizliliğinin korunması, sahiplerine güvenle ulaştırılması, kopyasının ya da izinsiz ulaşımın engellenmesi, yedeklenmesi, güncellenmesi ve iptal edilmesi gibi işlemleri içerir.

2.11.3.10 Sertifika Yönetimi

Anahtarla veri arasında ilişki kuran bağ olan sertifikaların depolanması, üretimi ve iptali gibi işlemlerin icra edilmesini sağlayan temel unsurdur.

2.11.3.11 Sorgulama Servisleri

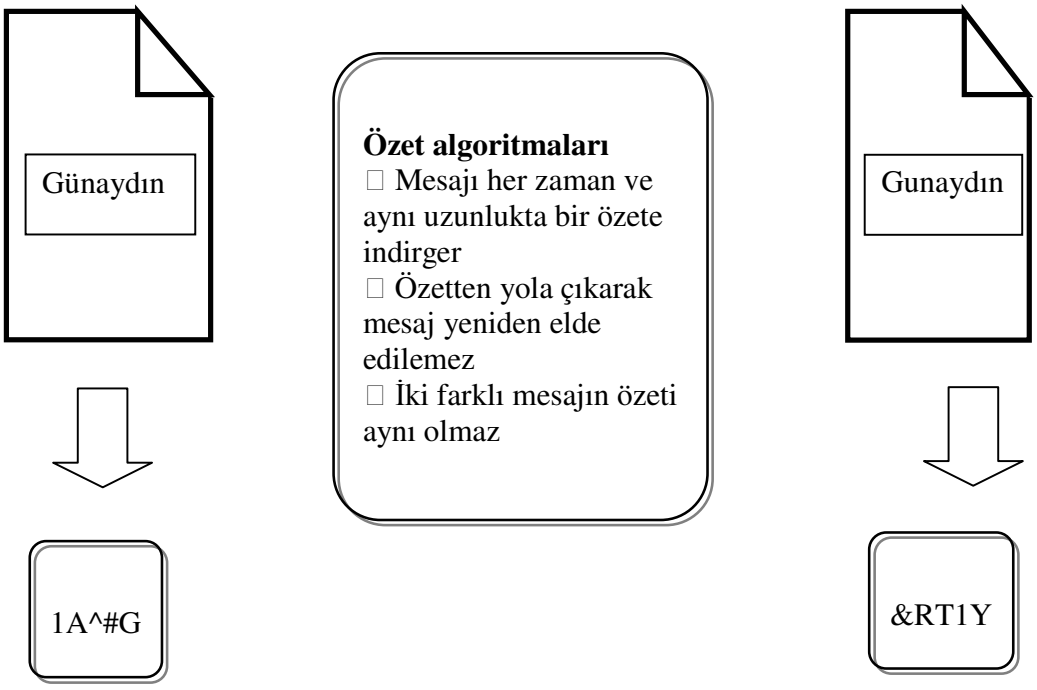
Açık anahtar altyapısında bulunan kullanıcıların bilgilerine erişim yetki ve imkanını sağlar. Her kullanıcının belli ölçüler dahilinde erişim ve arama yetkisinin tanımlanması için yine üçüncü tarafın görev yaptığı bir temeldir. Bu temelde güncellemeler, iptal listeleri, yedeklemeler ve dağıtım işlemleri bulunur.

2.11.3.12 Yetki Verme

Bu temelde yetkilerin veya erişimlerin paylaşılması söz konusudur. Grupların tanımlanması, grup içi hakların yönetilmesi ve yönetim haklarının belirlenmesi fonksiyonlarını içerir.(Genç, Açık Anahtar Altyapısı ve Problemleri)

2.11.3.13 Özet Alma ve Şifreleme Yöntemi

Hash fonksiyon şifrelemesi olarak da adlandırılan yöntem, gönderilen mesajın içerisinden sabit olmayan değerlere bağlı olarak mesajın anlamsız bir özetinin alınarak şifrelenmesi sistemi esasına dayanır. Bu özet bir sabit değere bağlı olarak alınmadığı için aynı kişi tarafından tekrarlansa bile aynı sonuçları vermez. Bu yolla elde edilen özet, mesaj ile birlikte şifrelenerek alıcıya gönderilmektedir. Bu durum, giden mesajın şifrelenmesi anlamına gelmemekte ve dört temel hususta gizlilik hususunu ihlal etmektedir. Yani gönderilen mesaj üçüncü kişi tarafından görülebilir durumdadır. Ancak şifrelenmiş özet alıcıya mesajın bütünlüğü, gönderen hakkında gerekli bilginin doğrulanması ve inkar etmenin engellenmesi hususunda güvenilirliği sağlamaktadır. Çünkü mesajda yapılan bir değişiklik şifrelenmiş olarak gönderilen özet ile mesaj metni arasında uyuşmayı engelleyeceği için anlaşılacaktır. Aynı şekilde üçüncü kişi tarafından değişmiş mesajın yeniden özetinin çıkarılması kişi bilgilerinin doğrulanmasını engelleyecektir. Bu sayede alıcı mesajın kaynağının kim olduğunu ve mesajın içeriğinin değişip değişmediğini kolayca anlayabilecektir. Bu yöntem özellikle imza altına alınması gereken, içerisinde gizli bilgiler barındırmayan ancak bütününün korunmuş olması esas olan anlaşma metinleri veya basit ve rutin mesajlaşmalarda kullanılır.



Şekil 2.3 Hash (özet) algoritması (Orta,2006)

2.12 Güvenli Elektronik İmza Tanımı

5070 sayılı Elektronik İmza Kanuna göre güvenli elektronik imza;

- Münhasıran imza sahibine bağlı olan,

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

- Nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan,

- İmzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan, elektronik imzalar güvenli elektronik imzadır." şeklinde tanımlanmıştır. Güvenli elektronik imzalar elle atılmış imza ile aynı hukuki sonucu doğurmaları nedeniyle büyük önem taşırlar. Güvenli elektronik imzaların ortak noktaları, nitelikli elektronik sertifikaya dayanarak ve güvenli

elektronik imza oluşturma aracıyla oluşturulmuş olmalarıdır. Kanunumuzda sadece elektronik imza ve güvenli elektronik imza ayrımı vardır.(Kanun,2004)

2.13 Güvenli Elektronik İmzanın Hukuki Açıdan Getirdiği Sorumluluklar

2.13.1 Elle Atılan İmza ile Aynı Hukuki Etkiye Sahip Olması

Kanunun 5nci maddesinde;

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

ibaresi yer almaktadır. Bu ibare kullanılan güvenli elektronik imzaya elle atılan imza yetkisi tanımladığı ve bu alandaki işlemlerde kolaylık sağladığı gibi kullanılması durumun aynı derecede sorumluluk da yüklediğinin açık bir ifadesidir. Yapılan anlaşmalar, iletilen veriler ve mesajlar gibi bir çok işlem de kullanılabilirliği olan güvenli elektronik imza, yukarıda sayılan bir çok temel unsurun tamamını barındırdığı ve inkar etmenin engellendiği anlamına gelmektedir.

2.13.2 Elektronik İmzanın Delil Niteliği

Kullanılan elektronik imzanın bir belgeye atılan imzadan farklı olmaması aynı oranda imzalanmış belge için onaylamanın yapıldığı ve belirlenen yükümlülük altına girildiğini belirler. Bu belgeler ve veriler senet niteliği taşırlar. Bu verilerin ya da yapılan işlemlerin inkarı aksi ispat edilmedikçe mümkün değildir. Burada önemli hususlardan birisinin de kanunumuzda tanımlanan hukuki etkinin sadece güvenli elektronik imza kapsamında tanınmış olmasıdır. Ancak elektronik imzalar;

- Elektronik biçimde olması,

- Nitelikli sertifikaya dayanmaması,

- Akredite edilmiş bir sertifika hizmet sağlayıcının sağladığı sertifikaya dayanmaması,

- Güvenli elektronik imza oluşturma aracı ile oluşturulmamış olması,

nedenlerinden herhangi birisi sebebiyle delil niteliğini yitirmezler. Bu da güvenli elektronik imzaların yanında diğer elektronik imzalara da delil niteliği kazandırma yolunu açmaktadır.

2.13.3 Elektronik İmzanın Kullanılamayacağı Alanlar

Kanun güvenli elektronik imzalara geniş ölçüde kullanım imkanı sağlarken istisnaları da belirtmiştir. Elektronik imzanın kullanılamayacağı yerlere ;

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

şeklinde açıklık getirilmiştir. Yani buradan nikahlar gibi fiilen memur önünde olması gereken işlemler, noter huzurunda yapılması gereken işlemler ve resmi bir kurumun katılımını veya tescilini gerektiren işlemlerin yapılamayacağı sonucu çıkarılmaktadır. Bu kısıtlama aslında hızla teknolojinin geliştiği günümüzde resmi makamların sunduğu fırsatların bir kısmına engel niteliği teşkil etmektedir. Ancak imkanların gelişmesi ölçüsünde bu maddenin değişmesi veya gözden geçirilmesi durumu mevcuttur.

2.13.4 Güvenli Elektronik İmzanın Oluşturulması Kavramı

Güvenli elektronik imza oluşturulması ile ilgili olarak Kanunun 6ncı maddesinde;

"Güvenli elektronik imza oluşturma araçları;

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

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

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

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

Sağlayan imza oluşturma araçlarıdır."

ifadeleri yer almaktadır. Bu ifadeler daha önceden ele alınmış olan konuların bir yansımasıdır. Güvenli elektronik imzanın eşsiz olması, güvenliği, gizliliği ve sahibine özel olması özelliklerini barındırması gerektiği üzerinde durulmaktadır.

2.13.5 Güvenli Elektronik İmzanın Doğrulanması Kavramı

Güvenli elektronik imzanın doğrulanması kanunda farklı bir madde içerisinde yer almasına rağmen imza oluşturma araçlarının bazıları aynı zamanda imza doğrulama aracı olarak da kullanılmaktadır. Bu durumu kanunda ayrıca ele alması, imza oluşturma aracı olmayanlar araçlar ile bir kavram kargaşası içerisine girilmemesi içindir. Güvenli elektronik imzanın doğrulanması kanunun 7nci maddesinde;

"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."

şeklinde yerini almıştır. Burada doğrulamanın önemli taraflarından birisinin yönetici konumunda olan üçüncü kişi olduğu görülmektedir. Bu kişi gerektiğinde verinin içeriği dahil olmak üzere kontrol yetkisini barındırmaktadır. Doğrulama yetkisine sahip kişi aynı zamanda bütün taraflarca güvenilirliği kabul edilmiş kişi niteliği taşıması bu noktada büyük önem taşımaktadır.

2.13.6 Elektronik Sertifika Hizmet Sağlayıcısı

Asimetrik şifrelemeye dayalı anahtar yapısı ile iletişimde kullanılan anahtarların kripto algoritmasını ve bunların güvenliklerini sağlayan kamu kurumu veya kuruluş, gerçek veya özel hukuk tüzel kişileridir. Elektronik sertifika hizmet sağlayıcısı güvenli ürün ve hizmet aracı sunmak, hizmeti güvenilir biçimde yürütmek ve sertifikaların taklit edilmesini engellemekten sorumludur. Bu durumların herhangi birisini yerine getirememesi durumunda bir ay süre ile eksiğini düzeltme süresi verilir ve faaliyetleri dondurulur. Bu süre zarfında eksiğini gideremeyen sertifika sağlayıcısının faaliyetine son verilir.

2.13.7 Nitelikli Elektronik Sertifika

Nitelikli elektronik sertifikalarda diğer elektronik sertifikalardan farklı olarak birkaç özellik daha eklenmektedir. Bunlar daha çok imza sahibinin bilgilerinin doğrulanması için gerekli işlemlerdir. Daha yüksek öneme haiz işlemlerin gerçekleştirilmesinde kullanılan nitelikli sertifikalarda bulunması gereken özellikler;

- Sertifikanın "nitelikli elektronik sertifika" olduğuna dair bir ibarenin,

- Sertifika hizmet sağlayıcısının kimlik bilgileri ve kurulduğu ülke adının,

- İmza sahibinin teşhis edilebileceği kimlik bilgilerinin,

- Elektronik imza oluşturma verisine karşılık gelen imza doğrulama verisinin,

- Sertifikanın geçerlilik süresinin başlangıç ve bitiş tarihlerinin,

- Sertifikanın seri numarasının,

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

- Sertifika sahibi talep ederse meslekî veya diğer kişisel bilgilerinin,

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

- Sertifika hizmet sağlayıcısının sertifikada yer alan bilgileri doğrulayan güvenli elektronik imzasının bulunmasıdır.

Nitelikli sertifika sağlayıcılar, düzenli olarak kullanıcıların imza yetkilerini ve kullanım sürelerini takip etmelidir. Kullanım süreleri dolan veya hatalı kullanım yapan imzalar için iptal listeleri yayınlamaları gerekmektedir. İmza sahipleri de düzenli olarak imza iptal listelerinin takibini yaparak kendi imzasının meşruiyetini takip etmesi gerekmektedir. Bu takip için her seferinde iptal listelerini indirerek tek tek incelemek yerine sertifika sağlayıcılarınca oluşturulmuş olan depoların kullanımı daha kolaydır. Bu depolara bir kez giriş yapıp bilgilerin oraya kaydı gerekmektedir. Daha sonra bu depolardan imza iptal listeleri takip edilebilir.

2.13.8 Nitelikli Elektronik Sertifikaların İptal Edilmesi

Nitelikli elektronik sertifikaların hizmet sağlayıcıları tarafından iptalini gerektiren durumlar Kanunun 11nci maddesinde;

- Nitelikli elektronik sertifika sahibinin talebi,

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

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

olarak belirtilmiştir. Bu durumlarda sertifika hizmet sağlayıcısı imzanın iptaline ilişkin zamanın tespiti için ve üçüncü kişilere verilecek bilgiler için bir kayıt oluşturur. Ayrıca eğer sertifika sağlayıcısı faaliyetine son vermişse ve başka bir sağlayıcıya devredemiyorsa da imzanın iptalini icra eder.

2.14 Elektronik İmza Aldığı Saldırılar

Elektronik imzaya yönelik saldırıları genel olarak iki başlık altında incelenebilir. Bunlardan birisi aktif saldırılarıdır. Direkt olarak şifreleme sisteminin araç yapısına saldırma yoluyla icra edilir. Bunlarda kendi aralarında ölçüm ve hata oluşturma saldırıları olarak ikiye ayrılırlar. Diğer bir saldırı çeşidi olan analiz saldırıları ise kendi arasında dört başlık altında incelenir:

- Zamanlama analizi saldırıları

- Güç analizi saldırıları
- Elektromanyetik analiz saldırıları
- Akustik analiz saldırıları

3 ELEKTRONİK TABANLI BELGELER

3.1 Genel Bilgiler

Elektronik tabanlı belgeler kamu adına görev yapan kurum ve kuruluşların, faaliyetlerini kayıt altına alması ve bu bilgileri vatandaşlarla paylaşması konusunda herkesin, her zaman, her yerden kolaylıkla ulaşabileceği şeffaf, verimli ve sade bir devlet yapısını destekleme açısında önemli yere sahiptir. Bilgisayar ve iletişim teknolojilerindeki gelişmeler bu alt yapının oluşması için üstün olanak sağlamaktadır. Kamu kurum ve kuruluşlarınca üretilen bilgi ve belgelerin verimliliğinin arttırılması için ortak standartların belirlenmesi göz ardı edilemez bir gereksinimdir. Böyle bir çalışma kullanımı kolay, erişimi hızlı, güvenilir, ucuz, sürekli ve sağlam "elektronik devlet" yapısının oluşumuna katkı sağlayacaktır. Bu yolla oluşan elektronik dokümanların belge vasfının korunması, onların üretim aşamasında ve hatta üretim öncesinde elektronik bilgi sistemleri tasarımı aşamasında ele alınmalarını gerekli kılmaktadır. Belge kavramının sistem tasarımcıları ve kullanıcılar tarafından iyi algılanması ve belge yönetimi gereksinimlerinin uygulanması gerekmektedir.

3.2 Elektronik Belgenin Nitelikleri

Elektronik belgede bulunması gereken diplomatik özelliklerin belirlenmesi, elektronik belgelerin hukuki geçerliliklerinin sağlanması için alınması gereken önlemler, elektronik imza ve mühür sistemlerinin uygulanması için gerekli sistem alt yapısının tanımlanmasıdır.

Elektronik belge yönetimi son derece geniş ve karmaşık bir alandır. Bu alan bir sistem yaklaşımı ile ele alınmalı ve sistemi oluşturan öğelerin birbiri ile uyumlu çalışması için gerekli önlemler alınmalıdır. Sistemi oluşturan öğelerin başında yazılım gelmektedir. Elektronik belgekullanmak kurum bu konuda uygun bir yazılıma ihtiyaç duyacaktır. Bu yazılımlar kurum fonksiyonlarını elektronik ortamda yürütmek için kullanılan diğer yazılımlarla entegre çalışabilen bağımsız bir paket olabilir. Bu bir yazılımda bulunması gereken asgari fonksiyonel özellikleri tanımlamaktadır.

3.3 Belge Yönetimi ve Doküman Yönetimi

Elektronik tabanlı belgelerin kurumların gündelik işlerini yerine getirirken oluşturulan her türlü dokümantasyonun içerisinden kurum aktivitelerinin delili olabilecek belgelerin ayıklanarak bunların içerik, format, ve ilişkisel özelliklerinin korunması ve bu belgeleri üretimden nihai tasfiyeye kadar olan süreç içerisinde yönetilmesi elektronik tabanlı belge yönetim sistemince üstlenilmektedir. Bu noktada karşımıza çıkan elektronik doküman yönetim (EDY) ve elektronik belge yönetimi (EBY) kavramları zaman zaman birbirinin yerine kullanılsa da amaçları açısından farklılık gösterirler.(Kandur,2006)

3.4 Dosyalama Planları

Elektronik belgeler ait olduğu kurumun yapısını ve fonksiyonlarını yansıtacak bir dosyalama planını içinde barındır ve kurum dosyalama planı ile uyumlu bir biçimde çalışır. İçerisinde temsil edilecek olan dosyalama planı hiyerarşik bir yapıda ve minimum üç seviyeden oluşmasına imkan sağlar. Minimum seviye tercih edildiğinde birim, seri ve dosya seviyeleri tercih edilir. Dosyalama planında temsil edilecek seviyelere herhangi bir sınırlama getirilmemektedir. Dosyalama planının kurulum aşaması sonrasında doğabilecek güncelleme ihtiyaçlarına imkan tanır. Ancak herhangi bir seviyeden bir elemanın çıkarılabilmesi sadece o elemana bağlı alt elemanların veya elektronik belgelerin olmadığı durumlarda mümkün olabilir.

Kullanıcıların elektronik belgelere erişimi için görsel bir kullanıcı ara yüzü kullanılmaktadır. Kullanıcılar, yetkileri dahilinde, grafik ara yüzü aracılığı ile elektronik belgeler arasında gezir, istedikleri belgeleri seçme, görüntüleme, kopyalama ve yazdırma gibi işlemleri ellerinde bulundururlar.

Dosyalama planı, içerisinde temsil edilen verilerin kimlikleri için iki tanım alanı bulundurur. Bu alanlar:

• Tekrar etmeyen alfa nümerik bir kod numarası alanı .

• Alfa nümerik bir ad alanı(Kandur,2006)

3.4.1 Dosyalama Planının İşletilmesi

Bir seri veya klasör altında sisteme dahil edilmiş olan elektronik belgeler, toplu halde başka bir seri veya klasör altına taşınabilir. Elektronik belgenin yeniden dosyalanmasına ilişkin işlemler kayıt altına alınmaktadır. İçerisinde planlanmış herhangi bir elektronik belgenin tamamının veya bir bölümünün silinmesi veya değiştirilmesi engellenilir. Elektronik bir belgenin imha işlemi ancak aşağıdaki şartlarda mümkün olabilir:

• Saklama zamanı planları gereğince yönetici kontrol ve yetkisinde,

• Herhangi bir hatayı düzeltmek amacıyla yapılan işlemler sırasında silinebilir.

Bu işlemler yetkili yönetici tarafından yapılır ve işlem kayıt altına alınır.

Klasörleri kapama veya yeni bölüm açma kriterleri kurulum aşamasında belirlenir. Yönetici klasörlerin kapanma zamanları ilgili olarak

• Yıl bitişi gibi zaman dilimleri,

• Klasöre ilk belge kaydından itibaren belli bir zamanın geçmesini esas alan zaman periyotları,

• İçerikte yer alacak dosya sayısı veya toplam büyüklük gibi sayısal kriterler geliştirebilir.

Sistem bütünlüğünün ve güvenirliğinin sağlanması için

• Her türlü onarım işlemlerini,

• Tüm kullanıcı hareketlerini,

• Sistem hatalarını ve arızalarını kayıt altına alınır. (Kandur,2006)

3.4.2 Belge Saklama Planları

Dosyalama planı ile sisteme dahil edilen her bir belge için bir saklama planı tanımlanır. Sistem, tanımlı her bir belgeye ait saklama planın otomatik olarak takip eder ve saklama süresi dolanların imha işlemlerinin yapılabilmesi için elektronik belge yöneticisini uyarır. (Kandur,2006)

3.4.3 Elektronik Belgelerin Hiyerarşik Yapısı

Sistem içerisinde elektronik belge hiyerarşisi en üst seviyeden başlayarak şu şekildedir:

Fon: Belgeyi üreten kuruma ait seviyedir.

Birim: Kurum içindeki birimlerin seviyesidir.

Seri: Birimlerin benzerlik gösteren fonksiyonlar sonucunda oluşan dosya ve klasörlerinini tamamıdır.

Klasör: Konu bütünlüğü açısından bir arada bulunan belgeler topluluğudur.

Belge: Tek bir işlemi gösteren dokümandır.

Belge bileşeni: Bir elektronik belgeyi oluşturan eklerdir. (Kandur,2006)

3.4.4 İmha İşlemi Tanımları

Sürekli Saklama: Sistem içerisinde tanımlanan herhangi bir elemanın saklama kriterlerinden bir veya birkaçı nedeniyle sürekli saklanacağını ve hiçbir şekilde imha edilmemesi gerektiğini ifade eder.

Değerlendirme: Elektronik belgenin ileri bir tarihte değerlendirmeye tabi tutulacağını ve imha kararının bu değerlendirme sonucuna göre alınacağını ifade eder.

İmha: Elektronik belgenin saklama süresinin bitiminde imha edileceğini gösterir.

Transfer: Elektronik belgenin üretildiği kurumdaki saklama süresinin bitiminde başka bir kuruma transfer edileceğini gösterir. (Kandur,2006)

3.5 Elektronik Belgelerin Kaydedilmeleri

Kayıt, elektronik belgelerin sistem içerisine dahil edilmesidir.

Elektronik belgelerin sisteme kaydı ile ilgili olarak:

• Teknolojik özellikleri ne olursa olsun her türlü elektronik belgeyi kayıt altına alma ve yönetebilme,

• Elektronik belgeleri dosyala ve saklama planları ile ilişkilendirme,

• Elektronik belgenin üretildiği uygulama programı ile entegre çalışabilme,

• Elektronik belgeye ait üst verilerin kontrol ve kayıt işlemlerini gerçekleştirebilme özellikleri bulunur. (Kandur,2006)

3.5.1 Taşıma, Kopyalama ve Silme

Sistem, elektronik belgelerin bulundukları klasörlerden alınarak başka bir klasörle taşınmaların imkan tanımaktadır. Yeniden dosyalama olarak adlandırılan bu işlem yalnızca yetkili kullanıcılar tarafından yapılabilir. Kopyalanan elektronik belgeye ait gizlilik statüsü ve erişim hakları kopyalanan elektronik belge için de geçerlidir. (Kandur,2006)

3.5.2 Arama

Bünyesinde bulunan belgeler üzerinde full-text arama yapabilmelidir. Kullanıcılar, arama işlemi sırasında herhangi bir elemana ait üst veri bilgilerini veya herhangi belgeye ait içeriği kaynak gösterebilmelidir.Bu durumda arama işlemi kaynak dosya içinde geçen anahtar kelimeler üzerinden yapılmalıdır. Arama işlemi birden fazla kavramla yapılabilmeli ve bu kavramlar farklı

kaynaklardan gelebilmelidir. Arama sonuçları kullanıcıya liste halinde sunulmalıdır. Arama sonucu olumsuz ise kullanıcı uyarılmalıdır. (Kandur,2006)

3.5.3 Raporlama

Sistem yöneticisine ve yetkili kullanıcılara sistem yönetimi, kullanıcı aktiviteleri ve istatistik raporları sunabilmelidir. (Kandur,2006)

3.5.4 Erişim Kontrolü ve Güvenlik

Kullanıcıların sisteme girişini kontrol altına almaya yönelik bir mekanizmaya sahip olmalıdır.

Böyle bir mekanizmanın en basit hali, kullanıcıya bir kullanıcı adı ve şifrenin verilmesidir. Kendisine kullanıcı adı ve şifresi verilenler için erişim haklarını gösteren bir profil tanımlanmalıdır. Ayrıca kullanıcının sistem içindeki rolleri ve ait olduğu kullanıcı grubu bu profil içerisinde tanımlanmalıdır. (Kandur,2006)

3.5.5 Erişim Hakları

Kullanıcılar; seri, klasör veya belge gibi sistem elemanlarına atanacak erişim haklarının sistem yöneticisi tarafından tanımlanmasına izin vermelidir. Sistem bünyesinde yer alan elemanlar için en azından beş kademeli erişim hakları tanımlayabilmelidir. Bunlar:

• **Tasnif dışı:** içerdiği konular itibariyle, gizlilik dereceli bilgi taşımayan, bilgi, belge, evrak, mesaj ve dokümanlara verilen gizlilik derecesidir.

• **Hizmete özel:** içerdiği konular itibariyle, gizlilik dereceli konular dışında olan, güvenlik işlemine ihtiyaç gösteren ve Devlet hizmetine ait özel bilgileri ihtiva eden bilgi, belge, evrak, mesaj ve dokümanlara verilen gizlilik derecesidir.

• **Özel:** İçerdiği konular itibariyle, müsaadesiz olarak açıklandığı takdirde, milli menfaatlerimizi olumsuz yönde etkileyecek olan bilgi, belge, evrak, mesaj ve dokümanlara verilen gizlilik derecesidir.

• **Gizli:** Müsaadesiz olarak açıklandığı takdirde, ulusal güvenliği, milli prestij ve menfaatlerimizi ciddi ve önemli derecede zedeleyecek olan bilgi, belge, evrak, mesaj ve dokümanlara verilen gizlilik derecesidir.

• **Çok Gizli:** Müsaadesiz olarak açıklandığı takdirde, ulusal güvenliği büyük ölçüde tehlikeye düşürecek, Devletimize ve müttefiklerimize büyük ölçüde zararlar verebilecek olan bilgi, belge, evrak, mesaj ve dokümanlara verilen gizlilik derecesidir.(Kandur,2006)

3.5.6 Kullanıcı Rolleri

Kullanıcıların sistem içerisindeki fonksiyonlarını belirleyici nitelikte roller tanımlayabilmelidir. Bu roller kullanıcıların erişim haklarını düzenleyici nitelikte olacaktır. Bu rollerin tanımlanması ve kullanıcılara atanması yetkisi sistem yöneticisinde olmalıdır. Bu rollerin neler olacağı kurumların hiyerarşik yapısına göre değişebilir. Aşağıdaki roller birçok kurum hiyerarşisine uygun olabilir.

• **Sistem Yöneticisi:** Sistem üzerindeki en yetkili kullanıcıdır. Bilgisayar sisteminin düzenli ve kurumsal fonksiyonlara uygun olarak çalışmasından sorumludur. (Kandur,2006)

3.5.7 Kullanıcı Grupları

EBYS, kullanıcı grupları tanımlamaya uygun olmalıdır. Bu gruplardan bazıları şunlar olabilir:

• **Fonksiyonel gruplar:** Aynı birimde çalışan benzer fonksiyonları gerçekleştiren kişilerden oluşan gruplar.

• **Yönetici grupları:** İdari olarak yönetici sorumluluğu bulunan kişilerden oluşan gruplar.

• **Proje grupları:** Belli projeleri gerçekleştirmek için belirli zaman dilimlerinde bir araya getirilmiş kişilerden oluşan gruplar. (Kandur,2006)

3.5.8 Denetim

EBYS otomatik olarak bir günlük tutabilmelidir. Bu günlük sistemdeki kullanıcı aktivitelerinin kayıt altına alınmasını sağlamalıdır. Günlükte asgari olarak şu bilgiler tutulmalıdır:

• Gerçekleştirilen aktivitenin ne olduğu (kayıt ekleme, değiştirme, arama, v.s),

• İşlemin hangi EBYS elemanı üzerinde gerçekleştirildiği,

• İşlemin kim tarafından gerçekleştirildiği,

• İşlemin gerçekleştirildiği tarih ve saat.

Günlük dosyasında takip edilmesi gereken aktivitelerden bazıları şunlardır:

• Elektronik dokümanların belge olarak tanımlanma işlemine ait tarih ve saat bilgisi,

• EBYS elemanların birbirleriyle ilişkilendirme ve/veya yer değiştirme işlemleri,

• Saklama planı ve saklama sürelerinde yapılacak değişiklikler,

• EBYS elemanlarına ait üstveri bilgilerinde yapılan değişiklikler,

• Erişim hakları ve bunların atanması ile ilgili yapılan değişiklikler,

• Elektronik belgelerin kopyalama, taşıma ve silme işlemleri(Kandur,2006)

3.6 Belge Özellikleri

Tanımlanabilirlik: Elektronik ortamda üretilen dokümanlardan belge statüsü kazananlar EBYS içerisinde tanımlanabilir olmalıdır. Tanımlanabilirlik, herhangi bir elektronik belge üreticisi, yazarı, alıcısı ve belgeye ait tarih bilgilerinin kayıt altına alınması ile sağlanır. Elektronik belgeleri diğer elektronik dokümanlardan ayırt etmek için aşağıdaki tanım referans olarak kullanılmalıdır. Buna göre elektronik belge; Herhangi bir bireysel veya kurumsal fonksiyonun yerine getirilmesi için

alınmış, ya da fonksiyonun sonucunda üretilmiş, içerik, ilişki ve formatı ile ait olduğu fonksiyon için delil teşkil eden kayıtlı bilgidir.

Üretici: Herhangi bir elektronik belgenin üretilmesi için yetkili tüzel kuruluş ve gerçek kişiler üretici olarak tanımlanır. Geleneksel sistemlerde bir belgeye ait üretici bilgisi evrakın başında antet olarak veya evrakın sonunda imza bölümünde yer alır.

Yazar: Herhangi bir belgenin entelektüel sorumluluğunu taşıyan kişi veya kurumdur. Genel olarak belgeyi imzalayan kişi yazar olarak tanımlanır. Yazar, entelektüel sorumluluğu kendi adına taşıyabileceği gibi yetkilisi olduğu kurum adına da taşıyabilir. Bir belgeye ait yazar sorumluluğu ile üretici sorumluluğu aynı kişi veya kuruluşu işaret edebilir.

Gönderen: Herhangi bir belgenin çıkış kaynağı olan kişi, kurum veya süreç sorumlusudur.

Bir belgenin üreticisi, yazarı veya göndericisi tarafından diğer bir kuruma veya şahsa gönderilmesi dokümanların belgeye dönüşmesindeki en önemli unsurdur. Gönderilme işlemi

fonksiyonu tetiklemesi ve şekillendirmesi açısından son derece önemlidir. Bir belgeye ait gönderen sorumluluğu, yazar ve / veya üretici sorumluluğu aynı kişi veya kuruluşu işaret edebilir.

Çıkış yeri: Elektronik belgenin üretildiği veya gönderildiği yere ait coğrafi bilgidir. Elektronik belgeye ait çıkış yeri bilgisi kurumsal ihtiyaçlara göre detaylandırılabilir. Ülke, bölge, şehir, ilçe gibi detaylar EBYS içerisinde gerekli olduğu durumlarda hiyerarşik olarak verilebilmelidir.

Üretim tarihi: Belgenin üretildiği tarih bilgisidir.

İletim tarihi: Belgenin gönderildiği tarihtir.

Arşivleme tarihi: Elektronik belgenin kurumsal arşiv sistemine dahil edildiği tarihtir.

Transfer tarihi: Elektronik belgenin kurum arşivine veya kurum dışı bir arşive transfer edilme tarihidir. Transfer işlemi birden fazla gerçekleşebilir. Bu nedenle belgenin mülkiyet zincirinde bir kopukluk olmaması için tüm transferlere ait tarih bilgileri kayıt altına alınmalıdır.

İmha tarihi: Elektronik belgenin kurum saklama planları çerçevesinde imha edildiği tarihtir.

Alıcı adı: Elektronik belgenin işlem yapılmak veya bilgilendirmek üzere gönderildiği kişi, kurum veya süreç sorumlularıdır. Alıcı birden fazla olabilir. Alıcının birden fazla olduğu durumlarda

gereği için gönderilenlerle bilgi için gönderilenler ayırt edilebilmelidir.

Fonksiyon adı: Elektronik belgenin ilgili olduğu kurumsal fonksiyonun adıdır. Bu bilgi elektronik belge üzerinde kayıtlı olmayabilir. Dolayısıyla genelde bir belgeye ait fonksiyon bilgisi içerik analizi yapıldıktan sonra belirlenebilir. Fonksiyon bilgisi oluşturulurken kullanılacak anahtar kelimeler kurumsal dosya tasnif planları içerisinden seçilmelidir. (Kandur,2006)

3.7 Onay ve Kayıt Bilgisi

EBYS, elektronik belgelerin üreticisi tarafından onaylanmasına ve kurumsal kayıt sistemleri içerisinde temsil edilmesine imkan sağlayacak teknolojileri bünyesinde barındırmalı ya da bu türden bağımsız sistemlerle entegre çalışabilmelidir. Bu sistemlerin yasal ve prosedürsel olarak kabul edilebilir olması uygulamada bir önkoşul olmalıdır. Geleneksel evrak yönetim sistemlerinde bir belgenin 'resmi' bir hüviyet kazanabilmesi için o belgenin imza yetkisine sahip

kişilerce imzalanmış olması ve belgenin kurumsal evrak kayıt sistemi içerisinde yer alması esastır. Belge ile ifade edilen mal ve hizmet alma ilişkileri, medeni ilişkiler, hak ve alacak ilişkilerinin hukuki geçerliğinin olabilmesi için belgenin ilgili ve yetkili kişilerce imzalanmış ve bir kayıt sistemi içerisinde gösterilmesi esastır. (Kandur,2006)

3.8 Doküman Yönetimi

Doküman yönetim sistemleri (DYS), genel olarak kurumsal bilgi kaynaklarının elektronik ortamda depolanması ve kullanılması için geliştirilmiş sistemlerdir. Bu sistemler kurum içerisinde belge statüsü kazanmış dokümanların yanı sıra belge özelliği taşımayan ancak içerdiği bilgi açısından depolanan ve kullanılan dokümanları düzenleme, tanımlama ve erişim gibi fonksiyonları yerine getirmek üzere kullanılır.

Doküman yönetim sistemleri kurum bilgi kaynaklarının etkin ve verimli bir şekilde kullanılması ile zaman, maliyet ve işgücü tasarrufu sağlaması açısından kurumlar için önemli bir araçtır. Bu sistemler, elektronik belge yönetimi sistem kriterleri açısından iki temel fonksiyonu yerine getirmek için kullanılabilir:

• Doküman yönetim sistemleri, diğer bilgi kaynakları için olduğu gibi, elektronik belge özellikleri korunduğu takdirde, elektronik belgelerin yönetimi için de kullanılabilir.

• Doküman yönetimi sistemi içerisine dahil her türlü bilgi kaynağı potansiyel olarak bir belge olarak tanımlanabilir. Bu nedenle doküman yönetim sistemleri EBYS için bir ön proses aracı olabilir. Sistem içindeki dokümanlardan bir bölümü belge statüsü kazandırılarak ayrı bir yönetim prosedürüne tabi tutulabilir. (Kandur,2006)

3.9 Elektronik Tabanlı Belge Yönetiminde Referans Alınan Kaynaklar

3.9.1 Uluslararası Arşiv Konseyi

Bu konsey şu konularla ilgilenmiştir:

• Belgelerin üretimi ve arşivleme yöntemleri için araştırmalar yapmak,

• Arşiv kurumları arasında iletişimi sağlamak,

• Elektronik belgeler ile ilgili olarak detaylı bir literatür çalışması yapmak.

1997 yılında yayınlanan rehber iki bölümden oluşmaktadır. Birinci bölüm elektronik belgelerin yönetimini etkileyen yasal, teknolojik ve kurumsal etkileri araştırmakta ve elektronik belgelerle ilgili bazı temel kavramları analiz etmektedir. Bu bölümde ayrıca arşiv kurumlarının elektronik belge yönetimi için geliştirebilecekleri stratejilere yer verilmektedir. İkinci bölüm daha uygulamaya yönelik konuları içermektedir. Özellikle birinci bölümde tanımlanmış olan stratejilerin nasıl hayata geçirileceğini göstermekte ve çeşitli uygulama taktikleri sunmaktadır. (Kandur,2006)

3.9.2 İngiliz Milli Arşivleri

İngiliz Milli Arşivleri bünyesinde oluşturulan EROS (Electronic Records from Office Systems) programı çerçevesinde üretilen bu kaynak iki cilt halinde hazırlanmıştır. Birinci cilt elektronik tabanlı belgelerin yönetim prensipleri üzerinde dururken ikinci cilt prosedürleri tanımlamaktadır. Rehber temel olarak elektronik belgelerin;

• kayıt altına alınması, korunması ve hizmete sunulması,

• envanterlerinin hazırlanması, ayıklanması ve tasfiyesi,

• sürekli saklama stratejileri ve arşive transfer işlemlerini,

ele almakta ve bu konularla ilgili prensipleri ve prosedürleri ortaya koymaktadır. Rehber, özellikle ofis sistemleri bünyesinde üretilmiş elektronik tabanlı belgeler ve görüntüleme sistemleri ile elektronik ortama aktarılmış olan belgelerinin kullanımı ile ilgili konuları ele almaktadır. (Kandur,2006)

3.9.3 Avustralya Milli Arşivleri

Avustralya Milli Arşivleri tarafından hazırlanan bu rehber kamu kuruluşlarında elektronik belgelerin üretim ve saklanması ile ilgili konularda tavsiyeler içermektedir. Rehberde elektronik belgelerin diğer belge formatlarında olduğu gibi kurumsal aktivitelerin kayıt altına alınmasında, kurumsal devamlılığın sağlanmasında ve kurumsal sorumluluklarına yerine getirilmesindeki önemine vurgu yapılmaktadır. Rehber spesifik olarak elektronik tabanlı belgelerin;

• Kullanımının önemi ve entegre bir modelin nasıl olması gerektiği,

• Üretimi ile ilgili verilerle birlikte nasıl temsil edileceği,

• Acil durum planlaması dahil olmak üzere güvenli depolama ve koruma koşullarının neler olabileceği,

• Erişim işlemlerinin nasıl gerçekleştirileceği,

• Tasfiye işlemlerinin nasıl yapılacağı konularında tavsiyeler içermektedir. Ayrıca elektronik tabanlı belge türlerinin yaygın olanlarının karakteristik özellikleri incelenmektedir. (Kandur,2006)

4 ELEKTRONİK İMZANIN GELİŞİMİ

4.1 Elektronik İmza Uygulamasına Geçmiş Bazı Avrupa Ülkeleri

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

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

Avrupa'da elektronik imzanın en yaygın kullanıldığı alan elektronik bankacılık olup elektronik devlet uygulamaları da yine önemli ölçüde göze çarpmaktadır.

Bireysel bankacılık işlemlerinde elektronik imza tüm AB ülkelerinde birkaç yıldır kullanılmaktadır. Bu işlemler genel olarak akıllı kart kullanılarak yapılmaktadır. Elektronik imza genel olarak bankacılık işlemlerinde giriş ve doğrulama amacıyla kullanılıyor olsa da bankalar arası işlemlerde elektronik sertifikalar yüksek oranda kullanılmaktadır. Çünkü bu işlemlerde yüksek oranda güvenlik gerekmektedir.

Elektronik devlet, Avrupa'da hızla gelişen bir elektronik imza uygulaması olmaktadır. Avusturya, Finlandiya, Almanya, İrlanda, İtalya, İsveç, Çek Cumhuriyeti, Polonya, Romanya, İngiltere gibi

birçok ülke elektronik devlet uygulamalarına başlamışlardır. Elektronik devlet uygulamaları genelde elektronik kimlik kartına dayalıdır.

Avrupa'da genel olarak elektronik imzanın yaygın kullanımının ve pazarda kabul görmesinin önündeki en büyük engel ulusal ve uluslararası düzeyde birlikte kullanılabilirlik konusundaki eksikliktir. Avrupa'da elektronik imza kullanıcı maliyetleri büyük değişiklikler göstermektedir. Elektronik bankacılık uygulamalarında neredeyse bedava olup elektronik devlet uygulamalarında akıllı karta dayalı olarak yıllık 60 Euro'yu bulmaktadır. (Karakoçak, 2005)

Elektronik İmza Uygulamasına Geçmiş Bazı Avrupa Ülkeleri

İtalya, Almanya, Portekiz,İspanya, Fransa, Danimarka, Lüksemburg, İngiltere, İrlanda, Avusturya, Çek Cumhuriyeti, Estonya, Litvanya, Slovenya, Belçika,İsveç, Macaristan, İzlanda, Norveç, Hollanda,Polonya

Amerika Kıtasında Elektronik İmza Uygulamasına Geçmiş Bazı Ülkeler

Bermuda,Peru, Kolombiya, Kanada, Arjantin

Elektronik İmza Uygulamasına Geçmiş Diğer Ülkeler

Rusya, Hindistan, Singapur, Japonya, Hong Kong, Filipinler, Tayland (Karakoçak, 2005)

4.2 Avrupa'dan Elektronik İmza Uygulama Örnekleri

4.2.1 Almanya: Köln Şehir Kartı Projesi

Şehir kartı projesi, belediye hizmetleri içerisinde bulunan iş süreçlerinin çalışanlar ve vatandaşlar için güvenli elektronik bir ortama taşınması süreçlerini kapsamaktadır. Vatandaş ve belediye arasındaki elektronik iletişimin sağlanması, yasal olarak kullanılan elektronik imzalar için teknik altyapı ve açık, ileriye dönük ve standart bir çözüm gibi ihtiyaçlara yönelik olarak Açık Anahtar Altyapısı ile akıllı kartların bütünleştirildiği bir çözüm sunmuştur. Buna bağlı olarak iş süreçleri sayısal imzalar yardımıyla iyileştirilmiş; çoklu uygulamalı kartlarla birlikte çözüm eğitim, kültür ve sağlık alanına da genişletilmiştir.(Karakoçak, 2005)

4.2.2 İtalya: İçişleri Bakanlığı Kimlik Kartı Projesi

İtalya, Avrupa'da elektronik imza uygulamasına geçen ikinci ülkedir. İtalya İçişleri Bakanlığı'nın vatandaşların kimliklerinin tanımlanmasının geliştirilmesi ve vatandaş ile kamu otoriteleri arasındaki ilişkinin kamu kuruluşlarının dışına taşınmasını sağlamak amacıyla oluşturduğu çözüm, akıllı kart teknolojisine dayalı yeni bir kimlik kartı üstüne kurulmuştur. Proje kapsamında merkezi yönetimi ile koordineli olarak belediyelerde online elektronik kimlik kartı dağıtımı prosedürleri ve süreçleri gerçekleştirilmiştir. Proje pilot aşamasında Milano, Palma ve Roma 'da bulunan 83 belediye ve 280,000 vatandaşı kapsamıştır. 5 yıl içerisinde İtalyan Hükümeti yaklaşık 40 milyon elektronik kimlik kartı oluşturacaktır. (Karakoçak, 2005)

4.3 Türkiye'deki Gelişmeler Ve Uygulamalar

Türkiye'de elektronik imzanın hukuki olarak anlam kazanması ve elektronik imza kullanımının hukuken geçerli sayılması 5070 Sayılı ve 23 Ocak 2004 tarihli Elektronik İmza Kanunu'nun çıkarılmasıyla sağlanmıştır. Söz konusu kanunun ülke gerçeklerine uygun olarak uygulamaya geçirilebilmesi için gerekli düzenlemeleri yapma görevi ise Telekomünikasyon Kurumu'na verilmiştir. Kurumun, elektronik imzanın uygulanmasına ilişkin ikinci mevzuatı, diğer ülkelerin ve özellikle Avrupa Birliği üye ülkelerinin hukuki düzenlemelerini ve teknik uygulamalarını, konuyla ilgili yetkili ve sorumlu uluslararası kuruluşlarca belirlenmiş standartları inceleyip, Türkiye'de oluşacak bu yeni sektörün önemli aktörlerinin de görüşlerini değerlendirerek 23 Ocak 2005 tarihinde çıkarmıştır. Kanunla, gerekli mevzuatın tamamlanması ile birlikte oluşacak elektronik imza sektörünün sağlıklı ve mevzuata uygun işleyişinin sağlanmasından da yine Telekomünikasyon Kurumu sorumlu tutulmuştur.

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

Türkiye'de oluşturulacak elektronik imza altyapısının ülke çıkarlarına ve uygulama kolaylığına hizmet verecek şekilde olabilmesi amacıyla; elektronik sertifika sağlayıcılarının kök anahtarlarının Türkiye'de üretilmiş olması, kamu kurum ve kuruluşlarının tek bir altyapı ve

standart altında toplanması, kıt kaynakların verimli kullanılması ve yapının tek elden koordinasyonunun sağlanması gerekmektedir. Bu anlamda, Türkiye e-Dönüşüm İcra Kurulu Kararı doğrultusunda tüm kamu kurum ve kuruluşlarının kurumsal sertifika ihtiyacının karşılanması için TUBİTAK- Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü görevlendirilmiş, bazı istisnalar dışında kamu kurum ve kuruluşlarının elektronik sertifika ihtiyacının bu kurum tarafından karşılanması sağlanmıştır.

Elektronik imzanın Türkiye'deki kamusal uygulamalarının;

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

Ticari uygulamalarının ise;

- İnternet bankacılığı
- Sigortacılık işlemleri
- Elektronik Sipariş
- Elektronik Sözleşmeler

alanlarından bir kısmı gerçekleşmiş bir kısmı ise geliştirilmektedir.

Haziran 2004 tarihinde Elektronik İmza Ulusal Koordinasyon Kurulu Altyapı Çalışma Grubu İlerleme Raporu'nda yer alan ve on beş adet kamu kurum ve kuruluşlarına yönelik yapılan bir araştırma sonucunda, Türkiye'de kamu sektörünün elektronik imza uygulamaları ile ilgili bazı beklentilerine ilişkin sonuçlar saptanmıştır. Elektronik imzanın genel olarak kurum içi ve

kurumlar arası kullanımının sistem girişleri şeklinde olacağı tespit edilmiştir. Araştırmaya tabi olan kamu kurum ve kuruluşları: Adalet Bakanlığı, Maliye Bakanlığı, Türkiye Noterler Birliği, Denizcilik Müsteşarlığı, Devlet Meteoroloji İşleri Genel Müdürlüğü, Devlet İstatistik Enstitüsü, Dış Ticaret Müsteşarlığı, Emekli Sandığı Genel Müdürlüğü, T.C. Merkez Bankası, Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü, T.C. Devlet Demiryolları, Türk İşbirliği ve Kalkınma İdaresi Başkanlığı, Türk Standartları Enstitüsü, Sermaye Piyasası Kurulu, Gümrük Müsteşarlığı'dır. (Karakoçak, 2005)

4.4 Ülkemizdeki Uygulama Örnekleri

Ülkemizde elektronik imza uygulamasına ilişkin aşağıda belirtilen iki projeden bahsedilecektir. Bunlar sırasıyla Sermaye Piyasası Kurulu'nun Kamuyu Aydınlatma Platformu ve Dış Ticaret Müstaşarlığı tarafından yürütülen Dahilde İşleme Rejimidir.

4.4.1 Sermaye Piyasası Kurulu'nun Kamuyu Aydınlatma Platformu

Sermaye piyasalarında işlem gören halka açık şirketlerin ve tüm aracı kuruluşların mali tablolarının, özel durum açıklamalarının ve diğer bildirimlerinin bilgisayar ağları üzerinden elektronik imza teknolojisi kullanılarak güvenli bir şekilde iletilmesini hedefleyen Kamuyu Aydınlatma Platformu, Sermaye Piyasası Kurulu ve İstanbul Menkul Kıymetler Borsası (İMKB) ortaklaşa gerçekleştirilmiştir. Tüm bağımsız denetim şirketleri de ilgili mali tabloları imzalamakla sınırlı olmak koşuluyla Kamuyu Aydınlatma Platfrmu kapsamında yer almaktadır.

Kamuyu Aydınlatma Platformu bir elektronik devlet uygulamasında olması gereken tüm unsurları (Devlet: Serbest Piyasalar Kurulu, Şirket: Kamuyu Aydınlatma Platformu şirketleri, Vatandaş: Sermaye Piyasası Yatırımcısı) içermesi sebebiyle, tam bir elektronik devlet uygulaması olarak Sermaye Piyasası Kurulunun Avrupa Birliği sürecinde attığı önemli bilişim yatırımlarından birisi olarak durmaktadır. Coğrafi olarak tüm Türkiye'ye yayılmış 530'ü aşkın şirketi ve 2500'ü aşkın kullanıcıyı kapsamaktadır.

Kamuyu Aydınlatma Platformu kapsamında geliştirilen ve şirketlerin kullanımı için hazırlanan uygulama yazılımı aracılığıyla bildirimler doldurulur ve belirli bir hiyerarşide imza yetkisine haiz kişilerce, elektronik imza ile imzalanarak internet üzerinden Serbest Piyasalar Kurulu sistemine gönderilir. Gönderilen bildirimler veri tabanına kaydedilir ve anında kamuoyu ile paylaşılır.

Şirket bildirimlerini yazılımlara çevrim dışı olarak kaydedebilir. Belli dönemlerde bağımsız denetim şirketleri de elektronik imzalarını bildirim gönderme sürecindeki sırası ile atarak bildirim gönderme sürecine katılmaktadırlar.

Kamuyu Aydınlatma Platformu, elektronik imzanın Türkçe elektronik belgelere entegrasyonunun sağlandığı ve Türkiye'de sertifika hizmet sağlayıcılığı konusundaki ilk işletme uygulamasıdır. (Karakoçak, 2005)

4.4.1.1 Kamuyu Aydınlatma Platformu'nun Gelişim Süreci

Günümüzde İstanbul Menkul Kıymetler Borsası'nda (İMKB) işlem gören 307 şirket ile 141 aracı kuruluş, sermaye piyasası mevzuatında belirlenen mali tabloları, tanımlanan aralıklar içinde kamuya açıklamak zorundadır.

Mali tablolar ve "Özel Durum Açıklamaları", halen yürürlükte olan uygulama dahilinde disketle ve son durumda mutlaka basılı bir biçimde kağıt çıktılarla SPK ve İMKB'ye gönderilmektedir. Bu uygulamada, bilgilerin sisteme ulaşması ve işlenmek üzere veri tabanına kaydedilmesi süreçleri, zaman ve işgücü kaybına yol açmakta; hata ve tekrarlardan doğan maliyet artışları ortaya çıkmaktadır.

Kamuyu Aydınlatma Platformu ile söz konusu kayıpların en aza indirilmesi için, şirket bildirimlerinin internet üzerinden güvenli bir şekilde yapılmasını sağlayacak elektronik imza teknolojilerine dayalı bir altyapının kurulması öngörülmüştür.

Bugün itibariyle, ilgili şirket ve kuruluşlarca bildirim gönderilmeye devam edilmektedir. Özellikle kullanım alışkanlığının kazanılması için belli bir süre öngörülmüştür. Bu süre içerisinde bildirimler doğrudan kamuoyuna sunulmamakla birlikte sisteme ilişkin gözlem, iyileştirme ve ayar konularında değerlendirmeler yapılmaktadır. Ayrıca KAP kapsamında yürütülen sertifika hizmetlerine ve şirketlere destek hizmeti kapsamında TÜBİTAK BİLTEN tarafından yardım hizmetleri yoğun olarak devam etmektedir.

KAP kapsamında duyuru yapabilecek diğer kurumlar olan İMKB Takas ve Saklama Bankası A.Ş. (TAKASBANK), Türkiye Sermaye Piyasası Aracı Kuruluşlar Birliği (TSPAKB) ve Merkezi Kayıt Kuruluşu (MKK) da Kamuyu Aydınlatma Platformu'nda yer almakta olup ilgili

kurum kullanıcıları proje hakkında bilgilendirilmiş ve uygulama kapsamında elektronik sertifikaları dağıtılmıştır.

Entegrasyon, elektronik belgelerin taşınması ve elektronik olarak imzalanması için kullanılan en yaygın açık standart olan "XML Signature" standardını desteklemektedir. Buna göre, Kamuyu Aydınlatma Platformu elektronik belgelerindeki elektronik imza, diğer kişilerce de doğrulanabilmektedir. Uygulama ayrıca, Elektronik İmza Kanunun da şart koştuğu gibi, imzalanacak metnin tamamının, imzalama işlemi öncesi kullanıcı tarafından görüntülenebilmesine olanak tanımaktadır. Uygulamanın özgün özelliklerinden biri de metinlerin birden fazla kullanıcı tarafından imzalanabilmesidir.

Uygulama açık standartlara uygun olarak geliştirildiği için, farklı elektronik sertifika hizmet sağlayıcıları tarafından verilmiş farklı kullanıcı sertifikalarıyla çalışabilme özelliğine sahiptir. Uygulama ayrıca, markadan bağımsız olarak farklı akıllı kart ve akıllı kart okuyucuları ile uyumlu çalışabilmektedir. Sistemin tüm modüllerinde, kimlik doğrulama ve güvenli iletişim protokolleri, açık standartlarla uyumlu ve açık anahtar altyapı teknolojileri kullanılarak gerçekleştirilmektedir.

Uygulamada, yönetim yazılımı olarak, tümü daha önceden platform bağımsız ve tamamıyla yerli geliştirilen Türkçe bir ürün olan ZEUGMA kullanılmıştır. Kullanılan ürün TÜBİTAK BİLTEN tarafından geliştirilmiş ve uluslararası standartlara uyumludur. (Karakoçak, 2005)

4.4.1.2 Kamuyu Aydınlatma Platformu'nun Etkileri

- Güvenilirlik: Faks veya posta yoluyla gelip yayınlanan bilgilerin elektronik imza ile gönderilmesi suretiyle verilerin güvenilirliği sağlanmaktadır.

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

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

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

- Tam ve Yeterli Bilgi: Tasarruf sahipleri, ortaklar ve diğer ilgililerin zamanında bilgilendirilmesini temin etmek suretiyle hazırlanan ilgili tebliğ uyarınca şirketler, tebliğde yer alan hususlarda kamuya özel durum açıklaması yapmaktadırlar. Kamuyu Aydınlatma Platformu kapsamında yapılacak her bir özel durum açıklaması için ayrı olmak üzere yaklaşık 250 adet özel durum şablonu oluşturulmuştur. Oluşturulan her bir şablonun her bir hücresi sorgulamaya müsait olarak dizayn edilmiştir. Bu sistem bulunduğu bölümde türleri açısında Dünyadaki ilk uygulamadır.

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

4.4.1.3 Dış Ticaret Müsteşarlığı: Dahilde İşleme Rejimi

Dış Ticaret Müsteşarlığı'nın Dahilde İşleme Rejimi , Türkiye çapında on üç İhracatçı Birliği'ne mensup 5000'den fazla firmanın, birlik kullanıcılarının, gümrük kapılarındaki kullanıcıların ve Dış Ticaret Müsteşarlığı uzmanlarının kullanıcısı olduğu bir sistem olarak hayata geçirilmiştir. Bu sistemle, Dahilde İşleme İzin belgelerinin Dış Ticaret Müsteşarlığı'na ulaştırılması ve onaylarının alınması sürecinde yaşanan bürokratik gecikmeler en aza indirilmiştir. Sistem sayesinde yine belge başvurusunda bulunacak olan şirket başvurusunu internet aracılığı ile elektronik ortamdan yapabilmekte ve başvuru sonucunu yine elektronik ortamda takip edebilmektedir. Ayrıca şirketin başvurusundan sonra Dış Ticaret Müsteşarlığı içerisindeki iş akışı da yine elektronik ortamda gerçekleştirilmektedir. Elektronik ortamdaki bu iş akışına katılan şirket ve Dış Ticaret Müsteşarlığı kullanıcıları, kimliklerini uygun bir şekilde doğrulayarak sisteme girmek için kendileri için özel olarak üretilmiş akıllı kartlarını kullanmaktadırlar. Ayrıca elektronik işlemlerde bütünlük ve inkâr edememe hizmetlerini vermek

amacıyla elektronik imza işlevleri uygulamaya dahil edilmiştir. Bu amaçla Tübitak Bilten tarafından geliştirilen Zeugma Açık Anahtar Altyapısı yazılımı kullanılmıştır. (Karakoçak, 2005)

4.4.1.4 Sağlık Hizmetleri Alanında Elektronik İmzanın Kullanılması

Sağlık hizmetleri, hizmetin verilmesinden verilen hizmetin ödenmesine kadar pek çok aşamayı içeren, sürekliliği olan bir süreçtir. Böyle bir hizmetin entegre ve sürekliliği göz önüne alınarak yerine getirilebilmesi, bilgilerin etkin yönetilmesini gerektirir. İhtiyaç duyulan tüm bilgiler, doğru zamanda, doğru yerde ve doğru kişinin kullanımı için kolaylıkla ulaşılabilir olmalıdır. Böyle bir hizmetin elektronik imza kullanılarak güvenli bir ortamlarda yapılması aşağıda sıralanan bazı kazançları sağlayacaktır.

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

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

- Kağıt işlemlerini azalttığı için toplam maliyeti düşürecektir.

- Eczacıya getirilen reçete yetkilendirilmiş kişiler tarafından yazılmış olacaktır. Böylece sahte reçete kullanımının önüne geçilecektir.

- Hekimlerin el yazılarının okunaksızlığı nedeniyle yanlış ilaç verilmesi durumunun önüne geçilecektir. Böylece yanlış ilaç sonucu zarar görmenin önüne geçilecektir.

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

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

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

-Reçete, rapor, hekim talimatı gibi hukuki sorumluluk isteyen belgelerin elektronik ortama taşınabilmesi için bu belgenin kimin tarafından oluşturulduğu ve oluşturulduktan sonra

değiştirilip değiştirilmediğinin saptanabilmesi gerekir. Satın alma gibi çeşitli bürokratik işlemlerde tarafların hukuki sorumlulukları vardır. Elektronik imza yardımı ile sağlık sektöründeki pek çok belge ve bunlarla ilgili süreçler elektronik ortama taşınabilecektir.

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

- Ayrıca bu bilgiler sayesinde daha önceden hastanın hangi rahatsızlıkları taşıdığı veya tedavi olduğu tespit edilebilecektir. (Karakoçak, 2005)

5 ELEKTRONİK İMZANIN ETKİLERİ

5.1 Ekonomik etkileri

Elektronik pazarlar, mal ve hizmetlere ilişkin geleneksel pazarlara paralel olarak ortaya çıkmış ve teknik gelişmeler doğrultusunda tüketim, üretim, pazarlama, ödeme gibi ticari işlem biçimlerini yeniden şekillendirmiştir. Elektronik ticaret, bu yeni pazarın anahtar elementi olarak görülmektedir. Firmadan müşteriye elektronik ticaretin, birkaç trilyon dolar düzeyine ulaşacağı tahmin edilmektedir. Bu düzeyde bir ekonomik hareketlilik elbette, tüm bilim dallarında olduğu gibi hukuk çevrelerinde de üst düzey bir heyecan yaratmıştır. Elektronik ticaretin boyutlarına ilişkin tahminler kimilerine göre çok yüksek kimilerine göre de çok düşük görünse de internetin açık bir ağ yapısı olması ve ticaret alanı olarak kullanılması yoluyla ekonominin küreselleşmesi unsurlarının, internet üzerinden gerçekleştirilen ticari işlemlerin, güvenlik, doğrulanabilirlik, gibi konularda hukuki sorunlar yarattığı görülmektedir. Firmalar ve tüketiciler de bu sorunlar çözümlere kavuşturulmadan, çok büyük oranlarda elektronik ticaret yatırımları yapmak konusunda çekingen davranmaktadırlar. Zira, dünyanın pek çok bölgesinde güvenlikli ve güvenilebilir bir online ticaret ortamı için yeterli garantiler sağlanamamaktadır. Buna bağlı olarak, güvenlik ile ilgili konular elektronik ticaretin daha yüksek boyutlara ulaşabilmesi için, hem ulusal hem uluslararası platformda çözüme kavuşturulmaktadır. Birbirlerini hiç görmemiş, coğrafi konumlarından habersiz, ticari durumlarını tespit edemeyecek kişi ve kuruluşlar, elektronik ticaret aracılığıyla alım satım, kiralama, danışmanlık, aracılık vb. her türlü hizmetin ticaretini yapacaklardır. Şu halde elektronik ortamda gerçekleştirilecek, her türlü işlemin güvenilirliğinin sağlanması, elektronik iletişimde doğrulanabilirliğin tespiti önemli olacaktır.

Elektronik devletin ve elektronik ticaretin güven noktası ve altyapısı olan elektronik imza, internetin ve teknolojilerin hızlı gelişimi, dünyada artan kullanıcı sayısı ve rekabet ortamı sayesinde, bilişim teknolojisi ve uygulamaları alanında kendisine oldukça önemli bir yer edinmiştir. Ancak elektronik imza ve uygulamaları, gerektirdiği teknolojik ve hukuki altyapıyla birlikte; sağladığı güvenlik, verimlilik ve tasarruf gibi faydaları ile yaygın hale gelmeye başlamıştır.

Günümüzde, yaklaşık bir tahminle, kurum ve kuruluşların % 90'ından fazlasının, iş süreçlerini kağıt belge ile yürüttüğü, dokümanların azımsanmayacak bir kısmının yanlış yerleştirilmiş ve bir daha bulunamayacak durumda olduğu, kullanıcıların haftada en az 8 saatini belge işlemleri için

bedensel hareket ile kaybettiği, belgelerin zaman içinde ortalama çok sayıda kopyasının yaratıldığı ve çalışanların zamanlarının büyük bir kısmını doküman yönetimine yönelik çalışmalara harcadığı söylenebilir. Özellikle kamu kurumları göz önüne alındığında bu kayıplar daha da artmaktadır. Elektronik imza bu anlamda birçok açıdan kurumlara ama özellikle kamu kurumlarına israf önleme ve verimlilik açısından büyük faydalar sağlamaktadır.

Elektronik imza ile; imzalanması gerekecek belgelerin ve yine kağıt ortamındaki kopyalarının taraflar arasında fiziksel olarak taşınması gerekmeyecektir. Bütün bilgi ve belgeler kullanıcıların izni dahilinde online olarak elektronik ortamdan taşınacak ve böylelikle kağıt tasarrufu sağlanabilecektir. Bu bilgi ve belgelerin taraflar arasında taşınması elektronik ortamdan yapılacağı için zaman tasarrufu da sağlanacaktır.

Elektronik imza altyapısının sağladığı güvenlik sayesinde bilgi ve belgelerin gizliliği sağlanacak ve bunun için önceden yapılan başka fiziki prosedürlere gerek kalmayacaktır. Ayrıca bilgi ve belgeler elektronik ortamda bir arşivde gizliliği sağlanarak tutulabilecek ve mevcut durumda kullanılan dosya, dolap ve arşiv odası gibi uygulamalarda tasarruf sağlanabilecektir.

Dolaysıyla kağıt ortamında yapılan belge yönetimine oranla elektronik ortamda yapılacak belge yönetimi çok daha etkili olacaktır. Zaman, mekan ve kağıt tasarrufu sağlandığında ise verimlilik artacaktır.

Elektronik imzanın ekonomiye etkilerini ;

- Düşük Maliyet,
- Karşılıklı işletilebilirlik
- İş süreçlerinin iyileştirilmesi,
- İş gücünün doğru kullanımı,
- Kağıt tüketiminde azalma,
- Daha düşük yönetim giderleri,
- Bilgi hırsızlığın azalması,

- Kayıt dışı ekonominin kayıt altına alınmasına katkısı,
- Verimliliğin artması,
- Telekomünikasyon giderlerinde azalma şeklinde sıralayabiliriz.(Karakoçak, 2005)

5.2 Sosyal Etkileri

Coğrafi, sosyo-ekonomik koşulları farklı kurumlar ve bireylerin, bilgi ve haberleşme teknolojilerine erişim olanakları açısından eşit konumda olmayışları bilgi çağının en önemli toplumsal problemidir. Birleşmiş Milletler Kalkınma Programı'nın İnsani Gelişmişlik Raporlarında da gündeme gelen aynı olanaklara erişim eşitsizliği ile ilgili olarak, 1997 yılında, "Bilgi ve iletişim alanındaki fırsatlar, kaynaklar ve erişim dağılımında gittikçe artan bir eşitsizliğin bulunduğu, gelişmiş ve gelişmekte olan ülkeler arasında bilgi teknolojileri ve bağlantılı uçurumun giderek derinleştiği ve bilgi yoksulluğu olarak adlandırılan bir çeşit yeni yoksulluk ortaya çıktığı" Birleşmiş Milletler tarafından açıkça ifade edilmiştir. BM gibi uluslar arası oluşumların yanı sıra, ulus devletler tarafından çeşitli tedbirlerin alınmaya çalışıldığı bu konuda sorun, aslında, maliyetin nasıl ve kimler tarafından karşılanacağına ilişkindir.

Elektronik imza bu duruma bir çözüm olmamakla birlikte, ulaşılabilirliğinin artması, bu uçurumu azaltmaya katkı sağlayacaktır.

Sayısal uçurumun engellenmesi bir yana, bilişim çağının önemli sorunlarından bir diğeri, bilgiye erişim olanaklarına sahip kesimin, içinde bulunduğu karmaşa ortamıdır ve adeta bilgi bombardımanının yanı sıra çok çeşitli saldırılara maruz kalan bireyin durumu güçtür. Olması gerektiği üzere, insan oğlunun iyiliği, refahı, mutluluğu için olduğu kadar, tam tersi yönde de kullanılabilen teknolojik gelişmelerin hızına ayak uydurması, hiç de kolay görünmeyen hukuki sistem eksikliği, varolan hukuk düzenlemelerinin de küresel çapta uygulanabilir olmayışı sonucunda, elektronik sahtekarlık gibi, her geçen gün çeşitlenen suçlar ortaya çıkmaktadır. Her türlü metin, görüntü, veri ve bilginin internet aracılığı ile denetimsiz biçimde akışı, küresel ağlara bağlı kitlelerin karşı karşıya kaldığı bahsi geçen tehlikeleri bertaraf edecek teknolojik çözümlerin de herkes tarafından etkin olarak kullanılamaması, hukukun ise yeterince cezalandırıcı ya da caydırıcı olamaması, ciddi bireysel ve toplumsal sorunlara neden olmaktadır. Bireysel bazda, aşırı bilgi yüklemesi ve bilgi kirlenmesi ile karşı karşıya kalan veya en hafifinden bilgi denizinde

boğulmama savaşı veren bilişim toplumu fertlerinin "doğru" ve "yararlı" bilgiye kolaylıkla ulaştığını söylemek artık zor bir olasılıktır.

Bu noktada elektronik imza, güvenlik, güvenilirlik ve reddedilemezlik sağlaması dolayısıyla bu problemlere teknolojik bir çözüm olarak düşünülebilir.

Endüstri toplumundan bilişim toplumuna geçişte "stratejik kaynak" sermaye olmaktan çıkmış, bilgi haline gelmiştir. Bugün en önemli kaynak olarak nitelenen bilginin, temelinde tüketimin yattığı endüstri çağında etkin olan diğer kaynaklardan farklılık gösteren özelliği, geleneksel manada tüketilir olmaması ve kullanılıp, paylaştıkça artan bir kaynak olmasıdır. Bilişim toplumunda endüstri çağının kimi üretim mekanlarının yerini bilgi merkezlerinin ve ağ ortamlarının almasıyla, fiziksel emeğin ikamesi, zihinsel emeğin ikamesi şekline dönüşmüştür. Bağlantılı olarak nitelikli çalışan ihtiyacı giderek artış göstermiş, her türlü eğitimin, önemi büyük ölçüde artarak, sosyo-ekonomik yapıdaki değişimin ardından yaratıcılık bağlamında niteliği, yaşam boyu sürekliliği bağlamında da, zaman boyutu değişiklik göstermiştir. Toplumun merkezi değişkenleri olan emek ve sermayenin yerini alan bilgi ile birlikte, Locke ve Smith'den Ricardo ve Marx'a dek birbiri peşi sıra gelen düşünürler tarafından formülleştirilen klasik "emek – değer" kuramı, yerini bir "bilgi-değer" kuramına bırakmak durumunda kalmıştır.

Geleceğin toplumuna bırakılacak en önemli miras, "kirletilmemiş" bilgi kaynakları olacaktır. Bilginin stratejik kaynak ve bilgi toplumunun temel değeri olması, bu kaynağın kirletilmeden korunmasını gerekli kılmaktadır. Elektronik imza da toplumun bu önemli kaynağını koruyan bir yapıdır.

Teknolojik değişim, ancak ve ancak yer aldığı sosyal yapı bağlamında anlaşılabilir. Bağlantılı olarak, sürekli ve son derece hızlı gelişen teknolojilerin, yeni yaşam biçimlerini belirleyen en önemli unsurlardan biri olduğuna dair şüphe yoktur. Bilgi devrimi olarak nitelenen olgunun da temelinde yatan yeni teknikler, yeni enerji türleri, yeni üretim biçimleri ve güçleri, toplumsal değişime önayak olur ve yapı derinden etkilenir. Öte yandan, mekanizasyon, endüstri devrimi için ne anlama geldiyse, bilgisayar teknolojisi de, bilgi çağı için aynı anlamı taşımakta ve önceden işçiler tarafından yerine getirilen fonksiyonları içerdiği için tehdit eder nitelik taşımaktadır.

Bugünkü ekonomik düzende "Bilgi", klasik üretim faktörlerini geride bırakarak birinci sıraya yerleşmiş, diğerleri arasında yerini nispeten koruyabilen faktör ise maddi sermaye olmuştur. Gelişmiş ülkelerdeki sermaye, bilgiyi hem izleyip, hem de beraberinde taşıyarak teknolojik ve hukuksal yapısı elverişli, işgücü potansiyeli yüksek, gelişmekte olan pazarlara yönlenmiştir.

Elektronik imzanın yaygınlaşması, iş yapış tarzlarını daha verimli ve etkin bir yönde değiştirecektir. Uygun hukuksal ve teknolojik altyapı kurulabilirse, ülkemize sermaye akışı sağlamaya yardımcı olabilir.

Internet ve teknolojik alanda yaşanan gelişmelerin hızına, hele ki coğrafi sınırların mevzu bahis olmadığı bir ortamda, hukuksal düzenlemeler vasıtasıyla hele ki uluslararası etkinlikte olacak şekilde yetişilmesi mümkün olamamaktadır. Internet üzerinden işlenen suçlar her geçen gün çeşitlenip, yaygınlaştıkça mevcut hukuk sistemlerinin yetersizliği daha da net anlaşılmıştır.

Her zaman ve her yerden anında kurulabilen küresel çapta iletişim sayesinde bilişim çağında zaman ve mekanın boyutları ve anlamları da değişime uğramıştır.

Enformasyonun, kültürü güce dönüştürebileceği düşüncesinde olan Castells'e göre; "Bilgi çağının güç savaşları, kültür savaşlarıdır. Gücün kaynağı olarak kültür ve sermayenin kaynağı olarak güç, bilgi çağının yeni sosyal hiyerarşisinin temelini oluşturmaktadır"

Bilişim toplumu üzerine çalışmaları ile tanınan Masuda'ya göre sanayi toplumunun siyasal sistemi olan "Parlamenter Demokrasi", bilişim toplumuna dönüşümle birlikte yerini, "Katılımcı Demokrasi"ye bırakacaktır. Nitekim, günümüzde, bilişim toplumu olgusunun savunucuları, bireyin ve sivil toplumun, politikaların belirlenmesine etki etme ve böylelikle kendi geleceklerine sahip çıkma potansiyelinin her geçen gün arttığını ileri sürmektedirler. Öte yandan, kullandıkça sürekli izlenebilir hale gelen birey ve kitleler hakkında üretilecek ve derlenip değerlendirilebilecek olan bilgilerin kontrolünü elinde bulunduranların çok büyük güç sahibi olduğu açıktır.

Elektronik imza ile ilgili düzenlemeler, bu gücün hukuksal çerçevede kontrolünü sağlamaktadır. Katılımcı demokrasiye ulaşılması konusunda elektronik imza önemli bir basamak teşkil etmektedir.(Karakoçak,2005)

5.3 Elektronik İmza Kanunu ve Yansımaları

Elektronik imza ve özellikle güvenli elektronik imza ve elektronik sertifika hizmet sağlayıcısı gibi, elektronik imza usulünde gerekli unsurlar Kanunda ayrıntılı olarak düzenlemekle birlikte, elektronik belge tanımı bulunmamaktadır.(Keser,2004)

5.3.1 Borçlar Kanunu'na Olan Yansımalar

5070 sayılı Elektronik İmza Kanununun 22. maddesine göre, Borçlar Kanununun 14. maddesinin birinci fıkrasına eklenen cümle şöyledir: "Güvenli elektronik imza elle atılan imza ile aynı ispat gücünü haizdir". Böylece Elektronik İmza Kanununun 5. maddesindeki istisnalar dışında her türlü hukuki işlem güvenli elektronik imza ile oluşturulabilecektir. Kanunun 5. maddesinin II. fıkrası şöyledir: "Kanunların resmî şekle veya özel bir merasime tabi tuttuğu hukukî işlemler ile teminat sözleşmeleri güvenli elektronik imza ile gerçekleştirilemez." (Keser,2004)

5.3.2 Hukuk Usulü Muhakemeleri Kanunu'na Olan Yansımalar

5070 sayılı Elektronik İmza Kanununun 23. maddesiyle Hukuk Usulü Muhakemeleri Kanununa 295. maddeden sonra gelmek üzere 295/A maddesi eklenmiştir. Bu maddenin birinci fıkrasına göre, "Usulüne göre güvenli elektronik imza ile oluşturulan elektronik veriler senet hükmündedir. Bu veriler aksi ispat edilinceye kadar kesin delil sayılırlar." İkinci fıkrada ise güvenli elektronik imza ile oluşturulmuş verinin inkarı durumunda nasıl bir inceleme yapılması gerektiği konusunda Hukuk Usulü Muhakemeleri kanununun 308. maddesine kıyas yoluyla uygulanmak üzere atıf yapılmıştır. Bu fıkraya göre, "Dava sırasında bir taraf kendisine karşı ileri sürülen ve güvenli elektronik imza ile oluşturulmuş veriyi inkâr ederse, bu Kanunun 308. maddesi kıyas yoluyla uygulanır."

308 inci madde ;"Davanın esnayı tahkikında bir taraf kendisine nispet olunan senette muharrer yazı ve imzayı inkar veya tanımadığını beyan ederse iki tarafın ifadatı ve olbapta serdolunan deliller üzerine hakim kafi derece kanaat hasıl eylediği takdirde senedi kabul veya hükümden ıskat ederek esas hakkında karar verir. Kanaat hasıl olmazsa hakim iki tarafın tayin olunacak günde bizzat ispati vücut etmelerine karar verir. Her iki taraf muayyen günde mütekabilen senet hakkında izahat ita ve medarı tatbik olacak evrakı irae ve tayin ve yazı ve imzanın mevsukiyetini

ne şekilde ve ne vasıta ile ispat edebileceklerini beyan ederler." Şeklinde olup elektronik imzada bu hükmün kıyasen uygulanmasında sıkıntılar yaşanabilir.

Hukuk Usulü Muhakemeleri Kanunu'nun 295/A maddesine göre inkar edilen husus "güvenli elektronik imza ile oluşturulmuş veri"dir. Maddenin birinci fıkrasına göre de bu veriler senettir. Bu nedenle imza değil, senet inkar edilmiş olmaktadır. Oysa, kıyasen uygulanacak olan 308 inci madde imza inkarını düzenlemektedir.

308 nci maddenin imza inkarı olarak yorumlanması halinde bile sorunlar yaşanacaktır. 308 nci maddeye göre; imza inkarı halinde hakimin önce tarafları dinlemesi ve gösterdikleri delillerle bir kanaat edinmeye çalışması, yeterli kanaat elde edemezse yeni bir duruşma günü belirleyerek iki tarafın bizzat duruşmada hazır bulunmalarını istemesi, tarafların da duruşmada uygulamaya elverişli belgeleri belirtmesi, göstermesi ve iddialarının doğruluğunu ne şekilde ve hangi vasıta ile ispat edeceklerini mahkemeye bildirmesi gerekmektedir. Nitelikli elektronik sertifikaya dayalı elektronik imzanın doğruluğunun tarafların beyanları ile anlaşılması veya ıslak imzada olduğu gibi tarafların uygulamaya elverişli bir belge sunmaları mümkün değildir. Mahkemeye sunulabilecek tek belge güvenli elektronik imzanın dayanağı olan nitelikli sertifika veya sertifika hizmet sağlayıcısından alınan ve güvenli elektronik imzanın geçerliliğine ilişkin sunacağı bir belge olabilir. Ama sertifika hizmet sağlayıcısı bir kamu otoritesi, bir noter olmadığına göre vereceği belgenin mahkemece kabul edilip edilmeyeceği de tartışma konusu olabilir. (Keser,2004)

5.3.3 İcra İflas Kanunu'na Olan Yansımalar

Elektronik imzalı belgelerin İcra ve İflas Kanunu (İİK) bakımından durumları ise şu şekilde değerlendirilebilir. Elektronik imzalı belgeler İİK.nın 68. maddesinde düzenlenen itirazın kesin kaldırılması bakımından imzası ikrar edilmiş bir senet sayılacak mıdır? Elektronik belgelerin, elektronik imzayla oluşturuldukları takdirde icra mahkemesindeki yargılamada imzası ikrar edilmiş senet olarak ibrazının nasıl mümkün olacağı ve icra mahkemesinin bu senedi incelemeye yetkili olup olmadığı değerlendirilmelidir.

Bu durum imzanın güvenli imza olması veya bu imza dışında kalan herhangi bir elekt-ronik imza çeşidiyle belgenin oluşturulmuş olması tartışmasından ziyade, elektronik belgelerin senet niteliğine (özellikle yazılılık ve cisim bulmuş olma unsurları açısından) sahip olup olmadığıyla

ilgilidir. Elektronik imzalı belgenin senet niteliği kabul edildiği takdirde, senedi imzalayan kişi tarafından imzanın ikrar edilmesi durumunda bu elektronik belge 68. madde anlamında belge olarak değerlendirilebilir. Buna karşılık, imzası ikrar edilmiş elektronik belgenin, senet özelliklerini taşımaması sebebiyle itirazın kaldırılmasında sınırlı inceleme yetkisi olan icra mahkemesi tarafından incelenmesi mümkün olamayacaktır. Çünkü, elektronik formda ibraz edilen, elektronik belgenin icra mahkemesince görülüp algılanabilmesi ve itirazın kaldırılması konusunda kanaat edinilebilmesi için bilirkişinin yardımı zorunludur. Bu sebeple hangi çeşit imzayla imzalanmış olursa olsun, imzası ikrar edilmiş elektronik imzalı belge icra mahkemesinin sınırlı inceleme yetkisi sebebiyle itirazın kaldırılması aşamasında 68/I anlamında belge olarak nitelendirilemez.

Bundan başka, alacaklı takip talebi ile senedin aslını vermemişse itirazın kaldırılma-sında, senedin aslını vermelidir. Fotokopi veya faks senet olmadığı için alacaklının itirazın kaldırılmasında bu belgelere dayanması mümkün değildir. Aynı şekilde senedin mikro filmi de tek başına itirazın kaldırılması için yeterli değildir .

Buna karşılık, alacaklının senet fotokopisini ibrazı halinde, fotokopinin borçlu tarafın-dan kabul edilmemesi durumunda icra mahkemesi tarafından fotokopinin değerlendirilemeyeceği görüşü dikkate alındığında borçlu tarafından fotokopinin kabul edilebileceği sonucu çıkmaktadır. Elektronik imzalı belge çıktısının bu anlamda itirazın kaldırılmasına yarar bir belge olduğu düşünülebilir. Çünkü, elektronik belgenin çıktısı, icra mahkemesi tarafından, görülüp algılanabileceği için, incelenebilecektir. Belgenin çıktısının, senedin özelliklerinden olan cisim bulma ve yazılılık niteliklerini karşıladığı söylenmelidir. Senedin diğer özelliği olan, imzanın bulunması unsurunun ise borçlu tarafından elektronik belgedeki imzanın ikrar edilmesi sonucu karşılanmış olduğu düşünülebilir. Ancak bütün bu söylenenler bakımından, takibin dayanağının itirazın kaldırılması duruşmasında ibraz edilen elektronik belge olması gerektiği belirtilmelidir.

Elektronik imzalı belgedeki imza inkarı durumunda ise icra mahkemesinin bu imzayı İcra İflas Kanununun 68/a maddesine göre incelemesi mümkündür. (Keser,2004)

5.3.4 Bankalar Kanunu'na Olan Yansımalar

Bankalar Kanununun, hesap ve kayıt düzeni başlıklı 13. maddesinin beşinci fıkrasında, bankaların, 213 sayılı Vergi Usul Kanunu hükümleri saklı kalmak kaydıyla, aldıkları yazılarla

faaliyetleri ile ilgili belgelerin asıllarını veya mümkün olmadığı hallerde sıhhatlerinden şüpheyi davet etmeyecek kopyalarını ve yazdıkları yazıların makine ile alınmış suretlerini tarih ve numara sırası ile düzenleyerek usulleri dairesinde saklamak zorunda oldukları düzenlenmiştir. Bu belgelerin Kurulca tespit olunacak usûl ve esaslar çerçevesinde mikrofilm, mikrofiş şeklinde veya elektronik, manyetik veya benzeri ortamlarda saklanmaları mümkündür. Bankaların yönetim kurulu kararları ile yurtdışında kurulu bankaların Türkiye'deki şubelerinin müdürler kurulu kararları, aralarında açıklık bırakılmamak ve satır aralarında çıkıntı olmamak şartıyla, tarih ve numara sırasıyla 29/6/1956 tarihli ve 6762 sayılı Türk Ticaret Kanununun defterlerle ilgili hükümleri gereğince onaylanmış müteselsil sayfa numaralı ayrı birer deftere metnin doğruluğundan hiçbir şekilde şüpheyi davet etmeyecek şekilde günü gününe kaydedilir ve her kararın altı üyeler tarafından imza olunur. İş hacimleri büyük olan bankalarda Kurumun izni ile ve yıl sonlarında ciltlettirilmeleri kaydıyla karar defterleri yerine yaprakları noterce tasdikli ve müteselsil sıra numaralı ayrı kalamoza kullanılabilir.

Bu fıkrada belgelerin saklanması ve karar defterleri ile ilgili bir düzenleme mevcuttur. Bankaların saklama zorunluluğu olan defter ve belgelerin fazlalığı sebebiyle bunların Maliye Bakanlığı'nın tespit edeceği şartlar çerçevesinde mikrofilm olarak saklanması imkanı getirilmiştir. Bankalar, belgelerin asıllarını veya bu mümkün değilse gerçekliklerinden şüphe duyulmayacak kopyalarını saklayabilirler. Bu düzenleme Bankalar Kanunu açısındandır. Mahkemelerde buna dayanarak, senetle ispat kuralları çerçevesinde her durumda belgelerin aslı yerine kopyasını ibraz etmek mümkün olmayacaktır. (Keser,2004)

5.3.5 Tüketicinin Korunması Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun'a Olan Yansımalar

Tüketicinin Korunması Hakkında Kanun 6.3.2003 tarihinde 4822 sayılı Kanun ile değiştirilmeden önce, mal, ticaret konusu taşınır eşya olarak tanımlanmıştı. Kanun değişikliğinde elektronik ticaret dikkate alınarak mal, "alış-verişe konu olan taşınır eşyayı, konut ve tatil amaçlı taşınmaz malları ve elektronik ortamda kullanılmak üzere hazırlanan yazılım, ses, görüntü ve benzeri gayri maddi malları", kapsayacak şekilde tanımlanmıştır. Tüketicinin korunması bakımından kanun koyucunun elektronik ortamda artan alış verişi gözardı etmemesi olumlu karşılanmalıdır.

Bundan başka, 4822 sayılı Kanunun 14. maddesi ile 4077 sayılı Kanuna 9. maddeden sonra gelmek üzere 9/A maddesi eklenmiştir. Bu maddede mesafeli sözleşmelere ilişkin düzenleme yapılmıştır. Kanuna göre, mesafeli sözleşmeler, yazılı, görsel, telefon ve elektronik ortamda veya diğer iletişim araçları kullanılarak ve tüketicilerle karşı karşıya gelinmeksizin yapılan ve malın veya hizmetin tüketiciye anında veya sonradan teslimi veya ifası kararlaştırılan sözleşmelerdir (TKK md.9/A/I).

Bu hükümle, elektronik ortamda ve tüketici ile karşı karşıya gelinmeksizin yapılan sözleşmeler Kanunun kapsamına alınmıştır. Ancak mesafeli satış sözleşmesinin elektronik ortamda yapılması durumunda da sözleşmenin yapılmasından önce, ayrıntıları Bakanlıkça çıkarılacak tebliğle belirlenecek bilgilerin tüketiciye verilmesi zorunludur. Sözleşmenin akdedilmesi için tüketicinin, bu bilgileri edindiğini yazılı olarak teyit etmesi gerekir. Elektronik ortamda yapılan sözleşmelerde teyit işleminin, yine elektronik ortamda yapılması mümkündür (TKK md.9/A/II). Elektronik ortamda yapılan mesafeli sözleşmeler bakımından, satıcı veya sağlayıcının elektronik ortamda tüketiciye teslim edilen gayri maddî malların veya sunulan hizmetlerin teslimatının ayıpsız olarak yapıldığını ispatla yükümlü olacağı belirtilmiştir (TKK md.9/A/IV). Aslında tüketicinin kendisine teslim edilen malın veya sunulan hizmetin ayıplı olduğunu ispat etmesi, genel kuraldan hareketle vakıadan lehine hak çıkaran (MK md.6) kişi olarak tüketiciye aitken, bu hüküm sonucunda, elektronik ortamda malın veya hizmetin ayıpsız teslim edildiğini ispatla yükümlü olan kişi satıcı ve sağlayıcı olacaktır. Böylece kanun tarafından ispat yükünün belirlendiği bir durum söz konusudur. (Keser,2004)

5.4 Elektronik İmzanın Toplumda Yaygınlaştırılması

5.4.1 Elektronik Bireyin Yeniden Tanımı

Bireylerin bilgisayar okuryazarı olması, hızla gelişen teknolojiden haberdar olması, bilgisayar kullanabilir olması, interneti kullanabilmesi, konumu veya mesleği gereği elektronik ortamda sunulan bir bilgiye erişme yollarını bilmesi ve o bilgiyi kullanabilme yetisine sahip olması, toplumu oluşturan bireylerin bilişim teknolojilerini kullanabilir donanımda olması o topluma hız ve dinamizm kazandırır.

Bilişim toplumunda elektronik kurumlar'ın oluşmasına paralel olarak ortaya elektronik birey oluşumları çıkacaktır. Yeni toplum yapılarında bireyler, teknolojileri yaşamlarının her evresinde büyük ölçüde kullanılır hale geleceklerdir.

Yaşamı boyunca, iletişimini istediği yer ve zamanda, elektronik ortamda kolaylıkla gerçekleştirebilen, katılımcı ve iletişimden öte oy verme dahil olmak üzere sanal ortamda gerçekleşebilecek tüm işlemlerini elektronik imza kullanarak bu ortamda yapmayı tercih eden, fikrini ve görüşünü paylaşabilecek yetenek ve motivasyona sahip kişi" yi elektronik birey olarak tanımlamak gerekir.

Elektronik birey**;** iş veya eğitim için araştırma yapmak, iletişim kanallarını kullanmak (elektronik posta, video konferans, anında mesaj), bankacılık hizmetlerini kullanmak, fatura ödemelerini yapmak, özel kurumlarla ilgili sunulan online hizmetleri kullanmak, devlet dairelerinin hangi hizmetleri verdiğini öğrenmek ve o hizmetten yararlanmak, potansiyel iş olanakları ile ilgili bilgi almak, herhangi bir konu üzerine yorum/şikayette bulunmak, oyun, eğlence kanallarını kullanmak, alışveriş yapmak gibi faaliyetleri elektronik ortamda da yapacak olan bireydir. Yaşamının her anında yapacağı bu faaliyetleri elektronik ortamda yapamayan birey, bilgi toplumunu bireyi olamayacağı gibi ülke ekonomisine de katkısı daha düşük bir birey olarak toplumda yerini alacaktır. (Karakoçak,2005)

5.4.2 Elektronik İmzanın Yaygınlaşmasını Engelleyen Bazı Hususlar

Elektronik imzanın toplumda yaygınlaştırılmasını sağlamak için öncelikle bireylerin elektronik imzanın ne olduğunu kavramaları ve elektronik yaşamla birlikte elektronik imza kullanımının hayatlarına getireceği kolaylıkları fark etmeleri gerekmektedir. Bu amaçla yapılacak etkinlikler;

Temel eğitim, Basılı ve görsel medya, Üniversiteler, Sivil toplum örgütleri aracılığıyla yapılabilir.

Temel eğitim: İlk ve orta öğretim kademelerinde mevcut müfredat programı içerisinde yer alan derslerin içeriğine elektronik devlet, e-dönüşüm ve elektronik imza kavramları eklenerek bu konuyla ilgili kavramların bu düzeyden başlanarak öğrencilere verilmesi sağlanmalıdır.

Basılı ve görsel medya: gerek günlük gazeteler ve süreli yayınlar gerekse radyo ve televizyon gibi yayın organları aracılığıyla vatandaşın elektronik imza konusunda anlayabilecekleri bir düzey ve şekilde bilinçlendirilmesi sağlanmalıdır.

Üniversiteler: Üniversiteler, öncelikle kendi içlerindeki elektronik uygulamalarda (öğrenci ve ders kaydı, not takibi, transkript, çıkış işlemleri gibi) elektronik imzayı kullanarak üniversite elemanları ve öğrencileri arasında e - imza uygulamalarını yaygınlaştırmalıdır. Bununla birlikte ilgili bölümlerde lisans düzeyinde kavramlar verilmeli, yüksek lisans düzeyinde de kavramların derinlemesine incelenmesi ve konuya özel akademik çalışmaların yapılarak sonuçların günlük hayattaki uygulamalara aktarılması sağlanmalıdır.

Sivil toplum örgütleri: Tüm sivil toplum örgütlerinin elektronik imza kavramı hakkında farkında olmanın artırılması, öncelikle kendi uygulamalarında elektronik imza uygulamalarını hayata geçirmeleri sağlanmalıdır. Farkında olmayı sağlamış sivil toplum örgütleri elektronik imzanın yaygınlaştırılması için hem vatandaşlar arasında yaygınlaştırma çalışmalarını sürdürmeli hem de konu ile ilgili yürütme organlarını sürekli takip etmeli ve üzerlerine düşen görevi yapmalıdır.

Elektronik imzanın yaygın olarak kullanıldığı alanları başında elektronik ticaret gelmektedir. Dolayısıyla elektronik ticaretin yaygınlaşması elektronik imzanın yaygınlaşmasıyla adete eş anlamlı olmaktadır. Bu itibarla, hukuksal kuralların ve kurumların, elektronik ticarette güvenliği ve güvenilirliği, şeffaflığı, ucuzluğu ve kolay erişilebilirliği sağlayacak biçimde tesisi devletin ikinci önemli rolünü oluşturmaktadır. Bu konu ile ilgili olarak;

- Elektronik işlemler sırasında açıklanan, kişisel verilerin gizliliği ve korunması konusunu da içeren ve Adalet Bakanlığı tarafından hazırlanan, "Kişisel Verilerin Korunması Kanun Tasarısının" bir an önce yasalaşması,

- Elektronik ödeme araçları arasında yer alan elektronik parayı çıkaracak olan kurum veya kurumlar ve bunlarla ilgili hukuki çerçeve ile elektronik paranın ihracına ilişkin koşulların belirlenmesi,

- Elektronik ödeme sistemlerinde faaliyet gösterecek operatörlerin saptanması, bu operatörler arasında yapılacak sözleşmeler açısından, Rekabet Kanunu'ndaki ilkeleri dikkate alan hukuki kuralların saptanması,

- Elektronik ödeme araçlarını verenler ile kullananlar arasındaki sorumluluk dağılımının, hukuken ve adil bir orantı gözetilerek tesisi; bu araçların çalınması veya kaybedilmesi halinde sorumluluk ve ispat yükü konularının düzenlenmesi,

- Elektronik ticaret ortamında, haksız rekabet, aldatıcı içerik ve reklamların irdelenmesi,

- Vergileme ilke ve kurallarının elektronik ticaret dikkate alınarak gözden geçirilmesi; ancak, vergileme konusundaki yaklaşımın, elektronik ticarete ilişkin ulusal politikanın belirlenmesinden sonra saptanması,

- Elektronik ticaret ortamının vergi denetimini güçleştirmesi nedeniyle, muhtemel vergi geliri kayıplarının telafisi için, iletişim teknolojisinin sunduğu olanaklardan da yararlanılarak yeni denetim yöntem ve tekniklerinin geliştirilmesi,

- İşyeri muhasebe kayıtlarında, elektronik ticaretin ayrı bir kalem olarak tutulmasını sağlayıcı düzenlemeler yapılması,

- Gümrüklerle ilgili olarak, fiziksel teslimin ucuz, kolay ve zamanında yapılmasını sağlayan tedbirlerin üzerinde durulması; Kyoto Sözleşmesi (Uluslararası Gümrük İşlemlerinin Basitleştirilmesi ve Uyumlaştırılması Sözleşmesi) ile ilgili çalışmaların yakından izlenmesi,

- Marka ve ticaret adları ile ikinci derece alan isimleri arasında çıkacak uyuşmazlıkların çözüm yeri, şekli ve ikinci derece alan isimlerinin devri ile ilgili kuralların belirlenmesi; marka, işletme adı ve unvanına ait veri tabanlarının kamuya açılması; özellikle markalar konusunda uluslararası bir çözüm arayışının gerekliliği ve ülkemizin bu hususu yakından izlemesi. (Karakoçak,2005)

Tablo 5.1 Dünyanın Türkiye hakkındaki verileri (Orta,2007)

	Değer	Kaynak	Yıl	Sıralama
Nüfus	73,197,200	internetworldstats.com	2003	
İnternet Kullanıcı Sayısı	2,500,000	nationmaster.com	2002	36/162
	4,900,000	internetworldstats.com	2003	
Kişisel Bilgisayar Sayısı	2,500,000	nationmaster.com	2000	
	2,700,000	Birleşmiş Milletler	2001	
Internet Ana Bilgisayarı	1,100,000	nationmaster.com	2003	64/119
ISP Sayısı	50	nationmaster.com	2001	19/28
20 saat internet kullanımının ortalama maliyeti	11,20$		2001	
e-Devlet Projesi Sayısı	200	Brown Üviversitesi	2003	
e-Devlet Olgunluk Düzeyi	56/190	Birleşmiş Milletler	2002	56/190

	83/196	Brown Üviversitesi	2001	83/196
	51/178	nationmaster.com	2003	51/178
e-Devlet Performansı	6/198	Brown Üviversitesi	2003	

5.4.2.1 Teknolojiden Kaynaklanmakta Olan Uygulama Güçlükleri:

Anahtar ve sertifika üretimi, dağıtımı, yenilenmesi, iptali, genel olarak anahtar ve sertifikaların yönetilmesi karmaşık bir süreçtir. Sertifika hizmet sağlayıcıları, sertifika yönetimi altında sertifika başvurularının gerçekleştirilmesi, sertifikaların üretilmesi, yenilenmesi, yayınlanması, gerek duyulduğunda iptal edilmesi ve tüm bu işlemlere ilişkin ayrıntılı kayıtları tutmak durumundadır. Sertifika başvurularının güvenilir bir biçimde yapılmasının sağlanması, gerçek kişilere doğru sertifikaların verilmesinde son derece önemlidir. Sertifika üretim süreci, azami fiziki, teknik ve idari güvenlik içinde gerçekleştirilmelidir. Hizmet sağlayıcının gizli anahtarına izinsiz erişim, telafisi güç sorunlara neden olur. Sertifikalar yaşayan bir sistemin en önemli unsurlardır. Genellikle bir yıl geçerlilik süresi verilen sertifikaların, süresi tamamlanmadan önce aynı anahtar çiftiyle yenilenmeleri veya yeni bir sertifikanın alınmasına ihtiyaç olacaktır. Süresi içinde olmasına karşın, bir sertifikanın çok farklı nedenlere dayalı iptali gerektiğinde, bu zaman yitirmeden ve güvenli bir biçimde hizmet sağlayıcı tarafından yapılabilmelidir.

Sertifika sahiplerinin gizli anahtarlarını korumaları için yeterince bilinçli olmaları, uygun araçları bu amaçla kullanmaları ve sistemin işleyişine ilişkin genel de olsa bilgi sahibi olmaları gerekmektedir. Aksi halde, imzadan doğacak yasal sorumlukların işletilmesinde ciddi sorunlarla karşılaşılabilir. (Karakoçak,2005)

Tablo 5.2 Gelir dağılımı ve bilgisayar sahipliği (Orta,2007)

Gruplar	Alt	Alt Orta	Orta	Üst Orta	Üst
Gelir Durumu (%)	42	33	14	8	3
Bilgisayar Sahipliği(%)	2	8	24	44	65

5.4.2.2 Yüksek Uygulama Maliyetleri

Açık anahtar sayısal imza teknolojilerinin yaygınlaşmasının önündeki diğer bir engel olarak, potansiyel kullanıcı kitlesinde belirli düzeyde bir bilgi birikimi gerektirmesidir. Teknolojinin karmaşıklığı nedeniyle kullanıcı, bilinçli bir kullanım düzeyi için en azından sertifika hizmet sağlayıcısının uygulama ilke ve esasları hakkında bilgi sahibi olmalıdır. Aksi takdirde, elektronik imza kanunuyla kendisine yüklenmiş sorumlulukları taşımasında güçlükler olacaktır. İmzanın olası ağır ve bağlayıcı sonuçlarıyla birlikte teknolojinin karmaşıklığı ve kullanım güçlüğü bir araya geldiğinde, kullanıcının gerçekten istekli, bilinçli ve bilgili olması zorunlu hale gelmektedir. (Karakoçak,2005)

5.4.2.3 Bilgi ve Bilinç Eksikliği

Açık anahtar sayısal imza teknolojileri yüksek maliyetli bir uygulamadır. Sertifika hizmet sağlayıcısı, sistemin gerektirdiği güvenliği sağlamak üzere bina, yazılım, donanım ve iletişim altyapısı yatırımı yapar; hizmette beklenen kaliteyi sağlamak üzere yüksek işletme giderleriyle karşı karşıya kalabilir. Bir yanda yasaların öngördüğü standartları yakalamak üzere çalışırken öte yanda rekabetçi bir ortamda yaşayabilmek için yüksek Pazar payı elde etmeye çalışır.

Sertifika kullanıcıları, kart, okuyucu ve token gibi yazılım ve donanım gereksinimlerinin yanı sıra, sertifikalara da belli bir ücret ödemek durumundadır. Sertifikadan sertifika sahibine veya diğer kişilere doğabilecek zararlar için mali sorumluluk sigortası yaptırılması bir zorunluluktur; bu durumda sertifika maliyetleri daha da artar. Sertifikaların geçerlilik süresi sonunda yenilenmeleri, iptal durumlarında yenilenmeleri diğer ek maliyet unsurlarıdır. (Karakoçak,2005)

Tablo 5.3 Dünyada internet kullanım sıralaması (Orta,2007)

Ülke	İnternet kullanıcısı (milyon kişi)	Nüfusa oranı (%)
1. ABD	202.9	68.5
2. Çin	103.0	67,9
3. Güney Kore	31.6	63.3
4. Japonya	78.0	60.9
5. Almanya	47.1	57.0
6. Hindistan	39.2	56,6
7. İngiltere	35.8	53.8
8. İtalya	28,6	48.8
...		

24. Türkiye	7,3	9,9

6 SONUÇ

Elektronik imza, eskiden filmlere konu olan ancak günümüz dünyasında artık bir ihtiyaç haline gelen dijital ortamlarda bilgi alışverişinin temelinde yerini almıştır. Artık devletler vatandaşına daha fazla imkan sağlayabilmek için daha hızlı iletişim araçlarını tercih etmektedir. Bu da elektronik ortamın güvenilir olarak kullanılması, daha korunaklı hale getirilmesi yoluyla olmaktadır. Elektronik imza tam bu noktada iletişimin güvenliğini sağlamak için devreye girmektedir. Dağıtımın ve ulaştırmanın güvenliğini koruma görevi üstlenen sistem tam bir kapalı kutu olarak çalışmayı sürdürmektedir. Bünyesinde dış etkenlerden etkilenmeyecek bir sistem barındırması gereken elektronik imzanın kullanıcıların;

- İmzalayanın tanımlanması

- Veri bütünlüğünün kontrol edilmesi

- Gizliliğin korunduğunun teyidi

- İnkar etmenin engellenmesi

- Zamanlama bilgisi

gibi ihtiyaçlarını da karşılaması gerekmektedir. Bunlar elektronik imza üreticilerince kullanıcılara sağlanan hizmetlerdir. Günümüzde elektronik imza her alanda faaliyet gösterme adayı olup teknoloji ile içiçe yaşayan kurum veya bireylerin kaçınılmazı olmuştur. Elektronik imza sadece yüksek maliyeti ile sınırlı kullanıcılara hitap eden bir sistem bütünü olmaktan çıkarılıp herkes tarafından kullanılabilecek seviyeye getirilmesi gereklidir. Bunun önündeki bazı büyük engeller;

- Teknolojiden kaynaklanmakta olan uygulama güçlükleri

- Yüksek uygulama maliyetleri

- Bilgi ve bilinç eksikliği olarak sıralayabiliriz. Bu engellerin aşılarak elektronik imzanın toplum hayatına geçirilmesi durumunda bir bütün olarak devlet daha fazla verimli bir hale gelecektir.

7 KAYNAKLAR

ARIFOĞLU, Ali, e-Dönüşüm Yol Haritası, Dünya, Türkiye, 2004
ÇAMURDAN, Çiğdem, "Elektronik İmza Kanunu Tasarısı Üzerine Bir Değerlendirme", http://dergi.tbd.org.tr/yazarlar/26052003/cigdem_camurdan.htm

Ford, W. (2000) Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption

Genç, H.(2006) http://www.bilmuh.gyte.edu.tr/~ispinar/BIL673/PKI-problems.pdf

Grant, G.L. (1997) Understanding Digital Signatures: Establishing Trust Over the Internet and Other Networks

Hammond, B. (2002) Digital Signature

İnalöz, A. (2003) http://www.tk.gov.tr/Yayin/Uzmanlik_Tezleri/tktezler/Ayse_Inaloz_Tez.pdf

Kandur, H. (2006) http://www.devletarsivleri.gov.tr/EBYS_v_2_0.pdf

Karakoçak, K. (2005) http://www.e-imza.gen.tr/templates/resimler/File/arastirma_dosyalari/E-IMZANIN_TOPLUMSAL_BOYUTU.doc

Katz, J. (2008) Digital Signatures (Advances In Informatıon Securıty)

Keser Berber, L. (2004) http://bthukuku.bilgi.edu.tr/documents/e-imza_hukuk_calisma_grubu_raporu.pdf

KESER BERBER, Leyla, (2000), "İmzalıyorum O Halde Varım", Dijital İmza, Dijital İmza Hakkındaki Yasal Düzenlemeler, Dijital İmzalı Belgelerin Hukuki Değeri, TBB Dergisi, 2000/2, s.503–556

Keser Berber, L. (2002) İnternet Üzerinden Yapılan İşlemlerde Elektronik Para ve Dijital İmza

Orta, M. (2005) Elektronik İmza ve Uygulaması

Orta, M. (2007) E – kavramlar, Uygulamalı Elektronik İmza Semineri

Orta, M. (2007) http://www.e-ticaret.gov.tr/Toplanti/T%C3%BCrkiyede%20Elektronik%20imza%20Uygulamari.doc

Sağlam, İ. (2007) Elektronik Sözleşmeler

Schellekens, M.H.M. (2004) Electronic Signatures: Authentication Technology from a Legal Perspective

Piper, F. Blake-Wilson, S. (2000) Digital Signatures Security and Controls

Tüfekçi, T. (2003) http://www.bilten.metu.edu.tr/Web_2002_v1/common/yayinlar
/Elektronik_imza_nicin_yayginlasamiyor-ppt.pdf
Diğer Kaynaklar

http://www.tbb.org.tr/turkce/mevzuat/5070/e-imza%20kanunu.doc

http://www.tk.gov.tr/Tuketici/Sorulanlar/Sorulanlar.htm#eimzasss

http://www.kamusm.gov.tr/tr/Bilgideposu/Belgeler/

http://www.tk.gov.tr/eimza/eimza_mevzuat.htm

http://www.adalet.gov.tr/duyurular/2007/nisan07/eimza/protokol.htm

http://www.ueimzas.gazi.edu.tr/pdf/poster/72.pdf

http://www.bilgitoplumu.gov.tr/OECD.asp

8 ÖZGEÇMİŞ

Doğum tarihi		10.05.1982
Doğum yeri		Çorum
Lise	1997-2001	Kuleli Askeri Lisesi
Lisans	2001-2005	Kara Harp Okulu
		Sistem Mühendisliği Bölümü

Çalıştığı kurumlar

2005-2007	Kara Kuvvetleri Komutanlığı bünyesinde takım komutanlığı