T.C.
BEYKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANA BİLİM DALI
BİLGİSAYAR MÜHENDİSLİĞİ BİLİM DALI

BAZI DEVLET KURUMLARINDA ELEKTRONİK İMZA UYGULAMASI ve KARŞILAŞILAN SORUNLAR

(Yüksek Lisans Tezi)

Kevser ŞAHİNBAŞ

İstanbul, 2009

T.C.
BEYKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANA BİLİM DALI
BİLGİSAYAR MÜHENDİSLİĞİ BİLİM DALI

BAZI DEVLET KURUMLARINDA ELEKTRONİK İMZA UYGULAMASI ve KARŞILAŞILAN SORUNLAR

(Yüksek Lisans Tezi)

Hazırlayan;
Kevser ŞAHİNBAŞ
060820008

Danışmanı;
Prof.Dr.İlhami YAVUZ

İstanbul, 2009

T.C.
BEYKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜ
TEZLİ YÜKSEK LİSANS TEZ SINAV TUTANAĞI

31/07/2009

Enstitümüz Bilgisayar Mühendisliği Anabilim Dalı Bilgisayar Mühendisliği Bilim Dalı yüksek lisans öğrencilerinden 060820006 numaralı **Kevser ŞAHİNBAŞ'** ***a*** *"Beykent Üniversitesi Lisansüstü Eğitim - Öğretim Yönetmeliği'*nin ilgili maddesine göre hazırlayarak, Enstitümüze teslim ettiği ***"Bazı Devlet Kurumlarında Elektronik İmza Uygulaması ve Karşılaşılan Sorunlar"*** *tezini*, Yönetim Kurulumuzun 02.07.2009 tarih ve 2009/08 sayılı toplantısında seçilen ve Fakülte binasında toplanan biz jüri üyeleri huzurunda, ilgili yönetmeliğin *(c) bendi gereğince* aday tarafından savunulmuş ve sonuçta adayın tezi hakkında **oybirliği** ile ***Kabul*** kararı verilmiştir.

İşbu tutanak Enstitü Müdürlüğü'ne sunulmak üzere tarafımızdan düzenlenmiştir.

DANIŞMAN
Prof.Dr. İlhami Yavuz
İ. Yavuz

ÜYE
Prof. Dr. Hüseyin CÖMERT

ÜYE
Yard. Doç. Dr. Zeynep ALTAN

ÖZET

Bu tezde, elektronik imzalama prosedürü, kullanılan algoritmalar ve bunların bazı devlet kurumlarında uygulanmasında karşılaşılan sorunlar ele alınmıştır. Ülkemizde elektronik imzalar gerçek kişilere verilmektedir, henüz tüzel şahıslar için bir kanun bulunmamaktadır. Fakat kurumsal olarak kullanılan elektronik imza örnekleri yaygınlaşmaktadır. Örneğin bazı GSM operatörleri (Turkcell ve Avea), Nitelikli Elektronik Sertifika Hizmet Sağlayıcısı olan TÜBİTAK/UKAE, e-güven, e-tugra vb. firmalarla işbirliği yaparak bazı kamu kurumlarıyla elektronik imza uygulamaları yürütmektedir. Bu kurumlar arasında birçok bakanlıklar, büyük şehir belediyeleri, müdürlükler, bankalar bulunmaktadır.

Bu tezde, bazı kurumlara bizzat gidilerek veya online olarak elektronik imza uygulamaları ile ilgili bilgi alınmış, nelerin/nerelerde kullanıldığı, sistemin genel olarak nasıl çalıştığı ve geçerlilikleri, karşılaşılan sorunlar ayrıntılı bir şekilde incelenmiştir. Ayrıca bu inceleme sonucunda elektronik imzanın yeterince kullanılmadığı saptanmıştır. Çağdaşlığı yakalamak ve geri düşmemek için devlet ya da özel tüm kurumlarda elektronik imza uygulamasına geçilmesi zorunlu bir olgudur.

Anahtar Kelimeler: Elektronik imza, elektronik sertifika, Açık Anahtar Altyapısı, Hash fonksiyonu

ABSTRACT

In this thesis, electronic signature procedure, the algorithms that are used and the problems of electronic signature usage in some public institutions are analyzed. In our country, electronic signature has been allowed to people, and there have not been any laws for artificial people yet. However, electronic signature models that are institutionally used have increasingly been expanding. For instance, by cooperating with Electronic Information Security Corp. (E-Güven), TurkTrust etc., some GSM operators (Turkcell and Avea) and Governmental Certification Center (TÜBİTAK/UKAE) as an Electronic Communications Service Provider (ECSP) carry out electronic signature applications with some public institutions. Of all these institutions, there are a number of ministries, metropolitan municipalities, directorships and banks.

In this thesis, after researching about electronic signature applications through visiting some institutions and/or via online communication, it is circumstantially explored how the system is generally operated; what the admissibilities are; and which problems are encountered. Additionally, it is proved that electronic signature is not efficiently used in the institutions as a result of this study. Electronic signature application is a must in all of public and private institutions in order to contemporize the foundations of a society.

Key Words: Electronic Signature, Public Key Infrastructure (PKI), Hash Functions

İÇİNDEKİLER

KISALTMALAR LİSTESİ

Bu çalışmada kullanılmış bazı kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	**Açıklama**
A.G.E :	Adı geçen eser
A.g.m :	Adı geçen makale
AAA :	Açık Anahtar Altyapısı
AES :	Advanced Encryption Standard
DES :	Data Encyption Standart
DSA :	Digital Signature Algorithm
EİK :	Elektronik İmza Kanunu
ESHS :	Elektronik Sertifika Hizmet Sağlayıcı
HUMK:	Hukuk Usulü Muhakemeleri Kanunu
Md. :	Madde
MD :	Message Digest
NIST :	National Institute of Standart and Technology
PIN :	Personal Identification Number, veri erişim kodu
PKC :	Açık Anahtarlı Sifreleme (Public Key Cryptography – PKC)
RSA :	Rivest-Shamir-Adleman
SHA :	Security Hash Algorithm
TK :	Telekomünikasyon Kurumu
UEKAE:	Elektronik ve Kriptoloji Araştırma Enstitüsü Müdürlüğü

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

I. GİRİŞ

Gelişen bilgi teknolojisi sayesinde posta ile mektup yollamak veya yazılı sözleşme yapmak yakında tarihe karışacaktır. Artık, bilgisayar ağları ile sadece dosya transferi, e-mail gönderimi gerçekleştirilmemekte aynı zamanda büyük oranda ticari alışveriş yapılmakta hatta büyük sözleşmeler, antlaşmalar yapılmaktadır. Tapu sicili gibi kütük kayıtları, imar durumları, bina beyanları, evlenme müracaatları bile elektronik olarak yürütülmesi mümkündür. Internet üzerinden yapılan ticari alışverişin büyük oranda artması ve bu gelişmeler bilgisayar ağlarında güvenliği, güvenirliği ve geçerliliği gündeme getirmektedir. Bilgisayar teknolojisinin günlük yaşamımızın her aşamasına girmesi elektronik ortamda el yazısıyla imzayı ikame edebilecek bir yapı olan elektronik imzayı gerekli kılmıştır. Bunu gerçekleştirmek için güvenilir sistem arayışlarına gidilmiştir. Bu sayede gönderilen verinin veya e-postanın güvenli bir şekilde alıcısına iletilmesi amaçlanmış ve bunun teknikleri araştırılmıştır. Bunun yanında hukuki geçerliliğini sağlamak için teknik çalışmalara başlanmıştır. E-imzanın kanuni dayanağının olması bu anlamda önemlidir. Çünkü insanlar, herhangi bir haksızlığa uğradıklarında devletin bu haksızlığı kanunları çerçevesinde gidermesi ve bir çözüm bulmasını istemektedir. Internet üzerinde dolaşan bir bilginin hukuksal açıdan geçerli olması ve güvenliğinin sağlanması için; gizlilik, verinin şifrelenmesiyle, bütünlük, özetleme algoritmalarıyla, kimlik doğrulama ve inkâr edilmezlik özellikleri diğer bazı tekniklerin yanında elektronik imza ile sağlanmaktadır. Bu saydığımız özellikleri itibariyle çalışma konumuz olan elektronik imza, bilgiyi kimliklendirme açısından, son derece önemli bir yere sahiptir.

Elektronik imza, Açık Anahtar Altyapısını (AAA, PKI = Public Key Infrastructure) kullanmaktadır. AAA teknolojisi kullanılarak oluşturulan elektronik imzalama verisi kişiye ve imzalanan dokümana özeldir, bu nedenle başkaları tarafından taklit edilemez ve imzalı belge üzerinde değişiklik yapılamaz. İstenildiğinde elektronik imzanın doğruluğu kontrol edilebilir. Elektronik imza, imzalayan kişinin kimlik doğruluğunu ispatlar; imzalanan verinin içeriğinin başka bir şahıs tarafından değiştirilip değiştirilmediğini (bütünlüğünün bozulup bozulmadığını) ortaya koyar.

Özellikle e-devlet uygulamalarının hayatımıza kapsamlı ve etkili bir şekilde girmesi, günlük yaşamda resmiyet ihtiva eden iş ve işlemlerin hızlı, güvenli ve hukuksal

olarak geçerli mahiyette oluşturulması, e-imza ile mümkün olmaktadır. Elektronik imza altyapısı, elektronik belgenin şifrelenmesini mümkün kılmakta, değiştirilmesini önlemekte ve ayrıca birden çok kişi ile, mesajın şifrelendiği anahtar kelimeyi öğrenmelerine gerek kalmadan, elektronik yoldan haberleşmeyi kolaylaştırmaktadır [1]. Diğer yandan elektronik imza elektronik ortamda ihtiyaç duyulan, özellikle elektronik ticaret için zorunluluk arz eden güvenli bir yöntem olarak öne çıkmaktadır.

15 Ocak 2004 tarihinde kabul edilen ve 23 Ocakta Resmi gazetede yayınlanan 5070 nolu yasa sayesinde, e-imzanın hukuksal alt yapısı kanuni bir çerçeveyi kazanmış oldu. Yani, yapılan anlaşmalara attığımız imza nasıl bizi bağlıyorsa, yapacağımız e-anlaşmalara atacağımız e-imzalarda aynı kanuni çerçevede değerlendirilecektir. 2005 yılından itibaren yoğun bir şekilde kullanılması beklenen e-imza, bu kanunla birlikte, Türk Telekomünikasyon kurumunun denetimi altında yürütülmektedir. 5070 sayılı Kanuna göre elektronik imza "başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri"dir. Elektronik sertifikanın niteliklerinden, denetim ve izinsiz kullanıma, sertifika hizmet sağlayıcısının özelliklerinden sahtekârlık ve idari para cezalarına kadar akla gelebilecek bütün noktalar kanunda tanımlanmıştır. Konuyla ilgili bir takım eksiklikler bulunmaktadır ancak bunların zamanla aşılacağı öngörülmektedir. 1994'lü yıllarda bu yasayı çıkartan ve şu anda yoğun bir şekilde kullanan Amerika'ya, 1999 da bu yasayı çıkaran Singapur'a yetişmemiz ve dijital bölünmede e-ülkelerin yanında yer almamız ülkemiz için büyük bir önem taşımaktadır.

Elektronik imza tıpkı ıslak imzada olduğu gibi evrakla kişinin kimliği arasında bir ilişki oluşturur. Ancak elektronik imzanın ıslak imzaya oranla üstünlükleri vardır. Islak imzaya oranla taklit edilmeleri imkânsız denecek oranda zordur, sadece kişinin kimlik bilgisiyle değil ayrıca mesajın içeriğiyle de ilişkilidir. Mesajdaki en küçük değişikliklerde bile elektronik imza değişir. Bu nedenle mesajın bütünlüğünü (bir yerden bir yere giderken bozulmadan, değiştirilmeden, orijinal haliyle gitmesi) sağlamada oldukça önemli rol oynar. Elektronik ortamlarda hukuki geçerlilik kazandırılmak istenen her işlemde elektronik imza kullanılmalıdır.

Bu tez kapsamında, birinci bölümde elektronik imza şemaları, elektronik imzanın dayandığı temeller incelenmiş, el yazısı imza ile elektronik imza karşılaştırılmış, AA Şifreleme Sistemleri, Hash fonksiyonları ve sayısal imza algoritması üzerinde durulmuştur.

İkinci bölümde, yasalaşma sürecinde elektronik imza incelenmiş, hukuki boyutu anlatılmış ve hukuki delil niteliği tartışılmıştır.

Üçüncü bölümde, bazı kamu kuruluşlarında elektronik imza uygulaması örnekleri verilmiş ve karşılaşılan sorunlara değinilmiştir.

Dördüncü bölümde, Elektronik Sertifika konusu incelenmektedir. Ülkemizde Nitelikli Elektronik Sertifika Hizmet Sağlayıcısı olan firmalardan söz edilmiştir.

Beşinci bölümde, geleceğe ilişkin öngörülere yer verilmiştir. Kamu kurumlarında elektronik imzanın geleceğine yönelik bazı saptamalar verilmiş ve çözüm önerileri sunulmuştur.

Son bölümde, sonuç ve bazı tartışmalara yer verilmiştir.

II. ELEKTRONİK İMZA ŞEMASI

1. ELEKTRONİK İMZA, DAYANDIĞI TEMELLER VE ELEKTRONİK İMZANIN GERÇEK İMZA İLE KARŞILAŞTIRILMASI

1.1 Elektronik İmza Tanımı

Elektronik imza, klasik imzaya tanınan işlevleri de kapsayan ve bir veri mesajında bulunan veya ona eklenen ya da mesaj ile mantıksal bağlantısı kurulabilen, bireyin kimliğini tanıtan ve bireyin, mesajın içeriğini onayladığını gösteren elektronik formattaki imzadır [2].

1.2 Elektronik İmzalama Prosedürü

Dijital imzanın hazırlanması matematiksel alt yapısı ikinci kısımda verilecektir. Bu alt yapı ve ilgili algoritmalar bilgisayara yüklendikten sonra kullanım için bir mesajı bilgisayar ortamında imzalamak son derece kolaydır. Kısaca açıklamak gerekirse; göndermek istediğiniz mesaj hazır ise, bilgisayar ekranındaki “imzala” komutunu klikledikten sonra, “imza anahtarını yerleştir” komutunu göreceksiniz. Bunun için, bir onay makamının veya sertifika kurumunun (Trust Center, Certification Authorities) size verdiği chip kartını, kart okuyucuya soktuktan sonra işin geri kalan kısmı bilgisayarca halledilmektedir.

Dijital imzanın tasdik edilmesi de karmaşık bir işlem değildir. Bu işlemde önceden bilgisayara yüklenmiş algoritmalar yardımıyla bilgisayarca yapılmaktadır.

Bir belgeyi elektronik olarak imzalayabilmek için, kullanıcıların bir Onay makamının veya daha sık kullanılan İngilizce karşılığı ile “Trust Center’ın” hizmeti yanında teknik bir alt yapıya da sahip olunması gerekir. Kullanıcının bir bilgisayarı ve kendine ait bir yazılım programının mevcut olması gerekir. Kullanıcının ayrıca bilgisayar üzerinden yapacağı işlemlerde kullanacağı bir de şifresinin olması gerekir. Bu şifre yazılım programları vasıtasıyla veya akıllı kart (SmartCard) olarak da adlandırılan Chip kartlardan elde edilebilir. Chip Kartların çalınması veya kaybedilmesi durumunda, eğer kullanıcı bu durumu fark ederse, aynen kredi kartları uygulamasında olduğu gibi, Chip Kart Dağıtım Merkezine yapılacak bildirim ile, kart derhal bloke edilecektir.

Elektronik imza kişiye özel üretildiğinden iadesi söz konusu değildir. Ancak, Elektronik Sertifika Hizmet Sağlayıcısı, tüketicinin hiçbir hukuki ve cezai sorumluluk üstlenmeksizin ve hiçbir gerekçe göstermeksizin teslim aldığı veya Sertifika Kullanıcı

Sözleşmesinin imzalandığı tarihten itibaren yedi gün içerisinde teslim aldığı araçları veya hizmeti reddederek sözleşmeden cayma hakkının var olduğunu ve cayma bildiriminin satıcı/sağlayıcıya ulaşması tarihinden itibaren araçları geriye almayı taahhüt eder. Söz konusu mal, elektronik imza oluşturma aracı ve kart okuyucu aygıtlarıdır [3].

1.3 Elektronik İmzanın El Yazısıyla İmza ile Karşılaştırılması

Elektronik imza, el yazısıyla imza değildir. Aynı şekilde elektronik imzalı belgenin bilgisayar çıktısında da, el yazısı ile imzada bulunan karakteristik kişileştirme özelliği eksiktir. Bundan başka, elektronik imzada, metnin altında kişisel bir imza bulunmamakta, aksine, sadece, imza sahibinin kimliğinin tespiti için ek bir veriyle tamamlanmış şekli bulunmaktadır. Bu sebeple elektronik imzadan söz edildiğinde, el yazısıyla imza ile aynı olduğunu söylemek mümkün olmamaktadır.

Elektronik imzanın el yazısıyla imzayla eşdeğerliliği için, elektronik imzanın iki şartı sağlanması gerekir: İmzalayan kişinin kimliğinin tespiti ve imzalanan açıklama metni ile imza arasında bağlantı yani sonuçlandırma işlevi. Bu iki şart gerçekleştiği takdirde imzanın ispat fonksiyonu da sağlanmış olacaktır.

El yazısıyla imza ile elektronik imzanın işlevleri karşılaştırırken elektronik imzada ve daha spesifik olarak dijital imzada, veri güvenliğinin, el yazısıyla imzaya nazaran daha yüksek olduğu belirtilmelidir. Bu durum, dijital imzada verinin bütünlüğünün sonraki değişmelere karşı korunması; imzalayanın kimliğinin dolaylı da olsa tespitinin sağlanması; imza ile metin arasındaki bağın kolaylıkla ve güvenilir şekilde tespit edilebilmesi ve imzanın kontrolünün tamamen makine tarafından ve otomatik olarak yapılması özellikleri dikkate alındığında daha iyi şekilde görülebilecektir.

Elektronik imzalı belgelerle kâğıt belgeler arasında, imzalanmış irade açıklamasının sonradan değiştirilmesi bakımından da fark vardır. Kâğıt belgelerde taraflar, daha önce imzaladıkları belgeyi değiştirmek istediklerinde, eski belgeleri yok ederek yeni bir belge düzenleyebilirler. Buna karşılık elektronik imzalı belgelerde, kullanıcı yanlışlıkla imzalanmış belgeyi sildiğinde, silinmiş belge tekrar yapılandırılabilir. Bundan başka, elektronik ortamda dosyalar geçici klasörlere kaydedilirler. Elektronik belgenin, güvenli olarak silinmemesi problemi, en son

hazırlanan belge yerine, daha önce hazırlanmış belgelerin imzalanması problemini de gündeme getirir.

Kâğıt belgelerde, senette sonradan çıkıntı veya silinti yapılabilir. Bu çıkıntı ve silintiler, ayrıca imzalanmadığı takdirde, inkâr edilirse yok sayılır (Hukuk Usulü Muhakemeleri Kanunu (HUMK) md.298/I). Eğer, imzalanmamış çıkıntı veya silinti inkâr edilmişse ve mahkemece bu durumun senedin geçerliliğine etki edeceği kanaatine varılmışsa, senet kısmen veya tamamen hükümsüz sayılabilir (HUMK md.298/II). Elektronik imzalı belgelerde ise durum daha farklıdır. Bir elektronik imzalı belgeye ek yapıldığı veya belgedeki bir husus silindiği takdirde, elektronik belgenin değiştirildiği, elektronik imzanın kontrolü sonucunda anlaşılacaktır. Bu şekilde imza kontrolünün negatif çıkması, belgenin tarafların iradesi dışında değiştirildiği şeklinde yorumlandığından, belgenin gerçek olarak değerlendirilmesi mümkün olmayacaktır. Çünkü belge değiştirildiği takdirde imza bozulmaktadır. Bu sebeple eğer elektronik imzalı belgede değişiklik yapılmak isteniyorsa, bu belgenin yeniden elektronik olarak imzalanması gerekir. Bu haliyle elektronik belgenin en son hali geçerli kabul edilebilir; çünkü, belgenin içeriği sonradan tarafların rızasıyla değiştirilmiştir. Belgenin hangi halinin en son durumu yansıttığı sorusunun cevabı ise zaman damgası sayesinde verilecektir. Böylece elektronik belgedeki değişikliklerin, imza sahibi tarafların, yeniden imzası alınmaksızın yapılamayacağı sonucuna varılabilir. Hukuk Usulü Muhakemeleri Kanununda yer alan senetteki çıkıntı ve silintinin ayrıca imzalanması gerektiği şeklindeki kuralın elektronik imzalardaki görünümü bu şekildedir. Elektronik imzalı belgelerde, belgeye ek yapıldığı veya belgedeki bazı hususların silindiği konusunda, imza sahibi tarafın herhangi bir inkârda bulunmasına gerek yoktur. Çünkü zaten belgenin değiştirilmemiş olması, o belgeye güvenilmesi için gerekli koşullardan biridir. Buna karşılık, sözleşmenin sonradan değiştirildiğine ilişkin savunmalar, senede karşı senetle ispat zorunluluğu (HUMK md.290) çerçevesinde, başka bir elektronik imzalı belgeye yapılabilir.

Kâğıt belgelerde, belgede herhangi bir değişiklik yapılmışsa, çoğunlukla, inceleme sonucunda, nerede değişiklik yapıldığı saptanabilir ve belgenin değiştirilmeden önceki haline ulaşabilir. Buna karşılık elektronik belgelerde, belgenin değiştirilmeden önceki haline ulaşılması ve önceki durumunun tespiti mümkün değildir. Taraflar eğer elektronik imzalı belgenin bir örneğini bilirkişiye verebilirse,

bilirkişinin değiştirilmiş elektronik imzalı belgede hangi değişikliğin yapıldığı konusunda bir açıklama yapma şansı bulunacaktır.

Elektronik kavramı ile el ile yazılılık kavramları karşılıklı olarak birbirini dışta bırakmaktadır. Bununla birlikte, el yazısıyla imzaya ilişkin hükümlerin elektronik imzaya uygulanmasına ilişkin kıyas tartışılmıştır. Böyle bir kıyasın yerinde olduğu söylense bile, elektronik imza, el yazısıyla imzanın sahip olduğu bütün işlevlere eksiksiz şekilde sahip değildir. Elektronik imzanın el yazısıyla imza ile özleştirilmemesi pek çok sebeple açıklanmaktadır. Buna göre; elektronik imzada, el yazısı imza ile temin edilen, başka bir kişi ile karıştırılmayı engelleme, açıkça ve değiştirilmeyecek şekilde bir kişiye özgülenme, daha açık bir ifadeyle imzalayanın kimliğinin tespiti unsuru eksiktir. Bundan başka, hukuki ilişkiye katılan kişinin, el yazısıyla imzada sahip olduğu bilinçle imzalama sürecini başlatması için şifre veya kod numarasını kullanması, el yazısı ile atılan imzayla henüz özleştirilemez. Ancak, örneğin, elektronik imza "pen-pad" üzerine el yazısı imza olarak atılırsa belki farklı şekilde bir karara varılabilir. Bunun için elektronik imzanın kullanımının ve bu bilincin yaygınlaşmasını beklemek gerekir. Bazı kullanıcılar, elektronik imza kullanırken, kendileri değil de bir makine imza attığı için huzursuz olmaktadırlar.

Elektronik imzanın fonksiyon eşitliğinin tanınması, bu imzanın, özellikle hukuki işlemlerde delil işlevini sağlayıp sağlamadığına bağlıdır. Elektronik belgelerde bir irade açıklaması söz konusu olduğu durumlarda, ispat elektronik imzalı belgeyle olacaktır.

Elektronik imzanın kullanımıyla elektronik belgelerin zayıflıklarının giderilmesi amaçlanmaktadır. İspat edilemeyecek şekilde ve iz bırakmaksızın kötüye kullanabilme ihtimalleri, basılı belgelerden farklı olarak doğrudan algılanmalarının zor oluşu ve el yazısıyla imzada bulunan kişiselleştirme özelliğinin eksik oluşu, elektronik belgelerin zayıf yönleridir. El yazısıyla imza sayesinde, kağıda dayalı belgelerde bu sakıncalar giderilmeye çalışılmaktadır.

Biyometrik şifreyle giriş kontrolü usulüyle kullanılan elektronik imza noter tarafından yapılan imza onayı ile karşılaştırılabilir. Noter senedinde her imza, hem de metnin kişinin iradesiyle imzalandığı ve imzanın o kişi tarafından bizzat atıldığı tespit edilir. Bu sebeple onaylama şeklindeki noter senetlerinde, noterin imza onaylaması,

sadece imzanın o kişiye ait olduğunun tespit edilmesinden ibaret değildir. Açıklama ile bağlantılı olarak irade anının tespiti, kişinin kendisinin imza atmasıyla mümkün olmaktadır.

Bilgisayara bağlı okuma aracı (cihazı) ile kullanılabilen çip kart gibi, teknik imza mekanizması, irade açıklayan kişinin imzalayan eli yerine geçmektedir. Bu mekanizma maddi olarak imzalayana bağlı değildir. İmza mekanizması çalınabileceği gibi, üçüncü kişiler tarafından, sahibinin izniyle veya izni olmaksızın kullanılabilir veya kaybolabilir. Aynı şekilde çalışma masası üzerinde veya işyerinde bilgisayarın üzerinde takılı halde bırakılan çip kartların iş arkadaşları tarafından çalınması ve kullanılması da mümkündür.

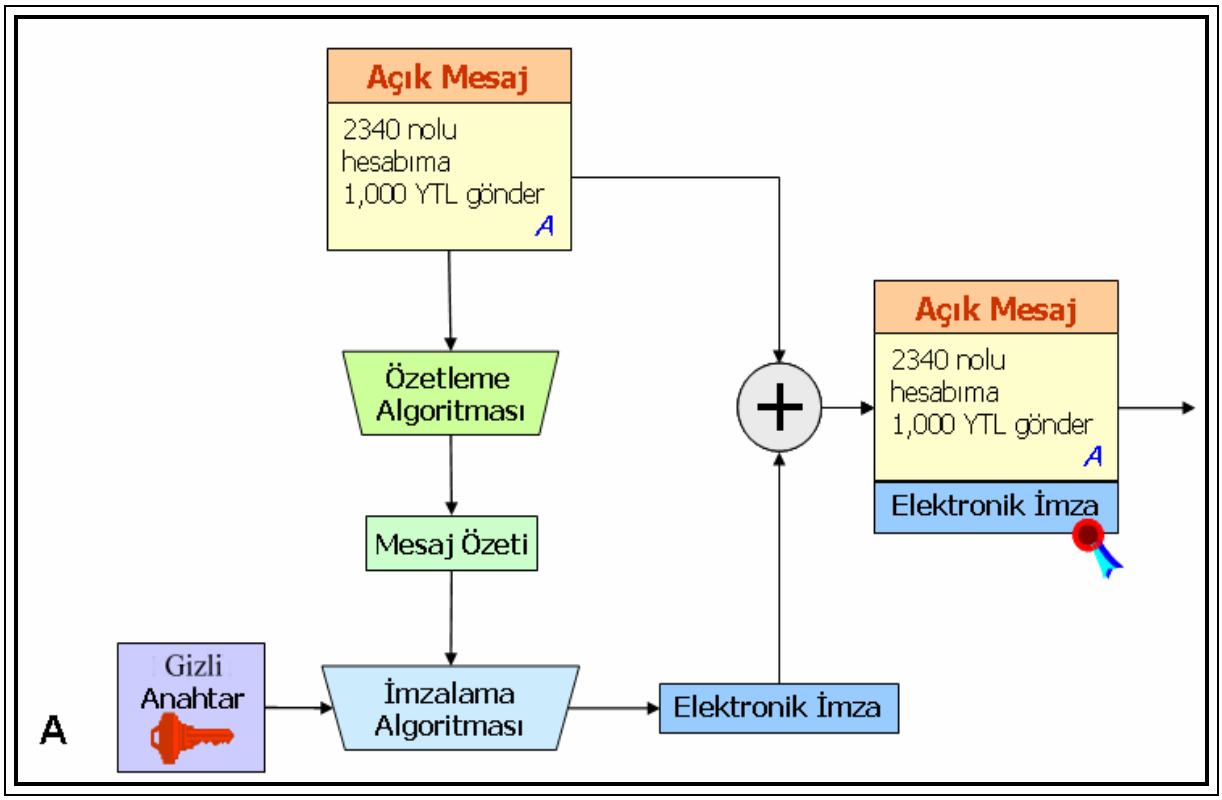
Sonuç olarak, belirtilen bütün tereddütlere rağmen, kanuni düzenlemeye kavuşmuş elektronik imza ve sertifika hizmeti sayesinde elektronik imza el yazısıyla imzaya eşdeğer bir konuma getirilebilmiştir.

Günümüzde, elektronik imzanın el yazısıyla her bakımdan eşdeğer olduğunu kabul etmek zordur. Buna karşılık, çeşitli teknik önlemler ve güvenlik önlemleriyle el yazısıyla imzadaki fonksiyonların aynısının elektronik imzayla karşılanması mümkündür. Fakat elektronik iletişimde, el yazısıyla imzanın fonksiyonlarını mümkün olduğunca karşılayacak bir “imza ikamesi” bulma çabası söz konusudur. Elektronik imza hem imza ikamesi, hem de elektronik hukuki işlemlerin temel teknolojisidir [4].

2. E-İMZANIN MATEMATİKSEL ALTYAPISI

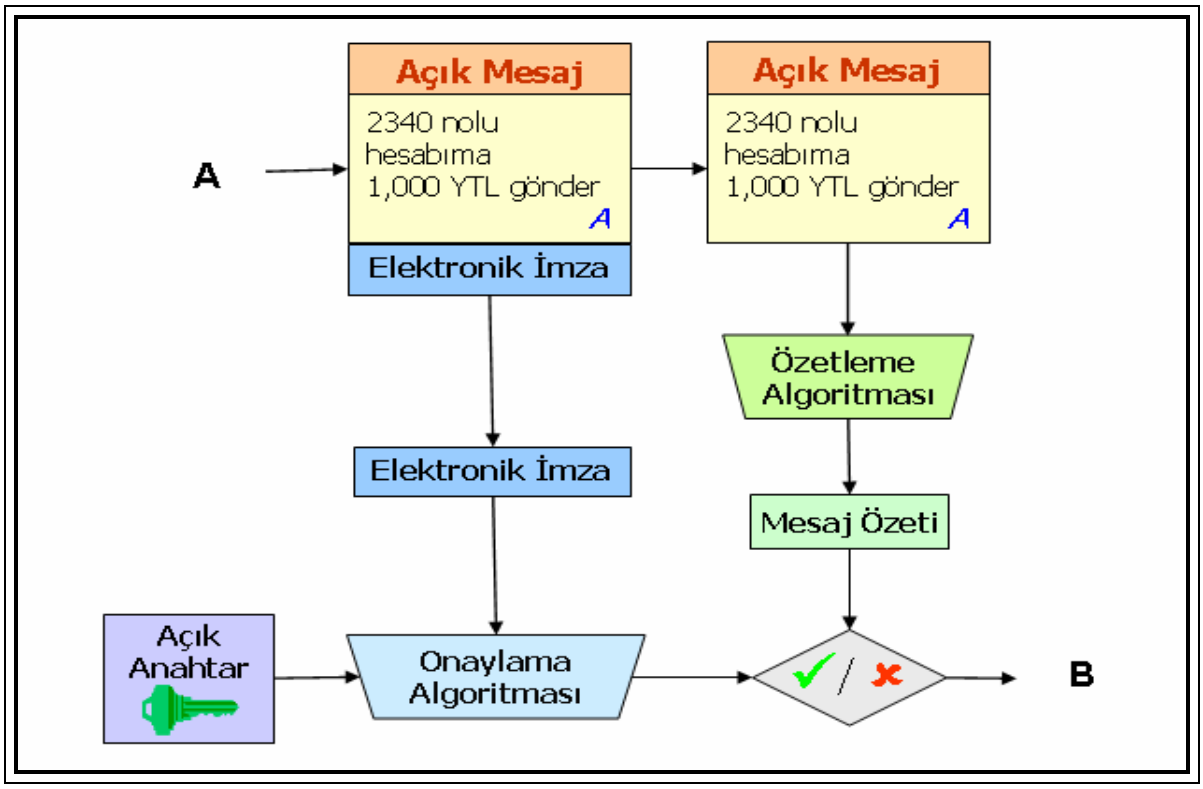
2.1. Elektronik İmza Primitifleri ve Elektronik İmza Şeması

Elektronik ortamda gönderilen mesaj, ileti veya dokümanlar e-imza açık anahtar şifrelemesi yöntemi ve özetleme algoritması kullanılarak oluşturulur. İmzalama ve doğrulama süreçleri aşağıda açıklanmıştır.



Şekil 1: Elektronik İmzalı Bir Mesajın Gönderilmesi

Şekil 1'de görüldüğü üzere; imzalanacak veri özetleme algoritmasından geçirilerek sabit uzunlukta olan bir özet değeri elde edilir. Özet değeri hem bütünlük kontrolü için kullanılır hem de gönderilecek verinin büyük olması durumunda imzalama süresini önemli miktarda kısaltır. Özet değeri, imzalama yapacak kişinin gizli anahtarıyla şifrelenir ve imzalanan verinin orijinali ile birlikte alıcıya gönderilir.



Şekil 2: Gelen Elektronik İmzalı Bir Mesajın Doğrulama

Şekil 2'de görüldüğü üzere; alıcı, kendisine gelen imzalanmış veriyi gönderen kişinin sertifikasında bulunan açık anahtar ile çözer. Ayrıca imzalanan verinin orijinali özetleme algoritması ile işlenerek özet değeri bulunur ve imzalanan özet değeri ile karşılaştırılır. Bu iki özet değeri arasında yaşanacak bir uyuşmazlık mesajın bütünlüğünün bozulduğunu gösterir.

2.1.1. Kriptografi

Bir metni dijital olarak imzalamak için bugün farklı yöntemler kullanılmaktadır. Bunlardan günümüzde en yaygını, şifreleme esasına dayanan yöntemlerdir.

Eski çağlarda kullanılan şifreleme yöntemleri, bugün modern bilgi teknolojisi alanında yeniden önem kazanmıştır. Kriptografik algoritmalar sadece mesajın şifrelenmesinde değil, aynı zamanda dijital imzanın hazırlanmasında ve kontrol edilmesinde de kullanılmaktadır.

Şifrelemenin temel amacı, herkesin okuyabileceği bir açık metinden, şifreleme yoluyla sadece istenilen veya birkaç kişinin okuyabileceği gizli bir metin yaratmaktadır. Alıcı bir şifrelenmiş metni daha sonra ilk şekline çevirerek, yani deşifre edecektir.

(Açık Metin)- Şifreleme- (Gizli Metin)

(Gizli Metin)- Şifreleme- (Açık Metin)

Günümüzde kullanılan şifreleme yöntemlerine farklı matematiksel metotlardan hareket edilmektedir. Başlıca yöntemler arsında;

- Data Encryption Standard (DES): 1997 tarihli olan bu yöntem, IBM'in 1970'li yıllarda geliştirdiği algoritmaya dayanmaktadır.
- International Data Encryption Algortim (IDEA): 1991 tarihli bir yöntemdir. Henüz çok yeni tarihli olmasına rağmen, bir çok analizde kullanılmıştır ve en emin algoritmalardan bir olarak kabul edilmektedir.
- RSA: 1978 yılında Rivest, Shamir ve Adleman tarından hazırlanan bu algoritma, Diffie ve Hellmann'ın 1976 tarihli algoritmalarına dayanmaktadır.
- ElGamal ve DSA: Diffie ve Hellmann'ın fikirlerinin çatısını oluşturduğu ve 1985 yılında Taher ElGamal tarından geliştirilen şema, aynı zamanda asimetrik bir algoritmadır.

2.1.1.1. Simetrik Şifreleme Yöntemi

Simetrik şifreleme yönteminde; şifreleme ve deşifre işlemi için, aynı şifre kullanılır. Örneğin; A ile B arasında haberleşmenin güvenli bir biçimde gerçekleşebilmesi için, şifrenin sadece birbiri ile haberleşen taraflarca bilinmesi, bunun dışındaki kimselere karşı ise mutlak bir şekilde saklı tutulması gerekir. Bir haberleşmeye ikiden çok kimse katılıyorsa, tüm katılanlar şifreyi öğrenmiş olacaklardır. Bu durum ise, birbiri ile haberleşen tarafların, yetkili olmayan bir kimse tarafından şu ya da bu şekilde öğrenilemeyeceğine inanarak nasıl haberleşecekleri sorununu ortaya çıkarmaktadır.

Bu konuda birçok olasılık söz konusu olabilir:

- Elektronik olmayan yoldan şifre değişimi:

Taraflar, haberleşme işlemine başlamadan önce örneğin, posta yoluyla şifreyi birbirine gönderebilirler. Ancak bu olasılık, haberleşmek isteyen tarafların birbirini tanıması şartıyla kullanılabilir.

- Örnek bir şifre ile elektronik yoldan şifre değişimi:

Haberin şifreleneceği şifre, gönderilmek istenen mesaj ile birlikte, örnek br şifre yardımıyla şifrelenmektedir. Şüphesiz bu örnek şifrenin de, haberleşmeden önce taraflar

arasında değişiminin yapılması gerekir. Bu yöntem de, haberleşen tarafların birbirini önceden tanımlarını gerektirmektedir.

- Hyribrid yöntemi ile şifre değişimi: Hem simetrik hem de asimetrik şifreleme yönteminde kullanabilen bu yönteme göre; asıl mesaj, tesadüfen yaratılan bir şifre ile şifrelenir. Bu şifre, toplantı şifresi (Session Key) olarak da adlandırılır. Daha sonra bu mesaj, alıcının açık şifresi (Public Key) yardımıyla şifrelenir. Alıcı, sadece kendisi tarafından bilinen gizli şifresi (Private Key) yardımıyla, mesajın toplantı şifresini açar ve bu şifre yardımıyla mesajı deşifre edebilir.

2.1.1.2. Asimetrik Şifreleme Yöntemi

Birbiri ile haberleşen iki kişi arasındaki, asimetrik şifreleme yöntemi şu şekilde açıklanabilir: Burada haberleşen her bir taraf, biri açık, diğeri ise gizli veya özel olmak üzere, yöndeş bir çift şifreye sahiptir. Bu durumda örneğin, A, B'ye bir mesaj yollamak isterse, bu mesajı şifrelemek için, B'nin aleni olarak ulaşılabilen açık şifresini kullanacaktır. B, şifreli mesajı aldıktan sonra, mesajı deşifre etmek için kendi gizli şifresini kullanacaktır. Tam tersi durum, yani bu sefer B'nin, A'ya mesaj yollaması da aynı şekilde gerçekleşecektir. Buna göre, asimetrik şifreleme yönteminde önemli olan herkesin kendi açık şifresini aleni olarak ulaşılabilir kılmasıdır.

Burada en büyük problem şüphesiz açık şifrenin belirli bir kişiye ait olup olmadığı hususudur. Bu yüzden, bir açık şifrenin belirli bir kişiye yüzde yüz ait olduğunun garanti edilmesi gerekir. Bu problemle Onay Makamı veya Trustcenter veya Certification Authorities adlandırılan kurumlar uğraşmaktadır. Asimetrik şifreleme yöntemlerinin güvenirliği, her şeyden önce gizli şifrenin kullanıcı tarafından iyi saklanmasına ve anahtar uzunluğuna bağlıdır[5].

2.1.2. Açık Anahtar Şifrelemeleri

Açık Anahtarlı Sifreleme (Public Key Cryptography – PKC) sisteminin tasarımı 1975 yılında Diffie, Hellman ve Merkle tarafından yapılmıştır. Bu sistemde haberleşen unsurlar için doğrulanmış bir kanal şarttır, ancak Simetrik Anahtarlı Şifreleme sistemlerinin tersine bu kanalın gizli olması şartı yoktur. Bu sistemde her bir unsur (e, d) olmak üzere kendisi için bir anahtar çifti seçer. Bu anahtar çiftinde *e açık anahtar* ve *d gizli anahtar* olarak adlandırılır. Bu anahtarların özelliği, sadece açık anahtara sahip olarak gizli anahtarın çözülmesinin zor olmasıdır.

PKC sistemlerinin çalışma prensibine göz atacak olursak; *A*, *B*'ye *m* düz metnini göndermek istediği takdirde *B*'nin açık anahtarının kopyası olan e_B 'yi ve açık anahtarlı

şifreleme fonksiyonu ENC'i kullanarak *m* metnini şifreleyerek *c* şifreli metnini elde eder.

m= ENC_{eB} (m)

B, c şifreli metnini aldıktan sonra deşifreleme fonksiyonu DEC'i ve kendi gizli anahtarı olan d_B 'yi kullanarak *c*'yi deşifre eder ve *m* düz metnini elde eder.

m= DEC_{dB} (c)

Şifreleme ve deşifreleme işlemleri bu şekilde yapılarak gizlilik (confidentially) ilkesi de sağlanmış olur.

Şayet bu tip şifreleme işlemlerinde dijital imza sistemleri de kullanılacak olursa, işlemlerin sonucunun unsurlardan herhangi birisi tarafından inkâr edilmesinin de önüne geçilmiş olur(non-repudiation). Bunun yanı sıra bilgi kaynağı doğrulaması (data origin authentication) ve bilgi bütünlüğü doğrulaması da (data integrity) yapılmış olur.

Dijital İmza Sistemleri (digital signature schemes) konusuna kısaca değinilecek olursa; A kişisi SIGN imza oluşturma algoritmasını (signature generation algorithm), m düz metnini ve kendine ait gizli anahtar d_A 'yı kullanarak s imza mesajını oluşturabilir;

s=$SIGN_{dA}$ (m)

m ve *s*'i alan *B* halihazırda *A*'ya ait açık anahtar e_A 'ya da sahiptir. Bunları kullanarak mesajın *A* tarafından gönderildiğini doğrulayabilir.

Bu sayede, Açık Anahtarlı Şifreleme sistemleri, anahtar dağıtımı, anahtar yönetimi ve inkar edilememe gibi Simetrik Anahtarlı Şifreleme sistemlerinde ortaya çıkan üç problemi de gidermiş durumdadır[6].

2.1.3. Elektronik İmza Algoritmaları

Elektronik imza sürecini gerçekleştirmek için tanımlanmış birçok algoritma ve protokol vardır. Her ne kadar RSA algoritması sunduğu avantajları nedeniyle e-imza uygulamalarında en çok kullanılan standart haline gelse de, değişik ihtiyaçlara binaen geliştirilmiş farklı algoritmalar da tercih edilebilmektedir. Farklı gereksinimlerin söz konusu olması halinde ortada kullanılacak ortak bir çözüm yapısı bulunmamakta, her ihtiyaç için özel çözüm üretilmesi yoluna gidilmekte veya standart çözümler kullanılmaktadır.

Geliştirilen e-imza uygulaması RSA algoritması başta olmak üzere EL-Gamal, DSA, E-Sign olarak belirlenmiştir[7].

2.1.3.1. RSA

RSA şifreleme sisteminin en büyük özelliklerinden birisi olan özel anahtarın, genel anahtarı oluşturan parçalardan üretilmesinin mümkün olmamasıdır. Bu nedenle RSA geliştirme projesinde öncelikli olarak ele alınmıştır.

2.1.3.1.1. RSA Anahtar Üretim Süreci

İmzalamada kullanılacak anahtarları üretmek için aşağıdaki işlem basamakları kullanılır.

1- İki adet birbirinden farklı, aynı büyüklükte, tesadüfî olarak belirlenmiş asal sayılar seçilir ve bunların adı p ve q olarak belirlenir.

2- n = p*q ‘dan n sayısı ve Φ=(p-1)*(q–1) ‘i bulunur.

3- Bir rasgele tamsayı üretilir ve adı da “e” koyulur, bu “e” sayısı $1<e<\Phi$ şartını ve obeb(e,Φ) = 1 şartını sağlamalıdır.

4- $e*d \equiv 1 \pmod{\Phi}$ ve $1 < d < \Phi$ şartlarını sağlayan bir “d” sayısı oluşturulur.

5- A’nın genel anahtarı (n,e); özel anahtarı ise “d” dir.

Görüldüğü gibi p,q,d,e sayılarının sadece içinde olabilecekleri bir aralık önceden bilinebilir. Bu dört sayının ne olacağı ise yazılım tarafından anahtar üretimi sırasında rasgele seçilir.

2.1.3.1.2. RSA İmzalama Süreci

İmzalama sürecini gerçekleştirmek için aşağıdaki işlem basamakları kullanılır.

1- $\tilde{m}$ = R (m) hesaplanır, burada aralık değeri [0 , n – 1] olur.

2- s = $\tilde{m}^d \pmod{n}$ formülünden s hesaplanır.

3- Mesaj için imza değeri s‘dir[7].

2.1.3.1.3. RSA Doğrulama Süreci

Doğrulama sürecini gerçekleştirmek için aşağıdaki işlem basamakları kullanılır.

1- Genel anahtar olan (n, e) değerleri elde edilir.

2- $\tilde{m} = s^e \pmod{n}$ hesaplanır.

$\tilde{m}$ ‘in M_R elemanı olduğunu doğrulanır, değilse reddedilir.

3- 4- m(message) = $R^{-1}(\tilde{m})$ elde edilir.

2.1.3.1.4. RSA ile İlgili Örnek

Anahtar Oluşturma: A kişisi p=7927 ve q=6997 asal sayılarını seçer ve, n=pq=55465219 ve Φ=7926.6996=55450296 değerlerini hesaplar. Daha sonra A,ed=5d≡1 (mod55450296) eşitliğinde d=44360237 sayısını bulur. A'nın açık anahtarı (n= 55465219, e=5); gizli anahtar d=44360237 olur.

İmzalama: m=31229978 mesajını imzalamak için A şunu hesaplar:

$\sigma = m^d \bmod n = 31229978^{44360237} \bmod 54465219 \equiv 30729435$

ve (m= 31229978, σ =30729435)'yi B'ye gönderir.

İmzayı Doğrulama: (m=31229978, σ= 30729435)'yi B mesajı doğrulamak için şunu yapar:

$m = \sigma^e \bmod n = 30729435^5 \bmod 55465219 \equiv 31229978$

Çıkan sayı m olduğu için imza doğrulanmış olur[8].

2.1.3.2.DSA (DIGITAL SIGNATURE ALGORITHM)

Ağustos 1991'de ABD Ulusal Standartlar ve Teknolojileri Enstitüsü Sayısal Imza Standardında (DSS) kullanılmak üzere, Sayısal Imza Algoritmasını (DSA) önerdi. DSA bir hükümet tarafından önerilen ilk sayısal imza sistemidir. Aynı zamanda Elgammal sisteminin değişik bir versiyonudur.

DSA aşağıdaki parametreleri kullanmaktadır.

- P bir asal modüldür. $2^{L-1}<p<2^L$

  $512 \leq L \leq 1024$ ve L, 64'ün bir katı olmalıdır.

- q, (p-1)'in bir asal çarpanıdır.

  $2^{159}<q<2^{160}$

- $g=h^{(p-1)/q} \bmod p$,h, $1<h<p-1$ ve $h^{(p-1)/q}$

  mod p>1 olan herhangi bir tamsayıdır.

- x rasgele bir sayıdır. 0<k<q
- $y=g^x \bmod p$
- k rasgele bir sayı. 0<k<q

p, q ve g tamsayıları herkese açık olabilir ve bir grup kullanıcı tarafından ortak olarak kullanılabilir. Bir kullanıcının gizli ve açık anahtarları sırasıyla **x** ve **y** dir. k parametreleri her imza için yeniden üretilmelidir.

2.1.3.2.1. İmza üretimi

Bir M mesajının imzası aşağıdaki eşitliklere göre üretilen **r** ve **s** sayılarıdır.

$r= (g^k \bmod p) \bmod q$

$s= (k^{-1}(SHA(M)+xr)) \bmod q$

Yukarıda k-1, k'nın q modülüne göre çarpımsal tersidir. SHA(M) güvenli çırpma algoritmasının ürettiği 160 bitlik bir katardır.

2.1.3.2.2. İmzanın Doğrulanması

İmzalanmış bir mesajdaki imzanın doğrulanmasından önce p, q ve g ile imzalayanın açık anahtarı doğrulamayı yapacak tarafa asıllanmış bir şekilde duyurulmalıdır.

M', r' ve s', sırasıyla M, r ve s'nin alıcı tarafından alınmış versiyonları olsun. Alıcı önce 0<r'<q ve 0<s'<q olup olmadığını kontrol eder. Eğer bu şartlar sağlanmıyorsa imza reddedilir. Eğer sağlanıyorsa alıcı aşağıdaki hesabı yapar.

$w= (s')^{-1} \bmod q$

$u_1=((SHA(M')) w) \bmod q$

$u_2=((r')w) \bmod q$

$v=(((g)^{u_1}(y)^{u_2}) \bmod p) \bmod q$

Eğer v=r' ise imza doğrulanmıştır. Aksi taktirde mesaj reddedilir.

Yukarıda q parametresinin sayısı 160 bit olarak gösterilmişti. Ancak p'nin uzunluğu 512 ve 1024 arasında 64'ün bir katı olacak şekilde değişebilir.

512 bitlik bir p saldırılara karşı yeterince güvenli olmayacaktır. p için tavsiye edilen uzunluk 768 ya da 1024 bittir[9].

2.1.3.3. ElGamal İmzası

ElGamal kriptosisteminde imza RSA'da olduğu gibi mesajın doğru kişiden geldiğini kontrol etmek için kullanılır. Sadece kapalı metin yerine imzalanmış kapalı metin gönderilerek o kapalı metnin istenen kişiden gelip gelmediği de kontrol edilmiş olur. A şahsının açık anahtarı (p, α, α^{α}=y) ve gizli anahtarının da α olduğu düşünülsün.

m mesajının Z_p nin bir elemanı olduğu düşünülür. Eğer değilse hash fonksiyonu kullanılarak m mesajının Z_p nin elemanı olması sağlanır. A şahsı m mesajını şu şekilde imzalar:

1. Rastgele bir t tamsayısı seçer öyleki $1 \leq t \leq p-2$ ve gcd(t,p-1)=1 koşulunu sağlamalıdır.
2. $r=\alpha^t$ ve $s=t^{-1}(m-r\alpha) \bmod (p-1)$ eşitliklerini kurar.
3. (m,r,s) A'nın imzalı mesajıdır.
4.

2.1.3.3.1. Doğrulama

(m,r,s) imzalı mesajı alan B şahsı aldığı mesajın A'dan geldiğini şu şekilde doğrular:

1. Öncelikle $1 \leq r \leq p-1$ olduğunu kontrol eder. Eğer değilse imzayı reddeder.

2. Daha sonra $v=\alpha^m$ ve $w=y^r r^s$ değerlerinin hesaplar (buradaki y sayısı A'nın açık anahtarındaki y sayısıdır.)

3. Eğer v=w eşitliği sağlanıyorsa imza kabul edilir, aksi takdirde reddedilir.

2.1.3.3.2. ElGamal ile İlgili Örnek

Anahtar Oluşturma: A şahsı bir p=2357 asal sayısı ve $\alpha=2 \in Z^*_{\in \ni}$ bir jeneratör seçer. Buna ilave olarak bir α= 1751 gizli anahtarı seçer ve

$\alpha^\alpha \bmod p=2^{1751} \bmod 2357=1185$

değerini hesaplar. A'nın açık anahtarı (p=2357, α=2, α^α=1185) tir.

İmza Oluşturma: Basit olması açısından mesaj m=1463 olarak seçilsin (Eğer mesaj p asal sayısından büyük olsaydı hash fonksiyonundan geçirilirdi.) m= 1463 mesajını imzalamak için A önce rastgele bir t=1529 sayısı seçer, daha sonra $r=\alpha^t \bmod p=2^{1529} \bmod 2357 \equiv 1490$ ve $t^{-1} \bmod (p-1)=1529^{-1} \bmod (2356) \equiv 245$

$s=t\ -1(m-r\alpha) \bmod (p-1)=245(1463-1490.1751) \bmod 2356 \equiv 1777$

A'nın imzası (m=1463, r=1490,s=1777)

İmzayı Doğrulama: B aldığı imzalı mesajı doğrulamak için önce

$v=\alpha^m \bmod p=2^{1463} \bmod 2357 \equiv 1072$

değerini hesaplar. Daha sonra

$w= y^r r^s \bmod p=1185^{1490}\ 1490^{1777} \bmod 2357 \equiv 1072$

değerini hesaplar ve v=w olduğu için imzayı kabul eder[8].

2.1.4. Hash Fonksiyonu

Hash fonksiyonlarının kriptografide çok geniş bir kullanım alanı vardır. Hash fonksiyonları, öncelikle tek-yönlü (one-way) fonksiyonlardır. Yani bir verinin fonksiyon altında görüntüsünü hesaplamak kolaydır ama görüntüden fonksiyonun tersi aracılığıyla ana veriyi elde etmek hesaplama gücü anlamında zordur.

Hash fonksiyonları (Tablo 1) ile elde ettiğimiz değer, yani hash değeri, fonksiyon girdisinin değişken boyuta sahip olmasına karşın sabit boyuta sahiptir ve genelde hash değeri, girdiye göre çok daha ufak boyuttadır. Kullanılan Hash fonksiyonlarından birbirine çok benzer girdi değerleri için dahi çok farklı çıktılar üretmesi beklenir. Ve yine önemli bir özellik olarak hash fonksiyonlarından çakışmasız (collision-free) olmaları umulur. Yani hash fonksiyonumuz altında aynı hash değerini veren iki girdinin bulunması hesaplama gücü göze alındığında çok zor olmalıdır.

Yukarda bahsedilen özellikler ışığında hash değerleri, verilerin parmak izi olarak düşünülebilir. Nasıl ki her insanın parmak izi farklıdır, aynı şekilde, her metin için, sabit uzunlukta çok büyük oranda benzersiz metin üretilebilen bir algoritmadır.

Bu algoritma aynı karakter kümesi için her zaman aynı sonucu üretir. Algoritma, yapısı gereği tek yönlü gerçekleşen bir matematiksel işlemdir. md5() ve sha1() algoritmaları kullanılarak sabit uzunlukta hash oluşturulabilir.

Bilgi Güvenliği sözcüğünün karşılığı:

MD5 hash: cce8d56ee8f5c5bd2815cd957603920d

SHA-1 hash: 335b29403781a638421f081084de1f3f423ad5b3

md5() 128-bit hash (32 alfanümerik karakter) döndürürken, sha1() 160-bit hash (40 alfanümerik karakter) döndürür.

Tablo 1 : Hash Fonksiyonları

Yöntem	Şifreleme Uzunluğu	Lisans Sınırlamaları
Hash Fonksiyonları		
MD5	128 Bit	Lisans zorunluluğu yok
SHA 1	160 Bit	Lisans zorunluluğu yok
HIPE-MD	128 veya 160 Bit	Lisans zorunluluğu yok

Bugün en çok tanınan ve en yaygın olarak kullanılan hash algortiması MD(Message Digest)'dir [10].

2.1.4.1.MD (Message Digest)

MD en basit şekilde “herhangi uzunluktaki bir veriyi isleyip sonuç olarak sabit uzunlukta bir veri elde eden fonksiyon” olarak tanımlanabilir. Matematiksel olarak tanımlayacak olursak;

M: degisken uzunlukta veri; h: sabit uzunlukta veri ; H: fonksiyon H:H(M)

Sabit uzunlukta çıktı elde etmenin yanında, MD fonksiyonun sağlaması gereken bazı özellikler vardır. Bu özellikler söyle sıralanabilir:

• “M” verildiği zaman, “h” yi hesaplamak kolay olmalı

• “h” verildiği zaman “M” i hesaplamak çok zor olmalı (hatta imkânsız olmalı). Bu yönüyle MD fonksiyonu “tek yönlü fonksiyon (one-way function)” olarak adlandırılır.

• “M” verildiğinde H(M) = H(M') eşitliğini sağlayan “M'” in bulunması çok zor olmalı (hatta imkânsız olmalı)

MD, verilerin bütünlüğünün kontrolü yani verinin değişikliğe uğrayıp uğramadığını kontrol için kullanılmaktadır. Örneğin internete indirilmek üzere yerleştirdiğiniz bir dosyaya ek olarak bu dosyanın MD sonucunuza dağıtırsanız, bu dosyayı sizin sitenizden indiren kullanıcılar, kendi bilgisayarlarında bu dosyanın MD'sini hesaplayıp sizin hesapladığınız MD değeri ile kontrol ederler ve böylece indirdikleri dosyanın değiştirilip değiştirilmediğini, yani güvenilir olup olmadığını anlayabilirler.

2.1.4.2.SHA Özetleme Fonksiyon

SHA (Secure Hash Algorithm – Güvenli Özetleme Algoritması), Amerika’nın ulusal güvenlik kurumu olan NSA (National Security Agency) tarafından tasarlanmış ve ilk olarak 1993 yılında FIPS PUB 180 standardında yayınlanmıştır. Sıkıştırma fonksiyonundaki küçük bir değişiklikle 2 yıl sonra tekrar NSA tarafından SHA-1 adında FIPS 180-1 de yayınlanmıştır.

SHA-1, uzunluğu en fazla 264 bit olan mesajları girdi olarak kullanır ve 160 bitlik mesaj özeti üretir. Bu işlem sırasında, ilk önce mesajı 512 bitlik bloklara ayılır ve gerekirse son bloğun uzunluğunu 512 bite tamamlar. SHA-1 çalışma prensibi olarak R. Rivest tarafından tasarlanan MD5 özet fonksiyonuna benzer ve iteratif bir yapısı vardır. Her iterasyonda bir sıkıştırma fonksiyonu kullanır. Bu fonksiyon, mesajın 512 bitlik bloğunu alır ve 16 bitlik kelimelere (m0, m1, ..., m15) çevirir. Daha sonra bu kelimeler, mi = (mi-3+ mi-8+ mi-14+ mi-16) <<1 fonksiyonu kullanılarak 2560 bite genişletilir ve

her biri 20 matematiksel fonksiyon içeren 4 tur çalıştırılır ve 160 bitlik mesajın özeti elde edilir.

2.2. Elektronik İmzanın İkincil Bileşenleri

Bir açık Anahtar Altyapısının sağlıklı bir şekilde işleyebilmesi için, aşağıdaki bileşenlerin uyum içinde çalışması gerekmektedir:

2.2.1 Elektronik Sertifika

Tablo 2'de görüldüğü üzere, Elektronik sertifika, dijital imzanın doğrulanabilmesi için gerekli olan veriler ile birlikte imza sahibinin kimlik bilgilerini de içeren elektronik kayda verilen isimdir.

Tablo 2: Dijital Sertifika Örneği

Version: 3
Serial Number:1001
Signature algorithm: 1.2.840.113549.1.1.5
Issuer: CN=Demo-CA-CA C=FI
Valid not before: Fri Mar 17 14:57:55 GMT+02:00 2000
Not after: Tue Mar 18 01:59:59 GMT+02:00 2003
Subject: CN=Dave Demouser, O=Demo-org, C=FI
public exponent:23
modulus:
b94e6061596cc2f35190b6979b2137247b1b07281fbab78845b33a36dddd551c79a3970
7431d9ef236f5aeaccf031c95f77b563a1cb73069bf27ad1f27ad1fdd2b675b7dbd754c105
ee6d7
ec3d1c3ad7f4862cce863d6569d820557735779af185ff3833a7a6a21f8359adc98049
47909515c227a293b84cb0433a9b7652a9355

Extension:1 not critical KeyUsage
digitalSignature

Certificate Fingerprint:64:AC:00:56:3B:1F:46:02:AE:93:E9:AD:F0:51:74:4E

Kaynak: Kamu Bilişim Platformu IV

Elektronik sertifikalarda temel olarak aşağıdaki alanlar bulunmalıdır:

- Sertifika sahibi bilgileri (isim, şirket, çalışan birim, yer, ülke, e-posta vb.),
- Sunucu sertifikalarında sunucu bilgileri (alan adı, sunucu adı, şirket adı vb.),
- Ülke adı TR (Türkiye) olmak üzere Elektronik Sertifika Hizmet Sağlayıcısı (ESHS) bilgileri,
- Sertifika geçerlilik süresinin başlangıç ve bitiş zamanı,
- Kullanılan elektronik imza doğrulama verisi,
- Sertifika seri numarası,
- ESHS'nin imzası,

Nitelikli elektronik sertifikalarda ise, Kanun gereği aşağıdaki bilgilerin de yer alması gerekmektedir;

- Sertifikanın "nitelikli elektronik sertifika" olduğuna dair bir ifade,
- Sertifika sahibi diğer bir kişi adına hareket ediyorsa bu yetkisine ilişkin bilgi,
- Sertifika sahibi talep ederse mesleki veya diğer kişisel bilgileri,
- Varsa sertifikanın kullanım şartları ve sertifika kullanımına yönelik maddi işlem sınırı.

2.2.2. Elektronik Sertifika Hizmet ve Sağlayıcısı (ESHS)

Dijital sertifikalar, 5070 Numaralı Elektronik İmza Kanunu'na göre, yetkilendirilmiş Elektronik Sertifika Hizmet Sağlayıcısı (ESHS) tarafından kullanıma sunulmaktadır. Söz konusu kanuna göre ESHS şu şekilde tanımlanmaktadır (Madde 8); "ESHS, elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuki tüzel kişilerdir."

Elektronik Sertifika Hizmet ve Sağlayıcıları'nın görevleri aşağıdaki gibidir;

1. Güvenli ürün ve sistemleri kullanmak,
2. Hizmeti güvenilir bir biçimde yürütmek,
3. Sertifikaların taklit ve tahrif edilmesinin önlemekle ilgili her türlü tedbiri almak olarak özetlenebilir.

2.2.3. Güvenlik Protokolleri

Elektronik imzanın, uygulamaların bir parçası olarak kullanılmasına izin veren iletişim kuralları dizisine "Güvenlik Protokolleri" adı verilmektedir.

2.2.4. Uygulamaya İlişkin Diğer Standartlar

Elektronik imzanın yaratılmasında kullanılan anahtarların saklanması, değiştirilmesi, elektronik imzanın oluşturulması, taşınması vb. konularla ilgili oluşturulmuş

standartlardır. Bugün RSA Laboratuarları öncülüğünde geliştirilmiş olan PKSC (“public key cryptography standards”-açık anahtar kriptografisi standartları) geniş kabul gören ve kullanılan standartlardan biridir [11].

2.2.5. Güvenli Elektronik İmza Oluşturma ve Doğrulama Araçları

E-İmza oluşturma aracının tanımı Kanun’a göre “Elektronik imza oluşturmak üzere, imza oluşturma verisini kullanan yazılım veya donanım aracı” şeklindedir.

Uygulamalarda imza oluşturma araçları donanım bazlı olarak akıllı kartlar (smart card), USB Token’lar, bilgisayarlar veya veri işleme kapasitesi olan el terminalleri (PDA, cep telefonları, Pocket PC’ler v.b.) ile yazılım bazlı olarak da bilgisayar programları, smartcard’lar, işletim sistemleri veya özel yazılımlar v.b şeklinde karşımıza çıkabilmektedir.

Güvenli elektronik imza oluşturma araçları, özellikle mevzuatın getirdiği zorunluluk sonucu, belirlenmiş standartlarda Şekil 3’de görülen akıllı çubuk (token) veya Şekil 4’te görülen akıllı kart olabilecektir.

Şekil 3: Akıllı Çubuk

Kaynak: Telekomünikasyon Kurumu

Şekil 4. Akıllı Kart

Kaynak: Telekomünikasyon Kurumu

III. E-İMZANIN HUKUKİ DELİL DEĞERİ

Mevcut hukuk sistemimizde deliler, kesin delil ve takdiri deliler olmak üzere ikiye ayrılmaktadır. Kesin deliller; ikrar (HUMK. md. 236), kesin hüküm (md.237), senet (md.287), yemindir (md.377). Takdiri deliller ise; şahit (md. 245 vd), bilirkişi (md.275 vd), keşif (md. 377), ve özel hüküm sebepleridir (md.367). Hukuki işlemler bakımından senetle (kesin delille) ispat zorunluluğu HUMK md. 288 vd. düzenlenmiştir. Bu hükümlerde açıkça düzenlenen kanuni ispat halleri dışında delil serbestisi esası geçerlidir [12].

Kanun, genel gerekçesinde de belirtildiği gibi elektronik belgeyi değil, elektronik imzayı düzenlenmiştir. Md. 5/f.1'deki hüküm ile güvenli bir elektronik imzaya elle atılan imza ile aynı hukuki sonuç bağlanmıştır.

Elektronik imzaya tanınan bu hukuki değer sadece medeni hukuk bakımından geçerlidir. Bu nedenle Elektronik İmza Kanunu ile HUMK'a 295'inci maddeden sonra gelmek üzere 295/A maddesi eklenmiştir. 295/A maddesinin birinci fıkrasında "güvenli elektronik imza ile oluşturulan elektronik veriler senet hükmündedir. Bu veriler aksi ispat edilinceye kadar kesin delil sayılırlar" hükmü getirilmiştir. Bu madde dolaylı bir şekilde elektronik senedi düzenlemiştir [13]. HUMK'nda kâğıda dayalı senet kavramının da Kanunda tanımı yapılmamış, uygulamada ortaya çıkacağı varsayılmıştır.

Güvenli elektronik imza ile imzalanmış belgeyi senet ve aksi ispat edilinceye kadar kesin delil kabul edileceğini tespit eden bu madde, hakimin takdir yetkisini kısıtlaması yönünde tenkit edilebilir. ABD'de birçok eyalet, elektronik imza ile imzalanmış belgeleri kesin delil olarak kabul etmekte ve bunların ispat kuvvetini de kesin delil olarak sayılan diğer delillerden daha üstün tutmaktadır [13]. Bunun amacı, elektronik imza kullanımının yaygınlaştırılması, itibarının arttırılması olarak düşünülebilir.

Elektronik imzanın delil niteliğiyle ilgili duruma açıklık getiren 99/93/EC sayılı AB Direktif'in 5/2 Md.'sine göre, üye devletlerin elektronik imza konusunda yapacakları düzenlemede, Kanunumuzda olduğu gibi sadece güvenli elektronik imzaya değil; diğer elektronik imza çeşitlerinin de kesin delil olmasa dahi delil niteliğine yer verilmesi istenmiştir. Direktifin bu hükmünün Kanunda tam olarak karşılandığı söylenemez.

Elektronik imzanın delil değerini sadece güvenli elektronik imza ile sınırlamak bir hukuk politikası yaklaşımı olsa da, güvenli elektronik imza dışındaki elektronik imzalara delil niteliği tanımamak direktifin bu maddesinin amaçlarına uygun düşmemektedir. Örneğin Avusturya'da olduğu gibi, HUMK 295/A maddesine güvenli elektronik imza olarak kanunun aradığı niteliğe sahip olmayan elektronik imzaların da delil niteliğinin inkar edilemeyeceği madde metnine eklenebilir.

Kanunun güvenli elektronik imza dışındaki elektronik imzaların hukuki sonuçlarını düzenlememiş olması, bilinçli olarak bırakılmış bir boşluktur. Kanun koyucu, böyle bir boşluk bırakarak güvenli olmayan elektronik imzaya da, güvenli elektronik imza kadar olmasa bile, bir ölçüde caiz delil sayılma özelliği tanınmak istenmiştir [14]. Dolayısıyla güvenli elektronik imza dışında kalan imzalarla imzalanmış veya hiç imzalanmamış elektronik veriler de delil olarak kullanılabilecektir. Ancak bu deliller takdiri delil olarak ileri sürülebilir.

Hukukumuzda kanuni ve takdiri ispata birlikte yer veren karma bir sistemin geçerli olduğu söylenebilir. Hukuki işlemler yönünden kesin delille ispat geçerli ise de, bu düzenleme kamu düzenine ilişkin değildir. Güvenli elektronik imza dışında kalan elektronik imzaların takdiri delil olarak kullanılabilmesi için geçerli bir delil sözleşmesi, yani taraflar arasında elektronik verilerin delil olarak sunulduğunda bunun tarafça muvaffak edilmesi gerekir.

1. ELEKTRONİK İMZA KANUNU

Elektronik imza, 5070 sayılı Elektronik İmza Kanunu 23 Ocak 2004 tarihinde Resmi Gazete'de yayımlanmış ve 23 Temmuz 2004 tarihinde yürürlüğe girmiştir.

Elektronik İmza Kanunu'ndaki temel amaç, elektronik imzanın hukukî ve teknik yönleri ile kullanımına ilişkin esasların düzenlenmesidir. Söz konusu kanun ile, güvenli elektronik imzanın, elle atılan imza ile aynı hukukî sonucu doğurduğu ancak kanunların resmî şekle veya özel bir merasime tabi tuttuğu hukukî işlemler ile teminat sözleşmelerinin güvenli elektronik imza ile gerçekleştirilemeyeceği hükmü getirilmiştir.

Kanun kapsamında elektronik imza kavramı, başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri olarak tanımlanmıştır. Güvenli elektronik imzanın elle atılan imza ile aynı hukukî sonucu doğurması, elle atılan imza ile aynı ispat gücünü haiz olması, usulüne göre güvenli elektronik imza ile oluşturulan elektronik verilerin senet

hükmünde olması ve bu verilerin aksi ispat edilinceye kadar kesin delil sayılması Kanunun hukuki açıdan getirmiş olduğu en önemli yeniliklerdir.

Söz konusu Kanun ile Bilgi Teknolojileri ve İletişim Kurumu (Telekomünikasyon Kurumu) güvenli elektronik imza oluşturma araçları, güvenli elektronik imza doğrulama araçları, elektronik sertifika hizmet sağlayıcısı, elektronik sertifika hizmet sağlayıcısının yükümlülükleri, nitelikli elektronik sertifikaların iptal edilmesi, yabancı elektronik sertifikalar ve sertifika mali sorumluluk sigortası ile ilgili ikincil düzenlemeleri yapmakla görevlendirilmiştir.

2004/21 sayılı Başbakanlık Genelgesi hazırlanmış ve 6 Eylül 2004 tarihli ve 25575 sayılı Resmi Gazete'de yayımlanmıştır. Bu kapsamda, tüm kamu kurum ve kuruluşlarının, kurumsal sertifika ihtiyaçlarının karşılanması amacıyla bir Kamu Sertifikasyon Yapısının oluşturulmasına karar verilmiştir. Bu çerçevede; tüm kamu kurum ve kuruluşlarının aynı kurumsal sertifika yapısı altında toplanmasını hedefleyen, sadece kamu kurum ve kuruluşlarına kurumsal sertifikaların oluşturulmasını ve sertifika yaşam çevriminin yönetilmesini sağlayacak Kamu Sertifikasyon Yapısının kurulması ve işletilmesi görev ve sorumluluğu TÜBİTAK – UEKAE'ye verilmiştir [15].

2. ELEKTRONİK İMZA İLE İMZALANMIŞ VERİLERİN DELİL DEĞERİ

Delil, Hukuk Usulü Muhakemeleri Kanunumuzda, "davranan halline tesir edebilecek münazaalı hususların ispatı için başvurulan vakıalar" şeklinde tarif edilmiştir (m.238/I). Delil, çekişmeli vakıaların ispatı için başvurulan vasıtalardır.

Mahkeme, bir vakıanın gerçeğe uygun olup olmadığına ikame olunan delillere göre karar verir. Her delil aynı değerde olmadığı için somut olarak ileri sürülen delilin değerlendirilmesi gerekir. Bu durumda bir delilin ispat kuvveti veya delil değerinden söz edilir. Hakim ikame olunan delilleri serbestçe takdir eder (HUMK md. 240).

Kanun bir yandan güvenli elektronik imzanın elle atılan imza ile aynı hukuki sonucu doğuracağını düzenlemişken (md. 5/I), diğer yandan md. 22 güvenli elektronik imza dışında kalan imzalar için herhangi bir hukuki düzenleme yapmamış, adeta sessiz kalmıştır. Bu bilinçli olarak bırakılmış bir boşluktur. Çünkü Direktifin 5/2 maddesine göre üye devletler, her türlü elektronik imzanın delil olarak kullanılmasını temin ile yükümlüdürler.

Güvenli elektronik imzalı belgeler, Elektronik İmza Kanunu (EİK md. 5, BK. Md. 14) ve HUMK 295/A hükümlerine göre kesin delil olma sonucunu doğurur. Diğer taraftan güvenli elektronik imza dışında kalan elektronik imzalar bakımından herhangi

bir düzenleme yapılmadığından HUMK 367'inci maddeye müracaat edilecek ve bu hüküm doğrudan uygulanacaktır.

Güvenli elektronik imza dışında kalan elektronik imzalar bugün 287 ve 367'inci maddeden dolayı uygulamada kullanılmaktadır. EİK bu konuda yeni bir düzenleme getirmemekle mevcut uygulamayı kabul etmiştir.

Kanun 23'üncü madde ile HUMK 295/A maddesini ilave etmekle yaptığı düzenlemeye, elektronik imza ile imzalanmış verilerin senet değil senet hükmünde olduğunu kabul etmiştir. Bu düzenleme isabetlidir. Çünkü, veri o anda senet halinde değil de elektronik belge halinde de olabilir.

Elektronik belge, elektronik bir usul yardımıyla imzalanmış belgedir[16]. Elektronik belgeler de irade açıklaması içerirler. Elektronik imzalı belgeler yazı yanında ses veya resim içerebilir. Elektronik imzalı belgelerin, imzanın taşıdığı özelliklere göre senet sayılması mümkündür (HUMK md.295A).

Öğretide Konuralp[10], HUMK md.295/A hükmünün dolaylı olarak elektronik senedi düzenlediğini, elektronik senedin tanımının ise yapılmadığını, ancak elektronik senedin "bir kimsenin kendi güvenli e-imzası ile meydana getirdiği ve aleyhine delil olarak kullanılma amacı taşıyan ve bilgisayar ortamında varlığını sürdürebilen elektronik veriler" şeklinde yapılacağı görüşündedir.

Kural olarak mahkemeye senetlerin aslının ibraz edilmesi gerekir. Şayet senet aslı ibraz edilmemiş ise davanın her aşamasında re'sen veya taraflardan birinin talebi üzerine senedin aslının ibrazı talep edilebilir. Bu durumda senet zayi veya telef olmamış ise aslının ibrazı mecburidir (HUMK md. 321).

Elektronik belgelerin mahkemeye ibrazı, elektronik veri taşıyıcıları (HD, CD, DVD, flaş disk, disket, vb.) kullanılarak olabileceği gibi e-posta yoluyla elektronik belgenin mahkemeye sunulması da mümkündür. Mahkeme gerekli görürse elektronik belgeyi veri taşıyıcılardan kendi veri taşıma aygıtlarına alabilir.

Mahkeme ibraz edilen elektronik belge, güvenli elektronik imzalı bir belge ise HUMK 295/A maddesi gereğince kesin delil olarak hakimi bağlayacaktır. Bu belgelere, resmi senetlere yaklaşır bir değer verildiğinden bu veriler aksi ispat edilinceye kadar kesin delil sayılır. Hakimin ibraz edilen elektronik belgenin güvenli elektronik imza ile imzalanıp imzalanmadığını re'sen araştırması gerekir. Aksi takdirde, güvenli elektronik imza taşımayan bir belgeye senet hükmü atfedilmiş olacaktır. Kağıda dayalı senette gözle senet niteliği görüldüğünden ayrıca bir incelemeye gerek yoktur. Oysa ibraz edilen bir elektronik belgenin, kanunun saydığı şartları haiz bir belge ve dolayısıyla

senet olup olmadığı hakim tarafından gözle görülebilir ve değerlendirilebilir durumda değildir.

Elektronik imzanın kendisine has özelliklerinden dolayı mahkemede güvenli elektronik imzalı belgenin nitelikli elektronik sertifikaya dayanıp dayanmadığı kontrol edilebilir. Bunun yanında sertifikanın yetkili bir sertifika hizmet sağlayıcıdan temin edilip edilmediği, halen geçerli olup olmadığı şüpheye yer bırakmayacak surette ortaya konulmalıdır. Bunun için mahkemeler yeterli altyapıya sahiptir [17].

3. KURUMLARIN ELEKTRONİK İMZA ALABİLME KOŞULLARI

Elektronik ortamda yapılan işlemlerde bilginin bütünlüğünden, inkar edilemezliğinden, işlemi gerçekleştirenin kimliğinin doğrulanabilirliğinden emin olmak ve yapılan bu işlemlere hukuksal geçerlilik kazandırmak isteyen her kuruluş veya kişi elektronik imza kullanabilir.

Bir firma elektronik İmza kullanmak istediğinde yerine getireceği koşullar şunlardır; öncelikle bir elektronik sertifika sahibi olması gerekir. Eğer kamu kurumuysa ve elektronik imzayı kurum içi ve kamu kurumları arasında işlemlerde kullanılacaksa sertifikasını Başbakanlık Genelgesi gereği TÜBİTAK UEKAE'den temin etmelidir. Bunun için kurumun TÜBİTAK UEKAE'ye çalışanlarına sertifika temin etmek üzere kurumsal başvuru yapması gerekir. Eğer elektronik imzayı kullanacak olan kuruluş kamu kurumu değilse ya da vatandaş olarak kurum dışındaki işlemlerde elektronik imzayı kullanmak istiyorsa, bu işi yapmaya yetkili özel şirketlerden, yani elektronik sertifika hizmet sağlayıcılardan, ücret karşılığında sertifika temin etmesi gereklidir. Bilgi Teknolojileri ve İletişim Kurumu nitelikli elektronik sertifika vermeye yetkili olan kuruluşları internet sayfasında duyurmaktadır.

IV. KAMU KURULUŞLARINDA E-İMZA UYGULAMASI VE KARŞILAŞILAN SORUNLAR

1. E-DEVLET VE KRİPTOLOJİ

Devletlerin kamusal faaliyet alanlarındaki sağlık, eğitim, vergi gibi bürokratik işlemleri İnternet ortamında hızlı ve güvenilir biçimde gerçekleştirebilmek için elektronik devlet (e-devlet) modelleri hayata geçirilmektedir. Bu faaliyetlerde temel amaç, ülke yönetiminde çağdaş yapısal değişimleri gerçekleştirmek ve yönetimi bilgi ve haberleşme teknolojisi üzerine uyarlayarak vatandaş-devlet ilişkisini kolaylaştırma ve verimleştirmedir. Haberleşmenin olduğu her alanda kriptoloji bilimi yer aldığından, e-devlet uygulamalarının başarılı olabilmesinde kriptoloji bilimi önemli bir yere sahiptir. Kriptoloji sayesinde e-devlet uygulamalarından herkes istediği zaman güvenliği tehlikeye atmadan faydalanabilmekte, kamu kurumları arasındaki bilgi paylaşımı güvenilir olarak sağlanabilmektedir.

Kamu kurumlarında yapılan birçok işlem için kimlik kanıtlanması ve imza atılması gerekmektedir. Bu tür işlemler elektronik ortamda yapılmak istendiği zaman ortama uygun kimlik kanıtlama ve imza atılması gerekmektedir. Elektronik imza (e-imza) elektronik ortamlarda ıslak imzanın yerine geçmekte ve bireyin kimliğini içermektedir. E-imza, gönderilmek istenen belgeye eklenen, kimlik doğrulama amacıyla kullanılan elektronik veridir. E-imza açık anahtar altyapısının en yaygın kullanılan bileşenidir. E-imza oluşturmak ve doğrulamak için çeşitli yazılım ve donanımlara ihiyaç bulunmaktadır. Yazılımı oluşturmak için öncelikle hangi e-imza algoritmasının kullanılmasının belirlenmesi gerekmektedir. Oluşturulacak e-imza biçimi için bir çok standart vardır. Yazılım bu standartlara uygun biçimde oluşturulur. Yazılımın standartları desteklemesi ve kriptografik donanimlar (akıllı kart, akıllı çubuk) ile uyumlu çalışması çok önemlidir. Akıllı kartlar (Smart card) en çok kullanılan ve bilinen kriptografik donanımlardandır. Akıllı kartlar, üzerinde şifreleme, şifre çözme, imzalama, imza onaylama ve anahtarları depolama gibi hizmetleri sunmaktadır. Akıllı kartı kullanabilmek için bilgisayar ile uyumlu çalışacak akıllı kart okuyuculara ihtiyaç vardır. Bu gereksinimler karşılandıktan sonra e-imza atılmaya hazırdır.

Ülkemizde e-devlet uygulamalarının büyük bir kısmı sadece kamu kurumlarının web sitesi yapmak olarak algılanmasından dolayı güvenlik zafiyetlerine sahiptir. Ayrıca güvenli elektronik arşivleme için herhangi bir eylem veya standart bulunmamaktadır. Her kurum kendi başına önlem almaya çalıştığından kurumlar arası güvenli veri iletişiminde de önemli sorunları bulunmaktadır. Akıllı kartların uygulama alanları

oldukça geniştir : e-kimlik (Akıllı kart tabanlı elektronik kimlik kartı), e-pasaport (elektronik pasaport). Bu tip uygulamalarda sayısal kimlik bilgileri ve biometrik bilgiler akıllı kart içine yerleştirilmektedir. Kimlik doğrulama yöntemleri ve akıllı kart üzerindeki verinin saklanması için de kriptoloji yöntemlerinin kullanılması gerekmektedir.

2. BAZI DEVLET KURUMLARINDA E-İMZA KULLANILMASI

2.1. Adalet Bakanlığı

Adalet Bakanlığınca, e-Dönüşüm süresince e-Devletin e-Adalet ayağını oluşturmak üzere yürütülen Ulusal Yargı Ağı Projesi (UYAP) ile; günümüzün gerekli tüm teknolojik gelişmeleri kullanılarak, Adalet Bakanlığının merkez ve taşra teşkilatı, bağlı ve ilgili kuruluşları ve adli ve idari tüm yargı birimlerinin (Cumhuriyet Başsavcılıkları, mahkemeler, icra daireleri, ceza infaz ve ıslah kurumları, adli tıp birimleri ve denetimli serbestlik birimleri vb.) donanım ve yazılım ihtiyaçları karşılanarak bilgi işlem otomasyonuna geçirilmesi ve dış kurum ve kuruluşların bilgi sistemleriyle entegrasyonu sağlanarak, avukatlar ile vatandaşlara internet üzerinden çevrimiçi (on-line) yargı hizmeti sunularak Türkiye Cumhuriyeti yargı sisteminin işleyişinin güvenirliği, doğruluğu ve şeffaflığının en üst düzeyde sağlanması, yargı sistemine hız kazandırılması amaçlanmıştır.

UYAP kapsamında; 2008 yılı sonu itibariyle Adalet Bakanlığı teşkilatı yanında 134 Ağır Ceza Mahkemesi, 587 Mülkahat Adliye, 25 Bölge İdare Mahkemesi, 134 Denetimli Serbestlik Birimi, 65 Adli Tıp Birimi, 425 Ceza İnfaz Kurumu UYAP projesine alınmıştır. Türkiye genelinde UYAP projesine geçme oranı %100'e yaklaşmıştır. Adalet Bakanlığı teşkilatı ile adli ve idari yargının tüm birimleri, Ulusal Yargı Ağı kapsamına alınmış olup bu birimlerin her türlü yargısal ve idari faaliyetleri, iş ve işlemleri UYAP otomasyonu sayesinde elektronik ortamda yürütülebilir hale gelmiştir.

UYAP ile merkezi bir bilgi sistemi kurulmuş ve bu sistemde yargı ve yargı destek birimleri arasında fonksiyonel olarak tam entegrasyon sağlanmıştır.

UYAP, en başından itibaren e-imza alt yapısına uygun olarak tasarlanıp geliştirilmiştir. UYAP ile tüm yargı birimleri tarafından yapılan tüm yargısal işlemlerin, aynı şekilde Bakanlık teşkilatı tarafından yapılan tüm idari işlemlerin e-imza ile imzalanması, arşivlenmesi, e-imzalı belgelerin elektronik ortamda ilgili makam ve

birimlere gönderilmesi, avukatların ve vatandaşların internet üzerinden e-imza ile UYAP'a bağlanarak dava açmaları, dava dosyalarını tüm ayrıntılarıyla inceleyebilmeleri mümkün hale getirilmiştir.

Bu nedenlerle UYAP'ın söz konusu alt yapısını kullanmak üzere, 6 Eylül 2004 tarihli ve 25575 sayılı Resmî Gazete'de yayımlanan 2004/21 sayılı Başbakanlık Genelgesi uyarınca, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE) ile 28.03.2007 tarihinde "Nitelikli Elektronik Sertifika Temini Sözleşmesi" imzalanmıştır. Bu sözleşme uyarınca; hâkim, Cumhuriyet savcısı ve diğer yargı personeli için NES talepleri TÜBİTAK-UEKAE'ye ulaştırılmakta, TÜBİTAK-UEKAE tarafından NES ve parolaları üretilerek NES sahiplerine teslimi sağlanmaktadır.

Bu kapsamda 30.12.2008 tarihi itibariyle e-imza için başvuru sayısı 39.691, üretilen e-imza sayısı ise 30.000'dir. Buna göre hâkim ve savcıları ile diğer personel e-imzaları büyük ölçüde sağlanmış ve UYAP'ta e-imza kullanımına başlanmıştır.

5070 sayılı Elektronik İmza Kanunu gereğince, UYAP'ta e-imza ile yapılan işlemler tam anlamıyla bir belge niteliğini kazanacağından aynı işlemlerin hukuksal geçerlilik bakımından fiziki ortamda tekrar yapılmasına gerek kalmamaktadır. E-imzalı bilgi ve belgelerin son hali, doğru, tutarlı, değişmez ve güvenli bir şekilde UYAP veritabanında saklandığından yargı birimlerinde ve idari birimlerde tutulan defter ile kartonlara ve büyük ölçüde dosyalara da ihtiyaç yoktur.

UYAP'ta tam anlamıyla e-imza kullanımına geçilmesiyle yargılamaların makul sürede bitirilmesine, personel, emek, zaman, kırtasiye, ulaşım ve iletişim giderlerinden tasarruf sağlanmasına büyük katkıda bulunacağı öngörülmektedir. Bu nedenle e-imza kullanımına büyük önem verilmektedir [18].

2.2. Ulaştırma Bakanlığı

Ulaştırma Bakanlığı'nda Elektronik imza Başbakanlık Genelgesine göre kamu kurumlarına Tübitak tarafından temin edilmektedir.

Elektronik imza taleplerine istinaden yazılımlarda elektronik imza desteği analizi yapılmış, yazılımların uygun olduğu onayından sonra imza üretimi sürecine girilmiştir. Daha sonra sistemlerde imzalar kullanılmaya başlanmıştır.

Elektronik imza kurum içi ve dışı evrak sistemlerinde kullanılmaktadır. Şuan için Kurum içinde paraf ve onay kısımlarında, kurum dışından ise online elektronik imzalı evrak kabulünde kullanılmaktadır.

Elektronik imza kullanımı şuan için çok az sayıda denilebilir, ancak mobil imza entegrasyonu çalışmaları devam etmekte olup onunda faaliyete geçmesi neticesinde çok daha fazla sayıda başvurunun olacağı öngörülmektedir.

Ulaştırma Bakanlığı'na temin edilen elektronik imzaların geçerlilik süreleri 3 yıldır.

Elektronik imzanın uygulamasının yazılımlara entegrasyonunda çok fazla sorunla karşılaşılmamış, ancak personelin e-imzayı anlama ve kullanmalarında zaman zaman sorunlar oluşmuştur. E-imzanın sanal olmasından dolayı çekinceler oluşmuş bunlar zamanla aşılmıştır [19].

2.3. Bilgi Teknolojileri Kurumu (BTK)

Bilgi Teknolojileri Kurumu, Türkiye'nin ilk sektörel düzenleyici kurumudur. Aynı zamanda, Türk Telekom Kamu İhale Kurumu(KİK) statüsünden çıkartılarak özel hukuk hükümlerine tabi bir anonim şirket haline getirilmiştir.

ESHS'nin her türlü faaliyet ve işleyişinin ilgili mevzuat hükümlerine uygunluğunun incelenmesi, muhtemel hata, noksanlık, usulsüzlük ve/veya suistimallerin tespit edilmesi ve ilgili mevzuatta öngörülen yaptırımların uygulanması amacıyla yapılan bütün çalışmalar Telekomünikasyon Kurumu'na verilmiştir.

Telekomünikasyon Kurumu, ikincil mevzuat çalışmalarına başlamış ve öngörülen süreden önce Yönetmeliği hazırlamıştır [20]. Yapılan düzenlemeler çerçevesinde sertifika hizmet sağlayıcılarının yetkilendirilmesi ve denetlenmesi Kurum tarafından yerine getirilecektir.

Kanun, sertifika otoritelerinin yetkilendirilmesi ve denetlenmesi görevini Telekomünikasyon Kurumu'na vermiştir (EİK. md.15). Sertifika otoriteleri, Kurum'a yapacakları bildirimden başlamak üzere iki ay sonra faaliyete başlayabilirler (EİK. md.8). Bu düzenleme 99/93/EC sayılı AB Direktifi ile paralellik sağlamaktadır.

Bilgi Teknolojileri ve İletişim Kurumu olarak kurum içi yazışmalarda e-imza kullanabilmek için çalışmalar devam etmektedir. Kurum içerisinde kullanılan Doküman ve arşiv Yönetim Sistemini elektronik imza altyapısı ile entegrasyonu tamamen sağlanmış durumdadır. Ancak hâlihazırda kurum içi yazışmalarda elektronik imza kullanılmaya başlanmamıştır.

Bilgi Teknolojileri ve İletişim Kurumuna elektronik imza başvurusunda bulunan mevcut değildir. Ama BTK ile GSM Operatörleri arasında oluşturulan bir altyapı üzerinden elektronik ortamda elektronik imzalı resmi evrak alışverişi gerçekleştirilmektedir. Bu altyapı aracılığı ile GSM Operatörleri TURKCELL ve AVEA'dan yaklaşık 1000 tane resmi evrak elektronik imzalı olarak Kurum bünyesindeki Doküman ve Arşiv Yönetim Sisteminde İşleme tabi tutulmuştur.

5070 sayılı Kanununa göre güvenli elektronik imza elle atılan imza ile aynı hukukî sonucu doğurmaktadır ve elle atılan imza ile aynı ispat gücünü haizdir.

Elektronik ortamda yapılan iş ve işlemlere hukuksal geçerlilik kazandıran elektronik imza teknolojisi aynı zamanda da iş ve işlemlerin hızlı bir şekilde gerçekleştirilmesini sağlamaktadır[21].

2.4. Türkiye Cumhuriyeti Merkez Bankası

Türkiye Cumhuriyeti Merkez Bankası'nda proje temelinde ihtiyaç duyulan noktalarda e-imza kullanma çalışmaları devam etmektedir. Ayrıca, Bankaya ait bazı kurumsal e-posta adreslerinden gönderilen mesajlarda da sayısal sertifikalar kullanılmaktadır.

Elektronik İmzalar TÜBİTAK 'dan alınmıştır [22].

2.5. Bankacılık Düzenleme Ve Denetleme Kurumu (BDDK)

E-devlet dönüşümü kapsamında, kamu kurumları arasında bilgi/belge paylaşımının ve yazışmaların elektronik ortama taşınarak, bu konuda etkinliğin arttırılması yönünde yapılan çalışmaların ivme kazanması nedeniyle, BDDK e-imza ve e-devlet konusundaki gelişmelerin gerisinde kalmamak için e-imza destekli Bilgi Yönetim Sistemi (BYS) satın alınmıştır. Kurum içi ve dışı her türlü yazışmanın kâğıt ortamından elektronik ortama taşınmasını hedefleyen BYS dahilinde elektronik olarak yazışmalara eklenen imzaların hukuki geçerliliğinin temini için, 5070 sayılı Elektronik İmza Kanunu gereğince Nitelikli Elektronik Sertifika (NES) kullanılması zorunludur. Bu nedenle, 2004/21 sayılı Başbakanlık Genelgesi ile Kamu Sertifikasyon Merkezi olarak atanan Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE)'den tüm Kurum personeli için NES temin edilmiştir.

Satın alınan BYS Kurumda teste açılıp farklı birimler tarafından test edilip, alınan geri beslemelere göre iş akışları Kurumun iş akışlarına uygun hale getirildikten

sonra TÜBİTAK tarafından görevlendirilen personel Kuruma gelerek elektronik imzanın BYS içerisinde 5070 sayılı kanuna uygun olarak çalışıp çalışmadığını denetlemiş ve gerçekleştirdiği testlerden sonra herhangi bir sorun olmadığını Kuruma iletmiştir.

Elektronik imzanın gelişimi süresince, imzalanacak dokümanın formatı (ilk önceleri sadece text dokümanı imzalanabilirken şu anda tiff imzalanabilmektedir), imzalanacak dokümanın imzalanmadan önce imzalayacak kişiye gösterilmesi, sertifika iptal listelerinin (sil) tek bir çatı altında toplanamayarak her sertifika sağlayıcının kendi sil listesini yayınlaması ve piyasada bulunan elektronik imza ile bütünleşik yazılımların bu farklı listeleri okurken sıkıntı yaşamaları gibi sorunlarla karşılaşılmış, ancak zamanla bu sorunlar kamu kurumları, elektronik servis hizmet sağlayıcıları ve özel sektörün ortak çalışmalarıyla giderilmiştir.

Kurumda elektronik imzalı BYS kullanımı için tüm altyapı hazır olmakla birlikte gerçek zamanlı kullanıma henüz geçilmemiştir. Bu nedenle dışarıdan elektronik imzalı dilekçe veya başvuru kabul edilmemektedir. Fakat zaman içerisinde kullanıma geçilmesi planlanmaktadır [23].

2.6. Devlet Malzeme Ofisi (DMO)

Ofis elektronik imzayı Tubitak Kamu Sertifikasyon Merkezi sağlamıştır. Öncelikle kök sertifikaları üretilip sunuculara yüklenmiştir. Sonrasında sertifika Kamu Sertifikaston Merkezinde oluşturulmuş ve özel bir firma ile birlikte test çalışmaları yapılmış ve personel için nitelikli elektronik sertifika üretilmiştir. Şu anda Genel Müdürlükte görev yapmakta olan imza yetkisine sahip bütün personele elektronik imza sağlanmıştır. Doküman yönetim sistemi eğitimleri verilmektedir. Bu nedenle elektronik imza kullanımına henüz başlanılmamıştır. Öncelikle genel müdürlükte kullanılmaya başlanacak olan elektronik imza zaman içinde bütün bölge müdürlüklerinde kullanılmaya başlanacaktır. Elektronik imza özel bir firma tarafından geliştirilmiş olan doküman yönetim sistemi içerisinde kullanılacaktır [24].

2.7. Zeytinburnu Belediyesi

Belediyede elektronik imza iki şekilde kullanılmaktadır:

1- Personele tahsis edilen imza Tübitak'tan temin edilmiştir. Kullanıcılar belediye personelidir (toplam 5 adet).

2- Mobil imza (personelden isteyenlere). Türkcell işbirliği ile temin edilmiştir. Elektronik imza uygulaması belediye otomasyon yazılımlarına elektronik imza uyarlama yazılımları özel bir firma tarafından hazırlanmıştır. Elektronik ve mobil imza mükelleflerin vergi ödemelerinde kullanılmaktadır. Geçerliliği 3 yıldır. Şimdiye kadar herhangi bir sorun çıkmamıştır [25].

2.8. İSKİ

İSKİ, e-imza entegrasyonu için kullanacağı yazılım kütüphanelerini TÜBİTAK UEKAE'den temin etti ve Altyapısı 30 Haziran 2006'da incelenerek, e-imza test kütüphaneleri ve test sertifikaları yetkililere teslim edildi. Halen devam eden test çalışmalarının tamamlanmasından sonra İSKİ yerel yönetimlerde bir ilke imza atıp e-imzayı devreye alacak.

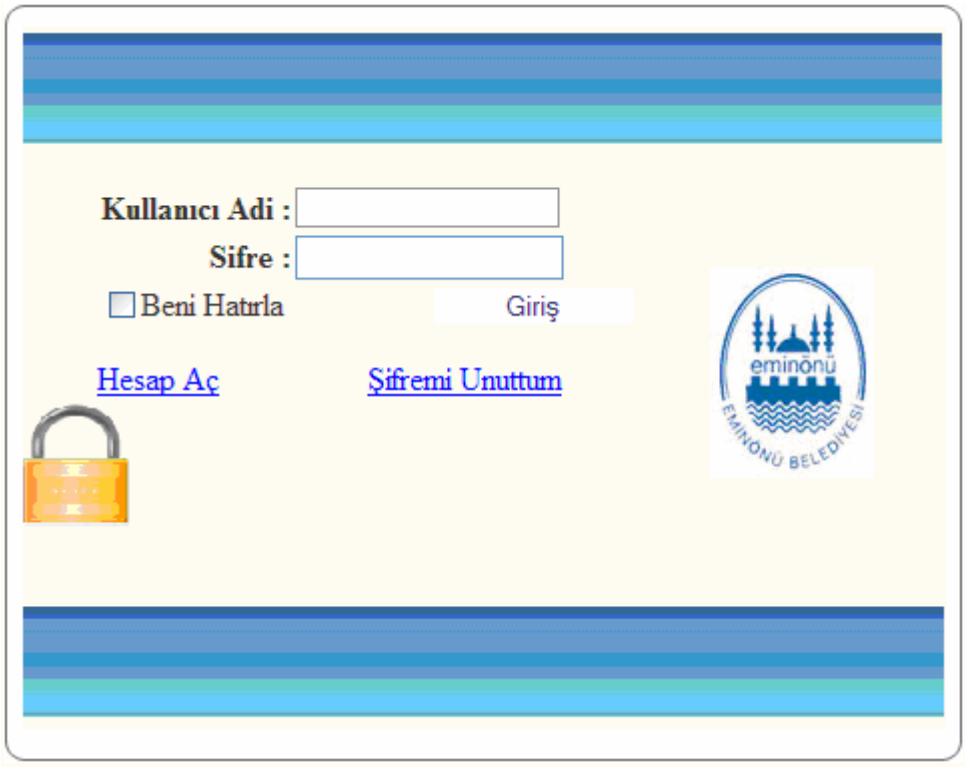
Abonelere yönelik yeniliklerin yanı sıra, İSKİ'ye ait kurumsal evrak yönetim sistemine de e-imza entegrasyonu çalışmaları başlatıldı. 3.400 adet PC'nin kullanıldığı İSKİ sistemlerindeki entegrasyon çalışmalarının tamamlanmasının ardından, kurum personeline akıllı kart üzerinde e-imza sertifikaları, kart okuyucuları ile birlikte teslim edilecektir [26].

3. UYGULAMA ÖRNEKLERİ

3.1. Eminönü Belediyesi E-İmza Uygulaması

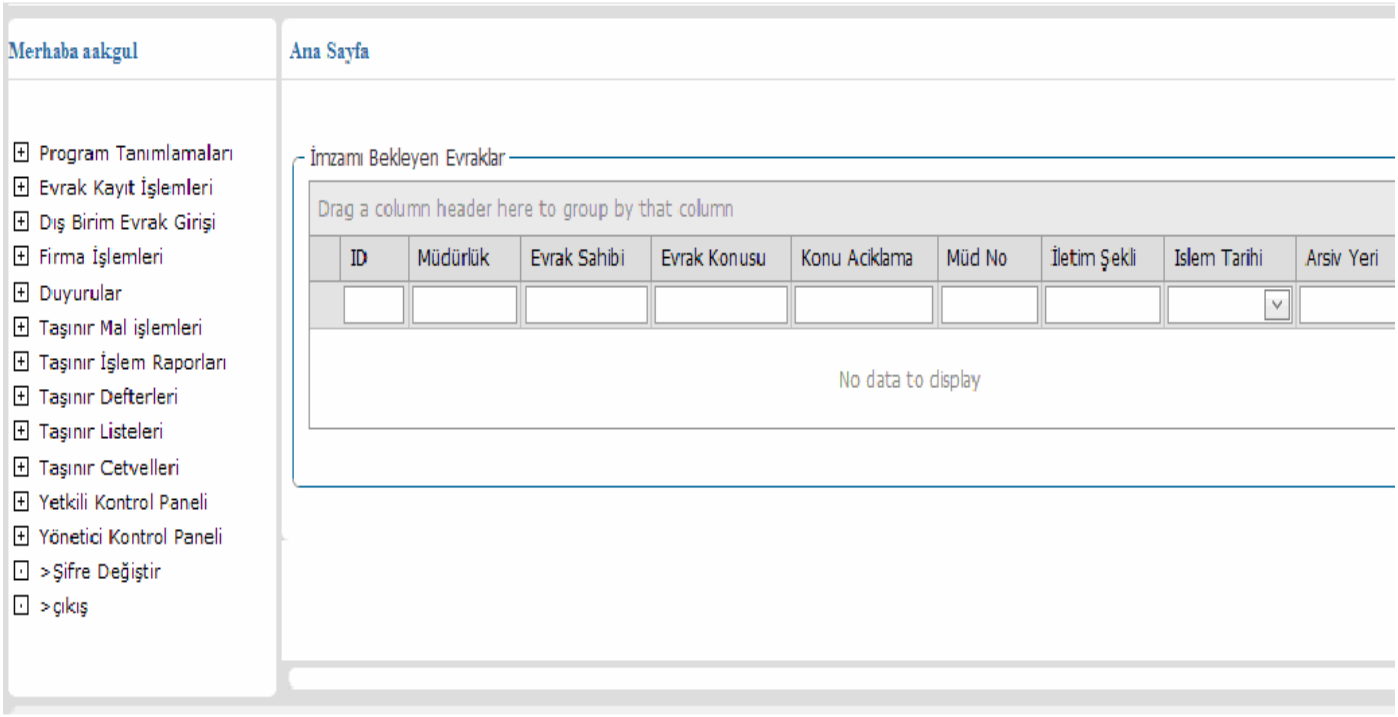
Bu uygulamada önce kurum içi sonra da bir kurum dışı yazışma örneği sunulmuştur[27].

Kurum içinde Bilgi İşlem biriminden Satın Alma birimine gönderilecek bir talep ele alınacaktır. Bunun için özel bir firmadan elde edilen bir yazılım kullanılmaktadır. Program açıldıktan sonra Şekil 5'te görülen giriş ekranı gelmektedir.



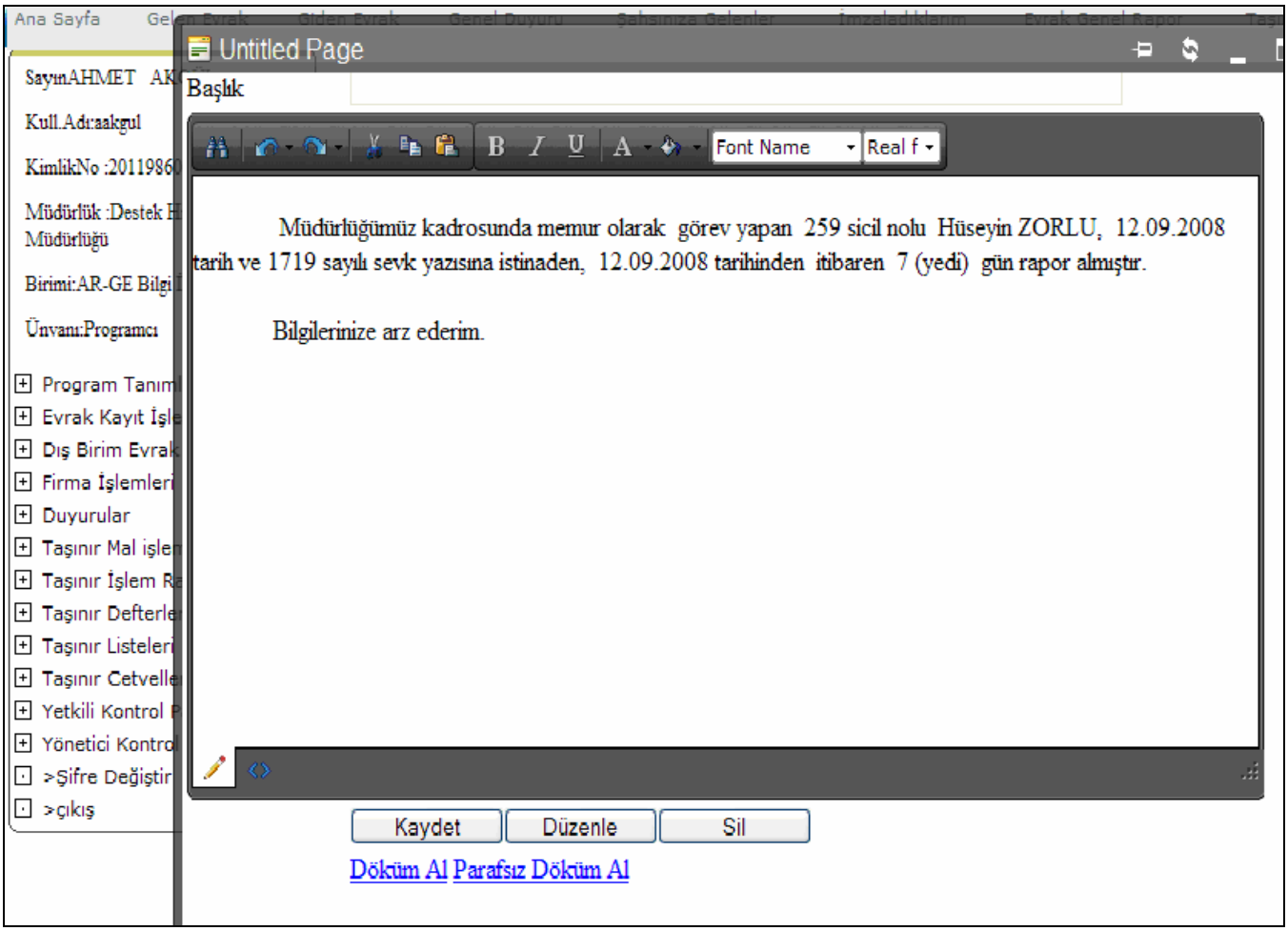
Şekil 5: Giriş Ekranı

Giriş ekranında Kullanıcı adı ve şifre bulunmaktadır. Kullanıcı adı ve şifre girilir.



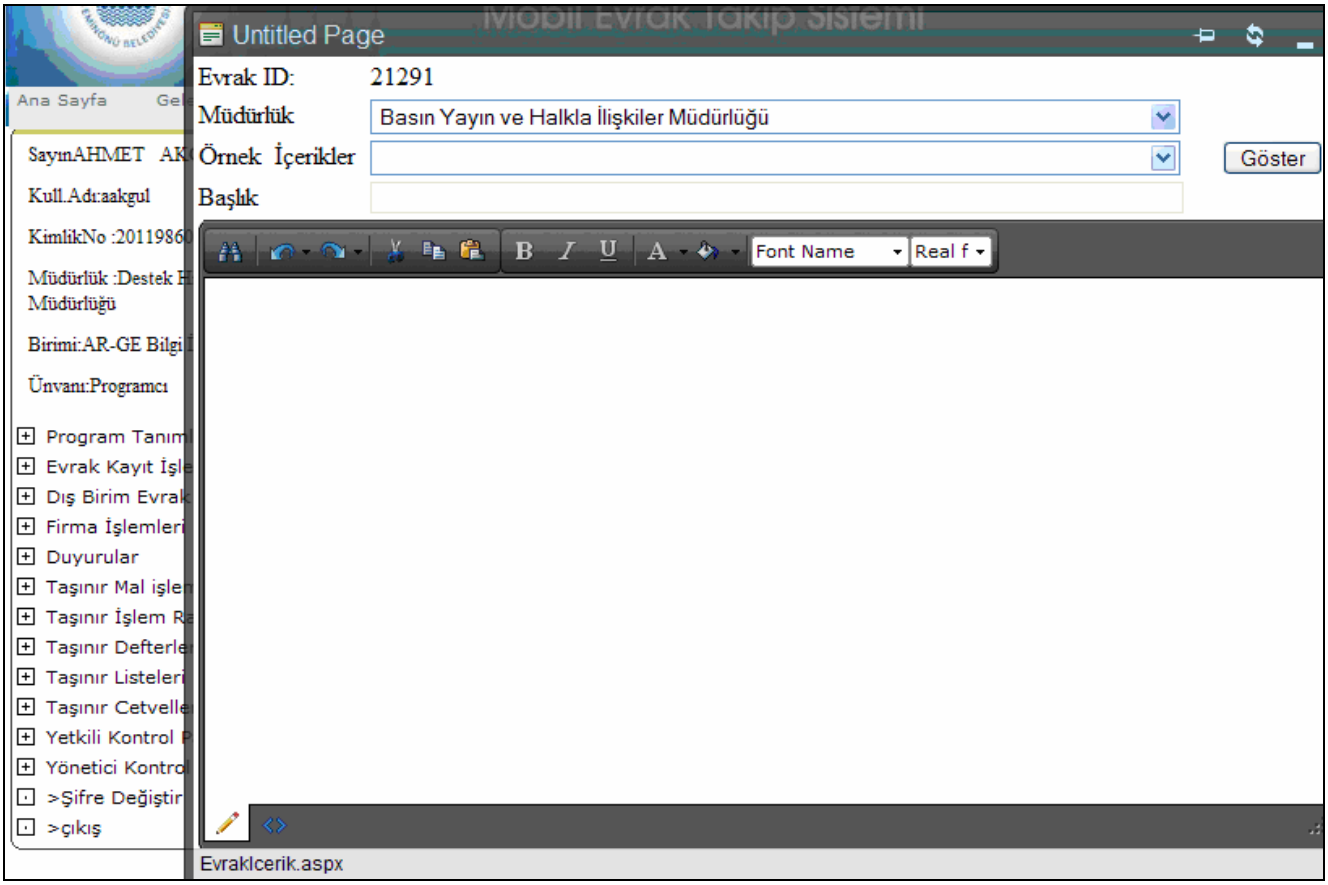
Şekil 6: İmza Bekleyen Evraklar

Kullanıcı adı ve şifre girildikten sonra Ana sayfa ekranı açılmaktadır. Burada ilgili birimlere gönderilmiş olan ve imzayı bekleyen evraklar görülmektedir. Bu ekranda henüz imzayı bekleyen herhangi bir veri bulunmamaktadır.



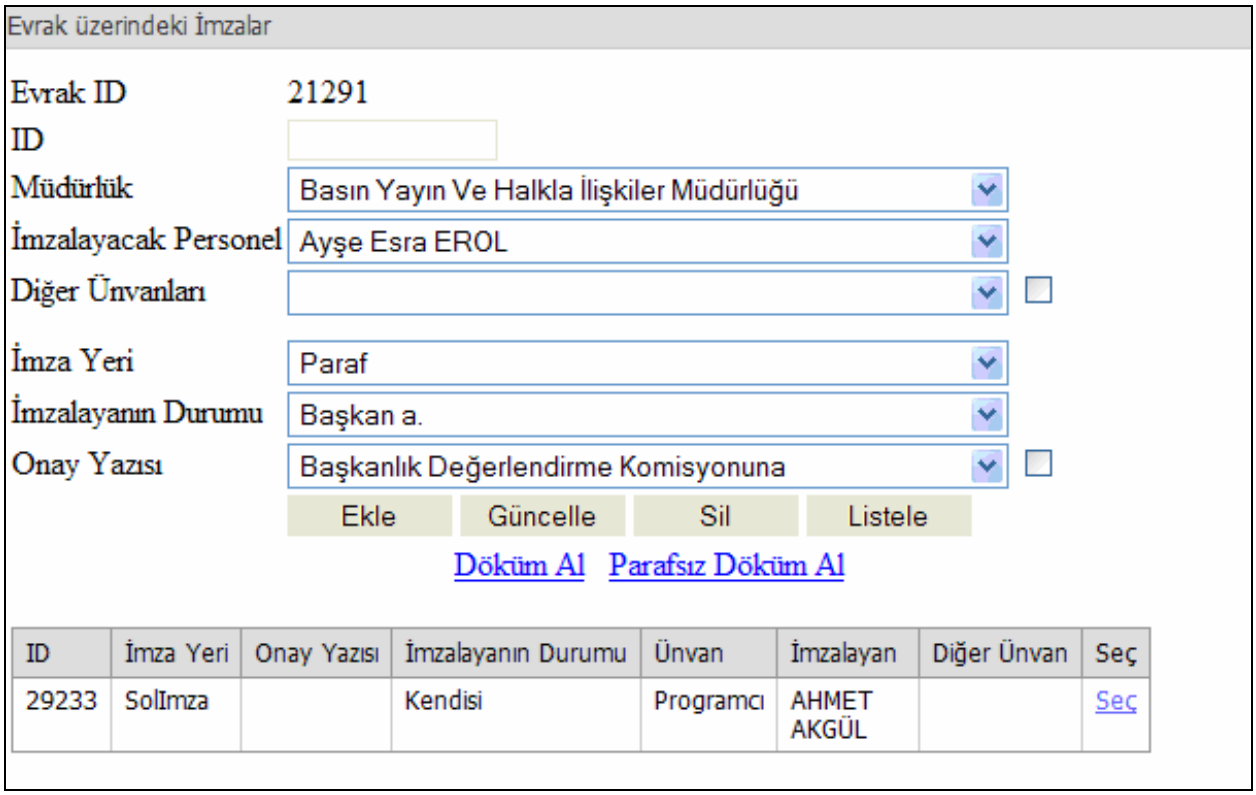
Şekil 7: Mesaj Yazma Editörü

İlgili birime gönderilmek üzere metin yazma editörüne mesaj yazılmaktadır. Deneme adında bir dosya oluşturulmuştur ve memur olarak görev yapan şahısa sevk için ilgili birime yazı yazılmaktadır.



Şekil 8: Mesaj Yazma Editörü

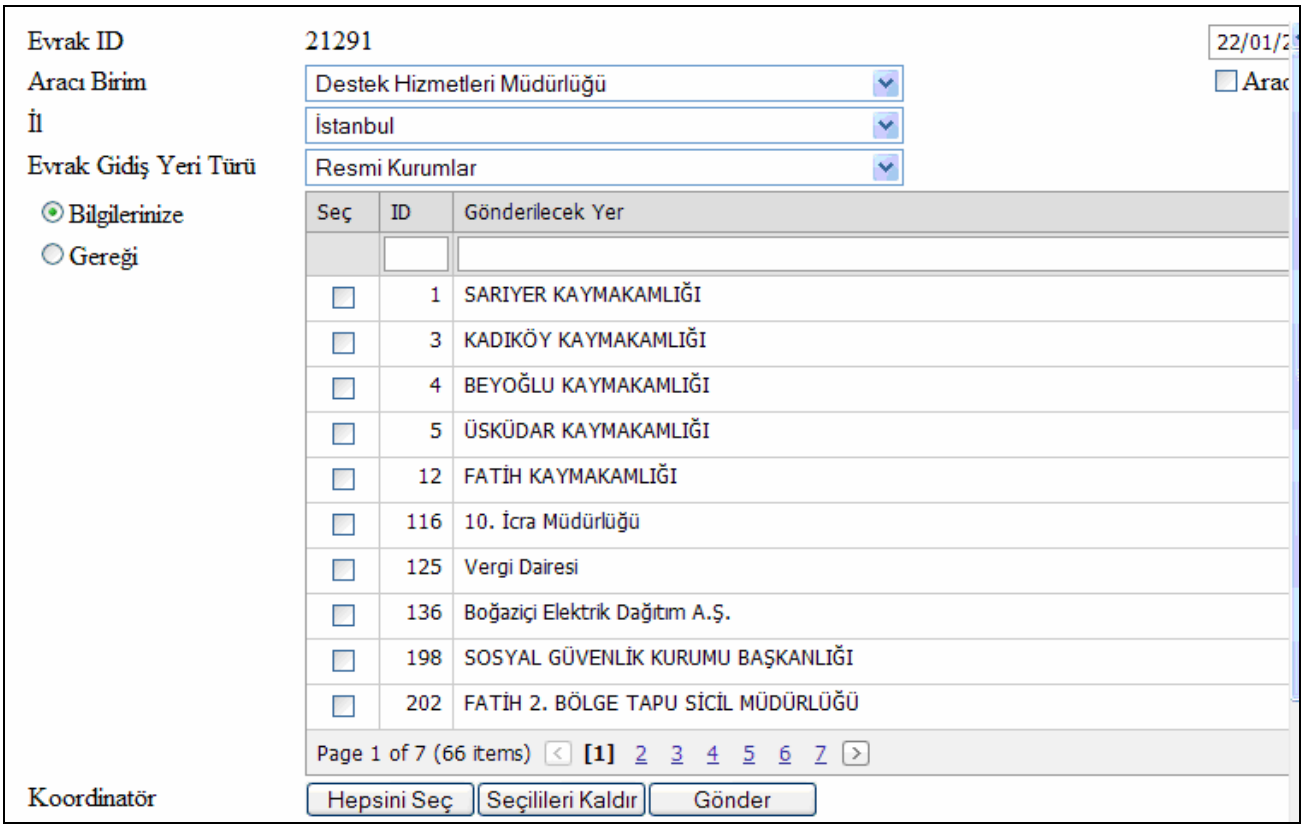
Evrak numarası verildikten sonra ilgili birim seçilir. Bu ekranda örnek içerikleri diğer bir deyişle hazır şablonları görmek de mümkündür. Bu deneme örneğinde Basın Yayın ve Halkla İlişkiler Müdürlüğü'ne bir yazı göderilmek istenmektedir.



Şekil 9: İmzalayanın Seçilmesi

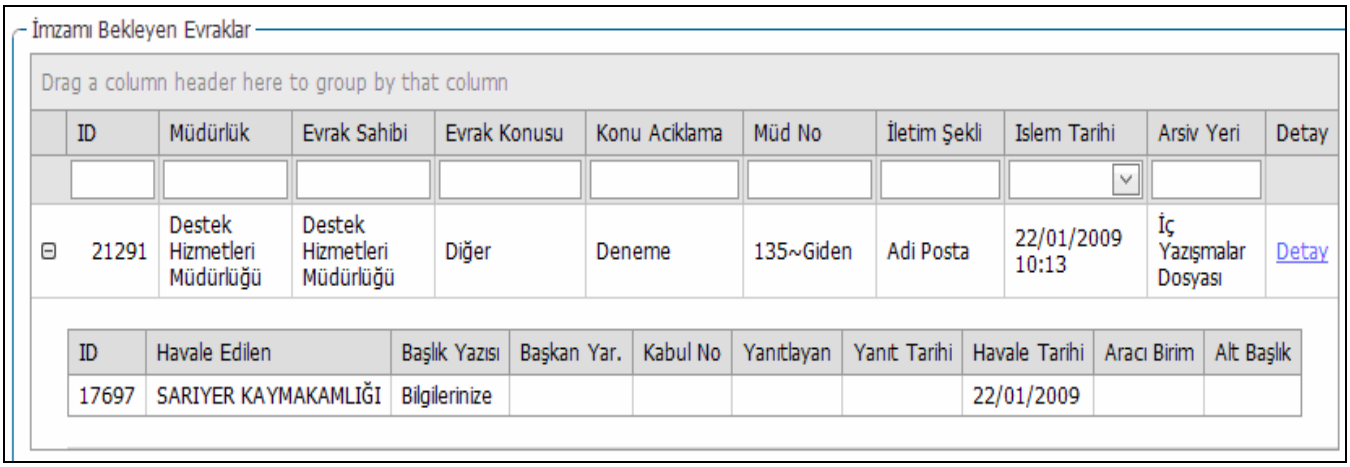
Bu ekranda imzalayacak personel, imzalayanın durumu ve onay yazısının nereye gidileceği belirtilmektedir.

İkinci durum olarak Şekil 10-18 arasında görülen kurum dışı bir yazışma örneği ele alınacaktır.



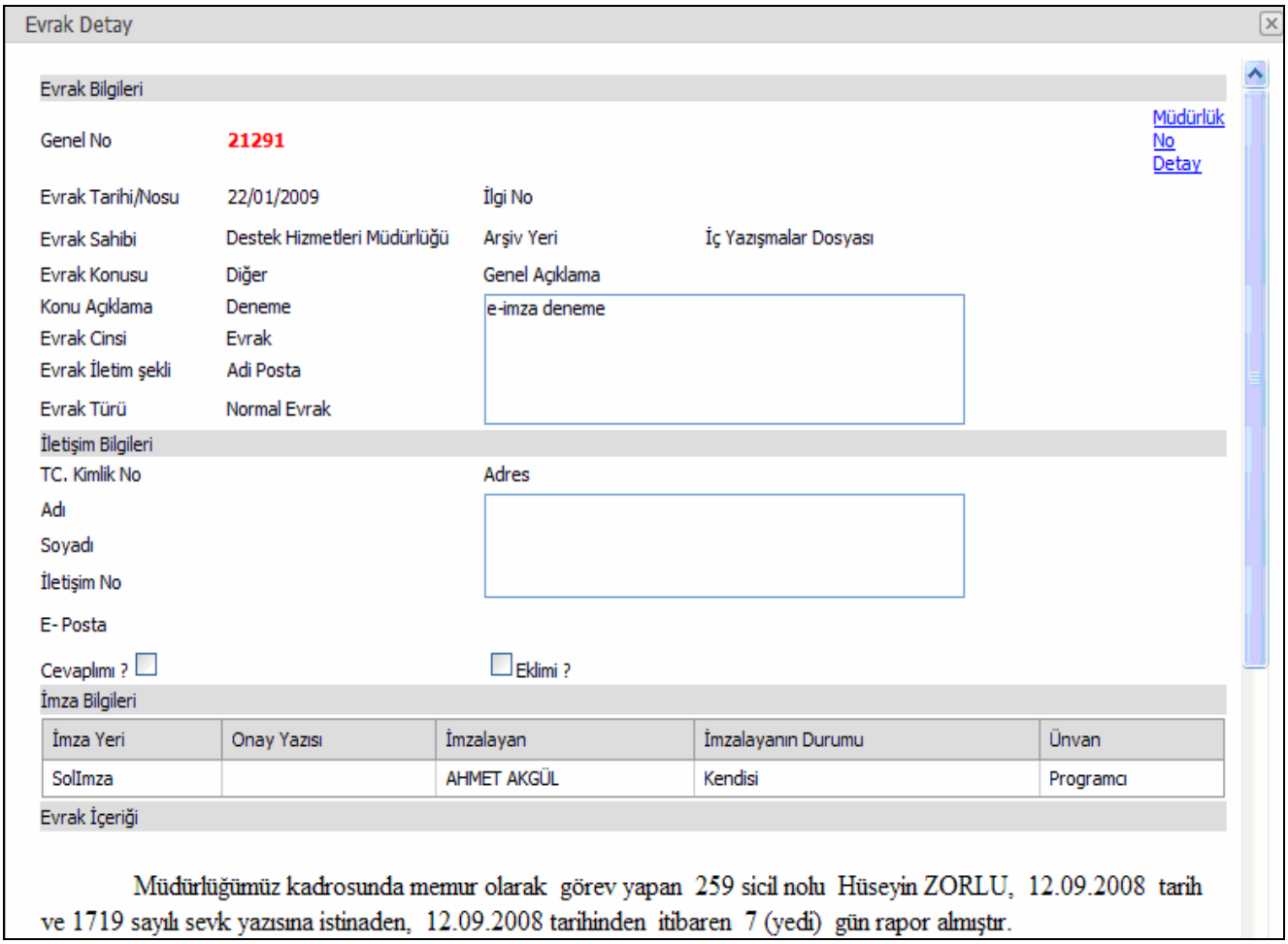
Şekil 10: Kurum Dışı Elektronik Belge Gönderimi Ekranı

Bu belediyede gönderilen evraklar Destek Hizmetleri Müdürlüğü aracılığıyla yapılmaktadır. Elektronik imza kullanan kurum bu ekrandan seçilir. Örneğimizde Sarıyer Belediyesine bir yazı gönderilmiştir.



Şekil 11: İmza Bekleyen Evraklar Ekranı

Başlangıçta imzayı bekleyen evraklar ekranı boşken, şu anda Sarıyer Belediyesi'ne gönderilmek üzere oluşturulan elektronik belge bulunmaktadır.

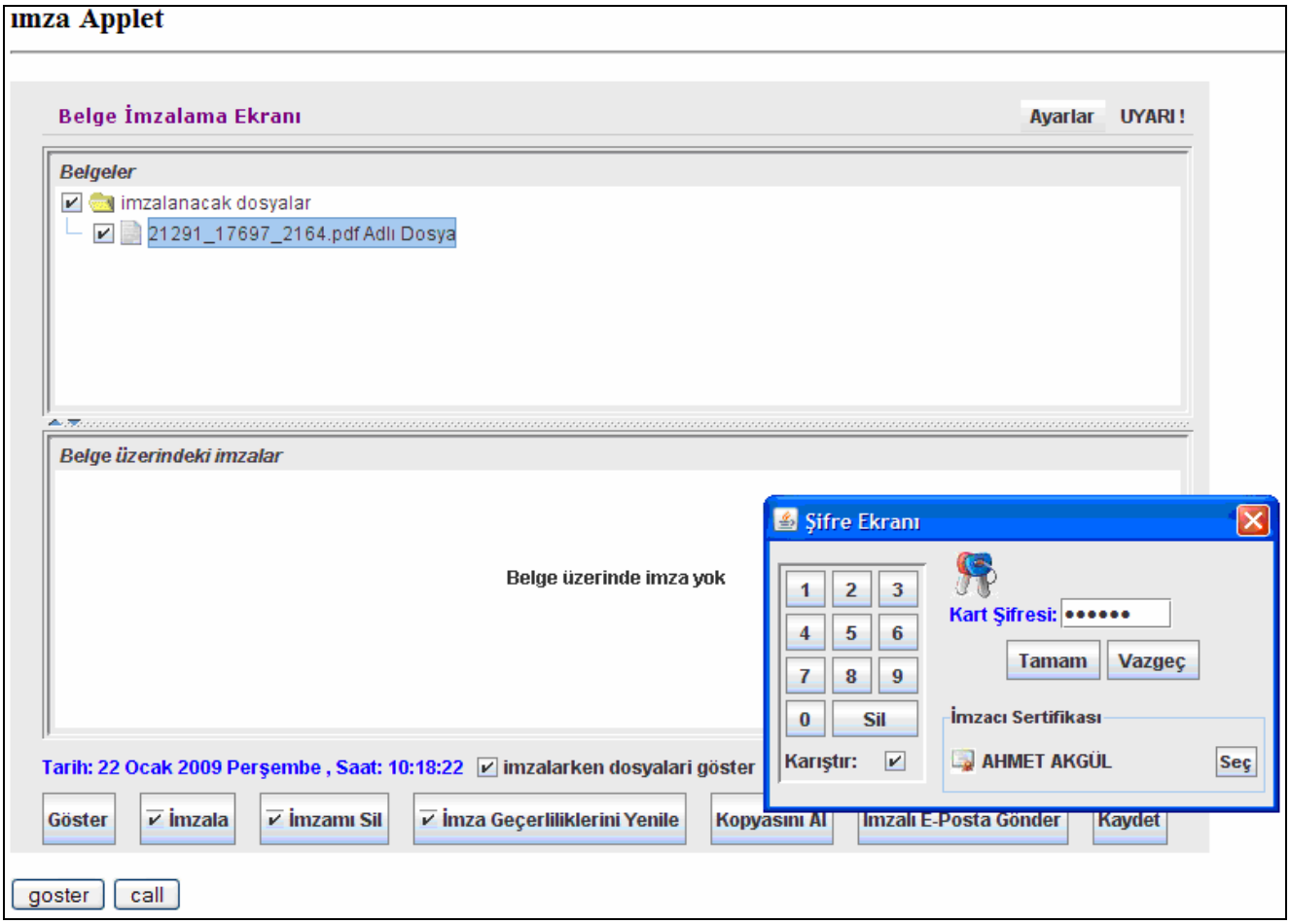


Şekil 12: Evrak Detay

Bu ekranda gönderilecek elektronik evrakla ilgili detaylı bilgiler bulunmaktadır. Evrak sahibi, genel açıklama, evrak türü, elektronik imzayı atan kişi, unvanı ve evrakın içeriği bu ekranda gösterilmektedir.

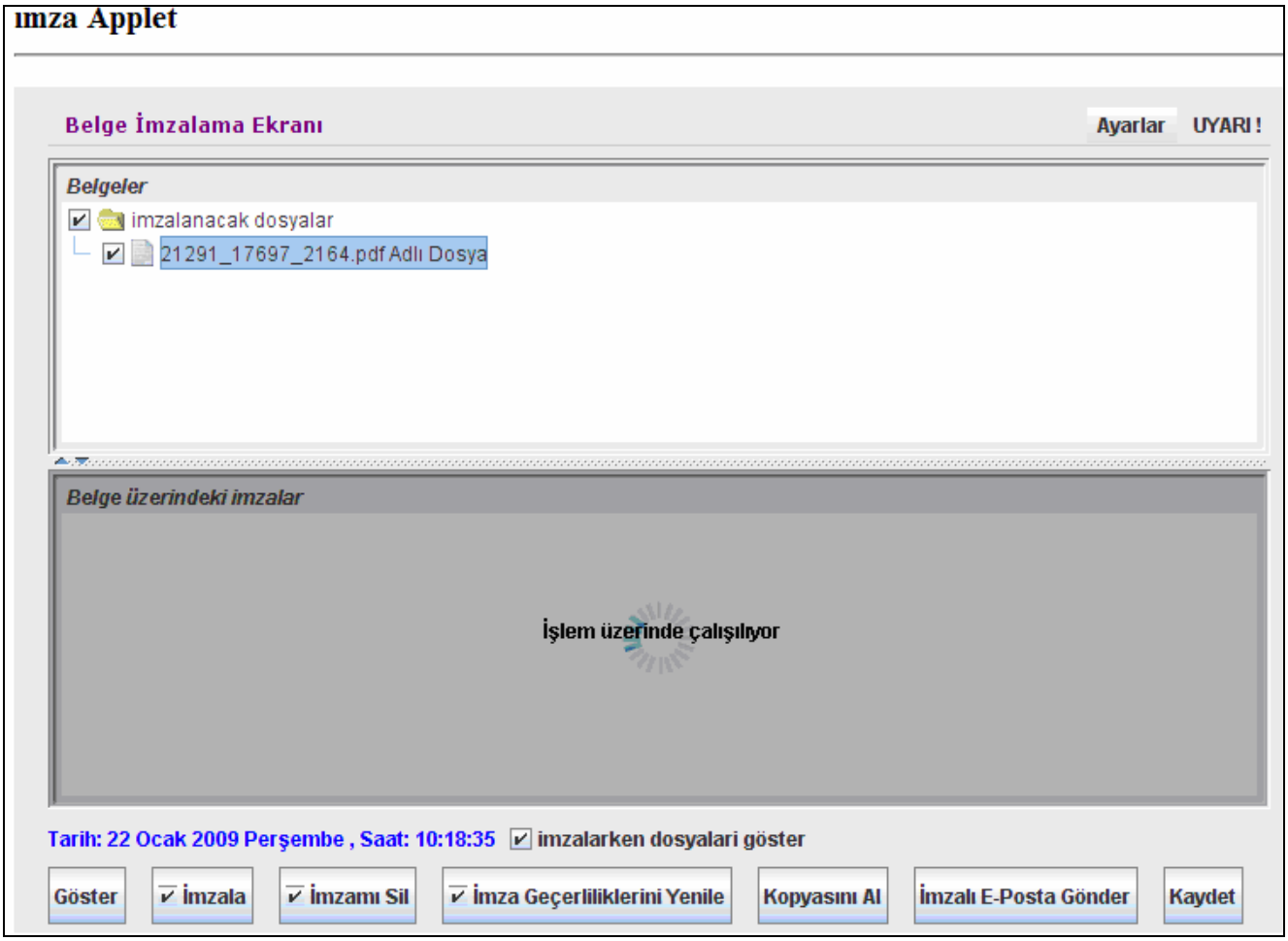
Şekil 13: Kurum dışına gönderilecek olan evrakın PDF olarak görünümü

Bu ekranda metnin PDF ortamında nasıl göründüğü kontrol edilmektedir. Mesajın içeriği görüldükten sonra diğer aşama bu metni imzalamaktır.



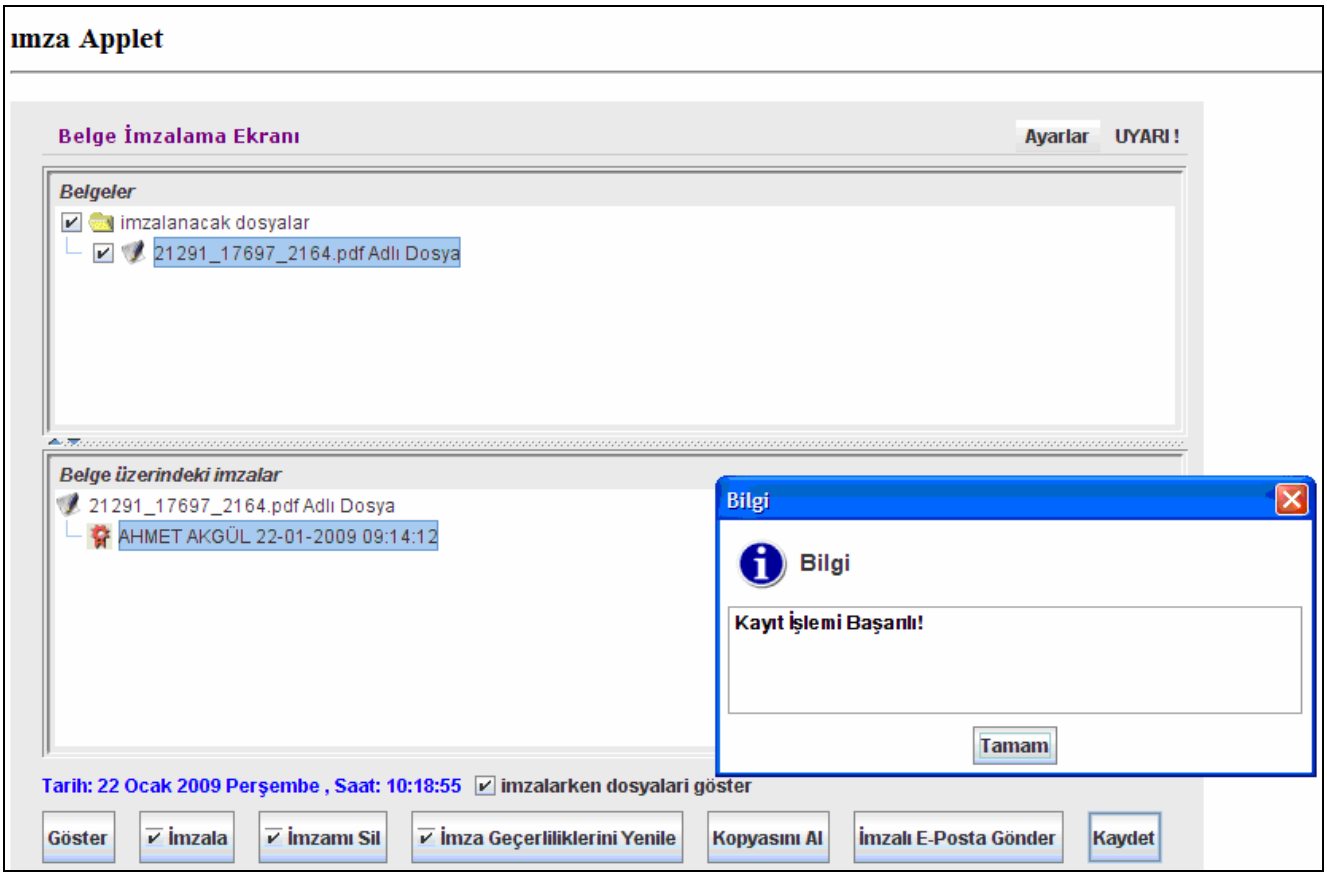
Şekil 14: İmza Applet

İmzalanacak dosya seçildikten sonra Şifre ekranı gelmektedir. İmzacı sertifikası bilgisi verilmektedir. Kart şifresi girildikten sonra dosya imzalanacaktır.



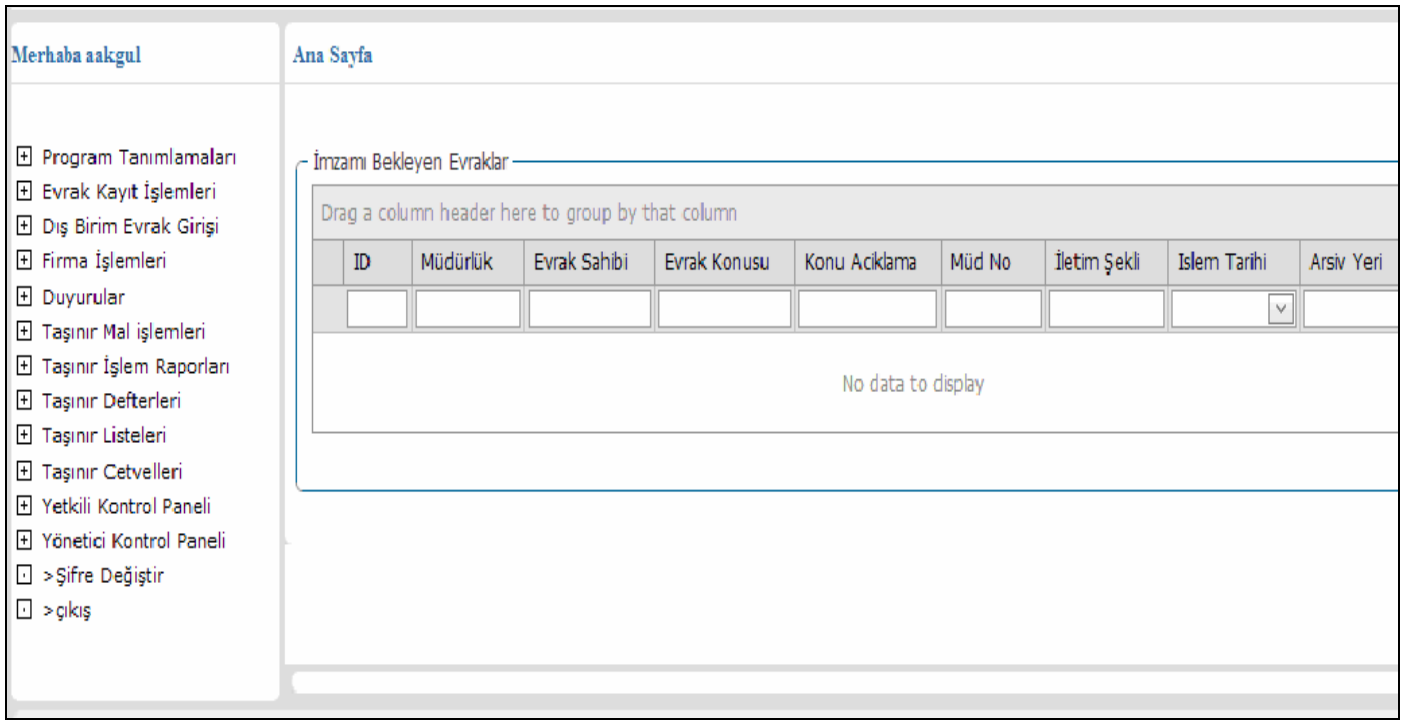
Şekil 15: İmza İşleminin devam edilmesi

İmzalama süreci birkaç saniyeyi almaktadır. Burada imzalama süreci devam etmektedir.



Şekil 16: İmza işleminin gerçekleştirilmesi

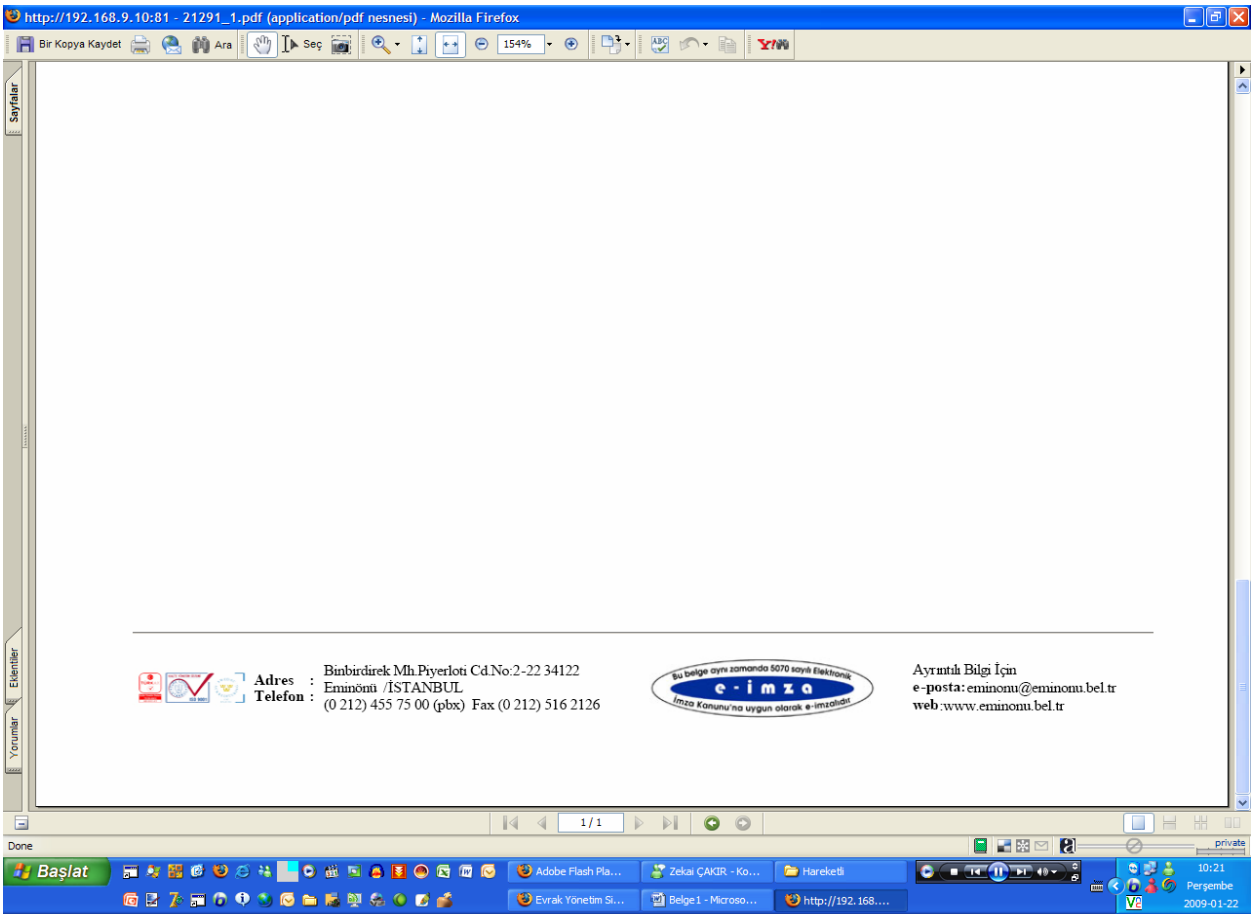
İmzalama işlemi başarıyla sonuçlanmıştır. Belge üzerindeki imzalar bu ekranda görülmektedir. İmzalama işlemi bittikten sonra ana sayfaya döndüğümüzde imza bekleyen evraklar ekranının boşaldığını görmekteyiz.



İmza Yeri	Onay Yazısı	İmzalayan	Ünvan	Diğer Ünvan
SolImza		AHMET AKGÜL	Programcı	

ID	EvrakID	HavaleID	Imzalayan	Imza Tarihi
8412	21291	17697	AHMET AKGÜL	22/01/2009

Şekil 17: İmzalanan Evrak Detayı



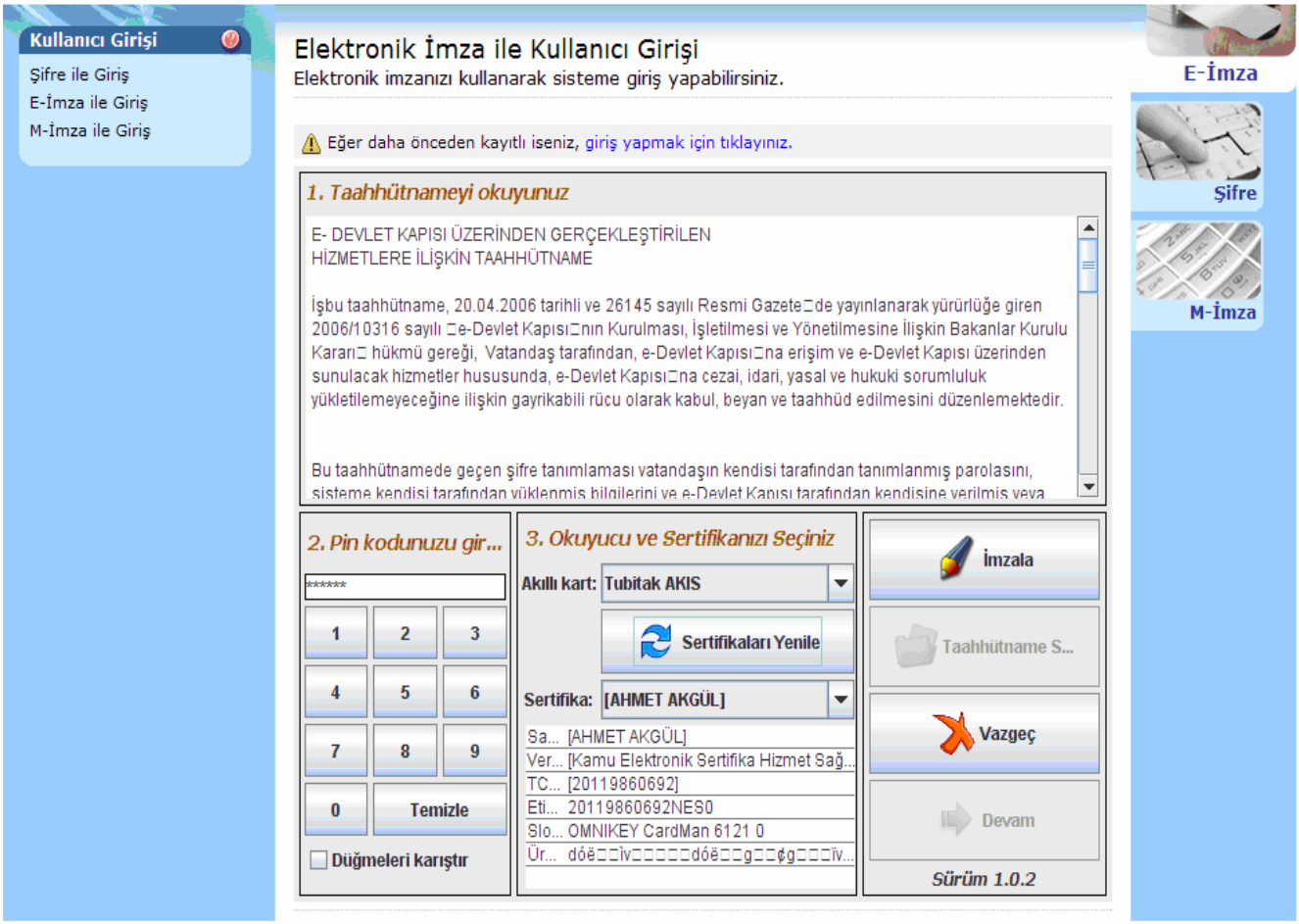
Şekil 18: E-İmzanın gönderilecek olan belgenin alt kısmında gösterilmesi

3.2. E-devlet Uygulaması (www.turkiye.gov.tr)

Şekil 19: e-devlet (www.turkiye.gov.tr) Ana sayfası

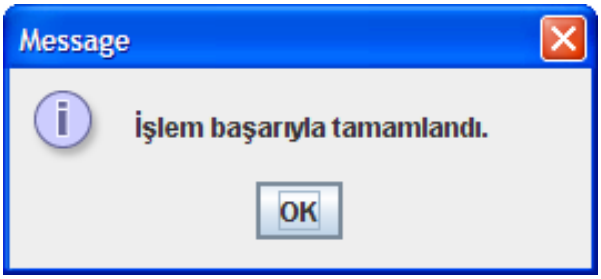
Devletin kısa yolu e-Devlet ana sayfasında şifre ile giriş, e-İmza ile giriş ve M-İmza ile giriş imkânları bulunmaktadır. Uygulamamızda e-İmza ile giriş yapmak için Akıllı kartın edinildiği firma seçilmiştir. Kamu Kurumları Tübitak'tan sertifika edindiği için Tübitak seçildi. Akıllı kart bilgisayara tanıtıldığı için otomatik olarak sertifika sahibi ile bilgiler ekrana gelmektedir. Sertifika Sahibi, versiyonu, TC kimlik numarası, etiketi ürün detayını görmekteyiz.

1.aşamada taahhütnameyi okuduktan sonra, ikinci aşamada Pin kodu girilmekte 3. aşamada okuyucu ve sertifika seçilmiştir.

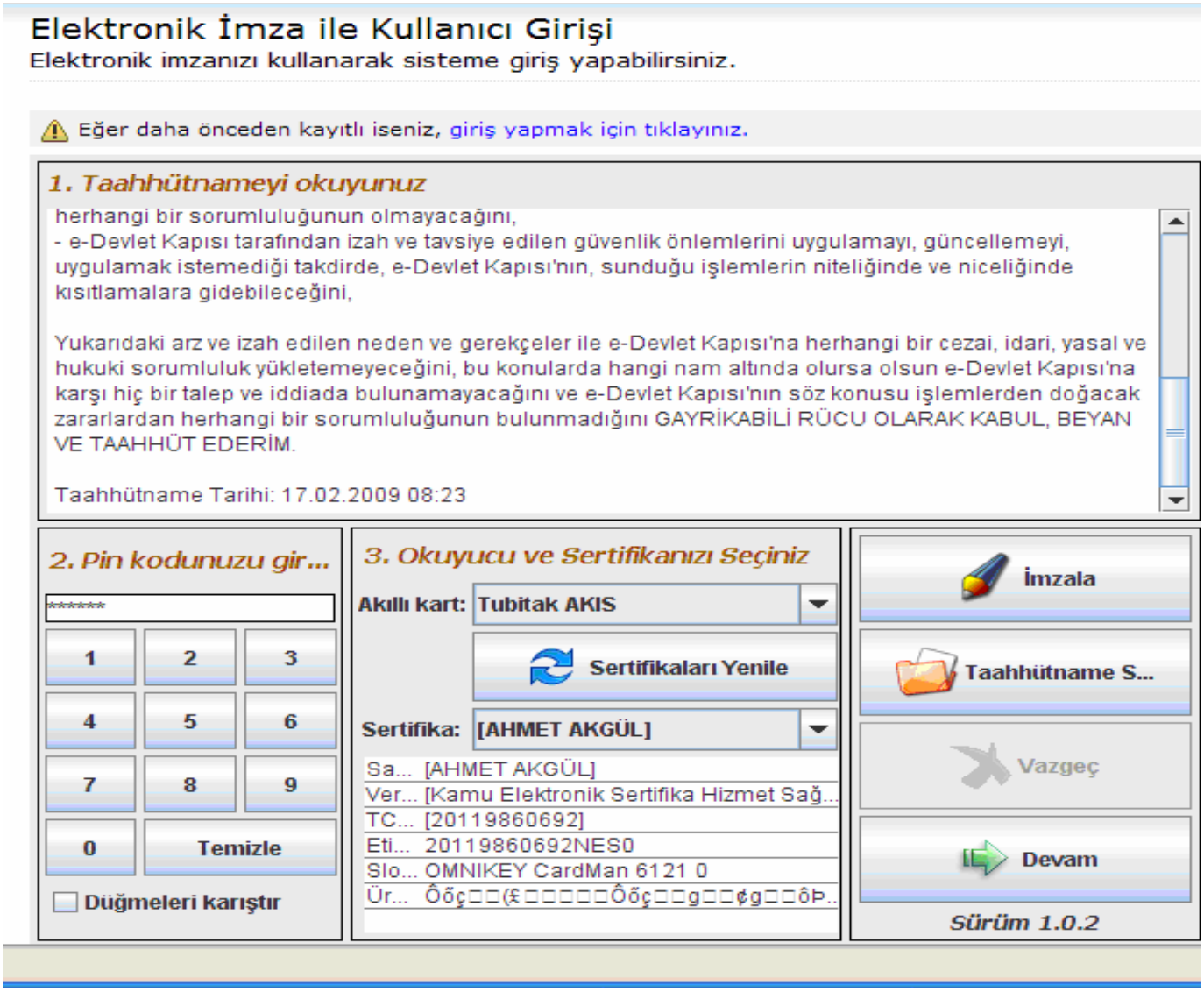


Şekil 20: E-devlet e-imza ile giriş ekranı

İmzala butonuna bastıktan sonra girilen bilgiler doğru olduğu için işlemimizin başarıyla tamamlandığı mesajı verilmektedir.

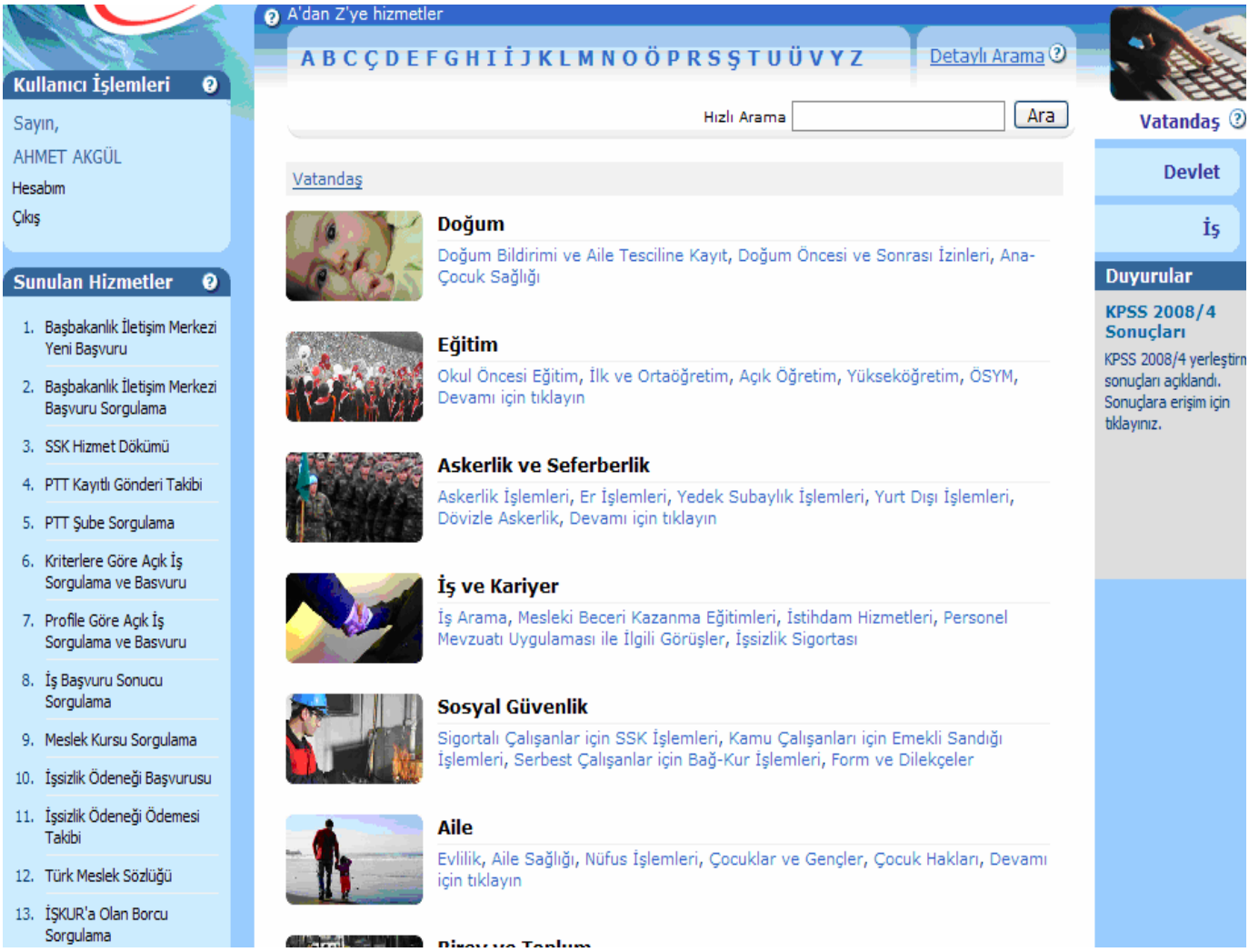


Şekil 21: e-İmza ile girişin tamamlanması



Şekil 22: İşlemlere devam etmek için gelen ekran

E-imza ile giriş yapıldıktan sonra ekrana Devam butonu aktif olarak gelir. Devam butonuna tıklandıktan sonra sertifika sahibine ait sayfa gelmektedir.



Şekil 23: E-imza Sahibine ait Sayfa

Bu ekranda e-imza ile giriş yapılıp devam butonuna bastıktan sonra elektronik sertifika sahibi ile ilgili sayfa açılmıştır. Kullanıcı bu sayfadan devlet ile ilgili istediği bütün işlemleri e-imzası sayesinde yapabilmektedir.

4. KAMU KURUMLARINDA E-İMZA UYGULAMASINDA KARŞILAŞILAN SORUNLAR VE ÇÖZÜM ÖNERİLERİ

4.1. Genel Sorunlar

Rekabet ve bunun getirdiği verimlilik arayışı son yıllarda Türkiye'de kurumları iş süreçlerini yalınlaştırmaya ve elektronik ortama almaya zorlamaktadır.

5070 sayılı E-İmza Yasası'nın yürürlüğe girmesi kuşkusuz bu pazarı olumlu yönde etkileyecektir. İlk başta Elektronik Sertifika Hizmet Sağlayıcıları sayısal sertifikaların faydalarını ve çeşitli olası uygulama alanlarını tanıtırken kurumlarda ve kullanıcılarda belli bir farkındalık yaratacaklardır. Yasanın istisna kabul ettiği tapu, evlilik, veraset, noter gibi alanlar dışında belgelerin elektronik ortamda da yasal bağlayıcı olarak kabul edilmesi elektronik ortamda doküman yönetimi yatırımlarının sadece kurum içi kullanılan bir lüksten daha öte büyük faydalar sağlayacak bir zorunluluk olduğunu göstermesi açısından önemlidir. Ancak burada iş akışının imzanın çok daha fazlası olduğunu, gerçek ve olması gereken yasal bağlayıcı e-imza uygulamalarının ise sadece basit bir doküman yönetimi yazılımı ile gerçekleşemeyeceğini iyi anlaşılması gerekiyor. Bu konuda büyük bir bilgi eksikliği vardır.

E-imza yasasının yürürlüğe girmesi, ardından da e-imza sertifika sağlayıcı kurumların lisanslarını almalarıyla canlanması umudedilen pazar, henüz bekleneni verememiştir. E-dönüşüm altyapılarını geliştirmeyen kamu kurumlarının e-imza sertifikalarını alamadıkları görülmüştür.

UEKAE'nın kurumlara e-imzaya yönelik hazırladıkları yazılımı yükleyebilmeleri için öncelikle kurumun e-dönüşüm altyapısını tamamlaması gerekmektedir.

Kamu kurumlarının yanı sıra bankaların da 5070 sayılı e-imza yasası kapsamında altyapı çalışmalarını tamamlayarak sertifika almaları gerekmektedir. Banka mudilerinin elektronik imza uygulaması olmamasından dolayı karşılaşacakları çeşitli üzücü olaylarda (hacker'ların şifreleri kırması, bankadan bankaya mudiden habersiz EFT yapılması, yine müşterilerin haberi olmadan hesaplarda oynamaların gerçekleşmesi gibi) yakın gelecekte açacakları davalar gündemin önemli bir maddesi

olacaktır. Sorun bankaların 5070 sayılı yasayı farklı yorumlamalarından kaynaklanmaktadır. Yakında e-imza davaları patlayacaktır ve e-imza mağdurları ortaya çıkacaktır. Elektronik imza uygulamasına geçmeyen bankaların yargı önünde hem teknik hem de hukuki açıdan haksız duruma düşecektir. Konu yargıya intikal ettiğinde e-bankacılığın gereği olarak bu işlemin yapılması gerektiği anlaşılacaktır.

Kamu kurum ve kuruluşları e-imzaya geçmek için çok etkin bir çalışma gerçekleştirmemişlerdir. Sonuç itibariyle kamu kurum ve kuruluşları e-imza kullanmadıkları için vatandaşlar da kamuyla olan işlemlerinde e-imza kullanmaya ihtiyaç duymamaktadır.

Kamu tarafında vatandaşa dönük yönü ile yakın zamanda gelişecek avukat portalı gibi farklı uygulamaların oluşması yanında, özel sektör tarafında da bankacılık e-imza bütünleşmesi ve piyasadaki yazılımlara elektronik imza bütünleşmesi çalışmalarına da ihtiyaç duyulacaktır.

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

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.

Elektronik sertifika hizmet sağlayıcılarının dağıttığı elektronik sertifikalarda yer alan bilgiler doğru kabul edilmektedir. Ancak bu konuda karşılaşılacak yanlış kimlik bilgileri sisteme olan güveni büyük ölçüde zedeleyecektir. Bu nedenle ESHS, sıkı bir şekilde denetlenmeli, gerekirse sorumlulukları yeniden gözden geçirilmelidir. Bu konuda denetleme ve düzenleme görevi Telekomünikasyon Kurumuna ait olduğundan Kurumun teknik bilgi düzeyi yüksek yeterince uzman personeli bulunmalıdır.

Daha zorlu bir sorun, sayısal imzanın kendisiyle ilişkilidir. Sayısal imza matematiksel olarak tam bir kesinlikle tanımlanmış olmasına karşın, uygulamalarda imzanın imzalanmış veriyle birlikte nasıl oluşturulacağı, nasıl taşınacağı ve nasıl korunacağına ilişkin yerleşmiş bir standart henüz bulunmamaktadır. Bu durumda,

birbirinden bağımsız taraflarca imzalanmış farklı belgelerin diğer taraflarca sağlıklı bir biçimde doğrulanmasında güçlükler yaşanması kaçınılmazdır.

Benzer bir sorun, sertifikanın ve gizli anahtarın taşınabilir olmasını sağlayan ve gizli anahtarın korunması için güvenilir bir araç olarak bilinen akıllı kart veya tokenlara ilişkin bulunmaktadır. Akıllı kartların kullanımı, bilgisayara dışarıdan bir akıllı kart okuyucusunun tanıtılmasıyla mümkündür.

Akıllı kart okuyucuları (veya tokenlar) belli bir kurulum programı gerektirmekte ve işletim sistemine ve hatta aynı işletim sisteminin farklı sürümlerine bağlı olarak çalışmaktadır. Bu sistemlerin bilgisayar kasasında standart bir sürücü olarak yer almaması, okuyucuların kullanım kolaylığı açısından başka bir sorundur. Hareket halinde olan bir kullanıcı için gittiği her yerde okuyucu bulabilmesi veya okuyucusunu beraberinde (gittiği her yerde kurulum yapmak üzere) taşıması kullanımı güçleştirmektedir. Daha da güç olanı, belirlenmiş standartların yetersiz gerçekleştirimleri sonucu kimi durumlarda her kartın her okuyucuyla birlikte uyumlu olmamasıdır.

Elektronik imzanın yaygınlaşmasında devlet öncü rol oynamalıdır. Elektronik İmza Kanununun hayata geçirilmesi ile birlikte devlet hizmetlerinde ve kurumların iş yapma yöntemlerinde büyük değişimlerin yaşanması kaçınılmaz hale gelecektir. Bu nedenle gelişmelerin zamanında farkına varılarak kamu kurum ve kuruluşları, iş süreçlerini gözden geçirmeli, e-devlet kurumu olmanın gereklerini yerine getirmelidirler.

4.2. Kurumlardaki Durum ve Alt Yapı

4.2.1. Telekomünikasyon Kurumu (BTK)

Elektronik imza teknolojisi oldukça karmaşık bir teknoloji olduğu için uygulama aşamasında birçok teknik problemle karşılaşılmaktadır. Standartlar henüz tam oturmamıştır. Diğer taraftan elektronik sertifika hizmet sağlayıcısı olma maliyetleri oldukça yüksek olup, sertifika pazarı gelişim sürecindedir.

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.

4.2.2. E-Devlet (www.turkiye.gov.tr)

Elektronik ortamda sunulacak kamu hizmetlerinin tek bir kapıdan verilmesini sağlayacak olan e-devlet kapısının açılması önemli bir gelişmedir. Ancak öte yandan 19 kurumun içeriklerinin toplanması, uyarlanması, koordinasyonu ve bilgi bütünlüğünün sağlanması, servislerin vatandaş için kullanılabilir hale getirilmesi için birtakım kanun değişikliklerinin yapılması gerekmektedir. Bunlar yapılmadan açılacak bir e-kapı, aceleye getirilmiş ve içi boş bir uygulama olmaktan öteye gidemeyecektir.

Gerek e-dönüşüm Türkiye İcra Kurulu ve Hükümet, gerekse Türksat e-kapı'nın bir an önce açılmasını isterken öte yandan içeriği tamamlanmayan, koordinasyonu sağlanmayan, servis çeşitliliği olmayan bir e-kapı'nın aceleye getirilerek açılmasının, projenin ölü doğumuna yol açacağı endişesini de beraberinde getirmektedir.

E-kapı'nın içinde yer alacak kurum bulunmaktadır ama öbür tarafta da şartname ile kısıtlanmış durumdadır. Bazı kurumlar henüz girmeye uygun değildir, uygun olmayanları uygun olanlarla değiştirmekle ilgili değiştirme kararı çıkamamıştır. Sonuçta kurulu bir araya getirip karar aldırmak zor bir iştir. e-devlet kapısı üzerinden verilecek her bir pilot hizmette, gerekli olan veri ya da uygulama bütünleştirilmesi için, veri sahibi kurumlarla, Türksat arasında veri paylaşım protokolünün yapılamamasının projede içerik sıkıntısına yol açmıştır. İcra kurulunda, e-Hizmetler Danışma Kurulu'nda yapılan çalışmalar yeniden değerlendirilmiş ve e-devlet kapısına yönelik hazırlanan yeni tasarım kurulun onayına sunulmuştur. Projenin donanım ve yazılım sistemlerinin kurulmuş, sırada pilot e-hizmetlerle kullanıma ve doğrulanmaya sunulması aşaması bulunmaktadır. Bir yaygınlaştırma süreci olan ikinci aşama için gerekli standart bütünleştirme yapısının ve e-hizmetlere dönüştürülecek kamu hizmetlerinin envanteri çıkarılacaktır.

Adalet ve Sağlık bakanlığına ilişkin e-devlet kapısına yönelik fizibilite raporlarının ilk sürümü hazırlanmıştır. Emekli Sandığı, Bağkur ve Emniyet Genel Müdürlüğü'ne yönelik çalışmaların yanı sıra 'ticaret' konulu fizibilite çalışmaları da

ilgili kurumlar ile başlatılmıştır. Yazılım geliştirme sürecinde merkez yazılımda prototip aşamasına gelinmiştir. Kurumlarda yapılan görüşmeler ile "çoğu kurum" tarafında gerekli çalışmalar başlatılmıştır. Buna göre, Başbakanlık ile BİMER projesinin bağlantısı yapıldı. www.turkiye.gov.tr alan adının transferi gerçekleştirildi. Maliye Bakanlığı Gelir İdaresi Başkanlığı ile e-beyanname ve vergi borç sorgulama konusunda destek çalışmalar gündeme geldi. Emniyet Genel Müdürlüğü ile e-Polis ihbar, Pasaport ve ehliyet başvurusu ile ortak yazılım geliştirme süreci ele alındı. İşkur ile, iş başvurusu, işsizlik sigortası ve kurumun yeni yazılımına yönelik bütünleştirme çalışmaları iş planına girdi. Maliye Bakanlığı Muhasebat Genel Müdürlüğü ile, kurumun diğer kurumlar ile kuracağı veri alışverişi bağlantılarına destek olunacağı kaydedildi.

Diğer kurumlara yapılan temaslar sonucunda da, PTT ile posta takibi, posta kodu sorgulama hizmetleri kapıdan sunulacak. Pilot hizmet kapsamında ele alınan bazı servislerin ise e-kapı bütünleştirilmesine uyumsuz olduğu bir kısmının ise yasal değişiklik ihtiyacı olduğu saptandı.

4.2.3. Ulaştırma Bakanlığı

Elektronik imzanın uygulaması yazılımlara entegrasyonda çok fazla sorunla karşılaşılmadı, ancak personelin e-imzayı anlama ve kullanmalarında zaman zaman sorunlar oluşmuştur. E-imzanın sanal olmasından dolayı çekinceler oluşmuş ama zamanla aşılmıştır.

4.2.4. Adalet Bakanlığı

UYAP'ta tam anlamıyla e-imza kullanımına geçilememesi, kanun ve Yönetmelik gereği el ile imzanın kullanılması zorunluluğu e-imza için sorun yaratmaktadır.

4.2.5. Bankacılık ve Denetleme Kurumu (BDDK)

Elektronik imzanın gelişimi süresince, imzalanacak dokümanın formatı (ilk önceleri sadece text dokümanı imzalanabilirken şu anda tiff imzalanabilmektedir), imzalanacak dokümanın imzalanmadan önce imzalayacak kişiye gösterilmesi, sertifika iptal listelerinin (sil) tek bir çatı altında toplanamayarak her sertifika sağlayıcının kendi sil listesini yayınlaması ve piyasada bulunan elektronik imza ile bütünleşik yazılımların bu farklı listeleri okurken sıkıntı yaşamaları gibi sorunlarla karşılaşılmış, ancak zamanla bu sorunlar kamu kurumları, elektronik servis hizmet sağlayıcıları ve özel sektörün

ortak çalışmalarıyla giderilmiştir.

Kurumumuzda elektronik imzalı BYS kullanımı için tüm altyapı hazır olmakla birlikte gerçek zamanlı kullanıma henüz geçilmemiştir.

4.2.6. Fatih Belediyesi

Açık anahtar sayısal imza teknolojilerinin yaygınlaşmasının önündeki 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.

Diğer problem ise; kurumlar arası uyumsuzluk. E-imzalı bir evrak göndermek için karşı kurumun da e-imzayı kullanması gerekmektedir. Aksi takdirde evrak gönderilememektedir.

4.2.7. Devlet Malzeme Ofisi (DMO)

Doküman yönetim sistemi eğitimleri devam etmektedir. Bu nedenle elektronik imza kullanımına henüz başlamamıştır. Kullanıcıların yeni sisteme adapte olması zaman almaktadır.

4.3. ÇÖZÜM ÖNERİLERİ

Geleneksel kağıt üzerinde el yazısıyla imza ile işleyen bir sistemi elektronik ortama uyarlamak, oldukça ciddi yatırımları gerektirmektedir. E-imza teknolojilerinde istenmeyen sonuçlarla karşılaşmamak, ancak iyi belirlenen ve dikkatli uygulanan politikalarla mümkündür.

Kurumsal ağlarda e-imza uygulamaları ilk seferde mutlaka kapsam ve amacı açısından sınırlı pilot uygulamalar biçiminde tasarlanmalıdır. Pilot uygulamalardan olumlu sonuçlar alındıkça kapsam genişletilmelidir. Pilot hizmet kapsamında ele alınan bazı servislerin diğer devlet kurumlarıyla bütünleştirilmesinde uyumsuz olması durumunda yasal değişikliğe gidilmelidir.

Geleneksel yönteme alışan ve bilgi eksikliğinden doğan tereddütler ve başarısız örnekler, kullanıcıları olumsuz yönde etkilemektedir. Bu nedenle kurumsal ağlarda en iyi örneği oluşturmak için, öncelikle kendi içinde kalan iş akışlarında, sonra diğer kurumsal ağlarla ilişkilerinde ve son olarak vatandaşlarla ilişkilerinde e-imzaya geçiş planlanmalı ve uygulanmalıdır.

Elektronik imzanın kamu kurumlarında yaygınlaşması için gerekli çalışmalar yapılmalıdır. Diğer kurumsal ağlar ve vatandaşlarla olan ilişkilerde e-imzaya geçişin sağlıklı olarak gerçeklenebilmesi için de, iletişim içinde olunan kurumlarla gerekli koordinasyon yapılmalı ve uygulamalar arasında uyum sağlanmalıdır.

E-imza kendi kendisinin amacı değil, belirlenmiş bir ihtiyacı karşılamak üzere geliştirilen bir elektronik uygulama aracıdır. Bu nedenle kurumsal ağlarda e-imza yeteneğinin sağlanması, mevcut uygulamalara e-imza desteğinin eklenmesi veya mevcut uygulamaların e-imza desteği bulunan uygulamalarla değiştirilmesi olarak algılanmalıdır.

Kurumsal ağlarda e-imza yeteneğinin kazandırılması için öncelikle kurum çalışanlarının bilgisayar yetkinliği artırılmalıdır.

Kurumsal alanlarda E-imzanın yaygınlaştırılmasını sağlamak için öncelikle kurum çalışanlarına e-imzanın ne olduğu ve uygulamalarında elektronik imzayı kullanmaları durumunda hayatlarına ne gibi kolaylıkları getireceği anlatılmalıdır. Bunu gerçekleştirmek için kurum içi etkinliklerin düzenlenmesi veya kurum dışı etkinliklere katılım sağlanması ile kurum çalışanlarının e-imza konusundaki bilgileri artırılmalıdır. Özellikle sertifika sahipleri sistemin işleyişi hakkında sağlıklı bilgilendirilmelidir.

Kurum içinde e-imza uygulamaları ilerledikçe kullanıcıların e-imza ile ilgili sorunlarını çözmek için bir çağrı merkezi oluşturulmalıdır. Bu sayede yeni getirilmiş bir sisteme adapte olmaları alışılmış iş düzenleri dışında hayatlarına giren yeni bir teknolojiye karşı gösterecekleri önyargı aşılmalıdır.

E-imza uygulaması için satın alınacak uygulamalar karmaşık ve anlaşılması zor olarak tasarlanmamalı, konunun kullanılması kolaylaştırılmalı ve bu konuda kullanıcılara yardımcı olunmalıdır. Uygulamada ve standartlarda kullanıcı işlemleri uzatılmamalıdır.

E-imza uygulamalarında maliyetler ve sorunlar olabildiğince minimum seviyelere çekilmelidir. Konunun uygulanabilmesi için kurum için özel politikalar belirlenmeli, bu konuda kurumlar arası ilişkiler netleştirilmelidir. Oluşturulan

standartların uygulanması için sınırlayıcı olmadan zorlayıcı tedbirler alınmalı ve gerek duyuldukça denetleme mekanizmaları oluşturulmalıdır.

E-imza uygulamalarını devreye alabilmek için, öncelikle yöneticiler bazında bir bilgilendirmenin düzenli bir şekilde yapılması gereklidir.

Kamu kurumlarında en fazla görülen problemlerden biri de idari olarak kamu kurumu yöneticilerinde ve çalışanlarında yıllar boyu oluşmuş iş süreçlerinin yeni bir sistem olan elektronik imza sistemine adaptasyon sürecidir. Ancak bu engel olarak görülmemelidir. Bu yaklaşımların mümkün olduğunca hızlı bir şekilde değiştirilmesi sağlanmalıdır. E-imza teknolojisinin devlete ve çalışma verimine getireceği yararlar kurum çalışanlarının anlayabileceği örneklerle anlatılmalıdır. Bu şekilde değişime direncin kırılması sağlanmalıdır.

Kurum, yapacağı yatırımlarda mevzuatın getirdiği e-imza ihtiyaçlarını da göz önünde bulundurmalı ve ihale şartnamelerini buna uygun hazırlamalıdır.

Özellikle uygulamalar arası entegrasyonun sağlanması amacıyla, henüz geliştirme aşamasında olan XML tabanlı standartlar olgunlaşana kadar (XML sayısal imza, XML sertifikaları, vs.), bir işlemin tüm adımlarında tek seferde bir uygulamaya gitmekten kaçınılmalıdır. Bunun yerine, örneğin önce vergi beyannamelerinin gönderilmesi, ardından ödeme işlemlerinin e-imzaya dayalı yapılması düşünülmelidir.

E-imza uygulamalarıyla birlikte en önemli tasarrufun kırtasiye (kağıt tüketiminde) kaleminde olduğu ortaya çıkmıştır. Bu itibarla kurum bütçesinde kırtasiye (kağıt alımı) için ayrılan paranın belli bir yüzdesi e-imza uygulamalarının yaygınlaştırılması için kullanılabilir [28].

V. ELEKTRONİK SERTİFİKA HİZMET SAĞLAYICILAR

Elektronik Sertifika Hizmet Sağlayıcısı (ESHS), elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişileridir (md. 8). Tanımda da anlaşılacağı üzere sertifika otoritesi olma konusunda herhangi bir sınırlama getirilmemiştir.

Elektronik ortamda, elektronik sertifikada yer alan kimlik bilgilerinin doğruluğunu, bu bilgilerin güncel şekilde kalmasını, sertifikaların yaşam döngülerinin sürdürülmesini sağlayan tek kurum ESHS'dır. Bu nedenle, ESHS, elektronik imza altyapısında çok önemli bir unsurdur. Sertifika hizmet sağlayıcıları açık anahtar altyapısının temel yapıtaşı olup; elektronik ödemeleri yapan ya da gönderen veya diğer temasları gerçekleştiren tarafların kimliklerini onaylayan noter benzeri kuruluşlardır.

Elektronik imza sahibi olmak isteyen kişiler, elektronik sertifika hizmeti sağlayan kuruma kimlik bilgileriyle başvuruda bulunur. Bu başvuruya göre, kanunda belirtilen unsurların yer aldığı elektronik sertifika düzenlenerek kurumun özel anahtarı ile imzalanır. Oluşturulan elektronik sertifika, kişinin bizzat kendisine teslim edilir.

Elektronik sertifika sağlayıcıları Telekomünikasyon Kurumu tarafından yetkilendirilmektedir. Kamu kurum ve kuruluşlarının elektronik sertifika ihtiyacı, 2004/21 sayılı Başbakanlık Genelgesi gereği Kamu Sertifikasyon Merkezi tarafından karşılanacaktır[29].

1. ESHS'NIN YÜKÜMLÜLÜKLERİ VE HUKUKİ SORUMLULUĞU

ESHS'nın yükümlülükleri Elektronik İmza Kanununda maddeler halinde sayılmıştır. Elektronik sertifika hizmet sağlayıcısı, imza oluşturma verisinin korunmasından ve bununla bağlantılı olarak, kötüye kullanılmasından, kaybından, şifrenin başkalarına açıklanmasından, değiştirilmesinden ve yetkisiz kullanımından asla sorumlu değildir.

Elektronik sertifika hizmet sağlayıcısının, elektronik sertifika sahibine karşı sorumluluğu genel hükümlere tâbidir. Elektronik sertifika hizmet sağlayıcısı, bu Kanun veya bu Kanuna dayanılarak çıkarılan yönetmelik hükümlerinin ihlâli suretiyle üçüncü

kişilere verdiği zararları tazminle yükümlüdür. Elektronik sertifika hizmet sağlayıcısı kusursuzluğunu ispat ettiği takdirde tazminat ödeme yükümlülüğü doğmaz.

Elektronik sertifika hizmet sağlayıcısı, söz konusu yükümlülük ihlâlinin istihdam ettiği kişilerin davranışına dayanması hâlinde de zarardan sorumlu olup, elektronik sertifika hizmet sağlayıcısı, bu sorumluluğundan, Borçlar Kanununun 55 inci maddesinde öngörülen türden bir kurtuluş kanıtı getirerek kurtulamaz. Elektronik sertifika hizmet sağlayıcısı, bu Kanundan doğan yükümlülüklerini yerine getirmemesi sonucu doğan zararların karşılanması amacıyla sertifika malî sorumluluk sigortası yaptırmak zorundadır (EİK. md. 13)[29].

2. ESHS'NIN DENETİMİ

Avrupa Birliğinin 3/3 maddesine göre, "*her üye devlet, ülkelerinde kurulmuş kamuya nitelikli sertifika veren sertifikasyon hizmeti sunucularını denetlemek amacıyla uygun bir sistem kurulmasını temin edecektir.*" hükmü Elektronik İmza Kanununun 15'inci maddesinde karşılanmıştır.

Denetim işlemini Telekomünikasyon Kurumu yerine getirir. Denetimini gerek gördüğü zamanlarda yapabileceği gibi şikâyet üzerine de yapabilir. Ancak yönetmeliğe göre denetimin en az iki yılda bir yapılması gerekmektedir (Yön. md. 22).

Denetim görevlileri denetimleri sırasında gerekli gördükleri her türlü defteri, belgeyi ve kayıtları istemeye, incelemeye ve bunların asıl ve örneklerini alma yetkisine sahiptir. Bunun yanı sıra denetim görevlileri, ESHS'na ait binaları ve eklentilerine girebilir, inceleme yapabilir, yazılı veya sözlü bilgi isteyebilir, her türlü işlem ve hesapları denetleyebilirler. ESHS, gizlilik ve sır saklama gibi gerekçeler ileri sürerek denetim yükümlülüklerinden imtina edemezler. ESHS denetim elemanlarınca talep edilen bilgi ve belgeleri vermezse yirmi bin YTL idarî para cezasına çarptırılacaktır (EİK. md. 18/e).

Bütün bu işlemlerin yapılması sırasında denetim görevlileri gerekli özeni göstermek durumundadırlar. Aynı zamanda tarafsız davranmaları, dürüstlük ve tarafsızlığı etkileyebilecek herhangi bir müdahaleye imkân vermemekle yükümlüdürler (Yön. md. 23).

Denetim sonunda hazırlanan denetim raporu en geç otuz gün içinde Telekomünikasyon Kurulu'na sunulur. Denetim sırasında, ESHS'nın faaliyetini

olumsuz yönde etkileyebilecek derecede önem arz eden hususların tespit edilmesi halinde denetim faaliyetinin sonuçlanmasını beklemeksizin söz konusu hususları Telekomünikasyon Kuruluna sunar. Sertifika sağlayıcısının faaliyetine tesir edecek derecede olumsuz durumlar, bu sağlayıcıdan alınmış bütün sertifika sahiplerini, dolayısıyla kamuyu ilgilendirmektedir. Bu nedenle hazırlanan rapor Kurul tarafından öncelikli olarak gündeme alınır; Kurul, raporları değerlendirerek ihlal edilen herhangi bir durum varsa mevzuatın öngördüğü yaptırım ve cezaların uygulanmasına kararını verir(Yön.md.28).[29]

Tablo 3: Türkiye'de Elektronik Sertifika Hizmet Sağlayıcısı olan Kurumlar

Elektronik Sertifika Hizmet Sağlayıcısı (ESHS)	**Bildirim Tarihi**	**Faaliyete Başlama Tarihi**	**Durum**
Elektronik Bilgi Güvenliği A.Ş. (E-Güven)	25.03.2005	24.06.2005	Faaliyetine devam etmektedir
TUBİTAK-UEKAE (Kamu Sertifikasyon Merkezi)	31.03.2005	30.06.2005	Faaliyetine devam etmektedir
TürkTrust Bilgi, İletişim ve Bilişim Güvenliği Hizmetleri A.Ş.	13.05.2005	16.07.2005	Faaliyetine devam etmektedir
EBG Bilişim Teknolojileri ve Hizmetleri A.Ş(E-Tugra)	20.06.2006	01.09.2006	Faaliyetine devam etmektedir

Kaynak: Telekomünikasyon Kurumu

VI. GELECEĞE İLİŞKİN ÖNGÖRÜLER

Elektronik imzanın yakın bir zamanda günlük yaşamımıza gireceği ve yaşamın ayrılmaz bir parçası olacağı konusunda yalnız uzmanlar değil; birçok kişi görüş birliği içindedir. Çünkü, güvenli bir imza yöntemi olmadan güvenli bir elektronik haberleşmeden söz etmek mümkün değildir. Bu gereksinim, yalnızca şirketler, kurum veya kuruluşlar için değil, aksine elektronik ortamda hukuken bağlayıcı işlemler yapmak isteyen kişiler bakımından da söz konusudur.

- **Sanal Bankacılık İşlemlerinde Yaşanabilecek Sorunlar:**

Elektronik ortamda farklı bir yasal geçerlilik mekanizması şu anda Türkiye'de bulunmamaktadır. Hem bankacılık hem de diğer resmi işlemlerde e-imzanın olması gerekmektedir. Dolayısıyla, elektronik imza, internet üzerinden kullanıcı adı ve şifreyle yapılan işlemlere göre çok daha hukuksal bir alt yapı getiriyor. Özellikle kurumsal bankacılık uygulamalarında başlayan elektronik imza uygulamalarının çok yakında bireysel bankacılık uygulamalarında da geliştiriliyor olması finans kurumlarının başına çok büyük sorun olan güvenlik kaçağının da çözümü olacaktır.

Önümüzdeki yıllarda vatandaş açısından bakıldığında Internet bankacılığı artık tamamen elektronik imza ile yapılacaktır. Kurumsal uygulamalarda da piyasadaki yazılımlar da elektronik imza ile bütünleşmiş hale gelmiş olacaktır. Artık elektronik imza konusunda çoklu kullanım aşamasına gelinmiştir. Bu durumun sonucu olarak elektronik imza sertifikasını alan kişi sertifikayı, ihracatçı ise hem ihracatta hem bankada hem kendi kurumu içinde kullanacaktır.

- **Kamu Kurumları e-İmza Projeleri:**

Kamu alanında elektronik imza alanındaki projeler; Gelirler Genel Müdürlüğü'nün e-beyanname projesi, SSK'nın e-bildirge projesi, Adalet Bakanlığı'nın UYAP Projesi, Türk Telekom'un ihale edeceği e-Devlet Kapısı Projesi'dir. Bu projelerden en azından birinin sağlıklı bir şekilde e-imza kullanılmaya hazır hale getirilmesi çok önemlidir. Özel sektör tarafında, özellikle bankalar ciddi hazırlıklar yapmaktadır.

- **Politika ve Strateji Oluşturma Etkinliği:**

E-imza projesi ile güvenilir ve ayrıntılı bilgiye anında ulaşılabileceğinden, karar verme süreçleri hızlanırken, politika belirleme ve strateji oluşturma etkinliğinin de artacağını söyleyebiliriz. Projeyle İhracat Genel Müdürlüğü'nce verilen dahilde işleme izin belgelerinin, düzenlenme aşamasından taahhüt hesaplarının kapatılmasına kadar geçen süreç hazırlanan web tabanlı programla internet üzerinden yapılması da sağlanacaktır.

İhracatçılar zaman ve mekan kısıtlaması olmaksızın ihracata yönelik izin belgelerine ilişkin tüm işlemleri bilgisayar üzerinden anında yapabilecekler. Dış Ticaret Müsteşarlığı da söz konusu talepleri aynı ortamda değerlendirerek çok hızlı bir şekilde sonuçlandıracaktır.

- **Teminat İadelerinde Yaşanacak Sorunlar:**

Diğer kurumlarla oluşturulan elektronik bilgi paylaşımı sayesinde kapatma işlemlerinin daha kısa sürede tamamlanacak ve ihracatçıların teminat iadelerinde yaşanan sorunlar sona erecektir [30].

Dış Ticaret Müsteşarlığı'nın bazı işlemlerin e-imza ile yapılmasını zorunlu kılmasıyla e-imza satışında büyük artış beklenmektedir. Diğer ihracatçı işlemlerinde de zorunluluğun başlamasıyla söz konusu tutarın çok daha büyüyeceği belirtilmektedir. Özellikle bankalar ile GSM operatörleri milyonlarca kredi kartı ekstresi ile cep telefonu faturasının fiziki olarak hem basımından hem de dağıtımından kurtulacaktır.Bu gelişmeler PTT ile özel kurye ve kargo şirketlerinin iş hacmini ciddi şekilde düşürecektir.

- **İş hayatına yansımaları:**

Orta ve uzun vadede e-devlet uygulamaları ve özel şirketlerin buna uygun yeni iş modellerini hayata geçirmesi, e-imzanın hayatın hemen hemen bütün alanlarında kullanılmasını beraberinde getirecektir. Bunun iş hayatına çok önemli yansımaları olacağı düşünülmektedir. E-imzanın yaygınlaşması, teknoloji ve internetin daha yoğun kullanımını beraberinde getirecektir. Bu da çipli çubuk (token) ve çipli kartlarda olduğu gibi, bilgisayar donanım ürünlerinde de talebi ciddi şekilde artıracaktır. Halen

kullanımdaki milyonlarca banka kartının, EAL+4 standardı olarak adlandırılan e-imza üretim cihazı özelliğini de barındıran yeni kartlarla değiştirilmesi gündeme gelecektir.

- **Cep telefonları ile e-mobil imza kullanımı:**

Çipli kart üreticileri buna yönelik iş planlarını geliştirmiş durumdadır. Çipli kartlar konusuna benzer bir durum da, sayıları 40 milyonu bulan GSM abonelerinin cep telefonlarındaki SIM kartlar için söz konusudur. Yani cep telefonları e-imza üretebilir cihazlar olacak.

- **Yazılım pazarına etkileri:**

E-imza uygulamaları için sadece sertifika, cihaz ve kart alımı yeterli olmamaktadır. Mevcut ve kurulacak yeni altyapıların bu uygulamalara zemin oluşturabilmesi için, gelişmelere uygun yazılım ürünlerini içermeleri gerekecektir. Hali hazırdaki birçok yazılımın güncellenmesi ya da yenileriyle değiştirilmesi zorunlu hale gelecektir. Bu da Türkiye'de ciddi bir gelişme potansiyeli taşıyan yazılım sektörü için yeni iş imkânlarının artmasını beraberinde getirecektir.

E-imza teknolojisinin gelmesi birçok bireysel ve kurumsal anlamdaki mevcut süreçlerin ciddi anlamda değişmesine neden olacaktır. E-imza yazılımını da ürünlerinin içine koymaları şart olacaktır. Mevcut bütün kurumsal yazılımların ciddi güncelleme ihtiyaçları doğacaktır. Bunlar da oldukça kapsamlı boyuttadır. Çünkü e-imza, insan kaynaklarından tedarik ve satış süreçlerine kadar birçok süreci değiştirecektir.

- **Noterlere yeni iş yükü:**

E-imza sahibi olmak, fiilen kimlik doğrulaması gerektirdiğinden noterlere yeni bir iş imkânı doğacaktır. Maliye Bakanlığı'nın e-devlet uygulamaları çerçevesinde vergi kimlik numarası verme işini e-imza karşılığında internet ortamına taşıması da gündemdedir. Ancak bu nedenle vergi dairelerine gitmesi gerekmese de insanların bu defa da e-imza için noterlere ve diğer kimlik doğrulama yetkisi bulunan kurum ya da kuruluşlara uğraması gerekecektir. Buradaki en önemli rollerden birisini de noterler oynayacaktır. Dolayısıyla noterlerin iş yükünün artması söz konusu olacak.

- **Rekabete Etkisi:**

Önümüzdeki dönemlerde e-imzanın yaygınlaşmasını hızlandıracak bazı uygulamalar gündeme gelecektir. E-imza kendi içinde taşıdığı müthiş kaynak tasarrufu imkânlarıyla şirketleri bu uygulamaya geçmeye zorlayacaktır.

Bankalar her ay milyonlarca kredi kartı ekstresi bastırıp bunu kart sahiplerine fiziken ulaştırmak zorundadır. Oysa e-imza uygulaması hukuki geçerliliği olan elektronik dekontlarla bu işi çözmektedir. Banka hem kağıt ve baskı masraflarından hem de dağıtım maliyetinden kurtulacaktır. Hatta e-imza, internet bankacılığı uygulamalarının başlangıcında olduğu gibi ciddi bir rekabet aracı olarak kullanabilecek. Örneğin, "e-ekstre kullanana düşük faiz" veya "e-imzalı bankacılık işlemleri bedava" benzeri tanıtım kampanyalarına rastlamak mümkün olacaktır.

- **Vatandaşın İlgisi:**

Nitelikli Elektronik İmza'nın yasalaşmasının ve ikincil düzenlemelerin çıkmasının ardından ESHS'les (Elektronik Sertifika Hizmet Sağlayıcı) vatandaşa Nitelikli Elektronik Sertifikası (NES) vermeye başlamışlardır. NES'e sahip olan vatandaş sayısı bugün ivmeli bir şekilde artmaktadır. Bugün kamu sektörü tarafında Dış Ticaret Müsteşarlığı'nın Dahilde İşleme Rejimi projesinin lokomotifliğini üstlendiği e-imza uygulamaları özel sektör tarafından bankaların yeni uygulamalar geliştirmesiyle vatandaşa yeni hizmetler olarak dönmeye başlamıştır.[31].

- **İnternetten e-imza ile açılabilecek davalar:**

Uygulamaya göre elektronik imza sahibi olan herkes, internet üzerinden dava açabilecek, harç ödeyebilecek, duruşma tarihini ve dava seyrini oturduğu yerden öğrenebilecek. Proje kapsamındaki Avukat Bilgi Sistemi ile de avukatlara, UYAP üzerinden mevcut dosyalarını izleme, davalara evrak gönderebilme ve yeni dava açma olanağı tanınacaktır.

Bunların yanı sıra, davalara ilişkin harç, dosya ücreti ve diğer masraflar için gerekli para transferleri de internet aracılığıyla yapılabilecek. Avukatlar, vekaletnameleri bulunmayan dosyaları ilgili hâkimin bilgisi dâhilinde inceleme

kolaylığına sahip olurken mahkemeler ve kurumlar arası bürokratik işlemler saniyeler içinde gerçekleştirilebilecektir [32].

VII. SONUÇ VE TARTIŞMA

Yapılan bu çalışmada, ıslak imza ve elektronik imzanın özellikleri ele alınmış, elektronik sertifika, sertifika sağlayıcı ve açık anahtar altyapısı irdelenip, kamu kurumlarında elektronik imza konusunda yapılan çalışmalar ve uygulamalar yerinde incelenerek, bazı devlet kurumlarından online olarak bilgi edinilmiştir.

Ayrıca, kamu kurumlarında elektronik imza uygulamalarında karşılaşılan sorunlar incelenerek bu sorunların ortadan kaldırılabilmesi için nelerin yapılması gerektiğine dikkat çekilmiştir.

Elektronik ortamda yapılan iş ve işlemlere hukuksal geçerlilik kazandıran elektronik imza teknolojisi aynı zamanda da işlemlerin hızlı bir şekilde gerçekleştirilmesini sağlamaktadır.

E-imza konusu oldukça yeni bir konudur ancak, dikkatli davranılmaması durumunda riskler taşıyabilir. Konu doğrudan güvenlikle ilgili olduğu için önemi oldukça yüksektir. Bu nedenle alınacak yazılım, donanım ve hizmetler konusunda çok dikkatli olunması, bilinçli yaklaşılması, yabancı ülke katkısının incelenmesi, güvenilirlilik, süreklilik ve kurumsallık sorgulamalarının iyi yapılması ve hizmet kalitesinin doğru değerlendirilmesi marjinal faydayı doğuracaktır.

E-imza ve AAA sisteminin ülke genelinde planlı bir şekilde kurulumuyla kamu işlemleri (vergiler, adli işlemler, SSK, Bağkur, Emekli Sandığı, nüfus işlemleri vb.), kurumsal işlemler (kimlik kartı, personel kartı, bina giriş sistemleri vb.), toplu taşıma işlemleri (otobüs, tren, vapur, metro vb.), rezervasyon ve bilet işlemleri (kültür-sanat, eğlence, spor, turizm vb.), finansal işlemler (banka kartı, kredi kartı, e-ticaret vb.) ve e-imza işlemleri gibi birçok işlem tek bir akıllı kart kullanılarak yapılabilecektir.

Gelişmiş ülkelerde ve ülkemizde e-imza ile ilgili yasallaşma süreci tamamlanmış olmasına rağmen, henüz e-imzaların yaygın bir şekilde kullanıldığını söylemek güçtür.

Elektronik imzanın yaygınlaştırılmasında devlet öncü rol oynamalıdır. Kurumsal ağlarda e-imza uygulamaları ilk seferde mutlaka kapsam ve amacı açısından sınırlı pilot uygulamalar biçiminde tasarlanmalıdır. Pilot uygulamalardan olumlu sonuçlar alındıkça kapsam genişletilmelidir. Adalet Bakanlığı tarafından yürütülen UYAP pilot olarak seçilmelidir.

Bilgi eksikliğinden kaynaklanan tereddütler ve başarısız örnekler, kullanıcıları olumsuz yönde etkilemektedir. Bu nedenle kurumsal ağlarda en iyi örneği oluşturmak

için, öncelikle kendi içinde kalan iş akışlarında, sonra diğer kurumsal ağlarla ve nihayetinde vatandaşlarla olan ilişkilerinde e-imzaya geçiş planlanmalı ve uygulamaya konmalıdır.

Diğer kurumsal ağlar ve vatandaşlarla olan ilişkilerde e-imzaya geçişin sağlıklı olarak gerçekleşebilmesi için, iletişim içinde olunan kurumlarla gerekli işbirliği yapılmalı ve uygulamalar arasında uyum sağlanmalıdır.

Sonuç olarak, kâğıt üzerinde işleyen bir sistemi elektronik ortama geçirmek ve buradaki uygulamaya e-imza ile ilgili özellikleri dâhil etmek önemli bir dönüşümdür ve büyük yatırım gerektirmektedir. Yapılan çalışmalar, kâğıt ortamında yapılan belge yönetimine oranla elektronik ortamda yapılacak belge yönetiminin çok daha etkin ve verimli olduğu, e-imza uygulamalarına yapılacak yatırımların kısa sürede geri kazandırabileceğini ortaya koymaktadır. Bu çerçevede, kurumsal ağlarda düşük maliyetli işlemler, standartlaşma, iş süreçlerinin iyileştirilmesi, iş gücünün uygun kullanımı, kırtasiye tüketiminde azalma, sahteciliğin azalması, haberleşme giderlerinde azalma göz önüne alındığında e-imza uygulamalarının hayata geçirilmesinin önemi büyük ölçüde artacağı aşikardır. Ancak bu fırsatları elde edebilmek ve e-imza teknolojilerinde istenmeyen sonuçlarla karşılaşmamak, iyi belirlenen ve dikkatli uygulanan kurumsal politikalarla mümkündür.

Türkiye'de elektronik imza konusunda yapılan yasal düzenlemeler yeterlidir ancak, uygulamaya geçiş konusunda yeterli bir fizibilitenin olmayışı büyük bir eksikliktir. Elektronik imzanın kullanılması, kamudaki dönüşümün, yeniden yapılanmanın, verimliliği sağlamanın, e-devlet olmanın ve çağdaşlığı yakalamanın bir fırsatı olarak görülüp iyi değerlendirilmelidir.

VIII. KAYNAKÇA

[1] Berber, K.,L, Dijital İmza, Seçkin, 2002, s.76.

[2] Arıkan, Saadet., "Dünyada ve Türkiye'de Elektronik Ticaret Çalışmalarına Hukuki Bir Yaklaşım", Ankara, 1999, s.151.

[3] http://etrust.com (02.02.2009)

[4] Erturgut,M., Medeni Usul Hukukunda Elektronik İmzalı Belgelerin Delil Olarak Değerlendirilmesi, Yetkin, Ankara, 2004,ss.104-106, 121-123

[5] Berber, K., L, İnternet Üzerinden yapılan İşlemlerde Elektronik Para ve Dijital İmzalama, Yetkin, Ankara, 2002, ss. 108-111

[6] Stinson, D. R., "Cryptography Theory and Practice", 2nd ed., Chapman & Hall/CRC, Florida, 173 – 180, 274 – 292 (2002).

[7] Çakar, M., A., Yiğit, T., Çoklu Algoritma Desteğine Dayalı E-İmza Uygulaması (E-Signat), Gazi Üniversitesi, Endüstriyel Sanatlar Eğitim Fakültesi, Bilgisayar Eğitimi Bölümü, 06500, ANKARA,ss.1-5

[8] Uygulamalı Matematik Enstitüsü, Kriptografi Bölümü, ODTÜ, ss.73-78

[9] Sarısakal, M.,N., Marangız, G., Uçan, O.N., Elektronik Ticaret'te Sayısal İmzanın Kullanımı, Istanbul Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü

[10] E-İMZADA SHA-1 ÖZETLEME ALGORİTMASININ KULLANIMI Çağdaş Çalık, Meltem Sönmez Turan, Zaliha Yüce,ss. 1-3

[11] Bulut, M., Dijital İmza Rehberi, İstanbul Ticaret Odası, İstanbul, 2005, ss.10-13

[12] Konurlap, H., "Genel Hatlarıyla Elektronik İmza Kanunu" http://www.tbb.org.tr/turkce/konferans.htm (15.01.2009)

[13] Hukuk Çalımla Grubu, www.tk.gov.tr (15.01.2009)

[14] Konuralp, H., "Genel Hatlarıyla Elektronik İmza Kanunu" http://www.tbb.org.te/turkce/konferans.htm. (15.01.2009)

[15] Bilgi Teknolojileri ve İletişim Kurumu (BTK)

[16] Erturgut, M., "Elektronik İmza Kanunu Bakımından e-Belge ve e-İmza" http://www.tbb.org.tr/turkce/konferans.htm (13.01.2009)

[17] Orta, M., Elektronik İmza ve Uygulaması, Seçkin, Ankara, 2005, 135-139

[18] Adalet Bakanlığı, Bilgi İşlem Daire Başkanlığı

[19] Ulaştırma Bakanlığı, Bilgi İşlem Daire Başkanlığı

[20] Telekom Dünyası, Aralık 2004, s.56

[21] Telekomünikasyon Kurumu Bilgi İşlem Daire Başkanlığı

[22] Türkiye Cumhuriyeti Merkez Bankası Bilgi İşlem Daire Başkanlığı

[23] Bankacılık ve Denetleme Kurumu Bilgi İşlem Daire Başkanlığı

[24] DMO Bilgi İşlem Daire Başkanlığı

[25] Zeytinburnu Belediyesi Bilgi İşlem Daire Başkanlığı

[26] İSKİ Bilgi İşlem Daire Başkanlığı

[27] Eminönü Belediyesi Bilgi İşlem Daire Başkanlığı

[28] Türkiye'de Elektronik İmza Uygulamalarında Durum Analizi Ve Öneriler Hüseyin Erol, M.Ali Akcayol, Gazi Üniversitesi, Mühendislik ve Mimarlık Fakültesi Bilgisayar, Mühendisliği Bölümü, Maltepe, Ankara

[29] Orta, M., Elektronik İmza ve Uygulaması, Seçkin, Ankara, 2005, ss.126-127

[30]http://www.e-imza.gen.tr/index.php?Page=Haberler&HaberNo=89 (09.01.2009)

[31] http://www.e-imza.gen.tr/index.php?Page=Haberler&HaberNo=123 (09.01.2009)

[32] http://www.e-imza.gen.tr/index.php?Page=Haberler&HaberNo=188 (16.01.2009)

ÖZGEÇMİŞ

Kevser ŞAHİNBAŞ, 23 Nisan 1982 yılında Çorum'da doğdu. Lise öğrenimini İstanbul İncirtepe Lisesi'nde tamamladıktan sonra 1999 yılında Beykent Üniversitesi Yönetim Bilişim Sistemleri bölümünü kazandı ve Matematik Bilgisayar bölümünden çift anadal yaptı. Bu bölümlerden 2004 yılında mezun oldu. 2006 yılında Beykent Üniversitesi Fen Bilimleri Enstitüsü'nde Bilgisayar Mühendisliği Anabilim Dalı'nda yüksek lisans çalışmalarına başladı. 2009 yılında yüksek lisansı başarıyla tamamladı. Temel ilgi alanları bilgisayar ağları ve yazılımdır. Kevser ŞAHİNBAŞ, 2006 yılından bu yana Öğretim Görevlisi olarak Beykent Üniversitesi'nde görevine devam etmektedir.