Mobil Elektronik İmza: Senaryolar, Uygulamalar, Standartlar ve Ülkeler

Demet KABASAKAL, Şeref SAĞIROĞLU, Mustafa ALKAN

***Özet*–Bu çalışmada mobil elektronik imza, imzalama işleminde kullanılan senaryolar, ülkelerin m ticaret uygulamaları, bazı ülkelerdeki mobil imza çalışmaları, mobil imza standartları ile kullanılan uygulamalar gözden geçirilmiştir. Bu çalışmanın ülkemizde mobil imzanın daha iyi anlaşılmasına, dünya ülkeleri ile karşılaştırılmasına ve me-imza konusunda ülke durumunun değerlendirilmesine katkılar sağlayacağı değerlendirilmektedir.**

***Anahtar Kelimeler*–Mobil elektronik imza, Uygulamalar, Senaryolar, Standartlar.**

MOBILE ELECTRONIC SIGNATURE: SCENARIOS, APPLICATIONS, STANDARDS and COUNTRIES

ABSTRACT–In this study, mobile electronic signature, scenarious used in mobile processes, applications for m-trade, mobie signature studies of the countries, mobile electronic signature standards, and its applications have been reviewed. It is concluded that this study might help and contribute opponents to understand, to compare and to evaluate mobile electronic signatures in many countries.

Keywords–Mobile Electronic Signature, Applications, Standards.

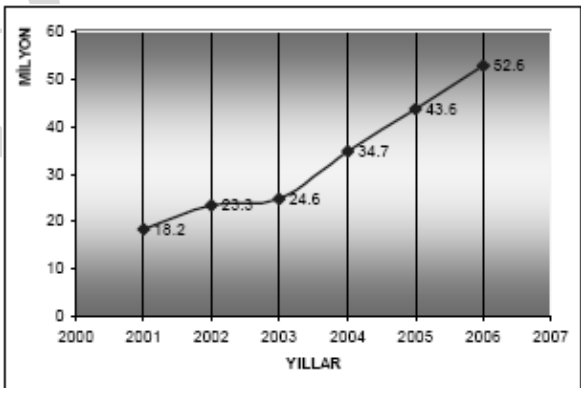
I. GİRİŞ

Bilgi ve iletişim teknolojilerindeki gelişmeler bilgiye her noktadan erişim isteği, zamandan ve yerden bağımsız olarak hizmet almaya duyulan ihtiyaçlar, mobil ve kablosuz sistemlere kaymaya başlamış böylece daha önceden alışık olmadığımız mobil iletişim, bugün hayatımızın vazgeçilmez bir parçası olmuştur [1].

Manuscript received September 25, 2007; revised November 23, 2007.
Demet KABASAKAL is with Telecommunications Authority, Ankara, 06570 Turkey. (e-mail: dkabasakal@tk.gov.tr).
Şeref SAĞIROĞLU is with the Computer Engineering Department and Faculty of Engineering and Architecture Gazi University, Ankara, 06570 Turkey. (e-mail: ss@gazi.edu.tr).
Mustafa ALKAN is with Telecommunications Authority, Ankara, 06570 Turkey. (e-mail: malkan@tk.gov.tr)

Ülkemizde de elektronik ortamların yaygınlaşmaya başlaması ve mobil cihaz sayısının ve haberleşmenin ülkemizde de artış göstermesi bu ortamlarda verilecek olan hizmetlerde de bir artış göstermektedir.

Mobil iletişim sektöründeki etkin rekabetin etkisiyle tüm dünyada olduğu gibi ülkemizde de hızlı bir gelişmenin meydana gelmiş 2001 yılı ortalarında GSM abone sayısı sabit şebeke abone sayısını geçmiştir. Şekil-1'de görüldüğü üzere ülkemizde 1996 yılında 692.779 olan GSM abone sayısının 10 yıl gibi bir sürede yaklaşık 63 kat artarak 2005 yılı sonu itibariyle yaklaşık 44 milyona, 2006 yılı sonu itibariyle 52,9 milyona ulaşmıştır [2]. Ülkemiz dünyada en çok mobil cihaz kullanan ülkeler arasında onuncu sırada yer almaktadır [2]. 2006 yılı sonu itibariyle ülkemizdeki 52,6 milyonluk GSM abone sayı ile penetrasyon oranı da %71,3'e yükselmiştir [3]. Ülkemizde %71'ler seviyesinde olan GSM penetrasyonunun, AB ülkelerinde ortalama %80 seviyelerinde olduğu rapor edilmişse de bu oranların Batı Avrupa'da 2007 yılı ortalarına kadar %100'ü bulacağı tahmin edilmektedir [4]. Bu oranların yüksekliği ve geniş pazar payı sebebiyle elektronik ortamlarda yapılan iş ve işlemlerin mobil ortamlara kayması, "e-"li kavramların yerini "m-"li kavramlara bırakması gayet doğaldır.



Şekil-1 Türkiye'de Yıllara Göre GSM Abone Sayısı

Dünyada ve ülkemizde hızla yayılmaya devam eden mobil cihazlar üzerinden internet hizmetinin de verilmeye başlanmasıyla, bu teknolojilerin sunduğu hizmetlerde farklılıklar oluşmuş, bilgiye mobil ortamlardan erişim sağlanmıştır. Mobil iletişim araçları üzerinde internet içeriği sağlayan WAP teknolojisinin GPRS gibi veri platformları ile desteklenmesiyle bu araçlar üzerinden mobil elektronik ticaret (m-ticaret), mobil bankacılık, mobil işlemler gibi birçok uygulamalar yapılmaya başlanmıştır.
Mobil ortamlarda iş ve işlemlerin yaygınlaşması da elektronik ortamlarda olduğu gibi mobil elektronik ortamlarda da güven sorununu ortaya çıkarmaktadır. Öncelikle m-ticaret gibi parasal servisler için tasarlanan sistemler, mobil cihazlardan yüksek güvenlikte işlemlerin yapılabilmesini sağlamalıdır. Güvenlik özellikleri kapsamında işlemlerin yetki kontrolü, şifrelenmesi, sayısal olarak imzalanması ve reddedilememesi gibi unsurlar bulunmaktadır. Mobil ortamlarda me-imzanın uygulanması için e-imzada olduğu gibi MAAA'nın kurulması ve işletilmesi gerekmektedir [5].

Aslında me-imzanın internet üzerinde kullanılan e-imzadan daha hızlı gelişip yaygınlaşacağı değerlendirilmektedir. Çünkü daha ucuz, hareket kabiliyeti çok yüksek ve kullanımı daha kolay olan me-imza, mobil pazarın büyümesi ve mobil cihazlar üzerinden sağlanan internet erişimiyle dünyada mobil elektronik ortamlarda, kimlik doğrulama gerektiren ve zamanın önemli olduğu tüm işlemlerde sadece mobil AAA kullanarak imzalama önem kazanmaktadır [6]. Mobil teknolojilerin sağlamış olduğu mekândan bağımsızlık ve kullanım kolaylığı ve bu ortamlarda belirgin bir şekilde hissedilen güvenlik gereksinimi sebebiyle me-imzanın kısa sürede ıslak imzanın yerini alacağı değerlendirilmektedir.

E-imza ve me-imza yaklaşımları, artık sadece e-ticaret yapanları, bankacıları, özel ve kamu hukukçularını değil herkesi ilgilendirmektedir. E-imza ile e-devlet yapısının yaygınlaşmasıyla, devletin vatandaşıyla, vatandaşın devletle, vatandaşın vatandaşla ve devletin devletle olan ilişkileri, elektronik ortama taşınarak, güvenli bir iletişim kanalı oluşturabilecektir. Ülkemizde, mobil elektronik ortamların yaygınlaşmasıyla sadece iş ve işlemleri hızlandırma, verimliliği ve güvenliği arttırmanın yanında me-imzanın aynı zamanda ekonomik, kültürel, sosyal ve yönetimsel yönden birçok gelişmeyi ve dönüşümü de beraberinde getireceği düşünüldüğünde konunun önemi ortaya çıkmaktadır.

II. MOBİL ELEKTRONİK İMZA

Genel olarak me-imza; "mobil bir cihaz kullanılarak oluşturulan ve haberleşme ortamından bağımsız bir konumda imza veya sertifikasyon servisinden destek alan e-imza" olarak tanımlanabilir. Aslında me-İmza bir cep telefonu veya cep bilgisayarı SIM kartı içerisinde bir gizli şifre (PIN) ile oluşturulan bilgi varlığıdır. SIM kart içerisinde tutulan bu gizli şifre, kriptografik bir algoritma tarafından üretilmektedir. e-İmza kullanıcılarının, elektronik belgeyi imzalayabilmeleri için gelişmiş bir SIM kartına veya yukarıdaki işlemleri gerçekleştirebilecek bir özel karta sahip olmaları gereklidir.

Birer akıllı kart olan SIM kartlar üzerinden sunulan eimza, teknolojisi ile kullanıcılara SIM kartları ile diledikleri yerde ve zamanda, ek bir kart veya kart okuyucuya ihtiyaç duymaksızın e-imza atabilme imkânı sunmaktadır.

Mobil telefonların pazardaki yüksek penetrasyonu, zaman ve yer bağımsız olarak sunulan imzalama imkânı, me-imzayı yaygınlaşması açısından potansiyel olarak başarılı kılmaktadır [7]. Mobil ortamda imzalama yaklaşımı sunucu ve istemci
tabanlı me-imza olmak üzere ikiye ayrılmaktadır
[8,9,10,12,13].

Sunucu Tabanlı Mobil Elektronik İmzalar
Bir ESHS tarafından özel kullanıcılar için merkezileştirilmiş güvenli bir sunucuda oluşturulan e-imzalardır. Bu me-imzalar, mobil araç tarafından aracın tuş takımı kullanılarak girilen PIN kodundan sonra oluşturulan uygun bir kod tarafından başlatılır. Kodun ESHS'deki sunucuda yapılacak olan imza oluşturma işlemini tetiklemesinden sonra sunucuda kullanıcı için imzalama işlemi gerçekleştirilir. Kullanıcıya ve üçüncü kişiye (güvenen tarafa) imza gönderilir.

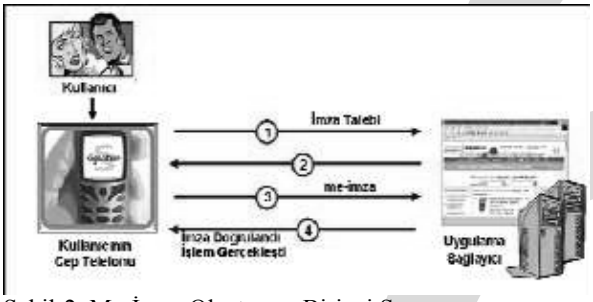
Bu imzalar veya imzayı içeren sertifikalar, ESHS'nin adına yayınlandığı için bu imzaların kullanıcıların yasal imzası olduğu sonucuna varılması zordur. Bu imzalar, ESHS'nin imzalarıdır ve sadece ESHS kimliğinin belirlenmesini sağlarlar. Ancak ESHS'nin imzası temel alınarak, kullanıcının kimliği doğrulanamaz ve imzalamaya gerçekten yetkisi olup olmadığı ispatlanamaz. Yani imzanın ne doğruluğu nede kullanıcı tarafından imzalanmış olduğu tespit edilemez [10,14].

İstemci Tabanlı Mobil Elektronik İmzalar
Bu imzalar**,** mobil araç içerisine ESHS tarafından onaylanmış SIM kart konulduktan sonra, SIM kart üzerindeki kripto
işlemcisi kullanılarak gerçekleştirilen imzalardır. Böylece imzalama süreci mobil cihazda gerçekleştirilmiş olur. Kullanıcılar SIM kart fonksiyonlarını ve güvenli imza oluşturma fonksiyonlarını ihtiva eden tek bir akıllı kart ile dokümanları kolaylıkla imzalayabilir ve cep telefonlarının GPRS ya da UMTS servisleri gibi iletişim hizmetleri yoluyla dağıtabilirler.

III. MOBİL ELEKTRONİK İMZA OLUŞTURMA SENARYOLARI

Bir me-imza oluşturma aracı olarak, mobil cihazın kendi içerisindeki imza yaratma uygulamaları ya da SIM kart kullanılabilir. Me-imzanın oluşturulma platformu olarak mobil cihaz seçildiğinde bu aracın kullanıcı kimliğini tanıma mekanizması, işlemler arasında hafıza dağılımı, yazılım ve veri bütünlüğünün ayarlanması, güvenilen kullanıcı ara yüzüne sahip olma gibi özelliklere haiz olması gereklidir. Ancak bugünkü mobil cihazların büyük bir çoğunluğu bu gerekliliklere uymazlar ve mobil pazarda paylaşılan mobil işlem sistemleri sadece minimum güvenlik sağlarlar [10]. Bu nedenle de me-imzaya ilişkin dünyadaki farklı çalışmalar incelendiğinde me-imza oluşturma aracı olarak SIM kartın kullanıldığı iki senaryo ön plana çıkmaktadır
[15].

Şekil-2'de verilen ilk senaryoda kullanıcı, me-imza uygulamasını mobil cihaz üzerinden ulaşmaktadır.



Şekil-2. Me-İmza Oluşturma Birinci Senaryo

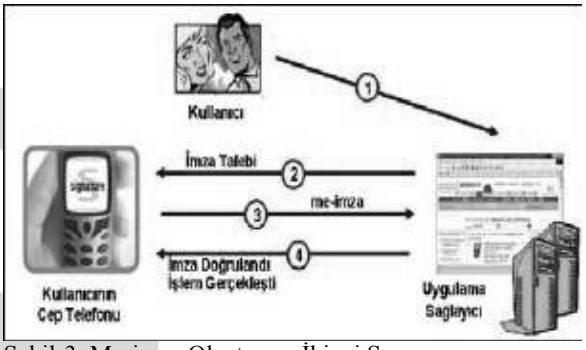
Şekil-2'de verilen senaryoda işlemler, kullanıcılar tarafından aşağıda belirtilen aşamalarda yapılmaktadır.

1. Kullanıcı mobil cihaz aracılığıyla ve WAP/GPRS servislerini kullanarak uygulama sağlayıcının uygulamasına bağlanır ve uygulamada imzalama işlemine kadar olan gerekli işlemleri yapar,
2. Uygulama, imzalama işleminin sırası geldiğinde kullanıcının mobil cihazına uygulama sistemi üzerinden imza talebi gönderir,
3. Kullanıcı, mobil cihazına imza talebi geldikten sonra imzalama emri verir ve imza oluşturma şifresini girer ve imzasını atar; mobil cihaz aracılığıyla uygulamaya gönderir,
4. Gerekli doğrulama işlemleri yapıldıktan sonra imzalama işlemi gerçekleşince uygulama ihtiyari olarak kullanıcının mobil cihazına veya e-posta adresine onay veya fatura bilgisi yollayarak

gerçekleştirir.

Şekil-3'de yer alan ikinci senaryoda kullanıcı uygulamaya mobil cihaz kullanmadan internet üzerinden ulaşmaktadır. Ancak imzalama işlevi mobil cihaz içerisine yerleştirilen SIM kart aracılığıyla yapılmaktadır [15].
Şekil 3'de verilen senaryoda;

1. Kullanıcı, mobil cihaz aracılığıyla internet üzerinden uygulama sağlayıcının uygulamasına bağlanır. İmzalama işlemine kadar olan gerekli işlemleri gerçekleştirir,
2. Uygulama, imzalama işleminin sırası geldiğinde kullanıcının mobil cihazına SMS ile imza talebi gönderir,
3. Kullanıcı, mobil cihazına imza talebi geldikten sonra imzalama emri verir ve imza oluşturma şifresini girer ve imzasını atar; mobil cihaz aracılığıyla imzalanmış veriyi SMS ile uygulamaya yollar,
4. Uygulama ihtiyari olarak kullanıcının mobil cihazına veya e-posta adresine onay veya fatura bilgisi yollar.



Şekil-3. Me-imza Oluşturma İkinci Senaryo

IV. MOBİL ELEKTRONİK İMZA UYGULAMA ALANLARI

Me-imza bir altyapı sistemi olması sebebiyle her türlü mobil uygulamada kullanılabilir ve hukuki olarak geçerli olma özelliğine ve birçok uygulamada kullanılabilecek potansiyele sahiptir. Mobil ortamlarda gerçekleştirilen mobil ticaret (m-ticaret) ve Mobil ödeme (m-ödeme) işlemleri me-imzanın
en çok kullanılabileceği uygulama alanlarıdır. Bu alanlar aşağıda alt başlıklarda özetlenmiştir.

4.1. Mobil Elektronik Ticaret

İletişim teknolojisi ve internetin sağladığı avantajlar akabinde e-ticareti tamamlayıcı nitelikte olan m-ticaret kavramı gelişmeye başlamıştır. Günümüzde dünyayı 24 saat açık küresel bir pazar haline dönüştüren internetin dezavantajları mobil iletişim araçlarıyla birlikte hızla ortadan kalkmaya başlamıştır. Kullanıcı sayısının hızla artmasına, öncelikle cep telefonu gibi mobil cihaz fiyatlarının düşmesi, kullanım kolaylığı, zaman ve mekândan bağımsız hareket etme rahatlığı gibi unsurlar m-ticaret uygulamalarının yapılmasını zorunlu hale getirmektedir. Mobil cihazlar yardımıyla sunulan mobil internet servisleri, kullanıcıların sabit bir bağlantı noktasına ihtiyaç duymasını gerektirmeden, diledikleri anda alım ve diğer işlemleri de anında yapma imkânı, kullanıcılara mobil cihazlarla kullanılabilecek şekilde özelleştirilebilen, sadece

ihtiyaç duyulan bilgi ve hizmeti verecek şekilde kişiselleştirilebilen özel servisler sunmaktadır [15,16].

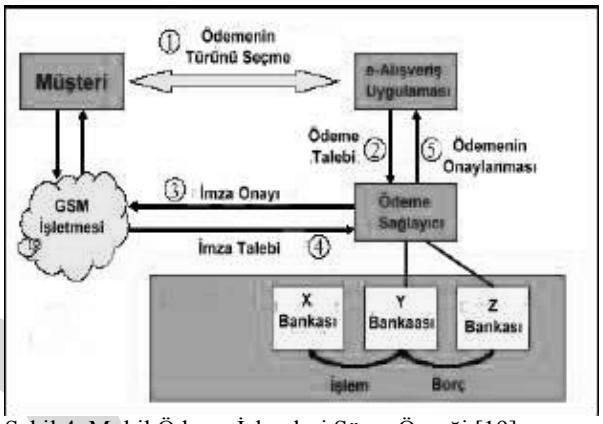
Me-imzanın en büyük kullanım alanı olan m-ticaret ile ilgili olarak birçok tanıma rastlamak mümkündür. Bu tanımların bir kısmı m-ticareti mali değerler içeren işlemler olarak sınırlandırırken, bir kısmı da iletişim, bilgi, işlem, eğlence gibi birçok işlemi içeren mobil ortamdaki servisler olarak tanımlamaktadır [17]. E-ticaret alanında gerçekleştirilen yeni bir devrim olarak nitelendirilmekte ve genel anlamda, kablosuz haberleşme ağları üzerinden yapılandırılan ve parasal değer ifade eden işlemler şeklinde ya da mobil cihaz veya benzeri araçlar yardımıyla yapılan, mal ve hizmetlerin satın alınması ve ücretlerinin ödenmesi işlemlerine verilen genel bir ad olarak tanımlanmaktadır [18].

Mobil iletişimin avantajları ve e-ticaretin özelliklerinin birleşimiyle oluşan mobil ortamlarda gerçekleştirilen, mobil mesajlaşma, çoklu ortam (multi-media) mesajlaşma servisi, m bankacılık, m-borsa, m-para, m-fatura gibi mobil finansal hizmetler, mobil güvenlik hizmetleri, m-rezervasyon, m-açık arttırma, m-posta kartı gibi mobil alışveriş, mobil reklâmcılık, m-üyelik, m-pasaport, m-oyun, m-müzik gibi mobil dinamik enformasyon yönetimi gibi m-ticaret uygulamaları, bankacılık, ticaret, rezervasyon ve bilet satışı, oyunlar ve bahisler gibi kategorilere ayrılabilir.

4.2. Mobil Ödeme

M-ticaret kavramı beraberinde ortaya çıkan m-ödeme kavramı, müşteri ile mal/hizmet sağlayıcı veya diğer bir müşteri arasındaki ticari işlemin bir parçası olarak mobil alet aracılığıyla yapılan, banka kartı veya kart temelli olmayan ve her iki durumda gerçek ve sanal dünyada gerçekleşen ödeme işlemleri olarak tanımlanmaktadır [19]. Kullanıcının tercihine, işlemin çeşidine ve karmaşıklığına bağlı olarak kullanılabilecek m-ödeme işlemleri için farklı şekiller ve farklı ödeme süreçleri mevcuttur [20]. Günümüzde m-ödeme işlemleri için kullanılan şekiller [19,20, 21]:

- SMS Ödemeleri: Şimdiye kadar ödeme servislerindeki tek yöntem olarak kullanılan, günlük çevrimiçi gazete veya zil melodisi gibi hizmetleri alabilmek için bu hizmetin bedelinin SMS olarak ödenmesi,
- Akıllı Para Olarak SMS: Park, satış otomatı veya geçiş ücreti kabinine ödeme işlemlerinin SMS olarak yapılması,
- Paylaştırılmış Ödemeler Sistemi: Gazete veya bir video klip görüntüsü gibi hizmetlerin kullanılan mobil araca yüklendikten sonra ücretinin ay sonunda mobil cihaz ödeme faturasından alınması,
- Elektronik Cüzdan: Kredi kartı veya bankamatik kartına benzer işlem yapmak için hücresel telefona, çip yerleştirilerek mobil aracın basit bir kablosuz kart okuyucu haline dönüştürülüp farklı ödeme işlemlerinde kullanılması,
- Etkileşimli Çağrı (Callback) Ödemeleri: Alıcının, satıcıya sağladığı mobil cihaz numarası, alıcı tarafından aranarak güvenilir bir ödeme işletmecisiyle bağlantı kurup ödemeyi doğrulamasından sonra miktarı toplayıp her iki tarafa teyit gönderdiğinde işlemin tamamlanması olarak sıralanabilir.



Şekil 4. Mobil Ödeme İşlemleri Süreç Örneği [19]

M-ödeme işlemlerinde işlemin karmaşıklığına ve çeşidine bağlı olarak farklı süreçler kullanılabilmektedir. M-ödeme işlemleri için kullanılan bu süreçlerin bir örneği Şekil 4'de gösterilmektedir. Bu örnekten görülebileceği üzere mödeme işlemlerindeki ilk adım kullanıcının mobil cihazı işlem yapmak istediği kuruluş uygulamasına ulaşmasıdır. Kullanıcı ve ticari hizmeti sunan taraf arasında ürün, teslimat, ödeme koşulları vb. gibi konularla ilgili anlaşma ya da onay sağlandıktan sonraki adım, kullanıcının satın almak istediği mal veya hizmeti seçmesi ve ödeme koşullarının belirlenmesidir. Bu aşamadan sonra hizmeti sunan taraf ya da kullanıcı tarafından, işlem bilgilerini içeren ödeme talebi ilgili finans kuruluşuna iletilir. Finans kuruluşu ödeme talebini kullanıcıya mobil cihaz aracılığıyla göndererek imza onayını alır ve ödeme işlemini başlatır. Böylece mobil cihaz kullanılarak başlatılmış olan işlem ve işleme ait ödeme, ilgili finans kuruluşunun da onayı alınarak gerçekleştirilmiş olur [19].

Bu işlemler sırasında finans kuruluşu, hizmet sağlayıcı ve kullanıcı arasında yapılacak işleme uygun ve güvenli olarak iletişim kurulması temel gereksinim olarak görülmektedir. Kullanıcının, kullandığı sistemde kendisine temin edilen güvenlik hakkında bilgi sahibi olması gerekmektedir. Hizmet sağlayıcı ve kullanıcı, m-ödeme işlemi sırasında ödemenin onaylanması/reddedilmesi konusunda uygun olması halinde kimlik bilgisi ile bilgilendirilmelidir [19]. M-ödeme işlemlerinde de karşılıklı tarafların birbirlerine duyacakları güven yine bu işlemlerde kullanılan MAAA teknolojisinin sağladığı bilginin bütünlüğü, inkâr edememe ve kimlik doğrulama işlevleri ile sağlanabileceğinden m-ödeme işlemlerinde MAAA teknolojisinin kullanımına talep süratle artmaktadır.

V. ÜLKE DURUMU

Eylül 2006'da ülkemizde de mobil ortamlara bilgi güvenliğinin sağlanabilmesi, mobil teknolojilerin sağlamış olduğu mekândan ve zamandan bağımsızlık ile kullanım kolaylığı ve e-imzanın yaygınlaşmasını sağlayabilmek hedefi ile mobil operatör Turkcell ile ESHS e-Güven ülkemizde me-imza ile ilgili test çalışmalarını başlattıklarını ilan etmişlerdir.

Ülkemizde me-imza kavramı hukuki karşılık olarak 5070 Sayılı Elektronik İmza Kanunu kapsamında elle atılmış imza ile aynı hukuki sonuca sahip **"**güvenli elektronik imza**"** ile aynı anlama gelmektedir. Bu nedenle mobil ortamlarda gerekleştirilen işlemlere hukuksal geçerlilik kazandırmak amacıyla ülkemizde birçok uygulamada e-imza ile birlikte me imza kullanımının da gerçekleştirilebilmesi için çalışmalar yapılmaktadır. Gümrük Müsteşarlığı mükelleflerinin gümrük idaresine gitmeden e-imza veya me-imza ile Gümrük Beyannamelerinin verebilmelerini sağlaya uygulama, Fatih Belediyesinin e-imzayı destekleyen uygulamalarına me-imza entegrasyonunu da gerçekleştirmiş olması gibi birçok uygulamaya süratle me-imza entegrasyonunda gerçekleştirilmesi için çalışmalar devam etmektedir [22,23].

Ülkemizde bankaların e-imzaya göstermedikleri ilgiyi me-imzaya göstermeleri ve Akbank, TEB, İş Bankası, Garanti Bankası, Yapı Kredi Bankası, HSBC, Bank Asya, TEB, Denizbank, Türkiye Finans gibi on bankanın internet bankacılığında me-imzayı kullanacaklarını Şubat 2007'de açıklamış olmaları ve müteakip altı ay içerisinde 50.000'in üzerinde kullanıcının me-imza almak üzere başvuruda bulunması, me-imzanın e-imza pazarını hareketlendireceğine işaret etmektedir [24].

Ülkemizde Karakaya Group'a bağlı olan KGC Consulting şirketini önerisi ve Adobe'nin desteğiyle Adobe ürünlerine Mobil İmza Entegrasyonunun sağlanmış olması ve bunun Telekomünikasyon Kurumunda bir uygulamada canlı olarak gösterilmesi ülkemizin mobil elektronik imzaya olan ilginin yüksek olmasının yanında yenilikçi unsurları da kapsaması açısından önem arz etmektedir [40].

Son günlerde Mobil Elektronik İmza'ya GSM operatörü Avea'nın da ilgi göstermesi ve TürkTrust ile işbirliği yaparak Ekim 2007 başında CEBİT'te Avea Mobil İmza'nın lansmanını yapacağını duyurması ise mobil elektronik ortamlara ilginin yüksek olacağı ve bu alandaki rekabetin artarak yaygınlaşmanın ve bu alanda yapılacak olan uygulamaların sayısının hızla artacağını göstermektedir.

Ülkemizdeki yüksek mobil cihaz penetrasyonunun ve me-imzanın avantajlarının me-imzanın yaygınlaşmasını hızlandıracağı değerlendirilmektedir.

VI. DÜNYA DURUMU

2002 yılı sonuna kadar pek çok ülkenin e-imza mevzuatlarını hazırlamış ve yasal altyapılarını oluşturmuş olmalarına rağmen elektronik imzaya sahip olma ve altyapıyı oluşturma maliyetlerinin yüksek olması, kullanılabilecek uygulama sayısının yeterli olmayışı ve elektronik ortamların mobil elektronik ortamlara kayması gibi sebeplerden dolayı aradan geçen süre içerisinde e-imza dünyada beklenen seviyede yaygınlaşamamıştır [5,39].

Mobil ortamların kullanıcılara sunduğu üstünlükler mobil cihaz penetrasyonunda artış ve bu ortamlara yapılan yatırımların her geçen ün artması sebebiyle bu ortamlar hızla yaygınlaşmaya başlamıştır. Bu yaygınlaşması beraberinde güven sorununu getirdiği için de bazı dünya ülkeleri me imzaya geçiş için çalışmalar yapmaya başlamışlardır. Özellikle Avrupa Ülkeleri, me-imzanın bilgi toplumunun gelişimine katkılar sağlayacağını değerlendirdiğinden bu konuya çok önem vermişlerdir.

Finlandiya, İsveç, Estonya, Norveç, Macaristan, Danimarka, Polonya, Lüksemburg, Litvanya, Portekiz, İngiltere, Fransa, İtalya, Çin, Almanya, İspanya, Slovenya, Kuveyt, Singapur ve Avusturya gibi ülkelerde farklı farklı uygulamalarda me-imza kullanılmakta yada kullanılabilmesi test çalışmaları yapılmaktadır. Bu ülkeler arasında mobil cihaz penetrasyonu %91 olan Finlandiya'daki me-imza uygulamaları dikkati çekmektedir.

Finlandiya'da özel sektör uygulamalarında me-imza kullanımı oldukça sınırlı olmasına rağmen kamuda halen e-devlet portalı, e-fatura ödeme, marka ve patent başvurusu, adres değişiklik bildirimi, inşaat, imar iskân izinleri, mesleki eğitim ve okul başvuruları, askerlik başvuru işlemleri, şahsi nüfus bilgilerine erişim ve kontrol, sosyal güvenlik kurumları, emeklilik ve çalışma durumu işlemleri, çalışma bakanlığına yapılan bildirimler, maliye bakanlığı vergi beyanları, sağlık bakanlığı sağlık kayıtlarına erişim gibi 50 serviste kullanılmaktadır. Bankalardan sadece bir bankada internet bankacılığında me-imza kullanabilme imkânı vardır. [24-29].

Estonya'da m-ticaret işlemleri, otopark ücreti ödeme, toplu taşım ücreti ödeme işlemlerinde me-imza kullanılabilmektedir ve ayrıca ülkede ID kart işlemlerinde kullanılabilmesi için çalışmalar Mayıs 2007'den itibaren başlamış durumdadır [30,31] .

Diğer ülkelere incelediğimizde,

- Norveç'de m-ticaret, bankacılık işlemlerinde,
- İsveç'te m-ödeme banka ve haberleşme işlemlerinde,
- Litvanya'da m-ödeme işlemlerinde,
- İngiltere'de m-ödeme işlemlerinde,
- Fransa'da park ücreti ödeme işlemleri, dondurma siparişi verme, at yarışları gibi m-ödeme işlemlerinde,

- Çin'de kimlik kartlarında,
- Almanya'da bankacılık işlemleri ve m-ödeme işlemlerinde,
- Slovenya'da m-devlet uygulamalarında, m-bankacılık işlemlerinde ve m-vergi işlemlerinde,
- Kuveyt'te m-ödeme ve m-ticaret işlemlerinde,
- Avusturya'da e-ID kart olarak,
- Macaristan'da vergi beyannameleri,
- İtalya'da bankalar ve finans işlemleri gibi birçok uygulamada me-imza uygulamaları dikkat çekmektedir [32,34] .

Me-imza konusunda çalışması olan veya bu konuda çalışmayı hedefleyen ülkeler genel olarak değerlendirildiğinde, me-imza konusunda çalışma yapan ülkelerin çoğunluğunun Avrupa Ülkesi olduğu, Amerika, Kanada gibi birçok ülkenin de söz konusu Avrupa Ülkelerindeki çalışmaları yakından izlediği, bu ülkelerde kesin olarak belirlenmiş bir model olmadığı genellikle uygulamalara yönelik farklı çözümlerin kullanıldığı ve birçok uygulamanın henüz test aşamasında olduğu, ülkelerin hepsinde e-imzanın denetiminden sorumlu kuruluşların me-imza denetiminden de sorumlu olduğu ve birçoğunun eimza için yapmış olduğu düzenlemelerinin me imza için de yeterli bulduğu ve çıkabilecek herhangi bir teknik uyumsuzluk problemini engellemek, birlikte çalışabilirliği sağlayabilmek amacıyla ETSI'nin bu konuya ilişkin standartlarına da uyum sağladıkları görülmektedir.

VII. STANDARTLAR

Bu bölümde me-imza ile ilgili doğrudan veya dolaylı olarak ilişkili standardizasyon kuruluşlarının ve düzenleyici kuruluşların oluşturdukları standartlar kısaca açıklanmıştır.

7.1. ITU-T Recommendation X.1122

ITU tarafından yayımlanan bu önerinin amacı; AAA teknolojisine dayalı mobil güvenlik sistemler kurulurken içerdiği yardımcı kurallar ile bu hizmeti verecekler ve alacaklara rehberlik etmektir [30]. Bu öneriler paketi Nisan 2004'de yayımlanmış ve 10 bölümden oluşmaktadır. Bu öneride bölümler; amaç, kaynaklar, tanımlar, kısaltmalar, AAA teknolojisine ait kategoriler, uçtan uca haberleşmelerde AAA çalışmaları, haberleşme sistemlerinde kullanıcı modeli, sistem oluşturulma modellerine örnekler, sistem konfigürasyon örnekleri ile uçtan uca mobil haberleşmede AAA üzerine düşünceler kısmından oluşmaktadır. Bu bölümlerden önemlileri aşağıda kısaca açıklanmıştır.

AAA teknolojisine ait kategoriler bölümünde AAA'nın mevcut teknolojileri ve sınıflandırılması yapılmıştır.

Uçtan uca veri haberleşmelerde AAA çalışmaları bölümünde anahtar çiftinin nasıl, kim tarafından nerede üretilmesi gerektiği, sertifika başvurusu, oluşturulması ve kullanımı ile bunlara bağlı modeller, sertifikanın kullanımında imzalayan, doğrulayan (sertifika geçerliliği, kullanıcı-SM, mesaja bağlı olan imza), sertifikanın iptali (online veya offline), sertifikanın yenilenmesi (yeni anahtar çifti, sertifika,
vb) işlemlere ait öneriler bulunmaktadır.

AAA tabanlı güvenli mobil sistem modelleri bölümünde kullanıcı-uygulama hizmeti sağlayıcı genel yapıları ile kullanıcı-mobil ortam arası güvenlik ile gateway-uygulama hizmeti sağlayıcı arası güvenlik modelleri önerilmiştir.

Haberleşme sistemlerinde kullanıcı modeli bölümünde oturum üstü katman kullanım modelinde gerçekleştirilen fonksiyonlar (Sunucu Onayı, İstemci Onayı, İletişim Kanalı Şifreleme ve Bütünlüğü) ile Uygulama Seviyesinde Kullanım Modeli (bütünlük ve doğrulama gibi imzalama fonksiyonları, gizlilik için şifreleme fonksiyonları) değerlendirilmiştir.

Sistem konfigürasyon örnekleri bölümünde; sertifika yönetim sistemi, yayımlama, doğrulama, sertifika iptal listeleri, sertifika tabanlı doğrulama modeli, kullanıcı, taşıyıcı ve uygulama hizmeti sağlayıcı ve finansal kurumlara örnekler verilmektedir. **Düşünceler** bölümünde; mevcut sistemler arası haberleşme (Yayımlama, Doğrulama, SİL), mobil ortamlarda AAA kullanımı ve genel olarak AAA kullanımı (anahtar üretimi, sertifika başvuru, yayımlama ve kullanma, Sertifika iptal, sertifika yenileme ve tanımlama) konularında gelecekle ilgili endişelere ve yapılabileceklere yer vermişlerdir.

7.2. ETSI TR 102 203 Mobil Ticaret (M-COMM); Mobil Elektronik İmzalar; İş ve İşlevsel Gereksinimler

Mayıs 2005 de çıkan bu standart, 14 bölümden oluşmaktadır. Bu standardın konusu; standart olan eimza çözümlerini kolaylaştırmak ve yaymak için GSM SIM kart dahil olmak üzere akıllı kart ve AAA'da kullanılan şifreleme teknikleri ile me-imza süreçlerinin koordine edilmesini ve yönetilebilmesini içeren hizmetin iş ve işlevsel gereksinimler olarak verilmiştir [35]. Burada amaç; birlikte çalışılabilirlik, güvenlik önlemleri ve arayüzlere ilişkin teknik özellikleri belirleyebilmek için yön gösterici olmak ve me-imza çözümlerinin tasarım ve uygulamasına yardımcı olmak olarak belirlenmiştir. Bu standardın bazı önemli bölüm başlıkları; Me-imza, Me-imza Tasarım Kriterleri, Me-imzanın Kullanım Durumu, Me-imza Süreci, Me-imza Hizmeti, Meimza Uygulama Sorunları, Potansiyel Roller ve Sorumluluklar, Etkileşimler ve Arayüzler ile Gereksinimler olarak verilmiştir.

7.3. ETSI TR 102 206 Mobil Ticaret (M-COMM) Mobil Elektronik İmza Hizmeti; Güvenlik Gereksinimleri

Ağustos 2003'de çıkan bu standart 7 bölümden oluşmaktadır. Genel Güvenlik Analizi, Me-imza Oluşturma Sistemi İçin Güvenlik Gereksinimleri ve Me-imza Profili gibi konuları değerlendirmekte ve bu konularda öneriler sunmaktadır [36].

7.4. ETSI TS 102 204 Mobil Ticaret (M-COMM); Mobil Elektronik İmza Hizmeti; WEB Servis Arayüzü

Ağustos 2003'de çıkan bu standart, 11 Bölüm, Ağustos 2003 Me-imza hizmet fonksiyonları ve 7 farklı me-imza web servislerini ve 13 mesaj formatını içermektedir [37]. Bu bölümde me-imza, me-imza statü sorgulama, me-imza görüntü sorgulama, me-imza kaydı, me-imza alındısı, me-imza uyumluluğu, fatura sorgulama, kayıt, bildirim ve uyumluluk ile Genel ESHS ve uygulama hizmet sağlayıcı gibi destek tipleri, iletişim protokol kuralları (kodlama kuralları, SOAP: header, body, hata giderme) ve web servisi (güvenlik ve gizlilik) konularını içermektedir.

7.5. ETSI TS 102 207 Mobil Ticaret (M-COMM); Mobil Elektronik İmza Hizmeti; Mobil Elektronik İmza Hizmetinin Dolaşım Şartları

Ağustos 2003'de çıkan bu standart 11 bölümden oluşmaktadır. Mobil ticaret ile mobil elektronik imza hizmetinin dolaşım şartlarını içermektedir [38]. Amacı ise kullanıcı ile uygulama sağlayıcı arasındaki me-imza mesajlarının dolaşımını kolaylaştırmak ve belirli bir modelin oluşumunu sağlamak için SOAP ve http mimarisi üzerinden teknik arayüzleri belirlemektir. Bölüm başlıkları ise; Mobil Elektronik İmza Dolaşım Hizmeti; Dolaşım Konuları, Birlikte Çalışabilirlik, İşlevsel Gereksinimler; Dolaşım Çözümü (kullanıcının ilişkili olduğu MESHS'nin bulunması -Uluslararası Mobil Abone Kimliği- ve bir şebeke vasıtasıyla yol bulunması), 5 farklı senaryoyu, dolaşım hizmetinin teknik tanımı, veri formatları (SOAP başlık ve XML veri tipi) ve işleme talimatları olarak verilebilir.

VIII. SONUÇLAR

İçinde bulunduğumuz bilgi çağının altyapısını oluşturan bilişim ve iletişim teknolojilerindeki gelişmeler doğal olarak bizleri elektronik ortamlara bağımlı hale getirmekte, bu ortamlardan beklentilerimizi arttırmaktadır. Yaşantımızın vazgeçilmez bir parçası haline gelen bu ortamlar ve bu ortamlarda sunulan hizmetler ve geliştirilen uygulamalar ile kaynakların etkin kullanımı, zaman ve mekân bağımsız olarak iş ve işlemlerin yapılması, açıklık, şeffaflık, hesap verilebilirlik, katılımcılık, hizmet kalitesi, verimlilik artışı ve en önemlisi mobil elektronik imza ile ise yüksek seviyede güvenli bir ortamın sunulması gibi fırsatlar sunmaktadır.

Öte yandan hukukende geçerli olması sebebiyle de bilgilerin yetkisiz değiştirilmesi, yok edilmesi, çalınması, kişi adına başkalarının işlem yapabilmesi, kişisel verilerin ele geçirilmesi gibi bazı tehditlere karşı teknik olarak koruma sağlamanın yanında hukukende geçerli iş ve işlemlerin yapılmasına da imkan sunmaktadır. Me-imza, sağlamış olduğu kimlik doğrulama, veri gizliliği ve bütünlüğü, inkâr edilemezlik gibi özellikleriyle sanal ortamda karşılaşılan söz konusu güvenlik açıklarının aşılmasına ve sanal ortamda yapılan işlemlerin hukuken de geçerli olmasına katkılar sağlamaktadır.

Ülkemizde 2004 yılında çıkarılan E-İmza Kanunu ile geçerlilik kazanan e-imza uygulamalarının sayısı bugün için 20,000'e yaklaşırken mobil elektronik ortamlarda bunun 3 kanına çıkması ise me-imzanın elektronik ortamlarda yapılan iş ve işlemlerin güvenli hale getirilmesinde katalizör bir etki yaratacağı ve ortam güvenliğinin yüksek seviyede sağlanmasına büyük katkılar sağlayacağı değerlendirilmektedir. 8 Dünyada hızla artan mobil cihaz sayısının ve haberleşmenin ülkemizi de etkilemiş mobil cihazlar üzerinden internet hizmetinin de verilmeye başlanmasıyla, bu teknolojilerin sunduğu hizmetlerde farklılıklar oluşmuş, bilgiye mobil ortamlardan erişim sağlanmış, iş ve işlemler mobil ortamlara kaymaya başlamıştır. Mobil ortamlarda yaşanan güven sorununu engelleyebilmek için gündeme taşınan me-imzanın hızla yaygınlaşmasının hem ülkemiz hem de diğer ülkeler için kaçınılmaz bir sonuç olduğundan dolayı ülkelerin me-imza uygulamalarını arttırabilmek için çalışmalarını hızlandıracağı ve kısa bir süre sonra ülke modellerini belirleyecekleri değerlendirilmektedir.

Bu çalışmada kullanılabilecek me-imza senaryoları, uygulamalar, standartlar, ülkeler değerlendirilmiştir ve me-imzaya daha geniş bir açıdan bakılmasına katkılar sağlanmaya çalışılmıştır. Literatüre bu tür kaynakların artmasıyla me-imza ve uygulamaların daha sağlıklı olarak gelişmesine katkılar sağlanabilecektir.

IX. KAYNAKLAR

1. Atlığ, C., Uçar, Ö., Uçar, E., Mobil ve Kablosuz Sistemlerde Bilgi Erişim Özellikleri http://ab.org.tr/ab06/168.doc
2. Cep Telefonunda Lider Çin, Türkiye Dünya 10'uncusu, Tele.com.tr Dergisi Ekim 2006, s.6
3. Telekomünikasyon Kurumu 2006 yılı Faaliyet Raporu
4. Europe Mobile Handset Market Analysis (2007), http://www.researchandmarkets.com/reports/c28137
5. Sağıroğlu, Ş., Kabasakal, D., Alkan,M., Mobil Elektronik İmza Altyapısı ve Türkiye, Ulusal Elektronik İmza Sempozyumu, Sheraton Hotel & Convention Center, Ankara, 7-8 Aralık 2006, s.91-97
6. The Future of Electronic Signatures, http://ntrg.cs.tcd.ie/undergrad/4ba2.02/sigs/future.html
7. GSM Association: GSM Statistics, www.gsmworld.com/news/statistics/index.shtml
8. ETSI TR 102 203: Mobile Commerce (MCOMM); Mobile Signatures; Business and Functional Requirements, http://portal.etsi.org/docbox/EC_Files/EC_Files/tr_102203v010101p.pdf
9. ETSI TR 102 206 Mobile Commerce (MCOMM); Mobile Signature Service; Security Framework, http://portal.etsi.org/docbox/EC_Files/EC_Files/tr_102206v010103p.pdf

10. Mark Gasson (University of Reading, UK), Martin Meints (ICPP, Germany), Kevin Warwick (University of Reading,UK), D3.2: A Study on PKI and Biometrics, Future of Identity in the Information Society (FIDIS), No:507512, 4 July 2005
11. L. Fritsch, J. Ranke, and H. Rossnagel: Qualified Mobile Electronic Signatures: Possible, but worth a try? In: Information Security Solutions Europe (ISSE) 2003 Conference, Vienna Austria
12. H. Rossnagel: Mobile Qualified Electronic Signatures for Secure Mobile Brokarage Possible, but worth a try? In: Proceedings of the 4th International Cyprus Information Security Conference & Workshops; Nicosia, Cyprus 2004-118
13. H. Rossnagel: Mobile Qualified Electronic Signatures and Certification on Demand, Proceedings of the 1st European PKI Workshop - Research and Applications, Springer LNCS 3093; Samons Island, Greece
14. Directive 1999/93/EC of the European Parrliament and of Council of 13 December 1999 on a Community frame-work for electronic signatures
15. Beceni, Y., Mobil Elektronik İmza, TK'ya Özel Olarak Sunulmuş Rapor, 2006
16. Sarısakal,M.N., Aydın,M.A., e-Ticaretin Yeni Yüzü Mobil Ticaret, Havacılık ve Uzay Teknolojileri Dergisi, Cilt 1, Sayı 2, 2003, s. 83-90
17. Schwiderski-Grosche, S.,Knospe, H., Secure m-Commerce, http://www.isg.rhul.ac.uk/~scarlet/documents/Secure%20m-commerce%20ECEJ.pdf
18. What is m-commerce, http://www.mobileinfo.com/Mcommerce/index.htm
19. ETSI TR 102 071, Mobile Commerce (MCOMM); Requirements for Payment Methods for Mobile Commerce,http://webapp.etsi.org/action/PU/20021029/tr_102071v010201p.pdf
20. Schwiderski-Grosche, S., Knospe, H., Secure Mobile Commerce, Electronics & Communication, Engineering Journal, volume 14, 2002, s.228-238
21. Reding, V., Towards a European Payment and Information Space: m-Payments, http://ec.europa.eu/information_society/newsroom/cf/itemshortdetail.cfm?item_id=2725
22. http://www.referansgazetesi.com/haber.aspx?HBR_KOD=70189&KTG_KOD=178&ForArsiv=1
23. http://www.uruninceleme.com/haberdetay.aspx?Id=620
24. D. Tunçalp, Mobil İmzanın Finans Sektöründe Güvenlik Alanındaki Olası Uygulamaları, 22.BMBB Toplantısı ve "Finans Sektöründe Güvenlik" Çalıştayları, TBV, Süleyman Demirel Kültür Merkezi, İTÜ, Maslak Kampusü, 21 Eylül 2007.
25. Services using an electronic ID card, http://www.fineid.fi/vrk/fineid/home.nsf/pages/5982EEE5795622DEC225709700387995
26. Finnish public sector online services, http://www.suomi.fi/suomifi/english/index.html
27. Sonera Mobile Certificate, http://www.sonera.fi/GetImages/GetImages_GetImage_pdf/0,2580,66424,00.pdf
28. Tunçalp,D.,Turkcell Mobil İmza Sunumu, Ulusal Elektronik İmza Sempozyumu, Sheraton Hotel & Convention Center, Ankara, 7-8 Aralık 2006
29. Finland to use Mobile Digital Signatures for eGovernment Services, http://www.contactlessnews.com/weblog/2005/07/21/finland-to-use-mobile-digital-signatures-foregovernment-services/, 28.12.2006
30. Mobile-ID service launched, http://www.ria.ee/?id=28639&langchange=1
31. Mobile Services in Tartu, http://www.tartu.ee/?page_id=58&lang_id=1&menu_id=6&lotus_url=/uurimused.nsf/Web/teemad/5C3CF5BE6E7B3689C22570E5004DF9E9
32. Kabasakal,D.,Elektronik İmzadan Mobil Elektronik İmzaya Geçiş Sürecinde Yansımalar, Uygulamalar ve Öneriler, Telekomünikasyon Kurumu Uzmanlık Tezi,
33. Valimo signs partnership with Capgemini Italia for Mobile Signature Services in Italy, http://www.mobileeurope.co.uk/news_wire/113109/WIRE:_Valimo_signs_partnership_with_Capgemini_Italia_for_Mobile_Signature_Services_in_Italy_.html
34. ITU-T Recommendation X.1122, Guideline For Implementing Secure Mobile Systems Based On PKI
35. ETSI TR 102 203: Mobile Commerce (MCOMM); Mobile Signatures; Business and Functional Requirements,http://portal.etsi.org/docbox/EC_Files/EC_Files/tr_102203v010101p.pdf
36. ETSI TR 102 206 Mobile Commerce (MCOMM); Mobile Signature Service; Security Framework,http://portal.etsi.org/docbox/EC_Files/EC_Files/tr_102206v010103p.pdf
37. ETSI TS 102 204 Mobile Commerce (MCOMM); Mobile Signature Service; Web Service Interface, http://portal.etsi.org/docbox/EC_Files/EC_Files/tr_102206v010103p.pdf
38. ETSI TS 102 207 Mobile Commerce (MCOMM); Mobile Signature Service; Specifications for Roaming in Mobile Signature Services, http://portal.etsi.org/docbox/EC_Files/EC_Files/ts_102207v010103p.pdf
39. Sağıroğlu, Ş., Kabasakal, D., Alkan,M., Elektronik İmzadan Mobil Elektronik İmzaya Geçiş Sürecinde Türkiye, Sheraton Hotel & Convention Center, Ankara, 7-8 Aralık 2006, s.21-27.
40. Ü. Karakaya, PDF Dokümanları Üzerinde Mobil Elektronik İmza Uygulamaları, 22. BMBB Toplantısı ve "Finans Sektöründe Güvenlik" Çalıştayları, TBV, Süleyman Demirel Kültür Merkezi, İTÜ, Maslak kampusü, 20 Eylül 2007.