Gazi Üniv. Müh. Mim. Fak. Der.
Cilt 23, No 1, 49-56, 2008

J. Fac. Eng. Arch. Gazi Univ.
Vol 23, No 1, 49-56, 2008

MOBİL ELEKTRONİK İMZA, ALTYAPISI ve TÜRKİYE

Şeref SAĞIROĞLU, Demet KABASAKAL* ve Mustafa ALKAN*
Bilgisayar Mühendisliği Bölümü, Mühendislik Mimarlık Fakültesi Gazi Üniversitesi, Ankara
*Telekomünikasyon Kurumu, Maltepe, Ankara
ss@gazi.edu.tr, dkabasakal@tk.gov.tr, malkan@tk.gov.tr

(Geliş/Received: 06.02.2007; Kabul/Accepted: 27.08.2007)

ÖZET

Dünyada olduğu gibi ülkemizde de mobil cihaz penetrasyonu hızla artmaktadır. Doğal olarak mobil ortamlarda yapılan iş ve işlemler çoğalmakta, bu ortamlara güven ise ön plana çıkmakta, yüksek seviyede bilgi ve iletişim güvenliğine ihtiyaç duyulmaktadır. Bu çalışmada, ülkemizde de önümüzdeki günlerde önemli hale gelecek olan mobil imza teknolojileri ve dünya uygulamaları ile mobil elektronik imzada (me-imza) kullanılan altyapılar incelenmiş, ülkemizde de me-imza'ya geçilebilmesi için gerekli olan düzenlemeler, hususlar ve hazırlıklar ile ilgili öneriler sunulmuştur.

Anahtar Kelimeler: E-imza, me-imza, uygulamalar.

MOBILE ELECTRONIC SIGNATURE, INFRASTRUCTURE AND TURKEY

ABSTRACT

Mobile phone penetrations have increased in Turkey in recent years, as well as in the world. As a result of that operations and businesses on mobile environments have also rised. Trust to those environments and securing information on those have become important. In order to cover this expectation, in this study, mobile electronic signature (me-sign) technologies were revised, the models used for infrastructures and the applications in the world used in these infrastructures were reviewed. Implementing me-sign in Turkey is discussed. Finally, a number of issues were suggested for me-sign applications and regulations in Turkey.

Keywords: E-sign, me-sign, applications.

1. GİRİŞ (INTRODUCTION)

İş ve işlemlerin elektronik ortamlarda yapılmaya başlanmasıyla, hayatımız kolaylaşmakta, yaşam kalitemiz artmakta, iş ve işlemler hızlanmakta ve iş verimliliği artışı sağlanmaktadır. Fakat karşılaşılan sıkıntılar, beklenmeyen durumlar ve maddi ve manevi kayıplar elektronik ortamlarda meydana geldikçe bu ortamlar bizleri çoğu zamanda hayal kırıklığına uğratabilmekte ve sonuç olarak bu ortamlarda güvensizliği ortaya çıkmaktadır [1].

5070 sayılı Elektronik İmza (e-imza) Kanunu ve ikincil düzenlemeler, bu ortamlara güven sorununu ortadan kaldırmakta, iş ve işlemlerin hukuken de geçerli olmasını sağlamakta ve bunun yerine getirilmesi için gerekli olan teknik altyapısıyı yani açık anahtar altyapısı (AAA) ve standartları belirtmektedir. Böylece e-imza mevzuatı, elektronik ortamlara güven sorununu da ortadan kaldırmaktadır [2].

Bu altyapının elektronik ortamlarda işlenen, taşınan ve saklanan verilerin güvenliğini çok yüksek seviyelere çıkarması ve bunun hukukende geçerlilik kazanması ile günlük hayatımızda, iş ve işlemleri yapış şekillerimiz değişmekte, iş verimliliği artışı sağlamakta, iş ve işlemler kısa sürelerde yapılabilmekte ve hayat daha yaşanılır bir hal almakta belki de en önemlisi sanal dünyayı tanıma ve etkili kullanma yüzdesi hızla artmaktadır. Bu sebeplerden dolayı e-devlet, e-sağlık, e-öğrenme, e-ekonomi, e-banka, e-kayıt, e-mağaza, e-üniversite gibi e-li kavramlar ve uygulamalar hayatımıza hızla girmektedir.

Ülkemizde elektronik ortamların yaygınlaştırılması hızla sürerken, iş ve işlemlerin mobil ortamlara kaymaya başladığı gözlemlenmektedir. Bunun haklı gerekçesi tüm dünyada hızla artan mobil cihaz sayısının ve haberleşmesinin ülkemizi de etkilemiş olmasıdır. Dünya mobil haberleşme sayısının 2006'nın ilk 6

ayında 2,25 milyarı aştığı [3], ülkemizdeki GSM abone sayısı 2005 yılı sonu itibariyle yaklaşık 44 milyona, 2006 yılı mart ayı itibariyle 46 milyona ulaştığı görülmektedir [4]. Bu sayılarla ülkemiz dünyada en çok mobil cihaz kullanan ülkeler arasında 10. sırada yer almaktadır [5]. Ülkemizde %60'lar 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 [2,4].

Ülkemizin gelecekteki abone yoğunluğunun üst sınırının %70 olacağı varsayımıyla, 2011 yılına kadar olan abone sayısının 54,53 Milyona ve %69,72'lik bir abone yoğunluğuna ulaşılması öngörülmüş [4] ise de bugün için bile bu öngörüler aşılmıştır. 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.

Dünyada ve ülkemizde hızla yayılmaya devam eden mobil araçlar üzerinden internet hizmetinin de verilmeye başlanmasıyla, bu teknolojilerin bizlere sunduğu hizmetlerde farklılıklar oluşmuş, bilgiye mobil ortamlardan erişim sağlanmıştır. Bu araçlar üzerinden mobil ticaret, mobil bankacılık, mobil işlemler gibi birçok uygulamalar yapılabilmeye başlanmıştır. Mobil ortamlarda iş ve işlemlerin yaygınlaşması da elektronik ortamlarda olduğu gibi mobil elektronik ortamlarda da güven sorununu ortaya çıkarmaktadır. Bu ortamlarda iş ve işlemlerin hızlı ve verimli olarak yapılabilmesinin yanında güvenli olarak da yapılmasını sağlamak gerekmektedir. İşte e-imzada olduğu gibi mobil ortamlarda da mobil elektronik imza (me-imza) AAA (MAAA)'sının ülkemizde de kurulması ve işletilmesi gerekmektedir [6].

Yukarıda açıklanan sebeplerden dolayı, bu çalışmada me-imza'ya geçiş için gerekli olan teknik hususlar gözden geçirilmiş, me-imza'ya geçiş sürecinde yapılması gerekenler tartışılmış, farklı ülke me-imza uygulama modelleri incelenmiş, karşılaşılabilecek olumlu ve olumsuz hususlar değerlendirilmiş ve ülkemizde de me-imza altyapısı oluşturulurken yapılması gerekenler sunulmuştur.

2. MOBİL ELEKTRONİK İMZA VE AÇIK ANAHTAR ALTYAPISI (MOBILE E-SIGN and PKI)

Günümüzde mobil ortamların kullanımı ve bu ortamlardaki uygulamalar yaygınlaştıkça bu ortamlara güven ön plana çıkmaktadır. Mobil ortamlarda yüksek seviyede bir bilgi güvenliğinin sağlanabilmesi için; bu ortamda saklanan, gönderilen veya alınan bilgilerin, bunları gönderen kişi veya kuruma ait olduğunun doğrulanması, iletilen veya alınan verilerin bildiğimiz kişiler tarafından gönderildiğinin belirlenmesi, bilgileri gönderenlerin gönderdiğini ve alanların aldığının inkar edilememesi, gönderilen veya alınan bilgilerin içeriğinin değiştirilememesi, başkaları tarafından elde edilse bile içeriğinin başkaları tarafından anlaşılamamasının garanti edilmesi gerekmektedir. Bunun için, mobil ortamda da elektronik ortamda olduğu gibi güvenli haberleşmeye ihtiyaç vardır. Mobil ortamda güvenli bir haberleşmenin sağlanabilmesi için yine elektronik ortamda olduğu gibi me-imza ve mobil açık anahtar altyapısı (MAAA) kullanılmalıdır.

Me-imza Wikipedia'da "bir cep telefonu içersisinde üretilen elektronik imza" olarak tanımlanmaktadır. Me-imza, mobil cihazların özelliklerinden bağımsız olarak teknik gereksinimlerinin tanımlandığı ETSI tarafından yayımlanan standartlarda "bir kullanıcının bir antlaşmayla ilgili kararının onayını mobil bir aletle almak için kullanılan evrensel yöntem" olarak tanımlanmaktadır [7-10]. Bu tanımda evrensel yöntem; son kullanıcı ve servis sağlayıcı için en büyük interaktif topluluk veya uyumluluğu artıran ve kurulum maliyetini düşüren bir mimari, mobil alet; iletişim kanalı olarak mobil ağ kullanan mobil telefon, PDA gibi her türlü alet, antlaşma kavramı ise; kullanıcının onayının beklendiği ve tüm detaylarının onay aşamasından önce kullanıcının mobil telefonuna gönderildiği ve ekranında gösterildiği etkileşim olarak kabul edilmiştir.

MAAA ise bu hizmetlerin aksamadan verilebilmesi, güvenlik unsurlarının bazılarının yerine getirilmesi, yüksek seviyede bir güvenlik sağlanması ve yapılan işlemlerin hukuken de geçerli olabilmesi için hizmet verilen ortamlardır. Bu ortamlarda; e-imzada olduğu gibi açık anahtar tekniğine dayanan bir sistemin ana işlemleri olan kullanıcı kaydı, anahtar çifti üretimi, sertifikanın oluşturulması, sertifikaların ve anahtarların güvenli dağıtımları, sertifika yolunun (güven zincirinin) oluşturulması ve sertifika ve imzanın onaylanması, kayıp, şüphe, çalıntı veya diğer sebeplerle anahtarları hükümsüz kılma, anahtar yedekleme ve kurtarma işlemlerinin desteklenmektedir. MAAA üzerinde çalışan me-imza genel olarak, mobil bir cihaz kullanılarak oluşturulan ve telekomünikasyon ortamından bağımsız bir konumda imza veya sertifikasyon hizmetleri verilen mobil güvenliğin sağlanmasında kullanılır [7,12].

AAA'da olduğu gibi MAAA'larda da gizlilik, bütünlük, kimlik doğrulama ve inkâr edememe unsurlarının sayısal sertifikalar kullanılarak sağlanmaktadır. Buradaki tek fark, arada mobil hizmeti sunan operatörlerin devreye girmesiyle oluşmaktadır. Me-imza, imza sahibine bağlı olmanın ötesinde mobilite, güvenli masaüstü iş istasyonları ve kişisel imzalama ekipmanlarıyla sağlamaktadır [7,12].

E-imza oluşturmak için mobil cihazlar kullanılmasının, ekran boyutu, haberleşme maliyeti, sınırlı hesaplama gücü gibi olumsuzlukları olmasına rağmen pazardaki yüksek penetrasyonu, zaman ve yer bağımsız olarak sunulan imzalama imkânı, me-imzayı yaygınlaşması açısından potansiyel olarak başarılı kılmaktadır [13].

Me-imzalar, elektronik sertifika hizmet sağlayıcılarda (ESHS) bulunan merkezileştirilmiş imza sunucu ortamında oluşturulan e-imzalar (sunucu tabanlı mobil elektronik imzalar) ve kullanıcının mobil cihazı içerisindeki akıllı kart kullanılarak oluşturulan elektronik imzalar (istemci tabanlı mobil elektronik imzalar) olmak üzere ikiye ayrılmaktadır [7,14]. Bu yaklaşımlar aşağıdaki bölümlerde kısaca açıklanmıştır.

2.1 Sunucu Tabanlı İmzalar (Server Based Signs)

STİ'ler, bir ESHS tarafından özel kullanıcılar için güvenli bir sunucuda oluşturulmuş imzalardır. Şekil 1'de bu imzalama yöntemine bir örnek verilmiştir.

Şekil 1'de görülebileceği gibi sunucu tabanlı me-imzalar, mobil cihaz tarafından cihazın tuş takımı kullanılarak girilen PIN kodundan sonra oluşturulan uygun bir kod (MAC vb mesaj onaylama kodu) tarafından başlatılır. Kodun ESHS'deki sunucuda yapılacak olan imza oluşturma işlemini başlatmasından sonra sunucuda, kullanıcı imzalama işlemi gerçekleştirilir. Kullanıcıya ve üçüncü kişiye (güvenen tarafa) oluşturulan imza gönderilir.

Sunucu tabanlı imzalarda kullanıcının kendi gizli anahtarını ESHS'ye devretmesi zorunludur. Bu imzalarda, ESHS'nin yayımlandığı 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.

AB tarafından hazırlanan 99/93/EC direktifinin 2. bölümünün (c) bendine göre, "güvenli elektronik imza elde etmek için; imza, imza sahibinin kendi özel kontrolünde kalacak şeklinde oluşturulmalıdır" şeklinde ifade edilmektedir. Buna göre kullanıcı kendi gizli anahtarını imza oluşturma aracının dışına çıkaramaz ya da imza oluşturma aracının dışında oluşturamaz [12,16]. Bu da sistemlerde güvenlik zaafiyeti oluşturabilmektedir.

2.2 İstemci Tabanlı İmzalar (Client Based Signatures)

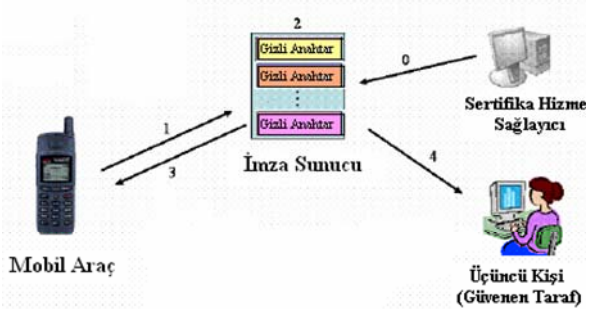
Şekil 2'de bu tür imzalama yaklaşımı verilmiştir. İstemci tabanlı imzalar (İTİ'ler), mobil cihaz içerisine ESHS tarafından onaylanmış SIM kart konulduktan sonra, SIM kart üzerindeki kripto işlemcisi kullanılarak gerçekleştirilir.

Bu imzada, imzalama süreci mobil cihazda gerçekleştirildiğinden, SIM kartın imza kartıyla (dual chip) değiştirilmesiyle ya da mobil cihaz (dual slot) içerisine akıllı kart okuyucu ilave edilerek yapılabilir. Birincisi tercih edilirse, güvenli olarak mobil ortamda haberleşmek isteyen bir kullanıcı için bu çözüm zahmetli ve karmaşıktır. Kullanıcı, imzalama işlemini gerçekleştirebilmek için mobil cihazını kapatarak SIM kartını imza oluşturma kartıyla değiştirmek zorundadır. Burada ikincisinin birincisine göre daha kolay yapılabilmekte ise de çok yönlü akıllı (smart) kart yuvasına sahip özel mobil cihazların kullanılması işlemlerin sayısını arttırdığından biraz daha karmaşık hale getirebilmektedir. Bu tür cihazların maliyetinin de yüksek olduğunu belirtmekte fayda vardır.

Kullanıcılar için en uygun çözümün, SIM kart ve güvenli imza oluşturma fonksiyonlarını ihtiva eden tek bir akıllı kartın kullanımıdır. Bu ise SIM kart içerisinde daha sonra imza oluşturma cihazı bileşenlerinin yüklenebileceği boş yer bırakılarak veya ilk kullanım anında etkinleştirilebilmesi mümkün olan imzalama fonksiyonlarının önceden yüklenmesiyle mümkün olabilir.

Kullanıcılar bu akıllı kartlar ile dokümanları kolaylıkla imzalayabilirler ve bunları kendilerinin cep telefonlarının GPRS ya da UMTS servisleri gibi iletişim hizmetleri yoluyla dağıtabilirler [11,14].

Me-imzanın ETSI standartlarında yer alan gereksinimleri sağlamak için, imzalama fonksiyonlarında güvenilir erişim kontrollerinin bazılarını sağlamak gereklidir. Mobil cihaz fonksiyonlarına erişim kontrolü olarak kullanılan alışılmış PIN yeterli olmamaktadır. Çünkü kullanıcılar araçlarını kolaylıkla kullanabilmek için telefonlarının SIM kilidini açık tutabilirler. Bu nedenle geleneksel imza kartları gibi bu kartlarda da imzalamaya özel bir PIN şifresi olması gereklidir. Bununla beraber, birçok amaç için tek akıllı kart kullanımı yeni soruların ve iddiaların ortaya çıkmasına sebep olmaktadır. Mesela, SSCD (Secure Signature Creation Device) ESHS tarafından sunulurken, SIM kart GSM operatörü tarafından sunulmaktadır. İkisinin fonksiyonlarını bir kartta birleştirmek kart üzerindeki anahtarları ve sertifikaları kimin kontrol edeceği konusundaki yeni soruları ortaya çıkarmaktadır.



Şekil 1. Sunucu tabanlı me-imza işleyişi

Şekil 2. İstemci tabanlı me-imza işleyişi

3. ME-İMZA VE AAA UYGULAMA ÖRNEKLERİ (ME-SIGN and PKI APPLICATIONS)

Me-imza henüz birkaç Avrupa ülkesinde kullanılmakla beraber yaygınlaşmasının oldukça hızlı olacağı tahmin edilmektedir. Dünyadaki GSM penetrasyonu, me-imza kullanım kolaylığı ve kullanıcıya olan düşük maliyeti, zamandan ve mekândan bağımsız imzalama işleminin gerçekleştirilebiliyor olması gibi üstünlükleri bu tahminlerin doğruluğunu desteklemektedir [13,14, 19,26].

Dünyada e-imza mevzuatının yürürlüğe girme tarihleri incelendiğinde 2002 yılına kadar birçok ülkenin yasal altyapıyı hazırladığı görülmektedir [1]. Fakat aradan geçen süre içerisinde e-imzanın beklenen seviyede yaygınlaşmasının sağlanamaması ve ülkelerde dikkati çeken mobil cihaz penetrasyonundaki artış, bazı ülkelerin me-imza'ya geçiş için çalışmalar başlatmasına neden olduğu izlenmektedir [19,26].

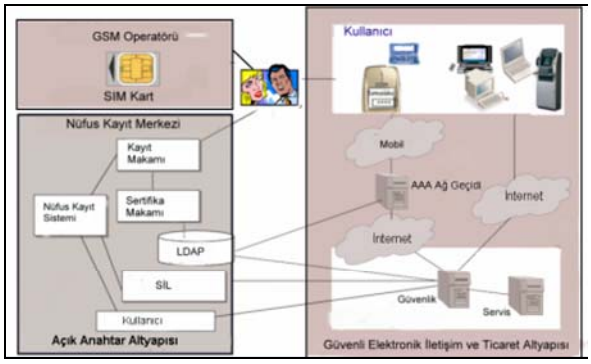
Avrupa ülkelerine göre me-imza, bilgi toplumunun gelişimi için çok önemlidir. Bu nedenle ülkelerin bazıları me-imza uygulamaları için kendi modelini ya oluşturmuştur ya da oluşturmak için başlattığı test uygulamaları devam etmektedir.

Norveç, Finlandiya, İngiltere, Polonya, İsveç, Hong-Kong, Estonya, Litvanya ve Almanya gibi ülkelerde bu konuda çalışmalar tamamlanmış, kısmen veya tamamen me-imza kullanılabilir hale gelmiştir. Me-imzanın farklı ülkelerde uygulamaları incelendiğinde ilk dikkati çeken ülke Finlandiya'dır. Bu ülkeler ve kullandıkları altyapılar aşağıda sunulmuştur.

3.1. Finlandiya (Finland)

Finlandiya Nüfus İdaresi, ülke çapında 37 adet Kayıt Makamı (KM) olan ve vatandaşlara nitelikli elektronik sertifika (NES) vermede tek yetkili ESHS'dir. Şekil 3'te bu hizmetin verilişinde kullanılan model açıklanmıştır. Bu ESHS'de adres değişikliğinin bildirilmesi ve Nüfus İdaresindeki vatandaş bilgilerinin doğrulanması gibi iki uygulama için kullanılan MAAA verilmiştir.

Me-imza'ya büyük ilgi gösteren Finlandiya Hükümeti projeyi bilgi toplumu oluşturmada en önemli projelerden birisi olarak gördüğü için desteklemiştir. Bu işlemin gerçekleştirilmesi için iki mobil operatör olan Elisa ve TeliaSoneria ile aynı proje kapsamında anlaşma imzalamıştır. Avrupa Birliği Direktifine ve Finlandiya Kanunlarına uygun olarak SIM kart üzerinde biri NES diğeri şifreleme için geçerliliği 5 yıl olan iki anahtar çifti üretilmiştir. NES'ler hem kamu hem de özel sektör uygulamalarında geçerli olabilmektedir. Mobil NES (me-imza) hizmetinden yararlanmak isteyen vatandaşlar kayıtlarını polise giderek yaptırmaktadır. Üzerinde sertifika bulunan SIM'ler Elisa'ya ait satış noktalarında satışa sunulmaktadır. Bu kartlarla yapılan uygulamalar, sadece telefon üzerinden değil bir bilgisayardaki Internet tarayıcı (browser) ile de kullanılabilmektedir. Uygulama



Şekil 3. Finlandiya'da kurulan MAAA

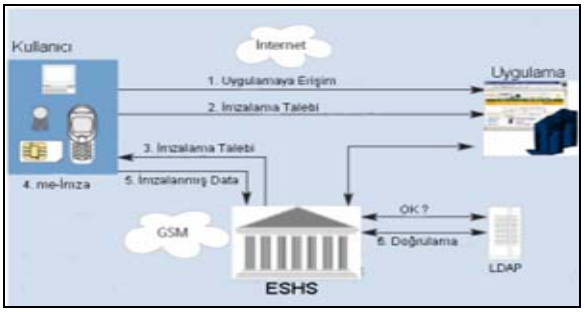
sürecinde internet üzerinde imza gerektiren bir işlem gerçekleştirildiğinde kullanıcının cep telefonuna imza gerektiğine dair bir SMS gelmektedir. Kullanıcı da PIN'ini girerek yapılan işlemi SIM kartındaki NES ile onaylamaktadır [17,19].

3.2. İngiltere (UK)

İngiltere'de Vodafone'nun altyapısını sunduğu GlobalSign'ın ihtiyaç duyulan sertifikaları sağladığı ve G&D'nin SIM kartlarının kullanıldığı ortak bir projede me-imza hizmeti verilmektedir [18].

Bu hizmette, Ticaret ve Sanayi Bakanlığına ait bir web platformu ara yüzünde, mobil telefon kullanılarak gider taleplerinin sayısal olarak imzalamasına imkân veren bir uygulama geliştirilmiş ve kullanıma sunulmuştur. Bu uygulama platformu aracılığıyla, bakanlık çalışanları kendi harcamalarını, ödemelerini ve alacaklarını kâğıt kullanmadan yapabilmektedir. Uygulamayla kullanıcıların, web platformuna logon olup kendi bilgilerini doldurmaları sonucunda oluşturulan çıktının mobil telefona gönderilerek imzalanması sağlanmaktadır. Bu işlemlerin akışını gösteren altyapı Şekil 4'de verilmiştir. Bu şekilde verilen altyapıdaki işlem basamakları aşağıda sunulmuştur [20-22]. Bunlar;

(1) Operatördeki güvenli ağ geçidinden kesin veriyi imzalamak için bir talep gönderilir.
(2) İstek, çalıştırılabilen, kullanıcıya gönderilebilen ve telefonla uyumlu hale çevrilebilen SMS bit koda dönüştürülür.
(3) İmzalama isteği uygun operatöre iletilir.
(4) Operatör bu isteği kullanıcıya iletir.
(5) Kullanıcı bu isteği kendi me-imzasıyla onaylar. Bu işlem kullanıcının imzalama PIN'ini girerek, gelen bilgiyi sayısal olarak telefonda imzalamasıyla sağlanır.
(6) İmzalanmış istek operatöre iletilir.
(7) Operatör bu imzalama işlemini uygun olan ESHS'dan doğrulatma işlemini gerçekleştirir.
(8) İmzanın doğrulama sisteminde doğrulanıp doğrulanmamasına bağlı olarak imzalama "başarılı" ya da "başarılı değil" diye bir cevap oluşturulup uygulama sunucusuna geri gönderilir.



Şekil 4. Vodafone'un İngiltere mobil açık anahtar altyapısı

Şekil 5. Küçük ölçekli uygulamalar için me-imza kullanımı

(9) Bu doğrulama işleminden sonra bu durum hizmet veren tarafa iletilir.
(10) Bu sayede uygulama yapılmak istenilen işlem güvenli olarak gerçekleştirilmiş olur.

3.3. Polonya (Poland)

Polonya'da ERA ağ operatörü Polska Telefonia Cyfrova, antlaşmaların mobil telefonlar aracılığıyla me-imzalar kullanılarak imzalanmasına imkan veren servisini uygulamaya geçirerek kendi ağında çalışan bir mobil telefon aracılığıyla imzalama işlemi gerçekleştirebilmektedir. İmza prosedürü süresince gizli kodlama anahtarı SIM kartına kaydedilmekte ve antlaşmanın onaylanma işlemi direkt olarak mobil telefondan yapılmaktadır. ERA ağında mobil telefon aracılığıyla kullanılabilir duruma gelen e-imza belgelerinin internetten ve ERA Omnix antlaşmalarının yanında direkt olarak bilgisayardan da onaylanabilmesine olanak sağlamaktadır. İmzalama sürecinde me-imzanın, mobil telefon tarafından her gönderilişinde ERA ağı bir doğrulama sertifikası oluşturmaktadır. Böylece me-imzayla imzalanmış bir antlaşma veya belge alan her kullanıcı imzanın geçerliliğini bu sertifikaları yayımlayan organlardan kontrol edebilmektedir [23].

3.4. Fransa (France)

Bu ülkede ise Orange Trust, sabit ve mobil internet hizmetinde kimlik doğrulama ve inkâr edememe hususunda hizmet veren bir mobil telefon ESHS'dir. Orange, e-imza uygulamalarını yaygınlaştırmak amacıyla, müşterilerinin taleplerini me-imzalı SIM kartları üzerinden ağ yoluyla kullanmalarını üç yıldır üç farklı ortak ile denemeye devam etmektedir. Orange, hisse senedi alışveriş işlemleri için BRED; WEB ödeme uygulamaları için COFINOGA; fon transfer onaylama uygulamaları için OBC ile test çalışmalarını devam ettirmektedir. Orange'ın geliştirdiği uygulamalarda mobil telefon otomatik ödeme aracı olarak kullanılabilmektedir. Ayrıca Fransa' da Orange ve Nestlé Grand Froid'ın başarıyla testlerini tamamladıkları mobil telefon aracılığıyla dondurma siparişi verme, Orange ve Parkeon'un ortaklaşa yaptıkları mobil telefon aracılığıyla park ücreti ödeme uygulamaları dikkat çeken me-imza uygulamalarına örnek olarak verilebilir. France Telecom'un me-imza uygulamaları için 2000 yılından bu yana kullandığı MAAA Şekil 5'de verilmiştir.

Bu altyapı ile küçük çaplı (15 Avro'nun altı) ödemelerin sabit, web ve mobil ortamlar üzerinden yapılabileceği çözümler sunulmaktadır. Bu yapıda;

(1) İlk önce Servis editöründen bir servis seçilir.
(2) Seçilen servis için w-HA platformundan bir para aktarmayı doğrulama isteğinde bulunulur.
(3) w-HA platformu bu isteği istemci operatörüne bildirir ve doğrulama istenilir.
(4) Bu aktarma isteğinin kabul edildiği kullanıcıya bildirilir.
(5) Dağıtım için servis editörüne yetki verilir.
(6) Sipariş verilen ürün kullanıcıya dağıtılır.

3.5. Estonya (Estonia)

Ülkenin en büyük ikinci şehri olan ve birçok e-uygulamaların hayata geçirildiği Tartu, m-uygulamalarda da öncülük eden şehirlerden biridir. Bunun temelde 2 sebebi vardır. Estonya %100 mobil penetrasyona sahip olması ve mobil telefonlardan her yerden her türlü web tabanlı hizmetlere erişilebilmesidir. Mobil parketme, otobüs bileti ödemesi yapma, taksi, restoran, mağaza gibi yapılan alışveriş ve harcamaları mobil ortamlardan ödeme, önemli trafik bilgileri alma, öğrenciler ve derslerle ilgili önemli bilgi transferinin içeren m-öğretmen, kayıp kişiler, çalıntı karayolu araçları gibi uygulamaları içeren m-gözetleme ve m-kütüphane bunlara örnek olarak verilebilir [24].

3.6. Çin (China)

Dünyanın en büyük nüfusuna sahip olan Çin'de, sahte kimlik kartlarıyla yapılabilecek sahtekârlıkların engellenmesi konusunda büyük önem taşıyan Kamu Güvenliği Bakanlığı'nın Ulusal Kimlik Bilgi Merkezi (NCIIS), China Mobile, Beijing GZT Teknolojileri ve diğer birimlerle ortaklaşa çalışmakta ve çevrimiçi hizmet vermektedir. Bu merkezin amacı, kamu tarafından belirlenen zamanda kimlik bilgisi doğrulama gereksinimini karşılamaktadır. 15 Eylül 2005'ten itibaren ticari veya özel kullanıcılar, NCIIS'i kullanarak kimlik bilgilerinin doğrulamasını mobil bilgi platformlarından kısa mesaj ve WAP dahil olmak üzere me-imzalı olarak yapabilmektedirler. Bu hizmetle, yönetim, finansman, ajans servisi, kargo trafiği ve e-ticaret gibi konularda sahte kimlikler kullanılarak yapılabilecek işlemler ve sahtekârlıklar engellenebilmekte, yasal olarak vatandaşların hakları korunabilmekte,

vatandaşların mobil ortam güvenliği sağlanmakta, kullanıcıların kayıpları azaltılabilmektedir [25].

3.7. Litvanya (Litvania)

Litvanya'da, Ukio Bankas telekomünikasyon firması Omnitel ile birlikte internet bankacılığı sisteminde, kullanıcıların mobil telefonlar üzerinden, özel bir telefona ihtiyaç duymadan sadece SIM kartlarını kullanarak sisteme bağlanıp banka antlaşmalarını bir PIN numarası girerek imzalayabilmektedirler. Bu işlemler, yüksek güvenlik özellikli mikro işlemcili çip kullanan banka kredi kartlarıyla aynı olan kartlar ile gerçekleştirilmektedir. Litvanya'da me-imza, kullanıcılar için en uygun sistemlerden biri olarak değerlendirildiği için Avrupa'da bazı ülkelerde tanıtılmaya başlanmıştır [26].

3.8. Norveç (Norway)

Norveç'de güvenli elektronik ticaret ve bankacılık işlemleri için birçok model kullanılmaktadır. ZebSign tarafından kısa bir süre sonra hizmet verilmeye başlanacak olan bir altyapı aşağıda tanıtılmıştır.

Bu altyapıda [27];

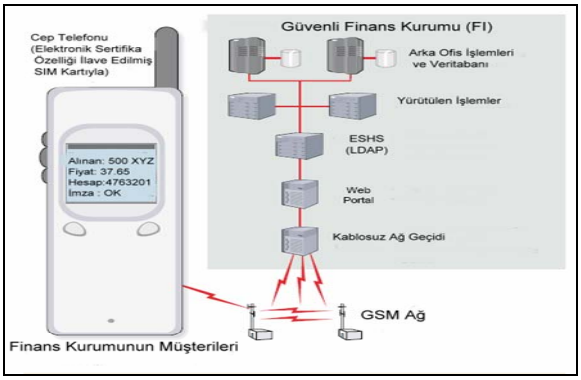
(1) Kullanıcı FI portalına bağlanır.
(2) Müşteri siparişlerini seçer.
(3) Müşteri siparişini elektronik olarak imzalar ve satın alma işlemini başlatır.
(4) Bu siparişi kablosuz ortamda alan uygulama sağlayıcı, imzalama verisini sertifika verisiyle karşılaştırır.
(5) Bu isteği sertifikayla beraber web portalına iletir.
(6) Bu isteği alan sistem FI'den bu işlemin gereğini yapar. Bu esnada gerekli belgelendirme ve kayıt işlemleri de bu aşamada tutulur.

3.9. Almanya (Germany)

Almanya'nın en büyük 4 bankası olan Commerzbank, Deutsche Bank, Dresdner Bank ve HypoVereinsbank birlikte işleyebilme kapasitesi olan bir mobil imzanın tanıtılması konusunda 2001 yılında işbirliği yaparak MoSign projesini başlatmışlardır. Projesinin amacı, Emsalsiz antlaşma numaraları tahsis etmeye dayalı mevcut prosedürler yerine e-imzaların ve AAA'lar ile mobil ortamda bağlayıcı antlaşmalar oluşturulmasına ve müşterilere mobil telefonları veya kişisel çağrı cihazlarıyla yaptıkları çevrimiçi antlaşmalarda açık ve aynı tarz standartlar sunmaktır [28] .

4. ME-İMZA, TÜRKİYE ve ÖNERİLER (M-SIGN, TURKEY AND SUGGESTIONS)

Elektronik ve mobil elektronik ortamlara tam bir bilgi güvenliğini sağlayabilmek için me-imzanın altyapısı olan MAAA'nın mevcut AAA'ya entegre edilmesiyle me-imzanın tüm dünyada kullanımının kısa sürede yaygınlaşacağı ortadadır.



Şekil 6. MAAA Norveç Modeli [27]

Bu çalışmada incelenen ülkeler genel olarak değerlendirildiğinde;

- Ülkelere has bir güven modeli bulunmadığı,
- Genellikle uygulamalara yönelik olarak farklı çözümlerin kullanıldığı,
- Bunlardan birçoğunun yıllardır test aşamasında olduğu,
- Test çalışmalarından sonra me-imza'ya geçişi erteleyen ülkelerin bulunduğu,
- Büyük uygulamalar yerine başlangıçta küçük çaplı uygulamaların geliştirilmesi ve hayata geçirilmesi gerektiği,
- Kısa sürede bir ülke güven modeli belirleme yerine ana taşların yerlerine oturduktan sonra genel bir model belirlenmesi gerektiği,
- Kullanıcıları, uygulama hizmeti verenleri, mevcut ESHS'leri, uygulama hizmet sağlayıcıları ve operatörleri mutlu edecek bir yaklaşımın belirlenmesinin uygun olacağı,
- Bu işlemlerin ülkemizde bağımsız kuruluşlarca da test edilebilmesi için gerekli girişimlerin yapılması ve buna da TK'nın öncülük etmesinin uygun olacağı,
- Uygulama servis sağlayıcı ve mobil kullanıcı arasındaki uçtan uca güvenli mobil iletişim için AAA'ya dayalı modellerin uygulanmasının faydalı olacağı
- Kullanıcıların bilgi birikimlerinin arttırılmasına yönelik olarak seminer, sempozyum ve konferansların düzenlenmesinin gerekli olduğu,
- Bu konuda ülkemizde gerek uygulama ve gerekse akademik çalışmalara ağırlık verilmesinin yerinde olacağı

değerlendirilmektedir.

Ülkemizde kullanılacak veya uygulanacak olan yapılarda; şifreleme, anahtar değişimi, me-imza, erişim kontrolü, veri doğrulama, onaylama ve onay değişimi gibi fonksiyonları gerçekleştirmek için açık şebekede sıklıkla AAA teknolojisi kullanılmasına rağmen, özellikle düşük işlem gücü ve küçük hafıza kapasitesi gibi uçtan uca mobil veri haberleşme özelliklerinden dolayı bu haberleşmeler için mobil veya kablosuz AAA teknolojilerinin ülke altyapısına uyarlanması gerektiği düşünülmektedir.

5. SONUÇLAR (RESULTS)

Bu çalışmada sunulan ülke örnekleri incelendiğinde, me-imzanın Avrupa Ülkelerinde önemsendiği ve bilgi toplumunun gelişimi ve e-imzanın yaygınlaşması için farklı çözümler üzerinde çalışıldığı görülmektedir. Bunun sonucu olarak, pek çok ülke me-imza konularında farklı uygulamalar geliştirmek için çalışmakta, kendi yapılarını oluşturmak için çaba göstermekte, herhangi bir güvenlik açığı oluşmaması için de test çalışmalarına da çok önem vermektedirler.

Ülkemizde me-imza uygulamalarının yaygınlaştırılması, geliştirilmesi ve bu konuda belirli inovasyonların oluşmasının, ülkeye katkılar sağlayacağı, ülkemize has güvenli özel altyapıların geliştirilmesine öncülük edilebileceği değerlendirilmektedir. Aşağıdaki hususlara dikkat edilerek gerekli adımların atılmasının yerinde olacağı da değerlendirilmektedir. Bunlar aşağıda başlıklar halinde verilmiştir.

- Mevcut ülke örneklerinin mutlaka detaylı olarak incelenmeli ve test edilmelidir.
- Ülke me-imza altyapısı oluşturulurken ya bütüncül bir çözüm üzerinde durulmalı veya aşama aşama küçük projelerden büyük projelere geçiş yapılabilecek bir yaklaşım üzerinde durulmalıdır.
- Me-imza'nın hukuken de geçerli olabilmesi için e-imza'da olduğu gibi me-imza kanununun çıkarılmasına yönelik çalışmalarına bir an önce başlanılmalıdır.
- Önerilecek olan yapıların mutlaka önceden pilot olarak uygulanması ve test edilmesi gereklidir.
- Ülkemizde me-imza konusunda da gündem oluşturulmalıdır.
- e-li ve m-li uygulamalarda bilgi güvenliğinin öne çıktığı ve bunun için konuya sadece e-imza veya me-imza açısından bakma yerine bilgi ve sistem güvenliği açısından bakılması gerekmektedir.
- Kullanıcılara kolaylıkla kullanılabilir yaklaşımlar sunulmalıdır.
- Kullanıcıların rekabetçi bir ortamda hizmet alabilmeleri için diğer tüm operatörlerin MAAA'yı desteklemeleri gerekmektedir.
- e-devlet uygulamalarının me-imza ile gerçekleştirilmesine yönelik projelerin hayata geçirilmesi gereklidir.
- Bankaların e-imzaya göstermedikleri ilgiyi me-imzaya mutlaka göstermeleri gerekmektedir.
- Başlangıçta yapılabilecek hataların me-imzanın gelişmesini ve yaygınlaşmasını yavaşlatacağını ve mobil ortamlara duyulacak güveni ortadan kaldırabileceği her zaman dikkate alınmalıdır.
- Devletin e-imza ve me-imza uygulamalarının yaygınlaşmasına yönelik olarak teşvikler vermesi yerinde olacaktır.
- Bu ve buna benzer konularda yapılacak olan ar-ge projeleri özel olarak desteklenmelidir.

KAYNAKLAR (REFERENCES)

1. Ş. Sağıroğlu ve M. Alkan, Her Yönüyle E-İmza, Grafiker Yayınları, Ankara, 2005
2. http://www.researchandmarkets.com/reports/c28137
3. http://www.gsmworld.com/news/statistics/pdf/gsma_stats_q2_06.pdf
4. Telekomünikasyon Kurumu Faaliyet Raporu 2005.
5. Tele.com.tr Dergisi Ekim 2006 sayısı,Cep Telefonunda Lider Çin, Türkiye Dünya 10'uncusu, Sayfa: 6
6. Mehrdad Jalali-Sohi, Peter Ebinger Fraunhofer Institute for Computer Graphics, Towards Efficient PKIs for Restricted Mobile Devices
7. ETSI TR 102 203 Standart Dokümanı
8. ETSI TR 102 206 Standart Dokümanı
9. ETSI TS 102 204 Standart Dokümanı
10. ETSI TS 102 207 Standart Dokümanı
11. Mark Gasson (University of Reading, UK), Martin Meints (ICPP, Germany), Kevin Warwick (University of Reading, UK), Future of Identity in the Information Society (FIDIS), No:507512
12. 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
13. GSM Association: GSM Statistics, www.gsmworld.com/news/statistics/index.shtml
14. H. Rossnagel: Mobile Qualified Electronic Signatures for Secure Mobile Brokerage Possible, but worth a try? In: Proceedings of the 4th Int. Cyprus Information Security Conference & Workshops; Nicosia, Cyprus 2004.
15. 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
16. Directive on Community Frame-work for Electronic Signatures, 1999/93/EC of the European Parliament of the Council, 13 December 1999.
17. http://www.cardsnowasia.com/article.cfm?id=1527
18. http://www.vodafone.hu/eng/vodafone/nemzsajtokozlemenyek/npr010312_eng.html
19. http://www.gi-de.com/portal/page?_pageid=44,123135&_dad=portal&_schema=PORTAL
20. http://www.gi-de.com/pls/portal/maia.display_custom_items.DOWNLOAD_SEEALSO_FILE?p_ID=5563
21. http://www.silicon-trust.com/pdf/secure_4/30_techno_3_1.pdf
22. http://www.highbeam.com/doc/1G1-75086272.html
23. http://www.era.pl/indekx.php?id=p_info_e&press_id=410&section=korp

24. http://www.tartu.ee/?page_id=58&lang_id=1&menu_id=6&lotus_url=/uurimused.nsf/Web/teemad/5C3CF5BE6E7B3689C22570E5004DF9E9
25. http://www.legalinfo.gov.cn/english/News/2005-09/INFO_20050911.htm
26. http://www.ub.lt/index.php/en/press/bank/a/,1097?PHPSESSID=b228a537b5e9c9e95e441a2f1017bea1
27. ZebSign ID for Secure eCommerce and mCommerce, http://www.entrust.com/resources/pdf/zebsign.pdf
28. http://www.finextra.com/fullstory.asp?id=1715
29. ITU-T Recommendation x.1122, Guideline for Implementing Secure Mobile Systems Based on PKI.
30. 5070 Sayılı Elektronik İmza Kanunu, 2004.