MOBİL ELEKTRONİK İMZA

Murad A. MOHAMMED AMIN

YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

EKİM 2007
ANKARA

Murad A. MOHAMMED AMIN tarafından hazırlanan MOBİL ELEKTRONİK İMZA adlı bu tezin Yüksek Lisans tezi olarak uygun olduğunu onaylarım.

Doç. Dr. Şeref SAĞIROĞLU
Tez Danışmanı, Bilgisayar Mühendisliği Ana Bilim Dalı

Bu çalışma, jürimiz tarafından oy birliği ile Bilgisayar Mühendisliği Anabilim Dalında Yüksek Lisans tezi olarak kabul edilmiştir.

Doç. Dr. Şeref SAĞIROĞLU

Bilgisayar Mühendisliği, Gazi Üniversitesi

Prof. Dr. İskender ÖKSÜZ

Kimya Mühendisliği, Gazi Üniversitesi

Prof. Dr. İrfan KARAGÖZ

Elektrik-Elektronik Mühendisliği, Gazi Üniversitesi

Tarih 23/10/2007

Bu tez ile G.Ü. Fen Bilimleri Enstitüsü Yönetim Kurulu Yüksek Lisans derecesini onamıştır.

Prof. Dr. Nermin ERTAN
Fen Bilimleri Enstitüsü Müdürü

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada orijinal olmayan her türlü kaynağa eksiksiz atıf yapıldığını bildiririm.

Murad A. MOHAMMED AMIN

MOBİL ELEKTRONİK İMZA

(Yüksek Lisans Tezi)

Murad A. MOHAMMED AMIN

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Ekim 2007

ÖZET

Bu çalışmada, mobil elektronik imza (me-imza) altyapıları, standartları ve me-imzadaki riskler detaylı olarak incelenmiş, güvenli imza oluşturma cihazlarının sağladığı güvenlik ile oluşabilecek muhtemel güvenlik açıkları araştırılmıştır. Dünya ülkelerinde uygulanan me-imza altyapıları ile önerilen me-imza modelleri karşılaştırılmıştır. Ülkelerin me-imza altyapıları özellikle bu konuda atılan adımlar, söz konusu ülkelerin gelecek için me-imza konusunda hedeflerine de bu çalışmada ayrıca yer verilmiştir. Mobil elektronik ortamlara yapılan saldırılar ile bu ortamlarda oluşabilecek açıklar, oluşan tehditler ayrıca bu tez kapsamında detaylı olarak incelenmiş ve alınabilecek önlemler sunulmuştur. Sonuç olarak, me-imza ve altyapısının ülkelerin gelişmesine ve işlemleri daha kolay ve güvenli yapılabilmelerine büyük katkılar sağlayacağı, yüksek seviyede bir mobil ortam güvenliği için uluslararası standartlara ve ilgili kanunların uygulanmasına, bu tez kapsamında sunulan ülke modellerinin değerlendirilmesi ve EAL4+ seviyesinde güvenlik sağlayan bir SIM kartı kullanılmasına gerek vardır.

Bilim Kodu : **912.1.011**
Anahtar Kelimeler : **Açık Anahtar Altyapısı, Mobil Elektronik İmza, Güvenli İmza Oluşturma Cihazları, Modeller, Mobil Ortamlar, Güvenlik Açıkları**
Sayfa Adedi : **115**
Tez Yöneticisi : **Doç. Dr. Şeref SAĞIROĞLU**

MOBILE ELECTRONIC SIGNATURE

(M.Sc. Thesis)

Murad A. MOHAMMED

GAZİ UNIVERSITY

INSTITUTE OF SCIENCE AND TECHNOLOGY

October 2007

ABSTRACT

In this study, the infrastructures, standards and risks on mobile electronic signature (me-sign) have been examined in detail. Security provided by the secure signature creation devices and possible security vulnerabilities have been researched. The me-sign infrastructures, and recommended me-sign models, have been compared. The me-sign infrastructures of countries, especially the steps that are taken on this issue, the targets of the countries for me-sign have also been considered. The attacks to me-sign and mobile electronic medias and the vulnerabilities and the risks encountered have been presented. As a result, me-sign and its infrastructure would be beneficial for the countries protecting information and electronic media. This will contribute to make the procedures easier and safer, allow for implementation of the laws related to the international standards for the high-level security of the mobile media, and will be beneficial to use a SIM card at EAL4+ level within the country models, presents under this thesis.

Science Code : 912.1.011
Key Words : PKI, me-sign, SSCD, Models, Mobile Platform, Security Vulnerability
Page Number: 115
Adviser : Assoc. Prof. Dr. Şeref SAĞIROĞLU

TEŞEKKÜR

Bu tez çalışmam süresince bilgi, tecrübe ve önerilerinden yararlandığım, yakın ilgilerini ve yönlendirici katkılarını gördüğüm, başta tez danışmanım Sayın Doç. Dr. Şeref SAĞIROĞLU'na, ayrıca telekomünikasyon uzmanı Sayın Demet KABASAKAL'a tezimin hazırlanmasında sağladığı kaynaklardan dolayı teşekkürlerimi sunarım.

İÇİNDEKİLER

Sayfa

Sayfa

Sayfa

Sayfa

Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

Şekil **Sayfa**

SİMGELER VE KISALTMALAR

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

Kısaltmalar	Açıklama
AAA	Açık Anahtar Altyapısı
AB	Avrupa Birliği
ASP	Uygulama Hizmeti Sağlayıcı
BSCs	Baz İstasyonu Kontrolörleri
BSS	Baz İstasyonu Alt Sistemi
BTSs	Baz Alıcı Verici İstasyonları
CEN	Avrupa Standardizasyon Komitesi
CENELEC	Avrupa Elektroteknik Standartlar Komitesi
CGA	Sertifika Oluşturma Uygulaması
CRL	Sertifika Geri Alma Listesi
CSP	Hizmet Sağlayıcısı Oluşturma
CWA	CEN Çalıştay Kararı
DH	Özet Aygıtı
Direktif	99/93/EC sayılı Avrupa Birliği Elektronik İmza Direktifi
DM	Mesaj Aygıtı
DTBSR	İmzalanacak Verinin temsili
EESSI	Avrupa Elektronik İmza Standardizasyon İnisiyatifi
eID	Elektronik Kimlik Kartı
e-imza	Elektronik İmza

Kısaltmalar	Açıklama
E-ticaret	Elektronik Ticaret
ETSI TR	ETSI Özel Raporu
ETSI TS	ETSI Teknik Özellikleri
FESA	Avrupa Denetleyici Otoritesi Forumu
FINEID	Finlandiya elektronik kimlik kartı
GSM	Küresel Mobil İletişim Sistemi
ICAO	Belçika Uluslararası Sivil Havacılık Organizasyonunun
IMSI	Uluslararası Mobil Abone Kimlik
INES	Güvenli Ulusal Elektronik Kimlik
ITU	Uluslararası Telekomünikasyon Birliği
ITU-T	Uluslararası Telekomünikasyon Birliği – Telekomünikasyon
KAAA	Kablosuz Açık Anahtar Yapısı
Kc	Oturum Anahtarı
Ki	Kullanıcı Kimlik Doğrulama anahtarı
LDAP	Hafifletilmiş Dizin Erişim Protokolü
MAAA	Mobil Elektronik İmza Altyapısı
me-imza	Mobil Elektronik İmza
MESHS	Mobil Elektronik Sertifika Hizmet Sağlayıcısı
MET	Mobil Elektronik İşlem
M-ödeme	Mobil Ödeme
möf	Mobil Ödeme Forumu
MS	Mobil İstasyonu

Kısaltmalar	**Açıklama**
MSISDN	Mobil kullanıcının telefon numarası
MSSP	Mobil Elektronik İmza Hizmet Sağlayıcısı
MT - SMS	Mobilde sonlanan - Kısa Mesaj Hizmeti
m-ticaret	Mobil Ticaret
NES	Nitelikli Elektronik Sertifika
NSS	Ağ Alt Sistemi
OASIS PKI	Yapısal Enformasyon Standartları İlerleme Kuruluşu
PDA	Cep Bilgisayarı
PKI	Açık Anahtar Altyapısı
SCA	İmza Oluşturma Uygulaması
SCD	İmza Oluşturma Cihazı
SCS	İmza Oluşturma Sistemi
SDP	Belge Sunum Bileşeni
SIM	Abone Kimlik Modülü
SM	Sertifika Makamı
SMS	Kısa Mesaj Hizmeti
SRES	İşaretlenmiş Karşılık
SSCD	Güvenli İmza Oluşturma Cihazları
SSCD PP	Güvenli İmza Oluşturma Aygıtı Koruma Profilinin
SSCS	Güvenli İmza Oluşturma Sistemi
SVD	İmza Doğrulama Verisi
TDC	Danimarka'nın En Büyük Telekomünikasyon Şirketi
TMSI	Geçici Mobil Abone Kimlik

Kısaltmalar	**Açıklama**
UMTS	Evrensel Mobil İletişim Sistemi
VA	Onay Makamı
WAP	Kablosuz Uygulama Protokolü
WSDL	Web Hizmetleri Tanımlama Dili

1. GİRİŞ

Mobil elektronik imza (me-imza), elektronik ortamlarda dokümanların imzalanması için kullanılabilen bir kimlik kartıdır. Bir başka deyişle, 5070 sayılı E-İmza Kanunu'nda tarif edilen ve ıslak imza ile eşdeğer olan e-imzanın, GSM SIM kartları kullanılarak mobil elektronik ortamlarda e-imzanın güvenle atılmasını sağlayan hizmete verilen addır.

Mobil ortamda e-imza kullanımı, Türkiye'de e-imza bilincinin yerleşmesinde çok önemli bir köşe taşı olmasının yanında GSM sektörüne sunduğu mevcut hizmetlere ve yeni servislerin geliştirilmesine de büyük bir katkı sağlayacaktır [1].

Mobil imza uygulamalarının hayata geçmesi ile dünyada bu ölçekte ortaya konulacak olan öncü teknolojik uygulamalardan biri olmasıyla da Türkiye'nin prestijine katkı sağlayacaktır. Mobil imza uygulamaları sayesinde GSM operatörü aboneleri e-imzalarını başta finansal kuruluşlar ile kamu kurumlarının uygulama sağlayıcıların (US) geliştireceği e-devlet, e-iş, e-ticaret ve m-ticaret uygulamalarında kullanabileceklerdir. Bu uygulamalarda abonelerin me-imzalarını kullanarak gerçekleştirecekleri işlemlerin kanuni bağlayıcılığı ve teknolojik olarak güvenliği en üst düzeyde olacak, böylelikle abonelerin elektronik ve mobil ortamdan sunulan servislere olan güven artacak ve bu ortamların yaygınlaşması da hızlanacaktır. US'lar açısından ise gerek mobil ortamlarda hizmet verme gerekse ticari işlemlerde mobil imza kullanımı yüksek seviyede bir güvenlik ve risk yönetimi açısından çok büyük avantajlar kazandıracaktır [2].

Me-imza, Kanunların resmi bir şekle veya özel bir merasime tabi tuttuğu hukuki işlemler ile teminat sözleşmeleri (evlilik, tapu gibi kanunen belirli bir şekilde törenle gerçekleştirilmesi şart olan ve üçüncü kişilerin kefaletini gerektiren işlemler) dışında, ıslak imza gerektiren tüm özel, kamu ve banka işlemlerinin internetten ve mobil ortamlardan yapılabilmesine imkan sağlamaktadır.

Me-imza kullanılarak her an ve her yerden kimlik kanıtlaması gereken bankacılık işlemleri ve kamudaki pek çok işlemin sıra beklemeden, bilgisayardan başından ayrılmadan veya bulunan ortamdan cep telefonu üzerinden tek bir şifre kullanılarak gerçekleştirilebiliyor olması, hayatımızı kolaylaştırmanın yanında hukuken de güvence altına alınmış olması birçok uygulama geliştirme açısından çok önemlidir. Kişisel ya da kurumsal uygulamalarda bilgilere izinsiz erişilmesi ve şifre bilgilerini ele geçirilmesi tehlikesi olmaksızın güven içinde ve hukuki dayanağa sahip bir altyapıyla gerçekleştirilmektedir.

Mobil cihazlar üzerinden gerçekleştirilen işlemlerin yaygınlaşmasının önündeki en büyük tehdit, elektronik ortamlarda olduğu gibi mobil elektronik ortamlara "güven sorunu"dur. Bu ortamlarda iş ve işlemlerin hızlı ve verimli olarak yapılabilmesinin yanında güvenli olarak da yapılmasının sağlanması gerekmektedir. Mobil ortamlarda gerçekleştirilen işlemler sırasında güvenliğin sağlanabilmesi için işlemi yapan kişinin kimliğinin onayı, kişisel bilgilerin gizliliği, verilerin bütünlüğünün sağlanması ve inkar edemezlik gibi e-imzanın vazgeçilmez güvenlik kriterlerinin sağlanması gerekmektedir. Daha önce de vurgulandığı gibi elektronik ortamlarda bilgi güvenliğinin sağlanabilmesi için vazgeçilmez bu dört temel unsur, asimetrik şifreleme teknolojisi ile desteklenen ve açık anahtar altyapısı olarak isimlendirilen bir yapı üzerinden sağlanmaktadır [3].

Bu altyapının elektronik ortamlarda oluşabilecek temel güvenlik açıklarını büyük ölçüde ortadan kaldırması, elektronik ortamlarda yapılan pek çok işlemin daha güvenli ve mobil teknolojileri de içine alan çözümler sunması gerek bu altyapıya gerekse bu altyapı üzerinden verilecek olan pek çok yeni hizmetin önünü açması, insan hayatını kolaylaştırırken iş ve işlerin yerden ve mekandan bağımsız hale gelmesini sağlamıştır.

Bu açıdan bu tez çalışması gerek bu ortamlara duyulan güvenin artırılması gerekse bu ortamlarda iş ve işlerin güvenilir olarak yapılmasında önem arz eden me-imza ve AAA ülke uygulamaları, ülke me-imza modelleri, standartlar ve karşılaşabilecek

tehdit ve tehlikelerin neler olabileceği ile ilgili geniş bir bilgi sunmak amacıyla hazırlanmıştır.

Bu tez çalışması takip eden şekilde yapılandırılmıştır. İkinci bölümde, dünyada açık anahtar altyapısı konusunda yapılan çalışmalara yer verilmiş, bu ülkelerin çalışmalarında uygulamalardan bahsedilmiş mevcut çözümlerin me-imza'ya katkıları açıklanmıştır.

Üçüncü bölümde, Avrupa Standartlar Komitesi (European Standardization Committee – CEN), Avrupa Telekomünikasyon Standartları Enstitüsü (European Telecommunications Standards Institute - ETSI) ve Uluslararası Telekomünikasyon Birliği (International Telecommunication Union - ITU) gibi kuruluşlar tarafından sunulan e-imza standartlarına yer verilmiş, bu standartların içeriği kısaca açıklanmıştır.

Dördüncü Bölümde, Avrupa Standartlar Komitesi CEN'nin sunduğu CWA 14170 adlı standardını "İmza Oluşturma Uygulamalarında Güvenlik Şartları" referans alınarak, Güvenli İmza Oluşturma Aygıtına (Secure Signature Creation Device – SSCD) yer verilmiştir. Bu sistemin me-imza'da güvenliği sağlamak amacıyla nasıl kullanıldığı gösterilmiştir.

Beşinci bölümde, Avrupa Telekomünikasyon Standartları Enstitüsü (ETSI) tarafından sunulan (ETSI TS 102 204 - Mobil Ticaret (M-COMM); Me-imza Hizmeti; WEB Servis Arayüzü) adlı standardındaki çalışma modellerini açıklanmış, bu modellerin işleyiş şekilleri sunulmuştur. Ayrıca ülkelerin me-imza uygulama modellerine yer verilmiş, modellerin mevcut standartlarda bulunan modellere göre karşılaştırılmıştır.

Altıncı bölümde ise, me-imza kullanıcılarını ve genel olarak mobil sistem kullanıcılarını ilgilendiren mobil ortamların kullanımında karşılaşabilecek tehditler incelenmiştir. Bu çerçevede GSM sisteminde güvenli haberleşme için kullanılan şifreleme algoritmaları araştırılmış, olası saldırılar incelenmiş, me-imza uygulaması esnasında karşılaşabilecek tehditler gözden geçirilmiş, mevcut standartlarda bulunan

uçtan uça güvenlik hususundaki öneriler dikkate alınarak, mevcut tehditler ve açıklar değerlendirilmiştir.

Yedinci bölümde, bu çalışma sonucunda elde edilen bulgular ile me-imzaya ilişkin dünya uygulamaları, modeller, standartlar, mobil ortamlarda açıklar ve tehditler genel olarak değerlendirilmiş, sonuç olarak karşılaşılabilecek tehditlerin ortadan kaldırılması için öneriler sunulmuştur.

2. DÜNYADA ELEKTRONİK İMZA VE MOBİL ELEKTRONİK İMZA ÇALIŞMALARI

II. Dünya Savaşında şifreleme yaklaşımlarının çok önemli rol oynaması ve yaşanmış acı tecrübeler, şifre bilimine olan ilgiyi ve önemi arttırmış ve yeni şifreleme yaklaşımları geliştirmek için büyük çabalar harcanmıştır.

Savaş sonrasında, hem askeri ve devlet güvenliğini sağlamak hem de diğer ülkelerin haberleşme bilgilerini ele geçirmek ve kriptografik standartların gelişmesini sağlamak amacıyla Amerika'da Ulusal Güvenlik Merkezi kurulmuştur. 1960'larda, bilgisayarların gelişmesi ve iletişim sistemlerinin kullanımının yaygınlaşmasıyla, konuya özel sektörün ilgisi artmıştır. 1970'de IBM ile başlayan çalışmalar, ABD Federal Bilgi İşleme Standardının (USA Federal Information Processing Standard) benimsenmesiyle, DES (Data Encryption Standard) sınıflandırılmamış bilginin şifrelenmesinde bir standart olarak kabul edilmiştir. Bu standart, bugün için çok güvenli olmasa da bankacılık, e-imza ve e-ticaret alanlarında hala kullanılan bir şifreleme tekniğidir.

1976 yılında Hellman ve Diffie tarafından açık anahtarlı şifreleme yaklaşımı teorik olarak geliştirilmiştir. Bundan iki yıl sonra, Rivest, Shamir ve Adleman isimli üç bilim adamı, ilk açık anahtarlı şifreleme yaklaşımını pratik olarak gerçekleştirmişlerdir. Geliştirenlerin adlarının ilk harflerinden oluşan bu yaklaşıma RSA (Rivest, Shamir ve Adleman) şifreleme metodu adı verilmiştir. Bu yaklaşım, büyük asal tamsayı çarpanlarının etkileşmesi gibi zor bir matematiksel temele dayanmaktadır. Daha sonraları, bu alanda birçok önemli ve yeni bir ilerlemeler olmuşsa da bunların hiçbiri RSA sisteminin güvenilirliğini bozamamıştır.

1990'da Lai ve Massey tarafından geliştirilen Uluslararası Veri Şifreleme Algoritması (IDEA) ve 1991 yılında Zimmerman tarafından geliştirilen PGP (Pretty Good Privacy) ile şifreleme biliminde büyük gelişmeler kaydedilmiştir. Açık anahtarlı şifre bilimi, bugün için sayısal ortamda bilgi güvenliğinin sağlanmasında

büyük kolaylık sağlayacak olan e-imza ortamının ve altyapısının geliştirilmesine büyük katkılar sağlamıştır.

DES'nin güvenlik ihtiyaçlarını tam olarak karşılayamaması üzerine yeni standartların aranmasına girişilmiş ve yapılan bir yarışma sonucunda Rejindal algoritmasının bu beklentilere cevap verebileceği tespit edilmiştir. Daha sonra AES (Advanced Encryption Standard) adını alan bu algoritma, 21. yüz yılda kullanılabilecek bir güvenlik standardı olarak kabul edilmiştir.

2.1. Dünya Ülkelerinde E-İmza Uygulamaları

Bu tez çalışması kapsamında Avusturya, Finlandiya, Fransa, Portekiz, İspanya, İsveç, İsviçre, Belçika, Çek Cumhuriyeti, Danimarka, Estonya, Almanya, Macaristan, İtalya, Malta, Norveç, Polonya, Lüksemburg, Çin, Kuveyt, Bulgaristan, Slovakya, Slovenya, İrlanda, Tunus, Ürdün, Bahrin, Mısır ve Türkiye incelenmiş ve bu ülkelere ait bilgiler aşağıdaki alt başlıklarda sunulmuştur

2.1.1. Avusturya

Avusturya Maliye Bakanlığı ve Avusturya Merkez Bankası Mayıs 1999'da Avusturya Güvenli Bilgi Teknolojisi Merkezini (A-SIT) kurdu. Bu merkez, özellikle vatandaşlık kartının (Bürgerkarte) tanıtılmasını ve kriptografik yöntemlerin değerlendirilmesi dahil resmi makamlara, ekonomiye ve vatandaşlara bilgi güvenliği alanında uzmanlık geliştirme görevine sahip kar amacı gütmeyen bir kuruluştur. Ek olarak A-SIT e-imzaların onaylanmasını sağlamak üzere yetkilendirilmiş ilk ve tek Avusturya organizasyonudur [7].

Avusturya hükümeti 2006 yılı itibariyle Avusturya vatandaşları tarafından kullanılacak olan yeni elektronik pasaportu sunmuştur. Pasaportlar belgenin iç kapak sayfalarının birine gömülü durumda bir mikroçip içermektedir. Bu mikroçip içerisinde, pasaportta yazılı şekilde bulunan verilerin neredeyse tamamı ile hamilinin yüz taramasını da bulunmaktadır. Bu mikroçipler ayrıca kopya koruma

mekanizmalarına, e-imzaya ve üçüncü tarafların pasaport bilgilerine erişmelerini imkansız hale getiren şifreleme mekanizmalarıyla donatılmıştır. Vatandaşlar açısından yeni belgenin çıkartılması çok fazla değişiklik yaratmaması için mevcut geçerli pasaportlar son kullanım tarihlerine kadar iade edilmek zorunda değildir [8].

Bu ülke, Ocak 2005'te vatandaşlarına, banka kartlarının vatandaşlık kartıyla entegre edilmesi için imkan sunan ilk ülkedir. Maliye Bakanlığı ve banka kartı tanzim eden Europay kuruluşu arasındaki bir anlaşmayı müteakiben, "vatandaş kartı" işlevi Avusturya'da tanzim edilen Maestro banka kartlarına dahil edilmiştir. İsteğe bağlı olan bu hizmet ile (banka kartının mikroçipinde saklanan e-imza) vatandaşların kendilerini çevrim içi olarak güvenli bir şekilde tanımlamasına izin vermektedir [7].

2.1.2. Finlandiya

Finlandiya Avrupa'da elektronik kimlik kartını (FINEID) sunan ilk ülkedir. İlk kart 7 Aralık 1999'da Fin Başbakanlığına e-devlet uygulamalarının başlatmasının yolunu açmıştır. Bu kart AAA ve sertifikalara dayalıdır. Kimlik kartı herhangi bir Finlandiya vatandaşına ya da kalıcı yerleşimcisine verilmektedir. FINEID projesi altyapının oluşturulmasını, açık ve güvenli olmayan ağlarda resmi işlemleri gerçekleştirmenin güvenli vasıtalarını sağlamayı hedeflemektedir [9].

Finlandiya kendi bünyesinde e-imza ve kriptoloji konusunda çalıştırmış olduğu uzmanlara ETSI, FESA ve AB Komisyonundaki uzmanlara göre çok daha fazla güvendiği için bu kuruluşlara üye olsa dahi kendi ülkesinin ihtiyaçları ve eksiklikleri doğrultusunda bağımsız karar alabilmekte ve uygulayabilmektedir. Uluslararası teşkilatlardan bağımsız olarak hareket edebilme ve karar verebilmeleri ülke açısından ayrı bir öneme sahip olduğu değerlendirilmektedir.

FESA çevrelerinde SHA-1'in güvenilirliği konusunda duyulan endişeler üzerine söz konusu teknik alanda yapılan çalışmalar yakından takip edilmekte olup, muhtemelen yakın bir gelecekte 128 bit'lik SHA–1 yerine İtalya'da olduğu gibi 256 bit'lik versiyonunun kullanılması başlandığı gözlenmektedir. Bu çerçevede mevzuatta

gerekli değişikliğin yapılmasının yakın bir süreçte gündeme gelebileceği belirlenmektedir [10].

2.1.3. Fransa

CNIE (Carte Nationale d'Identité Electronique) olarak adlandırılan elektronik kimlik kartı planları, INES programının (Identification Nationale Electronique Sécurisée) bir parçası olarak ilk olarak 2003'te açıklanmıştır.

Güvenli Ulusal Elektronik Kimlik (INES) projesi 11 Nisan 2005'te resmi olarak onaylanmıştır. INES projesi diğer pek çok şeyin yanı sıra kimlik kartlarının ve pasaportlarının talep etme işlemlerini birleştirecek, güvenli kılacak ve basitleştirecek, kimlik belgelerinin yönetimini iyileştireceği ve vatandaşlara e-hükümet ve e-ticaret hizmetlerinin e-imza destekli olarak verilmesini sağlayacağı belirlenmektedir [11].

2.1.4. Portekiz

Yeni Portekiz Kimlik Kartı (*Cartão do Cidadão*) üzerinde yapılan ilk testlerin sonuçları 8 Mart 2006'da resmi olarak açıklanmıştır. *Cartão* bir kimlik kartı üzerinde görünen bütün bilgiler ile kart hamilinin elektronik olarak tanımlanması ve doğrulanması için gereken e-imzayı içeren bir elektronik çip içermektedir. Dolayısıyla yeni kartın, çok sayıda çevrim içi olarak kullanılabilen idari hizmetlere ulaşım sağlayan bir elektronik kimlik kartı olacağı, mevcut diğer kartlarla birleştirilerek ve soysal güvenlik kartı, kamu sağlığı hizmeti kartı, vergi kartı, seçmen kartı ve elbette geçerli kimlik kartı olarak kullanımını sağlamıştır [12].

2.1.5. İspanya

İspanya Hükümetinin en yakın tarihli e-hükümet stratejisi, "Plan Conecta" olarak adlandırılan ilk sürümü Eylül 2004'te sunulmuştur. AAA ve Elektronik Kimlik araştırmaları, biri doğrulama diğeri ise imzalama olmak üzere iki sertifika içermektedir: Bu kart ile hizmet 2006 Mart ayından itibaren verilmeye başlamıştır.

Bu elektronik kart, elektronik belgelerde kullanıcı güvenliğini arttırmayı ve özel hayatlarını korumayı hedefleyen bir elektronik doğrulama ve imza sistemi içermektedir. Polis Genel Müdürlüğü de ayrıca İspanyol vatandaşlarının yeni kartlar hakkındaki bilincini arttırmak üzere "Identíficate con él" (Kendini tanıt) sloganı ile bilgilendirme kampanyası yapmaktadır [8].

2.1.6. İsveç

Elektronik kimlik kartları, SM olarak hizmet veren İsveç Posta İşletmesi tarafından satılmaktadır (Posta'nın SM işletmesi Eylül 2003'te telekom şirketi TeliaSonera tarafından satın alınmıştır). İsveç Kamu Yönetimi Kurumu ve elektronik sertifika hizmet sağlayıcıları (ESHS) arasında imzalanan bir çerçeve sözleşmesine göre, yazılıma dayalı elektronik kimlikler (özellikle en büyük İsveç bankaları tarafından geliştirilen Banka ID) de ayrıca belirli e-hükümet hizmetleri için kullanılabilmektedir. Gelecekte, hükümet biyometrik tanımlayıcıları içeren resmi bir elektronik kimlik kartı tanıtmak üzere planlar yapmaktadır [13].

2.1.7. İsviçre

E-imza Kanunu İsveçre Temsilciler Meclisi tarafından 02.12.2003 tarihinde onaylanmış ve 2005'te yürürlüğe girmiştir. Elektronik bir imza ile mühürlenmiş sözleşmeler yazılı imzalarla aynı yasal statüye sahip olacaktır. Elektronik işlemin tarafları onaylı SM'dan elde edilmiş bir e-imza kullanılarak çevrim içi olarak sözleşmeleri imzalayabilecektir. Bununla birlikte vasiyetnameler ya da binaların satış senetleri gibi belirli resmi belgeler hala geleneksel şekilde imzalanmak zorundadır.

İsviçre'de farklı alanlarda e-imza kullanımının yaygınlaşmasının kısa sürede gerçekleşmesi beklenmektedir [8].

2.1.8. Belçika

Belçika eID (elektronik kimlik) kartı, kart hamilinin kişisel verilerini ve uzaktan doğrulamayı sağlayan elektronik bir sertifikayı saklayan gömülü bir mikroçip içermektedir. 2003-2004'te ülkenin kalan 578 belediyesi artık 2009'un sonuna kadar geçişi tamamlamak zorundadır. Bu süreden sonra tüm Belçikalı vatandaşların elektronik kimlik kartına sahip olması gerekmektedir. Halihazırda 2005'te Belçika elektronik kimlik kartı ile uyumlu olan bir dizi uygulama ve hizmet kullanılmaktadır. Çevrim içi vergi beyannameleri, onaylı e-posta, resmi belgelerin çevrim içi talebi, internet banka hizmetleri ve e-kütüphane gibi hizmetler bu çerçevede sunulmaktadır. Kasım 2004'te Belçika Uluslararası Sivil Havacılık Organizasyonunun (ICAO) tavsiyelerine uyan elektronik pasaportlar tanzim etmeye başlayan dünyadaki ilk ülke olmuştur. Biyometrik pasaport, hamilinin yüz görüntüsünü bir mikroçip içerisinde içermektedir [8,14].

2.1.9. Çek Cumhuriyeti

Temmuz 2006'da vatandaşlarına güvenilir ve güvenli e-Hükümet hizmetleri sağlama vaadinin bir parçası olarak Çek Cumhuriyeti e-imza ve e-mühür doğrulama hizmetlerini tanıtmıştır. Çek BT Bakanlığı bütün kamu kuruluşlarına hükümet makamlarının kanunun görev kıldığı gerekleri – sunulan bilgileri elektronik formda kabul etmek, belgeleri elektronik adreslere teslim etmek, e-formu vs. şeklinde idari eylemleri gerçekleştirmek vs. gibi - karşılayabilmesi için etkili bir doğrulama sistemi sağlamak istemektedir. Vatandaşlar, gerçek ve tüzel kişiler aynı teknolojiye erişime sahip olmalıdır. Şu anda, kurumlar temel olarak mali yönetimler ve diğer idari işlemler için kullanılmaktadır.

Temmuz 2006'da bir sertifika makamı olan První Certifikaèní Autorita ve Çek Posta İdaresi e-imzalar ve elektronik mühürler tanzim etmekle görevlendirilmiştir. Bu kurumlar basit *PostSignum* VCA sertifikası ve nitelikli *PostSignum QCA* sertifikası dahil olmak üzere pek çok tipte doğrulama sertifikaları tanzim edebilmektedir. Çek Çalışma ve Sosyal İşler Bakanlığı şu anda önemli miktarda çipli kart kullanan tek

devlet organizasyonudur. Bakanlık elektronik kimlikleri temel olarak bakanlığın bilgi sistemine erişim ya da bakanlık içerisinde gizli bilgilerin korunması için kullanılmaktadır [7].

2.1.10. Danimarka

Şubat 2003'ten bu yana, Danimarka hükümeti kullanıcı doğrulaması için vatandaşlarına "ücretsiz e-imzalar" sağlamaktadır [8].

E-imza projesi, kamu sektöründe artan modernizasyon ve gelişim taleplerini karşılamak üzere başlatılan Danimarka Elektronik Hükümet Programının bir parçası olarak başlatılmıştır. E-imza projesinin amacı AAA'ya dayalı olarak açık ölçeklendirilebilir bir güvenlik altyapısı oluşturmak ve e-imzaların vatandaşlara, şirketlere ve kamu kuruluşlarına etkili bir şekilde tescil edilme prosedürlerini ve dağıtım mekanizmalarını tespit etmektir. E-imza projesi Bilim, Teknoloji ve Yenilik Bakanlığı ile Danimarka'nın en büyük telekomünikasyon şirketi olan TDC arasında bir kamu / özel ortaklığı olarak organize edilmektedir. TDC e-imzaları oluşturmak, sunmak, korumak ve yönetmek ile sorumlu bir SM olarak hizmet vermektedir [7].

2.1.11. Estonya

Estonya 2003'te bir bütün olarak Avrupa'daki e-hükümet gelişimi açısından en gelişmiş ülkelerden biri olarak görülmektedir. Estonya Ocak 2002'de ulusal kimlik kartları tanzim etmeye başlamıştır. Bu kart Estonya'nın E-İmza Kanunu'nun gereklerini yerine getirmektedir. Estonya vatandaşları ve 15 yaşın üstündeki bütün kalıcı ikametli yabancılar bu kartı kullanmak zorundadır. Bu kartın vatandaşları ve ikamet edenleri tanımlamak için ana belge olması amaçlanmaktadır ve işlevleri; işletme, hükümet ya da özel iletişimde kullanılabilmesi olarak tanımlanmıştır. Vatandaşlık ve Göçmenlik Kurulu tarafından tanzim edilen bu kartlar (AB içerisinde) tanımlama ve seyahat belgesi olarak 10 yıl süreyle geçerlidir. Fiziksel tanımlama belgesi olmasına ek olarak, bu kartları güvenli doğrulamayı kolaylaştıran

gelişmiş elektronik işlevlere ve kamu ve özel çevrim içi hizmetler için yasal olarak bağlayıcı e-imzaya sahiptirler [8,10].

2.1.12. Almanya

Almanya Hükümetin Direktifinde, kamu-özel "İmza İttifakı" Almanya'da e-imzaların kullanımını artırma hedefiyle 3 Nisan 2003'te Berlinde kurulmuştur. Ortak bir deklarasyonda, ittifak ortakları özellikle uygulama ve ürünlerin teknik standartları, orta güvenlik standartları ve gelişmiş ve nitelikli e-imzaların kullanımı üzerinde mutabık kalmıştır.

E-kart stratejisi 9 Mart 2005'te Alman Federal Hükümeti tarafından duyurulmuştur. Bu strateji gelecekteki elektronik sağlık sigorta kartının ve kimlik kartının vatandaşların e-hükümet hizmetlerine kolaylıkla ulaşmasını sağlamak üzere tek bir evrensel belgeye birleştirilmesini önermektedir. E-kart stratejisi, kullanıcı tanımlama, sosyal güvenlik tanımlama ve sağlık sigorta hizmetleri alanlarında bir dizi e-hükümet Direktifi için ortak bir stratejik çerçeve sağlamayı hedeflemektedir. Ortak strateji (e-sağlık sigortası kartı, eID kart, iş kartı gibi) farklı federal e-kart Direktifleri ile sosyal güvenlik ve vergi işlemleri alanlarındaki önemli veritabanlarına ve hizmetlere erişimi koordine etmektedir. Diğer şeylerin yanı sıra, e-hükümet hizmetlerinin geliştirilmesini, alınmasını artırmakta, verimi yükseltmekte ve maliyetleri en düşük düzeye çeken orta standartları tanımlamaktadır [8].

E-Hükümet uygulamalarının tanıtılmalarını ve kamu kurumları, sanayi ve finansman sektörü tarafından kullanılmasını desteklemek için, Almanya'da (TeleTrusT), güvenilir İnformasyon ve Haberleşme tekniğinin ilerlemesi konusunda çalışan bir kuruluştur. T7 grubuyla birlikte başka platformlarda kullanılabilir çözümlerin geliştirilmesi ve test edilmesi için temel öğeler sunulmuştur. Çalışma grubu, AAA'larının kamu için koordine edilebilir bir foruma dönüştürülmesi için çalışmalar yapılmaktadır. Kuruma müracaat eden bir şirketin halihazırda veya bir yıllık bir süre içerisinde akredite olmuş bir SM olmasını gerektirmektedir [14].

2.1.13. Macaristan

Macar İdari Usul Kanunu ve buna bağlı tebliğler farklı kamu idaresi hizmetleri için tanımlama ve doğrulama süreçlerini tanımlamaktadır. Şifre ile tanımlama ve elektronik sertifika ile tanımlama olmak üzere iki farklı durum tanımlanmaktadır [8].

Temmuz 2006'da, Macaristan yeni bir e-imza uygulamaları başlatmıştır. Netlock KFT, "başkalarına sertifika verme" hakkını yani Macaristan'da geçerli e-sertifikalar tanzim edebilecek yabancı elektronik sertifika sağlayıcılarına lisanslar tanzim etme hakkını almıştır. Ulusal İletişim Kurumu uygun tescil emrini tanzim ettiğinde, Netlock sivil hizmetlerde kullanılabilecek elektronik sertifikaları tanzim edecek ilk şirket haline gelecektir [15].

2.1.14. İzlanda

Elektronik tanımlama, vatandaşlara elektronik hizmetleri sağlamada kilit rol oynayacağı değerlendiğinden yüksek bir önceliğe sahiptir. İzlanda hükümetinin 2004 – 2007 bilgi toplumu politikası 2007 yılı sonuna kadar elektronik sertifikaların kullanımının yaygınlaştırılacağı belirlemektedir [8].

2.1.15. İtalya

İtalya'da e-hükümet hizmetlerine ulaşım için 13,1 milyondan fazla akıllı kart değerlendirilmiştir. Buna ilave olarak Ulusal Hizmetler Kartı (NCS) birimi 3 milyon yeni kart üreterek 9,3 milyon bu hizmetleri yürütmektedir. Kullanıcılara e-hükümet hizmetlerine güvenli bir şekilde ulaşmasını sağlamak üzere tasarımlanmış olan NSC kartı, kişinin fotoğrafını içermemesi haricinde aynı özelliklere sahip İtalyan e-Kimlik kartına benzemektedir [8].

2.1.16. Malta

Malta elektronik kimlik kartı dağıtımı Mart 2004'te başlamıştır ve bir kişinin kimliğini gerektiren çevrim içi hizmetlere güvenli bir şekilde erişilmesini sağlamak amacıyla üretilmiş bir karttır. Kullanıcılara esneklik ve kolaylık sağlamanın yanında katma değerli e-hizmetlerinin güvenli bir şekilde sağlanmasını sağlamaktır. Hükümet ayrıca kişisel ve hassas verilerin iletilmesini gerektiren çevrim içi idari prosedürler hakkında genel olarak halk arasındaki şüpheciliği azaltmaya yardımcı olmasını beklemektedir.

Malta Pasaport Ofisi Ağustos 2005'te vatandaşların herhangi bir yerde ve zamanda pasaport almaya müracaat etmelerini sağlayan bir çevrim içi hizmet vermeye başlamıştır. Pasaport Ofisinin web sitesinde bulunan çevrim içi hizmet ile geçerli bir Malta kimlik kartının hamili 18 yaşın üzerindeki herhangi bir Malta vatandaşı tarafından kullanılabilir. Hizmeti kullananlar daha önceden –Pasaport hizmetine kayıtlı olmalı ve e-Hükümet elektronik kimlik kartına (eID) sahip olmalıdır [8].

2.1.17. Norveç

Norveç'te e-imzada kullanılan algoritmalara ilişkin bir düzenleme yapılmamıştır ve herhangi bir standardın uygulanması hukuken zorunlu değildir. Sadece sertifikayı veren ESHS'nın açık adının sertifikada yer alması hukuken yeterli sayılarak her türlü sorumluluk sertifikayı veren ESHS'ya bırakılmıştır. Bu ilkeden hareketle Norveç'te bazı bankalar ESHS gibi sertifika verebilmektedir. Ülkede birisi nitelikli diğeri ise niteliksiz elektronik sertifika veren iki adet ESHS mevcuttur. Bu ESHS'ler kendilerinin yayımladıkları sertifikalardan dolayı meydana gelebilecek maddi zararı karşılamakla yükümlüdür. Me-imzaya ilişkin hizmetlerin Telenor ASA firması tarafından sunulmakta olup ve sertifika hizmetleri ise bir ESHS olan ZebSign AŞ. Tarafından verilmektedir. Norveç'te vatandaşlar akıllı kartları, bağımsız kimlik (keycard) olarak kullanabildiği gibi mobil cihazdaki SIM kartlarının içinde de kullanabilmektedirler. Bunun için kullanıcı bir posta hizmetine veya bir mobil cihaz satış noktasına geçerli bir kimlik (ulusal kimlik beraberinde banka kartı) sunmak

zorundadır. Kayıt bilgileri bu merkezlerde, merkez nüfus kayıtlarından ve telekom firmasının müşteri veritabanından doğrulandıktan sonra sistemde bir müşteri profili oluşturulmaktadır. Bu hizmetler, bir AAA içerisinde (bir SIM tarayıcısı kullanılarak) tek girişlik bir şifre mobil cihazına gönderilir. Bu aşamadan sonra SIM kartta bir anahtar çifti oluşturulur. Kullanıcı, kişisel anahtarı başlatabilmek için bir PIN kodu belirler ve açık anahtarını, sertifika sürecinin tamamlanabilmesi için gizli anahtarı ile imzalayarak ESHS'ya gönderir. Bundan sonra sertifika SIM karta geri gönderilir ve MAAA kullanıma hazır hale getirilmektedir. Artık finansal antlaşmaların doğrulanması ve imzalanması esnasında me-imza kullanabilmektedir [3,17].

2.1.18. Polonya

Polonya'da 2000 yılında yürürlüğe giren E-imza Kanununda, Direktif'te yer alan taraflar arasındaki ilişkiler düzenlenmemiş sadece e-imza ve güvenli e-imzaya ait düzenlemeler sunulmuştur. Polonya'da kamusal hizmetlerde e-imza kullanımı çok yaygın değildir. eID kartlarda ya da sağlık sigorta kartlarında da e-imza kullanımı mümkün olmadığından e-imzanın yaygınlaşması beklenen seviyede olmamıştır. Ekonomi Bakanlığı'nın nitelikli ve niteliksiz sertifikaların yönetilmesinden sorumludur, ancak bu sorumluluğun bilgiden sorumlu İçişleri Bakanlığı'na kaydırılması planlamaktadır. Ekonomi Bakanlığı'nın mobil hizmeti de içeren pazar yönetiminden, denetiminden ve Polonya Milli Bankası ile birlikte NES sağlayıcılarının milli kaydının yürütülmesinden sorumludur. NES'in güvenli e-imzanın doğrulanması için kullanılmakta, güvenli e-imza'ın, güvenli imza oluşturma cihazı ile oluşturulması ve bu araçların ITSEC v1.2 E3, FIBS PUB 140 level3, ISO/IEC 15408 EAL4+ standartlarından birine uyması gerekmektedir. SIM kartların hepsinin bu standartlara uymadığı için me-imzanın hepsi güvenli kabul edilememekte, bu nedenle de SIM kartlarda hem nitelikli, hem de niteliksiz imzaların oluşturulabileceği, konuyla ilgili birçok standart arasında CWA 14355 standardı göz önünde bulundurulmaktadır [3].

Polonya'daki düzenleme çalışmaları Direktif ve ona takiben Avrupa Komisyonu direktifilerine ve gerekli standartlara uyum gösterdiği vurgulanarak yapılacak

düzenlemelerde Avrupa Komisyonunun ve FESA'nın direktifilerinin göz önünde bulundurulmasının uygun olacağı yönünde tavsiyede bulunulmaktadır. Polonya'da ERA ağ işletmeci Polska Telefonia Cyfrova, antlaşmaların mobil cihazlar aracılığıyla me-imza kullanılarak imzalanmasına imkân veren hizmetini uygulamaya geçirerek kendi ağında çalışan mobil cihazlar aracılığıyla imzalama işlemi gerçekleştirebilmektedir. İmza prosedürü süresince gizli kodlama anahtarı SIM kartına kaydedilmekte ve antlaşmanın onaylanma işlemi direkt olarak mobil cihazdan yapılmaktadır. ERA ağında mobil cihaz aracılığıyla kullanılabilir duruma gelen e-imza belgelerinin internetten ve ERA Omnix antlaşmalarının yanında direkt olarak bilgisayardan da onaylanabilmesine olanak sağlamaktadır ve-Posta mesajlarının, yapılacak vergi bildirimlerinin imzalanması da bu yolla kolay bir hale gelmektedir. İmzalama sürecinde me-imzanın, mobil cihaz 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 mekanlardan kontrol edebilmektedir [3,18].

2.1.19. Lüksemburg

2000 yılındaki E-Ticaret kanunu içerisinde normal ve nitelikli olmak üzere iki şekilde e-imza tanımı yapılarak geçerli hale getirilen Lüksemburg E-İmza Hizmetlerinin ve Uygulamaları hükümet tarafından desteklenerek pazarın büyümesinin teşvik edilmesinin gerekli olduğu kaydedilmektedir. Halihazırda e-imzanın eID kart olarak kullanımı için çalışmalar devam etmektedir.

Sunucu tabanlı imza kullanımına dayanan bir MAAA'yı kurmayı planlanmaktadır. Bu sunucuların, herhangi bir elektronik dokümanı güçlü bir kimlik doğrulamadan sonra kullanıcıların yerine imzalayacakları, kimlik doğrulamanın mobil cihaz aracılığıyla yapılabileceği belirtilmektedir [3,7,8].

2.1.20. Çin

Çin'de, sahte kimlik kartlarıyla yapılabilecek sahtekarlıkların engellenmesi konusunda önemli rolü olan Kamu Güvenliği Bakanlığı'na bağlı Ulusal Kimlik Bilgi Merkezi (NCIIS), China Mobile, Beijing GZT Teknolojileri ve diğer birimlerle ortaklaşa çalışarak çevrim içi hizmet vermektedir. Bu merkezin amacı, kamu tarafından belirlenen zamanda kimlik bilgisi doğrulama gereksinimini karşılamaktır. 15 Eylül 2005'ten itibaren ticari veya özel kullanıcılar, Ulusal Kimlik Bilgi Merkezi'ni kullanarak kimlik bilgilerinin doğrulamasını mobil bilgi platformlarından kısa mesaj ve WAP dahil olmak üzere me-imzalı olarak yapabilmektedirler. Bu hizmetle, yönetim, finansman, ajans hizmeti, kargo trafiği ve e-ticaret gibi konularda sahte kimlikler kullanılarak yapılabilecek işlemler ve sahtekarlıklar engellenebilmekte, yasal olarak vatandaşların hakları korunabilmekte, vatandaşların mobil ortam güvenliği sağlanmakta, kullanıcıların kayıpları azaltılabilmektedir [82].

2.1.21. Slovenya

%70'lik pazar payıyla Slovenya'nın önde gelen mobil işletmecilerinden biri olan Mobitel, mobil portalı olan Planet altında işlem görecek ve e-bankacılık, e-devlet ve diğer e-servisleri destekleyecek olan Valimo Validator ile MESHS kurarak me-imza hizmetleri sağlayabilmek için SIM kart üzerinde imzalamanın gerçekleştirilebilecek, ETSI standartlarına uygun pilot çalışmalar yapmaya devam etmektedir. Gemolta ve Oberthur'un USIM kartları, OTA1 platformu için SmartTrust, AAA için Valimo ürünleri ve mobil iletişim için Mobitel'in ürünleri kullanılmaktadır. E-devlet, e-bankacılık, e-vergi gibi uygulamaların me-imzayı destekleyeceği ve personel bulunmasını gerektiren çağrı merkezlerinin kullanıcılara cihazla hizmet verme gibi yenilikçi bir MAAA kullanıcısı olacağı tahmin edildiği kaydedilmektedir. Test çalışmalarındaki işlem basamakları şöyle sıralanabilir. Kullanıcının mobil cihazına kimlik doğrulayabilmek için sayısal imza isteğine dair bir yasal sorgulama mesajı gelir. Bu hizmet, SIM Toolkit ve OTA teknolojisiyle desteklendiği için kullanıcı kendi mobil cihazından sayısal imzasını seçer ve özel bir PIN kodunu girerek gönder butonuna basar. Bu işlem pazardaki her mobil cihaz tarafından pratikte

desteklenebilir. Ülkede resmi olarak tanınan ve NES yayımlayan dört ESHS, bir AAA kurmuş olup halen sayısal sertifika kullanıcılarının sayısı yaklaşık 200.000 civarındadır. MAAA sistemi henüz tam oluşmadığı için halihazırda me-imza kullanıcısı da mevcut değildir. Me-imza kullanıcı sayısının 2007 yılının sonuna kadar 20.000 – 100.000 kullanıcıya ulaşacağı tahmin edilmektedir. MAAA kullanıcısı olarak e-devlet ve e-bankacılık hizmetlerinin ilk öncü uygulamalar olması beklenmektedir. Ayrıca şu ana kadar yapılan çalışmalarda yasal olarak büyük bir sıkıntı yaşanmadığı, devletin büyük bir desteği olmasına rağmen teknik olarak ilk kullanıcıların işlevleri gerçekleştirebilmeleri için ihtiyaç duydukları USIM kartların oluşturulması ve kullanıcılara ulaştırılmasında sıkıntı yaşadıkları belirtilmektedir. Slovenya'da e-imza için yapılan yasal düzenlemelerin ve standartların me-imza için de kullanılacağı ve 1024 bit'lik RSA anahtarlar kullanılacağı, ETSI TS 102 204 standardının dikkate alınacağı belirtilmektedir. Teknik olarak SIM kartlarının NES ve niteliksiz sertifikaları barındırabilme özelliğine sahip olduğu, ESHS'nın iki tip sertifikayı da destekleyebilmesi için ek bir yatırım yapması gerektiğinden sadece NES'leri desteklemeyi tercih edecekleri belirtilmektedir [3, 8, 20].

2.1.22. Kuveyt

Nüfusun %55'inin mobil cihaz sahibi olduğu Kuveyt'te GSM işletmecisi Wataniya Telekom, Valimo ile yaptığı işbirliği sonucunda, kullanıcılarına teknik olarak ETSI standartlarına uygun ve sahip oldukları mobil cihazlarındaki SIM kartları aracılığıyla elektronik ortamda işlem imkânı sunmaktadır. Kuveyt Wataniya Telekom'dan me-imza proje sorumlusu Marc Zirka'dan gelen e-postaya göre; Kuveyt'te oluşturulan yapıda imzalama SIM kart üzerinde gerçekleştirilmekte olup sertifika SIM kartlara önceden yüklenmektedir. Ülkede me-imza kullanımının artırılabilmesi için kullanıcılar talepte bulunmadan SIM kartları değiştirilerek şifreler verilmiştir. Kullanıcıların büyük bir çoğunluğu bu nedenle şifrelerini unutmuş durumda olduğundan halen kullanmak isteyen kullanıcıların kartlarının değiştirilmesi gerekmektedir. Hâlihazırda Wataniya Telekom'un ortağı olan Burgan Banka'nın m-ödeme işlemlerinde ve Virgin Store'da m-ticaret işlemlerinde kullanılmaktadır. İşlem sayısı az olduğundan me-imzanın kullanımının da sınırlı olduğu belirtmektedir [20].

2.1.23. Bulgaristan

Bulgaristan'da güvenli e-imzanın düzenleme ve kontrolünden Bulgaristan Haberleşme Düzenleme Komisyonu (Bulgaria Communications Regulation Commission-CRC)' sorumludur. E-imzanın elle atılan imzayla aynı hukuksal geçerliliği sağlayabilmesi için CRC tarafından yetkilendirilmiş ESHS'lerin yayımladığı sertifikaların olması gerekmektedir. Halen dört ESHS'nın aktif olduğu, 2001 yılında yürürlüğe giren yasalarında CRC'yi yönetmelik yapmaya zorlayan me-imzanın kullanımını kısıtlayan veya yasaklayan herhangi bir hüküm, herhangi bir düzenleme ve me-imza uygulamalarına yönelik bir planın bulunmadığı belirlenmektedir [3]

2.1.24. Slovakya

Slovakya'da akreditasyon için başvuru yapmış bir ESHS ve biri nitelikli diğeri niteliksiz sertifika veren akredite edilmiş iki ESHS olmak üzere üç ESHS mevcuttur. Bu ESHS'ler, kendilerinin yayımlamış olduğu politikalarda belirtilen işlem başına olan maddi zararı karşılamakla yükümlüdür. E-imzanın akreditasyon ve denetiminden sorumlu Slovakya Cumhuriyeti Ulusal Güvenlik Kurumu'dur. Me-imzanın mobil cihaz ile oluşturulan bir e-imza olduğu kabul edilmektedir. Direktif'i kendi yasal düzenlemelerine aktararak e-imzayı basit e-imza ve güvenli e-imza olmak üzere iki şekilde ele almakta, yüksek güvenliğinden dolayı düzenlemelerinde güvenli e-imza şart koşulmuş durumda olduğu, bu sebeple de e-imzanın mobil cihazlar ile oluşturulmasında bir kısıtlama olmadığı değerlendirmesi yapılmaktadır [3,22].

2.1.25. İrlanda

eID kartlarının kullanımına dayalı e-devlet uygulamalarını başlatmış ve e-imzaya ilişkin düzenlemelerini 2000 yılında tamamlamış olan İrlanda'da İletişim, Denizcilik ve Doğal Kaynaklar Birimi e-imzadan sorumludur. İrlanda'da mal ve hizmetlerin

alımında mobil cihaz, ödeme aracı olarak da kullanılabilmektedir. Ödenecek ücret, kişinin mobil cihazına ait faturaya yansıtılmaktadır [3, 8, 10].

2.1.26. Tunus

Tunus'un Elektronik Sözleşme Kanunu'nun 2000 yılında çıktığı birinci maddeye göre " Elektronik sözleşmeler yazılı sözleşmelere tabi tutulur", aynı kanunun 4. maddesi ise "Yazılı doküman kaydetme kanunu" olduğu gibi, elektronik dokuman kaydetme kanunu olarak ifade edilmektedir [80].

2.1.27. Ürdün

2001 yılında çıkarılan 73. kanuna göre, 1952'de çıkarıldığı 30. maddeye düzeltme yapmıştır. Bu düzenlemeler şifrelenen elektronik belgelerli kapsamaktadır. Aynı yılda çıkan ikinci maddede elektronik sözleşmeleri tanımlamada bulunmaktadır. Bu tanıma göre "elektronik sözleşme, elektronik ortamlardaki tamamen veya kısmen gerçekleşen anlaşmalar" olarak ifade edilmektedir [80].

2.1.28. Bahreyn

2002 yılında çıkardığı Elektronik İmza Kanunu'nun üçüncü maddesinde elektronik anlaşmaları tanımlayan maddede "kimsenin rızası olmadan alma, satma veya e-imzasını kullanma işlemi geçerli sayılmaz". Beşinci maddede sözleşmelerin elektronik belge halinde sunulması, kanun çerçevesi şartlarına uygun bulunduğunda yazılı belgelerin yerine geçebilir nitelikte olduğu belirtmektedir [80].

2.1.29. Dubai Emirliği

Dubai Emirliğinin Elektronik Ticaret Kanunu ile ilgili üçüncü maddesinde, bu maddenin elektronik sözleşmelerin elektronik belgelere dönüştürülerek kolaylaştırması için ve kullanıcıların elektronik ortamlarındaki gerçekleşen anlaşmalarda güvenlerini sağlamak için sunulmuştur [80].

2.1.30. Mısır

Enformasyon Teknolojileri Sanayi Geliştirme Enstitüsü tarafından 2004 yılında. "E-İmza Düzenleme Kanunu" adı altında 15. maddeyi düzenlemiştir. Kanun 30 maddeden oluşmaktadır. Birinci Madde kanunda geçen sözcükleri açıklamaktadır. 14–22 Maddeler, medeni, idari ve ticari sözleşmelerde e-imza düzenlemelerinin nasıl yapılması gerektiği ile ilgili bilgiler içermektedir [80].

2.1.31. Türkiye

2001 yılında Dış Ticaret Müsteşarlığı bünyesinde kurulan Hukuk Çalışma Grubu tarafından hazırlanan "Elektronik Veri, Elektronik Sözleşme ve E-imza Kanunu Tasarısı Taslağı" ile başlamıştır. Bu kanun tasarısının 17 Nisan 2002 tarihinde Başbakanlığa gönderilmesi öncesinde, Adalet Bakanlığı tarafından 14 Ocak 2002 tarihinde ikinci bir çalışma ele alınmıştır. Adalet Bakanlığı'nın hazırladığı "E-imzanın Düzenlenmesi Hakkında Kanun Tasarısı "10 Eylül 2002 tarihinde Başbakanlığa sunulmuştur. Bu taslak, "E-imza Kanunu" olarak küçük değişikliklerle 23 Ocak 2004 tarih ve 25355 sayılı Resmi Gazete'de yayımlanmıştır. Yürürlülük tarihi 23 Temmuz 2004 olarak öngörülmüş olan Kanun'un, ülke gerçeklerine uygun olarak uygulamaya geçirilebilmesi için 23 Ocak 2005 tarihine kadar gerekli düzenlemeleri yapma görevi TK' ya verilmiştir. Türkcell ve e-Güven "CeBIT Bilişim Eurasia 2006"'da ve 7–8 Aralık 2006'da yapılan ilk Ulusal E-İmza Sempozyumunda, ülkemizde me-imza ile ilgili test çalışmalarını başlattıklarını ilan etmişlerdir. Duyurusu yapılan test çalışmalarında me-imza için güvenli taşıma ortamı olarak Gemolta ürünü olan EAL4+ SIM kartı kullanılmakta ve SIM kart dışında ek bir donanıma ihtiyaç duyulmamaktadır [23, 83].

Çizelge 2.2. AAA çalışmaları olan ülkeler ve detay bilgiler

Ülke	Verilen hizmetler	Sorumlu Kuruluş[3]	Uygulama alanları	Yıl
Avusturya	e-pasaport eID	Yayın ve Telekomünikasyon Kurumu	Pasaport müracaat	2000 e-imza kanunu 2006 e-pasaport 2005 eID
Finlandiya	me-imza eID	Haberleşme Regülâsyon Kurumu (FICORA)	Nüfus İdaresi Bankalar Kamu Kurumları	2000 e-imza kanunu
Fransa	Kısıtlı me-imza eID	Ticaret ve Endüstri Bakanlığı	Küçük ödemeler Sinema bileti satın alma	2005 eID 2000 e-imza kanunu
Portekiz		Elektronik Sertifika Sistemi Kurumu (SCEE)		2006 eID
İspanya	eID me-imza	Telekomünikasyon ve Bilgi Güvenliği	m-ödeme	2003 e-imza kanunu 2006 eID
İsveç	e-imza	Posta ve Telekom Kurumu		
İsviçre	e-imza			2003–2005 e-imza kanunu onaylama ile yürürlüğe girme süreci

Çizelge 2.2. (Devam) AAA çalışmaları olan ülkeler ve detay bilgiler

Ülke	Verilen hizmetler	Sorumlu Kuruluş[3]	Uygulama alanları	Yıl
Belçika	e-pasaport eID		Banka Hizmetleri e-kütüphane hizmetleri	2004 e-pasaport 2005 eID
Çek Cumhuriyeti	e-mühür e-imza	Çek Posta İdaresi ve Sertifika makamı (SM)	Bankacılık işlemleri	2006 e-imza 2006 e-mühür
Danimarka	e-imza	Bilgi Teknolojileri ve Telekomünikasyon Kurumu		2000 e-imza kanunu 2003'ten itibaren ücretsiz e-imza dağıtımı
Estonya	me-imza eID	SIDEAMENT	m-ticaret	2002 eID
Almanya		Federal Elektrik, Telekomünikasyon, Posta Hizmetleri ve Demiryolları Ağı Kurumu	m-ödeme	2000 e-imza kanunu 2003 e-imza ittifakı 2005 e-kart duyurusu
Macaristan	me-imza	Milli Haberleşme Kurumu		2006 e-imza başlattı
İtalya	e-kart			

Çizelge 2.2. (Devam) AAA çalışmaları olan ülkeler ve detay bilgiler

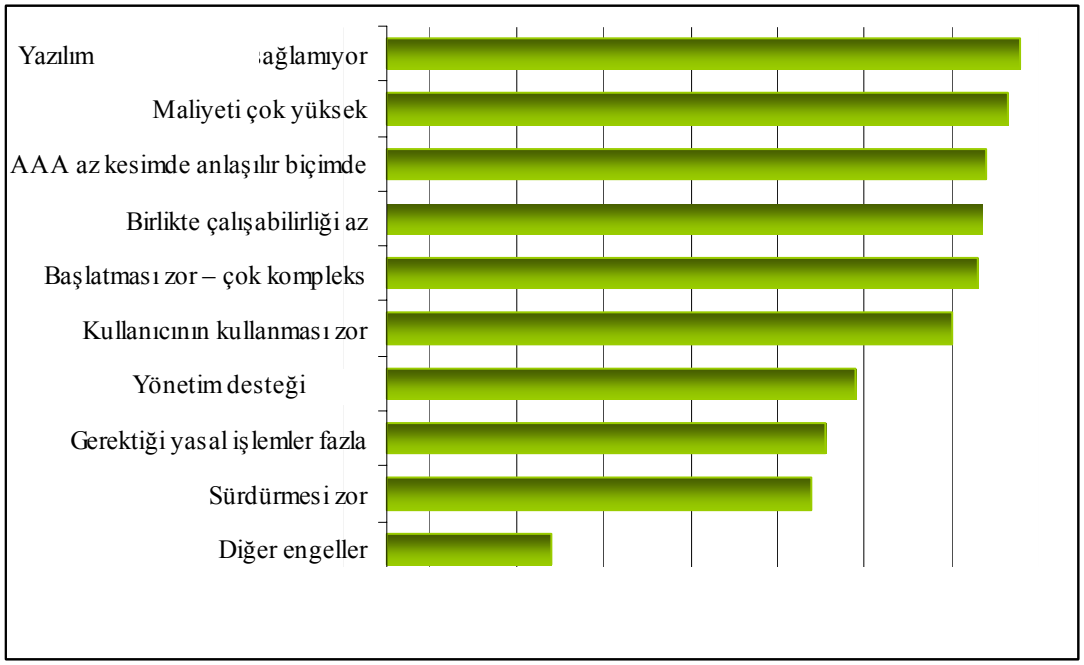
Ülke	Verilen hizmetler	Sorumlu Kuruluş[3]	Uygulama alanları	Yıl
Malta	eID e-pasaport	Sosyal Güvenlik Bakanlığı	Web üzerinden pasaport başvurusu	2004 eID 2005 e-pasaport
Norveç	me-imza	Post-Og Teletilsynet	m-ticaret Bankacılık	
Polonya	e-imza	Ekonomi Bakanlığı		2000 e-imza kanunu
Lüksemburg		Ekonomi ve Ticaret Bakanlığı		2000 e-imza kanunu
Çin		Kamu Güvenlik Bakanlığı		2005 me-imza uygulaması
Kuveyt	me-imza		m-ödeme m-ticaret	
Bulgaristan	e-imza	Haberleşme Düzenleme Komisyonu		2001 e-imza kanunu
Slovakya	e-imza	Ulusal Güvenlik Kurumu		
Slovenya	me-imza	Bilgi Teknolojileri Bakanlığı	m-devlet m-bankacılık m-vergi	

Çizelge 2.2. (Devam) AAA çalışmaları olan ülkeler ve detay bilgiler

Ülke	Verilen hizmetler	Sorumlu Kuruluş[3]	Uygulama alanları	Yıl
İrlanda	e-imza	İletişim, Denizcilik ve Doğal Kaynaklar Birimi	m-ödeme	2000 e-imza kanunu
Tunus				2000 e-imza kanunu
Ürdün				2001 e-imza kanunu
Bahrin				2002 e-imza kanunu
Mısır	e-imza	Enformasyon Teknolojileri Sanayi Geliştirme Enstitüsü		2004 e-imza
Türkiye	e-imza me-imza			2004 e-imza kanunu 2005 e-imza uygulamaları 2006 me-imza test çalışmalarını başlattı

2.2. Açık Anahtar Altyapısı Kullanımının Önündeki Engeller

Açık Anahtar Altyapısının (AAA) temel görevi; elektronik ortamlarda haberleşen, işlem gören ve çalışan kişiler, kurumlar veya cihazlar arasında güvenilir bir haberleşme ortamı oluşturmaktır [2]. Yapısal Enformasyon Standartları İlerleme Kuruluşu (OASIS), AAA kullanımı ve devreye sokulması önündeki engelleri tanımlamak ve öncelikler belirlemek atamak üzere bir araştırma gerçekleştirmiştir [4]. Bu anketin 2003'te gerçekleştirilmiş olmasına rağmen, sonuçları hala bugün geçerli gibi görünmektedir.



Şekil 2.1. AAA kullanımında gözlenen engeller [4]

2003 yılında J. Dumortier, yayınladığı raporda [5] e-imza kullanımının yaygınlaştırılmasına olan yönelik açık konular ile Avrupa Komisyonunun etkinlikleri dikkate alınarak önemli hususlar aşağıda sunulmuştur.

• Nitelikli sertifikalar ve ilgili hizmetler için doğal bir pazar talebi bulunmamaktadır. Avrupa'da e-imzaların en büyük uygulama alanı genel olarak kapalı kullanıcı ortamındaki elektronik bankacılık uygulamalarıyla bağlantılıdır ve böylece Direktifin kapsamı dışındadır. Direktifin kapsamı içerisinde, çok az sayıda uygulama kullanımdadır ve bunlar hemen hemen tamamıyla e-devlet uygulamaları ile sınırlıdır.

• Pek çok US'ları, uygulamalarının yasal olarak uyumlu olması için minimum Nitelikli E-imzalar gerektirdiğine inanmaktadır. Bu gerekli olsa da sertifikaların nitelikli olmadan da kullanabileceği bilinci olmadığından maliyet artışı ve karmaşıklıklara karşılaşabilmektedir.
• Hem ulusal hem de uluslararası boyutta e-imzanın uygulanması için isteksizlikler ve pazar boyutunun azlığı, e-imza uygulamalarının artırılmasının önündeki büyük engellerdir.
• Kısmen AB Direktifinin şu anda SSCD'ler hakkında çok yüksek gereksinimleri belirlemesi nedeniyle, bu gibi aygıtlar nadiren piyasada bulunmakta ve bu günden yeni artmaya başlamıştır.
• AB İmza Direktifin düzenleyici çerçevesi sertifika sağlayıcılar için oldukça ayrıntılı kurallar içerirken, sertifika sağlayıcıların diğer kategorileriyle ilgilenmemektedir [5].

Enformasyonda Kimliğin Geleceği Derneği (FIDIS)'e göre [6]:
AAA sistemlerinin e-imzalar, eID ya da e-devlet hizmetleri açısından uygulaması yalnızca başlangıç aşamasında olup aşağıdaki engellerle karşılaşılabilmektedir
• Altyapıyı oluşturmak için gereken karmaşıklık ve başlangıç yatırımının yüksek olması.
• Maliyetlerin (kart okuyucu, yazılım) yüksekliği ve mevcut e-uygulamaların azlığı.
•Sertifika yönetiminde karşılaşan güçlükler, zaman damgası konusundaki standartların eksikliği, farklı platformda kullanılabilirlik gibi sorunlar.
• SM'leri ve ülkeler ve de ilgili yetki alanları arasında karşılıklı güven tanıma oluşturmanın yasal ve usul düzenleme yönleri yani, (e-imzalar ve akdi sorumluklar hakkındaki) politikaların, akdi sözleşmelerin ve yasal çerçeveler,
• Farklı SM'leri arasındaki teknik olarak uyumsuzluklarla karşılaşma ve özellikle uygulama düzeyinde kriptografik tekniklerin, sertifika özelliklerinin, akıllı kart teknolojilerinin ve sertifika yönetiminin oluşturulmasındaki zorluklar.

Nitelikli e-imzaların kullanımı beklenenden daha düşüktür ve pazar bugün çok iyi gelişmiş değildir. Bugün için e-imza uygulamalarının e-devlet ve kişisel e-bankacılık hizmetleri ile bağlantılı olması ve ekonomik getirilim bugün için fazlaca olmasını bunun ana nedenlerinin başındadır. Hizmet sağlayıcılar birden fazla uygulama için e-

imza geliştirmek üzere çok az teşvike sahiptir. Sadece bankacılık gibi paralı sektörlere çözümler sunmayı tercih etmektedirler. Diğer nedenler ise, elektronik arşivler için kapsamlı çözümlerin hala olmamasıdır.

Bunların dikkate alınmasıyla, e-devlet hizmetlerinin yaygınlaşmasıyla e-imza kullanımının yaygınlaştırılması sağlanabilecektir.

2.3. Genel Değerlendirme

Bu tez çalışması kapsamında, ülkelerin AAA ile ilgili yapmış oldukları çalışmaları özet halinde Çizelge 2.2'de yer almaktadır.

Bu bölümde incelenen ülke çalışmaları kısmen [3] numaralı kaynaktan yararlanarak genel olarak değerlendirildiğinde aşağıdaki bulgular sunulmuştur

1. Finlandiya ve Norveç'in AAA çalışmalarında öncü oldukları ve özellikle Finlandiya e-imza ve me-imza konusunda önde gelen ülkeler arasında olduğu tespit edilmiştir.
2. Ülkelere kesin olarak belirlenmiş bir güven modelinin bulunmamaktadır.
3. Birçok ülkedeki çalışmaların e-imzayı yaygınlaştırmak amacıyla başladığı belirlenmiştir.
4. Avrupa ülkelerinde me-imza çalışmalarının dünya geneline göre daha yaygın olduğu görülmüştür.
5. E-imza ve me-imza uygulamalarını başlatmayan ülkelerde bile E-imza Kanunlarının yürürlüğe girdiği anlaşılmıştır.
6. Pek çok ülkenin me-imza çalışmalarını başlattığı ve test aşamasında olduğu belirlenmiştir.
7. Türkiye'nin me-imza altyapısı ve uygulamaları konusunda dünyada önemli rol oynayabilecek ülkelerden olduğu görülmüştür.

3. ELEKTRONİK İMZA STANDARTLARI

Bu bölümde Avrupa Standartlar Komitesi (European Standardization Committee – CEN), Avrupa Telekomünikasyon Standartları Enstitüsü (European Telecommunications Standards Institute - ETSI) ve Uluslararası Telekomünikasyon Birliği (International Telecommunication Union - ITU) gibi kuruluşlar tarafından sunulan e-imza standartları yer almaktadır. Bu standartlar aşağıda alt başlıklarda açıklanmıştır.

3.1. Avrupa Standartlar Komitesi (CEN) Standartları

Kısa adı CEN olan Avrupa Standartlar Komitesi, standartların AB düzeyinde uyumlaştırılması amacıyla faaliyette bulunan temel kurumdur. Çalışma alanı diğer iki kuruma (CENELEC[1] ve ETSI[2]) oranla daha geniş olan CEN, tüm sektörlerde uyumlaştırılmış AB standartları oluşturarak, ulusal standartların farklılığından doğan ve tek pazar'ın işleyişini olumsuz yönde etkileyen teknik engellerin kaldırılması yönünde çalışmalar yapmaktadır. Merkezi Belçika'nın Brüksel kentinde bulunan Avrupa Standartlar Komitesi, Türk Standartları Enstitüsü de dahil olmak üzere, toplam 19 Avrupa Birliği CEN'e üyedir [83]. E-imzayla ilgili standartlar aşağıda kısaca açıklanmıştır.

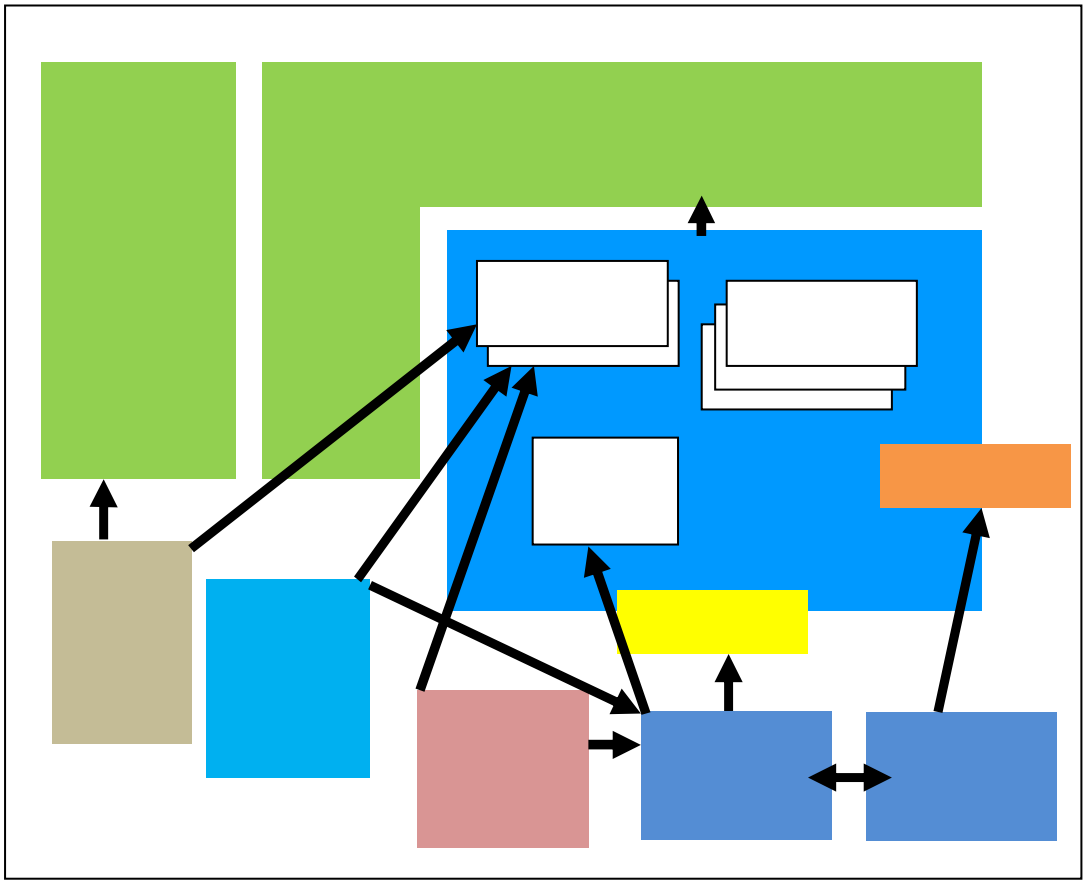
3.1.1. CWA 14172–1 EESSI uygunluk değerlendirmesi kılavuzu, genel bakış

Elektronik Sertifika Hizmet sağlayıcıları (ESHS) tarafından nitelikli ve nitelikli olmayan sertifikalar ortaya çıkarken kullanılan ürün ve teknoloji bileşenleri güvenlik şartlarını vermektedir. Özellikle sertifikaların yönetiminde kullanılan güvenilir sistem (TWS) üreticilerini ilgilendirmektedir. Belli sayıda hizmetlere bölünmüş bir ESHS'ye genel bir bakış verilmiştir. Sekiz bölümden oluşan bu standardın bölümleri

[1] Avrupa Elektroteknik Standartlar Komitesi. Avrupa düzeyinde standardizasyon alanında çalışmalarda bulunan üç kurumdan biridir, ürün emniyeti ve ürünün elektroteknik yapısına yönelik standartlar hazırlamaktadır.

2 Avrupa Telekomünikasyon Standartlar Komitesi. telekomünikasyon, televizyon ve radyo yayıncılığı ile bilgi teknolojisi alanlarında standardizasyon çalışmalarında bulunmaktadır.

arasındaki bağlantı Şekil 3.1'de özetlenmiştir. Bu hizmetlerin bazıları "Çekirdek Hizmetler" zorunluyken, "Tamamlayıcı Hizmetler" denen bazıları isteğe bağlıdır.



Şekil 3.1. CWA 14172 Sertifika Bölümleri [24]

3.1.2. CWA 14172–2 Belgelendirme yetkili hizmetleri ve süreçler

Bu bölümde yetkili Belgelendirme Yetkili Kuruluşları (SM'ler) için ETSI TS 101 456 ve ETSI TS 102 042 standartlarına göre uygunluk değerlendirmesi kılavuzu verilmektedir. Bu kılavuz bağımsız kuruluşlar ve onların tahakkuk memurları tarafından kullanım amacı taşımaktadır.

Bu standart yedi bölümden oluşmaktadır. Birinci bölümde, kılavuza toplu bir bakış sağlamakta ve kılavuzun numaralandırmasını ve şartlarla ilgili terminolojiyi açıklamaktadır. İkinci bölüm SM standartlarda kullanılan SM kavramını

sunmaktadır. Üçüncü bölümde, SM değerlendirilmesindeki standartların içeriği, bu standartların bağımsız kuruluşlarca kullanımını ve uyumlu hale getirme deneyimini paylaşmaktadır. Dördüncü bölümde, bağımsız kuruluşlar, tahakkuk memurları ve değerlendirme ekipleri için şartlar, yönetim sistemlerinin akreditasyonu / belgelendirilmesindeki mevcut uygulamalara dayanan kılavuzluk sağlamaktadır. Bir sonraki bölümde, bilgi güvenliği yönetim sistemleri gibi oldukça karmaşık yönetim sistemlerinin belgelendirilmesinde uygulanan mevcut pratikler açısından değerlendirme sürecini tanımlamaktadır. Bu tür değerlendirme süreçlerinin SM'lerin değerlendirilmesinde kullanılabilecek kriterler olduğu kabul edilmektedir [25].

3.1.3. CWA 14172–3 E-imza sertifikalarının yönetilmesinde güvenli sistemler

Bu standart, (CWA 14167–1) olan standardın "E-imza Sertifikalarının Yönetilmesinde Güvenli Sistemler için Güvenlik Şartları, Sistem Güvenlik Şartları" karşısında TWS uygunluk değerlendirilmelerini vermektedir. Bu kılavuzluk TWS'lerin ve TWS kullanan ESHS'lerin üreticileri ve tedarikçileri yanında IT Denetçileri için de kullanılma amacı taşımaktadır.

Bu standart altı bölümden oluşmaktadır [26]. Birinci bölümde kılavuza bir toplu bakış sağlamakta ve kılavuzun numaralandırmasını ve şartlarla ilgili terminolojiyi açıklamaktadır. İkinci bölümde, TWS kavramı ve üçüncü bölümde IT Denetim prensiplerini tanımlamaktadır. Bir sonraki bölümde, TWS'lerin uygunluk değerlendirmesine giriş, (CWA 14167–1) içeriğini TWS'lerin değerlendirilmesi şartnamesi olarak genel terimlerle açıklamaktadır. Beşinci bölümde, IT Denetçileri şartları hakkında kılavuz, IT Denetçilerinin yeterlilikleri ve davranışları için şartları tanımlamaktadır. Son olan altıncı bölümde, (CWA 14167–1) kullanımı hakkında kılavuz, IT Denetimlerinin (CWA 14167–1)'de belirtilen güvenlik şartlarına göre yapılması için kılavuzluk sunmaktadır.

3.1.4. CWA 14172–4 İmza oluşturma uygulamaları ve e-imzanın doğrulanması için kılavuzlar

Bu standart (CWA 14170) "İmza Oluşturma Uygulamaları için güvenlik şartları" ve (CWA 14171) "E-imza Doğrulanmasında Genel Kılavuzlar" şartnamelerinin metinlerine dayanmaktadır. İmza oluşturma ve doğrulama fonksiyonlarını yerine getirmek için gereken süreçlerin karmaşıklığından dolayı bu uygulamalar ve genel kılavuzlar, bu fonksiyonları mümkün kılan bir işletim sistemi / uygulamaya entegre olmadığı sürece biçimsel değerlendirme süreçleri için uygun değildir. (CWA 14171) tavsiyelerinin bilgilendirici yapısı da bunu ayrıca destekler.

Bu standart altı bölümden oluşmaktadır [27]. Birinci bölümde, kılavuza bir toplu bakış sağlamakta ve kılavuzdaki ifadelerin numaralandırılmasını açıklamaktadır. İkinci bölümde, uygunluk beyanına giriş sunmaktadır. Üçüncü bölümde, uygunluk beyanında bulunan imalatçılara imza oluşturma uygulamalarıyla ilgili kılavuzluk sağlar ve buların formatını tanımlamaktadır. Dördüncü, beşinci ve altıncı bölümlerde, kamusal ortamda imza oluşturma uygulamalarının Servis sağlayıcılarına kılavuzluk sağlar ve sağlayıcıların beyanlarının formatını tanımlamaktadır.

3.1.5. CWA 14172–5 Güvenli imza oluşturma aygıtları

Bu bölüm Güvenli İmza Oluşturma Aygıtlarının (CWA 14169) "Güvenli İmza Oluşturma Aygıtları EAL4+" versiyonuna göre uygunluk değerlendirmesi hakkında kılavuzluk sağlamaktadır. Kılavuzluk tayin edilmiş kuruluşlar, tahakkuk memurları, değerlendiriciler ve üreticiler tarafından kullanım amacı taşımaktadır.

Bu standart altı bölümden oluşmaktadır [28]. Birinci bölümde, kılavuza toplu bir bakış sunmakta ve kılavuzun numaralandırılmasını ve şartlarla ilgili terminolojiyi açıklamaktadır. İkinci bölümde, SSCD'lerin uygunluk değerlendirmesine giriş sunmaktadır. Üçüncü bölümde, tayin edilmiş kuruluşlar için minimum gereksinimlerle ilgili Avrupa Komisyonu Direktifine dayanan SSCD uygunluk değerlendirmeleri için organizasyon yapısı hakkında yönlendirici bilgiler

sunmaktadır. Dördüncü bölümde, SSCD'lerin değerlendirilmesi ve uygunluklarının doğrulanması hakkında da kılavuzluk sağmaktadır. Beşinci bölümde, SSCD'nin değişikliğe (kayıp, çalışma, süre bitimi, yeni versiyonlar) uğraması halinde SSCD onayının sürdürülmesiyle ilgili bilgilere yer verilmektedir.

3.1.6. CWA 14172–6 Nitelikli olanların dışında imzaları destekleyen imza oluşturma aygıtı

Bu standart CWA 14365–2 "PP– Yazılım İmza Oluşturma Aygıtı SCDev-PP'ye göre imza oluşturma aygıtlarının (SCDev'ler) uygunluk değerlendirmeleriyle ilgili bilgiler sunmaktadır. Bu bilgiler belgelendirme kuruluşları, tahakkuk memurları, değerlendiriciler ve imalatçılar tarafından kullanım amacı taşımaktadır.

Bu standart beş bölümden oluşmaktadır [29]. Birinci bölümde, kılavuza toplu bir bakış sunmakta ve kılavuzun numaralandırılmasını ve şartlarla ilgili terminolojiyi açıklamaktadır. İkinci bölümde, SCDev'lerin uygunluk değerlendirmesine giriş sunmaktadır. Üçüncü bölümde, ürün belgelendirme uygulamalarına dayanarak SCDev uygunluk değerlendirmesi yapan kuruluşlarla ilgili şartlarla ilgili kapsamaktadır. Dördüncü bölümde, SCDev'lerin uygunluğunun değerlendirilmesi ve teyit edilmesiyle ilgili kılavuzluk kapsamaktadır. Beşinci bölümde, SCDev'in değişikliğe (tadil, zeyil, yeni versiyonlar) uğraması halinde SSCD onayının sürdürülmesiyle ilgili kılavuzluk kapsamaktadır.

3.1.7. CWA 14172–7 İmzalama işlemleri ve anahtar oluşturma hizmetleri için belgelendirme hizmeti sağlayıcılar tarafından kullanılan kriptografik modüller

Bu bölüm CSP'ler tarafından imzalama işlemlerinde ve anahtar oluşturma hizmetlerinde sırasıyla CWA 14167 bölümleri olan 2, 3 ve 4'e göre kullanılan kriptografik modüllerin uygunluk değerlendirmeleriyle ilgili kılavuzluk sağmaktadır. Bu kılavuzluk belgelendirme kuruluşları, tahakkuk memurları, değerlendiriciler ve imalatçılar tarafından kullanım amacı taşımaktadır.

Bu standart beş bölümden oluşmaktadır [30]. Birinci bölümde, kılavuza toplu bir bakış sunulmakta ve kılavuzun numaralandırılmasını ve şartlarla ilgili terminolojiyi açıklamaktadır. İkinci bölümde, CSP'ler tarafından kullanılan kriptografik modüllerin uygunluk değerlendirmelerine giriş sunmaktadır. Üçüncü bölümde, ürün belgelendirme uygulamalarına dayanarak CSP'ler tarafından kullanılan kriptografik modüllerin uygunluk değerlendirmelerini yapan kuruluşlarla ilgili kılavuzluk sağlamaktadır. Dördüncü bölümde, CSP'ler tarafından kullanılan kriptografik modüllerin uygunluğunun değerlendirilmesi ve teyit edilmesiyle ilgili kılavuzluk kapsamaktadır. Beşinci Bölümde, kriptografik modüllerin değişikliğe uğraması halinde SSCD onayının sürdürülmesiyle ilgili kılavuzluk sağlamaktadır.

3.1.8. CWA 14172–8 Zaman damgalama yetkili servisleri ve süreçler

Bu bölüm ETSI TS 102 023 V1.1.1. standardına dayanarak Zaman Damgalama Yetkilileri (TSA) ile ilgili kılavuzluk sağmaktadır. Bu kılavuz bağımsız kuruluşlar ve onların tahakkuk memurları tarafından kullanım amacı taşımaktadır.

Bu standart altı bölümden oluşmaktadır [31]. Birinci bölümde, kılavuza toplu bir bakış sunmakta ve kılavuzun numaralandırılmasını ve şartlarla ilgili terminolojiyi açıklamaktadır. İkinci bölümde, TSA kavramın. Üçüncü bölümde, TSA'ların uygunluk değerlendirmesine giriş sunmakta, TSA değerlendirme standartlarının içeriğini, bağımsız kuruluşlar tarafından standardın kullanımını ve uyumlu hale getirilmiş değerlendirme uygulamalarını genel terimlerle açıklamaktadır. Dördüncü bölümde, bağımsız kuruluşlar, tahakkuk memurları ve değerlendirme ekipleriyle ilgili şartlar hakkında kılavuz sunmakta, yönetim sistemlerinin belgelendirilmesiyle ilgili mevcut uygulamalara göre kılavuzluk sağlamaktadır. Beşinci bölümde, uygunluk değerlendirme süreci hakkında bilgilerin yanında Enformasyon Güvenliği Yönetim Sistemleri gibi oldukça karmaşık yönetim sistemlerinin belgelendirilmesinde uygulanan mevcut pratikler açısından değerlendirme sürecini tanımlamaktadır. Bu tür değerlendirme süreçlerinden olan TSA'ların değerlendirilmesine uygulamalar. Son bölümde, ETSI TS 102 023 kullanımı ve

değerlendirmelerin uyumlu olmasını sağlamak için özel dikkat istediği düşünülen bazı elemanlar hakkında kılavuzluk sunmaktadır.

3.1.9. CWA 14167–1 E-imzada güvenilir sistemlerin sertifika yönetimleri için güvenlik şartları, sistem güvenlik şartları

Standardın amacı, e-imzada güvenilir sistemlerin sertifika yönetimleri için güvenlik şartlarının tanımlanmasıdır. Sistemin tamamı için güvenlik şartlarını tanımlamak olduğu halde, diğer kısımlar kriptografik modüller için spesifik güvenlik şartlarını tanımlamaktadırlar.

CWA e-imza sertifikalarının yönetim sistemlerinin tasarımcıları ve geliştiricileri için olduğu kadar bu sistemlerin müşterileri içinde kullanım amacı taşımaktadır [32].

3.1.10. CWA 14167–2 CSP imzalama işlemleri için yedekli kriptografik modül – PP- CMCSOB PP

Standart, orijinal olarak tek bir koruma profili olarak hazırlanmış ve CWA 14167–2:2002 olarak onaylanmıştır.

Daha sonra, bu koruma profili (PP) Ortak Kriterlere uygun hale getirilmesi için gözden geçirilirken aynı TOE için yaratılmış olan ve biri yedekleme için mecburi fonksiyonu, diğeri bu fonksiyonun hariç tutulmasını içeren iki Koruma profili daha yaratılmıştır [33]. Bunlar;

— CSP İmzalama İşlemleri İçin Yedekli Kriptografik Modül – Koruma Profili (CMCSOB-PP).

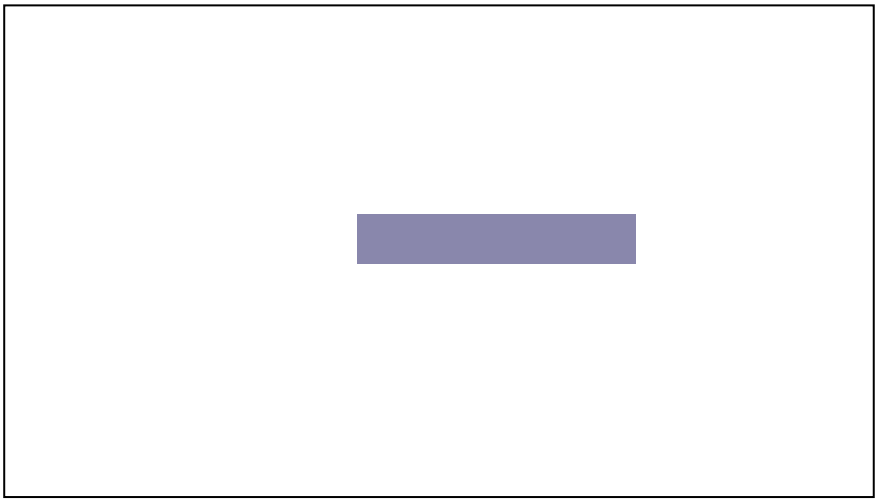
— CSP İmzalama İşlemleri İçin Yedekli Kriptografik Modül – PP(CMCSO-PP).

3.1.11. CWA 14167–3 CSP anahtar oluşturma servisleri için kriptografik modül koruma profili CMCKG-PP

Bu belge aşağıdaki Ortak Kriterler versiyonu kurallarını ve formatlarını izleyen bir koruma profili olarak yaratılmıştır. Güvenli imza oluşturma aygıtlarının algoritmalar seti ve güvenli imza oluşturma aygıtlarının algoritmalar parametreleri ayrı bir belge halinde verilmektedir [34].

3.1.12. CWA 14169 Güvenli imza oluşturma aygıtları "EAL 4+"

Standart, e-imzalar için bir topluluk çerçevesi oluşturulması amacıyla düzenlenmiştir. SSCD'ler için güvenlik şartlarının standardize edilmesi çabalarının amacı bunların AB Yönergesine uygunluğunu ve karşılıklı olarak çalışabilmelerini sağlamaktır. Bu şartların mümkün olduğunca teknoloji açsından tarafsız olmaları gerekmektedir. Bu yaklaşımı izleyen bu CWA mevcut teknoloji durumuna göre mümkün olduğu kadar çok SSCD uygulamalarını kapsamaktadır. Gelişmelerin ele alınabilmesi için teknoloji geliştikçe CWA'lar da düzenli olarak güncellenmektedir.



Şekil 3.2. Güvenli İmza Oluşturma Aygıtları ve Ona Ait alan Çevreler

Farklı SSCD uygulamaları bir dereceye kadar değişebilse de, bu yaklaşım imza oluşturma verileri etrafında Şekil 3.2'de gösterildiği gibi işlevselliği kapsayacak şekilde yapılandırılmıştır.

Standart, SCD içeren ve ilgili sertifikada imza doğrulama verileriyle (SVD) ilgili bir SSCD için Ortak Kriterlere göre üç PP tanımlamaktadır. SSCD bileşenleri ve mekanizmaları [35] nolu kaynakta açıklanmaktadır.

3.1.13. CWA 14170 İmza oluşturma uygulamalarında güvenlik şartları

Standart, imza oluşturma uygulamaları için güvenlik şartları ile bazı tavsiyeleri içermektedir. İmza oluşturma uygulamasında güvenlik şartlarının desteklenmesi için gereken tanımlar, modelleme ve teknik girişler tanımlanmaktadır. İmza oluşturma uygulamasının her bir işlevsel bileşeni ve güvenlik şartları bu standartta verilmektedir [36].

3.1.14. CWA 14171 E-imza doğrulanması için genel kılavuz

Standardın amacı e-imza doğrulanması için genel bir kılavuz ve tavsiyeler sağlanmasıdır. İmza doğrulama uygulamaları ve bileşenlerini geliştiren ve değerlendirenlerin güncellerini sunmaktadır.

Bu standartta ilk amacı elle atılan imzanın eşdeğeri olan nitelikli e-imzaların doğrulanması için bir kılavuz sağlamak ve bunların imzalanmalarından sonra geçerliliklerinin değerlendirilmesine yardımcı olabilecek ek verilerle tamamlamaktır. Bu ek verileri olan imzalara "yükseltilmiş e-imza" denmektedir [37].

3.1.15. CWA 14355 Güvenli İmza oluşturma aygıtlarının kullanılması kılavuzu

Standardın amacı akıllı kartlar, PC'ler, PDA'lar ve mobil telefonlar gibi spesifik platformlarda ve kamusal terminaller ve güvenli ortamlar gibi spesifik ortamlarda SSCD'lerin kullanımının tanımlanması için yapılan önceki çalışmaların genişletilmesidir. Hem yasal hem de teknik uzmanlar, bu alandaki sistem tasarımcıları tarafından e-imza alanında kullanım amacı taşımaktadır [38].

3.1.16. CWA 14365–1 E-imzaların kullanılması hakkında kılavuz, yasal ve teknik hususlar

Standardın amacı e-imzaların genel yasal ve teknik hususlarını tanımlamak ve böylece güven alışmayı yüksek yayılma kapasitesi olan teknolojilere özel olarak dikkat ederek uymak gerekmeden e-ticaret senaryolarının ele alınmasıdır.

Standart, yasal ve teknik uzmanlar tarafından e-imza alanında ve bu alandaki sistem ve ürün tasarımcıları tarafından kullanım amacı taşımaktadır [39].

3.1.17. CWA 14365–2 Yazılım imza oluşturma aygıtları için PP

Standardın amacı, yazılımlarda kullanılabilen imza oluşturma aygıtları için güvenlik şartlarını belirleyerek nitelikli e-imzalar için gereken "Güvenli İmza Oluşturma Aygıtı"ndakinden daha geniş pazar gereksinimini karşılamaktır.

Standart, e-imza alanında teknik uzmanlar ve sistem ve ürün tasarımcıları tarafından kullanım amacı taşımaktadır [40].

3.1.18. CWA 14890–1 Güvenli imza oluşturma aygıtları olarak kullanılan akıllı kartları için uygulama ara yüzü, temel şartlar

Bu belge Güvenli İmza Oluşturma Aygıtlar (SSCD) olarak kullanılan Akıllı Kartların uygulama ara yüzünü, bu kartların ulusal veya Avrupa düzeyinde uluslararası karşılıklı çalıştırılabilmesini ve kullanımını aktifleştirmek için kullanım aşamasında belirlemektedir.

Şartname e-imzalar hakkındaki AB yönergesine dayanmaktadır ve e-imza belgelerine ve kapsamda söz edilen standartlara uyulacağını kabul eder. Bu belgede tanımlanan işlevler koruma profilinin gerektirdiği şekliyle AB yönergesinin asimetrik tekniklerle ilgili genel şartlarının haritasını çıkarır ve imza ortamlarında faydalı olan ek hizmetleri kapsar.

Standart, akıllı kartların SSCD olarak kullanımı için zorunlu şartlara dayanır. Buna imzalama fonksiyonu, ilgili kullanıcı doğrulama, güvenilen yol ve kanalın kurulması, anahtar oluşturma ve bu fonksiyonların ve ilgili kriptografik bilgilerinin yerine getirilmesi için gereken kaynak tahsisi ve formatlarını kapsar.

3.1.19. CWA 14890–2 Ek servisler

Bu bölümde kullanılabilir imza aygıtları olarak aynı teknolojiye dayanan isteğe bağlı servisler tanımlanmaktadır. Buna anahtar şifre çözümü ve HS (kart sahibi) sunucu yetkilendirme, imza doğrulama ve kriptografik bilgilerini kapsanır [42].

3.1.20. CWA 14921 Web servisleri, teknoloji ve standardizasyonla ilgili hususlar

Bu standart XML[3] yapısını ve e-imzaların oluşturulması ve temsil kurallarını belirmektedir. XML İmzaları, XML de dahil olmak üzere her türlü elektronik içeriğe uygulanabilir (veri nesnesi). Bir XML imzası bir veya daha fazla kaynağın içeriğine uygulanabilir.

Zarflanmış veya zarf içine alan imzalar aynı XML belgesi içinde bulunan verilerin üzerindedir. Ayrılmış imzalar ise imza elemanının dışındaki veriler üzerindedir. Daha spesifik olmak gerekirse, bu şartname XML' yi imza elemanı tipi olarak ve bir XML imza uygulaması olarak tanınmaktadır. Her biri için şartları sırasıyla şematik olarak ve metin şeklinde anlatılır. Bu şartname kaynak koleksiyonlarının, algoritmaların ve yönetim bilgilerinin referansları için yöntemler belirleyen başka faydalı tipleri de içerir [43].

[3] herhangi bir işletim sistemine, protokole, firmaya veya platforma bağlı olmayan bir çeşit veri formatıdır

3.2. Avrupa Telekomünikasyon Standartları Enstitüsü (ETSI) Standartları

ETSI, 1988 yılında Avrupa Posta ve Telekomünikasyon Birliği (CEPT) bünyesinde ülkelerin yapmış olduğu haberleşmenin standartlaştırılması ile ilgili görevleri yürütmek üzere kurulmuştur. Avrupa'da kullanılacak telekomünikasyon standartlarını belirleyen bağımsız bir kuruluş olan ETSI özellikle bilgi ve iletişim teknolojilerine ilişkin standartlar gelişmektedir. TK'nın da aralarında bulunduğu 688 üyeye sahip olan ETSI, pazar ihtiyaçlarına göre üyeleri tarafından belirlenen çalışma programı kapsamında faaliyetlerini sürdürmektedir. ETSI'de belli bir konuda yapılacak çalışmaların belirli bir zamanda tamamlanarak gerekli olan standartların bir bütün halinde oluşturulmasını sağlamak amacıyla çeşitli projeler başlatılmaktadır. Bu projelerden bir tanesi, m-ticaret işlemlerinin güvenlik altyapısını oluşturan, şebeke sistemlerini, mobil cihaz teknolojisini (SIM sistemi dâhil olmak üzere) ve GSM işletmecileri tarafından yürütülen müşteri ilişkilerini etkileyebileceği için çekici görünen, diğer mobil cihazlara uyarlanabilen me-imza kavramının, evrensel olarak benimsenmesi için imza istek/cevabının kullanılan mobil cihazın özelliklerinden bağımsız olarak standart bir formatla gönderilip alınabildiği bir halde standartlaştırılmasını sağlamaktır. Me-imzanın oluşturulabilmesi ve yönetilebilmesi için gerekli teknik kriterlerin belirlenebilmesi amacıyla ETSI içerisinde oluşturulan özel bir grup (Specialist Task Force- STF–221) 2000 – 2003 yılları arasında bir takım standartlar hazırlanmıştır. Bu standartlar aşağıda alt başlıklarda sunulmuştur [3].

3.2.1. ETSI TR 102 203 Mobil ticaret, me-imzalar, iş ve işlevsel gereksinimler

ETSI TR 102 203 standardı, e-imza çözümlerini kolaylaştırmak ve yaymak için GSM SIM kart dahil olmak üzere akıllı kart ve AAA'da kullanılan şifreleme tekniklerini de ihtiva eden, me-imza süreçlerinin koordine edilebilmesini ve yönetilebilmesini içeren hizmetin iş ve işlevsel gereksinimlerini konu alan bu standardın amacı Direktif doğrultusunda me-imza hizmeti çözümlerinin birlikte çalışabilirliği, güvenlik önlemleri ve arayüzlere ilişkin teknik özellikleri belirleyebilmek için yön gösterici olmak ve me-imza hizmeti çözümlerinin tasarım

ve uygulamasına yardımcı olmaktır. Ayrıca standartta Direktif'te tanımlanan e-imzaya eşdeğer olan me-imzayı tanıyabilen teknolojilere odaklanılmıştır.

Bu standart dokuz bölümden oluşmaktadır [3,44]. Birinci bölümde, me-imza'ya genel bir bakış yapılmış ve paralel tanımlamalar yapılmıştır. İkinci bölümde, me-imza tasarım kriterlerinden bahsedilmektedir. Üçüncü bölümde, me-imzanın kullanım durumu açıklamakta ve sınıflandırmaktadır. Dördüncü bölüm, me-imza sürecini açıklamaktadır. Beşinci bölüm ise me-imza hizmetinden bahsetmektedir. Diğer bölümlerde, me-imza uygulama sorunları, potansiyel roller ve sorumluluklar, etkileşimler ve arayüzler ile gereksinimler açıklanmaktadır.

3.2.2. ETSI TR 102 206 Mobil ticaret me-imza hizmeti; güvenlik gereksinimleri

Bu standardın amacı, me-imza, e-imzanın mobil ortamdaki hali olarak gerekli güvenlik kriterlerini Direktif çerçevesinde değerlendirmek ve me-imza hizmetiyle ilgili belirlenen güvenlik kriterlerinin derecelerinin belirlenmesine yardımcı olmaktadır.

Bu standart dokuz bölümden oluşmaktadır [3,45]. Birinci bölümde, genel güvenlik analizine yer ayırılıtılmaktadır. İkinci bölümde, me-imza oluşturma sistemi için güvenlik gereksinimleri açıklamaktadır. Üçüncü bölümde, me-imza profiline yer verilmektedir.

3.2.3. ETSI TS 102 204 Mobil ticaret, me-imza hizmeti, web servis arayüzü

Standardın amacı, me-imza hizmetini bir web servisi olarak tanımlayarak, TR 102 203' ün işletme ve fonksiyonel ihtiyaçları bakımından me-imza web servisi tarafından sağlanan metotları, XML Schema ve Web hizmetleri tanımlama dili (WSDL) metotlarıyla ilgili yapıları ve mesaj modellerini açıklamaktır. Dokümanda Basit Nesne Erişim Protokolü (SOAP) zorunlu bir protokol olarak önerilmektedir.

Bu Standart yedi bölümden oluşmaktadır [3,46]. Bunlar; Me-imzaya giriş, me-imza hizmeti fonksiyonları, me-imza web servisi, mesaj formatları, yardımcı tipler, iletişim protokol kuralları ve web servisinin güvenlik ve gizlilik konuları olarak verilmektedir.

3.2.4. ETSI TS 102 207 Mobil ticaret, Me-imza Hizmeti; Me-imza Hizmetinin Dolaşım Şartları

Bu standart son kullanıcı ile US arasındaki me-imza mesajlarının dolaşımını kolaylaştırmak ve belirli bir modelin oluşumunu sağlamak için SOAP ve http mimarisi üzerinden teknik arayüzleri belirlemektir.

Bu standart altı bölümden oluşmaktadır [3,47]. Bunlar; me-imza dolaşım hizmeti, dolaşım çözümü, senaryolar, dolaşım hizmetinin teknik tanımı, veri formatları ve işleme talimatları olarak verilebilir.

3.3. ITU-T, Recommendation (tavsiye) X.1122

ITU (International Telecommunication Union), Birleşmiş Milletlere bağlı olarak dünya çapında telekomünikasyon standardizasyonu, uluslararası frekans tahsisi ve telekomünikasyonun kalkınma boyutu hususlarında faaliyet gösteren, devletlerarası bir uzmanlık kuruluşudur. ITU'nun üç bölümünden birisi olan ITU-T (International Telecommunication Union-Telecommunication Standardization Sector)'nin görevi ITU içerisinde tavsiye olarak yüksek kalitede tüm telekomünikasyon alanlarını ihtiva eden referans standartlar oluşturmaktır [3].

ITU-T X.1122 önerisinin amacı, AAA teknolojisine dayalı mobil güvenlik sistemler kurulduğunda içerdiği yardımcı kuralları ile rehberlik etmektir. Bu standart altı bölümden oluşmaktadır [48]. Birinci bölümde önerinin amacına, ikinci bölümde referanslara, üçüncü bölümde tanımlara, dördüncü bölümde kısaltmalara, beşinci bölümde AAA teknolojisine ait kategorilere yer verilmiştir. Dokuzuncu bölümde sistem oluşturulma modellerine örnekler sunulmuştur.

4. İMZA OLUŞTURMA SİSTEMLERİ

Bu bölümde, Güvenli İmza Oluşturma Sistemlerine (Secure Signature Creation Systems - SSCS) güvenli şekilde e-imza oluşturma isteklerinden bahsedilmiş, daha sonra SSCD'lerin hukuki taleplere sağladığı katkılara yer verilmiştir. E-imza oluşturma sistemlerinin de farklı yapıları sunulacaktır.

4.1. İmza Oluşturma Sistemlerine Genel Bakış

Bilgisayarlar üzerinde e-imzalar oluşturmak mümkündür. Ancak bir belgenin içeriğine mutabık kalındığı zaman, imzalayan kişinin suç işlemesi halinde yasal sonuçlarla karşılaşacağı göz önünde bulundurulmalıdır. İmzanın taklit edilememesinin ve belgenin imzalama süreci sırasında değiştirilmemesinin sağlanması gerekmektedir. Eğer belge daha sonra değiştirilmişse, imzanın doğrulanması başarısız olmalıdır. Dolayısıyla güvenli bir ortam sağlayan imza cihazları oluşturmak üzere yüksek güvenlik standartları uygulanmalıdır. Bu, gereken bütün yasal standartları karşılayacak e-imzalar oluşturmak için gereklidir. Ayrıca, bu nitelikli imzalar bunları imzalayanlarla ilişkilendirmek üzere doğrulanmalıdır. Bu durum güvenilir doğrulama sistemlerine olan gereksinimi ortaya koymaktadır.

Bu gibi sistemleri gerçekleştirmek üzere pek çok husus göz önünde bulundurulmalıdır. Bu sistemler donanım ve yazılım kısmından oluşmaktadır. Yazılım birden fazla parçaya ayrılabilir. Bunlar imzayı oluşturan uygulama ve işletim sistemi olarak adlandırılır. İşletim sistemi yazılım ve donanımı birbiriyle ilişkilendiren kısımdır. Bütün giriş çıkış işlemlerini yönetmesi ve uygulamadan donanıma veri göndermesi nedeniyle tüm sistemin kritik bir parçasıdır. Eğer donanıma güvenliği azalmış imzalanacak bir veri gönderilirse, yanlış belgenin imzalanmasını işletim sistemi önleyebilmekte veya imzalayana bu belgenin yanlış belge olduğunu gösterebilmektedir. Dolayısıyla genel olarak güvenilir olan bir işletim sistemine sahip olmak arzu edilen bir durum olarak karşımıza çıkmaktadır.

Tamamen güvenli olan bir e-imza sertifikası oluşturmak kolaydır. Ancak, bu sistem yasal olarak bağlayıcı imzalar oluşturmak üzere kullanılabilmektedir. Bu durum bütün kullanıcılar için uygun değildir. Kullanıcılar bireylerden oluşmaktadır ve bunlar kendi imzalarını oluşturmak üzere kendi bireysel aygıtlarını kullanmak isteyebilmektedir. Örneğin; birisi kendi PC'sini kullanmak isterken, diğeri PDA'sını kullanmak isteyebilir veya imzalamak için mobil telefonunu kullanmayı arzu edebilir. Özellikle mobil cihazlar günümüzde giderek daha kullanılmakta ve popüler hale geldiği ve ülkemizde de hızla yapılanmasına başlandığını hatırlatmakta fayda vardır.

Normalde bu cihaz kullanıcıları bu cihazları sadece internet olarak görmekte ve veri indirmek veya veri göndermek için kullanmaktadırlar. Çoğu kullanıcı bu cihazlar üzerinden veri iletişimi yaparken yükledikleri programlarda virüs var mı veya cihazın dışarıya ne kadar açık olup olmadığı ile ilgilenmemektedir. Bu şekilde açıkların olması sitemin açık vermesi anlamına gelmektedir. Buda cihazın ve cihazda bulunan verilerin güvenliğinin tehlikede olması anlamına gelmektedir.

Diğer yandan bu güvenlik risklerinden haberdar olan kullanıcılar da bulunmaktadır. Bu kullanıcılar güvenli imzalar oluşturmak ve bu sayede güvenliği arttırmak için gerekli yazılım ve donanımı cihazlarına yüklemektedirler. Güvenlik için oluşturulan imza bazen kullanıldığında bu imzayı doğrulamak isteyen bir kullanıcı imzalayanın sisteminden şüphelenebilir ve böyle bir olay meydana geldiğinde, matematik doğrulama doğru olsa bile verinin güvenilir bir şekilde imzalandığına karar verilemez.

Dolayısıyla, bu tip olaylarla karşılaşılmaması için güvenli e-imzaları oluşturan her sistemin izlemesi gereken kurallar Avrupa Birliği Direktifinde ana hatlarıyla belirlenmiştir. Eğer sistem yalnızca imzalama için kullanılacaksa aşağıdaki talepleri karşılamalıdır.

- Bu sistem, imza anahtarını yüksek potansiyele sahip saldırganlar tarafından kullanımına ve ifşa edilmesine karşı korumalıdır.
- Kullanıcının imzalayacağı tüm verileri kullanıcının tanıyacağı şekilde

gösterebilmelidir.

- Kullanıcının imzalamayı istediği verileri imzalayabilme olanağı sağlamalıdır.
- Eğer sistem ayrıca imzaları doğrulamak için de kullanılıyorsa, belli hususları da yerine getirmelidir. Bu hususlar:
- İmzanın geçerliliğini açık bir şekilde göstermelidir.
- İmzayı oluşturana imzalayan hakkında bilgi göstermelidir.
- İmza tarafından kapsanan tüm verileri kullanıcının tanıyabileceği bir şekilde göstermelidir.
- Geçersiz bir imzayı geçerli, geçerli bir imzayı geçersiz olarak görmemelidir.

Güvenli SCS'ler ve aygıtlar için standartlar geliştirmek üzere pek çok çalışma yapılmıştır. Avrupa E-imza Standardizasyon İnisiyatifi (EESSI) çerçevesinde Comité Européen de Normalisation/Information Society Standardization System (CEN/ISSS) ve Avrupa Telekomünikasyon Standartları Enstitüsü (ETSI/SEC) imzaları oluşturmak ve doğrulamak üzere gerekli olan kullanım ortamları konusunda çalışmak için çalışma grupları oluşturmuşlardır.

4.2. İmza Oluşturma Sistemleri

Bu bölüm SCS'lerin (İmza Oluşturma Sistemleri) çeşitli yönleri ve gerektirdikleri ile ilgilidir. SCS'ye sahip olduğu yapıları vermek üzere alınan kararları uygulayabilmek için ilk olarak, Avrupa Direktifi tarafından talep edilen yasal yönler açıklanmalıdır. İkinci olarak, bir SCS'nin yapıları ve bileşenleri tanımlanmakta, bunu imza oluşturma sürecinin bir tanımı izlemektedir.

Genel olarak SSCD'lerin ve SCS'lerin uygulaması için bir dizi kurallar belirlenmiştir. Avrupa Direktifinde Ek III bir SCS'nin en hassas parçası olan SSCD'nin gerektirdiklerini tanımlamaktadır. Ek III'te aşağıdaki gibi tanımlanan bazı temel açıklamaları vermektedir:

1. Güvenli imza oluşturma aygıtları uygun teknik ve usul vasıtalarıyla en azından aşağıdaki hususları sağlamalıdır. Bunlar:

a. İmza oluşturma için kullanılan imza oluşturma verileri pratik olarak yalnızca bir kere oluşturulmalı ve gizlilikleri ciddi biçimde sağlanmalıdır. Bu madde, imza oluşturma verilerinin (SCD) saklanması ve oluşturulması ile ilgilidir. Gizli anahtar, (yani gerçekte SCD) imzalayan şahıs dâhil olmak üzere herhangi bir şahıs ya da kurum açısından kullanılabilir olmamalıdır. Dolayısıyla SSCD SCD'nin gizli kalmasını teknik olarak sağlamak zorundadır. İkinci madde ise; SCD'nin oluşturulmasının gizli anahtarın benzersiz olmasını garanti etmek üzere yeterince rasgele bir süreç olmasının sağlanmasıdır. SCD'lere tanım itibariyle herhangi bir şahıs tarafından doğrudan erişilemez olması nedeniyle SCD'ler doğrudan karşılaştırılamaz. Bu sorunun olası bir çözümü anahtar çiftinin açık kısmı olan imza doğrulama verilerinin (SVD) karşılaştırılması olabilir.

b. İmza oluşturma için kullanılan imza oluşturma verileri, yeterli güvence ile üretilmeli ve imza geçerli olarak mevcut teknoloji kullanılarak sahtekarlığa karşı korunmalıdır. Bu madde, SCD'nin korunmasıyla ilgilidir. Gizli kısım türetilememeli ve böylece halka açık hale gelmemelidir. SCD'ler güçlü cihazlarla korunmalıdır. Bu durum güçlü kriptografinin uygulanması gerektiği anlamına gelmektedir. Bu gizli kısma anahtarın ömrü boyunca herhangi bir cihazla ulaşılamamalıdır. Ancak gizli kısmın dayanıklılığı hakkında hiçbir hükümde bulunulmamıştır. Gelecekte geliştirilecek teknolojilerle SCD'yi korumak üzere kullanılan kriptografinin kırılmasının mümkün olması nedeniyle bu durum böyledir.

c. İmza oluşturma için kullanılan imza oluşturma verileri imzalayan tarafından diğerlerinin kullanımına karşı korunabilmelidir. Bu maddede, yalnızca imzalayanın SCD'yi kullanabilmesini talep etmektedir. Bu durum imzalayanın gizli kısım üzerinde münhasır kontrole sahip olması ve imzalayanın yanlış kullanıma karşı onu koruyabilmesi anlamına gelmektedir. "SSCD imzalayan ve diğer şahıslar arasında ayrım yapabilmelidir" [38].

Bu durum bilgi ile (Kişisel Tanımlama Numarası – PIN) ya da kullanıcının biyometrik özellikleri ile gerçekleştirilebilir. Kullanıcı şifre cümleciğini kendisi seçebilmelidir ancak bu PIN'ın kolaylıkla tahmin edilmesini önlemelidir.

2. Güvenli imza oluşturma aygıtları, imzalanacak veriyi değiştirmemelidir veya imza sürecinden önce imzalayana bu gibi verilerin sunulmasını önlemelidir. Bu madde, bir SSCD' deki veri akışı konusuyla ilgilidir. İmzalanacak veriler SSCD tarafından değiştirilememelidir ve imzalama sürecinde kabul edilmeme olasılığına göre veri imzalayana gösterilmemelidir. Fakat verinin daima kullanıcıya gösterilmesi gerekmeyebilir. İmzalayan imzalayacağı mesajı gözden geçirmemeyi seçebilmelidir ancak bunu yapma isteği cihaz tarafından sağlanmalıdır.

Nitelikli sertifikalara ilişkin olarak, SSCD SCD'nin ve SVD'nin uyumluluğunu da gösterebilmelidir. Bu durum nitelikli sertifika oluşturulduğunda imzalayan kişinin gerçekten gizli anahtara sahip olduğunu kanıtlamak içindir. Özetleme işleminden geçirilmiş bir belgeyi imzalama yaklaşımı gizli anahtara sahip olmayı kanıtlamaya yeterli değil gibi görünmektedir [38]. Bu durum kullanıcının gerçekten özetleme işleminden geçirilmiş bir belgeyi ya da bazı rasgele verileri imzalayıp imzalamadığına karar verememesinden kaynaklanmaktadır.

SSCD'lerin bu sıkı gereksinimlerinden dolayı WS/E-Sign, SCS'yi iki ana bileşene ayırma kararı alınmıştır [36]. Bunlar:

- İmza Oluşturma Uygulaması (SCA), ve
- Güvenli İmza Oluşturma Aygıtı (SSCD).

SCA bir işletim sisteminin ya da sanal makinenin üzerinde çalışan bir programdır. Amacı imzalayanın SCS ile etkileşime girebileceği bir arabirim oluşturmaktır. Bu verileri imzalamak isteyen kullanıcının yeteneklerine karşılık gelmektedir. Normal olarak giriş aygıtları bir PC kullanıldığında bir fare, klavye veya örneğin bir PDA kullanıldığında bir dokunmatik ekrandır. Buradaki ana nokta kullanıcının sistemi belirsiz olmayan bir şekilde işletebilmesidir. Bunun anlamı bir belgeyi kaza sonucu imzalayamamasıdır. Diğer bir konu ise imzalanacak verilerin, kullanıcıların içeriği anlayabilmesi ve kullanıcıya içeriği imzalanan ile aynı içeriği göstermektedir.

SSCD e-imzayı fiili olarak oluşturan ve SCD'yi içeren bileşendir. Bu cihazın karşılaması gereken Avrupa Direktifi tarafından tespit edilen yüksek güvenlik gereksinimleri bulunmaktadır. Bu yüksek güvenlik standartlarını oluşturmak için bu sistemi donanım olarak tasarlamak gerekmektedir. Akıllı kartların kullanımı SSCD'nin küçük olmasından dolayı bir avantaj oluşturmaktadır ve akıllı kartları PDA'lar ya da mobil telefonlar üzerindeki mobil uygulamalar için çok uygun hale getirmektedir. Özellikle SSCD'ye gönderilen verilerin çok hassas olması nedeniyle SCA'lar donanımla (örneğin bir akıllı kart okuyucu) en azından güvenli bir kanal üzerinden SSCD'ye bağlanmaktadır. Bu bağlantının kanal dinleme veya benzer saldırıları ortadan kaldırmak için güvenli olması gerekmektedir. Ayrıca imza sürecini başlatmak için doğrulama verileri de SSCD'ye gönderilmektedir. Uygulamanın bu kısmını korumak için, doğrudan okuyucuya doğrulama girdi cihazı (örneğin PIN'in girilmesi için) takmak mümkün olmalıdır.

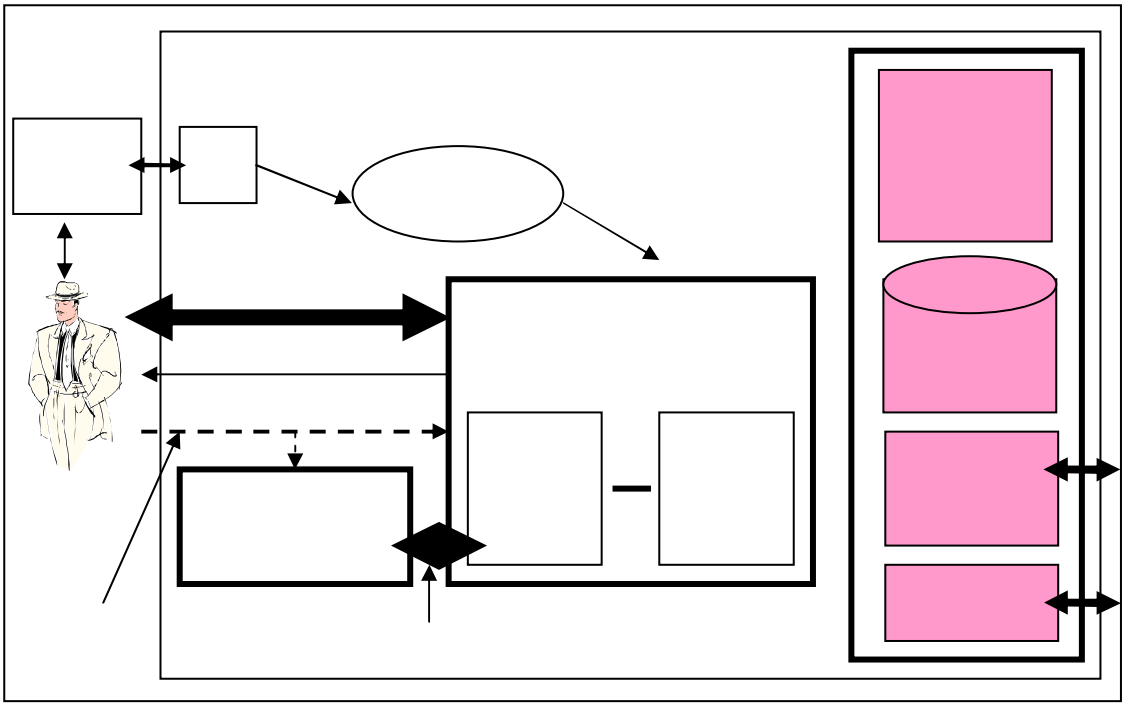
Eğer sistem bir imza doğrulama cihazı olarak kullanılıyorsa, genelde benzer olmalarına rağmen gereksinimler açısından imzalama sisteminden çok az bir farkı vardır. Ana fark SSCD'ye gereksinim duyulmamasıdır.

İsteğe bağlı olarak kullanılan imzaların geçerliliğini sorgulamak üzere çevrim içi olarak zaman işaretlerinin alınıp alınamayacağı çok uygun bir özelliktir. Bu durumda zaman işareti imza tarafından kapsanacaktır. Bu nedenle, internet bağlantısı neredeyse olmazsa olmaz bir gereksinimdir.

Bir SCS'nin önemli bir özelliği de kullanılabilirliğidir. Sistemin kullanıcıların çalışamayacağı kadar çok karmaşık hale gelmemesi çok önemlidir. Güvenliğin zarar görmemesi için bu çok hassas bir konudur. Uygulamanın anlaşılması kolay olmalı ve yanıt süreleri makul süreler içerisinde olmalıdır, aksi takdirde kullanıcı sistemin çalışıp çalışmadığını göremez. Eğer cihaz çok yavaş çalışıyorsa, bu sistemler kullanıcılar tarafından tercih edilmezler.

4.2.1. İmza oluşturma süreci

İmza oluşturma süreci e-imza oluşturulduğunda çalışma akışı olarak görülebilir [36]. İlk olarak imzalanacak belge sisteme girilmelidir. Daha sonra kullanıcı İmzalayanın Belge Sunum Bileşeni (SDP)'ni kullanılarak belgeyi gözden geçirebilmelidir. SDP cihazın gösterim yeteneğine bağlıdır. Bu güvenilir bir görüntüleyici veya başka bir ekran olabilir. Kullanıcı arabirimi SCA'yı kullanarak belgeyi imzalar. Bu durum bir PIN girilmesi ya da kullanıcının biyometrik özellikleri gibi bazı diğer vasıflarla gerçekleştirilebilir. En azından bunun kullanıcı tarafından gerçekleştirilen bir adım olması ve bu adımın kaza sonucu oluşturulamayacağı garanti edilmelidir.



Şekil 4.1. SCS'nin işlevsel modeli [36]

Artık imzalanacak verinin özeti, SCA'nın veri bileşeni tarafından oluşturulur. Bu özet SCS kullanılarak imzalanacak verilerdir. Dolayısıyla kısa bir mesajın şifrelenecek olması, imzalanacak verinin temsili (DTBSR) olarak adlandırılır. DTBSR, imzalama sürecinde SSCD üzerinden SCD (gizli anahtar) ile verileri şifreleyecek olan SSCD'ye gönderilir. Bu iki bileşen arasındaki iletişim yalnızca

imzalanması amaçlanan verilerin SSCD'ye gönderilmesini sağlamak için güvenli bir yol üzerinden gerçekleştirilir.

Bu işlemin sonucu SCA'ya geri döndürülür. Bu şifrelenen değer ile imzalanan veri imzalanan belgeyi oluşturur. Bu işlemin bir sonucu olan imzalanan veri, sertifikalar ve imzalayanın imzalama politikaları kullanılarak oluşturulur. Bu işlem imza oluşturma sürecinin son adımıdır ve oluşturulan belge kullanıcıya geri döndürülür.

Şekil 4.1'de imza oluşturma sürecinin işlevsel modeli gösterilmektedir. Şeklin sol tarafında kullanıcı ve SCA'nın arabirimleri gösterilmektedir. Normal olarak bir CSP ve kullanıcı arasındaki sözleşme, imzalama için gereken sertifikaları almak üzere yapılmaktadır. İmza politika oluşturucu tüm süreç sırasında riayet edilmesi gereken kural ve politikaları sağlamaktadır. Sertifika ve politikalar doğrudan SCA'ya yerleştirilmektedir. SCA'nın kendisi güvenli göstericiler ve özel bileşenlerden oluşmaktadır. SCA kullanıcı arabirimden eylemlerin sonuçlarını alabilmektedir.

SSCD, SCA ve güvenilen bir kanal üzerinden doğrulama verilerini sağlamak zorunda olan kullanıcıya bağlanmaktadır ve kullanıcı ile SCD'nin kriptografik profilini (örneğin özel anahtar) içermektedir. Sistemi tamamlamak için, donanım bileşenlerine erişimleri ele alan, depolama alanı sağlayan ve ağ bağlantıları gibi diğer giriş – çıkış bileşenleri ile ilgilenen işletim sistemi de dâhil edilmektedir.

4.2.2. İmza oluşturma sistemlerinin tipleri

Şu ana kadar bir SCS'nin yapısı genel olarak açıklanmıştır. Bu bölümde SCS'lerin farklı tiplerini tanıtılacaktır. SCS'lerin olası uygulama alanları genişletmek ve bu gibi sistemleri uygulamak için kullanılabilecek farklı aygıtların olanaklarını artırmak için dört farklı "kullanım durumu" tanımlanmıştır [38]. Farklı cihazların ekran tiplerine ilişkin olarak değişken özelliklere sahip olması ve SSCD'nin SCA'dan farklı bir hesaplama motoru üzerinde uygulanabilecek olmasından dolayı bu sınıflandırma yapılmıştır.

Çizelge 4.1'de olası ekran tiplerini göstermektedir. Yalnızca PC'lerin ve büyük ekrana sahip cihazların SCS'leri uygulamak için planlanmamasından dolayı, ekran sınırlamaları hakkındaki irdelemeler de yapılmalıdır. PDA'lar ve mobil telefonlar gibi pek çok aygıt yalnızca sınırlı ekran yetkilerine ya da büyüklüğüne sahiptir. Dolayısıyla iki farklı ekran tipi tanıtılmıştır [38]. Ekran Mesaj Aygıtı (DM), ekran üzerinde tüm mesajı gösterebilmektedir.

Çizelge 4.1. SCS'lerin Farklı Tipleri [38]

	Mesajlaşma Aygıtları Gösteren	Özetleme Aygıtlarını Gösteren
Sınıf 1 Paylaşımlı Hesap Cihazı	Sınıf 1 Mesajlaşma Sistemini Gösteren Güvenilir Giriş / Çıkışlı Emniyetli Bilgisayar)	Sınıf 1 özetleme Sistemini Gösteren ekranlı Akıllı kart
Sınıf 2 Dağılımlı hesap Cihazları	Sınıf 2 Mesajlaşma Sistemini Gösteren (Akıllı Kart kullanan PDA'lar)	Sınıf 2 özetleme Sistemini Gösteren (S/WIM'li Cep telefonları)

Dolayısıyla bu tipten aygıt SCA'yı bir bütün olarak içerebilmektedir. Diğer yandan, Ekran Özet Aygıtı (DH) yalnızca sınırlı bir ekran alanına sahiptir. Bu durumda, SCA'nın bir kısmı aygıtın üzerinde diğer kısmı ise uzak terminal üzerinde yer alan iki kısma bölünmüştür. Eğer belge imzalanacaksa, bu belge ilk olarak uzak terminalde kullanıcıya gösterilmektedir. Daha sonra uygulama belgenin özetinin oluşturmasında, bu özet DH aygıtına göndermekte ve bunu terminalde göstermesinde görev almaktadır. Artık kullanıcı bunların eşlenik olduğundan emin olmak üzere iki özet karşılaştırabilir ve daha sonra imza oluşturma sürecinin gerçekleştirilip gerçekleştirilmeyeceğine ilişkin onayını verir.

Çizelge 4.1'de sunulan bilgiler SSCD ve SCA'nın aynı hesaplama motoru üzerinde olup olmadığını göstermektedir. Bir Sınıf 1 aygıt iki uygulamanın aynı motoru paylaştığı bir sistemdir. SCD ve imzalanacak DTBSR'nin korunmuş olması ve aygıtın Giriş/Çıkış kanallarının güvenli olması garanti edilmelidir. Dahası, "SCA ve SSCD'nin bütün diğer hesaplama süreçlerinden ayrılmış olması" anlamına gelen hakimiyet alanı ayırma sağlanmak zorundadır [38]. Bir Sınıf 1 aygıt üzerindeki ana başlangıç saldırıları bu hakimiyet alanı ayırma ve SCD üzerindeki saldırılardır.
Sınıf 1 cihazının aksine bir Sınıf 2 cihaz SSCD ve SCA için iki farklı hesaplama motoru kullanmaktadır. Dolayısıyla SCA ve SSCD arasında güvenilen kanallar tatbik edilmelidir ve bunlar birlikte çalışmadan önce birbirlerine kendilerini tanıtmak zorundadır. Ayrıca SCA'nın Giriş/Çıkış kanalları güvenli olmalı ve SSCD imzalayana gerçekten imza oluşturma sürecini gerçekleştirmeyi amaçlayıp amaçlamadığını sormalıdır. Bu tipten aygıtlar üzerindeki ana saldırılar SCA ve SSCD arasındaki kanalı hedef almaktadır.

Genel olarak bir Sınıf 2 SCS'nin bir Sınıf 1 SCS'den daha kolay, ancak (iki ayrı hesaplama motoru göz önünde bulundurulduğunda) gereken donanım miktarına ilişkin daha fazla çabayla uygulanabileceği söylenebilir. Aşağıdaki bölümler Çizelge 4.1'de tanımlanabilecek kullanım sınıflarını tanımlamaktadır.

Sınıf 1 Mesajlaşma Sistemini Gösteren: Bu sistem yalnızca bir hesaplama motorundan oluşmaktadır ve tamamen kendi kendisini içermektedir. İmzalanması gereken belgeler tamamen kullanıcının anlayabileceği şekilde gösterilebilir. Tanımlanan sistemlerin örnekleri güvenli bir işletim sistemine sahip bir PC ya da PDA ve bütün giriş ve çıkış aygıtları için güvenilir Giriş/Çıkış kanallarıdır. Yalnızca Giriş/Çıkış işlemleri için mobil telefonu kullanan bir SIM kart diğer bir seçenektir [38].

Sınıf 2 Mesajlaşma Sistemini Gösteren: SCA ve SSCD için iki ayrı hesaplama motoru Sınıf 2 DM sisteminde uygulanmaktadır. Belgeler ana işlemciye bağlı olan ekranda gösterilmektedir. Kullanıcının imzalama işlemini gerçekleştirmek için iznini almak üzere, ya SCA ya da doğrudan SSCD'ye güvenilir bir kanal oluşturulmalıdır.

Bunların örnekleri akıllı kart okuyuculu bir PDA ya da PC'dir. SSCD'yi temsil eden akıllı kart bu okuyucuya takılır.

Sınıf 1 Özetleme Sistemini Gösteren: Bu sistem SCA ve SSCD için tek bir hesaplama motoru kullanmaktadır ve her ikisini olası saldırılara karşı korumaktadır. Ancak aygıt, mesajın yalnızca özet ekranda gösterilebileceği sınırlı bir ekran alanına sahiptir.

Sınıf 2 Özetleme Sistemini Gösteren: Sınıf 2 DM sisteminde olduğu gibi, Sınıf 2 DH sistem için iki farklı hesaplama motoru kullanılır. Ekran tüm mesajı göstermek üzere çok küçüktür ancak DTBSR kullanıcıya gösterilebilir. Bu nedenle SCA iki ayrı parçaya ayrılmıştır ve her ikisi de kullanıcıya bunların aynı olup olmadığını kontrol etme fırsatını vermek üzere kullanıcıya DTBSR'yi göstermek zorundadır. Bu iki parça arasındaki bağlantı güvenli olmalıdır. Verilen bu tipten [38] bir sistemin örneği "SIM tabanlı bir WIM olan S/WIM (Kablosuz Erişim Protokolü Kimlik Modülü) içerisindeki SSCD'ye sahip bir mobil telefon" olabilir. Bu durumda mobil telefon mesajın kendisini gösteremeyebilir. Farklı tipteki SCS'ler hakkında daha fazla bilgi de bulunabilir [38].

4.3. Güvenli İmza Oluşturma Cihazı (SSCD)

SCS'ler hakkında Bölüm 4.2'de daha önce açıklandığı gibi, bu gibi bir sistemin ana parçalarından biri bir SSCD'dir. Bu aygıt SCD içerir ve bu en yüksek güvenlik gereksinimleri ile imza oluşturma sürecindeki en kritik bölümdür. Bu gereksinimler Avrupa Direktifinde tanımlanmıştır.

Gelişmiş e-imzaların tanımından yalnızca imzalayanın SCD'ye erişime sahip olduğu düşünülebilir. Hiçbir diğer şahıs ya da kurum imzalayanın SCD'ini kullanarak imzalar oluşturamaz. Bu durum doğrulama işlemi ile gerçekleştirilebilir. Bu durumda imzalayan kişi imzalama süreci başlatılmadan önce kendisini tanımlamalıdır. Bu durumu elde etmek için verilerin yanlış kullanımını engellemek üzere bazı yöntemler saptanmıştır. PIN girilmesi gibi çözümler bilgi ile tanımlama ya da imzalayanın

biyometrik özelliklerinin kullanımı gibi diğer araçlar olabilir. Bununla birlikte, hiç kimsenin imzalayanın SCD üzerindeki kendisine ait olan kontrolünden vazgeçmesini engelleyemeyeceği de ayrıca göz önünde bulundurulmalıdır. Eğer bilgi ile tanımlama uygulanırsa, imzalayanın gizli PIN'i ile birlikte SSCD'yi başkalarına vermesini önleyecek hiçbir teknik vasıta uygulanamaz.

Bu tanımın diğer bir sonucu ise SSCD'nin uygulanmasının, imzalayan SCD'nin oluşturulma anında bilinmiyor olsa bile SCD'nin oluşturulması, saklanması, kullanımı ve imha edilmesi ile başa çıkmak zorunda kalmasıdır. Dolayısıyla, imzalayan ile e-imza arasındaki ilişki SCD'yi içeren aygıt yani SSCD tarafından tanımlanmaktadır. Aksi takdirde SCD kişiselleştirmeden önce kullanılabilir ve imzalayan kişi bu konuda hiçbir şey yapamaz.

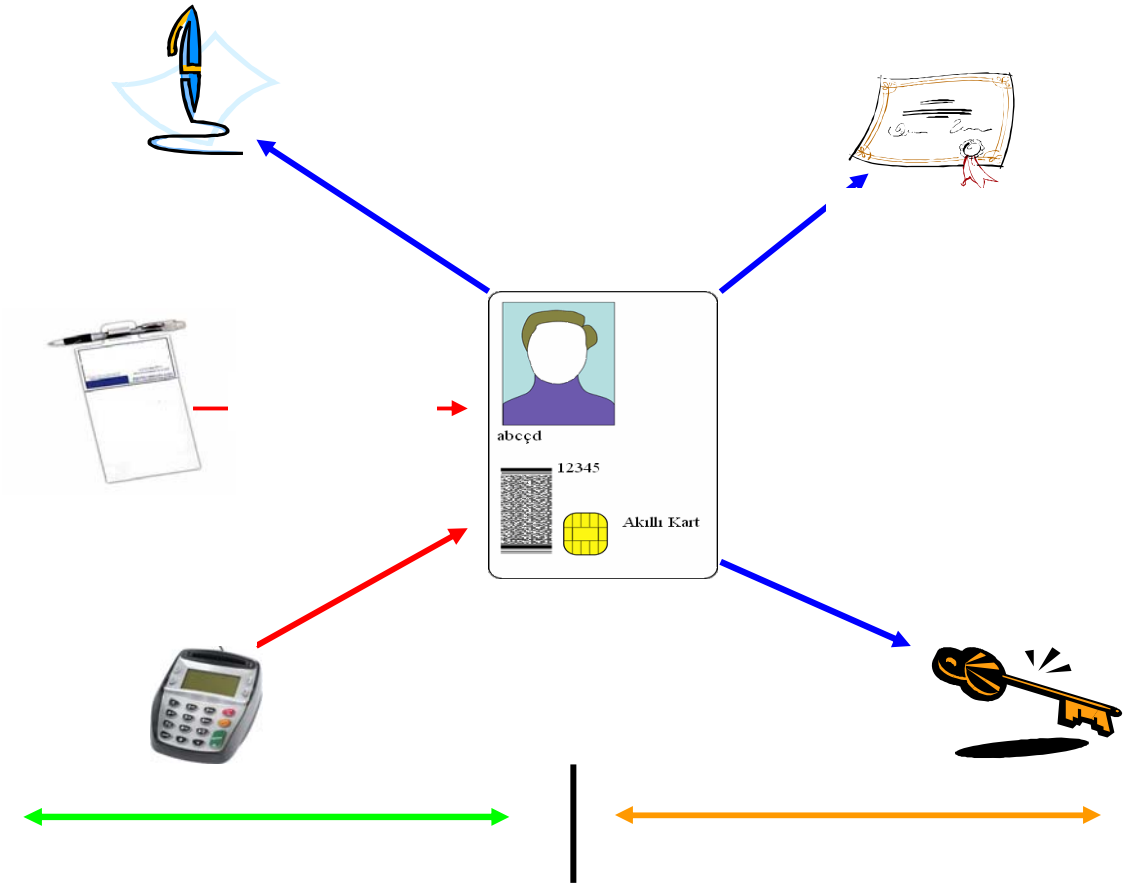
SCD'ye yalnızca oluşturma, kullanım ve imha süreçleri sırasında ulaşılabilir ve SSCD bu işlevlere erişim hakkına sahip olan tek aygıttır. SCD'nin depolanması ve kopyalanması e-imzaların yasal geçerliliği açısından bir tehdit oluşturabilir. Dolayısıyla SCD yedeklenmemeli ve SCD'nin kopyası aktarıldıktan sonra tamamen imha edilmelidir. Kopyalama ciddi problemlere neden olmasından dolayı yasaklanmalıdır [38].

İmza oluşturma aygıtının tanımı, "imza oluşturma verilerini uygulamak üzere kullanılan yapılandırılmış yazılım ya da donanım" olarak ifade edilmektedir.

SSCD'nin aşamaları iki tümleşik parçaya bölünmüştür [38]. İlk aşama başlatmadır. Bu aşamada SCD ve SVD oluşturulur. Bu süreç saldırılara karşı kuvvetle korunmalıdır. Bu aşama ayrıca SCD ve imzalayanın kişisel verilerini birbirine bağlayan nitelikli sertifikaların oluşturulmasını da içermektedir. İkinci aşama ise kullanım aşaması olarak adlandırılmaktadır. Burada veri imzalanmaktadır ve kullanıcı doğrulanmasının yapıldığı garanti edilmelidir. Bu durum bir PIN girilerek gerçekleştirilebilir.

Şekil 4.2'de SSCD aşamaları verilmiştir. Sol taraf verinin imzalandığı ve gösterildiği, verinin SSCD'ye aktarıldığı ve tanımlama işleminin gerçekleştirildiği kullanım aşamasını göstermektedir. Sağ tarafta ise, başlatma aşaması yani SCD ve SVD' nin oluşturulması ve sertifika oluşturulması gösterilmiştir.

SCD, SSCD'nin her iki aşamasında da korunmalıdır. Aksi takdirde SCD'yi eline geçiren bir saldıran istediği kadar çok sayıda sahte imza oluşturabilir. Dahası doğrulama verileri gizli tutulmalıdır. Çünkü eğer bir saldırgan kendisini imzalayan olarak tanımlıyorsa tekrar yasadışı imzalar oluşturabilir. Herhangi bir şahsın gizli anahtarı elde etmesini ve onu yanlış bir isimle tasdik etmesini önlemek üzere SCD'yi başlangıç aşamasında korumak gereklidir. Dahası, PIN'in okunması ya da DTBSR'nin geçersiz verilerle değiştirilmesinin de SSCD'nin güvenliğini riske atacak olmasından dolayı SSCD'nin kullanım aşamasında da güvenli olması gerekmektedir.



Şekil 4.2. SSCD Aşamaları [38]

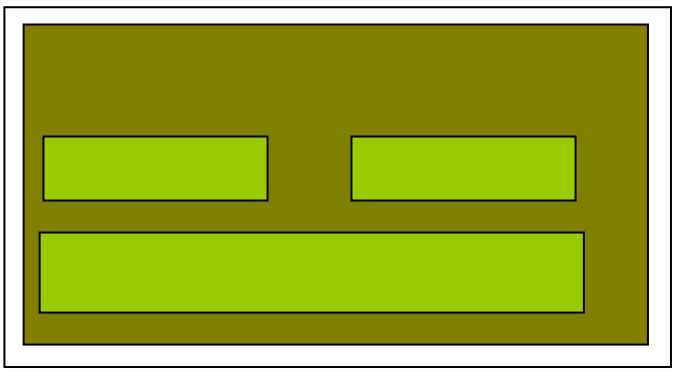
SSCD tasarımında iki farklı yaklaşım bulunmaktadır. İlk yaklaşım SCD ve SVD oluşturma yetkileri içeren ve ayrıca imzalayan tarafından veri imzalamada kullanılabilen bir aygıt oluşturmaktır. Ancak bu türden aygıt SCD oluşturma bütünsel işlevselliğini miras almasından ve dolayısıyla anahtar oluşturucunun kalitesinin düşük olabileceğinden dolayı çok karmaşık olması problemine sahip olabilir. İkinci yaklaşım ise şu ana kadar çok az sayıda aygıtın SCD / SVD oluşturmak üzere gerektiğini ve pek çok aygıtın ise imzalar oluşturmak üzere kullanılabileceği varsayımına dayalıdır. Böylece iki farklı aygıt uygulanmakta, birisi anahtar üretim sürecine ve yalnızca imzalanma için kullanılan ikincisine veri göndermek için tahsis edilmiştir.

SSCD PP içerisinde tanımlanan üç farklı tip bulunmaktadır. Bunlar

- SSCD Tip 1: SCD/SVD çifti oluşturma
- SSCD Tip 2: İmza oluşturma
- SSCD Tip 3: SCD/SVD çiftinin oluşturulması ve imza oluşturulması

olarak verilebilir. Bunları aşağıda açıklayalım.

SSCD Tip 1: E-imza sistemleri asimetrik kriptografi kullanmaktadır. Bu aygıt için iyi kalite elde edebilmek için, anahtar çiftlerinin oluşturulması kritik bir faktördür. Bu durumun bilinen bir gerçek olması nedeniyle, oluşturma süreci istenen güvenlik düzeyine ulaşmak için pek çok kaynak tüketebilir.

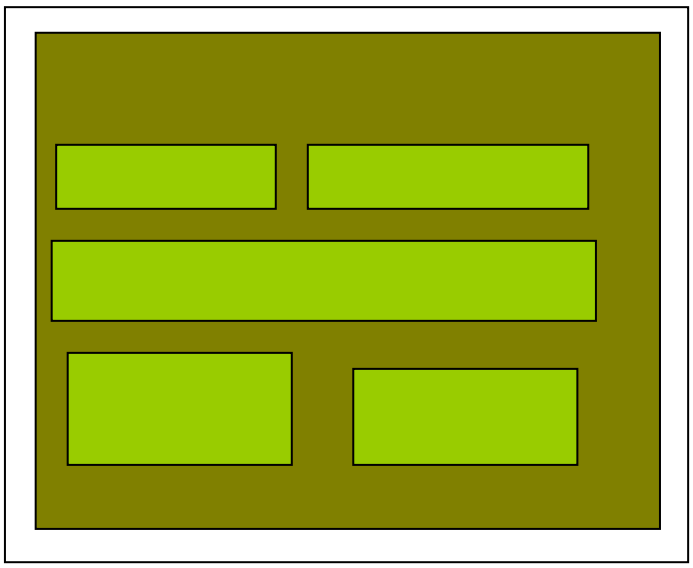


Şekil 4.3. SSCD Tip 1 Yapısı (SSCD PP)

İyi anahtarların oluşturulması sırasında, rasgele rakamların kalitesi belirleyicidir. Bu numaraların oluşturulması, anahtarların test edilmesinden ayrı olarak gereksinim duyulan hesaplama gücü göz önünde bulundurulduğunda çok "maliyetli" bir süreçtir. Böylece bu süreci başarmak üzere yalnızca birkaç aygıt kullanmak kitlesel üretim için daha uygundur.

SSCD Tip 1 sisteminin yapısı Şekil 4.3'te gösterilmiştir. Bir kısmı SCD/SVD çiftinin oluşturulmasında kullanılmaktadır. SCD aktarma bloğu, oluşturulan SCD'yi imzalayanın imzalamak için kullandığı aygıta göndermektedir. Bu aygıt bir Tip 2 SSCD'dir. SVD aktarma bloğu SCD'nin doğrulanması için gerekir.

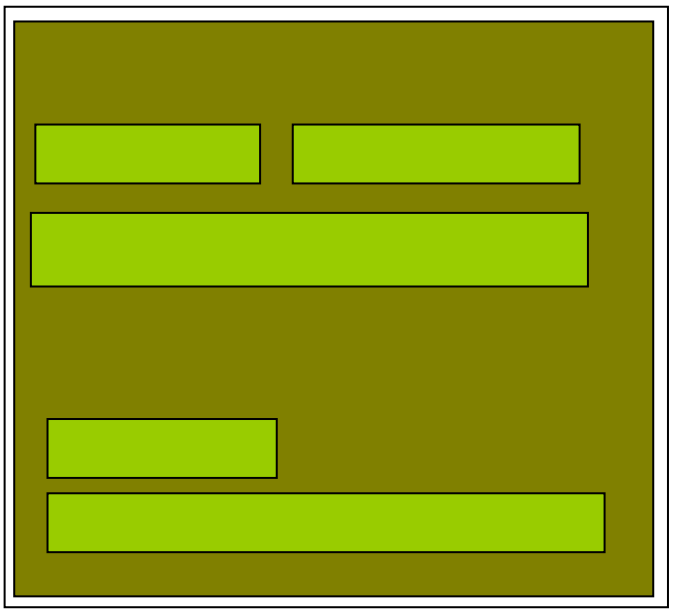
SSCD Tip 2: SSCD Tip 2 bir kullanıcı tarafından e-imzalar oluşturmak üzere fiili olarak kullanılan aygıttır. İşlevsel bloklar Şekil 4.4'te gösterilmiştir. Kişiselleştirme Bloğu, kullanıcıyı tanımlamak üzere gereken bilgiyi içerir (örneğin PIN). Kullanıcı onaylama bloğu ise imzalayanın aygıtı kendi kontrolü altında tutabilmesini sağlamak üzere gereklidir. SCD bir SSCD Tip 1'den aktarılmıştır. İmza oluşturma bloğu ise aygıtın çekirdeğidir ve imza oluşturma sürecini gerçekleştirir. SVD Giriş-Aktarma, SVD'nin SSCD Tip 1'den alınabileceği isteğe bağlı bir bloktur.



Şekil 4.4. SSCD Tip 2 Yapısı (SSCD PP)

SSCD Tip 3: SSCD PP açısından, SCD/SVD çiftini "kendi üzerinde" oluşturma işlevleri içeren ve aynı zamanda imzalar oluşturmak için de kullanılan bir aygıt SSCD Tip 3 olarak adlandırılmaktadır. Bu aygıt SSCD Tip 1 ve Tip 2'lerini tek aygıtta toplamaktadır. İki farklı SSCD tipini kullanan tasarımın avantajı, iletişim için daha az sayıda güvenli kanala gereksinim duyması ve böylelikle SSCD Tip 1 ve SSCD Tip 2'nin, bu gibi kanallar üzerinden iletişim kurmak zorunda olmamasıdır.

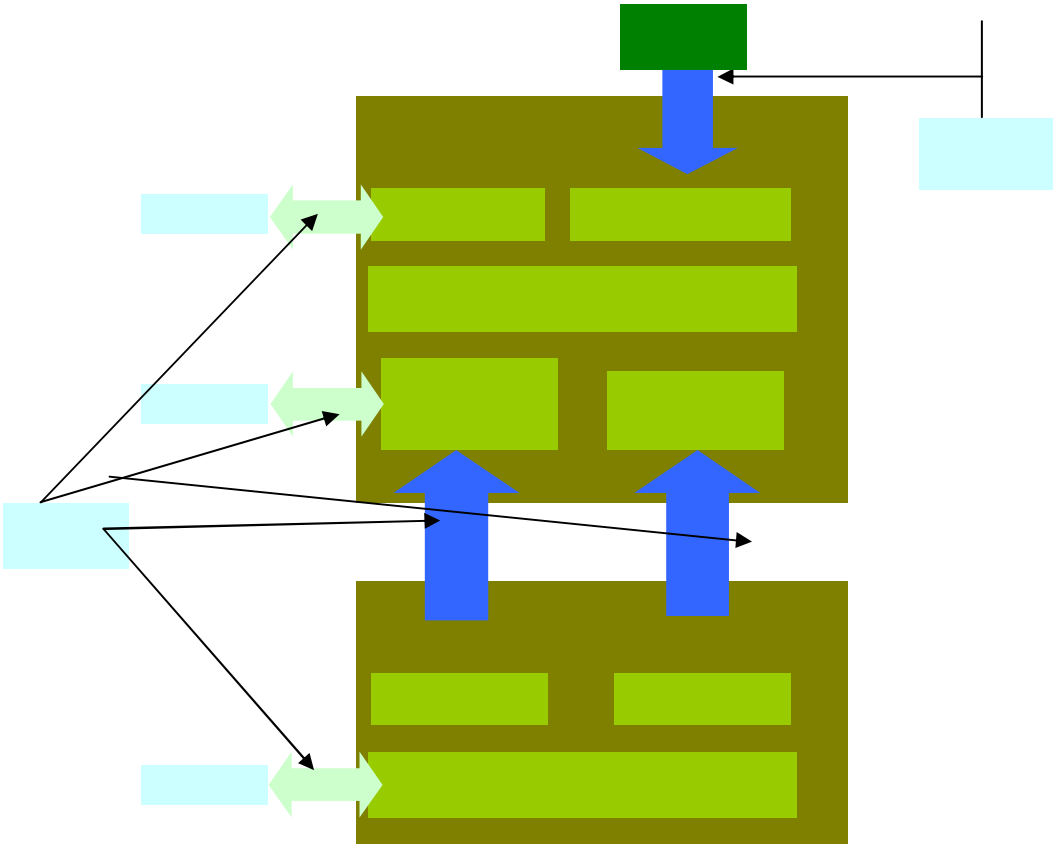
SSCD Tip 3'de, yapı taşları diğer aygıtlara benzemektedir. Kişiselleştirme, kullanıcıyı tanımlamak üzere gereken verileri içerir. Kullanıcı onaylama bloğu yalnızca imzalayanın aygıtı kullanmasını sağlamaktadır. İmzalar oluşturma, İmza Oluşturma bloğunda işlemden geçirilmektedir. SVD giriş bloğu, SCD'nin onayı için gereklidir. Son olarak SCD/SVD oluşturma bloğu gereken anahtar çiftini oluşturur.



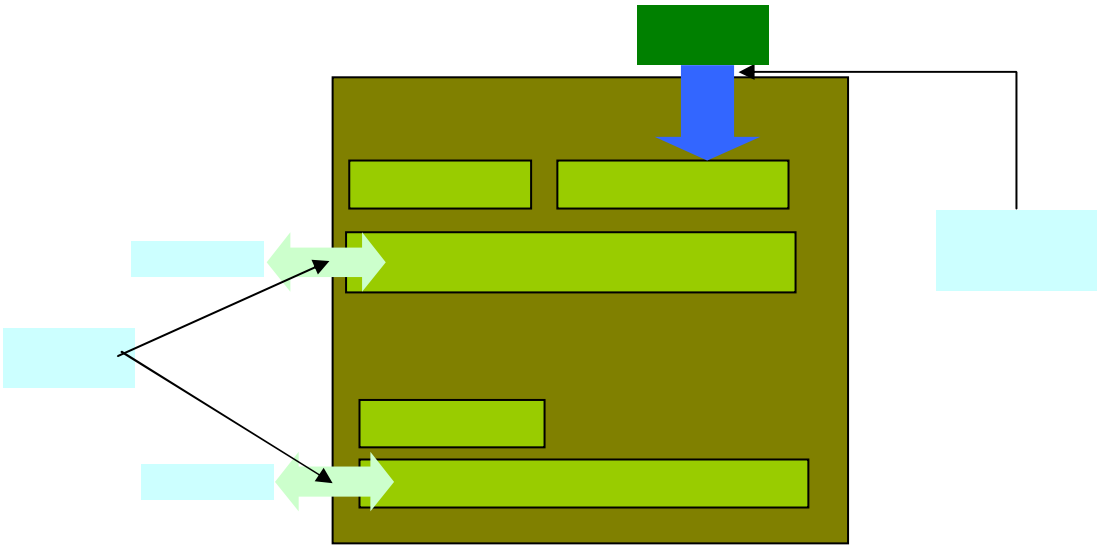
Şekil 4.5. SSCD Tip 3 Yapısı (SSCD PP)

SSCD tek başına çalışan bir aygıt olmaması nedeniyle, çalışmak üzere çevresiyle iletişim kurmak zorundadır. Ancak SSCD ve çevresindeki uygulamalar arasında aktarılan veriler hassastır ve korunması gereklidir. Bu durum sırasıyla tanımlanan

güvenilen kanallar ve güvenilen yollar kullanılarak gerçekleştirilmektedir [36].



Şekil 4.6. SSCD Tip 1 ve 2'nin İletişim Kanalları (SSCD PP)



Şekil 4.7. Tip 3 SSCD'nin İletişim Kanalları (SSCD PP)

SSCD'nin iletişim kurmak zorunda olduğu aygıtlar ve uygulamalar tanımlanmıştır ve SCA, sertifikalar oluşturmak üzere SVD'yi alması gereken sertifika oluşturma uygulaması (CGA) ve imzalayanın doğrulama verilerinin alınması için gereken insan arabirimidir (HI) [38]. Şekil 4.6'da SSCD Tip 1 ve Tip 2'nin bir kombinasyonu olarak oluşturulan bir sistemi göstermektedir.

SSCD Tip 3 sisteminin yapısı Şekil 4.7'de gösterilmiştir. Bu türden aygıtlar iki aygıttan oluşan diğer sistemden daha az sayıda iletişim kanalına gereksinim duyar.

Bir SSCD gerçekleştirilmişse, güvenli olup olmadığına karar verilmeden önce değerlendirilmesi gerekmektedir. Ancak bundan sonra gerçek yaşamda kullanılabilir.

5. MOBİL ELEKTRONİK İMZA MODELLERİ

Bu bölümde, me-imza hizmetleri verecek olan Elektronik Sertifika Hizmet Sağlayıcısı (ESHS) ile bu ortamların güvenli olması için kullanılabilecek mobil ESHS (MESHS) modelleri ile ülke örnekleri modelleri gözden geçirilmiştir.

5.1 Önerilen / Kullanılan Modeller

Birçok durumda, MESHS kullanıcının onayını almak için verileri son kullanıcının cihazına aktarmalıdır. Bazı durumlarda bu işlem zaman almaktadır çünkü:

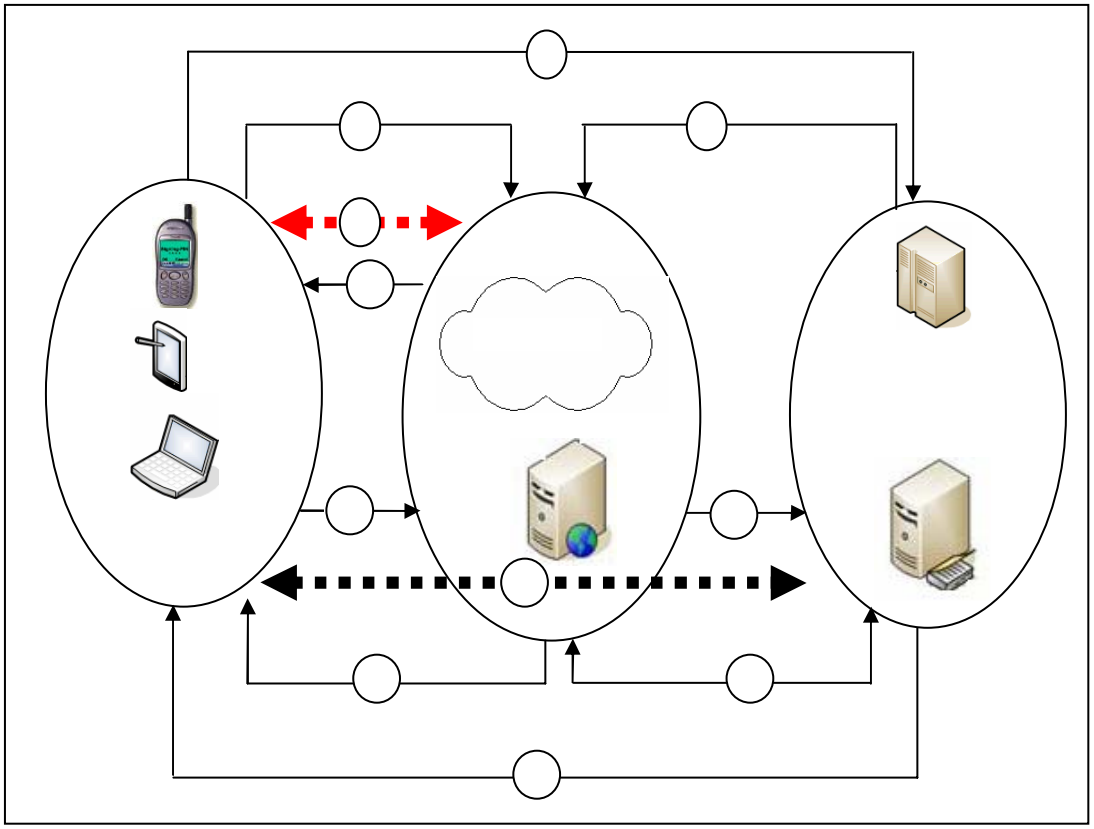
- Son kullanıcının olduğu yerde bağlantı kötü veya sorunlu olabilir
- Son kullanıcı onaylama işlemine hazır değil
- Farklı nedenler

MESHS harici aktarma işlemleri yapılmadığından bu duruma da "asenkron model" denilmektedir. Önerilen farklı modeller bulunmaktadır [46,50]. Modeller bu bölümün alt başlıklarda verilmiş ve kısaca açıklanmıştır.

5.1.1 Mobil ödeme modeli

Mobil ödeme (m-ödeme) modelleri, finansal kuruluşlarda para transferini güvenli olarak yapılabilmesi için güvenli bir ortam oluşturmak amacıyla sunulmaktadır. Bazı modeller mobil telefonla ulaşılabilen hesaplar için önceden ödenmiş çözümler de sunmaktadırlar. Bu hesaplarda toplanan paralar (e-para veya şirket paraları) ürün ve hizmet alımları için kullanılmaktadır.

Farklı m-ödeme modelleri arasında işlem yapmaya olanak tanıyan yapıların da oluşturulması için modeller bulunmaktadır. Örneğin MET (Mobile Electronic Transactions), möf (mobil ödeme forumu) vb. Bu girişimler mobil telefonların finansal hizmetler alanında kullanımını artırmakta, finansal hizmetlerde teknolojinin kullanımını teşvik etmekte ve mobil iletişim ile finans sektörüne ait standartları belirleyen yapılar arasında bağlantı sağlamaktadır [49]. Şekil 5.1'de bir mobil ödeme modeli sunulmaktadır.



Şekil 5.1. MET tabanlı mobil ödeme modeli [50]

Bu modelin işleyiş şekli, Şekil 5.1'de verilmiştir. İşleyiş şekli üzerinde verilen numaralara göre aşağıda açıklanmıştır;

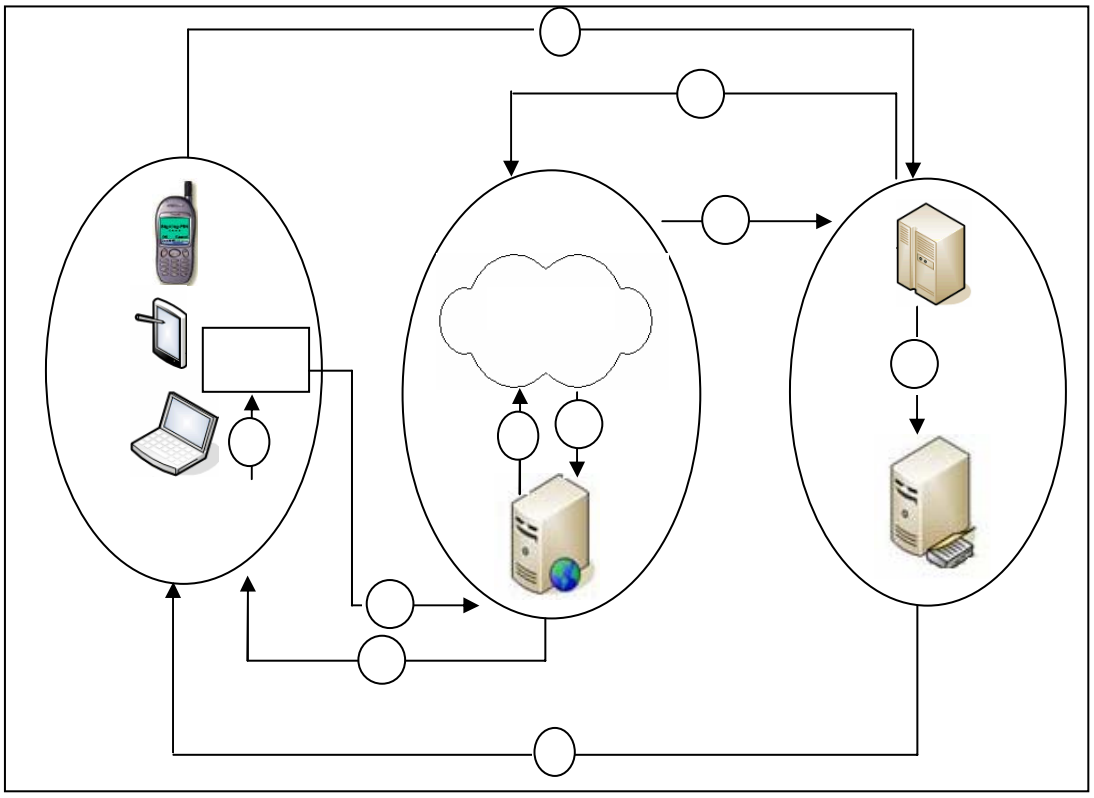
1. Kullanıcı satın almak istediği ürünü, uygulama sağlayıcısı (US) sistemine giriş yapar.
2. US, kullanıcının hizmet sertifikasına ihtiyaç duyar ve bunu kullanıcıya bildirir.
3. Kullanıcı ile ESHS arasında güvenli WTLS (Telsiz taşıma katmanı güvenliği) oturumu hazırlanır.
4. Kullanıcı satın almak istediği ürünleri seçer.
5. Kullanıcı satın almak istediği ürünün bilgilerini hizmet sağlayıcıya bildirir.
6. Bu esnada US, satın alma işlemini gerçekleştirmek için, hizmet sağlayıcıdan, doğrulama talebinde bulunur.
7. Doğrulama işlemi tamamlanırsa, ESHS, US'ye onay gönderir.
8. ESHS, kullanıcıya işlemin detaylarını ve tutar gibi bilgilerini imzalamak için kullanıcıya gönderir.

9. İmzalama işlemi tamamlandıktan sonra, kullanıcı imzalı belgeyi hizmet sağlayıcısına geri gönderir.
10. Hesap raporu aktarımı, ESHS ile US arasında gerçekleşir.
11. Mal gönderme işi artık gerçekleşebilir.

5.1.2. Senkron model

Bu modelin işleyişi Şekil 5.2 üzerinde verilen numaralara göre aşağıda açıklanmıştır;

1. Kullanıcı isteklerini US'ye bildirir (Örnek para çekmek işlemi).
2. US (örnek banka) kullanıcının bilgilerini doğrulatır.



Şekil 5.2. Senkron model

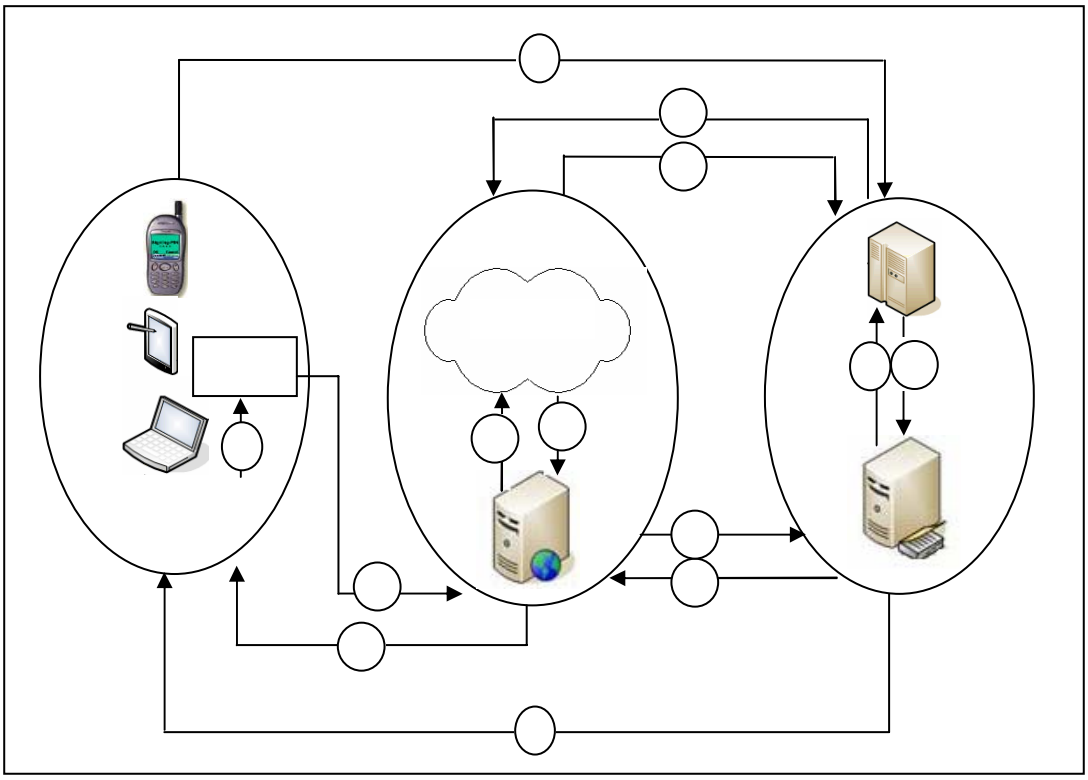
3. US kullanıcıya, imzasının doğrulatması için hizmet sağlayıcısından imzasını isteyeceğine dair bilgi gönderir.
4. US, MESHS'dan kullanıcın imzasını ister.
5. MESHS, US'dan kullanıcının bilgilerini alır, imza talebi işlemini başlatır.

6. MESHS, kullanıcıya me-imza isteme talebi gönderir.
7. Mobil kullanıcın cihazı ekranda imzalanacak metni gösterir sonra imzasını girilmesini ister (örneğin: PIN şifresi olarak).
8. Kullanıcı şifresini (imzayı) tamam tuşuna basarak MESHS'na göndermiş olur.
9. MESHS'ı kullanıcıdan gelen imzayı doğrulatır (doğru girilip girilmediğini, geçerliliği, son kullanım tarihi gibi).
10. MESHS'ı mobil imza yöntemi cevabını US'ye gönderir kullanıcının imzası ile veya imzasız.

5.1.3. Asenkron-istemci sunucu model

Bu modelin işleyiş şekli Şekil 5.3 üzerinde verilen numaralara göre aşağıda açıklanmıştır;

1. Kullanıcı isteklerini US'ye bildirir (örnek para çekme işlemi).
2. US (banka) kullanıcının bilgilerini doğrulatır.
3. US kullanıcıya, imzasının doğrulatması için hizmet sağlayıcıdan imzasını isteyeceğine dair bilgi gönderir.
4. US, Me-imza hizmet sağlayıcıdan (MESHS) kullanıcın imzasını ister.
5. MESHS, US'dan kullanıcının bilgilerini alır, imza talebi işlemini başlatır.
6. MESHS'ı mobil imza yöntemi cevabını mobil imzanın işleme alındığını ve cevap beklendiğini bildiren durum ile US'ye gönderir.
7. US, işlemi kayda alır.
8. MESHS, Kullanıcıya Me-imza isteme talebi gönderir.
9. Mobil kullanıcın cihazı ekranda imzalanacak metni gösterir sonra imzasını girilmesini ister (örneğin: PIN şifresi olarak).
10. Kullanıcı şifresini (imzayı) tamam tuşuna basarak MESHS'na göndermiş olur. Burada MESHS'ı imzayı doğrulatır ve geçerliliğini dener.
11. US, standart durum talebini MESHS'a gönderir.
12. MESHS'ı durum cevabını US'ye göndermek üzere hazırlar.
13. Durum cevabını US'ye gönderilir.

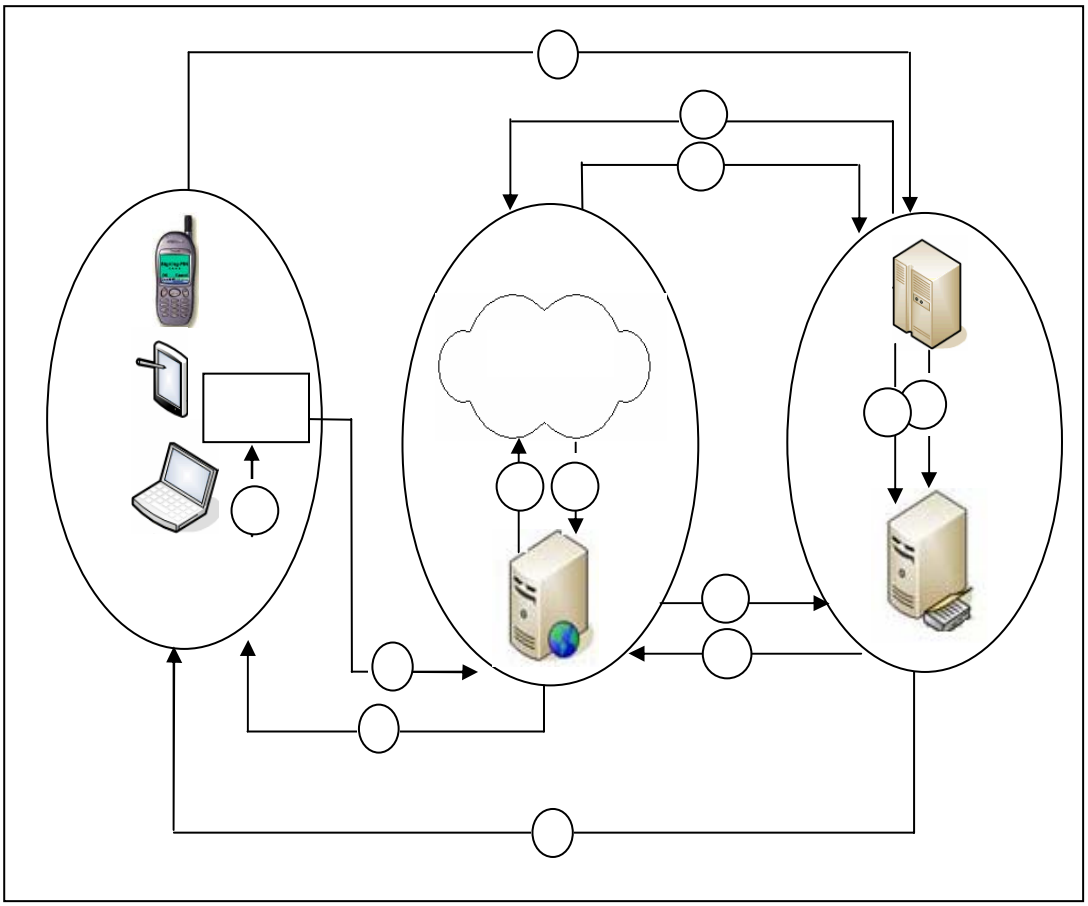


Şekil 5.3. Asenkron-İstemci Sunucu model

5.1.4. Asenkron-sunucu sunucu model

İşleyiş şekli Şekil 5.4'te numaralarla işaretlendiği gibi açıklamaları sıralanmıştır;

1. Kullanıcı isteklerini US'ye bildirir, (örnek para çekmek işlemi)
2. US (banka) kullanıcının bilgilerini doğrulatır
3. US kullanıcıya, imzasının doğrulatması için hizmet sağlayıcısından imzasını isteyeceğine dair bilgi gönderir
4. MESHS, hizmet sağlayıcısından kullanıcının bilgilerini alır. İmza talebi işlemini başlatır
5. MESHS'ı me-imzalama isteğini US'ye gönderir, imza talebinin işleme alınıp da doğrulatmasını beklendiğini belirten durum ile
6. MESHS, Kullanıcıya me-imza isteme talebi gönderir.
7. Mobil kullanıcın cihazı ekranda imzalanacak metni gösterir sonra imzasını girilmesini ister (örneğin: PIN şifresi olarak)



Şekil 5.4. Asenkron-Sunucu Sunucu model

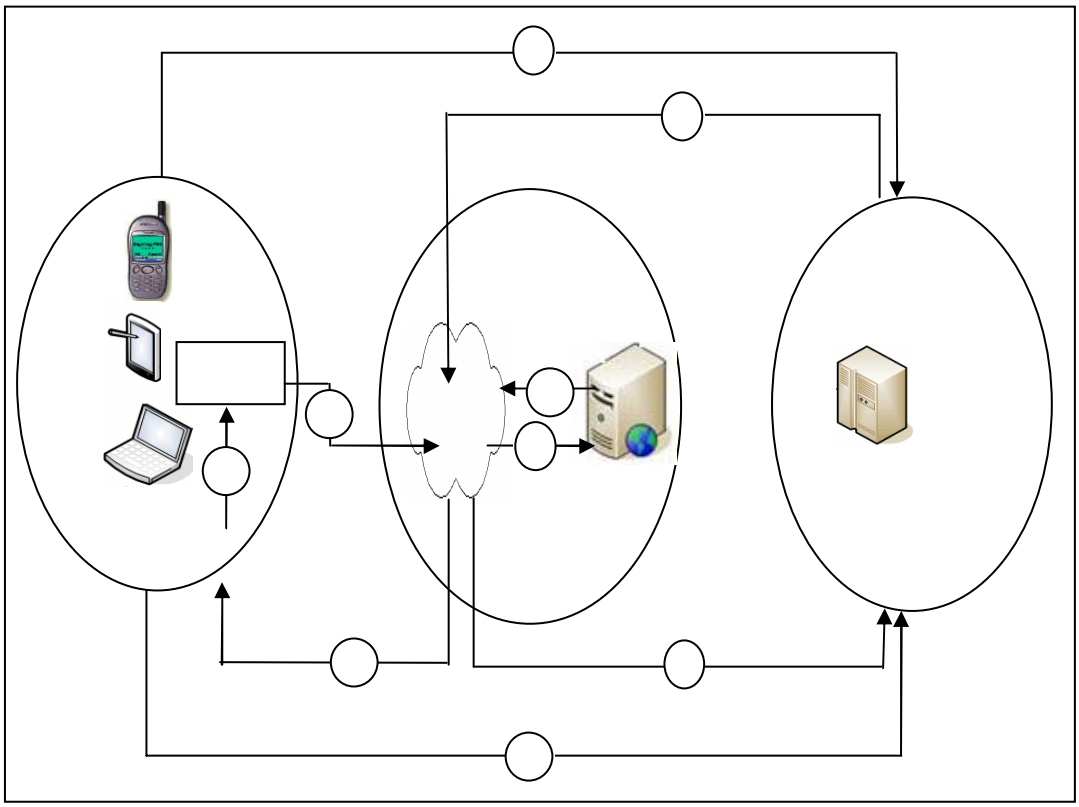
8. Kullanıcı şifresini (imzayı) tamam tuşuna basarak MESHS'na göndermiş olur.
9. MESHS'ı imzayı doğrulatır ve geçerliliğini dener son kullanım tarihi
10. MESHS'ı mobil imza ihtar talebini usanın mobil imza ihtar yöntemine gönderir
11. US imza ihtarını işleme alır
12. US mobil imza ihtar cevabını MESHS'na geri gönderir

5.2. Farklı Ülkelerde Uygulanan Modeller

5.2.1. İngiltere

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. Bu hizmette, Ticaret ve Sanayi Bakanlığına ait bir web

platformu ara yüzünde, mobil cihaz 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 bağlanıp kendi bilgilerini doldurmaları sonucunda oluşturulan çıktının mobil cihaza gönderilerek imzalanması sağlanmaktadır [3]. Bu işlemlerin akışını gösteren altyapı Şekil 5.5'te verilmiştir.



Şekil 5.5. İngiltere'de uygulanan me-imza altyapısı [51]

Bu modelin işleyiş şekli Şekil 5.5 üzerinde verilen numaralara göre aşağıda açıklanmıştır;

1. Kullanıcı işlem yapmak istediği uygulamaya bağlanır.
2. Uygulamadaki güvenli ağ geçidinden kesin veriyi imzalamak için bir talep gönderir. İstek, çalıştırılabilen, kullanıcıya gönderilebilen ve cihazla uyumlu hale çevrilebilen SMS bit koda dönüştürülerek MESHS'na gönderilir.
3. US MESHS'na kullanıcının mobil imza talebini gönderir.

4. İmzalama isteği, MESHS'den GSM işletmecisi aracılığıyla kullanıcıya iletilir.
5. Kullanıcı bu talebi kendi me-imzasıyla onaylamaktadır. Bu işlem kullanıcının imzalama PIN kodunu girerek, gelen bilgiyi sayısal olarak cihazda imzalamasıyla sağlanır.
6. İmzalanmış talep GSM işletmecisi aracılığı ile MESHS'na iletilir.
7. MESHS'nde imzanın doğrulama işlemi gerçekleştirilir. Gelen imzayı Hafifletilmiş Dizin Erişim Protokolü'ne (LDAP) gönderir
8–9. LDAP' dan gelen yanıt ile birlikte imzanın doğrulanıp doğrulanmamasına bağlı olarak imzalama "başarılı" ya da "başarılı değil" diye bir cevap oluşturulup uygulama sunucusuna geri gönderilir.

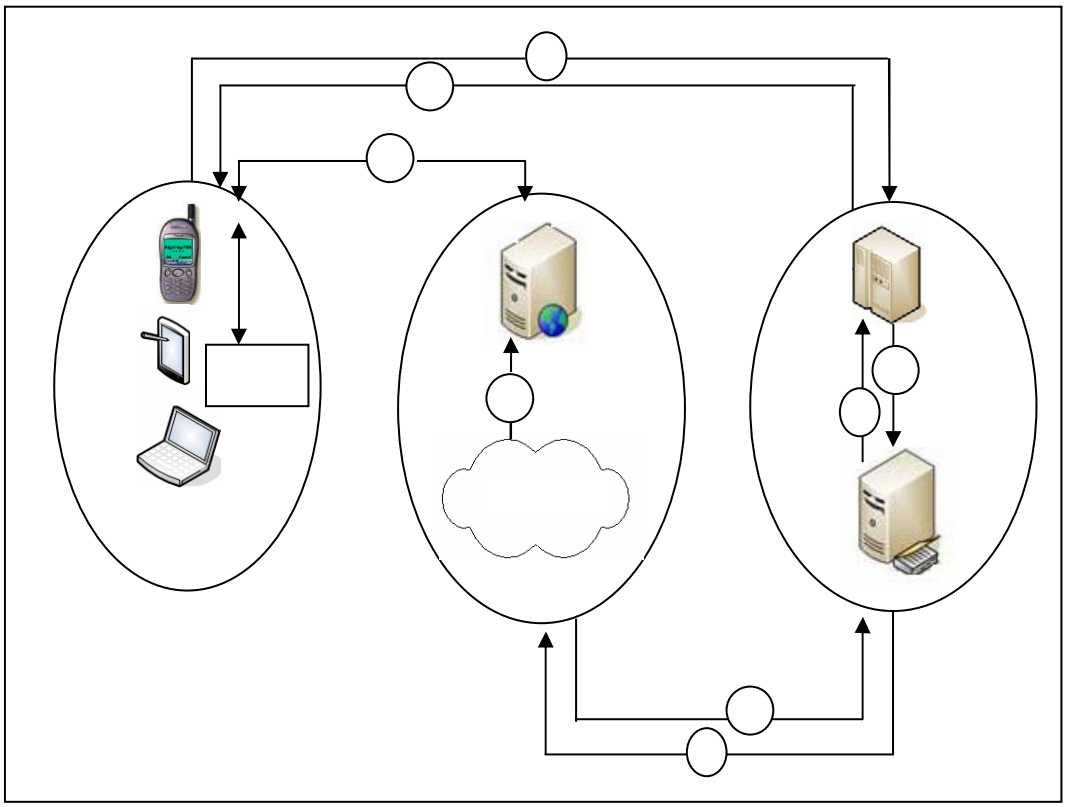
5.2.1. Singapur

Sistem Bilimleri Enstitüsü (Institute of Systems Science – ISS) tarafından me-imza hizmetinin oluşturulabilmesi için me-imza altyapısı Şekil 5.6'da sunulmuştur. Kullanıcı me-imza kullanmak için kayıt olduğunda kendisine verilen PIN kodu ve her işlem için üretilen eşsiz anahtar eşleştirilerek çevrim içi işlemlerin güvenli bir şekilde yapılmasına imkân sağlamak üzere her kredi kartında doğrulama işlemi yapılmaktadır [52].

Bu modelin işleyiş şekli Şekil 5.6 üzerinde verilen numaralara göre aşağıda açıklanmıştır;

1. Kullanıcı, öncelikle mobil cihazı vasıtasıyla m-bakkal uygulamasının web sitesine girerek, arzu ettiği malları satın almak üzere talepte bulunur ve kredi kartına ait anahtarı girer.
2. Kredi kartı, veri tabanında doğrulanır.
3. İşlemin gerçekleştirilmesini sağlamak amacıyla anahtarı bir kerelik üretmek üzere me-imza sunucusuna ilgili talep gönderilir.
4. SMS sunucusu aracılığıyla uygun mesaj haline dönüştürülür.
5. Kredi kart sahibine (kullanıcıya) GSM şebekesi kullanılarak ulaştırılır. SMS sunucusu mesajı ile gönderilir. PIN kodunu ve anahtarı kişinin girmesini talep

eden sayfa, mobil cihaz ekranında gözükür. Kullanıcının talebe verdiği cevap aynı yol izlenerek me-imza sunucusuna iletilir.



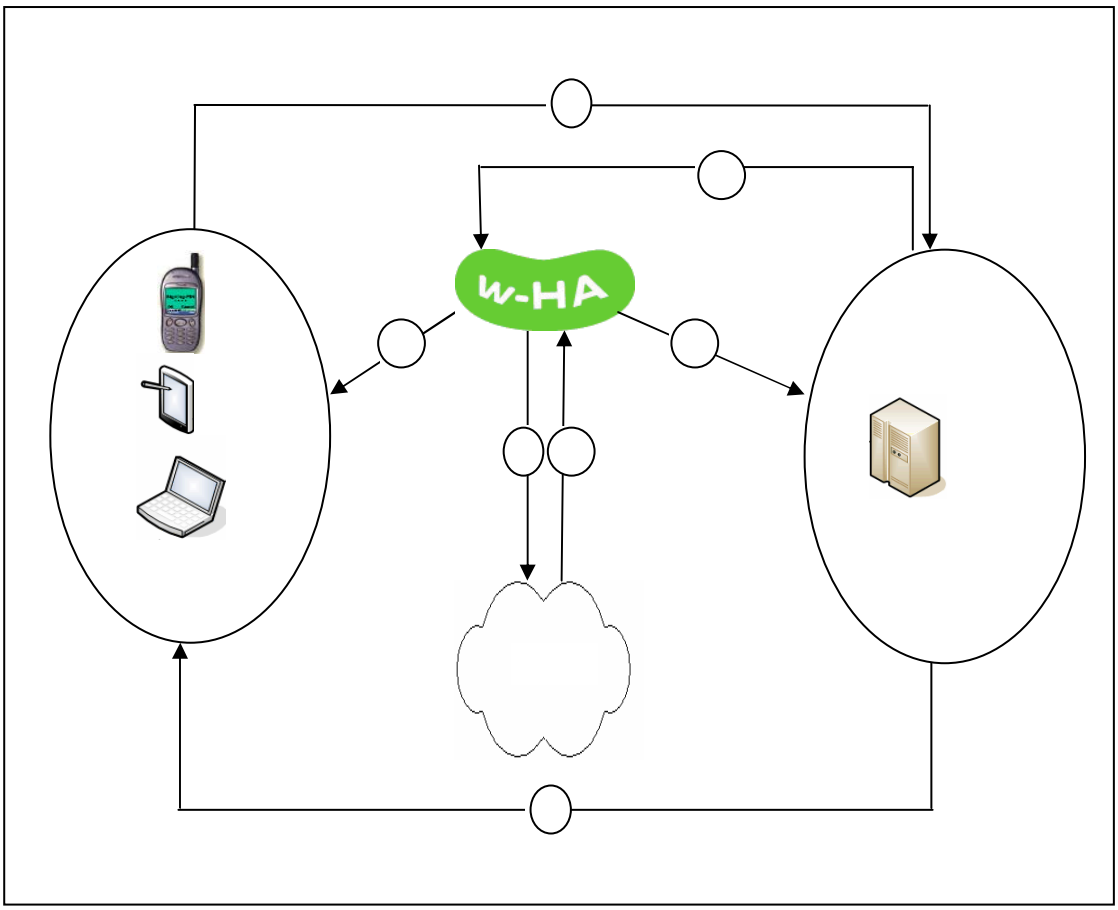
Şekil 5.6. Singapur'da uygulanan me-imza altyapısı

6. Me-imza sunucusunda gerekli aktarma yapılıp doğrulama işlemi gerçekleştirilir. Ödenecek miktar ve ticarethanenin adı gibi detay bilgiler dâhil olmak üzere gerekli bilgileri içeren teyit bilgisi veri tabanına iletilir.
7. Veritabanına gelen doğrulama bilgisi US'ya iletilir.
8. İşlemin tamamlandığına ilişkin bilgi mesajı kişinin mobil cihazına gönderilir ve işlem tamamlanmış olur [3].

5.2.3. Fransa

Fransa'da Orange ve Nestlé Grand Froid'ın başarıyla testlerini tamamladıkları mobil cihaz aracılığıyla dondurma siparişi verme, Orange ve Parkeon'un ortaklaşa yaptıkları mobil cihaz aracılığıyla park ücreti ödeme uygulamaları dikkat çeken me-

imza uygulamalarına örnek olarak verilebilir. Bu modelde Mobil Cihaz Aracılığıyla Park Ücreti Ödeme İşlem Basamakları France Telekom'un me-imza uygulamaları için kullandığı MAAA Şekil 5.7'de verilmiştir [53].



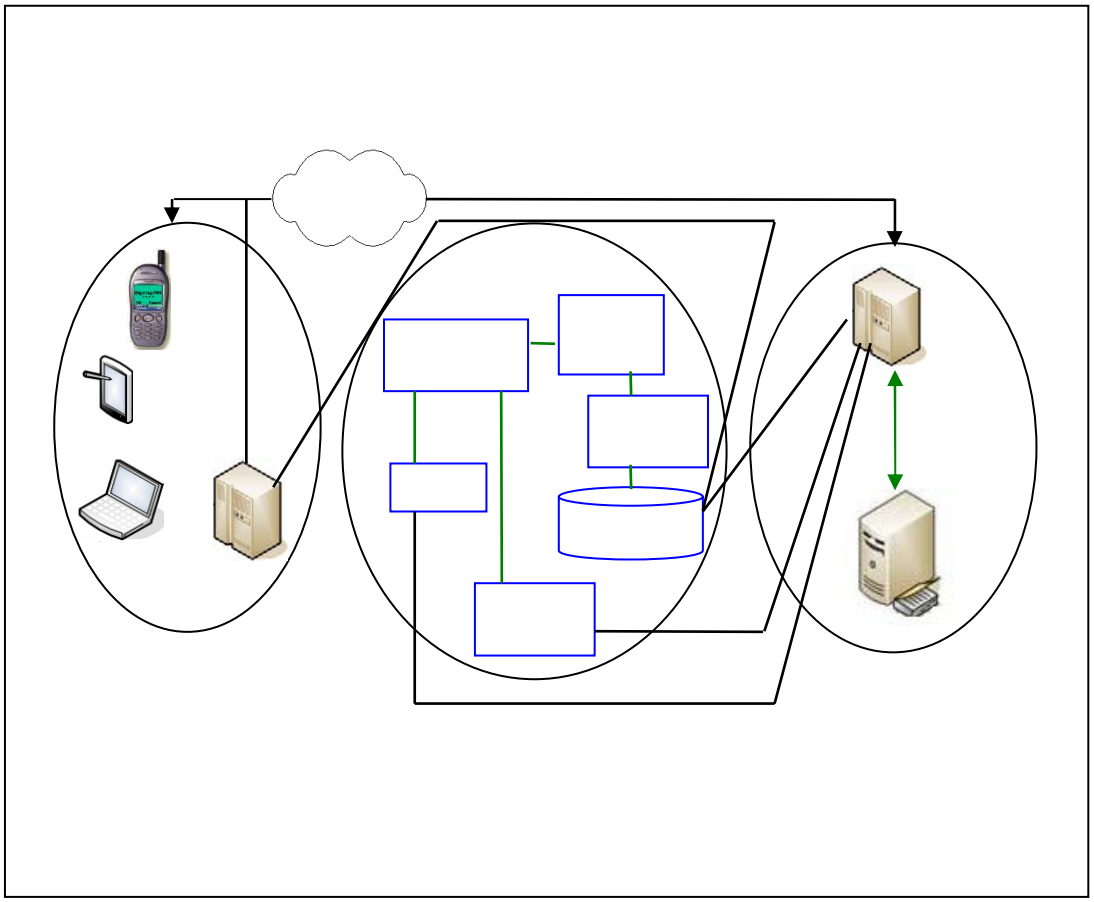
Şekil 5.7. Fransa'da uygulanan me-imza altyapısı

Bu altyapı ile küçük çaplı ödemelerin sabit, web ve mobil ortamlar üzerinden yapılabileceği çözümler sunulmaktadır. Bu yapıda:

1. İlk olarak hizmet sağlayıcısından alınan hizmet türü seçilir.
2. Seçilen hizmet için w-HA platformundan para aktarmayı doğrulama isteğinde bulunulur.
3. w-HA platformu bu isteği istemci işletmeciye bildirir ve doğrulama istenilir.
4. İşletmeci doğrulama işini onaylamaktadır.
5. Bu aktarma isteğinin kabul edildiği kullanıcıya bildirilir.
6. Dağıtım için hizmet sağlayıcısına yetki verilir.

7. Sipariş verilen ürün kullanıcıya bir yolla dağıtılır.

5.2.4. Finlandiya

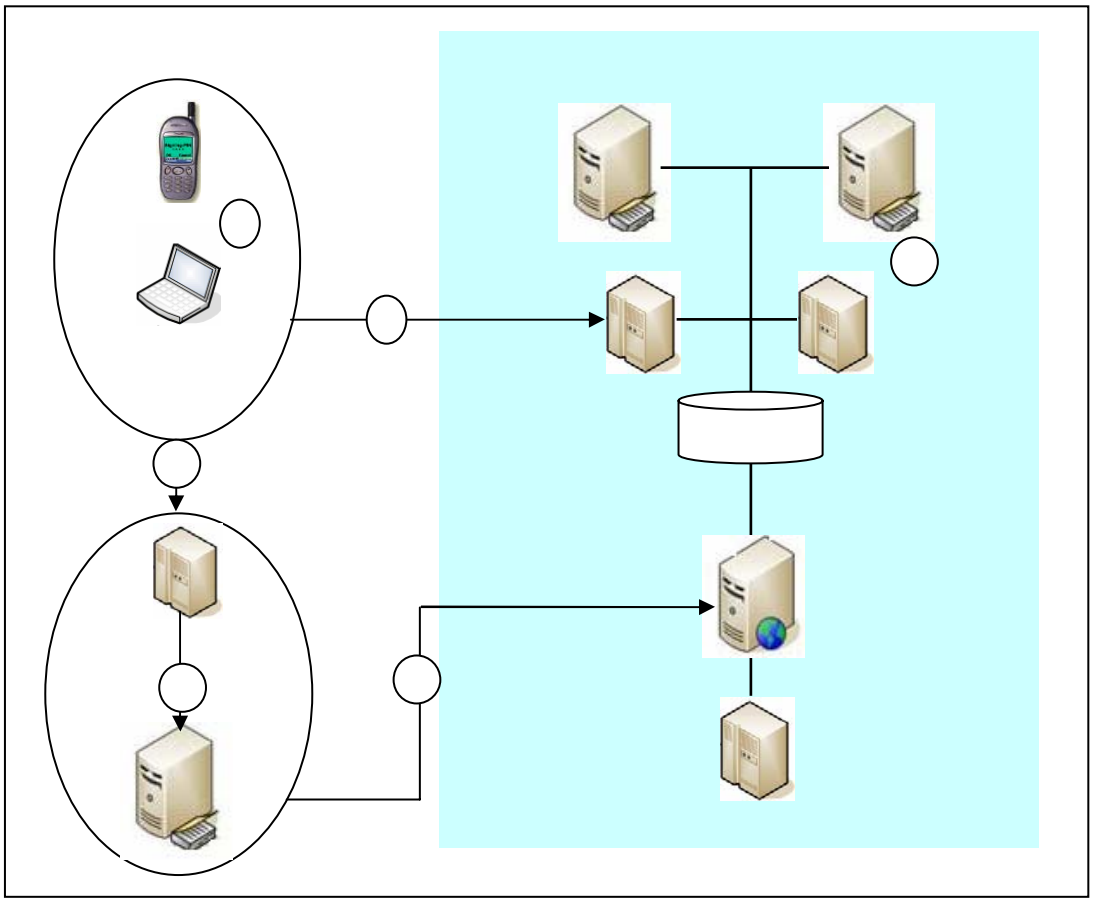


Şekil 5.8. Finlandiya'da uygulanan me-imza altyapısı

Mobil cihaz penetrasyonu %91 olan ülkede hükümet bu işlemin gerçekleştirilmesi için iki mobil işletmeci olan Elisa ve TeliaSoneria ile aynı proje kapsamında anlaşma imzalamıştır. Me-imza'ya büyük ilgi gösteren Finlandiya Hükümeti projeyi bilgi toplumu oluşturmada en önemli projelerden birisi olarak gördüğü için desteklemektedir . Şekil 5.8'de belirtilen model Finlandiya'da MESHS'na adres değişikliğinin bildirilmesi ve Nüfus İdaresindeki vatandaş bilgilerinin doğrulanması gibi iki uygulama için kullanılan MAAA olarak kullanılmaktadır [3, 54].

5.2.5. Norveç

Norveç'te e-imzada kullanılan algoritmalara ilişkin bir düzenleme yapılmamıştır ve herhangi bir standardın uygulanması hukuken zorunlu değildir. Norveç'te güvenli e-ticaret ve bankacılık işlemleri için birçok me-imza kullanım imkânı sağlayan farklı modeller mevcuttur. Norveç'te NES yayımlayan ESHS olan ve mobil sertifikaların sahibi ZebSign tarafından kısa bir süre sonra hizmet verilmeye başlanacak olan altyapı Şekil 5.9'da verilmiştir [3, 55].



Şekil 5.9. Norveç'te uygulanan me-imza altyapısı

Bu modelin işleyiş şekli Şekil 5.9 üzerinde verilen numaralara göre aşağıda açıklanmıştır;

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 US, 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].

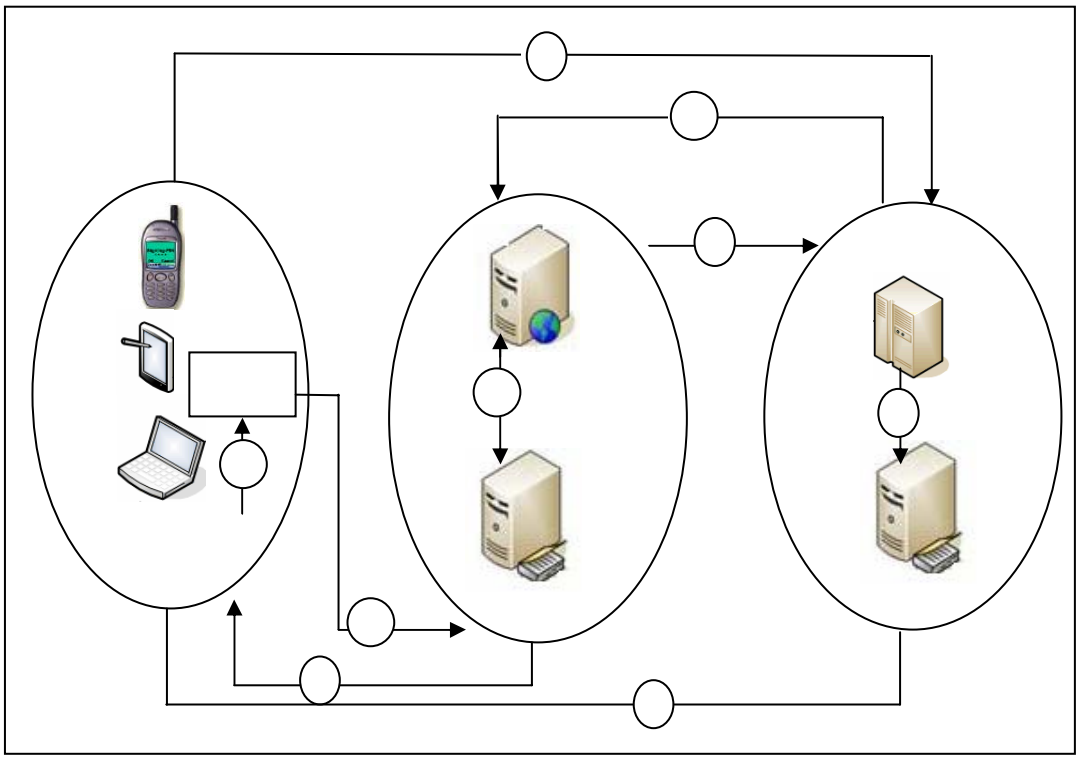
5.2.6. Türkiye

Türkiye'de ilk me-imza çalışmasını gerçekleştiren Türkcell, 50 bin üzerinde me-imza kullanıcısı ile mobil kullanıcılarına güncel mobil hizmeti sunan dünyanın en büyük operatörlerinden biridir [3]. Test çalışmalarında me-imza için güvenli taşıma ortamı olarak Gemolta ürünü olan EAL4+ SIM kartı kullanılmakta ve SIM kart dışında ek bir donanıma ihtiyaç duyulmamaktadır. Bu operatörün e-imza ve AAA olarak e-Güven'le iş birliği yapılmıştır e-Güven, Türkcell'de me-imza konusundaki çalışmalarına 2006 yılı Ocak ayında başlamıştır ve me-imzanın e-imza kullanımını etkinleştireceğine inanmaktadır. Türkcell ve e-Güven tarafından me-imzanın kullanılabilmesi için tasarlanan işlem basamakları aşağıda gösterilmiştir [56].

Bu modelin işleyiş şekli Şekil 5.10 üzerinde verilen numaralara göre aşağıda açıklanmıştır;

1. Kullanıcı, US'ye girerek işlemini yapar.
2. Uygulama kullanıcının imzalama talebini Türkcell servisine iletir.
3. Türkcell, gelen talebi kullanıcının mobil cihazına SMS protokolünü kullanan yapılandırma mesajı olarak gönderir.
4. Kullanıcı mobil cihazına gelen mesajdaki özet değer ile uygulamadaki karşılaştırıldıktan sonra imzalayarak Türkcell'e geri gönderir.
5. İmzalı işlem Türkcell aracılığıyla banka uygulamasına iletilir.
6. Uygulama gelen me-imzanın doğruluğunu kontrol etmek için e-Güven'in sunucusuna gönderir
7. Sunucuda atılan imzanın doğruluğu kontrol edildikten sonra zaman damgası eşliğinde uygulamaya geri gönderilir.

8. Banka uygulamasında imzanın kontrol sonucuna göre işlem yapılır.
9. Kullanıcının mobil cihazına bilgi mesajı gönderilir.



Şekil 5.10. Türkcell tarafından banka uygulaması için tasarlanan altyapı

5.3. Genel Değerlendirme

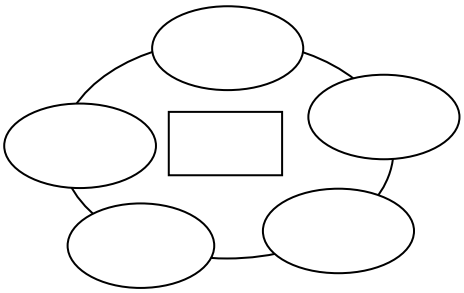
Genel Olarak ETSI'nin sunduğu modellerde, Asenkron-İstemci Sunucu Model ve Asenkron-Sunucu Sunucu Model iyi ve avantajlı gözükse de bu tez kapsamında incelenen ülkelerdeki durumlar daha farklıdır. Türkiye, Singapur ve İngiltere ülkelerindeki model senkron model olarak tasarlanmış, Fransa'da ise model hemen hemen Asenkron-Sunucu Sunucu Modeli olarak tasarlanmıştır.

6. MOBİL ORTAMLARDAKİ ZAYIFLIKLAR VE OLASI SALDIRILAR

Günümüz mobil sistem kullanıcılarında ortak olan bir konu "güvenliktir" [57]. Bilgi güvenliği kavramı içinde kişisel ve kurumsal güvenlik gibi temel hususlar yer almakla birlikte, bunların altında iletişim ağı güvenliği, işletim sistemi güvenliği, veri tabanı güvenliği, internet erişim güvenliği, terminal cihazı ve sistem güvenliği gibi oldukça önemli hususlar bulunmaktadır. Bu bölümde, GSM güvenlik mekanizmaları, saplanan güvenlik servisleri, güvenlik algoritmalar ile bu sistemlere yapılan saldırılar özetlenmiş, me-imza sisteminin korunması için yapılması gerekçeler ile yüksek seviyede bir mobil imza hizmet ortamı için oluşturulması gereken mimarisine yer verilmiştir. Bu hususlar alt başlıklarda sunulmuştur

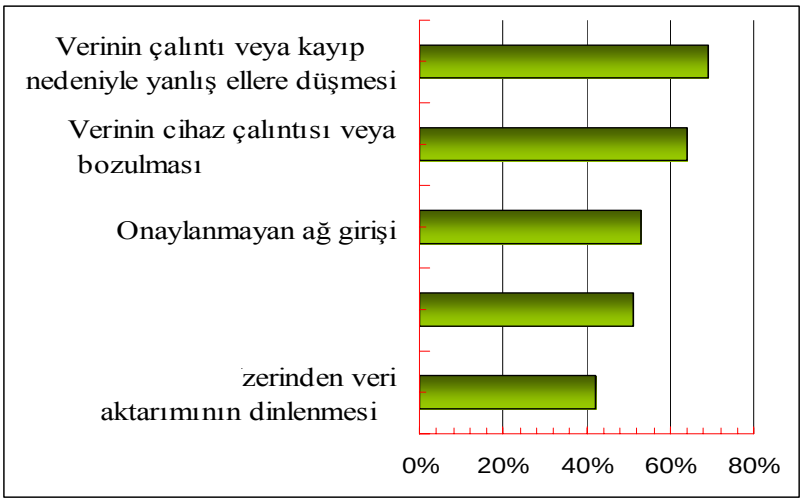
6.1. GSM Güvenlik Mekanizması

GSM ağlarındaki abone kimlik modülü (SIM)'in görevi, sadece yetkili kullanıcıların ağa erişebilmelerini sağlamaktır. Bir kullanıcıyı tam olarak onaylamak için ağ, veriyi depolayabilmeli, depolanmış veriye yetki dışı erişimden koruyabilmeli ve güvenlik şartları altında şifreli algoritmayı uygulayabilmelidir. SIM ve mobil cihaz arka plan sistemleri ve hizmetleri ile kullanıcıyı korumaya çalışır. GSM ağlarında temel güvenlik bileşenleri Şekil 6.1'de verilmiştir [58]. Şekilde görüldüğü gibi GSM ortamında güvenlik şifrelerine PIN, yönlendirme, gizlilik ve kimlik doğrulama bileşenleri ile yapılmaktadır.



Şekil 6.1. GSM güvenlik bileşenleri

Mobil istasyonunun[4] hangi açıklardan daha çok etkileneceği ve hangi tehditler altında ciddi kayıplara yol açtığını anlamak için yapılan bir anket sonucu, "en önemli mobil güvenliği meselesi nedir?" sorusuna alınan cevabın grafik gösterimi Şekil 6.2'de verilmiştir



Şekil 6.2. Mobil cihazları ve kullanıcıları [59]

Bu saldırıların nasıl gerçekleştirildiğini ve mobil ortam güvenlik seviyesinin ne kadar ihlal edildiğini anlamak için önce GSM ağında üç ana bileşeni gözden geçirmekte fayda vardır. Bunlar [69]:

• Kullanıcının tek bir kimliğini sağlayan abone kimliği modülüne (SIM) sahip mobil istasyonu (veya mobil telefon)dur.

• Diğer mobil/sabit hat kullanıcılarına mobil istasyon üzerinden kullanıcıyı bağlayan baz istasyonu alt yapısıdır (BSS).

• Farklı mobil istasyonlara baz istasyonu kontrolörleri (BSCs) ve baz alıcı verici istasyonları (BTSs) yoluyla sabit ağlardan gelen çağrıları yönlendirebilen ağ alt sistemi (NSS)dır.

GSM ağları üzerinde SIM onaylama prosedürü, abonenin SIM kartının geçerliliğini kontrol eder ve ardından mobil istasyona özel bir ağ üzerinde onay verilip verilmediğini kontrol eder. Onaylama sürecine katılan taraflar, gri listede olmayan

[4] SIM kart ve mobil cihazı ikilisi için "mobil istasyonu" kavramı kullanılır

(çalınmamış) ve onaylı el cihazı olan SIM kartın son kullanıcısı veya sahibi ve ağ operatörüdür [60].

6.2. GSM Tarafından Sağlanan Güvenlik Servisleri

GSM in sağladığı güvenlik servisleri üç kategoride sınıflandırılabilinir. Bunlar kimlik doğrulama (authentication), kimliğin gizlenmesi (anonymity) ile kullanıcı veri ve sinyal korunmasıdır (user data and signaling protection) . bu servisler aşağıda alt başlıklarda açıklanmıştır.

6.2.1 Kimlik Doğrulama (Authentication)

Kimlik doğrulama işlemi, GSM ağ operatörü tarafından SIM kart sahibinin kimliğinin tanımlanması ve doğrulanması için yapılır. Bu teknik "meydan okuma – karşılık verme" (Challenge and Response) prensibine göre çalışır. Kimlik doğrulama güvenlik mekanizmasının başlıca amacı yetkilendirilmemiş ve onaylanmamış kullanımlara karşı ağ sistemini korumaktır. Ayrıca bu mekanizma sayesinde, başkasının yerine geçilerek yapılmak istenen izinsiz ve yasadışı konuşmalar da engellenmiş olur. Kimlik doğrulama işlemi şu şekilde gerçekleştirilir: 128 bit uzunluğundaki rasgele atanan bir sayı (RAND) mobil istasyona (MS) gönderilir. Daha sonra MS bu sayıyı ve SIM kartta bulunan kullanıcı kimlik doğrulama anahtarı Ki'yi girdi olarak alıp A3 algoritmasında kullanır. Bunu takiben 32 bit uzunluğunda "işaretlenmiş karşılık" (signed response) olarak bilinen SRES çıktısını üretir. Bu çıktı MS den GSM ağına gönderilir. Ki, GSM ağ sisteminde de mevcut olduğundan ve RAND sayısı da bilindiğinden dolayı GSM ağı A3 algoritmasını kullanaraktan uygun SRES'i kendisi üretir. Eğer MS den gelen SRES ile kendisinin ürettiği SRES aynı ise kimlik doğrulama işlemi gerçekleşmiştir ve iletişim prosedürlerine devam edilir. Eğer SRES'ler uyuşmamışsa işlem o anda bitirilir, çünkü kullanıcı tarafından bilgilerle ağ sistemindeki bilgiler çelişmektedir ve bu da kullanıcının kimliğinin doğru olmadığı sonucunu ortaya çıkarır.

6.2.2. Kimliğin Gizlenmesi

GSM sisteminde, haberleşme her ne kadar hava üzerinden gerçekleşiyor olsa da kullanıcının kimliğinin gizli tutulması sağlanmakta ve üçüncü şahıslar tarafından ele geçirilmesi engellenmektedir. Bunu gerçekleştirebilmek için geçici kimlikler kullanılır. Kullanıcı sisteme ilk olarak girdiğinde SIM kartında saklanan "Uluslararası Mobil Abone Kimlik" (IMSI) gönderilir. Fakat daha sonra "Geçici Mobil Abone Kimlik" (TMSI) ilişkilendirilir. TMSI kimlik doğrulama işleminden sonra şifreleme işlemi devam ederken MS'ye gönderilir ve MS bu bilgiyi aldığına dair bir yanıt gönderir. TMSI ilişkilendirildiği alan içerisinde geçerlidir. Sonuç olarak TMSI ve IMSI sayesinde kullanıcının kimliği gizlenmiş olur ve herhangi bir üçüncü şahıs kullanıcının telefon numarasını (MSISDN) tespit edemez.

6.2.3. Kullanıcı Veri ve Sinyal Korunması

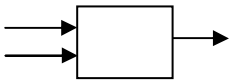
GSM sisteminde kullanıcı veri ve sinyal korunması şifreleme ile gerçekleştirilir. Şüphesiz veriyi şifrelemek için yalnız MSC ve MS'in bildiği ve başka kimsenin bilmediği gizli bir anahtara ihtiyaç vardır. SRES kimlik doğrulama işlemiyle onaylandıktan sonra Ki ve RAND bilgileri A8 algoritmasına geçer ve A8 sesin şifrelenmesinde kullanılacak gizli anahtar Kc'yi çıktı olarak üretir. GSM, şifreleme anahtarı Kc'yi saldırılara karşı zayıf olan hava ortamında kullanıcı bilgilerini istenmeyen kişilerin elde etme çabalarından koruyabilmek maksadıyla kullanır. A8 ve A3 algoritmaları SIM kartın içinde saklanır. Ses, MS ve BS arasında 114 bitlik frameler halinde gönderilir. A5 algoritması Kc ve frame numarasını alır ve 114 bitlik "anahtar akım dizisi'ni oluşturur. Aynı Kc günlerce kullanılabilinir. Eğer MSC MS'i tekrar kimlik doğrulaması işleminden geçirmek isterse yeni bir Kc oluşturulur. Şifreleme işlemi sırasında yeterli oranda hız elde edebilmek için, A3 ve A8 de olduğu gibi SIM kartın içinde olmak yerine, A5 cep telefonunun donanım kısmında gerçekleştirilir.

6.3. GSM Güvenlik Algoritmaları

GSM'de güvenlik uygulanan üç algoritma sayesinde yerine getirilmektedir. Bu algoritmalar Mobil İstasyonu Doğrulama Algoritması, Anahtar Üretme Algoritması ve Şifreleme Algoritması olarak tanımlanır.

6.3.1 Mobil İstasyonu Doğrulama Algoritması A3

Yukarıda adı geçtiği gibi doğrulama işinden sorumludur. İlk olarak A3 algoritması 128 bit uzunluğundaki RAND sayıyı BS'den ve 128 bit uzunluğundaki kullanıcı kimlik doğrulama anahtarı Ki'yi SIM'den girdi olarak alır (Şekil 6.3). Daha sonra 32 bit uzunluğundaki SRES çıktısını oluşturur. Bu 32 bitlik SRES, GSM ağındaki SRES ile karşılaştırılır. Eğer birbirleriyle uyuşuyorsa kimlik doğrulanır. A3 algoritması tek yönlü özetleme fonksiyonu kullanır, dolayısıyla ele geçirilen bir SRES'den Ki'nin bulunması çok zordur [61].



Şekil 6.3. A3 Algoritmasının işleyiş şekli [60]

6.3.2. A8 Anahtar Üretme Algoritması:

Bu algoritma ses verisini şifrelemekte kullanılacak anahtarı üretme algoritmasıdır. A8, gizli anahtar Ki'yi ve MSC'den RAND'ı alarak oturum anahtarı Kc'yi üretir (Şekil 6.4).

Şekil 6.4. A8 anahtar üretme algoritmasının işleyiş şekli [62]

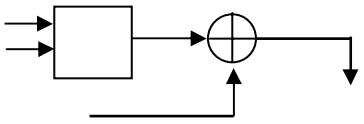
İlk olarak A8 algoritması 128 bitlik RAND ve 128 bitlik Ki yi girdi olarak alır. Bunları kullanarak 64 bitlik şifreleme anahtarı Kc'yi çıktı olarak verir. Oturum

anahtarı (Kc), MSC tarafından MS'nin doğruluğu tekrar onaylanmaya karar verilene kadar kullanılır.

Bu bazen birkaç gün alabilir. A3 ve A8 algoritmalarının ikisi de tek yönlü fonksiyonlardır [62].

6.3.3. Şifreleme Algoritması A5

Bu algoritma hava kanalı üzerinden şifreli veri gönderiminde kullanılır. A5 algoritmasının A5/1, A5/2 ve A5/3 gibi çeşitli varyasyonları vardır. A5/1 hava kanalı üzerinden ses şifrelemesinde kullanılan güçlü şifreleme algoritmalarından biridir. Ancak A5/2 gibi başka sürümleri de Avrupa dışında kullanılmaktadır. Üçüncü nesil cep telefonları içinse A5/3 tasarlanmıştır. A5 ilk olarak A8 tarafından üretilen 64 bitlik şifreleme anahtarı Kc ile her çerçevenin numarasını (frame number) girdi olarak alır ve 228 bitlik anahtar akım dizisi oluşturur. Bu 228 bitin 114'ü MS'den BS'e gönderilen verilerin şifrelenmesinde diğer 114 bitlik blok ise BS'den MS'e gönderilen verilerin şifrelenmesinde kullanılır (Şekil 6.5). A5, A3 ve A8'in aksine SIM kart yerine cep telefonunun kendisinde çalışır. A5 algoritması şifreleme için akım şifreleme (stream cipher) mekanizmasını kullanır. Veri hava ortamıyla Kc kullanılarak şifrelenmiş çerçeveler (frame) olarak gönderilir.

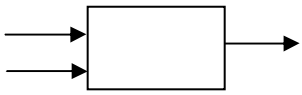


Şekil 6.5. A5 şifreleme algoritmasının işleyiş şekli [60]

6.3.4. COMP128 Algoritması:

Dünyanın hemen hemen her yerinde GSM operatörleri A3 ve A8 algoritması birlikte gerçekleştiren COMP128 algoritmasını kullanmaktadır. COMP128 RAND'i BS'den ve Ki'yi SIM'den alır. Fakat A3 ve A8'in aksine çıktı olarak 128 bit üretir, bunun ilk

32 biti SRES olup, son 54 bitinin sonuna 10 tane sıfır ekleyerek ise Kc'yi üretir (Şekil 6.6).



Şekil 6.6. COMP128 algoritmasının işleyiş şekli [62]

6.4. GSM Sisteminin Saldırıları

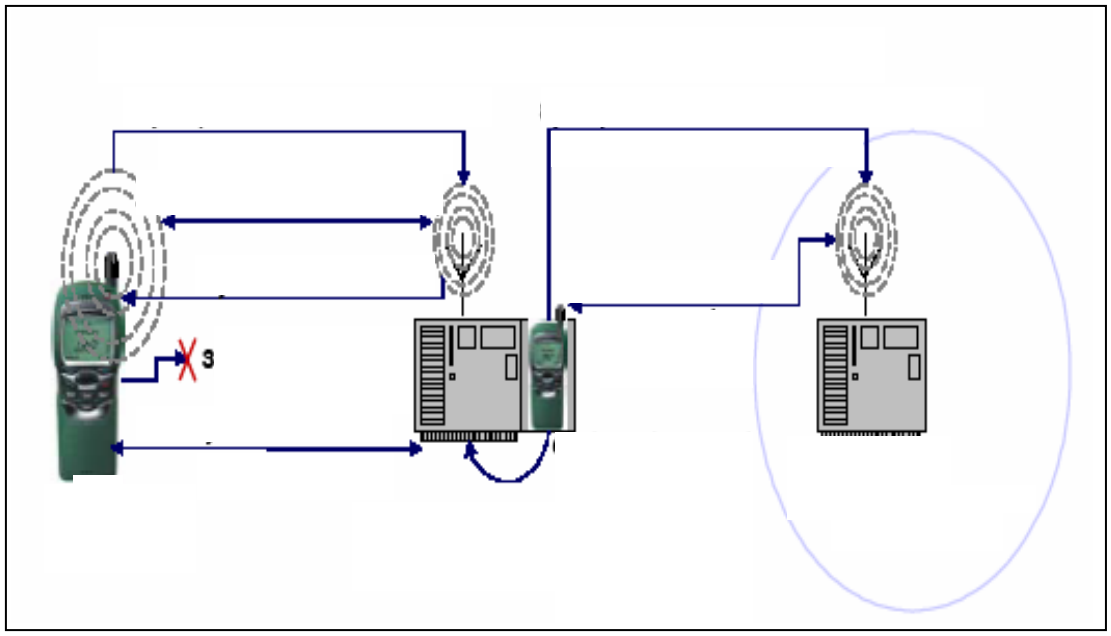
GSM güvenliğinin ana prensibi gizli Ki üzerine dayanmaktadır. Bu anahtar hem kimlik doğrulama (authentication) hem de oturum anahtarı Kc'nin oluşturulmasında kullanılmaktadır. Bu yüzden Ki hiçbir şekilde havadan gönderilmez, yalnızca iki yerde saklı tutulur. Bunlar kullanıcı SIM kartı ve GSM ağ birimi HLR'dir. Aslında A3 ve A8 algoritmalarının SIM kartının içerisinde yapılmasının bir nedeni de Ki bilgisinin SIM dışına çıkmasının engellenmesidir. Bu yüzden, eğer Ki saldırgan tarafından ele geçirilirse, sadece konuşmaları dinlemekle kalmaz, SIM kartı sahibi abonenin hesabına yanlış faturalar yerleştirebilir. Mevcut aboneyi Ki'yi kullanarak taklit edebilir. Aslında GSM sisteminin, bu durum için kısmi bir önlemi vardır. Aynı ID'li (kimlik numaralı) iki telefon aynı anda açıldığında, GSM ağı bunu fark ederek telefonlar için yer belirleme sorgusu yapar ve aynı kullanıcı numarasının aynı zamanda iki farklı yerde bulunduğunun farkına varırsa saldırganın ve meşru abonenin arama yapmasını engellemektedir. Ne var ki, saldırgan yalnızca kullanıcının konuşmalarını dinlemek isterse bu bir çözüm olmayacaktır. Bunun sebebi, saldırganın pasif olarak kalıp sadece konuşmaları dinleyerek GSM sisteminin kendisini tespit etmesini engellemesidir.

SIM kartın önemi gizli anahtar Ki'nin içinde saklı olmasıdır. Bu anahtar, hem kimlik doğrulama hem de oturum anahtarı Kc'nin oluşturulmasında kullanılmaktadır. Bu yüzden Ki hiçbir şekilde hava arayüzü üzerinden gönderilmez. Aslında A3 ve A8 algoritmalarının SIM kartının içerisinde çalışmasının bir nedeni de Ki bilgisinin SIM dışına çıkmasının engellenmesidir. Bu yüzden, eğer Ki saldırgan tarafından ele geçirilirse, sadece konuşmaları dinlemekle kalmaz, SIM kartı sahibi abonenin

hesabına yanlış faturalar yerleştirebilir. Aslına GSM sisteminin, bu durum için kısmi bir önlemi vardır. Aynı ID'li (kimlik numaralı) iki telefon aynı anda açıldığında, GSM ağı bunu fark ederek telefonlar için yer belirleme sorgusu yapar ve aynı kullanıcı numarasının aynı zamanda iki farklı yerde bulunduğunun farkına varırsa saldırganın ve meşru abonenin arama yapmasını engellemektedir.

6.4.1. Baz istasyonları

Sahte baz istasyonları herhangi bir operatörün faaliyet gösterdiği frekanslarda daha fazla güç vererek o operatöre ait kullanıcıların kendisine bağlanmasını sağlamaktadır. Böyle bir durumda kullanıcı kendisini normal olarak GSM ağına bağlandığını düşünmekte ve bütün veri aktarımını bu baz istasyonu üzerinden yapmaktadır. Kullanıcının böyle bir durumu fark edememesinin sebebi, GSM de kimlik doğrulamanın tek yönlü olarak yapılmasıdır. Yani ağ kullanıcıyı kabul etmek için kimlik doğrulama işlemine tabi tutarken, kullanıcı karşısındaki GSM ağının doğru olup olmadığını test edemez (Şekil 6.7) .



Şekil 6.7. Sahte baz istasyonu saldırısı [63]

Şekil 6.7'de sahte bir baz istasyonuna bağlanmış kullanıcıya, sahte baz istasyonu sürekli olarak RAND gönderip ona tekabül eden SRES'leri alabilir. Bir önceki

bölümde bahsedilen metotla elde edilen SRES'lerden kullanıcının Ki'si elde edilebilinir. Bu saldırıyı gerçekleştirmek yaklaşık olarak 8 -13 saate ihtiyaç vardır. Eğer kullanıcı sürekli olarak RAND bombardımanına tutulursa, telefon şarjı daha çabuk biteceğinden, kullanıcı durumdan şüphelenebilir. Dolayısıyla saldırı çeşitli zaman dilimlerinde yapılarak da gerçekleştirilebilir [63].

6.4.2. Kablolu hattan gelen tehditler

Teknoloji uyumu, e-posta, Web ve SMS ile WAP gibi telsiz servisleri biçimindeki geleneksel kablolu hat servislerine köprü kuran cihazların ve servislerin maliyetini düşürmeye yardımcı olmaktadır.

Cep telefonundan gönderilen SMS'nin oldukça yüksek maliyeti, ekonomik bariyerler, kablosuz boşluğun kablolu hat ağları ile görülen mesajlaşmanın kötüye kullanımını kolaylaştırılmaktadır. Ancak bu bariyer, iki teknoloji arasındaki gittikçe artan kesintisiz ara birimle hafifletilmektedir. E-postadan SMS'ye olan ağ geçitleri, herhangi bir e-posta kullanıcısının dünyanın dört bir yanındaki mobil abonelerine ücretsiz mesajlar göndermesine olanak sağlamaktadırlar. İstenmeyen e-posta göndericileri (spammer) SMS/metin mesajları göndermek için cezalandırılmadıklarından dolayı bu, mobil kullanıcıları için bir sorun olan "Viagra" spam'ı gibi düşük karlı spam olasılığını potansiyel olarak açmaktadır. E-postadan SMS, abonelerin arkadaşlara ve kullanıcı gruplarının sayfasına ulaşmak için kullandıkları popüler bir servistir, bu nedenle bu servisin kesilmesi veya kısıtlanması iyi bir seçim olmaz. Ayrıca mobil operatörleri aynı tip filtrelerle e-postadan SMS'e geçişler için kendi e-postalarını ve geniş ISS'lerin kendi e-posta altyapısını kapsaması için kullandığı içerik analiz sistemlerini korumaktadır. Mobil müşterilerinin sadece Internet üzerinden halen mevcut daha fazla özellik talep ettikleri için mobil mesaj iletişiminin kötüye kullanımını sınırlayan ekonomik kısıtlamalar, laptoplar ve bilgisayarlarda sınırlananlar gibi benzer mesaj iletişiminin kötüye kullanma biçimlerine açık mobil cihazlarını bırakarak ortadan kalkacaktır. Konuları daha karmaşık hale getirmek için e-posta ve diğer iletişim formları cep telefonlarının ve PDA'ların ötesine geçerek yeni cihaz kategorilerine uzanmaktadır.

Televizyon set üstü kutularından buzdolaplarına kadar değişen aralıkta internete bağlı cihazlar mesaj gönderebilen platformların ayak izinde hızla yayılmaktadır. Oyun konsollarının ve portatif eğlence cihazlarının son dalgası da bu cihazların kullanıcılarının büyük çoğunluğu olan küçüklere ulaşan uygun olmayan içerik hakkında ek endişeler ortaya çıkaran İnternet bağlantısı ve mesajlaşma kapasitesine sahiptir. Bu platformlarda suiistimal olayı hala bilinmezken kullanıcıların bilgisiyle birlikte sırf bu cihazların sayısı bu platformların spamcılar için zorunlu hedefler haline getirmektedir [64].

6.4.3. Kablosuza özgü tehditler

Kablosuza özgü mesajlaşma tehditleri, kablolu alanda öncülük yapanlara benzeyecektir fakat özel ekonomik faktörlere bağlı olarak değişkenlik gösterecektir. Asya, mobil içerik ve kullanım eğilimlerinde tutarlı bir şekilde yol açmıştır ve ABD ve Avrupa gibi gelişmiş diğer mobil pazarlarında nelerin ortaya çıkacağını gösterecek olaylar olabilir. SMS gönderme maliyetinin yaklaşık bir peni olduğu Japonya ve Güney Kore'de mobil spam oranı neredeyse e-posta spam'ı ile birlikte eşit durumdadır. Japonya'nın NTT DoCoMo ağında 10 mesajdan 9'u spam'dır. Güney Kore'de aboneler, cep telefonlarına her gün ortalama bir spam almaktadırlar. SMS göndermeyle bütünleşen her mesajın maliyeti ABD ve Avrupa'dakine denk gelinceye kadar buradaki kullanıcılar, kablolu ağlarda hâkim olan URL'lerin ve geniş yayın postalarının yerine muhtemelen kısa kodlar ve dar bir şekilde hedeflenmiş duyurular görecektir. Örneğin bir kullanıcı, mobil operatörün ücretlendirme sistemine bağlı kısa bir kod kullanan metin servisi için kendisinin bağlanmasını teşvik eden bir spam alabilir ya da özel bir ücret rakamıyla arama için aldatılabilir. Bu "yanlış ön metin" mesajları, daha fazla müşteri memnuniyetsizliğine yol açarak aboneler üzerinde doğrudan ve ani mali etkiye sahip olur [64].

6.4.4. SMS sazan avlama (smishing) tehditleri

Mobil bankacılık ve mobil ödemenin on milyonlarca abone katılımıyla Japonya ve Güney Kore'de son derece popüler olduğu ispatlanmıştır. Bankalar tarafından düşük

maliyetle bankacılık hizmetleri vermenin bir yolu olarak kabul edildiğinden banka memurlarından cep telefonuna doğru bir dönüş vardır. ABD'deki 1 numaralı mobil operatörü olan Cingular Wireless, müşterilerinin cep telefonlarından hesaplarını yönetmelerine olanak sağlayan mobil bankacılık hizmetini 2007 yılı başında uygulamaya koymaya başlamıştır. Dünyadaki mali kurumlar, SMS üzerinden hesaba erişim gibi SMS hizmetleri sunmaktadırlar ve SMS, işlemler veya hesaptan çekilen fazla paralar gibi yapılan hesap faaliyetleri konusunda müşterileri uyarır. Daha önce mobil ortamda bulunmayan sazan avlama yapanlar ekonomik teşvikler şu anda mevcuttur. Banka ile mobil müşteri arasındaki bu yeni doğrudan etkileşim, sazan avlama yapanlar için kimlik hırsızlığı ve diğer sahtekârlık türleri amacıyla mobil kullanıcılardan mali bilgilere alma fırsatı oluşturmaktadır. Bu saldırılardan bazıları, virüsü kendi el cihazlarına kabul etmeleri ya da kredi kartı numaraları ve diğer özel bilgileri vermeleri için girişimde bulunduktan sonra - alıcıların bir servise kaydolmalarını ister. Kontörlü cep telefonlarının kullanıcılarına karşı SMS sazan avlama bildirimleri de alıcıların cep telefonu kontörlerini tekrar yüklemeleri için hesap bilgilerini girmelerini isteyen yerlerde yüzeyseldir. Geniş ölçekli SMS sazan avlama veya "Smishing" muhtemelen birçok büyük banka bu hizmetleri sunduktan ve yeterli sayıda kullanıcı kabul ettikten sonra kısa bir süreye kadar ortaya çıkmayacaktır. Ara dönemde bu saldırılar spor amaçlı olacaktır. Azalan saldırı hacmi, hacim tabanlı içerik bloklamaya bağlı olmayan çözümler gerektirmektedir fakat bunun yerine hem balçanakları (honeypotlar) ve diğer sensör ağları üzerinden algılanan saldırıları öncelikli olarak hem de kullanıcıya destek sağlamak için hızlı bir şekilde tepki gösterebilir [64].

6.4.5. Mobil ortam virüsleri ve solucan tehditleri

Yaygın bir sorun olarak kablosuz kötü niyetli yazılımın ortaya çıkışı mobil yazılım ve platformların standartlaşmasına bağlıdır. Homojen bir yazılımın kritik kütlesi mobil toplulukta kendiliğinden oluşan ve kendiliğinden yayılan kötü niyetli yazılım için henüz mevcut değildir. Bu durum, anti-virüs topluluğunda haber haline gelirken fiilen birçok kullanıcıyı etkilemeyen çok sayıda Symbian OS varyantlarıyla gösterilmiştir. Windows Mobil veya Symbian gibi işletim sistemleri olan mobil

cihazların popülaritesi artarken mobil virüslerin meydana gelme ihtimali de artacaktır [65].

6.4.6. Kontrol edilmemiş mobil mesajlaşma suistimalinin etkisi

Spam, e-postada kullanıcılarını kızdırırken mobil cihazlarda izinsiz giren ve maliyetli olan bir şeydir. Bir SMS mesajı, herhangi bir zamanda ve ABD'de aboneyi kesintiye uğratabilir, bu istenmeyen kesintiler genellikle mesaj başına büyük bir maliyete sahiptir. Ayrıca öncelikli ücret rakamlarına aramaları ve mesajları davet eden dolandırma mesajları birçok defa genel SMS gönderme/alma maliyetlerinden çok daha büyük mali etkiye sahip olabilir. Bu nedenle mobil spam, müşterinin şikayetlere kaydolmasını veya kontör istemesini destekleyecek aramaları tetikleyecektir. Mobil sazan avlama, aboneyle mali grup arasındaki ilişkiyi felce uğratarak abone için çok daha ciddi mali ve özel etkilere sahip olur. Mobil spam, abone ile servis sağlayıcısı arasındaki güven bağını da bozabilir. Bu kaybolan güven, abonelerin operatörden ve ortaklarından gelen yasal mobil reklamı kabul etmelerini zorlaştıracaktır. Son olarak kontrol edilmemiş SMS spam akışı, mobil operatörün servis kalitesi üzerinde ciddi sonuçlar doğurabilir. SMS mesajları, sesli aramalar olarak aynı kanal üzerinden aktarılmakta, böylece büyük hacimli SMS spam'ı ağa aşırı yükleme yapıp sesli hizmetlerin kabul edilmemesine yol açar. Bazı gelecek nesil SMSC'ler SMS ağı üzerinden sınırlı-ücretli trafik kapasitesine sahip olurken durum genellikle ekipmanı kurulu değildir. Ayrıca dış kaynaklı MT SMS trafiği doğrudan abone MSC'lerine gönderildiğinden harici ağlardan gelen trafiğin kabul oranı üzerinde genellikle çok az kontrol bulunmaktadır [64].

6.4.7. Frekans taramalı sistemler

Saldırganın, kullanıcı ile baz istasyonu arasındaki trafiği frekans tarayıcısı tarafından alınmasıdır. Daha önce bahsedildiği gibi alınan bilgi A5 algoritmasında Kc anahtarıyla şifrelenen metindir ancak saldırgan A5 algoritmasındaki farklı zafiyetlerden yararlanarak şifre çözümünün süresini daha kısa sürelere indirebilir. Frekans tarayıcılı sistemler aracılığıyla yapılan saldırılarda karşılaşılabilecek en

büyük problem GSM operatörü tarafından yapılan frekans atlamasıdır (frequency hopping). Ayrıca bu tip saldırganların kullanıcının IMSI'sini yakalaması çok yüksek bir ihtimal değildir. Bunun sebebi kullanıcının IMSI'sini yalnızca belirli zamanlarda göndermesidir [61].

6.4.8. Kullanıcının bloke edilmesi

Bu saldırı saldırganın, yalnızca GSM operatörünün faaliyet gösterdiği frekanslarda yüksek güçte sinyaller göndermesiyle gerçekleşebilir. Ancak bu durum kullanıcı tarafından rahatlıkla fark edilebilir ve ayrıca bu saldırı modelinde kullanıcı ayırt etmeksizin o frekanstaki bütün kullanıcılar bloke edilmiş olur. Örneğin cezaevlerinde bu tarz sistemler kurularak, bütün mahkumların cep telefonu ile iletişime geçmeleri engellenmektedir. Fakat bu sistemle istenmeyen kullanıcılarda bloke edilmiş olabilir. Mesela verilen örnekte cezaevi etrafında bulunan evlerdeki kullanıcılar da büyük ihtimalle sistem tarafından bloke edilmiş olmaktadır. Eğer saldırgan daha önceki bölümlerde bahsedildiği gibi kullanıcıyı sahte bir baz istasyonu vasıtasıyla kendisine bağlamışsa, bu durumda saldırgan yalnızca istediği kullanıcıları fark edilmeksizin rahatlıkla bloke edip onların iletişime geçmesini engelleyebilir.

6.4.9. Abis ara bağlamı ortamında yapılan saldırı

GSM sisteminde kullanıcı ile baz istasyonu arasında veri aktarımı şifreli gerçekleşiyor olsa da BTS'den sonraki kısımlara veri iletimi şifresiz yapılmaktadır. BTS ile onu kontrol eden BSC arasındaki veri trafiği ya fiber optik mikrodalga ya da uydu hattı üzerinden gönderilmektedir. Genelde fiber optik yatırımı masraflı olduğundan, coğrafi şartlar el veriyorsa iletişimi mikrodalga üzerinden yapmaktadırlar. Eğer iletişim mikrodalga üzerinden yapılıyorsa ve saldırganın uygun bir teçhizat sistemi varsa saldırgan rahatlıkla BTS ile BSC arasındaki yaklaşık 2Mbps olan şifresiz veri aktarımını ele geçirebilir. Eğer iletim uydu üzerinden yapılıyorsa, uydu iletişimine yönelik yapılan saldırılardan biriyle, verilerin ele geçirilmesi sağlanabilir. BTS ile BSC arasında LDAP protokolü kullanılmakta, çok kapsamlı olmayan bir protokol analizörü ile veriler ses dosyası şeklinde saldırgan

tarafından alınabilir. Ancak bazı BTS ile BSC deki antenleri tedarik eden bazı firmalar veri iletiminde çok dinamik olmayan şifreleme de koymaktadır. Bu ise saldırganın işini zorlaştırmaktadır.

6.4.10. Ara bağlantı ortamında yapılan saldırı

BSC, BTS den aldığı verileri normal olarak MSC'ye yine şifresiz olarak aktarmaktadır. Aktarım yine fiber optikle olabileceği gibi mikro dalga üzerinden de olabilmektedir. BSC ile MSC arasında SS7 protokolü kullanılmaktadır. Bir önceki bölümdeki benzer bir saldırı burada da gerçekleşebilir. Ancak genelde BSC ile MSC aynı ve güvenli bir mekanda tutulmaktadır. Dolayısıyla bu bölüme yapılacak saldırı çok kolay gözükmemektedir.

6.5. Me-imza Sistemlerinin Korunması

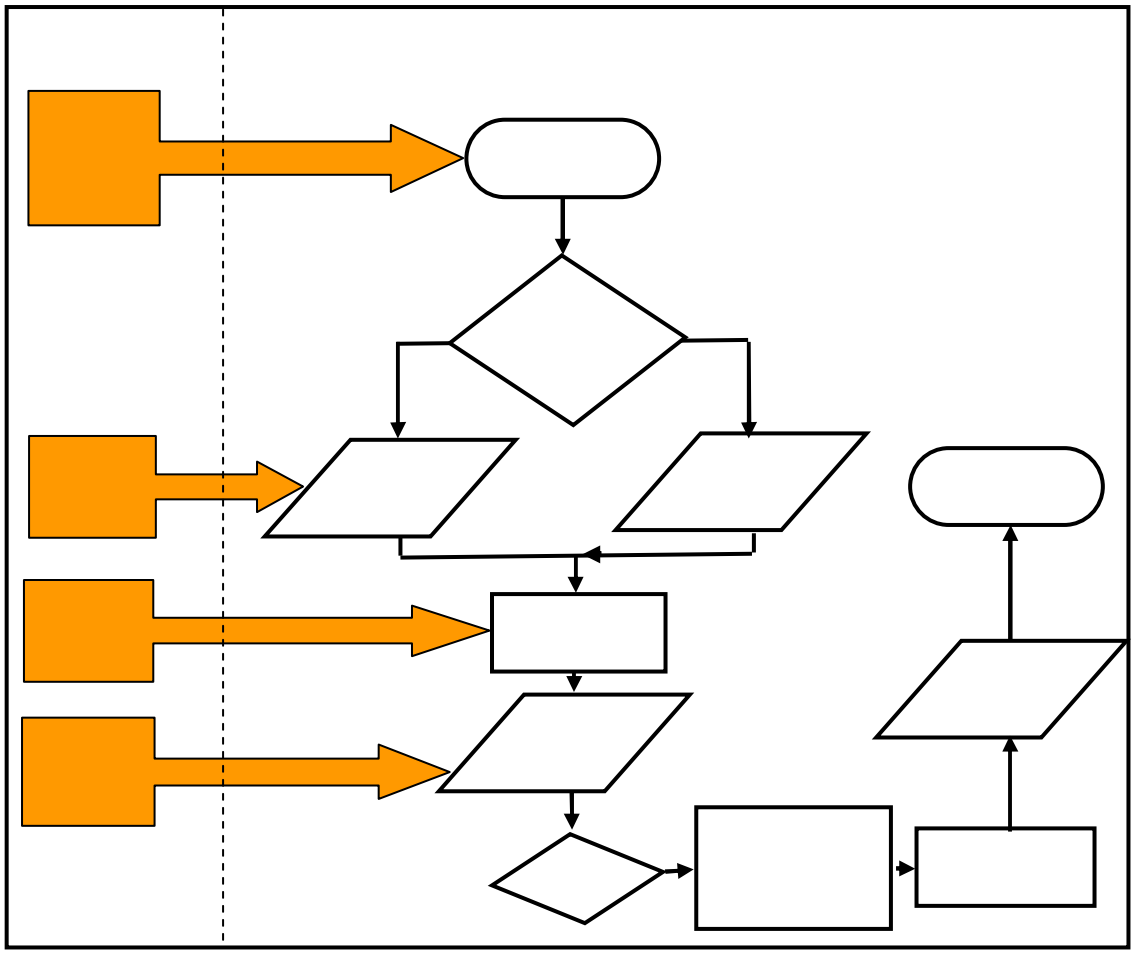
Son birkaç yılda mobil pazara sunulan mobil aygıtların çoğu açık platformlar haline gelmektedir. Bu açıklık içsel riskler taşımaktadır. Kötü niyetli yazılımların (malware) bulaşması ve yayılması bunların başında gelmektedir. İmza uygulamalarında olası Kötü niyetli saldırıları aşağıdaki gibidir:

- Tahrif edilmiş program başlatması
- İmzalanacak veriler için tahrif edilmiş diyalog
- İmzalanacak verilerin gizlice değiştirilmesi
- Hesaplanan değerin değiştirilmesi
- PIN gizli dinleme.

Şekil 6.8'de, me-imza ve genel olarak e-imza sistemine gerçekleşebilecek olan saldırılar belirlenmiştir.

Tüm bu istenmeyen işlemler mobil imza uygulama iş akışının başka programlardan etkilenmesini önleyerek engellenebilir. Bugün güvenilir icra ortamları inşa etmek için farklı yaklaşımlar bulunmaktadır. Bunlar aşağıdaki gibi sınıflanabilir:

- *İcra ortamı sanallaştırma;* Mobil imzalar gibi güvenliğin önemli olduğu uygulamalara tahsis edilmiş ayrı bir ortam sağlayan güvenilir bilgi işlem teknolojisine dayanır [66].
- *Mobil aygıt fonksiyonlarına haklara dayanan erişim;* Mobil aygıt üzerinde işletilen tüm mobil uygulamalar içindir. Bu haklar uygulamalara uygulama sertifikalarına göre verilecektir. Örneğin, SIM oku/yaz veya şebeke biçimlendirme bilgileri gibi güvenliğin kritik olduğu MNO fonksiyonları yalnızca yüksek derecede güvenilirliği olan sertifikalara verilir [67].



Şekil 6.8. E-imza Sistemine Gerçekleşebilecek Olan Saldırılar

Bu yaklaşımların hiçbiri ekonomik ve teknik gereksinimlerin tamamını karşılamamaktadır. Ancak ikinci yaklaşım mobil pazarda başarıyla kullanılmakta, bu büyük ölçüde yoğun MNO desteği sayesinde olmaktadır. Kullanılabilirlik açısından

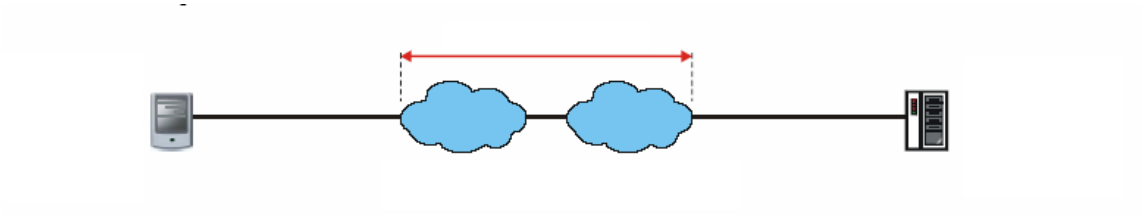
zayıflığı ne olursa olsun, bu yaklaşım mobil yazılım için temel korumayı sağlamakta ve daha sonraki ilerlemeler için büyük bir potansiyel oluşturmaktadır [68].

6.5.1. Güvenli mobil uçtan uca veri iletişimleri

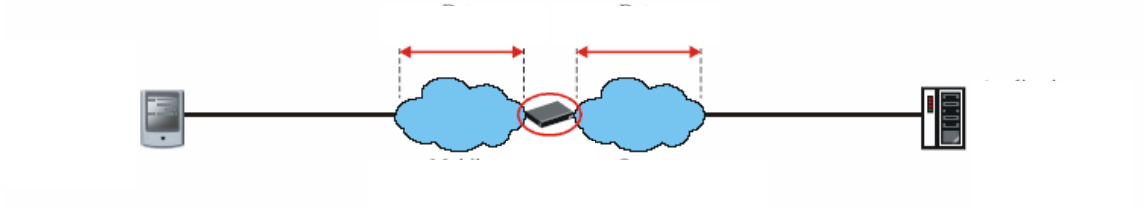
Mobil operatörün bakış açısından incelemede olan birçok güvenlik alanı vardır. Ancak mobil operatörün bakış açısından ve uygulama hizmeti sağlayıcısının (ASP) bakış açısından bunu incelemek de önemlidir. Mobil kullanıcının ve ASP'nin bakış açısından mobil iletişimde güvenlik incelenirken mobil terminal ile uygulama sunucusu arasındaki mobil uçtan uca iletişim konuları en önemli konulardan biri olmuştur. Ayrıca mobil ağların (örneğin IMT–2000 cep telefonu ağı, kablosuz LAN, Bluetooth) veya açık ağların olası çeşitli uygulamalarından dolayı mobil ağı açık bir ağa bağlayan mobil sistem için OSI Referans Modelinin üst tabakalarında (uygulamalar, sunuş ve oturum tabakaları) güvenlik incelemesi gereklidir [19].

6.5.2. Mobil uçtan uca veri iletişimleri için güvenlik teknolojilerinin çerçeve çalışması

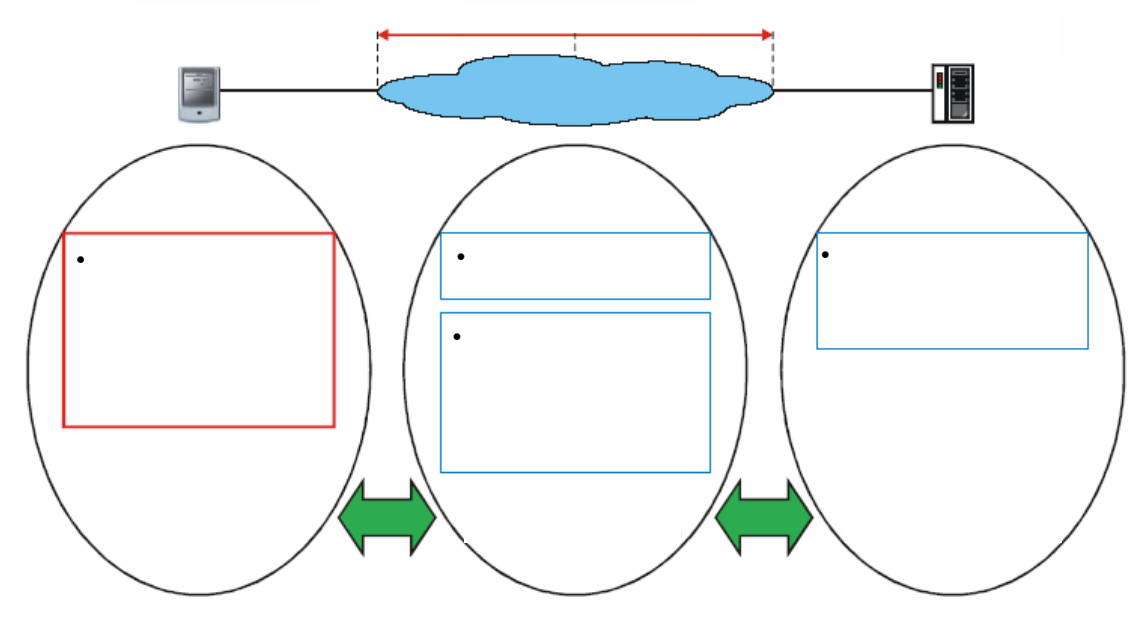
ITU-T X.1121 standardı, üst tabakalarda mobil terminallerle uygulama sunucuları arasındaki güvenli mobil uçtan uca veri iletişimlerinin modellerini açıklamaktadır. İki güvenlik modeli türü, mobil kullanıcı ile ASP arasında mobil uçtan uca veri iletişiminin güvenlik çerçevesi için tanımlanmaktadır: Genel model ve Ağ Geçidi modeli. Mobil kullanıcı, ASP'lerden çeşitli mobil hizmetlere erişim için mobil terminal kullanmaktadır. ASP, uygulama sunucusu üzerinden mobil kullanıcılara mobil hizmet sunmaktadır. Mobil güvenlik ağ geçidi, mobil terminallerden uygulama sunucularına giden paketleri geciktirir. Mobil ağ tabanlı iletişim protokolünü açık ağ tabanlı protokole veya tam tersine çevirir [19].



Şekil 6.9. Kullanıcı ile ASP arasında uçtan uca iletişimin genel modeli [19]



Şekil 6.10. Mobil kullanıcı ile ASP arasında uçtan uca veri iletişiminin ağ geçidi modeli [19]

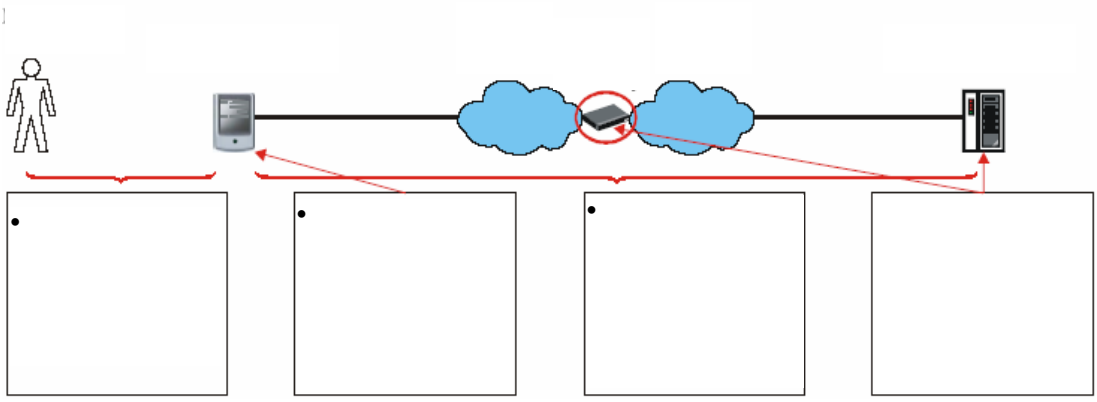


Şekil 6.11. Uçtan uca iletişimlerde tehditler [19]

ITU-T X.1121 standardı, mobil uçtan uca veri iletişimleri için güvenlik tehditlerini ve her iki modelde mobil kullanıcının ve ASP'nin bakış açısından güvenlik gereksinimlerini açıklamaktadır. İki türlü tehdit vardır: açık herhangi bir ağda genel

türde bulunan ve güvenlik tehdidinin özel bir mobil yönlendirmeli başka bir türü. Şekil 6.11, mobil uçtan uca veri iletişimi ağındaki tehditleri belirtmektedir [48].

Ayrıca ITU-T X.1121 standardı, güvenlik teknolojilerinin mobil uçtan uca veri iletişiminde varlıklar arasındaki ilişkiye ve gerektiğinde her varlığa uygulandığı yerleri tanımlamaktadır. Bu tanım Şekil 6.12'de verilmiştir.



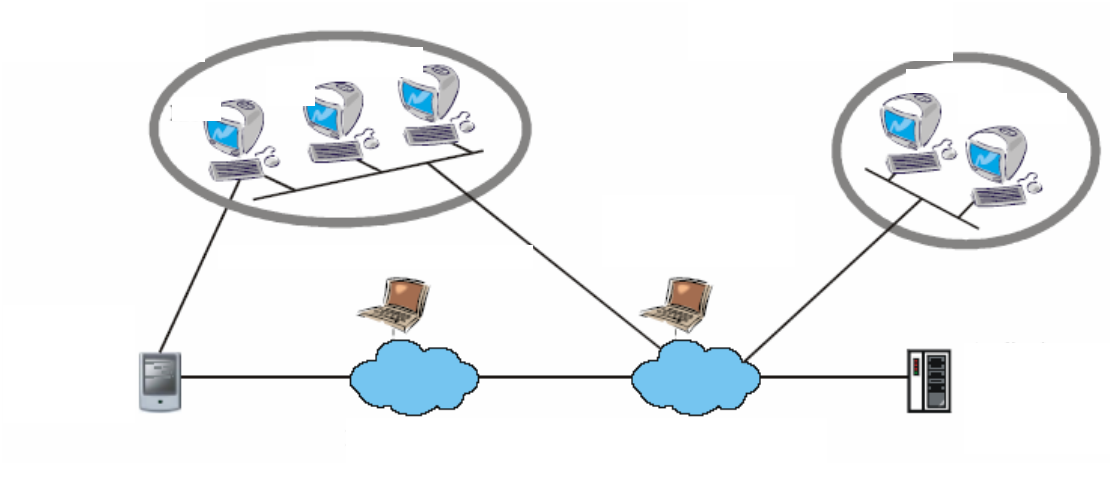
Şekil 6.12. Her varlık ve varlıklar arasındaki ilişki için gerekli güvenlik fonksiyonu [48]

6.5.3. Güvenli uçtan uca veri iletişimi için AAA kaygıları

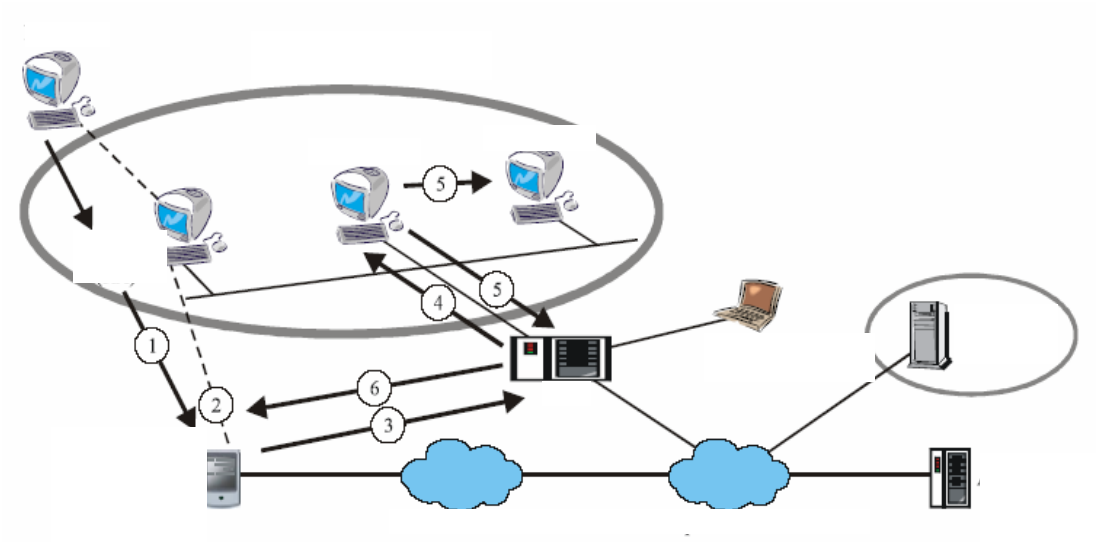
AAA teknolojisi mobil uçtan uca veri iletişimlerini korumak için çok yararlı bir teknoloji olmasına rağmen mobil veri iletişimine özgü bazı özellikler, AAA teknolojisinin güvenli mobil sistemleri oluştururken uyarlanmasını gerektirebilir. Mobil uçtan uca iletişimlerde güvenlik hizmetlerini sağlamak için iki AAA modeli türü tanımlanmıştır. Biri, mobil uçtan uca veri iletişiminde hiçbir güvenlik ağ geçidi işlevinin bulunmadığı genel AAA modeliyle ilgilidir, diğeri ise mobil ve açık ağla birlikte ara yüz için güvenlik ağ geçidinin bulunduğu ağ geçidi AAA modeliyle ilgilidir [19].

Şekil 6.13, mobil uçtan uca iletişimler için genel AAA modelini açıklamaktadır. Bu model dört varlık içerir. Mobil kullanıcının SM'yi, kullanıcı SM'ı tarafından hazırlanmış olan sertifika iptal listesini (CRL) saklamak için depoyu yönetir ve mobil

kullanıcıya mobil kullanıcı sertifikası hazırlamaktadır. Mobil kullanıcının SM, mobil kullanıcıya çevrimiçi sertifika onaylama hizmeti sunar. ASP'nin SM'yi, ASP SM tarafından hazırlanmış olan sertifika geri alma listesini (CRL) saklamak için depoyu yönetir ve uygulama hizmeti sağlayıcısına ASP sertifikası hazırlamaktadır. ASP'nin SM'si, ASP sertifikaları için çevrimiçi sertifika onaylama hizmeti sunar [48].



Şekil 6.13. Mobil uçtan uca veri iletişimleri için genel AAA modeli

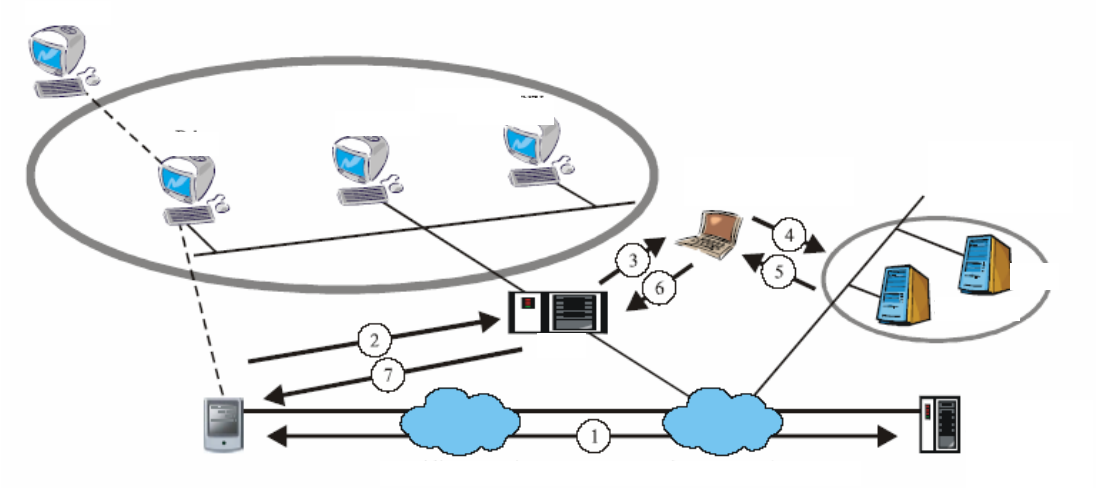


Şekil 6.14. Mobil terminal için sertifika hazırlama prosedürü

1. Kullanıcı cihazı satın alma emri verir.
2. Anahtar üretimi yapılır.

3. Sertifika oluşturulur.
4. Sertifika Uygulaması hazırlanır.
5. Sertifika saklama ve hazırlama işlemleri yapılır.
6. Sertifika hazırlama işlemi tanımlanır.

Açık/kapalı anahtarın, üretim yerine bağlı olarak iki sertifika hazırlama yöntemi vardır. Biri, kriptografik anahtar çiftinin üretilip mobil terminal fabrikasında hazırlandığı yöntem diğeri ise kriptografik anahtar çiftinin mobil terminalde veya mobil terminale bağlı smart kart gibi değiştirilmez bir ortamda üretilen yöntemdir. Şekil 6.14 kriptografik anahtar çiftinin mobil terminalde üretildiği sertifika yönetim prosedürünü kullanarak sertifikayı alan mobil terminal prosedürünü açıklamaktadır [48].



1. İmzalı bilgi
2. Geçerlilik onayı talebi
3. Geçerlilik onayı talebi
4. CRL talebi
5. CRL
6. Geçerlilik onayı sonucu
7. Geçerlilik onayı sonucu

Şekil 6.15. Mobil uçtan uca veri iletişimi için sertifika onaylama prosedürü [48]

Mobil terminal sınırlı hesaplama gücüne ve hafıza boyutuna sahiptir. Sonuç olarak online sertifika onaylama programı, CRL temelinde çevrim dışı sertifika onaylama programı için tercih edilebilir. Mobil terminal sertifika zinciriyle birlikte mesaj imza

çiftini aldığında ve imzanın geçerliliğini kontrol etmek istediğinde sertifika, sertifika geçerlilik programı kullanılarak kontrol edildikten sonra kullanılmalıdır. Şekil 6.15, mobil terminal için çevrimiçi sertifika onaylama prosedürünü açıklamaktadır.

Mobil uçtan uca iletişim için AAA sistemi, iki kullanım modeli için kullanılabilir: Biri, oturum seviyesi için kullanılabilir ve diğeri ise uygulama seviyesi için kullanılabilir. Oturum seviyesi, kullanım modeli müşteri onayı, sunucu onayı ve gizlilik ve bütünleşme servisi gibi güvenlik hizmetlerini sağlamaktadır. Uygulama seviyesi kullanım modeli, mobil uçtan uca veri iletişimi için tanıma ve gizlilik hizmeti sunar.

6.5.4. Talep üzerine sertifikasyon

Mobil operatör, imza işlevselliği için kullanılabilecek bir veya daha fazla anahtar çift(leri) için bir anahtar üreteciyle donatılmış SIM kartları satabilirler. Mobil operatörden SIM kart alındıktan sonra, müşteri kendi anahtarlarını üretebilir ve imza bileşenini faal hale getirebilir. Kamu anahtar(ları) talep üzerine Sertifikasyon ESHS tarafından onaylanabilir.

Telefon işlevselliğinin ayrılması ve ESHS tarafından kullanıcı kimliğinin (muhtemelen daha sonra) onaylanması sayesinde her iki işlev de ayrı olarak satılabilir ve farklı sağlayıcılardan alınabilir.

Taşıyıcı muhtemelen imza kapasiteli SIM kart için artan maliyetlerle karşılaşacaktır fakat bunun imza hizmetleri verilirken artan trafiği de sebep olabileceği değerlendirilmektedir. Bütün dağıtım kanalları değişmeden kalacaktır.

1. Taşıyıcı, kart üreticisine IMSI/Ki çiftlerini verir.
2. Kart üreticisi, imza uygulaması için bir anahtar üreteci olan IMSI/Ki çiftini içeren SIM kartı ve kök SM kamu anahtarını taşıyıcıya iade eder.
3. SIM kart müşteriye satılır ve taşıyıcı, anahtarları üretmek ve imza işlevselliğini faal hale getirmek için kullanılan bir başlangıç PIN sağmaktadır.

4. Müşteri, başlangıç PIN'i girerek anahtarları üretir ve imza işlevselliğini faal hale getirir.
5. Müşteri, kimlik bilgilerini ve kamu anahtarını vererek seçeceği KM'ye kaydolur.
6. Müşteri, özel anahtarıyla imzaladığı kimlik bilgilerini yayın yoluyla SM'ye gönderir.
7. KM, kamu anahtarını ve kimlik bilgilerini SM'na gönderir.
8. Müşteri ile KM tarafından verilen bilgiler uyuşursa SM müşteri için bir sertifika hazırlar ve bunu yayın yoluyla cep telefonuna gönderir.
9. Kullanıcı, ESHS'nin Kök SM'nin tarafından hazırlanan sertifikayı kontrol ederek sertifikasının geçerliliğini onaylayabilirler.

Bu protokol, mobil operatörlerin mevcut dağıtım alt yapısında değişiklik yapmaz. Adım 1'den 3'e kadar olan adımlar, kart üreticilerinin SIM kartı üzerinde ek bilgi vermeleri ve işlevsellik (imza anahtarı üreteci, Kök SM kamu anahtarı) sağlamaları olgusundan ayrı olarak daha önce kullandıkları aynı yolda kalırlar. Kart üreticisinin, kullanıcının özel anahtarını bilmemesini sağlamak için anahtar üretimi kart tarafından yapılmalıdır. Müşteri, anahtarlarını onaylamaya zorlanmamalıdır ve SIM'i yalnızca telefon işlevi için kullanabilir. Örneğin güvenlik belirtisi olarak sertifikasyon işlemine gitmeden imza işlevini de faal hale getirebilir. Yasal olarak bağlayıcı e-imzaları hazırlayabilmek istiyorsa nitelikli sertifikası almak için bütün işlemleri yapmak zorundadır. Bunu ESHS'yi serbestçe seçerek yapabilir.

Adım 4'te anahtarları üretecek ve imza işlevselliğini faal hale getirecek başlangıç PIN, hiçbir imzanın, müşteri SIM kartı üzerinde kontrol sağlamadan önce oluşturulamamasını sağlamak için kullanılır. İmza uygulaması daha önce faal hale getirilirse kullanıcı, başlangıç PIN'i girerken bunu kabul edecektir.

Adım 6 göz ardı edilebilir fakat müşteri için kimlik bilgilerinin bütünlüğünün korunmasını sağlamak için güvence olarak hizmet eder.

Müşteri ESHS'sini değiştirmek isterse yeni ESHS'si ile yalnızca adım 5'den 9'a kadar olan adımları tekrarlamalıdır. Müşteri taşıyıcısını değiştirmek isterse bütün protokolü tekrar yerine getirmelidir fakat mevcut ESHS'ye kaydolabilir.

6.5.5. Güvenli mobil aracılığı

Mobil bankacılık ve aracılık hizmetleri dahil mobil mali hizmetlerin piyasa gelişimi bu beklentilere bağlı olarak canlı kalmamıştır. Mevcut mobil mali hizmetlerin uygulamalarını tekrar dikkate alarak artık çoğunlukla web tabanlı karşı tarafların üretimlerini bulabiliriz. Bu, duruma göre güvenlik mekanizmalarının kullanılmasına uygulanmaktadır. Sonuç olarak mobiliteden ve alt yapısal açıdan kaynaklanan özel vasıfları kullanmıyorlar. Örneğin hesap bakiyelerinin ve talep edilen borsa ücretlerinin kontrolü eğlenceli olabilirdi fakat normalde müşterilere katma değer sağlamaz ve yolundayken izin verilen işlemler için işlem numaralarının kullanılması uygun olmaz.

Çevrimiçi aracılık hizmetlerinin geleneksel kavramla elde edilemez. İlgili bildirimi içeren bir SMS mesajı birleştirme veya onaylama koruması sağlamaz. Potansiyel bir saldırgan, haberlerle yanlış bildirimler gönderen sunucuyu besleyerek şaşırtabilecektir.

Yatırımcı için bir süre basılı duran işlem numarasını taramak ve girmek de çok uygun olmayacaktır. Mobil imzalar kullanılarak bildirimin bütünlüğü ve onayı yatırımcı tarafından kontrol edilebilir. Yatırımcı tarafından yapılan işlemler için onay ve bütünlük sağlanarak bildirim ve işlem hizmetlerinin güvenli entegrasyonuna da olanak sağmaktadır.

COD alt yapısı finans kuruluşlarının onaylamasına imkan sağlar ve mobil abonelerinin mobil terminalleri ve SIM'leri sayesinde online bankacılık hizmetlerini kullanmasına olanak verir. Belgeler, banka kartlarında kullanılanlar gibi bankanın kendisi tarafından onaylanabilir. Bu nedenle mobil operatör hala IMSI/Ki çiftlerini

bankaya vermeden SIM kartları hazırlayabilirken banka ise hala belgeler üzerinde kontrole sahip olabilir.

6.5.6. Mobil hizmet mimarisi

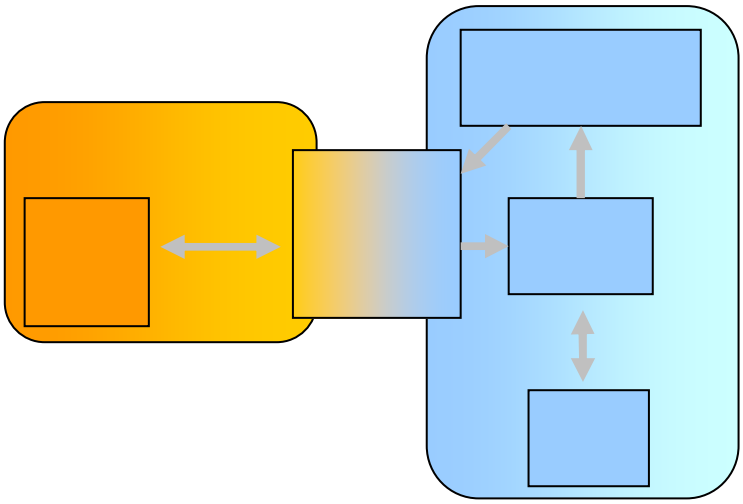
Bir mobil imza uygulama birimi ve mobil kullanıcı arasındaki mobil hizmet etkileşimlerinin iki tipini ayırabiliriz: kullanıcı tabanlı olanlar ve uygulama tabanlı olanlar. Kullanıcı tabanlı etkileşim mobil hizmet aboneleri tarafından, mobil hizmeti sunan sunucunun Web ara yüzü üzerinden başlatılır. Bu etkileşim tipi tam gelişmiş Internet tarama programı ve dokunmatik ekranı olan mobil aygıtlar, örneğin PDA kullanan aboneler içindir. Bu durumda kullanıcı etkinlikleri bu işlemleri sabit PC üzerinden yapanlarınkine benzer, imzanın oluşturulması tarayıcı programda açılan bir Web sayfasının kontrol elemanı tarafından başlatılır.

Uygulama tabanlı etkileşim mobil aygıt uygulaması ve mobil hizmet sunucusu arasında bir mesajlı iletişim şeklinde gerçekleşir. Bu etkileşimi göstermek için, bir satış noktasındaki (POS), örneğin bir süper marketteki veya benzin istasyonundaki ödemeleri kullanabiliriz. Krediyle veya kredi kartıyla ödeme yapan müşterilerin imzalarını kullanarak kart kullanımına yetki vermeleri gerekir. POS terminali karttaki verileri her zamanki gibi kartın manyetik şeridinden veya bütünleşmiş çipten okur, sonra bir elektronik alındı çıkarır. Bu alındı müşterinin mobil aygıtına yollanır. Müşteri bundan sonra alındıyı mobil aygıtında imzalayarak POS terminaline geri yollar. POS terminali imzayı doğrular ve ödemeyi teyit eder. Bundan sonra imzalanmış elektronik alındı müşterinin bankasına yollanır ve orada kendi güvenlik yaklaşımlarına göre ele alınır [68].

Mobil hizmetlerin uygulama tabanlı etkileşimle tüm kullanımlarını analiz ederek mobil imzanın kullanıldığı mobil hizmetler için birleştirilmiş bir mimaridir. Bu mimari iki hizmet çeşidinin bileşenlerini tanımlamaktadır: mobil HS ve mobil aygıt.

Şekil 6.16'da verilen mobil cihaz ve hizmet sağlayıcısının jenerik hizmet iş akışı aşağıdaki işlemlerden oluşur:

1. Mobil hizmet istemi: abone mobil aygıt üzerinde Mobil Hizmet Uygulamasını başlatarak hizmeti başlatır;
2. İmza istemi: aboneden istem mesajını imzalaması istenir;
3. İmzalayıcının yetkilendirilmesi: imzanın oluşturulması için abonenin bir yetkilendirme karakteristiğini, örneğin PIN'i girmesi gerekir;
4. İmzanın oluşturulması; Veri formatlama: imzalanan mesaj ve buna karşı gelen sertifika Mobil Elektronik Hizmet Sağlayıcısının (MESHS) istediği formata dönüştürülür.
5. İmzanın doğrulanması, MESHS istem mesajını ve üzerindeki imzanın bütünselliğini doğrulmaktadır.
6. Hizmet kullanımı: doğrulama olumluysa abonenin hizmeti kullanmasına izin verilir.



Şekil 6.16. Mobil Cihazı ve Hizmet Sağlayıcı Arasındaki Arayüz [68]

Mobil hizmetin tipine bağlı olarak istem mesajı bir ödeme isteği, banka transfer bilgisi, imzalanacak bir alındı ve uzaktan erişim şifresi olabilir. Mobil hizmet ayrıca mobil aygıtla HS arasındaki iletişim taşıyıcısını da belirmektedir. İletişim yöntemi olarak Bluetooth seçilebilir.

Bu hizmet mimarisinin özel bir durumu mobil aygıtların bir PC ile birlikte kullanımıdır. Mobil aygıtlar masaüstü PC'lerin sabit kart okuyucuları olarak USB, seri kablo,

Bluetooth veya enfraruj port üzerinden kullanılabilir. Bu durumda kullanıcı PC üzerinde imza atmak için bir belge hazırlar veya seçer, imza uygulaması hesaba dayalı bir adres değeri hesaplar ve bunu mobil aygıta gönderir. Kullanıcı yetkilendirmesinin başarılı olmasının ardından imza mobil aygıt üzerinde hesaplanır. İmza uygulamasının kullanıcı ara yüzü PC üzerinde yürütülür, imza hesaplanması ise mobil aygıtta yapılır. Uygulama mimarisi çeşitli iletişim bileşenlerini de desteklemektedir.

Kullanım Frauenhofer-Institute SIT liderliğinde TruPoSign projesinde yürütülmüştür. Mobil aygıtta özel olarak geliştirilmiş güvenli Pocket Signer adındaki PDA ek biyometrik kimlik bilgileri ve güvenilen kullanıcı ara yüzüyle birlikte kullanılmıştır.

7. SONUÇLAR VE ÖNERİLER

Bu çalışmada, me-imza dünya uygulamaları gözden geçirilmiş, bizim ülke dahil olmak üzere 31 farklı ülkedeki çalışmalar incelenmiş, me-imza uygulamalarında ideal ülkelerin Finlandiya olduğu anlaşılsa da son günlerde ülkemizde de bu konuda yapılan çalışmaların dünya ülkelerinde örnek olduğu değerlendirilmiştir. 25 farklı e-imza standardı özetlenmiştir. Dört farklı modele dayanarak, altı ülkede me-imza çalışma modelleri belirlenmiştir.

Son günlerde önemli hale gelen mobil elektronik ortamlarda meydana gelen açıklar farklı parametreler açısından değerlendirilmiştir.

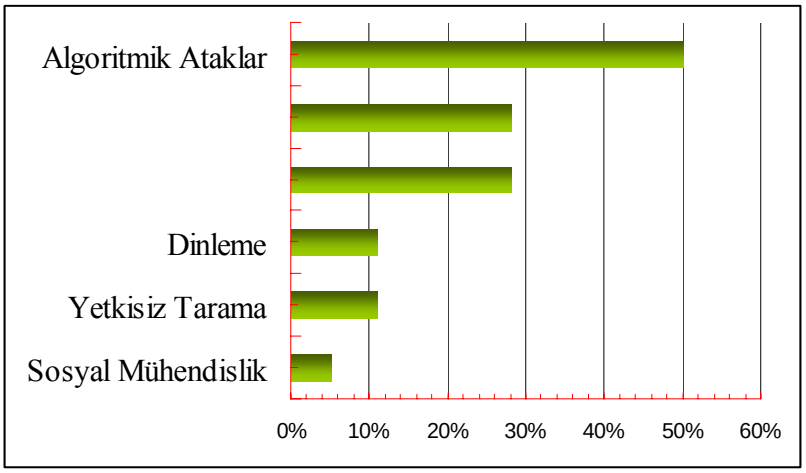
Elde edilen sonuçlardan, mobil elektronik ortamlarda verilecek olan hizmetlerde farklı güvenlik açıkları oluşturabileceği, bu ortamlarda yapılacak olan işlemlerde me-imza kullanımının farklı açıkları gidermede etkili olacağı değerlendirilmektedir. Ülkelerin kullandığı me-imza modelleri incelendiğinde ülkemizde kullanılan modelin en yüksek ve güvenli modeller arasında olduğunu belirlemekte fayda vardır.

Mobil imza kullanımı ile mobil elektronik ortamlarda oluşabilecek

- SIM kartları saldırıları
- Baz istasyonları
- Kablolu hattan gelen tehditler
- Kablosuza özgü tehditler
- SMS sazan avlama tehditleri
- Mobil ortam virüsleri ve solucan tehditleri
- Kontrol edilmemiş mobil mesajlaşma suistimalinin etkisi
- Frekans taramalı sistemler
- Kullanıcının bloke edilmesi ve ara bağlamı ortamında yapılan saldırıların giderebileceği değerlendirilmektedir.

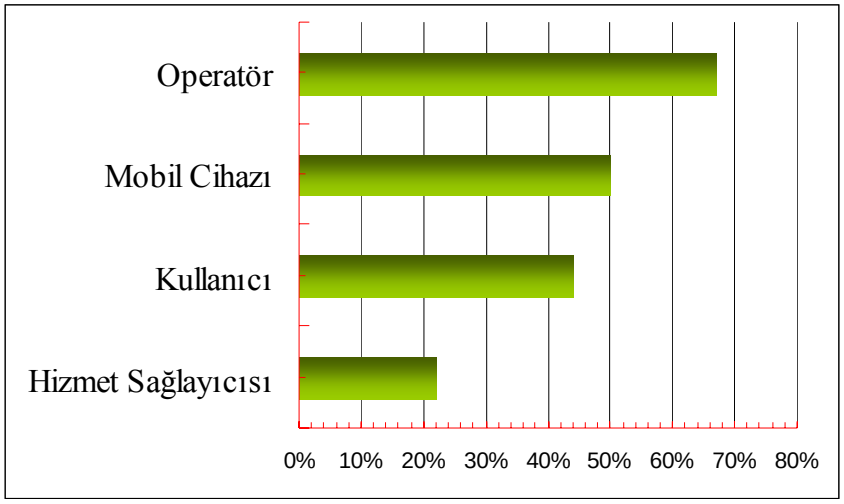
Mobil ortamlarda meydana gelebilecek açıkların fazlalığı sebebiyle bu ortamlarda her zaman açıkların olabileceği göz önüne alındığında bu ortamlarda yapılabilecek iş ve işlemlerde daha dikkatli olmaları ve bağımsız kuruluşlar tarafından bu ortamlara sızma tesislerinin yapılması pek çok açığın önceden tespit edilmesine fayda vardır.

Bu tür ortamlara yapılan saldırılar incelendiğinde, algoritmik atakların en fazla olduğu, sazan avlama ve virüsün bunları takip ettiği anlaşılmıştır. Şekil 7.1'de mobil istasyona yapılan saldırı türleri verilmektedir. Çizelge 7.1'de ise bunlar açıklanmaktadır. Dinleme, yetkisiz tarama ve sosyal mühendislik saldırılarının da bu sistemlere yapıldığını belirlemekte de fayda vardır.



Şekil 7.1. Mobil istasyonuna yapılan saldırı türleri

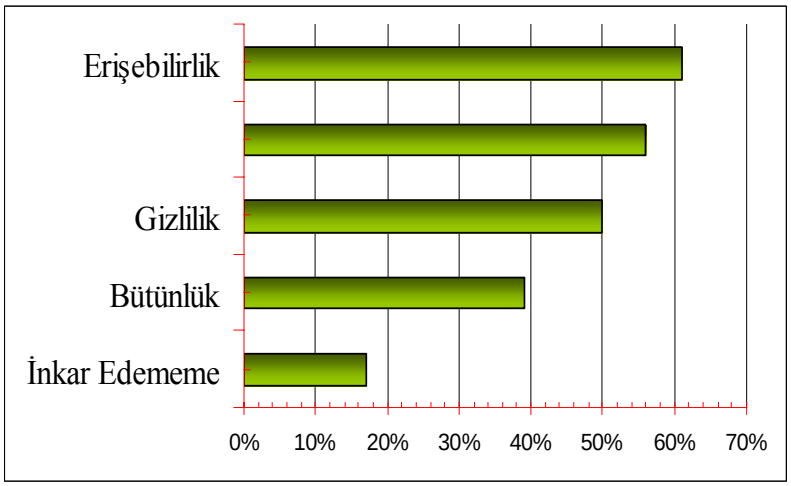
Şekil 7.2'de incelenen kaynaklardan elde edilen sonuçlara göre operatörlere karşı saldırıların gerçekten çok fazla olduğu görülse de operatör kısmı en zayıf noktalardan biri olarak kabul edilmektedir. Ancak Şekil 7.2'de görüldüğü gibi yapılan araştırmalarda hizmet sağlayıcısı saldırıları hakkında yapılan saldırıların ve araştırmaların daha az olduğu görülmektedir. Bu da hizmet sağlayıcılarının daha güçlü güvenlik sunduklarının göstergesidir. Ancak hizmet sağlayıcısı iletişimde çok önemli bir faktör olduğundan güvenliğin en üst seviyede tutulması gerekmektedir. Şu ana kadar yapılan saldırıların genellikle hizmet sağlayıcılarına karşı yapılmamasından dolayı hizmet sağlayıcılarının güvenlikleri iyi olarak bilinmektedir. Bu bağlamda, önemli olan yerlerin güvenliği devamlı olarak geliştirilmeli ve kontrol edilmelidir.



Şekil 7.2. Mobil sistemine yapılan saldırılar

Şekil 7.3'te güvenlik bileşenlerinin ihlali hakkında yapılan araştırmalar incelenmiş ve bu kaynaklardan elde edilen sonuçlar yüzde olarak verilmiştir. Ayrıca Çizelge 7.3'te kullanılan kaynaklara göre elde edilen sonuçlar belirlenmiş ve çizelge haline getirilmiştir. İnternet ortamında yapılan iletişimlerde en fazla ihlal edilen bileşenler görülmektedir. Burada en fazla güvenlik ihlalinin erişilebilirlik bileşeninde olduğu görülmektedir. İnkar edememe ve bütünlük gibi önemli bileşenlerde yapılan çalışmaların daha az olduğu görülmektedir. Ancak mobil elektronik imza güvenliği çerçevesinde bütün unsurlara aynı miktarda önem vermek gerekmektedir. Bunlardan bir tanesinin ihlali bile güvenliğin ihlaline sebep olmaktadır. Bu kapsamda, bütün unsurlar hakkında daha fazla araştırma ve çalışma yapılması sistemin daha güvenli hale gelmesi için uygun bir adım olabilir.

Mobil elektronik imza, elektronik imzanın aksine günlük hayatımıza yeni girmesine rağmen hızla gelişmektedir. Bunun en önemli nedenlerinde bir tanesi mobil cihazların kullanımının devamlı artmasıdır. Dolayısıyla, bu teknoloji ilerledikçe ve günlük hayatta kullanımı arttıkça oluşan veya oluşabilecek ihlaller ve saldırılar artmaktadır. Bu ihlal ve saldırılardan korunmak ve güvenliği sağlamak için bu konularda daha fazla araştırma yapılması gerekmekte ve elektronik imza için geçerli olan birçok güvenlik unsurunun rahat bir biçimde mobil cihazlarda uygulanması sağlanabilmelidir.



Şekil 7.3. Güvenlik Bileşenlerinin İhlali

Son olarak, kullanımı gittikçe artan ve yaygınlaşan mobil ortamları kullanımının hayatımıza daha çok etkinleşip ve bu ortamlarda iş ve işlemleri daha çok yapılmasını kaçırılmaz bir gerçektir. Bu ortamlarda karşılaşılabilecek tehdit ve tehlikeler ile oluşabilecek güvenlik açıklarının giderilmesi ise me-imza ve açık anahtar altyapısı gibi yaklaşımların kullanılmasıyla giderilebilecektir. Bu tez çalışmasının da buna büyük katkılar sağlaması değerlendirilmiş, gelecekte yapılacak bu tür çalışmalara ışık tutması beklenmektedir.

Bu tez çalışması esnasında karşılaştığım güçlükleri de burada açıklamakta fayda görüyorum. Bu konuda yapılan ilk kapsamlı çalışmalardan biri olması, konunun yeni olması, konuyla ilgili kaynaklara erişimde zorluklar yaşanması ve beklenen seviyede de kaynak bulunmaması ve farklı dillerdeki kaynakların Türkçeye çevrilmesi olarak sıralanabilir.

Çizelge 7.1. Mobil Sistemine Yapılan Saldırılar

Saldırı Yerleri	[58]	[59]	[60]	[61]	[62]	[69]	[63]	[64]	[70]	[71]	[72]	[74]	[63]	[75]	[76]	[77]	[78]	[79]
ESHS		√		√												√	√	
Operatör	√	√	√	√	√	√	√			√			√		√	√	√	√
Kullanıcı (SIM)	√	√			√			√		√	√			√		√		
Mobil Cihazı	√		√	√	√			√	√			√				√		

Çizelge 7.2. Güvenlik Bileşenlerinin İhlali

Saldırı Türleri	[58]	[59]	[60]	[61]	[62]	[69]	[63]	[64]	[70]	[71]	[72]	[74]	[63]	[75]	[76]	[77]	[78]	[79]
Kanıtlama	√	√	√		√		√			√	√			√			√	√
İnkar Edememe		√		√				√										
Bütünlük	√	√				√	√					√					√	√
Gizlilik	√		√	√	√	√	√	√		√				√		√		
Erişebilirlik	√	√		√		√		√	√				√	√	√	√	√	

Çizelge 7.3. Mobil Ortamlara yapılan saldırı türleri

Yapılan Ataklar	[58]	[59]	[60]	[61]	[62]	[69]	[63]	[64]	[70]	[71]	[72]	[74]	[63]	[75]	[76]	[77]	[78]	[79]
Yetkisiz Tarama		√								√								
Sosyal Mühendislik																		
Algoritmik Ataklar	A3, A5, A8		A5, COMP128	A3	COMP128	A5	A5		A3, A8		A3, A5			COMP128				A5
Virüs		√						√				√				√		
Sazan avlama								√					√	√		√		
Dinleme															√		√	

KAYNAKLAR

1.Türkiye İş Bankası, "Türkcell Mobil İmza", http://www.isbank.com.tr/interaktif/i-interaktif-mobilimza.html, (05.10.2007).

2.Sağıroğlu, Ş., Alkan, M.., "Her Yönüyle E-imza", ***Grafiker Yayınları***, Ankara, 30-45, (2005).

3.Kabasakal, D., "E-imzadan Me-imzaya Geçiş Sürecindeki Yansımalar, Uygulamalar Ve Öneriler", ***Uzmanlık Tezi***, Telekomünikasyon Kurumu, Ankara, 20-33, 47-82, 65-86, (2006).

4.***OASIS PKI TC***, "Analysis of June 2003 Survey on Obstacles to PKI Deployment and Usage", (2003), http://www.oasisopen.org/committees/pki/pkiobstaclesjune 2003 surveyreport, (12.04.2007).

5.Dumortier, J., Kelm, S., Nilsson, H., Skouma, G., Van Eecke, P., "The Legal and Market Aspects of Electronic Signatures", ***Study for the European Commission-DG Information Society***, (2003).

6.***EU FIDIS Project***, Deliverable D4.1:, "Structured account of approaches on Interoperability", (2005), http://www.fidis.net, (12.04.2007).

7.European Commission / DG Enterprise and Industry, "Benchmarking of existing national legal e-business practices", ***Country Report Austria***, (07.10.2007).

8.Hoepner, P, "Study PKI and Certificate Usage in Europe 2006", ***Fraunhofer Institute***, (2006).

9.Regulation on Certification Authorities, "Obligation to Notify FICORA", http://www.ficora.fi/englanti/document/FICORA072003M.pdf, (12.10.2007).

10.Özenç, K., "Avrupa Birliği' nde E-imza", ***Ulusal E-imza Sempozyumu***, Sheraton Hotel & Convention Center, Ankara,172-176, (2006).

11. Authentication, the keystone of m-Transactions, http://www.francetelecom.com/ sirius/rd/en/ddm/en/technologies/ddm2004 05/techfiche3.php, (04.10.2007)

12.European Commission/DG Enterprise and Industry, "Benchmarking of existing national legal e-business practices", ***Country Report United Kingdom***, (11.06.2007).

13.Vodafone Sweden and Valimo evaluate mobile eID, http://www.valimo.com/ news_and_events/news/2006/63, (10.09.2007).

14.German banks agree mobile digital signature code, http://www.finextra.com /fullstory.asp?id=1715, (10.09.2007).

15."Mobile Signature Service Pilot for Tax Declarations in Hungary", http:// www.mgsg.org/digitalcity/documents.jsp?dok=AAAALSQO&dom=AAAALQYV &prt=AAAALQVW&fmn=AAAALQWD&men=AAAALQVZ, (12.9.2007).

16.Brisis., K., "Issuing Keys to Citizens and Businesses", ***Norway***, http://www.s olutions.gc.ca/pki-icp/wrk-w-othrs/othrcountr/forum/forum12_e.asp, (12.09.2007).

17."ZebSign ID for Secure eCommerce and mCommerce", http://www.entr ust.com/resources/pdf/zebsign.pdf, (12.10.2007).

18."First electronic signature through a mobile phone in Poland", http://www.era.pl /indekx.php?id=p_info_e&press_id=410&section=korp, (03.09.2007).

19.International Telecommunication Union, ITU-T, "Security in Telecommunications and Information Technology", (2004), (12.10.2007).

20."Mobitel deploys Valimo Validator–MSSP", http://www.valimo.com/news_and _events/news/2006/62, (03.09.2007).

21."State proposes to cover part of citizens' eSignature costs", http://ec.europa.eu /idabc/en/document/5815/194, (12.10.2007).

22."eGovernment in the Member States of the European Union", ***2nd Edition*** , IDABC Programme, Belgium, (2005), (12.10.2007).

23.Sağıroğlu, Ş., Kabasakal, D., Alkan, M., "Elektronik İmzadan Mobil Elektronik İmzaya Geçiş Sürecinde Türkiye", ***Ulusal Elektronik İmza Sempozyumu***, Ankara, 21–27, (2006).

24.CWA 14172–1, "EESSI Conformity Assessment Guidance - Part 1: General Introduction", ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/ cwa14172-01-2004-Mar.pdf, (01.10.2007).

25.CWA 14172–2, "EESSI Conformity Assessment Guidance - Part 2: Certification Authority services and processes", ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14172-02-2004-Mar.pdf, (01.10.2007).

26.CWA 14172–3, "EESSI Conformity Assessment Guidance - Part 3: Trustworthy systems managing certificates for electronic signatures", ftp://ftp.cenorm.be/ PUBLIC/CWAs/e-Europe/eSign/cwa14172-03-2004-Mar.pdf, (01.10.2007).

27.CWA 14172–4, “EESSI Conformity Assessment Guidance – Part4: Signature creation applications and general guidelines for electronic signature verification”, ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14172-04-2004-Mar.pdf, (01.10.2007).

28.CWA 14172–5, “EESSI Conformity Assessment Guidance – Part5: Secure signature-creation devices”, ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14172-05-2004-Mar.pdf, (01.10.2007).

29.CWA 14172–6, “EESSI Conformity Assessment Guidance – Part6: Signature creation device supporting signatures other than qualified”, ftp://ftp.cenorm.be /PUBLIC/CWAs/e-Europe/eSign/cwa14172-06-2004-Mar.pdf, (01.10.2007).

30.CWA 14172–7, “EESSI Conformity Assessment Guidance – Part7: Cryptographic modules used by Certification Service Providers for signing operations and key generation services”, ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14172-07-2004-Mar.pdf, (01.10.2007).

31.CWA 14172–8, “EESSI Conformity Assessment Guidance – Part8: Time stamping Authority services and processes”, ftp://ftp.cenorm.be/PUBLIC/CWAs /e-Europe/eSign/cwa14172-08-2004-Mar.pdf, (01.10.2007).

32.CWA 14167–1, “Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements”, ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14167-01-2003-Jun.pdf, (01.10.2007).

33.CWA 14167–2, “Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic module for CSP signing operations with backup - Protection profile - CMCSOB PP”, www.commoncriteriaportal.org/public/files/ppfiles/pp0308.pdf, (01.10.2007).

34.CWA 14167–3, “Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 3: Cryptographic module for CSP key generation services protection profile CMCKG-PP”, ftp://ftp.cenorm. be/PUBLIC/CWAs/e-Europe/eSign/cwa14167-03-2004-May.pdf, (1.10.2007).

35.CWA 14169, “Secure signature-creation devices “EAL 4+”, ftp://ftp.cenorm.be /PUBLIC/CWAs/e-Europe/eSign/cwa14169-00-2004-Mar.pdf, 01.10.2007.

36.CWA 14170, “Security requirements for signature creation applications”, ftp://ftp. cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14170-00-2004-May.pdf, (01. 10.2007).

37.CWA 14171, “General guidelines for electronic signature verification”, ftp://ftp. cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14171-00-2004-May.pdf, (01. 10.2007).

38.CWA 14355, "Guidelines for the implementation of Secure Signature-Creation Devices", ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14355-00-2004-Mar.pdf, (01.10.2007).

39.CWA 14365–1, "Guide on the Use of Electronic Signatures - Part 1: Legal and Technical Aspects", ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14365-01-2004-Mar.pdf, (01.10.2007).

40.CWA 14365–2, "Guide on the Use of Electronic Signatures - Part 2: Protection Profile for Software Signature Creation Devices", ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14365-02-2004-Mar.pdf, (01.10.2007).

41.CWA 14890–1, "Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic requirements", ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14890-01-2004-Mar.pdf, (01.10.2007).

42.CWA 14890–2, "Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional Services", (ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14890-02-2004-May.pdf), (01.10.2007).

43.CWA 14921, "Web Services: Technology and Standardization Aspects", http://www.saiglobal.com/PDFTemp/Previews/OSH/IS/EN/2004/I.S.CWA14921-2004.pdf, (01.10.2007).

44.ETSI TR 102 203, "Mobile Commerce (M-COMM); Mobile Signatures; Business and Functional Requirements", http://portal.etsi.org/docbox/EC_Files/EC_Files/tr_102203v010101p.pdf, (22.11.2006).

45.ETSI TR 102 206, "Mobile Commerce (M-COMM); Mobile Signature Service; Security Framework", http://portal.etsi.org/docbox/EC_Files/EC_Files/tr_102206v010103p.pdf, (25.12.2006).

46.ETSI TS 102 204, "Mobile Commerce (M-COMM); Mobile Signature Service; Web Service Interface", http://portal.etsi.org/docbox/EC_Files/EC_Files/tr_102206v010103p.pdf, (28.12.2006).

47. ETSI TS 102 207, "Mobile Commerce (M-COMM); Mobile Signature Service; Specifications for Roaming in Mobile Signature Services", http://portal.etsi.org/docbox/EC_Files/EC_Files/ts_102207v010103p.pdf, (05.01.2007).

48.ITU-T Recommendation x.1122, "Guideline for Implementing Secure Mobile Systems Based on PKI", (12.10.2007).

49.Erdoğdu, C., "Avrupa Birliği'nde Elektronik Ödeme Sistemlerindeki Gelişmeler", ***Bankacılar Dergisi***, Sayı 48, (2004).

50.Morioka, M., Yonemoto, Y., Suzuki, T., Etoh, M., "Scalable Security Description Framework for Mobile Web Services Communications", ICC '03. ***IEEE International Conference on Publication***, (2003).

51."Mobile PKI Trial for Vodafone UK", http://www.gide.com/pls/portal/maia.display_custom_items. DOWNLOAD_SEEALSO_FILE?p_ID=5563, (12.10.2007).

52."Mobile Signature System", http://www.iss.nus.edu.sg/iss/catalyst_display.jsp?artid=1038&type=9&rid =45&pid=45&cid=25, (12.10.2007).

53."Authentication, The Keystone of m-Transactions", http://www.francetelecom.com/sirius/rd/en/ddm/en/technologies/ddm2004 05/techfiche3.php, (12.10.2007).

54."Act on Electronic Signature", http://www.finlex.fi/fi/laki/kaannokset/2003/en20030014.pdf, (12.10.2007).

55."ZebSign ID for Secure eCommerce and mCommerce", http://www.entrust.com/resources/pdf/zebsign.pdf, (12.10.2007).

56.Tunçalp, D., "e-Güven-Türkcell Mobil İmza Denetiminde Sunum Dökümü", ***İstanbul***, (2007).

57.Alkan, M., Özen, Ç.K., "E-Ticaretten M-Ticarete Doğru Süreçteki Yeni Yansımalar", ***Türkiye'de Internet Konferansı*** , 77-84, (2003).

58.Arreymbi, J., "Modelling to Enhance GSM Network Security", ***University of East London***, http://ww1.ucmss.com/books/LFS/CSREA2006/SAM5086.pdf, 121-127, (12.10.2007).

59.Bamforth, R., Tarzey, B., "Mobile Security and Responsibility", ***Quocirca Insight Report***, (2006).

60.Topark-Ngarm,P., Poocharoen,P., "GSM security Vulnerability", http://islab.oregonstate.edu/koc/ece478/03Report/toparkngarm-poocharoen- project578.pdf, (12.10.2007).

61.Bocan,V., Crețu,V., "Threats and Countermeasures in GSM Networks", ***Journal Of Networks***, Vol. 1, No. 6, 18-27, (2006).

62.Li,Y., Chen, Y., Tie-Jun M.A, "Security in GSM", http://www.gsmsecurity.net/papers/securityingsm.pdf, (12.10.2007).

63.Paulo, S.P., "A Contemporary Foreword on GSM Security", Lecture Notes In Computer Science, ISBN:3-540-44309-6, Vol. 2437, Proceedings of the ***International Conference on Infrastructure Security***,129 – 144, (2002).

64.“Taxonomy of Current and Potential Mobile Threats”, 2001-2007 ***Cloudmark, Inc.***, January 2007, http://www.cloudmark.com/releases/docs/wp_taxonomy_of_mobile_threats.pdf, (12.10.2007).

65.Tang, C., “Summary Of Mobile Threats For Year 2005”,www.it-observer.com/pdf/dl/mobile_threat_sum.pdf, (2006).

66.The Trusted Computing Group, Securing Mobile Devices on Converged Networks, White Paper, https://www.trustedcomputinggroup.org, (September 2006)

67.“OMTP Application Security Framework”, http://www.omtp.org/docs/OMTP_Application_Security_Framework_v2_0.pdf, (12.10.2007).

68.Pisko, E., “Mobile Electronic Signatures: Progression from Mobile Service to Mobile Application Unit”, ***Sixth International Conference on the Management of Mobile Business***, (2007).

69.Stausholm, M., Dahl, M., “Insecurity of GSM Communication”, ***Exam project in Cryptography course***, DAIMI AU, (2006).

70.Daniel, E., Castle, Darensburg,A., Griffin,B., Hickman,T., Stuart,P., Warders, and Grant A. Jacoby, “Gibraltar: A Mobile Host-Based Intrusion Protection System”, ***National Conference on Undergraduate Research***, (2006).

71.Suominen, M., “GSM security”, ***Helsinki University of Technology***, www.netlab .hut.fi/ opetus/s38153/k2003/Lectures/g42GSM_security.pdf, (2003).

72.Guo, Ch., Helen, J.W., Zhu, W., “Smart-phone Attacks and Defenses”, ***in Proc. ACM SIGCOMM HotNets***, 125–130, (2004).

73.Tang, C., “Summary Of Mobile Threats For Year 2005”, www.it-observer.com/pdf/dl/mobile_threat_sum.pdf, (2006).

74.Bocan, V., “Security and Denial of Service Threats in GSM Networks”, ***Vladimir*** Vol.49 (63), (2004).

75.Ahmad, A., Chandler, R., Dharmadhikari, A., Sengupta, U., “SIM-Based WLAN Authentication for Open Platforms”. ***Technology at Intel Magazine***, (2003).

76.Çetintaş, E., Levi, A., Aydos, M., Koç, Ç.K., Çağlayan, M.U., "Relay Attacks on Bluetooth Authentication and Solutions", ***LNCS 3280, ISCIS, Antalya***, (2004).

77.Bonesa, E., Hasvolda, P., Henriksena, E., Strandenæsb, T., “Risk Analysis of Information Security in a Mobile Instant Messaging and Presence System for Healthcare”, ***International Journal of Medical Informatics***, IJB-2286; No. of Pages 11, (2006).

78.Orioka, M., Yonemoto, Y., Suzuki, T., Etoh, M., "Scalable Security Description Framework for Mobile Web Services, Communications", ICC '03. IEEE ***International Conference on Publication***, (2003).

79.Barkan, E., Biham, E., Keller, N., "Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication", http://cryptome.org/gsm-crack-bbk.pdf, (2003).

80.Bekir, I.A., "Elektronik Sözleşmeler", Arapça, ***Al-salam yayın evi***, Baghdad, 12-28, (2007).

81."E-Güven, Dünya'ya bir ilk, me-imza", http://www.e-guven.com, (05.10.2007).

82.Sağıroğlu, Ş., Kabasakal, D.,Alkan, M., "Mobil Elektronik İmza, Altyapısı ve Türkiye", ***Ulusal Elektronik İmza Sempozyumu***, Ankara, 91–98, (2006).

83.Wikipedia,http://en.wikipedia.org/wiki/CEN_Workshop_Agreement, (12.10.2007).

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı : MOHAMMED, Murad

Uyruğu : Irak

Doğum tarihi ve yeri : 27.09.1979 Kerkük

Medeni hali : Bekar

Telefon : 0 (543) 449 50 12

e-posta : m25t@hotmail.com.

Eğitim

Derece	Eğitim Birimi	Mezuniyet tarihi
Lisans	Bağdat Üniversitesi/ Bilgisayar Bilimleri	2002
Lise	Velit Lisesi/ Kerkük	1998

Yabancı Dil

İngilizce, Arapça

Hobiler

Voleybol, Seyahat