TEŞEKKÜR

Bu tezin her aşamasında yardım, öneri ve desteğini esirgemeden beni yönlendiren danışman hocam Prof.Dr. Hafız ALİSOY'a;

Tüm hayatım boyunca benden desteklerini esirgemeyen hayattaki en değerli varlıklarım olan AİLEM'e (Annem Babam Emine-Halil AVAROĞLU'na ve Sevgili Eşim Nuray'a);

Bana katkı sağlayan ve destek veren tüm arkadaşlarıma;

Teşekkür ederim.

İÇİNDEKİLER

ŞEKİLLER DİZİNİ

TABLOLAR ÇİZELGESİ

SİMGELER VE KISALTMALAR

AAA	Açık anahtar alt yapısı
AES	Gelişmiş şifreleme standardı
AH	Kimlik doğrulama başlığı
BGYS	Bilgi yönetim sistemi
BSI	İngiliz standartlar enstitüsü
CIBC	Canadian imperial bank of commerce
CMS	Kriptografik mesaj sözdizimi
DES	Veri kriptolama standardı
DIR	Dâhilde işleme rejimi
DSV	Deutscher sparkassen verlog
DTM	Dış ticaret müsteşarlığı
E-CERT	Sayısal sertifika
EDİ	Elektronik veri değişimi
E-İMZA	Elektronik imza
E-POSTA	Elektronik posta
ESHS	Elektronik sertifika hizmet sağlayıcı
ETSI	Avrupa telekomünikasyon standartları enstitüsü
FESA	Avrupa elektronik imza denetim kurumları formu
FIPS	Federal bilgi işleme standartları
HSM	Donanım güvenlik modülü
IKE	Otomatik anahtar değişimi
ISS	İnternet security system
IT	Bilişim teknolojisi
İDEA	Uluslar arası veri şifreleme algoritması
İETF	İnternet mühendisliği görev gücü
İPSEC	İnternet güvenlik protokolü
KAMU SM	Kamu sertifikasyon merkezi
KBYS	Kurumsal bilgi yönetim sistemi
KDC	Kerberos protokolü
KM	Kayıt makamı
KSM	Kök sertifika makamı
LDAP	Basit dizin erişim protokolü
MAC	Mesaj onaylama algoritması
MD	Mesaj özet algoritması
NIST	Ulusal teknoloji standartları enstitüsü
NSA	Ulusal güvenlik ajansı
OCSP	Çevrimiçi sertifika durum protokolü
PGP	Güvenli e-mail, dosya şifreleme protokolü
PKCS	Açık anahtar alt yapısı standardı
PKI	Public key infrastructure(Açık Anahtar Altyapısı)
RIPE-MD	RACE Bütünlük Asli Mesaj Değerlendirme Özeti
RSA	Rivest, Shamir, Adlemon
S/MİME	Güvenli e-posta haberleşmesi
SA	Güvenlik ilişkisi
SCEP	Üyelik Protokolü
SCVP	Basit sertifika onaylama protokolü
SHA	Güvenli özetleme algoritması
SID	Güvenlik İD
Sİ	Sertifika ilkeleri
SİL	Sertifika iptal listesi
SKIP	Internet Protokolleri için Basit Anahtar Yönetimi

SM	Sertifika makamı
SMTP	E-posta gönderme protokolü
SSH	Güvenli kabuk
SSL	Güvenli Soket Kademesi
SUE	Sertifika uygulama esasları
TGT	Bilet-sağlayıcı Bilet
TK	Telekomünikasyon kurumu
TLS	Nakil katmanı güvenliği
TSP	Zaman damgası protokolü
TÜBİTAK-UAKAE	Ulusal elektronik ve kriptoloji araştırma enstitüsü
UYAP	Ulusal yargı ağı projesi
VPN	Sanal özel ağ
WWW	Dünya çapında ağ

1. GİRİŞ

Günlük yaşamımızdaki değişiklerin kaynağında teknolojik gelişmeler yatmaktadır. Bu gelişmeler yaşamımızı etkilemektedir. Teknolojik gelişmelerin sonucunda ortaya çıkan bu ürünler hem toplumda hem de işletmelerde büyük değişikliklere neden olmaktadır. Bugün, eskiden hayal bile edemediğimiz yenilikler teknoloji ve teknolojinin sürekli gelişmesi sayesinde ortaya çıkmaktadır.

Teknolojinin gelişmesi ile birlikte bilgiye gereksinim daha da artmaktadır. Bilginin toplanıp derlenerek anlamlı bir duruma getirilmesi ve bu bilgilere erişim önem kazanmaktadır. Bilginin istenilen zaman ve yerde doğru olarak elde edilebilmesi için bilişim (teknolojisi) sistemleri kurulmaktadır.

- Bilişim teknolojilerinde yaşanan gelişmeler; toplumlarda ve devlet yapılarında değişimleri, dönüşümleri ve gelişmeleri zorunlu hale getirmektedir.
- Bilişim teknolojilerin hayatımıza girmesi ile:
- Yeni iş alanları açılabilecek
- Kayıplar azaltılmış olacak
- Rekabet ortamı sağlanacak
- Bürokrasi azaltılacak
- Yeni bilgilerin üretilmesi ve teknolojilerin gelişmesine katkıda bulunacak
- Yaşam kalitesi artacak
- Bilgilerin aktarılması paylaşılması durumlarında karşılaşılacak tehlikeler ortadan kalkacaktır.

Yukarıda bahsedilen beklentilerin karşılanabilmesi için; bilişim teknolojisinin daha çok kullanılmasını sağlamak, politika ve hedefler ortaya koymak, yöntemler geliştirmek ve dokümanlar oluşturmak gerekmektedir. Bunları yerine getirebilmek için, bilgi, bilgisayar ve bilişim sistemleri güvenliği çok önemlidir. Bunun sağlanması için, bilginin karşılaşılabilecek tehlikelerden korunması ve bu korumanında yasal olarak denetlenmesi gerekmektedir.

Bilgi ve bilgisayar teknolojilerinin güvenliğinin sağlanabilmesi için, doğru teknolojileri doğru amaçla ve doğru şekilde kullanarak, bilginin her türlü elektronik ortamda istenmeyen kişiler tarafından elde edilmemesi en önemli faktördür. Elektronik ortamları kullanan kişilerin karşılaşabilecekleri tehlikelere ve tehditlere karşı gerekli önlemleri almaları veya alma yollarını bilmeleri gerekmektedir. Günümüzde kullanılan birçok metodu bulunmaktadır, fakat önemli olan bunlardan en uygun ve doğru olanını kullanabilmektir. Yüksek bir güvenlik için, gizlilik,

bütünlük, kimlik kanıtlama inkâr edememe, fiziksel güvenlik, şifreleme ve antivirüs yazılımları gibi yöntemler kullanımı hızla artmaktadır.

Elektronik ortamda iletilen veya alınan verilerin, kime ait olduğunun doğrulanması, kimin tarafından gönderildiğinin belirlenmesi, gönderen kişinin gönderdiğini inkâr edememesi, iletilen veya alınan verinin içeriğinin değiştirilememesi, başkaları tarafından elde edilse bile değiştirilemediğinin garanti edilmesi gerekmektedir. İşte bunları gerçekleştirebilmek için e-imza ve açık anahtar altyapısı kullanılmalıdır.

Açık anahtar altyapısının; elektronik imza ile kullanılmasıyla kanuni açıklar ortadan kaldırılacak, kayıplar en aza indirilecek, yasal zorunluluklar yerine getirilecek, bilgi toplumu olma süresi kısalacak ve yukarıda belirttiğimiz maddeler uygulandığı takdirde bilgi güvenliği de sağlanabilecektir.

Elektronik yaşamın uygulanabilmesinin en önemli şartlarından birisi, elektronik ortama ve ağ sistemine olan güvenin sağlanmasıdır. Mevcut bilginini güvenliği vazgeçilmez ve önceliği çok yüksek uygulamalardan biridir. Bundan dolayı, karşılıklı haberleşmelerde; bilginin gizliliği, bütünlüğü, haberleşen kişilerin kimlik kontrolleri kurulacak olan teknik ve yasal altyapılarla garanti edilmelidir. İşte bu noktada elektronik imza ortaya çıkmaktadır.

Elektronik imza sağlamış olduğu kimlik doğrulama, veri bütünlüğü ve inkâr edememelik gibi özellikler ile sanal ortamda karşılaşılan söz konusu güvenlik ve güvenilirlik sorunlarının aşılmasına katkıda bulunmaktadır. Ayrıca elektronik imza, elektronik ortamdaki belge ve işlemlerin hukuki açıdan da geçerli olmasını da mümkün kılmaktadır.

Elektronik imza altyapısı, bize, kimlik tespiti, bütünlük kontrolü ve inkâr edilemezlik gibi ıslak imza ile sağlanan fonksiyonların elektronik ortamda temin edilmesi için geliştirilen bir yöntemdir. Elektronik imzanın yakın bir zamanda günlük yaşamımıza gireceği ve yaşamın ayrılmaz bir parçası olacağı konusunda yalnız uzmanlar değil; pek çok kişi görüş birliği içindedir. Çünkü güvenli bir imza yöntemi olmadan güvenli bir elektronik haberleşmeden söz etmek mümkün değildir. Bu gereksinim, yalnızca şirketler, kurum veya kuruluşlar için değil, aksine elektronik ortamda hukuken bağlayıcı işlemler yapmak isteyen herkes bakımından söz konusudur.

1.1 Dünyada Yapılan Çalışmalar

1.1.1 Avustralya federal hizmet uygulamaları

- Centrelink
- Avustralya Seçim Komisyonu
- Sağlık Sigortası Kurumu
- Gümrükler
- Elektronik İhaleler
- İş ve İşçi Bulma

Şirketler için Australian Business Number – Digital Signature Certificate (ABN-DSC), şirket tescili ile birlikte e-imza sertifikası

1.1.2 Estonya ID card projesi

- Estonya vatandaşları ve oturma izni olan yabancılar için zorunlu kimlik kartı – ID card
- Tüm ID card'lar birer akıllı kart ve üzerinde hem özel hem kamu uygulamalarında kullanılabilecek e-imza için gerekli gizli anahtar ve sertifika
- Ocak 2002'den bugüne 500 000 kart verilmiş (nüfus 1,4M)

1.1.3 Proje riverside county California

- Kullanıcı
  - Riverside County Hazine ve Tapu Kayıt Kurumları
- Amaç
  - Faz I- Vergi beyannamelerinin elektronik kaydı
  - Faz II- Tapu Sicil değişikliklerinin elektronik kaydı
- Durum
  - Faz I tamamlandı
  - Faz II hazırlık aşamasında

1.1.4 Almanya DSV

DSV (Deutscher Sparkassen Verlag) Alman bankacılık sisteminin (Sparkassen Finanzgruppe) servis sağlayıcısıdır. Deutscher Sparkassen Verlag (DSV), sunduğu bankacılık alanına yönelik ürün ve hizmetleri ile yaklaşık 600 kuruluşu (tasarruf bankaları, kamu bankaları, kamu sigorta şirketleri, v.b.) ve 18,000 şubeyi içeren Sparkassen-Finanzgruppe (Almanya

tasarruf bankaları kurumu) için ana tedarikçi konumundadır. DSV, Finans kuruluşlarına Pazarlama ve medya hizmetleri, debim ve kredi kartları basımı, elektronik ödeme sistemleri ve ATM'ler için terminaller de dâhil olmak üzere fonksiyonel bazda ürün ve hizmet sunmaktadır. DSV, Mayıs 2001'de Verisign ile yaptığı partnerlik anlaşmasıyla, sayısal sertifika kullanımına olanak sağlayan akıllı kartlar için Verisign'ın altyapısından faydalanmaya başlamıştır. Önümüzdeki yıllarda basılacak 20 milyon akıllı karta, Verisign'ın dijital sertifika hizmetlerini kullanarak sertifika eklemeyi ve 600 üye finans kuruluşunun e-mail doğrulama işlemleri için dijital sertifika altyapısı sunmayı planlamaktadır. Sayısal sertifikalı akıllı kartlar, kullanıcılarının doğrulanmasında ve kullanıcıların internet üzerinden daha güvenli işlem yapmalarına olanak sağlamaktadır. Buna göre DSV, Verisign'ın yönetilen sayısal sertifika hizmetlerini genel bankacılık hizmetlerini daha güvenilir hale getirmek için kullanmaktadır.

1.1.5 Kanada CIBC (Canadian Imperial Bank of Commerce)

CIBC, 9 milyondan fazla bireysel ve kurumsal müşterisi bulunan, Kuzey Amerika'nın lider finansal kuruluşlarından biridir. CIBC, kapsamlı elektronik bankacılık ağı boyunca müşterilerine bankacılık alanında uçtan uca ürün ve hizmetler sunmaktadır ve aynı zamanda Verisign'ın Kanada'daki iş ortağı, işleme merkezi (processing center) olarak da faaliyet göstermektedir. CIBC işleme merkezi, Verisign'ın PKI platformu, güven hizmetleri altyapısını ve işletme hizmetlerini içine almaktadır. CIBC temelde web sunucu ve işletme sertifika hizmetlerini sunmaktadır. CIBC, Kanada çapında sertifika yetkilendirme hizmetlerini sağlamakta ve sertifika işlemlerinin yanı sıra pazarlama, satış, güvenlik, müşteri destek ve operasyon yönetimi gibi hizmetleri de sunmaktadır.

İhtiyaçlar / Çözüm: CIBC, imza gerektiren uygulama ve hizmetlerine online olarak ulaşma ve kullanma olanağını müşterilerine sunmayı ve böylelikle de müşteri rahatlığı ve memnuniyetini artırırken uygulama süreç maliyetlerini azaltmayı hedeflemiştir. Normalde bütün CIBC müşterileri VISA kartı, banka hesabı açtırma gibi işlemler için şubeleri ziyaret ederek, yada posta yoluyla başvuru talebini yaparak süreci başlatabiliyorlardı. Bütün başvuruların müşteri tarafından imzalanmış olması gerektiğinde müşterilerin formu ya direk şubeden almaları yada posta yoluyla alıp imzalayıp tekrar geri göndermeleri gerekiyordu. CIBC bu süreci hızlandırmak ve kolaylaştırmak istedi. 2001'in Şubat ayında CIBC bireysel banka müşterilerine sayısal imza kullanarak uygulamaları imzalama ve bütün bankacılık hizmetlerini online olarak alabilme olanağını tanıyan Kanada'daki ilk banka olmuştur.

Sağlanan Faydalar: Daha fazla Kanadalı firmanın ve bireyin elektronik ticaret işlemlerini güvenli bir şekilde gerçekleştirmeleri sağlanmış, banka müşterilerinin memnuniyeti artarken, CIBC de maliyetlerden ve işlemler için harcanan zamandan tasarruf sağlamıştır.

1.1.6 İngiltere – Barclays

Barclays, temelde bireysel bankacılık, yatırım bankacılığı ve yatırım yönetimi konularında faaliyet gösteren, İngiltere'deki finansal hizmet sunan en büyük gruplardan biridir. Barclays'in 2003 sonu itibariyle 700,000'in üzerinde kurumsal müşterisi ve internet bankacılığını kullanan 4,5 (285,000'i kurumsal) milyon müşterisi bulunmaktadır.

İhtiyaçlar / Çözüm: Barclays, PKI altyapısını kurması ve işletmesi için BT Ignite ile çalışmaya karar vermiş, güvenlik çözümleri sağlayan bu kurum, elektronik ticaretin kullanımı sırasında hem Barclays grubu şirketlerini, hem de müşterilerini korumak üzere güvenli teknoloji çözümlerini (PKI) sağlamıştır. Bu hizmet ile Barclays, müşterileri ile arasında ve aynı zamanda kurum içerisinde, elektronik ortamdaki bilgi alışverişini güvenli hale getirmiştir. Ayrıca kurumsal müşterilerine kendi müşteri ve tedarikçileriyle internet ortamında daha güvenli işlemler gerçekleştirmelerini sağlayacak hizmetler geliştirme fırsatına sahip olmuştur.

1.1.7 Japonya – Suzuken firması

Suzuken, merkezi Nagoya'da yer alan ve ülke çapında 110.000 eczane ve ilaç kuruluşuna ilaç ve tanı medikal ekipmanı sağlayan bir ilaç toptancısıdır. Suzuken Grubu, Sanwa Kagaku Kenkyusho Co., Ltd. (ilaç şirketi), Nihon Seiyaku Kogyo Co., Ltd. (ilaç üreticisi), Kenzmedico Co.,Ltd. (ekipman üreticisi) ve Lifemedico Co., Ltd. (sağlık alanda faaliyet gösteren reklam şirketi) şirketlerinden oluşmakta olup sağlık hizmetleri alanında toplu bir güce sahiptir.

İhtiyaçlar / Çözüm: Suzuken, 2001 yılında ilaç şirketleri yani müşterileri ile olan bilgi alışverişi ve online ürün talepleri için web tabanlı bir satış destek sistemini hizmete sokmuştur. Bu sistemdeki e-posta, ürün talep bilgileri ve diğer değerli bilgilerin güvenli için PKI teknolojisi kurulmuştur. Buna göre bir sertifika otoritesi her kurumdaki her bir satış temsilcisi için sertifika dağıtımını gerçekleştirmiş ve bu sertifikalar sayesinde kimlik doğrulama ve onay işlemleri gerçekleştirilmeye başlanmıştır. Müşterilerin ilk giriş sayfasında kimlikleri onaylandıktan sonra diğer sayfalarda tekrardan güvenlik için bilgi sormaya gereklilik ortadan kalkmış ve böylelikle de sistemin kullanıcılar tarafından kullanımı kolaylaşmıştır.

1.1.8 Hong Kong – Hong Kong Post

Hong Kong sertifika otoritesi 2000 yılından itibaren sadece 110,000 e-Cert (sayısal sertifika) satabilmiştir. Kurum sertifika kullanımını artırmak için, akıllı kimlik kart sahiplerine sertifikaları kartlarına yerleştirme olanağını bir yıl için uluslar arası ücret almadan gerçekleştirme önerisiyle gitmiştir.

1.2 Türkiye'de Durum

Ülkemizde elektronik imzanın kullanımı için gerekli yasal çalışmalar, ilk kez 29 Haziran 2001 tarihinde Hazine Dış Ticaret Müsteşarlığı koordinasyonunda oluşturulan Hukuk Alt Çalışma Grubu tarafından başlatılmıştır. Adalet Bakanlığı, 14 Ocak 2002 tarihli yazısı yeni bir çalışma komisyonu kurarak kısa sürede "Elektronik İmzanın Düzenlenmesi Hakkında Kanun Tasarısı" taslağını hazırlamış, söz konusu tasarı taslağı, 10 Eylül 2002 tarihli yazı ile kurumların görüşüne sunulmuş ve 19 Şubat 2003 tarihinde Başbakanlığa gönderilmiştir.

Elektronik İmza Kanun Tasarısı, 15 Ocak 2004 tarihinde TBMM Genel Kurulu'nda görüşülerek kabul edilmiş, Kanun, 23 Ocak 2004 tarih ve 25355 sayılı Resmi Gazete'de yayımlanmıştır. İkincil düzenleme çalışmaları Telekomünikasyon Kurumuna verildiğinden Kanunun verdiği 6 aylık zamandan önce ikincil mevzuat çalışmaları tamamlanarak yürürlüğe girmiştir. Mevzuat çalışmalarının ardından elektronik imzanın uygulamaya girmesi için gerekli çalışmalar başlamıştır.

Elektronik imza kullanımında en önemli aktörlerin başında elektronik imza hizmet sağlayıcıları (ESHS) gelmektedir. Elektronik sertifika hizmet sağlayıcısı olmak için şimdiye kadar biri kamu, üçü özel olmak üzere dört kurum faaliyete geçmek üzere Telekomünikasyon Kurumu'na bildirimde bulunmuş ve lisanslarını almıştır. Dolayısıyla elektronik imza kullanımı için gerekli elektronik sertifikalar bu kurumlardan sağlanabilmektedir. Diğer taraftan ilk elektronik imza, 18 Temmuz 2005 tarihinde kullanılmıştır.

İlk olarak ülkemizde yapılan çalışmada Dâhilde İşleme Rejimi (DİR) Otomasyon Uygulamasıdır. Uygulama ile ihracatçı firmalar zaman ve mekân kısıtlaması olmaksızın Dış Ticaret Müsteşarlığınca düzenlenen Dâhilde ve Hariçte İşleme Rejimi kapsamındaki belgelerine ilişkin tüm işlemleri elektronik ortamda gerçekleştirebilecektir.

1.3 Bazı Ülkelerde Yapılan Çalışmalar ve Yaşanılan Sorunlar

1.3.1 Almanya

E-imza Kanunu 2000 yılında yürürlüğe girmiştir. Nitelikli İmza için talep hala düşüktür. Bu durumun sebeplerinden birisi, vatandaşların kendi arasındaki, vatandaş ile şirketler arasındaki ve şirketlerin kendi arasındaki birçok işlemin kanunlara göre ıslak imza gerektirmemesidir. Dolayısıyla, nitelikli imzadan daha kolay ve ucuz olan çözümler kullanılır. Örneğin, birçok banka işlemi nitelikli imza yerine şifreler ile yapılmaktadır. Devlet ile vatandaşlar arasındaki ve devlet ile şirketler arasındaki işlemler çoğunlukla ıslak imza gerektirse de devlet ile etkileşim az olduğundan nitelikli imzaya yatırım yapmak gereksiz görülmektedir. Dolayısıyla, nitelikli imza kullanıcılarının çoğu avukatlar veya belli devlet kurumlan ile yüksek

oranda işlem yapan şirketlerdir. E-imzanın yaygınlaşmasını engelleyen bir diğer önemli sebep de, orta ve uzun vadede e-İmzalı belgelerin dosyalama sorunudur. Bu konuda standartların geliştirilmesinin gerektiği belirtilmektedir. Düşük seviyedeki nitelikli sayısal imza kullanım oranını arttırmak için e-imza kanununda bazı değişiklikler yapılmıştır. Bu değişiklik ile bizzat başvuru gerekliliği kaldırılmıştır. Buna göre kişinin daha önceden alınan bilgilerine dayanarak kimlik tanımlama yapılabilmekte (Örn; banka müşterileri) ve internet üzerinden başvuru alınabilmektedir. Başvuru prosedürünün kolaylaştırılması ile maliyetlerin azaltılması hedeflenmiştir.

1.3.2 İngiltere

E-imza Kanunu 2002 yılında yürürlüğe girmiştir. En fazla gerçekleştirilen ticari elektronik işlem tipi bireysel elektronik bankacılıktır ve bu alanda şifreleme teknikleri kullanılmaktadır. İşlemlerin sertifika tabanlı kimlik doğrulama yöntemleri ya da güvenli elektronik imza oluşturma aracı ile güvenli şekilde yapılmasına çok az ihtiyaç duyulmaktadır. Elektronik imzaların yaygınlaşmasını engelleyen başlıca sebep talep eksikliğidir. Potansiyel kullanıcıların neye ihtiyaçları olduğu konusunda kafaları karışıktır. Sertifikalar kazanılacak olan faydaya göre çok pahalı (satın alım ücreti, yükleme, eğitim vs masrafları dahil) olarak algılanmaktadır ve tüketiciler şu an için gerçek bir fayda görememektedirler. Kullanıcının bu konudaki eğitim eksikliği de bir diğer faktördür. Bu durum için sorumluluk, teknoloji üstünde çok odaklanıp, yeterli seviyede e-imzanın faydalarını anlatmadıkları için, kısmen hizmet sağlayıcılara yüklenmiştir. Birbiriyle uyumlu çalışan uygulamaların eksikliği pazarın büyümesini engelleyen önemli bir faktör olarak değerlendirilmektedir. İş dünyası ise daha fazla güvenlik, bütünlük ve gizlilik olmadan iş yapmayı çok gerekli görmemektedirler. Zaman İçinde şirketlerin risk analizi yapmayı öğrenip, güvenlik ile ilgili seçimleri konusunda bilinçli olacakları ve e-imzaya olan talebin artacağı değerlendirilmektedir. Devletin, e-imza kullanımından doğacak kazanımlar hakkında halkı ve iş dünyasını bilinçlendirme konusunda yetersiz kaldığı şeklinde eleştiriler de mevcuttur.

1.3.3 İspanya

E-imza Kanunu 2003 yılında yürürlüğe girmiştir. Kamu sektöründe e-imza kullanımını teşvik etmek için vergi İade işlemlerinde olduğu gibi bazı başarılı girişimler olduysa da, e-imza diğer sektörlerde yaygınlaşmamıştır. Elektronik kimlik kartlarının çıkmasının e-imza kullanımının yaygınlaşmasını sağlayabileceği belirtilmektedir. Özel sektördeki e-imza kullanımının düşük olmasının olası sebepleri şu şekilde ifade edilmiştir;

- E-imza kullanımının faydası sadece, gerçek dünyada prosedürlerin karmaşık ve bürokrasinin çok olduğu yerlerde görülebilmektedir.

- SSL gibi basit ve hâlihazırda mevcut olan alternatif teknolojiler kullanıcıya az veya orta derecede değerli e-ticaret işlemleri için yeterli seviyede güvenlik ve rahatlık sağlamaktadır.
- Hukuki açıdan geçerli olan e-imza elde etmek için prosedürler olarak daha uzundur ve imza gerekliliklerin maliyeti tüketiciye yansıyabilmektedir.
- İspanyol e-imza kanununa göre hukuki açıdan tanınmış bir sertifika başvurusu esnasında işinin bizzat bulunma zorunluluğu vardır.

1.3.4 Çek Cumhuriyeti

E-imza Kanunu 2000 yılında yürürlüğe girmiştir. Enformatik Bakanlığı e-imza kullanımını teşvik etmeye çalışmaktadır. "Belediyeler için E-imza" projesi altında, Bakanlık yaklaşık 1850 adet belediye için, kendi idari işlerinde kullanmak üzere ücretsiz e-imza sağlamıştır. Bakanlık, e-imzanın kullanımını kamu idareleri ve vatandaşlar için daha kolay hale getirmek üzere bir uygulama hazırlamaktadır.

1.3.5 Türkiye

- Adalet Bakanlığı

Adalet Bakanlığı Bilgi İşlem Dairesi Başkanlığı, kurum içi yazışmalarda Kamu SM e-imza sertifikalarını 14.08.2006 tarihinden itibaren kullanmaya başladı. Adalet Bakanlığı Müsteşar Yardımcıları'nın da aralarında bulunduğu sertifika sahiplerine teslim edilen sertifikalar aktif hale getirilerek kullanıma açıldı. Yapılan bu uygulama için gelen en önemli şikâyet işlerin yavaş yürümesi olmuştur.

- Problemler

Yukarıda bahsettiğimiz konuların uygulanmasında yaşanılan bazı problemler aşağıda genel olarak sıralanmıştır:

- Kullanıcıların bilgisayar ve bilgi güvenliği konusunda yeteri bilgiye sahip olmamaları
- Elektronik ortamda gelebilecek saldırıları bilmiyor olmaları
- Gelebilecek bu saldırılara karşı ne tür önlem alınabileceğinin bilinmemesi
- Şifre veya şifrelemenin doğru olarak uygulanamaması
- Elektronik imza uyum maliyetlerinin yüksek olması
- Standartlaşma konusunda önemli eksiklerin bulunması
- Mevcut düzenlemelerde halen bazı sorunların aşılamamış olması
- Hukuki açıdan önemli sayılabilecek eksikliklerin bulunması
- Elektronik imza konusunda kullanıcıların yeterince bilgilendirilmemesi

- Elektronik imzaya yeterince talebin yaratılamamış olmaması
- Elektronik imza yazılımlarının güvenilirliği
- Kullanıcıların elektronik imza uygulamalarına adapte olacak bilgi seviyelerine sahip olmamaları (bilgisayar okuryazarlığının düşük olması)
- Türkiye'de Internet alt yapısının yeterli olmaması
- Teknik bilgi konusunda yetersiz kalınması
- Devletin elektronik imza konusunda yeterince aktif olmaması
- Kullanıcı ile kurumlar arasında 3. bir aracı kurumun olmasından (ESHS'ler) dolayı kullanıcılarda güvensizlik oluşması
- ESHS'lerin kullanıcılara tanıtılmaması
    - ESHS nedir?
    - Görevleri nelerdir?
    - Kime bağlıdır?
    - Denetimi nasıl yapılmaktadır?

Bu çalışmada, ilk olarak bilgi ve bilgisayar güvenliğini inceleyip güvenlik problemleri, çözümü ve yapılması gereken konular üzerinde durduktan sonra Türkiye'de elektronik imzanın kullanımı konusunda gelinen aşamayı teknik altyapı açılarından ele alınacaktır. Elektronik imza kullanımında asli unsur denilebilecek Kamu SM (kamu sertifikasyon merkezi) ESHS (Elektronik Sertifika Hizmet Sağlayıcı) yapısının, Kamu SM sertifika ilkelerinin, kök sertifika hizmet sağlayıcılarının, NES (Nitelikli Elektronik Sertifika),e-imza uyum çalışmalarının, elektronik sertifika sağlayıcıları, Türkiye'de öngörülen sertifikasyon modeli, Telekomünikasyon Kurumu, Kamu Sertifikasyon Merkezi, elektronik imzanın uygulamaya konması için aşılması gereken problemler ve çözüm yolları tartışılmıştır. Örnek bir web uygulamasının yapılıp e-imza oluşturulması ve doğrulanması sağlanacaktır. Bu örnek için Windows işletim sistemi tercih edilecektir. Web sunucusu (apache) kurulacak ve web ara yüzü (php veya java script ile) oluşturulacaktır. Ayrıca elektronik imzaya geçmiş kurum ve kuruluşların incelenmesi yapılacaktır.

2. KURAMSAL TEMELLER

Elektronik imza sahip olduğu kimlik doğrulama, bütünlük ve inkâr edilemezlik ile sanal ortamda hızla artan oranlarda ihtiyaç duyulan güvenlik, güvenilirlik ve hukuki açıdan ihtiyaçlara cevap veren bir teknolojidir

Elektronik imza; başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veriyi tanımlar. Elektronik imza; bir bilginin üçüncü tarafların erişimine kapalı bir ortamda, bütünlüğü bozulmadan (bilgiyi ileten tarafın oluşturduğu orijinal haliyle) ve tarafların kimlikleri doğrulanarak iletildiğini elektronik veya benzeri araçlarla garanti eden harf, karakter veya sembollerden oluşur.

Elektronik imza; gelişmiş teknolojiler kullanarak, elektronik ortamda gönderilen veya alınan bilgilerin, bunların gönderen kişi veya kuruma ait olduğunun doğrulanmasını, iletilen veya alınan verilerin bilinmeyen kişiler tarafından gönderilmediğini veya bildiğimiz kişiler tarafından gönderildiğinin belirlenmesini, verileri gönderenlerin gönderdiği ve alanların aldığını inkâr edememesini, başkaları tarafından elde edilse bile, içeriğinin başkaları tarafından anlaşılamamasını sağlayan, elektronik ortamda bit katarlarından oluşturulmuş güvenli haberleşme ortamına verilen addır.

Bit ise: En küçük birim bit'tir. Bilgisayar içinde karakterler ikilik sayı siteminde 8 haneli bir sayıyla ifade edilir. İşte bu sayının her bir basamağına 1 Bit denir. Örneğin: A karakteri bilgisayar içinde 0100001 sayısıyla ifade edilir. İşte bu sayının her basamağına 1 Bit denir. O zaman Bilgisayar içindeki her bir karakter 8 bit'ten oluşur. A karakteri=8 Bit, + karakteri=8 bit.

Elektronik imzanın iletiminde şifreleme yöntemlerinden asimetrik şifreleme ve simetrik kriptolama yöntemleri kullanılmaktadır.

Kriptografi kriptolama ve dekriptolama diye bilinen iki işlem üzerine kuruludur. Kriptolama bir mesajını okunamayacak şekle sokma işlemine denir. Bu kriptolama anahtarı ile gerçekleştirilir(Bir anahtar rasgele bit`lerden oluşan yazıdır. Bit sayısı kripto-sistemi`ne göre değişir.).

Dekriptolama mesajı orijinal şekline çevirme işlemidir. Buda bir dekriptolama anahtarı ile gerçekleştirilir. Bir mesaj kriptolanmadan önce düz-yazı formatındadır. Kriptolama işlemi sonrası mesaj şifreli-yazı formatına geçer.

Asimetrik şifrelemede iki adet anahtar oluşturulur. Bu anahtarlar genel anahtar (public key) ve özel anahtar (private key) olarak adlandırılır. Public key ile veri şifrelenir private key ile de sadece şifrelenmiş veri deşiflenip orijinal hale getirilir. Public key olarak belirtilen anahtar umuma açıktır ve herkes tarafından bilinmesinde herhangi bir sakınca yoktur. Çünkü bu anahtarla sadece veri şifrelenir ve bu anahtarla şifrelenmiş veriler ancak ve ancak public key e karşılık oluşturulmuş private key (özel anahtarla) çözülebilir. Bu itibarla private key'in kesinlikle gizli olarak kalması gerekir.

Simetrik kriptografi, şifrelemede ve şifreyi çözmede aynı kriptolama anahtarını kullanır. Simetrik kriptografi aynı zamanda Özel Anahtar Kriptografi olarak da bilinir. Asimetrik kriptografi ya da açık anahtar kriptografi sistemi ise kriptolama ve dekriptolama için bir çift anahtar kullanır. Bir anahtar (açık anahtar) mesajı kriptolamak için kullanılır ve diğer anahtar (özel anahtar) dekriptolamak için kullanılır.

Elektronik imzanın teknik altyapısı olan Açık Anahtar Altyapısı kriptolama işlemi üzerine kuruludur ve bu bilgiler kişi bilgileri ile birlikte elektronik sertifikada tutulmaktadır.

Elektronik sertifika, kullanıcı kimliği ile kullanıcı için üretilen imza doğrulama verisini, yani kullanıcının açık anahtarını birbiri ile ilişkilendiren bir veri yapısıdır. Bu özelliği ile elektronik sertifika kullanıcıların sanal ortamdaki kimlik kartı olarak nitelendirilebilir.

Elektronik imza konusunda yukarıda belirtilmiş olan kavramların belli miktarda bilinmesi gerekmektedir.

3. BİLGİ VE BİLGİSAYAR SİSTEMLERİ GÜVENLİĞİ

Bilgi teknolojilerinin kullanımının hızla yaygınlaştığı ve arttığı günümüzde bilgi ve bilgisayar sistemlerinin güvenliği en önemli konu olmaktadır. Bu konuyu anlamak, kavramak ve uygulayabilmek için konumuz içerisinde geçen terimleri iyi bilmek gerekir.

Bilgi, üzerinde çalışılan içerik ve perspektife göre pek çok çeşitte anlamlar içeren karmaşık bir kavramdır. Bazı tanımları[1] :

- Öğrenme, araştırma veya gözlem sonucu elde edilen gerçek ve ilkelerin bütününe verilen isim
- Üzerinde kesin bir yargıya varılmamış, anlam kazanmış her türlü ses, görüntü ve yazılara verilen isim
- Bilişim kurallardan yararlanarak kişinin veriye yönelttiği anlam

Bilgiyi 3 farklı başlık altında toplayabiliriz: veri (data), bilgi (information) ve özbilgi (knowledge)

Sayısal ve mantıksal her türlü değer (sinyaller, bitler) bir veridir. Verinin belli bir anlam ifade edecek şekilde sınıflandırılmış hali de bilgidir. Bir araç haline dönüşmek üzere daha fazla işlenmiş bilgi ise asıl değerli olan öz bilgidir[2]. Bilginin değerli veya değersiz olduğunun belirlenmesi bilgi kadar önemlidir. Değersiz olan bir bilgiyi değerli gibi görüp onu korumak ve işlemek için kullanılan kaynakların gereksiz olarak harcamasına sebep olabileceği gibi, değerli olan bilginin gerektiği gibi korunmaması sonucu maddi ve çok önemli kayıplar ile haksız rekabet ortaya çıkacaktır. Değerli olan bu bilginin, kişiler, kurumlar veya ülkeler için önemli olduğu ve korunması gerektiği aşikârdır.

Güvenlik ise bilgisayar sistemlerinde karşılaşılabilecek tehditlere karşı önlem alma işlemleridir ve dünya gündeminde olan bir konudur. Uluslar arası bilgi güvenliği standardı olan BS 7799–1:2000'de bilginin güvenliği için şu ifadeler kullanılmıştır: Bilgi bir aktif varlıktır ve bir işyerinin diğer önemli aktif varlıkları gibi, kuruluş için bir değeri vardır ve dolayısıyla uygun bir biçimde korunması gereklidir. ISO 17799–1:2000'de ise: Bilgi birçok formlarda bulunabilir. Kâğıda basılabilir, elektronik olarak depolanabilir, posta veya elektronik yollar ile gönderilebilir, filmler üzerinde gösterilebilir, sohbetlerle konuşulabilir. Bilgi hangi biçimde olursa olsun her zaman uygun olarak korunmalıdır.

Bilginin güvenliğini; bilginin bir varlık (asset) olarak hasarlardan korunması, doğru teknolojilerin kullanılarak bilginin istenilemeyen kişiler tarafından ele geçirilmesini önleme olarak tanımlayabiliriz[3].

Bilgi güvenliğini;

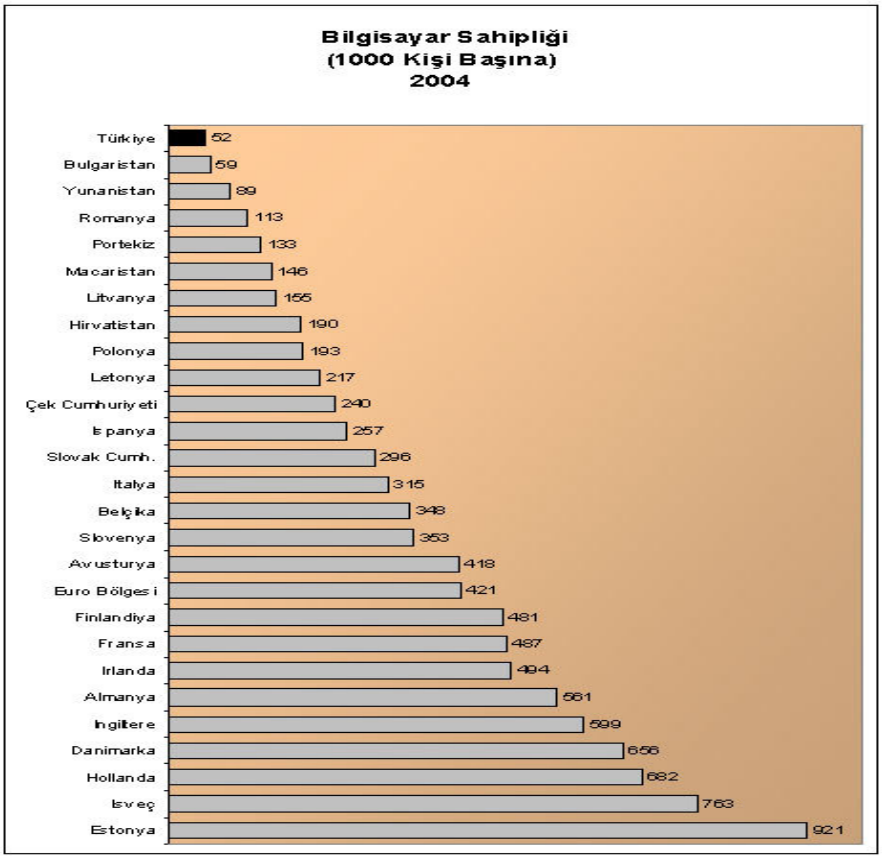
Gizlilik (Confidentiality), Doğruluk/Bütünlük (İntegrity), Bulunurluk (Availability) olarak üç temel bileşen altında toplayabiliriz. Bunları açıklayacak olursak:

- Gizlilik (Confidentiality): Bilginin sadece erişmeye hakkı olan kişiler tarafından erişilebilir olduğundan emin olmak
- Doğruluk/Bütünlük (İntegrity) : Bilgi ve bilgi işleme süreçlerinin doğru, kesin ve eksiksiz olduğunun güvence altına alınması
- Bulunurluk (Availability) : Bilgi varlıklarına izin verilen kullanıcıların ihtiyaç duydukları zamanlarda erişilebilir olduklarının güvence altına alınması

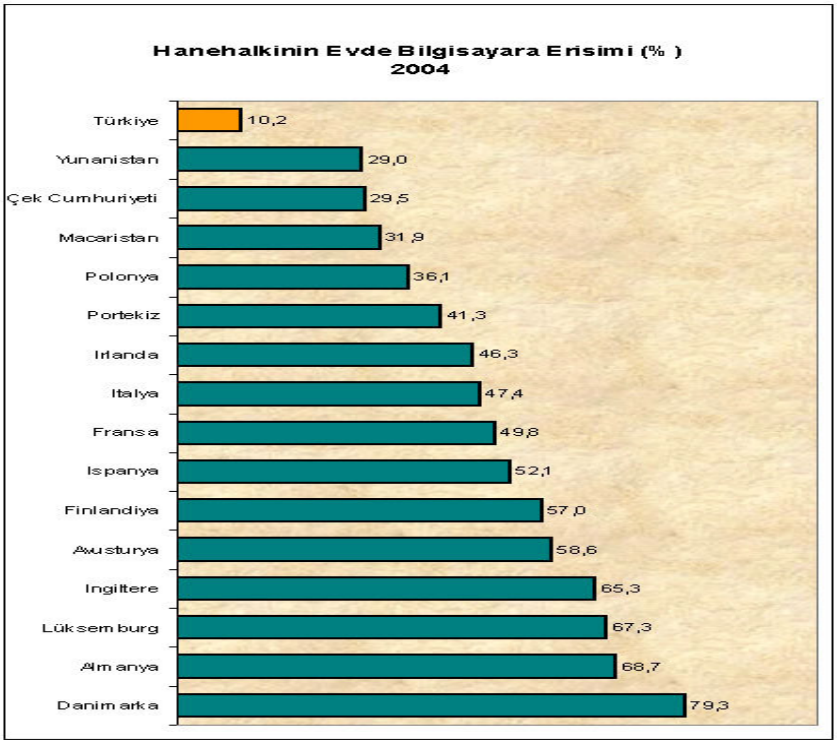
Bilişim teknolojilerinde güvenliğin amacı, elektronik ortamlarda tutulan bilgilerin, bu teknolojileri kullanarak karşılaşabilecek tehdit ve tehlikelerin daha önceden analizlerinin yapılarak gerekli önlemlerin kişi, kurum ve kuruluşlar tarafından alınması, bilginin bir varlık olarak hasarlardan korunması ve doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda istenmeyen kişiler tarafından elde edilmesini önlemektir. Bilgileri koruma seviyesi ve çeşidi arttıkça saldırı seviyesi ve çeşidi de artmaktadır. Bilgiyi koruyabilmek için kimlik kanıtlama, inkâr edememe, fiziksel güvenlik, insan faktörü, güvenlik duvarı, antivirüs yazılımları, sayısal imza, atak tespit sistemleri ve şifreleme metotlarının ve yaklaşımlarını kullanılması gerekir.

3.1 Bilgi Güvenliğinin Önemi

Türkiye, bilgi çağının en önemli araçlarından bilgisayar ve internet kullanımı, bilgisayara ve internete erişen hane halkı sayısında Avrupa sıralamasının en sonunda yer almaktadır. Ülkemizde her 1000 kişiden 52'si bilgisayara, 142'si internet bağlantısına sahipken her 100 aileden 10'unun evde bilgisayarı ve 7'sinin evde internet bağlantısı bulunmaktadır. Estonya'da her 1000 kişiden 921'i bilgisayar kullanırken, İsveç'te 756'sı internet bağlantısına sahiptir. Hane halkının bilgisayara erişimi sıralamasında Danimarka %79,3 ile ilk sırada yer alırken, Almanya % 68,7 ile ikinci olmuştur. Hane halkının internet sahipliği sıralamasında yine Danimarka %69,4 ile birinci, Almanya %60 ile ikinci sıradadır. Diğer taraftan, Türkiye 14,72 $ ile internet erişiminin en pahalı olduğu ülkedir. Danimarka'da internet erişimi fiyatı Türkiye'ye kıyasla yaklaşık 3,5 kat daha ucuzdur. Yeni rekabet koşullarına ayak uydurarak küresel bir aktör haline gelebilmek için Türkiye'de de bilgisayar ve internet kullanımı desteklenmelidir.



Şekil 3.1. Dünya Bilgisayar Sahipliği Oranı[4]



Şekil 3.2. Hane Halkının Bilgisayara Erişim Oranı[5]

Yıl	Kullanıcılar	Nüfus	% Nüfus	Kullanılan Kaynak
2000	2.000.000	70.140.900	%2.9	ITU
2004	5.500.000	73.556.173	%7.5	ITU
2006	10.220.000	74.709.412	%13.9	Comp.Ind. Almanac

Tablo 3.1. Türkiye'deki İnternet Kullanımının Nüfusa Göre İstatistiği[6]

Türkiye'de 1000 civarında firma üzerinde yapılan testlerde bu kurum ve şirketlerin[7]:

- %85'sinin farklı düzeylerde güvenlik açığı taşımakta oldukları
- %60'nın web sunucusuna kolaylıkla erişilebildiği, web sayfalarının kolaylıkla değiştirebildiği
- %40'nın ana sunucularında ki açılardan dolayı e-posta, adres ve içeriklerinin ele geçirildiği veya bankacılık işlemlerinde kullanılan şifrelerin çalındığı
- %25'inin firewall'unun (güvenlik duvarının) kötü olduğu için her türlü bilgiye ulaşılabildiği
- %30'unun sitemlerinde çok yüksek seviyelerde açıklar bulunduğu ortaya çıkmıştır.
- Son zamanlarda yapılan araştırmalarda ise güvenlik açıklarının çoğunun kötü niyetli olmayan personel hatalarından kaynaklandığı bildirilmiştir.

Bilgi tüm kuruluşların can damarıdır ve birçok şekilde karşımıza çıkabilmektedir. Yazıcıdan yazdırılabilir veya kâğıda yazılabilir, elektronik ortamda saklanabilir, posta veya elektronik yolla iletilebilir, toplantı odanızdaki tahtada yazabilir, masanızdaki post-it de yazabilir, filmlerde gösterilebilir, ya da sohbet esnasında konuşulabilir. Günümüzün rekabete dayanan iş ortamında, bu tür bilgiler devamlı olarak birçok kaynağın tehdidi altındadır. Bu tehditler dâhili, harici, rastlantısal veya kötü niyet şeklinde olabilir. Bilginin saklanması, iletilmesi ve alınması için yeni teknolojinin artan bir şekilde kullanılmasıyla, kendimizi artan sayıdaki tehditlere ve tehdit tiplerine tamamen açmış oluyoruz. Bilgi güvenliği, günümüzde kişisel olarak önemli olduğu kadar, toplumların, kurum ve kuruluşların geleceklerinin teminatıdır. Bunun sağlanması için, yeni teknolojilerin geliştirilmesi, yeni bilgilerin üretilmesi, kayıpların en aza indirilmesi, bilgi ve öz bilgi oluşturulması, depolama ve aktarma esnasında karşılaşılabilecek tehlike ve tehditlerin ortadan kaldırılması ve e-dönüşüm projelerinin hayata geçirilmesi hızlandırılmalıdır.

3.2 Saldırı Sebepleri Ve Türleri

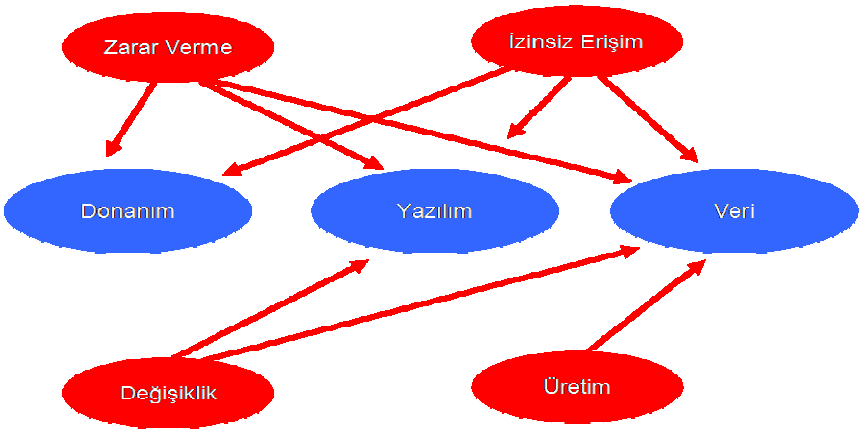
Saldırganlar buldukları en kolay yol ile güvenliğinizi bozmak isterler, bunu da çeşitli yöntemlerle gerçekleştirebilir. Burada en önemli nokta neyin saldırı olarak tanımlandığıdır. Bu noktada saldırıların genel bir gruplandırmasını yapmak mümkündür[8]:

- **İzinsiz Erişim:** Bu saldırı türünde, saldırgan bilgiye (yazılım, donanım ve veri) yetkisi olmadığı halde erişebilmesidir. Aynı bilgiye yetkili kullanıcılar da olağan şekilde erişebilirler, yani bilginin kendisinde bir bozulma yoktur. Bununla birlikte o bilgiye erişmesi beklenmeyen kişilerin bunu yapabilmesi, saldırı olarak nitelendirilir(örn: ağ koklama).
- **Engelleme veya Zarar Verme:** Bu saldırı türünde, bilgiye erişim engellenir. Bilgi ya kaybolmuştur/silinmiştir; ya kaybolmamıştır, ama ulaşılamaz durumdadır veya kaybolmamıştır ve ulaşılabilir durumdadır, ama yetkili kullanıcılar tarafından kullanılamaz durumdadır (örn: donanımın kırılması).
- **Değişiklik Yapma:** Bu saldırı türü, bilginin yetkili kullanıcıya ulaşmadan önce saldırganın amaçları doğrultusunda bilgide değişiklik yapmasını içerir. Program kodları, durgun veri veya aktarılmakta olan veri üzerinde yapılması mümkündür (örn: virüsler).
- **Üretim:** Bu saldırı türü, gerçekte olmaması gereken verinin üretilmesini içerir. Üretilen veri, daha önceki gerçek bir verinin taklidi olabileceği gibi, gerçeğe uygun tamamen yeni bir veri şeklinde olabilir (örn: sahte veri, ya da veri taklidi).

Bunların yanı sıra saldırıları aktif ve pasif olmak üzere de gruplandırılabilir. İzinsiz erişim türündeki saldırılar pasif grupta, diğer saldırılar aktif saldırı grubunda yer alır.

3.2 Güvenlik Açıkları

Sistem kullanıcıları ve yöneticileri için değerli olan ve saldırganlar için hedef anlamına gelen yazılım, donanım ve verinin, yukarıda açıklanan saldırı türlerinden hangilerine maruz kalabileceği aşağıdaki şekilde görülebilir[8]:



Şekil 3.3. Saldırı Türleri

Şekil 3.3'de görüldüğü gibi engelleme ve izinsiz erişim her üç sisteme de, değişiklik yapma sadece yazılım ve veriye, üretim ise sadece veriye yönelik bir saldırıdır. Değişiklik yapma ilk bakışta donanıma da yöneltilebilecek bir saldırı gibi görünse de, buradaki değişiklikten kasıt, fiziksel bir parçanın değiştirilmesi değil, daha çok çalışmanın veya içeriğin beklenenden ayırt edilebilen veya edilemeyen şeklin farklı olmasıdır.

Donanımın maruz kalabileceği iki saldırı türü bulunur: Zarar Verme ve İzinsiz Erişim. Zarar verme nerdeyse her seferinde izinsiz erişim sonucu olur. Ama İzinsiz erişimin olmadığı durumlarda da zarar verme saldırısı olabilir; bu tür saldırıların içeriden, örneğin bizzat donanımdan sorumlu personel tarafından yapılması mümkündür.

Yazılımın maruz kalabileceği saldırılar arasında, *silinme* baş sırayı almaktadır. Silinme de kasıtlı veya kasıtsız olabilir. Kullandığınız işletim sisteminin yönetici yetkilerindeki kullanıcısını (örn: Windows için Administrator, Unix için root kullanıcısı), sadece ihtiyacınız olduğunda kullanmalı, diğer zamanlardaki olağan işlerinizi, normal yetkilerde, yani yetkileri kısıtlandırılmış olan bir kullanıcı ile gerçekleştirilmelisiniz. Özellikle sistem yöneticilerine sıkça yapılan bu hatırlatmanın amaçlarından biri, yanlışlıkla silinen dosyaların en aza indirgenmesi içindir. Yazılıma yönelik bir başka açık, hırsızlıktır. Nispeten daha kolay kopyalanabilmesinden kaynaklanan lisanssız kullanım örnek olarak gösterilebilir. İzinsiz kopyalama da bu anlamda hırsızlığa dâhil edilebilir. Yani mutlaka lisanssız kullanmak gerekmez, örneğin başkalarının lisanssız kullanabilmesine olanak tanımak da yazılıma yönelik bir saldırı olarak düşünülebilir.

Yazılım ve donanımın olduğu kadar, verinin de açıkları, yani zayıf yönleri vardır. Her şeyden önce veri, niteliği gereği, zaman zaman yazılım ve donanımdan çok daha değerli olabilmektedir

3.4 Zararlı Yazılımlar

Geçmişte bir bilgisayarı zor durumda bırakabilecek tek yöntem zararlı taşıyan disketleri bilgisayara yerleştirmekti. Yeni teknoloji çağının başlamasıyla, artık, neredeyse her bilgisayar dünyanın geri kalanına bağlanmış durumda. Dolayısıyla zararlı bulaşmalarının kaynak yerlerini ve zamanlarını kesin olarak tespit etmek gün geçtikçe zorlaşıyor. Bunlar yetmezmiş gibi yeni bilgisayar çağında yeni tür zararlı yazılımlar türemiş durumda. Günümüzde virüs terimi bir bilgisayarın zararlı yazılımlarca saldırıya maruz bırakacak tüm değişik yöntemleri belirtmekte kullanılan genel bir terim halini almıştır. Yukarıda açıkladığımız virüs tiplerinin dışında günümüzde yenice karşılaştığımız problemler bulunmaktadır[9].

3.4.1 Truva atları

Truva atları ilgi çekici görünen ama aslında aldatmaya yönelik zararlı dosyalardır. Sistemde var olan dosyalara kod eklemektense ekran koruyucu yüklemek, e-maillerde resim göstermek gibi bir işle iştigal oldukları izlenimi uyandırırlar. Ancak, aslında arka planda dosya silmek gibi zararlı etkinlikler gerçekleştirmektedirler. Truva atları bilgisayar korsanlarının bilgisayarınızdaki kişisel ve gizli bilgilerinize ulaşmalarına imkân tanıyan gizli kapılar da yaratırlar. Truva atları aslında sanılanın aksine virüs değillerdir çünkü kendilerini çoğaltamazlar. Bir Truva atının yayılması için saklı bulunduğu e-mail eklentisinin açılması ya da Truva atını içerir dosyanın internet üzerinden bilgisayara indirilip yürütülmesi gerekir.

3.4.2 Spam

Internet üzerinde aynı mesajın yüksek sayıdaki kopyasının, bu tip bir mesajı alma talebinde bulunmamış kişilere, zorlayıcı nitelikte gönderilmesi spam olarak adlandırılır. Spam çoğunlukla ticari reklâm niteliğinde olup, bu reklâmlar sıklıkla güvenilmeyen ürünlerin, çabuk zengin olma kampanyalarının, yarı yasal servislerin duyurulması amacına yöneliktir. Spam gönderici açısından çok küçük bir harcama ile gerçekleştirilebilirken mali yük büyük ölçüde mesajın alıcıları veya taşıyıcı, servis sağlayıcı kurumlar tarafından karşılanmak zorunda kalınır[10,11].

- **Peki spam denilen bu böceklerden nasıl kurtulabiliriz? Ya da kurtulabilir miyiz?**

İlk başta forumlardan e-posta adresinizi gizleyerek bu korunmayı gerçekleştirebilirsiniz. Forumlarda dijital imza olarak bazen e-posta adresi yazılıyor. Eğer forumlarda e-posta adresiniz eavaroglu@internet.net şeklindeyse spam gönderenler bunu kolaylıkla listelerine kaydederler. Bu şekilde bir yazım yerine eavaroglu@***internet.net yazılırsa spam kaydedicilerin bu adresi otomatik olarak kaydetmesini engeller.Site üyelikleri için de mutlaka bir ikinci e-posta adresi kullanılmalıdır. Mesela normal yazışmalar, arkadaşlarınızla görüştüğünüz bir hesabınız

olmalıdır. Buna alternatif olarak forumlara, çeşitli sitelere yapacağınız üyelik işlemleri için ise başka bir e-posta hesabı daha açılmalıdır. Üye olunan bütün sitelerde de bu adres kullanılmalıdır. Böylece reklam kokan e-postalar burada birikecek ve gerçek mail adrsinize zararlı içerik gelmeyecektir. Eğer bir POP3 e-posta hesabı kullanıyorsa ve hesabınızı bilgisayar üzerinden Outlook Express gibi bir program ile takip ediyorsa SpamPal isimli program ile spam postalarını temizlenebilir.

3.4.3 Phishing

PHISHING bankanızın, e-postanızın veya bunun gibi bilgi girmenizi gerektiren bir kuruluşun web sayfasının bir kopyasını yapıp kullanıcının hesap bilgilerini çalmayı amaçlayan bir İnternet dolandırıcılığı. İngilizce "Balık tutma" anlamına gelen "Fishing" sözcüğünün 'f' harfinin yerine 'ph' harflerinin konulmasıyla gelen terim, oltayı attığınız zaman en azından bir balık yakalayabileceğiniz düşüncesinden esinlenerek oluşturulmuş ve uygulanıyor[12,13]. Örneğin kullandığınız elektronik posta servisinin giriş ekranının bir kopyası elektronik posta olarak geliyor ve bir şekilde kullanıcı adınızı ve şifrenizi girmenizi istiyor. Dikkatsiz bir şekilde bilgileri verdiğinizde, sayfanın içine gizlenmiş bir kod parçası kullanıcı adınızı ve şifrenizi dolandırıcılara gönderiyor.

3.5 Saldırgan Grupları

Saldırılardan ve saldırganlardan çokça bahsedilmesine rağmen, genelde tam olarak somut örneklerden aynı çoklukta bahsedilmez. Bilgisayarlarımıza girmek isteyen, "kötü adam"ları şu şekilde gruplandırmak mümkün[8]:

- **Amatörler:** Bu grupta yer alan saldırganlar, aslında sıradan bilgisayar kullanıcılarından başkası değildir. Bu tür saldırılarda genelde saldırının oluş şekli sistemdeki bir açıklığı fark edip yararlanma şeklinde olur.
- **Kırıcılar (Cracker):** Bu grupta yer alan saldırganlar çoğunlukla bir lise veya üniversite öğrencisinin merak duygusuna sahiptirler. Çoğunlukla yanlış bir biçimde "hacker" olarak adlandırılan bu grubun doğru isimlendirmesi "cracker" olup, saldırılarını amatörlere göre biraz daha planlı ve programlı yapan kişilerden oluşur[14].
- **Profesyonel suçlular:** Bu gruptaki saldırganlar, yukarıdaki iki grubun aksine, güvenlik kavramlarını ve amaçlarını anlayan ve bozmaya yönelik organize eylemler içinde bulunan kişilerdir. Birden fazla kişilerden oluşan ekipler kurarak güvenliği bozmaya yönelik saldırılar gerçekleştirebilirler.

3.6 Savunma Denetimleri

Güvenliğin amaçlarını açıkladıktan, hedeflere kimler tarafından ne tür saldırıların olabileceğini, saldırganların hedeflerinin zayıf noktalarını inceledikten sonra, artık savunmaya yönelik neler yapılabilir tartışabiliriz[8]. En güçlü savunma yöntemlerinden biri şifrelemedir. Özellikle verinin şifreli biçimde tutulması, veriye olan izinsiz erişimi anlamsız hale getirir. Ayrıca şifreleme, kimlik doğrulama ve kimliğin inkâr edilememesi gibi doğrulama mekanizmalarında da önemli bir yoldur. Şifreleme yalnız başına etkili olmadığı gibi, yanlış veya dikkatsiz kullanım sonucu kendisi bir güvenlik açığı haline gelebilir. Örneğin, açık anahtarlı şifreleme tekniğinde iki anahtar vardır, biri herkese açık, diğeri sadece kişiye özeldir. Bütün açık anahtarlı şifrelemenin güvenliği kişiye özel anahtarın ne denli iyi korunduğuna bağlıdır. İyi korunmayan veya iyi seçilmemiş bir özel anahtar, kolayca bulunup şifreli verinin şifresi çözülebilir. Üstelik şifreli olduğu için iyi korunduğu varsayılan bilgi için aslında olmayan bir güvenlik varmış gibi görünür. Bu yüzden şifreleme kullanırken diğer güvenlik önlemlerini gözden kaçırmamak gerekir.

- Şifreleme

Şifreler, bilgisayarların ve bilgisayar sistemlerinin Güvenliğini sağlamak için kullanılan karakter dizilerinden oluşur. Bilgisayarınızı açarken, kurumsal ağa bağlanırken, web sitelerine erişirken kullandığınız şifrelerin güvenlik açısından önemi tartışılmazdır.

Şifre belirlerken dikkat edilmesi gereken kurallar vardır. Bunlar:

1. En az 7 karakterden oluşmalıdır. Ne kadar uzun olursa o kadar iyi olur.
2. İçinde büyük, küçük harf, semboller ve rakamlar olmalıdır.
3. Altıncı karakterden sonraki kısımda en azından bir sembol bulunmalıdır.
4. En az 4 farklı karakterden oluşmalıdır (Tekrarlama yapılmamalıdır).
5. Rasgele uydurulmuş sayı ve rakamlardan oluşuyormuş gibi görünmelidir.

Savunmaya yönelik diğer bir denetim, yazılım denetimidir. Özellikle birden fazla kullanıcının kullanması düşünülen yazılımlarda, yazılımın iç güvenlik denetiminin beklendiği gibi çalıştığından emin olunmalıdır. Yazılım kimlik doğrulamayı düzgün yapabilmeli ve buna uygun erişim sınırlamalarını eksiksiz yerine getirebilmelidir. Yazılımın bunu yapamadığı durumlarda işletim sistemi bu denetimi devralmalı ve yazılımın yetki sınırını aşmadığını garantileyebilmelidir. Yazılım geliştirme aşamasında yapılan tararım, kodlama, sınama ve yazılımdaki sorun gidermeye yönelik bakım işleri standartlara bağlı olmalı ve buna uygun bir yordam hazırlanmalıdır.

En az yazılım denetimi kadar önemli bir diğer savunma yolu donanımın denetimidir. Bu denetim için bazen çok basit ve masrafsız ama etkili çözümler üretilebilir. Kasaların kilit takılabilen türlerinin seçilmesi ve kilitlerin sürekli kasalar üzerinde tutulması, her şeyden önce kilitsiz bir kasaya göre çok daha caydırıcı bir etki sağlar. Belki kilit kasanın açılamamasını sağlamaz, ama açılan bir kasanın çok daha çabuk fark edilmesini sağlayacaktır, çünkü büyük olasılıkla açılmanın fiziksel izleri daha belirgin olacaktır.

Güvenliği sağlamak için, ilk adım bir güvenlik politikasının oluşturulmasıdır. Fakat güvenlik politikasının ve savunmaya yönelik diğer güvenlik denetimlerinin güvenliği sağlamada etkili olabilmesi için uluslar arası noktayı akıldan çıkarmamak gerekir[8].

Bunlardan ilki ve bütün güvenliğin temeli, sorunun farkında olmaktır. Güvenliği sağlamak bir sorundur ve bu sorunun farkında olmak, çözüme yönelik atılacak ilk adımdır. Sadece kullanıcı veya sistem yönetimi bazında değil, idari yönetim bazında da sorunun farkına varma ve çözüme yönelik eylemler için katkıda bulunma isteği tabanı oluşturulmadan, bilişim teknolojileri unsurlarının güvenliğini sağlamak mümkün değildir.

Güvenlik, örneğin kurulan bir program veya bir defaya mahsus alınması gereken uluslar arası önlemler topluluğu değildir. Herhangi bir sistem için "güvenliği sağlandı, artık yapılması gereken bir şey yok" denemez. Güvenlik, içinde sürekliliği taşır. Güvenliğin kendisi bir süreçtir, üstelik oldukça uzun bir süreçtir. Güvenlik, ne kadar sürekli denetim altında tutulması gereken bir olgu olarak anlaşılırsa, bilişim sistemlerinin güvenliğini korumada oluşturulacak savunma denetimleri de o kadar etkili olur.

Bilişim Teknolojileri, şimdiye tek hızla gelişmiş, şu anda hızla gelişen ve gelecekte de hızla gelişmeye devam edecek gibi görünen konuları içerir. Temel güvenlik kavramlarını anlamak ve benimsemek, bu hıza ayak uydurabilmek açısından son derece önemlidir. Bugün bir ateş duvarı, bir antivirüs yazılımı veya basit şifreleme kullanımı, birçok kişisel bilgisayarın veya sunucunun güvenliğini sağlamada etkili birer denetim olabilir, fakat bu yarın da aynı derecede etkili olacaklarının garantisi değildir.

Bilginin güvenliğini sağlamak ve özellikle hızlı teknoloji ile değişen şartlara uygun araç ve savunma denetimlerini belirleyebilmek için, temel bilgi güvenliği kavramlarının iyi anlaşılması ve yerleştirilmesi, şimdi olduğu kadar, gelecekte de önemini korumaya devam edecek gibi görünmektedir

3.7 Değerlendirme ve Öneriler

Bilgi ülkelerin, kurumların veya kişilerin en değerli en değerli varlılarıdır ve mutlaka korunmalıdır. Bu konuda gerekli önlemlerin alınmaması büyük kayıplara ve zararlara sebebiyet vermektedir. Amerika Birleşik Devletlerinde kurulmuş olan Echelon sistemi ile bilginin 5 farklı ülkede (ABD, Kanada, Türkiye, Avustralya ve İngiltere) bulunan dinleme istasyonları ile dinlenildiği, 3 milyar iletişimin (%90) analiz edildiği bilinmektedir.

Kullanıcıların ve sistem yöneticilerinin bilgilerini daha iyi koruyabilmeleri için alınması vurgulanan gerekli güvenlik önlemleri aşağıda sıralanmıştır.

- Virüs tanımlamalarını güncel tutma
- Parola kullanma kuralını uygulatma
- Virüs bulaşmış bilgisayarların daha fazla kayıp verilmeden temizlenmesi
- E-posta sunucuları .vbs, .bat, .exe, .pif ve .scr dosyaları gibi virüs yaymak için kullanılan ekler içeren e-postaları bloke etmek üzere yapılandırılmaları
- İhtiyaç duyulmayan hizmetlerin kapatılması
- Her seviyedeki personel bilinen kişilerden gelen dosyaları veya internetten indirilen yazımlıları, virüs taraması yapmadan açmamaları veya çalıştırmamaları konusunda eğitilmelidir.
- Kurumları veya şirketleri güvenlik için bütçe ayırma konusunda eğitme
- Yeterli kontrollerin yerinde olmasını sağlamak için güvenliği test etme
- Acil saldırı cevaplama uygulamaları oluşturma gibi hususlardır.

Yukarıda sayılan hususlara dikkat etmek karşılaşılabilecek saldırı ve tehditlere karşı güvenliği yüksek oranda sağlayacaktır. Ama şu da unutulmamalıdır ki %100 güvenlik hiçbir zaman mümkün değildir.

4. BİLGİ GÜVENLİĞİ BİLİMİ

Bilgi güvenliği biliminin amacı saldırganların, korsanların, casusların, iyi niyetli olan veya olmayan kişilerin iletişim sistemlerini dinlemelerini ve elektronik depolama ünitelerine girip mevcut bilgileri elde etme ve onlara ulaşabilme isteklerdir. Verilerin güvenli olarak bir ortamdan diğer ortama gönderilmesinde veya saklanmasında matematiksel yaklaşımlar kullanılmaktadır. Bu kullanılan yaklaşımlar şifreleme bilimi, kriptoloji veya gizli dünyadır.

Kriptoloji kelimesi, köken olarak eski Yunancada yer alan "kryptos logos" kelimelerinden gelmektedir. "Kryptos" kelimesi "gizli dünya" anlamını, "logos" ise sebep-sonuç ilişkisi kurma, mantıksal çözümleme alanı anlamını taşımaktadır. Kriptoloji, kavram olarak şöyle tanımlanabilir[15]: "Kriptoloji, haberleşen iki veya daha fazla tarafın bilgi alışverişini emniyetli olarak yapmasını sağlayan, temeli matematiksel zor problemlere dayanan tekniklerin ve uygulamaların bütünüdür."

Günümüzde kriptoloji, matematik, elektronik, optik, bilgisayar bilimleri gibi birçok disiplini kullanan özelleşmiş bir bilim dalı olarak kabul edilmektedir. Kriptolojinin iki temel alt dalı vardır: Kriptografi ve kriptoanaliz[16].

Kriptografi, belgelerin şifrelenmesi ve şifresinin çözülmesi için kullanılan yöntemlere verilen addır. Kısaca mesajların içeriğini gizleyerek bir şifreleme sisteminin oluşturulmasıdır. Kriptografi, şifreleme ve deşifreleme için kullanılan matematiksel fonksiyonlardan oluşur. Bu olaylar içinde bir anahtar değeri kullanılmaktadır.

Kriptoanaliz, şifreleme anahtarı bilinmeden şifreyi çözme yöntemleriyle uğraşmaktadır. Bu yöntemin başarısı, mesaj ya da anahtarın elde edilmesiyle değerlendirilmektedir[17,18].

Günümüzde elektronik bilgi sistemlerinin yaygınlaşması kriptolojinin önemini çok fazla arttırmıştır. Kriptolojinin başlıca kullanım alanı hareket halindeki veya depolanmış bilginin şifrelenmesi ve istendiğinde bu şifrenin çözülmesidir. Kriptolojinin temel malzemesi bilgi olduğu için neredeyse sınırsız sayıda uygulamada kullanılması söz konusu olmuştur.

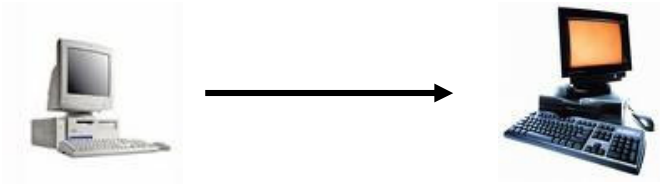
4.1 Haberleşmede Emniyet

Haberleşen iki tarafın güvenlikle ilgili çeşitli beklentileri vardır. Bu beklentiler haberleşmenin emniyet öğeleri olarak sınıflandırılmıştır. Haberleşmede emniyet öğeleri aşağıdaki görülmektedir[19]:

- Gizlilik: Bilginin içeriğinin gizli kalmasıdır
- Bütünlük: Bilginin içeriğinin iletimde değiştirilememesidir
- Kimlik Doğrulama: Bilgiyi gönderen kişinin kimliğinin doğruluğundan emin olmaktır
- İnkâr Edemezlik: Bilgiyi gönderen veya işleyen kişinin yaptığı işi sonradan inkâr edememesidir.
- Haberleşmenin Sürekliliği: Haberleşmenin kesintiye uğramadan yapılmasıdır

4.2 Elektronik Tehditler

Haberleşen iki taraf, bilgisayar ağları, kablolu veya kablosuz iletişim kanalları kullanarak bir bilgiyi, mesajı bir taraftan diğerine iletirler. Elektronik ortamda haberleşen taraflar çeşitli tehditlerle karşı karşıya kalırlar[19].



- Gizlilik İhlali
- Bütünlük İhlali
- Kimlik Doğrulama İhlali
- İnkâr Edemezlik İhlali
- Süreklilik İhlali

Şekil 4.1. Normal Mesaj İletimi

4.3 Elektronik Tedbirler

Elektronik haberleşmedeki tehditlere karşı yine elektronik tedbirler alınarak korunma sağlanabilir. Bu tehditlere karşı alınabilecek tedbirler ve kullanılabilecek yöntem ve araçlar aşağıda görülmektedir.

- Gizlilik sağlamak için veri şifreleme yöntemleri kullanılır
- Bütünlük sağlamak için özetleme algoritmaları, mesaj özetleri, sayısal (elektronik) imzalar kullanılır.
- Kimlik doğrulaması için özetleme algoritmaları, mesaj özetleri, sayısal (elektronik) imzalar, sertifikalar kullanılır.
- İnkâr edemezlik için sayısal (elektronik) imzalar, işlem kayıtları kullanılır
- Süreklilik için yedek sistemler, bakım, yedekleme, alternatif haberleşme kanalları kullanılır

4.4 Elektronik Emniyet Yöntemlerinin Karşılaştırılması

Elektronik tehditlere karşı kullanılan yöntemlerin karşılaştırmasını aşağıdaki tabloda görebilirsiniz[19].

	Kimlik Doğrulama	Gizlilik	Bütünlük	İnkâr Edememe
Anti-virüs			✓	
Güvenlik Duvarları	✓	✓		
Erişim Denetimi	✓	✓		
Şifreleme		✓		
Açık Anahtar Altyapısı	✓	✓	✓	✓

Şekil 4.2. Elektronik Emniyet Yöntemlerinin Karşılaştırılması

4.5 Şifreleme

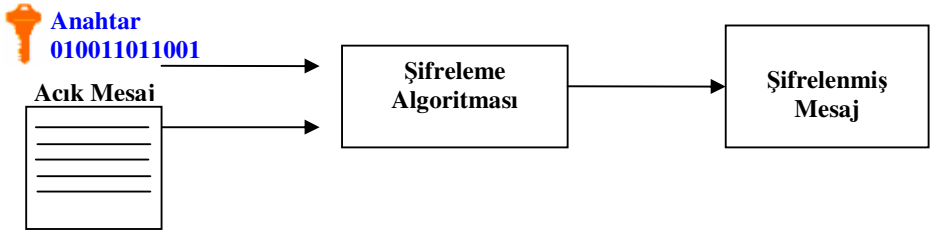
Şifreleme, bir bilginin özel bir yöntemle değiştirilerek farklı bir şekle sokulması olarak tanımlanabilir. Şifreleme işlemi sonucunda ortaya çıkan yeni biçimdeki bilgi, şifre çözme işlemine tabi tutularak ilk haline dönüştürülebilir.

Şifreleme yönteminde aranan bir takım özellikler vardır. Bunlar aşağıda listelenmiştir:

- Şifreleme ve şifre çözme işleminin zorluğu ihtiyaç duyulan güvenlikle doğru orantılı olmalıdır. Çok önemli olmayan bir bilginin şifrelenmesi için bilginin kendisinden daha fazla işgücü ve zaman harcanması verimli olmayacaktır.
- Anahtar seçimi ve şifreleme algoritması özel koşullara bağlı olmamalıdır. Şifreleme yöntemi her türlü bilgi için aynı şekilde çalışmalıdır.
- Sürecin gerçeklenmesi mümkün olduğunca basit olmalıdır. Çok karışık bir sistemin gerçeklenmesi hem hatalara sebep olabilir hem de performans açısından tatmin edici olmayabilir.
- Şifrelemede yapılan hatalar sonraki adımlara yansımamalı ve mesajın tamamını bozmamalıdır. Saldırılara karşı bu özellik koruyucu olacaktır. Ayrıca haberleşme hattında meydana gelen bir hata bütün mesajın bozulmasına neden olmayacağı için bu özellik tercih edilmektedir.
- Kullanılan algoritmanın karıştırma özelliği olmalıdır. Mesajın şifrelenmiş hali ile açık hali arasında ilişki kurulması çok zor olmalıdır.

4.5.1 Güvenli şifreleme yöntemleri

Güvenli şifreleme yöntemleri klasik şifreleme yöntemlerinin zayıf yönlerini ortadan kaldıran ve kriptoanalize karşı dirençli olan algoritmalarla gerçeklenir. Bu yöntemler elektronik sistemlerde (bilgisayar, telekomünikasyon vb) kullanılır ve ikili düzende (binary) saklanan ve taşınan bilgi üzerinde uygulanır. Bu nedenle anahtar olarak bit dizileri kullanılır[19].



Şekil 4.3. Güvenli Şifreleme Yöntemi

Bir şifreleme algoritmasının güvenliği belirleyen en önemli değişkenlerden birisi anahtar uzunluğudur. Örneğin 64 bitlik bir anahtar kullanan şifreleme algoritması için toplam anahtar sayısı 2^{64}= 1019 adettir. Şifrelemede bu anahtarlardan herhangi birisi kullanılabileceği için bu anahtarı tahmin yoluyla elde etme olasılığı çok düşüktür.

64 bitlik Anahtar = 1100101010110001 0001101000000111 0110100010011110 1100111010011011

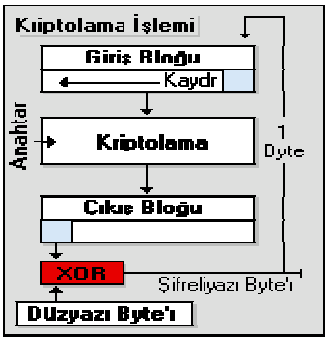
Güvenli şifreleme temel olarak iki çeşittir:

- Simetrik Kriptografi
- Asimetrik Kriptografi

4.5.1.1 Simetrik kriptografi

Simetrik Kriptografi, şifrelemede ve şifreyi çözmede aynı kriptolama anahtarını kullanır. Simetrik Kriptografi aynı zamanda Özel Anahtar Kriptografi olarak da bilinir. Asimetrik Kriptografi ya da açık anahtar Kriptografi sistemi ise kriptolama ve dekriptolama için bir çift anahtar kullanır. Bir anahtar (açık anahtar) mesajı kriptolamak için kullanılır ve diğer anahtar (özel anahtar) dekriptolamak için kullanılır. Simetrik Kriptografi bilgiyi kriptolamak ve dekriptolamak için tek bir anahtar kullandığından mesajı sadece kriptolama da kullanılan anahtarı kullanarak açabilirler. Simetrik kriptografinin blok (block) ve akış (stream) şifreleme olarak bilinen iki tip kriptolama algoritması vardır. Bir blok şifreleme bilgiyi bloklar halinde işler. Bir akış şifreleme bilgiyi bit`lere veya bazı durumlarda byte`lara göre işler. Blok şifreleme şifrelenecek bir blok bilgiyi alır (genelde 64 bit), ve tek anahtarı ile seçilmiş

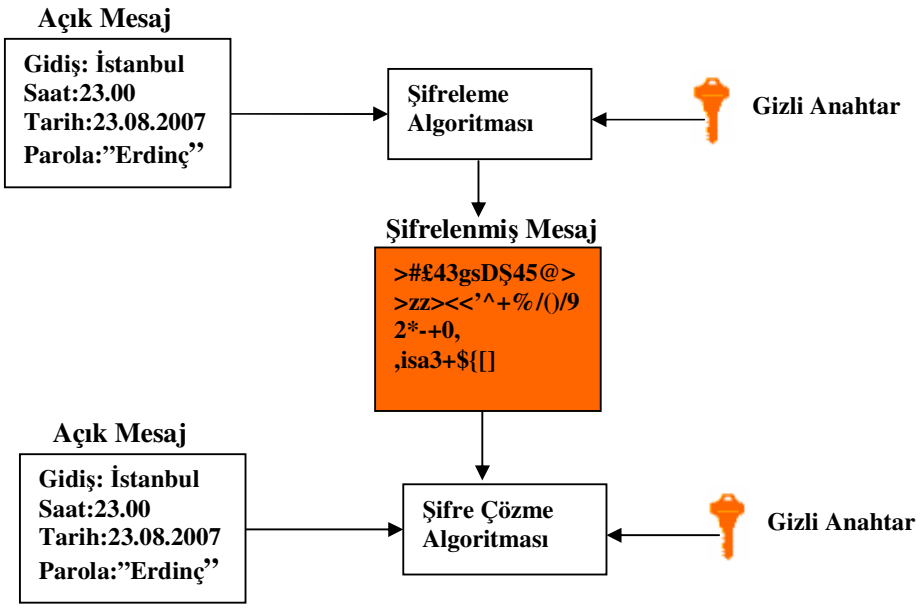
fonksiyonu kullanarak onu aynı boyuttaki başka bir bloğa dönüştürür. Akış şifreleme farklı uzunluklardaki girişlerle çalışabilir. Yani algoritma, işlenmeden önce belirli boyuttaki bir bilginin girilmesini beklemez[20].



Şekil 4.4. Simetrik Kriptolama

Bu sistemde haberleşen taraflar:

- Aynı şifreleme algoritmasını kullanırlar
- Birbirine uyumlu gerçeklemeler kullanırlar
- Aynı anahtarı kullanırlar



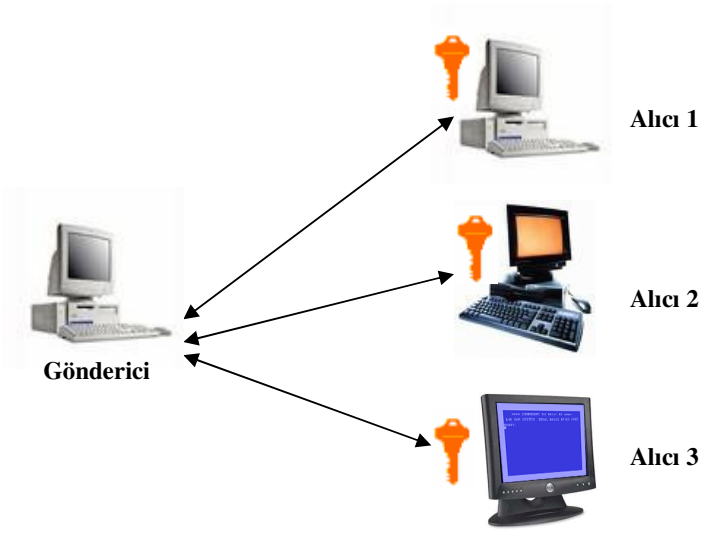
Sekil 4.5. Gizli Anahtarlı Şifreleme

Simetrik kriptografinin en önemli öğesi anahtar gizliliği olduğu için birden fazla kişinin haberleştiği bir ortamda anahtar yönetimi büyük dikkat gerektirmektedir.

4.5.1.1.1 Simetrik kriptografi anahtar yönetimi

- Birden çoğa (One-to-Many) anahtar yönetimi

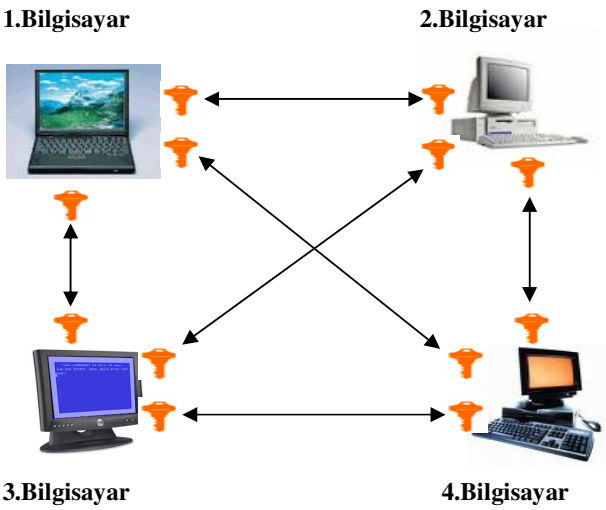
Bu yöntemde iletişim kuran tüm kişiler aynı gizli anahtarı kullanırlar. Bundan dolayı da bütün taraflar birbirinin şifreli mesajlarını açıp okuyabilir.



Şekil 4.6. Birden-Çoğa (One-to-Many) Anahtar Yönetimi

- Çoktan çoğa (Many-to-Many) anahtar yönetimi

Bu yöntemde iletişim kuran tüm kişiler kendi aralarında bir gizli anahtar kullanmak üzere haberleşirler. Bundan dolayı herkes şifreli haberleşeceği her kişi için bir anahtar tutar.



Şekil 4.7. Çoktan-Çoğa (Many-to-Many) Anahtar Yönetimi

Bu yöntem sistemdeki kişi sayısına bağlı olarak çok fazla anahtar üretimini gerektirdiği için çok kullanışlı değildir. Anahtar sayısının kullanıcı sayısına bağlı olarak artışı aşağıda görülebilir.

Kullanıcı Sayısı	Anahtar Sayısı
3	3
4	6
10	45
100	4,950
1,000	499,500
10,000	49,995,000
n	n*(n-1) /2

Tablo 4.1. Anahtar Sayısının Kullanıcı Sayısına Bağlı Artışı (Simetrik kriptografi)

4.5.1.1.2 Simetrik kriptografi artılar eksiler

Simetrik kriptografinin kuvvetli yönleri aşağıdaki gibi özetlenebilir:

- Algoritmalar hızlıdır
- Algoritmaların donanımla gerçeklenmesi kolaydır
- "Gizlilik" güvenlik hizmetini yerine getirir

Simetrik kriptografinin zayıf yönleri aşağıdaki gibidir:

- Ölçeklenebilir değil
- Emniyetli anahtar dağıtımı zor
- "Bütünlük" ve "Kimlik Doğrulama" güvenlik hizmetlerini gerçeklemek zor

4.5.1.1.3 Simetrik kriptografi algoritmaları

Simetrik Kriptografinin başlıca algoritmaları aşağıda verilmiştir[19]:

- DES (Data Encryption Standard) algoritması

Bankacılık ve finans sektöründe ağırlıklı olarak kullanılan bu algoritma IBM firması tarafından 1974 yılında bulunmuş ve 1977 yılında Amerikan Standardı olarak kabul edilmiştir [21,22]. Üzerinde en çok çalışılmış olan algoritmadır. Günümüzde bu algoritma 3DES (triple DES) şeklinde, üç farklı anahtarla aynı bloğa 3 defa DES uygulanarak da kullanılmaktadır. Algoritmanın kullanılması için herhangi bir lisans ödenmesi gerekmemektedir.

DES algoritması bir Block Cipher algoritmasıdır. Yani şifrelenecek metin bloklar halinde şifreleme işleminden geçirilir. Ayrıca DES algoritması simetrik şifreleme prensibine dayanmaktadır. Yani DES, veri bloklarını şifrelemek ve deşifrelemek için aynı anahtarları kullanmaktadır. DES 64 Bitlik düz metin blokları üzerinde işlem yapmaktadır. 64 bitlik veri blokları, 56 bitlik bir anahtarın kontrolünde şifrelenerek yine 64 bitlik şifrelenmiş metin bloklarına dönüştürülür. Deşifrelenirken de 64 bitlik şifrelenmiş veri blokları, 56 bitlik bir anahtarın kontrolünde deşifrelenerek yine 64 bitlik deşifrelenmiş metinlere (düz metne) dönüştürülür[23].Fakat DES kırılmış durumdadır[24].

- AES (Advanced Encryption Standard) algoritması

AES (Advanced Encryption Standard; Gelişmiş Şifreleme Standardı), uluslar arası olarak kullanılan bir şifreleme(kripto) sistemidir[25]. Belçikalı Vincent Rijmen ve Joan Daemen tarafından geliştirilmiş, DES'in ve diğer olası algoritmaların zayıf olan yönlerini tamamen temizleyerek, matematikle oluşturulmuş algoritmadır. Bruce Schneier'in RSA'sını, twofish'ini[26] ve rc6'sini eleyerek 1997'de nist'in yarışmasını kazanmış ve yeni şifreleme standardı olmuştur[27].

- AES algoritması 128 bit veri bloklarını 128, 192, 256 bit anahtar seçenekleri ile şifreleyen bir algoritmadır.
- 128 bit anahtar için 10 döngüde şifreleme yaparken 192 ve 256 bit anahtarlar için sırasıyla 12 ve 14 döngüde şifreleme yapmaktadır.
- AES algoritmasında her döngü dört katmandan oluşur.
- İlk olarak 128 bit veri 4×4 byte matrisine dönüştürülür.
- Daha sonra her döngüde sırasıyla byte'ların yer değiştirmesi, satırların ötelenmesi, sütunların karıştırılması ve anahtar planlamadan gelen o döngü için belirlenen anahtar ile XOR' lama işlemleri yapılır

- Skipjack

Skipjack 64-bitlik blok, 80-bitlik anahtar ve 32 dahili tur kullanan diğer bir blok şifreleme metodudur. DES`in aksine Skipjack gizlidir ve herkesin kullanımına açık değildir. Skipjack sadece 'Clipper' çipi yada Fortezza token gibi onaylanmış donanımlarla uygulanabilir. Fortezza token hükümet kullanımı için yaratılmış bir token'dır[28].

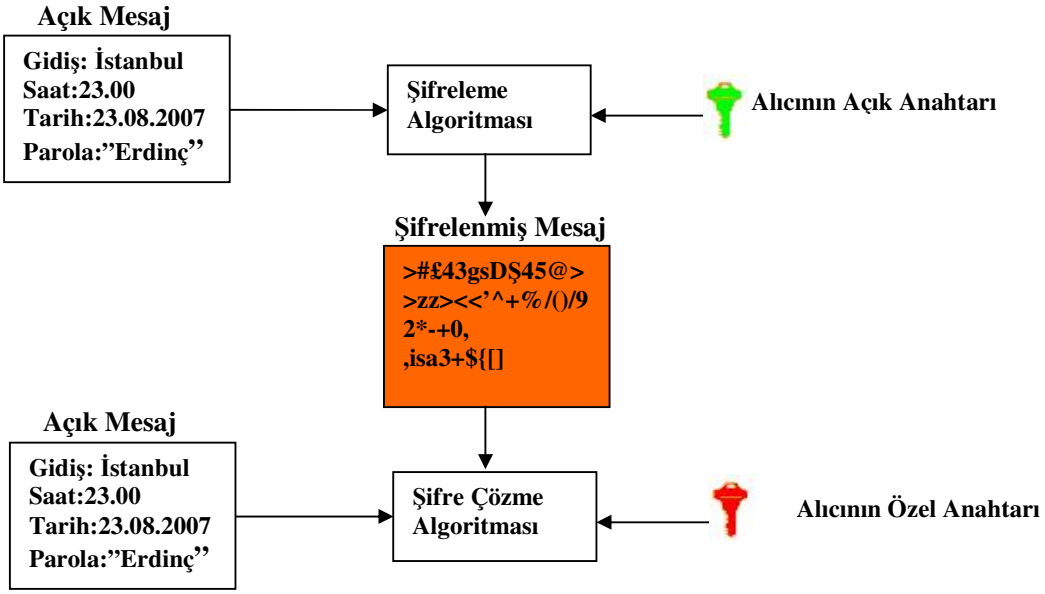
4.5.1.2 Asimetrik kriptografi

Asimetrik kriptografide, şifreleme ve şifre çözme işlemi farklı anahtarlar ile yapılır[29]. Bu anahtar çiftini oluşturan anahtarlara açık ve özel anahtar adı verilir. Bu kriptografi yönteminde özel anahtar gizli tutulmalıdır fakat açık anahtar gerekli kişilere verilebilir ve başka

kişilerle paylaşılabilir. Bu özelliğinden dolayı asimetrik kriptografi, açık anahtarlı şifreleme adıyla da anılır.

Bu sistemi kullanarak haberleşen taraflar:

- Aynı şifreleme algoritmasını kullanırlar
- Birbiriyle uyumlu gerçeklemeler kullanırlar
- Gerekli anahtarlara erişebilirler



Şekil 4.8. Asimetrik Kriptografi

4.5.1.2.1 Asimetrik kriptografi anahtar yönetimi

Asimetrik kriptografi için anahtar yönetimi çok önemlidir. Anahtar yönetimi için dikkat edilmesi gereken noktalar şöyle sıralanabilir[19]:

Açık anahtarlar kontrollü olarak bir otorite tarafından yayınlanmalı ve değiştirilmeleri önlenmelidir. Anahtar çiftleri merkezi bir otorite tarafından üretilebilir veya her kullanıcı kendi anahtar çiftini üretebilir. Şifreleme ve imzalama için ayrı ayrı anahtar çiftleri olmalıdır. Çok özel durumlar için imzalama ve şifreleme anahtar çiftlerinin aynı olmasına izin verilebilir. Anahtar iptalleri kontrollü bir şekilde yapılmalı ve duyurulmalıdır. Asimetrik kriptografi için anahtar yönetimi simetrik kriptografiye göre daha kolaydır çünkü bir kullanıcıyla şifreli haberleşmek isteyen kişi karşı tarafın açık anahtarına ihtiyaç duyar. Bu açık anahtar kamuya açık olarak yayınlandığı için sisteme giren bir kişi için sadece bir anahtar çifti üretmek yeterli olmaktadır.

Kullanıcı Sayısı	Anahtar Çifti Sayısı
3	3
10	10
100	100
1,000	1,000
10,000	10,000
n	n

Tablo 4.2. Anahtar Sayısının Kullanıcı Sayısına Bağlı Artışı(Asimetrik Kriptografi)

4.5.1.2.2 Asimetrik kriptografi artıları eksileri

Asimetrik kriptografinin kuvvetli tarafları aşağıdaki gibi özetlenebilir:

- Anahtar yönetimi ölçeklenebilir
- Kripto-analize karşı dirençli (Kırılması zor)
- Bütünlük, kimlik doğrulama ve inkâr edemezlik güvenlik hizmetleri sağlanabilir.

Asimetrik kriptografinin zayıf yönleri ise aşağıdaki gibidir:

- Algoritmalar genel olarak yavaş çalışırlar. Simetrik kriptografi algoritmalarına göre yaklaşık 1500 kat daha yavaştırlar.
- Anahtar uzunluğu bazı durumlar için kullanışlı değildir. Mobil cihazlar için klasik algoritma anahtar uzunlukları sorunlu olabilir.

4.5.1.2.3 Asimetrik kriptografi algoritmaları

Başlıca asimetrik kriptografi algoritmaları RSA, Eliptik Eğri Sistemleri, El Gamal ve Diffie-Hellman anahtar belirleme olarak sıralanabilir. Asimetrik kriptografi algoritmaları, simetrik algoritmalardan farklı olarak çözülmesi zor olan matematiksel problemlere dayanır.

- RSA algoritması

En yaygın olarak kullanılan asimetrik algoritmadır. R. Rivest, A. Shamir, L. Adleman tarafından 1977 yılında bulunmuş ve 1978 yılında yayınlanmıştır. Adını mucitlerinin isimlerinin ilk harflerinden almıştır[30]. Aşağıdaki özelliklere sahiptir[31,32].

- Açık anahtar kriptografik sistemi ve sayısal imzalama yöntemi olarak kullanılır.
- Çarpanlarına ayırma problemi üzerine inşa edilmiştir.
- Bileşik tam sayı olan n'i oluşturan, asal sayılar p ve q bulunur, öyleki n=pq 'dir.

- Yeterince büyük bir n için kırılması çok zordur.
- Ayrıca kök bulma problemine de dayanır.
- Çok güvenlidir fakat fazla hızlı değildir.

- Elektronik imza

Sayısal imza veya kanunlara geçen adıyla elektronik imza kriptografik bir dönüşüm olarak tanımlanabilir. Elektronik imza, mesajın içeriği ile mesajı imzalayan kişinin asimetrik özel anahtarının beraber kullanılması ile elde edilir. Sayısal (elektronik) imza aşağıdaki özelliklere sahiptir:

- Mesajın sonuna eklenir
- Mesaj alıcısının, mesajın göndericisinin kimliğini doğrulamasını ve mesajın bütünlüğünü kontrolünü sağlar.
- İnkâr edemezlik hizmetini sağlar.
- Asimetrik kriptografi kullanır.

Sayısal imzanın bu şekilde kullanılması bir problemi beraberinde getirir. Bu kullanım şeklinde sayısal imza mesaj uzunluğunu iki katına çıkarır. Bu sorunu çözmek için özetleme fonksiyonu kullanılarak bir "Mesaj Özeti" çıkarılır.

- Özetleme (Hash) algoritmaları

Herhangi bir uzunluktaki veriyi alıp işleyen ve bu veriye özgü olan, sabit uzunlukta bir değer çıkaran algoritmalara mesaj özeti algoritması denir. Bu algoritmaların çıktısı olan değer, mesaj özetidir. En çok bilinen özet algoritmaları MD5 ve SHA ailesidir.

MD serisi özetleme algoritmaları, Ron Rivest tarafından geliştirilmiştir. 128 bit özetleme sağlamaktadır. Bu seride MD2 en yavaşı, MD4 en hızlı olanıdır. MD5, MD4'e göre daha kapsamlı geliştirildiğinden hızı daha düşüktür. MD5 güvenilir olarak kabul edilmiş olmasına rağmen yapılan son araştırmalar MD5'inde kırılabileceğini göstermiş ve MD5'e duyulan güvende kaybolmuştur[33].

Diğer özetleme algoritmalarından biri olan **SHA–1** (Güvenli Özetleme Algoritması-Secure Hahshing Algorithm) NSA (Ulusal Güvenlik Ajansı-National Security Agency) tarafından geliştirilmiştir. SHA–1 MD algoritmalarına göre daha uzun bit üretebilmektedir. 160 bit uzunluğunda üretilen bir dizi için gerekli süre MD5 algoritmasından %25 daha yavaş olsa da bu algoritmanın kullanılması tavsiye edilmektedir. İlk sürüm SHA–0 olarak adlandırılmıştır. SHA-0 ve SHA-1 en fazla 2^{64} uzunlukta mesajlardan 160 bitlik özet değeri üretir. Daha sonra

SHA'nın 256, 384 ve 512 bit versiyonları çıkarılmıştır[34]. Bruce Schneier bloğunda Şandung Üniversitesinden bir grup araştırmacının SHA–1 algoritmasını kırdığını belirtti[35]. SHA–0 ve SHA-1'e yönelik daha önceki kırma girişimlerinden üretilen yeni metot büyük bir kripto-analitik sonuç olarak belirtilmiştir. En son güncel versiyonu ise SHA–2 (sha–224, sha–256, sha–384, sha–512 algoritmalarına verilen genel isimdir. Bunlarda henüz bir zayıflık bulunamamıştır)olarak kullanılmaya başlanmıştır.

RIPE-MD–160 (Race İntegrity Primitives Evaluation Message Digest) algoritması da [36], Avrupa Birliğinde kullanılan bir algoritmadır. Farklı uzunluktaki dosya ve veriler için 160 bitlik sabit uzunlukta bir bit dizisi üretmesi ve diğer şifreleme yaklaşımlarından daha hızlı olması avantajlı yanıdır. Dezavantajı ise sadece bütünlüğü sağlamasıdır. Bu algoritmanın gelecek yıllarda güvenilir olacağı düşünülse de, bazı ataklara karşı zayıf olduğu yönünde çalışmalarla belirtilmiştir.

MAC(Mesaj Onaylama Algoritması-Message Authentication Codes) ise diğer bir algoritma yöntemidir. Bu algoritmada diğer algoritmaların aksine bir MAC oluşturma ve doğrulama için tek bir anahtar kullanılmaktadır.

Tablo 4.3'de özetleme algoritmaları için karşılaştırma yapılmıştır. Verilen örnekte bir karakterin bile değişmesinin özetleme algoritmalarının özetleme sonuçlarının değiştiği görülmektedir.

Algoritma	**Algoritma Çıktısı**
MD4	4512E154E25S0UQ1EA33C4C687178G98
MD5	65789DF8N0F8B2604578HG996B214N5
SHA-1	B145698HB4562C5C69U79945HB21LP6547ER8485

a) "Erdinç Avaroğlu" için çıktılar

Algoritma	**Algoritma Çıktısı**
MD4	FEB456KJ87LKMA45842YT8B5LY45Y9
MD5	8F4DPL6589D25AV36947F8FD723LP548
SHA-1	BN215S6G48RT89MSL545SKFJ556UYGE4554DFS5

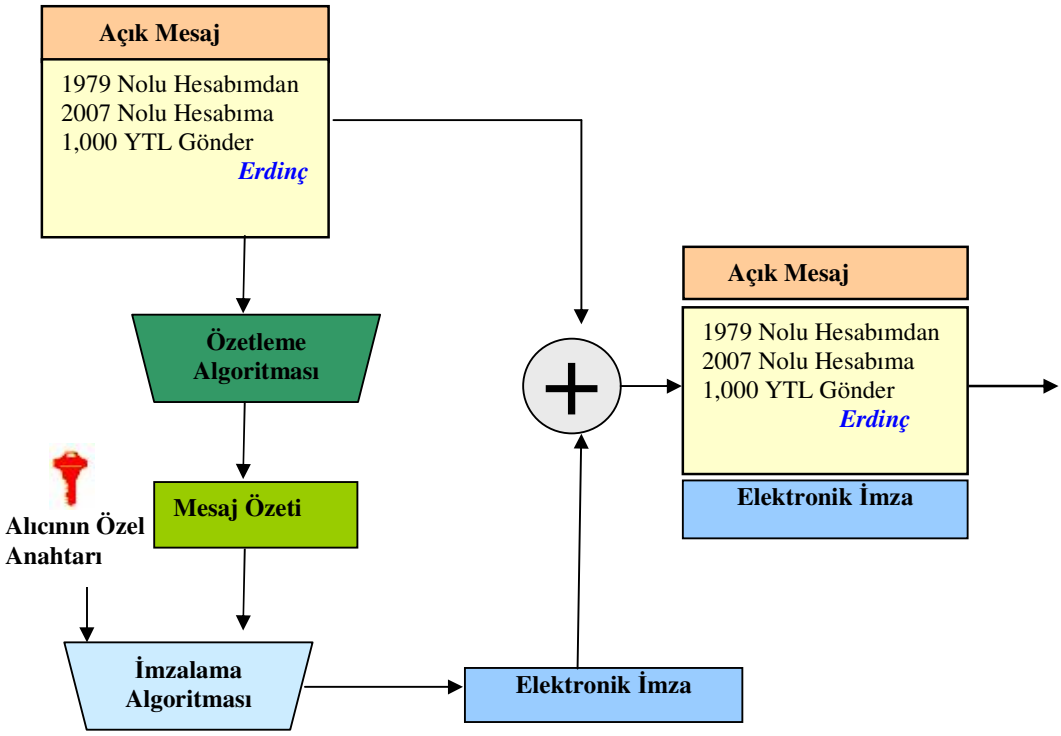
b) "ErDinç Avaroğlu" için çıktılar

Tablo 4.3. Özetleme Algoritmalarını Karşılaştırılması

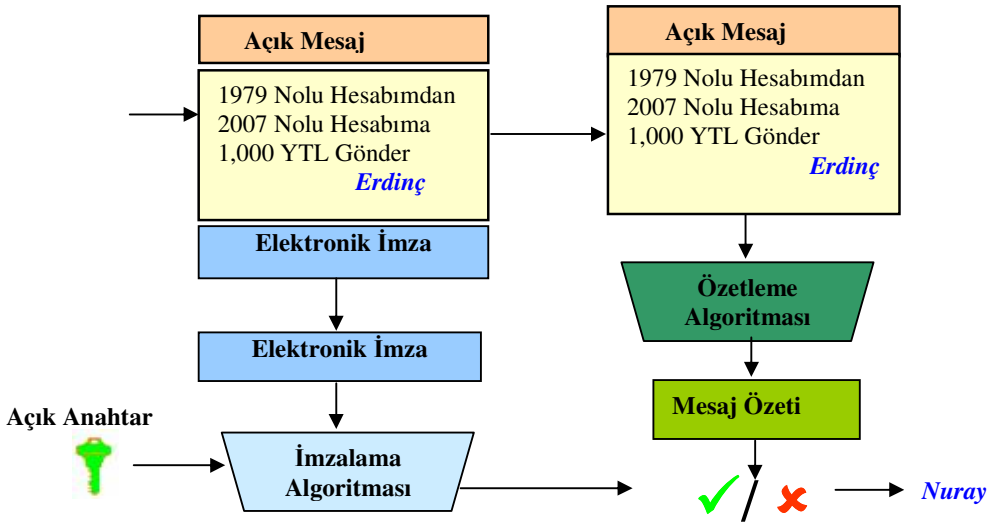
Mesaj özeti elde etmek için kullanılan fonksiyonların özellikleri şunlardır:

- Özet fonksiyonları sabit çıkış uzunluğu üretirler (mesajdan çok kısa). Mesaj hangi uzunlukta olursa olsun MD5 fonksiyonu 128 bit uzunluğunda, SHA-1 fonksiyonu 160 bit uzunluğunda özet değeri üretir.
- Mesajdaki küçük değişiklikler bile özette büyük değişikliklere yol açabilir.
- Özet fonksiyonları kriptografik tek yönlü fonksiyonlardır. Bir mesajın özetini elde etmek çok kolaydır, bir özetten asıl mesajı çıkarmak ise çok zordur.

Mesaj özeti kullanarak sayısal imzalama aşağıdaki gibi yapılır:



Şekil 4.9. Elektronik İmzalı Bir Mesajın Gönderilmesi



Şekil 4.10. Gelen Elektronik İmzalı Bir Mesajın Doğrulanması

4.6 Kripto Sistemlerinin Karşılaştırması

Asimetrik ve simetrik kriptografi sistemlerinin özelliklerini aşağıdaki karşılaştırma tablosunda görebilirsiniz:

Konu	Simetrik Kriptografi	Asimetrik Kriptografi
Gizlilik	Sağlar	Sağlar
Bütünlük	--	Sağlar
Kimlik doğrulama	--	Sağlar
İnkâr Edemezlik	--	Sağlar
Performans	Hızlı	Yavaş
Güvenlik	Anahtar uzunluğuna bağlı	Anahtar uzunluğuna bağlı

Tablo 4.4. Kripto Sistemlerinin Karşılaştırması

4.7 Güvenlik Protokolleri

4.7.1 PGP

PGP (Pretty Good Privacy)mesaj gönderirken mesajları şifrelemeye yarayan bir programdır. Peki, biri benim mesajlarımı ben gönderirken nasıl görebilir? Bunun birçok bilgisayar kullanıcısı mümkün olmayacağını düşünebilir fakat kullanıcılar hiç farkında olmadan bunu yapmak mümkündür. Sniffing yani koklama yöntemiyle, bir ağ altında çeşitli araçlar kullanılarak kullanıcıların veri alış verişiniz görülebilinir[37]. PGP anahtarlar yardımıyla çalışır,

özel (private) ve genel (public) olmak üzere kullanılan iki anahtar vardır. Genel anahtar herkeste serbest olarak bulunabilinir. Özel anahtar ise sadece göndericide bulunur. Özel anahtarla şifrelenmiş olarak gönderilen mesaj alıcının anahtarı ile çözülebiliyorsa alıcı mesajı okur. Bunlar yapılırken kullanılan şifreleme yöntemleri çok karışık ve çözülmesi neredeyse imkânsız olduğundan mesaj alış verişinde çok büyük güvenlik sağlar[38]. Dijital imza bu gereksinimi karşılamak için geliştirilmiş bir teknolojidir.

4.7.2 SSL/TLS

Secure Socket Layer (SSL) ve Transport Layer Security (TLS) adıyla bilinen protokoller TCP/IP protokollerine güvenlik katmak amacıyla geliştirilmiştir. SSL protokolü aşağıdaki güvenlik ihtiyaçlarını karşılamak için kullanılır:

- Özel kullanıcı verilerinin görülmesinin engellenmesi: ör./ Şifre, Kart Bilgileri, Özel Detaylar
- Sunucu taklidi: ör./ Fiyatlandırma Bilgisi Kaynağı, www.isbank.com.tr sunucusu gibi davranmak
- Özel sayfaların ele geçirilmesi: ör./ Şirket Özel Sayfaları
- Doğrulama amaçlı gönderilen kullanıcı özel bilgilerinin gizliliğini sağlamak

SSL Netscape firmasının geliştirdiği bir standarttır. Bu standart en son Secure Socket Layer (SSL) sürüm 3.1 olarak yayınlanmıştır. Daha sonra IETF (Internet Engineering Task Force- Internet Mühendisliği Görev Gücü)tarafından TSL standardı olarak [RFC2246] yayınlanmıştır. SSL'in eski sürümü (SSL v2) güvenli değildir. TLS aşağıdaki hizmetleri sağlar.

- Kullanıcı ve sunucu arasında uçtan uca güvenlik
- TCP üzerine inşa edilmiştir
- Güvenilir bağlantıya ihtiyacı vardır.
- En önemli Internet şifreleme protokolüdür.
- Haberleşen iki uygulama arasında sağlanan hizmetler
- Kimlik doğrulama
- Bütünlük
- Gizlilik
- Sunucunun kimliğini istemciye ispat eder
- İstemcinin kimliğini sunucuya ispat eder
- Uygulama protokolünden bağımsız çalışır

4.7.3 SSH

SSH (Secure Shell/Güvenli Kabuk) ağ üzerinden başka bilgisayarlara erişim sağlamak, uzak bir bilgisayarda komutlar çalıştırmak ve bir bilgisayardan diğerine dosya transferi amaçlı geliştirilmiş bir protokoldür. Güvensiz kanallar(internet vs) üzerinden güvenli haberleşme olanağı sağlar. Bir iletişimde SSH aşağıda belirtilen temel unsurları sağlar.

- Authentication /Kimlik denetimi
- Encryption /Şifreleme
- İntegrity /Bütünlük

SSH güvenli iletişimin gerektiği her ortamda kullanılabilir. Sadece karşı sisteme bağlanıp komut çalıştırmak ya da dosya aktarımı yapmak için değil, doğasında güvensiz (şifrelenmemiş trafik) olarak çalışan protokoller SSH üzerinden güvenli bir şekilde kullanabilir.

4.7.4 S/MIME (Secure/Multipurpose Internet Mail Extensions)

S/MIME güvenli e-posta alışverişi için kullanılan bir standarttır. Güvenli bir mesaj aşağıdaki güvenlik hizmetlerini sağlamalıdır[39]:

- Temel mesaj koruması

- Veri kaynağının doğrulanması
- Gizlilik
- Bütünlük
- İnkâr Edememe

- Geliştirilmiş mesaj koruması

- İmzalı Alındı Notu: inkâr edememe
- Güvenlik etiketleri
- Güvenli Mesaj Listesi

4.7.5 IPSEC

IPSEC[40] (Internet Protocol Security) standardı IP protokolünün ihtiyaç duyduğu aşağıdaki güvenlik ihtiyaçlarını karşılamak için geliştirilmiştir.

- IP adresini taklit etmek kolay (Kimlik doğrulama sorunu)
- Veri paketlerini değiştirmek kolay (Bütünlük, tekrarlama güvenliği ile beraber)
- Veri trafiğini izlemek kolay (Gizlilik ihlali)

- IPSEC kullanımı

IPSEC aşağıdaki işlemler için kullanılabilir:

- Bilgisayarlar arasındaki tüm haberleşme
- Kripto cihazlarının haberleşmesi
- Bilgisayar ile kripto cihazlarının haberleşmesi
- VPN (Virtual Private Network) haberleşmesi / IP ESP Tünel Mod
- Her IP paketinin tek tek şifrelenmesi
- Çevrimiçi anahtar değişimi

4.7.6 Windows logon, kerberos ve AAA

Kerberos ilk olarak Needham ve Shroeder tarafından 1978'de bulundu ve 1981'de Sytek Secure LocalNet tarafından geliştirilerek ticari ürün olarak gerçeklendi. Kerberos protokolü simetrik anahtarların bir anahtar sunucusu tarafından dağıtılması için kullanılır. Kerberos protokolü "Key Distribution Center"dan "ticket" alınmasıyla başlar, dolayısıyla KDC'ın her zaman ayakta olması gerekir. AAA ve sertifika kullanılması halinde kimlik doğrulama mekanizmasında güvenilir üçüncü taraf SM olacağından "KDC" a gerek kalmaz. Windows 200x, Windows NT Lan Manager'dan farklı olarak kimlik doğrulama mekanizması olarak Kerberos kullanır. Kerboros, AAA ile birlikte de kullanılabilir. Windows Logon işlemi akıllı kart kullanarak yapılabilir. Bu durumda akıllı kartta imzalama anahtarı ve logon için uygun imzalama sertifikası olmalıdır.

4.7.7 Güvenilir zaman damgası

Güvenilir zaman damgası, RFC 3161 dokümanında Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) adıyla tanımlanmıştır. Güvenilir zaman damgası sunucusu bir AAA sisteminde zaman damgası vermeye yetkili sertifikaya sahip olmalıdır. Bu sunucu zaman bilgisini güvenilir bir zaman sunucusundan alır. Güvenilir zaman damgası sunucusu kendisine gelen mesaj özeti ve kendi zaman bilgisiyle bir yapı oluşturur ve bu yapıyı imzalayıp yanıt olarak gönderir.

- Güvenilir zaman damgası sunucusu verdiği yanıtları kendi veritabanında tutabilir.
- Güvenilir zaman damgası sunucusu ilkelere ve bilginin önemine göre verdiği yanıtları çevrimdışı bir yöntemle de yedekleyebilir.
- Güvenilir zaman damgası "Sayısal Noter" gibi uygulamalarda kullanılabilir.

4.8 Değerlendirme ve Öneriler

Bu bölümde kripto sitemler ve imza sistemleri incelenmiştir. Kripto sistemler kullandıkları anahtara göre 2 sınıfa ayrılmaktadırlar. Simetrik kripto sistemlerde şifreleme ve deşifreleme aynı anahtar kullanılarak gerçekleştirilirken asimetrik kripto sistemlerde ise şifreleme için açık ve gizli anahtar olmak üzere 2 anahtar kullanılmaktadır.

Simetrik şifreleme asimetrik şifrelemeye göre daha hızlı ve etkili olduğu için uzun mesajların şifrelenmesinde kullanılmaktadır. Asimetrik şifrelemede ise simetrik şifrelemede kullanılan gizli anahtarın iki taraf arasında güvenli şekilde değiştirilebilmesi için ve e-imzaya temel oluşturması amacıyla kullanılmaktadır.

Hashing (Özet) Algoritmaları ile de herhangi bir uzunluktaki metnin sabit uzunlukta özeti oluşturulur.

E-imza, elektronik ortamda kimlik tespitinin yapılabilmesi için geliştirilmiş bir imzalama tekniğidir.

Genel olarak kullanılan mesaj özeti algoritmalarından md5 özelliklede SHA-1 algoritmalarının kırılması ile özetleme fonksiyonları tekrar önem kazanmıştır. Artık bu algoritmalarının kullanılmaması yerine SHA-2 algoritmasının kullanılması gerekmektedir (SHA-2'ninde 10 yıl içerisinde kırılacağı düşünülmektedir.). Şifreleme tekniği olarak da daha güvenli ve e-imza temelini oluşturan asimetrik algoritmalar kullanılmadır. Ancak ne kullanılırsa kullanılsın teknolojinin bu hızla gelişmesi göz önüne alınırsa şifreleme yöntemlerinin her 10 yılda bir daha güçlü hale getirilmesi gerektiği aşikârdır.

5. ELEKTRONİK İMZA

İmza, bir yazının kimin tarafından yazıldığını veya içeriğinin tasdik edildiğini belli etmek amacıyla metnin altına konulan isim veya işarettir. İmza, bir yandan kişinin hüviyetini, diğer yandan da beyanda bulunma iradesini tespit eder. Böylece imzalayanın metni okuyup anladığı ya da belgeyi bizzat hazırlayan kişi olduğu ve bağlanma iradesinin varlığı anlaşılır. İmza, genel olarak, bir belgenin doğruluğunu gösterme niyetiyle yapılan her türlü işaret olarak tanımlanabilir. İmza çok eski çağlardan beri değişik şekillerde kullanılmıştır. Örneğin Roma Hukukunda, bir sözleşmenin oluşturulabilmesi için, sözleşme yapan kişilerin mühür yüzüklerini balmumuna basarak metni mühürlemeleri gerekiyordu. Orta çağ boyunca Avrupa'da, belgeler, topraktan yapılmış mühürlerle mühürlenerek doğrulukları/güvenilirlikleri ispat edilmiştir. Daha sonraları, taraflar, el yazısı ile atılmış imzaları, sözleşmenin geçerliliğini ispat vasıtası olarak kullanmaya başlamışlardır[41–47].

Elektronik imza bir üst kavramdır. Her türlü elektronik ses, karakter, sembol veya uygulamayı kapsayan ve kullanılan teknolojiden bağımsız bir terim olduğundan bir üst kavram olarak kabul edilebilir[48,49]. Ancak sayısal imza kavramı yerine kullanımına rastlamak da mümkündür[50]. Genel olarak elektronik imza kavramı, çok genel bir tanım olup; kişilerin elle atmış olduğu imzaların tarayıcıdan geçirilmiş hali olan sayısallaştırılmış imzaları, kişilerin göz retinası, parmak izi ya da ses gibi biyolojik özelliklerinin kaydedilerek kullanıldığı biyometrik yöntemleri içeren elektronik imzaları veya bilginin bütünlüğünü ve tarafların kimliklerinin doğruluğunu sağlayan sayısal imzaları da içermektedir[45,51,52].

Başka bir tanıma göre elektronik imza, ıslak imzanın fonksiyonlarını da kapsayan ve bir veri mesajında bulunan veya ona eklenen ya da mesaj ile mantıksal bağlantısı kurulabilen, bireyin kimliğini tanıtan ve bireyin, mesajın içeriğini onayladığını gösteren elektronik formattaki imzadır[42,43,51,53,54].

5070 sayılı Elektronik İmza Kanunu'nda yer alan şekliyle elektronik imza; başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veriyi tanımlar. Elektronik imza; bir bilginin üçüncü tarafların erişimine kapalı bir ortamda, bütünlüğü bozulmadan (bilgiyi ileten tarafın oluşturduğu orijinal haliyle) ve tarafların kimlikleri doğrulanarak iletildiğini elektronik veya benzeri araçlarla garanti eden harf, karakter veya sembollerden oluşur[55].

13 Aralık 1999 tarihli Avrupa Birliği Direktifinde[56] elektronik imza, doğrulama yöntemi olarak hizmet veren ve başka bir elektronik veriye eklenmiş veya mantıksal olarak ilişkilendirilmiş elektronik biçimindeki veri olarak tanımlanmıştır.

Elektronik imza ile sayısal imza aynı şey değildir. Sayısal imzanın işlevi, elektronik ortamda aslından ayrılması güç olan sahte imzayı önlemek ve orijinal dokümanların olduğu şekilde, herhangi bir tahrip ve tahrife uğramaksızın iletilmesini sağlamaktır[57]. Bu nedenle sayısal imza, elektronik ortamın vazgeçilmez unsurlarından birisidir denilebilir.

E-imzada, sertifika sahibinin adı, e-posta adresi, çalıştığı kurum adı, telefon numarası, seri numarası, gizlilik derecesi, üretim tarihi, geçerlilik periyodu yer alır. Ayrıca e-imza kanunların resmi şekle veya özel bir merasime gerek duyduğu hukuki işlemler olan, noterlik işlemleri, tapu işlemleri, evlenme merasimleri, veraset ve intikal ile teminat sözleşmelerinde uygulanamayacaktır[49].

5.1 Elektronik İmza Çeşitleri

5.1.1 Gelişmiş elektronik imza

Gelişmiş elektronik imza, genel olarak elektronik imza tanımından yola çıkılarak, bu tanıma çeşitli unsurların eklenmesi suretiyle tanımlanmaktadır. Gelişmiş elektronik imza, verinin bütünlüğünün korunduğunu göstermesi yanında, imzalayanın kimliğinin tespitini de sağlar. Avrupa Birliği Direktifine göre gelişmiş elektronik imza, sadece imzalayana bağlı olan; imzalayanın kimliğini belirlemeye imkân veren; sadece imzalayanın kontrolü altında tutabileceği araçlarla oluşturulan ve verilerde sonradan yapılacak değişikliklerin bilinmesini sağlayan elektronik imza olarak tanımlanmıştır. Buna karşılık, Türk hukukunda gelişmiş elektronik imza tanımına yer verilmemiştir. Ancak gelişmiş elektronik imzanın unsurları, güvenli elektronik imza tanımındaki unsurlarda yer almaktadır.

5.1.2 Güvenli elektronik imza

Gelişmiş elektronik imzanın unsurlarını taşıyan bir elektronik imzanın, nitelikli elektronik sertifikaya dayanması ve güvenli imza oluşturma araçları ile oluşturulmuş olmasıdır. Türk hukukunda, "güvenli elektronik imza" kavramı tercih edilmiştir. Buna göre güvenli elektronik imzada bulunması gereken özellikler şunlardır:

- Münhasıran imza sahibine bağlı olmalı,
- Sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulmuş olmalı,
- Nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlamalı,
- İmzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlamalıdır.

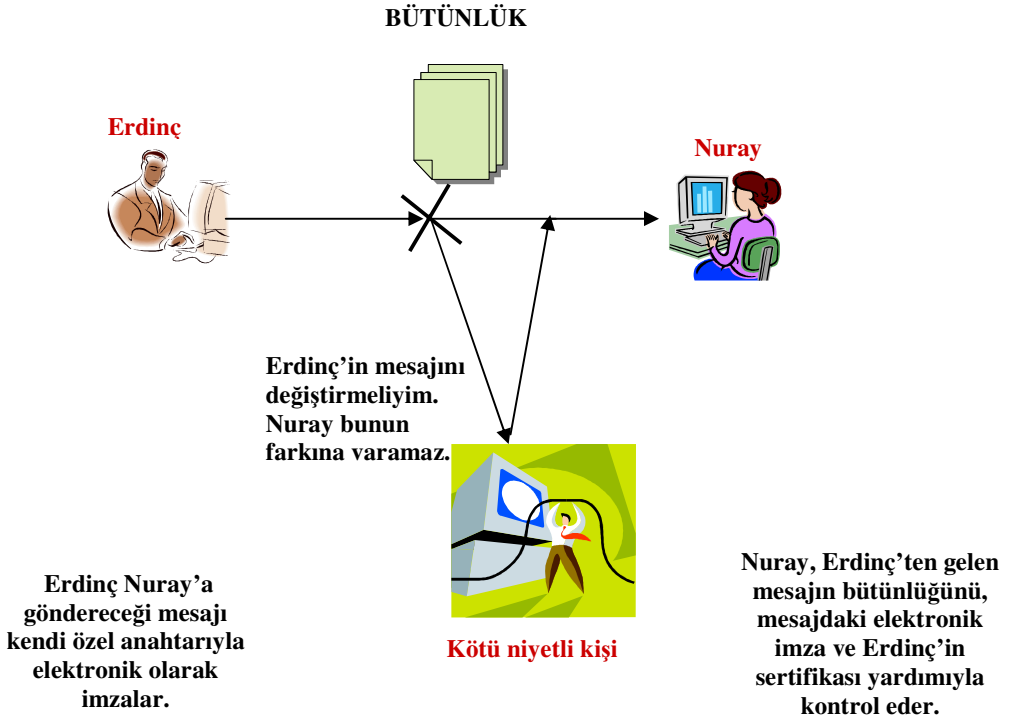
5.1.3 Akredite edilmiş sertifika hizmet sağlayıcısı tarafından verilen imza

Hukukumuzda sertifika hizmet sağlayıcıları bakımından akreditasyon sistemi kabul edilmemiştir. Buna karşılık, Avrupa Birliği Direktifinde ihtiyari akreditasyona yer verilmiştir. İhtiyari akreditasyon, bir sertifika hizmet sağlayıcısı işletmesi için özel hak ve yükümlülüklere bağlı olarak izin verilme usulüdür. Sertifika hizmet sağlayıcısı, yetkili makama başvurarak akredite edilmek isteyebilir. Bu durumda elektronik imza kanununda yer alan ve elektronik imza kanununa dayanarak çıkartılmış olan tüzükteki şartları taşıdığını ispat etmelidir. Bu halde yetkili makam, ilgili sertifika hizmet sağlayıcısının akreditasyonunu sağlar.

5.2 Elektronik İmza Özellikleri

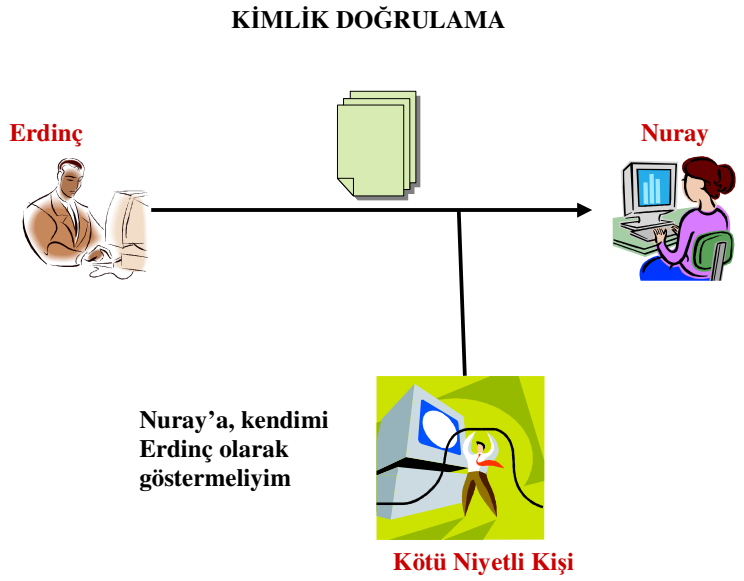
Elektronik imza kullanıcılarına aşağıda belirtilen dört temel özelliği sağlamaktadır [58,59]:

- **Veri Bütünlüğü:** Verinin izinsiz ya da yanlışlıkla değiştirilmesini, silinmesini ve veriye ekleme yapılmasını önlemek,



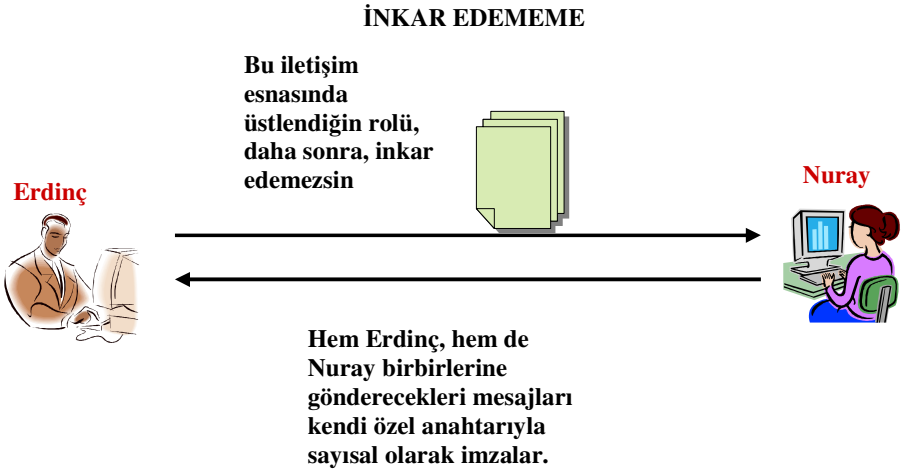
Şekil 5.1. Bütünlük

- **Kimlik Doğrulama ve Onaylama:** Mesajın ve mesaj sahibinin iletiminin geçerliliğini sağlamak,



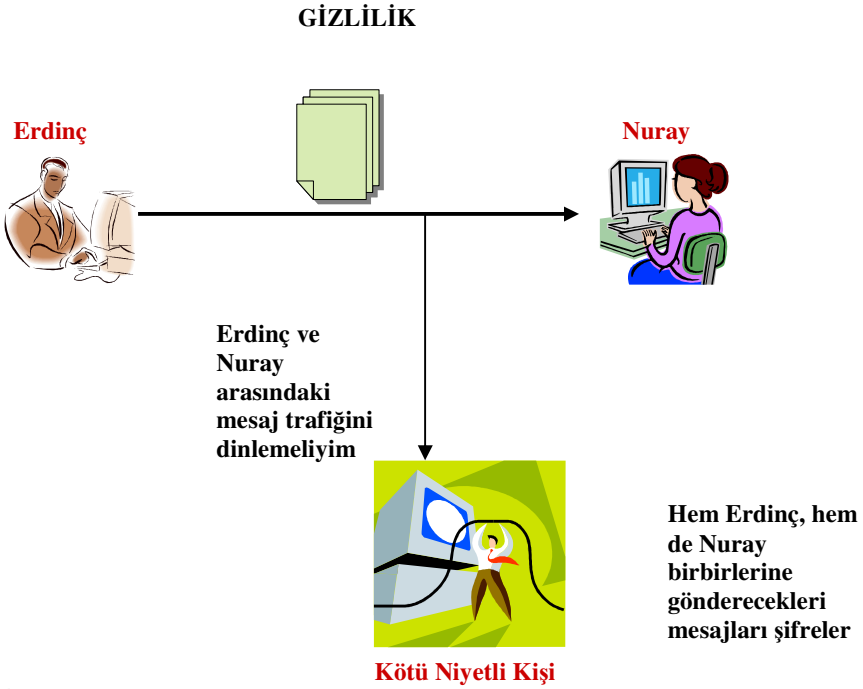
Şekil 5.2. Kimlik Doğrulama

- **İnkâr Edilemezlik:** Bireylerin elektronik ortamda gerçekleştirdikleri işlemleri inkâr etmelerini önlemektir.



Şekil 5.3. İnkar Edememe

- **Gizlilik**: Verilerin karşı tarafa doğrudan ulaştırılmasını sağlar. Başka kişiler tarafından erişilemez veya kullanılamaz.



Şekil 5.4. Gizlilik

- Düşük maliyet ve iş akış sürecinin hızlanması, bir dokümanı imzalamak için print edilmesinin gerekli olmaması ve kâğıt tasarrufunun sağlanması ve kırtasiyeciliği azaltmak

5.3 E-İmzaya Geçiş Nedenleri

Dünya çapında e-ticaretin hızla geliştiğini ve online yaşamın hayatın vazgeçilmez bir parçası olduğunu söyleyebiliriz. Fakat bunların önündeki en büyük engel "güvenlik"tir. İşte bu noktada e-imza ortaya çıkmaktadır.

Dijital kimlik ve verilerin güvenliği, şirketlerdeki ve kurumlardaki işleyişi önemli oranda etkilemektedir. Tüm araştırma raporları hack olaylarının ve internet zayıflıklarının alarm verecek durumda arttığını göstermektedir. 2006'lı yıllara kadar birçok kredi kartı bilgileri veya internet bankacılığı bilgilerinin hackerlerin eline geçtiği birçok araştırmacı kurum tarafından raporlanmıştır. İşte e-ticaret ve dijital kimliklere olan saldırılar, bu tür bilgilerin korunmasına özel bir ihtiyaç yaratıyor.

Bu sorunların sitelerin (e-ticaret, internet bankacılığı gibi) muhatap oldukları kişiyi tanımlamamasından kaynaklandığını göstermektedir. Bu sorunlar gidermek içinde dünya çapında dijital imzalar devreye girmiş durumdadır.

5.4 Elektronik İmzanın Faydaları

Elektronik imza, elle atılan imzaya eşdeğer nitelikte kullanılabildiği için, elektronik ortamda her türlü resmi işlemin, kâğıt ortamına göre daha hızlı, güvenilir ve maliyet etkin biçimde yürütülmesini sağlar. Bu bağlamda elektronik imza, kamu kuruluşlarıyla yapılan işlemlerde, bankacılık ve sigortacılık işlemlerinde, e-devlet, e-iş ve e-ticaret uygulamalarında, elektronik haberleşme ve sözleşmelerde, kanun kapsamındaki hukuki işlemlerde kullanılabilir[60–62].

E-İmza interneti kullanarak işlem yapan bireylerin sanal ortamda da, aynen gerçek hayatta olduğu gibi kimlik sahibi olması sonucunu doğuracaktır. Ayrıca e-imzanın hayatımızda yaratacağı en büyük değişikliklerden biri de; aslında tüm dünya ülkelerindeki yasal düzenlemelerin e-imzaya verdikleri hukuki değerle ilgilidir. Mesela; bilindiği üzere güvenli elektronik imza, ıslak imza ile aynı yasal sonuçları doğuruyor ve olası herhangi bir uyuşmazlıkta da kesin delil teşkil ediyor. Bu hukuki sonuç sayesinde artık kâğıtsız bir dünya idealine bir adım daha yaklaşmış olunmaktadır. Yazdığımız hiçbir maili, gönderdiğimiz hiçbir dosyayı, faturayı, herhangi bir belgeyi bundan sonra ne olur ne olmaz diye yazdırıp dosyalarda saklamak zorunda olmayacağız. Elektronik imzalı verilerin arşivlenmesi de son derece rahat olduğu için, dünyamızda e-imza ve benzeri teknolojiler sayesinde artık daha çok orman görmek mümkün olacaktır[63]. İnsanların işini kolaylaştıran, bilişim toplumu için uygun olan e-imza yönetimsel süreçlerin düzenlenmesi ve hızlandırılması, vatandaşa ait bilgilerin gizliliğinin sağlanması, hizmetlere kolay erişim, sayısal imzaların kullanımıyla zaman kazanımı sağlanmıştır.

E-imzanın özel ve iş hayatına çok önemli yararlar sağlamıştır. Bu yararları kısaca şu şekilde de sıralayabiliriz:

- Kimlik doğrulama ve kullanıcıların kimliğinden emin olmayı sağlar. Böylece tereddütleri ortadan kaldırır.
- Kullanıcı haklarını ve yetkilerini tanımlamayı kolaylaştırır. Bu şirketlere önemli ölçüde kolaylık sağlar.
- Kullanıcının inkâr edilme olasılığını ortadan kaldırır. İletişimde ve alışverişte güven unsuru artar.
- Gizlilik ve bütünlük sağlar. Veriler istenmeyen değişikliklere karşı korunur. Veri kaynağı rahat kontrol edilebilir.
- İletilen dokümanların tarih ve zamanını doğrular. Doküman arşivi oluşturulması kolaylaşır.

- E-imzanın ekonomiye olabilecek etkilerini de şu şekilde sıralayabiliriz:

- Düşük Maliyet,
- Karşılıklı işletilebilirlik (kurumlar arası),
- Standart çözüm,
- İş süreçlerinin iyileştirilmesi,
- İş gücünün doğru kullanımı,
- Kâğıt tüketiminde azalma,
- Daha düşük yönetim giderleri,
- Elektronik hırsızlığın azalması,
- Kayıt dışı ekonominin kayıt altına alınmasına katkısı,
- Verimliliğin artması,
- Telekomünikasyon giderlerinde azalma şeklinde sıralayabiliriz.

5.5 Elektronik İmzanın Uygulama Alanları

Elektronik imzanın; bankalar ve finans kurumları, şube ağına sahip sigorta şirketleri, kamu kurum ve kuruluşları, holdingler ve diğer büyük şirketler, üniversiteler, yüksek iletişim ve bilgi güvenliği gereksinimi olan organizasyonlar başta olmak üzere orta ve uzun vadede yaygın bir uygulama alanı bulabileceği değerlendirilmektedir.

5.6 Dünyada E-İmza ve Yapılan Çalışmalar

Elektronik imza konusunda dünyada çeşitli çalışmalar yapılmış, özellikle iki binli yıllara gelindiğinde bu çalışmalar hız kazanmıştır. Dünyada 50'den fazla ülkede e-imza kanun ve yönetmelik olarak uygulanmaktadır. Ancak, bu güne kadar çok yaygınlaşamamıştır. Bu amaçla ilk yapılan çalışmalardan birisi Birleşmiş Milletler Uluslar arası Ticaret Hukuk Komisyonunca hazırlanarak BM Genel kurulunda kabul edilen

- UNCITRAL Elektronik Ticaret Model Kanunu[64] çalışmasıdır.

Avrupa Birliği 1999/93/EC sayılı ve 13 Aralık 1999 tarihli,

Elektronik İmzanın Müşterek Çerçeve Şartlarının Belirlenmesi Hakkındaki Avrupa Birliği Yönergesi ile 2000/31 sayılı ve 8 Haziran 2000 tarihli Elektronik Ticaret Hakkındaki Avrupa Birliği Yönergesi çıkarılmıştır.

Avrupa Birliğine üye ülkeler bu yönergelere göre iç hukuklarında düzenlemelere gitmiştir[65,66].

Bazı ülkelerde yapılan elektronik imza çalışmaları aşağıda verilmiştir:

5.6.1 Danimarka

E-imza Kanunu 2000 yılında yürürlüğe girmiştir. Danimarka Bilgi Teknolojileri ve Telekom Otoritesi tarafından yapılan açıklamaya göre Mayıs 2005 itibariyle, 350,000 adetten fazla sayısal imza dağıtılmış durumdadır ve 5,5 milyonluk bir nüfusa sahip olan ülkede hedef 2007 yılı itibariyle 1,3 milyon sayısal imzaya ulaşmaktır. Ancak, iş dünyasında e-imza kullanımı çok kısıtlıdır. Bunun nedeni ticari alanda yasal çerçevenin iyi çalışmasından dolayı e-imzaya yatırım yapma isteğinin düşük olması olarak açıklanmaktadır. Ayrıca, mahkemeler, e-imza ile imzalanmış olan ticari sözleşmelerin geçerli olup olmadığını sorgulamakta serbesttir, bu durum ise şirketlerin e-imza kullanma isteğini azaltmaktadır. EDI (Electronic Data Interchange (Elektronik Veri Değişimi)) gibi bilinen teknolojiler hala etkindir ve iş dünyasında yaygın olarak kullanılmaktadır. Bu durum e-imza İçin gereksinimi ve talebi azaltmaktadır. Ticari ilişkilerde çok az kullanılmasının aksine e-imza, kimlik tanımlama mekanizması olarak e-devlet hizmetlerinde sıklıkla kullanılmaktadır[65].

5.6.2 Finlandiya

E-imza Kanunu 2003 yılında yürürlüğe girmiştir. 1998 yılında, Fin Hükümeti elektronik kimlik tanımlama, veri transferinde şifreleme ve elektronik işlemler için sayısal imza kullanımına imkân tanıyan bir sistem yaratmaya karar vermiş ve Nüfus Kayıt Merkezince PKI (Public Key Infrastructure(Açık Anahtar Altyapısı))tabanlı sertifikasyon hizmetleri sunulmaya başlanmıştır. Vatandaşlar bu merkezden, üzerinde gizli anahtar ve sertifikaların yüklü olduğu bir elD kartı satın alabilmektedirler. Nitelikli sertifikalara olan talep yavaş gelişmektedir ve bunun nedeni nitelikli sertifika gerektiren hizmetlerin henüz olmamasıdır, Nitelikli sertifika gerektiren hizmetlerin eksikliğinin sebebi, kısmen internet bankacılığı hizmetlerinin yaygın olması ve Finli tüketicilerin bunların kullanımına alışmış olmasıdır[65].

5.6.3 İsveç

E-imza Kanunu 2001 yılında yürürlüğe girmiştir. E-imzanın, çok nadir olarak çevrim içi sitelerden alışveriş yapan bir tüketici için hala çok pahalı ve karmaşık olduğu belirtilmektedir[65].

5.6.4 Hollanda

E-imza Kanunu 2003 yılında yürürlüğe girmiştir. Hollanda'da e-imza kanununa göre, ESHS (Elektronik Sertifika Hizmet Sağlayıcı) tarafından sertifika verilecek olan kişi, kimlik tespiti esnasında bizzat hazır bulunmak zorundadır. Bu durumun, e-imzanın kısıtlı kullanımı

için bir sebep olabileceği belirtilmiştir. Ticari iş ilişkilerinde e-imza kullanımının çok az olmasına karşın, e-devlet hizmetlerinde kimlik tanımlama mekanizması olarak kullanımı gittikçe artmaktadır[65].

5.6.5 Fransa

E-imza Kanunu 2000 yılında yürürlüğe girmiştir. İş dünyasında e-imzanın çok kısıtlı kullanılmasının nedeni, ticari alanda delil hukukunun etkin bir şekilde işliyor olması ve bu durumun e-imza teknolojisine yatırım eğilimini azaltmasıdır. Özellikle, mahkemeler, e-imza ile imzalanmış olan ticari sözleşmelerin geçerli olup olmadığını sorgulamakta serbesttir ki bu durum e-imza kullanma isteğini azaltmaktadır[65].

5.6.6 Estonya

E-imza Kanunu 2000 yılında yürürlüğe girmiştir. Estonya devleti elektronik kimlik kartını tüm vatandaşlarına zorunlu hale getirmiştir. Bu kartlarda sayısal kimlik tanımayı ve sayısal imzayı sağlayan, direktife göre nitelikli olan bir sertifika vardır. Yaklaşık 1,3 milyonluk bir nüfusa sahip olan Estonya'da 900,000 kart basılmıştır ve bunların 800,000 adedi aktif olarak kullanılmaktadır[65].

5.6.7 Yunanistan

E-imza Kanunu 2001 yılında yürürlüğe girmiştir. 2004 yılında e-iş forumu, e-imzanın durumunu hukuki ve teknik açıdan tartışmak üzere özel bir çalışma grubu kurmuştur. Söz konusu grup aşağıdaki hususlara dikkat çekmiştir;

- E-imza uygulamasını desteklemek için gerekli olan teknik çerçevenin geliştirilmesi ve idamesi hala oldukça pahalıdır ve yatırımların dönüşü belirsizdir.
- Farklı e-imza ürünleri ve hizmetleri arasında uyumlu çalışabilirlik olmadığı için, e-imza kullanımında "kritik kitle"ye henüz erişilememiştir.
- İhtiyari akreditasyonun nasıl organize olacağı, kamu sektöründe hangi çeşit imzanın kullanılması gerektiği, e-imzanın uzun vadede geçerliliğinin nasıl sağlanacağı, bankacılık sektöründe e-imzanın uyumlu çalışabildiğinin nasıl sağlanacağı, e-imza kullanıcısının kişisel verilerinin nasıl korunacağı gibi hususlar uygulamada yaşanan zorluklar olarak belirtilmiştir.

Mayıs 2006'da Yunan Bankalar Birliği, e-bankacılık işlemlerinde yaşanan korsan saldırıları tartışmışlar ve Önerilen diğer yöntemlerin yanı sıra e-imza kullanımının desteklenmesini kararlaştırmışlardır[65].

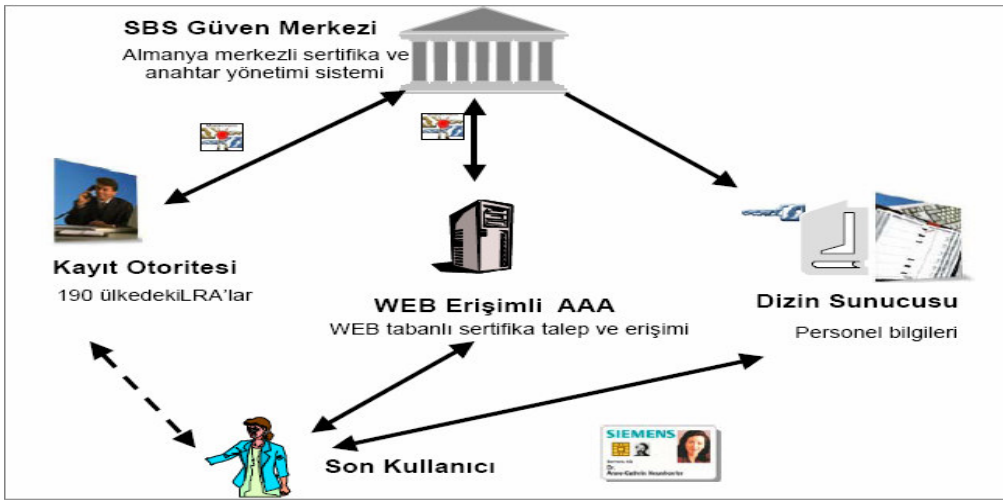
5.7 Dünyada Elektronik İmzaya İlişkin Örnek Uygulamalar

5.7.1 Siemens ve SBS kurumsal PKI projesi

Dünyanın en büyük kurulu sitelerinden birini kurmuş ve işletmektedir. Sertifika Otoritesi, tek merkezden tüm dünyadaki Siemens ve SBS çalışanlarına (2001'den itibaren 190 ülkede, 500 lokasyonda 484.000 kullanıcı) sayısal imzalar ve şifreleme yoluyla güvenlik çözümü sağlanmıştır[67].

İhtiyaçlar / Çözüm: E-posta, dosya ve veri şifreleme, logon, intranet ve ERP erişimi ve iş süreçleri yönetimi alanlarında güvenlik talep eden müşteriye sayısal imzalar, sayısal sertifikalar, sertifika yönetimi, son kullanıcı yazılımları sunulmuştur. Proje kapsamında Açık Anahtar Altyapısı hizmetleri Akıllı Kartlar ile bütünleşik halde sunulmuştur.

Faydaları: Kurum içi ve kurumlar arası güvenli iletişim, iyileştirilmiş ve otomasyonu sağlanmış iş süreçleri, zamandan tasarruf ve yönetilen Açık Anahtar Altyapısı sayesinde kolay uygulanabilen ve düşük maliyetli çözüm sağlanmıştır.



Şekil 5.5. Siemens ve SBS Kurumsal PKI Projesi

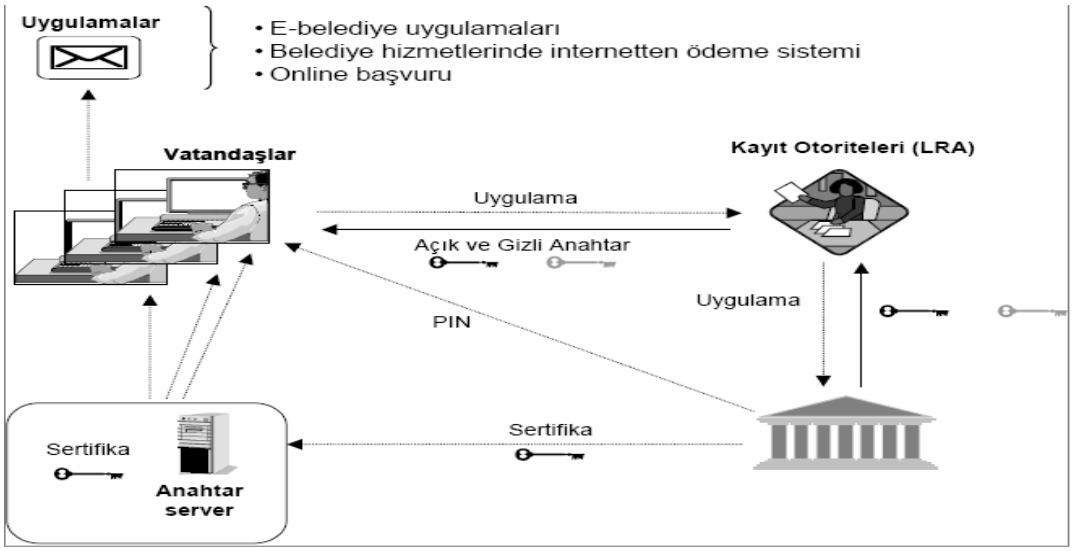
5.7.2 Sanal şehir hagen projesi

Sanal Şehir Hagen projesi tüm kamu hizmetlerine sanal ortamda erişim sağlayarak "e-devlet" uygulamalarının temelini oluşturmuştur[67].

İhtiyaçlar / Çözüm: İhtiyaçları, erişimde gizlilik ve doğrulama, sayısal imzalar, açık, ileriye dönük ve standart bir çözüm, güvenli ödeme sistemleri ve "e-devlet" ve "çevrim-içi yönetim"de yönetim süreçlerinin düzenlenmesi olan müşteriye yeni teknolojiye geçişte esnek

bir yapı, gizliliğin, doğrulamanın şifreli veri transferi ve sayısal imzalarla sağlanması ve Açık Anahtar Altyapısı ile bütünleşik bir çözüm sunulmuştur.

Faydaları: Vatandaşın işini kolaylaştıran, "bilişim toplumu" için uygun olan bu çözümle yönetimsel süreçlerin düzenlenmesi ve hızlandırılması, vatandaşa ait bilgilerin gizliliğinin sağlanması, hizmetlere kolay erişim, sayısal imzaların kullanımıyla zaman kazanımı sağlanmıştır.



Sekil 5.6. Sanal şehir hagen projesi

5.7.3 Fransa Maliye Bakanlığı

Fransa Maliye Bakanlığı, 1998 yılında kurumların internet üzerinden vergi beyanını mümkün kılmaya karar verdi. 15 milyon €'dan fazla geliri olan 20,000 firmanın vergi beyanlarını internet üzerinden gerçekleştirmesi zorunluluğu yasalarla getirildi[67]. Bakanlık, kendisi sertifika otoritesi olarak davranmak yerine bu kararını gerçekleştirmek üzere, sertifika dağıtımını yapmayı üçüncü partilere bırakmayı tercih etti.

İhtiyaçlar / Çözüm: Güvenlik alanında çözümler sunan Verisign'ın bölgedeki iş ortağı Certplus, belli başlı Fransız bankaları ile çalışarak kurumlara sayısal sertifikaların dağıtımı ve kurulumu için gerekli çalışmaları gerçekleştirmiştir. Certplus'ın ilk aşamada dağıttığı 25,000 sertifika aktif bir şekilde kullanılmaktadır. Bu sayı 80,000'lere ulaşmaktadır.

Sağlanan Faydalar: Sağlanan çözüm ile hem zaman, hem de maliyet ve insan kaynağından tasarruf sağlanmıştır.

5.7.4 Köln şehri kartı

Köln Şehir Kartı Projesi, belediye hizmetleri içerisinde bulunan iş süreçlerinin, çalışanlar ve vatandaşlar için güvenli elektronik bir ortama taşınması süreçlerini kapsamaktadır.

İhtiyaçlar / Çözüm: Vatandaş ve belediye arasındaki elektronik iletişimin sağlanması, yasal olarak kullanılan sayısal imzalar için teknik altyapı ve açık, ileriye dönük ve standart bir çözüm gibi ihtiyaçlara yönelik olarak Açık Anahtar Altyapısı ile akıllı kartların bütünleştirildiği bir çözüm sunulmuştur. Buna bağlı olarak iş süreçleri sayısal imzalar yardımıyla iyileştirilmiş; çoklu uygulamalı kartlarla birlikte çözüm eğitim, kültür ve sağlık alanına da genişletilmiştir.

Sağlanan Faydalar: Proje "Bilişim toplumu"na geçişte önemli bir adım olarak görülmüştür. Yönetimsel süreçlerin düzenlenmesi ve hızlandırılması, bilgisayar ağları ve fiziksel erişimde aynı altyapının kullanılması, vatandaşa ait bilgilerin gizliliğinin sağlanması, hizmetlere kolay erişim ve sayısal imzaların kullanımıyla zaman kazanımının sağlanması sağlanan diğer önemli faydalar olarak sıralandırılabilir[67].

5.7.5 İtalya İçişleri Bakanlığı İtalyan kimlik (ID) kart projesi

İtalya Avrupa bölgesinde elektronik karta geçen ikinci ülkedir. İtalyan İçişleri Bakanlığı'nın vatandaşlarının kimlik tanınmalarının geliştirilmesi ve vatandaş ile kamu otoriteleri arasındaki ilişkinin kamu kuruluş binalarının dışına taşınmasını sağlamak amacıyla oluşturduğu çözüm, akıllı kart teknolojisine dayalı yeni bir kimlik kartı üstüne kurulmuştur. Proje kapsamında merkezi PKI yönetimi ile güvenli, belediyelerde online elektronik kimlik kartı dağıtımı prosedürleri ve süreçleri gerçekleştirilmiştir. Proje pilot aşamasında Milano, Palma ve Roma'da bulunan 83 belediye ve 280,000 vatandaşı kapsamıştır. 5 yıl içerisinde İtalyan Hükümeti yaklaşık 40 milyon elektronik kimlik kartı oluşturacaktır[67].

5.7.6 Danimarka – KPMG

Dünya çapında 100,000'den fazla çalışanıyla, KPMG 152 ülkedeki şirketlere sigorta, vergi ve hukuk, finansal danışmanlık hizmetleri sunmaktadır. KPMG'nin, Danimarka'da ülke çapında 19 ofisinde yaklaşık 1400 çalışanı bulunmaktadır[67].

İhtiyaçlar / Çözüm: KPMG son zamanlarda müşteri tarafından gelen internet üzerinden güvenli iletişim talepleriyle karşı karşıya kalmaktaydı. Bu zamana kadar çok önemli belgelerin müşteri ile iletişimi normal posta ile gerçekleştirilmekteydi. PKI çözümünü kurarak, KPMG müşterileri ile arasında güvenli bilgi alışverişini gerçekleştirerek, müşteri arasındaki güven öğesini pekiştirirken müşteri memnuniyetini de artırmıştır. Çözüm kapsamında KPMG müşterilerine sertifika dağıtım ve onaylama işlemlerini gerçekleştirmiş ve yeni müşterilerin

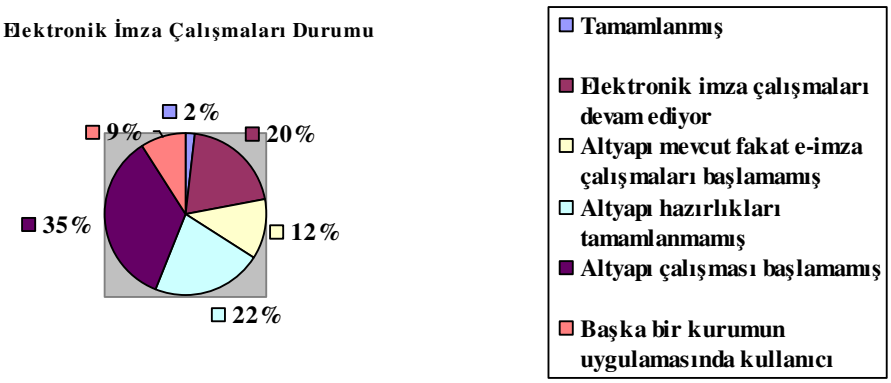
kolaylıkla eklenmesini sağlayan esnek ve varolan IT altyapısı ile tamamıyla bütünleşik bir sistem kurmuştur. Dünyaca tanınan Verisign sertifikaların kullanılmasıyla, KPMG ve müşterileri aynı zamanda güvenlik çözümleri açısından sadece ülke sınırları içerisinde geçerli bir sistem kullanmamış oldu.

5.8 Türkiye'de E-İmza

5070 sayılı Elektronik İmza Kanunu 23.01.2004 tarihli ve 25355 sayılı Resmi Gazete'de yayımlanmış ve 23.07.2004 tarihinde yürürlüğe girmiştir. Söz konusu Kanunun 20'nci maddesi uyarınca Telekomünikasyon Kurumunun, ilgili tüm taraflarla yaptığı çalışmalar neticesinde hazırlanan "Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik" (Yönetmelik) ile "Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ" 6 Ocak 2005 tarihli ve 25692 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Müteakiben, söz konusu ikincil düzenlemelerin bazı hükümlerinde görülen lüzum ve Telekomünikasyon Kurul'unun onayı üzerine kısmi değişiklikler yapılmıştır[65].

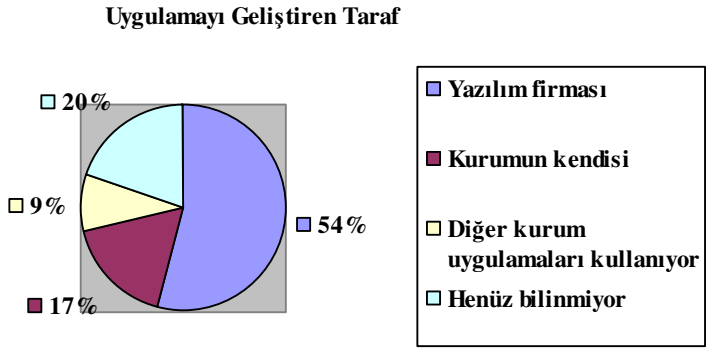
13 Ekim 2006 tarihi itibariyle 65 kamu kurumunun KSM ile elektronik imza konusunda görüşmelerde bulunmuştur[81]. Bu kurumlardan görüşmelerden elde edilen sonuçlara göre:

- 13 Ekim 2006 tarihi itibariyle 19 kuruma toplam 2518 adet nitelikli elektronik sertifika verilmiştir. Aktif olarak kullanılan sertifika sayısı 350'dir.
- KSM' ye başvuran kurumların %35'inde altyapı çalışmaları başlamamıştır. Ayrıca altyapısı tamamlanan kurumların oranı (%2)oldukça düşüktür. Ekleme çalışması devam eden kurumların oranı ise %20'dir.



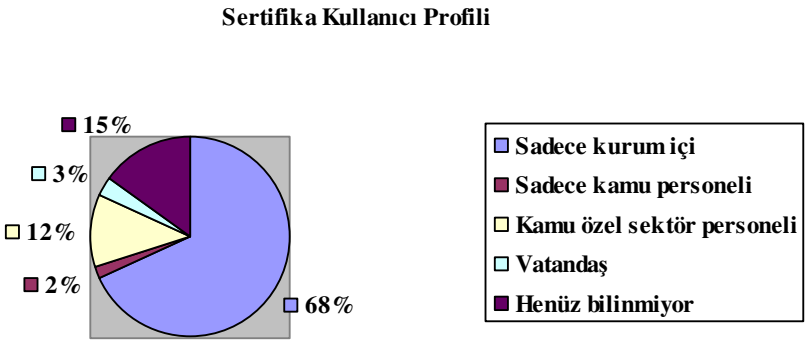
Şekil 5.7. Elektronik İmza Çalışma Durumu

- Kurumlarda elektronik imza uygulaması büyük çoğunlukla (%54) yazılım firmaları tarafından geliştirilmektedir. Kurumların %17'si ise kendi uygulamalarını gerçekleştirirken;%9'u da diğer kurumların uygulamalarından yararlanmaktadır.



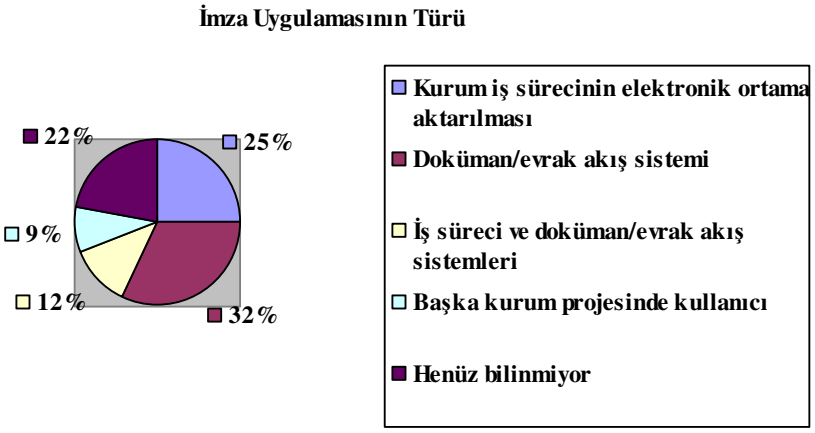
Şekil 5.8. Uygulamayı Geliştiren Taraf

- Kurumların çoğu (%68) Nitelikli Elektronik Sertifikayı kurum içi personeline kullandırmayı düşünmektedir. Kurumlar genelde kendi iç yazışmalarını elektronik ortama geçirmek için elektronik imzaya ihtiyaç duymaktadır. Kurum personeli dışı potansiyel kullanıcıları olan kurumların sayısı azınlıkta kalmaktadır.



Şekil 5.9. Sertifika Kullanıcı Profili

- Uygulamayı kendisi geliştiren kurumlar, genelde kurum içi yazışmaları elektronik imza kullanarak elektronik ortama geçirme çalışması yapmaktadır(%32).



Şekil 5.10. İmza Uygulama Türü

Elektronik imza düzenlemelerinin tamamlanması ve ESHS'lerin faaliyete geçmeleri neticesinde güvenli elektronik imzanın kullanılabilir hale gelmesiyle birlikte kamu kurum ve kuruluşları, kamu hizmetlerini vatandaşlara azami kalite ile asgari maliyette sunabilmek ve bürokratik işlemleri azaltabilmek amacıyla, ilgili taraflarla olan işlemlerini elektronik ortamda e-imzalı olarak yürütebilmek için projeler geliştirmeye başlamışlardır. 01.08.2005 tarihinde Devlet Bakanı tarafından pilot olarak başlatılan ve kamudaki ilk e-imza uygulaması olan Dış Ticaret Müsteşarlığı (DTM)'nın Dahilde İşleme Rejimi (DİR) Otomasyon Projesi kapsamında, ihracatçı firmalara nitelikli elektronik sertifika dağıtılmıştır. DİR uygulaması 01.02.2006'dan itibaren DTM tarafından zorunlu hale getirilmiştir. Daha sonra geçen veya geçmeye çalışan kurumlar:

- Adalet Bakanlığı

Adalet Bakanlığı Bilgi İşlem Dairesi Başkanlığı, kurum içi yazışmalarda Kamu SM e-imza sertifikalarını 14.08.2006 tarihinden itibaren kullanmaya başladı. Adalet Bakanlığı Müsteşar Yardımcıları'nın da aralarında bulunduğu sertifika sahiplerine teslim edilen sertifikalar aktif hale getirilerek kullanıma açıldı. Bakanlık bünyesinde testleri süren UYAP (Ulusal Yargı Ağı Projesi)yazılımına e-imza entegrasyonu sırasında Kamu SM tarafından teknik destek ve danışmanlık verilecek. E-imzaya geçişin sorunsuz yaşanması için Adalet Bakanlığı ve TÜBİTAK UEKAE arasında iletişim kanalları oluşturuldu. Çalışmalar sonunda bakanlık teşkilatındaki 30.000 hakim ve savcı ile yurt genelindeki 40.000 avukat Kamu SM güvencesiyle e-imza kullanabilecek.

- İSKİ

E-devlet çalışmalarını sürdüren lider kurumlardan İstanbul Su ve Kanalizasyon İdaresi (İSKİ), abone sisteminde e-imzaya geçme kararı aldı. Düzenlemeyle birlikte e-imza sahipleri, İSKİ müdürlüklerine gitmeye gerek duymadan, mukavelelerini ıslak imzaya eşdeğer nitelikteki elektronik imza ile onaylayabilecekler. Vatandaşların bu yenilikten faydalanmaları için herhangi bir ulusal ESHS'den alınmış geçerli bir nitelikli elektronik sertifika bulundurmaları yeterli olacaktır. Yeniliğin, 4 milyon İSKİ abonesine hem kolaylık hem de zamandan ve ulaşım ücretinden tasarruf olanağı sağlaması beklenmektedir. İSKİ, e-imza entegrasyonu için kullanacağı yazılım kütüphanelerini TÜBİTAK UEKAE'den temin etmiştir. 29 Haziran 2006 tarihinde İSKİ Bilgi İşlem Daire Başkanlığı Heyeti ile Kamu SM yetkililerinin TÜBİTAK UEKAE'de yaptığı toplantıda İSKİ'nin hazırlıklı olduğu gözlendi. Kurumun altyapısı 30 Haziran 2006'da yerinde incelenerek, e-imza test kütüphaneleri ve test sertifikaları yetkililere teslim edildi. Kurum, test çalışmalarının ardından e-imzayı devreye almayı planlıyor. Abonelere yönelik yeniliklerin yanı sıra, İSKİ'ye ait kurumsal evrak yönetim sistemine de e-imza entegrasyonu çalışmaları başlatılmıştır. 6 binden fazla PC'nin kullanıldığı İSKİ sistemlerindeki entegrasyon çalışmalarının tamamlanmasının ardından, kurum personeline akıllı kart üzerinde e-imza sertifikaları, kart okuyucuları ile birlikte teslim edilecektir.

- TÜBİTAK UEKAE

30 Haziran 2006 TÜBİTAK UEKAE, kendi geliştirdiği Kurumsal Bilgi Yönetim Sistemi(KBYS) üzerinde 5070 sayılı E-imza Kanununa uygun sayısal imza kullanımı için çalışmalarını sürdürüyor. Sistemde ilk olarak 5018 sayılı kanunla iş yükü artan Satın alma ve Genel Harcama Talimatı Sistemi e-imza uyumlu hale getirilecek. KBYS'de daha önce de sayısal imza ile onaylamanın yapıldığını bildiren yetkililere göre, hukuki nitelikte e-imza olmadan kağıt ortadan kaldırılamazken, satın alma talepleri ve elektronik olarak hazırlanan OLUR belgeleri çıktı alınarak ıslak imza ile imzalanmakta, bu da süreçlerde darboğaza neden olmaktadır. Pilot çalışma ile TÜBİTAK UEKAE'nin Satın alma Birimi'nde kağıt trafiğinin azaltılması ve verimlilik artışı hedefleniyor.

E-imza, zamanla diğer KBYS bileşenlerine entegre edilecek.

- TURKCELL

Turkcell, cep telefonları için geliştirilmiş, yasal olarak ıslak imzaya eşdeğer elektronik imza uygulamasını, SIM kart üzerindeki ek güvenlik özellikleriyle beraber kullanıcılarının hizmetine sunuyor. Turkcell, yasal olarak ıslak imzaya eşdeğer yeni servisi Turkcell Mobil

imzayı, ilk olarak Internet bankacılığında Akbank, Garanti, Türk Ekonomi Bankası, Türkiye İş Bankası ve Yapı Kredi işbirliğiyle müşterilerine sunuyor.

Turkcell Mobil İmza, 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 mobil olarak yapılabilmesine olanak sağlıyor. E-imza teknolojisini mobil ortama taşıyan Turkcell Mobil imza ile ayrı bir akıllı kart ve kart okuyucu kullanmaya gerek olmadan, imza gerektiren işlemlerin de Internet bankacılığına taşınabiliyor, resmi başvurular uzaktan yapılabiliyor. Turkcell kullanıcıları, ekstra cihaz ve elektronik sertifika yatırımı olmaksızın mevcut telefonlarıyla mobil imzanın sağladığı kolaylık ve ekstra güvenlikten yararlanabilecekler. Turkcell Mobil imza ile kişilerin imza atarken kullanacakları "Nitelikli Elektronik Sertifika"lar E-Güven tarafından sağlanacak.

5.9 Elektronik İmza Uygulamalarını Hayata Geçirirken/Planlarken Kurumlarımızca Karşılaşılan Temel Sorunlar Ve Öneriler:

Sorunları 3 ana başlık altında toplayabiliriz:

5.9.1 Kurumlar arası uyum problemi

Elektronik imzanın veri formatı, genel kabul görmüş bir format olarak belirlenmelidir. Tüm kurumlar elektronik imzayı standart bir formata uygun olarak oluşturmalıdır. Aksi durumda, ileride kurumların kendi sistemleri içinde oluşturdukları imzanın diğer kurumun sistemi içinde anlaşılamaması ve imzanın doğrulanamaması problemi ortaya çıkacaktır. Bu konuda Telekomünikasyon Kurumu'nun 1 Haziran 2006 tarihli kurul kararında tavsiye edilen ETSI'nin (European Telecommunications Standart Institute) yayınladığı TS 101 733 veya TS 101 903 dokümanlarında yer alan imza formatları kamu kurumlarında standart olarak kabul edilmelidir.

5.9.2 Elektronik imza yazılımlarının güvenilirliğinin sağlanması

Elektronik imzanın güvenliği, kullandığı açık anahtarlı altyapı teknolojisine dayanmaktadır. Ancak, elektronik olarak imzalanan dokümanın formatı ve elektronik imzayı oluşturan yazılımlarda bu teknolojiden bağımsız olarak imzanın güvenilirliği ile doğrudan ilgilidir[68]. Dokümanların içinde barındırdığı macro, script gibi program parçacıkları elektronik imzanın güvenilirliğini tehlikeye düşürmektedir. Bu tür program parçacıkları yaygın virüs taşıyıcılar, dokümanın farklı ortamlarda(işletim sitemi, dokümanı gösteren program gibi)farklı biçimlerde ekrandan kullanıcıya gösterilmesine neden olabilir. Bu durumda, imza doğrulanabildiği halde, imzalayan kişi ile imzayı doğrulayan kişinin ekrandan gördüğü metin veya anlamlı bilgiler farklılık gösterebilir. Bu olumsuz duruma meydan vermemek için kamu

kurumlarının, uygulamalarında güvenli kabul edecekleri şartlar altında elektronik imza kullanımına izin veren bir politika oluşturması gerekir.

Kurumlar veya özel firmalar tarafından geliştirilen elektronik imza oluşturma ve doğrulama yazılımlarının, mevzuatta belirtilen standartlara uygun olması sağlanmalıdır. Ancak, mevzuatta bu standartlara uyum zorunluluğu sadece ESHS'lere (Elektronik Sertifika Hizmet Sağlayıcısı) şart koşulmuştur. Oysaki imza yazılımları çoğunlukla ESHS'ler dışındaki yazılım firmaları tarafından geliştirilmektedir. Yazılımı geliştiren tarafların aşağıdaki standartlara uyması, elektronik imzanın güvenilirliği açısından oldukça önemlidir:

- CWA 14170: Security Requirements for Signature Creation Applications(İmza Oluşturma Uygulamaları için Güvenlik Gereksinimleri)
- CWA 14171: Procedures for Electronic Signature Verification(İmza Doğrulama için Prosedürler)

5.9.3 Kurumlar arası yazışmaların elektronik imzaya geçirilmesi için çalışmalar yapılması

Altyapısı olmadığı halde, genellikle kurum içi veya dışı yazışmalarını kağıt olmadan, elektronik imza ile elektronik ortamdan yapmak isteyen kurumlar mevcuttur. Tüm kamu kurumlarının özellikle diğer kurumlarla olan yazışmalarını elektronik ortamdan yapacakları bir altyapının sağlanması için çalışma yapılması gerekliliği ortaya çıkmaktadır.

Yapılacak çalışma içersinde aşağıdaki konulara açıklık getirilmesi ve tüm kurumların bu çalışmanın çıktılarına uygun yazılımlar geliştirerek yazışmaları elektronik ortama aktarması gerekmektedir:

- Resmi yazışmalarda üst yazı için standart veri tipi tanımlanmalıdır. Veri tipi tanımlanırken "Resmi Yazışmalarda Uygulanacak Esas ve Usuller Hakkında Yönetmelik"te belirtilen şartlara uyulmalıdır.
- Üst yazının eklerinin imzalanması konusunda bir yöntem belirlenmelidir.
- Paraf atılması gereken noktalarda elektronik imzanın kullanılıp kullanılmayacağı konusu netleştirilmelidir.
- Kurumlar arasında resmi yazışmaların iletilmesi için ortak bir protokol belirlenmelidir.
- Elektronik ortamdaki yazışmalarda mühür kullanımının tanımı yapılmalıdır.

Elektronik imzanın doğru kullanımı sağlamak ve ileride oluşabilecek, öngörülen problemleri engellemek için uygulamalar Gerçekleştirilirken yukarıda değinilen durumlara dikkat edilmelidir.

Adalet Bakanlığı	Islak imzanın kullanma mecburiyetinin yönetmelikler, kanunlar gereği devam etmesi Kullanıcıların bu uygulamalara adapte olacak bilgi seviyesinde olmaması
Devlet Meteoroloji İşleri GM	Islak imzanın kullanma mecburiyetinin yönetmelikler, kanunlar gereği devam etmesi Türkiye'deki internet altyapısının yeterli derecede yaygın olmaması Kurum içinde elektronik imza altyapısına uygun olmayan istisnai süreçlerin bulunması Kullanıcıların bu uygulamalara adapte olacak bilgi seviyesinde olmaması
Dış Ticaret Müsteşarlığı	Öncelikle kurumda çalışanların elektronik imza uygulamaları konusunda yeterli teknik bilgi eksikliği olması nedeniyle çalışanların bu tür uygulamaları kabullenmesi ve inanması konusunda zorluk çekilmiştir. Ayrıca, elektronik imza kanunun projeye başlandıktan sonra çıktı. Bu kanun çıkıncaya kadar hukuksal anlamda bir boşluk olması nedeniyle projenin tam PKI yapısında başlanılamadı. Bunun yanında, PKI yapısına dayalı uygulamaların dünyada ve özellikle ülkemizde çok örnekleri olmaması ve bu konuda kamu/özel sektör uzmanlarının da yeterli teknik bilgiye sahip olmaması, hukuki ve teknik boşlukları doldurmaya çalışmamız projeyi hızlı bir şekilde devreye almamızı zorlaştırmıştır.
Emekli Sandığı GM	Islak imzanın kullanma mecburiyetinin yönetmelikler, kanunlar gereği devam etmesi Uygulamanın hayata geçirilmesinde kurum içi teknik yetkinliğin yeterli olmaması Kullanıcıların bu uygulamalara adapte olacak bilgi seviyesinde olmaması
T.C. Merkez Bankası	Kullanıcıların bu uygulamalara adapte olacak bilgi seviyesinde olmaması
Nüfus ve Vatandaşlık İşleri	Islak imzanın kullanma mecburiyetinin yönetmelikler, kanunlar gereği devam etmesi uygulamanın hayata geçirilmesinde kurum içi teknik yetkinliğin yeterli olmaması Elektronik ortama dayalı iş süreçlerine hukuksal dayanak oluşturmak için

Tablo 5.1. Kurumlar Arasında Yapılan Anket Sonuçları

5.9.4 Diğer öneriler

- Kurumsal ağlarda e-imza uygulamaları kapsam ve amacına uygun sınırlı pilot uygulamalar biçiminde tasarlanmalıdır. Bu uygulamadan olumlu sonuç alındığı taktirde kapsam genişletilmelidir.
- Diğer kurum ve vatandaşlarla olan ilişkilerde e-imzaya geçişin sağlıklı olabilmesi için kurumlarla gerekli koordinasyonun sağlanması ve uygulamalar arasında uyum sağlanmalıdır. Yani e-imza uygulamalarının belli standartlara ve kriterlere uygun olarak gerçekleştirilmesi, ileride yaşanabilecek problemlerin en aza veya çözülebilir düzeye indirilmesi için yapılması gereken bir zorunluluktur.
- E-imzanın yetkin olarak kullanılması için kurum ve kuruluşlarda çalışanların bilgisayar bilgisi arttırılmalı ayrıca e-imza kavramı konusunda bilgi verilmeli veya arttırılmalıdır.
- E-imza kullanılan yerlerde kullanıcılara gerektiğinde bilgi verecek ve sorunlarına çözüm getirecek çağrı merkezleri kurulmalıdır.
- E-imza desteği sağlayan uygulamalar anlaşılması kolay, karmaşık olmayan yapıda olmalıdır.
- E-imza konusunda ki maliyet ve sorunlar en alt seviyeye çekilmelidir. Maliyet konusunda devlet bazı dış ülkelerde olduğu gibi kurum, kuruluş ve kullanıcılar üzerinden mali yükün bir kısmını kaldırmalıdır.
- E-imza uygulamalarını devreye sokabilmek için öncelikli olarak yöneticiler bazında bilgi verilmelidir.
- Yapılacak olan ihaleler mevzuata uygun olarak yazılmalıdır.
- E-imza uygulamasının yeterli bir şekilde geliştirilebilmesi için AR-GE toplulukları oluşturulmalı ve bu şekilde e-imzada meydana gelebilecek gelişmeler ve güncellemeler daha düzenli olarak takip edilebilecektir.
- E-imzanın bir araç olduğu unutulmamalıdır. Belirli bir uygulamayla ilişkilendirilmediği sürece, bir e-imza projesinden bahsetmek mümkün değildir. E-imza teknolojilerinde istenmeyen sonuçlarla karşılaşmamak, iyi belirlenen ve dikkatli uygulanan politikalarla mümkün olacaktır.
- Her ne kadar teknik altyapı hazırlanmış olsa da kurum veya kuruluşlarda belli alışılmış durumlardan vazgeçmekte zorluklar çıkacaktır. Bu sebeple e-imza uygulamaları sırasında kullanıcılar tarafından belli bir direnç gösterilecektir. Bu e-imzanın önündeki en önemli engel olarak görülmektedir. Onun içinde bu yaklaşımların en kısa biçimde yok edilmesi sağlanmalıdır. E-imzanın getireceği yararlar kullanıcıların anlayacağı örneklerle anlatılmalıdır.

5.10 Elektronik İmzanın Yaygınlaştırılması İçin Yapılabilecekler

Elektronik imza yasası ile birlikte kamuda ve özel sektörde elektronik imza yavaş yavaş hayatımıza girmeye başlayacaktır. Bu sürecin ekonomik bir yarar sağlayabilmesi ise teknolojik değişikliklere ayak uydurabilecek özellikle eşgüdümlü bir planın uygulanmasıyla mümkündür. Bu amaçla devlet, diğer ülkelerdeki devletlerin üstlendiği role benzer olarak, iş dünyası, son kullanıcı, AR-GE birimleri, üniversiteler gibi bu teknolojinin ülkemizde kullanılması, benimsenmesi ve üretilmesi aşamalarında işbirliği yapması gereken kurumlar arasında ilk sırada yer almalıdırlar[82]. Devlet elektronik imzanın yaygınlaşması için destek olmalıdır. Bu kapsamda elektronik imzanın bir cep telefonunu kullanmak kadar kolay kullanımının sağlanması için çalışmalar yapılması düşünülebilir. Daha önceki dönemlerde YTL geçişi sırasında Sanayi Bakanlığı tarafından yapılan tanıtım ve reklâm çalışmalarının benzerleri elektronik imzanın yaygınlaştırılması sürecinde de düşünülebilir. Eşgüdümü sağlamak amacıyla bilişim teknolojileri kapsamındaki tüm tarafların (donanım üreticileri, altyapı/iletişim ağı kurucuları ve işleticileri, yazılım hizmetleri üreticileri, hizmet sunucuları, içerik üreticileri/sunucuları) ilgililerinin temsil edildiği bir kurumsal yapılanma en kısa zamanda oluşturmalıdır. Benzer düzenleyici kurumlar Almanya, Norveç, Danimarka, İtalya, Fransa ve İspanya gibi birçok ülkede bakanlık olarak bulunmaktadır. Ayrı bir bakanlık çatısı altında olmasa da İngiltere, Finlandiya ve İsviçre'de düzenleyici kurum enformatik alanında tek bir otoritededir. Amerika Birleşik Devletleri'nde ise düzenleyici kuruluş Kongre'ye doğrudan bağlı olarak çalışmaktadır. Bu modellerden de yararlanılarak oluşturulan düzenleyici kurum, bilişim teknolojileri alanındaki düzenlemelerde doğrudan ya da dolaylı olarak taraf olan Radyo Televizyon Üst Kurulu, Telekomünikasyon Kurumu, Türk Telekom, Türk Standardları Enstitüsü arasındaki eşgüdümü ve onların da katkıda bulunmasını sağlamalıdır.

Ülkemizde bilişim teknolojileri alanında oluşturulacak bir mastır planı, bilişim teknolojilerinin gerektireceği altyapı, sunulabilecek hizmetler ve hizmetlerin sunulmasıyla değişecek ekonomik, toplumsal/kurumsal yapılanma ve düzenlemeler başlıkları ile birlikte elektronik imzanın yaygınlaşması ve bu konuda bir kültür ve bilinç oluşması ile ilgili bilgiler de içermelidir. Bu planda gerekli insan kaynağının yetiştirilmesi, teknoloji geliştirme / uyarlama, topluma yaygınlaştırabilme, uluslar arası rekabet gücü olan ürünler üretebilme gibi temel sorulara cevap üretebilecek yapabilirlik incelemelerine, diğer konular gibi elektronik imza konusu da dâhil edilmelidir.

5.11 Altyapı

Elektronik imza teknolojisini kullanabilmenin temel gereksinimi tabii ki bilgisayar kullanabilmektir. Bilgisayar kullanabilmek için de bilgisayara ihtiyaç vardır. Bu nedenle, bilgisayar sahipliği oranının yükseltilmesi konusunda projeler üretilmelidir. Benzerleri başka ülkelerde görülen, doğrudan ve düşük faizli kredi desteği ve vergi indirimi sağlanması gibi yöntemlerle bilgisayar sahipliği oranı arttırılmaya çalışılmalıdır[69]. Muhtarlar, halka en yakın devlet görevlisi olarak halkın E-Devlet uygulamalarını kullanmasında ön ayak olabilir. Mahalle muhtarının ofisinde sağlanacak bir E-Devlet erişim noktası sayesinde, halkın işlemlerini başka bir devlet dairesine gitmeden gerçekleştirmesi sağlanabilir.

E-Devlet hizmetlerinin vatandaşa yönelik olarak artması, vatandaşın da bu konuda istekli olmasına bağlıdır. Bununla birlikte E-Devlet uygulamalarını kullanmak istemeyen ya da kullanamayacak derecede engelli vatandaşlar için de çözümler oluşturulmalıdır. E-Devlet hizmetlerini kullanmak istemeyen kullanıcılar için normal yoldan (kâğıt tabanlı) işlem yapma faaliyeti devam ettirilmelidir. Engelli vatandaşlar yine muhtar ya da devletin oluşturduğu hizmet merkezlerindeki görevliler aracılığı ile bu hizmetlerden yararlanabilirler.

5.12 Elektronik İmza Uygulamaları

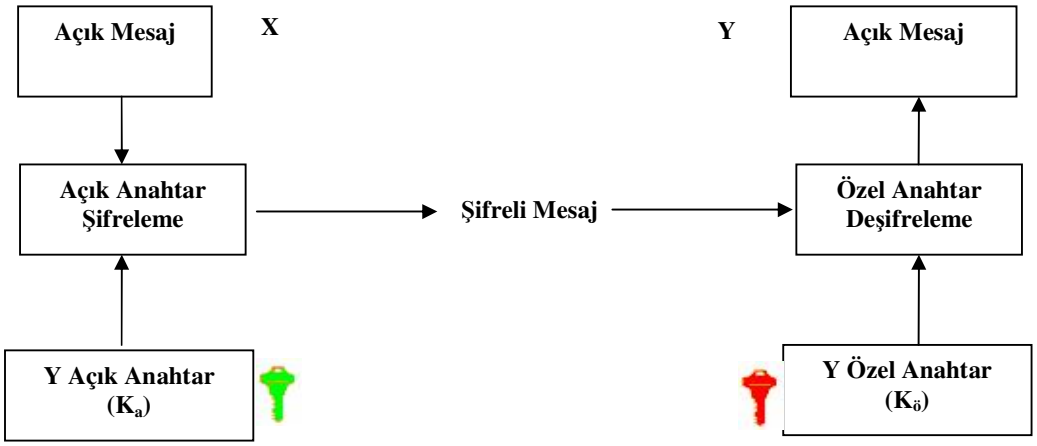
Elektronik ortamda, iletilerin güvenli olarak gönderilmesi ve alınması için farklı işlemler ve farklı yaklaşımlar kullanılmaktadır. Bu farklı yaklaşımlar aşağıda şekillerle açıklanmıştır[7].

5.12.1 Gizlilik, asimetrik uygulama

Burada amaç, iletişim sırasında bilginin bir saldırgan veya istenmeyen bir kişinin eline geçse bile kolaylıkla deşifre edilmesini önleme ve haberleşmenin gizliliğinden emin olunmasını sağlamaktır. Şekil 5.11 ‘de şifreleme ile sağlanan gizlilik unsurunun oluşturulması için takip edilen aşamalar aşağıda verilmiştir.

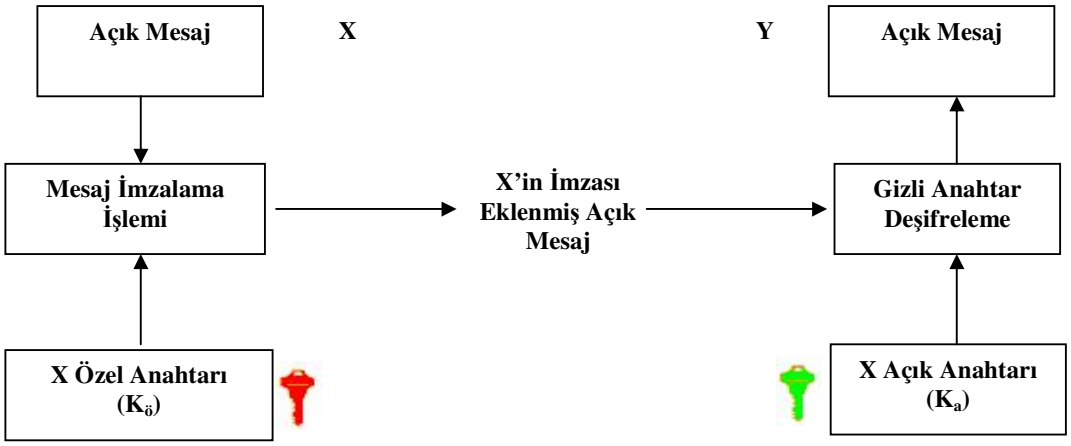
Bu işlemlerde;

1. X,Y’ye göndereceği mesajı, Y’nin açık anahtarı olan K_a ‘i kullanarak şifreler ve bunu Y’ye gönderir.
2. Y ise, mesajı aldığında, kendisine ait olan ve sadece kendine özel olan, gizli anahtar $K_ö$ ile mesajın şifresini çözebilir.



Şekil 5.11. Açık Anahtarlı Şifreleme

5.12.2 Kimlik doğrulama uygulaması



Şekil 5.12. Açık Anahtarlı Şifreleme (Asimetrik)

Burada yapılan işlem, aslında bir öncekinin tersidir. Takip edilmesi gereken basamak aşağıda verilmiştir.

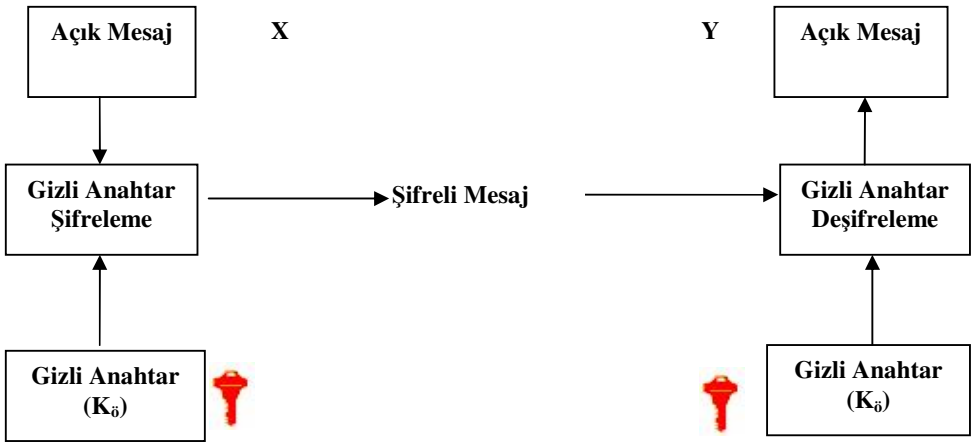
1. X, Y'ye göndereceği mesajı kendi özel anahtarı ile imzalar ve bu mesajı Y'ye gönderir.
2. X'den mesajı alan Y X'in açık anahtarını kullanarak mesajı doğrulama ve onaylama işleminden geçirerek imzalı mesajı deşifre eder. Bu işlem açık mesaj ile elde edilmiş olur.
3. Elde edilen mesaj sadece X'in açık anahtarıyla açılacağından, bu mesajın X'den geldiği doğrulanmış olur. Yani kimlik doğrulama işlemi gerçekleşmiş olur.

5.12.3 Gizlilik, simetrik uygulama

Bu uygulama, 5.12.1'deki uygulamaya çok benzemektedir. Şekil 5.13'de bu yapı verilmiştir. Önceki uygulamaların tersine burada tek anahtar kullanılmaktadır.

Bu yöntemde;

1. X,Y'ye gönderecek olduğu mesajı Y'nin de bildiği bir gizli anahtarı ($K_ö$) kullanarak şifreler ve bunu Y'ye gönderir.
2. Y ise mesajı aldığında, X'in ve kendisinin de bildiği gizli anahtar ile mesajın şifresini çözebilir.



Şekil 5.13. Gizli (Özel) Anahtarlı Şifreleme (Simetrik)

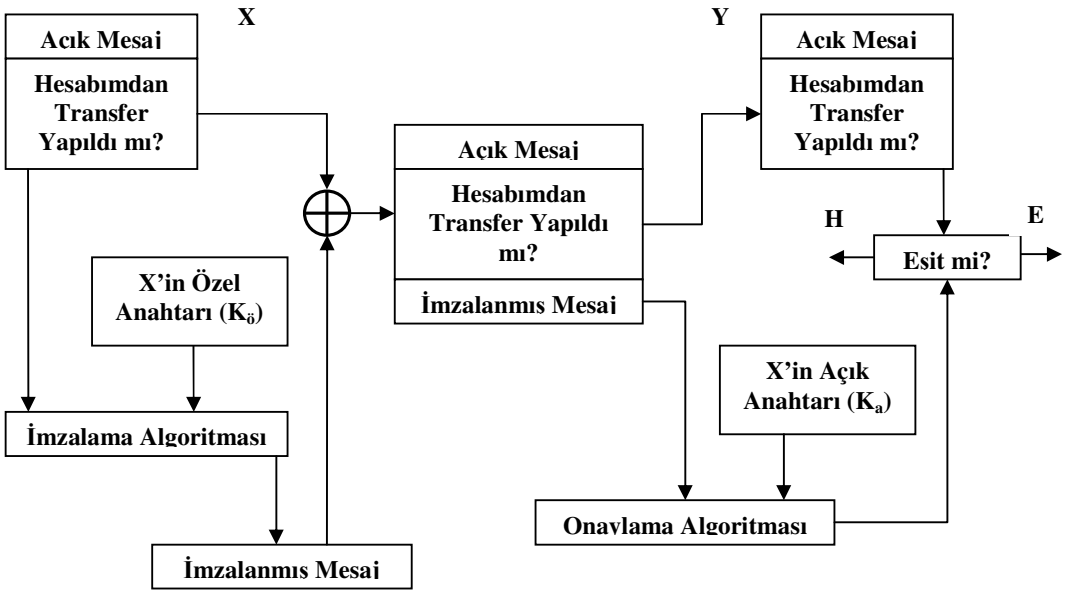
Bu şifreleme yaklaşımında yüksek derecede gizlilik sağlanmamaktadır. Fakat yüksek kapasiteye sahip dokümanların şifrelemesinde asimetrik şifrelemeye göre daha az işlem zamanına ihtiyaç duyulmasından dolayı tercih edilebilmektedir. Bu tür algoritmalarda, $K_ö$ 'yü bilen veya elde edebilen bir kişinin de mesajı deşifre etmesi mümkündür.

5.12.4 E-imza uygulama

İnternet ortamında güvenliği arttırmanın bir diğer adımı da, haberleşme anında aktarılan bilgilerin, belgelerin, mesajların doğru kişilere ulaştırıldığından veya doğru kişiler tarafından alındığından emin olunmasıdır. E-imza ile mesajı şifrelemek için de asimetrik algoritma kullanılmaktadır. Bu işlemde asimetrik şifreleme algoritmasına ek olarak, mesajın imzalanması için bir imzalama/onaylama algoritmasına ihtiyaç vardır.

Şekil 5.14'de verilen imzalama sürecini adımları aşağıdadır,

1. Mesajı göndermek isteyen X, mesajını oluşturduktan sonra bu mesajı kendi özel anahtarıyla ($K_{ö}$) imzalama algoritmasından geçirerek mesaj imzasını elde eder.
2. Bu işlem sonucunda oluşan mesaj imzası, orijinal açık mesajın sonuna mesaj imzası olarak eklenir.
3. Bu mesaj imzası, açık mesaja eklenerek Y'ye gönderilir.
4. Y mesajı aldığında, imzayı onaylamak için mesajın imzasını X'in açık anahtarı (K_a) ile onaylama algoritmasını kullanarak çözer. Eğer imzalı mesaj, X'in açık anahtarı ile açılırsa, Y, bu mesajın, gerçekten X'den geldiğinden emin olur. X'in açık anahtarı sadece, X'in özel anahtarı ile imzalanmış mesajların çözülebilecektir.
5. Bu işlem sonucunda, mesaj imzasının X'den gelip gelmediğinin kontrolü yapılır. Eğer mesaj açılıyorsa, bunun X'den geldiği tespit edilmiş olur. Eğer sağlanmaz ise mesajın X'den gelmediği anlaşılır.
6. İşlem sonucunda bir eşitlik sağlanırsa bu mesajın X'den geldiğini Y X'in mesajındaki eklentiyi açarak X hakkında detaylı bilgi edinebilir.



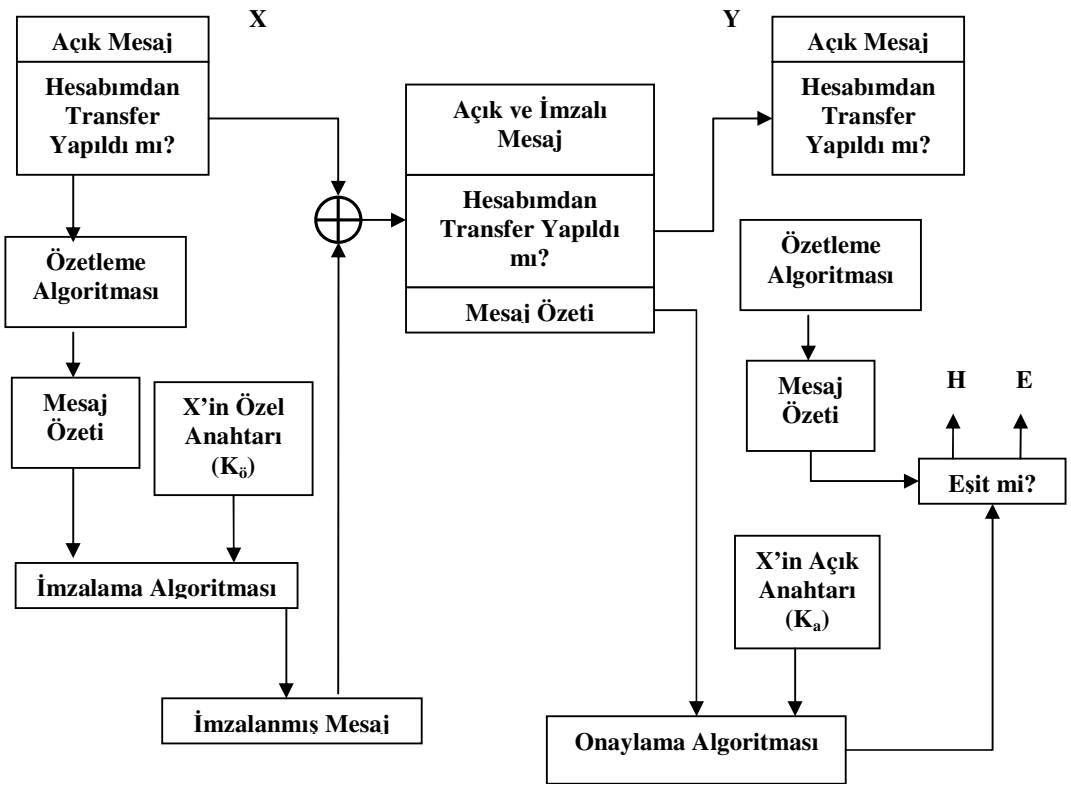
Şekil 5.14. Elektronik İmzalama Süreci

Şekil 5.14'de kimlik doğrulama ve açık mesajında eklenmesiyle bütünlük işlemleri sağlanmıştır. Fakat hem açık mesajın imzalanması ve aynı zamanda buna ek olarak karşı tarafa gönderilirken açık mesajda eklendiği için mesaj doğal olarak 2 katına çıkacaktır. Bunun sonucu olarak da mesajlaşma hızı düşmekte ve işlemler artmaktadır. Bu sorunu aşmak için özetleme algoritmaları kullanılmaktadır.

5.12.5 Özetleme algoritmalı e-imza uygulaması

5.12.4'teki uygulamada karşılaşılan sorunu aşmak için, mesajın tamamı yerine belirli uzunlukta oluşturulmuş, sadece o mesaja ait olan mesaj özeti kullanılır. Bunun olabilmesi içinde özetleme fonksiyonlarının kullanılması gerekir. Şekil 5.15'da özetleme algoritması eklenmiş e-imza yapısı gösterilmiştir. Özetleme algoritmaları, herhangi bir uzunluktaki veriyi alıp işleyen ve bu veriye özgü olan sabit uzunlukta bir değer çıkaran algoritmalara denir. Bu algoritmaların çıktısı ise, sabit uzunlukta bir değer olup, mesajın özeti olarak bilinir. Özetleme algoritmalı e-imza için takip edilmesi gereken aşamalar aşağıda verilmiştir.

1. Mesajı göndermek isteyen X, bir önceki uygulamaya ek olarak özetleme algoritmasından geçirmesi gereklidir.
2. Özet mesajı alındıktan sonra, bu mesaj X'in özel anahtarı ($K_ö$) ile imzalama algoritmasından geçirilerek X'in mesaj imzası alınır.
3. Bu işlem sonucu orijinal açık mesaja, imzalanmış özet mesaj ve X'in sertifika bilgileri eklenir.
4. İmzalanmış mesaj, Y'ye gönderilir.
5. Y bu mesajı aldığında, mesajı okuyabilmek için, mesajın imzasını X'in açık anahtarını (K_a) kullanarak açar ve mesajın X'den gelip gelmediğini kontrol eder. Eğer mesajın imzasını X'den gelen açık anahtar ile açarsa mesajın X'den geldiğine emin olur. Mesajın X'den geldiğine emin olduktan sonra, onaylama algoritmasından elde edilen özet değer ile Y'nin elde etmiş olduğu özet değer karşılaştırılır.
6. Bu işlem sonucunda da, orijinal mesajın değişip değişmediği anlaşılır. Eğer onaylama işlemi sonucu elde edilen özet ile açık olarak gelen orijinal mesajdan elde edilen özet aynı ise, mesajın yolda değişmediği anlaşılır.



Şekil 5.15. Özetleme Algoritmalı Elektronik İmzalama Süreci

5.12.6 Elektronik imzalı gizlilik

5.12.4 ve 5.12.5'te açıklana e-imza yaklaşımlarında gizliliğinde sağlanması için 5.12.1 ve 5.12.3'teki yaklaşımlarında kullanılması gerekmektedir.

5.12.7 İmzalama ve zaman damgaları

Genel olarak yapılan işlemlerde, yanlışlık olamaması için genelde tarih bilgisi kullanılmaktadır. Eğer bu kullanılmaz ise işlemlerde, haberleşmelerde problem çıkabilmekte, kişiler zarar görebilmekte ve kurumlarda ise kayıplar oluşabilmektedir.

Elektronik ortamlarda da bu tarz durumlarla karşılaşılmaması için, yapılan iş ve işlemlerde, tarih ve saat bilgilerinin MS'ler tarafından tutulması gerekmektedir. Eğer bu yapılmaz ise birçok problemle karşılaşılabilir ve kayıplar yaşanabilir. Zaman damgasının kullanılması ile karşılaşılabilecek, mahkemelik durumların sonuca bağlanmasında önemlidir ve diğer açıklara karşıda koruma sağlanmaktadır.

5.13 Değerlendirme ve Öneriler

E-imza oldukça yeni bir konu olduğu için dikkatli davranılmalıdır, aksi takdirde çeşitli riskler taşıyabilir. Güvenlik ön planda olduğu için önemi çok yüksektir. Bundan dolayı yazılım, donanım vb. hizmetler konusunda çok dikkatli olunması, bilinçli yaklaşılması ve hizmet kalitesinin doğru değerlendirilmesi gerekmektedir.

E-imza kâğıt ortamında yapılan belge yönetimine oranla elektronik ortamda yapılacak belge yönetimi çok daha etkin ve verimli olacaktır. Yapılacak bu uygulama ile düşük maliyetli iş ve işlemler, iş süreçlerinin iyileştirilmesi, iş gücünün doğru kullanımı, kağıt tüketiminde azalma, sahteciliğin azalması, haberleşme giderlerinde azalma sağlanarak etkinliğin ve verimliliğin çok büyük oranda artması sağlanmıştır.

Kurumlar veya özel firmalar tarafından geliştirilen elektronik imza oluşturma ve doğrulama yazılımlarının, mevzuatta belirtilen standartlara uygun olması sağlanmalıdır

Ayrıca kağıt üzerinde işleyen bir sistemi elektronik ortama geçirmek, elektronik ortamdaki bir uygulamaya elektronik imza ile ilgili özellikleri dâhil etmek ciddi yatırımlardır. Özellikle Elektronik İmza mevzuatında ayrıcalık tanınmış altı kurum (Türk Silahlı Kuvvetleri, Jandarma Genel Komutanlığı, Sahil Güvenlik Komutanlığı, Dışişleri Bakanlığı, Emniyet Genel Müdürlüğü ve Milli İstihbarat Teşkilatı), kendi Açık Anahtar Altyapısı sistemlerini kuracaklarından diğer kurumlara göre yapacakları yatırım çok daha fazladır. Bu ayrıcalık tanınan kurumlar örneğin kendi ESHS'lerini, Donanım Güvenlik Modüllerini, gerekli iletişim altyapısını kuracaklar, bu altyapıyı ayakta tutacak personeli eğitip istihdam edeceklerdir. Özellikle önümüzdeki dönemden itibaren geçilecek üç yıllık bütçe uygulaması nedeniyle yatırımlarda gecikmeler yaşanması olasıdır.

Yukarıda bahsedilen problemlere çözüm olarak elektronik imza ile ilgili yatırımlar ayrıcalıklı bir kapsamda düşünülmelidir. Özellikle e-imzanın gelişimi için 5.9, 5.10 ve 5.11'te bahsettiğimiz konular dikkate alınmalıdır.

Yasal geçerliliği bulunmasına rağmen halen yeterince yaygınlaşamamış olan e-imza için ülke genelinde bilinç ve bilgi birikimi oluşturulmalı ve planlı bir şekilde kurum ve kuruluşların e-imza projelerini hayata geçirmeleri sağlanmalıdır.

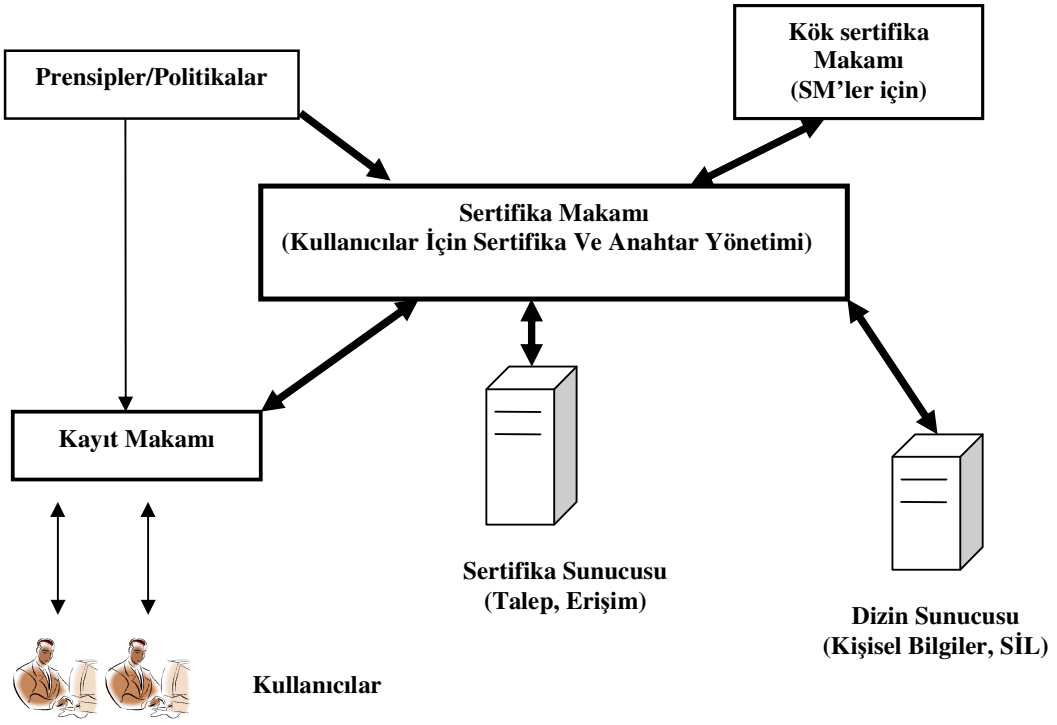
6. E-İMZA TEKNİK ALTYAPISI (AÇIK ANAHTAR ALTYAPISI(AAA))

Açık Anahtar Altyapısı (AAA, PKI – Public Key Infrastructure), veri/bilgi iletişiminde açık anahtarlı kriptografinin yaygın ve güvenli olarak kullanılabilmesini sağlayan ve birbirleriyle eşgüdüm içinde çalışan anahtar üretimi, anahtar yönetimi, onay kurumu, sayısal noterlik, zaman damgası gibi hizmetlerin tümünü kapsamaktadır. Tek anahtarlı simetrik şifreleme sistemlerinde, veriyi şifrelemek için kullanılan anahtar ile şifrelenmiş veriyi okuyabilmek için aynı anahtar kullanılmak zorundadır. Karşılıklı olarak şifreli haberleşebilmek için her iki taraf simetrik şiflemeleri birbirleriyle paylaşmak zorundadırlar. Açık anahtarlı şifreleme sistemlerinde bu durum farklıdır; tek anahtar değil de iki anahtar (açık anahtar ve özel anahtar) bulunmaktadır. Bu anahtarlar tek yönlü çalışmakta ve birbirlerini tamamlamaktadırlar. Açık anahtar (public key), veriyi şifrelemek; özel anahtar (private key) ise açık anahtar tarafından şifrelenmiş veriyi deşifre etmek rollerini üstlenmişlerdir. Özel anahtarlar sadece ait oldukları kişide bulunurlar. Açık anahtarlar ise adından da anlaşılacağı üzere açık (public) durumdadırlar ve dağıtımları açık olarak yapılır[70,71].

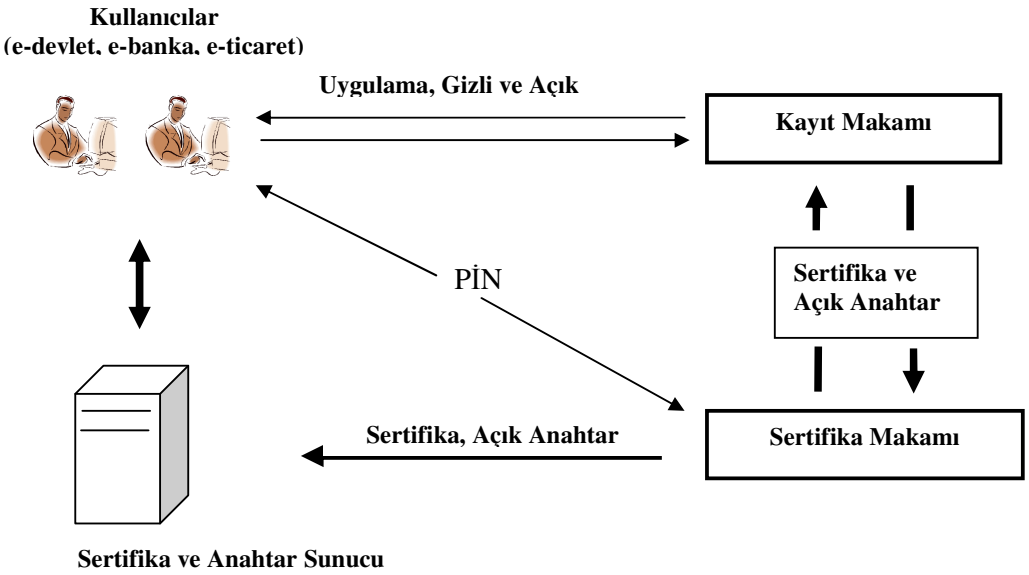
AAA; gizlilik (confidentiality), bütünlük (integrity), kimlik belirleme (authentication) ve reddedememe (non-repudiation) fonksiyonlarını kullanıcıların dijital sertifika kullanması yolu ile sağlar. Sertifika, dijital bir kimlik olduğu gibi aynı zamanda sahibine ait bilgiler ile gerekli algoritma anahtarlarını üzerinde bulundurur. Sertifikalar kişiye özeldirler. Güvenli bir şekilde ve güvenli ortamlarda muhafaza edilmeleri gerekmektedir. Şayet sertifikalar sabit disk gibi güvensiz ortamlarda muhafaza edilirse, kolayca değiştirilebilir ve başka kişiler tarafından kötü niyetli olarak kullanılabilirler. Bu, aslında AAA'nın bir güvenlik açığıdır. Bu açık, ancak depolama aracı olarak akıllı kartların kullanımıyla ortadan kaldırılır. Akıllı kartların kullanımı ve taşınması, yapısı nedeniyle oldukça kolaydır. Akıllı kartlar, bir kredi kartına benzerler. Akıllı kartlar, sahip oldukları güvenlik mekanizmaları sayesinde fiziksel, elektriksel ve kimyasal (kart içindeki bilgiyi çalma amaçlı yapılan tüm saldırılar) etkilere karşı kendilerini kilitleyebilirler. Kart üzerine gizli anahtarlar yüklendiğinde, kesinlikle bu bilgiler karttan okunamazlar ve kullanımları bir şifre ile korunur. AAA üzerinde çalışan elektronik imza ile internet üzerinde yapılan tüm elektronik işlemlerin (e-mail gönderimi/alımı, elektronik bankacılık uygulamaları, e-devlet platformları) ve gönderilen her türlü bilginin iletimi esnasında, bilgiyi gönderen kişinin kendisi olduğunun (authentication), gönderilen bilginin taşıma esnasında değiştirilmediğinin (integrity), bilgiyi gönderen kişinin bilgiyi gönderdiğini inkâr edemeyeceğinin (non-repudiation) garantisi ve güvenliği sağlanır Elektronik imzalar, güvenilir olarak kabul görmüş sertifika otoritesi denilen kurumlar tarafından dağıtılır ve takip edilir. Sertifika Otoriteleri, tüm ülkelerde kimlik üreten makamlar konumundadır[72,73].

AAA'nın yukarıda bahsedilen işlemleri gerçekleştirebilmesi için, güvenilir birimlere, şifreleme mekanizmalarına, güncel yaklaşımların ve donanımların kullanılmasına, farklı uzunluklarına sahip anahtarların seçimine ve bunların işleyişini sağlayan bilgisayar altyapısı ile uyulması ve denetlenmesi gereken uluslar arası kurullara, standartlara ve politikalara ihtiyaç vardır. AAA'yı daha iyi anlayabilmek için simetrik ve asimetrik şifreleme yöntemlerini iyi anlamak gerekir. Bölüm 4'de bu iki teknikten de ayrıntılı olarak bahsedilmiştir.

Bir AAA'da; makamlar(kayıt makamı, sertifika makamı, kök sertifika makamı), sertifikalar, depolama, arşivleme birimleri ve güvenlik prensipleri bulunur. Bu yapıda, kullanıcı sertifikaları, kullanıcı imza ilişkileri, açık ve nadiren de olsa gizli anahtarlar, sertifikalarla ilgili işlemler, sertifika ve dizin sunucuları yer almaktadır. Bir AAA'nın bu özelliklerinin birbiriyle uyumlu ve uluslar arası standartlara uygun olması gerekmektedir. Bu altyapıda, güvenilir makamlar tarafından anahtar ve sertifika oluşturma, onaylama, saklama, yayımlama, dağıtma, onayları geçici olarak durdurma ve sonlandırma işlemleri gerçekleştirilir. Şekil 6.1.'de verilen genel yapıda, sadece bir SM verilmiştir. Bir AAA'nın kurulabilmesi için birden çok sertifika makamı (SM), bu yapı içerisinde bulunmalıdır. Bir sertifika makamı, sayısal imzayı kullanan kişilerin açık anahtarlarını veya sertifikalarını onaylamak, verdiği onayları geri almak ve onayladığı sertifikaların, geri alınan onayların listesini, kullanıcıların zarar görmemesi için yayımlamak zorundadır.



Şekil 6.1. Genel Bir AAA Yapısı



Şekil 6.2. AAA Temel Bileşenleri Arası Haberleşme

Genel bir AAA içerisinde, temel bileşenler arası haberleşme, Şekil 6.2'de verilmiştir. Bu haberleşmedeki işlem sırası, aşağıda verilmiştir.

1. E-devlet, e-iş, e-ticaret veya bankacılık yapmak isteyen bir kullanıcı, kayıt makamına müracaat eder.
2. Kullanıcı, kayıt makamından gizli anahtarını almak için istenilen bilgi ve belgeleri, hazırlar ve KM'ye teslim eder.
3. Bilgi ve belgeler, KM tarafından güvenli bir şekilde SM'ye ulaştırılır. Belgeler kontrol edilir.
4. Kayıt makamında veya SM'de, o kullanıcı için bir açık ve gizli anahtar çifti üretilir.
5. Üretilen açık anahtar, bir sertifika ile ilişkilendirilir.
6. Kullanıcıya ait gizli anahtar ise, kullanıcıya, bir akıllı çubuk veya akıllı kart içerisine aktarılarak sunulur.
7. Güvenliği arttırmak için, kullanıcıya, geçici olarak (veya sürekli) bir PIN numarası da verilebilir veya bir PIN numarası belirlenmesi istenebilir. Bunu sebebi, kaybolma veya çalınma durumlarında gizli anahtarın direkt olarak kullanımını zorlaştırmaktır.
8. SM, verilen sertifikanın anahtar ve sertifika bilgilerini, sürekli olarak yayınlanması için, uygun bir sunucuya yönlendirir. Kullanıcıların kendileri veya iş ve işlem yapacağı diğer kullanıcıların, sertifika detayları hakkında bilgi alabilecekleri şekilde, kullanıcılara sunulur.
9. Problemli sertifikalar ise, sertifika iptal listelerinde (SİL) yayımlanır.

6.1 AAA'nın Oluşturulması

Böyle bir altyapı sitemini oluşturmak için, bir KSM' ye ve buna bağlı bir veya birden çok SM' ye ihtiyaç vardır. SM birimleri, daha öncede belirtildiği gibi kullanıcıların, açık anahtarlarını üzerinde tutmak, sertifikanın geçerliliğini kontrol etmek, gerekirse sertifikaları iptal etmek, yayımlamak, kaydını tutmak, onayladığı sertifikaları ve iptal listelerini (SİL)dağıtmak veya yayımlamak zorundadır. Bu işlemler belirli politikalar çerçevesinde gerçekleştirilir[7].

Her SM'nin, güvenlik politikası, kurulum sırasında belirlenir ve güvenliğin her zaman sağlanması gerekmektedir. Güvenlik politikalarının önceden belirlenmesi, daha sonra kullanıcılar arasında doğabilecek sıkıntıların ortadan kaldırılması açısından önemlidir. Güvenilir tek bir yetki biriminin olması, AAA'nın yönetilmesi ve çalışması için gerekmektedir. Bu güvenliğin oluşturulmasında; X.509 standardında sertifikaların oluşturulması ve saklanması için, bu standartta iletişim kurabilecek olan yazılımlar kullanılmalıdır. Hangi yazılım kullanılırsa kullanılsın, bu yazılımın, düzenli olarak kontrol edilmesi, test edilmesi ve verilerin yedeklenmesinin yapılması gerekir. Sertifika makamı sunucusu, alt kayıt makamlarından gelen bilgileri bünyesinde barındırır ve gerekli ise bunları ilgili sunuculara yönlendirir. Kullanıcılar haberleşecekleri diğer kişilerin açık anahtar ve sertifika bilgilerini sertifika ve anahtar sunucusundan bir defaya mahsus isteyebilirler. İmzalama için gerekli olan gizli anahtar, bir akıllı kart veya çubuk üzerinde saklanır. Bu kartı veya çubuğu kullanan yetkisi, karışıklığı engellemek ve güvenliği arttırmak için, tek bir kişide bulunmalıdır ve farklı kişilerle, asla paylaşılmamalıdır.

Genel olarak değerlendirildiğinde, bir AAA içerisinde, sertifika oluşturmak, yayımlamak ve bunun dağıtım altyapısını kurmak kolaydır. Fakat açık anahtar yapılandırılmasını oluşturmak zordur. AAA oluşturulurken, kullanıcı sayıları, tercih edilecek uygulamalar, mevcut kaynaklar, altyapının genişlemesi, oluşturulacak güvenlik politikaları ve en önemlisi, E-imza Kanunu ve yayımlanan Tebliğ, dikkate alınmalıdır. Bir AAA'da, pratik yerleşimi ve işleyişi sağlamak için, birçok bileşen ve hizmet bulunmaktadır. AAA'nın ve e-imza kullanımının yaygınlaşması, problemlerle ve risklerle mümkün olduğunca karşılaşılmaması, uygulamalara son derece iyi entegre edilmeleri, denetimlerin zamanında ve düzgün yapılması, bilgi güvenliği kavramlarının kullanıcılar tarafından anlaşılması ile mümkündür.

6.2 Makamlar

6.2.1 Sertifika makamı

Sertifika makamı (SM), açık anahtar altyapısında yer alan sertifikaları ve sertifika iptal listelerini üretmekle görevli olan merkezi birime verilen addır. Sertifika makamı, donanım ve yazılım parçalarından ve sistemi işleten kişiler ve kurallardan oluşan bir yapıdır. Bir sertifika makamını diğer sertifika makamlarından ayırt edici özellikleri; adı ve anahtar çiftidir (açık ve özel anahtardan oluşan)[7,19,73,74].

Sertifika makamının görevleri şunlardır:

- Kullanıcı kimlik bilgilerini doğru tespit etmek, özel anahtar bilgilerini, hem kullanım sırasında, hem de kullanımdan sonra gizli tutmak, kendi özel anahtarını saklamak ve korumak için yeterli önlemeleri almak
- Sertifika yayınlamak
- Sertifikaları yayınlamadan önce de içeriğin doğru olup olmadığını kontrol edilmelidir. Bu amaçla kullanıcının kimliği, şahsi bilgileri ve yetki seviyeleri tespit edilmelidir.
- SM yayınladığı tüm sertifikaların ve sertifika iptal listelerinin (SİL) kendi standart profiline uygun olmasını sağlamaktır. Farklı ya da eksik alanları olan sertifikalar yayınlamamalıdır
- Sertifika durum bilgilerini güncel tutmak ve sertifika iptal listeleri (SİL) hazırlamak
- Güncel sertifikaları ve SİL'leri isteyen kişilere sunmalıdır. Bu hizmeti verirken erişilebilirliğinin sürekli olması çok önemlidir
- Süresi dolan ya da iptal edilen sertifikaların arşivini tutmak

Sertifika makamının yayınladığı sertifikalarla ilgili olarak aşağıdakiler söylenebilir:

- Bir SM, kullanıcılar ya da diğer SM'ler için sertifika yayınlayabilir.
- SM tarafından yayınlanan sertifika içindeki bilgiler, doğruluğu onaylanmış bilgiler olmalıdır.
- Eğer sertifika başka bir SM için yayınlanmışsa bu diğer SM'nin yayınladığı sertifikalara güvenildiğini gösterir.
- SM her sertifikanın içine kendi ismini yazar ve sertifikayı kullanan kişiler bu ismi ve SM'nin sayısal imzasını kontrol ederek sertifikanın doğruluğunu kontrol eder.

Bütün bu görevleri aynı anda tek sistemle yerine getirmek zordur. SM temel görevi olan, kendi özel anahtarlarını saklamak ve korumak için fiziksel, süreçsel ve teknik bir takım kontroller kullanır. SM, diğer görevlerini aşağıda gösterilen AAA bileşenlerine aktarabilir:

- Sertifika bilgilerini doğrulayan ve kullanıcı kayıtlarını yapan: Kayıt Makamı
- Sertifika ve sertifika iptal listeleri dağıtımını yapan: Sertifika Deposu
- Uzun süreli arşivleme yapan: Arşiv Modülü

6.2.2 Kayıt makamı

Kayıt makamı (KM), sertifika makamı için sertifika başvurularını alır ve sertifika içine yerleştirilecek bilgilerin doğruluğunu kontrol eder. KM, bu bilgilerden bir sertifika isteği oluşturur. Kayıt makamı topladığı bilgileri SM'ye kendi sayısal imzasıyla imzalayarak iletir. Böylece SM sertifika isteğinin güvendiği bir kaynaktan gelip gelmediğini anlayabilir. Bu nedenle kayıt makamı kendi özel anahtarını çok iyi korumalıdır. Bir kayıt makamı birden çok SM için bu hizmeti verebilir[7,19,74].

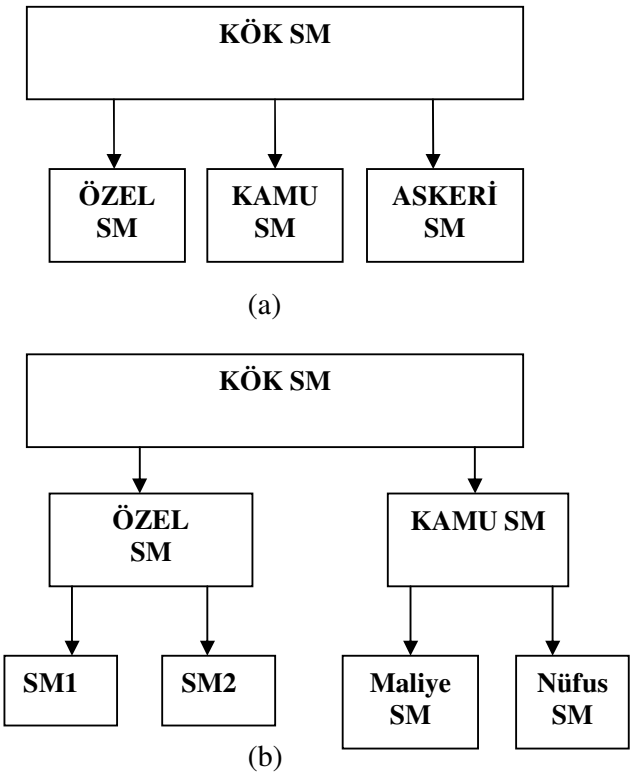
KM'nin SM ile çalışması genelde iki şekilde olur:

- KM sertifika isteği yapmadan önce gerekli bilgileri toplar ve doğruluğunu kontrol eder. Bu genelde KM' ye yapılan şahsi başvurularda kullanılan yoldur. Başvuran kişi kimlik ya da ehliyet gibi bir belge ile kim olduğunu KM' ye kanıtlar. Bu bilgilerle oluşturulan sertifika isteği SM' ye iletilir.
- Kişi sertifika isteğini elektronik ortamda yapar. Örneğin bir e-posta adresinin kendisine ait olduğunu iddia eder ve sertifika ister. SM bu isteği alır ve istek içindeki bilgileri doğruluğunu kontrol etmesi için KM' ye gönderir. KM onay verdikten sonra SM sertifika isteğini cevaplar.

6.2.3 Kök sertifikasyon makamı

KSM, AAA hizmetlerinin güvenli verilebilmesi için, en önemli ve en üstteki makamdır. Bu makamın güvenilir olması ve herkes tarafından güven duyulacak bir makam olması şarttır. SM'ler, sertifikalarını internet üzerinden bilgisayarına yüklerken, KSM'nin güvenilirliğini kabul ederek, işlem yapmaktadır. Sertifika ile birlikte gelen açık anahtar, öncelikle, sertifikasyon kurumunun (SM) kimliğini doğrulamakta kullanılır. Bu açık anahtar, sertifikasyon kurumunun dağıttığı sertifikaların da okunabilmesini ve böylece, bu sertifikaların, doğruluğunun kontrol edilmesini sağlar. KSM'ler, farklı ülkelerde farklı şekillerde yapılandırılmışlardır. Farklı KSM oluşumları Şekil 6.3'de verilmiştir. KSM'ler altında farklı SM'ler olabileceği gibi, SM'lere sertifika sağlayan farklı SM'ler de bulunabilir. Burada unutulmaması gereken konu, KSM'nin, bu yapılanmanın en tepesinde veya başında olmasıdır [7,74].

E-imza konusunda yasal düzenlemelerin güncellemesi, yapılana gelişmelere makamların uyumu, teknik ve hukuksal açıdan doğabilecek açıkların giderilmesi, bu makamların görevleri arasındadır.



Şekil 6.3. Farklı şekillerde KSM gösterimi

6.3 Sertifikalar

Sertifikalar, sayısal olarak oluşturulmuş kimliklerdir. Günlük hayatta kullanılan kimlik kartlarının, elektronik ortamdaki karşılığı olarak da bilinirler. Bu sertifikalar, kişilerin kimliğini ve söz konusu bilgiye veya hizmete erişim hakkını doğrulamak ve yetkilendirmek üzere geliştirilmiştir. Bilgileri şifrelemek ve şifrelenen bilgileri çözmek için kullanılan bir çift elektronik anahtarın biri ile kimlik bilgisini içerirler. Sertifikalar sayesinde kullanıcılar, haberleşme esnasında, bilgilerini güvenli bir şekilde iletebilirler. Sayısal sertifikada, kullanıcıya ait açık anahtar, kullanıcının adı, son kullanma tarihi, sertifikanın alındığı kurumun adı ve seri numarası gibi bilgiler bulunur[7]. Sertifikalar ve sertifika yönetiminde kullanılan sistemlerle ilgili bilgiler bölüm 7'de detaylı olarak açıklanmıştır.

6.4 Diğer AAA Bileşenleri

AAA'da, yukarıda anlatılan kısımlar dışında; zaman damgası, imza sunucusu, e-imza, şifreleme algoritmaları, inkâr edemezliği destekleme, anahtar yönetimi, dizin servisleri, yetkilendirme, anahtar üretimi tekrarı, anahtar yedekleme ve kurtarma, çapraz sertifikasyon, kullanıcı taraf yazılım işlemleri gibi bileşenler mevcuttur. Bu bileşenler, aşağıda açıklanmıştır[7].

Bir AAA ortamı, daha önce de vurgulandığı gibi, açık ve gizli anahtar çiftlerinin güvenliği kadar güvenlidir. Kullanıcıların sahip olduğu gizli anahtarların kaybolması, bozulması veya çalınması her zaman mümkündür. Bu nedenle, gizli anahtarlarının arşivlenmesi ve bu arşivlerden tekrar elde edilmesi mümkün olmaktadır. Bu anahtarı tekrar elde etme hizmeti ile güvenlik seviyesi azalmakta ise de, başlangıçta oluşabilecek sıkıntıları azaltmak, kayıpları önlemek, kullanıcılar arasında e-imza kullanma kültürü oluşturmak ve yaygınlaştırmak açısından önemlidir.

Zaman damgası, e-imza uygulamalarında önemli bir bileşendir ve güvenilen bir zaman bilgisi kullanılmasını sağlar. Zaman sunucusu, doğrulanabilir bir zaman damgasını oluşturan elektronik bir yapıdır. Veri ve dokümanlara eklenen zaman damgası ile bunların geçerli olduğu zaman aralığı belirlenir. Bu fonksiyonları içeren hizmet içinde, zaman damgası İstekleri, zaman damgası sertifikalarının doğrulanması, depolanması ve üretilmesi gibi fonksiyonlar bulunur. Bu hizmetler, kurulan bir AAA İçerisinde oluşturulup verilebileceği gibi güvenilir bir üçüncü-parti zaman damgası hizmet sağlayıcısından da alınabilir.

Bölüm 5'te de açıklandığı gibi, e-imza mesajların doğrulanması, bütünlüğü ve inkâr edilememe gibi unsurlar, AAA hizmetleridir. Bu hizmetlerle, mesaj özetinin çıkarılması ile bütünlük, açık ve gizli anahtarlar kullanılarak, kimlik doğrulama ve inkâr edemezlik sağlanabilmektedir. Bir ağ ortamında mesajların gizliliğini sağlamak için şifreleme yaklaşımları kullanılır. AAA'nın önemli hizmetlerinden birisi de, anahtar yönetimidir. Bu hizmet şifreleme anahtarlarının güvenli ve ölçeklenebilir olarak tutulmasından sorumludur. Bu hizmet, anahtarların üretimi, anahtarların ilişkilendirilmesi, dağıtılması, depolanması, geri alınması, yedeklenmesi, güncellenmesi anahtar erişim isteklerinin doğrulanması ve yönetim fonksiyonlarından oluşur.

Dizin servisleri ise, AAA'daki kullanıcıların, diğer kullanıcılar hakkında bilgi alabilmelerini sağlayan fonksiyonları içerirler. Bunun içinde, yeni sertifikaların ilanı, mevcut sertifikaların güncellenmesi, sertifika iptal listelerinin yayımlanması ve güncellenmesi, dağıtım, yedekleme, arama, sertifika isteklerinin karşılanması gibi fonksiyonlar bulunmaktadır.

6.5 AAA Mimarisi

Bir açık anahtar altyapısının sadece bir sertifika makamı barındırması şart değildir. AAA sistemlerinde genellikle birçok sertifika makamı bulunur ve bunlar kendi aralarında iletişimde bulunabilirler. Ayrıca farklı açık anahtar altyapılarına ait sertifika makamları arasında da iletişim ve güven mekanizması kurulması gerekebilir. Bütün bu ihtiyaçlardan dolayı değişik AAA mimari tasarımları yapılmıştır[7,19,74]. Bir AAA mimarisi incelenirken aşağıdaki sorulara cevap aranır:

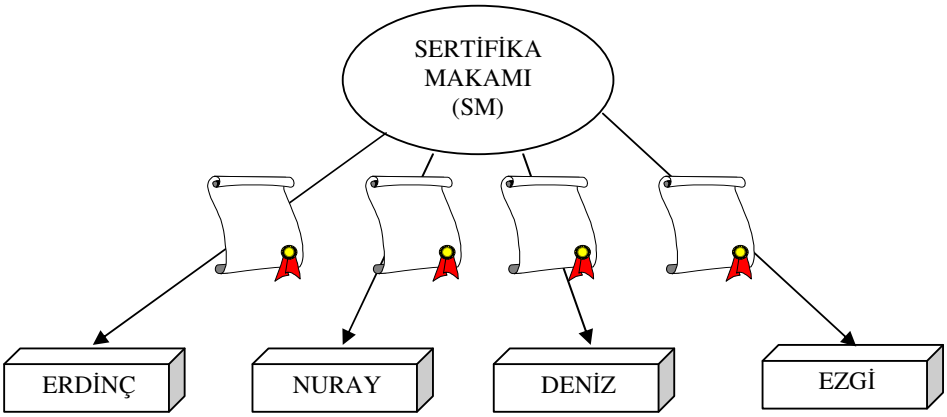
- Kaç tane sertifika makamı güvenilir kabul edilecek?
- Sertifika makamları arasında ne tür ilişkiler var?
- Yeni sertifika makamları sisteme ne kadar kolay (ya da zor) ekleniyor?
- Sertifikasyon yolunun oluşturulması ne kadar karışık? Sertifikasyon yolu kurulduktan sonra doğrulama ne kolaylıkta yapılabiliyor?
- Bir sertifika makamı kullanılamaz hale gelirse (güvenilirliğini kaybederse, ulaşılamaz duruma gelirse vb.) sistem bundan nasıl etkileniyor? Bu durumdaki bütün SM'lerin etkisi aynı mı olur

6.5.1 Basit mimariler

Basit mimariler aynı SM'den ya da çok az sayıda değişik SM'den sertifika alan kapalı bir grup kullanıcı için kullanılmaya uygun tasarımlardır. Bu yapıda SM'ler arasında ilişki yoktur. Bu yapıda SM'ye güven esas olup büyüme yapılamaz. Bundan dolayı da, SM, kullanılamaz hale gelirse, AAA yapısı çalışmaz hale gelecektir. Gerekirse SM'yi tekrar kurmak ve tüm sertifikaları yenilemek gerekecektir. Basit mimari yapılar "Tek SM" ve "SM Listesi" olarak iki grupta incelenebilir[7,19,74].

- Tek SM

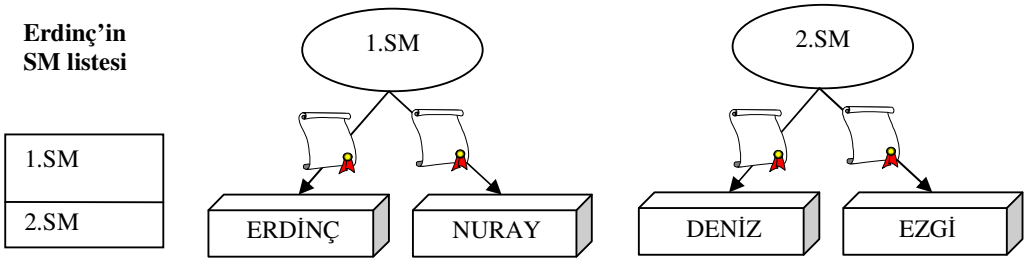
- Kullanıcılar sertifika veren SM'ye güveniyor.
- AAA'da sadece bir SM var ve yeni SM eklenmiyor.
- SM tek olduğu için diğer SM'lerle arasında bir güven ilişkisi kurma ihtiyacı yok.
- Sertifikasyon yolu tek sertifikayla kurulabiliyor.
- Genişleme ve büyüme kabiliyeti yok.
- SM kullanılamaz hale gelirse bütün AAA çalışamaz hale geliyor. SM' yi yeniden kurmak için bütün sertifikalar yenilenmeli.



Şekil 6.4. Tek SM Gösterimi

- SM Listesi

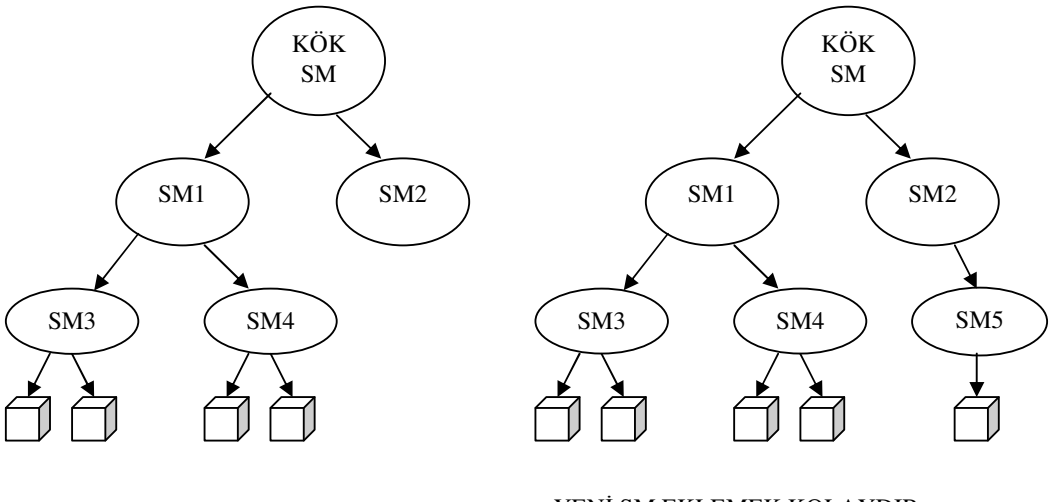
- Kullanıcı birden fazla SM'den gelen sertifikaları kullanıyor.
- Kullanıcı güvendiği tüm SM'leri kendi SM listesine alıyor.
- SM'ler arasında güven ilişkisi yok.
- Sertifikasyon yolu çok kolay kuruluyor.
- SM sayısı artarsa bakımı zorlaşıyor.
- Listeye eklenen SM'nin güvenilirliği belli değil.
- SM güvensiz hale gelirse bunu sadece kendisine kayıtlı sertifika sahiplerine duyurabilir. SM hangi kullanıcının SM listesinde olduğunu takip edemez.



Şekil 6.5. SM Listesi Gösterimi

6.5.2 Hiyerarşik mimariler

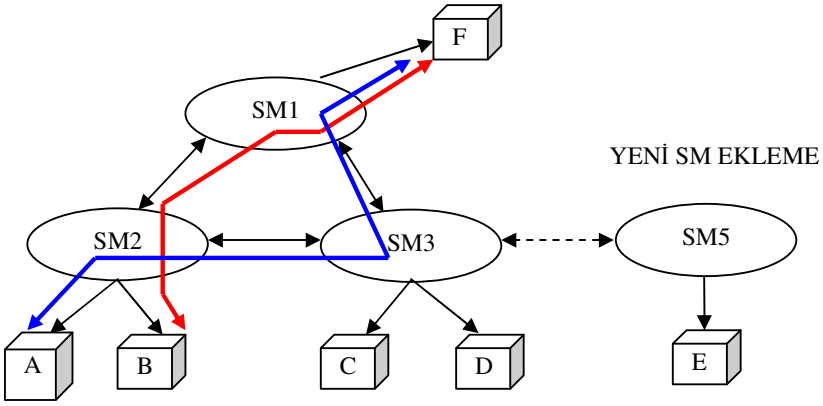
- Bu mimari tipi en yaygın kullanılan mimaridir.
- SM'ler arasında alt-üst ilişkisi vardır.
- Ağaç yapısının en üstünde yer alan SM'ye Kök SM denir.
- Hiyerarşide üstte yer alan SM kendi altındaki SM'lere sertifika verir.
- Sertifikasyon yolu oluşturmak kolaydır.
- SM'ler, altlarında yer alan SM'lerin yetkisini kısıtlayabilirler.
- SM kullanılmaz hale gelirse sadece onun altındaki sertifika sahiplerine yeniden sertifika üretmek yeterli olacaktır.



Şekil 6.6. Hiyerarşik Mimari Yapısı

6.5.3 Dağıtık mimariler

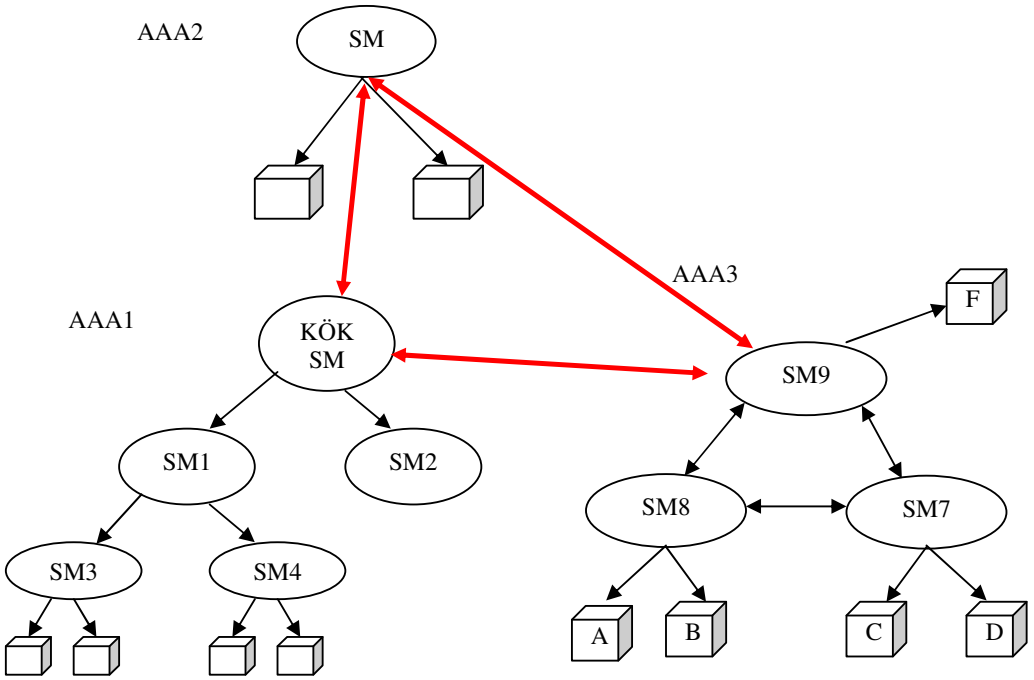
- Hiyerarşik mimarinin alternatifidir. Güven ağı olarak da adlandırılır.
- Birbirine güvenen iki SM karşılıklı sertifika verirler. Bu işleme çapraz sertifikasyon adı verilir.
- Yeni SM eklemek kolaydır.
- Sertifikasyon yolu oluşturmak zordur.
- SM'ler birbirlerinin yetkilerini kısıtlayamaz.
- Sertifikalar daha çok bilgi içerdiği için daha karışıktır.
- Kullanıcılar ilk önce kendi sertifikalarını üreten SM' ye ve onun üstünden eriştikleri diğer SM'lere güvenirler.
- SM özel anahtarını kaybederse sadece sertifika verdiği kullanıcılar etkilenir. En kötü durumda AAA yapısı bölünebilir.



Şekil 6.7. Dağıtık Mimari Yapısı

- Çapraz sertifikasyon

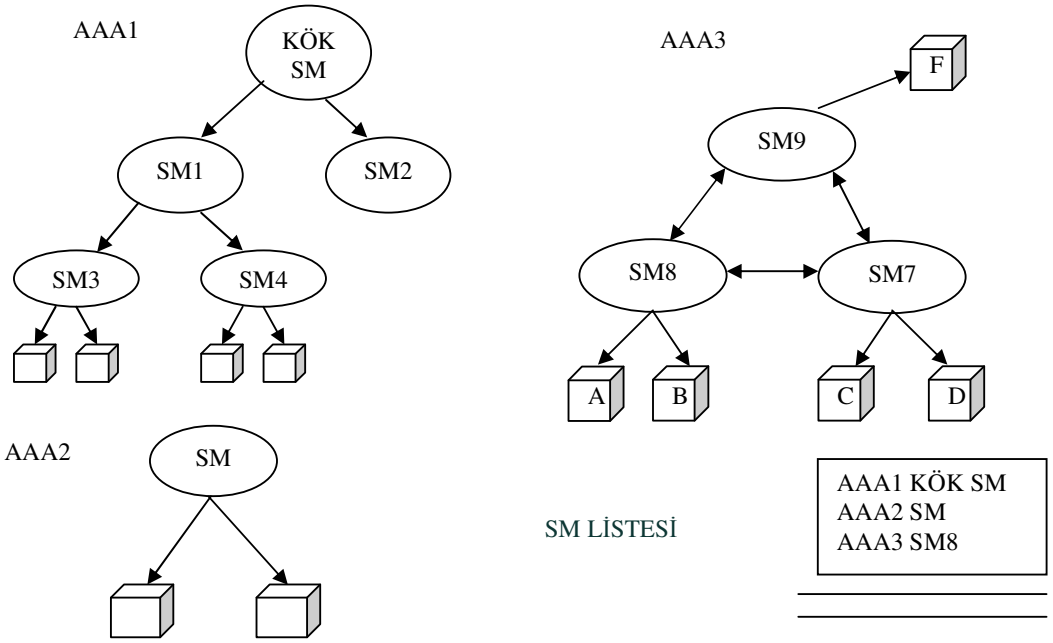
- AAA sistemleri arasında olur.
- Kullanıcı değil SM yöneticisi sorumludur.
- Sertifikasyon yolu çok karışık olabilir.
- Herhangi bir SM özel anahtarını kaybederse bu çapraz sertifikasyondaki tüm SM'lere duyurulur.
- AAA sistemlerinin sayısı çok değilse uygulanması tavsiye edilir.



Şekil 6.8. Çapraz Sertifikasyon Yapısı

- Genişletilmiş SM listesi

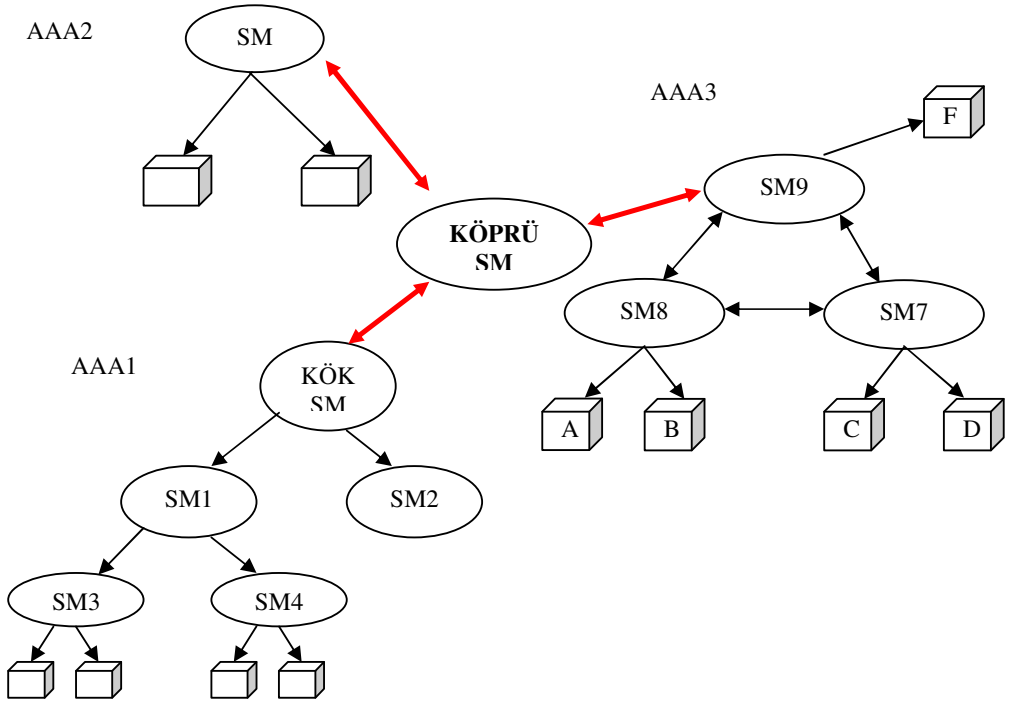
- SM listesine tek SM'ler dışında hiyerarşik AAA'nın Kök SM'si ya da dağıtık AAA'nın bir SM'si eklenebilir. Böylece basit SM listesindeki gibi listenin çok büyümesi önlenmiş olur.
- SM'nin özel anahtarı geçersiz olursa bu durumun duyurulması zordur.
- Sertifikasyon yolunun oluşturulması zordur.



Şekil 6.9. Genişletilmiş SM Listesi Yapısı

- Sertifikasyon köprüsü

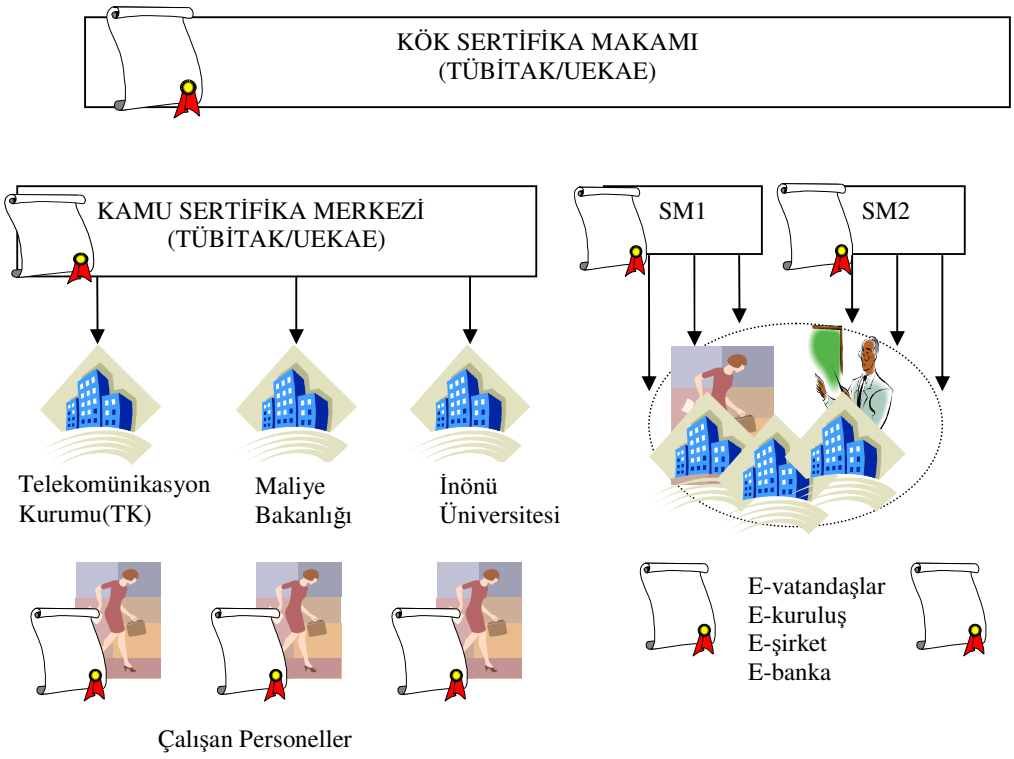
- Çapraz sertifikasyon çok sayıda AAA arasında olursa yönetimi zorlaşır. Yeni SM eklemek kolaydır. Sadece köprü SM ile sertifika değiş tokuşu yapılır.
- Köprü SM özel anahtarını kaybederse sistem birbirinden bağımsız AAA'lar haline gelir fakat yeniden normal duruma dönmek kolaydır.



Şekil 6.10. Sertifikasyon Köprüsü Yapısı

6.6 Türkiye'de AAA Yapısı

Ülke genelinde, kamunun koordinasyonun tek bir noktadan yapılmasını sağlamak İçin, Telekomünikasyon Kurumu tarafından önerilen, "kamu kurumlarının Kamu SM altında birleşmesi" görüşü, E-Dönüşüm Türkiye icra Kurulunda benimsenmiş ve 10 Haziran 2004'te (zaman ve kaynak israfının önlenmesi için). Kamu kuruluşlarının tamamının Kamu SM altında toplanması kararlaştırılmıştır. Bu genelgeye göre oluşturulan ülkemiz SM yapılandırma şeması Şekil 6.11'de verilmiştir.



Şekil 6.11. Türkiye SM Yapısı

Bu kararın yanında, ilgili tüm tarafların katıldığı açık ve şeffaf bir süreçte;

- Tüketici haklarını koruyan,
- Sürdürülebilir rekabeti sağlayan,
- Vatandaşa hizmeti esas alan (tek sertifika ile birden çok işlem),
- Kamu ve özel sektörün farklı gereksinimlerini karşılayabilecek esnekliğe sahip,
- Varolan hizmetlerin, elektronik ortama taşınmasını teşvik edecek,
- Yeni uygulamaların önünü açacak,

- Yeni yatırımları ve yabancı sermaye girişini özendirirken, mükerrer yatırımlar sonucu oluşacak kaynak israfını ve ülkemizin teknoloji çöplüğüne dönmesini engelleyecek,
- Birçok ülkenin kabul ettiği ortak standartları kullanacak,
- Teknoloji tarafsız olacak,
- Ulusal güvenlik gereklerini dikkate alacak ve
- Ülkemizde e-Dönüşümün gerçekleştirilmesine destek olacak düzenlemeler yapılması hedeflenmiştir, e-Dönüşüm icra Kurulu Kararı doğrultusunda, bu görüşleri, kamu kurumlarına aktaran bir Başbakanlık Genelgesi hazırlanmış ve Resmi Gazetede yayınlanmıştır.

Tüm kamu kurum ye kuruluşlarının kurumsal sertifika ihtiyacının karşılanması için, TÜBİTAK-UEKAE (Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü) görevlendirilmiştir. TSK, MİT, EGM, Dış İşleri Bakanlığı gibi istisnalar dışında, kamu kurum ve kuruluşları hiçbir şekilde kendi içlerinde elektronik sertifika hizmet sağlayıcısı kuramayacaklardır. Bu yapının uygunluğunun izlenmesi görevi ise, E-imza Kanunda da belirtildiği gibi, Telekomünikasyon Kurumu'na verilmiştir.

6.7 AAA'yı Değerlendirme Kriterleri

Başarılı bir AAA'yı değerlendirmede 6 ana faktör kullanılmaktadır. Bunlar;

- Esneklik,
- Kolay kullanılabilirlik,
- KSM/SM/KM güvenliği,
- Ölçeklenebilirlik,
- Düzenleme veya politika desteği
- Kullanılan standartlardır.

6.8 AAA Uygulama Aşamaları

AAA uygulama; kart ve okuyucu sistemler, sertifika yenileme, sertifika işlemleri ve iptaller, sertifika dağıtım ve kart basımı için yazılım ve donanımlar, sertifika makamı işlemleri, kimlik doğrulama ve yetkilendirme, gizlilik, veri bütünlüğü ve inkâr edememeyi gerektiren işlemlerdir. Uygulama aşamaları; karar, kurulum ve yönetim olmak üzere üçe ayrılır. *Karar aşaması,* mevcut durum analizi, bilgi güvenliği biriminin kurulması ve güvenlik politikasının oluşturulmasını içerir. *Kurulum aşaması,* SM'nin kurulması ve sistem içi kullanılan uygulamaların yenilenmesini içermektedir. *Yönetim aşaması* ise; İmza anahtarının güvenliği, yedekleme, sertifika dağıtımı ve SİL'in yayımlanması işlemlerini kapsamaktadır.

6.9 AAA Yazılımları

Bir AAA içerisinde, belirli bir zaman için anahtar çiftlerini ve sertifikaları oluşturmak ve bunları kontrol etmek için, çeşitli yazılımlar kullanılmaktadır. Günümüz tarayıcıları ve e-posta mesajlarının, sayısal sertifikalar ve "özenle korunan" anahtar çiftleriyle verilerin imzalanması, doğrulanması, şifrelenmesi ve şifrelerinin çözümü, mevcut yazılımlar kullanılarak, kolaylıkla yapılabilmektedir. UniCERT, Entrust, VeriSign, iTrus, eSign, ComSign, PT Trust, Trust Asia, DSV, CertPIus, IBM Trust Authority, RSA Keon, TürkTRUST, EŞYA (UEKAE), BİLTEN-ZEUGMA mevcut yazılımların bazılarıdır.

6.9.1 ESYA

Milli Açık Anahtar Altyapısı (MA3) Projesi kapsamında tübitak tarafından TSK için geliştirilen sertifika makamı yazılımının, ölçeklenebilirlik göz önünde bulundurularak, geliştirilen yeni sürümüdür. Elektronik sertifikalar ile ilgili yaşam döngüsü kapsamında elektronik sertifika üretme, iptal etme, askıya alma, askıdan indirme, sertifika iptal listesi yayınlama gibi hizmetleri sunar. Ölçeklenebilir mimari tasarım üzerinde Java Enterprise teknolojisi kullanılarak geliştirilmektedir.

ESYA, Kamu Sertifikasyon Merkezi'nin gelecekte ihtiyacı olabilecek ulusal çapta bir dağıtık kayıt makamı yapısını destekler niteliktedir. Milli yazılım oluşu ve sayılan teknolojik özelliklerinden dolayı Kamu Sertifikasyon Merkezi'nde sertifika makamı yazılımı olarak ESYA tercih edilmiştir. Başlangıçta Türk Silahlı Kuvvetleri, MİT ve Güvenlik Güçlerinin kullanımı için geliştirilen bu yazılım daha sonra, ülkemizdeki Kamu Kurum ve Kuruluşlarının Kamu SM altında toplanmasının, ülkemiz yapısına daha uygun olduğu kararlaştırılmış ve bu çerçevede Kamu SM'nin kurulması görevi ise TÜBİTAK/UEKAE' YE verilmiştir. TSK, MİT ve Dışişleri için geliştirilen bu yazılım Kamu SM kurulumunda kullanılmaktadır. Bu enstitünün görevi, "ulusal bilgi güvenliği ve ileri elektronik teknolojileri alanlarında, Türkiye'nin teknolojik bağımsızlığını sağlamaya katkıda bulunmak amacı ile faaliyetlerde bulunmak" ve vizyonu ise "uluslar arası düzeyde kabul görmüş altyapısı ve seçkin insan gücü ile temel bir çözüm ve bilim yeri olmak" olarak belirlenmiştir. Bu amaçla, bugüne kadar üzerine düşen görevi hassasiyetle yerine getiren ve ülkemiz milli bilgi ve bilgi sistemleri güvenliğine büyük katkı sağlayan UEKAE, bu görevi de başarıyla ve layıkıyla yürütmektedir[7,75].

6.9.2 Zeugma (TÜBİTAK/BİLTEN)

Zeugma, açık anahtarlı altyapının (PKI) temelini oluşturan sertifika üretim ve yönetim işlevlerini yerine getiren sertifika hizmet sağlayıcısı yönetim yazılımıdır. Yazılım, sertifika hizmet sağlayıcıların hiyerarşik düzende tanımlanmasına, sertifikaların üretiminde ve

yönetiminde izlenecek politikaların oluşturulmasına, sertifikaların içeriğinin ve kullanım alanlarının belirlenmesine imkân tanımaktır[76].

Genel Özellikler:

- Tümüyle Java'da geliştirilmiş, platform bağımsız bir yazılımdır.
- Web üzerinden gelen sertifika istek formlarını alıp değerlendirme seçeneği vardır.
- Anahtar çiftinin üretiminde RSA, DSA ve ECDSA algoritmaları kullanılır.
- Türkçe karakterlerin de dahil olduğu Unicode karakterlerini destekler.
- Üretilen sertifikaları ve sertifika iptal listelerini isteğe göre LDAP dizin sunucuya yazar

Uyumlu Olduğu Standartlar:

- X.509 v3, PKCS#1, PKCS#5, PKCS#7, PKCS#8, PKCS#10, PKCS#11, PKCS#12
- OCSP desteği
- FIPS 46-2 Veri Şifreleme Standardı
- FIPS 140-1 NIST 800-22: Rasgele Sayı Üretim Testi
- FIPS 180-1 Güvenli Mesaj Özeti Standardı
- FIPS 186-1 Elektronik İmza Standardı

LİDYA (Güvenliği Elektronik Belge Sistemi), e-ticarete olanak tanıyan bir mimari yapıdır. Kâğıt üzerinden maliyet ve zaman kayıplarına yol açarak yürüyen işlemlerin, güvenli elektronik ortamlarda hızlı ve hatasız yürütülmesini sağlar. Elektronik belgeler elektronik olarak imzalandığı ve şifrelendiği için bu belgelerin gizliliği, kaynağı ve belge üzerinde tahrifatın ortaya çıkarılması sağlanmış olur.

Genel Özellikler:

- Netscape Navigator ve MS Internet Explorer tarayıcıları ile uyumlu çalışır.
- İmzalı belgeler imzalarıyla birlikte veri tabanında tutulur.
- Bir belgede birden fazla imza bulunabilir.
- SSL üzerinden güvenli kullanıcı-sunucu bağlantısı kurar.
- Ağ üzerinden şifre gönderilmez, kullanıcı sunucuya "SSL Client Authentication" ile bağlanır.

Uyumlu Olduğu Standartlar:

- PKCS#7 Kriptografik Mesaj Yapı Standardı

DOSIA, Microsoft Windows işletim sistemi üzerinde dosya ve metin şifreleme, imzalama ve imza doğrulama yapabilen, akıllı kartlarla çalışabilme yeteneğine sahip, Microsoft Office ve Outlook eklentilerinin de imzalı ve şifreli olarak gönderilmesi ve alınabilmesini sağlayan, C# kullanılarak geliştirilmiş bir uygulama yazılımıdır[7].

AGORA, Anahtar Değişim Protokolü Standartları'na (Internet Key Exchange – IKE) uygun olarak, Java'da geliştirilmiş bir anahtar değişim protokolü yazılımıdır. Yazılımın platform bağımsız bir ürün olması, e-imza, ön paylaşımlı anahtarlı şifreleme ile kimlik doğrulama yöntemlerinin kullanılmasını desteklemesi bilinen özellikleridir.

6.10 AAA Fiyatları

Bugün, piyasada bulunan AAA yazılımlarının uç başına karşılaştırmalı ücretleri, Tablo 6.1.'de verilmiştir[77-80].

Firmalar/Uç	Baltimore($)	Entrust	IBM Trust	RSA
100	72.500	29.500	1.000	14.100
1.000	92.500	63.250	10.000	109.000
10.000	162.500	272.500	100.000	620.000
100.000	472.500	1.150.00	700.000	4.300.000
1.000.000	572.500	4.525.00	7.000.000	Pazarlığa

(a) Dünya Fiyatları

Firmalar/Uç Fiyatları	E-Güven(birim fiyat $)	TürkTRUST (birim fiyat)
>200.000	8.25	Yıllık fiyatının 177 YTL (KDV Dahil) olduğu bildirilmiştir. Uç birim sayısı arttıkça ücretlerini düşürebilecektir. Kurumsal fiyatlar KDV Dahil 210-235 YTL arasındadır.
<200.000	8.94	
<1 00.000	9.84	
<75.000	10.40	
<50.000	11.28	

(b) Türkiye Fiyatları

Tablo 6.1. AAA Yazılımları Fiyat-Uç Karşılaştırması

Ülkemizdeki fiyatları değerlendirdiğimizde, özele hizmet veren henüz 3 elektronik sertifika hizmet sağlayıcısı {e-Güven,e-Tuğra ve TürkTRUST} olduğundan, henüz bu konuda sağlıklı bir fiyatlandırma politikasının oluşmadığı söylenebilir. Bu sayının artması ile zamanla fiyatlandırma yerleşebilecektir.

ESHS	NES (Nitelikli Elektronik Sertifika)	SSL Sunucuları
Kamu-SM	39 YTL (Nes)	352 YTL
Türk Trust	310 YTL(Nes+Akıllı kart+Kart Okuyucu)	413 YTL
E-Güven	306 YTL(Nes+Akıllı kart+Kart Okuyucu)	
E-Tuğra	250 YTL(Nes+Akıllı kart+Kart Okuyucu)	

Tablo 6.2. Kurumların ESHS Fiyatları

6.11 AAA Donanımları ve Yazılımları

Açık anahtar altyapısı uygulamalarının en yaygın olanı elektronik imzadır. Elektronik imza için çeşitli araçlar kullanılır. Bu araçlar aşağıdaki gibi sınıflandırılabilir.

- Elektronik İmza Oluşturma Araçları
- Elektronik imza oluşturma yazılımları
- Elektronik imza oluşturma donanımları
- Akıllı kartlar
- Akıllı çubuklar
- Donanımsal Güvenlik Modülleri (Hardware Security Module: HSM)
- Akıllı kart okuyucular
- Elektronik İmza Doğrulama Araçları
- Elektronik imza doğrulama yazılımları

Elektronik imza araçları üreten firmalar çok çeşitli ve değişik özelliklerde ürünler üretmektedirler. Bu ürünlerin hepsi aynı türde elektronik imzalar üretmediği gibi güvenlik seviyeleri açısından da çok farklı olabilmektedir. Bu nedenle kurulan sistemlerde standartlara uygun çalışan yazılım ve donanım araçlarını tercih etmek gerekmektedir. Bazı durumlarda da – örneğin nitelikli elektronik imza kullanımı- kullanılacak araçların özellikleri yasal mevzuatla tespit edilmektedir.

6.11.1 E-imza yazılımları

Elektronik imza oluşturan ve doğrulayan yazılımlar genellikle standardı belirlenmiş bir elektronik imza biçimini kullanırlar. Elektronik imza biçimini tarif eden birçok standart vardır. Bunların başlıcaları aşağıda görülebilir:

- PKCS #7: Sayısal imzalama ve şifrelemede kullanmak üzere kriptografik yöntemleri destekleyen genel bir mesaj formatı tanımlar.

- CMS (Cryptographic Message Syntax): Elektronik imzalı ve/veya şifreli bilgilerin formatını tarif eden standart.
- ETSI CADES: CMS Advanced Electronic Signature (ETSI 101733 standardı) : ETSI tarafından yayınlanan ASN tabanlı elektronik imza standardıdır.
- ETSI XADES: XML Advanced Electronic Signature (ETSI 101903 standardı): ETSI tarafından yayınlanan XML tabanlı elektronik imza standardıdır.
- ETSI TS 101862 : (Qualified Certificate Profile) ETSI tarafından yayınlanan nitelikli elektronik sertifika standardıdır.

Ayrıca bu standartlarla beraber kullanılabilen birçok asimetrik kripto ve özetleme algoritması mevcuttur. Kullanılan yazılımın hangi programlama dili ile geliştirildiği, akıllı kartları nasıl kullandığı, hangi sertifika deposunu kullandığı gibi konular da çok önemlidir. Bu nedenle ideal bir e-imza oluşturma ve doğrulama yazılımında aşağıdaki özelliklerin bulunması gerekir:

- Seçilen elektronik imza standardını desteklemelidir
- Entegre edileceği sistemde kullanılabilecek bir programlama dili ile geliştirilmiş olmalıdır
- Akıllı kartlarla çalışabilmelidir
- Sertifika deposu kullanıcı tarafından kontrol edilebilmelidir
- E-imza oluşturma ve doğrulama sırasında X.509 ve RFC 3280'de anlatılan kurallara uygun olarak çalışmalıdır

E-imza yazılımları akıllı kartlarla çalışabilmek için başka yazılım kütüphanelerinden yararlanırlar. Bu kütüphaneler aşağıda listelenmiştir:

- Akıllı kart kripto yazılım kütüphanesi (Microsoft Crypto API uyumlu veya PKCS 11 standardına uyumlu)
- Kripto yazılım kütüphanesi (imza doğrulama için gerekli)
- Akıllı kart erişim yazılım kütüphanesi (PCSC vb uyumlu)

6.11.2 E-imza donanımları

Elektronik imza ile ilgili donanımlar aşağıdaki şekilde sınıflandırılabilir:

- Akıllı kartlar
- Akıllı çubuklar
- Akıllı kart okuyucular
- Donanım Güvenlik Modülleri (Hardware Security Module: HSM)

Bu donanımlarla ilgili detaylı bilgi takip eden bölümlerde verilmiştir[19].

- Akıllı kartlar

Şekil 6.12. Kredi kartı boyutunda akıllı kart

Şekil 6.13. Sim kart boyutunda akıllı kart

X.509 Sertifikalarını ve bunlarla bağlı olan anahtarları taşımak için kullanılan en yaygın ve güvenli cihazlar akıllı kartlardır (smartcard). Akıllı kartların genel sınıflandırması aşağıdaki gibidir:

Elektronik Devre Yapısına Göre:

- Bellek Kartları
- Güvenlik Donanımlı
- Güvenlik Donanımı Olmayan
- İşlemcili Kartlar
- Kripto İşlemcili
- Kripto İşlemcisi Olmayan

Veri Aktarım Tipine Göre:

- Temaslı
- Temassız
- İki Ara yüzlü (Temaslı+temassız)

Boyutuna Göre:

- Kredi Kartı Boyutunda (ID-1)
- SIM Kart Boyutunda (ID-000)

Açık anahtar altyapısı ve e-imza sistemlerinde kullanılabilecek akıllı kartlar kripto işlemcili sınıfta yer alırlar. Bu akıllı kartlar, programlanabilir alanları olan, dayanıklı, taşınabilir bilgisayarlar olarak tanımlanabilir. Akıllı kartlar veri güvenliği, kimlik gizliliği ve mobil kullanıcı ihtiyaçlarına sahip sistemlerde faydalıdır. Bu kartların başlıca teknik özellikleri şöyle sıralanabilir:

- Mikroişlemci olarak gerçeklenmiştir (8, 16 ve 32 bit modeller vardır)
- Bir işletim sistemine sahiptir (AKIS, CardOS, Multos vb)
- RSA, DSA, ECDSA gibi asimetrik algoritmaları çalıştırabilen yardımcı kripto işlemcisine sahiptir
- İşletim sistemi ve kripto kütüphanesi mikroişlemcinin ROM belleğinde saklanır
- Kripto anahtarlarını ve sertifikaları saklamak için yeterli büyüklükte EEPROM belleğe sahiptir (Tercihen 8Kb ve üstü)
- Özel anahtarlar kart içine yerleştirildikten sonra asla kart dışına çıkarılamaz.
- Kart içindeki özel anahtarla işlem yapmak için (örneğin e-imza oluşturmak) karta PIN kodu girilmesi zorunludur

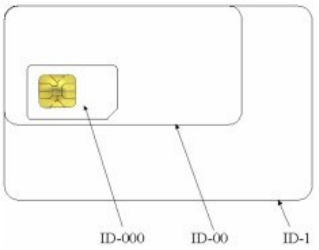
Bu tip akıllı kartlar aşağıdaki hizmetleri sunar:

- Kart üzerinde şifreleme ve şifre çözme
- Kart üzerinde imzalama ve imza onaylama
- Kart üzerinde özel ve açık anahtarların tutulması
- Kart içine bilgi yazabilme
- Kartın şifre ile korunması

Akıllı kartların özel (private) ve açık (public) alanları vardır. Özel alanda anahtar üretimi, imzalama, şifre çözme gibi işlemler yapılır, bu alana dışarıdan erişim yasaklanmıştır. Bu alanda yapılan işlemler Açık alana genel bilgiler yazılır. Akıllı kart yönetim yazılımı yardımıyla buradaki bilgiler görülebilir.

- Kart özellikleri

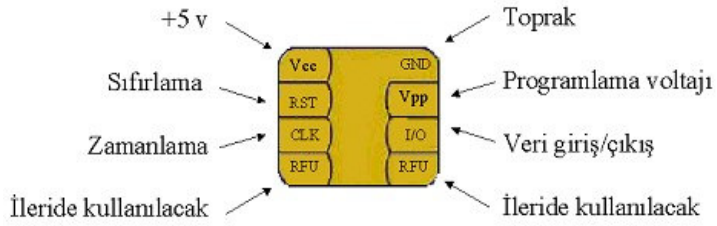
ISO 7816'da verilen kart formatları aşağıdaki şekilde ve tabloda verilmiştir.



Format	Genişlik	Yükseklik	Kalınlık	Köşe Yarıçapı
ID-1	85,6 mm	54 mm	0,76 mm	3,18 mm
ID-00	66 mm	33 mm	0,76 mm	3,18 mm
ID-000	24 mm	15 mm	0,76 mm	1,00 mm

Tablo 6.3. ISO 7816'da Verilen Kart Formatları ve Şekli

Kart üzerinde yer alan temas noktaları ve açıklamaları aşağıda verilmiştir.



Şekil 6.14. Kart Üzerinde Yer Alan Temas Noktaları Ve Açıklamaları

- Akıllı çubuklar

Şekil 6.15. Akıllı Çubuklar

Akıllı çubuklar, akıllı kartlarla aynı teknik özellikleri taşıyan fakat bilgisayarlara USB kapısından bağlanan cihazlardır. Yaygın olarak USB Token adıyla da anılırlar. Aslında akıllı çubuklar akıllı kart mikroişlemcisinin ve kart okuyucusunun bir araya getirildiği cihazlardır. Bu nedenle kullanılmaları için akıllı kart okuyucusuna gerek duyulmaz fakat maliyet olarak akıllı

kartlardan 4-5 kat daha pahalıdırlar. Ayrıca bu tür cihazlarda kriptografik anahtarların ve sertifikaların saklanması için kullanılan EEPROM bellekler fiziksel olarak daha büyüktür. Bu nedenle akıllı çubukların içindeki kritik bilgilerin izinsiz olarak okunmasını hedefleyen saldırılar kolayca gerçekleştirilebilmektedir. Akıllı çubuklarla ilgili olarak yararlar ve sakıncalar aşağıda listelenmiştir.

Üstünlükleri

- Ayrı bir kart okuyucuya ihtiyaç duyulmaması
- Kolay taşınabilmesi
- Fiziki olarak dış etkilere daha dayanıklı olması

Zayıf Yanları

- Akıllı kartlara kıyasla 4-5 kat pahalı olması
- Güvenlik açısından akıllı kartlara göre çok daha zayıf olması
- USB uçları çok fazla takma ve çıkarma işlemi sonucunda kısa sürede bozulabilmektedir
- Akıllı çubuk üzerine cihazın kime ait olduğunu gösterecek bir bilgi yazmak çok zordur (Farklı kişilerin akıllı çubuklarını ayırt etmek çok güçleşmektedir)

Yukarıda belirtilen sakıncalar nedeniyle akıllı çubukların kullanımı e-imza açısından çok faydalı görülmemektedir. Fakat yukarıda belirtilen yararları taşıyan akıllı çubuk şeklindeki kart okuyucuların kullanılması pratikte uygulanabilecek bir çözüm gibi gözükmektedir.

- Akıllı Kart Okuyucular

Akıllı kartlar düşük kapasiteli birer bilgisayar olarak nitelendirilebilir. Bu kartların kendi enerji kaynakları olmadıkları için ancak bir okuyucu terminale bağlanarak kullanılabilirler. Bu terminallere akıllı kart okuyucu adı verilir. Akıllı kart okuyucuların bağlandıkları bilgisayarda kullanılabilmesi için sürücü yazılımlarının o bilgisayar yüklenmesi gerekir. Değişik akıllı kart okuyucu tipleri aşağıda anlatılmaktadır.

- Masaüstü Akıllı Kart Okuyucular

Şekil 6.16. Masaüstü Akıllı Kart Okuyucu

Bu kart okuyucular en yaygın kullanılan modellerdir. Kredi kartı boyutundaki akıllı kartlarla kullanılırlar. Bilgisayara USB veya seri bağlantı ile bağlanırlar. Üzerinde yer alan ışık sayesinde kart ile işlem yapılıp yapılmadığı gözlenebilir.

- Tuş Takımlı Kart Okuyucular

Şekil 6.17. Tuş Takımlı Kart Okuyucu

Bu tip okuyucular akıllı kart parolasını kendi üzerlerindeki tuş takımı aracılığıyla alabilirler. Böylece kart parolası başka bir cihaza (örneğin bilgisayara) iletilmez. Bu yöntem diğer okuyuculara göre daha güvenli çalışmasını sağlar. Bazı modeller tuş takımının yanı sıra LCD ekran da barındırır. Bilgisayara USB veya seri bağlantı ile bağlanırlar.

- Akıllı Çubuk Şeklinde Kart Okuyucular

Şekil 6.18. Akıllı Çubuk Şeklinde Kart Okuyucu

Bu tür kart okuyucular USB kapısından bilgisayara bağlanır ve SIM Kart boyutundaki akıllı kartlarla çalışırlar. Taşıdıkları akıllı kart nedeniyle akıllı çubuklardan daha güvenlidirler. SIM kart üstündeki plastik alan sınırlı da olsa bu bölgeye kart sahibi ile ilgili bazı bilgiler sığdırılabilir. Sadece kart okuyucu olduğu için masaüstü kart okuyucularla aynı fiyat aralığında temin edilebilmektedir.

- PC Card Şeklinde Kart Okuyucular

Şekil 6.19. PC Kart Şeklinde Kart Okuyucu

Genellikle bu okuyucular taşınabilir bilgisayarların (notebook, laptop vs) PCMCIA yuvalarına takılarak kullanılır. Taşınabilir bilgisayarlar ile kullanımı pratiktir.

- Klavye ile Bütünleşik Kart Okuyucular

Şekil 6.20. Klavye İle Bütünleşik Kart Okuyucu

Bu tür okuyucular bilgisayarlar için üretilen klavyelere bütünleşiktir. Bu tip klavyeler normal klavyelerden daha pahalıdır. Eğer klavyedeki tuşlar bozulursa kart okuyucu kısmı sağlam bile olsa klavyenin değiştirilmesi gerekir; bu da maliyeti yükseltici bir faktördür.

- Disket Sürücü Şeklinde Kart Okuyucular

Şekil 6.21. Disket Sürücü Şeklinde Kart Okuyucu

Bu tür okuyucular bilgisayarları 3.5" veya 5.25" genişleme yuvasına monte edilir ve bilgisayarın ana kartına bağlanır. Mevcut bilgisayarlara takılması ayrı bir işgücü gerektirdiği için çoğu kişi tarafından kullanışlı bulunmamaktadır.

- Donanım güvenlik modülleri

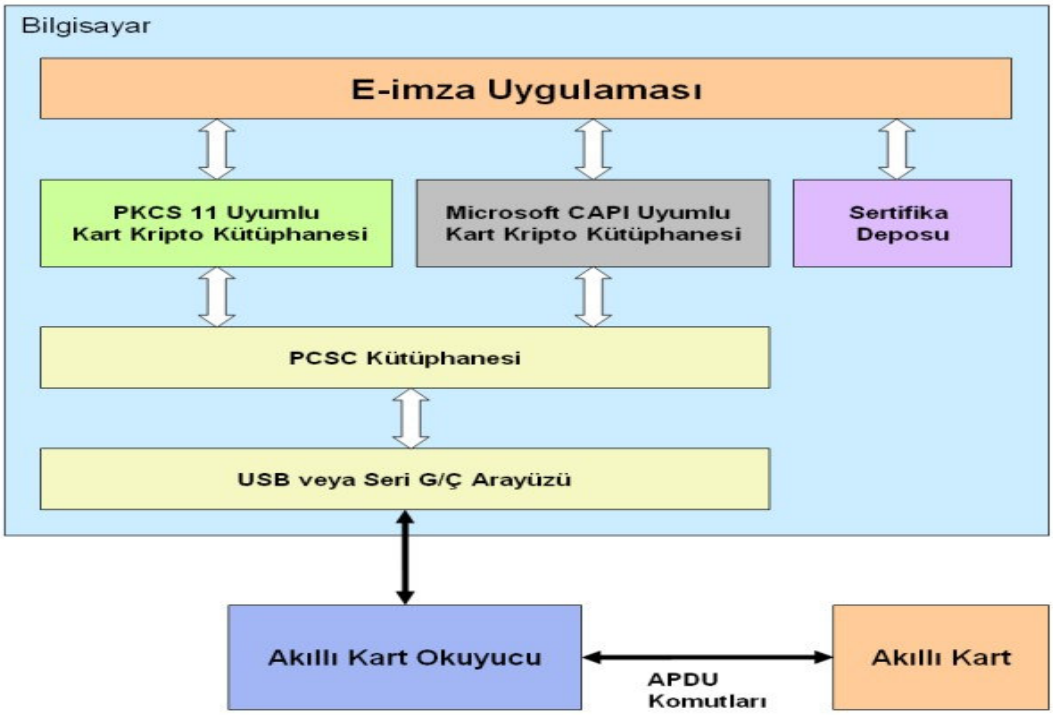
Donanım güvenlik modülleri çok yüksek kapasiteli akıllı kartlar gibi iş gören özel donanımlardır. Bu tür cihazlar da akıllı kartlar gibi kriptografik anahtarların saklanması ve cihaz vasıtasıyla kullanılması işine yararlar. Çok özel donanımlar oldukları için maliyetleri oldukça yüksektir. Bu cihazlar hem daha uzun anahtarlar kullanılmasına (4096 bit RSA gibi) yarar hem de çok yüksek performansla kripto işlemi yapabilirler (bazı modellerde saniyede 400 adet 1024 bit RSA işlemi gibi). Donanım güvenlik modülleri İngilizce HSM (Hardware veya Host Security Module) adıyla tanınır.

Donanım güvenlik modülleri iki temel tipte yer alır:

- Adanmış modeller: Bu modeller sadece bir bilgisayara bağlı olarak çalışır. PCI kart şeklinde veya bilgisayardaki bir SCSI kontrol kartına bağlana harici cihaz şeklinde olan modeller vardır.
- Ağ modelleri: Bu modeller kendi başlarına çalışırlar ama bir ağ ara yüzüne sahiptirler. Genellikle bir yerel alan ağı (LAN) üzerinde çalışan birden fazla bilgisayara tarafından kullanılırlar

- İşletim Sistemleri ile Uyum

Akıllı kartların ve kart okuyucuların işletim sistemleri ile beraber çalışabilmesi için aşağıdaki çizimde gösterilen mimariye benzer bir yapı kullanılır.



Şekil 6.22. Kart Okuyucu Çalışma Şekli

Bir akıllı kartın işletim sisteminde kullanılabilmesi için aşağıdaki yazılımların yüklenmiş olması gereklidir:

PKCS 11 Uyumlu Kütüphane: Bu kütüphane tipi genellikle açık kaynak kodlu ürünlerin akıllı karta erişim için tercih ettikleri kütüphanedir. Windows işletim sistemi dışındaki işletim sistemlerinde çok yaygın kullanılır.

Microsoft CAPI Uyumlu Kütüphane: Bu tip kütüphane Microsoft Windows işletim sistemi üzerinde kullanılmak üzere tanımlanmış bir standarda uygun yazılmıştır.

Akıllı Kart Okuyucu Sürücüsü: Bilgisayara bağlanan tüm cihazlar gibi akıllı kart okuyucu için de bir sürücü yüklenmesi gereklidir.

İşletim Sistemi Akıllı Kart Bileşenleri: Windows işletim sisteminde ve çoğu Linux dağıtımında hazır olarak gelen akıllı kart erişim altyapısı kullanılır. Yaygın olarak PCSC standardı kullanılır.

6.12 AAA Hizmeti Sunan Şirketler

Bugün için, ülkemizde AAA hizmetlerini sunabilecek üç şirketin bulunduğu bilinmektedir. Bunlardan ilki kanunla da bu görevi üstlenen TÜBİTAK-UEKAE, diğerleri ise e-Güven, e-Tuğra ve TürkTRUST şirketleridir.

6.13 AAA Uygulamalarında Karşılaşılabilecek Problemler

AAA gibi, yeni teknolojilerin kullanımı her ne kadar kullanıcılara güvenli bir ortam sunmuş olsa da, yeni kullanılan her teknolojide olduğu gibi, birçok problemle karşılaşılabileceği unutulmamalıdır. AAA ve sertifika yönetimi ile birçok problem aşılmış olsa da yine de bazı noktalarda problemler doğabilecek ve kimi soru işaretleri oluşabilecektir. Bir AAA uygulamasında[7];

- Kime güvenmeliyim? Niçin?
- Anahtarım kopyalanabilir mi?
- Doğrulamayı yapan bilgisayar güvenli mi?
- Benim İsmimde başka bir kullanıcı var mı?
- SM' ye gerçekten güvenmeli miyim?
- Kullanıcı olarak güvenlik tasarımının bir parçası mıyım?
- Bu teknolojiyi kullanmak için güvenlik uzmanı mı olmalıyım?
- Bu sistemlerin hiç açıklan yok mu?

Gibi, oluşabilecek daha birçok soru sıralanabilir. Teknolojilerdeki gelişmeler ile yukarıda sıralanmış olan soruların birçoğu her geçen gün ortadan kaldırılmakta ise de, çok az da olsa, bazı problemler oluşabilecektir. Bunlar:

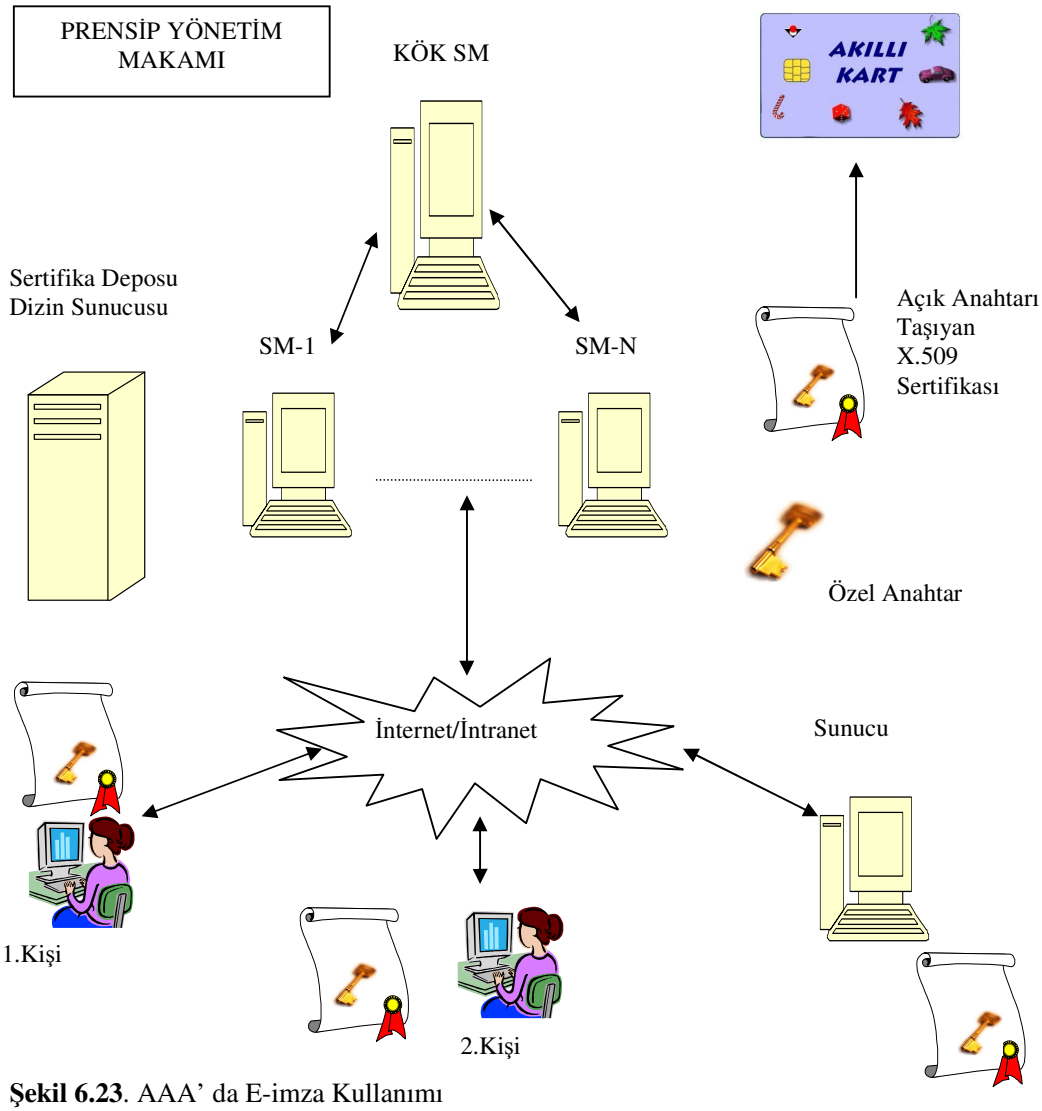
- Bilgi ve bilgisayar sistemleri güvenliğinin bilinmesi zorunluluğu,
- Kayıt esnasında yaşanabilecek zorluklar,

- Ücretli olarak sertifikaların sunulması, sertifikaların tekrar üretilmesinde karşılaşılan problemler,
- Hizmet alınacak makamlara güven sorunu,
- İptal edilmiş sertifikaların zamanında öğrenilememesi,
- Sertifika iptalinin getirdiği ek yükler ve zaman kaybı,
- Uygulamalarda yaşanabilecek, fakat o ana kadar karşılaşılmayan problemler,
- Sunucu bilgisayarların, sistemler arası bilgi alışverişini otomatik olarak yapmalarından dolayı karşılaşılabilecek sorunlar olarak sıralanabilir.

6.14 AAA İçerisinde E-İmza Kullanımı

Bölüm 5'te, e-imzanın farklı uygulamaları verilmiştir. Bu bölümde ise, AAA içerisinde e-imza kullanımı detaylı olarak açıklanacaktır. Şekil 6.23'de genel bir AAA uygulamasında e-imza kullanımının nasıl yapılması gerektiği verilmiştir. Bu yapı içerisinde, N adet SM, Prensip Yönetim Makamının belirlemiş olduğu politikalara göre, sertifika hizmet Bağlayıcılığı görevlerini yerine getirmektedirler. Bu yapı içerisinde, 1.Kişi, 2.Kişi ve Sunucunun, kullanıcılar olduğunu düşünelim. Bu kullanıcıların özel (gizli) anahtarları, akıllı kartlar veya güvenli sunucular üzerinde bulunabilmektedir[7].

E-imza almak isteyen bir kullanıcı, başlangıçta bir KM'ye müracaat edip kendini elektronik ortamda tanıtacak olan sertifikasını, yani özel anahtarını almak zorundadır. Bu anahtarı alırken, bu özel anahtara bağlı olarak üretilen açık anahtar ve bu açık anahtarla özdeşleşen veya ilişkilendirilen bir sertifika üretilir. SM'ler, bazı durumlarda, kullanıcılarla, KM'Ier aracılığıyla irtibata geçerken, bazı durumlarda da, direkt olarak kendilerine müracaat edilmesini isteyebilirler.



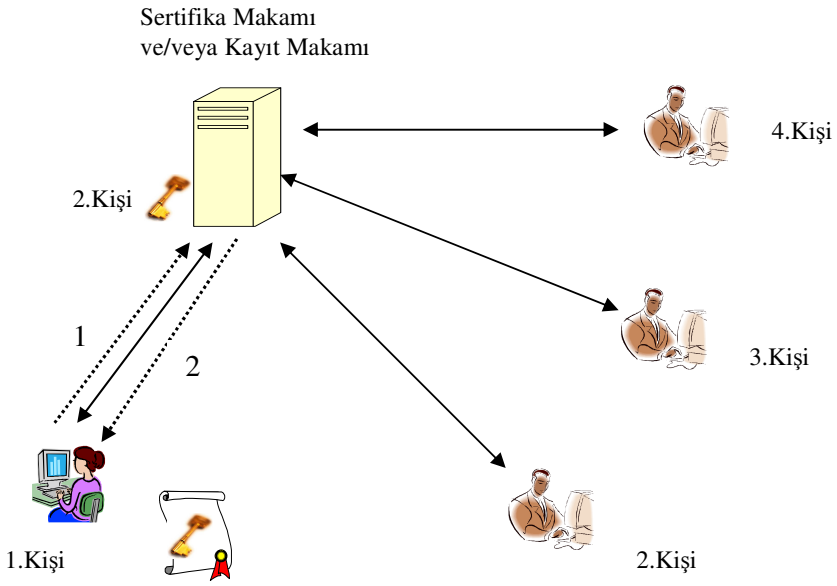
Şekil 6.23. AAA' da E-imza Kullanımı

Gerekli olan yöntemler aşağıda sırasıyla anlatılmıştır.

1. 2.kişi, 1.kişi'nin açık anahtarını içeren sertifikasını, SM bünyesinde bulunan sertifika deposundan sorgular.
2. Açık anahtarı bulan 2.Kişi, 1. Kişi'nin sertifikasını, kendi bilgisayarına, o sunucudan indirir. Bu İşlem, başlangıçta bir kez yapılır ve 1.kişi'ye ait olan sertifika daha sonra, tekrar sertifika sunucusuna gerek duyulmadan kullanılabilir. Burada dikkat edilmesi gereken husus ise, 1.Kişi'ye ait olan sertifikada bir problem oluşmuş ve bu SM'de o kullanıcıya ait olan sertifikayı, SİL'de yayımlamış ise, geçersiz olan bir sertifikayla işlem yapılmasının önüne geçilmesidir. Bu durumda, sertifikanın geçerli olduğu sorgulanarak teyit edilmelidir. Bu işlemler OCSP ile de otomatik olarak yapılabildiği

gibi, ESHS web sitesinden de kontrol edilebilir. Bunun otomatik olarak yapılıp yapılmadığını ESHS'den teyit etmeniz önerilir.

3. Bu aşamalardan sonra, 2.Kişi, mesajını daha güvenli olarak 1.Kişi'ye gönderebilecektir.
4. İmzalı mesajı alan 1.Kişi, kendi özel veya gizli anahtarıyla mesajları açabilir. Böylece, hem mesajı alma, hem de kimlik doğrulama işlemlerini, burada gerçekleştirmiş olur. Bu noktada, bir hususu belirtmekte fayda vardır. Yapılan haberleşmenin güvenlik unsurlarını tam olarak karşılayabilmesi için, gizlilik ve bütünlük işlemleri de tamamlanmalıdır. Burada, gizlilik için simetrik algoritmalar, bütünlük için de özetleme algoritmaları kullanılmalıdır.



Şekil 6.24. AAA İçerisinde Anahtar Ve Sertifika İşlemleri

AAA ortamında, Şekil 6.24'de verilen şekilde de hizmet verilebilir. Bunun için, 1.Kişi'nin, 2.Kişi'ye, bir mesaj göndermek İstediğini varsayalım. Bu durumda, 1.Kişi, kendi özel anahtarıyla mesajı şifreleyip, karşı tarafa gönderebilir (1).

1.Kişi'den gelen şifreli mesajı alan 2.Kişi ise, hemen Özel SM' ye bağlı olan Özel Sertifika Deposuna bağlanır ve 1.Kişi'ye ait olan açık anahtarı ve sertifikayı sorgular (2) ve kendi bilgisayarına, 1.Kişi'ye ait olan sertifikayı indirir (3).

1.Kişi'ye ait olan genel anahtarı artık elde eden 2.Kişi, bu anahtarı kullanarak, şifrelenmiş mesajı deşifre edebilir (4),

Burada açık anahtarı elde eden her kullanıcının, 2.Kişi'ye gönderilen mesajı açabileceği gözden kaçırılmamalıdır. Gerçekte, bu işlem kimlik doğrulama için kullanılır. Yukarıda da belirtildiği gibi, haberleşmenin yüksek güvenlikle sağlanması için, gizlilik ve bütünlük işlemlerinin (3) nolu adımdan önce yapılması gereklidir.

Zaman damgası da bu işlemlere eklenebilir. Zaman damgasının uygulanabilmesi için, uygun olan bir atom saatinden gerekli zaman bilgisi alınmalıdır.

6.15 Değerlendirme ve Öneriler

Bu bölümde AAA'yı değerlendirdiğimiz zaman, AAA'nın amacı özel sektör, kurum ve kuruluşların ve kullanıcıların iş ve işlemlerini hızlandırmak, kolaylaştırmak, yaşam kalitesini arttırmak, mevcut kaynakları verimli şekilde kullanmalarını sağlamak, kurumsal, kişisel bilgi ve bilişim teknolojilerinin güvenliğini sağlamak, hukuki olarak sorumluluk yüklemek, doküman kullanımı azaltmak, internet suçlarını azaltmak ve daha da önemlisi gizlilik, bütünlük, kimlik tanımlama ve doğrulama, inkar edemezlik ve erişim sürekliliğini sağlamaktır. Bu sayede bilgi ve sistem güveliği sağlanmış olacak ve böylece hayat daha yaşanılır hale gelecektir.

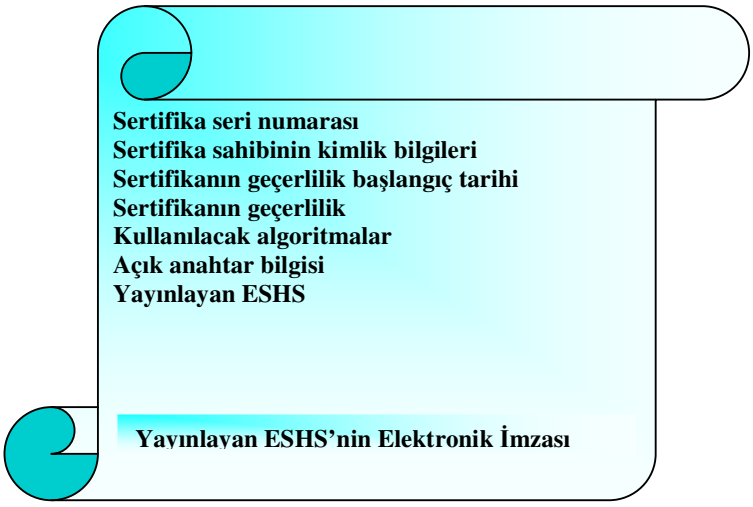
Bu yukarıda bahsettiğimiz konuların gerçekten düzenli çalışabilmesi için, uygun olan yapıların seçimi, bilgi standartlarına olan uygunluğu, yüksek bir güven ortamı oluşturma, uygun anahtarlama ve şifreleme seçimleri ile uygun bir sertifikasyon ve sertifika yönetiminin sağlanması gerekmektedir.

AAA'nın güvenliği her zaman ön planda tutulmalıdır. AAA'nın gelişen teknolojiyi sürekli takip etmesi ve güncellenebilir olması gereklidir. Kurulumu sırasında ise bir AR-GE grubunun kurulması faydalı olacaktır. Çünkü böyle bir grubun kurulu olmasıyla yukarıda bahsettiğimiz konularda daha titiz olunup, gelişmeler güncel olarak takip edilebilecektir.

7. ELEKTRONİK SERTİFİKA

Bir ESHS'nin temel görevi elektronik sertifika yayınlamaktır. Yasada elektronik sertifika şöyle tanımlanır: "İmza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kaydı"[81–84]. Bir elektronik sertifika, kullanıcı kimliği ile kullanıcı için üretilen imza doğrulama verisini, yani kullanıcının açık anahtarını birbiri ile ilişkilendiren bir veri yapısıdır. Bu özelliği ile elektronik sertifika kullanıcıların sanal ortamdaki kimlik kartı olarak nitelendirilebilir.

Elektronik Sertifika, bir ESHS tarafından yayınlanır. Temel olarak bir elektronik sertifika içinde yer alan bilgiler Şekil 7.1.'de belirtilmiştir. Aşağıda bu bilgilerin kısa açıklamaları verilmiştir:



Şekil 7.1. Elektronik Sertifika

Sertifika seri numarası: Yayınlayan tarafından üretilen sertifikaya ait tekil kimlik numarasıdır.

Sertifika sahibinin kimlik bilgileri: Sertifika sahibini tekil olarak tanımlayabilen kimlik bilgileridir. Bu bilgilere örnek olarak T.C. Kimlik Numarası, adı, soyadı, e-posta bilgileri verilebilir.

Sertifika geçerlilik başlangıç tarihi: Sertifika belirtilen bu tarihten önce kullanılamaz.

Sertifika geçerlilik sonlama tarihi: Sertifika belirtilen bu tarihten sonra kullanılamaz.

Sertifikanın kullanım amacı: Bu sertifika ve içinde yer alan açık anahtar bilgisinin ne amaçla kullanılmak üzere yayınlandığı belirtilir. Bir sertifika, örneğin, elektronik imzalama, şifreleme, kimlik doğrulama gibi amaçlarla kullanılabilir.

Kullanılacak algoritmalar: Bu açık anahtar bilgisinin hangi algoritmalarla birlikte kullanılabileceği yazılır. Örnek olarak RSA, DSA, EC, DH verilebilir.

Açık anahtar bilgisi: Bu sertifikada kimliği tanımlanan kullanıcıya ait açık anahtardır.

Yayınlayan ESHS: Bu sertifikayı yayınlayan ESHS'nin kimlik bilgileri.

Yayınlayanın elektronik imzası: Bu sertifikayı yayınlayan ESHS, sertifika bilgilerini kendi özel anahtarını kullanarak imzalar. Bu sertifikayı kullanacak bir kullanıcı, imzayı ESHS'nin açık anahtarı ile onaylayarak, gerçekten belirtilen ESHS tarafından yayınlandığından emin olur.

Yukarıda özellikleri belirtilen bir elektronik sertifikanın yasal olarak geçerli olan güvenli elektronik imza oluşturmak amacıyla kullanılabilmesi için, yasada tarif edilen "Nitelikli Elektronik Sertifika" özelliklerine sahip olması gerekir.

7.1 Sertifika Türleri

7.1.1 Bireysel sertifikalar

Kişisel bazlı tanımlamalarda kullanılan sertifikalardır. Bu sertifikalar, günlük olarak kullandığımız ehliyet, pasaport ya da kimlik kartlarının elektronik karşılığıdır. Bu sertifikalar ile kimlik doğrulama, bütünlük, gizlilik ve inkâr edememe gibi işlemler gerçekleştirilir. Bireysel veya kişisel sertifikalar ile elektronik bankacılık, alışveriş, çevrimiçi abonelik ve resmi yazışmalar gibi işlemler güvenli bir şekilde yapılabilir. Gönderilen bilgiler şifrelenebilir veya deşifre edilebilir dokümanların gizliliği sağlanabilir, güvenli arşivleme yapılabilir, haberleşmelerin gizliliğinden emin olunabilir, özel ve korumalı bilgilere erişmek için yetkilendirme oluşturulabilir, maliyetler düşürülebilir, verimlilik artabilir ve daha da önemlisi kendimizi diğer kişilere güvenle tanıtabilir veya güvenle tanıyabilir ve güvenli bir şekilde haberleşebiliriz [83,85].

7.1.2 Sunucu sertifikası

Sunucu sertifikaları, Web sunucularının kimlik bilgilerini ve açık anahtarını taşıyan ve bu sunuculara bağlanan kullanıcılara sunulan elektronik sertifikalardır. Özellikle son dönemlerde artan ve ülkemizde de görülen internet üzerinden dolandırıcılık faaliyetlerinin bir

kısmı, gerçeğine çok benzeyen taklit Web siteleri aracılığı ile gerçekleştirilmektedir. Sunucu sertifikaları ile bağlanılan web sitesinin kimliği güvenilen bir ESHS aracılığı ile doğrulanabilir. Sunucu sertifikası, kişisel sertifikalar gibi X.509 standardına uygun üretilirler. Bu sertifika sayesinde, bağlanılan Web sunucusunun, kullanıcılar açısından kimlik doğrulaması yapılmış olur. Bu yöntemde kullanıcı, bağlandığı web sitesinde hiçbir işlem yapmadan önce sunucu sertifikasının doğruluk sınamasını gerçekleştirir. Sertifikadaki sunucu kimlik bilgisi, sertifika geçerlilik süresi gibi bilgiler elle kontrol edilir. Bunun yanında, en önemlisi, bu sertifikanın TK tarafından yetkilendirilmiş bir ESHS tarafından yayınlanıp yayınlanmadığına bakılır. İsteğe bağlı olarak, bu kimlik doğrulaması çift taraflı olarak gerçekleşebilir. Bu yöntemle hem Web sunucusu, karşısındaki kullanıcının kimliğinden hem de kullanıcı Web sunucusunda emin olabilir. Bu kimlik doğrulama işleminde bugün yaygın olarak kullanılan yöntem, aynı zamanda kullanıcı ile Web sunucusu arasında şifreli haberleşmeye de olanak tanıyan SSL protokolüdür[85].

7.1.3 Yazılım sertifikası

Sertifikalar, sadece kişiler için değil yazılımların tespitinde de kullanılmaktadır. Bilgisayar kullanıcıları, yazılımı geliştirenlerin kimliğinden, yükledikleri programın, gerçekten o kurum, firma veya kişi sunucusundan geldiğinden emin olmak için bu tip sertifikaları kullanmaktadırlar. Bu sertifikalarda, kuruluş ve ülke adresleri ile e-posta adresleri yer alabilmektedir.

7.1.4 Çok amaçlı (Wildcard) sertifikalar

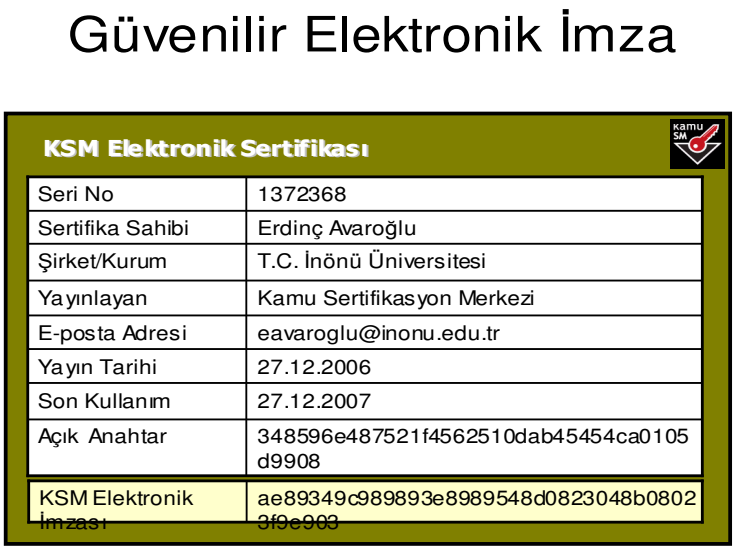
Bu sertifikalar, tek bir sunucu sertifikası kullanarak, birden fazla web sitesine hizmet verebilen sertifikalardır. Çok amaçlı sertifika normal bir sunucu sertifikasına benzemektedir. Sertifika imzalama isteğinin oluşturulması esnasında, bir web yöneticisi, sertifikanın ortak isim bilgisinin içerisinde birçok amaçlı sertifika kullanılır. İnternet tarayıcıların çoğu, bu sertifikaları, standart sunucu sertifikaları gibi kabul etmektedir[86].

7.2 Nitelikli Elektronik Sertifika

5070 sayılı Kanun uyarınca gereken şartları sağlayan ve TK tarafından yetkilendirilmiş nitelikli bir ESHS tarafından verilmiş sertifikalardır[86]. Nitelikli elektronik sertifikalar ITU-T Rec. X.509V.3 standardına uymak zorundadır. Buna göre bir nitelikli elektronik sertifikada yer alması zorunlu olan bilgiler şunlardır[85,87–89]:

- Sertifikanın “nitelikli elektronik sertifika” olduğuna dair bir ibare
- ESHS’nin kimlik bilgileri ve kurulduğu ülkenin adı
- İmza sahibinin teşhis edilebileceği kimlik bilgileri

- Elektronik imza oluşturma verisine karşılık gelen imza doğrulama verisi (yani kullanıcının açık anahtarı)
- Sertifikanın geçerlilik süresinin başlangıç ve bitiş tarihleri
- Sertifikanın seri numarası
- Sertifika sahibi diğer bir kişi adına hareket ediyorsa bu yetkisine ilişkin bilgi
- Sertifika sahibi talep ederse meslekî veya diğer kişisel bilgileri
- Varsa sertifikanın kullanım şartları ve kullanılacağı işlemlerdeki maddi sınırlamalara ilişkin bilgiler
- ESHS'nin sertifikada yer alan bilgileri doğrulayan güvenli elektronik imzası



Şekil 7.2. Güvenilir Elektronik İmza

7.3 Zaman Damgası

Özellikle belirli bir son işlem tarihi olan vergi beyannamesi vermek, fatura ödemesi yapmak gibi işlemlerde, elektronik hizmetten önce son gün beyannamesini vermeyen ya da ödemesini yapmayan rahatlıkla tespit edilebilirdi. Çünkü vergi dairesi ya da bankalar belli bir saatte kapanırlardı. O saate kadar da işlemi gerçekleştirmeyen yükümlüler geç kalmış sayılırdı. Ancak elektronik ortamda gerçekleşen işlemlerde alıcının saati ile göndericinin saati birbirinden farklı olabilir. Bu nedenle işlemin gerçekleştiği tam saatin bilinmesi bir gereklilik halini almıştır. Elektronik bir veriye, bu veriye ilişkin tarih/saat bilgisinin güvenilir bir kaynaktan edinilerek eklenmesine "Zaman Damgası" denir. Yasanın 3h maddesinde Zaman Damgası şöyle tanımlanmaktadır[81,90–93]:

"Bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı ve / veya kaydedildiği zamanın tespiti amacıyla, ESHS tarafından elektronik imza ile doğrulanan kaydı."

Buna göre ESHS'nin temel görevlerinden biri de kullanıcılara zaman damgası hizmeti vermektir. ESHS bu hizmeti verirken bir takım uluslar arası standartlara uygun olarak vermekle yükümlüdür. Ayrıca ESHS zaman damgası hizmetlerini vermesi ile ilgili ilke ve uygulama esaslarının belirtildiği belgeleri yayınlamakla yükümlüdür. Kullanıcının bu hizmeti almak için ESHS'den talep etmesi gereklidir.

7.4 Elektronik Sertifika Hizmet Sağlayıcısı

Yasaya göre Elektronik Sertifika Hizmet Sağlayıcısı (ESHS), elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişilerdir[81,91,93].

Elektronik sertifika hizmet sağlayıcısı yapacağı bildirimde;

- Güvenli ürün ve sistemleri kullanmak,
- Hizmeti güvenilir bir biçimde yürütmek,
- Sertifikaların taklit ve tahrif edilmesini önlemekle ilgili her türlü tedbiri almak ile ilgili şartları sağladığını ayrıntılı bir biçimde gösterir.

Her sertifika hizmet sağlayıcısı, çalışma ilkesi ile ilgili ayrıntılı bilgilerin bulunduğu Sertifika Uygulama Esasları (SUE) ve Sertifika İlkeleri (Sİ) adlı belgeleri yayınlamalıdır.

7.4.1 ESHS'nin yükümlülükleri

TK tarafından nitelikli sertifika vermek üzere yetkilendirilen ESHS'lerin yükümlülükleri şunlardır[81,83,91,93]:

- Hizmetin gerektirdiği nitelikte personel istihdam etmek
- Nitelikli sertifika verdiği kişilerin kimliğini resmî belgelere dayanan güvenilir bir biçimde tespit etmek
- Sertifika sahibinin diğer bir kişi adına hareket edebilme yetkisi, meslekî veya diğer kişisel bilgilerinin sertifikada bulunması durumunda, bu bilgileri de resmî belgelere dayandırarak güvenilir bir biçimde belirlemek
- İmza oluşturma verisinin ESHS tarafından veya sertifika talep eden kişi tarafından ESHS'ye ait yerlerde üretilmesi durumunda bu işlemin gizliliğini sağlamak veya ESHS'nin sağladığı araçlarla üretilmesi durumunda, bu işleyişin güvenliğini sağlamak

- Sertifikanın kullanımına ilişkin özelliklerin ve uyuşmazlıkların çözüm yolları ile ilgili şartların ve kanunlarda öngörülen sınırlamalar saklı kalmak üzere güvenli elektronik imzanın elle atılan imza ile eşdeğer olduğu hakkında sertifika talep eden kişiyi sertifikanın tesliminden önce yazılı olarak bilgilendirmek
- Sertifikada bulunan imza doğrulama verisine karşılık gelen imza oluşturma verisini başkasına kullandırmaması konusunda, sertifika sahibini yazılı olarak uyarmak ve bilgilendirmek
- Yaptığı hizmetlere ilişkin tüm kayıtları yönetmelikle belirlenen süreyle saklamak
- Faaliyetine son vereceği tarihten en az üç ay önce durumu TK'na ve elektronik sertifika sahibine bildirmek
- ESHS'ye yüklenen yukarıdaki yükümlülükler ile yasa şunları garanti etmektedir:
- İmzası doğrulanan şahıs, gerçekten kimliği belirtilen şahıstır.
- ESHS'nin faaliyetleri sonlansa bile, ondan elektronik sertifika almış kişilere hizmetin devamlılığını sağlamak için gerekli önlemler alınmıştır.
- Kullanıcının, kullanım konusunda bilinçlendirilmesi sağlanmıştır.

ESHS, üretilen imza oluşturma verisinin (yani sertifika sahibinin özel anahtarının) bir kopyasını alamaz veya bu veriyi saklayamaz. Bu demektir ki ESHS sadece nitelikli elektronik sertifikanın yayınlanma aşamasında devreye girer. Bir ESHS'nin yaptığı iş esas olarak, kendisi tarafından verilmiş nitelikli elektronik sertifikayı kullanan imza sahibinin kimliğini tarafsız 3. şahıs sıfatıyla doğrulamaktır. Bu sertifikayı kullanarak gerçekleşen güvenli iletişim yalnızca iletişime katılan tarafları ilgilendirir.

7.4.2 Sertifika ilkeleri ve sertifika uygulama esasları

ESHS tarafından yayınlanması zorunlu olan bir belgelerdir. Sertifika İlkeleri, sertifika kullanımı, sertifika yaşam çevrimi ile ilgili kurallar listelenir. ESHS, elektronik sertifikalar ve kurduğu AAA ile ilgili tüm iş sürecini bu belge ile tanımlar[81,94]. Sertifika Uygulama Esasları'nda, Sertifika İlkeleri belgesinde belirtilen kuralların nasıl uygulanacağı ayrıntılı bir biçimde ifade edilir. Genellikle Sertifika Uygulama Esasları, Sertifika İlkeleri'ne göre daha uzun, kapsamlı ve teknik bilgiler içeren bir belgedir. ESHS, bu iki belgeyi IETF RFC 3647'ye uygun olarak hazırlamalıdır.

7.4.3 Elektronik sertifikaların kullanım süresi

Her elektronik sertifikanın belli bir kullanım süresi vardır. Bir kişi için bir ESHS tarafından yayınlanan elektronik sertifika, sertifika sahibi tarafından hayatı boyunca kullanılamaz. Sertifikanın kullanımının bir başlangıç bir de bitiş süresi vardır. Elektronik imza uygulamaları, elektronik sertifikalarla işlem yapmadan önce sertifikanın geçerlilik süresini

kontrol ederler. Genellikle bu süre bir yıldır[81,94]. ESHS'nin sertifikasının da bir geçerlilik süresi vardır. Bu süre 10 yılı aşamaz.

7.4.4 Sertifika yaşam çevrimi

Bir sertifikanın üretilmesinden iptaline kadar geçirdiği aşamalara "Sertifika Yaşam Çevrimi" denir. Bu çevrim, ESHS tarafından net bir şekilde Sertifika İlkeleri ve Sertifika Uygulama Esasları belgeleri içinde tanımlanır. Aşağıda bir sertifika yaşam çevrimi, genel hatlarıyla tarif edilmiştir. Gerçek uygulamalarda bazı farklılıklar olabileceği unutulmamalıdır[81].

7.4.5 Sertifikanın yayınlanması

- Kullanıcı, elektronik sertifika almak için ESHS'ye başvurur. Bu başvuru adımında, kimlik doğrulamanın güvenliği için yüz yüze görüşme gereklidir.
- ESHS, kullanıcının kimliğini doğrular ve sertifikayı yayınlar.
- ESHS, sertifikayı, herkese açık bir ortama (örneğin bir dizin hizmeti üzerine) aktarır.

7.4.6 Sertifikanın kullanımı

- Kullanıcı gerçekleştirdiği işlemi ya da göndereceği mesajı kendi özel anahtarı ile imzalar ve alıcıya iletir.
- Alıcı mesajı alır, mesajdaki sayısal imzayı göndericinin açık anahtarıyla doğrulaması gerekir. Bunun için kullanıcının nitelikli elektronik sertifikasını ESHS'nin herkese açık dizin hizmeti üzerinden sorgular ve sertifikayı elde eder.
- Sertifikadaki geçerlilik süresini, nitelikli sertifika olup olmadığını ve imzalayan ESHS'nin imzasının doğruluğunu kontrol eder.
- ve 3. aşamadan sorunsuz geçildikten sonra, mesajdaki elektronik imzanın alıcıya ait olup olmadığını kontrol eder. Bunu imza onaylama işlemi ile gerçekleştirir. İmza onaylanırsa alıcı, mesajı gönderinin kimliğinden, mesajın alıcıdan çıktığı şekliyle kendisine ulaştığından ve göndericinin bu mesajı gönderdiğini daha sonra inkâr edemeyeceğinden emin olur.

7.4.7 Sertifikanın iptali ve askıya alınması

Bir nitelikli elektronik sertifika, özel anahtarın kaybolması veya sertifikanın geçerlilik süresinin sonuna gelmesi durumlarında iptal edilebilir. Geçici süreyle kullanımdan kaldırılacak olan sertifikalar ise askıya alınır. İptal edilen sertifika tekrar kullanılamaz. Askıya alınan sertifika, askıda olduğu süre boyunca kullanılamaz. Ancak askıda olan bir sertifika askıdan indirildiğinde normal kullanımına devam edilebilir[81,91]. ESHS, iptal edilen sertifikaları

Sertifika İptal Listesi (SİL) adında bir liste ile periyodik olarak yayınlar. SİL için genel kabul görmüş X.509 v2 standardı kullanılmaktadır. ESHS, aynı yayınladığı sertifikalarda olduğu gibi yayınladığı SİL'leri de elektronik olarak imzalar. Bir sertifika iptal edildiğinde, bir sonraki SİL içerisinde iptal edilen sertifikaya ilişkin bilgileri yayınlanır. Sertifikaların tutarlı bir şekilde kullanılabilmesi için SİL her kullanımda kontrol edilmelidir.

SİL'de üç tür sertifika yer alır:

- İptal edilen sertifikalar
- Geçerlilik süreleri dolan sertifikalar
- Geçici olarak kullanımdan kaldırılan (askıya alınan) sertifikalar

Türkiye'deki nitelikli elektronik sertifikaların askıya alınması yasal olarak tanımlanmış bir işlem değildir. Bu nedenle bu bölümde askıya alma konusunda verilen bilgiler sadece okuyucuyu bilgilendirme amaçlıdır.

7.4.8 ESHS'lerin yetkilendirilmesi

Yasaya göre ESHS'ler faaliyete geçmek üzere TK'na bildirimde bulunurlar. Düzenleyici kurum olan TK, bildirim yapan ESHS üzerinde yaptığı denetimlerde yasada belirtilen şartların sağlandığına kanaat getirdikten sonra, bekleme süresinin sonunda ESHS çalışmaya başlamaktadır. Bu süreç ayrıntılı olarak aşağıda tarif edilmiştir[81,94]:

Bildirimin Yapılması: Kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişileri, ESHS olma talebini, gerekli bilgi ve belgeleri eksiksiz olarak TK'na ibraz etmek suretiyle bildirimde bulunur.

Bildirimin İncelenmesi ve Sonuçlandırılması: TK, yapılan bildirim üzerindeki incelemesini iki ay içinde sonuçlandırır. Bildirim şartlarını eksiksiz olarak yerine getiren ESHS, bildirim yaptığı tarihten iki ay sonra faaliyete geçer. TK, ESHS'nin gerekli şartları sağlamadığını tespit ederse ESHS'ye ek süre verir. Eksiklerini verilen süre içerisinde gidermeyen ESHS, ESHS olma vasfını kaybeder.

Bildirimdeki Değişiklikler: ESHS, faaliyete geçtikten sonra, yapmış olduğu bildirimde herhangi bir değişiklik meydana gelmesi halinde, bu değişiklikleri 7 gün içinde TK'na bildirir.

7.4.9 ESHS'nin nitelikleri

Bu bölümde ise yasa ve yönetmelikler gereği ülkemizde kurulacak ESHS'lerin ne tür niteliklere sahip olacağından bahsedilecektir[81,94].

- Süreklilik

Gerek kamuya hizmet veren KSM gerekse ticari ESHS'ler, verdikleri hizmetler bakımından kesintisiz hizmet vermesi gereken bir kurumdur. Gerek özel gerekse kamu sektöründeki uygulamalarda, ESHS'lerden 7 gün 24 saat kesintisiz hizmet ihtiyacı olacaktır. Bunun yanında ESHS'nin kök sertifikasını, sertifika başvuru bilgilerini koruması ve saklaması ile ilgili kriterlere uygun davranması da önemli bir gereksinimdir.

- ESHS'nin uyacağı kriterler, standartlar, parametreler

Hizmet verecek olan ESHS'lerin kullanabilecekleri kriptografik fonksiyonlar ve parametreler ile ilgili sınırlamalar açıkça tarif edilmiştir. Bu nitelikler şunlardır:

- ESHS'nin işleyişi ile ilgili sağlayacağı standartlar
- İmza oluşturma ve doğrulama verileri (yani özel ve açık anahtarlar)
- Sertifika ilkeleri ve Sertifika Uygulama Esasları
- Kullanılacak güvenli elektronik imza oluşturma ve doğrulama araçlarının uyacağı standartlar
- ESHS'nin uyacağı güvenlik kriterleri

Kriptografi çok hızlı ilerleyen bir bilim dalıdır. Bu nedenle bugün güvenli sayılan bir algoritma bir sene sonra güvensiz hale gelebilir. ESHS'ler belirtilen tarihten sonra TK tarafından yayınlanacak yeni parametrelere uygun olarak kendi altyapılarını güncellemek zorundadırlar.

7.4.10 ESHS'lerin denetimi

Yasaya göre ESHS yetkisi alındıktan sonra TK, ESHS'leri bu niteliklerin devamlılığını garanti etmek amacıyla denetlemeye devam edecektir. Bu nedenle yetki belgesine sahip olan ESHS, ancak sahip olduğu nitelikleri sürdürdüğü takdirde hizmet vermeye devam edebilecektir. Kamu kurumlarına hizmet veren KSM de bu kapsama dâhildir.

7.5 Kök Sertifika

ESHS'nin elektronik sertifikasına kök sertifika denir. ESHS'nin, kendisinden elektronik sertifika alan kullanıcılar gibi bir çift anahtarı vardır. Bu anahtarlardan özel anahtar, yayınlanan elektronik sertifikaları imzalamak için kullanılır. ESHS'nin açık anahtarı ise ESHS'nin kök sertifikası içinde yer alır ve kullanıcılar tarafından bu ESHS'nin yayınladığı elektronik sertifikalara attığı elektronik imzasının doğrulanması için kullanılır. Bir nitelikli elektronik sertifika, ancak yayınlayan ESHS'nin sertifika üzerindeki imzası geçerliyse kullanılabilir. Bir

nitelikli elektronik sertifikaya ulaşan bir kullanıcı, öncelikle bu sertifikanın geçerliliğini, sertifika üzerindeki ESHS imzasının geçerliliğini kontrol ederek sınar Kök sertifika açık anahtarın ESHS'nin olduğunu onaylar[81,91,95–97].

ESHS'nin özel anahtarı, bir AAA sistemindeki güven zincirinin en önemli halkasıdır. ESHS'nin özel anahtarı, yetkisiz bir kullanıcının eline geçerse, AAA üzerinde verilen tüm güvenlik hizmetleri ve kurulan güvenli iletişim altyapısı tehlikeye düşer. Bu nedenle ESHS'nin özel anahtarını saklamak için özel ve yüksek güvenlik içeren saklama ortamları kullanılır. Küçük bir kutuya benzeyen ve yalnızca yetkili kullanıcıların ve programların erişmesine izin verecek şekilde ESHS'nin özel anahtarını saklayan bu cihazlara Donanım Güvenlik Modülü (Hardware Security Module) denir.

7.6 Elektronik Sertifikaların Uygulama Alanları

Elektronik imza ve buna bağlı olarak elektronik sertifikalar, sağladıkları güven altyapısı sayesinde kendisine birçok uygulama alanı bulmuştur. Bu alanlardan bazıları şöyle özetlenebilir[81].

Bütünlük, Kimlik Denetimi ve İnkâr Edemezlik Hizmetleri: Kurumlar mesajların doğru kişi tarafından, içeriği değiştirilmeden ve karşı tarafın inkâr edemeyeceği şekilde iletimini sağlamak için elektronik sertifikalar kullanırlar. Yönetmeliğin 15d maddesine göre nitelikli elektronik sertifikalar yalnızca bütünlük hizmetini karşılamak amacıyla yayınlanabilir ve kullanılabilir. Bununla birlikte bir belgenin elektronik imzasını doğrulama işlemi, o belgenin bütünlüğünü garanti ederken, göndericinin kimlik doğrulamasını da otomatik olarak gerçekleştirdiği unutulmamalıdır. Kimlik doğrulama hizmetinin kapsam dışı bırakılmasının sonucunda kamu kurumları ya eski zayıf kimlik doğrulama yöntemlerinde devam edecekler ya da güçlü kimlik doğrulama sistemleri kurmak için yüksek maliyetli yatırımlar yapacaklardır. Bu bağlamda yönetmeliğin 15d maddesi hakkında Kamu SM yetkilileri görüşlerini gerekçeleri ile birlikte daha net bir şekilde ortaya koymalıdırlar.

- **Erişim Denetimi:** Bilgisayar sistem ve terminallerine, İnternet sitelerine, kurum içi ağ üzerindeki hizmetlere erişim denetimini sağlamak amacıyla kullanılırlar.
- **Belge İletiminin ve İletim Zamanının İspatı:** Kritik belgelerin hukuksal açıdan zamanını ve tarihini doğrulamak için elektronik imza yasası ile birlikte gelen zaman damgası hizmeti kullanılabilir.
- **Elektronik İş Akışı:** Kâğıt üzerinde işleyen bürokrasi, ıslak imza yerine geçebilen güvenli elektronik imza sayesinde elektronik ortamda çok daha hızlı, düşük maliyetli ve güvenilir bir şekilde gerçekleştirilebilir.

- **Resmi başvuru işlemleri:** Bu işlemler, devlet dairesine gitmeden, zaman kaybetmeksizin, bilgisayar başından gerçekleştirilebilir. İşlemlerin sonuçları da aynı yolla izlenebilir.
- **Arşivleme:** Depolanmış elektronik belgelere ya da mesajlara erişildiğinde, belgenin değiştirilmeden orijinal haliyle saklandığından emin olunması amacıyla kullanılabilir.

Bütün bu hizmetlerin yanında elektronik imzanın verinin gizliliği için kullanılamayacak bir teknoloji olduğu unutulmamalıdır. Elektronik imzanın dayandığı açık anahtarlı kriptografik sistem ile veri şifrelemek yüksek maliyetli ve uzun süreler gerektiren bir işlemdir. Bu nedenle elektronik imza teknolojisi, teknolojik olarak mümkün olsa bile, dünyadaki uygulamalarda da gizlilik hizmetini sağlamak için kullanılmaz. Gizlilik hizmeti, elektronik imzanın da birlikte çalışabildiği SSL protokolünün kullanımı ile sağlanabilir.

7.7 Yabancı Elektronik Sertifikalar

Yabancı elektronik sertifikaların Türkiye'de geçerli olabilmesi için gerekli koşullar, Elektronik İmza Kanunu'nun 14'üncü maddesinde belirlenmiştir. Buna göre yabancı elektronik sertifikaların geçerlilikleri ve hukukî sonuç doğurabilmeleri, milletlerarası anlaşmaların varlığına veya yerli bir elektronik sertifika hizmet sağlayıcısı tarafından garanti edilmesine bağlıdır. Söz konusu sertifikaların ait olduğu ülkede o ülkenin mevzuatına göre faaliyette bulunuyor olması da gereklidir. Bu suretle yabancı sertifikaya ait sorumluluklar yerli ESHS tarafından üstlenilmiş olmaktadır[94]. Her iki durumda da yabancı elektronik sertifikalar Türkiye'de geçerli nitelikli elektronik sertifika ile aynı hukuki statüye sahip olacaklardır. Burada gözden kaçırılmaması gereken önemli bir konu, Türkiye'deki elektronik sertifika hizmet sağlayıcı tarafından garanti edilen yabancı sertifikaların kendi ülkelerinde nitelikli olup olmadıklarına bakılmaksızın, 5070 Sayılı Kanunda tanımlanan nitelikli elektronik sertifikalar ile aynı hukuki etki ve sonuçlara sahip olacağı hususudur.

7.8 Elektronik Sertifika Hizmet Sağlayıcıları İle Noterlerin Farkı

Elektronik Sertifika Sağlayıcılığı ile noterler arasında bir takım benzerlikler bulunmakla beraber aslında hizmet yapılarında farklılıklar bulunmaktadır. Noterler, bir işlemin vaki olduğunun resmi kaydını zaman mührüyle birlikte tutarlar. Bu anlamda işleme ve/veya kişilere güvenilir tanık durumundadırlar. Örneğin noterde bir sözleşme yapıldığında, noter açısından sözleşme içeriğinin hukuki boyutları önemli değildir. Önemli olan, evrakın ilgili taraflarca belirtilen tarihte noterin huzurunda ve tanıklığında imzalandığıdır. Noterin kimlik tespiti de beyan usulünde çalışır. Kimliği doğrulamak yerine evraktaki kimlikle kişinin beyan ettiği kimlik belgesini karşılaştırır. Bir noter, noterlik hizmeti alan bir vatandaşla daha önce çalışmış olmak zorunda değildir. Kimlik doğrulamada ESHS, noterde olmayan bir sorumluluk taşımaktadırlar.

ESHS, işlemi gerçekleştiren şahsın kimliğin doğruluğunu da kontrol eder. Bununla birlikte gerçekleştirilen işlemle ilgisi yoktur. Gerçekleştirilen işlem veya gönderilen belge tamamen iletişim kuran tarafları ilgilendirir. ESHS, bu iletişimde güven altyapısının oluşmasını sağlayan ve iletişimin temel güvenlik gereksinimlerine uygun bir biçimde çalışır. ESHS, bir kimyasal tepkimede, uygun ortam şartlarını sağlayan bir katalizör gibi görev yapar[106]. İletişim esnasında, elektronik imzanın onaylanması aşamasında sertifikanın geçerliliğinin kontrolüne ihtiyaç duyulabilir. Ayrıca belgeye eklenmek üzere zaman damgası hizmeti alınabilir. Bu hizmet, belgeyi görmeden zaman bilgisinin belgeye iliştirilmesi olarak düşünülebilir. Bu işlemde de ESHS, tam olarak noter gibi davranmaz. Çünkü noter, noterlik hizmeti alınan belgenin bir kopyasını alır, içini görür, yapılan sözleşmenin/anlaşmanın miktarına bağlı olarak bir hizmet bedeli ve devlet adına damga vergisi alır. Bununla birlikte ESHS belgenin içeriği ile ilgilenmez. Ancak mesaj sahibi, mesajı imzalamakta kullanacağı nitelikli elektronik sertifika için ya da zaman damgası hizmeti için ESHS'ye bir ücret ödediğinden, dolaylı olarak da olsa bir ücretlendirme söz konusudur.

ESHS belgenin içeriği ile hiç ilgilenmez sadece belgenin gönderenin gönderdiği gibi alıcıya ulaştırılmasını yani değiştirilmediğini ve inkâr edilemeyeceğini garanti eder. Öte yandan, noter huzurunda yapılan diğer pek çok işlemin (alım-satım işlemleri, vekâletler ve benzeri) yasal olarak elektronik işlem çeklinde gerçekleşmesi mümkün değildir. Çünkü yasaya göre, kanunların resmi şekle veya özel bir merasime tabi tuttuğu hukuki işlemler ile teminat sözleşmeleri işlemleri elektronik imza ile gerçekleştirilmesi mümkün değildir.

Kısaca, hem işlevsel olarak hem de Türk Hukuku açısından, noterler ile ESHS'ler birbirine benzer ve farklı yanları olan ve birbirlerini tamamlayan işlevlere sahip iki kurum gibi düşünülmelidir.

7.9 Türkiye'deki Eshs Yapılanması

7.9.1 Kamudaki yapılanma

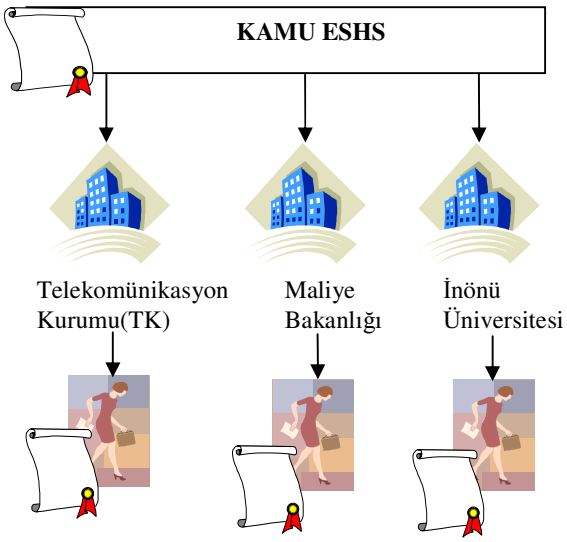
6 Eylül 2004 tarihinde yayınlanan ve 2004/21 numaralı Kamu Sertifikasyon Merkezi (KSM) oluşturulması konulu bir Başbakanlık Genelgesi yayınlanmıştır[81]. Genelge, kamu kurum ve kuruluşlarının iş ve işlemlerini elektronik ortama dönüştürme sürecinde elektronik imza ve sertifikasyon işlemlerini yürütecek yapıları kendi bünyelerinde ve münferit olarak sağlamaları durumunda ortaya çıkacak sistemsel karmaşaya ve emek ve kaynak israfına engel olunmasını hedeflemektedir. Ayrıca, ulusal güvenlik gerekleri göz önünde bulundurularak KSM' de, ulusal yazılım ürünleri kullanılacağı belirtilmektedir. Genelge ile istisnalar dışındaki hiçbir kamu kurumu, elektronik sertifika ihtiyaçlarını karşılamak amacıyla kendi bünyelerinde yeni bir yatırım yapmayacaktır. Kamu kurumları ve çalışanları, bu ihtiyaçlarını KSM'den temin

edilecek elektronik sertifikalar ile karşılayacaklardır. Bu konuda daha önceden başlamış olan ve devam eden çalışmalar durdurulacak, hâlihazırda kullanılmakta olan sistemler ise TK'nun da görüşü alınmak suretiyle en kısa sürede bu yapıya uygun hale getirilecektir.

Bunun sonucunda tüm kamu kurum ve kuruluşlarının aynı kurumsal sertifikasyon yapısı altında toplanmasını, kamu kurumlarının kurum içi ve kurumlar arası elektronik sertifika ihtiyaçlarının karşılanmasını ve sertifika yaşam çevriminin yönetilmesini sağlayacak KSM, TÜBİTAK UEKAE bünyesinde oluşturulmuştur (www.kamusm.gov.tr). KSM, yetki belgesi almak üzere TK'na başvuruda bulunmuştur. Haziran 2005 ayı içerisinde sertifika dağıtımına başlaması beklenmektedir.

Kamu kurumlarının, KSM'den hizmet alması için kendi altyapılarının uygunlaştırılması için gerekli çalışmaları Devlet Planlama Teşkilatı (DPT) ile eşgüdümlü olarak yürüteceklerdir.

Elektronik imza hukuki olarak ıslak imzanın yerine geçebildiğinden mahkemede delil olarak da sunulabilir. Bu bağlamda geçmişe dönük olarak elektronik imza işlemleri ile ilgili bir takım verilerin saklanması gereklidir. Kanuna ve yönetmeliklere göre bilgiler 20 yıla kadar saklanmalıdır. Bu şekilde geçmişte yapılmış işlemlerde kullanılan imza oluşturma anahtarları, oluşturulan imzalar ve imzalanan veri saklanır. Ayrıca bir süre sonra devreye girecek olan E-Devlet Kapısı projesi, tüm kurumları bu tür bilgiler saklamaktan kurtararak merkezi bir elektronik kayıt saklama hizmeti verebilir.



Şekil 7.3. Kamuda Sertifikasyon Yapılanması

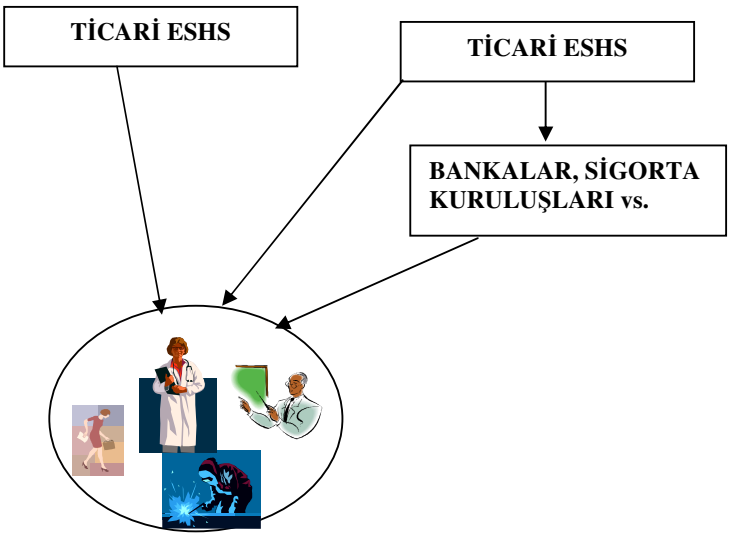
7.9.2 Özel sektörde yapılanma

Önümüzdeki zaman içerisinde kademeli bir şekilde, elektronik olarak verilmekte ve verilecek olan kamu hizmetlerinde vatandaşın elektronik imzası istenmeye başlanacaktır. Bu hizmetler sadece kamu kurumlarıyla sınırlı değildir. Örneğin bir özel banka da İnternet şubesinden hizmet almak isteyen müşterilerine nitelikli elektronik sertifika sahibi olma zorunluluğu getirebilir. Vatandaşların bu tür hizmetlerden yararlanabilmek için ticari ESHS'lerden birinden elektronik sertifika temin etmek zorundadır.

Yasanın ve yönetmeliğin çıkması ile ticari olarak ESHS hizmeti verecek olan kurumların TK'na başvuruları başlamıştır. TK'na ESHS hizmeti vermek üzere şu ana kadar başvuran kurumlar şunlardır:

- E-güven Elektronik Bilgi Güvenliği A.Ş.
- Türktrust Bilgi iletişim ve Bilişim Güvenliği Hizmetleri A.Ş.
- E-tuğra

Ticari ESHS olmak üzere başvuru yapmanın en son tarihi diye bir kavram söz konusu değildir. İsteyen her gerçek ya da özel hukuk tüzel kişileri, ESHS olmak üzere başvuruda bulunabilir.



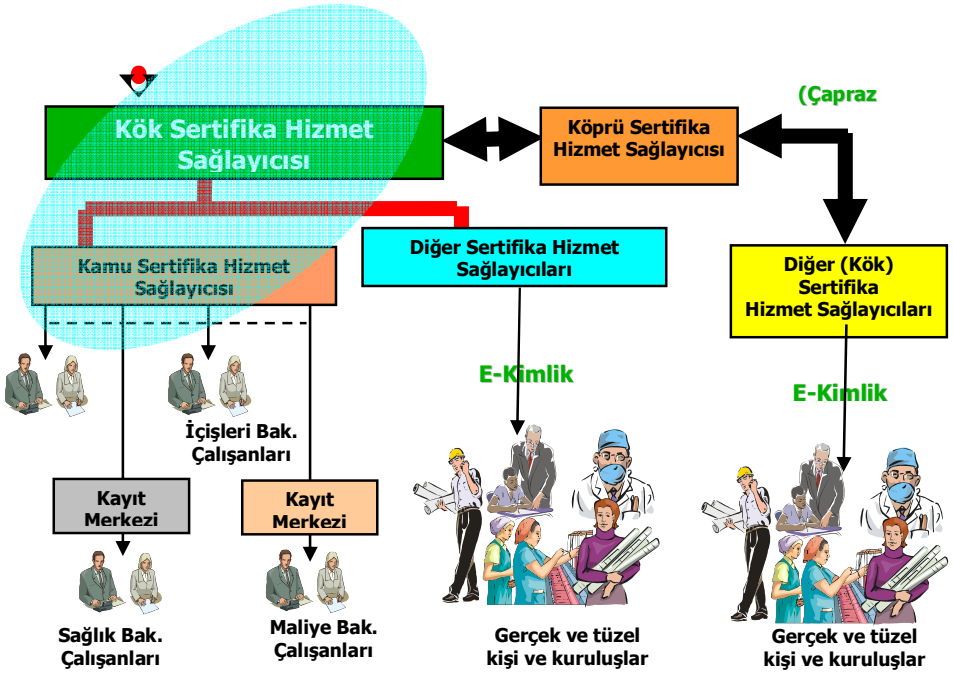
Şekil 7.4. Türkiye'de Ticari ESHS Yapılanması

TK'na ticari ESHS hizmeti vermek üzere başvuracak kurumlar yasa, tebliğ ve yönetmelikte belirtilen şartları sağlamak zorundadır.

7.9.3 Ayrıcalıklı durumlar

KSM Kök Sertifika Hizmet Sağlayıcısı ile buna bağlı olarak Kamu Sertifika Hizmet Sağlayıcısı olarak hizmet verecektir. Yürüttükleri görevler açısından özel niteliği haiz Türk Silahlı Kuvvetleri, Emniyet Genel Müdürlüğü, MİT Müsteşarlığı, Jandarma Genel Komutanlığı, Sahil Güvenlik Komutanlığı ve Dışişleri Bakanlığı kök sertifika ihtiyaçlarını kurulacak Kök Sertifika Hizmet Sağlayıcısından karşılayacaklar, Kamu Sertifika Hizmet sistemlerini kendi bünyelerinde oluşturabileceklerdir. Diğer kamu kurum ve kuruluşları, sertifikalarını, KSM'den temin edeceklerdir.

TÜBİTAK UEKAE



Şekil 7.5. Türkiye'deki ESHS Yapısı

7.10 Dünyada Eshs

7.10.1 Avrupa Birliğinde durum

Avrupa Birliği'ne üye tüm ülkelerde elektronik imzaya yönelik olarak yayınlanmış olan 1999/93/EC direktifi yerine getirilmiştir. İrlanda hariç 14 üye ülkede en az bir nitelikli sertifika üreten ESHS vardır. Fransa ve İrlanda hariç 13 üye ülkede nitelikli sertifika üreticilere lisans veren bir kurum vardır. İrlanda ve İngiltere dışında 13 üye ülkede nitelikli sertifika üreticileri düzenleyen ve denetleyen bir kurum vardır. 9 üye ülkede ise ESHS'lere ilişkin yukarıda belirtilen lisanslama ve denetleme işlevleri aynı kurum tarafından yerine getirilmektedir[81].

7.10.2 ABD'de durum

ABD Kongresi e-imza yasasını (Electronic Signatures in Global and National Commerce Act) 2000 yılında kabul etti. Bu çerçeve yasası e-imzanın uluslar arası geçerliliğine değiniyor olmakla birlikte daha önce yayınlanmış olan AB Yönergesi ile tam bir uyum içerisinde olduğunu söylemek mümkün değildir. UNCITRAL (United Nations Comission on International Trade Law) Birleşmiş Milletler bünyesinde oluşturulmuş ve uluslar arası ticaret yasalarının uyumluluğunu amaçlayan bir komisyon. Çalışma alanları arasına e-ticareti de alan UNCITRAL 2001 yılında e-imza konusunda bir model yasa metni oluşturdu.

7.11 Elektronik İmza Ve Uluslararası Geçerliliği

Elektronik sertifikaların, yayınlandığı ESHS kapsamı içerisinde kullanılması ile beraber diğer ulusal ve yabancı ESHS'ler ile de çalışabilmesi gerekmektedir. Faktör, bilginin gizliliği, bütünlüğü, iki tarafta da kimlik belirleme, zaman kavramının sabitlemesi, ulusal ve uluslar arası kanun/mevzuat ihtilaflarının giderilmesi için elektronik kayıtların ihtilaflarda ispat gücünün ihtilafsız kabulü, uç kullanıcıya kadar güvenli altyapı gibi temel işlemler için ulusal bazda hukuki altyapı, idari, teknik ve uluslar arası altyapının kurulması gerekir. ESHS'lerin karşılıklı çalışabilirliği sağlanırsa, elektronik sertifikaların uluslar arası kullanımı mümkün olacaktır. Teknik özellikler, ilkeler, iş ilişkileri ve yasal değerlendirmeler de göz önüne alınarak ESHS'ler arasında karşılıklı çalışabilirliği sağlamak üzere önerilmiş ve geliştirilmiş birçok yöntem vardır. Bu yöntemler dünya'nın çeşitli ülkelerinde ortak çalışmalarla test edilmekte ve uygulanmaktadır[81].

7.12 Eshs'ler Arası Karşılıklı Çalışabilirliğin Gerekliliği

ESHS'ler arasında teknik, ilke, iş ve yasal bakımdan farklılıklar bulunabilmesinden dolayı karşılıklı çalışabilirlik, üzerinde özenle durulması gereken bir konudur. Ülkelerarası ve farklı AAA etki alanları arasında karşılıklı çalışabilirliği sunmak amacıyla, standartlaşma sağlamak üzere birçok çalışma devam etmektedir[81].

- Karşılıklı çalışabilirlik, bir ESHS tarafından yayınlanan elektronik sertifikaların, yurt içindeki ve yurt dışındaki güven duyabileceği başka ESHS'ler ile de sorunsuz olarak iletişim ve güven ilişkileri kurabilmesi yeteneğidir. Karşılıklı çalışabilirliği sağlamak üzere önerilen seçenekler arasından seçim yapmak üzere aşağıdaki üç ana alan üzerinde belirginlik sağlanmalıdır.
- Karşılıklı anlaşma düzeyine bağlı olarak karşılıklı çalışabilirliği kolaylaştırmaya yardımcı olacak protokol, veri yapısı, sertifika ilkeleri, sertifika uygulama esasları,

sertifika ve sertifika iptal listelerinin paylaşılması gibi teknik değerlendirmelerin göz önüne alınmasıdır.

- Karşılıklı ilkeler ve iş ilişkileri ile ilgili konuların değerlendirilmesidir. Bu alan, ESHS'ler arasındaki ilişkileri tesis etmek üzere, teknik olmayan detayları kapsar.
- Bu alanda ise, yasal değerlendirmeler göz önüne alınır. Karşılıklı çalışabilirlik konusunda karşılaşılabilecek en önemli sorun, farklı hukuki altyapılara sahip ortamlardır. Bu kapsamda ESHS'ye ve kullanıcıya düşen sorumluluk ve yükümlülüklerin iyi anlaşılması gerekir. Buna, göz önüne alınması gereken "Yasal bildirimler ne içerecek ve bu bildirimler güvenen tarafa nasıl taşınacak?" gibi kullanıcı bilgilendirme gereksiniminin kapsadığı yükümlülükler örnek olarak verilebilir.

7.12.1 Hukuki altyapı

Elektronik imza ile ilgili hukuki altyapının oluşturulması ile ilgili şu çalışmalar gerçekleştirilmiştir:

- Her türlü ikili ve kurumsal iş ve işlemlerde kayıt tutma, standart ve tekniklerinin belirlenmesi,
- Elektronik kayıtların kamu kurum ve kuruluşları tarafından belge olarak kabulü ile ilgili standart ve iç mevzuatlarının düzenlenmesi,
- Ticaret Kanunu, Sayıştay denetim usulleri, Borçlar Kanunu, Bankalar ve Vergi Usul kanunlarının elektronik belge tutma ve gönderme şartları göz önüne alınarak tekrardan düzenlenmesi,
- Elektronik ortamda oluşturulan yabancı belgelerin geçerliliği konusunda dış ticaret, gümrük ve bankalar kanununda değişiklik, uluslar arası/ulusal olarak yapılan elektronik sözleşmelerde ve sanal ticarette oluşabilecek ihtilaflar konusunda elektronik tahkim yasasının çıkarılması,
- Özel ve kurumsal bilgilerin gizliliği, bütünlüğü için Ulusal Bilgi Güvenliği Yasasının çıkarılması buna bağlı olarak SPK gibi kurumların ve ürün borsalarında kontrat bazlı, spot ve opsiyon piyasalarında sanal işlem uygulama yönetmelikleri ile uluslar arası sanal ticaret için akreditasyon kurumları için yeni mevzuatların çıkarılması,
- Açık anahtar (public key) ile ilgili onay kurumlarının (Nitelikli Elektronik Sertifika sağlayan kurumların) kurulum izinleri ve denetimi kamu tarafından yapılmalı, %51 hissesi kamu elinde bulunan kurumların bu pazardan ivedi çekilmesi gerekmektedir, uluslar arası kredi ve finans kurumlarının ticarette uyguladığı kriterlerin devlet kurumlarının hizmet ve mal alımında da uygulanması için devlet ihale kanunu, elektronik imza kanunu ile elektronik imza yönetmeliği'ne kesin ve bağlayıcı maddelerin ilave edilmesi,

- Elektronik suçların evrenselliği konusunda yapılan uluslar arası mevzuat çalışmaları ve yapılacak ikili anlaşmaların hızlı bir şekilde yapılması, işlerlik açısında delil toplama ve alma/verme standartlarının belirlenmesi.
- Elektronik kontrat ve elektronik imza gerektiren sanal işlemlerde tüketicinin korunması ile ilgili mevzuatın elektronik ticaret açısından yeniden gözden geçirilmesi, e-ticaret yapan kurumların uyacağı kuralların ivedilikle yayınlanması, bankacılık kanunu ile ilişkilendirilmeli ve geri ödeme (charge-back) sisteminin sanal ticarette uygulamaya sokulması,
- Elektronik ödeme araçları arasında yer alan elektronik paranın (elektronik senet, elektronik çek, elektronik teminat, gibi) uygulanacağı standart, teknikler ve güvenlik kriterleri ile ulusal ve uluslar arası dolaşımı mevzuat ve anlaşmaların yapılması,
- Elektronik imza yasası,
- Elektronik imza ile ilgili yönetmelik,
- Elektronik arşivle ilgili yasal mevzuat.

7.12.2 İdari altyapı

Elektronik İmza Yasası ile idari sorumlu tamamen Türk Telekomünikasyon Üst Kurumu olarak tayin edilmiştir. Yönetmelik gereği nitelikli sertifika sağlayıcı kurumların yetkilendirme işlemlerinden tutun uygulamadaki kurallara kadar hazırlanmış bulunmaktadır. Uluslar arası bilgi değişim modülü ve anlaşmalar konusunda Adalet Bakanlığı, Dış Ticaret Müsteşarlığı, Gümrük Müsteşarlığı ve Bankalar Birliği ile ortak çalışma başlatması beklenilmektedir. Elektronik Arşiv konusu ve veri değişim standartları konusunda Başbakanlık Arşivler Genel Müdürlüğü ilgili mevzuatı çıkarmış ve bundan sonra kurumların yazışma ve değişim modüllerinde uyacağı kurallar belirlenmiştir.

7.12.3 Teknik altyapı

ESHS'lerin yayınladığı Nitelikli Elektronik Sertifikaların uluslar arası çapta da geçerliliğine ihtiyaç olabilir. Bu amaçla, ulusal ve uluslar arası çapta birlikte çalışabilirliği ve uyumluluğu sağlamak üzere önerilmiş ve geliştirilmiş birçok yöntem vardır. ESHS'ler arası karşılıklı çalışabilirlik, herhangi bir yöntemle ESHS'ler arasında kurulan güven ilişkisine dayanır. Çeşitli uluslar arası ESHS'lar tarafından kullanılmakta ve/veya test edilmekte olan bazı yöntemler aşağıda sıralanmıştır:

- Çapraz-Sertifikasyon
- Köprü ESHS
- Çapraz-Tanıma
- Sertifika Güven Listeleri

- Akreditasyon Sertifikası
- Mutlak Hiyerarşi
- Yetkilendirilmiş Yol Onaylama ve Bulma

Karşılıklı çalışabilirlik için AAA'lar ve ESHS'ler tarafından gerçekleştirme biçimine ve düzeyine bağlı olarak bu önerilerden biri veya birkaç tanesi kullanılabilmektedir. Oluşturulmak istenen güven ilişkileri sağlanırken, belirli durumlarda ortaya çıkabilecek riskleri hafifletmek ve farklı türdeki problemleri gidermek üzere seçenekler arasından tercihler yapılabilir. Hangi güven formunun seçileceği genellikle kuruluş politikaları ile belirlenir.

- Çapraz sertifikasyon

Çapraz-sertifika, bir ESHS tarafından başka bir ESHS'ya, karşıdaki ESHS'nin genel anahtarını içerecek şekilde dijital olarak imzalayıp yayınladığı genel anahtar sertifikasıdır. Temel olarak bir ESHS kullanıcılarının, kendi ESHS'leri ile çapraz-sertifikalandırılmış diğer ESHS kullanıcılarına güven duymasıdır. ESHS'ler arasında Çapraz-Sertifikasyon gerçekleştirilirken çalışma ilkeleri, birbirlerine duyacakları güven düzeyi (tamamen eş-düzeyli veya belirledikleri güven düzeyleri arasında eşleştirme biçiminde olabilir) ve teknik bağlantılarla ilgili karşılıklı uzlaşmaya varmış olmaları gerekir[91].

- Köprü ESHS

Köprü ESHS, "merkez-ve-konuşma" diye de adlandırılan özel bir güven modeline dayanır. Ve kendisine üye olan ESHS'ler arasında "güven aracısı" olarak işlev görerek bu ESHS'lerin birbirini tanımasını kolaylaştırır (Şekil 7.6.). Köprü ESHS'ler, etki alanları arasındaki karşılıklı çalışabilirlik için geçerli eğilim olarak Çapraz-Sertifikasyon kullanırlar. Çapraz-Sertifikasyonun ESHS'lerin birbirleri arasında iki yönlü uygulanmasının ortaya çıkardığı en önemli sorunlardan birisi ölçeklenebilme problemidir. Az sayıda ESHS arasında iki yanlı Çapraz-Sertifikasyon kurulsa bile, bu durum oldukça önemsenecek bir yük getirebilmektedir. Köprü ESHS uygulanarak, bu yük ciddi anlamda azaltılabilir. ESHS'ler birbirleri ile iki yanlı Çapraz-Sertifikasyon kurmak yerine, Köprü ESHS ile bir veya birden fazla sertifika ilkesi kullanarak Çapraz-Sertifikasyon sağlarlar. Sertifika ilkelerinin eşleşmesi durumunda, Köprü ESHS üzerinden ESHS'ler arasında bir güvenilen yol ortaya çıkar.

Şekil 7.6. Köprü ESHS

Gerçekleştirilmiş bazı Köprü ESHS'ler aşağıda verilmiştir:

- Federal Bridge CA (ABD)
- DoD Bridge CA (ABD Savunma Birimi)
- EuroPKI (İtalya)
- European Bridge CA (Almanya)

- Çapraz tanıma

Çapraz-Tanıma, tanımlı bir kullanıcı topluluğunun, başka bir ESHS tarafından çıkarılan sertifikalara, belirli uygulamalarda kullanmak üzere güven duyabilmesi durumudur. Çapraz-Tanıma, Çapraz-Sertifikasyon ile birkaç bakımdan farklılığa sahiptir. Örneğin, ESHS'ler arasında iki yanlı tanınma söz konusu değildir. Diğer farklılıklardan bir diğeri ise, güven kararlarını ESHS'lerin değil, güvenen kısmın kendisinin yapmasının beklenmesidir. Çapraz-Tanıma, yüksek düzeyde güvencenin gerekli olduğu durumlarda pek kabul edilebilir çözüm olarak görünmemektedir.

- Sertifika güven listeleri

Sertifika Güven Listesi (SGL), güvenilen ESHS'leri içeren listedir. Güvenilen bir ESHS'nin genel anahtar sertifikasının bir özeti, Sertifika Güven Listesi içerisinde tanıtılır. SGL'ler, ilke tanımlayıcılarını ve eklentilerin kullanım desteğini de içerir. SGL'lerin güvenen tarafa taşınması için tanımlanmış bazı yöntemlerin dışında bant-dışı dağıtım mekanizması da kullanılabilmektedir.

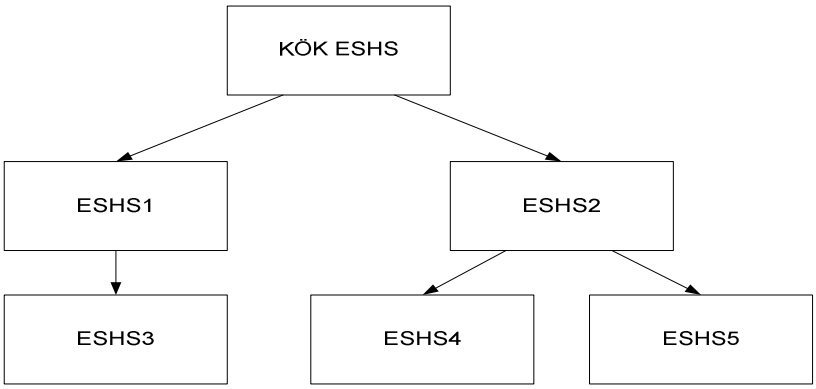
- Akreditasyon sertifikası

ESHS'ler arasında karşılıklı çalışabilirlik için çapraz-sertifikasyon ve çapraz-tanıma ile karşılaşılan bazı sorunların yaşanmaması için Geçiş Denetimi Akreditasyon Sertifikası uygulanabilir. Bu Akreditasyon Sertifikası, ulusal bazda kamu kurumları arasında merkezi ESHS tarafından akredite edilen ESHS'ler için verilebileceği gibi, uluslar arası boyutta da verilebilmektedir. Temel olarak, akredite edilmiş ESHS, akredite eden ESHS tarafından imzalanan kendi genel anahtarına sahip olmaktadır. Görünüşte, bir sonraki maddede bahsedilecek olan kök hiyerarşi kavramına çok benzese de, kök hiyerarşiden iki önemli farkı vardır. Birincisi, akredite edilmiş her ESHS'nin her biri kendisine has Sertifika İlkeleri ve Sertifika Uygulama Esaslarına sahip olabilmektedir. Diğeri de, ESHS'lerin, mutlak hiyerarşide genellikle izin verilmeyen kendi-imzalı genel anahtar sertifikasına sahip olabilmesine engel durumun olmamasıdır. Dolayısı ile akredite edilmiş ESHS'ler özerk yapılardır.

Akreditasyon Sertifikası, Çapraz-Tanımada olduğu gibi, Çapraz-Sertifika yayınlanmasını gerektirmez. Akreditasyon işlemi, akredite edecek ESHS'nin tanımladığı kriterlere göre gerçekleştirilir.

- Mutlak hiyerarşi

Mutlak Hiyerarşide, tüm "güven" ortak bir kök ESHS'den çıkar. Dolayısı ile etki alanındaki tüm güvenen taraflar için kök ESHS, güven noktasıdır. Alt ESHS'ler gerçekleştirilebiliyor olsa da, kök ESHS'ya dayandırılmış olmadığı takdirde alt ESHS'den yayınlanan herhangi bir sertifikaya güven duyulmayacaktır. Alt ESHS'lerin kendi-imzalı sertifikasına sahip olmasına izin verilmez, sadece kök ESHS kendi-imzalı sertifikasına sahip olabilir. Mutlak Hiyerarşideki yapılar bir kök ESHS ve sıfır veya daha fazla alt ESHS'den oluşur. Şekil 7.7.'de örnek bir Mutlak Hiyerarşi yapısı gösterilmiştir. Bu örnekte, kök ESHS sertifikaları iki alt ESHS'ye (ESHS1 Ve ESHS2) yayınlar ve daha sonra bu ESHS'ler de kendi alt ESHS'lerine sertifika yayınlarlar. En üstteki ESHS'nin yayınladığı sertifika, aslında iki-yanlı Çapraz-Sertifikadır.



Şekil 7.7. Mutlak Hiyerarşi

- Vekillendirilmiş yol onaylama ve bulma

Vekillendirilmiş yol onaylama, güven kararlarını güvenilen taraftan kısmen veya tamamen kaldırmaya izin verir. Bu da, istemci tarafında, güvenilen taraf gibi davranan ve gerektiğinde güvenilen bir üçüncü-parti sunucuya sorgu gerçekleştiren bir yazılım gerektirir. Güvenilen uzak sunucuya "bu sertifikaya güvenmeli miyim?" gibi basit bir istek sorgusu gönderilebildiği gibi, daha karmaşık sorgular da gerçekleştirilebilmektedir. Bu fonksiyonu desteklemek üzere tanımlanan herhangi bir protokol, istek içerisinde farklı düzeylere izin vermelidir.

Bu konuyu şekillendirmek üzere İnternet Görev Gücü (IETF) tarafından çalışmalar yapılmaktadır. Çevrimiçi Sertifika Durum Protokolü'nün ikinci versiyonu (On-Line Certificate Status Protocol – OCSP) ve ilişkili yol vekillendirme ve onaylama İnternet Taslaklarında belirtilen yöntemler ile bu durum başarılabilir. Diğer bir alternatif de, Basit Sertifika Onaylama Protokolü'dür (Simple Certificate Validation Protocol – SCVP). IETF'nin bu alternatiflerden birisini benimseyeceği beklenmektedir.

Bu seçenek her ne kadar, güvenen taraf ile güvenilen taraf arasında bilginin taşınması ve işlenmesi ile ilgili karmaşıklığı azaltması açısından cazip görünse de, bu uyumu sağlamak üzere gerçekleştirilecek arka-uç altyapısı oldukça karmaşıktır.

7.13 Değerlendirme ve Öneriler

ESHS'ler, anahtar çiftlerini ve nitelikli elektronik sertifikaları oluşturmak, bu sertifikaları korumak ve yayınlamak, anahtar çiftlerini güvenli şekilde üretmek ve korumak, gerektiğinde SİL'leri kullanıcılara sunmak ve gerekli her türlü güvenlik önlemini almak ve uygulamak zorundadır. E-imzanın yaygınlaştırılması, uygulanması konularda gerekli altyapıyı sağlayacak, hizmeti verecek ve yürütecek kurumlardır.

ESHS'lerin yapması gerekenler kanunlarda belirtilmiştir. Ülkemizde şuanda hizmet veren E-Güven, E-tuğra, TürkTrust ve UEKAE'e bulunmaktadır. Hizmet verecek olan bu kurumların kanuni sorumlulukları yerine getirmeleri, özelliklede konuya çok önem vermeleri ve bu ortamlara duyulabilecek güvensizliğin veya güven eksikliğinin e-imzanın yaygınlaşmasını olumsuz yönde etkileyeceğini unutmamalı bunun içinde çalışmalarını büyük bir sorumluluk içinde yürütmeleri gereklidir. Sayıları şu aşamada yeterli değildir. Çünkü bu sayı ne kadar çok olursa hizmet kalitesi artacak ve rekabet de o oranda artacaktır.

Bu kurumların ilk başlarda sıkıntılar duyacağı büyük ihtimaldir. Çünkü e-imzaya olacak güvensizlik, maliyetlerin yüksekliği, bu konuda ki bilgi eksikliği, kurumlarda çalışan kişilerde olabilecek zaaflar ve kişi ile e-imza arasında 3. kişi olacağından bu e-imza alacak kişilerde güvensizlik yaratacaktır. Bu konuda kişilere güven konusu mutlaka verilmeli, yüksek olan fiyatlar aşağı çekileli ve devlet vatandaşlarına destek vermelidir.

8. UYGULAMALAR

8.1 Web Tabanlı E-imza Uygulaması

Web tabanlı elektronik imza uygulaması elektronik imza mantığı üzerine oluşturulmuştur. Bu sistemde sunucu olarak apache web sunucusu, programlama dili olarak php ve veritabanı olarak da mysql kullanılmıştır. Programın oluşturulma ve çalışma şekli aşağıda sırayla verilmiştir:

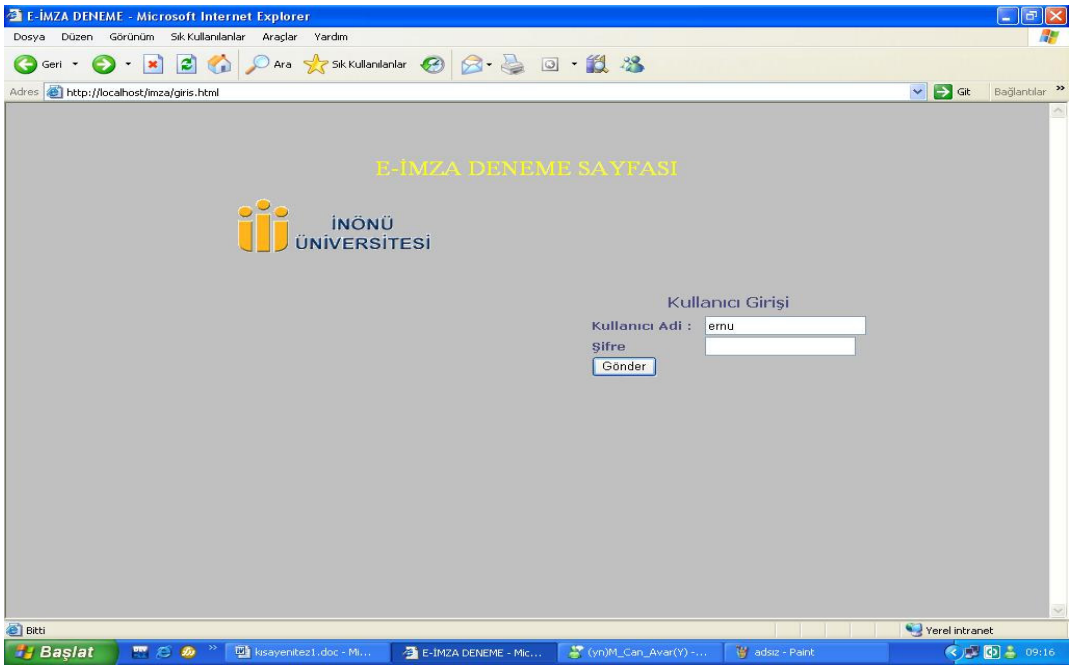
1. Program kisi, mesaj, sunucu olmak üzere 3 veri tabanından oluşmaktadır. Kisi veritabanında kişisel bilgiler ile kişiye verilen özel anahtar değeri bulunmaktadır. Mesaj kısmında ise kişilere gelen açık ve şifreli mesaj bilgileri tutulmaktadır. Sunucu veritabanında ise kişilere ait özel anahtar değerleri bulunmaktadır.
2. Program giris.html ile başlamaktadır. Burada kişi kendisine ait kullanıcı adı ve şifresi ile giriş yapıp, giris.php ile kontrol yapılıp giris.php sayfasına geçecektir. Yanlış kullanıcı adı ve şifre girdiği taktirde giris.php açılmayacak kullanıcıya hata mesajı verdirilip tekrar giris.html sayfası getirilecektir.
3. Giris.php sayfasında mesaj gönder ve mesaj okuma kısmı vardır. Mesaj gönder dendiği zaman mesaj gönderme formu gelmektedir. Bu formda mesajın kimden olduğu, kime gönderildiği ve mesaj kısmı bulunmaktadır. Gönder denildiği takdirde mesaj asimetrik algoritmadan geçirilip, kişi veritabanından çekilen kişiye ait özel anahtar kullanılarak şifrelenir, ayrıca MD5 kullanılarak mesaj özeti alınıp mesaj veritabanına kaydedilip, kullanıcının karşısına yeni bir form getirilmektedir. Bu formda açık mesaj, şifreli mesaj, mesaj özeti gözükmekte olup mesajın başarıyla iletildiği bilgisi verilmektedir. Gönderilen mesaj bilgileri ayrıca mesaj veritabanına kaydedilmektedir.
4. Mesaj oku kısmında ise kişiye gelen mesajlar listelenmekte doğrula dediği takdirde gönderen kişiye ait açık anahtar sunucu veritabanından alınarak deşifreleme işlemi yapılır. Bu şekilde mesajın gerçekten gönderen kişiden gelip gelmediği tespit edilir. Ayrıca gelen açık mesaj tekrar MD5 algoritmasından geçirilir ve mesaj özeti çıkarılır. Daha önce alınan mesaj özetiyle karşılaştırılarak mesajın içeriğinin değişip değişmediğinin tespiti yapılır.
5. Yukarıda bahsedilen aşamaların gerçekleşmesi esnasında kullanıcılara program aşamalarında yeterli düzeyde mesaj verilmiştir.

Programda kullanılan php ve html sayfalarının görüntüleri ve kodları aşağıda verilmiştir:

- giriş.html

```
<html><head>
<title>E-İMZA DENEME</title>
<meta http-equiv=”Content-Type” content=”text/html; charset=□lor□ws-1254”>
<meta http-equiv=”Content-Language” content=”tr” />
<meta http-equiv=”Content-Type” content=”text/html; charset=ISO-8859-9”>
<base target=”_self”></head>
 <body bgcolor=”#C0C0C0” text=”#4A4B80” link=”#4A4B80” vlink=”#00CCFF”
alink=”#000066”>  <table>   <tr><td> </td></tr> <tr><td> </td></tr> </table>
 <table width=”760” border=”0” align=”center” cellpadding=”0” cellspacing=”0”
height=”377”>
    <tr align=”center”>
    <td colspan=”2” background=”tablehead.gif” height=”26” width=”760”>
    <font color=”#FFFF00” size=”5”>E-İMZA DENEME SAYFASI</font></td>
   </tr> <tr><td height=”326” rowspan=”2” width=”388”>
    <div align=”right”>
     <table border=”0” cellspacing=”0” cellpadding=”0” width=”387” style=”border-collapse:
collapse” bordercolor=”#111111”>
       <tr>          <td align=”center” width=”387”> <p>
         <img border=”0” src=”logo.gif” width=”193” height=”72”></p>
         <p> <p> </p> <p> <p> </p> <p> </td>
       </tr>    </table>  </div>  <p> </p>   <p> </p>  <p> </p>  </td></tr>
  <TR>    <td height=”269” width=”372”>
<form action=”giris.php” method=”post” >
<table border=”0” align=”center” cellpadding=”0” cellspacing=”0” class=”formTable”
width=”264” height=”49”>  <tr>
          <td class=”labelcell” width=”264” colspan=”2” height=”29” >
          <p align=”center”><b> <font face=”Verdana, Arial, Helvetica, sans-serif”>Kullanıcı
Girişi</font></b></td>  </tr>
                <tr>
          <td class=”labelcell” width=”154” height=”22” ><b><font color=”#4A4B80” size=”2”
face=”Verdana, Arial, Helvetica, sans-serif”> Kullanıcı Adi :</font></b></td>
          <td class=”fieldcell” width=”110” height=”22”>
```

<input type=”text” name=”kulad” onFocus=”this.className=’boxFocus’” onBlur=”this.className=’boxBlur’” size=”20”>
</td> </tr> <tr>
<td class=”labelcell” width=”154” height=”21”>
Şifre</td>
<td class=”fieldcell” width=”110” height=”21”>
<input name=”sifre” onFocus=”this.className=’boxFocus’” onBlur=”this.className=’boxBlur’” size=”20” type=”password”></td>
</tr> <tr> <td align=”center” class=”fieldcell” width=”110” height=”1”>
<input type=”submit” value=”Gönder” face=”Verdana, Arial, Helvetica, sans-serif” style=”float: left”> </td> </tr> </table>
 </form></td> </tr> <tr>
<td align=”center” height=”26” colspan=”2” background=”tablehead.gif” width=”760” >   </td> </tr></table></body>
</html>

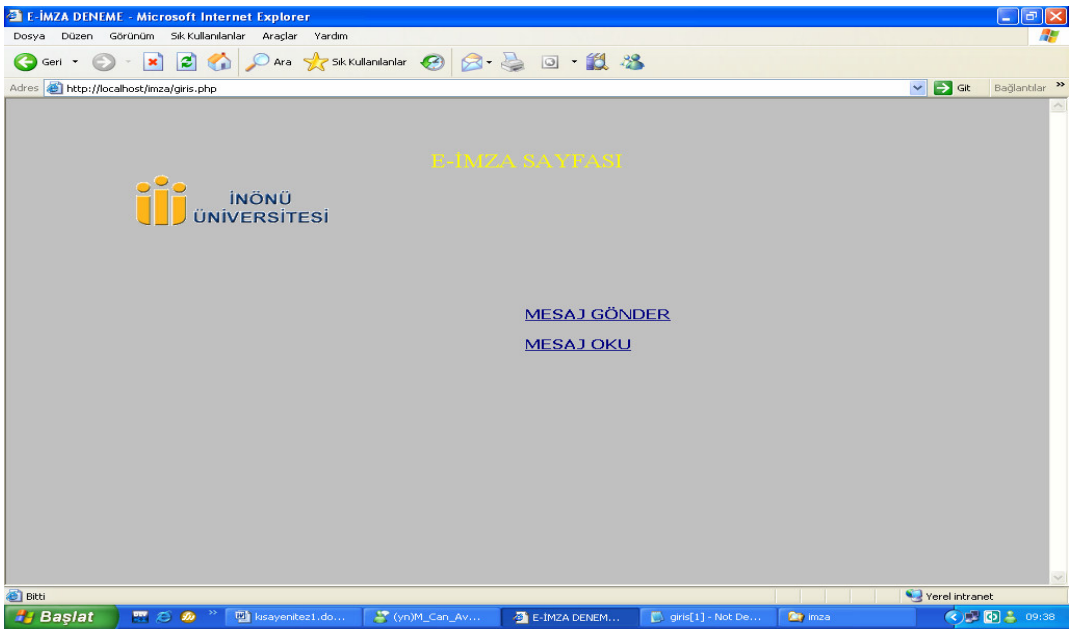


Şekil 8.1. Giriş Sayfası

- giris.php

<? $baglan=@mysql_connect(“localhost”,”root”,”ernu1981”);
if(!$baglan) {echo”bağlantı kurulamadı” ;exit(); }
if(!@mysql_select_db(“imza”,$baglan)){echo”veritabanı ile bağlantı kurulamadı” ; exit();}$result=mysql_query(“select * from kisi where kulad=’$kulad’ and sifre=’$sifre’”);

```
 $sor=mysql_numrows($result);
if ($sor!=1)
{echo"yanlış giriş yaptınız veya henüz oturum açmadınız.Lütden Giriş Yapınız";
include"giris.html"; exit();}
    $i = 0; while ( $i < $sor ) :
 $tckimlik = mysql_result($result,$i,"tckimlik");    ?>
<html><head><title>E-İMZA DENEME</title>
<meta http-equiv="Content-Type" content="text/html; charset=□lor□ws-1254">
<base target="_self"> </head>
 <body bgcolor="#C0C0C0" text="#4A4B80" link="#4A4B80" vlink="#00CCFF"
alink="#000066">   <table>  <tr><td> </td></tr> <tr><td> </td></tr> </table>
 <table width="760" border="0" align="center" cellpadding="0" cellspacing="0"
height="377">  <tr align="center"> <td colspan="2" background="tablehead.gif" height="26"
width="760"> <font color="#FFFF00" size="5">E-İMZA SAYFASI</font></td>  </tr>
 <tr><td height="326" width="268" align="left" valign="top"><img border="0" src="logo.gif"
width="193" height="72"><div align="right">  </div>      <p> </p>
       <p> </p>   <p> </p>   </td><td height="41" width="492">
  <p align="center"><b><font face="Verdana, Arial, Helvetica, sans-
serif">            
      </font></b>
          <p align="left"><b><font face="Verdana, Arial, Helvetica, sans-
serif">            
       <font
color="#000080">   </font> <a href="mgonder.php?kad=<?echo
$kulad;?>"><font color="#000080">MESAJ GÖNDER</font></a></font></b><p
align="left">
          <b><font face="Verdana, Arial, Helvetica, sans-
serif">            
       
          <font color="#000080">  </font> <a href="moku.php?kad=<?echo $kulad;?>&
tckimlik=<?echo $tckimlik?> ">
          <font color="#000080">MESAJ OKU</font></a></font></b></td></tr>
</table></body></html> <? $i++;endwhile;?>
```



Şekil 8.2. Anasayfa

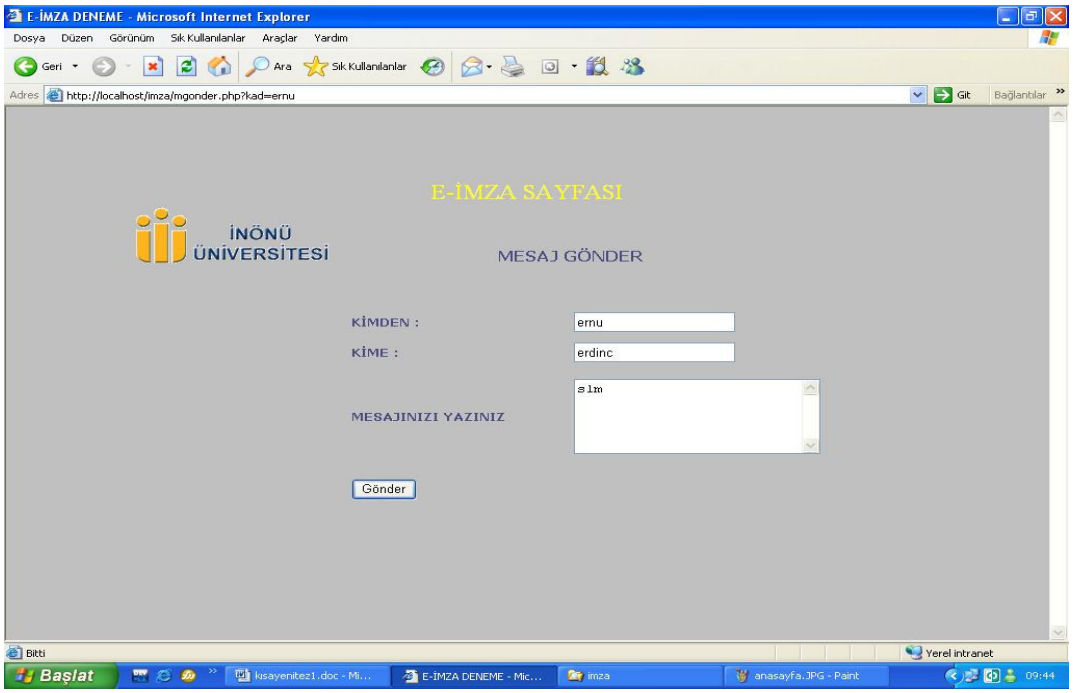
- mgonder.php

<html><head><title>E-İMZA DENEME</title><meta http-equiv=”Content-Type” content=”text/html; charset=□lor□ws-1254”><base target=”_self”></head>
<body bgcolor=”#C0C0C0” text=”#4A4B80” link=”#4A4B80” vlink=”#00CCFF” alink=”#000066”> <table> <tr><td> </td></tr><tr><td> </td></tr> </table>
<form action=”mesaj.php” method=”GET”>
<table width=”760” border=”0” align=”center” cellpadding=”0” cellspacing=”0” height=”377”> <tr align=”center”> <td colspan=”3” background=”tablehead.gif” height=”26” width=”760”> E-İMZA SAYFASI</td> </tr>
<tr><td height=”326” rowspan=”5” width=”129” align=”left” valign=”top”>
<img border=”0” src=”logo.gif” width=”193” height=”72”>

</td><td height=”21” width=”308” colspan=”2”>

<font face=”Verdana, Arial, Helvetica, sans-serif”>

```
MESAJ GÖNDER</font></b><p> </td></tr>
<tr><td height=”20” width=”154”><b><font color=”#4A4B80” size=”2” face=”Verdana,
Arial, Helvetica, sans-serif”> KİMDEN :</font></b></td><td height=”20”
width=”154”><input type=”text” name=”kad”  onFocus=”this.className=’boxFocus’”
onBlur=”this.className=’boxBlur’” size=”20”<?print “value=’$kad’”; ?>  </td></tr>
<tr><td height=”31” width=”196”> <b><font color=”#4A4B80” size=”2” face=”Verdana,
Arial, Helvetica, sans-serif”> KİME :</font></b></td><td height=”31” width=”306”><input
type=”text” name=”kulad” onFocus=”this.className=’boxFocus’”
onBlur=”this.className=’boxBlur’” size=”20”></td></tr>
<tr><td height=”46” width=”196”> <b>
        <font color=”#4A4B80” size=”2” face=”Verdana, Arial, Helvetica, sans-serif”>
        MESAJINIZI YAZINIZ</font></b></td><td height=”46” width=”306”>
  <textarea name=”diger” rows=”5” cols=”27”></textarea></td></tr>
<tr><td height=”45” width=”308” colspan=”2”><input type=”submit”  value=”Gönder”
face=”Verdana, Arial, Helvetica, sans-serif” style=”float: left”></td></tr>  </table>
</form></body></html>
```



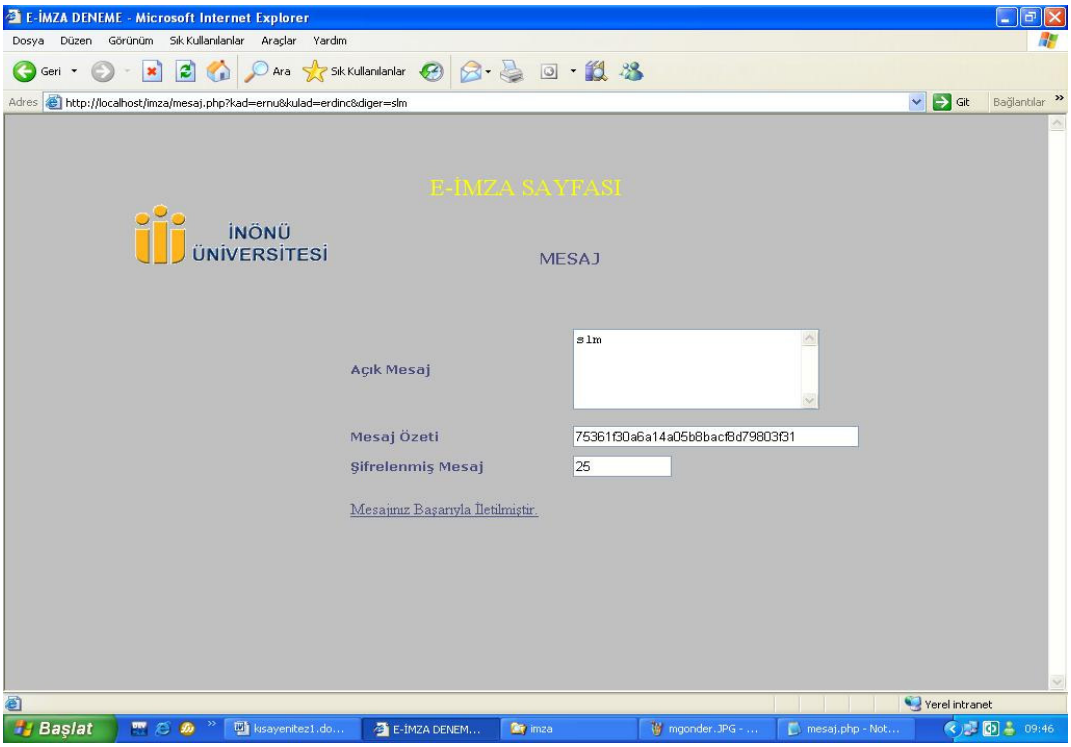
Şekil 8.3. Mesaj Gönderme Sayfası

- **mesaj.php**

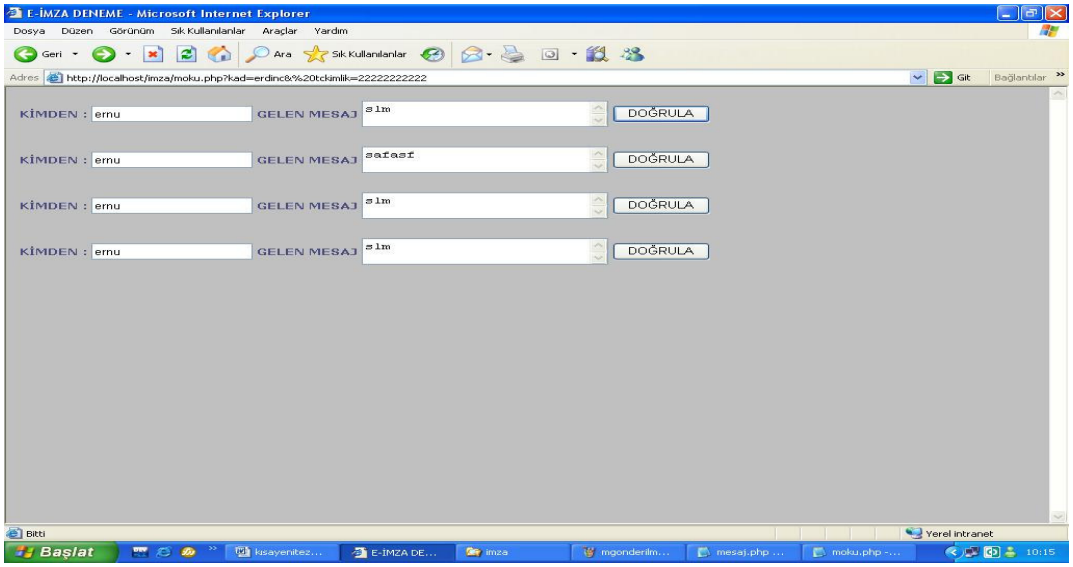
```
<? $d_kulad=$kulad;
$baglan=@mysql_connect(“localhost”,”root”,”ernu1981”);
        if(!$baglan)  {echo”bağlantı kurulamadı” ;exit(); }
```

```
        if(!mysql_select_db(“imza”,$baglan) ){echo “veritabanı ile bağlantı kurulamadı” ; exit();}
$result2=mysql_query(“select * from kisi where kulad=’$d_kulad’ “);
  $sor2=mysql_numrows($result2); if ($sor2!=1)
{echo “yanlış kullanıcı girdiniz”; include “mgonder.php”; exit(); }
$result=mysql_query(“SELECT * FROM kisi where kulad=’$kad’ “);
$satir=mysql_num_rows($result);  $i = 0; while ( $i < $satir ) :
  $d_sayisi = mysql_result($result,$i,”d_sayisi”);
  $n_sayisi = mysql_result($result,$i,”n_sayisi”);
  $gonderen_tckimlik=mysql_result($result,$i,”tckimlik”);
$sifre=mysql_result($result,$i,”sifre”);   $i++; endwhile;
$result1=mysql_query(“SELECT * FROM kisi where kulad=’$d_kulad’”);
$satir1=mysql_num_rows($result1);     $i = 0; while ( $i < $satir1 ) :
  $gelen_tckimlik= mysql_result($result1,$i,”tckimlik”);   $i++; endwhile;
$rasgele_mesaj_degeri=16; $s_mesaj=pow($rasgele_mesaj_degeri,$d_sayisi);
$sifreli_mesaj=$s_mesaj%$n_sayisi; $mesaj_ozeti=md5($diger);
mysql_query(“insert into mesaj values
(‘’,’$gonderen_tckimlik’,’$gelen_tckimlik’,’$kad’,’$diger’,’$mesaj_ozeti’,’$sifreli_mesaj’,’$ra
sgele_mesaj_degeri’)”) ?>
<html> <head> <title>E-İMZA DENEME</title>
<meta http-equiv=”Content-Type” content=”text/html; charset=□lor□ws-1254”>
<meta http-equiv=”Content-Language” content=”tr” /> <base target=”_self”>
</head> <body bgcolor=”#C0C0C0” text=”#4A4B80” link=”#4A4B80” vlink=”#00CCFF”
alink=”#000066”>  <table>  <tr><td> </td></tr>
<tr><td> </td></tr> </table> <table width=”760” border=”0” align=”center”
cellpadding=”0” cellspacing=”0” height=”377”>    <tr align=”center”>
   <td colspan=”3” background=”tablehead.gif” height=”26” width=”760”>
   <font color=”#FFFF00” size=”5”>E-İMZA SAYFASI</font></td>   </tr>
 <tr><td height=”326” rowspan=”5” width=”129” align=”left” valign=”top”>
        <img border=”0” src=”logo.gif” width=”193” height=”72”><div align=”right”>
     </div>     <p> </p>    <p> </p>          <p> </p>
   </td><td height=”21” width=”308” colspan=”2”>
  <p align=”center”><b><font face=”Verdana, Arial, Helvetica, sans-
serif”>            
      </font></b>
          <p align=”center”><b><font face=”Verdana, Arial, Helvetica, sans-
serif”>            
          
```

```
MESAJ</font></b><p> </td></tr> <tr><td height=”46” width=”196”>
  <b>  <font color=”#4A4B80” size=”2” face=”Verdana, Arial, Helvetica, sans-serif”>
       Açık Mesaj </font></b></td><td height=”46” width=”306”>
  <textarea name=”diger” rows=”5” cols=”27”  ><?print “$diger”;?></textarea></td></tr>
<tr><td height=”20” width=”154”>
  <b><font color=”#4A4B80” size=”2” face=”Verdana, Arial, Helvetica, sans-serif”>
       Mesaj Özeti</font></b></td><td height=”20” width=”154”>
        <input type=”text” name=”kad”  onFocus=”this.className=’boxFocus’”
onBlur=”this.className=’boxBlur’” size=”40”<?print “value=’$mesaj_ozeti’”; ?>  </td></tr>
 <tr><td height=”20” width=”154”> <b><font color=”#4A4B80” size=”2” face=”Verdana,
Arial, Helvetica, sans-serif”>Şifrelenmiş Mesaj</font></b></td><td height=”20”
width=”154”><input type=”text” name=”sifreli_mesaj”
onFocus=”this.className=’boxFocus’” onBlur=”this.className=’boxBlur’” size=”10”<?print
“value=’$sifreli_mesaj’”; ?>  </td></tr>
 <tr><td height=”45” width=”308” colspan=”2”>
        <a href=”giris.php?kulad=<?echo $kad;?> & sifre=<?echo $sifre;?>”> Mesajınız
Başarıyla İletilmiştir.</a></td></tr>  </table></body></html>
```



Şekil 8.4. Şifrelenmiş Mesaj Gösterme Sayfası



-

Şekil 8.5. Şifrelenmiş Mesaj Gösterme Sayfası

- moku.php

```
<html><head><title>E-İMZA DENEME</title><meta http-equiv=”Content-Type”
content=”text/html; charset=□lor□ws-1254”><base target=”_self”></head>
 <body bgcolor=”#C0C0C0” text=”#4A4B80” link=”#4A4B80” vlink=”#00CCFF”
alink=”#000066”>
<?$baglan=@mysql_connect(“localhost”,”root”,”ernu1981”);
        if(!$baglan)  {echo”bağlantı kurulamadı” ;exit(); }
       if(!mysql_select_db(“imza”,$baglan) )
       {echo “veritabanı ile bağlantı kurulamadı” ; exit();}
$result=mysql_query(“SELECT * FROM mesaj where gelen_tckimlik=’$tckimlik’ “);
$satir=mysql_num_rows($result); $i = 0;
while ( $i < $satir ) :
  $acik_mesaj = mysql_result($result,$i,”acik_mesaj”);
  $sifreli_mesaj=mysql_result($result,$i,”sifreli_mesaj”);
  $mesaj_ozeti= mysql_result($result,$i,”mesaj_ozeti”);
  $gelen=mysql_result($result,$i,”gelen”);  ?>
   <form action=”dogrula.php” method=”get”>  <table>  <tr><td>
   <b><font color=”#4A4B80” size=”2” face=”Verdana, Arial, Helvetica, sans-serif”>
         KİMDEN :</font></b></td><td>
              <input type=”text” name=”kulad” onFocus=”this.className=’boxFocus’”
onBlur=”this.className=’boxBlur’” size=”20” <?print “value=’$gelen’”; ?>  ></td> <td>
```

```
  <b><font face=”Verdana, Arial, Helvetica, sans-serif” size=”2”>GELEN </font>
        <font color=”#4A4B80” size=”2” face=”Verdana, Arial, Helvetica, sans-serif”>
        MESAJ</font></b></td><td>  <textarea name=”diger” rows=”2” cols=”27”><? Print
“$acik_mesaj”; ?></textarea></td> <td><input type=”submit”  value=”DOĞRULA”
face=”Verdana, Arial, Helvetica, sans-serif” style=”float: left”></td></tr> </table> </form>  <?
$i++;endwhile;?></body></html>
```

- dogrula.php

```
<? $d_kulad=$kulad;
$baglan=@mysql_connect(“localhost”,”root”,”ernu1981”);
        if(!$baglan) {echo”bağlantı kurulamadı” ;exit(); }
       if(!mysql_select_db(“imza”,$baglan) )
       {echo “veritabanı ile bağlantı kurulamadı” ; exit();}
$result=mysql_query(“SELECT * FROM kisi where kulad=’$d_kulad’ “);
$satir=mysql_num_rows($result);  $i = 0;
while ( $i < $satir ) :
   $tckimlik=mysql_result($result,$i,”tckimlik”);   $i++;
endwhile;
$result=mysql_query(“SELECT * FROM mesaj where gonderen_tckimlik=’$tckimlik’ “);
$satir=mysql_num_rows($result);  $i = 0;
while ( $i < $satir ) :
 $gelen_tckimlik=mysql_result($result,$i,”gelen_tckimlik”);
 $sifreli_mesaj=mysql_result($result,$i,”sifreli_mesaj”);
$mesaj_ozeti=mysql_result($result,$i,”mesaj_ozeti”);
  $sifrelenen_mesaj=mysql_result($result,$i,”sifrelenen_mesaj”);
  $i++; endwhile;
$result=mysql_query(“SELECT * FROM sunucu where tckimlik=’$tckimlik’ “);
$satir=mysql_num_rows($result);  $i = 0;
while ( $i < $satir ) :
   $e_sayisi=mysql_result($result,$i,”e_sayisi”);
$n_sayisi=mysql_result($result,$i,”n_sayisi”); $i++; endwhile;
$a_mesaj=pow($sifreli_mesaj,$e_sayisi);
$desifre_mesaj=$a_mesaj%$n_sayisi;
$mesaj_ozeti1=md5($diger);
if ($desifre_mesaj==$sifrelenen_mesaj) {echo “<b>Gönderen Kişi $d_kulad’dır</b>”;} else
{echo”<b>Gönderen kişi değildir</b>”;}echo “<br>”;
```

if($mesaj_ozeti1==$mesaj_ozeti) {echo “Mesaj Değişikliğe Uğramamıştır”; }else {
echo “ Fakat Mesaj Değişikliğe Uğramıştır”;}?>
Gönderen Kişi Doğru ise: “Gönderen Kişi Kullanıcı_adı ‘dır. Mesaj değişikliğe uğramamıştır” diye mesaj vercektir.
Gönderen Kişi Doğru Fakat Mesaj Değişti ise: “Gönderen Kişi Kullanıcı_adı ‘dır. Fakt Mesaj değişikliğe uğramıştır” diye mesaj vercektir.

8.2 RSA Algoritma Uygulaması

Bu uygulamamızda asimetrik algoritma yöntemlerinden olan RSA algritması kullanılarak yapılan şifrelemedir. 3 bölümden oluşmaktadır. Anahtar oluşturma bölümü, şifreleme bölümü ve deşifreleme bölümüdür. Bölümlerin görüntüleri ve kodları aşağıda belirtilmiştir.

- **Anahtar Oluşturma Bölümü(key.html**)

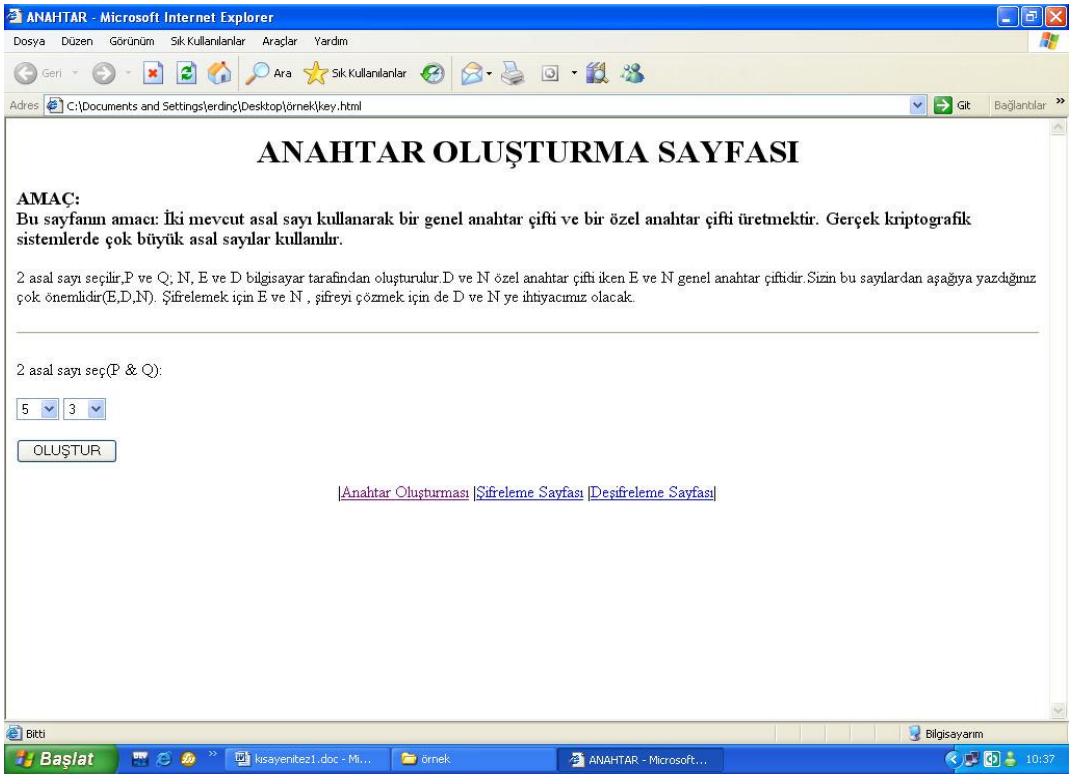
```
<html><head> <script><!—hide from old browsers var newWindow = null
function GCD(e,PHI) {
if (e > PHI) {
    while (e%PHI != 0) {
      a = e%PHI
       e = PHI
       PHI = a      }
    great = PHI
} else {
    while (PHI%e != 0) {
       a = PHI%e
       PHI = e
       e = a     }
    great = e}
return great }
function tofindE(PHI,P,Q) {
great = 0
e = 2
while (great != 1) {
    e = e + 1
    great = GCD(e,PHI)
```

```
    PHI = (P — 1) * (Q — 1) }
return e }
function extend(E,PHI) {
u1 = 1
u2 = 0
u3 = PHI
v1 = 0
v2 = 1
v3 = E
while (v3 != 0) {
    q = Math.floor(u3/v3)
    t1 = u1 — q * v1
    t2 = u2 — q * v2
    t3 = u3 — q * v3
    u1 = v1
    u2 = v2
    u3 = v3
    v1 = t1
    v2 = t2
    v3 = t3
    z = 1}
uu = u1
vv = u2
if (vv < 0) {
        inverse = vv + PHI
} else {
    inverse = vv}
return inverse }
 function result(form) {
var P = (form.prime1.options[form.prime1.selectedIndex].value)
var Q = (form.prime2.options[form.prime2.selectedIndex].value)
PHI = (P — 1) * (Q — 1)
E = tofindE(PHI,P,Q)
if (newWindow == null) {
    var newWindow = window.open("","","height=400,width=400")
    }
    newWindow.document.write("<html><body><b>")
```

```
    newWindow.document.write("N = P x Q = " + P + "x " + Q + "= ")
    newWindow.document.write(P * Q)
    newWindow.document.write("</b><br>")
    newWindow.document.write("PHI = (P-1)(Q-1) = " + PHI)
    newWindow.document.write("<br>")
    newWindow.document.write("Genel üs E bilgisayar ")
    newWindow.document.write("tarafından üretilecek ")
    newWindow.document.write("bu yüzden E ve PHI'nın en büyük ortak  ")
    newWindow.document.write("böleni 1 dir. Diğer bir deyişle, ")
    newWindow.document.write("E,PHI ile asaldır.")
    newWindow.document.write("<br>")
    newWindow.document.write("<b>E = " + E)
        newWindow.document.write("</b><p>")
    newWindow.document.write("N ve E açık anahtarlar mı? . Senin ")
    newWindow.document.write("özel anahtarın (D) E mod PHI'nın ")
    newWindow.document.write("tersidir.")
    newWindow.document.write("<p>")
    newWindow.document.write("Öklid algoritması ")
    newWindow.document.write("kullanılarak, Özel anahtar, <b>D, ")
    newWindow.document.write(extend(E,PHI)+" dir ")
    newWindow.document.write("<p> N, E ve D'yi kaydetmeyi unutma!")
    newWindow.document.write("</b><p> Şimdi, Erdinç'e genel anahtar çifti ")
    newWindow.document.write("N ve E'yi verebiliriz ")
    newWindow.document.write("öyleyse gönderilen bu anahtarlar kullanılarak ")
    newWindow.document.write(" veri şifrelenir. Daha sonra, D ve N 'yi  ")
    newWindow.document.write("kullanarak şifrelenmiş veriyi çözebilirsin")
    newWindow.document.write("</body> </html>")
    newWindow.document.close()
}// end script hiding → </script> <title>ANAHTAR</title></head>
<body bgcolor="FFFFFF"><center>
<h1>ANAHTAR OLUŞTURMA SAYFASI</H1> </center>
<font size=+1><b>AMAÇ:</b><br>
Bu sayfanın amacı: İki mevcut asal sayı kullanarak bir genel anahtar çifti ve bir özel anahtar
çifti üretmektir. Gerçek kriptografik sistemlerde çok büyük asal sayılar kullanılır.
</font> <p>
```

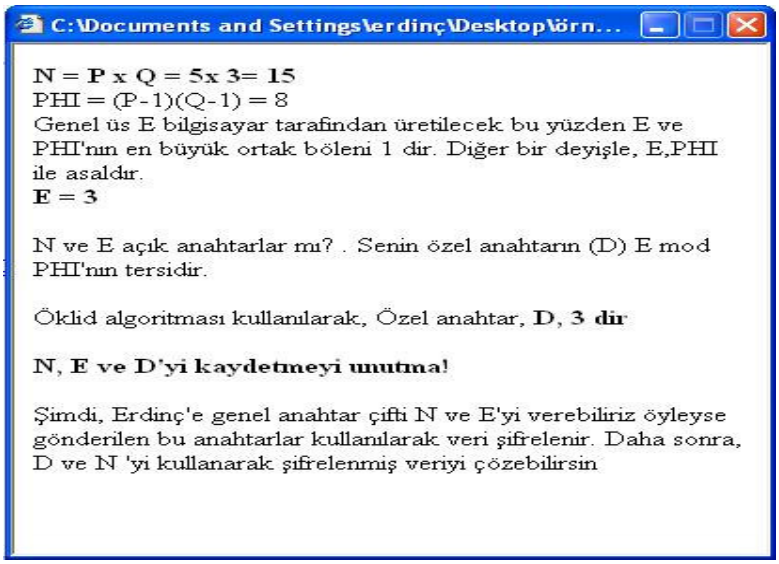
2 asal sayı seçilir,P ve Q; N, E ve D bilgisayar tarafından oluşturulur.D ve N özel anahtar çifti iken E ve N genel anahtar çiftidir.Sizin bu sayılardan aşağıya yazdığınız çok önemlidir(E,D,N). Şifrelemek için E ve N , şifreyi çözmek için de D ve N ye ihtiyacımız olacak.

```
<p> <hr> <p>2 asal sayı seç(P & Q): <form>
<select name=”prime1”> <option value=”5” selected>5
<option value=”7”>7 <option value=”11”>11 <option value=”13”>13
<option value=”17”>17 <option value=”19”>19 <option value=”23”>23
<option value=”29”>29 <option value=”31”>31 <option value=”37”>37
</select> <select name=”prime2”>
<option selected value=”3”>3 <option value=”5”>5
<option value=”7”>7 <option value=”11”>11 <option value=”13”>13
<option value=”17”>17 <option value=”19”>19 <option value=”23”>23
</select> <p>
<input type=”□uton” value=”OLUŞTUR” onClick=”result(this.form)”>
</form> <p>
<center> |<a href=”key.html” target=””>Anahtar Oluşturması</a> |<a href=”sifre.html” target=””>Şifreleme
   Sayfası</a> |<a href=”desifre.html” target=””>Deşifreleme Sayfası</a>|
 </center> </body> </html>
```



Şekil 8.6. Anahtar Oluşturma Sayfası

Oluştur dendiği zaman çıkan mesaj ve kodu aşağıdadır:



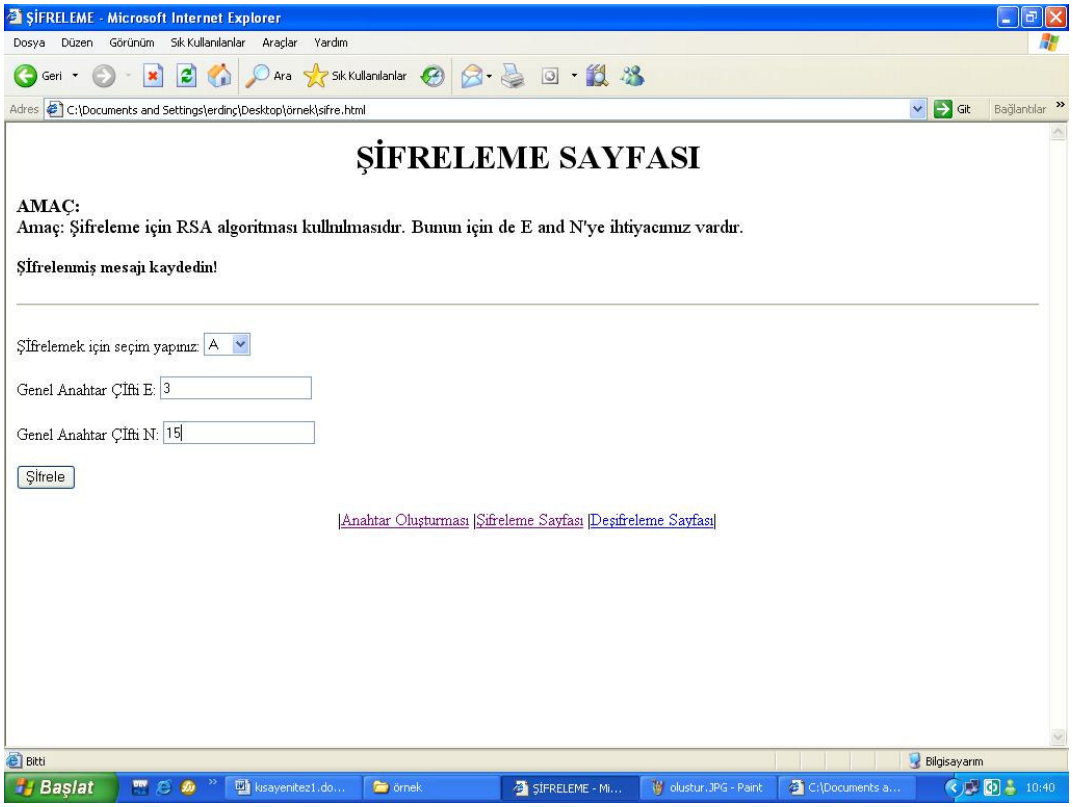
Şekil 8.7. Oluştur dendiğinde gelen mesaj

<html><body>N = P x Q = 5x 3= 15
PHI = (P-1)(Q-1) = 8
Genel üs E bilgisayar tarafından üretilecek bu yüzden E ve PHI'nın en büyük ortak böleni 1 dir. Diğer bir deyişle, E,PHI ile asaldır.
E = 3<p>N ve E açık anahtarlar mı? . Senin özel anahtarın (D) E mod PHI'nın tersidir.<p>Öklid algoritması kullanılarak, Özel anahtar, D, 3 dir <p> N, E ve D'yi kaydetmeyi unutma!<p> Şimdi, Erdinç'e genel anahtar çifti N ve E'yi verebiliriz öyleyse gönderilen bu anahtarlar kullanılarak veri şifrelenir. Daha sonra, D ve N 'yi kullanarak şifrelenmiş veriyi çözebilirsin</body> </html>

- Şifreleme bölümü

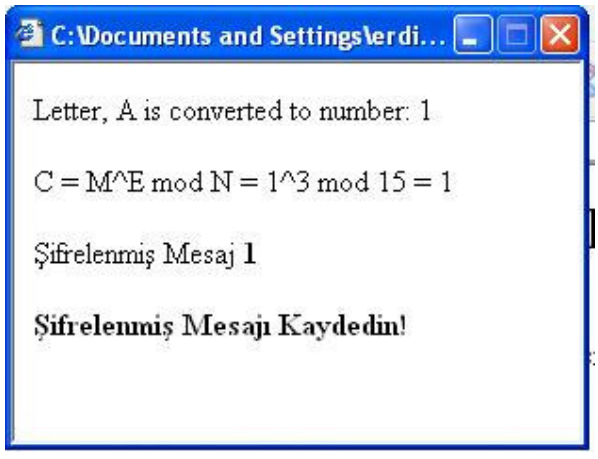
```
<html><head><title>ŞİFRELEME</title>
<script language="javascript"><!—hide from old browsers
var newWindow = null
function result(form) {
var M = (form.message.options[form.message.selectedIndex].value)
var U = (form.message.options[form.message.selectedIndex].text)
var E = form.exponent.value
var N = form.Nvalue.value
C = Math.pow(M,E) % N
if (newWindow == null) {
    var newWindow = window.open("","","height=200,width=300")     }
```

```
    newWindow.document.write("<html><body bgcolor='FFFFFF'>")
    newWindow.document.write("Letter, " + U + " is converted to")
    newWindow.document.write(" number: " + M)
    newWindow.document.write("<p> C = M^E mod N = ")
    newWindow.document.write(M + "^" + E+" mod "+N+" = "+C)
    newWindow.document.write("<p>Şifrelenmiş Mesaj <b>" + C)
    newWindow.document.write("<p>Şifrelenmiş Mesajı Kaydedin!</b>")
    newWindow.document.write("</body></html>")
    newWindow.document.close() }// end script hiding → </script>
<body bgcolor="FFFFFF"> <center> <h1>ŞİFRELEME SAYFASI</H1>
</CENTER> <font size=+1> <b>AMAÇ:</b><br>
Amaç: Şifreleme için RSA algoritması kullnılmasıdır. Bunun için de  E and N'ye ihtiyacımız
vardır.</font> <p><b>Şifrelenmiş mesajı kaydedin!</b><p><hr><p>
<form> <p>Şifrelemek için seçim yapınız:<select name="message">
<option selected value="1">A <option value="2">B <option value="3">CE
<option value="4">D <option value="5">E <option value="6">F
<option value="7">G <option value="8">H <option value="9">I
<option value="10">J </select><p>
Genel Anahtar Çifti E: <input type="text" name="exponent" value=0> <p>
Genel Anahtar Çifti N: <input type="text" name="Nvalue" value=0><p>
<input type="□uton" value="Şifrele" onClick="result(this.form)"><p>
</form> <center> |<a href="key.html" target="">Anahtar Oluşturması</a> |<a
href="sifre.html" target="">
Şifreleme Sayfası</a> |<a href="desifre.html" target="">Deşifreleme Sayfası</a>|
</center></body></html>
```



Şekil 8.8. Şifreleme Sayfası

Şifrele dendiği zaman çıkan mesaj ve kodu aşağıdadır:



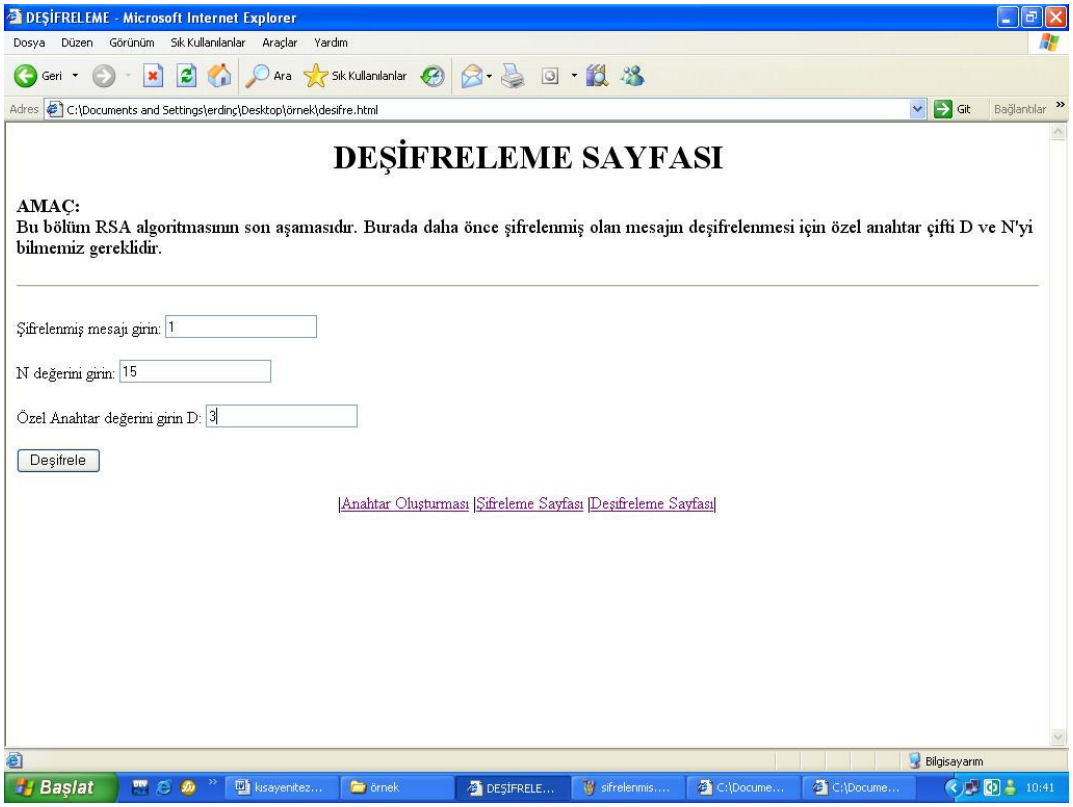
Şekil 8.9. Şifreleme sonrası gelen mesaj

<html><body bgcolor=’FFFFFF’>Letter, A is converted to number: 1<p> C = M^E mod N = 1^3 mod 15 = 1<p>Şifrelenmiş Mesaj 1<p>Şifrelenmiş Mesajı Kaydedin!</body></html>

- Deşifreleme Sayfası

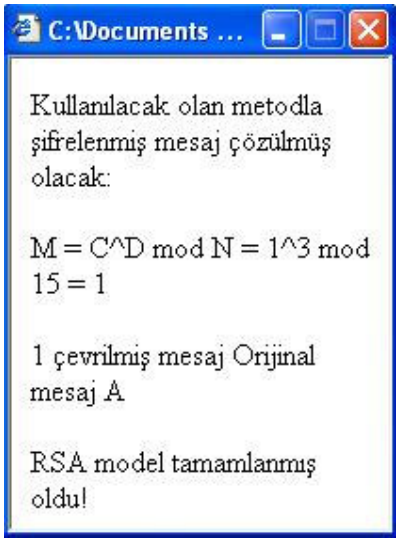
```
<html><head><title>DEŞİFRELEME</title><script language=”javascript”>
<!—hide from old browsers
var newWindow = null
function MakeArray(n) {
    this.length = n
    for (var i = 1; i <= n; i++) {
        this[i] = 0     }
    return this }
cipher = new MakeArray(10)
cipher[1] = “A”
cipher[2] = “B”
cipher[3] = “C”
cipher[4] = “D”
cipher[5] = “E”
cipher[6] = “F”
cipher[7] = “G”
cipher[8] = “H”
cipher[9] = “I”
cipher[10] = “J”

function result(form) {
var C = form.message.value
var N = form.Nvalue.value
var D = form.key.value
if ( D % 2 == 0) {
    G = 1
    for ( var i = 1; i <= D/2; i++) {
            F = (C*C) % N
            G = (F*G) % N   }
} else {
    G = C
    for ( var i = 1; i <= D/2; i++) {
            F = (C*C) % N
            G = (F*G) % N     }}
cipher = cipher[G]
```

```
if (newWindow == null) {
    var newWindow = window.open(“”,””,”height=250,width=200”)
    }
    newWindow.document.write(“<html><body bgcolor=’FFFFFF’>”)
    newWindow.document.write(“Kullanılacak olan metodla şifrelenmiş mesaj “)
    newWindow.document.write(“çözülmüş olacak:”)
    newWindow.document.write(“<p>”)
    newWindow.document.write(“ M = C^D mod N = “+C+”^”+D+” mod “)
    newWindow.document.write(N +” = “+ G)
    newWindow.document.write(“<p>”+G+” çevrilmiş mesaj “)
    newWindow.document.write(“Orijinal mesaj “ + cipher)
    newWindow.document.write(“<p>RSA model tamamlanmış oldu!”)
    newWindow.document.write(“</body></html>”)
    newWindow.document.close() }// end script hiding → </script>
<body> <center><h1>DEŞİFRELEME SAYFASI</h1></center>
<font size=+1> <b>AMAÇ:</b><br>
Bu bölüm RSA algoritmasının son aşamasıdır. Burada daha önce şifrelenmiş olan mesajın
deşifrelenmesi için özel anahtar çifti D ve N’yi bilmemiz gereklidir.
</font> <p> <hr> <p> <form>
Şifrelenmiş mesajı girin: <input type=”text” name=”message” value=0><p>
N değerini girin: <input type=”text” name=”Nvalue” value=0><p>
Özel Anahtar değerini girin D: <input type=”text” name=”key” value=0><p>
<input type=”□uton” value=”Deşifrele” onClick=”result(this.form)”> </form> <p><center>
    |<a href=”key.html” target=””>Anahtar Oluşturması</a> |<a href=”sifre.html”
target=””>Şifreleme
   Sayfası</a> |<a href=”desifre.html” target=””>Deşifreleme Sayfası</a>|
 </center> </body> </html>
```



Şekil 8.10. Deşifreleme Sayfası

Deşifrele dendiği zaman çıkan mesaj ve kodu aşağıdadır:

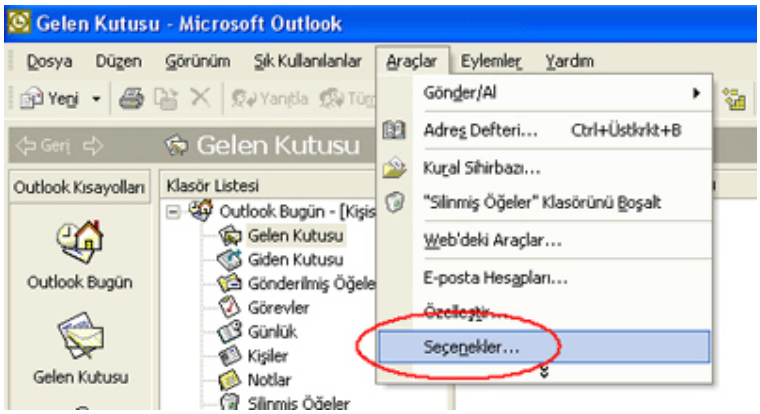


Şekil 8.11. Deşifreleme sonucu çıkan mesaj

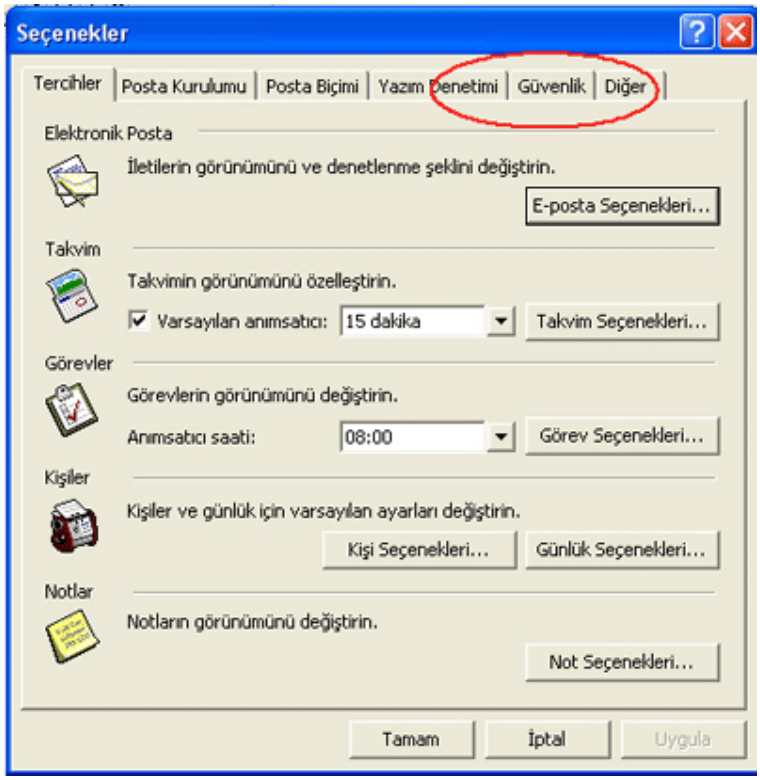
<html><body bgcolor='FFFFFF'>Kullanılacak olan metodla şifrelenmiş mesaj çözülmüş olacak:<p> M = C^D mod N = 1^3 mod 15 = 1<p>1 çevrilmiş mesaj Orijinal mesaj A<p>RSA model tamamlanmış oldu!</body></html>

8.3 Microsoft Outlook ile E-imza Gönderilmesi

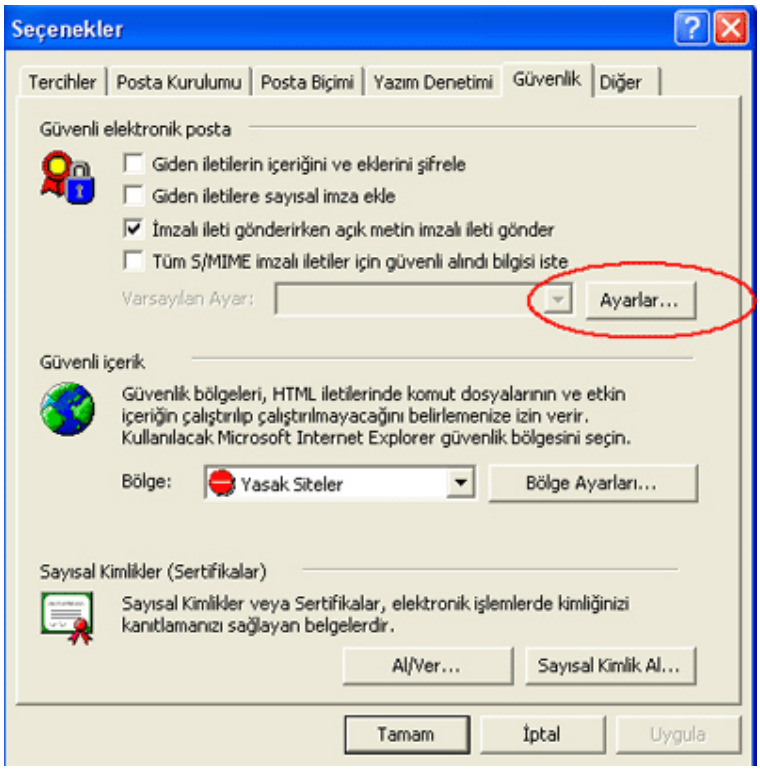
Araçlar menüsünden Seçenekler butonuna tıklayınız



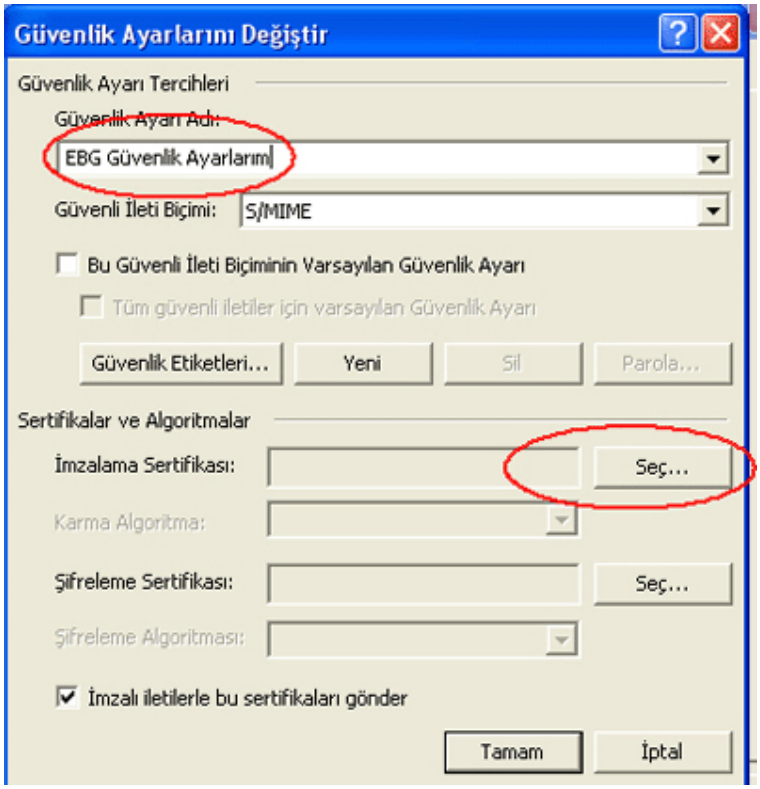
Seçenekler penceresinden Güvenlik sekmesine tıklayınız.



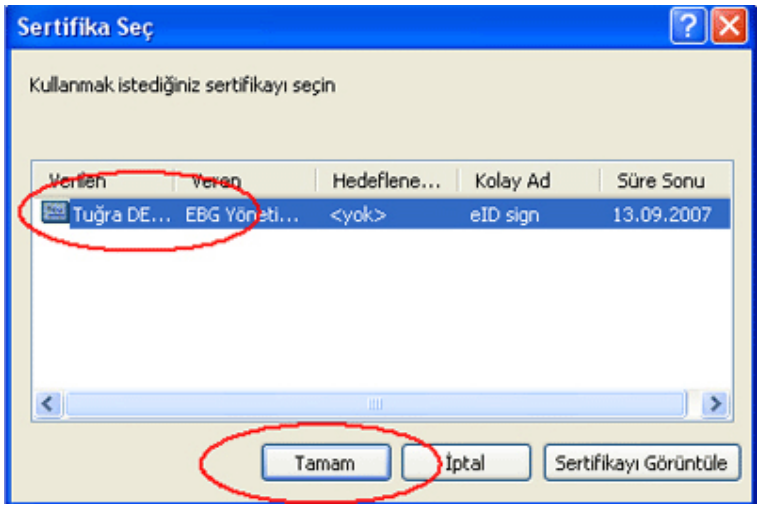
Güvenlik sekmesinden Güvenli elektronik posta seçeneğinin altında yer alan Ayarlar butonuna tıklayınız.



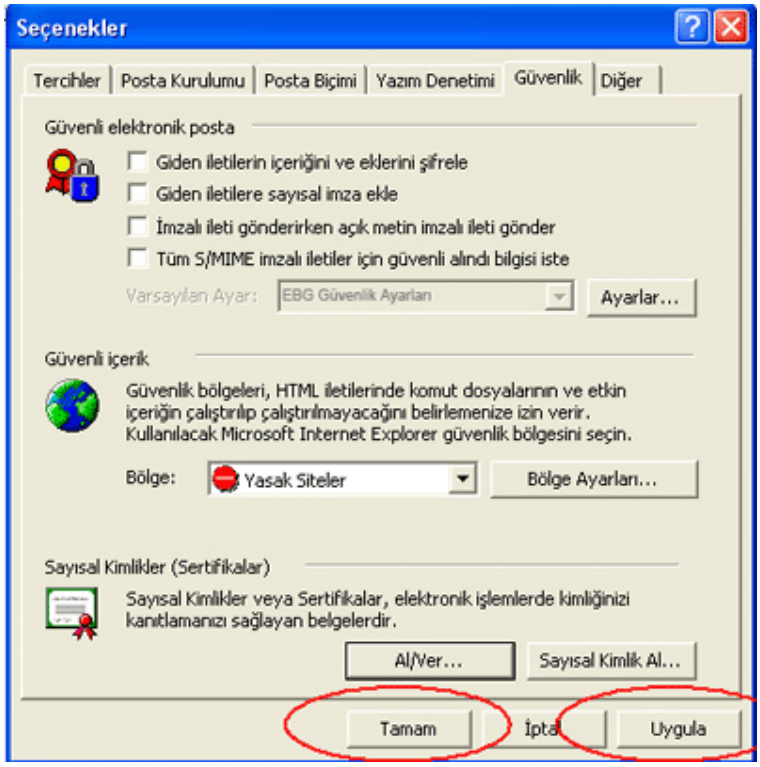
Güvenlik ayarlarından öncelikle yaptığınız ayar bir isim yazınız, sonrasında ise Seç butonuna tıklayınız



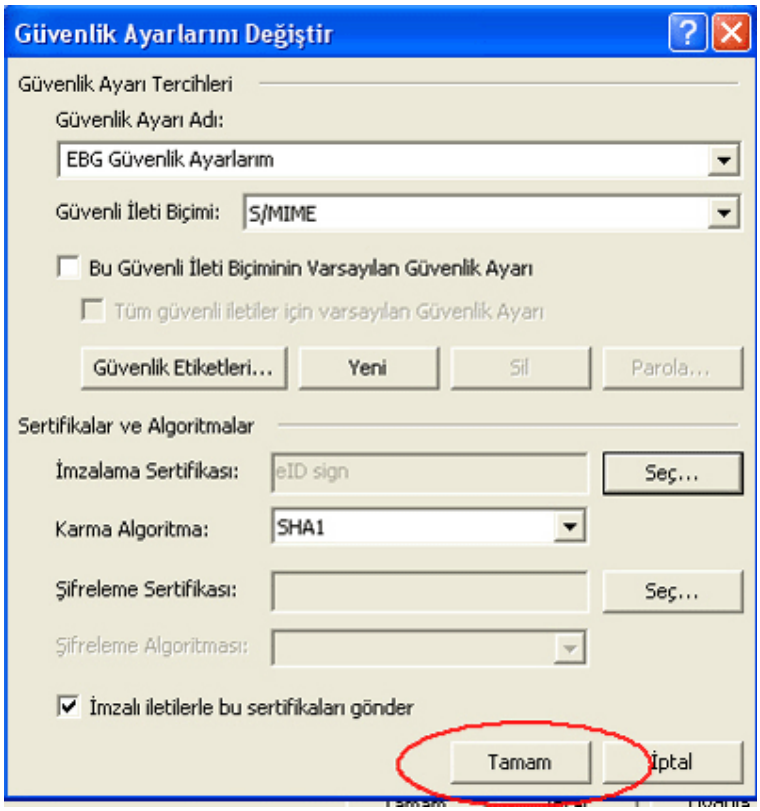
Sertifika seçeneklerinden nitelikli elektronik sertifikanızı seçiniz ve Tamam butonuna tıklayınız



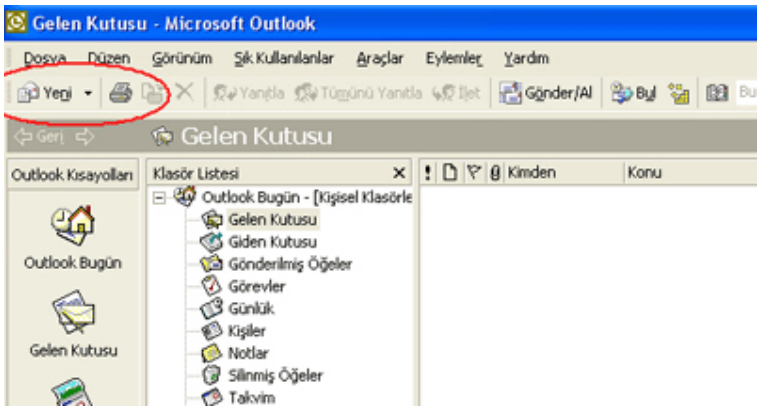
Seçenekler penceresinden sırasıyla Uygula ve Tamam butonlarına basınız



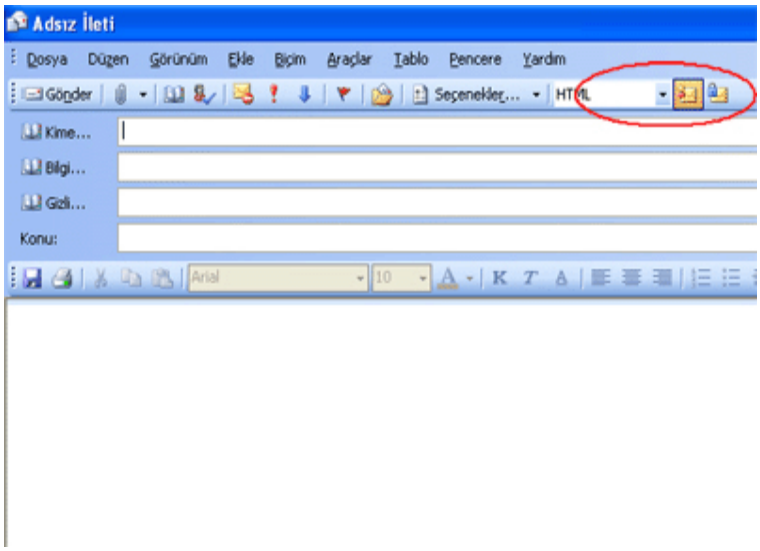
Güvenlik seçenekleri penceresinde yer alan Tamam butonuna tıklayarak ayarlarınızı tamamlayınız



E-imzalı e-posta göndermek için Yeni Posta İletisi oluştur butonuna tıklayınız



Açılan Yeni Posta İletisinde yer alan sertifika simgesini (kırmızı kurdele) tıklayınız. Gönder butonuna tıkladıktan sonra karşınıza gelen PIN giriş ekranına sertifika kullanım PIN kodunuzu giriniz ve ardından Tamam butonuna tıklayınız



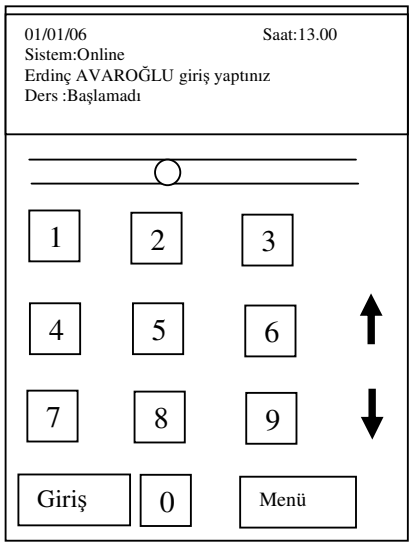
Tablo 8.1. Microsoft Outlook ile E-imzalı mail gönderme

8.4 Elektronik İmza ile Ders Takibi

Elektronik imza öğrenci kontrol sisteminde öğrencilere tekrar yazılabilir kontaksız kart vermek suretiyle öğrencilerin derse devamı sağlanmıştır. Öğrenciler sınıfa girerken kartını sınıfın girişinde bulunan okuyucuya gösterdiği anda okuyucu ekranın da öğrencinin ismi belirecek ve sistem tarih ve saat bilgileriyle beraber girişi kaydedilmiştir. Öğretim elemanının içeri girerken kartını okutması durumunda ders başlayacak ve o andan itibaren giriş yapan öğrencilerin bilgilerine geç geldiği işareti konulmuştur. Öğrenci istemesi halinde kendi kartını okutarak menü tuşuna bastığında kendi devam tablosu gösterilmiştir.

Sistem sınıf içerisine kurulacak bilgisayar sitemiyle öğrencilerin devam bilgileri takip edilecektir.

Bilgisayardaki bilgiler sistemde bulunan bir server üzerinde toplanacaktır. Cihaz içerisinde batarya kullanmak suretiyle elektrik kesintisi halinde çalışmaya devam edecektir. Cihazda bulunan dahili hafıza sayesinde bilgisayar bağlantısının olmadığı durumlarda (offline) log lar bellekte saklanıp online duruma geldiğinde aktarımı yapılacaktır.



Şekil 8.12. Kart Okuyucu Şeması

Yapılan bu uygulamadan beklenen yararlar ve ekonomiye olan katkısı aşağıda listelenmiştir.

a)Islak imza için sınıfta dolaşan bir kağıt olmayacak bu şekilde zaman kaybı ve karışıklıklar önlenmiştir.

b)Öğretim elemanlarının üzerindeki yük azalmıştır. Devam durumu daha kolay takip edimiştir.

c)Öğrencilerde mail yolu ile veya kart okuyucular aracılığıyla devam durumu bilgisini almışlardır.

d)Öğrenci işleri istediği takdirde veritabanından bu sorgulara ulaşabilecek öğrenci devam durumunu almışlardır.

9. SONUÇ

Bu çalışmada, e-imza konusunda ülkemizde oluşması gereken bilinç ve bilgi birikimine katkı sağlamak amacıyla bilgi ve bilgisayar sistemleri güvenliği, şifreleme bilimi, e-imza kavramı, e-imza teknik altyapısı (AAA) ve elektronik sertifikalar konusunda bir araştırma yapılamıştır. Özellikle konumuzun ana teması olan e-imzanın kişilere ne olduğunun tanıtılması, ne amaçla kullanıldığı, yararları, eksiklikleri, e-imza konusunda yaşanılan problemler ile e-imzada kullanılan altyapıdan bahsedilmiş olup e-imza sistemlerinin hayata geçirilmesinde dikkat edilmesi gereken hususlar ile e-imzanın yaygınlaşmasına yönelik öneriler sunulmuştur.

Dünyada 1996, ülkemizde de 2004 yılında hazırlana mevzuatlarla hukuki altyapısı belirlenmiş olan e-imza şuanda birçok ülkede yasal olarak uygulanmaktadır.

E-imza konusu oldukça yeni bir konudur. Bundan dolayı da bu konuda çok dikkatli davranmak gereklidir, aksi takdirde çeşitli riskler meydana gelecektir. Çünkü e-imza konusu direkt olarak "güvenlik" ile ilgili olduğu için önemi oldukça yüksektir. Bu yüzden e-imza sistemlerinde seçilecek olan yazılım, donanım ve hizmetler konusunda çok dikkatli olunması, bilinçli yaklaşılması, güvenirlik | süreklilik | kurumsallık sorgulamalarının iyi yapılması ve hizmet kalitesinin doğru değerlendirilmesi faydalı olacaktır.

E- imza kağıt ortamında yapılan işlemlere göre oldukça etkin ve verimli olacaktır. Geliştirilecek olan uygulamalar ile düşük maliyet, kağıt tüketiminde önemli bir azalma, sahtecilik ve dolandırıcılığın azalması, iş gücünün artması ve doğru kullanımı, haberleşme giderlerinde azalma sağlanmış olup böylelikle etkinliğin ve verimliliğin büyük ölçüde arttığı görülmüştür.

Eğer e-imza ve AAA sistemleri planlı bir şekilde kurulur ise kamu işlemleri (Vergiler, SSK, Bağkur vs.), kurumsal işlemler (Kimlik kartı, Personel kartı vs.), toplu taşıma işlemleri (Tren, Vapur vs.) vb. birçok işlem tek bir akıllı kart kullanılarak gerçekleştirilecektir.

E-imzanın bu kadar önemli katkıları olmasına karşın gelişmiş Avrupa ülkelerinde ve ülkemizde çok yaygın olarak kullanılmadığı görülmüştür. Bu yaptığımız çalışma sonucunda elde ettiğimiz veriler doğrultusunda ülkemizde e-imzanın daha rahat kullanımı ve yaygınlaşması için yapılabilecek öneriler aşağıda sunulmuştur:

- E-imza teknolojisi kullanabilmenin en önemli gereksinimlerinden ilki bilgisayar okur-yazarlığının arttırılmasıdır. Bu nedenle ülkemizde bilgisayar sahipliği ve okur-

yazarlığının yükseltilmesi konusunda çalışmalar yapılmalıdır. Yapılabilecek olan çalışmalar şu şekilde sıralayabiliriz:

- İlkokuldan itibaren başlamak koşuluyla kişilere bilgisayar eğitimi verilmelidir.
- Tüm okullarda bu konuda laboratuarlar kurulmalı ve bu hizmetlerinde tüm herkese açık olması sağlanmalıdır.
- Kamu kurum ve kuruluşlarında personele hizmet içi eğitim adı altında bilgisayar eğitimi verilmelidir.
- Kişilerin bilgisayar sahibi olabilmesi için bilgisayar parçalarına uygulanan KDV tutarının düşürülmesi veya tamamen kaldırılması gerekmektedir. En önemlisi artık ülke olarak bilgisayar parçalarını kendimiz üretecek konuma gelmeliyiz.
- Çeşitli kampanyalar düzenlenerek kişilere bilgisayar alımlarında kolaylıklar sağlanabilmelidir. Örneğin Milli Eğitim Bakanlığının öğretmenler ve akademisyenler için düzenlemiş olduğu veya öğrencilere özel 100$ 'lık laptop kampanyaları gibi uygulamalar düzenlenmelidir.

- E-imzanın toplumda yaygınlaşabilmesi için halkın e-imza kavramını ve e-imzanın hayatlarında sağlayacağı kolaylıklar hakkında bilgi sahibi olmaları sağlanmalıdır. Bu konuda birçok yerde e-imza tanıtımı için çeşitli seminerler düzenlenmeli, belirli yerlerde pilot uygulama alanları seçilip bilen kişiler gözetiminde bazı uygulamaların(SSK işlemleri gibi) kullanılması sağlanarak kişilere e-imza sonucunda işlemlerin ne kadar kolay, hızlı ve verimli bir şekilde gerçekleştiği gösterilmelidir.
- E-imzanın ülke genelinde yaygınlaşabilmesi için özellikle kamu kurumları seçilmelidir. Özellikle üniversiteler bu konuda ön ayak olmalıdır. Halka birebir ulaşabilmek için bazı muhtarlıklarda kişilerin çeşitli işlemleri yapmaları sağlanmalıdır. Bu ve benzeri uygulamalar sonucunda başarıya ulaşıldığı takdirde diğer alanlara geçiş daha kolay olacaktır.
- E-imzanın ilk uygulamaları kişilerin anlayabileceği ve uygulayabileceği sadelikte tasarlanmalıdır.
- Kurum ve kuruluşlar arasında AAA uygulamaları için mutlaka bir işbirliği sağlanmalı ve belirli bir standart oturtulmalıdır. Eğer bu sağlanamaz ise tüm kurumlar ayrı ayrı AAA ve e-imza uygulamaları yapacağından dolayı kurumlar arası entegrasyon sağlanamayacak ve bundan dolayı da işlemler sağlıksız ve verimsiz bir şekilde olacaktır. Buna imkan vermemek için kurumlarda e-imza çalışma grubu kurulmalı ve bu grupların toplanarak ortak kararlar almaları sağlanmalıdır.
- Devletin e-imzanın gelişmesi, kullanılması, benimsenmesi ve üretilmesi için tüm kurum ve kuruluşlar arasında katalizör görevi üstlenmesi gereklidir.

- Çeşitli dünya ülkelerinde e-imzanın kullanımı zorunlu hale getirilmiştir. Ülkemizde de bazı uygulamalarda e-imza zorunlu hale getirilmelidir.
- Kurumlar ihtiyaçlarına yönelik yapacakları yatırımlarda e-imzayı göz önünde bulundurmalı ve yapacakları ihaleleri kanunda belirtilmiş olan mevzuata uygun olarak hazırlamalıdır.
- Ülkemizin haberleşme altyapısının çok iyi olmadığını düşünürsek bu konuda da gerekli çalışmaların yapılması gereklidir. Bu altyapının gelişimi vergi veya katkı payları arttırılarak kişilere yüklemek yerine daha yeni politikalar ve yaklaşımlar üretilmelidir. Mevcut altyapının hızlandırılması, internet kullanımının yaygınlaştırılması için yeni stratejiler geliştirilmelidir. Bu gelişimler sağlandığı takdirde AAA ve e-imza yapılarının daha sağlıklı olarak kurulacağı, işleyeceği ve yaygınlaştırılacağı düşünülmektedir. Bu konuda şuanda hali hazırda Türk Telekomun yapmış olduğu telefon hatların üzerinden ADSL en önemli çalışmadır. Bu sayede birçok evde internet bağlantısı yapılmıştır. Telefon hatlarının yeteri kadar iyi olmaması dolayısıyla veri kayıpları meydana gelmekte ve verimli bir hizmet alınamamaktadır. Öncelikle hatların dijital teknolojiye uygun hale getirilmesi gerekmektedir. Ayrıca illere kurulacak olan wireless bağlantı ile istenilen yerlerde internet bağlantısı sağlanmalıdır. Bu sunduğumuz hizmetler çoğu Avrupa ülkelerinde ücretsiz olarak sunulmaktadır. Ülkemizde de bu hizmetlerin ücretsiz olarak sunulması en azından daha makul seviyelere çekilmesi gerekmektedir. Diğer en önemli sorun ise bu tür haberleşme kaynaklarımızın şuanda özelleştirme adı altında yabacı kurumlara satılmış olmasıdır. Güvenlik açısından çok büyük bir sorun olarak düşünülmektedir.
- E-imza ve AAA'nın hukuki, idari ve teknik olarak gelişmesi ve bu teknolojide kullanılacak yazılımların ülkemiz tarafından geliştirilmesi hem kişisel güvenliğimiz hem de ulusal güvenliğimiz açısından çok önemlidir.
- E-imza konusunda arada özel ESHS'ler olması kişilerde güvensizlik sorunu oluşturmaktadır. Bu sorunun ortadan kalkması için devlet tarafından bu görevin devlete bağlı olan bir kuruma verilmesi özelliklede sadece e-imza konusu ile ilgili bir kurum oluşturulup yetkinin bu kuruma verilmesi sağlanmalıdır.
- E-imza konusunda yasal olarak da birçok eksik bulunmaktadır. Bu eksiklikler aşağıda sıralanmıştır:

    - İmzanın nerelerde kullanılacağı net olarak belirtilmemiştir.
    - Sertifika iptal işlemleri kurumlara bırakılmış, hiçbir standart belirtilmemiştir.
    - Kamu kurumları denetim ve cezadan muaf bırakılmışlardır.
    - İmza sahibi her ne kadar kanunda tanımlanmış olsa da sorumlulukları hakkında bilgi verilmemiştir.

- Sertifikaların uluslar arası kullanımı için hiçbir standart belirtilmemiştir.
- İmza atma ve doğrulama için kullanılacak araçlar olan applet ve api adları yasada belirtilmemiştir.

Yukarıda belirtilen durumların kısa sürede düzenlenmesi gereklidir. Aksi taktirde e-imza konusunda belirli bir standart ve düzen söz konusu olamayacaktır. Özellikle aşağıdaki değişiklikler mutlaka yasalarımızda yapılmalıdır:

- E-imzaya tabi olmayan durumlar tek tek ifade edilmelidir.
- Sertifikalara ulusal hatta global çapta bir standartlaşma getirilmelidir.
- Api ve appletlerde standart belirlenmeli ve üretim yetkileri verilmelidir.
- Sertifika iptal işlemleri tüm kurumlar için belli standartlara oturtulmalıdır.
- Kamu kurumlarının ceza ve denetimlerden muaf olması hükmü yeniden düzenlenmelidir.

- Kanunlarda bulunan belgelerin asıllarının sunulma zorunluluğu kavramının e-belgenin durumu göz önüne alınarak yeniden düzenlenmesi gerekmektedir.
- Mahkemelerin e-imza altyapısına hazır hale getirilmelidir.
- E-imzada kullanılan teknolojiler yüksek maliyetlidir. Ayrıca kullanıcılar kart, kart okuyucu, token yazılımları, donanım gereksinimleri ve nitelikli sertifikalar gibi birçok yazılım ve donanıma ücret ödemek zorunda bırakılıyorlar. Ayrıca sertifikadan, sertifika sahibine doğabilecek zararlara karşı mali sorumluluk sigortası yapılması zorunluluğu getiriliyor. İşte bu ve bunun gibi yüksek maliyetler sebebiyle kullanıcılar ve e-imzaya geçmek isteyen kurumlar e-imzaya uzak durmaktadır. Bu durumun önüne geçebilmek için birçok dış ülkede olduğu gibi devletin kişi ve kurumlar üzerindeki maliyeti düşürmesi gerekmektedir.

Sonuç olarak:

- Bu çalışmada günümüzde e-imzanın güvenli bir şekilde uygulanabilmesi için birçok tedbir alınması gerekliliği görülmüştür.
- Uygulama güçlükleri getiren teknolojik, bireysel, uyumsal ve maddi sorunların bir an önce giderilmesi veya en aza indirgenmesi gerekliliği öngörülmüştür.
- Yasal düzenlemelerin asla ihmal edilememesi ve bu yasal düzenlemeler yapılmadan e-imzanın yaygınlaştırılmaması gerektiği sonucuna varılmıştır.
- Yasal düzenlemeler tam olarak oturduktan sonra e-imzanın mutlaka kullanılması gereken bir teknoloji olduğu sonucuna varılmıştır.

10. KAYNAKLAR

1. http://www.tdk.gov.tr
2. Bilgi Ağları Süleyman Sungur 2004,Huten
3. ULAKNET Sistem Yönetimi Konferansı Güvenlik 3-4 Ekim 2003, Ankara Dr. M. Ufuk Çağlayan)
4. The World Bank, World Development Indicators 2006
5. OECD, OECD Factbook 2006
6. (http://internetworldstats.com/eu/tr.htm)
7. Her yönüyle elektronik imza Doç.Dr. Şeref Sağıroğlu,Doç.Dr.Mustafa Aklan Ankara 2005
8. http://security.metu.edu.tr/belge.php?Bilgi_Guvenligi.html
9. http://tr.wikipedia.org/wiki/Bilgisayar_vir%C3%BCs%C3%BC
10. http://www.spam.org.tr/nedir.html
11. .http://email.about.com/od/spamandgettingridofit/a/what_is_spam.htm
12. http://www.iem.gov.tr/iem/?idno=147
13. http://www.webopedia.com/TERM/p/phishing.html
14. http://en.wikipedia.org/wiki/cracker_%28computing%29
15. [http://searchsecurity.techtarget.com/sDefinition/0,290660,sid14_gci214431,00.html]
16. http://searchsecurity.techtarget.com/sDefinition/0,290660,sid14_gci214431,00.html
17. Mezenes, A., J., Van Oorschot, P., C. and Vanstone, S., A., Handbook of Applied Crptography, CRC Press,October 1996
18. 24.Godlwasser, S.and Bellare, M., Lecture Notes on Cryptography,M.I.T. Loboratory for Computer Science,August 1999
19. http://www.kamusm.gov.tr/tr/Bilgideposu/Belgeler/teknik/aaa/index.html
20. http://www.olympos.org/article/articleview/265/1/10/ kriptografi___bolum_1_simetrik_kriptografi,http://world.std.com/~franl/crypto.html
21. http://en.wikipedia.org/wiki/Data_Encryption_Standard
22. http://www.schneier.com/essay-071.html
23. http://www.cryptographyworld.com/des.htm
24. Web Security: A Step-by-step Reference by Lincoln D. Stein (Paperback - 31 Jan 1998)
25. Nadehara, K. Ikekawa, M. Kuroda, I., Media & Inf. Res. Labs., NEC Corp., kawasaki, Japan, Signal Processing Systems, 2004. SIPS 2004. IEEE Workshop on, 152-157, 2004
26. http://csrc.nist.gov/CryptoToolkit/aes/
27. Twofish: A 128-Bit Block Cipher B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson 15 June 1998

28. On the structure of Skipjack ,Discrete Applied Mathematics, Volume 111, Issues 1-2, 15 July 2001, Pages 103-116, Lars Knudsen and David Wagner
29. [http://world.std.com/~franl/crypto.html]
30. Rivest, R., L.,Shamir, A.and Adleman, l:, A Method for Obtaining Digital Signatures and PublicKey Crytosystems, Comminicationa of the ACM, Vol.21, Nr.2,1978,120-126.
31. http://world.std.com/~franl/crypto/rsa-guts.html
32. http://www.cryptographyworld.com/rsa.htm
33. http://www.faqs.org/rfcs/rfc1321.html,Rivest, R., "The MD5 Message-Digest Algorithm",RFC 1321,1992
34. http://www.faqs.org/rfcs/rfc3174.html
35. http://www.schneier.com/blog/archives/2005/02/sha1_broken.html
36. Dobbertin H.,Bosselaers A., Preneel B.,"RİPEMD-160: A Strengthened Version of RİPEMD", Fast software Encryption,71-82,1996
37. http://www.msmproductionsltd.com/test_pgp.html
38. http://www.trincoll.edu/depts/cpsc/cryptography/pgp.html
39. http://www.ietf.org/html.charters/smime-charter.html
40. A generic characterization of the overheads imposed by IPsec and associated cryptographic algorithms , Computer Networks, Volume 50, Issue 17, 5 December 2006, Pages 3225-3241,Christos Xenakis, Nikolaos Laoutaris, Lazaros Merakos and Ioannis Stavrakakis
41. Reed, Chris, 'What is a Signature?', The Journal of Information, Law and Technology (JILT).2003/3,
42. 54.Mesut Orta Adalet Bakanlığı Bilgi İşlem Dairesi Başkanlığı Uygulamalı Elektronik İmza Semineri 20-21 Aralık 2005
43. Electronic signature legislation passed Joe Rice, Veincheck, UK Available online 11 April 2002.
44. State of North Dakota Information Technology Department October 2004
45. http://www.nd.gov/itd/records/e-signatureguidelines.pdf
46. http://www.infomosaic.net/electronic-signature.htm
47. Lupton W. Everett, The Digital Signature: Your Identity by the Numbers, 6 RICH. J.L. & TECH. 10 (Fall 1999)
48. Alkan, İnalöz, (Telekom Reg.), 2004, s.111.
49. Pınar ERDEM Dış Ekonomik İlişkiler Müdürlüğü Uzman Yardımcısı Ağustos,2005
50. www.turkpoint.com/e-yasam/sayisal imza.asp (01.12.2003)
51. Arıkan, Saadet., "Dünyada ve Türkiye'de Elektronik Ticaret Çalışmalarına Hukuki Bir Yaklaşım", Ankara 1999, s.151.

52. Electronic Signatures http://www.arx.com/products/cosign_faq.php
53. http://searchsecurity.techtarget.com/sDefinition/0,290660,sid14_gci211953,00.html 10 Jul 2006
54. Electronic signatures: technology developments and legislative issues Richard M. Nunnoa 6 october 2000
55. www.tk.gov.tr/eimza/eimza_yasasi.htm
56. Elektronik İmzalar İçin Topluluk Çerçevesi konusunda 13 Aralık 1999 tarihli 1999/93/AT sayılı Avrupa Parlamentosu ve Konsey Direktifi, Topluluk Resmi Gazetesi, No:L 013, 19.1.2000, s.0012-0020.
57. Keser Berber, "İmzalıyorum O Halde Varım" s.503
58. http://www.tk.gov.tr/eimza/E-Imza_Faydali_bilgiler.htm
59. http://www.maksimum.com/teknoloji/haber/30/38705.php
60. http://www.kirbas.com/index.php?id=202&sec=e-imza
61. http://www.e-imza.gen.tr/
62. KAHRAMAN, Alaaddin, "Elektronik İmza Uygulaması", Yerel Yönetim ve Denetim Dergisi, Sayı:3, Cilt:10, Mart 2005, ss.16-17.
63. http://shiftdelete.net/site/content/view/308/62/
64. http://www.e-ticaret.gov.tr/hukuk/uncitral.htm
65. E-imza Uygulamalarında AB ve Türkiye'de Mevcut Durum ve Öneriler Sezen Yeşil, Mustafa Alkan, Tayfun Acarer, 7-8 Aralık 2006 Ulusal Elektronik İmza Semineri
66. Ab Komisyonunun 15.3.2006 Tarihli Raporu 16a Yrd. Doç. Dr. Şafak Ertan Çomaklı Atatürk Üniversitesi İktisat Bölümü 5070 Sayılı Elektronik İmza Kanunu Uygulaması Ve Hukuki Sonuçları 04/04/2006
67. E-İmza Ulusal Koordinasyon Kurulu Altyapı Çalışma Grubu İlerleme Raporu
68. Türkiye'de Kamu Kurumlarının Elektronik İmza Altyapı ve Uygulamalarının Değerlendirilmesi T.Kaya Bensghir, Ferda Topcan, 7-8 Aralık 2006 Ulusal Elektronik İmza Semineri
69. TBD Kamu-BİBKamu Bilişim Platformu VII 26-29 Mayıs 2005 Antalya
70. http://www.pki.iam.metu.edu.tr/
71. PKI Jim Brayton, Andrea Finneman, Nathan Turajski, and Scott Wiltsey 10 Oct 2006
72. A Survey of Public-Key Cryptosystems, cSIAM REVIEW 2004 Society for Industrial and Applied Mathematics, Neal Koblitz, Alfred J.Menezes,
73. http://www.sun.com/blueprints/0801/publickey.pdf]
74. Bilgi ve Bilgisayar Güvenliği Dersi Araştırma Projesi, Hüseyin Erol, Ankara, 2004
75. http://www.kamusm.gov.tr/tr/Urunler/Yazilimlar/
76. http://www.bilten.metu.edu.tr/Web_2002_v1/tr/sayfa_d4.asp?sayalim=sayfa_d4

77. http://www.turktrust.com.tr/
78. http://www.uekae.tubitak.gov.tr/
79. www.e-guven.com/
80. http://www.e-tugra.com/
81. TBD Kamu-BİB Kamu Bilişim Platformu VII 26–29 Mayıs 2005 Antalya
82. http://seminer.linux.org.tr/konferanslar/inet-tr98/ppthtml/bd-abc-certs/bd-abc-certs.ppt
83. http://www.genbilim.com/content/view/470/91/
83. Elektronik sertifika hizmet sağlayıcılığı, Veysi SEVİĞ, Dünya Gazetesi, 16.02.2005
85. http://www.e-imza.gen.tr/index.php?Page=Sss&SssNo=49,
86. http://www.globalsign.com.tr/sertifikalar/wildcard.asp
87. http://www.itsweden.com/docfile/34608_n2000_35e.pdf
88. http://www.nbusr.sk/en/electronic-signature/products-certification-for-qualified-electronic-signature/index.html
89.www.pts.se/Archive/Documents/SE/engelsk%20oversattning%20av%20lag%20elektroniska%20signaturer.pdf
90. The digital signature paradox Stapleton, J.; Doyle, P.; Esquire, S.T.;Systems, Man and Cybernetics (SMC) Information Assurance Workshop, 2005. Proceedings from the Sixth Annual IEEE 15-17 June 2005,
91. http://dijital-imza.com/sorular.htm#004
92. http://tr.wiktionary.org/wiki/zaman_damgas%C4%B1
93. http://www.kobitek.com/makale.php?id=66
94.http://www.eticaret.gov.tr/Toplanti/T%C3%BCrkiyede%20Elektronik%20imza%20Uygulamari.doc
95. http://en.wikipedia.org/wiki/Root_certificate
96. http://www.globalsign.com.tr/destek/dijital_sertifika_body.asp
97.http://publib.boulder.ibm.com/iseries/v5r1/ic2924/index.htm?info/rzahu/rzahurzahu02mcertificateauthority.htm

11. ÖZGEÇMİŞ

Erdinç Avaroğlu 27.07.1979 tarihinde Adana'nın Karataş ilçesinde doğmuştur. İlk, orta ve lise öğrenimini Adana'da tamamlamıştır. Mersin Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği bölümünden 2001 yılında mezun olmuştur. 2001–2003 yılları arasında askerliğini yedek subay olarak tamamlamıştır. Askerden döndükten sonra Merdin Bimeks Bilgi İşlem A.Ş.'de teknis servis sorumlusu olarak göreve başlmıştır. 6 ay sonunda bu işinden ayrılıp mikrosoft sistem mühendisliği kursuna başlamıştır. Kurs devam ederken 2003 yılı sonunda kursdan ayrılarak İnönü Üniversitesi Enformatik Bölüm Başkanlığında göreve başlamıştır. Halen buradaki görevine devam etmektedir.