KURUMSAL AĞLARDA AÇIK ANAHTAR ALTYAPISI TABANLI ELEKTRONİK İMZA UYGULAMASI

Hüseyin EROL

YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

EKİM 2006
ANKARA

Hüseyin EROL tarafından hazırlanan KURUMSAL AĞLARDA AÇIK ANAHTAR ALTYAPISI TABANLI ELEKTRONİK İMZA UYGULAMASI adlı bu tezin Yüksek Lisans tezi olarak uygun olduğunu onaylarım.

Doç.Dr. M.Ali AKÇAYOL
Tez Yöneticisi

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

Başkan: : Prof.Dr. M. Sezai DİNÇER

Üye : Doç.Dr. Şeref SAĞIROĞLU

Üye : Doç.Dr. M.Ali AKÇAYOL

Tarih : 06/10/2006

Bu tez, Gazi Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına uygundur.

TEZ BİLDİRİMİ

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

Hüseyin EROL

KURUMSAL AĞLARDA AÇIK ANAHTAR ALTYAPISI TABANLI ELEKTRONİK İMZA UYGULAMASI
(Yüksek Lisans Tezi)

Hüseyin EROL

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
Ekim 2006

ÖZET

Kurumsal ağlarda karar alma sürecinin basitleştirilmesi, işlemlerin daha güvenilir yapılması, hizmetteki kalitenin arttırılması ve zamanın daha verimli bir şekilde kullanılması için elektronik imza kullanımı vazgeçilmez bir ihtiyaç haline gelmiştir. Ülkemizde elektronik imzanın 2004 yılı itibariyle resmi olarak yürürlüğe girmesi ile kurumların mevcut iş akışlarını bilgisayar ortamına aktarmalarının yasal olarak önü açılmıştır. Ancak elektronik imza, çok sayıda avantaja sahip olmasının yanı sıra oldukça yeni bir konudur ve uygulamaya geçiş sürecinde özellikle kurumsal ağlarda çok dikkatli olunması gerekmektedir. Bu nedenle kurumsal ağlarda elektronik imza sistemlerine geçiş projelerinde, uygulama seçimi, alınacak yazılım, donanım ve hizmetler konusunda iyi derecede bilgi sahibi olunması, mevcut örneklerin incelenmesi, güvenilirlik, süreklilik ve kurumsallık analizlerinin iyi yapılması ve hizmet kalitesinin doğru değerlendirilmesi gerekmektedir.

Bu çalışmada, kurumsal ağlarda açık anahtar altyapısı tabanlı elektronik imza sistemleri tüm bileşenleriyle detaylı olarak incelenmiş ve kurumsal elektronik imza projelerinin hayata geçirilmesine yönelik olarak kurumsal bir ağ üzerinde örnek bir uygulama geliştirilmiştir. Bu kapsamda, kurumsal ağlarda güvenlik altyapısı, elektronik imza sistemleri, elektronik imza sistemlerinin altyapısını

oluşturan açık anahtar altyapısı konuları detaylı olarak incelenmiştir. Ayrıca kurumsal elektronik imza sistemlerine örnek olması açısından dünyada ve ülkemizde elektronik imzaya ilişkin mevzuat, kurumsal altyapı ve örnek uygulamalar hakkında araştırma sonuçları sunulmuştur.

Tez çalışması kapsamında Gazi Üniversitesi'nin birimleri arasında örnek bir elektronik imza uygulaması simule edilmiştir. Bu uygulama ile kurumsal bir ağın elektronik imza sistemlerine geçişinde dikkat edilmesi ve izlenmesi gereken yollar, gereksinimlerin nasıl belirleneceği, uygulama seçiminde nelere dikkat edilmesi gerektiği, sistemlerin analiz, tasarım, gerçekleştirim, test, kullanım ve yaygınlaştırma aşamaları detaylı olarak anlatılmıştır. Gerçekleştirilen uygulamanın sonuçlarına göre elektronik imzanın kurumsal ağlarda iş akışlarını hızlandırdığı, maliyetleri düşürdüğü, güvenliği ve iş verimliliğini artırdığı görülmüştür.

Bu çalışma, kurumsal ağların güvenlik altyapısını; elektronik imzanın teknik ve hukuksal boyutunu; dünyada ve ülkemizde elektronik imzaya ilişkin mevcut durum, hukuksal altyapı ve örnek uygulamaları; kurumsal bir ağda elektronik imza sistemlerinin nasıl hayata geçirileceği konusunu adım adım içeren bir uygulama bölümünü kapsamaktadır. Elektronik imza konusunun tüm detaylarıyla incelendiği bu çalışmayı diğerlerinden ayıran en önemli nokta, kurumsal ağlarda elektronik imza sistemlerinin nasıl hayata geçirilmesi gerektiği konusunun detaylı olarak anlatıldığı güncel bir kılavuz doküman olma özelliğidir. Sonuç olarak, bu çalışma ile ülkemizde elektronik imza teknolojisinin yaygınlaşmasına katkı sağlanmıştır.

Bilim Kodu : 912.1.080
Anahtar Kelimeler : Elektronik İmza, Açık Anahtar Altyapısı, Güvenlik
Sayfa Adedi : 258
Tez Yöneticisi : Doç. Dr. M. Ali AKCAYOL

THE APPLICATION OF PUBLIC KEY INFRASTRUCTURE BASED E-SIGNATURE IN INSTITUTIONAL NETWORKS

(M.Sc. Thesis)

Hüseyin EROL

GAZİ UNIVERSITY

INSTITUTE OF SCIENCE AND TECHNOLOGY

October 2006

ABSTRACT

E-signature became a vital requisite in order to simplify the decision process in institutional networks, to make processes more reliable, to increase quality of service and to use time effectively. Starting by 2004 when e-signature has become official, institutions started to transfer their work flows to computers legally. Although e-signature has lots of advantages, it is a quite new subject and it is necessary to be careful in the process of transition, especially in institutional networks. Thus, it is very important to have a good knowledge about the application choices, software, hardware and services that will be bought along the process of application of e-signature systems in institutional network; to examine present samples; to make a thorough analysis of the reliability, continuity, institutional features and to correct evaluation of quality of service.

In this study, Public Key Infrastructure (PKI) based e-signature systems, are examined in institutional networks in a detailed way and a sample application is developed in an institutional network to demonstrate the practice of the institutional e-signature projects. In this scope, security substructure subjects, e-signature systems, PKI that forms the substructure of e-signature systems in institutional networks are worked out in detail. Additionally, to provide a sample to the institutional e-signature systems, the current laws, research

results about institutional substructure and sample applications of e-signature in the world and our country are presented.

Within the scope of this thesis, an e-signature application is simulated between two departments of Gazi University. Using this application, the methods that have to be followed and taken into consideration while establishing e-signature systems of institutional networks; determining the requirements, the points to take into consideration while choosing the application, the steps of system analysis, design, application, test, usage and propagation of systems are presented in a detailed way. According to the results of the application that was put into practice, it is seen that e-signature speeds up work flows in institutional networks, brings down costs and increases the security and work productivity.

This study covers, the security substructure of institutional networks; the technical and legal dimension of e-signature; the existing status, legal substructure and sample applications concerning to e-signature in the world and our country; an application section that includes step by step application of e-signature systems in an institutional networks. The most important feature that distinguishes this study from others is its being a detailed up-to-date guide examining the topic of installation of the e-signature systems in institutional networks. As a result, this study intends to help the widespread usage of e-signature technology in our country.

Science Code : 912.1.080
Key Words : Digital Signature, Public Key Infrastructure, Security
Page Number: 258
Adviser : Assist. Prof. Dr. M. Ali AKCAYOL

TEŞEKKÜR

Çalışmalarım boyunca değerli yardım ve katkılarıyla beni yönlendiren danışman hocam Doç. Dr. M.Ali AKÇAYOL'a, özellikle İmzager yazılımı konusunda sağladığı katkılardan dolayı başta Serdar DOĞAN olmak üzere tüm Tübitak-UEKAE personeline ve manevi destekleriyle beni hiçbir zaman yalnız bırakmayan annem, babam, sevgili eşim ve biricik kızıma teşekkürü bir borç bilirim.

İÇİNDEKİLER

Sayfa

Sayfa

Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

Şekil **Sayfa**

Şekil **Sayfa**

Şekil **Sayfa**

Şekil **Sayfa**

Şekil **Sayfa**

SİMGELER VE KISALTMALAR

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

Kısaltmalar	Açıklama
AAA	Açık Anahtar Altyapısı
AES	Advanced Encryption Standard
CA	Certificate Authority
CMP	Certificate Management Protocol
CWA	CEN Workshop Agreement
DES	Data Encryption Standard
E-imza	Elektronik İmza
ESHS	Elektronik Sertifika Hizmet Sağlayıcısı
EU	European Union
GEİA	Güvenli Elektronik İmza Aracı
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IETF RFC	IETF Request for Comments
ICC	International Commerce Chamber
IPSec	Internet Protocol Security
ISO	International Standards Organization
ITU	International Telecommunications Union
Kamu SM	Kamu Sertifikasyon Makamı
KSM	Kök Sertifikasyon Makamı
KM	Kayıt Makamı
MAC	Message Authentication Codes
NIST	National Institute of Standards and Technology
NES	Nitelikli Elektronik Sertifika

Kısaltmalar	Açıklama
NSA	National Security Agency
PGP	Pretty Good Privacy
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
RSA	Rivest, Shamir ve Adleman
SSH	Secure Shell
SİL	Sertifika İptal Listesi
Sİ	Sertifikasyon İlkesi
S/MIME	Secure/Multipurpose Internet Mail Extension
SM	Sertifikasyon Makamı
SSL	Secure Socket Layer
SUE	Sertifika Uygulama Esasları
UNCITRAL	UN Conference on International Trade Law
WTO	World Trade Organization

1. GİRİŞ

Bilgi teknolojilerindeki ilerleme, kişilerin ve kurumların iş ve işleyişini etkilemekte ve değiştirmektedir. Bu gelişimine paralel olarak artan bilgi alışverişi içerisinde güvenlik kavramı da önemini giderek artırmaktadır. Özellikle internet, herkes tarafından kolayca erişilebilir olmakla birlikte, günlük hayatta çok popüler ama aynı zamanda da riskli bir ortam haline gelmiştir. İnsanlara, işlerinin önemli bir kısmını kolayca gerçekleştirebilme imkanı sağlayan internet, sunduğu hizmetlerin yanı sıra bazı önemli tehditlere de meydan vermektedir.

Şirketler, kurumlar, kuruluşlar veya kişiler internet aracılığıyla bir işlem yapmak istediğinde, herkese açık bir ortamdan iletişimini sağlamak zorundadır. İletilecek olan bilgi, kaynağını terk ettikten sonra İnternet Servis Sağlayıcısı (İSS) üzerinden diğer aracılara iletilerek en az birkaç noktadan geçtikten sonra hedefine ulaşabilmektedir. Bu aradaki noktalardan herhangi birinde ya da yolda bilginin okunması veya değiştirilmesi olasılığı bulunmaktadır. İşte bu durumda bilgi güvenliğinin sağlanması için minimum gereksinimleri oluşturmak gerekmektedir. Bunlar haberleşen iki taraf arasındaki gizlilik, bütünlük, kimlik doğrulama ve inkar edememe gibi hizmetlerin sağlanmasıdır.

Elektronik imza (e-imza); bir veri bloğuna özgü olarak hesaplanan özet bilgi yardımıyla bütünlük, kimlik doğrulama ve inkar edememe hizmetlerini sağlayan bir güvenlik teknolojisidir. E-imza hesaplanırken kişiye özgü özel anahtar kullanılır. Bu yüzden farklı kişilerin aynı veri bloğu için hesapladığı e-imzalar farklı olur. Bunun yanısıra bir kullanıcının değişik veri blokları için hesaplayacağı e-imzalar da birbirinin aynısı olmaz. Bu iki özellik e-imzanın kişiye özel olmasını garanti eder.

E-imza sistemini gerçeklemek için kurulan en yaygın altyapı Açık Anahtar Altyapısıdır. Açık anahtarlı şifreleme yöntemlerinin kullanımı yoluyla bütünlük, kimlik doğrulama ve inkâr edilmezlik hizmetlerini kullanıcılara vermek ve e-imza teknolojisinin kolay kullanımını sağlamak için gerekli teknoloji, standart, yasa,

yönetmelik, kuruluş, ürün ve hizmetlerin bütününe "Açık Anahtar Altyapısı (AAA, Public Key Infrastructure-PKI)" denir.

Büyük ağlardaki güvenlik ve güvenilirlik sorunları ve bunlara yönelik çözümler ilk kez 1976 yılında Hellman ve Diffie tarafından ortaya konulmuştur [1]. Hellman ve Diffie tarafından teorik olarak öne sürülen e-imza ve AAA'nın temelleri 1978 yılında Ronald Rivest, Adi Shamir ve Len Adleman tarafından pratikte uygulanan açık anahtar tabanlı şifrelemeye (public key cryptography) dayanmaktadır. Açık anahtar tabanlı şifreleme yaklaşımı, e-imza ortamının ve altyapısının geliştirilmesine büyük katkı sağlamıştır. Büyük asal tamsayı çarpanlarının kullanıldığı zor bir matematiksel temele dayanan ve günümüzde de güvenilirliği henüz bozulmamış olan bu şifreleme yaklaşımına "RSA (Rivest, Shamir ve Adleman)" adı verilmiştir [2].

Tarihte ilk şifreleme yaklaşımları M.Ö. 1900'lü yıllarda Mısırlılar tarafından kullanılmaya başlanmıştır. Şifreleme yaklaşımlarının özellikle 2 nci Dünya Savaşı'nda çok önemli rol oynaması bu bilime olan önem ve ilgi artırmış ve yeni yaklaşımların gelişmesini sağlamıştır. 1960'lı yıllardan sonra özel sektöründe konuya ilgisinin artmasıyla başlayan çalışmaların sonucu olarak 1970'li yıllarda geliştirilen DES (Data Encryption Standard) algoritması, 1990 yılında geliştirilen IDEA (International Data Encryption Algorithm) algoritması ve 1991 yılında geliştirilen PGP (Pretty Good Privacy) algoritması ile şifreleme biliminde büyük gelişmeler kaydedilmiştir. 1991'de e-imza konusunda ilk uluslar arası standart olan ISO/IEC 9796 oluşturulmuştur. 1994 yılında ise Amerika Birleşik Devletleri (ABD) hükümeti El-Gamal açık anahtar sistem temeline dayalı e-imza standardını benimsemiştir [3].

Data Encryption Standard (DES)'ın güvenlik ihtiyaçlarını karşılayamaması üzerine son dönemde yapılan bir yarışma sonucu Rejindal veya şimdiki adıyla Advanced Encryption Standard (AES) günümüzde kullanılabilecek bir güvenlik standardı olarak kabul edilmiştir.

Günümüzde AAA ve e-imza sistemlerinde çeşitli algoritmalar (simetrik ve asimetrik) kullanılmaktadır. En çok kullanılan simetrik algoritmalar DES, 3DES, IDEA, AES, SKIP JACK, RC2, RC4 ve RC5'tir. Asimetrik algoritmalar ise RSA, Diffie-Hellman, PGP, El-Gamal ve Digital Signature Algorithm (DSA)'dir.

İlk e-imza sistemlerinde, imzalanacak metnin boyu büyüdükçe imza eklentisinin de boyu büyümekte ve buna bağlı olarak hız ve kapasite sorunları yaşanmaktaydı. Bu problemini çözmek için yapılan çalışmalar sonucunda 1990'lı yıllarda özetleme kavramı ve buna bağlı olarak özetleme algoritmaları ortaya çıkmıştır. Farklı uzunluklarda mesaj, doküman veya yazıyı işleyerek, sabit uzunlukta veri oluşturma işlemine özetleme; bu işlemleri gerçekleştiren algoritmalara özetleme algoritmaları adı verilmiştir. Bugün, farklı güvenlik seviyelerinde kullanılan bir çok özetleme algoritması bulunmaktadır. MD (Message Digest) serisi algoritmalar, SHA (Secure Hash Algorithm) serisi algoritmalar, RIPE-MD-160 (RACE Integrity Primitives Evaluation Message Digest 160) algoritması ve MAC (Message Authentication Codes) algortimaları en önemli özetleme algoritmalarıdır.

Ron Rivest tarafından geliştirilen MD serisi mesaj özetleme algoritmaları son yıllarda en çok kullanılan özetleme algoritmalarındandır. MD5'in bazı zayıflıklarının bulunduğu Mayıs 1996'da Alman Bilgi Güvenliği Servisinde görev yapan Dr. Hans Dobbetin tarafından tespit edilmiştir. Uzun bir süredir yaygın olarak kullanılan MD5, güvenilir bir yaklaşım olarak kabul edilmiş olsa da, yapılan son araştırmalar, MD5'in kırılabileceğini göstermiş ve MD5'e duyulan güven kaybolmuştur. MD5'in çarpışma saldırılarına karşı zayıf olduğunun keşfedilmesinden sonra, bilimadamları MD5 yerine SHA-1 veya RIPEMD-160 gibi alternatiflerin kullanılmasını önermişlerdir. SHA-1, ilk olarak "Ulusal Güvenlik Ajansı" (National Security Agency, NSA) tarafından geliştirilmiş ve "Ulusal Standartlar ve Teknoloji Enstitüsü" (National Institute of Standards and Technology, NIST)'in desteğiyle, 1993 yılında ABD'de standart olarak kabul edilmiştir. Son günlerde, SHA-1'in güncel bir versiyonu olan SHA-2 kullanılmaya başlanmıştır. RIPE-MD-160 algoritması ise halen Avrupa Birliğinde kullanılan bir algoritmadır [3].

Ülkemizde e-imza teknolojisinin etkin kullanımına yönelik olarak 23 Ocak 2004 tarihinde 25355 sayılı Resmi Gazete ile 5070 nolu E-İmza Kanunu yayımlanmıştır. Bu kanun ile "e-imza" teknolojisinin ülkemizdeki kamu ve özel sektör uygulamalarında nasıl hayata geçirileceği ile ilgili hukuki bir altyapı oluşturulmuştur. Kanunda tanımlanan güvenli e-imza, ıslak imza ile aynı hukuki sonuçları doğurmaktadır [4].

E-imza kanunları içerisinde öngörülen mekanizmalar yoluyla sayısal ortamda gerçekleştirilen işlemlere hukuki korunma sağlanırken aynı zamanda teknik açıdan bu işlemlerin kaynağının tespiti, gizliliği, bütünlüğü ve inkar edilmezliği sağlanmaktadır. Dünyadaki ve Avrupa Birliğindeki ülkelere bakıldığı zaman e-imza uygulamalarında %90'ı aşan bir oranda AAA teknolojisi kullanıldığı ve ülke kanunlarında da bu teknolojiyi temel alan yaklaşımların esas alındığı görülmektedir.

Açık anahtar altyapısının avantaj ve dezavantajları

Bilgisayar teknolojilerindeki ilerleme, kişilerin ve kurumların iş ve işleyişini etkilemekte ve değiştirmektedir. Günümüzün elektronik ortamları, işlemlerin daha hızlı, verimli ve güvenli bir şekilde yapılmasını sağlayacak hizmetleri kullanıcılarına sunmaktadır. AAA kullanımıyla, elektronik ortamlarda yapılan haberleşmeler, e-devlet işlemleri, e-ticaret, e-bankacılık hizmetleri gibi işlemler internet üzerinden güvenli olarak anında gerçekleşebilecektir [3].

AAA'nın en önemli üstünlüğü; kişilerin-kişilerle, kişilerin-kurumlarla, kurumların-kişilerle ve kurumların-kurumlarla elektronik ortamda iletişiminin çok hızlı yapılması için güvenli bir altyapı oluşturması ve gerek kişisel gerekse kurumsal bilgi ve iletişim güvenliğini tam anlamıyla sağlamasıdır.

Bu altyapının oluşturulması başlangıçta maliyetli ve zaman alıcıdır. Ancak uzun vadede dokümantasyon takibini hızlandıracak, alındı/gönderildi onaylarında karşılaşılabilecek işgücü kayıplarını azaltacak, orta ve uzun vadede maliyetleri

düşürecek ve verimliliği yükseltecektir.

Elektronik imzanın avantaj ve dezavantajları

Elektronik ortamda hayata geçirilen uygulama ve hizmetler, kağıt ortamına oranla zaman, iş gücü, maddi tasarruf ve hizmetlerin 7 gün 24 saat alınıp verilebilmesine olanak sağlayacak, ayrıca bütün dünyayı bir ağ ortamında birleştirebilecektir. Elektronik ortama geçiş, hizmet konusundaki anlayışı değiştirerek, hizmetin vatandaşın ayağına gitmesine imkan tanıyacak ve insanın hedef kitlesini sadece çevresindeki insanlar olmaktan çıkarıp dünyanın tümüne yaygınlaştırabilecektir.

E-imza, elektronik verinin elektronik ortamda verilen uygulama ve hizmetlerde güvenli bir biçimde kullanılabilmesi için bilinen en iyi yöntemdir. Diğer bir deyişle, e-ticaret ve e-devlet işlemlerinin hukuksal geçerliliğinin sağlanmasında henüz daha iyi bir alternatif yoktur.

Kurumsal ağlardaki uygulamalarda karşılaşılan sorunlar ve çözüm yöntemleri

Dünyada ve ülkemizde kurumsal ağlardaki AAA ve e-imza uygulamaları incelendiğinde, uygulamaların genellikle kurum içinde diğer kurumlardan bağımsız projeler olarak ortaya çıktığı görülmektedir. Ancak bu durum, ülke genelinde mükerrer uygulamaların ortaya çıkmasına, kurumlar arası birlikte çalışamama sorunlarına, her kurumun benzer uygulamalar için çalışma yapması ve ödenek ayırması nedeniyle israfa ve bazı durumlarda da gereksinimlerin karşılanamamasına neden olmaktadır. Bu sorunlar, ülke genelinde (özellikle kamu kurumları için) uygulamalarda standardizasyonun sağlanması yoluyla çözülmeye çalışılmıştır. Birçok ülke kamu için gerekli AAA ve e-imza ihtiyacını merkezi olarak karşılamayı uygun görmüş ve hatta ürün seçimi konusunda da sınırlamalar getirmiştir. Ayrıca birçok ülke de e-imza altyapısıyla ilgili kuralları önceden belirleyerek kamuya duyurmuş ve bu kapsamda çalışmalarını şart koşmuştur. Ülkemizde de kamu ve özel sektöre hizmet vermek üzere ayrı elektronik sertifika hizmet sağlayıcıları mevzuatla

düzenlenmiş olmasına rağmen, kurumsal uygulamalarda yukarıda bahsedilen sorunların çözümüne yönelik düzenlemelerin yapılmasına ihtiyaç vardır.

Kurumsal ağlarda e-imza çalışmalarında yaşanan diğer bir problem de ilk bakışta maliyetlerin yüksek görünmesidir. Ancak e-imza uygulamalarının kuruma sağlayacağı tasarruf ve maliyet analizi yapıldığında kısa sürede yapılan harcamaların kendini amorti edebileceği ortaya çıkmaktadır. Bu durum, özellikle kurumda e-imza uygulamalarının hayata geçirilmesine karar verecek yöneticilere aktarılarak kurum için doğru kararların alınması sağlanmalıdır.

Kurumsal ağlarda tüm iş akışlarında aynı anda e-imza desteğinin sağlanması da genellikle kurumda başarısız uygulamaların ortaya çıkmasına ve kullanıcıların ortaya çıkan bu yeni sisteme karşı direnç göstermelerine neden olmaktadır. Bilgi eksikliğinden doğan tereddütler ve başarısız örnekler, kullanıcıları olumsuz yönde etkilemektedir. Bu sorun da e-imza uygulamalarının ilk seferde kapsam ve amacı açısından sınırlı pilot uygulamalar biçiminde tasarlanması ve pilot uygulamalardan olumlu sonuçlar alındıkça kapsamının genişletilmesi yoluyla çözülebilir. Bu nedenle kurumsal ağlarda en iyi örneği oluşturmak için, öncelikle kendi içinde kalan iş akışlarında, sonra diğer kurumsal ağlarla ilişkilerinde ve son olarak vatandaşlarla ilişkilerinde e-imzaya geçiş planlanmalı ve uygulanmalıdır. Bu yaygınlaştırma çalışmalarında başarıya ulaşabilmek için kurum çalışanlarının e-imzanın ne olduğunu kavramaları ve elektronik yaşamla birlikte e-imza kullanımının hayatlarına getireceği kolaylıkları fark etmeleri de gerekmektedir. Bu amaçla kurum personeline e-imza ve uygulamaları hakkında eğitimler verilmeli, uygulamaların basit ve anlaşılır seviyede olması sağlanmalı ve kurum içinde bilgisayar kullanımı ön plana çıkarılmalıdır.

Sonuç olarak e-imzanın bir araç olduğu asla akıldan çıkarılmamalıdır. Belirli bir uygulamayla ilişkilendirilmediği sürece, bir e-imza projesinden söz etmek anlamlı değildir. E-imza teknolojilerinde istenmeyen sonuçlarla karşılaşmamak, iyi belirlenen ve dikkatli uygulanan politikalarla mümkündür.

Tezin amacı

E-devletin ve yaklaşık 6 trilyon dolar değerindeki e-ticaretin altyapısı olan e-imza, internetin ve teknolojilerin hızlı gelişimi, dünyada artan kullanıcı sayısı ve rekabet ortamı sayesinde, bilişim teknolojisi ve uygulamaları alanında kendisine oldukça önemli bir yer edinmiştir [5]. E-imza ve uygulamaları, gerektirdiği teknolojik ve hukuki altyapıyla birlikte; sağladığı güvenlik, verimlilik ve tasarruf gibi faydaları sayesinde yaygın hale gelmeye başlamıştır.

Kurumlar yaptıkları iş itibariyle toplumun ihtiyaçlarına cevap vermek ve üstlendiği görevleri etkili bir şekilde yerine getirmek esasına yönelik olarak kurulmuştur. Bu nedenle karar alma sürecinin basitleştirilmesi, işlemlerin daha güvenilir yapılması, hizmetteki kalitenin arttırılması ve zamanın daha verimli bir şekilde kullanılması modern toplumsal yaşamın bir gereği olmuştur. Bu kapsamda yazışma ve doküman paylaşımı işlemlerinin bilgisayar ortamında resmi olarak yapılabilmesi, elektronik arşiv ve kâğıtsız ofisin kurumlarda yapılandırılması ve elektronik doküman yönetim bilgi sistemleri için e-imza kullanımı vazgeçilmez bir ihtiyaç haline gelmiştir.

Bu tez çalışması kapsamında kurumsal ağlara yönelik olarak e-imza sistemlerine geçişin nasıl olması gerektiği tüm detaylarıyla incelenerek Gazi Üniversitesi için yapılan örnek uygulamayla kurumsal ağlarda e-imzaya geçiş sürecinin doğru yöntemlerle hızlı ve planlı bir şekilde yapılmasına ve e-imza kullanımının yaygınlaşmasına katkı sağlamak amaçlanmıştır. Bu kapsamda, e-imzanın teknik detayları ile birlikte dünyada ve ülkemizdeki mevcut durum incelenerek kurumsal ağlarda e-imza sistemlerini uygulayabilmek için dikkat edilmesi gereken noktalar ve izlenmesi gereken işlem adımları örnek uygulamayla birlikte ele alınmıştır. Gazi Üniversitesi'nde seçilen iki birim arasında gerçekleştirilen örnek e-imza uygulaması ve uygulama sonuçları 5 nci bölümde anlatılarak konu somutlaştırılmıştır.

Tezin yapısı

Toplam 6 bölümden oluşan tez çalışmasının giriş bölümü olan 1. bölümünde e-imza ve AAA sistemlerine kısa bir giriş yapılarak bu sistemlerin tarihsel gelişimi, avantajları ve dezavantajları anlatılmıştır. Kurumsal ağların yapısı, kurumsal ağlarda e-imzaya neden gerek duyulduğu, kurumsal ağlardaki e-imza uygulamalarında yaşanılan sorunlar ve çözüm yöntemleri ile tezin gerekçesi açıklanarak, geliştirilen örnek uygulama ile ilgili kısa bilgi verilmiştir. 2. bölümde kurumsal ağlarda güvenlik, şifreleme bilimi, e-imza ve AAA sistemlerinin temelini oluşturan güvenli şifreleme yöntemleri ile kurumsal ağlarda güvenliğin sağlanması için etkin bir çözüm sağlayan AAA konuları anlatılmıştır. 3. bölümde e-imza konusu ve AAA tabanlı kurumsal e-imza sistemleri teknik açıdan detaylı olarak incelenmiştir. 4 ncü bölümde, kurumsal ağlarda e-imza sistemlerinin hayata geçirilmesi için yapılacak çalışmalara katkı sağlaması açısından Dünyada ve Türkiye'de e-imzaya ilişkin son durum, yasal düzenlemeler, kurumsal altyapı ve örnek uygulamalar anlatılmıştır. 5. bölümde kurumsal bir ağda e-imza sistemlerinin nasıl hayata geçirilebileceği Gazi Üniversitesi'nde seçilen iki birim için yapılan örnek e-imza uygulaması ile detaylı olarak anlatılmıştır. Uygulamadan elde edilen sonuçlar da aynı bölümde verilmiştir. Bu bölümde ayrıca kurumsal ağlarda e-imza uygulamalarının hayata geçirilmesinde ve yaygınlaştırılmasında dikkat edilmesi gereken hususlar da açıklanmıştır. 6. bölümde ise tez çalışmasının genel sonuçları ve öneriler sunulmuştur.

2. KURUMSAL AĞLARDA GÜVENLİK ALTYAPISI

Bu bölümde kurumsal ağlarda güvenlik altyapısını oluşturan teknolojiler, haberleşme güvenliği ve şifreleme bilimi konuları ile güvenli şifreleme yöntemleri detaylı olarak incelenmiş; kurumsal ağlarda güvenliğin sağlanması için etkin bir çözüm sunan AAA konusuna kısa bir giriş yapılmıştır.

2.1. Bilgi ve Bilgisayar Sistemleri Güvenliği

Genel olarak bilgi; veri (data), bilgi (information) ve özbilgi (knowledge) olmak üzere üç farklı başlık altında toplanmaktadır. Veri, bir durum hakkında birbiriyle bağlantısı henüz kurulmamış, bilinenler veya kısaca sayısal ortamlarda bulunan ve taşınan sinyaller ve/veya bitler olarak tanımlanabilir. Verinin belli bir anlam ifade edecek şekilde sınıflandırılmış hali ise bilgidir. Bir güç yaratabilecek, katma değer sağlayabilecek veya bir araç haline dönüşmek üzere daha fazla işlenmiş bilgi ise asıl değerli olan özbilgidir [3].

Bilgisayar sistemleri güvenliği ise, bilgisayar sistemlerinde karşılaşılabilecek tehditlere karşı önlem alma işlemleridir ve çok güncel ve önemli bir konudur. Bilgi güvenliği; bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak, bilginin her türlü ortamda istenmeyen kişiler tarafından elde edilmesini önleme olarak tanımlanır. Bunun yanında bilgi güvenliği, kişi ve kurumların bilgisayar teknolojilerini kullanırken karşılaşabilecekleri tehdit ve tehlikelerin daha önceden analizlerinin yapılarak gerekli önlemlerin alınmasını sağlama işlemidir. Kısaca; öneme sahip veya değerli bilginin korunmasına yönelik çabaların tümüdür. İçinde bulunduğumuz yüzyılda en önemli çalışma alanlarının başında yer almaktadır.

Uluslararası bilgi güvenliği standardı olan BS 7799-1:2000'de "Bilgi, diğer bütün kurum varlıkları gibi organizasyon için değeri olan ve aralıksız olarak uygun bir şekilde korunması gereken bir varlıktır" şeklinde tanımlanmaktadır. ISO/IEC

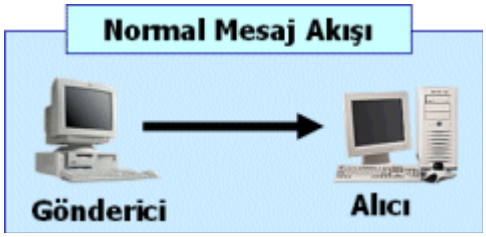
17799'a göre bilgi ve bilgi güvenliği tanımları ise; "Bilgi, çıktı halinde veya kağıda yazılı bir halde, elektronik ortamda kayıtlı bir halde, posta yoluyla veya elektronik olarak gönderilmiş halde, sinema ve televizyon aracılığıyla gösterilerek veya konuşmalar sırasında olduğu gibi herhangi bir yapıda bulunabilir. Hangi yapıda bulunursa bulunsun veya nasıl kayıt ediliyor veya saklanıyorsa saklansın, bilgi sürekli olarak uygun bir şekilde korunmalıdır." şeklinde ifade edilmiştir.

Bilişim teknolojilerinde güvenliğin amacı, elektronik ortamlarda tutulan bilgilerin, bu teknolojileri kullanarak karşılaşılabilecek 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.

Bilgilerin koruma seviyesi ve çeşitliliği arttıkça saldırıların niteliği ve çeşitliliği de artmıştır. Bu seviyeyi tutturabilmek için, gizlilik (confidentiality), bütünlük (integrity) ve hazır bulunabilirlik (availability) temel bilgi güvenliği içerikleri olsa da bilgi bulunduran ortamlarda kimlik kanıtlama (authentication), inkar edememe (nonrepudiation), fiziksel güvenlik, insan faktörü, güvenlik duvarları, anti-virüs yazılımları, e-imza, saldırı tespit sistemleri ve şifreleme gibi metotların ve yaklaşımların kullanılması gerekmektedir [7].

2.2. Haberleşme Güvenliği ve Çözümleri

Haberleşen iki taraf, bilgisayar ağları, kablolu veya kablosuz iletişim kanalları kullanarak bir bilgiyi/mesajı bir taraftan diğerine iletirler. Haberleşen iki taraf arasındaki normal mesaj akışı Şekil 2.1'de gösterildiği gibi gerçekleşir [6]. Ancak, elektronik ortamda haberleşen taraflar çesitli tehditlerle karşı karşıya kalırlar. Bu tehditler iki taraf arasındaki mesajın gizliliğinin ihlali, bütünlüğünün ihlali, karşılıklı kimlik doğrulamanın ihlali, karşılıklı mesaj trafiğini inkar edememenin ihlali ve haberleşmenin sürekliliğinin ihlali olabilir.

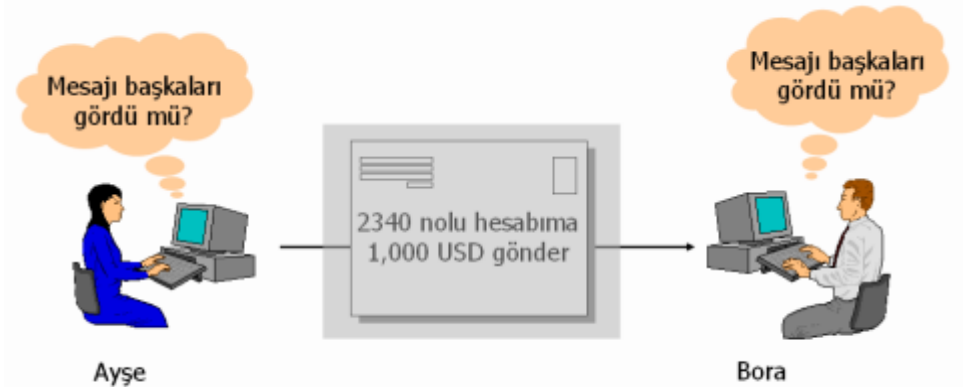


Şekil 2.1. Normal mesaj akışı

Elektronik tehditler

Elektronik tehditler temel olarak 5 ana başlık altında incelenebilir. Bunlar; gizlilik ihlali, bütünlük ihlali, kimlik doğrulama ihlali, inkar edememezlik ihlali ve süreklilik ihlalidir.

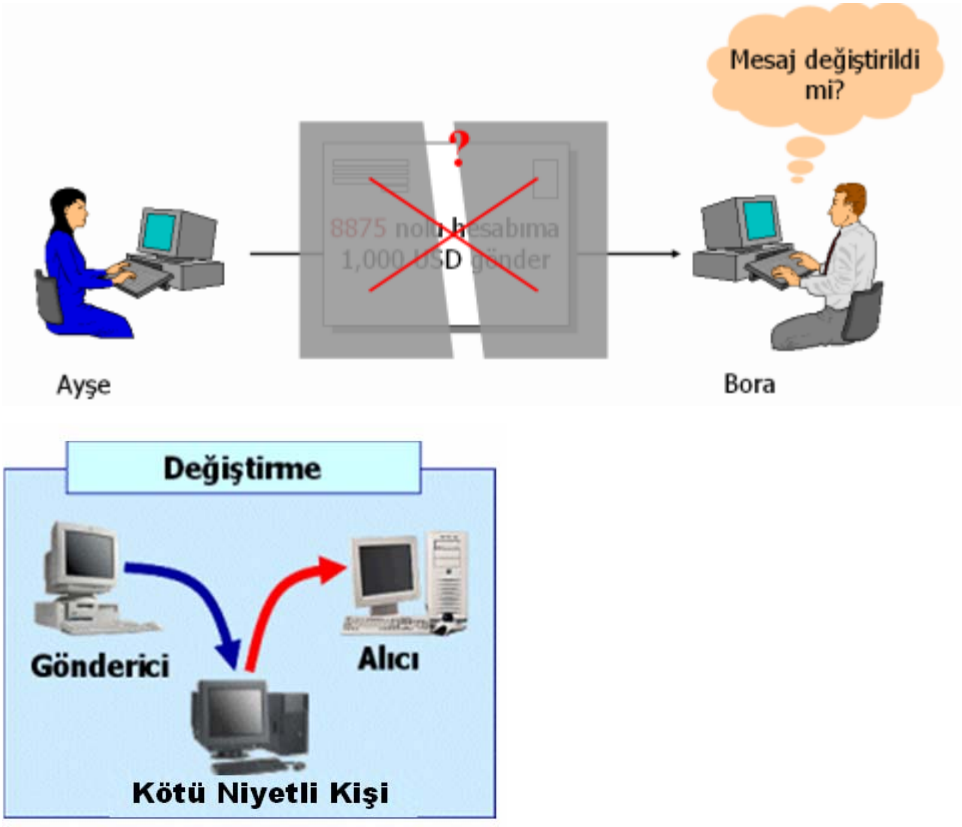
a. Gizlilik ihlali: Haberleşme kanalına erişen kötü niyetli kişi, gönderici ile alıcı arasındaki mesaj trafiğini dinleyebilir ve elde ettigi mesajları okuyarak bu haberlesmenin gizliliğini bozabilir. Şekil 2.2'de görülen bu tehdit dinleme tehdidi olarak bilinir [6].



Şekil 2.2. Dinleme tehdidi

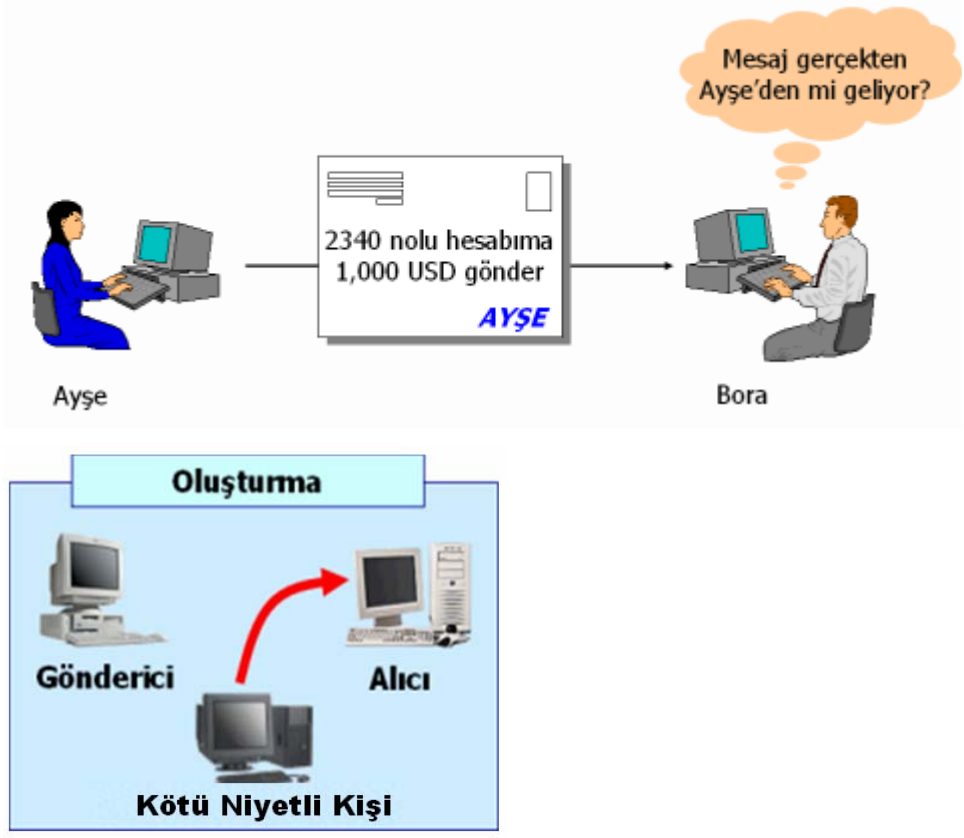
Şekil 2.2. (Devam) Dinleme tehdidi

b. Bütünlük ihlali: Haberleşme kanalını dinleyerek gönderici ile alıcı arasındaki mesajları ele geçiren kötü niyetli bir kişi, bu mesajı istediği gibi değiştirerek gönderen kişiden geliyormuş gibi alıcıya gönderebilir. Şekil 2.3'te gösterilen bu tehdit, mesajın bütünlüğünü bozan değiştirme tehdididir [6].



Şekil 2.3. Değiştirme tehdidi

c. Kimlik doğrulama ihlali: Kötü niyetli bir kişi, alıcıya göndericinin kimliğini taklit ederek bir mesaj gönderebilir. Bu durumda eğer alıcı güvenilir bir kimlik doğrulaması yapmıyorsa yanlış mesajlarla kandırılabilir. Şekil 2.4'te gösterilen bu tehdide de oluşturma tehdidi adı verilir [6].

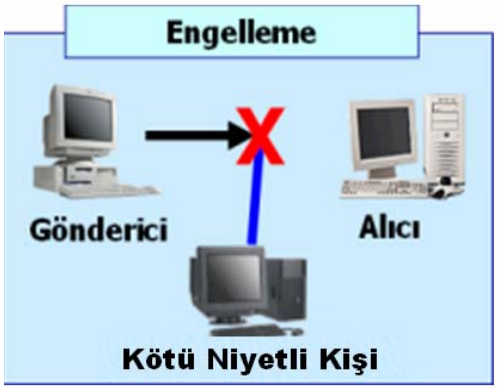


Şekil 2.4. Oluşturma tehdidi

d. İnkar edememezlik ihlali: Bazı durumlarda mesajı gönderen veya alan tarafın bu işi yaptığını inkar etmesi söz konusu olabilir. Taraflar arasında güvenliği tam olarak sağlamak için Şekil 2.5'de gösterilen inkar edememezlik ihlali girişimi boşa çıkaracak mekanizmalara ihtiyaç vardır [6].

Şekil 2.5. İnkar edememezlik ihlali

e. Süreklilik ihlali: Kötü niyetli kişi, çeşitli yollarla haberleşen taraflar arasındaki hattı veya haberleşme araçlarını kullanılmaz hale getirerek haberleşmenin sürekliliğini engellemeye çalışabilir. Şekil 2.6'da gösterilen bu tehdide de engelleme tehdidi adı verilmektedir [6].



Şekil 2.6. Engelleme tehdidi

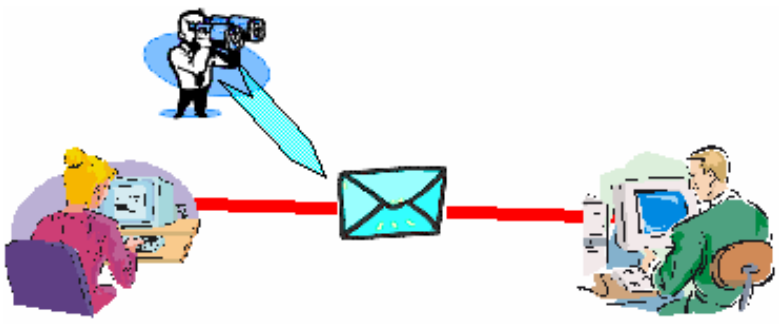
Haberleşme güvenliği

E-imza, iletişim ve veri güvenliğini sağlamak amacıyla geliştirilmiş bir teknolojidir. Günümüzde İnternet başta olmak üzere açık ve korunmasız ağlar üzerinden gerçekleşen veri iletişiminin güvenliğinin sağlanması için bir takım gereksinimler belirlenmiştir. Elektronik işlemlerdeki temel güvenlik gereksinimleri gizlilik,

bütünlük, kimlik doğrulama, inkar edememezlik, haberleşmenin sürekliliği, yetkilendirme ve kayıt tutma olarak sıralanabilir. İki taraf arasındaki haberleşmenin güvenliğini sağlayan bu öğeler aşağıda açıklanmıştır:

a. Gizlilik: Gizlilik, bilginin içeriginin gizli kalmasıdır. Bir diğer ifadeyle, veri/bilgi/belgenin durağan veya hareket halinde sadece yetkili kişiler tarafından anlamlandırılmasını sağlamak anlamına gelmektedir. Bu, kriptolama ve dekriptolama teknikleri ile mümkün olabilmektedir. Amaç, bilgi/belgenin başkalarının eline geçmesine engel olmak değil, eline geçse dahi anlaşılamaz bir halde olmasını sağlamaktır. Modern kriptolama teknolojileri anahtarlar içermektedir ve yetkili kişide bulunan anahtar ile bilgi kolaylıkla okunabilmektedir. Bu bakımdan, kripto algoritmalarının güvenliğinin anahtar uzunluğu ile birlikte, anahtar güvenliği ile de eşdeğer olduğunun unutulamaması gereklidir. Bunun yanısıra, tüm kripto algoritmalarının sonsuza dek bir güvenlik sağlamadığı da herkesçe bilinmektedir. Anahtar uzunluğunu belirlenirken, bilginin geçerlilik süresi parametresi en önemli girdi olacağı düşünülmektedir [8].

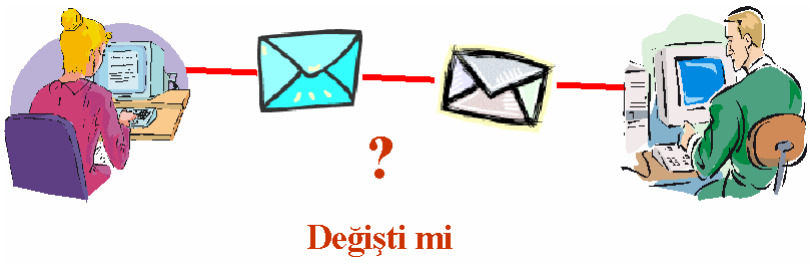
Sonuç olarak gizlilik, verinin/içeriğin görüntülenmesinin sadece veriyi görüntülemeye izin verilen şahısların erişimiyle kısıtlanmasıdır (Şekil 2.7). Bu şekilde, artık çok da zor olmayan ve kişisel bilgi mahremiyetini tehdit eden iletişim trafiğinin yetkisiz olarak dinlenmesine karşı bir önlem alınmış olur. Gizlilik bilginin şifrelenmesi ile gerçekleştirilebilir [4].



Şekil 2.7. Gizlilik

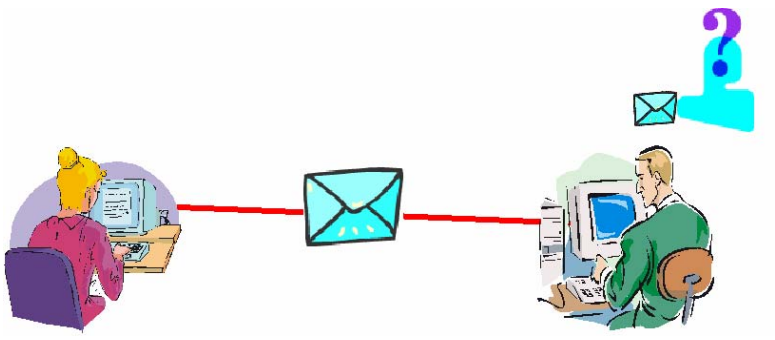
b. Bütünlük: Verinin izinsiz olarak veya yanlışlıkla değiştirilmesinin, silinmesinin veya veriye ekleme yapılmasının önlenmesidir (Şekil 2.8). Bu şekilde verinin göndericiden alıcıya, göndericiden çıktığı haliyle değişmeden ulaşması sağlanır. Alıcı, iletinin göndericiden çıktığı haliyle kendisine ulaştığını bir bütünlük sınaması yaparak anlar.

Bilginin yolda değişmediğinin garantisi, hash veya e-imza teknolojileri ile mümkün olabilmektedir. E-imza sayesinde hareket halindeki bir bilgi/belgenin gönderenini doğrulamak da mümkün olabilmektedir [8].



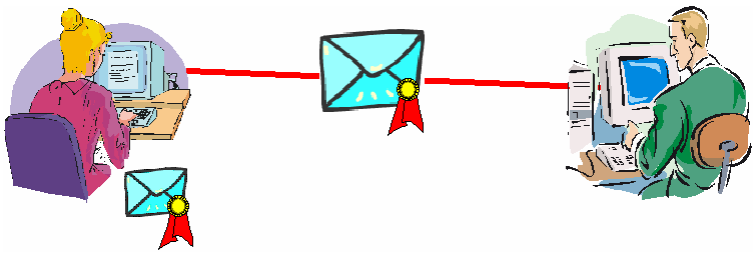
Şekil 2.8. Bütünlük

c. Kimlik doğrulama: Mesajın iletiminin geçerliliğinin ve mesaj sahibinin kimliğinin doğrulanmasının sağlanmasıdır (Şekil 2.9). Örneğin bir elektronik posta mesajı üzerinde yer alan gönderici adresi, mesajın asıl göndericisi olmayabilir. Bu nedenle alıcı, göndericinin kimliğini doğrulamak için bir takım yöntemler kullanır. E-imza, kimlik doğrulama için kullanılabilecek yöntemlerden biridir [4].



Şekil 2.9. Kimlik doğrulama

d. İnkâr edememezlik: Bireylerin elektronik ortamda gerçekleştirdikleri işlemleri inkar etmelerinin önlenmesidir (Şekil 2.10).



Şekil 2.10. İnkâr edilmezlik

e. Haberleşmenin sürekliliği: Haberleşme sürekliliği haberleşmenin kesintiye uğramadan yapılmasıdır.

f. Yetkilendirme: Kurumlar arası bilgi/belge akışında, yetkilendirme mekanizmalarını kurumların kendilerinde tutmaları önerilmektedir. Böylece, kurumlar kendilerine doğrulanmış olarak gelen isteklere, isteğin konusu olan bilgi/belgeyi verip vermemekte, kendi ihtiyaçları doğrultusunda kendi kara liste veya doğrulama metodları ile bir kere daha doğrulama veya tümden reddetme hakkını saklı tutabilirler.

g. Kayıt tutma: Yapılan tüm işlemler, anında veya daha sonra incelenmek üzere saklanmalıdır. Bu anlamda, kurum içi veya kurumlar arası tüm bilgi/belge akışı ve bu akışa ilişkin adımlar hem kaynak, hem de hedef kurumda kayıt altına alınmalıdır. Eğer, bu iletişim merkezi bir yapı üzerinden gerçekleşiyor ise o zaman tüm işlemin merkezde de kayıt altına alınması (logging) gerekmektedir. Ancak, merkezde tutulacak bu kayıtların gerekli durumlarda ihtilaf çözme işlevi de bulunmaktadır [8].

Haberleşme güvenliği çözümleri

Günlük hayatta yukarıda açıklanan temel güvenlik gereksinimlerini karşılamak için aşağıdaki yöntemler kullanılmaktadır [6].

- Gizlilik sağlamak için mühürlü zarf,
- Bütünlük sağlamak için imza, barkod, damgalama,
- Kimlik doğrulaması için noter, kimlik kartı, trafik ehliyeti, kişinin şahsen başvuru yapması,
- İnkâr edememezlik için imza, alındı, onay,
- Haberleşmenin sürekliliğini sağlamak için farklı, birbirine alternatif iletişim yolları kullanılır.

Elektronik ortamdaki haberleşmenin güvenliğini ortadan kaldıran tehditlere karşı alınması gereken önlemler, kullanılacak yöntem ve araçlar ise aşağıda sıralanmıştır:

- Gizlilik sağlamak için veri sifreleme yöntemleri,
- Bütünlük sağlamak için özetleme algoritmaları, mesaj özetleri, e-imzalar,
- Kimlik doğrulaması için özetleme algoritmaları, mesaj özetleri, e-imzalar, sertifikalar,
- İnkâr edememezlik için e-imzalar, işlem kayıtları,
- Süreklilik için yedek sistemler, bakım, yedekleme ve alternatif haberleşme kanalları kullanılır.

Elektronik güvenlik yöntemlerinin karşılaştırılması

Elektronik tehditlere karşı kullanılan çeşitli yöntemler ve hangi tehditlere karşı tedbir aldıkları Çizelge 2.1'de gösterilmiştir.

Çizelge 2.1. Elektronik emniyet yöntemlerinin karşılaştırılması

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

Çizelge 2.1 daha detaylı incelenirse; öncelikle virüslerin, bilgisayar programlarını değiştirdikleri için bütünlüğe yönelik tehdit oluşturdukları görülmektedir. Anti-virüs programları da, bilgisayardaki programların kontrol dışı değiştirilip değiştirilmediğini kontrol ederler. Bu nedenle sadece bütünlük hizmetini verebilirler.

Güvenlik duvarları (firewall) ve erişim denetim sistemleri, güvenli ve güvensiz olarak kabul edilen iki sistem arasında kimlik dogrulama yaparak belirli kaynaklara erişimi sınırlarlar. Bu nedenle sadece kimlik doğrulama ve gizlilik hizmetlerini sağlarlar.

Şifreleme programları veya yöntemleri tek başlarına kullanıldığında sadece gizlilik hizmetini sağlayabilirler.

E-imza, kimlik kanıtlama, bütünlük ve inkar edememe hizmetlerini sağlar.

AAA ise e-imzadan farklı olarak gizlilik hizmetini de sağlayarak tüm elektronik tehditlere karşı önlem alabilecek altyapıyı oluşturur. Bu altyapıda kimlik doğrulama, bütünlük ve inkar edememe hizmetleri e-imza ile sağlanır.

2.3. Şifreleme Bilimi

Şifreleme bilimi, matematiğin hem şifreleme bilimi (kriptografi), hem de şifre analizini (kriptoanaliz) kapsayan dalıdır [3].

Kriptoloji (gizli dünya (kryptos logos)), genel bir ifade ile bilgileri gizli tutma bilimidir. Örneğin haberleşme yapılırken mesaj bir algoritma vasıtasıyla şifrelenerek gizliliği sağlanır. Şifreleme işlemi sonucunda alıcının şifre çözme anahtarını kullanarak açabileceği şifreli mesaj ortaya çıkar. Kriptoloji uygulamalarının hemen hepsinde en önemli problem bu anahtarları gizli tutmak ve anahtarın dağıtımını sağlamaktır. Kriptoloji, kriptografi ve kriptoanaliz kavramlarının kısa tanımları aşağıda sunulmuştur.

Kriptoloji, haberleşen iki veya daha fazla tarafın bilgi alışverişini emniyetli olarak yapmasını sağlayan, temeli matematiksel zor problemlere dayanan tekniklerin ve uygulamaların bütünüdür [6].

Kriptografi, belgelerin şifrelenmesi ve şifrenin çözülmesi için kullanılan yöntemlere verilen addır [6]. Burada kullanılan şifreleme algoritmasının gücü, gizliliği bertaraf etmek için gizli metinden açık metine ulaşmak amacıyla yapılan kriptoanaliz saldırılarına dayanıklılığın derecesinin ölçümüdür.

Kriptoanaliz ise, kriptografi sistemleri tarafından ortaya konan bir şifreleme sistemini inceleyerek zayıf ve kuvvetli yönlerini ortaya koymayı amaçlayan bilim dalıdır.

2.3.1. Şifre biliminin tarihçesi

Tarihte ilk şifreleme yaklaşımlarının M.Ö. 1900'lü yıllarda Mısırlılar tarafından, hiyeroglif yazıların değiştirilmesi ile kullanıldığı tespit edilmiştir. M.Ö. 100-44 yılları arasında sunulan Sezar yaklaşımı da tarihte ilk şifreleme yaklaşımlarındandır. 1623'te Francis Bacon tarafından geliştirilen 5-bit ikili kodlamayla karakter tipi değişikliğine dayanan yaklaşım; 1790'da Thomas Jefferson tarafından icat edilen

“strip cipher” makinesı; 2 nci Dünya Savaşı’nda kullanılan M-138-A makinası; 1917’de Joseph Mauborgne ve Gilbert Vernam tarafından geliştirilen “one time pad” algoritması şifre bilimi tarihinde 2 nci Dünya Savaşına kadar olan dönemde yaşanan önemli gelişmelerdir [9].

2 nci Dünya Savaşı’nda çok önemli rol oynayan şifreleme yaklaşımları bu bilime olan önem ve ilgiyi artırmış ve yeni yaklaşımların gelişmesini sağlamıştır. O yıllarda ABD’nin ilk kriptoanaliz laboratuarı ile Ulusal Güvenlik Merkezini kurması ve Purple Machine ile askeri haberleşmelerde kullanılan şifreleme sisteminin, Alan Turing ve ekibi tarafından da Enigma’nın çözülmesi dönemin önemli gelişmeleri olmuştur.

1960’lı yıllarda özel sektörün de konuya ilgisi artmış ve 1970’de IBM ile başlayan çalışmaların sonucu olarak DES bir şifreleme standardı olarak kabul edilmiştir. 1976 yılında ise Hellman ve Diffie tarafından teorik olarak geliştirilen açık anahtarlı şifreleme yaklaşımı 1978 yılında Rivest, Shamir ve Adleman tarafından pratikte uygulanmıştır. Büyük asal tamsayı çarpanlarının etkileşmesi gibi zor bir matematiksel temele dayanan ve günümüzde de güvenilirliği henüz bozulmamış olan bu yaklaşıma RSA adı verilmiştir [6].

1990’da Lai ve Massey tarafından geliştirilen IDEA ve 1991 yılında Zimmerman tarafından geliştirilen PGP ile şifreleme biliminde büyük gelişmeler kaydedilmiştir. Açık anahtarlı şifre bilimi, bugün için sayısal ortamda bilgi güvenliğinin sağlanmasında büyük kolaylık sağlayacak olan e-imza ortamının ve altyapısının geliştirilmesine büyük katkı sağlamıştır. 1991’de e-imza konusunda ilk uluslar arası standart olan ISO/IEC 9796 hayata geçirilmiş olup, RSA açık anahtar yaklaşımı kullanılmıştır. 1994’de ise ABD hükümeti El-Gamal açık anahtar sistem temeline dayalı e-imza standardını benimsemiştir.

DES’in güvenlik ihtiyaçlarını karşılayamaması üzerine son dönemde yapılan bir yarışma sonucu Rejindal algoritması veya bilinen adıyla AES günümüzde

kullanılabilecek bir güvenlik standardı olarak kabul edilmiştir.

2.3.2. Şifre biliminin amacı ve önemi

Şifre biliminin amacı işlenen, saklanan, depolanan ve iletilen verilerin güvenliğini sağlamaktır. Yani temel amaç, verilere bilmesi gereken kişiler dışındaki kişilerin erişiminin engellenmesidir.

Günümüzde teknolojik gelişmelere paralel olarak insanlar arasında bilgi transferinde bilgi sistemlerinin kullanımı artmış, web teknolojilerinde yaşanan gelişmeler ile web uygulamalarında önemli gelişmeler yaşanmış ve e-iş, e-pazarlama, e-bilim, e-öğrenme, e-sağlık, e-bankacılık, e-devlet, e-imza ve e-dönüşüm gibi birçok kavram ortaya çıkmıştır. Günlük hayatı kolaylaştıran ve hızlandıran tüm bu yeni kavram ve teknolojilerin güvenli kullanımı için şifreleme bilimi gereklidir. Ayrıca kurumların ve kişilerin özel ve/veya gizli bilgilerini korumak için de şifreleme bilimi gerekli ve önemlidir. Kısacası insanların fiziksel dünyada sahip oldukları güven ortamına sanal dünyada da sahip olmak istemeleri şifreleme bilimini önemli hale getirmiştir.

2.3.3. Şifre bilimi standartları

Bilgisayar sistemlerinin ülke içi ve ülkeler arası haberleşmelerinde, bir uyum içerisinde problemsiz çalışmalarını sağlamak için ortak olarak belirlenmiş kural ve politikalara ihtiyaç duyulmaktadır. Bu politikalar ve kurallar bütününe standart denilmektedir. Başka bir ifadeyle, kaliteyi tutturmak, verimliliği arttırmak, zaman kaybını azaltmak ve birlikte çalışabilirliği sağlamak için ortak kurallar, yani standartlar gereklidir [3].

Şifre biliminde bunun sağlanması için, devlet, özel sektör ve diğer organizasyonlar ortak standartlar belirlenmesine katkıda bulunmaktadırlar. Konuyla ilgili önemli organizasyonlar ve açılımları Çizelge 2.2'de verilmiştir.

Çizelge 2.2. Şifre bilimiyle ilgili organizasyonlar

ISO	International Standards Organization (Uluslararası Standarlar Organizasyonu)
ANSI	American National Standards Institute (Amerikan Ulusal Standartlar Enstitüsü)
IEEE	Institute of Electrical and Electronics Engineers (Elektrik ve Elektronik Mühendisleri Odası)
NIST	National Institute of Standards and Technology (Ulusal Standartlar ve Teknoloji Enstitüsü)
IETF	Internet Engineering Task Force (İnternet Mühendisliği Çalışma Grubu)
EU	European Union (Avrupa Birliği)
WTO	World Trade Organisation (Dünya Ticaret Örgütü)
ICC	International Commerce Chamber (Uluslar arası Ticaret Odası)
ITU	International Telecommunications Union (Uluslararası Telekomünikasyon Birliği)
ETSI	European Telecommunication Standards Institute (Avrupa Telekomünikasyon Standartları Enstitüsü)
UNCITRAL	United Nations Conference on International Trade Law (Uluslararası Ticaret Kanunu Üzerine Birleşmiş Milletler Konferansı)
BS	British Standards (İngiliz Standartları)
CWA	CEN Workshop Agreement (CEN Çalıştay Kararı)
FIPS PUB	Federal Information Processing Standards Publications (Federal Bilgi İşleme Standartları Yayınları)
IETF RFC	Internet Engineering Task Force Request for Comments (İnternet Mühendisliği Görev Grubu Yorum Talebi)
ISO/IEC	International Organisation for Standardisation/International Electrotechnical Commitee (Uluslararası Standardizasyon Teşkilatı/Uluslararası Elektroteknik Komitesi)

2.3.4. Şifreleme algoritmaları

Algoritmalar, şifreleme ve şifre çözmede kullanılan matematiksel işlemlerdir. Şifreleme biliminde kullanılan algoritmaların çalışma biçimi veya algoritmada kullanılan matematiksel yaklaşım gizli veya açık olabilir. Algoritmaların güvenilirlikleri bu çalışma biçimlerine ve kullanılan anahtar uzunluklarına bağlıdır. Bugün literatürde, şifreleme bilimi ihtiyaçlarına cevap verebilecek herkese açık algoritmalar mevcuttur. Günümüzde kullanılan algoritmalarla ilgili açıklayıcı bilgiler Bölüm 2.3.6 ve Bölüm 2.3.7'de verilmiştir.

Şifreleme algoritmalarında aranan temel özellikler aşağıda sıralanmıştır [3,6]:

- Şifrelenmiş mesajın deşifre edilmesi esnasında bilgi kaybı olmamalıdır.
- İhtiyaç duyulan güvenlik seviyesine göre şifreleme işleminin zorluk seviyesi seçilebilmelidir.
- Önemli olmayan bilgiler düşük seviyeli şifreleme yaklaşımları ile, yüksek seviyeli bilgi içeren dokümanlar ise yüksek seviyeli şifreleme yaklaşımlarıyla şifrelenebilmelidir.
- Verimi düşürecek, maliyet ve işgücü kaybını artıracak yaklaşımlar içermemelidir.
- Şifreleme işlemlerinde güvenlik seviyesi mümkü olduğunca yüksek olmalıdır.
- Basitlik ve kolaylıkla gerçekleştirilebilirlik özelliği ön planda olmalıdır.
- Kullanılan algoritmanın karıştırma özelliği olmalı, mesajın şifrelenmiş hali ile açık hali arasında ilişki kurulması çok zor olmalıdır.
- Kullanılan algoritmanın dağıtma özelliği olmalı, mesajın açık hali şifreli hale gelirken içerdiği kelime ve harf grupları şifreli mesajın içinde olabildiğinde dağıtılmalıdır.
- Şifrelenmiş metin ile açık metin arasında ilişki kurulamamalıdır.
- Şifreleme yaklaşımları herkese açık olmalıdır.
- Açıklarının ortaya çıkarılabilmesi için, başkaları tarafından test edilebilmesi sağlanmalıdır.

2.3.5. Anahtarlar

Modern kriptolama yaklaşımları, anahtar tabanlı olduğundan, bu yaklaşımlarda algoritmanın detayları ile ilgilenilmez. Anahtarın güvenliğinin sağlanması, sistemin genel güvenliğinin sağlanması ile eş anlamlıdır. Dolayısıyla anahtarlar, kriptografik yaklaşımların temel yapı taşlarıdır ve güvenlik, anahtarın güvenliğine ve bit katarlarının uzunluğuna bağlıdır [3].

Anahtar uzunlukları farklılık gösterse de, anahtarlar, büyük bir sayı kümesinden seçilmiş değerlerdir. Örneğin 64 bitlik bir anahtara örnek aşağıda verilmiştir:

64 bitlik anahtar = 1100101001001010 0001001001101001 0111001010110001
1001101001101101

Yukarıdaki gibi 64 bitlik bir anahtar kullanan şifreleme algoritması için toplam anahtar sayısı 2^{64} (10^{19}) adettir. Şifrelemede bu anahtarlardan herhangi birisi kullanılabileceği için bu anahtarı tahmin yoluyla elde etme olasılığı çok düşüktür.

Kriptolojide kullanılan rakamlar genellikle çok büyük olduğu için, fiziksel dünyadaki bazı büyük rakamları bilmek faydalı olacaktır [6]. Örneğin;

Bir insanın yıldırım düşmesi sonucu ölme ihtimali (1 gün için) = 9 milyarda 1 (2^{33})
Evrenin yaşı = 10^{10} (2^{34}) yıl
Dünyadaki atomların sayısı = 10^{51} (2^{170})

Anahtar uzunluğunun artması güvenliği artırmaktadır. Çizelge 2.3'de görülebileceği gibi bit sayısı arttıkça anahtarların kırılma sürelerinde artış çok büyük oranda olmaktadır. Bu sürelerin fazlalığı, anahtarların güvenli olduğunu göstermektedir [3].

Çizelge 2.3. Farklı anahtar uzunluklarına göre şifre kırma zamanları

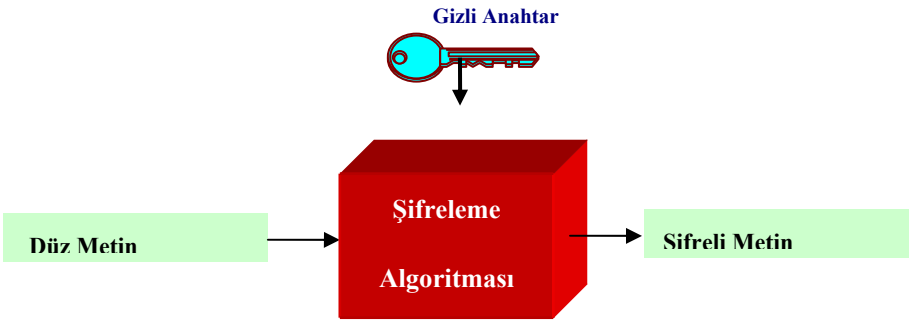
Anahtar Uzunluğu	**Sayı Değeri**	**10^2 şifre/sn**	**10^9 şifre/sn**	**10^{12} şifre/sn**
32 bit	~$4x10^9$	36 dk	2.16 sn	2.16 ms
40 bit	~10^{12}	6 gün	9 dk	1 sn
56 bit	~$7.2x10^{16}$	1142 yıl	1 yıl 2 ay	10 saat
64 bit	$1.8x10^{19}$	292 000 yıl	292 yıl	3.5 ay
128 bit	$1.7x10^{38}$	$5.4x10^{24}$ yıl	$5.4x10^{21}$ yıl	$5.4x10^{18}$ yıl

2.3.6. 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 [6].

Gizliliğin sağlanması, bilginin şifrelenmesi ile gerçekleştirilebilir. Şifrelemede en yaygın kullanılan yöntem "gizli anahtarlı şifreleme" adı verilen yöntemdir. Bu yöntemde mesaj şifrelenirken bir "anahtar" kullanılır ve şifrenin açılması için şifrelemede kullanılan anahtara ihtiyaç vardır. Şekil 2.11'de gösterilen bu şifreleme yönteminin güvenliği anahtarın gizli tutulmasına bağlıdır. Anahtar "0" ve "1"lerden oluşan bir bit dizisidir ve her şifreleme algoritmasında farklı boylarda anahtarlar kullanılır. Örneğin gizli anahtarlı şifreleme algoritmasına örnek olarak verilebilecek AES algoritmasında 128 bit anahtar kullanılır. Anahtarlar, üretilirken rasgele sayı üreteci denen fonksiyonlardan yararlanılır [4].

Yüzyıllar boyu kullanılan ve bir çok mesajı yabancılardan ve düşmanlardan korumaya yarayan gizli anahtarlı şifrelemenin de kendine özgü sorunları bulunmaktadır. Mesajın değiştirilmesinin önlenmesi, şifrelemede ve şifre çözmede kullanılan anahtarın gönderici ve alıcı arasında paylaşımı, mesajı gönderenin kimlik doğrulamasının yapılamaması bu sorunların en önemlileridir.

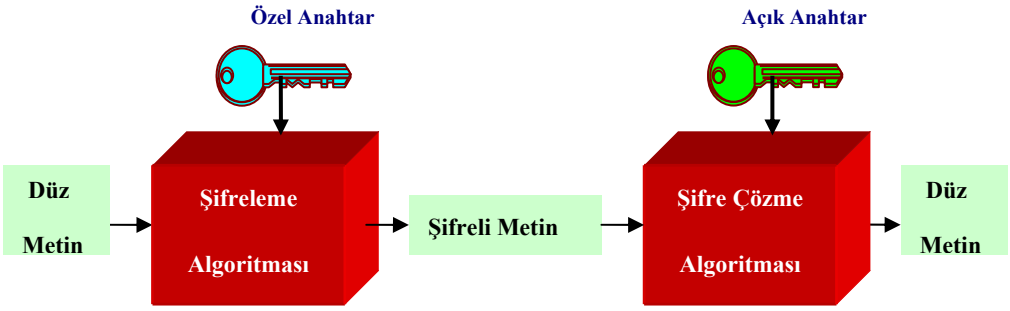


Şekil 2.11. Gizli anahtarlı şifreleme

Gizli anahtarlı şifrelemenin bu gibi sorunlarını aşmak için açık anahtarlı şifreleme yöntemleri geliştirilmiştir. Burada biri açık diğeri özel olarak nitelenen bir anahtar çiftinin bulunduğu (asimetrik) bir yöntem kullanılmaktadır. Şekil 2.12'de örnek olarak bir açık anahtar verilmiştir. Bu yöntemde kullanılan açık ve özel anahtarlar birlikte üretilirler. Yani matematiksel olarak aralarında gizli bir bağ bulunur. Bu sayede, Şekil 2.13'de görüldüğü gibi bir anahtar çiftindeki bir anahtar ile, diğer anahtarla şifrelenmiş bir metnin şifresi çözülebilir. Bununla birlikte bir anahtara sahip olan bir kişinin, matematiksel yollarla diğer anahtarı elde etmesi mümkün değildir. Açık anahtarlı şifreleme e-imza teknolojisinin temelini oluşturur [4].

```
MIIF4jCCBMqgAwIBAgIKQg6ypAAAAAAAJjANBgkqhkiG9w0BAQUFADCBsDELMAkGA1UEBhMCVVMxCzAJBgNVBAg
TAlVUMRcwFQYDVQQHEw5TYWx0IExha2UgQ2l0eTEeMBwGA1UEChMVVGhlIFVTRVJUUlVTVCBOZXR3b3JrMSEwH
wYDVQQLExhodHRwOi8vd3d3LnVzZXJ0cnVzdC5jb20xODA2BgNVBAMTL1VUTiAtIFVTRVJUcnVzdCBDbGllbnQgQXV
0aGVudGljYXRpb24gYW5kIEVtYWlsMB4XDTAwMDQyNzE3NDQyM1oXDTAxMDQyNzE3MzU1MFowgbQxKDAmBgkq
```

Şekil 2.12. Açık anahtar



Şekil 2.13. Açık anahtarlı şifreleme

Sonuç olarak şifreleme işlemi, açık bir metni, şifreli bir metine dönüştürmek için; yerine koyma, permütasyon veya bir dizi teorik yöntemleri (veya bunların bileşimlerini) kullanır. Şifreleme işlemi sonucu oluşan şifreli metin, şifre çözle işlemi ile ilk haline dönüşebilir. Şifreleme algoritmalarının herkes tarafından bilinebileceği, ama anahtarların gizli tutulacağı varsayılır. İki tür yaygın şifreleme tekniği vardır. Bunlar sırasıyla simetrik (gizli anahtarlı-private key) şifreleme ve asimetrik (açık anahtarlı-public key) şifreleme teknikleridir. Simetrik ve asimetrik şifreleme tekniklerinin karşılaştırması genel olarak Çizelge 2.4'de verilmiştir [3,6,10].

Çizelge 2.4. Simetrik ve asimetrik şifreleme yöntemlerinin karşılaştırılması

Simetrik şifreleme	**Asimetrik şifreleme**
Şifre ve şifre çözme işlemleri için tek anahtar kullanılır. (Gizli anahtar)	Şifre ve şifre çözme işlemleri için her kullanıcı iki anahtar kullanılır. (Açık anahtar ve özel anahtar)
Güvenli anahtar dağıtımı gerektirir.	Açık anahtar, özel anahtarın ele geçirilme riskinden bağımsız olarak dağıtılabilir.
Algoritmalar hızlıdır.	Simetrik şifreleme algoritmalarına göre yaklaşık 1500 kat daha yavaştır.
E-imza desteği yoktur.	E-imza desteği vardır.

Simetrik şifreleme

Simetrik şifrelemede şifreleme ve şifre çözme işlemi, alıcı ve gönderen tarafından bilinen bir anahtar ile yapılır. Her iki taraf da aynı algoritma ve anahtarı kullanırlar. Sistem, kullanılan anahtarın gizliliği kadar güvenlidir [11].

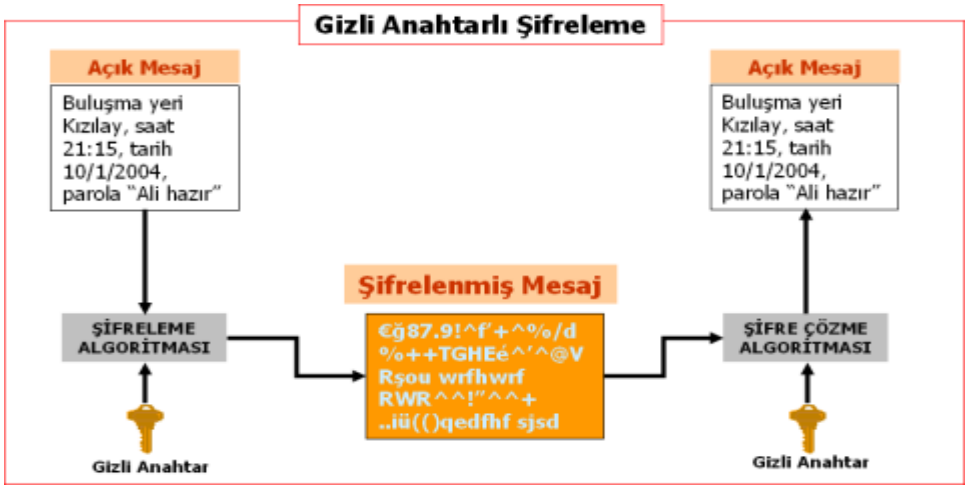
Simetrik şifrelemenin en önemli öğesi anahtar gizliliği olduğu için bu sistemde anahtar yönetimi de çok önemlidir. Genel olarak anahtar yönetimi birden-çoğa ve çoktan-çoğa olacak şekilde 2 yöntemle yapılır. Birden-çoğa yönteminde sistemdeki her kullanıcı aynı anahtarı kullanır. Bu nedenle herkes birbirinin şifreli mesajlarını açabilir. Dışardan kötü niyetli bir kişi de bu anahtarı elde ederse tüm sistemin

güvenliği yitirilmiş olur. Diğer yöntem olan çoktan-çoğa anahtar yönetiminde ise sistemdeki tüm taraflar kendi aralarında bir gizli anahtar üzerinde anlaşırlar. Böylelikle 2 kullanıcı arasındaki şifreli haberleşmenin üçüncü bir kullanıcı tarafından çözülmesi engellenmiş olur. Ancak bu durumda da anahtar yönetimi büyük problem olarak karşımıza çıkar [11]. Çünkü bu sistemde n adet kullanıcı için kullanılması gereken anahtar sayısı n*(n-1)/2 ile ifade edilir. Bu da 10.000 kullanıcılı bir sistem için 49.995.000 anahtar demektir.

Simetrik şifrelemenin kimlik doğrulama, bütünlük ve inkar edememezlik hizmetlerini sağlamaması en önemli dezavantajıdır. Dolayısıyla e-imza desteği yoktur. Ayrıca anahtar yönetimi de çok zordur. Ancak en önemli avantajı, asimetrik şifrelemeye göre yaklaşık 1500 kat daha hızlı çalışmasıdır.

Şekil 2.14'de simetrik şifrelemenin nasıl çalıştığı gösterilmiştir [6]. Buna göre;

- Mesajı gönderen kişi, yazmış olduğu mesajı gizli anahtar ile şifreleme algoritmasından geçirerek şifrelenmiş mesajı elde eder.
- Bu şifrelenmiş mesaj sadece onu şifreleyen gizli anahtar ile açılabilir.
- Karşı taraf bu şifreli mesajı aldığında, bu gizli anahtarı ve şifre çözme algoritmasını kullanarak mesajın şifresini çözer.



Şekil 2.14. Simetrik (gizli anahtarlı) şifreleme

Yaygın olarak kullanılan simetrik şifreleme algoritmaları ve bu algoritmalar hakkında özet bilgiler aşağıda açıklanmıştır:

a. DES algoritması: Bankacılık ve finans sektöründe ağırlıklı olarak kullanılan DES algoritması IBM firması tarafından 1974 yılında bulunmuş ve 1977 yılında Amerikan standardı olarak kabul edilmiştir [6].

Günümüzde bu algoritmanın 56 bit olan anahtar uzunluğu yeterli gibi görünse de mevcut teknolojilerle kısa sürede çözülebilmektedir. Bu algoritma 1997 yılında İsrailli araştırmacılar tarafından kırılmıştır. Bu algortimanın anahtar ve şifreleme güvenliğini artırmak için, 3DES (triple DES) adı verilen ve üç farklı anahtarla aynı bloğa üç defa DES uygulanarak çalışan yöntem geliştirilmiştir. 168 bit anahtar uzunluğuna sahip olan bu yaklaşım, günümüzde güvenli olarak kullanılabilecek bir şifreleme yaklaşımı olarak bilinmektedir [3].

DES algoritmasının hızlı olması (250 MHz hızındaki donanımda donanımsal olarak 1 Gbit/sn hızda çalışabilir) ve lisanssız kullanımının serbest olması önemli özelliklerindendir [6].

b. IDEA algoritması: IDEA algoritması Xuejia Lai ve James Massey tarafından geliştirilmiş ve 1992 yılından itibaren kullanıma sunulmuştur. PGP şifreleme sistemlerinde kullanılan güvenli bir algoritmadır. 128 bit anahtar uzunluğuna sahip olan algoritmanın kullanımı için lisans satın alınması gerekmektedir [6].

c. AES algoritması: AES algoritması A.B.D. tarafından yapılan bir yarışma sonucunda yeni Amerikan standardı olarak seçilmiştir. Bu algoritma, 128 bit uzunluğunda anahtarlar kullanmaktadır [6].

d. RC4 Algoritması: Ronald Rivest tarafından 1987 yılında bulunmuştur. 1994 yılında meçhul kişilerce kaynak kodu internette yayınlanmıştır. Kullanımı lisans gerektirmektedir. Değişken anahtar uzunluğuna sahip bir algortimadır [6].

e. Diğer simetrik algoritmalar: Bilinen diğer simetrik algortimalar ise 80 bit anahtar uzunluğuna sahip olan SKIP JACK, değişen 40-56 bit anahtar uzunluğuna sahip RC2 ve 2048 bite kadar anahtar uzunluğuna sahip olan RC5'tir [10,12].

Asimetrik şifreleme

Asimetrik şifreleme işleminde, her kullanıcı için 2 anahtar kullanılır. Bunlar açık anahtar ve özel anahtardır. Açık anahtar herkes tarafından bilinir. Özel anahtar sadece sahibi tarafından bilinir. Açık ve özel anahtar ikilisi sistem içinde birlikte kullanılmakta ve birinin şifrelediği metni diğeri açabilmektedir. Aralarında matematiksel bir ilişki bulunan bu iki anahtarın herhangi birisi kullanılarak, diğer anahtar elde edilemez. Şifreleme anahtarı bilinse dahi şifre çözme anahtarı bu bilgilerden bulunamaz.

E ve D sırasıyla şifreleme ve deşifreleme işlemini göstermek için kullanılırsa ve M de şifreli gönderilecek metin olarak bilinirse asimetrik şifreleme aşağıdaki dört özellikle tanımlanabilir:

- Şifrelenmiş M mesajının deşifre edilmesi tekrar M mesajını oluşturur;

D(E(M))=M

- Hem E, hem de D işlemleri kolay hesaplanabilir olmalıdır.
- Açık dağıtılan anahtarlardan gizli anahtarların hesaplanmaması gerekir.
- M mesajı önce deşifrelenir sonra şifrelenir ise yine M elde edilmelidir;

E(D(M))=M

Açık anahtarlı kripto sisteminde "M" metnini şifrelemek için öncelikle mesajı 0 ile "n-1" arasında sayı cinsinden ifade etmek gerekir. Sonra metnin "e" üzeri alınarak bulunan sayının "modulus n" işlemine tabi tutulması sonucu şifreli metin "C" elde edilmiş olur. Burada kullanılan "n" ve "e" pozitif sayılardır.

Deşifre işlemi için şifreli "C" metninin "d" üzeri alınır ve bulunan sayı "modulus n"

işlemine tabi tutulur. Böylelikle orijinal metin “M” elde edilir. Bu işlemlerde kullanılan “e” şifreleme anahtarı ve “d” deşifreleme anahtarlarının nasıl elde edildiği ise aşağıda anlatılmıştır.

Öncelikle “n” sayısı bulunur. Bunun için çok büyük iki asal sayı “p” ve “q” rastgele olarak seçilir. Bu iki sayının çarpımından “n” elde edilir.

$$n = p * q$$

Daha sonra rastgele olarak seçilen büyük bir “d” asal sayısı ile (p-1)*(q-1) eşitliğinin En Büyük Ortak Böleni’nin (EBOB) 1 olduğu görülür.

$$EBOB (d, (p-1)*(q-1)) = 1$$

Son olarak “d” sayısı ile çarpımın sonucunda bulunan ve (p-1)*(q-1) ile modulus işlemine tabi tutulduktan sonra 1’i veren “e” sayısı hesaplanır.

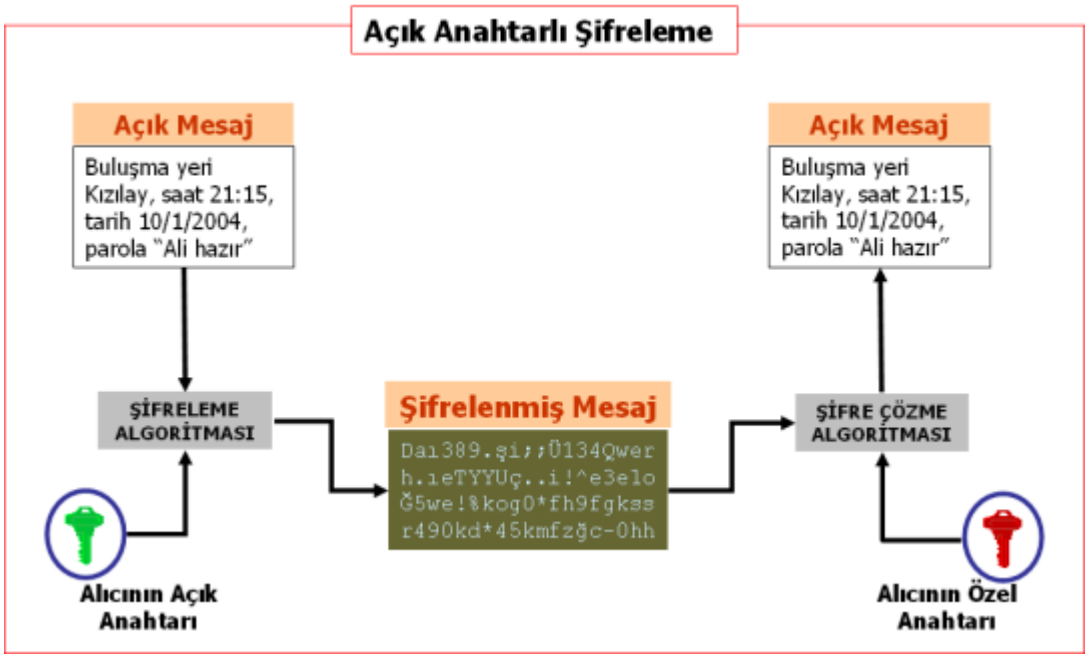
$$(e*d) \bmod ((p-1) * (q-1)) = 1$$

Böylelikle metni şifreleyecek ve deşifreleyecek anahtar ikilisi oluşmuştur. Kullanıcı “e”yi açık olarak yayımlar ve “d”yi özel anahtarı olarak gizli tutar.

Asimetrik şifrelemede anahtar yönetimi simetrik şifrelemeye göre daha kolaydır. Çünkü sistemi kullanan her kullanıcı için sadece bir anahtar çifti üretmek yeterlidir ve bu anahtarlar içinden açık olan anahtar tüm kullanıcılar tarafından bilinir. Yani “n” adet kullanıcı için “n” adet anahtar çifti oluşturmak yeterlidir. Ayrıca asimetrik şifreleme kriptoanalize karşı da dirençlidir. Bütünlük, kimlik doğrulama ve inkar edememezlik hizmetlerini sağlaması da e-imza sistemlerinde kullanımını sağlayan en önemli avantajlarından biridir. En zayıf yönü ise simetrik şifrelemeye göre yavaş çalışmasıdır [11].

Asimetrik şifrelemenin nasıl çalıştığı Şekil 2.15'de gösterilmiştir [6]. Buna göre;

- Mesajı gönderecek kişi, yazmış olduğu mesajı alıcıya ait olan ve herkese açık olan alıcının açık anahtarı ile şifreleme algoritmasından geçirerek şifreler.
- Alıcının açık anahtarı ile şifrelenmiş olan mesaj alıcıya gönderilir. Bu mesaj sadece alıcının özel anahtarı (sadece alıcıda bulunan) ile açılabilir.
- Alıcı şifreli mesajı kendine ait olan özel anahtarı ve şifre çözme algoritmasını kullanarak açar.



Şekil 2.15. Asimetrik (açık anahtarlı) şifreleme işlemi

Yaygın olarak kullanılan asimetrik şifreleme algoritmaları ve bu algoritmalar hakkında özet bilgiler aşağıda açıklanmıştır [10]:

a. RSA algoritması: RSA, en yaygın olarak kullanılan asimetrik algortimadır. R. Rivest, A. Shamir, L. Adleman tarafından 1978 yılında yayınlanmıştır. Adını mucitlerinin isimlerinin ilk harflerinden almıştır. Açık anahtar kriptografik sistemi ve e-imzalama yöntemi olarak kullanılır. Çarpanlara ayırma ve kök bulma problemleri

üzerine inşa edilmiştir [2]. 512 bit anahtar uzunluğuna (genişletilebilir) sahiptir. Çok güvenilir olmasına rağmen fazla hızlı değildir.

Algoritmanın kullandığı parametreler şunlardır:

Açık anahtar: n, e
Özel anahtar: d
n bileşik bir tamsayıdır (“modulus”)
e bir tamsayıdır (“açık üs ifadesi”)
d bir tamsayıdır (“gizli üs ifadesi”)
öyle ki “$ed \equiv 1 \pmod{(p-1)(q-1)}$” ve “p ve q sayıları n’in asal çarpanlarıdır.”

Algortimanın kullanımı:

Ayşe, Bora’ya “m” mesajını şifreli göndermek için “m”in “e”nci üssünü alır, yani “m”yi Boranın açık anahtarı ile şifreler. Böylelikle şifreleme işlemi gerçekleşir:

$c = m^e \bmod n$

Elde edilen “c” şifreli mesajını Bora’ya gönderir. Bora “c” sayısının “d”nci üssünü alır, yani “c”nin şifresini kendi özel anahtarını kullanarak çözer. Böylelikle şifre çözme işlemi gerçekleşir:

$m = c^d \bmod n$

b. Diffie-Hellman algoritması: W. Diffie ve M. Hellman tarafından 1976 yılında geliştirilmiştir. Birçok özel gerçekleştirimle birlikte temel algoritmadır. Ayrık logaritma problemine dayanır [1].

c. PGP algoritması: IDEA ve RSA tekniklerini birleştirmiş olan PGP algoritması, e-posta haberleşmesindeki kişisellik ihtiyacından doğmuş, yaygın kullanılan bir e-

posta şifreleme ve e-imzalama protokolüdür. PGP kullanımı ile iletilerin doğru kişiye ve değişmeden ulaşması amaçlanır. PGP, bilgiyi sıkıştırarak şifreler ve mesaja ekler. PGP servisleri arasında, e-imza, mesaj şifreleme, sıkıştırma, e-posta uygunluğu ve mesajın parçalara ayrılması sayılabilir [12].

Güvenli bir e-posta protokolü olan PGP'nin, ücretsiz ve açık kodlu olması ve güçlü şifreleme algoritmaları içermesi en önemli üstünlükleridir. Kullanımı çok da kolay olmayan bu protokolün, kendine has ve oldukça karmaşık bir güven ve sertifika modeli bulunmaktadır. Bu sayede, güvenlik konularında az da olsa bilgi sahibi olan birisi, kendi güven sistemini istediği şekilde oluşturabilmektedir [3].

d. El-Gamal algoritması: T. El-Gamal tarafından 1984 yılında geliştirilmiştir. Birçok özel gerçekleştirimle birlikte temel algoritmadır. Ayrık logaritma problemine dayanır. RSA'dan daha yavaştır.

e. DSA algoritması: DSA, ABD e-imza standardıdır.

Hibrit yaklaşımlar

Simetrik algoritmaların hızlı olması, asimetrik algoritmaların güvenilir fakat yavaş olması "Hibrit Kriptosistem" adı verilen bir yapının ortaya çıkmasına sebep olmuştur. Simetrik algoritmalarda en büyük problem anahtarın karşı tarafa iletimindedir. Bu yapı temelde bilginin simetrik bir algoritma ile şifrelenmesini, bu algoritmada kullanılan anahtarın da asimetrik bir algoritma ile şifrelenip gönderilecek bilgi ile iletilmesinde temel teşkil eder. Böylelikle bilginin şifrelenmesi, simetrik algoritmadan dolayı hızlı olup, anahtarın iletimi de, asimetrik algoritmadan dolayı güvenli olacaktır. Bu yapıların ortak kullanılması ile hız ve güvenlik bir arada sağlanabileceğinden, verimlilik artmaktadır. Bundan dolayı birçok işlemde, bu ve buna benzer yaklaşımlar tercih edilmekte ve geliştirilmektedir.

Steganografik yaklaşımlar

Bilişim teknolojilerinin gelişmesi ve yaygınlaşmasıyla birlikte bilgi güvenliği konusunda ortaya çıkan farklı yaklaşım ve metadolojilerden olan steganografik yaklaşımlar, kısaca, bir nesnenin içerisine bir verinin gizlenmesi olarak ifade edilebilir [3].

Steganografik işlemleri daha iyi anlamak için, temel yöntem olan en az öneme sahip bit (LSB:Least Significant Bit) kavramının bilinmesi gereklidir. Örneğin, bir resmin piksellerinin son bitlerinin mesaj bitleriyle yer değiştirmesiyle steganografi işlemi gerçekleştirilir. Bu işlem sonucunda resimde meydana gelecek değişim gözle görülemeyecek seviyededir. Böylelikle resmin içine bilgi gizlendikten sonra, beklendiği gibi, boyutlarda da çok fazla bir değişim gözlenmemektedir. Boyut değişikliğinin fazlaca olmaması ve işlemin uygulandığı nesnede değişikliklerin hissedilmemesi, şifreleme işleminin başarısının ayrı bir göstergesidir. Gizlenen bilginin tekrar elde edilebilmesi için deşifreleme işlemleri kullanılır. Bu yaklaşım ile ses, sayısal resim, video görüntüleri içerisine veri saklanabilir ve bu veriler metin dosyası olabileceği gibi, görüntü veya ses dosyaları da olabilir [14,15,16].

Kuantum şifreleme

Son dönemde üzerinde çalışılan ve yoğun ilgi toplayan diğer bir şifreleme yaklaşımı da kuantum şifrelemedir. Bu şifreleme yaklaşımına ilginin yüksek olmasının sebebi, haberleşmenin gizli veya açıktan dinlenme tehdidini tamamen ortadan kaldırmasıdır. Bu yaklaşım, optik haberleşmede fotonların kuantum özelliklerini temel almalarından dolayı mutlak güvenliği garanti etmektedir. Kuantum kriptolama kullanılarak gerçekleştirilen iletişimde, fiber optik ortam kullanılmasının yanında ilerde uydu haberleşmesinde de bu yaklaşımın kullanılmaya başlayacağı değerlendirilmektedir. Bu sayede gelecek yıllarda saniyede gigabit mertebesinde akan trafiği de şifreleyebilmek mümkün olabilecektir.

Kuantum anahtar dağıtımında, tek fotonluk alıcılar ve vericiler kullanılarak, kırılamayan anahtarlar iki taraf arasında güvenli ve hızlı bir şekilde değiş tokuş edilir. Kuantum yaklaşımıyla şifrelenen bir verinin, iki taraf arasında iletim sırasında, bir saldırgan tarafından araya girilerek okunmaya çalışılması halinde, kuantum fizik yasalarına göre, ortaya çıkan "kuantum gürültüsü" saldırganın veriyi çözebilmesini imkansız kılmaktadır. Buna karşın gerçek alıcı, elindeki anahtar sayesinde kuantum gürültüsünü ortadan kaldırarak orijinal veriye ulaşır [3].

Sayısal veri içindeki her bir bitin değeri, fotonlara polarizasyon uygulanarak belirlenir ve polarizasyon, elektrik alanının osilasyon yönüdür. Düşey ve yatay fotonları birbirinden ayırt etmek için, bir filtre ve diyagonal fotonlar için de ikinci bir filtre kullanılır. Foton, doğru filtreden geçirilirse, polarizasyonu değişmez, aksi halde polarizasyon rasgele bir değişime uğrar. İşte bu nedenle, iletim yolu üzerinde istenmeyen üçüncü bir şahıs veya saldırgan fotonları gözetlemeye çalışırsa, yüksek bir olasılıkla fotonların polarizasyonunu değişikliğe uğratacaktır. Bu girişim, alıcı tarafından kolaylıkla öğrenilebilecek ve sonuç olarak verici ve alıcı taraflar gerekli önlemleri alabileceklerdir [3].

2.3.7. Özetleme algoritmaları

Farklı uzunluklardaki verileri işleyerek, sabit uzunlukta veri oluşturma işlemine, özet veya özetleme (hashing) denir. Elde edilen özet verinin, orijinal veriyi temsil edebilecek bir formda olması beklenir. Bundan dolayı, elde edilen özet değerin mümkün olduğunca tekil olması veya benzerinin olmaması istenilir. Bu işlemde, bir özetleme (hash) fonksiyonu kullanılır ve bir grup veriden sabit uzunlukta bir dizi üretilir. Üretilen bu dizi, orjinal verinin bütünlüğünün test edilebilmesi için kullanılan bir imza niteliğindedir. Bu işlemleri gerçekleştiren algoritmalara, özetleme algoritmaları veya fonksiyonları denir. Bir özetleme fonksiyonu aşağıdaki özelliklere sahip olmalıdır [17]:

- Uzunlukları farklı olan verileri, sabit uzunluklu bir çıktıya dönüştürmelidir.

- Özet değeri kolay hesaplanabilmelidir.
- Özet değerinden mesajı elde etmek zor olmalıdır.
- Farklı mesaj veya dokümanlardan aynı özet değeri üretilmemelidir.
- Elde edilecek özet değeri tekil (unique) olmalıdır.
- Aynı özet değerini üretecek iki farklı mesajı bulmak oldukça zor olmalıdır.

Tüm özetleme fonksiyonları ortak ilkeler üzerinde çalışmaktadır. Girdi olan veri, n-bit'ten oluşan bloklara ayrılmakta ve her bir blok tek tek işlemden geçirilerek sonuçta n-bit'lik özet veri elde edilmektedir.

Özetleme algoritmaları, şifre doğrulama, bütünlük kontrolü, e-imza ve güvenli e-posta uygulamalarında kullanılmaktadır. Genellikle veri bütünlüğünü garanti etmesi, hızlı olması, sabit uzunlukta çıktı vermesi, açık anahtar algoritmalarından daha iyi olması, dosya boyutunun alınan özeti etkilememesi ve yüksek performanslı bir haberleşme sağlaması bu yaklaşımın üstünlükleridir.

Bugün, farklı güvenlik seviyelerinde kullanılan bir çok özetleme algoritmaları bulunmaktadır. MD serisi, SHA serisi, RIPE-MD-160 veya MAC algortimaları bunlardan bazılarıdır. Bu algoritmalara aşağıda kısaca açıklanmıştır:

MD serisi mesaj özetleme algoritmaları

MD serisi mesaj özetleme algoritmaları, Ron Rivest tarafından geliştirilmiştir. Son yıllara en çok kullanılan özetleme algoritmalarındandır. Bu algoritmaların tamamı, 128-bit özetleme sağlar. Bu serinin en yavaş algoritması MD2, en hızlısı ise MD4'tür. MD5, MD4'e göre daha kapsamlı geliştirildiğinden, hızı nispeten düşüktür. Tüm bu algoritmaların herkese açık olması önemli üstünlükleridir. MD5'in bazı zayıflıklarının bulunduğu Mayıs 1996'da Alman Bilgi Güvenliği Servisi'nde görev yapan Dr. Hans Dobbetin tarafından tespit edilmiştir. Uzun bir süredir yaygın olarak kullanılan MD5, güvenilir bir yaklaşım olarak kabul edilmiş olsa da, yapılan son araştırmalar, MD5'in kırılabileceğini göstermiş ve MD5'e duyulan güven kaybolmuştur [3].

MD5'in çarpışma saldırılarına karşı zayıf olduğunun keşfedilmesinden sonra, bilimadamları MD5 yerine SHA-1 veya RIPEMD-160 gibi alternatiflerin kullanılmasını tavsiye etmektedirler.

SHA-1 algoritması

SHA-1 (secure hashing algorithm-güvenli özetleme algoritması), ilk olarak NSA tarafından geliştirilmiş ve NIST'in desteğiyle, 1993 yılında ABD'de standart olarak kabul edilmiştir. Bu algoritma, MD serisi algoritmalardan daha uzun özet bit üretebilmektedir. 160-bit uzunluğunda üretilen bir dizi için gerekli süre MD5 algoritmasından yaklaşık olarak %25 oranında daha yavaş olsa da, kullanılması tavsiye edilen bir algoritmadır.

Bu algoritmanın ilk sürümü, karışıklığı önlemek amacıyla SHA-0 olarak adlandırılır. SHA-0 ve SHA-1, en fazla 264 uzunlukta mesajlardan 160-bitlik özet değeri üretir. NIST, 2001 yılında SHA'nın 256, 384 ve 512 bit versiyonlarıyla SHA-256, SHA-384 ve SHA-512 yapılabildiğini duyurmuştur. Son günlerde, bunun güncel bir versiyonu olan SHA-2 kullanılmaya başlanmıştır.

RIPE-MD-160 algoritması

RIPE-MD-160 algoritması, Avrupa Birliği'nde kullanılan bir algoritmadır. Farklı uzunluktaki dosya veya veriler için 160 bitlik sabit uzunlukta dizi üretmesi ve diğer şifreleme yaklaşımlarından daha hızlı olması, bilinen üstünlükleridir. Sadece bütünlüğü sağlaması ise, en önemli dezavantajı olarak bilinmektedir [13].

RIPE-MD-160'ın gelecek yıllarda güvenilir olacağı öngürülmekte ise de, bu algoritmanında bazı ataklara karşı zayıf olduğu birkaç farklı çalışmada vurgulanmıştır. Algoritmanın tasarımı MD4, MD5 ve RIPE-MD'nin zayıf yönlerinin değerlendirilmesi prensibine dayanmaktadır. İki farklı ve paralel hesaplama işleminin sonucunun, her bir sıkıştırma işlemi sonunda birleştirilmesi, bu fonksiyonun ayırt

edici özelliğidir. Diğer özetleme algoritmaları gibi, 32 bit işlemcilerde en iyi performansı verecek şekilde ayarlanmıştır. Bununla beraber, RIPE-MD'nin 258 bitlik ve 320 bitlik sürümleri de mevcuttur [3].

MAC algoritması

MAC algoritması, bilinen diğer bir ilginç özetleme algoritmasıdır. Diğer algoritmalardan farkı, bir MAC oluşturma veya doğrulama için, yalnız bir anahtara ihtiyaç duymasıdır. Bu özelliğin, özetlerin iletişim anında ele geçirilemeyeceğini doğrulama için önemli bir yaklaşım olduğunu savunanlar vardır. Anahtarlı özetlemeli mesaj doğrulama kodları (HMAC) (RFC 2104) ve SHA-1 temelli NMAC bu algoritmalara örnek olarak verilebilir. HMAC'lar, veri alışverişinde kullanıldığı gibi, herhangi bir şahıs dosyalarının değiştirilip değiştirilmediğini kontrol etmek amacıyla da kullanılabilir.

Mesaj özetleme algoritmalarının karşılaştırılması

Bosselaers, özetleme algoritmalarını hesaplama hızı bakımından karşılaştırmıştır. Çizelge 2.5'de verilen bu karşılaştırma, 90 MHz Pentium işlemcili bilgisayarlar ile çalıştırılarak, Assembler dilinde gerçekleştirilmiştir [3].

Çizelge 2.5. Özetleme algoritmalarının karşılaştırması

Algoritma	**Döngü no**	**Mbit/s**	**MB/s**
MD4	241	191,2	23,90
MD5	337	136,7	17,09
RIPEMD	480	96,0	12,00
RIPEMD-	592	77,8	9,73
SHA-1	837	55,1	6,88
RIPEMD-	1013	45,5	5,68

Bu algoritmalar, güvenilirlilik açısından karşılaştırıldığında, en güvenli olanının RIPEMD-160 olduğu ve ardından SHA-1 algoritmasının geldiği bilinmektedir. MD5'in güvenilirliği ise zayıflıklarından dolayı şüpheli bulunmaktadır.

2.4. Açık Anahtar Altyapısı

E-İmza'nın kullanılması için elverişli bir ortam sağlayan açık anahtarlı şifreleme yöntemleri, hedeflenen güvenlik gereksinimlerini karşılamakla birlikte bir takım zorluklara da sahiptir. Bunlar;

- Anahtar çiftlerinin üretimi,
- Anahtarla sahibinin eşleştirilmesi,
- Anahtarların tanınması,
- Özel anahtarın korunması,
- Farklı uygulamalarda aynı imzanın kullanılabilmesidir.

Yukarıda sıralanan sorunlara çözüm getirmek, açık anahtarlı şifreleme yöntemlerinin kullanımı yoluyla bütünlük, kimlik doğrulama ve inkâr edilmezlik hizmetlerini kullanıcılara vermek ve e-imza teknolojisinin kolay kullanımını sağlamak için gerekli teknoloji, standart, yasa, yönetmelik, kuruluş, ürün ve hizmetlerin bütününe "Açık Anahtar Altyapısı (AAA)" denir [4].

Son yılların önemli teknolojilerinden olan AAA'nın temelleri açık anahtar tabanlı şifreleme (public key cryptography) ile aynı yıllara, yani 1970'lerin sonuna dayanır. Amaç, Diffie ve Hellman'ın temellerini attığı bu modern şifreleme sisteminin en büyük sorunlarından biri olan açık anahtarların kimlik doğrulamalı bir şekilde dağıtımını çözmektir. Herkesçe bilinmesinde bir sakınca olmayan bu açık anahtarlar bir şekilde kişilere dağıtılmalı ancak açık anahtarlar ile sahipleri arasında da güvenilir bir bağ yaratılmalıdır [18].

Sayısal sertifikalar, ortaya atılan ilk çözümlerden biridir. Bu sistemde güvenli bir

Sertifika Otoritesi (CA – Certificate Authority) kişilerin açık anahtarları ile kimlikleri arasındaki bağıntıya kefil olarak kendi e-imzaları ile sertifika yaratır. CA'nın imzasını doğrulayan ve ona güvenen herhangi bir kullanıcı da istediği kişinin açık anahtarını öğrenir. Çok kolay gibi gözüken bu sistemde organizasyonel ve yönetimsel olgular ön plana çıkmaktadır. Kimlerin hangi koşullar altında güvenilir CA olabileceği, CA'ların sertifika üretimi sırasında izleyeceği işlem ve çevrim-dışı (off-line) kurallar, sertifika iptali ile ilgili kural ve uygulamalar bu tür olgulara örnek olarak verilebilir. Bu nedenle AAA, sayısal sertikaların kullanımı ile ilgili bütün oluşumların bir araya toplanmış hali olarak tanımlanabilir [25].

2.4.1. Açık anahtar altyapısının gerekliliği

Gizliliğin sağlanması için yapılması gereken işlem, bir şifreleme yöntemiyle mesajın gizlenmesidir. Ancak şifreleme, diğer güvenlik sorunlara bir çözüm getirmez. Yani, kimlik bilgisiyle ilişkilendirilmediği gibi, mesajın yolda başkası tarafından değiştirilip değiştirilmediğinin anlaşılmasına da yardımcı olmaz. Öte yandan, simetrik bir şifreleme yönteminde, şifreleme anahtarlarının mesajlaşan taraflar arasında taşınması ve paylaşılması da gizliliğin korunması için ayrıca ciddi bir sorun oluşturur.

Açık anahtarlı şifreleme yöntemleri, biri açık diğeri gizli olarak nitelenen bir anahtar çiftinin kullanıldığı (asimetrik) yöntemlerdir. Buna göre, çiftin bir anahtarı diğerinin şifrelediğini çözmede kullanılır. Buna karşın, açık anahtar bilgisinden yola çıkarak gizli anahtarı üretmek de mümkün değildir.

Açık anahtarlı şifreleme yöntemleri ile güvenlik sorunlarının çözümü için iyi bir yöntem keşfedilmiştir. bu yöntem ile kişiler, başkasında bir eşi daha olmayan bir anahtar çiftinin gizli anahtarıyla e-imza oluşturabilirler. İmzayı doğrulamak için açık anahtar kullanılır. Eğer kimde hangi anahtar çiftinin bulunduğu (daha doğru bir ifadeyle, hangi açık anahtarın kimde olduğu) bilinirse, imza doğrulanırken kimlik de doğrulanmış olur. Aynı zamanda, mesajın yolda değiştirilmiş olması durumunda

imza doğrulanamayacağı için, mesajının bütünlüğünün korunup korunmadığı da anlaşılmış olur.

Bu kapsamda açık anahtarlı şifreleme yöntemleri, elektronik güvenliğin ana gereksinimleri olan gizlilik, bütünlük, kimlik doğrulama ve inkar edememeyi sağlamaktadır. Ancak bunlar kendi başlarına uygulanamazlar. Bu noktada akla aşağıdaki gibi birçok soru gelecektir:

- Sertifikayı kim verir?
- Anahtar çiftleri nasıl üretilir?
- Özel anahtar nerede saklanır?
- Karşı tarafın özel anahtarının güvende olduğundan nasıl emin olunur?
- Sertifikalar nerden bulunup alınır?
- Çok büyük sayılar olan bu anahtarları (örneğin RSA yönteminde önerilen anahtar uzunluğu olan 1024 bit, yaklaşık 350 basamaklı bir sayıya karşılık gelir) kişiler nasıl tanıyacak ve anahtarın sahibi olan kişiyle eşleştirecekler?
- Farklı uygulamalarda aynı imzaların geçerli olması nasıl sağlanacak?
- İmzanın yaygınlıkla kullanılması ve hukuki sonucu olması için gerekli teknik altyapı ve güven nasıl sağlanacak?

Bu soruların sayısı daha da arttırılabilir. Ancak AAA gibi sayısal sertifika ve e-imza bazlı bir güvenlik sistemi ile yukardaki soruların çözümleri için gerekli temel oluşturulabilir [44].

Ayrıca e-imza desteği sadece asimetrik şifreleme yöntemlerinde bulunmakta, simetrik şifrelemede bulunmamaktadır. Asimetrik şifreleme sistemlerini gerçeklemek için ve oluşturulacak olan anahtar çiftlerini (açık ve özel anahtarlar) yönetmek için AAA gereklidir [27].

AAA sistemleri, kimlik doğrulama, inkar edememezlik, mesaj bütünlüğü ve gizlilik gibi hizmetleri simetrik kriptografinin kullanıldığı bir yöntemle sunar. Böylece

anahtar dağıtımı ve e-imza özelliklerini asimetrik şifrelemenin, gizlilik hizmetini simetrik şifrelemenin sağladığı güvenli bir altyapı oluşturulmuş olur.

E-imza yasaları içersinde öngörülen mekanizmalar yoluyla sayısal ortamda gerçekleştirilen işlemlere hukuki korunma sağlanırken aynı zamanda teknik açıdan bu işlemlerin orijininin tespiti, gizliliği, bütünlüğü ve inkar edilmezliği sağlanmaktadır. Dünya pratiği ve Avrupa Birliği ülkelerine bakıldığı zaman %90'ı aşan bir oranda e-imza uygulamalarında AAA teknolojisi kullanıldığı ve kanunlaştırılmalarında da bu teknolojiyi temel alan çözümlemeler üretildiği gözlemlenmektedir. Düzenlemelerin belli bir teknoloji hedef alarak gerçekleştirilmemesi gerektiği yolundaki teknoloji yansızlık (technology neutrality) ilkesi ile bu tutum çelişki yaratıyor gibi görünse de, mevcut ihtiyaçlar ve dünya pratiği, tutarlı bir düzenleme yapılması için bu durumu gerekli kılmaktadır. Bununla birlikte, yasa bünyesinde diğer e-imza teknolojilerinin kullanımına izin veren mekanizmaların bulunması teknoloji yansızlık ilkesini sağlayacaktır. Diğer bir ilke de, e-imza kullanımı konusunda belirli standartların sağlanarak e-imzaların küresel ağlar ve farklı etki alanlarında kullanılabilecek bir yapıda üretilmesinin sağlanması ve imzaların temelini oluşturan elektronik sertifikaların karşılıklı işlerliliklerini (inter-operability) gerçekleştirecek mekanizmaların tasarıya uyarlanmasıdır [28].

2.4.2. Açık anahtar altyapısı değerlendirme kriterleri

Başarılı bir AAA'nı değerlendirmede 6 ana kriter kullanılmaktadır. Bunlar;

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

Bir AAA'yı tercih edecek olan kullanıcıların, satın alacakları hizmetin fiyatını düşünmeden önce, yukarıda belirtilen hususları dikkate almaları faydalı olacaktır. Bu hususlar, ileride karşılaşılabilecek problemlerin azaltılması açısından önem arzetmektedir [3].

2.4.3. Açık anahtar altyapısı uygulama alanları

Son zamanlarda birçok özel ve kamu kuruluşu, müşterilerine özellikle de uluslararası ticaretde gerektiği durumlarda daha hızlı ve esnek hizmet sunmanın yollarını araştırmaktadır. Buna bağlı olarak da bugün AAA uygulamaları kamudan finansa, endüstriden telekoma kadar birçok sektörde, çok geniş bir uygulama yelpazesinde kullanılmaktadır. AAA hizmetlerinin kullanıldığı başlıca sektörler aşağıda sıralanmıştır [29]:

- Bankalar, şube ağına sahip sigorta şirketleri,
- Büyük kurum ve kuruluşlar,
- Üniversiteler,
- Kamu kuruluşları,
- Finansal kuruluşlar,
- Yüksek iletişim ve güvenlik gereksinimi olan organizasyonlar,
- Açık anahtar şifreleme sistemi kullanan organizasyonlar,
- Sağlık hizmeti sunan kuruluşlar,
- Teknoloji ve ARGE şirketleri,
- İlaç şirketleri,
- Üretim,
- Posta hizmeti sunan firmalar.

AAA kullanımının yaygınlaşması, bu yapının uygulama alanlarını bilme veya belirlemeyle doğru orantılıdır. Yukarıda listenenen ve bilişim teknolojilerinin yoğun olarak kullanıldığı sektörlerde AAA hizmetleri kolaylıkla uygulanabilir. AAA'nın uygulama alanlarından bazıları aşağıda listelenmiştir:

- Güvenli e-posta haberleşmesi (S/MIME),
- Verilerin imzalı ve şifreli saklanması (Masaüstü güvenliği/Desktop security),
- Akıllı kartla güvenli oturum açma (Windows logon, Kerberos),
- İmzalı formlar (Signed forms),
- Sayısal noter,
- Kod imzalama,
- XML imzalama,
- İnternet protokolü güvenliği (Internet protocol security, IPSEC),
- Taşıma katmanı güvenliği (Transport layer security, TLS),
- Güvenli yuvalar katmanı (Secure socket layer, SSL),
- Güvenilir zaman damgası (Time stamp protocol, TSP),
- Sanal özel ağ (Virtual private network, VPN),
- E-birey veya e-vatandaş,
- E-ticaret, e-iş, e-bankacılık, e-kimlik, e-devlet, e-kurum, e-cüzdan, e-sınav, e-eğitim, e-imza, e-bilim, e-üniversite, e-yaşam, e-sağlık, vb.

E-imza uygulamlarının yaygınlaşması, yukarıda belirtilen alanlarla da sınırlı olmayıp, ülkelerin sayısal ortamları kullanım oranları ve e-devletleşme süreçleriyle doğru orantılıdır.

2.4.4. Açık anahtar altyapısı 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 bir çok problem aşılmış olsa da yine de bazı noktalarda problemler ortaya çıkabilmekte ve kimi soru işaretleri oluşabilmektedir. Bu soru işaretlerinden bazıları aşağıda listelenmiştir [3,30]:

- Kime güvenmeliyim? Niçin?
- Anahtarım kopyalanabilir mi?

- Doğrulamayı yapan bilgisayar güvenli mi?
- Benim ismimde 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 açıkları yok mu?

Teknolojilerdeki gelişmeler ile, yukarıda sıralanmış olan soruların bir çoğu her geçen gün ortadan kaldırılmakta ise de, çok az da olsa, bazı problemler oluşabilecektir. Bu problemlerin en önemlileri aşağıda listelenmiştir:

- Bilgi ve bilgisayar sistemleri güvenliğinin bilinmesi zorunluluğu,
- Kayıt esnasında yaşanabilecek zorluklar,
- Sertifikaların ücretli olarak sunulması,
- Sertifikaların tekrar üretilmesinde karşılaşılan problemler,
- Kullanılacak makamlara güven sorunu,
- İptal edilmiş sertifikaların zamanında öğrenilememesi,
- Sertifika iptalinin getirdigi ek yükler,
- Uygulamalarda yaşanabilecek, fakat o ana kadar karşılaşılmayan problemler,
- Sunucu bilgisayarların sistemler arası bilgi alışverişini otomatik olarak yapmalarından dolayı karşılaşılabilecek sorunlar.

Sertifikaların KM'de üretilmesi esnasında, sertifika alma talebinde bulunan kişilerin, kimlik bilgilerine ve belgelerine ihtiyaç duyulmaktadır. Bu bilgi ve belgelerin sağlanması ise, sertifika sahibi olmayı zorlaştırmaktadır.

Her ne kadar deneme amaçlı veya belirli bir süre ücretsiz olarak verilen sertifikalar bulunsa da asıl sertifikalar ücret karşılığı verilmektedir. Bu sertifikalar sınıf-1 (class-1), sınıf-2 (class-2) ve sınıf-3 (class-3) gibi gruplandırmalarla, birbirinden ayrılırlar. Sınıf-1 tipi sertifikalar ücretsiz olarak, belirli bir süre verildikleri için, ataklara maruz kalabilirler. Genellikle, geçici süreyle verilen sertifikalarda, süre bitiminde aynı

anahtarın kullanımına devam edilmesinin istenildiği durumlarda, ücretli sisteme geçilmesi gerekmektedir. Daha yüksek derecede güvenlik ve kimlik doğrulama işlemleri gerektiren durumlarda sınıf-2 ve sınıf-3 sertifikaları kullanılmalıdır. Bu sertifikalar için dönemlik ücretlerin ödenmesi gerekmektedir [3].

Sertifika üretmede kullanılan yazılımlar, internetten kolaylıkla elde edilebilmektedir. Dolayısıyla, buna zaman ayıran kişiler, kişisel bir SM ve/veya bir KSM ve buna bağlı SM'ler kurarak, ücretsiz olarak sertifika dağıtabilir. Bu SM'lerin güvenli makamlar arasına girmesi mümkün olmasa da, kişisel olarak oluşturulan makamlar kafa karıştırıcıdır. Bu yüzden kullanıcılar, güven duyulan SM'ler tarafından üretilen sertifikalara da aynı kuşkuyla bakabilmektedirler. Bu da AAA yapısına duyulması gereken güveni zayıflatmaktadır.

Sertifikalar belirli bir süre için üretilirler. Bu süre içerisinde karşılaşılabilecek bazı durumlardan dolayı, sertifikalar iptal edilebilir. Bu durumda, kullanılacak olan sertifikaların iptal edilip edilmediğinin sorgulanması gereklidir. Bu, hem kullanıcıya, hem de SM'lere ek yükler getirebilmekte ve karşılıklı olarak sıkıntılara sebebiyet verebilmektedir.

AAA'yı kurmak zahmetli ve pahalı bir iştir. Mevcut uygulamaların da, bu altyapıya uygun hale getirilme zorunluluğu, kurumların veya kuruluşların uygulama değişikliklerinde yeni yatırımlar yapmayı istememeleri, gerek kurulumda karşılaşılabilecek bazı zorluklar, gerekse zaman ve bant genişliği eksikliği, gerekse de virüs korkusu, yazılım kurmayı gerektiren uygulamaların yaygınlaşmasını engelleyebilecek hususlardır.

3. KURUMSAL AĞLARDA ELEKTRONİK İMZA SİSTEMLERİ

Bu bölümde e-imza ve kurumsal ağlar için AAA tabanlı e-imza sistemleri detaylı olarak anlatılmıştır. Bu kapsamda e-imza ile ilgili teknik detaylar, e-imza türleri, e-imza modelleri, uygulama alanları ve kurumsal ağlarda e-imzanın temelini oluşturan AAA sisteminin tüm bileşenleri incelenmiştir.

E-imza, elektronik ortamda iletilen bilgilerin, gönderen kuruma ya da kişiye ait olduğunu doğrulayarak, verinin başkası tarafından yollanmadığını garanti eder. E-imzalar göndericinin kimliğinin açık ve net bir biçimde teyidini (kimlik doğrulama-authentication), elektronik dokümanın orjinalliğini ve güvenilirliğini (bütünlük-integrity) mümkün kılar. E-imza ile imzalanmış bir belgeyi yollayan kişi, onu yolladığını, alıcı da aldığını inkar edemez (inkar edememe-non repudiation). İnternet üzerinden yollanan bilgilerin güvenliği e-imza kullanımı ile sağlanabilir [10].

E-imza, bir veri bloğuna özgü olarak hesaplanan özet bilgiye verilen addır. E-imza hesaplanırken kişiye özgü özel anahtar kullanılır. Bu yüzden farklı kişilerin aynı veri bloğu için hesapladığı e-imzalar farklı olur. Bunun yanısıra bir kullanıcının değişik veri blokları için hesaplayacağı e-imzalar da birbirinin aynısı olmaz. Bu iki özellik e-imzanın kişiye özel olmasını matematiksel olarak garanti eder.

Günümüzde internetin ve e-ticaretin yaygın kullanımı 2 nci bölümde bahsedilen güvenlik risklerini daha fazla gündeme getirmiş ve bunları ortadan kaldıran AAA sistemlerinin kullanılmasını kaçınılmaz hale getirmiştir. Ayrıca hukuki açıdan e-imzanın ıslak imza ile eşdeğerde tutulması birçok bilişim uygulamasına da AAA entegrasyonunu neredeyse zorunlu hale getirmektedir.

3.1. Elektronik İmza Tanım ve Kavramları

E-imza ile ilgili kavram kargaşasını ortadan kaldırmak için öncelikle “e-imza”/“sayısal imza”/”dijital imza” kavramları kendi sınırları içinde ele alınmalıdır. E-imza, “başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal

bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri" olarak tanımlanabilir [26]. Ancak bu tanımın olabildiğince geniş olduğu gözden kaçmamalıdır. Örneğin optik yolla da imza oluşturulabilir: Kağıt üzerine elle atılan bir imzanın sayısal bir fotoğraf makinesiyle fotoğrafı çekilip kullanılabilir. Ya da doğrudan elektronik bir kalemle tahtaya veya ekrana atılan bir imza da aynı şekilde kullanılabilir. Hatta, sadece kullanıcı adı ve şifre bilgileri bile kimlik doğrulamaya yaradığından e-imza sayılabilir. Bugün akla gelmeyen veya kullanılmayan ancak bu tanıma göre e-imza sayılabilecek başka teknolojiler de olacaktır (Yüz tanıma, ses tanıma, biyometrik yöntemler, genetik yöntemler vs.).

Tanımın bu kadar geniş olması yadırgatıcı bulunabilir. Neyin e-imza sayılabileceğini söylemektense neyin sayılamayacağını söylemek daha güç görünebilir. Ancak bu tanım dışında kalan pek çok uygulama vardır. Örneğin, her kullanıcı adı ve şifresi e-imza sayılmaz. Kullanıcı adı ve şifresinin nasıl belirlendiği önemlidir. Kendinizi dilediğiniz gibi tanıttığınız web sitelerinden almış olduğunuz kullanıcı adı ve şifresi, kimlik doğrulaması amacıyla kullanılamaz. Çünkü aynı kimlik bilgileriyle farklı kullanıcı adı ve şifreleri almak mümkündür. Benzer bir biçimde, elektronik veriye eklenen tek bir "a" harfi de e-imza sayılmaz, bu "a" harfinin kimlik doğrulama amacıyla kullanılmakta olduğu ikna edici bir önerme değildir [19].

E-imza tanımının ikinci bölümü, bu noktada anlamlandırılabilir: Yukarıda sayılan durumların hiç birinde, eklendiği veriyle "mantıksal bağlantı içinde olma" söz konusu değildir. Her zaman aynı kullanıcı adı ve şifresi kullanılır, her mesaja aynı imza resmi eklenir; dolayısıyla bunların eklendiği veriyle mantıksal bir bağı olmaz.

Tez çalışması genelinde kavram kargaşasına neden olmamak için konuyla ilgili olan "sayısal imza", "dijital imza" gibi diğer kavramlar kullanılmamış ve tez genelinde sadece "e-imza" kavramı kullanılmıştır.

E-İmza Kanunu'nda bulunan e-imza tanımı ve diğer önemli tanımlar aşağıdadır:

Elektronik İmza: Başka bir elektronik veriye eklenen veya elektronik veriyle

mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veridir.

Elektronik Veri: Elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıtlardır.
İmza Sahibi: E-imza oluşturmak amacıyla bir imza oluşturma aracını kullanan gerçek kişidir.

İmza Oluşturma Verisi: İmza sahibine ait olan, imza sahibi tarafından e-imza oluşturma amacıyla kullanılan ve bir eşi daha olmayan şifreler, kriptografik gizli anahtarlar gibi verilerdir. Bu tanım uygulamada "private key" olarak bilinen özel veya kapalı anahtarı belirtmektedir.

İmza Doğrulama Verisi: E-imzayı doğrulamak için kullanılan şifreler, kriptografik açık anahtarlar gibi verilerdir. Bu tanım uygulamada "public key" olarak bilinen açık anahtarı belirtmektedir.

İmza Oluşturma Aracı: E-imza oluşturmak üzere, imza oluşturma verisini kullanan yazılım veya donanım aracıdır. Uygulamada imza oluşturma araçları donanım bazlı olarak akıllı kartlar (smart cards), akıllı çubuklar (USB tokens), bilgisayarlar veya veri işleme kapasitesi olan el terminalleri (PDA, cep telefonları, Pocket PC'ler v.b.) ile yazılım bazlı olarak da bilgisayar programları, işletim sistemleri veya özel yazılımlar v.b. şeklinde karşımıza çıkabilmektedir [20].

İmza Doğrulama Aracı: E-imzayı doğrulamak amacıyla imza doğrulama verisini kullanan yazılım veya donanım aracıdır.

Güvenli E-İmza: Kanuna göre;

- Münhasıran imza sahibine bağlı olan,

- Sadece imza sahibinin tasarrufunda bulunan güvenli e-imza oluşturma aracı ile oluşturulan,
- Nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan,
- İmzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan e-imzalar güvenli e-imzadır.

Güvenli e-imzaların önemi elle atılmış imza ile aynı hukuki sonucu doğurmalarıdır. Yabancı mevzuatta bu hukuki etkiye sahip e-imzalar çeşitli adlarla (nitelikli, evrensel, e-imza v.b.) ve farklı teknik gereksinimlerle tanımlanmıştır. Ancak bütün bu imzaların ortak noktası, nitelikli elektronik sertifikaya dayanarak ve güvenli e-imza oluşturma aracıyla oluşturulmuş olmalarıdır.

Elektronik Sertifika: İmza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kayıttır. Elektronik sertifikalar; imzalama-doğrulama işlemi sırasında imzalayanın kimliğinin güvenilir üçüncü taraf (ESHS) tarafından teyit edilmesi amacıyla kullanılırlar.

3.2. Elektronik İmzanın İşlevi

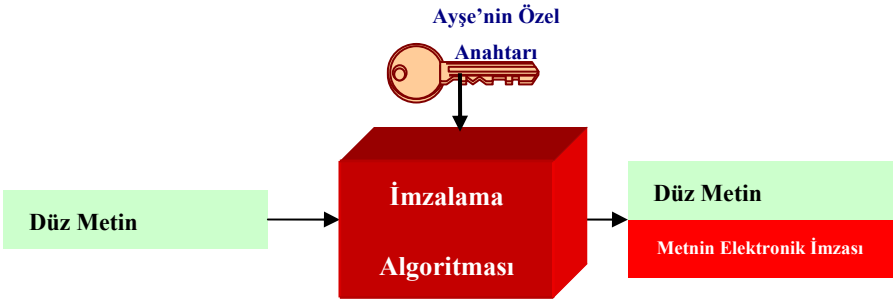
Yazılı dokümanlarda kullanılan ıslak imzalar gibi, e-imzalar da günümüzde e-posta veya elektronik verilerin yazarlarını/sahiplerini tanılamada kullanılmaktadır. E-imzalar, elektronik sertifikalar kullanılarak yaratılır ve doğrulanırlar. Bir bilgiyi imzalamak, güvenli bir alışverişi gerçekleştirmek için kullanıcıya özel elektronik sertifikaya ihtiyaç vardır. Günümüzde uluslararası yasama organları e-imzaları ıslak imzalar gibi yasal olarak bağlayıcı ve uluslararası çapta kabul edilebilir kılmak için yasalar çıkarmışlardır [5].

E-imzaların sağladığı başlıca önemli işlevleri kimlik doğrulama, gizlilik, veri bütünlüğü ve inkar-edilememezliktir.

3.3. Elektronik İmzanın Yapısı

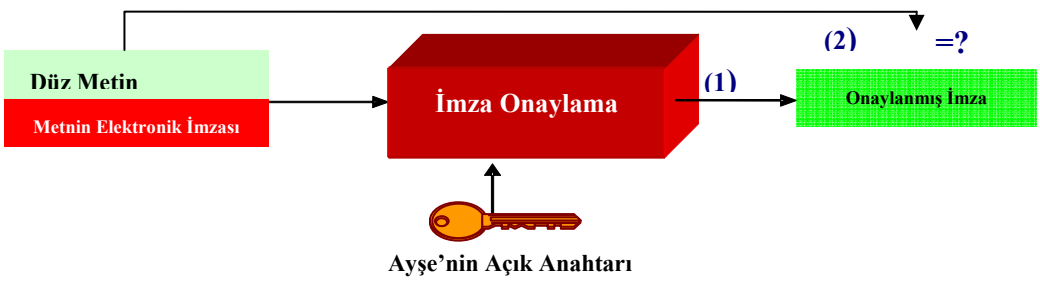
Bu bölümde e-imzanın nasıl çalıştığı bir senaryo üzerinden anlatılacaktır. Bu senaryoda, Ayşe kendi oluşturduğu bir e-postayı imzalayarak Barış'a güvenli bir şekilde ulaştırmak istemektedir. Ayşe'nin bir açık, bir de özel anahtarı vardır ve açık anahtarını Barış'a daha önceden ulaştırmıştır. Bu gönderim şu şekilde gerçekleşir [4]:

1. Ayşe, Şekil 3.1'de görüldüğü gibi, özel anahtarı ile göndereceği metni şifreler, böylelikle metnin imzasını oluşturmuş olur. Ayşe'nin özel anahtarı, Ayşe'den başkasında olmadığından ve başka bir anahtar kullanarak bu imzanın birebir aynısını oluşturmak mümkün olmadığından, üretilen bu imza bilgisi Ayşe'ye özeldir.



Şekil 3.1. E-imzanın oluşturulması

2. Ayşe imzalı metni Barış'a gönderir.
3. Barış, Ayşe'nin açık anahtarını kullanarak imzayı onaylama işlemini gerçekleştirir (Şekil 3.2-1. adım). Ortaya çıkan onaylanmış imza metni ile düz metin aynı ise imza doğrulanmış olur (Şekil 3.2-2. adım).

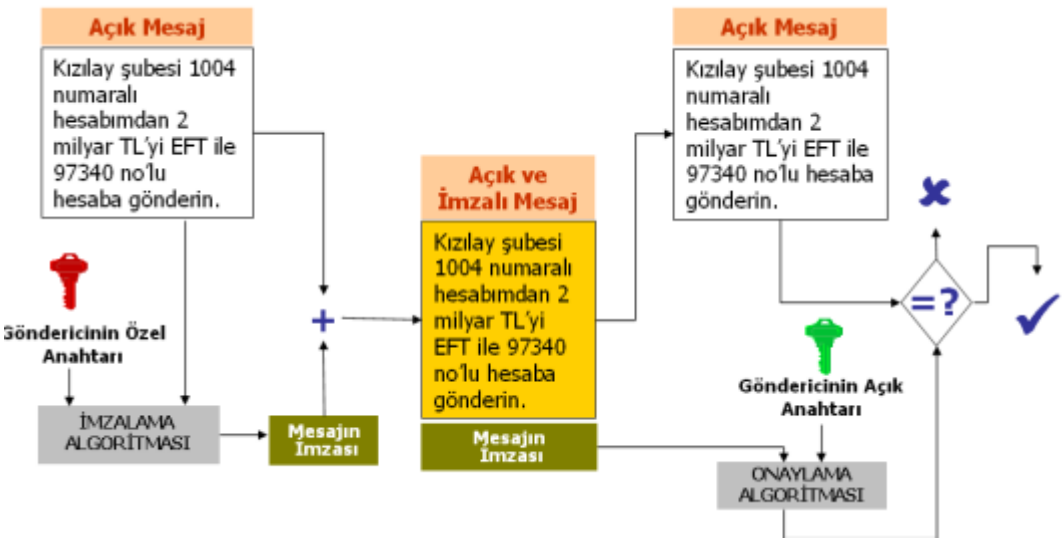


Şekil 3.2. E-imzanın onaylanması

Buradaki senaryoda, Ayşe, imza bilgisini düz metnin sonuna ekleyerek Barış'a göndermiştir. Barış, Ayşe'nin e-imzasını onayladıktan sonra aşağıdaki sonuçlara varabilir [4]:

- "Düz metin değiştirilmeden bana ulaştı",
- "Metnin e-imzası Ayşe'nin açık anahtarı ile doğrulandı. Demek ki bu imza Ayşe'den başkası tarafından atılmış olamaz. Öyleyse mesajı gerçekten Ayşe gönderdi",
- "Daha sonra Ayşe bana gönderdiği bu mesajı göndermediğini iddia ederse, ona yalnızca kendisi tarafından özel anahtarını kullanarak oluşturulabilecek e-imzasını gösterebilirim".

E-imza ile bir veriyi imzalamak için asimetrik şifreleme yöntemi kullanılır. E-imza, imzalanacak verinin imzalayacak kişiye ait özel anahtarla imzalama algoritmasından geçirilmesiyle elde edilir ve mesajın sonuna eklenir. En yaygın imzalama algoritmaları RSA, DSA ve ECDSA'dır. E-imza ile bir mesajın imzalanması Şekil 3.3'te tek bir şekil üzerinde gösterilmiştir [6].



Şekil 3.3. E-imzanın yapısı

İmzalanacak metnin boyu büyüdükçe imzalama süresi ona bağlı olarak yükselir. Pratik uygulamalarda açık anahtar algoritmaları, uzun metinlerin imzalanmasında, imzalama süresinin saniyeler hatta dakikalar alması nedeniyle başarım açısından çok yetersiz kalmaktadır. Metin boyutlarının çok değişken olması imzalama sürecinin ne kadar zaman alacağına ilişkin net bir tahmin yapılmasını engellemektedir. Buna ek olarak, imzalanacak veri ile e-imza aynı boydadır. Yani e-imza verisinin boyu, imzalanan verinin boyuna eşittir. Yukarıdaki örnekte olduğu gibi düz metnin doğrudan imzalanması, iletim hattının iki kat daha fazla kullanılmasına neden olacaktır [4].

E-imza ile ilgili bu problemleri çözmek ve başarımı arttırmak için elektronik olarak imzalama yapılmadan önce tek-yönlü özet algoritması (hash) kullanılarak metnin sabit uzunlukta bir özeti üretilir.

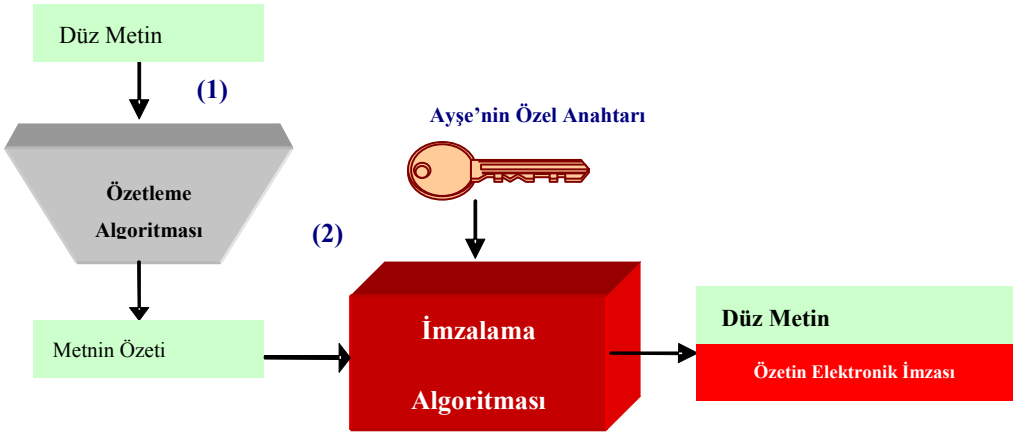
3.4. Mesaj Özeti

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 [6]. En çok bilinen özet algoritmaları MD5 ve SHA-1'dir. Mesaj özeti elde etmek için kullanılan fonksiyonların özellikleri aşağıda listelenmiştir:

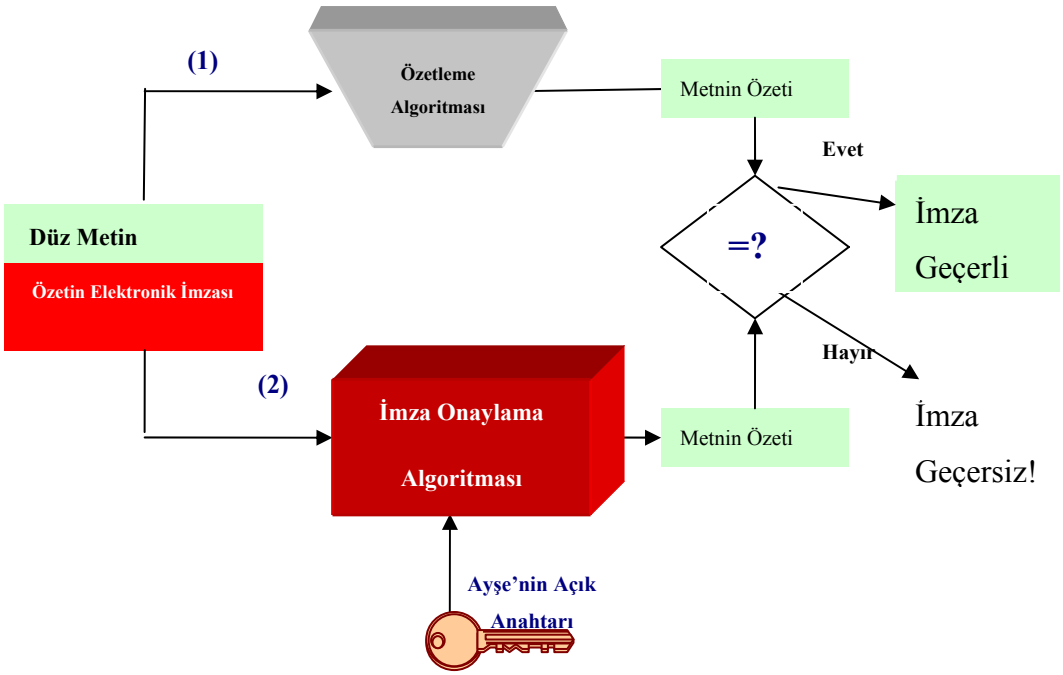
- Özet fonksiyonları mesajdan çok kısa bir sabit çıkış uzunluğu üretirler. Mesaj hangi uzunlukta olursa olsun MD5 fonksiyonu 128 bit uzunluğunda, SHA fonksiyonu 160 bit uzunluğunda özet değeri üretir.
- Mesajdaki küçük değişiklikler bile özette büyük değişikliklere yol açabilir.
- Özet fonksiyonları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

Bölüm 3.3'te anlatılan e-imza senaryosunu, mesaj özeti fonksiyonunu da kapsayacak şekilde aşağıdaki gibi değiştirebiliriz [4]:

1. Ayşe gönderilecek metni tek-yönlü özet fonksiyonundan geçirir ve metnin boyundan bağımsız olarak ancak metnin karakterini içerecek şekilde sabit uzunluklu bir özet oluşturmuş olur (Şekil 3.4.– 1. adım).



Şekil 3.4. E-imzanın metin özeti alınarak oluşturulması



Şekil 3.5. E-imzanın onaylanması

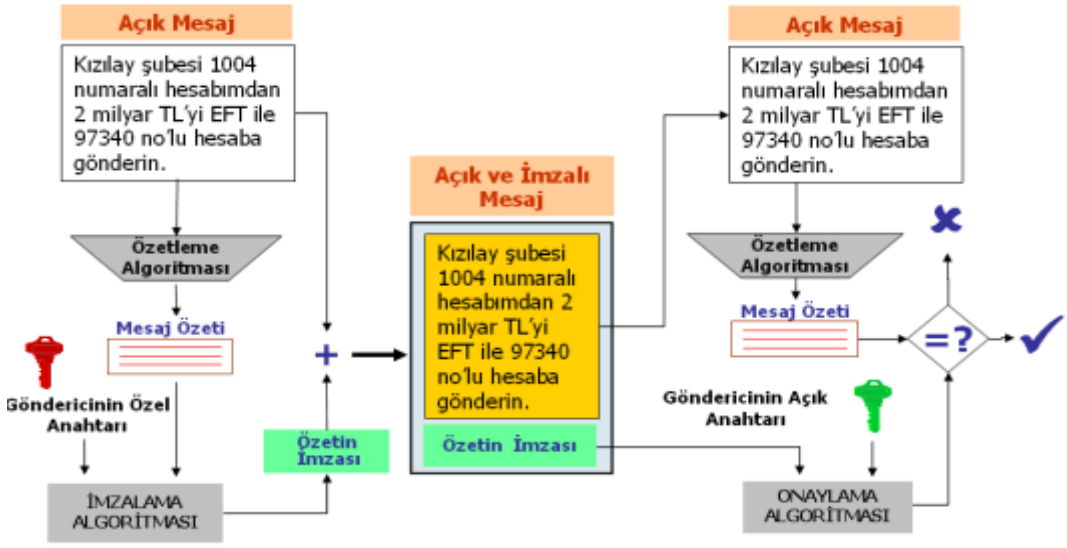
2. Ayşe tek-yönlü fonksiyon çıktısını özel anahtarı ile şifreler. Böylece metnin e-imzasını oluşturmuş olur (Şekil 3.4.– 2. adım).

3. Ayşe, metnin sonuna 2. adımda oluşturduğu metnin e-imzasını ekleyerek mesajı Barış'a gönderir.

4. Barış Ayşe'nin gönderdiği düz metnin tek yönlü fonksiyon ile özetini üretir (Şekil 3.5.- 1. adım). Ardından, imza onaylama algoritmasını kullanarak, Ayşe'nin açık anahtarıyla bu metnin e-imzasının şifresini çözer (Şekil 3.5.– 2. adım).

5. Eğer 1. adım ve 2. adımda elde edilen sonuçlar birbirinin aynısı ise, metnin e-imzası geçerli anlamına gelir.

Mesaj özeti kullanılarak yapılan imzalama işlemi Şekil 3.6'da tek bir şekil üzerinde gösterilmiştir [6]. Şekil 3.6'nın Şekil 3.3'ten farkı; gönderici tarafında, mesajın önce özetleme algoritmasından geçirilerek elde edilen özetin imzalama algoritmasından geçirilmesidir. Alıcı tarafında ise, onaylama işlemi sonucu elde edilen mesaj özetinin, açık olarak gelen orjinal mesajın özeti ile karşılaştırılmasıdır.



Şekil 3.6. Özet kullanarak e-imza yapısı

3.5. Elektronik İmza Türleri

Normal (ıslak) imzalarda olduğu gibi, e-imza tiplerinde de farklılıklar mevcuttur. İnkar edilemez imza, tuzak imza, sahte imza, vekalet imza ve kör imza bunlardan bazılarıdır. İnkar edilemez imza, imzayı atanın bilgisi olmadan doğruluğu kanıtlanamayan imza şeklidir. Bir kimsenin, içeriğini görmeden veya bilmeden bir belgeyi imzalamasına imkan veren e-imza tipi ise kör imza olarak bilinir. Atılan bir e-imzanın sahte olduğunu kanıtlamaya çalışan e-imza yaklaşımı ise tuzak imza olarak isimlendirilir. Vekalet imza ise, e-imza kullanacak kişiye, kendi gizli anahtarını açmadan bir başkasına imzasını kullandırma hakkı tanıyabilmesine imkan veren imza şeklidir [3].

Her ne kadar bu imzaların sayısını artırmak mümkün olsa da, elektronik ortamda mümkün olduğunca tek bir imza kullanılması, her zaman güvenliği ve kullanılabilirliği artıracaktır. Bu nedenle, farklı farklı imzalar kullanma yerine, tek bir imza kullanılmalıdır. Bu sayede gizli anahtarların güvenliği artacak ve karşılaşılabilecek güçlükler ve tehlikeler azaltılmış olacaktır. Bu, günümüzde kullandığımız kredi kartlarına benzetilebilir. Kredi kartının sayısı arttıkça, hiç şüphesiz kontrolü de zorlaşmaktadır. Bu bağlamda, birden fazla e-imza kullanımının, benzer zorluğu yaşatabileceği söylenebilir.

E-imza; farklı formatlarda ve formlarda bulunabilmektedir. Gelecek nesilde, e-imzaların veya m-imzaların (mobil imzalar) yerini, kişilerin veya kullanıcıların parmak izi, retina, ses ve yüz gibi biyometrik özelliklerden oluşturulacak imzaların alacağı düşünülmektedir.

3.6. Elektronik İmza Uygulama Alanları

E-imza yaklaşımları farklı seviyelerde güvenlik sağlayabildiklerinden dolayı birçok alanda uygulanabilirler. Kimlik tanımlama, doğrulama ve sır paylaşımı gibi uygulamalarda kullanılabileceği gibi, ulusal güvenlikten kişisel güvenliğe; elektronik ticaretten mobil ticarete; B2B (Business to business)'den B2C (Business to

customer)'ye; güvenli e-posta, e-banka ve güvenli bilgisayar erişimleri oluşturmaya kadar birçok karmaşık alanlarda uygulanabilmektedir. Bu sadece bilgiye, belgeye ve işlemlere ulaşmada önemli yenilikler getireceği, yeni altyapılar oluşturulmasıyla yeni altyapıları daha güvenli kılacağı ve çok farklı uygulamalar için, daha güvenli bir iletişim ortamı oluşturabileceği muhakkaktır [3].

E-imza ve buna bağlı olarak elektronik sertifikalar, sağladıkları güven altyapısı sayesinde kendisine birçok uygulama alanı bulmuştur. Bu alanlardan bazıları şöyle özetlenebilir [4].

- Bütünlük, Kimlik Denetimi ve İnkar Edememezlik Hizmetleri: Kurumlarda, mesajların doğru kişi tarafından, içeriği değiştirilmeden ve karşı tarafın inkar edemeyeceği şekilde iletimini sağlamak amacıyla kullanılabilir.
- Erişim Denetimi: Bilgisayar sistem ve terminallerine, internet sitelerine, kurum içi ağ üzerindeki hizmetlere erişim denetimini sağlamak amacıyla kullanılabilir.
- Belge İletiminin ve İletim Zamanının İspatı: Kritik belgelerin hukuksal açıdan zamanını ve tarihini doğrulamak için e-imza yasası ile birlikte gelen zaman damgası hizmeti kullanılabilir.
- Elektronik İş Akışı: Kağıt üzerinde işleyen bürokrasi, ıslak imza yerine geçebilen güvenli e-imza sayesinde elektronik ortamda çok daha hızlı, düşük maliyetli ve güvenilir bir şekilde gerçekleştirilebilir.
- Resmi Başvuru İşlemleri: 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 e-imzanın verinin gizliliği için kullanılamayacak bir teknoloji olduğu unutulmamalıdır. E-imzanın dayandığı açık anahtarlı kriptografik sistem ile veri şifrelemek yüksek maliyetli ve uzun süreler gerektiren bir işlemdir. Bu

nedenle e-imza teknolojisi, teknolojik olarak mümkün olsa bile, dünyadaki uygulamalarda da gizlilik hizmetini sağlamak için kullanılmaz. Gizlilik hizmeti, e-imzanın da birlikte çalışabildiği SSL protokolünün kullanımı ile sağlanabilir [4].

Ülkemizde, kurumların hemen hepsinin e-imzadan temel beklentisi, kurum içi ve kurumlar arası işlemlerin hızlandırılmasını ve elektronik ortamda yapılan işlemlere yasal geçerlilik ve güven unsuru kazandırılmasının sağlanmasıdır. Bununla birlikte e-imzanın özellikle kamu kuruluşları arasındaki işlemlerde ve kurumların iş ilişkisi içinde bulundukları bankalar, finansal şirketler, ithalat-ihracat şirketleri, medya kuruluşları gibi özel kurumlar ile yapılan elektronik ortamdaki belge ve veri alışverişi için kullanılmasının planlandığı göze çarpmaktadır. Vatandaşa sunulacak hizmetlere erişimin kolaylaştırılması kısıtlı oranda hedeflenmektedir. Bu alanların hemen hepsinde, sistem erişimlerinin temel kullanım amacı olarak görüldüğü anlaşılmaktadır. Ayrıca kurum içinde elektronik belge/verilerin imzalanmasının ve kurumlar arasında bunların şifrelenmesine yönelik kullanımın amaçlandığı da göze çarpmaktadır. Vatandaşlara yönelik kullanımda çok yaygın olarak hedeflenen ise belge ve verilerin elektronik ortamda imzalı olarak iletilmesidir [21].

Ülkemizde, bir çok kurumun e-imza kullanımını planlamakta olduğu görülmekle birlikte teknik konulardaki bilgi eksikliği ve ülkemizde fazla örnek uygulama olmamasından dolayı e-imza kullanımı istenilen ölçüde yaygınlaşamamıştır. Bu nedenle, e-imza konusunda ilgili kuruluşların kamu kurumlarına yönelik bilgilendirme çalışmaları yapmaları, kamu kurumlarının da ilgili personellerini bu konuda eğitmeleri gerekmektedir. Ayrıca e-imzayı aralarındaki ilişkilerde kullanacak kamu kurumları arasında koordinasyon ve bilgi bütünlüğü de sağlanmalıdır. Bu hususun, "E-Dönüşüm Türkiye Projesi Kısa Dönem Eylem Planı"nda yer alan "birlikte çalışabilirlik esaslarının belirlenmesi"ne yönelik eylem kapsamında dikkate alınması gereklidir [21,22,36].

Türkiye'de kamu sektörüne yönelik e-imza uygulamalarının, aşağıda verilen kamu hizmetleri alanlarında olması beklenilmektedir [4,5,37,38]:

- Her türlü başvurular (ÖSS, KPSS, pasaport, ikametgah, taşınma vb.),
- Elektronik belgeler: Bireylerin devletten almak zorunda olduğu ve devletin tuttuğu kayıtlar (nüfus kağıdı, pasaport, tapu ve kadastro, nüfus, adli kayıt ve sicil, askerlik, ithalat/ihracat vb.),
- Veri aktarımı (Devlet içi yazışmaların, belge ve veri aktarımların yapılması),
- Yerel yönetim uygulamaları,
- Kurum içi ve kurumlararası resmi yazışmalar,
- Kurumlararası işlemler (Emniyet/nüfus ve vatandaşlık işleri),
- Sosyal güvenlik uygulamaları (Emekli sandığı, SSK, Bağkur),
- Sağlık uygulamaları (Sağlık personeli – hastaneler - eczaneler, Sağlık veri bankaları),
- Yargı hizmetleri (Yargı sistemindeki etkileşimlerin kağıt ortamından elektronik ortama taşınması),
- Ödemeler (Vergi, harç vb. ödemeler),
- Elektronik oy verme işlemleri vb.

Türkiye'de özel sektöre yönelik e-imza uygulamalarının ise aşağıda verilen alanlarda olması beklenilmektedir [5,37,38,39]:

- Tüm ilk anlaşmalar,
- Kağıtsız ofisler,
- İnternet bankacılığı (Güvenli giriş, güvenli ödeme işlemleri, online hesap açımları vb.),
- İnternetten borsa,
- Sigortacılık işlemleri, menkul kıymetler,
- Elektronik alışveriş,
- E-sipariş,
- E-sözleşme,
- E-fatura,
- E-kütüphane vb.

Yukarıda e-imzanın kamu ve özel sektördeki uygulama alanları genel olarak verilmiştir. Ayrıca daha da detaya inilerek, e-devlet hizmetleri ve uygulamalarından çeşitli kamu kurumları tarafından hayata geçirilen/geçirilebilecek uygulamalardan bazıları Çizelge 3.1'de listelenmiştir [4]. Liste elbette çok uzayabilir. Burada amaç, vatandaşın ve devlet kurumlarının ilk anda ihtiyaç duyabileceği ve e-imzanın yararlarından en çok faydalanılabilecek bir liste sunmaktır:

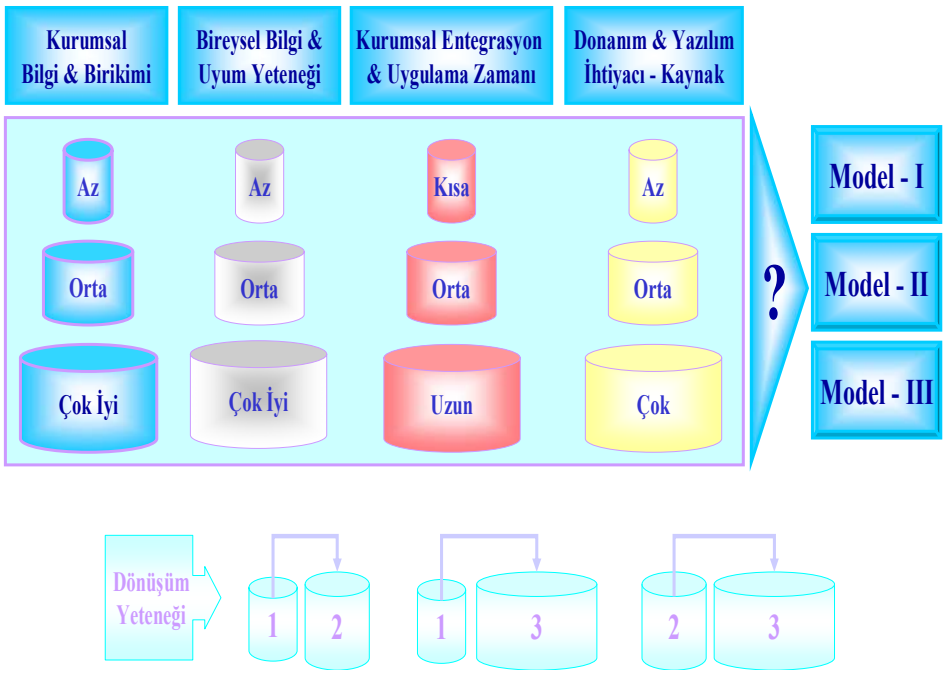
Çizelge 3.1. E-imzanın kullanılabileceği kamu hizmetleri

Maliye Bakanlığı	e-beyanname
Sanayi ve Ticaret Bakanlığı	e-esnaf, e-tüketici Ticaret Sicil Memurlukları Otomasyonu,
Bayındırlık Bakanlığı	Yapı Denetim Uygulaması
Adalet Bakanlığı	Ulusal Yargı Ağı Projesi
SSK	e-bildirge
Emekli Sandığı	e-sağlık (Sağlık Harcamalarının Uygulama ve Denetimi)
Emniyet Genel Müdürlüğü	e-pasaport, e-ehliyet hizmetleri
Dış Ticaret Müsteşarlığı	Dahilde İşleme Rejimi Projesi
Türk Patent Enstitüsü	e-marka, e-patent, e-tasarım
İşkur	e-iş
Sermaye Piyasası Kurulu	Kamu Aydınlatma Projesi

Burada belirtilen hizmetlerde e-imzanın tek başına kullanımı mümkün değildir. Örneğin bir e-ödeme uygulamasında e-imzanın kullanılabilmesi için önce, o uygulamanın mevzuatta yer alan iş akışının tanımlanması ve bunun için gerekli donanım ve iletişim altyapısının oluşturularak, iş akışının bir yazılım uygulamasında gerçekleştirilmesi gereklidir. E-imzanın kullanılabilmesi, bu yazılım uygulamasının sahip olduğu özelliklerden biri olacaktır [4].

3.7. Elektronik İmza Modelleri

Kurumsal ağlar için uygulanabilir e-imza modelleri "Kurumsal Bilgi&Birikimi", "Bireysel Bilgi&Uyum Yeteneği", "Kurumsal Entegrasyon&Uygulama Zamanı" ve "Donanım&Yazılım İhtiyacı-Kaynak" kriterlerine bağlı olarak 3 modelde incelenebilir. Söz konusu kriterlerin durumuna bağlı olarak seçilebilecek model ve modeller arası dönüşüm yeteneği Şekil 3.7'de verilmiştir [40].



Şekil 3.7. E-imza temel uygulama modelleri

Model I

Bu modelde, kurumsal olarak tüm evrak yönetim sistemi aynen devam etmekte (klasik-ıslak imzalı), e-imza ile gelen evrakların kabülü ve kontrolü ile giden evraklarda e-imza işlemi evrak kayıt işleminden sonra yetkili bir kişi tarafından (Evrak Şefi, Evrak Müdürü vb.) gerçekleştirilebilmektedir. Bu model, daha ziyade henüz networkü bulunmayan kurumlar için uygundur. Aynı zamanda network ortamı mevcut olan ancak e-imza sürecine hazır olmayan ve kısa zamanda tam hazırlık sürecini tamamlama imkanı olmayan kurumlar için de uygulanabilir.

Bu modele uygun kurumların, başlangıç itibarı ile e-imza sürecinin aktif hale getirilebilmek için bir "Elektronik Doküman Yönetim Sistemine (EDYS)" ihtiyacı bulunmamaktadır. Kurumsal gelişim ve hazırlık süreci sonucunda Model-II veya Model-III tercihinin yapılması aşamasına gelindiğinde, kuruma ve modele uygun olan bir EDYS ihtiyacı otomatik olarak oluşacaktır.

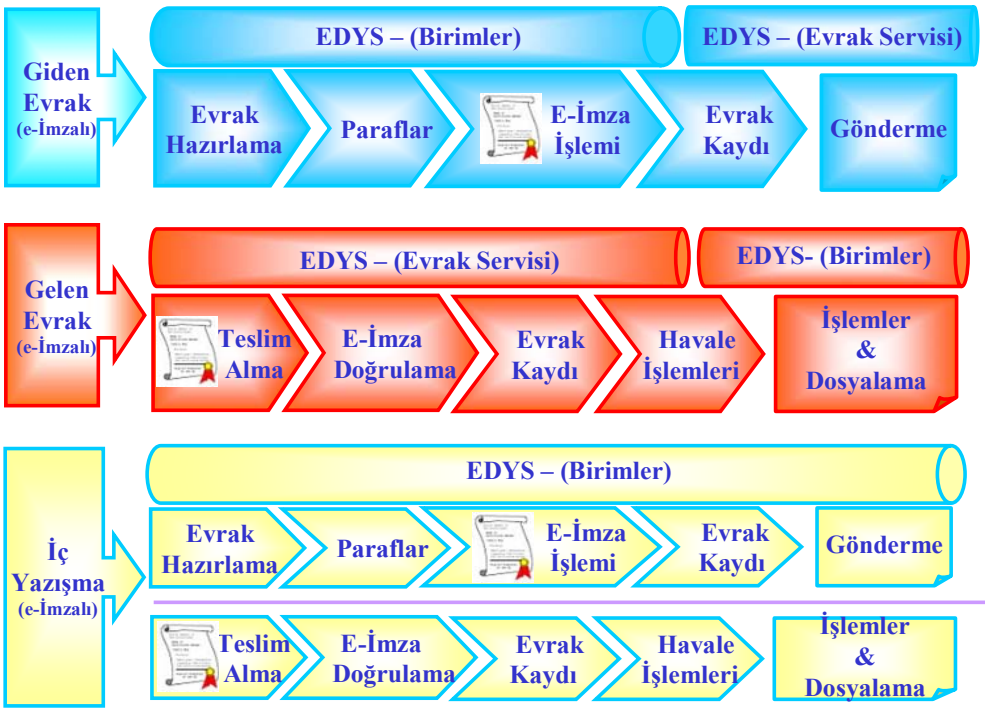
Bu modele ilişkin özet iş süreçleri Şekil 3.8'de gösterilmiştir [40]. Her bir birim için minimum sistem ihtiyaçları ise aşağıda listelenmiştir:

- 1 adet tarayıcı (scanner)
- 1 adet e-imza kartı & sertifikası
- 1 adet e-imza oluşturma-doğrulama aracı
- 1 adet yazıcı (printer)
- 1 adet e-posta adresi ve bağlantısı

Şekil 3.8. Model I özet işlem süreçleri

Model II

Bu modelde, evrak yönetimi uygun bir EDYS aracılığı ile sağlanmaktadır. Evrak hazırlama ve paraf işlemleri gibi yönetsel işlemler EDYS'nin sağladığı yazılım imkanları ile yerine getirilmekte iken e-imza sadece evrakı imzalayan son imza makamı tarafından kullanılmaktadır. Kuruma gelen evrak açısından ise, EDYS tarafından e-imza doğrulama işlemi evrak servisinde tamamlanmakta ve evrakın kalan hayat döngüsü (havale,dosyalama vb) EDYS'nin sağladığı yazılım imkanları ile yürütülmektedir.



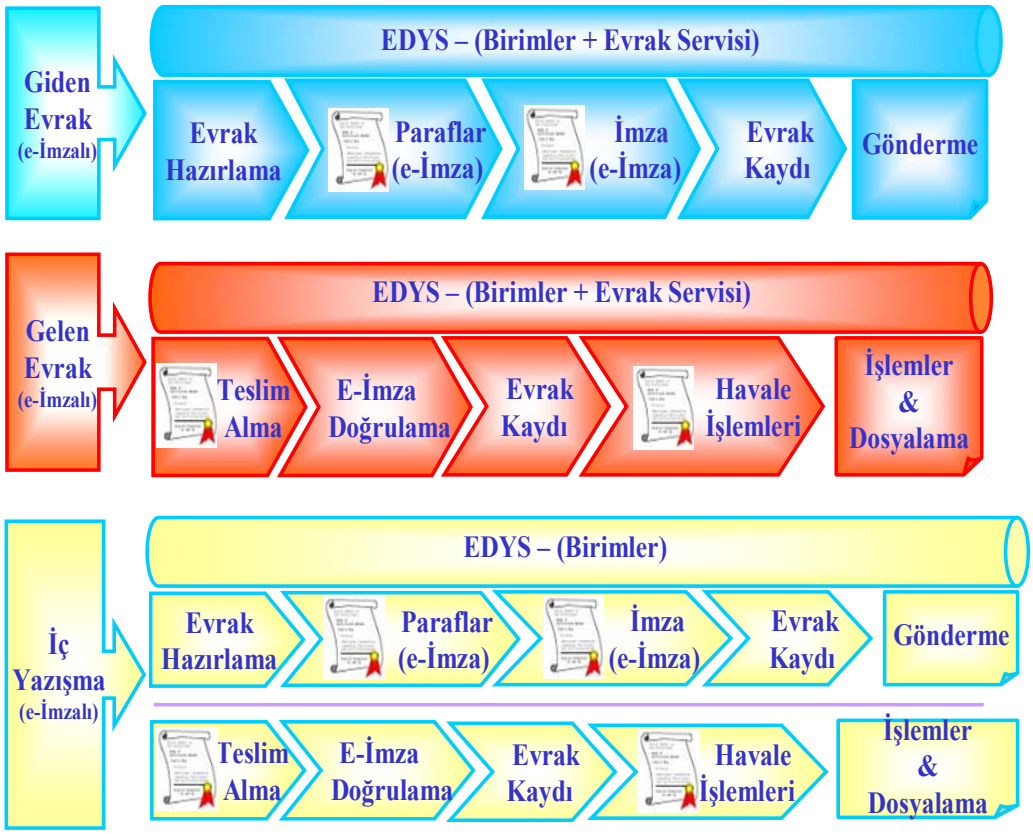
Şekil 3.9. Model II özet işlem süreçleri

Bu model daha ziyade, network ortamı mevcut olan, ancak e-imza sürecine tam olarak hazır olmayan kurumlar için uygulanabilir. Bu modele ilişkin özet iş süreçleri Şekil 3.9'da gösterilmiştir [40]. Her bir birim için minimum sistem ihtiyaçları ise aşağıda listelenmiştir:

- 1 adet EDYS yazılımı + e-imza oluşturma-doğrulama aracı (entegre),
- E-imza kartı & sertifikası (imza yetkilisi makam sayısı kadar),
- 1 adet e-posta adresi ve bağlantısı (evrak servisi için).

Model III

Bu modelde de evrak yönetimi uygun bir EDYS aracılığı ile sağlanmaktadır. Evrak hazırlama ve gönderme, EDYS'nin sağlandığı yazılım imkanı ile oluşturulmakta ve tüm paraf işlemleri ile tüm imzalama işlemleri için e-imza kullanılmaktadır. Kuruma gelen evrak açısından ise, EDYS tarafından e-imza doğrulama işlemi evrak servisinde tamamlanmakta ve evrakın kalan hayat döngüsü içinde havale işlemleri de e-imza ile gerçekleştirilmektedir. Diğer işlemler EDYS'nin sağladığı yazılım imkanları ile yürütülmektedir.



Şekil 3.10. Model III özet işlem süreçleri

Bu yaklaşım daha ziyade, network ortamı mevcut olan ve e-imza sürecine tam olarak hazır olan kurumlar için uygulanabilir. Bu modele ilişkin özet iş süreçleri Şekil 3.10'da gösterilmiştir [40]. Her bir birim için minimum sistem ihtiyaçları ise aşağıda listelenmiştir:

- 1 adet EDYS yazılımı + e-imza oluşturma-doğrulama aracı (entegre)
- E-imza kartı & sertifikası (tüm personel için)
- 1 adet e-posta adresi ve bağlantısı (evrak servisi için)

3.8. Kurumsal Ağlar İçin Açık Anahtar Altyapısı Tabanlı Elektronik İmza Sistemleri

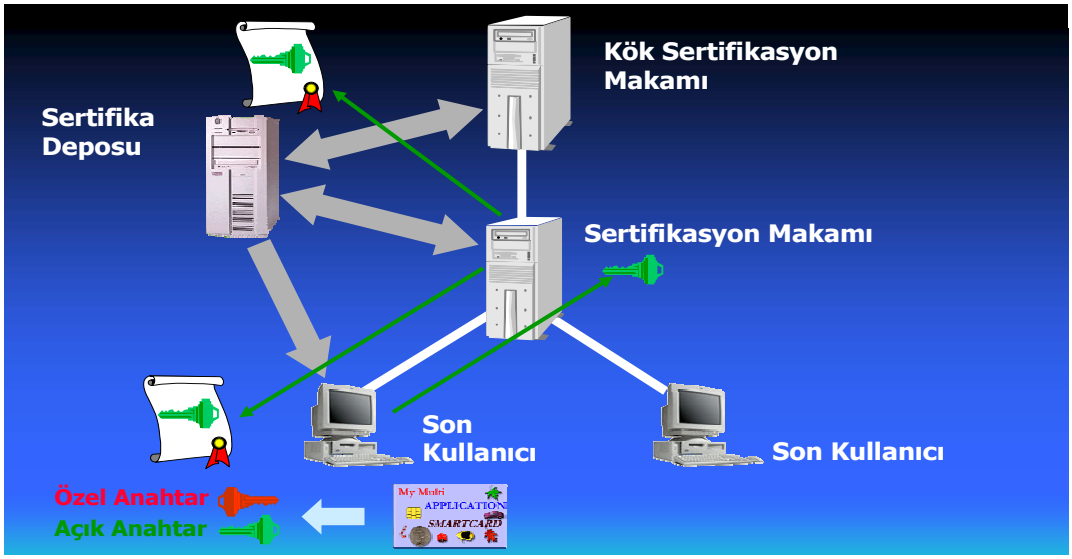
Şekil 3.11.'de basit bir AAA sistemi görülmektedir. Buradaki bileşenler:

- Kök sertifikasyon makamı sunucusu,
- Sertifikasyon makamı sunucusu,
- Dizin sunucusu/sertifika deposu,
- Son kullanıcı bilgisayarları,
- Kullanıcının anahtar çiftleridir.

Şekil 3.11'deki örnek AAA sistemi üzerinde bir kullanıcı için sertifika üretim adımları aşağıda sıralanmıştır:

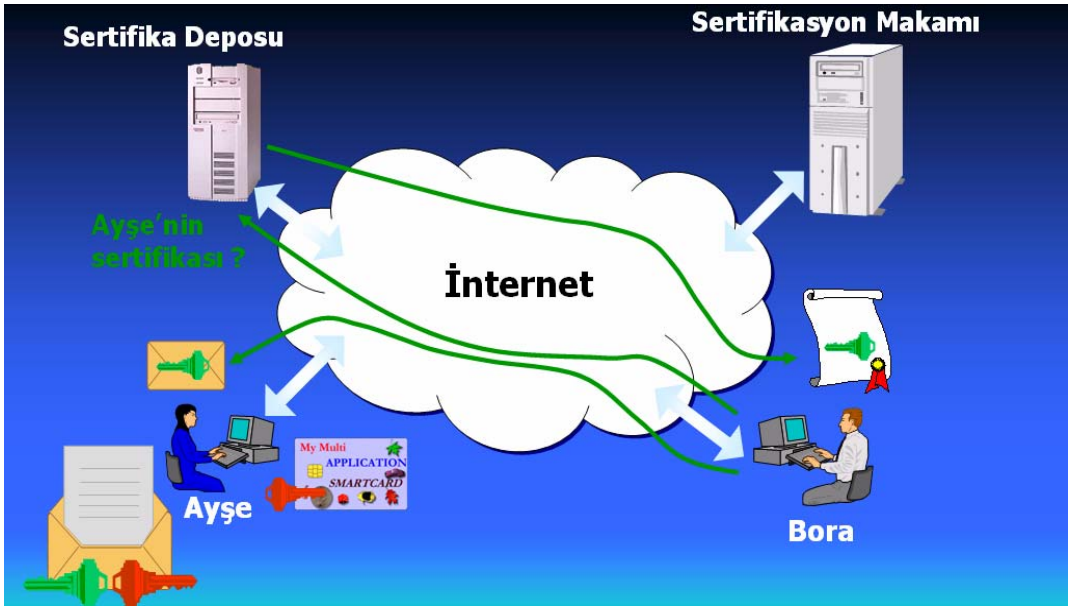
1. Son kullanıcı, sertifika talebi yapmak için kendisine ait imzalama anahtar çiftini akıllı kartında üretir.
2. Açık anahtarını sertifika talebi olarak SM sunucusuna iletir, özel anahtarını hiçbir şekilde başka bir kişiye iletmez.
3. SM bu açık anahtarı ve kullanıcı ile ilgili e-posta adresi gibi ayırdedici bilgileri sayısal sertifika şekline dönüştürür.
4. Oluşturulan sertifika kullanıcıya iletilir ve ayrıca herkesin erişebileceği dizin sunucusuna konur. Bu sunucu sertifika deposu olarak görev yapar.

5. Kullanıcı artık e-imzalama, kimlik tanıtma ve benzeri işlemler için kullanabileceği bir sertifikaya sahip olmuştur.



Şekil 3.11. AAA sisteminde sertifika üretimi

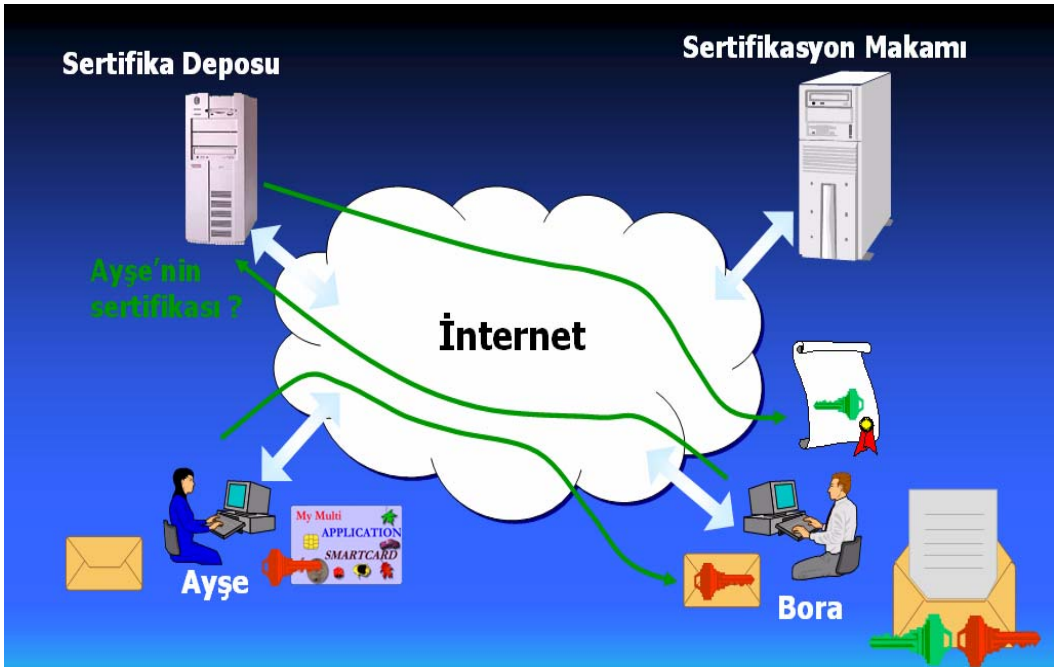
Sertifikası olan bir kullanıcıya, AAA sistemi üzerinde şifreli mesaj gönderme işlemi Şekil 3.12'de gösterilmiş ve işlem adımları aşağıda listelenmiştir:



Şekil 3.12. AAA ile şifreli haberleşme

1. Bora Ayşe'ye şifreli bir mesaj göndermek için Ayşe'nin sertifikasını sertifika deposundan ister.
2. Sertifika deposundan Ayşe'nin sertifikasını alır ve bu sertifika içindeki açık anahtarı kullanarak yazdığı mesajı şifreler.
3. Bora bu şifreli mesajı Ayşe'ye yollar.
4. Ayşe gelen mesajı sadece kendisinde bulunan özel anahtarı kullanarak açar. Bunun için akıllı kartını kullanır, çünkü özel anahtarı akıllı kartının içinde saklıdır.

Sertifikası olan bir kullanıcıya, AAA sistemi üzerinde imzalı mesaj gönderme işlemi ise Şekil 3.13'de gösterilerek ilgili işlem adımları da aşağıda listelenmiştir:



Şekil 3.13. AAA tabanlı e-imzanın çalışması

1. Ayşe Bora'ya imzalı bir mesaj göndermek için göndereceği mesajın özetini kendi özel anahtarı ile şifreler ve Bora'ya yollar.
2. Bora Ayşe'den gelen mesajın şifreli imza kısmını çözmek için sertifika deposundan Ayşe'nin sertifikasını alır ve bu sertifika içindeki açık anahtarı kullanarak Ayşe'nin özel anahtarı ile şifrelediği imza mesajını açar. Şifreli bu mesaj

Ayşe'nin özel anahtarı ile şifrelendiği için sadece Ayşe'nin açık anahtarı ile çözülebilecektir.

3. Bu durumda Bora, şifreli imzayı Ayşe'nin açık anahtarı ile açabildiği için mesajın Ayşe'den geldiğinden emin olur.

4. Açılan şifreli imza mesajı, Ayşe'den gelen mesajın orjinal halinin özeti ile de karşılaştırılarak mesaj bütünlüğünün değişmediği kontrol edilir.

Yukarıdaki uygulamalar ile AAA sisteminde kimlik doğrulama ve mesaj bütünlüğünün nasıl sağlandığı örneklerle açıklanmıştır. E-imzanın diğer desteği olan inkar edememenin de sağlanabilmesi için sistemde Ayşe ile Bora arasındaki imzalı mesaj trafiği ile ilgili kayıtlar tutulmalıdır. Alınan mesajın imzası, göndericinin onay anahtarı ile onaylandıktan sonra gönderici bunu inkar edemez. Çünkü onun imza özel anahtarına sadece kendisi sahiptir.

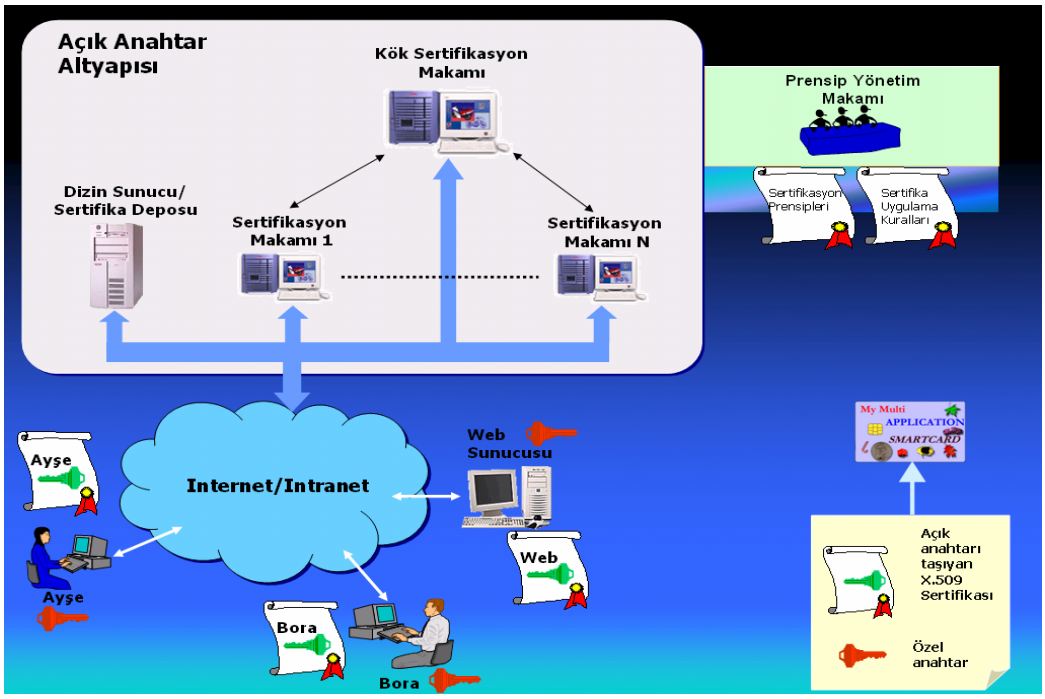
3.9. Kurumsal Ağlarda Açık Anahtar Altyapısının Bileşenleri

AAA, kurum ve kuruluşların elektronik ortamda ihtiyaç duyduğu güvenlik hizmetini sağlamak için kullanılır. Bu altyapı, tepede bir Kök Sertifikasyon Makamı (KSM) ile ona bağlı bir veya daha fazla Sertifikasyon Makamı (SM) sunucusu ve diğer yardımcı yazılımlardan oluşur. Kullanıcılar belli prensipler çerçevesinde bu sisteme kayıt olurlar. Bu kayıt işlemi sonucunda kullanıcı, kimliğini ispat etmek ve bilgi güvenliğini sağlamak için kullanabileceği elektronik belgeye sahip olur. Sertifika adı verilen bu belgeler elektronik (sayısal) imza atmak ve bilgileri şifrelemek için kullanılır [41,44].

Şekil 3.14'te bir AAA sisteminin genel resmi verilerek sistem bileşenleri gösterilmiştir. Bir AAA sistemi genel olarak aşağıdaki bileşenlerden oluşur:

- Kök Sertifikasyon Makamı (KSM)
- Sertifikasyon Makamı (SM)
- Kayıt Makamı (KM)
- Elektronik Sertifika Hizmet Sağlayıcısı (ESHS)

- Sertifika deposu/Dizin sunucusu
- Arşiv modülü
- Güvenlik protokolleri
- Kriptografik anahtar çiftleri
- Elektronik (sayısal) sertifikalar
- E-imza/AAA yazılımı
- E-imza algoritmaları
- Sertifika sahipleri
- Güvenli e-imza oluşturma ve doğrulama araçları
- Ürünler ve bu ürünlere ilişkin standartlar
- Uygulama, ilke, esas ve yönetmelikleri



Şekil 3.14 Açık anahtar altyapısı resmi

3.10. Açık Anahtar Altyapısında Makamlar

AAA sistemlerinin temel bileşenlerinden ilki makamlardır. Bu bileşenler aşağıda detaylı olarak açıklanmıştır:

3.10.1. Kök sertifikasyon makamı

Kök sertifikasyon makamı (KSM), hiyerarşik olarak en üstte yer alan ve altyapıdaki tüm bileşenlerin e-imzasına güvendiği makamdır.

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 e-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 [4].

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 [4].

3.10.2. Sertifikasyon makamı

Sertifikasyon makamı (SM), AAA sisteminde yer alan sertifikaları ve sertifika iptal listelerini (SİL) üretmekle görevli olan merkezi birime verilen addır. SM, donanım ve yazılım parçalarından ve sistemi işleten kişiler ve kurallardan oluşan bir yapıdır. Bir SM'yi diğer SM'lerden ayıran en önemli özellikleri adı ve anahtar çiftidir (açık ve özel anahtar) [6]. SM'nin görevleri aşağıda listelenmiştir [42]:

- Sertifika yayınlamak,
- Sertifika durum bilgilerini güncel tutmak ve SİL hazırlamak,
- Güncel sertifikaları ve SİL'leri isteyen kişilere sunmak,
- Süresi dolan ya da iptal edilen sertifikaların arşivini tutmak.

SM'nin yayınladığı sertifikalarla ilgili olarak aşağıdaki ifadeler 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 e-imzasını kontrol ederek sertifikanın doğruluğunu kontrol ederler.

3.10.3. Kayıt makamı

Kayıt makamı (KM), kullanıcılar ve onların açık anahtarları arasındaki bağı onaylayan makamdır. Bir başka deyişle, kullanıcıların SM'ye erişmeden önce tanımlama ve kimlik kontrollerinin yapıldığı yerdir. Her sistemde KM bulunması gerekmez. KM, kullanıcı ile ilgili topladığı bilgileri SM'ye kendi e-imzasıyla imzalayarak iletir. Böylece SM, sertifika isteğinin güvendiği bir kaynaktan gelip gelmediğini anlayabilir. Bu nedenle KM kendi özel anahtarını çok iyi korumalıdır. Bir KM, birden çok SM için bu hizmeti verebilir [43]. KM'nin SM ile çalışması genelde iki şekilde olur. Bunlar aşağıda açıklanmıştır [6]:

1. 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.

2. 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.

3.11. Elektronik Sertifikalar

E-imza yasasında elektronik sertifika; "İmza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kaydıdır" şeklinde tanımlanır.

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 [4].

İdeal sertifika tanımına uyan bir elektronik sertifika oluşturabilmek için uluslararası ISO ve ITU kurumları X.509 standardını tanımlamışlardır. X.509, AAA sistemlerinde yaygın olarak kullanılan sertifika standartlarının başında gelir [41]. Bu standart IETF tarafından RFC 2459 olarak yayınlanmıştır. "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" adını taşıyan bu standart dahilinde X.509 Sertifikası V1, V2, V3 sürümleri ve X.509 SİL V1, V2 sürümleri tanımlanmıştır.

Bir sayısal sertifika dört ana bileşenden oluşur. Bunlar; açık anahtar, anahtarı sahibine bağlayan kişisel bilgiler, sertifikayı veren makam hakkında bilgi ve sertifikayı veren makamın imzasıdır.

Sayısal sertifikalar genel olarak açık anahtar için bir taşıyıcı görevi görürler. Ancak açık anahtardan daha fazla belirleyici bilgiye sahip oldukaları için çok daha işlevseldirler [42]. Şekil 3.15'te örnek bir açık anahtar sertifikası görülmektedir. Bir sertifika;

- Sayısaldır, bilgisayarda veya elektronik bir cihazda hazırlanır,
- Sahibinin adını ve açık anahtarını içerir,
- Sahibinin görev yaptığı birlik/kurum adını içerir,
- Genelde sahibinin e-posta adresini içerir,
- Yayınlama ve geçerlilik tarihlerini içerir,
- Yayınlayan güvenilir kurumun adını içerir,
- İçeriğin bütünlüğü, yayınlayan kuruluşun e-imzasıyla koruma altına alınmıştır,
- Yayınlayan kuruluş tarafından verilmiş tekil bir seri numarasına sahiptir.

X.509 sertifikasının bütünlüğünün korunması için sertifika içinde yer alan tüm bilgiler sertifikayı veren makam tarafından elektronik olarak imzalanır ve oluşan e-imza bu sertifikanın arkasına eklenir. Böylece sertifika alanlarından herhangi birisi üzerinde sonradan değişiklik yapılıp yapılmadığı kontrol edilebilir. Bir sertifikanın bütünlüğünün bozulması engellenemez ama böyle bir durum e-imzanın kontrol edilmesiyle hemen anlaşılır.

Seri No	2368
Sertifika Sahibi	Hüseyin EROL
Kurum	Gazi Üniversitesi
Yayınlayan	Tübitak
E-posta Adresi	Herol @ gazi.edu.tr
Yayın Tarihi	01.09.2006
Son Kullanım	01.09.2007
İlke/Prensip	E-posta imzalama, dosya imzalama
Açık Anahtar	2489349e894859f45489450dab45454ca0908d8809
Tübitak E-İmzası	Ae89349c989893e8989548d0823048b08023f9e903hsasde345l62m234

Şekil 3.15. Örnek sertifika

Bir sertifika, byte dizilerinden oluşan elektronik bir veridir. Gerçekte Şekil 3.16'daki gibi görülen ve birkaç kilobyte'ı geçmeyen sertifika bu şekilde bir anlam ifade etmeyeceği için çeşitli platformlarda ve çeşitli arayüz programları ile daha anlamlı bir biçimde gösterilmektedir.

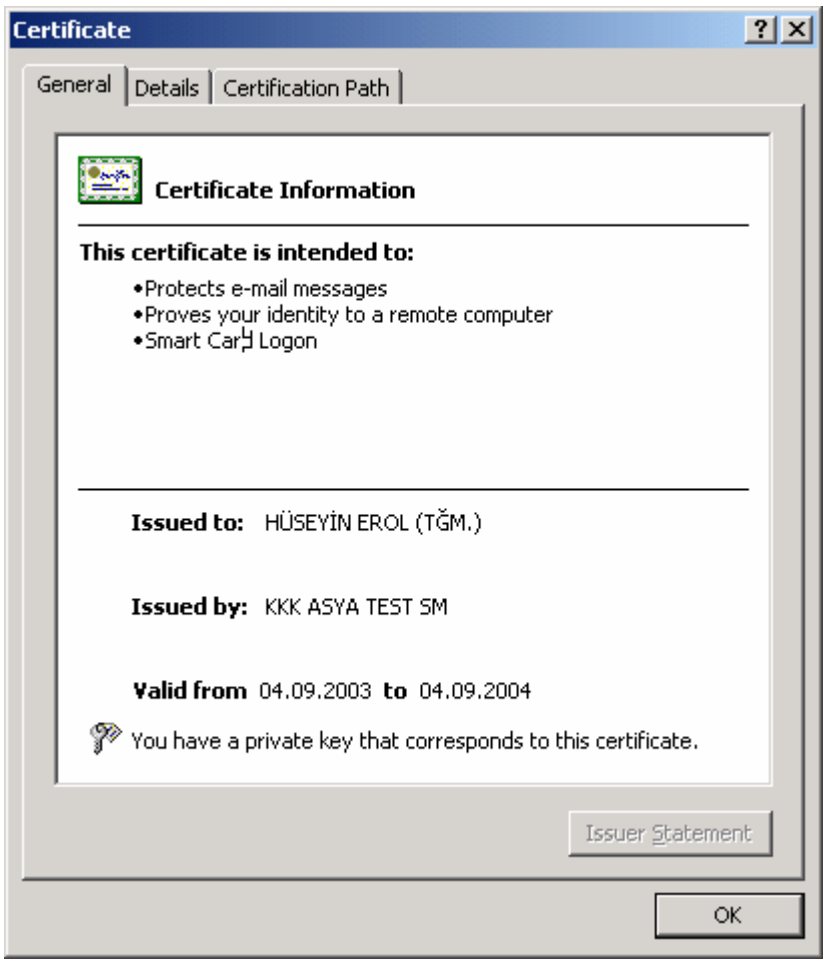

```
-----BEGIN CERTIFICATE-----
MIIDXzCCAkegAwIBAgIBATANBgkqhkiG9w0BAQUFADBTMRMwEQYKCZImiZPyLGQB
GRMDdHNrMRMwEQYKCZImiZPyLGQBGRMDa2trMQswCQYDVQQGEwJUUjEaMBgGA1UE
ChMRS0tLIEFTWUEgVEVTVCBLU00wHhcNMDMwNTIxMjMyNzAwWhcNMTgwNTIxMjMy
NzAwWjBTMRMwEQYKCZImiZPyLGQBGRMDdHNrMRMwEQYKCZImiZPyLGQBGRMDa2tr
MQswCQYDVQQGEwJUUjEaMBgGA1UEChMRS0tLIEFTWUEgVEVTVCBLU00wggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCd9EgwoqhfQ/BORmhX48RPVLFIe701
7CaZTxYTvjDUzmEMAMHMbdGYgeP1EbZWcM6k7ArquiXoaXxNVy690H+U8rlvhHcB
xYosMqPHRzN9j76cB/PSLPqj8vlki0MI9cdxRhphicYjPSs2HGFgjUfYGVNwCfOy
cHgAH9FmZfxfuXK/VIFcq5pyMuHA50wVfhKqy5/DvBsOwY+XFovhqYFgYvjGOvjI
/dGS97UWBiC2Xa/KuVuBpGFDOtXsaXtdnykVo1eEQx2BEGiF5ikq3NqIis2RJlQc
UuzDcSJGI/8OZu5OQ7pL7kR1sb13Ylr109KDje3TcHIrb80dODspFtBPAgMBAAGj
PjA8MA4GA1UdDwEB/wQEAwIAxjAPBgNVHRMBAf8EBTADAQH/MBkGA1UdDgQSBBAF
gbLPT+J21t9O4tSU2PHUMA0GCSqGSIb3DQEBBQUAA4IBAQB39K/XCTVXZKhUmi3X
NR2dyQFX4R6BA5MShRgje22t/dHhOGJyv+R5UivjPw6kmUHzVhypaqpC72erO8O5
R2233OJ5E1dKPn6IXa+ZC8SIKKNtnST2ythLwTfRgNwgnoawOL/lkA4jV1s2T9Dp
6b4V5yGu3YLdZwK9JL66k8wo63n+Sx0I5XKh5urjtyBt/pPzoCwoiKxsbH/vitMv
RCJK0JJCdFvqXw4QgWvC/Ko7HAl4AviSWxzBIQPQ+ykox1DMF2Y0TN5tpMwv8znK
jzJ4FQZiKwLkWKmT08mpqcNJQSC/Saoxpxf7TE0ZuHlnDO9BnwW25WzDIsTKGU71
Kupk
-----END CERTIFICATE-----
```


Şekil 3.16. Örnek sertifika verisi

Windows ortamında bir sertifika "cer" uzantılı bir dosya olarak tutulur. Bu dosyanın görünümü de Şekil 3.17'de gösterilmiştir.

Şekil 3.17. Bilgisayarda sertifika dosyası

"Cer" uzantılı bu sertifika dosyası açıldığında Şekil 3.18'deki arayüz ile sertifika bilgilerine kolaylıkla ulaşılabilir.



Şekil 3.18. Windows ortamında bir sertifika

Nitelikli elektronik sertifika

Yukarıda özellikleri belirtilen bir elektronik sertifikanın yasal olarak geçerli olan güvenli e-imza oluşturmak amacıyla kullanılabilmesi için, yasada tarif edilen "nitelikli elektronik sertifika (NES)" özelliklerine sahip olması gerekir [4].

NES, 5070 sayılı Kanun uyarınca gereken şartları sağlayan ve TK tarafından yetkilendirilmiş nitelikli bir ESHS tarafından verilmiş sertifikalardır. Yayımlanan tebliğe göre nitelikli elektronik sertifikalar ITU-T Rec. X.509 V.3 standardına uymak zorundadır. Bu kapsamda bir nitelikli elektronik sertifikada yer alması zorunlu olan bilgiler aşağıda listelenmiştir [46]:

- Sertifikanın "NES" olduğuna dair bir ibare,
- ESHS'nin kimlik bilgileri ve kurulduğu ülkenin adı,
- İmza sahibinin teşhis edilebileceği kimlik bilgileri,
- E-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 e-imzası.

NES, teknik güvenlik kriterlerine uygun donanım aracı (akıllı kart) üzerinde sağlanır.

Sunucu/Cihaz sertifikası

Sunucu/Cihaz sertifikaları, sunucuların kimlik bilgilerini ve açık anahtarını taşıyan ve bu sunuculara bağlanan kullanıcılara sunulan elektronik sertifikalardır. Sunucu/Cihaz sertifikası, SSL protokolünde sunucu kimliğinin doğrulanması ve şifreli iletişim yapılabilmesi için ESHS'ler tarafından yayınlanır. Cihaz sertifikaları, AAA destekli VPN cihazlarında aynı amaçla kullanılabilir [47]. Özellikle son dönemlerde artan ve ülkemizde de görülen internet üzerinden dolandırıcılık faaliyetlerinin bir kısmı, gerçeğine çok benzeyen taklit web siteleri aracılığı ile gerçekleştirilmektedir. Sunucu/Cihaz sertifikaları ile bağlanılan web sitesinin kimliği güvenilen bir ESHS aracılığı ile doğrulanabilir [4].

Sunucu/Cihaz sertifikası, kişisel sertifikalar gibi X.509 standardına uygun üretilirler. Bu sertifika sayesinde, bağlanılan web sunucusunun, kullanıcılar açısından kimlik doğrulaması yapılmış olur. İsteğe bağlı olarak, bu kimlik doğrulaması çift taraflı olarak gerçekleşebilir. Bu yöntemle hem web sunucusu karşısındaki kullanıcının

kimliğinden hem de kullanıcı web sunucusundan 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.

3.12. Anahtar ve Sertifika Yönetimi

Anahtar ve sertifika yönetimiyle ilgili olarak sertifikasyon otoritesinin sorumlulukları aşağıda açıklanmıştır [37]:

- Her anlamda güvenli bir sistem kurmak ve kullanmak,
- Güvenlik uygulama ve işlemlerini tanımlamak,
- Sertifika talebinde bulunan kişi veya kurumu tam ve doğru tanımlamak,
- Sertifika üretim ve yönetimini gerçekleştirmek,
- Yayınlanan sertifikaları ulaşılabilir bir dizin sunucusunda tutmak,
- Sertifikaları iptal etmek ve/veya askıya almak.

3.13. Elektronik Sertifika Hizmet Sağlayıcısı

Yasaya göre Elektronik Sertifika Hizmet Sağlayıcısı (ESHS), elektronik sertifika, zaman damgası ve e-imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişilerdir [48].

Serbest rekabet koşulları içinde ticari faaliyet gösterecek bu kişiler, bir düzenleyici kurumun belirlediği koşullarda hizmet verir. Düzenleyici kurum, ESHS'lerin hizmet koşullarını belirlemek ve denetlemenin yanı sıra, kişilerin kullanacağı araçlarla ilgili standartları belirleme ve yayınlamaktan da sorumludur [19].

Elektronik sertifikada yer alan bilgilerin doğruluğundan emin olunması için bir güven modeline ihtiyaç duyulmaktadır. E-imza yasasında tanımlanan ESHS'ler, sertifika veren kuruluşlar olarak tanımlanmaktadır. ESHS, güven ve itibarın tesisi için belirlenmiş kurallara bağlı olarak faaliyetlerini yürütmek ve yasa ile belirlenen bir kuruluş tarafından denetime açık olmak zorundadır. Türkiye'de ESHS

faaliyetlerini düzenleyici kurum olarak Telekomünikasyon Üst Kurulu (TK) görevlendirilmiştir [4].

ESHS 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.

ESHS ile noterlerin farkı

ESHS 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 işlem 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 [4].

Kimlik doğrulamada ESHS, noterde olmayan bir sorumluluk taşımaktadırlar. ESHS, işlemi gerçekleştiren şahsın kimliğinin doğruluğunu da kontrol eder. Bununla birlikte gerçekleştirilen işlemle ilgisi yoktur. Gerçekleştirilen işlem veya gönderilen belge tamamen iletişim kuran tarafları ilgilendirir. ESHS, bir kimyasal tepkimede, uygun ortam şartlarını sağlayan bir katalizör gibi görev yapar.

İletişim esnasında, e-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 NES için ya da zaman damgası hizmeti için ESHS'ye bir ücret ödediğinden, dolaylı olarak da olsa bir ücretlendirme söz konusudur [4].

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.

3.14. Sertifikasyon İlkeleri ve Sertifika Uygulama Esasları

Sertifikasyon İlkeleri (Sİ) ve Sertifika Uygulama Esasları (SUE), bir AAA sisteminde ESHS tarafından yayınlanması zorunlu olan belgelerdir [46]. Sİ ile, sertifika kullanımı ve sertifika yaşam çevrimi ile ilgili kurallar listelenir. ESHS, elektronik sertifikalar ve kurduğu AAA ile ilgili tüm iş sürecini bu belge ile tanımlar. SUE'de ise, Sİ dokümanında belirtilen kuralların nasıl uygulanacağı ayrıntılı bir biçimde ifade edilir. Genellikle SUE, Sİ'ye göre daha uzun, kapsamlı ve teknik bilgiler içeren bir belgedir. ESHS, bu iki belgeyi IETF RFC 3647'ye uygun olarak hazırlamalıdır [4].

Sertifikasyon ilkeleri

Sertifikasyon İlkeleri (Sertifikasyon Prensipleri olarak da kullanılır), sertifika yayımlayan kurum tarafından belirlenen kurallardır. Bu kurallar genel olarak bir sertifikanın hangi uygulamalarda kullanılabileceğini ve hangi durumlarda güvenilir kabul edilebileceğini belirler. Günlük hayatta bunun benzeri kuralları bankaların kredi kartlarında görebiliriz. Örneğin silver, gold, platinum gibi değişik kart sahiplerinin değişik harcama limitleri ve değişik kullanım kuralları bulunur. Bazı kartlar sadece o sisteme üye mağazalarda geçerli kabul edilir. Elektronik

sertifikalarda bulunan alanlar, sertifikaların (ve ilgili özel anahtarların) e-posta imzalama ya da dosya imzalama gibi değişik amaçlarla kullanılabileceğini gösteren özel değerler taşıyabilirler. Sİ dokümanı zamanla değişecek, uygulama bağımlı detayları içermez. Bir sertifika içerisinde tekil bir Sİ referansı (Sertifika İlkesi OID) vardır [6]. Sİ bilgisi taşıyan bir sertifika, Şekil 3.19'da gösterilmiştir.

Seri No	2368
Sertifika Sahibi	Hüseyin EROL
Kurum	Gazi Üniversitesi
Yayınlayan	Tübitak
E-posta Adresi	Herol @ gazi.edu.tr
Yayın Tarihi	01.09.2006
Son Kullanım	01.09.2007
İlke/Prensip	E-posta imzalama, dosya imzalama
Açık Anahtar	2489349e894859f45489450dab45454ca09 08d8809
Tübitak E-İmzası	Ae89349c989893e8989548d0823048b080 23f9e903hsasde345l62m234

Şekil 3.19. Sertifikasyon ilkesi

Sertifika uygulama esasları

Sertifika Uygulama Esasları (Sertifika Uygulama Kuralları olarak da kullanılır), SM'nin bir Sİ'yi nasıl gerçekleyeceğini detaylı anlatan dokümandır. Bu dokümanda, bir SM tarafından sertifika yayınlamakta kullanılan ayrıntılı işlemler anlatılır. Tek bir SUE, birden çok Sİ'yi destekleyebilir veya farklı SUE'leri olan SM'ler aynı Sİ'yi kullanarak birlikte çalışabilirler.

Sertifikasyon ilkeleri-sertifika uygulama esasları ilişkisi

Sİ – SUE arasındaki farklar aşağıda açıklanmıştır [6]:

- Sİ, bir sertifikanın hangi emniyet düzeyini sağlayacağını belirtir.
- SUE, Sİ'de belirtilen emniyet düzeyinin nasıl gerçekleneceğini ortaya koyar.
- Bir SUE, belli bir SM için hazırlanır.
- Bir Sİ, SUE'den daha evrenseldir ve başka SM'lere de uygulanabilir.

Örneğin bir Sİ'de aşağıdaki ifade geçebilir:

Sİ: Kullanıcılar, özel anahtarlarının yetkisiz şahısların eline geçtiğini fark ettiklerinde, zaman kaybetmeden işletme makamına haber vereceklerdir.

Bu Sİ ile ilgili SUE'de ise aynı madde ile ilgili olarak aşağıdaki ifadeler geçebilir:

SUE: Tüm kullanıcılar (son kullanıcı SM operatörleri dahil), özel anahtarlarının yetkisizce açığa çıkması durumlarında, bu durumu bildirmeleri gerektiği konusunda bilgilendirilmelidir.

SUE: Özel anahtarların yetkisizce açığa çıkarılması durumu tespit edilirse, kullanıcılar 1 iş günü içerisinde bağlı oldukları SM ile bağlantıya geçeceklerdir. SM ile bağlantıya geçme yöntemi, SUE içerisinde belirtilen yöntemlerden biri şeklinde olabilir.

SUE: Kullanıcılar, kullanımda olmadığı zaman özel anahtarlarını, üzerlerinde taşımalılar veya kilitle korunan bir yerde tutmalıdırlar.

3.15. Sertifika Yaşam Çevrimi

Bir sertifikanın üretilmesinden iptaline kadar geçirdiği aşamalara sertifika yaşam çevrimi denir. Bu çevrim, ESHS tarafından net bir şekilde Sİ ve SUE dokümanları içinde tanımlanır. Aşağıda bir sertifika yaşam çevrimi, genel hatlarıyla tarif edilmiştir [4].

Sertifikanın yayınlanması

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

Sertifikanın kullanımı

1. Kullanıcı gerçekleştirdiği işlemi ya da göndereceği mesajı kendi özel anahtarı ile imzalar ve alıcıya iletir.
2. Alıcı mesajı alır, mesajdaki e-imzayı göndericinin açık anahtarıyla doğrulaması gerekir. Bunun için kullanıcının nitelikli elektronik sertifikasını ESHS'nin herkese açık dizin hizmeti üzerinden sorgular ve sertifikayı elde eder.
3. Sertifikadaki geçerlilik süresini, nitelikli sertifika olup olmadığını ve imzalayan ESHS'nin imzasının doğruluğunu kontrol eder.
4. 2. ve 3. aşamadan sorunsuz geçildikten sonra, mesajdaki e-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.

Sertifikanın iptali ve askıya alınması

Bir NES, 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.

Genellikle bir sertifika, kullanım süresi dolana kadar geçerliliğini korur. Ancak bu

süre dolmadan aşağıdaki sertifika iptal nedenlerinden biri gerçekleşirse sertifikanın geçerliliği kaldırılır ve bu sertifika SİL listesinde yayınlanır.

Sertifika iptal nedenleri

Bir sertifikanın iptal olma nedenleri aşağıda listelenmiştir [42]:

- Sertifikaya ait anahtarın kaybedilmesi veya çalınması,
- Sertifika politikalarının değişmesi,
- SM'nin anahtarının çalınması,
- SM'nin iptal edilmesi,
- Kullanıcının kendi isteği ile sertifikasını iptal ettirmesi,
- Kullanıcı bilgilerinin (ad, soyad, e-posta adresi vb.) değişmesi,
- Kullanıcının yetkilerinin askıya alınması.

Bir sertifikanın seri numarası SİL içinde yayınlandığında bu iptalin nedeni de SİL'de belirtilir. Bu nedenler şunlar olabilir:

- Belirtilmemiş (Unspecified)
- Anahtar çalınması (Key compromise)
- SM anahtarının çalınması (CA key compromise)
- Askıya alma (Cessation of operation)

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 tarihi vardır. E-imza uygulamaları, elektronik sertifikalarla işlem yapmadan önce sertifikanın geçerlilik süresini kontrol ederler. Genellikle bu süre bir yıldır.

3.16. Sertifika İptal Listesi

Sertifika sahibi, sertifikasını kullanmak isteyen kişilere dağıttıktan sonra geri toplayamaz. Ayrıca sertifika sahibinin kendisi ile ilgili değişiklikleri duyurması çok zordur. Bu nedenle 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 ve zaman damgası vurur. 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 [4].

SİL'de üç tür sertifika yer alır:

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

SM, SİL'i düzenli aralıklarla sertifikaların tutulduğu depoya gönderir. Bu durumda akla gelen soru ne kadar sıklıkla SİL'in depoya gönderilmesi gerektiğidir. Örneğin özel anahtarı açığa çıkmış olan bir sertifika en kısa zamanda ipral edilmelidir. Ancak, SM SİL'i depoya gönderene kadar bu işlem gerçekleşemez. Bu nedenle SİL yayınlama periyotları mümkün olduğunca kısa tutulmalı ya da iptal anında SİL yayınlanması sağlanmalıdır. Örnek bir sertifika iptal listesi Şekil 3.20'da gösterilmiştir.

SİL'in özellikleri aşağıda listelenmiştir [42]:

- Sayısaldır.
- Artık güvenilemeyecek olan ve kullanım süresi dolmamış sertifikaların seri numaralarını içerir.

- Yayın tarihini ve son kullanım tarihini içerir.
- Yayınlayan kuruluşun adını ve e-imzasını içerir.
- Sık aralıklarla elektronik ortamda (örneğin internette) yayınlanır.

Şekil 3.20. Örnek bir sertifika iptal listesi

Finansal işlemler gibi anlık doğrulamaya ihtiyaç duyulan uygulamalarda SİL yöntemi yeterince güvenlik sağlamamaktadır. Bu nedenle çözüm olarak çevrimiçi sertifika durum protokolü (online certificate status protocol, OCSP) kullanılmaktadır.

3.17. Sertifikasyon Yolu

Sertifikaların doğruluğu kontrol edilirken her zaman sertifikayı imzalayan makamın e-imzasının doğruluğu kontrol edilir. Bu kontrol işlemi, Şekil 3.21'deki gibi birbirine bağlı olarak bir veya daha fazla sertifikadan oluşan bir zincirin (veya yolun) takibini ve doğrulamasını gerektirebilir [6].

Şekil 3.21. Sertifikasyon yolu

Bu amaçla geliştirilen sertifikasyon yolu çözümleri aşağıdaki özellikleri taşır [42]:

- Ölçeklenebilir bir sistem kurulmaya çalışılır.
- Sertifika yöntemi, hiç tanınmayan kişilere güvenilir bir kurum aracılığıyla güvenmeyi sağlar.
- Haberleşilen bir kişi herhangi bir yayıncı kuruluştan sertifika almış olabilir.
- Kişi/kurum e-posta koruması, sözleşme onaylama, web güvenliği sertifikalarını ayrı ayrı yayıncılardan alabilir.
- Güvenilen tüm sertifika yayıncılarını bir listede tutabilir.
- Bir sertifika yayıncısı diğer yayıncıların güvenilirliğini gösteren sertifikalar yayınlayarak bir sertifikasyon zinciri ya da hiyerarşisi oluşturabilir.
- İki sertifika yayıncısı birbirlerine güvendiklerini gösteren sertifikalar yayınlayarak çapraz sertifikasyon yapabilirler.

3.18. Sertifika Deposu

Sertifika deposu, AAA sistemlerinde kullanılan sertifikaların ve SİL'lerin depolanması ve dağıtımından sorumludur. Bir sertifika deposu birden çok SM'nin sertifika ve SİL'lerini depolayabilir. Sertifika depoları olarak genellikle dizin sistemleri kullanılır. Dizin sistemleri genelde X.500 standardıyla uyumlu olarak

çalışan ve bilgilerin hiyerarşik bir yapıda saklanmasını sağlayan yazılımlardır. Dizin sistemleri genellikle LDAP (Ligthweight Directory Access Protocol) protokolünü desteklerler [6]. En yaygın kullanılan dizin sistemleri olarak Netscape-iPlanet, Microsoft-Active Directory, Critical Path-Injoin, Siemens-Dirx vb. sayılabilir.

AAA açısından bir sertifika deposu tek başına güvenilir kabul edilmez. Sertifika deposu içindeki sertifikalara ve SİL'lere güvenilmesinin sebebi bunların SM tarafından e-imza ile korunmuş olmalarıdır.

Sertifika deposunun barındırdığı sertifika ve SİL'leri sadece yetkili kişiler güncellemelidir. Aksi bir durumda saldırganlar depo içindeki bilgileri kullanılmaz hale getirip AAA'nın çalışmasını engelleyebilir.

3.19. Arşiv Modülü

Arşiv modülü, uzun dönemli veri saklama görevini SM adına yapan modüldür. Arşiv modülü bilginin kendisine ulaştığında doğru olduğunu ve geçen süre içinde değişmediğini garanti altına alır. Arşivlenecek bilgiler (sertifika ve SİL) SM tarafından arşiv modülüne iletilir. İlerde doğabilecek bir anlaşmazlıkta (örneğin eski bir dokümandaki e-imzanın kontrolünde) geçmiş tarihli sertifikanın arşiv modülü tarafından isteyen taraflara verilebilmesi gereklidir. Bu hizmetleri sağlayabilmek için arşiv modülü olarak SM tarafından bir veritabanının kullanılması yaygın bir uygulamadır. Veritabanındaki bilgilerin şifreli ve e-imzalı olarak korunması sayesinde güvenlik hizmetleri sağlanır.

3.20. 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 yapmayanlar 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 [4].

Buna göre ESHS'nin temel görevlerinden biri de kullanıcılara zaman damgası hizmeti vermektir. ESHS bu hizmeti verirken bir takım uluslararası standardlara uygun olarak vermekle yükümlüdür. Kullanıcının da bu hizmeti alabilmesi için ESHS'den talep etmesi gereklidir [46].

3.21. Sertifika Kullanıcıları

Açık anahtar altyapısının ürettiği sertifikaları ve anahtarları kullanan kişiler bu yapının önemli bir parçasını oluştururlar. Sertifika kullanıcıları, açık anahtar altyapısını kullanırken SM veya KM'ye sertifika talebinde bulunurlar. Bir sertifika kullanıcısı SM, KM, bilgi sistem birimi (yönlendirici, güvenlik duvarı, web sunucu vb.) veya gerçek kişi olabilir [43].

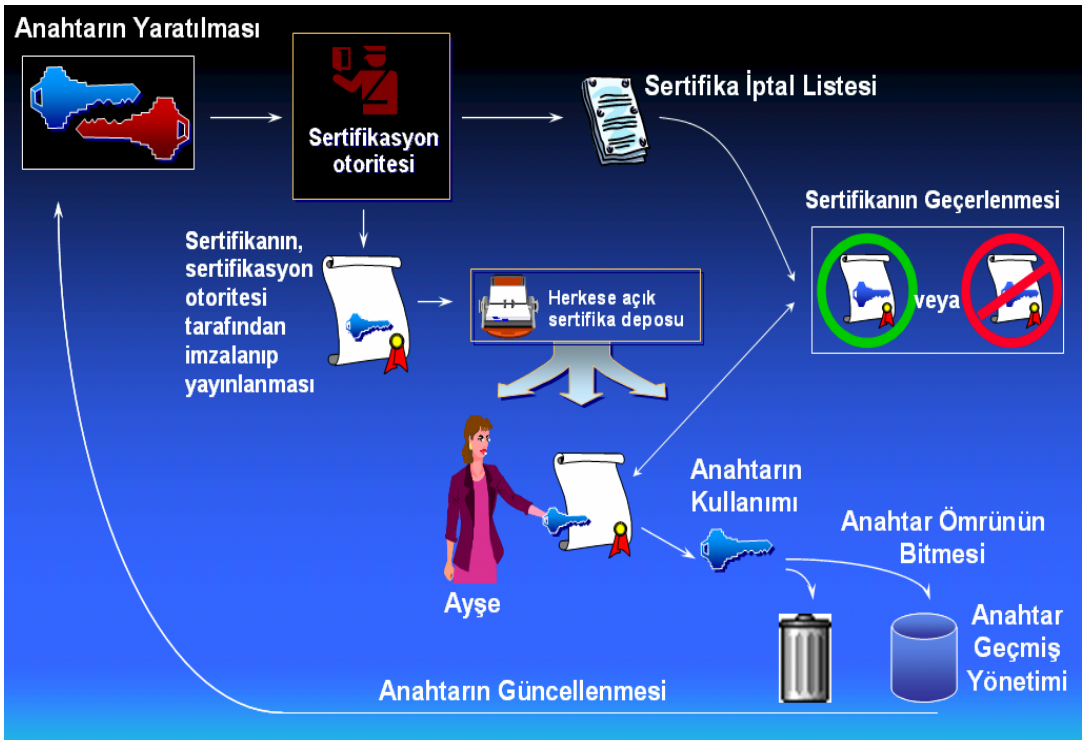
Sertifika kullanıcıları, aldıkları sertifika ile bir özel ve bir açık anahtar sahibi olurlar ve e-imza, simetrik anahtar değiş tokuşu, kimlik doğrulama gibi işlemleri yaparlar. Sertifika kullanıcıları [6]:

- Sertifikalarını yayınlayan SM'yi güvenilen taraf olarak kabul ederler.
- Sertifika deposundan iletişim kurmak istedikleri kişinin sertifikasını ve SM'nin yayınladığı SİL'leri alırlar.
- Sertifikaları kullanarak karşı tarafın e-imzasını ve kimliğini doğrulayabilirler.
- Sertifikasyon yolunu oluşturur ve doğrularlar.
- Sertifika deposu ile anlık haberleşirler.

3.22. Kriptografik Anahtar Çiftleri

AAA sisteminde her kullanıcı için açık ve özel anahtar çiftleri üretilir. İmzalama,

şifreleme, imza onaylama ve şifre çözme işlemlerinde bu anahtar çiftleri kullanılır. Kullanıcının açık anahtarı tüm kullanıcılara dağıtılırken, özel anahtar ise sadece kullanıcı tarafından bilinir. E-imza ve AAA sistemlerinde kullanılan kriptografik anahtar çiftlerinin (özel ve açık anahtarlar) yaşam döngüsü Şekil 3.22'de açıklanmıştır.



Şekil 3.22. Anahtar yaşam döngüsü

Anahtar yaşam döngüsünde, anahtar çiftleri oluşturulduktan sonra sertifikasyon otoritesi tarafından imzalanır ve kullanıcıların açık anahtarları herkese açık sertifika deposunda depolanır. Sertifika SİL listesinde yayınlandığında ise artık diğer kullanıcılar için geçersiz bir sertifikadır ve bu nedenle çöpe atılır ya da geçmişte bu anahtar ile yapılmış işlemlere geri dönebilmek için muhafaza edilir. Bu anahtarın yerine yeni anahtar çiftleri üretilir. Döngü bu şekilde devam eder [35].

3.23. Güvenli Elektronik İmzalama Araçları

Bir e-imza uygulamasında, e-imzanın oluşturulması ve bu imzanın

doğrulanmasından bahsedilebilir. E-imza kanununda belirtilen e-imza oluşturma verisi, e-imzalama amacıyla kullanılan kriptografik özel anahtardır. E-imza doğrulama verisi ise e-imzayı doğrulama amacıyla kullanılan kriptografik açık anahtardır [4].

E-imza kanununa göre, e-imza uygulamalarında imza üretmek için güvenli e-imza oluşturma aracı; varolan bir e-imzayı doğrulamak için güvenli e-imza doğrulama aracı kullanılır. Bu iki amaç için kullanılan cihazlara "Güvenli E-İmza Aracı" (GEİA) denir.

Günümüzde akıllı kartlar (smartcard) ve akıllı çubuklar (token) en yaygın olarak kullanılan GEİA'lardır. Akıllı kart ve akıllı çubuk cihazlarına örnekler Şekil 3.23'te verilmiştir.

Şekil 3.23. Akıllı kart ve akıllı çubuk cihazları

AAA tabanlı uygulamalarda güvenliğin sağlanabilmesi için anahtarların güvenli bir ortamda oluşturulması ve korunması gerekir. X.509 sertifikalarını ve bunlarla bağlı olan anahtarları taşımak için kullanılan en yaygın ve güvenli cihazlar GEİA'lardır. GEİA'lar, programlanabilir alanları olan, dayanıklı, taşınabilir bilgisayarlardır. Bu cihazlar bilgisayardan ayrı olarak çalışırlar ve bilgisayarlar ile olan iletişimleri de şifrelidir. Sahip oldukları PIN/parola ile kaybolması durumunda kullanılması koruma altına alınabilir. Yine kötü niyetli erişim için PIN/parolanın kırılıp içindeki bilgilerin kullanılmasını önleyici mekanizmalara sahiptirler. Portatif ve mobil özelliği sayesinde anahtar/sertifika sahibi anahtar/sertifikasını sürekli yanında taşıyabilir ve ihtiyaç duyulabilen heryerde güvenli bir şekilde kullanabilir. Bu cihazların

dezavantajları ise, akıllı kartlar için kullanılacak donanımların akıllı kart okuyucu gerektiriyor olması veya ilgili araçların kullanımı esnasında kullanılacak işletim sistemi vb. ortamlar için sürücü (driver) yüklenmesinin gerekebileceği şeklinde sıralanabilir [21].

Akıllı kart ve akıllı çubuk cihazları arasında birtakım farklılıklar vardır. İlk fark, şekil ve bilgisayarlara bağlantı arayüzleridir. Akıllı kartların kullanımı için bir akıllı kart okuyucuya ihtiyaç vardır. Akıllı çubuk ise artık birçok bilgisayarda bulunan USB arabirimi üzerinden bilgisayara bağlanabilir. Bunun yanında akıllı kartlar, üzerlerinde farklı uygulamalarda kullanılmak üzere birden çok elektronik devre barındırabilirler. Örneğin bilgisayara giriş için kullanılan bir akıllı kart, elektronik kapı kilitlerini açmakta da kullanılabilir (Şekil 3.24) [4].

Şekil 3.24. Akıllı kartların kullanımı

GEİA üreten firmalar artık AAA icin özel cihazlar üretmektedirler. Bu kartlarda özellikle rastgele sayı üretici (random number generator, RNG) modülleri vardir ve üretilen açık ve özel anahtar çiftinden sadece açık anahtar bilgisayara gönderilir. Daha fazla güvenlik istenirse özel anahtar GEİA üzerinde simetrik şifreli olarak da saklanabilir. Genellikle açık anahtar GEİA üzerinde sertifika olarak saklanır [49]. Bu cihazların kriptolojik işlemci taşıyan modelleri aşağıdaki yeteneklere sahiptir [21,34]:

- GEİA üzerinde şifreleme ve şifre çözme,
- GEİA üzerinde imzalama ve imza onaylama,
- GEİA üzerinde özel ve açık anahtarların güvenli bir şekilde tutulması,
- GEİA içine bilgi yazabilme,
- GEİA'nın şifre ile korunması,
- Entegre yongayı çalıştırmak için yerel tanılama (örneğin PIN, biometrik vb.),
- Çoklu uygulama özellikleri.

GEİA'ların gizli (private) ve (açık) public alanları vardır. Gizli alanında anahtar üretimi, imzalama, şifre çözme gibi işlemler yapılır, bu alana erişim yasaklanmıştır. Açık alana ise genel bilgiler yazılır. GEİA programı yardımıyla buradaki bilgiler görülebilir [34]. Bir AAA sistemi tarafından kullanılan bir GEİA'da olması gereken nesneler aşağıda listelenmiştir:

- İmzalama özel anahtarı,
- Şifreleme özel anahtarı,
- O an geçerli olan imzalama sertifikası,
- O an geçerli olan şifreleme sertifikası,
- Daha önce geçerli olan şifreleme özel anahtarları ve karşılığı olan sertifikaları.

E-imzalama amacıyla kullanılacak GEİA'lar aşağıdaki standartlara da uygun olmalıdırlar [46]:

- CWA 14169,
- TS ISO/IEC 15408 veya ISO/IEC 15408'e göre en az EAL4+ ,
- CWA 14171.

Güvenli elektronik imzalama aracının kullanımı

GEİA'nın bir e-imza uygulamasında kullanımında genel olarak beş aşamadan söz edilebilir [4]:

- Kullanıcının uygulamayı kullanmak üzere kaydedilmesi,
- GEİA'nın kişiselleştirilmesi,
- GEİA'nın kullanıcıya ulaştırılması,
- GEİA'nın kullanımı,
- Beklenmeyen durumların kotarılması.

E-imza uygulamasını kullanacak belli bir kullanıcı grubu vardır. Bu kullanıcı grubu örneğin, bir kamu kurumuna ait bir iç uygulamada kurumun personeli, bir kamu kurumunun vatandaşın kullanımına yönelik olarak hazırladığı bir uygulamada ise vatandaşlar olacaktır. Uygulamayı kullanacak olanlar için mutlaka bir kullanıcı kaydı oluşturularak bu kullanıcılar için en az bir e-imza oluşturma ve doğrulama verisi çifti (yani kullanıcının açık ve özel anahtar çifti) oluşturulmalıdır.

Kullanıcı e-imzasını atmak istediği zaman GEİA'sını kullanacaktır. E-imzanın atılması demek, aslında GEİA üzerinde bulunan bir e-imza fonksiyonuna, yine GEİA'da bulunan özel anahtar ile imzanacak dökümanın kriptografik olarak özetlenmiş halinin verilmesi ve bu fonksiyondan sonuç olarak imza bilgisinin oluşturulmasıdır. Burada en önemli nokta, imzalama işlemi GEİA üzerinde yapılabildiğinden, özel anahtarın GEİA dışına çıkması gerekmemektedir.

3.24. Açık Anahtar Altyapısı Yönetim Protokolleri

SM, sertifikaları ve SİL'leri doğru bir şekilde yayınlamak ve aynı zamanda özel anahtarını da korumak zorundadır. AAA'nın bileşenleriyle haberleşirken haberleşmenin içeriği korunmalı, bütünlük ve gizlilik kurallarına uyulmalıdır.

SM, sertifika için başvuran kişinin kimlik bilgilerini doğrulamalı ve verdiği sertifikanın yanlış bilgi içermediğinden emin olmalıdır. Benzer şekilde, bir sertifika iptal isteği geldiğinde, bunun yerinde bir istek olduğundan emin olmalı ve yanlış iptal yapmamalıdır. İptal edilmemesi gereken bir sertifikayı SİL'de yayınlamak da; iptal edilmesi gereken bir sertifikayı SİL'de yayınlamamak da SM için hatadır. Hata

yapmamak haberleşme yollarının hatasız olmasını gerektirir.

Tüm ihtiyaçları karşılayabilmek için SM'nin aldığı bilgiler güvenilir olmalıdır. AAA yönetim protokolleri, SM'nin bilgi toplaması ve bilgileri dağıtması için kullanılır. En yaygın olarak kullanılan yönetim protokolleri aşağıda listelenmiştir [34]:

- PKCS #10 Sertifika Talep Standardı ve SSL
- PKCS #10 Sertifika Talep Standardı ve PKCS #7
- Sertifika Yönetim Protokolü (CMP)
- Certificate Management Using CMS
- Simple Certificate Enrollment Protocol (SCEP)

Yönetim için özel bir protokol tasarımı yapılıp kullanılabilir ama yaygın kullanılan protokoller çok daha fazla incelendiğini için daha fazla güven sunarlar.

PKCS Yönetim Standartları

PKCS (Public Key Cryptography Standards) standartları, RSA firması tarafından yayınlanmış ve kriptografi dünyasında yaygın kabul görmüş standartlardır. Bu standartlar Çizelge 3.2'de verilmiştir:

Çizelge 3.2. PKCS yönetim standartları

#1	RSA açık anahtar algoritması kullanarak şifreleme ve e-imzalama işlemi yapılmasını tanımlar
#3	Diffie-Hellman anahtar belirleme protokolünü tanımlar
#5	Bir şifre kelimesinden elde edilen gizli anahtarla şifrelemenin nasıl yapılacağını anlatır
#7	E-imzalama ve şifrelemede kullanmak üzere kriptografik yöntemleri destekleyen genel bir mesaj formatı tanımlar
#8	Değişik açık anahtar algoritmalarında kullanılabilecek bir özel anahtar formatı tanımlar
#9	Diğer PKCS standartlarında kullanılabilecek nitelik tiplerini tanımlar

Çizelge 3.2. (Devam) PKCS yönetim standartları

#10	Sertifika talep formatını tanımlar
#11	Kriptografik cihazlarda (akıllı kart vb.) kullanılabilecek donanım bağımsız bir programlama kütüphanesini tanımlar (Cryptoki adıyla da bilinir)
#12	Bir kullanıcının özel anahtarı, sertifikası gibi bilgileri saklamak ve taşımak için bir format tanımlar
#13	Eliptik eğri kriptografi kullanarak şifreleme ve e-imzalamayı tanımlar
#14	Pseudo-random sayı üretimini tanımlar (geliştirme aşamasında)
#15	PKCS#11'i tamamlayan bir standarttır, kriptografik cihaz tiplerini çeşitlendirir

3.25. Açık Anahtar Altyapısı Mimarileri

Bir AAA'nın sadece bir SM barındırması şart değildir. AAA sistemlerinde genellikle bir çok SM bulunur ve bunlar kendi aralarında iletişimde bulunabilirler. Ayrıca farklı AAA'lara ait SM'ler arasında da iletişim ve güven mekanizması kurulması gerekebilir. Bütün bu ihtiyaçlardan dolayı değişik AAA mimari tasarımları yapılmıştır. Bir AAA mimarisi incelenirken aşağıdaki sorulara cevaplanmalıdır [42]:

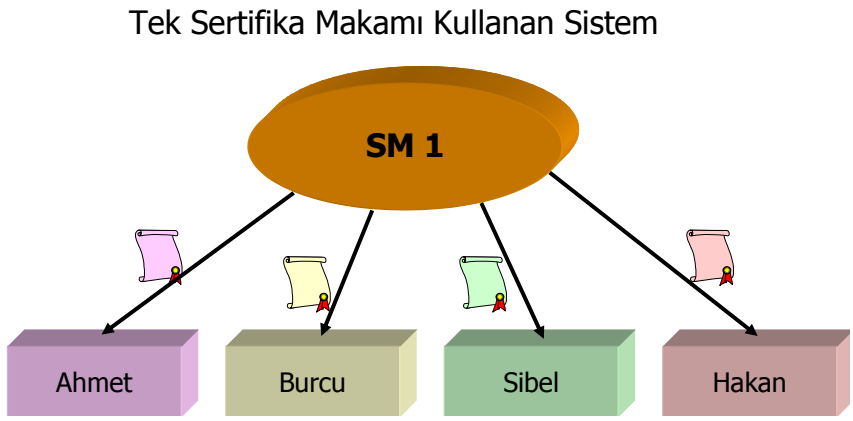
- Kaç tane SM güvenilir kabul edilecek?
- SM'ler arasında ne tür ilişkiler var?
- Yeni SM'ler sisteme ne kadar kolay (ya da zor) ekleniyor?
- Sertifikasyon yolunun oluşturulması ne kadar karışık? Sertifikasyon yolu kurulduktan sonra doğrulama ne kolaylıkta yapılabiliyor?
- Bir SM kullanılamaz hale gelirse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

3.25.1. Tekli/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 mimari, "Tek SM" ve "SM Listesi" olarak iki grupta incelenebilir.

Tek SM

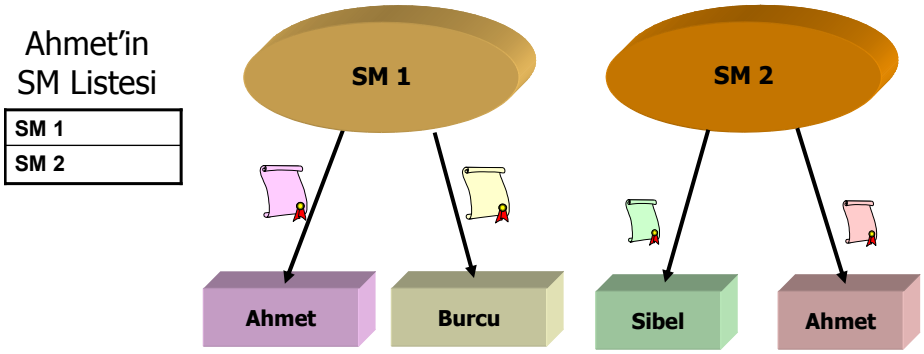
AAA mimarileri içinde, genişleme ve büyüme kabiliyeti olmayan en basit mimaridir. Kullanıcılar, sertifika veren tek bir SM'ye güvenirler [6]. Şekil 3.25'de gösterilen bu sistemde sadece bir SM vardır ve yeni SM eklenemez. Tek SM olduğu için de diğer SM'ler ile güven ilişkisi kurmasına da gerek kalmamaktadır. En büyük dezavantajı SM'nin kullanılamaz hale gelmesi durumunda tüm sistemin çalışamaz hale gelmesidir. Bu durumda SM'yi yeniden kurmak için tüm sertifikaların yenilenmesi gerekmektedir [43].



Şekil 3.25. Tek sertifika makamı kullanan sistem

SM listesi

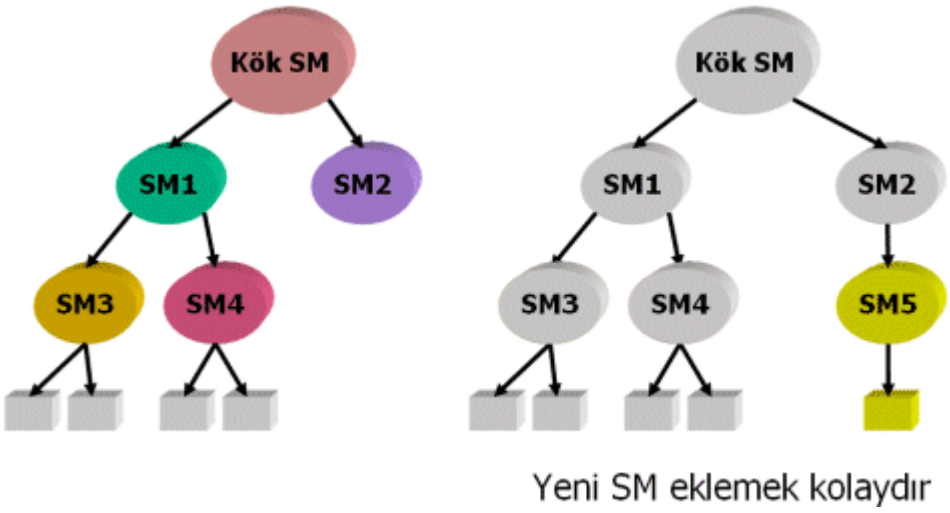
Bu mimaride ise yapı biraz daha genişlemiştir. Bir kullanıcı birden fazla SM'den sertifika almış olabilir. Bu durumda güvenmiş olduğu tüm SM'leri kendi SM listesinde toplar. SM'ler arasında güven ilişkisi yoktur. Bu mimari Şekil 3.26'da gösterilmiştir [6,43].



Şekil 3.26. SM listesi

3.25.2. Hiyerarşik mimariler

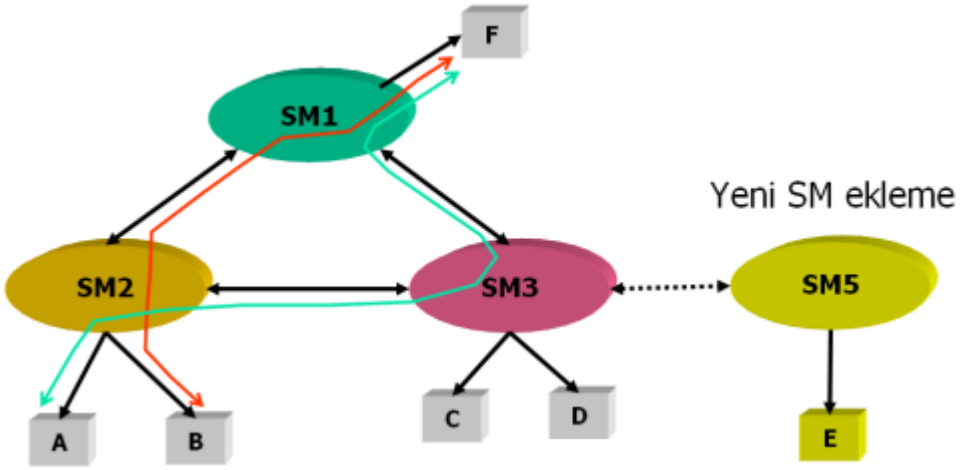
En yaygın kullanılan mimari tipi hiyerarşik mimaridir. Şekil 3.27'de gösterilen bu mimaride SM'ler arasında alt-üst ilişkisi vardır [6]. Ağaç yapısının en üstünde yer alan SM'ye Kök Sertifikasyon Makamı (KSM) denir. Hiyerarşide üstte yer alan SM kendi altındaki SM'lere sertifika verir. Sertifikasyon yolu oluşturmak kolaydır. SM'lerden biri kullanılmaz hale gelirse sadece onun altındaki sertifika sahiplerine yeniden sertifika üretmek yeterli olmaktadır. KSM özel anahtarının kaybolma durumunda ise sadece onun hemen altındaki SM'lere yeni sertifika üretmek yeterli olacaktır [42].



Şekil 3.27. Hiyerarşik mimari

3.25.3. Dağıtık mimariler

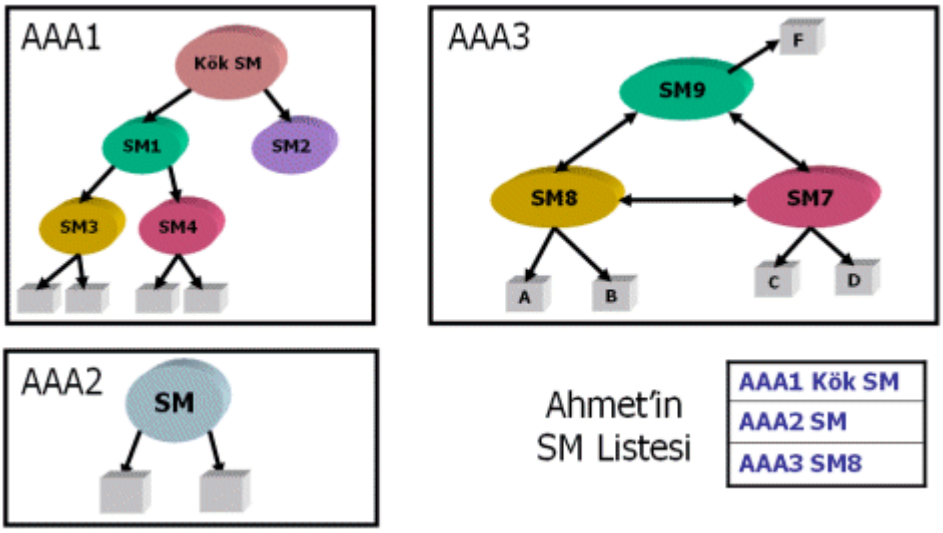
Dağıtık mimari, hiyerarşik mimarinin alternatifidir. Güven ağı olarak da adlandırılır. Bu mimaride birbirine güvenen iki SM birbirlerine sertifika vererek güven ilişkisi kurarlar. Şekil 3.28'de gösterilen bu mimaride, kullanıcılar ilk önce kendi sertifikalarını üreten SM'ye ve onun üstünden eriştikleri diğer SM'lere güvenirler [6]. SM özel anahtarını kaybederse sadece sertifika verdiği kullanıcılar etkilenir. En kötü durumda AAA yapısı bölünebilir [43].



Şekil 3.28. Dağıtık mimari

3.25.4. Genişletilmiş SM listesi

SM listesine tek SM'ler dışında hiyerarşik AAA'nın KSM'si ya da dağıtık AAA'nın bir SM'si eklenebilir. Böylece basit SM listesindeki gibi listenin çok büyümesi önlenmiş olur. Bu mimari Şekil 3.29'da verilmiştir [6]. Bu mimaride SM'lerden birinin özel anahtarı geçersiz olursa bu durumun duyurulması zordur [43].

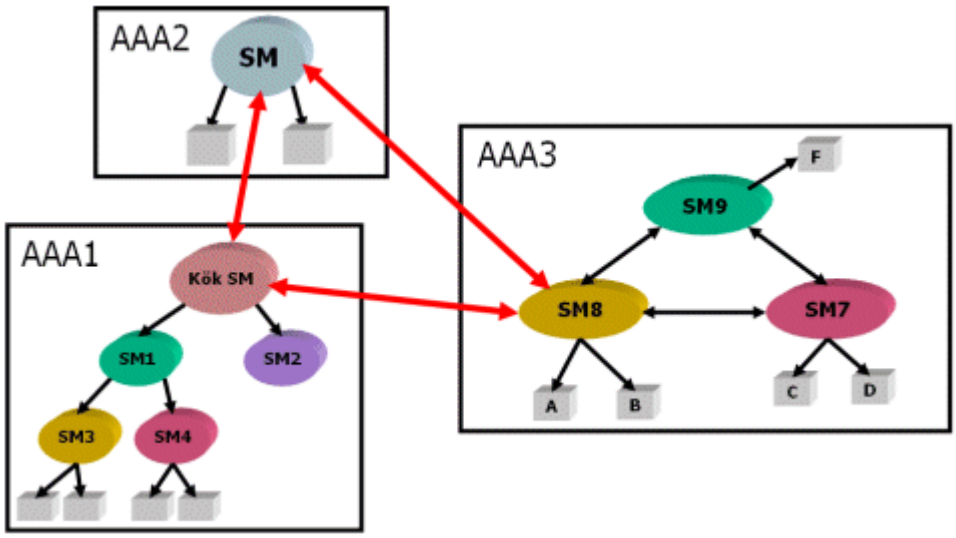


Şekil 3.29. Genişletilmiş SM listesi

3.25.5. Çapraz sertifikasyon

Çapraz sertifikasyon, farlı SM'ler altında bulunan kullanıcıların birbirlerinin sertifikalarına erişimini sağlamak için kullanılır. Bu işlemde bir SM diğer SM için bir sertifika üretir. Böylece sanki kullanıcıymış gibi ikinci SM diğerinden sertifikaları güvenli bir şekilde alabilir. Çapraz sertifikasyon tek yönlü ya da çift yönlü olarak uygulanabilir [6,23]. Bu mimari Şekil 3.30'da gösterilmiştir.

Çapraz sertifika, bir ESHS tarafından başka bir ESHS'ye, karşıdaki ESHS'nin genel anahtarını içerecek şekilde elektronik olarak imzalayıp yayınladığı genel anahtar sertifikasıdır. Temel olarak bir ESHS kullanıcılarının, kendi ESHS'leri ile çapraz sertifikalandırılmış diğer ESHS kullanıcılarına güven duymasıdır [31]. 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.

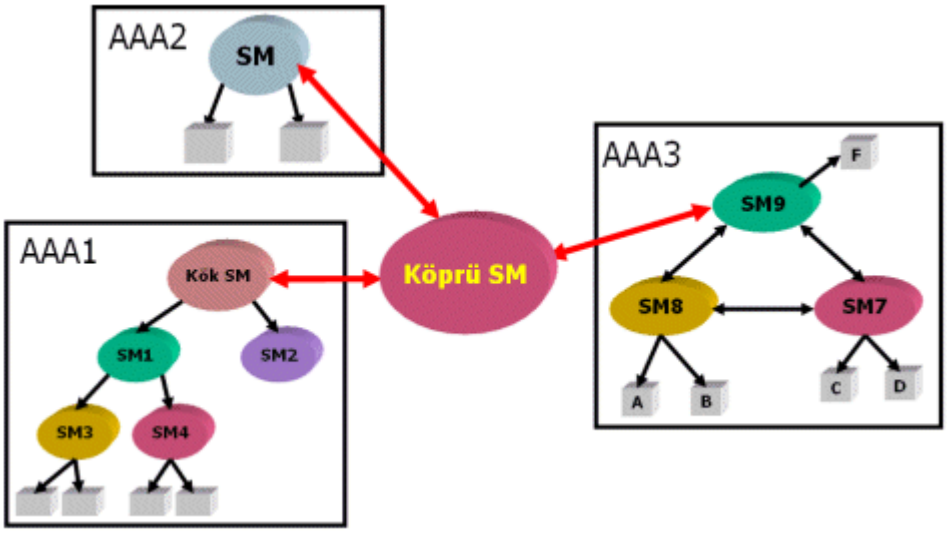


Şekil 3.30. Çapraz sertifikasyon

Çapraz sertifikasyonda karşılaşılan birtakım problemler vardır. Bunlardan en önemlisi, birden çok ESHS boyunca "geçişli güven" diye de adlandırılan, istenmeyen güven zincirlerinin ortaya çıkabilmesidir. Örneğin ESHS1, ESHS2'ye güveniyor ve ESHS2 de ESHS3'e güveniyorsa, ESHS1'in ESHS3'e güveniyor olmasını önlemek gerekebilir. Çapraz sertifikalarda bu tarz prolemleri önlemek ve güven ilişkilerini sınırlandırmak üzere geliştirilmiş bazı eklentiler mevcuttur. Bu eklentiler, isim sınırlamaları, ilke sınırlamaları ve yol uzunluğu sınırlamalarıdır [4].

3.25.6. Sertifikasyon köprüsü

Çapraz sertifikasyon çok sayıda AAA arasında olursa yönetim zorlaşır. Bu durumda AAA'lar arasında güven ilişkisini kuran bir köprü SM kurulabilir. Burada aralarında güven ilişkisi kuracak olan SM'ler sadece köprü SM ile sertifika değiş tokuşu yaparlar. Köprü SM özel anahtarını kaybederse sistem birbirinden bağımsız AAA'lar haline gelir fakat yeniden normal duruma dönmek kolaydır. Bu mimari Şekil 3.31'de gösterilmiştir [6,43].



Şekil 3.31. Sertifikasyon köprüsü

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. Köprü ESHS'ler, etki alanları arasındaki karşılıklı çalışabilirlik için geçerli eğilim olarak çapraz sertifikasyon kullanırlar [24].

4. DÜNYADA VE ÜLKEMİZDE KURUMSAL ELEKTRONİK İMZA ALTYAPILARI VE ÖRNEK UYGULAMALAR

Gelişmiş ülkelerin neredeyse tamamında ve ülkemizde e-imza ile ilgili yasallaşma süreci tamamlanmış olmasına rağmen, henüz e-imzanın yaygınlıkla kullanılmadığı görülmektedir [5]. Ancak günümüzde, bütün dünya ülkeleri AAA ve e-imza konusundaki çalışmalarını yoğun şekilde sürdürmektedir. Bu bölümde dünyada ve ülkemizde e-imzaya ilişkin mevzuat, kurumsal altyapı ve örnek uygulamalar anlatılmıştır. Özellikle dünyada ve ülkemizde ön plana çıkan e-imza projelerinin uygulama alanları ve kazanımları incelenerek, ülkemizde hayata geçirilecek projelere örnekler sunmak, böylelikle e-imzanın yagunlaşma sürecine katkı sağlamak hedeflenmiştir.

Uygulamalar açısından Türkiye'deki mevcut duruma bakıldığında; kurumsal işlemlerin ve vatandaşa yönelik hizmetlerin elektronik ortama aktarılmakta olduğu, bu anlamda kamu sektöründe birbirinden bağımsız çalışmalar yapıldığı, kurumların bilgi verme amaçlı olarak altyapı oluşturduğu, ancak elektronik işlem yapılması çalışmalarının henüz tamamlanmamış olduğu görülmektedir [21].

Her ne kadar e-imza kullanımı ülkemizde fazla yaygınlaşmamış olsa da, gerek devlet gerek özel sektör gerekse de silahlı kuvvetler bünyesinde, AAA ve e-imza uygulamaları kullanılmakta, bu konuyla ilgili AR-GE yatırımları yapılmakta ve bu uygulamaların etkin olacağı kullanım ve güvenlik alanları oluşturulmaktadır.

4.1. Dünyada Elektronik İmza'ya İlişkin Mevzuat

AAA ve e-imza uygulamalarının da temelini oluşturan yasaların dünya ülkelerindeki gelişimleri genel olarak 2000 yılında gerçekleşmiştir. Başta ABD'nin e-imza yönergesi ve Avrupa Birliği (AB)'nin üye ülkelerini kapsayan e-imza yönergesi olmak üzere birçok ülke yasal çerçeveyi belirlemiş, ardından da diğer ilgili yasa ve yönetmelikleri yürürlüğe girmiştir.ABD e-imza yönergesi 2000 yılında, AB e-imza yönergesi ise 17 Temmuz 2001'de bütün üye ülkelerde aynı anda yürürlüğe girmiştir.

Ülkelerin e-imza ile ilgili yasal düzenlemelerini yaparak e-imzaya geçtikleri tarihler ve halen e-imza çalışmaları devam eden ülkeler aşağıda listelenmiştir [5,21,29].

Avrupa kıtası ülkelerinin e-imzaya geçiş tarihleri

- 1997 yılı : İtalya
- 1998 yılı : Almanya
- 1999 yılı : Portekiz, İspanya
- 2000 yılı : Fransa, Danimarka, Lüksemburg, İngiltere, İrlanda, Avusturya, Çek Cumhuriyeti, Estonya, Litvanya, Slovenya
- 2001 yılı : Belçika, İsveç, Macaristan, İzlanda, Norveç
- 2002 yılı : Hollanda, Polonya
- 2004 yılı : Türkiye

Amerika kıtası ülkelerinin e-imzaya geçiş tarihleri

- 1999 yılı : Bermuda, Peru, Kolombiya
- 2000 yılı : ABD
- 2001 yılı : Kanada, Arjantin

Asya kıtası ve diğer ülkelerin e-imzaya geçiş tarihleri

- 1995 Yılı : Rusya
- 1998 Yılı : Hindistan, Malezya
- 1999 Yılı : Singapur, Güney Kore
- 2000 Yılı : Japonya, Hong Kong, Filipinler, Avustralya, İsrail
- 2002 Yılı : Tayland

E-imza geçiş çalışmaları devam eden ülkeler

- Bulgaristan
- Malta
- Slovak Cumhuriyeti
- Ukrayna
- Brezilya
- Ekvator
- Meksika
- Çin Cumhuriyeti
- Tayvan
- Yeni Zelanda
- Gibralta

4.2. Dünya'da Elektronik İmza Altyapıları ve Örnek Uygulamalar

Bu bölümde, dünyada e-imza konusundaki mevcut projeler ve oluşturulan AAA'lar hakkında bilgi verilmiş ve ülkemizde hayata geçirilecek projelere örnek olması açısından uygulama alanları ve kazanımları incelenmiştir.

Fransa Maliye Bakanlığı projesi

Fransa Maliye Bakanlığı, 1998 yılında kurumların internet üzerinden vergi beyanı yapmaları amacıyla 15 milyon €'dan fazla geliri olan 20,000 firmanın vergi beyanlarını internet üzerinden gerçekleştirmesi zorunluluğunu yasalarla getirmiştir. Bu kapsamda, 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 sayının 80,000'lere ulaşması yönünde çalışmalar devam etmektedir. Bu projede sağlanan çözüm ile zaman, maliyet ve insan kaynağı açısından tasarruf sağlanmıştır [21,29].

Köln şehri kartı projesi

Köln Şehri Kartı projesi, Almanya'da kamu alanında yürütülen en büyük projedir. Bu proje, belediye hizmetleri içerisinde bulunan iş süreçlerinin, çalışanlar ve vatandaşlar için güvenli elektronik bir ortama taşınması süreçlerini kapsamaktadır. Proje ile, vatandaş ve belediye arasındaki elektronik iletişimin sağlanması ve bu iletişimin yasal geçerliliğinin de olması için AAA ile akıllı kartların bütünleştirildiği bir e-imza çözümü sunulmuştur. Buna bağlı olarak iş süreçleri e-imzalar yardımıyla iyileştirilmiş; çoklu uygulamalı kartlarla birlikte eğitim, kültür ve sağlık alanına da çözümler getirilmiştir [5].

Sanal şehir Hagen projesi

Tüm kamu hizmetlerine sanal ortamda erişim sağlayarak "e-devlet" uygulamalarının temelini oluşturan sanal şehir Hagen projesi, yeni teknolojiye geçişte esnek bir yapı, gizliliğin ve doğrulamanın şifreli veri transferi ve e-imzalarla sağlanması ve AAA ile bütünleşik bir çözüm sunmaktadır.

Proje ile, vatandaşın işini kolaylaştıran, "bilişim toplumu" için uygun bir altyapı oluşturan e-imza ve AAA çözümüyle yönetimsel süreçlerin düzenlenmesi ve hızlandırılması, vatandaşa ait bilgilerin gizliliğinin sağlanması, hizmetlere kolay erişim, e-imzaların kullanımıyla zaman kazanımı sağlanmıştır [21,29].

Alman bankalarında e-imza kullanımı

Almanya'nın büyük bankalarından Postbank AG, pek çok yemleme (phishing) saldırısına konu olması üzerine, müşterilerinin online kişisel bilgilerinin çalınmasını engellemek için e-imza kullanımına geçmiştir. Proje kapsamında banka, müşterileri ile yapacakları bütün e-mail haberleşmelerinde e-imza kullanmayı hedeflemektedir. Bankanın kullandığı e-imza GeoTrust'un Almanya temsilcisi olan TC Trust GmbH tarafından sağlanmaktadır. Diğer bankalarda da benzer sorunları çözmek nedeniyle

e-imza kullanımının kısa sürede yaygınlaşacağı beklenmektedir.

İtalya İçişleri Bakanlığı İtalyan kimlik kartı projesi

İtalya, Avrupa bölgesinde elektronik karta ilk geçen ülkelerden biridir. 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 AAA yönetimi ile güvenli, belediyelerde online (çevrimiçi) elektronik kimlik kartı dağıtımı işlemleri ve süreçleri gerçekleştirilmiştir. Proje pilot aşamasında Milano, Palma ve Roma'da bulunan 83 belediye ve 280,000 vatandaşı kapsamıştır. İtalyan Hükümeti 2009 yılı sonuna kadar yaklaşık 40 milyon elektronik kimlik kartı oluşturmayı hedeflemektedir [5,21,29].

Hong Kong akıllı kimlik kartları projesi

Hong Kong, bilgi ve iletişim teknolojilerinde yüksek kullanım oranlarının olduğu ülkelerden biridir. Hong Kong'ta, yaklaşık 7 milyon nüfusa karşılık, 6 milyonun üzerinde cep telefonu kullanıcısı ve 2.5 milyon internet hesabı vardır [19].

Hong Kong sertifika otoritesi 2000 yılından itibaren 110,000 sayısal sertifika satmıştır. Kurum, sertifika kullanımını artırmak için, Temmuz 2003'ten itibaren akıllı kimlik kart sahiplerine sertifikaları kartlarına yerleştirme olanağını bir yıl için hiç bir ücret almadan gerçekleştirme önerisiyle gitmiştir. Hong Kong kimlik kartı sahiplerinin, varolan kimlik kartlarını akıllı kimlik kartları ile değiştirecebilecekleri sürecin dört yıl sürmesi hedeflenmektedir [21].

Yeni Zelanda hükümeti e-imza uygulamaları

Yeni Zelanda'da 1999 yılından bu yana elektronik ortamda şifreleme, kullanıcılara

uygulamalara giriş izni verme gibi işlerde AAA kullanılmaktadır. Kullanılan sertifika otoritesinin de ilgili bakanlığa ait olmasının, kritik birçok altyapı bileşeninde, otomasyona geçmiş kullanıcı yönetimi için maliyetten tasarruf ettiren bir yöntem olduğunu kanıtlanmıştır. Bu sayede bakanlık, yaklaşık 9000 kullanıcıyı yaklaşık kullanıcı başına 12NZ$'lık bir marjinal maliyetle yönetebilmektedir [29].

Yeni Zelanda'da 30'un üzerinde devlet dairesinde sayısal sertifikalar ile internet üzerinden güvenli bilgi alışverişi sağlanmaktadır. Ayrıca, Hazine Finansal Bilgi Sistemi (CFISnet) kullanıcılarının tarayıcı doğrulanması işlemi için de sayısal sertifikalar kullanılmaktadır. Hazine sayısal sertifikaları aynı zamanda kullanıcıların kurum dışı çalışma alanına girişleri, dizüstü bilgisayarları şifrelemek ve uzaktan giriş izinleri için de kullanmaktadır. Ayrıca 4000 kullanıcı ile Landonline sisteminde, yaklaşık 10000 kullanıcı ile sağlık hizmeti alanında sayısal sertifikalar kullanılmaktadır [21].

ABD'de e-imza altyapısı ve Savunma Bakanlığı ECA projesi

ABD'de elektronik sertifika hizmet sağlayıcıları (ESHS) 1990'lı yılların ikinci yarısıyla birlikte faaliyete geçmişlerdir. ABD'de aynı zamanda federal düzeyde hizmet veren bir kamu ESHS da vardır. Bir ana kök işlevi üstlenen bu kurum, tüm ABD'de kamusal alanda elektronik sertifika kullanımının sağlanmasında anahtar rol oynamaktadır [19].

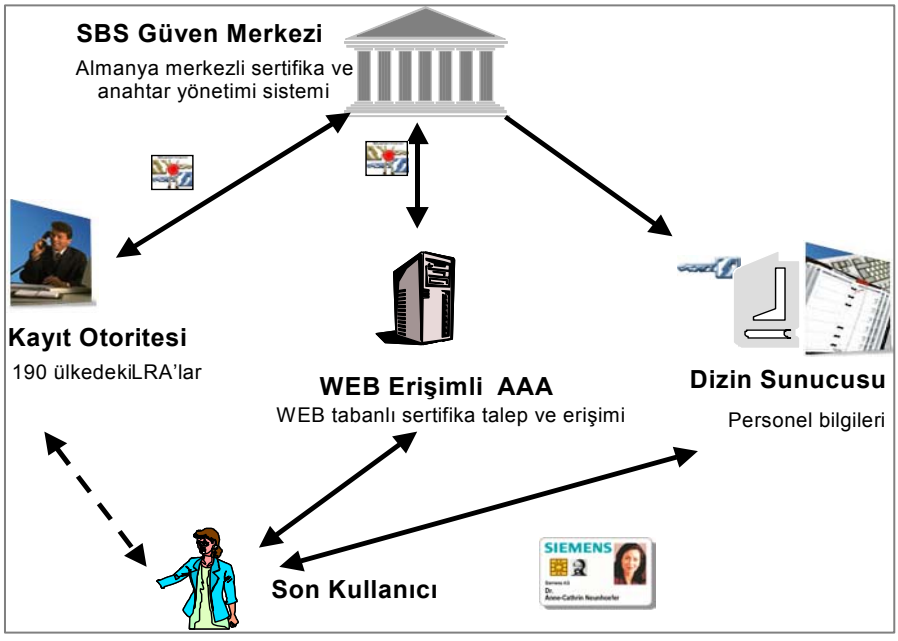
ABD Savunma Bakanlığı'nın ECA projesi, ülkenin en önemli e-imza uygulamalarındandır. ECA (Dışsal Sertifika Otoritesi), bakanlık ile tedarikçiler arasındaki online işlemleri daha güvenli hale getirmek üzere hazırlanmıştır. ECA, Savunma Seyahat Sistemi, Elektronik Doküman Girişi ve Geniş Alan İş Akışı olmak üzere üç programı kapsamaktadır. İleriki dönemlerde programın, bakanlığın 350.000'den fazla iş ortağını da kapsayan, daha geniş uygulamalar ile daha da gelişeceği değerlendirilmektedir. Bu programda gerekli olan sayısal sertifikaların sağlayıcısı olarak Verisign kullanılmaktadır [29].

Güney Kore e-imza çalışmaları

Dünyada e-imzanın uygulama ve yaygınlığı açısından önde sayılabilecek ülkelerden birisi de Güney Kore'dir. Güney Kore, e-imza kanununu 1999 yılında çıkarmıştır. Ülkede 2000 yılından başlayarak kurulan 6 ESHS faaliyete geçmiştir ve bu sağlayıcıların her birinin milyonlarca dolar yatırım yaptıkları bilinmektedir. 2000 yılında 50,000 ile başlayan sertifika sahibi sayısı, 2003 yılı itibariyle yaklaşık 7 milyona ulaşmış durumdadır. Güney Kore için çarpıcı istatistikler arasında, yaklaşık 18 milyon internet bankacılığı kullanıcısı olduğunu ve borsa işlemlerinin %64'ünün ağlar üzerinde gerçekleştiği bilinmektedir [19].

Siemens ve SBS kurumsal açık anahtar altyapısı projesi

Siemens ve SBS bünyesinde kurulan sertifika otoritesi, tek merkezden tüm dünyadaki Siemens ve SBS çalışanlarına (2001'den itibaren 190 ülkede, 500 lokasyonda 484.000 kullanıcı) e-imza ve şifreleme yoluyla güvenlik çözümü sağlamaktadır (Şekil 4.1) [21,29].



Şekil 4.1. Siemens ve SBS kurumsal AAA projesi

Bu proje ile e-posta, dosya ve veri şifreleme, oturum açma (logon), intranet erişimi ve iş süreçleri yönetimi alanlarında güvenlik talep eden müşteriye e-imzalar, sayısal sertifikalar, sertifika yönetimi, son kullanıcı yazılımları sunulmuştur. Proje kapsamında AAA hizmetleri akıllı kartlar ile bütünleşik haldedir.

Proje ile kurum içi ve kurumlar arası güvenli iletişim, iyileştirilmiş ve otomasyonu sağlanmış iş süreçleri, zamandan tasarruf ve yönetilen AAA sayesinde kolay uygulanabilen ve düşük maliyetli çözüm sağlanmıştır.

Japonya - Suzuken firması e-imza projesi

Suzuken firması, merkezi Nagoya'da yer alan ve ülke çapında 110.000 eczane ve ilaç kuruluşuna ilaç ve tanı medikal ekipmanı sağlayan bir ilaç toptancısıdır. Suzuken, 2001 yılında ilaç şirketleri yani müşterileri ile olan bilgi alışverişi ve çevrimiçi (online) ürün talepleri için web tabanlı bir satış destek sistemini hizmete sokmuştur. Bu sistemdeki e-posta, ürün talep bilgileri ve diğer değerli bilgilerin güvenliği için AAA 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 [21].

Almanya DSV

DSV (Deutscher Sparkassen Verlag), Alman bankacılık sisteminin (Sparkassen Finanzgruppe) servis sağlayıcısıdır. DSV, finans kuruluşlarına pazarlama ve medya hizmetleri, debit ve kredi kartları basımı, elektronik ödeme sistemleri ve ATM'ler için terminaller de dahil 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. DSV, proje kapsamında basılacak 20 milyon akıllı karta, VeriSign'ın dijital sertifika hizmetlerini kullanarak sertifika eklemeyi ve 600 üye finans kuruluşunun e-posta doğrulama işlemleri için sayısal sertifika altyapısı sunmayı planlamaktadır. Sayısal sertifikalı akıllı kartlar, kullanıcılarının doğrulanmasında ve kullanıcıların internet üzerinden daha güvenli işlem yapmalarına olanak sağlamaktadır. Buna göre DSV, genel bankacılık hizmetlerini daha güvenilir hale getirmeyi hedeflemektedir [29].

Identrus

Nisan 1999'da 8 büyük banka (ABN AMRO Bank, Bank of America, Bankers Trust, Barclays Bank, Chase Manhattan, Citibank, Deutsche Bank ve Hypo Verinsbank) tarafından bir "güven şirketi" olarak kurulan Identrus, şu anda 60'ın üzerinde finansal kuruluşu bünyesine katmış durumdadır. Identrus, Verisign'ın partnerliği ile, üye bankaların, müşterileri olan şirketlere sayısal sertifika vermesini sağlayan sistem operatörlüğü görevini yürütmektedir [21].

Kanada CIBC bankası

CIBC (Canadian Imperial Bank of Commerce), 9 milyondan fazla bireysel ve kurumsal müşterisi bulunan, Kuzey Amerika'nın en büyük finansal kuruluşlarından biridir. CIBC, Kanada çapında sertifika otoritesi hizmetlerini sağlamakta ve sertifika işlemlerinin yanısıra pazarlama, satış, güvenlik, müşteri destek ve operasyon yönetimi gibi hizmetleri de sunmaktadır.

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 ya da posta yoluyla başvuru talebini yaparak süreci başlatabiliyorlardı. Bütün

başvuruların müşteri tarafından imzalanmış olması gerektiğinde müşterilerin fornu ya direk şubeden almaları ya da posta yoluyla alıp imzalayıp tekrar geri göndermeleri gerekiyordu. Bu süreci hızlandırmayı ve kolaylaştırmayı amaçlayan CIBC, 2001'in Şubat ayında bireysel banka müşterilerine e-imza kullanarak uygulamaları imzalama ve bütün bankacılık hizmetlerini çevrimiçi olarak alabilme olanağını tanıyan Kanada'daki ilk banka olmuştur [29].

Proje ile, 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.

İngiltere – Barclays

Barclays, temelde bireysel bankacılık, yatırım bankacılığı ve yatırım yönetimi konularında faaliyet gösteren, İngiltere'deki finansal hizmet sunan en büyük gruplardan biridir. Barclays, AAA altyapısını kurması ve işletmesi için BT Ignite ile çalışmaktadır. Güvenlik çözümleri sağlayan bu kurum, e-ticaretin kullanımı sırasında hem Barclays grubu şirketlerini, hem de müşterilerini korumak üzere güvenli teknoloji çözümlerini (AAA) 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 fırsatını sunmuştur [21].

Finlandiya kimlik belgesi projesi

Finlandiya, bilgi ve iletişim teknolojilerinin gelişmişliği ve yaygınlığı ile bilenen ülkelerden biridir. Finlandiya Nüfus Kayıt Merkezi, 2003'ten bu yana akıllı kartlar üzerinde kimlik belgesi projesi yürütmektedir. Yürütülen projede şimdiye kadar birçok kişiye akıllı kartlar üzerinde elektronik sertifika verilmiştir [19].

Danimarka – KPMG

Dünya çapında 152 ülkede 100,000'den fazla çalışanı bulunan KPMG, şirketlere sigorta, vergi, hukuk ve finansal danışmanlık hizmetleri sunmaktadır. KPMG'nin, Danimarka'da ülke çapında 19 ofisinde yaklaşık 1400 çalışanı bulunmaktadır. AAA çözümü öncesinde, çok önemli belgelerin müşteri ile iletişimini normal posta ile gerçekleştiren KPMG, müşteri tarafından gelen internet üzerinden güvenli iletişim talepleriyle karşı karşıya kalması üzerine AAA çözümünü kurarak, müşterileri ile arasında güvenli bilgi alışverişini gerçekleştirmiş ve 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 tamamiyle bütünleşik bir sistem kurmuştur. Verisign sertifikalarının kullanıldığı sistem, KPMG ve müşterileri için güvenlik çözümleri açısından sadece ülke sınırları içerisinde değil, dünyada geçerli bir sistem olmuştur [29].

4.3. Türkiye'de Elektronik İmza'ya İlişkin Mevzuat

Türkiye'de 5070 sayılı E-İmza Kanunu 23 Ocak 2004 tarihli ve 25355 sayılı Resmi Gazete'de yayımlanarak 23 Temmuz 2004 tarihinde yürürlüğe girmiştir. Söz konusu kanun ile Telekomünikasyon Kurumuna (TK) ikincil düzenlemeler ve denetleme yapma görevleri verilmiştir.

Ülkemizde e-imza ile ilgili yasal süreç aşağıda sunulmuştur:

1. 5070 sayılı e-imza kanununun resmi gazetede yayımlanması (23 Ocak 2004),
2. E-imza kanununun uygulanmasına ilişkin usul ve esaslar hakkında yönetmeliğin yayımlanması (06 Ocak 2005, yayımlayan: TK, 1 adet değişiklik yayımlanmıştır),
3. E-imza ile ilgili süreçlere ve teknik kriterlere ilişkin tebliğin yayımlanması (06 Ocak 2005, yayımlayan: TK, 3 adet değişiklik yayımlanmıştır),

4. Sertifika mali sorumluluk sigortası yönetmeliğinin yayımlanması (26 Ağustos 2004, yayımlayan: TK),
5. Zorunlu sertifika mali sorumluluk sigortası genel şartlarının yayımlanması (27 Ocak 2005, yayımlayan: Devlet Bakanlığı),
6. Sertifika mali sorumluluk sigortası tarife ve talimatının yayımlanması (yayımlayan: Devlet Bakanlığı),
7. 2004/21 sayılı Başbakanlık genelgesinin yayımlanması (kamu sertifikasyon merkezi oluşturulması),
8. 2006/13 sayılı başbakanlık genelgesinin yayımlanması (kamu sertifikasyon hizmetlerine ilişkin usul ve esaslar),
9. Güvenli e-imza oluşturma ve doğrulama uygulamaları hakkında TK kararının yayımlanması (01 Haziran 2006, yayımlayan: TK).

Kanuna göre güvenli e-imza;

- Sadece imza sahibine bağlı olan,
- Sadece imza sahibinin tasarrufunda bulunan güvenli e-imza oluşturma aracı ile oluşturulan,
- Nitelikli elektronik sertifikaya (NES) dayanarak imza sahibinin kimliğinin tespitini sağlayan,
- İmzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan elektronik imzadır.

Bu kapsamda oluşturulan güvenli e-imza;

- Elle atılan imza ile aynı hukuki sonucu doğurmaktadır,
- Elle atılan imza ile aynı ispat gücünü haizdir,
- Oluşturulan elektronik veriler senet hükmündedir.

Türkiye'de 5070 sayılı "E-İmza Kanunu" dışında da e-imza kullanımına izin veren, aynı zamanda belli kurumlara e-imza kullanım usul ve esaslarını düzenleme yetkisi tanıyan kanunlar bulunmaktadır. Bu kanunlardan en önemlileri Sermaye Piyasası Kanunu, Vergi Usul Kanunu ve Nüfus Kanunu'dur [32].

4.4. Türkiye'de Elektronik İmza Altyapısı ve Örnek Uygulamalar

Türkiye'de oluşturulacak e-imza altyapısının ülke çıkarlarına ve uygulama kolaylığına hizmet verecek şekilde olabilmesi amacıyla; elektronik sertifika sağlayıcılarının kök anahtarlarının Türkiye'de üretilmiş olması, kamu kurum ve kuruluşlarının tek bir altyapı ve standart altında toplanması, sınırlı kaynakların verimli kullanılması ve yapının tek elden koordinasyonunun sağlanması gerekmektedir. Bu anlamda, konuya ilişkin mevzuat doğrultusunda tüm kamu kurum ve kuruluşlarının kurumsal sertifika ihtiyacının karşılanması için Kamu Sertifikasyon Makamı (Kamu SM) olarak TUBİTAK-UEKAE (Türkiye Bilim ve Teknoloji Araştırma Kurumu - Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü) görevlendirilmiş, yürüttükleri görevler açısından özel niteliği haiz olan Türk Silahlı Kuvvetleri (TSK), Emniyet Genel Müdürlüğü (EGM), Milli İstihbarat Teşkilatı (MİT) Müsteşarlığı, Jandarma Genel Komutanlığı (JGK), Sahil Güvenlik Komutanlığı (SGK) ve Dışişleri Bakanlığı gibi istisnalar dışında kamu kurum ve kuruluşlarının elektronik sertifika ihtiyacının TUBİTAK–UEKAE tarafından karşılanması sağlanmıştır. Özel sektörün ve vatandaşın sertifika ihtiyacının ise yetki verilen özel ESHS'ler tarafından karşılanması ile ilgili yasal düzenleme yapılmıştır.

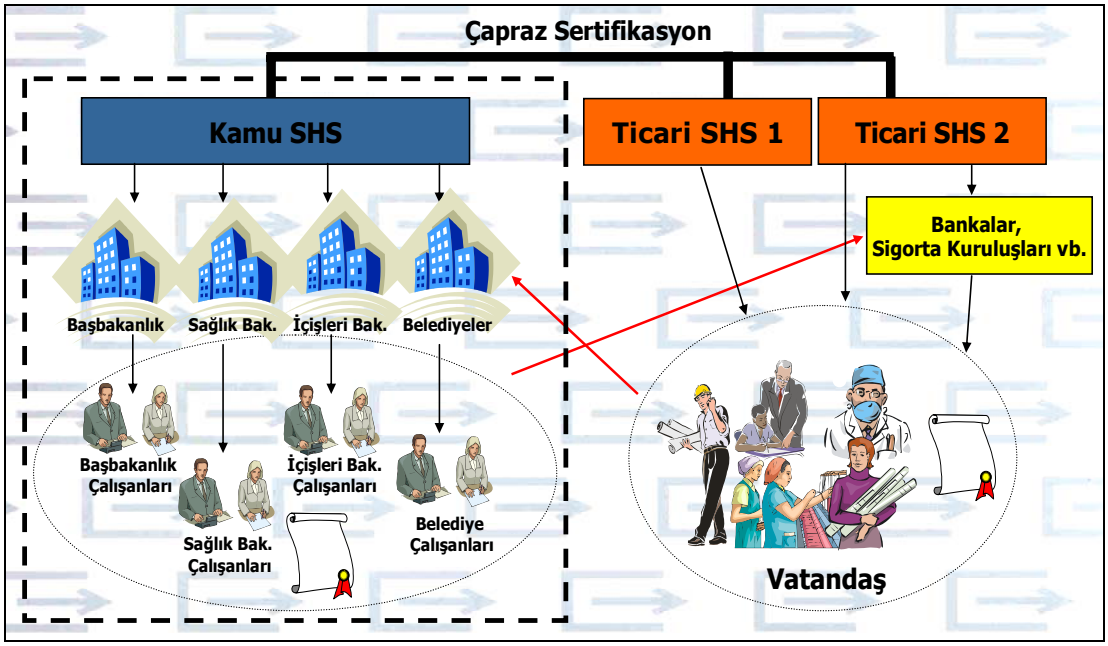
Ülkemizde yapılan yasal düzenlemeler kapsamında, yürüttükleri görevler açısından özel niteliği haiz olan ve yukarıda belirtilen kurumlar kamu sertifika hizmet sistemlerini kendi bünyelerinde oluşturabileceklerdir.

Bu kapsamda, istisnalar dışındaki hiçbir kamu kurumu, elektronik sertifika ihtiyaçlarını karşılamak amacıyla kendi bünyelerinde yeni bir yatırım yapmayacaktır. Kamu kurumları ve çalışanları, bu ihtiyaçlarını Kamu SM'den temin edilecek elektronik sertifikalar ile karşılayacaklardır. Bu konuda daha önceden başlamış olan ve devam eden çalışmalar durdurulacak, halihazırda kullanılmakta olan sistemler ise TK'nun da görüşü alınmak suretiyle en kısa sürede bu yapıya uygun hale getirilecektir [4].

Önümüzdeki zaman içerisinde kademeli bir şekilde, elektronik olarak verilmekte ve verilecek olan kamu hizmetlerinde vatandaşın da e-imzası istenmeye başlanacaktır. Bu hizmetler sadece kamu kurumlarıyla sınırlı değildir. Örneğin bir özel banka da İnternet şubesinden hizmet almak isteyen müşterilerine NES sahibi olma zorunluluğu getirebilir. Vatandaşlar da 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'ya başvurmaları gerekmektedir. Bu kapsamda yapılan başvuru ve yetkilendirmeler sonucunda halen ESHS hizmeti veren kurumlar E-güven Elektronik Bilgi Güvenliği A.Ş. (E-Güven) ve TürkTrust Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. (TürkTrust)'dir. 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. TK'ya ticari ESHS hizmeti vermek üzere başvuracak kurumlar yasa, tebliğ ve yönetmelikte belirtilen şartları sağlamak zorundadır.

Ülkemizde oluşturulan ESHS yapılanması Şekil 4.2'de verilmiştir [33,37]. Ancak bu yapılanmada Kamu ESHS ile Ticari ESHS'ler arasında oluşturulması gereken çapraz sertifikasyon henüz oluşturulmamıştır. Bu konudaki belirsizliğin bir an önce giderilerek Kamu ESHS ile Ticari ESHS'ler arasındaki güven ilişkilerinin net bir şekilde ortaya konulması gerekmektedir.



Şekil 4.2. Türkiye'de ESHS yapılanması

TSK'da yürütülen e-imza çalışmaları

Yürüttükleri görevler açısından özel niteliği haiz olan ve bu duruma yönelik olarak mevzuatta da düzenleme yapılan kurumlardan olan TSK'da, son yıllarda yapılan somut çalışmalar sonucunda AAA ve e-imza uygulamaları hayata geçirilmiştir. Ayrıca kimlik, elektronik cüzdan, sağlık kartı, giriş kartı ve e-imza gibi birçok işlevin tek kartta toplanmasını hedefleyen TSK Akıllı Kart Projesi kapsamında da e-imza çalışmaları yapılmaktadır. Kurum içinde dış dünyadan bağımsız olarak kurulan AAA ve e-imza sisteminde, TUBİTAK–UEKAE tarafından geliştirilen ESYA yazılımları kullanılmaktadır [47].

TSK Akıllı Kart Projesi ile ilgili olarak TSK WEB sitesinden yapılan duyuruya göre (http://www.tsk.mil.tr/guncel/diger_faaliyetler/akillikartbasinduyurusu.htm) sistemde kullanılacak akıllı kartlarını Cenevre sözleşmelerine uyumlu ve merkezi olarak üreten TSK, kartları görevdeki ve emekli personel ile bunların hak sahibi aile fertlerine dağıtmaya başlamıştır. Çoklu işlevlerin tek kartta toplandığı, çağdaş görünümlü ve taklit edilemeyen kartlar, gerek sahip oldukları mikroişlemcileri ve

gerekse görsel özellikleri bakımından en üst düzeyde güvenlik sağlamaktadır. Kartlar, kimlik kartı, giriş kartı, elektronik cüzdan, e-imza ve sağlık kartı gibi işlevleri üzerinde barındırmaktadır.

Kartların sahip olduğu işlevler ve dağıtılacak sayı bakımından dünya orduları arasında sayılı büyük projeler arasında yer alan TSK Akıllı Kart Sistemi, doğru, güncel ve yönetilebilir bilgiye dayalı, tanımlı ve ölçülebilen süreçlere sahip, e-devlet'e geçişin temelini oluşturan, birlikte çalışabilirlik esaslarına uygun bir yapıda geliştirilmiştir. Sistem, Türkiye'de yakın bir gelecekte yaygın bir kullanım alanı bulacak e-imza, kimlik ve sağlık kartı gibi uygulamalar için de bir ilk olma özelliği taşımaktadır.

Dış Ticaret Müsteşarlığı - dahilde işleme rejimi projesi

Dış Ticaret Müsteşarlığı'nın (DTM) Dahilde İşleme Rejimi (DİR) projesi, Türkiye çapında 13 ihracatçı birliğine mensup 5000'den fazla firmanın, birlik kullanıcılarının, gümrük kapılarındaki kullanıcıların ve DTM uzmanlarının kullanıcısı olduğu bir sistem olarak hayata geçirilmiştir. Bu proje ile, dahilde işleme izin belgelerinin DTM'ye ulaştırılması ve onaylarının alınması sürecinde yaşanan bürokratik gecikmeler en aza indirilmiştir. Proje ile, belge başvurusunda bulunacak olan şirket, başvurusunu internet aracılığı ile elektronik ortamdan yapabilmekte ve başvuru sonucunu yine elektronik ortamda takip edebilmektedir. Ayrıca şirketin başvurusundan sonra DTM içerisindeki iş akışı da yine elektronik ortamda gerçekleştirilmektedir. Elektronik ortamdaki bu iş akışına katılan şirket ve DTM kullanıcıları, kimliklerini güçlü bir şekilde doğrulayarak sisteme girmek için kendileri için özel olarak kişiselleştirilen akıllı kartlarını kullanmaktadırlar. Elektronik işlemlerde bütünlük ve inkâr edememe hizmetleri de uygulamaya dahil edilen e-imza işlevleri ile sağlanmaktadır [5].

Bu proje Türkiye'de AAA ve e-imza kullanımı ile vatandaşa hizmet veren ilk projedir. Eylül 2003'te başlayan proje Ağustos 2005 itibarıyla uygulamaya açılmıştır.

2004 yılındaki verilere göre 4 bin 968 adet dahilde işleme izin belgesi düzenlenmiştir. Bu belgelerin toplam ihracat taahhüdü 33.7 milyar dolardır. Bu rakam genel ihracatın yüzde 53.7'sine karşılık gelmektedir. Bir dahilde işleme belgesinin düzenlenmesi revizesi ve kapatma işlemleri için ortalama 450 adet kağıt kullanılmaktadır. 2004 yılında sadece dahilde işleme izin belgeleri için 2.3 milyon civarında kağıt kullanılmıştır ve bu da yaklaşık olarak 1127 ton veya 112 kamyon kağıt anlamına gelmektedir.

Projenin hayata geçmesi ile DTM, zaman tasarrufu sağlama, maddi tasarruf sağlama, karar süreçlerini hızlandırma, yapılan işlemlerin takibini yapma, ölçme, değerlendirme, elektronik evrak akışı ve arşiv gibi kazanımlarla iş yükünü hafifletmiştir. Yapılmış ve yapılacak olan ihracat ve ithalat ile ilgili her türlü bilgiye merkezden eş zamanlı erişim sağlanmıştır.

Emeklilik işlemlerinde e-imza kullanımı

Emekli Sandığı Genel Müdürlüğü, çalışanların prim günlerinin takibini sağlayacak, "Emeklilik İşlemlerinin On-Line Yürütülmesi Projesi"ni hayata geçirmektedir. Genel Müdürlük, e-imza ile desteklenecek olan bu proje ile primlerin olduğundan daha fazla gösterilmesi gibi usulsüzlükleri ortadan kaldırmayı amaçlamaktadır. Borcu en yüksek sosyal güvenlik kurumu olarak gündeme gelen Emekli Sandığı, proje ile alacaklarını tahsil etmeyi ve borçlarını azaltmayı hedeflemektedir.

2007 yılı içinde hayata geçirilmesi hedeflenen projenin son aşamasında, e-imza desteği ile kurumlarca sandığa gönderilen emeklilik onayını elektronik ortama taşıyacak altyapı da oluşturulacaktır. Emekli olmak isteyen kişi, kurumuna başvurduğunda bu durum sandığa e-imzalı olarak iletilecek ve aylık bağlama işlemine hemen başlanılacaktır. İşlemlerdeki kırtasiye ve zaman kaybı önlenecektir.

İçişleri Bakanlığı - il özel idareleri analitik bütçe ve muhasebe sistemi

Ülkemizdeki tüm il ve ilçelerin analitik bütçe ve muhasebe işlemleri, internet tabanlı bir yazılım aracılığıyla İçişleri Bakanlığı sistemlerinde çalışmaktadır. İl ve ilçe özel idare personelinin kullanımı için geliştirilen proje ile bütün özel idarelerin bütçe ve muhasebe işlemlerinin tek merkezde yapılabilmesi, yasa gereği yıllık konsolidasyonların kolayca yapılabilmesi ve analitik bütçe uygulamalarında bir bütünlük sağlanması hedeflenmiştir. Proje 26 Mayıs 2005'te uygulamaya geçmiş olup kullanıcı sayısı 1800'dür. İnternet tabanlı olan uygulama e-imza fonksiyonunu da içermektedir [45].

Gümrük sektöründe e-imza kullanımı

Ankara ve İstanbul Gümrük Müşavirleri Derneği, 1 Ocak 2006'dan itibaren Dahilde İşleme Rejimi (DİR) Otomasyon Projesi kapsamında ihracat izin belgeleriyle ilgili işlemlerde kullanılması zorunlu olan 'e-imza' alanında üyelerine en uygun koşullarla hizmet sağlayabilmek için TürkTrust ile 14 Aralık 2005 tarihinde işbirliği yaparak e-imza kullanımına başlamışlardır.

İSKİ'nin e-imzaya geçiş çalışmaları

E-devlet çalışmalarını sürdüren kurumlardan İstanbul Su ve Kanalizasyon İdaresi (İSKİ)'nin, abone sisteminde e-imzaya geçiş çalışmaları devam etmektedir. Düzenlemeyle birlikte e-imza sahipleri, İSKİ müdürlüklerine gitmeye gerek duymadan, mukavelelerini ıslak imzaya eşdeğer nitelikteki e-imza ile onaylayabilecekler. Vatandaşların bu yenilikten faydalanmaları için herhangi bir ulusal ESHS'den alınmış geçerli bir NES bulundurmaları yeterli olacaktır. Yeniliğin, 4 milyon İSKİ abonesine hem kolaylık hem de zamandan ve ulaşım ücretinden tasarruf olanağı sağlaması beklenmektedir. Kurumda, abonelere yönelik yeniliklerin yanısıra, 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 [47].

Dış Ticaret Müsteşarlığı - doküman yönetimi ve iş akış sistemi

DTM doküman yönetimi ve iş akış sistemi projesi, kurum çalışanları ve vatandaşlara yönelik olarak hazırlanmıştır. İş akışları ve dokümantasyonun elektronik ortamda güvenli bir şekilde yönetiminin hedeflendiği projede e-imza kullanımı da sağlanacaktır [45].

Doğal gaz sektöründe e-imza uygulaması (Zetacad Projesi)

2006 yılı Haziran ayı içinde TürkTrust ve Tekhnelogos firmalarının işbirliği ile gerçekleştirilen Zetacad projesi ile, ülkemizde e-imza doğal gaz sektöründe ilk defa uygulanmaya başlanmıştır. Zetacad isimli "Doğalgaz Projesi Tasarım Yazılımı"na gerçekleştirilen e-imza entegrasyonu sayesinde doğalgaz sektöründe projeleri çizen mühendisler ve onaylayan gaz dağıtım şirketlerinin yetkilileri e-imza kullanmaya başlamışlardır. 2006 yılı sonuna kadar en az 10 ile yaygınlaşacak olan bu projenin 1000'in üzerinde kullanıcıya ulaşması beklenmektedir. Özellikle büyük şehirlerdeki gaz dağıtım şirketlerinin ve doğal gaz projesi çizen mühendislerin de e-imza uygulamasına geçmesiyle, kullanıcısı sayısının 5000'i geçeceği tahmin edilmektedir.

E-imzalı dijital proje yönetim yazılımı sayesinde önemli miktarlarda tasarruf sağlanmakta ve proje onay süreçleri çok hızlanmaktadır. Türk mühendislerince gerçekleştiren bu uygulama, doğalgaz projelerinin çiziminden, onayına, tadilat işlemlerinden arşivlenmesine kadar tüm işlemlerin e-imzalı yapılabilmesini sağlamaktadır.

Koçbank e-imzalı e-posta bankacılığı uygulaması

E-imzalı e-posta bankacılığı, banka müşterilerinin havale, EFT ve buna benzer işlem

talimatlarını şubelerine faks ya da telefon yerine e-imzalı e-posta aracılığıyla ulaştırdıkları bir sistemdir. Koçbank'ın sağladığı bu hizmet ile, müşteriler tarafından gönderilen e-postalar, müşterinin talebine göre Koçbank yada E-Güven tarafından verilmiş olan elektronik sertifikalar ile imzalı olarak gönderilmektedir. Geçerli talimatlar, müşterinin bağlı olduğu şubenin sistemine aktarılarak işlemin gerçekleştirilmesi sağlanmaktadır.

TÜBİTAK-UEKAE KBYS sisteminde e-imza kullanımı

TÜBİTAK-UEKAE, kendi geliştirdiği Kurumsal Bilgi Yönetim Sistemi (KBYS) üzerinde kanuna uygun e-imza kullanımı için çalışmalarını sürdürmektedir. Sistemde ilk olarak 5018 sayılı kanunla iş yükü artan Satınalma ve Genel Harcama Talimatı Sistemi e-imzaya uyumlu hale getirilecektir. Pilot çalışma ile, TÜBİTAK-UEKAE'nin Satınalma Birimi'nde kağıt trafiğinin azaltılması ve verimlilik artışı hedeflenmektedir. E-imza, zamanla diğer KBYS bileşenlerine entegre edilecektir [47].

İçişleri Bakanlığı e-bakanlık projesi

Kurum çalışanları, kamu kurum ve kuruluşları, valilikler, kaymakamlıklar, iş dünyası ve vatandaşlara yönelik hazırlanan projenin öncelikli amacı kurumsal uygulamaların e-dönüşümünün sağlanmasıdır. Proje kapsamında öncelikle e-devlet hizmetlerinin kolay sunulabileceği teknolojik alt yapı ve yazılımların tamamlanması düşünülmüştür. 26 Mayıs 2005'te başlatılan projenin 2006 yılı son çeyreğinde tamamlanması proje takvimine bağlanmıştır. Proje kapsamında tüm yazılımlarda sisteme giriş ve işlem yapabilmek için e-imza kullanılacaktır [45].

E-ihale çalışmaları

Türkiye Odalar Borsalar Birliği (TOBB), Ekonomi ve Teknoloji Üniversitesi (ETÜ) ve Kamu İhale Kurumu (KİK) arasında 27 Eylül 2005 tarihinde imzalanan protokol

kapsamında, kamu ihalelerinin daha açık, şeffaf ve geniş kitlelere duyurulabilecek şekilde yapılabilmesi için, TOBB ve ETÜ, KİK'e altyapı desteği verecektir. bu kapsamda KİK, e-ihale sürecinin altyapı çalışmalarını tamamlamayı amaçlamaktadır.

Türkiye'de yaklaşık 36 bin kamu kuruluşu, her yıl değişik ihaleler açmakta ve buna 87 bin civarında şirket katılmaktadır. Yapılan ihalelerin yaklaşık bedeli ise 40 milyar doları bulmaktadır. Ancak ihalelerin yeterince duyurulmaması veya 'eksik belge' nedeniyle yarışmalara katılımın tam sağlanamamaktadır. İhalelerin açık ve şeffaf olmasıyla ve geniş şekilde duyurulmasıyla %10 tasarruf sağlansa, bu 4 milyar dolar anlamına gelmektedir. Bu çok önemli rakamlardan da tüm Türk halkı kazançlı çıkacaktır.

Adalet Bakanlığı - ulusal yargı ağı projesi

Kullanıcı grubu Adalet Bakanlığı merkez ve taşra birimleri ile iş dünyası ve vatandaşlar olan Ulusal Yargı Ağı Projesi (UYAP) ile, tüm yargı birimlerini kapsayan otomasyon ve dış birimlerle entegrasyonu sağlamak suretiyle yargılama sırasında usul hatalarının önlenmesi ve diğer hataların en aza indirilmesi, yargılamanın sağlıklı ve süratli bir şekilde gerçekleştirilmesi ve adalete daha da fazla güven kazandırılması hedeflenmektedir.

Hedeflenen sistem kurulduğunda, dava adliyeye intikal ettiği andan itibaren elektronik ortama geçecek, tekrarlardan kaçınılacak, Cumhuriyet Savcılığı'ndan girilen bilgiler mahkeme aşamasında tekrar bilgisayara girilmeyecektir. Üst mahkemeye gidiş, üst mahkemeden dönüş, kesinleşme, ilamat, cezanın infazı ve adli sicile intikali aşamasına kadar tüm evreler bilgisayar ortamında gerçekleşecektir. Projenin elektronik belge akışı ve arşivleme düzeninde e-imza fonksiyonları kullanılacaktır [45].

Türkiye noterler birliği e-imza çalışmaları

Türkiye Noterler Birliği (TNB), e-imza ile ilgili çalışmalarına 2001 yılı Ocak ayı itibarı ile başlamış olup, 2003 yılında başlatılan bir proje ile yönetim kurulunun e-imza güvenliği altında yönetim kurulu toplantılarını internet üzerinden de yapabilmesi sağlanmış, bu kapsamda evrak akışı ve karar süreçlerini de kapsayan pilot bir e-imza uygulaması başlamıştır [21].

Kamuyu aydınlatma projesi

İstanbul Menkul Kıymetler Borsası'nda (İMKB) işlem gören şirketler ile aracı kuruluşlar, sermaye piyasası ve Sermaye Piyasası Kurulu (SPK) mevzuatında belirlenen mali tabloları, tanımlanan aralıklar içinde kamuya açıklamak zorundadırlar [45]. Mali tablolar ve özel durum açıklamaları, halen yürürlükte olan uygulama dahilinde disketle ve son durumda mutlaka basılı bir biçimde kağıt çıktılarla SPK ve İMKB'ye gönderilmektedir. Bu uygulamada, bilgilerin sisteme ulaşması ve işlenmek üzere veri tabanına kaydedilmesi süreçleri, zaman ve işgücü kaybına yol açmakta; hata ve tekrarlardan doğan maliyet artışları ortaya çıkmaktadır. Kamuyu Aydınlatma Projesi (KAP), sermaye piyasalarında işlem gören ve halka açık şirketlerin ve aracı kuruluşların kamuyu aydınlatma amacı ile bilanço ve mali tablolarına ilişkin olarak yapacakları bildirimler ile özel durum açıklamaları ve diğer tipindeki bildirimlerin bilgisayar ağları üzerinden e-imza teknolojisi kullanılarak güvenli bir şekilde iletilmesini hedeflemektedir. Bu şekilde, mevcut uygulamada karşılaşılan zaman ve işgücü kaybı, hata ve tekrarlardan doğan maliyet artışları gibi olumsuzlukların ortadan kaldırılması mümkün olacaktır. KAP, SPK ve İMKB tarafından ortaklaşa gerçekleştirilmiştir [5].

KAP, bir e-devlet uygulamasında olması gereken tüm unsurları (Devlet: SPK, Şirket: KAP şirketleri, Vatandaş: sermaye piyasası yatırımcısı) içermesi sebebiyle, tam bir e-devlet uygulaması olarak SPK'nın AB sürecinde attığı önemli bilişim yatırımlarından birisi olarak durmaktadır. Coğrafi olarak tüm Türkiye'ye yayılmış

540'ü aşkın şirketi ve 2500'ü aşkın kullanıcıyı kapsamaktadır. Proje kapsamında 4 büyük ilde (Ankara, İstanbul, İzmir ve Adana) yaklaşık 500 şirkete KAP konusunda eğitimler verilmiş ve yaklaşık 2200 akıllı kart dağıtılmıştır. Projenin 2006 yılında tamamlanması hedeflenmektedir [5,45].

Toplu Konut İdaresi Başkanlığı - arşiv ve doküman yönetim sistemi

Toplu Konut İdaresi Başkanlığı (TOKİ) çalışanları ve vatandaşlara yönelik olarak geliştirilen arşiv ve doküman yinetim sisteminin amacı; kurum arşivinin elektronik ortama aktarılması ve kurum içi evrak dolaşımının e-imzalı olarak yine elektronik ortamda kurumun ve vatandaşların hizmetine sunulmasıdır. Sistemin arşiv bölümü 2005 yılı başında tamamlanmış ve kurum çalışanlarının hizmetine sunulmuş olup arşiv evraklarına elektronik ortamda erişilebilmektedir [45].

Merkezi Kayıt Kuruluşu bilgi güvenliği ve sertifika hizmetleri uygulama projesi

Aracı kuruluşların, yatırımcıların bilgisi dışında yatırımcı adına işlem yapmasını engellemek ve yatırımcıların sermaye piyasalarına olan güvenini arttırmak amacıyla, Merkezi Kayıt Kuruluşu, internet üzerinden gerçekleştireceği bir uygulamada bilgi güvenliğinin elektronik sertifika ve e-imza teknolojileriyle sağlanmasını planlamıştır. Uygulama kapsamındaki kullanıcılara elektronik sertifika verilmesi ve ilgili hizmetlerin yürütülmesi işini Tübitak-BİLTEN gerçekleştirecektir [21].

Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü - kimlik paylaşım sistemi

İlgili kamu kurum ve kuruluşlarının kullanımı için hazırlanan ve kamu kurum ve kuruluşlarının vatandaşların elektronik ortamdaki kimlik bilgilerine ihtiyaç duyulduğunda, gerektiği kadar, doğrudan ve hızlı bir biçimde erişimlerinin sağlanması için tasarlanan proje 23 Şubat 2005 tarihinde hizmete açılmıştır. Projede, alıcı kurumlar açısından aktarılan bilgilerin resmiliğini sağlamak maksadıyla, e-imza ve benzeri güvenlik unsurlarının azami düzeyde kullanımı hedeflenmektedir [45].

Denizbank açık anahtar altyapısı projesi

Kurumsal müşterilere internet bankacılığı hizmetini daha güvenli sunmak amacıyla Denizbank bünyesinde bir AAA sistemi geliştirilmiştir. Web üzerinden kimlik doğrulama işleminin akıllı kartlarla yapıldıgı bu sistemde Gemplus'ın akıllı kartları ile Todos akıllı kart okuyucuları kullanılmıştır. Microsoft Sertifika Otoritesi yazılımı kurum içerisindeki sertifikaların yaratılması, dağıtımı ve iptal edilmesi işlemlerini gerçekleştirmektedir [21].

Telif Hakları ve Sinema Genel Müdürlüğü'nün e-imza projesi

Telif Hakları ve Sinema Genel Müdürlüğü, "Korsanlıkla Mücadele Kapsamında Fikri Mülkiyet Sisteminin Güçlendirilmesi" başlıklı proje ile "Bilgi Yönetimi Projesi"nde gerçekleştirdiği tüm yazılım modüllerinin AB standartlarına göre geliştirilmesi, güncellenmesi ve entegrasyonu; sistemin gerektirdiği donanımın sağlanması ile evrak akış ve belge yönetimi sistemi, e-imza, akıllı raporlama sistemi, internet portalı ve e-eğitim çözümlerini sağlamış olacaktır [45].

NETSİS ürünlerine e-imza entegrasyonu

Kurumsal kaynak planlaması yazılımı geliştirici markalarından NETSİS, ürünlerine e-imza entegre edilmesi konusunda TürkTrust ile yaptığı işbirliğinin sonucu olarak özellikle e-posta ve iş akış onay süreçlerine e-imza uygulamalarını yaygın olarak kullanmayı hedeflemektedir.

İller Bankası Genel Müdürlüğü - iller bankası bilgi sistemi (İL-BİS)

İller Bankası İL-BİS Projesi ile merkez ve bölge müdürlüklerine intranet üzerinden, belediyelere ise internet üzerinden bilgi ve veri bankası hizmetleri sağlanacaktır. Projenin tamamlanmasıyla bilgi akışı tamamen sayısal ortamda yapılacaktır. Böylece bölgeler ve yerel yönetimler arasındaki iletişim internet ortamında olacağından

işlemler hızlandırılmış olacak, AAA ve e-imza kullanılarak bürokrasi en alt seviyeye çekilecektir. Proje ile, Genel Müdürlük ve 18 Bölge Müdürlüğü arasında intranet (Geniş Alan Ağı, Wide Area Network-WAN) bağlantısı kurularak çevrimiçi bağlantı sağlanacak ve Türkiye genelindeki 3225 adet yerel yönetim internet üzerinden bilgi ve veri bankası hizmetlerine ulaşabilecektir [45].

Docuart elektronik doküman yönetim sistemi

Docuart tarafından geliştirilen EDYS, kağıt ortamında bulunan dokümanları elektronik belge haline dönüştürmek, dönüştürülen belgelerin ve mevcut belgelerin tanımlanan iş akışları ile dolaşımını yönetmek, bu belgeleri doküman ambarları içerisinde güvenli bir şekilde saklamak ve belge ve bilgi kaynaklarına hızlı ve etkin ulaşım sağlamak amacı ile ISO Kalite standartlarında ve T.C. Evrak Dolaşım Yönergeleri'ne uygun olarak üretilmiştir.

Sistemin e-imza entegrasyonu ile kurum içi ve kurumlar arasındaki yazışmalarda güvenli e-imza kullanılarak belgelerin değişmezliği ve inkar edilemezliği sağlanmaktadır.

Gümrük Müsteşarlığı – BİLGE EDI projesi

Kullanıcı grubu iş dünyası olan proje çerçevesinde yükümlülerin hem internet hem de Elektronik Veri Değişimi (Electronic Data Interchange - EDI) yöntemiyle gümrüğe gelmeksizin kendi bürolarından BİLGE sistemine erişerek beyanname tescil etmeleri imkanı sağlanmıştır. EDI sistemiyle verilerini farklı formatta saklayan kullanıcılar arasında veri iletişimi mümkün kılınmıştır. Gümrük Müsteşarlığının kendi mevzuatında düzenleme yaparak zaten asgariyeye indirdiği fiziksel olarak yükümlülerin idareye uğraması olayı, e-imza uygulaması ile tümüyle ortadan kaldırılacaktır. EDI uygulaması ile toplam ithalat ve ihracat beyannameleri içinde elektronik yolla tescil işlemi % 65 düzeyine erişmiştir [45].

5. KURUMSAL AĞLAR İÇİN ELEKTRONİK İMZA UYGULAMASI

Bu bölümde kurumsal ağlarda e-imzaya geçişte dikkat edilmesi gereken hususlar ve takip edilmesi gereken işlem adımları sırasıyla sunulmuş ve Gazi Üniversitesi'nde gerçekleştirilen örnek uygulama kapsamında kurumsal ağlarda e-imza uygulamaları için gereksinimlerin belirlenmesi, analiz, tasarım, gerçekleştirim ve test aşamaları detaylı olarak anlatılmıştır.

5.1. Kurumsal Ağlarda E-İmza Uygulamalarının Hayata Geçirilmesinde ve Yaygınlaştırılmasında Dikkat Edilmesi Gereken Hususlar

Kağıt üzerinde işleyen bir sistemi elektronik ortama geçirmek, elektronik ortamdaki bir uygulamaya e-imza ile ilgili özellikleri dahil etmek ciddi yatırımlardır. E-imza teknolojilerinde istenmeyen sonuçlarla karşılaşmamak, iyi belirlenen ve dikkatli uygulanan politikalarla mümkündür. Bu nedenle, kurumsal ağlarda e-imza uygulamalarının başarı ile hayata geçirilebilmesi ve yaygınlaştırılabilmesi için aşağıdaki hususlara dikkat edilmelidir:

- Kurumsal ağlarda e-imza uygulamaları ilk seferde mutlaka kapsam ve amacı açısından sınırlı pilot uygulamalar biçiminde tasarlanmalıdır. Pilot uygulamalardan olumlu sonuçlar alındıkça kapsam genişletilmelidir.
- Bilgi eksikliğinden doğan tereddütler ve başarısız örnekler, kullanıcıları olumsuz yönde etkilemektedir. Bu nedenle kurumsal ağlarda en iyi örneği oluşturmak için, öncelikle kendi içinde kalan iş akışlarında, sonra diğer kurumsal ağlarla ilişkilerinde ve son olarak vatandaşlarla ilişkilerinde e-imzaya geçiş planlanmalı ve uygulanmalıdır.
- Diğer kurumsal ağlar ve vatandaşlarla olan ilişkilerde e-imzaya geçişin sağlıklı olarak gerçeklenebilmesi için, iletişim içinde olunan kurumlarla gerekli koordinasyon yapılmalı ve uygulamalar arasında uyum sağlanmalıdır.
- E-imza kendi kendisinin amacı değil, belirlenmiş bir ihtiyacı karşılamak üzere geliştirilen bir elektronik uygulamada güvenliğin sağlanmasının aracı

olmalıdır. Bu nedenle kurumsal ağlarda e-imza yeteneğinin sağlanması, mevcut uygulamalara e-imza desteğinin eklenmesi veya mevcut uygulamaların e-imza desteği bulunan uygulamalarla değiştirilmesi olarak algılanmalıdır.

- E-imzanın bir araç olduğu asla akıldan çıkarılmamalıdır. Belirli bir uygulamayla ilişkilendirilmediği sürece, bir e-imza projesinden söz etmek anlamlı değildir. E-imza teknolojilerinde istenmeyen sonuçlarla karşılaşmamak, iyi belirlenen ve dikkatli uygulanan politikalarla mümkündür.
- Kurumsal ağlarda e-imza yeteneğinin kazandırılması için öncelikle kurum çalışanlarının bilgisayar yetkinliği artırılmalıdır.
- E-imzanın kurumda yaygınlaştırılmasını sağlamak için öncelikle kurum çalışanlarının e-imzanın ne olduğunu kavramaları ve elektronik yaşamla birlikte e-imza kullanımının hayatlarına getireceği kolaylıkları fark etmeleri gerekmektedir. Bu amaçla kurum içi etkinliklerin düzenlenmesi veya kurum dışı etkinliklere katılım sağlanması ile kurum çalışanlarının e-imza konusundaki bilgileri artırılmalıdır. Özellikle sertifika sahipleri sistemin işleyişi hakkında sağlıklı bilgilendirilmelidir.
- Kurum içinde e-imza uygulamaları devreye girdikçe, kullanıcıların e-imza ile ilgili soru ve sorunlarına çözüm getirecek bir çağrı merkezi oluşturulmalıdır. Böylelikle kullanıcıların alışılmış iş düzenleri dışında hayatlarına giren yeni bir teknolojiye karşı gösterecekleri direnç kırılmalıdır.
- E-imza desteği sağlanan uygulamalar karmaşık ve anlaşılması zor olarak tasarlanmamalı, konunun kullanılması kolaylaştırılmalı ve bu konuda kullanıcılara yardımcı olunmalıdır. Uygulamada ve standartlarda kullanıcı işlemleri uzatılmamalıdır.
- E-imza uygulamalarında maliyetler ve sorunlar olabildiğince minimum seviyelere çekilmelidir. Konunun uygulanabilmesi için kurum için özel politikalar belirlenmeli, bu konuda kurumlar arası ilişkiler netleştirilmelidir. Oluşturulan standartların uygulanması için sınırlayıcı olmadan zorlayıcı tedbirler alınmalı ve gerek duyuldukça denetleme mekanizmaları oluşturulmalıdır.
- E-imza uygulamalarını devreye alabilmek için, öncelikle yöneticiler bazında bir bilgilendirmenin düzenli bir şekilde yapılması gereklidir.

- Teknik yönden problemler aşılsa bile, idari olarak kamu kurumu yöneticilerinde ve çalışanlarında yıllar boyu oluşmuş ve değişime dirençli iş yapma yaklaşımları, e-imzanın yaygınlaşmasında ve kurumlar tarafından kullanımına geçilmesinde en önemli engel olarak görülmektedir. Bu yaklaşımların mümkün olduğunca hızlı bir şekilde değiştirilmesi sağlanmalıdır. E-imza teknolojisinin devlete ve çalışma verimine getireceği yararlar, kurum çalışanlarının anlayabileceği örneklerle anlatılmalıdır. Bu şekilde değişime direncin kırılması sağlanmalıdır.
- Kurum, yapacağı yatırımlarda mevzuatın getirdiği e-imza ihtiyaçlarını da göz önünde bulundurmalı ve ihale şartnamelerini buna uygun hazırlamalıdır.
- Özellikle uygulamalar arası entegrasyonun sağlanması amacıyla, henüz geliştirme aşamasında olan XML tabanlı standartlar olgunlaşana kadar (XML sayısal imza, XML sertifikaları, vs.), bir işlemin tüm adımlarında tek seferde bir uygulamaya gitmekten kaçınılmalıdır. Bunun yerine, örneğin önce vergi beyannamelerinin gönderilmesi, ardından ödeme işlemlerinin e-imzaya dayalı yapılması düşünülmelidir.
- E-imza uygulamalarıyla birlikte en önemli tasarrufun kırtasiye (kağıt tüketiminde) kaleminde olduğu ortaya çıkmıştır. Bu itibarla kurum bütçesinde kırtasiye (kağıt alımı) için ayrılan paranın belli bir yüzdesi e-imza uygulamalarının yaygınlaştırılması için kullanılabilir.

5.2. Elektronik İmza Başvuru İşlemleri

Türkiye'de e-imza için gerekli sertifika satışları 18 Temmuz 2005 tarihinden itibaren fiilen başlamıştır. Kamu kurumlarının bu konudaki ihtiyacını Kamu SM olarak görevlendirilen TÜBİTAK-UEKAE karşılarken; TürkTrust ile E-Güven ise özel kişi ve kuruluşlara e-imza satışı gerçekleştirmektedir.

ESHS'lerden NES almaya yönelik başvuru işlemleri ve gerekli belgeler söz konusu ESHS'lerin web sayfalarında detaylı olarak açıklanmıştır. Bu kapsamda TurkTrust'a yapılacak NES başvuruları, TurkTrust ofislerine bireysel başvuru, TurkTrust yetkililerinin kuruma gelmesi veya noter kanalıyla yapılabilmektedir. E-Güven'e

yapılacak NES başvuruları ise anlaşmalı bankalar vasıtasıyla yapılabilmektedir.

Kamu kurumlarına sertifika hizmeti verecek olan Kamu SM'den NES almaya yönelik başvuru işlemleri ile diğer NES işlemleri de, tez çalışması kapsamında Gazi Üniversitesi'nde simule edilen örnek uygulama ile ilişkili olarak bu bölümde detaylı olarak açıklanmıştır [47]:

Kurumsal başvuru işlemleri

Kamu SM elektronik sertifika başvurularını kurumsal olarak almaktadır. Kamu veya özel kurum çalışanları NES başvurularını bağlı bulundukları kurum aracılığı ile Kamu SM'ye yaparlar. Kamu SM tarafından kişisel sertifika başvuruları kabul edilmemektedir.

Kamu SM'den NES talebinde bulunan kurumların öncelikli olarak e-imza kullanımına dair gereken uygulama ortamlarını hazırlamış, e-imza oluşturma ve doğrulama işlemlerini mevzuata göre gerçekleştirmiş olması gerekmektedir. Başvuru işlemleri sırasında tüm yazışmaların posta yolu ile yapılması ve yazıların kurum yetkilisi tarafından imzalı ve kurum onaylı olması gerekmektedir. Kurumlar, Kamu SM NES hizmetlerinden faydalanabilmek için aşağıdaki 6 adımı takip ederek başvurularını yaparlar:

1. ADIM 1-Kurumun resmi yazı ile Kamu SM'ye başvurması

Kurum, Kamu SM'ye resmi yazı ile başvurur. Resmi yazı içeriğinde kurum, ihtiyaç duyduğu hizmetler için kendisine teklif gönderilmesini ister. Kurumun ihtiyaçları doğrultusunda resmi yazıda bulunması beklenen bilgiler aşağıdaki gibidir:

- Talep edilen NES sayısı,
- Talep edilen akıllı kart okuyucusu miktarı ve türü,
- Sertifikaların kullanılacağı uygulamanın veya projenin kısa tanımı.

Kurum, e-imza yazılım kütüphanesi de talep ediyorsa bununla ilgili aşağıdaki bilgiler resmi yazı içeriğinde bulunur:

- Talep edilen yazılım kütüphanesi (Java ve/veya .NET),
- Yazılım kütüphaneleri proje başına lisanslandırıldığından, kütüphanenin kullanılacağı proje sayısı.

Resmi yazı kurum tarafından posta ile Kamu SM'ye gönderilir.

2. ADIM 2-Kurumsal başvurunun değerlendirilmesi

Resmi yazıya istinaden Kamu SM, kurumla iletişime geçerek kurumun ihtiyacını değerlendirmeye alır. Değerlendirme kurumun NES kullanımına ilişkin gerekli altyapıya sahip olduğunun belirlenmesi yoluyla yapılır. Bu amaçla kuruma "E-İmza Uyumu Analiz Formu" e-posta ile gönderilerek, formun doldurulup Kamu SM'ye iletilmesi istenir. Formda verilen bilgiler doğrultusunda kurumun e-imza altyapısına sahip olup olmadığının değerlendirmesi Kamu SM tarafından yapılır.

"E-İmza Uyumu Analiz Formu" içeriğinde kurum iletişim noktası bilgileri de yer alır. Kurum iletişim noktası, sertifika başvuru ve dağıtımında kurum ile ortak yürütülecek adımlarda Kamu SM ile koordineli çalışacak bir kurum çalışanı olmalıdır.

Sertifika kullanımıyla ilgili hazırlıkları tamamlamamış olan kurumların başvurusu olumsuz değerlendirilir ve ADIM 3'e geçilir. Hazırlıklarını tamamlamış kurumların başvurusu olumlu değerlendirilir ve ADIM 4'e geçilir.

3. ADIM 3-Kurumun bilgilendirilmesi

Kamu SM, kurumu olumsuz bulunan başvurular ve olumsuzluk sebebi konusunda resmi yazı ile bilgilendirir. Kurum bilgilendirmeyi aldıktan sonra gerekli hazırlıkları

tamamlayarak yeniden kurumsal başvuruda bulunmak üzere ADIM 1'e geri döner.

4. ADIM 4-Kamu SM tarafından kuruma teklif yazısı gönderilmesi

Geçerli bulunan başvurunun ardından, Kamu SM kendisinden talep edilen hizmetlerin ücretlerinin ve hizmetin veriliş biçiminin belirtildiği ilgili teklif yazılarını kuruma gönderir. NES ve akıllı kart okuyucusu tekliflerinin ekinde "Kurum Sipariş Formu" da kuruma gönderilir.

5. ADIM 5-Kurum tarafından Kamu SM'ye sipariş yazısı gönderilmesi

Kurum teklifleri kabul ettiğine dair resmi yazıyı Kamu SM'ye gönderir. NES ve akıllı kart okuyucusu siparişleri için resmi yazı ekinde "Kurum Sipariş Formu" da Kamu SM'ye gönderilir. Sipariş yazısı Kamu SM'nin eline geçtikten sonra talep edilen ürün ve hizmetler kuruma sağlanır.

Sipariş formu içeriğinde NES başvurusunda bulunulan tüm kurum çalışanlarının ad, soyad ve T.C. kimlik numaralarının belirtilmesi gerekmektedir. Ayrıca bu bilgilerin kurum iletişim noktası tarafından elektronik ortamda NES_Basvuru@kamusm.gov.tr adresine de gönderilmesi işlemlerin hızlı yürütülmesi için gereklidir.

6. ADIM 6-Kamu SM ile kurum arasında sertifika temini sözleşmesinin imzalanması

Kamu SM, NES hizmetlerinin ücretlerinin ve hizmetin veriliş biçiminin belirtildiği NES Temini Sözleşmesi'ni kuruma gönderir. Sertifika üretim işlemleri kurum ile Kamu SM arasında sözleşmenin karşılıklı imzalanmasının ardından başlatılır.

Nitelikli elektronik sertifika başvuruları

Kamu SM tarafından bu sürecin işletilebilmesi için, ön koşul olarak yukarıda anlatılan kurumsal başvurunun Kamu SM'ye yapılmış, kurum ile sözleşme imzalanmış olması gerekir. Prosedür aşağıdaki 3 adımdan oluşmaktadır:

1. ADIM 1-Bilgi ve belgelerin Kamu SM'ye gönderilmesi

Kurumsal başvurunun yapılmasının ardından, Kamu SM, NES başvurusu ile ilgili aşağıdaki form ve belgeleri kuruma iletir:

- NES başvuru formu,
- Nüfus cüzdanı sureti formu,
- Her başvuru sahibi için 2 nüsha NES sözleşmesi.

Kurum, yukarıdaki form ve belgeleri sertifika alınacak kişilere dağıtır. NES başvurusu, sertifika alınacak kişilere ait aşağıdaki belgelerin hazırlanarak resmi yazı ekinde Kamu SM'ye gönderilmesi ile yapılır:

- Sertifika başvurusunda bulunan kişi tarafından doldurulup imzalanmış NES başvuru formu,
- Noter veya kurum onaylı nüfus cüzdanı sureti,
- Sertifika başvurusunda bulunan kişi tarafından imzalanmış 2 nüsha NES Sözleşmesi.

Yukarıda belirtilen belgeler, kurum yetkilisinin imzasının ve kurum onayının bulunduğu resmi yazı ekinde Kamu SM'ye kapalı zarf içinde posta ile gönderilir. Resmi yazının içeriğinde ekte belgeleri bulunan NES alınacak kurum çalışanlarının açık adlarının bulunduğu listenin de mevcut olması gerekmektedir.

2. ADIM 2-Bilgi ve belgelerin değerlendirilmesi

Kurum tarafından gönderilen resmi yazı ve ekleri Kamu SM tarafından kontrol edilir. Başvuruların onaylanıp sertifika üretimine geçilebilmesi için aşağıdaki kontroller yapılır:

- Kurumdan gelen yazı ve ekindeki belgelerin geçerli imza veya onayı olup olmadığına bakılır,
- Kurumdan gelen yazı ve ekindeki belgelerde tahrifat, hata ya da eksik bilgi olup olmadığına bakılır,
- Başvuru belgeleri gönderilen kişilerin isimlerinin resmi yazı içeriğinde bildirilen listede olup olmadığı kontrol edilir,
- MERNİS'ten nüfus cüzdanı bilgilerinin kontrolü yapılır.

Yukarıdaki kontrollerin geçersiz bulunması durumunda ADIM 3'e geçilir. Yukarıdaki kontrollerin geçerli bulunması durumunda aşağıda açıklanan NES üretim, dağıtım ve kullanıma açma prosedürü işletilir.

3. ADIM 3-Kurumun bilgilendirilmesi

Geçersiz bulunan başvurular ile ilgili bilgilendirme kurum iletişim noktasına e-posta ile yapılır. Kurum, Kamu SM tarafından bildirilen hata ve/veya eksikliklerden haberdar olur. ADIM 1'deki işlemler tekrarlanarak hata veya eksiklerin düzeltildiği yeni formlar resmi yazı ekinde yeniden Kamu SM'ye gönderilir.

<u>NES üretim, dağıtım ve kullanıma açma işlemi</u>

Bu işlem, NES başvurusu geçerli bulunan kişilerin sertifika üretim, dağıtım ve kullanıma açma işlemlerinin yürütülmesi sürecini anlatmaktadır. Prosedür aşağıdaki adımlardan oluşmaktadır:

1. ADIM 1-Sertifika sahibine akıllı kartın ve NES sözleşmesinin teslimi

Sertifika sahibi adına anahtar çiftleri Kamu SM tarafından üretilerek, imza oluşturma verisi ve NES kişiselleştirilmiş akıllı kart üzerine yüklenir ve sahibine kurye ile teslim edilir. Sertifika sahibi akıllı kartını resimli resmi kimlik belgesi ibrazı ve imza karşılığında teslim alır; teslim tutanağını imzalayarak Kamu SM'ye iletilmek üzere kuryeye geri verir. Akıllı kartın teslimi sırasında sertifika sahibi, Kamu SM yetkilisi tarafından imzalanmış NES Sözleşmesini de teslim alır.

2. ADIM 2-Akıllı kart erişim verisinin kapalı parola zarfı içinde teslimi

Sertifika sahibine akıllı kart erişim verisi kapalı parola zarfı içinde, akıllı kart teslim tutanağının Kamu SM'ye ulaşmasından ve bilgilerin kontrol edilmesinden sonra (tahminen birkaç hafta içinde) kurye ile gönderilir. Sertifika sahibi teslim tutanağını imzalayarak Kamu SM'ye iletilmek üzere kuryeye geri verir.

<u>Bireysel sertifika işlemleri/sertifikanın kullanıma açılması</u>

Kamu SM sistemi içinde NES'lerle ilgili işlemler aşağıda belirtildiği biçimde yerine getirilmektedir. Sertifika sahibinin, akıllı kart ve kapalı parola zarfını teslim aldıktan sonra, Kamu SM'nin "http://www.kamusm.gov.tr/KullaniciServisleri" internet adresi üzerinden sertifikasını kullanıma açması gerekmektedir. Kullanıma açılmayan NES'lerle işlem yapılamaz. 1 (bir) ay içerisinde kullanıma açılmayan sertifikalar iptal edilir. Sertifika sahibi sertifikasını kullanıma açmadan önce sertifika içeriğindeki bilgilerin doğruluğunu kontrol eder.

Kullanıma açma işlemine, kapalı zarf içinde gönderilen "Uygulama Kodu" girilerek erişim sağlanır. Sertifika sahibi ilgili internet sayfasından sertifika etkinleştirme belgesine ulaşır ve belgeyi elektronik olarak imzalar. Bu işlemlerin yapılabilmesi için sistemde akıllı kart sürücüleri ve Java 1.4 ya da üzeri sürümü bulunmalıdır.

NES güncelleme işlemi

Sertifika güncelleme, sertifikanın iptali, içeriğindeki bilgilerin değişmesi ya da son kullanma tarihinin geçmesi gibi sebeplerle geçerliliğini kaybetmesi sonrasında sertifika sahibine yeni sertifika üretilmesi olarak tanımlanmıştır.

Güncellenen sertifika için yeni bir anahtar çifti oluşturulur ve seri numarası farklı yeni bir sertifika üretilir. İmza oluşturma verisi ve sertifika yeni bir akıllı kart içine yüklenerek sertifika sahibine ulaştırılır. Prosedür aşağıdaki adımlardan oluşmaktadır:

1. ADIM 1-Kamu SM'ye sertifika güncelleme başvurusunun yapılması

Sertifika güncelleme başvurusu, sertifika sahibinin bağlı bulunduğu kurum tarafından resmi yazı ile Kamu SM'ye yapılır. Başvuru sırasında, sertifika talep eden kullanıcı tarafından doldurulup imzalanan, NES başvuru formu Kamu SM'ye kapalı zarf içinde iletilir. Güncelleme başvurusunda, içeriğinin değişmemiş olması şartıyla, sertifika sahibine ait onaylı nüfus cüzdanı suretinin yeniden Kamu SM'ye gönderilmesine gerek yoktur.

Nüfus cüzdanı bilgilerinin değişmesi durumunda kurum veya noter onaylı nüfus cüzdanı sureti de Kamu SM'ye iletilir. Resmi yazının içeriğinde ekte belgeleri bulunan sertifikası güncellenecek sertifika sahibinin adı, soyadı, T.C. kimlik numarası ve eski sertifikasının seri numarası yer alır.

2. ADIM 2-Başvurunun Kamu SM tarafından değerlendirilmesi

Kurum tarafından gönderilen resmi yazı ve ekleri Kamu SM tarafından kontrol edilir. Başvuruların onaylanıp sertifika üretimine geçilebilmesi için aşağıdaki kontroller yapılır:

- Kurumdan gelen yazı ve ekindeki belgelerin geçerli imza veya onayı olup olmadığına bakılır,
- Kurumdan gelen yazı ve ekindeki belgelerde tahrifat, hata ya da eksik bilgi olup olmadığına bakılır,
- Başvuru belgeleri gönderilen kişilerin isimlerinin resmi yazı içeriğinde bildirilen listede olup olmadığı kontrol edilir,
- Sertifika içeriğindeki kişiye ait kimlik bilgilerinin değişmesi durumunda noter veya kurum onaylı nüfus cüzdanı suretinin gönderilip gönderilmediği kontrol edilir.

Yukarıdaki kontrollerden geçemeyen belgeler ile ilgili olarak kurum yazı ile bilgilendirilir. Kurum, Kamu SM tarafından bildirilen hata veya eksikliklerden haberdar olur. ADIM 1'e dönülerek hata ve eksikliklerin düzeltildiği yeni belgeler Kamu SM'ye gönderilir. Bilgi ve belgelerin hatasız olması, ancak sertifika içeriğinde değişme olması durumunda ADIM 3'e geçilir. Bilgi ve belgelerin hatasız olması ve sertifika içeriğinde değişme olmaması durumunda ADIM 4'e geçilir.

3. ADIM 3-Sertifika içeriğinde değişme olması durumunda eski sertifikanın iptali

Sertifikanın güncellenme sebebi sertifika içeriğinde değişme olması ise yeni sertifikanın üretilmeden önce eskisinin iptal edilmesi gerekmektedir. Eski sertifikanın iptal edilip edilmediği Kamu SM tarafından kontrol edilir. Eski sertifika iptal edilmiş ise ADIM 4'e geçilir.

Eski sertifika iptal edilmemiş ise güncelleme başvurusunun Kamu SM'nin eline geçmesinin ardından sertifika Kamu SM tarafından iptal edilir. Sertifika sahibi sertifikanın iptal edildiğine dair e-posta ile bilgilendirilir ve ADIM 4'e geçilir.

4. ADIM 4-Sertifika güncelleme başvurusunun Kamu SM tarafından onaylanması

Kamu SM, geçerli başvurunun alınmasıyla sertifikanın güncellenmesine onay verir. Sertifikanın üretimi için NES üretim, dağıtım ve kullanıma açma prosedürü işletilir.

NES yenileme işlemi

Kamu SM tarafından üretilen kişisel sertifikaların geçerlilik süresi 3 (üç) yıldır. Bu geçerlilik süresinin dolmasından 6 (altı) hafta öncesinden itibaren sertifika yenileme talebinde bulunulabilir. Yenilenen sertifikada sertifika sahibine ait yeni bir anahtar çifti oluşturularak, seri numarası farklı yeni bir sertifika üretilir. İmza oluşturma verisi ve sertifika yeni bir akıllı karta yüklenerek sertifika sahibine ulaştırılır. Sertifika yenilemesi yapılabilmesi için aşağıdaki şartların sağlanıyor olması gerekir:

- Kamu SM'den alınmış geçerli sertifikanın bulunması,
- Sertifikanın kullanım süresinin dolmamış olması ve kullanım süresinin dolmasına en fazla 6 (altı) hafta kalması,
- Sertifikanın içeriğindeki bilgilerde herhangi bir değişiklik olmaması.

Kamu SM sisteminde geçerli bir kullanıcı olarak tanımlı olduğu halde yukarıdaki şartların sağlanamadığı durumlarda yenileme başvurusunda bulunulamaz. Sertifika talep eden bu durumdaki kullanıcılar için NES güncelleme prosedürü işletilir.

Sertifika yenilemede NES başvuru prosedürü sırasında alınan belgelere dayanılarak işlem yapılır ve sertifika sahibinden yeni belgeler istenmez. Prosedür aşağıdaki adımlardan oluşmaktadır:

1. ADIM 1-Sertifika sahibine yenileme başvuru uyarısının gönderilmesi

Kamu SM, sertifika geçerlilik süresinin dolmasına 6 (altı) hafta kala sertifika sahibine bilgilendirme notu ile birlikte sertifika yenileme başvurusunu yapacağı internet adresi bilgisini e-posta ile gönderir. Daha önce yenileme başvurusu yapılamaz. Sertifikasını yenilemek isteyen kullanıcı, kendisine e-posta ile bildirilen internet sitesine bağlanarak, yenileyeceği sertifikası ile ilgili imza oluşturma verisini kullanarak elektronik olarak imzaladığı yenileme başvuru formunu Kamu SM'ye gönderir.

2. ADIM 2-Yenileme başvurusunun kurum tarafından onaylanması

Yenileme başvurusunun işleme alınabilmesi için kurumun onayı gerekmektedir. Kurumun onay vermediği yenileme başvuruları Kamu SM tarafından işleme alınmaz. Sertifikaların yenilenmesine onay verildiği kurum tarafından Kamu SM'ye resmi yazı ile iletilir. Resmi yazı içeriğinde sertifikasının yenilenmesine onay verilen sertifika sahibinin adı, soyadı, T.C. kimlik numarası ve eski sertifikanın seri numarası yer alır. Kamu SM, kurum tarafından kabul edilmeyen yenileme başvuruları için yenileme işlemini yapmaz ve sertifika sahibini e-posta ile bilgilendirir. Başvurunun kurum tarafından kabul edilmesi durumunda ADIM 3'e geçilir.

3. ADIM 3-Yenileme başvurusunun Kamu SM tarafından onaylanması

Kamu SM, başvurunun kurum tarafından kabul edilmesi sonucunda sertifikanın yenilenmesine onay verir. Sertifikanın üretimi için NES üretim, dağıtım ve kullanıma açma prosedürü işletilir.

<u>NES iptal/askıya alma işlemi</u>

İptal edilen veya askıya alınan sertifika bilgisi Kamu SM SİL listesi ve ÇİSDUP sunucu üzerinden yayınlanır. Sertifika iptal edildikten sonra kullanıcı yeni sertifikaya ihtiyaç duyuyorsa, NES güncelleme prosedürü uyarınca yeni bir sertifika başvurusunda bulunabilir. Sertifikanın iptali/askıya alınması aşağıda belirtilen iki farklı şekilde gerçekleştirilebilir:

1. İmzalı NES iptal/askıya alma başvuru formunun Kamu SM'ye gönderilmesi

Sertifika sahibi NES iptal/askıya alma başvuru formunu doldurur ve imzalayarak posta ile Kamu SM'ye gönderir. Formun eksiksiz doldurulmuş olup olmadığı ve imzalı olup olmadığı Kamu SM tarafından kontrol edilir. Sertifika sahibi formun

Kamu SM'ye ulaştığı gün içinde telefonla aranarak, sertifikanın iptalini veya askıya alınmasını onaylayıp onaylamadığı sorulur. Sertifika sahibine ulaşılamaması durumunda işlem yapılmaz.

Gönderilen formun geçersiz bulunması ve sertifika sahibinin telefonda durumu onaylamaması durumunda, Kamu SM sertifikayı iptal etmez/askıya almaz ve başvuru sahibini geçersiz iptal/askıya alma başvurusunun alındığına dair e-posta ile bilgilendirir. Gönderilen formun geçerli bulunması ve sertifika sahibinin telefonda onayının alınması durumunda ise NES iptal/askıya alma başvuru formu Kamu SM tarafından da onaylanır, sertifika aynı gün içinde iptal edilir/askıya alınır ve sertifika sahibi e-posta ile bilgilendirilir.

2. Sertifika sahibinin Kamu SM çağrı merkezinden sertifika iptali veya askıya alma başvurusunda bulunması

Sertifika sahibi Kamu SM'nin çağrı merkezini arayarak sertifikasını iptal ettirebilir veya askıya alabilir. Çağrı merkezinden yapılan başvurularda, sertifika sahibinin kimliği Kamu SM sisteminde tanımlı bilgileri kullanılarak doğrulanır ve iptal/askıya alma talebi yerine getirilir.

<u>NES askıdan çıkarma işlemi</u>

Sertifikanın askıda kalma süresi 1 (bir) ayı aşamaz. Bu süre sonuna kadar Kamu SM'ye askı durumunun sonlandırılması isteğinin sertifika sahibi tarafından gelmesi gerekir. Verilen süre dolduğu halde sertifikanın askıdan çıkarılma talebi gelmez ise sertifika Kamu SM tarafından iptal edilir.

Askıdan çıkarılan sertifika bilgisi Kamu SM SİL listesinden çıkarılır ve ÇİSDUP sunucu üzerinde sertifikanın durumu geçerli konumuna getirilir. Sertifikanın askıdan çıkarılması aşağıda belirtilen iki farklı şekilde gerçekleştirilebilir:

1. İmzalı NES askıdan çıkarma başvuru formunun Kamu SM'ye gönderilmesi

Sertifika sahibi NES askıdan çıkarma başvuru formunu sertifikanın askıya alınmasını takip eden 1 (bir) ay içinde doldurur ve imzalayarak Kamu SM'ye posta ile gönderir. Sertifika askıdan çıkarma işleminin aciliyeti durumunda form faks ile de kabul edilebilir. Ancak formun aslının Kamu SM'ye iletilmesi gerekmektedir.

NES askıdan çıkarma başvuru formu Kamu SM'ye ulaşınca, başvurunun onaylanıp sertifikanın askıdan çıkarılması için formun eksiksiz doldurulmuş ve imzalı olup olmadığı kontrol edilir. Sertifika sahibi telefonla aranarak sertifikanın askıdan çıkarılmasını onaylayıp onaylamadığı sorulur. Sertifika sahibine ulaşılamaması durumunda işlem yapılmaz.

Gönderilen formun geçersiz bulunması ve sertifika sahibinin telefonda durumu onaylamaması durumunda, Kamu SM sertifikayı askıdan çıkarmaz ve başvuru sahibini geçersiz askıdan çıkarma başvurusunun alındığına dair e-posta ile bilgilendirir. Gönderilen formun geçerli bulunması ve sertifika sahibinin telefonda onayının alınması durumunda ise NES askıdan çıkarma başvuru formu Kamu SM tarafından da onaylanır, sertifika aynı gün içinde askıya alınarak sertifika sahibi e-posta ile bilgilendirilir.

2. Sertifika sahibinin Kamu SM çağrı merkezinden sertifika askıdan çıkarma başvurusunda bulunması

Sertifika sahibi Kamu SM'nin çağrı merkezini arayarak sertifikasını askıdan çıkarabilir. Çağrı merkezinden yapılan başvurularda, sertifika sahibinin kimliği Kamu SM sisteminde tanımlı bilgileri kullanılarak doğrulanır ve sertifikası askıdan çıkarılır.

5.3. Nitelikli Elektronik Sertifika Maliyetleri

Çizelge 5.1'de NES, akıllı kart ve akıllı kart okuyucuya ilişkin ESHS'lerin perakende fiyatları bulunmaktadır. Belirtilen fiyatlara %18 KDV tutarı dahil değildir. Söz konusu ESHS'lerin web sayfalarında yüksek sayılı kurumsal satışlara yönelik olarak da fiyatların ayrıca belirleneceği belirtilmektedir.

Ayrıca sunucu (SSL) sertifikası KDV hariç ortalama fiyatları 1 yıllık 350 YTL, 2 yıllık 600 YTL ve 3 yıllık 750 YTL'dir. Zaman damgası hizmetine yönelik ortalama fiyatlandırma ise (KDV hariç) 1 aylık 75 YTL, 3 aylık 200 YTL, 6 aylık 350 YTL ve 1 yıllık 600 YTL'dir.

Çizelge 5.1. NES fiyatları

ESHS	NES (1 Yıllık)	Akıllı Kart	Akıllı Kart Okuyucu	Paket Fiyatı (NES+Akıllı Kart+ Akıllı Kart Okuyucu)
Kamu SM	99 YTL			
TürkTrust	150 YTL	30 YTL	30 YTL	182 YTL
E-Güven	110 YTL	35 YTL	40 YTL	185 YTL

NES'lere yönelik olarak diğer işlem/yenilemelere ilişkin ortalama fiyatlar da aşağıda sunulmuştur:

- Mevcut akıllı kart üzerinde, bir yıllık normal kullanım süresi sonunda sertifika yenileme: 85 YTL,
- Kart kullanılamaz duruma geldiğinde yeni kart üzerine yenileme (Kurye gönderisinin teslim alınmasından itibaren 1 ay içinde): 72 YTL
- Kart kullanılabilir durumda olduğunda mevcut kart üzerine yenileme (Kurye gönderisinin teslim alınmasından itibaren 1 ay içinde): 43 YTL

- Akıllı karttan sertifika silindiğinde (imza oluşturma verisinin zarar görmediği durumda) mevcut kart üzerine mevcut sertifikayı yeniden yükleme işlemi: 21 YTL
- Kurulum ücreti ortalama 75 YTL'dir.

5.4. Açık Anahtar Altyapısı Yazılımları

E-imza, bilgisayar ortamındaki verilerin değiştirilmesini engellemek ve ıslak imzanın işlevini, elektronik olarak da sağlamak için kullanılır. E-imza, standartlar ve güvenlik üzerine kuruludur. Sertifikanın üretilmesinden, sertifika sahibine teslim edilmesine kadar tüm aşamalar ciddi güvenlik önlemleri ile korunmakta ve sertifika standartları yasal mevzuat ile belirlenmiş bulunmaktadır. Fakat, sertifika kullanılarak imza atılması ve atılan imzanın doğruluğunun kontrol edilmesi işlemleri için gerekli olan programlar için böyle bir güvenlik kısıtı ve format sınırlaması mevcut değildir [47].

Bir AAA içerisinde, belirli bir zaman için anahtar çiftlerini ve sertifikaları oluşturmak ve bunları kontrol etmek için, çeşitli yazılımlar kullanılmaktadır. Sayısal sertifikalar ve "özenle korunan" anahtar çiftleriyle verilerin imzalanması, doğrulanması, şifrelenmesi ve şifrelerinin çözümü, mevcut yazılımlar kullanılarak, kolaylıkla yapılabilmektedir. ESYA, İmzager, UniCERT, Entrust, IBM Trust Authority, RSA Keon, VeriSign, ZEUGMA, Lidya, DOSIA, Agora, GlobalSign, TürkTRUST, Bergama, iTrus, eSign, ComSign, PT Trust, Trust Asia, DSV ve CertPlus mevcut yazılımların bazılarıdır. Bu yazılımların bazıları aşağıda kısaca tanıtılmıştır [3].

ESYA yazılımı

Bünyesinde birçok ileri test merkezleri bulunan TÜBİTAK-UEKAE'de, bir çok güvenlik yazılımları ve donanımları geliştirmektedirler. AAA'yı destekleyen bir yazılım olan ESYA (Elektronik Sertifika Yönetim Altyapısı) da bu enstitü bünyesinde geliştirilmiştir. Geliştirilen bu yazılımın bileşenleri; KSM, SM, KM sunucu servisleri ile son kullanıcının kullanımına yönelik olan İstemci Modülü'dür. ESYA yazılımı, elektronik sertifikalar ile ilgili yaşam döngüsü kapsamında elektronik sertifika üretme, iptal etme, askıya alma, askıdan indirme, sertifika iptal listesi yayınlama gibi hizmetleri sunar. Yazılım, ölçeklenebilir mimari tasarım üzerinde Java Enterprise teknolojisi kullanılarak geliştirilmiştir.

ESYA yazılımının en önemli tarafı, genel güvenlik kriterleri göz önüne alındığında üstünlükleri, uluslararası standartlara göre yazılımın geliştirilmesi, istenildiğinde Linux işletim sistemine uyarlanabilmesi, tüm yazılımların kendi bünyesinde geliştirilmesi, isteğe bağlı olarak kısa sürede yazılımın farklı bünyelere adapte edilebilmesi ve en önemlisi ise, bünyesinde geliştirebileceği milli yazılım desteğini de verebilecek olmasıdır [3].

ESYA, Kamu SM'nin gelecekte ihtiyacı olabilecek ulusal çapta bir dağıtık kayıt makamı yapısını destekler niteliktedir. Milli yazılım oluşu ve teknolojik özelliklerinden dolayı Kamu SM'de sertifika makamı yazılımı olarak ESYA tercih edilmiştir. Bu ürün, ESHS'lere ve kurumsal AAA altyapısını kurmak isteyen kuruluşlara ticari olarak lisanslanmaktadır [47]. ESYA ürünleri sunucu ve istemci yazılımları olarak iki ana grup altında toplanmıştır:

ESYA SM sunucu yazılımı

Bu yazılım bir ESHS olarak hizmet vermek için gereklidir. SM yazılımı elektronik sertifikalar ile ilgili tüm yaşam döngüsünü yönetir. Bunun için elektronik sertifika üretme, iptal, askıya alma, askıdan indirme, SİL yayınlama gibi hizmetleri sunar.

ESYA zaman damgası sunucu yazılımı

Zaman damgası sunucusunun temel görevi, istemcilerden gelen taleplere göre e-imzalı zaman damgası üretmektir. Zaman damgaları belli bir verinin belirtilen bir tarihte var olduğunu kanıtlarlar. Zaman damgası sunucusu, zaman damgalarını imzalamak için açık anahtar teknolojisini kullanarak, verinin bütünlüğünü ve belirli bir tarihteki varlığını onaylar.

ESYA çevrimiçi sertifika durum protokolü sunucusu

Çevrimiçi Sertifika Durum Protokolü--ÇİSDUP (Online Certificate Status Protocol--OCSP) sunucusu sertifikaların geçerli olup olmadıklarını kontrol etmek için kullanılır. Bu sunucu, ESHS'nin ürettiği sertifikalar hakkında yapılan sorgulara çok hızlı bir şekilde, e-imzalı cevaplar üretir. Böylece e-imza ve elektronik sertifika geçerlilik kontrolleri, SİL kullanmaya göre daha yüksek güvenilirlikle yapılabilir [47].

ESYA istemci yazılımları

ESYA istemci yazılımı, Microsoft Outlook üzerinden S/MIME kullanarak imzalı/şifreli mesajlaşmayı sağlar. ESYA istemci yazılımının ayrıca, masaüstü dosya imzalama, şifreleme, güvenli dizin gibi işlevleri yerine getiren Windows Explorer ile entegre yazılım modülleri de bulunur. Bu yazılımların, 5070 sayılı kanuna uygun e-imza destekleyen sürümleri geliştirilmiştir [47].

<u>İmzager yazılımı</u>

İmzager masaüstü imzalama yazılımı (İmzager MİM)

İmzager MİM, TÜBİTAK-UEKAE tarafından geliştirilen ve 5070 sayılı kanuna uygun dosya imzalayabilen masaüstü imzalama aracıdır. Hazırlanan belgelerini uygulamadan bağımsız bir şekilde ETSI formatında imzalamayı ve ETSI formatında

imzalanmış belgeleri açıp doğrulamayı ve içeriğine ulaşabilmeyi sağlar.

İmzagerMİM, İmzagerAPI ve ESYA kütüphaneleri kullanılarak geliştirilmiştir. Ürün özellikleri [47]:

- İmzagerAPI'nin sahip olduğu özellikleri kullanabilir.
- TK'nın standartlarını belirlediği dosya formatlarını imzalayabilir.
- İçeriğin değişmeyeceğini garanti ettiğinden E-imza Kanunu 6. Md. (d) bendine uygundur. Standart ve açık olmayan formatlara sahip dokümanların içerikleri çeşitli nedenlerle garanti edilemediği için, bu dokümanların imzalanması tavsiye edilmemektedir.
- İmzalı belgelerin yönetimi (dosyalanması, kopyalanması, silinmesi, imza eklenmesi).

İmzager akıllı kart yönetim yazılımı (İmzager AKAY)

Akıllı kart yöneticisi olan İmzager AKAY ile bilgisayardaki tüm kart okuyuculara erişilebilir, akıllı kartlar ile ilgili temel ve ileri seviyede işlemler yapılabilir. Bu program sayesinde akıllı kartın içindeki tüm sertifikalara ulaşılabilir, bu sertifikalar kolayca yönetilebilir.

İmzager AKAY'ın Özellikleri [47]:

- Kart okuyucuya ait temel bilgileri gösterir.
- Akıllı kart bilgilerini gösterir.
- Akıllı karta erişim verisinin (PIN ve PUK kodlarının) değiştirilmesini sağlar.
- Akıllı karttaki sertifikalar hakkında bilgi verir.
- Sertifika silme, ekleme, görüntüleme gibi yönetim işlemlerini yapmayı sağlar.
- Güvenilir ESHS sertifikaları ile çalışır.
- ESHS kök sertifikalarını kendi içinde güvenli bir şekilde tutar.

E-imza kütüphaneleri

Kamu SM tarafından, kurumlar tarafından geliştirilen yazılımlara e-imza entegrasyonu sağlamak için Java ve .NET platformlarında birer yazılım kütüphanesi (API) geliştirilmiştir. Web tabanlı uygulamalara yönelik bir Java applet, kütüphaneyle birlikte ücretsiz verilmektedir.

a. İmzager API

İmzager API, e-imza ile ilgili işlemlerin yapıldığı yazılım kütüphanesidir. Diğer Kamu SM ürünlerinin de temelini oluşturan bu kütüphane, standartlar, güvenlik ve kullanım kolaylığı gözetilerek hazırlanmıştır. İmzager API kullanılarak, sunucu ya da istemcilerde imzalama ve imza kontrollerine dair her tür işlem hızlı bir şekilde program/projelere entegre edilebilir.

İmzager API'nin Özellikleri [47]:

- ETSI (Avrupa Birliği) TS 101 733 ve TS 101 903 e-imza formatı
- Farklı imza tipleri: İmzalanan belgenin türüne, kullanım amaçlarına göre, değişik ihtiyaçları karşılayacak imzalama tipleri
  - Temel imza
  - Zaman damgalı imza
  - İlkeli imza
  - Arşiv imzası
- İmza bilgileri
  - Yetki bilgisi: İmza atan kişinin kurum bilgilerini, yetkisini, içerir.
  - Zaman bilgisi: İmzanın atıldığı tarih
  - Yer bilgisi: İmzanın atıldığı yer, ülke, şehir, adres bilgileri
  - İmza amacı: Belgeyi üreten, gönderen, teslim eden, alan, onaylayan ya da belgenin kaynağı olarak, temel tipleri mevcuttur. İstendiğinde bu sebepler çoğaltılabilir.

- Belge numarası: İmzaları belirtmek için kullanılabildiği gibi, sorumlu kişinin belirlediği bir numara ile belge numarası olarak da kullanılabilir.
- Referans belge numarası: Bir imzadan diğer imzaya ya da bir belgeden diğer belgeye atıf amacıyla kullanılır.
- Belge format bilgisi: İmzalanan belgenin doküman formatı
- Zaman damgası: Zaman bilgisi, zaman damgası sunucuları tarafından atılan bir çeşit imzadır. Belirli tarihte bu belgenin varlığını garanti eder.

- Temel veri içeriği: İmzalanan belgenin türüne, kullanım amaçlarına göre, değişik ihtiyaçları karşılayacak veri içerik tipleri
  - İmzalanan Belge -opsiyonel olarak eklenip çıkarılabir-
  - İmzalar
  - Sertifikalar -opsiyonel olarak eklenip çıkarılabir-
- XML ve ASN.1 standardı
- Bağımsız imza kontrolleri: Belge üzerindeki tüm imzaların kontrol bilgilerini ayrı ayrı tutarak imzaların bağımsız olarak işlem görmesini sağlar. Böylece belge üzerindeki imzalardan biri ya da birkaçı geçersiz olduğunda bile geçerli imzalar üzerinden işlem yapabilmek mümkündür.
- Bağımsız sertifika kontrolleri: Her imzanın sahip olduğu sertifikanın kontrol bilgilerine de ayrı ayrı ulaşılabilmektedir.
- Tüm imza bilgilerine ulaşım: Standartların ve formatın elverdiği tüm bilgilere erişmek mümkündür.
- Java ve .net desteği: İki yaygın platform temel alınarak, farklı uygulamalara destek verilmektedir.
- Seri/paralel imza ekleme
  - Bir belgeye birden çok imza atılabilmektedir.
  - İmzalar seri ve paralel olmak üzere ikiye ayrılır. Paralel imza, sadece belgenin imzalanmasını ifade eder. Seri imza ise, daha önce imzalanmış belgenin, imzalarının da onaylanması için kullanılır.
- İmzalı belgeden imza çıkarma: İmzalı bir belgenin üzerindeki imzalar ihtiyaca göre silinip, yeni işlemler için kullanılabilir.

- İmza hiyerarşisi: Farklı hiyerarşik yapılanmalar, seri ve paralel imza kombinasyonları kullanılmasına ihtiyaç duyar. Bu bilgiler imza ağacı şeklinde gösterilebilmektedir.
- Zaman damgası
  - Zaman damgası atabilme: Yalnızca zaman damgası adresi, kullanıcı adı ve şifre kullanarak zaman damgası sunucusundan zaman damgası alınabilmektedir.
  - Zaman damgası kontrolü: Atılan zaman damgası bilgileri, imza gibi doğruluğu kontrol edilebilmektedir.
  - Zaman damgası bilgileri: Zaman damgası atılmış bir belgenin ilgili tüm bilgilerine ulaşılabilmektedir.
- İptal listeleri, OCSP işlemleri: Sertifika geçerlilik kontrolleri için, otomatik olarak sunuculara bağlanıp kontrolleri yapılabilmekle birlikte, intranet ortamlarında da, dışarıdan aynalanmış OCSP ya da SİL sunucularına bağlantı imkanı mevcuttur.
- Güvenilir kök sertifikaları barındırabilme: Nitelikli imza sertifikaları üreten kök sertifikalarını, işletim sisteminden bağımsız olarak yönetebildiği için, maniplasyon ya da silme işlemlerine karşı dışarıdan müdahelere karşı korunaklıdır.

b. İmzager GAMO web applet

İmzager GAMO, web uygulamalarına kısa yoldan imza entegrasyonu sağlayan, İmzager API üzerine kurulu bir Java applet'tir. İmza oluşturma sırasında kullanıcıdan PIN kodu ister, imzalanacak metni ve kullanılacak sertifikayı gösterir. İmzager GAMO, şimdilik sadece düz metin ve türevi veri formatlarını desteklemektedir. Üzerinde Kamu SM'nin imzasını taşıdığından, kullanıcıların yaptıkları imzalama işlemlerinin Kamu SM e-imza programları tarafından gerçekleştirildiğini garanti eder. Bu anlamda, web sitesi sahibi, yöneticisi ya da programcısına ait hata, güvenlik eksikliği ya da yanlış yönlendirmeleri ve kötü niyetli saldırıları engellemede yardımcı olur.

İmzager GAMO, mevzuatı, güvenliği, standartları gözeterek kullanıcılara imzalama işlemi boyunca eşlik eder. Böylelikle kullanıcı, hangi web sitesinde olursa olsun,

Kamu SM'nin güvencesi altında, tereddüt etmeden imzalama işlemini gerçekleştirebilir.

İmzager GAMO'nun Özellikleri [47]:

- Kanuna uygun olarak "Nitelikli İmza" atabilme: Mevzuata uygun bir şekilde imza içeriğini gösterek imza atılmasını sağlar.
- Çoklu kart okuyucu ve çoklu sertifika desteği: Bilgisayara bağlı birden fazla kart okuyucu ve sertifika olduğu durumlarda, kullanıcıya istediği sertifikayı seçme imkanı tanır.
- İmza kontrolü yapabilme: Daha önce imzalanmış bir belgeye imza atılmak istendiğinde, önceki imzaların geçerliliklerini sayfadan bağımsız bir şekilde kontrol eder.
- İmza bilgilerini belirtme: Belge üzerindeki imzalara ait tüm bilgileri kullanıcıya gösterir.
- Sertifika bilgilerini belirtme: İmza atılacak sertifika ya da daha belge üzerindeki imzalara ait sertifika bilgierini ve geçerlilik kontrollerini kullanıcıya gösterir.

UniCERT

UniCERT, Baltimore Teknolojileri tarafından üretilen bir AAA yazılımı olup, tam bir güvenlik sağlamak amacıyla sunulmuş bir SM ürünüdür.

X.509 V3 sayısal sertifika çerçevesinde, UniCERT ile güvenli e-posta, e-ticaret, güvenli web bankacılığı, online alışveriş ve VPN ile anahtar yönetimi, onaylama ve inkar edememezlik işlemleri gerçekleştirilir. Bu yapı, çok geniş bir alanda iş ve hukuki ihtiyaçları mümkün olduğunca karşılamak için tasarlanmıştır [3].

Entrust

Entrust, uzun süredir AAA pazarında bulunan ürünlerden birisidir. Son kullanıcı arayüzünün görünmezliği, bu ürünün, en önemli özelliklerindendir. Bu, kullanıcıya tek bir noktadan erişim ve güvenlikle ilişkili, yoğun şifreleme gerektiren her hangi bir uygulamanın ve imzalama işlemlerinin, kolaylıkla yapılmasını sağlar.

Aynı zamanda, bu ürün AAA ile tamamen entegre olabilmektedir. Uygulamalara, tek giriş (login) imkanı sunma, anahtar güncellemelerinin şeffaf olarak sağlanması, anahtar tarihçesi ve yaşam döngüsünü otomatik olarak oluşturma ve görebilme, anahtar oluşumunun güvenlik açığı oluşturmadan basitleştirilmesi, SİL'in daha güçlü olarak kontrolü ve son olarak da masa üstünde zekice özellikler sunulması bu ürünün belirtilen farklılıklarıdır.

IBM trust authority

IBM Trust Authority, FirstSecure ailesinin bir ürünüdür. Bu ürün ile, virüs koruma, saldırı tespit, giriş kontrol, trafik içerik kontrolü, kodlama, sayısal sertifika, güvenlik duvarı teknolojileri ve uygulama geliştirme ortamları sunulmaktadır. Ürün, KSM, SM, KM, yetkilendirme altsistem, websphere uygulama sunucusu, veritabanı sistemi, dizin sunucusu ve kullanıcı bileşenlerinden oluşmaktadır.

RSA keon

RSA Keon, "Keon Sertifika Sunucusu" ve "Geliştirilmiş Keon" olmak üzere, iki farklı AAA çözümü sunmaktadır. "Keon sertifika sunucusu", anahtar yönetimi sistemi, anahtar sistemi, LDAP sertifika deposu, sertifika ambarı ve veritabanını içeren yönetim sistemidir. "Geliştirilmiş Keon" ise, sertifika sunucusunun hizmet alanını, bütünleştirilmiş masaüstü bileşenleri ile genişleten, ileri doğrulama ve AAA özellikleri sunan yaklaşımlar içermektedir.

VeriSign

Sayısal haberleşmede ve ticarette devam eden gelişmelerin herkes tarafından kullanılmasını ve faydalanmasını amaçlayan VeriSign, dünya çapında bilgi güvenliği pazarında öncü ve güvenilir hizmet veren güvenlik şirketlerinden biridir. 100'den fazla ülkede hizmet veren Verisign, farklı sektörlere özel çözüm sunmasıyla, geniş ve deneyimli destek ve danışmanlık hizmetleri vermesiyle, işlemci, donanım ve yazılım güvenliği sağlamasıyla öne çıkan bir şirkettir.

20 farklı tarayıcı ve 45 farklı web sunucuda çalışabilmesi, yüksek güvenilirlik ve işlerliğe sahip olması, hızlı kurulabilmesi, kurumlara özel hizmetler sunabilmesi ile esnek, ölçeklenebilir ve tekrarlanabilir olması, proje yönetimi, danışmanlık, operasyon ve bakım destek hizmetleri tecrübesi, finansal güvenilirlik ve anlaşmalarla garanti edilmiş uzun vadeli uygulama desteği, e-imza yasaları ve çeşitli güvenlik uygulamalarına yön veren çalışmalar yürütmesi, bu firmanın ve ürünlerinin üstünlükleri olarak sıralanabilir [3].

ZEUGMA

Bünyesinde birçok güvenlik yazılımı geliştirilen Tübitak-BİLTEN tarafından, AAA, elektronik sertifika ve e-imza teknolojileri ile güvenlik sorununa etkin çözümler sunabilen, ZEUGMA, Lidya, DOSIA, Agora ve Bergama isminde yazılımlar geliştirilmiştir.

Uluslararası standartlara uyumlu olarak geliştirilen, AAA'nın kurulması ve işletilmesi için gerekli olan elektronik sertifikaların üretim ve yönetimini sağlayan bir yazılım paketi olan ZEUGMA, AAA'ların temelini oluşturan sertifika üretimi ve yönetimi işlemlerinin yürütülmesini sağlayan, sertifika hizmet sağlayıcısı yönetim yazılımıdır. Platform, bağımsız olarak tümüyle Java teknolojisi kullanılarak geliştirilmiştir. Bu yazılımın, Türkçe karakterleri desteklemesi, modüller yapıda olması ile farklı yapıları desteklemesi, web üzerinden gelen sertifika istek formlarını

değerlendirme, akıllı kart ve akıllı çubuklarla uyumlu çalışması, sertifikaların üretim ve yönetim politikalarının oluşturulabilmesi, sertifikaların içeriğinin ve kullanım alanlarının belirlenebilmesi, SİL yayımlanması, LDAP (Lightweight Directory Access Protocol) ve OCSP desteklerinin bulunması, HSM (Hardware Secure Module) ile birlikte çalışabilmesi, anahtar kurtarma ve çapraz sertifikasyon özelliklerine sahip olması bilinen özellikleridir. Bunun yanında; X.509 V3, PKCS #1, PKCS #5, PKCS #7, PKCS #8, PKCS #10, PKCS #11, PKCS #12, FIPS (The Federal Information Processing Standards) 46-2, FIPS 180-1 ve FIPS 186-1 standartlarını da desteklemektedir.

Kök SM ve KM olmak üzere iki ana parçadan oluşan bir mimariye sahip olan ZEUGMA'nın, KSM sertifikası ve gizli anahtarının tutulmasından, sertifikaların imzalanması ve yönetimleriyle ilgili işlemler ile KM'nin görevlerini de destekleyecek yapılanması vardır. Zeugma, KSM ve SM modülleri, gizli anahtar, yetkilendirme, sunucu, istemci ve internet başlığı altında hizmetler sunmaktadır [3].

Lidya

Tübitak-BİLTEN tarafından geliştirilen LİDYA (Güvenliği Elektronik Belge Sistemi), e-devlet, e-ticaret ve e-iş uygulamalarında ticari ve resmi belgelerin elektronik ortamlarda güvenli olarak iletimi için geliştirilmiş bir yazılımdır. İşlemlerin elektronik ortamlarda güvenli, hızlı ve hatasız yürütülmesini destekleyen bu yazılım, ZEUGMA'da olduğu gibi, uluslararası standartlar baz alınarak geliştirilmiştir. Bu yazılım, akıllı karta veya bilgisayara yüklü sertifika ile kullanıcıyı sunucuya tanıtma, elektronik belge imzalama, imzalı bir belgenin verilerini doğrulama, imzalı bir belgeyi şifreleme, sertifika bilgileri ile kullanıcı kimliği doğrulama, verilerin ve imzanın veri tabanı kaydı gibi işlemleri desteklemektedir.

DOSIA

Tübitak-BİLTEN tarafından geliştirilen 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 [3].

Agora

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

GlobalSign

GlobalSign, tarafsız ve güvenilir bir kurum ve SM olarak, Avrupa, Asya ve Amerika kıtalarında 20'den fazla ülkede kurduğu KM'ler ile hizmet veren bir şirkettir. Güven ağını ve hizmetlerini her geçen gün genişleten bu şirket, güvenli ve güvenilir e-ticaret ve mobil iş ortamları ile imzalanmış/mühürlenmiş e-posta mesajları için, sayısal sertifikaların üretilmesi ve yönetilmesi gibi hizmetler sunan bir güvenlik servis sağlayıcısıdır. Tüm ticari ve sivil kuruluşlara ve hükümet birimlerine kurumsal AAA çözümleri, mobil ticaret güvenliği, tarafsız rapor hazırlama ve AAA danışmanlığı gibi, değişik sertifikasyon hizmetleri de vermektedir [3].

TürkTrust

TürkTrust Sertifika Yönetim Süreçleri Yazılımı, çok katmanlı esnek mimari sahip olmasının yanında yüke bağlı ölçeklenebilir ve dağıtık çalıştırılabilir yazılım mimarisini de desteklemektedir. Çevrim dışı merkezi sertifika üretimi, paketler bazında merkezi toplu sertifika üretim desteği, sertifika üretiminde HSM entegrasyonu, PKCS#11 ile uyumlu her türlü donanımla entegrasyon yeteneği, ayrı

istemci ve web tabanlı başvuru alma ve işleme ara yüzleri ile kayıt sisteminde özelleştirilebilen yetkilendirmeye de sahiptir. Tüm işlem kayıtları, başvuruların barkod sistemiyle takibi, güvenli ve eşsiz başvuru barkod üretimi ve yönetimi, otomatik barkodlu başvuru formu üretimi ile hızlıca yapılabilmektedir. JAVA tabanlı, platform bağımsız, X509 V4, PKCS#10, PKCS#12, PKCS#7, PKCS#11, RSA, SHA-1, CRLi, CMP desteği de veren TürkTrust yazılımı, ORACLE tabanlı olarak geliştirilmiştir. Ayrıca yazılımın LDAP uyumu da vardır.

5.5. Gazi Üniversitesi İçin Örnek E-İmza Uygulamasının Gerçekleştirilmesi

Bu bölümde, kurumsal ağlarda e-imza sistemlerine geçiş aşamasında yapılması gereken işlemler, izlenecek yollar ve örnek uygulamalar, Gazi Üniversitesi için hazırlanan örnek bir e-imza uygulaması ile detaylı olarak anlatılmıştır.

Kurumsal ağlarda e-imza sistemlerinin hayata geçirilmesi için öncelikle gereksinimler ortaya konmalı ve doğru gereksinimleri karşılayacak şekilde analiz yapılmalıdır. Yapılacak doğru analiz çalışmaları sonucunda hayata geçirilecek e-imza sistemlerinden beklenen fayda sağlanabilir.

Kurumsal ağların e-imza sürecine geçişte kurumsal yapılarına en uygun şekilde hareket etmesi, hem e-imzanın uygulanması açısından hem de kaynak israfının ve atıl yatırımların ortaya çıkmaması açısından son derece önemlidir. Esas alınması gereken en önemli nokta, kaynakların etkin ve verimli kullanılması ve uygun modeller çerçevesinde harcama yapılması yaklaşımı olmalıdır. Kurumsal ağların e-imzaya geçiş modelleri Bölüm 3.7'de açıklanmıştır.

Kurumların, kurum-vatandaş ilişkileri ve kurum-kurum ilişkileri dikkate alındığında, tüm evrak sisteminin kısa süre içinde tamamen e-imza sürecine geçmesi mümkün olmadığından e-imza süreci ile ıslak imza sürecinin birlikte devam edeceği unutulmamalıdır. Bu çalışmada ıslak imza süreçleri dikkate alınmaksızın sadece e-imza süreçleri incelenmiştir.

Kurumda e-imza sistemi ile ilgili yapılacak çalışma, sırasıyla aşağıda verilen adımlardan oluşacaktır:

1. Gereksinimlerin belirlenmesi
2. Analiz
3. Tasarım
4. Gerçekleştirim
5. Test
6. Kullanım ve yaygınlaştırma

5.5.1. Gereksinimlerin belirlenmesi

E-imza işlemlerinde kullanılacak toplam bilgisayar sayısı

Proje kapsamında kullanılacak bilgisayar sayısı, proje kapsamında e-imza kullanması hedeflenen personel sayısı kadar olacaktır. Kurum içindeki resmi yazışmaları hazırlayan ve imza yetkisi olan personel, sistemin öncelikli kullanıcıları olacaktır. Bu kapsamda üniversite içinde e-imza kullanması hedeflenen personelin, tüm idari ve akademik birimlerde yazışma yapan ve imza yetkisi olan personel olacağı değerlenmiştir. Bu sayı örnek uygulama için toplam 18 olarak belirlenmiştir. Söz konusu personel zaten bilgisayara sahip olduğundan ilave bilgisayar ihtiyacı doğmamıştır.

Kullanıcı bilgisayarlarının internet bağlantısı durumu

Proje kapsamında e-imza sistemlerini kullanacak tüm personelin bilgisayarının internet erişiminin olması gerekmektedir. Belirlenen personelin tamamının kullandığı bilgisayarların internet erişimi olduğundan bu kapsamda ilave ihtiyaç doğmamıştır.

Kullanıcı bilgisayarlarının işletim sistemleri

Proje kapsamında e-imza kullanacak personelin bilgisayarlarının işletim sistemlerinin de incelenmesi ve mümkün olduğunca hepsinde standart bir işletim sistemi kullanımının sağlanması gerekmektedir. Çünkü belirlenecek iş akışları ve e-imza uygulamaları tamamen işletim sistemi üzerinde çalışacağından farklı işletim sistemleri için farklı uygulama ihtiyaçlarının doğması sistemin uyum ve birlikte çalışabilirliğini bozacaktır. Bu kapsamda e-imza kullanacak personelin bilgisayarları incelenmiş ve tamamının Microsoft Windows XP işletim sistemi kullandığı görülmüştür. Sonuç olarak bu işletim sistemi standart olarak kabul edilmiştir. Proje kapsamında kullanılacak tüm bilgisayarların bu işletim sistemi ile çalışması sağlanmıştır.

Kullanıcı bilgisayarlarının tipi

Kullanıcı bilgisayarları PC (personal computer, kişisel bilgisayar), unix terminal, thin client gibi çeşitli tiplerde olabilmektedir. Sistemin genelinde standardı ve uyumu sağlamak amacıyla kullanılacak kullanıcı bilgisayarlarının aynı tipte olması gerekmektedir. Yapılan inceleme sonucunda üniversite içinde proje kapsamında kullanılacak bilgisayarların PC tipinde olduğu ve bu konuda ilave bir gereksinim doğmadığı görülmüştür.

Sunucu modülleri

Üniversitede örnek e-imza uygulamalarının hayata geçirilebilmesi için dosya sunucu ve e-posta sunucu hizmetlerini verecek sunuculara ihtiyaç vardır. Dosya sunucu ile, e-imzalı belgelerin bilgisayar ortamında muhafaza edilmesi; e-posta sunucu ile de imzalı e-posta haberleşmesi hizmetinin verilmesi sağlanacaktır. Üniversite bünyesindeki mevcut sunucuların, proje kapsamında sunulacak hizmetleri vermek için yeterli olduğu görülmüştür. Bu sunuculara ilişkin bilgiler Çizelge 5.2'de sunulmuştur.

Çizelge 5.2. Sunucu modülleri

Sunucu Tipi	**İşletim Sistemi**	**Uygulama**	**Sunucu Adedi**
Dosya Sunucu	Windows 2003 Server	Microsoft File Server	1
E-posta	Windows 2003 Server	Exchange Server 2003	1

Sunucuların internet bağlantısı durumu

Proje kapsamında kullanılacak her iki sunucu bilgisayarda da internet erişimi mevcut olduğundan bu konuda ilave bir gereksinim doğmamıştır.

E-imza için kullanılacak yazılım ve sistem

Proje kapsamında bilgisayar ortamında muhafaza edilen/edilecek kurumsal belge ve verilerin elektronik olarak imzalanması işlemi Kamu SM tarafından geliştirilen "İmzager" yazılımı kullanılarak gerçekleştirilecektir. Bu nedenle söz konusu yazılımın sistemi kullanacak kullanıcı sayısına bağlı olarak tedarik edilmesi gerekmektedir.

Kurum içi haberleşmenin bilgisayar ortamında e-imzalı olarak yürütülmesi fonksiyonu ise, MS Outlook 2003 e-posta programının e-posta imzalama seçeneği kullanılarak gerçekleştirilecektir. Söz konusu program, sistemde kullanılacak bilgisayarlarda zaten mevcut olduğundan bu konuda ilave bir ihtiyaç doğmamıştır.

E-imza için kullanılacak donanım

Proje kapsamında e-imza kullanacak personelin tümünün sertifika ve anahtar çiftlerini güvenli bir şekilde muhafaza etmesi için kanuna uygun olarak GEİA kullanmaları gerekmektedir. Bu kapsamda GEİA olarak akıllı kart veya akıllı çubuk donanımlarında biri seçilmelidir. Her iki çözüm de benzer güvenlik özelliklerinde olmakla birlikte, akıllı çubuğun fiziksel boyutunun daha büyük olmasından dolayı

fiziksel saldırı yoluyla bilgilerinin açığa çıkarılması tehlikesi daha yüksektir.

Akıllı kart maliyetleri ortalama 15-25 YTL, okuyucu maliyetleri ise ortalama 25 YTL civarında olacaktır. Bu durumda akıllı kart temelli çözümün kurulum maliyeti ortalama 40 YTL olacak ve akıllı kartın yenilenmesi durumunda ilave kart maliyeti (ortalama 15-25 YTL) oluşacaktır. Akıllı çubuk maliyetleri ise ortalama 60 YTL civarındadır ve her yenilemede de aynı maliyet tekrarlanacaktır.

Gerek akıllı kartların ve gerekse okuyucuların yerli kaynaklarla üretilmesi yoluna gidildiğinde ilk sahip olma maliyetinin ortalama 20 YTL'ye, yenileme maliyetinin de 5 YTL'ye kadar düşebileceği; bunun yanında ülkede yaratılan katma değerin önemli bir artış göstereceği belirlenmiştir. Akıllı çubuklar ise tümüyle dış kaynaklı temin edilmekte ve yarattığı katma değer hayli düşük kalmaktadır. Akıllı kartların gerek fiziksel (fotoğraf basımı, kabartma ya da laser isim basımı, vb.) ve gerekse elektronik kişiselleştirme işlemleri (çip ilklendirme ve sertifika yükleme) yüksek kapasiteli makinelerle seri üretim düzeneğinde yapılabilmektedir. Ufak bir operasyon dahi hemen hiç operatör müdahalesi olmadan günde 10.000 kart üretebilecek kapasite oluşturabilir. Akıllı çubuklarda fiziksel kişiselleştirme mümkün olmayıp elektronik kişiselleştirme de elle yapılmak durumundadır. Çok iyimser tahminlerle bile günlük her 500 akıllı çubuk kişiselleştirilmesi için bir operatör gerekmektedir. Bu durumda akıllı çubuk işleme maliyeti de akıllı karta göre ortalama 1-2 YTL daha yüksek olacak ve bu ek maliyet sertifika ücretlerine yansıtılacaktır.

Tüm bu nedenlerle proje kapsamında üniversitede güvenli donanım aracı olarak akıllı kart kullanımının daha maliyet etkin olacağı değerlendirilmiştir. Uygun ve kullanışlı kart okuyucuların yaygınlaşması ile akıllı çubuğun tek avantajı olan taşınabilirlik de önemsiz duruma gelecektir.

Sonuç olarak proje kapsamında e-imza kullanması hedeflenen personel sayısı kadar akıllı kart; kullanılacak bilgisayar sayısı kadar da akıllı kart okuyucu ihtiyacı belirlenmiştir. İhtiyaç duyulan akıllı kart ve akıllı kart okuyucular sertifika alma

işlemleri sırasında Kamu SM'den tedarik edilecektir.

Sertifika hizmetleri

Sertifika hizmetleri kapsamında, güvenli e-imza uygulamalarında kullanılmak üzere kurum tarafından belirlenen personel adına, imza oluşturma verisi ve NES üretme, üretilen imza oluşturma verisi ile NES'i kişiselleştirilmiş akıllı kart üzerine yükleyerek sahiplerine elden teslim etme, NES'lerle ilgili iptal, yenileme gibi sertifika yönetimi işlemlerini yerine getirme hizmetlerinin alınmasına ihtiyaç vardır. Bu kapsamda alınacak hizmet Kamu SM'den tedarik edilecektir.

Üretilen NES'lerin ve ilgili imza oluşturma verilerinin yükleneceği akıllı kart ve akıllı kart okuyucular da Kamu SM'den temin edilecektir. Kamu SM, temin edeceği akıllı kartların, e-imza mevzuatında belirtilen güvenlik standartlarına uygun ürünler olduğunu garanti etmelidir.

Buna göre, e-imza kullanacak personelin sertifika hizmetlerini alabilmeleri için Bölüm 5.2'de anlatılan sürece göre kurum tarafından Kamu SM'ye NES başvurusunda bulunulması gerekmektedir.

Elektronik imza yazılımı temini

Elektronik sertifikaların bilgisayar sistemlerine tanıtılması ve e-imzalı metinlerin imza doğrulaması için çeşitli istemci yazılımları kullanılabilir. Bu yazılımlar uygulamaya özel geliştirilebileceği gibi, bu işlevi yerine getiren paket programlar da bulunabilir. Pek çok e-posta programı ve internet tarayıcısı da elektronik sertifika kullanım özelliklerine sahiptir.

En temel e-imza çözümleri masaüstü uygulamalar olup, bu uygulamalar çeşitli masaüstü dosyalarını (Microsoft Word, Excel, Adobe Acrobat, AutoCAD, text vb.) yasal ve güvenlik şartlarını yerine getirerek imzalamakta, başkalarına imzalı e-posta olarak gönderilmesini sağlamaktadır.

Ancak artan ihtiyaçlar, yaşanan tecrübeler ve gelişen teknolojiler sunucu bazlı e-imza çözümlerinin de gelişmesini ve diğerlerinin yerini almasını sağlamıştır. Böylece dinamik olarak web-bazlı belgeler yaratılabilmekte, onaylama ve imzalama sağlanabilmektedir. Detaylı ve imzalı denetleme raporu, saklama sağlanırken dahili ve harici taraflar ile (iş akış programları, kredi kurumu, noterler, sertifika hizmet sağlayıcıları) entegrasyon da sağlanmaktadır. Farklı kurumların güvenli e-imza oluşturmak için kullandığı yazılımların karşılıklı uyumunun sağlanabilmesi (bir kurum tarafından atılan e-imzanın başka bir kurum tarafından doğrulanabilmesi) için imza oluşturma ve doğrulama yazılımlarının ortak bir formata uygun olması gerekmektedir. Bu anlamda Kamu SM e-imza formatının ETSI TS 101 733 standartına uygun biçimde gerçekleştirilmesini uygun bulmaktadır. Avrupa Birliğinin belirlediği ilkelere uygun olarak tanımlanmış bir standart olan ETSI TS 101 733'ün Avrupa Birliği ülkeleri tarafından da uygulanması öngörülmüştür. E-imzaya geçmek isteyen kurumların öncelikli olarak imza oluşturma ve doğrulama işlemlerini gerçekleştireceği uygulama ortamlarının hazır olması gerekmektedir. Bu konuda gerekli hazırlıklarını tamamlamış olan kurumlar, Kamu SM veya konuyla ilgili diğer firmalardan ETSI TS 101 733 standardında geliştirilmiş e-imza oluşturma ve doğrulama yazılımlarını temin edebilir. Kurum temin ettiği bu yazılımları kendi uygulamasına entegre ederek kullanabilir.

Kamu SM'nin e-imza uyum desteğine ilişkin kurumsal başvuru adımları aşağıda sıralanmıştır:

1. Kurum, ETSI TS 101 733 standartında geliştirilmiş e-imza oluşturma ve doğrulama yazılımları talebini, içeriğinde e-imza yazılımlarının ücretlerinin belirtildiği teklifin kendisine ulaştırılması isteğini belirten resmi yazı ile Kamu SM'ye bildirir.
2. Kamu SM'nin başvuruyu değerlendirmesi, kurumun e-imza entegrasyonu için gerekli uygulama ortamına sahip olduğunun belirlenmesi yoluyla yapılır. Bu amaçla kuruma "E-İmza Uyumu Analiz Formu" e-posta ile gönderilerek, doldurulması istenir. Formda verilen bilgiler doğrultusunda kurumun e-imza uygulamasına geçmek

için gereken altyapıya sahip olup olmadığının değerlendirmesi yapılır. Bu aşamada gerekli hallerde kurum ile toplantı düzenlenerek kuruma verilecek hizmetler detaylandırılır. Gerekli altyapıya sahip olmadığı belirlenen kurumlar resmi yazı ile bilgilendirilerek söz konusu eksikleri tamamlandıktan sonra birinci adımdan itibaren işlemi tekrarlamaları istenir. Altyapılarının hazır olduğu belirlenen kurumlara Kamu SM tarafından e-imza yazılımlarının ücretlerinin ve hizmetin veriliş biçiminin belirtildiği resmi teklif gönderilir.

3. Kurumun, yapılan teklifi kabul ettiğine dair cevabını içeren resmi yazının Kamu SM'ye ulaşmasının ardından Kamu SM e-imza yazılımlarını kuruma iletir. Gerekli hallerde yazılımların kurumun uygulama ortamına entegrasyonunun sağlanması için Kamu SM tarafından teknik destek sağlanabilir.

Gazi Üniversitesi'nde gerçekleştirilecek örnek uygulama kapsamında, bilgisayar ortamında muhafaza edilen/edilecek kurumsal belge ve verilerin elektronik olarak imzalanması işlemi Kamu SM tarafından geliştirilen "İmzager MİM" yazılımı kullanılarak gerçekleştirilecektir. İmzalı e-posta heberleşmesi için de Microsoft Office programı kullanılacaktır.

Eğitim ve danışmanlık hizmetleri

E-imzaya geçiş projeleri kapsamında, sistemi kullanacak personel ve kurum sistem yöneticileri e-imza, elektronik sertifikalar ve AAA konularında eğitim almalıdır. Söz konusu eğitimler ya kurum sistem yöneticilerinin gerekli eğitimi almasından sonra kurum personeline eğitim vermesi yönünde ya da bu eğitim hizmetinin tüm personel için eğitim hizmeti veren ilgili kurumlardan satın alınması yönünde olabilir. Ayrıca, projenin hayata geçirilmesi ve proje kapsamında yaşanacak sorunların çözümü için ilgili kurumlardan danışmanlık hizmeti de alınmalıdır.

Bu tez çalışması, kurumsal ağlarda e-imza uygulamalarını hayata geçirmek isteyen tüm kurumlar için gerekli eğitim bilgilerini kapsamaktadır. İlgili sistem/proje yöneticilerinin bu tez çalışmasından istifade etmesinin ve bu kapsamda kendi

kullanıcı personeline de bilmesi gereken prensibine uygun olarak uygulama ağırlıklı eğitim vermesinin maliyet etkin bir çözüm olacağı değerlendirilmiştir.

Genel proje gereksinimleri

- Proje kapsamında belirlenen personel için Kamu SM'den alınacak 8 adet NES (akıllı kart ve akıllı kart okuyucular da bu kapsamda tedarik edilecektir),
  - 8 Adet E-İmza Kartı & Sertifikası
  - 8 Adet E-İmza Oluşturma-Doğrulama Aracı
- 8 Adet E-Posta Adresi ve Bağlantısı
- 8 Adet Tarayıcı (Scanner)
- 8 Adet Yazıcı (Printer)
- Proje kapsamında belirlenen personel için 8 adet kişisel bilgisayar,
  - İşletim sistemi Microsoft Windows XP SP2 olacaktır.
  - En az intel Pentium III-800 MhZ veya AMD Athlon 1700 işlemciye sahip olacaktır.
  - En az 128 MB Ram bulunacaktır.
  - En az 300 MB Boş disk alanı bulunacaktır.
  - USB Bağlantı noktası olacaktır.
  - İnternet erişimi olacaktır.
  - Akıllı kart okuyucu bulunacak ve akıllı kartların kullanımı için gerekli sürücü/yazılım yüklemesi yapılacaktır.
  - E-imzalı haberleşme için MS Outlook 2003 programı olacaktır. (Kurumun e-posta hizmeti mevcut E-posta sunucu ile sağlanmaktadır.)
  - Kullanıcıların bilgisayar ortamındaki belgelerini e-imzalamalarına imkan sağlayacak İmzager MİM yazılımı yüklü olacaktır.
  - Kullanıcıların akıllı kartlarının yönetimi ve parola değişikliği için İmzager AKAY programı yüklü olacaktır.
  - Kurumsal belgelerin ortak bir dosya sunucuda e-imzalı muhafazası için merkezi dosya sunucuya yetki dahilinde erişim imkanı olacaktır.

- Kurumsal dosya sunucu üzerinde her birim için sadece o birim personelinin yetki dahilinde girerek imzaladıkları belgeleri muhafaza edebilecekleri bir disk alanının tahsis edilmiş olması ve bu alana kaydedilen bilgilerin sürekli yedeklenebiliyor olması gerekmektedir.
- Kullanıcı personele sistemin kullanımı ve bu sistemde hangi iş süreçlerinin kullanılacağı konusunda eğitim verilecektir.

5.5.2. Analiz

Bu aşamada Üniversitede kurulacak e-imza sisteminin detaylı analizi yapılmaktadır.

E-imza uygulaması için proje kapsamının belirlenmesi

Henüz herhangibir e-imza uygulaması bulunmayan kurumda e-imzanın kullanılabileceği ya da entegre edilebileceği birçok alan ve iş akışı vardır. Öncelikle kurum bünyesinde e-imza kullanılabilecek iş akışları, hizmet ve uygulamalar listelenmiştir. Buradaki amaç, kurum personeli ve kurum ile çalışan diğer kurum, şirket ya da vatandaşın ilk anda ihtiyaç duyabileceği ve e-imzanın yararlarından en çok faydalanılabilecek bir liste oluşturmaktır.

Gazi Üniversitesi için bu amaçla hazırlanan e-imza kullanılabilecek iş akışları, hizmet ve uygulama alanları üç temel grup altında aşağıda listelenmiştir:

1. Kurum içi kullanım

a. Kurum içi yazışmalarda e-imza kullanımı,

b. Kurumda bulunan dokümanların e-imzalı olarak bilgisayar ortamında arşivlenmesi,

c. Kurum çalışanları ve öğrencilerle ilgili işlemlerin bilgisayar ortamında e-imzalı olarak yürütülmesi,

d. Kurum çalışanları ve öğrenciler tarafından yayımlanan bildiri ve makalelerin e-imzalı olarak yayımlanması ve zaman damgası ile imzalanması,

e. Kurum içinde geliştirilen yazılım ve projelerin elektronik olarak imzalanması,

f. Kurum sunucularında SSL sertifikası kullanımı yoluyla güvenliğin artırılması,

g. İşletim sistemi oturum açma işlemlerinde e-imza kullanımı ile güvenliğin artırılması.

2. Kurumlar arası kullanım

a. Diğer kurumlarla yapılan yazışmalarda e-imza kullanımı.

3. Vatandaşlarla/Öğrencilerle yapılan işlemler

a. Yüksek Lisans/Doktora müracat işlemlerinin e-imzalı olarak web ortamından yürütülmesi,

b. Öğrencilerin ders seçme ve kayıt yenileme işlemlerinin e-imzalı olarak web ortamından yürütülmesi,

c. Öğrenciler/öğrenci adayları ile üniversite arasında yapılan yazışma ve belge alış-verişinin e-imzalı olarak web ortamından yürütülmesi.

E-imza kullanım amacı ve hedeflenen kazanımların belirlenmesi

Öncelikle, belirlenecek iş süreçleri ve hedef kitle ile birlikte, hayata geçirilmesi planlanan e-imza uygulamalarının kullanım amacı ve bu projeden beklenen kazanımlar ortaya konulmalıdır. Böylelikle, yönetim/idari kademede e-imza projelerine ilişkin tereddütlerin giderilmesi ve projeye geçiş için onay makamı olan yönetim kademesinin projenin gerekliliği konusunda ikna edilmesi sağlanacaktır. Ayrıca bu projeleri kullanacak kullanıcıların da alışmış oldukları iş akışlarından farklı olarak hayatlarına girecek yeni bir iş akışına karşı direnç göstermelerinin önüne geçilmiş olacaktır.

Tez çalışması kapsamda Gazi Üniversitesi'nde simule edilecek örnek sistem, öncelikle üniversite içi bazı resmi yazışmaların kağıt ortamından kurtarılarak e-imza desteğiyle bilgisayar ortamına aktarılması şeklinde yapılmıştır. Bu kapsamda üniversite içinde e-imzanın kullanılacağı süreçler ve yöntemler aşağıdaki gibi belirlenmiştir:

1. Bilgisayar ortamında muhafaza edilen/edilecek kurumsal belge ve verilerin elektronik olarak imzalanması,
2. Kurum içi haberleşmenin bilgisayar ortamında e-imzalı olarak yürütülmesi.

Projenin hayata geçirilmesiyle elde edilecek kazanımlar aşağıda listelenmiştir:

1. Üniversite içi iş süreçleri elektronik ortama aktarılarak daha hızlı ve güvenilir hale gelecektir,
2. Çok yavaş yürüyen ve maliyeti daha fazla olan kağıt tabanlı ıslak imzalı süreçler ve kağıt stokları azalacaktır,
3. İş akışlarının bilgisayar ortamına aktarılması ile iş akışı takibi ve gerekli bir belgenin bulunması kolaylaşacaktır,
4. Bilgisayar ortamında yapılan işlemler için hukuksal geçerlilik oluşturulacaktır,
5. Gelişen ve değişen teknolojik standartlara uyum sağlanacaktır,
6. Belirlenen iş akışları için iş yapma maliyetleri düşecektir,
7. Personelin iş verimliliği artacaktır.

Proje takviminin belirlenmesi

Projeye ilişkin başlangıç tarihi 01.01.2006, bitiş tarihi 01.07.2006 olarak belirlenmiştir.

Proje kapsamında e-imza kullanacak kişi sayısı

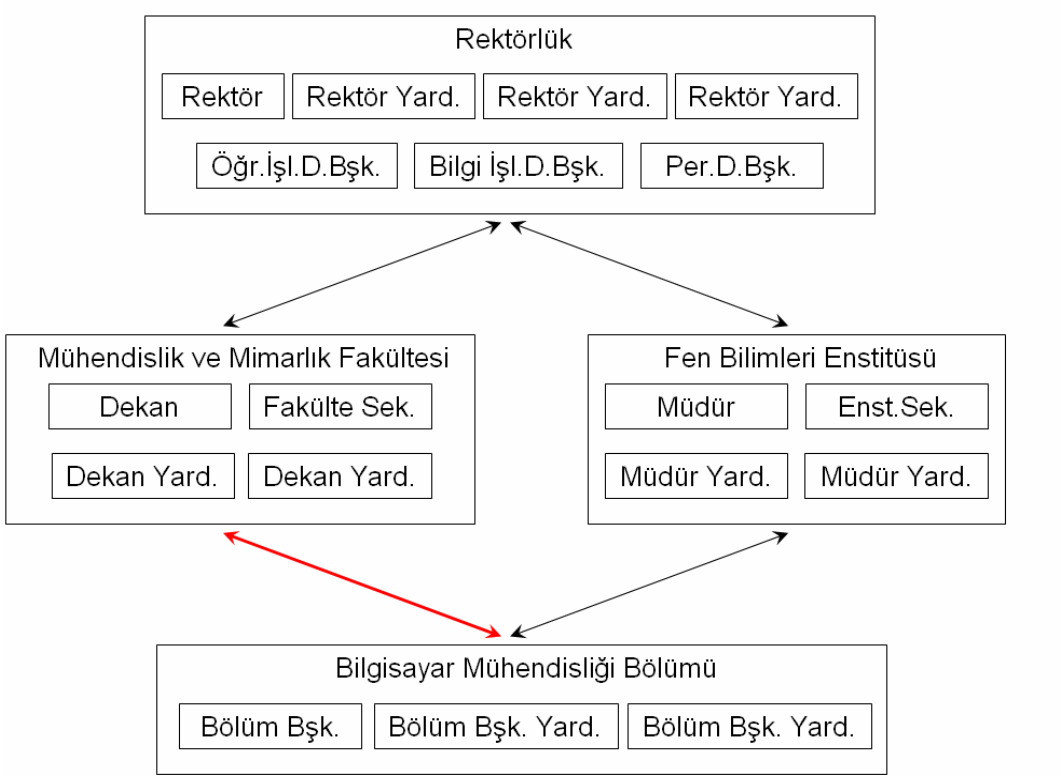
Proje kapsamında kurum içindeki resmi yazışmaları hazırlayan ve imza yetkisi olan personel sistemin öncelikli kullanıcıları olacaktır. Bu kapsamda üniversite içinde e-imza kullanması hedeflenen kişi sayısı, tüm idari ve akademik birimlerde yazışma yapan ve imza yetkisi olan personel olarak belirlenmiştir. Bu sayı toplam 18'dir. Şekil 5.5'te bu 18 personel hiyerarşik yapı içinde görülmektedir.

5.5.3. Tasarım

Bu aşamada, yukarıda gereksinimleri belirlenen ve analizi gerçekleştirilen sistemin tasarımı detaylı olarak anlatılmıştır.

Proje kapsamı

Gazi Üniversitesi e-imza geçiş projesi kapsamında simule edilecek örnek uygulama, öncelikle Şekil 5.1'de gösterilen Mühendislik ve Mimarlık Fakültesi Dekanlığı ve Bilgisayar Mühendisliği Bölümü arasındaki resmi yazışmalarda ve bu birimlerin elektronik ortamda muhafaza ettikleri bilgilerin imzalanmasında kullanılmıştır.



Şekil 5.1. Gazi Üniversitesi e-imza geçiş projesi örnek uygulama alanı

Bu aşamada Bölüm 3.7'de açıklanan kurumsal ağların e-imzaya geçiş modellerinden "Model I"de tanımlanan ve Şekil 5.2'de gösterilen özet işlem süreçleri kurum içi iş

akışında uygulanmıştır. Bu uygulamanın başarılı olması durumunda üniversitenin tüm birimlerine ve aşama aşama diğer iş akışı ve uygulamalarına yaygınlaştırma faaliyeti gerçekleştirilebilecektir.

Şekil 5.2. Örnek uygulama özet işlem süreçleri

Örnek uygulamada, seçilen birimlerden imza atma yetkisine sahip olan ve evrak hazırlayan toplam 8 personelin sistemi kullanmaları sağlanmıştır. Bu personelin görev odaklı listesi aşağıdadır:

- Mühendislik ve Mimarlık Fakültesi Dekanı,
- Mühendislik ve Mimarlık Fakültesi Dekan Yardımcısı,
- Mühendislik ve Mimarlık Fakültesi personeli (2 adet),
- Bilgisayar Mühendisliği Bölüm Başkanı,
- Bilgisayar Mühendisliği Bölüm Başkanı Yardımcısı,
- Bilgisayar Mühendisliği Bölümü personeli (2 adet).

E-imza için kullanılan yazılım ve sistem

Proje kapsamında bilgisayar ortamında muhafaza edilen/edilecek kurumsal belge ve verilerin elektronik olarak imzalanması işlemi, Kamu SM tarafından geliştirilen "İmzager MİM" yazılımı kullanılarak gerçekleştirilmiştir.

Kurum içi haberleşmenin bilgisayar ortamında e-imzalı olarak yürütülmesi ise MS Outlook 2003 e-posta programının e-posta imzalama seçeneği kullanılarak gerçekleştirilmiştir.

Ayrıca kullanıcıların akıllı kartlarının yönetimi ve parola değişikliği işlemlerini daha kolay yapabilmesi için "İmzager AKAY" yazılımı kullanılmıştır.

E-imza için kullanılan donanım

Proje kapsamında sistemi kullanacak personelin sertifika ve anahtar çiftlerinin güvenli muhafaza ve kullanımı için akıllı kart kullanılmıştır. Akıllı kartlar ile bilgisayarlarda işlem yapabilmek için proje kapsamında kullanılacak tüm bilgisayarlarda akıllı kart okuyucu bulunması da gerekmektedir. İhtiyaç duyulan akıllı kart ve akıllı kart okuyucular sertifika alma işlemleri sırasında Kamu SM'den tedarik edilmiştir.

Sertifika hizmetleri

Proje kapsamında e-imza kullanacak personelin tümü için Kamu SM'ye Bölüm 5.2'de anlatılan sürece göre başvuru yapılarak NES satın alınmıştır. Akıllı kart ve akıllı kart okuyucuları da bu aşamada tedarik edilmiştir.

Proje takvimi

Belirlenen örnek çalışma 6 ayda tamamlanmış ve bu süre sonunda yaygınlaştırma planı belirlenmiştir. Örnek çalışma kapsamında gereksinim belirleme ve analiz

aşamaları 2 hafta, tasarım aşaması 4 hafta, gerçekleştirim aşaması 8 hafta ve test aşaması 10 hafta sürmüştür.

5.5.4. Gerçekleştirim

Bu aşamada, yukarıda gereksinimleri belirlenerek tedarik edilen, analiz ve tasarımı gerçekleştirilen sistemin kullanıma hazır hale gelebilmesi için yapılan işlemler ve sistemin nasıl kullanılacağı detaylı olarak anlatılmıştır.

Projeye ilişkin kurum içi mevzuatın hazırlanması

Sistemin hangi tür resmi yazışmalarda ve hangi belgelerin e-imzalı muhafazasında nasıl kullanılacağı, bilgilerin nerede/nasıl muhafaza edileceği, NES başvurularının nasıl yapılacağı, sertifika yönetimi ile ilgili senaryolar (anahtarların kaybedilmesi durumunda nasıl yenileneceği, anahtar sahibinin ortadan kaybolması durumunda nasıl bir süreç ile anahtarların yetkinliğinin ortadan kaldırılacağı vb.), kullanıcıların yetki ve sorumlulukları vb. tüm ayrıntıları içerecek şekilde kurum içi e-imza sistemi kullanım talimatı hazırlanarak kullanıcı personele dağıtılmıştır.

Kullanıcı eğitimlerinin verilmesi

5070 sayılı E-İmza Kanunu, geleneksel imzanın hukuki, idari, ticari vb. ortamlarda kullanım amacını genişletip, elektronik ortamda da kullanılmasına olanak sağlamaktadır. Fakat konu hakkında bilinen yanlışların başında, kağıt ortamında kullanılan imzanın bir tarayıcı tarafından taranıp, elektronik ortamda saklanması ve kullanılması gibi algılanması gelmektedir. Hatta bu yanlış algılamanın, üretilen ve kullanılan örneklerine de rastlanmaktadır. Kullanıcıların bu konuda aydınlatılması, kullanıcıya yönelik olarak eğitim dokümantasyonunun (kitap, kitapçık, broşür, video, sunum vb.) hazırlanması ve bu konudaki standartların belirlenmesi, özellikle sertifika sahiplerinin sistemin işleyişi hakkında sağlıklı bilgilendirilmesi gereklidir.

E-imzanın, günlük hayatta kullanılan imzanın yerine geçmesi için belirli bir SM tarafından verilmesi ve kullanım anında onaylanması gerekmektedir. Bu alandaki kullanıcıları ilgilendirecek bölüm, bu imzaların hangi şekilde üretileceği, nereye müracaat edileceği, nasıl saklanacağı ve nasıl kullanılacağı ile ilgilidir.

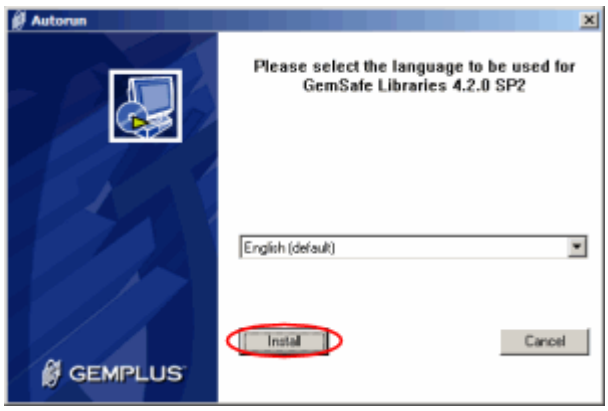
Tüm bu açıklamalar dikkate alındığında, kullanıcıların e-imzalar konusunda bilgilendirilmesi gerekmektedir. Kullanıcılar, teknolojinin kullanımından gelen ek güvenlik problemleri ve bunlara karşı e-imzanın getirdiği güvenlik çözümleri konusunda bilgilendirilmiştir.

Akıllı kart okuyucuların bilgisayarlara tanıtılması

Bu bölümde, kullanıcılara ait sertifika ve anahtar çiftlerini muhafaza eden akıllı kartların bilgisayarlarda kullanılabilmesi için gerekli akıllı kart okuyucuların bilgisayarlara kurulumu anlatılmıştır. Bu kurulum işlemi GemPlus marka bir akıllı kart okuyucu kullanılarak gerçekleştirilmiştir.

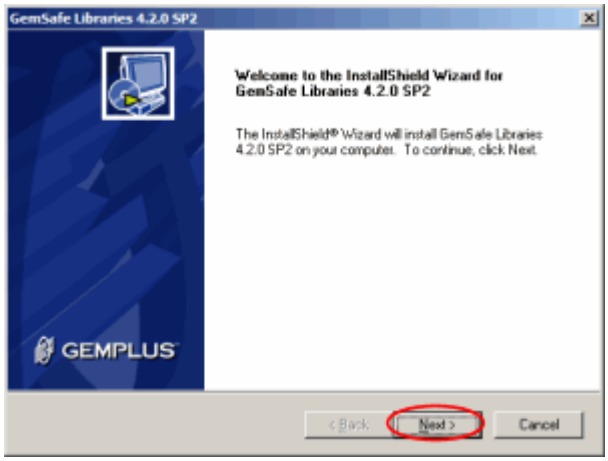
Akıllı kart okuyucu kurulumunun yapılabilmesi için öncelikle akıllı kart okuyucusuyla birlikte verilen akıllı kart okuyucu kurulum CD'si bilgisayara takılmalıdır. CD bilgisayara takıldığında otomatik olarak kurulum başlayacaktır. Kurulumun ayrıntılı adımları aşağıdadır:

1. Kuruluma başlandığında ilk olarak Şekil 5.3'deki dil seçim ekranı gelmektedir. Bu ekranda eğer farklı bir dil tercihi yoksa mevcut seçime dokunmadan "Install" butonuna basılmalıdır.



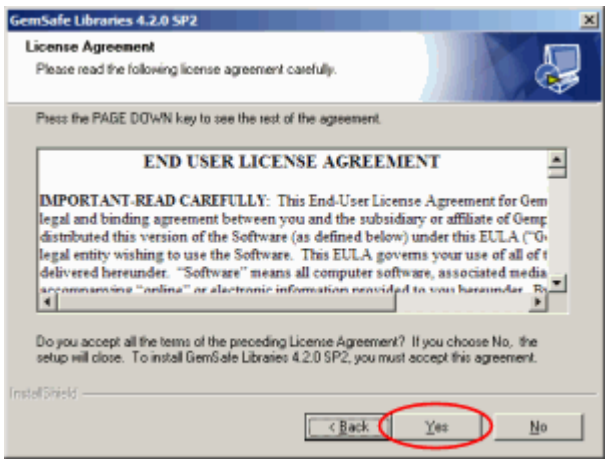
Şekil 5.3. Akıllı kart okuyucu kurulum adımları (adım 1)

2. Gelen Şekil 5.4'deki ekranda doğrudan "Next" butonuna basılarak kuruluma devam edilir.



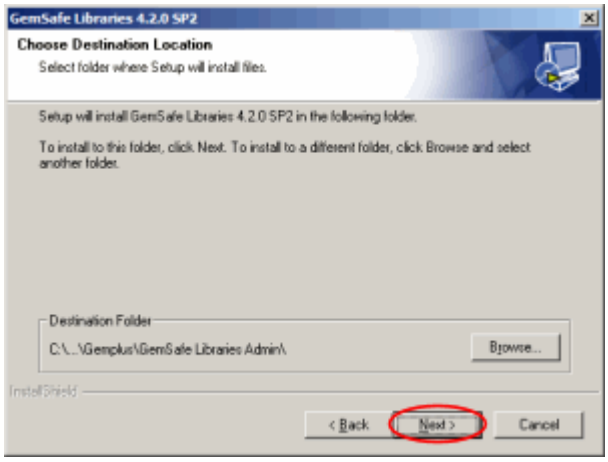
Şekil 5.4. Akıllı kart okuyucu kurulum adımları (adım 2)

3. Şekil 5.5'deki ekranda, kurulumdan önce kullanıcı tarafından okunarak kabul edilmesi gereken "Son Kullanıcı Lisans Antlaşması" bulunmaktadır. Kuruluma devam edebilmek için burada yazılanların kabul edilmesi gerekmektedir. Bunun için "Yes" butonuna basılarak kuruluma devam edilir.



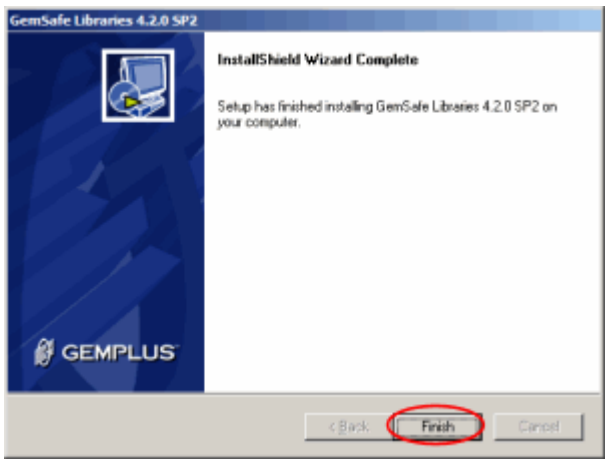
Şekil 5.5. Akıllı kart okuyucu kurulum adımları (adım 3)

4. Şekil 5.6'daki ekranda, uygulamanın sabit disk üzerinde kurulacağı dizin sorulmaktadır. Eğer uygulama standart dizin dışında başka bir yere kurulacaksa gerekli değişiklik bu ekranda yapılabilir. Standart kuruluma devam etmek için "Next" butonuna basılır. (Bu adımdan sonra kurulum işlemi 2-10 dakika sürebilir.)



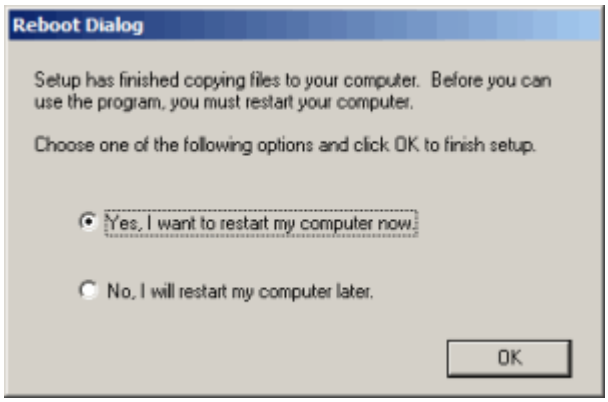
Şekil 5.6. Akıllı kart okuyucu kurulum adımları (adım 4)

5. Kurulum tamamlanmış durumdadır. Şekil 5.7'deki "Finish" butonuna basılarak kurulum ekranı kapatılır.



Şekil 5.7. Akıllı kart okuyucu kurulum adımları (adım 5)

6. Tamamlanan kurulum işlemi sonucunda bilgisayarın değişmiş olan tüm ayarlarının geçerli olması için bilgisayarın kapatılıp yeniden açılması gerekmektedir. Bunun için gelen Şekil 5.8'deki ekranda "OK" butonuna basılarak bilgisayar yeniden başlatılır.



Şekil 5.8. Akıllı kart okuyucu kurulum adımları (adım 6)

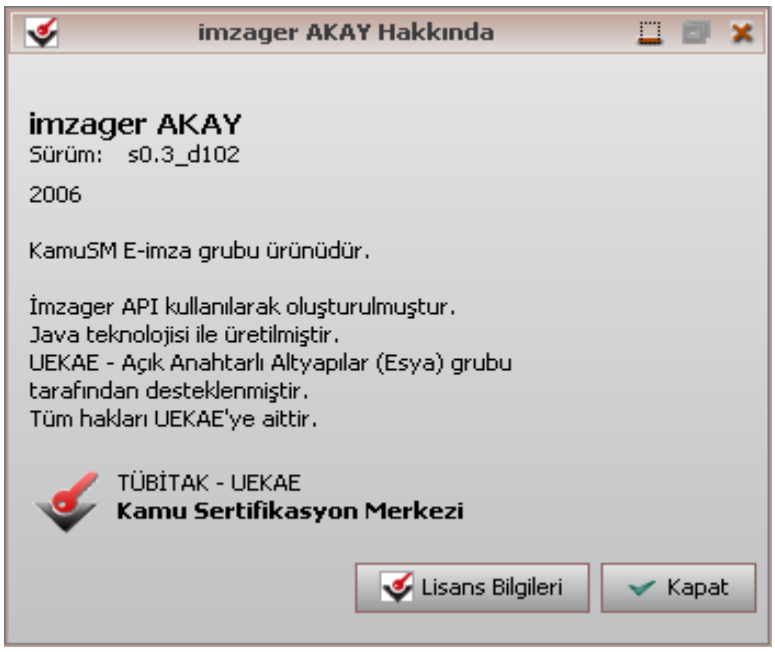
İmzager AKAY yazılımı ile akıllı kart yönetimi

Akıllı kart okuyucu kurulumu yapıldıktan sonra sistemde kullanılacak akıllı kartlar bilgisayarlarda kullanılabilir hale gelmiştir. Ancak akıllı kart ile ilgili bazı işlemlerin yapılabilmesi için yardımcı yazılımlara ihtiyaç duyulmaktadır. Bu amaçla akıllı kart

veya akıllı kart okuyucu ile birlikte gelen, ürüne özel yazılımlar kullanılabileceği gibi Kamu SM tarafından geliştirilen İmzager Akıllı Kart Yönetim Yazılımı (İmzager AKAY) da kullanılabilir.

Gazi Üniversitesi'nde yapılan örnek uygulama kapsamında İmzager AKAY yazılımı kullanılmıştır. İmzager AKAY yazılımının açılışı ekranı Şekil 5.9'da, yazılım hakkında bilgi veren ekran da Şekil 5.10'da gösterilmiştir.

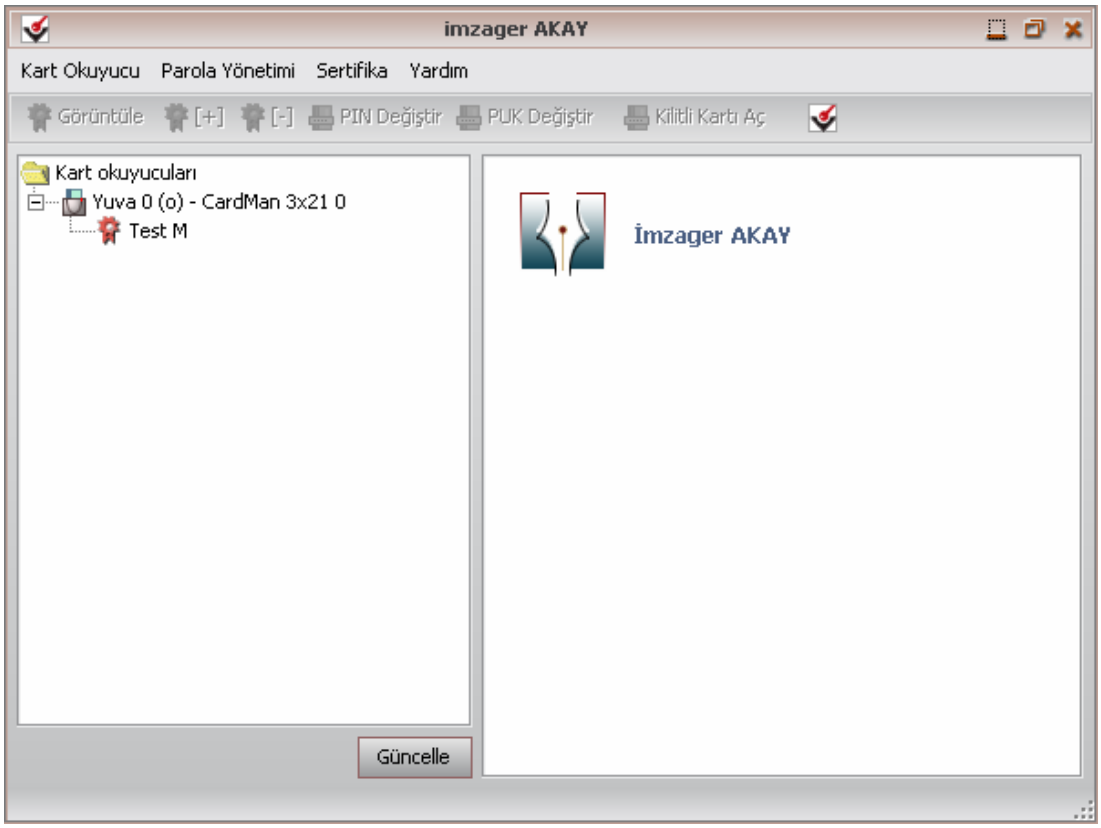
Şekil 5.9. İmzager AKAY yazılımı açılış ekranı



Şekil 5.10. İmzager AKAY yazılımı hakkında ekranı

İmzager AKAY yazılımının ana ekranı Şekil 5.11'de verilmiştir. Yazılımın temel fonksiyonlarını içeren bu ekrandaki menüler yardımıyla kart okuyucu, akıllı kart parola yönetimi ve sertifikalarla ilgili işlemler yapılabilmektedir.

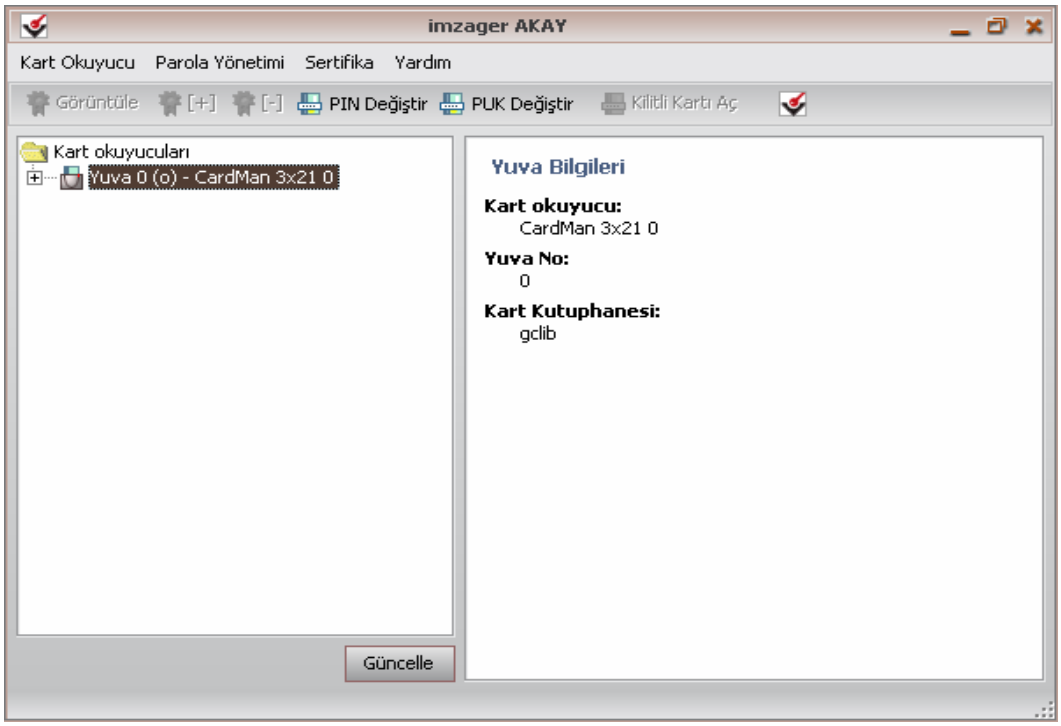
İmzager AKAY, akıllı kart ile ilgili işlemler için kullanılır. Bu arayüz ile bilgisayara bağlı kart okuyucular görülebilir, araç çubuğundaki düğmeler yardımıyla PIN (Personal Identification Number - User PIN) ve PUK (Personal Unblocking Key - Admin PIN) değiştirebilir ve seçili sertifika "Görüntüle" düğmesiyle görüntülenebilir. İmzager AKAY ekranı açık olduğu sırada bilgisayara eklenen/çıkarılan kart okuyucuları ya da akıllı kartları takip edebilmek için "Güncelle" düğmesi kullanılır.



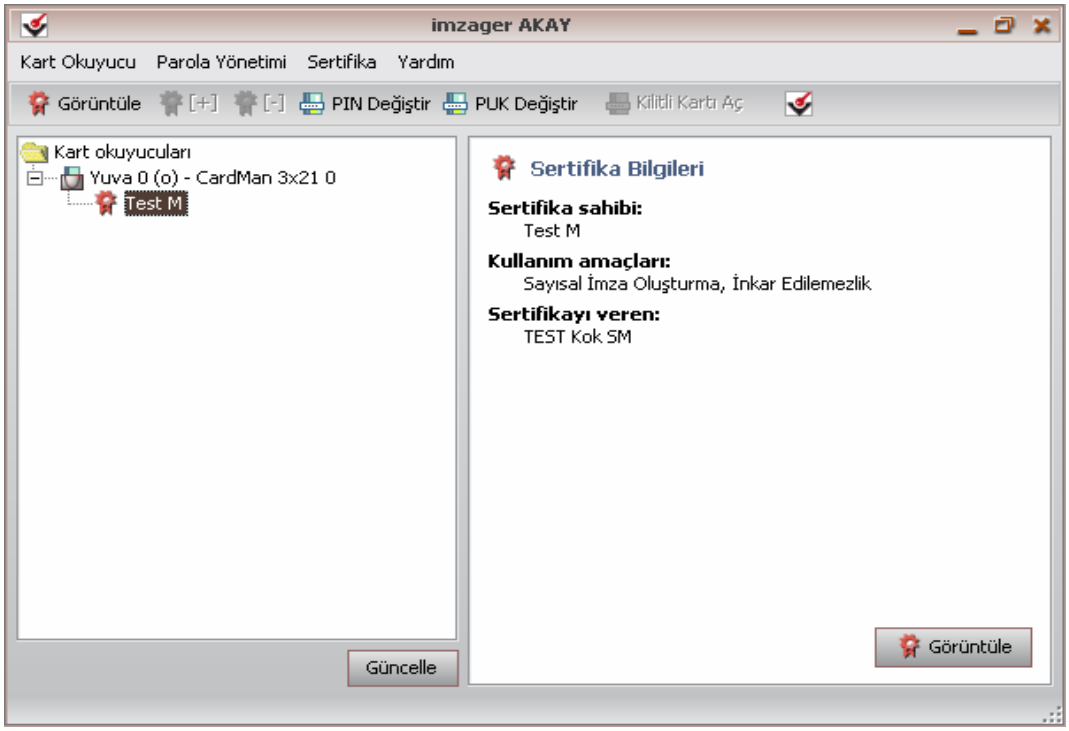
Şekil 5.11. İmzager AKAY yazılımı ana ekran görüntüsü

Şekil 5.12'deki ekran üzerinde görülen yuva ikonuna tıklanarak yuva bilgilerine erişilebilir. "Ayarlar" menüsündeki "Akıllı Kartlarım" seçildiğinde "Akıllı kart

yönetimi (AKAY)" arayüzü açılır. Kart ile ilgili işlemleri yapmak için bu arayüz kullanılır. Ayrıca aynı yerde sertifika ikonuna tıklanıldığında da Şekil 5.13'de gösterilen aynı arayüz açılır.

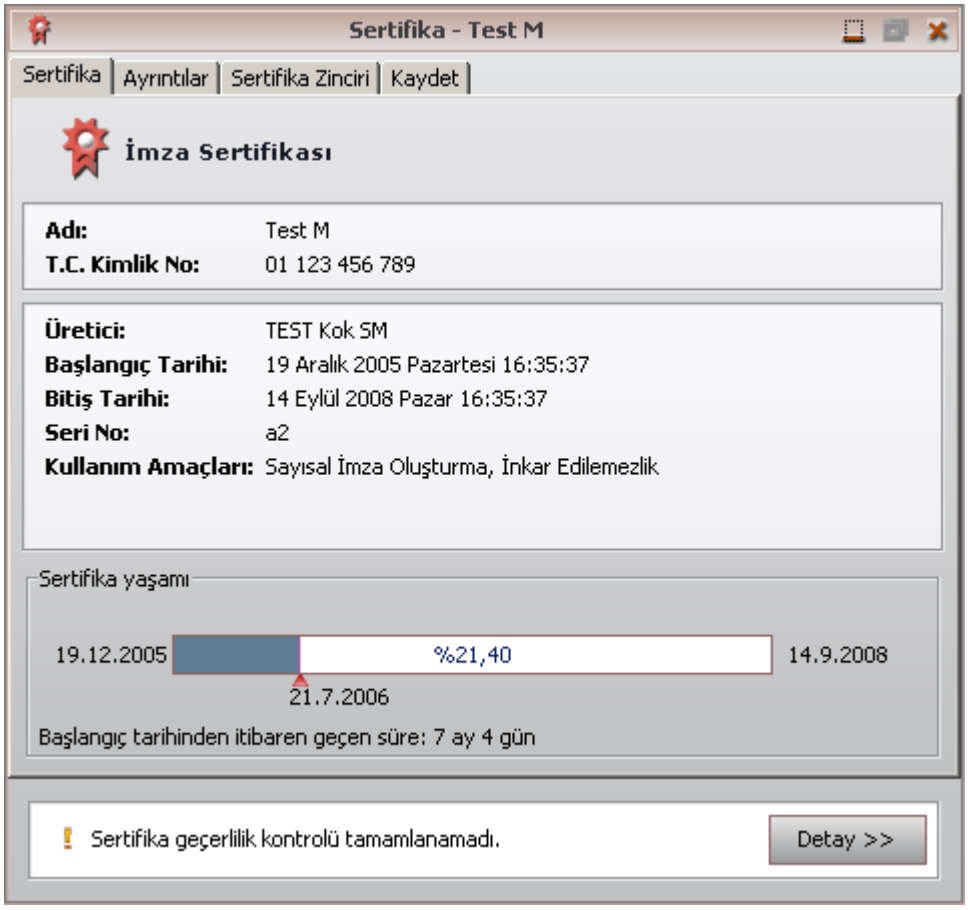


Şekil 5.12. İmzager AKAY yazılımı ana ekran görüntüsü (yuva)



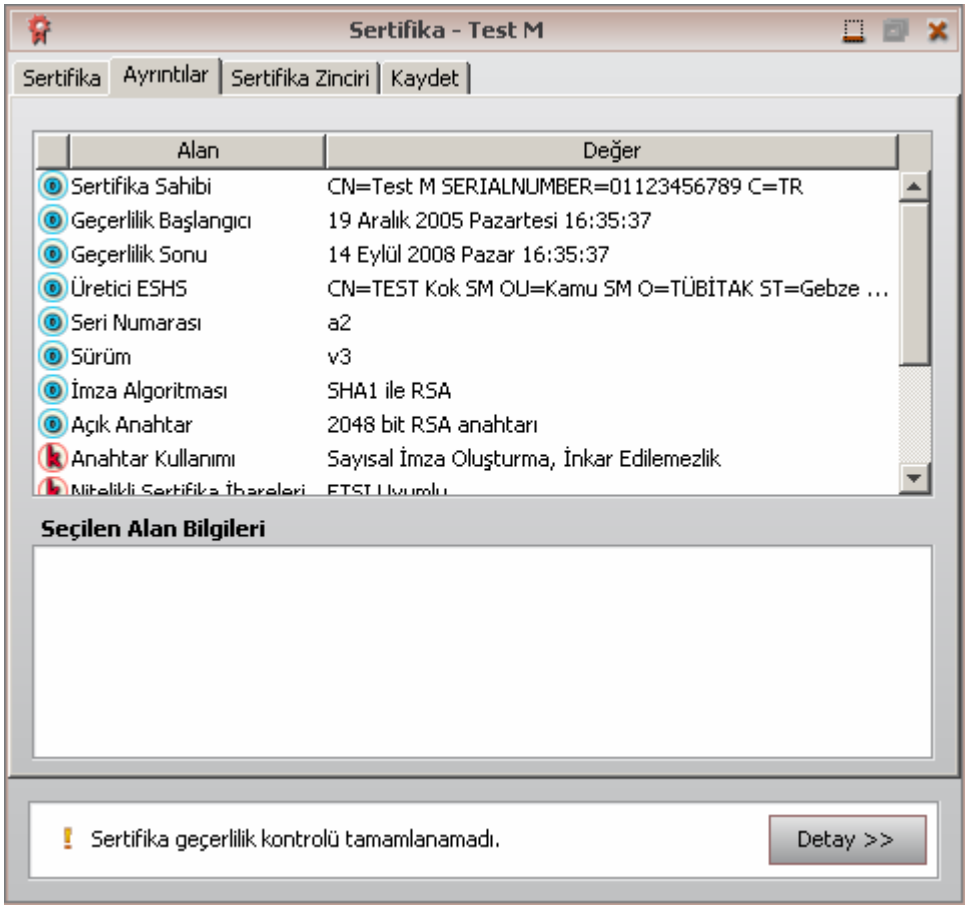
Şekil 5.13. İmzager AKAY yazılımı ana ekran görüntüsü (sertifika)

Sertifika bilgilerinin görüldüğü Şekil 5.13'deki pencerede "Görüntüle" butonuna tıklandığında, seçilen sertifikaya ilişkin detaylı bilgilere erişilebilir. Şekil 5.14'de görülen ekran ile gelen bu bilgiler "Sertifika", "Ayrıntılar", "Sertifika Zinciri" ve "Kaydet" grupları altında sunulmuştur. İlk olarak "Sertifika" grubu altında sertifika sahibinin adı, T.C. kimlik numarası, sertifika üreticisinin adı, sertifika başlangıç/bitiş tarihleri, kullanım amaçları ve sertifika ömrü bilgileri görülmektedir.



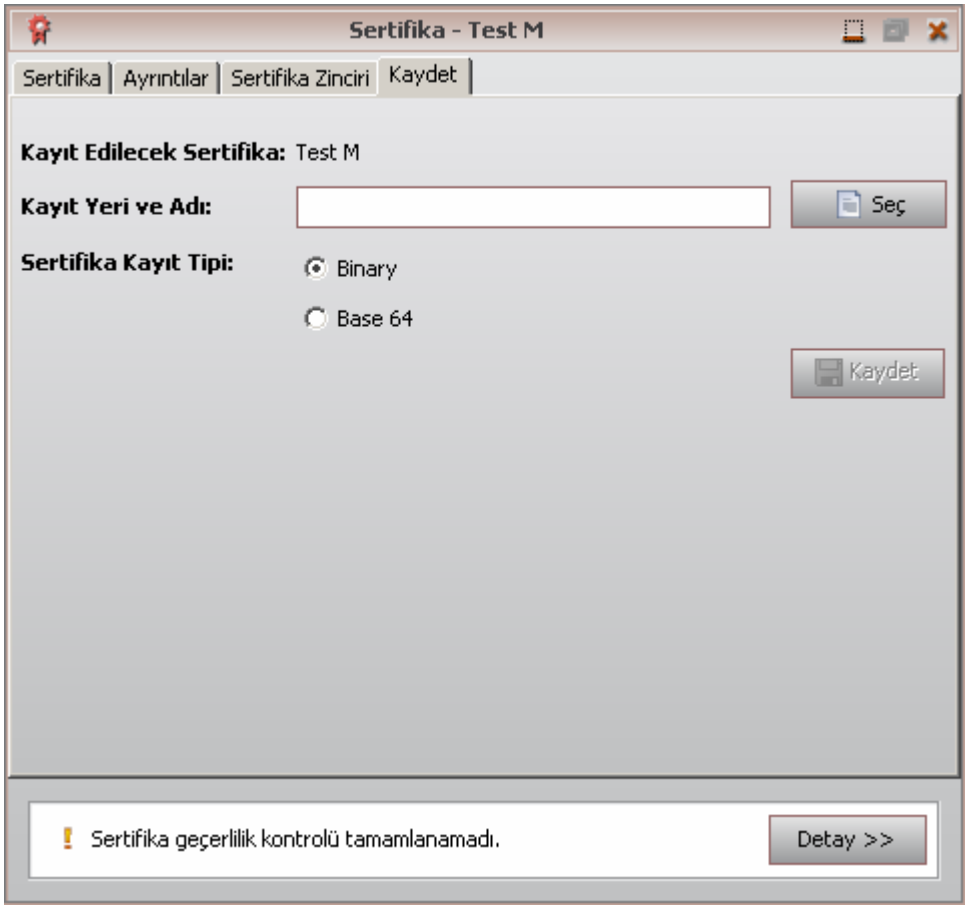
Şekil 5.14. İmzager AKAY yazılımı sertifika ekranı (sertifika)

Ayrıntılar alanında ise sertifikaya ilişkin daha ayrıntılı ve teknik bilgilere erişilebilir. Ayrıntılar alanında bulunan bilgilere ilişkin ekran görüntüsü Şekil 5.15'de sunulmuştur.



Şekil 5.15. İmzager AKAY yazılımı sertifika ekranı (ayrıntılar)

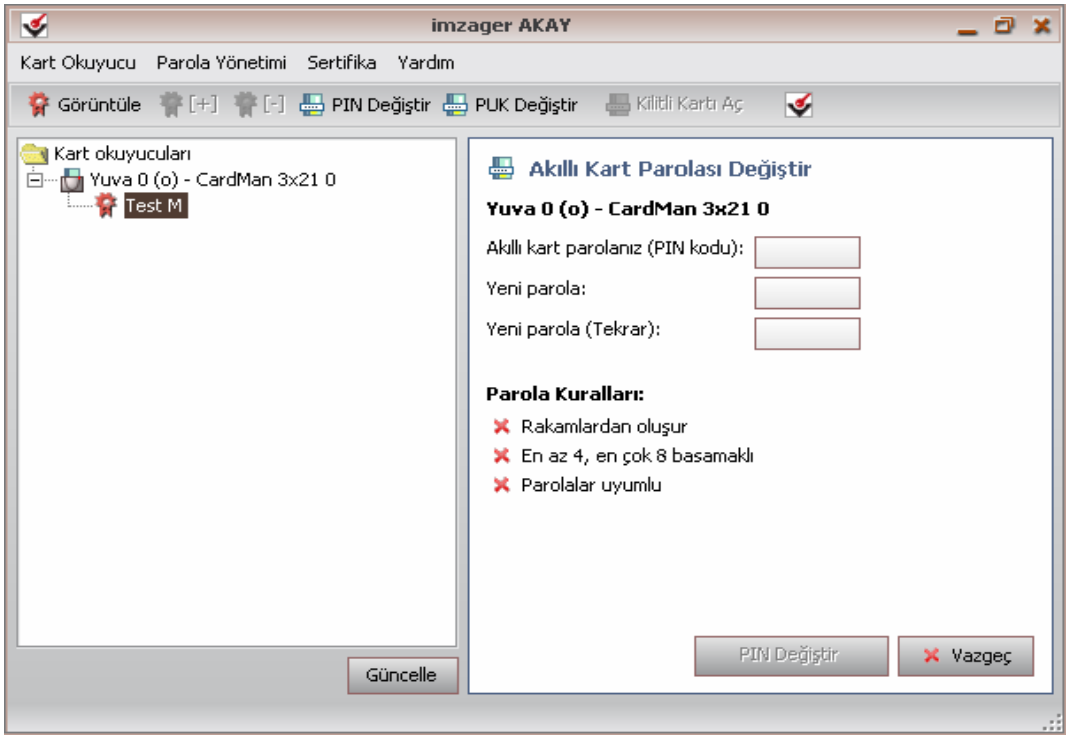
Sertifika bilgileri ekranında “sertifika zinciri” alanına tıklandığında ilgili sertifikaya ilişkin SM ve KSM bilgilerine erişilirken “kaydet” alanına tıklandığında ise Şekil 5.16’daki ekran açılır. Bu ekran yardımıyla ilgili sertifika istenilen alana kaydedilebilir.



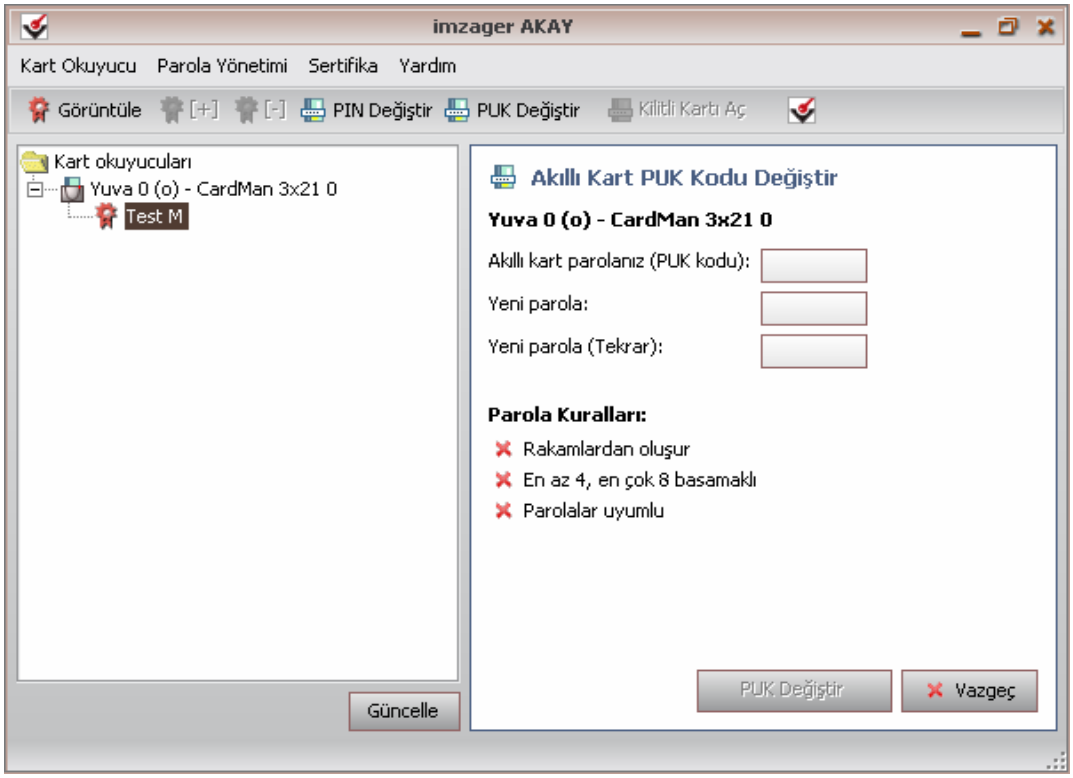
Şekil 5.16. İmzager AKAY yazılımı sertifika ekranı (kaydet)

İmzager AKAY yazılımında kullanıcıların en çok kullanacağı fonksiyonlar parola yönetim ile ilgili olanlardır. Akıllı kartların 2 adet şifresi bulunmaktadır. Bunlar PIN ve PUK şifreleridir. PIN şifresi, kartın e-imza işlemleri yapmak için kullanacağı şifredir. PUK şifresi ise PIN şifresinin unutulması ya da kartın geçici olarak bloke olması durumunda yeni bir PIN şifresi belirlemek için kullanılabilecek şifredir.

Her iki şifre de kart kullanılmadan önce kullanıcı tarafından kolay hatırlanabilecek bir şifre ile değiştirilmelidir. Bu şifreler 4 ila 8 basamaklı ve ard arda tekrar edilmeyen sayılardan oluşmalıdır. İmzager AKAY yazılımı kullanılarak PIN şifresi değiştirmek için kullanılan ekran Şekil 5.17'de, PUK şifresi değiştirmek için kullanılan ekran ise Şekil 5.18'de sunulmuştur.



Şekil 5.17. İmzager AKAY yazılımı parola yönetimi pin girişi



Şekil 5.18. İmzager AKAY yazılımı parola yönetimi puk girişi

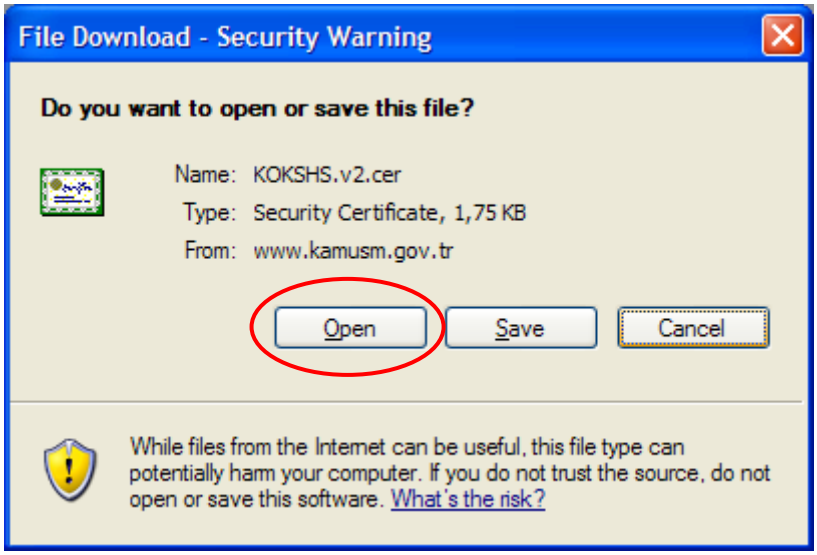
Kök sertifikaların kurulumu

E-imza kullanılmaya başlamadan önce e-imzanın üretilmiş olduğu güncel kök ve alt kök sertifikaları, ilgili bilgisayarlara yüklenmelidir. Kamu SM, üretmiş olduğu kök ve alt kök sertifikalarını web sayfasında yayınlamaktadır. Bu kapsamda e-imza ile işlem yapabilmek için yüklenmesi gereken 3 adet sertifika mevcuttur. Bunlar aşağıda listelenmiştir:

- TÜBİTAK-UEKAE Kök Sertifika Hizmet Sağlayıcısı Sertifikası
- TÜBİTAK-UEKAE Kamu ESHS Sertifikası
- TÜBİTAK-UEKAE Cihaz Sertifikası Hizmet Sağlayıcısı Sertifikası (gerekirse)

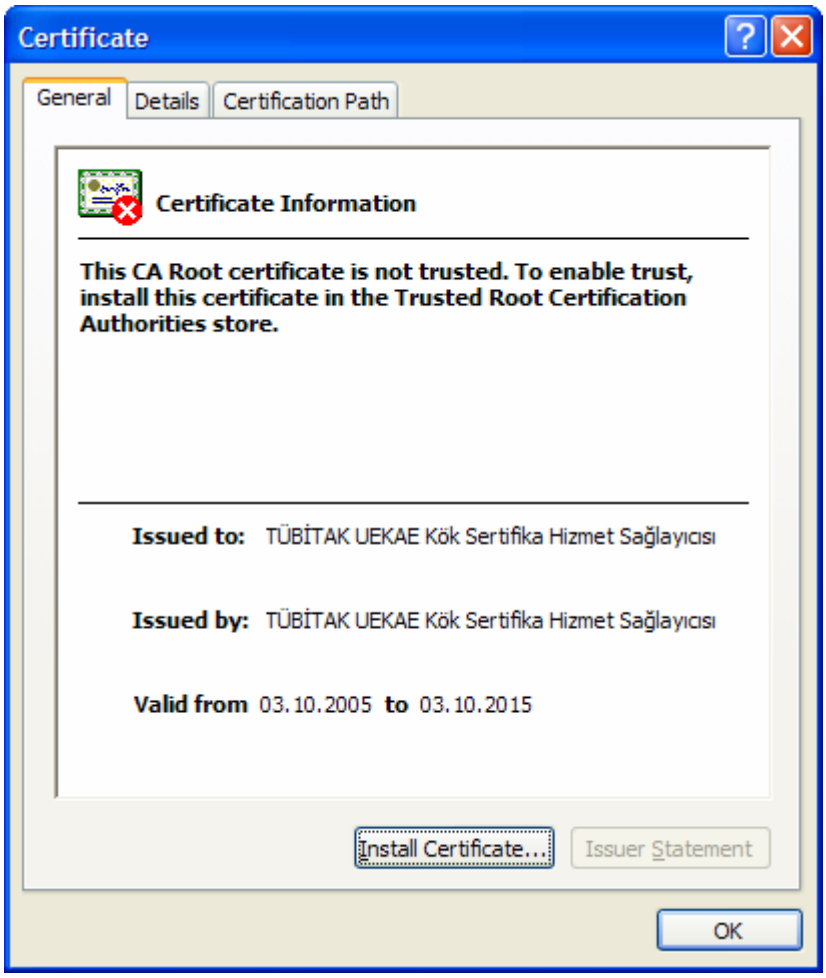
İlgili sertifikaları bilgisayara yükleyebilmek için Kamu SM web sayfasında ilgili sertifikaların üzerine tıklanarak aşağıdaki işlemler her sertifika için ayrı ayrı gerçekleştirilir:

1. Sertifika linkinin üzerine tıklandıktan sonra gelen ve Şekil 5.19'da gösterilen ekranda "Open" butonuna basılır.



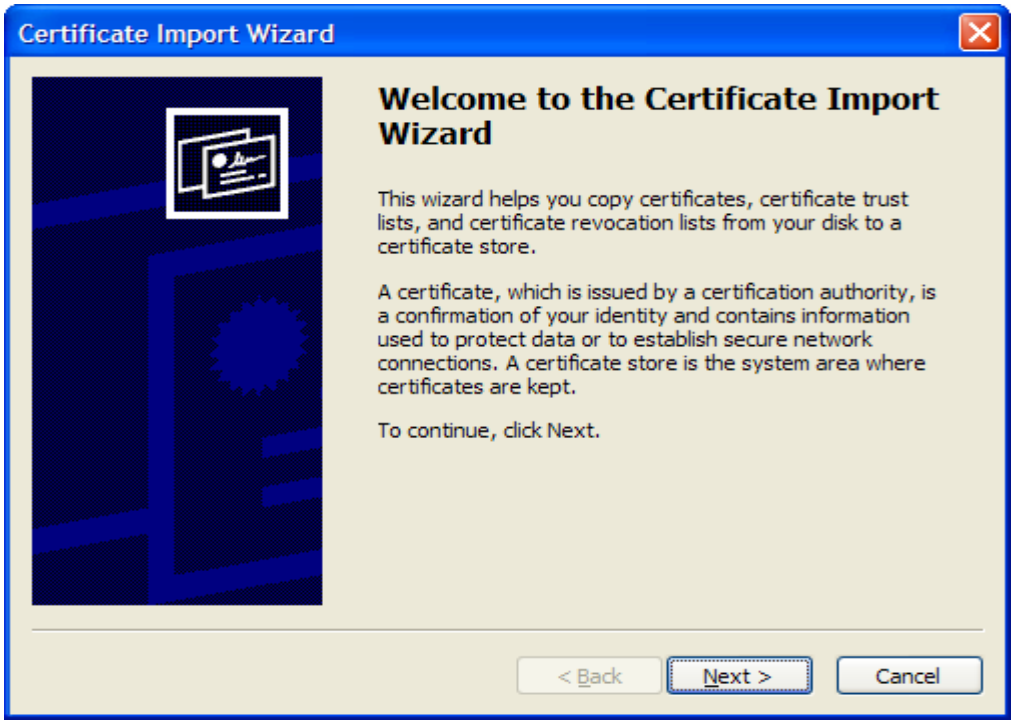
Şekil 5.19. Kök sertifikaların kurulumu (adım 1)

2. Şekil 5.20'de gösterilen sertifika ekranında "Install Certificate" butonuna basılır.



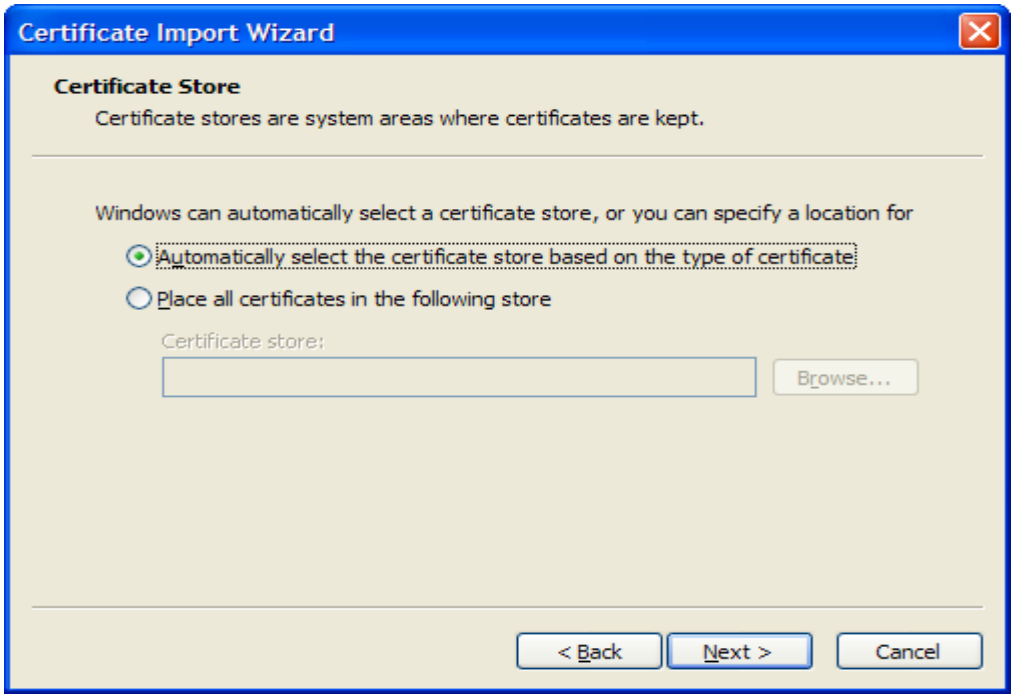
Şekil 5.20. Kök sertifikaların kurulumu (adım 2)

3. Sertifika yükleme sihirbazı otomatik olarak başlayacaktır. Şekil 5.21'deki ekranda "Next" butonuna basılarak devam edilir.



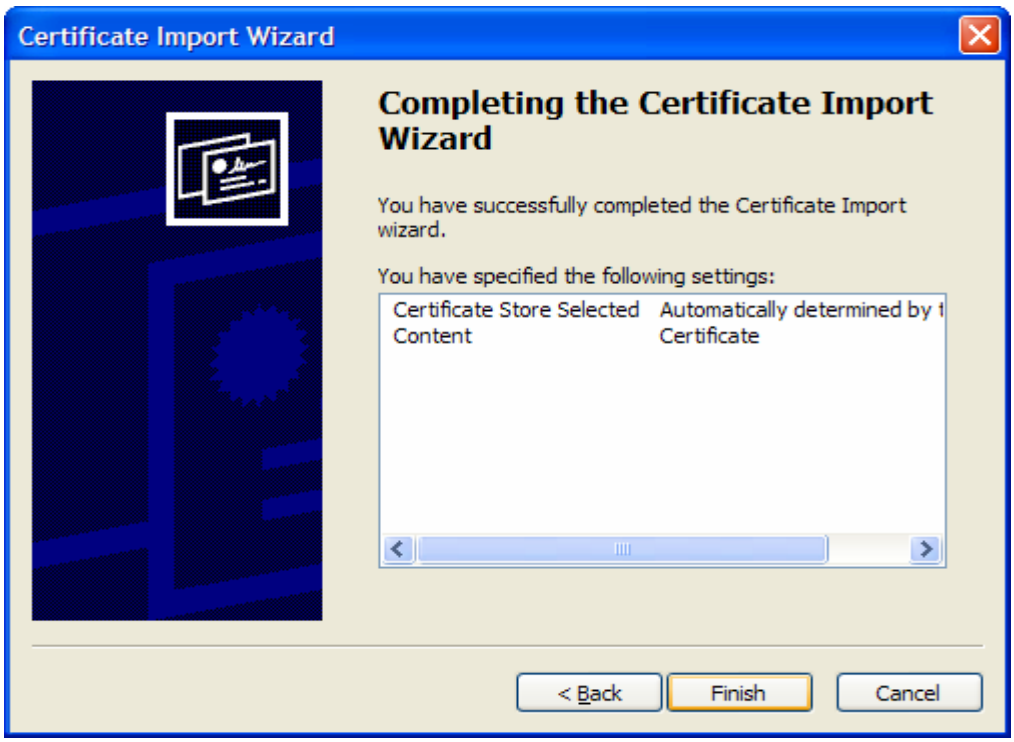
Şekil 5.21. Kök sertifikaların kurulumu (adım 3)

4. Şekil 5.22'deki ekranda kök sertifikanın bilgisayar tarafından depolanacağı alan seçimi yapılabilir. Varsayılan yere depolamanın yapılması için herhangi bir değişiklik yapmadan "Next" butonuna basılarak devam edilebilir.



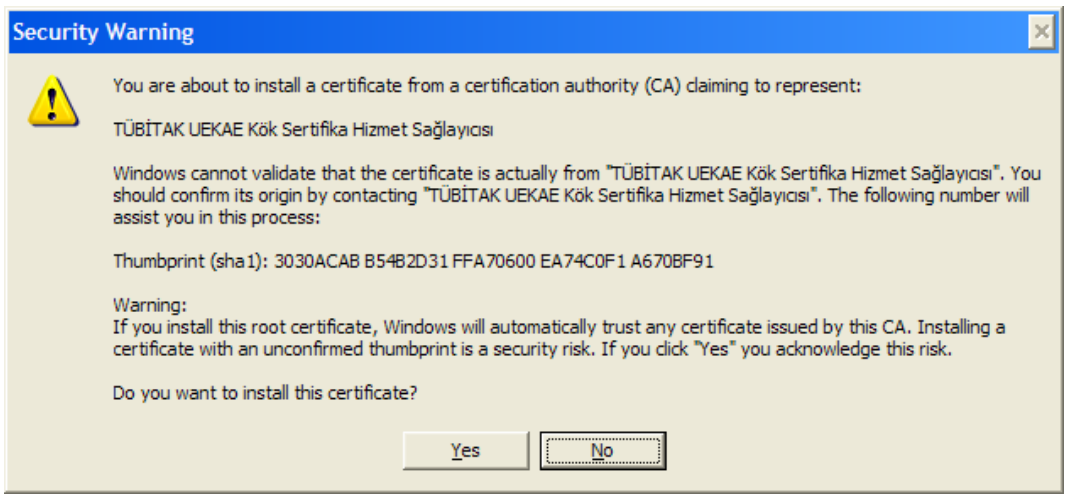
Şekil 5.22. Kök sertifikaların kurulumu (adım 4)

5. Kök sertifikanın bilgisayara yüklenmesi işlemi tamamlanmıştır. Şekil 5.23'te verilen ekranda "Finish" butonuna basılarak kök sertifika kurulum işlemi tamamlanır.



Şekil 5.23. Kök sertifikaların kurulumu (adım 5)

6. Kök sertifika kurulumunda Şekil 5.24'deki gibi bir güvenlik uyarısı ile karşı karşıya kalınması durumunda "Yes" butonuna basılmalıdır.

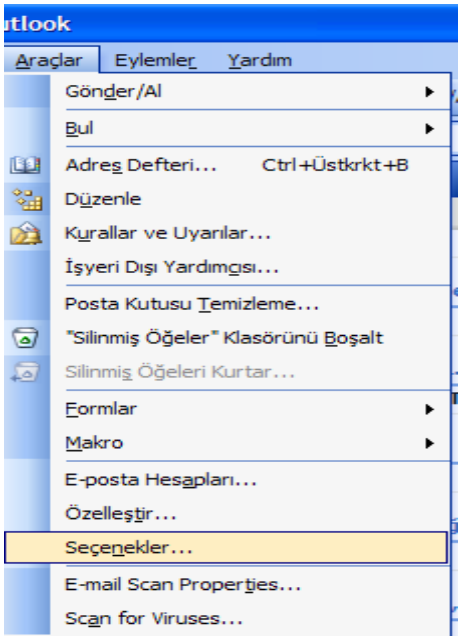


Şekil 5.24. Kök sertifikaların kurulumu (adım 6)

Microsoft Office Outlook 2003 programı ile e-imzalı haberleşme uygulaması

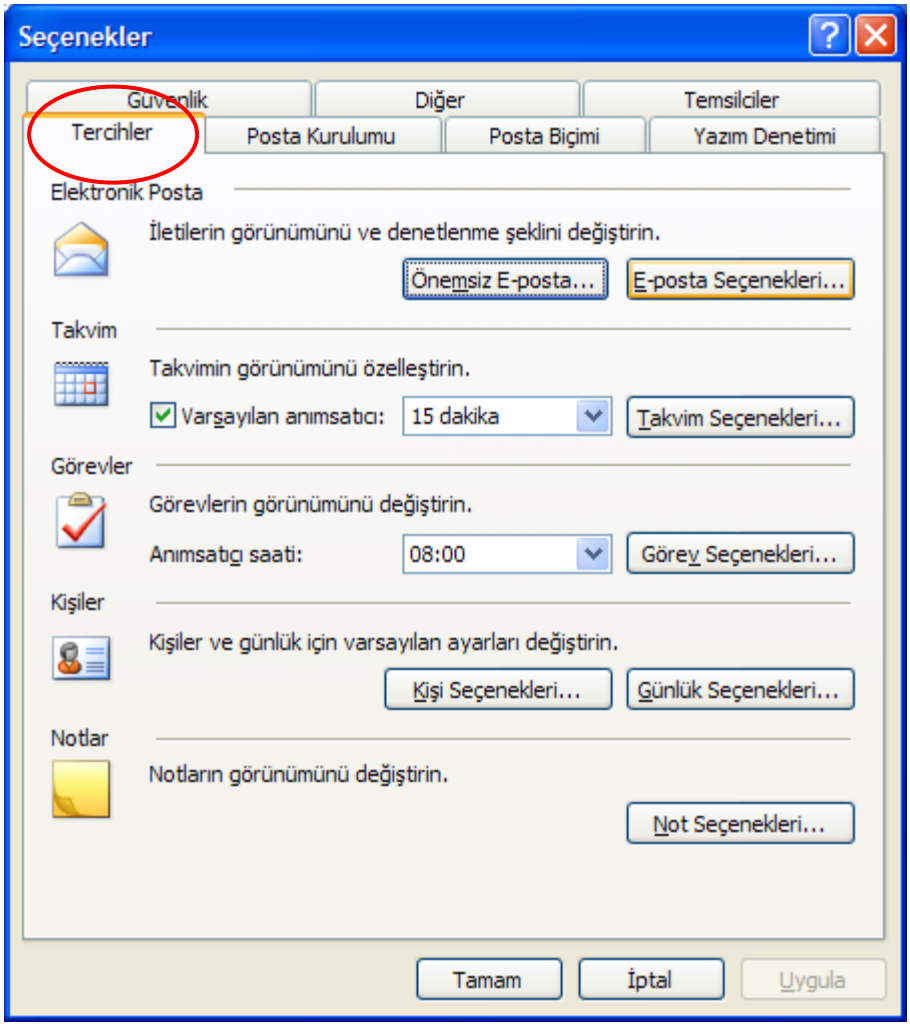
Microsoft Outlook 2003 programı ile e-imzalı e-posta göndermek için öncelikle program üzerinde bazı ayarların yapılması gerekmektedir. Bu ayarlar aşağıda adım adım gösterilmiştir:

1. Microsoft Office Outlook 2003 programının Şekil 5.25'de görülen "Araçlar" menüsünden "Seçenekler" seçeneği tıklanır.



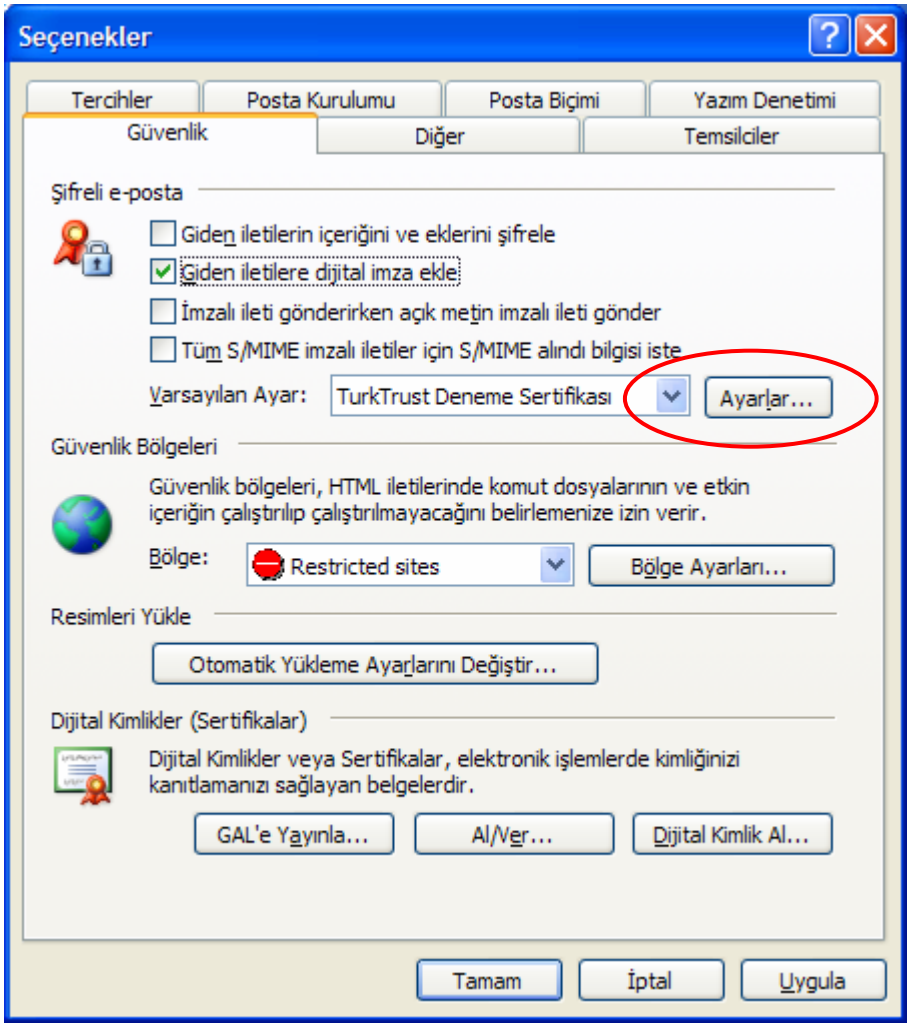
Şekil 5.25. Outlook programı e-imza ayarları (adım 1)

2. Açılan Şekil 5.26'daki ekranda, işaretlenmiş olan "Güvenlik" sekmesine tıklanır.



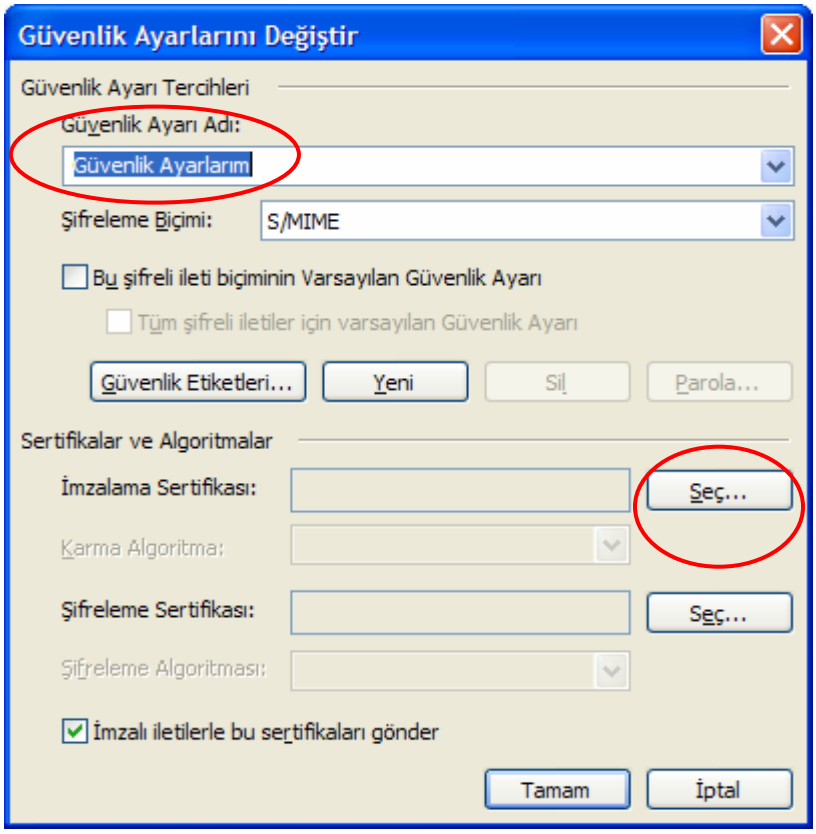
Şekil 5.26. Outlook programı e-imza ayarları (adım 2)

3. Şekil 5.27'deki gelen ekranda "Ayarlar" butonuna basılır.



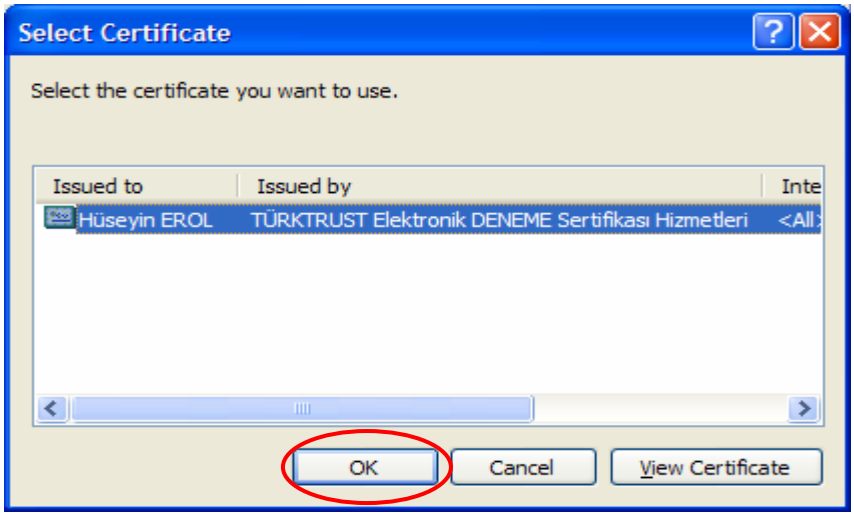
Şekil 5.27. Outlook programı e-imza ayarları (adım 3)

4. Şekil 5.28'deki ekranda, yapılan güvenlik ayarına bir isim verilerek "İmzalama Sertifikası"/"Signing Certificate" seçeneğininin yanındaki "Seç" butonuna basılır.



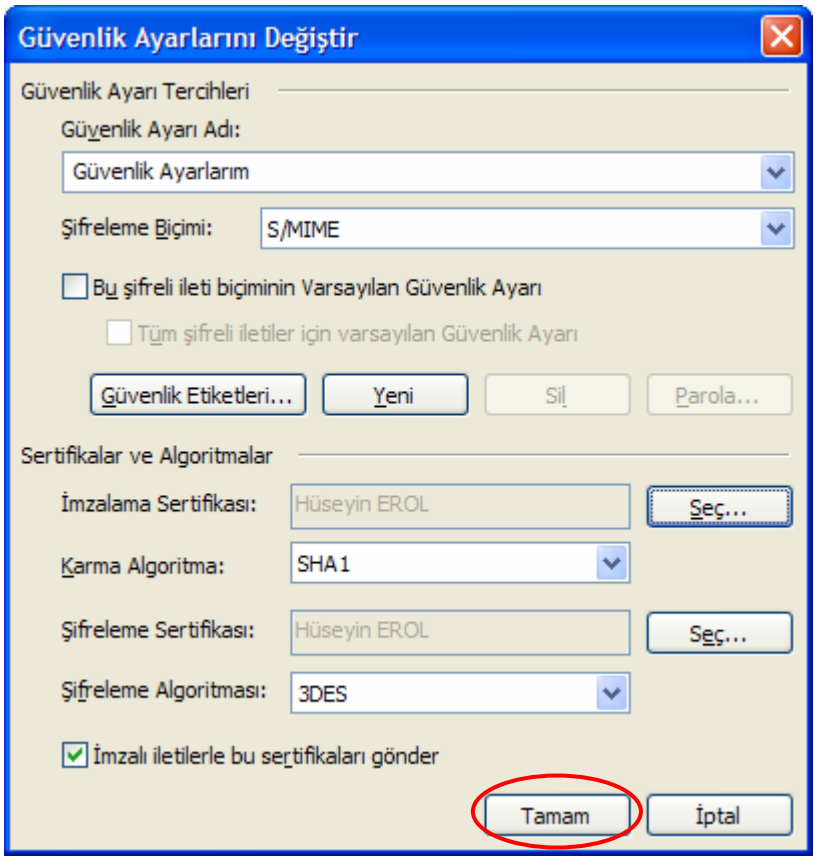
Şekil 5.28. Outlook programı e-imza ayarları (adım 4)

5. Elektronik posta gönderirken kullanılacak olan sertifika Şekil 5.29'daki ekrandan seçilerek "Tamam" butonuna basılır.



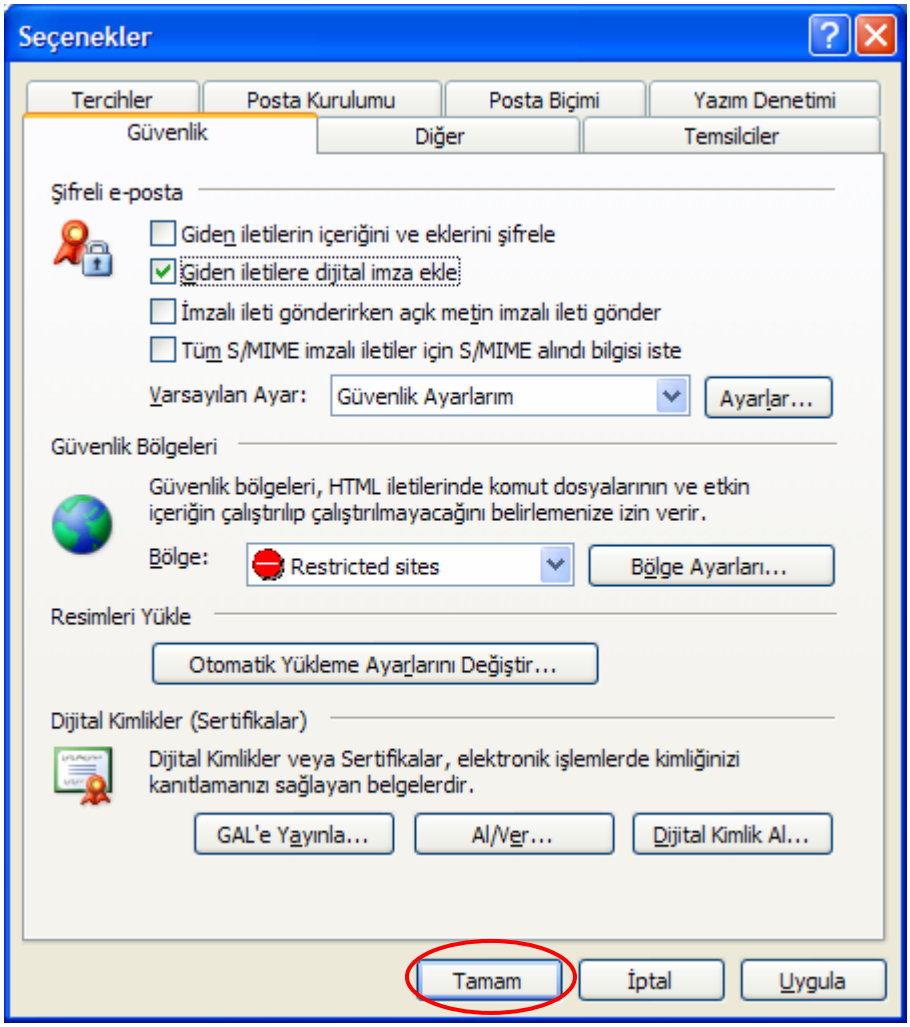
Şekil 5.29. Outlook programı e-imza ayarları (adım 5)

6. Şekil 5.30'daki güvenlik ayarları ekranı, "Tamam" butonuna basılarak kapatılır.



Şekil 5.30. Outlook programı e-imza ayarları (adım 6)

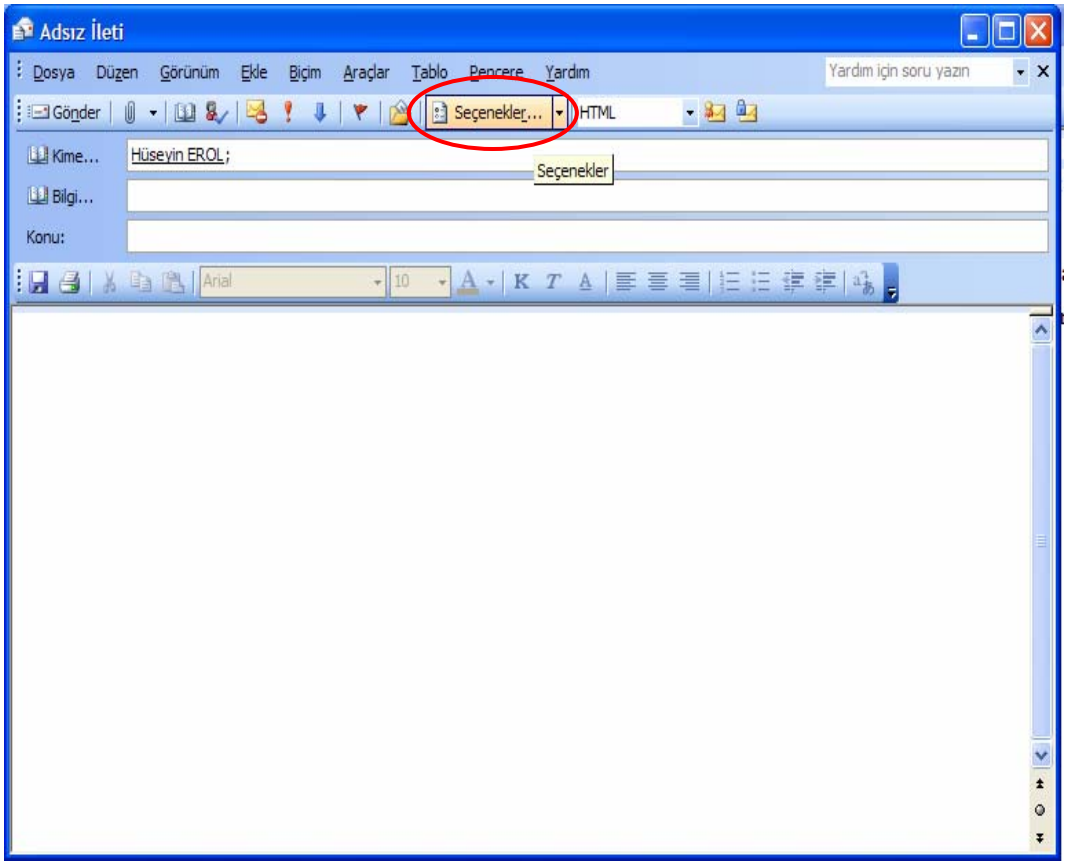
7. Açık olan Şekil 5.31'deki "Seçenekler" ekranı da "Tamam" butonuna basılarak kapatılır ve Microsoft Office Outlook 2003 programında e-imza kullanımına yönelik yapılması gereken ayarlar tamamlanmış olur.



Şekil 5.31. Outlook programı e-imza ayarları (adım 7)

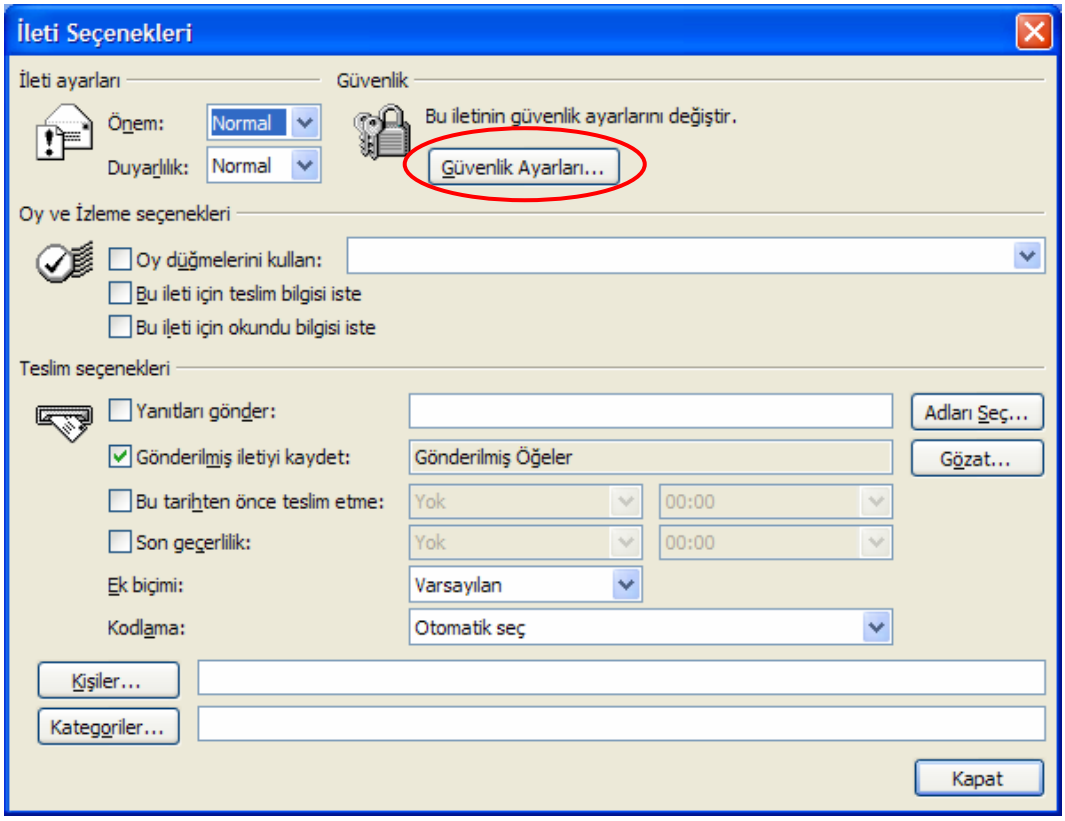
Yukardaki ayarların yapıldığı bilgisayarlarda artık e-postalar imzalı olarak gönderilebilir. Aşağıda e-imzalı bir e-postanın nasıl gönderileceği ve karşı tarafın bu e-imzalı postayı nasıl açarak imza bilgisini kontrol edeceği adım adım anlatılmıştır:

1. Microsoft Outlook 2003 programında, Şekil 5.32'de gösterilen yeni elektronik posta iletisi oluşturma ekranında "Seçenekler" butonuna tıklanır.



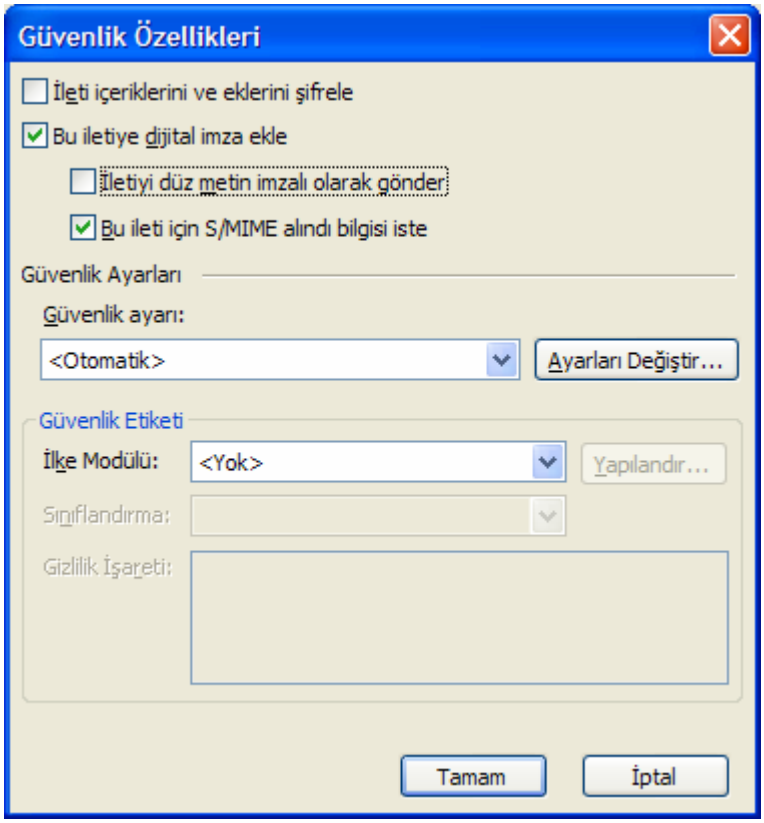
Şekil 5.32. Outlook programı ile e-imzalı posta haberleşmesi (adım 1)

2. Şekil 5.33'deki açılan ekranda işaretlenmiş olan "Güvenlik Ayarları" butonuna tıklanır.



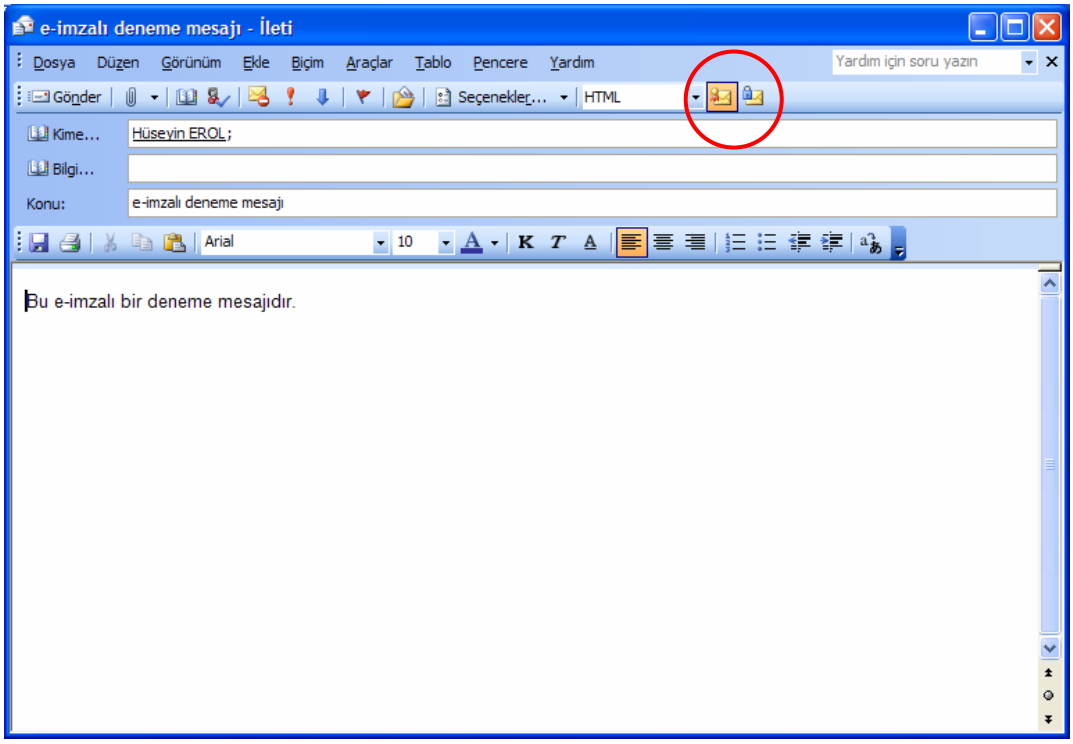
Şekil 5.33. Outlook programı ile e-imzalı posta haberleşmesi (adım 2)

3. Şekil 5.34'deki ekran açılır. Bu ekranda, "Bu iletiye dijital imza ekle" seçeneği işaretlenir. Ayrıca iletinin karşı tarafa ulaştığından emin olmak için "Bu ileti için S/MIME alındı bilgisi iste" seçeneği de işaretlenirse karşı tarafa ileti ulaşınca alındı bilgisi imzalı olarak gelmektedir. İlgili seçeneklerin seçilmesinin ardından "Tamam" butonuna basılır ve ekran kapatılır. Gelen ekranda da "Kapat" butonuna basılarak elektronik posta yazma ekranına geri dönülür.



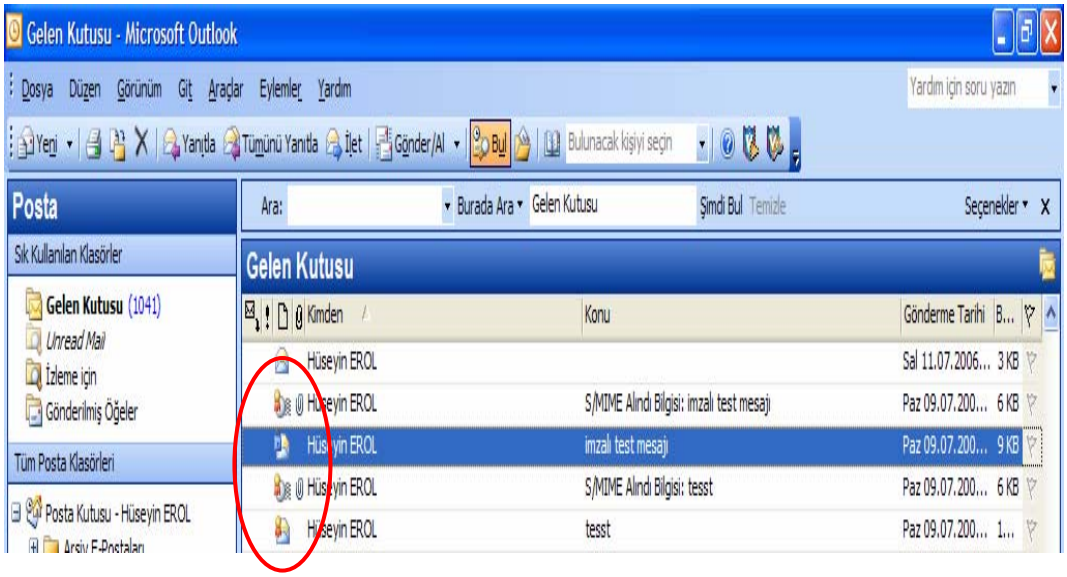
Şekil 5.34. Outlook programı ile e-imzalı posta haberleşmesi (adım 3)

4. E-posta yazma ekranında mesaj içeriği ve gönderilecek kişiler eklenerek e-posta gönderilir. Bu ekranda mesajın e-imzalı olarak gideceği Şekil 5.35'deki aktif hale gelen e-imza ikonundan da anlaşılabilir.



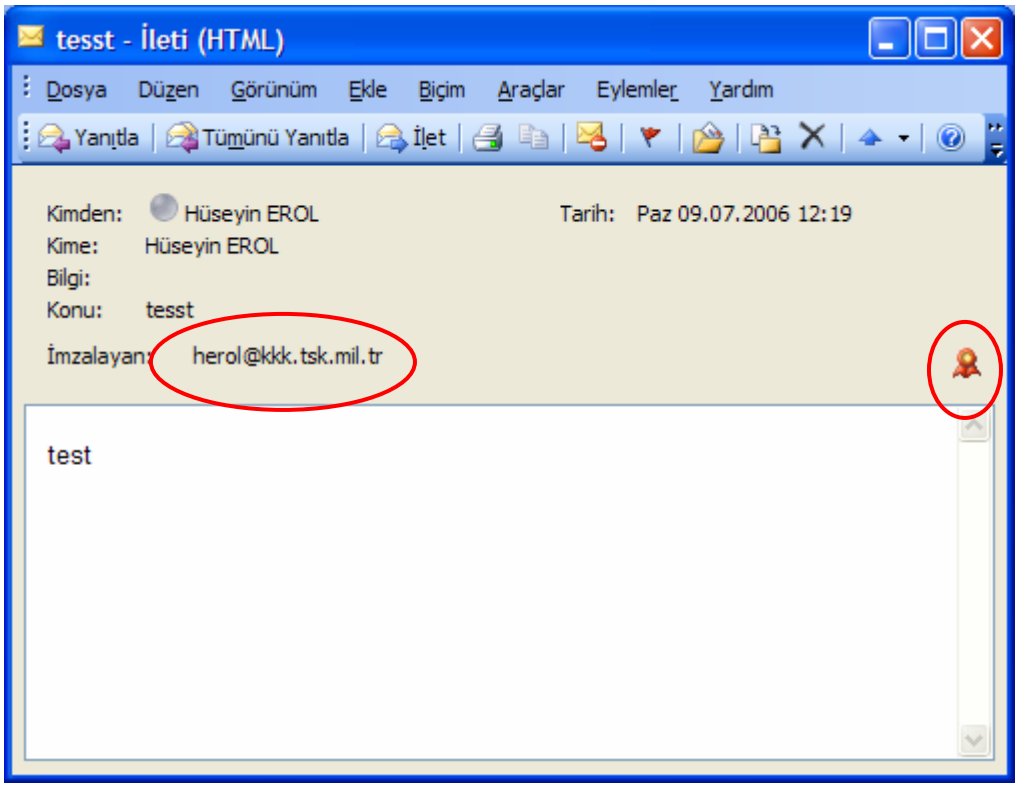
Şekil 5.35. Outlook programı ile e-imzalı posta haberleşmesi (adım 4)

5. E-imzalı olarak gönderilen e-postalar alıcının "Gelen Kutusu"nda Şekil 5.36'daki gibi görünür.



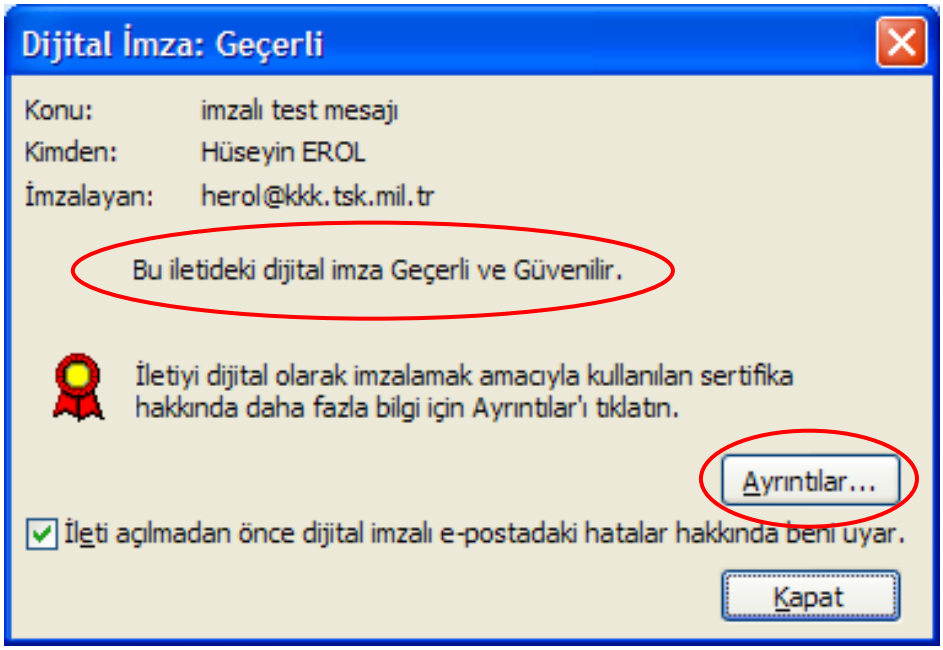
Şekil 5.36. Outlook programı ile e-imzalı posta haberleşmesi (adım 5)

6. Bu e-postalar alıcı tarafından açıldığında da Şekil 5.37'deki gibi görünür. Burada mesajın imzalı olduğu ve kim tarafından imzalandığı görülmektedir.



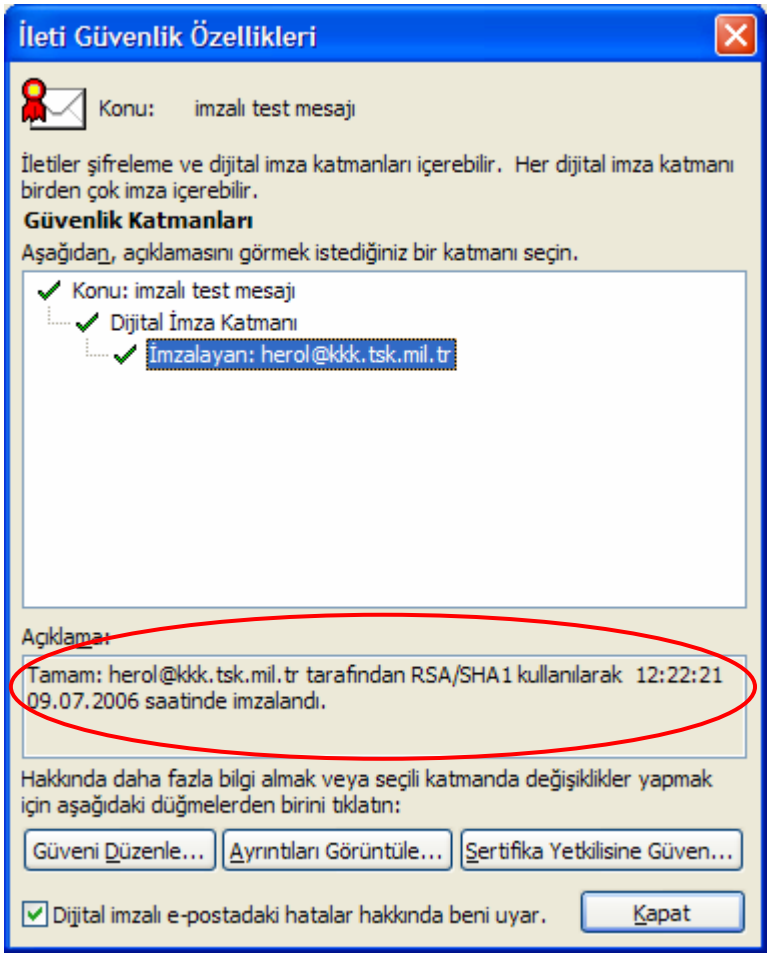
Şekil 5.37. Outlook programı ile e-imzalı posta haberleşmesi (adım 6)

7. Bu e-posta içindeki sertifika ikonuna tıklandığında Şekil 5.38'deki ekran açılır. Bu ekranda mesaj, imzalayan kişi, sertifikanın geçerliliği ve güvenilirliği ile ilgili bilgiler bulunmaktadır. Eğer imzada veya sertifikada bir problem olursa, kullanıcı Şekil 5.37 ve Şekil 5.38'deki ekranlarda uyarılır.



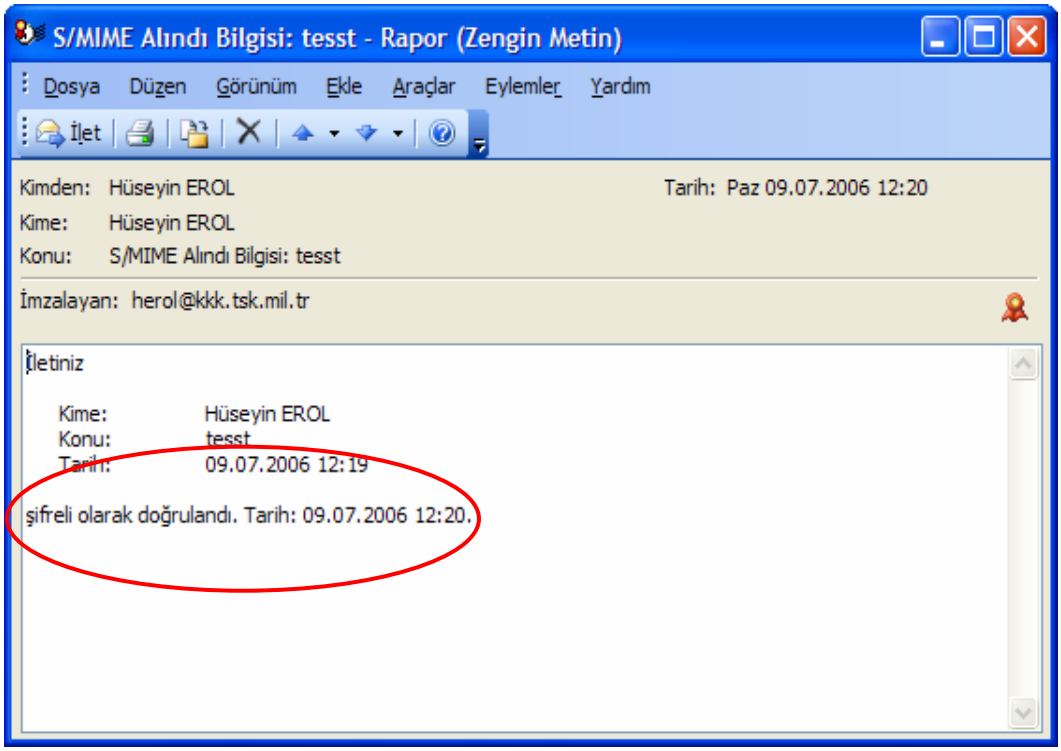
Şekil 5.38. Outlook programı ile e-imzalı posta haberleşmesi (adım 7)

8. Şekil 5.38'deki ekranda "Ayrıntılar" butonuna tıklandığında Şekil 5.39'da verilen "İleti Güvenlik Özellikleri" ekranı açılır. Bu ekranda iletinin kim tarafından, hangi algoritma ile ve hangi tarih/saatte imzalandığı bilgisi detaylı olarak verilmektedir. Ayrıca ilgili sertifika ve güven ilişkileri de ayrıntılı olarak ilgili butonlara basarak görülebilmektedir.



Şekil 5.39. Outlook programı ile e-imzalı posta haberleşmesi (adım 8)

9. Son olarak, e-imzalı e-postayı gönderen kişinin, karşı tarafa postanın ulaştığından emin olabilmek için istediği "S/MIME alındı bilgisi", mesaj alıcıya ulaştığında gönderene e-posta yoluyla iletilmektedir. Bu bilgi e-postası da Şekil 5.40'da görülmektedir. Böylelikle mesajı alan kişi mesajı aldığını da inkar edememektedir.



Şekil 5.40. Outlook programı ile e-imzalı posta haberleşmesi (adım 9)

İmzager MİM yazılımının kullanımı

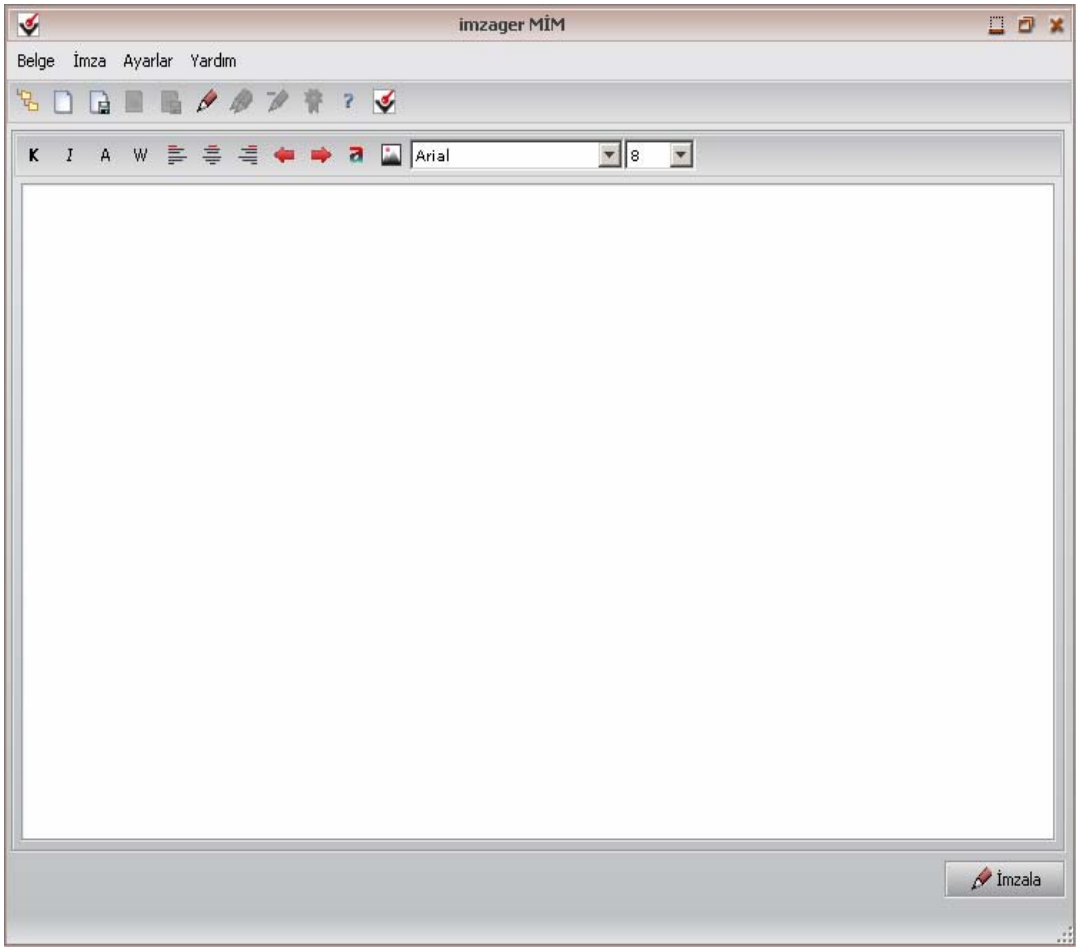
Kamu SM tarafından, kurumsal ağlarda e-imza uygulamalarını somut bir şekilde gösterebilmek amacıyla geliştirilen İmzager MİM yazılımı, kurumsal ağlarda hayata geçirilebilecek temel e-imza uygulamalarını kapsamaktadır. Kurumların talebine bağlı olarak istenilen uygulamalarla ilgili yazılım kütüphaneleri Kamu SM tarafından ücret karşılığında kurumlara sunulmaktadır. Tez çalışması kapsamında Gazi Üniversitesi'nde simule edilecek örnek e-imza uygulamaları, doğrudan İmzager MİM yazılımı kullanılarak hayata geçirilmiştir.

İmzager MİM yazılımı Şekil 5.41'deki ekran görüntüsü ile açılmaktadır. Ayrıca yazılım hakkında bilgi veren "Hakkında" ekranı da Şekil 5.42'de sunulmuştur.

Şekil 5.41. İmzager MİM yazılımı açılış ekranı

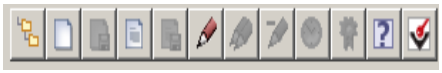
Şekil 5.42. İmzager MİM yazılımı hakkında ekranı

Açılış ekranının ardından Şekil 5.43'de gösterilen ana ekran açılmaktadır. Bu ekrandaki "Belge", "İmza", "Ayarlar" ve "Yardım" menüleri kullanılarak yazılımın temel fonksiyonlarını gerçekleştirmek ve yardım almak amacıyla ilgili fonksiyonlara kolayca ulaşılabilir. Ayrıca, imzalamak amacıyla yazı yazmaya imkan sağlayan bir metin editörü de bu pencerede açılmaktadır. Kullanıcının, editör yardımıyla imzalamak istediği bilgiler üzerinde biçimlendirme yapmasına imkan sağlayacak fonksiyonlar da editörün üzerinde yer almaktadır.



Şekil 5.43. İmzager MİM yazılımı ana ekranı

Program içerisinde farklı yerlerde kullanılan düğmelerin kısayollarını içeren araç çubuğu Şekil 5.44'de görülmektedir. Sırasıyla "Dizin Ağacını Görüntüle" (kayıtlı dosyaları seçmek için kullanılan ağacı görüntüler), "Yeni Belge" (yeni boş bir metin dosyası açar), "Yeni Belgeyi Kaydet" (yeni metin dosyasını kaydeder), "İçerik Görüntüle" (formatı editörde görüntülenmeye uygun olmayan dosyaları kendi uzantıları ile açar), "İçeriği Kaydet" (imzalı belgelerin içeriğini kaydeder), "İmzala" (imzalama işlemini başlatır), "Seri İmzala" (belgeyle birlikte içindeki bir imzayı imzalar), "İmza Sil" (belgeden imza çıkarır), "Zaman Damgası Ekle" (imzaya zaman damgası ekler), "Sertifika Görüntüle" (imza sahibinin sertifikasını görüntüler), "Yardım" (programın yardım menülerini içerir) ve "Hakkında" (program hakkındaki genel bilgileri görüntüler) düğmelerini içerir.



Şekil 5.44. İmzager MİM yazılımı araç çubuğu

Yazılımın menü çubuğu ise “Belge”, “İmza”, “Ayarlar” ve “Yardım” menülerini içerir. “Belge” menüsünde dizin ağacını görüntüleyebilmek için “Dosya Aç”, yeni boş bir metin dosyası açmak için “Yeni Belge”, bu belgeyi kaydetmek için “Yeni Belge Kaydet”, formatı editörde görüntülenmeye uygun olmayan dosyaları kendi uzantıları ile açmak için “İçeriği Görüntüle”, imzalı belgelerin içeriğini kaydetmek için “İçeriği Kaydet”, imza sahibinin sertifikasını görüntüleyebilmek için “İmza Sertifikası Görüntüle” ve programı kapatmak için “Çıkış” seçenekleri bulunur.

“İmza” menüsünde imzalama işlemi için “İmzala”, belgeyle birlikte bir imzayı imzalamak için “Seri İmza Ekle”, belgeden imza çıkarmak için “İmza Sil” ve imzaya zaman damgası eklemek için “Zaman Damgası Ekle” seçenekleri bulunur.

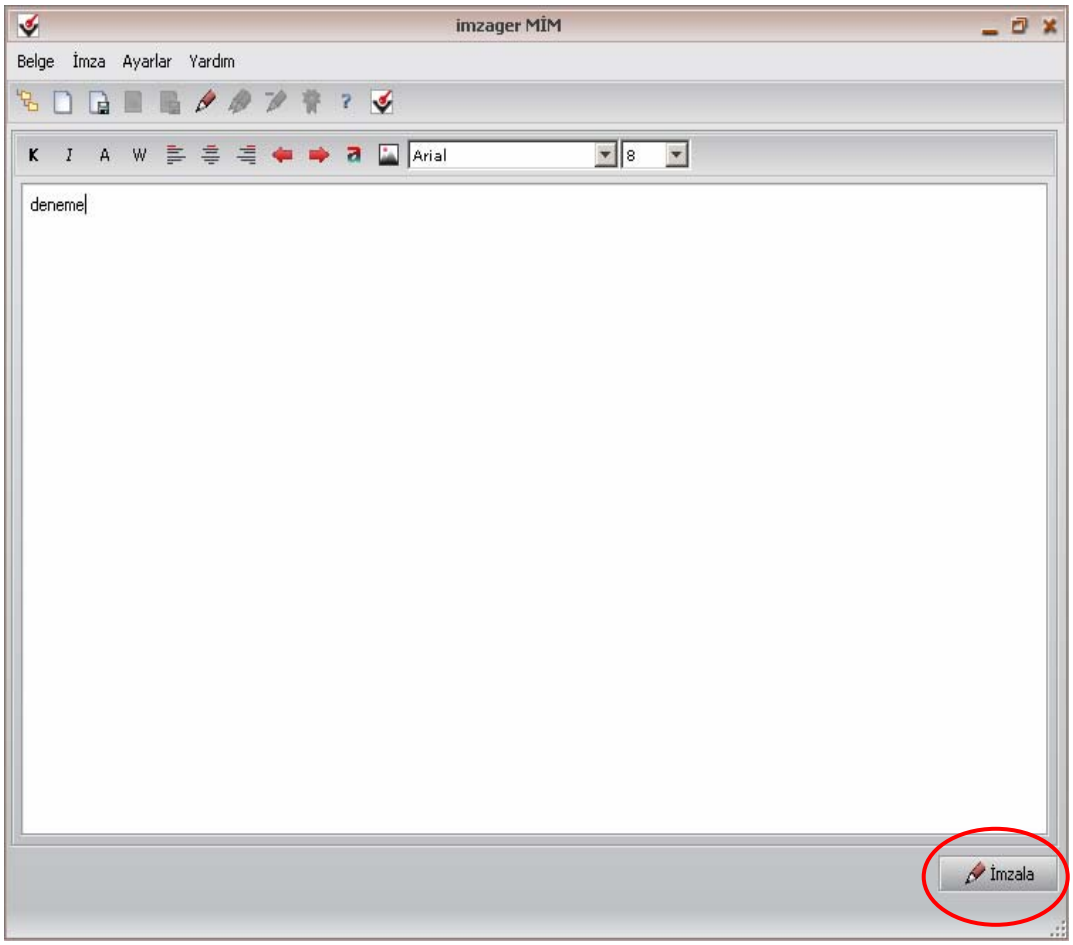
“Ayarlar” menüsünde konfigürasyon ayarları için “Tüm Ayarlar” ve kart ile ilgili işlemler için “Akıllı Kartlarım” seçenekleri bulunur.

“Yardım” menüsünde ise kullanım ile ilgili açıklamar için “Yardım” ve program hakkındaki genel bilgileri görmek için “İmzager MIM Hakkında” seçenekleri bulunur (Şekil 5.42).

<u>İmzager MİM yazılımı ile imzalama işlemleri</u>

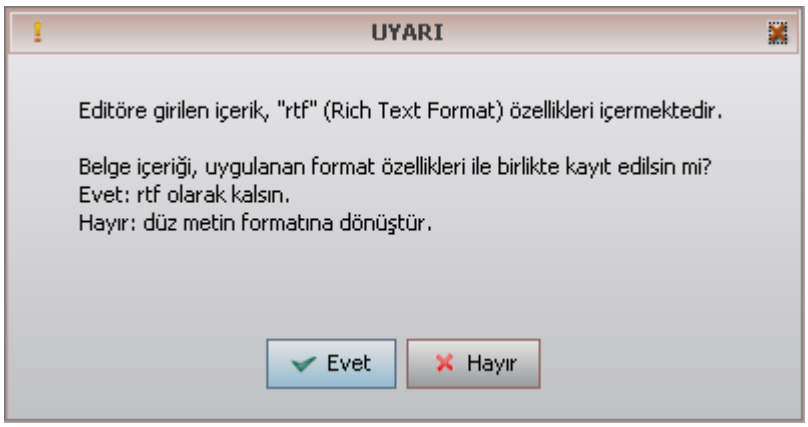
İmzager MİM yazılımı kurulu bir bilgisayarda imzalama işlemi 3 farklı yöntemle yapılabilir. İlk yöntem, imzalanacak bilginin imzager yazılımı ana ekranındaki editörün içine yazılması ve ardından “İmzala” butonuna basılmasıdır. Şekil 5.45’de gösterilen bu yöntemde kullanıcı, metin editörü üzerinde imzalamak istediği bilgileri yazarak “İmzala” butonu yardımıyla yazdığı metni imzalayabilir. Kullanıcının metin

üzerinde biçimlendirme yapmasına imkan sağlayacak fonksiyonlar da editörün üzerinde yer almaktadır.



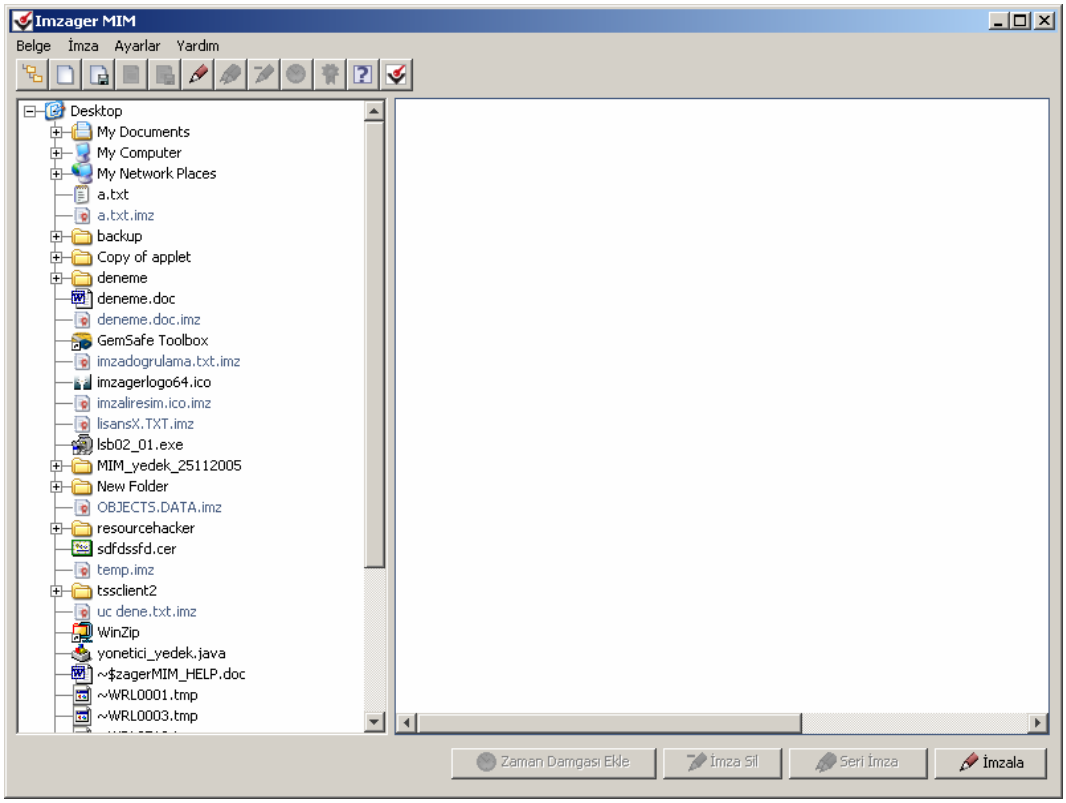
Şekil 5.45. İmzager MİM yazılımı ile metin imzalama

İmzager MİM editörü kullanılarak gerçekleştirilen imzalama işlemlerinde "İmzala" butonuna basıldıktan sonra Şekil 5.46'daki uyarı ekranı açılır. Bu ekranda "rtf" (rich text format, zengin yazı formatı) içerikli belgenin aynı formatta mı yoksa düz metin olarak mı kaydedileceği kullanıcıya sorulmaktadır. Bu uyarı "Evet" butonuna basılarak geçilebilir.



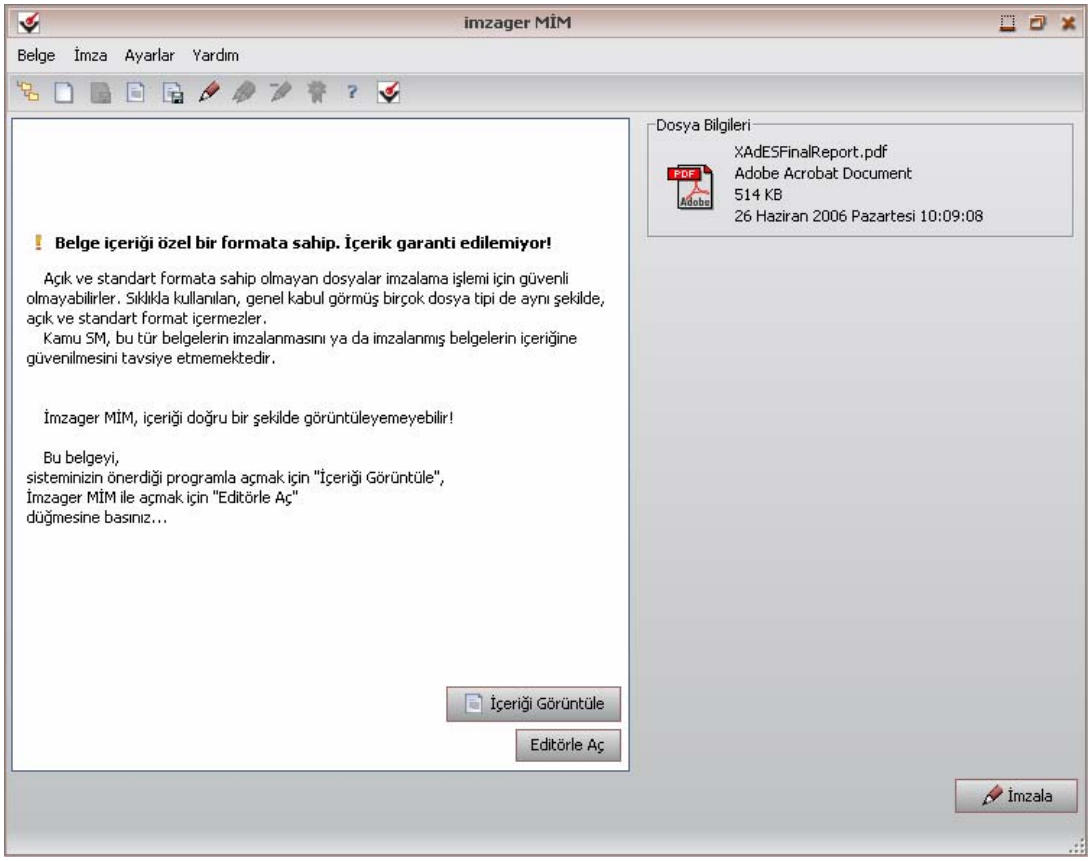
Şekil 5.46. İmzager MİM yazılımı ile metin imzalama uyarı ekranı

İmzalama işlemi için kullanılabilecek 2 nci yöntem, bilgisayarda kayıtlı bulunan bir dosyanın İmzager MİM yazılımı dizin ağacı yardımıyla seçilerek imzalanmasıdır (Şekil 5.47). Bu yöntemde, "Belge" menüsündeki "Dosya Aç" ya da araç çubuğundaki ilk düğme olan "Dizin Ağacını Görüntüle" seçenekleri ile imzalanmak istenen kayıtlı dosya dizin ağacından çift tıklanarak seçilir ve dosya bilgileri görüntülenir. Eğer belge imza içeriyor ise imzalar da görüntülenir (İmzalı bir dosya seçildiğinde, imzaların görüntülenmesi kontrolleri yapıldıktan sonra işlem gerçekleşeceğinden, bu işlem belirli bir zaman alacaktır). Ardından "İmzala" düğmesi ile imzalama işlemi başlatılabilir.



Şekil 5.47. İmzager yazılımı dizin ağacı ekranı

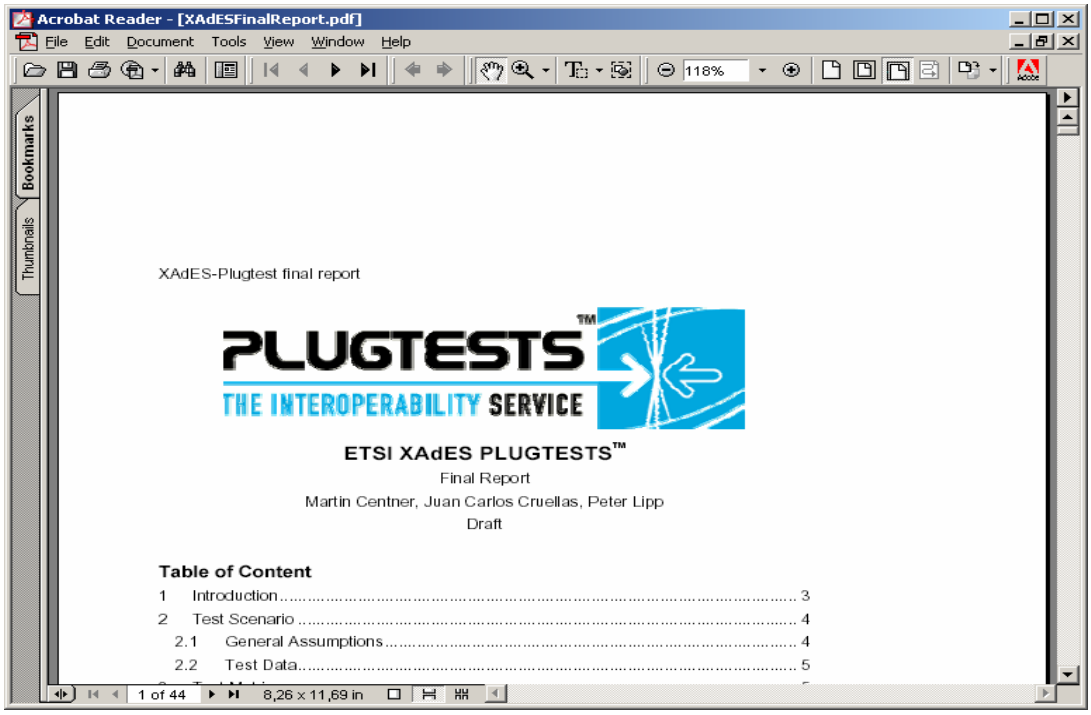
Seçilen dosya içeriği imzager editörü ile görüntülenebilecek formatta değilse bir uyarı penceresi çıkar. İmzalamadan önce belgenin görülmesi gerektiğini söyleyen ve Şekil 5.48'de gösterilen bu uyarı penceresinde "İçeriği Görüntüle" veya "Editörle Aç" butonları kullanılarak belge içeriği kontrol edilmelidir.



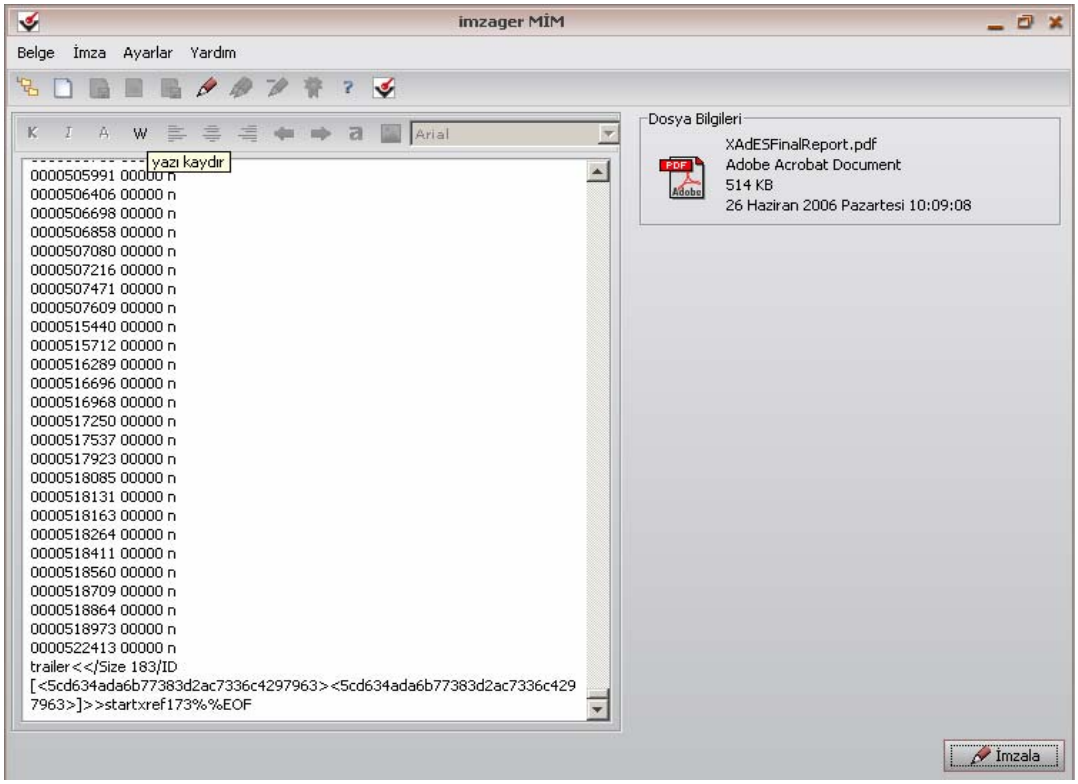
Şekil 5.48. İmzager MİM yazılımı dosya imzalama ekranı

Ekran üzerinde “Editörle Aç” butonuna basılmasıyla Şekil 5.49’daki ekran, “İçeriği Görüntüle” butonuna basılmasıyla da Şekil 5.50’deki ekran açılır. Burada dikkat edilmesi gereken konu, açık ve standart formata sahip olmayan dosyaların imzalama işlemi için güvenli olmamalarıdır. Zaten Şekil 5.50’de de belgenin içeriği anlamlı bir şekilde görüntülenememiştir.

Günlük hayatta sıklıkla kullanılan *.doc, *.pdf uzantılı dosyalar da açık ve standart bir format içermezler. Açık ve standart olmayan dosyalar içine yerleştirilecek kodlarla belge içeriğinin farklı koşullarda farklı olması sağlanabilir. Bu durumda da söz konusu belgenin farkında olunmadan içindeki kötü niyetli kodla birlikte imzalanması sonucu istenmeyen sonuçlar doğabilir. Bu nedenle açık ve standart formatta olan belgelerin (*.txt, *.tiff gibi) imzalanması tavsiye edilmektedir.

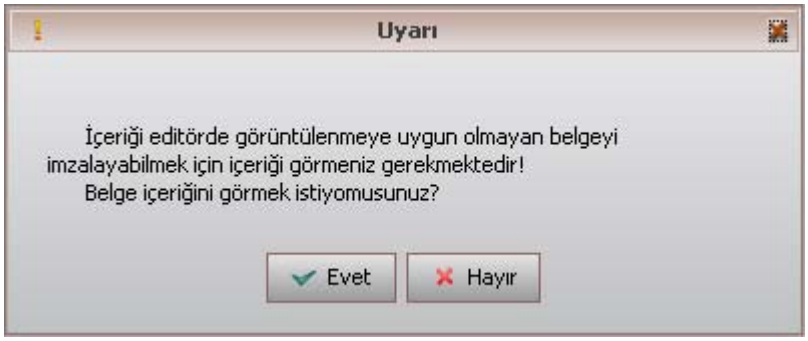


Şekil 5.49. Belge içeriğinin görüntülenmesi (editörle aç)



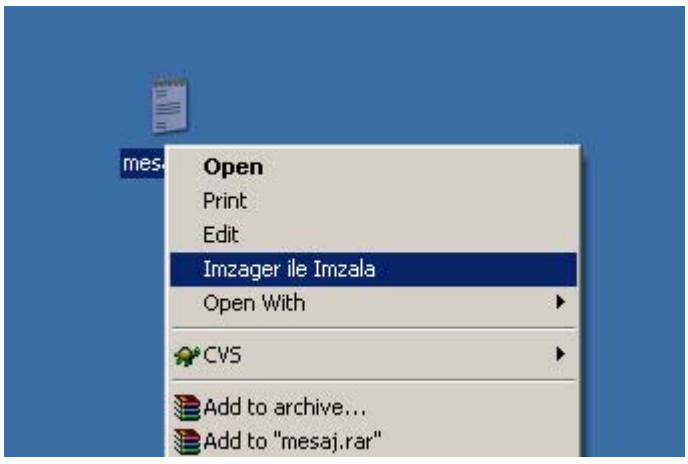
Şekil 5.50. Belge içeriğinin görüntülenmesi (içeriği görüntüle)

Belgenin görüntülenmesi sonucunda “İmzala” butonuna basılmasıyla Şekil 5.51’deki uyarı ekranı açılır. Bu uyarı ekranı, kullanıcıyı imzalayacağı belgenin içeriğini son kez görmesi için uyarmaktadır.

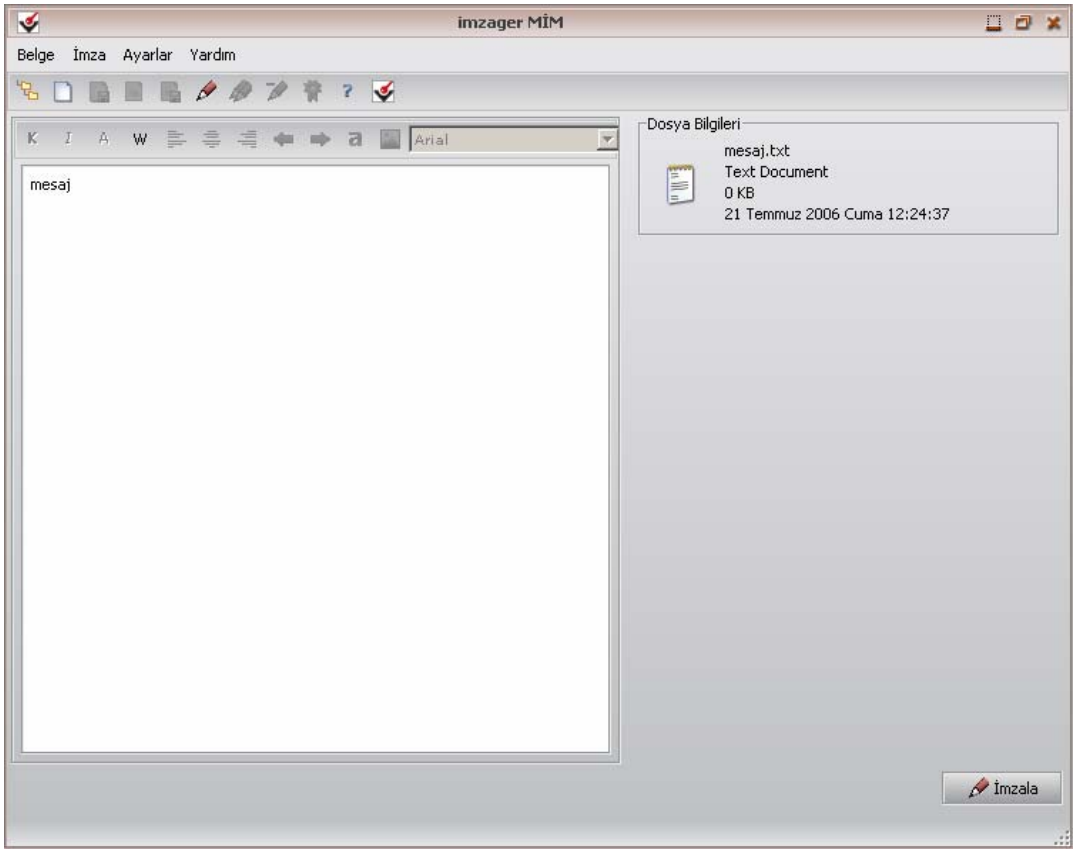


Şekil 5.51. İmzager MİM yazılımı belge imzalama uyarı ekranı

İmzager MİM yazılımı yardımıyla yapılacak imzalama işlemi için kullanılacak 3 ncü ve son yöntem de, bilgisayar ortamındaki belgenin üzerine sağ tuş ile tıklanması sonucu gelen Şekil 5.52’deki menüde “İmzager ile İmzala” seçeneğinin seçilmesidir. Bu durumda Şekil 5.53’deki ekran açılır ve işlemler “İmzala” butonuna basılarak yukarıda anlatıldığı şekilde devam ettirilir.



Şekil 5.52. İmzager MİM yazılımı belge imzalama menüsü



Şekil 5.53. İmzager MİM yazılımı ile belge imzalama

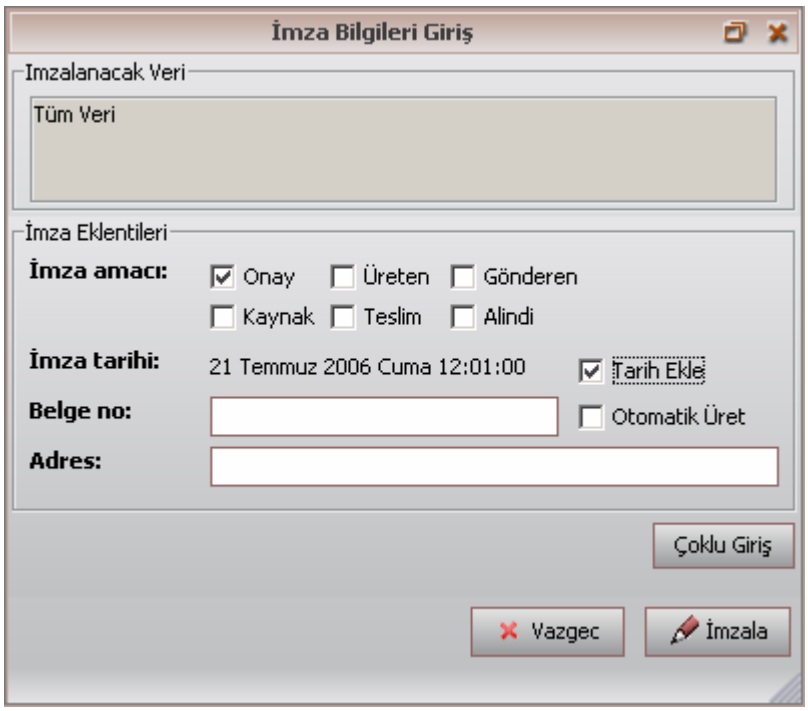
Yukarıda anlatılan 3 yöntemde de imzalanacak belge için "İmzala" butonuna basıldıktan sonra, imzalanacak belgenin türüne göre gelecek uyarı mesajının ardından yapılacak işlemler aynıdır. Bu aşamadan itibaren yapılacak imzalama işlemi, akıllı karta erişim işlemlerini de içermektedir. Dolayısıyla imzalama yapılacak olan sistemde en az bir kart okuyucu ve akıllı kart bulunmalı ve sürücüleri doğru şekilde kurulmuş olmalıdır. Her 3 yöntemde de yapılacak ortak işlemler aşağıda adım adım anlatılmıştır

1. "İmzala" butonuna basıldıktan sonra gelen "Uyarı" ekranının ardından imzalama işlemi için gerekli bilgi ve imza eklentilerinin girileceği Şekil 5.54'deki "imza bilgileri giriş ekranı" açılır. ETSI (European Telecommunications Standard Institude)'nin standart dokümanında tanımladığı e-imza oluşturulurken imzaya eklenecek zorunlu alanların yanısıra isteğe bağlı bazı alanların eklenmesi,

çıkarılması gibi işlemler de API tarafından kullanıcının denetimine sunulmuştur. Şekil 5.54'de e-imza eklentilerinden "imza amacı", "imza tarihi", "belge no" ve "adres" bilgilerinin kullanıcı tarafından girilmesi sağlanır.

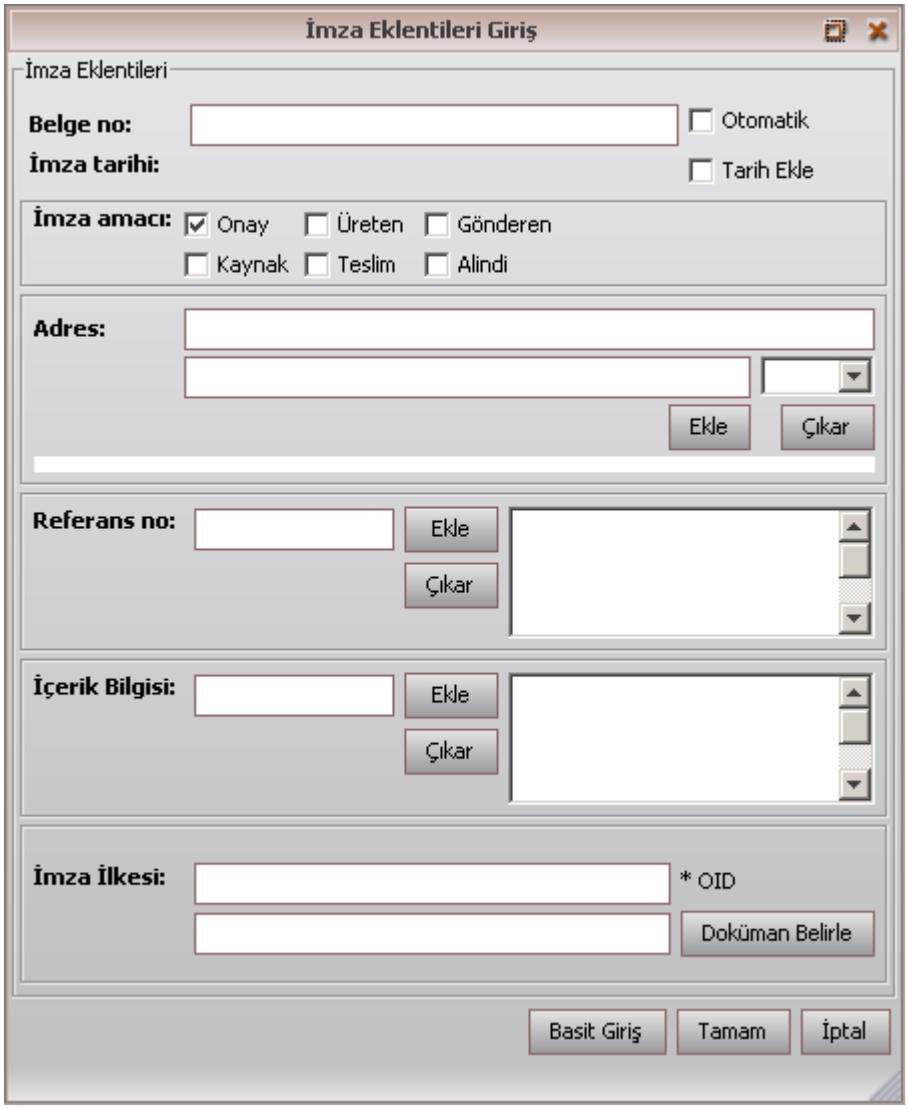
- İmza Amacı: İmza amacı imzanın hangi amaçla oluşturulduğunu belirtmek için kullanılabilir. Böylelikle imzalanan verinin kim tarafından oluşturulduğu, sadece imzanın içeriğinin onaylandığı vb. bilgiler belirtilebilir. İmza amacı olarak kullanılabilecek değerler, "Onay", "Üreten", "Gönderen", "Kaynak", "Teslim" ve "Alındı" olarak gruplanmıştır.
  - "Onay", imza sahibinin belge içeriğini onayladığını belirtmek için kullanılır.
  - "Üreten", imza sahibinin belgeyi oluşturan kişi olduğunu belirtmek için kullanılır. Belge içeriğini onayladığı veya gönderdiği anlamına gelmez.
  - "Gönderen", imzalı veriyi gönderenin (imzalı veri bir yere gönderiliyor ise) veriyi sadece gönderen kişi olduğunu belirtmek için kullanılır. Yani imza sahibinin gönderilen verinin içeriğini onayladığı anlamına gelmez sadece bunu ben gönderdim demektir.
  - "Kaynak", imza sahibinin belgeyi oluşturduğunu, içeriğini onayladığını ve gönderenin de kendisi olduğunu belirtmek için kullanılır.
  - "Teslim", bir mesaj gönderildiğinde, bu mesajın karşı tarafa iletildiğini belirtmede kullanılır. Bu tür bir imza genelde güvenilir servis sağlayıcılar (TSP - Trusted Service Provider) tarafından kullanılır.
  - "Alındı", imza sahibinin imzalı belgeyi aldığını (bir yerden geliyor ise) belirtmek için kullanılır.
- İmza Tarihi: İmzaya tarih bilgisini de eklemek için bu alandaki "tarih ekle" kutusu seçilerek içinde bulunulan tarih otomatik olarak bu alana yazdırılır.
- Belge No: Belge tanımlayıcısı özelliğinin bir parçası olan belge no ile imzalı belgelere belge numarası eklenebilir. Burada dikkat edilmesi gereken en önemli husus bu bilginin biricik (unique) olmasıdır. Böyle bir belge numarası belirlemek için sertifikanın açık anahtarı, zaman bilgisi ve rasgele bir sayı üçlüsünden oluşturulmuş bir değer kullanılabilir. Eğer parametre olarak boş string("") verilirse bu işlem yazılım tarafından otomatik olarak gerçekleştirilir.

- Adres: İmzanın nerede oluşturulduğu önem arzediyor ise bu alan kullanılabilir. İmza yeri bilgisi ülke, şehir ve adres bilgilerinden oluşabilir.



Şekil 5.54. İmza bilgileri giriş ekranı (basit giriş)

2. Şekil 5.54'de "Çoklu Giriş" butonuna basıldığında ise daha fazla imza eklentisinin girilebileceği ve Şekil 5.55'de verilen çoklu giriş ekranı açılır. Bu ekranda Şekil 5.54'deki ekrana ilave olarak "Referans No", "İçerik Bilgisi" ve "İmza İlkesi" eklenti giriş seçenekleri bulunmaktadır. "Referans No" ile imzada başka imzalara (dolayısıyla imzalı belgelere) referans verilebilir. Referans vermek için referans verilen imzanın belge tanımlayıcısı özelliğinin bulunması gerekmektedir, çünkü referans olarak bu değer kullanılacaktır. "Referans No" özelliği, bir mesajlaşma yazılımında cevap mesajdan orjinal mesaja referans vermek için kullanılabilir. Ayrıca mesaja içerik bilgisi ve imza ilkesi bilgileri de bu ekrandaki ilgili alanlardan girilebilir.



Şekil 5.55. İmza bilgileri giriş ekranı (çoklu giriş)

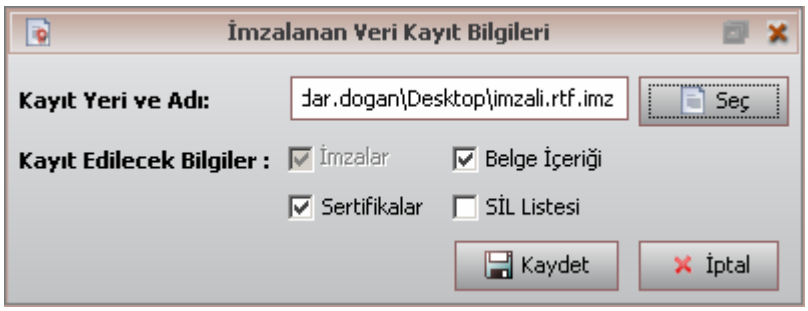
3. Şekil 5.55'deki ekranlarda imza eklentilerine ilişkin girişler yapıldıktan sonra "Tamam" butonuna basılır ve Şekil 5.54'deki ekran üzerinde "İmzala" butonuna basılır. Bu işlemin ardından Şekil 5.56'daki "PIN Giriş Ekranı" açılır. Bilgisayara bağlı kart okuyucu ve kartların kontrolü yapılır ve eğer var ise takılı olan ilk kart okuyucudaki sertifika varsayılan sertifika olarak görüntülenir. Seçili sertifikanın yanındaki "Seç" düğmesi kart okuyucu ve sertifikaları listelemeye ve varsayılan sertifikayı değiştirmeye yarar. "Görüntüle" düğmesi ise seçili olan sertifikayı görüntüler.

Şekil 5.56. PIN giriş ekranı-1

4. Seçilen karta uygun olarak Şekil 5.57'deki ekranda akıllı kart PIN kodu girildikten sonra "Tamam" butonuna basılarak işleme devam edilir.

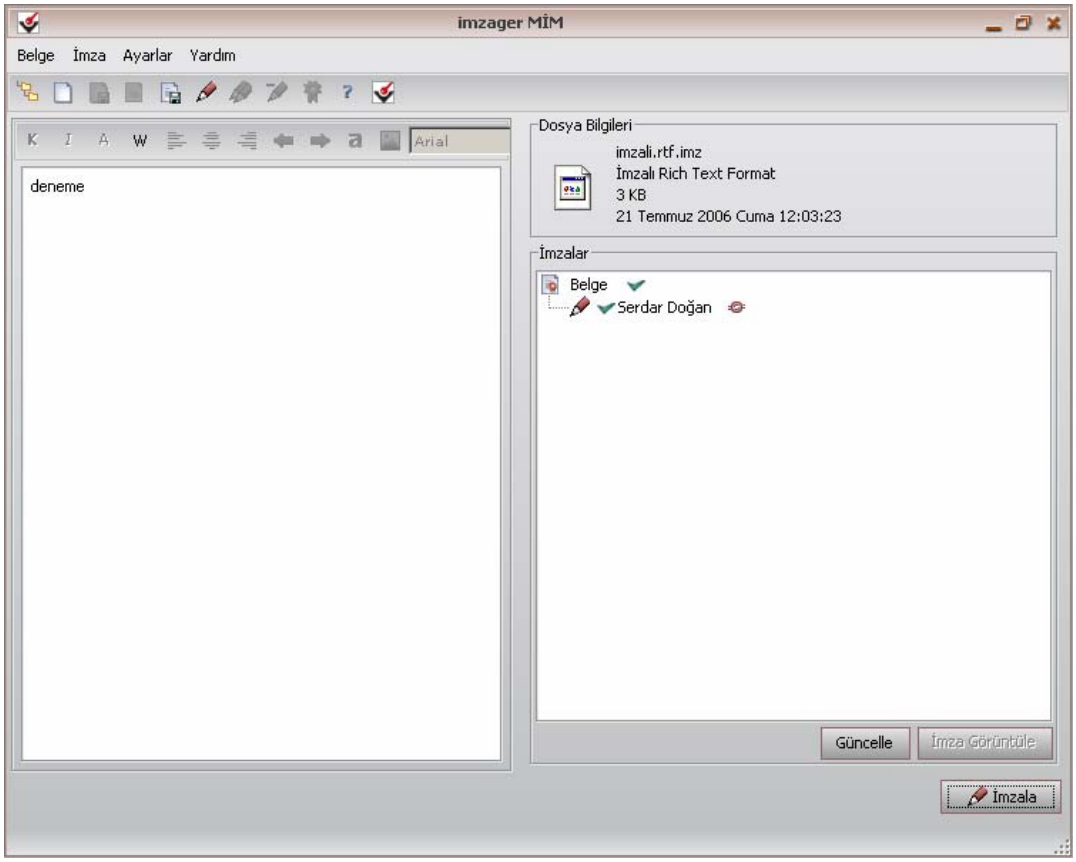
Şekil 5.57. PIN giriş ekranı-2

5. Gelen ekranda belgenin imzalandıktan sonra kaydedileceği yer ve adı ile kayıt edilecek bilgilerin girilmesini sağlayan Şekil 5.58'deki "İmzalanan veri kayıt bilgileri" ekranı gelmektedir. Belgenin imzalandıktan sonra kaydedileceği yer ve ismini tutan metin kutusunun içeriği ancak yanındaki "Seç" düğmesiyle değiştirilebilir. Varsayılan kayıt yeri "Ayarlar" menüsünden ayarlanır. Kaydedilecek imzalı belge ismi kullanıcı tarafından belirlenebilir ancak uzantısı değiştirilemez.

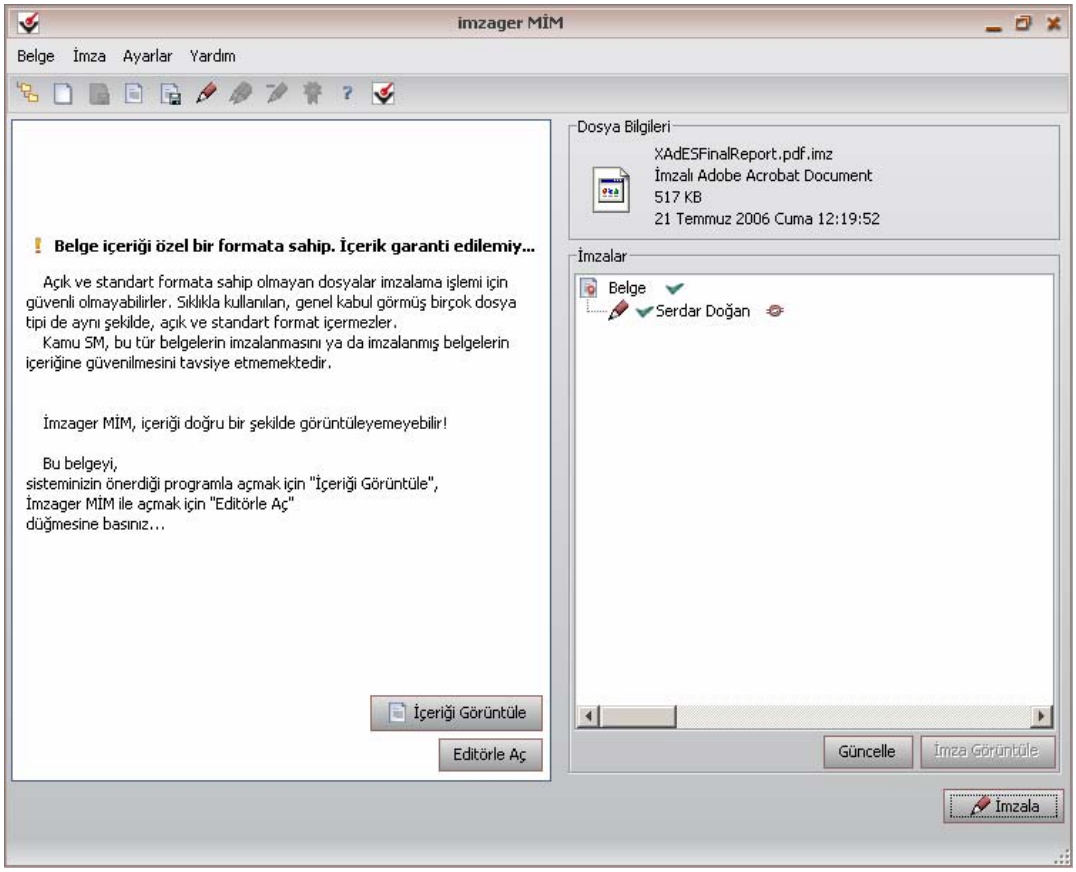


Şekil 5.58. İmzalanan veri kayıt bilgileri ekranı

6. Şekil 5.58'de "Kaydet" butonuna basılarak imzalama işlemi tamamlanır ve belge e-imzalı olarak belirtilen disk alanına "*.imz" uzantılı bir dosya olarak kaydedilir. Böylelikle tamamlanan imzalama işleminin ardından İmzager MİM editörü yardımıyla imzalan belgeye ilişkin bilgi ekranı Şekil 5.59'da, İmzager MİM yazılımı ile imzalanan kayıtlı bir belgeye ilişkin bilgi ekranı ise Şekil 5.60'da verilmiştir.



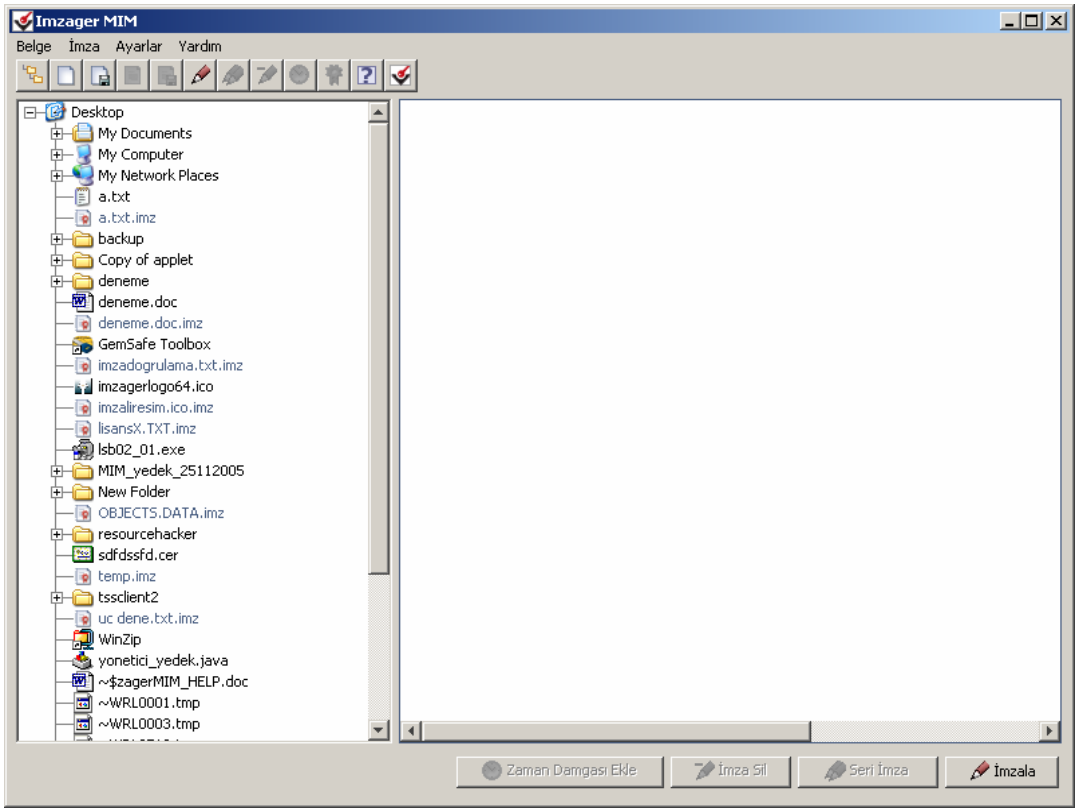
Şekil 5.59. İmzager MİM editörü yardımıyla imzalan belgenin görüntüsü



Şekil 5.60. İmzager MİM ile imzalan kayıtlı belgenin görüntüsü

Bir belgedeki imzaların görüntülenmesi

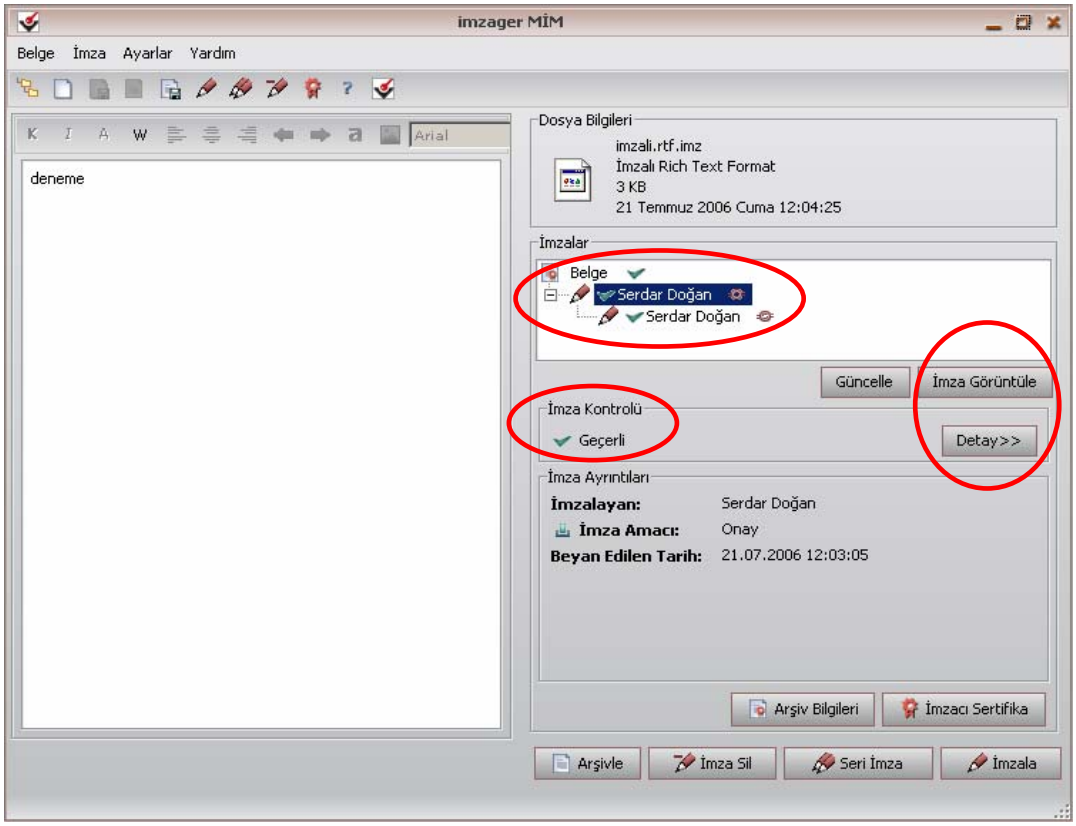
Herhangi bir belgedeki imzanın geçerliliğinin kontrolü ve görüntülenmesi için Şekil 5.61'deki dizin ağacından imzanın ait olduğu belgenin bulunup çift tıklanması gereklidir. Böylelikle dosya bilgileri ve içerdiği imzalar kontrol işlemi sonucunda görüntülenir (İmzalı bir dosya seçildiğinde, imzaların görüntülenmesi kontrolleri yapıldıktan sonra gerçekleşeceğinden bu esnadaki bekleme süreci olağandır).



Şekil 5.61. İmzager yazılımı dizin ağacı ekranı

Belgenin içeriğinin görüntülenmesi için, belge dizin ağacından çift tıklanarak seçildikten sonra eğer içeriği imzager editöründe görüntülenebilecek formatta ise editörde görüntülenir. Aksi taktirde formatın uygun olmadığına dair uyarı mesajı verilir. Uyarı mesajının altında iki düğme bulunur. Şekil 5.60'daki "İçeriği Görüntüle" düğmesi belgenin uzantısının ait olduğu programı açarak içeriği görüntüler. "Editörle Aç" düğmesi ise Şekil 5.50'deki gibi belge formatı uygun olmadığı halde içeriği editörde görüntüler, bu ise içeriğin okunaklı ve anlaşılır olmaması sonucunu doğurabilir.

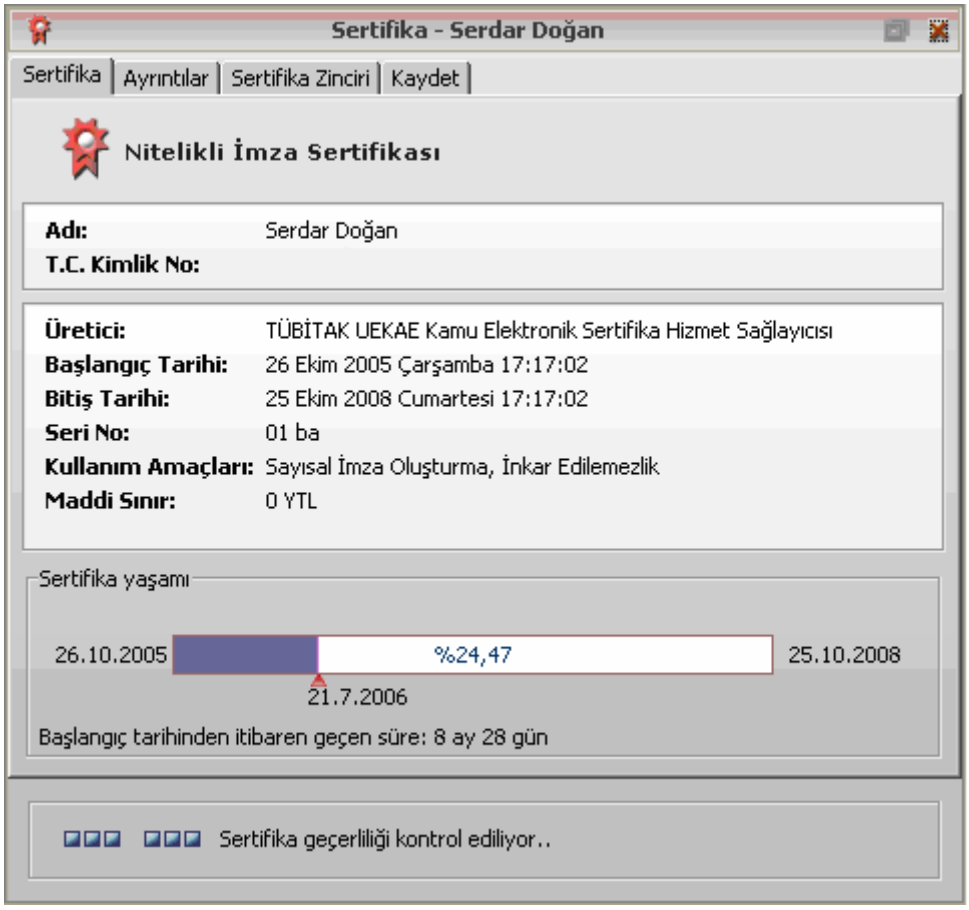
"İmza Bilgileri" başlığı altında görüntülenen imza ağacındaki imzaların sonuna kontrol sonucuna göre belirlenen ikonlar yerleştirilir. Sonucu detaylı görebilmek için imza çift tıklandığında veya seçilip "İmza Görüntüle" düğmesine basıldığında imza bilgileri ve kontrol sonucu görüntülenecektir. "İmza Kontrolü" başlığı altında bulunan "Detay" düğmesi ile kontrol detaylarına ulaşılabilir (Şekil 5.62).



Şekil 5.62. İmzager MİM yazılımı ile imza kontrolü

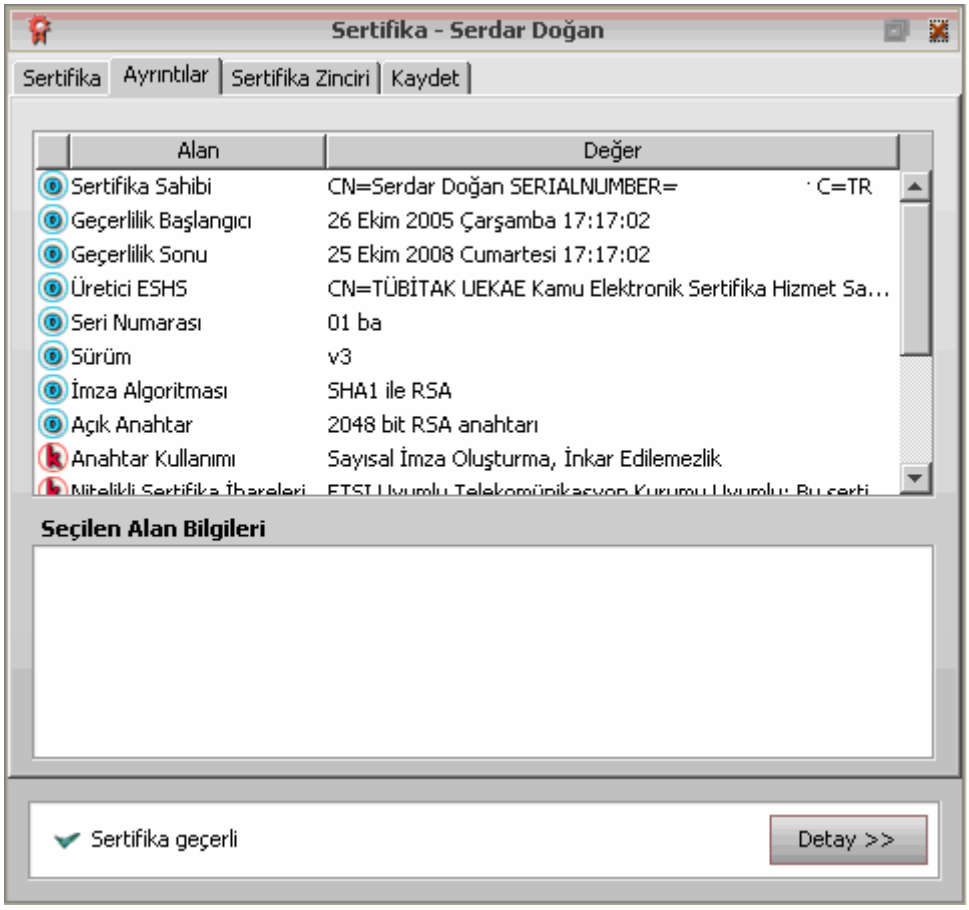
İmzanın seçilmesiyle aktif duruma gelen "İmza Görüntüle" düğmesi imza bilgilerini görüntüler. Görüntülenen bu imza bilgilerinin alt tarafındaki "Sertifika Görüntüle" düğmesi ise imza sahibinin sertifikasını görüntüler. Şekil 5.63'de gösterilen "Sertifika" ekranında "Sertifika", "Ayrıntılar", "Sertifika Zinciri" ve "Kaydet" alt menüleri yardımıyla detaylı sertifika bilgilerine erişilebilir.

Şekil 5.63'de açılan "Sertifika" ekranında sertifika sahibinin adı, T.C. kimlik numarası, sertifika üreticisinin adı, sertifika başlangıç/bitiş tarihleri, kullanım amaçları ve sertifika ömrü bilgileri görülmektedir.



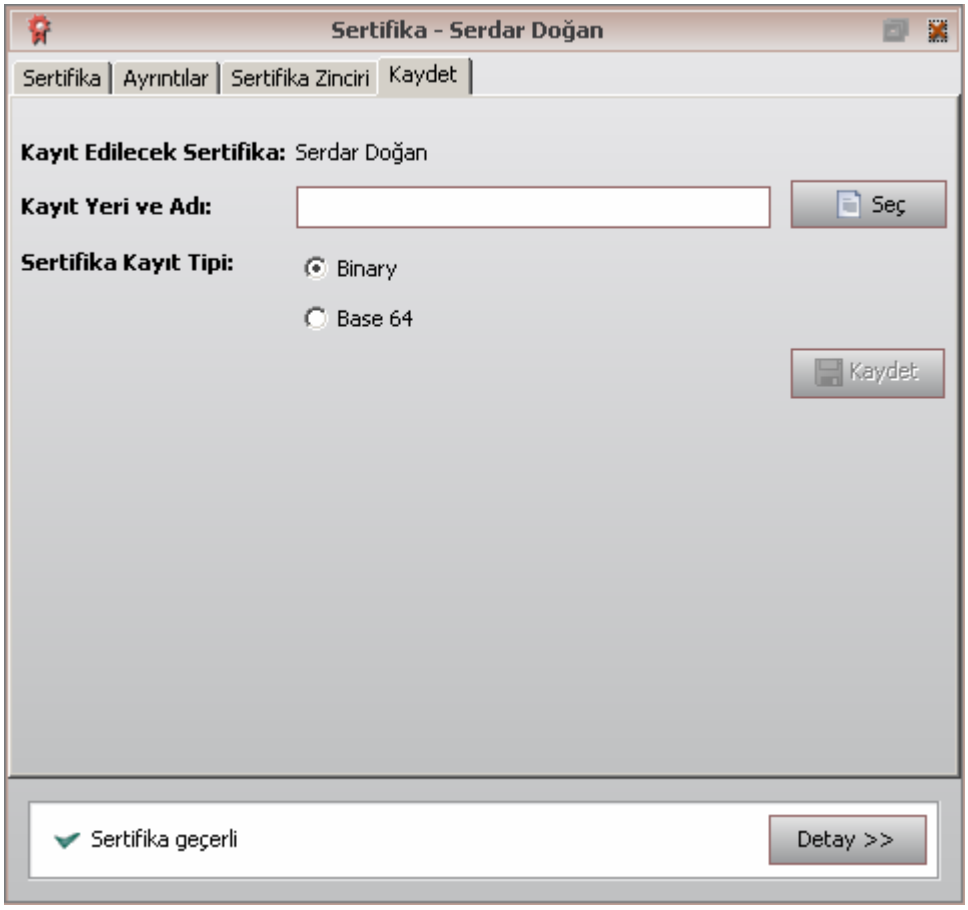
Şekil 5.63. İmzager MİM yazılımı sertifika ekranı (sertifika)

Ayrıntılar alanında ise sertifikaya ilişkin daha ayrıntılı ve teknik bilgilere erişilebilir. Ayrıntılar alanında bulunan bilgilere ilişkin ekran görüntüsü Şekil 5.64'de sunulmuştur.



Şekil 5.64. İmzager MİM yazılımı sertifika ekranı (ayrıntılar)

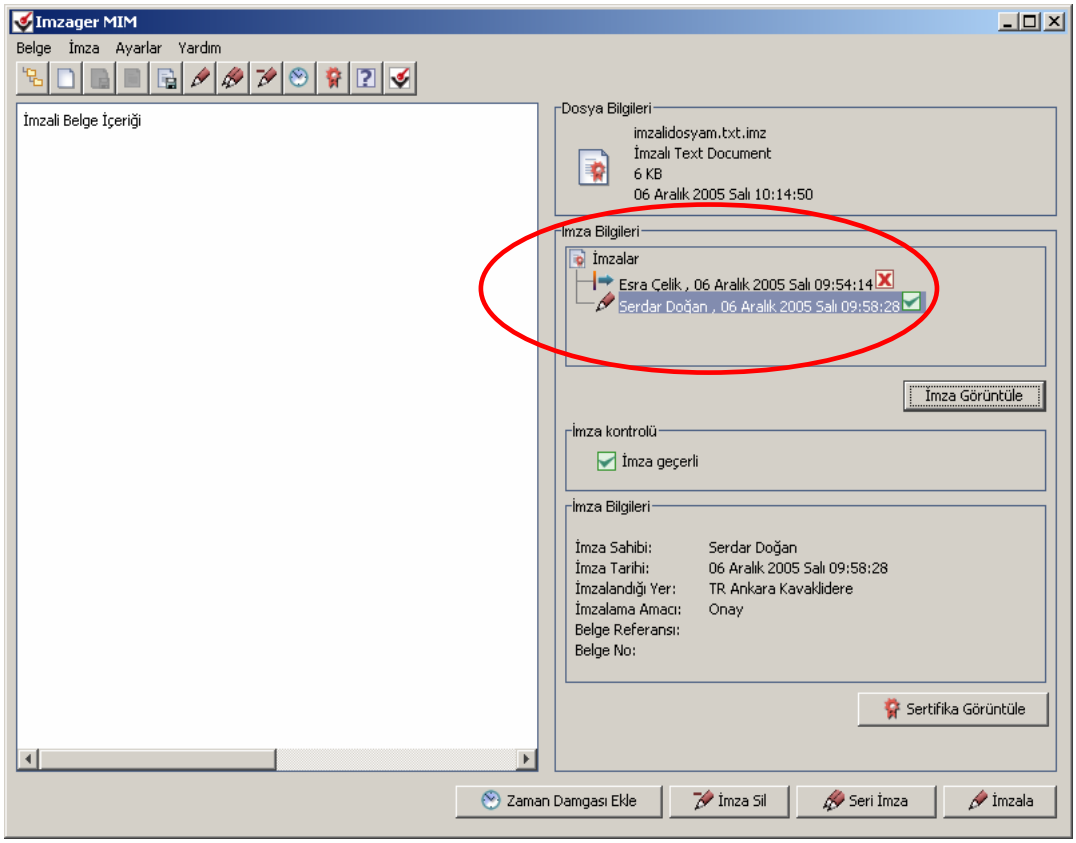
Sertifika bilgileri ekranında “sertifika zinciri” alanına tıklandığında ilgili sertifikaya ilişkin SM ve KSM bilgilerine erişilirken, “kaydet” alanına tıklandığında ise Şekil 5.65’deki ekran açılır. Bu ekran yardımıyla ilgili sertifika istenilen alana kaydedilebilir.



Şekil 5.65. İmzager MİM yazılımı sertifika ekranı (kaydet)

<u>İmzalı belgeye yeni imza ekleme işlemi</u>

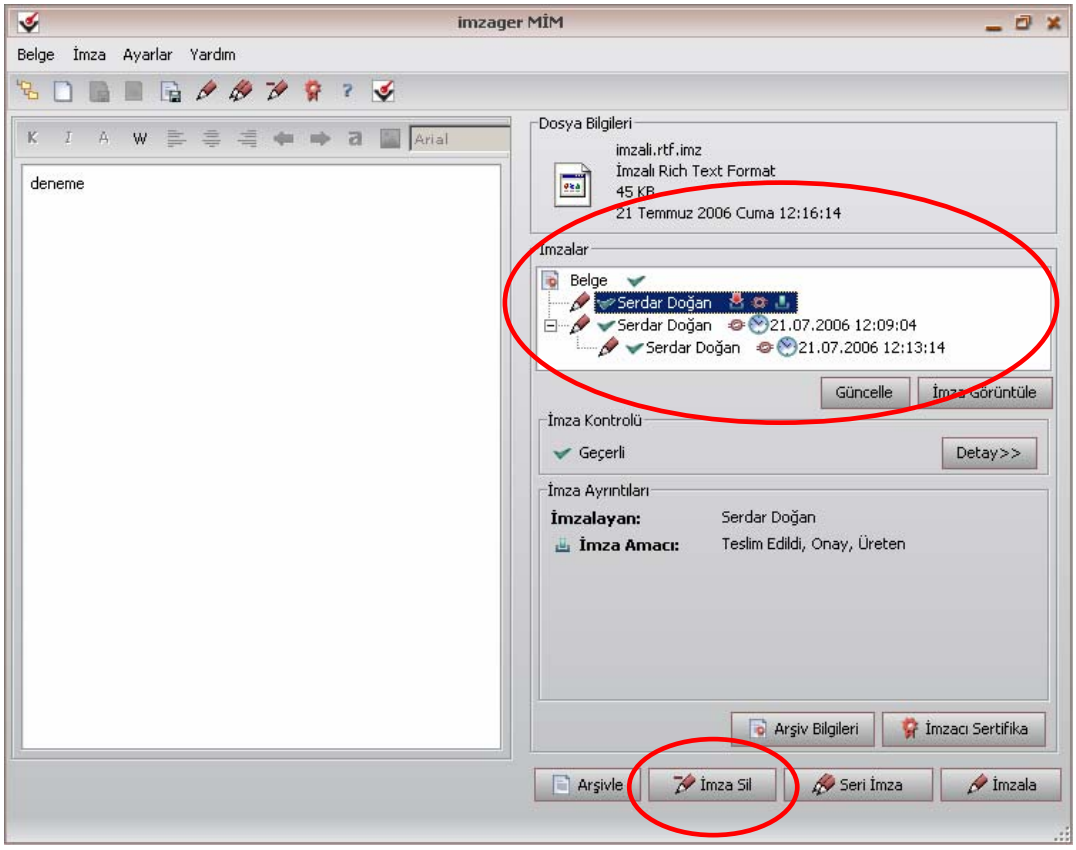
İmza içeren bir belgeye yeni bir imza ekleme işlemi, yukarıda detaylı olarak anlatılan kayıtlı bir belgeyi imzalamak işlemiyle aynıdır. Bu işlem sonunda söz konusu belgede yapılan imza kontrolü sonucu belgedeki tüm imzalar eklenti özellikleri ile birlikte detaylı olarak görülebilir (Şekil 5.66).



Şekil 5.66. İmzalı belgeye yeni imza ekleme işlemi

İmzanın Silinmesi

Silmek istenen imza seçildikten sonra aktif duruma gelen "İmza Sil" düğmesi ile imza silme işlemi başlatılır. Belgenin silme işleminden önceki hali kaydedilmek isteniyorsa çıkan uyarı mesajı onaylanır ve belge seçilen yere istenilen isimle kaydedilir. Bu işlemin tamamlanmasının ardından seçilen imza belgeden çıkarılır (Şekil 5.67).



Şekil 5.67. İmzanın silinmesi

<u>İmzalı bir belgenin içeriğinin kaydedilmesi</u>

İmzalı belgenin imzasız içeriği editörde görüntülenebilir formatta ise görüntülenen bu imzasız içerik “Belge” menüsünden “İçeriği Kaydet” ya da araç çubuğundan “İçeriği Kaydet” seçilerek kayıt edilebilir. Editörde görünmeyen imzalı belgeler ise “İçeriği Görüntüle” butonuna basıldıktan sonra açılan ilgili belgenin editörü üzerinden “Farklı Kaydet” seçeneği ile kaydedilebilir.

<u>Belgedeki bir imzanın imzalanması (seri imzalama)</u>

Hem belge içeriğini hem de belge içinde bulunan bir imzayı imzalama işlemine “seri imzalama” adı verilir. Standart imza kullanımı ETSI'nin tanımlamış olduğu paralel imza yapısına karşılık gelmektedir. Yani yeni bir imza eklendiğinde önceki imza ile

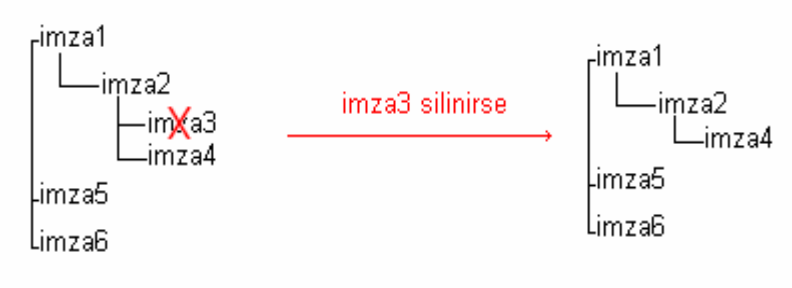
aynı seviyede bir imza eklenmektedir. Kağıt üzerindeki imzaya da mantık olarak en yakını paralel imza olarak düşünülebilir, öyle ki paralel imzada her imza belge içeriğini imzalar ve imzaya yeni bir nesne olarak eklenir, yeni imza bir önceki imzadan tamamiyle bağımsızdır. Seri imza (Counter Signature) ise başka birinin imzasının imzalanması şeklinde çalışır ve üzerinde bulunduğu imza ile bağlantılıdır. Paralel imzada imzalardan birini silmek diğer imzaları etkilemez, fakat seri imzada bir imzayı silmeniz durumunda o imza üzerindeki tüm imzalar da silinir.

Şekil 5.68. Seri imzalama-1

Şekil 5.68'de imza1, imza5 ve imza6 birbirlerine paralel imzalardır. imza2, imza1 üzerine atılmış, imza3 ve imza4 de imza2'ye atılmış seri imzalardır. imza3 ve imza4 birbirine paraleldir.

Şekil 5.69. Seri imzalama-2

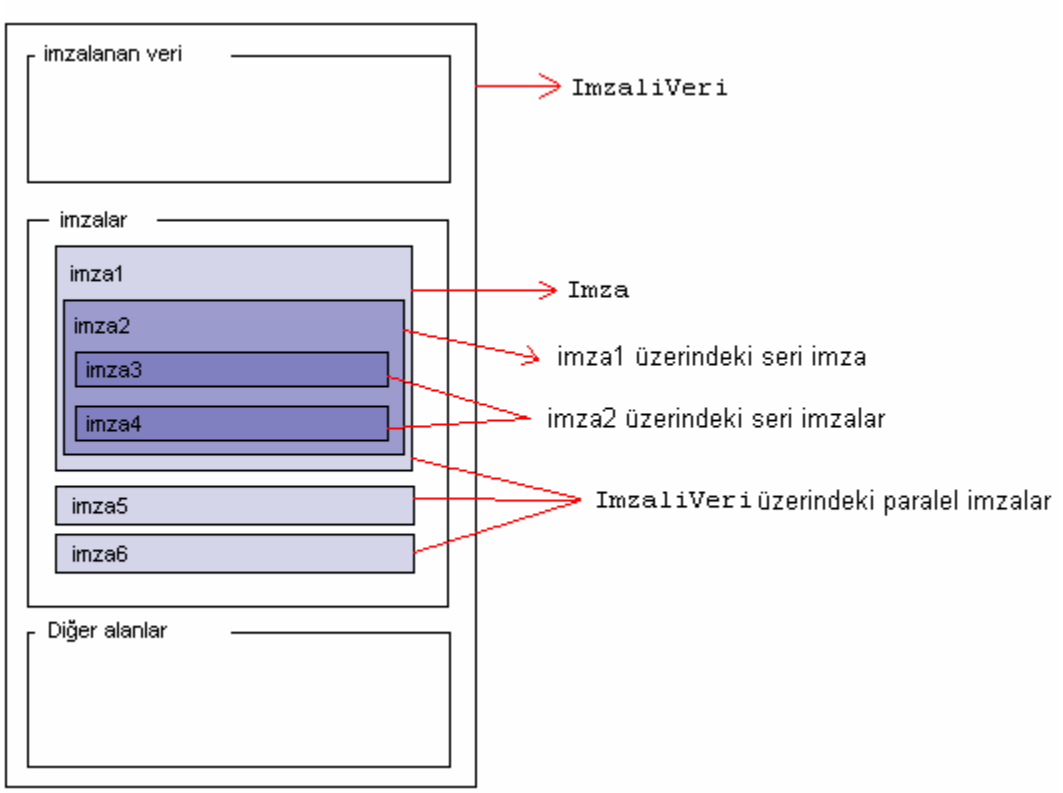
Şekil 5.68'de, imza1'in silinmesi durumunda ona bağlı olan tüm imzalar da silinir. Çünkü imza2 tamamiyle imza1'e bağlı olarak oluşturulmuş bir imzadır. İmza1 silindikten sonra, bu imzaya paralel olan imza5 ve imza6'ya birşey olmaz çünkü bu imzalar imza1'e paraleldir (Şekil 5.69).



Şekil 5.70. Seri imzalama-3

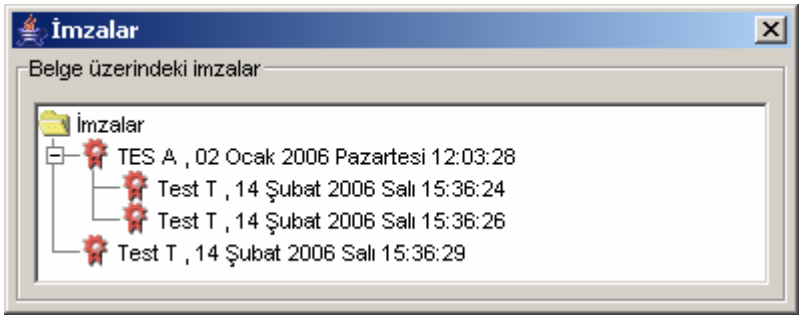
Yine Şekil 5.68'de imza2'ye seri ve imza4'e paralel olan imza3'ün silinmesi durumunda imza2'ye seri olarak imza4 kalmaktadır (Şekil 5.70).

Yukarıda seri ve paralel imza arasındaki ayrım örnekler ile açıklanmıştır. Islak imzadaki yöntemi paralel imzaya benzetebiliriz, çünkü ıslak imza ile bir belge imzalanacağı zaman aynı belgenin farklı kişiler tarafından imzalanması sözkonusu oluyor ve genelde herkes aynı kağıt üzerine imza atıyor. Bu kağıt üzerindeki imzalardan herhangibirini kişi istediği zaman silebilir ve bu başkalarının imzalarının geçerliliğini etkilemez. Paralel imzada da bu işlem aynı şekilde olur. Seri imzada ise alttaki imza silindiğinde ona bağlı tüm imzaların da silinmesi sözkonusudur (Şekil 5.71).



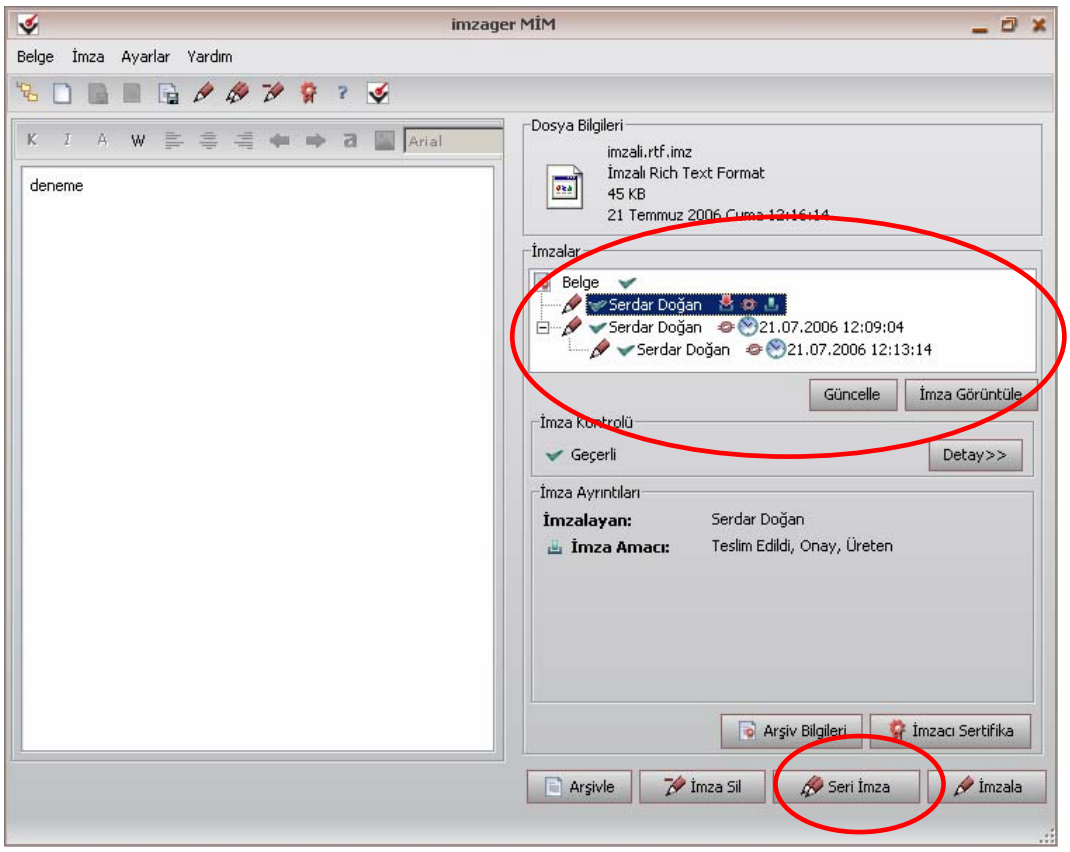
Şekil 5.71. Seri imzalama-4

İmzalı bir belge üzerindeki paralel ve seri imzalar ağaç yapısında temsil edilebilir. İmza hiyerarşisini göstermek için en iyi yöntemlerden biri imzaları ağaç yapısında göstermektir (Şekil 5.72).



Şekil 5.72. İmzaların ağaç yapısında gösterimi

İmzager MİM yazılımıyla seri imzalamayı gerçekleştirmek için imzayı seçtikten sonra aktif duruma gelen "Seri İmzala" düğmesi kullanılır. Sonraki adımlar kayıtlı bir belgeyi imzalamak işlemiyle aynıdır. Şekil 5.73'de seri imzalama yapılmış olan bir belge görüntülenmiştir.



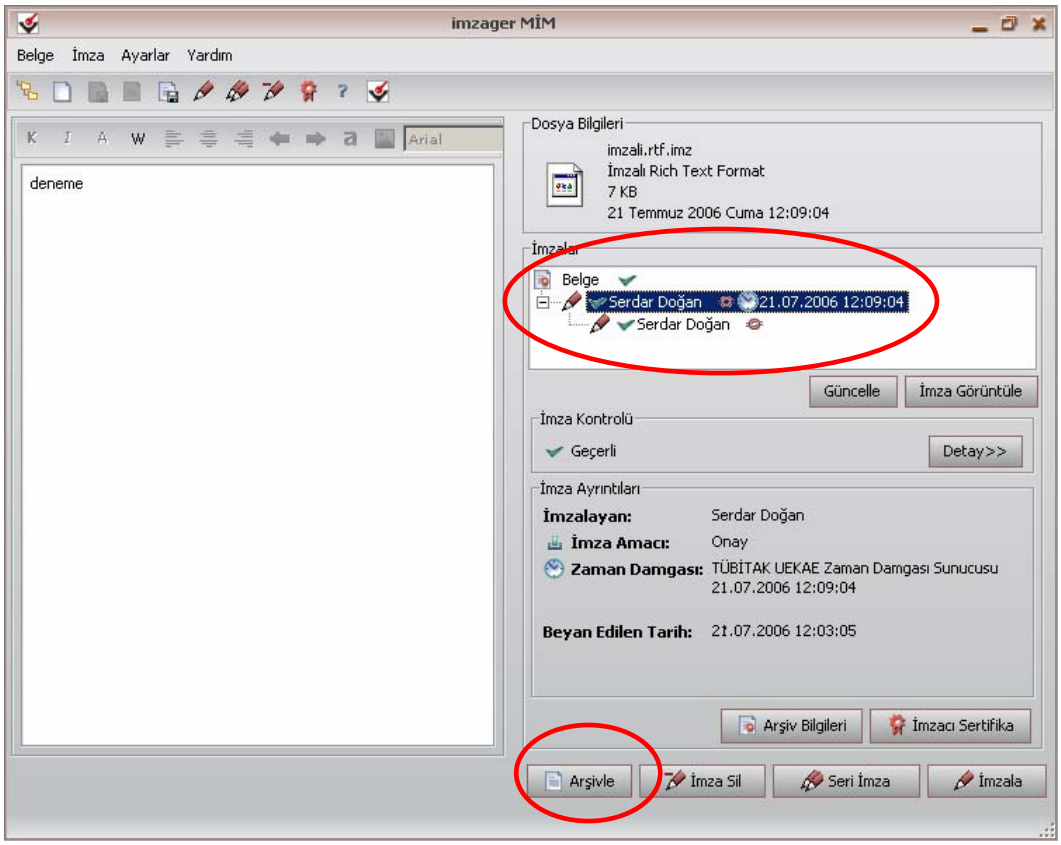
Şekil 5.73. İmzager MİM yazılımı ile seri imzalama

İmzalı belgenin arşivlenmesi

İmzalı belgelerdeki imza bilgileri, işleminin yapıldığı sertifika geçerli ve ilgili işlemi yapmaya yetkili olduğu sürece geçerli olarak görünür. Yani bugün geçerli bir sertifika ile imzalanan bir belge, ilerde belgeyi imzalayan sertifika iptal olduğunda imzası geçersiz bir belge olarak görünecektir. Bu da kurumsal ağlarda istenmeyen bir durumdur. Çünkü bugün imza yetkisi olan ve bu yetki ile birtakım belgeleri e-imza ile imzalayan bir personel yarın kurumdan ayrıldığında ya da imza yetkilerinde

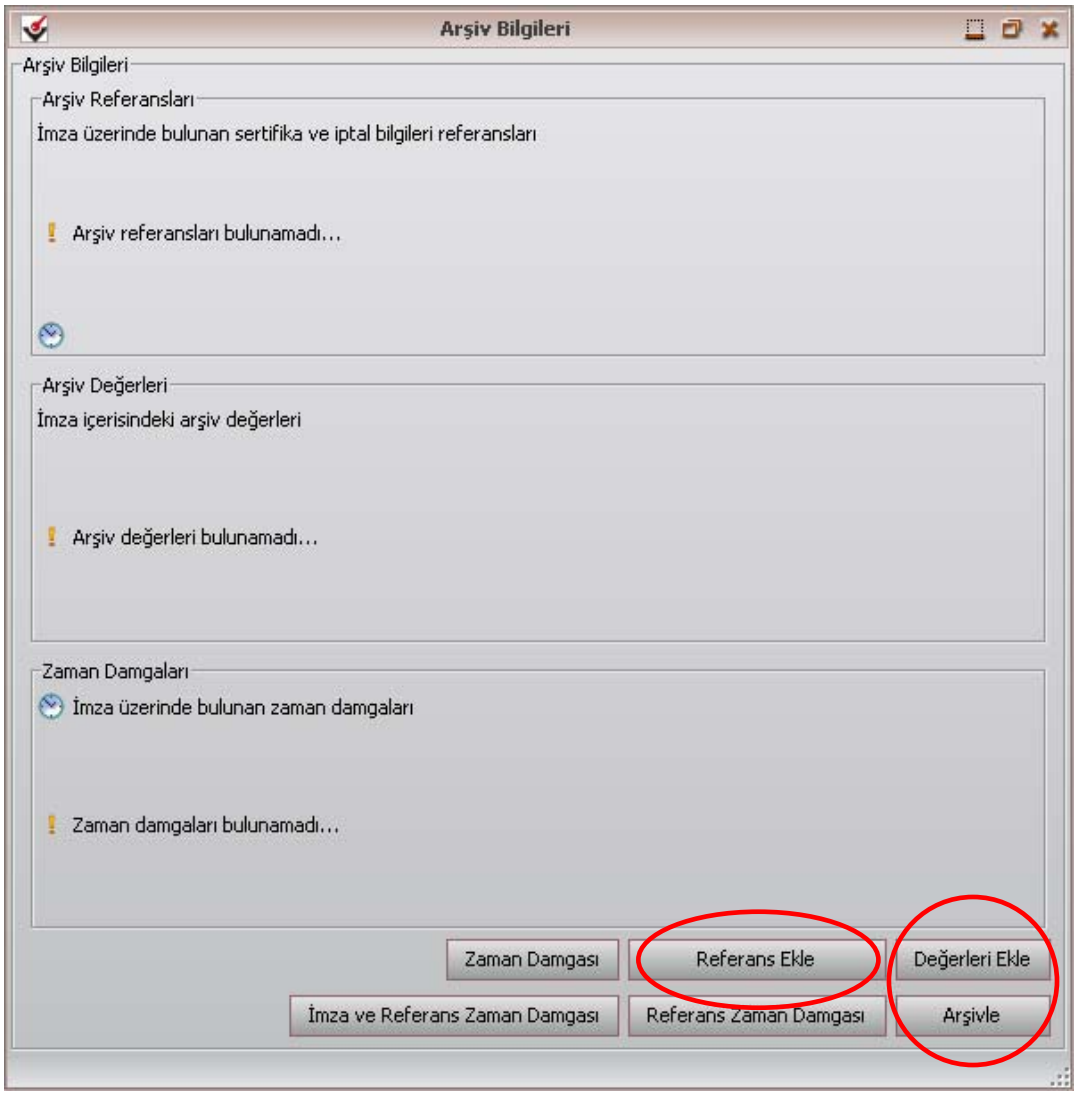
değişiklik olduğunda (bu durumda personelin mevcut sertifikası iptal edilir) artık onun yetkili olduğu dönemde imzaladığı tüm belgeler üzerindeki imzalar da geçersiz görünecektir. E-imza sistemlerindeki bu sorunun çözümü arşivleme fonksiyonu ile sağlanmıştır. Bu fonksiyon ile, belgenin arşivlendiği ve dolayısıyla imzanın geçerli olduğu andaki imza üzerinde bulunan tüm sertifika, iptal bilgisi referansları ve bunlara ilişkin değerler belgenin içine arşivlenir. Böylelikle, ilerde belgeyi imzalayan personelin sertifikası iptal dahi olsa, arşivlenen tarihte bu belgeyi imzalamaya yetkisi olduğu ve geçerli bir sertifika ile imzalama işlemini yaptığı anlaşılır.

İmzager MİM yazılımı ile arşivleme işlemi, Şekil 5.74'deki imzalı belge üzerindeki imzaların görüldüğü ekranda "Arşivle" butonuna basılarak yapılır.



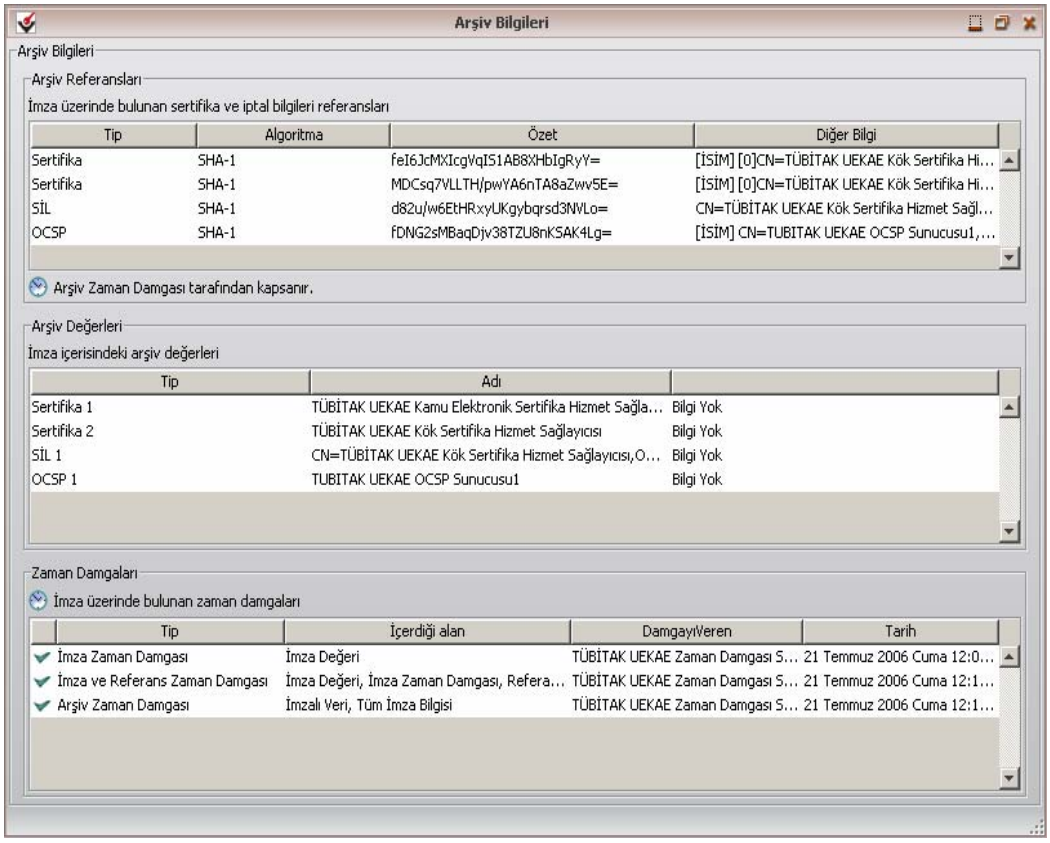
Şekil 5.74. İmzager MİM yazılımı ile arşivleme

Şekil 5.74'deki ekranda "Arşivle" butonuna basıldığında Şekil 5.75'deki "Arşiv Bilgileri" ekranı açılır. Bu ekrandaki "Referans Ekle", "Değerleri Ekle" ve "Arşivle" butonları ile arşivleme işlemi yapılır.



Şekil 5.75. İmzager MİM yazılımı arşiv bilgileri ekranı (boş)

Arşivleme işlemi yapıldıktan sonra ilgili arşiv bilgileri Şekil 5.76'daki ekran yardımıyla görülebilir. Bu ekrana, imzalı bir belge İmzager MİM yazılımı ile açıldığında gelen ekrandaki "Arşiv Bilgileri" butonuna basılarak da erişilebilir.



Şekil 5.76. İmzager MİM yazılımı arşiv bilgileri ekranı (dolu)

<u>İmzaya zaman damgası eklenmesi</u>

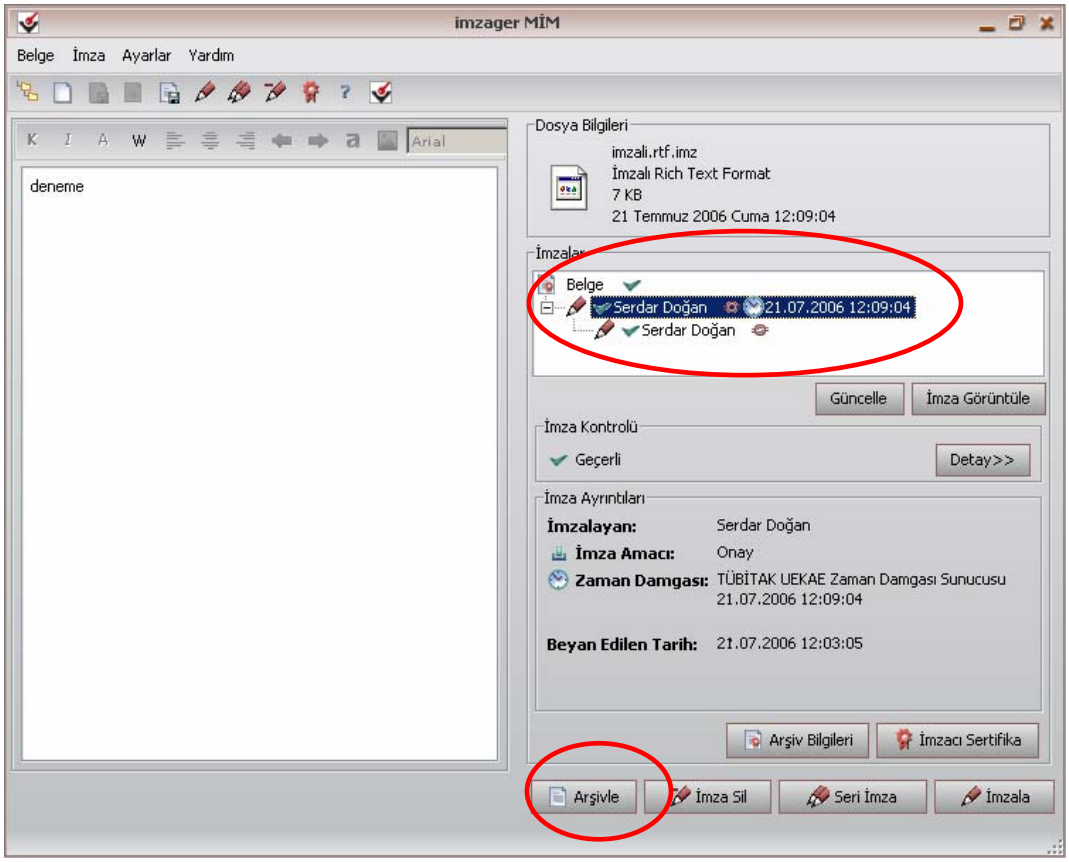
İmzanın üretildiği zamanı tespit etmek üzere oluşturulan güvenli elektronik veriye "zaman damgası" adı verilir. Zaman damgası, üzerinde bulunduğu verinin belirli bir tarihteki varlığını garanti eder. İmzayla birlikte kaydedilen sistem tarihi ve saatinin doğruluğundan emin olunamayacağından zaman damgası kullanılır. Zaman damgası, imzaya bağlı olarak oluşturulduğundan, imzanızın gerçekten o tarihte var olduğunu ispatlamak için kullanılır. Zaman damgası bir imza değil imzaya eklenen bir veridir.
İmza tarihinin önemli olduğu uygulamalarda zaman damgasının kullanımı büyük önem arzetmektedir. Çünkü zaman damgası olmayan bir imza üzerindeki zaman bilgisi, kullanıcının belirleyebildiği ve genelde kullanıcının sistem saatinden alınmış olan zaman bilgisidir. Dolayısıyla imzayı oluşturan kişi zaman bilgisini de istediği gibi belirleyebilir (Islak imzada olduğu gibi). Zaman damgası ise imzanın o tarihten

(zaman damgası otoritesinin verdiği tarihten) önce var olduğunu garanti eder. Belge üzerinde birden fazla imza var ise ve her imza için de zaman bilgisi önem arzediyor ise her imza için ayrı ayrı zaman damgası alınır.

Zaman damgası, güvenilir bir servis sağlayıcısı olan zaman damgası otoritelerinden alınır. Tüm ESHS'ler bu hizmeti vermektedirler.

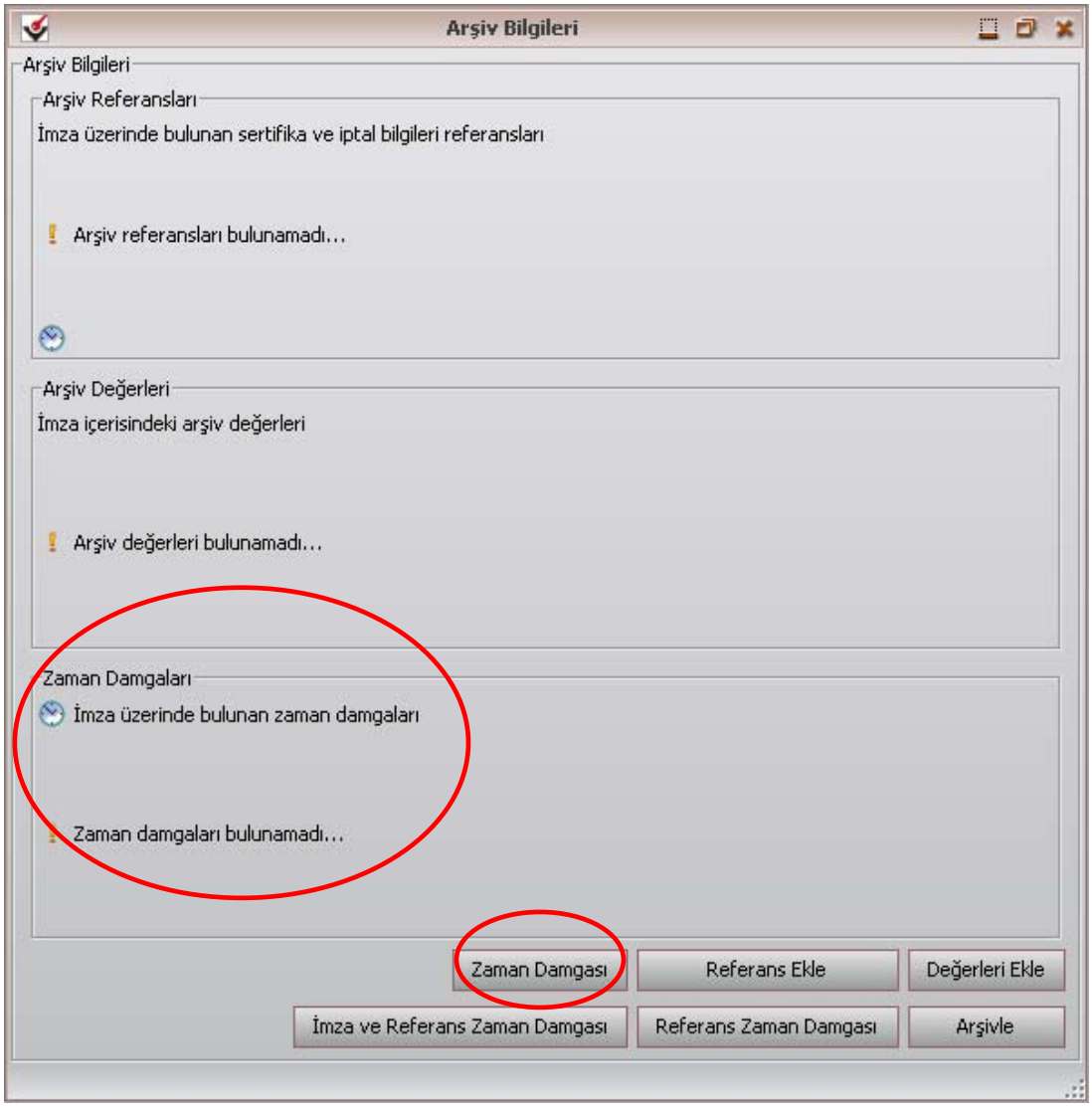
Zaman damgası bir zaman damgası otoritesinden alındığı için işlem sırasında bu otoritenin sunucusuna bağlantı gereksinimi mevcuttur. Bu yüzden zaman damgası alınacak olan bilgisayardan, otoritenin sunucusuna bağlantının sorunsuz olması ve güvenlik duvarı vb. uygulama ve donanımlarda bu işlem için gerekli ayarlamaların yapılması gerekir. Zaman damgası HTTP protokolü üzerinden (port 80) alındığından genelde güvenlik duvarı sıkıntısı yaşanmaz ama yine de bu portun açık olduğundan emin olunmalıdır.

İmzager MİM yazılımıyla imzaya zaman damgası ekleyebilmek için, belge üzerindeki imzaların görüntülendiği Şekil 5.77'deki ekranda zaman damgası eklenecek imza seçildikten sonra "Arşivle" butonuna basılır.



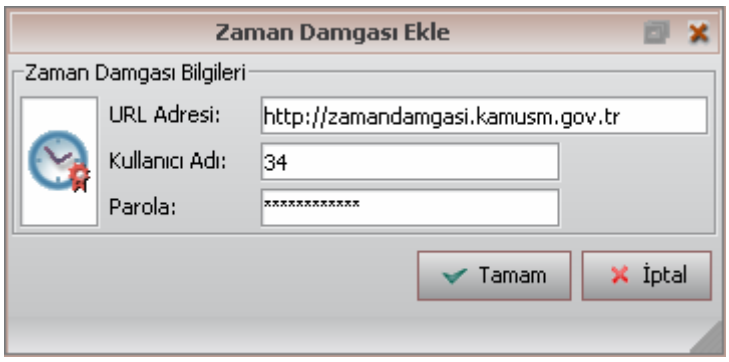
Şekil 5.77. İmzaya zaman damgası ekleme (imza bilgileri ekranı)

Açılan "Arşiv Bilgileri" ekranında imza üzerinde varsa zaman damgaları görülebilir. İmzaya zaman damgası eklemek için Şekil 5.78'deki "Zaman Damgası" butonuna basılır. Ayrıca "İmza ve Referans Zaman Damgası" ve "Referans Zaman Damgası" da bu ekrandan eklenir.



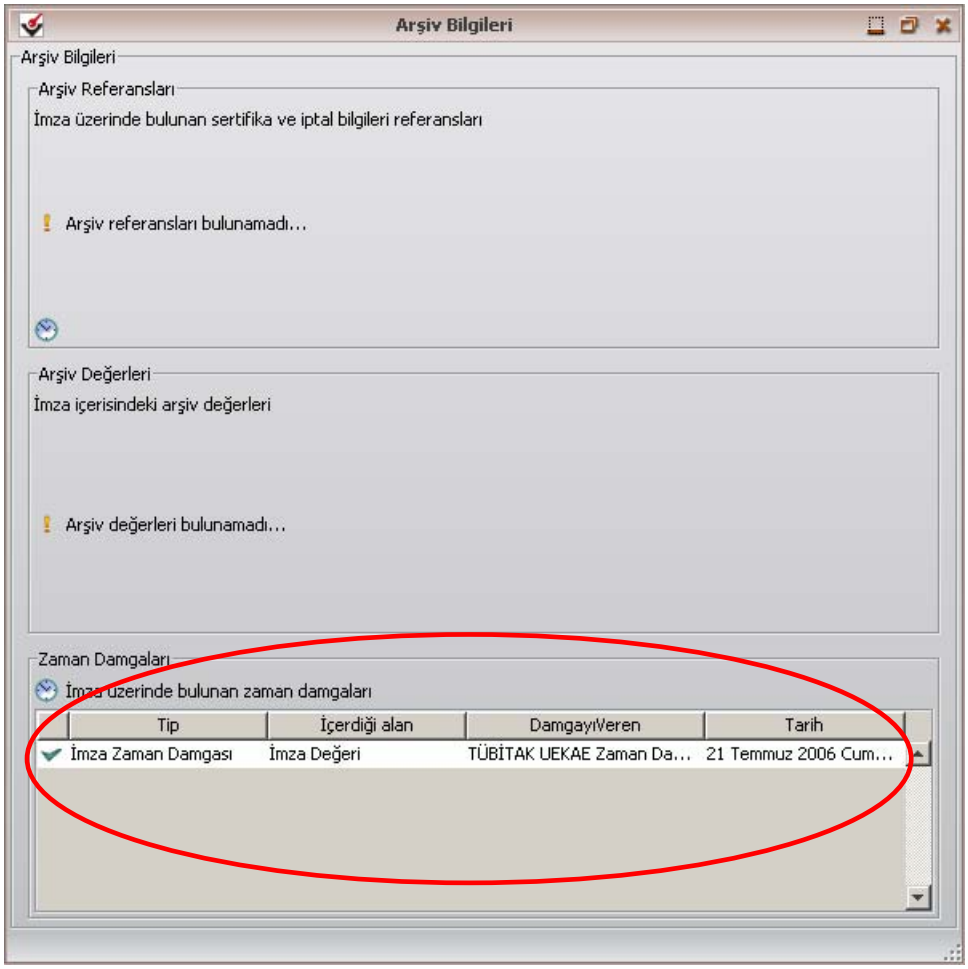
Şekil 5.78. İmzaya zaman damgası ekleme (arşiv bilgileri ekranı)

"Zaman Damgası" butonuna basıldığında, yazılım zaman damgası bilgilerini almak üzere Şekil 5.79'daki diyalog penceresini açar. Bilgiler girilip onaylandıktan sonra seçilen imzaya zaman damgası eklenir. Bu bilgiler zaman damgası otoritesinden ücreti karşılığında alınan bilgilerdir.



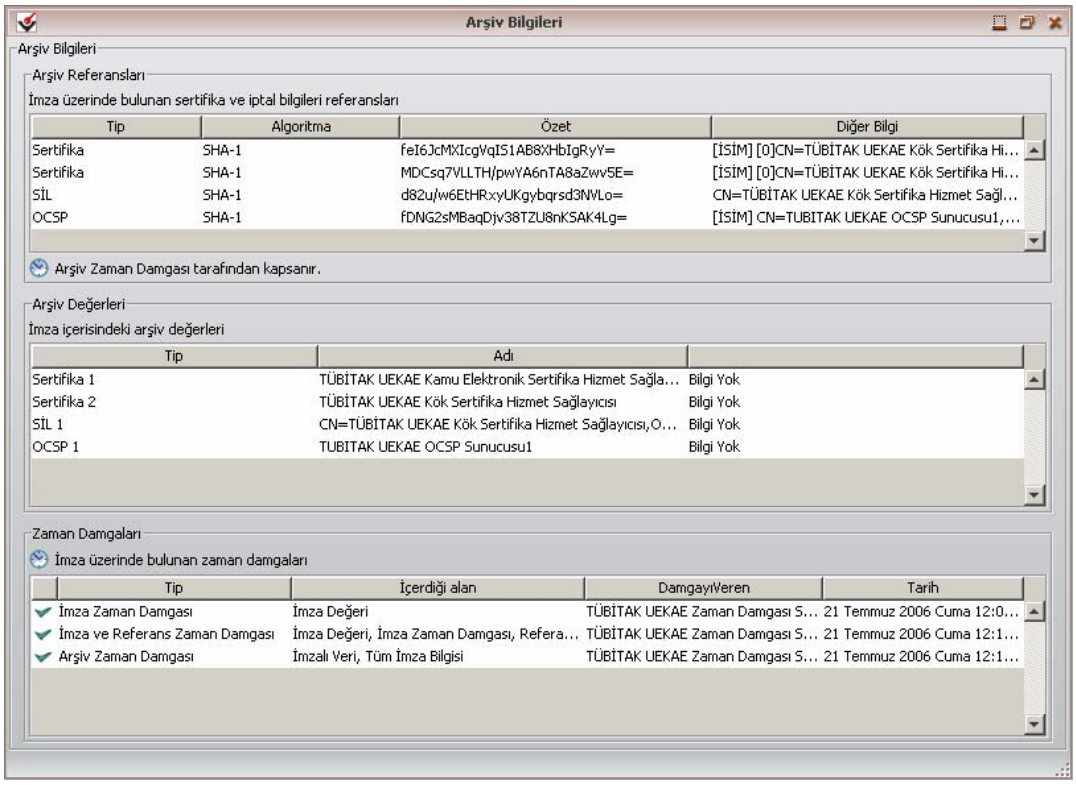
Şekil 5.79. Zaman damgası ekleme ekranı

"Zaman Damgası" ekleme işleminin ardından eklenen zaman damgası Şekil 5.80'deki "Arşiv Bilgileri" ekranında görüntülenir.

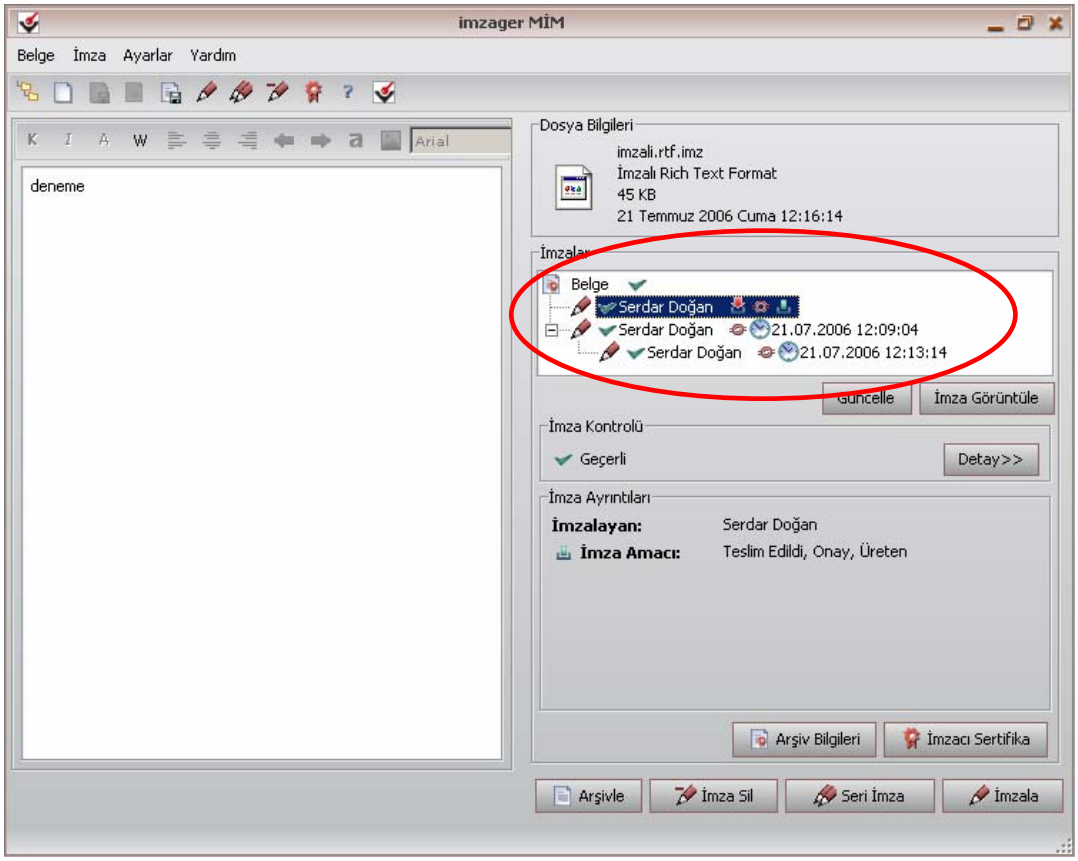


Şekil 5.80. Zaman damgası ekranı

Şekil 5.81'de arşiv referansları ve arşiv değerleri girilmiş bir imza için alınan "imza zaman damgası", "imza ve referans zaman damgası" ve "arşiv zaman damgası" bilgileri görülmektedir. Bu bilgiler ayrıca, Şekil 5.82'deki İmzager MİM yazılımının imza bilgilerini görüntülediği ana ekranında da tarih bilgisi ve simge olarak görülmektedir.



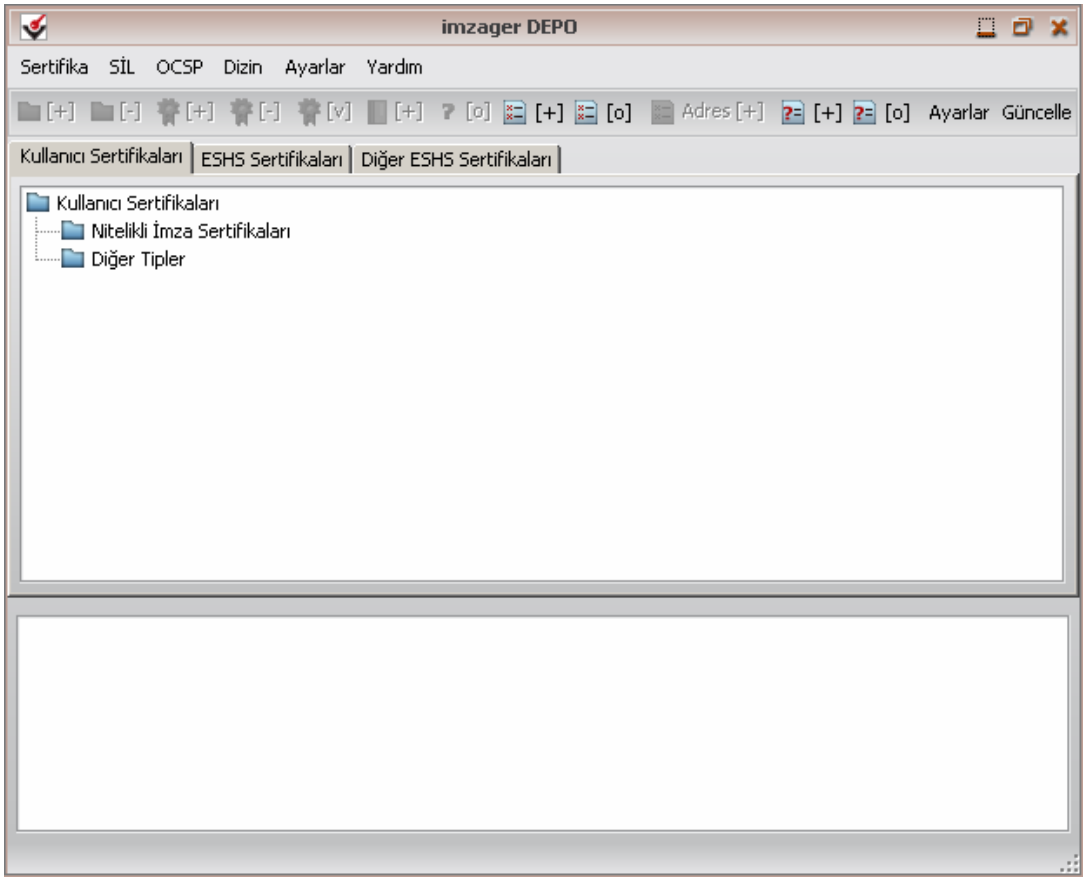
Şekil 5.81. İmzager MİM yazılımı arşiv bilgileri ekranı



Şekil 5.82. İmza üzerindeki arşiv ve zaman damgaları

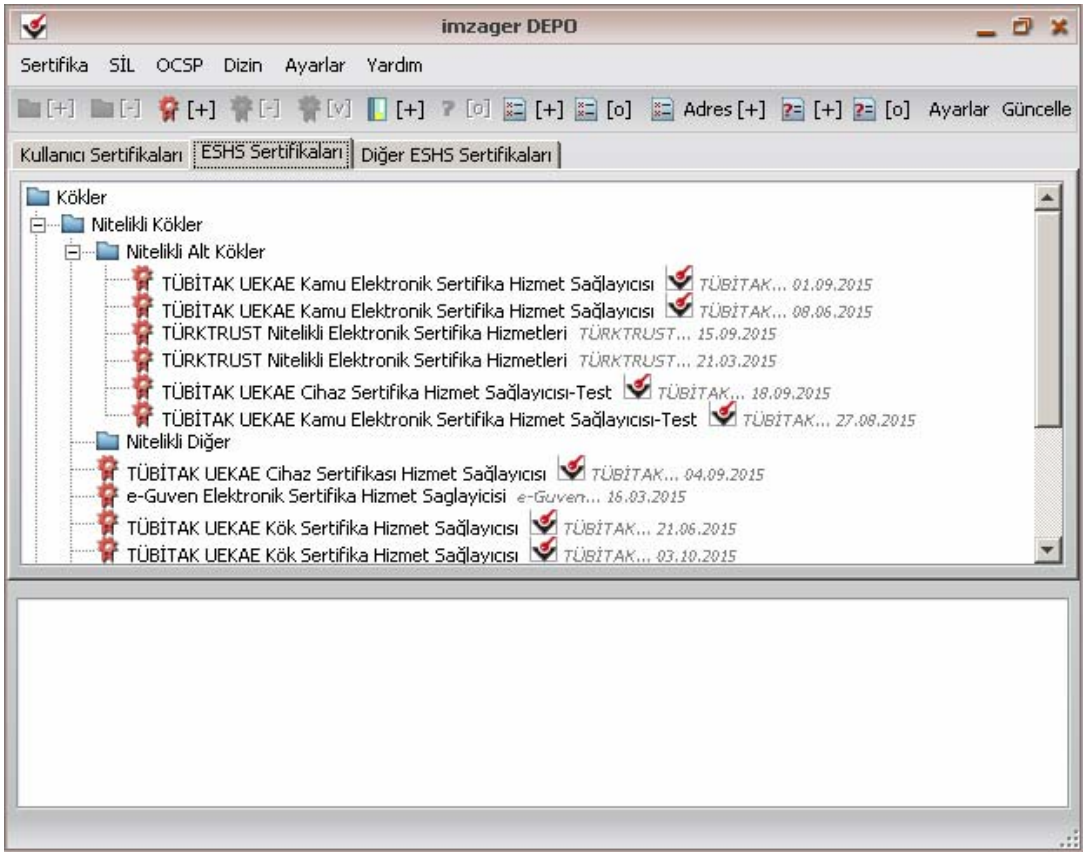
İmzager DEPO (sertifika deposu)

İmzager DEPO ile bilgisayar üzerinde yüklü olan sertifikalar kolaylıkla görülerek yönetilebilir. Bu fonksiyon ile bilgisayar üzerinde bulunan sertifikalar Şekil 5.83'de gösterildiği gibi "Kullanıcı Sertifikaları", "ESHS Sertifikaları" ve "Diğer ESHS Sertifikaları" alt başlıklarında gruplar halinde görüntülenebilir.



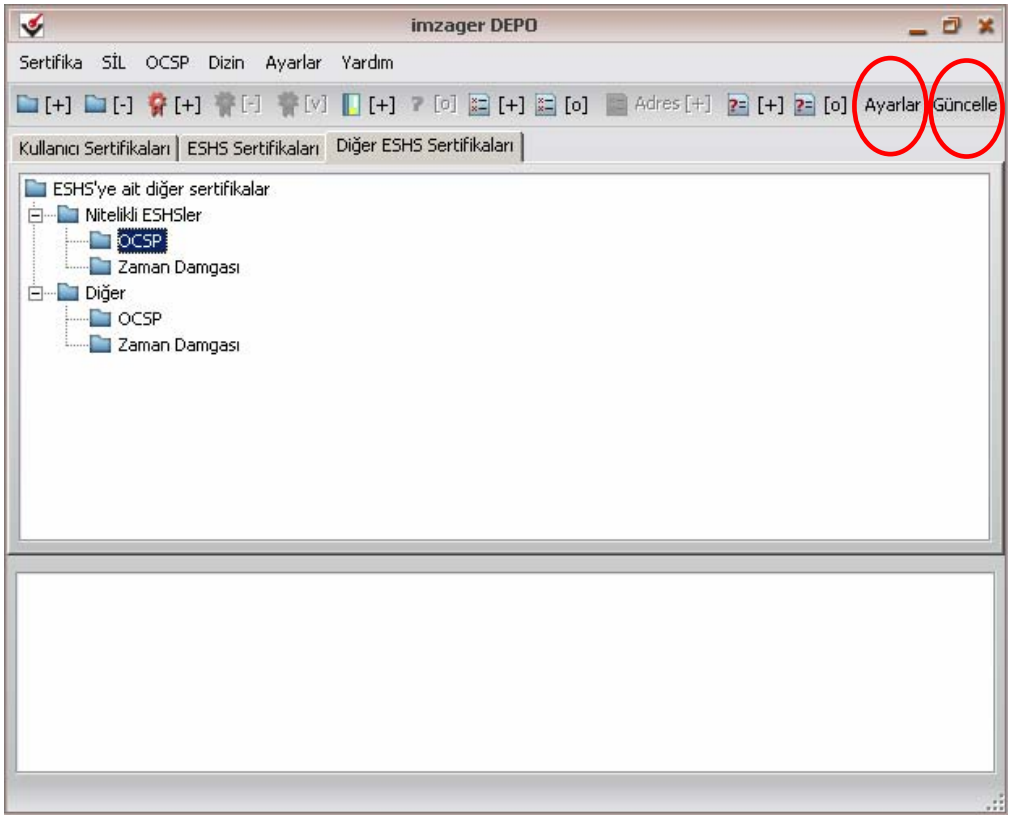
Şekil 5.83. İmzager DEPO kullanıcı sertifikaları ekranı

Yazılım menülerindeki “ESHS Sertifikaları” butonuna basıldığında Şekil 5.84’deki ekran açılır. Bu ekranda, bilgisayarda yüklü olan ve kanuni geçerliliği olan nitelikli sertifikalar görülmektedir.



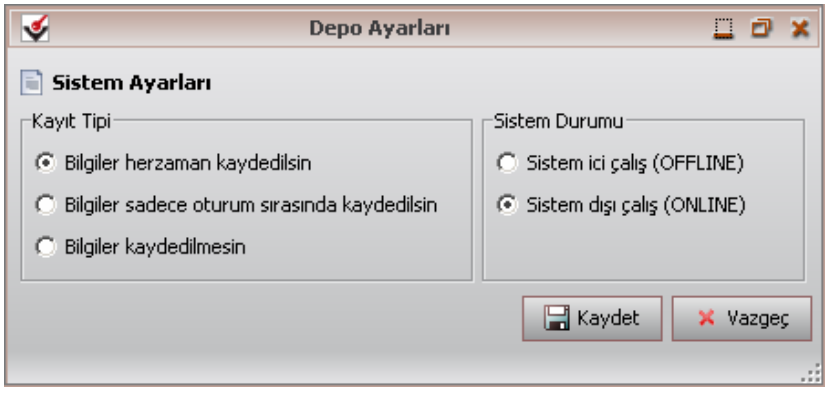
Şekil 5.84. İmzager DEPO ESHS sertifikaları ekranı

"Diğer ESHS Sertifikaları" butonuna basıldığında ise "OCSP" ve "Zaman Damgası" sertifikaları, Şekil 5.85'de görüldüğü gibi "Nitelikli ESHS'ler" ve "Diğer" alt grupları altında görülmektedir.



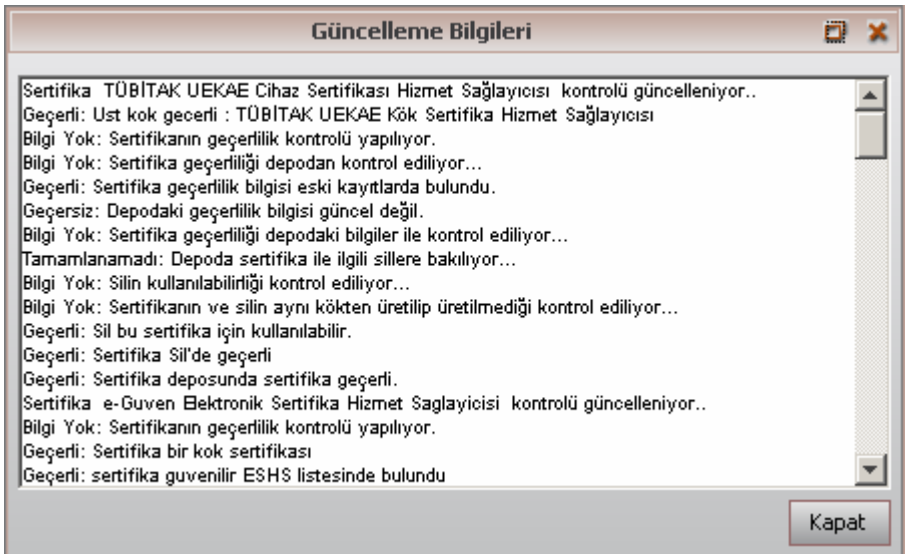
Şekil 5.85. İmzager DEPO diğer ESHS sertifikaları ekranı

Şekil 5.85'de de görülen İmzager DEPO'nun ana ekranı üzerinde "Ayarlar" butonuna basıldığında sistem ayarlarına ilişkin Şekil 5.86'daki ekran açılır. Bu ekranda sertifikaların kayıt tipi ve sistemin çalışma durumu (sistem içi-sistem dışı) kullanıcı tarafından belirlenebilmektedir.



Şekil 5.86. Depo ayarları ekranı

Şekil 5.85'deki ekranda "Güncelle" butonuna basıldığında ise Şekil 5.87'deki sisteme ilişkin güncelleme bilgileri ekranı açılır.



Şekil 5.87. Güncelleme bilgileri ekranı

5.5.5. Test

Yapılan gereksinim belirleme, analiz, tasarım ve gerçekleştirim çalışmaları sonucu Gazi Üniversitesi'nde Bölüm 5.5.3'de belirlenen birimlerde simule edilen örnek uygulama, öncelikle test amaçlı olarak kullanıma açılmıştır. Bu testler sonucu kullanıcılardan sisteme ilişkin geri beslemeler alınmıştır. Geri beslemeler doğrultusunda gerekli iyileştirmeler yapılarak sistemin gerçek kullanıma açılacak seviyeye gelmesi sağlanmıştır.

5.5.6. Kullanım ve yaygınlaştırma

Gazi Üniversitesi'nde örnek uygulama olarak belirli birimler arasında ve belirli alanlarda hayata geçirilen e-imza uygulamasının testleri başarıyla tamamlandıktan sonra Üniversite geneline ve aşama aşama tüm iş akışlarına e-imza entegrasyonunun sağlanması uygun olacaktır. Bu çalışmada örnek uygulama gerçekleştirildiği için yaygınlaştırma yapılmamıştır.

5.6. Uygulama Sonuçları

Bu çalışmada gerçekleştirilen örnek uygulama ile Gazi Üniversitesi'nde bazı birimler arasında kağıt ortamında ve klasik yöntemlerle yapılan yazışmalar elektronik ortama aktarılmıştır. Simule edilen örnek uygulama ile birimler arasında masraflı ve yavaş bir şekilde süren ve bürokratik yük oluşturan yazışmaların çok daha hızlı, güvenli ve ucuz olarak gerçekleştirilebildiği görülmüştür.

Gazi Üniversitesi'nde iki birim arasında gerçekleştirilen örnek e-imza uygulamasının ortalama maliyeti Çizelge 5.3'de verilmiştir. Burada verilen maliyetler ortalama ve KDV hariç değerlerdir.

Çizelge 5.3. Örnek e-imza uygulamasının maliyeti

NO	GEREKSİNİM	ADET	MALİYET
1	Nitelikli Elektronik Sertifika (Akıllı kart ve kart okuyucu dahil)	8 adet	145 YTL*8 adet=1160 YTL
2	Kişisel Bilgisayar (PC)	8 adet	Kurumun mevcut bilgisayarları kullanıldığından ilave maliyet yoktur.
3	Tarayıcı (Scanner)	8 adet	Kurumun mevcut tarayıcıları kullanıldığından ilave maliyet yoktur.
4	Yazıcı (Printer)	8 adet	Kurumun mevcut yazıcıları kullanıldığından ilave maliyet yoktur.
5	Kişisel bilgisayar internet erişimi	8 adet	Kurumun mevcut internet altyapısı kullanıldığından ilave maliyet yoktur.
6	Kullanıcılar için e-posta adresi	8 adet	Kurum tarafından zaten e-posta hizmeti verildiğinden ilave maliyet yoktur.
7	Merkezi dosya sunucu	1 adet	Kurumun mevcut dosya sunucusu kullanıldığından ilave maliyet yoktur.
8	MS Outlook 2003 Programı	8 adet	Kurumda mevcut olan lisanslı ürün kullanıldığından ilave maliyet yoktur.

Çizelge 5.3. (Devam) Örnek e-imza uygulamasının maliyeti

NO	GEREKSİNİM	ADET	MALİYET
9	E-imza yazılımı (İmzager)	1 adet	Kamu kurumları için İmzager yazılım kütüphanesi fiyatı (E-imza, .NET veya Java) 7500 YTL+KDV'dir.
10	Danışmanlık ve eğitim hizmetleri	10 gün	10 günlük eğitim ve danışmanlık hizmeti fiyatı 11000 YTL+KDV'dir.

Örnek uygulama, iki birim arasında, sınırlı uygulama alanlarında ve mevcut donanımların kullanımıyla gerçekleştirildiğinden Çizelge 5.3'de verilen maliyetler oldukça düşük çıkmıştır. Ancak e-imza projelerinin kapsam ve uygulama alanları arttıkça maliyetler de aynı oranda artacaktır. E-imza projelerinin en önemli ve maliyetli kısmını kullanılacak e-imza uygulaması oluşturmaktadır. Kurumsal ağlarda e-imza uygulamaları farklı yöntemlerle gerçeklenebilir. Bunlardan ilki ve daha düşük maliyetli olanı, e-imza uygulamalarının veya mevcut kurum uygulamalarında sağlanacak e-imza desteğinin kurum yazılımcıları tarafından ESHS yazılım kütüphaneleri kullanılarak gerçekleştirilmesidir. Diğer yöntem ise kurum tarafından doğrudan hazır e-imza yazılımlarının tedarik edilmesi veya e-imza ihtiyacının projelendirilerek ihale edilmesidir. Bu yöntemde özellikle elektronik doküman yönetim sistemleri de devreye girdiğinde maliyetler artmaktadır. Ancak sisteme yapılan yatırım kendini kabul edilebilir sürelerde maddi olarak geri kazandırmaktadır. Sistemin kazanımları ve maddi tasarruf sağlanan alanlar aşağıda açıklanmıştır.

Gazi Üniversitesi'nde gerçekleştirilen e-imza uygulaması ile birçok alanda maddi tasarruflar sağlandığı görülmüştür. Genel olarak e-imza ile gerçekleşen iş süreçlerine harcanan toplam zaman, kağıt ortamında ıslak imza kullanılarak gerçekleşen iş süreçlerine harcanan zamandan daha az olmaktadır. Ayrıca e-imza ile yürütülen iş süreçleri ağırlıklı olarak imza yetkisi olan personel tarafından gerçekleneceği için, ıslak imzalı süreçlerdeki birimler arası evrak taşıyan veya bu evrakları imzaya hazırlayan/çıkaran personel yönünden de ciddi tasarruflar sağlanmaktadır. Bu

kapsamda e-imza ile gerçekleşen iş süreçlerinin daha az sayıda personel ile daha etkin ve hızlı olarak yapılabildiği görülmüştür.

Yukarıda açıklanan personel ve zaman tasarruflarına ek olarak elektronik veya kağıt ortamında belge işleme maliyetleri de göz önünde bulundurulmalıdır. Gartner'a göre klasik bir sistemde;

- Ortalama olarak bir belge, kağıt veya elektronik ortamda 9 ile 11 kez arasında kopyalanıyor ve maliyeti 18 dolar,
- Belgelerin dosyalanma maliyeti belge başına 20 dolar,
- Yanlış dosyalanmış bir belgenin bulunmasının maliyeti 120 dolar,
- Kaybolmuş veya bulunamayan belgelerin maliyeti ise rakamla ifade edilememektedir.

Elektronik doküman yönetim sistemleriyle de entegre olan e-imza sistemleri yukarıda listelenen ilave maliyetleri de ortadan kaldırarak daha ciddi ölçüde tasarruf ve iş verimi sağlayacaktır.

Günümüzde, yaklaşık bir tahminle, kurum ve kuruluşların % 90'ından fazlasının, iş süreçlerini kağıt belge ile yürüttüğü, dokümanların önemli bir kısmının yanlış yerleştirilmiş ve bir daha bulunamayacak durumda olduğu, kullanıcıların haftada en az 8 saatini belge işlemleri için bedensel hareket ile kaybettiği, belgelerin zaman içinde çok sayıda kopyasının yaratıldığı ve çalışanların zamanlarının büyük bir kısmını doküman yönetimine yönelik çalışmalara harcadığı görülmektedir. Özellikle kamu kurumları gözönüne alındığında bu kayıplar daha da artmaktadır. Simule edilen örnek uygulama sonucunda, e-imzanın birçok açıdan kurumlara, özellikle kamu kurumlarına israf önleme ve verimlilik açısından büyük faydalar sağlayacağı sonucuna varılmıştır.

Geliştirilen e-imza uygulaması ile, imzalanması gerekecek belgelerin ve yine kağıt ortamındaki kopyalarının taraflar arasında fiziksel olarak taşınması da

gerekmemektedir. Bütün bilgi ve belgeler kullanıcıların izni dahilinde çevrim-içi olarak elektronik ortamdan taşınmakta ve böylelikle kağıt ve nakliye konularında tasarruf sağlanmaktadır. Bu bilgi ve belgelerin taraflar arasında taşınması elektronik ortamda daha hızlı yapılacağı için zaman tasarrufu da sağlanmaktadır.

Geliştirilen uygulamada belirlenen birimler arasındaki ayda ortalama 800 sayfa evrak trafiği olduğu ve bu trafiğin e-imza ile bilgisayar ortamına aktarılması sonucu sadece kağıt ve mürekkep kaleminden (iş gücü hariç) iki birim arasındaki haberleşme için ayda 100 YTL tasarruf edilebileceği görülmüştür. Ayrıca kağıt ortamında yapılan belge yönetimine oranla elektronik ortamda yapılacak belge yönetimi çok daha etkili ve maliyet etkin olmuştur. Yapılan hesaplamalar, e-imza sisteminin hayata geçirilmesi için yapılacak harcamaların (sertifika, akıllı kart, akıllı kart okuyucu, eğitim, danışmanlık maliyetleri vb.) kendini kısa sürede geri kazandıracağını göstermiştir.

E-imza altyapısının sağladığı güvenlik sayesinde bilgi ve belgelerin gizliliği de sağlanabildiğinden önceden sağlanan fiziki önlemlere de gerek kalmamıştır. Ayrıca bilgi ve belgeler elektronik ortamda kurumsal bir arşivde gizliliği sağlanarak tutulduğundan mevcut durumda kullanılan dosya, dolap ve arşiv odası gibi uygulamalardan da tasarruf sağlanmıştır. Dolayısıyla kağıt ortamında yapılan belge yönetimine oranla elektronik ortamda yapılacak belge yönetimi çok daha etkili olmaktadır. Zaman, mekan ve kağıt tasarrufu sağlandığında ise verimlilik artmaktadır.

Gazi Üniversitesi'nde gerçekleştirilen örnek e-imza uygulaması ile tespit edilen, e-imza uygulamalarının kurumsal ağlara sağlayacağı kazanımlar maddeler halinde aşağıda özetlenmiştir:

- Yüksek seviyede güvenliğin sağlanması,
- İş süreçlerinin iyileştirilmesi,
- İş gücünün etkin kullanımı,

- Düşük maliyet,
- Kurum içi birimler arası karşılıklı işletilebilirlik,
- Güncel çözüm,
- Kağıt tüketiminde azalma,
- Daha esnek yönetim,
- Verimliliğin artması.

6. SONUÇ VE ÖNERİLER

Bu çalışmada, Gazi Üniversitesi'nde örnek bir e-imza uygulaması simule edilmiştir. Gerçekleştirilen uygulama sonucunda e-imza ile elektronik ortamda yüksek seviyede güvenliğin sağlanabileceği, iş süreçlerinin iyileştirilebileceği, iş gücünün daha etkin kullanılabileceği, iş yapma maliyetlerinin düşürülebileceği, kurum içi birimler arası karşılıklı işletilebilirliğin sağlanabileceği, kurumda kağıt ve kırtasiye tüketiminin azaltılabileceği ve daha esnek yönetimin gerçekleştirilebileceği görülmüştür.

Dünyada ve ülkemizdeki mevcut e-imza projeleri ve Gazi Üniversitesi'nde simule edilen örnek uygulama, e-imzaya geçiş işleminin çok kapsamlı olduğunu göstermiştir. Kurumsal ağlarda e-imzaya geçiş süreçlerinde dikkatli davranılmazsa başarısız e-imza uygulamaları ortaya çıkabilir. Bu nedenle alınacak yazılım, donanım ve hizmetler konusunda çok dikkatli olunmalı, bilinçli yaklaşılmalı, güvenilirlik / süreklilik / kurumsallık sorgulamaları iyi yapılmalı ve hizmet kalitesi doğru değerlendirilmelidir.

Bu çalışma kapsamında araştırılan konular ve yapılan örnek uygulama sonucunda elde edilen, Türkiye'de e-imzanın yaygınlaşmasına yönelik öneriler aşağıda sunulmuştur:

- Devlet, diğer ülkelerdeki devletlerin üstlendiği role benzer olarak, e-imza teknolojisinin ülkemizde kullanılması, yaygınlaştırılması, benimsenmesi ve üretilmesi aşamalarında işbirliği yapması gereken kurumlar arasında (iş dünyası, son kullanıcı, AR-GE birimleri, üniversiteler vb.) katalizör görevini daha etkin olarak üstlenmelidir.
- E-imzanın toplumda yaygınlaştırılmasını sağlamak için öncelikle bireylerin e-imzanın ne olduğunu kavramaları ve elektronik yaşamla birlikte e-imza kullanımının hayatlarına getireceği kolaylıkları fark etmeleri gerekmektedir. Bu amaçla yapılacak etkinlikler, temel eğitim, basılı ve görsel medya, üniversiteler, sivil toplum örgütleri aracılığıyla yapılabilir.

- e-Dönüşüm çalışmalarının ülkemizde hızlanmasıyla bir çok problemle karşılaşılabileceğinden, bu yeni teknolojinin sık sık yeniden değerlendirilmesi ve ilgili birimler ve kurumlarca tartışılması gerekmektedir. Bu çalışmalarda e-imzanın Türkiye geneline yaygınlaştırılması, geliştirilmesi ve uygulamaları konusunda ortaya çıkan problem ve sıkıntıların ortadan kaldırılması için bilimsel bir ortam hazırlanmalı ve ülkemizin e-imza konusunda yapması gerekenler belirlenerek gelecek vizyonunun oluşturulmasına katkı sağlanmalıdır. Telekomünikasyon Kurumu ve Gazi Üniversitesi'nin işbirliği ile 7-8 Aralık 2006 tarihlerinde ilki düzenlenecek olan "Ulusal Elektronik İmza Sempozyumu" (http://www.eimza.org.tr) bu kapsamda ülkemizde yapılan en önemli ve kapsamlı çalışmalardan biridir. Bu sempozyum ve benzeri platformlar, ülkemizde e-imza konusunda karşılaşılabilecek sıkıntıların azaltılmasına katkı sağlayacaktır.
- Devlet dairelerinde veya halka açık devlet kontrolündeki merkezlerde, halka e-devlet uygulamalarına erişmekte kullanılmak üzere ücretsiz bilgisayar ve internet erişim hizmeti verilmelidir. Bu merkezlerde bilgi eksikliği olan vatandaşa eğitimli ve güvenilir personel tarafından uygulamaların kullanımında yardım edilmelidir.
- E-Devlet konusunda henüz yatırım yapmamış olan kurumlar ile yeni yatırımlar yapacak kurumların, mevzuatın getirdiği e-imza ihtiyaçlarını da göz önünde bulundurarak yatırım yapmaları, ihale şartnamelerini mutlaka e-imzaya uygun hazırlamaları gereklidir.
- Vergi numarasında olduğu gibi e-imzanın da mecburi tutulması kullanımı artırmak için gereklidir.
- Kamu, maliyetleri düşürmek, hizmet kalitesini ve devletin etkinliğini arttırmak için elektronik uygulamalara geçmek ve kağıdı kaldırmak üzere, e-imzanın kullanımını teşvik etmelidir.
- Kamu en iyi örneği oluşturmak üzere, önce kendi içinde kalan iş akışlarında, sonra özel kurum ve kuruluşlarla ilişkilerinde ve son olarak vatandaşlarla ilişkilerinde e-imzaya geçişi planlamalı ve adım adım uygulamalıdır.
- Kamu kurumları bütçe kaynağı sıkıntısı çekmektedir. E-imza uygulamaları ise belli yatırımların yapılmasını gerektirmektedir. Bu nedenle kurumların talep ettikleri bütçeler çoğunlukla kesintiye uğramaktadır. TBMM ve Hükümet nezdinde bu

konunun gündeme getirilmesi ve e-imza uygulamaları için düşünülen bütçelerin kesintiye uğratılmamasının sağlanması yönünde çalışmalar yapılmalıdır.

- Kurumsal ağlar için uygulanabilir e-imza modelleri "Kurumsal Bilgi Birikimi", "Bireysel Bilgi ve Uyum Yeteneği", "Kurumsal Entegrasyon ve Uygulama Zamanı" ve "Donanım ve Yazılım İhtiyacı-Kaynak" kriterlerine bağlı olarak değerlendirilmeli ve Bölüm 3.7'de önerilen 3 modelden kuruma en uygun olana göre e-imzaya geçiş planı yapılmalıdır. Kurum için planlanan model ve modeller arası dönüşümler adım adım takip edilerek en ideal sisteme ulaşılmalıdır.
- Kurumlar arası e-imza uygulamalarının sağlıklı şekilde hayata geçirilmesi için standart çözümler kullanılmalı ve uygulamalar hayata geçirilmeden önce işbirliği içinde bulunulan kurumlarla koordinasyon sağlanmalıdır.
- Kurum yöneticileri ve çalışanlarının, alışkın oldukları mevcut iş süreçlerinin, e-imzalı iş süreçleri ile değişmesine karşı gösterecekleri direnç, e-imzanın kurumlar tarafından kullanımına geçilmesinde ve yaygınlaşmasında en önemli engel olarak görülmektedir. Bu direncin mümkün olduğunca hızlı bir şekilde ortadan kaldırılması sağlanmalıdır. Bu nedenle, e-imza teknolojisinin devlete ve çalışma verimine getireceği yararlar, kurum çalışanlarının anlayabileceği örneklerle anlatılmalıdır.
- E-imza uygulamaları ilk seferde mutlaka kapsam ve amacı açısından sınırlı örnek uygulamalar biçiminde tasarlanmalıdır.

Sonuç olarak, yasal geçerlilik kazanmış olmasına rağmen ülkemizde henüz yeterince yaygınlaşamayan e-imza konusuna yönelik olarak ülke genelinde bir bilinç ve bilgi birikimi oluşturulmalı ve planlı bir şekilde tüm kurum ve kuruluşların bir an önce e-imza projelerini hayata geçirmeleri sağlanmalıdır. Ancak bu çalışmalar yapılırken e-imzanın bir araç olduğu asla akıldan çıkarılmamalıdır. Belirli bir uygulamayla ilişkilendirilmediği sürece, bir e-imza projesinden söz etmek anlamlı değildir. Kurumsal ağlarda e-imza uygulamalarının hayata geçirilmesinde karşılaşılabilecek en önemli problem mevcut iş akışı ve uygulamalara e-imzanın nasıl entegre edileceğidir. Bu problem, ihtiyaçların ve e-imzadan beklenen faydanın doğru belirlenmesi ve kuruma uygun yaygınlaştırma modelinin doğru seçilmesi ile çözülebilir. Kurulum va yaygınlaştırmanın başlangıçta küçük kapsamlı

uygulamalarla başlayarak adım adım yapılması da bu problemin çözümüne yönelik en başarılı yöntemdir.

Gazi Üniversitesi'nde gerçekleştirilen simülasyon çalışmasında da, kurum genelinde e-imzanın yaygınlaştırılması aşamasında benzer problemlerin yaşanabileceği görülmüştür. Ancak üniversitede e-imza sistemlerini kullanacak olan hedef kitlenin akademik personel olması, personelin genel olarak e-imza konusunda bilgi sahibi olmaları, kurumun mevcut bilgi sistem altyapısı ve uygulamalarının e-imza entegrasyonu için yeterli ve uygun olması nedeniyle yaygınlaştırma aşamasında karşılaşılabilecek olası problemlerin çok hızlı bir şekilde aşılarak e-imzanın kısa sürede kurum içinde yaygınlaşabileceği görülmüştür.

Bu tez çalışması ile, e-imza konusunda ülkemizde oluşması gereken bilinç ve bilgi birikimine katkı sağlanmış ve simule edilen örnek bir uygulama ile kurumsal ağların e-imza sistemlerine geçişinde dikkat edilmesi gereken hususlar ve izlenmesi gereken yöntemler tüm detayları ile sunulmuştur. Kurumsal bir bakış açısı ile, kurumsal bir ağda AAA ve e-imza uygulamalarının hayata geçirilmesinde karşılaşılabilecek birçok probleme yönelik çözüm önerilerinin de sunulduğu bu çalışma, kurumsal ağlarda e-imza sistemlerinin hayata geçirilmesinde örnek olma özelliği taşıması nedeniyle bu alandaki diğer çalışmalardan farklılık göstermektedir.

KAYNAKLAR

1. Diffie, W., Helman, M., "New Directions in Cryptography", ***IEEE Trans. Inform. Theory***, IT-22 (6): 644-654, (Nov. 1976).

2. Rivest, R. L., Shamir, A., Adleman, L., "A Method for Obtaining Digital Signatures and Public Key Cryptosystem", ***Commun. ACM***, 21 (2): 120-127, (Feb. 1977).

3. Sağıroğlu, Ş., Alkan, M., "Her Yönüyle Elektronik İmza (E-İmza)", ***Grafiker Yayınları***, Ankara, 21-25, 32-63, 90-97, 106-108, 183-200, (2005).

4. "Nitelikli Sertifikasyon Altyapısı ve Yetkilendirme, E-imza 1. Çalışma Grubu Raporu", ***TBD Kamu-BİB Kamu Bilişim Platformu VII***, Antalya, 5-20, 25-30, 34-43, (26-29 Mayıs 2005).

5. "E-İmza'nın Toplumsal Boyutu, E-imza 2. Çalışma Grubu Raporu", ***TBD Kamu-BİB Kamu Bilişim Platformu VII***, Antalya, 7-15, 23-30, (26-29 Mayıs 2005).

6. "Açık Anahtar Altyapısı ve Elektronik İmza Uygulamaları Eğitim Kitapçığı", ***TÜBİTAK-UEKAE,*** 7-40, 46-49, 51-53, 57-62, 69-73, 75-81, (2004).

7. Sağıroğlu, Ş., Say, M., Alkan, M., "Bilgisayar Sistemlerinde Güvenlik", ***Telekom Dünyası***, 48-57, (Ekim 2004).

8. "Kamuda Bilgi ve Belge Değişimi, E-imza 3. Çalışma Grubu Raporu", ***TBD Kamu-BİB Kamu Bilişim Platformu VII,*** Antalya, 15-18,(26-29 Mayıs 2005).

9. Canbek, G., Sağıroğlu, Ş., "Şifre Bilimi Tarihine Genel Bakış I-II-III", ***Telekom Dünyası***, 34-42, 36-44, 26-32, (Mayıs-Haziran-Temmuz 2005).

10. Schneier, B., "Applied Cryptography, Protocols, Algorithms, and Source Code in C", 2nd ed., ***John Wiley & Sons Inc.,*** Canada, 213-233, 265-300, 435-445, 466-474, 597-618, (1996).

11. Pfleeger, C. P., "Security in Computing", Second Edition, ***Prentice-Hall Inc.***, USA, 82-122, (2000).

12. Aydın, H., "Bilgi Güvenliği ve Özcük Fonksiyonları Uygulamaları", Yüksek Lisans Tezi, ***Hava Harp Okulu Komutanlığı Havacılık ve Uzay Teknolojileri Enstitüsü***, İstanbul, 39-44, (2003).

13. Bosselaers, A., "The Hash Function RIPEMD-160", ***internet:http://www.esat.kuleuven.ac.be/~bosselae/ripemd160.html***, (25 Ağustos 2004).

14. Sağıroğlu, Ş., Tunçkanat, M., Altuner, M., "Kriptolojide Yeni bir Yaklaşım Resimli Mesaj", ***Telekomünikasyon Ekseni Dergisi, Telekomünikasyon Kurumu***, 2:22-24, (Haziran 2002).

15. Sağıroğlu, Ş., Tunçkanat, M., "Gizli Bilgilerin İnternet Ortamında Güvenli Olarak Aktarımı İçin Yeni Bir Yaklaşım", ***Popüler Bilim Dergisi***, Yıl.9, 105:21-24, (Eylül 2002).

16. Sağıroğlu, Ş., Tunçkanat, M., "Gizli Bilgilerin Elektronik Ortamda Güvenli Aktarımı", ***TBD 19. Bilişim Kurultayı, Beylikdüzü, İstanbul,*** 47-50, (3-6 Eylül 2002).

17. Simmons, G., "Contemporary Cryptology: The Science of Information Integrity", ***Institute of Electrical & Electronics Enginee***, USA, 177-209, (1991).

18. Hunt, R., "Technological infrastructure for PKI and digital certification", ***Computer Communications***, 1460-1471, (2001).

19. Tüfekçi, T., "Elektronik İmza İçin Neredeyiz?", ***EMO Ankara Şubesi, İletişim Teknolojileri Çalıştayı,*** Ankara, 5-10, (13 Kasım 2003).

20. "Elektronik İmza Ulusal Koordinasyon Kurulu Hukuk Çalışma Grubu İlerleme ve Sonuç Raporu", ***E-İmza Ulusal Koordinasyon Kurulu***, İstanbul, 18-27, 30-44, (Temmuz 2004).

21. "Elektronik İmza Ulusal Koordinasyon Kurulu Altyapı Çalışma Grubu İlerleme Raporu", ***E-İmza Ulusal Koordinasyon Kurulu***, 4-15, (2004).

22. Akcayol, M. A., "Türkiye'de E-Dönüşüm Çalışmaları, Karşılaşılan Sorunlar ve Çözüm Önerileri", ***Türkiye Bilişim Derneği 21. Ulusal Bilişim Kurultayı***, ODTÜ Kültür Kongre Merkezi, Ankara, 274-290, (04-06 Ekim, 2004).

23. Raina, K., "PKI Security Solutions for the Enterprise: Solving HIPAA, E-Paper Act, and Other Compliance Issues", ***Wiley,*** 30-33, (2003).

24. Lloyd, S. ve diğerleri, "CA-CA Interoperability", ***PKIforum white paper (http://www.pkiforum.org/ pdfs/ca-ca_interop.pdf),*** (2001).

25. Brands, S., "Rethinking Public Key Infrastructures and Digital Certificates-Building in Privacy", ***The MIT Press***, Cambridge, 3, 208, 253, (2000).

26. Tüfekçi, T., "Elektronik İmza Niçin Yaygınlaşamıyor?", ***Türkiye Bilişim Haftası***, İstanbul, 9-12, (1-7 Eylül 2003).

27. Isaac, D. S. and Isaac, M. J., "The SSCP® Prep Guide Mastering the Seven Key Areas of System Security", ***Wiley Publishing Inc.,*** Indiana, USA, 248-

250, (2003).

28. "E-Türkiye, E-Ekonomi Çalışma Grubu E-Ekonomi Taslak Raporu", ***2 nci Türkiye Bilişim Şurası***, 52, (09 Şubat 2004).

29. "PKI Uygulamalarındaki Gelişmeler ve Dünyadan Örnekler", ***Siemens Business Services Sistem Hizmetleri A.Ş. Stratejik Planlama ve Pazarlama Grubu***, 3-14, (19.05.2004).

30. Ellison, C., Schneier, B., "Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure", ***Computer Security Journal***, XVI(1):1-7, (2000).

31. Entrust, "The Concept of Trust in Network Security", ***Entrust Security Digital Identities & Information***, Canada, 3-5, (2000).

32. "2 nci Türkiye Bilişim Şurası Hukuk Çalışma Grubu Sonuç Raporu", ***2 nci Bilişim Şurası***, İstanbul, 4-12, (2004).

33. Tekman, E., "E-İmza ve Kamu SM", ***Orta Doğu Teknik Üniversitesi Uygulamalı Matematik Enstitüsü Açık Anahtar Altyapısı Araştırma Grubu Web Sayfası (http://www.pki.iam.metu.edu.tr)***, ***TÜBİTAK-UEKAE***, 3-12, 15, (25.12.2004).

34. Gutmann, P., "Cryptographic Security Architecture: Design and Verification", ***Springer-Verlag,*** 14-40, 71-77, 109-117, 290-303, (2003).

35. Menezes, A., Oorschot, P. V., Vanstone, S., "Handbook of Applied Cryptography", ***CRC Pres LLC,*** Florida, USA, 487-490, 543-590, (1996).

36. "E-Dönüşüm Türkiye Projesi Birlikte Çalışabilirlik Esasları Rehberi Sürüm 1.0", ***T.C. Başbakanlık, Devlet Planlama Teşkilatı Müsteşarlığı, Bilgi Toplumu Dairesi***, 25-26, (Temmuz 2005).

37. Çelikyılmaz, S., "Türkiye'de Kurumlar İçin E-Güven Altyapısı", ***İstanbul BT Vizyon Toplantıları***, İstanbul, 4-6, 10, (23-24 Kasım 2004).

38. Lostar, M., "E-İmza Projeleri: Fırsatlar, Önlemler, İpuçları", ***Microsoft Zirvesi İlkbahar 2005,*** İstanbul, 3-10, (25 Nisan 2005).

39. Akcayol, M. A., Şimşek, M., Bay, İ., "Türkiye'de E-Kütüphane Çalışmalarının Durum Analizi ve Öneriler", ***Akademik Bilişim 2005, Gaziantep Üniversitesi,*** Gaziantep, 2-3, (02-04 Şubat, 2005).

40. Boyacı, H., "Kamu Kurumları İçin Uygulanabilir E-İmza Modelleri Sunumu", ***Özelleştirme İdaresi Başkanlığı***, 4-13, (Aralık 2005)

41. Canavan, J. E., "Fundamentals of Network Security", ***Artech House Inc.,*** Norwood, USA, 55-71, (2001).

42. Rhee, M. Y., "Internet Security, Cryptographic Principles, Algorithms and Protocols", ***John Wiley & Sons Inc.,*** England, 57-111, 123-138, 149-150, 161-172, 184-187, 201-243, (2003).

43. Housley, R., Polk, T., "Planning for PKI: Best Practices Guide for Deploying Public Key Infrastructure", ***John Wiley & Sons Inc.,*** USA, 5-12, 18-27, 43-123, 137-163, (2001).

44. Gomez, F., Martinez, G., Canovas, O., "New Security Services Based On PKI", ***Future, Generation Computer Systems 19 (2003)***, 251-262, (2003).

45. "E-Devlet Proje ve Uygulamaları", ***Devlet Planlama Teşkilatı Müsteşarlığı Bilgi Toplumu Dairesi***, 33, 37-38, 41, 47-50, 59-60, 66-67, 140-142, (Eylül 2005).

46. "E-İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ", ***Telekomünikasyon Kurumu***, 2-4, (Ocak 2005).

47. İnternet: Kamu SM Web Sitesi, http://www.kamusm.gov.tr, (2006).

48. "5070 nolu Türkiye Elektronik İmza Kanunu", ***25355 sayılı Resmi Gazete,*** Ankara, (23 Ocak 2004).

49. Kilicli, T., "Üniversiterde Akıllı Kart Destekli PKI Uygulaması ve E-Kimlik", ***Türkiye'de İnternet Konferansları-VII***, İstanbul, 3-5, (2001).

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı : EROL, Hüseyin

Uyruğu : T.C.

Doğum tarihi ve yeri : 16.09.1979 Almanya

Medeni hali : Evli

Telefon :

Faks :

e-mail : erolhuseyin@hotmail.com

Eğitim

Derece	**Eğitim Birimi**	**Mezuniyet tarihi**
Lisans	İstanbul Üniversitesi/ Bilgisayar Mühendisliği Bölümü	2001
Lise	Giresun Lisesi	1997

İş Deneyimi

Yıl	**Yer**	**Görev**

Yabancı Dil

İngilizce

Hobiler

Bilgisayar teknolojileri, Tenis, Yüzme