T.C.
MALTEPE ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

TEZ ADI

Elektronik Posta İle Haberleşmede Güvenlik Protokolleri

Öğrenci Adı Soyadı
Cenk ULUCAN

Tez Danışmanı
Prof. Dr. İlhami YAVUZ

İSTANBUL – 2007

T.C.
MALTEPE ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

TEZ ADI

Elektronik Posta İle Haberleşmede Güvenlik Protokolleri

YÜKSEK LİSANS TEZİ

Öğrenci Adı

Cenk ULUCAN

Tez Danışmanı
Prof. Dr. İlhami YAVUZ

İSTANBUL – 2007

Bu tez çalışması, Maltepe Üniversitesi Fen Bilimleri Enstitüsü Yönetim Kurulu'nun ..... / ..... / ..... tarih ve ..... / ..... sayılı kararıyla oluşturulan jüri tarafından ***Bilgisayar Mühendisliği Yüksek Lisansı Tezi*** olarak kabul edilmiştir.

JÜRİ

Prof. Dr. İlhami YAVUZ
Danışman

Prof. Dr.
Üye

Prof. Dr.
Üye

ÖZET

Yüksek Lisans Tezi, Elektronik posta ile haberleşmede, güvenlik protokollerinin incelenmesi ve bir sertifika alanında elektronik posta haberleşme ortamının güvenli hale nasıl getirildiğinin incelenmesi, T.C. Maltepe Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı.

Kullanıcının yalnızca varlığının bile bir kimlik delili olarak hizmet ettiği bilgisayar ağları, artık kapalı sistemler olmaktan çıkmıştır. Bu bilgi bağlantıları çağında, bir kuruluşun ağ sistemi intranet'ler den, Internet sitelerinden ve extranet'ler den oluşabilir. Bunların tümü, bir kuruluşun dijital bilgi varlıklarını kötü amaçla görüntülemek veya değiştirmek isteyen yetkisiz kişilerin erişimine açıktır.

Ağlardaki bilgilere yetkisiz erişim için pek çok olasılık vardır. Bir kişi, e-posta, elektronik ticari işlemler ve dosya transferleri gibi bilgi akışlarını izleme veya bunları değiştirme girişiminde bulunabilir. Sistem yöneticisi bilgilere erişen bir kişinin kimliğinden nasıl emin olabilir ve bu kimlikle bu kişinin hangi bilgilere eriştiğini nasıl anlar? Ayrıca, sistem yöneticisi bir kuruluş içinde kimlik bilgilerini nasıl kolayca ve güvenli bir şekilde dağıtabilir ve yönetebilir? Bunlar, iyi planlanmış bir ortak anahtar altyapısı ile başarılabilecek konulardır.

Ortak anahtar altyapısı (PKI), dijital sertifikalar, sertifika yetkilileri (CA) ve diğer kayıt yetkililerinden (RA) oluşan bir sistemdir. Bu sistem ortak anahtar şifrelemesi kullanarak elektronik bir işleme katılan tüm tarafların geçerliliğini ve kimliğini doğrular.

Bu çalışmada, artık günümüzde hızla kullanım alanı genişleyen ve sayısal imza kanununun da çıkmasıyla resmiyet kazanan sayısal (elektronik) imza konusu ve Açık Anahtar Altyapısı Sistemleri incelenmiştir.

Tez Çalışması; bir açık anahtar altyapısı sistemi konfigürasyonunun belirlenmesi ve belirlenen sisteme uygun Sertifika Prensipleri ve Sertifika Uygulama Kurallarının hazırlanması ve bir mesajlaşma ortamının şifreleme algoritmaları ve sertifika sunucu ile nasıl güvenilir bir noktaya getirilebileceği üzerinde olacaktır

Bu tez 2007 yılında yapılmıştır ve 112 sayfadan oluşmaktadır.

Anahtar Kelimeler: Elektronik Posta, S/MIME, PGP, Açık Anahtar Altyapısı , Genel – Özel Anahtarlar , Aktif Dizin, Sertifika.

ABSTRACT

Master Thesis, Analyzing of protocols and infrastructure for secure electronic messaging and certification structures , T.C. Maltepe University, Graduate School of Natural and Applied Sciences, Department of Computer Engineering.

The closed computer systems are no longer valid in which the user is the core of identity.The company networks consists intranet's , internet web sites , and extranet's. All of these systems are open to any kind of attacks from unauthorized people in or outside the company.

There are many ways for unauthorized people to access the network resources.These people can attempt to trace the e-mail transactions, electronic transactions and file transfers on the network. How could a system admin locate these people or find out the identity of them , or which files have been accesed? How could a system admin manage the user rights effectively? These issues can be solved by a Public Key InfraStructure (PKI) .

The PKI system is a combination of digital certificates, certification authority(ca) and other authorities(ra). This system approves the identity and validity of the parties who wants to use the system by key algoritims.

In this thesis I discussed the PKI and the electronic signature systems which were widely used and has been legalized by the signature law which was issued lately.

This thesis will focus on, preparing the configuration and certificate principles according to PKI system needs and how to make the messaging algoritms and certificates more safe.

This thesis has been completed in 2007 and consists of 112 pages.

Keywords:. E-mail , S/MIME , PGP, Public Key InfraStructure , Public–Private Keys , Aktive Directory, Certificate.

TEŞEKKÜR

Bu tez konusunu seçmemde ve çalışmalarım esnasında değerli fikir ve katkılarıyla beni yönlendiren tez danışmanım Prof. Dr. İlhami YAVUZ'a teşekkür ederim.

KISALTMALAR

Kısaltma	**İngilizcesi**	**Türkçesi**
CA	Certification Authority	Sertifikasyon Makamı
PGP	Pretty Good Privacy	İyice Gizli
PKCS	Public Key Cryptography Standards	Açık Anahtar Kriptoloji Standartları
PKI	Public Key Infrastructure	Açık Anahtar Altyapısı
RSA	Rivest, Shamir and Adleman	Rivest, Shamir ve Adleman
SSH	Secure Shell	Güvenli Kabuk
SIL	Certificate Revocation List	Sertifika İptal Listesi
SI	Certification Principle	Sertifikasyon İlkesi
S/MIME	Secure/Multipurpose Internet Mail Extension	Güvenli Çok Amaçlı İnternet Posta Uzantısı

ŞEKİLLER

Sayfa

TABLOLAR

1. GİRİŞ

En önemli Internet servislerinden olan E-posta, bir tür iki taraflı elektronik veri iletişimi olarak nitelendirilebilir. Bu veri iletişiminin güvenlik gerekleri diğer Internet uygulamalarından farklı değildir. E-postada ön plana çıkan en önemli gereksinim iletilen bilginin kişiselliğidir. Nasıl normal bir postanın alıcısına, başka hiç bir kimsenin postanın içeriğini görmeden ulaşmasını istiyorsak, E-postanın da alıcısına aynı şekilde ulaşmasını istemek en doğal hakkımızdır. E-posta kullanıcısının bir başka gereksinimi ise iletilen bilginin alıcısına değişmeden ulaşmasıdır. Normal postada iletinin zarfa konulması ile çözülen bu iki sorun, E-posta uygulamalarında şifreleme yöntemleriyle çözülmektedir. Normal postada bir iletinin göndericisi, kendi kimliğini iletiyi imzalayarak ispatlayabilir. Böylelikle, alıcı hem gönderenin kimliğinden emin olur, hem de bir anlaşmazlık durumunda gönderenin söz konusu iletiyi gönderdiğini üçüncü bir şahsa ispatlayabilir. E-posta uygulamasında ise bu gereksinim sayısal imzalar ile sağlanmaktadır. Bu tez çalışmasında önce E-posta güvenliği için kriptoloji temelleri, en yaygın kullanılan algoritmalar, açık anahtar altyapısı ve sertifika yönetimi tanıtılacak ve son olarak Microsoft Windows 2003 sertifika denetleyicisi ve Microsoft Exchange mesaj uygulaması kullanarak güvenli bir mesajlaşma ortamının nasıl oluşturulması gerektiği anlatılacaktır. [3]

Gönderilen mesajın içeriğine ve iletişim uçlarının isteğine bağlı olmakla beraber, E-posta uygulamalarında kimlik kanıtlama, bilgi gizliliği, bilgi bütünlüğü ve inkar edememe sorunlarının hepsinin varlığından bahsedilebilir. Kimlik kanıtlama, gönderenin ve alıcının E-posta adreslerinin gerçekten de bahsi geçen kişilere ait olup olmadığı ile ilgilidir ve iki taraf da birbirlerinin gerçek kimliklerinden emin olmak isteyebilir. İnkar edememe ise alıcının gönderenin kimliğini gerektiğinde üçüncü bir kişiye E-posta mesajını göstererek ispatlayabilmesidir. Bu sorunu çözen bir sistemde kimse başkasının adını kullanarak E-posta gönderemeyecektir. Bilgi gizliliği, gönderilen E-posta mesajının sadece alıcı tarafından okunabilmesinin sağlanması sorunudur. Bilgi bütünlüğü ise E-posta mesajının değişmeden alıcısına ulaşması ile ilgilidir.

İnkar edememe ve dolayısıyla başkasının adını kullanarak E-posta mesajı gönderememe özelliği, ancak açık anahtar tabanlı şifreleme algoritmaları kullanan sayısal imzalar (digital signatures) destekli sistemler ile mümkündür. Açık anahtar tabanlı şifreleme algoritmalarında şifreleme anahtarı (açık anahtar) ve şifre çözme anahtarı (gizli anahtar) farklıdır ve şifreleme anahtarı herkese açıktır. Ancak, şifreleme anahtarından şifreyi çözme anahtarını elde etmek pratik olarak imkansız dır. Bundan başka, bu iki anahtar birbirlerinin tersi işlemler yaparlar. Birinin kodladığını diğeri çözer. Bu özelliği sayesinde açık anahtar tabanlı sistemler hem mesaj gizleme, hem de sayısal imzalama yapabilmektedir. Bir mesaj, alıcının açık anahtarı (public key) ile kodlandığında, ancak alıcının gizli anahtarı (private key) ile açılabileceğinden ve bu anahtara sadece alıcı sahip olduğundan, esas mesajı sadece alıcı okuyabilecektir. O yüzden, bu kodlama bilgiyi gizleyen bir şifreleme işlemidir. Böylelikle, bilgi gizleme ve bilgi bütünlüğü sorunları çözümlenebilir. Öte yandan, bir mesajın gönderenin gizli anahtarı ile kodlandığını düşünelim. Söz konusu gizli anahtarı sadece gönderen bildiğinden, bu kodlama işlemi o mesaja gönderenin attığı bir sayısal imza olarak değerlendirilebilir. İmzanın kontrolü ise kodlanmış mesajın gönderenin açık anahtarı ile açılmasından başka bir şey değildir. Açık anahtar da herkes tarafından bilindiğinden, herkes sayısal imza kontrolü yapabilmektedir. Böylelikle, inkar edememe, başkasının yerine mesaj gönderememe ve gönderenin alıcıya kimliğini kanıtlaması sorunları çözülebilmektedir.[18]

Geriye kalan tek sorun alıcının gönderene kimliğini kanıtlaması sorunudur. Başka bir deyişle, gönderenin mesajı, alıcıya ait olduğuna emin olduğu bir açık anahtarla şifrelemesi gerekir. Aksi halde alıcı şifreyi çözemeyecektir ve doğru olmayan açık anahtarın gizli anahtarını bilen fakat gerçekte istenilen alıcı olmayan biri gizli mesajı okuyabilecektir. Benzer bir durum sayısal imza doğrulanmasında da yaşanabilir. Eğer alıcı yanlış bir açık anahtar biliyorsa, sayısal imzayı doğrulayamayacaktır. O yüzden, hem alıcının hem de gönderenin kullandıkları açık anahtarların doğruluğundan emin olmaları gerekir. Bunun için de en iyi yöntem açık anahtarları sahibinden doğrudan almaktır. Bunun mümkün olmadığı durumlarda sertifika (certification) mekanizmaları kullanılabilir. Sertifika, bir açık anahtar, açık

anahtarın sahibinin kimliği ve E-posta adresinden oluşan bir veriye herhangi birinin koyduğu sayısal imzadır. Eğer bir başkası sertifikayı imzalayan insana güveniyorsa, sertifikanın içindeki açık anahtara ve açık anahtarın sahibinin kimliğine de güvenecektir.

2. KRİPTOLOJİ

Yunanca Kryptos Logos (Gizli kelime) tanımlamasından gelen Kriptoloji, toplumda bir haberleşmenin gizli tutulabilmesi üzerinde çalışan bilim olarak düşünülse de aslında anlamı daha geniştir, çözülebilmesi çok zor matematik problemleri ve mekanizmaları inceleyen Kriptografiyi ve bu problemleri ve mekanizmaları çözmeyi hedefleyen ve saldırıları belirleyen Kriptoanalizi içerir. Kabaca, belgelerin veya bilgilerin şifrelenmesi ve şifrelerinin çözülmesi için kullanılan yöntemlere verilen genel addır. Bir başka ifade ile, üçüncü şahıslar tarafından algılanamayacak veya öğrenilemeyecek farklı bir formata veriyi işleyerek dönüştürme işlemidir. Bu işlemler veri kaybı olmadan gerçekleştirilir. Matematiksel temele dayanan bu bilimde, matematiksel fonksiyonlar şifreleme (encryption), ve şifre çözme (decryption) kullanılır. [1]

Şifreleme (Encryption), Veriyi bir anahtarla şifrelemeye verilen addır. Hedef, veriyi, gerekli anahtar olmadan çözülebilmesi imkansıza mümkün olduğunca yakın şekilde kodlamaktır. Bu işlem matematiksel bir fonksiyon ve bir anahtar veya anahtar çiftinin biri kullanılarak yapılmaktadır. Şifre Çözme ise (Decryption) şifrelenmiş veriyi çözüp eski haline getirme işlemidir. Şifrelenmiş mesajı, şifrelemede kullanılan fonksiyonun tersini ve bir anahtar veya bir anahtar çiftinin diğerini kullanarak açık metne dönüştürme işlemidir. Kriptolojide en çok kullanılan kelimelerden olan anahtar (key) ise bir metni şifrelemekte veya açmakta kullanılan veri parçasına (sayı, kelime veya herhangi bir sayısal veri parçası) verilen isimdir. Kriptoanaliz ise; kriptografik sistem mekanizmalarını ve yaklaşımlarını inceleme ve çözme bilimidir. Şifrelenmiş verileri çözmek ve onları anlamlı hale getirme yaklaşımlarını içerirler. Kriptoloji içindeki önemi büyüktür. Ortaya konan bir şifreleme sistemini inceleyerek, zayıf ve kuvvetli yönlerini ortaya çıkarabileceği gibi, şifrelerin çözülmesi içinde kullanılabilir. Şifreleme anahtarı olmadan, açık metni şifrelenmiş metinden elde etme işlemi olarak bilinir ve bu işlem çoğunlukla şifreleme anahtarına sahip olmadan yapılır. Kriptoanaliz yöntemleri, kaba kuvvet ve diferansiyel kriptoanaliz olmak üzere ikiye ayrılır. Kaba kuvvet, bir şifreleme algoritması tarafından kullanılan bir anahtarı veya anahtar çiftini, tüm anahtarları tek

tek veya belirli bir mantık çerçevesinde deneyerek, kullanılmış olan şifreleme anahtarını bulma yaklaşımı iken, diferansiyel kriptoanaliz; bilinen açık şifreli mesaj çiftleri arasındaki farkların hesaplanması temeline dayanır. [1]

Kriptoloji başlangıcı itibariyle daha çok askeri uygulamalarda kullanılmıştır. Günümüzde ise İnternet uygulamalarının hız kazanması kriptografinin Web güvenliği alanında uygulanabilirliğini kanıtlamıştır. Özellikle elektronik ticaret, online banka işlemleri gibi birçok dinamik uygulamada bilginin saklanması şarttır. Kriptografi bu anlamda en uygun teknikleri önermektedir.

Verinin şifrelenmesi nasıl yapılmaktadır? Orijinal verinizin şifrelenmesi için bir algoritmaya, bir de anahtara ihtiyaç duyulmaktadır. Algoritma aslında hangi şifreleme yöntemini kullandığınızı gösterir. Kriptografi algoritmaları kabaca iki grupta toplanabilir: Kısıtlı algoritmalar, anahtar tabanlı algoritmalar. Kısıtlı algoritmaların güvenilirliği algoritmanın kendisi saklı kaldığı müddetçe geçerlidir. Anahtar tabanlı algoritmalarda ise tam tersine algoritmanın yapısı saklı değildir. Herkes tarafından bilinebilir. Saklı olan şifreleme için kullanılan anahtarın kendisidir. Algoritma açıkça bilinse de anahtar gizli olduğu için algoritma çıktısı (şifrelenmiş veri) gizli olmuş olmaktadır. Kısıtlı algoritmalar büyük işletmeler için uygun bir şifreleme yöntemi değildir. Kullanılan algoritmayı bilen birinin işten ayrılması veya kazara algoritmanın açığa çıkması durumunda sistemin yeni bir algoritmaya göre yeniden güvenliğinin sağlanması gereklidir. Bu da işletmenin büyüklüğüyle orantılı olarak artan, başlı başına hacimli bir iştir. Bu nedenle işletmeler güvenliğin sağlanmasında anahtar tabanlı algoritmaları tercih etmektedirler. [9]

2.1. Güvenlik Gereklilikleri

Kablolu veya kablosuz haberleşme ortamlarında bilgi ve haberleşme güvenliliğinin sağlanması için farklı şekillerde güvenlik yaklaşımları ve metodolojileri kullanılarak, farklı seviyelerde bir güvenlik ortamı oluşturulmalıdır. Tam güvenli bir ortam oluşturmada;

- Gizlilik (secrecy),
- Bütünlük (integrity),

- Kimlik tanımlama ve doğrulama (identification ve authentication),
- İnkar edemezlik (non-repudiation),
- Süreklilik (availability),
- Belgelendirme (certification)

gibi hususlar önemli rol oynamaktadır. Güvenli bir haberleşmenin ve iletişimin elektronik ortamda sağlanabilmesi için bu hususların gerçekleştirilmesi gerekmektedir. Tam bir güvenliğin gerçekleştirilmesi için, bu hususların bir altyapı üzerinde gerçekleştirilmesi gerekir. Bu altyapıya Açık Anahtar Altyapısı (AAA) denilmektedir. Tam bir güvenlik için elektronik imzanın AAA ile desteklenmesi gerekmektedir. [10]

E-imza ve AAA yapıları güvenlik unsurları bakımından Tablo 2.1.'de karşılaştırılmıştır.

Unsurlar	**E-imza**	**Açık Anahtar Altyapısı**
Gizlilik	Sağlamaz	Sağlar
Bütünlük	Kısmen sağlar	Sağlar
Kimlik doğrulama	Sağlar	Sağlar
İnkar edilemezlik	Sağlamaz	Sağlar
Belgelendirme	Sağlamaz	Sağlar
Süreklilik	Sağlamaz	Sağlar
Tam bir güvenlik	Sağlamaz	Sağlar

Tablo 2.1. Güvenlik unsurları bakımından E-imza ve AAA nın karşılaştırılması. [10]

2.1.1. Gizlilik

Güvenliğin en temel adımı olan gizlilik, şifre bilimi ile sağlanır. Şifre bilimi, elektronik haberleşmede bilginin üçüncü şahısların eline geçse bile, anlaşılamayacak veya çözümlenemeyecek bir forma dönüştürülmesi işlemidir. Gönderilen veya alınan mesajlar bir şifreleme algoritması kullanılarak farklı bir formata dönüştürülür. Bu sayede, üçüncü şahıslar farklı formata dönüştürülmüş olan gizlenmiş mesajları

çözemeyecekleri için güvenli ortam oluşturulmuş olur. Genel olarak gizlilik, şifreleme algoritmaları veya yaklaşımları kullanılarak yapılmaktadır.

2.1.2. Bütünlük

Bütünlük, bir dökümanın veya mesajın içeriğinin değiştirilmemesinin sağlanması veya temini olarak tanımlanır. Güvenli bir haberleşme için bütünlük vazgeçilmez unsurlardan birisi olmakla birlikte mutlak suretle tam olarak tanımlanması gereklidir. Bunun için özetleme algoritmaları kullanılır. Bir mesajın bütünlüğünü sağlamak için gönderilen mesajların özetleri alınır. Özetler mesaj ile karşı tarafa gönderilir. Karşı taraf ise alınan mesajın özetini çıkartır ve yine karşı taraftan alınan özetle bunu karşılaştırır. Karşılaştırmada bir eşitlik sağlanırsa, bu mesajın içeriğinin değiştirilmediği anlamına gelmektedir. Eşitlik sağlanamamış ise mesajın değiştirildiği ortaya çıkar.

2.1.3. Kimlik tanımlama ve doğrulama

Kimlik tanımlama, bir sisteme kişinin kimliğinin tanıtılmasından sonra sistem tarafından, kişinin kimliğinin tespit edilmesi işlemidir. Bu işlemin elektronik ortamda yapılabilmesi için kişi kimliğinin sisteme tanıtılabilmesini sağlayacak sayısal bir kimliğe ihtiyaç vardır. Bu sayısal kimlik, bir AAA içerisinde, belirlenmiş bir güvenilir makam veya otoriteden alınmalıdır. Bu makama sertifika makamı (certification authority) kısaca SM denilmektedir. Bu işlemler, SM ye bağlı olarak çalışan bir kayıt makamında (KM) yapılır. KM, SM ye bağlı olarak çalışan bir alt birimdir. KM'den alınan sayısal kimlik veya sertifika ile, elektronik ortamda hizmetlerin güvenli olarak yürütülmesi için ilk işlem gerçekleştirilmiş olur. Elektronik ortamda güvenilir SM 'lerin oluşturulması ve bu SM lerin birbirlerini tanımalarıyla hizmetlerin güvenli olarak verilmesi için bir altyapı oluşturulmuştur.

Kimlik doğrulama ise, bir kişinin kimliğinin doğrulanması işlemidir. Bu işlemin elektronik ortamda Kişi A ile Kişi B arasında yapılabilmesi için elektronik ortamda haberleşen tarafların kimliklerinin, bir AAA içerisinde belirlenmiş olan makamlar (SM) tarafından onaylanmış olması gerekmektedir. Buradaki Kişi A'nın

mesajını Kişi B'ye göndermesi ve Kişi B 'nin bu mesajı Kişi A'dan aldığını teyit etmesi işlemine kimlik doğrulama denir. Kimlik doğrulama ihlalini ortadan kaldırmak ve gerekli tedbirleri almak için, özetleme algoritmaları, mesaj özetleri, elektronik imzalar ve sertifikalar kullanılmaktadır.

2.1.4. İnkar edemezlik

Yüksek seviyeli bir güvenlik ortamı oluşturmak için bu işlemlerin elektronik ortamda yapılması ve inkar edilemezliğin sağlanması gereklidir. Kişi A'dan Kişi B'ye gönderilen bir mesajın Kişi B'ye ulaşmaması veya ulaştırılamaması, Kişi A'dan gönderilen bir mesajı Kişi B alsa bile bunu inkar etmesi veya Kişi B'nin mesajı Kişi A'dan alsa bile Kişi A'nın gönderdiğini inkar etmesi mümkündür. Bu tip durumlar ile karşılaşılmaması için, karşılıklı haberleşmede tarafların birbirlerinden gelen mesajları aldığını veya gönderdiğini teyit etmesi ve bunu inkar edememesi gereklidir. Bunu sağlama için, mesajı gönderen ve alan kişilerin kayıtları güvenilir bir makam tarafından tutulur. Bir AAA içerisinde kimin kiminle ne zaman bir haberleşme yaptığı tespit edilmektedir.

2.1.5. Süreklilik

İşlemlerin sürekliliği işlem akışının bozulmaması için son derece önemlidir. Hizmet veren kurumlar haberleşme sürekliliğini sağlamak zorundadırlar. Bunun için alternatif haberleşme yöntemleri yedekleme sistemleri geliştirilmelidir.

2.1.6. Belgelendirme

Sertifika makamları, kullanıcıların, doğru kişilerle irtibatlandırılmasını garanti eden çözümler içerirler. Belgelendirme teknolojileri, büyük oranda kimlik tanımlama ve doğrulama işlemlerini gerçekleştirmek veya zaman damgası bilgilerini tutmak ve gerektiğinde sunmak için geliştirilmiştir.

2.2. Şifrelemede Kullanılan Teknikler

Genel olarak bakıldığında şifreleme yaklaşımları kapalı anahtarlı ve açık anahtarlı olmak üzere ikiye ayrılmaktadır. Kapalı anahtarlı yaklaşımlara simetrik yaklaşımlar denilmektedir. Simetrik yaklaşımlarda hm şifre çözümleme hem de şifreleme de tek bir anahtar kullanılmaktadır. En çok kullanılan simetrik anahtar yaklaşımı veri şifreleme standartı DES (Data Encryption Standart) 'dir. Açık anahtarlı yaklaşımlar ise, asimetrik yaklaşımlar olarak bilinirler. Kullanıcı bir çift anahtara yani hem açık hem de gizli bir anahtara sahiptir. Bu anahtarlar özel (private) veya gizli, ve genel (public) veya açık olarak isimlendirilir. Açık anahtar herkese açık iken, özel anahtar ise sadece kişiye özeldir. Şifreleme açık anahtar ile yapılırken, şifre çözme özel anahtar ile yapılmaktadır. Bunun tersi de olasıdır. Açık anahtarlı şifre yaklaşımlarında en popüler olanı, RSA (Rivest, Shamir Adleman) 'dir. Açık ve kapalı anahtarlar arasında gizli bir bağ vardır. [10]

Simetrik ve asimetrik yaklaşımlar, güvenlik unsurları açısından değerlendirildiğinde ortaya çıkan hususlar Tablo 2.2' de belirtilmiştir.

Unsurlar	**Simetrik Yaklaşımlar**	**Asimetrik Yaklaşımlar**
Gizlilik	Sağlar	Sağlar
Bütünlük	Sağlar	Sağlar
Kimlik doğrulama	-	Sağlar
İnkar edememezlik	-	Sağlar
Hesaplama hızı	Yüksek	Düşük
Güvenlik	Anahtar uzunluğuna bağlı	Anahtar uzunluğuna bağlı
Genel değerlendirme	Mesaj şifreleme de kullanılması iyi sonuç vermektedir.	Anahtar şifreleme de kullanılması iyi sonuç vermektedir.

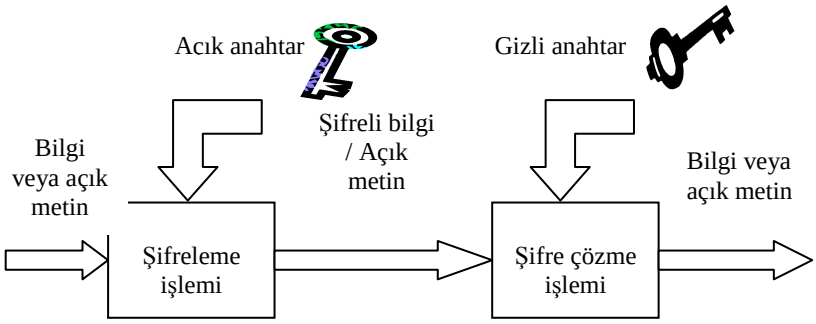
Tablo 2.2. Şifreleme Yaklaşımlarının Karşılaştırılması [10]

2.2.1. Asimetrik algoritmalar

Asimetrik algoritmalar, açık anahtarlı algoritmalar olarak bilinmektedir. Bu algoritmalarda şifreleme ve şifre çözme için farklı anahtar çiftleri kullanılmaktadır. Bu anahtarlar çift olarak üretilirler, tek yönlü çalışırlar, birbirlerini tamamlarlar. Bu anahtar çiftinde, şifreleme anahtarı açık anahtar (public key), şifre çözme anahtarı ise özel anahtar (private key) olarak adlandırılır.

Açık anahtar şifreleme işleminde, açık anahtar ile şifrelenen mesajlar, yalnızca gizli (özel) anahtar kullanılarak deşifre edilir. Gizli anahtar yalnızca ait olduğu kişide bulunurken, açık anahtar çeşitli şekillerde iletilebilmektedirler. Bu algoritmalara açık anahtarlı algoritmalar denmesinin sebebi, açık anahtarın herkese açık olması yani genel kullanıma açık olmasıdır. Algoritmanın bir kısıtlayıcı yönü fazla CPU işlemi gerektirmesidir. CPU yoğun başka işlerin tamamlanması gerektiği zamanlarda ciddi performans problemlerine sebebiyet verebilir. Asimetrik anahtar algoritmaları daha çok verinin paylaşılması veya verinin network üzerinde dolaşması gereken ortamlarda veriyi şifreleme amacıyla kullanılmaktadır.

Farklı bir kişi bir bilgiyi şifrelemek için birinin genel anahtarını kullanır ise, sadece o ilgili birinin özel anahtarına sahip bir kişi, bu bilginin şifresini çözebilir. Bilgiler genel anahtar ile şifrelenip özel anahtar ile çözülebilirler. Ayrıca özel anahtar ile şifrelenip, genel anahtar ile de çözülebilirler. RSA, açık anahtarlı bir şifreleme tekniğidir. Şekil 2.1. ‘te açık anahtarlı şifreleme ve şifre çözme işlemleri gösterilmiştir.

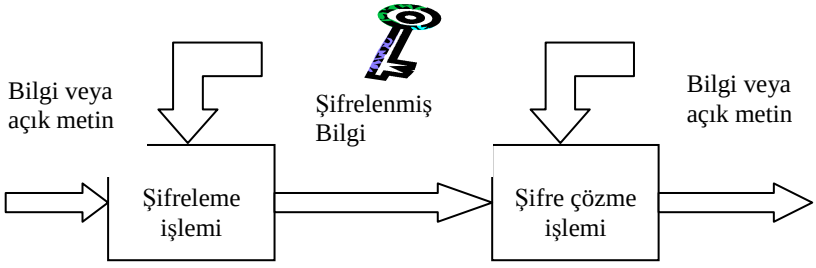


Şekil 2.1. Açık Anahtarlı Şifreleme ve Şifre Çözme İşlemleri [10]

Diğer açık anahtarlı şifreleme tekniği, Sayısal İmza Algoritması (Digital Signature Algorithm- DSA)'dır. Bu teknik imzalama için kullanılır. Eliptik Eğri Şifreleme sistemi ise eliptik eğriler üzerine oturtulmuş, şifreleme de kullanılan yaklaşımlardır. Diffie-Hellman Anahtar Anlaşması Protokolü (Diffie-Hellman Key Aggrement Protocol), güvensiz bir kanalda gizli anahtar oluşturmada kullanılan diğer popüler açık anahtar şifreleme teknikleridir.

2.2.2. Simetrik algoritmalar

Bu tür şifrelemede şifreleme ve şifre çözme için aynı anahtar kullanılır. Anahtarın saklı tutulmasından ötürü bu tür algoritmalara "gizli anahtar" algoritmaları da denilmektedir. Bu algoritmaların avantajı basit ve kolay uygulanabilir oluşudur. Aynı zamanda bunlar hızlı ve verimlidir. Ancak bu algoritmaların en zayıf tarafı şifreleme ve şifre çözme için aynı anahtarın kullanılıyor olmasıdır. Tek bir anahtarın güvenliği nasıl sağlanabilir? Diğer şahıslara bu anahtar güvenli olarak nasıl gönderilebilir? Kendi içinde tekrar eden bir durum, ilaveten diğer şahısların anahtarı gizli tutacağından nasıl emin olabilirsiniz? Dolayısıyla bu algoritmalar daha çok paylaşımın olmadığı durumlarda uygundur. Bilgisayarınızdaki dosyaların veya sabit diskinizin şifrelenmesi gerektiğinde rahatlıkla kullanılabilir. Güvenli bir iletişim için gönderici ve alıcı, bir gizli anahtar üzerinde uzlaşırlar. Seçilen gizli anahtar ile, mesajlar veya açık metinler şifrelenir veya şifrelenmiş mesajların, açık metinlerin şifreleri çözülebilir. Birbiri ile şifreli haberleşmek isteyen taraflar, seçilen gizli anahtarı paylaşmak zorundadırlar. Şekil 2.2.'te tek anahtarlı (gizli) şifreleme ve şifre çözme işlemleri gösterilmiştir.



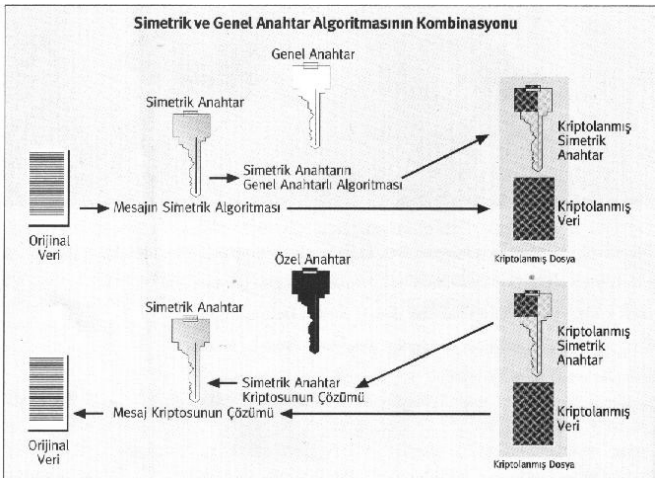
Şekil 2.2. Tek Anahtarlı (Gizli) Şifreleme ve Şifre Çözme İşlemleri.[10]

Anahtarın genel kullanıma sunulması, isteyen herkesin şifrelenmiş mesajları çözebileceği anlamına geldiği için, bu yaklaşımda anahtarlar gizli tutulmak zorundadır. Modern bilgisayarlar ile kullanılan anahtarın bulunması mümkün olduğundan, simetrik algoritmalarda güvenlik anahtar uzunluğuyla doğru orantılıdır. DES ve 3DES en çok kullanılan yaklaşımlardandır.

2.2.3. Karışık (hybrid) algoritmalar

Simetrik algoritmaların hızlı olması ve asimetrik algoritmaların güvenilir fakat yavaş olması Hibrid Kriptosistem isimli bir yapının ortaya çıkmasına sebep olmuştur. Simetrik algoritmalarda en büyük problem anahtarın karşı tarafa iletimidir. Bu yapı temelde bilginin simetrik bir algoritma ile şifrelenmesini ve bu algoritmada kullanılan anahtarında asimetrik bir algoritma ile şifrelenip gönderilecek bilgi ile birlikte iletilmesinde temel teşkil eder. Bu sayede bilginin şifrelenmesi, simetrik algoritmadan dolayı hızlı olup, anahtarın iletimi de, asimetrik algoritmadan dolayı güvenli olacaktır. Karışık algoritmalar her iki yöntemin artı yönlerinden yararlanmayı hedeflemektedir. Orijinal veri simetrik anahtar kullanılarak şifrelenir. Daha sonra simetrik anahtarın kendisi alıcının açık anahtarı kullanılarak şifrelenir ve mesajın sonuna eklenir. Şifre çözme işlemi sırasında alıcının gizli anahtarı kullanılarak öncelikle simetrik anahtar elde edilir. Ardından simetrik anahtarla mesajın kendisi çözülür.

Şekil 2.3.' te Simetrik ve Genel Anahtar Algoritmasının Kombinasyonu gösterilmektedir.



Şekil 2.3. Simetrik ve Genel Anahtar Algoritmasının Kombinasyonu.[22]

2.3. Anahtarlar

Anahtarlar kriptografik yaklaşımların temel taşlarıdır ve güvenlik, anahtarın güvenliğine veya bit sayılarının uzunluğuna bağlıdır. Anahtarları temel alarak, algoritmalar değerlendirildiğinde, simetrik yaklaşımlarda tek bir anahtar üretimi yapılırken, asimetrik algoritmalarda, anahtarlar bir çift olarak üretilirler. Anahtarlar bit olarak ifade edildikleri gibi farklı bir formda da ifade edilebilirler. 48 bitlik anahtar veya Base48 gibi.

Simetrik bir algoritma için anahtarın alıcıya iletilmesi, gizli bir yoldan yapılmalıdır. İkiden fazla kişi ile güvenli haberleşileceği zaman anahtar yönetimi gereklidir. Her bir bilgisayar bir başka bilgisayarla, diğer bilgisayarlardan bağımsız bir iletim hattı oluşturmaktadır. N elemanlı bir hatta N'in 2'li kombinasyonu kadar iletim hattı oluşacaktır. Bu kadar büyük bir çapta iletim ağı oluşturmak imkansızdır. Her bir eleman diğer elemanların anahtarlarını depolamak zorundadır.

Simetrik algoritma anahtarlarının iletiminde, TTP (trusted third party), kullanılan yöntemlerden biridir. Bu yöntemde güvenilirliği kabul edilen üçüncü bir ara yapı kullanılır. Gönderici bir alıcıya bilgi göndermek istediği zaman, bu ara yapıdan anahtar talebinde bulunur. TTP adı verilen bu yapı ise, göndericiye anahtar temin eder. Göndericinin bildirdiği alıcıya da aynı anahtarı gönderir. Yani ağa bağlı kullanıcılar anahtar teminini TTP den elde ederler. Bu yapının avantaj ve dezavantajları bulunmaktadır. Herhangi bir eleman ağdan atıldığında veya ağa bir eleman eklendiğinde bu yapının bundan etkilenmemesi, her bir elemanın yalnızca TTP 'nin gönderdiği anahtarı depolamak zorunda olması, bilinen avantajları iken , her bir bilgi iletiminde öncelikle TTP ile iletişim kurulmak zorunda olması, TTP 'de n adet anahtar depolama zorunluluğu, TTP'nin tüm mesajları okuması ve TTP'nin anahtar iletiminde güvenliği sağlayamaması bilinen dezavantajlarıdır.

Asimetrik algoritma anahtarlarının anahtar iletiminde kullanılan yöntemlerinden birisi Genel Anahtar Tekniği' dir. Bu yapıda iki anahtar bulunduğu için, genel anahtarlar her kullanıcının erişebileceği bir ortamda tutulur. Kişi A, Kişi B'ye bir bilgi göndereceği zaman, önce merkezden Kişi B'nin genel anahtarını temin eder. Daha sonra göndermek istediği bilgiyi bu anahtarla şifreleyip Kişi B'ye gönderir. Bu yapıda üçüncü bir ara yapıya gerek yoktur. Böylelikle iletilecek bilginin

üçüncü kişi tarafından okunma riski ortadan kalkmış ve çok sayıda anahtar depolama sıkıntısı giderilmiştir.

Kriptografik yaklaşımların temel taşları olan anahtarlar, açık anahtar alt yapısının da temel taşlarıdır. Tablo 2.3. 'te desteklenen unsurlar ve ihtiyaç duyulan anahtarlar verilmiştir. Açık anahtar altyapısı güvenlik unsurlarının tamamını destekledikleri için tam bir güvenlik sağlayabilirler.

Anahtar uzunluğu güvenliğe oldukça etki eder. Tablo 2.4. 'te görüleceği üzere bit sayısı (anahtar uzunluğu) arttıkça anahtarların kırılma sürelerinde artış olmaktadır. Bu süre artar ise anahtar o kadar güvenlidir.

Desteklenen Unsurlar /Kişiler	Gizlilik	Bütünlük	Kimlik tanımlama ve doğrulama	İnkar Edemezlik
Herkes	Açık Anahtar			
Kişiye özel	Özel anahtar	Özel anahtar	Özel anahtar	Özel anahtar

Tablo 2.3. AAA Yapılandırmasında Özel ve Genel Anahtarlar. [10]

Anahtar Uzunluğu	Sayı Değeri	10^2 şifre/s	10^9 şifre/s	10^{12} şifre/s
32 bit	~$4x10^9$	36 dk	2.16 s	2.16 ms
40 bit	~10^{12}	6 gün	9 dk	1 s
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

Tablo 2.4. Farklı Anahtar Uzunluklarına Göre Şifre Kırma Zamanları. [10]

Anahtar elektronik ortamda en çok akıllı çubuk (smart token) veya akıllı kart (smart kart) lar da tutulurlar.

2.4. Şifreleme Algoritmaları

Algoritmalar, şifreleme ve şifre çözmek için kullanılan matematiksel işlemlerdir. Güvenlikleri seçilen anahtarın uzunluğuna ve çalışma biçimlerine bağlıdır. Kullanılan matematiksel yaklaşım gizleniyor ise buna "sınırlandırılmış algoritma yaklaşımı" denilir. Bu algoritmalar, kullanıcı sayısının artması, gruptan bir kullanıcının ayrılması veya gizlenen bir algoritmanın yanlışlık ile ortaya çıkması durumunda, geri kalan herkesin başka bir algoritma kullanmasını gerektirdiği için tercih edilmezler. Bu algoritmalar geneli kapsamadığı, maliyetinin yüksek olması, üçüncü şahıslar tarafından öğrenebilme olasılığının yüksek olması sebebi ile tercih edilmezler. Genellikle, az sayıda kullanıcısı olan ve alt seviye güvenlik gerektiren uygulamalarda kullanılırlar.

Bir algoritmanın güvenilirliği teorik yapısının herkes tarafından biliniyor olmasından yani algoritmanın herkese açık olmasından geçmektedir. Modern şifreleme ve anahtarlama teknikleri, stenografik yaklaşımlar en çok kullanılan yaklaşımlardır. Algoritmalarda şifreleme işlemleri, matematik fonksiyonlar yardımı aracılığı ile yapılır. Bu tür fonksiyonlarda, X tanım kümesinden Y aktarım veya dönüşüm kümesine bir f fonksiyonu tanımlanmıştır. X kümesinin her bir elemanına f fonksiyonu uygulandığında, Y kümesi çıkışları elde edilir. Tek yön fonksiyonu olarak ta bilinen bu yaklaşımda, çıkışlardan hareket ederek girişler elde edilemezler. Yani Y kümesinden X kümesine bir f^{-1} fonksiyonu elde edilemez. Bunun nedeni, her Y kümesi elemanıyla bir X kümesi elemanı eşleştirilememektedir.

Algoritmalarda, eşleşme (bijeksiyon) fonksiyonu, diğer bir yaklaşım olup, X tanım kümesinden Y aktarım kümesine bir f fonksiyonu olarak tanımlanır. Tek yön fonksiyonun aksine, bu fonksiyonun çıkışlarından girişler elde edilebilmektedir. Bunun nedeni ise, X kümesinin her bir elemanına f fonksiyonu uygulandığında, Y kümesinin tüm elemanları çıkış olarak elde edilmesidir. Sonuç olarak, Y kümesinden X kümesine f^{-1} fonksiyonu elde edilebilir.

Şifreleme algoritmaları, simetrik ve asimetrik fonksiyonlar olarak ikiye ayrılır. Temel de her iki fonksiyonunda yaptıkları aynıdır. Girdi olarak alınan veriler, parametrelere ile işlenir ve çıktı olarak, şifrelenmiş veri elde edilir. Bu veri güvenli ve gizli olarak alıcısına gönderilmeye hazırdır. İletim esnasında herhangi bir

saldırganın bu verilerden bilgi edinebilmesi fonksiyonun içeriğine bağlı olarak zordur. Fonksiyon, sabit ve parametresiz ise, güvenilirlik esneklik azdır. Üçüncü şahıslardan veriyi gizlemek ve saklamak sabit bir yöntem ile pek mümkün değildir. Genellikle parametrik bir fonksiyon tercih edilir. Bu fonksiyonların güvenilirlik derecesini parametre ve bunlara karşılık gelen çıktı kombinasyonları belirler.

2.4.1. Şifreleme algoritmalarında aranan özellikler

- Şifrelenmiş mesajın deşifre edilmesi esnasında bilgi kaybı olmaması
- İhtiyaç duyulan güvenlik seviyesine göre şifreleme işleminin zorluk seviyesinin seçilebilmesi
- Önemli olmayan verilerin düşük seviyeli şifreleme yaklaşımları ile, önemli verilerin ise yüksek seviyeli şifreleme yaklaşımları ile şifrelenebilmeleri
- Verimi düşürecek, maliyeti ve işgücü kaybını artıracak yaklaşımlar içermemesi
- Şifreleme işlemlerinde güvenlik seviyesinin mümkün olduğunca yüksek olması
- Basitlik ve kolaylıkla gerçekleştirilebilme özelliğinin ön planda tutulması
- Kullanılan algoritmaların karıştırıcı özelliği olması
- Şifrelenmiş mesaj ile açık metin arasındaki ilişkilerin zor kurulabilmesi
- Şifreleme yaklaşımlarının herkese açık olması
- Açıklarının ortaya çıkarılabilmesi için, başkaları tarafından test edilebilmelerinin sağlanması.

Sezar, MD2, MD5, RSA, blowFish, AES, CAST 128, DES, 3 DES, IDE, el-Gamal , Elliptic Curve, Diffie-Hellman, PGS, S/MIME, IpSec, Kerberos, SHA-1, SHA-2 güvenli bir iletişimde kullanılabilen şifreleme algoritmaları yaklaşımları , protokolleri ve fonksiyonlardan bazılarıdır. Bu fonksiyonlardan bazıları aşağıda açıklanmıştır.

2.4.2. Sezar şifreleme yaklaşımı

Verilerin bir ortamdan diğerine aktarılmasında kullanılan bir yöntemdir. Simetrik aynı zamanda eşleşme özelliği gösteren bir şifreleme metodudur. Şifreleme ve şifre çözme anahtarları aynıdır. Bu anahtarın alıcıya gizli yolla iletilmesi şarttır. Alıcıya anahtarın gönderilmesinde güvenilir bir yol bulunması gereklidir. Bu mümkün olsa bile alıcıya farklı bir anahtar temin etmek gerekebilir. Bu zahmetli ve oldukça zordur. Bir mesajın bu yaklaşımla şifrelenmesi için aşağıdaki matematiksel fonksiyon kullanılır.

$$E(M) = (M+3) \bmod 29 = C$$

Bu fonksiyondaki ‘M’ mesajı, ‘E’ şifreleme işlemini, ‘C’ şifrelenmiş mesajı ifade eder. ‘29’ ise, şifreleme yapılacak olan dildeki karakter sayısıdır. Türkçede 29 alfabetik karakter olduğu için 29 rakamı kullanılmıştır. Şifrelenmiş mesajın deşifre edilmesi;

$$D(C) = (C-3) \bmod 29 = M$$

formülü kullanılarak yapılır. Bu formülde ‘D’, deşifreleme işlemini ifade eder. Buradaki en önemli nokta, harflerin sayıya dönüştürülmesidir. Mesela İngiliz alfabesi için ,

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3																				23	24	25

harfler 0’dan 25’e kadar etiketlenir. Bunun sonucunda elde edilen sayılar formülde yerine konulur ve her bir harfin farklı bir sayıya dönüşmesi sağlanır. Mesela; “e imza” kelimesini ele alırsak ve Sezar’a göre şifreleyelim. İngiliz alfabesini kullandığımızı varsayar isek,

e i m z a

4 8 12 25 0

karakter karşılıkları bulunur. Buradaki elde edilen değerleri E (M)=(M+3) mod 26 şifreleme fonksiyonundan geçirdiğimizde,

7 11 15 3 sayılarını elde ederiz. Bu sayılara karşılık gelen harfler ise,
h l p c d şeklindedir.

2.4.3. Açık anahtar şifreleme yaklaşımı

Bu şifreleme yaklaşımı Sezar metodunun genişletilmiş bir versiyonudur. Kaydırma temelli bir yaklaşımdır. Şifreleme işlemi,

E (M) = (M+N) mod 29 = C ile yapılırken deşifreleme işlemi,

D (C) = (C-N) mod 29 = M formülü ile gerçekleştirilir. Burada $0 \leq N \leq 29$ olduğunu hatırlatmakta fayda vardır.

Örneğin, (x+1) mod 29 fonksiyonu ile "BİLİM" kelimesi şifrelenirse, çıktı olarak "CJOJK" kelimesi elde edilir. İletim işlemi yeni veriler ile gerçekleştirilir. Üçüncü bir şahsın bu veriyi algılaması bir derece daha zorlaşacaktır. Bu fonksiyonun ters işlemi ile mesaj (x-1) mod 29 ile deşifre edilir. Bu sayede şifrelenmiş mesaj kolaylıkla geril elde edilebilir.

2.4.4. Polialfabetik şifreleme (Vigenere Tablosu)

İlk olarak 1553 yılında Giovan Batista Belasa tanıtılmış 16. yüzyılın sonlarında Blaise De Vigenere bu yöntemi düzenleyip kullanmıştır ve bu yöntemin adı "Vigenere şifresi" olarak kalmıştır. Bu yöntemin en büyük özelliği çoklu alfabe kullanmasıdır. Tablo 2.5. 'te Vigenere tablosu gösterilmiştir.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Tablo 2.5. Vigenere Tablosu. [10]

Bu yaklaşım ile bir mesajın şifrelenebilmesi için, bir anahtar kelimeye ihtiyaç duyulur. Mesajın her bir karakteri sütun üzerinde, anahtar kelimenin her bir

harfi ise satırda bulunur. Satır ve sütunun kesiştiği noktadaki harf şifrelenmiş mesajın harfidir.

Tablodaki her satır Sezar(Caesar) Şifresine karşılık gelmektedir. İlk satırdaki dönme sıfırdır, ikincide 1 ve son satırda 25'tir. Örnek olarak , "EİMZA KULLANMALIYIZ" cümlesi şifrelenecek olsun. "HEMEN" kelimesini ise anahtar kelime olarak kullanalım. Bu harflere karşılık olarak, anahtar kelimenin yardımı ile Vigenere tablosundan yeni harfler elde edilir.

Açık Mesaj	EİMZA	KULLA	NMALI	YIZ
Anahtar Kelime	HEMEN	HEMEN	HEMEN	HEM
Şifreli Mesaj	LNBDN	ŞİAPN	ÜRMPV	GML

Elde edilen şifreli mesajın şifrelerinin çözümü için ise, aynı anahtar kullanılarak yine Vigenere Tablosu aracılığı ile açık metin elde edilir.

2.4.5. Vernam (One Time Pad) şifreleme yaklaşımı

Rasgele üretilen tek bir kullanımlık karakter dizisi ile şifreleme gerçekleştirilir. Açık mesaj içinde yer alan her karakter üretilen dizide karşısına gelen karakterlerle işleme sokularak şifreli mesaj elde edilir. Mesajı çözebilmek için rasgele dizinin bilinmesi gereklidir.

Açık Mesaj	EİMZA	KULLANMALIYIZ
Rastgele Dizi	HNMET	KSYROQAZWPGLU
Şifreli Mesaj	LYBDT	VJN.....

Bu yöntemde güvenlik rasgele üretilen diziye bağlı olduğundan bu şifreleme sistemi, mükemmel bir şifreleme yöntemi olarak bilinir. Önemli olan husus, rasgele dizinin gerçekten rasgele seçilmesi ve anahtar uzunluğu ile aynı olmasıdır.

2.4.6. DES (Data Encryption Standart) algoritması

1977 yılında IBM tarafından geliştirilmiştir. Bu algoritmanın anahtar uzunluğu 56 bittir. Mevcut teknolojiler ile kolaylıkla çözülebilmektedir. DES algoritmasındaki fonksiyonların simetrik olması da güvenliği önemli ölçüde tehdit etmektedir. Bu şifreleme de A verisi B anahtarıyla şifrelenir ve C verisine dönüştürülür. Şifrelenmiş C verisi alıcıya gönderilir ve C verisi, alıcı üzerinden göndericiye gönderilmiş B anahtarı ile sadece deşifre edilir. DES tek yönlü fonksiyon özelliği gösteren bir algoritmadır.

64 bit blok şifreleme de yapabilen bu algoritmada, şifreleme esnasında 16 farklı döngü kullanılır. Bu işlemler de veri, anahtar ve önceki döngü ile karıştırılır ve bir permütasyon işlemine tabi tutularak anlaşılamayacak bir forma getirilir. Bir önceki döngünün çıkışı bir sonraki döngüye giriş olur. Her bir döngüdeki en sağdaki girişin 32 biti, çıkışın solundaki 32 bite kaydırılır. Sonra, sağ ve sol bitler ve anahtar, bir fonksiyondan geçirilerek çalıştırılır. Her bir döngüde anahtar kaydırılır ve son bir permütasyon ile işlem tamamlanır.

DES algoritması,1997 yılında İsrail tarafından kırılmıştır. Ardından 3DES (Triple DES) geliştirilmiştir. 168 bit anahtar uzunluğundaki bu yaklaşım güvenli bir şifreleme yaklaşımı olarak bilinir. Bu algoritmaların hızlı ve lisansız olması önemli özellikleridir. Daha çok AAA ve bankacılıkta kullanılır. [10]

2.4.7. RSA (Rivest,Shamir ve Adleman) algoritması

İlk defa 1977 yılında Ron Rivest, Adi Shamir ve Len Adleman tarafından oluşturulan RSA algoritması geliştiricilerinin soy isimlerinin ilk harfleriyle anılmaktadır. Açık algoritma mantığı ile çalıştığı ve yüksek güvenlik sunduğu için en çok tercih edilen asimetrik algoritmadır. Bir genel anahtarlı şifreleme tekniği olan RSA, çok büyük tamsayıları oluşturma ve bu sayıları işleminin zorluğu üzerine düşünülmüştür.[21] Anahtar oluşturma işlemi için asal sayılar kullanılarak daha güvenli bir yapı oluşturulmuştur. Anahtar oluşturma algoritması şu şekildedir:

- P ve Q gibi çok büyük iki asal sayı seçilir.

- Bu iki asal sayının çarpımı N = PxQ ve bu bir eksiklerinin

  ?(N)=(P-1)x(Q-1) hesaplanır

- 1'den büyük ?(N)'den küçük ?(N) ile aralarında asal bir E tamsayısı seçilir.
- Seçilen E tamsayısının mod ?(N)'de tersi alınır, sonuç D gibi bir tamsayıdır.
- E ve N tamsayıları genel anahtarı, D ve N tamsayıları ise özel anahtarı oluşturur.

Genel ve özel anahtarları oluşturduktan sonra gönderilmek istenen bilgi genel anahtar ile şifrelenir. Şifreleme işlemi şu şekilde yapılmaktadır: Şifrelenecek bilginin sayısal karşılığının E' ninci kuvveti alınır ve bunun mod N deki karşılığı şifrelenmiş metni oluşturmaktadır. Genel anahtar ile şifrelenmiş bir metin ancak özel anahtar ile açılabilir. Bu yüzden şifrelenmiş metin, yine aynı yolla, şifrelenmiş metnin sayısal karşılığının D'ninci kuvveti alınır ve bunun mod N deki karşılığı orijinal metni oluşturur.

Basit bir örnek ile algoritmayı tekrar anlatalım. Örneğin basitliği açısından daha küçük asal sayılarla çalışacağız. Öncelikle genel ve özel anahtarlarımızı oluşturalım.

- P=7 ve Q=17 gibi iki asal sayı seçelim.
- Bu iki asal sayının çarpımı N=PxQ; N=119 ve bu iki asal sayının bir eksiklerinin çarpımı ?(N) = (P - 1)x(Q-1); ?(N) =96 olarak hesaplanır.
- 1'den büyük 96'dan küçük 96 ile aralarında asal bir E=5 tamsayısı seçelim.
- Seçilen E=5 tamsayısının mod 96'da tersi alınır, sonuç D=77 gibi bir tamsayıdır.
- 5 ve 119 tamsayıları genel anahtarı, 77 ve 119 tamsayıları ise özel anahtarı oluşturur.

Bu algoritmada iki asal sayının çarpımını kullanarak anahtar oluşturulmasının sebebi, iki asal sayının çarpımını asal çarpanlarına ayırmak asal olmayan sayıları ayırmaktan daha zorlu olmasıdır. Şimdi oluşturduğumuz {5, 119} ve {77, 119} anahtarlarımızı kullanarak şifreleme yapalım. Örnek olarak, 19 sayısını genel anahtarımızla{5, 119} şifreleyelim. 19 sayısının 5'inci kuvvetinin mod 119 daki karşılığı olan 66, 19 sayısının RSA şifrelenmiş halidir. Özel anahtarımızı {77, 119} kullanarak 66'nın 77'nci kuvvetinin mod 119 daki karşılığı tahmin de edebileceğiniz gibi 19 dur.

İki tamsayının aralarında asal olup olmadığının testi için matematikten de bildiğimiz Öklit algoritması kullanılır. Çok büyük asal sayı oluşturmak oldukça zor bir iştir. RSA ile günümüzde 1024 bitlik bir anahtar (yaklaşık 300 basamaklı bir sayı) basit uygulamalar için yeterli bir şifreleme tekniği olarak kullanılabilir.

RSA algoritması, bir şifreleme algoritması için oldukça basit bir algoritmadır. Buna karşın sürekli çok büyük asal sayı oluşturmak oldukça zor bir işlemdir. Asal sayılarının bilinen bir formülü yoktur.

2.4.8. Steganografik yaklaşımlar

Steganografi önemli bir bilgi gizleme yöntemidir ve son yıllarda teknolojinin gelişmesiyle birlikte dijital nesneler üzerinde sıklıkla kullanılmaya başlanmıştır. Steganaliz ise bir örtü verisi içinde gizli veri olup olmadığını anlamaya yarayan saldırı yöntemleridir. Literatürde vektör çok şifreleme algoritması herkes tarafından bilinmektedir. Örneğin AES ve DES gibi simetrik şifreleme algoritmaları ile şifrelenmiş metinler ters yönde çalışan fonksiyonlarla birbirine bağlı ve paralel çalışan on binlerce bilgisayarla çözülebilmesi teknik olarak mümkündür. Günümüzde kullanılan bu şifreleme algoritmalarındaki temel hedef şifreli metni çözmeyi geciktirmek ve dolayısıyla kuantalama, k-n eşikleme yöntemi ve çeşitli dönüşümler kullanılarak (Ayrık Kosinüs Değişimi) gerçekleştirilen steganografik uygulamalar vardır. Steganografik işlemleri anlayabilmek için temel yöntem olan en az öneme sahip olan bit (LSB : Least Significant Bit) kavramının bilinmesi

gereklidir. Bir resmin piksellerinin son bitlerinin yer değiştirilmesi ile bu işlem gerçekleştirilir.

2.4.9. Kuantum şifreleme

Kuantum kriptografisi şifrelemede kullanılan anahtar değişim protokolü ile ön plandadır. Yani kuantum kriptografi tekniği mesajın iletilmesinden çok mesajın şifrelenmesinde ve şifrelenmiş mesajın çözülmesinde kullanılan anahtarın(tek kullanımlık-on time pad-) güvenilir bir biçimde alıcı ve verici arasında değişimi ile ilgilenir. Kuantum kriptografisi %100 güvenliği şimdilik sağlamaktadır. %100 güvenlikteki kasıt şudur: Alıcı ve verici arasına giren bir kişinin kendisini fark ettirmeden anahtarı tamamıyla elde etmesinin önüne geçilmesidir. Yani alıcı ve verici arasındaki anahtar değişim kuralını güvenli hale getirir. Kuantum kriptografi tekniği temel bir fizik kanunu olan Heisenberg'in belirsizlik ilkesine dayanmaktadır. Bu ilkeye göre kuantum mekaniğinin temel öğesi olan bir foton'un aynı anda iki özelliği bilinemez. Bu da iletişim kanalında ki bir fotonun klonlanmasını (kopyalanmasını) imkansız hale getirmektedir. Kısacası günümüz teknolojisinde fiber optik ağ üzerindeki bir fotonun yeni bir kopyası çıkarılamaz. İşte kuantum kripto tekniği fotonun bu özelliğinden faydalanarak güvenli bir anahtar iletimi sağlar.

Kuantum kriptografi tekniğinde veri iletimi klasik yollarla yapılmaz. Veri iletimi elektriksel işaretler yerine fotonlar ile yapılmaktadır. Dolayısıyla iletişim kanalı için fiber optik ağ gerekmektedir. Bu da kuantum kriptografi tekniğinin aslında sivil yaşamda kullanılamayacağını göstermektedir. Zaten bu teknik şu anda sadece askeri amaçlarla çok kısıtlı ölçülerde kullanılmaktadır. Ancak fiber kanallarının maliyeti ve bu ağların kurulum maliyeti düştükçe bu tekniğin sivil kullanımda görmek mümkün olacaktır. Fotonları alıcıdan vericiye göndermek için fiber optik ağ gereklidir. Aynı zamanda anahtarı alıcıya göndermek için foton tabancalarına(foton üreteci) ve kristal süzgeçlere ihtiyaç vardır. Anahtar iletişimi sırasında foton'un baz alınan bir sisteme göre herhangi bir açıyla polarize olma özelliğinden faydalanır. Fotonların dikeyde veya yatayda polarize olması için kristal süzgeç çiftleri kullanılır. Temel olarak birbirine dik olan iki süzgeç seçilir.

Rasgeleliği artırmak için birde bu süzgeçlerle 45 derecelik açı yapan ikinci bir süzgeç takımı kullanılır. Kuantum fiziğine göre 45 derecelik polarizasyonlu bir fotonun birbirine dik iki süzgeç takımından geçirildiğinde fotonun yeni polarizasyonunun yönü 45 derece olmayacaktır. Peki 0 derecemi yoksa 90 derecemi olacaktır. Bunun kesin bir cevabı yoktur. Ancak her iki polarizasyon yönü içinde olasılık eşittir. Yani 10000 tane 45 derecede polarize olmuş bir fotonu artarda dikey ve yatay konumda yerleştirilmiş kristal süzgeçlerinden geçirdiğimizde istatistiksel olarak 5000 tanesi dikey yönde 5000 tanesi de yatay yönde polarize olacaktır. Bu yönlerden birisi 0 diğer 1 seçilerek iletişim anlamlı hale getirilir. Şunu da unutmamak gerekir ki eğer bu açı 45 derece olsaydı oran bu sefer 1/2 olmayacaktı. Matematiksel ve fiziksel veriler bu oranın ilgili açının kosinüs karesine eşit olduğunu göstermektedir. (cos245 = 1/2) [10]

2.4.10. Özetleme (Hashing) algoritmaları

Farklı uzunluklardaki mesaj, döküman veya yazıyı işleyerek, sabit uzunluktaki veri oluşturma işlemine özetleme denir. Elde edilen özet bilginin, mesaj döküman veya yazıyı temsil edebilecek bir formda olması beklenir. Elde edilen özet verinin mümkün olduğunca benzerinin olmaması beklenir. Bu işlemde bir özetleme (hashing) fonksiyonu kullanılır. Bir grup veriden veya mesajdan sabit uzunlukta bir dizi üretilir. Üretilen bu dizi, o mesajın, dökümanın veya yazının bütünlüğünün test edilebilmesi için kullanılan bir imza niteliğindedir. Bu işlemleri gerçekleştiren algoritmalara özetleme (hashing) algoritmaları denir. Bir özetleme fonksiyonu,

- Özet değeri kolay hesaplayabilmelidir.
- Özet değerinden mesajı elde etmek zor olmalıdır.
- Uzunlukları farklı olan verileri, sabit uzunlukta bir çıktıya dönüştürmelidir.
- Farklı mesaj veya dökümanlardan aynı özet değerinin üretilmemesi gereklidir.
- Elde edilecek özet değeri tekil (unique) olmalıdır.

- Aynı özet değeri üretecek iki farklı mesajı bulmak oldukça zor olmalıdır.

Özetleme fonksiyonları pratikte, şifre doğrulama, bütünlük kontrolü, e-imza ve güvenlik e-posta uygulamalarında kullanılmaktadır. 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 en belirleyici özellikleridir. MD serisi, SHA serisi, RIPE-MD-160 algoritmaları bunlardan bazılarıdır.

2.4.11. MD serisi mesaj özetleme algoritmaları

Bu algoritma Ron Rivest tarafından geliştirilmiştir. 128 bit özetleme sağlar. Bu serideki MD2 en yavaş iken, MD4 en hızlı olanıdır. MD5, MD4 'e göre daha kapsamlıdır fakat hızı düşüktür. Bu algoritmaların tümü herkese açıktır. MD5'ın saldırılara karşı çok güçlü olmadığı Alman Bilgi Güvenliği servisince tespit edilmiştir. Bu algoritma yerine SHA-1 veya RIPEMD-160 tavsiye edilmektedir.

2.4.12. SHA-1 (güvenli özetleme algoritması - secure hashing algorithm)

NSA (Ulusal Güvenlik Ajansı – National Security Agency) tarafından geliştirilmiş ve NIST desteği ile ABD'de standart olarak kabul edilmiştir. Bu algoritmalar, MD serisi algoritmalardan daha uzun özet bit üretirler. İlk sürüm SHA-0 olarak bilinir. SHA-0 ve SHA-1, en fazla 2^{64} uzunlukta mesajlardan 160 bitlik özet değer üretir. NIST 2001 yılında SHA'nın 256, 384 ve 512 bit versiyonlarını duyurmuştur. Son günlerde SHA-2 kullanılmaya başlamıştır.

2.4.13. RIPE-MD-160 (RACE Integrity Primitives Evaluation Message Digest)

Farklı uzunluktaki dosya veya veriler için 160 bitlik sabit uzunlukta bir bit dizisi üretmesi ve diğer şifreleme yaklaşımlarından daha hızlı olması üstünlükleridir. Yalnızca bütünlüğü sağlaması ise dezavantajıdır. İki farklı ve paralel hesaplama işleminin sonucunun, her bir sıkıştırma işlemi sonunda birleştirilmesi, bu

fonksiyonun ayırt edici özelliğidir. 32 bit işlemcilerde en iyi performansı verecek şekilde ayarlanmıştır. RIPE-MD nin 258 ve 320 bitlik sürümleri vardır.

2.4.14. MAC (message authentication codes)

Bir MAC oluşturma veya doğrulama için yalnızca bir anahtara ihtiyaç duyulur. HMAC (RFC 2104) ve SHA-1 temelli NMAC örnekleridir. Anahtar özetlemeli mesaj doğrulama kodları (HMAC) , bir anahtara dayalı ve tek yönlü çalışan bir özetleme yöntemidir. Hem veri bütünlüğünün hem de veri kaynağının doğrulanmasını sağlar. Daha önceden bahsettiğimiz özetleme fonksiyonları ile aynı özellikleri taşırlar. Bu özetleme fonksiyonlarından birini kullanır fakat ilave olarak bir gizli anahtar kullanır. HMAC ler veri alışverişinde kullanılabilecekleri gibi dosyaların değiştirilip değiştirilmediğinin kontrol edilmesinde de kullanılır.

Bu algoritmalar güvenilirlik açısından karşılaştırıldığında en güvenilir olanı RIPEMD-160 ve ardından SHA-1’ dir.

3. GÜVENLİK PROTOKOLLERİ

Açık anahtar tabanlı şifreleme kullanılan protokoller arasında, PGP (Pretty Good privacy), SSL (Secure Socket Layer) ve çoğunlukla sertifika gerektirmeden kullanılabilse de SSH (Secure socket shell) yer almaktadır.

3.1. Pgp

PGP güvenli e-mail, dosya şifreleme protokolüdür (RFC 2440). Bir dizi şifreleme algoritmasını destekler IDEA, RSA, DSA, MD5, SHA-1. PGP sayesinde e-mail ve dosyalar üçüncü şahıslar tarafından gizlenebilir. İstemediğiniz kişiler dosyalarınızı e-maillerinizi ele geçirse bile, eğer PGP ile şifrelenmişse bu dosyaların içeriklerine ulaşamazlar. PGP' nin en önemli yanlarından biri çok ciddi derecede güvenli olmasıdır. Tüm kaynak kodu açıktır (sitesinden kaynak kodunu sipariş edebilirsiniz) ve ücretsiz bir versiyonu da mevcuttur. Kaynak kodunun açık olması, PGP' nin tüm dünyadaki güvenlik uzmanları tarafından incelenmeye açık olduğunu gösterir ki, bu ne derece güvenli olduğunu kanıtlamaktadır. Algoritması açık

olmayan bir şifre standartına güvenilmez. Örneğin ABD hükümeti kendi şifreleme standartlarını ortaya çıkarmaktadır, ancak bunlar hükümet odaklı şifreleme standartları olduklarından, genelde kodları yayınlanmaz. PGP' nin bildiğiniz gibi en yaygın kullanım alanı e-mail yazışmalarıdır.

PGP melez bir şifreleme kullanır. Geleneksel ve Asimetrik şifrelemenin bir karışımıdır.

PGP Çalışma Modeli;

1. E-mail' i alacak kişi (alıcı) gönderecek olana Genel Anahtarını gönderir.
2. E-mail' i gönderecek kişi, (gönderici) alıcının Genel Anahtarını "import" eder.
3. Gönderici yeni e-mailini alıcının genel anahtarı ile şifreler.
4. Alıcı gelen e-maili kendi özel anahtarı ile çözümler.

PGP' nin birçok ücretli ve ücretsiz versiyonları bulunmaktadır. Ücretli versiyonların birçoğu PGP Corporation tarafından geliştirilmektedir. PGP Corporation tarafından geliştirilen PGP ürünlerinin kaynak kodları tamamen açıktır ve sitesinden (www.PGP.com) sipariş edilebilir.

PGP' nin bunun yanında birçok da ücretsiz versiyonu vardır. Bu ücretsiz versiyonlar hakkında bilgi vermeden önce bunları kullanabilmek için Amerika ya da Kanada' da yaşayan bir Amerikan ya da Kanada vatandaşı olmak gerekiyor. Bunun sebebi, Amerika'nın güçlü şifreleme algoritmalarını yurtdışına çıkarma ile ilgili bir yasası. Ek olarak, bu ücretsiz versiyonlar kurumsal kullanımlara izin vermez. Eğer kurumsal kullanım istenirse PGP Corporation' dan satın alınması gereklidir. Kısaca yukarıdaki şartlara uyulmuyor ise bu programların lisans anlaşmaları ihlal edilmiş olunabilir.

3.2. Ssl/Tsl

SSL genel amaçlı kullanım için geliştirilmiş bir standarttır. Güvenli HTTP bağlantısı sağlaması ile popülerdir. SSL ve TSL protokolleri, TCP/IP protokollerine güvenlik katmak amacı ile geliştirilmiştir.

SSL ‘in SSL-1, SSL-2 ve SSL-3 olmak üzere farklı versiyonları vardır. En basit hali iletişim hattının şifrelenmesi durumudur. Bu protokol, bağlantı kuran iki uç arasındaki kimlik doğrulamayı, doğrulama işlemini şifrelemeden ayırmayı ve daha önceki bağlantının kaldığı yerden devam etmesini sağlamayı içeren daha karmaşık seçenekler sunmaktadır. SSL protokolü, birbirlerine gönderilen ya da gönderilmeyen bir dizi mesaj kümesinden oluşur.

SSL protokolü Netscape tarafından geliştirilmiş fakat internette yaygın kullanımından ötürü, IETF için kritik bir hale gelmiştir ve biraz daha geliştirilerek IETF tarafından TSL (Transport Security Layer – Ulaşım Güvenlik Katı) olarak değiştirilmiştir.

3.3. Ssh

Güvenli uzaktan erişim alanında çok önemli ve ücretsiz olan bir protokoldür. Daha çok FTP ve telnet gibi uzaktan erişim protokolleri yerine kullanılan ve sunucu ile istemci arasındaki iletişimi şifreleyen bir protokoldür. İstemci, sunucuya ilk bağlantı sırasında sunucunun gönderdiği açık anahtarı çevrim dışı yollar ile doğrulayıp listesine ekleyebilir. Böylelikle sertifika gerektirmeden, sunucunun açık anahtarı istemci tarafından öğrenilmiş olur. Bu işlem bir seferlik olup, SSH sisteminin kullanım amacı, sunucuda hesabı olan kısıtlı sayıdaki kullanıcıya hizmet vermektir.

3.4. S/mime

Bu protokol, güvenli elektronik posta ortamı oluşturmak için kullanılan bir standarttır. PKCS#7 yapısı üzerine kurulmuştur. RSA-DSA ve MIME standartlarını içerir. Bu protokolde mesaj içerikleri açıktır. Fakat tüm yapı şifrelenmiştir. Mesajın alındı teyidi, güvenlik etiketleri, posta listeleri, anahtar belirleme gibi işlemleri destekler. MD2, MD4, DES, 3DES , SHA-1, MD5, RSA, Diffie-Hellman gibi özetleme , imzalama, şifreleme, ve anahtar şifreleme algoritmaları bu yapı içinde kullanılır. [4]

3.5. Ipsec

Bu protokol iki bilgisayar arasındaki haberleşmeden, IP paketlerinin şifrelenmesi, online anahtar dağıtımı, sanal özel ağ haberleşmesi, internet tabanlı tüm haberleşmelerde güvenliği sağlamak veya güvenli bir ortam oluşturmak için kullanılır. IPSec işlemi, IP doğrulama başlığı ve IP zarflama modları olmak üzere iki türde gerçekleştirilebilir. Değiştirilmiş veriyi ve taklit edilen IP adreslerini anlama ve tüm paketlerin bütünlüğünün ve kimlik doğrulamasının yapılması, birinci türde gerçekleştirilmektedir. İzlemeyi önleme için, şifreleme ve paketteki verinin bütünlüğü ve kimlik doğrulama işlemi ise ikinci türde gerçekleştirilir.

4. ELEKTRONİK İMZA

Bilgi ve iletişim teknolojilerinin yaygınlaştırılması, sadece etkin ve verimli kullanımına değil, aynı zamanda teknolojilerde kullanılan cihaz, ekipman, ve sistemlerde, bilgi ve veri güvenliğinin de tam olarak sağlanmasına bağlıdır. Bunun tam olarak sağlanması içinde bu uygulamaların hukuken tanımlanması ve düzenlenmesi zorunludur. Bunun yanında, günlük hayatta yapmış olduğumuz iş ve işlemlerin, elektronik ortamlarda da yapılabilmesi için, hukukende geçerli olan bir teknik yaklaşımın kullanılması ve yaygınlaştırılması gerekir. Bu noktada e-imza karşımıza çıkar. E-imzanın dünyadaki ilk örneği EDI dir. (Elektronik Veri Değişimi) Katma Değerli Şebekeler, elektronik fon transferi, satış noktası ve bankamatik teknolojilerinin geliştirilmesinde önemli rol oynamıştır. Sayısal imza ve elektronik

imza terimlerini karıştırmamak gereklidir. Sayısal imza elektronik ortamda imzanın kullanılmasını ifade ederken, elektronik imza elle atılan ıslak imzanın yerini elektronik ortamda alan bütün teknolojileri kapsayan geniş bir alanı ifade etmektedir. Türkiye'de 2004 yılında "Elektronik Veri, Elektronik Sözleşme ve Elektronik İmza Yasası" uygulamaya alınmıştır. [10]

E-imza; gelişmiş teknolojiler kullanarak, elektronik ortamda gönderilen veya alınan bilgilerin, bunlara gönderen kişi veya kuruma ait olduğunun doğrulanmasını, iletilen veya alınan verilerin başkaları tarafından gönderilmediğini veya bildiğimiz kişiler tarafından gönderildiğinin belirlenmesini, verileri gönderenlerin gönderdiğini ve alanların aldığını inkar edememesini, gönderilen veya alınan bilgilerin içeriğinin değiştirilmemesini, başkaları tarafından elde edilse bile, içeriğin başkaları tarafından anlaşılmamasını garanti eden, elektronik ortamda bitlerden oluşturulan güvenli haberleşme ortamıdır. Diğer bir ifade ile e-imza, bir elektronik mesaj veya iletiye eklenen ve göndereni emsalsiz şekilde tanımlayan veya taklit edilmesi çok zor olan bir sayısal kod olarak tanımlanır. [2]

Bir e-imzada bulunması gerekli özellikler;

- Güvenilirlik,
- Taklit edilemezlik,
- Yeniden kullanamazlık,
- İnkar edilemezlik,
- İçerik değiştirilemezlik,
- Kolay kullanılabilirlik.

4.1. E-imza Uygulamaları

İnternet / intranet ortamında gönderilen mesajlar, iletiler veya dökümanlar çoğu zaman düz bir metin veya açık bir metin olarak adlandırılırlar. Metinlerin saklanılması, başka bir formata dönüştürülmesi işlemine şifreleme denilir. Şifreleme ile mesaj güvenli olarak iletilebilir fakat tam bir güvenlik için şifreleme yeterli değildir. İlave olarak kimlik doğrulama, belirlenen kişi olduğunu ispatlama,

bütünlük, ve aldığını veya gönderdiğini red etmeme gibi işlemlerin de, haberleşme sırasında sağlanması gereklidir.[15] Elektronik ortamda, mesajların güvenli olarak gönderilmesi ve alınması için farklı yaklaşımlar kullanılmaktadır. Bu yaklaşımlar, aşağıdaki senaryolarda açıklanmıştır. Bu senaryolar, bilgi güvenliği temel unsurları temel alınarak oluşturulmuştur ve farklı seviyelerde güvenlik sağlarlar. E-imza uygulamalarında, simetrik algoritmalarda yapılacak şifreleme işlemlerinin, asimetrik şifreleme algoritmalarından daha hızlı olduğunu hatırlatmakta fayda vardır. Bu tür uygulamalarda, mesajların şifrelenmesi için imzalama algoritmaları olarak simetrik algoritmalar ve anahtarların şifrelenmesi için de çoğunlukla asimetrik algoritmalar kullanılır. [14]

4.1.1. Uygulama 1 (gizlilik, asimetrik)

Bu uygulamada gizlilik işlemi, açık anahtar şifreleme ile gerçekleştirilir. Burada Kişi A veya Kişi B, kendisine ait bulunan bir çift gizli ve açık şifreleme anahtarlarına sahiptir. Burada amaç iletişim sırasında bilginin istenmeyen bir kişinin eline geçse bile mesajın deşifre edilmesini önleme ve haberleşmenin gizliliğinden emin olunmasını sağlamaktır. Bu işlem de temel güvenlik unsurlarından gizlilik sağlanmış olur. Bu işlemde,

- Kişi A, Kişi B'ye gönderecek olduğu mesajını, Kişi B 'nin açık anahtarı olan Ka 'yı kullanarak şifreler ve bunu Kişi B 'ye gönderir.
- Kişi B ise, mesajı aldığında kendisine ait olan ve sadece kendine özel olan gizli anahtar Kö ile mesajın şifresini çözer.

Burada mesajı şifreleyen kendisi bile deşifre edemez. Bu uygulama gizlilik işleminin gerçekleştirilmesinde en çok kullanılan yöntemdir. Bu uygulamada yalnızca anahtar bazlı düşünüldüğü içinde, yalnızca gizlilik işlemi gerçekleştirilir.

4.1.2. Uygulama 2 (kimlik doğrulama)

Bu uygulamada kimlik doğrulamaya yönelik bir işlem yapılmaktadır. Burada yapılan işlem bir öncekinin tam tersidir.

- Kişi A, Kişi B ‘ye bir mesaj göndermek istediğinde Kişi A mesajı kendi özel anahtarı Kö ile imzalar ve imzalı mesajı Kişi B ‘ye gönderir.
- Kişi B ise mesajı Kişi A’nın açık anahtarı olan Ka ile mesaj doğrulama ve onaylama işleminden geçirerek imzalı mesajı deşifre eder. Sonuç olarak açık mesaj elde edilmiş olur.
- Elde edilen açık mesaj yalnızca Kişi A’nın açık anahtarı ile açılabileceğinden, bu mesajın A’nın açık anahtarı ile açılması ile , A’dan geldiği doğrulanmış olur. Kimlik doğrulama işlemi gerçekleştirilmiş olur.

Bu yaklaşım şeklinin mesaj şifreleme de kullanılması uygun değildir. Kişi A’nın açık anahtarının birçok yerden elde edilebilir olması, Kişi A ‘nın özel anahtarı ile şifrelenmiş mesajın deşifre edilmesi işlemini mümkün kılar.

4.1.3. Uygulama 3 (gizlilik, simetrik)

Bu uygulamada şifreleme de tek bir anahtar kullanılmaktadır. Bu yöntem de,

- Kişi A, Kişi B’ye gönderecek olduğu mesajı Kişi B’nin de bildiği bir gizli anahtarı Kö kullanarak şifreler ve Kişi B’ye gönderir.
- Kişi B ise mesajı aldığında, Kişi A’nın ve kendisinin de bildiği gizli bir anahtar ile mesajın şifresini çözer.

Bu şifreleme yaklaşımında, yüksek derece de gizlilik sağlanmamış olsa bile, yüksek kapasiteli dökümanların şifrelenmesine asimetrik yaklaşımlara göre daha az işlem zamanına ihtiyaç duymasından dolayı daha çok tercih edilmektedir. Buradaki tehlike Kö’ yü bilen veya elde edebilen bir kişinin mesajı deşifre edebilecek olmasıdır.

4.1.4. Uygulama 4 (gizlilik, steganografik yaklaşım)

Bu yaklaşım bir nesnenin içerisine, bir verinin gizlenmesi olarak tarif edilebilir. Ses, sayısal resim, video görüntüleri üzerine veri saklanabilir. Bu veriler bir metin dosyası olabileceği gibi herhangi bir görüntü içerisine başka bir görüntüyü gizlemekte olasıdır. Bu yöntemde açık mesajı Kişi A, bir resim içerisine uygun bir yazılım kullanarak saklar ve açık mesajı içeren resmi Kişi B'ye gönderir. Kişi B ise Kişi A'dan aldığı resmin içinde bir mesaj olduğunu bilir ve buna uygun bir yazılım ile mesajı resim içinden elde eder. Bu yaklaşım diğer uygulamalara göre güvenilirliği düşüktür. Resim içine gizlenecek olan verinin, simetrik veya asimetrik bir yaklaşım ile şifrelenerek resim içine gömülmesi ile gizlilik seviyesi daha üst seviyelere çıkarılabilir.

4.1.5. Uygulama 5 (gizlilik, yapay zeka metotları)

Bu uygulama ile bilgi bir formdan başka bir forma dönüştürülür. Bu yöntemde açık mesaj, Kişi A tarafından bir yapay zeka metodu ile şifrelenir ve şifrelenmiş mesaj diğer tarafa gönderilir. Şifreli mesajı alan Kişi B ise, Kişi A dan aldığı mesajı ancak deşifre ettiği takdirde çözebilir. Yapay zeka parametreleri Kişi A dan Kişi B ye gönderilmedikçe, bu işlem gerçekleştirilmez. Bu işlem simetrik bir yaklaşım olarak değerlendirilir. Gönderici ve alıcının güvenliği açık anahtar şifrelemede olduğu gibi tam olarak sağlanamasa da farklı bir yaklaşım sunduğu için saldırganların işini zorlaştırmaktadır. Güvenlik seviyesi çok yüksek değildir.

4.1.6. Uygulama 6 (e-imza)

Sanal ortamda güvenliği artırmanın bir diğer adımı, haberleşme anında aktarılan bilgilerin, mesajların doğru kişilere ulaştırıldığından veya doğru kişilerden alındığından emin olunmasıdır. Bu işlem yalnızca e-imza kullanılarak gerçekleştirilebilir. E-imza ile bir mesajı imzalamak için asimetrik şifreleme kullanılır. Bu işlemde bir asimetrik şifreleme algoritmasına ve de mesajın imzalanması için bir imzalama algoritmasına ihtiyaç duyulmaktadır. İmzalama ve onaylama algoritmasına DSA örnek olarak verilebilir. Bu işlemlerin hızlı ve

problemsiz olarak yapılmasını sağlayacak bir yazılıma ihtiyaç vardır. Bu işlemi gerçekleştirmenin amacı mesajı gönderen kişinin kimlik bilgilerinin mesaja eklenerek, kimlik doğrulama işlemini yapmaktır.

- Mesajı göndermek isteyen Kişi A, mesajını oluşturduktan sonra bu mesajı kendi özel anahtarı Kö ile imzalama algoritmasının geçirerek, mesaj imzasını elde eder.
- Oluşan mesaj imzası, orjinal açık mesajın sonuna mesaj imzası olarak eklenir.
- Bu mesaj imzası açık mesaja eklenerek Kişi B'ye gönderilir.
- Kişi B mesajı aldığında, imzayı onaylamak için mesajın imzasını, Kişi A nın açık anahtarı Ka ile onaylama algoritmasını kullanarak çözer. Eğer imzalı mesaj, Kişi A nın açık anahtarı ile açılırsa , Kişi B i bu mesajın gerçekten Kişi A dan geldiğinden emin olur. Kişi A'nın açık anahtarı ile sadece, Kişi A'nın özel anahtarı ile imzalanmış mesajların çözülebileceğini unutmamak gerekir.
- Bu işlem sonunda mesaj imzasının Kişi A'dan gelip gelmediği kontrol edilir. Mesaj imzası açılıyor ise, bu mesajın Kişi A dan geldiği tespit edilmiş olur. Bu sağlanmaz ise mesajın Kişi A'dan gelmediği anlaşılır.
- İşlem sonunda eşitlik sağlanır ise, bu mesajın Kişi A'dan geldiğini Kişi B, Kişi A'nın mesajındaki eklentiyi açarak Kişi A hakkındaki detaylı bilgileri öğrenebilir.

Bu işlemde sadece kimlik doğrulama işlemi gerçekleştirilmektedir. İlave olarak bütünlük kontrolü de yapılmak istenirse mümkündür. İmzalama algoritmasına açık mesajında eklenmesi ile bu önemli güvenlik unsuru da gerçekleştirilmiş olur. açık mesaj ile imzalanmış ve açık mesaja eklenmiş olan bir dökümanda gönderilecek dökümanın boyutu iki katına çıkacaktır. Bu mesajın karşı tarafa gönderilmesi ile imzalanmış olan açık mesaj ile açık olarak gönderilen mesaj karşılaştırılır. Bu mesajı alan kişi karşılaştırmayı yaparak mesajın içeriğinin değiştirilip değiştirilmediğini anlar. Buradaki en önemli problem mesaj uzunluğunun iki katına çıkmasıdır. Mesaj boyutunun büyümesi doğal olarak mesajlaşma hızını da düşürmektedir. Bu problemi aşmak için de özetleme algoritmaları kullanılır. Özetleme ile sabit uzunlukta ve çok

küçük mesaj özeti çıkarılır. Bu mesaj özetini imzalayan kişinin özel anahtarı ile imzalama algoritmasından geçirilerek e-imza oluşturulur. Özetlenmiş dosyanın boyutu çok yüksek olmadığı için bütünlük doğrulamada bu yaklaşımın kullanılması uygundur.

4.1.7. Uygulama 7 (özetleme algoritmalı e-imza)

Bu uygulama da mesajın tamamı yerine, belirli uzunlukta oluşturulmuş sadece o mesaja ait olan mesaj özeti kullanılır. Bunun için bir özetleme fonksiyonu kullanılır. Bu algoritmaların çıktısı ise, sabit uzunlukta bir değer olup mesajın özeti olarak bilinir. Mesaj özeti diğer veriler ile birlikte gönderilir. Daha sonrada bu özetler karşılaştırılır. İçerikte bir değişiklik yok ise, mesajın değiştirilmeden Kişi B'ye ulaştırıldığı eğer varsa, mesajın değiştirildiği anlaşılarak gerekli önlemler alınır. Bu uygulama ile veri bütünlüğü de sağlanmış olmaktadır. Bu sayede hızlı bir haberleşme ortamı sağlanabilecektir. Bu, uygulama 6 da ifade edilen yapıya özetleme algoritmasının eklenmesinden ibarettir. Bu işlemlerin yapılabilmesi için takip edilmesi gereken adımlar şu şekilde gerçekleştirilmektedir.

- Mesajı göndermek isteyen Kişi A, kimlik doğrulamaya ilave olarak bütünlük unsurunu da ilave etmek isterse, açık mesajını bir özetleme algoritmasından geçirmek zorundadır. Eklenen özetleme algoritması ile mesajın özeti alınır.
- Özet mesaj oluşturulduktan sonra, bu mesaj Kişi A nın özel anahtarı Kö ile imzalama algoritmasından geçirilir ve Kişi A nın mesaj imzası alınır.
- Bu işlem sonucunda orijinal açık mesaja, imzalanmış özet mesaj ve Kişi A nın sertifika bilgileri eklenir.
- İmzalanmış mesaj, haberleşme ortamından Kişi B'ye gönderilir.
- Kişi B mesajı aldığında, imzayı onaylama için mesajın imzasını Kişi A'nın açık anahtarını Ka kullanarak açar ve mesajın Kişi A dan gelip gelmediğini kontrol eder. Mesajın Kişi A dan geldiği anlaşıldığında onaylama algoritmasından elde edilen özet değer ile B nin elde etmiş olduğu özet değer karşılaştırılır.
- Bu işlem sonucunda, orijinal mesajın değiştirilip değiştirilmediği tespit edilir. Eğer onaylama işlemi sonunda elde edilen imza özeti açık olarak gelen

orijinal mesajdan elde edilen özet ile aynı ise mesajın yolda değişmediği garanti edilmiştir.

4.1.8. Uygulama 8 (e-imzalı gizlilik)

Uygulama 6 ve uygulama 7 de açıklanan e-imza yaklaşımlarında, gizliliğin sağlanmadığı ortadadır. Bilgi güvenliğindeki gizlilik unsurunu sağlarken fazla işlem zamanına ihtiyaç duyulmaması açısından, uygulama 3 teki gibi simetrik bir yaklaşım kullanılmalıdır.

4.1.9. Uygulama 9 (imzalama ve zaman damgaları)

Elektronik ortamlarda karışıklıklara sebebiyet vermemek için yapılan iş ve işlemlerde tarih ve saat bilgilerinin SM ‘ler (sertifika makamları) tarafından kullanılması gereklidir. AAA ‘da bulunan bir atom saati sunucusu ile o anki saat bilgilerinin elde edilmesi ile karşılaşılabilecek sorunlar ortadan kaldırılır. Elektronik imza da mesaja imzanın tarihi ve saati de eklenir. Bunlar iletinin geri kalan kısmı ile imzalanır.

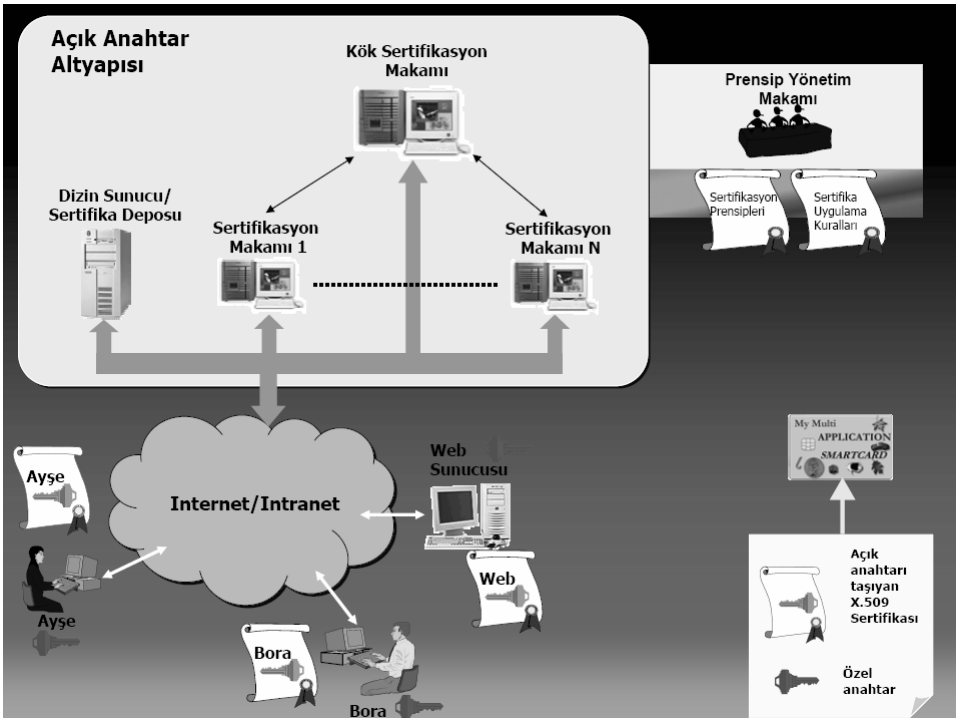
5. AÇIK ANAHTAR ALTYAPISI

Açık anahtar altyapısının temel görevi, elektronik ortamda haberleşen, işlem gören ve çalışan kişiler, kurumlar veya cihazlar arasında güvenilir bir haberleşme ortamı oluşturmaktır. Bu altyapı içerisinde, gizlilik, inkar edememe, kimlik doğrulama veya onaylama, yetkilendirme ve imzalama, süreklilik ve zaman damgası gibi hizmetler verilerek sanal ortam güvenli hale getirilir. Bunun için günümüzde bilgi ve bilgisayar sistemlerinde yüksek güvenlik sağlayan açık anahtar altyapısı kullanılır.

Açık anahtar ile şifrelenen bir veri, sadece bu anahtarın gizli olanı kullanarak deşifre edilir. Bu anahtar çiftinin açık olanı farklı şekillerde kullanıcılara duyurulabilir ve bu duyuru işlemi elektronik posta, kişisel web sayfası veya başka bir şekilde dağıtılabilir. Bu yapıda kullanılan gizli anahtarların güvenliği yüksek

ortamlarda üretilmesi ve korunmaları gereklidir. Bunun için akıllı çubuklar veya akıllı kartlar kullanılır.

Bir AAA'da ; makamlar (Kayıt Makamı, Sertifika Makamı, Kök Sertifika Makamı) , sertifikalar, depolama ve arşivleme birimleri ve güvenlik prensipleri bulunur. Bu yapıda kullanıcı sertifikaları, kullanıcı-imza ilişkileri, açık ve nadiren gizli anahtarlar, sertifikalarla ilgili işlemler, sertifika ve dizin sunucusu yer almaktadır. Bu özelliklerin birbiri ile uyumlu ve uluslararası standartlara uygun olması gerekmektedir. Bu altyapıda, güvenilir makamlar tarafından anahtar ve sertifika oluşturma, onaylama saklama, yayımlama, dağıtma, onayları geçici olarak durdurma, ve sonlandırma işlemleri gerçekleştirilir. Bir AAA 'nın kurulabilmesi için birden çok SM (sertifika makamı) bu yapı içinde olmalıdır. Bir sertifika makamı, sayısal imzayı kullanan kişilerin açık anahtarlarını veya sertifikalarını onaylamak, verdiği onayları geri almak ve onayladığı sertifikaların geri alınan onay listesini, kullanıcıların zarar görmemesi için yayımlamak zorundadırlar. Bir AAA yapısında, birden çok SM bulunduğunda, bu SM lerin güvenli olarak sertifikalarını alabileceği, güvenli bir makama ihtiyaç duyulmaktadır. Bu makama kök sertifika makamı (KSM) denilir. AAA'ya duyulan güvenin sürekli olması için, KSM 'lerin ve SM'lerin; güvenlik, uygulama, ve denetim politikaları iyi yapılandırılmalıdır. Bunun yanında fiziksel güvenliğin sağlanması, kullanılan yazılımların ve donanımların dikkatli seçilmesi gereklidir. [6] Şekil 5.1.' de genel bir açık anahtar altyapısı gösterilmiştir.



Şekil 5.1. Genel Bir Açık Anahtar Altyapısı. [22]

Genel bir AAA yapısında, temel bileşenler arası haberleşmedeki işlem sırası şu şekilde olmaktadır.

- E-devlet, e-iş, e-bankacılık yapmak isteyen bir kullanıcı Kayıt Makamına müracaat eder.
- Kullanıcı kayıt makamından gizli anahtarını almak için istenilen bilgi ve belgeleri hazırlar ve KM'ye teslim eder.
- Bilgi ve belgeler , KM tarafından güvenli bir şekilde SM'ye ulaştırılır. Belgeler kontrol edilir.
- Kayıt makamında ve SM'de, o kullanıcı için bir açık ve bir gizli anahtar üretilir.
- Üretilen açık anahtar bir sertifika ile ilişkilendirilir.
- Kullanıcıya ait olan gizli anahtar, kullanıcıya bir akıllı çubuk veya akıllı kart içerisinde verilir.
- Güvenliği artırmak için kullanıcıya bir IN numarası geçici olarak verilebilir.

- SM, verilen sertifikaların anahtar ve sertifika bilgilerini, sürekli olarak yayınlanması için, uygun bir sunucuya yönlendirir. Kullanıcıların, kendileri veya iş ve işlem yapacağı diğer kullanıcıların, sertifika detayları hakkında bilgi alabilecekleri şekilde kullanıcılara sunulur.
- Problemli sertifikalar ise sertifika iptal listelerinde (SİL) yayınlanır.

5.1. AAA' nın Oluşturulması

AAA sistemini oluşturabilmek için, bir KSM 'ye ve SM 'lere ihtiyaç duyulmaktadır. SM 'ler kullanıcıların açık anahtarlarını tutmak, sertifikanın geçerliliğini kontrol etmek, sertifikaları gerektiği durumlarda iptal etmek, yayınlamak, kaydını tutmak, onayladığı sertifikaları ve iptal listelerini (SIL) dağıtmak ve yayımlamak zorundadırlar. Tüm bu işlemler belirli politikalar çerçevesinde yürütülür. [5]

Her SM'in güvenlik politikası, kurulum aşamasında belirlenir ve güvenliğin her zaman sağlanması gereklidir. Güvenilir tek bir yetki biriminin olması AAA'nın yönetilmesi ve çalışması için gerekmektedir. Bu güvenilirliğin oluşturulmasında, X509 standartında sertifikaların oluşturulması ve saklanması için, bu standartta iletişim kurabilecek yazılımlara ihtiyaç duyulur.

Sertifika makamı sunucusu, alt kayıt makamlarından gelen bilgileri barındırır ve gerekli ise ilgili sunuculara yönlendirir. Kullanıcılar haberleşecekleri kişilerin açık anahtar ve sertifika bilgilerini sertifika ve anahtar sunucusundan bir defaya mahsus alırlar. İmzalama için gerekli olan gizli anahtar bir akıllı kart üzerinde saklanır. Bu kart tek bir kişi de bulunmalıdır. AAA oluşturulurken kullanıcı sayıları, tercih edilecek uygulamalar, mevcut kaynaklar, altyapının genişlemesi, güvenlik politikaları, E-imza kanunu dikkate alınmalıdır. [10]

Bir açık anahtar altyapısı aşağıdaki bileşenlerden oluşur.

- Kök Sertifikasyon Makamı
- Sertifikasyon Makamı

- Kayıt Makamı
- Sertifika Deposu
- Arşiv Modülü
- Sertifika Kullanıcıları
- Kriptografik Anahtar Çiftleri
- Sayısal Sertifikalar
- Sertifika İptal Listesi (SİL)
- Sertifikasyon Prensipleri
- Sertifikasyon Yolu
- Akıllı Kart / Token Cihazları
- AAA Yönetim Protokolleri

5.2. Makamlar

Bir AAA yapısında kayıt, sertifika ve kök sertifika gibi makamlar bulunmaktadır.

5.2.1. Kayıt makamı (KM)

Sertifika makamı için sertifika başvurularını alır ve sertifika içine yerleştirilecek bilgilerin doğruluğunu kontrol eder. Topladığı bilgilerden bir sertifika isteği oluşturur. Kayıt makamı topladığı bilgileri SM' ye kendi sayısal imzasıyla imzalayarak iletir. Böylece SM sertifika isteğinin güvendiği bir kaynaktan gelip gelmediğini anlayabilir. Kendi özel anahtarını çok iyi korumalıdır. Birden çok SM için bu hizmeti verebilir.

5.2.2. Sertifika makamı (SM)

Donanım, yazılım ve sistemi işleten kişiler sertifika makamını oluşturur. Ayırt edici özellikleri; adı ve anahtar çiftidir. Görevleri, sertifika yayınlamak, sertifika durum bilgilerini güncel tutmak ve sertifika iptal listeleri (SİL) hazırlamak, güncel sertifikaları ve SİL'leri isteyen kişilere sunmak, süresi dolan ya da iptal edilen sertifikaların arşivini tutmaktır. Bir SM, KM ve sertifika deposu gibi pek çok farklı

alt bileşenden veya hizmetten oluşmaktadır. Bu makamların en ayırt edici özelliği kullandıkları, özel ve açık anahtar çiftlerini nasıl ürettikleri ve bunu nasıl koruduklarıdır. Bunun en güvenilir yollarından biri, şifreleme bilimi tabanlı akıllı kart veya donanımsal güvenlik modülleri kullanmaktır. Bu modüllerin standartları, NIST ve benzeri kurumlar tarafından belirlenmektedir ve belirli aralıklar ile yayınlanmaktır. SM 'nin en önemli görevlerinden biri, sertifikaları yayınlamadan önce, içeriğinin tamamen doğru olduğunu teyit etmektir. Bu doğrulama işlemi için, her sertifika SM 'nin özel anahtarı ile imzalanarak sertifikaya eklenir. Kişisel bilgilerin doğrululuğun sağlanması, KM'de kullanıcı kimliğinin, pasaportunun veya ehliyetinin bir fotokopisinin alınması ile gerçekleştirilir.

5.2.3. Kök sertifikasyon makamı (KM)

Hiyerarşik olarak en üstte yer alan ve altyapıdaki tüm bileşenlerin elektronik imzasına güvendiği makamdır. Sadece sertifikasyon makamları için sertifika üretir. Son kullanıcılar için sertifika üretmez .[16]

5.2.4. Sertifika deposu

Sertifikaların ve sertifika iptal listelerinin dağıtımını yapar. Birden çok SM'nin sertifika ve SİL'lerini depolayabilir. Kendi başına çalışan ve belli bir erişim protokolünü (ör: LDAP) kullanan bir bilgisayar sistemidir. Güvenilir değildir; içindeki sertifikalara ve SİL'lere güvenilmesinin sebebi SM tarafından sayısal imza ile korunmuş olmalarıdır. Barındırdığı sertifika ve SİL'leri sadece yetkili kişiler güncellemelidir. Aksi bir durumda saldırganlar depo içindeki bilgileri kullanılmaz hale getirip AAA'nın çalışmasını engelleyebilir.

5.2.5. Arşiv modülü

Arşivleme bileşeni uzun dönemli veri saklama görevini SM adına yapan modüldür. Arşivleme 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 sayısal imzanın kontrolünde) geçmiş tarihli sertifikanın arşiv modülü tarafından isteyen taraflara verilebilmesi gereklidir.

5.2.6. Sertifikalar

Sertifikalar sayısal olarak oluşturulmuş kimliklerdir. Bilgileri şifreleme ve şifrelenen bilgileri çözmek için kullanılan bir çift elektronik anahtarın biri ile kimlik bilgilerini içerirler. Sayısal sertifikada kullanıcıya ait açık anahtar, kullanıcının adı, son kullanma tarihi, sertifikanın alındığı kurumun adı ve seri numarası gibi bilgiler bulunur. [17]

5.2.7. AAA donanımları

Piyasada kullanıma sunulmuş birçok AAA donanımı mevcuttur. FDD diskleri, USB akıllı çubuklar, hibrit kartlar, akıllı kartlar mevcut donanımlardır.

Akıllı kartlar kullanıcılara ait özel anahtarların muhafaza edilmesi için en güvenli ortamı sunar. Akıllı kartlar, programlanabilir alanları olan, dayanıklı, taşınabilir bilgisayarlardır. Bir kredi kartı ile aynı büyüklükte ve şekildedir. Veri güvenliği, kimlik gizliliği ve mobil kullanıcı ihtiyaçlarına sahip sistemlerde faydalıdırlar.

5.2.8. Akıllı kartlar ve kullanımları

Akıllı kartların private ve public alanları vardır. Private alanında anahtar üretimi, imzalama, şifre çözme gibi işlemler yapılır, bu alana erişim yasaklanmıştır. Public alana genel bilgiler yazılır. Akıllı kart programı yardımıyla buradaki bilgiler görülebilir. Bir PKI akıllı kartında minimum olması gerekenler :

- 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.

5.2.9. AAA yönetim protokolleri

SM, sertifika ve SİL'leri doğru bir biçimde yayınlamalıdır. Kendi özel anahtarını korumalıdır. Kendini AAA'nın diğer bileşenleriyle haberleşirken korumalıdır. AAA Yönetim protokolleri, bilgi toplamak ve yayınlamak için kullanılır.

5.2.10. Yaygın olarak kullanılan yönetim protokolleri

- PKCS #10 Sertifika Talep Standardı ve SSL
- PKCS #10 Sertifika Talep Standardı ve PKCS #7
- Sertifika Yönetim Protokolü (CMP)
- CertificateManagementUsingCMS
- SimpleCertificateEnrollmentProtocol [8]

5.2.11. PKCS standartları

- #1: RSA açık anahtar algoritması kullanarak şifreleme ve sayısal imzalama işlemi yapılmasını tanımlar.
- #3: Diffie-Hellman anahtar belirleme protokolünü tanımlar.
- #5: Bir şifre kelimesinden elde edilen gizli anahtarla şifrelemenin nasıl yapılacağını anlatır.
- #7: Sayısal 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.
- #10: Sertifika talep formatını tanımlar.

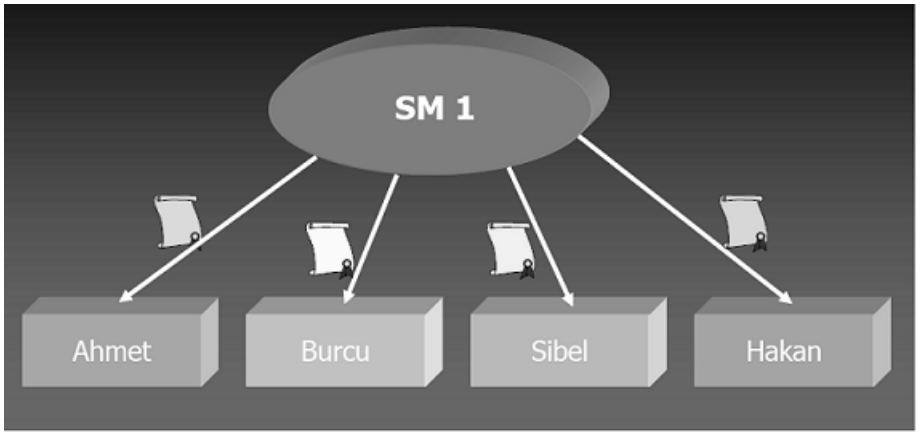
- #11: Kriptografik cihazlarda (akıllı kart vb.) kullanılabilecek donanım bağımsız bir programlama kütüphanesini tanımlar.
- #12: Bir kullanıcının özel anahtarı, sertifikası gibi bilgileri saklamak ve taşımak için bir format tanımlar.
- #13: Eliptik eğri kriptografi kullanarak şifreleme ve sayısal imzalamayı tanımlar.
- #14: Pseudo-randomsayı üretimini tanımlar (geliştirme aşamasında)
- #15: PKCS#11'i tamamlayan bir standarttır. Kriptografik cihaz tiplerini çeşitlendirir.

5.3. Kullanılan Açık Anahtar Altyapıları

Elektronik ortamda iletişimin dünyayı kapsaması için farklı AAA lara ait SM'ler arasında güvenli haberleşme ortamları oluşturulmuştur. Uluslararası sertifika makamları arasındaki ilişkiler ve güvenli haberleşme ortamının oluşturulabilmesi için protokoller, politikalar, prosedürler ve karşılıklı anlaşmalara ihtiyaç duyulmaktadır. Dolayısı ile kurulacak olan AAA ların uluslararası standartlara uyumlu olacak şekilde kurulması gerekmektedir. Bunlar yapılmaz ise sertifika makamları işlemez, kullanılamaz. Bu ve buna benzer sorunlardan dolayı farklı yapılandırmalar mümkün olmaktadır. Basit, dağıtık, hiyerarşik ve çapraz yapılar bu yapılardan bazılarıdır. [11]

5.3.1. Tekli basit yapılar

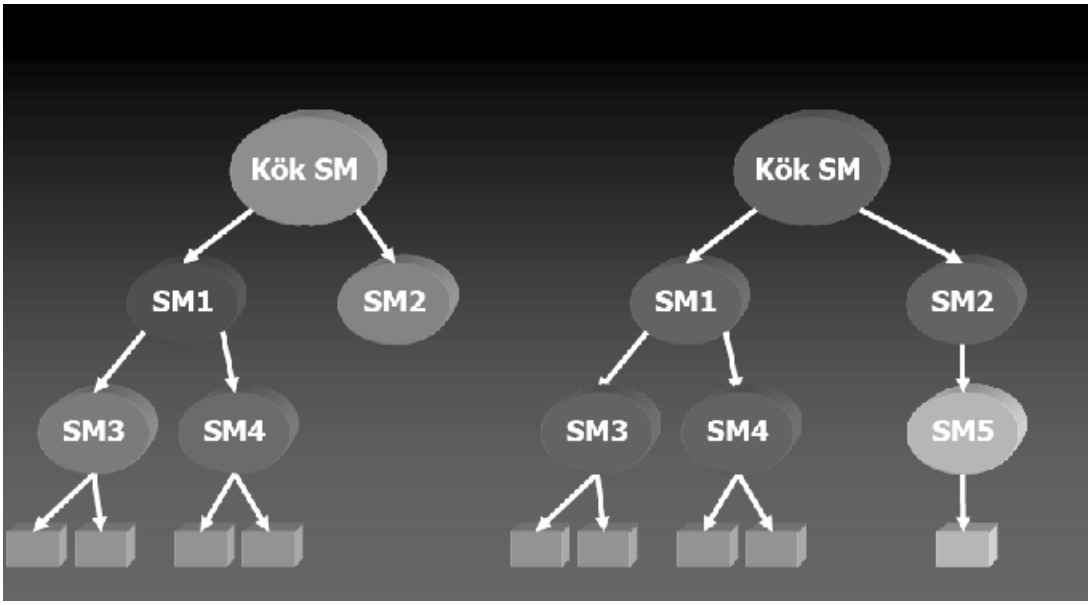
Bu yapılar aynı SM den veya az sayıda farklı SM den sertifika alan bir grup kullanıcı için uygun olup basit yapıdadırlar. Çok az sayıda kullanıcının bulunması ve SM ler arasında bir bağlantı bulunmaması bu yapının özellikleri arasındadır. Bu yapıda SM'ye güven esas olup büyüme ve genişleme yapılamaz. Bu sebeple SM herhangi bir sebepten ötürü kullanılamaz SM leri kendi SM listesine alabildiği için sertifikasyon işlemleri kolaydır. SM sayısının artması ile problemler artmaktadır. Listeye eklenen SM nin güvenilirliğinin belli olmadığı durumlarda ise SM ler güvensiz hale gelmektedir. Aşağıdaki şekilde tek sertifika makamı kullanan AAA yapısı görülmektedir. Şekil 5.2'te SM kullanan AAA yapısı gösterilmiştir.



Şekil 5.2. Tek SM kullanan AAA Yapısı. [22]

5.3.2. Hiyerarşik yapılar

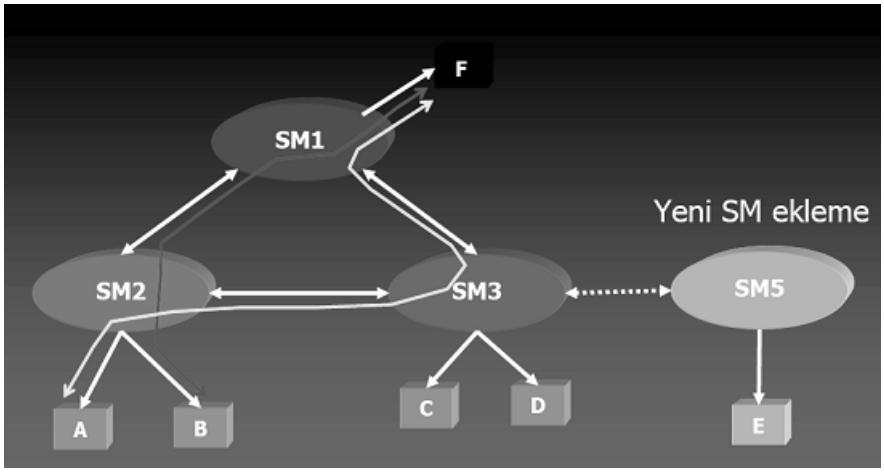
Bu yapılar adından da anlaşılacağı gibi daha karmaşık yapıda olan ve en yaygın kullanılan yapılardır. Ağaç yapısında alt üst ilişkileri mevcuttur. Bu yapılanmada en üstte Kök Sertifika Makamı KSM en altta ise kullanıcılar bulunmaktadır. Üst SM ler alt SM lere sertifika verirler. Bu kapsamda üst SM ler her zaman alt SM lerin yetkilerini sınırlandırabilirler. Basit yapının aksine kullanılamaz hale gelen herhangi bir SM de o makama bağlı olan sertifika sahiplerinin sertifikalarını yeniden oluşturmak yeterli olacaktır ve bu durumdan diğer sertifika sahipleri etkilenmeyecektir. KSM de herhangi bir problem olursa örneğin özel anahtar kaybolursa hemen altındaki SM lere yeni sertifika verilmesi gerekecektir. Bu yapıda sertifika yolu oluşturmak ve yeni SM ler eklemek oldukça kolaydır. [13] Şekil 5.3.'te hiyerarşik yapıdaki AAA mimarisi gösterilmiştir.



Şekil 5.3. Hiyerarşik Yapıdaki AAA Mimarisi.[22]

5.3.3. Dağıtık yapılar

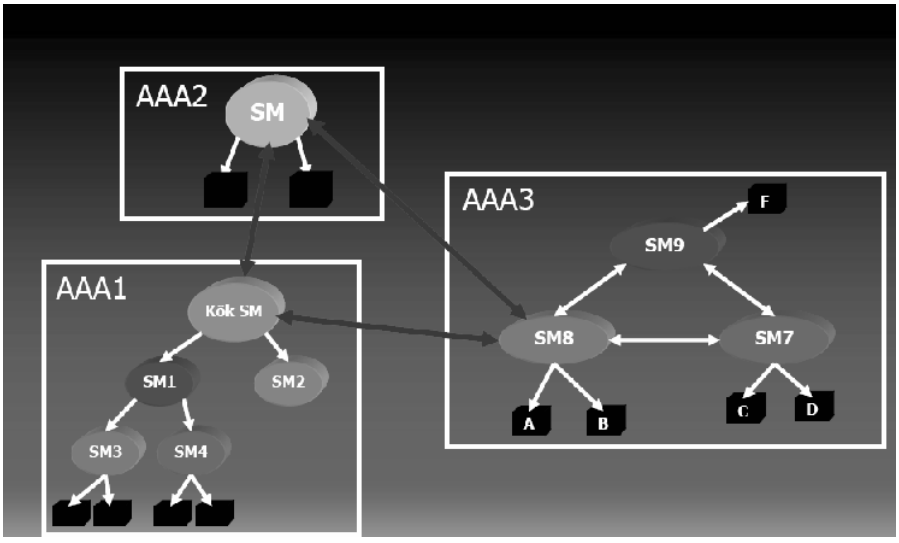
Hiyerarşik yapıya alternatif olarak geliştirilmiştir. Birbirine güvenen SM ler karşılıklı olarak birbirlerine sertifika verirler. Bu sayede kullanıcılar SM lerden bağımsız olarak birbirleri ile güvenli bir ortamda haberleşebilirler. Bu yapıdaki sertifikalar daha fazla bilgi içerdikleri için daha karmaşıktır. Bu yapı altında tekli ve hiyerarşik gibi farklı AAA yapıları ve SM ler oluşturularak birleştirilebildiğinden yapıda çıkabilecek bir problem sertifika sahiplerini de etkileyebilecektir. Bu tür yapılarda SM lerin fazlalığı problem oluşturabilmektedir. Şekil 5.4.'te dağıtık yapıda AAA mimarisi gösterilmiştir.



Şekil 5.4. Dağıtık Yapıdaki AAA Mimarisi.[22]

5.3.4. Çapraz yapılar

Bu yapılanmada farklı AAA sistemleri bir araya getirilebilir. Bu birleştirmelerden SM yöneticileri sorumludur. Bu tasarımı gerçekleştirecek olanlar, birleştirilecek AAA sayısı arttıkça problemlerin de artacağını dikkate almalıdır. Bu yapı çok sayıda AAA dan oluştuğu için yönetimi zor ve zaman alıcı olduğu gibi güvenlik açığı da oluşturabilmektedir. Bunu kolaylaştırmak için AAA yapıları arasında bir Köprü SM kullanılmaktadır. Şekil 5.5'te çapraz yapıdaki AAA mimarisi gösterilmiştir.



Şekil 5.5. Çapraz Yapıdaki AAA Mimarisi.[22]

5.4. AAA' yı Değerlendirme Kriterleri

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

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

5.5. AAA Uygulama Aşamaları

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

5.6. Piyasadaki AAA Yazılımları

AAA içerisinde belirli bir zaman için anahtar çiftlerini ve sertifikalarını üretmek ve bunları kontrol etmek için çeşitli yazılımlar kullanılmaktadır. Günümüz tarayıcıları ve e-posta mesajlarının, sayısal sertifikalar ve iyi korunan anahtar çiftleriyle verilerin imzalanması, doğrulanması, şifrelenmesi, şifrelerin çözülmesi mevcut yazılımlar ile kolaylıkla yapılabilmektedir. VeriSign, GlobalSign, UniCERT, Entrust, TürkTrust, iTrus, eSign, IBM Trust Authorty bunlardan bazılarıdır.

AAA Niçin Önemlidir?

- İş ve işlem sürelerini kısaltmak,

- Uluslararası işbirliği sağlamak,
- Mevcut kaynakların verimli kullanılmasını sağlamak,
- Kişi ve kurumların güvenli ve hızlı haberleşmelerini desteklemek,
- Ortamdan bağımsız güvenlik sağlamak,
- Düşük maliyetli ve yüksek güvenilirlikli haberleşme sistemleri oluşturmak,
- Ülke bilgi güvenliğinin sağlanmasına katkıda bulunmak,
- Ulusal, kurumsal ve kişisel bilgi güvenliğinin sağlanmasını desteklemek,
- Bilişim suçlarının artmasını engellemek,
- Uluslararası standartları kullanmak ve uygulamak.

5.7. AAA Uygulama Alanları

AAA uygulamasının yaygınlaşması, bu yapının uygulama alanlarını belirleme ile doğru orantılıdır. AAA bilişim teknolojilerinin bulunduğu her alanda kolaylıkla uygulanabilmektedir. Bu alanlardan bazıları şunlardır:

- E-birey,
- E-ticaret,
- E-bankacılık,
- E-kimlik,
- E-posta,
- E-devlet,
- E-eğitim,
- E-imza,
- E-yaşam,
- E-sağlık,
- E-bilim.

5.8. AAA Uygulamalarında Karşılaşılabilecek Problemler

AAA ve sertifika yönetimi ile ilgili birçok problem aşılmış olmakla birlikte, bazı noktalarda problem olması ihtimali vardır. Bunlar,

- Bilgi ve bilgisayar sistemlerinin güvenliğinin bilinmesi zorunluluğu,
- Kayıt esnasında yaşanabilecek sorunlar,
- Ücretli olarak sertifikaların sunulması,
- Sertifikaların tekrar üretilmesinde yaşanan sorunlar,
- Hizmet alınacak makama güven sorunu,
- İptal edilmiş sertifikaların zamanında öğrenilememesi,
- Sertifika iptalinin getirdiği ek yükler ve zaman kaybı .[12]

Deneme amaçlı veya belirli bir süre ücretsiz olarak verilen sertifikalar bulunsa da, esas sertifikalar ücret karşılığı verilir. Sınıf-1, sınıf-2 ve sınıf-3 gibi sertifika grupları bulunmaktadır. Sınıf-1 tipi sertifikalar ücretsiz olarak verildikleri gibi ataklara maruz kalabilir daha yüksek güvenlik ve kimlik doğrulama gerektiren durumlarda sınıf-2 ve sınıf-3 sertifikalar kullanılır ve bunlara da bir ücret ödenir. [7]

5.9. Güvenli E-İmza Oluşturma

E-imza oluşturma araçları, SM tarafından verilerin imzaların güvenli bir şekilde oluşturulmasını sağlayan yazılım, donanım veya her ikisinin birlikte kullanılmasını sağlayan araçlardır. İmzaların güvenli bir şekilde oluşturulabilmesi ve saklanması için PKCS#11, Capi, X.509 Sertifika depolanması, ISO 7816, FIPS 140-1, ITSEC LE4 akıllı kart güvenlik sertifikalama vb. Standartlar kullanılmaktadır. Anahtarlar, güvenli merkezlerde offline olarak üretilir. Bu güven merkezlerinde, kullanıcı veri tabanı, açık anahtar üretimi, kayıt ve sertifika makamı, PIN/PUK üretimi, kart basım yazılımı, PIN/PUK kodları basımı, PIN/PUK lu sertifika oluşturma, güvenlik anahtarı oluşturma ve bunları yine güvenli olarak uygun donanımlara ve makamlara aktarma işlerinden sorumlu birimler bulunmaktadır. Güven merkezlerinde anahtarlar asla kart dışında bulunmamalıdır. Her sertifika oluşturma ve yenileme işlemlerinde başka anahtar çiftlerinin oluşturulması güvenlik açısından önemlidir.

5.10. Ülkemizde AAA Hizmeti Sunan Şirketler

- TÜBİTAK-UEKAE,
- E-GÜVEN,

- TÜRKTRUST.[23]

5.11. AAA İçerisinde E-İmza Kullanımı

Açık anahtar altyapısı içinde N adet SM, Prensip Yönetim Makamının belirlemiş olduğu politikalara göre sertifika hizmet sağlayıcı görevlerini yerine getirmektedirler. Bu yapı içinde Kişi A, Kişi B ve Sunucu C nin kullanıcılar olduğunu düşünelim. Bu kullanıcıların özel(gizli) anahtarları akıllı kartlar veya güvenli sunucular üzerinde bulunmaktadır. E-imza almak isteyen bir kullanıcı bir KM'ye müracaat edip sertifikasını yani özel anahtarını almak zorundadır. Bu anahtarı alırken bu gizli anahtara bağlı olarak bir de açık anahtar ve bu açık anahtar ile ilişkilendirilen bir sertifika üretilir.

E-imzası olan Kişi A nın Kişi B ile haberleşmesi gerektiğini düşünelim. Kişi A nın yapması gereken ilk iş haberleşmek istediği Kişi B nin açık anahtarını bilmek ve bunu sistemden sorgulamak olmalıdır. Açık anahtarı elde edilen Kişi B nin bu anahtarı kendi sertifikası ile ilişkilendirilmiştir. Kişi A SM yardımı ile Kişi B ye ait olan sertifikayı arar ve bulur. Sertifika hangi dizinlerde tutuluyor ise o dizin altından sertifikayı alır ve SM üzerinden Kişi A ya iletilir. Güvenli bir haberleşme için aynı şekilde Kişi B nin , Kişi A nın açık anahtarına ve sertifikasına sahip olması gerekir. Bu işlemin aynısını Kişi B de yapmak zorundadır. Bu işlemler başlangıçta bir kez yapılır. Güvenli haberleşmek isteyen kullanıcıların sertifikaları kullanıcı bilgisayarına bir kez indirilir ve bu işlemlerin bir daha yapılmasına gerek kalmaz. Bu yapı içinde kullanıcılar birbirleri ile güvenli olarak haberleşmek isterlerse haberleşmek istedikleri kullanıcıların açık anahtarlarını ve sertifikalarını tüm kullanıcılara açık olan ve SM bünyesinde bulunan bir sertifika deposundan elde edebilirler.

SM altında bir KM var ise, Kişi A'nın imzasını almak için KM ye müracaat etmesi gereklidir. Belgeleri sağlayan kullanıcı e-imzasını kısa sürede alabilir. Anahtar üretimi ve sertifika ile ilişkilendirilmesi KM de yapılır. Üretilen bu sertifika her zaman kullanılmak üzere SM bünyesinde bir sertifika deposunda veya sistemde bulunan bir dizin sunucu üzerinde belirlenen dizinler altında tutulur.

AAA yapısında güvenli olarak haberleşebilmek için açık anahtarlara, sertifikalara, sertifika yönetimine ve bu hizmeti veren destek ünitelerine ihtiyaç

vardır. Kullanıcıların birbirlerinin sertifikalarına sahip olmaları güvenli bir haberleşme için gerekli fakat yeterli değildir. Kişi B nin Kişi A ile güvenli olarak haberleşebilmesi takip edilmesi gereken adımlar şu şekilde olmaktadır.

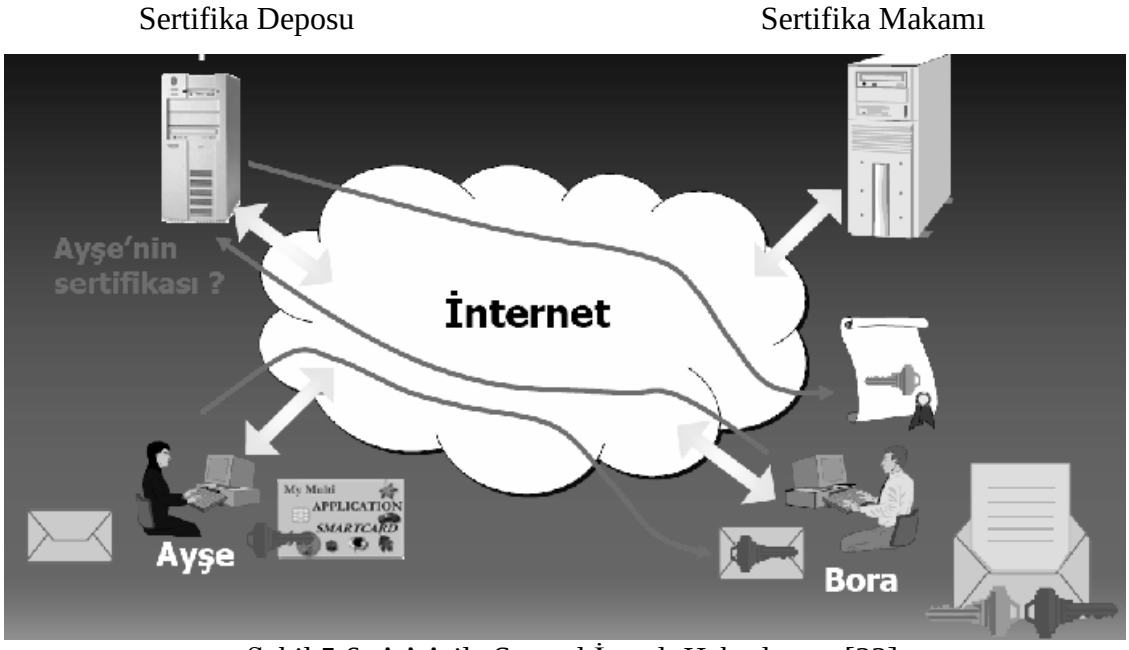
1. Kişi B, Kişi A nın açık anahtarını içeren sertifikasını SM bünyesinde buluna sertifika deposundan sorgular.

2. Açık anahtarı temin eden Kişi B , Kişi A nın sertifikasını kendi bilgisayarına sunucudan indirir. Bu işlem başlangıçta bir kez yapılır ve Kişi A nın sertifikası sonradan sunucuya tekrar sorulmadan kullanılabilir. Burada dikkat edilmesi gereken husus Kişi A ya ait olan sertifikada bir problem oluşmuş ise bu SM de o kullanıcıya ait olan sertifikayı SİL de yayımlamış ise geçersiz olan bu sertifikanın kullanımının önüne geçilmesi gerekliliğidir. Bu durumda sertifikanın geçerli olduğu sorgulanarak teyit edilmelidir. Bu işlemler OCSP de otomatik olarak yapılabilir.

3. Bu aşamaların ardından kişi B mesajını güvenli olarak Kişi A ya gönderebilecektir.

4. İmzalı mesajı alan kişi A, kendi özel anahtarı ile mesajları açabilir. Böylece hem mesajı alma hem de kimlik doğrulama işlemlerini burada gerçekleştirmiş olur. Yapılan haberleşmenin güvenlik unsurlarını tam olarak karşılayabilmesi için gizlilik ve bütünlük işlemleri de tamamlanmalıdır. Gizlilik için simetrik algoritmalar, bütünlük için ise özetleme algoritmaları kullanılır.

Açık anahtar şifreleme de, asimetrik şifreleme algoritmalarının çoğunluk ile anahtarları, simetrik algoritmaların ise hızlı çevrim yapmalarından dolayı mesajları şifrelemede kullanıldıkları bilinmelidir. Zaman damgası da bu işlemler eklenebilir. Zaman damgasının uygulanabilmesi için uygun olan bir atom saatinden gerekli zaman bilgisi alınmalıdır. Şekil 5.6’da AAA ile sayısal imzalı haberleşme gösterilmiştir.



Şekil 5.6. AAA ile Sayısal İmzalı Haberleşme.[22]

6. SERTİFİKALAR ve SERTİFİKA YÖNETİMİ

Kullanıcı kişinin, nesnenin veya kurumun elektronik ortamda tanınması veya bilinmesi için kullanılan elektronik veya sayısal kimliğe veya dökümana sayısal sertifika denir. Sertifikaların güvenli olarak oluşturulabilmesi için, belli bir formatta hazırlanmış olan kimlik bilgilerini ve anahtar bilgisini içeren elektronik ortamda oluşturulmuş nitelikli bir döküman olması gereklidir.

Sertifikalar ve sertifika yönetimi bilgisayar sistemleri ile güvenli olarak haberleşme sağlanmasında AAA nın önemli bileşenlerinden biri olup kimlik sahibi hakkında detaylı bilgi vermenin yanında bu bilgilerin doğruluğu, güvenilirliği, kullanıcıların ve sertifika hizmet sağlayıcıların zarar görmemesi için nasıl kullanılması ve hangi kurallara uyulması gerektiği gibi detayları içerir. Aynı zamanda elektronik ortamda kişilerin gizliliğini ve kimlik doğrulamasını sağlamak amacı ile kimlik sahibine ait olan açık ve gizli anahtar çiftleri ile kimlik bilgileri arasında ilişki kurulmasını sağlarlar. [10]

Sertifikalarda tanımlama, sertifika sahibi ve sertifika kullanıcısı tanımlarını iyi bilmek gerekir. Tanımlama, sertifikada tanımlanan kullanıcı kişi veya objedir. Yani sertifika kullanıcı bilgileridir. Sertifika sahibi, sertifikanın başlık alanında

tanımlanır ve kime ait ise onun adını içerir. Sertifika kullanıcısı ise bu sertifikayı alan ve onu sertifika sahibinin kimliğini saptama amacı ile kullanan kişidir. Sertifikaları kişiler alabileceği gibi haberleşme cihazları da (sunucu, ağ cihazları gibi) alabilir. Sertifika kullanıcıları güvenen taraf olarak bilinir.

6.1. Sertifikalar

Sertifikalar erişimi yetkilendirmek, kimlik doğrulamak, inkar edememeyi sağlamak, bilgileri şifrelemek ve şifrelenen bilgileri çözmek için kullanılan elektronik anahtar çiftleri ile ilişkilendirilirler. Oluşturulan sayısal kimlik veya sertifika sayesinde kullanıcılar, bilgilerinin haberleşme esnasında güvenli bir şekilde bilgilerin iletilmesini alınmasını ve korunmasını sağlarlar. Sertifikalar ile bilgisayar ağları üzerinde haberleşilirken ya da iş yapılırken güven, güvenlik, güvenilirlik sağlanmaktadır. Sayısal bir sertifikada kullanıcı adı, kullanıcı özellikleri, kullanıcı açık anahtarı, geçerlilik tarihi, kullanıcı e-posta adresi, sertifikanın alındığı kurumun adı, seri numarası ve açık imzası gibi bilgiler bulunur. Sertifikalar;

- Gönderilen veya alınan bilgilerin iletişim anında gizliliğinin sağlanması,
- Mesajı gönderenin ve alanın doğru kişiler veya kurumlar olup olmadığını tespit etme,
- Gönderilen veya alınan dökümanların tarih ve zamanının doğrulanması,
- Döküman arşiv oluşturulmasını kolaylaştırma,
- Haberleşmenin sürekliliğinin sağlanması gibi temel özellikleri sağlarlar.

6.1.1. Basit sertifikalar

Asimetrik kriptografi de bir kişi için üretilen anahtar çifti, özel ve açık anahtardan oluşur. Bu anahtarlardan açık olanı anahtarın sahibiyle haberleşmek isteyen herkes tarafından görülebilir ve kullanılabilir. Bu açık anahtarın isteyen kişilerce kullanımını kolaylaştırmak için değişik şekillerde yayınlanması ve isteyenlerin erişimine açılması mümkündür. Bu yayınlama şekline sertifika adını verilmektedir.

Açık anahtar yayınlama biçimlerinden birisi kişisel kartvizitin bu amaçla kullanılması olabilir. Kartvizitleri basit sertifikalar olarak kullanmak mümkündür. Bir toplantı yapıldığını ve Ahmet'in herkese kartvizitini dağıttığını düşünelim.

6.1.2. İdeal sertifika

Basit sertifikalar bölümünde bahsedilen, kartvizit ve kredi kartı yöntemiyle açık anahtar yayınlanması oldukça zor ve kullanışsız görünmektedir. Bu örneklerde görülen problemleri çözmek amacıyla ideal sertifika tanımı yapılmıştır. Bu tanıma göre ideal bir sertifika

• Elektronik ortamda (örneğin: internette) yayınlanabilmesi ve otomatik olarak işlenebilmesi için tamamen sayısal olmalıdır.

• Özel anahtarın sahibinin adını, çalıştığı şirketin/kurumun adını ve irtibat kurmak için gerekli bilgileri içermelidir.

• Sertifikanın ne zaman yayınlandığını anlamak kolay olmalıdır.

• Özel anahtarın sahibi tarafından değil güvenilir bir 3. kurum tarafından yaratılmalıdır.

• Güvenilen kurum birçok sertifika yaratacağı için (aynı kullanıcı için bile birden fazla) her bir sertifikanın diğerinden kolayca ayırt edilebilmesi gereklidir.

• Bir sertifikanın gerçek veya sahte olduğu kolayca tespit edilebilmelidir.

• Değiştirmeye karşı korunmuş olmalıdır.

• İçindeki bilgilerin güncel olup olmadığı istendiği anda tespit edilebilmelidir.

• Hangi uygulamalar için kullanılabileceği sertifikanın içinde yazmalıdır

6.1.3. Açık anahtar sertifikaları

İdeal sertifika tanımına uygun bir elektronik sertifika oluşturabilmek için uluslararası ITU kurumu X.509 standardını tanımlamıştır. Bu standarda uygun olarak hazırlanan bir sertifika aşağıdaki özellikleri taşır:

• Sayısaldır, bilgisayarda veya elektronik bir cihazda hazırlanır.

• Sahibinin adını ve açık anahtarını içerir.

• Kullanıma giriş tarihini ve son kullanım tarihini içerir.

• Yayınlayan güvenilir kurumun adını içerir.

• Yayınlayan kuruluş tarafından verilmiş tekil bir seri numarasına sahiptir.

• İçeriğin bütünlüğü yayınlayan kuruluşun sayısal imzasıyla koruma altına alınmıştır.

Şekil 6.1. ’te bu özellikleri taşıyan örnek bir sertifika gösterilmiştir.

Seri No	2368
Sertifika Sahibi	
Şirket/Kurum	
Yayınlayan	
E-posta Adresi	
Yayın Tarihi	05.02.2004
Son Kullanım	05.02.2005
Açık Anahtar	2489349e894859f45489450dab45454 ca0908d8809
Yayınlayan Kurumun Sayısal İmzası	ae89349c989893e8989548d0 823048b08023f9e903

Şekil 6.1. Sertifika Örneği.[24]

6.2. Açık anahtar sertifika özellikleri

Açık anahtar sertifikaları aşağıdaki özellikleri taşır:

• Sayısaldır.

• Sahibi hakkında gerekli olan tüm bilgileri içerir.

• Yayın tarihi ve son kullanma tarihi vardır.

• Yayıncısının adını barındırır ve onun sayısal imzasıyla doğrulanması yapılır.

• Yayıncı adı ve sertifika seri numarası sertifikanın tekil olmasını sağlar.

• Sertifikanın bütünlüğünün bozulması engellenemez ama böyle bir durum sayısal imzanın kontrol edilmesiyle hemen anlaşılır.

Bu özellikler, açık anahtar sertifikasını ideal sertifika tanımını karşılamaya çok yaklaştırır ama bu sertifikalarda eksik kalan iki nokta vardır:

• Sertifikanın içindeki bilgilerin güncel olduğu kesin değildir. (Ahmet işten çıkarılmış olabilir)

• Sertifikanın örnekteki gibi bir sipariş için kullanılabileceğini Burcu nasıl tespit edecektir?

6.3. Sertifika iptalleri

Açık anahtar sertifikasının içeriğinin güncel olup olmadığı sorusuna cevap vermek gerekmektedir. Çünkü:

• Sertifika sahibinin erişim bilgileri değişmiş olabilir

• Sertifika sahibi özel anahtarını kaybettiği için yeni bir açık anahtar kullanmaya başlamış olabilir.

Sertifika sahibi sertifikasını kullanmak isteyen kişilere dağıttıktan sonra geri toplayamaz. Ayrıca sertifika sahibinin kendisi ile ilgili değişiklikleri duyurması çok zordur. Bu nedenle sertifika iptal listeleri (SİL) kullanılır.

Sertifika iptal listeleri aşağıdaki özellikleri taşır:

• Sayısaldır.

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

• Yayın tarihini ve son kullanım tarihini içerir.

• Yayınlayan kuruluşun adını ve sayısal imzasını içerir.

• Sık aralıklarla elektronik ortamda (örneğin internette) yayınlanır.

Şekil 6.2.'te örnek bir sertifika iptal listesi gösterilmiştir.

Şekil 6.2. Sertifika İptal Listesi Örneği.[24]

SİL'lerin bir periyot boyunca geçerli olması, örneğin 24 saatte bir yenilenmesi, bu periyot boyunca iptal edilen sertifikalardan haberdar olmayı geciktirmektedir. Kullanıcılar iptal olan bir sertifikayı bir sonraki periyot ta yayınlanan SİL içinde görebilmektedirler. Finanssal işlemler gibi anlık doğrulamaya ihtiyaç duyulan uygulamalarda SİL yöntemi yeterince güvenlik sağlamamaktadır. Bu

nedenle çözüm olarak Çevrimiçi Sertifika Durum Protokolü kullanılmaktadır (OCSP - Online Certificate Status Protocol).

6.4. Sertifika ilkeleri

Sertifika ilkeleri, 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 sözleşme onaylama gibi değişik amaçlarla kullanılabileceğini gösteren özel değerler taşıyabilirler.

Şekil 6.3.'te sertifika ilke bilgisi taşıyan bir sertifika gösterilmiştir.

Şekil 6.3. Sertifika İlke Bilgisi Taşıyan Sertifika Örneği.[24]

6.5. Sertifikasyon yolu:

Sertifikaların doğruluğu kontrol edilirken her zaman sertifikayı imzalayan makamın elektronik imzasının doğruluğu kontrol edilir. Bu kontrol işlemi birbirine bağlı olarak bir veya daha fazla sertifikadan oluşan bir zincirin, yolun takibini ve doğrulamasını gerektirebilir.

Şekil 6.4.'te bu amaçla geliştirilen değişik sertifikasyon yolu çözümleri gösterilmiştir.

Şekil 6.4. Sertifikasyon Yolu.[24]

• Ölçeklenebilir bir sistem kurulmaya çalışılır.

• Sertifika yöntemi hiç tanımadığımız kişilere güvenilir bir kurum aracılığıyla güvenmemizi sağlıyor.

• Haberleştiğimiz 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 yaratabilir.

• İki sertifika yayıncısı birbirlerine güvendiklerini gösteren sertifikalar yayınlayarak çapraz sertifikasyon yapabilirler.

6.6. X.509 Sertifikaları ve Sertifika İptal Listeleri

AAA sistemlerinde yaygın olarak kullanılan sertifika standartlarının başında X.509 standardı gelir. 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 Sertifika İptal

Listesi (SİL) V1, V2 sürümleri tanımlanmıştır. X.509 sertifikaları ile ilgili diğer IETF RFC dokümanları ise şunlardır:

RFC 2560 Online Certificate Status Protocol (Çevrimiçi Sertifika Durum Protokolu)

RFC 3039 Internet X.509 Public Key Infrastructure Qualified Certificates Profile (Nitelikli AAA Sertifikaları)

RFC 3281 An Internet Attribute Certificate Profile for Authorization (Özellik Sertifikaları)

6.7. X.509 sertifika tanımı

X.509 Sürüm 1 dokümanı aşağıdaki temel alanları tanımlar:

• Sertifikayı yayınlayanın tekil kayıt adı, ör: ou=UEKAE, o=TUBITAK

• Sertifika sahibinin tekil kayıt adı, ör: cn=Müge Çevik, ou=UEKAE, o=TUBITAK

• Sertifikalandırılan Açık Anahtarın kendisi

• Geçerlilik süresi (Başlangıç-Bitiş) (Yerel Sistem saatine yada GMT'ye göre)

• Açık anahtar algoritması (RSA, DSA, Elliptic Curve)

• Sertifika makamının imzalama algoritması (RSAMD5, RSASHA-1, DSASHA-1, ECDSA)

• Sertifika makamının imzası

X.509 Sürüm 2, Sürüm 1'e ek olarak tekil kayıt adındaki "cn" alanın tekilliğini sağlamak için başka bir tekil id kullanır. Sürüm 2 artık kullanılmamaktadır.

X.509 Sürüm 3, Sürüm 1'e ek olarak eklentiler içerir. Bunlar

• Standart eklentiler

• Özel eklentiler

olarak iki tipte olabilirler. X.509 Sürüm 3 sertifika yapısı tüm beklentilere yanıt verebilecek esneklikte ve kapasitededir.

6.7.1. Sertifika bütünlüğünün korunması

X.509 Sertifikasının bütünlüğünün korunması için sertifika içinde yer alan tüm bilgiler sertifikayı veren makam tarafından elektronik olarak imzalanır ve oluşan elektronik imza bu sertifikanın arkasına eklenir. Böylece sertifika alanlarından herhangi birisi üzerinde sonradan değişiklik yapılıp yapılmadığı kontrol edilebilir. Bir elektronik sertifikanın üstündeki elektronik imza doğrulanarak sertifikanın geçerliliği kontrol edilir.

6.7.2. Sertifikanın kodlanması

X.509 Sertifikaları byte dizilerinden oluşan elektronik dokümanlardır. Bir elektronik sertifikanın uzunluğu, kullanılan anahtar uzunluğu ve eklentilere bağlı olarak değişmekle beraber genellikle birkaç kilobyte'ı geçmez.

X.509 Sertifikasının nasıl kodlanacağı ASN.1 kodlama formatında RFC 2459'da belirtilir. Bu kodlama kuralları DER (Distinguished Encoding Rules) ile byte'lara çevrilir.

ASN.1 temel bileşenler ve bu bileşenlerin içiçe geçmesinden oluşan karmaşık yapılardan oluşur. DER uygulamak için bu kurallara uygun yazılım geliştirmek gerekir.

Örnek bir sertifika aşağıda görülmektedir (Base64 formatında):

-----BEGIN CERTIFICATE-----
MIICbDCCAdWgAwIBAgICAfAwDQYJKoZIhvcNAQEEBQAwWjETMBEGCgmSJomT8ixk
ARkTA25ldDEUMBIGCgmSJomT8ixkARkTBGFzeWExCzAJBgNVBAYTAlRSMRMwEQYD
VQQKEwpLU00gMzFFa2ltMQswCQYDVQQLEwJTTTAeFw0wMzExMTcxNDU1MDBaFw0w
NTAxMTcxcxU1MDBaMG0xGzAZBgNVBAseEgBNAEEAMwAgAEcAcgB1AGIAdTErMCkG
A1UECx4iAEEAcwBrAGUAcgBpACAATQBlAHMAYQBqAGwAYQFfAG0AYTEhMB8GA1UE
Ax4YATzzcwBtAGEAaQBsACAARwD8AG4AZQFfMIGfMA0GCSqGSIb3DQEBAQUAA4GN
ADCBiQKBgQCgiPkpKqQCdyc8PXUf+XYCP9+ArPIMVKvLsN384534o149BdFTdrn6
e6sqejRHxfCw2Aw1ufvLnkoV+mgdZA8abaPB5I10LzwMen9XKH+SkRGRjtsJGYMJ
NNoWA/78PvcTZT3IyGscaI+4ng6PkiXunFUj7AP1CNoUphYXkOr/zQIDAQABoy4w
LDAaBgNVHREEEzARgQ9pc21haWxAYXN5YS5uZXQwDgYDVR0PAQH/BAQDAgAgMA0G
CSqGSIb3DQEBBAUAA4GBAHFhqb8p5uYNNG36AJdrbPgZBR2hUNiWPv8vAzOQZv+V
bsV8v+D4d4o8iYU18wM/WqMe1O9n5thJMHvaUAkSbfoz8OVN5KVqjjNGcN5GdcXB
q1yszIGB1pBCoUENTi8rGrtO2Mmoa0O3ynW6u8us18b63mj8RctdOn0xJm19m+H6
-----END CERTIFICATE-----

6.7.3. X.509 sertifika eklentileri

Sertifika eklentileri X.509 Sürüm 3'de tanımlanmıştır. Bu eklentiler sertifikaların kullanımı kolaylaştıran ve yaygınlaştıran özelliklerdir. Tüm sertifikalarda olabilen eklentiler aşağıda görülmektedir:

• Anahtar kullanım amacı- Key Usage (İmzalama, Şifreleme)

• Özel anahtar kullanım amacı - Enhanced Key Usage (İstemci kimlik doğrulama, sunucu kimlik doğrulama, zaman damgalama, e-posta koruma)

• Öznenin Alternatif Adı - Subject Alternative Name (e-mail adresi, X.400 adı, IP adresi, DNS adı)

• Makam İmzalama Sertifikası Yeri

• Sertifika İptal Listesi Yeri

• Sertifika Politikası Nesne Belirteci - Policy Object Id

• Temel Kısıtlamalar

• Özel eklentiler

6.7.4. Sertifikasyon makamı imzalama sertifikasına özel eklentiler

• Sertifika Politikası Eşleştirme - Mapping

• İsim Kısıtlaması

• Politika Kısıtlaması

6.7.5. Anahtar kullanım amacı

Anahtar Kullanım Amacı (KeyUsage) alanı X.509 Sürüm3 tipinde bir sertifikada bulunur. Bu alan kritik bir alandır. Bu alan aşağıdaki değerlerin bir veya daha fazlasını taşır:

• Sayısal İmza: Bu sertifika ile sayısal imza oluşturulabilir. (DigitalSignature)

• Red Olmayan: Bu sertifika ile inkar edemezlik hizmeti sağlanabilir. (NonRepudiation)

• Anahtar Şifreleme: Bu sertifika ile başka anahtarlar taşıma amacıyla şifrelenebilir. (keyEncipherment)

• Veri Şifreleme: Bu sertifika ile anahtar haricindeki veriler şifrelenebilir. (dataEncipherment)

• Anahtar Anlaşması: Bu sertifika ile anahtar anlaşması işlemleri yapılabilir. (keyAgreement)

• Sertifika İmzalama: Bu sertifika ile üretilen sertifikalar imzalanabilir. Bu tip sertifikalar SM'ler için üretilir. (keyCertSign)

• SİL İmzalama: Bu sertifika ile üretilen sertifika iptal listeleri imzalanabilir. (cRLSign)

• Sadece Şifrele: Anahtar anlaşması işleminde bu sertifikadaki anahtarın sadece şifreleme amacıyla kullanılabileceğini gösterir. (encipherOnly)

• Sadece Şifre Çöz: Anahtar anlaşması işleminde bu sertifikadaki anahtarın sadece şifre çözme amacıyla kullanılabileceğini gösterir. (decipherOnly)

6.7.6. Öznenin alternatif adı

Kullanışlı İsim (Subject Alternative Name) olarak da bilinen bu eklenti içinde bulunduğu sertifikanın uygulama amacına uygun olarak kullanılmasına yardımcı

olan bilgileri taşır. Aşağıda değişik sertifika tipleri için bu alanın taşıyabileceği bilgiler gösterilmektedir:

• E-posta (S/MIME) sertifikası

Subject Alternative Name: RFC822Name=e-posta adresi

• X.400 sertifikası

Subject Alternative Name: X.400Adress= X.400 adresi

• VPN-IP sertifikası

Subject Alternative Name: Ip Address=IP adresi

• VPN-DNS sertifikası

Subject Alternative Name: DNS Name=DNS adı

• Windows Logon sertifikası

Subject Alternative Name: RFC822Name=e-posta adresi, UPN=kullanıcı adı

6.7.7. Çeşitli eklentiler

Yetkili Bilgi Erişimi (Authority Information Access) eklentisi, içinde yer aldığı sertifikayla ilgili makamlara nasıl ulaşılabileceğini gösteren bilgiler içerir. Bu alanda aşağıdaki bilgiler yer alabilir:

• Kullanıcı sertifikasını yayınlayan SM'nin imzalama sertifikasının bulunduğu yer

• ÇİSDUP- Çevrimiçi Sertifika Durum Protokolü(OCSP-Online Certificate Status Protocol) sunucusunun bulunduğu yer

SİL Dağıtım Noktaları (CRL Distribution Point) eklentisi, içinde bulunduğu sertifikanın yayıncısı tarafından yayınlanan Sertifika İptal Listesi'nin bulunduğu yeri gösterir.

6.7.8. Özel eklentiler

Tekil bir nesne belirteci kullanılarak (Object ID) istenen bilgiler sertifika içindeki özel alanlara yazılabilir. Bu bilgilerin yorumlanması sertifikayı kullanan uygulamaya (yazılım veya donanıma) göre değişir. Bu eklentilerin kullanımını düzenleyen uluslararası bir standart yoktur.

6.7.9. SM sertifikalarındaki eklentiler

Bu eklentiler yalnızca SM sertifikalarına konup kullanıcı sertifikalarına konmazlar.

Temel Kısıtlamalar Eklentisi (Basic Constraints)

Bu eklenti kendi altında Özne Tipi ve Sertifika Yolu Kısıtlaması değerlerini tanımlar.

6.7.10. Özne tipi

Subject Type=CA : Bu sertifikanın bir SM sertifikası olduğunu belirtir.

6.7.11. Sertifika yolu kısıtlaması

Path Length Constraint= X

X aşağıdaki değerlerden birisi olabilir:

• None: Kısıtlama yok

• 0: Bu SM altına SM tanımlayamaz ya da çapraz sertifikasyon yapamaz.

• 1, 2, 3..: Bu SM altına en fazla 1, 2, 3 SM tanımlayabilir ya da en fazla 1, 2, 3 çapraz sertifikasyonu kabul edebilir.

6.7.12. Politika nesne belirteci eklentisi (Policy Object Id)

Her SM kendine ait, tüm dünyada tekil olacak bir Nesne Belirteci (Object Id) satın alır. Bu nesne belirteci uluslararası standartlara uygun olarak alınır, örneğin ISO veya yerel temsilcisi olan TSE aracılığıyla.

6.7.13. Politika eşleştirme eklentisi

Çapraz sertifikasyonda kullanılır.

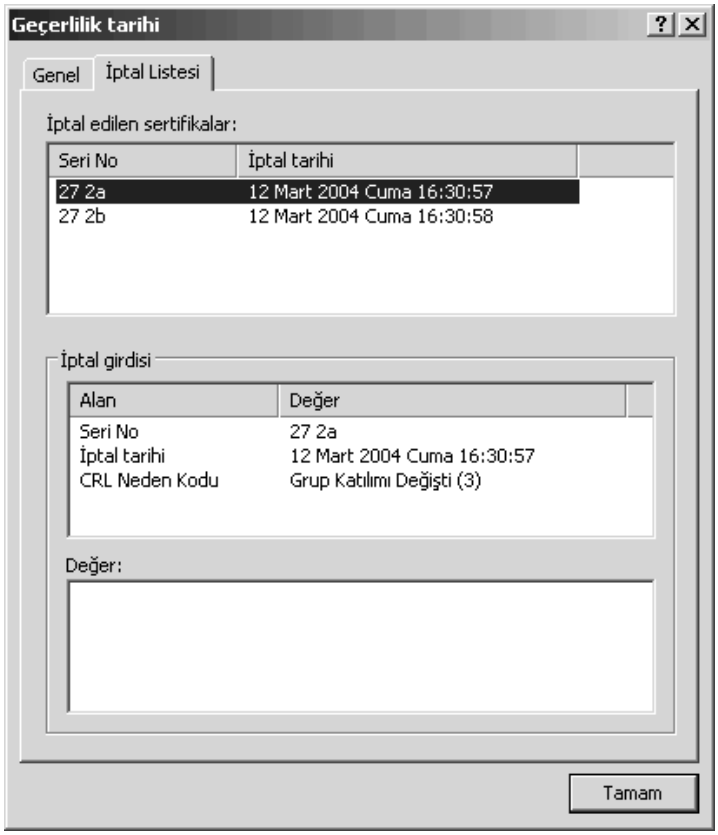
6.7.14. X.509 sertifika iptal listesi

CRL (Certificate Revocation List) ya da SİL (Sertifika İptal Listesi) geçerliliği bitmediği halde kullanılması istenmeyen sertifikaların seri numaralarının tutulduğu SM tarafından imzalanmış bir yapıdır.

SİL dizinde ve/veya bir web sunucuda kullanıcıların ulaşabileceği bir yerde tutulur ve belli aralıklarla geçerlilik periyodu yenilenir.

AAA sisteminde, sertifika tabanlı işlem yapan (kimlik doğrulama, elektronik imza doğrulama vb) her türlü yazılım ve donanım kullanacağı sertifikaların geçerliliğini kontrol ederken güncel bir sertifika iptal listesine bakmak zorundadır. Eğer işlemde kullanılacak bir sertifikanın seri numarası SİL içinde bulunursa o sertifika geçersiz kabul edilir.

Şekil 6.5'te Windows işletim sistemlerinde bir sertifika iptal listesi gösterilmiştir.



Şekil 6.5. Windows İşletim Sisteminde Bir Sertifika İptal Listesi

6.8. Sertifika İptal Nedenleri

Bir sertifika aşağıdaki nedenlerle SİL içinde yer alabilir:

• Sertifikaya ait anahtarın kaybedilmesi veya çalınması

• Sertifika politikalarının değişmesi

• Sertifikasyon Makamı'nın anahtarının çalınması

• Sertifikasyon Makamı'nın iptal edilmesi

• Kullanıcının kendi isteği ile sertifikasını iptal ettirmesi (örneğin başka bir SM altında tanımlanmak istenmesi)

• Kullanıcı bilgilerinin (ad, soyad, email adresi gibi) 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)

• Görev Değişikliği (Affiliation Changed)

• Görev devri (Superseded)

• SM'nin faaliyetini sona erdirmesi (Cessation of Operation)

• Askıya alma (certificateHold)

• SİL'den çıkarma (removeFromCRL)

• Yetkinin elinden alınması (privilegeWithdrawn)

• Üst SM'nin anahtarının çalınması (aACompromise)

6.9. OCSP (Online Certificate Status Protocol)

OCSP, SİL'nin sayısal sertifikalar hakkında sağladığı durum bilgisiyle karşılaştırıldığında sadece daha güncel durum bilgisi sağlamakla kalmaz aynı zamanda sertifika durumu hakkında ek bilgilerin de elde edilebilmesini sağlar. OCSP protokolüne göre OCSP istemcisi, OCSP sunucusuna bir sertifikaya ilişkin durum istek bilgisi gönderir, OCSP sunucusu ise istemciye söz konusu sertifikayla ilgili durum bilgisini cevap olarak gönderir.

Günümüzde bilgi sitemlerindeki güvenliği arttırmak üzere büyük güvenlik altyapıları kurulmaktadır. Bilgisayar dünyasında güvenliğin tanımı yapılırken

genellikle güvenlik ihtiyaçları göz önüne alınmaktadır. Bu ihtiyaçlar, gizlilik, bütünlük, doğruluk ve inkar edemezlik olarak sıralanabilir. Söz konusu ihtiyaçlar karşılanırken de şifreler, sayısal imzalar gibi kriptolojik teknikler kullanılmaktadır. Güvenlik hizmetlerinin sağlanmasında varlıklara ait anahtarların (genellikle açık anahtar) ve kimlik bilgilerinin bu hizmeti alacak varlıklar arasında paylaşılması gerekmektedir. Sayısal sertifikalar, bahsedilen türden bir paylaşımı sağlayabilecek en ideal araçlar olarak görülmektedir. Çok sayıda varlık barındıran birbirine bağlı açık sistemlerde, varlıklar arasındaki güven ilişkisinin kurulmasında sertifikalar büyük önem taşımaktadır.

Sertifikalar, sertifika makamı (SM) olarak adlandırılan güvenilir otoriteler tarafında üretilir ve dağıtılır. Sertifikalara ait geçerlilik periyodu SM'nin güvenlik politikasıyla belirlenir ve bu periyot boyunca sertifikanın geçerliliği garanti edilebilir.

SM bazı durumlarda bir sertifikayı geçerlilik süresi içinde iptal edebilir. Sistemdeki tüm varlıkların bu iptal durumundan haberdar olabilmesi için SM'nin bunu bir güvenlik politikasıyla belirlemesi gerekir. Sertifika durum yönetimi için günümüzde birçok model önerilmiştir .

6.10. Sertifika Durum Yönetimi Metotları

Sertifika durum yönetimi çevrimiçi veya çevrim dışı olarak yapılabilir. Bazen her iki metodun birlikte kullanıldığı durumlarla da karşılaşılabilir. Çevrimiçi durumda, sertifikalara ait geçerlilik bilgisi SM tarafından önceden oluşturulur ve sistemde yer alan kullanıcıların erişebileceği ortak bir alana yerleştirilir. Çevrimiçi durumda ise, geçerlilik durumu sorgulanan sertifikaya ait durum bilgisi çevrimiçi olarak çalışan güvenilir bir otorite tarafından güncellenir. SİL yöntemi çevrimdışı, OCSP ise çevrimiçi sertifika durum yönetimi metotlarına örnek verilebilir.

Sertifikalar birçok farklı nedenden ötürü iptal edilebilir. Bu nedenlerden başlıcalarına bakılacak olursa,

- Kullanıcının veya Sertifika makamının özel anahtarı çalınmış olabilir.
- Sertifikanın verdiği bilgilerden bir veya bir kısmı değişmiş olabilir

- Sertifikanın imzalanmasında kullanılan imzalama algoritması kırılmış olabilir
- Sertifikanın yer aldığı sertifika zincirindeki başka bir sertifika iptal edilmiş olabilir .

6.11. Sertifika İptal Listesi (SİL)

Sertifika İptal Listeleri, X.509 tipindeki sertifikalarla birlikte ilk olarak 1988'de ITU-T tarafından ortaya atılmıştır. 1993 yılında ise ikinci sürümüne erişmiştir. SİL'ler, iptal edilmiş sertifikaların listesini taşır ve çevrimdışı olarak belirli periyotlarla üretilir. Bir SİL iptal edilmiş sertifikalara ait seri numaralarını, iptal tarihlerini, ve kendi oluşturulma ve bir sonraki güncelleme tarihlerini içerir. İsteğe bağlı olarak, sertifikaların iptal nedenlerini de içerebilir. SİL yayınlayıcısı tarafından sayısal olarak imzalanır, böylece SİL listesinin geçerliliği de kontrol edilebilir. Herhangi bir sertifikanın geçerliliği kontrol edilirken, söz konusu sertifikayı yayınlayan SM'nin yayınladığı SİL'in imzası kontrol edilir, eğer imza doğruysa sorgulanan sertifikanın SİL'de yer alıp almadığı kontrol edilir. Eğer sertifikaya ait seri numarası SİL içinde bulunamazsa söz konusu sertifika geçerli kabul edilir, aksi durumda sertifika geçersizdir.

6.12. Çevrimiçi Sertifika Durum Protokolü (OCSP)

OCSP, bir sertifikaya ait güncel iptal bilgisinin çevrimiçi elde edilmesini sağlayan bir protokoldür. X.509 sertifikaları için tasarlanmış olmasına rağmen farklı tipteki sertifikalarla da çalışabilir. OCSP, SİL yönteminin yerine veya bu yöntemle birlikte kullanılabilir, böylece sorgulanan sertifikaya ait en güncel durum bilgisi elde edilebilir.

OCSP istemcisi bir sayısal sertifikanın kontrolü sırasında, OCSP sunucusuna bir geçerlilik durum sorgusu içeren isteği gönderir ve söz konusu sertifikayla herhangi bir işlem yapmadan önce OCSP sunucusundan gelecek olan geçerlilik durum bilgisini bekler. OCSP isteği içinde bulunan alanlar ;

- Protokol sürüm bilgisi
- Hizmet isteği (Hizmeti almak isteyen)
- Sorgulan sertifikaya ait ayırt edici bir özellik (Yayıncı-Seri No, veya Açık Anahtarın Özeti vb...)
- OCSP Sunucusu tarafından işlenebilecek eklentiler

İstek mesajının sunucuya ulaşmasından sonra OCSP sunucusu,

- Mesaj biçiminin düzgün olup olmadığını kontrol eder
- İstenilen hizmeti sağlar (Sorgulanan sertifika(lar) hakkında geçerlilik durum bilgisi oluşturur)
- OCSP istemcisine sertifika durum bilgisini içeren bir cevap gönderir. Aksi durumda hata mesajı üretir.

OCSP yanıtları farklı tiplerde olabilir. Bir OCSP yanıtı, yanıt tipi ve yanıt sekizlilerinden (octet) oluşur. Tüm OCSP istemci ve sunucularının desteklemesi beklenen bir OCSP yanıtı bulunmaktadır. Bu bildiride tüm OCSP istemci ve sunucuların desteklemesi beklenen bu yanıt üzerinde durulacaktır. Tüm "anlamlı" OCSP yanıtları elektronik olarak imzalanmalıdır. Yanıtın imzalanmasında kullanılan özel anahtar aşağıdakilerden birine ait olabilir,

- Geçerliliği sorgulanan sertifikayı veren Sertifika Makamı
- İstemci tarafından açık anahtarına güvenilen bir OCSP sunucusu
- Sertifika Makamı tarafından verilen ve söz konusu Sertifika Makamına ait sertifikaların geçerliliği hakkında sorgulama yapılabilmesini sağlayan özel işaretli bir sertifikaya sahip olan Yetkili Sunucu

Anlamlı bir yanıt mesajı aşağıdaki bileşenleri içerir.

- Yanıtın sürümü
- Yanıt verenin adı
- İstek içinde yer alan tüm sertifikalar için ayrı ayrı yanıt bilgileri
- Seçime bağlı eklentiler
- İmzalama algoritması OID'i (Object Identifier)
- Yanıtın özetinden hesaplanan imza değeri

- İstek içinde yer alan tüm sertifikaların yanıtlarının her birinde ise,
- Sorgulanan sertifikaya ait ayırt edici bir özellik (Yayıncı-Seri No, veya Açık Anahtarın Özeti vb...)
- Sertifika durum bilgisi
- Yanıtın geçerli olduğu zaman dilimi
- Seçime bağlı eklentiler yer alır.

"Anlamlı" sertifika durum bilgisi aşağıdakilerden biri olabilir,

- İyi
- İptal edilmiş
- Bilinmeyen

"İyi" durumu, sertifika geçerlilik sorgulamasına verilen olumlu bir yanıttır. En azından, sertifikanın iptal edilmiş sertifikalar arasında yer almadığını belirtir. Fakat "iyi" durumu, sertifikanın daha önce yayınlandığı veya cevabın söz konusu sertifikanın geçerlilik süresi içinde üretildiği anlamına gelmez. "İptal edilmiş" durumu, sertifikanın iptal edilmiş (sürekli veya geçici) olduğunu belirtir. "Bilinmeyen" durumu ise, OCSP sunucusunun geçerliliği sorgulanan sertifika hakkında bilgiye sahip olmadığını gösterir. OCSP yanıtı, OCSP sunucusu tarafından sayısal olarak imzalanır. Herhangi bir hata durumunda OCSP yanıtı bir hata mesajı içerir. Hata içeren OCSP yanıt mesajları sayısal olarak imzalanmaz. Hata mesajları aşağıdakilerden biri olabilir.

- İstek biçimi doğru değil
- İç hata
- Daha sonra yeniden dene
- İmza gerekli
- Yetkisiz sorgu

OCSP sunucusu, istemciden gelen istek mesajı OCSP istek yapısına uymuyorsa "istek biçimi doğru değil" yanıtını üretir.

"İç hata" yanıtı OCSP sunucusunun tutarsız bir duruma geldiğini belirtir. İstek başka bir OCSP sunucusuna gönderilebilir.

“Daha sonra yeniden dene” yanıtı OCSP sunucusunun, gelen isteğe şu an için yanıt veremediğini gösterir.

“İmza gerekli” yanıtı OCSP sunucusu tarafından üretilir ve istemciye isteği imzalayarak göndermesini belirtmek amacıyla oluşturulur.

OCSP sunucusu tarafından gönderilen “Yetkisiz sorgu” yanıtı ise, istemcinin söz konusu sorgulamayı yapma yetkisinin olmadığı durumları ifade eder.

OCSP kullanıcıya daha güvenli ve kapsamlı bilgi sunabilmek için istek ve yanıt yapılarında eklentiler (extensions) kullanılmasını desteklemektedir.

OCSP, günümüzde birçok ticari örneklerini görebileceğimiz bir protokoldür. Bu örnekler genellikle HTTP protokolü üzerinde gerçeklenmiştir ve internet üzerinden sorgulanabilmektedirler. Internet gibi dışarıya açık bir sistem içerisinde ticari bir OCSP gerçeklemesine sahip olmak beraberinde dikkat edilmesi gereken güvenlik sorunları getirmektedir. “İyi” durumu barındıran ve imzalı bir OCSP yanıtı, istemci ile sunucu arasında başka bir bilgisayar tarafından yakalanır ve saklanırsa, geçerliliği sorgulanan sertifikanın herhangi bir sebepten iptal edilmesinden sonra istemci söz konusu sertifikayı tekrar sorguladığında bu ara bilgisayar tarafından istemciye daha önceden saklanmış olan “iyi” yanıtının döndürülmesi bu duruma örnek olarak verilebilir. OCSP, nonce kullanarak bu güvenlik açığının üstesinden gelebilir. Nonce, bir istek ve yanıtı kriptografik olarak örtüştüren rasgele üretilen büyük bir sayıdır. OCSP istemcisi, oluşturduğu istek içerisine kendi oluşturduğu bir nonce değerini yerleştirir ve OCSP sunucusuna gönderir. Sunucu ise cevap oluştururken istemciden gelen nonce değerini alıp OCSP yanıtının içine yerleştirir. Böylece istemci-sunucu arasına üçüncü bir varlığın girip istemciye yanıltıcı yanıtlar göndermesi engellenmiş olur. Bunun yanısıra TLS/SSL veya başka alt düzeyli protokoller kullanılarak HTTP üzerindeki OCSP gerçeklemelerinin güvenliği sağlanabilir.

6.13. SİL ve OCSP Karşılaştırması

Sertifikaların doğrulanmasında SİL yöntemi yerine OCSP kullanılması aşağıdaki nedenlerden dolayı tercih edilebilir.

- OCSP sertifikaların iptal durumları hakkında daha güncel bilgi sağlar.

- İstemcilerin SİL'leri kendi yerel depolarına çekmelerine gerek kalmaz. Bu durum daha düşük ağ trafiğine neden olarak bant genişliği kullanımını azaltır
- OCSP kullanıldığında istemciler, SİL'leri incelemek zorunda kalmaz, istemci tarafındaki işlem yükü azalır.
- SİL'ler iptal edilmiş sertifikaları gereksiz şekilde afişe ederler. (Bu durum bir kredi kartı şirketinin yayınladığı kötü müşteri listesine benzetilebilir)

Öte yandan OCSP'nin SİL'e göre dezavantajı olarak, OCSP sunucusunun kimlik kanıtlamak için ürettiği tüm OCSP yanıtlarını imzalaması örnek verilebilir. Bu da OCSP sunucusundaki işlem yükünü arttıran ve OCSP'nin ölçeklenebilirliğini sınırlayan bir durum olarak ortaya çıkmaktadır.

6.14. Nitelikli Sertifika

Nitelikli Sertifika (Qualified Certificate), X.509 Sertifikası baz alınarak hazırlanan ve sadece gerçek kişilere verilen bir sertifika çeşididir. Bu sertifika tipi RFC 3739'da tanımlanmıştır. Nitelikli sertifikalar Türkiye'de ve birçok Avrupa ülkesinde elle atılan ıslak imzaya eşdeğer elektronik imzalar atmak için kullanılır. Bu sertifikaları standart X.509 sertifikasından farklı kılan en önemli özellik üretiminde ve sahibine verilmesinde çok sıkı kimlik doğrulama kuralları uygulanması ve sertifika merkezlerinin işletiminin denetlenmesi olarak sayılabilir.

Nitelikli sertifikalar Türkiye'de, 5070 Sayılı Elektronik İmza Kanununda (Kanun) tarif edilmiştir. Kanunda görevlendirilen Telekomünikasyon Kurumu tarafından hazırlanan Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik (Yönetmelik) ve Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ (Tebliğ) ile Elektronik Sertifika Hizmet Sağlayıcıları (ESHS) ve onların üreteceği nitelikli elektronik sertifikalar konusunda düzenlemeler yapılmıştır.

Nitelikli sertifika alanları ile ilgili önemli bilgiler aşağıda verilmiştir:

Yayınlayıcı adı (Issuer Name) aşağıdakilerin bir alt kümesidir:

domainComponent, countryName, stateOrProvinceName, organizationName, localityName, serialNumber.

Kullanıcı adı(Subject Name) aşağıdakilerin bir alt kümesidir:

countryName, commonName, surname, givenName, pseudonym, serialNumber, organizationName, organizationalUnitName, stateOrProvinceName ,localityName, postalAddress.

X.509 'da olmayan ya da var olanları genişleten eklentiler

Kullanıcı Dizin Özellikleri (Subject Directory Attributes)

title, dateOfBirth, placeOfBirth, gender, countryOfCitizenship, countryOfResidence.

Biyometrik Bilgi (Biometric Information)

Elle atılan imza, resim, parmak izi gibi bilgilerin özeti sertifikada, kendisi ulaşılabilen bir sunucuda bulunur. Bu bilgilerin yorumlanmasının insanlara bırakılması tavsiye edilmiştir.

6.15. Görev Sertifikası

Görev Sertifikası (Attribute Certificate), açık anahtarın bulunduğu sertifikaya bağımlı ek bir sertifikadır. Bu sertifikanın başlıca özellikleri şöyledir:

• Ömrü genellikle daha kısa, sık sık yenilenebilir

• Açık anahtar sertifikası kişi bazlı tanımlama yaparken, görev sertifikası bu kişinin hangi gruba ya da role dahil olduğunu belirtir. Böylece kişi o grubun ya da rolün haklarına sahip olur.

• Görev sertifikası yayınlayan makamın açık anahtar yayınlayan makamdan ayrı olması zorunludur ve bu makam kendi başına güvenilmek zorundadır. Bu makam açık anahtar sertifikası yayınlamaz.

6.16. Çapraz Sertifikasyon

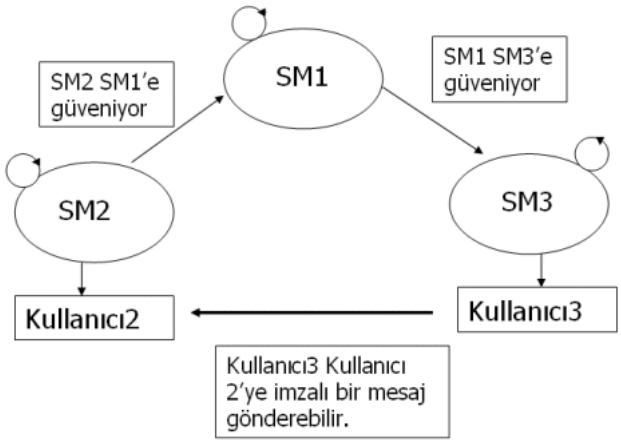
Kendi kendine imzalanmış (Self Signed) sertifika yayınlayabilen yani güvenilir nokta olan bir sertifikasyon makamının (otonom SM'nin) –ki bu kesin

hiyerarşide kök sertifikasyon makamıdır- diğer otonom SM'lerle karşılıklı veya tek taraflı olarak açık anahtarları sertifikalandırmasıdır.

Çapraz sertifikasyonda kullanılan eklentiler

- Policy Constraints
- Name Constraints
- Path Length Constraints

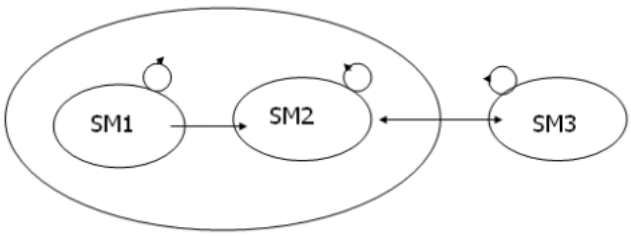
Şekil 6.6. ’da örnek bir çapraz sertifikasyon gösterilmiştir.



Şekil 6.6. Çapraz Sertifikasyon

6.17. Sertifika Yolu Kısıtlaması

SM1, SM2'ye "path length=0" olan bir sertifika vermişse SM3'e güvenmez. Şekil 6.7’de sertifikasyon yolu kısıtlaması gösterilmiştir.

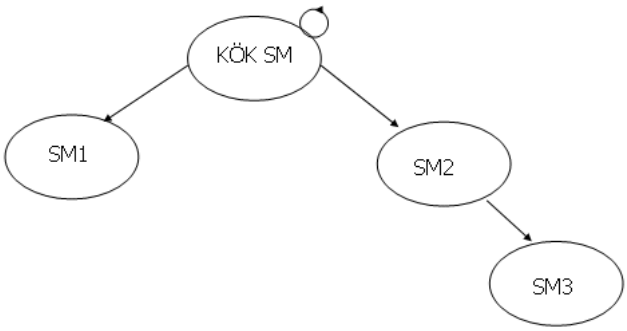


Şekil 6.7. Sertifika Yolu Kısıtlaması

6.18. Kesin Hiyerarşide Sertifika Yolu Kısıtlaması

KÖK SM, SM1'e path length=0 olan bir sertifika verdiği için SM1 altına SM tanımlayamaz.

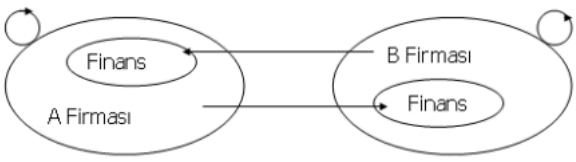
KÖK SM, SM2'ye path length=1 olan bir sertifika verdiği için SM2 altına yalınızca bir SM tanımlayabilir. Şekil 6.8' te kesin hiyerarşide sertifika yolu kısıtlaması gösterilmiştir.



Şekil 6.8. Kesin Hiyerarşide Sertifika Yolu Kısıtlaması.

6.19. İsim Kısıtlaması

İsim kısıtlaması sayesinde yalnızca A firmasında finans departmanıyla B firmasındaki finans departmanı imzalı haberleşebilir. Burada kısıtlama olarak departman adının "Finans" olması kullanılmaktadır. Şekil 6.9'ta isim kısıtlaması gösterilmiştir.

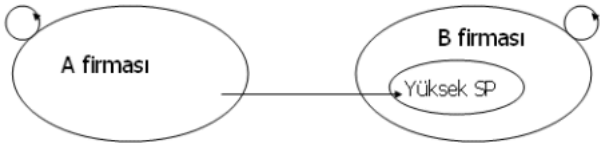


Şekil 6.9. İsim Kısıtlaması.

6.20. Politika Kısıtlaması

Her SM'nin kendine uygun sertifika politikaları vardır ancak genelde bunlar düşük, orta ve yüksek olarak sınıflandırılırlar. Farklı SM'lerin Sertifika Politikalarını(SP) eşlemek için politika eşleme (policy mapping) kullanılır.

Aşağıdaki örnekte A firması AAA, B firmasındaki AAA'nın yalnızca yüksek SP ile verilmiş olan sertifikalarına güveniyor. Şekil 6.10 'da politika kısıtlaması gösterilmiştir.



Şekil 6.10. Politika Kısıtlaması.

7. MİCROSOFT EXCHANGE, WİNDOWS 2003 CA SUNUCU VE OUTLOOK 2003 İLE DİJİTAL İMZALI VE ŞİFRELİ MESAJLAŞMA

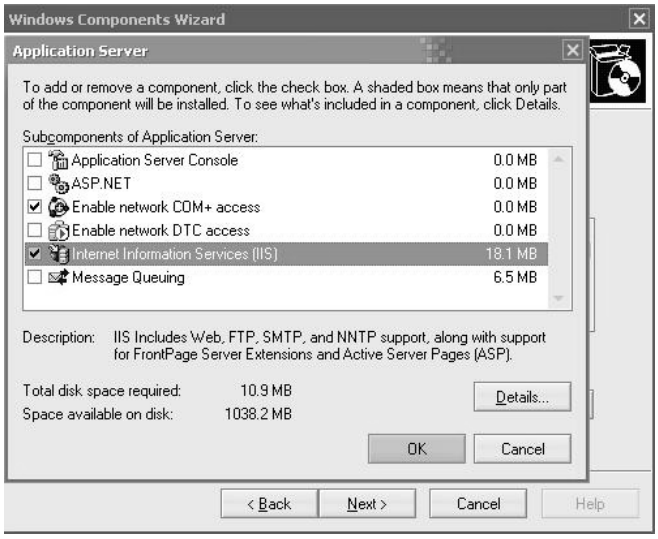
Microsoft Exchange Sunucu 2003 ile Windows 2003 Sertifika Sunucu kullanılarak dijital imza ve mesaj şifreleme özellikleri ile mesajların güvenli olarak gönderilmesi ve alınması mümkün olmaktadır.

Exchange 2003 ile mesajların güvenilir olarak iletilmesi için öncelikli olarak domain ortamında bir adet Sertifika Sunucu (CA) konumlandırmak gerekir.

7.1. IIS Servisinin Kurulması

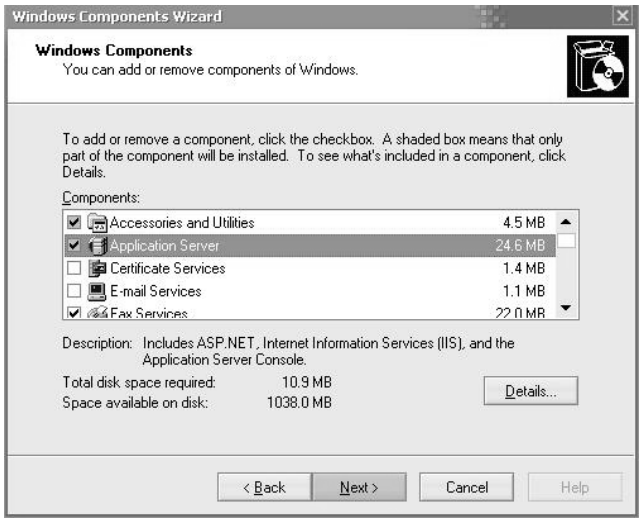
CA kurulumundan önce ilk yapılması gereken işlem Windows 2003 Sunucu olarak çalışan bir makina üzerinde IIS (Internet Information Services) kurulumunu yapmaktır. Bu sunucu Exchange sunucu olmak zorunda değildir. Domain denetleyici veya domain ortamında farklı bir sunucu üzerinde kurulabilir. Varsayılan olarak normal kurulumda IIS servisi Windows 2003 sunucuda otomatik olarak kurulmaz. IIS servisinin kurulumu için aşağıdaki adımlar izlenir.[20]

1. Start > Control Panel > Add or Remove Programs ‘a tıklanır.
2. Add or Remove Programs,’ ta Add/Remove Windows Components seçeneğine tıklanır.
3. Components seçeneğinin altında , Application Server tıklanır ve Details butonuna basılır.
4. Application Server penceresin de IIS seçilir ve OK ‘e tıklanır.



Şekil 7.1. IIS Kurulumu.[19]

5. Next butununa basılır.



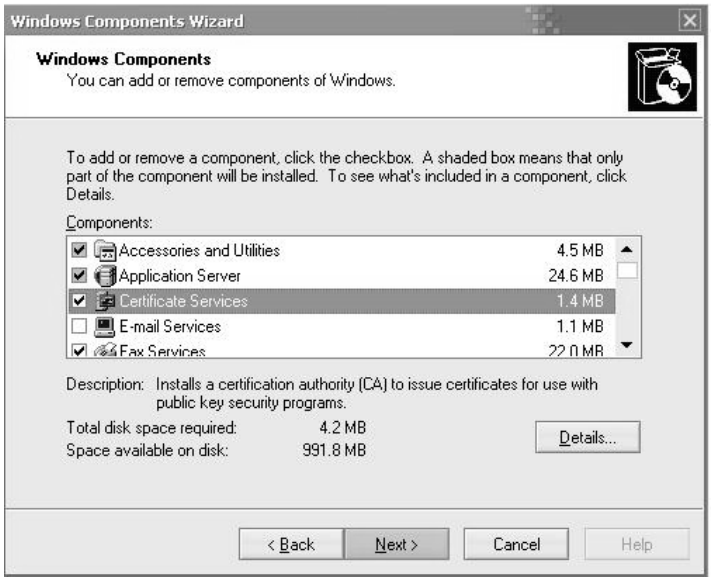
Şekil 7.2.IIS Kurulumu Devam. [19]

6. Sihirbaz kurulumu tamamlanınca Finish butonuna basılır.

7.2. CA Servisinin Kurulumu

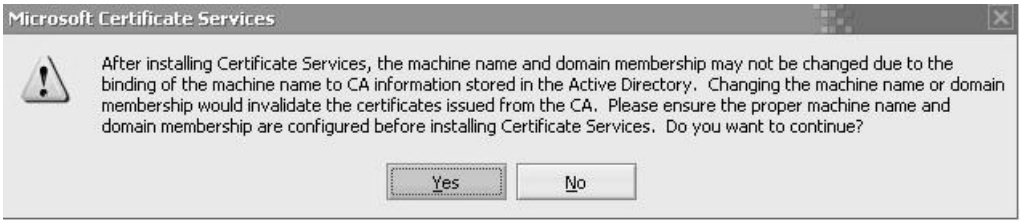
CA servisinin kurulumu için aşağıdaki adımlar izlenir.

1. Start > Control Panel > Add or Remove Programs seçeneğine tıklanır.
2. Add or Remove Programs ta Add/Remove Windows Components seçilir.
3. Components altında , Certificate Services seçilir.



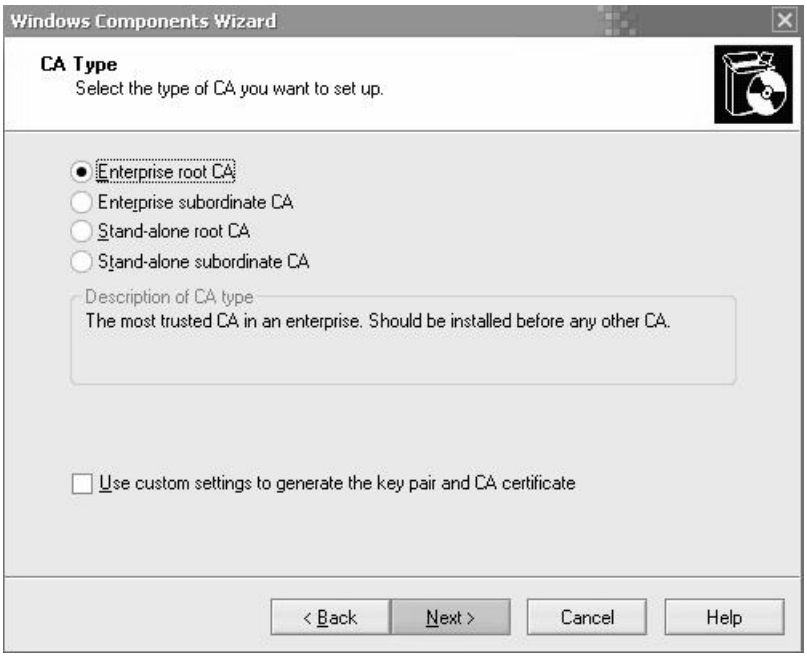
Şekil 7.3. Sertifika Servis Kurulumu. [19]

4. Bu adımda bir uyarı alınır ve YES butonuna tıklanır.



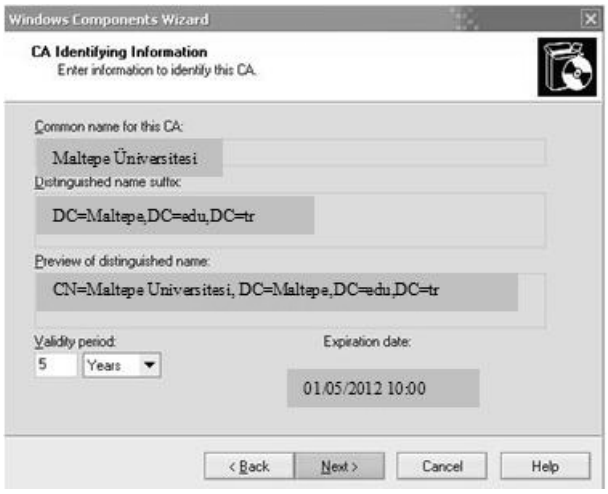
Şekil 7.4. Sertifika Servis Kurulurken Alınan Uyarı. [19]

5. CA türü seçim sayfasında, Enterprise root CA seçilir ve Next butonuna basılır.



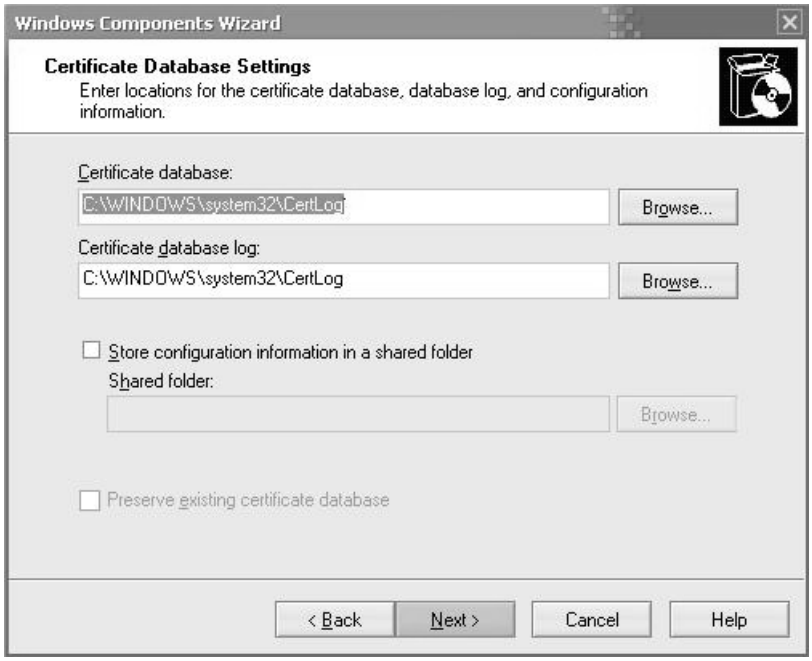
Şekil 7.5. Sertifika Sunucu Tipi Seçimi. [19]

6. CA Identifying Information sayfasında, Common name for this CA kutusunda , sunucunun ismi yazılır ve Next butonuna basılır.



Şekil 7.6. Sertifika Tanımlama Bilgisi. [19]

7. Certificate Database Settings sayfasında varsayılan ayarlamalar kabul edilip next butonuna basılır.



Şekil 7.7. Sertifika Veritabanı Ayarları. [19]

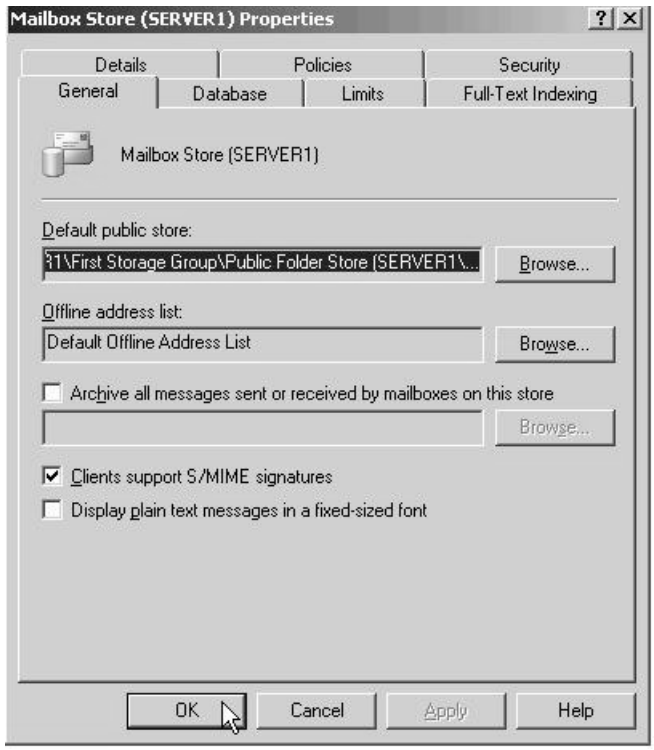
8. IIS servisinin durdurulacağına yönelik bir uyarı alınır ve YES butonuna basılır.
9. Active Server Pages (ASPs) aktif edilir .
10. Kurulum tamamlandığında Finish butonuna basılır.

7.3. Exchange sunucunun S/MIME mesajlarını desteklemesi için konfigüre edilmesi

Normal olarak Exchange 2003 sunucu S/MIME mesajlarını desteklemez. Desteklemesi için aşağıdaki tanımlamalar yapılır.

1. Exchange System Manager açılır.

2. Administrative Groups > First Administrative Group > Servers > *Your Server Name* (Maltepe Exchange) > First Storage Group > Mailbox Store (SERVER 1) üzerinde sağ tuşa basılır ve Properties seçilir.
3. Properties tabında , "*Clients support S/MIME signatures* "onay kutusu işaretlenir.



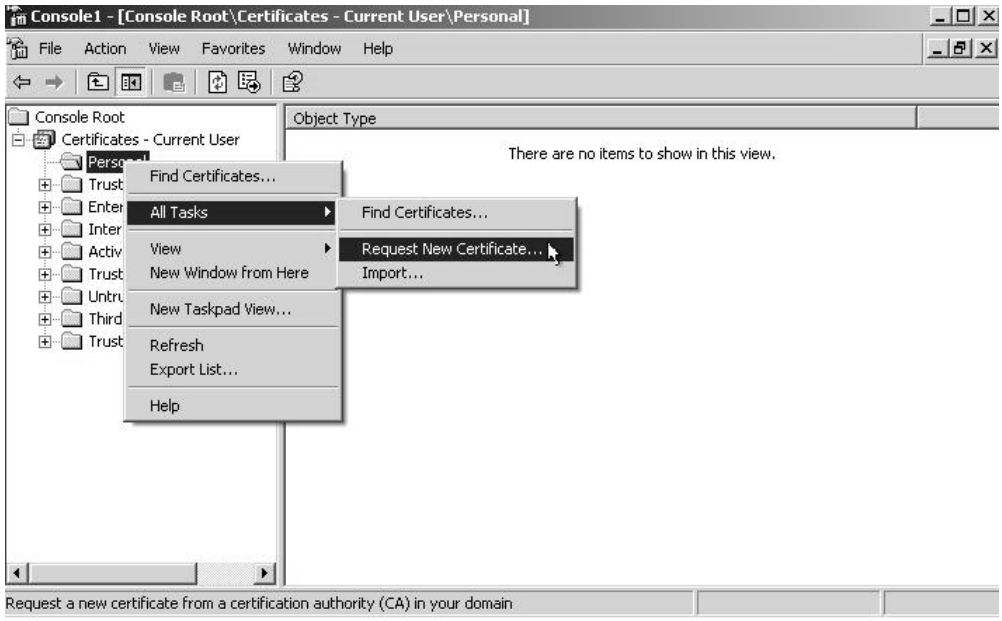
Şekil 7.8. Exchange Sunuucuda SMIME Aktivasyonu. [19]

7.4. CA den Dijital Kullanıcı Sertifikası Alma (MMC konsol kullanılarak)

MMC konsol kullanılarak dijital sertifika alabilmek için aşağıdaki adımlar izlenir.

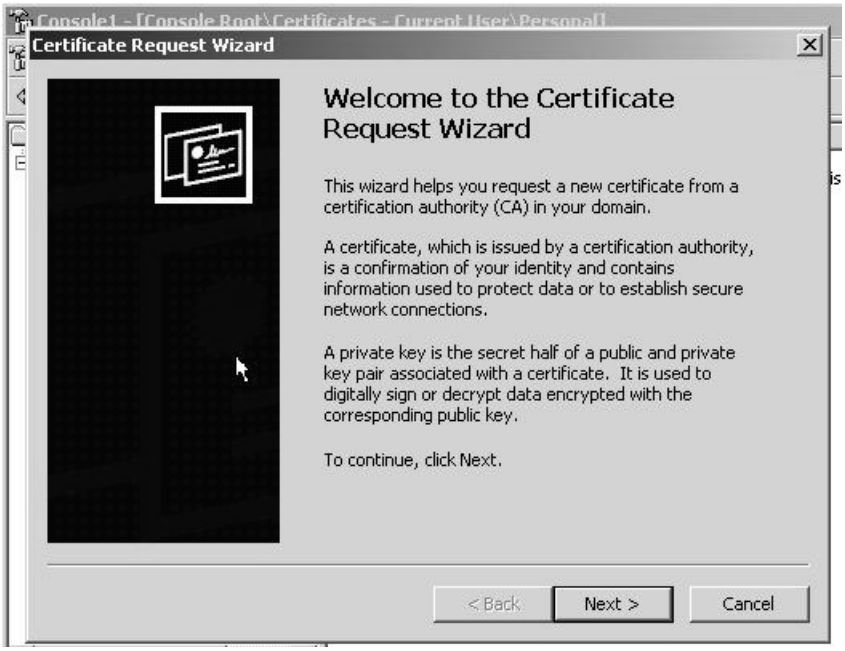
1. Start menu > Run > kutusuna MMC yazılır ve Enter 'a basılır.
2. MMC penceresinde, File mensüne tıklanır ve Add/Remove Snap-In seçilir.
3. Add/Remove Snap-In penceresinde Add butonuna basılır.
4. Var olan seçeneklerden Certificates seçilir.

5. Sertifikanın bir kullanıcı hesabına mı, bilgisayar hesabına mı veya bilgisayardaki bir servis hesabına mı ait olacağı seçilir. My User Account seçeneği ile bu sertifikanın bir kullanıcı sertifikası olduğu belirtilir ve ardından Finish butonuna basılır.
6. Certificates genişletilir. Current User > Personal.
7. Personal klasörü üzerinde sağ tuşa basılır. All Tasks > Request New Certificate seçilir.



Şekil 7.9. Sertifika İsteğinde Bulunma. [19]

8. Certificate Request sihirbazında Next butonuna basılır.

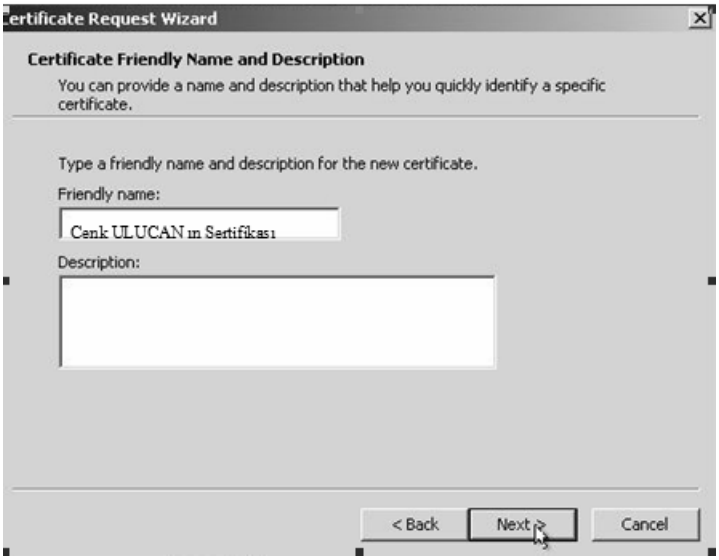


Şekil 7.10. Sertifika İsteği Sihrbazı. [19]

11. Certificates Type ta User seçilir.

Şekil 7.11. Sertifika Tipi Seçme. [19]

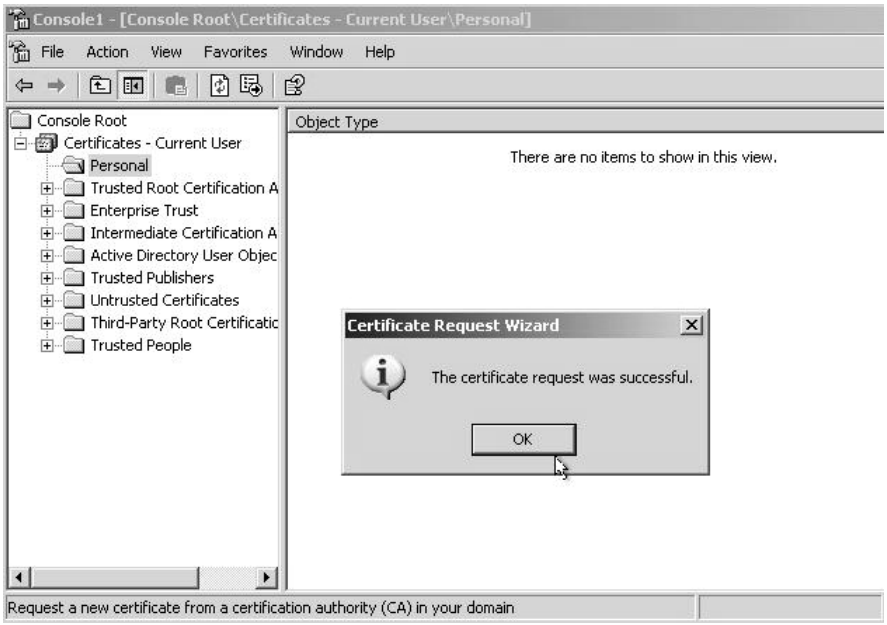
12. Friendly name kutusunda sertifika için bir isim yazılır. Örneğin Cenk Ulucan ın Sertifikası gibi. Ardından Next butonuna basılır.



Şekil 7.12. Sertifika İsim ve Tanımlama. [19]

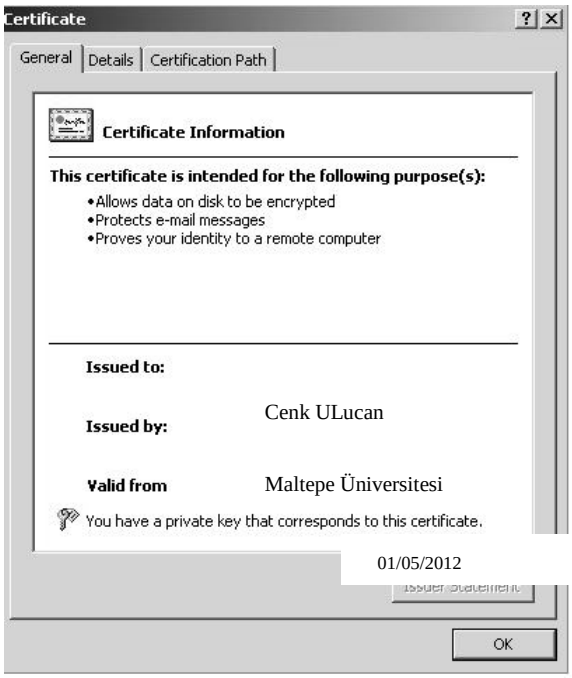
13. En son sayfada Finish butonuna basılır.

Şekil 7.13. Sertifika İsteği Sihirbazı Sonlandırma. [19]



Şekil 7.14. Sertifika İsteğinin Başarılı Olduğunu Gösteren Konsol. [19]

14. Artık yeni bir dijital sertifikaya sahip olunmuştur. Bu sertifikayı görebilmek için Certificates - Current User > Personal > Certificates klasörüne tıklanır. Şekil 7.15 te tanımlanan bir sertifika örneği gösterilmiştir.

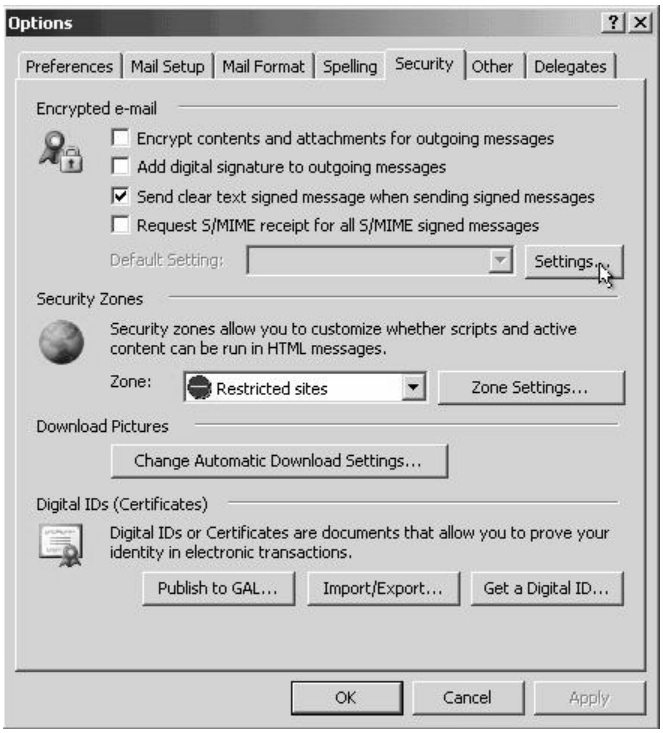


Şekil 7.15. Tanımlanan Sertifika. [19]

7.5. Outlook 2003 ‘ün Konfigüre Edilmesi

Outlook 2003, hem mesajları şifreleme hem de imzalama için ayrı ayrı konfigüre edilebilir. Bunlar için aşağıdaki işlemler takip edilir.

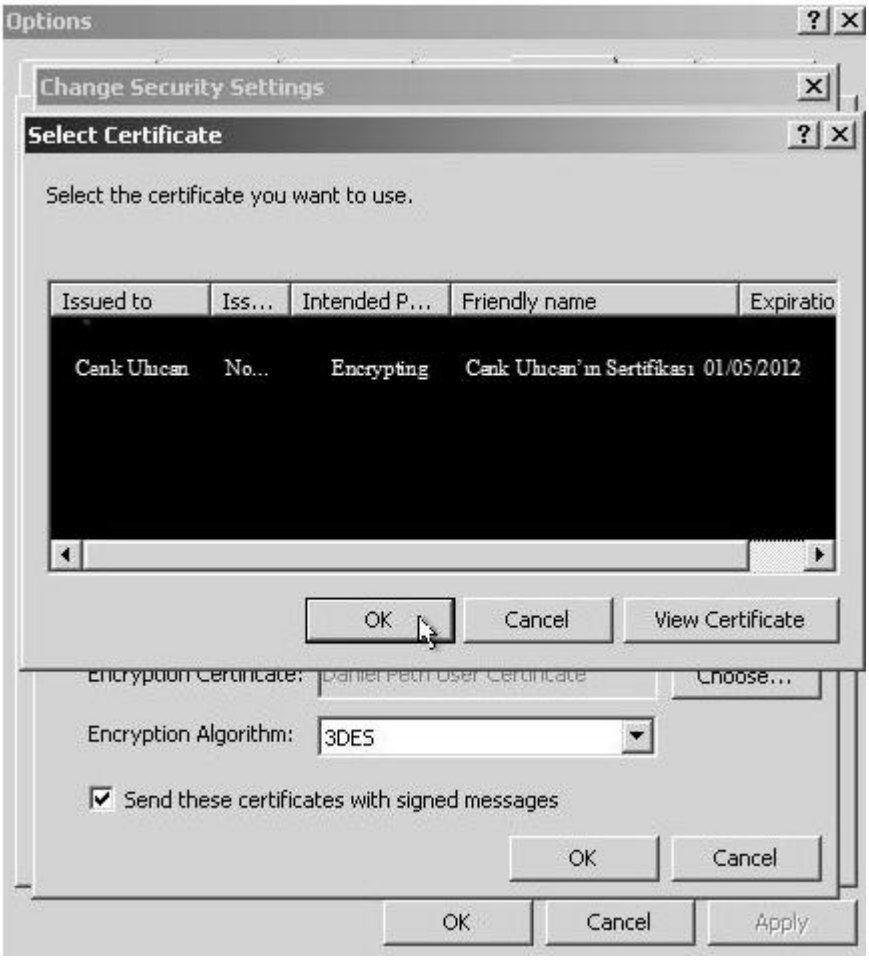
1. Outlook açılır.
2. Tools > Options > Security tabına tıklanır.
3. Encrypted E-Mail kısmında Settings butonuna basılır. Şekil 7.16’da ve Şekil 7.17’de Outlook ayarlamalarının nasıl yapılacağı gösterilmiştir.



Şekil 7.16. Outlook Ayarlamalarının Yapılması.[19]

Şekil 7.17. Kriptoloji Formatı Olarak SMIME Seçilmesi. [19]

4. Cryptography Format olarak S/MIME seçilir.
5. Certificates and Algorithms kısmında, Signing Certificate kısmının altında kendimize ait sertifikanın seçildiğinden emin olmamız gerekir. Aksi takdirde yandaki seçenekten ilgili sertifika seçilir.



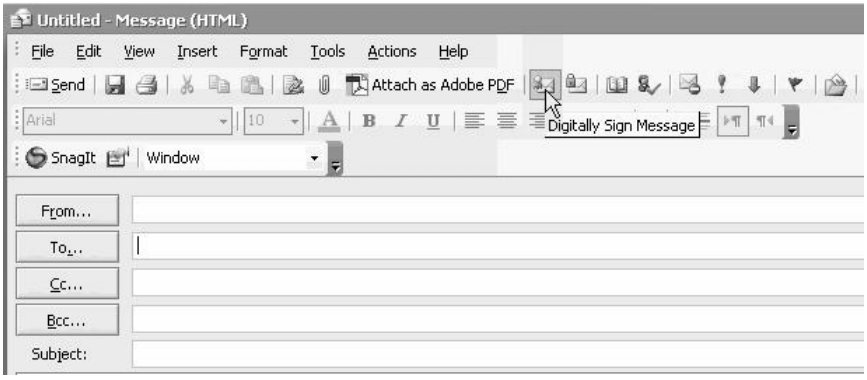
Şekil 7.18. Sertifika Seçimi. [19]

6. Encryption Certificate kısmında , Encryption Certificate altında daha önceden ilişkilendirilmiş dijital sertifikanın listelendiğinden emin olunması gerekir.
7. Gönderilecek mesajlar veya gelmiş olan her mesaja cevap verilirken Public Key kullanılacak olursa "Send these certificates with signed messages" onay kutusu seçilmelidir.
8. Ardından iki kez OK butonuna basılır.

7.6. Dijital İmzalı Mesajlar

Dijital imzalı mesaj özelliğini kullanabilmek için herhangi bir özel tanımlamaya gerek yoktur. Yapılması gereken tek şey mesaj yazıldıktan sonra

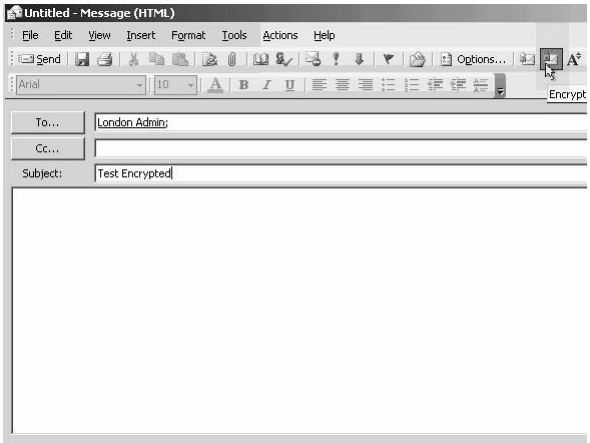
"Add a Digital Signature to this message" ikonuna tıklayıp Gönder butonuna basmaktır. Şekil 7.19 ‘da dijital imzalı mesaj göndermenin nasıl yapılacağı gösterilmiştir.



Şekil 7.19. Dijital İmzalı Mesaj Gönderme. [19]

7.7. Dijital Şifreli Mesajlar.

Dijital şifreli mesaj kullanabilmek için alıcının Public Key’ine ihtiyaç duyulur. Mesaj yazılır ve ardından "Encrypt message content and attachment" ikonuna basılır ve Gönder butonuna basılır. Şekil 7.20’de şifreli mesaj gönderme örneği gösterilmiştir.



Şekil 7.20. Şifreli Mesaj Gönderme. [19]

8. SONUÇLAR

Dünyadaki ve ülkemizdeki mevcut e-imza projeleri, 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.

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.

Bu tez çalışması ile, e-imza ile güvenli bir mesajlaşma ortamının nasıl oluşturulması gerektiği konusunda var olan bilgi birikimlerine katkı sağlanmış, 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 problemlerin de bu çalışma, kurumsal ağlarda e-imza sistemlerinin hayata geçirilmesinde örnek olma özelliği taşıması nedeniyle bu alandaki diğer çalışmalardan farklılık göstermektedir.

KAYNAKLAR

1. Diffie W. ve Hellman M. E. , "New directions in cryptography," IEEE Transactions on Information Theory,vol. 22, pp. 644-654, Kasım 1976
2. Rivest R. , Shamir A. ve Adleman L., "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Communications of the ACM, vol. 21, no.2, pp. 120-126, Subat 1978
3. Levi A. , ve Koc C. , "Risks in email security," Communications of the ACM, vol. 44 no. 8, pp.112, Agustos 2001
4. Ramsdell B. , S/MIME Version 3 Certificate Handling, RFC 2632, Haziran 1999
5. Nash A. , Duane W. , Joseph C. , Vrink D. , "PKI Implementing and Managing E Security", RSA Press, 2001
6. Adams C., Lloyd S. , Understanding PKI: Concepts, Standarts, and Deployment Considerations, 2nd Edition, Addison Wesley Professional, 2002
7. Gomez F., Martinez G., Canovas O., "New security services based on PKI", Future Generation Computer Systems 19 ,2003, page 251-262,2003
8. Brands S., Rethinking Public Key Infrastructures and Digital Certificates – Building in Privacy, The MIT Press, August 2000
9. Stallings W., Cryptography and Network Security, Second Edition, Prentice Hall 1988
10. Sağıroğlu Ş., Alkan M. , "Her Yönüyle Elektronik İmza", Grafiker Offset, 975-6355-23-9, Ankara 2005
11. Hunt R., "Technological infrastructure for PKI and digital certification", Computer Communications, 2001
12. Ellison C., Schneier B., "Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure", Computer Security Journal, XVI(1), 2000
13. Housley R., Polk T., "Planning for PKI: Best Practices Guide for Deploying Public Key Infrastructure", John Wiley & Sons Inc., USA, 2001
14. www.e-imza.gen.tr/index.php , Mart 2007
15. http://www.tk.gov.tr/eimza/eimza_mevzuat.htm , Ocak 2007
16. http://www.globalsign.com.tr , Aralık 2006

17. http://www.verisign.com , Aralık 2006
18. http://www.bilgitoplumu.gov.tr , Şubat 2007
19. http://www.petri.co.il/configure_message_security_in_exchange_2003.htm, Mart 2007
20. http://technet.microsoft.com/en-us/library/aa998500.aspx , Mart 2007
21. http://www.rsasecurity.com/rsalabs/ , Nisan 2007
22. http://inet-tr.org.tr/inetconf9/sunum/tip-bilisimi.pdf , Mart 2007
23. http://www.e-guven.com , Mayıs 2007
24. http://www.tubitak.gov.tr, Mart 2007
25. http://www.schneier.com/paper-pki.pdf, Mayıs 2007
26. M. Rhee, Internet Security Cryptographic Principles, Algorithms and Protocols, School of Electrical and Computer Engineering, Seoul National University, Republic of Korea, 2003
27. M. Alkan, Elektronik İmza Teknolojisi, Şifreleme ve Güvenlik Mekanizmaları, Akademik Bilişim Karadeniz Teknik Üniversitesi, Şubat 2004
28. Y. Samasti "e-imza e- dönüşümün anahtarı" CRMpro Dergisi, Ekim 2005, www.crmpro.com.tr
29. F. Topcan, PKI'da Kullanılan standartlar, TK Eğitimi, TÜBİTAK BİLTEN, ODTÜ, Ankara, 5 Nisan 2004.
30. T. Tüfekçi, Açık Anahtarlı Yapılar, TK Eğitimi, TÜBİTAK BİLTEN, ODTÜ, Ankara, 5 Nisan 2004.
31. Ö. Serhat, Bilgi Güvenliği, e-imza&e-Türkiye Sempozyumu, Ankara, 2004.
32. T. Gökhun, Bilgi Güvenliği Yönetimi ve Standartlar, Bilgi Güvenliği 2004, TSE Konferans Salonu, 18 Şubat 2004.

ÖZGEÇMİŞ

Cenk ULUCAN, 16 Mayıs 1977 yılında İzmir'de doğdu. Lise öğrenimini İzmir Buca Teknik Lisesi'nde tamamladıktan sonra 1995 yılında Marmara Üniversitesi Elektronik ve Bilgisayar Eğitimi Bölümü'nü kazandı. Bu bölümden 2000 yılında mezun oldu. 2000 yılı Mart ayında Siemens Sanayi ve Ticareti A.Ş. de Uzman Sistem Yöneticisi olarak çalışmaya başladı. 2004 yılında Maltepe Üniversitesi Fen Bilimleri Enstitüsü'nde Bilgisayar Mühendisliği Anabilim Dalı'nda yüksek lisans çalışmalarına başladı. 2007 yılında yüksek lisansı başarıyla tamamladı. **Cenk ULUCAN,** 2006 yılından beri Proje Müdürü olarak Siemens Sanayi ve Ticareti A.Ş.'de görevine devam etmektedir.