PAMUKKALE ÜNİVERSİTESİ MÜHENDİSLİK FAKÜLTESİ
PAMUKKALE UNIVERSITY ENGINEERING FACULTY
MÜHENDİSLİK BİLİMLERİ DERGİSİ
JOURNAL OF ENGINEERING SCIENCES
YIL : 2008
CİLT : 14
SAYI : 1
SAYFA : 31-40

BİLGİSAYAR AĞLARINDA GÜVENLİ MESAJLAŞMA İÇİN AKILLI KART DESTEKLİ BİR SİSTEM MİMARİSİ

Geylani KARDAŞ*, Ebru ÇELİKEL, Ayşegül ALAYBEYOĞLU*****
*Ege Üniversitesi, Uluslararası Bilgisayar Enstitüsü, 35100/Bornova/İzmir/Türkiye
**University of Texas at Dallas, Erik Jonsson School of Engineering and Computer Science, TX, ABD
***Ege Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, 35100/Bornova/İzmir

Geliş Tarihi : 16.04.2007

ÖZET

Bu çalışmada, bilgisayar ağlarında güvenli mesaj alışverişi için akıllı kart olanaklarından yararlanan taşınabilir bir sistem mimarisi tanıtılmaktadır. Akıllı kartların sistem mimarisi bünyesinde yer alması mesaj alışverişlerinde kimlik denetimi ve mahremiyet gibi başlıca iki önemli güvenlik hizmetini sunmaktadır. İletişimlerde asimetrik şifrelemenin uygulanması hedeflendiği için akıllı kartlar, kullanıcılarına ait hesap bilgilerinin yanı sıra ilgili asimetrik şifreleme için yine kullanıcılarına ait özel anahtarları saklamaktadırlar. Önerilen sistemin JavaCard teknolojisi kullanılarak gerçek bir uygulaması da yine bu çalışma içerisinde sunulmuştur.

Anahtar Kelimeler : Akıllı kart, Yazılım güvenliği, Mobil sistem mimarisi, Dağıtık nesne protokolü.

A SECURE MESSAGE TRANSMISSION SYSTEM ARCHITECTURE FOR COMPUTER NETWORKS EMPLOYING SMART CARDS

ABSTRACT

In this study, we introduce a mobile system architecture which employs smart cards for secure message transmission in computer networks. The use of smart card provides two security services as authentication and confidentiality in our design. The security of the system is provided by asymmetric encryption. Hence, smart cards are used to store personal account information as well as private key of each user for encryption / decryption operations. This offers further security, authentication and mobility to the system architecture. A real implementation of the proposed architecture which utilizes the JavaCard technology is also discussed in this study.

Key Words : Smart card, Software security, Mobile system architecture, Distributed object protocol.

1. GİRİŞ

Bilgisayar ve ağ teknolojilerindeki yeni gelişmeler sayesinde bilgisayar iletişimi, gün geçtikçe daha hızlı ve nispeten ucuz hale gelmektedir. Bunun sonucu olarak her geçen gün daha çok sayıda bilgisayar ağ üzerinden birbirine bağlanmakta ve Internet trafiği artmaktadır.

Ağ altyapısına bağlı çok sayıda bilgisayarın oluşu, ağ üzerinde iletilen bilginin içerik ve önem derecesi bakımından çeşitlilik taşıması anlamına gelmektedir. Bu sebeple iletilen bilginin güvenliğini sağlamak, çoğu zaman iletiyi başarıyla gerçekleştirmek kadar büyük önem taşır. Burada sözü edilen güvenlik aşağıdaki bileşenlerden oluşmaktadır (Stallings, 2006):

- Gizlilik: İletinin sadece yetki verilmiş kişi(ler) tarafından erişilebilir olması, üçüncü kişilerin eline geçmesinin engellenmesidir.

- Bütünlük: İletinin sadece yetki verilmiş kişiler tarafından değiştirilebilir olması ve kayıpsız olarak göndericiden alıcıya transferinin sağlanmasıdır.
- Kimlik doğrulama: Sisteme erişim sağlamaya yönelik tüm etkinliklerin tespit edilip, onay verilen ve onay verilmeyen erişim isteklerinin ayırt edilebilmesi ve onay verilmeyen erişim taleplerinin reddedilmesidir.
- Erişim hakkı: Kimliği doğrulanmış bir kullanıcının, sisteme hangi erişim haklarıyla (yetkilerle) erişebileceğinin belirlendiği güvenlik bileşenidir.
- Reddedememe: Gönderici veya alıcının iletimi ve/veya ileti üzerinde gerçekleştirdikleri değişiklikleri reddedememesidir.
- Erişilebilirlik: İletim sistemi çok yoğun ya da bir sorun sebebiyle çalışamaz halde de olsa, sistemin erişilebilirliğinin aksamamasıdır.

Günümüzde ağ üzerinden gerçekleştirilen bilgi iletişimi için, çeşitli iletişim yöntemleri mevcuttur. Bunlardan en yaygın kullanılanı, elektronik posta yoluyla iletişimdir. Bu yöntemde bir ana bilgisayar elektronik posta sunucusu olarak hizmet verirken, buna bağlı istemci bilgisayarlar kendi aralarında elektronik posta yolu ile iletişim kurarlar. Bu tür bir iletişimde güvenlik, çeşitli şekillerde sağlanabilir. Mesaj iletişiminde, kimlik doğrulama için *sayısal imza* algoritmalarının kullanılması ve elektronik postaların virüs taşıma riski nedeniyle kontrollerinin yapılması bunlara birer örnektir.

Güvenli ağ iletimi için kullanılan yöntemlerden biri de Kerberos tekniğidir (Miller v.d., 1987). Bu yöntemde bir kullanıcı bir iş istasyonunda oturum açmak istediğinde, iş istasyonu bu kullanıcının kimliğini doğrular ve böylece kullanıcının şifresinin ağ üzerinden iletimi engellenir. Daha sonra bu iş istasyonu, kullanıcıya sisteme dahil olan diğer sunucuları kullanmaya yarayan şifrelenmiş bilgiyi içeren bir bilet sağlamak üzere, Kerberos sunucusuna bağlanır. Bu sistemin dezavantajlarından biri, sistemde bağlanılmak istenen her bir bilgisayarın Kerberos tekniği ile çalışıyor olmasının gerekliliğidir. Bu yöntemin bir diğer dezavantajı ise Kerberos sunucusunun üçüncü kişilerce ele geçirilmesi durumunda, sistem güvenliğinin tamamıyla ortadan kalkacak olmasıdır. Kerberos sisteminde yetkilendirme sürecinin kendisi şifreli iken bilgisayarlar arası iletişim şifreli değildir.

Mesaj iletiminde güvenliği sağlamak amacıyla kullanılmakta olan bir başka yöntem de SSL (Secure Socket Layer – Güvenli Soket Katmanı) yöntemidir. Bu yöntemde bir Web sunucusu ile Web tarayıcısı arasındaki iletişimin tamamı, RSA (Rivest, Shamir, Adleman) (Rivest v.d., 1978) açık anahtar şifreleme algoritması kullanılarak şifrelenir.

Güvenli elektronik posta iletişimi için bu makalede önerilen çözüm ise akıllı kart teknolojisine dayanmaktadır. Bu çalışmada akıllı kartların güvenli elektronik posta iletişimini sağlamak amacıyla kullanıldığı mobil bir sistem mimarisini tanıtılmaktadır. Tasarlanan mimari mesaj iletişimlerinde asimetrik anahtarlamayı temel almakta; mahremiyet ve kimlik denetiminin sağlanması için de kriptografik bir mesajlaşma omurgası sunmaktadır. Söz konusu güvenlik gereksinimlerinin karşılanması için mimari içerisinde PGP (Pretty Good Privacy) (Zimmermann, 1995) bileşenleri kullanılmıştır. Yüksek seviyede güvenlik için önerilen mimari, taşınabilir, esnek, ve uygun veri depolama kapasitesi sunan akıllı kartları kullanmakta; kullanıcılar kimlik doğrulama için bu kartların sağladığı kolaylıklardan yararlanmaktadır.

Akıllı kartların güvenlik uygulamalarında kullanılması yeni bir çalışma değildir. Özellikle Java Card (Chen, 2000) gibi kullanımı nispeten kolay akıllı kart uygulama geliştirme ortamlarının ve yazılım çerçevelerinin ortaya çıkması ile söz konusu uygulamalarda akıllı kartların kullanılması giderek yaygınlaşmaktadır. Guthery ve arkadaşları akıllı kartlara dayalı bir Internet altyapısı geliştirmişlerdir (Guthery v.d., 2000). Rees ve Honeyman, SPEKE adını verdikleri ve akıllı kartlara dayanan protokollerinde alan adı sunucuları için konum bağımsız bir isimlendirme şeması ortaya koymuşlardır (Rees ve Honeyman, 2000). Brinkman ve Hoepman, JASON (JavaCard As Secure Objects Networks – Güvenli Nesne Ağları Olarak JavaCard) adını verdikleri platform için güvenli bir metot çağırma çatısı geliştirmişlerdir (Brinkman ve Hoepman, 2002).

Bakker, IBM tarafından geliştirilen KryptoKnight protokol ailesini kullanarak ağ tabanlı işlemler için KLOMP adını verdiği bir karşılıklı kimlik doğrulama ve anahtar dağıtma protokolünü tasarlamıştır (Bakker, 1999). Song ve Ahn ise akıllı kartlara dayanan bir sipariş iletim sistemi tasarlamış ve geliştirmiştir (Song ve Ahn, 2002). Akıllı kartlara dayalı bu sistemde güvenlik açık anahtar altyapısı ile sağlanmaktadır.

Belli açılardan birbirlerine göre üstünlükleri olsa da yukarıda bahsedilen çalışmaların hiçbiri dağıtık mesajlaşma sistemlerinin ihtiyaçları göz önünde bulundurulduğunda somut olarak tanımlanmış ve tam anlamıyla hayata geçirilmiş bir akıllı kart

sistemini ortaya koymamışlardır. Bu makalede önerilen akıllı kart destekli sistem mimarisi ise ihtiyaç duyulan mimari bileşenlerini tanımlamakta, tanımladığı bu bileşenleri içeren somut bir yazılım altyapısını sunmakta ve yeni akıllı kart ve güvenlik teknolojilerini kullanması nedeniyle söz konusu mesajlaşma sistemlerinin hayata geçirilmesini mümkün kılmaktadır.

Makalenin ikinci bölümünde sistem mimarisinin altında yatan akıllı kart ve güvenlik teknolojileri hakkında bilgi verilmiştir. Sistem mimarisinin bileşenleri üçüncü bölümde detaylı bir şekilde ele alınmıştır. Mimarinin uygulandığı bir gerçek durum çalışması dördüncü bölümde yer almaktadır. Son bölümde ise çalışma sonucu ve ileriye yönelik hedefler verilmiştir.

2. SİSTEMİN ALTYAPISINI OLUŞTURAN TEKNOLOJİLER

Önerilen mobil platformun ortaya konması için bu çalışmada yer alan sistem mimarisi akıllı kart, elektronik posta ve asimetrik şifreleme teknolojilerini kullanmaktadır. Takip eden altbölümlerde sistemin dayandığı yazılım ve donanım altyapı teknolojileri ve bunların sistemde nasıl kullanıldıkları hakkında bilgi verilmiştir.

2. 1. Akıllı Kart

Akıllı kart, içinde bilgi saklayan ve bu bilgiyi işleyen taşınabilir bir entegre olup standart hafıza-yonga kartlarının gelişmiş bir versiyonudur. Mikroişlemci içeren bu kartlar yerleşik hesaplama güçleri, taşınabilir güvenlik sağlamaları ve kolay kullanımları sayesinde başta telekomünikasyon (cep telefonlarında SIM kart olarak) ve ulaşım olmak üzere birçok sektörde geniş kullanım alanına sahiptir.

Standart hafıza-yonga kart sistemlerinde (örneğin manyetik kart) veri işleme donanım ve yazılımı karttaki bilgiyi okumakta, hesaplamaları yapmakta ve veriyi tekrar karta yazmaktadır. Akıllı kart sistemlerinde ise kartın içinde hafızaya ilave olarak bir mikroişlemci bulunmakta ve gerekli hesaplamalar onun vasıtası ile yapılabilmektedir.

Bir akıllı kart entegresi; bir mikroişlemci, ROM (Read Only Memory - Salt Okunur Bellek), EEPROM (Electrically Erasable Programmable ROM - Elektriksel Silinebilir Programlanabilir ROM) ve RAM (Random Access Memory - Rastgele Erişimli Bellek) bileşenlerini içermektedir. Kart üretilirken bellek mimarisinde yer alan ROM bölgesine kart işletim sistemi, kalıcı uygulamalar ve kullanıcı bilgileri yazılmaktadır. EEPROM bölgesinde de tıpkı ROM'da olduğu gibi kalıcı bilgiler tutulmaktadır. EEPROM'un ROM'dan farkı bu alana kart üretildikten sonra dahi bilgi ve uygulama kaydedilmesinin mümkün olmasıdır. Bu bellek alanı kişisel bilgisayarlardaki sabit disklere benzetilebilir. RAM bölgesi bilgi modifikasyonu ve depolamada geçici çalışma alanı olarak kullanılmaktadır. Bu bellekte bilgiler, kart bir güç kaynağına bağlı kaldığı sürece tutulmaktadır. Karttan elektrik kesildiğinde bu bilgiler kaybedilmektedir (Rankl ve Effing, 2000).

2. 1. 1. Akıllı Kart İletişim Modeli

Uygulamalarda akıllı kartların kullanılması için kartların CAD (Card Acceptance Device - Kart Kabul Aygıtı) adı verilen cihazlara yerleştirilmesi gerekir. Kart ile ev sahibi (host) bilgisayar arasındaki iletişim kanalı yarı çift yönlüdür (half-duplex). Bilgisayar ağlarında nasıl veriler bir protokole (örneğin TCP / IP) dayanan paketler halinde transfer ediliyorsa aynı durum akıllı kart ile iletişimde bulunduğu bilgisayar arasında da geçerlidir. ISO 7816 spesifikasyonunda tanımlanan APDU (Application Protocol Data Unit – Uygulama Protokolü Veri Birimi) adı verilen protokol ile akıllı kart ve bilgisayar arasında veri paketleri taşınmaktadır. Bu paketler emir ya da cevap mesajlarını içermektedir.

Kullanılan model efendi / köle modeli olup akıllı kart köle, iletişimde bulunduğu terminal ise efendi durumundadır. Akıllı kart her zaman ana bilgisayardan emir APDU'larını beklemekte; gelen APDU içindeki komutları işlemekte ve ana bilgisayara cevap APDU'su ile yanıt vermektedir (Hansmann v.d., 2000).

2. 1. 2. JavaCard Teknolojisi

JavaCard teknolojisi akıllı kart uygulamalarının daha etkin, kolay ve hızlı bir biçimde tasarlanıp hayata geçirilmesini sağlamaktadır. Akıllı kartların ve diğer bellek-sınırlı cihazların Java programlama dilinde yazılmış uygulamaları – ki bu uygulamalara *applet* adı verilir – çalıştırmalarına olanak sunar.

JavaCard teknolojisinde, Java sistem yazılımının uygulamalara yeterince çalışacak alan bırakacak şekilde akıllı karta yerleştirilmesi hedeflendiğinden Java dilinin özelliklerinin belli bir alt kümesi desteklenmiş ve biri kart üzerinde biri de kart dışında çalışan iki parçadan oluşan bir Java sanal makine mimarisi uygulanmıştır (Chen, 2000). Uygulama çalışma zamanında yer almayan sınıf yükleme, baytkodu (bytecode) doğrulama, bağlama ve optimizasyon gibi sistem kaynak kapasitesinin

önemli olmadığı bir çok işlem kart dışında çalışan sanal makine üzerinde gerçekleştirilmektedir.

JavaCard API (JavaCard Application Program Interface – JavaCard Uygulama Programı Arayüzü), akıllı kart uygulamalarını programlamada kullanılacak olan çekirdek ve uzantı Java paketlerini ve sınıflarını tanımlar. Bu paketler ve sınıflar JCF (JavaCard Framework – JavaCard Çatısı)'nı oluştururlar. Bu çalışmada tanıtılan sistem üzerinde kullanılan akıllı kartlar birer JavaCard olup kart üzeri yazılımlar JCF'e dayanmaktadır.

2. 2. OpenCard Çatısı

OCF (OpenCard Framework – Açık Kart Çatısı), Java programlama dili kullanılarak hazırlanmış bir akıllı kart ara yazılımıdır. OpenCard Konsorsiyumu tarafından geliştirilen OCF (Opencard Consortium, 1999) mimaride, bir akıllı kart ev sahibi uygulaması ile kart okuyucu (CAD) aygıtı arasında yer almaktadır. Çok esnek bir altyapısının olması ve Java dilinde hazırlanmasından kaynaklanan platform bağımsızlığı, akıllı kart uygulama geliştiricilerinin yüksek seviyeli programlama ara yüzlerini kullanabilmelerine ve farklı kart üreticilerine ait kart okuyucular ile uğraşmaya gerek kalmadan uygulama hazırlamalarına imkan sağlar. Bu çalışmada önerilen sistem mimarisinde de akıllı kartlar ile bağlı oldukları bilgisayarlar arasındaki iletişimin altyapısını OCF kullanılarak hazırlanan yazılım bileşenleri oluşturmaktadır.

2. 3. JavaMail Uygulama Programlama Arayüzü

JavaMail API'si (jGuru, 2001) mesaj okuma, yazma, alma ve gönderme amaçlı seçimlik bir Java paketidir. Bu kütüphane aracılığı ile Microsoft Outlook, Eudora ve Pine benzeri posta istemci yazılımları hazırlamak mümkündür. Bu makalede tanıtılan sistemin uygulanmasında akıllı kart etkileşimli posta istemci bileşenlerini hazırlamak için bu kütüphaneden yararlanılmıştır. Elektronik posta gönderilmesi ve alınması için sırasıyla SMTP (Simple Mail Transfer Protocol - Basit Posta Transfer Protokolü) ve POP3 (Post Office Protocol version 3 - Posta Ofisi Protokolü sürüm 3) protokollerinin uygulanması amacıyla yukarıda söz edilen yazılım kütüphanesi kullanılmıştır.

2. 4. PGP (Pretty Good Privacy)

PGP iletilen veya depolanan verilerin güvenliğini sağlamak amacıyla Phil Zimmerman tarafından geliştirilen bir açık anahtar şifreleme sistemidir (Zimmermann, 1995). En önemli avantajı anahtar değiş tokuşu sırasında özel bir güvenlik kanalına ihtiyaç duymamasıdır. Ayrıca PGP mesajın hangi işletim sisteminden geldiği bilgisini de mesaj paketine ekleyerek iletişimi sağladığından dolayı platform bağımsızdır.

PGP şifreleme, imzalama, sıkıştırma ve kod dönüşümü gibi servislerin yanı sıra, gizli anahtar ve açık anahtardan oluşan anahtar çiftleri ile ilgili hizmetler de sunmaktadır. PGP ile RSA algoritması için gizli anahtar ve ona karşılık gelen açık anahtar çiftleri yaratılır. RSA anahtarlarının uzunluğu genellikle 512 ile 2048 bit arasında seçilir. Bu uzunluktaki rasgele gizli anahtarı ezberlemek çok güç olduğundan, PGP'de gizli anahtar 128 bit uzunluğunda anahtar kullanan IDEA (International Data Encryption Algorithm - Uluslararası Veri Şifreleme Algoritması) (Menezes v.d., 1997) yardımıyla şifrelenerek, "secring.pgp" adlı dosyada saklanır. Gizli anahtarın ele geçirilmesini önlemek için "secring.pgp" dosyası sabit diskte değil, mobil ortamda saklanabilir. Bu makalede tanıtılan sistemde *bu dosya yani PGP özel anahtarı, akıllı kart üzerinde saklanmış* ve bu sayede sistem güvenliği artırılmaya çalışılmıştır.

PGP, adı ve işlevi gereği şifrelenmesine gerek olmayan açık anahtarı "pubring.pgp" adlı bir dosyada saklar. Bu çalışmada yer alan sistemde açık anahtarları ağ üzerinde istekte bulunan kullanıcılara iletmek amacıyla bir veya duruma göre daha fazla sayıda anahtar sunucusu yer almaktadır.

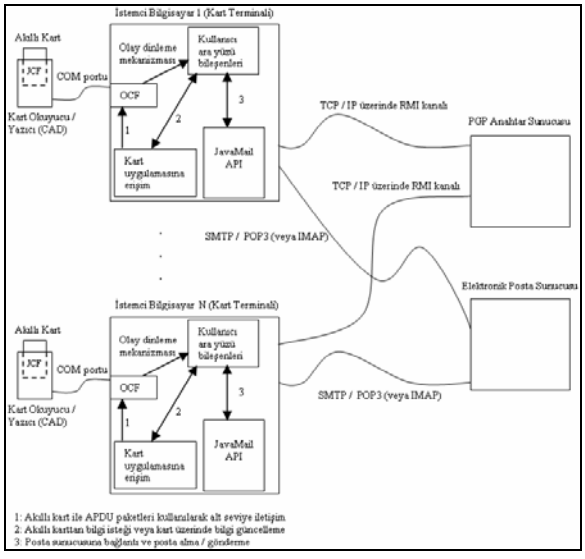
3. SİSTEM MİMARİSİ

Bilgisayar ağlarında güvenli mesajlaşma için önerilen ve akıllı kartların kullanılmasına dayanan sistem mimarisi Şekil 1'de verilmiştir. Mimari akıllı kart medyaları, kart kabul cihazları (CAD), kart terminalleri, elektronik posta ve şifreleme anahtarı sunucuları gibi bileşenleri içermektedir. Her bir bileşenin işlevi ve sistemdeki rolü mantıksal olarak ayrıktır. Ancak sistemin gerçek uygulamalarında birkaç bileşen aynı donanım içerisinde yer alabilir. Örneğin, elektronik posta sunucusu ve şifreleme anahtarı sunucusu yazılımı aynı bilgisayara yerleştirilebilir ve çalıştırılabilir.

Bir elektronik posta istemci bilgisayarı sistemde aynı zamanda bir akıllı kart terminalidir. Bu bilgisayar bir kart okuma / yazma birimine iletişim portu (COM) üzerinden bağlıdır. Bu makine üzerindeki elektronik posta istemci yazılımı OCF kütüphanesini akıllı kart uygulamalarını kontrol etmek amacıyla kullanır. Daha önce de belirtildiği gibi OCF kullanımı akıllı kartları kullanmak isteyen programların bu kartlar ile APDU protokolü

aracılığıyla iletişime geçmesini sağlamaktadır. Ancak APDU alt seviye bir protokol olup kart uygulama programı geliştiricilerinin akıllı kart iletişim modelinin ilkel ve kısıtlı paket yapısı ile uğraşmalarına neden olmaktadır.

Yazılım geliştiricileri yukarıda söz edilen zorluklardan kurtarmak amacıyla bir akıllı kart istemci ara yazılımı bu çalışmada tasarlanmıştır ve uygulanmıştır. Sistem mimarisinde "Kart uygulamasına erişim" bileşeni ile temsil edilen bu yazılım bilgisayarlar üzerinde akıllı kart ortamını hazırlamakta, güvenli kart oturumlarını yönetmekte ve yüksek seviyeli uygulamalar için onların yerine akıllı kartlar ile APDU protokolü üzerinden iletişime geçmektedir. Bu bir API (Application Program Interface - Uygulama Programı Arayüzü) olup kart istemcilerinin APDU iletişiminden soyutlanmasını hedeflemektedir. Böylelikle, örneğin kullanıcı ara yüzü bileşenleri bu API'nın sunduğu hazır nesneleri kısıtlı akıllı kart veri yapısı dönüşümleri yerine kullanabilmektedirler. Özellikle APDU bayt vektörü (Hansmann v.d., 2000) oluşturulmasında onaltılık (hexadecimal) kodlarla uğraşmadan iletişim paketlerinin hazırlanabilmesi imkanı kart iletişim yazılımı geliştirme sürecini hızlandırmaktadır. Bu mekanizma (Erdur ve Kardas, 2005; Kardas ve Tunali, 2006)'da tanıtılan yazılım mimarisi çalışmalarında da başarıyla uygulanmıştır. Ayrıntılı bilgi için söz konusu çalışmalar incelenebilir.



Şekil 1. Sistemin genel mimarisi.

Sistemde yer alan akıllı kartlar birer JavaCard olup içlerinde kullanıcılarının posta hesap bilgileri (kullanıcı adı, şifresi ve sunucu bağlantı parametreleri) yanında PGP özel anahtarını da saklamaktadırlar. Kart içi sistem yazılımı JavaCard Çatısı (JCF) kullanılarak tasarlanmış ve uygulanmıştır.

Sistem de akıllı kart dışı bir bileşen ile (özellikle bir elektronik posta istemci uygulaması) bir akıllı kart arasındaki herhangi bir iletişimin ilk adımı karşılıklı kimlik doğrulamayı sağlamaktır. Bu işlem her iki tarafın ilgili anahtar dosyalarında sakladıkları anahtarlarının karşılıklı kontrolünü içermektedir. Her akıllı kart oturumu iki tarafın da anahtar kontrolü gerçekleştirdikleri yetkilendirme safhası ile başlar: Akıllı kart anahtar dosyasındaki anahtarın kendisininkiyle aynı olup olmadığını kontrol eder. Elektronik posta istemci yazılımı ise akıllı kart üzerindeki anahtarın kendi anahtar dosyasındaki değer ile eşlenip eşlenmediğini kontrol eder. Her iki taraftaki kontroller de olumlu sonuçlanıp yetkilendirmeler sağlandığında iki taraf arasında güvenli bir iletişim kanalı oluşturulur.

Akıllı kart terminalleri Java RMI (Remote Method Invocation - Uzak Metot Çağrımı) protokolü dahilinde uzak yazılım nesnelerinin uygun metotlarını çağırarak bu protokol için birer istemci gibi davranmaktadırlar. RMI bir Java sanal makinesinde çalışan bir nesnenin başka bir Java sanal makinesi üzerinde çalışan bir nesnenin metodunu sanki kendi metoduymuş gibi çağırıp kullanmasına imkan vermektedir. Bu çalışmada yer alan sistemde de söz konusu uzak nesneler şifreleme anahtarı sunucularında (PGP sunucuları) görev almaktadırlar. Bir sistem kullanıcısı başka bir kullanıcıya şifreli bir elektronik posta göndermek istediğinde alıcının PGP açık anahtarına erişmesi gerekmektedir. İhtiyaç duyulan bu anahtarlar RMI kanalı üzerinden temin edilmektedir. PGP servisi açık anahtar halkasından anahtarların yukarıda bahsedildiği gibi temin edilmesi sistemin güvenliğini arttırmaktadır. Kart terminalleri RMI uzak bileşenleri ile RMI protokolüne uygun bir biçimde iletişime geçerek söz konusu anahtarları elde eder. Protokol "parameter marshalling" adı verilen tekniği kullandığı için açık anahtar nesnesi ağ üzerinden serileştirilmiş ve üçüncü şahıslara karşı korunmuş bir şekilde iletilir. RMI uzak nesnesi tarafından uygulanmaya konmuş ve ağ üzerinde iletilen ara yüz sadece ilgili istemci ve sunucu bileşen tarafından bilinebilir. Bu da kanal üzerinde iletilen anahtarın başka biri tarafından ele geçirilse dahi nesne ara yüzünü bilmediğinden dolayı içeriğinin çözümlenemeyeceği anlamına gelmektedir. Sistemde bir uygulaması yer alan RMI dağıtık nesne protokolü hakkında detaylı bilgi (Horstmann ve Cornell, 2000)'de bulunabilir.

Tasarımda yer alan elektronik posta istemci yazılımı posta alışverişlerinde bir önceki bölümde değinilen JavaMail Uygulama Programlama Ara yüzünü

kullanmaktadır. İstemciler elektronik posta sunucuları ile SMTP ve POP3 (eğer sunucu destekliyorsa IMAP) protokolleri üzerinden iletişimde bulunurlar. Söz konusu iletişime şu anki sistem mimarisi dahilinde ek güvenlik mekanizmaları dahil edilmemiştir çünkü tüm elektronik postalar PGP ile korumalı bir şekilde sistemde iletilmektedirler.

Sistem mimarisinin kullanıcı ara yüzü bileşenleri elektronik posta yazılımını kullanmak isteyen kişiler için kullanıcı dostu grafiksel bir ara yüz sağlamaktadırlar.

Sistemin işletilmesi sırasında gerçekleştirilen veri alışverişi, kimlik doğrulama, veri şifreleme ve deşifreleme işlemlerine ait model Şekil 2'de görülmektedir. Buna göre bir posta sunucusundan postalarını indirip okumak isteyen veya posta göndermek isteyen bir kullanıcı kart terminaline içerisinde kendisine ait PGP gizli anahtarının saklandığı akıllı kartını yerleştirir. Olay dinleme mekanizması sayesinde posta istemci programı tetiklenerek karşılıklı anahtar doğrulama gerçekleştirilir ve doğrulama sonrası istemci program kart ile APDU iletişimine başlar (Şekil 2: Adım 1). Güvenli kart oturumunun başlatılması için kullanıcıdan PIN (Personal Identification Number - Kişisel Tanımlama Numarası) girişi istenmektedir. Başarılı PIN girişi sonucunda akıllı kart üzerinde kimlik doğrulama sağlanır ve posta sunucusuna bağlantı bilgileri akıllı karttan transfer edilir (Şekil 2: Adım 2).

k: akıllı kart yazılımı, pc: terminal yazılımı,
kta: kart tanımlama anahtarı, ta: terminal anahtarı,
PGP_g: PGP gizli anahtarı,
PGP_a: PGP açık anahtarı,
f: işlem fonksiyonu,
$\forall b \in \{k, pc\}$,
$\forall g, \exists ç \in \{kta, ta, PIN, PGP_g, PGP_a, mesaj,$
şifreli_mesaj, kullanıcı_id,
kullanıcı_şifre, alıcı_id$\}$,
b: f(g) → ç olmak üzere sistem işleyişi:
1. k: doğrulama(ta) ∧ pc: doğrulama(kta) → APDU iletişimi başlat

2. k: kontrol(PIN) → kart oturumu başlat

3.a. pc: POP3(kullanıcı_id, kullanıcı_şifre) → şifreli_mesaj
b. pc: APDU_transfer() → PGP_g
c. pc: deşifre_et(şifreli_mesaj, PGP_g) → mesaj

4.a. pc: RMI_transfer()→ alıcı_id, PGP_a
b. pc: şifrele(mesaj, PGP_a) → şifreli_mesaj
c. pc: SMTP(alıcı_id, şifreli_mesaj)

Şekil 2. Sistem işletimi sırasında gerçekleştirilen işlemlere ait model.

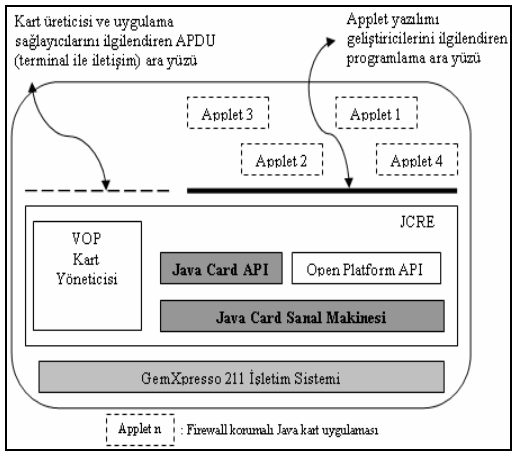
Kullanıcıya ait elektronik postalar sunucudan transfer edilir (Şekil 2: Adım 3a.). Transfer edilen postalar ilgili kullanıcının açık (public) PGP anahtarı ile şifrelendiğinden okunabilmeleri için öncelikle deşifre edilmeleri gerekmektedir. Tabi bunun için kullanıcının PGP gizli (private) anahtarına ihtiyaç duyulmaktadır. Bu noktada posta istemcisi kullanıcı akıllı kartı ile yeni bir iletişim dizisi başlatarak karttan kullanıcıya ait PGP gizli anahtarını ister. Kart üzerinde kimlik doğrulama tamamlandığı için kart, APDU paketleri içerisinde istemci yazılıma anahtarı transfer eder (Şekil 2: Adım 3b.). PGP gizli anahtarı elde edildiği için gelen postalar deşifre edilir ve kullanıcıya görüntülenir (Şekil 2: Adım 3c.).

Elektronik posta gönderimi de yine bu kart oturumu içerisinde gerçekleştirilebilir. Posta alıcılarının açık anahtarlarına yukarıda bahsedilen RMI iletişimi ile erişilmektedir (Şekil 2: Adım 4a.). İleti gönderilmek istenen kişi veya kişilerin açık PGP anahtarları ile ileti şifrelenir (Şekil 2: Adım 4.b.) ve ilgili protokol aracılığı ile posta sunucusuna gönderilir. Posta sunucusu da kullanıcı adına şifreli postaları alıcılarına gönderecektir (Şekil 2: Adım 4c.).

4. SİSTEM MİMARİSİNİN GERÇEKLEŞTİRİMİ

Bir önceki bölümde sunulan sistem mimarisinin gerekli yazılım ve donanım bileşenleri kullanılarak gerçek bir uygulaması hayata geçirilmiştir. Bu bölümde söz konusu uygulama ele alınmaktadır.

Uygulamada güvenli PGP anahtarı saklama ve elektronik posta iletimini sağlamak amacıyla kullanılan akıllı kartlar Gemplus firmasınca üretilen, çoklu applet desteğine sahip GemXpresso 211/PK model JavaCard'lardır. Şekil 3'te iç mimarisi verilen bu kartlar tek iş parçacıklı (single-threaded) bir işletim sistemine ve 8-bitlik bir mikroişlemciye sahiptir. Kart işletim sisteminin giriş-çıkış alt sistemi ISO 7816-3 ve ISO 7816-4 standartları ile uyumludur.



Şekil 3. GemXpresso 211/PK JavaCard iç mimarisi.

Kartların 32K Salt Okunur Bellek'leri (ROM), 32K Elektronik Silinebilir Programlanabilir Salt Okunur Bellek'leri (EEPROM) ve 2K Rastgele Erişimli Bellek'leri (RAM) vardır. Ancak bu kaynakların büyük bir bölümü kart işletim sistemi ve diğer sistem yazılımları tarafından kullanıldığından, kart üzerinde uygulama yazılımları için 16.5K EEPROM ve 0.5K RAM ayrılmıştır. Söz konusu kaynaklar burada sözü edilen uygulama için yeterli olmuştur: Kart içi yazılımı ve PGP özel anahtarı gibi kalıcı veri nesneleri için kart üzerinde 10K'lık bir EEPROM alanı kullanılmıştır. Kart içi yazılımın geliştirilmesinde kullanılan yazılım çatısı ise JCF 2.1'dir.

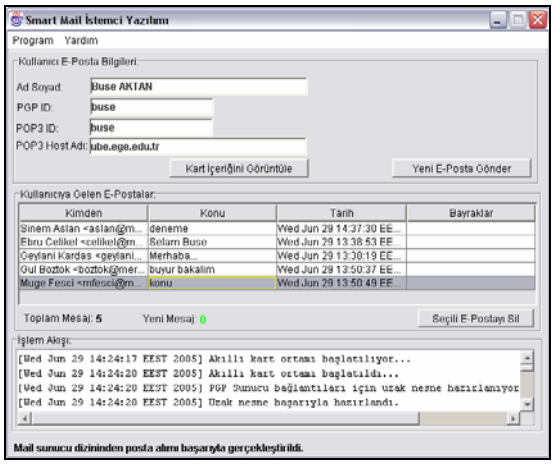
Kart kabul aygıtı (CAD) olarak uygulamada Gemplus GCR410 model, seri bağlantılı, kart okuma / yazma cihazı kullanılmıştır. Elektronik posta istemci terminallerine bağlanan bu aygıtın veri iletim hızı 9600 baud'dur. Uygulama sırasında gerçekleştirilen ölçümlerde, 9600 baud'luk bu veri kanalında 255 baytlık bir verinin akıllı karttan alınması ve ara yüzde gösteriminin yaklaşık 1.5 saniye sürdüğü gözlenmiştir. Bu süreye bir komut APDU paketinin karta gönderilmesi, veri bloğunun cevap APDU paketi içerisinde bilgisayara transferi ve kullanıcıya bilginin gösterilmesi işlemlerinin tuttuğu süre dahildir. Gerçekleştirilen bir diğer ölçüm ise kullanıcı kart oturumlarının başlatılması için geçen süre ile ilgilidir. Buna göre oturumun başlatılması ve akıllı kartın CAD'e yerleştirilip PIN girişi diyalog penceresinin kullanıcı önüne getirilmesi yaklaşık 5 saniye sürmektedir.

Akıllı kart içi yazılımlardan sunucu tarafı yazılımlara kadar tüm sistem Java programla dili ile geliştirilmiştir. Kart istemci, RMI istemci, JavaMail ve kart terminali kullanıcı ara yüzü yazılımları Intel Pentium 4 3.0 GHz işlemciye sahip ve üzerinde MS Windows XP işletim sistemi çalışan bilgisayarlara kurulmuştur. Bu bilgisayarlar Java 1.5 çalışma zamanı ortamı ve akıllı kart iletişimleri için OCF 1.2 kütüphanesini içermektedirler. Sistem testleri sırasında bu bilgisayarlar elektronik posta istemcisi olarak kullanılmışlardır. Aynı donanım konfigürasyonu ve işletim sistemine sahip başka bir bilgisayara ise sunucu bileşenleri kurulmuştur. Ancak bu bilgisayarda akıllı kart ortamı yer almamıştır.

Kullanıcı aynı zamanda başka kullanıcılara PGP kullanarak şifreli elektronik postalar da gönderebilir. Kullanıcı mesajını yazıp ilgili ara yüzden şifreleme isteğini belirttiğinde sistem alıcının PGP id'sini mesajı şiflemek amacıyla kullanıcıdan istemektedir. Alıcının PGP id'sini aldıktan sonra sistem PGP sunucusuna RMI kanalı üzerinden bağlanmakta ve bir önceki bölümde detayları verilen işleyişe uygun bir şekilde alıcının PGP açık anahtarını elde etmektedir. Elde edilen bu anahtar ile mesaj şifrelenir (Şekil 6) ve SMTP protokolü ile elektronik posta gönderilir.

Geliştirilen platform hakkında bilgi vermesi açısından örnek bir elektronik posta istemci oturumu, seçilmiş bazı uygulama ekran görüntüleri eşliğinde bu bölümde ele alınmıştır.

Elektronik posta oturumu, akıllı kart oturumunun açılması ve PGP sistemine RMI kanalı üzerinden bağlanılması ile başlamış olur. Kullanıcı akıllı kartına erişim için girmesi gereken PIN değerini doğru girdiğinde kart üzerindeki kimlik doğrulaması tamamlanmış olur ve Şekil 4'te gösterildiği gibi kart üzerinde depolanan bilgileri uygulama ekranında kullanıcıya gösterilir. Oturumun başlatılması tamamlandığında ilgili kullanıcıya gelen elektronik postalar posta sunucusundan otomatik olarak elde edilir ve Şekil 4'teki gibi gösterilir. Bu işlem sırasında posta hesabına ait erişim bilgileri ve bağlantı parametreleri (sunucu IP'si, kullanıcı adı ve şifresi) kullanıcının akıllı kartından elde edilerek iletişim sırasında kullanılmaktadır. Böylelikle kullanıcının her oturumda tekrar tekrar bu bilgileri girmesine gerek yoktur.



Şekil 4. Akıllı kart sahibinin kart üzerindeki yetkilendirilmesi onaylandıktan sonra kart üzerindeki bilgilerin ve kullanıcıya gelen elektronik postaların görüntülenmesi.

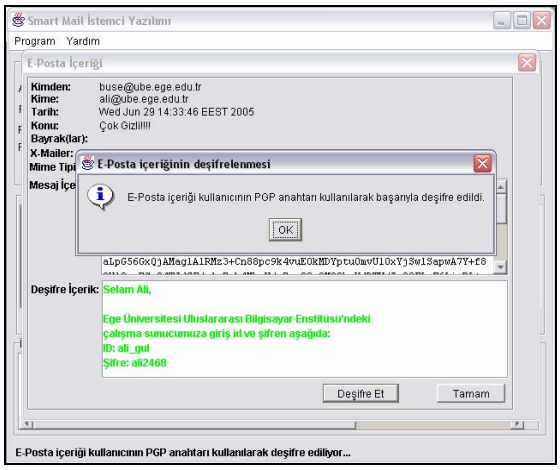
Kullanıcı kendisine gelen şifreli bir postayı görmek istediğinde kullanıcının akıllı kartındaki PGP özel anahtarı kullanılarak posta içeriği deşifre edilmekte ve kullanıcıya görüntülenmektedir (Şekil 5).

Kullanıcı aynı zamanda başka kullanıcılara PGP kullanarak şifreli elektronik postalar da gönderebilir. Kullanıcı mesajını yazıp ilgili ara yüzden şifreleme isteğini belirttiğinde sistem alıcının PGP id'sini mesajı şiflemek amacıyla kullanıcıdan istemektedir. Alıcının PGP id'sini aldıktan sonra sistem PGP

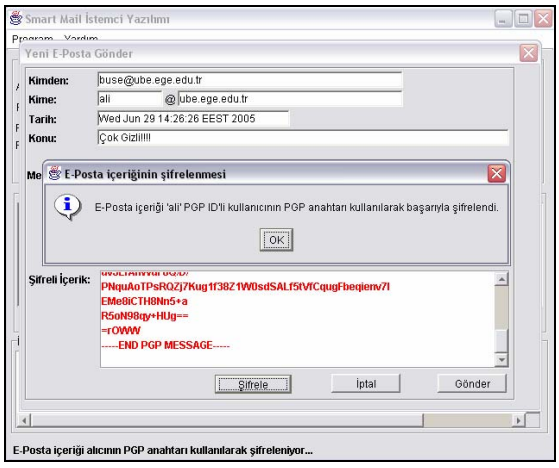
sunucusuna RMI kanalı üzerinden bağlanmakta ve bir önceki bölümde detayları verilen işleyişe uygun bir şekilde alıcının PGP açık anahtarını elde etmektedir. Elde edilen bu anahtar ile mesaj şifrelenir (Şekil 6) ve SMTP protokolü ile elektronik posta gönderilir.

Geliştirilen akıllı kart destekli güvenli elektronik posta sisteminin çalışmasına ilişkin aksaklıkların belirlenmesi ve sistemde güvenliği artırmak adına hangi zamanda ne işlem yapıldığının izlenebilmesi amacıyla kayıt dosyaları da tutulmaktadır. Şekil 7'de bu dosyalardan birinin içeriğinden bir kesit görülmektedir. Bu kayıtlama sayesinde sistemin çalışması sırasında gerçekleşen sorunlar, sistemde hangi kullanıcı tarafından ne zaman ne işlemin yapıldığı gibi bilgiler inkar edilemez bir şekilde elde edilebilmektedir. Kayıt dosyası üzerinde periyodik olarak yapılacak yönetici kontrolleriyle, sistemde olası aksaklık sinyalleri zamanında farkedilebilir ve sistem buna göre gözden geçirilebilir. Ayrıca sistemde meydana gelen yanlış çalışma, sistem kaynaklarını kötüye kullanma gibi istenmeyen durumlarla karşılaşıldığında sorumlu kullanıcı(lar) tespit edilebilir.

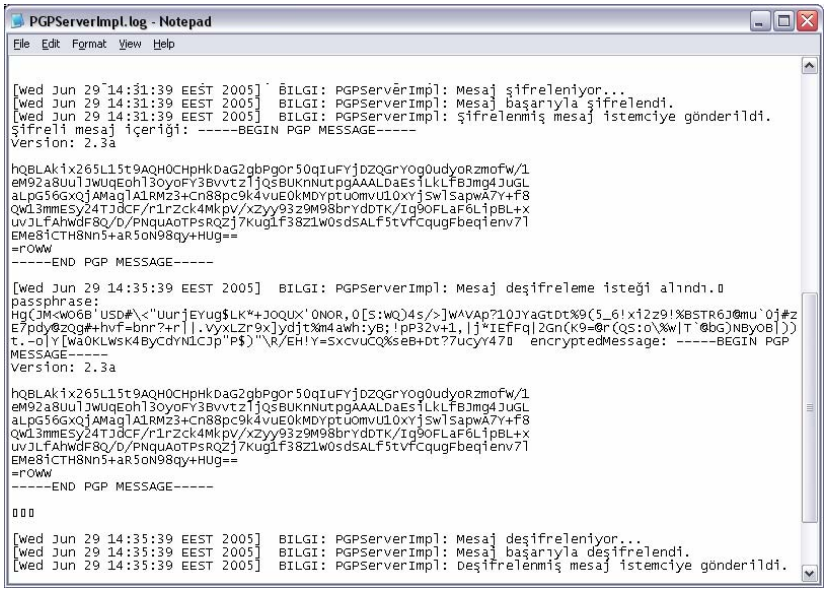
Sistemde istemci ve sunucu tarafların bağlantısı ile mesaj alıp gönderme, şifreleme, yeni kullanıcı kartları hazırlama, yenileme gibi sistem yönetim işlemlerinin tümünü gerçekleştirmek üzere iş akışı RMI sunucuları tarafından gerçekleştirilmektedir.



Şekil 5. Bir sistem kullanıcına gelen şifreli elektronik postanın kullanıcının akıllı kartından alınan PGP özel anahtarı kullanılarak deşifre edilmesi ve kullanıcıya görüntülenmesi.



Şekil 6. Bir elektronik postanın gönderilmeden önce alıcının PGP açık anahtarı ile şifrelenmesi.



Şekil 7. Sistemde tutulan kayıt dosyalarından birinin içeriği. Ekran görüntüsündeki kayıt içeriği sistemde istemcilere PGP anahtarlarını dağıtmayla görevli bir uzak nesnenin yapmış olduğu işlemlere aittir.

5. SONUÇ VE DEĞERLENDİRME

Bu çalışmada, bilgisayar ağlarında güvenli mesaj alışverişinin yerine getirilmesi için akıllı kartlardan yararlanılan mobil bir sistem mimarisi tanıtılmış; mimarinin gerçek yazılım ve donanım bileşenleri kullanılarak hayata geçirildiği bir uygulamaya yer verilmiştir. Mimari bünyesinde akıllı kartların kullanılması elektronik iletişimde kimlik denetimi ve gizlilik gibi iki önemli güvenlik servisini sistem kullanıcılarına sağlamıştır.

Geliştirilen sistem PGP temelli asimetrik şifrelemeyi kullanmaktadır. Posta hesap bilgilerine ek olarak her kullanıcının kendi kartında PGP özel anahtarı yer aldığından kullanıcı sisteme ait herhangi bir istemci terminalden posta alışverişinde bulunabilmektedir. PGP özel anahtarlarının akıllı kart gibi güvenli bir medyada saklanıp kontrollü bir şekilde kullanılabilmesi sistemin önemli avantajlarından biridir.

Sistemin güvenliğini değerlendirirken PGP'ye dayalı sistem analizinin de yapılması yerinde olacaktır. PGP asimetrik şifreleme yöntemini kullanarak gizlilik, kimlik doğrulama ve sayısal imza hizmetlerini sunar. Başlangıçta PGP algoritması güven ağı (web of trust) esasına dayanarak tasarlanmış olsa da, sonradan eklenen özelliklerle X.509 standardı ile anılan sertifika otoritelerini kullanacak şekilde geliştirilmiştir. PGP yöntemine alternatif olarak S/MIME (Secure / Multipurpose Internet Mail Extensions – Güvenli / Çok Amaçlı Internet Mesaj Uzantıları) yöntemi kullanılabilir. Ancak adı geçen yöntem ile oluşturulan mesaj imza bloğu hem imzanın kendisini hem de imza sahibinin sayısal sertifikasını içerdiğinden, PGP mekanizması ile oluşturulan mesaj imza bloğundan daha uzundur (Zubeldia, 2004). Bu sebeple bu makalede tanıtılan sistemde
S/MIME yöntemi yerine PGP kullanılmıştır.

Güvenli mesaj iletimi için geliştirilen bir başka sistem Microsoft'un RMS (Rights Management Services - Hak Yönetim Hizmetleri) yazılımıdır. Bu teknoloji PGP'den farklı olarak anahtar değişimi ve politika kontrol yöntemleri kullanmaktadır. İki sistemin karşılaştırması Tablo 1'de verilmiştir.

Tablo 1. PGP ve RMS Yöntemlerinin Karşılaştırılması (GigaTrust, 2005).

	Kurulum	Şifreleme	İletim	Kimlik Doğrulama	Şifre Açma
PGP	- Tek anahtar çifti, - Amaç odaklı yönetim	- AES vb. şifreleme algoritmaları, - X.509 sertifikaları, - Tüm hakları ver ya da hiç hak verme	- İletişim hattı için özel gereksinimleri yok	- Gerekmiyor	- Şifre açmadan sonra alıcı taraf veriye her zaman erişme hakkına sahip
RMS	- Sunucu tarafından kontrol edilen çok sayıda anahtar	- AES, - XrML sertifikaları, - Değişken haklar	- Anahtar değişimi şifreli iletişim hattı üzerinden yapılıyor	- Kimlik doğrulama RMS sunucusunda yapılıyor	- Sürekli koruma: Şifre açılsa da veri erişimi içerik anahtarı ile mümkün

Her ne kadar RMS güvenlik sağlama sürecinin birden fazla aşamasında PGP'den daha iyi olanaklar sunuyor görünse de RMS tekniğinin en büyük dezavantajı sadece Microsoft işletim sistemi altında çalışıyor olması ve başka işletim sistemleri tarafından desteklenmiyor olmasıdır. Tasarlanan sistemin platform bağımsız olması temel hedeflerden biri olduğundan bu çalışmada RMS tekniği yerine PGP tercih edilmiştir.

Akıllı kartların depolama kapasiteleri PGP oturum anahtarlarının güvenli bir şekilde saklanması için yeterli olmuştur. Bu kartların mimari de kullanılmasının bir diğer avantajı akıllı kartların taşınabilir olması sayesinde sisteme kazandırılan esneklik ve kullanımı kolaylığıdır.

Geliştirilen sistem şu an için Microsoft Outlook ve benzeri diğer posta istemci programları ile direkt iletişime geçememektedir. Bu yazılımlarla tam anlamıyla bir birlikte çalışılabilirlik (interoperability) henüz sağlanamamıştır. Ancak POP3 ve SMTP protokollerini kullanan tüm posta sunucuları ile uyumlu bir şekilde çalışabilmektedir. Ek fonksiyonların da sisteme katılmasıyla şu anki tasarım daha modüler olacaktır ve gelecekte diğer sistemler ile daha uyumlu bir halde çalışabilecektir.

Şu anki sistem yapısına yakın zamanda birkaç yeni özelliğin de katılması hedeflenmektedir. Bunların başında sistem bünyesinde güvenli dosya transferinin dahil edilmesi gelmektedir. Bundan başka, PGP'nin dijital imza bileşeninin sisteme entegrasyonu ile mimarideki yetkilendirme ve kimlik denetimi özelliklerinin geliştirilmesi planlanmaktadır.

6. TEŞEKKÜR

Bu çalışma, Ege Üniversitesi Rektörlüğü Araştırma Fonu'nca desteklenen 2004/UBE/001 numaralı Bilimsel Araştırma Projesi kapsamında gerçekleştirilmiştir. Çalışma için gerekli kaynağı sağlayan Ege Üniversitesi Rektörlüğü Araştırma Fonu'na teşekkür ederiz. Bu makaleyi değerlendiren ve çalışmanın iyileştirilmesi yönünde görüşlerini ve eleştirilerini belirten hakemlere de katkılarından dolayı ayrıca teşekkür ederiz.

7. KAYNAKLAR

Bakker, B. 1999. Mutual Authentication with Smart Cards, USENIX Technical Program paper, Smartcard 99, Chicago, IL, USA.

Brinkman, R. and Hoepman, J. H. 2002. Secure Method Invocation in JASON, Vth Smart Card Research and Advanced Application Conference, 29-40, San Jose, CA, USA.

Chen, Z. 2000. JavaCard Technology for Smart Cards Architecture and Programmer's Guide 368 s. Addison - Wesley, MA - USA.

Erdur, R. C. and Kardas, G. 2005. Personalized Access to Semantic Web Agents Using Smart Cards, Euro-Par 2005 Parallel Processing, Lecture Notes in Computer Science, Springer-Verlag, 3648, 1110-1119.

GigaTrust. 2005. Comparison of RMS and PGP Technologies. URL: http://www.gigatrust.com/docs/GigaTrust_White_Paper_RMS_PGP.doc (son erişim yılı: 2007).

Guthery, S., Baudoin, Y., Possega, J. and Rees, J. 2000. IP and ARP Over ISO 7816-3 10s. Network Working Group Internet Draft, web sayfasi: http://www.citi.umich.edu/projects/smartcard/webcard/draft-guthery-ip7816-00.txt (son erişim tarihi: 2006).

Hansmann, U., Nicklous, M. S., Schack, T. and Seliger, F. 2000. Smart Card Application Development Using Java, 293s. Springer, Berlin – Germany.

Horstmann, C. S. and Cornell, G. 2000. Core Java 2 Volume II - Advanced Features 920s., Sun Microsystems Press, California - USA.

JGURU web sayfası 2006. "Fundamentals of the JavaMail API" URL: http://java.sun.com/developer/onlineTraining/JavaMail/contents.html (son erişim tarihi, 2006).

Kardas, G., and Tunali, E. T. 2006. Design and Implementation of a Smart Card Based Healthcare Information System, Computer Methods and Programs in Biomedicine, Elsevier, Vol. 81, 66-78.

Menezes, A., Oorschot, P. V. and Vanstone, S. 1997. Handbook of Cryptography 816s., CRC Press Inc., USA.

Miller, S.P., Neuman, B.C. and Saltzer, J. H. 1987. Section E.2.1: Kerberos Authentication and Authorization System MIT Project Athena, (Technical Specification), 36s., USA.

OpenCard Consortium 1999. OpenCard Framework 1.2 Programmer's Guide 82s. IBM Deutschland Entwicklung GmbH, Boeblingen - Germany.

Rankl, W. and Effing, W. 2000. Smart Card Handbook 746s. John Wiley & Sons, West Sussex - England.

Rees, J. and Honeyman, P. 2000. Webcard: A Java Card Web Server, IVth Working Conference on Smart Card Research and Advanced Applications, (CARDIS), 197-208, Bristol, UK.

Rivest, R.L., Shamir, A. and Adleman, L. 1978. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of ACM 21, 120-126.

Song, W. J. and Ahn, B. H. 2002. Secure Transmission of the Prescription Order Communication System Based on the Internet and the Public-Key Infrastructure Using Master Smart Cards in the 2-way Type Terminal, 35th Annual Hawai International Conference on System Sciences, Big Island, Hawai, USA, 156-163.

Stallings, W. 2006. Cryptography and Network Security 592s. Prentice Hall, NJ, USA.

Zimmermann, P. R. 1995. The Official PGP User's Guide 216s. MIT Pres, Boston, USA.

Zubeldia, K. 2004. HIPAA and Electronic Signatures. URL: http://www.ncvhs.hhs.gov/041208p1.pdf (son erişim yılı: 2007).