ÖZEL ANAHTARIN GÜVENLİĞİNİN SAĞLANMASINDA PARMAK İZİ TARAYICISI İLE KUVVETLENDİRİLMİŞ AKILLI KART ÇÖZÜMÜ

Metin ÖZKAN[1] **İbrahim SOĞUKPINAR[2]**

[1,2]Gebze Yüksek Teknoloji Enstitüsü Bilgisayar Mühendisliği Bölümü
[1]e-posta: mozkan@alumni.bilkent.edu.tr [2] e-posta: ispinar@bilmuh.gyte.edu.tr

Anahtar Kelimeler : Açık Anahtar Kriptografisi, Özel Anahtarın Güvenliği, Biometrik Çözüm

ÖZET

Bu bildiride sanal ortamın bu kadar yaygınlaşmasıyla beraber ön plana çıkan e-güvenlik kavramının temel taşlarından olan sayısal imzanın en zayıf ve önemli noktası olan özel anahtarların üretimi, saklanması ve kullanılması aşamalarında oluşan tehditlere karşı en üst güvenlik düzeyinde bir yöntem önerilmiştir. Bu yöntemin gerçeklenmesinde akıllı kart ve parmak izi tarayıcısı teknolojilerinden faydalanılmıştır. Bu çalışmayla özel anahtarının güvenliğinden emin olmak isteyen kullanıcılar için güvenli ve düşük maliyetli bir sistem oluşturulmuştur. Bu çalışmada önerilen çözüm ile, kullanıcıya ait biyometrik özelliklerin de (something you are) yetkilendirmede gözönünde bulundurulması ve bunun akıllı kart ve parola ile entegre edilmesi ile üç kademeli bir güvenlik seviyesi oluşturmamız sağlanmıştır.

1 GİRİŞ

Son yıllarda internette özellikle elektronik ticaretin ön plana çıkmasıyla güvenli ve özel bağlantılar istenir hale geldi. Bu tür bağlantıların sağlanmak zorunda olması, araştırmacıları İnternet kullanımını daha güvenli hale getirmek için çeşitli yollar bulmaya yönlendirdi. İlk başlarda güvenlik duvarları (firewall), sonra saldırı tespit sistemleri (intrusion detection system), daha sonra sanal özel ağlar (Virtual Private Networks). Şimdilerde ise açık anahtar altyapısı (PKI) ve sertifika otoriteleri (CAs). Açık anahtar kriptografisi üzerine oturan açık anahtar altyapısı (AAA), kullanıcılarının anahtarlarının merkezi olarak oluşturulmasını, dağıtımını, takibini ve iptalini gerçekler. Bunları sağlamak içinde anahtarları sayısal sertifika biçiminde dağıtır.

Bu yöntem insanlara sanal ortamda bir kimlik kazandırmayı hedeflemektedir. Herkesin kendi kimlik kartı yerine geçen sayısal sertifikaları olacak ve bu sertifikalar onların bu sanal dünyanın faydalarından en iyi şekilde yararlanmaları için uygun ortamı sağlayacaktır. Alışveriş, haberleşme, bilgi transferi, anlaşma, sözleşme, noter gibi normal yaşamımızda faydalandığımız hizmetlerden sanal ortamda da faydalanmamızı gerçekleştirecektir.

Bu bildiride sanal ortamın bu kadar yaygınlaşmasıyla beraber ön plana çıkan e-güvenlik kavramının temel taşlarından olan sayısal imzanın en zayıf ve önemli noktası olan özel anahtarların üretimi, saklanması ve kullanılması aşamalarında oluşan tehditlere karşı en üst güvenlik düzeyinde bir yöntem önerilmiştir. Bu yöntemin gerçeklenmesinde akıllı kart ve parmak izi tarayıcısı teknolojilerinden faydalanılmıştır. Bu çalışmayla özel anahtarının güvenliğinden emin olmak isteyen kullanıcılar için güvenli ve düşük maliyetli bir sistem oluşturulmuştur.

2 SAYISAL İMZA VE AÇIK ANAHTAR ALTYAPISI

2.1 Sayısal İmza

E-ticaretin daha geniş kitleler tarafından kabul görebilmesi için güvenlik çözülmesi gereken en önemli problemdir. Güvenli bir uygulamanın minimum gereksinimleri şunlardır:
Gizlilik (Confidentiality).
Veri Bütünlüğü (Data Integrity).
Kimlik Doğrulama (Authentication).
İnkar Edememe (Non-repudiation).

Bu dört önemli özellikten biri veya bir kaçının sağlanmaması durumunda söz konusu sistemin güvenilirliğinden bahsedilemez.

E-güvenlik kapsamı içerisinde veri bütünlüğü, kimlik doğrulama ve inkar edilememe özellikleri sayısal imza sayesinde sağlanır. Sayısal imza tek yönlü matematiksel bir fonksiyonun çıktısının asimetrik bir algoritma ile şifrelenmesi ile elde edilir. Açık-anahtar şifreleme algoritmaları olarak da geçen asimetrik algoritmaların en önemli özelliği kapama ve açma işlemleri için farklı iki anahtara ihtiyaç duymasıdır [4]. Bu anahtar çifti açık anahtar ve özel anahtar olarak adlandırılmaktadır. Açık anahtar sizin imzanızın tanınmasını sağlar ve herkesin erişimine açıktır. Özel anahtarın ise sadece sizin tarafınızdan bilinmesi, kullanılması ve özenle saklanması gerekir.Açık anahtar kendi içerisinde kime ait olduğuna dair bir bilgiye sahip değildir. Bu problemin çözümünde sayısal sertifikalar kullanılarak kullanıcı bilgileri ile açık anahtarı ilişkilendirilmesi sağlanır.

2.2 Açık Anahtar Altyapısı

Güvenli haberleşmenin çok geniş bir kitleyi kapsadığı göz önüne alındığında bunun çok büyük ve sistemli bir organizasyon gerektirdiği anlaşılmaktadır. Bu

kadar çok sayıda sayısal sertifikanın oluşturulması, dağıtımı, takibi ve gerektiğinde iptal edilme işlemlerinin bir sistematik haline getirilmiş şekline Açık Anahtar Altyapısı (AAA) denmektedir.
AAA e-güvenliğin ana gereksinimleri olan gizlilik, bütünlük, doğrulama ve inkar edememeyi sağlayan açık anahtar kriptografisi üzerine oturmaktadır.

Bir AAA aşağıdaki bileşenlerden oluşur:

- **SO:** Sertifika otoritesi, sertifikaların üretimi ve iptalinden sorumludur,
- **KO:** Kayıt otoritesi, kullanıcılar ve onların açık anahtarları arasındaki bağı onaylar,
- **Sertifika sahipleri:** Kullanıcılar ya da bilgisayarlar kendilerine ait olan sertifikaları kullanarak sayısal dokümanları imzalar ve şifrelerler,
- **Depolar:** Depolar sertifikaları ve sil listelerini depo eder ve kullanıma sunarlar,
- **Güvenlik Prensipleri:** Kurumun en üst düzey bilgi güvenliği yönetimini tanımlarlar. Aynı zamanda kriptografinin kullanımındaki yöntem ve prensipleri belirlerler, [2].

AAA kullanıcıların sisteme kaydedilmesini, sertifikalarının üretilmesini, sertifikaların iptal edilmesini ve gerektiğinde diğer AAA'lar ile çapraz sertifikasyon yapılması gibi temel fonksiyonları sağlamalıdır.

Sertifika tabanlı sistemlerin en büyük risklerinden bir tanesi de kendimizin imzalama özel (private signing) anahtarının korunma problemidir [1-3].

2.3 Özel Anahtarın Güvenliği

AAA'nı oluşturmaya çalıştığımızda en kritik konulardan bir tanesi özel anahtarın korunmasıdır. Özellikle de Sertifika Otoritesinin özel anahtarının korunması sistemin kalbidir [1]. Bu anahtar çalınırsa sistemin en baştan ilklendirilmesi gerekecektir. Yani o ana kadar oluşturulmuş bütün sertifikalar geçersiz kılınacaktır. Bütün sertifika sahiplerine bunun duyurulması, yeni sertifikaların gönderilmesi büyük zaman, para ve prestij kaybına sebep olacaktır. Micro planda tek kullanıcıyı düşünürsek, onun özel anahtarının çalınması da bu kişinin başına telafisi mümkün olmayan problemler açabilecektir. Özellikle sayısal imza yasalarının kabulünden sonra özel anahtarımızın çalınmış olduğunu ve bizim yerimize başka birisinin bizi zor durumda bırakabilecek yazışmalar yapabileceği ihtimali çözülmesi gereken ciddi bir problemdir. Özel anahtarın güvenliği konusunu üç ayrı aşamada incelemek zorundayız. Bunlar anahtarın üretimi, saklanması(korunması) ve kullanılması aşamalarıdır. Bu konuda getirilen çözümün bu aşamaların hepsini ayrı ayrı ele alması ve bunları güvenli hale getirmesi gerekmektedir.

2.3.1 Özel Anahtarın Üretimi

Anahtar çiftlerinin üretimi yapılırken dikkat edilmesi gereken en önemli konu bu üretimin donanımsal olarak gerçeklenmesidir. Genelde uygulama maliyetleri gözönünde bulundurulduğunda bu önemli nokta gözardı edilmektedir. Şu anda kullanılan Entrust, Baltimore gibi önde gelen yazılımlar dahi anahtarların oluşturulması işlemini ekranda farenin hareketleriyle topladıkları datayı kullanarak (taban kabul ederek) yazılımsal olarak rastgele sayı hesaplayarak yapmaktadırlar. Bu da anahtarların sağlamlığını ve güvenilirliğini oldukça zedelemektedir. Yapılması gereken ise bu üretimi tamamen bu iş için özelleştirilmiş donanımsal cihazlarla gerçeklemektir. Bu donanımsal cihazlar rastgele sayı üreteçlerine sahip olmalıdırlar ve üretilen sayı dizilerini daha dayanıklı ve güvenilir hale getirmek için sağlamlaştırma algoritmalarından faydalanmalıdırlar. Bu da zayıf anahtar çiftlerine sahip olma ihtimalini minimum düzeye indirir.

2.3.2 Özel Anahtarın Saklanması

Bilindiği gibi anahtarlar, bit dizileridir ve onların hafızada tutulamayacağı açıktır. Anahtarları saklayabilecek teknolojiler ise çeşitlilik açısından sınırlıdır. Bunlar disket sürücüler, sabit diskler ve donanımsal cihazlardır.

Disket sürücüler ve sabit diskler düşük maliyetli ve geniş bir kullanım alanına sahip oldukları için iyi bir çözüm olarak görünmektedir. Üzerinde taşıyacağımız anahtara erişim kontrolünü bir parolayla yapabiliriz. Diğer taraftan kolay kopyalanabilir olmaları ve manyetik alanlardan etkilenmeleri kullanımı riskli hale getirmektedir. Donanımsal cihazlar ise bizlere en iyi çözümü sunmaktadır. Kullanılacak sisteme göre, kripto kartlarından akıllı kartlara kadar geniş bir yelpazeye sahiptirler. Cüzdanımızda rahatlıkla taşıyabileceğimiz akıllı kartlar kredi kartı büyüklüğünde bilgisayarlar olarak çalışabilmektedirler. Fiziksel dayanıklılıkları da oldukça yeterlidir. Son yıllarda üretilen kripto işlemcili akıllı kartlar anahtar üretiminden imzalama ve şifreleme işlemlerine kadar kart içinde yapılmasına olanak sağlamaktadır. Bu sayede özel anahtarın kartı terketmesine ihtiyaç kalmamıştır. Bu mikroişlemcili kartlar manyetik depolama ortamlarına nazaran büyük bir avantaja sahiptirler. Akıllı kart okuyucusundan dolayı ilk maaliyetleri biraz arttırsalar da uzun vadede oluşabilecek risk giderlerini azalttıklarından uygulamalarda ki kullanım oranları giderek artmaktadır.

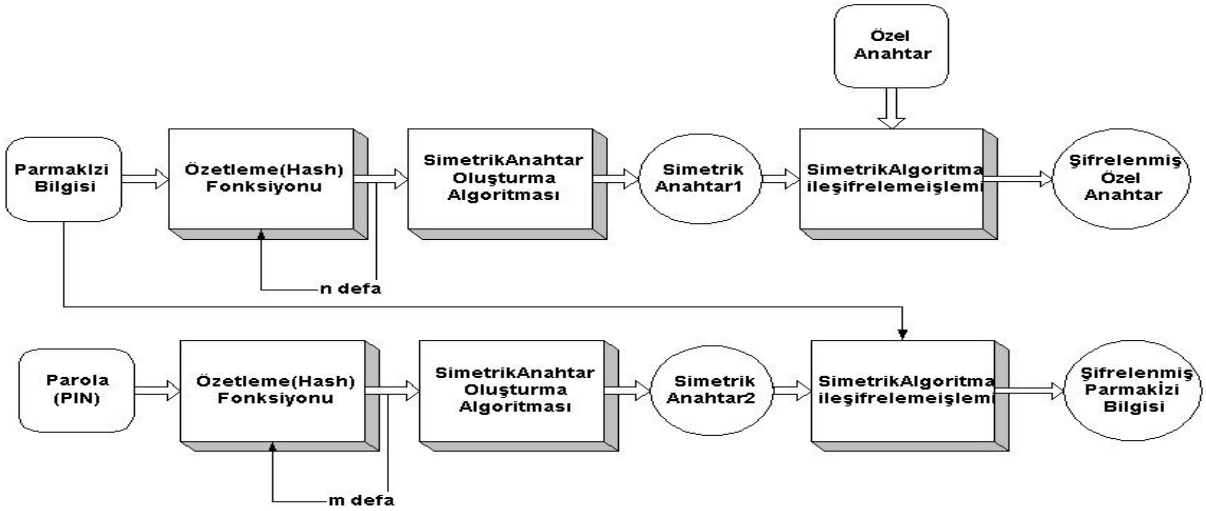
2.3.3 Özel Anahtarın Kullanılması

Kullanıcının özel anahtarının erişim yöntemleri temel olarak iki sınıfa ayrılabilir,

A) Kullanıcının hiç bir şekilde ham özel anahtara ulaşamadığı sistemler

B) Kullanıcının ham özel anahtara ulaşabildiği sistemler.

Tabii ki kullanıcının anahtara hiç bir şekilde ulaşamadığı sistemler güvenlik açısından çok daha kuvvetlidir. Bu tip sistemlerde anahtara ulaşım



Şekil 1:Kullanıcının anahtarlarının üretilmesi ve saklanması

kullanıcı tarafında imkansızdır. Anahtar bir cihaz veya donanım içerisinde saklanır ve anahtarın bu cihaz içerisinden çıkmasına kesinlikle izin verilmez. Yapılacak işlemler bu cihazın içerisinde yapılır ve bu cihazın kopyalanması ve yedeklenmesi engellenir. Kullanıcının özel anahtara ulaşabildiği sistemlerde ise anahtarın güvenli bir şekilde korunduğundan bahsedilemez. Uygulamaların kullanılması için anahtar farklı bir ortama aktarılabilir. Kullanıcı tarafından elde edilip farklı bir kaynağa kopyalanabilir. Bu şekilde anahtarın birçok kopyası etrafta dolaşıyor olabilir. Sonuç olarak anahtarın istenmeyen kişilerin eline geçme ihtimali çok yüksektir.

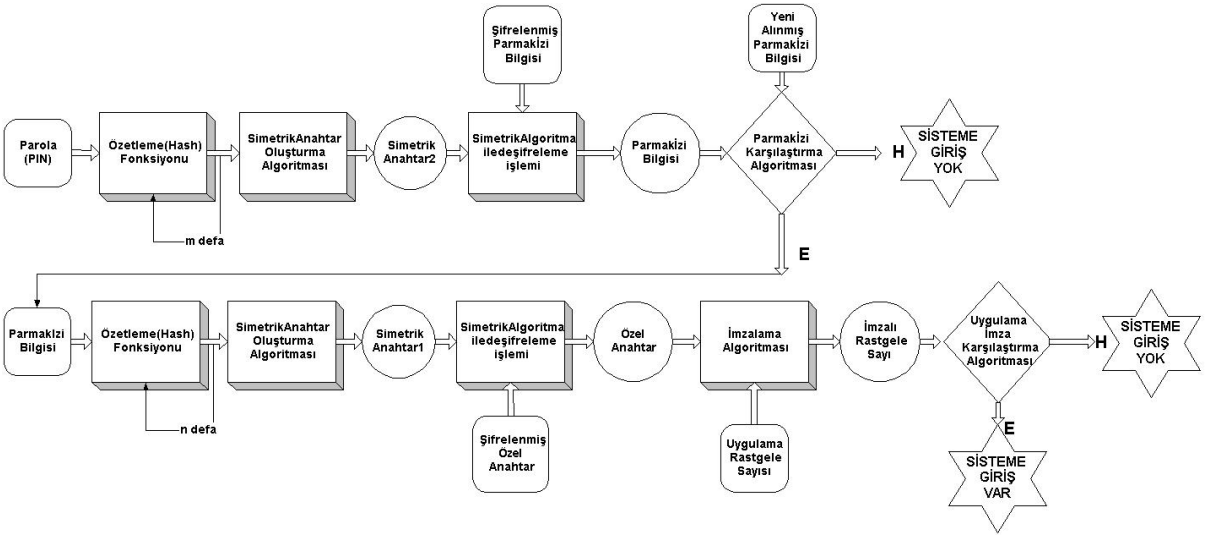
3 PARMAKİZİ TARAYICISI DESTEKLİ AKILLI KART ÇÖZÜMÜ

Yukarıda incelenen bütün depolama yöntemlerinde özel anahtar bir paroladan elde edilen bir şifreleme anahtarı ve bir simetrik algoritmayla şifrelenerek saklanmaya çalışılır. Kullanıcı, sisteme doğru parolayı girerek yetki elde ettiğinde bir takım alt kriptografik uygulamalara ulaşır ve imzalama, şifreleme gibi işlemleri yapabilir. Sonuçta eğer bir saldırgan da gerekli parolayı bir şekilde ele geçirirse herhengi bir kullanıcıdan farkı kalmaksızın çeşitli kriptografik işlemleri yapabilir. Burada eksik bırakılan sadece kullanıcının sahip olduğu biyometrik özelliklerin ölçülerek bu yetkilendirme işlemine katılamamasıdır. Bu işlemler parmakizi taraması, ses veya yüz taraması, dokulardan DNA karşılaştırması, retina ya da kornea taramasıdır. Bunlardan en eski ve kabul görmüş olanı parmakizi taramasıdır. Her parmağın kendine özgü karakteristik eğrileri vardır. Bu eğrilerin görüntülenmesiyle parmakizi elde edilir. Bu data kullanılan parmakizi algoritmasına göre 256 – 2048 bit arasında değişebilir. Elde edilen bu datadan tekrar parmakizi görüntüsü elde etmek imkansızdır. Bu data tekrar tarama sonucunda elde edilen bilgiyle parmakizi algoritması yardımıyla karşılaştırma işlemi yapmak için saklanır. Eğer bu parmakizi datasını bir akıllı kart üzerinde saklarsak, sadece parolaya bağlı basit yetkilendirme işleminden kurtularak kullanıcının sahip olduğu bir özellikten faydalanıp daha sağlıklı bir yetkilendirme kontrolü yapmış oluruz. Bu amaçla tasarlanan anahtar üretimini de içine alan yöntemde akıllı kart olarak üzerinde mikroişlemcisi ve donanımsal rastgele sayı üreteci olan bir kart kullanılmıştır.. Parmakizi tarayıcısı olarak da termal (ısıya duyarlı) bir tarayıcı seçilmiştir.

3.1 Kullanıcının Sisteme Tanıtılması, Anahtarın Üretilmesi ve Saklanması

1. Kullanıcı akıllı kartını kart okuyucusuna yerleştirir. Akıllı kart herhangi bir anahtar ya da data içermemektedir.
2. Anahtar çifti akıllı kart üzerinde donanımsal rastgele sayı üretecinden faydalanılarak üretilir.
3. Kullanıcıdan kişisel bilgileri ile birlikte parmakizi tarayıcısından parmakizi alınır.
4. Kullanıcıdan 6 – 18 karakterlik bir parola istenir.
5. Parmakizi bilgisinden kriptografik karıştırma ve ekleme yöntemleri kullanılarak bir simetrik anahtar oluşturulur [4]. Bu simetrik anahtar simetrik algoritma ile kullanılarak özel anahtar koruma altına alınır. Özel methodla şifrelenen özel anahtar akıllı kart üzerinde saklanır.
6. Girilen paroladan başka bir yöntemle diğer bir simetrik anahtar oluşturulur. Bu simetrik anahtar ve farklı bir simetrik algoritmayla parmakizi bilgisi şifrelenerek akıllı kart üzerinde saklanır.
7. Açık anahtar ise kullanıcının bilgisayarına, bir sertifika otoritesi tarafından sertifikalandırılmak üzere gönderilir. Veritabanında kullanıcı bilgileri ile birlikte tutulur.

Sonuçta kullanıcının anahtar çifti akıllı kartta üretilmesi ile özel anahtarının hiç bir şekilde akıllı kartı terketmemesi sağlanmış olur. Akıllı kart



Şekil 2: Kullanıcının yetki kontrolü ve özel anahtarının kullanıma açılması.

içerisinde de şifrelenerek saklanır. Açık (public) anahtar ise gerektiğinde sertifikalandırılmak ve diğer kullanıcılarla paylaşmak için bilgisayara aktarılır. Sertifikalandırılmış açık anahtar daha sonra akıllı karta da kopyalanabilir. Bu şekilde kullanıcı, ihtiyacı olduğunda sertifikasını akıllı kartından diğer kullanıcıların bilgisayarlarına kopyalayabilir.

3.2 Kullanıcının Yetki Kontrolü ve Özel Anahtarının Kullanıma Açılması

1. Kullanıcı akıllı kartını kart okuyucusuna yerleştirir. Akıllı kart kullanıcının özel anahtarını ve parmakizi bilgisini içermektedir.
2. Kullanıcıdan daha önce sisteme girdiği parolası istenir. Bu parola yardımıyla şifrelenmiş parmakizi bilgisi deşifre edilir.
3. Kullanıcının parmakizi taraması tekrar yapılır. Elde edilen parmakizi bilgisi, akıllı kart üzerinde şifresi çözülen parmakizi bilgisiyle karşılaştırılır.
4. Parmakizleri tutmuyorsa kullanıcının sisteme girişi engellenir. Parmakizleri tutuyorsa akıllı kart üzerinde şifresi çözülen parmakizi bilgisinden simetrik anahtar tekrar oluşturulup özel anahtarın şifresi çözülür.
5. Uygulama tarafından bilgisayarda random sayı üretilip akıllı karta gönderilir.
6. Akıllı kart içerisinde bu rastgele sayı özel anahtarla imzalanıp bilgisayara geri gönderilir.
7. Uygulama sertifikalandırılmış açık anahtarla bu bilgiyi deşifre eder ve gönderdiği rastgele sayı ile karşılaştırır.Eğer aynıysa yetkilendirme işlemi tamalanmıştır. Eğer tutmuyorsa yetkilendirme verilmez.

Bu yöntem sayesinde kartın sahibinin gerçekten kartın gerçek sahibi olup olmadığı tereddüde meydan vermeyecek şekilde anlaşılmış olur. Sadece parolayı bilmesi ya da sadece parmak izi sahteciliği yapması ki oldukça zor işe yaramayacaktır.Bundan sonra yapılacak imzalama işlemleri (yani özel anahtarın kullanılması) gene akıllı kartın içerisinde yapılacaktır. Hiçbir şekilde özel anahtar akıllı kartı terketmeyecektir. Uygulamanın bu şekilde gerçeklenmesi maksimum güvenliği sağlayacaktır.

4 SONUÇ

AAA uygulamalarında gerek sertifika otoritesinin gerek de kullanıcıların özel anahtarlarının üretilmesi ve saklanması sistemin en zayıf ve önemle çözülmesi gereken bir problemidir.

Şu ana kadar tasarlanan sistemlerin çoğunda özel anahtarın korunması için sadece parola ya da PIN (something you know) kullanıldı. Geri kalan az bir kısmında ise akıllı kartlar, jetonlar (something you have) kullanılmaya başlandı.

Bu çalışmada önerilen çözümde ise, kullanıcıya ait özelliklerin de (something you are) yetkilendirmede gözönünde bulundurulması ve bunun akıllı kart ve parola ile entegre edilmesi üçlü bir güvenlik seviyesi oluşturdu.

Zaten en yüksek güvenlik seviyesi üç faktörlü yetkilendirmeyi birlikte kullanır: bildiğin bir şey, sahip olduğun bir şey ve kendine ait bir şey.

KAYNAKLAR

[1 Ellison, Schneier, Ten Risks of PKI: What You're not Being Told about PKI, Computer Security Journal, Number 1, 2000/Vol. 16 pp 1-8

[2] Ortiz, Will PKI Become a Key to Online Security, Industry Trends, December 2000, pp 13-15

[3] Henry, D., Who's Got the Key? , SIGUCCS 1999, Denver, Colorado.

[4] Schneier, B., 1996. Applied Cryptography, John Wiley & Sons Inc., New York.