Bir Açık Anahtar Altyapısı Nasıl Planlanmalı?

Ersin GÜLAÇTI
TÜBİTAK UEKAE, Gebze/Kocaeli
egulacti@uekae.tubitak.gov.tr

ÖZET : Bu makalede açık anahtar altyapısı (AAA) sistemleri tasarlanırken ve gerçeklenirken dikkat edilmesi gereken konular ele alınmaktadır. Bir AAA sistemi kuracak kuruma yol göstermek amacıyla "Neden AAA Kurulur?", "Kurulacak AAA Sistemi Kaç Kişiye Hizmet Verecek?", "Hangi AAA Hizmetleri Sunulacak?", "AAA Hizmetleri Kim Tarafından Sunulacak?", "AAA Mimarisi Nasıl Olacak?", "Hangi AAA Ürünleri Seçilecek?" gibi sorulması gerekli sorular ve bunların olası cevapları ele alınmaktadır.

ANAHTAR KELİMELER: Açık Anahtar Altyapısı (AAA), Elektronik İmza, Elektronik Sertifikalar, Elektronik Sertifika Hizmet Sağlayıcısı, Kriptografi

How to Plan for a Public Key Infrastructure?

ABSTRACT : This article covers topics which should be considered during planning and implementation of a public key infrastructure (PKI) system. An organization which will establish a PKI system should ask a number of questions which should be answered clearly. "Why do you establish a PKI?", "How many clients the PKI system will serve?", "Which PKI services will be provided?", "Who will provide the PKI services?", "What will be the PKI architecture?", "Which PKI products should be selected?" are among the questions explored in the article.

KEYWORDS : Public Key Infrastructure (PKI), Electronic Signature, Digital Certificates, Electronic Certificate Service Provider, Cryptography

Giriş

Açık Anahtar Altyapısı (Public Key Infrastructure - PKI) (AAA) bilgi güvenliğini sağlamak için yaygın olarak kullanılan ve temelinde açık anahtar kriptografisi bulunan sistemlere verilen isimdir. AAA içinde çeşitli kriptografi algoritmaları ve bunlarla bağlantılı protokoller kullanılmaktadır. AAA sistemleri planlanırken ve gerçeklenirken dikkat edilmesi gereken, ağırlıklı olarak idari ve işletme alanlarında karşılaşılan sorunlar AAA projelerinin başarısı açısından çok büyük önem taşımaktadır.

Bu makalede bir AAA sistemi planlanırken, gerçekleştirilirken ve işletilirken dikkat edilmesi gereken noktalar ele alınacak ve çeşitli öneriler aracılığıyla okuyuculara yaşanmış tecrübeler aktarılacaktır. Konular ele alınırken AAA sistemlerinin teknik yönlerine sadece gerektiğinde değinilecektir.

Neden AAA Kurulur?

Bir AAA sistemi kurulmasının nedeni, çeşitli bilgi güvenliği hizmetlerinin belli bir grup insana ve kuruma sunulması ihtiyacıdır. Bu güvenlik hizmetleri aşağıdaki başlıklar altında toplanabilir:

- Gizlilik
- Veri Bütünlüğü
- Kimlik Doğrulama
- İnkâr Edemezlik

Bu hizmetler günlük hayatta elektronik imza ve veri şifreleme olarak somutlaşmaktadır.

Bilgi güvenliği hizmetlerine duyulan ihtiyaç çeşitli kaynaklar tarafından gündeme getirilebilir. Örneğin ABC firması için :

- Firmanın Bilgi Sistemleri Bölümü, kurum içi işlemlerde güvenlik için
- Firmanın Müşterileri, Internet üzerinden yapılan işlemlerin güvenliği için
- Firma Üst Yönetimi, elektronik sertifika satacak bir Elektronik Sertifika Hizmet Sağlayıcısı (ESHS) kurmak için

bir AAA kurulmasını isteyebilirler. Yukarıda sayılan nedenler dışında dile getirilmeyen veya başka nedenlerin arkasına saklanan gerekçeler de olabilir. Bu gerekçeler arasında,

- Teknolojinin popüler olması nedeniyle projeyi yapmak isteyen bölüme cazip gelmesi
- Rakip firmaların AAA sistemi kurmuş olmaları
- Kurumda AAA hakkında çok büyük beklentilerin olması (Birçok bilişim teknolojisi sorununun çaresi olarak pazarlanması ve görülmesi)

sayılabilir.

Öznel bir değerlendirmeyle başlanacak AAA projelerinin başarıya ulaşma şansı düşüktür. Bu nedenle nesnel değerlendirme için projenin hazırlık aşamasında aşağıdaki bölümlerde ele alınan soruların cevaplarının bulunması ve bu cevaplara göre karar alınması gerekir.

Kurulacak AAA Sistemi Kaç Kişiye ve/veya Cihaza Hizmet Verecek ?

Hizmet alacak kişilerin bilgisayar teknolojileri bilgisinin hangi düzeyde olduğu çok önemlidir. Sadece bilgisayar okuryazarlığı olan son kullanıcılara karmaşık sertifika kuralları ve kullanımı zor AAA yazılımları ürkütücü gelecektir.

AAA yazılım üreticileri, yazılımlarının ve sundukları bilgi güvenliği hizmetlerinin olabildiğince basit ve anlaşılır olması için çok çaba harcamakta ve mesafe kat etmektedir. Bu duruma rağmen hala AAA yazılımları son kullanıcıların çok fazla teknik konudan anlamasını gerektirmektedir. Normal kullanım sırasında şeffaf bir şekilde çalışan AAA yazılımları meydana gelen sıra dışı durumlarda kullanıcıya sordukları sorularda gerçek yüzlerini göstermektedirler. Eğer kullanıcıların bu sorulara cevap bulmasına yardımcı olacak yetişmiş AAA destek personeli yoksa kullanıcıların cevaplarının ve yazılımları kullanım şeklinin hatalı olacağını varsaymak yanlış olmayacaktır.

Eğer kurulacak AAA tarafından çoğunlukla cihazlar için sertifika üretimi yapılacaksa (SSL, VPN vb.), bu cihazları işletenlerin AAA teknolojileri hakkında bilgi birikimi veya eğitimi olması gerekecektir. Bu durum son kullanıcıların destek ihtiyacından farklı olmakla beraber yine de piyasada bulunan çok sayıda farklı cihaz ve sunucu için sertifika talebi üretme, bu sertifikaları sisteme yerleştirme gibi konularda cihaz/sunucu işleticilerinin de uygun seviyede desteklenmesi gerekir.

Hangi AAA Hizmetleri Sunulacak?

Kurulacak sistemden hangi hizmetlerin verileceği planlama için çok önemlidir. Verilecek hizmetler sertifika üretimi ile sınırlı olabileceği gibi özellikle kurum içi AAA uygulamalarında üretilen sertifikaların kullanıldığı e-posta ve dosya güvenliği yazılımlarının kullanıcı bilgisayarlarına yüklenmesi ve işletilmesi de önemli bir hizmet kalemi olarak ortaya çıkmaktadır. Aşağıdaki hizmet listesi bu konuda yol gösterici olacaktır:

- Sertifika Üretimi ve Yaşam Döngüsü
  - Elektronik İmza Sertifikaları
  - Şifreleme Sertifikaları
  - SSL Sertifikaları
- Zaman Damgası Sunucu Hizmeti
- OCSP Sunucu Hizmeti
- E-Posta İçin Elektronik İmza ve Şifreleme İstemci Yazılımı
- Dosya Ve Klasörler İçin Elektronik İmza ve Şifreleme İstemci Yazılımı
- Zaman Damgası İstemci Yazılımı

AAA hizmetlerinin işletilmesi nispeten kolay olan bölümü sunucu tarafıdır çünkü sunucuların yaptığı işlemler iyi tarif edilmiştir. Ayrıca sunucu donanım ve yazılımları bu işin eğitimini almış işletme personeli tarafından kullanılır.

AAA hizmetlerinin son kullanıcılar tarafından kullanıldığı ortamlarda kullanıcıların çok farklı yazılım ve donanım kombinasyonlarıyla çalışıyor olması önemli bir sorun kaynağıdır. Kullanıcılar ayrıca çok çeşitli uygulamaların içinden AAA hizmetlerini kullanmak isteyebilirler ve sistemlerini önceden öngörülemeyen durumlara getirebilirler. Kullanıcı bilgisayarları için bir yönetim ve kullanım politikası belirlenmemiş kurumlarda AAA politikalarından bahsetmek ve uygulamak da mümkün olmayacaktır. Bu tip kurumlarda son kullanıcı bilgisayarlarında güvenlik açıkları ve ihlalleri de yaygın olarak görülür. Bu tür açıklar ve ihlaller AAA yazılımları ile sağlandığı düşünülen güvenlik mekanizmalarının devre dışı kalmasına neden olabilirler.

AAA Hizmetleri Kimin Tarafından Sunulacak?

AAA hizmetleri kurum içinde oluşturulacak bir birim tarafından verilebilir veya kurum dışından kaynak kullanılarak bu hizmetler alınabilir. Bu konuda karar verirken maliyet ve güvenlik ön plana çıkmaktadır. Kullanıcı başına AAA maliyeti hangi seçenekte ucuz oluyorsa o tercih edilebilir, ancak güvenlik ihtiyaçlarının çok üst düzeyde olduğu kurumlarda AAA hizmetlerinin kurum içinde üretilmesi bir zorunluluk olabilir. Kullanıcı başına maliyet hesaplanırken ilk satın alma maliyeti dışında, yıllık lisans ve bakım bedeli, destek hizmeti bedeli de dikkate alınmalıdır.

Bazı durumlarda zorunlu olarak hizmetler kurum dışından alınabilir. Buna güzel bir örnek T.C. 5070 Sayılı Elektronik İmza Kanunudur. Bu kanuna uygun

güvenli elektronik imza oluşturmak için Telekomünikasyon Kurumu (TK) tarafından yetkilendirilmiş bir ESHS'ndan elektronik sertifika hizmeti satın almanız gereklidir. Türkiye'de Kamu Kurumları bu kanuna ek olarak 2004/21 Sayılı Başbakanlık Genelgesi uyarınca Nitelikli Elektronik İmza sertifikalarını Kamu Sertifikasyon Merkezi'nden almak zorundadırlar (İstisnai hak tanınan 6 kurum dışında).

Kurum dışından hizmet alınırken genelde iki alternatif vardır. Bunlardan birincisi sertifikaları kurum dışından ticari olarak hizmet veren bir ESHS'ndan almak, ikincisi ise kendi kurumunuza ait ESHS faaliyetlerini bu konuda uzmanlaşmış bir firmaya yaptırtmaktır. Birinci yöntem genel olarak kabul görmüş olan yoldur. İkinci yöntemde ESHS kök sertifikası sizin kurumunuzun adını taşıyabilir. Bu tip hizmet alınacak dış firmaların çok titiz bir şekilde seçilmesi gerekir çünkü hizmeti verecek firma sizin adınıza kök anahtar çiftini barındıracaktır. Bu anahtar çiftinin emniyeti ve doğru kullanılması çok önemlidir.

AAA hizmetleri kurum içindeki bir birim tarafından sunulacaksa burada çalışacak yeterli sayıda personelin görevlendirilmesi gereklidir. Bu personelin kaliteli hizmet verebilmesi için iyi bir eğitim alması gerekir, çünkü AAA hizmetleri DH, RSA, DSA, ECDSA gibi asimetrik kriptografi algoritmaları, DES, RC2, AES gibi simetrik kriptografi algoritmaları, SHA1, SHA2, RIPEMD160 gibi özetleme algoritmaları, SSL, CMP, OCSP gibi protokolleri kullanır. Bu algoritma ve protokollerin nasıl kullanılacağını anlatan RSA PKCS 1, IETF RFC 3280, ITU.T X.509, S/MIME birçok standart da AAA sistemleri tarafından gerçeklenir. Bu çok teknik ve detaylı alanda hizmet verecek personelin iyi bir bilgi birikimine sahip olması şarttır.

Hizmet Seviyesi Beklentisi Nedir?

Kurulacak olan AAA sisteminden beklenen hizmet seviyesi en baştan tespit edilmelidir. 7 gün / 24 saat çalışması beklenen bir sistemdeki sertifika yönetim birimi ve destek masası ile sadece mesai saatleri içinde çalışacak bir sistemin birimleri aynı yapıda olmayacaktır. Eğer profesyonel bir ESHS olarak çalışılacaksa kurulacak sistem içerisinde çağrı merkezi de yer alması gerekebilir.

Kurulacak donanım ve yazılım altyapısının beklentileri karşılayacak düzeyde olması gerekir. Hizmet sürekliliği istenen ve yoğun yük altında kalacak sistemler için yedekli çalışacak yapılar düşünülmelidir. Ayrıca felaket durumlarında kullanılmak üzere ayrı bir fiziki ortamda yedek tutulması da gerekebilir.

AAA kurulacak kurumda mevcut olan bilgi sistemleri altyapısı (veritabanı sistemleri, dizin sunucuları, bant genişliği, sunucu işlem gücü vb.) istenen hizmeti vermeye yetecek düzeyde değilse bu alanda eksiklerin giderilmesi için yatırım yapılması gerekecektir.

AAA'nın hizmet vereceği ağ Internet'e açık olabilir veya kurum içi bir Intranet üzerinde de hizmet verilebilir. Her iki durumda da hem güvenlik hem de haberleşmenin sürekliliği için gerekli tedbirlerin alınması gerekir. Alınacak başlıca önlemler arasında AAA sunucularının çevrim dışı olması veya güvenlik duvarları ve saldırı tespit sistemleri ile korunan ağ bölgelerinde çalıştırılması sayılabilir.

AAA Mimarisi Nasıl Olacak?

Kurum içi hizmet verecek bir AAA için tek bir sertifikasyon makamı sunucusu kurulması ve tüm sertifikaların bu sunucu tarafından üretilmesi yeterli olacaktır. Eğer AAA kurulacak kurum coğrafi olarak birbirinden uzak noktalarda birimleri bulunan bir yapıdaysa ve birimler arasında haberleşme güçlükleri varsa AAA mimarisi bir kök sertifikasyon makamı ve ona bağlı alt birim sertifikasyon makamları şeklinde de gerçeklenebilir. Eğer kurum içi birimler özerk bir yapıda çalışıyorlarsa ayrı sertifikasyon makamlarına sahip olmaları tercih edilebilir.

Çapraz sertifikasyon ve köprü sertifikasyon kullanımı düşünülürken bu konuda AAA ürünleri arasında tam bir uyum olmama ihtimali göz önünde tutulmalıdır. Çapraz ve köprü sertifikasyon uygulamaları için sisteme dahil olacak sertifikasyon makamları ve AAA uygulama yazılımlarının aynı üreticiden veya birbirine uyumlu üreticilerden tedarik edilmesi daha doğru olacaktır.

Mimari yapıya karar verirken en önemli kıstaslardan birisi de maliyet ve personel ihtiyacı olacaktır. AAA sistemlerinin yüksek maliyetli ve işgücü gerektiren bir yapıda olduğu unutulmamalıdır. Kurulacak her bir sertifikasyon makamı toplam maliyeti arttıracaktır.

AAA Ürünleri Nasıl Seçilecek?

İhtiyaç duyulan hizmetin içeriğine, güvenlik seviyesine ve proje bütçesine göre AAA için kullanılacak sunucu ve istemci yazılımları, akıllı kartlar/çubuklar ve donanımsal güvenlik modülleri (Hardware Security Module – HSM) seçimi yapılmalıdır. Eğer kurum içinde yüksek güvenlik düzeyine ihtiyaç duyulmayan bir AAA sistemi kurulacaksa sertifikasyon makamı yazılımı olarak 0 (sıfır) maliyetli ürünler cazip görünecektir. Bu tür ürünlerin destek maliyetinin (işgücü ve zaman) olarak aslında 0 olmadığı göz önünde bulundurulmalıdır.

Kullanıcılar için asimetrik anahtar ve sertifika saklama aracı için en güvenli yöntem akıllı kart veya akıllı çubuk kullanmaktır. Sertifikasyon makamı anahtarlarını saklamak için HSM kullanmak güvenliği büyük ölçüde arttıracaktır. Bu ürünleri seçerken

değerlendirme tabloları üstünde puanlama yapmak faydalı olacaktır. Bu amaçla Gülaçtı [1] tarafından hazırlanan tablo kullanılabilir.

Hukuki Bağlayıcılık

Türkiye'de AAA ile ilgili kanuni düzenlemeler 5070 Sayılı Elektronik İmza Kanunu ve buna bağlı ikincil mevzuat ile sınırlıdır [2]. Bu düzenlemeler kanun karşısında elle atılan ıslak imzaya denk olan güvenli elektronik imzayı ve bu tür imzalar için gerekli altyapıyı ve kuralları tarif eder. Elektronik imza ve AAA teknolojisi ile ilgili henüz mahkemelere yansımış ve emsal teşkil edecek bir dava yoktur.

5070 Sayılı kanuna göre güvenli elektronik imza kesin delil niteliği taşımaktadır ve bu tür delillerin mahkemeler tarafından kullanılması zorunludur. Eğer bir kurum kendi içinde kuracağı ESHS ile üretilen sertifikaları kullanarak elektronik imza uygulaması yapmak istiyorsa dikkatli davranmak zorundadır. Bu tür bir sistemde oluşturulacak elektronik imzalar kesin delil niteliği taşımamaktadır. Konuyla ilgili hukukçuların yorumlarına göre bu tür elektronik imzalar davaya bakan mahkeme heyetinin takdirine göre delil olarak kabul edilebilir veya ret edilebilir.

ESHS Olarak Hizmet Verilecek mi?

Eğer AAA sistemini kurmak isteyen kurum bu işi yasal bir ESHS olarak yapmak istiyorsa daha önceki bölümlerde belirtilen sorulara ek olarak aşağıdaki soruların cevaplarını da araştırmalıdır:

- Bilgi Güvenliği Yönetim Standardı ISO 27001'e göre sertifikasyonu nasıl alacağız ?
- Ticari olarak çalışılacaksa, sertifika ve hizmet satışı gerçekleştirilecek potansiyel müşteri sayısı nedir?
- Yapılan yatırımın geri dönüş süresi ne kadar olacak?
- AAA hizmetleri pazarının toplam hacmi ve yıllık büyüme oranı nedir?

Sonuç

AAA teknolojisinin temeli olan ilk açık anahtar kriptografik algoritması Diffie ve Hellman [3] tarafından ortaya konulduğundan bu yana 30 yıl geçti. Ticari AAA hizmetlerinin başlamasından bu yana ise 12 yıl geçti (Entrust–1994 [4], Verisign–1995 [5]). Bu yıllar boyunca AAA sistemlerinin patlama yapacağı ve çok yaygın kullanıma gireceği söylemlerinin yoğunlaştığı dönemler oldu. Yaşanan tecrübeler ise AAA sistemlerinin kurulmasının ve işletilmesinin karmaşık, çok zaman alan ve toplamda pahalı olan projeler olduğunu ortaya koydu. "Bu olumsuz özelliklerine rağmen niye AAA sistemleri hala kullanılmakta?" sorusunun cevabı "İhtiyaç duyulan güvenlik hizmetlerini sunan daha iyi bir çözümün bulunmamış olmasıdır."

Yukarıda anlatılanlar AAA sistemlerinin ne kadar ciddi planlanması gerektiğini vurgulamak için dile getirilmiştir. Bir AAA sistemi kurulması projesini sıradan bir bilgi teknolojisi (BT) projesi olarak algılamak ve yeterince önem vermemek yapılabilecek en kötü harekettir. Bu tür yaklaşımların sonucunda başlanan AAA projelerinde başarı oranının %50 ve altındaki seviyelerde kaldığı rapor edilmiştir (Örnek için bak. [6]).

Kurulan AAA ile hizmet verilecek kişi sayısı arttıkça ve bu kişilerin fiziksel olarak bulundukları yerler farklılaştıkça projenin güçlüğü artmaktadır. AAA projelerinde mümkün olduğunca bu işte uzmanlaşmış kurumlardan, kişilerden danışmanlık almak gereklidir. Bu makalede bahsedilen soruların ve daha fazlasının cevapları hazır olmadan AAA kurma kararı alınmamalıdır. Son olarak AAA sisteminin ilk satın alma maliyetini değil toplam sahip olma maliyetini hesaplamak başarılı bir proje için şarttır.

Kaynaklar

[1] Gülaçtı, Ersin, "Anahtar Saklama Yöntemleri Karşılaştırması", Teknik Rapor, TÜBİTAK UEKAE, 2005

[2] http://www.tk.gov.tr/eimza/eimza_mevzuat.htm, 5070 Sayılı Elektronik İmza Kanunu ve İlgili Yönetmeliklerin toplu olarak bulunduğu adres

[3] Diffie,W., Hellman,M.E., New Directions in Cryptography, IEEE Transactions on Information Theory, vol. IT-22, Kasım. 1976, sayfa: 644-654.

[4] Entrust Tarihçesi (Entrust History), http://www.entrust.com/corporate/history.htm

[5] Verisign Tarihçesi (Verisign History), www.verisign.com/static/036566.pdf

[6] Kanada Hükümeti, AAA Tarama Raporu 31.05.2005, http://www.solutions.gc.ca/pki-icp/pki-in-practice/efforts/2005/05/scan-analyse_e.pdf