Türkiye için bir *Açık Anahtar Altyapısı Modeli*

A Public Key Infrastructure Model for Turkey

ÖZET

Internet üzerinde, açık anahtar tabanlı şifreleme algoritmaları kullanan güvenli elektronik ticaret, güvenli elektronik posta gibi uygulamaların yaygınlaşması ile birlikte, açık anahtarların belirli bir düzende tutulması gereği ortaya çıkmıştır. Bu düzen, açık anahtar altyapısı olarak anılmaktadır. Bu bildiride, Türkiye için, Türkiye koşullarına ve uluslarası standartlara uygun bir açık anahtar altyapısı için taslak bir model önerilmiştir. Bu model aynı zamanda, çeşitli uygulamaların açık anahtar altyapılarını bir çatı altında toplayabilecektir. Ancak, bu bildiri ile temelleri verilen modelin gerçeklenmesi için daha geniş bir platformda detayların tartışılması ve daha kapsamlı finansal, teknik ve hukuksal çalışmalar gerekmektedir.

ÖZGEÇMİŞ

Albert Levi
1969 yılında İstanbul'da doğdu. Boğaziçi Üniversitesi Bilgisayar Mühendisliği bölümünden 1991'de lisans, 1993'da yüksek lisans derecelerini aldı. Şu anda Boğaziçi Üniversitesi, Bilgisayar Mühendisliği Bölümü'nde doktora çalışmalarına devam etmekte ve araştırma görevlisi olarak çalışmaktadır. E-posta: levi@boun.edu.tr

M. Ufuk Çağlayan
1951'de Ankara'da doğdu. 1973'te ODTÜ Elektrik Mühendisliği bölümünden lisans, 1975'te ODTÜ Bilgisayar Mühendisliği bölümünden yüksek lisans derecelerini aldı. 1981'de Northwestern Üniversitesi'nde doktorasını tamamladı. Yurt içi ve dışında çeşitli üniversitelerde öğretim üyeliği yaptıktan sonra şu anda Boğaziçi Üniversitesi, Bilgisayar Mühendisliği Bölümü'nde profesör olarak görevini sürdürmektedir. E-posta: caglayan@boun.edu.tr

ABSTRACT

Starting with the widespread usage of public key based applications, like secure electronic commerce and secure electronic mail, the necessity of an order for the public key storage has been evolved. This order is called as the Public Key Infrastructure. In this paper, we proposed a draft model for a public key infrastructure for Türkiye which comforts Türkiye conditions and the international standards. This model will be able to combine the public key infrastructures of different applications under the same roof as well. However, in order to implement the model, for which the base is given in this paper, the details should be discussed in a larger platform and more detailed technical, economical and legal studies are necessary.

Türkiye için bir Açık Anahtar Altyapısı Modeli

1. *GİRİŞ*

Internet kullanımının askeri alandan sivil alana kaymasıyla beraber, WWW, e-posta, elektronik ticaret gibi medya olarak Internet'i kullanan çeşitli uygulamalar geniş kitlelere yayılmıştır. Bu durum, açık bir ağ olan Internet'te çeşitli güvenlik sorunlarını [4] da beraberinde getirmiştir. En büyük güvenlik tehdidi, yetkisiz kişilerin sunuculara sızıp bilgi hırsızlığı yapması veya bilgilere zarar vermesidir. Bu sorunun çözümünde kullanılan klasik kullanıcı adı – şifre (username – password) yöntemleri artık yeterli olamamaktadır, çünkü ağı dinleyen biri tamamıyle açık olan kullanıcı adı ve şifrelerini görebilir. Bu sorunu önlemek için Kerberos [1], Secure SHell (SSH), Yaksha gibi sistemler geliştirilmiştir. Lokal ağı genel olarak dış tehditlerden korumak için ateş duvarları (firewalls) [2] yazılımları da yaygın olarak kullanılmaktadır.

Internet'teki güvenlik isterlerinden biri de ağ üzerinde dolaşan bilginin sadece istenen insanlar tarafından görülebilmesinin sağlanmasıdır. Kısaca *kişisellik* olarak adlandırılan bu isteri sağlamak için önerilen sistemlerin hepsi şifreleme bilimine (cryptography) [3] dayanmaktadır. Çözümü şifrelemeye dayalı diğer bir güvenlik isteri ise *kimlik kanıtlama*dır (*authentication*). Kimlik kanıtlama, ağ üzerinde işlem yapan bir kullanıcının gerçekten iddia ettiği kişi olduğunu karşı tarafa ispatlamasıdır. Bunun bir ileri aşaması ise işlem yapan kullanıcının yaptığı işlemi hiçbir zaman *inkar edememe*si (*non-repudiation*) isteridir. Kimlik kanıtlama ve inkar edememe sistemlerinde kullanılan en yaygın teknik *sayısal imzalama* (*digital signatures*) tekniğidir. Sayısal imza, bir iletinin şifreleme yöntemlerini kullanan bir işlemden geçirilmesi sonucunda oluşan sayısal bir bilgidir. Buradaki en önemli özellik, imzayı sadece ileti sahibinin yaratabilmesi ve bir başkasının bu imzayı taklit edememesidir. Bundan başka, herhangi bir alıcının imzalanmış iletiyi aldığında, üzerindeki imzayı konrol edip doğrulayabilmesi de gerekmektedir. Bu şekilde bir sayısal imza sistemi ancak *açık anahtar* (*public key*) tabanlı şifreleme algoritmaları kullanılarak kurulabilir.

1976'da Diffie ve Hellman'ın [5] temellerini attığı açık anahtar tabanlı şifreleme algoritmalarının en önemli özelliği herkesin iki tane anahtarının olmasıdır. Şifreleme için kullanılan açık anahtar (public key) ve şifreyi çözmek için kullanılan gizli anahtar (secret key) farklı anahtarlardır ve birinden diğerini elde etmek imkansızdır. Bu yüzden, açık anahtarların herkesçe bilinmesinde bir sakınca yoktur. Açık anahtar tabanlı sistemlerde bir kişi kendi gizli ve açık anahtarını kendisi yaratır ve açık anahtarını yayınlar, gizli anahtarını ise saklar. Açık anahtarın gizli olması gerekmediği için bu dağıtım işleminin gizli ve özel kanallardan olmasına da gerek yoktur.

Açık anahtar tabanlı sistemlerde şifreleme kullanıcının açık anahtarı ile yapılır, şifreyi çözme ise yine aynı kullanıcının gizli anahtarı ile mümkündür. Bu yüzden, bir şifreyi ancak sahibi çözebilir. Bir iletiyi sayısal olarak imzalamak için ise imzalayanın gizli anahtarı kullanılır. Aynı imzayı doğrulamak için imzalayanın açık anahtarını bilmek yeterlidir. Bir sayısal imza ancak gizli anahtar ile oluşturulabildiğinden, aynı imza bir başkası tarafından taklit edilemez veya başka bir iletiye uyarlanamaz.

Açık Anahtar kullanımının önündeki en önemli sorun insanların yanlış açık anahtar kullanmaları yönünde kandırılmalarıdır. Bu bildirinin ileri kısımlarında daha detaylı olarak incelenecek bu sorunun çözümünde yaygın olarak kullanılan yöntem *sertifikasyon* (*certification*) yöntemidir. Sertifika, bir kullanıcının açık anahtarının o kullanıcıya ait olduğunu gösteren sayısal bir belgedir. Bu belge güvenilir bir kişi tarafından sayısal olarak imzalanır. Sertifika imzalayan güvenilir kişilere *Sertifika Otoritesi* (*SO*) denilmektedir. Bir SO'ya güvenen ve onun açık anahtarını bilen bir kullanıcı, SO'nun imzaladığı sertifikayı doğrulayabilecektir. Böylelikle, sertifika içinde bahsi geçen kişinin doğru açık anahtarı da öğrenilmiş olur.

Internet gibi milyonlarca kullanıcısı olan bir ağda bir tek SO'nun yeterli olmayacağı açıktır. Gerçekten de sertifika sisteminin etkili bir şekilde kurulabilmesi için çeşitli SO'ların, belirli bir düzende ve birbirleriyle etkileşimli olarak çalışacağı bir küresel yapı oluşturması gerekmektedir. Bu yapı, *Açık Anahtar Altyapısı* (*AAA*) (*Public Key Infrastructure*) olarak adlandırılmaktadır. AAA'ların önemi, açık anahtar tabanlı algoritmalar kullanan güvenli e-posta, elektronik ticaret ve ödeme, elektronik bankacılık gibi uygulamaların yaygınlaşmasıyla daha da belirginleşmiştir. Açık anahtar tabanlı şifreleme algoritmaları ve AAA kullanımı, yakın bir gelecekte güvenli uzaktan oylama, dağıtık açık artırma, elektronik iş ve döküman takibi gibi değişik sanal uygulamalarda da kendini gösterecektir. Bir AAA'nın topolojisinin ne olması gerektiği konusunda çeşitli tezler vardır. Bu bildirinin ileri kısımlarında sertifika kavramı, SO'lar, AAA'lar ve bunlarla ilgili konularda daha detaylı bilgiler verilecektir.

Bu bildiride, Türkiye için bir ulusal AAA modeli oluşturmak amacıyla bir çerçeve çalışma yapılmıştır. Bunun için öncelikle varolan temel sertifika ve AAA yapıları incelenmiştir. Önerilen modelde, uluslararası bir standart olan X.509 sertifika standardına uygun yapılar kullanılması tercih edilmiştir. Bunun nedeni ise, bir ulusal AAA'nın, küresel AAA ile uyumlu bir şekilde çalışması gerekliliğidir. Ayrıca bu bildiride, standartlarla belirlenmeyen ve her ulusal AAA'nın kendi ekonomik, sosyal ve hukuksal şartlarına göre belirleyeceği hususlar için de önerilerde bulunulmuştur. Ancak, bu bildirinin bir taslak çerçeve çalışma olduğunu ve işler bir AAA kurmanın daha detaylı ve projelendirilmiş teknik, ekonomik ve hukuksal etüdler gerektirdiğini de belirtmek isteriz.

Bu bildirinin ikinci kısmında, sertifika kullanımının ardındaki nedenler ve uluslararası kabul görmüş sertifikasyon sistemleri olan X.509 ve PGP tanıtılacaktır. Bu kısımda ayrıca, sayısal sertifikaların sosyal alandaki anlamından da bahsedilecektir. Bildirinin üçüncü kısmında, genel olarak açık anahtar altyapıları incelenecek, PGP ve X.509 tabanlı açık anahtar altyapılarından söz edilecektir. Dördüncü kısımda ise, varolma nedenleri, temel özellikleri ve bazı detayları ile Türkiye için önerilen açık anahtar altyapısı taslak modeli anlatılacaktır.

2. YANLIŞ AÇIK ANAHTAR SORUNU VE SERTİFİKALAR

Açık anahtarların dağıtımındaki en önemli sorun, insanların yanlış açık anahtar kullanmaları yönünde kandırılmalarıdır. Bu durumu, hem şifrelemede hem de sayısal imzalarda ayrı ayrı incelemek gerekir.

Bir iletinin şifrelenmesi sırasında alıcıya ait olduğu sanılan fakat ona ait olmayan bir açık anahtarın kullanılması, alıcının o iletinin üzerindeki şifreyi çözememesine neden olacaktır. Bununla da kalmayıp, anahtarın gerçek sahibi şifreyi çözüp kendisine gönderilmeyen mesajı okuyabilecektir. Bu durum, kişisellik ve bilgi gizliliği açısından son derece sakıncalıdır.

Sayısal olarak imzalanan bir iletinin üzerindeki imzanın doğrulanması sırasında yanlış bir açık anahtar kullanılıyorsa, imza doğru olsa bile doğrulanamayacaktır.

Açık anahtar tabanlı sistemlerde, açık anahtar sahteciliğini önlemek için kullanılan en yaygın yöntem *sertifikasyon* (*certification*) yöntemidir. Sertifika, bir açık anahtar, açık anahtarın sahibinin kimliği ve elektronik adresinden (e-posta adresi veya URL) oluşan bir veriye herhangi birinin koyduğu sayısal bir imzadır. Eğer bir başkası sertifikayı imzalayan insana güveniyorsa ve onun açık anahtarını biliyorsa, sertifikayı doğrulayacak ve sertifikanın içindeki açık anahtara ve açık anahtarın sahibininin kimliği ile elektronik adresinin doğruluğuna da güvenecektir. Sertifikasyon yöntemleri, açık anahtar imzalama yöntemleri olarak da adlandırılmaktadır. Bu sistemde sertifikaları üreten makama *Sertifika Otoritesi* (*SO*) (*Certification Authority*) denir. Bir SO olmak için en önemli önkoşul güvenilir olmaktır. Burada sözü edilen güven, sertifikayı doğrulayan kullanıcının SO'ya duyduğu güvendir. Bir SO ile onun sertifika verdiği kullanıcı arasındaki ilintiyi güven olarak tanımlamak doğru değildir. Çünkü, bir SO'nun verdiği sertifika sadece kullanıcının kimliği ile açık anahtarı arasındaki bağlantıyı doğrular, SO'yu sertifika sahibinin davranışlarına karşı kefil durumuna sokmaz. O yüzden, bir SO'nun sertifika verdiği kullanıcıya güvenmesine gerek yoktur, onun kimliğinden emin olması yeterlidir.

Sertifika yapılarına, özelliklerine ve SO kavramına iki farklı bakış açısı vardır:
1. X.509 standart önerisi
2. Pretty Good Privacy (PGP) yazılımı

2.1. *X.509 Sertifika Yapısı*

International Telecommunication Union (ITU) ve International Standards Orrganization (ISO) tarafından geliştirilen X.509 standart önerisi [6], sertifika yapılarına, işlevlerine ve güven kavramına ortak bir yaklaşım getirmektedir. Sertifika yapılarındaki bu standart oluşum, değişik amaçlı uygulamaların tek bir sertifika yapısı ile çalışabilmesini amaçlamaktadır. Bu amaca ne kadar ulaştığı tartışılsa da, konusundaki uluslararası otoritelerce kabul edilmiş tek standart olması, X.509'un açık anahtar tabanlı değişik sistemlerdeki uygulanırlılığını artırmıştır.

Bir X.509 sertifikasında temel olarak aşağıdaki bilgiler bulunur:

- X.509 versiyonu
- Sertifika seri numarası
- İmza
- İmzalayıcı (SO) adı
- Geçerlilik süresi
- İlgili (sertifika sahibi) adı
- İlgilinin açık anahtar bilgileri
- Opsiyonel uzantılar

Bir sertifikanın doğrulanabilmesinin temel prensibi üzerindeki imzanın geçerliliğidir. Sertifikanın geçerliliğini kontrol eden kullanıcı, SO'nun açık anahtarını kullanarak imzayı doğrular.

Doğrulayıcının bir sertifikayı doğrulayabilmesinin bir başka presibi de SO'nun güvenilir olmasıdır. X.509'un birinci ve ikinci versiyonlarında bütün SO'ların son derece güvenilir olduğu varsayılmıştır. Ancak, bu durum kendi güvenlik politikalarını kendileri belirlemek isteyen geniş bir çevrenin tepkisine yol açmıştır. X.509'un 1997'de yayımlanan üçüncü versiyonuna opsiyonel uzantılar ile eklenen *politika tanımlayıcıları*, sertifikaların ve dolayısıyla SO'ların, güvenilirliği ile ilgili bilgileri bir şekilde doğrulayıcıya iletmek için kullanılmaktadır. Politika tanımlayıcıları, SO'lar tarafından sertifikaların içine yazılan ve SO'nun sertifika sahibini ne derece iyi tanıdığını, dolayısıyla sertifikaya ne derece güvenileceğini, belirleyen bir bilgidir. Bir SO'nun değişik sertifika verme politikaları olabileceğinden, verdiği sertifikalarda değişik politika tanımlayıcılarına rastlamak olasıdır. Buna benzer olarak, farklı iki SO aynı sertifika verme politikasını uygulayabileceğinden, iki SO'nun aynı politika tanımlayıcısını kullanabilmesi de mümkündür. Öte yandan, bir sertifika doğrulayıcısı, güvenilir olarak nitelendirdiği politika tanımlayıcılarını kendisi belirler ve doğrulamaya çalıştığı her sertifikada kendi güvendiği bir politika tanımlayıcısını arar. Eğer sertifikadaki politika tanımlayıcısı doğrulayıcı için güvenilir değilse, o zaman sertifika üzerindeki imza doğru bile olsa reddedilir. Bu durum doğrulayıcılara, ismen olmasa da sertifika grubu bazında, kendi güven politikalarını belirleme şansı vermektedir.

X.509 sertifikalarının diğer bir özelliği de SO ile son kullanıcı ayrımı olmasıdır. Başka bir deyişle, bir sertifikanın bir SO'ya mı yoksa bir son kullanıcıya mı verildiği bilgisi bir sertifika uzantısı ile belirtilmektedir. Böylelikle, son kullanıcıların aynı zamanda SO olması önlenmektedir.

2.2. *PGP Sertifika Yapısı*

Pretty Good Privacy (PGP) [7], [8], 1990'lı yılların başında Phil Zimmermann'ın kişisel çabalarıyla geliştirilmiş ve hiç bir standardı kabul etmeyen dosya bazlı şifreleme ve sayısal imzalama yazılımıdır. PGP, çeşitli e-posta yazılımları ile uyumlu çalışabildiğinden, daha çok e-posta güvenliği alanında kullanılmaktadır. Kuvvetli şifreleme algoritmaları kullanan PGP, bu özelliği sayesinde kişisel bilgi gizliliğine önem veren çok geniş bir çevrede kabul görmüş ve kısa sürede alanında "de facto" bir standard haline gelmiştir.

PGP'nin ardındaki en büyük tasarım prensibi kullanıcıya sağlanan geniş özgürlüklerdir. ABD hükümetinin tüm karşı çıkmalarına rağmen kırılması zor şifreleme algoritmaları kullanılması bunun bir örneğidir. Bu prensipten hareketle oluşturulan PGP, sertifika ve güven yapılarında da benzer özgürlükler sağlamıştır. PGP'nin

kullandığı sertifikasyon sisteminde SO – son kullanıcı ayrımı yoktur, herkes SO olabilir. Başka bir deyişle, herkes bir başkasının açık anahtarının doğruluğuna garanti verebilir. Bir açık anahtar birden fazla SO tarafından da imzalanabilir ve bu imzalar aynı sertifika yapısı içinde saklanır. Bir PGP sertifikası temel olarak aşağıdaki bilgileri taşır:

- Açık anahtar seri numarası ve yaratılış tarihi
- Açık anahtarın kendisi
- Açık anahtar sahibinin kimliği
- Sertifika üzerindeki imzalar

Ayrıca her kullanıcı, kendi veritabanındaki açık anahtarlar için aşağıdaki bilgileri de tutar:

- Açık anahtar sahibine duyulan güven
- Sertifikanın doğruluk derecesi
- Sertifika üzerindeki imza sahiplerine (SO'lara) duyulan güven

Görüldüğü üzere, PGP'de güven bilgileri doğrudan anahtar ve imza sahiplerine duyulan güven şeklinde saklanmaktadır. Bu güven bilgileri ve bu bilgiler ışığında karar verilen sertifika doğruluk derecesi, her sertifika doğrulayıcısı tarafından ayrı ayrı belirlenir ve her doğrulayıcı bu bilgileri kendi yerel veritabanında saklar. X.509'un güven kavramı ile karşılaştırıldığında, PGP'deki bu durumun kullanıcılara, kendi güven politikalarını oluşturma yönünde daha detaylı karar verme olanağı sağladığı görülmektedir.

Her PGP kullanıcısı kendi veritabanındaki açık anahtarların sahiplerine SO olarak ne kadar güvendiğini kendisi belirler. PGP'de 4 değişik güven seviyesi vardır: 1) tam güvenilir, 2) marjinal güvenilir 3) güvenilmez, 4) bilinmiyor. Kullanıcı veritabanındaki açık anahtarların üzerindeki imzaların güvenilirliği, her imzanın sahibinin açık anahtarına kullanıcının verdiği güvenlik seviyesi kopyalanarak bulunur. Bir açık anahtarın doğruluğu ise üzerindeki imzaların güvenilirliği ile ilgilidir. Bir anahtarın üzerinde bir tane tam güvenilir veya iki tane marjinal güvenilir imza bulunuyor ise, o zaman o açık anahtarın doğruluğuna karar verilir. Bir ve iki sayıları varsayılan değerlerdir ve doğrulayıcı tarafından değiştirilebilir.

2.3. *Sertifikaların Sosyal Anlamı*

Sertifikalar çoğu zaman "sayısal kimlik" olarak nitelendirilmektedir. Ortak noktaları olmakla beraber, bir sayısal sertifika ile gerçek kimlik kartını özdeşleştirmek doğru değildir. Kimlik kartları da sertifikalar gibi belirli otoritelerce verilmektedir, ancak aralarında işlevsel farklar vardır. Bir kimlik kartı sahibinin kimliği ile bedeni arasındaki bağlantıyı belgeler. Bir sertifika ise sahibinin kimliği ile açık anahtarı arasındaki bağlantının belgesidir. Kartın üzerindeki resmin kart sahibine ait olması ve kimlik kartının güvenilir bir yerden verilmiş olduğunun anlaşılması, kimlik kartının kartı gösteren kişiye ait olduğununun garantisidir. Böylelikle, doğrulayıcı karşısında duran insanın kimliğinden emin olur. Öte yandan, bir sertifikanın doğrulanması için üzerindeki SO imzasının geçerli olması ve SO'nun güvenilir olması yeterlidir. Sertifika sahibinin kimliği bu şekilde doğrulanır ama o kimliğin fiziksel olarak kime ait olduğunun garantisi sertifika içinde verilmez. Garanti edilen bilgi o kimliğin sahip olduğu açık anahtardır. Bu da ancak, o açık anahtarı belirli bir amaç için kullanacak olan birinin işine yarar. Örneğin, sayısal olarak imzalanmış bir ileti alan ve üzerindeki imzayı doğrulamak isteyen biri, imza sahibinin açık anahtarını kullanarak imzayı doğrular ve iletinin kimden geldiğinden emin olur. Ama o kimliğin fiziksel olarak kime ait olduğunu ne imzalanmış iletiden, ne de gönderenin sertifikasından anlayamaz. Öte yandan, gerçek hayatta kullanılan kimlik kartları, imzalanmış bir yüzeysel mektubun üzerindeki imzayı doğrulamak için kullanılamazlar. Çünkü, kimlik kartları genelde kişiler ile imzaları arasındaki bağlantıyı belgelemezler.

Bazıları, insanların kendilerinin sanal ortamda önemli olmadığı gerekçesiyle, sertifikaların sanal kimlikler olarak nitelendirilmesini destekleyebilirler. Gerçekten de sanal ortamda sertifikadan daha etkili bir kimlik olamaz ama bu durum sertifikaları gerçek kimlik kartları ile özdeş de kılamaz. Çünkü, sanal ortamda da olsa insanlar yaptıklarından sorumludurlar. Örneğin, sanal ortamda alışveriş yapan biri bu alışverişin bedelini ödemek zorundadır. O yüzden, insanların sanal sertifikaları ile gerçek bedenleri arasındaki bağlantının bir şekilde tutulması gerekmektedir. Sertifikalar bu işi yapamadıklarından, SO'lar imzaladıkları sertifikalar ile ilgili bu bilgileri tutmakla yükümlü olmalıdırlar.

Bir sertifika ile özdeşleştirilecek en iyi belge noterlerden alınan *imza sirküleri*dir. Çünkü, imza sirküleri, tıpkı sertifikalar gibi, kişilerin kimliği ile işlemlerde kullanacağı imzası arasındaki bağlantıyı belgeler. İmza sirkülerini alan bir kişi, o sirküleri onaylayan notere güvendiğinden, sirküler üzerinde kimliği yazılı kişinin gerçek imzasını öğrenir. Bahsi geçen kişiden imzalanmış bir yüzeysel mektup aldığında ise, mektup üzerindeki imza ile sirküler üzerindeki imzayı karşılaştırarak mektup üzerindeki imzayı doğrular. Bu özdeşleştirmeyi daha da genelleyerek SO'ların işlevini bir çesit noterlik olarak nitelendirebiliriz. Bu yüzden, bir SO *Internet noteri* olarak da adlandırılabilir.

Yukarıda bahsi geçen sertifikalar genel amaçlı sertifikalar, kimlik kartları ise sadece insanların kimlikleri ile kendileri arasındaki bağlantıyı belirleyen nüfus cüzdanlarıdır. Bunlardan başka, özel amaçlı kimlikler ve sertifikalar da olabilir. Örneğin, kütüphane kartı bir insanın kütüphaneden faydalanmasını sağlayan bir kimliktir, ama başka bir yerde bu kimliğin bir anlamı yoktur. Belirli bir amaca yönelik özel sertifikalar üretmek X.509 için mümkündür. Opsiyonel bir uzantı olarak sertifikalara eklenen politika tanımlayıcıları, sertifikanın ne amaca yönelik olduğu bilgisini de içerebilir. Doğrulayıcı da bu bilgiyi kullanarak sertifikanın ne için verilmiş olduğunu anlar. Böylelikle, sertifikalar *kimlik kanıtlama* (*authentication*) amacının yanısıra, *yetkilendirme* (*authorization*) amacıyla da kullanılabilir. ICE-TEL projesi [9], sertifikaların yetkilendirme amacıyla nasıl kullanılacağını gösteren bir örnektir. Carl Ellison [15], sertifikaların potansiyel kullanım yerlerinin ilginç ve uzun bir listesini vermiştir.

3. AÇIK ANAHTAR ALTYAPISI

Internet gibi geniş ve dağıtık bir ağda birçok SO bulunması gerekmektedir. Ayrıca, bu SO'lar belirli bir düzende ve birbirleriyle etkileşimli bir şekilde çalışmak zorundadırlar. Aksi halde, tüm Internet kullanıcılarının gerektiğinde birbirlerini tanımalarını sağlamak imkansızlaşır. SO'lar ve bunların sertifika verdiği son

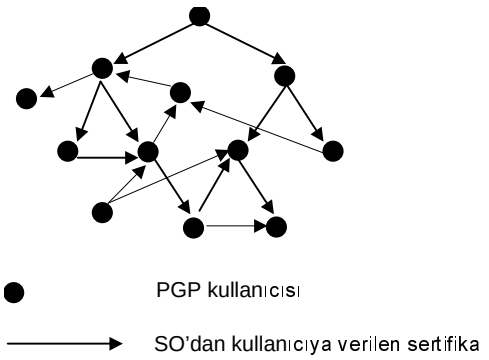
kullanıcıların oluşturduğu bu düzene *Açık Anahtar Altyapısı* (*AAA*) (*Public Key Infrastructure*) denir.

Bir sertifikayı doğrulamak isteyen bir kullanıcı, o sertifikayı veren SO'nun açık anahtarını bilemeyebilir. Bu durumda, doğrulayıcı sertifikayı veren SO'ya ait sertifikayı edinip onu doğrulamak isteyecektir. Bunun için ise o SO'nun SO'sunun açık anahtarı gerekir. Eğer doğrulayıcı sözkonusu anahtarı biliyorsa doğrulama işlemi gerçekleşecektir, bilmiyorsa aynı işlemleri yeni SO için tekrarlayacaktır. Bu zincir, açık anahtarı bilinen bir SO'ya rastlanana kadar devam eder. Birinin sertifikasını doğrulamak için takip edilen bu zincire *sertifika yolu* denir. Bu yol, açık anahtarı bilinen güvenli bir SO ile başlar ve doğrulanmak istenen sertifika ile biter. Bu yol üzerindeki her SO'nun ve sertifikanın güvenilir olması, ve her SO'nun bir sonrasına sertifika vermiş olması gerekir.

AAA'lar sertifika yapılarına bağlı olduklarından, PGP ve X.509 tabanlı AAA'ları ayrı ayrı incelemek gerekir.

3.1. *PGP Açık Anahtar Altyapısı*

PGP'de herkes SO olabilir. Bu durum ortaya herkesin birbirine sertifika verebildiği, merkeziyetçi olmayan bir sertifika ağı çıkarmaktadır. O yüzden PGP AAA'sı bir yönlü ağ şeklindedir. Bu ağın okları verilen sertifikaları temsil etmektedir (SO'dan kullanıcıya). Örnek bir PGP AAA'sı Şekil 1'de resmedilmiştir.



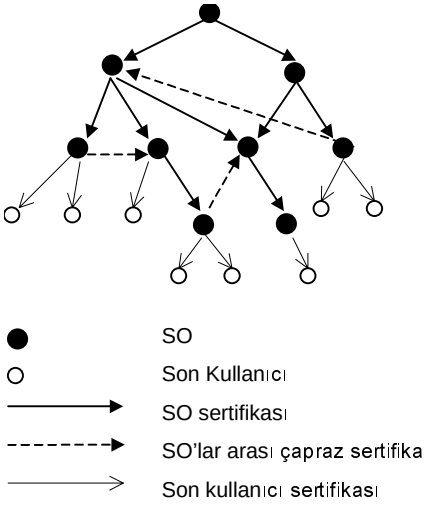
Şekil 1 *Örnek bir PGP AAA'sı*

PGP AAA'sının özellikleri şu şekilde sıralanabilir:

- SO – kullanıcı ayrımı yoktur, herkes sertifika verebilir.
- Bir sertifika yolu doğrulayıcının kendisi ile başlar.
- Sertifika yolu üzerindeki sertifikaların doğrulanmasında PGP'nin sertifika doğrulama ve güven kuralları uygulanır.
- Bir sertifikanın doğrulanabilmesi için sertifika yolu üzerindeki bütün SO'ların güvenilir olması şarttır.
- Doğrulayıcı sertifika yolunun uzunluğunu kısıtlayabilir.

3.2. *X.509 tabanlı Açık Anahtar Altyapıları*

X.509 standardı herhangi bir AAA düzeni önermese de, bu standarda uygun AAA'ların ortak özelliği hiyerarşik bir düzende olmalarıdır. SO – kullanıcı ayrımının olduğu bu AAA'larda bir SO veya kullanıcı birden fazla sertifika sahibi olabilir. Farklı dallardaki SO'lar isterlerse birbirlerine çapraz sertifika (cross certificate) da verebilirler. X.509 tabanlı bir AAA örneği Şekil 2'de verilmiştir.



Şekil 2 *X.509 tabanli bir AAA örneği*

X.509 tabanlı AAA'ların en önemlileri PEM [10], PKIX [11,12], SET [13] ve ICE-TEL [9],[14] sistemlerinin birer parçası olarak olarak tasarlanmışlardır. Değişik uygulama amaçları olan bu sistemlerin AAA'larının genel (ama ortak olmaları zorunlu olmayan) özellikleri aşağıda özetlenmiştir.

- En üstte ana SO'nun, en altta da son kullanıcıların olduğu 4 – 6 seviyeli bir ağaç hiyerarşisi, AAA'nın temelini teşkil etmektedir. Her seviyedeki SO'ların görev ve sorumlulukları uygulamadan uygulamaya değişse de, etki alanlarının yukarıdan aşağıya doğru daralması hiyerarşinin getirdiği ortak özellikleridir.
- Bir son kullanıcı SO olamaz.
- Ancak SO'lar hiyerarşinin dışına çıkıp birbirlerine çapraz sertifika verebilirler, ama bu işlem temel hiyerarşiyi bozacak bir şekilde yapılamaz ve doğrulayıcılar bu sertifikaları reddetme hakkına sahiptir.
- Bir sertifika yolu doğrulayıcının güvendiği herhangi bir SO ile başlayabilir. Ama herkesin en azından ana SO'ya güvenmesi şarttır.
- Bir sertifikanın doğrulanmasında X.509 sertifika doğrulama kuralları uygulanır.
- Doğrulayıcı güvendiği sertifikaları politika tanımlayıcıları vasıtasıyla belirler, ancak sertifika yolundaki diğer SO'ların getireceği fazladan kısıtları da kabul etmek zorundadır.
- Sertifika yolunun boyu ve isim bazlı birtakım kısıtlamalar SO'lar tarafından sertifika içinde verilebilir.
- SO'lar deklare ettikleri sertifika verme politikalarına sıkı bir şekilde uymak zorundadırlar.
- SO'lar imzaladıkları bir bilginin doğruluğundan sorumludurlar.

3.3. *Pratikte Açık Anahtar Altyapıları*

Her uygulamanın değişik isterleri olacağından, AAA hiyerarşisinde ve sertifikasyon politikalarında farklılıklar olması da gayet doğaldır. Bütün uygulamalar için tek tip sertifika kullanmak zaten pratik olarak imkansızdır. Nasıl ki günlük hayatta farklı amaçlarla farklı kimlikler taşıyorsak, sanal ortamda da farklı uygulamalar için farklı sertifikaların olması yetkilendirme esasları

açısından gereklidir. Farklı uygulamaların AAA'larının birbirleriyle etkileşimli çalışması da çok elzem değildir.

Sertifikasyon hiyerarşisini ve sertifika politikalarını çeşitlendiren diğer bir etken ise hükümetlerin kendi ulusal sertifika ağlarını kurmak istemeleridir. Her devlet, kendi hukuksal, sosyal ve ekonomik şartlarına göre, kendilerine özgü ama standartlara da uygun bir AAA modeli benimseyebilir. Ancak, ulusal AAA'ların global AAA hiyerarşisi(leri)ne bağlanmaları şarttır. Aksi halde ulusal AAA kullanıcılarının sertifikaları uluslararası platformlarda doğrulanamaz.

Günümüzde, gerçek dünyadan sanal dünyaya aktarılan ve kullanıcı tanımlaması gerektiren her yaygın beşeri uygulamada açık anahtar tabanlı sistemler kullanılmaktadır. Bu uygulamaların dünya çapında yaygınlaşması da ancak o uygulamaya özgü bir AAA'nın varlığı ile mümkün olacaktır. E-posta [7], [8], [10], elektronik ticaret ve elektronik ödeme [13] şu an en popüler olan ve AAA gerektiren sanal uygulamalardır. Bu uygulamalar arasıda tasarım ve deneme aşamasından geçmiş, ve yaygın olarak kullanılan tek AAA, PGP sisteminin AAA'sıdır [8]. X.509 tabanlı AAA'lardan olan PEM [10] uygulamaya geçmiş olmasına rağmen, rakibi PGP'nin sunduğu daha esnek bir AAA'nın varlığı nedeniyle fazla yaygınlaşamamıştır. SET, PKIX ve ICE-TEL halen tasarım ve test aşamalarındadır.

Güvenli ve kimlik denetimli bir TCP bağlantısı hedefleyen, yaygın olarak kullanılan ve değişik platformlarca destekelenen bir başka yazılım ise SSL (Secure Socket Layer) yazılımıdır. Genel Internet bağlantısını konu aldığı için SSL yazılımı, istemci – sunucu mimarisi ile çalışan ve TCP protokolünü kullanan HTTP, POP gibi servislerde yaygın olarak kullanılmaktadır. SSL, HTTP kullanan elektronik ticaret ve elektronik ödeme sistemlerinde de kullanılmaktadır. Ancak, genel bir amaca hizmet ettiği için SSL'nin bir AAA'sı yoktur. SSL uygulamalarında sertifikalar, gerektiğinde belli başlı sertifika otoritelerinden alınır (örneğin Verisign [15]). Bu SO'ların açık anahtarları gözatıcıların içinde derlenmiş olduğundan, her kullanıcı otomatik olarak bu SO'lara güvenmiş olur.

4. *TÜRKİYE MODELİ*

Bu kısımda Türkiye için bir AAA modeli (TAAA) önerilecektir.

4.1. Amaç, Kapsam ve Nedenler

Türkiye için ayrı bir AAA olmasının ardındaki amaç, Türkiyenin ekonomik ve hukuksal şartlarına uygun, ve açık anahtar tabanlı çeşitli sanal uygulamaları bir çatı altında toplayacak bir düzenin kurulmasıdır. Tüm dünyada olduğu gibi Türkiye'de de, Elektronik ticaret ve elektronik ödeme sistemleri bu sanal uygulamaların lokomotifi durumundadır. SET ve SSL tabanlı çeşitli pilot veya uygulamaya geçmiş elektronik ticaret sistemleri mevcuttur. Şu an için, bu uygulamalar için gerekli tüm sertifikalar yurtdışındaki SO'lardan temin edilmektedir. Bu durumun ardındaki sakıncalar, aynı zamanda Türkiye için bir AAA gerekliliğinin de temel nedenleridir. Bu sakınca ve nedenler iki grupta incelenebilir. 1) Sosyal ve ekonomik nedenler, 2) hukuksal nedenler.

Sosyal ve ekonomik nedenler: Yurtdışından temin edilen bir sertifikanın doğrulanması için o sertifikayı veren SO'ya güvenilmesi gereklidir. Başka bir ülkenin SO'suna herkes güvenmeyebilir. Benzer bir sorun, SO'nun sertifika verdiği kişi ile ilgili bilgilerin doğruluğuna emin olmasında da yaşanabilir. SO'nun, kendi ülkesinin vatandaşı olmayan birinin kimliğini nasıl doğrulayacağı tartışma konusudur. Güven ve kimlik doğrulama sorunları aşılsa bile, bu şekilde sertifika verilirken ve doğrulanmak üzere bu sertifikalar edinilirken bir takım fazladan gecikmeler olacağı kesindir. Bu gecikmeleleri ve güven sorunlarını çözmenin en doğru yolu, herkesin kendi ülkesindeki yerel bir SO'dan sertifika temin etmesidir. Böylelikle, sertifika temini için yurtdışına ödenen döviz de yurtiçinde kalacaktır.

Hukusal Nedenler: Her SO, sertifika verdiği kişinin kimliği ile açık anahtarı arasındaki bağlantıya garanti vermektedir. Bu sertifikayı doğrulayanlar, sertifikadaki açık anahtarın sahibinin kimliğine, SO'nun imzasından ötürü güvenmektedir. SO'lara duyulan bu güvenin uygulamadan uygulamaya değişen bir hukuksal boyutu da vardır. Bir SO, imzaladığı sertifika ile sorumluluk altına girmektedir. Sertifika içindeki kimlik – açık anahtar bağlantısı yanlış ise, bunun cezasını sertifika sahibinin yanısıra, o sertifikayı veren SO da çekmelidir. Bu ceza uygulamadan uygulamaya değişebilir ama burada bir sahtecilik sözkonusudur. Sertifikaların hukuksal yorumlaması henüz netlik kazanmamıştır. Bir yanlış sertifika durumunda kimin yalan söylediğinin anlaşılması da kolay değildir. Bu konuda Crispo ve Lomas'ın [16] bir çalışması vardır.

Yukarıda belirtildiği üzere, SO olmanın hukuksal bir sorumluluğu vardır. Bir ihtilaf durumunda, Türkiye dışında verilmiş ama bir T.C. vatandaşına ait sertifika için yurtdışındaki bir SO'yu T.C. hukukuna göre yargılamak ve cezalandırmak doğru değildir. O yüzden, en azından T.C. vatandaşları arasındaki açık anahtar tabanlı işlemlerde, Türk SO'larının vereceği sertifikaları kullanmak doğru olacaktır. Bunun için ise bir ulusal AAA gereklidir.

4.2. *TAAA'nın temelleri*

TAAA'nın temel prensibi, TAAA kullanıcılarının açık anahtar gerektiren herhangi bir sistemi kullanabilmeleri için gerekli tüm sertifikaları üretmektir. Bunun bir sonucu olarak, bu sertifikaları doğrulamak isteyen bir kullanıcının TAAA SO'larına güvenmesi yeterli olacaktır. SO'lara belirli sorumluluklar vermek için, TAAA'nın merkeziyetçi ve hiyerarşik bir yapıda olması gerekmektedir. Ancak, bu şekildeki bir yapı ile yetki ve sorumluluklar belirli kriterler çerçevesinde dağıtılabilir. Aksi halde, PGP'de olduğu gibi kaotik bir AAA oluşur.

Türkiye için olusturulması düşünülen AAA'nın sertifika yapısı X.509 tabanlı olmalıdır. Çünkü, X.509'un alternatifi olan PGP tabanlı bir sistemde merkeziyetçi bir AAA kurmak zordur. X.509'un diğer bir avantajı da resmi bir standart olması ve AAA tabanlı uygulamaların bu yönde gelişme göstermesidir. Böylelikle, hem TAAA'yı destekleyecek uygulama yazılımları bulmak kolaylaşacak, hem de TAAA'nın küresel AAA'larla entegrasyonu mümkün olacaktır.

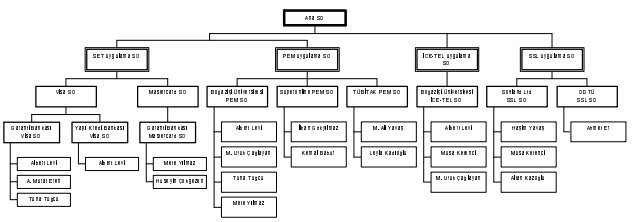
TAAA'nın, her türlü X.509 tabanlı uygulamaya ait AAA'yı bünyesinde barındırması temel tasarım prensiplerindendir. Her uygulamanın farklı AAA modeli olacağından, TAAA için sabit bir hiyerarşik yapı önerilemez. Örneğin, SET sistemlerinde 4 seviyeli bir

ağaç hiyerarşisi gerekli iken, PEM ve ICE-TEL sistemlerinde 3 seviye yeterlidir. Bu yüzden, TAAA'nın ağaç hiyerarşisinde ilk iki seviyeden sonrası uygulamaya bağlıdır. TAAA'nın önerdiği hiyerarşinin en üst seviyesinde *Ana SO* yer almaktadır. Onun bir alt seviyesinde ise *Uygulama SO*'ları bulunur. Uygulama SO'larının altındaki yapılar, her uygulamanın kendi AAA gereksinimine göre o uygulama SO'su tarafından belirlenir.

Ana SO, herkesin güvendiği ve TAAA'nın en yetkili düzenleyicisidir. TAAA'nın temel oluşumları onun izni olmadan değiştirilemez. Ana SO, sadece uygulama SO'larına sertifika verir. Uygulama SO'ları, AAA kullanımını gerektiren, SET tabanlı ödeme, PEM gibi her genel uygulamanın üst seviyeli SO'su konumundadır. Böylelikle TAAA'ya, farklı uygulamalara ait AAA'ların kendi kurallarına göre işlemesini sağlayacak bir esneklik kazandırılmış olur. Ana SO, uygulama SO'larına sertifika vererek, hem onların açık anahtarlarının doğruluğuna garanti verir, hem de herkesin ona güvenmesini sağlayarak TAAA üzerindeki denetim görevini üstlenir ve bir ihtilaf durumda karar verici makam olur. Ana SO'nun varlığının bir başka yararı ise, son kullanıcıların her uygulama için başka bir SO'ya güvenmek zorunda kalmamalarıdır. Kullanıcılar, sadece ana SO'ya güvenerek TAAA'nın bütün sertifikalarını doğrulayabilirler. Şu an için çok gerekli olmasa da, bütün uygulama SO'larının bir tek ana SO'ya bağlanması, farklı uygulamalara ait sertifikaların birlikte kullanımına olanak sağlayacaktır. Örneğin, bir SET sertifikası PEM sisteminde kullanılabilecektir. Ana SO olmasa, başka bir deyişle uygulama AAA'ları birbirlerinden bağımsız olsa, farklı uygulamalara ait sertifikalar birbirleri tarafından doğrulanamazlar ve birlikte çalışamazlar.

TAAA, açık anahtar altyapısı belli olmayan ama açık anahtar kullanan SSL benzeri sistemleri de desteklemelidir. Bunun için önerilen yöntem, ana SO ve o uygulama SO'sunun altında, üçüncü bir seyiye olarak, son kullanıcılara sertifika verecek *organizasyonel SO*'ların olmasıdır. Bu SO'lar sertifikalarını bağlı bulundukları uygulama SO'larından alırlar. Organizasyonel SO'lar, yaygın kullanım alanı olan uygulamalarda, son kullanıcılara sertifika verme yükünü ve sorumluluğunu her kullanıcının bağlı bulunduğu organizasyona (ticari kuruluş, eğitim kurumu veya Internet servis sağlayıcı) devretmek için olması gereken bir ara seviyedir. Çok yaygın olmayan uygulamalarda bu ara seviye hiç olmayabilir ve son kullanıcılar sertifikalarını doğrudan uygulama SO'sundan alırlar. Öte yandan, organizasyonların kendi iç hiyerarşileri olabileceğinden, organizasyonel SO'lar kendi içlerinde bir kaç seviyeye dallanabilirler.

Tipik bir TAAA hiyerarşisi örneği Şekil 3'de verilmiştir.



Şekil 3 *Tipik bir TAAA hiyerarşisi*

4.3. *İleri Konular*

TAAA'nın temelinin X.509 tabanlı bir hiyerarşi olacağı evvelce sunulmuştu. Ancak, bu hiyerarşinin işleyişi ile ilgili bazı konuların daha etraflıca tartışılması gerekmektedir. Bu konular, 4 değişik kategoride değerlendirilecektir. 1) Güven ve sertifika politikaları, 2) sorumluluk ve denetim, 3) ücretlendirme ve işletim, 4) Küresel AAA'larla bağlantı ve çapraz sertifikasyon

Ancak, TAAA'yı etkili bir şekilde çalışır hale getirmek için bu ve benzeri konuların daha da detaylı bir şekilde projelendirilmesi gerektiğini bir kez daha vurgulamak isteriz.

Güven ve sertifika politikaları: Her SO'nun en az bir sertifika verme politikası olmalıdır. Bir tür deklarasyon niteliğinde olan bu politikada, SO'nun sertifika verirken izlediği her prosedür detaylı olarak anlatılır. Bu deklarasyon hem sertifika alacakları yöntem hakkında bilgilendirmek, hem de sertifikaları doğrulamak isteyenlere, o SO'nun ne derece güvenilir olduğunu ifade etmesi açısından önemlidir. O yüzden, her SO deklare ettiği politikasına sıkı bir şekilde uymak zorundadır.

TAAA'da, her uygulama SO'sunun politikası uygulamaya bağlı da olsa, en azında ana SO'nun belirleyeceği belirli kriterlere uyması elzemdir. Ancak, uygulama SO'larının ve onların altındaki SO'ların politikalarının belirlenmesinde izlenecek yöntem daha detaylı bir çalışma gerektirmektedir. TAAA'da, ana SO'nun sertifika politikası kısaca şöyle özetlenebilir.

- Ana SO olarak çalışacak bilgisayar, fiziksel olarak güvenli bir yerde tutulmalı ve yetkisiz kişilerin o ortama girmeleri kesinlikle önlenmelidir.
- Ana SO olarak çalışacak bilgisayarın dış dünya ile veri bağlantısı sadece ve sadece disket ve CD-ROM'larla olmalıdır.
- Ana SO'nun gizli anahtarını saklamak için kullanılan şifre zor tahmin edilir ve uzun olmalı, ve kesinlikle yazılı ortamlarda saklanmamalıdır.
- Ana SO, sertifika vereceği kişi ve kuruluşların gerçek kimliklerinden emin olmak için gerekli tüm kontrolleri yapmalıdır. Bu kontrollere çevrim dışı kimlik kontrolleri de dahildir.
- Ana SO, kimliğinden emin olamadığı hiç kimse için sertifika üretmemelidir.

Sorumluluk ve denetim: Her SO, verdiği sertifikaların doğruluğundan sorumludur. O yüzden, o sertifikadaki olabilecek her yanlış bilginin doğuracağı sonuçlara da katlanmak zorundadır. Her ne kadar SO'lar güvenli otoriteler olarak tanınsalar da, en azından verdikleri sertifikaların kendi deklare ettikleri politikalara uyup uymadığının denetlenmesi gerekmektedir. TAAA'da bu denetim görevini, her SO'ya sertifika veren SO üstlenmelidir. Bunun yeterli olmadığı durumlarda, gerekirse bir SO kendi altındaki bütün SO'ları denetleyebilmelidir. Bu şekilde düşünüldüğünde, ana SO'nun tüm TAAA hiyerarşisi üzerinde denetim hakkı olduğu kolayca gözlemlenebilir. Aslında olması gereken de budur, çünkü her kullanıcı aradaki SO'lara bir bakıma ana SO'dan dolayı güvenmektedir. Bu güvenin getirdiği sorumlulukla, ana SO tüm sistemi denetleyebilir. Bu denetimler sonucu herhangi bir SO'nun sertifikası gerekirse iptal edilebilir.

Ücretlendirme ve işletim: Böylesine bir sistemi kurmanın ve işletmenin hem emek hem de sermaye gerektirdiği ortadadır. TAAA'nın kurulması için belli destekler bulunabilir ama sistemi işler halde tutmak için sürekli bir gelir kaynağı olmalıdır. Bu kaynak, büyük ölçüde, verilecek sertifikalardan alınacak ücretlerle karşılanmalıdır. Uygulamadan uygulamaya değişkenlik gösterebilen bu ücretlendirme için daha detaylı bir finansal analiz gerekmektedir.

Özellikle üst düzey SO'lar için, kimin ne şartlar altında SO olabileceğine belirli kıstaslar dahilinde karar verilmelidir. Bir başka deyişle, birinin SO olabilmesi için güvenilirliğini ve yeterliliğini ispatlamış olması şarttır. Bu tür kararların nasıl ve kimler tarafından verileceğinin prensipleri, SO'lara sertifika verecek SO'ların kendi sertifika verme politikaları çerçevesinde belirlenebilir.

Kimin ana SO olacağı da başka bir tartışma konusudur. Ana SO, tüm TAAA'yı çökertebilecek veya vereceği yanlış sertifikalarla başkalarına haksız menfaat ve güç kazandırabilecek bir pozisyondadır. TAAA içinde yer alacak muhtemel rakip ve hasımların aynı ana SO'ya güvenmeleri gerektiğini de düşünürsek, bu sorunun ne kadar hassas olduğunu daha iyi vurgulamış oluruz. Ana SO'luk görevini bir tek kişiye veya kuruluşa vermek riskli bir davranış olur. O yüzden, ana SO'luk yetki ve sorumlulukları, konusunda uzman ve güvenilir birtakım kişi veya kuruluşlar arasında, eşit olarak paylaştırılmalıdır. Bu paylaşımın teknik olarak nasıl gerçekleştirileceği de ayrı bir bildiri olabilecek bir tartışma konusudur.

Küresel AAA'larla bağlantı ve çapraz sertifikasyon: TAAA kullanıcılarının tüm dünyada tanınmaları, ancak TAAA'nın dünyadaki diğer AAA'lara bağlanması ile mümkündür. Bunun için ise, ana SO'ya diğer AAA'ların ana SO'ları tarafından çapraz veya doğrudan sertifika verilmelidir. Uygulama SO'ları ve daha alt seviyedeki SO'lar da diğer AAA'lardaki SO'lardan çapraz sertifika alabilirler. Ancak bu durum, sadece o daldaki sertifikaların uzak AAA'lar tarafından doğrulanmasını sağlar. O yüzden, küresel AAA'larla bağlantı yolunun ana SO'dan geçmesi tercih edilmelidir.

Küresel AAA'larla bağlantının diğer bir yönü ise, TAAA kullanıcılarının uzak AAA kullanıcılarının sertifikalarını doğrulayabilmesidir. Bunu sağlamak için ise, ana SO uzak AAA ana SO'larına çapraz sertifika vermelidir. Böylelikle, bir TAAA kullanıcısı, uzak AAA'dan herhangi bir SO'ya güven duyması gerekmeden oradaki bir sertifikayı doğrulayabilir. Ancak ana SO, başka bir AAA ana SO'suna sertifika vermeden önce, politikasında belirtilen kontrollerin yanısıra, diğer AAA'nın politikasının da yeterince iyi olduğundan emin olmalıdır. Aynı zamanda, sözkonusu politikanın hangi yerel politikaya karşılık geldiğini, çapraz sertifika içinde bir opsiyonel uzantı olarak belirterek, TAAA kullanıcılarını bu konuda bilgilendirmelidir. TAAA kullanıcıları bu bilgiye göre uzaktaki AAA kullanıcısının sertifikasını kabul veya reddedecektir. Ana SO dışındaki TAAA SO'ları da uzak AAA SO'larına çapraz sertifika verebilirler. Ancak, TAAA'nın merkeziyetçi yapısını bozacağından, böyle bir uygulamadan olabildiğince kaçınılmalıdır. Uzaktaki bir AAA kullanıcısının sertifikasındaki yanlış bir bilgiden dolayı, TAAA kullanıcısının uğrayacağı zararın nasıl tazmin edileceği tartışma konusudur. Buradaki sorumluluk elbette ki o sertifikayı veren uzaktaki SO'dadır ama sözkonusu SO'yu Türkiye'de yargılamak doğru değildir. Bu soruna en iyi yaklaşım, bu tür uluslararası sorunları çözecek bir sistemin kurulmasıdır.

5. SONUÇLAR

Bu bildiride, X.509 ve PGP açık anahtar sertifikaları ve açık anahtar altyapıları tanıtılmış ve Türkiye için bir taslak açık anahtar altyapısı modeli önerilmiştir. X.509 tabanlı ve merkeziyetçi bir yapıda olan bu modelin genel hiyerarşik yapısının yanısıra, uygulamada karşılaşılacak ve standartlarca açıklanmayan birtakım sorunlar da tartışılmıştır. Ancak, bu bildiride önerilen açık anahtar altyapısının işler bir şekilde kurulabilmesi için daha geniş platformlarda tartışılması, daha detaylı bir analiz ve projelendirme sürecinden geçmesi gerekmektedir.

6. *TEŞEKKÜR*

Bu çalışmayı 97A0102 numaralı proje ile destekleyen Boğaziçi Üniversitesi Araştırma Fonu'na, 96K120490 numaralı proje ile destekleyen Devlet Planlama Teşkilatı'na teşekkür ederiz.

7. KAYNAKÇA

[1] Neuman C., T. Ts'o, "Kerberos: An Authentication Service for Computer Networks", IEEE Communications Magazine, vol. 32, no. 9, pp 33-38, Eylül 1994.

[2] Cheswick, Bellovin, Firewalls and Internet Security, Addison - Wesley, 1994

[3] Seberry, J. and J. Pieprzyk, Cryptography: An Introduction to Computer Security, Prentice-Hall, Sydney, 1989.

[4] Stallings, W., Network and Internetwork Security, Prentice-Hall, New Jersey, 1995.

[5] Diffie, W., and M. E. Hellman, "New Directions in Cryptography", IEEE Trans. Inform. Theory, vol. IT-22, no. 6, sayfa. 644 - 654, Kasım 1976.

[6] ITU-T Recommendation X.509, ISO/IEC 9594-8, Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, 1997 sürümü.

[7] P. Zimmermann, PGP User's Guide Volume I: Essential Topics, `http://www.pgpi.com/download` *adresinden ücretsiz PGP yazılımı ile birlikte edinilebilir.*

[8] P. Zimmermann, PGP User's Guide Volume II: Special Topics, `http://www.pgpi.com/download` *adresinden ücretsiz PGP yazılımı ile birlikte edinilebilir.*

[9] D. W. Chadwick, A. J. Young, N. K. Cicovic, "Merging and Extending the PGP and PEM Trust Models – The ICE-TEL Trust Model", IEEE Network, vol. 11, no. 3, sayfa 16 – 24, Mayıs/Haziran 1997.

[10] S. Kent, "Internet Privacy Enhanced Mail", Communications of the ACM, vol. 36, no. 8, sayfa 48 – 60, Ağustos 1993.

[11] R. Housley, W. Ford, W. Polk, D. Solo," Internet Public Key Infrastructure: X.509 Certificate and CRL Profile", Internet Draft <draft-ietf-pkix-ipki-part1-06.txt>, Ekim 14, 1997.

[12] C. Adams, S. Farrell, " Internet X.509 Public Key Infrastructure: Certificate Management Protocols", Internet Draft <draft-ietf-pkix-ipki3cmp-07.txt>, Şubat, 1998.

[13] Secure Electronic Transaction (SET) Homepage, `http://www.mastercard.com/set/`

[14] ICE-TEL Project Homepage, `http://www.darmstadt.gmd.de/ice-tel/`

[15] Verisign Inc. Homepage, `http://www.verisign.com/`

[16] B. Crispo, M. Lomas, "A Certification Scheme for Electronic Commerce", Security Protocols International Workshop, LCNS vol. 1189, Springer-Verlag, sayfa 19 – 32, Nisan 1996, Cambridge, UK.