Açık Anahtar İmzalama Partileri

Emin İslam Tatlı
Department of Computer Science, University of Mannheim

October 4, 2005

1 Giriş

Penguence'nin 2. sayısında Açık Anahtarlı Şifre Bilimi (*Public Key Cryptography*) hakkında A. Murat Eren imzalı daha çok teknik içerikli bir yazı okuduk [9]. Ben bu yazımda, Eren'in yazısına tamamlayıcı olarak açık anahtarlı şifre biliminin günümüz uygulamalarında nasıl kullanıldığı, açık anahtar altyapısı (*public key infrastructure*), PGP ve güven ağı (*web of trust*) konularından bahsedeceğim. Yazımın ana teması olarak da güven ağının genişletilmesini hedefleyen açık anahtar imzalama partilerinin nasıl organize edildiğini, parti öncesi ve sonrası yapılması gerekenleri anlatacağım.

2 Açık Anahtarlı Şifre Bilimi

Açık anahtarlı şifreleme bilimi *açık* (*public key*) ve *özel* (*private key*) anahtar çifti temeline dayanan bir sistemdir. Asimetrik şifreleme (*asymmetric encryption*) ve sayısal imzalama (*digital signature*) uygulamaları başlıca açık anahtarlı şifre bilimi uygulamalarıdır.

Şifreleme, iletilerin gizliliğini (*confidentiality*) sağlar. Kullanılan anahtara göre iki türlü şifreleme vardır: şifrelemede ve deşifrelemede aynı anahtarı kullanan *simetrik şifreleme*, ve şifreleme ile deşifrelemede farkı anahtarları kullanan *asimetrik şifreleme*. Asimetrik şifreleme, gizliliği gereken bir iletinin (e-posta v.b.) şifrelenip gönderilmesinden ziyade bu gizlilik gerektiren iletinin simetrik şifrelenmesinde kullanılacak olan *simetrik anahtarın* güvenli bir şekilde iletişim partnerleri arasında aktarılmasında kullanılır. Bu amaçla oluşturacağınız bir simetrik anahtarı partnerinizin açık anahtarı ile şifreleyip partnerinize gönderirsiniz ve partneriniz ise şifrelenmiş olan simetrik anahtarı *sadece* kendisinin sahip olduğu özel anahtarı ile deşifre eder.

Sayısal imzalar ise bütünlük (*integrity*), asıllama (*authentication*) ve inkar edememe (*non-repudiation*) gereksinimlerini yerine getirirler. Sayısal imzalamada iletinizi kendi özel anahtarınız ile imzalayıp partnerinize gönderirsiniz ve partneriniz sizin açık anahtarınızı kullanarak kendisine ulaşan iletinin gerçekten sizin tarafınızdan gönderilip gönderilmediğini (*asıllama*) ve iletinin iletişim kanalı üzerinde taşınırken izinsiz değişime uğratılmış olup olmadığını (*bütünlük*) sınar. Yine partneriniz, ileti üzerindeki imzanız sayesinde bu iletinin sizin tarafınızdan gönderildiğini ispat edebilir (*inkar edememe*). Açık anahtarlı şifre bilimi hakkında daha detaylı ve teknik bilgi için Penguence'nin 2. sayısındaki [9] yazısına göz atmanızı tavsiye ederim.

Buraya kadar özetlersek biri size özel, diğeri herkese açık olan bir anahtar çifti oluşturuyorsunuz ve bu anahtar çifti sayesinde bilgi güvenliğinin temel gereksinimlerinden olan gizlilik, bütünlük, asıllama ve inkar edememe gereksinimlerini yerine getiriyorsunuz. Ne yazık ki işimiz bu cümlede bahsedildiği kadar basit değildir. Şu örneği bir inceleyelim: E-postanızı şifreleyip göndermek istiyorsunuz. Dolayısı ile e-postayı göndereceğiniz partnerinizin açık anahtarına önceden sahip olmalısınız. Bu açık anahtar değişimi işleminin *güvenilir* bir şekilde yapılmış olmalı ki her partner diğerinin açık anahtarının doğruluğundan emin olsun. Bunun bir yolu partnerinizle yüz yüze buluşup disket, CD gibi bir kayıt medyası aracılığı ile açık anahtarlarınızı değiş tokuş etmek olabilir. Ancak iletişim kuracağınız birden fazla partneriniz olduğunu düşündüğümüzde bu yöntem yeterince ölçeklenebilir (*scalable*) değildir. Üstelik partnerlerinizin açık-özel anahtar çiftlerini zamanla yenilediklerini düşünürsek bu iş içinden çıkılamaz bir hal alır.

Bu problemin çözümü açık anahtar altyapısıdır (*PKI-Public Key Infrastructure*). PKI'nın en temel fonksiyonu, kullanıcı kimliğini açık anahtarına bağlayan sertifikaların yönetimini gerçekleştirmesidir. Bir kullanıcının sertifikasını onun açık anahtarının geçerliliğinin bir kanıtı olarak düşünebiliriz. Sertifika yönetimi; sertifika başvurularının değerlendirilmesi, sertifikaların oluşturulması, dağıtılması, sorgulandığında iletilmesi ve gerektiğinde iptal edilmesi gibi işlemleri kapsar. PKI içerisindeki bu farklı görevlerden sorumlu çeşitli bileşenler bulunmaktadır. Sertifika Yetkilisi (*CA-Certificate Authority*) bu bileşenlerin merkezinde bulunur. CA'nın oluşturduğu sertifikalar üzerinde kendi sayısal imzası bulunur. Böylece bir kullanıcıya ait sertifikanın (*dolayısı ile açık anahtarın*) geçerliliği sertifika üzerindeki CA imzası sayesinde sınanabilir.

3 Güven Ağı (Web of Trust)

PKI ve CA sayesinde istediğimiz partnerimizin açık anahtarını güvenilir şekilde elde edebiliyoruz. Ama bu noktada diğer bir sorunla karşı karşıyayız. PKI ve CA'nın yönetiminden kim sorumlu olacak? Sadece bir organizasyon, bir şirket içi iletişimin güvenliğini sağlamak istiyorsak bu organizasyon ya da şirket içinde kurulacak olan bir PKI problemi çözecektir. Ancak evrensel bir dünyada yaşamakta olan bizlerin hiç görüşmediğiniz, dünyanın diğer bir ucundaki bir kimse ya da bir kurum ile güvenli iletişim kurmamız gerektiğinde yine *evrensel* bir PKI'ya ihtiyacı vardır. Öyle ki bu evrensel PKI dünyadaki bütün kullanıcıları içine alan en azından alabilecek olan bir yapıya sahip olmalıdır. Belirli bir ücret karşılığı böyle evrensel PKI hizmeti sunan çeşitli firmalar bulunmaktadırlar [1, 6].

Diğer taraftan, merkezi yönetim şekline dayalı PKI'nın insanların mahremiyetini tehdit ettiğini söyleyen Philip R. Zimmermann 1990 yılında PGP (*Pretty Good Privacy*) yazılımını geliştirdi. Zimmermann PGP için "PGP insanlara kendi mahremiyetlerini kendi ellerinde tutma yetkisi verir. Bu konuda büyüyen bir ihtiyaç var. Bu yüzden böyle birşey yazdım." demektedir [10]. PGP, merkezi bir yapının aksine güven ağı modeline (*web of trust*) dayanan bir PKI yapısı sunmaktadır.

Güven ağı modelinde, kullanıcılar kendi sertifikalarını kendileri oluşturup ve aynı zamanda kendileri imzalayıp (*self-signed certificates*) kullanırlar. Bu modelde, katılımcılar birbirlerinin açık anahtarlarını imzalamak sureti ile güven

ağını genişletirler ve bu sayede ağın kullanım alanı genişletilmiş olur. Bir kimsenin açık anahtarını imzalamak o kişinin kimliğine bağladığı açık anahtarının geçerliliğini onaylamak anlamındadır. Örneğin birbirlerini tanıyan A ve B kullanıcıları birbirlerine güvendikleri için açık anahtarlarını karşılıklı imzalarlar. Yine B ve C kullanıcıları da birbirlerinin açık anahtarlarını imzalamış olsunlar. Bu sayede A ve C kullanıcıları arasında çift yönlü bir güven ağı oluşmuş olur. A ve C kullanıcıları oluşan bu güven ağına dayanarak şifreleme ve sayısal imza doğrulamada birbirlerinin açık anahtarlarını kullanabilirler.

4 Anahtar İmzalama Partileri

PGP'nin dayandığı güven ağı modelinde ideal olan mümkün olduğunca fazla katılımcının birbirinin anahtarını karşılıklı imzalayıp güven ağını genişletmesidir. Bu amaçla PGP şifreleme sistemini kullananların bir araya gelip güven ağına katılmalarını sağlamak ve ağın eksik olan halkalarını tamamlamak için anahtar imzalama partileri düzenlemek gerekmektedir. Bu partiler, güven ağının genişlemesini sağlamaları yanında katılımcıların bir araya gelip tanışma imkanı bulmalarına, bilişim dünyasının sosyal konuları ve özellikle açık kaynak kod dünyası hakkında bilgi alışverişinde bulunmalarına imkan sağlarlar.

Buraya kadar güven ağı modeli ve açık anahtar imzalama partilerine niçin gerek olduğu konuları anlaşılmış olmalı. Bundan sonraki bölümde bu partilerin organizasyonunda nelere dikkat edilmesi gerektiğini, katılımcıların partiye nasıl hazırlanmaları gerektiğini, neleri beraberlerinde getirmeleri ve de getirmemeleri gerektiğini ve parti sonrası yapılması gerekenleri anlatacağım [7].

4.1 Katılımcılar

Katılımcıların partiye gelmeden önce bir takım hazırlıklar yapmaları gerekmektedir. Öncelikle açık-özel anahtar çifti bulunmayan katılımcılar kendilerine bir anahtar çifti oluşturmalıdırlar.

4.1.1 Anahtar Oluşturma

PGP yazılımı şuanda PGP Corp. şirketi tarafınfan ücretli olarak satışa sunulmaktadır. GnuPG (*GNU Privacy Guard*) programı, PGP'nin açık kaynak kodlu ve ücretsiz karşılığı olup anahtar yönetimi, şifreleme ve sayısal imzalama gibi işlevleri destekler. GnuPG'nin son sürümü *www.gnupg.org* sitesinden indirebilir ve detaylı kullanım bilgileri için türkçeye çevrilmiş [8] belgesinden yararlanabilirsiniz.

GnuPG kurulumunu gerçekleştirdikten sonra anahtar çiftinizi oluşturmaya başlayabilirsiniz:

$ gpg --gen-key

komutu anahtar çeşidi, uzunluğu ve geçerlilik süresi gibi soruların cevabını sizden aldıktan sonra açık ve özel anahtar çiftinizi oluşturacaktır. Güvenli bir anahtar için anahtar uzunluğunu en az 1024-bit seçin. Bu komut, kullanıcının ana klasörü altında *.gnupg* isminde yeni bir klasör oluşturur. Kullanıcının ve partnerlerinin açık anahtar bilgilerini içeren *pubring.gpg* dosyası (*anahtar*

zinciri) ve yine kullanıcının özel anahtar bilgilerini içeren parola korumalı *secring.gpg* dosyası .gnupg klasörü altına yerleştirilir. secring.gpg dosyasını çok iyi korumalısınız. Zira bu dosyasının yabancı ellere geçmesi bir nevi kimliğinizin çalınmasıdır.

Anahtar oluşturma işleminden sonra açık anahtar başkalarının erişimine sunulmak üzere merkezi anahtar sunucularına (örneğin *http://pgp.mit.edu*) gönderilmelidir. Ancak bazı kimseler açık anahtarlarını da aynı özel anahtarları gibi kendilerinde saklayıp merkezi sunuculara *göndermemeyi* tercih ederler. Bu kimseler, açık anahtarlarının merkezi sunucularda değişikliğe uğratılmasından ya da merkezi sunucuların sorgulandıklarında güncel olmayan anahtarı sunmalarından endişe ederler ve açık anahtalarını gerektiğinde ilgili kişiye kendileri gönderirler. Bu ne kadar haklı bir gerekçe olsa da PGP'nin kullanımını kısıtlamaktadır. Bunun yerine anahtar parmakizinizi e-postalarınızın imza kısmına ekleyebilir ya da web sayfalarınızda yayınlayabilirsiniz. Bu sayede, diğer kullanıcıların güncel olan açık anahtarınızdan haberdar olmalarını sağlayabilir ve merkezi sunuculardan kaynaklanan risklerin önüne geçebilirsiniz. Şayet açık anahtarınızı merkez sunucuya göndermeye karar verdiyseniz, şu komutu kullanın:

$ gpg --keyserver anahtar_sunucusu --send-key anahtar_id

4.1.2 Gerekli Evraklar

Katılımcıların partiye gelirken beraberlerinde getirmeleri gerekenler ise şunlardır:

- *Kendiniz:* Partiye sizi temsilen kimseyi gönderemezsiniz. Partide katılımcıların kimlik doğrulaması yapmaları gerekmektedir, ancak bundan sonra anahtarınızı imzalamayı kabul ederler.
- *Açık anahtar bilgileri:* İmzalanmasını istediğiniz açık anahtarınızın id, parmakizi, uzunluğu ve çeşidi, sahibinin adı-soyadı ve e-posta bilgilerini içeren bir belgeyi (Tablo 1) çıktı alıp partiye beraberinizde götürmelisiniz. Şayet dağınık bir parti yürütülecek ise (*bakınız bölüm Organizasyon*) bu belgeden katılımcı sayısı kadar hazırlamanız gerekmektedir. Var olan açık anahtarınıza dair bu bilgileri öğrenmek için

  $ gpg --list-keys anahtar_id

  komutunu kullanmalısınız.
- *Kimlik:* Üzerinde resminiz bulunan nüfus cüzdanı, ehliyet ya da pasaport gibi bir kimliği de beraberinizde götürmelisiniz.
- *Kalem:* Merkezi partilerde yanınızda mutlaka bir kalem bulundurmalısınız.

4.2 Organizasyon

Organizasyon için öncelikle partinin şeklini ve yerini tespit edip duyurusunu yapacak, parti düzenini sağlayacak bir organizatöre ihtiyaç vardır.

Table 1: Açık Anahtar Bilgileri

Anahtar ID	**Uzunluğu**	**Çeşidi**	**Sahibi**
71766551	1024	DSA	Emin İslam Tatlı <tatli@th.informatik.uni-mannheim
Parmakizi	105E E5CE 5476 3E0C 96C9 5DCE 53DB D21C 7176 6551		
Anahtar Onay?		**Kimlik Onay?**	

Partinin şekli *merkezi* veya *dağınık* olmak üzere iki türlü olabilir. Parti duyurusu e-posta, web sayfası ve/veya basın yoluyla yapılabilir. Duyuruda özellikle partinin zamanı ve yeri, katılımcıların getirmeleri gerekenler ve partinin işleyişi ile ilgili bilgiler belirtilmelidir. Bunlara ek olarak, açık anahtar imzalama partilerinin ne olduğu ve bu partilerin niçin gerektiği üzerine açıklayıcı bilgilerin de duyurulması katılımcı sayısının artmasını sağlayabilir.

Merkezi partiler, katılımcı sayısının az olduğu ve partinin düzenlendiği ortamın sakin ve uygun olması halinde tercih edilmelidir. Merkezi partilerde, parti katılımcıları kendi açık anahtarlarına ait tanımlayıcı bilgileri (Tablo 1) parti öncesinde organizatöre e-posta yolu ile gönderirler. Organizatör, bütün katılımcılara ait anahtar bilgilerini bir araya getirdiği belgeyi parti esnasında bütün katılımcılara dağıtmak üzere katılımcı sayısı kadar çoğaltır.

Merkezi partilerde anahtar ve kimlik onaylama işlemi aynı anda sadece bir katılımcı için yapılır ve bu sebeple bu tür partiler uzun sürmektedir. Dolayısı ile katılımcı sayısının çok ya da ortamın müsait olmadığı durumlarda organizatörler dağınık bir parti düzenlemelidirler. Dağınık partiler için katılımcılar kimlik belgelerine ek olarak açık anahtar tanımlayıcı bilgilerini katılımcı sayısı kadar çoğaltıp beraberlerinde getirmelidirler.

Organizatör, katılımcıları motive etmek ve katılımcıların ilgilerini çekmek için katılımcılar arasındaki parti öncesi ve sonrası güven bağını grafiksel olarak oluşturup bunu katılımcılarla paylaşırabilir. sig2dot [5] ve neato [4] programları yardımıyla bu grafiği oluştumak oldukça kolaydır. Daha detaylı bilgi için [2]'ye başvurunuz.

4.3 Partinin İşleyişi

Anahtar imzalama partilerinde başlıca iki tür doğrulama yapılması gerekmektedir: katılımcıların *açık anahtarlarının doğrulanması* ve *kimliklerinin doğrulanması*. Merkezi ve dağınık partilerin temel farkı bu doğrulamaların işleyişindedir.

Merkezi partilerde önce anahtar daha sonra kimlik doğrulaması gerçekleştirilir. Organizatör, başlangıçta bütün katılımcılara herkesin anahtar tanımlayıcı bilgilerini içeren belgeden dağıtır ve sonra bütün katılımcıları sırası ile yanına çağırır. Her katılımcı, yanında getirdiği anahtar bilgileri ile organizatörün dağıttığı belge üzerindeki anahtar bilgilerini karşılaştırır. Bu doğrulamada bir sorun yok ise katılımcı yüksek sesle anahtar bilgilerini diğer katılımcılara okur. Diğer katılımcılar da organizatörün kendilerine verdiği belge üzerinde bu katılımcının anahtar bilgilerini kontrol ederler ve şayet bir farklılık yok ise bu katılmcı için *Anahtar Onay* kısmına bir onay işareti koyarlar. Bu işlem, sırası ile bütün katılımcılar için yapıldığında anahtar doğrulaması sona erer ve sıra kimlik doğrulamasına gelir. Kimlik doğrulaması için bütün katılımcılar yan yana tek sıra halinde dizilirler. En baştaki kişi yanındakinden başlamak sureti ile herkesin kimliğindeki adının ve fotoğrafının doğrulamasını yapar. Doğrulama sonucunda,

kimliği doğrulayan katılımcı diğer kimliğini doğruladığı katılımcının *Kimlik Onay* kısmına da bir onay işareti koyar. Hem anahtar hem de kimlik için onay almış bir katılımcının anahtarı artık imzalanmak için kabul edilmiştir. Bu kimlik onaylama işlemini sırası ile bütün katılımcılar yaparlar.

Görüldüğü üzere merkezi partilerde paralel bir onaylama mümkün olmadığı için katılımcı sayısının az olduğu durumlarda bu parti çeşidi seçilmelidir. Aksi takdirde dağınık partiler tercih edilmelidirler. Dağınık partilerde her katılımcı rastgele diğer katılımcılarla buluşarak karşılıklı kimlik doğrulaması yapar ve bu doğrulama sonucunda diğerlerine beraberinde getirdiği anahtar tanımlayıcı belgesinden verir. Böylece kimlik doğrulama işlemi paralel bir şekilde daha kısa sürede tamamlanır. Dağınık partilerde organizatörlerin özellikle dikkat etmeleri gereken katılımcıların mümkün olduğunca fazla sayıda katılımcı ile buluşmalarını sağlamak olmalıdır.

4.4 Parti Sonrası

Partinin sonunda her katılımcının elinde imzalaması gereken bir açık anahtarlar listesi bulunmaktadır. Organizatör ya da katılımcılar partiye bilgisayarlarını getirip hemen parti sonrasında imzalama işleminin gerçekleştirilmesi için bu bilgisayarları kullanıma sunabilirler. Ancak bu *kesinlikle yapılmamalıdır*. Çünkü bu bilgisayarlardan birinin üzerinde var olabilecek bir truva atı, örneğin katılımcıların imzalamada kullandıkları gizli parolaları çalarak PGP sisteminin tehlikeye düşmesine sebep olabilir. İmzalama işlemi için evinizdeki ya da ofisinizdeki kendi şahsi bilgisayarınızı kullanın.

4.4.1 Anahtar İmzalama

Bir açık anahtarı imzalamak için sırası işe şu adımları gerçekleştirin:

1. Katılımcının açık anahtarını merkezi sunucudan kendi sisteminizdeki anahtar zincirine ekleyin:

   $ gpg --keyserver anahtar_sunususu --recv_keys imzalanacak_anahtar_id

2. Şayet katılımcı açık anahtarını merkezi anahtar sunucusuna göndermemiş ise size açık anahtarını e-posta yolu ile göndermelidir. Bu durumda ise size gönderilen anahtarı anahtar zincirinize eklemelisiniz:

   $ gpg --import açık_anahtar_dosyası

3. Katılımcının partide belirttiği anahtar parmakizi ile bilgisayarınızda imzalamak üzere olduğunuz anahtar parkamizinin aynı olup olmadığını karşılaştırın:

   $ gpg --fingerprint imzalanacak_anahtar_id

4. Açık anahtarı imzalayın:

   $ gpg --sign-key imzalanacak_anahtar_id

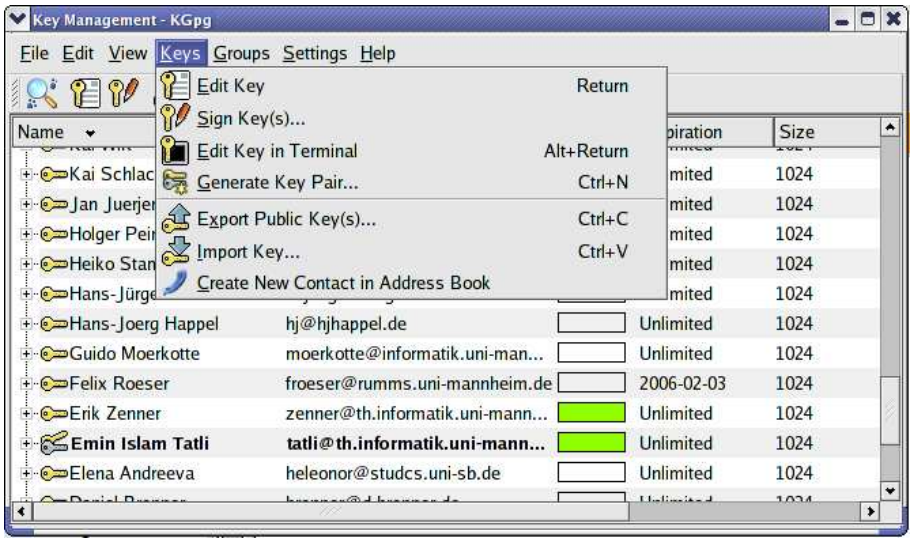

Figure 1: KGPG (gpg yazılımı için grafiksel arayüz)

5. Son olarak imzaladığınız anahtarı merkezi sunucuya gönderin:

   $ gpg --keyserver anahtar_sunususu --send_key imzalanan_anahtar_id

6. Şayet katılımcı imzaladığınız anahtarını merkezi sunucu yerine kendisine e-posta yolu ile gönderilmesini parti esnasında belirtmiş ise imzaladığınız anahtarını önce dışa aktarın:

   $ gpg --export anahtar_sahibi --output anahtar_dosyası

   Daha sonra *anahtar_dosyası*'nı ilgili katılımcıya e-posta ile gönderin.

gpg yazılımı için bir grafiksel arabirim sunan KGPG [3] (Şekil 1) yazılımı sayesinde yukarıda anlattığım bütün gpg komutlarını bir grafik arabirim üzerinden de kolayca yapabilirsiniz.

5 Sonuç

Bilgi güvenliği sağlığa benzer. Önemi ancak kaybedildiği zaman (*daha iyi*) anlaşılır. Ancak anlaşıldığı zaman da iş işten geçmiş olabilir. PGP sistemi, sayısal dünya ile iletişiminizde güvende olmanızı sağlayacak çeşitli çözümler sunmaktadır. Tavsiyem odur ki PGP'nin güvenlik ağına kendinizi biran önce ekleyin ve güvenli iletişimin nimetlerinde faydalanmak için zaman kaybetmeyin.

Son olarak, merkezi partinin işleyişini özetlediğim Şekil 2 ile yazımı burada noktalıyorum. Herkese bol güvenli günler dileğiyle!

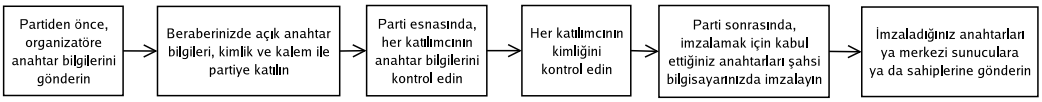

Figure 2: Merkezi Partinin Akış Diagramı

References

[1] Entrust. URL: www.entrust.com.

[2] Güven ağı grafiği oluşturma. URL: www.chaosreigns.com/code/sig2dot/.

[3] KGPG. URL:http://developer.kde.org/ kgpg.

[4] Neato. URL: www.graphviz.org/.

[5] sig2dot.pl. URL: www.chaosreigns.com/code/sig2dot/sig2dot.pl.

[6] Verisign Inc. URL: www.verisign.com.

[7] V. Alex Brennen. Gnupg keysigning party HOWTO.
URL: www.cryptnet.net/fdp/crypto/gpg-party.html, Haziran 2004.

[8] Brenno de Winter, Çeviren: Barış Çiçek. GnuPG Minik Nasıl.
URL: www.gnupg.org/howtos/tr/GPGMinikNasil.html, Nisan 2004.

[9] A. Murat Eren. Açık Anahtarlı Kriptografi. *Penguence*, 2:28–32, 2005.

[10] Philip R. Zimmermann, Çeviren: Burak Demircan. Neden PGP'ye İhtiyaç var? URL: www.pgpi.org/doc/whypgp/tr/.