Linux 'ta PGP Kullanımı

Fatih Özavcı
IT Security Consultant

f.ozavci@btg.com.tr
http://www.btg.com.tr

holden@siyahsapka.com
http://www.siyahsapka.com

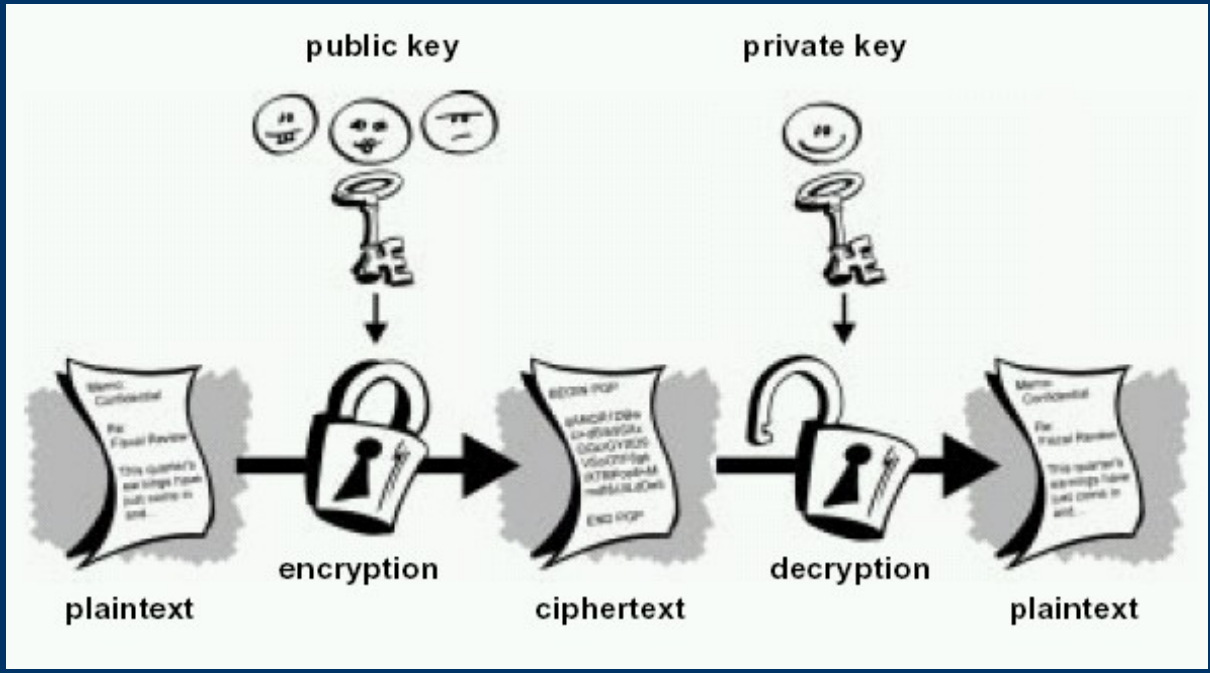
PGP – Pretty God Privacy

- 1990 Yılında Philip Zimmermann Tarafından Geliştirilmiştir
- İnternet'te Kişilerin Veri Aktarımları ve Yazışmalarını Güvenli Hale Getirmek Amaçlanmıştır
- RFC 1991 ile PGP'nin İşleyişi Açıklanmış ve RFC 2015 ile Standart Olması Teklif Edilmiştir
- RFC 2440 ile OpenPGP Formatı Açıklanmış ve Standart Olması Teklif Edilmiştir
- RFC 2726 ile RIPE Veritabanı Güncellemelerinde PGP Kullanımı Aktarılmış ve Standart Olması Teklif Edilmiştir

PGP'nin Sağladıkları

-
- Veri Bütünlüğünün Doğrulanması
-
- Veri Gizliliğinin Korunması
-
- Veriyi Gönderen Kişinin Doğrulanması

PGP'nin İşleyişi



PGP'nin İşleyişi

- PGP Kullanımı İçin Her Kullanıcının 1 Özel 1 Genel Anahtarı Bulunmalıdır
- Veri Kriptolanırken, Kriptolayan Kişinin Özel Anahtarı ile Bu Veriye Ulaşması İstenen Kişilerin Genel Anahtarları Kullanılır
- Kriptolu Verinin Çözülmesinde Özel Anahtar Kullanılır
- Veri İmzalanırken Sadece Özel Anahtar Kullanılır, İmza Geçerliliğini Kontrol Edecek Kişinin Genel Anahtarı İmzalamada Kullanılmaz

Anahtar Yönetimi

- Anahtar Üretmek İçin Bir Otorite Bulunmaz ve Otorite Onayına Gerek Yoktur
- 1 Çift Anahtar Üretilmelidir (Genel ve Özel)
- Genel Anahtar Halka Açık Olmalı ve Kolayca Erişilmelidir
- Özel Anahtar Sadece Sahibinde Bulunmalıdır

Anahtar Dağıtımı

- Genel Anahtarların Düzenli Olarak Dağıtımı ve Yönetimi İçin Halka Açık Anahtar Sunucuları Bulunmaktadır
-
- Kuruma Özel Anahtar Sunucusu Kurulumu ve Kullanımı Mümkündür
-
- Dağıtılmış Genel Bir Anahtarın Farklı Kişi/Kurumlarca İmzalanması ve Güvenilmesi Mümkündür

Kullanım Amaçları

- Özel Yazışmaların Kriptolanması
- Bir Dosyanın Kriptolanması
- Yazışmaların Bütünlüğünün Doğrulanması
- Bir Dosyanın Bütünlüğünün Doğrulanması
- Yazışma Taraflarının Doğrulanması

Kullanılan Algoritmalar

- Cipher Katmanı
  - 3DES, CAST5, BLOWFISH, AES, AES192, AES256,TWOFISH
- Genel Anahtar
  - RSA, RSA-E, RSA-S, ELG-E, DSA, ELG
- Veri Özeti
  - MD5, SHA-1, RIPEMD160

Kriptolanmış Bir Veri

-----BEGIN PGP MESSAGE-----

Version: GnuPG v1.0.4 (GNU/Linux)

Comment: Gnome PGP version 0.4

hQIOA7HMZGc8Py7SEAf/eWVrPAF/k75uWRthVdsQcy7e725F2cl5kQDlDl44/KdP
vyaCEMd+4eVqEh3Ao3PmdGzAc31KGLA56sWPYySk4f7YlbyRF8bLL1odZNa3Mbwu
B0mH6vsUDmgMAoSSvTn3ckWNaDaVjXMn1RFD+1yzrs/hCoBzTMx12aH628JE+qeg
KG9fRununsabmV3a29uaZKSaxkyXlBMVms7E377SEuiDj+Q4+xjqVL49v8u9nWci
EaUovJEcrJVDBEfP/575jc6DJZZ9I448nK5IHHpV68O8s+xwZ7GESGHfLUcoBPcn
HOUuC7I9o2dry+zFDT9aIsWGtPL9nSMJ1fSGNbpkLQf9Hybi96v8QEp8F+8bomHs
qEfsumIxWRsMtNNj3gc3YAZquiUGDqcUD58uOssUqe/vdE6LaTV99rPThI2zf3r0
sMe7U9CmvFa6h0YkkAt6hoLdkDkM+lXzVNuyibvsWSOez3fko9BJ+YUOLNvTgWwO
rTIX6c+f2tObTk9P3jzzu9qy2GVgV8zajd23Bh12JTLygBhOa4WivYibVvCNHu3n
DdpgQ9WaSVWSsKyE9wLYxM90Wz3cVjFeNd2ZQsIxoxZv+1yTyyIR1nOpz5MjuGrZ
WPLVThjfUUeAbOsqF2MhIEW0XH+j25DWgUrjnK0CxPKC1TR3hX8yHhGPglow+MFH
LNKRAdJ5uOqgd3ET6NfV5x2gFaW2Bn/fta024Z1P4IEQ/dis3M8QW/71Z5CZ7/8w
MUREmJiEaWc6YOxahWO/2D3i5DflM2dArDRu4c9hXlA5+dwyxewEKErGUvb1X5X0
9ZFgULUtWKXC7ZzoODxvIQvCUBO+nMUD/lo4OAPDxWrHKHE7lDhpCBGxa/ja/9fD
XtwrvA===nDBS

-----END PGP MESSAGE-----

Gnu Privacy Guard

- GPL Lisansı ile Dağıtılan Özgür Bir Yazılımdır
- PGP 2.x ve OpenPGP ile %100 Uyumludur
- Çok Sayıda İşletim Sistemi Platformunu Desteklemektedir (*BSD, Linux, Windows,MacOSX vs)
- Anahtarlar ile Beraber Fotoğraf Kullanımını da Desteklemektedir
- Güncel ve Kararlı Sürümü 1.3.1'dir
- http://www.gnupg.org Adresinden Temin Edilebilir

GnuPG Özellikleri

- Anahtar Formatı
  - RSA, DSA, El Gamal
- Anahtar Boyu
  - 768 Bit, 1024 Bit, 2048 Bit
- Cipher Katmanı
  - 3DES, CAST5, BLOWFISH, AES, AES192, AES256,TWOFISH
- Genel Anahtar
  - RSA, RSA-E, RSA-S, ELG-E, DSA, ELG
- Veri Özeti
  - MD5, SHA-1, RIPEMD160

GnuPG Anahtar Yönetim Komutları

Anahtar Üretme	gpg --gen-key
Anahtar Dahil Etme	gpg --import
Anahtar Aktarımı	gpg --export
Anahtarları Listeleme	gpg --list-keys
Özel Anahtar Listeleme	gpg --list-secret-keys
Anahtar İmzalama	gpg --sign-key
Anahtar Silme	gpg --delete-keys
Anahtar Geçersizleştirme	gpg --gen-revoke
Anahtar Gönderme	gpg --send-keys sunucu
Anahtar Alma	gpg --recv-keys sunucu

GnuPG İşlem Komut ve Seçenekleri

İmzalama	gpg --sign
Veri Kriptolama	gpg --encrypt
Dosya Kriptolama	gpg --encrypt-files
Fotoğraf Görme	gpg --show-photos
OpenPGP Uyumu	gpg --openpgp
PGP 2.x Uyumu	gpg --pgp2
Ascii Kalkan	gpg --armor

Anahtar Üretme (1)

```
# gpg --gen-key

gpg (GnuPG) 1.0.7; Copyright (C) 2002 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See the file COPYING for details.

Please select what kind of key you want:
   (1) DSA and ElGamal (default)
   (2) DSA (sign only)
   (4) ElGamal (sign and encrypt)
   (5) RSA (sign only)
Your selection? 4
```

Anahtar Üretme (2)

- The use of this algorithm is deprecated - create anyway? y
- About to generate a new ELG keypair.
- minimum keysize is 768 bits
- default keysize is 1024 bits
- highest suggested keysize is 2048 bits
- What keysize do you want? (1024) 2048
- Requested keysize is 2048 bits
- Please specify how long the key should be valid.
- 0 = key does not expire
- <n> = key expires in n days
- <n>w = key expires in n weeks
- <n>m = key expires in n months
- <n>y = key expires in n years
- Key is valid for? (0) 0

Anahtar Üretimi (3)

- Key does not expire at all
- Is this correct (y/n)? y
-
- You need a User-ID to identify your key; the software constructs the user id
- from Real Name, Comment and Email Address in this form:
- "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"
-
- Real name: Fatih Ozavci
- Email address: f.ozavci@btg.com.tr
- Comment:
- You selected this USER-ID:
- "Fatih Ozavci <f.ozavci@btg.com.tr>"
-
- Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O

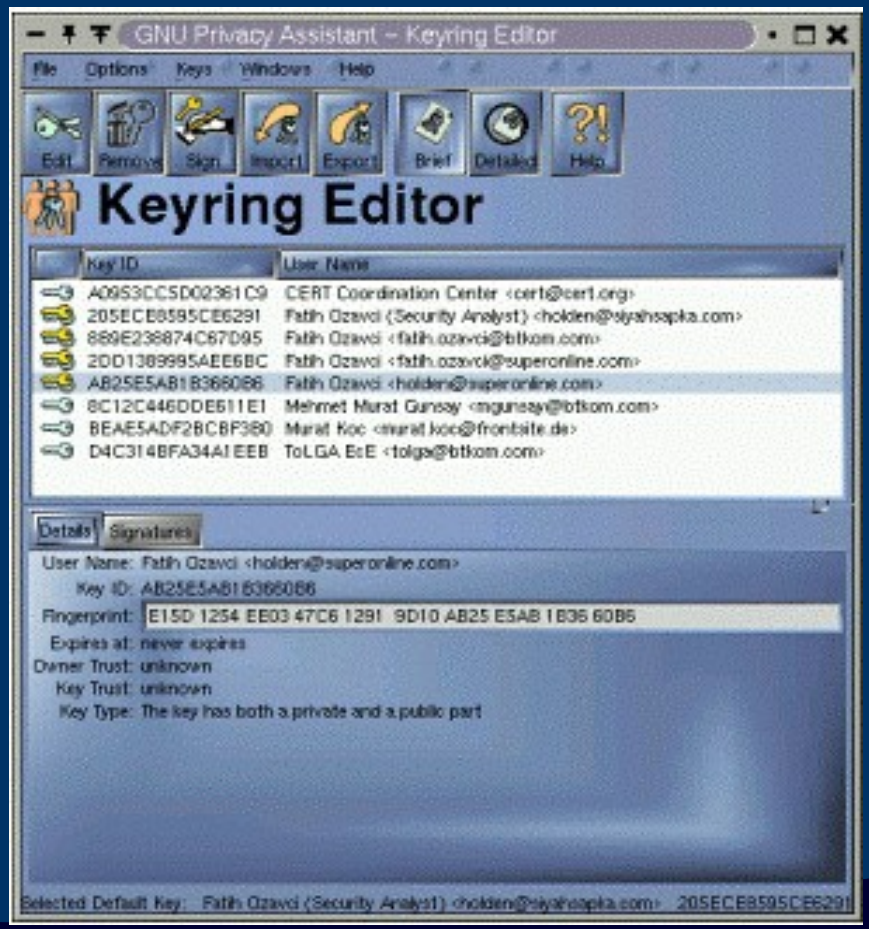
Anahtar Üretimi (4)

- You need a Passphrase to protect your secret key.
-
- Enter passphrase:
-
- We need to generate a lot of random bytes. It is a good idea to perform
- some other action (type on the keyboard, move the mouse, utilize the
- disks) during the prime generation; this gives the random number
- generator a better chance to gain enough entropy.
- .++++++++++++++++++++++++++.++++++++++++++++...++++++++++++++..++++++++++..++++++
++++++++.++++++++++++++++++++++++++.+++++.+++++.++++++++++...+++++..++++++++++++++
++>+++++.+++++>..++++
+.....>++++
+.....+++++^^^
- public and secret key created and signed.
- key marked as ultimately trusted.
-
- pub 2048G/629743BC 2003-02-04 Fatih Ozavci <f.ozavci@btg.com.tr>
- Key fingerprint = 88AE 5FDE 4A46 4A13 1867 2D29 FFCB 373C 6297 43BC

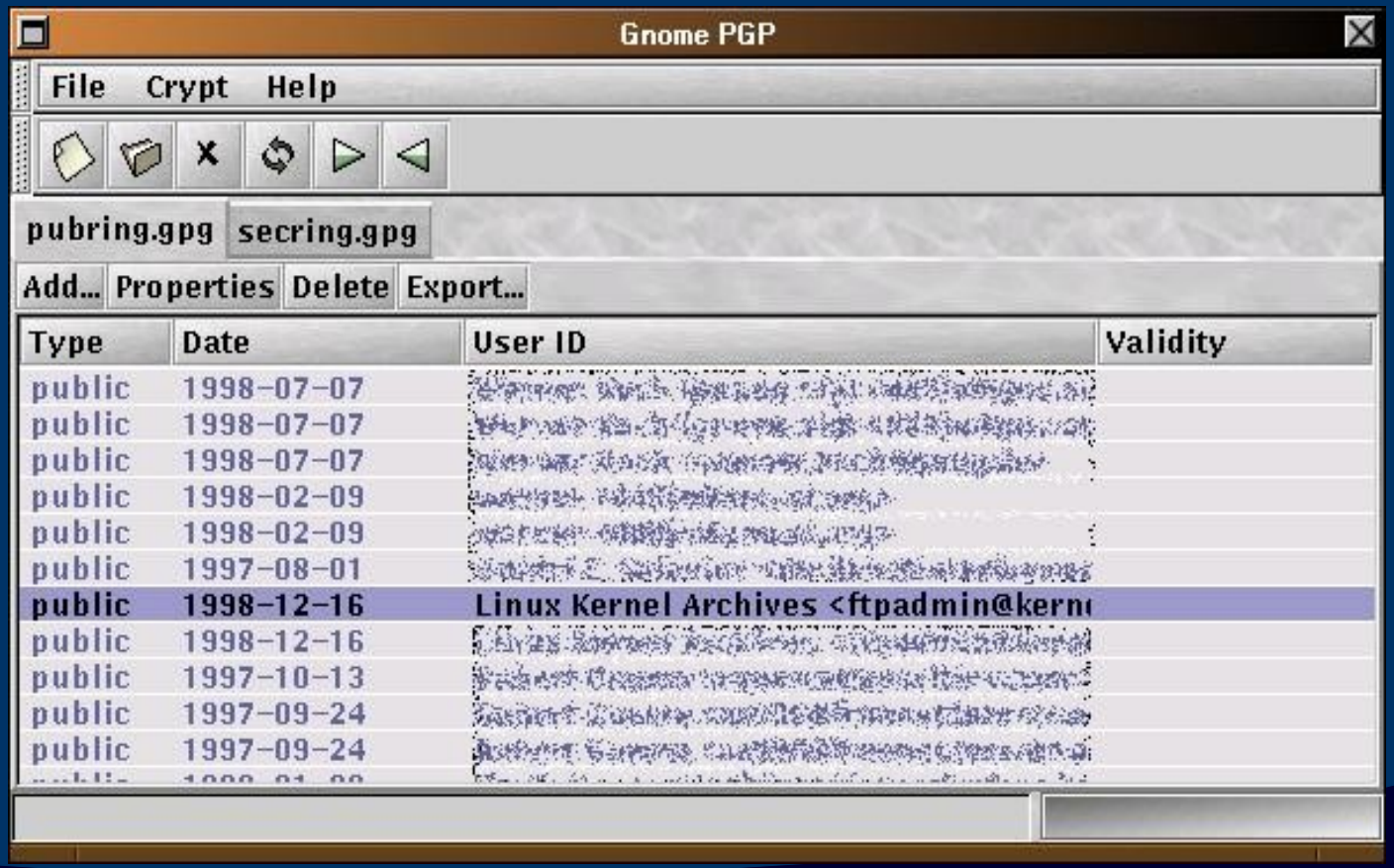
Destekleyen E-Posta İstemcileri

- Evolution
- Kmail
- Mutt
- Pine
- Sylpheed
- MS Outlook
- MS Outlook Express
- .....

Arayüzler - GPA



Arayüzler - GnomePGP



Kaynaklar

- Linux Security http://www.linuxsecurity.com
- PGP Homepage http://www.ipgp.com
- GnuPG Homepage http://www.gnupg.org
- GPA Homepage http://www.gnupg.org
- LinuxDOC http://www.linuxdoc.org
- Linux.ORG.TR http://www.linux.org.tr
- Siyah Şapka http://www.siyahsapka.com

Sorular ?

Teşekkürler.....