FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA
ZAVOD ZA ELEKTRONIČKE SUSTAVE I OBRADBU INFORMACIJA

PGP (Pretty Good Privacy)

Seminar iz kolegija:
"Sustavi za praćenje i vođenje procesa"

Dejan Ciglar
0036395083

Lipanj 2005.

SADRŽAJ

1. UVOD

PGP (Pretty Good Privacy) je program koji omogućava privatnost elektroničke pošte. Riječ je o programu koji kriptira (šifrira) poštu tako da je nitko ne može pročitati (dekriptirati) osim upravo osobe kojoj je namijenjen. Tekst nakon takvog procesa šifriranja nekoj trećoj strani izgleda kao besmisleni niz slučajnih znakova, i takve kriptirane poruke su sposobne "izdržati" i najsloženije kriptografske analize. No, nije samo šifriranje jedina mogućnost zaštite e-maila: moguće je na proizvoljan tekst dodati i digitalni potpis, bez šifriranja. To se obično primjenjuje kad je sadržaj javnog tipa, ali se želi osigurati da drugi mogu provjeriti autentičnost takvog materijala - budući da nitko neće moći promijeniti sadržaj bez da se ista lako detektira putem digitalnog potpisa.

2. KRIPTOGRAFIJA

Kriptografija je znanost koja koristi matematiku i matematičke metode za kriptiranje i dekriptiranje podataka. Kriptografija nam omogućava pohranjivanje ili transportiranje "osjetljivih informacija" preko nesigurnih komunikacijskih kanala bilo to korištenjem staromodnih pisama, radio odašiljača ili u današnje vrijeme interneta na način da nitko ne može pročitati sadržaj tajne informacije osim osobe kojoj je stvarno namijenjena. Sama enkripcija se sastoji od toga da se čisti tekst (ili bilo kakvu drugu informaciju) sakrije tj. prikaže na nerazumljiv način svima koji ne poznaju dekripcijski ključ.

Slika 1. Kriptiranje i dekriptiranje

Kriptografija ima dugu povijest. Postoje čak podaci da su Egipćani prije više od 4000 godina koristili kriptografske sustave za zaštitu informacija. Zna se da je još i u Rimskome carstvu Cezar koristio vrlo jednostavni algoritam kriptiranja. On je sva slova u testu pomaknuo za tri u desno. Kriptografija se počela ubrzano razvijat tijekom 2. svjetskog rata. Jedno od poznatijih kriptografskih metoda je bila njemačka Enigma. To je bio mehanički stroj za kriptiranje koji je pomoću rotora i mehaničkih kontakata šifrirala poruke te omogućava njemcima da tajno razgovaraju sa svojim podmornicama.

Početkom 60-ih sa razvojem računala došlo je do sve većih zahtjeva za zaštitom informacija a time i do razvoja kriptografije. U zadnjih 20-ak godina desila se prava eksplozije u razvoju kriptografije kod akademskih zajednica. Dok je klasična kriptografija bila u upotrebi već duže vrijeme, kompjuterska kriptografija se koristila pretežno u vojnoj domeni. Američka NSA (National Security Agency) i njihovi ekvivalenti u bivšem Sovjetskom savezu, Engleskoj, Izraelu, Francuskoj i drugdje potrošili su milijarde dolara na razno razne igre osiguranja svojih komunikacija. Privatne osobe sa manje znanja i novaca su bile bespomoćne u zaštiti svoje privatnosti. Danas je situacija bitno drugačija. Postoji puno sustava (i besplatnih) koji omogućavaju vrlo visoki nivo kriptiranja svakome tko želi.

Osnovni ciljevi kriptografije su:

- tajnost podataka: da podacima mogu pristupiti samo oni koji smiju
- integritet podataka: da se otkrije neovlaštena promjena podataka
- provjera identiteta: dokazivanje da su stranke u komunikaciji zaista one koje tvrde da jesu
- neosporivost: onemogućava sudioniku komunikacije da zaniječe svoje prethodne poruke

Postoji par osnovnih metoda enkripcije:

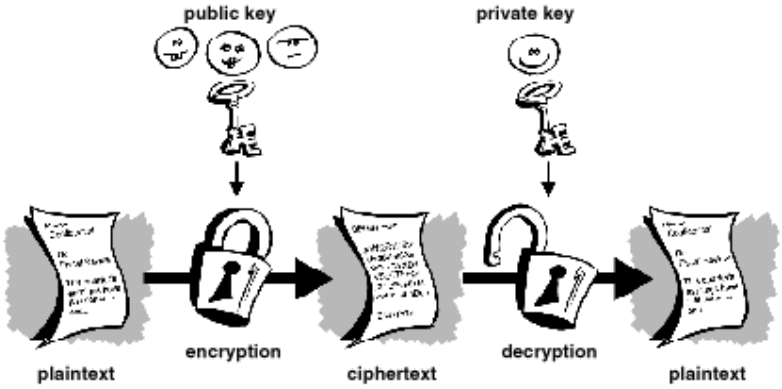
- **Konvencionalno kriptiranje** ili još poznato po nazivu kriptiranje **"simetričnim ključem"** koristi jedan ključ za enkripciju i dekripciju. Ovaj tip kriptiranja ima svoje prednosti. On je jako brz. Posebno je pogodan za kriptiranje podataka koji ne moraju "putovati". Tu se javlja problem sigurne razmjene ključeva koji uveliko poskupljuje siguran prijenos informacija. Da bi dvije stranke komunicirale moraju se usaglasiti oko tajnog ključa i moraju ga čuvati tajnim. Ako se oni nalaze na različitim fizičkim udaljenostima moraju vjerovati "kuriru" koji između njih dvoje razmijeniti dogovoreni ključ.

Slika 2. Konvencionalno kriptiranje

- Problem razmjene ključeva rješava metoda kriptiranja sa **"javnim ključem"**. Taj koncept je predstavljen od Whitfield Diffie i Martin Hellman 1975. Metoda javnog ključa je asimetrična šema koja koristi par ključeva za enkripciju:
  - Javni ključ: koji služi za kriptiranje podataka
  - Tajni ključ: koji služi za dekripciju

  Javni ključ objavimo svima koji žele sigurno komunicirati sa nama. Svatko sa kopijom javnog ključa može kriptirati podatke koje jedino mi možemo dekriptirati

pomoću našeg tajnog ključa. To nam omogućuje da komuniciramo i sa ljudima koje i ne poznajemo. Nemoguće je iz javnog ključa nikakvom metodom dobiti tajni ključ.



Slika 3. Kriptiranje javnim ključem

3. Povijesni pregled i nastanak PGP

Povijesni nastanak onoga što Englezi zovu *Public key cryptography* službeno je nastalo kada su 1976 advokat Whitfield Diffie i inženjer elektrotehnike Martin Hellman smislili javni i tajni ključ. 1977 Ron Rivest, Adi Shamir, Len Adleman su otkrili još generalniji algoritam koji je nazvan prvim slovima imena RSA. Ovaj algoritam se koristi i u PGP-u. Pri nastajanju ovih algoritama autori su imali velikih problema sa objavljivanjem rezultata jer NSA, američka organizacija, nije htjela da algoritam bude javno dostupan. No autori su preuzeli rizik i objavili rezultate koje su postigli u članku "New Directions in Cryptography". Za Pgp je važan i IDEA (International Data Encryption Algorithm) kojeg su osmislili Xuejia Lai i James Massey u Zurichu jer se njegov simetrični ključ koristi u Pgp algoritmu .

Za nastanak samog Pgp je glavni odgovorni Phill R. Zimmermann. Da osmisli PGP ga je naveo ovaj članak:

The 17 Apr 1991 New York Times reports on an unsettling US Senate proposal that is part of a counterterrorism bill. If this nonbinding resolution became real law, it would force manufacturers of secure communications equipment to insert special "trap doors" in their products, so that the Government can read anyone's encrypted messages. It reads: "It is the sense of Congress that providers of electronic communications services and manufacturers of electronic communications service equipment shall insure that communications systems permit the Government to obtain the plain text contents of voice, data, and other communications when appropriately authorised by law."

(This was 1991 Senate Bill 266 and it eventually failed to pass into law.)

U njemu ukratko se kaže da je vlada htjela uvesti zakon koji bi primoravao tvrtke koje se bave enkripcijom da u svojim algoritmima ostave mogućnost "stražnjih vrata" odnosno način na koji bi vlada mogla čitati sve kriptirane dokumente. Prvi PGP 1.0 je nastao kada je Phill R. Zimmermann implementirao RSA algoritam u kombinaciji sa simetričnim algoritmom svoga dizajna nazvanog Bass-o-Matic.

Počela je borba sa vladom koja je namjeravala uvesti ubrzano zakon koji bi PGP stavio izvan zakona. Korištene su sve metode pa su čak neki Phillovi prijatelji preko "pay phones" na BBS stavljali PGP kako im se ne bi moglo ući u trag. U međuvremenu

RSA se počinje buniti kako je korišten njihov patent bez dozvole. Phill pokušava prebaciti krivnju sa sebe na korisnike. Evo ulomka iz prvog PGP manuala :

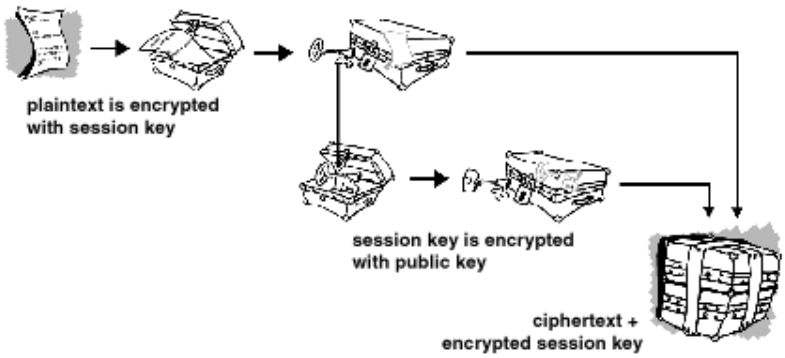
The RSA public key cryptosystem was developed at MIT with Federal funding from grants from the National Science Foundation and the Navy. It is patented by MIT (U.S. patent #4,405,829, issued 20 Sep 1983). A company called Public Key Partners (PKP) holds the exclusive commercial license to sell and sub-license the RSA public key cryptosystem. For licensing details on the RSA algorithm, you can contact Robert Fougner at PKP, at 408/735-6779. The author of this software implementation of the RSA algorithm is providing this implementation for educational use only. Licensing this algorithm from PKP is the responsibility of you, the user, not Philip Zimmermann, the author of this software implementation. The author assumes no liability for any breach of patent law resulting from the unlicensed use by the user of the underlying RSA algorithm used in this software

Pritisnut pravnim zahtjevima mora potpisati kako više neće distribuirati PGP, no on je već toliko uzeo maha da ga više nije bilo moguće kontrolirati. Ljudi su ga počeli skidati da vide oko čega se diže tolika buka i zbog čega je se američka vlada oko njega toliko zabrinula . Phill Zimmermann i njegovi suradnici su mogli mirno sjediti kod kuće i gledati kako se njihov program širi diljem svijeta i postaje najpoznatiji kripcijski program za široku uporabu.

U igru se uključuje i MIT koji je imao djelomična prava na RSA patent, i uz njihovo odobrenje Phill Zimmermann preuzima prava na distribuciju PGP. Više nije postojala legalna zabrana distribucije PGP-a.

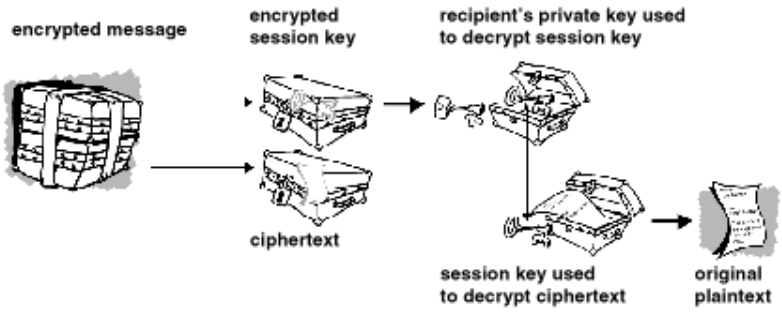
4. Kako radi PGP ?

PGP kombinira najbolje osobine oba kriptografskoga algoritma, konvencijalnog kriptiranja i kriptiranja s javnim ključem. Kada kriptiramo tekst sa PGP-om prvo se tekst komprimira. Postoji više razloga za komprimiranje teksta, a prvi je taj što se smanjuje veličina podataka koji se moraju prenositi i komprimirati. Bolji razlog je to što se postiže veća sigurnost kriptiranoga materijala jer se smanjuje uzorak teksta koji se može prepoznati, na primjer prepoznavanjem uzoraka, jer se tako izbacuju pojedina ponavljanja karakteristična za jezik. Idući korak je stvaranje *sesion key* (sjednički ključ), stvara se tako da se gledaju neki slučajni uzorci kao što je npr. micanje miša ili broj pritisnutih tipki. Njegova je uloga da omogući brzo kriptiranje, a da se ne izgubi na snazi dekripcije . Nakon toga se *sesion key* kriptira sa javnim ključem primatelja i to se šalje do primaoca preko mreže. Postupak je prikazan slikom 4.



Slika 4.

Sad kad smo poslali kriptirani tekst primaocu, logičan je korak otključavanja poslanog paketa, a taj radi u suprotnom smjeru. Prvo čitamo *sesion key* koji će nam poslije služiti da dekriptiramo sami tekst . Dakle obrnuti postupak je prikazan slikom 5 :

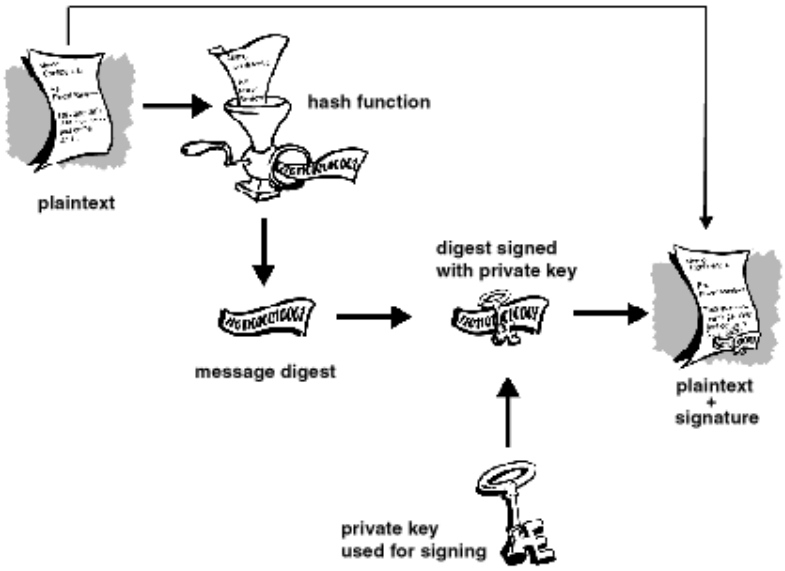


Slika 5.

Ključevi koji se koriste pri kriptiranju su dosta veliki, ali pri tome se mora znati procijeniti kolika je veličina ključa doista potrebna. Jako veliki ključ nosi sa sobom odgovornost velikoga vremena koje je potrebno za kriptiranje i dekriptiranje. Tajni simetrični ključ veličine 80 bita odgovara javnom ključu od 1200 bita (po sigurnosti), dakle što se toga tiče, prednost je koristiti simetrične ključeve. PGP sprema ključeve u posebne datoteke zvane *key rings* (koluti za ključeve).

5. Hash funkcije

Kod slanja i primanja poruka nam je dosta važno da znamo da je poruka koju smo dobili točna i cjelovita te da je takva odaslana od pošiljatelja. Hash funkcija se koristi tako da se uzme poruka varijabilne duljine koja može biti velika od nekoliko stotina do nekoliko milijuna bitova i od nje se pravi *mesage digest* konstantne veličine npr. 200 bita. Ako je i jedan bit poruke promijenjen *msage digest* će biti jako promijenjen. PGP koristi *mesage digtest* i privatni ključ te stvara "digitalan potpis". Digitalan potpis se šalje zajedno s porukum. Nije moguće ukrasti tuđe digitalne potpise. Hash funkcije igraju u PGP glavnu ulogu u validaciji i autentizaciji dokumenata.



Slika 6. Digitalan potpis

6. Digitalni certifikati i njihova distribucija

Digitalni certifikati imaju svrhu da dokažu da je netko ono što tvrdi za sebe da je. Digitalni certifikati u osnovi služe za autentifikaciju jer ono što je dosta bitno u komunikaciji je to da mi doista znamo s kime komuniciramo.
Digitalni certifikat se sastoji u osnovi od tri stvari:

- javnog ključa
- certifikata (korisničkoga ID ili neke druge informacije o korisniku)
- jednoga ili više digitalnih potpisa

Pri korištenju certifikata važan je i način prijenosa ili komunikacije među korisnicima. Pri malim grupama korisnika nije problem prenijeti ključeve manualno jedan po jedan, ali u velikim organizacijama i sa velikim brojem korisnika ta komunikacija postaje zamorna i složena. Zato su stvoreni CS (Certifikat Servers) koji služe za razmjenu i spremanje velikoga broja ključeva. Strukturirani sistemi koji nude osim spremanja ključeva kao CS i druge usluge kao što su manipulacije ključevima se zovu PKI (Public Key Infrastructures).

- CS (Certifikat Servers) imaju svrhu olakšati komunikaciju između korisnika pomoću treće povjerljive strane. Ovi serveri su u stvari baze podataka, no imaju i neke administrativne funkcije. Koristi se u velikim tvrtkama gdje nemaju svi pravo praviti svoje ključeve i spremati ih u bazu podataka.
- PKI (Public Key Infrastructures) osim funkcija čuvanja i spremanja imaju neke dodatne sposobnost, npr. izdavanje, ukidanje, manipulacija, ograničavanje certifikatima. U stvarnome svijetu pandan možemo naći u uredu za izdavanje putovnica. Tu se kao i kod PKI gleda vrijeme do kojeg je neki certifikat valjan i kada mu ta valjanost ističe.

Kod PGP razlikujemo dvije vrste certifikata:

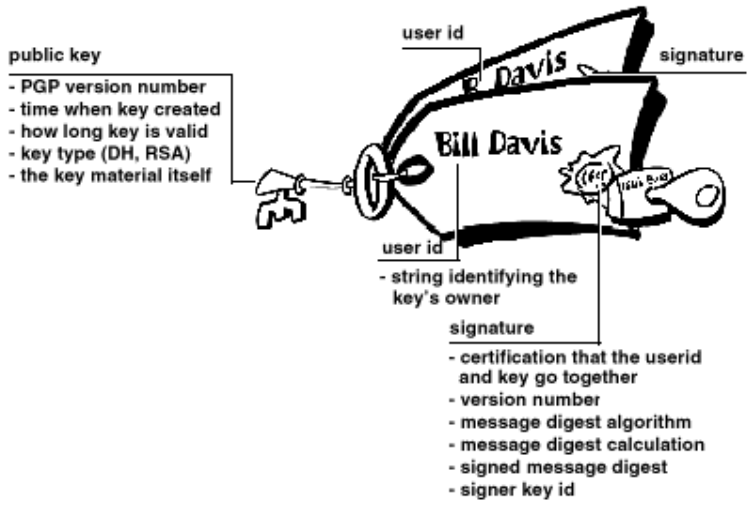
- PGP format
- X.509 format

PGP format

PGP format se sastoji (ali nije ograničen na njih) od nekoliko važnih točaka:

- Broj verzije PGP
- Certifikat o korisnikovu javnome ključu i algoritmima koji se koriste
- Certifikat o korisniku - Govori o tome koje je ime, ID ili neka druga osobina korisnika
- Digitalni potpis korisnika
- Datum odnosno rok trajanja - kada je napravljen i dokle vrijedi
- Preferirani korišteni algoritmi

Jedna stvar koja je karakteristična za PGP format certifikata je da nema ograničenja na broj osoba koje će potvrditi identitet neke druge osobe. Kod ovoga načina postoji više labela koje predstavljaju korisnika krenuvši od one najjednostavnije imena i prezimena do, slike, e-mali adrese i slično.



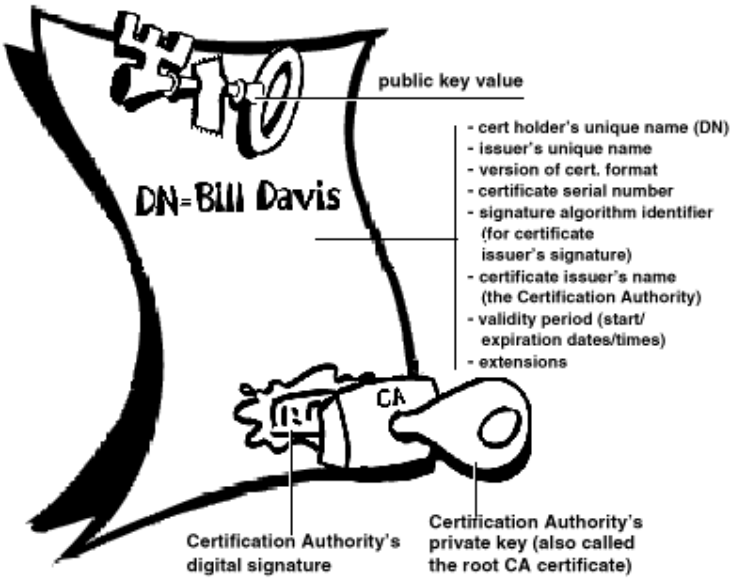
Slika 7. PGP certifikat

X.509 certifikaciski format

Svi X.509 certifikati su kompatibilni sa ITU-T X.509 međunarodnim standardom. To je u stvari polje koje sadrži skup korisnika i njihovih javnih ključeva. X.509 određuje što ide u certifikat i način na koji se dekodiraju podatci.

Sadrži slijedeće podatke:

- X.509 broj verzije
- Vlasnikov javni ključ
- Serijski broj certifikata (osoba koja stvori certifikat odgovorna je za stvaranje jedinstvenoga broja)
- Jedinstveno ime korisnika - teoretski pripisano samo tome korisniku
- Vrijeme valjanja certifikata
- Jedinstveno ime osobe koja je izdala certifikat
- Digitalni potpis izdavača
- Vrsta algoritma koja je korištena za kriptiranje



Slika 8. X.509 certifikat

Između X.509 i PGP postoje mnoge razlike. Tri najvažnije su:

- Pgp certifikat možemo načiniti sami a X.509 moramo zatražiti od CA(Certification authority)
- X.509 podržava samo jedno ime kao vlasnika ključa
- X.509 podržava smo jedan digitalni potpis koji autentizira korisnika

7. Pitanje pravovaljanosti i povjerenja

Problem pravovaljanosti ključa, odnosno saznanje da ključ kojim je neki dokument kriptiran ili dekriptiran valjan, je dosta velik i njemu se pridodaje dosta pažnje u Pretty Good Privacy jer gotovo da je isto činjenica da li nam je netko probio ključ ili podmetnuo nam svoj ključ. Kako bi bili sigurni u dotičnu informaciju mi moramo imati "treću stranu". To je nekakav server u kojem možemo pročitati i naći informaciju o korisniku. Kod PGP-a tu ulogu preuzima Certification Authorities (CA). Dakle najvažnija uloga CA je pridjeljivanje pravoga ključa pravoj osobi. Toj trećoj strani, moraju svi vjerovati da bi mogli normalno komunicirati .

Uspostava povjerenja

Ako nam neka osoba ne može potvrditi da je to ona sama napisala onda mi moramo vjerovati nekome drugome da je poruka valjana. O tome nam govori uspostava povjerenja među korisnicima. Mi imamo CA i njemu možemo vjerovati do neke granice broja korisnika i stranica, a kada pređemo takav broj moramo naći drugačiji način validacije.

Zbog toga CA ima pravo praviti nešto što se zove META-INTRODUCER. Nazovimo ju "četvrta strana" kojoj vjerujemo i ona nam predstavlja novi CA. To je prvi put korišteno u PGP-u. META-INTRODUCER nemaju sva prava kao CA, ali ih zamjenjuju do neke granice. Najvažnije je da oni nemaju pravo stvarati nove META-INTRODUCERE. U X.509 okružju oni se zovu *root CA* .

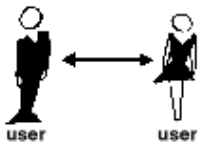
Modeli povjerenja

Pri uspostavi povjerenja možemo se ravnati na nekoliko načina pa tako i postoje tri načina uspostave povjerenja :

- Direktni model
- Hijerarhijski model
- Mreža povjerenja

- Direktni model

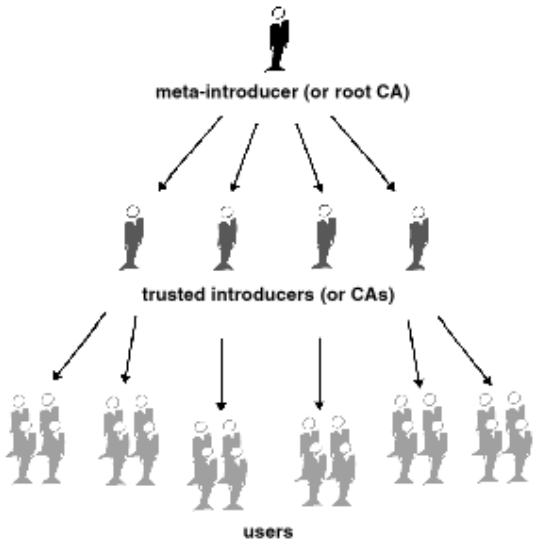
Najsigurniji model jer osoba koja je dobila ključ sigurno zna odakle potječe i prije je dogovoreno o kojemu ključu je riječ.



Slika 9. Direktni model

- Hijerarhijski model

Vrlo jednostavna raspodjela povjerenja. Svi vjeruju serveru koji imenuje svoje pomoćnike. Kod ovoga načina je važno povjerenje u server.



Slika 10. Hijerarhijski model

- Mreža povjerenja

Kod ovoga načina mi miješamo gornja dva načina, s tim da ostavljamo korisniku na izbor kome želi vjerovati. Nekoj stranoj osobi ili meta-itroduceru ili trusted-introduceru kako god želimo .

8. Zaključak

Nažalost, zbog svog relativno neobičnog razvoja i pokušaja da se u kasnijem razvoju legalizira (specifično na području USA), PGP dolazi u nekoliko inačica koji se ne razlikuju previše u osnovnoj funkcionalnosti, ali one starije (PGP2.x) neće nužno "razumjeti" sve dijelove PGP5 i PGP6 ključeva (PhotoID-jevi, podključevi, itd). PGP kao takav je danas komercijalni proizvod (koji je zapravo sve više namijenjen velikim korporativnim okolinama, a sve manje malim korisnicima), no postoje i slobodni i vrlo kvalitetni klijenti koji se pridržavaju OpenPGP (RFC2440) standarda, kao što je recimo GnuPG.

Kriptografski algoritmi koji se koriste za enkripciju i potpisivanje u PGP-u su vrlo razrađeni i danas nemaju skoro nikakve praktične kriptografske slabosti. Jasno, postoji niz rasprava na temu kvalitete korištenja RSA kao algoritma za koji se čini da je u praksi nešto slabije kvalitete od DH/DSS kombinacije: za sada je provaljen samo 512-bitni RSA ključ i to za 8000 MIPS godina, dok je sa druge strane provaljen tek 283-bitni DH ključ.

9. Literatura

http://www.pgp.com/

http://www.pgpi.org/

PGP Freeware for Windows 95, 98, NT, 2000 & Millennium / User's Guide :
ftp://ftp.pgpi.org/pub/pgp/7.0/docs/english/PGPWinUsersGuide.pdf