6. Programska oprema PGP z navodili za uporabo

6.1. Uvod

Zavod pri računalniškem izmenjevanju podatkov z izvajalci zdravstvenih storitev za kodiranje in elektronsko podpisovanje elektronskih sporočil uporablja program PGP - Pretty Good Privacy, ki je eden od najbolj uporabljenih programov za ta namen v svetu. Uporabljamo nekomercialno verzijo 2.6.3i, za katero ni potrebno pridobiti licence. Program je uporaben v MS-DOS, Microsoft Windows, OS/2, VMS, UNIX in drugih operacijskih sistemih.

Na priloženi disketi boste dobili datoteko za instalacijo programa PGP263I.ZIP.

Vsi ključi, ki jih uporabljamo v PGP, morajo biti dolžine 512 bitov. Isti ključi se uporabljajo za testiranje in produkcijsko (redno) izmenjevanje podatkov.

Za čim hitrejšo uporabo smo vam pripravili kratka navodila z napotki za instalacijo, kreiranje ključev, kodiranje in odkodiranje datotek, ter varovanje zasebnih ključev.

6.2. Instalacija programa

Za PGP datoteke kreirajte posebni direktorij na disku C:ÐPGP in odpakirajte datoteko PGP263I.ZIP s programom PKUNZIP, in sicer z ukazom:

pkunzip -d a:pgp263i

S tem boste dobili datoteki PGP263II.ZIP in PGP263II.ASC in nato ponovno odpakirajte še datoteko PGP263II.ZIP.

V datoteko AUTOEXEC.BAT je potrebno vpisati nastavitev okolja spremenjivke TZ z ukazom SET TZ=GTM-2 in ponovno pognati računalnik, da vpisani parametri stopijo v veljavo.

6.3. Administriranje ključev

Kodiranje sporočil se izvaja s pomočjo ključa, ki ga uporabnik izdela s pomočjo PGP programa. To je niz znakov, ki je dodatno zavarovan z geslom, ki ga pozna le uporabnik.

Uporabljamo sistem dvojnih ključev - javnega in zasebnega. Vsak pošiljatelj ima svoj zasebni ključ, ki je znan le njemu in ga lahko dodatno zavaruje z geslom. Da bi prejemnik lahko sporočilo odkodiral, mu mora biti znan pošiljateljev t.i. javni ključ.

PGP omogoča veliko načinov za administriranje ključev: pregledovanje, menjava identifikacijskega niza uporabnika (ime) ključa ali gesla, izločanje javnega ključa za namen pošiljanja le-tega prejemnikom sporočila.

Kreiranje ključev poženemo z ukazom:

pgp -kg

Program vpraša za dolžino ključa:

```
Pick your RSA key size:
    1)  512 bits- Low commercial grade, fast but less secure
    2)  768 bits- High commercial grade, medium speed, good security
    3)  1024 bits- "Military" grade, slow, highest security
Choose 1, 2, or 3, or enter desired number of bits:
```

Izberemo številko 1, kar pomeni 512 bitov dolgi ključ:

```
You need a user ID for your public key. The desired form for this
user ID is your name, followed by your E-mail address enclosed in
<angle brackets>, if you have an E-mail address.
For example: John Q. Smith <12345.6789Žcompuserve.com>
```

Program vpraša za ime uporabnikovega ključa:

```
Enter a user ID for your public key:
```

Vnesemo npr.:

zdrdom <elektronski naslov>

Sledi zahteva za dvakratni vnos gesla:

```
You need a pass phrase to protect your RSA secret key.
Your pass phrase can be any sentence or phrase and may have many
words, spaces, punctuation, or any other printable characters.
```

Geslo se vnaša dvakrat zaradi kontrole, da ga ne bi prvič pomotoma vnesli:

```
Enter pass phrase:
Enter same pass phrase again:

Note that key generation is a lengthy process.
.........**** ....****
Pass phrase is good. Just a moment....
Key signature certificate added.
Key generation completed.
```

Postopek izdelave para ključa je končan. Uporabnikov javni ključ je spravljen v datoteki PUBRING.PGP, zasebni ključ pa v datoteki SECRING.PGP.

Da bi prejemnik lahko preveril elektronski podpis pošiljatelja mu mora ta posredovati svoj javni ključ. To stori tako, da kopijo javnega ključa prepiše na disketo z ukazom:

pgp -kxa zdrdom a:zdrdom.asc

```
Extracting from key ring: 'pubring.pgp', userid "zdrdom".

Key for user ID: zdrdom <elektronski naslov>
512-bit key, key ID 8D966B51, created 1999/05/11

Transport armor file: a:zdrdom.asc

Key extracted to file 'a:zdrdom.asc'.
```

Sedaj imamo na direktoriju, kjer smo izdelali par ključev, še vedno javni in zasebni ključ pošiljatelja, na disketi pa samo javni ključ, ki ga pošljemo prejemniku.

Javni ključ prejemnika dodamo v PUBRING.PGP z ukazom:

pgp -ka a:zzzs.asc

```
Looking for new keys...
pub 1024/D390E9BD 1994/05/30 ZZZSIC <s=zzzsic/o=ic1/p=zzzs/a=mail/c=si>

Checking signatures...
```

Program sporoči, da je dodal en ključ. Po obvestilu, da eden od ključev ni certificiran na posebni način (funkcija PGP), program vpraša, če podpisnik sam jamči, da je javni ključ prejemnika pravi.

```
Keyfile contains:
    1 new key(s)

One or more of the new keys are not fully certified.
Do you want to certify any of these keys yourself (y/N)?
```

Odgovorite z “Y”.

```
Key for user ID: ZZZSIC <s=zzzsic/o=ic1/p=zzzs/a=mail/c=si>
1024-bit key, key ID D390E9BD, created 1994/05/30
Key fingerprint = 01 24 41 AA D4 0F 5F 1D 89 A3 04 12 78 CB 28 FC
This key/userID association is not certified.

Do you want to certify this key yourself (y/N)? y

Looking for key for user 'ZZZSIC <s=zzzsic/o=ic1/p=zzzs/a=mail/c=si>':

Key for user ID: ZZZSIC <s=zzzsic/o=ic1/p=zzzs/a=mail/c=si>
1024-bit key, key ID D390E9BD, created 1994/05/30
        Key fingerprint = 01 24 41 AA D4 0F 5F 1D 89 A3 04 12 78 CB 28 FC

READ CAREFULLY: Based on your own direct first-hand knowledge, are
you absolutely certain that you are prepared to solemnly certify that
the above public key actually belongs to the user specified by the
above user ID (y/N)?
```

Program zahteva še eno potrditev, da certificiramo pravi ključ. Še enkrat odgovorimo z “Y”.

```
You need a pass phrase to unlock your RSA secret key.
Key for user ID: zdrdom <elektronski naslov>
512-bit key, key ID 8D966B51, created 1999/05/11
```

Program nato zahteva vnos gesla, ki omogoča uporabo zasebnega ključa pošiljatelja in še vnos stopnje zaupanja za javni ključ prejemnika.

```
Enter pass phrase: Pass phrase is good. Just a moment....
Key signature certificate added.

Make a determination in your own mind whether this key actually
belongs to the person whom you think it belongs to, based on available
evidence. If you think it does, then based on your estimate of
that person's integrity and competence in key management, answer
the following question:

Would you trust "ZZZSIC <s=zzzsic/o=ic1/p=zzzs/a=mail/c=si>"
to act as an introducer and certify other people's public keys to you?
(1=I don't know. 2=No. 3=Usually. 4=Yes, always.) ?
```

Odgovorimo s 4, kar pomeni največjo stopnjo zaupanja.

S tem je postopek dodajanja in certificiranja javnega ključa prejemnika končan.

Javne ključe in certifikate lahko pregledamo z ukazom:

pgp -kvv

```
Key ring: 'pubring.pgp'
Type Bits/KeyID          Date       User ID
pub 1024/D390E9BD        1994/05/30 ZZZSIC <s=zzzsic/o=ic1/p=zzzs/a=mail/c=si>
sig  8D966B51   zdrdom <elektronski naslov>
pub 512/8D966B51         1999/05/11 zdrdom <elektronski naslov>
sig  8D966B51   zdrdom <elektronski naslov>
2 matching keys found.
```

Postopke zamenjave imena in gesla ključa si poglejte v priročniku za uporabo programa pgpdoc1.txt in pgpdoc2.txt, ki sta vključena v datoteki PGP263I.ZIP.

6.4. Kodiranje in odkodiranje datotek

Za kodiranje sporočila s prejemnikovim javnim ključem se uporablja ukaz:

pgp -e datoteka.txt zzzsic

datoteka.txt ..... ime datoteke, ki jo kodiramo
zzzsic ..... primer imena javnega ključa prejemnika

```
Recipients' public key(s) will be used to encrypt.
Key for user ID: ZZZSIC <s=zzzsic/o=ic1/p=zzzs/a=mail/c=si>
1024-bit key, key ID D390E9BD, created 1994/05/30
.
Ciphertext file: datoteka.pgp
```

Za kodiranje in podpisovanje se uporablja ukaz:

pgp -es datoteka.txt zzzsic -u zdrdom

datoteka.txt .. ime datoteke, ki jo kodiramo
zzzsic ..... primer imena javnega ključa prejemnika
zdrdom..... ime zasebnega ključa pošiljatelja

```
A secret key is required to make a signature.
You need a pass phrase to unlock your RSA secret key.
Key for user ID: zdrdom <elektronski naslov>
512-bit key, key ID 8D966B51, created 1999/05/11

Enter pass phrase:
```

Vnesemo geslo. Rezultat obeh ukazov je datoteka.pgp, ki je pripravljena za pošiljanje prejemniku.

Za odkodiranje datoteke in preverjanje podpisa se uporablja ukaz:

pgp datoteka.pgp -o r-datoteka.txt

datoteka.pgp ..... kodirana datoteka
r-datoteka.txt..... ime datoteke v katero bomo shranili odkodirane podatke

6.5. Varovanje zasebnega ključa

Priporočljivo je, da ključe prepišemo tudi na disketo in jo spravimo na varno zaklenjeno mesto. Na disketo prepišemo datoteke PUBRING.PGP, SECRING.PGP, CONFIG.TXT in RANDSEED.BIN.

Če iz kakršnegakoli razloga (okvara diskete, diska, nenamerno brisanje,..) izgubite ključ, je potrebno izdelati novega in ga poslati prejemniku.

Zasebni ključ je sestavljen iz razmeroma dolgega niza binarnih podatkov in si ga zato ni preprosto zapomniti, zaradi tega je zapisan v datoteki, ki jo hranimo na magnetnem mediju. Da pa te datoteke ne moremo nepooblaščeno uporabljati, je varovana z geslom (tajni stavek). Geslo mora biti dovolj dolgo, saj se tako zmanjša nevarnost za hitro razkritje. Sestavljeno naj bo iz nekaj besed ali pojmov, ki so med seboj nenavadno povezani ali pa sploh nimajo povezave, tako, da jih ni možno uganiti. Če si geslo zapišete, ga shranite na varnem mestu, nikakor pa ga ne zapišite na ovojnico diskete, na kateri hranite svoj zasebni ključ.