

POSTUP PRI PRÁCI S PGP

Úvod

Táto príručka slúži užívateľom ako pomôcka pri práci s aplikáciou PGP v.2.6.3i. Ide o voľne šíriteľnú verziu určenú na šifrovanie súborov v prostredí MS DOS, alebo v príkazovom režime prostredia Windows. Predpokladom pre prácu s uvedenou aplikáciou je základná znalosť PC.

Inštalácia programu

- 1) Na disku C vytvoriť adresár PGP, nakopírovať do neho šifrovací program (PGP263i.zip) a dekomprimovať ho.
- 2) V AUTOEXEC.BAT nastaviť nasledovné:

```
SET PGPPATH = C:\ PGP
```

```
SET TZ = GMT-1
```

```
SET PATH=C:\PGP;%PATH%
```

V prípade práce v prostredí Win 2000/XP alebo Win NT, nastavenie vykonať cez ponuku Control panel / Systems / Enviroment nasledovne:

Variable: TZ Value: GMT-1

Variable: PGPPATH Value: C:\ PGP

Variable: PATH Value: C:\PGP;%PATH%

Upozornenie: Po nastavení je potrebné zavrieť súborový manažér jako napr.FAR (príp.NC), aby načítal nové údaje.

Generovanie a výmena kľúčov

- 1) Zadať do príkazového riadku príkaz pre vygenerovanie kľúčov:

```
PGP -kg.
```

Následne systém sa opýta na:

- a) silu kľúča 1024 bits (číslo 3)
- b) ID: meno klienta

- c) HESLO: môžete si zvoliť ľubovoľné heslo
- d) Generovanie: je potrebné stlačiť ľubovoľné klávesy až kým systém nezastaví

2) Vyexportovať svoj verejný kľúč príkazom:

PGP -kxa ID

Na otázku systému zadať znova ID

Systém vytvorí súbor s názvom ID.asc, ktorý treba nahrať na disketu/CD/USB kľúč a doručiť do banky.

3) Naimportovať verejný kľúč banky príkazom:

PGP -ka pabk.asc

Na prvé tri otázky systému stlačiť Y , následne zadať heslo a stlačiť numerickú klávesu s číslom 4.

Šifrovanie a dešifrovanie súborov

1) Súbor šifrovať príkazom:

PGP -e názov súboru pabk

2) Súbor dešifrovať príkazom:

PGP názov súboru.pgp názov súboru.txt

potvrdiť a zadať svoje heslo.