Kreiranje ključa za šifriranje dokumenata i mailova {gpg}

written by js | 2021-08-18

Tema

Kreiranje ključeva za razmjenu e-poruka i dokumenata na siguran, šifriran način, šifriranje datoteka, teksta, ...

Postupak – tl;dr

Instaliranje i priprema

(..uskoro..)

Kreiranje ključa

Brzinsko

- `gpg --quick-gen-key ime.prezime@domena.tld rsa4096 cert,auth,sign,encr never`

Kreiranje ključa skriptom

iliti "*Unattended key generation*"

- Kreiraj datoteku "`podaci_za_kljuc.txt`":
- ```
  %echo Generiram...
  Key-Type: RSA
  Key-Length: 4096
  Subkey-Type: RSA
  Subkey-Length: 4096
  ```
  ```

```
Key-Usage: encrypt,sign,auth,cert
Name-Real: ime.prezime
Name-Comment: ime.prezime
Name-Email: ime.prezime@domena.tld
Expire-Date: 0
Passphrase: admin123
%commit
%echo Gotovo
```

- kreiraj ključ:`gpg --batch --full-generate-key podaci_za_kljuc.txt`
- provjeri: `gpg --list-secret-keys`

https://www.gnupg.org/documentation/manuals/gnupg/Unattended-GPG-key-generation.html

Izvoz privatnog ključa (private key)

..kojega ne daješ nikome

- `gpg --export-secret-key --armor ime.prezime@domena.tld > ime.prezime@domena.tld.PRIVATNI_TAJNI.SECRET.key`

Izvoz javnog ključa (public key)

..kojega daješ osobama s kojima razmjenjuješ šifrirane poruke/dokumente; i oni tebi trebaju dati svoj javni ključ

- `gpg --export --armor ime.prezime@domena.tld > ime.prezime@domena.tld.javni.public.key`

Povjerenje i potpis

Osobe A i B sada trebaju izmijeniti javne ključeve (jer, jelte, to su javni ključevi)

Moraju im vjerovati i potpisati njihove javne ključeve svojim privatnim ključevima

Slike

…

Video

…

---

gpg xgpgx key xkeyx xprivatex xpublicx xencryptionx xšifriranjex xprivatnostx Unattended full key generation xunattended xfull xkey xgeneration keygen xkeygen secret xsecret secret key xsecret xkey public key xpublic pgp xpgp tplt xtplt ssh ssl xssh xssl