SSL - Convert PBX

Berikut langkah-langkah lengkap (dengan perintah OpenSSL dan konfigurasi nginx) untuk mengambil isi dari file `.pfx` yang diproteksi password. Berikut langkah-langkah praktis dan langsung bisa dijalankan di server Linux (atau WSL/Git-Bash di Windows).

1. Periksa isi .pfx (opsional, hanya melihat)
akan diminta Import Password — masukkan password .pfx Anda

```
openssl pkcs12 -info -in mycert.pfx
```

2. Ekstrak private key (tanpa encrypt / tanpa passphrase) (Legacy Mode)
Note : **OpenSSL versi terbaru (3.x)** sudah *drop support* untuk algoritma lama RC2-40-CBC yang dipakai oleh Microsoft PFX. Jadi OpenSSL Anda tidak bisa membaca bagian CA chain (bagian PKCS7 Encrypted data).

```
openssl pkcs12 -in ilusi.pfx -nodes -legacy -out ilusi-all.pem
```

3. Pisahkan file hasil ekstrak

```
# Private key (BEGIN PRIVATE KEY sampai END PRIVATE KEY)
awk 'BEGIN {p=0} /BEGIN PRIVATE KEY/ {p=1} p; /END PRIVATE KEY/ {p=0}' ag-all.pem > key.pem


# Certificate (BEGIN CERTIFICATE sampai END CERTIFICATE)
awk 'BEGIN {p=0} /BEGIN CERTIFICATE/ {p=1; i++} p {print > "cert" i ".pem"} /END CERTIFICATE/ {p=0}' ag-all.pem
```

Hasilnya:

- `key.pem` → private key
- `cert1.pem` → biasanya **server certificate**
- `cert2.pem`, `cert3.pem` → biasanya **CA intermediate/root**

Gabungkan cert nya :

```
cat cert1.pem cert2.pem cert3.pem > fullchain.pem
```

4. Simpan ke lokasi standar

```
sudo mkdir -p /etc/ssl/private /etc/ssl/certs
sudo mv key.pem /etc/ssl/private/ilusi.key
sudo mv fullchain.pem /etc/ssl/certs/ilusi-fullchain.pem
```

```
sudo chmod 600 /etc/ssl/private/ilusi.key
sudo chmod 644 /etc/ssl/certs/ilusi-fullchain.pem
```

Revision #1
Created 29 September 2025 02:30:50 by Kevin
Updated 29 September 2025 02:41:39 by Kevin