□□ Hoe gebruik je Public en Private Keys in WireGuard?

WireGuard gebruikt **public key cryptografie** (ook wel "asymmetrische encryptie") om veilige verbindingen op te zetten. Hierbij heb je twee sleutels per apparaat:

- **Private Key (Privésleutel)**: Deze hou je geheim. Alleen het apparaat zelf mag deze kennen.
- **Public Key (Publieke sleutel)**: Deze mag je delen met andere apparaten.

□□ Hoe werkt dit in de praktijk?

Denk aan het als een soort slot en sleutel mechanisme:

- Je **private key** is de **sleutel**.
- Je **public key** is het **slot** dat bij die sleutel hoort.

Alleen de juiste sleutel (private key) past op het slot (public key), en andersom werkt het niet.

In WireGuard:

- De **client** gebruikt zijn **private key** om zich te authenticeren.
- De **server** gebruikt zijn **public key** van de client om die te herkennen (en andersom).

□□ Sleutels genereren en uitwisselen

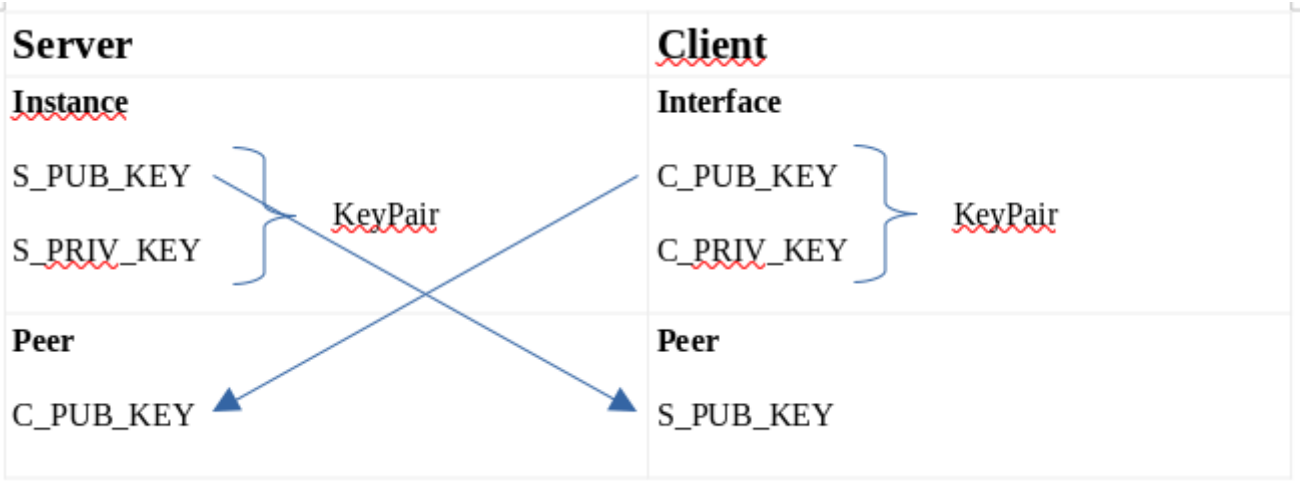
Bijvoorbeeld:

	Server	Client (mobiele telefoon)

Private Key	`S_PRIV_KEY` (geheim)	`C_PRIV_KEY` (geheim)
Public Key	`S_PUB_KEY` (maggedeeld worden)	`C_PUB_KEY` (mag gedeeld worden)

Je doet dan het volgende:

- Op de **server** voeg je een **peer** toe:
  - Public key van de **client**: `C_PUB_KEY`
  - Allowed IPs van de client (bv. `10.6.0.2/32`)
- Op de **client** voeg je een **peer** toe:
  - Public key van de **server**: `S_PUB_KEY`
  - Endpoint (IP of domeinnaam + poort) van de server
  - Allowed IPs (bv. `0.0.0.0/0` om al het verkeer via VPN te sturen)



In Debian, waar ik zelf mee werk, maak je een keypair als volgt aan:

Create the private key for WireGuard and change its permissions using the following command:

```
wg genkey | tee /etc/wireguard/private.key && chmod go= /etc/wireguard/private.key
```

The next step is to create the corresponding public key derived from the private key. Use the following command to **create the public key file**:

```
cat /etc/wireguard/private.key | wg pubkey | tee /etc/wireguard/public.key
```

□□ Voorbeeldconfiguratie (basis)

□□ Voorbeeldconfiguratie (basis)

Serverconfig (bijv. OPNsense WireGuard instance):

```
[Interface]
PrivateKey = S_PRIV_KEY
Address = 10.6.0.1/24
ListenPort = 51820

[Peer]
PublicKey = C_PUB_KEY
AllowedIPs = 10.6.0.2/32
```

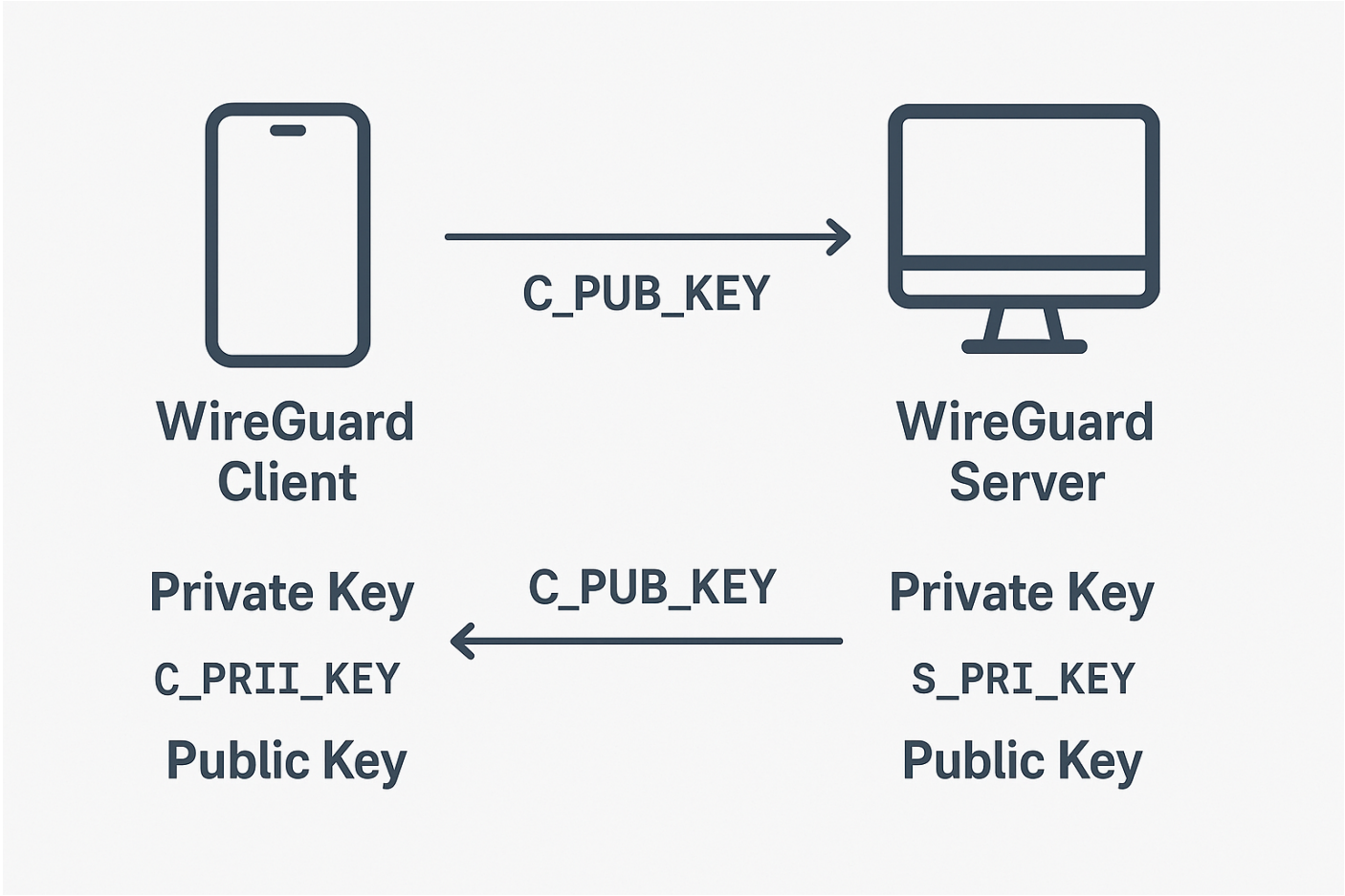
Clientconfig (mobiele telefoon):

```
[Interface]
PrivateKey = C_PRIV_KEY
Address = 10.6.0.2/24

[Peer]
PublicKey = S_PUB_KEY
Endpoint = jouw.domein.nl:51820
AllowedIPs = 0.0.0.0/0, ::/0
```

□□ Belangrijk

- Je **mag nooit** de private key delen.
- Je **moet altijd** de public key van de andere partij in jouw configuratie zetten.
- De sleutelparen worden automatisch gegenereerd met tools zoals `wg genkey` (CLI), of via de GUI (zoals in OPNsense of mobiele apps).



Revisie #4
Gemaakt: 25 mei 2025 16:06:37 door Gert
Bijgewerkt: 26 mei 2025 06:20:14 door Gert