

creazione chiave ssh per trust tra due server

Ultimo aggiornamento: 2026-09-18

Creazione di una chiave SSH (Ed25519) e configurazione del trust tra due o più server, per accedere senza password.

1. Creare la chiave

```
ssh-keygen -t ed25519 -C "tua.email@esempio.com"
```

- -t ed25519: algoritmo moderno, chiave corta e sicura.
- -C: commento identificativo (consigliato l'email).
- Premere Invio per accettare il percorso di default (~/.ssh/id_ed25519) e, volendo, una passphrase.

2. Copiare la chiave pubblica sui server

```
ssh-copy-id utente@serverA  
ssh-copy-id utente@serverB
```

ssh-copy-id aggiunge la chiave pubblica a ~/.ssh/authorized_keys di ciascun server: da quel momento l'accesso con chiave funziona senza password.

3. Verificare il trust

```
ssh utente@serverA 'hostname'  
ssh utente@serverB 'hostname'
```

Se risponde senza chiedere la password, il trust è attivo.

Note

- I permessi contano: ~/.ssh deve essere 700 e authorized_keys 600, altrimenti sshd ignora la chiave.
- La chiave privata (id_ed25519) non va mai copiata sui server: resta solo sul client.