

SSH-Key

Inhaltsverzeichnis

- [1 Funktionsweise](#)
- [2 Einsatz](#)
- [3 Sicherheit](#)
- [4 Fazit](#)

Ein SSH-Key ermöglicht die Anmeldung per Schlüsselpaar statt per Passwort. Bei richtiger Verwendung erhöht er Sicherheit und Komfort administrativer Zugänge.

Ein [SSH](#)-Key besteht aus einem privaten und einem öffentlichen Schlüssel. Der öffentliche Schlüssel wird auf dem Zielsystem hinterlegt, während der private Schlüssel beim Benutzer verbleibt.

1 Funktionsweise

Bei der Anmeldung weist der Client nach, dass er den passenden privaten Schlüssel besitzt.

- **Public Key:** darf auf Servern hinterlegt werden.
- **Private Key:** muss geheim bleiben.
- **Passphrase:** schützt den privaten Schlüssel zusätzlich.

2 Einsatz

[SSH](#)-Keys werden für Serverzugänge, Deployments, [Automatisierung](#) und [Git](#)-Repositories genutzt.

- Administrativer Serverzugriff.
- Automatisierte Backups oder Deployments.
- Authentifizierung bei [Git](#)-Diensten.

3 Sicherheit

[SSH](#)-Keys sind nur sicher, wenn sie sorgfältig verwaltet werden.

- Private Keys nicht weitergeben.
- Alte Keys aus `authorized_keys` entfernen.
- Nach Möglichkeit Passwortlogin deaktivieren.

4 Fazit

[SSH](#)-Keys sind ein Standardwerkzeug sicherer Administration und sollten mit Passphrase, sauberer Rechtevergabe und regelmäßiger Pflege genutzt werden.