

SSL-Zertifikat erstellen für SFTP SSH Übertragung

Schritt-für-Schritt: SSH-Key mit PuTTYgen erstellen

☐ 1. PuTTYgen starten

- ☐ Geh zu deinem Startmenü → PuTTYgen
- ☐ (Falls nicht installiert: [Download hier](#))

☐ 2. Key-Typ und Größe auswählen

- ☐ Type: RSA oder ED25519 (ED25519 ist moderner, aber RSA ist universeller – wenn du unsicher bist, nimm RSA 4096)
 - Bits: 4096 (für RSA)

☐ 3. Key generieren

- ☐ Klicke auf „Generate“
- ☐ Bewege die Maus im Feld, um den Schlüssel zu erzeugen

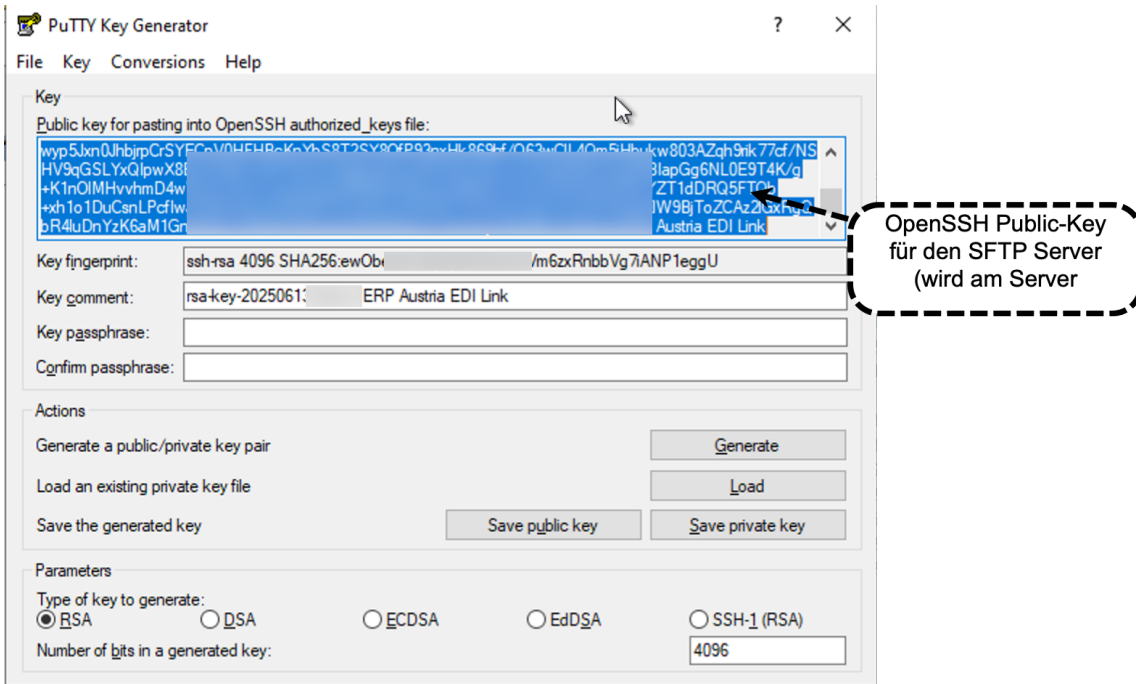
☐ 4. Kommentar setzen

- ☐ Im Feld „Key comment“ kannst du z. B. `italcos-prod@firma.com` eintragen

☐ 5. Schlüssel speichern

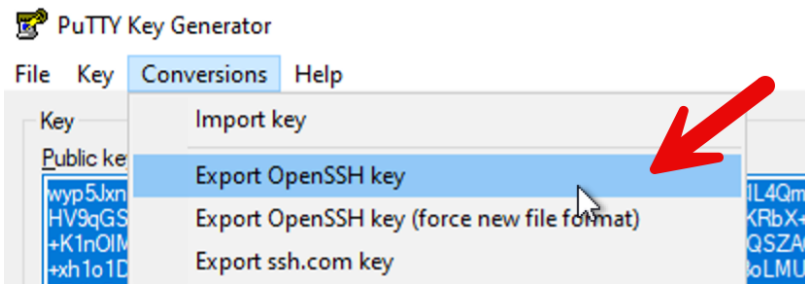
- ☐ Klicke auf:
 - ☐ Save private key → z. B. `id_rsa.ppk`
 - ☐ Save public key → z. B. `id_rsa.pub`

Wichtig: Umwandlung in OpenSSH-Format
Public Key: (Wird am SFTP-Server hinterlegt)



Private Key in OpenSSH umwandeln:

(wird für den Client verwendet. z. B. Filezilla, EDI4BW)



INFO:

Der private-Key wird immer im FTP-Client eingetragen und darf NICHT weitergegeben werden. Der Public Key wird im SFTP-Server eingetragen und beim entsprechenden User hinterlegt.

Revision #4

Created 2025-06-13 16:19:02 CEST by Martin Dauwa

Updated 2025-07-21 17:15:05 CEST by Martin Dauwa