CSR erstellen

Diese Seite befindet sich aktuell noch im Aufbau ⚠️

Bevor Sie ein Nutzerzertifikat oder Serverzertifikat von einer CA (Certificate Authority) anfordern, müssen Sie ein Schlüsselpaar erstellen.

Ein CSR ist ein **digitaler Antrag**, aus einem öffentlichen Schlüssel ein digitales Zertifikat zu erstellen.

Hinweis

Wenn Sie bei der Erstellung Ihres Nutzerzertifikats die Option **„Key Generation“** wählen, ist das Erstellen eines CSRs nicht erforderlich.

Was ist ein Schlüsselpaar?
Schlüsselpaare bestehen aus einem öffentlichen und einem privaten Schlüssel. Mit einem öffentlichen Schlüssel werden Daten verschlüsselt. Der private Schlüssel ist der Teil des Schlüsselpaars, der geheim bleibt und niemandem weitergegeben werden darf. Mit einem privaten Schlüssel werden Daten entschlüsselt. Der öffentliche Schlüssel ist nicht geheim und kann an jeden weitergegeben werden. Schlüsselpaare verwenden einen Algorithmus, mit dem Informationen von lesbarem Text in verschlüsselte Daten transformiert werden.

Was ist die Schlüssellänge?
Der Schlüssel Ihrer digitalen Identität hat eine bestimmte Länge. Je länger er ist, desto schwerer können andere ihn entschlüsseln und missbrauchen. Eine größere Schlüssellänge verlangsamt jedoch auch alle Aktionen mit diesem Identitätsschlüssel. Die Schlüssellänge wird in „Bit“ gemessen.

Schlüsselpaar erstellen

Anleitungen für die Betriebssysteme:

- CSR unter macOS
- CSR unter Ubuntu
- CSR unter Windows