

CSR (Certificate Signing Request)

CSR (Certificate Signing Request)

Ein CSR (Certificate Signing Request), zu Deutsch Anforderung auf Ausstellung eines Zertifikats, ist eine speziell formatierte und verschlüsselte Nachricht. Die wird von einem Antragsteller für ein digitales SSL-Zertifikat ([Secure Sockets Layer](#)) an eine CA (Certificate Authority / Zertifizierungsstelle) gesendet. Der CSR bestätigt die Informationen, die eine CA benötigt, um das [Zertifikat](#) ausstellen zu können.

Ein [PKI-System \(Public Key Infrastructure\)](#) ermöglicht den sicheren Austausch von Daten über das Internet zwischen verifizierten Parteien. In so einem System muss vor der Bestellung und dem Kauf eines SSL-Zertifikats ein CSR erschaffen werden. Der Antragssteller muss zunächst ein Schlüsselpaar generieren. Der [Private Key](#) (privater Schlüssel) dient zu Entschlüsselung der verschlüsselten Daten und der Generierung von [digitalen Signaturen](#). Den [Public Key](#) (öffentlichen Schlüssel) benutzt man, um die Daten zu [verschlüsseln](#) und die Signaturen zu verifizieren. Sie müssen sowohl das Schlüsselpaar als auch den CSR auf dem [Server](#) erstellen, auf dem Sie das SSL-Zertifikat benutzen wollen. Das ist zwingend erforderlich, um die Integrität des Schlüsselpaars und der PKI im Allgemeinen zu garantieren.

Sobald das Schlüssel-Paar präpariert ist, kann der CSR generiert werden. Die CA wird all die notwendigen Daten des CSRs (siehe Tabelle) verwenden, um das Zertifikat

auszustellen. Wie ein CSR generiert wird, hängt von der eingesetzten Webserver-Software ab. Sobald der CSR erstellt ist, kann man ihn bei der CA einreichen. Ist ein Antrag erfolgreich und für gültig erklärt, wird die CA das SSL-Zertifikat ausstellen und unterzeichnen.

| Information | Beschreibung | Beispiel |
|--------------------------------|--|---|
| Common Name | Der FQDN (Fully Qualified Domain Name) des entsprechenden Servers. | www.meinefirma.de mail.meinefirma.de * |
| Business Name / Organization | Der offizielle Name Ihres Unternehmens | Meine Firma, Mein Unternehmen |
| Department / Organization Name | Die Abteilung Ihres Unternehmens, die für das Zertifikat verantwortlich ist. | IT, Finanz-Abteilung |
| City / Town | Die Stadt, in der Ihre Firma den Sitz hat. | München, Hamburg |
| State & County / Region | Das Bundesland oder die Region, in der sich Ihre Firma befindet. Verwenden Sie hier keine Abkürzungen. | Bayern, Hessen |
| Country | Der zweistellige ISO-Code für das Land, in dem sich Ihr Unternehmen befindet. | DE, US |

| | | |
|---------------|---|--|
| Email Address | Eine E-Mail-Adresse, um die Firma kontaktieren zu können. | admin@meinefirma.de zertifikate@meinefirma.de |
|---------------|---|--|

** Generiert man einen CSR für ein so genanntes Wildcard-Zertifikat, sollte der Common Name mit einem * beginnen. Ein Beispiel wäre *.meinefirma.de*