

Austausch SSL-Server-Zertifikate

Folgende Voraussetzungen müssen zum Zertifikatstausch gegeben sein: → Auflösbarer DNS-Name des Servers → Aktuelles mp-System (stable)

CSR erzeugen

Im ersten Schritt muss ein CSR erzeugt werden, für den dann das neue SSL-Zertifikat ausgestellt werden kann. Die Erzeugung des CSR auf dem mp-Server erfolgt wie nachfolgend beschrieben:

- Anmeldung als Administrator **config** auf dem mp-Server und Auswahl des Menüpunkts **SSL-Verwaltung > Zentralschlüssel CSR**.
- Die Abfrage, ob ein **Wildcard-Zertifikat** angefordert werden soll mit **Nein** beantworten, es sei denn es gibt den Sonderfall, dass ein Wildcard-Zertifikat verwendet werden soll.
- Im nachfolgenden Menü sind folgende Felder auszufüllen:

Feld	Wert
Organizational Unit (OU)	[Name des Servers] [Standort] Bsp.: mp-cloud Berlin
Common Name (CN)	Domänenname, für die das Zertifikat ausgestellt wird. Bsp. mp-cloud.m-privacy.de

Hinweis: Außer dem Common Name (CN) werden keine Informationen im später ausgestellten Zertifikat angezeigt.

- Über den Menüpunkt **Speichern** die Einstellungen sichern.
- Dann über den Menüpunkt Erzeugen den CSR-Request erstellen lassen. Dieser wird im Anschluss direkt angezeigt. Der Abschnitt, welcher mit „**—BEGIN CERTIFICATE REQUEST—**“ beginnt markiert den Anfang des CSR. Nun kann man den CSR herauskopieren, um ihn für die Bestellung des neuen SSL-Zertifikats beim Dienstleister zu nutzen.
- Alternativ kann man sich auch jederzeit den CSR über den Menüpunkt **SSL-Verwaltung > Zertifikats-CSR anzeigen** am Bildschirm anzeigen lassen.
Hinweis: Bei SSL-Zertifikaten für E-Mail oder virtuelle Webdomänen den CSR-Request aus dem jeweiligen Unterpunkt anzeigen lassen.

SSL-Zertifikat einspielen

Sind die SSL-Zertifikate ausgestellt und liegen diese vor, dann sollten Sie zwei Dateien haben. Zum einen die Datei mit dem Zertifikat (in der Anleitung **certificate.crt** genannt) und die Datei mit der CA, bzw. dem Bundle aller CA-Dateien (in der Anleitung **cabundle.ca** genannt).

Liegen diese Dateien vor, erfolgt das Einspielen (für den Hauptwebserver) wie folgt:

- Per SCP sind die beiden Dateien (certificate.crt und cabundle.ca) in das Transfer-Verzeichnis des Administrators **config** zu laden.
- Nun als Administrator **config** unter dem Menüpunkt **SSL-Verwaltung > Fremdzertifikat importieren** den Import der Zertifikate starten. Es öffnet sich ein Assistent, bei dem im ersten

Schritt nach der **Zertifikats-Datei** gefragt wird. Hier ist das Zertifikat (**certificate.crt**) auszuwählen und mit Auswahl zu bestätigen. Es wird nun gefragt, ob die Zertifikatsdatei überschrieben werden soll. Dies ist mit JA zu bestätigen.

- Im nächsten Schritt wird nach der **CA-Zwischen-Zertifikats-Datei** gefragt. Hier ist die CA-Datei (**cabundle.ca**) auszuwählen.

Es wird noch gefragt, ob das **Überschreiben des Zwischenschlüssels** erfolgen soll. Bitte dazu nachfolgenden Hinweis lesen.

Hinweis: Das Überschreiben des Zwischenschlüssels nur dann bestätigen, wenn ein komplett neues Zertifikat mit einem neuen Namen erstellt wird! Wird das Zertifikat nur verlängert und der alte CSR-Request weiter verwendet, darf der Zwischenschlüssel nicht überschrieben werden!

- Ist der Assistent erfolgreich durchlaufen, sind die Einstellungen noch als Administrator **config** über den Menüpunkt **Einstellungen > Sanft Anwenden** zu aktivieren.
- Kontrolle: Es ist zu kontrollieren, ob das SSL-Zertifikat richtig verwendet wurde. Dazu bitte auf die Webseite gehen und Zertifikatseigenschaften anzeigen lassen. Wurde das Zertifikat richtig verwendet und hat es die richtige Laufzeit? Wenn ja, kann das SSL-Zertifikat für die Nutzung weiterer Dienste verwendet werden.

SSL-Zertifikat für weitere Dienste verteilen

Ist das Zertifikat für den Hauptwebserver eingespielt und funktional, besteht noch die Möglichkeit, das SSL-Zertifikat auch für andere Dienste auf dem mp-Server zu nutzen. Die geschieht wie nachfolgend beschrieben:

- Als Administrator **config** den Menüpunkt **SSL-Verwaltung > Webserver-Schlüssel kopieren** aufrufen. Es wird gefragt, ob das SSL-Zertifikat des Webserver für alle anderen Dienste des mp-Servers genutzt werden soll. Wird dies mit **Ja** bestätigt, so kopiert das System die SSL-Zertifikate auf alle anderen Dienste.
- Ist der Assistent erfolgreich durchlaufen, sind die Einstellungen noch als Administrator **config** über den Menüpunkt **Einstellungen > Sanft Anwenden** zu aktivieren.
- Fertig!

From:
<https://help.m-privacy.de/> -

Permanent link:
<https://help.m-privacy.de/doku.php/faq:ca-cert>

Last update: **2024/06/19 12:22**

