

# **Hinweise zur automatischen Verlängerung von Lets Encrypt Zertifikaten**

## **Aktuelle Sicherheitsinformationen vom Let's Encrypt Team**

Update vom 03.03.2020

**Let's Encrypt hat kurzfristig darüber informiert, dass über 3 Millionen SSL-Zertifikate aufgrund einer Sicherheitslücke innerhalb von 24 Stunden ausgetauscht werden müssen, damit die Erreichbarkeit der verschlüsselten Webseiten weiterhin möglich ist.**

**Ihre Let's Encrypt Zertifikate bei uns sind nicht davon betroffen, da wir die Certbot-Methode zur Validierung nutzen, so dass die Zertifikate Ihre Gültigkeit beibehalten.**

## **Einsatzgebiete**

- Für kommerzielle Zwecke (z.B. Online Shops) empfehlen wir grundsätzlich ein inhabervalidiertes SSL-Zertifikat einer unabhängigen Registrierungsstelle. Eine Auswahl der von uns angebotenen SSL-Zertifikaten finden Sie auf unserer Webseite unter folgendem Link: <https://www.profihost.com/ssl>
- Ein Lets Encrypt Zertifikat empfehlen wir für nicht kommerzielle Webseiten, Entwicklungsumgebungen und für Domains, die als Weiterleitung auf die Hauptdomain genutzt werden.

## **Voraussetzungen für die Ausstellung**

- Lets Encrypt Zertifikate werden immer für die ausgewählte Domain (z.B.

ihredomain.de) und für den jeweiligen www-Alias (z.B. www.ihredomain.de) ausgestellt. Dies trifft auch auf Subdomains zu (z.B. shop.ihredomain.de und www.shop.ihredomain.de)

- Der A-Record für die Domain und für den www-Alias müssen bei der Erstellung des Zertifikates auf den Server bei uns zeigen. Wenn Sie Ihre Domain extern verwalten, wenden Sie sich bitte an Ihren Domainverwalter.
- Wenn der A-Record auf einen anderen Server verweist, müssen Anfragen an den Pfad `/.well-known/acme-challenge/` weitergeleitet werden
- Wenn ein AAAA-Record für die Domains existiert, muss sichergestellt werden, dass Anfragen an den Pfad `/.well-known/acme-challenge/` an unseren Server weitergeleitet werden.
- Lets Encrypt Zertifikate können nicht für Sub- oder Extradomains beantragt, oder verlängert werden, die als Weiterleitung auf eine andere Domain eingerichtet sind. Eine Beantragung und Verlängerung ist nur dann möglich, wenn die Domain auf ein Zielverzeichnis auf Ihrem Speicherplatz verweist.

## **Verlängerung eines Let's Encrypt Zertifikats**

Lets Encrypt Zertifikate sind 90 Tage gültig und werden automatisch 30 Tage vor Ablauf verlängert. Wenn bei der Verlängerung Fehler auftreten sollten, werden Sie automatisch per Mail zu folgenden Zeitpunkten informiert: 20, 15, 10, 7, 4, 2, 1 Tage vor Ablauf und am Tag an dem das Zertifikat ausläuft. Wenn die Verlängerung 20 Tage vor Ablauf nicht erfolgreich war, wenden Sie sich bitte mit einem Ticket an unseren technischen Support: Wie erstelle ich ein Ticket?

## **Sonstige Informationen**

Anleitung zur Einrichtung von Lets Encrypt Zertifikaten

Welche Typen von SSL-Zertifikaten gibt es?

SSL-Zertifikat! Wofür brauche ich das?

Wie binde ich das Logo meines SSL-Zertifikats (EV) in meine Webseite ein?