

cPanel CSR (Certificate Signing Request = Zertifikatsanforderung) erstellen

STEP 1

- Bitte klicken Sie zuerst in Ihrer cPanel Verwaltungsoberfläche unter der Spalte "Sicherheit" den Punkt "SSL/TLS" aus:



STEP 2

- Danach klicken Sie auf den Punkt "[Zertifikatsregistrierungsanforderung erzeugen, anzeigen oder löschen](#)".



STEP 3

- Im nächsten Schritt erhalten Sie die Übersicht der bereits generierten CSR Anträge (wenn schon einmal ein CSR erzeugt wurde). Darunter werden die Felder für einen neuen CSR Antrag befüllt. Als "Schlüssel" wird mit dem Drop-down Menü "Einen neuen 2.048 Bit langen Schlüssel erzeugen" ausgewählt. Unter "Domänen" kommt die Domain eingetragen, für die Ihr SSL Zertifikat gelten soll. . Wenn eine Domain oder Subdomain nicht auf Ihrem Account existiert, so erhalten Sie, wie im Beispielbild ersichtlich, recht vom Feld die Fehlermeldung. Beim Menüpunkt "Ort" ist der Ortsname einzutragen. Bei "Bundesland" ist das Bundesland Ihres Standortes anzugeben. Mit dem Drop-down Menü beim Punkt "Land" ist der Staat Ihres Standortes auszuwählen, in unserem Beispiel "AT (Österreich)". Als letztes Pflichtfeld (diese sind mit dem * gekennzeichnet) wird Ihre Firmenbezeichnung eingetragen, bei Privatpersonen ist hier nochmals der vollständige Name einzutragen. Optional kann noch der Unternehmensbereich, die Emailadresse (empfehlenswert), ein Passwort (nicht erforderlich) und die Beschreibung angegeben werden. Nachdem die Daten eingetragen sind, klicken Sie nun auf den Button "Erzeugen".

Neue Zertifikatsregistrierungsanforderung (CSR) erzeugen

Hier können Sie eine neue Zertifikatsregistrierungsanforderung (CSR) für Ihre Domäne erzeugen. Die Anforderung wird von dem System, um den Zertifikatsantrag abzuschließen. Möglicherweise müssen für die Zertifizierungsstelle spezifische Informationen Sie bei der Zertifizierungsstelle nach, welche Voraussetzungen für den Apache-Webserver erfüllt werden müssen.

Schlüssel*

Einen neuen 2.048 Bit langen Schlüssel erzeugen.

Domänen *

www.ihredomain.at

 Sie verwalten diese Domäne nicht.

Provide the FQDNs that you are trying to secure, one per line. You may use a wildcard domain by adding an asterisk in a domain name in the form: *.example.com. HINWEIS: Viele CA verlangen für Zertifikate mit mehreren Domänen (auch als „UCCS“ oder „SAN-Zertifikate“ bezeichnet) und für Zertifikate mit Platzhaltern als Domännennamen einen höheren Preis.

Ort*

Graz

Geben Sie den vollständigen Namen des Ortes oder der Gegend ein. Verwenden Sie keine Abkürzungen.

Bundesland*

Styria

Geben Sie den vollständigen Namen des Bundeslandes ein. Verwenden Sie keine Abkürzungen.

Land*

AT (Österreich)

Wählen Sie das Herkunftsland des Unternehmens für das Zertifikat aus.



Firma*

Ihre Firmenbezeichnung

Geben Sie den eingetragenen Firmennamen Ihres Unternehmens ein. Wenn der Firmenname andere Sonderzeichen als einen Punkt oder ein Komma enthält, prüfen Sie bei der Zertifizierungsstelle, ob diese zulässig sind.

Unternehmensbereich

IT Dienstleistung

Geben Sie den Namen des Unternehmensbereichs oder der Gruppe im obigen Unternehmen ein. Wenn der Name der Abteilung andere Sonderzeichen als einen Punkt oder ein Komma enthält, prüfen Sie bei der Zertifizierungsstelle, ob diese zulässig sind.

E-Mail

office@ihredomain.at

Geben Sie eine gültige E-Mail-Adresse ein, über die Sie zur Überprüfung der Eigentümerschaft für die Domäne erreichbar sind.

Passphrase

Bei manchen Zertifizierungsstellen kann es erforderlich sein, dass die Zertifikatsregistrierungsanforderung eine Passphrase enthält. Diese Passphrase wird von der Zertifizierungsstelle verwendet, um die Identität der betreffenden Person oder Organisation zu bestätigen. Die Passphrasen werden **unverschlüsselt** in der Anforderung gespeichert. Aus diesem Grund (und weil Sie diese Passphrase an Dritte weitergeben werden), sollten Sie hier kein wichtiges Kennwort verwenden.

Beschreibung

Erzeugen



Domainangabe

Wenn Sie das SSL Zertifikat für Ihre Webseite benötigen, kann entweder "ihredomain.at" oder auch "www.ihredomain.at" verwendet werden. Bei Abdeckung einer speziellen Subdomain (z.B. hilfe.ihredomain.at) muss diese exakt hinterlegt werden. Für jede Subdomain wäre ein eigener CSR notwendig (ausgenommen ist www und die Domain). Für die Abdeckung aller Subdomains (Wildcard SSL Zertifikat) wird vor der Domain einfach ein Stern vorangesetzt: *.ihredomain.at, bei SAN Zertifikaten werden die gesamten Domänen (jeweils pro Zeile eine) hinterlegt. Bei OV Zertifikaten muss unbedingt der korrekte Ort des Firmenstandortes eingetragen werden, da diese Informationen mit öffentlichen Einträgen abgeglichen werden und bei unterschiedlichen Informationen eine Verzögerung und erhöhter Supportaufwand entstehen kann.

ZIEL

- Danach erhalten Sie basierend auf Ihren Eingaben den Zertifikatsantrag (CSR). Diesen bitte notieren und an Telematica für die SSL Zertifikatsbestellung übermitteln (Den Inhalt von "Codierte Zertifikatsregistrierungsanforderung".. Der CSR wird automatisch abgespeichert (zeitgleich wird damit auch der benötigte "Private Key" erstellt, sofern noch nicht vorhanden).

The screenshot shows a web interface for generating a CSR. It includes a green success message, a 'Domäne:' field with 'at', and a 'Beschreibung:' field with 'at'. Below is a section for the 'Codierte Zertifikatsregistrierungsanforderung' containing a long base64-encoded string. At the bottom, there is a section for the decoded 'Zertifikatsregistrierungsanforderung' showing the raw CSR text.

CSR Code

```

-----BEGIN CERTIFICATE REQUEST-----
MIICoTCCAYkCAQAwXDETMdbGdfdbdfbd2V1dHNjaGFjaDESMBAGA1UECgwJT1Nj
TlMgTk1TMREwDwYDVQIdfweergtnnmtzzRMA8GALUEAwwIb3Npb3MuYXQxXzZAJ
BgNVBAYTAkFUMiIIBjJrferferferdvsdfwefegesdfsfsfew2CgKCAQEAnHq/rM
906CWa+RIE5Tbue04ut+uUiRdvx3XyZLCQaYb551+U7B1GxQ2rSUSCq/v6+81qsU
isQmTlExVQgCEuOCVl1xnWhCwXwRp2efhuVLvDsZPd8hhdCwF1YAJaJ6C15VDNjy
vuErEU7TqymsadasdasdasdfvegetrterY5F8d1GXPqWs5Bbt08ftzZob0KxOew
YlJHZydcjJlJE4SMIF7h/rgtgfgngnferesfgrtnrngdfgeerdRLgCRB6Lhzc
NKT2m7mEXomYkIhpQuqXAQ09HI8cJpHpYcg3Q1+fz05LWYw1BhDmfv1bzSJXe8DW
dTNwz+zaQerervfgsdrgrthrtddcvdfIhvcNAQELBQADggEBAJRvpWenj3a8nxv3
IOlt1HRGPnKnfs6031tPzwdfgddfggrerg8WcWuSJAL1NjFBd16GyMjAG0zd+MUZAM
zM9G6fF/jReMDyOfTzmiAgdQRZbzRpoQAL26HSC+ln9IGmZUxMPsnQ/MGUDqR9u
KoPONTewfwfwevrev234th5gbaFh5k5tghgFSbZzIOyE1ewV5tyVEvEYH5qv/E3
zeZ98QewM7dXlMwffz3kzW9nb+Ljlb1XJx+JyNrj41ZSNQzK75pHW3ZFhg8ps3H
NxPjd/XIL4reteht43z6il,jn54z6edd5kj45dckAVTCucr4ikeg7iCx0qaayjz/
bBSCYgw=
-----END CERTIFICATE REQUEST-----

```

ZUSATZ

- Sollten Sie ein SSL Zertifikat verlängern wollen, für den bereits ein CSR erstellt worden ist, können Sie (sofern die Daten gleichbleibend sind) denselben CSR Code für die entsprechende Domain an uns übermitteln. Diesen finden Sie, wie Anfangs erwähnt, in der Übersicht, in dem Sie bei Ihrer Domain auf "bearbeiten" klicken.

- Mit der Übermittlung des "CSR" an Telematica haben Sie den ersten Schritt zu Ihrem SSL Zertifikat abgeschlossen. Als zusätzliche Information benötigen wir noch, auf welchem Wege Sie Ihre Domain verifizieren möchten. Die einzelnen Methoden werden in den nachstehenden Links erläutert.



Unbedingt notwendig

Es ist unbedingt erforderlich, dass für die Überprüfung eine Emailadresse (oder eine Aliasadresse als Weiterleitung) mit den folgenden Namen vor dem @ Zeichen angelegt werden: admin@ , administrator@, webmaster@, postmaster@ oder hostmaster@