Domains & SSL

How do I create a (trusted) SSL certificate?

To offer HTTPS pages on your server you need an SSL certificate.

Since this certificate is usually bound to a separate IP address and a (sub)domain name, you need a separate IP address for each (sub)domain to be secured. The basis for creating a certificate is a Certificate Signing Request (CSR). You must create this on your server. Confixx from version 3.1.2 and Plesk offer their own functions for creating the request. However, you can also create the request manually:

To create a key pair consisting of a private key and a public certification request (CSR), enter the following command: (Linux systems)

openssl req -new -nodes -newkey rsa:2048 -keyout filename.key -out filename.csr

It is advisable to select the file name in such a way that you can assign it uniquely to the page later. We therefore recommend the use of the domain to be certified by replacing the dots with underscores as file names, for example www_example_net.key or www_example_net.csr.

The command creates two files. The file with the extension key contains the private key, so do not pass this file on to third parties. Please make a backup of your private key in any case, as there is no possibility of recovery after a loss. The private key serves as the basis for the certificate request (CSR) and is therefore also the basis for the certificate.

When creating the CSR, you will be asked for some details that will be included next to the public key in the CSR and make it unique. Some fields have a default value, to accept it simply press Enter, if you want to leave the field blank enter a dot (.).

Country Name (2 letter code) : DE
enter your country code here

State or Province Name (full name) Hesse
enter your state here

Locality Name (eg, city) <>: Fulda
enter your location here

Organization Name (eg, company) MyCompany
here you enter your company name / organisation name / first and last name, whichever is most appropriate for you

Organizational Unit Name (eg, section) <>: IT
here you can enter a department, but this field can also remain empty

Common Name (eg, YOUR name) <>: www.domain.de
here you enter the site to be secured, the information must contain a complete domain name, so if you want to use https://www.domain.de/... protect, enter www.domain.de, domain.de is not sufficient here, this only protects https://domain.de/. Files and subdirectories, on the other hand, are always included.

E-mail Address <>: info@domain.de
enter your e-mail address here. If necessary you will be asked for the following 'extra' information

A challenge password <>:

An optional company name <>:
please always leave this empty.

Domains & SSL

Your CSR will now be created. Then open the file filename.csr in a text editor and copy the content into a ticket with the request for a certificate.

We will sign the request as soon as possible and send you the finished certificate.

Please note that the e-mail address admin@<Domainname> must be available to check the accessibility of the domain name. <domain name> corresponds to the domain for which you have ordered the certificate. At this address you will first receive an e-mail in which you have to confirm the order of the certificate and then the created certificate will be sent to this address.

Please also make sure that the public key of your certificate has a key length of at least 2048 bit, otherwise we cannot sign the request.

Unique solution ID: #1455
Author: Bettina Brauer
Last update: 2021-04-01 08:13