MANUAL:

How to check if an SSL is properly installed (e.g. with the SSL Checker) and where to get from the Web the CA and SubCA if you have to install them on the Server.

Contents

INTRODUCCIÓN

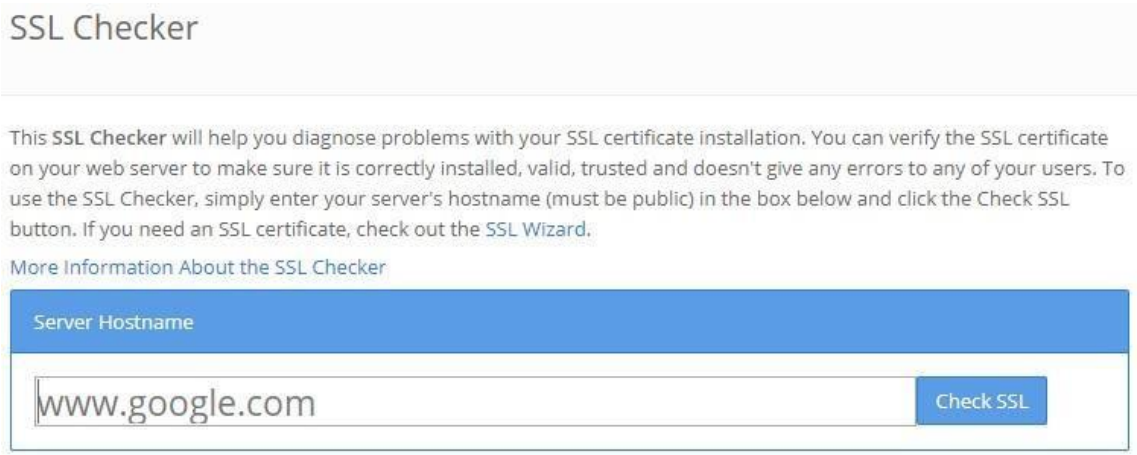
This manual will explain how to check if an SSL certificate is properly installed using the SSL Checker tool.

It will also indicate where to obtain the CA and SubCA from within our website in case it is necessary to install them on the server.

CHECKING A WELL INSTALLED SSL

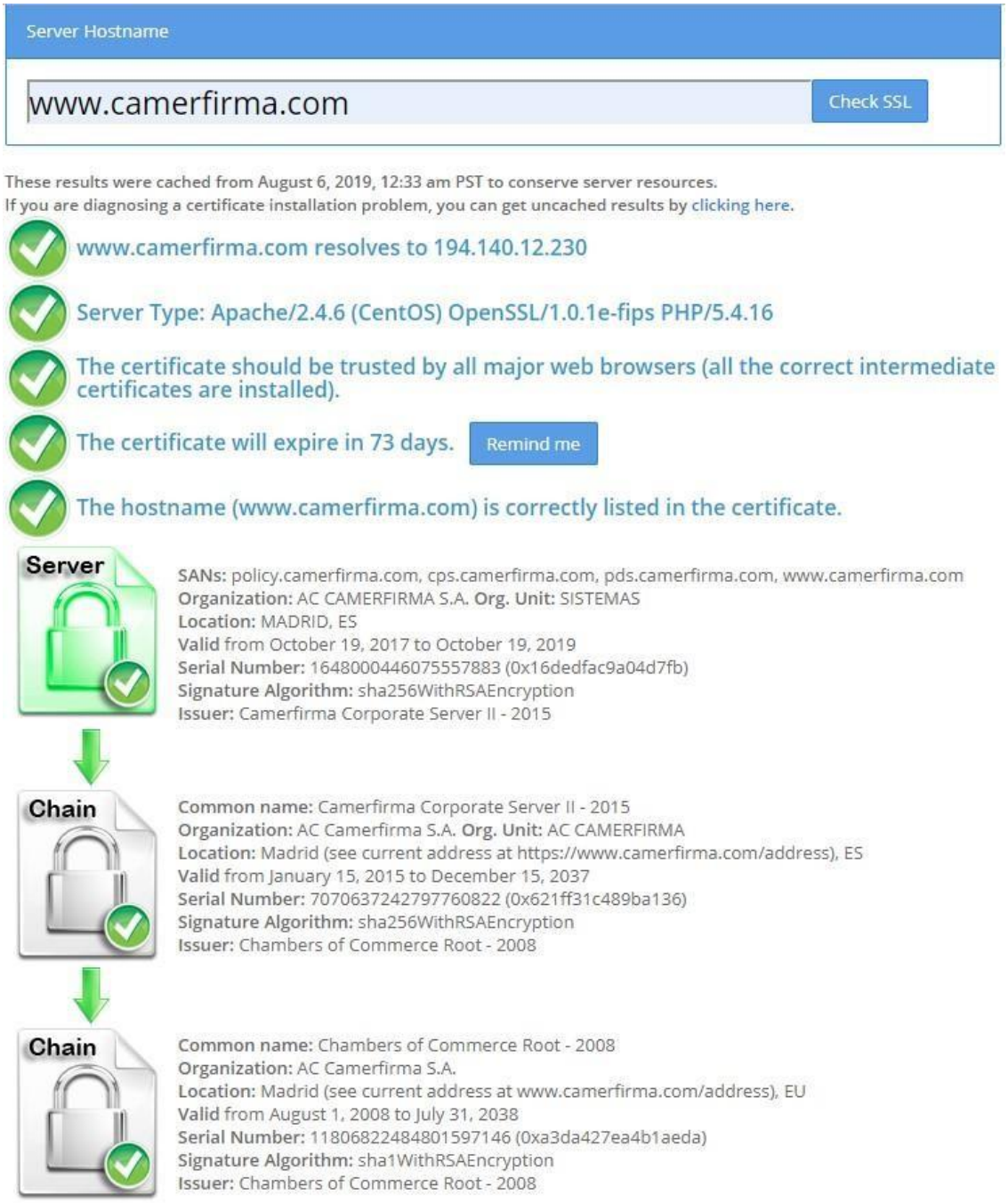
To check that an SSL is properly installed, simply go to the following web page:

https://www.sslshopper.com/ssl-checker.html



In the box we have to put the domain we want to check. 2 situations may occur :

1. The domain is correct than you will see something displayed like below :


Server Hostname
www.camerfirma.com
Check SSL
These results were cached from August 6, 2019, 12:33 am PST to conserve server resources.
If you are diagnosing a certificate installation problem, you can get uncached results by clicking here.
www.camerfirma.com resolves to 194.140.12.230
Server Type: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16
The certificate should be trusted by all major web browsers (all the correct intermediate certificates are installed).
The certificate will expire in 73 days.
Remind me
The hostname (www.camerfirma.com) is correctly listed in the certificate.
Server
SANs: policy.camerfirma.com, cps.camerfirma.com, pds.camerfirma.com, www.camerfirma.com
Organization: AC CAMERFIRMA S.A. Org. Unit: SISTEMAS
Location: MADRID, ES
Valid from October 19, 2017 to October 19, 2019
Serial Number: 1648000446075557883 (0x16dedfac9a04d7fb)
Signature Algorithm: sha256WithRSAEncryption
Issuer: Camerfirma Corporate Server II - 2015
Chain
Common name: Camerfirma Corporate Server II - 2015
Organization: AC Camerfirma S.A. Org. Unit: AC CAMERFIRMA
Location: Madrid (see current address at https://www.camerfirma.com/address), ES
Valid from January 15, 2015 to December 15, 2037
Serial Number: 7070637242797760822 (0x621ff31c489ba136)
Signature Algorithm: sha256WithRSAEncryption
Issuer: Chambers of Commerce Root - 2008
Chain
Common name: Chambers of Commerce Root - 2008
Organization: AC Camerfirma S.A.
Location: Madrid (see current address at www.camerfirma.com/address), EU
Valid from August 1, 2008 to July 31, 2038
Serial Number: 11806822484801597146 (0xa3da427ea4b1aeda)
Signature Algorithm: sha1WithRSAEncryption
Issuer: Chambers of Commerce Root - 2008

2. The domain is not correct or is not registered, than you will see something displayed like below:

WHERE TO GET FROM THE WEB THE CA AND THE SUBCA

The root CA and SubCA certificates can be found on our website where shown below. Installing the root certificates resolves, for example in this type of certificate, the warning that the certificate cannot be verified because the issuer is unknown.

1. Root certificate in format .cer: En https://www.camerfirma.com/politicas-de-certificacion-ac-camerfirma/ download and install the *CHAMBERS OF COMMERCE ROOT - 2008.cer*.
2. SubCA certificate in format .cer: En https://www.camerfirma.com/politicasde-certificacion-ac-camerfirma/ download and install the *Corporate Server II – 2015.cer*.

To convert the above certificates to .pem, the following process must be followed:

1. Open public key, from Internet options or from Status.
2. Go to details
3. Click on “copy file”

4. Select "X.509 coded base 64 (.cer)" and click next.
5. Click on "Browse" and save the file where you want.
6. Click next.
7. Click on finish.
8. Go to the created file and change the .cer extension to .pem.
9. Accept the warning message.