



MANUAL:

ORDERING AND INSTALLING A SECURE SERVER
CERTIFICATE IN APACHE 2.X USING OPENSSE EX-
2009-10-10

Tabla de contenido

OBJECTIVES	3
REQUEST	3
SUPPORTING DOCUMENTS	7
SSL DOMAIN CONTROL	7
CERTIFICATE ISSUANCE.....	8
INSTALLATION.....	9
CHECKING A WELL INSTALLED SSL	10
WHERE TO GET FROM THE WEB THE CA AND THE SUBCA.....	¡Error! Marcador no definido.

OBJETIVES

The purpose of this document is to inform AC Camerfirma customers, who are going to request a secure server certificate, of the technical requirements to make the request and the subsequent installation of the certificate obtained in Apache 2.

REQUEST

The user will enter the SSL certificate request data in the request form.

The user will need to have a CSR and enter it in the form data and must have the private key for installation.

The openssl tool must be installed on the server.

*To generate the private key you must run:

openssl genrsa -des3 -out miservidor.key 2048

2048 is the key length. You must specify a key length of at least 2048 bits. This command will generate the file miservidor.key, which contains your private key and which you must keep safe.

Carefully protect this private key by backing it up and storing it in a safe place.

* To generate the server certificate request (CSR) you must run:

openssl req -new -key miservidor.key -out solicitud.csr

You will now be prompted to generate the CSR. Some fields may have a predefined value, if you enter '.' the field will be left blank (if you press enter, the predefined value will be passed).

Country Name (2 letter code) []

State or Province Name []

Locality Name []

Organization Name []

Organizational Unit Name []

Common Name* []

Email Address []

A challenge password []

An optional company name []

Common Name (CN): Domain name for which the certificate is to be requested.
(example: www.camerfirma.com)

Your CSR will be generated in the application file .csr.

Ejemplo de CSR:

-----BEGIN NEW CERTIFICATE REQUEST-----

```
MIIDYDCCAskCAQAwgYQxHjAcBgNVBAMTFWFWYWN0ZS5jYW1lcmZpcm1h LmNvbTER
MA8GA1UECxMIU2lzdGVtYXMxGzAZBgNVBAoTEkFDIENhbWVyZmlybWEgU y5BLjEO
MAwGA1UEBxMFQXZpbGExFTATBgNVBAgeDABFAHMAcABhAPEAYTELMA
kGA1UEBhMC
RVMwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMqoOFQDRPQdccVu
nNjr7dCS
e4YmW7NuA0Ss9i3RyzQkh4vf5MOxWSzF89pTSTqIWzfHZFDm330wsI36Wi7G6Jn S
38LUE89Hlf87rYakp2NFi3oyRVCZ+cXk5SKl1YLURpWfpmU479yufDL1zRQoajKV
GYflwaPRDehyFz05h8+lAgMBAAAGggGZMBoGCisGAQQBgjcNAgMxDBYKNS4wLjlx
OTUuMjB7BgorBgEEAYI3AgEOMW0wazAOBgNVHQ8BAf8EBAMCBPAwRAYJ
KoZIhvcN AQkPBDCwNTAOBggqhkiG9w0DAGlCAIAwDgYIKoZIhvcNAwQCAgCAMAcGBS
sOAwIH MAoGCCqGS1b3DQMhMBMGA1UdJQQMMAoGCCsGAQUFBwMBMIH9BgorBg
EEAYI3DQIC
MYHuMIHrAgEBHloATQBpAGMAcgbvAHMAbwBmAHQAIABSAFMAQQAgAF
MAQwBoAGEA
bgBuAGUAbAAgAEMAcb5AHAAdABvAGcAcgBhAHAAaABpAGMAIABQAH
AbwB2AGkA
ZABIAHIDgYkAJ1L9qpiQmoL5dNIVLkM2P6UFcMYME1cUMidPEUHEGfxOB1eT GXu8
rhguJfDScUi9h1SOKHO8CnjCQFoYPhb/iRhaCbbu1UsNfoJG1imCP07Lr8k8gOW
76zuvn+zfU5AbSQjJf/SbXyLZO9TDbe4Y2aklRo2aeZBVm2GXz3ezjYAAAAAAAAA
ADANBgkqhkiG9w0BAQUFAAOBgQCORCkQNRHGVwiTB+EsK+5xuP1AOhdmUFLwZGxZ
PjmkCXTJw3zJ2ifVbwXKB6eg2mCoRt1PZavhcFDOFTP+gxV6kJH83Hu6n6Sq+kO2
9psfFUSKrlV7Xhv/Vsh7pnJqNeytQSID3DSgyWiMcCKQf7RUG8GBtyVWRpxHc3M T
rpPxyQ==
```

-----END NEW CERTIFICATE REQUEST-----

This is the CSR that must be copied (including the headers -----BEGIN NEW CERTIFICATE REQUEST----- and -----END NEW CERTIFICATE REQUEST) in the AC Camerfirma secure server certificate request form.

Once the user has entered the certificate application data in the form and clicked on send, CAMERFIRMA will send an e-mail to the e-mail address provided by the certificate applicant to accept the conditions of use of the certificate.

SUPPORTING DOCUMENTS

1. AUTHORISATION DOCUMENT FOR THE APPLICANT

This document, provided by the Operations department, is necessary for the company to which the certificate is issued to designate the certificate applicant. The document must be signed by a person with power of representation of the company and the representative's powers of attorney must be provided.

2. COPY OF THE AUTHORISING PERSON'S IDENTITY CARD

This document is required to validate the Authorisation.

3. COPY OF THE APPLICANT'S IDENTITY CARD

This document is required to validate the Authorisation.

In the case of EV certificates, it would be necessary to verify the Applicant in person, either at the Chamber of Commerce or through a Camerfirma Registry Operator.

SSL DOMAIN CONTROL

Due to the entry into force of the new RGPD, (General Data Protection Regulation) when consulting the domain registration, neither the registering ORGANISATION, nor the technical or administrative contact appears in order to send an email and validate control of the domain.

AC Camerfirma offers different options to validate the Applicant's control of the domain:

1. We would have the option of confirming the validation by any of these addresses proposed by the regulations admin, administrator, webmaster, hostmaster, postmaster (@dominioasecurizar). If they inform us of one or two associated addresses, we could send the confirmation code to them and once confirmed we could proceed with the validation.
2. DNS entry. In order for Camerfirma to have evidence of domain control, a code could be sent and the Applicant, as the domain manager, publishes it in their area to confirm that they are the domain owners.

In order to carry out this validation, the Applicant must indicate to Operations (operaciones@camerfirma.com) which option he/she wishes to carry out the validation.

Option 1 : a message will be sent to the email address provided by the Applicant (admin, administrator, webmaster, hostmaster, postmaster) to accept control of the domain.

Option 2 : a code will be sent to the Applicant's email address for them to enter in their DNS to verify control of the domain.

Until these checks have been completed, the certificate cannot be issued.

CERTIFICATE ISSUANCE

Once the supporting documentation has been validated and control of the domain has been verified, the certificate is issued. A link to download the certificate's public key is sent to the certificate applicant's e-mail address.

Finally, CAMERFIRMA sends the revocation PIN to the certificate Applicant's e-mail address.

INSTALLATION

First, you must verify that the httpd.conf section of the general configuration file is enabled:

```
# Secure (SSL/TLS) connections
Include conf/extra/httpd-ssl.conf
```

The httpd-ssl.conf file contains the data relating to secure connections. The following lines should be included in this file.

The certificate issued by AC Camerfirma for your server:

```
SSLCertificateFile conf/ssl.crt/03de.crt
```

Your private key

```
SSLCertificateKeyFile conf/ssl.key/miservidor.key
```

And finally the line referring to a file with our two CAs (the Root and the subordinate) concatenated.

```
SSLCACertificateFile conf/ssl.crt/certificadosCAs.pem
```


To compose this file, you can copy the certificate of our Root CA (Chambers Of Commerce Root) and that of the subordinate CA (CA Camerfirma Express Corporate Server) one after the other.

The links to these certificates can be found in the email in which AC Camerfirma sends you your certificate.

Download them in PEM format (base 64).

Save your modifications to the httpd.conf and httpd-ssl.conf files and restart your Apache server.

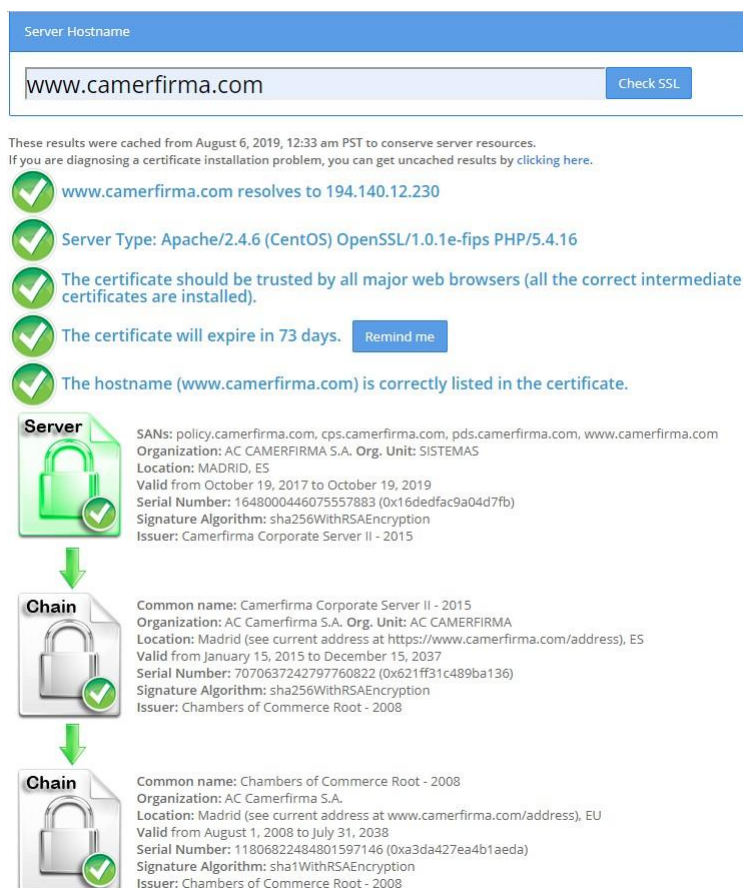
CHECKING A WELL INSTALLED SSL

Once the SSL certificate is installed, we need to check if it is working properly by using various testers.

SSL Checker: <https://www.sslshopper.com/ssl-checker.html>, insert the URL associated at the certificate and click on Check SSL

You can encounter 2 cases :

1. If correctly installed, it should show the complete sequence, as shown in the picture:




Server Hostname


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.
- ✓ 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 has not been registered.



In this case it shows that the chain is broken and it is because the trust chain has not been correctly installed. This could be installed directly from the Camerfirma website: <https://www.camerfirma.com/servicios/respondedor-ocsp/>

Access <http://www.camerfirma.com> to Cloud Services - OCSP Responder. Download and execute the 2008 Chambers of Commerce Root - 2008 and Camerfirma Corporate Server II - 2015 keys, as indicated below, to solve the lack of trust.

Respondedores OCSP – Claves 2008					
CA	Cert. CA	Tipo Certificados	Cert. Resp. OCSP	Valido desde	Valido hasta
Chambers of Commerce Root – 2008		SubCAs		2019-07-29	2020-07-28
AC Camerfirma AAPP II – 2014		Administraciones Públicas		2019-07-30	2020-07-29
Camerfirma Corporate Server – 2009 CA Caducada (No se renueva certificado)		Certificados SSL y Sellos de empresa		2018-08-10	2019-03-15
Camerfirma Corporate Server II – 2015		Certificados SSL y Sellos de empresa		2019-07-30	2020-07-29

NOTE: If the certificate to be installed is a SEDE certificate, and there is an error when checking the installation, in addition to the CA Chambers of Commerce Root - 2008, the SubCA AC Camerfirma AAPP II - 2014 should also be installed.

Respondedores OCSP – Claves 2008					
CA	Cert. CA	Tipo Certificados	Cert. Resp. OCSP	Valido desde	Valido hasta
Chambers of Commerce Root – 2008		SubCAs		2019-07-29	2020-07-28
AC Camerfirma AAPP II – 2014		Administraciones Públicas		2019-07-30	2020-07-29

If necessary, we provide instructions how to convert the certificates into .pem format:

1. Open public key, from Internet options or under Status.
2. Go to the details tab.
3. Click on "copy file".
4. Select "X.509 base 64 encoded (.cer)" and click next.
5. Click on "Browse" and save the file.
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.