MANUAL:

SOLICITUD E INSTALACIÓN DE UN CERTIFICADO DE SERVIDOR SEGURO EN APACHE 2.X MEDIANTE OPENSSL EX-2009-10-10

Tabla de contenido

OBJETIVOS

El objetivo de este documento es informar a los clientes de AC Camerfirma, que vayan a solicitar un certificado de servidor seguro, de los requisitos técnicos para realizar dicha solicitud y la posterior instalación del certificado obtenido en servidor de páginas Apache 2.X.

SOLICITUD

El usuario introducirá los datos de solicitud del certificado SSL en el formulario de solicitud.

Para ello tendrá que disponer de un CSR e introducirlo en los datos del formulario y debe disponer de la clave privada para su instalación.

Es necesario tener instalada en el servidor la herramienta **openssl**

*Para generar la clave privada debe ejecutar:

openssl genrsa -des3 -out miservidor.key 2048

Donde 2048 es la longitud de la clave. Debe especificar una longitud de clave de al menos 2048 bits. Este comando generará el fichero **miservidor.key**, que contiene su clave privada y que debe custodiar convenientemente.

Proteja cuidadosamente esta clave privada haciendo una copia de seguridad y guardándola en un lugar seguro.

*Para generar la solicitud de certificado de servidor (CSR) debe ejecutar:

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

Ahora se le solicitarán datos para generar el CSR. Puede que en algunos campos exista un valor predefinido, si introduce '.' el campo se dejará en blanco (si pulsa enter, se pasará el valor predefinido)

Country Name (2 letter code) [ ]: (Código del país - 2 letras)

State or Province Name [ ]: (Provincia)

Locality Name [ ]: (Ciudad)

Organization Name [ ]: (Organización)

Organizational Unit Name [ ]: (Departamento)

Common Name* [ ]: (dominio o subdominio para el certificado)

Email Address [ ]: (dirección de e-mail)

Después le pedirá los siguientes datos extras que se enviarán con su petición del certificado.

A challenge password [ ]: (Contraseña)

An optional company name [ ]: (Nombre altenativo de la compañia)

Common Name (CN). Nombre de dominio para el que se va a solicitar el certificado.

(ejemplo: www.camerfirma.com)

Su CSR se generará en el fichero solicitud.csr.

Ejemplo de CSR:

-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDYDCCAskCAQAwgYQxHjAcBgNVBAMTFWFwYWNoZS5jYW1lcmZpcm1h
LmNvbTER
MA8GA1UECxMIU2lzdGVtYXMxGzAZBgNVBAoTEkFDIENhbWVyZmlybWEgU
y5BLjEO
MAwGA1UEBxMFQXZpbGExFTATBgNVBAgeDABFAHMAcABhAPEAYTELMA
kGA1UEBhMC
RVMwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMqoOFQDRPQdccVu
nNJr7dCS
e4YmW7NuA0Ss9i3RyzQkh4vf5MOxWSzF89pTSTqIWzfHZFDm330wsI36Wi7G6Jn
S
38LUE89HIf87rYakp2NFi3oyRVCZ+cXk5SKl1YLUrpWfpmU479yufDL1zRQoajKV
GYflwaPRDehyFz05h8+lAgMBAAGgggGZMBoGCisGAQQBgjcNAgMxDBYKNS4
wLjIx
OTUuMjB7BgorBgEEAYI3AgEOMW0wazAOBgNVHQ8BAf8EBAMCBPAwRAYJ
KoZIhvcN
AQkPBDcwNTAOBggqhkiG9w0DAgICAIAwDgYIKoZIhvcNAwQCAgCAMAcGBS
sOAwIH
MAoGCCqGSIb3DQMHMBMGA1UdJQQMMAoGCCsGAQUFBwMBMIH9BgorBg
EEAYI3DQIC
MYHuMIHrAgEBHloATQBpAGMAcgBvAHMAbwBmAHQAIABSAFMAQQAgAF
MAQwBoAGEA
bgBuAGUAbAAgAEMAcgB5AHAAdABvAGcAcgBhAHAAaABpAGMAIABQAHI
AbwB2AGkA
ZABlAHIDgYkAJ1L9qpiQmoL5dNlVLkM2P6UFcMYME1cUMidPEUHEGfxOB1eT
GXu8
rhguJfDScUiy9h1SOkHO8CnjCQFoYPhb/iRhaCbbu1UsNfoJG1imCP07Lr8k8gOW
76zuvn+zfU5AbSQjJf/SbXyLZO9TDbe4Y2aklRo2aeZBVm2GXz3ezjYAAAAAAAA
A
ADANBgkqhkiG9w0BAQUFAAOBgQCORcKQNRHGVwiTB+EsK+5xuP1AOhdmU
FLwZGxZ
PjmkCXTJw3zJ2ifVbwxKB6eg2mCoRt1PZavhcFDOFTP+gxV6kJH83Hu6n6Sq+kO2
9psfFUSKrIV7Xhv/Vsh7pnJqNeytQSID3DSgyWiMcCKQf7RUG8GBtyVWRpxHc3M
T rpPxyQ==
-----END NEW CERTIFICATE REQUEST-----

Este es el CSR que debe copiar (incluidas las cabeceras -----BEGIN NEW CERTIFICATE REQUEST----- y -----END NEW CERTIFICATE REQUEST-----) en el formulario de solicitud del certificado de servidor seguro de AC Camerfirma.

Una vez el usuario ha introducido los datos de solicitud del certificado en el formulario y ha pulsado enviar, CAMERFIRMA enviará un correo electrónico al E-mail facilitado por el Solicitante del certificado para Aceptar las condiciones de uso del certificado.

DOCUMENTACIÓN DE RESPALDO

1. DOCUMENTO DE AUTORIZACIÓN PARA EL SOLICITANTE

Este documento facilitado por el departamento de Operaciones, es necesario para que la Empresa a la que se le emite el certificado designe a la persona solicitante del certificado. El documento tendrá que ir firmado por una persona con poder de Representación de la empresa y tendrá que aportar los poderes del Representante.

2. COPIA DEL DNI DEL AUTORIZANTE

Este documento es necesario para validar la Autorización.

3. COPIA DEL DNI DEL SOLICITANTE

Este documento es necesario para validar la Autorización.

En caso de certificados EV sería necesaria la Verificación presencial del Solicitante bien sea en la Cámara de Comercio o por medio de un Operador de Registro de Camerfirma.

CONTROL DEL DOMINIO DEL SSL

Debido a la entrada en vigor del nuevo RGPD, (Reglamento General de Protección de datos) al consultar el registro del dominio no aparecen la ORGANIZACIÓN registrante, ni el contacto técnico ni el administrativo para poder enviar un correo electrónico y validar el control del dominio.

Desde AC Camerfirma, ofrecemos distintas opciones sobre las que podríamos validar el control del dominio por parte del Solicitante:

1. Tendríamos la opción de que confirmen la validación por cualquiera de estas direcciones que propone el reglamento admin, administrator, webmaster, hostmaster, postmaster (@dominioasecurizar). Si nos informan de una o dos direcciones asociadas, podríamos enviar el código de confirmación a las mismas y una vez confirmada podríamos proceder con la validación.

2. Entrada en el DNS. Para que Camerfirma pueda tener evidencia del control del dominio se podría enviar un código y el Solicitante como gestor del dominio publica en su zona para confirmar que son los propietarios del dominio.

Para llevar a cabo esta validación es necesario que el Solicitante indique a Operaciones (operaciones@camerfirma.com) que opción quiere llevar a cabo para poder efectuar la validación.

En el caso de la Opción 1, se le enviará al correo electrónico facilitado por el Solicitante (admin, administrator, webmaster, hostmaster, postmaster) un mensaje para que acepte el control del dominio.

En el caso de la Opción 2, se le enviará al correo electrónico del Solicitante un código para que lo introduzca en su DNS para verificar el control del mismo.

Hasta que no se realicen estas comprobaciones no se podrá emitir el certificado.

EMISIÓN DEL CERTIFICADO

Una vez se haya validado la documentación de respaldo y se haya verificado el control del dominio, se procede a la emisión del certificado. Con ello se envía al correo

electrónico del Solicitante del certificado un enlace para proceder a la descarga de la clave pública del certificado, se facilita en

Finalmente, CAMERFIRMA envía al correo electrónico del Solicitante del certificado el PIN de revocación.

INSTALACIÓN

En primer lugar, debe verificar que en el fichero general de configuración httpd.conf se encuentra activada la sección:

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

En el fichero httpd-ssl.conf se encuentran los datos relativos a las conexiones seguras. En dicho fichero deben figurar las siguientes líneas.

El certificado que le ha entregado AC Camerfirma emitido para su servidor:

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

Su clave privada

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

Y por último la línea en la que se hace referencia a un fichero con nuestras dos CAs (la Root y la subordinada) concatenadas.

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

Para componer dicho fichero puede copiar uno tras otro el certificado de nuestra CA Root (Chambers Of Comerse Root) y el de la subordinada (CA Camerfirma Express Corporate Server).

Los enlaces a estos certificados se encuentran en el correo electrónico en el que AC Camerfirma le envía su certificado.

Descárguelos en formato PEM (base 64).

Guarde las modificaciones efectuadas en los archivos httpd.conf y httpd-ssl.conf y reinicie su servidor Apache.

COMPROBACIÓN DE UN SSL BIEN INSTALADO

Una vez instalado el certificado de SSL, debemos comprobar si está correctamente instalado, para ello podemos hacer uso de varios comprobadores.

Por ejemplo, si cogemos el Ssl Checker: https://www.sslshopper.com/ssl-checker.html, ponemos la url asociada al certificado y damos a Check SSL

Tras esto, pueden aparecer 2 situaciones:

1. Si está correctamente instalado tiene que mostrar la cadena completa, como aparece en la imagen:

2. Que el dominio no sea correcto o no esté dado de alta, por lo que se mostrará algo como lo siguiente:

En este caso se muestra que la cadena está rota y es porque falta por instalar correctamente la cadena de confianza. Esta se podría instalar directamente desde la web de Camerfirma: https://www.camerfirma.com/servicios/respondedor-ocsp/

Habría que acceder a www.camerfirma.com à Servicios Cloud à Respondedor OCSP y descargar y ejecutar de las claves 2008 Chambers of Commerce Root – 2008 y Camerfirma Corporate Server II – 2015, como se indica a continuación, para solucionar la falta de confianza.

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

NOTA: En el caso de que el certificado a instalar sea un certificado de Sede, y de error al comprobar la instalación, además de la CA Chambers of Commerce Root – 2008, habría que instalarse también la SubCA AC Camerfirma AAPP II – 2014

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

Por si fuera necesario, le damos las instrucciones para convertir los certificados en formato .pem:

1. Abrir clave pública, desde opciones de Internet o en Status.

2. Ir a la pestaña detalles.
3. Hacer clic en “copiar archivo”.
4. Seleccionar "X.509 codificado base 64 (.cer)" y hacer clic en siguiente.
5. Hacer clic en “Examinar” y guardar el archivo donde se quiera.
6. Hacer clic en siguiente.
7. Hacer clic en finalizar.
8. Ir al archivo creado y cambiar la extensión .cer por .pem.
9. Aceptar el mensaje de advertencia.