



**SOLICITUD E INSTALACIÓN DE UN CERTIFICADO DE SERVIDOR
SEGURO EN WINDOWS 2008 SERVER CON IIS 7.0 EX-2008-10-02**

1. Índice

Índice	2
Objetivo del documento	3
Solicitud	3
Instalación	8
Configuración básica.....	11
Comprobación de la correcta instalación	13

2. Objetivo del documento.-

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 un sistema con Windows 2008 Server con IIS

3. Solicitud.-

El primer paso es acceder a la administración de Internet Information Server: pulse sobre el botón de inicio, seleccione Herramientas Administrativas y después Internet Information Services Manager. Cuando se abra la ventana correspondiente, haga clic en el nombre de su servidor. En el menú central, haga clic sobre el icono de Certificados de Servidor (dentro del grupo de Seguridad, al final de la lista):

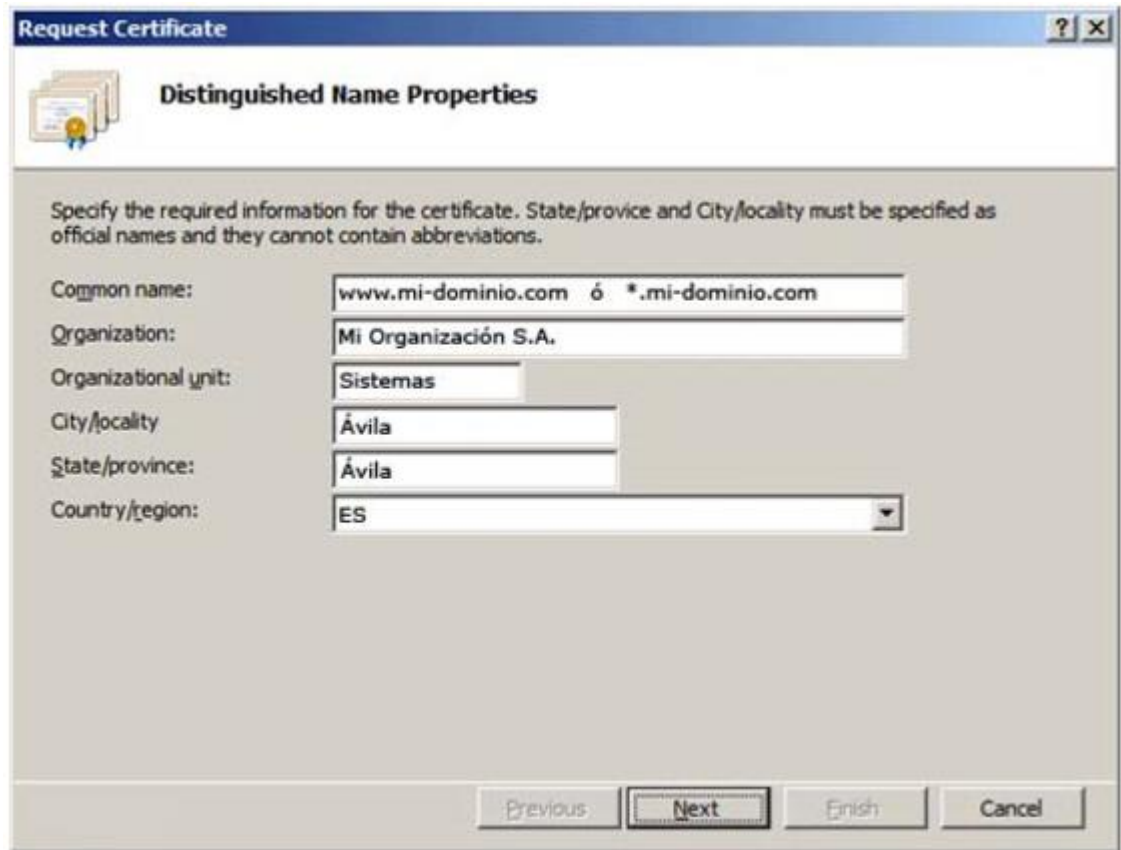


Posteriormente, en la parte derecha de la pantalla (Acciones) seleccione la opción “Crear solicitud de certificado”, tras lo que se ejecutará el asistente de solicitud de certificado.



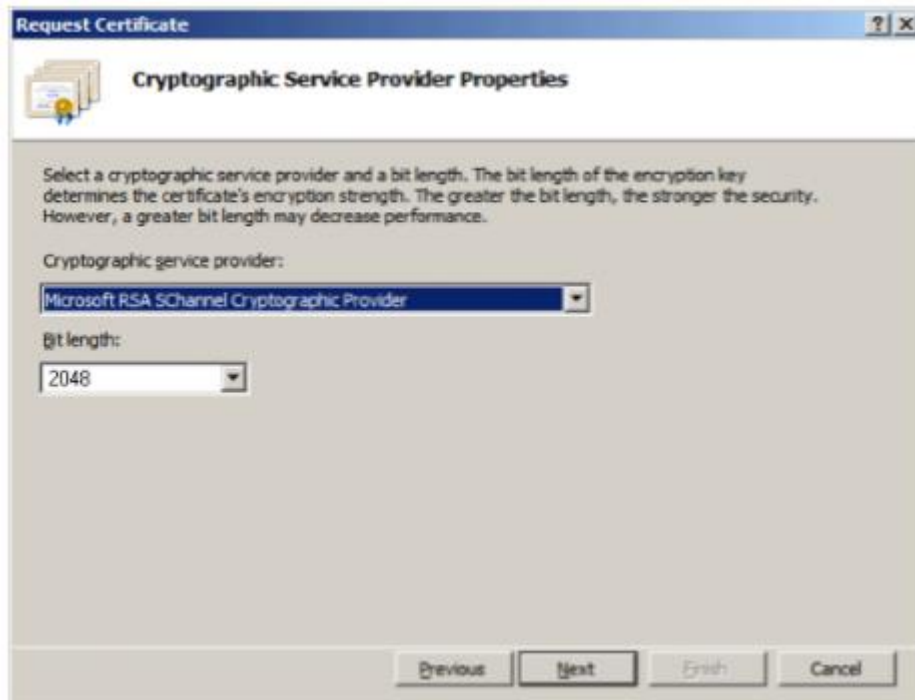
En las “Propiedades del Nombre Distintivo” es necesario completar los siguientes campos:

- Common name: el nombre del dominio para el que vayamos a solicitar el certificado de servidor seguro. Por ejemplo: www.mi-dominio.com o facturación.mi-dominio.com. Si va a necesitar más de un subdominio quizá deba valorar de solicitar un certificado multidominio, por ejemplo: *.mi-dominio.com
- Organización: El nombre de su empresa u organización
- Unidad organizacional: Su departamento
- Ciudad, Provincia y País.

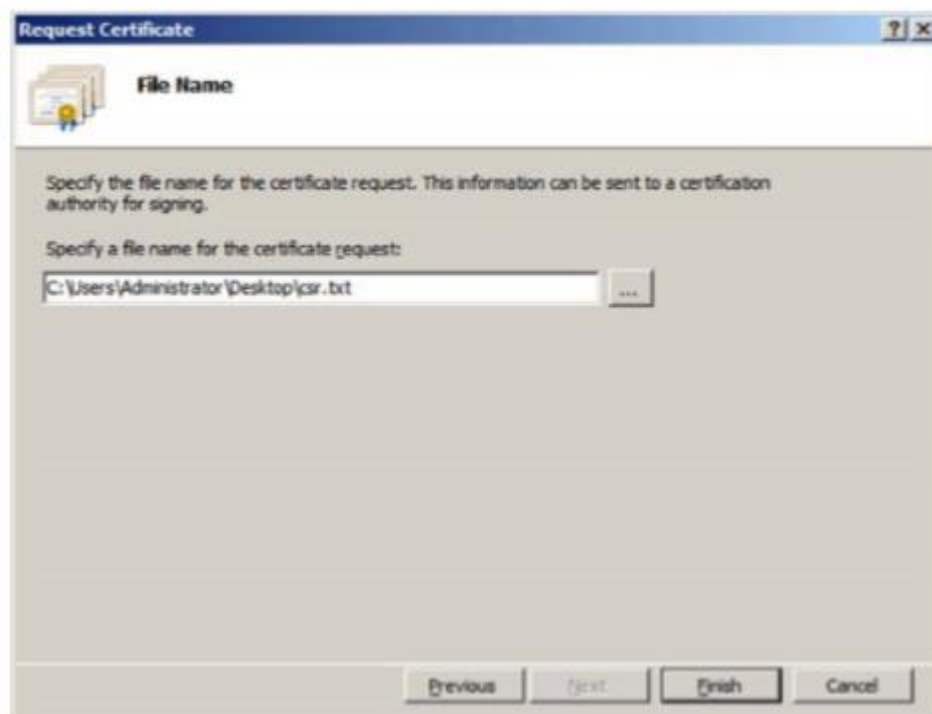


The image shows a Windows dialog box titled "Request Certificate" with a sub-header "Distinguished Name Properties". It contains a text box with the instruction: "Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations." Below this are several input fields: "Common name:" with the text "www.mi-dominio.com ó *.mi-dominio.com"; "Organization:" with "Mi Organización S.A."; "Organizational unit:" with "Sistemas"; "City/locality" with "Ávila"; "State/province:" with "Ávila"; and "Country/region:" with a dropdown menu showing "ES". At the bottom, there are four buttons: "Previous", "Next", "Finish", and "Cancel".

En el apartado de Proveedor de Servicios Criptográficos deje los campos que aparecen por defecto. Debe seleccionar una longitud de clave mayor o igual a 2048 bits.



En la siguiente pantalla especifique la ubicación donde se va a almacenar la solicitud.



Una vez completado el asistente editamos el fichero de la petición, y copiamos el contenido al campo del formulario de petición de certificado de servidor (www.camerfirma.com) llamado CSR (Certificate Signing Request) y junto con los demás datos, enviamos la solicitud.

La petición tendrá este formato. Debemos “pegarla” (con las cabeceras) en el formulario.

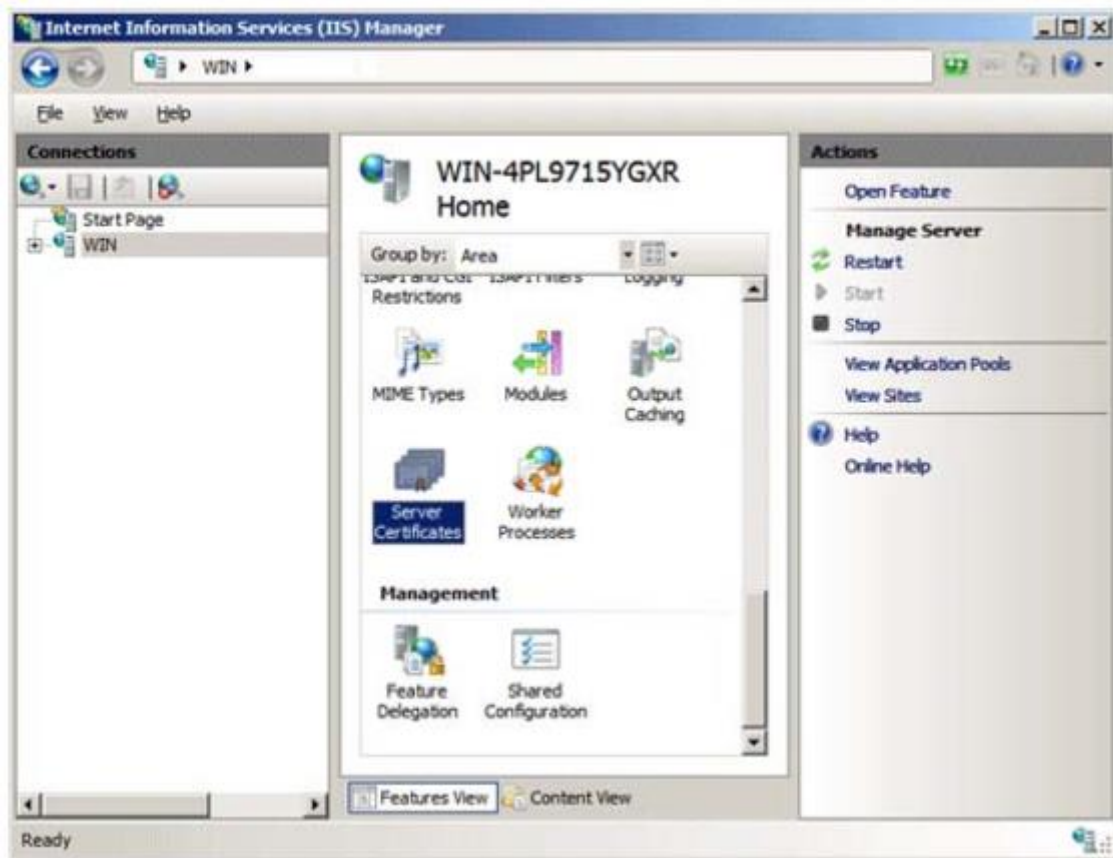
-----BEGIN NEW CERTIFICATE REQUEST-----

```
MIIDVjCCAr8CAQAwezEhMB8GA1UEAxMYbW9ydGFkZWxvLmNhbWVyZmlybWEuY29t
MREwDwYDVQQLewhTaXN0ZW1hczEWMBQGA1UEChMNQUMgQ2FtZXJmaXJtYTEOMAwwG
A1UEBxMFQXZpbGExDjAMBgNVBAgTBUEwY29ydGFkZWxvLmNhbWVyZmlybWEuY29t
hkiG9w0BAQEFAAOBjQAwgYkCgYEAAtB1yMlqIrXKpaLJYZKjCodlHsGjNKhgznI3e
SfNEaDncfA6jY5s9X6WTPECUidfSYaU6e6AroGIEiCYX1TOLitgobm6xvlg+vKgQ
wksv/VvV4RiJWAhYuLh3zmm5L1Yz2dZpropqVDazOSI5zgVlflHV/IrbhajuwPD
vWvuGrECAwEAAaCAAZkwGgYKKwYBBAGCNw0CAzEMFgo1LjAuMjE5NS4yMHsGCisG
AQQBgjcCAQ4xbTBrMA4GA1UdDwEB/wQEAwIE8DBEBGkqhkiG9w0BCQ8ENzA1MA4G
CCqGSIb3DQMCAglAgDAOBggqhkiG9w0DBAICAIawBwYFKw4DAgcwCgYIKoZIhvcN
AwwEwYDVR0IBAwcCgYIKwYBBQUHAwEwgf0GCisGAQQBgjcNAglxge4wgesCAQEE
WgBNAGkAYwByAG8AcwBvAGYAdAAgAFIAUwBBACAAUwBDAGGAYQBuAG4AZQBzACAA
QwByAHkAcAB0AG8AZwByAGEAcABoAGkAYwAgAFAAcgBvAHYAaQBkAGUAcgoBiQBQ
v1G2vDWC9vlizq2Tw35H8AE38oQL76HgPwyKwxqBwK97TtcRyWC8sYKZCsB3E1z+
BwLme8NSShpyluUjh0gBxmH97DiOE2ozuYUR4YI3TpPHZSGBm1ZdcioZomKFZrkpy
JC8jAX02G3DdyKLXJBBHwz6Kx4bGBz5Krnpmc8rxHAAAAAAAAAAAAAAAAA0GCSqGSIb3
DQEBAQUAA4GBAHNEwgk1YVf9SIZrntUFVDYYSms/95iYPo5ApldP+F6RGUJXdkMC
Hg2SpvBAQK25ysPlbrAmVnMhYmEkYPf0D0t6g3SPfcU//+yLrYuYnTkuprCj7D12
sXKeoUc2XcW8qj/kwbymRdqLXSi5uraavUDrPQb5T6VU0ry1nXm64ZYW -----END NEW
CERTIFICATE REQUEST-----
```

4. Instalación.-

Una vez Camerfirma le haya enviado su certificado, vuelva a acceder a la administración de Internet Information Server: pulse sobre el botón de inicio, seleccione Herramientas Administrativas y después Internet Information Services Manager. Cuando se abra la ventana correspondiente, haga clic en el nombre de su servidor.

En el menú central, haga clic sobre el icono de Certificados de Servidor (dentro del grupo de Seguridad, al final de la lista):



Posteriormente, en la parte derecha de la pantalla (Acciones) seleccione la opción "Completar solicitud de certificado", tras lo que se ejecutará un asistente para completar la solicitud del certificado.



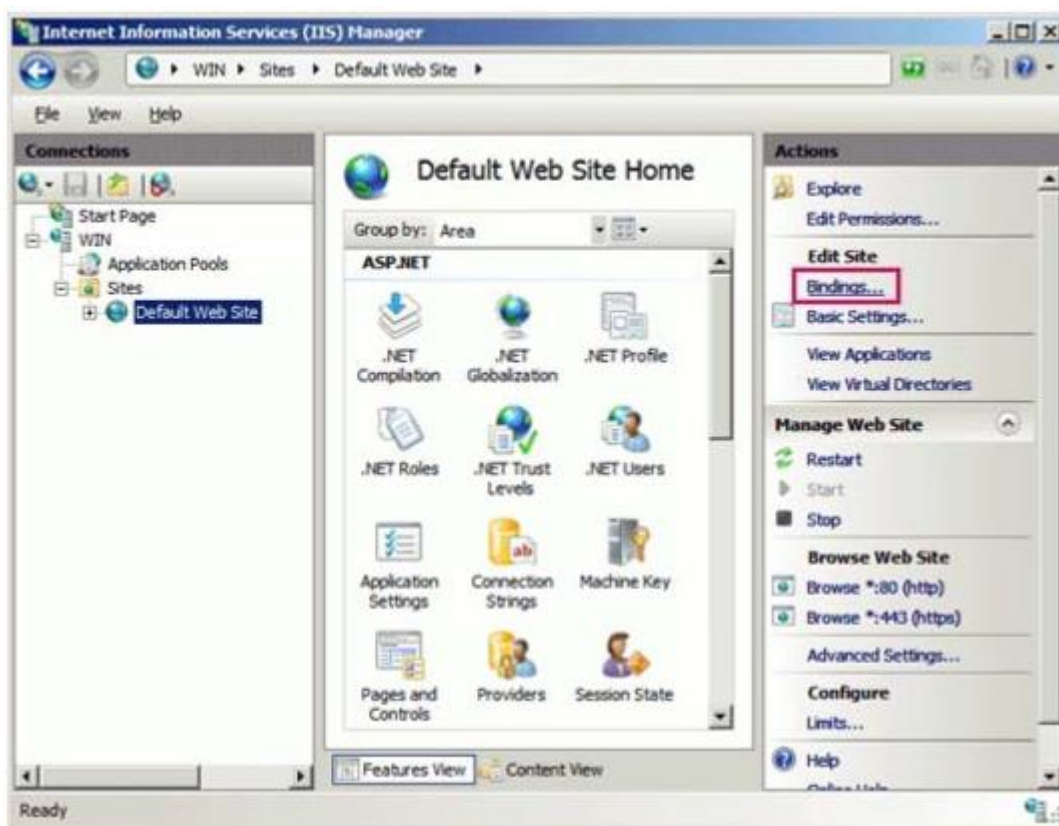
En el asistente, es necesario indicar la ubicación del certificado que le ha enviado AC Camerfirma, así como un nombre descriptivo del certificado. Este nombre se utiliza únicamente para facilitar la administración de certificados de servidor



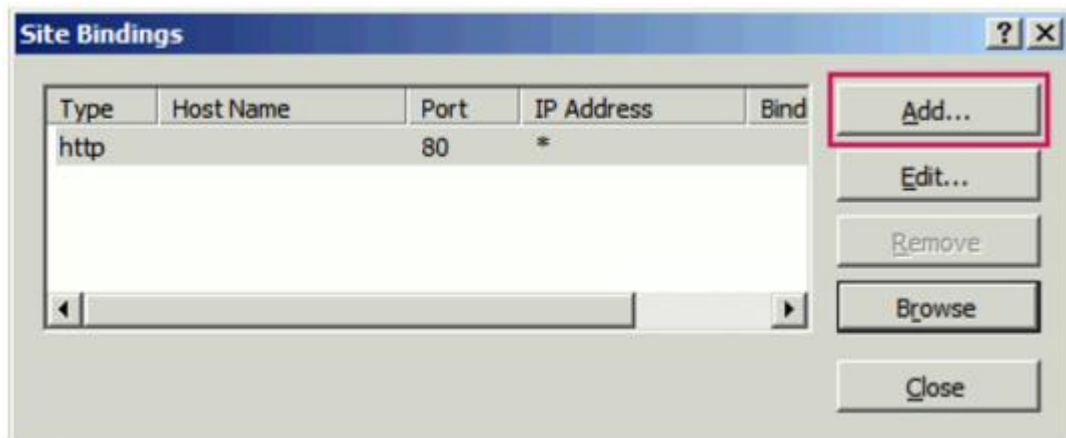
Al pulsar OK el certificado quedará instalado en el servidor.

5. Configuración básica.-

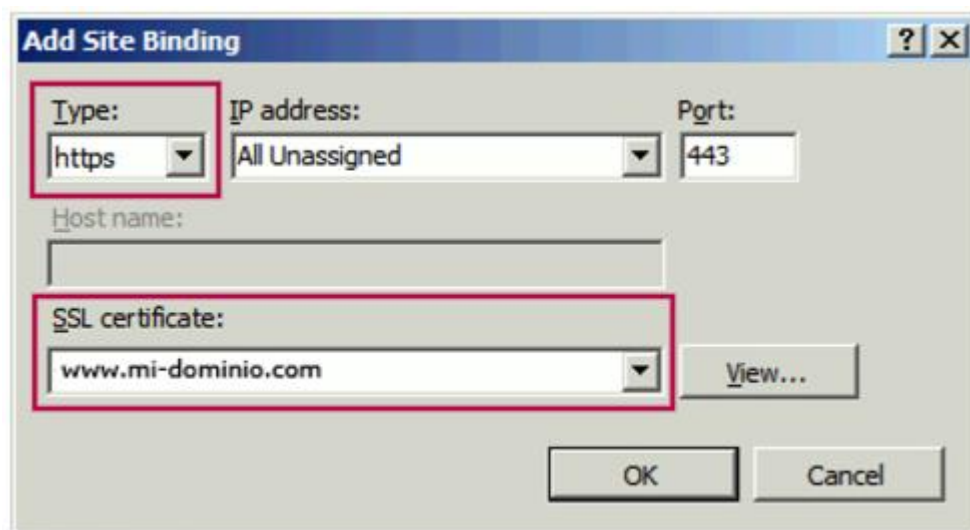
Una vez instalado, deberá asignar el certificado al sitio web correcto. Para ello seleccione en la zona izquierda de la pantalla (Conexiones) el nombre del servidor para el que se ha solicitado el certificado. Despliegue la rama “Sitios” y seleccione el sitio en el que vamos a utilizar el certificado de servidor instalado anteriormente. En la parte derecha (Acciones), seleccione “Conexiones”



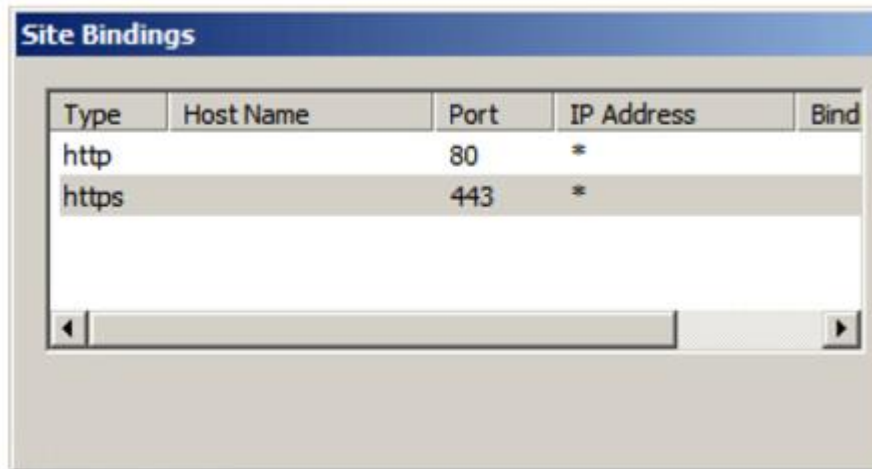
Dentro de la siguiente ventana, seleccione la opción añadir definir una nueva conexión.



En la opción Tipo: seleccione el protocolo HTTPS. El puerto estándar para las conexiones seguras es el 443. En el campo del certificado SSL debe seleccionar el certificado a utilizar. Seleccione el nombre que asignó en el último paso de la instalación.



Tras pulsar aceptar, su sitio está listo para realizar conexiones seguras.



6. Comprobación de la correcta instalación.-

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, si está correctamente instalado tiene que mostrar la cadena completa, como aparece en la imagen.

Use our SSL Checker to help you quickly diagnose problems with your SSL certificate installation. You can verify the SSL certificate on your web server to make sure it is correctly installed, valid, trusted and doesn't give any errors to any of your users. To use the SSL Checker, simply enter your server's public hostname (internal hostnames aren't supported) in the box below and click the Check SSL button. If you need an SSL certificate, check out the [SSL Wizard](#).

[More Information About the SSL Checker](#)

Server Hostname

These results were cached from November 19, 2019, 7:44 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 597 days.](#)
- ✓ [The hostname \(www.camerfirma.com\) is correctly listed in the certificate.](#)



Common name: www.camerfirma.com
SANs: policy.camerfirma.com, cps.camerfirma.com, pds.camerfirma.com, www.camerfirma.com.pe, www.camerfirma.com
Organization: AC CAMERFIRMA SA Org. Unit: SISTEMAS
Location: MADRID, ES
Valid from July 16, 2019 to July 15, 2021
Serial Number: 2191ab80f31231558d
Signature Algorithm: sha256WithRSAEncryption
Issuer: Camerfirma Corporate Server II - 2015



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








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

Si no está correctamente instalado, se mostraría así:



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 → Servicios Cloud → 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