

¿Qué es el código CSR o solicitud de firma de certificado SSL ?

¿Qué es el código CSR (Certificate Signing request) o solicitud de firma de certificado SSL ? Algunas de las preguntas a las que espero dar respuesta aquí: ¿Qué detalles se incluyen en el código CSR?; ¿Cuál es el formato del código CSR?;¿Cómo puedo verificar los detalles incluidos en el código CSR?;¿Cómo puedo generar un código CSR? Una solicitud de firma de certificado (código CSR) es un bloque de texto codificado que contiene la información sobre la organización que solicita un certificado SSL y el dominio que debe protegerse. Un CSR es lo que le da a la Autoridad de Certificación de COMODO (ahora Sectigo CA), para generar su certificado SSL. Es una parte esencial para obtener un certificado SSL.

El código CSR también contiene la clave pública que se incorporará en el certificado emitido. El código CSR se genera a partir de la clave privada RSA y, en la mayoría de los casos, la clave CSR y RSA se generan al mismo tiempo, dependiendo del tipo de panel de control o servidor web en el que se genera el par de claves. Las claves públicas y privadas están relacionadas de tal manera que solo se puede usar una clave pública para cifrar mensajes, y solo se puede usar la clave privada correspondiente para descifrarlos. Por lo tanto, después de generar la clave RSA y el código CSR, puede utilizar el código CSR para la activación del certificado a través de su cuenta con nosotros. Mientras tanto, la clave privada debe permanecer secreta y almacenarse en el servidor, se necesitará para la instalación del certificado en el servidor y se usará para descifrar la información cifrada con la clave pública.

Por lo tanto, recomendamos generar códigos CSR (con claves

privadas RSA) en los servidores en los que se instalará el certificado posteriormente.

Si la clave privada se perdió, se eliminó o se comprometió, se debe generar un nuevo par de CSR y RSA y se debe volver a emitir el certificado .

¿Qué detalles se incluyen en el código CSR?

Como regla general, el código CSR contiene los siguientes detalles; deben rellenarse al crear el código CSR:

- Nombre común: un nombre de dominio completo que debe estar protegido con un certificado SSL. Si desea generar un código CSR para un certificado Wildcard, use un asterisco delante del dominio (por ejemplo, *.ydominio.com).El nombre de dominio completo (FQDN) de su servidor. Debe coincidir exactamente con lo que escribe en su navegador web o recibirá un error de coincidencia de nombre .
- Organización: nombre de la empresa legalmente registrado.El nombre legal de su organización. Esto no debe ser abreviado y debe incluir sufijos como Inc, Corp o LLC, por ejemplo.
- Unidad de organización: División o departamento de la organización que solicita un certificado SSL.La división de su organización que maneja el certificado.
- Localidad: ciudad donde se encuentra la empresa.
- Estado/Condado: Estado o región donde se encuentra la empresa.
- País: Código ISO de dos letras del país donde se encuentra la empresa.
- Dirección de correo electrónico: Dirección de correo electrónico del solicitante de la organización.
- Tamaño de clave: Tamaño de las claves públicas y privadas. El valor mínimo posible es de 2048 bits. Los

códigos CSR de 4096 bits generados en servidores Linux también son compatibles.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBYjCCATMCAQAwwYkxCzAJBgNVBAYTAlVTMRMwEQYDVQOIEwppDYWxpZm9ybmlh
MRYwFAYDVQQHEw1Nb3VudGFpbm93MjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEw
HQYDVQQLExZJb29udGFpbm93MjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEw
Z2x1LmNvbTCBnzANBjQAwgYkCgYEAzYJCHJ4VpVXHFV
IlstQTl04qC03hjX+ZkPyvdYd1Q4+qbAeTwXmCUKYHThVRd5aXSqLPzyIBwieMzr
WFLRQddZ1IzXALVRDwwAo60KecqeAXnnUK+5fXoTI/UgWshre8tJ+x/TMHaQKR/J
4PvFq+e7ipARgI5ZM+GZx6mpCz44Dt0JkwfRdf+BtrsaC0q68eTf2XhYosq4fkH
Q0uA0aVog3f5iJxCa3Hp5gxbJQ6zV6kJOtesuaaOhEko9sdpCoPOnRBm2i/XRD2D
6iNh8f8z0ShGsFqjDgFHyF3o+lUyj+UC6H1QW7bn
-----END CERTIFICATE REQUEST-----
```

¿Cuál es el formato del código CSR?

Un código CSR es un bloque de texto Base-64 enmarcado con `-----` COMIENZO DE SOLICITUD DE CERTIFICADO `-----` y `-----` SOLICITUD DE CERTIFICADO DE FINALIZACIÓN. Un CSR en formato PEM se puede abrir en un editor de texto y se parece al siguiente ejemplo:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBYjCCATMCAQAwwYkxCzAJBgNVBAYTAlVTMRMwEQYDVQOIEwppDYWxpZm9ybmlh
lh
MRYwFAYDVQQHEw1Nb3VudGFpbm93MjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEw
8w
HQYDVQQLExZJb29udGFpbm93MjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEw
9v
Z2x1LmNvbTCBnzANBjQAwgYkCgYEAzYJCHJ4VpVXHFV
fV
IlstQTl04qC03hjX+ZkPyvdYd1Q4+qbAeTwXmCUKYHThVRd5aXSqLPzyIBwieMzr
Zr
WFLRQddZ1IzXALVRDwwAo60KecqeAXnnUK+5fXoTI/UgWshre8tJ+x/TMHaQKR
```

```
/J
cIWPhqaQhsJuzZbvAdGA80BLxdMCAwEAAaAAMA0GCSqGSIb3DQEBBQUAA4GBAI
hl
4PvFq+e7ipARgI5ZM+GZx6mpCz44DTo0JkwfRDf+BtrsaC0q68eTf2XhY0sq4f
kH
Q0uA0aVog3f5iJxCa3Hp5gxbJQ6zV6kJ0TEsuaa0hEko9sdpCoP0nRBm2i/XRD
2D
6iNh8f8z0ShGsFqjDgFHyF3o+lUyj+UC6H1QW7bn
-----END CERTIFICATE REQUEST-----
```

¿Cómo puedo verificar los detalles incluidos en el código CSR?

Para verificar la información utilizada para la generación del código CSR, puede decodificar el código CSR usando una de las siguientes herramientas:

Decoder.link
Comodo CSR Check
Certlogik

El código CSR también se puede decodificar con la línea de comando de Linux usando el siguiente comando:

```
openssl req -in server.csr -noout -text
```



¿Cómo puedo generar un código CSR?

En la mayoría de los casos, una solicitud de firma de certificado es generada por la empresa de alojamiento web en el servidor en el que se va a instalar el certificado. Si tiene su propio servidor o software independiente, puede consultar la documentación del servidor o consultar las instrucciones de generación de CSR .

De todas formas, siempre que necesite [Certificados digitales SSL en Colombia](#), cuente con HostDime.

Leer también: [¿Qué tan importante es el SSL/TLS? ¿Para qué sirve?; ¿Debo tener cifrado SSL así no venda nada en mi sitio web?; ¿Su sitio web necesita un certificado SSL? ¿Cuándo es necesario?](#)