What is a CSR? A CSR or Certificate Signing request is a block of encoded text that is given to a Certificate Authority when applying for an SSL Certificate. It is usually generated on the server where the certificate will be installed and contains information that will be included in the certificate such as the organization name, common name (domain name), locality, and country. It also contains the public key that will be included in the certificate. A private key is usually created at the same time that you create the CSR, making a key pair. A CSR is generally encoded using ASN.1 according to the PKCS #10 specification.

A certificate authority (certificate-authority-reviews.html) will use a CSR to create your SSL certificate, but it does not need your private key. You need to keep your private key secret. The certificate created with a particular CSR will only work with the private key that was generated with it. So if you lose the private key, the certificate will no longer work.

What is contained in a CSR?

Name	Explanation	Examples
Common Name	The fully qualified domain name (FQDN) of your server. This must match exactly what you type in your web browser or you will receive a name mismatch error (ssl-certificate-name-mismatch-error.html).	*.google.com mail.google.com
Organization	The legal name of your organization. This should not be abbreviated and should include suffixes such as Inc, Corp, or LLC.	Google Inc.
Organizational Unit	The division of your organization handling the certificate.	Information Technology IT Department
City/Locality	The city where your organization is located.	Mountain View
State/County/Region	The state/region where your organization is located. This shouldn't be abbreviated.	California
Country	The two-letter ISO code for the country where your organization is location.	US GB
Email address	An email address used to contact your organization.	webmaster@google.com
Public Key	The public key that will go into the certificate.	The public key is created automatically

What does a CSR look like?

Most CSRs are created in the Base-64 encoded PEM format. This format includes the "-----BEGIN CERTIFICATE REQUEST-----" and "-----END CERTIFICATE REQUEST-----" lines at the begining and end of the CSR. A PEM format CSR can be opened in a text editor and looks like the following example:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIByjCCATMCAQAwgYkxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlh
MRYwFAYDVQQHEw1Nb3VudGFpbiBWaWV3MRMwEQYDVQQKEwpHb29nbGUgSW5jMR8w
HQYDVQQLExZJbmZvcm1hdGlvbiBUZWNobm9sb2d5MRcwFQYDVQQDEw53d3cuZ29v
Z2xlLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEApZtYJCHJ4VpVXHfV
IlstQTlO4qC03hjX+ZkPyvdYd1Q4+qbAeTwXmCUKYHThVRd5aXSqlPzyIBwieMZr
WFlRQddZ1IzXAlVRDWwAo60KecqeAXnnUK+5fXoTI/UgWshre8tJ+x/TMHaQKR/J
cIWPhqaQhsJuzZbvAdGA80BLxdMCAwEAAaAAMA0GCSqGSIb3DQEBBQUAA4GBAIhl
4PvFq+e7ipARgI5ZM+GZx6mpCz44DTo0JkwfRDf+BtrsaC0q68eTf2XhYOsq4fkH
```

```
Q0uA0aVog3f5iJxCa3Hp5gxbJQ6zV6kJ0TEsuaaOhEko9sdpCoPOnRBm2i/XRD2D
6iNh8f8z0ShGsFqjDgFHyF3o+lUyj+UC6H1QW7bn
-----END CERTIFICATE REQUEST-----
```

How do I generate a CSR and private key?

You need to generate a CSR and private key on the server that the certificate will be used on. You can find instructions in your server documentation or try the instructions from one of these certificate authorities:

Comodo CSR Generation Instructions (http://www.instantssl.com/ssl-certificate-support/csr_generation/ssl-certificate-index.html)
DigiCert CSR Generation Instructions (http://www.digicert.com/csr-creation.htm?rid=011592)
GeoTrust CSR Generation Instructions (http://www.rapidssl.com/ssl-certificate-support/generate-csr/index.htm)
Thawte CSR Generation Instructions (http://www.thawte.com/ssl-digital-certificates/technical-support/keygen/)
VeriSign CSR Generation Instructions (http://www.verisign.com/support/ssl-certificates-support/page_DEV019431.html)

Once you have your CSR generated, you can use our SSL Wizard to find the best SSL certificate (ssl-certificate-wizard.html) that will meet your needs. If you are familiar with OpenSSL you can use the following command to generate a CSR and private key:

```
openssl req -new -newkey rsa:2048 -nodes -out servername.csr -keyout servername.key
```

How do I decode a CSR?

You can easily decode your CSR to see what is in it by using our CSR Decoder (csr-decoder.html). In order to decode a CSR on your own machine using OpenSSL, use the following command:

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

What is a CSR/Private Key's bit length?

The bit-length of a CSR and private key pair determine how easily the key can be cracked using brute force methods. As of 2016, a key size of less than 2048 bits is considered weak and could potentially be broken in a few months or less with enough computing power. If a private key is broken, all the connections initiated with it would be exposed to whomever had the key. The Extended Validation guidelines (https://cabforum.org/extended-validation/) that SSL certificate providers are required to follow, require that all EV certificates use a 2048-bit key size to ensure their security well into the future. Because of this, most providers encourage 2048-bit keys on all certificates whether they are EV or not.

Originally posted on Sun Dec 7, 2008