



## Certificate Signing Requests

---



Copyright © www.ine.com

# Keith Bogart

CCIE #4923



-  [kbogart@ine.com](mailto:kbogart@ine.com)
-  [@keithbogart1](https://twitter.com/keithbogart1)
-  [linkedin.com/in/keith-bogart-2a75042](https://www.linkedin.com/in/keith-bogart-2a75042)

CCIE Routing & Switching



Copyright © [www.ine.com](http://www.ine.com)



# Topic Overview

---

- ▷ What is a Certificate Signing Request?
- ▷ CSR Structure
- ▷ CSR Required Fields
- ▷ Generating a CSR
- ▷ Submitting a CSR

Copyright © www.ine.com



# Certificate Signing Request (CSR)

▶ A block of encoded text that is given to a Certificate Authority when **applying for an SSL Certificate**.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBzTCATYCAQAwg1hwxC2AJBgNVBAYTAUFRMrcwFQYDVOQIEw50b3J0eCBOYXJv
bGluYUVEQMAA4GA1UEBxMUMmFzZWlnaDEbMBKGA1UEChM5VzdzCDBb2SzdW0oW5n
JGNlMRswGQYDVOQLEqJUZkN0aW5nERlCGFydG11bnQxGDAWBgNVBAMTD3d3dy5z
dGVmYW5lLnVzTCBzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAuETMZEwashf3
EAHT9+LdkNqYTLc3kQ9KwK0XslqK5X98lsXjcrewKDPFzle59u+wqRdy3Yh2
er2yKdUu/fMecqk9PooluH25iNKvVhW/Rm8DKW2sfmLhii+xQX7V0k8KfRhc
ChkCG0zshv+Hic17okbQJD+RT5icGJECAwEAQAAAMA0GCSqGSIb3DQEBBAUAA4GB
AImvzjFQUW3p7LElUEP2H0lq0dtsfHxQcv620/NX8aGatgA72F6L679G92Gjlb
UOnngy4emQH9uyzZWb+JckrOSDphskKspjucD6UIMOATWAPyuojm8sCjH2U03d
thlcpDYMRZv+Bp16BkzP5XLIlyBpZFfXskBdr+Df
-----END CERTIFICATE REQUEST-----
```

- ▶ Format defined by PKCS#10
- ▶ Generated on server that is requesting a Cert
- ▶ Public/Private keypair generated at same time.

Copyright © www.ine.com



PKCS = Public Key Cryptography Standard devised and published by RSA Security in early 1990s.

- A CSR is generally encoded using ASN.1 (Abstract Syntax Notation 1) according to the PKCS #10 specification.

- More information about the syntax can be found here: [https://en.wikipedia.org/wiki/Certificate\\_signing\\_request](https://en.wikipedia.org/wiki/Certificate_signing_request)

## CSR Structure

- ▶ A CSR is divided into three, main parts;
  - ▶ Certificate Request Information
    - ▶ Version number (0) and required identification information (next slide)
  - ▶ Signature Algorithm Identifier
    - ▶ CSR will be signed with Private Key of the Requestor
    - ▶ Prevents an entity from requesting a bogus CSR on your behalf.
  - ▶ Digital Signature

Copyright © www.ine.com



So as we can see here...just as the final Digital Certificate is “signed” by the CA (which proves that ONLY the CA could have created it because it was signed by THEIR private key) the initial CSR is also signed...in this case with the Private Key of the Requestor.

In this way, nobody could steal your certificate, modify a couple of fields (like replacing a few characters in the Common-Name with their own URL) and resubmit it with your Public Key...because they couldn't sign in.

## CSR: Required Fields

- ▶ Certain fields are required by the standard to submit a CSR to a Certificate Authority:
  - ▶ **Common Name**
    - ▶ FQDN if the Cert is to be used for a Web Server
    - ▶ Must match DNS Resolution lookups
  - ▶ **Country Code**
    - ▶ [https://www.nationsonline.org/oneworld/country\\_code\\_list.htm](https://www.nationsonline.org/oneworld/country_code_list.htm)
  - ▶ **City/Locality Code**
  - ▶ **State/Province**
  - ▶ **Organization**
    - ▶ Registered and legal Organization Name (corporation, limited partnership, university, or government agency)
  - ▶ **Organizational Unit**
    - ▶ Mandatory field to differentiate between divisions within an organization
  - ▶ **Email Address** of Certificate Administrator or IT Department
  - ▶ **Public Key**

Copyright © www.ine.com



Depending on CA...sometimes the key-type (RSA) and key-size is also required.

-





Most SSL CAs require a key that is at least 2048-bits in length.

# Generating A CSR

▶ Most CA websites have links with instructions on how to generate a CSR:

▶ <https://www.instantssl.com/ssl-certificate-support/csr-generation/ssl.html>

▶ <https://www.digicert.com/csr-creation.htm?rid=011592>

 Microsoft Internet Information Services	 Microsoft Exchange Server	 APACHE	 Microsoft Office Communications Server 2007
Generate a CSR with Comodo Certificate Utility Microsoft IIS 8.x Microsoft IIS 7.x Microsoft IIS 5.x / 6.x Microsoft IIS 4.x	Generate a CSR for Exchange 2010 Generate a CSR for Exchange 2007 Generate a CSR with Comodo Certificate Utility	Apache Server (OpenSSL)  Generate a CSR for Apache Mod SSL Open SSL Generate a CSR for Apache Open SSL Generate a CSR for Apache ECC	Generate a CSR with Comodo Certificate Utility Office Communications Server 2007

**Decode a CSR!!** <https://www.sslshopper.com/csr-decoder.html>

Copyright © www.ine.com



# Submitting A CSR

- ▶ Once a CSR is generated in the correct format on your Server, most CA's have secure websites for uploading it:

The screenshot shows the 'DigiCert Order Form - Purchase Digital Certificates' interface. It features a progress bar at the top with three steps: '1 Select Product', '2 Organization Information', and '3 Payment'. A 'LIVE CHAT' button is visible in the top right corner. Below the progress bar, there is a blue information box with a 'Log in' button. The main content area is titled 'Step 1: Select a Product' and is divided into two columns. The left column lists product categories: 'Business SSL/TLS' (with 'Secure Site SSL' selected) and 'Basic SSL/TLS'. The right column provides detailed benefits for the selected 'Secure Site SSL' product, such as 'Provides encryption and authentication for one domain' and 'No licensing fees - install the certificate on multiple servers at no extra cost'. On the far right, there is an 'Order Summary' box showing a price of '\$399.00 USD' and a 'SECURE SITE SSL' term of '1 Year'. Below the order summary, there is a 'Buy with Confidence' section listing several benefits like '24/7 support' and 'Strongest 256-bit encryption'. The bottom left corner of the page contains the text 'Copyright © www.ine.com' and the bottom right corner features the 'INE' logo.

CSRs typically have a 24-72 hour turnaround time.



Thanks for watching!