Certificate Signing Requests

Keith Bogart

CCIE #4923

- kbogart@ine.com
- @keithbogart1
- linkedin.com/in/keith-bogart-2a75042

CCIE Routing & Switching

Topic Overview

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

Certificate Signing Request (CSR)

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

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

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

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

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
  - **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**

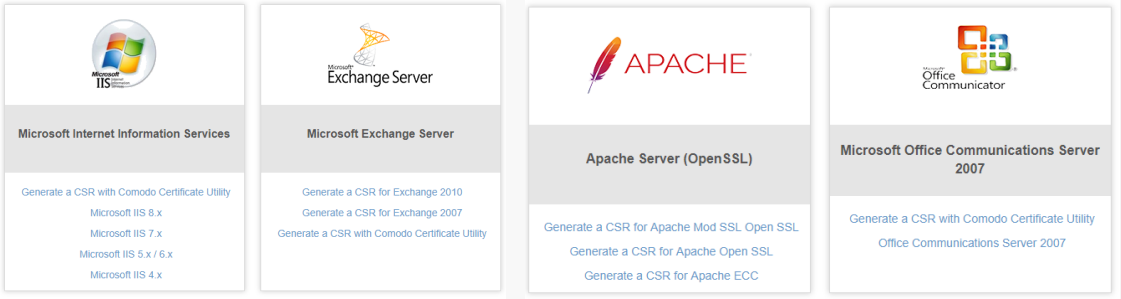
Depending on CA…sometimes the key-type (RSA) and key-size is also required.

-

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

Generating A CSR

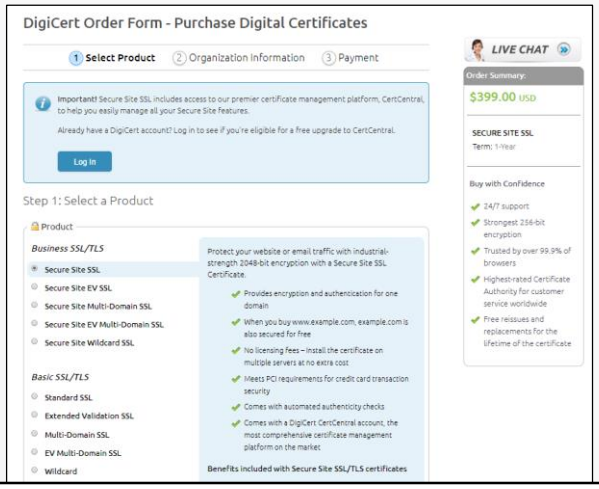
- Most CA websites have links with instructions on how to generate a CSR:
  - https://www.instantssl.com/ssl-certificate-support/csr-generation/ssl.html
  - https://www.digicert.com/csr-creation.htm?rid=011592



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

Submitting A CSR

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



CSRs typically have a 24-72 hour turnaround time.