Types Of Digital Certificates

Keith Bogart

CCIE #4923

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

CCIE Routing & Switching

Topic Overview

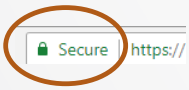
- Domain-Validated Certificates
- Organization-Validated Certificates
- Extended-Validation Certificates

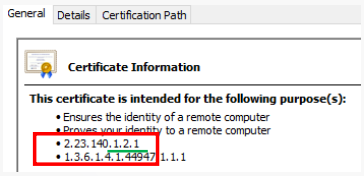
Digital Certificate Types

- Three categories of Certificates
  - DV: Domain-Validated
  - OV: Organization-Validated
  - EV: Extended-Validation
- Different categories provide different degrees of trust.
- More validation = more $$$ for purchaser of the cert.

Domain-Validated

- Most common form of SSL Certificate
- Only verifies that the requestor has valid control over the domain name listed in the Certificate.
- A variety of methods are used for validation:
  - Put a CA-provided challenge at a specific place on the web site.
  - Put a CA-provided challenge in a DNS record corresponding to the target domain.
  - Receive a CA-provided challenge at a (hopefully) administrator-controlled email address corresponding to the domain and then respond to it on the CA's web page
  - CA requests installation of software on your web host (i.e. ACME protocol)





ACME = Automatic Certificate Management Environment (ACME)

-

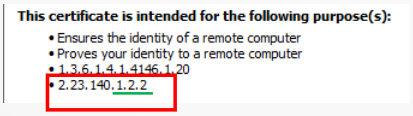
The value starting with 2.23.140 is called the X.509 Issuer Unique Identifier and somehow allow the receiving system to understand what kind of Cert this is.

-

FUNNY EXAMPLE: fbi.gov

Organization-Validated

- Very common form of SSL Certificate
  - Also known as “High Assurance” Certificates
- CA will verify the actual business that is attempting to get the certificate.
  - Identity and Street Address
- A variety of methods is used for validation:
  - A link to a **government agency** in the jurisdiction of the Applicant’s **legal creation**, **existence**, or **recognition.**
  - A link verifying your information in a **third party database** that is periodically updated and considered a Reliable Data Source.
  - Copies of government-issued business license
  - MANY other options available.



With an OV certificate, you are validating that you not only control the domain-name of your server, but that you are a legitimate business with a legitimate street address.

-

For example, a company doing business in Alaska but incorporated in Nevada would need to appear in a search of Nevada businesses.

-

Your company’s information might be validated by searching for it within the BBB website.

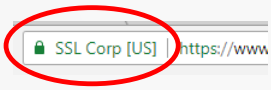
-

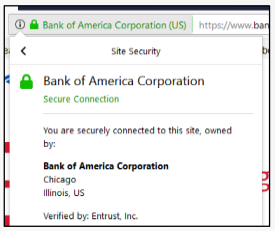
Example: nsa.gov

Extended-Validation

- Provide the maximum amount of trust to visitors, and also require the most effort by the CA to validate.
- Have the greatest cost $$$
- A fully validated EV certificate will also show the name of the company or organization in the address bar itself, and the address bar (may be) displayed in green.
- Too many verification steps to list here.

https://www.ssl.com/faqs/ssl-ev-validation-requirements/





Example: CIA.gov

Depending on the browser you may-or-may not see the green bar. But at MINIMUM you should see the name of the company right next to the padlock symbol.

-

Some of the steps include that a company must submit three documents:

A **signed copy** of the EV Subscriber agreement

A **signed copy** of the EV Authorization Form

Please choose **one** of the following items to submit:

- Your company's Dun & Bradstreet number
- A letter from a Certified Public Accountant to verify your business
- A letter registering a legal opinion, or a letter from a Latin Notary, to confirm your EV request.
- (For government entities only) A legal opinion letter verifying a government organization

Then verification proceeds as follows:

Verify Legal Existence and Identity by verifying the organization registration directly with the incorporating or registration agency.

Verify Trade/Assumed Name (if necessary)- this is only applicable if the company does business under a name which is different from the official name of their corporation. The company's trade name must be **registered** and **verifiable.**

Verify Operational Existence – typically this means confirming that the company has a current active demand deposit account with a regulated financial institution to verify that the company is able to conduct business operations.

Verify Physical Existence through the company's address and organization phone number.

Verify Domain Ownership via a WHOIS search.

Verify the name, title, authority and signature of the person(s) involved in requesting the certificate and agreeing to the terms and conditions.