CAB CA/BROWSER FORUM

Home » Information for the Public

INFORMATION FOR THE PUBLIC

Helpful information for the public.

What are the different types of SSL Certificates?

Domain Validation (DV)

A Domain Validated SSL certificate is issued after proof that the owner has the right to use their domain is established. This is typically done by the CA sending an email to the domain owner (as listed in a WHOIS database). Once the owner responds, the certificate is issued. Many CAs perform additional fraud checks to minimize issuance of a certificate to a domain which may be similar to a high value domain (i.e. Micros0ft.com, g00gle.com, b0fay.com). The certificate only contains the domain name. Because of the minimal checks performed, this certificate is typically issued quicker than other types of certificates. While the browser displays a padlock, examination of the certificate will not show the company name as this was not validated.

Organizational Validation (OV)

For OV certificates, CAs must validate the company name, domain name and other information through the use of public databases. CA's may also use additional methods to insure the information inserted into the certificate is accurate. The issued certificate will contain the company name and the domain name for which the certificate was issued for. Because of these additional checks, this is the minimum certificate recommended for ecommerce transactions as it provides the consumer with additional information about the business.

Extended Validation (EV)

EV Certificates are only issued once an entity passes a strict authentication procedure. These checks are much more stringent than OV certificates.

The objectives of EV Certificates are twofold:

- **Identify the legal entity that controls a Web site:** Provide a reasonable assurance to the user of an Internet browser that the Web site the user is accessing is controlled by a specific legal entity identified in the EV Certificate by name, address of Place of Business, Jurisdiction of Incorporation or Registration and Registration Number or other disambiguating information; and

- **Enable encrypted communications with a Web site:** Facilitate the exchange of encryption keys in order to enable the encrypted communication of information over the Internet between the user of an Internet browser and a Web site.

The secondary purposes of an EV Certificate are to help establish the legitimacy of a business claiming to operate a Web site or distribute executable code, and to provide a vehicle that can be used to assist in addressing problems related to phishing, malware, and other forms of online identity fraud. By providing more reliable third-party verified identity and address information regarding the business, EV Certificates may help to:

1. Make it more difficult to mount phishing and other online identity fraud attacks using Certificates;
2. Assist companies that may be the target of phishing attacks or online identity fraud by providing them with a tool to better identify themselves to users; and
3. Assist law enforcement organizations in their investigations of phishing and other online identity fraud, including where appropriate, contacting, investigating, or taking legal action against the Subject.

Because of the strict vetting procedures which CA's use to check the information about the applicant, the issuance of EV certificates usually takes longer than other types of certificates. An overview of this vetting process can be found here. The resultant EV SSL certificate will contain the information here.

Figure 1 compares the features of the three types of certificates:

Type of certificate	*Domain validated?*	*Subject Name Validated?*	*Address Validated?*	*Pad Lock Displayed by Browser?*	*Green address bar or other special treatment?*	*Relative price*

to search type and hit enter

RECENT NEWS

- Ballot 212 – Canonicalise formal name of the Baseline Requirements September 1, 2017
- Ballot 210 – Misc. Changes to the NCSSR August 31, 2017
- 2017-08-03 Minutes August 3, 2017
- 2017-07-20 Minutes July 20, 2017
- Ballot 204 – Forbid DTPs from doing Domain/IP Ownership July 11, 2017
- Ballot 205 – Membership-Related Clarifications July 6, 2017
- Ballot 192 – Notary Revision June 28, 2017
- 2017-06-21 F2F Minutes Meeting 41 in Berlin June 21, 2017
- Ballot 203 – Formation of Network Security Working Group June 19, 2017

PAST PROCEEDINGS

Past Proceedings Select Month

BY CATEGORY

By Category Select Category

Current Work » Resources »

DV	X			X		$
OV	X	X	X	X		$$
EV	X	X	X	X	X	$$$

Figure 1

What are Public Certificate Authorities?
Public Certificate Authorities are companies or government agencies that have been authorized by browsers to issue SSL and code signing certificates. These organizations must undergo annual audits by third parties in order to insure they are following rules regarding the proper vetting, issuance and revocation of certificates. Certificates issued by companies that have not been approved by browsers will display a warning [Rick: will cause a warning to be displayed] when consumers browse to a page secured by that certificate.

Can Certificates be used to defraud consumers?
An OV or EV certificate has undergone checks to insure that the business owns the domain and is a valid business.

If the certificate error indicates a “name mismatch”, it could indicate that the certificate is being used in a “phishing site” to defraud consumers. Do not proceed if this warning is present on ecommerce sites.
If the certificate error indicates the certificate authority is “not trusted”, this means the browser has not approved the certificate authority that issued the certificate. Do not proceed if this warning is present on ecommerce sites.

It does not however indicate that the organization is reputable or worthy of your business. Nor does the presence of an SSL certificate guarantee that the web site is correctly implemented and free from malware. When shopping at an unknown, online merchant site, in addition to looking at the certificate details, consumers should check the reputation of that business via third party review sites such as the Better Business Bureau, Yelp, Dunn and Bradstreet, or other reliable consumer information web sites (i.e. http://www.consumer.ago.mo.gov/Know_MO/).

I’m getting a certificate error message when I go to a certain ecommerce website. What should I do?
It depends on what the exact error is. Most browsers will allow you to get more details about the error. If the error indicates the certificate has expired or not yet valid, check the clock on your PC to make sure it is set correctly. Also, check the date the certificate expired (located in the certificate details, usually accessed by clicking on the certificate). If it expired a few days ago, the website owner may have forgotten to renew it.

ONE COMMENT

Pingback: Track Certificates to Help Users Stay Safe - Webnesday