How to differentiate between Domain & Organization Validated SSL

How to Identify DV SSL & OV SSL apart

There are three levels of SSL Certificates. They are Domain Validated (DV) SSL, Organization Validated (OV) SSL and Extended Validation (EV) SSL.

A lot of information is available about how an EV SSL is differently displayed in a browser (only a website with EV SSL displays green bar) than an OV SSL or DV SSL. But in order to spot the difference between DV and OV SSL, the non EV SSL ones, we need to look at the structure of these certificates.

Deterministic Approach

To know what specific type a certificate is, the only way is to know about practices of every CA (Certification Authority).In the Digital Certificate /X.509 PKI standard, Certificate Policies extension defined in RFC 5280 explains different methods through which an issuer is presumed to demonstrate their practices.

This enables a CA to show an OID (a unique identifier) in certificates that are issued. It maps its practices associated with the certificate to a document. This identifier can be utilized according to the program in making trust decisions about a certificate or to distinguish the user interface in an application

on the basis of certificate type.

This is how browsers can differentiate if a certificate is EV SSL or not. Actually, it can be said that the browsers have some configuration that tells that "I trust GlobalSign to issue EV Certificates when a certificate is presented to me from them that has this policy OID, show the EV user experience, such as activating the green address bar."

The same approach is followed by CAB/Forum Baseline Requirements to define identifiers for DV SSL and OV SSL Certificates. They are:

Type	Policy Identifier
Domain Validated	2.23.140.1.2.1
Organization Validated	2.23.140.1.2.2

These identifying measures help us reach the goal of deterministic evaluation of policy regarding certificate issuance. But, not all CAs follow them yet.

Heuristic Approach

It is obvious that existing install base of certificates will take a while in reissuing to use the policy identifiers because the CA/B Forum

ZNETLIVE™
THE HOSTING ARCHITECT   SINCE 2002

How to differentiate between Domain & Organization Validated SSL

Baseline Requirements have been established very recently in 2012. RYAN Hurst, GlobalSign's CTO have put out some example code on how to configure an application with an aim to determine class of the certificate without relying on object identifiers.

More on Ryan Hurst heuristic approaches to determine classes of certificates: http://unmitigatedrisk.com/?p=2 03

Summary

It is unfortunate that no deterministic way exists today to recognize if a certificate is DV SSL or an OV SSL, but with changing technology, it is hoped that there will be a way out. Meanwhile, these heuristics can prove helpful to tell EV SSL from non EV Certificates.

About GlobalSign

GlobalSign has been in the business of providing SSL Certificates since 1996. It is one of the world's first CA (Certificate Authority). It offers services in multiple languages and its technical support is present in places like London, Brussels, Boston, Tokyo and Shanghai.

GlobalSign is a leader in public trust services the market of SSL Certificates. Its Certificates include SSL, Code Signing, Adobe CDS Digital IDs, Email and Authentication, internal PKI

and Microsoft Certificate Service etc. GlobalSign's root CA Certificates are trusted and recognized by all the major web browsers, operation systems, internet applications, email clients and all the mobile devices as well.

About ZNetLive

ZNetLive is India's leading web hosting provider which has been providing its services since 2001. At ZNetLive, our goal is simple- our customers' online success. And we touch this goal every day, providing Domains Registration, Web Hosting, Business Email, Websites, Business Apps and more, to our diverse global customer base, who make us what we are.

Our state of the art infrastructure and datacenters in Washington, Seattle, Dallas, Mumbai and Bangalore are second to none, we are successful because we promise, and deliver 99.9% network uptime to every single customer of ours. We've been in the industry since 11 years and our experience shows in the finesse of our unparalleled products.