Certificate Authorities & Trust Hierarchies

What are CAs & Trust Hierarchies?

Digital Certificates are issued by Certificate Authorities/ Certification Authorities or CAs. Digital Certificates are small verifiable files of data that include identity credentials, which aid devices, websites and people to show their credible or authentic online identity (authentic as the identity has been verified by the CA). CAs play a key role in the operation of the internet as well as the way in which trusted and transparent transactions happen online. Millions of digital certificates are issued by CAs every year and these certificates ensure secure transactions and safe communication, thereby protecting crucial information by encrypting billions of transactions, leading to safe operations.

An SSL Certificate is nothing but a well-known Digital Certificate which uses cryptographic keys for binding the details of ownership of a website or web server to them. These keys find usage in the SSL/TLS protocol for activating a safe session between the web server and a browser that hosts the SSL Certificate. The browser trusts an SSL certificate and establishes a secure session without generating any warnings only if the SSL certificate:

- Includes the domain name of the website that is using it.
- Should not be expired.
- Should be issued by a trusted Certificate Authority (CA).

An analyst site Netcraft (www.netcraft.com) declared that there were nearly 2.5m SSL certificates that were in use by public facing sites in Aug 2012. But actually, there must be atleast 50% more websites than this number which were not identified by Netcraft. Thus, SSL is one of the leading technologies in usage in the present day IT scenario.

Who decides which CA can be trusted and which cannot be trusted?

Accredited CA membership programs are being run by browsers, mobile devices and operating systems, where a CA needs to fulfill detailed norms so that they can be accepted as members. If a CA is accepted , he is allowed to issue SSL Certificates that are trusted plainly by the browsers, devices and subsequently people which rely on the certificates issued by him for their data safety. The more time the CA is operational, the more trusted he becomes and more browsers and devices trust him. There is a relatively small number of authorized CAs, from private companies to governments and the certificates are more plainly trusted, if they possess 'Ubiquity', which is the ability of being backward compatible i.e. compatible with older mobile devices and browsers. This is an important and valuable feature which a CA can offer to its clients.

Certificate Authorities & Trust Hierarchies

Before issuing an SSL certificate, the CA runs a number of checks to verify the applicant's identity. The checks are directly related to the type and class of certificate being applied to. For example, a DVSSL Certificate verifies only the domain ownership as it is included in the Certificate, whereas an EVSSL requires multiple details and checks on the company by the CA.

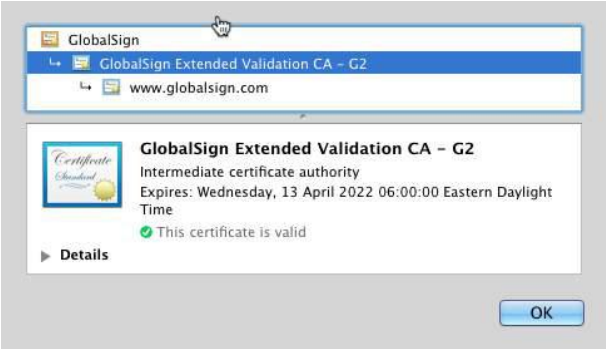
PKI & Trust Hierarchies

A Certificate Authority is trusted by devices and browsers by including the Root Certificate of the CA into its own root store, which actually is approved CAs database and comes pre-installed in a device or browser. All browsers and mobile carriers like Windows, Apple, and Mozilla (for its Firefox browser) runs their own root stores.

The Apple OSX store of trusted Root Certificates

These pre-installed Root CA Certificates are utilized by CAs for issuing end entity Digital Certificates and Intermediate Root Certificates. The CA takes in certificate requests, performs application validations, issues the certificates, and provides the recent validity status of issued certificates so that anyone looking for certificate's validity comes to know about its validity status.

CAs normally create multiple Intermediate CA (ICA) Root Certificates which are utilized for issuing end entity certificates, like SSL Certificates. This is known as a trust hierarchy, and looks like the figure below:



The GlobalSign Extended Validation CA - G2 is shown in this example as the ICA - it's trust is inherited from the publicly trusted GlobalSign root (top of the hierarchy). This ICA is able to issue publicly trusted end entity certificates, in this example, the ICA issued an Extended Validation Certificate to www.globalsign.com.

Certificate Authorities & Trust Hierarchies

Digital Certificates should not be issued by the CAs directly from the root provided to the carriers, but instead through any of their ICAs. This is counted among best practices and it prevents the Root CA from being exposed to attackers. GlobalSign is among those CAs who always utilizes ICAs (since 1996).