SSL Certificates: Chained Root vs. Single Root

SSL certificates from a trusted Certificate Authority that owns all of its own roots provide the highest level of credibility, certificate stability and server security.

For a Certificate Authority to have its own Trusted Root CA certificate already present in browsers is a clear sign that they are long-time, stable and credible organizations who have long term relationships with the browser vendors (such as Microsoft and Netscape). Most SSL certificates are issued by Certificate Authorities (CAs) who own and use their own Trusted Root CA certificates. They are known to browser vendors as a trusted issuing authority since their Trusted Root CA certificate has already been added to all popular browsers. A browser must contain this CA Certificate in its "Trusted Root Library" in order to "trust" certificates signed by the CA's private key. These SSL certificates are known as "single root" certificates.

Some CAs, however, do not have a Trusted Root CA certificate present in browsers, and therefore need to “chain” their roots for their certificates to be trusted by browsers. Essentially, a CA with a Trusted Root CA certificate issues a certificate to the third-party certificate provider which then "inherits" the browser recognition of the Trusted Root CA. These SSL certificates are issued off of an intermediate root certificate (not the top level root certificate) and are known as "chained root" SSL certificates.

HOW SSL TECHNOLOGY USES ROOT CERTIFICATES IN THE ENCRYPTION PROCESS

When connecting to a web server over SSL, a visitor's browser decides whether or not to trust the website's SSL certificate based on which CA issued the actual SSL certificate. To determine this, the browser looks at its list of trusted issuing authorities -- represented by a collection of Trusted Root CA certificates added into the browser by the browser vendor.

Like SSL certificates, root certificates also have a public and private key pair used to encrypt and decrypt information that is sent between two devices. The private key of the root certificate is heavily guarded and kept in the certificate provider's secure data center; while the public key of the root certificate is given to browser and application manufacturers to be added to their list of trusted roots. Embedding the public key into the browser or application allows the software to automatically recognize and trust any SSL or client certificate that has been signed by that root certificate.

The more browsers, web servers and applications that a certificate provider embeds their root certificates in, the higher their certificate "ubiquity" is. Certificate ubiquity is a term that essentially means "the percentage of the most popular browsers, web servers, and applications that inherently recognize and trust the providers root certificate." For example, GeoTrust maintains 99% browser ubiquity in the marketplace, which means that all GeoTrust certificates will be recognized and trusted by all the most popular browsers, web servers and applications available today.

KEY DIFFERENCES BETWEEN SINGLE ROOT AND CHAINED ROOT CERTIFICATES

There are several key differences between single root and chained root certificates, namely:

- **Installation Complexity**

  Because chained certificates are issued off of an intermediate root and not the top level root certificate, the intermediate root must be manually loaded on every web server and application that is hosting the certificate. This makes the installation of chained root certificates much more complex and cumbersome for network administrators. It also poses serious security risks since some web servers are not compatible with chained root certificates.

  Conversely, single root certificates do not require any intermediate roots to be loaded since the root certificate is automatically recognized and trusted by browsers, email clients and applications.

- **Root Stability**
  Because chained root certificate providers must rely on a trusted root certificate owner to allow them to issue certificates, they have no control over what the owner of the certificate actually does with the certificate. For example, if the parent company that owns the roots goes out of business, then all the companies that have a root chained to that parent company would have invalid certificates.

- **Root Expiration**
  All root certificates have a finite expiration date and it is the responsibility of the certificate provider to formulate a transition plan to a new root certificate before it expires. This process involves serious planning and forethought on the part of the root owner, as the new root must be embedded into future browsers, web servers, and applications that will use their certificates.

  Since chained intermediate roots also have an expiration date they must expire prior to the root certificate, which adds to the complexity of transitioning over to a new root. If the owner of the chained root does not ensure that this occurs, the chained root certificates become invalid and not trusted once the root certificate expires.

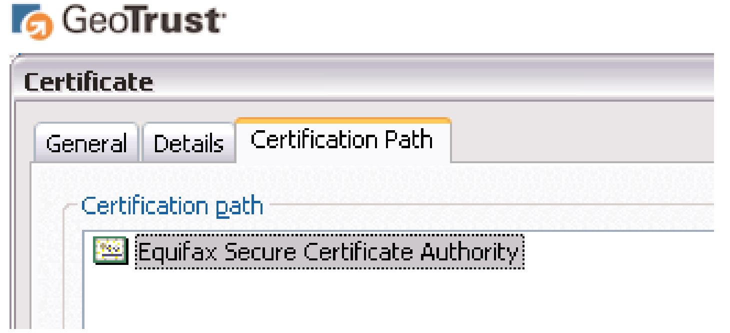
HOW TO DETERMINE IF A CA OWNS ITS OWN CERTIFICATE ROOT

Every browser contains a Trusted CA root certificate store that can be easily accessed. For example, in Internet Explorer:

- Go to “Tools”
- Select “Internet Options”
- Select the “Content” tab
- Click on “Certificates”
- Finally, select the “Trusted Root Certification Authorities” tab

You will then see a dialog box presenting a list of all Certification Authorities who own their own Trusted CA roots (you can examine the root certificate by double clicking it).

You can also examine trusted root ownership by double clicking the padlock seen in the browser during an SSL connection with a web server. When the SSL Certificate appears, simply click the "Certification Path" tab to see which trusted root CA certificate issued the SSL certificate (see example right).



GeoTrust owns the Equifax root (Equifax Digital Certificate services became GeoTrust in 2001).

ABOUT GEOTRUST.

GeoTrust is a leader in identity verification and trust services for e-business. Its products include web security services for secure e-commerce transactions, identity verification, managed security services and TrustWatch (www.trustwatch.com), a free toolbar and search site that helps consumers recognize whether a site has been verified and is safe for the exchange of confidential information. With more than 100,000 companies in over 140 countries using its technology for online security, GeoTrust has rapidly become the second largest Certificate Authority in the world.

Visit www.geotrusteurorope.com or call +44 1622 764789 option 3 for more information.

GeoTrust
6 Kings Row, Armstrong Road
Maidstone, Kent, UK
Phone: +44 1622 764789
E-mail: info@geotrusteurope.com
www.geotrusteurope.com