Secure SSL Connection with Intermediate Certificates

When browsers connect to a web site over HTTPS, SSL is used to ensure the data transmitted is encrypted to prevent eavesdropping. This is standard technology as used by online banking and shopping etc.

In order to set up an 'SSL Connection', certificates are used to verify the authenticity of the web site. Without this, the browser would not be able to determine if the site they are connected to is the real one (such as in a 'man in the middle' attack, where a 'fake' site masquerades as something different to intercept the data stream).

To ensure this authenticity, Certificate Authorities (CA – the companies who issue certificates) sign them so that the browser can determine if they are genuine, and that they have not been tampered with.

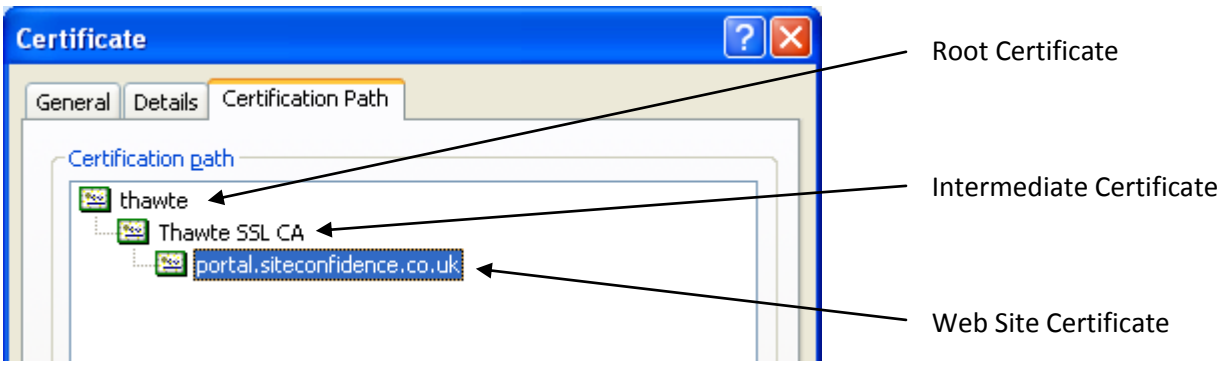
For all valid SSL connections, there is a web server certificate that has been purchased from a CA and is installed on to the web server (or load balancer if off loaded), which hosts the site. This certificate will specify an issuer, for which there must also be a valid certificate.

Sometimes, the issuer will be a root certificate. This is distributed by the browser vendor, such as Microsoft for Internet Explorer, or Mozilla for Firefox.

Some web server certificates use an intermediate (or chained) certificate as the issuer. In these cases, the intermediate certificate must also be installed on the web server (or load balancer), alongside the main certificate. If it is not, the SSL connection may be shown as "Not Trusted" by some browsers. These certificates are provided by the CA when they issue the main web site certificate.

Different browsers behave differently, but essentially if the intermediate certificate is not installed alongside the certificate for the web site, users of your site may get security warnings because of connection that cannot be trusted.

The certificate 'chain' can be seen in the browser – for example, in Internet Explorer the Portal certificate chain is:



In order to successfully validate your site, we check all the certificates are installed correctly, including intermediate certificates. If they are missing, we will report the item as failing SSL validation.

There are numerous external sites that can be used to independently validate your web server's SSL configuration and clearly identify if your site is correctly set up, indicating if your customers may experience problems.

For example the following site will do this, but also offers links on how to install your certificates correctly for your particular web server:

http://www.sslshopper.com/ssl-checker.html

Sometimes, this issue is not particularly apparent in a user's browser – here are some more details why:

Internet Explorer:

> If the intermediate certificate is not installed on the web server, IE will use the Authority Information Access (AIA) defined in the certificate it has got from the web server to work out where else it could get the next certificate in the chain. The browser then gets this certificate separately, as it is not correctly installed on the web server.

Firefox:

> Firefox will not do this. However, one reason why it is not obvious is because if Firefox visited "Site A" that was correctly configured and then "Site B" that was not, but so happened to use the same intermediate certificate as "Site A", it will have kept a copy of the intermediate (from "Site A"), so will also be ok from that point on.