

Sales: 01622 766766 Log In Search:

[Products](#)[SSL](#)[Enterprise](#)[Partners](#)[About Us](#)[Contact Us](#)[Resources](#)[Support](#)

SSL Certificates

A brief explanation

[Home](#) [SSL Information Centre](#) [What is an SSL Certificate?](#)

What is an SSL Certificate?

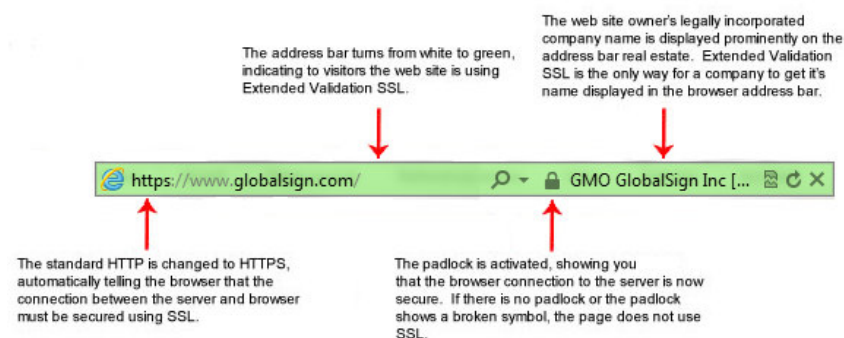
SSL Certificates are small data files that digitally bind a cryptographic key to an organisation's details. When installed on a web server, it activates the padlock and the https protocol (over port 443) and allows secure connections from a web server to a browser. Typically, SSL is used to secure credit card transactions, data transfer and logins, and more recently is becoming the norm when securing browsing of social media sites. SSL Certificates bind together:

A domain name, server name or hostname

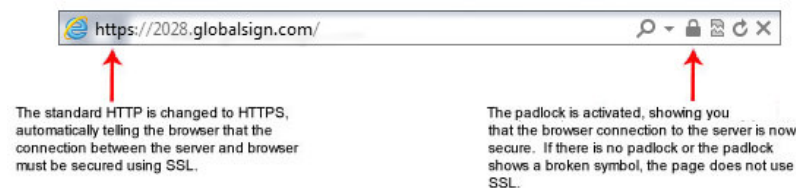
An organisational identity (i.e. company name) and location

An organisation needs to install the SSL Certificate onto its web server to initiate secure sessions with browsers. Depending on the type of SSL Certificate applied for, the organisation will need to go through differing levels of vetting. Once installed, it is possible to connect to the website over <https://www.domain.com>, as this tells the server to establish a secure connection with the browser. Once a secure connection is established, all web traffic between the web server and the web browser will be secure. Browsers tell visitors a website is SSL secure via several visible trust indicators:

Extended Validation (EV) SSL Certificates (such as [GlobalSign ExtendedSSL](#)):



Standard SSL Certificates (such as [GlobalSign DomainSSL](#) and [OrganizationSSL](#)) display:



To view the details of an SSL Certificate, go to a secure site, click on the padlock and select "View Certificate". All browsers are slightly different, but the certificate always contains the same information.

SSL Information Centre

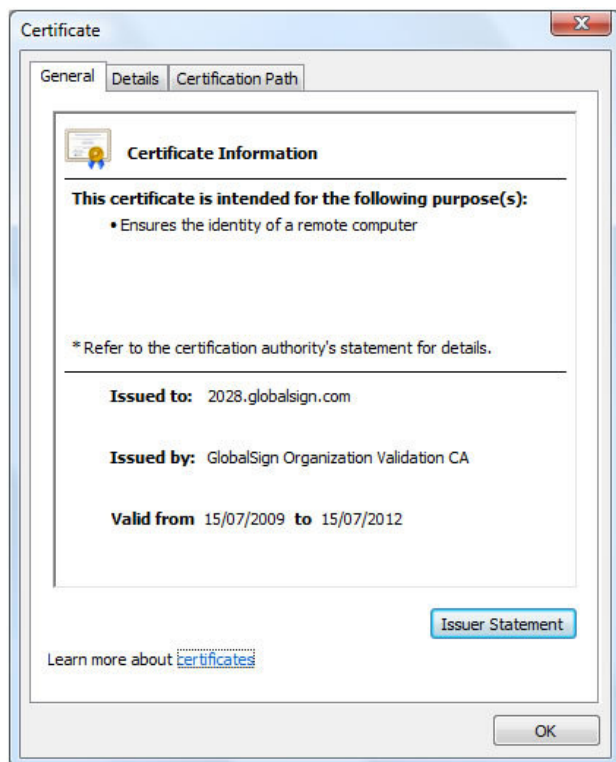
[What is SSL?](#)[What is an SSL Certificate?](#)[Certificate Authority Root](#)[What are the types of SSL?](#)[Using a Secure Site Seal](#)[What is SGC?](#)[CA Network Security Practices](#)[What is EV SSL?](#)[Telling DV & OV Apart](#)[Choosing Safe Key Sizes](#)[Security and website performance](#)

Contact a Solutions Specialist to discuss your needs
[Contact Us](#)

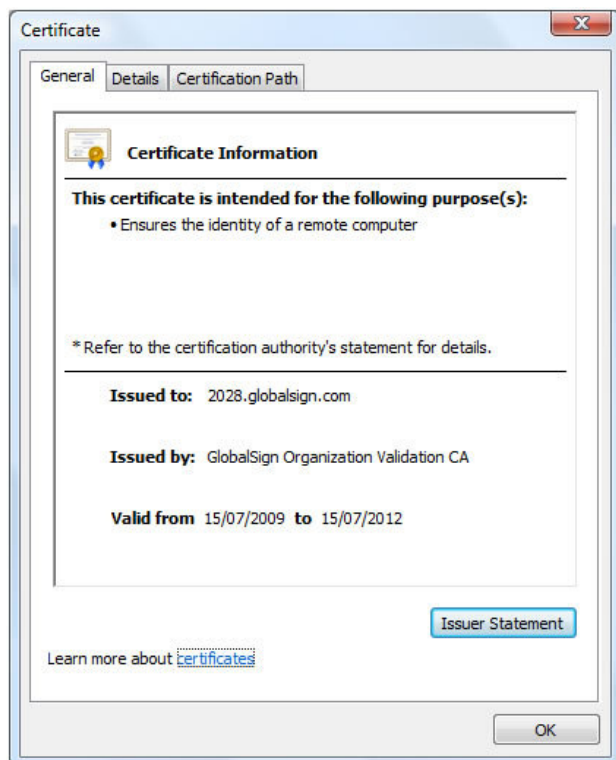


We use cookies to improve the quality of this site. [Read our cookie policy here](#), or simply click "Accept Cookies & Continue".

[Accept Cookies & Continue](#)



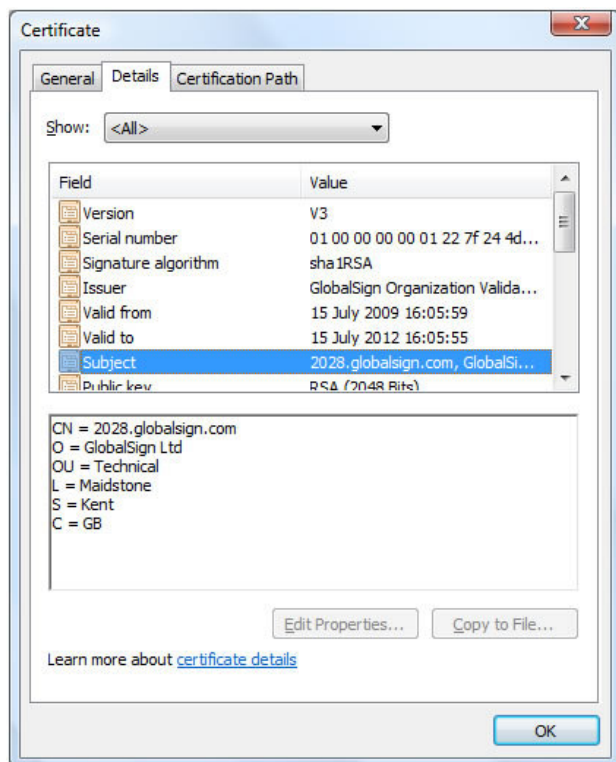
To view the actual contents of the certificate click the "Details" tab:



Click the "Certification Path" tab to see which Trusted Root Certificate has been used to issue the SSL Certificate:

We use cookies to improve the quality of this site. [Read our cookie policy here](#), or simply click "Accept Cookies & Continue".

[Accept Cookies & Continue](#)



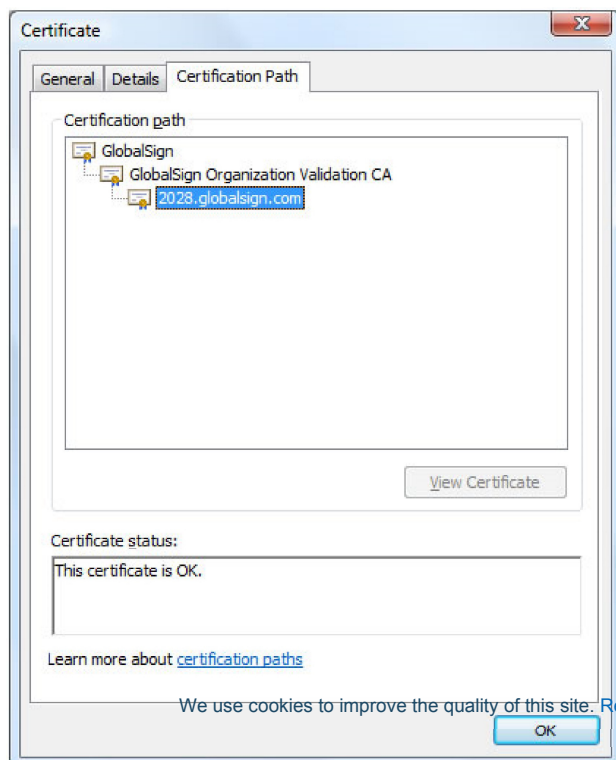
Why is the Root Certificate important?

SSL Certificates need to be issued from a trusted Certification Authority's Root Certificate, and preferably by a 2048 bit Certificate that's widely distributed. The Root Certificate must be present on the end user's machine in order for the Certificate to be trusted. If it is not trusted the browser will present untrusted error messages to the end user. In the case of e-commerce, such error messages result in immediate lack of confidence in the website and organisations risk losing confidence and business from the majority of consumers.

Companies like GlobalSign are known as trusted Certification Authorities. This is because browser and operating system vendors such as Microsoft, Mozilla, Opera, Blackberry, Java, etc., trust that GlobalSign is a legitimate Certification Authority and that it can be relied on to issue trustworthy SSL Certificates. The more applications, devices and browsers the Certification Authority embeds its Root into, the better "recognition" the SSL Certificate can provide.

GlobalSign has, for over 15 years, been operating the GlobalSign Ready program for Root Certificate embedding. This program ensures its in-house engineers from America, Europe and Asia are in constant communication with the application, device and browser vendors to ensure the GlobalSign Root Certificate is present everywhere that may be used for SSL sessions.

Read more about [GlobalSign Root Certificate compatibility](#) and how it benefits your website security



The GlobalSign Root Certificate is marked for a number of intended purposes. This makes it a very strong and flexible Root Certificate able to perform all Public Key Infrastructure (PKI) related activities:

- Ensures the identity of a remote computer**
- Proves your identity to a remote computer**
- Ensures software came from software publisher**
- Protects software from alteration after publication**
- Protects e-mail messages**
- Allows data to be signed with the current time**
- Allows data on disk to be encrypted**
- Allows secure communication on the Internet**
- Permits all key usage policies**
- OCSP Signing**

GlobalSign provides PKI applications, products and services for all the above security functions. Should your organisation have a specific PKI rollout or project, do not hesitate to contact us.



GMO GlobalSign is one of the longest established Certificate Authorities (CA) and leaders in Cloud PKI identity credentialing and automated SSL Certificate management. GlobalSign x.509 Digital Certificates are trusted by all browsers and mobile devices and include: Multi-Domain & Extended Validation SSL, Code Signing, Adobe PDF Signing, Microsoft Office Digital Signatures, S/MIME Secure Email, Strong Authentication for networks and mobile access, and root signing for enterprise Certificate Authorities.

[Contact GlobalSign](#) | [News](#) | [GlobalSign Blogs](#) | [Resources](#) | [Legal Repository](#) | [Site Map](#) | © 2013 GlobalSign



[Get a GlobalSign Site Seal](#)

We use cookies to improve the quality of this site. [Read our cookie policy here](#), or simply click "Accept Cookies & Continue".

[Accept Cookies & Continue](#)