Basics of SSL Certification

Introduction

To secure transmission of information from browser to a web server, a security protocol is used. SSL (Secure Socket Lock) is one of the most popular and widely accepted security protocols, which secures the connection between web browser and a web server. Deciding upon which SSL Certificate will meet your business requirements and using it could be a challenging task.

In this white paper, we have thrown light on the basic features and benefits of SSL. We have also informed in brief about each type of SSL and when it should be used. After going through this piece of information, you will rest assured that SSL is not as complicated as it is thought to be and with ZNetLive's services; it's rather simple to use.

What is SSL?

SSL (Secure Socket Layer) along with TLS (Transport Layer Security) is the most popular and widely accepted security protocol. One of the reasons why SSL is widely accepted is because it is uncomplicated for the end users. It enables the information to pass through a secure channel between two machines that are exchanging data on an unsecure network such as internet or internal network.

In technical terms, SSL is a transparent protocol (set of rules) which does not require the involvement of end users in order to establish a secure session. A padlock or a green bar with padlock on the address bar of a website is displayed to make end users aware of the presence of SSL on it. Websites are written in HTTP

format which is vulnerable to snooping and sensitive information such as credit card details, online banking passwords etc. can be easily taken from there to exploit.

The growing demand of SSL is attributed to the increase in online shopping trend and advancement of several other web applications and web services that need browser based security.

The global growth rate in the number of active SSL Certificates is 25% per year, but strangely, less than 2% of the total websites worldwide use this security measure, whereas a large number of websites still lack an SSL Certificate.

What is an SSL Certificate?

SSL (Secure Socket Layer) is a security protocol, or in simple terms, it is a set of rules that are required to maintain security during data transmission on the internet. The SSL Certificate is required to use and access that set of protocol. The SSL certificates are small data files that digitally bind a cryptographic key to the corporate details of an organization such as domain name, server or host name, company

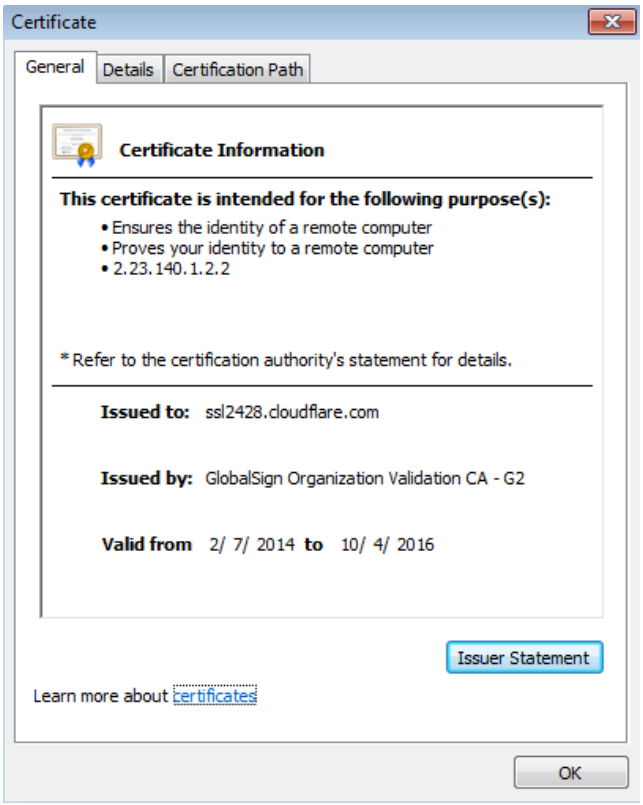
Basics of SSL Certification

name, its location and other relevant details. SSL Certificates can only be issued by few Certificate Authorities and ZNetLive's SSL Certificates are authorized by GlobalSign.

https://manage.znetlive.com/admin/hrmsaddon.php
In order to establish a SSL session on the browsers, organizations are required to install SSL Certificates on their web servers. The SSL Certificates offer various levels of security for which organizations are vetted differently by CAs (Certification Authority).

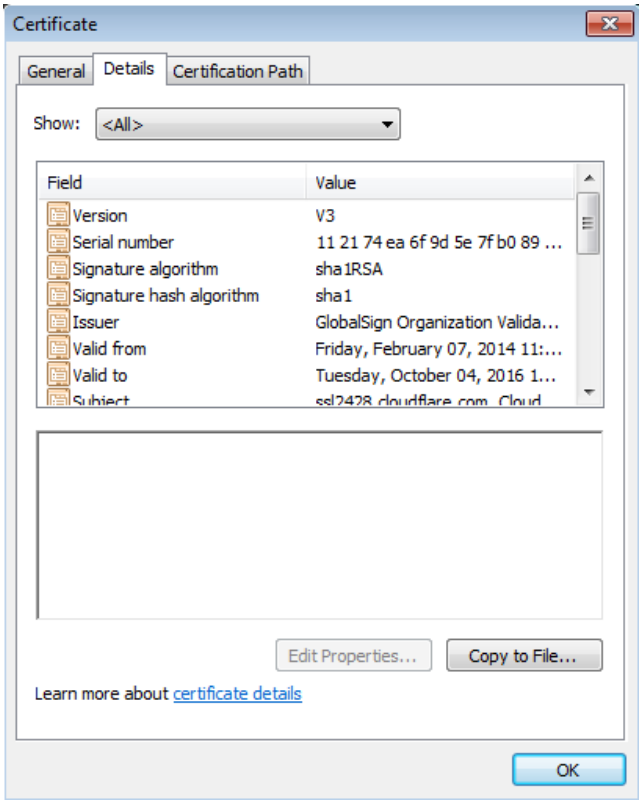
After a Certificate is installed on the web server, the website is connected with it using a HTTPS connection which instructs the server to establish a secure connection with the browser. A secure connection between the web server and the web browser creates a secure channel for all the web traffic between them.

An SSL certificate can be viewed on the website by clicking on the padlock and selecting view certificate. Different browsers display the certificate differently, but the information is same everywhere.

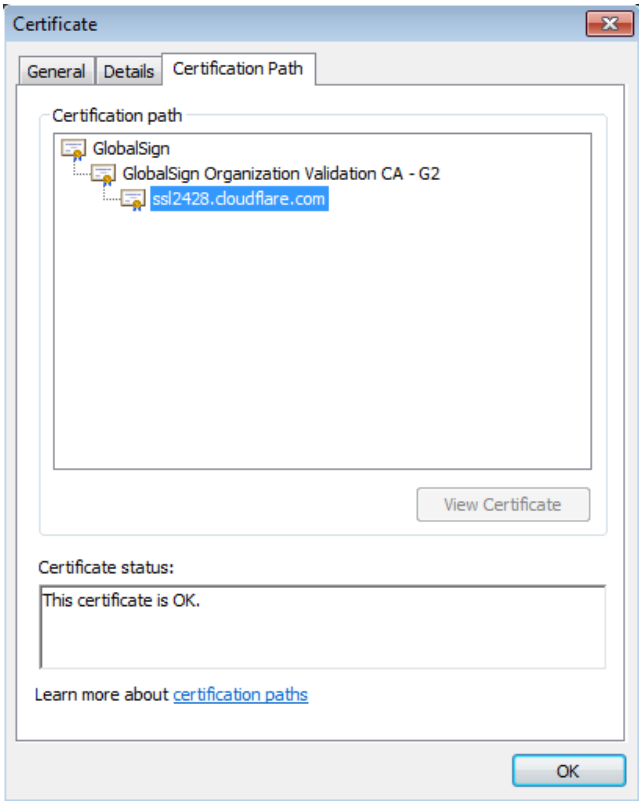


Basics of SSL Certification

Actual content of the certificate can be viewed by clicking on the Details tab:



The Certification path shows which Trusted Root Certificate belonging to which Certificate Authority has been used to issue the SSL Certificate:



When should SSL be used?

SSL Certificate should be implemented whenever a website requires personal and sensitive information to be entered on the internet or any internal network. Personal information can

Basics of SSL Certification

include filling forms online or logging into accounts for that matter.
It is a common perception that SSL Certificates should be used only for securing payment pages and credit card transactions, whereas basically all the websites on which exchange of personal information takes place should have an SSL certificate in order to encrypt the information filled in by the user. SSL should be the minimum security standard used by a website while collecting/submitting the data.

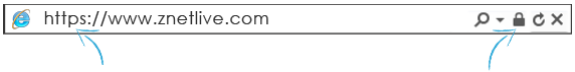
The following situations require SSL certificate on a website.

- To secure online transaction done using a credit card.
- To secure login details and other activities of hosting control panels such as Parallels etc.
- To secure login information and other sensitive data filled by the users.
- To secure Outlook Web Access, Exchange and Office and other webmail and applications.
- To secure the file transfer over HTTPS and FTP(s) services, like when a large file is transferred.
- To secure cloud based computing platforms or workflow and virtualization applications.
- To secure the connection between an email client and an email server, for example Microsoft Outlook and Microsoft Exchange.
- To secure intranet traffic like internal networks, sharing files, data base connections and so on.
- To provide security to the network logins and other network traffic with SSL VPNs like VPN Access Servers or applications such as Citrix Access Gateway. The products and technology provided by ZNetLive to secure these applications are discussed below.

Types of SSL Certificates

Domain Validated (DV) SSL

Before issuing the Domain SSL certificate, the right of an applicant to use the domain name is verified by the Certification Authority (CA). The vetting is done simply via an email challenge. The CA does not verify any other detail about the company and thus it is not displayed in SSL certificate on the website. The Domain SSL does not require any detailed vetting which makes its issuance time fast and is issued within minutes.



The standard HTTP is changed to HTTPS, automatically telling the browser that the connection between the server and browser must be secured using SSL.

The padlock is activated, showing you that the browser connection to the server is now secure. If there is no padlock or the padlock shows a broken symbol, the page does not use SSL.

Basics of SSL Certification

When should DV SSL be used?

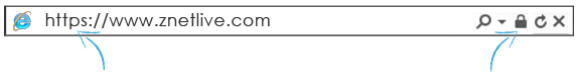
In case when only the basic encryption is required, like for internal and lower profile public sites or when the applicant is not a legally incorporated entity or applicants who want the certificate quickly, Domain SSL is suitable. It can also be used when company documents are not

available for vetting and when Managed or VPS hosting is needed.

Organization Validated (OV) SSL

When an applicant applies for an Organization Validated SSL certificate, the Certificate Authority validates his right to use that domain name as well as the existence of that organization. The visitors are able to view this authorized company information by viewing the certificate details. This way a website is able to generate trust amongst its visitors by providing them with validated information about the organization whose website they are visiting.

As compared to Domain SSL, obtaining an OV SSL takes time because it requires vetting of the organization.



The standard HTTP is changed to HTTPS, automatically telling the browser that the connection between the server and browser must be secured using SSL.

The padlock is activated, showing you that the browser connection to the server is now secure. If there is no padlock or the padlock shows a broken symbol, the page does not use SSL.

When should OV SSL be used?

When a website requires identity assurance and requires higher trust as encryption, and the applicants can wait for 2 business days to obtain the certificate, then OV SSL should be used. Additionally, when subdomains need to be secured with a single SSL certificate and if the customers want to secure Public IP addresses, OV SSL should be preferred. The other reasons remain same as for the Domain Validated SSL Certificate.

Extended Validation (EV) SSL

Extended Validation SSL comes highest in the levels of security provided by the SSL Certificates. Activation of green bar with a padlock on the website makes it the most visually noticeable SSL Certificate amongst all. The customer's trust is boosted as the green bar alternates between organization name and the Certification Authority that issued it.

The Certification Authority (CA) issues the Extended Validation SSL, the most advanced type of SSL to an applicant after conducting a thorough vetting of the organization which also includes checking its right to use the domain name. The EV guidelines define the issuance process of EV SSL. EV guidelines were formally approved by CA/Browser forum in 2007, which laid down all the steps to be followed before a CA can issue an EV SSL. To obtain an EV SSL, an

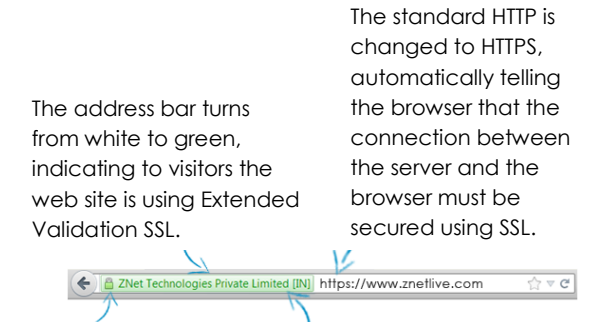
organization is required to verify the following:

- The physical, operational and legal existence of the entity.

Basics of SSL Certification

- Organization's exclusive right to use the domain specified in the EV SSL Certificate.
- The identity of the organization should match official records.
- That the organization has properly approved the issuance of the EV SSL Certificate.

Issuance time of EV SSL is 3-5 business days.



When should EV SSL be used?

Extended Validation SSL provides highest level of security and trust, thus it should be deployed when the highest level of identity assurance and encryption are required, for example incorporated companies and organizations. High profile brands are prone to phishing attack and miscreants may create their lookalike websites, thus they should use EV SSL to forestall it. Also, websites that wish to build trust amongst its customers and assure them of the fact that they care for the customers' data should use EV SSL. This will help in greater conversion from visitors to customers. Presence of EV SSL enhances the image of a website and makes it stand in the league of other big competitors.

ZNetLive Certificate Features:

Amongst myriad of options available, it's difficult to decide which one to go for. We at ZNetLive offer SSL certificates validated by Global Sign that are trusted by all known devices. Our SSL certificates have many features that are otherwise chargeable if taken from other SSL providers. The features of our SSL Certificates are:

- 2048 bit future proof issuing authority.
- SGC Security for minimum 128 bit to 256 bit SSL encryption levels.
- Unlimited server licensing which means that one SSL Certificate can be used on several servers.
- For complex multi domain server configuration, our wildcard SSL and Unified Communications provide simple and cost effective support.
- Secure site seal with every SSL Certificate.

Contact ZNetLive's SSL Specialists
+91-8875002200 ssl@znetlive.com www.znetlive.com/ssl-certificates

Basics of SSL Certification

- Multi-year discounts are available on SSL certificates.
- SSL certificates can be re issued any number of times which contributes towards savings.
- Malware alert service
- Installation health check is provided.
- Universally compatible with all the browsers and mobile phone devices.
- Can secure both www.domain.com and domain.com (without the www).
- Underwritten warranty.

Why choose ZNetLive over other SSL providers?

ZNetLive's SSL Certificates are validated by GlobalSign, a leading entity in public trust service and are trusted by all the major web browsers and devices. By availing ZNetLive's services, customers can have following advantages:

- Easy ordering system and a 24*7 access to customer account.
- Product range is simple but sophisticated.
- Superior customer services.

Contact ZNetLive's SSL Specialists
+91-8875002200 ssl@znetlive.com www.znetlive.com/ssl-certificates