The Basics of SSL Certificates (FAQs)

What are SSL certificates?

SSL certificates provide validated identity and encryption in order to secure websites, users, and data. They initiate secure sessions with the user's browser via the secure sockets layer (SSL) protocol. (SSL certificates are also known as TLS/SSL certificates; TLS stands for transport layer security.)

The secure connection cannot be established without the SSL certificate, which digitally connects company information to a cryptographic key. Any organization that engages in ecommerce must have an SSL certificate on its web server to ensure the safety of customer and company information, as well as the security of financial transactions.

What are Organization Validated (OV) Certificates?

Organization validated (OV) TLS/SSL certificates provide website encryption, identification, and authentication for one domain – securing a web page's visitors' private information during transmission.

What are Extended Validation (EV) Multi-Domain Certificates?

Extended validation (EV) TLS/SSL certificates are created by an industry consortium called the CA/Browser Forum. This category of certificate was conceived in response to the growing threat of phishing attacks. EV certificates are issued to websites only after rigorous validation of their identity. EV certificates require verification of the business organization's operational existence, physical address, and the employment status of the requestor.

Web browsers will reflect this higher level of identity assurance with prominent and distinct trust indicators, such as a green address bar in Internet Explorer and Mozilla Firefox, and advanced green indicators in the latest versions of Opera and Google Chrome.

What are Unified Communications (UC) Multi-Domain Certificates?

UC multi-domain TLS/SSL certificates verify organization identity on a primary domain and three additional domains with one certificate.

Learn more about our certificate solutions at entrust.com

The Basics of SSL Certificates

What are Wildcard Certificates?

Wildcard TLS/SSL certificates secure one domain and an unlimited number of its subdomains across an unlimited number of servers.

What are Private Certificates (Dedicated Certificate Authority)?

Private SSL certificates are ideal for internal use cases where non-fully qualified domain names (FQDNs) aren't required and have the same key sizes and signing algorithms as publicly trusted SSL certificates.

What are Domain Validated (DV) Certificates?

Domain validated (DV) certificates are limited-security certificates that validate domain ownership only. A website secured with a DV certificate offers only a locked padlock in the address bar, but does not show organization details because they have not been validated. DV certificates can be acquired anonymously, and do not tie a domain to a person, place, or entity. For this reason, many websites using DV certificates are linked to fraudulent activity.

Which web browsers are Entrust SSL certificates compatible with?

Entrust SSL certificates are compatible with and trusted by all major browsers. For a list of servers and browsers that have been confirmed to work with our certificates, go to our SSL Certificate Supported Browsers webpage.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223