COMODO
Certification Authority

A-Z Guide in Choosing the Right SSL Certificate

A White Paper from Comodo CA

Introduction to SSL Certificates

A parent preparing a toddler for her first beach vacation and a seasoned kayaker preparing for Zambia's Ghostrider rapid will not reach for the same life jacket. In the world of digital security, the purposes and specs of the various products are also highly relevant to the consumer, although the differences between them may not be so immediately clear. But in both cases, it's important that the customer find the right fit. Whether you're a business owner looking for the right SSL certificate for your own website or a domain provider looking to curate a solid SSL offering for your customers, here's what you should know about TLS/SSL certificates and what to look for when selecting a certificate provider.

SSL certificates apply encryption to websites to protect data, enable safe transactions, and inspire consumer confidence.

What Are TLS/SSL Certificates?

SSL is short for "Secure Sockets Layer," and SSL certificates are used to secure communications between a website, host, or server and the end users that are connecting to it (or between two machines in a client-server relationship). An SSL certificate confirms the identity of the domain name (for example, ComodoCA.com) that is operating the web site, and enables encryption of all information between the server and the visitor to ensure the integrity of all the transmitted information.

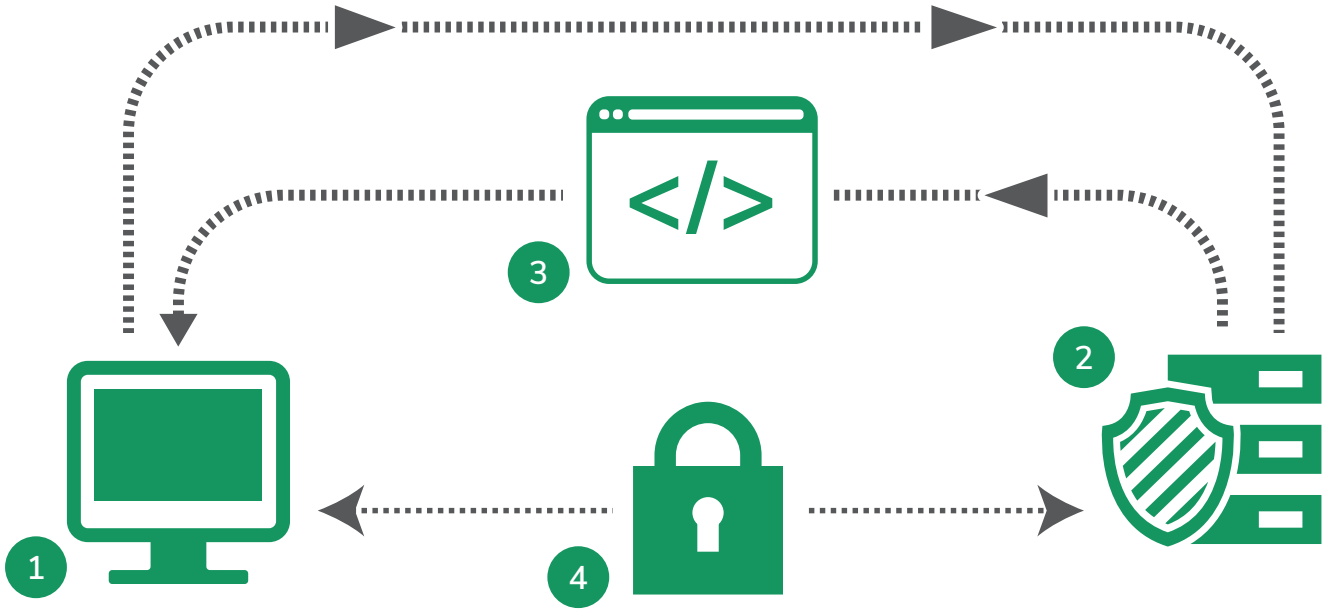
Why Are TLS/SSL Certificates So Important?

Identity theft and browser warnings are growing concerns among consumers. Failure to select the right TLS/SSL certificate for your website can erode customer trust and lower your rate of completed transactions, negatively impacting your bottom line.

©2018 Comodo CA, All Rights Reserved

How Does SSL Encryption Work?

Encryption makes use of keys to lock and unlock your information, meaning you need the right key to “open,” or decode, secured information. Each SSL certificate comes with two keys; A public key, which is used to encrypt (scramble) the information and a private key, which is used to decrypt (un-scramble) the information and restore it to its original format to make it readable. For the average user the process is seamless but here is how it works in the background:



1 User accesses a site with an SSL certificate installed

2 A secure SSL connection is requested from the website host

3 Host responds with the valid SSL certificate

4 A secure connection is established between the browser and host enabling the transfer of encrypted data

©2018 Comodo CA, All Rights Reserved

Where Are SSL Certificates Used?

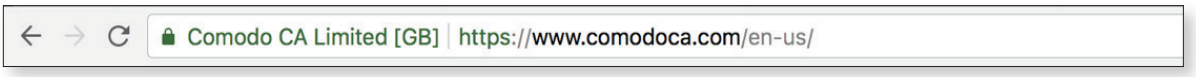
SSL certificates should be used in any instance where information needs to be transmitted securely. This includes:

- Communications between your website and your customers' internet browsers.
- Internal communications on your corporate intranet.
- Email communications sent to and from your network (or private email address).
- Information between internal and external servers.
- Information sent and received from IoT and mobile devices.

Online consumers are demanding assurance that the identity of the website they are visiting has been verified by authentication procedures.

How to Determine If a Site Has a Valid SSL Certificate

A website without an SSL certificate displays "http:// " before the website address in the browser address bar. This moniker stands for "Hypertext Transfer Protocol," the conventional way to transmit information over the Internet. Most internet users are aware that this indicates a website is not secure and historically have looked for https:// and a closed padlock symbol in their browser window to confirm that they are on the site of an authenticated organization:



However, it's no longer sufficient for business websites to simply enable HTTPS and display the standard padlock symbol to their visitors. Online consumers are demanding assurance that the identity of the website they are visiting has been verified by authentication procedures that are proven to be highly trustworthy. And this assurance is provided in the form of an Extended Validation (EV) SSL certificate. EV certificates display a hard-to-miss green identifier in the URL bar and indicate to the visitor that the website was subjected to extensive scrutiny by the issuing Certificate Authority. The consumer can be confident that they are at a legitimate website, not a phishing website.

That's not to say an EV certificate is necessary in every situation. But they can generate a higher level of consumer trust than other options, such Organization Validation (OV) certificates, or Domain Validation (DV) certificates, which undergo far less scrutiny.

©2018 Comodo CA, All Rights Reserved

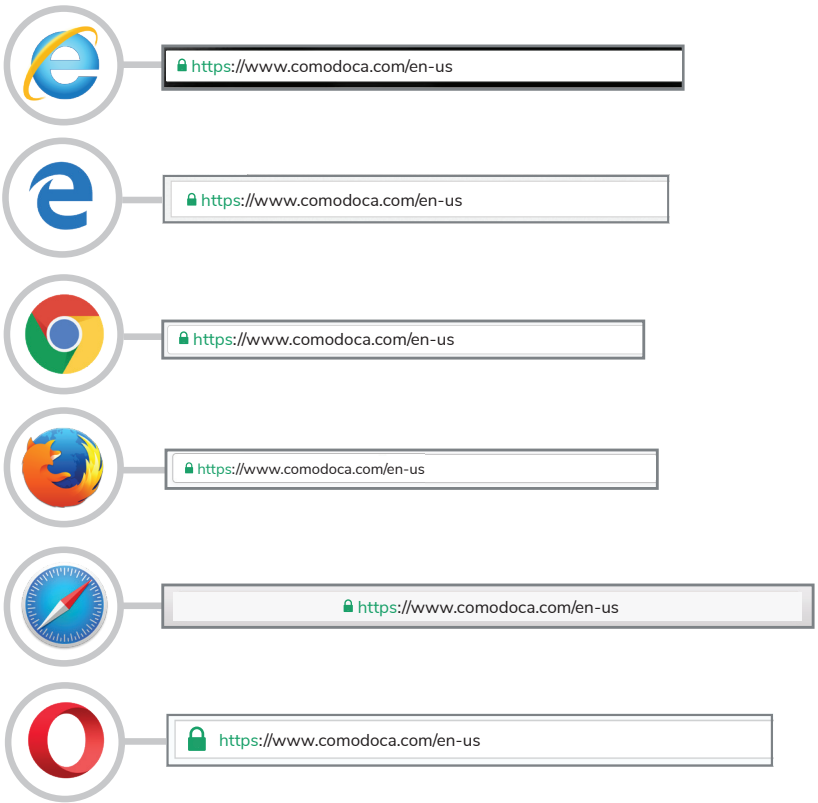
How to Choose Between an EV, OV, or DV Certificate

Domain Validation (DV) SSL Certificates

DV certificates are best for small to medium-sized businesses seeking cost-effective security with no need to establish site visitor trust. Issuance of a DV certificate only requires proof of ownership of the associated domain name, which is provided through a simple email validation process. These certificates can be issued in minutes, enable HTTPS, and display a clear indicator, such as the padlock symbol, in internet browsers.

However, DV certificates do not vet the legitimacy of the organization the website represents and should therefore not be used for e-commerce sites or sites that deal in sensitive information. They are however, a great option for many internal sites, test servers, and test domains.

DV Certificate Security Indicators



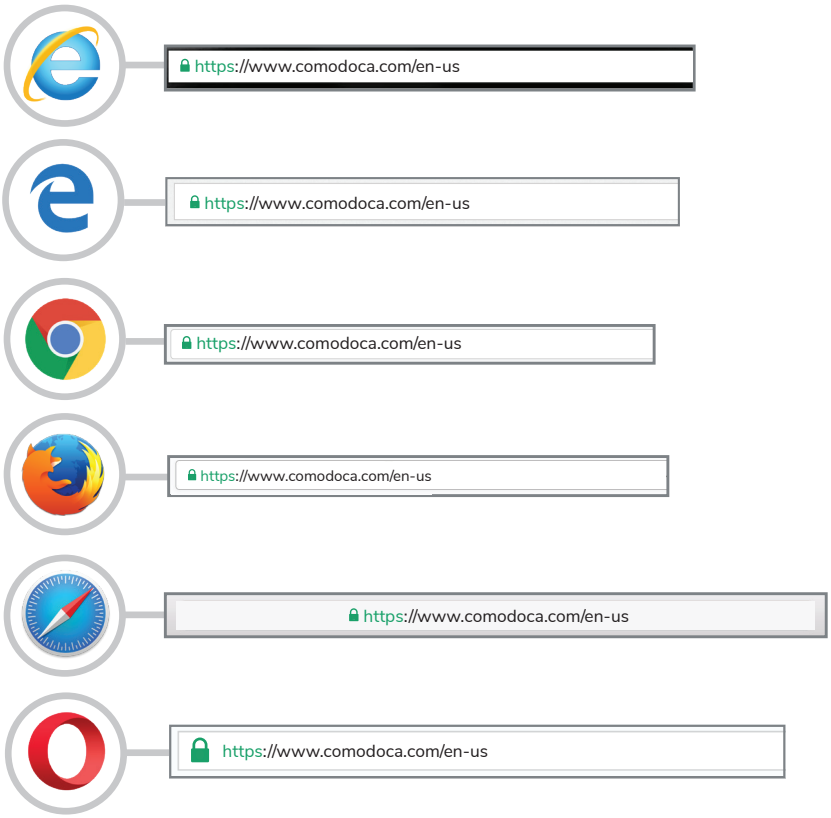
1. **Activates HTTPS**
2. **Displays the symbol**
3. **Enables dynamic site seals**

©2018 Comodo CA, All Rights Reserved

Organization Validation (OV) SSL Certificates

OV certificates provide the same level of protection as DV certificates but go one step further than simply requiring proof of domain ownership. With an OV certificate, the issuing Certificate Authority confirms the business associated with the domain name is registered and legitimate by checking details such as the business name, location, address, and incorporation or registration information. This makes the OV certificate a more suitable option for public-facing websites that represent companies or organizations.

OV Certificate Security Indicators



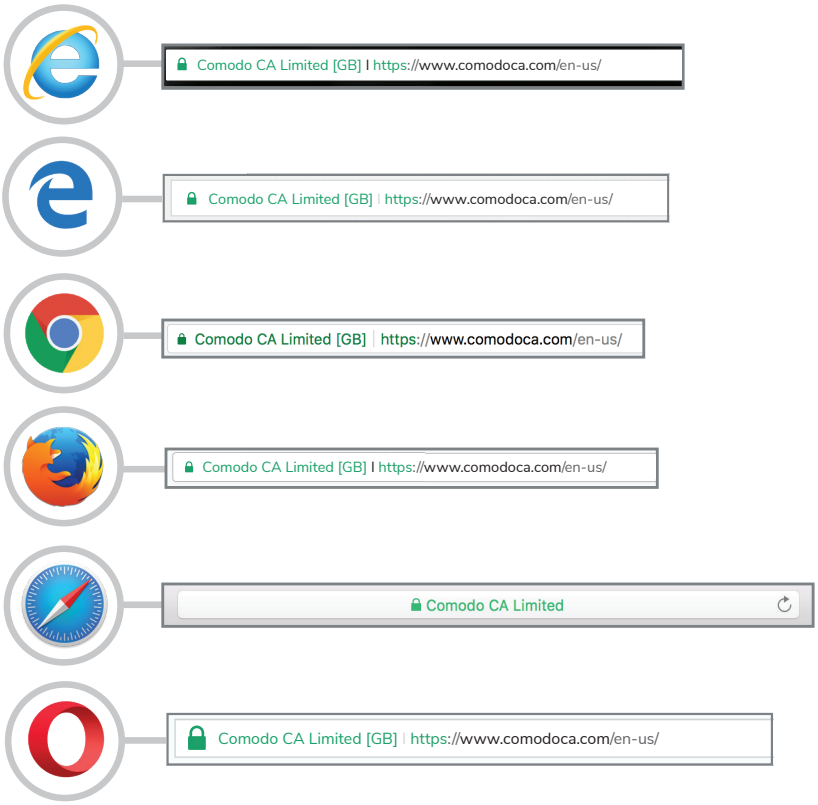
1. **Activates HTTPS**
2. **Displays the symbol**
3. **Enables dynamic site seals**

©2018 Comodo CA, All Rights Reserved

Extended Validation (EV) SSL Certificates

EV certificates provide the highest level of trust by assuring consumers that they are conducting business through a trusted website. For this reason, these certificates have become the industry standard for ecommerce websites. EV SSL certificates trigger high-security web browsers to display a green address bar that includes the name of the company or organization that owns the domain. They also show the name of the issuing Certificate Authority:

EV Certificate Security Indicators



1. **Activates HTTPS**
2. **Displays the symbol**
3. **Company name in browser**
4. **Enables dynamic site seals**

Confirmation of the website's identity, and validation of the organization, is carried out according to the rigorous industry guidelines established by the CA/Browser Forum and involves a strict vetting process that is shown to be effective over the course of more than ten years of real-world use.

EV SSL certificates are essential for large businesses or e-commerce sites as they can enhance credibility by showing discerning consumers that a prospective transaction is with a legitimate recipient and that the site is serious about protecting the data of its customers.

©2018 Comodo CA, All Rights Reserved

What You Should Look for in Choosing a Certificate Authority (CA)

As the world's largest commercial Certificate Authority, Comodo CA is proactively monitoring for potential threats and attacks, working hand-in-hand with government agencies, browser providers, and our customers, to ensure it is keeping up with the ever changing market.

When evaluating a CA, be sure that it:

1. Follows CA/B Forum Baseline Requirements.

This industry group consisting of Certificate Authorities and browser manufacturers developed standards that each CA must meet for its roots to remain trusted in browsers. These include:

- All information contained within the certificate must be validated to be true through a strict, clearly defined authentication process.
- Certificates must meet specific minimum levels of cryptographic strength to protect the integrity of the certificate and private key from evolving threats.
- Certificates must not exceed maximum specified durations.
- CAs must follow guidelines for CA security, certificate revocation mechanisms, audit requirements, liability, privacy and confidentiality, and delegation of authority.

2. Conducts Annual Audits – Both WebTrust and SOC 3

Annual audits are crucial to CA security, yet not every CA makes them a priority. At a minimum, your CA should meet these auditing standards.

3. Maintain membership in the WebTrust program for CAs

The WebTrust for Certification Authorities program was developed to increase consumer confidence in the Internet as a vehicle for conducting e-commerce and to increase consumer confidence in the application of PKI technology. Comodo CA, for example, undergoes an annual audit from Ernst & Young, which validates that:

- The Certification Authority (CA) discloses its SSL certificate practices and procedures and its commitment to provide SSL certificates in conformity with the applicable CA/Browser Forum Requirements.

Trust is everything in the world of online business. Investment in technology to protect customers and earn their trust is a critical success factor for any company that does business online or hosts an e-commerce website.

©2018 Comodo CA, All Rights Reserved

- Subscriber information was properly collected, authenticated, and verified.
- The integrity of keys and certificates is established and protected throughout their life cycles.
- Logical and physical access to CA systems and data is restricted to authorized individuals.
- The continuity of key and certificate management operations is maintained.
- CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity.
- The Certification Authority maintains effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum.

Comodo CA has maintained effective controls over its system as it relates to these core principles: security availability, processing integrity, and confidentiality.

4. Submit to publish an annual Service Organization Control

The SOC3 report is published to confirm that the security controls for this cloud service have been examined by an independent accountant. Again as an example, Comodo CA undergoes an annual audit from Ernst and Young to validate that Comodo CA has maintained effective controls over its system as it relates to four core principles: security availability, processing integrity, and confidentiality.

To sum it up...

Trust is everything in the world of online business. Investment in technology to protect customers and earn their trust is a critical success factor for any company that does business online or hosts an e-commerce website. The effective implementation of TLS/SSL certificates is a proven tool to help establish customer trust.

Want to learn more? Visit www.ComodoCA.com

COMODO
Certification Authority

©2018 Comodo CA, All Rights Reserved