Why HTTPS Is Important for Websites

If you are requesting your visitors to provide sensitive information on your website:

- In case of login pages
- subscribing to newsletters or submitting orders
- In case of Facebook applications, since Facebook only accepts content from secure web sites.
- If the website contains a datasheet where we request personal information from the visitor
  Google Chrome and Mozilla Firefox browsers alert visitors if the connection does not have an SSL certificate.
  For websites without HTTPS, an unsafe label will appear in the browser's title bar. Because of this, fewer people will click through Google's search results page.
- Credit card payments
  If you want to use such a service, then you must have and use theOrganization validated SSL (OV SSL).
- To improve search engine optimization
  Nowdays, search engines are treating emphasized in ranking when a website has SSL certification.

we recommend that you send the requested information through the server encrypted protocol. The SSL certificate ensures that an unauthorized person can not listen to communications on a web site. The SSL certificate, which is used to secure web pages, is http: instead of https: prefix, so many people rely on SSL as "HTTPS". If that site is accessible via https, a small green pad will usually appear in the browser to indicate to your visitors that the data will be transmitted via a secure encrypted attachment to your server.

WHAT IS A CERTIFICATE AUTHORITY?

CA is the abbreviation of the Certificate Authority. The certificate issuer is an organization that issues digital (SSL and TLS) certificates.

The digital certificate consists of two parts, a public key and a secret key. The certificate can be used to verify ownership of the public key as per the data provided during the purchase of the certificate.

The organization issuing the certificate authenticates the data provided during the purchase of the certificate.

SSL certificates are issued by certification issuing organizations.

Example:

- Netlock Kft.
- GlobalSign
- Symantec
- Comodo

SSL CERTIFICATE TYPES

Domain Validated SSL (DV SSL)

It only protects the specified domain name, before the issue, only the existence and ownership of the domain name checked. The organization or company behind the domain name will not be checked. It is possible to apply for a so-called Wildcard certificate for several subdomains.

Organization Validation SSL (OV SSL)

In this certificate type, the details of the domain name owner are also checked. It is possible to apply for a so-called Wildcard certificate for several subdomains.

Extended Validation SSL (EV SSL)

For this type of certificates, the certificate also displays the name of the certified organization. Before the issue, the domain name, the owner’s details, and the contact details of the organization are also verified. For extended certified certificates, it is not possible to issue multiple subdomains with one certificate.

Revision #2
Created 2023-10-19 13:35:53 CEST by DotRoll Knowledge Base
Updated 2026-05-14 14:10:13 CEST by DotRoll Knowledge Base