Workshapes

The SSL Certificate (Secure Sockets Layer)

An SSL (Secure Sockets Layer) certificate and its successor TLS (Transport Layer Security), are standard protocols that protect Internet communications; that is, they ensure that sensitive information provided by users on the web (such as passwords, personal data and credit card numbers) remain confidential and are not in any way intercepted by third parties; this happens thanks to an encrypted communication between the client server and the web server.

What happens specifically? When the first communication between client server and web server occurs, the latter sends its digital certificate to the browser that verifies its validity and if everything is ok it starts a secure connection between client and web server.

When we navigate with a connection that is based on SSL protocols we already understand it from the address on the navigation bar, where we will see a padlock and instead of http: // we will find https: // just to specify that we are making a secure connection that uses of SSL or TLS certificates.

The guarantee given to users by the SSL protocols on the authentication of the domain of the site to which it is connected and on the real identity of the company connected to that domain, protects them from fraud and theft, which is particularly important when dealing with sites and -commerce and for all those sites that provide online services that include the exchange of sensitive and private information, which raises many concerns for web users who need a site that guarantees their maximum reliability instead.

SSL certificates are issued by a Certification Authority (CA).