

□ What a SSL certificate is!

The SSL certificate Secure Socket Layer is a file which is settled down on an Internet server. This certificate has for purpose **to secure the sending of some (or of all) the data of the server** . This security is made by a more or less important encoding, but generally, for web sites, the level of encoding is 128 bits, what insures a level of confidentiality and a difficulty to break the certificate rather important. This certificate does not insure against the interception of the coded data, but insures an effective protection.

The SSL certificate was invented by Netscape in 1994 in association with some companies as MasterCard or the Bank of America. THE IETF bought the certificate from Netscape in 2001.

Four objectives of security are looked for the use of the certificate:

-The **authentication** of the Internet server which passes on the data: needs to assure that it is a site, and not another one, which emits the certificate;

- The **confidentiality** of the passed on and exchanged information;

- The **integrity** of the exchanged data: the certificate must be rather "powerful" to avoid the passed on data to be altered.

-Last optional stage: **the authentication of the customer**: to insure that the data were well passed on by the Internet user who made the request.

[Joomla SEO by AceSEF](#)