

RFC6101 - The Secure Sockets Layer (SSL) Protocol Version 3.0

[return to the IETF Standards](#)

Table 1: Data sheet for The [Secure Sockets Layer \(SSL\)](#) Protocol Version 3.0

Title	The Secure Sockets Layer (SSL) Protocol Version 3.0
Acronym	SSL
Version	3.0
Document Number	RFC6101
Release Date	August 2011
Reference	https://tools.ietf.org/html/rfc6101

Note: The following is an excerpt from the official IETF RFC. It is provided here as a convenience and is not authoritative. Refer to the original document as the authoritative reference.

Introduction

The primary [goal](#) of the SSL protocol is to provide privacy and reliability between two communicating [applications](#). The protocol is composed of two layers. At the lowest level, layered on top of some reliable transport protocol (e.g., TCP [RFC0793](#)), is the SSL record protocol. The SSL record protocol is used for encapsulation of various higher level protocols. One such encapsulated protocol, the SSL handshake protocol, allows the server and [client](#) to authenticate each other and to negotiate an [encryption](#) algorithm and cryptographic [keys](#) before the application protocol transmits or receives its first byte of data. One advantage of SSL is that it is application protocol independent. A higher level protocol can layer on top of the SSL protocol transparently. The SSL protocol provides connection [security](#) that has three basic properties:

- The connection is private. Encryption is used after an initial handshake to define a secret key. Symmetric [cryptography](#) is used for data encryption (e.g., DES, 3DES, RC4).
- The peer's identity can be authenticated using asymmetric, or [public key](#), cryptography (e.g., RSA, DSS).
- The connection is reliable. Message transport includes a message integrity check using a keyed Message [Authentication](#) Code (MAC) [RFC2104]. Secure hash functions (e.g., SHA, MD5) are used for MAC computations.

Last
update:
2021/08/17 13:12 dido:public:ra:xapend:xapend.b_stds:tech:ietf:ssl https://omgwiki.org/dido/doku.php?id=dido:public:ra:xapend:xapend.b_stds:tech:ietf:ssl&rev=1629220375

From:
<https://omgwiki.org/dido/> - **DIDO Wiki**

Permanent link:
https://omgwiki.org/dido/doku.php?id=dido:public:ra:xapend:xapend.b_stds:tech:ietf:ssl&rev=1629220375



Last update: **2021/08/17 13:12**