RFC2246 - The TLS Protocol

return to the IETF Standards

Table 1: Data sheet for The TLS Protocol (TLS)

Title	TThe TLS Protocol
Acronym	TLS
Version	1.0
Document Number	RFC2246
Release Date	January 1999
Reference	https://tools.ietf.org/html/rfc2246

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 TLS Protocol is to provide privacy and data integrity between two communicating applications. The protocol is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol. At the lowest level, layered on top of some reliable transport protocol (e.g., TCP[TCP]), is the TLS Record Protocol. The TLS Record Protocol provides connection security that has two basic properties:

- *The connection is private. Symmetric cryptography is used for data encryption (e.g., DES DES , RC4 RC4, etc.) The keys for this symmetric encryption are generated uniquely for each connection and are based on a secret negotiated by another protocol (such as the TLS Handshake Protocol). The Record Protocol can also be used without encryption.*
- *The connection is reliable. Message transport includes a message integrity check using a keyed MAC. Secure hash functions (e.g., SHA, MD5, etc.) are used for MAC computations. The Record Protocol can operate without a MAC, but is generally only used in this mode while another protocol is using the Record Protocol as a transport for negotiating security parameters.*

The TLS Record Protocol is used for encapsulation of various higher level protocols. One such encapsulated protocol, the TLS 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. The TLS Handshake Protocol provides connection security that has three basic properties:

- *The peer's identity can be authenticated using asymmetric, or public key, cryptography (e.g., RSA RSA, DSS DSS, etc.). This authentication can be made optional, but is generally required for at least one of the peers.*

- *The negotiation of a shared secret is secure: the negotiated secret is unavailable to eavesdroppers, and for any authenticated connection the secret cannot be obtained, even by an attacker who can place himself in the middle of the connection.*
- *The negotiation is reliable: no attacker can modify the negotiation communication without being detected by the parties to the communication.*

One advantage of TLS is that it is application protocol independent. Higher level protocols can layer on top of the TLS Protocol transparently. The TLS standard, however, does not specify how protocols add security with TLS; the decisions on how to initiate TLS handshaking and how to interpret the authentication certificates exchanged are left up to the judgment of the designers and implementors of protocols which run on top of TLS.

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

Permanent link:
https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:xapend:xapend.b_stds:tech:ietf:tls&rev=1605252045

Last update: **2020/11/13 02:20**