

A new Request for Comments is now available in online RFC libraries.

[RFC 3546](#)

Title: Transport Layer Security (TLS) Extensions
Author(s): S. Blake-Wilson, M. Nystrom, D. Hopwood,
J. Mikkelsen, T. Wright
Status: Standards Track
Date: June 2003
Mailbox: sblakewilson@bcisse.com, magnus@rsasecurity.com,
david.hopwood@zetnet.co.uk,
janm@transactionware.com,
timothy.wright@vf.vodafone.co.uk
Pages: 29
Characters: 63437
Obsoletes: 2246

I-D Tag: [draft-ietf-tls-extensions-06.txt](#)

URL: <ftp://ftp.rfc-editor.org/in-notes/rfc3546.txt>

This document describes extensions that may be used to add functionality to Transport Layer Security (TLS). It provides both generic extension mechanisms for the TLS handshake client and server hellos, and specific extensions using these generic mechanisms.

The extensions may be used by TLS clients and servers. The extensions are backwards compatible - communication is possible between TLS 1.0 clients that support the extensions and TLS 1.0 servers that do not support the extensions, and vice versa.

This document is a product of the Transport Layer Security Working Group of the IETF.

This is now a Proposed Standard Protocol.

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

This announcement is sent to the IETF list and the RFC-DIST list. Requests to be added to or deleted from the IETF distribution list should be sent to IETF-REQUEST@IETF.ORG. Requests to be added to or deleted from the RFC-DIST distribution list should be sent to RFC-DIST-REQUEST@RFC-EDITOR.ORG.

Details on obtaining RFCs via FTP or EMAIL may be obtained by sending an EMAIL message to `rfc-info@RFC-EDITOR.ORG` with the message body `help: ways_to_get_rfcs`. For example:

To: `rfc-info@RFC-EDITOR.ORG`
Subject: `getting rfcs`

`help: ways_to_get_rfcs`

Requests for special distribution should be addressed to either the author of the RFC in question, or to `RFC-Manager@RFC-EDITOR.ORG`. Unless specifically noted otherwise on the RFC itself, all RFCs are for unlimited distribution.

Submissions for Requests for Comments should be sent to `RFC-EDITOR@RFC-EDITOR.ORG`. Please consult [RFC 2223](#), Instructions to RFC Authors, for further information.