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

RFC 3268

Title: Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)
Author(s): P. Chown
Status: Standards Track
Date: June 2002
Mailbox: pc@skygate.co.uk
Pages: 6
Characters: 13530
Updates/Obsoletes/SeeAlso: None

I-D Tag: draft-ietf-tls-ciphersuite-06.txt

URL: ftp://ftp.rfc-editor.org/in-notes/rfc3268.txt

This document proposes several new ciphersuites. At present, the symmetric ciphers supported by Transport Layer Security (TLS) are RC2, RC4, International Data Encryption Algorithm (IDEA), Data Encryption Standard (DES), and triple DES. The protocol would be enhanced by the addition of Advanced Encryption Standard (AES) ciphersuites.

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.echo
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.

Joyce K. Reynolds and Sandy Ginoza
USC/Information Sciences Institute