

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

[RFC 3610](#)

Title: Counter with CBC-MAC (CCM)
Author(s): D. Whiting, R. Housley, N. Ferguson
Status: Informational
Date: September 2003
Mailbox: dwhiting@hifn.com, housley@vigilsec.com,
niels@macfergus.com
Pages: 26
Characters: 64509
Updates/Obsoletes/SeeAlso: None

I-D Tag: [draft-housley-ccm-mode-02.txt](#)

URL: <ftp://ftp.rfc-editor.org/in-notes/rfc3610.txt>

Counter with CBC-MAC (CCM) is a generic authenticated encryption block cipher mode. CCM is defined for use with 128-bit block ciphers, such as the Advanced Encryption Standard (AES).

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. 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.