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

RFC 3537

Title: Wrapping a Hashed Message Authentication Code (HMAC) key with a Triple-Data Encryption Standard (DES) Key or an Advanced Encryption Standard (AES) Key
Author(s): J. Schaad, R. Housley
Status: Standards Track
Date: May 2003
Mailbox: jimsch@exmsft.com, housley@vigilsec.com
Pages: 9
Characters: 16885
Updates/Obsoletes/SeeAlso: None

I-D Tag: draft-ietf-smime-hmac-key-wrap-02.txt

URL: ftp://ftp.rfc-editor.org/in-notes/rfc3537.txt

This document defines two methods for wrapping an HMAC (Hashed Message Authentication Code) key. The first method defined uses a Triple DES (Data Encryption Standard) key to encrypt the HMAC key. The second method defined uses an AES (Advanced Encryption Standard) key to encrypt the HMAC key. One place that such an algorithm is used is for the Authenticated Data type in CMS (Cryptographic Message Syntax).

This document is a product of the S/MIME Mail 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.