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

RFC 3560

Title: Use of the RSAES-OAEP Key Transport Algorithm in Cryptographic Message Syntax (CMS)
Author(s): R. Housley
Status: Standards Track
Date: July 2003
Mailbox: housley@vigilsec.com
Pages: 18
Characters: 37381
Updates/Obsoletes/SeeAlso: None

I-D Tag: draft-ietf-smime-cms-rsaes-oaep-07.txt

URL: ftp://ftp.rfc-editor.org/in-notes/rfc3560.txt

This document describes the conventions for using the RSAES-OAEP key transport algorithm with the Cryptographic Message Syntax (CMS). The CMS specifies the enveloped-data content type, which consists of an encrypted content and encrypted content-encryption keys for one or more recipients. The RSAES-OAEP key transport algorithm can be used to encrypt content-encryption keys for intended recipients.

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.