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

RFC 3211

Title: Password-based Encryption for CMS
Author(s): P. Gutmann
Status: Proposed Standard
Date: December 2001
Mailbox: pgut001@cs.auckland.ac.nz
Pages: 17
Characters: 30527
Updates/Obsoletes/SeeAlso: None

I-D Tag: draft-ietf-smime-password-06.txt

URL: ftp://ftp.rfc-editor.org/in-notes/rfc3211.txt

This document provides a method of encrypting data using user-supplied passwords and, by extension, any form of variable-length keying material which is not necessarily an algorithm-specific fixed-format key. The Cryptographic Message Syntax data format does not currently contain any provisions for password-based data encryption.

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