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

RFC 3447

Title: Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1
Author(s): J. Jonsson, B. Kaliski
Status: Informational
Date: February 2003
Mailbox: jonsson@mathematik.uni-marburg.de, bkaliski@rsasecurity.com
Pages: 72
Characters: 143173
Obsoletes: 2437

I-D Tag: **draft-jonsson-pkcs1-v2dot1-00.txt**

URL: ftp://ftp.rfc-editor.org/in-notes/rfc3447.txt

This memo represents a republication of PKCS #1 v2.1 from RSA Laboratories' Public-Key Cryptography Standards (PKCS) series, and change control is retained within the PKCS process. The body of this document is taken directly from the PKCS #1 v2.1 document, with certain corrections made during the publication process.

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.