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

RFC 3110

Title: RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS)
Author(s): D. Eastlake 3rd
Status: Standards Track
Date: May 2001
Mailbox: Donald.Eastlake@motorola.com
Pages: 7
Characters: 14587
Updates/Obsoletes/SeeAlso: None

I-D Tag: draft-ietf-dnsext-rsa-03.txt

URL: ftp://ftp.rfc-editor.org/in-notes/rfc3110.txt

This document describes how to produce RSA/SHA1 SIG resource records (RRs) in Section 3 and, so as to completely replace RFC 2537, describes how to produce RSA KEY RRs in Section 2.

Since the adoption of a Proposed Standard for RSA signatures in the DNS (Domain Name Space), advances in hashing have been made. A new DNS signature algorithm is defined to make these advances available in SIG RRs. The use of the previously specified weaker mechanism is deprecated. The algorithm number of the RSA KEY RR is changed to correspond to this new SIG algorithm. No other changes are made to DNS security.

This document is a product of the DNS Extensions 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.