Internet Draft
draft-ramsdell-smime31-cert-00.txt
July 14, 2000
Expires January 14, 2001

Author: Blake Ramsdell,
Tumbleweed Communications

S/MIME Version 3.1 Certificate Profile Addendum

Status of this memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at
http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at
http://www.ietf.org/shadow.html.

1. Overview

In light of the expiration of the primary RSA patent, it is proposed that the RSA algorithm replace the DSS and Diffie-Hellman as the MUST implement algorithms in the S/MIME profile. This draft will describe only the proposed changes to the S/MIME Version 3 Certificate Handling RFC [SMIMEV3CERT], and the rest of that RFC will remain identical.

1.1 Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [MUSTSHOULD].

1.2 Discussion of This Draft

This draft is being discussed on the "ietf-smime" mailing list.
To subscribe, send a message to:
ietf-smime-request@imc.org
with the single word
subscribe

in the body of the message. There is a Web site for the mailing list at <http://www.imc.org/ietf-smime/>.

2. Changes to the S/MIME Version 3 Certificate Handling RFC

The following changes to are proposed to [SMIMEV3CERT]:

1. Section 4.3 is replaced with the following:

> 4.3 Certificate and CRL Signing Algorithms
>
> Certificates and Certificate-Revocation Lists (CRLs) are signed by the certificate issuer. A receiving agent MUST be capable of verifying the signatures on certificates and CRLs made with md2WithRSAEncryption, md5WithRSAEncryption and sha-1WithRSAEncryption signature algorithms with key sizes from 512 bits to 2048 bits described in [PKCS#1V2].
>
> A receiving agent MAY be capable of verifying the signatures on certificates and CRLs made with id-dsa-with-sha1 [DSS].

3. Security Considerations

The security considerations are the same as for [SMIMEV3CERT].

A. References

[SMIMEV3CERT] "S/MIME Version 3 Certificate Handling", RFC 2632

[DSS] NIST FIPS PUB 186, "Digital Signature Standard", 18 May 1994.

[MUSTSHOULD] "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119

[PKCS#1V2], "PKCS #1: RSA Cryptography Specifications Version 2.0", RFC 2437

B. Acknowledgements

<tbd>

C. Changes from last draft

Initial revision.

D. AuthorÆs address

Blake Ramsdell
Tumbleweed Communications
17720 NE 65th St Ste 201
Redmond, WA 98052
+1 425 376 0225
blake.ramsdell@tumbleweed.com