Update to Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS)
draft-ietf-smime-rfc3278-update-00.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

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

This Internet-Draft will expire on July 12, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2008).

Abstract

RFC 3278 describes how to use Elliptic Curve Cryptography (ECC) public-key algorithms in the Cryptographic Message Syntax (CMS). This document updates RFC 3278 to add support for the SHA2 family of hash algorithms.
Conventions used in this document

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 [MUST].

Discussion

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/>.

Table of Contents

1. Introduction........................................................................2
2. Updates to Paragraph 2.1.1.............................................3
3. Updates to Paragraph 8.1................................................3
4. Updates to Paragraph 9...................................................5
5. Changes to Security Considerations.................................5
6. Security Considerations................................................5
7. IANA Considerations....................................................5
8. References........................................................................6
   8.1. Normative References.............................................6
   8.2. Informative References..........................................6

1. Introduction

RFC 3278 describes how to use Elliptic Curve Cryptography (ECC) public-key algorithms in the Cryptographic Message Syntax (CMS). This document updates RFC 3278 to add support for the SHA2 family of hash algorithms.

There are changes to four paragraphs:

- Paragraph 2.1.1 limited the digest algorithm to SHA-1. This document expands the allowed algorithms to SHA-224, SHA-256, SHA-284, and SHA-512.

- Paragraph 8.1 listed the algorithm identifiers for SHA-1 and SHA-1 with ECDSA. This document adds algorithms for SHA-224, SHA-256, SHA-284, and SHA-512 and SHA-224, SHA-256, SHA-284, and SHA-512 with ECDSA.

- Paragraph 9 references need to be updated.
- Security considerations paragraph referring to definitions of SHA-224, SHA-256, SHA-284, and SHA-512 needs to be deleted.

2. Updates to Paragraph 2.1.1

Old:

digestAlgorithm MUST contain the algorithm identifier sha-1 (see Section 8.1) which identifies the SHA-1 hash algorithm.

signatureAlgorithm contains the algorithm identifier ecdsa-with-SHA1 (see Section 8.1) which identifies the ECDSA signature algorithm.

New:

digestAlgorithm MUST contain the algorithm identifier of the hash algorithm (see Section 8.1): id-sha1 identifies the SHA-1 hash algorithm, id-sha224 identifies the SHA-224 hash algorithm, id-sha256 identifies the SHA-256 hash algorithm, id-sha384 identifies the SHA-384 algorithm, and id-sha512 identifies the SHA-512 algorithm.


3. Updates to Paragraph 8.1

Old:

The algorithm identifiers used in this document are taken from [X9.62], [SEC1] and [SEC2].

The following object identifier indicates the hash algorithm used in this document:

    sha-1 OBJECT IDENTIFIER ::= { iso(1) identified-organization(3)
        oiw(14) secsig(3) algorithm(2) 26 }

New:

The algorithm identifiers used in this document are taken from [SMIME-SHA2]

The following object identifier indicates the hash algorithm used in this document:
id-sha1 OBJECT IDENTIFIER ::= { iso(1) identified-organization(3) oiw(14) secsig(3) algorithm(2) 26 }

id-sha224 OBJECT IDENTIFIER ::= { joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 4 }

id-sha256 OBJECT IDENTIFIER ::= { joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1 }

id-sha384 OBJECT IDENTIFIER ::= { joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 2 }

id-sha512 OBJECT IDENTIFIER ::= { joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 3 }

Old:

The following object identifier indicates the digital signature algorithm used in this document:

ecdsa-with-SHA1 OBJECT IDENTIFIER ::= { ansi-x9-62 signatures(4) 1 }

New:

The following object identifier indicates the digital signature algorithm used in this document:

ecdsa-with-SHA1 OBJECT IDENTIFIER ::= { ansi-x9-62 signatures(4) 1 }

ecdsa-with-SHA224 OBJECT IDENTIFIER ::= { ansi-x9-62 signatures(4) ecdsa-with-SHA2(3) 1 }

ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { ansi-x9-62 signatures(4) ecdsa-with-SHA2(3) 2 }

ecdsa-with-SHA384 OBJECT IDENTIFIER ::= { ansi-x9-62 signatures(4) ecdsa-with-SHA2(3) 3 }

ecdsa-with-SHA512 OBJECT IDENTIFIER ::= { ansi-x9-62 signatures(4) ecdsa-with-SHA2(3) 4 }
4. Updates to Paragraph 9

Add the following reference:


Update the following references:

Old:


New:


5. Changes to Security Considerations

Delete the following:

When 256, 384, and 512 bit hash functions succeed SHA-1 in future revisions of [FIPS], [FIPS-186-2], [X9.62] and [SEC1], then they can similarly succeed SHA-1 in a future revision of this document.

6. Security Considerations

No new security considerations to those already specified in [RFC3278], [SMIME-SHA2], and [PKI-ALG].

7. IANA Considerations

None: All identifiers are already registered. Please remove this section prior to publication as an RFC.
8. References

8.1. Normative References


8.2. Informative References

None.
Author’s Addresses

Sean Turner

IECA, Inc.
3057 Nutley Street, Suite 106
Fairfax, VA 22031
USA

Email: turners@ieca.com