

NETWORK WG  
Internet Draft  
Intended Status: Informational  
Expires: December 14, 2013

Sean Turner  
IECA  
A. Melnikov  
ISODE Ltd  
Carl Wallace  
Red Hound Software  
June 12, 2013

vCard S/MIME Capabilities Property  
draft-turner-vcard-smimecaps-00.txt

## Abstract

This document defines a vCard S/MIME Capabilities property and it defines or references values for many algorithms. The SMIME Capability values can also be included in S/MIME messages as a signed attribute and in public key certificates as an extension. The S/MIME Capabilities property is a complement to key property, which together enable usage of S/MIME without an initial exchange of email messages.

## Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

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."

## Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must

Internet-Draft

vCard S/MIME Capabilities Property

June 12, 2013

include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## 1. Introduction

This document defines or references values for the vCard S/MIME Capabilities property. The syntax for the property is defined in [\[RFC5751\]](#), but the values for each capability instance are defined in separate RFCs and in some cases not at all. Capability values can also be included in S/MIME messages as an attribute and in public key certificates as an extension [\[RFC4262\]](#).

The majority of the values in this document are defined in other RFCs, and this document references those RFCs before the SMIME Capability. Values are encoded using the Distinguished Encoding Rule (DER) [\[X.690\]](#) and are a sequence of algorithm object identifier plus any parameters. The values provided in this document are values for single SMIMECapability instance, which contain one algorithm-parameter pair. These values may be concatenated and preceded by a tag and length value to produce a SMIMECapabilities value. The syntax for the attribute is as follows and is repeated here from [\[RFC5751\]](#) for convenience:

SMIMECapabilities ::= SEQUENCE OF SMIMECapability

SMIMECapability ::= SEQUENCE {  
    capabilityID OBJECT IDENTIFIER,  
    parameters ANY DEFINED BY capabilityID OPTIONAL }

As specified in [\[RFC5751\]](#): "the object identifiers (OIDs) are listed in order of their preference, but SHOULD be separated logically along the lines of their categories (signature algorithms, symmetric algorithms, key encipherment algorithms, etc.)" As the "structure of the SMIMECapabilities attribute is [designed] to facilitate simple table lookups and binary comparisons in order to determine matches", the values are given in encoded format.

In the following sections, the DER [\[X.690\]](#) values for the capabilities are preceded by the algorithm's name, and, if they were previously defined a reference for the document in which they are defined.

## 1.1. Requirements Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this

Turner

December 14, 2013

[Page 2]

---

Internet-Draft

vCard S/MIME Capabilities Property

June 12, 2013

document are to be interpreted as described in [[RFC2119](#)].

## 2. Message Digest Algorithms

[RFC3370] and [[RFC5754](#)] define the following message digest algorithms for use with CMS:

MD5: 300a 0608 2a86 4886 f70d 0205

NOTE: Though [[RFC3370](#)] allows NULL parameters for SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, parameters MUST NOT be included in SMIMECapability values as per [[RFC5751](#)] because there is no differentiating by parameters for SHA-1 (e.g., output length).

SHA-1: 3007 0605 290e 0302 1a

[RFC5754] SHA-224: 300b 0609 6086 4801 6503 0402 04

[RFC5754] SHA-256: 300b 0609 6086 4801 6503 0402 01

[RFC5754] SHA-384: 300b 0609 6086 4801 6503 0402 02

[RFC5754] SHA-512: 300b 0609 6086 4801 6503 0402 03

Internet-Draft

vCard S/MIME Capabilities Property

June 12, 2013

### 3. Digital Signature Algorithms

[[RFC3370](#)], [[RFC4056](#)], [[RFC5754](#)], and [[RFC5753](#)] define the following digital signature algorithms for use with CMS:

RSA Encryption: 3009 0608 2a86 4886 f70d 0101 01

RSA With MD5: 3009 0608 2a86 4886 f70d 0101 04

RSA With SHA-1: 3009 0608 2a86 4886 f70d 0101 05

RSA With SHA-224: 3009 0608 2a86 4886 f70d 0101 0e

RSA With SHA-256: 3009 0608 2a86 4886 f70d 0101 0b

RSA With SHA-384: 3009 0608 2a86 4886 f70d 0101 0c

RSA With SHA-512: 3009 0608 2a86 4886 f70d 0101 0d

NOTE: [[RFC4055](#)] includes NULL parameters with SHA-1.

RSASSA-PSS Defaults: 300D 0609 2a86 4886 f70d 0101 0a30 00

DSA With SHA-1: 3009 0607 2a86 48ce 3804 03

[[RFC5754](#)] DSA With SHA-224: 300b 0609 6086 4801 6503 0403 01

[[RFC5754](#)] DSA With SHA-256: 300b 0609 6086 4801 6503 0403 02

NOTE: [[RFC5753](#)] shows the ECDSA with SHA-1 with NULL parameter values, but the NULL parameters should not have been included according to [[RFC5751](#)]. The NULL is retained for backwards compatibility.

[RFC5753] ECDSA With SHA-1: 300b 0607 2a86 48ce 3d04 0105 00

[RFC5753] ECDSA With SHA-224: 300a 0608 2a86 48ce 3d04 0301

[RFC5753] ECDSA With SHA-256: 300a 0608 2a86 48ce 3d04 0302

[RFC5753] ECDSA With SHA-384: 300a 0608 2a86 48ce 3d04 0303

[RFC5753] ECDSA With SHA-512: 300a 0608 2a86 48ce 3d04 0304

#### [4](#). Key Transport Algorithms

[[RFC3370](#)], [[RFC3560](#)], [[RFC5990](#)] define the following key transport algorithms for use with CMS:

Turner

December 14, 2013

[Page 4]

---

Internet-Draft

vCard S/MIME Capabilities Property

June 12, 2013

RSA Encryption: 300d 0608 2a86 4886 f70d 0101 01

[RFC3560] RSAES-OAEP Default: 300D 0609 2a86 4886 f70d 0101 0730 00

NOTE: [[RFC3560](#)] shows the RSAES-OAEP with SHA-224, SHA-256, 384, and 512 with NULL parameter values for the SHA algorithms, but the NULL parameters should not have been included according to [RFCTBD1].

[RFC3560] RSAES-OAEP SHA-224: 3038 0609 2a86 4886 f70d 0101 0730 2b30  
0d06 0960 8648 0165 0304 0201 0500 301a 0609 2a86 4886 f70d  
0101 0830 0d06 0960 8648 0165 0304 0204 0500

[RFC3560] RSAES-OAEP SHA-256: 3038 0609 2a86 4886 f70d 0101 0730 2b30  
0d06 0960 8648 0165 0304 0201 0500 301a 0609 2a86 4886 f70d  
0101 0830 0d06 0960 8648 0165 0304 0201 0500

[RFC3560] RSAES-OAEP SHA-384: 3038 0609 2a86 4886 f70d 0101 0730 2b30  
0d06 0960 8648 0165 0304 0202 0500 301a 0609 2a86 4886 f70d  
0101 0830 0d06 0960 8648 0165 0304 0202 0500

[RFC3560] RSAES-OAEP SHA-512: 3038 0609 2a86 4886 f70d 0101 0730 2b30  
0d06 0960 8648 0165 0304 0202 0500 301a 0609 2a86 4886 f70d

0101 0830 0d06 0960 8648 0165 0304 0203 0500

[RFC5990] RSA-KEM KDF3 based on SHA-256, AES Key Wrap with a 128-bit  
KEK: 3047 060b 2a86 4886 f70d 0109 1003 ??30 3830 2906  
0728 818c 7102 0204 301e 3019 060a 2b81 0510 8648 092c  
0102 300b 0609 6086 4801 6503 0402 0102 0110 300b 0609  
6086 4801 6503 0401 05

[RFC5990] RSA-KEM KDF3 based on SHA-384, AES Key Wrap with a 192-bit  
KEK: 3047 060b 2a86 4886 f70d 0109 1003 ??30 3830 2906  
0728 818c 7102 0204 301e 3019 060a 2b81 0510 8648 092c  
0102 300b 0609 6086 4801 6503 0402 0202 0118 300b 0609  
6086 4801 6503 0401 19

[RFC5990] RSA-KEM KDF3 based on SHA-512, AES Key Wrap with a 256-bit  
KEK: 3047 060b 2a86 4886 f70d 0109 1003 ??30 3830 2906  
0728 818c 7102 0204 301e 3019 060a 2b81 0510 8648 092c  
0102 300b 0609 6086 4801 6503 0402 0302 0120 300b 0609  
6086 4801 6503 0401 2d

[RFC5990] RSA-KEM KDF2 based on SHA-1, Triple-DES Key Wrap with a  
128-bit KEK (two-key triple-DES): 3045 060b 2a86 4886  
f70d 0109 1003 ??30 3630 2506 0728 818c 7102 0204 301a  
3015 060a 2b81 0510 8648 092c 0101 3007 0605 2b0e 0302  
1a02 0110 300d 060b 2a86 4886 f70d 0109 1003 06

## 5. Key Agreement Algorithms

[RFC2876], [RFC3370], and [RFC5753] define the following key agreement algorithms for use with CMS:

NOTE: The parameters for key agreement algorithms are the key wrap algorithm (see [Section 6](#)).

[RFC2876] KEA: 3018 0609 6086 4801 6502 0101 1830 0b06 0960 8648 0165  
0201 0117

KA=DH S-S Wrap=Triple-DES: 301c 060d 2a86 4886 f70d 0109 1003 0a30  
0d06 0d2a 8648 86f7 0d01 0910 0306

KA=DH S-S Wrap=RC2 Para=40-bit: 3020 060d 2a86 4886 f70d 0109 1003

0a30 1106 0d2a 8648 86f7 0d01 0910 0306 0202 00a0

KA=DH S-S Wrap=RC2 Para=64-bit: 301f 060d 2a86 4886 f70d 0109 1003  
0a30 1006 0d2a 8648 86f7 0d01 0910 0306 0201 78

KA=DH S-S Wrap=RC2 Para=128-bit: 301f 060d 2a86 4886 f70d 0109 1003  
0a30 1006 0d2a 8648 86f7 0d01 0910 0306 0201 3a

KA=DH E-S Wrap=Triple-DES: 301c 060d 2a86 4886 f70d 0109 1003 0530  
0d06 0d2a 8648 86f7 0d01 0910 0306

KA=DH E-S Wrap=RC2 Para=40-bit: 3020 060d 2a86 4886 f70d 0109 1003  
0530 1106 0d2a 8648 86f7 0d01 0910 030a 0202 00a0

KA=DH E-S Wrap=RC2 Para=64-bit: 301f 060d 2a86 4886 f70d 0109 1003  
0530 1006 0d2a 8648 86f7 0d01 0910 030a 0201 78

KA=DH E-S Wrap=RC2 Para=128-bit: 301f 060d 2a86 4886 f70d 0109 1003  
0530 1006 0d2a 8648 86f7 0d01 0910 030a 0201 3a

NOTE: [[RFC5753](#)] shows the ECDH with SHA-1|Triple-DES wrap capabilities with NULL parameter values, but the NULL parameters should not have been included according to [RFCTBD1]. The NULL is retained for backwards compatibility.

[RFC5753] KA=ECDH standard KDF=SHA-1 Wrap=Triple-DES: 301c 0609 2b81  
0510 8648 3f00 0230 0f06 0b2a 8648 86f7 0d01 0910 0306 0500

[RFC5753] KA=ECDH standard KDF=SHA-224 Wrap=Triple-DES: 3017 0606  
2b81 0401 0b00 300e 060b 2a86 4886 f70d 0109 1003 06

[RFC5753] KA=ECDH standard KDF=SHA-256 Wrap=Triple-DES: 3017 0606

2b81 0401 0b01 300e 060b 2a86 4886 f70d 0109 1003 06

[RFC5753] KA=ECDH standard KDF=SHA-384 Wrap=Triple-DES: 3017 0606  
2b81 0401 0b02 300e 060b 2a86 4886 f70d 0109 1003 06

[RFC5753] KA=ECDH standard KDF=SHA-512 Wrap=Triple-DES: 3017 0606  
2b81 0401 0b03 300e 060b 2a86 4886 f70d 0109 1003 06

[RFC5753] KA=ECDH standard KDF=SHA-1 Wrap=AES-128: 3018 0609 2b81  
0510 8648 3f00 0230 0b06 0960 8648 0165 0304 0105

[RFC5753] KA=ECDH standard KDF=SHA-224 Wrap=AES-128: 3015 0606 2b81  
0401 0b00 300b 0609 6086 4801 6503 0401 05

[RFC5753] KA=ECDH standard KDF=SHA-256 Wrap=AES-128: 3015 0606 2b81  
0401 0b01 300b 0609 6086 4801 6503 0401 05

[RFC5753] KA=ECDH standard KDF=SHA-384 Wrap=AES-128: 3015 0606 2b81  
[RFC5753] KA=ECDH standard KDF=SHA-512 Wrap=AES-128: 3015  
0606 2b81 0401 0b03 300b 0609 6086 4801 6503 0401 05

[RFC5753] KA=ECDH standard KDF=SHA-1 Wrap=AES-192: 3018 0609 2b81  
0510 8648 3f00 0230 0b06 0960 8648 0165 0304 0119

[RFC5753] KA=ECDH standard KDF=SHA-224 Wrap=AES-192: 3015 0606 2b81  
0401 0b00 300b 0609 6086 4801 6503 0401 19

[RFC5753] KA=ECDH standard KDF=SHA-256 Wrap=AES-192: 3015 0606 2b81  
0401 0b01 300b 0609 6086 4801 6503 0401 19

[RFC5753] KA=ECDH standard KDF=SHA-384 Wrap=AES-192: 3015 0606 2b81  
0401 0b02 300b 0609 6086 4801 6503 0401 19

[RFC5753] KA=ECDH standard KDF=SHA-512 Wrap=AES-192: 3015 0606 2b81  
0401 0b03 300b 0609 6086 4801 6503 0401 19

[RFC5753] KA=ECDH standard KDF=SHA-1 Wrap=AES-256: 3018 0609 2b81  
0510 8648 3f00 0230 0b06 0960 8648 0165 0304 012d

[RFC5753] KA=ECDH standard KDF=SHA-224 Wrap=AES-256: 3015 0606 2b81  
0401 0b00 300b 0609 6086 4801 6503 0401 2d

[RFC5753] KA=ECDH standard KDF=SHA-256 Wrap=AES-256: 3015 0606 2b81  
0401 0b01 300b 0609 6086 4801 6503 0401 2d

[RFC5753] KA=ECDH standard KDF=SHA-384 Wrap=AES-256: 3015 0606 2b81  
0401 0b02 300b 0609 6086 4801 6503 0401 2d

[RFC5753] KA=ECDH standard KDF=SHA-512 Wrap=AES-256: 3015 0606 2b81



0401 0B03 300b 0609 6086 4801 6503 0401 2d

NOTE: [[RFC5753](#)] shows the ECMQV with SHA-1 and Triple-DES wrap capabilities with NULL parameter values, but the NULL parameters should not have been included according to [RFCTBD1]. The NULL is retained for backwards compatibility.

[RFC5753] KA=ECDH cofactor KDF=SHA-1 Wrap=Triple-DES: 301c 0609 2b81 0510 8648 3f00 0330 0f06 0b2a 8648 86f7 0d01 0910 0306 0500

[RFC5753] KA=ECDH cofactor KDF=SHA-224 Wrap=Triple-DES: 3017 0606 2b81 0401 0e00 300d 060b 2a86 4886 f70d 0109 1003 06

[RFC5753] KA=ECDH cofactor KDF=SHA-256 Wrap=Triple-DES: 3017 0606

[RFC5753] KA=ECDH cofactor KDF=SHA-384 Wrap=Triple-DES: 3017 0606 2b81 0401 0e02 300d 060b 2a86 4886 f70d 0109 1003 06

[RFC5753] KA=ECDH cofactor KDF=SHA-512 Wrap=Triple-DES: 3017 0606 2b81 0401 0e03 300d 060b 2a86 4886 f70d 0109 1003 06

[RFC5753] KA=ECDH cofactor KDF=SHA-1 Wrap=AES-128: 3018 0609 2b81 0510 8648 3f00 0330 0b06 0960 8648 0165 0304 0105

[RFC5753] KA=ECDH cofactor KDF=SHA-224 Wrap=AES-128: 3015 0606 2b81 0401 0e00 300b 0609 6086 4801 6503 0401 05

[RFC5753] KA=ECDH cofactor KDF=SHA-256 Wrap=AES-128: 3015 0606 2b81 0401 0e01 300b 0609 6086 4801 6503 0401 05

[RFC5753] KA=ECDH cofactor KDF=SHA-384 Wrap=AES-128: 3015 0606 2b81 0401 0e02 300b 0609 6086 4801 6503 0401 05

[RFC5753] KA=ECDH cofactor KDF=SHA-512 Wrap=AES-128: 3017 0606 2b81 0401 0e03 300b 0609 6086 4801 6503 0401 05

[RFC5753] KA=ECDH cofactor KDF=SHA-1 Wrap=AES-192: 30 18 06 09 2b 81 0510 8648 3f00 0330 0b06 0960 8648 0165 0304 0119

[RFC5753] KA=ECDH cofactor KDF=SHA-224 Wrap=AES-192: 3015 0606 2b81 0401 0e00 300b 0609 6086 4801 6503 0401 19

[RFC5753] KA=ECDH cofactor KDF=SHA-256 Wrap=AES-192: 3015 0606 2b81 0401 0e01 300b 0609 6086 4801 6503 0401 19

[RFC5753] KA=ECDH cofactor KDF=SHA-384 Wrap=AES-192: 3015 0606 2b81 0401 0e02 300b 0609 6086 4801 6503 0401 19

[RFC5753] KA=ECDH cofactor KDF=SHA-512 Wrap=AES-192: 3015 0606 2b81  
0401 0e03 300b 0609 6086 4801 6503 0401 19

[RFC5753] KA=ECDH cofactor KDF=SHA-1 Wrap=AES-256: 3015 0609 2b81  
0510 8648 3f00 0330 0b06 0960 8648 0165 0304 012d

[RFC5753] KA=ECDH cofactor KDF=SHA-224 Wrap=AES-256: 3015 0606 2b81  
0401 0e00 300b 0609 6086 4801 6503 0401 2d

[RFC5753] KA=ECDH cofactor KDF=SHA-256 Wrap=AES-256: 3015 0606 2b81  
0401 0e01 300b 0609 6086 4801 6503 0401 2d

[RFC5753] KA=ECDH cofactor KDF=SHA-384 Wrap=AES-256: 3015 0606 2b81

[[RFC5753](#)] KA=ECDH cofactor KDF=SHA-512 Wrap=AES-256: 3015 0606 2b81  
0401 0e03 300b 0609 6086 4801 6503 0401 2d

NOTE: [[RFC5753](#)] shows the ECMQV with SHA-1 and Triple-DES wrap capabilities with NULL parameter values, but the NULL parameters should not have been included according to [RFCTBD1]. The NULL is retained for backwards compatibility.

[RFC5753] KA=ECMQV 1-Pass KDF=SHA-1 Wrap=Triple-DES: 301c 0609 2b81  
0510 8648 3f00 1030 0f06 0b2a 8648 86f7 0d01 0910 0306 0500

[RFC5753] KA=ECMQV 1-Pass KDF=SHA-224 Wrap=Triple-DES: 3017 0606 2b81  
0401 0f00 300d 060b 2a86 4886 f70d 0109 1003 06

[RFC5753] KA=ECMQV 1-Pass KDF=SHA-256 Wrap=Triple-DES: 3017 0606 2b81  
0401 0f01 300d 060b 2a86 4886 f70d 0109 1003 06

[RFC5753] KA=ECMQV 1-Pass KDF=SHA-384 Wrap=Triple-DES: 3017 0606 2b81  
0401 0f02 300d 060b 2a86 4886 f70d 0109 1003 06

[RFC5753] KA=ECMQV 1-Pass KDF=SHA-512 Wrap=Triple-DES: 3017 0606 2b81  
0401 0f03 300d 060b 2a86 4886 f70d 0109 1003 06

[RFC5753] KA=ECMQV 1-Pass KDF=SHA-1 Wrap=AES-128: 3018 0609 2b81 0510  
8648 3f00 1030 0b06 0960 8648 0165 0304 0105

[RFC5753] KA=ECMQV 1-Pass KDF=SHA-224 Wrap=AES-128: 3015 0606 2b81  
0401 0f00 300b 0609 6086 4801 6503 0401 05

[RFC5753] KA=ECMQV 1-Pass KDF=SHA-256 Wrap=AES-128: 3015 0606 2b81  
0401 0f01 300b 0609 6086 4801 6503 0401 05

[RFC5753] KA=ECMQV 1-Pass KDF=SHA-384 Wrap=AES-128: 3015 0606 2b81

0401 0f02 300b 0609 6086 4801 6503 0401 05

Internet-Draft

vCard S/MIME Capabilities Property

June 12, 2013

[RFC5753] KA=ECMQV 1-Pass KDF=SHA-512 Wrap=AES-128: 3015 0606 2b81  
0401 0f03 300b 0609 6086 4801 6503 0401 05

[RFC5753] KA=ECMQV 1-Pass KDF=SHA-1 Wrap=AES-192: 3018 0609 2b81 0510  
8648 3f00 1030 0b06 0960 8648 0165 0304 0119

[RFC5753] KA=ECMQV 1-Pass KDF=SHA-224 Wrap=AES-192: 3015 0606 2b81  
0401 0f00 300b 0609 6086 4801 6503 0401 19

[RFC5753] KA=ECMQV 1-Pass KDF=SHA-256 Wrap=AES-192: 3015 0606 2b81

[[RFC5753](#)] KA=ECMQV 1-Pass KDF=SHA-384 Wrap=AES-192: 3015 0606 2b81  
0401 0f02 300b 0609 6086 4801 6503 0401 19

[RFC5753] KA=ECMQV 1-Pass KDF=SHA-512 Wrap=AES-192: 3015 0606 2b81  
0401 0f03 300b 0609 6086 4801 6503 0401 19

[RFC5753] KA=ECMQV 1-Pass KDF=SHA-1 Wrap=AES-256: 3018 0609 2b81 0510  
8648 3f00 1030 0b06 0960 8648 0165 0304 012d

[RFC5753] KA=ECMQV 1-Pass KDF=SHA-224 Wrap=AES-256: 3015 0606 2b81  
0401 0f00 300b 0609 6086 4801 6503 0401 2d

[RFC5753] KA=ECMQV 1-Pass KDF=SHA-256 Wrap=AES-256: 3015 0606 2b81  
0401 0f01 300b 0609 6086 4801 6503 0401 2d

[RFC5753] KA=ECMQV 1-Pass KDF=SHA-384 Wrap=AES-256: 3015 0606 2b81  
0401 0f02 300b 0609 6086 4801 6503 0401 2d

[RFC5753] KA=ECMQV 1-Pass KDF=SHA-512 Wrap=AES-256: 3015 0606 2b81  
0401 0f03 300b 0609 6086 4801 6503 0401 2d

## [6](#). Key Wrap Algorithms

[[RFC2876](#)], [[RFC3058](#)], [[RFC3370](#)], [[RFC3565](#)], [[RFC3657](#)], [[RFC4010](#)],  
[[RFC5649](#)] define the following key wrap algorithms for use with CMS:

NOTE: In most instances, the key wrap algorithm is included in the capabilities set as part of the key agreement algorithm.

[RFC2876] FORTEZZA Wrap 80: 300b 0609 6086 4801 6502 0101 17

[RFC3058] IDEA: 300D 060B 2B06 0104 0181 3C07 0101 02

3-DES Wrap: 300e 060b 2a86 4886 f70d 0109 1003 06

RC2 40-bit: 3011 060d 2a86 4886 f70d 0109 1003 0602 0200 a0

RC2 64-bit: 3010 060d 2a86 4886 f70d 0109 1003 0602 0178

Turner

December 14, 2013

[Page 10]

---

Internet-Draft

vCard S/MIME Capabilities Property

June 12, 2013

RC2 128-bit: 3010 060d 2a86 4886 f70d 0109 1003 0602 013a

AES-128 Key Wrap: 300b 0609 6086 4801 6503 0401 05

AES-196 Key Wrap: 300b 0609 6086 4801 6503 0401 19

AES-128 Key Wrap with Padding: 300b 0609 6086 4801 6503 0401 08

AES-196 Key Wrap with Padding: 300b 0609 6086 4801 6503 0401 1c

AES-256 Key Wrap with Padding: 300b 0609 6086 4801 6503 0401 30

Camellia 128-Wrap: 300d 060b 2a83 088c 9a4b 3d01 0103 02

Camellia 196-Wrap: 300d 060b 2a83 088c 9a4b 3d01 0103 03

Camellia 256-Wrap: 300d 060b 2a83 088c 9a4b 3d01 0103 04

SEED Wrap: 300c 060a 2a83 1a8c 9a44 0701 0101

## 7. Content Encryption Algorithms

[RFC2876], [RFC3058], [RFC3370], [RFC3565], [RFC3657], [RFC5084], and [RFC5649] define the following content encryption algorithms for use with CMS:

RC2-CBC 40-bit: 300d 0608 2a86 4886 f70d 0302 0201 28

RC2-CBC 64-bit: 300d 0608 2a86 4886 f70d 0302 0201 40

RC2-CBC 128-bit: 300e 0608 2a86 4886 f70d 0302 0202 0080

3-DES-CBC: 300a 0608 2a86 4886 f70d 0307

NOTE: [[RFC2876](#)] incorrectly included 00 at the end of the SMIMECapability.

[RFC2876] SKIPJACK: 300b 0609 6086 4801 6502 0101 04

[RFC3058] IDEA-CBC: 300d 060b 2b06 0104 0181 3c07 0101 02

[RFC3565] AES-CBC-128: 300b 0609 6086 4801 6503 0401 02

[RFC3565] AES-CBC-196: 300b 0609 6086 4801 6503 0401 16

[RFC3565] AES-CBC-256: 300b 0609 6086 4801 6503 0401 2a

Turner

December 14, 2013

[Page 11]

---

Internet-Draft

vCard S/MIME Capabilities Property

June 12, 2013

AES-CCM-128: 300b 0609 6086 4801 6503 0401 07

AES-CCM-196: 300b 0609 6086 4801 6503 0401 1b

AES-CCM-256: 300b 0609 6086 4801 6503 0401 2f

AES-GCM-128: 300b 0609 6086 4801 6503 0401 06

AES-GCM-196: 300b 0609 6086 4801 6503 0401 1a

AES-GCM-256: 300b 0609 6086 4801 6503 0401 2e

AES-128 Key Wrap: 300b 0609 6086 4801 6503 0401 05

AES-196 Key Wrap: 300b 0609 6086 4801 6503 0401 19

AES-256 Key Wrap: 300b 0609 6086 4801 6503 0401 2d

AES-128 Key Wrap with MLI: 300b 0609 6086 4801 6503 0401 08

AES-196 Key Wrap with MLI: 300b 0609 6086 4801 6503 0401 1c

AES-256 Key Wrap with MLI: 300b 0609 6086 4801 6503 0401 30

NOTE: Camellia defines their capability parameters as NULL.

[RFC3657] Camellia 128-CBC: 300f 060b 2a83 088c 9a4b 3d01 0101 0205  
00

[RFC3657] Camellia 196-CBC: 300f 060b 2a83 088c 9a4b 3d01 0101 0305  
00

[RFC3657] Camellia 256-CBC: 300f 060b 2a83 088c 9a4b 3d01 0101 0405  
00

NOTE: SEED defines their capability parameters as NULL.

[RFC4010] SEED CBC: 300C 0608 2a83 1a8c 9a44 0104 0500

## 8. Message Authentication Code Algorithms

[[RFC3370](#)], [[RFC4231](#)], and [[RFC4490](#)] define the following message authentication code algorithms for use with CMS:

HMAC SHA-1: 3009 0608 2b0601 0505 0801 02

HMAC SHA-224: 300a 0608 2a86 4886 f70d 0208

Turner

December 14, 2013

[Page 12]

---

Internet-Draft

vCard S/MIME Capabilities Property

June 12, 2013

HMAC SHA-256: 300a 0608 2a86 4886 f70d 0209

HMAC SHA-384: 300a 0608 2a86 4886 f70d 020a

[RFC4490] HMAC GOST: 3008 0606 2A85 0302 0209

## 9. Compression Algorithms

[RFC3274] define the following compression algorithms for use with CMS:

[RFC3274] ZLIB: 300D 060B 2A86 4886 F70D 0109 1003 08

## 10. Security Considerations

This document does not advocate the use of any particular algorithm. The strength of the algorithms and applicability to their use in a

particular environment is defined in the algorithms specifications.

Unlike the S/MIME Capabilities attribute that may be included in S/MIME messages or the S/MIME capabilities attribute that may be included in X.509 certificates, the vCard property defined in this document is not signed. Locally stored copies of the vCard property should be updated as necessary when presented a signed S/MIME capabilities instance.

## 11. IANA Considerations

This document registers a new vCard property [[RFC6350](#)] for S/MIME Capabilities defined in [Section 1](#). The registration template is specified below:

Purpose: To specify a list of S/MIME capabilities associated with the object that the vCard represents. Each value represents a single SMIMECapability.

Value type: A text value (base64-encoded DER [[X.690](#)]). It can also be reset to a single URI. [[Or just always use data: URIs?]]

Cardinality: \*

ABNF:

```
SMIMECAPA-param = SMIMECAPA-uri-param / SMIMECAPA-text-param
SMIMECAPA-value = SMIMECAPA-uri-value / SMIMECAPA-text-value
; Value and parameter MUST match.
```

```
SMIMECAPA-uri-param = "VALUE=uri" / mediatype-param
SMIMECAPA-uri-value = URI
```

```
SMIMECAPA-text-param = "VALUE=text"
SMIMECAPA-text-value = text
```

```
SMIMECAPA-param =/ altid-param / pid-param / pref-param /
                  type-param / any-param
```

Examples:

SMIMECAPA:<... remainder of base64-encoded data ...>  
[[Add a real example]]

## [12. References](#)

### [12.1. Normative References](#)

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC5751] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification", [RFC 5751](#), January 2010.
- [RFC6350] Perreault, S., "vCard Format Specification", [RFC 6350](#), August 2011.
- [X.690] ITU-T Recommendation X.690 (2002) | ISO/IEC 8825-1:2002, Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).

### [12.2. Informative References](#)

- [RFC2876] Pawling, J., "Use of the KEA and SKIPJACK Algorithms in CMS", [RFC 2876](#), July 2000.
- [RFC3058] Teiwe, S., Hartmann, P., and D. Kuenzi, "Use of the IDEA Encryption Algorithm in CMS", [RFC 3058](#), February 2001.
- [RFC3274] Gutmann, P., "Compressed Data Content Type for Cryptographic Message Syntax (CMS)", [RFC 3274](#), June 2002.

- [RFC3370] Housley, R., "Cryptographic Message Syntax (CMS) Algorithms", [RFC 3370](#), August 2002.

- [RFC3560] Housley, R., "Use of the RSAES-OAEP Key Transport



- Algorithm in Cryptographic Message Syntax (CMS)", [RFC 3560](#), July 2003.
- [RFC3565] Schaad, J., "Use of the Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Syntax (CMS)", [RFC 3565](#), July 2003.
- [RFC3657] Moriai, S. and A. Kato, "Use of the Camellia Encryption Algorithm in Cryptographic Message Syntax (CMS)", [RFC 3657](#), January 2004.
- [RFC4010] Park, J., Lee, S., Kim, J., and J. Lee, "Use of the SEED Encryption Algorithm in Cryptographic Message Syntax (CMS)", [RFC 4010](#), February 2005.
- [RFC4055] Schaad, J., Kaliski, B., and R. Housley, "Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", [RFC 4055](#), June 2005.
- [RFC4056] Schaad, J., "Use of the RSASSA-PSS Signature Algorithm in Cryptographic Message Syntax (CMS)", [RFC 4056](#), June 2005.
- [RFC4231] Nystrom, M., "Identifiers and Test Vectors for HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512", [RFC 4231](#), December 2005.
- [RFC4262] Santesson, S., "X.509 Certificate Extension for Secure/Multipurpose Internet Mail Extensions (S/MIME) Capabilities", [RFC 4262](#), December 2005.
- [RFC4490] Leontiev, S., Ed., and G. Chudov, Ed., "Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS)", [RFC 4490](#), May 2006.
- [RFC5084] Housley, R., "Using AES-CCM and AES-GCM Authenticated Encryption in the Cryptographic Message Syntax (CMS)", [RFC 5084](#), November 2007.
- [RFC5649] Housley, R. and M. Dworkin, "Advanced Encryption Standard (AES) Key Wrap with Padding Algorithm",

[RFC 5649](#), September 2009.

- [RFC5753] Turner, S. and D. Brown, "Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS)", [RFC 5753](#), January 2010.
- [RFC5754] Turner, S., "Using SHA2 Algorithms with Cryptographic Message Syntax", [RFC 5754](#), January 2010.
- [RFC5990] Randall, J., Kaliski, B., Brainard, J., and S. Turner, "Use of the RSA-KEM Key Transport Algorithm in the Cryptographic Message Syntax (CMS)", [RFC 5990](#), September 2010.

#### Authors' Addresses

Sean Turner

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

Email: [turners@ieca.com](mailto:turners@ieca.com)

Alexey Melnikov  
Isode Ltd  
5 Castle Business Village  
36 Station Road  
Hampton, Middlesex TW12 2BX  
UK

Email: [Alexey.Melnikov@isode.com](mailto:Alexey.Melnikov@isode.com)

Carl Wallace

Email: [carl@redhoundsoftware.com](mailto:carl@redhoundsoftware.com)

