Internet Engineering Task Force (IETF)
Request for Comments: 7107
Category: Informational
ISSN: 2070-1721

R. Housley
Vigil Security

January 2014

Object Identifier Registry for the S/MIME Mail Security Working Group

Abstract

When the S/MIME Mail Security Working Group was chartered, an object identifier arc was donated by RSA Data Security for use by that working group. This document describes the object identifiers that were assigned in that donated arc, transfers control of that arc to IANA, and establishes IANA allocation policies for any future assignments within that arc.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7107.

Table of Contents

1. Introduction

When the S/MIME Mail Security Working Group was chartered, an object identifier arc was donated by RSA Data Security for use by that working group. These object identifiers are primarily used with Abstract Syntax Notation One (ASN.1) [ASN1-88] [ASN1-08]. The ASN.1 specifications continue to evolve, but object identifiers can be used with any and all versions of ASN.1.

The S/MIME object identifier arc is:

```
id-smime OBJECT IDENTIFIER ::= { iso(1) member-body(2)
            us(840) rsadsi(113549) pkcs(1) pkcs9(9) 16 }
```

This document describes the object identifiers that were assigned in that donated arc, transfers control of that arc to IANA, and establishes IANA allocation policies for any future assignments within that arc.

2. Subordinate Object Identifier Arcs

Thirteen subordinate object identifier arcs were used, numbered from zero to twelve. They were assigned as follows:

```
-- ASN.1 modules
id-mod  OBJECT IDENTIFIER ::= { id-smime  0 }

-- Cryptographic Message Syntax (CMS) content types
id-ct   OBJECT IDENTIFIER ::= { id-smime  1 }

-- attributes
id-aa   OBJECT IDENTIFIER ::= { id-smime  2 }

-- algorithm identifiers
id-alg  OBJECT IDENTIFIER ::= { id-smime  3 }

-- certificate distribution
id-cd   OBJECT IDENTIFIER ::= { id-smime  4 }

-- signature policy qualifier
id-spq  OBJECT IDENTIFIER ::= { id-smime  5 }

-- commitment type identifier
id-cti  OBJECT IDENTIFIER ::= { id-smime  6 }

-- test security policies
id-tsp  OBJECT IDENTIFIER ::= { id-smime  7 }

-- symmetric key distribution control attributes
id-skd  OBJECT IDENTIFIER ::= { id-smime  8 }

-- signature type identifier
id-sti  OBJECT IDENTIFIER ::= { id-smime  9 }

-- encoded information types
id-eit  OBJECT IDENTIFIER ::= { id-smime 10 }

 -- S/MIME capabilities
id-cap  OBJECT IDENTIFIER ::= { id-smime 11 }

-- PSKC attributes
id-pskc OBJECT IDENTIFIER ::= { id-smime 12 }
```

The values assigned in each of these subordinate object identifier arcs are discussed in the next section.

3. IANA Considerations

IANA is asked to update one registry table and create fourteen additional tables.

Updates to the new tables require both Specification Required and Expert Review as defined in [RFC5226]. The expert is expected to ensure that any new values are strongly related to the work that was done by the S/MIME Mail Security Working Group; examples include content types, attributes, and identifiers for algorithms used with S/MIME and CMS. Object identifiers for other purposes should not be assigned in this arc.

3.1. Update to "SMI Security for Mechanism Codes" Registry

The "SMI Security for Mechanism Codes" table generally contains entries with a positive integer value, but the value donated by RSA Data Security cannot be described in this manner. An accompanying table is needed with this entry:

OID Value	Name	Description	References
1.2.840.113549.1.9.16	smime	S/MIME Mail Security	This RFC

3.2. "SMI Security for S/MIME Mail Security" Registry

Within the SMI-numbers registry, add an "SMI Security for S/MIME Mail Security (1.2.840.113549.1.9.16)" table with three columns:

Decimal	Description	References
0	Module identifiers	This RFC
1	CMS content types	This RFC
2	Attributes	This RFC
3	Algorithm identifiers	This RFC
4	Certificate distribution	This RFC
5	Signature policy qualifiers	This RFC
6	Commitment type identifiers	This RFC
7	Test security policies	This RFC
8	Symmetric key dist ctrl attrs	This RFC
9	Signature type identifiers	This RFC
10	Encoded information types	This RFC
11	S/MIME capabilities	This RFC
12	PSKC attributes	This RFC

Future updates to this table require both Specification Required and Expert Review as defined in [RFC5226].

3.3. "SMI Security for S/MIME Module Identifier" Registry

Within the SMI-numbers registry, add an "SMI Security for S/MIME Module Identifier (1.2.840.113549.1.9.16.0)" table with three columns:

Decimal	Description	References
1	id-mod-cms	[RFC2630]
2	id-mod-ess	[RFC2634]
3	id-mod-oid	Reserved and Obsolete
4	id-mod-msg-v3	[RFC2633]
5	id-mod-ets-eSignature-88	[RFC3126]
6	id-mod-ets-eSignature-97	[RFC3126]
7	id-mod-ets-eSigPolicy-88	[RFC3125]
8	id-mod-ets-eSigPolicy-97	[RFC3125]
9	id-mod-certdist	Reserved and Obsolete
10	id-mod-domsec	[RFC3183]
11	id-mod-compress	[RFC3274]
12	id-mod-symkeydist	[RFC5275]
13	id-mod-cek-reuse	[RFC3185]
14	id-mod-cms-2001	[RFC3369]
15	id-mod-v1AttrCert	[RFC3369]
16	id-mod-cmsalg-2001	[RFC3370]
17	id-mod-cms-pwri-88	[RFC3211]
18	id-mod-cms-pwri-97	[RFC3211]
19	id-mod-cms-aes	[RFC3565]
20	id-mod-cms-rsaes-oaep	[RFC3560]
21	id-mod-msg-v3dot1	[RFC3851]
22	id-mod-cms-firmware-wrap	[RFC4108]
23	id-mod-cms-camellia	[RFC3657]
24	id-mod-cms-2004	[RFC3852]
25	id-mod-cms-seed	[Err3865]
26	id-mod-contentCollection	[RFC4073]
27	id-mod-binarySigningTime	[RFC4049]
28	id-mod-ets-eSignature-explicitSyntax88	[RFC5126]
29	id-mod-ets-eSignature-explicitSyntax97	[RFC5126]
30	id-mod-ess-2006	[RFC5035]
31	id-mod-cms-authEnvelopedData	[RFC5083]
32	id-mod-cms-aes-ccm-and-gcm	[RFC5084]
33	id-mod-symmetricKeyPkgV1	[RFC6031]
34	id-mod-multipleSig-2008	[RFC5752]
35	id-mod-timestampedData	[RFC5544]
36	id-mod-symkeydist-02	[RFC5911]
37	id-mod-cmsalg-2001-02	[RFC5911]

38	id-mod-cms-aes-02	[RFC5911]
39	id-mod-msg-v3dot1-02	[RFC5911]
40	id-mod-cms-firmware-wrap-02	[RFC5911]
41	id-mod-cms-2004-02	[RFC5911]
42	id-mod-ess-2006-02	[RFC5911]
43	id-mod-cms-authEnvelopedData-02	[RFC5911]
44	id-mod-cms-aes-ccm-gcm-02	[RFC5911]
45	id-mod-cms-ecc-alg-2009-88	[RFC5753]
46	id-mod-cms-ecc-alg-2009-02	[RFC5753]
47	id-mod-aesKeyWrapWithPad-88	[RFC5649]
48	id-mod-aesKeyWrapWithPad-02	[RFC5649]
49	id-mod-MD5-XOR-EXPERIMENT	[Err3866]
50	id-mod-asymmetricKeyPkgV1	[RFC5958]
51	id-mod-encryptedKeyPkgV1	[RFC6032]
52	id-mod-cms-algorithmProtect	[RFC6211]
53	id-mod-pskcAttributesModule	[RFC6031]
54	id-mod-compressedDataContent	[RFC6268]
55	id-mod-binSigningTime-2009	[RFC6268]
56	id-mod-contentCollect-2009	[RFC6268]
57	id-mod-cmsAuthEnvData-2009	[RFC6268]
58	id-mod-cms-2009	[RFC6268]
59	id-mod-multipleSign-2009	[RFC6268]
60	id-mod-rpkiManifest	[RFC6486]
61	id-mod-rpkiROA	[RFC6482]
62	id-mod-setKeyAttributeV1	[SET-KEY]
63	id-mod-keyPkgReceiptAndErrV2	[CMS-TYPES]
64	id-mod-mts-hashsig-2013	[MTS-in-CMS]

Future updates to this table require both Specification Required and Expert Review as defined in [RFC5226].

3.4. "SMI Security for S/MIME CMS Content Type" Registry

Within the SMI-numbers registry, add an "SMI Security for S/MIME CMS Content Type (1.2.840.113549.1.9.16.1)" table with three columns:

Decimal	Description	References
0	id-ct-anyContentType	[RFC6010]
1	id-ct-receipt	[RFC2634]
2	id-ct-authData	[RFC2630]
3	id-ct-publishCert	Reserved and Obsolete
4	id-ct-TSTInfo	[RFC3161]
5	id-ct-TDTInfo	Reserved and Obsolete
6	id-ct-contentInfo	[RFC2630]
7	id-ct-DVCSRequestData	[RFC3029]
8	id-ct-DVCSResponseData	[RFC3029]
9	id-ct-compressedData	[RFC3274]

10	id-ct-scvp-certValRequest	[RFC5055]
11	id-ct-scvp-certValResponse	[RFC5055]
12	id-ct-scvp-valPolRequest	[RFC5055]
13	id-ct-scvp-valPolResponse	[RFC5055]
14	id-ct-attrCertEncAttrs	[RFC5755]
15	id-ct-TSReq	Reserved and Obsolete
16	id-ct-firmwarePackage	[RFC4108]
17	id-ct-firmwareLoadReceipt	[RFC4108]
18	id-ct-firmwareLoadError	[RFC4108]
19	id-ct-contentCollection	[RFC4073]
20	id-ct-contentWithAttrs	[RFC4073]
21	id-ct-encKeyWithID	[RFC4211]
22	id-ct-encPEPSI	Reserved and Obsolete
23	id-ct-authEnvelopedData	[RFC5083]
24	id-ct-routeOriginAuthz	[RFC6482]
25	id-ct-KP-sKeyPackage	[RFC6031]
26	id-ct-rpkiManifest	[RFC6486]
27	id-ct-asciiTextWithCRLF	[RFC5485]
28	id-ct-xml	[RFC5485]
29	id-ct-pdf	[RFC5485]
30	id-ct-postscript	[RFC5485]
31	id-ct-timestampedData	[RFC5544]
32	id-ct-ASAdjacencyAttest	Reserved and Obsolete
33	id-ct-rpkiTrustAnchor	Reserved and Obsolete
34	id-ct-trustAnchorList	[RFC5914]
35	id-ct-rpkiGhostbusters	[RFC6493]
36	id-ct-resourceTaggedAttest	Reserved and Obsolete

Future updates to this table require both Specification Required and Expert Review as defined in [RFC5226].

3.5. "SMI Security for S/MIME Attributes" Registry

Within the SMI-numbers registry, add an "SMI Security for S/MIME Attributes (1.2.840.113549.1.9.16.2)" table with three columns:

Decimal	Description	References
1	id-aa-receiptRequest	[RFC2634]
2	id-aa-securityLabel	[RFC2634]
3	id-aa-mlExpandHistory	[RFC2634]
4	id-aa-contentHint	[RFC2634]
5	id-aa-msgSigDigest	[RFC2634]
6	id-aa-encapContentType	Reserved and Obsolete
7	id-aa-contentIdentifier	[RFC2634]
8	id-aa-macValue	Reserved and Obsolete
9	id-aa-equivalentLabels	[RFC2634]
10	id-aa-contentReference	[RFC2634]

11	id-aa-encrypKeyPref	[RFC2633]
12	id-aa-signingCertificate	[RFC2634]
13	id-aa-smimeEncryptCerts	Reserved and Obsolete
14	id-aa-signatureTimeStampToken	[RFC3126]
15	id-aa-ets-sigPolicyId	[RFC3126]
16	id-aa-ets-commitmentType	[RFC3126]
17	id-aa-ets-signerLocation	[RFC3126]
18	id-aa-ets-signerAttr	[RFC3126]
19	id-aa-ets-otherSigCert	[RFC3126]
20	id-aa-ets-contentTimestamp	[RFC3126]
21	id-aa-ets-CertificateRefs	[RFC3126]
22	id-aa-ets-RevocationRefs	[RFC3126]
23	id-aa-ets-certValues	[RFC3126]
24	id-aa-ets-revocationValues	[RFC3126]
25	id-aa-ets-escTimeStamp	[RFC3126]
26	id-aa-ets-certCRLTimestamp	[RFC3126]
27	id-aa-ets-archiveTimeStamp	[RFC3126]
28	id-aa-signatureType	[Err3757]
29	id-aa-dvcs-dvc	[RFC3029]
30	id-aa-CEKReference	[RFC3185]
31	id-aa-CEKMaxDecrypts	[RFC3185]
32	id-aa-KEKDerivationAlg	[RFC3185]
33	id-aa-intendedRecipients	Reserved and Obsolete
34	id-aa-cmc-unsignedData	[RFC5272]
35	id-aa-firmwarePackageID	[RFC4108]
36	id-aa-targetHardwareIDs	[RFC4108]
37	id-aa-decryptKeyID	[RFC4108]
38	id-aa-implCryptoAlgs	[RFC4108]
39	id-aa-wrappedFirmwareKey	[RFC4108]
40	id-aa-communityIdentifiers	[RFC4108]
41	id-aa-fwPkgMessageDigest	[RFC4108]
42	id-aa-firmwarePackageInfo	[RFC4108]
43	id-aa-implCompressAlgs	[RFC4108]
44	id-aa-ets-attrCertificateRefs	[RFC5126]
45	id-aa-ets-attrRevocationRefs	[RFC5126]
46	id-aa-binarySigningTime	[RFC4049]
47	id-aa-signingCertificateV2	[RFC5035]
48	id-aa-ets-archiveTimeStampV2	[RFC5126]
49	id-aa-er-internal	[RFC4998]
50	id-aa-er-external	[RFC4998]
51	id-aa-multipleSignatures	[RFC5752]
52	id-aa-cmsAlgorithmProtect	[RFC6211]
53	id-aa-setKeyInformation	[SET-KEY]
54	id-aa-asymmDecryptKeyID	[RFC7030]

Future updates to this table require both Specification Required and Expert Review as defined in [RFC5226].

3.6. "SMI Security for S/MIME Algorithms" Registry

Within the SMI-numbers registry, add an "SMI Security for S/MIME Algorithms (1.2.840.113549.1.9.16.3)" table with three columns:

Decimal	Description	References
1	id-alg-ESDHwith3DES	Reserved and Obsolete
2	id-alg-ESDHwithRC2	Reserved and Obsolete
3	id-alg-3DESwrap	Reserved and Obsolete
4	id-alg-RC2wrap	Reserved and Obsolete
5	id-alg-ESDH	[RFC2630]
6	id-alg-CMS3DESwrap	[RFC2630]
7	id-alg-CMSRC2wrap	[RFC2630]
8	id-alg-zLibCompress	[RFC3274]
9	id-alg-PWRI-KEK	[RFC3211]
10	id-alg-SSDH	[RFC3370]
11	id-alg-HMACwith3DESwrap	[RFC3537]
12	id-alg-HMACwithAESwrap	[RFC3537]
13	id-alg-MD5-XOR-EXPERIMENT	[RFC6210]
14	id-alg-rsa-kem	[RFC5990]
15	id-alg-authEnc-128	[RFC6476]
16	id-alg-authEnc-256	[RFC6476]
17	id-alg-mts-hashsig	[MTS-in-CMS]

Future updates to this table require both Specification Required and Expert Review as defined in [RFC5226].

3.7. "SMI Security for S/MIME Certificate Distribution Mechanisms" Registry

Within the SMI-numbers registry, add an "SMI Security for S/MIME Certificate Distribution Mechanisms (1.2.840.113549.1.9.16.4)" table with three columns:

Decimal	Description	References
1	id-cd-ldap	Reserved and Obsolete

Future updates to this table require both Specification Required and Expert Review as defined in [RFC5226].

3.8. "SMI Security for S/MIME Signature Policy Qualifier" Registry

Within the SMI-numbers registry, add an "SMI Security for S/MIME Signature Policy Qualifier (1.2.840.113549.1.9.16.5)" table with three columns:

Decimal	Description	References
1	id-spq-ets-uri	[RFC3126]
2	id-spq-ets-unotice	[RFC3126]

Future updates to this table require both Specification Required and Expert Review as defined in [RFC5226].

3.9. "SMI Security for S/MIME Commitment Type Identifier" Registry

Within the SMI-numbers registry, add an "SMI Security for S/MIME Commitment Type Identifier (1.2.840.113549.1.9.16.6)" table with three columns:

Decimal	Description	References
1	id-cti-ets-proofOfOrigin	[RFC3126]
2	id-cti-ets-proofOfReceipt	[RFC3126]
3	id-cti-ets-proofOfDelivery	[RFC3126]
4	id-cti-ets-proofOfSender	[RFC3126]
5	id-cti-ets-proofOfApproval	[RFC3126]
6	id-cti-ets-proofOfCreation	[RFC3126]

Future updates to this table require both Specification Required and Expert Review as defined in [RFC5226].

3.10. "SMI Security for S/MIME Test Security Policies" Registry

Within the SMI-numbers registry, add an "SMI Security for S/MIME Test Security Policies (1.2.840.113549.1.9.16.7)" table with three columns:

Decimal	Description	References
1	id-tsp-TEST-Amoco	[RFC3114]
2	id-tsp-TEST-Caterpillar	[RFC3114]
3	id-tsp-TEST-Whirlpool	[RFC3114]
4	id-tsp-TEST-Whirlpool-Categories	[RFC3114]

Future updates to this table require both Specification Required and Expert Review as defined in [RFC5226].

3.11. "SMI Security for S/MIME Control Attributes for Symmetric Key Distribution" Registry

Within the SMI-numbers registry, add an "SMI Security for S/MIME Control Attributes for Symmetric Key Distribution (1.2.840.113549.1.9.16.8)" table with three columns:

Decimal	Description	References
1	id-skd-glUseKEK	[RFC5275]
2	id-skd-glDelete	[RFC5275]
3	id-skd-glAddMember	[RFC5275]
4	id-skd-glDeleteMember	[RFC5275]
5	id-skd-glRekey	[RFC5275]
6	id-skd-glAddOwner	[RFC5275]
7	id-skd-glRemoveOwner	[RFC5275]
8	id-skd-glKeyCompromise	[RFC5275]
9	id-skd-glkRefresh	[RFC5275]
10	id-skd-glFailInfo	Reserved and Obsolete
11	id-skd-glaQueryRequest	[RFC5275]
12	id-skd-glaQueryResponse	[RFC5275]
13	id-skd-glProvideCert	[RFC5275]
14	id-skd-glManageCert	[RFC5275]
15	id-skd-glKey	[RFC5275]

Future updates to this table require both Specification Required and Expert Review as defined in [RFC5226].

3.12. "SMI Security for S/MIME Signature Type Identifiers" Registry

Within the SMI-numbers registry, add an "SMI Security for S/MIME Signature Type Identifiers (1.2.840.113549.1.9.16.9)" table with three columns:

Decimal	Description	References
1	id-sti-originatorSig	[RFC3183]
2	id-sti-domainSig	[RFC3183]
3	id-sti-addAttribSig	[RFC3183]
4	id-sti-reviewSig	[RFC3183]

Future updates to this table require both Specification Required and Expert Review as defined in [RFC5226].

3.13. "SMI Security for S/MIME X.400 Encoded Information Types (EIT) for S/MIME objects" Registry

Within the SMI-numbers registry, add an "SMI Security for X.400 Encoded Information Types (EIT) for S/MIME objects (1.2.840.113549.1.9.16.10)" table with three columns:

Decimal	Description	References
1	id-eit-envelopedData	[RFC3855]
2	id-eit-signedData	[RFC3855]
3	id-eit-certsOnly	[RFC3855]
4	id-eit-signedReceipt	[RFC3855]
5	id-eit-envelopedX400	[RFC3855]
6	id-eit-signedX400	[RFC3855]
7	id-eit-compressedData	[RFC3855]

Future updates to this table require both Specification Required and Expert Review as defined in [RFC5226].

3.14. "SMI Security for S/MIME Capabilities (other than cryptographic algorithms)" Registry

Within the SMI-numbers registry, add an "SMI Security for S/MIME Capabilities (other than cryptographic algorithms) (1.2.840.113549.1.9.16.11)" table with three columns:

Decimal	Description	References
1	id-cap-preferBinaryInside	[RFC3851]

Future updates to this table require both Specification Required and Expert Review as defined in [RFC5226].

3.15. "SMI Security for S/MIME Portable Symmetric Key Container (PSKC) Attributes" Registry

Within the SMI-numbers registry, add an "SMI Security for S/MIME Portable Symmetric Key Container (PSKC) Attributes (1.2.840.113549.1.9.16.12)" table with three columns:

Decimal	Description	References
1	id-pskc-manufacturer	[RFC6031]
2	id-pskc-serialNo	[RFC6031]
3	id-pskc-model	[RFC6031]
4	id-pskc-issueNo	[RFC6031]
5	id-pskc-deviceBinding	[RFC6031]

6	id-pskc-deviceStartDate	[RFC6031]
7	id-pskc-deviceExpiryDate	[RFC6031]
8	id-pskc-moduleId	[RFC6031]
9	id-pskc-keyId	[RFC6031]
10	id-pskc-algorithm	[RFC6031]
11	id-pskc-issuer	[RFC6031]
12	id-pskc-keyProfileId	[RFC6031]
13	id-pskc-keyReference	[RFC6031]
14	id-pskc-friendlyName	[RFC6031]
15	id-pskc-algorithmParams	[RFC6031]
16	id-pskc-counter	[RFC6031]
17	id-pskc-time	[RFC6031]
18	id-pskc-timeInterval	[RFC6031]
19	id-pskc-timeDrift	[RFC6031]
20	id-pskc-valueMAC	[RFC6031]
21	id-pskc-keyStartDate	[RFC6031]
22	id-pskc-keyExpiryDate	[RFC6031]
23	id-pskc-noOfTransactions	[RFC6031]
24	id-pskc-keyUsages	[RFC6031]
25	id-pskc-pinPolicy	[RFC6031]
26	id-pskc-deviceUserId	[RFC6031]
27	id-pskc-keyUserId	[RFC6031]

Future updates to this table require both Specification Required and Expert Review as defined in [RFC5226].

4. Security Considerations

This document populates an IANA registry, and it raises no new security considerations. The protocols that specify these values include the security considerations associated with their usage.

5. References

5.1. Normative References

[ASN1-08] International Telecommunication Union, "Abstract Syntax Notation One (ASN.1): Specification of basic notation", ITU-T Recommendation X.680, 2008.

[ASN1-88] International Telephone and Telegraph Consultative Committee, "Specification of Abstract Syntax Notation One (ASN.1)", CCITT Recommendation X.208, 1988.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

5.2. Informative References

[CMS-TYPES] Housley, R., "Cryptographic Message Syntax (CMS) Key Package Receipt and Error Content Types", Work in Progress, December 2013.

[Err3757] RFC Errata, Errata ID 3757, RFC 3183, <http://www.rfc-editor.org>.

[Err3865] RFC Errata, Errata ID 3865, RFC 4010, <http://www.rfc-editor.org>.

[Err3866] RFC Errata, Errata ID 3866, RFC 6210, <http://www.rfc-editor.org>.

[MTS-in-CMS] Housley, R., "Use of the Hash-based Merkle Tree Signature (MTS) Algorithm in the Cryptographic Message Syntax (CMS)", Work in Progress, August 2013.

[RFC2630] Housley, R., "Cryptographic Message Syntax", RFC 2630, June 1999.

[RFC2633] Ramsdell, B., Ed., "S/MIME Version 3 Message Specification", RFC 2633, June 1999.

[RFC2634] Hoffman, P., Ed., "Enhanced Security Services for S/MIME", RFC 2634, June 1999.

[RFC3029] Adams, C., Sylvester, P., Zolotarev, M., and R. Zuccherato, "Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols", RFC 3029, February 2001.

[RFC3114] Nicolls, W., "Implementing Company Classification Policy with the S/MIME Security Label", RFC 3114, May 2002.

[RFC3125] Ross, J., Pinkas, D., and N. Pope, "Electronic Signature Policies", RFC 3125, September 2001.

[RFC3126] Pinkas, D., Ross, J., and N. Pope, "Electronic Signature Formats for long term electronic signatures", RFC 3126, September 2001.

[RFC3161] Adams, C., Cain, P., Pinkas, D., and R. Zuccherato, "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)", RFC 3161, August 2001.

[RFC3183] Dean, T. and W. Ottaway, "Domain Security Services using S/MIME", RFC 3183, October 2001.

[RFC3185] Farrell, S. and S. Turner, "Reuse of CMS Content Encryption Keys", RFC 3185, October 2001.

[RFC3211] Gutmann, P., "Password-based Encryption for CMS", RFC 3211, December 2001.

[RFC3274] Gutmann, P., "Compressed Data Content Type for Cryptographic Message Syntax (CMS)", RFC 3274, June 2002.

[RFC3369] Housley, R., "Cryptographic Message Syntax (CMS)", RFC 3369, August 2002.

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

[RFC3537] Schaad, J. and R. Housley, "Wrapping a Hashed Message Authentication Code (HMAC) key with a Triple-Data Encryption Standard (DES) Key or an Advanced Encryption Standard (AES) Key", RFC 3537, May 2003.

[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.

[RFC3851] Ramsdell, B., Ed., "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification", RFC 3851, July 2004.

[RFC3852] Housley, R., "Cryptographic Message Syntax (CMS)", RFC 3852, July 2004.

[RFC3855] Hoffman, P. and C. Bonatti, "Transporting Secure/Multipurpose Internet Mail Extensions (S/MIME) Objects in X.400", RFC 3855, July 2004.

[RFC4049] Housley, R., "BinaryTime: An Alternate Format for Representing Date and Time in ASN.1", RFC 4049, April 2005.

[RFC4073] Housley, R., "Protecting Multiple Contents with the Cryptographic Message Syntax (CMS)", RFC 4073, May 2005.

[RFC4108] Housley, R., "Using Cryptographic Message Syntax (CMS) to Protect Firmware Packages", RFC 4108, August 2005.

[RFC4211] Schaad, J., "Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)", RFC 4211, September 2005.

[RFC4998] Gondrom, T., Brandner, R., and U. Pordesch, "Evidence Record Syntax (ERS)", RFC 4998, August 2007.

[RFC5035] Schaad, J., "Enhanced Security Services (ESS) Update: Adding CertID Algorithm Agility", RFC 5035, August 2007.

[RFC5055] Freeman, T., Housley, R., Malpani, A., Cooper, D., and W. Polk, "Server-Based Certificate Validation Protocol (SCVP)", RFC 5055, December 2007.

[RFC5083] Housley, R., "Cryptographic Message Syntax (CMS) Authenticated-Enveloped-Data Content Type", RFC 5083, November 2007.

[RFC5084] Housley, R., "Using AES-CCM and AES-GCM Authenticated Encryption in the Cryptographic Message Syntax (CMS)", RFC 5084, November 2007.

[RFC5126] Pinkas, D., Pope, N., and J. Ross, "CMS Advanced Electronic Signatures (CAdES)", RFC 5126, March 2008.

[RFC5272] Schaad, J. and M. Myers, "Certificate Management over CMS (CMC)", RFC 5272, June 2008.

[RFC5275] Turner, S., "CMS Symmetric Key Management and Distribution", RFC 5275, June 2008.

[RFC5485] Housley, R., "Digital Signatures on Internet-Draft Documents", RFC 5485, March 2009.

[RFC5544] Santoni, A., "Syntax for Binding Documents with Time-Stamps", RFC 5544, February 2010.

[RFC5649] Housley, R. and M. Dworkin, "Advanced Encryption Standard (AES) Key Wrap with Padding Algorithm", RFC 5649, September 2009.

[RFC5752] Turner, S. and J. Schaad, "Multiple Signatures in Cryptographic Message Syntax (CMS)", RFC 5752, January 2010.

[RFC5753] Turner, S. and D. Brown, "Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS)", RFC 5753, January 2010.

[RFC5755] Farrell, S., Housley, R., and S. Turner, "An Internet Attribute Certificate Profile for Authorization", RFC 5755, January 2010.

[RFC5911] Hoffman, P. and J. Schaad, "New ASN.1 Modules for Cryptographic Message Syntax (CMS) and S/MIME", RFC 5911, June 2010.

[RFC5914] Housley, R., Ashmore, S., and C. Wallace, "Trust Anchor Format", RFC 5914, June 2010.

[RFC5958] Turner, S., "Asymmetric Key Packages", RFC 5958, August 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.

[RFC6010] Housley, R., Ashmore, S., and C. Wallace, "Cryptographic Message Syntax (CMS) Content Constraints Extension", RFC 6010, September 2010.

[RFC6031] Turner, S. and R. Housley, "Cryptographic Message Syntax (CMS) Symmetric Key Package Content Type", RFC 6031, December 2010.

[RFC6032] Turner, S. and R. Housley, "Cryptographic Message Syntax (CMS) Encrypted Key Package Content Type", RFC 6032, December 2010.

[RFC6210] Schaad, J., "Experiment: Hash Functions with Parameters in the Cryptographic Message Syntax (CMS) and S/MIME", RFC 6210, April 2011.

[RFC6211] Schaad, J., "Cryptographic Message Syntax (CMS) Algorithm Identifier Protection Attribute", RFC 6211, April 2011.

[RFC6268] Schaad, J. and S. Turner, "Additional New ASN.1 Modules for the Cryptographic Message Syntax (CMS) and the Public Key Infrastructure Using X.509 (PKIX)", RFC 6268, July 2011.

[RFC6476] Gutmann, P., "Using Message Authentication Code (MAC) Encryption in the Cryptographic Message Syntax (CMS)", RFC 6476, January 2012.

[RFC6482] Lepinski, M., Kent, S., and D. Kong, "A Profile for Route Origin Authorizations (ROAs)", RFC 6482, February 2012.

[RFC6486] Austein, R., Huston, G., Kent, S., and M. Lepinski, "Manifests for the Resource Public Key Infrastructure (RPKI)", RFC 6486, February 2012.

[RFC6493] Bush, R., "The Resource Public Key Infrastructure (RPKI) Ghostbusters Record", RFC 6493, February 2012.

[RFC7030] Pritikin, M., Ed., Yee, P., Ed., and D. Harkins, Ed., "Enrollment over Secure Transport", RFC 7030, October 2013.

[SET-KEY] Herzog, J. and R. Khazan, "A set-key attribute for symmetric-key packages", Work in Progress, October 2012.

6. Acknowledgements

Many thanks to Suresh Krishnan, Jim Schaad, Sean Turner, and Carl Wallace for their careful review and comments.

Author’s Address

Russ Housley
918 Spring Knoll Drive
Herndon, VA 20170
USA

EMail: housley@vigilsec.com