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.

Copyright Notice

Copyright (c) 2014 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 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

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:

```plaintext
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:

<table>
<thead>
<tr>
<th>OID Value</th>
<th>Name</th>
<th>Description</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2.840.113549.1.9.16</td>
<td>smime</td>
<td>S/MIME Mail Security</td>
<td>This RFC</td>
</tr>
</tbody>
</table>

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:

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

Housley   Informational   [Page 4]
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:

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

<table>
<thead>
<tr>
<th>Decimal</th>
<th>Description</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>id-ct-anyContentType</td>
<td>[RFC6010]</td>
</tr>
<tr>
<td>1</td>
<td>id-ct-receipt</td>
<td>[RFC2634]</td>
</tr>
<tr>
<td>2</td>
<td>id-ct-authData</td>
<td>[RFC2630]</td>
</tr>
<tr>
<td>3</td>
<td>id-ct-publishCert</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>id-ct-TSTInfo</td>
<td>[RFC3161]</td>
</tr>
<tr>
<td>5</td>
<td>id-ct-TDTInfo</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>id-ct-contentInfo</td>
<td>[RFC2630]</td>
</tr>
<tr>
<td>7</td>
<td>id-ct-DVCSRequestData</td>
<td>[RFC3029]</td>
</tr>
<tr>
<td>8</td>
<td>id-ct-DVCSResponseData</td>
<td>[RFC3029]</td>
</tr>
<tr>
<td>9</td>
<td>id-ct-compressedData</td>
<td>[RFC3274]</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Decimal</th>
<th>Description</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>id-aa-receiptRequest</td>
<td>RFC2634</td>
</tr>
<tr>
<td>2</td>
<td>id-aa-securityLabel</td>
<td>RFC2634</td>
</tr>
<tr>
<td>3</td>
<td>id-aa-mlExpandHistory</td>
<td>RFC2634</td>
</tr>
<tr>
<td>4</td>
<td>id-aa-contentHint</td>
<td>RFC2634</td>
</tr>
<tr>
<td>5</td>
<td>id-aa-msgSigDigest</td>
<td>RFC2634</td>
</tr>
<tr>
<td>6</td>
<td>id-aa-encapContentType</td>
<td>RFC2634</td>
</tr>
<tr>
<td>7</td>
<td>id-aa-contentIdentifier</td>
<td>RFC2634</td>
</tr>
<tr>
<td>8</td>
<td>id-aa-macValue</td>
<td>RFC2634</td>
</tr>
<tr>
<td>9</td>
<td>id-aa-equivalentLabels</td>
<td>RFC2634</td>
</tr>
<tr>
<td>10</td>
<td>id-aa-contentReference</td>
<td>RFC2634</td>
</tr>
</tbody>
</table>

Future updates to this table require both Specification Required and Expert Review as defined in [RFC5226].
11 id-aa-encKeyPref [RFC2633]
12 id-aa-signCert
13 id-aa-smimeEncryptCerts [Reserved and Obsolete]
14 id-aa-signTime
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-escTime
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-cekMaxDecr
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-asymmDecrypKeyID [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:

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

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


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:

<table>
<thead>
<tr>
<th>Decimal</th>
<th>Description</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>id-cd-ldap</td>
<td>Reserved and Obsolete</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Decimal</th>
<th>Description</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>id-spq-ets-uri</td>
<td>[RFC3126]</td>
</tr>
<tr>
<td>2</td>
<td>id-spq-ets-unotice</td>
<td>[RFC3126]</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Decimal</th>
<th>Description</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>id-cti-ets-proofOfOrigin</td>
<td>[RFC3126]</td>
</tr>
<tr>
<td>2</td>
<td>id-cti-ets-proofOfReceipt</td>
<td>[RFC3126]</td>
</tr>
<tr>
<td>3</td>
<td>id-cti-ets-proofOfDelivery</td>
<td>[RFC3126]</td>
</tr>
<tr>
<td>4</td>
<td>id-cti-ets-proofOfSender</td>
<td>[RFC3126]</td>
</tr>
<tr>
<td>5</td>
<td>id-cti-ets-proofOfApproval</td>
<td>[RFC3126]</td>
</tr>
<tr>
<td>6</td>
<td>id-cti-ets-proofOfCreation</td>
<td>[RFC3126]</td>
</tr>
</tbody>
</table>

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


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:

<table>
<thead>
<tr>
<th>Decimal</th>
<th>Description</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>id-tsp-TEST-Amoco</td>
<td>[RFC3114]</td>
</tr>
<tr>
<td>2</td>
<td>id-tsp-TEST-Caterpillar</td>
<td>[RFC3114]</td>
</tr>
<tr>
<td>3</td>
<td>id-tsp-TEST-Whirlpool</td>
<td>[RFC3114]</td>
</tr>
<tr>
<td>4</td>
<td>id-tsp-TEST-Whirlpool-Categories</td>
<td>[RFC3114]</td>
</tr>
</tbody>
</table>

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:

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

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:

<table>
<thead>
<tr>
<th>Decimal</th>
<th>Description</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>id-sti-originatorSig</td>
<td>[RFC3183]</td>
</tr>
<tr>
<td>2</td>
<td>id-sti-domainSig</td>
<td>[RFC3183]</td>
</tr>
<tr>
<td>3</td>
<td>id-sti-addAttribSig</td>
<td>[RFC3183]</td>
</tr>
<tr>
<td>4</td>
<td>id-sti-reviewSig</td>
<td>[RFC3183]</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Decimal</th>
<th>Description</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>id-eit-envelopedData</td>
<td>[RFC3855]</td>
</tr>
<tr>
<td>2</td>
<td>id-eit-signedData</td>
<td>[RFC3855]</td>
</tr>
<tr>
<td>3</td>
<td>id-eit-certOnly</td>
<td>[RFC3855]</td>
</tr>
<tr>
<td>4</td>
<td>id-eit-signedReceipt</td>
<td>[RFC3855]</td>
</tr>
<tr>
<td>5</td>
<td>id-eit-envelopedX400</td>
<td>[RFC3855]</td>
</tr>
<tr>
<td>6</td>
<td>id-eit-signedX400</td>
<td>[RFC3855]</td>
</tr>
<tr>
<td>7</td>
<td>id-eit-compressedData</td>
<td>[RFC3855]</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Decimal</th>
<th>Description</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>id-cap-preferBinaryInside</td>
<td>[RFC3851]</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Decimal</th>
<th>Description</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>id-pskc-manufacturer</td>
<td>[RFC6031]</td>
</tr>
<tr>
<td>2</td>
<td>id-pskc-serialNo</td>
<td>[RFC6031]</td>
</tr>
<tr>
<td>3</td>
<td>id-pskc-model</td>
<td>[RFC6031]</td>
</tr>
<tr>
<td>4</td>
<td>id-pskc-issuerNo</td>
<td>[RFC6031]</td>
</tr>
<tr>
<td>5</td>
<td>id-pskc-deviceBinding</td>
<td>[RFC6031]</td>
</tr>
</tbody>
</table>
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


5.2. Informative References


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