Internet Engineering Task Force (IETF)
Request for Comments: 7299
Category: Informational
ISSN: 2070-1721

R. Housley
Vigil Security

July 2014

Object Identifier Registry for the PKIX Working Group

Abstract

When the Public-Key Infrastructure using X.509 (PKIX) Working Group was chartered, an object identifier arc was allocated by IANA for use by that working group. This document describes the object identifiers that were assigned in that arc, returns 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/rfc7299.

Table of Contents

1. Introduction 3
2. Subordinate Object Identifier Arcs 3
3. IANA Considerations 6
3.1. Update to "SMI Security for Mechanism Codes" Registry 6
3.2. "SMI Security for PKIX" Registry 6
3.3. "SMI Security for PKIX Module Identifier" Registry 7
3.4. "SMI Security for PKIX Certificate Extension" Registry 9
3.5. "SMI Security for PKIX Policy Qualifier" Registry 10
3.6. "SMI Security for PKIX Extended Key Purpose" Registry 10
3.7. "SMI Security for PKIX CMP Information Types" Registry 11
3.8. "SMI Security for PKIX CRMF Registration" Registry 12
3.9. "SMI Security for PKIX CRMF Registration Controls" Registry 12
3.10. "SMI Security for PKIX CRMF Registration Information" Registry 12
3.11. "SMI Security for PKIX Algorithms" Registry 13
3.12. "SMI Security for PKIX CMC Controls" Registry 13
3.13. "SMI Security for PKIX CMC GLA Requests and Responses" Registry 14
3.14. "SMI Security for PKIX Other Name Forms" Registry 15
3.15. "SMI Security for PKIX Personal Data Attributes" Registry 15
3.16. "SMI Security for PKIX Attribute Certificate Attributes" Registry 16
3.17. "SMI Security for PKIX Qualified Certificate Statements" Registry 16
3.18. "SMI Security for PKIX CMC Content Types" Registry 16
3.19. "SMI Security for PKIX OIDs Used Only for Testing" Registry 17
3.20. "SMI Security for PKIX Certificate Policies" Registry 17
3.21. "SMI Security for PKIX CMC Error Types" Registry 17
3.22. "SMI Security for PKIX Revocation Information Types" Registry 18
3.23. "SMI Security for PKIX SCVP Check Types" Registry 18
3.24. "SMI Security for PKIX SCVP Want Back Types" Registry 19
3.25. "SMI Security for PKIX SCVP Validation Policies and Algorithms" Registry 20
3.26. "SMI Security for PKIX SCVP Name Validation Policy Errors" Registry 20
3.27. "SMI Security for PKIX SCVP Basic Validation Policy Errors" Registry 21
3.28. "SMI Security for PKIX SCVP Distinguished Name Validation Policy Errors" Registry 21
3.29. "SMI Security for PKIX Other Logotype Identifiers" Registry 22

3.30. "SMI Security for PKIX Proxy Certificate Policy Languages" Registry 22
3.31. "SMI Security for PKIX Proxy Matching Rules" Registry 22
3.32. "SMI Security for PKIX Subject Key Identifier Semantics" Registry 23
3.33. "SMI Security for PKIX Access Descriptor" Registry 23
3.34. "SMI Security for PKIX Online Certificate Status Protocol (OCSP)" Registry 24
4. Security Considerations 24
5. References 25
5.1. Normative References 25
5.2. Informative References 25
Acknowledgements 30

1. Introduction

When the Public-Key Infrastructure using X.509 (PKIX) Working Group was chartered, an object identifier arc was allocated by IANA for use by that working group. These object identifiers are primarily used with Abstract Syntax Notation One (ASN.1) [ASN1-88] [ASN1-97] [ASN1-08]. The ASN.1 specifications continue to evolve, but object identifiers can be used with any and all versions of ASN.1.

The PKIX object identifier arc is:

```
id-pkix OBJECT IDENTIFIER ::= { iso(1) identified-organization(3)
            dod(6) internet(1) security(5) mechanisms(5) pkix(7) }
```

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

2. Subordinate Object Identifier Arcs

Twenty-five subordinate object identifier arcs were used, numbered from 0 to 23 and 48. In addition, there are seven subordinate arcs. They were assigned as follows:

```
-- Module identifiers
id-mod  OBJECT IDENTIFIER ::= { id-pkix 0 }

-- PKIX certificate extensions
id-pe   OBJECT IDENTIFIER ::= { id-pkix 1 }

-- Policy qualifier types
id-qt   OBJECT IDENTIFIER ::= { id-pkix 2 }
```

```
   -- Extended key purpose identifiers
   id-kp   OBJECT IDENTIFIER ::= { id-pkix 3 }

   -- CMP information types
   id-it   OBJECT IDENTIFIER ::= { id-pkix 4 }

   -- CRMF registration
   id-pkip OBJECT IDENTIFIER ::= { id-pkix 5 }

   -- CRMF registration controls
   id-regCtrl OBJECT IDENTIFIER ::= { id-pkix 5 1 }

   -- CRMF registration information
   id-regInfo OBJECT IDENTIFIER ::= { id-pkix 5 2 }

   -- Algorithms
   id-alg  OBJECT IDENTIFIER ::= { id-pkix 6 }

   -- CMC controls
   id-cmc  OBJECT IDENTIFIER ::= { id-pkix 7 }

   -- CMC GLA Requests and Responses
   id-cmc-glaRR OBJECT IDENTIFIER ::= { id-pkix 7 99 }

   -- Other name forms
   id-on   OBJECT IDENTIFIER ::= { id-pkix 8 }

   -- Personal data attribute
   id-pda  OBJECT IDENTIFIER ::= { id-pkix 9 }

   -- Attribute certificate attributes
   id-aca  OBJECT IDENTIFIER ::= { id-pkix 10 }

   -- Qualified certificate statements
   id-qcs  OBJECT IDENTIFIER ::= { id-pkix 11 }

   -- CMC content types
   id-cct  OBJECT IDENTIFIER ::= { id-pkix 12 }

   -- OIDs for TESTING ONLY
   id-TEST OBJECT IDENTIFIER ::= { id-pkix 13 }

   -- Certificate policies
   id-cp   OBJECT IDENTIFIER ::= { id-pkix 14 }

   -- CMC error types
   id-cet  OBJECT IDENTIFIER ::= { id-pkix 15 }
```

```
   -- Revocation information types
   id-ri   OBJECT IDENTIFIER ::= { id-pkix 16 }

   -- SCVP check type
   id-sct  OBJECT IDENTIFIER ::= { id-pkix 17 }

   -- SCVP want back types
   id-swb  OBJECT IDENTIFIER ::= { id-pkix 18 }

   -- SCVP validation policies
   id-svp  OBJECT IDENTIFIER ::= { id-pkix 19 }

   -- SCVP name validation policy errors
   id-nvae  OBJECT IDENTIFIER ::= { id-pkix 19 2 }

   -- SCVP basic validation policy errors
   id-bvae  OBJECT IDENTIFIER ::= { id-pkix 19 3 }

   -- SCVP distinguished name validation policy errors
   id-dnvae OBJECT IDENTIFIER ::= { id-pkix 19 4 }

   -- Other logotype identifiers
   id-logo OBJECT IDENTIFIER ::= { id-pkix 20 }

   -- Proxy certificate policy languages
   id-ppl  OBJECT IDENTIFIER ::= { id-pkix 21 }

   -- Matching rules
   id-mr   OBJECT IDENTIFIER ::= { id-pkix 22 }

   -- Subject key identifier semantics
   id-skis OBJECT IDENTIFIER ::= { id-pkix 23 }

   -- Access descriptors
   id-ad   OBJECT IDENTIFIER ::= { id-pkix 48 }

   -- Online Certificate Status Protocol
   id-pkix-ocsp  OBJECT IDENTIFIER ::= { id-pkix 48 1 }
```

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

3. IANA Considerations

IANA has updated one registry table and created 33 additional tables.

Updates to the new tables are to be made according to the Specification Required policy 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 PKIX Working Group. That is, additional object identifiers are to be related to X.509 certificates, X.509 attribute certificates, X.509 certificate revocation lists (CRLs), or protocols associated with them. Object identifiers for other purposes should not be assigned in this arc.

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

The reference for the Public Key Infrastructure using X.509 (PKIX) entry (decimal value 7) has been updated to point to this document.

3.2. "SMI Security for PKIX" Registry

Within the SMI-numbers registry, a "PKIX (1.3.6.1.5.5.7)" table with three columns has been added:

Decimal	Description	References
0	Module identifiers	[RFC7299]
1	PKIX certificate extensions	[RFC7299]
2	Policy qualifier types	[RFC7299]
3	Extended key purpose identifiers	[RFC7299]
4	CMP information types	[RFC7299]
5	CRMF registration	[RFC7299]
6	Algorithms	[RFC7299]
7	CMC controls	[RFC7299]
8	Other name forms	[RFC7299]
9	Personal data attribute	[RFC7299]
10	Attribute certificate attributes	[RFC7299]
11	Qualified certificate statements	[RFC7299]
12	CMC content types	[RFC7299]
13	OIDs for TESTING ONLY	[RFC7299]
14	Certificate policies	[RFC7299]
15	CMC error types	[RFC7299]
16	Revocation information types	[RFC7299]
17	SCVP check type	[RFC7299]
18	SCVP want back types	[RFC7299]
19	SCVP validation policies	[RFC7299]
20	Other logotype identifiers	[RFC7299]

21	Proxy certificate policy languages	[RFC7299]
22	Matching rules	[RFC7299]
23	Subject key identifier semantics	[RFC7299]
48	Access descriptors	[RFC7299]

Future updates to this table are to be made according to the Specification Required policy as defined in [RFC5226].

3.3. "SMI Security for PKIX Module Identifier" Registry

Within the SMI-numbers registry, an "SMI Security for PKIX Module Identifier (1.3.6.1.5.5.7.0)" table with three columns has been added:

Decimal	Description	References
1	id-pkix1-explicit-88	[RFC2459]
2	id-pkix1-implicit-88	[RFC2459]
3	id-pkix1-explicit-93	[RFC2459]
4	id-pkix1-implicit-93	[RFC2459]
5	id-mod-crmf	[RFC2511]
6	id-mod-cmc	[RFC2797]
7	id-mod-kea-profile-88	[RFC2528]
8	id-mod-kea-profile-93	[RFC2528]
9	id-mod-cmp	[RFC2510]
10	id-mod-qualified-cert-88	[RFC3039]
11	id-mod-qualified-cert-93	[RFC3039]
12	id-mod-attribute-cert	[RFC3281]
13	id-mod-tsp	[RFC3161]
14	id-mod-ocsp	[RFC3029]
15	id-mod-dvcs	[RFC3029]
16	id-mod-cmp2000	[RFC4210]
17	id-mod-pkix1-algorithms	[RFC3279]
18	id-mod-pkix1-explicit	[RFC3280]
19	id-mod-pkix1-implicit	[RFC3280]
20	id-mod-user-group	Reserved and Obsolete
21	id-mod-scvp	[RFC5055]
22	id-mod-logotype	[RFC3709]
23	id-mod-cmc2002	[RFC5272]
24	id-mod-wlan-extns	[RFC3770]
25	id-mod-proxy-cert-extns	[RFC3820]
26	id-mod-ac-policies	[RFC4476]
27	id-mod-warranty-extn	[RFC4059]
28	id-mod-perm-id-88	[RFC4043]
29	id-mod-perm-id-93	[RFC4043]
30	id-mod-ip-addr-and-as-ident	[RFC3779]
31	id-mod-qualified-cert	[RFC3739]
32	id-mod-crmf2003	Reserved and Obsolete

33	id-mod-pkix1-rsa-pkalgs	[RFC4055]
34	id-mod-cert-bundle	[RFC4306]
35	id-mod-qualified-cert-97	[RFC3739]
36	id-mod-crmf2005	[RFC4210]
37	id-mod-wlan-extns2005	[RFC4334]
38	id-mod-sim2005	[RFC4683]
39	id-mod-dns-srv-name-88	[RFC4985]
40	id-mod-dns-srv-name-93	[RFC4985]
41	id-mod-cmsContentConstr-88	[RFC6010]
42	id-mod-cmsContentConstr-93	[RFC6010]
43	id-mod-pkixCommon	Reserved and Obsolete
44	id-mod-pkixOtherCerts	[RFC5697]
45	id-mod-pkix1-algorithms2008	[RFC5480]
46	id-mod-clearanceConstraints	[RFC5913]
47	id-mod-attribute-cert-02	[RFC5912]
48	id-mod-ocsp-02	[RFC5912]
49	id-mod-v1AttrCert-02	[RFC5912]
50	id-mod-cmp2000-02	[RFC5912]
51	id-mod-pkix1-explicit-02	[RFC5912]
52	id-mod-scvp-02	[RFC5912]
53	id-mod-cmc2002-02	[RFC5912]
54	id-mod-pkix1-rsa-pkalgs-02	[RFC5912]
55	id-mod-crmf2005-02	[RFC5912]
56	id-mod-pkix1-algorithms2008-02	[RFC5912]
57	id-mod-pkixCommon-02	[RFC5912]
58	id-mod-algorithmInformation-02	[RFC5912]
59	id-mod-pkix1-implicit-02	[RFC5912]
60	id-mod-pkix1-x400address-02	[RFC5912]
61	id-mod-attribute-cert-v2	[RFC5755]
62	id-mod-sip-domain-extns2007	[RFC5924]
63	id-mod-cms-otherRIs-2009-88	[RFC5940]
64	id-mod-cms-otherRIs-2009-93	[RFC5940]
65	id-mod-ecprivatekey	[RFC5915]
66	id-mod-ocsp-agility-2009-93	[RFC6277]
67	id-mod-ocsp-agility-2009-88	[RFC6277]
68	id-mod-logotype-certimage	[RFC6170]
69	id-mod-pkcs10-2009	[RFC5912]
70	id-mod-dns-resource-record	[Ableу]
71	id-mod-send-cert-extns	[RFC6494]
72	id-mod-ip-addr-and-as-ident-2	[RFC6268]
73	id-mod-wlan-extns-2	[RFC6268]
74	id-mod-hmac	[RFC6268]
75	id-mod-enrollMsgSyntax-2011-88	[RFC6402] [Err3860]
76	id-mod-enrollMsgSyntax-2011-08	[RFC6402]
77	id-mod-pubKeySMIMECaps-88	[RFC6664]
78	id-mod-pubKeySMIMECaps-08	[RFC6664]
79	id-mod-dhSign-2012-88	[RFC6955]
80	id-mod-dhSign-2012-08	[RFC6955]

81	id-mod-ocsp-2013-88	[RFC6960]
82	id-mod-ocsp-2013-08	[RFC6960]
83	id-mod-TEST-certPolicies	[RFC7229]
84	id-mod-bgpsec-eku	[BGPSEC]

Future updates to this table are to be made according to the Specification Required policy as defined in [RFC5226].

3.4. "SMI Security for PKIX Certificate Extension" Registry

Within the SMI-numbers registry, an "SMI Security for PKIX Certificate Extension (1.3.6.1.5.5.7.1)" table with three columns has been added:

Decimal	Description	References
1	id-pe-authorityInfoAccess	[RFC2459]
2	id-pe-biometricInfo	[RFC3039]
3	id-pe-qcStatements	[RFC3039]
4	id-pe-ac-auditIdentity	[RFC3281]
5	id-pe-ac-targeting	Reserved and Obsolete
6	id-pe-aaControls	[RFC3281]
7	id-pe-ipAddrBlocks	[RFC3779]
8	id-pe-autonomousSysIds	[RFC3779]
9	id-pe-sbgp-routerIdentifier	Reserved and Obsolete
10	id-pe-ac-proxying	[RFC3281]
11	id-pe-subjectInfoAccess	[RFC3280]
12	id-pe-logotype	[RFC3709]
13	id-pe-wlanSSID	[RFC4334]
14	id-pe-proxyCertInfo	[RFC3820]
15	id-pe-acPolicies	[RFC4476]
16	id-pe-warranty	[RFC4059]
17	id-pe-sim	Reserved and Obsolete
18	id-pe-cmsContentConstraints	[RFC6010]
19	id-pe-otherCerts	[RFC5697]
20	id-pe-wrappedApexContinKey	[RFC5934]
21	id-pe-clearanceConstraints	[RFC5913]
22	id-pe-skiSemantics	Reserved and Obsolete
23	id-pe-nsa	[RFC7169]

Future updates to this table are to be made according to the Specification Required policy as defined in [RFC5226].

3.5. "SMI Security for PKIX Policy Qualifier" Registry

Within the SMI-numbers registry, an "SMI Security for PKIX Policy Qualifier Identifiers (1.3.6.1.5.5.7.2)" table with three columns has been added:

Decimal	Description	References
1	id-qt-cps	[RFC2459]
2	id-qt-unotice	[RFC2459]
3	id-qt-textNotice	Reserved and Obsolete
4	id-qt-acps	[RFC4476]
5	id-qt-acunotice	[RFC4476]

Future updates to this table are to be made according to the Specification Required policy as defined in [RFC5226].

3.6. "SMI Security for PKIX Extended Key Purpose" Registry

Within the SMI-numbers registry, an "SMI Security for PKIX Extended Key Purpose Identifiers (1.3.6.1.5.5.7.3)" table with three columns has been added:

Decimal	Description	References
1	id-kp-serverAuth	[RFC2459]
2	id-kp-clientAuth	[RFC2459]
3	id-kp-codeSigning	[RFC2459]
4	id-kp-emailProtection	[RFC2459]
5	id-kp-ipsecEndSystem	Reserved and Obsolete
6	id-kp-ipsecTunnel	Reserved and Obsolete
7	id-kp-ipsecUser	Reserved and Obsolete
8	id-kp-timeStamping	[RFC2459]
9	id-kp-OCSPSigning	[RFC2560]
10	id-kp-dvcs	[RFC3029]
11	id-kp-sbgpCertAAServerAuth	Reserved and Obsolete
12	id-kp-scvp-responder	Reserved and Obsolete
13	id-kp-eapOverPPP	[RFC4334]
14	id-kp-eapOverLAN	[RFC4334]
15	id-kp-scvpServer	[RFC5055]
16	id-kp-scvpClient	[RFC5055]
17	id-kp-ipsecIKE	[RFC4945]
18	id-kp-capwapAC	[RFC5415]
19	id-kp-capwapWTP	[RFC5415]
20	id-kp-sipDomain	[RFC5924]
21	id-kp-secureShellClient	[RFC6187]
22	id-kp-secureShellServer	[RFC6187]
23	id-kp-sendRouter	[RFC6494]

24	id-kp-sendProxiedRouter	[RFC6494]
25	id-kp-sendOwner	[RFC6494]
26	id-kp-sendProxiedOwner	[RFC6494]
27	id-kp-cmcCA	[RFC6402]
28	id-kp-cmcRA	[RFC6402]
29	id-kp-cmcArchive	[RFC6402]
30	id-kp-bgpsec-router	[BGPSEC]

Future updates to this table are to be made according to the Specification Required policy as defined in [RFC5226].

3.7. "SMI Security for PKIX CMP Information Types" Registry

Within the SMI-numbers registry, an "SMI Security for PKIX CMP Information Types (1.3.6.1.5.5.7.4)" table with three columns has been added:

Decimal	Description	References
1	id-it-caProtEncCert	[RFC2510]
2	id-it-signKeyPairTypes	[RFC2510]
3	id-it-encKeyPairTypes	[RFC2510]
4	id-it-preferredSymmAlg	[RFC2510]
5	id-it-caKeyUpdateInfo	[RFC2510]
6	id-it-currentCRL	[RFC2510]
7	id-it-unsupportedOIDs	[RFC4210]
8	id-it-subscriptionRequest	Reserved and Obsolete
9	id-it-subscriptionResponse	Reserved and Obsolete
10	id-it-keyPairParamReq	[RFC4210]
11	id-it-keyPairParamRep	[RFC4210]
12	id-it-revPassphrase	[RFC4210]
13	id-it-implicitConfirm	[RFC4210]
14	id-it-confirmWaitTime	[RFC4210]
15	id-it-origPKIMessage	[RFC4210]
16	id-it-suppLangTags	[RFC4210]

Future updates to this table are to be made according to the Specification Required policy as defined in [RFC5226].

3.8. "SMI Security for PKIX CRMF Registration" Registry

Within the SMI-numbers registry, an "SMI Security for PKIX CRMF Registration (1.3.6.1.5.5.7.5)" table with three columns has been added:

Decimal	Description	References
1	id-regCtrl	[RFC2511]
2	id-regInfo	[RFC2511]
3	id-regEPEPSI	[RFC4683]

Future updates to this table are to be made according to the Specification Required policy as defined in [RFC5226].

3.9. "SMI Security for PKIX CRMF Registration Controls" Registry

Within the SMI-numbers registry, an "SMI Security for PKIX CRMF Registration Controls (1.3.6.1.5.5.7.5.1)" table with three columns has been added:

Decimal	Description	References
1	id-regCtrl-regToken	[RFC2511]
2	id-regCtrl-authenticator	[RFC2511]
3	id-regCtrl-pkiPublicationInfo	[RFC2511]
4	id-regCtrl-pkiArchiveOptions	[RFC2511]
5	id-regCtrl-oldCertID	[RFC2511]
6	id-regCtrl-protocolEncrKey	[RFC2511]
7	id-regCtrl-altCertTemplate	[RFC4210]
8	id-regCtrl-wtlsTemplate	Reserved and Obsolete
9	id-regCtrl-regTokenUTF8	Reserved and Obsolete
10	id-regCtrl-authenticatorUTF8	Reserved and Obsolete

Future updates to this table are to be made according to the Specification Required policy as defined in [RFC5226].

3.10. "SMI Security for PKIX CRMF Registration Information" Registry

Within the SMI-numbers registry, add an "SMI Security for PKIX CRMF Registration Information (1.3.6.1.5.5.7.5.2)" table with three columns:

Decimal	Description	References
1	id-regInfo-utf8Pairs	[RFC2511]
2	id-regInfo-certReq	[RFC2511]

Future updates to this table are to be made according to the Specification Required policy as defined in [RFC5226].

3.11. "SMI Security for PKIX Algorithms" Registry

Within the SMI-numbers registry, an "SMI Security for PKIX Algorithms (1.3.6.1.5.5.7.6)" table with three columns has been added:

Decimal	Description	References
1	id-alg-des40	Reserved and Obsolete
2	id-alg-noSignature	[RFC2797]
3	id-alg-dh-sig-hmac-sha1	[RFC2875]
4	id-alg-dhPop-sha1	[RFC2875]
5	id-alg-dhPop-sha224	[RFC6955]
6	id-alg-dhPop-sha256	[RFC6955]
7	id-alg-dhPop-sha384	[RFC6955]
8	id-alg-dhPop-sha512	[RFC6955]
15	id-alg-dhPop-static-sha224-hmac-sha224	[RFC6955]
16	id-alg-dhPop-static-sha256-hmac-sha256	[RFC6955]
17	id-alg-dhPop-static-sha384-hmac-sha384	[RFC6955]
18	id-alg-dhPop-static-sha512-hmac-sha512	[RFC6955]
25	id-alg-ecdhPop-static-sha224-hmac-sha224	[RFC6955]
26	id-alg-ecdhPop-static-sha256-hmac-sha256	[RFC6955]
27	id-alg-ecdhPop-static-sha384-hmac-sha384	[RFC6955]
28	id-alg-ecdhPop-static-sha512-hmac-sha512	[RFC6955]

Note: id-alg-dhPop-sha1 is also known as id-alg-dh-pop.

Note: id-alg-dh-sig-hmac-sha1 is also known as id-alg-dhPop-static-sha1-hmac-sha1 and id-dhPop-static-hmac-sha1.

Future updates to this table are to be made according to the Specification Required policy as defined in [RFC5226].

3.12. "SMI Security for PKIX CMC Controls" Registry

Within the SMI-numbers registry, an "SMI Security for PKIX CMC Controls (1.3.6.1.5.5.7.7)" table with three columns has been added:

Decimal	Description	References
1	id-cmc-statusInfo	[RFC2797]
2	id-cmc-identification	[RFC2797]
3	id-cmc-identityProof	[RFC2797]
4	id-cmc-dataReturn	[RFC2797]
5	id-cmc-transactionId	[RFC2797]

6	id-cmc-senderNonce	[RFC2797]
7	id-cmc-recipientNonce	[RFC2797]
8	id-cmc-addExtensions	[RFC2797]
9	id-cmc-encryptedPOP	[RFC2797]
10	id-cmc-decryptedPOP	[RFC2797]
11	id-cmc-lraPOPWitness	[RFC2797]
15	id-cmc-getCert	[RFC2797]
16	id-cmc-getCRL	[RFC2797]
17	id-cmc-revokeRequest	[RFC2797]
18	id-cmc-regInfo	[RFC2797]
19	id-cmc-responseInfo	[RFC2797]
21	id-cmc-queryPending	[RFC2797]
22	id-cmc-popLinkRandom	[RFC2797]
23	id-cmc-popLinkWitness	[RFC2797]
24	id-cmc-confirmCertAcceptance	[RFC2797]
25	id-cmc-statusInfoV2	[RFC5272]
26	id-cmc-trustedAnchors	[RFC5272]
27	id-cmc-authData	[RFC5272]
28	id-cmc-batchRequests	[RFC5272]
29	id-cmc-batchResponses	[RFC5272]
30	id-cmc-publishCert	[RFC5272]
31	id-cmc-modCertTemplate	[RFC5272]
32	id-cmc-controlProcessed	[RFC5272]
33	id-cmc-popLinkWitnessV2	[RFC5272]
34	id-cmc-identityProofV2	[RFC5272]
35	id-cmc-raIdentityWitness	[RFC6402]
36	id-cmc-changeSubjectName	[RFC6402]
37	id-cmc-responseBody	[RFC6402]
99	id-cmc-glaRR	[RFC5275]

Note: id-cmc-statusInfo is also known as id-cmc-cMCStatusInfo.

Future updates to this table are to be made according to the Specification Required policy as defined in [RFC5226].

3.13. "SMI Security for PKIX CMC GLA Requests and Responses" Registry

Within the SMI-numbers registry, an "SMI Security for PKIX CMC GLA Requests and Responses (1.3.6.1.5.5.7.7.99)" table with three columns has been added:

Decimal	Description	References
1	id-cmc-gla-skdAlgRequest	[RFC5275]
2	id-cmc-gla-skdAlgResponse	[RFC5275]

Future updates to this table are to be made according to the Specification Required policy as defined in [RFC5226].

3.14. "SMI Security for PKIX Other Name Forms" Registry

Within the SMI-numbers registry, an "SMI Security for PKIX Other Name Forms (1.3.6.1.5.5.7.8)" table with three columns has been added:

Decimal	Description	References
1	id-on-personalData	Reserved and Obsolete
2	id-on-userGroup	Reserved and Obsolete
3	id-on-permanentIdentifier	[RFC4043]
4	id-on-hardwareModuleName	[RFC4108]
5	id-on-xmppAddr	[RFC3920]
6	id-on-SIM	[RFC4683]
7	id-on-dnsSRV	[RFC4985]

Future updates to this table are to be made according to the Specification Required policy as defined in [RFC5226].

3.15. "SMI Security for PKIX Personal Data Attributes" Registry

Within the SMI-numbers registry, an "SMI Security for PKIX Personal Data Attributes (1.3.6.1.5.5.7.9)" table with three columns has been added:

Decimal	Description	References
1	id-pda-dateOfBirth	[RFC3039]
2	id-pda-placeOfBirth	[RFC3039]
3	id-pda-gender	[RFC3039]
4	id-pda-countryOfCitizenship	[RFC3039]
5	id-pda-countryOfResidence	[RFC3039]

Future updates to this table are to be made according to the Specification Required policy as defined in [RFC5226].

3.16. "SMI Security for PKIX Attribute Certificate Attributes" Registry

Within the SMI-numbers registry, an "SMI Security for PKIX Attribute Certificate Attributes (1.3.6.1.5.5.7.10)" table with three columns has been added:

Decimal	Description	References
1	id-aca-authenticationInfo	[RFC3281]
2	id-aca-accessIdentity	[RFC3281]
3	id-aca-chargingIdentity	[RFC3281]
4	id-aca-group	[RFC3281]
5	id-aca-role	Reserved and Obsolete
6	id-aca-encAttrs	[RFC3281]
7	id-aca-wlanSSID	[RFC4334]

Future updates to this table are to be made according to the Specification Required policy as defined in [RFC5226].

3.17. "SMI Security for PKIX Qualified Certificate Statements" Registry

Within the SMI-numbers registry, an "SMI Security for PKIX Qualified Certificate Statements (1.3.6.1.5.5.7.11)" table with three columns has been added:

Decimal	Description	References
1	id-qcs-pkixQCSyntax-v1	[RFC3039]
2	id-qcs-pkixQCSyntax-v2	[RFC3739]

Future updates to this table are to be made according to the Specification Required policy as defined in [RFC5226].

3.18. "SMI Security for PKIX CMC Content Types" Registry

Within the SMI-numbers registry, an "SMI Security for PKIX CMC Content Types (1.3.6.1.5.5.7.12)" table with three columns has been added:

Decimal	Description	References
1	id-cct-crs	Reserved and Obsolete
2	id-cct-PKIData	[RFC2797]
3	id-cct-PKIResponse	[RFC2797]

Future updates to this table are to be made according to the Specification Required policy as defined in [RFC5226].

3.19. "SMI Security for PKIX OIDs Used Only for Testing" Registry

Within the SMI-numbers registry, an "SMI Security for PKIX OIDs used Only for Testing (1.3.6.1.5.5.7.13)" table with three columns has been added:

Decimal	Description	References
1	id-TEST-certPolicyOne	[RFC7229]
2	id-TEST-certPolicyTwo	[RFC7229]
3	id-TEST-certPolicyThree	[RFC7229]
4	id-TEST-certPolicyFour	[RFC7229]
5	id-TEST-certPolicyFive	[RFC7229]
6	id-TEST-certPolicySix	[RFC7229]
7	id-TEST-certPolicySeven	[RFC7229]
8	id-TEST-certPolicyEight	[RFC7229]

Note: The object identifiers in this table should not appear on the public Internet. These object identifiers are ONLY for TESTING.

Future updates to this table are to be made according to the Specification Required policy as defined in [RFC5226].

3.20. "SMI Security for PKIX Certificate Policies" Registry

Within the SMI-numbers registry, an "SMI Security for PKIX Certificate Policies (1.3.6.1.5.5.7.14)" table with three columns has been added:

Decimal	Description	References
1	id-cp-sbgpCertificatePolicy	Reserved and Obsolete
2	id-cp-ipAddr-asNumber	[RFC6484]

Future updates to this table are to be made according to the Specification Required policy as defined in [RFC5226].

3.21. "SMI Security for PKIX CMC Error Types" Registry

Within the SMI-numbers registry, an "SMI Security for PKIX CMC Error Types (1.3.6.1.5.5.7.15)" table with three columns has been added:

Decimal	Description	References
1	id-cet-skdFailInfo	[RFC5275]

Future updates to this table are to be made according to the Specification Required policy as defined in [RFC5226].

3.22. "SMI Security for PKIX Revocation Information Types" Registry

Within the SMI-numbers registry, an "SMI Security for PKIX Revocation Information Types (1.3.6.1.5.5.7.16)" table with three columns has been added:

Decimal	Description	References
1	id-ri-crl	[RFC5940]
2	id-ri-ocsp-response	[RFC5940]
3	id-ri-delta-crl	[RFC5940]
4	id-ri-scvp	[RFC5940]

Future updates to this table are to be made according to the Specification Required policy as defined in [RFC5226].

3.23. "SMI Security for PKIX SCVP Check Types" Registry

Within the SMI-numbers registry, an "SMI Security for PKIX SCVP Check Types (1.3.6.1.5.5.7.17)" table with three columns has been added:

Decimal	Description	References
1	id-stc-build-pkc-path	[RFC5055]
2	id-stc-build-valid-pkc-path	[RFC5055]
3	id-stc-build-status-checked-pkc-path	[RFC5055]
4	id-stc-build-aa-path	[RFC5055]
5	id-stc-build-valid-aa-path	[RFC5055]
6	id-stc-build-status-checked-aa-path	[RFC5055]
7	id-stc-status-check-ac-and-build-status-checked-aa-path	[RFC5055]

Future updates to this table are to be made according to the Specification Required policy as defined in [RFC5226].

3.24. "SMI Security for PKIX SCVP Want Back Types" Registry

Within the SMI-numbers registry, an "SMI Security for PKIX SCVP Want Back Types (1.3.6.1.5.5.7.18)" table with three columns has been added:

Decimal	Description	References
1	id-swb-pkc-best-cert-path	[RFC5055]
2	id-swb-pkc-revocation-info	[RFC5055]
3	id-swb-pkc-cert-status	Reserved and Obsolete
4	id-swb-pkc-public-key-info	[RFC5055]
5	id-swb-aa-cert-path	[RFC5055]
6	id-swb-aa-revocation-info	[RFC5055]
7	id-swb-ac-revocation-info	[RFC5055]
8	id-swb-ac-cert-status	Reserved and Obsolete
9	id-swb-relayed-responses	[RFC5055]
10	id-swb-pkc-cert	[RFC5055]
11	id-swb-ac-cert	[RFC5055]
12	id-swb-pkc-all-cert-paths	[RFC5055]
13	id-swb-pkc-ee-revocation-info	[RFC5055]
14	id-swb-pkc-CAs-revocation-info	[RFC5055]
15	id-swb-partial-cert-path	[RFC5276]
16	id-swb-ers-pkc-cert	[RFC5276]
17	id-swb-ers-best-cert-path	[RFC5276]
18	id-swb-ers-partial-cert-path	[RFC5276]
19	id-swb-ers-revocation-info	[RFC5276]
20	id-swb-ers-all	[RFC5276]

Future updates to this table are to be made according to the Specification Required policy as defined in [RFC5226].

3.25. "SMI Security for PKIX SCVP Validation Policies and Algorithms" Registry

Within the SMI-numbers registry, an "SMI Security for PKIX SCVP Validation Policies and Algorithms (1.3.6.1.5.5.7.19)" table with three columns has been added:

Decimal	Description	References
1	id-svp-defaultValPolicy	[RFC5055]
2	id-svp-nameValAlg	[RFC5055]
3	id-svp-basicValAlg	[RFC5055]
4	id-svp-dnValAlg	[RFC5055]

Note: id-svp-nameValAlg is also known as id-nvae.

Note: id-svp-basicValAlg is also known as id-bvae.

Note: id-svp-dnValAlg is also known as id-dnvae and id-nva-dnCompAlg.

Future updates to this table are to be made according to the Specification Required policy as defined in [RFC5226].

3.26. "SMI Security for PKIX SCVP Name Validation Policy Errors" Registry

Within the SMI-numbers registry, an "SMI Security for PKIX SCVP Name Validation Policy Errors (1.3.6.1.5.5.7.19.2)" table with three columns has been added:

Decimal	Description	References
1	id-nvae-name-mismatch	[RFC5055]
2	id-nvae-no-name	[RFC5055]
3	id-nvae-unknown-alg	[RFC5055]
4	id-nvae-bad-name	[RFC5055]
5	id-nvae-bad-name-type	[RFC5055]
6	id-nvae-mixed-names	[RFC5055]

Future updates to this table are to be made according to the Specification Required policy as defined in [RFC5226].

3.27. "SMI Security for PKIX SCVP Basic Validation Policy Errors" Registry

Within the SMI-numbers registry, an "SMI Security for PKIX SCVP Basic Validation Policy Errors (1.3.6.1.5.5.7.19.3)" table with three columns has been added:

Decimal	Description	References
1	id-bvae-expired	[RFC5055]
2	id-bvae-not-yet-valid	[RFC5055]
3	id-bvae-wrongTrustAnchor	[RFC5055]
4	id-bvae-noValidCertPath	[RFC5055]
5	id-bvae-revoked	[RFC5055]
9	id-bvae-invalidKeyPurpose	[RFC5055]
10	id-bvae-invalidKeyUsage	[RFC5055]
11	id-bvae-invalidCertPolicy	[RFC5055]
12	id-bvae-invalidName	Reserved and Obsolete
13	id-bvae-invalidEntity	Reserved and Obsolete
14	id-bvae-invalidPathDepth	Reserved and Obsolete

Future updates to this table are to be made according to the Specification Required policy as defined in [RFC5226].

3.28. "SMI Security for PKIX SCVP Distinguished Name Validation Policy Errors" Registry

Within the SMI-numbers registry, an "SMI Security for PKIX SCVP Distinguished Name Validation Policy Errors (1.3.6.1.5.5.7.19.4)" table with three columns has been added:

Decimal	Description	References

Note: This table is currently empty.

Future updates to this table are to be made according to the Specification Required policy as defined in [RFC5226].

3.29. "SMI Security for PKIX Other Logotype Identifiers" Registry

Within the SMI-numbers registry, an "SMI Security for PKIX Other Logotype Identifiers (1.3.6.1.5.5.7.20)" table with three columns has been added:

Decimal	Description	References
1	id-logo-loyalty	[RFC3709]
2	id-logo-background	[RFC3709]
3	id-logo-certImage	[RFC6170]

Future updates to this table are to be made according to the Specification Required policy as defined in [RFC5226].

3.30. "SMI Security for PKIX Proxy Certificate Policy Languages" Registry

Within the SMI-numbers registry, an "SMI Security for PKIX Proxy Certificate Policy Languages (1.3.6.1.5.5.7.21)" table with three columns has been added:

Decimal	Description	References
0	id-ppl-anyLanguage	[RFC3820]
1	id-ppl-inheritAll	[RFC3820]
2	id-ppl-independent	[RFC3820]

Future updates to this table are to be made according to the Specification Required policy as defined in [RFC5226].

3.31. "SMI Security for PKIX Proxy Matching Rules" Registry

Within the SMI-numbers registry, an "SMI Security for PKIX Proxy Matching Rules (1.3.6.1.5.5.7.22)" table with three columns has been added:

Decimal	Description	References
1	id-mr-pkix-alphanum-ids	Reserved and Obsolete

Future updates to this table are to be made according to the Specification Required policy as defined in [RFC5226].

3.32. "SMI Security for PKIX Subject Key Identifier Semantics" Registry

Within the SMI-numbers registry, an "SMI Security for PKIX Subject Key Identifier Semantics (1.3.6.1.5.5.7.23)" table with three columns has been added:

Decimal	Description	References
1	id-skis-keyHash	Reserved and Obsolete
2	id-skis-4BitKeyHash	Reserved and Obsolete
3	id-skis-keyInfoHash	Reserved and Obsolete

Future updates to this table are to be made according to the Specification Required policy as defined in [RFC5226].

3.33. "SMI Security for PKIX Access Descriptor" Registry

Within the SMI-numbers registry, an "SMI Security for PKIX Access Descriptor (1.3.6.1.5.5.7.48)" table with three columns has been added:

Decimal	Description	References
1	id-ad-ocsp	[RFC2459]
2	id-ad-caIssuers	[RFC2459]
3	id-ad-timestamping	[RFC3161]
4	id-ad-dvcs	[RFC3029]
5	id-ad-caRepository	[RFC3280]
6	id-ad-http-certs	[RFC4387]
7	id-ad-http-crls	[RFC4387]
8	id-ad-xkms	Reserved and Obsolete
9	id-ad-signedObjectRepository	Reserved and Obsolete
10	id-ad-rpkiManifest	[RFC6487]
11	id-ad-signedObject	[RFC6487]
12	id-ad-cmc	[RFC6402]

Note: id-ad-ocsp is also known as id-pkix-ocsp.

Future updates to this table are to be made according to the Specification Required policy as defined in [RFC5226].

3.34. "SMI Security for PKIX Online Certificate Status Protocol (OCSP)" Registry

Within the SMI-numbers registry, an "SMI Security for PKIX Online Certificate Status Protocol (OCSP) (1.3.6.1.5.5.7.48.1)" table with three columns has been added:

Decimal	Description	References
1	id-pkix-ocsp-basic	[RFC2560]
2	id-pkix-ocsp-nonce	[RFC2560]
3	id-pkix-ocsp-crl	[RFC2560]
4	id-pkix-ocsp-response	[RFC2560]
5	id-pkix-ocsp-nocheck	[RFC2560]
6	id-pkix-ocsp-archive-cutoff	[RFC2560]
7	id-pkix-ocsp-service-locator	[RFC2560]
8	id-pkix-ocsp-pref-sig-algs	[RFC6277]
9	id-pkix-ocsp-extended-revoke	[RFC6960]

Future updates to this table are to be made according to the Specification Required policy 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.

The id-pe-nsa certificate extension should not appear in any certificate that is used on the public Internet.

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, November 2008.

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

[ASN1-97] International Telecommunication Union, "Abstract Syntax Notation One (ASN.1): Specification of basic notation", ITU-T Recommendation X.680, 1997.

[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

[Err3860] RFC Errata, Errata ID 3860, RFC 6402, <http://www.rfc-editor.org/>.

[Abley] Abley, J., Schlyter, J., and G. Bailey, "DNSSEC Trust Anchor Publication for the Root Zone", Work in Progress, June 2014.

[BGPSEC] Reynolds, M., Turner, S., and S. Kent, "A Profile for BGPSEC Router Certificates, Certificate Revocation Lists, and Certification Requests", Work in Progress, March 2014.

[RFC2459] Housley, R., Ford, W., Polk, W., and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC 2459, January 1999.

[RFC2510] Adams, C. and S. Farrell, "Internet X.509 Public Key Infrastructure Certificate Management Protocols", RFC 2510, March 1999.

[RFC2511] Myers, M., Adams, C., Solo, D., and D. Kemp, "Internet X.509 Certificate Request Message Format", RFC 2511, March 1999.

[RFC2528] Housley, R. and W. Polk, "Internet X.509 Public Key Infrastructure Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates", RFC 2528, March 1999.

[RFC2560] Myers, M., Ankney, R., Malpani, A., Galperin, S., and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", RFC 2560, June 1999.

[RFC2797] Myers, M., Liu, X., Schaad, J., and J. Weinstein, "Certificate Management Messages over CMS", RFC 2797, April 2000.

[RFC2875] Prafullchandra, H. and J. Schaad, "Diffie-Hellman Proof-of-Possession Algorithms", RFC 2875, July 2000.

[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.

[RFC3039] Santesson, S., Polk, W., Barzin, P., and M. Nystrom, "Internet X.509 Public Key Infrastructure Qualified Certificates Profile", RFC 3039, January 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.

[RFC3279] Bassham, L., Polk, W., and R. Housley, "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3279, April 2002.

[RFC3280] Housley, R., Polk, W., Ford, W., and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.

[RFC3281] Farrell, S. and R. Housley, "An Internet Attribute Certificate Profile for Authorization", RFC 3281, April 2002.

[RFC3709] Santesson, S., Housley, R., and T. Freeman, "Internet X.509 Public Key Infrastructure: Logotypes in X.509 Certificates", RFC 3709, February 2004.

[RFC3739] Santesson, S., Nystrom, M., and T. Polk, "Internet X.509 Public Key Infrastructure: Qualified Certificates Profile", RFC 3739, March 2004.

[RFC3770] Housley, R. and T. Moore, "Certificate Extensions and Attributes Supporting Authentication in Point-to-Point Protocol (PPP) and Wireless Local Area Networks (WLAN)", RFC 3770, May 2004.

[RFC3779] Lynn, C., Kent, S., and K. Seo, "X.509 Extensions for IP Addresses and AS Identifiers", RFC 3779, June 2004.

[RFC3820] Tuecke, S., Welch, V., Engert, D., Pearlman, L., and M. Thompson, "Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile", RFC 3820, June 2004.

[RFC3920] Saint-Andre, P., Ed., "Extensible Messaging and Presence Protocol (XMPP): Core", RFC 3920, October 2004.

[RFC4043] Pinkas, D. and T. Gindin, "Internet X.509 Public Key Infrastructure Permanent Identifier", RFC 4043, May 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.

[RFC4059] Linsenbardt, D., Pontius, S., and A. Sturgeon, "Internet X.509 Public Key Infrastructure Warranty Certificate Extension", RFC 4059, May 2005.

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

[RFC4210] Adams, C., Farrell, S., Kause, T., and T. Mononen, "Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)", RFC 4210, September 2005.

[RFC4306] Kaufman, C., Ed., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

[RFC4334] Housley, R. and T. Moore, "Certificate Extensions and Attributes Supporting Authentication in Point-to-Point Protocol (PPP) and Wireless Local Area Networks (WLAN)", RFC 4334, February 2006.

[RFC4387] Gutmann, P., Ed., "Internet X.509 Public Key Infrastructure Operational Protocols: Certificate Store Access via HTTP", RFC 4387, February 2006.

[RFC4476] Francis, C. and D. Pinkas, "Attribute Certificate (AC) Policies Extension", RFC 4476, May 2006.

[RFC4683] Park, J., Lee, J., . Lee, H., Park, S., and T. Polk, "Internet X.509 Public Key Infrastructure Subject Identification Method (SIM)", RFC 4683, October 2006.

[RFC4945] Korver, B., "The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX", RFC 4945, August 2007.

[RFC4985] Santesson, S., "Internet X.509 Public Key Infrastructure Subject Alternative Name for Expression of Service Name", RFC 4985, August 2007.

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

[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.

[RFC5276] Wallace, C., "Using the Server-Based Certificate Validation Protocol (SCVP) to Convey Long-Term Evidence Records", RFC 5276, August 2008.

[RFC5415] Calhoun, P., Ed., Montemurro, M., Ed., and D. Stanley, Ed., "Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification", RFC 5415, March 2009.

[RFC5480] Turner, S., Brown, D., Yiu, K., Housley, R., and T. Polk, "Elliptic Curve Cryptography Subject Public Key Information", RFC 5480, March 2009.

[RFC5697] Farrell, S., "Other Certificates Extension", RFC 5697, November 2009.

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

[RFC5912] Hoffman, P. and J. Schaad, "New ASN.1 Modules for the Public Key Infrastructure Using X.509 (PKIX)", RFC 5912, June 2010.

[RFC5913] Turner, S. and S. Chokhani, "Clearance Attribute and Authority Clearance Constraints Certificate Extension", RFC 5913, June 2010.

[RFC5915] Turner, S. and D. Brown, "Elliptic Curve Private Key Structure", RFC 5915, June 2010.

[RFC5924] Lawrence, S. and V. Gurbani, "Extended Key Usage (EKU) for Session Initiation Protocol (SIP) X.509 Certificates", RFC 5924, June 2010.

[RFC5934] Housley, R., Ashmore, S., and C. Wallace, "Trust Anchor Management Protocol (TAMP)", RFC 5934, August 2010.

[RFC5940] Turner, S. and R. Housley, "Additional Cryptographic Message Syntax (CMS) Revocation Information Choices", RFC 5940, August 2010.

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

[RFC6170] Santesson, S., Housley, R., Bajaj, S., and L. Rosenthol, "Internet X.509 Public Key Infrastructure -- Certificate Image", RFC 6170, May 2011.

[RFC6187] Igoe, K. and D. Stebila, "X.509v3 Certificates for Secure Shell Authentication", RFC 6187, March 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.

[RFC6277] Santesson, S. and P. Hallam-Baker, "Online Certificate Status Protocol Algorithm Agility", RFC 6277, June 2011.

[RFC6402] Schaad, J., "Certificate Management over CMS (CMC) Updates", RFC 6402, November 2011.

[RFC6484] Kent, S., Kong, D., Seo, K., and R. Watro, "Certificate Policy (CP) for the Resource Public Key Infrastructure (RPKI)", BCP 173, RFC 6484, February 2012.

[RFC6487] Huston, G., Michaelson, G., and R. Loomans, "A Profile for X.509 PKIX Resource Certificates", RFC 6487, February 2012.

[RFC6494] Gagliano, R., Krishnan, S., and A. Kukec, "Certificate Profile and Certificate Management for SEcure Neighbor Discovery (SEND)", RFC 6494, February 2012.

[RFC6664] Schaad, J., "S/MIME Capabilities for Public Key Definitions", RFC 6664, July 2012.

[RFC6955] Schaad, J. and H. Prafullchandra, "Diffie-Hellman Proof-of-Possession Algorithms", RFC 6955, May 2013.

[RFC6960] Santesson, S., Myers, M., Ankney, R., Malpani, A., Galperin, S., and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", RFC 6960, June 2013.

[RFC7169] Turner, S., "The NSA (No Secrecy Afforded) Certificate Extension", RFC 7169, April 1 2014.

[RFC7229] Housley, R., "Object Identifiers for Test Certificate Policies", RFC 7229, May 2014.

Acknowledgements

Many thanks to Lynne Bartholomew, David Cooper, Jim Schaad, and Sean Turner for their careful review and comments.

Author’s Address

Russ Housley
918 Spring Knoll Drive
Herndon, VA 20170
USA

EMail: housley@vigilsec.com