

---

# rfc7299

## OID pour le groupe de travail PKIX

Quand le groupe de travail PKIX a démarré, un arc OID a été alloué par l'IANA. Ce document décrit les identifiants assignés dans cet arc, et établit les stratégies d'allocation pour tout assignement dans cet arc. l'arc OID pkix est :

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

## Arcs OID subordonnés

25 arcs OID subordonnés ont été utilisés, de 0 à 23 et 48. De plus, il y a 7 arcs subordonnés. Ils ont été assignés comme suit :

**Identifiants de module** id-mod OBJECT IDENTIFIER ::= { id-pkix 0 }

**Extensions de certificat PKIX** id-pe OBJECT IDENTIFIER ::= { id-pkix 1 }

**Type de qualifiant de stratégie** id-qt OBJECT IDENTIFIER ::= { id-pkix 2 }

**Identifiant de clé étendue** id-kp OBJECT IDENTIFIER ::= { id-pkix 3 }

**Type d'information CMP** id-it OBJECT IDENTIFIER ::= { id-pkix 4 }

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

**Contrôles d'enregistrement CRMF** id-regCtrl OBJECT IDENTIFIER ::= { id-pkix 5 1 }

**Informations d'enregistrement CRMF** id-regInfo OBJECT IDENTIFIER ::= { id-pkix 5 2 }

**Algorithmes** id-alg OBJECT IDENTIFIER ::= { id-pkix 6 }

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

**Requêtes et réponses CMC GLA** id-cmc-glaRR OBJECT IDENTIFIER ::= { id-pkix 7 99 }

**Autres formes de nom** id-on OBJECT IDENTIFIER ::= { id-pkix 8 }

**Attribut personnel** id-pda OBJECT IDENTIFIER ::= { id-pkix 9 }

**Attribut de certificat d'attributs** id-aca OBJECT IDENTIFIER ::= { id-pkix 10 }

**Déclarations de certificat qualifié** id-qcs OBJECT IDENTIFIER ::= { id-pkix 11 }

**Types de contenu CMC** id-cct OBJECT IDENTIFIER ::= { id-pkix 12 }

**OID pour test uniquement** id-TEST OBJECT IDENTIFIER ::= { id-pkix 13 }

**Stratégies de certificat** id-cp OBJECT IDENTIFIER ::= { id-pkix 14 }

**Type d'erreur CMC** id-cet OBJECT IDENTIFIER ::= { id-pkix 15 }

**Types d'information de révocation** id-ri OBJECT IDENTIFIER ::= { id-pkix 16 }

**Types de retour SCVP** id-swb OBJECT IDENTIFIER ::= { id-pkix 18 }

**Stratégies de validation SCVP** id-svp OBJECT IDENTIFIER ::= { id-pkix 19 }

**Erreurs de stratégie de validation de nom SCVP** id-nvae OBJECT IDENTIFIER ::= { id-pkix 19 2 }

**Erreurs de stratégie de validation de base SCVP** id-bvae OBJECT IDENTIFIER ::= { id-pkix 19 3 }

**Erreurs de stratégie de validation de nom distinct SCVP** id-dnvae OBJECT IDENTIFIER ::= { id-pkix 19 4 }

**Autres identifiants logotype** id-logo OBJECT IDENTIFIER ::= { id-pkix 20 }

**Langages de stratégie de certificat proxy** id-ppl OBJECT IDENTIFIER ::= { id-pkix 21 }

**Règles de correspondance** id-mr OBJECT IDENTIFIER ::= { id-pkix 22 }

**Sémantiques d'identifiant de clé du sujet** id-skis OBJECT IDENTIFIER ::= { id-pkix 23 }

---

**Descripteurs d'accès** id-ad OBJECT IDENTIFIER ::= { id-pkix 48 }

**OCSF** id-pkix-ocsp OBJECT IDENTIFIER ::= { id-pkix 48 1 }

L'IANA a mis à jours une table d'enregistrement et créé 33 tables additionnelles. Les mises à jours dans les nouvelles tables sont faites en accord avec la spécification définie dans la rfc5226.

## 1.3.6.1.5.5.7

### 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]

## 1.3.6.1.5.5.7.0

### 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	[Abley]
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]

## 1.3.6.1.5.5.7.1

### 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]

## 1.3.6.1.5.5.7.2

### 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]

---

## 1.3.6.1.5.5.7.3

### 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]

## 1.3.6.1.5.5.7.4

### 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-supplLangTags	[RFC4210]

---

## 1.3.6.1.5.5.7.5

### Decimal Description References

---

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

## 1.3.6.1.5.5.7.5.1

### 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

## 1.3.6.1.5.5.7.5.2

### Decimal Description References

---

1	id-regInfo-utf8Pairs	[RFC2511]
2	id-regInfo-certReq	[RFC2511]

## 1.3.6.1.5.5.7.6

### 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-shal est également appelé id-alg-dh-pop.

Note: id-alg-dh-sig-hmac-shal est également appelé id-alg-dhPop-static-shal-hmac-shal et id-dhPop-static-hmac-shal.

## 1.3.6.1.5.5.7.7

### 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 est également appelé id-cmc-cMCStatusInfo.

## 1.3.6.1.5.5.7.7.99

### Decimal Description References

- 
- 1\_\_\_\_\_id-cmc-gla-skdAlgRequest\_\_\_\_\_ [RFC5275]
  - 2\_\_\_\_\_id-cmc-gla-skdAlgResponse\_\_\_\_\_ [RFC5275]

## 1.3.6.1.5.5.7.8

### 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]

## 1.3.6.1.5.5.7.9

### 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]

## 1.3.6.1.5.5.7.10

### 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]

## 1.3.6.1.5.5.7.11

### Decimal Description References

- 
- 1\_\_\_\_\_id-qcs-pkixQCSyntax-v1\_\_\_\_\_ [RFC3039]
  - 2\_\_\_\_\_id-qcs-pkixQCSyntax-v2\_\_\_\_\_ [RFC3739]



---

## 1.3.6.1.5.5.7.12

### Decimal Description References

-----

- 1\_\_\_\_\_id-cct-crs\_\_\_\_\_Reserved and Obsolete
- 2\_\_\_\_\_id-cct-PKIData\_\_\_\_\_ [RFC2797]
- 3\_\_\_\_\_id-cct-PKIResponse\_\_\_\_\_ [RFC2797]

## 1.3.6.1.5.5.7.13

### 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]

## 1.3.6.1.5.5.7.14

### Decimal Description References

-----

- 1\_\_\_\_\_id-cp-sbgpCertificatePolicy\_\_\_\_\_Reserved and Obsolete
- 2\_\_\_\_\_id-cp-ipAddr-asNumber\_\_\_\_\_ [RFC6484]

## 1.3.6.1.5.5.7.15

### Decimal Description References

-----

- 1\_\_\_\_\_id-cet-skdFailInfo\_\_\_\_\_ [RFC5275]

## 1.3.6.1.5.5.7.16

### 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]

---

## 1.3.6.1.5.5.7.17

### 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]

## 1.3.6.1.5.5.7.18

### 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]

## 1.3.6.1.5.5.7.19

### Decimal Description References

---

- 1\_\_\_\_\_id-svp-defaultValPolicy\_\_\_\_\_ [RFC5055]
- 2\_\_\_\_\_id-svp-nameValAlg\_\_\_\_\_ [RFC5055]
- 3\_\_\_\_\_id-svp-basicValAlg\_\_\_\_\_ [RFC5055]
- 4\_\_\_\_\_id-svp-dnValAlg\_\_\_\_\_ [RFC5055]

## 1.3.6.1.5.5.7.19.2

---

## 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]

## 1.3.6.1.5.5.7.19.3

### 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

## 1.3.6.1.5.5.7.20

### Decimal Description Reference

- 
- 1\_\_\_\_\_id-logo-loyalty\_\_\_\_\_ [RFC3709]
  - 2\_\_\_\_\_id-logo-background\_\_\_\_\_ [RFC3709]
  - 3\_\_\_\_\_id-logo-certImage\_\_\_\_\_ [RFC6170]

## 1.3.6.1.5.5.7.21

### Decimal Description Reference

- 
- 0\_\_\_\_\_id-ppl-anyLanguage\_\_\_\_\_ [RFC3820]
  - 1\_\_\_\_\_id-ppl-inheritAll\_\_\_\_\_ [RFC3820]
  - 2\_\_\_\_\_id-ppl-independent\_\_\_\_\_ [RFC3820]

## 1.3.6.1.5.5.7.22

### Decimal Description References

---

-----  
1\_\_\_\_\_id-mr-pkix-alphanum-ids\_\_\_\_\_Reserved and Obsolete

## 1.3.6.1.5.5.7.23

### Decimal Description References

-----  
1\_\_\_\_\_id-skis-keyHash\_\_\_\_\_Reserved and Obsolete  
2\_\_\_\_\_id-skis-4BitKeyHash\_\_\_\_\_Reserved and Obsolete  
3\_\_\_\_\_id-skis-keyInfoHash\_\_\_\_\_Reserved and Obsolete

## 1.3.6.1.5.5.7.48

### 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]

## 1.3.6.1.5.5.7.48.1

### 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]