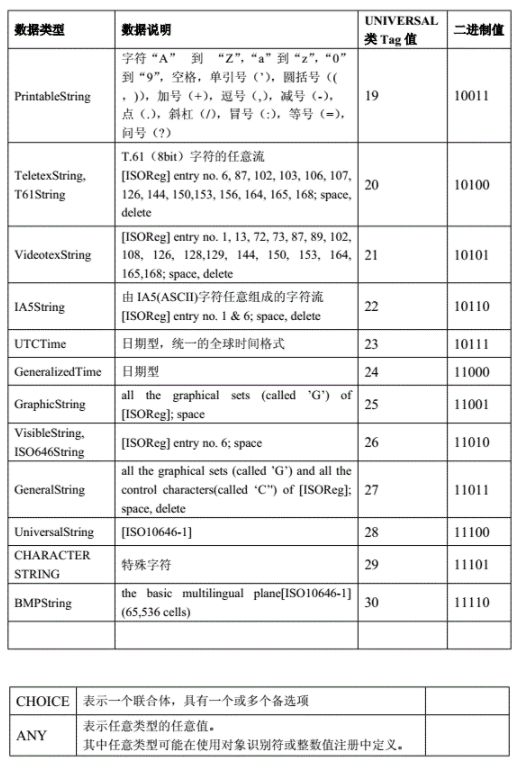
# ASN.1 常用类型编码详解







Openssl

#0 asn1\_parse2 (bp=0x6ba180, pp=0x7fffffffdba0, length=809, offset=0, depth=0, indent=0, dump=0) at crypto/asn1/asn1\_par.c:92

#1 0x00007ffff767a4f2 in ASN1\_parse\_dump (bp=0x6ba180, pp=0x6d76b0 "0\202\003%0\202\002\r\240\003\002\001\002\002\001\002\060\r\006\t\*\206H\206\367\r\001\001\v\005", len=809, indent=0,

dump=0) at crypto/asn1/asn1\_par.c:66

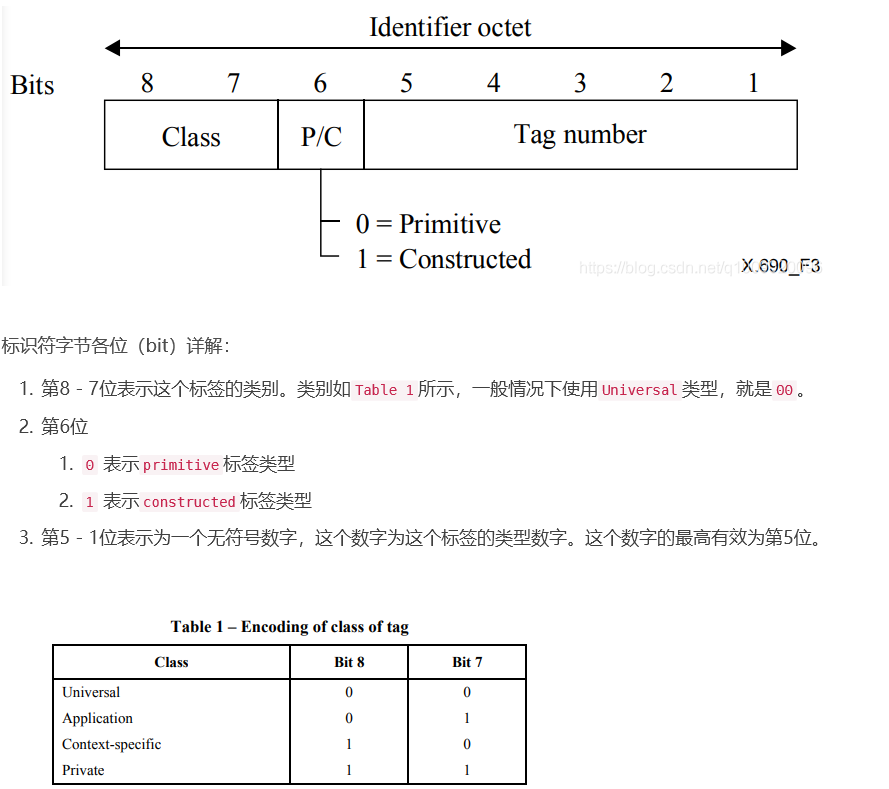
#2 0x000000000041d0b4 in asn1parse\_main (argc=0, argv=0x7fffffffe2d0) at apps/asn1pars.c:290

#3 0x0000000000437c37 in do\_cmd (prog=0x6d5b40, argc=5, argv=0x7fffffffe2d0) at apps/openssl.c:570

#4 0x000000000043708a in main (argc=5, argv=0x7fffffffe2d0) at apps/openssl.c:189

用到的证书文件 

1. steven@ubuntu:~/study2/openssl-1.1.1g/apps$ hexdump -C server.der
2. 00000000  30 82 03 25 30 82 02 0d  a0 03 02 01 02 02 01 02  |0..%0...........|
3. 00000010  30 0d 06 09 2a 86 48 86  f7 0d 01 01 0b 05 00 30  |0...\*.H........0|
4. 00000020  12 31 10 30 0e 06 03 55  04 03 0c 07 52 6f 6f 74  |.1.0...U....Root|
5. 00000030  20 43 41 30 20 17 0d 31  36 30 31 31 34 32 32 32  | CA0 ..160114222|
6. 00000040  39 34 36 5a 18 0f 32 31  31 36 30 31 31 35 32 32  |946Z..2116011522|
7. 00000050  32 39 34 36 5a 30 19 31  17 30 15 06 03 55 04 03  |2946Z0.1.0...U..|
8. 00000060  0c 0e 73 65 72 76 65 72  2e 65 78 61 6d 70 6c 65  |..server.example|
9. 00000070  30 82 01 22 30 0d 06 09  2a 86 48 86 f7 0d 01 01  |0.."0...\*.H.....|
10. 00000080  01 05 00 03 82 01 0f 00  30 82 01 0a 02 82 01 01  |........0.......|
11. 00000090  00 d5 5d 60 6a df fc 61  ee 48 aa 8c 11 48 43 a5  |..]`j..a.H...HC.|
12. 000000a0  6d b6 52 5d aa 98 49 b1  61 92 35 b1 fc 3a 04 25  |m.R]..I.a.5..:.%|
13. 000000b0  0c 6d 79 ff b4 d5 c9 e9  5c 1c 3b e0 ab b3 b8 7d  |.my.....\.;....}|
14. 000000c0  a3 de 6d bd e0 dd d7 5a  bf 14 47 11 42 5e a6 82  |..m....Z..G.B^..|
15. 000000d0  d0 61 c1 7f dd 13 46 e6  09 85 07 0e f2 d4 fc 1a  |.a....F.........|
16. 000000e0  64 d2 0a ad 20 ab 20 6b  96 f0 ad cc c4 19 53 55  |d... . k......SU|
17. 000000f0  dc 01 1d a4 b3 ef 8a b4  49 53 5d 8a 05 1c f1 dc  |........IS].....|
18. 00000100  e1 44 bf c5 d7 e2 77 19  57 5c 97 0b 75 ee 88 43  |.D....w.W\..u..C|
19. 00000110  71 0f ca 6c c1 b4 b2 50  a7 77 46 6c 58 0f 11 bf  |q..l...P.wFlX...|
20. 00000120  f1 76 24 5a ae 39 42 b7  51 67 29 e1 d0 55 30 6f  |.v$Z.9B.Qg)..U0o|
21. 00000130  17 e4 91 ea ad f8 28 c2  43 6f a2 64 a9 fb 9d 98  |......(.Co.d....|
22. 00000140  92 62 48 3e eb 0d 4f 82  4a 8a ff 3f 72 ee 96 b5  |.bH>..O.J..?r...|
23. 00000150  ae a1 c1 98 ba ef 7d 90  75 6d ff 5a 52 9e ab f5  |......}.um.ZR...|
24. 00000160  c0 7e d0 87 43 db 85 07  07 0f 7d 38 7a fd d1 d3  |.~..C.....}8z...|
25. 00000170  ee 65 1d d3 ea 39 6a 87  37 ee 4a d3 e0 0d 6e f5  |.e...9j.7.J...n.|
26. 00000180  70 ac c2 bd f1 6e f3 92  95 5e a9 f0 a1 65 95 93  |p....n...^...e..|
27. 00000190  8d 02 03 01 00 01 a3 7d  30 7b 30 1d 06 03 55 1d  |.......}0{0...U.|
28. 000001a0  0e 04 16 04 14 c0 e7 84  bf e8 59 27 33 10 b0 52  |..........Y'3..R|
29. 000001b0  4f 51 52 2f 06 d6 c0 7a  cd 30 1f 06 03 55 1d 23  |OQR/...z.0...U.#|
30. 000001c0  04 18 30 16 80 14 70 7f  2e ae 83 68 59 98 04 23  |..0...p....hY..#|
31. 000001d0  2a cd eb 3e 17 cd 24 dd  01 49 30 09 06 03 55 1d  |\*..>..$..I0...U.|
32. 000001e0  13 04 02 30 00 30 13 06  03 55 1d 25 04 0c 30 0a  |...0.0...U.%..0.|
33. 000001f0  06 08 2b 06 01 05 05 07  03 01 30 19 06 03 55 1d  |..+.......0...U.|
34. 00000200  11 04 12 30 10 82 0e 73  65 72 76 65 72 2e 65 78  |...0...server.ex|
35. 00000210  61 6d 70 6c 65 30 0d 06  09 2a 86 48 86 f7 0d 01  |ample0...\*.H....|
36. 00000220  01 0b 05 00 03 82 01 01  00 7b d3 04 43 75 8a 0f  |.........{..Cu..|
37. 00000230  11 ae c4 fb d7 a1 a2 9e  fe 20 18 d5 f4 2f 31 88  |......... .../1.|
38. 00000240  46 b6 75 8c ee e5 9b 97  a6 b9 a3 cd 60 9a 46 c3  |F.u.........`.F.|
39. 00000250  48 97 e5 97 68 f7 5a 86  35 73 d9 69 9e f9 5f 74  |H...h.Z.5s.i..\_t|
40. 00000260  b9 e6 94 13 01 cb 6a dc  e3 c4 04 e9 65 da 9c a4  |......j.....e...|
41. 00000270  8b 28 f3 f9 9a 7f bf 97  1f 45 92 e5 05 b1 56 e6  |.(.......E....V.|
42. 00000280  0b f6 47 de 1e 89 b6 2b  e1 4d df 4a 7e 01 d3 23  |..G....+.M.J~..#|
43. 00000290  dc 97 8c 47 fe 5f c7 cc  98 46 0e c4 83 5b ca 8a  |...G.\_...F...[..|
44. 000002a0  f1 52 09 be 6b ec 3f 09  8b d0 93 02 bf e1 51 e7  |.R..k.?.......Q.|
45. 000002b0  d1 7e 34 56 19 74 d0 ff  28 25 de b7 9f 56 52 91  |.~4V.t..(%...VR.|
46. 000002c0  7d 20 29 85 0a 80 44 5f  71 32 25 71 0f c2 16 e2  |} )...D\_q2%q....|
47. 000002d0  5f 6b 1d 3f 32 5b 0a 3c  74 1c b9 62 f1 ed 07 50  |\_k.?2[.<t..b...P|
48. 000002e0  a3 6d b4 b4 31 0a c0 53  44 6a 3a 88 84 8b 2d a9  |.m..1..SDj:...-.|
49. 000002f0  b0 37 8e e6 18 36 bd 9a  20 40 0f 01 92 8b 3d aa  |.7...6.. @....=.|
50. 00000300  61 e7 ae 2c ed 36 cd 3a  07 86 74 3a 29 b3 d7 3a  |a..,.6.:..t:)..:|
51. 00000310  b4 00 a9 c2 f5 92 78 0e  e2 0f a3 fe bb be e0 06  |......x.........|
52. 00000320  53 84 59 1d 90 69 e5 b6  f9                       |S.Y..i...|
53. 00000329
54. 0:d=0  hl=4 l= 710 cons: SEQUENCE
55. 0 表示节点在整个文件中的偏移长度
56. d=0 表示节点深度
58. hl=4 表示节点头字节长度
60. l=710 表示节点数据字节长度
62. cons 表示该节点为结构节点，表示包含子节点或者子结构数据
64. prim 表示该节点为原始节点，包含数据
66. SEQUENCE、OCTETSTRING等都是ASN.1中定义的数据类型，具体可以参考ASN.1格式说明。
68. 最后一个节点OCTET STRING      [HEX DUMP]，就是加密后的私钥数据。
69. steven@ubuntu:~/study2/openssl-1.1.1g/apps$ openssl asn1parse -inform DER -in server.der
70. 0:d=0  hl=4 l= 805 cons: SEQUENCE
71. 4:d=1  hl=4 l= 525 cons: SEQUENCE
72. 8:d=2  hl=2 l=   3 cons: cont [ 0 ]
73. 10:d=3  hl=2 l=   1 prim: INTEGER           :02
74. 13:d=2  hl=2 l=   1 prim: INTEGER           :02
75. 16:d=2  hl=2 l=  13 cons: SEQUENCE
76. 18:d=3  hl=2 l=   9 prim: OBJECT            :sha256WithRSAEncryption
77. 29:d=3  hl=2 l=   0 prim: NULL
78. 31:d=2  hl=2 l=  18 cons: SEQUENCE
79. 33:d=3  hl=2 l=  16 cons: SET
80. 35:d=4  hl=2 l=  14 cons: SEQUENCE
81. 37:d=5  hl=2 l=   3 prim: OBJECT            :commonName
82. 42:d=5  hl=2 l=   7 prim: UTF8STRING        :Root CA
83. 51:d=2  hl=2 l=  32 cons: SEQUENCE
84. 53:d=3  hl=2 l=  13 prim: UTCTIME           :160114222946Z
85. 68:d=3  hl=2 l=  15 prim: GENERALIZEDTIME   :21160115222946Z
86. 85:d=2  hl=2 l=  25 cons: SEQUENCE
87. 87:d=3  hl=2 l=  23 cons: SET
88. 89:d=4  hl=2 l=  21 cons: SEQUENCE
89. 91:d=5  hl=2 l=   3 prim: OBJECT            :commonName
90. 96:d=5  hl=2 l=  14 prim: UTF8STRING        :server.example
91. 112:d=2  hl=4 l= 290 cons: SEQUENCE
92. 116:d=3  hl=2 l=  13 cons: SEQUENCE
93. 118:d=4  hl=2 l=   9 prim: OBJECT            :rsaEncryption
94. 129:d=4  hl=2 l=   0 prim: NULL
95. 131:d=3  hl=4 l= 271 prim: BIT STRING
96. 406:d=2  hl=2 l= 125 cons: cont [ 3 ]
97. 408:d=3  hl=2 l= 123 cons: SEQUENCE
98. 410:d=4  hl=2 l=  29 cons: SEQUENCE
99. 412:d=5  hl=2 l=   3 prim: OBJECT            :X509v3 Subject Key Identifier
100. 417:d=5  hl=2 l=  22 prim: OCTET STRING      [HEX DUMP]:0414C0E784BFE859273310B0524F51522F06D6C07ACD
101. 441:d=4  hl=2 l=  31 cons: SEQUENCE
102. 443:d=5  hl=2 l=   3 prim: OBJECT            :X509v3 Authority Key Identifier
103. 448:d=5  hl=2 l=  24 prim: OCTET STRING      [HEX DUMP]:30168014707F2EAE8368599804232ACDEB3E17CD24DD0149
104. 474:d=4  hl=2 l=   9 cons: SEQUENCE
105. 476:d=5  hl=2 l=   3 prim: OBJECT            :X509v3 Basic Constraints
106. 481:d=5  hl=2 l=   2 prim: OCTET STRING      [HEX DUMP]:3000
107. 485:d=4  hl=2 l=  19 cons: SEQUENCE
108. 487:d=5  hl=2 l=   3 prim: OBJECT            :X509v3 Extended Key Usage
109. 492:d=5  hl=2 l=  12 prim: OCTET STRING      [HEX DUMP]:300A06082B06010505070301
110. 506:d=4  hl=2 l=  25 cons: SEQUENCE
111. 508:d=5  hl=2 l=   3 prim: OBJECT            :X509v3 Subject Alternative Name
112. 513:d=5  hl=2 l=  18 prim: OCTET STRING      [HEX DUMP]:3010820E7365727665722E6578616D706C65
113. 533:d=1  hl=2 l=  13 cons: SEQUENCE
114. 535:d=2  hl=2 l=   9 prim: OBJECT            :sha256WithRSAEncryption
115. 546:d=2  hl=2 l=   0 prim: NULL
116. 548:d=1  hl=4 l= 257 prim: BIT STRING
117. steven@ubuntu:~/study2/openssl-1.1.1g/apps$ openssl x509 -inform DER -in server.der -noout -text
118. Certificate:
119. Data:
120. Version: 3 (0x2)
121. Serial Number: 2 (0x2)
122. Signature Algorithm: sha256WithRSAEncryption
123. Issuer: CN=Root CA
124. Validity
125. Not Before: Jan 14 22:29:46 2016 GMT
126. Not After : Jan 15 22:29:46 2116 GMT
127. Subject: CN=server.example
128. Subject Public Key Info:
129. Public Key Algorithm: rsaEncryption
130. Public-Key: (2048 bit)
131. Modulus:
132. 00:d5:5d:60:6a:df:fc:61:ee:48:aa:8c:11:48:43:
133. a5:6d:b6:52:5d:aa:98:49:b1:61:92:35:b1:fc:3a:
134. 04:25:0c:6d:79:ff:b4:d5:c9:e9:5c:1c:3b:e0:ab:
135. b3:b8:7d:a3:de:6d:bd:e0:dd:d7:5a:bf:14:47:11:
136. 42:5e:a6:82:d0:61:c1:7f:dd:13:46:e6:09:85:07:
137. 0e:f2:d4:fc:1a:64:d2:0a:ad:20:ab:20:6b:96:f0:
138. ad:cc:c4:19:53:55:dc:01:1d:a4:b3:ef:8a:b4:49:
139. 53:5d:8a:05:1c:f1:dc:e1:44:bf:c5:d7:e2:77:19:
140. 57:5c:97:0b:75:ee:88:43:71:0f:ca:6c:c1:b4:b2:
141. 50:a7:77:46:6c:58:0f:11:bf:f1:76:24:5a:ae:39:
142. 42:b7:51:67:29:e1:d0:55:30:6f:17:e4:91:ea:ad:
143. f8:28:c2:43:6f:a2:64:a9:fb:9d:98:92:62:48:3e:
144. eb:0d:4f:82:4a:8a:ff:3f:72:ee:96:b5:ae:a1:c1:
145. 98:ba:ef:7d:90:75:6d:ff:5a:52:9e:ab:f5:c0:7e:
146. d0:87:43:db:85:07:07:0f:7d:38:7a:fd:d1:d3:ee:
147. 65:1d:d3:ea:39:6a:87:37:ee:4a:d3:e0:0d:6e:f5:
148. 70:ac:c2:bd:f1:6e:f3:92:95:5e:a9:f0:a1:65:95:
149. 93:8d
150. Exponent: 65537 (0x10001)
151. X509v3 extensions:
152. X509v3 Subject Key Identifier:
153. C0:E7:84:BF:E8:59:27:33:10:B0:52:4F:51:52:2F:06:D6:C0:7A:CD
154. X509v3 Authority Key Identifier:
155. keyid:70:7F:2E:AE:83:68:59:98:04:23:2A:CD:EB:3E:17:CD:24:DD:01:49
157. X509v3 Basic Constraints:
158. CA:FALSE
159. X509v3 Extended Key Usage:
160. TLS Web Server Authentication
161. X509v3 Subject Alternative Name:
162. DNS:server.example
163. Signature Algorithm: sha256WithRSAEncryption
164. 7b:d3:04:43:75:8a:0f:11:ae:c4:fb:d7:a1:a2:9e:fe:20:18:
165. d5:f4:2f:31:88:46:b6:75:8c:ee:e5:9b:97:a6:b9:a3:cd:60:
166. 9a:46:c3:48:97:e5:97:68:f7:5a:86:35:73:d9:69:9e:f9:5f:
167. 74:b9:e6:94:13:01:cb:6a:dc:e3:c4:04:e9:65:da:9c:a4:8b:
168. 28:f3:f9:9a:7f:bf:97:1f:45:92:e5:05:b1:56:e6:0b:f6:47:
169. de:1e:89:b6:2b:e1:4d:df:4a:7e:01:d3:23:dc:97:8c:47:fe:
170. 5f:c7:cc:98:46:0e:c4:83:5b:ca:8a:f1:52:09:be:6b:ec:3f:
171. 09:8b:d0:93:02:bf:e1:51:e7:d1:7e:34:56:19:74:d0:ff:28:
172. 25:de:b7:9f:56:52:91:7d:20:29:85:0a:80:44:5f:71:32:25:
173. 71:0f:c2:16:e2:5f:6b:1d:3f:32:5b:0a:3c:74:1c:b9:62:f1:
174. ed:07:50:a3:6d:b4:b4:31:0a:c0:53:44:6a:3a:88:84:8b:2d:
175. a9:b0:37:8e:e6:18:36:bd:9a:20:40:0f:01:92:8b:3d:aa:61:
176. e7:ae:2c:ed:36:cd:3a:07:86:74:3a:29:b3:d7:3a:b4:00:a9:
177. c2:f5:92:78:0e:e2:0f:a3:fe:bb:be:e0:06:53:84:59:1d:90:
178. 69:e5:b6:f9



0x30 class 0 0 P/C 1

steven@ubuntu:~/study2/openssl-1.1.1g/doc/man1$ pod2text asn1parse.pod