PKCS7 格式

ContentInfo ::= SEQUENCE{

contentType ContentType,

content

[0] EXPLICIT ANY DEFINED BY contentType OPTIONAL

}

ContentType ::= OBJECT IDENTIFIER

Data content type

Data ::= OCTET STRING

Signed-data content type

SignedData ::= SEQUENCE{

version Version,

digestAlgorithms DigestAlgorithmIdentifiers,

contentInfo ContentInfo,

certificates

[0] IMPLICIT ExtendedCertificateAndCertifcates OPTIONAL,

crls

[1] IMPLICIT CertificateRevocationLists OPTIONAL,

signerInfos SIgnerInfos

}

DigestAlgorithmIdentifiers ::= SET OF DigestAlgorithmIdentifier

SignerInfos := SET OF SignerInfo

SignerInfo ::= SEQUENCE{

version Version,

issuerAndSerialNumber IssuerAndSerialNumber,

digestAlgorithm DigestAlgorithmIdentifier,

authenticatedAttributes

[0] IMPLICIT Attributes OPTIONAL,

digestEncryptionAlgorithm DigestEncryptionAlgorithmIdentifier,

encryptedDigest EncryptedDigest,

unauthenticatedAttributes

[1] IMPLICIT Attributes OPTIONAL

}

EncryptedDigest ::= OCTET STRING

<http://qistoph.blogspot.com/2012/01/manual-verify-pkcs7-signed-data-with.html>

1 **openssl asn1parse -inform der -in test.RSA**

0:d=0 hl=4 l=1322 cons: SEQUENCE

4:d=1 hl=2 l= 9 prim: OBJECT :pkcs7-signedData

15:d=1 hl=4 l=1307 cons: cont [ 0 ]

19:d=2 hl=4 l=1303 cons: SEQUENCE

23:d=3 hl=2 l= 1 prim: INTEGER :01

26:d=3 hl=2 l= 11 cons: SET

28:d=4 hl=2 l= 9 cons: SEQUENCE

30:d=5 hl=2 l= 5 prim: OBJECT :sha1

37:d=5 hl=2 l= 0 prim: NULL

39:d=3 hl=2 l= 11 cons: SEQUENCE

41:d=4 hl=2 l= 9 prim: OBJECT :pkcs7-data

52:d=3 hl=4 l= 867 cons: cont [ 0 ]

56:d=4 hl=4 l= 863 cons: SEQUENCE

60:d=5 hl=4 l= 583 cons: SEQUENCE

64:d=6 hl=2 l= 3 cons: cont [ 0 ]

66:d=7 hl=2 l= 1 prim: INTEGER :02

69:d=6 hl=2 l= 4 prim: INTEGER :7D1D238B

75:d=6 hl=2 l= 13 cons: SEQUENCE

77:d=7 hl=2 l= 9 prim: OBJECT :sha256WithRSAEncryption

88:d=7 hl=2 l= 0 prim: NULL

90:d=6 hl=2 l= 96 cons: SEQUENCE

92:d=7 hl=2 l= 11 cons: SET

94:d=8 hl=2 l= 9 cons: SEQUENCE

96:d=9 hl=2 l= 3 prim: OBJECT :countryName

101:d=9 hl=2 l= 2 prim: PRINTABLESTRING :CN

105:d=7 hl=2 l= 18 cons: SET

107:d=8 hl=2 l= 16 cons: SEQUENCE

109:d=9 hl=2 l= 3 prim: OBJECT :stateOrProvinceName

114:d=9 hl=2 l= 9 prim: PRINTABLESTRING :GuangDong

125:d=7 hl=2 l= 18 cons: SET

127:d=8 hl=2 l= 16 cons: SEQUENCE

129:d=9 hl=2 l= 3 prim: OBJECT :localityName

134:d=9 hl=2 l= 9 prim: PRINTABLESTRING :ShenZheng

145:d=7 hl=2 l= 11 cons: SET

147:d=8 hl=2 l= 9 cons: SEQUENCE

149:d=9 hl=2 l= 3 prim: OBJECT :organizationName

154:d=9 hl=2 l= 2 prim: PRINTABLESTRING :CL

158:d=7 hl=2 l= 11 cons: SET

160:d=8 hl=2 l= 9 cons: SEQUENCE

162:d=9 hl=2 l= 3 prim: OBJECT :organizationalUnitName

167:d=9 hl=2 l= 2 prim: PRINTABLESTRING :CL

171:d=7 hl=2 l= 15 cons: SET

173:d=8 hl=2 l= 13 cons: SEQUENCE

175:d=9 hl=2 l= 3 prim: OBJECT :commonName

180:d=9 hl=2 l= 6 prim: PRINTABLESTRING :caoliu

188:d=6 hl=2 l= 30 cons: SEQUENCE

190:d=7 hl=2 l= 13 prim: UTCTIME :150908045605Z

205:d=7 hl=2 l= 13 prim: UTCTIME :430124045605Z

220:d=6 hl=2 l= 96 cons: SEQUENCE

222:d=7 hl=2 l= 11 cons: SET

224:d=8 hl=2 l= 9 cons: SEQUENCE

226:d=9 hl=2 l= 3 prim: OBJECT :countryName

231:d=9 hl=2 l= 2 prim: PRINTABLESTRING :CN

235:d=7 hl=2 l= 18 cons: SET

237:d=8 hl=2 l= 16 cons: SEQUENCE

239:d=9 hl=2 l= 3 prim: OBJECT :stateOrProvinceName

244:d=9 hl=2 l= 9 prim: PRINTABLESTRING :GuangDong

255:d=7 hl=2 l= 18 cons: SET

257:d=8 hl=2 l= 16 cons: SEQUENCE

259:d=9 hl=2 l= 3 prim: OBJECT :localityName

264:d=9 hl=2 l= 9 prim: PRINTABLESTRING :ShenZheng

275:d=7 hl=2 l= 11 cons: SET

277:d=8 hl=2 l= 9 cons: SEQUENCE

279:d=9 hl=2 l= 3 prim: OBJECT :organizationName

284:d=9 hl=2 l= 2 prim: PRINTABLESTRING :CL

288:d=7 hl=2 l= 11 cons: SET

290:d=8 hl=2 l= 9 cons: SEQUENCE

292:d=9 hl=2 l= 3 prim: OBJECT :organizationalUnitName

297:d=9 hl=2 l= 2 prim: PRINTABLESTRING :CL

301:d=7 hl=2 l= 15 cons: SET

303:d=8 hl=2 l= 13 cons: SEQUENCE

305:d=9 hl=2 l= 3 prim: OBJECT :commonName

310:d=9 hl=2 l= 6 prim: PRINTABLESTRING :caoliu

318:d=6 hl=4 l= 290 cons: SEQUENCE

322:d=7 hl=2 l= 13 cons: SEQUENCE

324:d=8 hl=2 l= 9 prim: OBJECT :rsaEncryption

335:d=8 hl=2 l= 0 prim: NULL

337:d=7 hl=4 l= 271 prim: BIT STRING

612:d=6 hl=2 l= 33 cons: cont [ 3 ]

614:d=7 hl=2 l= 31 cons: SEQUENCE

616:d=8 hl=2 l= 29 cons: SEQUENCE

618:d=9 hl=2 l= 3 prim: OBJECT :X509v3 Subject Key Identifier

623:d=9 hl=2 l= 22 prim: OCTET STRING [HEX DUMP]:0414AC0C9E51D9D30798B1FB44732B23DEF59E0F641A

647:d=5 hl=2 l= 13 cons: SEQUENCE

649:d=6 hl=2 l= 9 prim: OBJECT :sha256WithRSAEncryption

660:d=6 hl=2 l= 0 prim: NULL

662:d=5 hl=4 l= 257 prim: BIT STRING

923:d=3 hl=4 l= 399 cons: SET

927:d=4 hl=4 l= 395 cons: SEQUENCE

931:d=5 hl=2 l= 1 prim: INTEGER :01

934:d=5 hl=2 l= 104 cons: SEQUENCE

936:d=6 hl=2 l= 96 cons: SEQUENCE

938:d=7 hl=2 l= 11 cons: SET

940:d=8 hl=2 l= 9 cons: SEQUENCE

942:d=9 hl=2 l= 3 prim: OBJECT :countryName

947:d=9 hl=2 l= 2 prim: PRINTABLESTRING :CN

951:d=7 hl=2 l= 18 cons: SET

953:d=8 hl=2 l= 16 cons: SEQUENCE

955:d=9 hl=2 l= 3 prim: OBJECT :stateOrProvinceName

960:d=9 hl=2 l= 9 prim: PRINTABLESTRING :GuangDong

971:d=7 hl=2 l= 18 cons: SET

973:d=8 hl=2 l= 16 cons: SEQUENCE

975:d=9 hl=2 l= 3 prim: OBJECT :localityName

980:d=9 hl=2 l= 9 prim: PRINTABLESTRING :ShenZheng

991:d=7 hl=2 l= 11 cons: SET

993:d=8 hl=2 l= 9 cons: SEQUENCE

995:d=9 hl=2 l= 3 prim: OBJECT :organizationName

1000:d=9 hl=2 l= 2 prim: PRINTABLESTRING :CL

1004:d=7 hl=2 l= 11 cons: SET

1006:d=8 hl=2 l= 9 cons: SEQUENCE

1008:d=9 hl=2 l= 3 prim: OBJECT :organizationalUnitName

1013:d=9 hl=2 l= 2 prim: PRINTABLESTRING :CL

1017:d=7 hl=2 l= 15 cons: SET

1019:d=8 hl=2 l= 13 cons: SEQUENCE

1021:d=9 hl=2 l= 3 prim: OBJECT :commonName

1026:d=9 hl=2 l= 6 prim: PRINTABLESTRING :caoliu

1034:d=6 hl=2 l= 4 prim: INTEGER :7D1D238B

1040:d=5 hl=2 l= 9 cons: SEQUENCE

1042:d=6 hl=2 l= 5 prim: OBJECT :sha1

1049:d=6 hl=2 l= 0 prim: NULL

1051:d=5 hl=2 l= 13 cons: SEQUENCE

1053:d=6 hl=2 l= 9 prim: OBJECT :rsaEncryption

1064:d=6 hl=2 l= 0 prim: NULL

1066:d=5 hl=4 l= 256 prim: OCTET STRING [HEX DUMP]:110383A203AC1AB751BFBE2797EB86F2850A43D8C9A6639260A57A33371FA4C378 D1778781D0A51C42E745BAEAD50BC1F10104FA7C2D0E451B3BD8CEE9C006C19AC8364A72C29BB4237105F07716D5396976CB1F3875E687249BA32A078D20 04CA8AAE4A66728C1A2C5C54ED57D5252A335D2DACC1CD5BF097017D6F44DD1498E2FD7C41BBCAAE5C6485C9362C64B267085AE6B6515921CEF481D314B3 B8CEC06DF1ADB5713A2A9A56AAD1497DC5BE27A0AC7223D53B762E144C3D820AB10FAF051A6409BB7BC70B502C5BFFEAD1C43210222C370A343301A72AC8 FFD42653301C04706C585A99893EFB37D5BD28E37D25A4C496580DE077F7CA9B1C61EFB0F2

2 openssl pkcs7 -print\_certs -inform der -in test.RSA -out cert.cer

3 **dd if=test.RSA of=signed-sha1.bin bs=1 skip=$[1066+4] count=256**

4 hexdump -C signed-sha1.bin

5 openssl x509 -inform pem -in cert.cer -noout -pubkey > pubkey.pem

6 openssl rsautl -verify -pubin -inkey pubkey.pem < signed-sha1.bin > verified.bin

7 hexdump -C verified.bin

8 **openssl asn1parse -inform der -in verified.bin**

0:d=0 hl=2 l= 33 cons: SEQUENCE

2:d=1 hl=2 l= 9 cons: SEQUENCE

4:d=2 hl=2 l= 5 prim: OBJECT :sha1

11:d=2 hl=2 l= 0 prim: NULL

13:d=1 hl=2 l= 20 prim: OCTET STRING [HEX DUMP]:**FDBC3CBBE9B1B8E05F728724FC26A8718C171055**

**正版：**

openssl asn1parse -inform der -in verified.bin

0:d=0 hl=2 l= 33 cons: SEQUENCE

2:d=1 hl=2 l= 9 cons: SEQUENCE

4:d=2 hl=2 l= 5 prim: OBJECT :sha1

11:d=2 hl=2 l= 0 prim: NULL

13:d=1 hl=2 l= 20 prim: OCTET STRING [HEX DUMP]:D2FC0085A2BCEDC6CA3CE3 53B1AA94BF2C46248C

Python hash.py –hash=all CERT.SF

[sha1]CERT.SF:d2fc0085a2bcedc6ca3ce353b1aa94bf2c46248c

破解版:

openssl asn1parse -inform der -in verified.bin

0:d=0 hl=2 l= 33 cons: SEQUENCE

2:d=1 hl=2 l= 9 cons: SEQUENCE

4:d=2 hl=2 l= 5 prim: OBJECT :sha1

11:d=2 hl=2 l= 0 prim: NULL

13:d=1 hl=2 l= 20 prim: OCTET STRING

[HEX DUMP]:**D2FC0085A2BCEDC6CA3CE353B1AA94BF2C46248C**

[sha1]ERROR.SF:a36ae005b7795f35d26cb6a9a63b1a39286b3f16