About the rsac specification

As a method of public key cipher, only RSA public key cipher can be handled.

It does not handle DSS, DSA, ECDSA, Elliptic Curve Cryptography etc.

X.509 public key certificates and digital signatures created using DSS, DSA, ECDSA, Elliptic Curve Cryptography etc. can not be handled at all.

The key length can be 512 bits long, 1,024 bits long and 2,048 bits long.
It does not support 4,096 bits long keys.

It can not handle ASN.1 syntax that uses the indefinite length form.

Certificate chain verification of X.509 certificates has not been performed.

It does not check CRL.

There is no compatibility or interoperability with pgp and SSH.
pgp and SSH are proprietary specifications.
It is not a specification called standard.

About ASN.1 syntax using the indefinite length form

The following is the beginning of Section 4.5 of RFC 4134.

4.5. All RSA Signed Message

Same as 4.2, but includes Carl's RSA root cert (but no CRL). A SignedData with no attribute certificates, signed by Alice using RSA, her certificate and Carl's root cert, no CRL. The message is ExContent, and is included in the eContent. There are no signed or unsigned attributes.

```
 0 30 NDEF: SEQUENCE {
 2 06    9:   OBJECT IDENTIFIER signedData (1 2 840 113549 1 7 2)
        :     (PKCS #7)
13 A0 NDEF:   [0] {
15 30 NDEF:     SEQUENCE {
17 02    1:       INTEGER 1
20 31   11:       SET {
22 30    9:         SEQUENCE {
24 06    5:           OBJECT IDENTIFIER sha1 (1 3 14 3 2 26)
        :             (OIW)
31 05    0:           NULL
        :           }
        :         }
33 30 NDEF:       SEQUENCE {
35 06    9:         OBJECT IDENTIFIER data (1 2 840 113549 1 7 1)
        :           (PKCS #7)
46 A0 NDEF:         [0] {
48 24 NDEF:           OCTET STRING {
50 04    4:             OCTET STRING 'This'
56 04   24:             OCTET STRING ' is some sample content.'
        :             }
        :           }
        :         }
```

13 A0 NDEF

like the above、the part marked as NDEF indicates that the length is in the indefinite length form.

rsac does not parse ASN.1 syntax using the indefinite length form for length values.

Therefore, rsac can not read ASN.1 syntax using the indefinite length form at all.

Reading stops immediately upon detection of the indefinite length form.