Simple explanation

rsac is software that performs encryption and digital signature using RSA public key cipher.

It supports keys of 512 bits long, 1,024 bits long and 2,048 bits long.

It does not support keys of 4,096 bits long.

As the encryption method, it supports PKCS#1 v.1.5 and RSA-KEM.

The digital signature uses PKCS#1 v.1.5 as a method.

The storage format is PKCS#7 SignedData.

You can use X.509 Public Key Certificate, PKCS#12 for encryption and creation (sign) and verification of digital signatures.

It can be used by any application that conforms to the standard specification.

It has a simple structure, but you can also create an X.509 public key certificate and PKCS#12.

It does not support DSS, DSA, ECDSA, and Elliptic Curve Cryptography etc. at all.

In addition, as auxiliary ones, random number split cipher, block cipher (AES-256-CBC), hash function, HMAC etc. are also implemented.