Usable keys for rsac

Key length

It can be 512 bits long, 1,024 bits long, or 2,048 bits long.
It does not support 4,096 bits long.

Private key

PKCS#8 PrivateKeyInfo (PEM format)

PKCS#12 (binary format)

Public key

PKCS#10 SubjectPublicKeyInfo (PEM format)

X.509 public key certificate (binary format)

These four things can be used with rsac.

It is assumed that the private key is encrypted.
If you want to use a private key, you need to specify a password.

Unencrypted PKCS#8 PrivateKeyInfo type is not supported.

It is assumed that the public key is not encrypted.

The PKCS#12 also contains the public key.
Therefore, it is also possible to use PKCS#12 as a public key.
However, rsac does not use PKCS#12 as a public key as a specification of the application.

Get the public key from PKCS#12.

Retrieve an X.509 public key certificate from PKCS#12.

If you do so, the public key in PKCS#12 can be used.

Private key

PKCS#8 PrivateKeyInfo

PKCS#12

for the above, there are clear rules and specifications for encryption and key generation.

You can not use keys that do not conform to the standard regulations and specifications.

The pgp key and the SSH key are not standard keys.

The pgp key is a key that conforms to pgp specifications.

The SSH key is a key that conforms to the SSH specification.

PEM format X.509 certificates can be used by converting them into binary format using "PEM → Binary conversion".

rsac itself also has commands to output PEM format X.509 public key certificates.

Even if created by rsac, PEM format X.509 certificates can not be used as is with rsac.