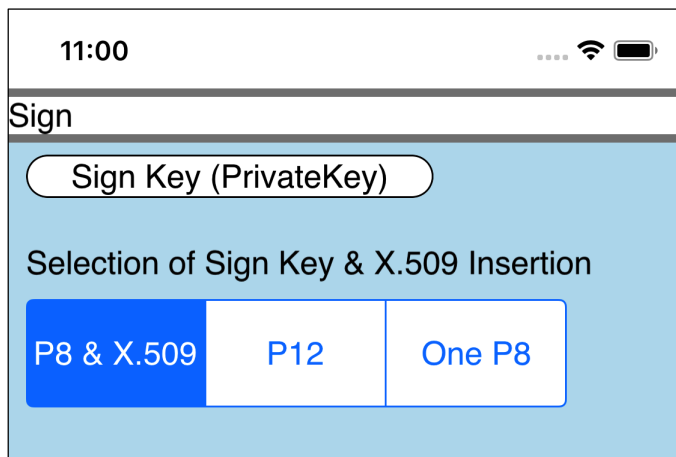


Digital signature code behavior

In rsac's digital signature, the type of private key below decides whether an X.509 certificate that contains the public key pair with private key used to sign is contained in digital signature.



In the following two case, the X.509 certificate noted on the right is contained in the digital signature.

“P8 & X509” leftmost	the X.509 certificate specified for storing
“P12” in middle	the X.509 certificate contained in PKCS#12

In the case of the rightmost “One P8”, an X.509 certificate is not stored in the digital signature.

Whether an X.509 certificate that contains the public key pair with private key used to sign is included in the digital signature?

Which an X.509 certificate is included if including?

It is the type of private key used to sign to decide this.

Such behavior may be a bit confusing.

However, from the experience so far, this designation method is the most appropriate.