About the sign rsac does

Signing is done using RSA public key cipher.

Sign and verification can not be handled at all for encryption methods other than RSA public key cipher.

The key length depends on the key used.
It supports keys of 512 bits in length, 1,024 bits in length, and 2,048 bits in length.
It does not support 4,096 bits keys.

The created digital signature value is stored in PKCS#7 SignedData.

> Whether the signature target is stored in the digital signature?
>
> Whether the X.509 certificate which store the public key of the private key pair used to create the signature is stored in the digital signature?

It is able to choose.

It have not verified the certificate chain for X.509 certificates.

PKCS#7 SignedData which have the indefinite length form for the Length Octets is not able to handled at all.

【About AuthenticatedAttributes of PKCS#7 SignedData】

The part to be subject to digital signature value calculation and the signature value are different in the signature using AuthenticatedAttributes and the signatures that do not use AuthenticatedAttributes.

rsac for iOS does not use AuthenticatedAttributes for signing.

rsac supports signing using AuthenticatedAttributes as the program code.

However, rsac for iOS does not perform (do not use) signatures using AuthenticatedAttributes.

It is out of support whether rsac for iOS can verify signatures using AuthenticatedAttributes created by other applications properly.

> Verification of signatures created by other applications that do not use AuthenticatedAttributes.

This is a normal PKCS#7 SignedData signature verification, so it works without any problems.