Sign 4

Signature creation using one private key

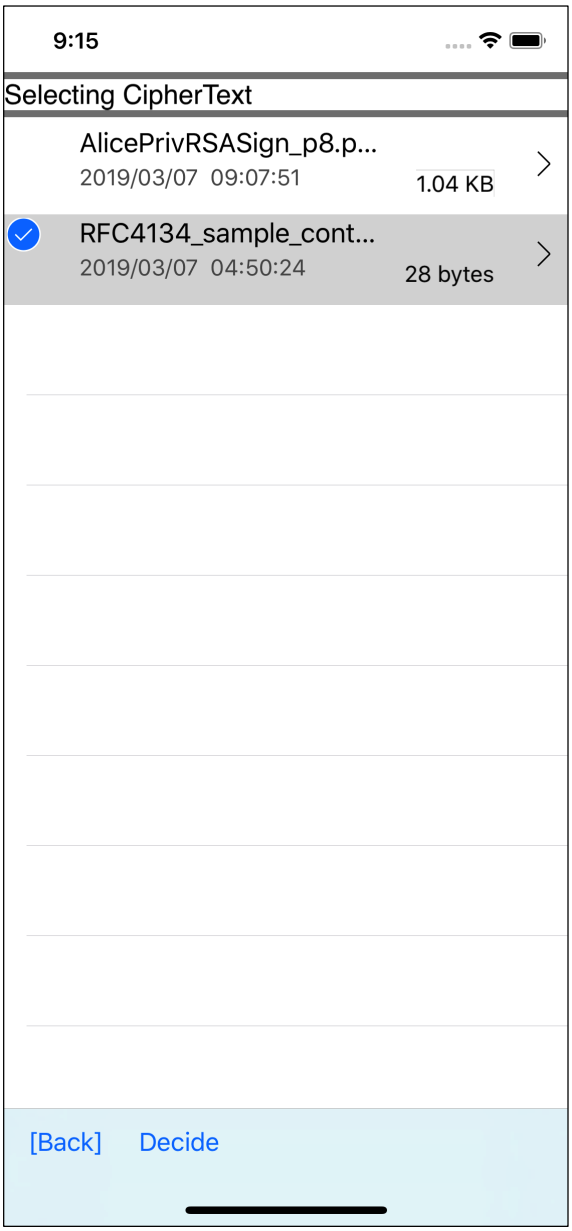
Includes signature targets.

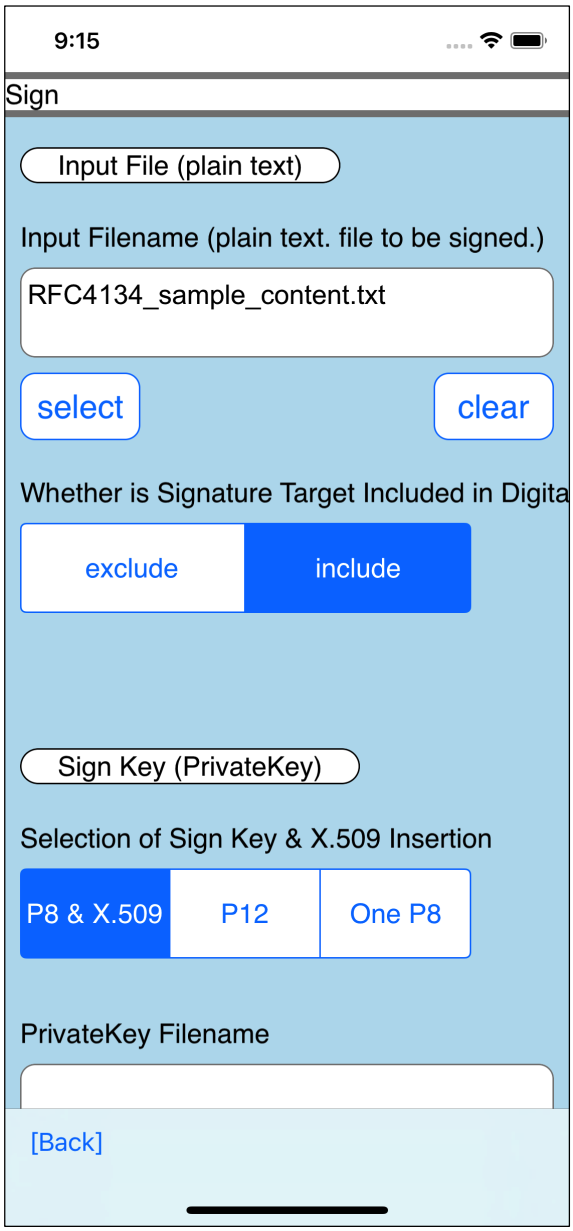
Does not include an X.509 certificate that contains the public key pair with the private key used for signing.

In rsac, when creating a digital signature using one private key, it is operated as "X. 509 certificate is not stored in digital signature (PKCS#7 SignedData)".

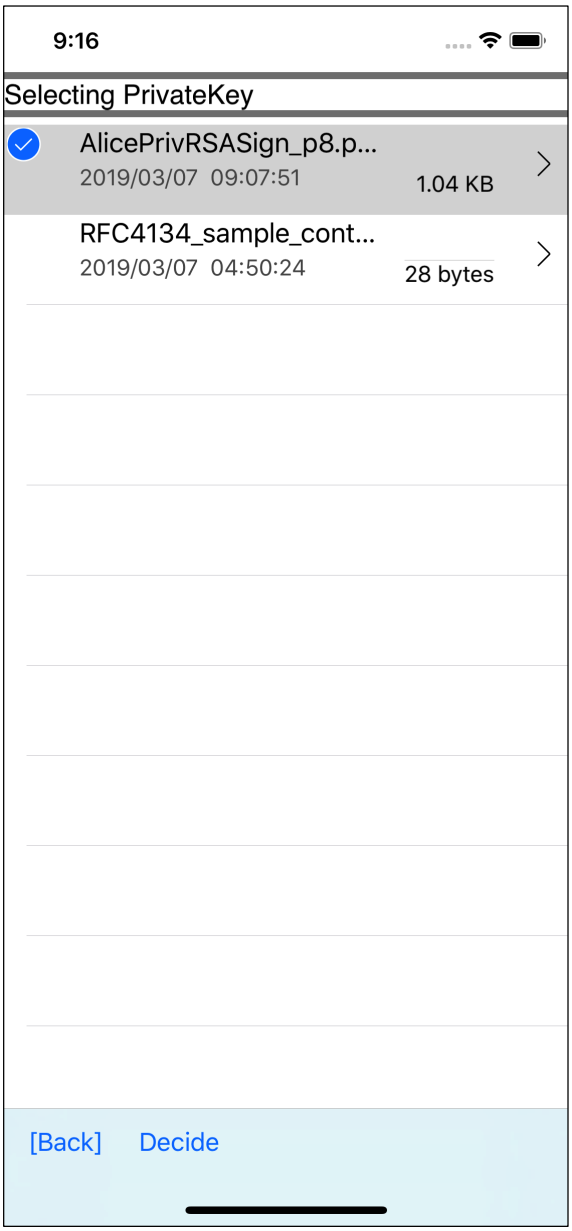
Use the segmented control to select whether to store the signature target in the digital signature (PKCS#7 SignedData).

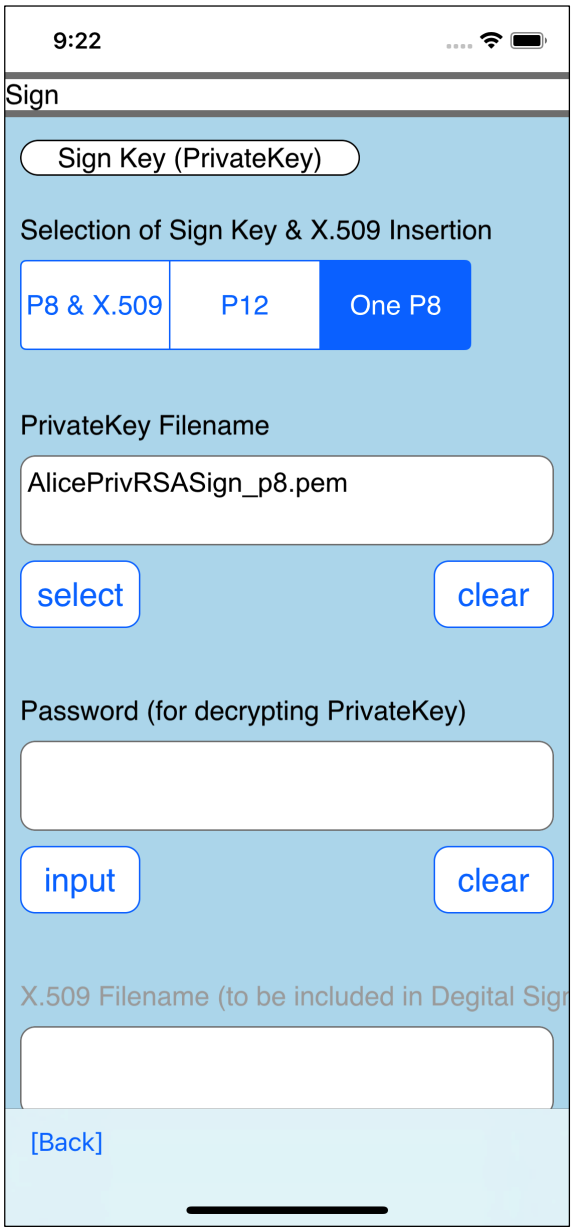
In this example, the signature target is stored in the digita4 signature (PKCS#7 SignedData).





In this example, since including the signature target in the digital signature (PKCS#7 SignedData)", so select the option of "include".

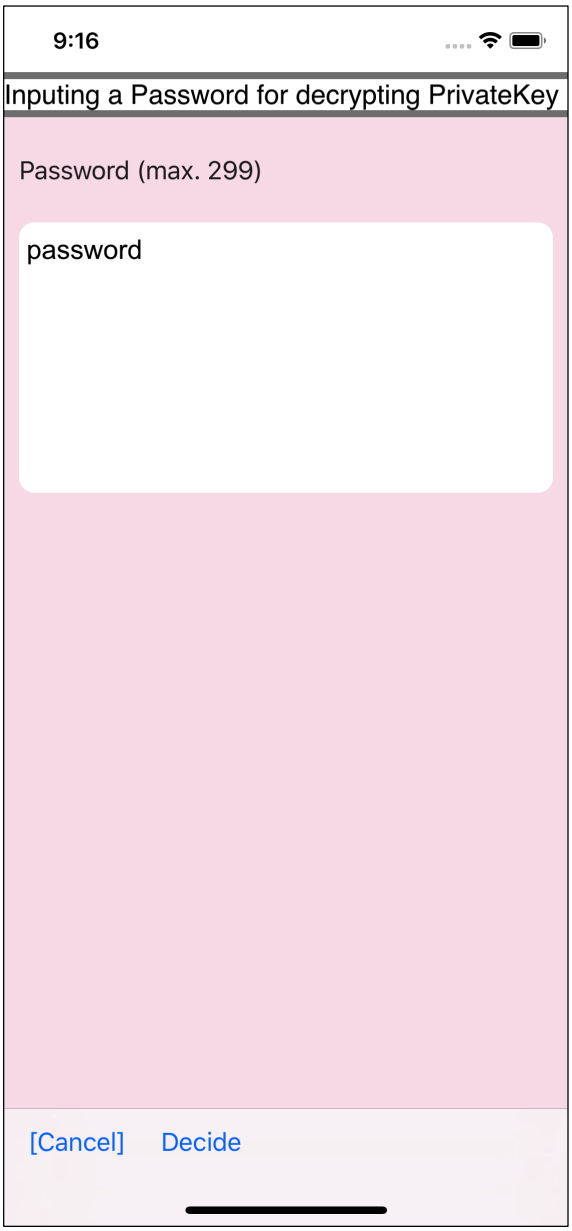


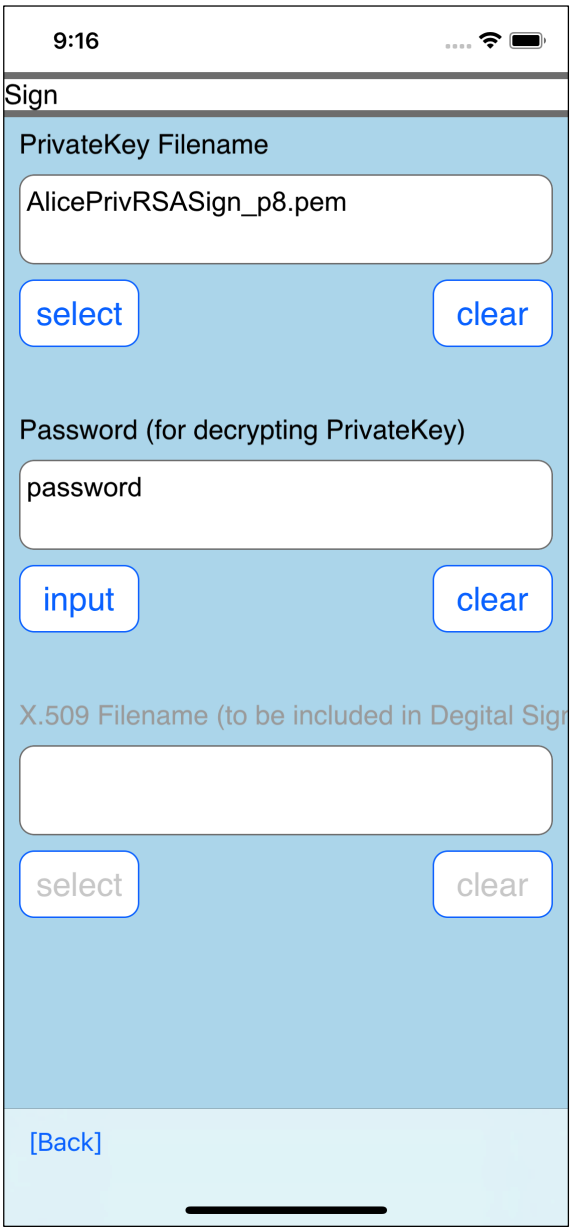


The private key type is selected as one private key.

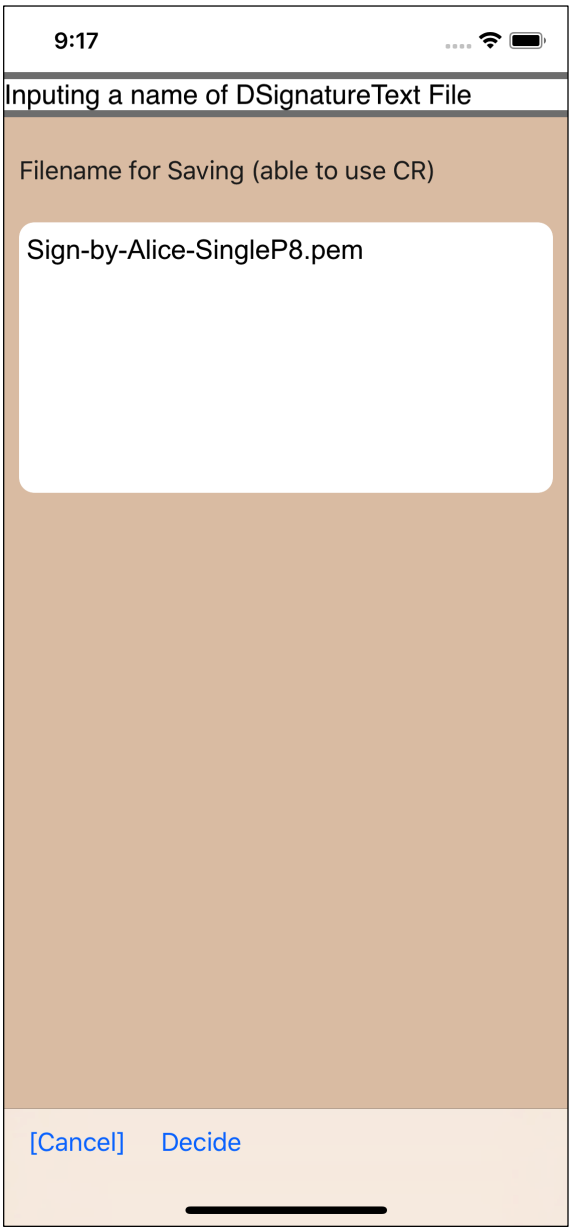
This is an indication that "X. 509 certificate is not stored in digital signature (PKCS#7 SignedData)".

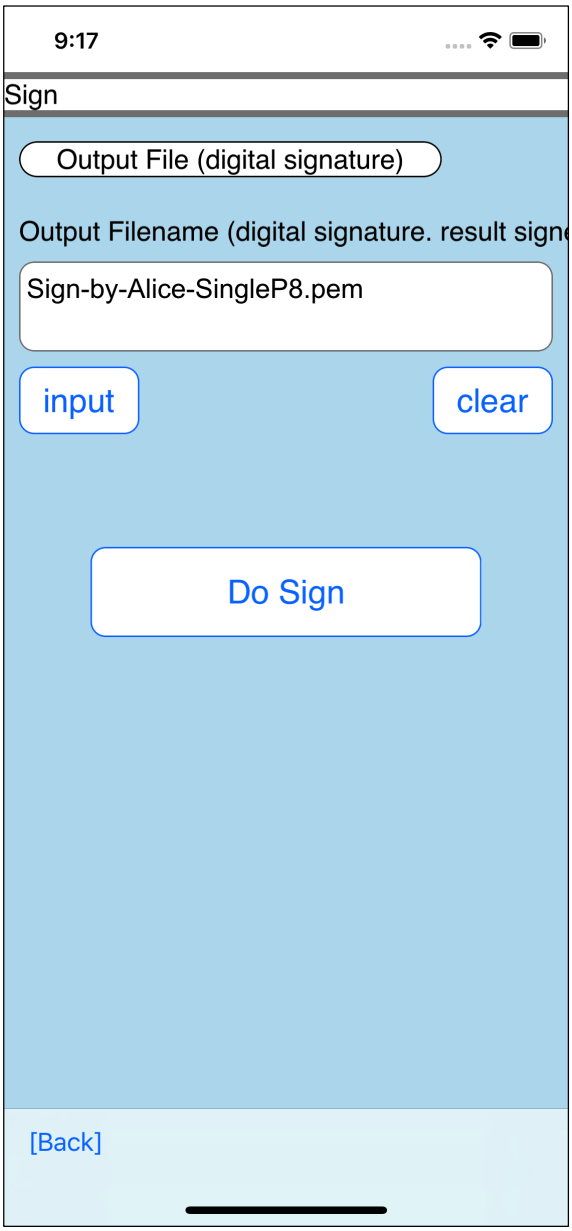
The X.509 certificate file name field is invalidated.





Specifies the password used to decrypt the private key.

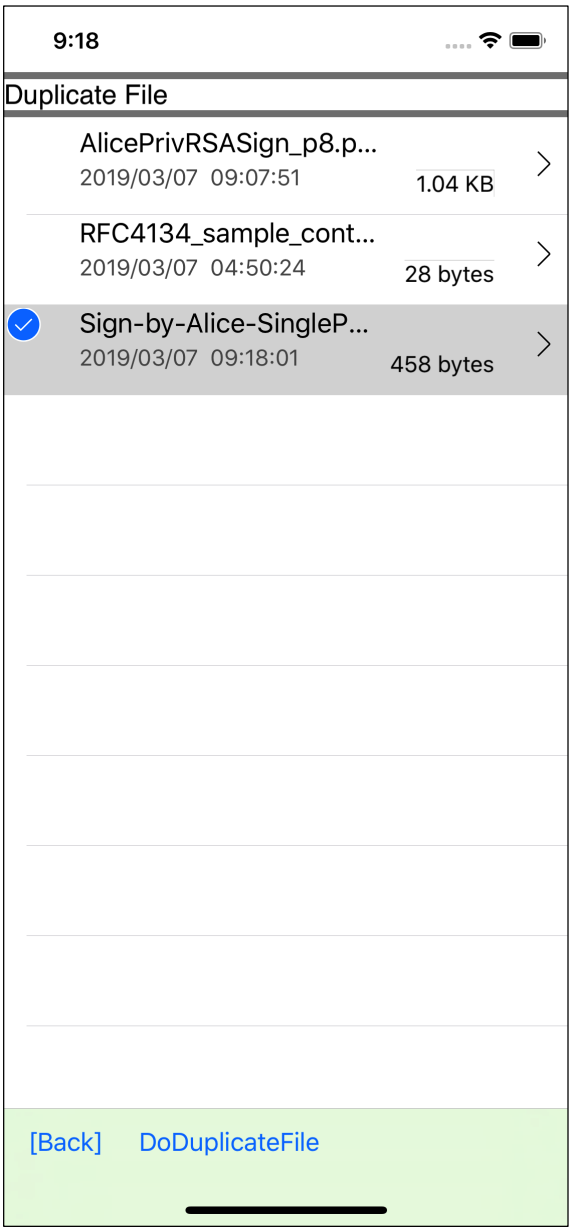




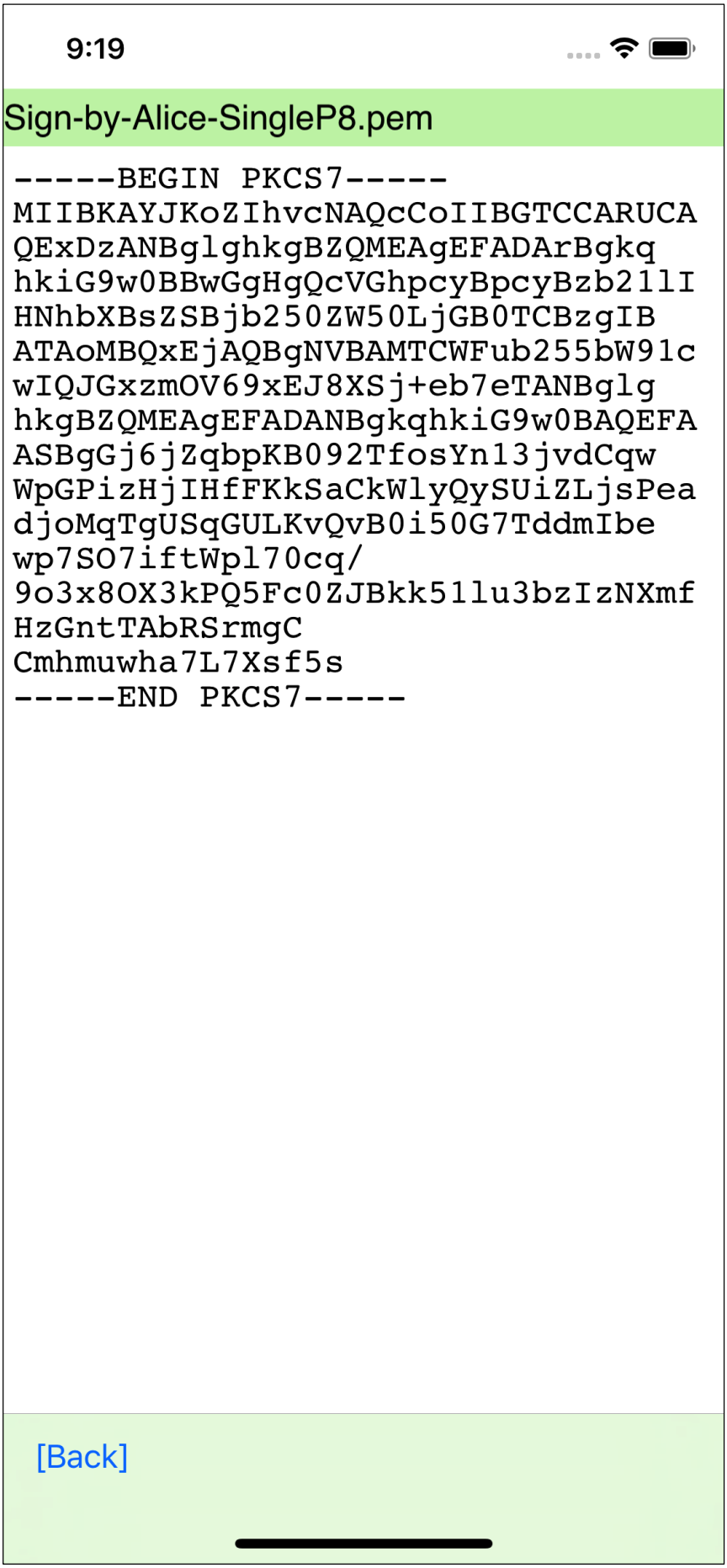
Specify the output destination file of the created digital signature.

In this state, press the "Do Sign" button to create a digital signature.

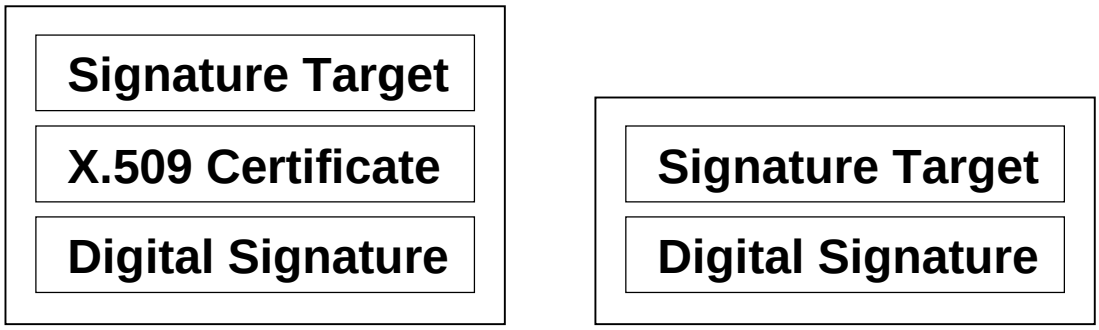
Messages are not displayed during or after execution.



Let's use "Duplicating File" command to see the created digital signature.


9:19
Sign-by-Alice-SingleP8.pem
-----BEGIN PKCS7-----
MIIBKAYJKoZIhvcNAQcCoIIBGTCCARUCA
QExDzANBglghkgBZQMEAgEFADArBgkq
hkiG9w0BBwGgHgQcVGhpcyBpcyBzb21lI
HNhbXBsZSBjb250ZW50LjGB0TCBzgIB
ATAoMBQxEjAQBgNVBAMTCWFub255bW91c
wIQJGxzmOV69xEJ8XSj+eb7eTANBglg
hkgBZQMEAgEFADANBgkqhkiG9w0BAQEFA
ASBgGj6jZqbpKB092TfosYn13jvdCqw
WpGPizHjIHfFKkSaCkWlyQySUiZLjsPea
djoMqTgUSqGULKvQvB0i50G7TddmIbe
wp7SO7iftWpl70cq/
9o3x8OX3kPQ5Fc0ZJBkk51lu3bzIzNXmf
HzGntTAbRSrmgC
Cmhmuwha7L7Xsf5s
-----END PKCS7-----
[Back]

The created digital signature (PKCS#7 SignedData) does not contain an X.509 certificate.



If it is a figure, it will be something like the right.

The size is smaller because there is no X.509 certificate.

When verifying this digital signature (PKCS#7 SignedData), it is necessary to specify either the public key itself or an X.509 certificate in which the public key is stored.

This is because the public key used for signature verification (decryption of public key cipher) is not included in the digital signature (PKCS#7 SignedData).