Sign 5

Signature creation using one private key

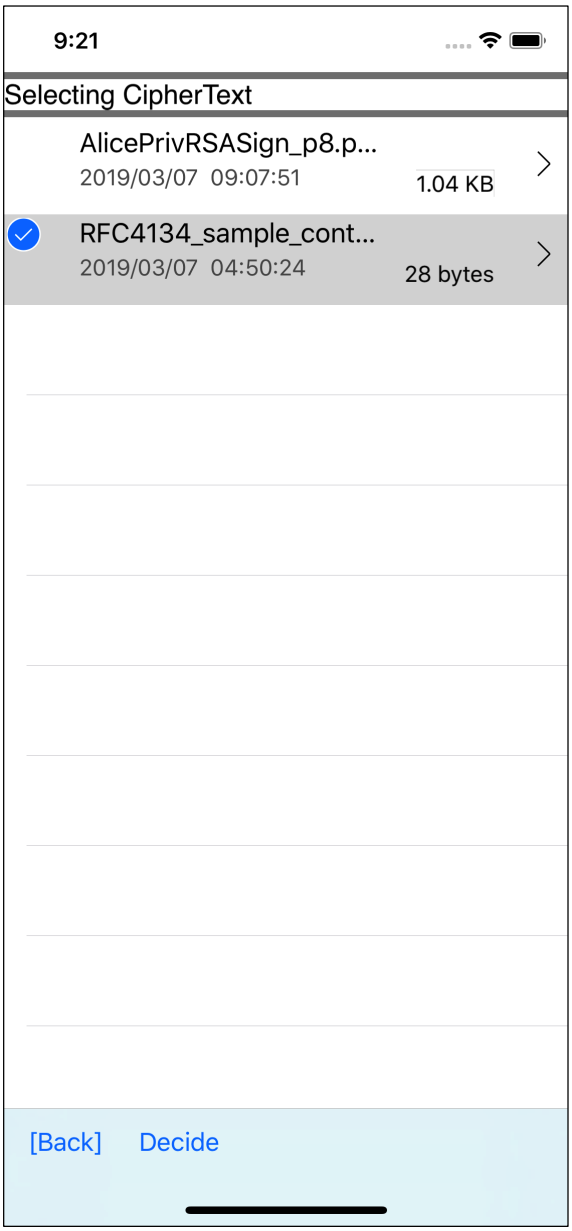
Does not include signature target.

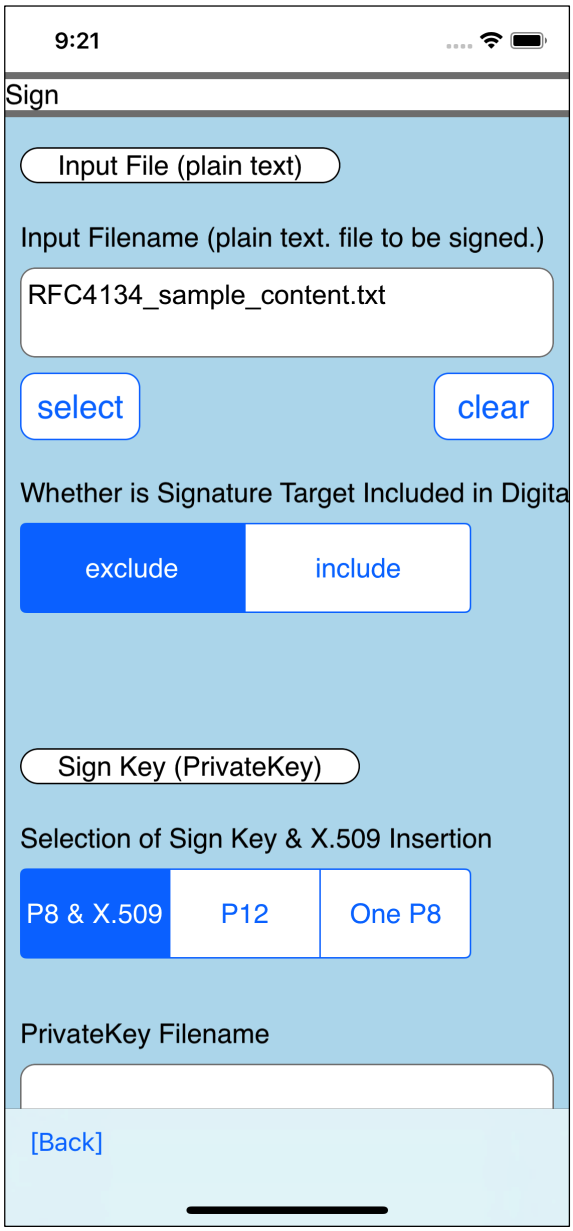
Does not include an X.509 certificate that contains the public key pair with the private key used for signing.

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)".

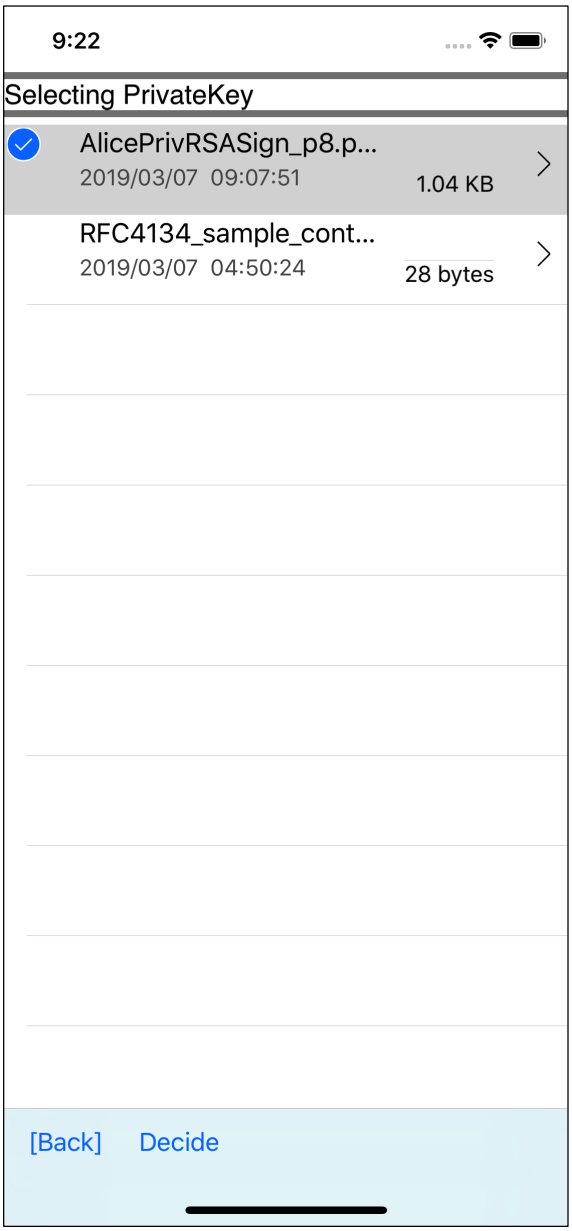
Use the segmented control to select whether to store the signature target in the digital signature (PKCS#7 SignedData).

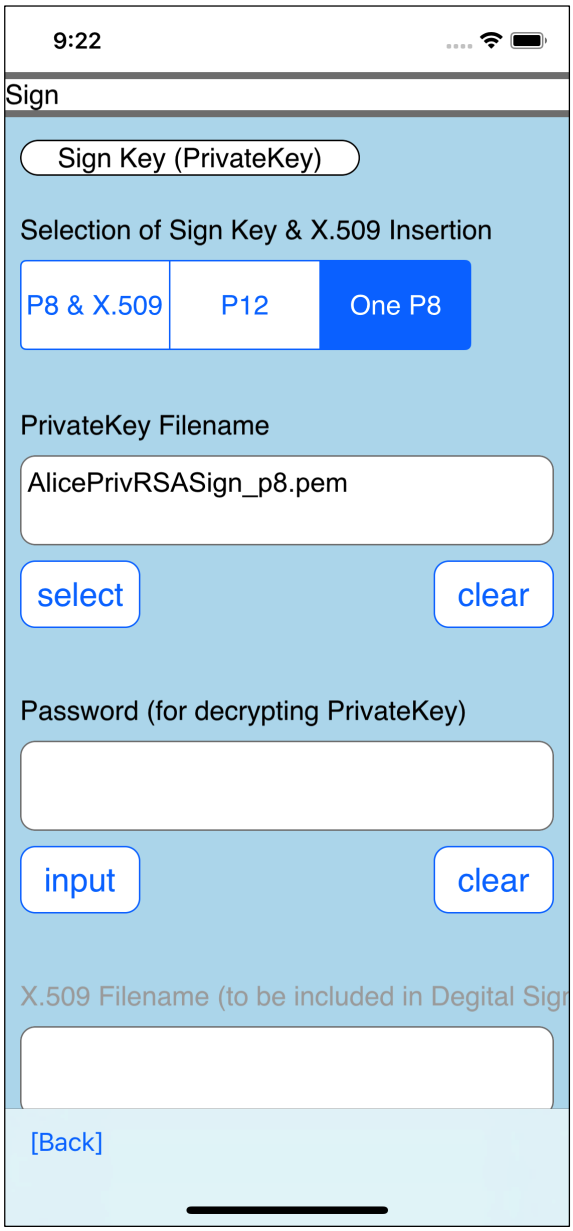
In this example, it is supposed that "the signature object is not stored in the digital signature (PKCS#7 SignedData)."





In this example, it is decided that the signature target is not stored in the digital signature (PKCS#7 SignedData), so select “exclude”.

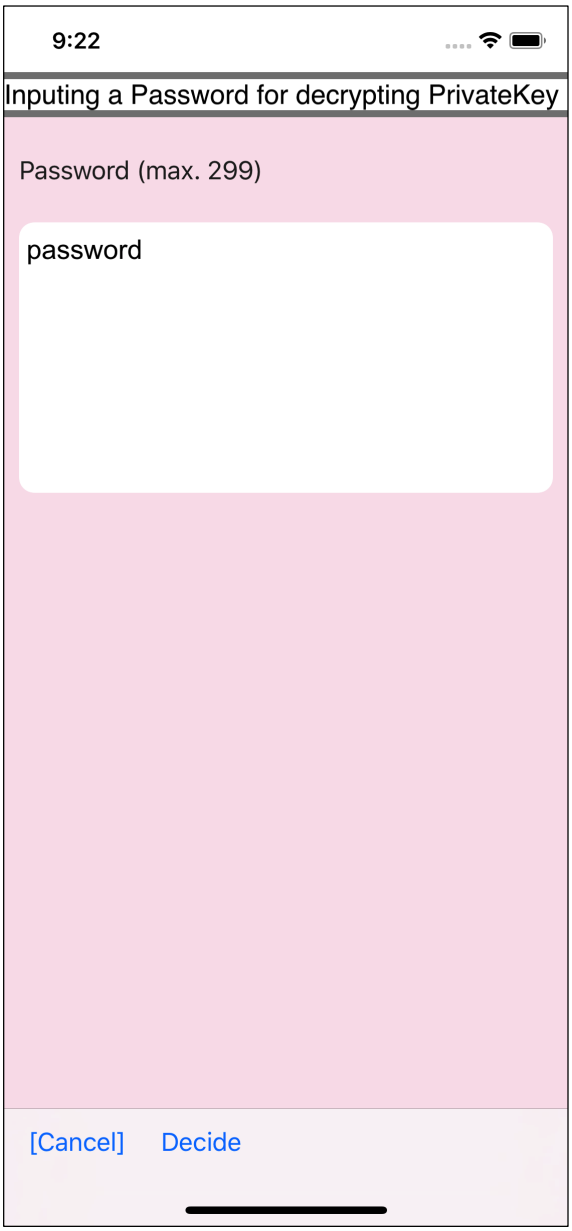


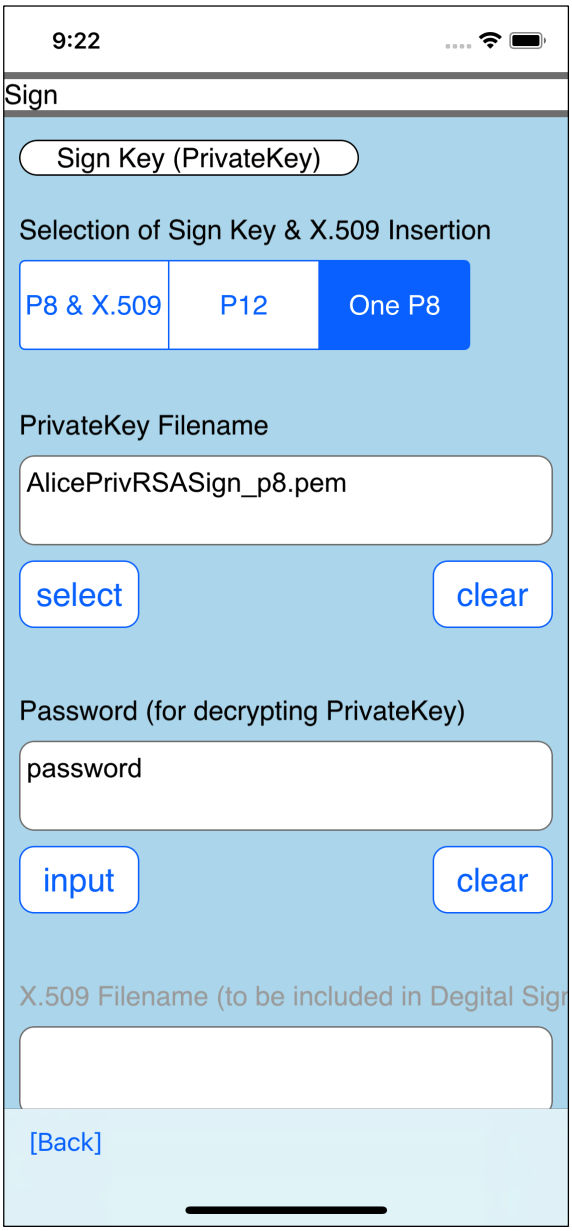


Select one private key as the private key type.

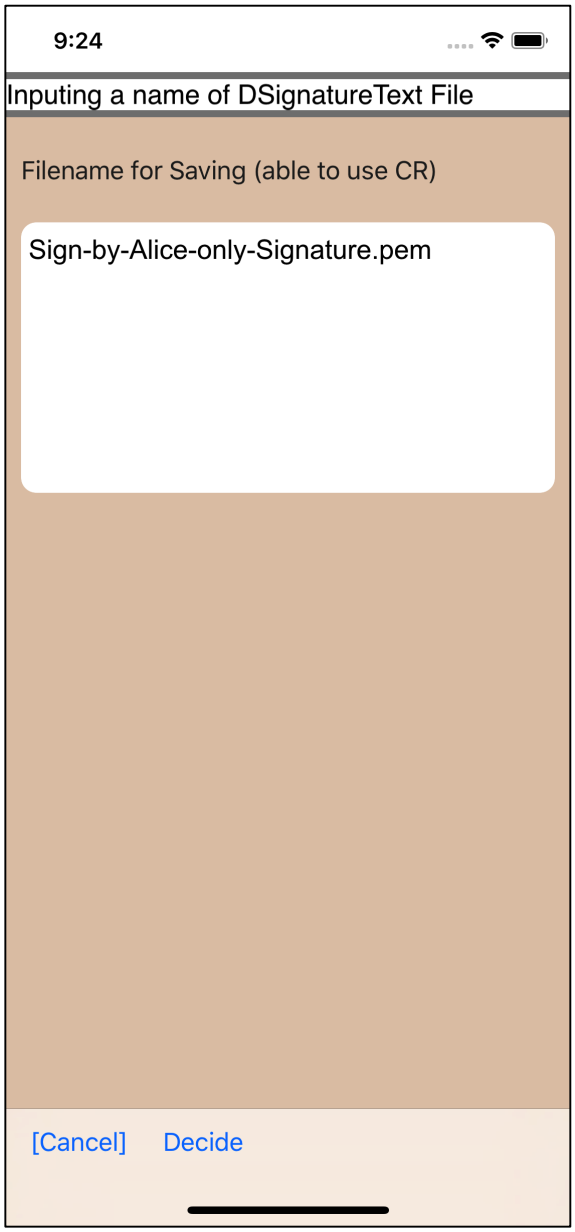
This is an indication that "X. 509 certificate is not stored in digital signature (PKCS#7 SignedData)".

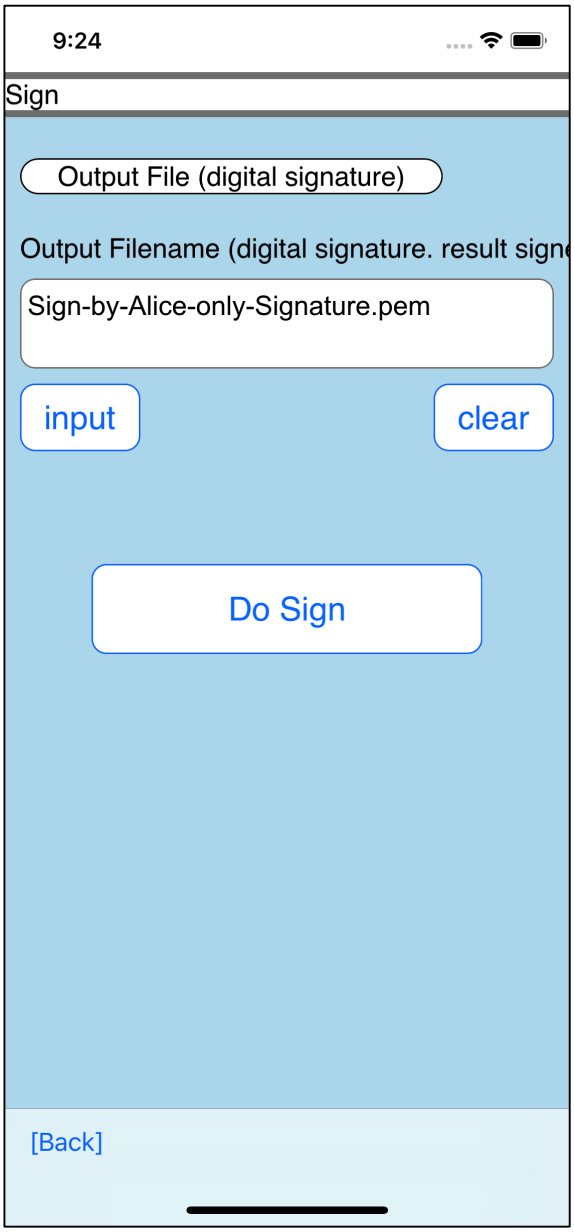
The X.509 certificate file name field is invalidated.





Enter the password used to decrypt the private key.

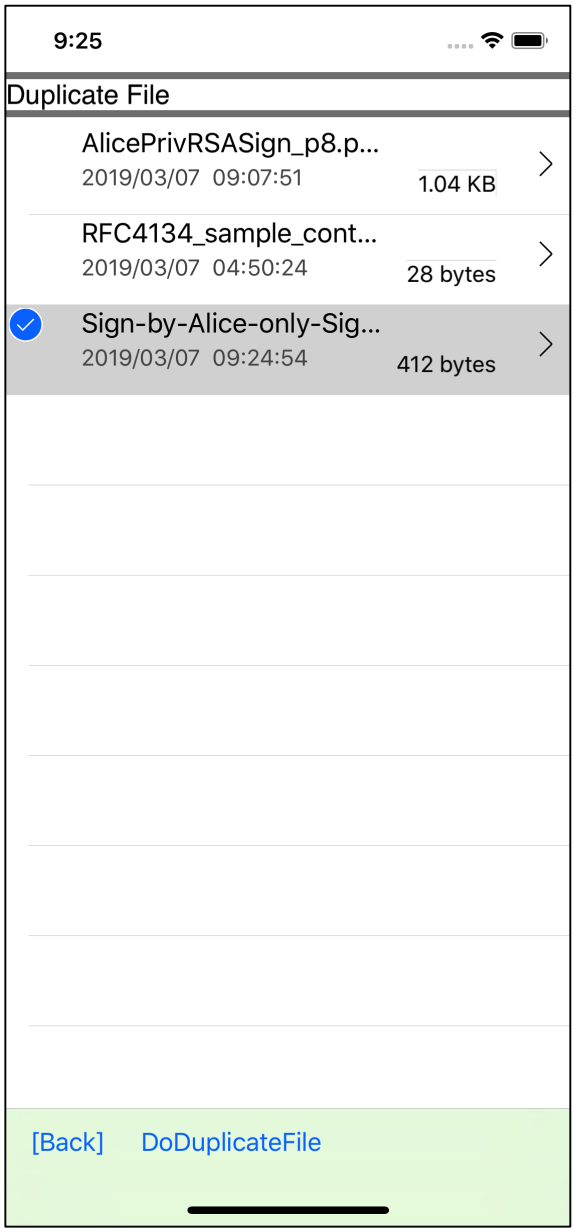


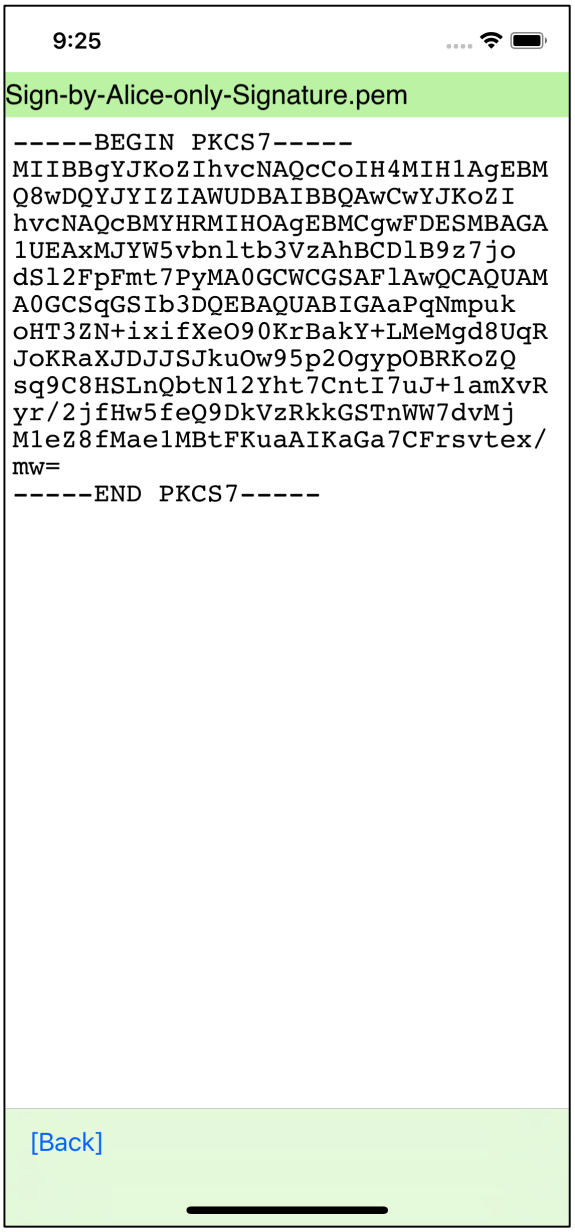


Specify the output destination file of the created digital signature.

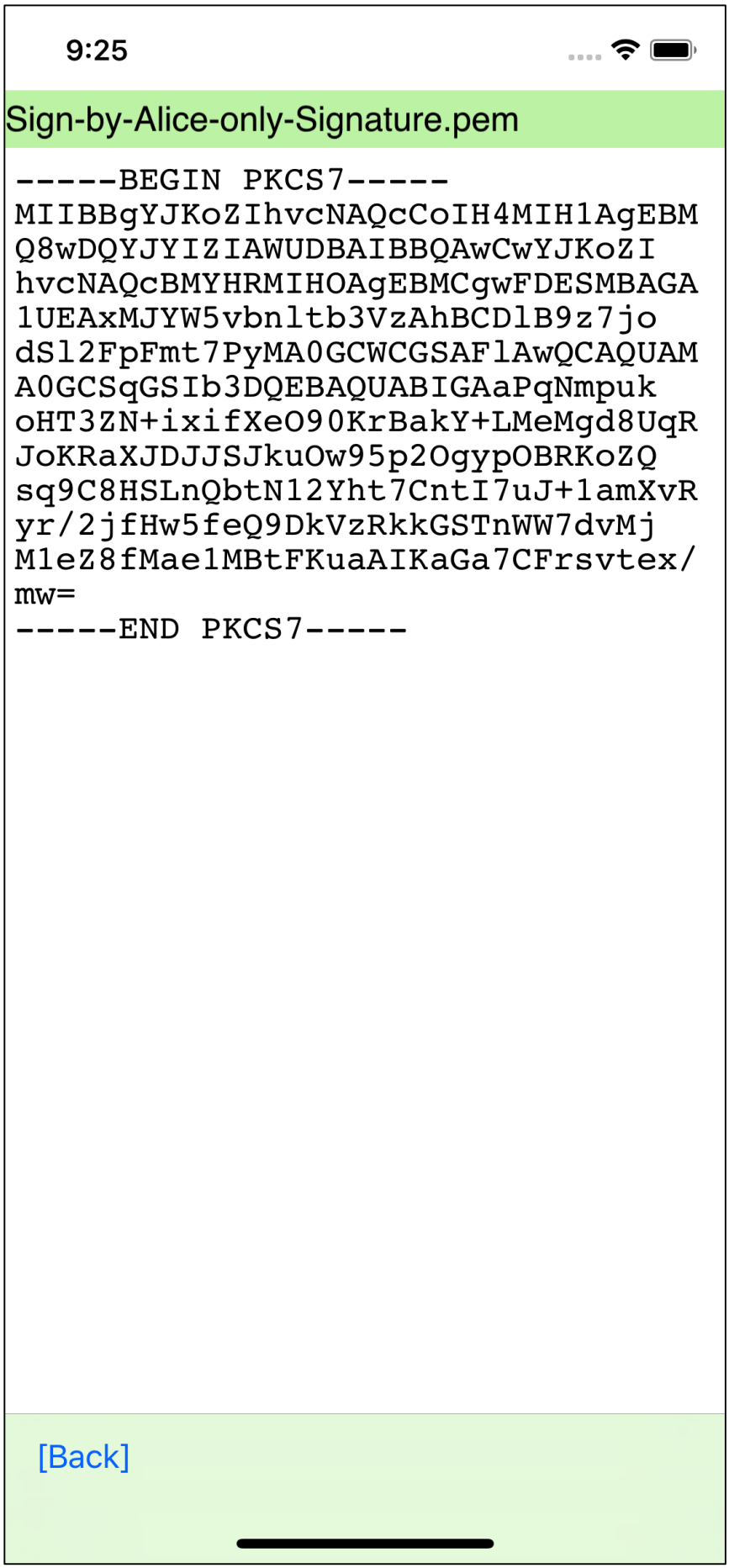
In this state, press the "Do Sign" button to create a digital signature.

Messages are not displayed during or after execution.





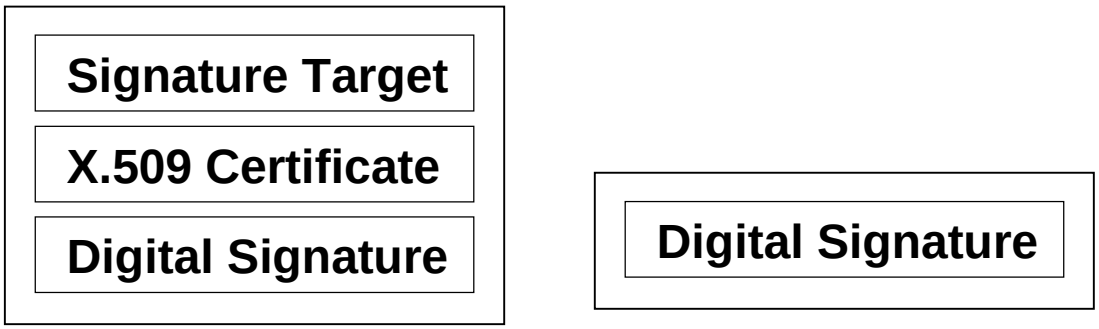
Let's use "Duplicating File" command to see the created digital signature.


9:25
Sign-by-Alice-only-Signature.pem
-----BEGIN PKCS7-----
MIIBBgYJKoZIhvcNAQcCoIH4MIH1AgEBM
Q8wDQYJYIZIAWUDBAIBBQAwCwYJKoZI
hvcNAQcBMYHRMIHOAgEBMCgwFDESMBAGA
1UEAxMJYW5vbnltb3VzAhBCDlB9z7jo
dSl2FpFmt7PyMA0GCWCGSAFlAwQCAQUAM
A0GCSqGSIb3DQEBAQUABIGAaPqNmpuk
oHT3ZN+ixifXeO90KrBakY+LMeMgd8UqR
JoKRaXJDJJSJkuOw95p2OgypOBRKoZQ
sq9C8HSLnQbtN12Yht7CntI7uJ+1amXvR
yr/2jfHw5feQ9DkVzRkkGSTnWW7dvMj
M1eZ8fMae1MBtFKuaAIKaGa7CFrsvtex/
mw=
-----END PKCS7-----
[Back]

The created digital signature (PKCS#7 SignedData) looks like this.

This digital signature (PKCS#7 SignedData) does not include the signature target and the X.509 certificate that contains the public key pair with the private key used to sign.

It will be PKCS#7 SignedData, which contains only digital signature values.



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

When verifying this digital signature, it is necessary to specify both the signature target and the X.509 certificate that contains the public key pair with private key used to sign.

If it is not specified, it will be that it is unknown

- what is the subject of the digital signature and
- unable to execute public key decryption which is the verification operation of the digital signature itself.