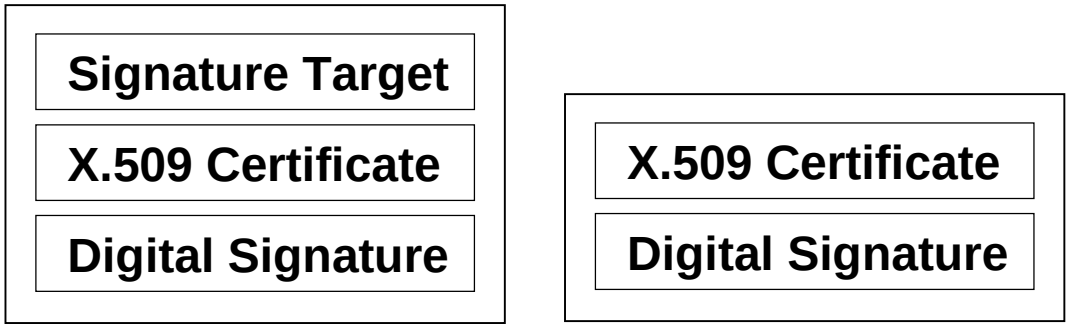
digital signature verification (3)

The example here is verification for a such a case:

"The signature target is not included."

"The X.509 certificate that contains the public key pair with the private key used to create the signature is included."

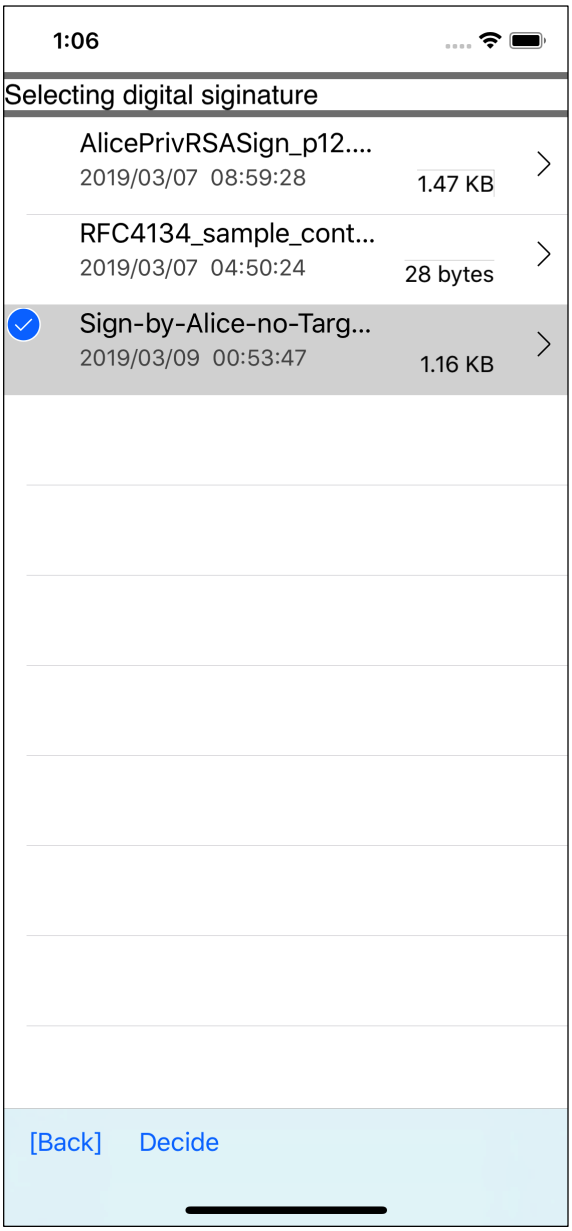


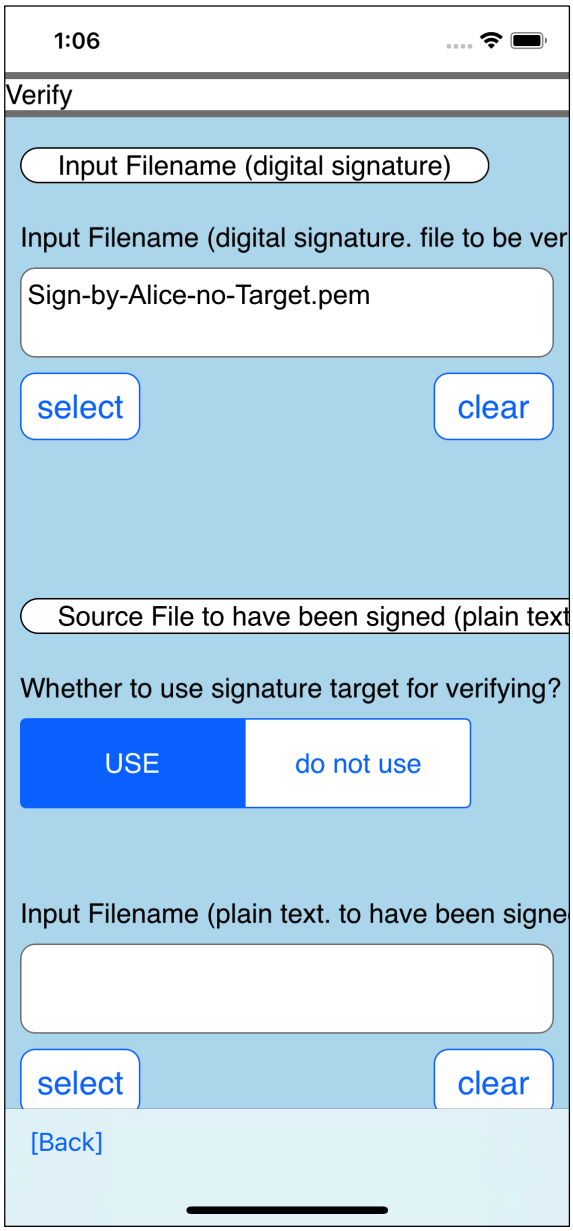
In the case of the figure, it means that the digital signature (PKCS#7 SignedData) as shown on the right is verified.

Therefore, in this example, it is necessary to specify

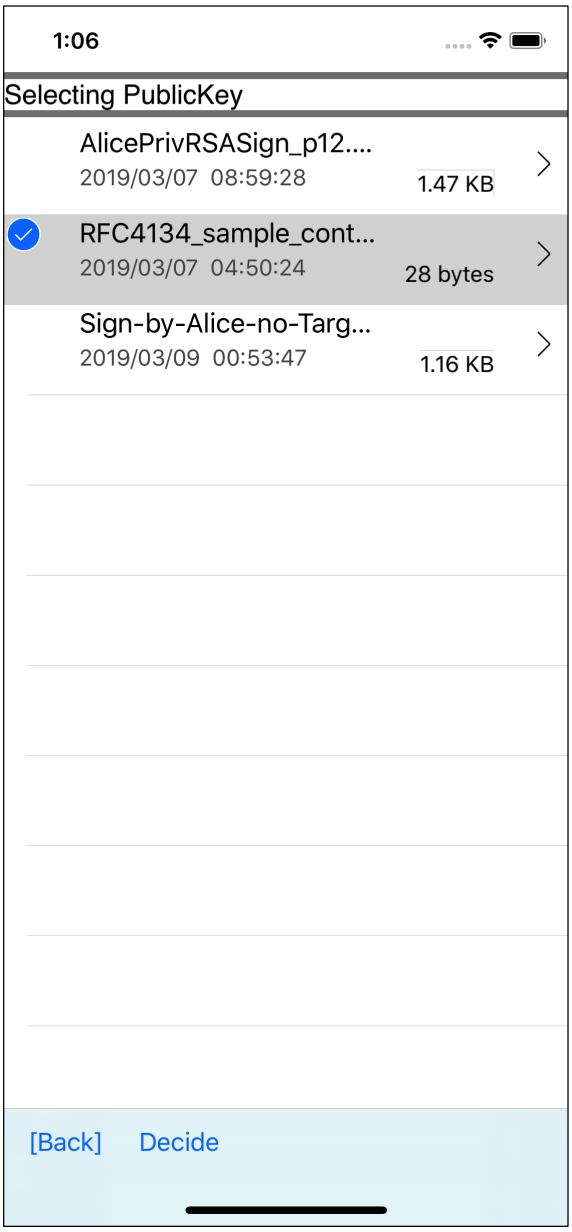
the file name of the digital signature (PKCS#7 SignedData) and

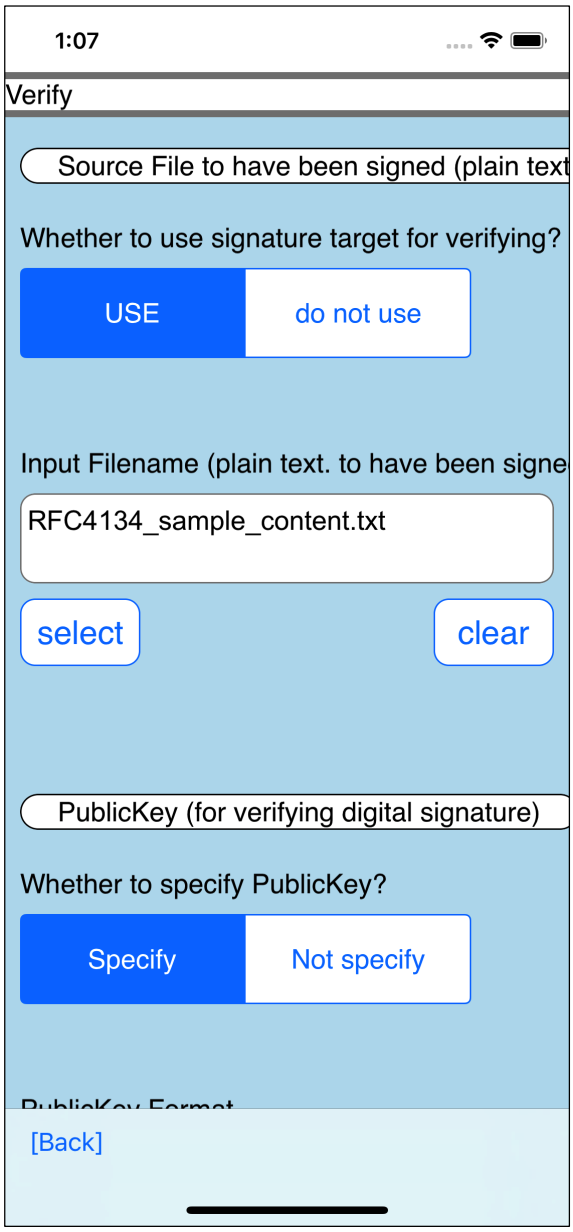
the target of the signature.



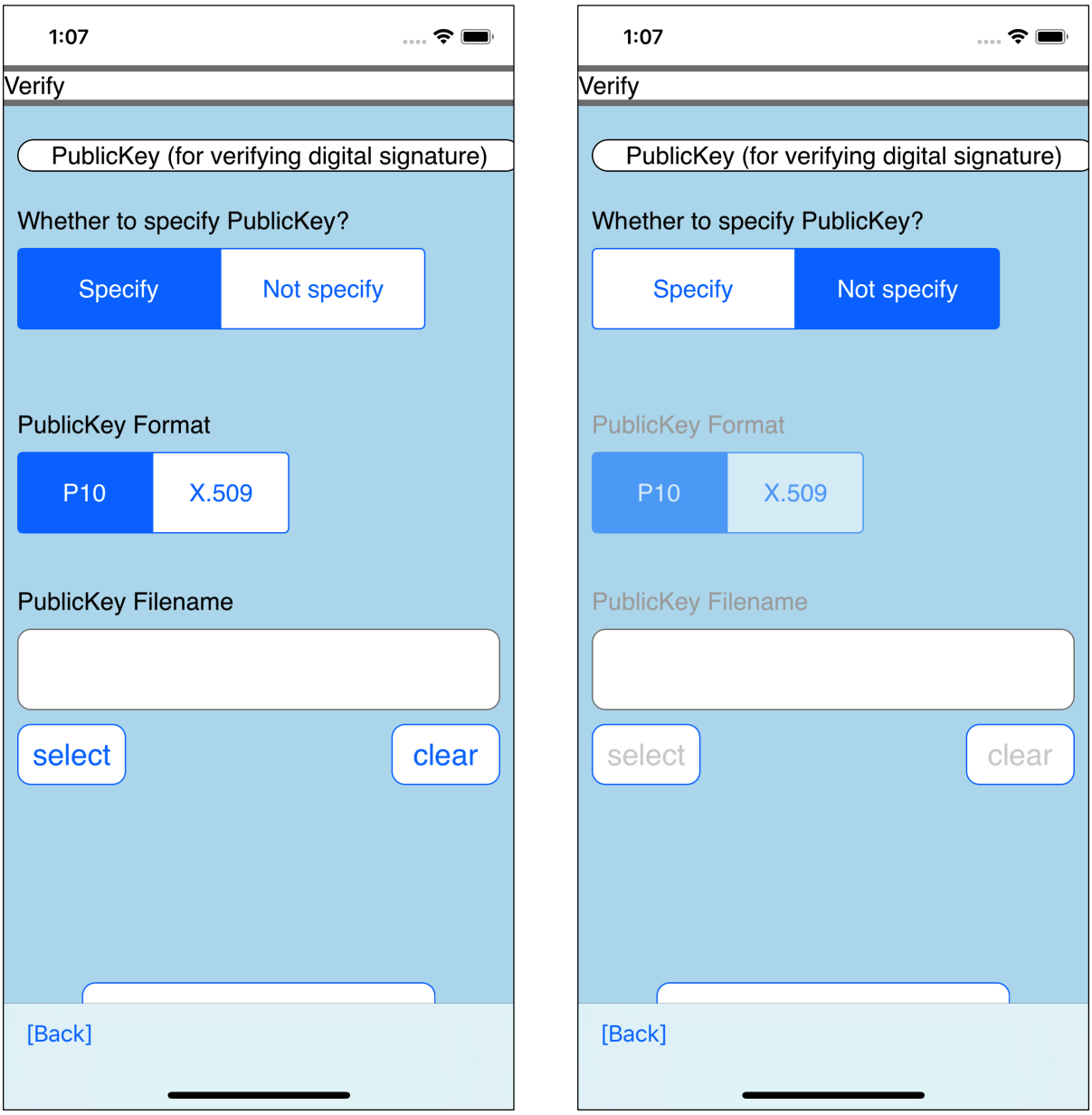


Specifies the file name of the digital signature (PKCS#7 SignedData).



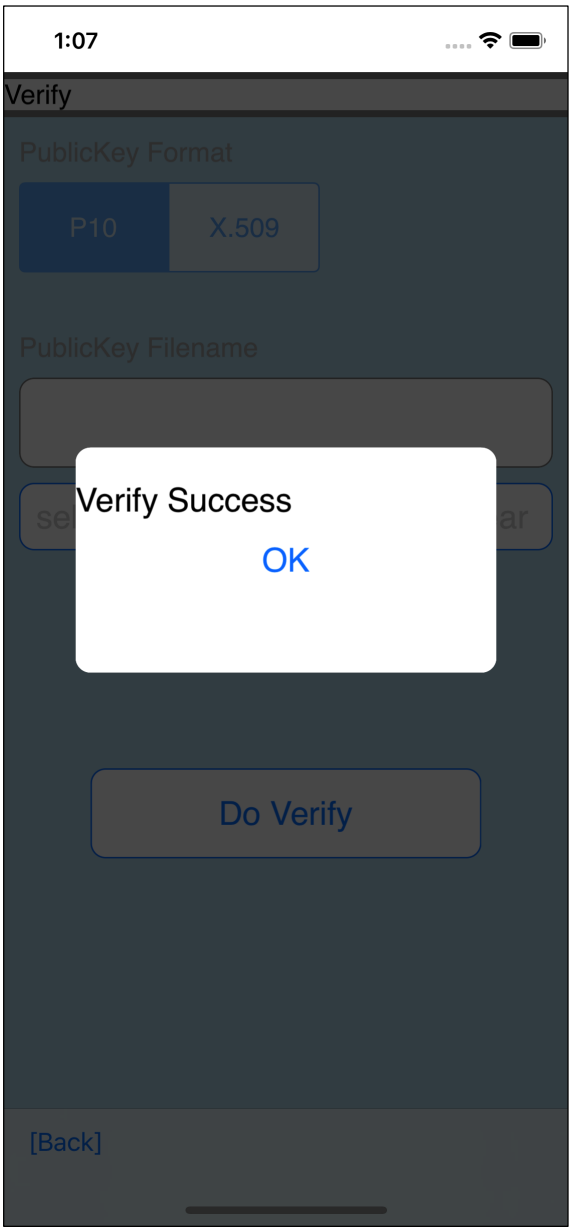


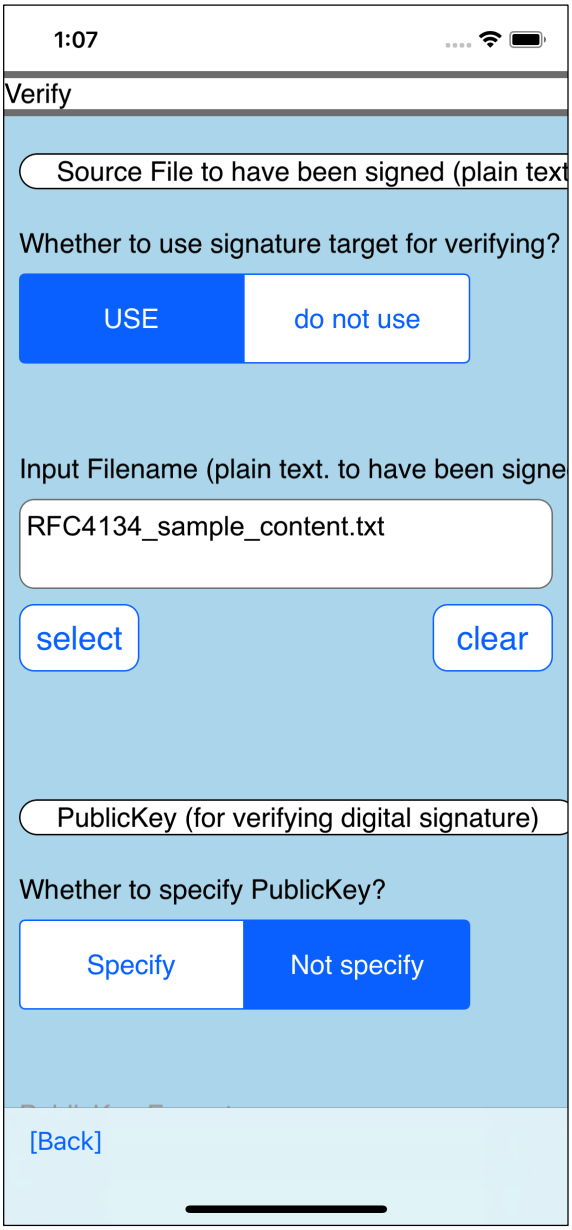
Specify the file to be signed.

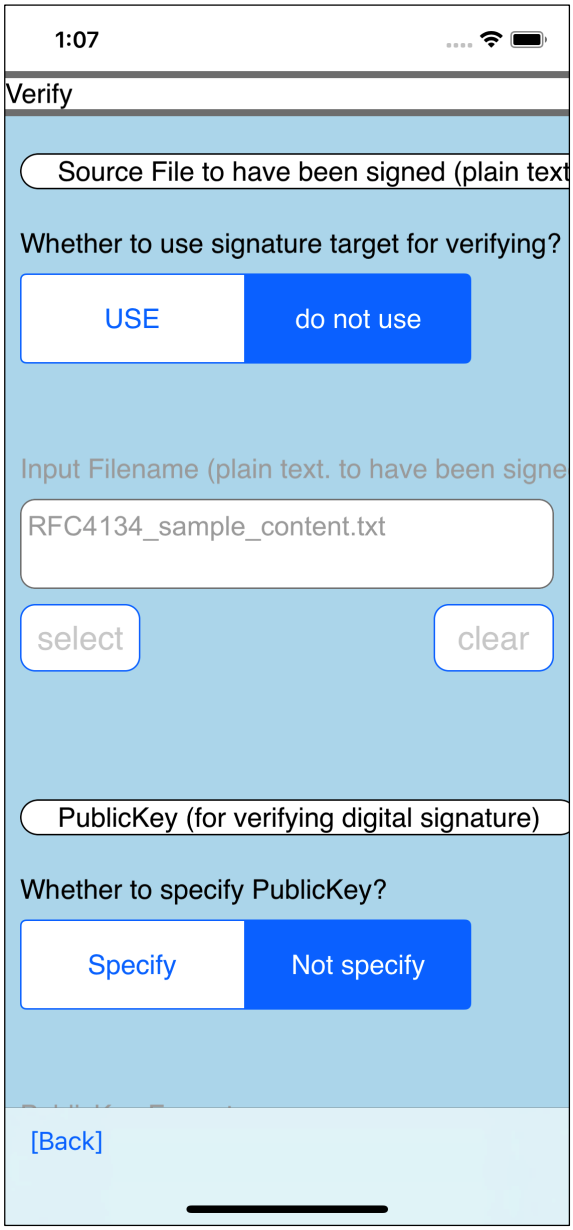


The X.509 certificate that contains the public key pair with the private key used to create the signature is included in the digital signature (PKCS#7 SignedData).

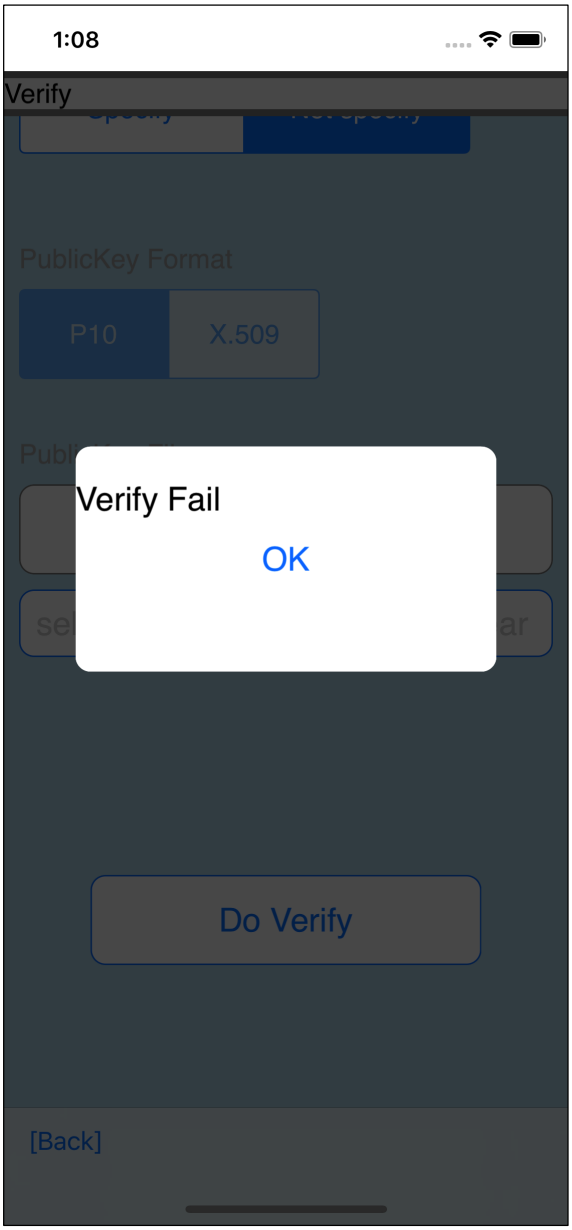
Therefore, select "Do not specify a public key".


1:07
Verify
PublicKey Format
P10
X.509
PublicKey Filename
Verify Success
OK
Do Verify
[Back]





If you do not specify the signature target like this, the verification will not pass.


1:08
Verify
PublicKey Format
P10
X.509
Verify Fail
OK
Do Verify
[Back]