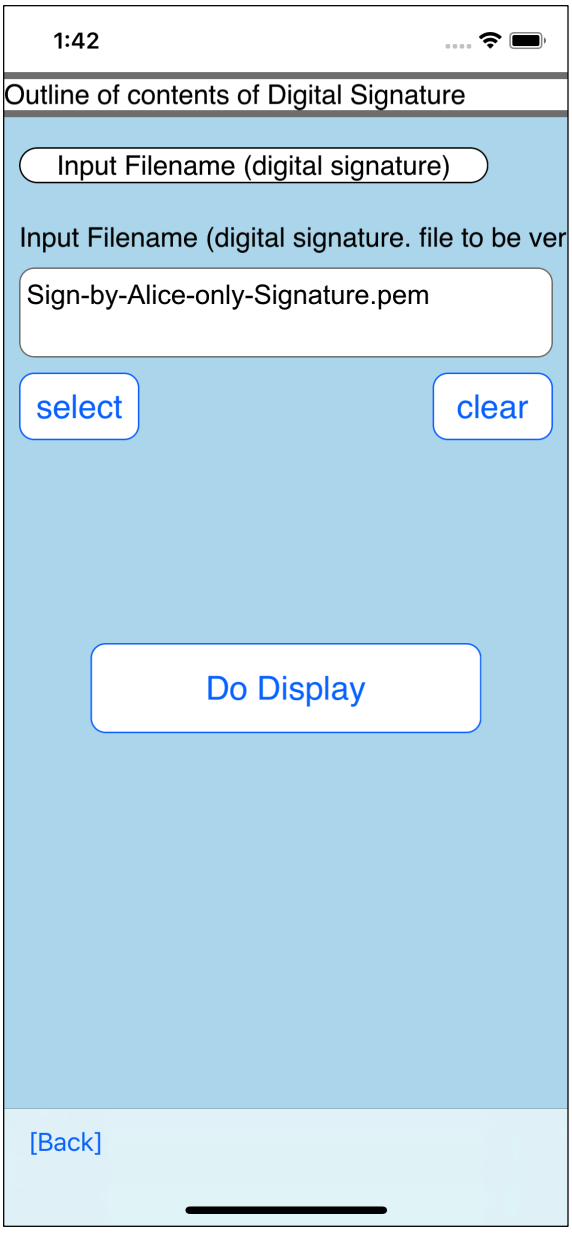
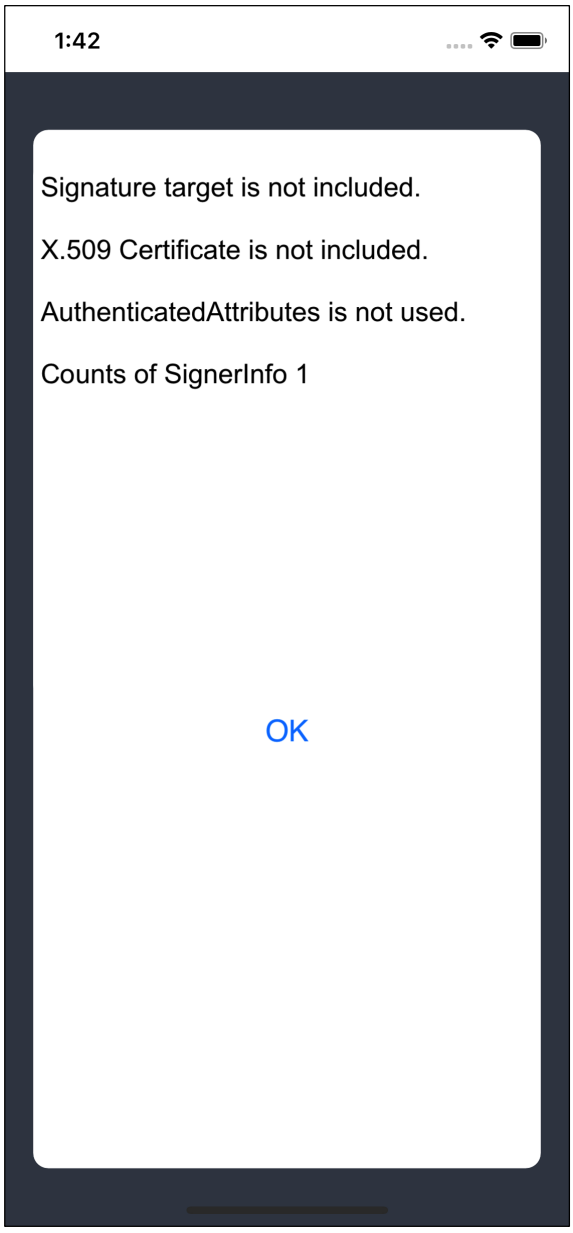
digital signature outline (5)

You can display the outline of the digital signature by the command to display the outline of the digital signature.





You can see that the Sign-by-Alice-only-Signature.pem created using one private key (signature 5) is as follows.

Sign subject is not included.

X. 509 public key certificates are not included.

AuthenticatedAttributes are not used.

digital signatures (SignerInfo) are included.

The number is one.

You see that it is such an outline.

When verifying this digital signature, it is necessary to specify

the signature target and

the public key used for verification
(PKCS#10 SubjectPublicKeyInfo or X.509 public key certificate).