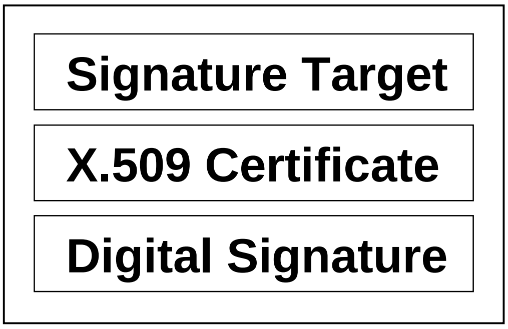
digital signature verification (1)

The example here is verification when following contents are included in digital signature:

- signature target
- X.509 certificate containing the public key pair with the private key used to create the signature



Signature Target

X.509 Certificate

Digital Signature

As shown in this figure,

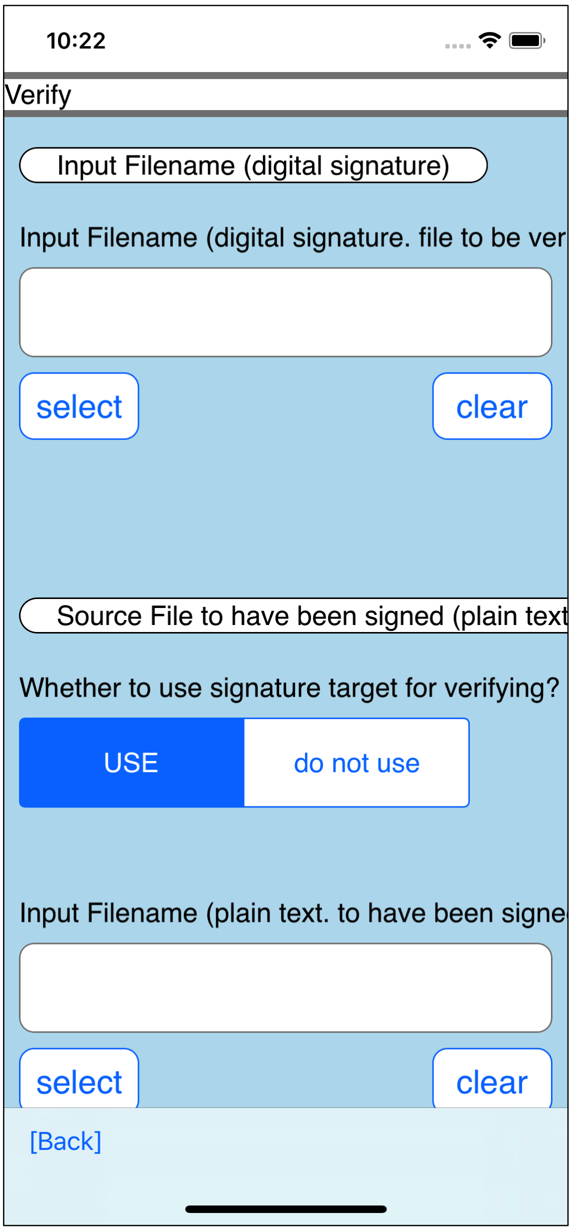
- Signature target
- Public key used for signature verification (public key stored in X.509 certificate)
- Digital signature

all of three needed to verify above is stored in the digital signature (PKCS#7 SignedData).

Therefore, there is no need to specify following individually:

- Signature target
- Public key used for signature verification (public key stored in X.509 certificate)

In this case, "just enter the file name of the digital signature (PKCS#7 SignedData)."



Input Filename (digital signature)

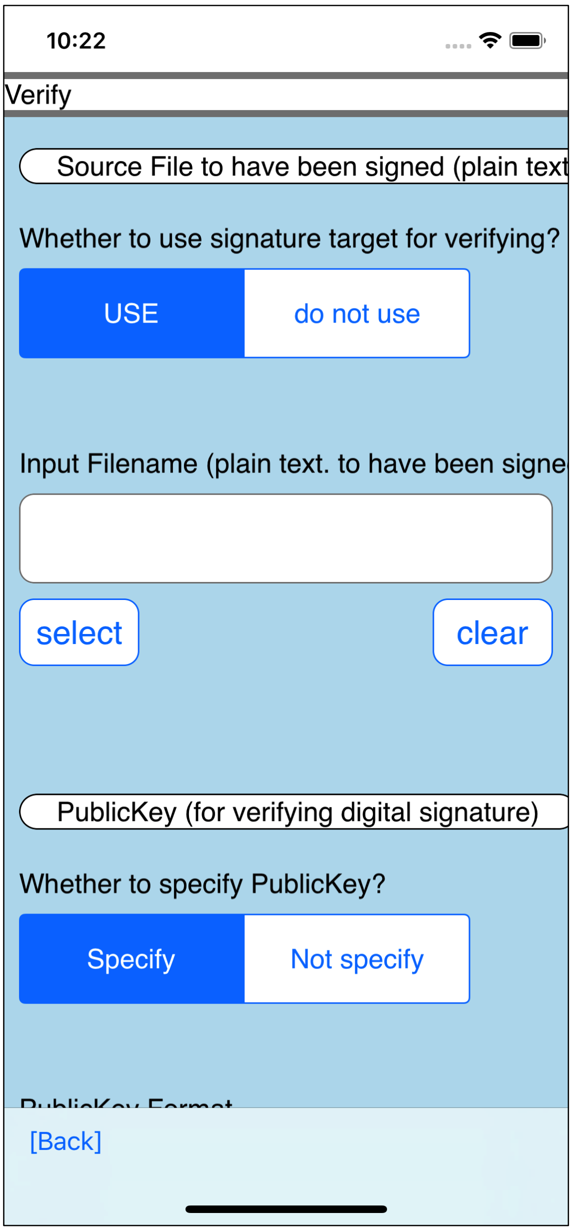
Input Filename (digital signature. file to be ver

Source File to have been signed (plain text

Whether to use signature target for verifying?

[✓ USE] do not use

Input Filename (plain text. to have been signe



Source File to have been signed (plain text

Whether to use signature target for verifying?

[✓ USE] do not use

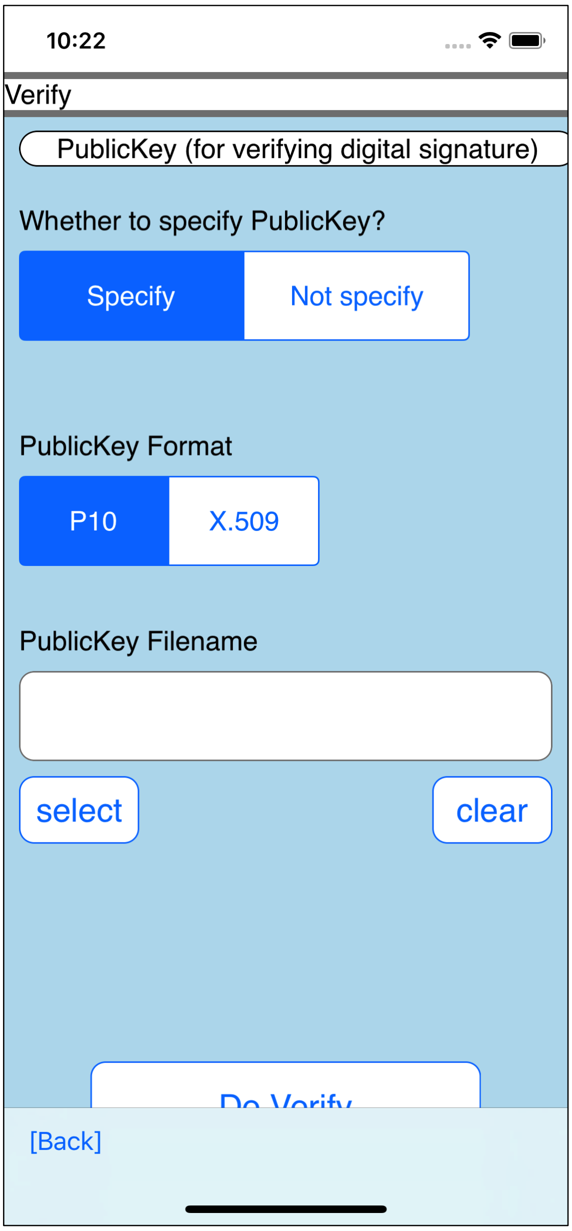
Input Filename (plain text. to have been signe

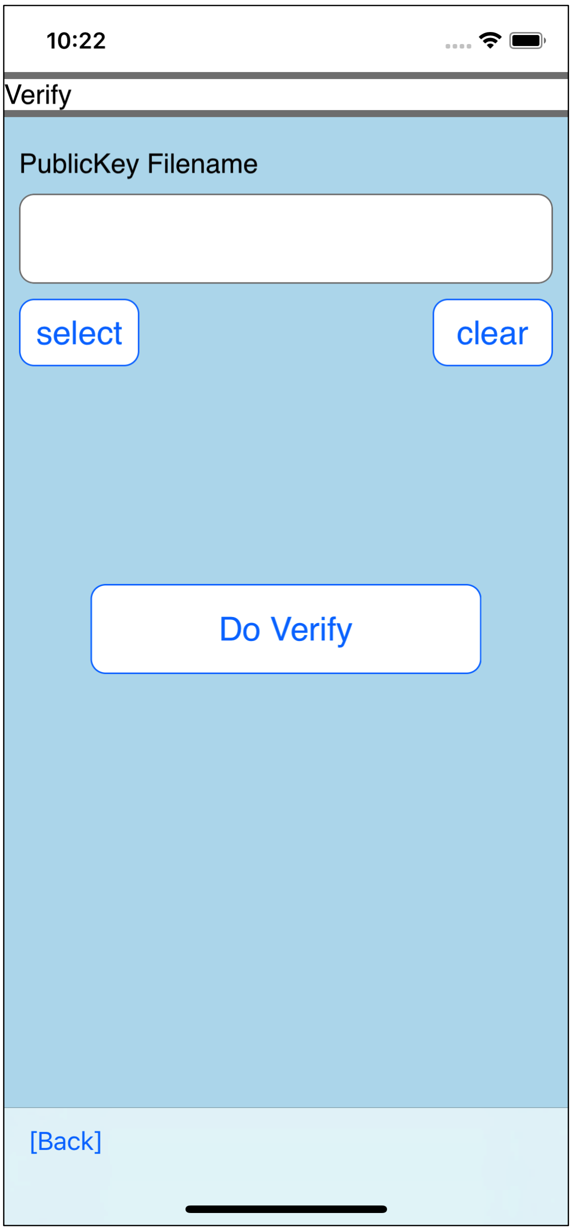
PublicKey (for verifying digital signature)

Whether to specify PublicKey?

[✓ Specify] Not specify

PublicKey Format





The user interface looks like this.

digital signature (PKCS#7 SignedData) file name

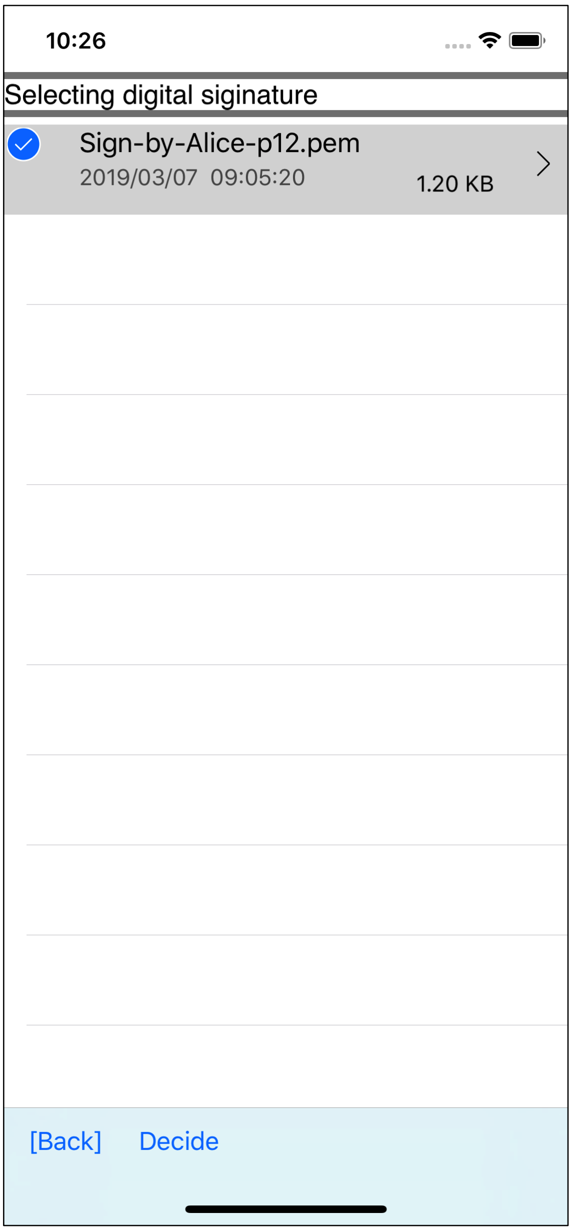
Whether to specify the target of the signature

Name of the file to be signed

Whether to specify the public key used for verification

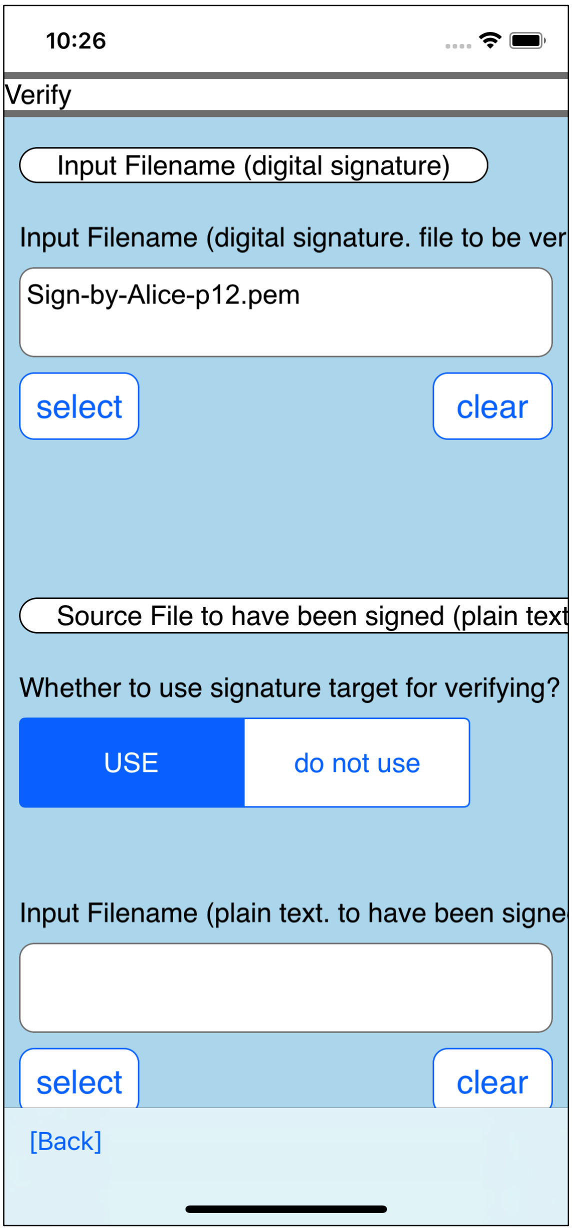
File name of public key used for verification

This is the meaning.



Selecting digital siginature

☑ Sign-by-Alice-p12.pem
2019/03/07 09:05:20 1.20 KB



Verify

Input Filename (digital signature)

Input Filename (digital signature. file to be ver

Sign-by-Alice-p12.pem

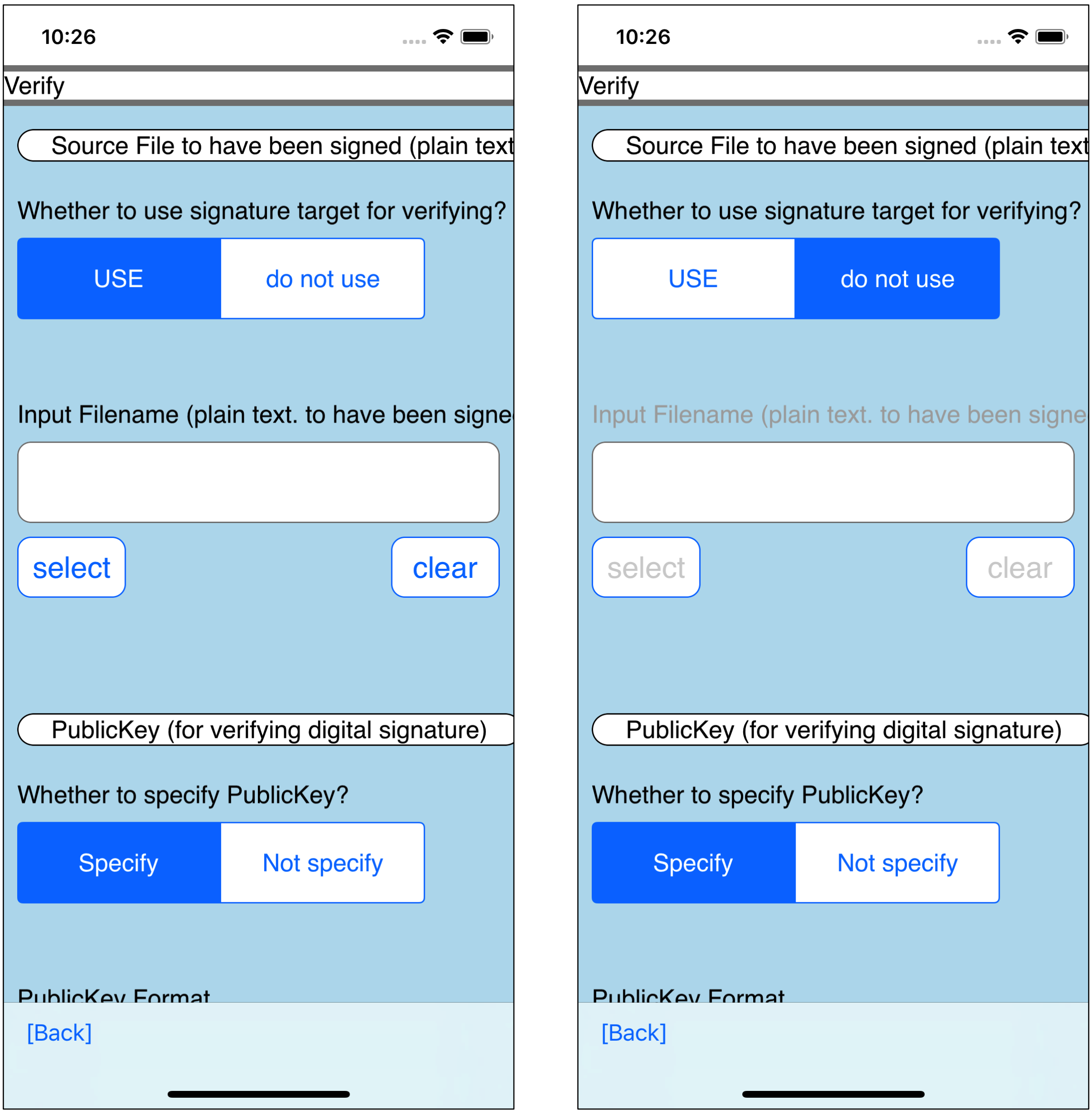
Source File to have been signed (plain text

Whether to use signature target for verifying?

[✓ USE] do not use

Input Filename (plain text. to have been signe

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



10:26

Verify

Source File to have been signed (plain text

Whether to use signature target for verifying?

[✓ USE] do not use

Input Filename (plain text. to have been signe

PublicKey (for verifying digital signature)

Whether to specify PublicKey?

[✓ Specify] Not specify

PublicKey Format

10:26

Verify

Source File to have been signed (plain text

Whether to use signature target for verifying?

USE [✓ do not use]

Input Filename (plain text. to have been signe

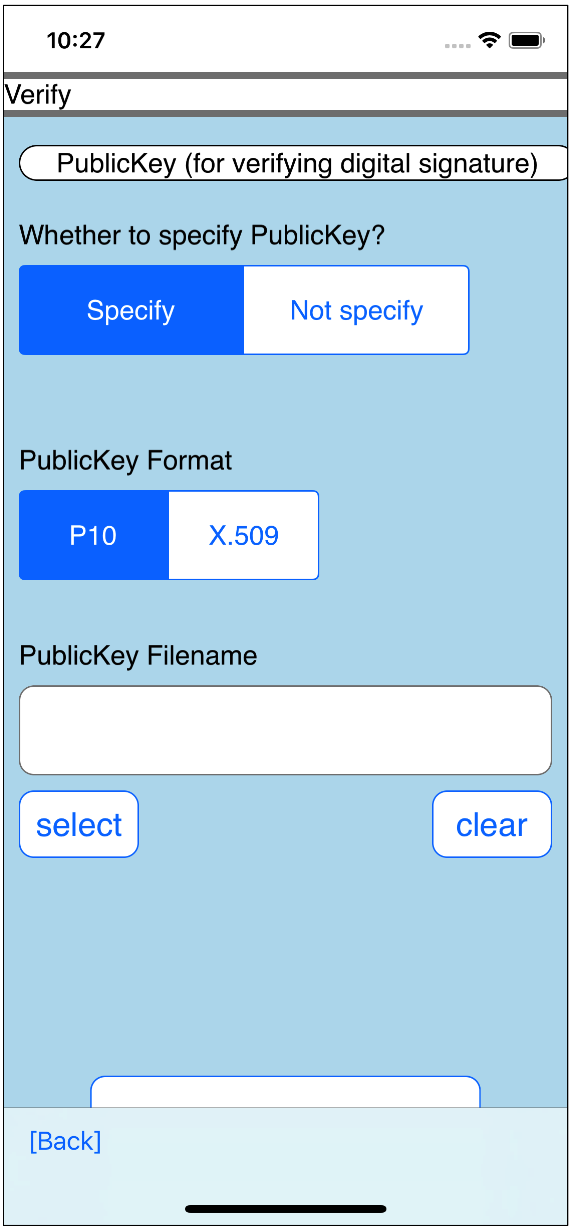
PublicKey (for verifying digital signature)

Whether to specify PublicKey?

[✓ Specify] Not specify

PublicKey Format

The signature target is not specified.



PublicKey (for verifying digital signature)

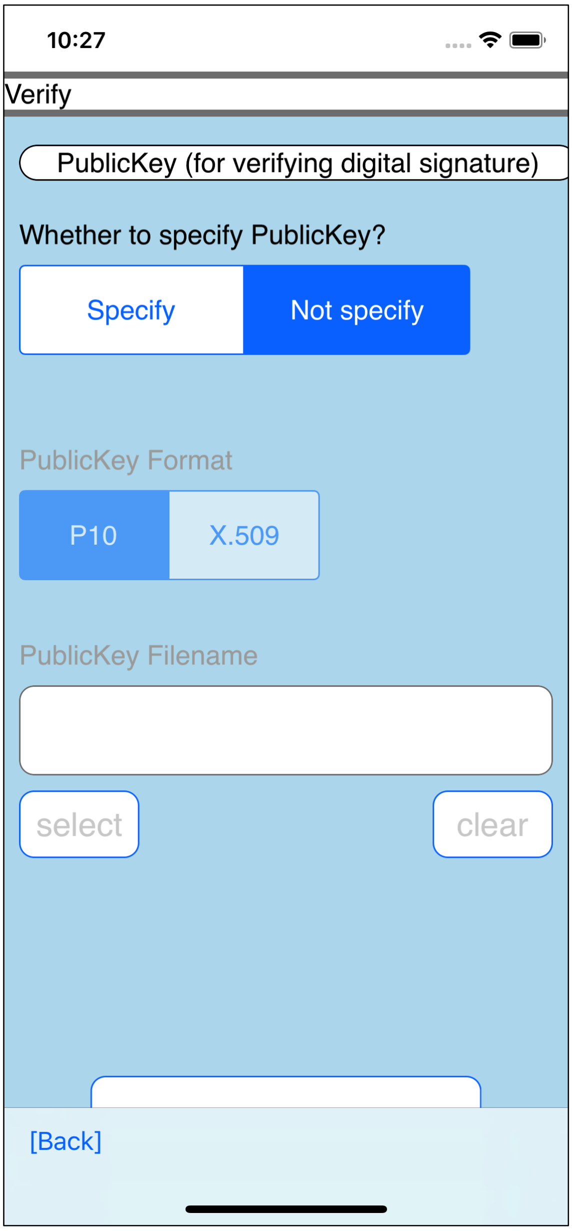
Whether to specify PublicKey?

[✓ Specify] Not specify

PublicKey Format

[✓ P10] X.509

PublicKey Filename



PublicKey (for verifying digital signature)

Whether to specify PublicKey?

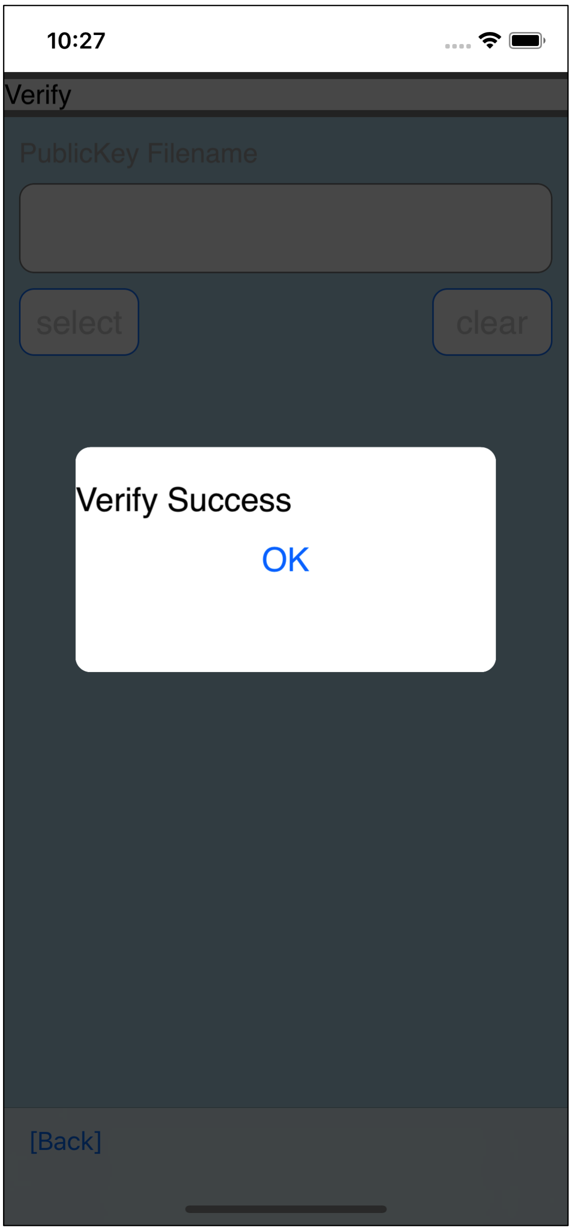
Specify [✓ Not specify]

PublicKey Format

[✓ P10] X.509

PublicKey Filename

It also does not specify the public key used to verify the signature.



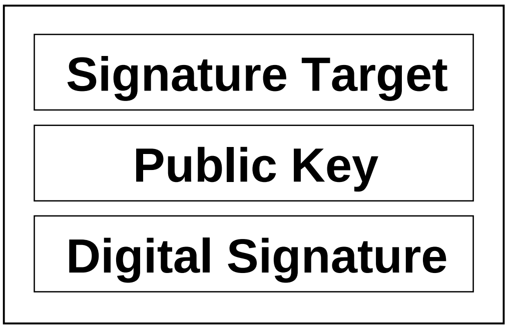
Verify Success

OK

it is passed to the signature verification in only enter the file name of the digital signature (PKCS#7 SignedData).

It may be difficult to understand what you are doing.

The digital signature of PKCS#7 SignedData type is simply structured as shown in the following figure.



Signature Target

Public Key

Digital Signature

Signature target

Public key used for signature verification (public key stored in X.509 public key certificate)

is also included.

Therefore, digital signature verification can be performed by specifying only one PKCS#7 SignedData.

If it passes to verification of the signature, it can be said that

"The signature was made by the owner of the private key pair with the public key used for verification." and

"The signature target has not been tampered with."

This makes it possible to say,

"The person who created the signature target is the owner of the private key pair with the public key used for verification."