Confirmation of whether the private key and the private key are identical

Make sure that the private key and the private key are identical.

Private key stored differently

Private key with different password

In the ASN.1 syntax stage, private keys with different values

The purpose is to confirm the identity of such private key.

In this command, the same check is performed using the value (Multi-Precision Integer) actually used when applying RSA public key cipher, not the value of ASN.1 syntax stage.

"It is actually the same as the value (Multi-Precision Integer) used when applying the RSA public key cipher, but it is different as an key encoded in ASN.1 syntax."

Sometimes such a thing occurs on the key value of the RSA public key cipher.

This means, "There is a subtle difference in encoding when making ASN.1 syntax."

Even in this case, this command can make the same judgment.

However, it does not mean that the same judgment can be made with certainty always.

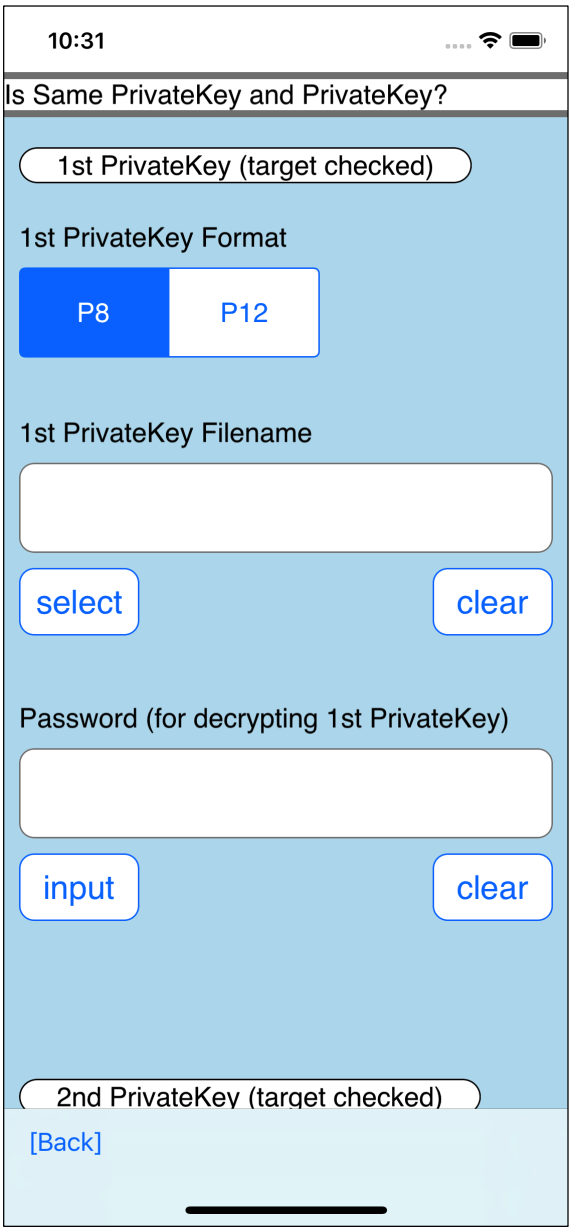
Subtle differences in encoding when making ASN.1 syntax

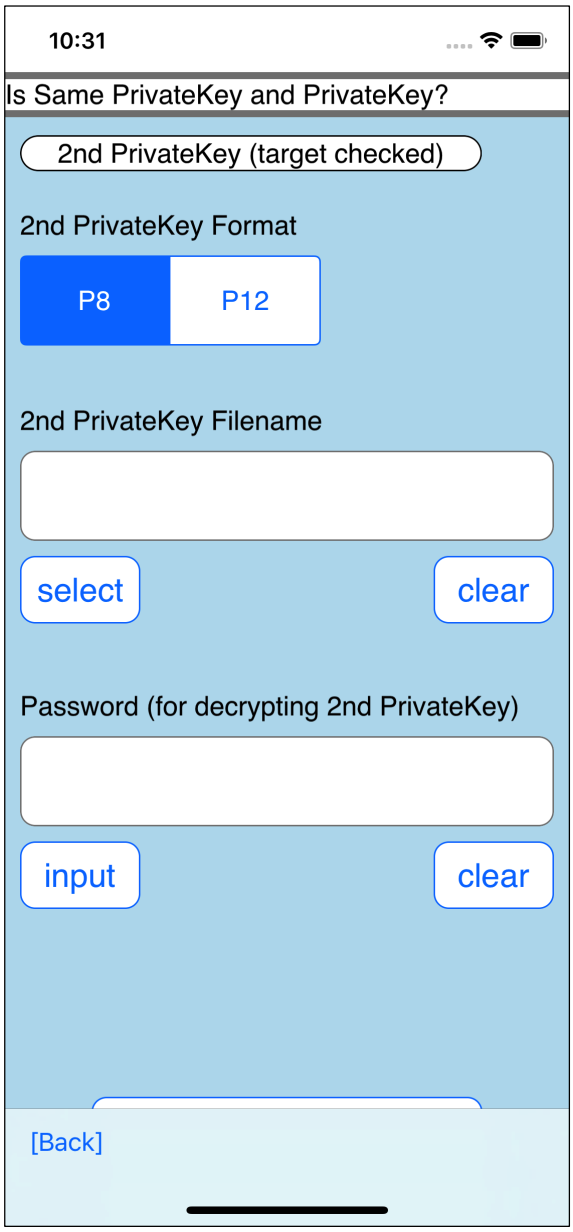
If it can not recognize this difference, even the same key may be determined to be different

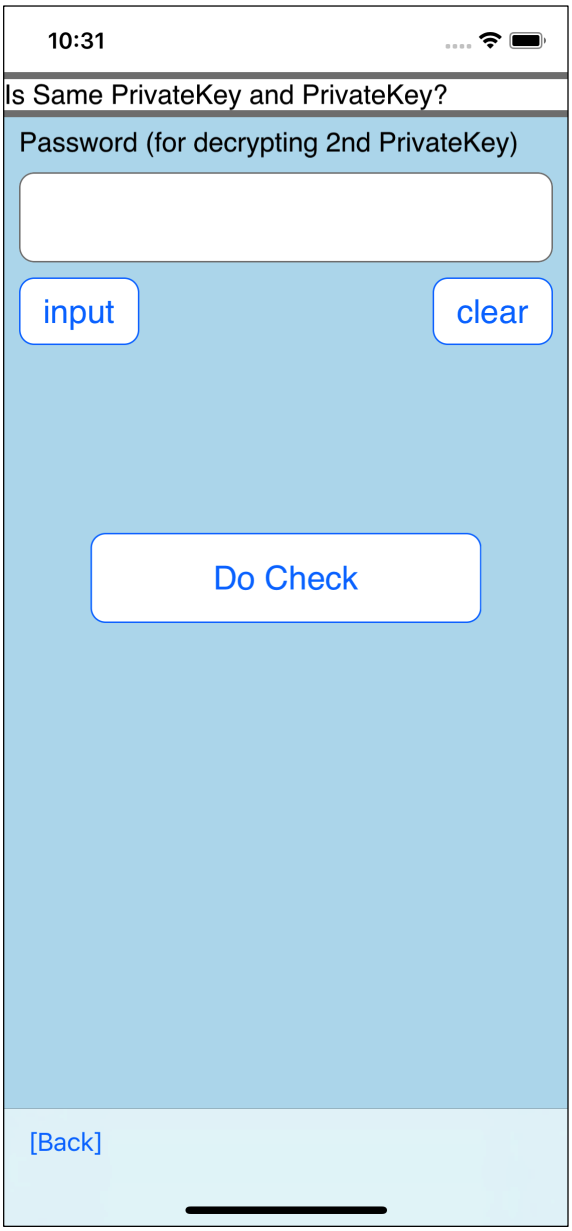
On the contrary,

“It is different as a value (Multi-Precision Integer) actually used when applying RSA public key cipher"

I think that it is unlikely to judge such the key as identical.


10:31
Is Same PrivateKey and PrivateKey?
1st PrivateKey (target checked)
1st PrivateKey Format
P8
P12
1st PrivateKey Filename
select
clear
Password (for decrypting 1st PrivateKey)
input
clear
2nd PrivateKey (target checked)
[Back]


10:31
Is Same PrivateKey and PrivateKey?
2nd PrivateKey (target checked)
2nd PrivateKey Format
P8
P12
2nd PrivateKey Filename
select
clear
Password (for decrypting 2nd PrivateKey)
input
clear
[Back]



The user interface looks like this.

First private key type

File name of first private key

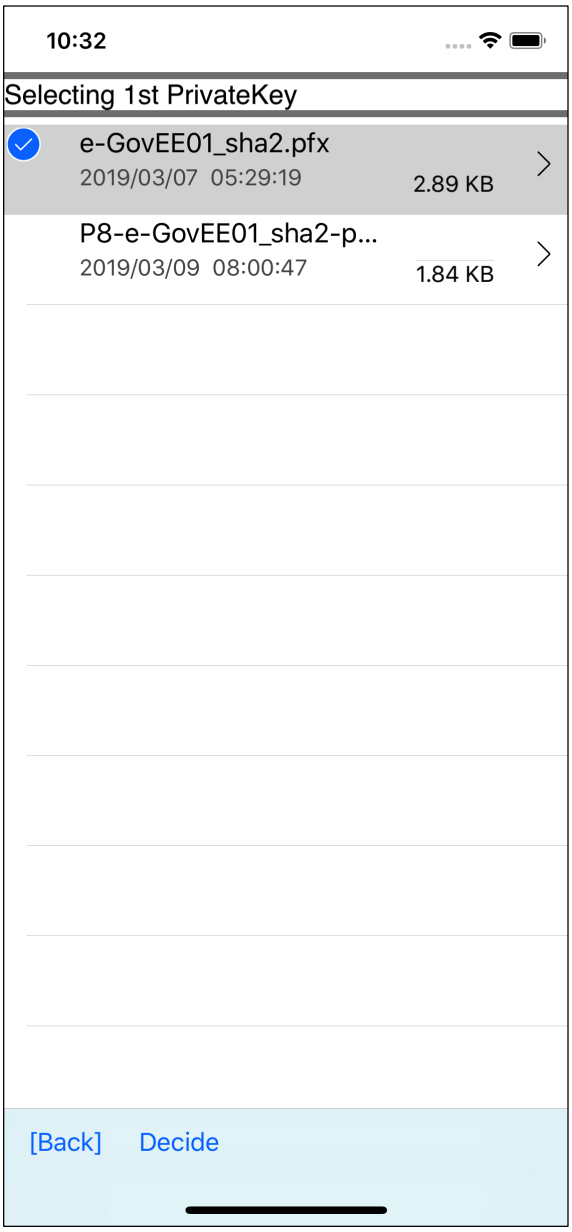
First private key password

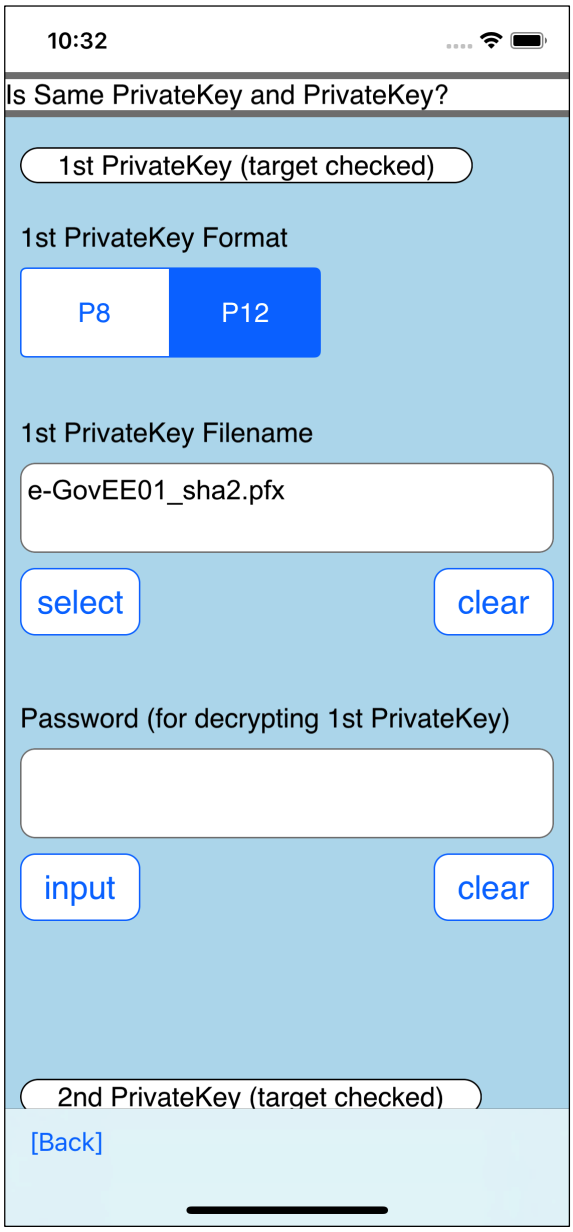
Second private key type

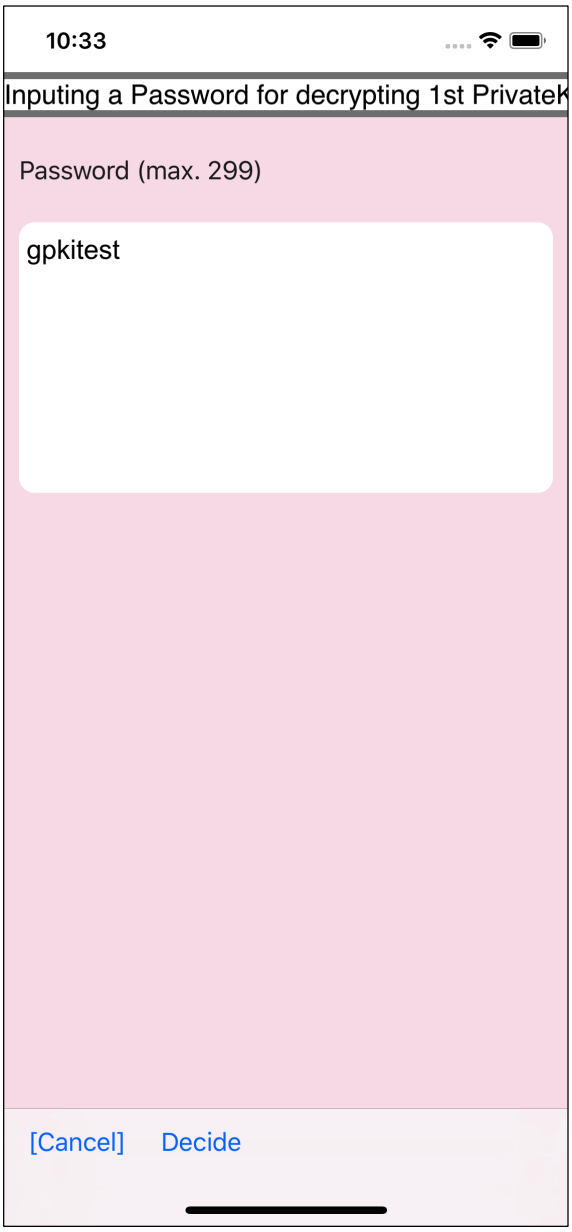
File name of second private key

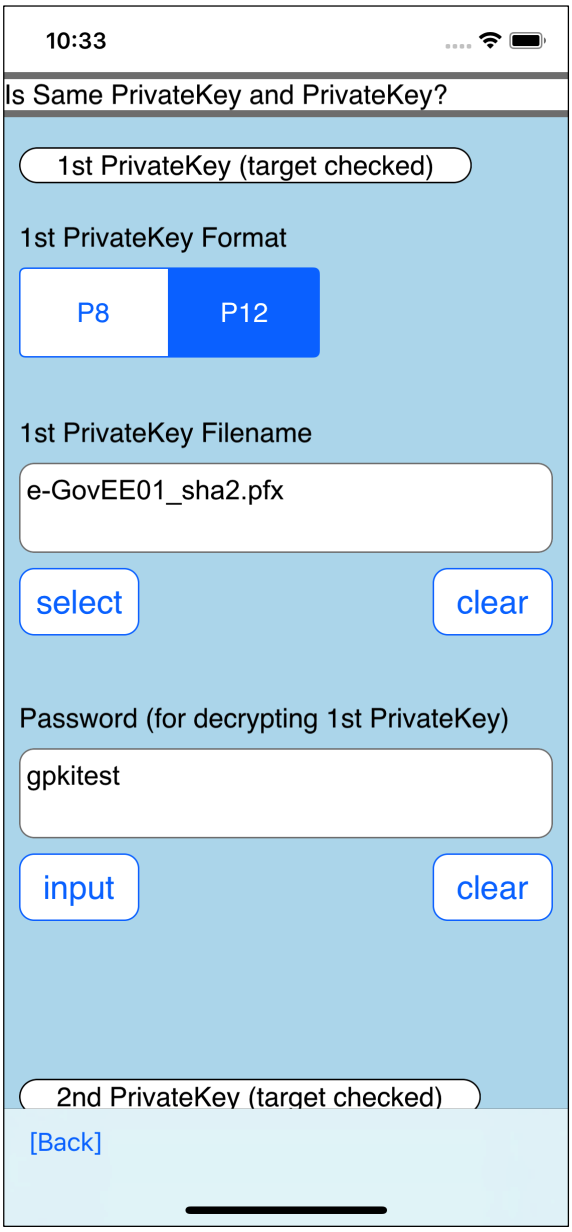
Second private key password

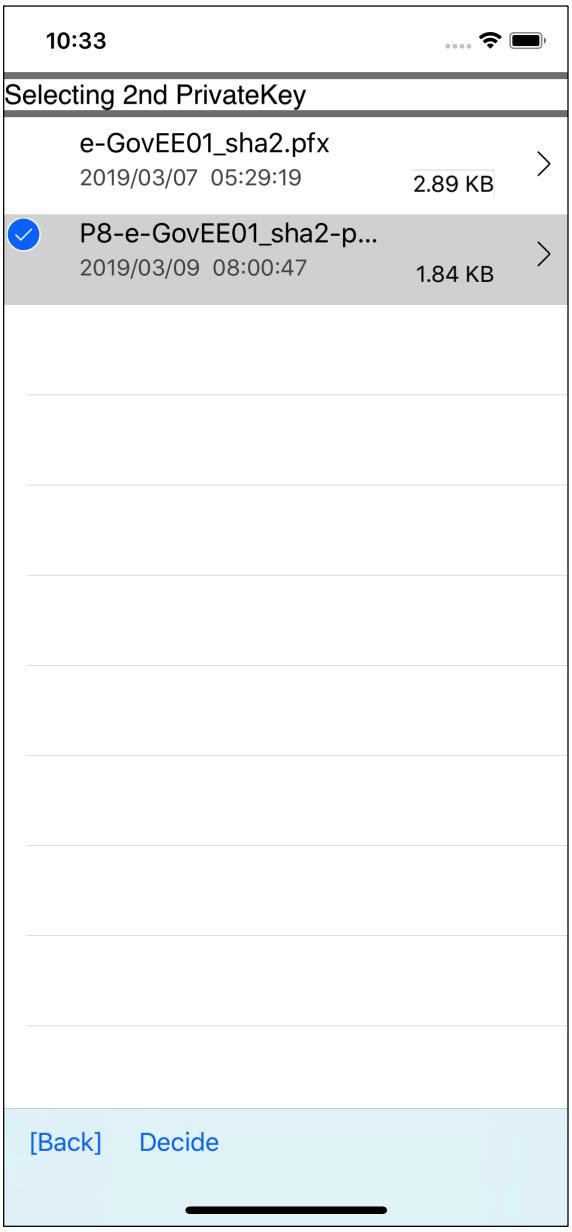
This is the meaning.

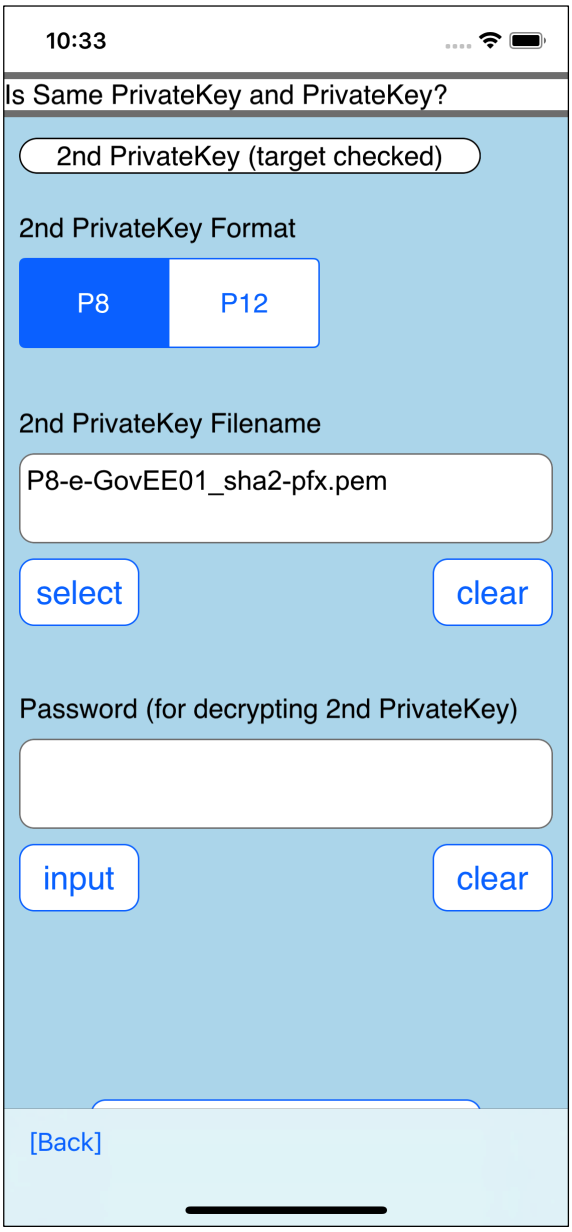

10:32
Selecting 1st PrivateKey
e-GovEE01_sha2.pfx
2019/03/07 05:29:19
2.89 KB
P8-e-GovEE01_sha2-p...
2019/03/09 08:00:47
1.84 KB
[Back]
Decide

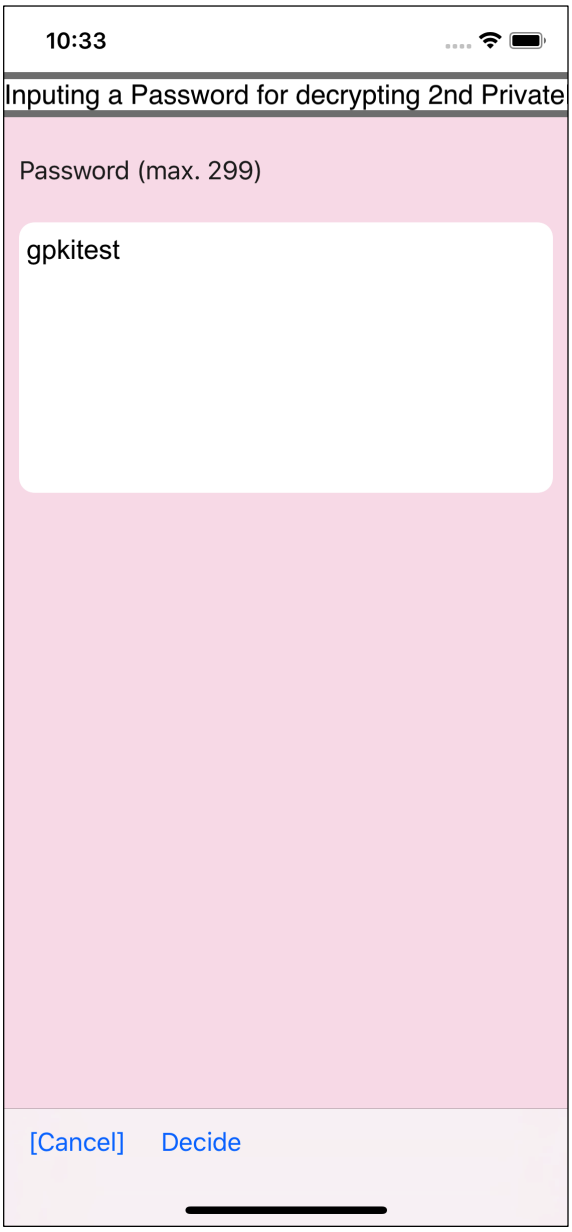

10:32
Is Same PrivateKey and PrivateKey?
1st PrivateKey (target checked)
1st PrivateKey Format
P8
P12
1st PrivateKey Filename
e-GovEE01_sha2.pfx
select
clear
Password (for decrypting 1st PrivateKey)
input
clear
2nd PrivateKey (target checked)
[Back]

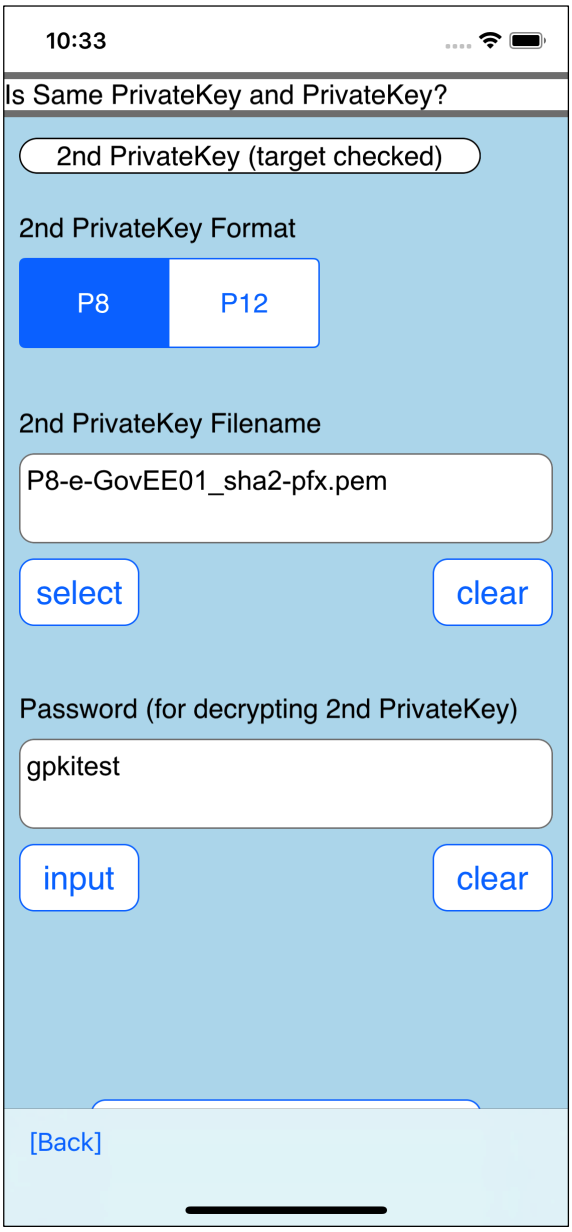

10:33
Inputing a Password for decrypting 1st PrivateK
Password (max. 299)
gpkitest
[Cancel]
Decide

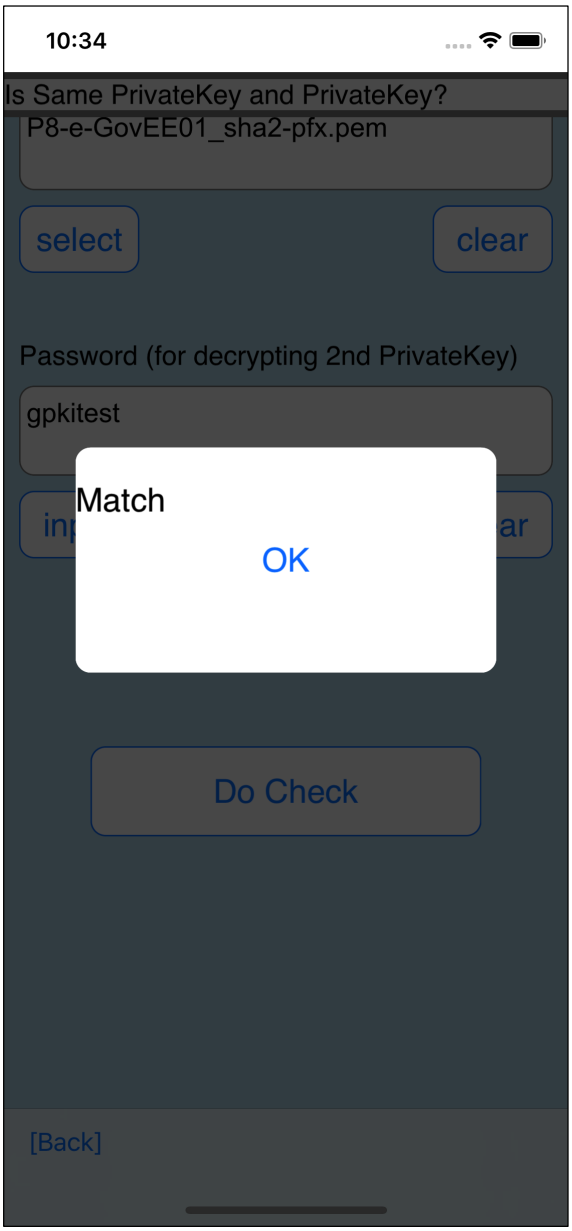

10:33
Is Same PrivateKey and PrivateKey?
1st PrivateKey (target checked)
1st PrivateKey Format
P8
P12
1st PrivateKey Filename
e-GovEE01_sha2.pfx
select
clear
Password (for decrypting 1st PrivateKey)
gpkitest
input
clear
2nd PrivateKey (target checked)
[Back]


10:33
Selecting 2nd PrivateKey
e-GovEE01_sha2.pfx
2019/03/07 05:29:19
2.89 KB
P8-e-GovEE01_sha2-p...
2019/03/09 08:00:47
1.84 KB
[Back]
Decide


10:33
Is Same PrivateKey and PrivateKey?
2nd PrivateKey (target checked)
2nd PrivateKey Format
P8
P12
2nd PrivateKey Filename
P8-e-GovEE01_sha2-pfx.pem
select
clear
Password (for decrypting 2nd PrivateKey)
input
clear
[Back]


10:33
Inputing a Password for decrypting 2nd Private
Password (max. 299)
gpkitest
[Cancel]
Decide


10:33
Is Same PrivateKey and PrivateKey?
2nd PrivateKey (target checked)
2nd PrivateKey Format
P8
P12
2nd PrivateKey Filename
P8-e-GovEE01_sha2-pfx.pem
select
clear
Password (for decrypting 2nd PrivateKey)
gpkitest
input
clear
[Back]



If the two private keys are identical, this will appear.

In addition to what I mentioned above, accurate comparison can not be made by comparing hash values of filed private keys.

Even the private keys that are not encrypted can not be correctly identified in the hash value comparison.

The reason is "subtle differences in encoding when ASN.1 is syntactically",
so the comparison of private keys after ASN.1 is syntactic can not make an exact same judgment.