Retrieve public key from private key

This command extracts the public key from the private key.

The private key of RSA public key cipher contains exactly the same elements as the public key.

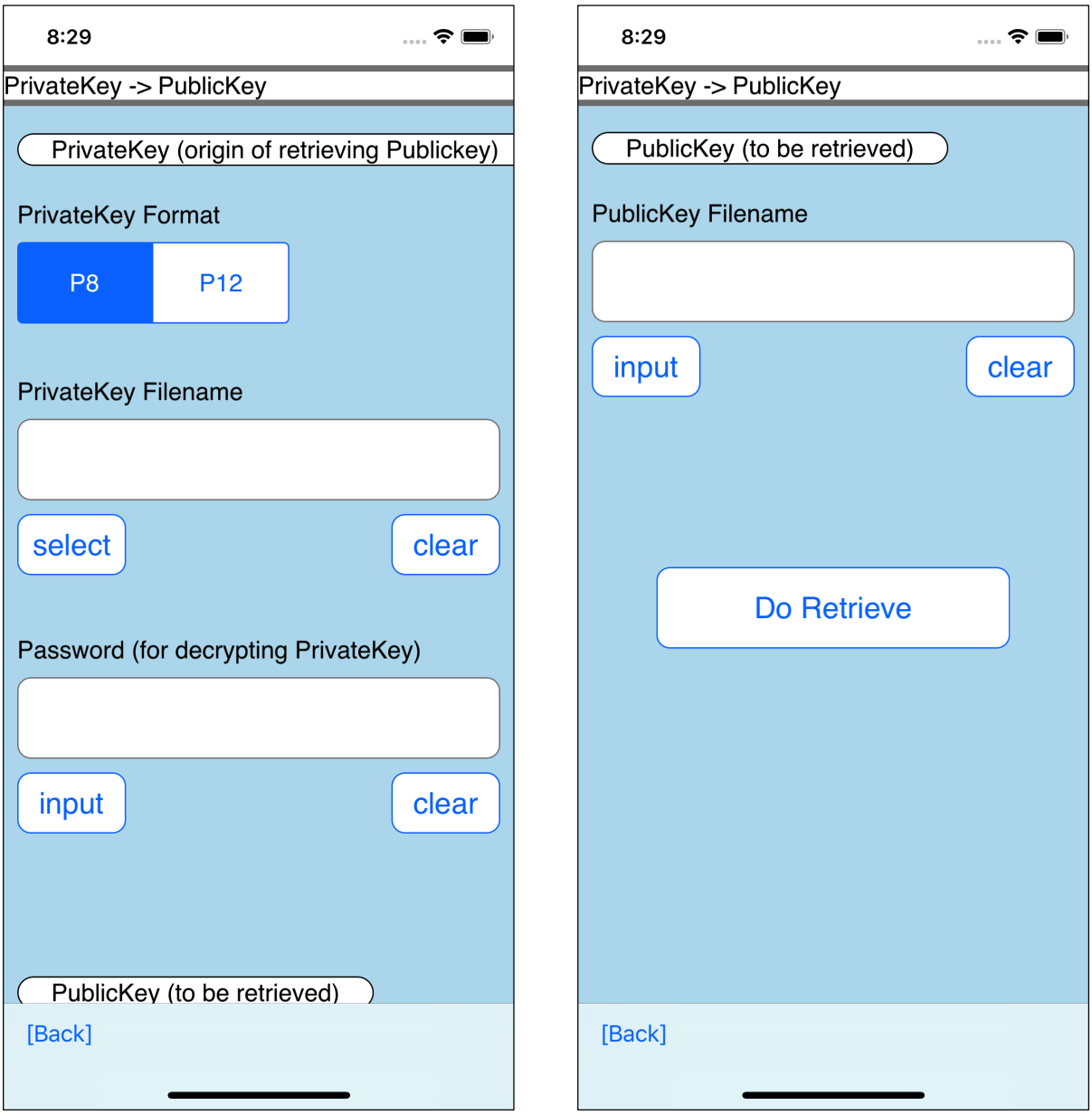
It just takes out the same element and converts it into a public key distribution forma

```
PKCS#1 RSAPrivateKey

RSAPrivateKey ::= SEQUENCE {
    version             Version,
    modulus             INTEGER, -- n
    publicExponent      INTEGER, -- e
    privateExponent     INTEGER, -- d
    prime1              INTEGER, -- p
    prime2              INTEGER, -- q
    exponent1           INTEGER, -- d mod (p-1)
    exponent2           INTEGER, -- d mod (q-1)
    coefficient         INTEGER, -- (inverse of q) mod p
    otherPrimeInfos     OtherPrimeInfos OPTIONAL
}
```

```
 modulus            INTEGER, -- n
 publicExponent     INTEGER, -- e
```

The values of these two elements in the private key are the same as the values of following two elements in the public key.

```
PKCS#1 RSAPublicKey

RSAPublicKey ::= SEQUENCE {
    modulus             INTEGER, -- n
    publicExponent      INTEGER  -- e
}
```



The user interface looks like this.

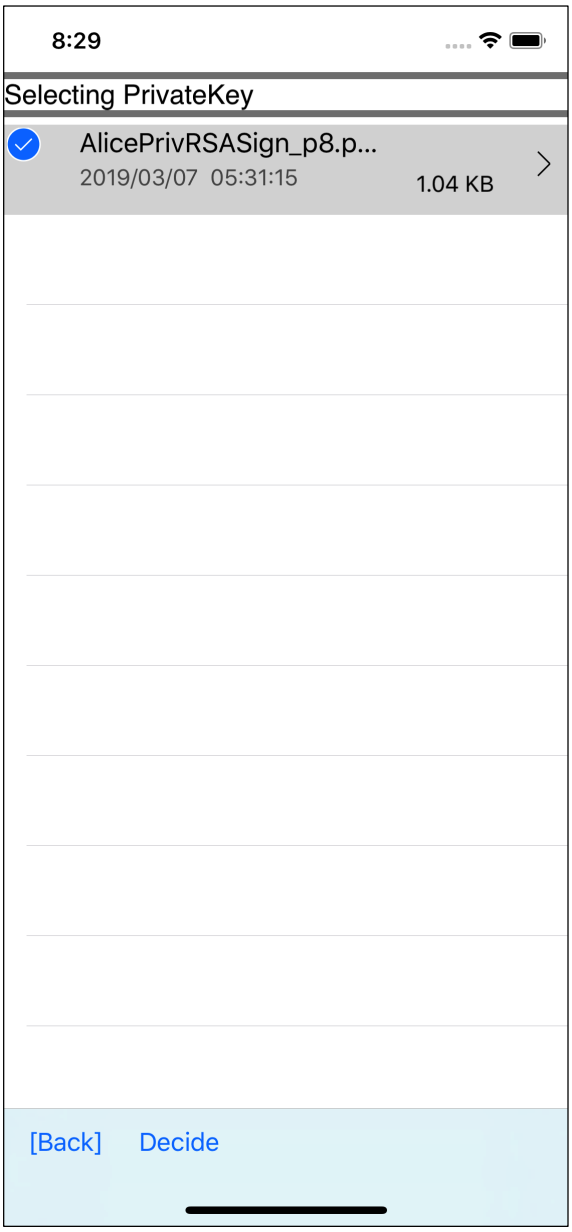
Private key type

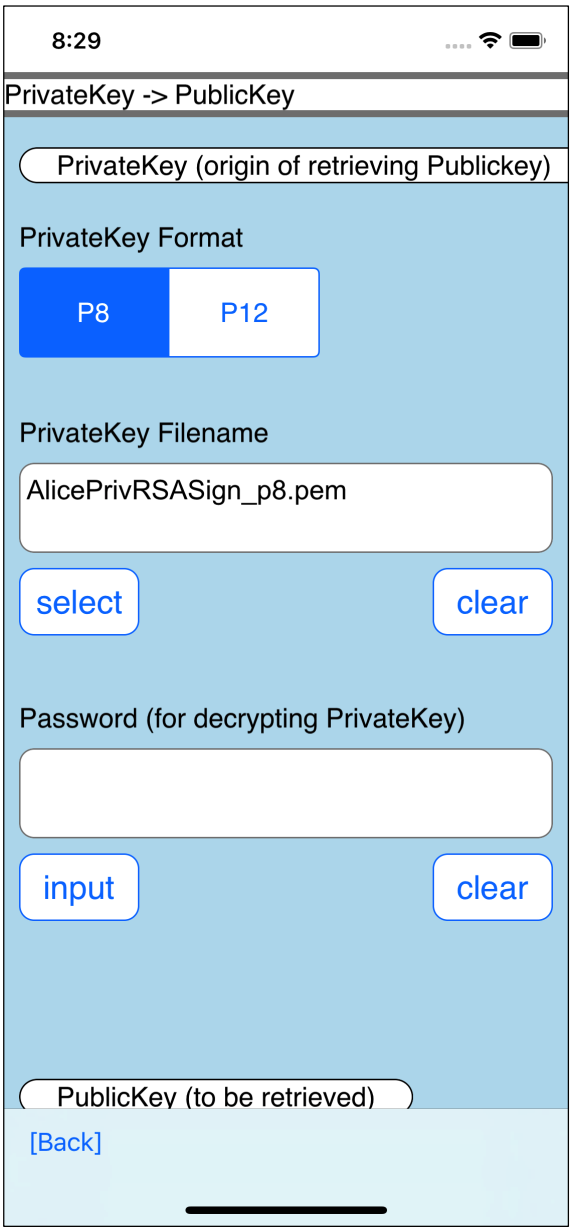
Private key file name

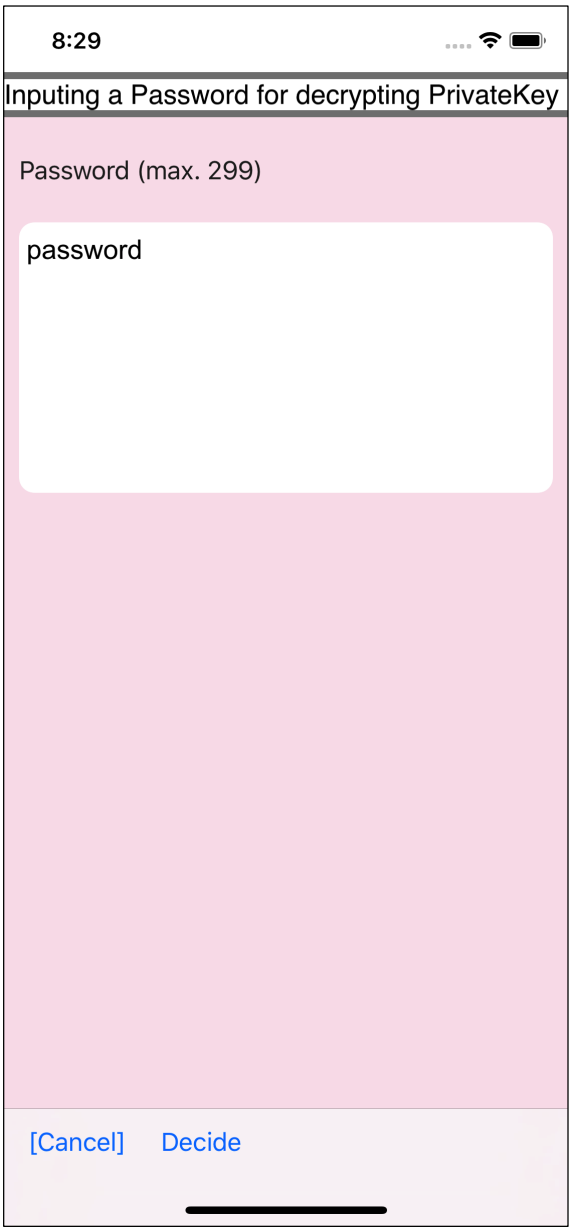
Password for private key decryption

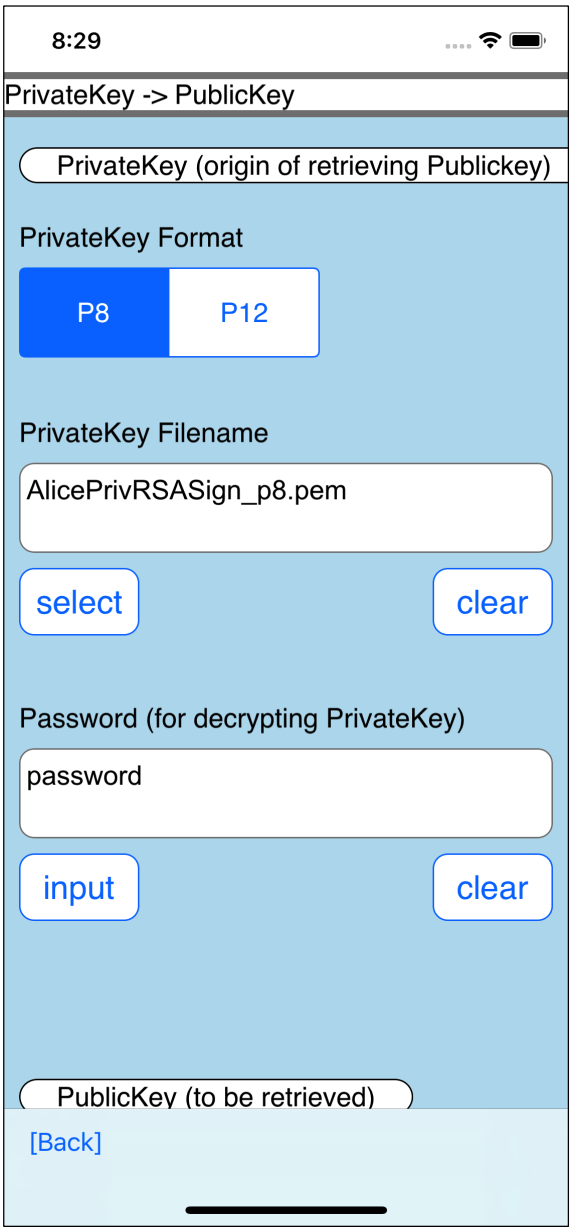
Public key output destination file name

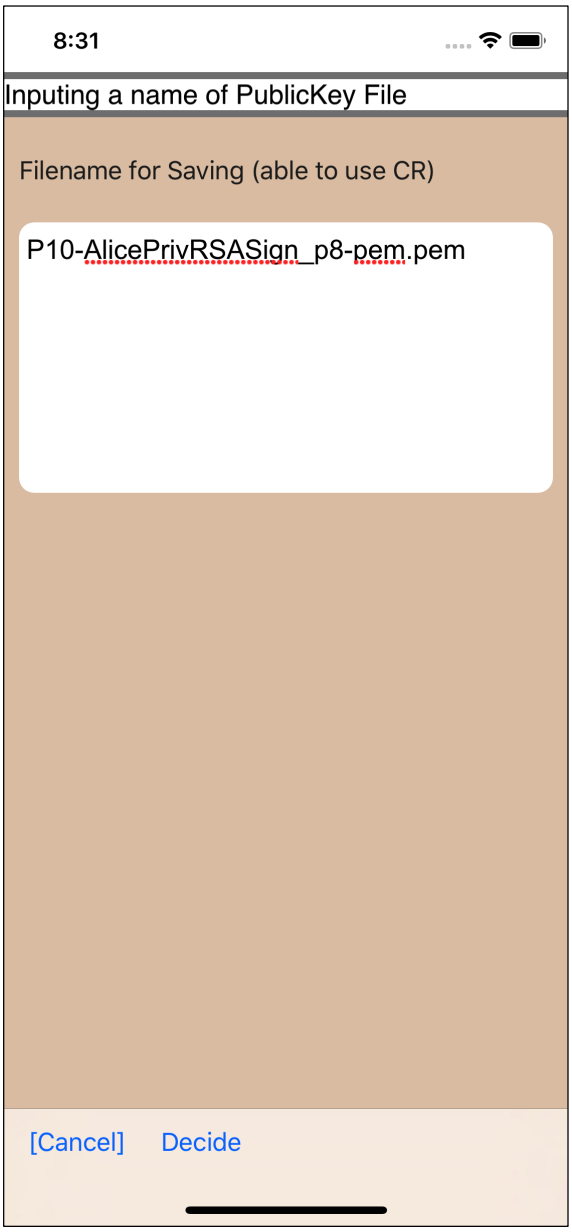
This is the meaning.

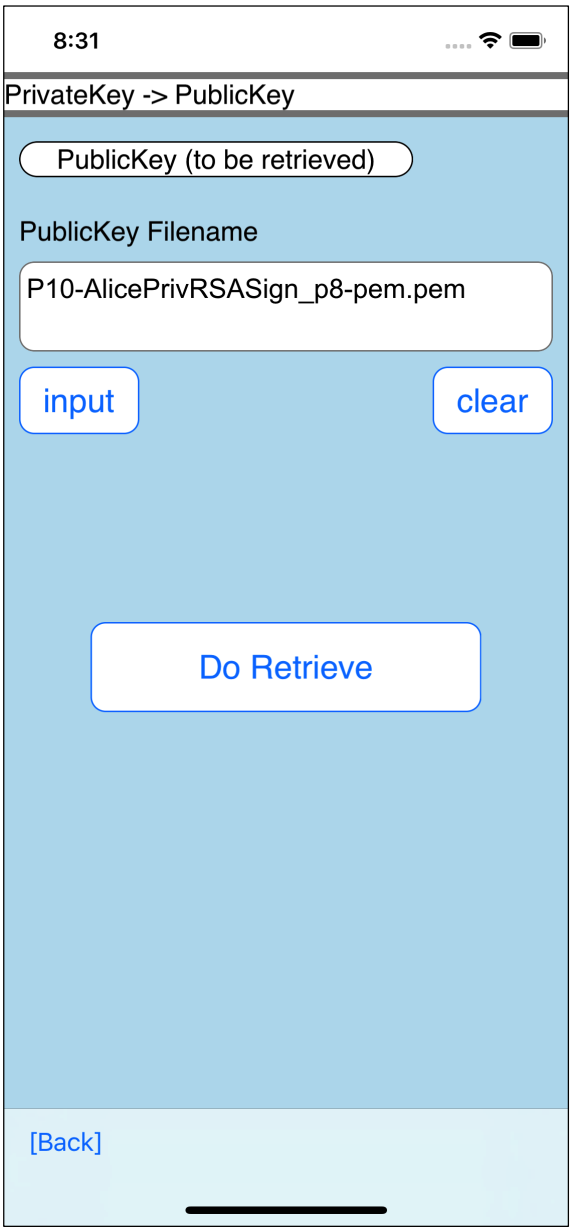

8:29
Selecting PrivateKey
AlicePrivRSASign_p8.p...
2019/03/07 05:31:15
1.04 KB
[Back]
Decide

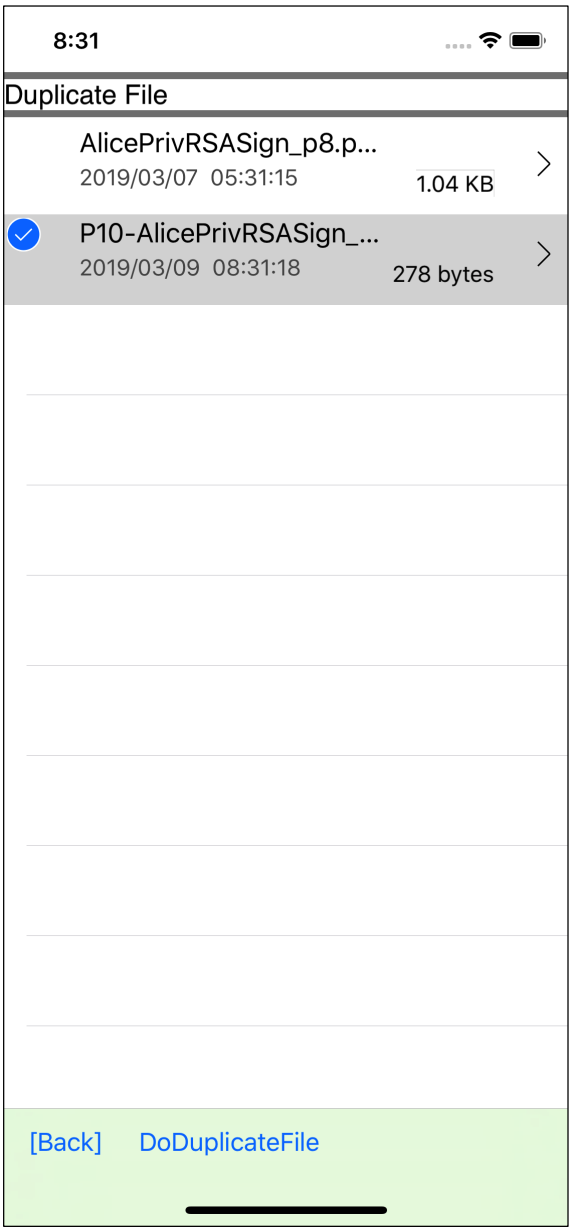

8:29
PrivateKey -> PublicKey
PrivateKey (origin of retrieving Publickey)
PrivateKey Format
P8
P12
PrivateKey Filename
AlicePrivRSASign_p8.pem
select
clear
Password (for decrypting PrivateKey)
input
clear
PublicKey (to be retrieved)
[Back]

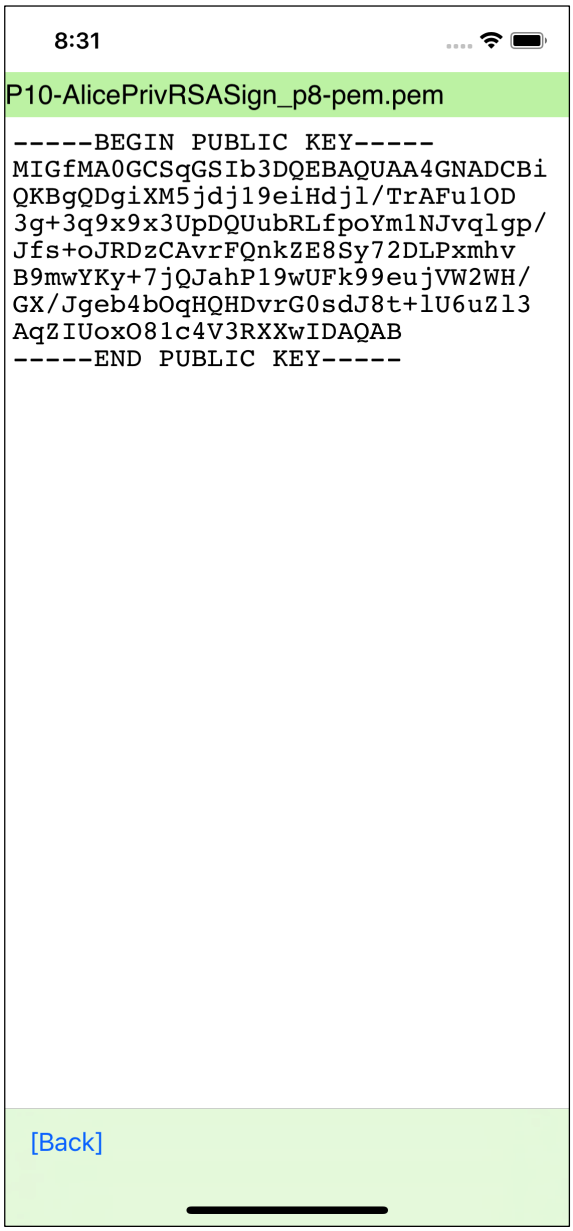

8:29
Inputing a Password for decrypting PrivateKey
Password (max. 299)
password
[Cancel]
Decide


8:29
PrivateKey -> PublicKey
PrivateKey (origin of retrieving Publickey)
PrivateKey Format
P8
P12
PrivateKey Filename
AlicePrivRSASign_p8.pem
select
clear
Password (for decrypting PrivateKey)
password
input
clear
PublicKey (to be retrieved)
[Back]


8:31
Inputing a name of PublicKey File
Filename for Saving (able to use CR)
P10-AlicePrivRSASign_p8-pem.pem
[Cancel]
Decide


8:31
PrivateKey -> PublicKey
PublicKey (to be retrieved)
PublicKey Filename
P10-AlicePrivRSASign_p8-pem.pem
input
clear
Do Retrieve
[Back]





If you look at the extracted result with “Duplicating File” command, it becomes like this.