

Key file confirmation

This command confirms the key file.

It is something like confirmation of contents, password is correct.



Press the main "Confirming Keyfile" button and you will see the view below.

7:18

Password Maker

Confirming Keyfile

Keyfile Filename

select clear

Password (for decryption)

input clear

Content

clear

Do Confirming Content

[Back]

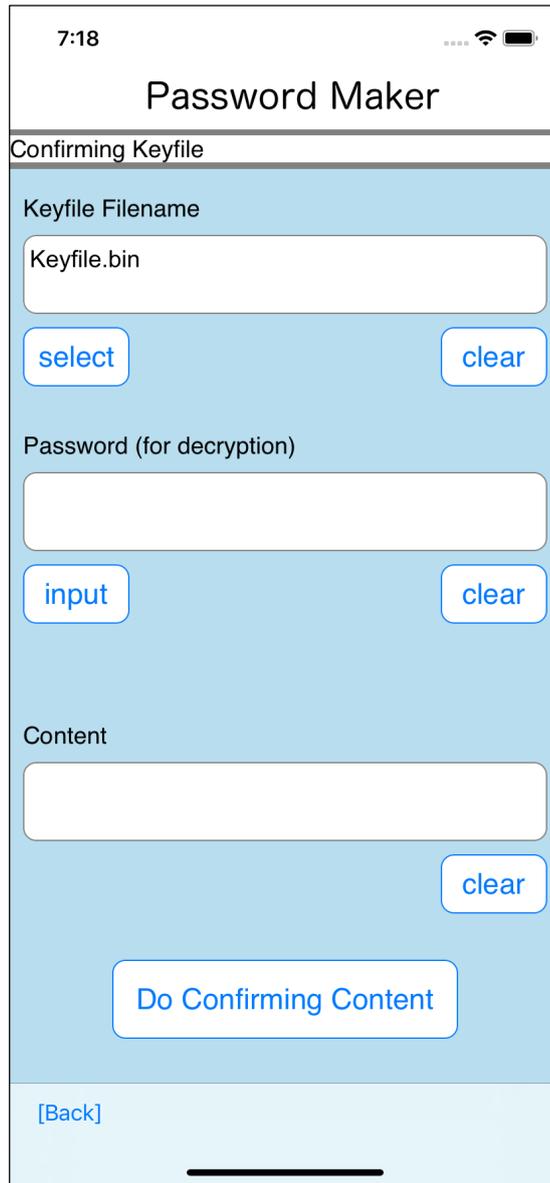
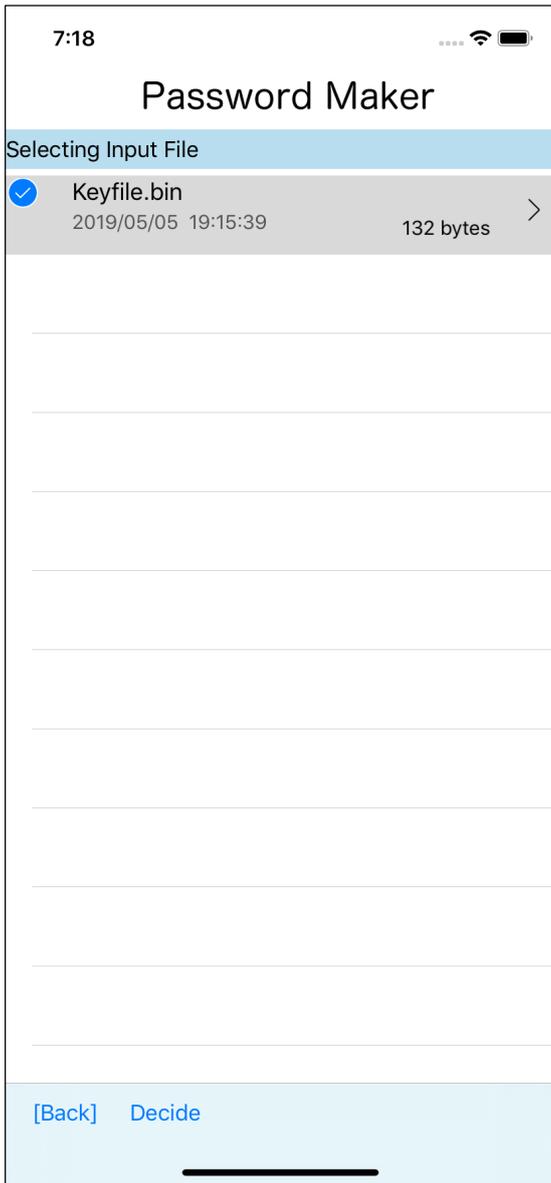
The user interface looks like this.

Key file name

Key file decryption password

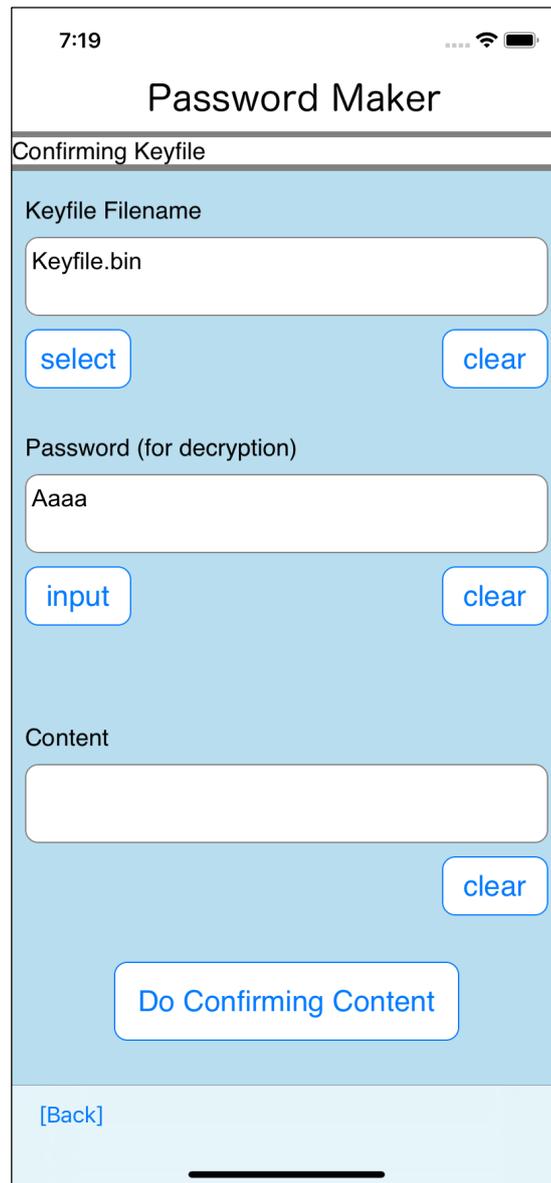
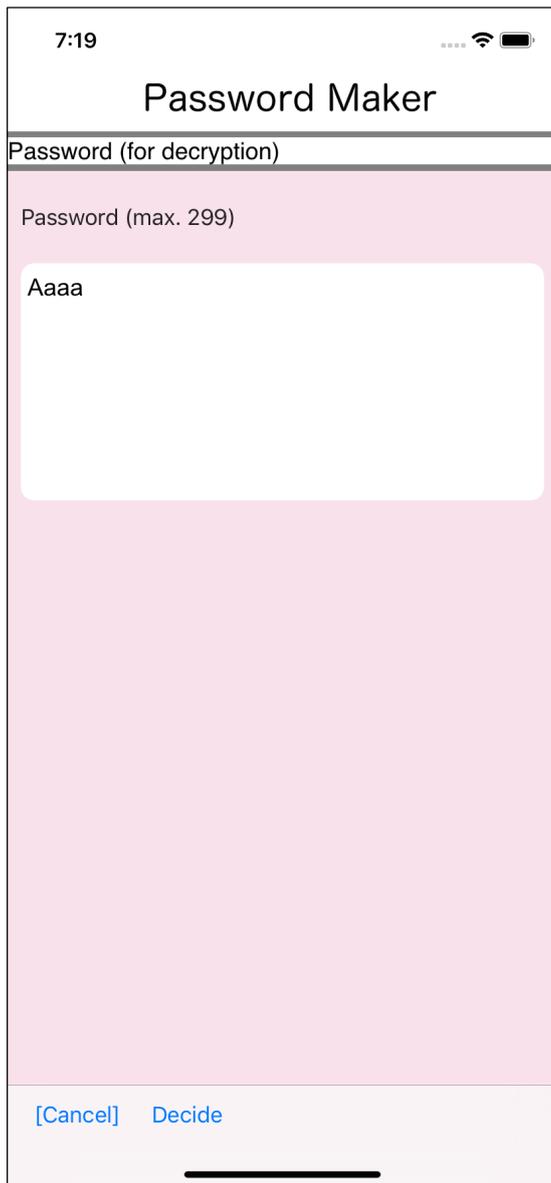
Contents value

This is the meaning.



When you press the “select” button under the key file name text view, the table view shown on the left will appear.

Select a file and press the “Decide” button on the toolbar to return.



Press the "input" button below the Password text view, and the password input view will appear as shown on the left.

Enter the password and press the "Decide" button on the toolbar to return.

7:19 ... 📶 🔋

Password Maker

Confirming Keyfile

Keyfile Filename

Keyfile.bin

[select](#) [clear](#)

Password (for decryption)

Aaaa

[input](#) [clear](#)

Content

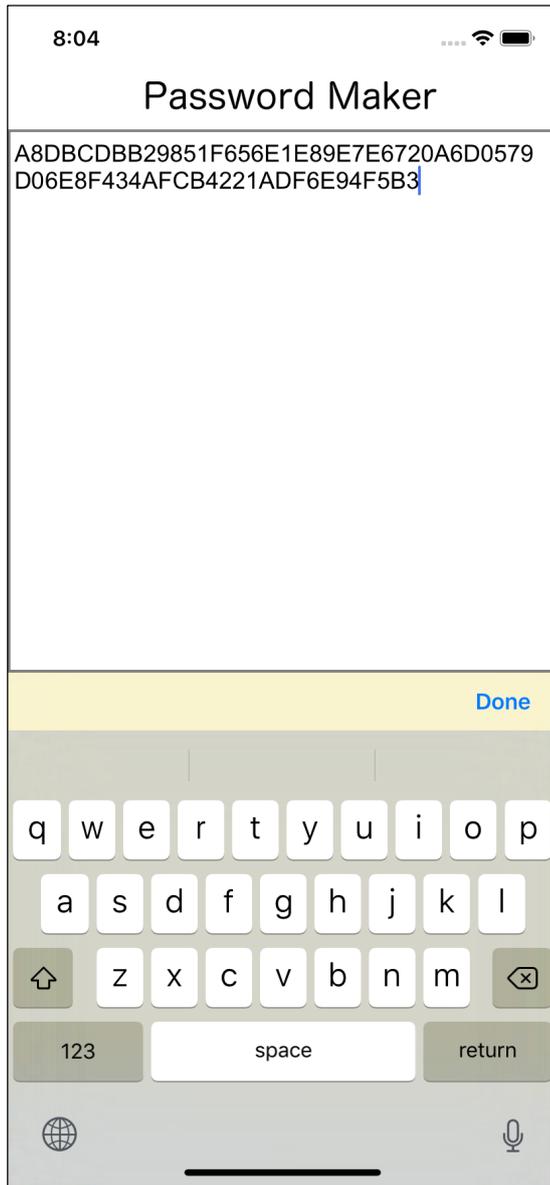
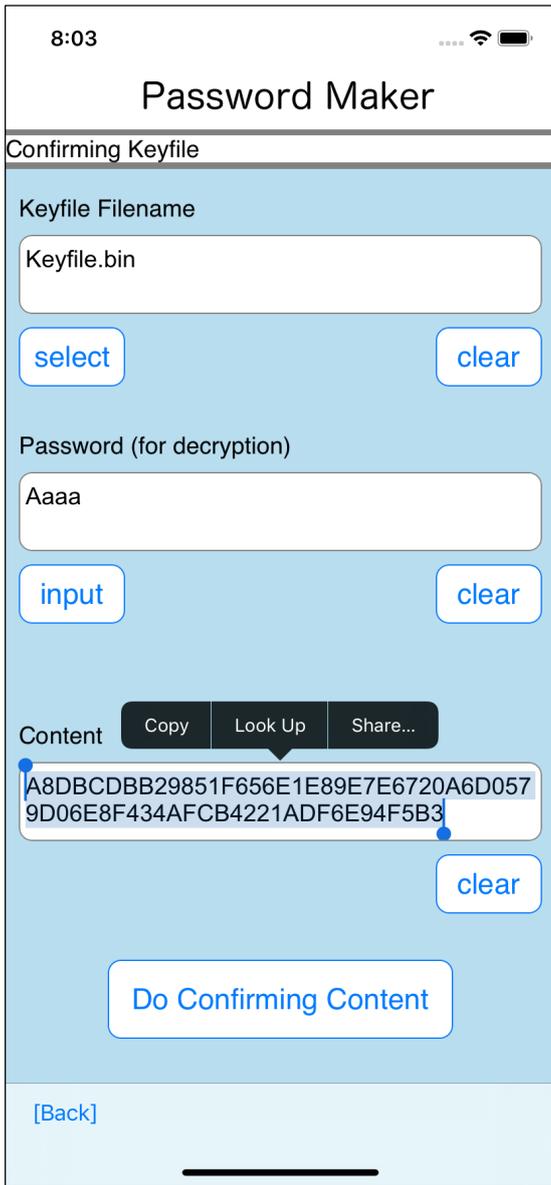
A8DBCDBB29851F656E1E89E7E6720A6D057
9D06E8F434AF4221ADF6E94F5B3

[clear](#)

[Do Confirming Content](#)

[\[Back\]](#)

After entering the file name and password, pressing the "Do Confirming Content" button will display the values stored in the key file like this.



If you need to copy, you can copy it this way.

If you press the “Do Confirming Content” button and the content is displayed,

The key file has not been tampered with (not broken, not damaged).

The password is correct.

it can be said so.

You can see that the cipher text created by AES-256-GCM encryption has been tampered with, regardless of where it is located.

If the contents are to be displayed, It can be said 'The key file has not been tampered with (not broken, not damaged).

The key file used by Password Maker includes encrypted text and authentication data.

Therefore, if the key file is completely replaced, it can not be detected that it has been replaced.

If replacement is also detected, the cipher text and authentication data must be bundled separately.

The key file used by Password Maker includes encrypted text and authentication data, so it can not detect that it has been completely replaced.

If you use a too simple password for the key file encryption, it is easy to replace the key file completely.

If you have to be wary of replacing key files, be careful.