

digital signature outline (3)

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

1:23

Outline of contents of Digital Signature

Input Filename (digital signature)

Input Filename (digital signature. file to be ver

Sign-by-Alice-no-Target.pem

select clear

Do Display

[Back]

This screenshot shows a mobile application interface with a light blue background. At the top, the status bar shows the time 1:23 and signal/battery icons. Below the status bar is a title bar with the text "Outline of contents of Digital Signature". The main area contains a text input field with the placeholder "Input Filename (digital signature)" and a label "Input Filename (digital signature. file to be ver". The input field contains the text "Sign-by-Alice-no-Target.pem". Below the input field are two buttons: "select" and "clear". At the bottom of the main area is a large button labeled "Do Display". At the very bottom of the screen is a "[Back]" link.

1:23

Signature target is not included.

X.509 Certificate is included.
counts 1

AuthenticatedAttributes is not used.

Counts of SignerInfo 1

OK

This screenshot shows a mobile application dialog box with a dark blue background. At the top, the status bar shows the time 1:23 and signal/battery icons. The dialog box contains the following text: "Signature target is not included.", "X.509 Certificate is included.", "counts 1", "AuthenticatedAttributes is not used.", and "Counts of SignerInfo 1". At the bottom of the dialog box is a button labeled "OK".

You can see that the Sign-by-Alice-no-Target.pem created in PKCS#12 signature creation (Sign 3) is as follows.

Sign subject is not included.

X. 509 public key certificates are included.

The number is one.

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.