

digital signature outline (5)

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

1:42

Outline of contents of Digital Signature

Input Filename (digital signature)

Input Filename (digital signature. file to be ver

Sign-by-Alice-only-Signature.pem

select clear

Do Display

[Back]

This screenshot shows the input screen of the application. The title is "Outline of contents of Digital Signature". There is a text input field with the placeholder "Input Filename (digital signature)" and the text "Sign-by-Alice-only-Signature.pem". Below the input field are two buttons: "select" and "clear". A large "Do Display" button is centered on the screen. At the bottom left, there is a "[Back]" link.

1:42

Signature target is not included.

X.509 Certificate is not included.

AuthenticatedAttributes is not used.

Counts of SignerInfo 1

OK

This screenshot shows the output of the application. The text displayed is: "Signature target is not included.", "X.509 Certificate is not included.", "AuthenticatedAttributes is not used.", and "Counts of SignerInfo 1". A large "OK" button is centered on the screen.

You can see that the Sign-by-Alice-only-Signature.pem created using one private key (signature 5) is as follows.

Sign subject is not included.

X.509 public key certificates are not included.

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 and

the public key used for verification

(PKCS#10 SubjectPublicKeyInfo or X.509 public key certificate).