

## digital signature outline (1)

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

1:36

Outline of contents of Digital Signature

Input Filename (digital signature)

Input Filename (digital signature. file to be ver

Sign-by-Alice-p12.pem

select clear

Do Display

[Back]

This screenshot shows the input screen of the application. The title bar reads 'Outline of contents of Digital Signature'. Below the title, there is a label 'Input Filename (digital signature)' and a text input field containing 'Sign-by-Alice-p12.pem'. To the right of the input field are two buttons: 'select' and 'clear'. Below the input field is a large 'Do Display' button. At the bottom left, there is a '[Back]' link.

1:36

Signature target is included.  
size 28

X.509 Certificate is included.  
counts 1

AuthenticatedAttributes is not used.

Counts of SignerInfo 1

OK

This screenshot shows the output of the application. The title bar reads '1:36'. The main content area displays the following text: 'Signature target is included. size 28', 'X.509 Certificate is included. counts 1', 'AuthenticatedAttributes is not used.', and 'Counts of SignerInfo 1'. At the bottom center, there is an 'OK' button.

You can see that the Sign-by-Alice.pem created in PKCS#12 signature creation (signature 1) is as follows.

Signature target are included.

The size of the signature target is 28.

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 not necessary to specify

the signature target and

the X.509 certificate that contains the public key used for verification.