Outline of contents of digital signature

This command displays an outline of the contents of the digital signature (PKCS#7 SignedData).

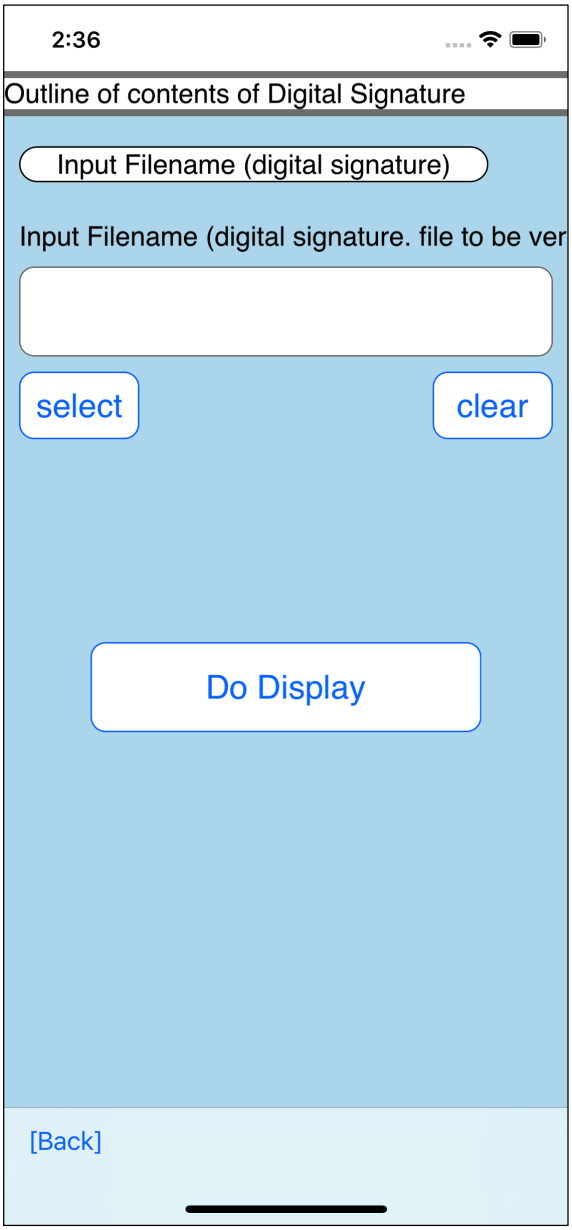
Whether the signature target is included?

Is an X.509 public key certificate included?

Whether AuthenticatedAttributes are used?

Does it contain an digital signature value?

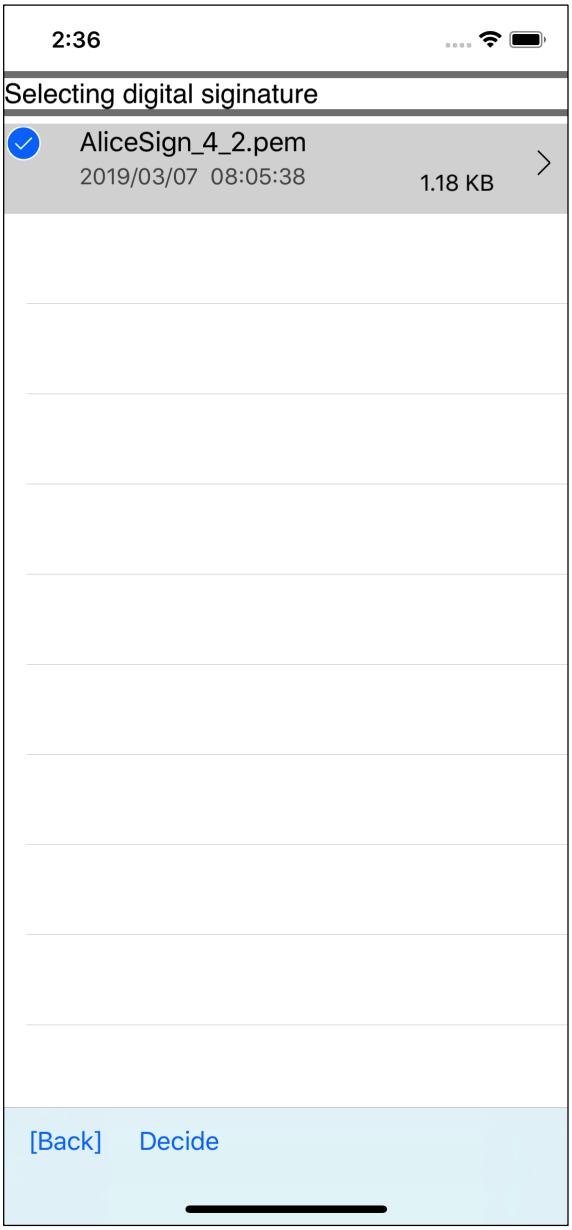
It displays these four points.

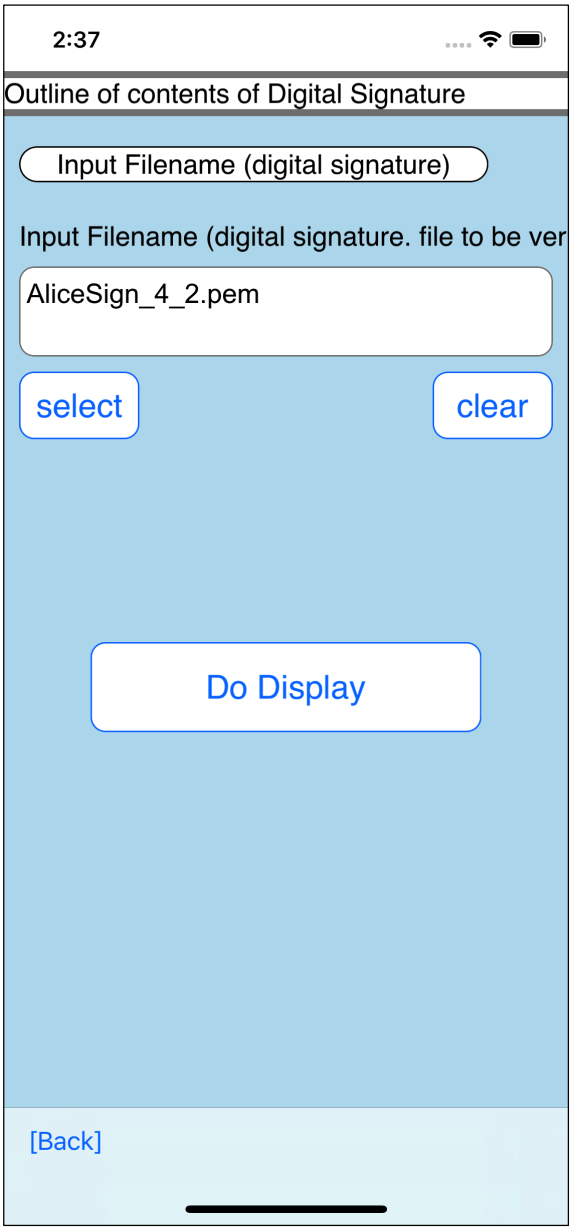


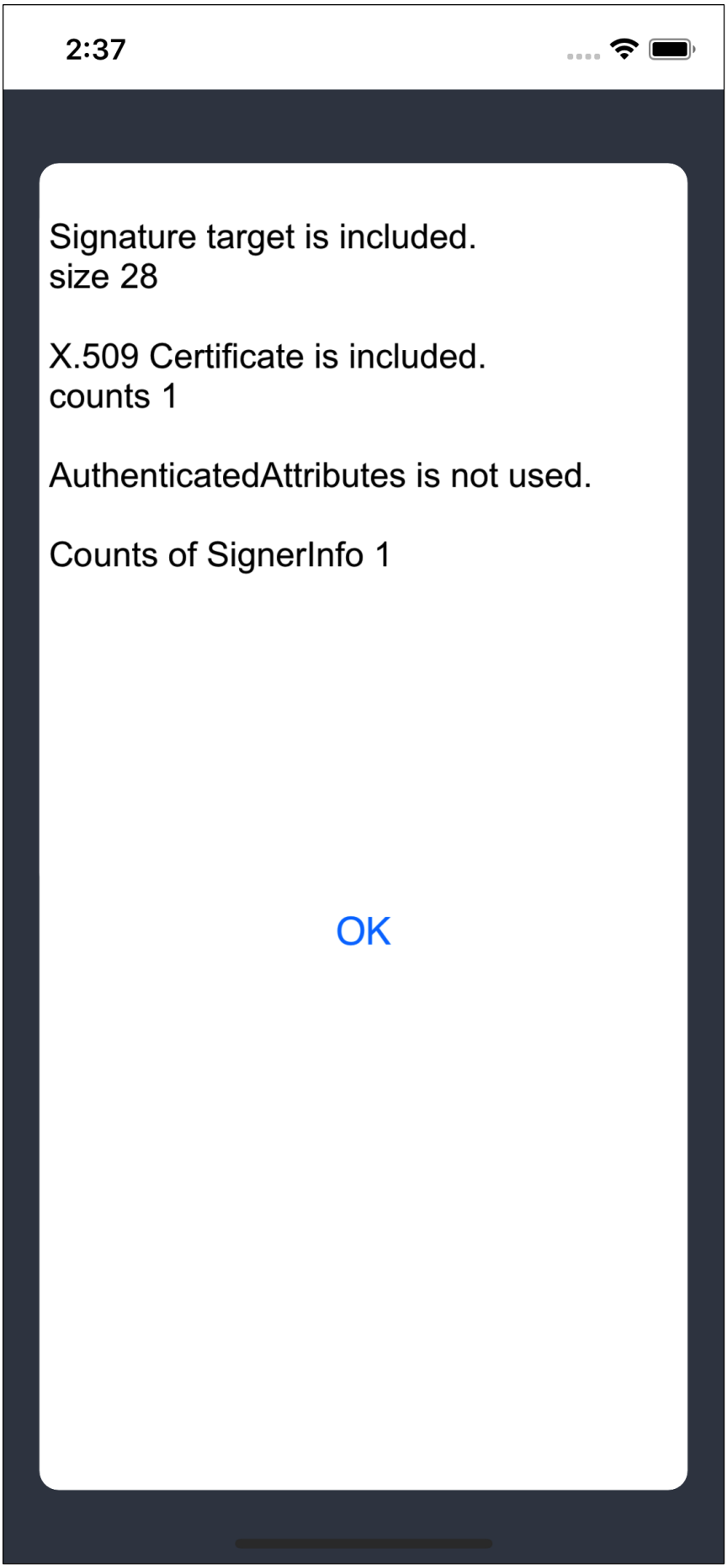
The user interface looks something like this.

Digital signature (PKCS#7 SignedData) file name

It is only this one on this command.


2:36
Selecting digital siginature
AliceSign_4_2.pem
2019/03/07 08:05:38
1.18 KB
[Back]
Decide


2:37
Outline of contents of Digital Signature
Input Filename (digital signature)
Input Filename (digital signature. file to be ver
AliceSign_4_2.pem
select
clear
Do Display
[Back]


2:37
Signature target is included.
size 28
X.509 Certificate is included.
counts 1
AuthenticatedAttributes is not used.
Counts of SignerInfo 1
OK

<table>
<tr><td rowspan="6">SignedData</td><td>version</td></tr>
<tr><td>digestAlgorithms</td></tr>
<tr><td>contentInfo</td></tr>
<tr><td>certificates</td></tr>
<tr><td>crls</td></tr>
<tr><td>
<table>
<tr><td rowspan="6">SignerInfo</td><td>version</td></tr>
<tr><td>issuerAndSerialNumber</td></tr>
<tr><td>digestAlgorithm</td></tr>
<tr><td>authenticatedAttributes</td></tr>
<tr><td>digestEncryptionAlgorithm</td></tr>
<tr><td>encryptedDigest</td></tr>
</table>
</td></tr>
</table>

This views’strings	PKCS#7 SignedData
Signature Target	contentInfo
X.509 Cerrificates	certificates
AtuthenticatedAttributes	atuthenticatedAttributes
SignerInfo	SignerInfos

It becomes such correspondence relation.

The Signature Target is, literally, a signature target.

A PKCS#7 SignedData may contain multiple X.509 certificates and multiple SigneresInfos.

In PKCS#7 SignedData, using AuthenticatedAttributes changes the signature method and signature value.

When agreement is obtained between the parties using PKCS#7 SignedData, it is often used AuthenticatedAttributes.

However, because there is a risk that generality will be lost, AuthenticatedAttributes is often not used when emphasis is on generality.

Signatures done by rsac do not use AuthenticatedAttributes.

Simply put, SingerInfo is a digital signature itself.

Indeed, the digital signature itself is encryptedDigest, at the bottom of SingersInfos.