Signature Creation Workflow and Configuration Options

The workflow is configurable through the GUI and registry settings.[3]

Supports 3rd party handlers.

Create signature appearances with the UI or programmatically. Contents are defined by the SigAP dictionary included in the form field.[4]

The signature appearance is included in the message digest.

The DSA/RSA algorithm is specified by the signer's digital ID private key in a P12/PFX file, smart card/token, roaming ID server, Mac Key Chain, or Windows store.

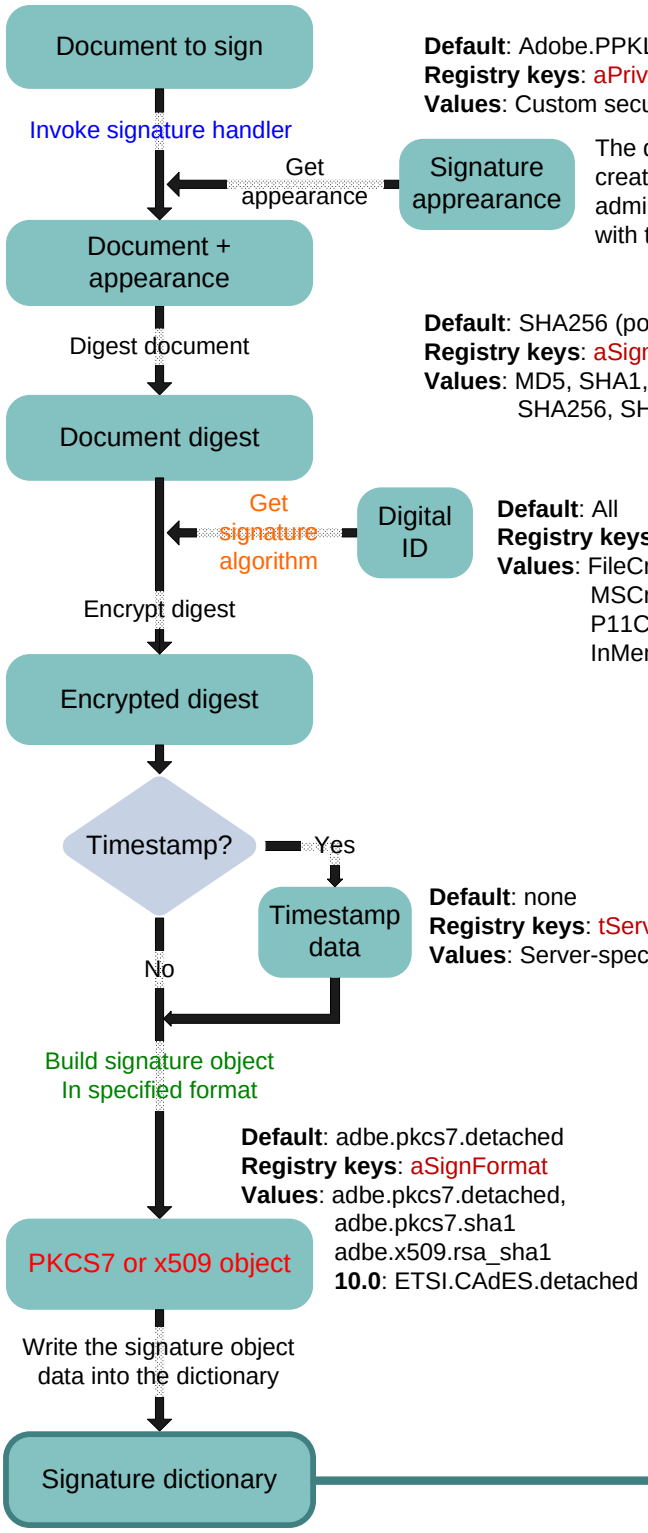
Revocation checking is configurable for any certificate in the chain, including the signers, the ICA, any timestamp CA, etc.[3]

If not time stamped or time stamping fails, use the local time.[3]

The signature object is built in memory until all the revocation checking, timestamp, and certificate data is retrieved.

The signature object is encoded using the Distinguished Encoding Rules (DER). The DER object is hex encoded and padded with zeros to make the signed byte range match the size that was set aside when the signing process began.

Dictionary contents are customizable through UI and registry settings such as cReasons, cContactInfo, etc.[3]



Default: Adobe.PPKLite
Registry keys: aPrivKey
Values: Custom security handlers

The default is none. Users can create appearances on the fly or admins can deploy appearances with the application.

Default: SHA256 (post 9.1), SHA1 earlier
Registry keys: aSignHash, tSignHash
Values: MD5, SHA1, **8.0**: RIPEMD160, SHA256, SHA384, SHA512

Default: All
Registry keys: cCredProvider
Values: FileCredentialProvider, MSCredentialProvider, P11CredentialProvider, InMemoryCredentialProvider

Default: none
Registry keys: tServer, tName, .etc
Values: Server-specific

Default: adbe.pkcs7.detached
Registry keys: aSignFormat
Values: adbe.pkcs7.detached, adbe.pkcs7.sha1 adbe.x509.rsa_sha1
10.0: ETSI.CAdES.detached

obj<<[1]

```
/Filter/Adobe.PPKLite
/SubFilter/adbe.pkcs7.detached
/M(D:20070215121851-08'00')
/Name(RSA1024 SHA1)
/ByteRange[0 6400 34008 7262 ]
/Contents<3745 [ SNIP ] 000000>
/Prop_Build[2]
    /Filter
        /Name/Adobe.PPKLite
        /R 131101
        /Date(Oct 22/06 11:11:05)
    /Other entries . . . .
/Reason(My boss made me sign.)
/Type/Sig
/ContactInfo(ben@example.com)
/Location(San Jose, CA)
```

>>endobj

References

[1] *PDF Reference*
[2] *Digital Signature Build Dictionary Specification*
[3] *Digital Signatures and Rights Mgmt in Acrobat*
[4] *Digital Signature Appearances (in the SDK)*