certicom™
securing innovation

Certicom CodeSign™ 2.1

Code Signing Application with Suite B support

Certicom CodeSign is a code signing application designed to enable device manufacturers and network operators to provide strong authentication and protect firmware and code file updates from tampering and malicious code.

Flexible and easy to use, CodeSign now includes support for the Suite B curves necessary to ensure government-approved security.

flexible

Designed to meet industry standards such as CableLabs™ DOCSIS BPI+ and CableLabs™ OpenCable security requirements, Certicom CodeSign can also be used to generate generic digital signatures for a wide range of code files. Digital signatures can be time-stamped with custom signing times, allowing you to more effectively manage the deployment of signed code by controlling when a device should accept signed firmware

easy to use

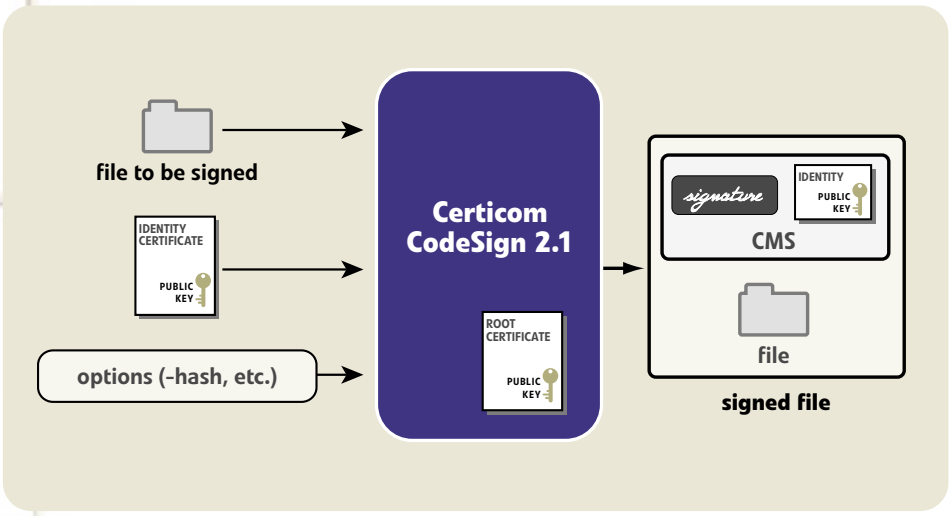
Certicom CodeSign can be called from a makefile to allow clean integration with system builds. It can also be used with digital certificate toolkits such as Security Builder® PKI™ to provide a complete package to secure delivery of firmware and code updates to your customer's equipment.

standards based

To ensure interoperability, Certicom CodeSign can be used to sign firmware that needs to adhere to IETF standards, including PKCS #7 SignedData and X.509 v3. CodeSign is also compliant with industry standards such as DOCSIS 1.1/2.0 BPI+ security requirements and supports Suite B requirements.

reduces cost

The introduction of Certicom CodeSign eliminates the requirement to create a custom system to sign code and firmware updates. CodeSign is a commercially supported product that allows you to focus on your core competency.



Certicom CodeSign allows developers to sign and verify code that is being developed in a distributed environment. Full certificate chaining and standards based support for Cable Labs DOCSIS BPI+ and Open Cable provide for wide interoperability.

Features

Feature		
Support for CableLabs™ DOCSIS 1.1/20 BPI+		X
Support for CableLabs™ OpenCable™ I05		X
Support for:	PKCS#1	X
	PKCS #5	X
	PKCS #7 SignedData	X
	PKCS #8	X
	PKCS #12	X
	X.509 v3 certificates	X
	Curves supported	secp163r1, secp256r1, secp384r1, secp521r1
	Platform Support	• Windows 32 • Linux x86 • Solaris SPARC 2.8 and 2.9 (32- and 64-bit platforms)

Options

address <address> [<length>]	Specifies the address where the final image (or piece of image) will be stored.
allow <option>	Forces Certicom CodeSign to ignore certain errors
asn	Enables the CMS data to be output in the ASN.1 format
format <docsis | opencable | trustedboot>	Allows specification of output format. The default is trustedboot.
hash <sha1 | sha256 | sha384 | sha512>	Specifies which hash algorithm to use.
help	Display tool usage information.
include certificate	Includes identity certificate(s) in the CMS object.
identity <filename1 [filename2…]>	Specifies the identity file(s). Currently supports PEM- or DER-encoded identities.
input <filename>	Specify the file to be signed.
output <filename>	Specifies the output file.
password <password>	Specify the private key password.
quiet	Suppresses all output.
relative <start | end>	Determines whther CMS data will be placed before the start of image or after the end of the image data.
signtime <certificate | current | <YYMMDDhhmmss>	Allows signing time to be specified. Choosing 'certificate will use the start time of the validity of the certificate.
trusted <filename1 [filename2…]>	Specify the certificate authority certificate file (s)
verbose <cms | identity | trusted>	Display additional information about the identity.
verify <filename>	Verify a previously produced CMS file.
version	Output version information.

about certicom

Certicom protects the value of your content, applications and devices with security offerings based on Elliptic Curve Cryptography (ECC). Adopted by the National Security Agency (NSA) for classified and sensitive but unclassified government communications, ECC provides the most security per bit of any known public-key scheme. Visit www.certicom.com.

certicom™

North America 1.800.561.6100
EMEA +44.20.7484.5025
International +1.905.507.4220
E-mail info@certicom.com
www.certicom.com