MOCANA

Security of Things Crypto [NanoCrypto™]

Mocana's high-performance, ultra-efficient and government-certified cryptography engine, purpose built for embedded device OEMs and ISVs.

Features & Benefits

- Small footprint, high performance
- FIPS 140-2 Level 1 validated (optional)
- Dramatically speeds integration & testing of complex cryptographic functions for your product
- NIST-Approved "Suite B" cryptography included
- Guaranteed "GPL-Free" code protects your intellectual property
- Expert development support from Mocana engineers

Mocana NanoCrypto is a sophisticated, government-certified cryptographic engine purpose built for difficult and resource-constrained embedded systems environments. Mocana's core cryptographic engine secures millions of devices from hundreds of technology manufactures worldwide. It is, quite simply, one of the smallest, fastest and most comprehensive cryptographic cores on the market.

With out of box support over 35 operating systems, NanoCrypto enables device OEMs and ISVs to add sophisticated cryptographic security features to almost any type of device or application.

On platforms that support hardware offload of crypto jobs, NanoCrypto's low host CPU utilization extends battery life on handheld devices and remote sensors, while enabling even the most humble processors to use robust cryptographic techniques to protect sensitive information from disclosure and authenticate legitimate users, systems and data. NanoCrypto is written entirely in C, and assembly optimizations are available for several popular hardware platforms, including PowerQUICC, ARM, PowerPC, MIPS, Coldfire, H8S and x86. Best of all, it's highly portable and supports over 30 operating systems and RTOS's out of the box. You can even use it in environments without any OS at all. NanoCrypto enables sophisticated developers to work directly with cryptographic primitives to build confidentiality, integrity and authentication features directly into their devices.

NanoCrypto offers developers a rich selection of cryptographic technologies, methods including RSA and elliptic curve, symmetric algorithms like 3DES and AES, message authentication, hashing and pseudorandom number generation. Best of all, FIPS 140-2 level 1 government certified NanoCrypto binaries are available for many popular platforms.

© 2015 Mocana Corporation

NanoCrypto Features

Tiny Memory Footprint

NanoCrypto is highly configurable and designed specifically for tight environments. Depending on the algorithms you choose, you can implement fully functional cryptographic implementations in as little as 30KB.

Rich Algorithmic Support

ASYMMETRIC CRYPTOGRAPHY

- Diffie-Hellman (groups – 1, 2, 5, 14, 15, 16, 17, 18, 24)
- ECDH (NIST p-Curve 192, 224, 256, 384 and 521)
- Ephemeral DH
- RSA
- DSA
- ECDSA (NIST p-Curve 192, 224, 256, 384 and 521)

SYMMETRIC CRYPTOGRAPHY

- AEAD-AES-GCM-128 (Suite B)
- AEAD-AES-GCM-256 (Suite B)
- AES-CBC
- AES-CTR
- AES-ECB
- AES-EAX
- AES-GCM
- AES-CCM
- AES-MMO
- AES-CFB
- AES-OFB
- AES-XTS
- DES
- Triple-DES
- ARC2
- Blowfish
- Hashing
- SHA1, SHA-224, SHA-256, SHA-384, SHA-512
- HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512, HMAC-MD5
- MD2, MD4, MD5
- AES-GMAC, AES-GCM
- AES-CMAC
- AES-XCBC-MAC-96
- AES-CCM
- AES-MMO

RANDOM NUMBER GENERATORS

- FIPS 186-2 – General Purpose (x-change notice; SHA1)
- FIPS 186-2 - Regular (x-change notice, k-change notice; SHA1)

PUBLIC KEY CRYPTOGRAPHY STANDARDS SUPPORT

- PKCS#1 version 1.5 and 2.1
- PKCS#3
- PKCS#5
- PKCS#7 (Supports Suite B)
- Cryptographic Message Syntax (CMS), support for S/MIME
- PKCS#8
- PKCS#10
- PKCS#12

Supported OS Platforms

- Microsoft Vista, Server 2003 SP2 or later, or Microsoft Server 2008
- Windows CE & WIndows Mobile
- Android
- Apple iOS
- RedHat Linux v4 and 5
- SUSE Linux, Enterprise 9 and 10, SP1 or later
- AIX v5.2 and 5.3
- Solaris 9 and 10
- HP-UX 11i
- BSD
- VxWorks
- Symbian
- Monta Vista Linux
- Many other platforms. Email **iotsales@mocana.com** to ask if your platform is supported.

Note: Mocana Security of Things™ products are highly portable across 35+ Operating Systems (OS) and all major processor architectures. Some Mocana Security of Things products require tight integration with an OS, while others either do not require an OS, rely on POSIX, or a primitive OS-application interface. Mocana's model is to provide the best out of box experience for all major Operating Systems, including newer versions upon availability. Please share your OS, OS version, and processor information with your Mocana Account Representative to ensure the necessary technical support is provided to you. Alternatively, Mocana Professional Services can assist in porting and integrating Mocana products onto your target platform if needed.

NanoCrypto Benefits

Works Where Others Won't

NanoCrypto fits into tiny memory footprints where other implementations simply can't… and open-source packages can't match Mocana's throughput performance.

FIPS Certified with NIST-Approved Suite B Support

All government agencies and most contractors require FIPS-certification of cryptographic engine—a difficult certification to achieve. NanoCrypto's core cryptographic engine is available to you in source, or as a government-certified FIPS 140-2 Level 1 validated binary. Both source and binary versions include full support for NIST-Approved Suite B algorithms, providing secure communications between high-assurance (classified) and basic-assurance systems.

Complete Solution

There are a lot of other cryptography packages out there. But almost all of them are incomplete—missing critical standards, algorithms or code that you'll need to finish your cryptography implementation. Only NanoCrypto offers everything you need together in one package, to get the job done right—and fast. Guaranteed.

GPL-Free Code

NanoCrypto is usually less expensive than "free" open source code, especially when engineering, testing and support costs are factored in. Since we guarantee that NanoCrypto contains absolutely no GPL code, you can be confident your intellectual property won't accidentally become public domain because of "GPL contamination"—something open source projects can't do.

Platform Independent

NanoCrypto, like all of Mocana's device security toolkits, is CPU-architecture and platform independent. NanoCrypto is immediately available for over 35 operating systems and 70 processors. Platforms supported out-of-the-box include Linux, Monta Vista Linux, VxWorks, OSE, Nucleus, Solaris, ThreadX, Windows, MacOS X, (ARC) MQX, pSOS, and Cygwin. NanoCrypto is endian-neutral, and can be used without an RTOS if required.

Dramatically Speeds Your Development Cycle

NanoCrypto is a ready-made, pre-optimized and exhaustively tested cryptography solution that frees your in-house development resources to focus on what's really important: the functionality of your project. NanoCrypto allows you to develop proprietary systems while giving you the freedom to substitute in the commercially available components you choose.

Which NanoCrypto Edition is Right for You?

Features	NanoCrypto Source	NanoCrypto Source - Suite B	NanoCrypto FIPS Binary
FIPS-Certified Algorithms	✓	✓	✓
FIPS-Certified Binary Implementation	✗	✗	✓
Suite B Algorithms	✗	✓	✓
Supports Offload of Crypto Jobs to Specialized Hardware	✓	✓	✓
RSA and Elliptic-Curve Support	✓	✓	✓
Platform Independent	✓	✓	✗
GPL-Free Code, Guaranteed	✓	✓	✓

NanoCryptoTM FIPS 140-2 Certified Platforms

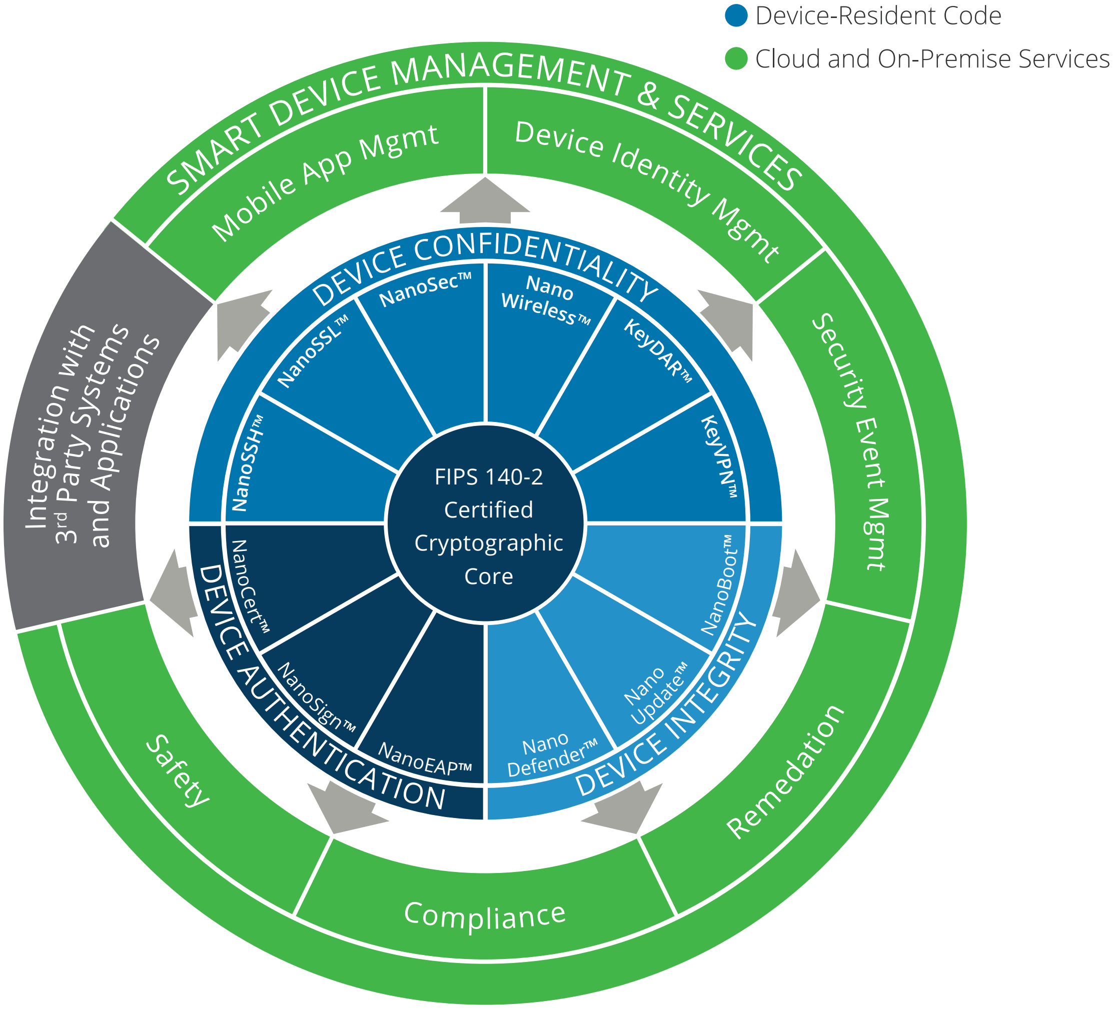
NanoCrypto FIPS 140-2 Binary is available off-the-shelf for the following operating systems/ processors. This list changes frequently, so please email **iotsales@mocana.com** if you don't see your platform here.

Operating System	Processor
FIPS LEVEL 1 – SOFTWARE	
VxWorks 6.7	Intel Core2 Duo
VxWorks 5.5	PowerQuicc III / e500
VxWorks 5.5	Freescale e600
VxWorks 6.4	PowerQuicc III / e500
VxWorks 6.4	PowerQuicc II (82xx) / 603e
VxWorks 6.2	PowerQuicc II Pro (83xx) / e300
VxWorks 6.4	PowerQuicc III / e500
VxWorks 5.5	Freescale e600
VxWorks 5.5	PowerQuicc III / e500

Operating System	Processor
FIPS LEVEL 1 – SOFTWARE	
Linux TBD	PowerQuicc III / e500
Linux TBD	MIPS64
Android 2.2	ARMv7 - (QSD 8250 -Snapdragon)
Android 3.0	ARMv7-A Cortex (NVIDIA Tegra 2)
Android 2.2	ARMv7 - (QSD 8250 -Snapdragon)
ThreadX ver 5.3	PowerQUICC III PC/104 PCB
Intel/WindRiver Linux v3	Freescale PowerQuic III
Integrity 5.0.11	Freescale 8540
Integrity 5.0.11	Freescale P2020
Integrity 5.0.11	Freescale 2910
Integrity	Freescale 8544
Linux 2.6.20	Freescale PowerQuic III
None	Neuron 5000
VxWorks 6.4	Intel XScale PXA (PXA270)
Android 2.3	ARMv7 (OMAP4)
VxWorks 5.5	Freescale e600
Intel/WindRiver Linux v4 (2.6.34)	Freescale PowerQuic III iOS5
FIPS LEVEL 2 – HARDWARE / SOFTWARE	
SnapGear Linux 2.6.19	Intel XScale IXP425
Linux magic 2.6.34.7	Intel Mobile Core 2 Duo
ThreadX ver 5.3	PowerQUICC III PC/104 PCB

Mocana's Security of Things Platform

NanoCrypto is part of the Mocana Security of Things, designed to secure all aspects of any connected device. All components of the Security of Things are built on a common architecture and share a common API and code base. As a device designer, you can choose only the components you need for your particular project or standardize company-wide on the Security of Things, future-proofing your investment with this broad, cross platform, flexible and extensible security architecture.



© 2015 Mocana Corporation

About Mocana IoT

Mocana IoT provides the Mocana Security of Things Platform—a high-performance, ultra-optimized, OS-independent, high-assurance security solution for any device class. The Platform is being rapidly adopted by next-gen IoT device designers who demand architectural freedom, and who understand the complexity and risk exposure inherent in in-house and other provider's solutions. Mocana's award-winning cryptographic solutions are used in the most stringently-constrained and life-critical systems by Fortune 500 companies, world-leading smart device manufacturers, and government agencies.

More information is available at **www.mocana.com/iot-security**

Mocana Corporation
20 California Street
San Francisco, CA 94111
tel (415) 617-0055 toll free (866) 213-1273
www.mocana.com/iot-security iotsales@mocana.com