MOCANA

Security of Things Connectivity [NanoSec™]

Mocana's comprehensive IPsec and IKEv1/v2 solution with integrated certificate management functionality.

Features & Benefits

- Small footprint, high performance
- FIPS 140-2 Level 1 validated (optional)
- Complete IPSec & IKEv1/v2 solution with certificate management
- Dramatically speeds integration & testing of IPsec and certificate management
- NIST-Approved "Suite B" cryptography included
- Full NIST USGv6 compliant implementation of IETF IPsec version 3
- Guaranteed "GPL-Free" code protects your intellectual property
- Zero-threaded, asynchronous architecture
- Expert development support from Mocana engineers

IPsec/IKE is a standard designed by IETF to provide interoperable, high quality, cryptographically-based security for IP communication. It's useful for providing authentication (to ensure peers are communicating with the intended trusted parties), data confidentiality (to ensure data cannot be read in transit) and message integrity (to ensure traffic has not been altered in transit). These security services are provided at the IP layer, offering protection to all the protocols carried over IP.

IPsec provides a great deal of flexibility and granular control over the security services offered. The most popular application of IPsec is the VPN (Virtual Private Network) which creates a secure encrypted "tunnel" over the unsecured Internet. Once a VPN is established, the two ends can run virtually any data, voice and video application securely. IPsec is terrific for reducing the threat of packet sniffers or man-in-the-middle attacks.

Unfortunately, most IPsec packages are designed for PC's, not embedded devices. That means that they can be somewhat unwieldy in memory-constrained device environments...and the performance of typical commercial or open-source IPsec offerings can be pretty disappointing, as well.

NanoSec is the answer.

NanoSec is Mocana's ultra-optimized, micro-footprint IPsec/IKE solution specifically designed to speed product development while providing best-in-class device security services for resource-constrained environments. And it's surprisingly affordable: your NanoSec total cost of ownership will usually be substantially less expensive than open source.

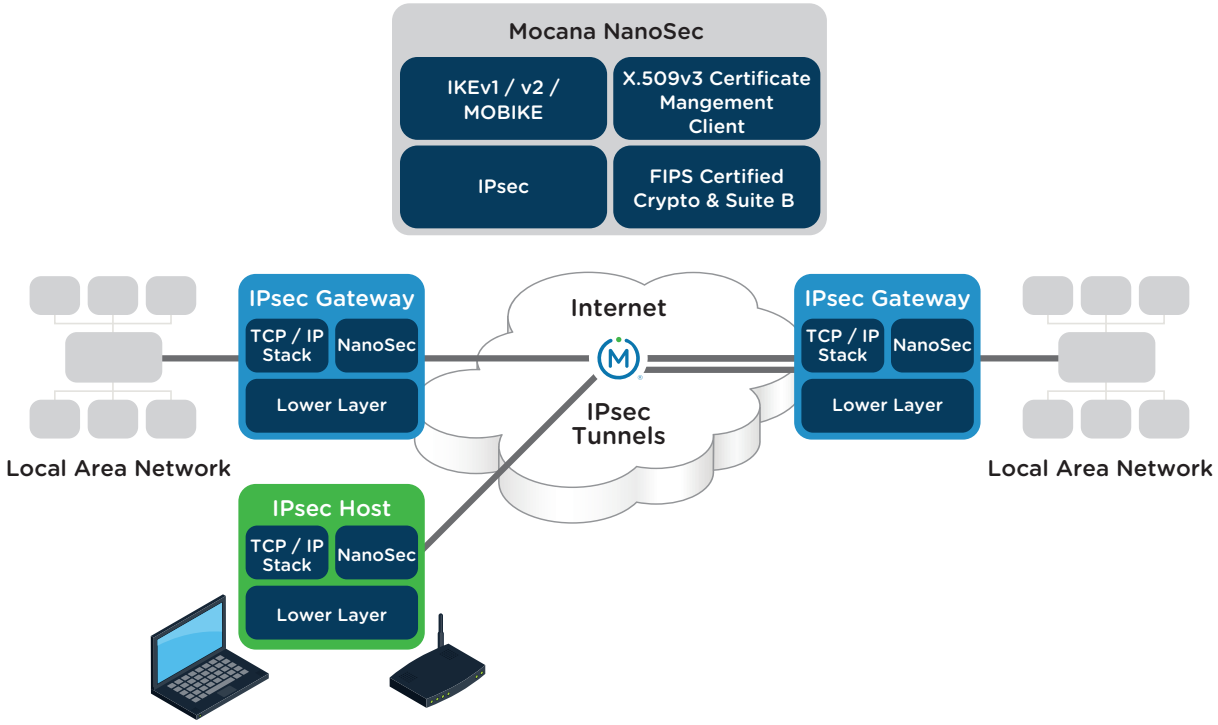


Figure 1. Mocana NanoSec Architecture

NanoSec Features

Mocana's NanoSec is an standards-based full featured and RFC-compliant IPsec toolkit. NanoSec is easy to use, uniquely architected with an asynchronous core to fully leverage hardware acceleration, is extremely portable and has an incredibly small memory footprint. It is ideally suited to securing voice, video and data communications. With NanoSec's integrated support for MOBIKE, the same security services can be extended to virtually any mobile device requiring VPN functionality.

NIST-Approved Suite B Crypto

NanoSec supports NIST-Approved Suite B crypto algorithms so your products can help link classified and unclassified government and civilian networks, securely.

NIST USGv6 Compliant

USGv6 is NIST's new specification for IPv6 devices and software intended for deployment inside the US Government. The profile is meant to define a minimal mandatory IPv6 capabilities set and identify significant configuration options so as to assist agencies in the development of more specific acquisition and deployment plans. This profile "raises the bar" for important areas of IPv6 technology, and Mocana's proud to be among the first to offer compliant solutions, like NanoSec.

Robust Certificate Management

NanoSec comes with an integrated certificate management client, because certificate-based authentication is a prerequisite for securely administering networked devices and services. Certificates need to be updated frequently to ensure the device is operated by the assigned user, that the device has the most updated user privileges, and that the device has the most recent upgrades in its service. Fortunately, Mocana makes embedding certificate management on devices easy, fast, and reliable. NanoSec supports SCEP based certificate Management client for fetching new certificate or renewing existing certificate used by IKE while setting up secured IPsec channel. Similarly with an OCSP client IKE can determine the revocation state of certificate in during this phase.

IETF RFC Compliance

- RFC-2367, PF_KEY Key Management API, Version 2
- RFC 2401/4301, Security Architecture for the Internet Protocol
- RFC-2402/4302, IP Authentication Header
- RFC-2403/4303, The Use of HMAC-MD5-96 within ESP and AH
- RFC-2404, The Use of HMAC-SHA-1-96 within ESP and AH
- RFC-2405/4305, The ESP DES-CBC Cipher Algorithm With Explicit IV
- RFC-2406/4306, IP Encapsulating Security Payload (ESP)
- RFC-2407, The Internet IP Security Domain of Interpretation for ISAKMP
- RFC-2408, Internet Security Association and Key Management Protocol (ISAKMP)
- RFC-2409, The Internet Key Exchange (IKE)
- RFC-2410, The NULL Encryption Algorithm and Its Use With IPsec
- RFC-3748, Extensible Authentication Protocol
- RFC-2451, The ESP CBC-Mode Cipher Algorithms
- RFC-3280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- RFC 3526, More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
- RFC-3566, The AES-XCBC-MAC-96 Algorithm and Its Uses With IPsec
- RFC-3602, The AES-CBC Cipher Algorithm and Its Use with IPsec
- RFC 3610, Counter with CBC-MAC (CCM)
- RFC 3686, Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)
- RFC-3706, A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers
- RFC-3715, IPsec-Network Address Translation (NAT) Compatibility Requirements
- RFC-3748, Extensible Authentication Protocol (EAP)

- RFC-3947, Negotiation of NAT-Traversal in IKE
- RFC-3948, UDP Encapsulation of IPsec ESP Packets
- RFC 4106: The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)
- RFC-4306, Internet Key Exchange (IKEv2) Protocol
- RFC 4307, Cryptographic Algorithms for Use in the Internet Key Exchange Version 2
- RFC 4308, Cryptographic Suites for IPsec
- RFC-4434, The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)
- RFC 4478, Repeated Authentication in Internet Key Exchange (IKEv2) Protocol
- RFC 4543, The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH
- RFC-4555, IKEv2 Mobility and Multihoming
- RFC-4718, IKEv2 Clarifications and Implementation Guidelines
- RFC 4739, Multiple Authentication Exchanges in IKEv2
- RFC 4753, ECP Groups for IKE and IKEv2
- RFC 4754, IKE and IKEv2 Authentication Using ECDSA
- RFC 4806, Online Certificate Status Protocol (OCSP) Extensions to IKEv2
- RFC 4835, Cryptographic Algorithm Implementation Requirements for ESP and AH
- RFC 4868, Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec
- RFC 4869, Suite B Cryptographic Suites for IPsec
- RFC 4894, Use of Hash Algorithms in Internet Key Exchange (IKE) and IPsec
- RFC 5685, Redirect Mechanism for the Internet Key Exchange Protocol Version 2 (IKEv2)
- RFC 5903, Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2)
- RFC 5998, An Extension for EAP-Only Authentication in IKEv2
- RFC 7383, IKEv2 Message Fragementation
- OCSP integrated with IKE for On Line Certificate Status check
- ModeConfig: draft-dukes-ike-mode-cfg-02.txt
- XAUTH: draft-ietf-ipsec-isakmp-xauth-6.txt

Certificate Management RFCs Supported

- IETF Draft: draft-nourse-scep-14.txt
- X.509 v3 certificate
- X.509 v2 CRL format
- RFC-2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
- RFC-2616, Hypertext Transfer Protocol -HTTP/1.1
- RFC-2617, HTTP Authentication: Basic and Digest Access
- RFC-3280, X.509 certificate and CRL profiles

Very Granular IKE/IPsec Feature Controls

- Complete control of AH and ESP protocols configuration
- Multiple concurrent instances for multi-homing, VLAN, per-interface, etc.

- Complete control of transport and tunnel modes
- Simple and complete control of shared secrets (IKE authentication)
- Complete control of IKE exchange
- Complete control of non-compliant security policy packets
- Full featured IKE implementation as initiator or responder
- IKE APIs to handle VendorIDs, customization of Initial Payload Exchange
- IKE APIs to set/retrieve information in XAUTH and ModeConfig interactions
- Support for Dead Peer Detection (DPD) and hooks for customization of DPD interactions.
- Supports Dual-Mode Operation (IKEv1 and IKEv2)
- Tight integration with Mocana NanoEAP
- Supports RSA tokens for EAP-GTC with IKEv2 (RFC 3748)

Rich Cryptography Algorithm Support

RANDOM NUMBER GENERATORS

- FIPS 186-2, General Purpose (x-change notice; SHA1)
- FIPS 186-2, Regular (x-change notice, k-change notice; SHA1)
- NIST SP 800-90, Random Number Generation Using Deterministic Random Bit Generators (DRBG) SYMMETRIC CRYPTO
- DES-56-CBC
- 3DES-168-CBC
- Blowfish—CBC
- AES-128-CBC
- AES-192-CBC
- AES-256-CBC

ASYMMETRIC CRYPTO

- RSA
- PKCS #1 v 1.5
- PKCS #7
- PKCS #8
- Diffie-Hellman Groups 1, 2, 5, 14, 24
- DHE with Perfect Forward Secrecy (PFS)
- ECDSA
- ECDH

SUITE B CRYPTO

- Suite-B-GCM-128
- Suite-B-GCM-256
- Suite-B-GMAC-128
- Suite-B-GMAC-256

SIGNATURES / AUTHENTICATION / INTEGRITY

- Certificate-based (X.509) authentication
- PKCS #10
- PKCS #12
- HMAC-SHA1-96
- HMAC-MD5-128
- HMAC-SHA1-160
- HMAC-MD5-96
- MD2
- MD4
- MD5
- SHA1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

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.

NanoSec Benefits

Works Where Others Won't

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

The Mocana Acceleration Harness for NanoSec is available for several popular platforms, offloading IPsec and IKE crypto operations from the main CPU and delivering 10x-30x performance enhancements. In fact, NanoSec is the highest performance IKE/IPsec package on the market.

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

GPL-Free Code

NanoSec is usually less expensive than "free" open source code, especially when engineering, testing and support costs are factored in. Since we guarantee that NanoSec 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.

Supported on a Variety of Platforms

NanoSec is available for many versions of Linux, Windows, VxWorks, ThreadX and QNX. If your platform isn't listed, give us a call, as this list changes frequently.

No Crypto Expertise Required

NanoSec features an extremely powerful, but simple and easy-to-use API. You don't need to be a crypto expert, because NanoSec hides all of the complexity of the cryptography. You can focus on your development project, and let NanoSec worry about the security. Plus Mocana's developer support team is always available to answer your questions about our products or embedded development in general.

Dramatically Speeds Your Development Cycle

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

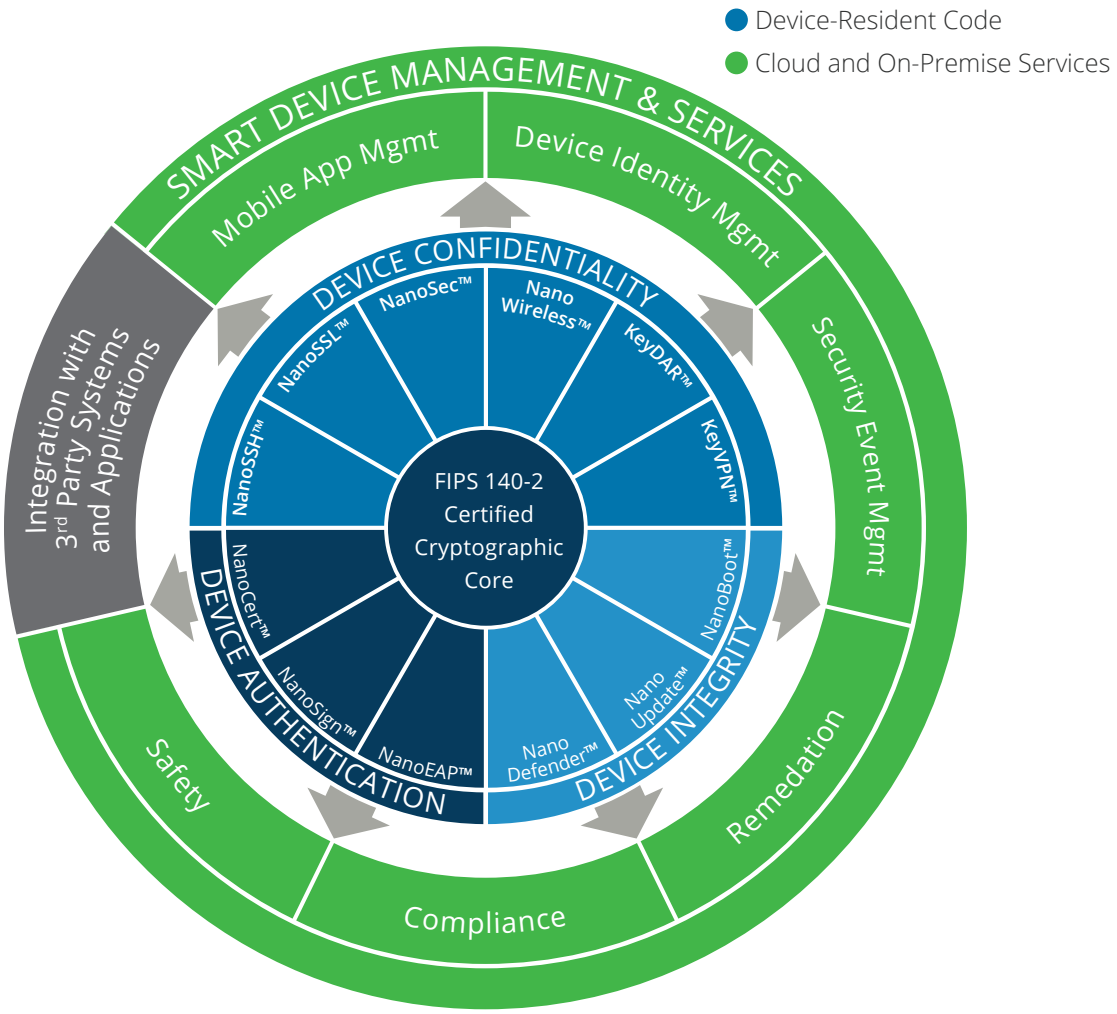
Which NanoSec Edition is Right for You?

Features	NanoSec Basic	NanoSec Advanced
IPsec Support	✓	✓
Suite B Support	✓*	✓*
FIPS Binaries Available	✓	✓
IKEv1 / v2 / MOBIKE Support	✓	✓
SCEP-based X.509 v3 Certificate Management	✗	✓
OCSP (On-Line Certificate Status Protocol) Checking	✗	✓
CRL (Certificate Revocation List) v2 Support	✗	✓

* Mocana Nano product editions are available with two options—with Suite B and without Suite B algorithms. Please contact **iotsales@mocana.com** for more details.

Mocana's Security of Things Platform

NanoSec 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.



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**

 Revised November 12, 2015