MOCANA

Security of Things Cloud Connectivity [NanoSSL™]

Mocana's comprehensive, standards-based SSL developers' suite, purpose-built for efficiency and high performance with support for TLS 1.2 and TLS certificate management.

Features & Benefits

- Small footprint, high performance
- FIPS 140-2 Level 1 validated (optional)
- Dramatically speeds integration & testing of SSL functionality
- NIST-Approved "Suite B" cryptography included
- Guaranteed "GPL-Free" code protects your intellectual property
- Zero-threaded, asynchronous architecture
- CPU, OS and transport-agnostic
- Fully documented with thousands of lines of sample code
- Expert development support from Mocana engineers

NanoSSL is Mocana's super fast, super small SSL / TLS solution specifically designed to speed product development while providing best-in-class device security services for resource-constrained environments. NanoSSL is open-standards-based, extensible, extremely small footprint, platform-agnostic and includes an optional government-certified FIPS 140-2 Level 1 validated crypto core. NanoSSL includes a full-featured key generator and certificate management client, and even supports Government Suite B crypto algorithms and the new RFC standard for TLS 1.2. Best of all it's surprisingly affordable: your NanoSSL total cost of ownership will usually be substantially less than that of open source.

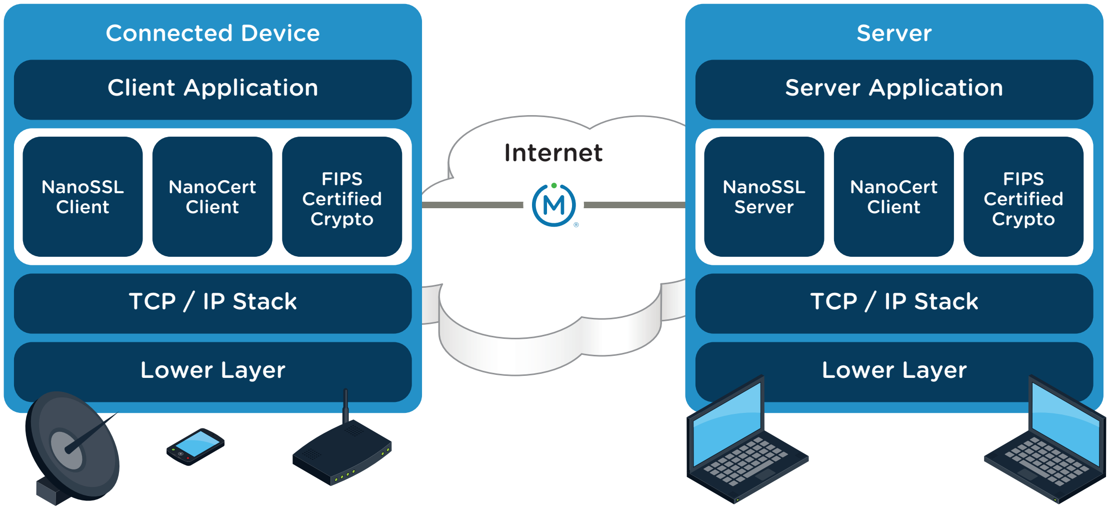
SSL and Device Environments

SSL/TLS (Secure Sockets Layer / Transport Layer Security) authenticates endpoints and encrypts channels to provide session privacy and security on the Internet. SSL operates at transport layer in the OSI stack and provides secured data transport to applications. It supports peer negotiation for algorithm selection, public key based exchange of secret session keys and X.509 certificates. SSL / TLS is the world's most widely-implemented security protocol.

Typically networking OEMs used SSL to provide secured management access to the devices like switches, routers, access points, DSL modems, etc. But with the "Internet of Things," several new types of devices are connected to IP networks—medical equipment, industrial sensors, smart grid devices, camcorders, and many other embedded devices. All of these devices need secured management access to transport data securely over the unsecured Internet.

NanoSSL is the answer.

NanoSSL provides easy to use APIs for integration with applications like web servers and browsers. Its certificate management module allows it to fetch or renew SSL certificates, check the status of SSL certificates using CRLs or to query a Certificate Authority (CA) or certificate chain.



NanoSSL Features

Mocana's NanoSSL is a standards-based full featured and RFC-compliant SSL / TLS client-server developer's suite. NanoSSL is easy to use, uniquely architected with an asynchronous core to fully leverage hardware acceleration, is extremely portable and has an ultra small memory footprint.

High Performance

NanoSSL, like all of Mocana's device security solutions, is designed with an asynchronous core to fully leverage hardware acceleration. NanoSSL throughput usually easily outperforms open source packages. Mocana's patented Acceleration Harness™, available for many popular hardware platforms, can boost NanoSSL's performance to 30x that of open source.

Ultra-Small Size

Highly modular, NanoSSL doesn't need a lot of memory. It has been optimized for stack and heap memory usage which makes it perfect for resource constrained environments. By just changing compile-time flags, you can build a NanoSSL client that fits in as little as 50KB of memory.

Government-Certified FIPS 140-2 Level 1 Cryptographic Engine (Optional)

The cryptographic engine at the heart of NanoSSL has undergone rigorous testing and government certification to assure that Mocana's cryptography is appropriate for the most sensitive applications. It's available to you in source code, or as a FIPS 140-2 Level 1 certified binary for many popular platforms.

IETF RFC Compliance

- RFC-1994, PPP Challenge Handshake Authentication Protocol (CHAP)
- RFC-2246, TLS Protocol Version 1.0
- RFC-2865, Remote Authentication Dial In User Service (RADIUS)
- RFC-2866, RADIUS Accounting
- RFC-3268, AES Ciphersuites for Transport Layer Security
- RFC-3280, Internet X.509 Public Key Infrastructure
- RFC-3546, Transport Layer Security Extensions (partially supported)
- RFC-3576, Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)
- RFC-4279, Pre-Shared Key Ciphersuites for Transport Layer Security
- RFC 4346, TLS 1.1
- RFC 4492: Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)
- RFC 5246: The Transport Layer Security (TLS) Protocol Version 1.2
- RFC 5288: AES Galois Counter Mode (GCM) Cipher Suites for TLS
- RFC 5289: TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)
- RFC 5430: Suite B Profile for Transport Layer Security (TLS)
- RFC 5746: Transport Layer Security (TLS) Renegotiation Indication Extension
- RFC 6066: Transport Layer Security (TLS) Extensions: Extension Definitions (Partially supported)
- RFC 6460, Suite B Profile for Transport Layer Security (TLS)
- Complete control over RADIUS server failover, including standby and round-robin configurations
- Multiple RADIUS Challenge-Response Authentication—ideal for SSH keyboard interactive authentication or token-based authentication.
- Support for multiple virtual instances of RADIUS
- Very high scalability

Rich Cryptography Algorithm / Construct Support

- DES
- 3DES
- AES -CBC
- AES-GCM
- Diffie-Hellman
- ECDH (NIST p-Curve 192, 224, 256, 384 and 521
- ECDSA (NIST p-Curve 192, 224, 256, 384 and 521)
- RSA
- PKCS #1, Version 1.5
- PKCS #5
- PKCS #7
- PKCS #8

- PKCS #10
- PKCS #12
- MD2
- MD4
- MD5
- SHA1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

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)

Extra-Flexible TLS Cipher Support

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_NULL_SHA
- TLS_ECDH_ANON_WITH_3DES_EDE_CBC_SHA
- TLS_ECDH_ANON_WITH_AES_128_CBC_SHA
- TLS_ECDH_ANON_WITH_AES_256_CBC_SHA
- TLS_ECDH_ANON_WITH_NULL_SHA
- TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDH_ECDSA_WITH_NULL_SHA
- TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDH_RSA_WITH_NULL_SHA
- TLS_PSK_WITH_3DES_EDE_CBC_SHA

- TLS_PSK_WITH_AES_128_CBC_SHA
- TLS_PSK_WITH_AES_128_CBC_SHA256
- TLS_PSK_WITH_AES_128_CCM
- TLS_PSK_WITH_AES_128_CCM_8
- TLS_PSK_WITH_AES_128_GCM_SHA256
- TLS_PSK_WITH_AES_256_CBC_SHA
- TLS_PSK_WITH_AES_256_CBC_SHA384
- TLS_PSK_WITH_AES_256_CCM
- TLS_PSK_WITH_AES_256_CCM_8
- TLS_PSK_WITH_AES_256_GCM_SHA384
- TLS_PSK_WITH_NULL_SHA256
- TLS_PSK_WITH_NULL_SHA384
- TLS_RSA_PSK_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_PSK_WITH_AES_128_CBC_SHA
- TLS_RSA_PSK_WITH_AES_128_CBC_SHA256
- TLS_RSA_PSK_WITH_AES_128_GCM_SHA256
- TLS_RSA_PSK_WITH_AES_256_CBC_SHA
- TLS_RSA_PSK_WITH_AES_256_CBC_SHA384
- TLS_RSA_PSK_WITH_AES_256_GCM_SHA384
- TLS_RSA_PSK_WITH_NULL_SHA256
- TLS_RSA_PSK_WITH_NULL_SHA384
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_DES_CBC_SHA
- TLS_RSA_WITH_NULL_MD5
- TLS_RSA_WITH_NULL_SHA
- TLS_RSA_WITH_NULL_SHA256

NanoSSL Benefits

Works Where Others Won't

NanoSSL 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 engines - a difficult certification to achieve. NanoSSL'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 SSL packages out there. But almost all of them are incomplete—missing critical standards, algorithms or code that you'll need to finish your SSL/TLS implementation. Only NanoSSL offers everything you need together in one package, to get the job done right—and fast. Guaranteed.

GPL-Free Code

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

NanoSSL, like all of Mocana's device security toolkits, is CPU-architecture and platform independent. NanoSSL 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 Micrium's uC/TCP-IP stack. NanoSSL is endian-neutral, and can be used without an RTOS if required.

No Crypto Expertise Required

NanoSSL features an extremely powerful, but simple and easy-to-use API. You don't need to be a crypto expert, because NanoSSL hides all of the complexity of the cryptography. You can focus on your development project, and let NanoSSL 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

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

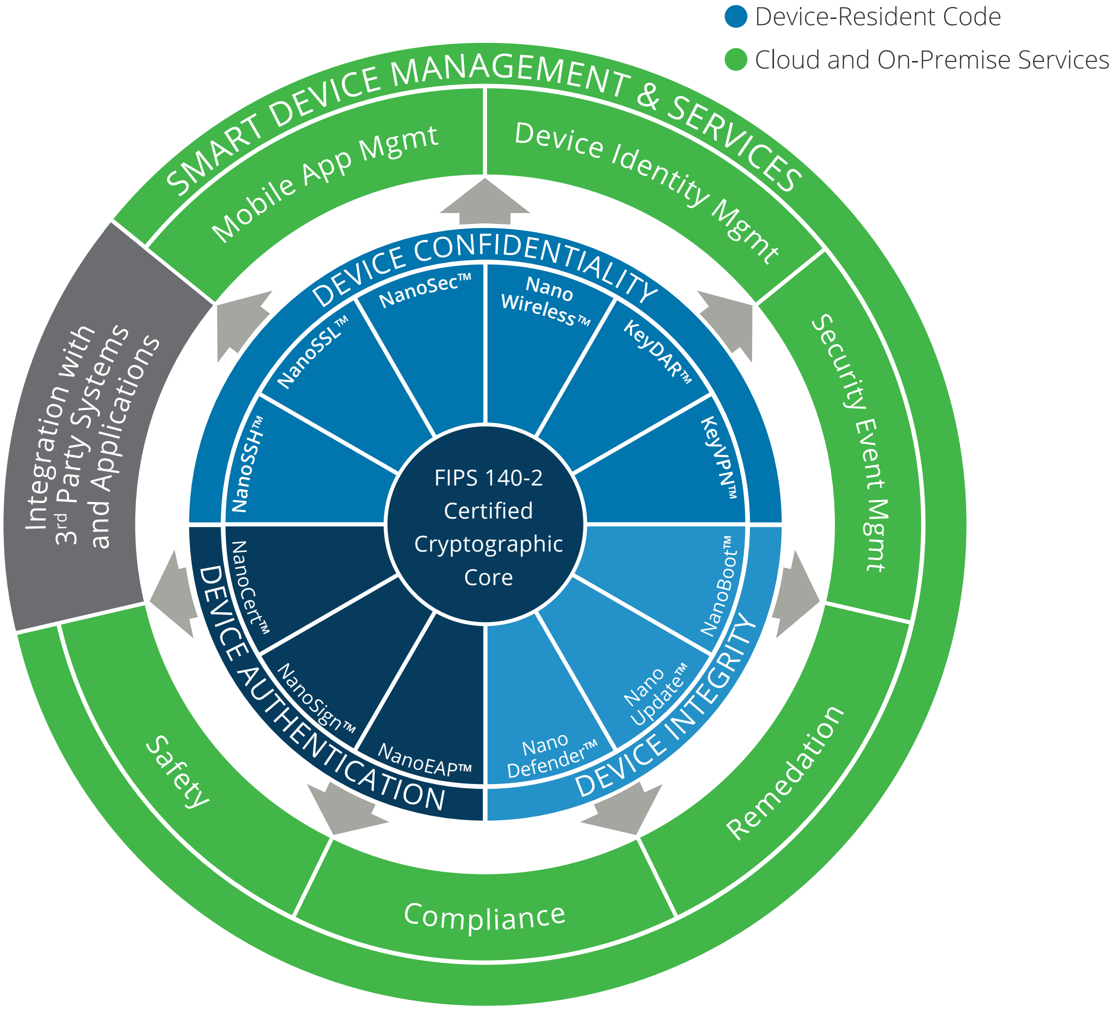
Which NanoSSL Edition is Right for You?

Features	NanoSSL Client	NanoSSL Server	NanoSSL Advanced	NanoSSL Freescale MQX™
SSL / TLS Client	✓	✗	✓	✓
SSL / TLS Server	✗	✓	✓	✗
Suite B Support	✓*	✓*	✓*	✗
FIPS 140-2 Level 1 Certified Cryptographic Engine Available (Binary)	✓	✓	✓	✓
X.509 v3 Certificate Management	✗	✗	✓	✗
SCEP Client	✗	✗	✓	✗
OCSP-Based Online Certificate Status Protocol Checking	✗	✓	✓	✗

* 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

NanoSSL 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