MOCANA

Security of Things Diagnostics [NanoSSH™]

Mocana's comprehensive SSH and RADIUS developers' suite, purpose-built for resource-constrained or high-performance device environments.

Features & Benefit

- Small footprint, high performance
- FIPS 140-2 Level 1 validated (optional)
- Complete solution includes certificate and RADIUS support that other packages lack
- 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
- RTOS neutral and transport agnostic
- Expert development support from Mocana engineers

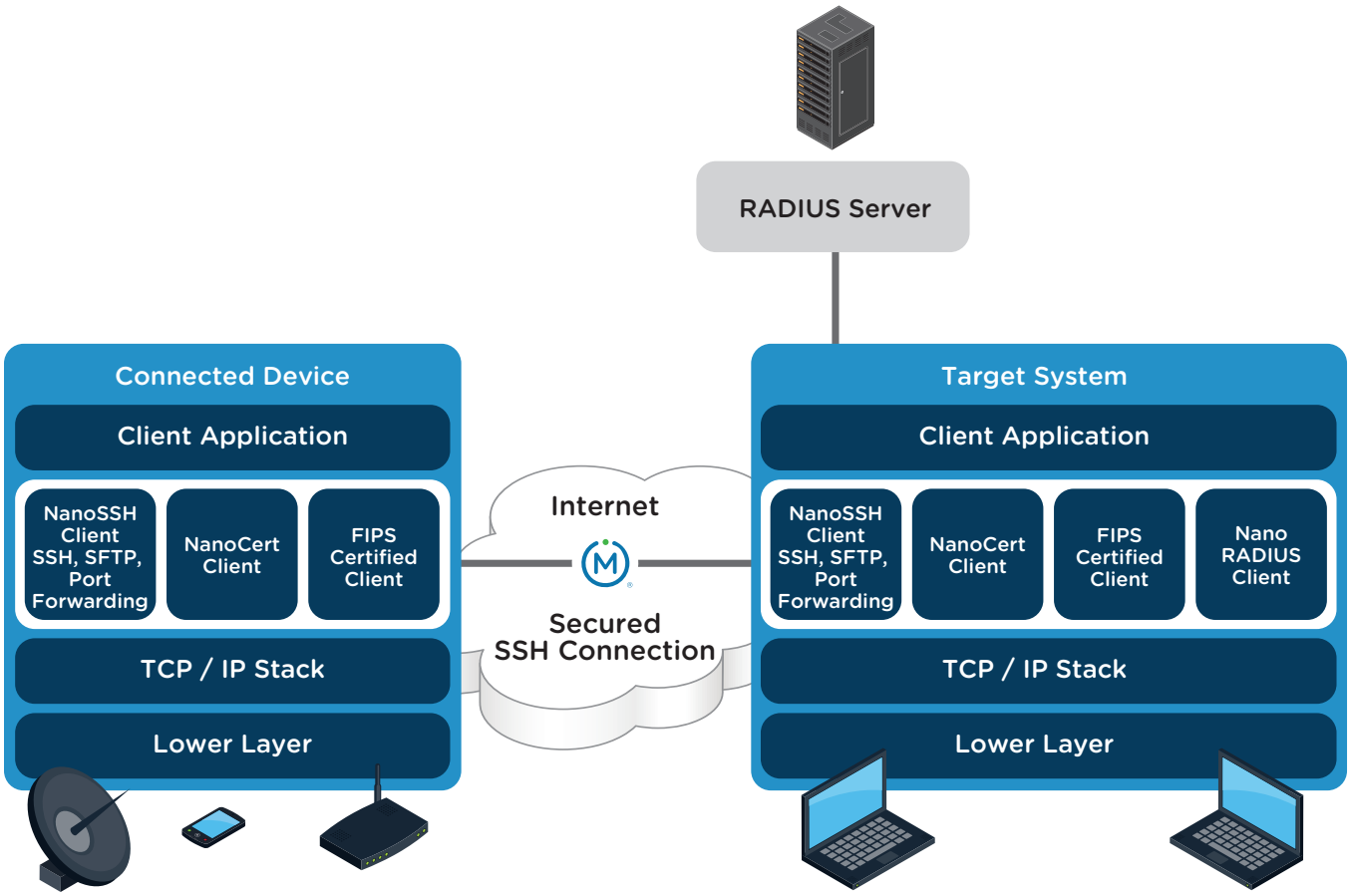
Secure Shell (SSH) encrypts communications between hosts over an insecure network, and it's great for logging into and executing commands remotely. It's also useful for port forwarding (sometimes called SSH Tunneling) which allows you to securely tunnel arbitrary TCP connections and for secure file transfers using the SFTP protocol.

Unfortunately, most SSH toolkits are designed for networked computers, not devices. That means that they can be somewhat unwieldy in memory-constrained device environments… and the performance of typical commercial or open-source SSH offerings can be pretty disappointing, as well.

NanoSSH is the answer.

NanoSSH is Mocana's super-fast, super-small SSH client/server solution with support for X509. v3 Certific9te based authentication and comes with RADIUS client, specifically designed to speed product development while providing best-in-class device security services for resource-constrained environments. It's royalty-free and surprisingly affordable: the NanoSSH total cost of ownership is almost always less than that of open source. NanoSSH provides a holistic approach for securing networked devices and services, and is ideally suited for resource-constrained devices as well as high-traffic eGMerprise and federal environments where performance is critical. NanoSSH is open-standards-based, extensible, extremely small footprint, platform-agnostic and features an optional government-certified FIPS 140-2 lo Level-1-validated crypto core. It even supports NIST-Approved

B crypto algorithms so your product can securely link civilian and classified government networks with a common cryptographic scheme.



NanoSSH Features

Mocana's NanoSSH secures communications between devices, or between a devices and a back-end SSH management console (or SFTP Server). The suite is a very small, very fast open standards-based solution that enables secure communications to any device on a network. The suite also includes a built-in client for RADIUS, aka Remote Authentication Dial In User Service. (RADIUS is often used in embedded devices in conjunction with SSH, because it eliminates the need to store sensitive user information (like passwords) locally on the device itself.) RADIUS is a "triple-A" protocol used for network access and mobility applications. The RADIUS client inside NanoSSH enables SSH to authenticate users with a central server, and log their access to systems or services.

Very High Performance

NanoSSH, like all of Mocana's device security solutions, is designed with an asynchronous core to fully leverage hardware acceleration. NanoSSH throughput typically outperforms open source packages by a factor of 2x or better, depending on the platform.

Ultra-Small Size

With its highly modular design, NanoSSH doesn't need a lot of memory. It's optimized for stack and heap memory usage and performs well in resource-constrained environments. Just by changing the compile time flags, you can build a NanoSSH client that fits in as little as 70KB memory. That's less than one-fifth the size of the typical open source client.

Government-Certified FIPS 140-2 Level 1 Cryptographic Engine

The cryptographic engine at the heart of NanoSSH has undergone rigorous testing and government certification to assure that Mocana's cryptography is appropriate for the most sensitive applications.

SSH IETF RFC Implementations Included:

- SSH File Transfer Protocol, v2, v3 and v4
- RFC 3447: Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications
- Version 2.1
- RFC-4250, The Secure Shell (SSH) Protocol
- Assigned Numbers
- RFC-4251, The Secure Shell (SSH) Protocol Architecture
- RFC-4252, The Secure Shell (SSH) Authentication Protocol
- RFC-4253, The Secure Shell (SSH) Transport Layer Protocol
- RFC-4254, The Secure Shell (SSH) Connection Protocol (partially supported)
- RFC-4344, The Secure Shell (SSH) Transport Layer Encryption Modes
- RFC 4335, The Secure Shell (SSH) Session Channel Break Extension
- IETF Internet-Draft draft-igoe-secsh-suiteb-00, Suite B Cryptographic Suites for Secure Shell
- draft-green-secsh-ecc-07: Elliptic-Curve Algorithm Integration in the Secure Shell Transport Layer
- draft-igoe-secsh-aes-gcm-02: AES Galois Counter Mode for the Secure Shell Transport Layer Protocol
- draft-igoe-secsh-suiteb-00: Suite B Cryptographic Suites for Secure Shell
- RFC 4419: Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol
- RFC 4432: RSA Key Exchange for the Secure Shell (SSH) Transport Layer Protocol
- RFC 6187: X.509v3 Certificates for Secure Shell Authentication

RADIUS Client and IETF RFC Implementations Included:

- Unlimited pending RADIUS requests (instead of the standard limit of 256)
- 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
- RFC-1994, PPP Challenge Handshake Authentication Protocol (CHAP)
- RFC-2865, Remote Authentication Dial In User Service (RADIUS)
- RFC-2866, RADIUS Accounting
- RFC-3576, Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)

Rich Algorithmic 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)

ASYMMETRIC CRYPTOGRAPHY

- RSA 1024-4096 bits
- RSA 1024-4096 bits host key
- RSA 1024-4096 bits key exchange
- Diffie-Helman Group 2, Group 14
- For Perfect Forward Secrecy (PFC), Ephemeral Diffie-Hellman using 1024-8192 bit key
- DSA/DSS 512-1024 bits per NIST specific tions
- ECDH for all P-curves (for Suite B)
- ECDSA for all P-curves (for Suite B)

SYMMETRIC CRYPTOGRAPHY

- AES128-CTR and CBC
- AES192-CTR and CBC
- AES256-CTR and CBC
- AEAD-AES-GCM-128 (Suite B)
- AEAD-AES-GCM-256 (Suite B)
- Blowfish 128-CBC
- 3DES-192-CBC

MESSAGE DIGEST

- HMAC-SHA1-96
- HMAC-SHA1-160
- HMAC-MD5-96
- HMAC-MD5-128
- AEAD-AES-GCM-128 (Suite B)
- AEAD-AES-GCM-256 (Suite B)

AUTHENTICATION

- NONE
- X.509v3 Certificates
- RSA Key Exchange
- DSA Public-Key
- Keyboard-interactive
- Password

NanoSSH Benefit

Works Where Others Won't

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

GPL-Free Code

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

NanoSSH, like all of Mocana's device security toolkits, is CPU-architecture and platform independent. NanoSSH 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. NanoSSH is endian-neutral, and can be used without an RTOS if required.

No Crypto Expertise Required

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

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

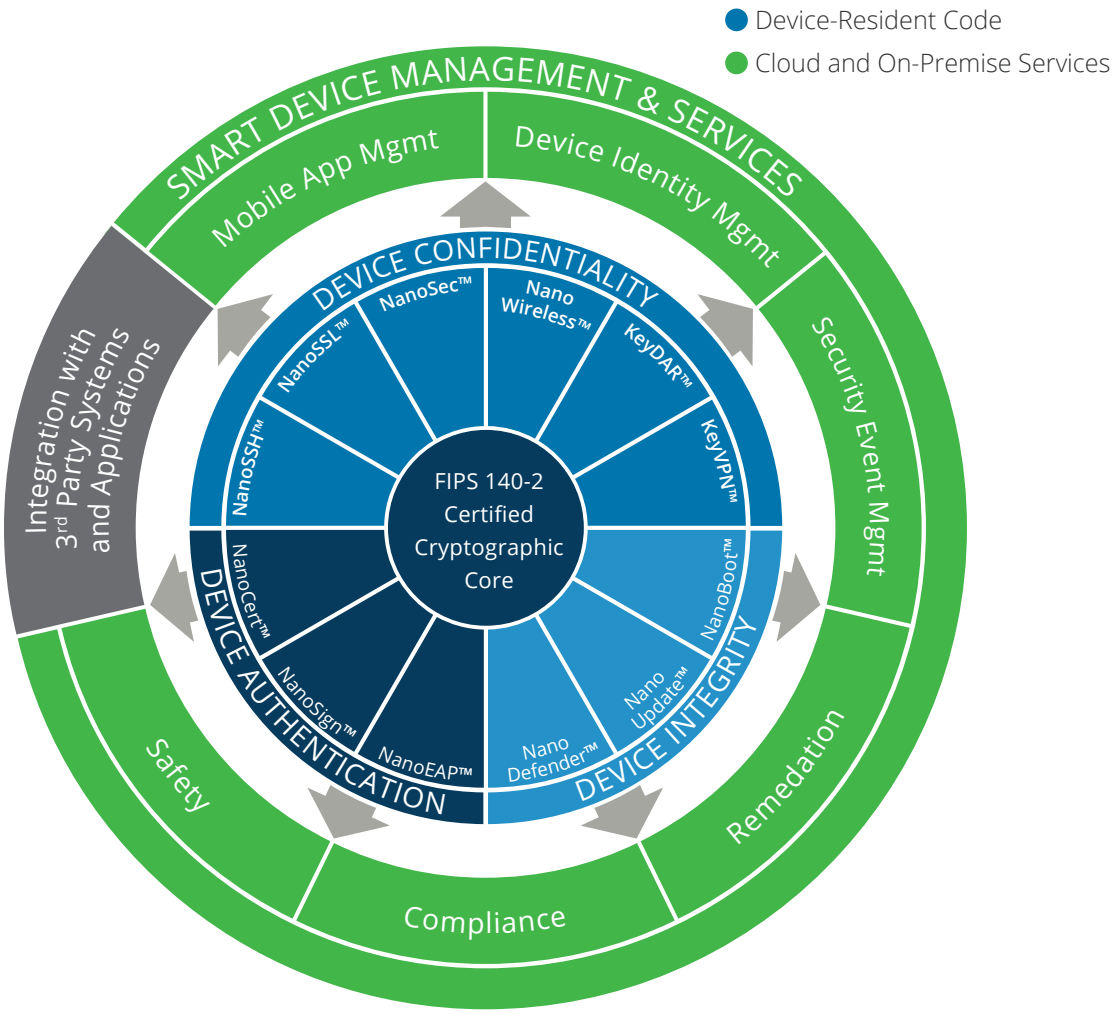
Which NanoSSH Edition is Right for You?

Features	NanoSSH Client	NanoSSH Server	NanoSSH Advanced	NanoSSH Freescale MQX™ RTOS
SSH Client	✓	✗	✓	✓
SSH Server	✗	✓	✓	✗
Suite B Support	✓*	✓*	✓*	✗
FIPS Binaries Available	✓	✓	✓	✓
X.509 v3 Certific te Management Client (SCEP)	✗	✗	✓	✗
On-Line Certific te Status Protocol Checking (OCSP)	✗	✗	✓	✗
RADIUS 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

NanoSSH 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