MOCANA SECURITY OF THINGS

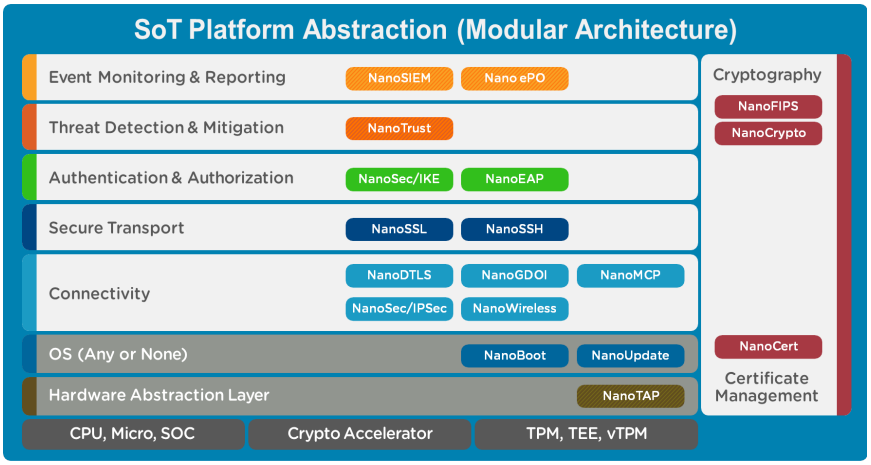
Mocana Security of Things Platform™

Features and Benefits:

- Share a common API and code base
- FIPS 140-2 Level 1 validated (optional)
- OS and CPU independent
- Guaranteed "GPL-Free" code protects your intellectual property
- Zero-threaded, asynchronous architecture
- Expert development support from Mocana engineers

Mocana Security of Things Platform™ (SoTP™) is designed to secure all aspects of any connected device. As a device designer, you can choose only the components you need for your particular project or standardize company-wide on the SoTP™, future-proofing your investment with this broad, cross platform, flexible and extensible security architecture.

*Patterned modules indicate future product



The Mocana Security of Things Platform comprises the following components:

NanoBoot- Provides all the tools and source code needed to perform pre-boot verification for firmware.

NanoCert- Security-centric embedded solution built around the Simple Enrollment Protocol (SCEP). NanoCert extends the SCEP protocol by automating the formerly manual administrative tasks of registering end entities, revoking certifications, and publishing CRLs (certificate revocation lists). Additionally, an OCSP client is included.

NanoCrypto- Government-certified cryptographic engine purpose-built for difficult and resource-constrained embedded system environments.

NanoSec- Provides data confidentially, integrity and authentication between networked peers at the IP layer. The NanoSec solution is uniquely architected with an asynchronous core to fully leverage hardware acceleration. It is ideally suited to securing voice, video and data networks.

NanoSSH- Fortifies CLI (command-line interface) management of connected embedded devices. Nano SSH provides a standards-based solution allowing secure CLI management of any device over any network.

NanoSSL- Provides endpoint authentication, protecting against eavesdropping, message forgery and interference. The client initiates connection to the server. Both are commonly used for securing remote device management via a web browser.

NanoUpdate- Securely delivers program updates and patches to devices over unsecure and unreliable networks (such as the Internet).

What You Need to Sucessfully Integrate Mocana Security

The user only needs to meet three requirements:

1. Development and target OS, CPU and toolchain
2. Understanding of C programming
3. Mocana sample code running on a reference platform (Linux)

What Does Mocana Test for?

- Performance
- Regressions
- Unit Testing
- Attack Testing
- FIPS 140-2 via NIST CAVP and CMVP
- Static Code Analysis via Klocwork
- Protocol fuzz testing via Codenomicon

About Mocana

Mocana provides high-performance, ultra-optimized, OS-independent, high-assurance security solutions for any device class. 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.

Contact Us

For more information on Mocana and our solutions, visit:

www.mocana.com

or please contact us at:

sales@mocana.com