MOCANA

Mocana NanoPNAC™

Device Admission Control over a wired interface

Security Features

- Single-threaded
- Leverages the FIPS 140-2 Level 1 certified NanoCrypto libraries
- Integration with NanoEAP™ and NanoSSL™ libraries for authentication methods and Communications
- Interoperability with 80211i compliant APs-Enterprise (IEEE 802.1X with EAP) over wired Interface
- Support for legacy security protocols (e.g. non-Enterprise authenticator)
- Authentication and control of IEEE 802.1X authentication using EAP methods
- Hardware/driver layer abstraction
- Support for ECDSA certificates
- Low memory footprint for resource constrained devices
- Linux and Free RTOS platforms
- Byte-efficient codebase that is smaller than open-source implementations
- Speeds integration and testing of complex cryptographic functions for your product
- No reliance on the open-source community libraries
- OS- and platform-agnostic for easy portability
- Guaranteed GPL-free code protects your intellectual property

Mocana® NanoPNAC™ (Port-Based Network Access Control) provides IEEE 802.1x EAP-TLS authentication over a wired Ethernet interface. Applications may then utilize the authenticated interface for network access.

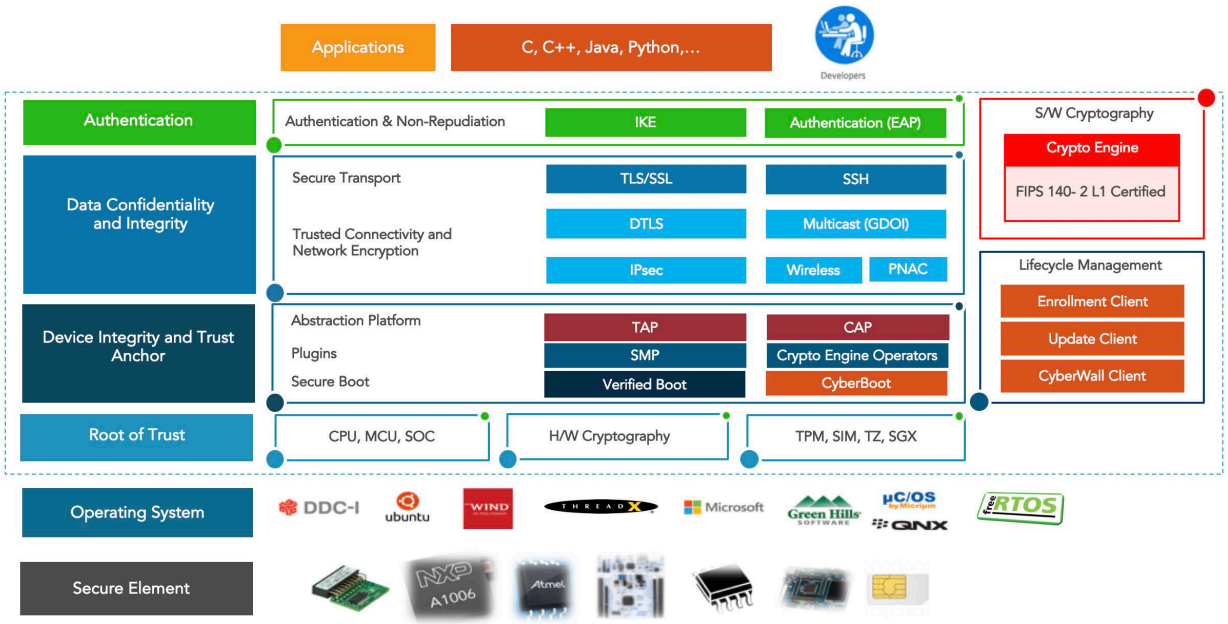
NanoPNAC provides the functionality required to develop an IEEE 802.1x compliant port-based network access supplicant for connectivity over a wired interface. The supplicant establishes a secure association with an authenticator and a AAA RADIUS server, and NanoPNAC enables certificate-based authentication over EAPOL. Additionally, NanoPNAC also manages legacy switches that do not support authentication and enables post-authentication network access to user applications.

NanoPNAC provides a platform independent abstraction layer for user space applications. The capabilities include a state machine to connect and authenticate with an authenticator using the Extensible Authentication Protocol (EAP) and cryptography for secure handshakes.

A major advantage of Mocana's solution is that it authenticates, or validates the identity of the device before it is allowed to communicate with the rest of the network. Unlike insecure network access methods such as unauthenticated Dynamic Host Configuration Protocol (DHCP) that provision network access before requiring authentication, Mocana's solution provides a secure method to use certificate-based, mutual machine-to-machine authentication, Mocana's solution provides a secure method to use certificate-based, mutual machine-to-machine authentication.

NanoPNAC is designed for embedded platforms. The reduced memory footprint, based on cipher suite, enables operation on resource constrained platforms.

Mocana TrustPoint™ Stack



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. For more information on Mocana and our solutions, please visit **www.mocana.com** or contact us at **sales@mocana.com.**

Mocana Corporation
111 W Evelyn Ave, Ste 210
Sunnyvale, CA 94086
tel (415) 617-0055 toll free (866) 213-1273
iotsales@mocana.com

