MOCANA

NANOEAP™

Mocana's open standards based, full-featured RFC compliant embedded EAP solution.

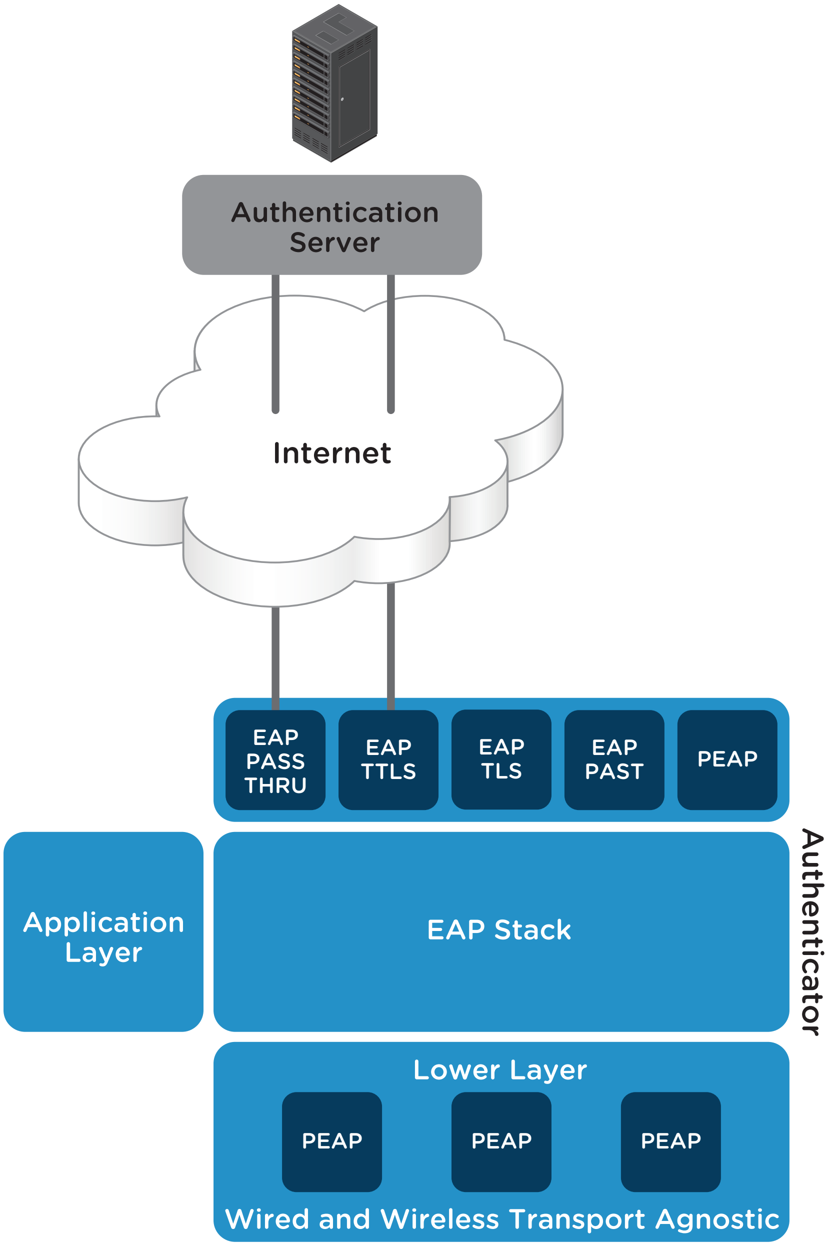
Features & Benefits

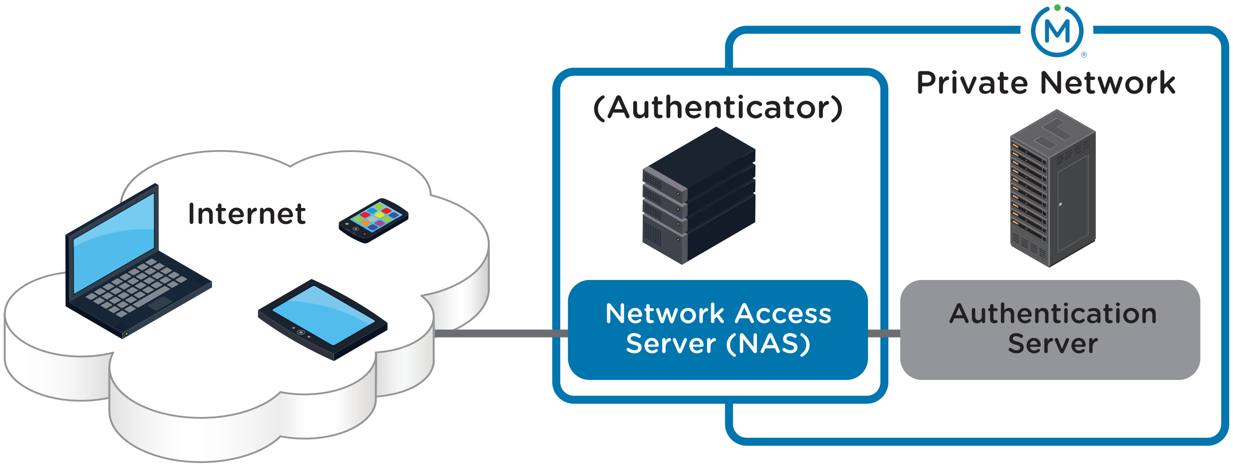
- Greatly speeds development cycle
- Open-standards, RFC compliant, full-featured
- Easy to install and use
- Source Code
- Code reuse for smaller memory footprint
- Advanced well-documented APIs
- Advanced cryptography support
- RTOS neutral and transport agnostic
- High performance zero-threaded, asynchronous architecture

Mocana delivers and open standards based, full featured, RFC compliant embedded EAP solution. The Mocana NanoEAP solution offers a complete peer (supplicant) as well as an authenticator that can support pass-through mode and stand-alone mode. Both the supplicant and the authenticator(s) are available individually or as a bundle. The Mocana NanoEAP solution can prevent unauthorized access to your network devices, easily update your security handling, and independently manage multiple users who require unique security configurations. Separate VLANs can be served by separate EAP instances. Upper-layer APIs enable session creation, initialization, and statistics collection. Lower-layer APIs enable EAP communication over PPP, UDP, or any other protocol.

The NanoEAP model contains the following elements:

- The peer (supplicant) is the device that needs to connect to the network.
- The network access server, NAS (also known as the edge device) controls access to the network.
- The authenticator acts in either stand-alone mode to authenticate the peer (in two-tier authentication models) or in pass-through mode to transmit messages between the peer and an authentication server (in three-tier authentication models).
- The authentication server contains the data and logic, such as user names, passwords, and access rights, to make decisions about what services a peer is authorized to use.


Authentication Server
Internet
EAP PASS THRU
EAP TTLS
EAP TLS
EAP PAST
PEAP
Application Layer
EAP Stack
Authenticator
Lower Layer
PEAP
PEAP
PEAP
Wired and Wireless Transport Agnostic


Private Network
(Authenticator)
Internet
Network Access Server (NAS)
Authentication Server

NanoEAP™ Features

Ease of Control

Mocana NanoEAP provides system administrators complete control of authentication configuration—deciding when supplicants should be authenticated, how to handle connectivity loss, adding new authentication methods, and more. This flexibility is easily achieved using common configuration templates as models for customization.

Platform Independent

NanoEAP, like all of Mocana's device security toolkits, is CPU-architecture and platform independent, working with any TCP/IP stack. It works seamlessly out of the box. Platforms supported out-of-the-box include Linux, Monta Vista Linux, VxWorks, OSE, Nucleus, Solaris, ThreadX, Windows, MacOS X, (ARC) MQX, pSOS, and Cygwin. NanoEAP is endian-neutral, and can be used without an RTOS if required.

IETF Compliant Implementations

- RFC-2284, PPP Extensible Authentication Protocol (EAP)
- RFC-2716, PPP EAP TLS Authentication Protocol
- RFC-2759, Microsoft PPP CHAP Extensions, Version 2
- RFC-2945, The SRP Authentication and Key Exchange System
- RFC-3268, AES Ciphersuites for Transport Layer Security
- RFC-3546, Transport Layer Security Extensions (partially supported)
- RFC-3579, RADIUS (Remote Authentication Dial In User Service) Support for Extensible Authentication Protocol (EAP)
- RFC-3580, IEEE 802.1x Remote Authentication Dial In User Service (RADIUS) Usage Guidelines
- RFC-3748, Extensible Authentication Protocol (EAP)
- RFC-4137, State Machines for Extensible Authentication Protocol (EAP) Peer and Authenticator
- RFC-4186, Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)
- RFC-4187, Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)
- RFC-4279, Pre-Shared Key Ciphersuites for Transport Layer Security
- EAP-PEAP (v0, v1, v2), all drafts-draft-josefsson-pppext-eap-tls-eap-07.txt and draft-josefsson-pppext-eap-tla-eap-10.txt
- EAP-TTLS (v0,v1), all drafts-draft-ietf-pppext-eap-ttls-02.txt
- EAS PSK draft-draft-bersani-eap_psk-11.txt
- EAP FAST draft-draft-cam-winget-eap-fast-03.txt

Authentication Support

- OTP (one time password)
- GTC (generic token card), supports RSA tokens for IKEv2 (RFC 3748)
- MS-CHAP-V2 (Microsoft version of the Challengehandshake authentication protocol)
- TLS (transport layer security)
- TTLS v0 and v1 SIM (subscriber identity module)
- AKA (authentication and key agreement)
- SRP (secure remote password)
- LEAP (lightweight extensible authentication protocol, developed by Cisco Systems)
- PEAP v0/v1/v2 (protected extensible authentication protocol)
- FAST (flexible authentication via secure tunneling)
- RADIUS (remote authentication dial in user service)
- MD5

EAP-TLS and EAP-TTLS Cipher Support

- TLS_DH_ANON_WITH_3DES_EDE_CBC_SHA
- TLS_DH_ANON_WITH_AES_128_CBC_SHA
- TLS_DH_ANON_WITH_AES_256_CBC_SHA
- TLS_DH_ANON_WITH_ARCFOUR _128_MD5
- TLS_DH_ANON_WITH_DES_CBC_SHA
- TLS_DH_ANON_WITH_AES_128_CBC_SHA256
- TLS_DH_ANON_WITH_AES_256_CBC_SHA256
- TLS_DHE_PSK_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_PSK_WITH_AES_128_CBC_SHA
- TLS_DHE_PSK_WITH_AES_256_CBC_SHA
- TLS_DHE_PSK_WITH_ARCFOUR_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_DES_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_PSK_WITH_3DES_EDE_CBC_SHA
- TLS_PSK_WITH_AES_128_CBC_SHA
- TLS_PSK_WITH_AES_256_CBC_SHA
- TLS_PSK_WITH_ARCFOUR_128_SHATLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_ARCFOUR_128_SHA
- TLS_RSA_WITH_ARCFOUR_128_MD5
- TLS_RSA_WITH_DES_CBC_SHA
- TLS_RSA_WITH_NULL_MD5
- TLS_RSA_WITH_NULL_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256

Additional Cryptography Support

- MD2
- MD4
- MD5
- PKCS #1, Version 1.5
- PKCS #5
- PKCS #7
- PKCS #8
- PKCS #10
- PKCS #12
- SHA1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

NanoEAP Features

- Transport agnostic with no dependacy on link layer (EAP packets can be transported over 802.1x, PPP, TCP, UDP and IKEv2).
- Highly customized for various timeouts, retransmission intervals and MTU configurations.
- EAP session can be configured as supplicant, stand-alone authenticator or Pass-through Authenticator.
- Each EAP session can be configured to use different EAP method.
- APIs to gather statistics and logs.
- Support for multiple virtual instances of EAP authenticator.
- Easy to integrate as a library in the existing task or a process.

Note: Mocana Device Security Framework (DSF) products are highly portable across 35+ Operating Systems (OS) and all major processor architectures. Some Mocana DSF 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.

NanoEAP™ Benefits

Speed

NanoEAP consistently outperforms. NanoEAP's assembly language optimization and support for hardware acceleration make it the fastest embedded EAP implementation on the market. Benchmark testing on a 700 MHz Pentium III CPU with Embedded EAP-SIM, Embedded EAP peer running on Linux, and Mocana NanoEAP authenticator in RADIUS pass-through mode with 100 sessions/sec yielded only a two percent CPU utilization rate. It includes strong code reuse for a smaller memory footprint.

Flexibility

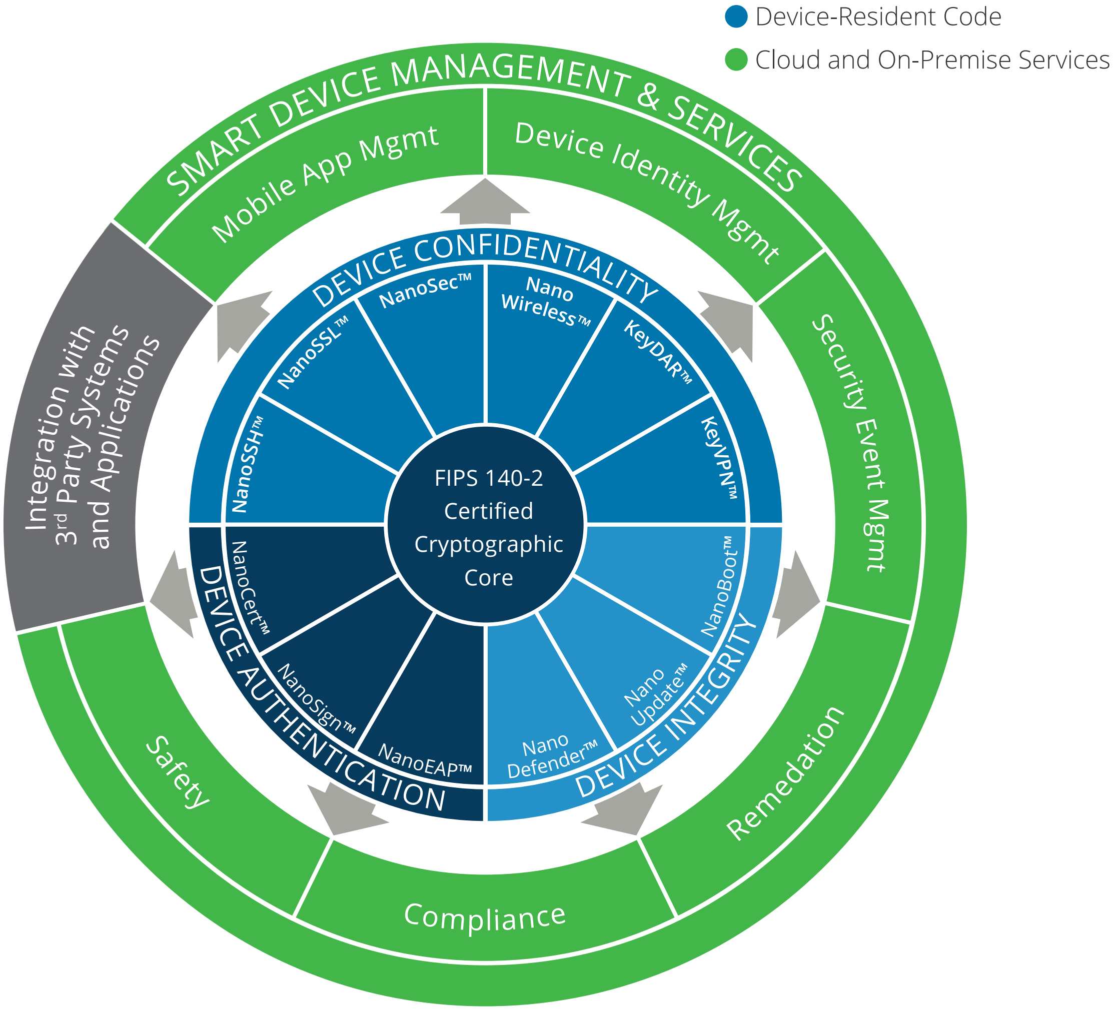
Mocana NanoEAP delivers incredible flexibility, as it is able to support multiple authentication schemes, including generic token cards, one-time passwords, AKA, TLS, RADIUS, LEAP and many others. You get to determine where supplicants should be authenticated as well as easily add new authentication methods. It's a snap to independently manage multiple users who require unique security configurations.

Dramatically Speeds Your Development Cycle

NanoEAP is a ready-made, pre-optimized and exhaustively tested EAP solution that frees your in-house development resources to focus on what's really important: the functionality of your project. As well, NanoEap is cleared for export. As always, Mocana's developer support team is available 24/7/365 to help you anytime.

Mocana's Device Security Framework™

NanoBoot is part of the Mocana Device Security Framework™ (DSF™), designed to secure all aspects of any connected device. All components of the Device Security Framework 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 DSF, future-proofing your investment with this broad, cross platform, flexible and extensible security architecture.



About Mocana

Mocana securely mobilizes enterprise data and protects millions of the smart connected devices that comprise the Internet of Things. The company's award-winning enterprise mobile app security platform provides organizations with an easy way to deliver business-critical mobile apps, with a high-quality end user experience, tap-and-go simplicity and strong security, for internal and external users. Mocana's customers include Fortune 50 enterprises, government agencies and the world's leading smart device manufacturers. More information is available at **www.mocana.com**.

Awards and Certificates

RED HERRING GLOBAL WINNER 100
SECURITY Innovation Network SINET Top 16 Winner
WORLD ECONOMIC FORUM Technology Pioneer 2012
Gartner 2012 CoolVendor
FIPS VALIDATED 140-2
VPNC CERTIFIED IPv6 Interop
CW 2014 100
FROST & SULLIVAN 2008 BEST PRACTICES AWARD
GG3 Tech Choice 2008
Tomorrow's Technology Today AWARDS 2008 Info Security Products Guide
IPSO Alliance

Mocana Corporation
710 Sansome Street
San Francisco, CA 94111
tel (415) 617-0055 toll free (866) 213-1273
www.mocana.com **sales@mocana.com**

TRIDENT CAPITAL

Mocana is Part of the Trident Portfolio