



Embeddable 802.1AE and 802.1X-REV
(formerly 802.1af)
implementations for any environment

BENEFITS

- Complete MACsec, Authentication, and Key Management Implementations
- Build a wide range of products: Bridges, Routers, Hosts
- Scalability, Reliability and Interoperability
- IEEE Standards Based Solution
- Hardware IP and Toolkit Available from a Single Vendor
- Small Footprint and Deterministic Memory Allocation
- Future proof - The MACsec/QuickSec Toolkit keeps up with the Evolving Standards
- Reduced Development Cost
- Bring Product to Market Fast
- Worldwide OEM Customer Support
- Rely on AuthenTec's Security Experts

Equipment developers and vendors are driven by regulation to build secure networking solutions and to solve compliance requirements.

The QuickSec/MACsec Toolkit enables developers to embed MACsec capabilities in to new and existing products. QuickSec/MACsec is suitable for Ethernet bridges, routers, and hosts. QuickSec/MACsec is the first security toolkit in the market to support this new Ethernet security standard. This toolkit is highly portable, well documented and commented ANSI C source code suitable for a wide range of platforms.

Complete MAC Security Solution

MACsec specifies how all or part of a LAN network can be transparently secured. MAC Security provides connectionless user data confidentiality, frame data integrity, and data origin authenticity. The MACsec security architecture composes two main components, an authenticated key agreement protocol defined in 802.1X-REV, and a data plane protocol which protects frames transmitted on the LAN know as MACsec.

Conform to the Latest Standards

QuickSec/MACsec provides a source code toolkit that implements the security functionality defined in IEEE standards 802.1X, 802.1AE, and 802.1X-REV (formerly 802.1af).

The enduring AuthenTec commitment to the security market and its standardization assure that the QuickSec/MACsec implementation stays current with these complex and evolving standards that are the foundation for building Layer 2 security solutions.

AuthenTec's experience and participation in the field of security protocol standardization (in the IETF, IEEE and other organizations) guarantees that our customers always have a head-start in the new developments of security standards.

Hardware and Software Support

The QuickSec/MACsec toolkit includes an optimized software implementation of AESGCM and 802.1AE transforms. The toolkit provides a well-defined API for interfacing between the hardware and software components, allowing for simple integration with third party hardware. QuickSec/MACsec is pre-integrated with AuthenTec's SafeXcel IP cores including the EIP-38 AES-GCM IP core, the EIP-60 look-aside MACsec security engine, and the EIP160 in-line MACsec security engine. The solution supports speeds scaling beyond 40Gbps.

Benefits of a SW/HW Combination

MACsec solution offers an entire and functional software implementation of the protocol core and key management functionality our customers are able to test, simulate, and prototype their solutions early (even before the actual hardware is taped off) and reach their markets quickly, with less development cost, while significantly reducing risk.

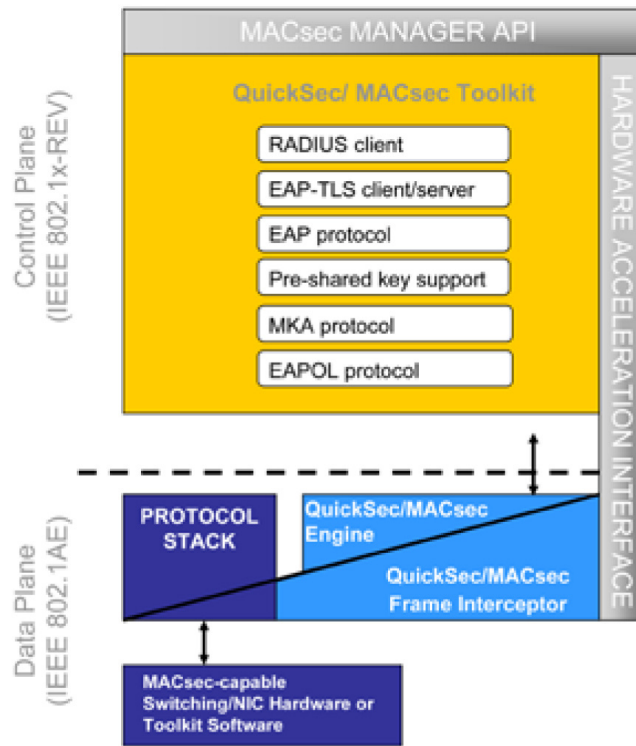
Layer 2 & Layer 3 Security

QuickSec/MACsec is part of the industry leading QuickSec family of products. QuickSec/ IPsec is the world's foremost IPsec toolkit. Combining the MACSec and IPsec toolkits in a single product provides total wired security at layer 2 and 3, and provides the possibility of leveraging the common XML policy management interface, as well as the EAP, TLS, and cryptographic libraries of the QuickSec product family.



AuthenTec OEM Security Solutions

AuthenTec's comprehensive security systems are deployed by the world's leading networking OEMs, including AMCC, AMD, Cisco Systems, Hitachi, HP, Juniper Networks, Lucent Technologies, PMC-Sierra, Samsung, Siemens, and Texas Instruments, to name a few. The leading global semiconductor, telecommunications, enterprise, and wireless OEMs trust AuthenTec's best-in-class security solutions for their next-generation networking solutions.



SPECIFICATIONS

Complete Software Implementation	Standards Compliance
<ul style="list-style-type: none"> 802.1X-REV. The implementation follows the version 2.0 of the draft 802.1X-REV. The toolkit will continue to support draft updates through to the final version 802.1AE with AES-GCM cipher Pre-shared keys or EAP for key management EAP-TLS, other methods available on request 	<ul style="list-style-type: none"> IEEE 802.1AE IEEE 802.1X-REV IETF RFC 3748 - EAP IETF RFC 2716 - EAP-TLS IETF RFC 2865 - RADIUS IETF RFC 2459 - X.509 IETF RFC 3280 - CRL Profile IETF RFC 4346 - TLS 1.1
<ul style="list-style-type: none"> API's for interfacing to hardware 802.1AE implementations API's for policy configuration and management XML based policy configuration RADIUS AES-GCM 	Pre-integrated with SafeNet IP <ul style="list-style-type: none"> EIP-38 - AES-GCM EIP-60 - Look-aside Packet Engine EIP-160 - In-Line Packet Engine

HEADQUARTERS

AuthenTec, Inc.
100 Rialto Place, Suite 100
Melbourne, FL 32901 USA
+1-321-308-1300

For more information on
Embedded Security Solutions
Email us at:
embedded@authentec.com

WORLDWIDE REPRESENTATIVES NETWORK

A complete listing of
AuthenTec's network of
representatives is
available at our web site.

www.authentec.com

