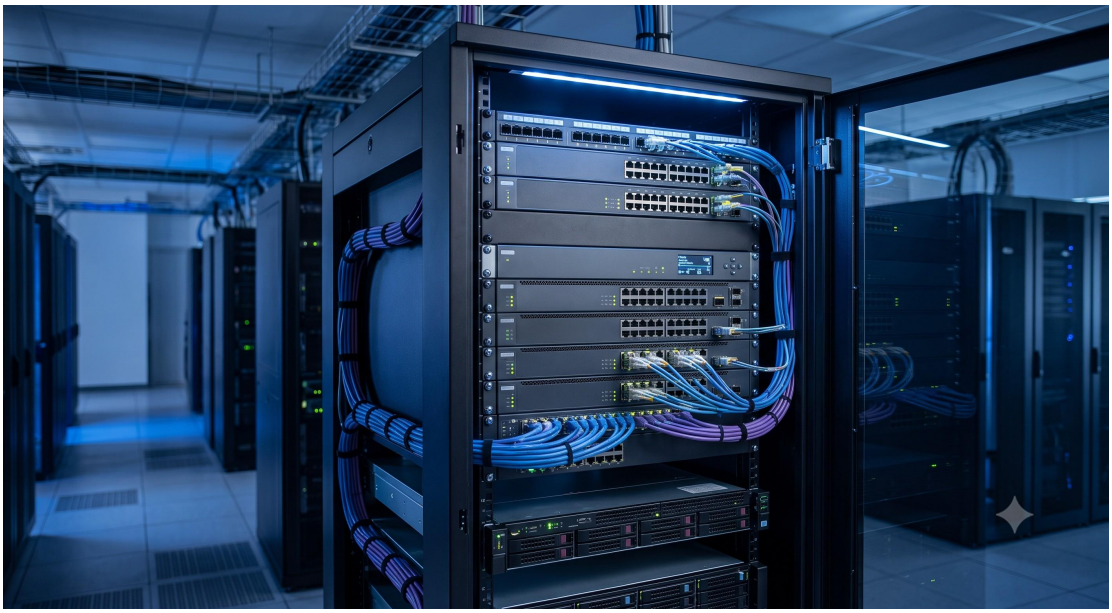
MACsec Encryption Implementation Guide - Official Technical Overview & Hardware Datasheet

EXECUTIVE SUMMARY

The relentless proliferation of high-speed data traffic and the escalating sophistication of cyber threats have rendered perimeter-only security models obsolete. Modern network infrastructures, particularly in carrier-grade, enterprise edge, and data center interconnect environments, require pervasive, line-rate encryption that protects data in motion across the entire physical and link layers. MACsec (Media Access Control Security), defined by the IEEE 802.1AE standard, addresses this critical requirement by providing point-to-point security on Ethernet links, ensuring data confidentiality, integrity, and origin authenticity between directly connected devices.

This document serves as the authoritative technical overview and hardware datasheet for the [COMPANY NAME] portfolio of MACsec-enabled switching and routing platforms. It details the hardware architecture, encryption performance, implementation frameworks, and compliance specifications essential for network architects, security engineers, and procurement specialists. The solutions outlined herein are engineered to deliver industry-leading, line-rate MACsec encryption without compromising forwarding performance, scalability, or operational simplicity, seamlessly integrating into existing

network management ecosystems and supporting a spectrum of deployment scenarios from enterprise access to high-density core routing.



ARCHITECTURE & CHASSIS DESIGN

The [COMPANY NAME] MACsec implementation is built upon a purpose-designed, programmable forwarding ASIC architecture that integrates hardware-accelerated encryption engines directly into the data path. This design philosophy ensures that MACsec encapsulation and decapsulation, along with the associated cryptographic operations (AES-GCM 128/256), occur at wire speed, introducing negligible latency (typically sub-100 nanoseconds) and zero performance degradation, regardless of packet size or line rate.

The system architecture is stratified into distinct functional planes to guarantee

high availability, resilient operation, and seamless management.

1. DATA PLANE (Forwarding & Encryption Engine):

The heart of the system is the Secure Forwarding Engine (SFE), a dedicated hardware block per physical port or port-group. The SFE performs parallel processing of ingress and egress packets. Key functions include:

- MACsec Frame Header Processing: Insertion and removal of the 8-byte MAC Security Tag (SecTAG) and 16-byte Integrity Check Value (ICV).

- Cryptographic Acceleration: Dedicated AES-GCM cores for encryption and decryption at rates up to 400 Gbps per chip, enabling line-rate throughput on all 100GE, 40GE, and 10GE interfaces.

- Secure Association Management: Hardware-based lookup tables (SAKs, SAs) supporting up to 64K concurrent secure associations, enabling secure connectivity in complex, multi-tenant environments.

2. CONTROL PLANE (Management & Key Negotiation):

The control plane is managed by a high-performance CPU complex running a hardened Linux-based operating system (OS). Its primary responsibilities include:

- Protocol Processing: Full support for the MACsec Key Agreement (MKA) protocol as defined in IEEE 802.1X-2010 and 802.1AE, using EAPoL (Extensible Authentication Protocol over LAN) frames for dynamic key derivation and

distribution.

- System & Security Management: Integration with RADIUS/TACACS+ for AAA, SSHv2 for secure CLI access, SNMPv3 for monitoring, and NETCONF/YANG for programmable automation. It also manages the secure storage and lifecycle of pre-shared keys (CAK, CKN) or certificates.

- High-Availability Synchronization: Stateful synchronization of MKA state and security associations between active and standby control modules in redundant configurations, ensuring sub-second failover of encrypted links.

3. MANAGEMENT PLANE (Operations, Administration, and Maintenance - OAM):

This plane provides the tools and interfaces for network operators to deploy, monitor, and troubleshoot MACsec-enabled services. It features a comprehensive set of telemetry and diagnostic capabilities, including:

- Per-port MACsec counters for encrypted/decrypted frames, replay errors, and integrity violations.

- Active and passive performance monitoring (IEEE 802.1ag, ITU-T Y.1731) over secured links.

- Integration with centralized network management platforms for unified visibility and policy control.

HARDWARE FEATURES

The MACsec solution is offered across a versatile range of hardware platforms, from compact fixed-configuration devices to modular, high-capacity chassis systems. This ensures that the same robust security framework can be applied consistently from the network edge to the core.

- MODULAR CHASSIS SYSTEMS: Designed for high-density carrier core and data center spine environments, these platforms support multiple slots for various line cards.

* Line Card Support: Dedicates line cards to provide 48 x 10GE SFP+, 48 x 25GE SFP28, or 36 x 100GE QSFP28 ports, all with hardware-accelerated MACsec. This allows for granular, pay-as-you-grow scalability.

* Fabric Redundancy: The system uses a fully redundant, non-blocking switch fabric architecture with N+1 fabric module redundancy for continuous operation.

* Power Redundancy: Supports up to N+N (AC or DC) power supply units (PSUs) for highest availability.

- FIXED-CONFIGURATION SWITCHES: Optimized for enterprise campus, data center ToR (Top-of-Rack), and edge aggregation. Offered in 1RU and 2RU form factors.

* Port Flexibility: Available with 24 to 48 ports of 10GE/25GE SFP+/SFP28

and 4 to 8 ports of 40GE/100GE QSFP/QSFP28 uplinks. All ports are MACsec-capable at line rate.

* Fan Redundancy: Hot-swappable, redundant fan trays with port-to-power or power-to-port airflow options to suit data center hot/cold aisle configurations.

* PSU Options: Field-replaceable AC or DC PSUs with 1+1 redundancy.

- RUGGEDIZED & OUTDOOR PLATFORMS: For deployment in harsh environments, such as base stations, roadside cabinets, and industrial networks.

* Extended Temperature Range: Operates reliably from -40°C to +75°C (-40°F to +167°F).

* Conformal Coating: All PCBs are coated for protection against moisture, dust, and corrosion.

* Fanless Design: Employ passive cooling for high reliability and silent operation.

COMPLIANCE & STANDARDS

The MACsec implementation strictly adheres to the relevant IEEE standards, ensuring interoperability with any standards-compliant networking equipment. Rigorous compliance testing is performed across all platforms and interface types.

- IEEE 802.1AE-2018 (MACsec): Core standard for link-layer encryption.

- IEEE 802.1X-2010 (Port-Based Network Access Control): Defines the use of EAPoL for MKA.

- IEEE 802.1AEbn-2011 (GCM-AES-256 Cipher Suite): Provides a mandatory-to-implement cipher suite for stronger encryption.

- IEEE 802.1AEbw-2013 (MACsec Cipher Suite): Defines additional cipher suites, including AES-XPN (eXtended Packet Numbering) for greater replay protection.

- MKA (MACsec Key Agreement) Protocol: Dynamically establishes and manages security keys and associations between peers.

- IEEE 1588v2 (Precision Time Protocol): Ensures accurate timing for synchronization over encrypted links, critical for mobile backhaul and financial applications.

- RoHS and WEEE: Compliant with environmental directives.

TECHNICAL SPECIFICATIONS

The following table provides comprehensive and detailed technical parameters for the primary hardware platforms supporting the MACsec implementation. It serves as a crucial reference for capacity planning and procurement evaluation.

Parameter	**Specification**

Form Factor	Modular Chassis (10RU / 12RU) and Fixed 1RU / 2RU
Switching Capacity	Up to 25.6 Tbps (Non-blocking, Full-Duplex)
MACsec Throughput	Line rate on all ports (10GE to 100GE) - 100% capacity
MACsec Cipher Suites	AES-GCM-128-ICV (16), AES-GCM-256 (IEEE 802.1AEbn), AES-XPN (IEEE 802.1AEbw)
Maximum Secure Associations	64,000 per system
Latency (MACsec on/off)	< 1 microsecond (10GE), < 500 nanoseconds (100GE)
Power Supply	1+1 / N+N Redundant AC (100-240V) or DC (-48V) PSUs, Hot-swappable
Typical Power Consumption	Varies by line card: 150W (10GE) to 450W (100GE)
Cooling	Hot-swappable, N+1 redundant fan trays with airflow options
Operating Temperature	0°C to 45°C (Standard), -40°C to +75°C (Ruggedized)
Management Ports	1 x 10/100/1000Base-T (Out-of-band), 1 x RJ-45 Console, 1 x USB

CPU & Memory	Dual-core ARM Cortex-A72, 16GB DDR4 RAM, 64GB eMMC Flash
Mean Time Between Failures (MTBF)	> 250,000 hours (at 25 ° C, per MIL-HDBK-217F)
Security Certifications	FIPS 140-2 Level 2 (In Process), Common Criteria EAL2+

ORDERING OPTIONS

MACsec functionality is available via flexible licensing and hardware ordering models to suit diverse deployment needs and budgetary requirements.

- HARDWARE SKUs:

    * [Example SKU: MAC-X-SF-10G-48T]: 48-Port 10GE SFP+ Switch, MACsec-ready hardware.

    * [Example SKU: MAC-X-CH-100G-36Q]: 36-Port 100GE QSFP28 Line Card, MACsec-ready.

    * [Example SKU: MAC-X-CH-FAB]: Redundant Fabric Module for modular chassis.

    * [Example SKU: MAC-X-PSU-AC-1200W]: 1200W AC PSU, N+N Redundant.

- SOFTWARE LICENSING:

* MACsec Base License: Enables MKA and AES-GCM-128 encryption on all ports. Bundled with hardware purchase.

* MACsec Advanced License: Enables AES-GCM-256 encryption, AES-XPN, and advanced MKA features. Available as a software add-on (SW-MAC-SEC-ADV).

* MACsec Orchestration License: Enables centralized key management and policy orchestration via the [COMPANY NAME] Network Management System. (SW-MAC-SEC-ORCH).