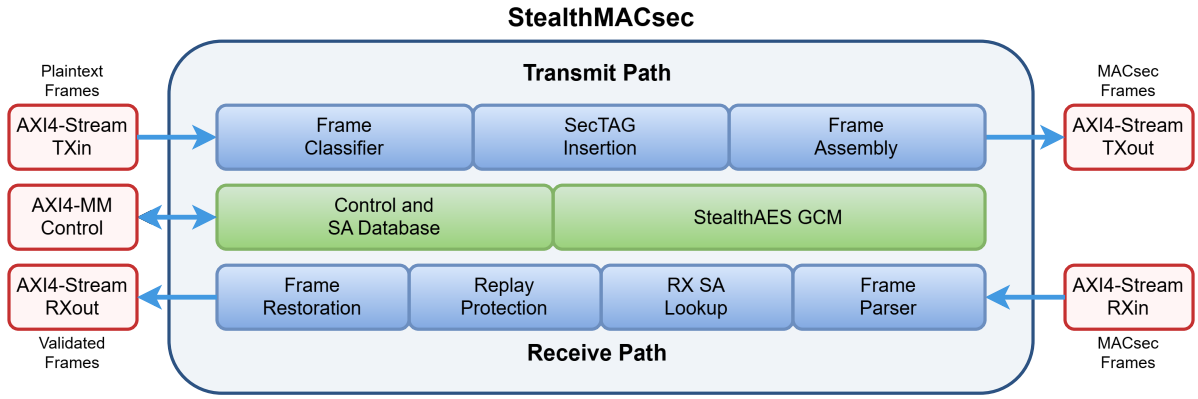
# StealthMACsec

IEEE 802.1AE MACsec Engine With Advanced Side-Channel Countermeasures

**Secure Ethernet networks with industry leading MACsec implementation featuring advanced side-channel countermeasures, automatic SA lifecycle management, and scalable multi peer architecture.**

| Up to 10 Gbps | 1B+ | 1-512 |
|---|---|---|
| Throughput | Trace SCA Resistance | Scalable SAs |




## Key Features

- **IEEE 802.1AE-2018 Compliant**
  Full MACsec with GCM-AES-256
- **Advanced SCA Countermeasures**
  Industry leading side-channel resistance
- **Scalable SA Architecture**
  Single TX SA, 1-N RX SAs (up to 512)
- **Automatic SA Management**
  Seamless TX SA rollover and lifecycle
- **Hardware Replay Protection**
  Per SA packet number validation
- **AXI4 Stream Interfaces**
  Four data path interfaces for integration
- **High Performance**
  Line rate processing up to 10 Gbps on FPGAs
- **FPGA and ASIC Ready**
  Optimized for multiple platforms

## Applications

**Embedded Systems**
- Inter module communications
- Sensor network security
- Distributed system protection
- Industrial automation

**Defense and Aerospace**
- Secure backplane links
- Secure sensor fusion
- Cross-domain data protection
- Tactical data link gateways

**Critical Infrastructure**
- Control system protection
- Multi-peer secure networks
- Real time data security
- Point to point connections

# StealthMACsec Product Overview

## Performance and Resource Utilization

| FPGA Platform | Max Frequency | Throughput | Resources |
|---|---|---|---|
| Xilinx UltraScale+ | 200 MHz | 1-10 Gbps | 16K-44K LUTs |
| Microchip PolarFire | 100 MHz | 0.8-5 Gbps | 23K-68K LUTs |
| Intel Agilex 5 | 180 MHz | 1-9 Gbps | 17K-52K LUTs |

## Architecture Overview

**Transmit Path:**
- Frame classification and protection
- SecTAG insertion with SCI
- GCM-AES-256 encryption
- ICV generation and appending
- Automatic PN management

**Receive Path:**
- MACsec frame parsing
- Multi SA lookup (SCI+AN)
- Hardware replay protection
- GCM-AES-256 decryption
- Frame validation and output

**SA Management:**
- Configurable SA database (8-512)
- TX SA lifecycle with rollover
- Multi peer RX SA support
- Hardware PN tracking

## Interface Specifications

**Data Path Interfaces:**
- Four AXI4 Stream interfaces
- Configurable 32/64/128-bit width
- TLAST frame delimiters

**Control Interface:**
- AXI4 Lite memory mapped
- SA configuration and management
- Statistics and error monitoring
- Interrupt generation

**Security Features:**
- GCM-AES-256 cipher suite
- 32-bit packet numbers
- Per SA replay protection
- Automatic SA rollover
- Hardware based processing

## Why Choose StealthCores?

**Industry Leading Security**
Advanced SCA countermeasures inherited from our proven StealthAES engine protect against sophisticated attacks.

**Seamless Integration**
Standardized AXI interfaces and comprehensive SA management enable rapid deployment.

**Expert Support**
Decades of cryptographic implementation experience with dedicated integration support.

**Proven Performance**
Line rate processing up to 10 Gbps on FPGAs with scalable multi peer architecture.

**Ready to Secure Your Systems?**

info@stealthcores.com | www.stealthcores.com |  | Rev. 25.1