Root of Trust Solutions

Broad portfolio of root of trust solutions provide hardware-based foundation for security

Overview

Providing a hardware-based foundation for security, Rambus offers a portfolio of robust Root of Trust solutions, ranging from richly featured military-grade co-processors to highly compact state machines. With a breadth of solutions applicable from the data center to Internet of Things (IoT) devices, Rambus has a Root of Trust solution for almost every application.

RT-100 and RT-200 State-Machine Root of Trust Solutions

Designed to be integrated in power and space-constrained SoCs or FPGAs, these state-machine-based root of trust hardware cores guard the most sensitive assets on chips and establish the foundation for platform security.

Configuration Options

Feature	Description	RT-100	RT-121	RT-130	RT-131	RT-140	RT-260
Application Focus	**Example Applications**	**IoT**	**IoT CN**	**IoT/ Edge**	**IoT/ Edge CN**	**IoT/ Cloud**	**IoT/ Cloud**
FIPS 140 CAVP	FIPS 140-2 CAVP & FIPS 140-3 CAVP (2020)	✓	✓	✓	✓	✓	✓
FIPS 140 CMVP	FIPS 140-2 CMVP & FIPS 140-3 CMVP (2020)	✓	✓	✓	✓	✓	✓
OTP Management	Interface	✓	✓	✓	✓	✓	✓
AES HW	ECB, CBC, CTR Modes – Max Key Size: 256 bits	✓	✓	✓	✓	✓	✓
AES Modes	AES-CCM, AES-CMAC, AES-GCM/GMAC (standard) AES-XTS (optional)	-	✓	✓	✓	✓	✓
Regional Crypto	SM2/SM3/SM4	-	✓	-	✓	-	-
HMAC-SHA2 HW	SHA-2 and HMAC-SHA2 – Max SHA-2 Mode (bits)	256	256	512	512	512	512
Public Key Engine	RSA, ECC Acceleration Core	16x16	16x16	32x32	32x32	32x32	32x32
ECC HW	Max Curve Size: 521 bits	✓	✓	✓	✓	✓	✓
RSA HW	Max Exponent Size: 3096 bits	✓	✓	✓	✓	✓	✓
Random Number Generator HW	NIST SP800 compliant TRNG	✓	✓	✓	✓	✓	✓
Optional Cryptography	ARIA, 3DES*, SHA-3, HMAC-SHA-3 *3DES is standard on RT-130, 131, 140	-	✓	✓	✓	✓	-
I/O Performance	Throughput (Gbps)	1	1	2	2	2	2
Crypto Performance	Crypto/Hash Performance (Gbps) @500MHz	1	1	2	2	2	2
DMA	Standard (STD) or Multi-channel (MC)	✓	✓	✓	✓	✓	✓
I/O Bus	AMBA Bus Master/Slave: AXI/AHB	✓	✓	✓	✓	✓	✓
OTP Interface	Interface to 3rd-Party OTP: TCM	✓	✓	✓	✓	✓	✓
Multiple Roots of Trust	Roots/Key Splits	1	1	1	1	1	1

RT-600 Secure Co-Processor Root of Trust Solutions

The RT-600 series Root of Trust solutions are integrated as independent hardware security blocks in semiconductor devices to provide a hardware-based foundation for security. Once integrated into a semiconductor device, an RT-600 series core provides a secure environment for performing a wide range of security functions in a simple and cost-effective manner, providing enhanced security functionality while providing faster time-to-market and significant differentiation.

Configuration Options

Feature	Description	RT-630	TR-640	RT-645	RT-660
Application Focus	**Example Applications**	**AI/ML/Cloud**	**Automotive**	**Automotive**	**FIPS/Gov**
Programmable	Secure Applications on embedded RISC-V CPU	✓	✓	✓	✓
FIPS 140 CAVP	FIPS 140-2 CAVP & FIPS 140-3 CAVP (2020)	✓	✓	✓	✓
FIPS 140 CMVP	FIPS 140-2 CMVP & FIPS 140-3 CMVP (2020)	✓	✓	✓	✓
DPA Resistance	RSA & ECC PKI operations	✓	✓	✓	✓
DPA Resistance	AES – 3DES – HMAC crypto and hash operations	-	-	-	✓
Automotive Standard	ISO 26262 ASIL	-	ASIL-B	ASIL-D	-
OTP Management	OTP management core	✓	✓	✓	✓
Key Derivation	Secure Key Derive	✓	✓	✓	✓
Anti-Tamper (Clock & Power)	Canary Core Monitor – Glitch Detection Logic	✓	✓	✓	✓
Secure Boot Management	ECDSA P256 with HMAC-SHA-2-256	✓	✓	✓	✓
Secure Debug	ECDSA P256 with HMAC-SHA-2-256	✓	✓	✓	✓
Secure Lifecycle Management	Secure lifecycle stages support	✓	✓	✓	✓
Secure Feature Management	Just-in-time – SKU Management	✓	✓	✓	✓
Memory ECC	Support for ECC or SECDED SRAM	✓	✓	✓	✓
Crypto Accelerator cores	AES – HMAC – RSA – ECC – TRNG HW cores	✓	✓	✓	✓
I/O Performance	Throughput (Gbps)	>8	>8	>8	>8
Crypto & Hash Performance	Crypto/Hash Performance (Gbps) @500MHz	3	3	3	3
Public Key Engine	RSA, ECC Acceleration Core multiplier width	32x32/64x64	64x64	64x64	64x64
DMA	Standard (STD) or Multi-channel (MC)	MC	MC	MC	MC
I/O Bus	AMBA Bus Master/Slave	AXI/AHB	AXI/AHB	AXI/AHB	AXI/AHB
OTO Interface	Interface to 3rd Party OTP	APB	APB	APB	APB
Multiple Roots of Trust	Roots/Key Splits	4/8	4/8	4/8	4/8

Features

- Custom-designed 32-bit secure processor
- Security model includes hierarchical privilege model, secure key management policy, hardware-enforced isolation/access control/protection, error management policy
- Anti-tamper and DPA-resistance protection
- Multi-layered security model protects all core components against a wide range of attacks
- Includes a wide range of security modules, including True Random Number Generator, Canary logic for protection against glitching and overclocking, secure key derivation and key transport, life cycle management, secure test and debug, feature management

rambus.com/security/root-of-trust

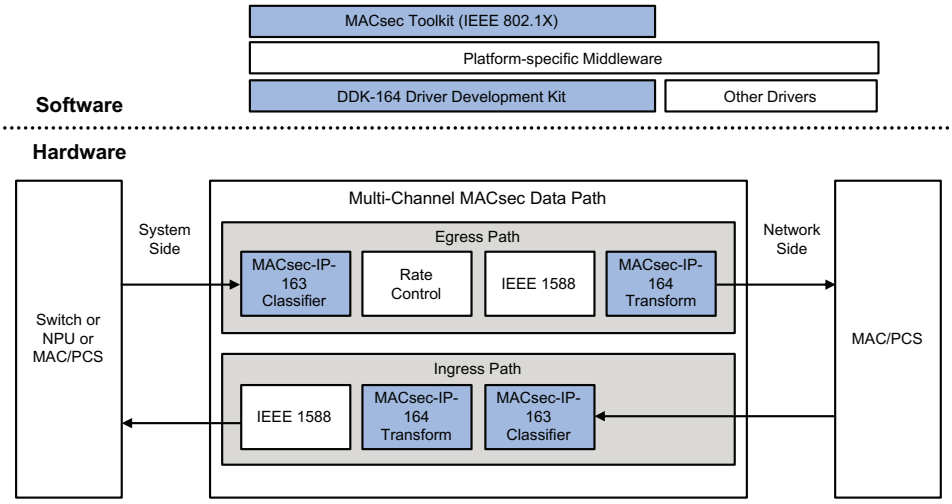
Multi-Channel Engine MACsec-IP-163/164

Complete MACsec solution for multi-port Ethernet with rates up to 800 Gbps

Overview

Cloud computing and data center throughput requirements have driven Ethernet and OTN standards to 100G, 400G and now to 800G. These standards deploy multiple SerDes lanes with various data rates, requiring support for flexible bandwidth allocation for a varying number of channels (ports) depending on the target silicon. The MACsec-IP-163/164 engine adds MACsec to high-speed multi-rate and multi-port Ethernet devices. The MACsec-IP-163/164 architecture provides an optimal solution for aggregate throughput ranging from 100G to 800G and beyond. This MACsec engine is designed for use in data centers, enterprise and carrier networks as well as in network-attached high-performance computing.

Solutions for 100G to 800G MACsec



The MACsec-IP-163/164 engine is a fully-compliant MACsec solution and supports VLAN-in-clear cases. Optionally, this engine can be enabled to fully support Cisco specifications including line-rate IPsec ESP transformation with AES-GCM cipher. To address regional requirements, the engine can be delivered with customer classification options supporting line-rate throughput.

The MACsec-IP-164 transform engine's cryptographic functions are FIPS-certification ready, supporting AES-ECB, AES-CTR, AES-GCM/GMAC transformations.

The MACsec-IP-163/164 engine is delivered with a widely adopted Driver Development Kit. To build a system-level solution, Rambus offers the MACsec Toolkit product that implements a complete IEEE 802.1X specification and has multiple features that facilitate development and testing of the MACsec compliant processing.

The MACsec-IP-163/164 has been used by leading customers over several generations thanks to its proven software compatibility and API scalability.

Highlights

Full Line-rate Throughput
- 800G in 7nm technology
- 400G/600G in 16nm technology
- 100G/200G in reduced area configurations
- Native TDM engine with fully flexible bandwidth allocation

Feature Rich
- Flexible classifer
- Full compliance with IEEE 802.1AE
- Optional Cisco features, IPsec
- FIPS certification support
- Forward-looking hardware and software compatibility
- Very efficient hardware-software interaction

Highly Configurable
- Numerous options for optimal area, throughput and features trade-off

Software and Integration Support
- Driver Development Kit
- IEEE 802.1X Toolkit
- World-class support from Rambus MACsec experts

Use Cases

- Ethernet PHYs
- Switch/router ASICs
- NPU data planes
- Smart NICs
- High-performance SOCs
- 5G SOCs
- Network-attached AI

How It Works

The MACsec-IP-164 engine provides complete MACsec SecY frame processing for multiple channels (ports). It supports multiple SecY (virtual ports) to realize protection for each individual virtual network running over the same physical port. Its pooled classification and transformation resources allow optimal implementation of multi-port designs. The fat-pipe design allows aggregating multiple ports to use the same MACsec SecY as well as protecting a single port with data rate up to 800Gbps.

The MACsec-IP-163 is a virtual port matching classifier that works with the MACsec-IP-164 to form an autonomous MACsec processing data path. Alternatively, the MACsec-IP-164 can be used in combination with an external classifier or stand alone, depending on the use case.

Integration

The MACsec-IP-163/164 engine offers flexibility on integration into the customer's Ethernet subsystem. Integration depends on the following major factors: data path design (channelized or port-based), location of the IEEE 1588 timestamping and preferred method for handling MACsec packet expansion (per-packet or port-based). The MACsec engine has a push interface. Customers can flexibly implement buffering and flow control according to their system requirements.

The MACsec engine can be supplied with fixed SOP-to-SOP latency feature or provide the minimum latency. In case of a minimum latency, the latency is still deterministic so that it can be used to correctly adjust the IEEE1588 timestamp.

For applications that require numerous SA and TCAM matching rules, the MACsec engine can be supplied with a TCAM controller that can interface to technology TCAM. Default TCAM implementation is logic-based.

Features

Packet Interface

- Cut-through TDM interface
- 1024-bit (default), 128/256/512-bit (options)
- Up to 64 channels (ports)
- Flexible bandwidth allocation
- FlexE ready

SA and Classification Scaling

- Pooled SA (up to 4K)
- TCAM internal/external

Control Interface

- AMBA APB3
- Interrupts (global and per-channel)

Default Protocol Support

- Full IEEE 802.1AE-2018 compliance
  - IEEE 802.1AE
  - IEEE 802.1AEbn
  - IEEE 802.1AEbw
  - IEEE 802.1AEcg
- MACsec with up to 4x VLAN-in-clear

Optional Features

- Cisco MACsec extensions
- IPsec ESP with AEC-GCM
- Other customer classifications

FIPS 140-2 CAVP ready

- Support for basic AES and AEC-GCM transformations

Deliverables

Packages

- Silicon IP
- Driver Development Kit

Complete Documentation

- Hardware integration guide
- Hardware and software reference manuals
- Programming guides
- IP-XACT Register description

Tools and Scripts

- Verilog for synthesis and simulation
- All scripts and support files needed for standard EDA tool flows

Integration Support

- Complete verification test bench
- Comprehensive set of test vectors

rambus.com/security/protocol-engines

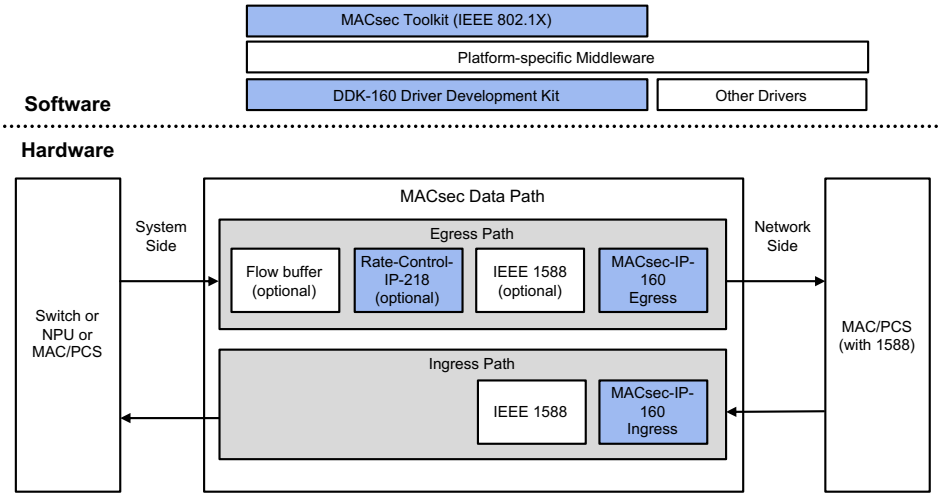
Single-port Engine MACsec-IP-160

Complete MACsec solution for single-port Ethernet with rates up from 1G to 100G.

Overview

Ethernet link encryption with MACsec is an important requirement of the connectivity revolution that is ongoing in the industrial, 5G infrastructure, broadband access and automotive areas. Numerous silicon devices need to be equipped with an area-efficient and feature rich MACsec data plane, complemented with software support in the form of drivers and the actual control plane for key management and security policy configuration.

Solutions for Single-port 1G to 100G MACsec



The MACsec-IP-160 engine is an industry-proven solution for adding a hardware MACsec data plane to the Ethernet port of silicon devices. The engine is available in throughput/area optimized configurations that cover the modern Ethernet rates of 1-10G, 10-25G, 25-50G and 50-100G.

The MACsec-IP-160 engine is a fully compliant MACsec solution and supports VLAN-in-clear cases. It has all necessary functionality to autonomously protect a full port or multiple VLAN-based EVC and count all required statistics. Flexible hardware and software interfaces allow different types of system integration, specifically around IEEE1588, important for 5G, industrial and automotive applications.

The MACsec-IP-160 engine is delivered with a widely adopted Driver Development Kit. To build a system-level solution, Rambus offers the MACsec Toolkit product that implements a complete IEEE 802.1X specification and has multiple features that facilitate development and testing of the MACsec compliant processing.

The MACsec-IP-160 has been used by leading customers over several generations thanks to its maturity, scalability and ease of use.

Highlights

Full Line-rate Throughput
- Optimized for 1G, 10G, 25G, 50G, 100G rates
- Lowest and fixed-latency modes

Feature Rich
- Flexible classifier
- IEEE 802.1AE-2018 compliance
- VLAN-in-clear
- FIPS certification support
- Forward-looking hardware and software compatibility
- Very efficient hardware-software interaction

Highly Configurable
- Numerous options for optimal area, throughput and features trade-off
- Available in ingress, egress and bidirectional configurations

Software and Integration Support
- Rate-Control-IP-218 rate shaper
- Driver Development Kit
- IEEE 802.1X Toolkit
- World-class support from Rambus MACsec experts

Use Cases

- Ethernet PHYs
- Ethernet NICs
- Switch/router ASICs
- 5G SoCs
- Broadband chipsets
- Automotive SoCs

How It Works

The MACsec-IP-160 engine provides complete MACsec processing for a port. It contains a flexible classifier with a table of programable rules with the programmable actions. The transformation engine supports all features and ciphers of the standard MACsec and VLAN-in-clear extension. The processing results are reflected in the MACsec-compliant statistics as additional non-standard counters. MACsec-IP-160 offers optional post-decryption consistency checking with a set of programmable rules.

The MACsec-IP-160 engine is a basis for building various use cases. Beside traditional point-to-point and point-to-multipoint use cases, it is also deployed in protecting data over carrier networks with bypass/drop/protect policy that is controlled per VLAN EVC.

The MACsec-IP-160 can be used in combination with external classifier and accepts secure channel pointer or packet bypass indication.

Integration

The MACsec-IP-160 engines offers flexibility on integration into the customer's Ethernet subsystem. It can be used as a FIFO-like component, or a fixed-latency engine with a push interface.

Customers can implement MACsec processing with IEEE1588 timestamping in the Tx MAC (unencrypted PTP) as well as timestamping ahead of the MACsec (supporting both - encrypted and encrypted PTP).

To implement fixed-latency mode at egress direction, Rambus offers the Rate-Control-IP-218, a programmable module that shapes the traffic according to line rate and accounts for the MACsec added header/trailer.

Deliverables

Packages
- Silicon IP
- Driver Development Kit

Complete Documentation
- Hardware integration guide
- Hardware and software reference manuals
- Programming guides
- IP-XACT Register description

Tools and Scripts
- Verilog for synthesis and simulation
- All scripts and support files needed for standard EDA tool flows

Integration Support
- Complete verification test bench
- Comprehensive set of test vectors

Features

Packet Interface
- Cut-through FIFO interface
- 128-bit (1G to 50G), 512-bit (100G)
- External classification inputs
- SOP and EOP pass-through bus for side-band information
- Lowest and fixed-latency modes

SA and Classification Scaling
- SA (16 to 256)
- Post-decryption consistency check (optional)

Control Interface
- Simple 32-bit interface
- Interrupts

Protocol Support
- Full IEEE 802.1AE-2018 compliance
  - IEEE 802.1AE
  - IEEE 802.1AEbn
  - IEEE 802.1AEbw
  - IEEE 802.1AEcg
- MACsec with up to 2x VLAN-in-clear

FIPS 140-2 CAVP ready
- Support for basic AES and AEC-GCM transformations

rambus.com/security/protocol-engines

Multi-Protocol Engines

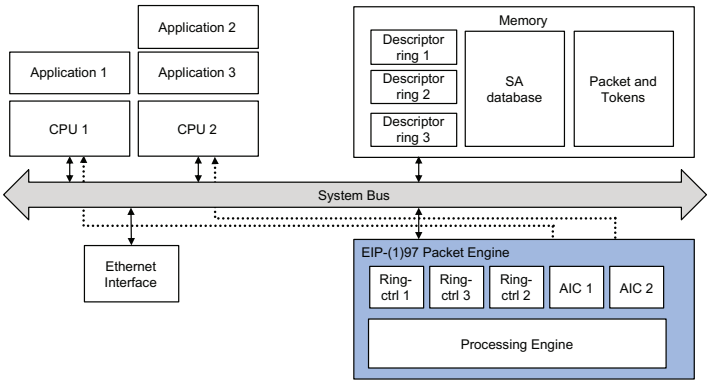
Packet-Engine IP Core Family for IPsec, SSL/TLS, DTLS and more

Highlights

Multi-Protocol Engine IPs offer acceleration of IPsec, MACsec, SSL/TLS/DTLS, sRTP and basic hash-crypto in architectures ranging from the look-aside engines to the more sophisticated, powerful inline packet engines.

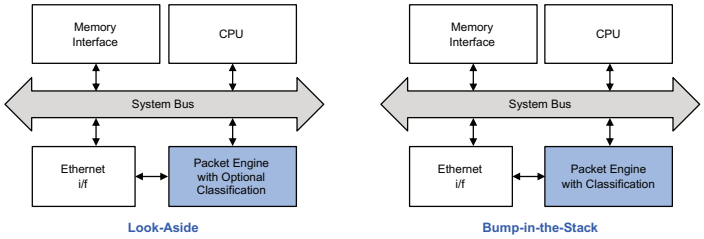
Engines Family

- **Protocol-IP-93** – Accelerate IPsec, SSL/TLS up to 1 Gbps
- **Protocol-IP-97** – Accelerate IPsec, SSL, TLS/DTLS, 3GPP and MACsec up to 5 Gbps
- **Protocol-IP-196** – Accelerate IPsec, SSL, TLS/DTLS, 3GPP and MACsec up to 10 Gbps
- **Protocol-IP-197** – Accelerate IPsec, SSL, TLS, DTLS (CAPWAP), 3GPP and MACsec up to 100 Gbps



Architecture

- Look-Aside/Hybrid: connected as security co-processor to a SoC bus,
- In-line Hybrid: connected in between two streaming interfaces that are indirectly connect to either SoC or some external interface
- Bump in the Stack: connected in between a SoC bus and Ethernet MAC,
- Bump in the Wire: connected in between two Ethernet MACs.



Example Architectures

Interfaces

- **AXI master** Host bus interfaces (data width 128bits, address width 56bits),
- **AXI slave** Host bus interfaces (data width 32bits, addresswidth 21bits),
- Virtualization support through bus sideband signals
- Internal scheduling of parallel descriptor-rings to avoid delays due to bus latency

Rambus Multi-Protocol Engines offer acceleration of IPsec, MACsec, SSL, DTLS, SRTP, as well as wireless and storage algorithms.

Protocols

IPsec Classification

- Psec-ESP header parsing to look-up a flow
- Fetch flow and corresponding transform record based on lookup result
- Update flow statistics
- Update transform statistics
- Support for IPv4 and IPv6

IPsec Transformation

- Full IPsec packet ESP transforms according to latest RFCs (2403, 2404, 2405, 2410, 2474, 3168, 3566, 3602, 3686, 4106, 4301, 4303, 4308, 4309, 4543, 4868, 4869, 6040, 6071, 7539 and 7634),
- Support for IPv4 and IPv6,
- Autonomous IPsec ESP packet classification and Security
- Association selection (both out- and inbound),
- IPsec ESP tunnel & transport mode,
- Complete IPsec Header/Trailer processing,
- Insert ESP header for outbound packets, strip and verify ESP header for inbound packets,
- Full sequence number processing, including ESN and full anti-replay check with various mask sizes, up to 384 bits
- Calculate and insert Integrity Check Value for outbound packets, strip and verify for inbound packets,
- Append (outbound) / strip and verify (inbound) padding up to 255 bytes.
- Support for processing packets for one SA on multiple processing engines, maintaining SA coherency.

SSLv3.0 / TLSv1.0 / TLSv1.1 / TLSv1.2 / TLSv1.3

- Packet transforms according to latest RFCs (2246, 4346, 5246, 6101, 6655, 7905 and 8446),
- Header processing
- Full autonomous single pass processing for stream and block cipher modes of operation,
- Padding insertion & removal up to 255 bytes,
- ICV/TAG insertion/verification.

DTLS v1.0 - v1.2

- Packet transforms according to latest RFCs (4347 and 6347),
- Header processing,
- Full autonomous single pass processing for stream and block cipher modes of operation,
- Padding insertion & removal up to 255 bytes,
- ICV/TAG insertion/verification
- Support for processing packets for one SA on multiple processing engines, maintaining SA coherency.

MACsec

- MACsec frame transforms according to IEEE 802.1AETM-2006 and 802.1AEbn,
- SecTAG insertion and removal,
- PN insertion, removal and verification,
- ICV generation, insertion, removal and verification
- Support for processing packets for one SA on multiple processing engines, maintaining SA coherency.

SRTP

- SRTP packet transforms according to RFC3711,
- ROC insertion and removal,
- MKI insertion and removal,
- TAG generation and insertion.

Wireless Algorithms

- Kasumi f8 and f9,
- SNOW 3G,
- ZUC.

Storage Algorithms

- AES-XTS (including CTS mode)

rambus.com/security

Protocol-IP-338 High-speed XTS-GCM Multi-stream Engine

Complete multi-stream cryptographic engine with rates up to 2 Tbps

Overview

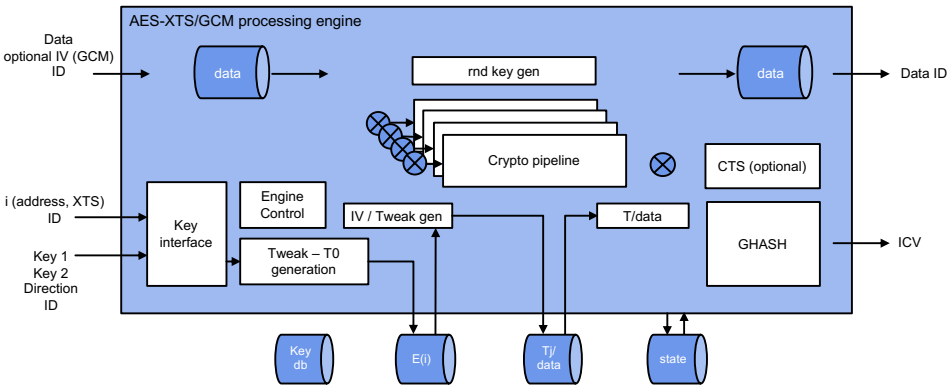
The Protocol-IP-338 (EIP-338) is a scalable, high-performance, multi-stream cryptographic engine that offers XTS and GCM modes of operation for the AES algorithms on bulk data. Its flexible data path is suitable to scale from 50 Gbps to 2 Tbps providing a tailored engine with minimal area for your application.

The flexible interface makes it possible to perform processing for many different applications and protocols, including inline memory encryption, inline disk encryption, MACsec, IPsec and OTN security. The multi-stream architecture allows interleaved data processing for many independent data streams simultaneously. Switching between streams can be done every clock cycle without loss of performance. Data is processed without flow control and with fixed latency, dependent on the static configuration selected.

The Protocol-IP-338 data path can be scaled to widths that are multiples of 128 bit to allow a tradeoff between area and performance that best fits the target application. Configuration options include or exclude support for CipherText Stealing (CTS) and AES-GCM.

On-chip SRAM external to the Protocol-IP-338 is used to store the key database as well as various precomputes and state information for each of the streams the engine is processing in interleaved fashion.

Rambus Solution for 50 Gbps to 2 Tbps XTS-GCM



Highlights

Multi-stream Processing

- True multi-stream design with time-sliced processing
- Every clock cycle may process a different stream; without limitations
- Configurable to support any number of streams, only limited by SRAM timing

Numerous Processing Modes

- XTS-AES mode, with optional support for cipher text stealing (CTS)
- AES-GCM mode supporting header bypass of any number of full 128-bit cipher blocks
- Encryption/decryption-only mode: AES-CTR
- Authentication-only mode: AES-GMAC
- Any size full packet bypassing

Compliance

- FIPS-197
- IEEE-P1619/D16
- NIST SP800 38A
- NIST SP800 38D
- NIST SP800 38E

Use cases

The Protocol-IP-338 is designed to support a variety of use cases, including:

- High-speed, Inline Memory Encryption with AES-XTS for DRAM, SRAM or Flash/SSD
- High-speed, Inline Packet Stream encryption with AES-GCM for PCIe, Ethernet or OTN
- A combination of the above

How it Works

The Protocol-IP-338 is a data-processing engine and contains input/output data interfaces and interfaces intended for supplying key material that is stored in the engine's local SRAM.

Before cryptographic processing can start, the Host CPU transfers the key material, together with the AES mode to use, to one of the key slots in the engine. Key material can be shared between multiple streams and many blocks while the key remains available in local SRAM.

The Tweak (for XTS) or IV (for GCM) is provided prior to or at the same time as the first data word, together with a reference to the Key slot and the direction of processing in case of GCM. After processing, the Protocol-IP-338 outputs the result data and, in case of GCM mode, authentication tag together with the last output data word.

The external system is responsible for the following items:

- Per-block Tweak or IV generation
- Key lifetime management, to ensure that the key is refreshed when the current key expires
- XTS decrypt key generation in case of an engine configuration without Decrypt Key generator
- Reacting to processing errors reported by the Protocol-IP-338

Separate IP cores can be provided to assist with Tweak or Decrypt Key generation.

Configuration and Verification

Example Configurations

The Protocol-IP-338 has a scalable number of processing pipes, key sets and streams. It is available in different configurations, suitable for different applications to meet different gate count and throughput objectives.

Verification

- Set of test vectors for chip integration verification
- Integration test vectors in a human-readable format
- Self-contained verification environment
- 100% verification coverage

Features

Performance and Configuration

- One input word per clock without any backpressure
- Design can switch stream, algorithm, mode, key and/or direction every clock cycle
- For GCM, throughput is solely determined by the data width, data alignment and clock frequency
- For XTS, block processing rate may be limited by the number of configured tweak encryption & CTS cores; a configuration allowing 1 block/clock is possible
- Design achieves up to 2 GHz in 7nm technologies

FIPS Certification

- Support for XTS-AES, AES-CTR, AES-GMAC, AES-GCM transformations. All modes meet requirements for FIPS certification of the crypto core

Low Latency with Zero Variation

- Low-latency processing with fixed latency per static pipeline configuration. Pipeline can be statically configured to reduce latency in cases where certain modes or algorithms are not in use

Cryptographic Processing

- Bi-directional design: direction is selected on a per-key (for XTS) or per-packet (for GCM) basis
- Uni-directional XTS design option for reduced area
- Authenticated encryption & decryption: AES-GCM
- Authentication: AES-GMAC
- Encryption: AES-CTR
- Supported key sizes for AES: 128 and 256 bits
- Tag output
- External 96-bit IV generation that allows supporting various use cases

Packet Interface

- Push-bus time-sliced interface (no handshake)
- Each data word may belong to a different stream
- Sideband signals for control and processing status
- Configurable bus width, depending on desired throughput in 128-bit units: minimum 128-bit, maximum only limited by area and congestion cost

Control Plane Interface

- Key loading interface can easily be mapped to a 32-bit wide host interface
- Key set separate from stream state; allows for many parallel streams sharing a limited set of keys to reduce storage requirements

External Memory Interface

- Set of memory interfaces to buffer data and control information
- All interfaces are for 1R / 1W memory with 2-cycle read latency to allow inserting ECC logic
- ECC uncorrectable status input
- Some memories have per-word chip selection for efficient power usage

Clocking

- Single-clock synchronous design with a number of switchable clock domains for efficient power usage

rambus.com/security

Protocol-IP-63 Multi-channel AES-GCM Engine

Complete cryptographic engine with rates up to 2.4 Tbps

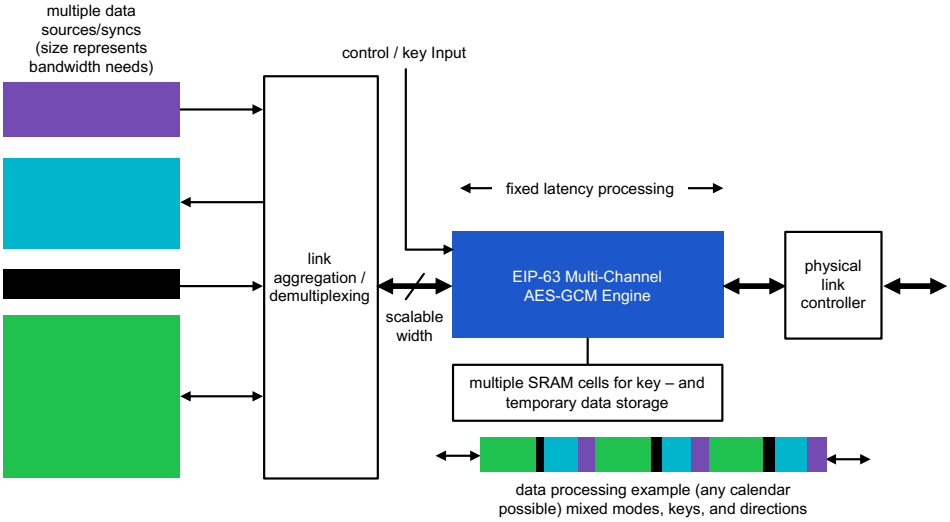
Overview

The Protocol-IP-63 (EIP-63) is a scalable high-performance, multi-channel cryptographic engine that offers AES-GCM operations as well as AES-CTR and GMAC on bulk data. Its flexible data path is suitable to scale from 100 Gbps to 2.4 Tbps to provide a tailored engine with minimal area for your application. The FIFO-like data interface makes it possible to perform frame processing for many different protocols, including MACsec, IPsec, and OTN security. The time-sliced processing architecture makes it possible to alternate data processing for different channels or tunnels simultaneously. Block switching can be done with a granularity of a single clock cycle. The engine is also designed to support FIPS vector processing.

The Protocol-IP-63 is designed to support multiple use cases, including:

- Security for 5G Transport with FlexE
- TMS transport network: encryption for OTNsec and FlexO (ITU-T)
- PCIe or CXL (Compute Express) Link Encryption
- NVMe over Fabric Security
- Link Encryption: Security for any high-speed copper or fiber link with channel/link aggregation
- Applications where low and/or fixed latency operation is vital

AES-GCM Solution for 100 Gbps to 2.4 Tbps



How it Works

Protocol-IP-63 is a packet-processing engine and contains input/output packet interfaces and interfaces intended for supplying key material. Before cryptographic packet processing can start, the Host CPU must transfer the key material to the engine. The packet processing mode (bypass, encryption, authentication, direction, IV) is provided on a per packet basis. After processing, the Protocol-IP-63 engine outputs the result packet as well as ICV (if authentication is enabled).

Highlights

Performance and Configurations

- Line rate performance without any restrictions
- Zero-Variation, Low Latency processing suitable for use with Precision Timing Protocol (IEEE 1588)
- Design achieves up to 1.6 GHz in 16nm technologies
- A configuration with 1536-bit bus processes at a rate of 2.4 Tbps at 1.6 GHz

Multi-Channel Processing

- True multi-channel design with time-sliced processing
- Single-slot calendar
- Configurable to support up to 255 independent channels with different rates
- Support for run-time channel and calendar reconfiguration
- Channel rate is achieved by aggregating bandwidth of the time slots without limitations

Compliance

- FIPS-197
- NIST SP800 38A
- NIST SP800 38D
- FIPS CAVP for above algorithms

How it Works (continued)

The external system is responsible for the following items:

- Per-packet IV generation
- Key lifetime management, ensures that the key is refreshed when the current key expires
- Reacting on processing errors reported by the Protocol-IP-63 engine

The Protocol-IP-63 engine detects the following data path exceptions:

- IV counter overflow
- When any RAM memory is read with an uncorrected error, its content cannot be trusted. Operation will continue normally but the report will be reported via an output pin
- Uncorrectable ECC errors on data RAMs should be handled by an upper-layer module

The Protocol-IP-63 engine is ready for FIPS certification. This can be done by providing the FIPS CAVP validation vectors through the packet interface and performing the required transformations.
The following transformations are supported:

- AES-ECB encrypt (in CTR mode, using the IV as data input)
- AES-GCM encrypt/decrypt and authentication
- AES-CTR encrypt/decrypt
- AES-GMAC authentication

Features

FIPS Certification

- Support for AES-CTR, AES-GMAC and AES-GCM transformations for FIPS certification of the crypto core

Frame Processing Modes

- AES-GCM mode
- En/decryption-only mode: AES-CTR
- Authentication-only mode: AES-GMAC
- Any size packet bypassing

Cryptographic Processing

- Bi-directional design. Direction is selected on a per-packet basis
- Authenticated encryption, authenticated decryption: AES-GCM
- Authentication: AES-GMAC
- Encryption: AES-CTR
- Supported key sizes: 128 and 256 bits
- ICV output
- External 96-bit IV generation that allows supporting various use cases

Low Latency with Zero Variation

- Low-latency processing fixed to 20 clock cycles for AES-CTR only configurations and 24 clock cycles for AES-GCM and AES-CTR+GMAC configurations

Packet Interface

- Push-bus time-sliced interface (no handshake)
- Each data word may belong to a different channel
- Sideband signals for control and processing status
- Configurable bus width, depending on desired throughput in 128-bit units: minimum 128-bit, maximum 1536-bit

Control Plane Interface

- Key loading interface that can easily be mapped to a 32-bit wide host interface
- For each channel, 2 keys (current, next) can be loaded

External Memory Interface

- Set of memory interfaces to buffer data and control information
- All interfaces are for 1R / 1W memory with 2 cycle read latency to allow inserting ECC logic
- ECC uncorrectable status input
- Some memories have per-word chip selection for efficient power usage
- Engine configurations with lower bus width and maximum number of channels requirements can be built with register storage instead

Clocking

- Single clock synchronous design with a number of switchable clock domains for efficient power usage

Configuration and Verification

Configuration

The Protocol-IP-63 has a scalable number of processing pipes and channels. It is available in different configurations, suitable for different applications to meet different gate count and throughput objectives. Available configurations scale from:

- 1-12 parallel pipelines
- 128-1536 bits/clock
- >1600 MHz (16nm)
- 2-256 channels
- Option for keys in registers or memories
- Configurations available from 400K gates

Verification

- Set of test vectors for chip integration verification
- Integration test vectors in a human-readable format
- Python / Verilog based verification environment
- 100% verification coverage

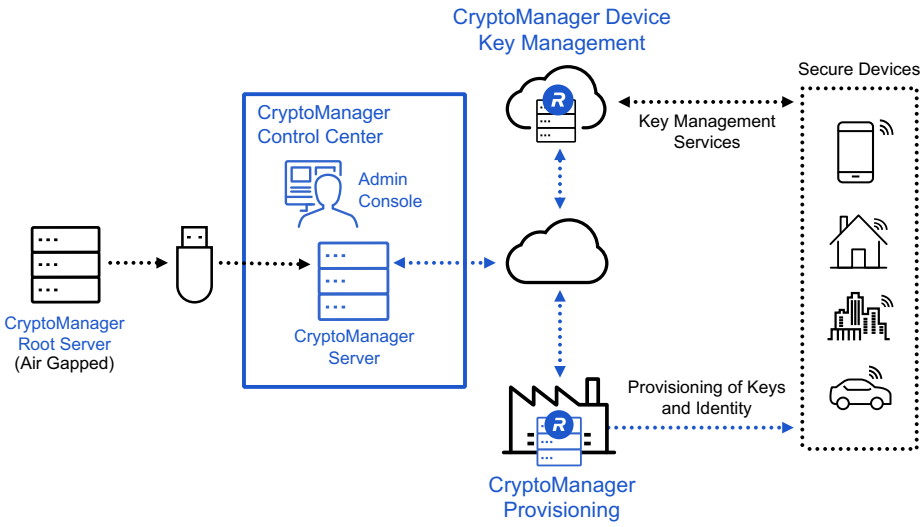
rambus.com/security

CryptoManager Provisioning

A secure supply chain solution for semiconductor and device manufacturers, enabling secure provisioning and key insertion.

Overview

CryptoManager™ Provisioning enables the secure injection of cryptographic keys and other sensitive data into chips and devices across a distributed supply chain. It supports both captive and 3rd-party (untrusted) manufacturing locations. CryptoManager Provisioning capabilities cover a broad range of secure operations, including key delivery and programming, protection of debug and other sensitive ports, and feature configuration. CryptoManager Provisioning can be used to provision device-specific information to any on-chip secure enclave, including the CryptoManager Root of Trust family of cores.



CryptoManager Control Center

The CryptoManager Control Center is a security control system that works in conjunction with an off-line Root Authority. It manages the distribution of data assets with the appropriate authorizations to connected CryptoManager Appliances. It includes an easy-to-use Administration Console for operators to centrally manage the infrastructure across multiple manufacturing sites.

CryptoManager Appliance

The Appliance is a tamper-resistant, rack-mounted server, deployed in high-volume manufacturing facilities or cloud services data centers, that provides local security and handles the distribution and programming of secret keys and device configuration data. It also delivers secure production logs and system health data to the CryptoManager tControl Center. The appliance is designed to integrate with existing

Highlights

Superior Security

- Extensible to third-party secure IP cores and chipsets
- Provisions cryptographic information securely in untrusted environments
- Protects against reverse engineering and counterfeiting

Improved Profitability

- Supports dynamic SKU management
- Enables new revenue with SoC feature activation
- Reduces operating costs through a single provisioning infrastructure and control system
- Deploys to any manufacturing facility and process flow

Secure Value Chain

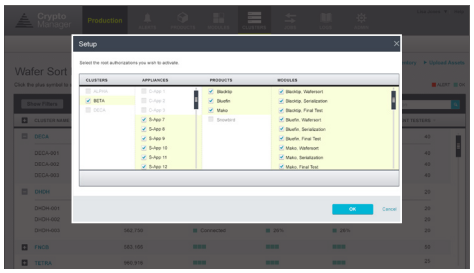
- Protects against cloning, counterfeiting, and overbuilding
- Monitors production status, availability, and inventory levels
- Protects IP and control access to sensitive ports & debug traces
- Verifies manufacturing volumes, yields and configurations

Working with CryptoManager Device Key Management

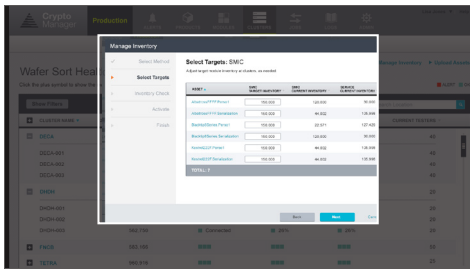
CryptoManager Device Key Management can be deployed in conjuction with CryptoManager Provisioning. CryptoManager Device Key Management is a cloud-based software platform enabling customers to build and deploy key management services that leverage hardwareprovisioned keys and certificates in chips and devices over the entire device lifecycle.

CryptoManager Administrator Console

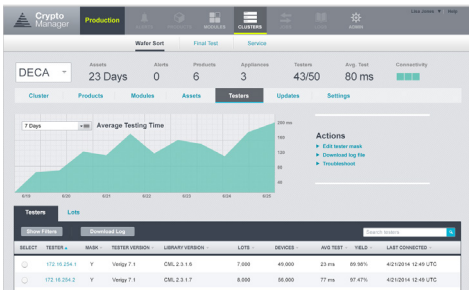
The Administrator Console provides device manufacturers with a secure real-time view of all manufacturing operations worldwide. Wizard-like tools guide users through workflows, providing extraordinary visibility and control.



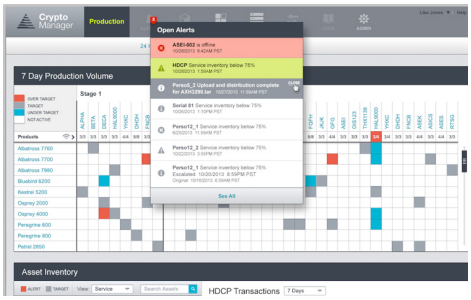
Set up factory infrastructure



Provision keys to appliance



Monitor system health



Resolve alerts proactively

Enterprise Class Features

- Cluster support for high availability and scalability
- Comprehensive system monitors and alerts
- Secure browser-based management console
- Business continuity/ disaster recovery
- Meets high-volume manufacturing critical performance requirements
- Advanced cryptographic key and secure data management
- Secure forensic audit logging

Security Features

- End-to-end encrypted communication channels
- Air gapped Root Authority for system permissions and authorizations
- Advanced encrypted key and data storage
- Two-factor user authentication for all user types
- Compatible with FIPS-140-2 Level 3

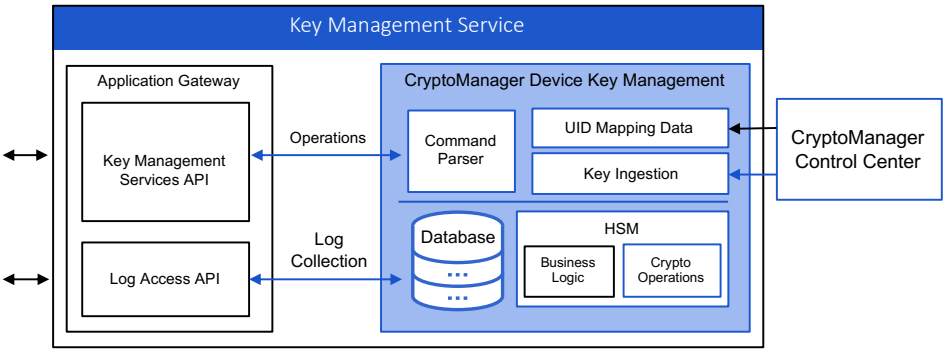
rambus.com/cryptomanager

CryptoManager Device Key Management

A cloud-based software platform enabling customers to build and deploy key management services that leverage hardware-provisioned keys and certificates in semiconductors and devices over the entire device lifecycle.

Overview

CryptoManager Device Key Management provides a cloud-based software platform which enables the building of key management services for chips and devices. Semiconductor and system OEMs can leverage these services to securely provision identities, device keys, and certificates to enable full lifecycle security management. CryptoManager Device Key Management enables an automated and secure capability to connect to trusted provisioning in manufacturing, and to leverage those provisioned identities and keys via the cloud to deliver value-add security services. These services provide chip and device makers additional opportunities to monetize their products after sale and shipment to end users.



Key management services built on the CryptoManager Device Key Management platform consist of four major components:

- **Cloud access proxy gateway** that controls access to keys and related services
- **Application gateway** and **associated APIs** to deliver services
- **Backend key and certificate database** to store and manage keys and certifications
- **Public key infrastructure** (PKI) to provide certificate lifecycle management services

CryptoManager Device Key Management enables capabilities and services including:

- **Verification of device ID and other chip/device meta data**. Using securely provisioned device unique keys, a transaction and a nonce is provided by the service, which is transmitted to and validated by the service. This forms the basis of a broader validation of the chip's identity and provenance for supply chain integrity validation.
- **Retrieval or secure replacement of device keys**. Semiconductor OEMs can provide their customers, either as a service or for a fee, the ability to retrieve device unique keys and/or certificates that were provisioned during production. These keys can subsequently be leveraged by end users to enable device or ecosystem-level security applications.
- **Certificate issuance, delivery and revocation**. For OEMs that require specific key material for specific applications, the platform enables provisioned keys to be used to securely deliver and install new customer keys.

Highlights

- Provides a cloud-based software platform for building key management services
- Automates the upload and activation of device keys and identities via the cloud
- Stores and manages device keys, certificates, and identity data
- Easily integrated through customer-branded application services gateway and APIs
- Provides chip identity validation at any stage of the chip/device lifecycle
- Enables high-value infield provisioning transactions as a service

Working with CryptoManager Provisioning

The CryptoManager Device Key Management platform can be deployed in conjunction with CryptoManager Provisioning. CryptoManager Provisioning enables the injection of cryptographic keys and other sensitive data into semiconductors and devices throughout a distributed supply chain. CryptoManager Provisioning capabilities cover a broad range of secure operations, including key delivery and programming, protection of debug and other sensitive ports, and feature configuration for chips and devices.

Secure Supply Chain

- Leverages securely provisioned keys and identities to enable supply chain integrity
- Provides device and data security for connected hardware

Trusted Identity

- Enables device OEMs and end users to cryptographically validate the identity of chips and devices at any point in the lifecycle
- Serves as the basis of managing keys and certificates required for intrinsic security purposes
- Establishes ecosystem-level trust between devices, services and data

Improved Profitability

- Provides “key material as a service” opportunities for the semiconductor and device OEMs
- Enables post-sale device monetization of additional key-based features and functions

Managed Service

CryptoManager Device Key Management is delivered exclusively as a managed service. Chipmakers and device OEMs typically require specific application services and security protocols driven by the security architecture of their specific offerings. To meet this need and provide for easy integration, Rambus can implement a custom, dedicated application gateway with associated APIs on behalf of the customer as part of the development effort.

Applications

- Memory chips and devices
- Automotive ECUs and sub-systems
- IoT MCUs and connectivity chips
- eSIM and iSIM chipsets
- Government (Supply Chain Integrity)
- Device lifecycle management services (e.g. firmware updates and feature activation)

rambus.com/cryptomanager

rev_20191022