ENT-AN1136

Application Note

Microsemi Intellisec™ FAQ

Released

Dec 2018

Contents

1 Revision History

The revision history describes the changes that were implemented in the document. The changes are listed by revision, starting with the most current publication.

1.1 Revision 2.0

In revision 2.0 of this document, formatting was updated.

1.2 Revision 1.0

Revision 1.0 was the first publication of this document.

2 Introduction

Recent reports on cybersecurity breaches highlights the need for critical network infrastructure protection, as enterprises and carriers alike move to cloud-based models. The security aspect also has implications for mobile 4G/LTE deployments and industrial networks. According to Hewlett-Packard's 2012 Cyber Security Risk Report, total security vulnerabilities are rising, with mobile vulnerabilities having grown 68% from 2011 to 2012 alone and 787% over the last five years.

Featured in Microsemi's SynchroPHY™ 1G, 10G, and 10G OTN physical layer devices, Intellisec IEEE 802.1 AE MACsec security encryption technology is the world's first and currently only FIPS 197-certified CGM-AES 256-bit strength flow-based MACsec, with legacy support for today's CGM-AES 128-bit strength field deployments.

Intellisec is the industry's first technology to enable flow-based IEEE 802.1AE MACsec security encryption end-to-end over any network, including multi-operator and cloud-based networks, independent of the network's awareness of security protocols. Other encryption technologies introduce variable delays, making it impossible to deliver the accurate IEEE 1588 timing required by TD-LTE, LTE-Advanced macro and small cell base stations and Smart Grid utility networks. Intellisec enables the industry's only secure 1588 solution available today, combining line-rate AES encryption with Microsemi's VeriTime™ IEEE 1588 nanosecond accurate timing.

As customers examine adopting Intellisec technology into their systems, a frequently asked set of questions are typically posed related to topics, such as interop with other MACsec implementations on the market, standards compliance, software, and more. The following questions and answers are provided for reference.

3 MACsec-Related Standards

What is the difference between 802.1X-2010, MKA, and KEYsec?

- MACsec Key Agreement (MKA) was defined in IEEE-802.1af as an amendment to 802.1X, adding MACsec key management functions.
- MKA is now encompassed by the IEEE-802.1X-2010 standard.

Are there any other documents I can read in order to better understand Intellisec, MACsec, 802.1X, MKA, KEYsec, supplicant, authentication, EAPOL, etc.?

- Yes, the following is a list of reference documents that can help explain the details.

IEEE-802.1AE-2006 (MACsec 128-bit): http://standards.ieee.org/getieee802/download/802.1AE-2006.pdf

IEEE-802.1AEbn-2011 (MACsec Amendment: 256-bit): http://standards.ieee.org/getieee802/download/802.1AEbn-2011.pdf

IEEE-802.1AEbw-2013 (MACsec Amendment: Extended Packet Numbering): http://standards.ieee.org/getieee802/download/802.1AEbw-2013.pdf

IEEE-802.1X-2010 (Port-based Network Access Control): http://standards.ieee.org/getieee802/download/802.1X-2010.pdf

Microsemi White Paper - Intellisec: Securing Cloud Services

Microsemi White Paper - Intellisec: Securing Carrier Ethernet Infrastructure and L2 VPN

Is a different encryption key used for every secure channel (SC) or every Secure association (SA) or both?

- Every SA, in a typical scenario there are two SAs for every SC. This is to allow hitless key rollover—one SA is currently in use, the other SA is preconfigured and becomes active at key rollover time. A complete answer is not possible as it ultimately depends on the shared medium.

What is the difference between standard MACsec and Intellisec?

The following are three critical innovations Microsemi Intellisec technology implements.

- Intellisec implements both port-based and tag-based MACsec encryption in a PHY.
  - Previous MACsec PHYs were only able to encrypt on a port-basis. Tag-based MACsec encryption allows encrypting at the edge of the network and runs over any L2 networks, including service provider multipoint Ethernet/MPLS VPN services. Confining the cost of encryption to just the edge, it also initiates multiple secure sessions from a single edge port. This could previously only be accomplished in expensive, standalone encryption appliances.
- Intellisec combines MACsec encryption with Microsemi's VeriTime, the industry's most accurate IEEE 1588v2 (1588) time stamping engine, without losing any timing accuracy.
  - Without Microsemi's Intellisec patent-pending technology, current MACsec implementations will seriously degrade 1588 timing accuracy. This is true, regardless of the location of the 1588 and MACsec implementation being in the PHY or the Switch/NPU/ASIC.
- Intellisec supports strong 256-bit GCM-AES encryption, in addition to, the more common 128-bit encryption.

Will equipment designed with Microsemi Intellisec PHYs be compliant to MACsec standard?

- Yes, any equipment designed with Microsemi Intellisec PHYs is capable of offering capabilities beyond the standard.

What is "tag-in-the-clear" (TIC) and how does it differ from Intellisec?

- TIC refers to the VLAN and MPLS Tag Bypass feature and is only one of the features of Intellisec.

Do I need Microsemi at both ends of the network if I want to use Microsemi's VLAN and MPLS Tag Bypass feature?

- Not necessarily, for example, if Microsemi is not used at the remote end the customer would need to use the two stage processing approach (described in the following question) at the remote end point.

Is it possible that the customer could maintain complete "MACsec specification compliance" and still achieve the same ability to use MACsec across a "MACsec agnostic network"?

- Yes, however, in order to do so, it would require two stages of processing. The first stage would perform the MACsec encryption per the specification and the second stage would add unencrypted tags (for example VLAN tags, MPLS headers). A network could then take this "post-processed" data and move it across the network without being MACsec "aware". This method is more expensive than the process implemented by Microsemi Intellisec PHYs, this method is completely MACsec specification compliant and interoperable with an Intellisec PHY enabled endpoint.

Is Intellisec compatible with other MACsec implementations on the market?

- Yes, if the VLAN and MPLS Tag Bypass are disabled (TIC is disabled) and the end point supports the same target level of encryption (128-bit/256-bit).

For other implementations currently on the market to perform what the TIC function can enable, it would require a two box setup at each end of the network, increasing the cost of implementation. Does complete "MACsec specification compliance" require that the VLAN tags and/or MPLS headers to be encrypted?

- Yes, please note that Intellisec PHYs provide both options—a customer can choose to encrypt VLAN /MPLS tags or leave them unencrypted.

I heard that the National Security Agency (NSA) has been working on a new Ethernet Security Specification (ESS). Where do I find this specification?

- The ESS can be obtained by accessing the public NCSMO website and navigating to the 'ESS Team' folder and 'Documentation' subfolder.

The new NSA ESS document v1.0 calls for 128-bit encryption for transmission of secret classified information and 192-bit encryption for transmission of top secret classified information. Do our PHYs need to support MACsec 192-bit encryption?

- No, the ESS document states that MACsec 256-bit encryption meets the requirements for both secret and top secret classification content since 256-bit encryption is stronger than 192-bit encryption.

What will happen to the downstream traffic in a user case where some devices in the network support 256-bit MACsec while some only support 128-bit MACsec?

- Only the 256-bit MACsec capable devices will be able to decrypt the 256- bit encrypted data. Microsemi PHY devices support both 128-bit and 256-bit MACsec.

4 Microsemi MACsec-enabled PHYs

What Microsemi products support MACsec features?

- The VSC8584, VSC8582, VSC8491, VSC8490, and VSC8258 PHYs all support MACsec features.

What is the capacity of the VSC8584, VSC8582, VSC8491, VSC8490, and VSC8258 PHYs when handling multiple VLANs, each one carrying flows with different keys?

- The VSC8584 and VSC8582 each offer up to 8-secure channels (SCs) and 16-secure associations (SAs).
- The VSC8491, VSC8490, and VSC8258 each offer up to 32-SCs and 64-SAs.

Can each of the SCs or SAs have a different VLAN tag?

- Yes, for example, the expected use case for the GE PHY is 8 full-duplex VLAN flows, which would use all 16 SAs.

Does Intellisec support operation where the VLAN tags and/or MPLS headers are not encrypted?

- Yes.

What is the largest packet size that our MACsec block will handle?

- 10K bytes

When a packet is encrypted, does the size of that packet change? If so, by how much?

- Yes, when a packet is encrypted it will become larger by 24-32 bytes due to the addition of the security tag and Integrity Check Value (ICV).

Can some of the ports of the PHY be programmed to support MACsec encryption while others do not?

- Yes.

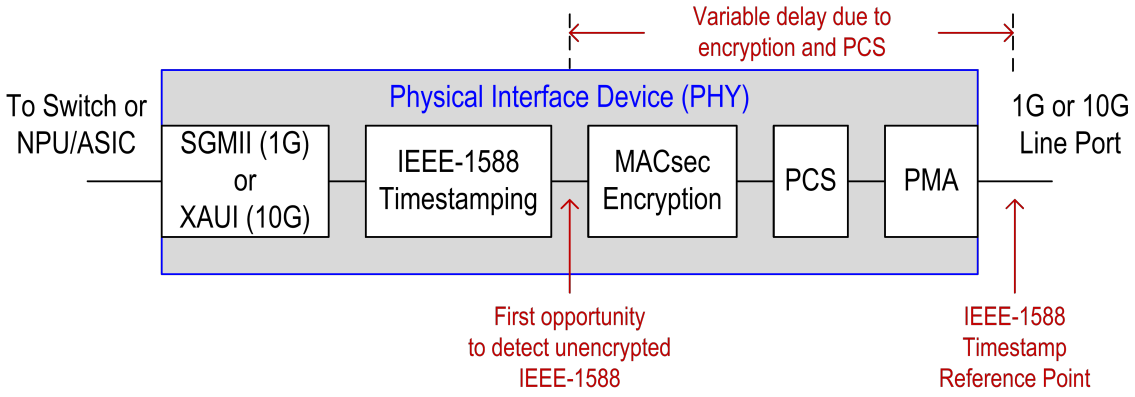
Can some of the ports of the PHY be programmed to support 128-bit MACsec encryption while others support 256-bit MACsec encryption?

- Yes, on the same port, these options can be selected flow-by-flow.

What is the challenge in enabling 1588 timestamping and MACsec encryption simultaneously on a port?

- High-accuracy 1588 requires timestamping at the physical port, but a received 1588 frame can only be detected and processed after it is decrypted. MACsec processing introduces highly variable delays. Standard MACsec destroys 1588 accuracy, even if 1588 remains unencrypted while other data is encrypted.
  For example, if the 1588 packet is immediately behind a packet that will be encrypted later, the encrypted packet grows by 24-32 bytes. This delays the 1588 packet by 192-256 ns compared to the case where the 1588 packet is behind a packet that won't be encrypted. Microsemi's solution maintains 1588 nanosecond-accuracy with MACsec enabled for both one-step and two-step.

Figure 1 • Physical Interface Device (PHY)



Is Microsemi the only vendor that has solved the packet delay variation (PDV) effect when MACsec is applied to 1588 PTP packets?

- Yes.

Is there a report for 1588v2 accuracy & latency test results with Intellisec/MACsec enabled for both Microsemi's 1G PHYs and 10G PHYs?

- Yes, this report is available upon request.

If I am designing a MACsec GE SFP module and all 16 SAs are active, and my NPU/Switch is running the 802.1X stack with KEYsec/MKA support, would the 100 kHz I2C bus (as specified per the SFP MSA standard) be sufficient to support the key rollover?

- Yes.

If I am designing a 4-port 10GE wireless access point with an integrated switch and want to add MACsec support, is this possible?

- Yes, MACsec can be moved over a Wi-Fi network.

In such a design where there is only a single 4-port 10GE PHY is the MDIO interface (running at 12.5 MHz) sufficient for supporting the rollover of KEYsec keys at line rate where each port has 64 SAs? What if more than one 4-port 10GE PHY is used in a system design?

- Yes, if there is more than one 4-port 10GE PHY used in a system design, the 4-pin SPI interface running at 25 MHz is the recommend serial interface for supporting KEYsec rollover.

What interoperability tests have been performed between Microsemi's Intellisec and other MACsec implementations?

- Microsemi has published an Interop report with a MACsec-enabled Cisco 3560 switch.
- Microsemi is FIPS 197 certified, ensuring compliance to the standard and interoperability with other FIPS 197 solutions.
- Microsemi successfully completed UNH IOL MACsec interop testing, reports are available.

What proof does Microsemi have that Intellisec has been NIST CAVP/FIPS 197 certified at both GCM-AES 256-bit and 128-bit encryption standards?

- Please visit the NIST website and search for "Microsemi".

Why is FIPS 197 certification important?

- FIPS 197 certification is a significant step toward FIPS 140-2 certification, which opens new market opportunities for the following customer products: U.S. Government network infrastructure equipment (NSA, FBI, and CIA), HIPAA-compliant network equipment, PCI-compliant network equipment, Sarbanes-Oxley compliant network equipment, and U.S. and select International Military network equipment.

5 Microsemi Intellisec PHY Software

What are the software components required to enable MACsec functionality in a customer system using Microsemi Intellisec-enabled PHYs?

- Microsemi Unified API software: provides device-specific register access and application-layer software APIs. In addition to other PHY device control interfaces, the Unified API software provides a MACsec API for use by higher layer software (either commercial third-party or customer-supplied).
  - The Microsemi MACsec API is modelled according to the IEEE standard 802.1AE-2006. It includes full support for the following:
    IEEE 802.1AE-2006 compliance supporting GCM-AES-128
    IEEE 802.1AEbn-2011 compliance supporting GCM-AES-256
- KEYsec (802.1X) software: provides the security control protocols described in IEEE 802.1AE and 802.1X, such as MACsec Key Agreement (MKA) and Extensible Access Protocol over LAN (EAPOL).

Where is the API for the MACsec engine in the PHY?

- Support for the MACsec API is included in the Microsemi Unified API, available today, VSC6802API v4.48 (and later).

Microsemi Headquarters
One Enterprise, Aliso Viejo,
CA 92656 USA
Within the USA: +1 (800) 713-4113
Outside the USA: +1 (949) 380-6100
Sales: +1 (949) 380-6136
Fax: +1 (949) 215-4996
Email: sales.support@microsemi.com
www.microsemi.com

VPPD-03839